

ESPECIALIDAD FORMATIVA GESTIÓN DE REDES DE VOZ Y DATOS IFCM0310

UF1872: Implementación y configuración de pasarelas

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en la plataforma denominada Portal del Alumno, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de propiedad intelectual vigente en España.

* Bibliografía usada en este documento:

UF1872: Implementación y Configuración de pasarelas, Autor: Gopal Bijani Chiquero, EDITORIAL ELEARNING S.L. Edición: 5.2

Capturas de pantalla y textos electrónicos de varias web únicamente para ilustrar la actividad educativa

Contenido

Comprobación del cableado.....	5
Tipos de corriente eléctrica.....	5
Conceptos:.....	5
Resistencia.....	5
Intensidad.....	5
Voltaje.....	5
Aparatos de Medida	5
Multímetro (polímetro).....	6
Medir continuidad.....	7
Medir Voltaje	7
1. Redes de comunicaciones de voz y datos	10
1.1 Elementos de una red de comunicaciones.....	10
Medios de transmisión	10
Tarjetas o Adaptadores de red	10
Equipos de interconexión.....	10
1.2. Niveles funcionales de una red de comunicaciones.....	10
Vídeos: Curso de Fibra óptica	11
Resumen de los Vídeos:.....	12
Video 5:.....	17
Empalmes:.....	17
Video 6:.....	18
Video 10:.....	22
Video 11:.....	23
Video 12:.....	27
Video 14:.....	30
Video 15:.....	31
Video 16:.....	32
1.2.1. Red de acceso	34
1.2.2. Red troncal de transporte	34
1.2.3. Red de distribución.....	34
1.3. Multiplexación	35
1.3.1. Multiplexores.....	35
1.3.2. Técnicas de multiplexación.....	36
1.4. Funciones de comutación, transporte y señalización	37
2. Arquitectura de redes de voz y datos.....	40
2.1. Redes de acceso: guiadas y no guiadas	40
2.1.1. Redes de acceso vía cobre: xDSL	40

2.1.2. Redes de acceso vía radio: WLL, MMDS, LMDS.....	43
2.1.3. Redes de acceso vía fibra óptica: HFC, PON y CWDM	46
2.2. Redes troncales.....	51
2.2.1. MTA (Modo de transferencia asíncrono – ATM).....	52
2.2.2. JDP (Jerarquía Digital Plesiócrona – PDH)	53
2.2.3. JDS (Jerarquía Digital Síncrona – SDH).....	55
2.3. Mecanismos de codificación y cifrado de la información	56
2.4. Sistemas de seguridad en el transporte de datos	67
3. Servicios de comunicaciones	73
3.1. Servicios de voz.....	73
3.2. Servicios corporativos y de red inteligente	76
3.3. Servicios de datos, servicios IP. Telefonía IP	77
3.4. Servicios telemáticos e interactivos	86
3.5. Otros servicios de valor añadido	87
3.6. Criterios de calidad de servicio (QoS).....	89
3.7. Control de retardos y congestión	89
4. Implementación y configuración de pasarelas.....	91
4.1. Tipos y funciones de pasarelas. Servicios que soportan	91
4.3. Condiciones de instalación de la pasarela	95
4.3.1. Análisis de los mapas de direcciones IP.....	95
4.3.2. Análisis de las líneas y nodos de transmisión de voz	97
4.4. Parámetros de configuración	98
4.4.1. Parámetros de configuración de servicios	98
4.4.2. Parámetros de seguridad	100
4.4.3. Información sobre la configuración de red del operador	100
4.5. Herramientas de configuración	101
4.6. Protocolos de gestión	101
4.7. Parámetros de calidad en el servicio.....	102
4.8. Pruebas funcionales y estructurales.....	103
4.9. Comandos para el mantenimiento y resolución de problemas	104
4.10. Normativa ambiental y estándares de señalización y digitalización	112
5. Equipos de conmutación telefónica. «Call Managers»	114
5.1. Equipos de conmutación telefónica.“Call managers”	114
6. Mercado de las telecomunicaciones	119
6.1. Situación de las telecomunicaciones. Marco legal y organismos de normalización	119
6.2. Principales servicios de telecomunicaciones.....	120
Servicio de telefonía	120
Servicio de televisión	121
Servicio de datos.....	122

6.3. Agentes en el mercado de las telecomunicaciones.....	122
6.3.1. Fabricantes y suministradores.....	123
6.3.2. Proveedores de servicio	123
6.3.3. Operadores	124
6.3.4. Perfiles de las operadoras	125
6.3.5. Usuarios. Derechos de los usuarios de telecomunicaciones.....	125
RESUMEN.....	127

Comprobación del cableado

Tipos de corriente eléctrica.

Básicamente existen dos tipos de corriente eléctrica: Corriente continua y corriente alterna:



Corriente continua (C.C. o D.C.).

La corriente continua: La intensidad de corriente circula siempre en el mismo sentido y con un valor constante.

La producen dínamos, pilas, baterías, acumuladores.

Corriente alterna (C.A. o A.C.).

La corriente alterna: La intensidad de corriente circula alternativamente en dos sentidos, variando al mismo tiempo su valor.

La producen los generadores de C.A.

Conceptos:

Resistencia

La resistencia eléctrica es una propiedad que tienen los materiales por la que se oponen al paso de la corriente.

Los conductores tienen resistencia eléctrica baja, mientras que en los aislantes tienen resistencia eléctrica alta. Esta propiedad se mide en Ohm (Ω).

Intensidad

La corriente eléctrica o intensidad eléctrica es el flujo de carga eléctrica por unidad de tiempo que recorre un material. La corriente eléctrica es la circulación de cargas eléctricas en un circuito eléctrico.

La corriente eléctrica se debe al movimiento de los electrones, de las cargas en el interior del material.

En el Sistema Internacional de Unidades se expresa en amperios, es decir C/s (coulombios por segundo).

La intensidad de corriente eléctrica expresada en Amperios (A).

Voltaje

El voltaje o diferencia de potencial eléctrico, es una magnitud física, con la que podemos cuantificar la diferencia de potencial eléctrico o la tensión eléctrica entre dos puntos.

Es una comparación de la energía que experimenta una carga entre dos ubicaciones físicas.

El símbolo con el que se representa el voltaje o tensión eléctrica es V

Aparatos de Medida

Medir significa determinar experimentalmente el valor de una magnitud física con un instrumento o dispositivo adecuado y verificar cuántas veces es mayor o; menor este valor que la unidad de la magnitud en cuestión.

Existen dos métodos de medición de magnitudes eléctricas:

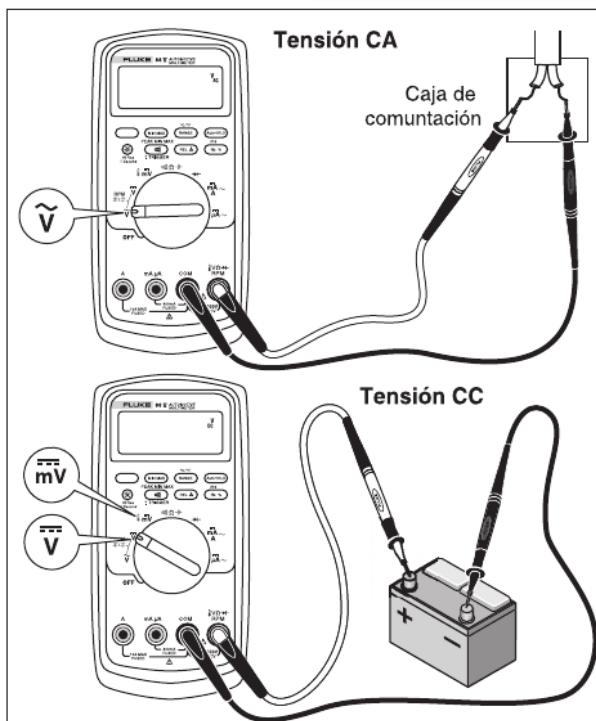
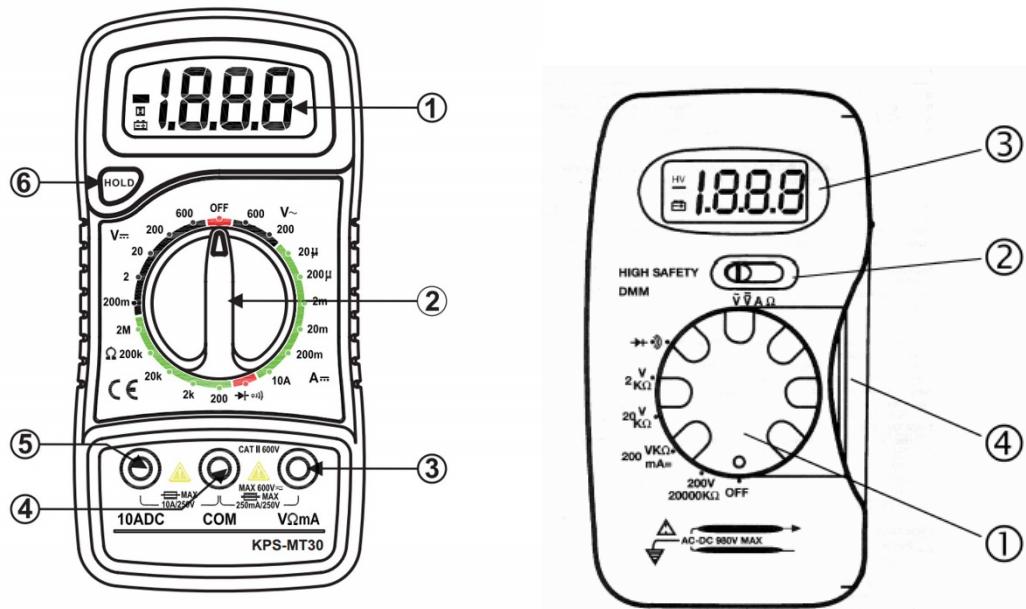
- La medición de desviación con instrumentos de medición directa.
- La medición por comparación por medio de puentes o compensación.

En el primer método se usan dispositivos de medida con indicación analógica o digital que permiten leer directamente la magnitud a medir o calcularla partiendo de la indicación. En el segundo caso, un dispositivo de medida apropiado sirve por comparación con otra conocida de la misma índole.

Hay diferentes aparatos de medida eléctrica:

- ⇒ Amperímetro
- ⇒ Voltímetro
- ⇒ Ohmímetro
- ⇒ Multímetro (polímetro)
- ⇒ Tester RJ45
- ⇒ Tester RJ11
- ⇒ Comprobadores de fibra óptica

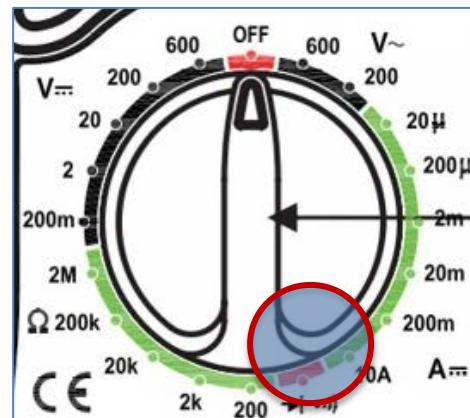
Multímetro (polímetro)



Medir continuidad

Para medir continuidad de cualquier cable: par trenzado, coaxial, alimentación....

Lo ponemos en el símbolo del diodo (componente electrónico que permite la circulación de la corriente eléctrica a través de él en un solo sentido) o uno similar a una wifi dentro del rango de medida en ohmios (Ω) (oposición al flujo de corriente en un circuito eléctrico)

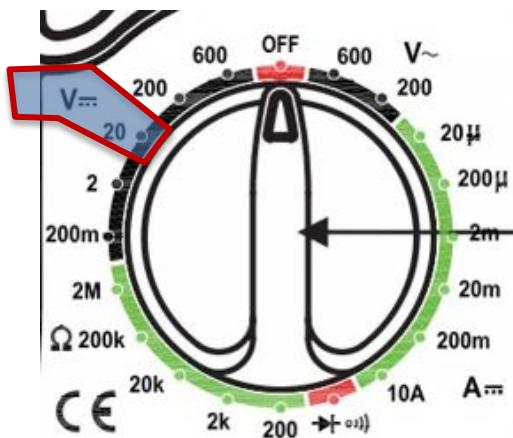


Medir Voltaje

Si miramos el cargador (transformador de corriente alterna en continua) nos dice que tendrá entre 18 y 20V

Con lo cual ponemos la ruleta del multímetro en la V con la raya continua ($V=$) en la posición 20.

Y tenemos que tocar con el electrodo negro la parte exterior del conector del transformador y con el rojo la parte interior.



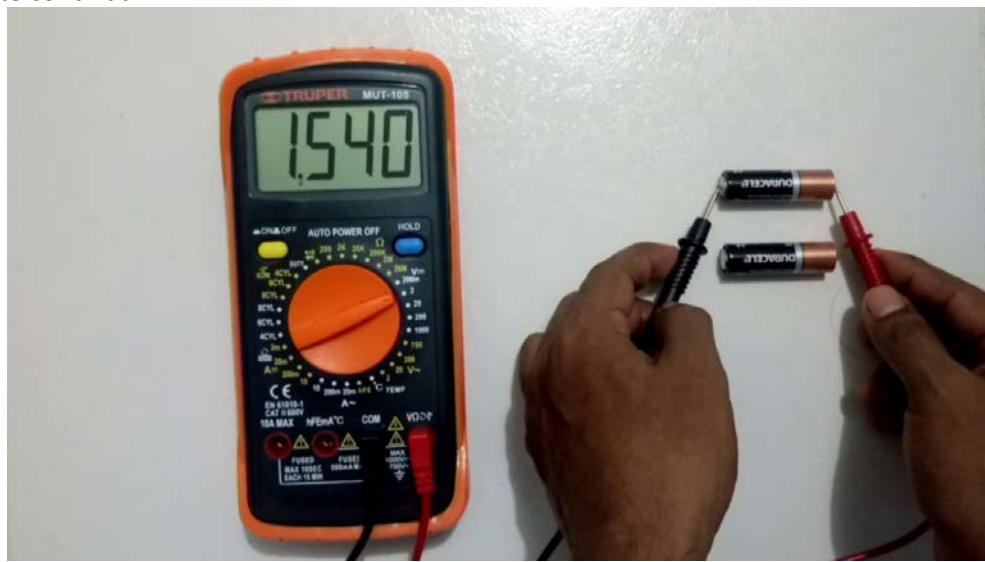
El De los móviles es de 5 V, así que lo dejamos en corriente continua (V=) en la posición 20, porque 2 es muy poco. Y tenemos que tocar los extremos del terminal (mini/micro USB,USB-C) del cargador con los electrodos, seguramente tendremos que ayudarnos de cualquier cable pelado para hacer buen contacto.



Para la batería de portátil, tendremos que localizar los polos positivo y negativo y mantendremos el Voltaje en Corriente continua y la escala en 20.



En cambio, para las pilas pequeñas: AA/AAA cuyo voltaje es de 1.5 V, tendremos que cambiar la escala a 2 de V corriente continua:



Y medir Voltaje en las regletas de Corriente Alterna cambiaremos a la V con la virgulilla ~ e insertaremos los electrodos en los 2 agujeros del enchufe (con cuidado) y lo pondremos en 600 ya que la corriente alterna en España es de 220V a una frecuencia de 50Hz



1. Redes de comunicaciones de voz y datos

1.1 Elementos de una red de comunicaciones.

Una red de comunicaciones está formada por un conjunto de elementos que permite la transmisión de información y datos entre diferentes equipos.

En este sentido, una red de comunicaciones fundamentalmente la forman los siguientes elementos:

Elementos	Funcionalidad
Equipos de interconexión	Son los elementos que permiten interconectar diferentes redes.
Medios de transmisión	Son los elementos que permiten conectar equipos de interconexión y equipos finales a una red.
Equipos finales	Son los elementos que generan o reciben los datos. Deberán estar equipados con los adaptadores de red necesarios.

Medios de transmisión

Visto en UF1869 – Ud. 3 (Página 94)

Visto en UF1870 – Ud. 2.8.1 (Página 114)

Medios de transmisión guiados y no guiados

El par trenzado: UTP, STP, FTP

El cable coaxial: delgado y grueso, banda base y banda ancha

La fibra óptica: monomodo y multimodo

Visto en UF1869 – Ud. 4 (Página 141) Medios no guiados: Transmisión por radiofrecuencia

Tarjetas o Adaptadores de red.

Visto en UF1870 – Ud. 2.10 (Página 127)

Tarjetas de red para redes cableadas: RJ-45, BNC

Tarjetas de red para redes inalámbricas

Equipos de interconexión.

Visto en UF1869 – Ud. 7 (Página 206) y Visto en UF1870 – Ud. 2.9 (Página 125)

Repetidores o Hub

Puente o switch

Punto de acceso

Encaminador o Router

Pasarelas o Gateways

1.2. Niveles funcionales de una red de comunicaciones

Para que los servicios de telecomunicaciones lleguen a los usuarios y equipos finales es necesaria una red que distribuya dichos servicios desde donde se generan hasta la ubicación donde están estos usuarios y equipos finales.

Así, las redes pueden ser más o menos grandes ya que implica su distribución por urbanizaciones, calles, edificios, hogares, etc.

Es por ello que la red presenta tres niveles funcionales.

Nivel de acceso

Es la parte de la red que hace que dichos servicios de telecomunicaciones lleguen hasta los hogares o sedes de empresas. Da el 'acceso' a estos usuarios.

Nivel troncal de transporte

Es la parte de la red que da servicio al nivel de acceso y constituye la parte de red que tiene la mayor capacidad de tráfico que luego se capilariza en los niveles de acceso. También es denominado habitualmente como **backbone**. Se encarga en definitiva de que los servicios puedan llegar a cualquier situación geográfica.

Nivel de distribución

Es la parte de la red que se encarga de la comutación y multiplexación de la información que procede de los proveedores de servicio y adaptarla a las características de la red troncal de transporte.

Vídeos: Curso de Fibra óptica

Vídeos muy interesantes sobre el funcionamiento de la fibra óptica y como llega hasta el usuario final.

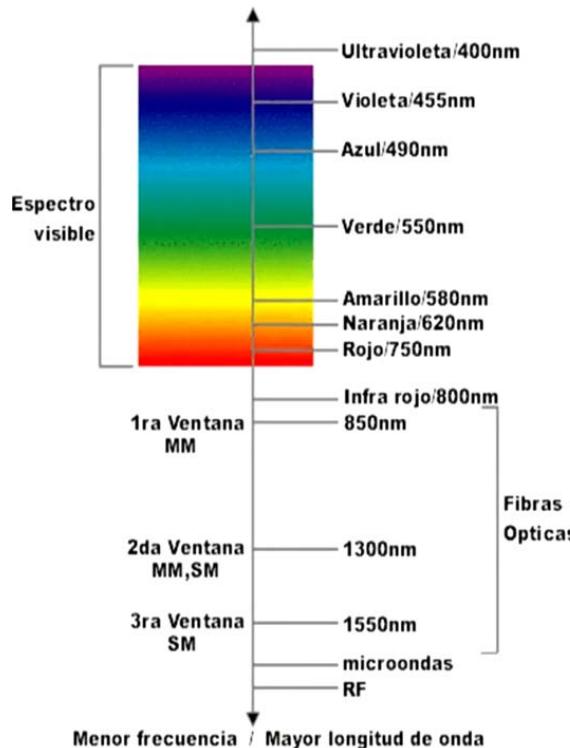
Estos vídeos nos sirven de introducción para entender los conceptos que tenemos que estudiar en los capítulos siguientes:

1. https://www.youtube.com/watch?v=M-PahKowgVM	Introducción
2. https://www.youtube.com/watch?v=WgHL3CWQRpc	En este video sentaremos las bases para entender los siguientes capítulos del curso. Nos introduciremos en la estructura de red FTTH, hablaremos de sus elementos Splitter, ONT y OLT, y del lugar donde se instalan.
3. https://www.youtube.com/watch?v=2nHnJl84EXU	Veremos una breve introducción de los protocolos que utilizamos al enviar y recibir la información en redes FTTH, así como las distintas longitudes de onda y su utilización.
4. https://www.youtube.com/watch?v=iIF-K8coKdc	En este video, vamos a poder ver y visitar los diferentes elementos que tiene la operadora en central..OLT, ROM, galería de cables, etc.
5. https://www.youtube.com/watch?v=wO4KR6hU-oM	En este video veremos cómo se llevan los cables de F.O. desde la sede de la operadora hasta el edificio del cliente, pasando por los diferentes elementos que nos podremos encontrar en el despliegue: cables, cajas de empalme, cámaras de registro, etc.
6. https://www.youtube.com/watch?v=kz_fGKZhpwl	Hoy veremos las cajas ópticas que se instalan en los edificios de cliente, en concreto, en fachadas y postes. Estas cajas son preconectorizadas y podrás ver la forma de conectar la acometida hasta el cliente.
7. https://www.youtube.com/watch?v=oPpSBwIxXDg	Cuando introducimos la acometida de fibra en cliente, podemos realizar una transición de cable, se denomina Roseta en paso. Presta atención a la colocación de la fibra en las Rosetas ya que es la parte más delicada de la instalación.
8. https://www.youtube.com/watch?v=-q-BmCwVLqE	Las cajas ópticas de exterior se instalan en distintos elementos de la Planta exterior, según la infraestructura del edificio del cliente. Podréis ver los entornos más comunes de instalación.
9. https://www.youtube.com/watch?v=l60GJQfdBdY	Actualmente, el proceso de fusionado de fibra óptica es sencillo y rápido gracias a la evolución en las máquinas de empalme. Para una buena finalización, es imprescindible tener cuidado en la limpieza de la máquina de empalme y la fibra óptica. Te lo mostramos en detalle.
10. https://www.youtube.com/watch?v=EcG7mC7f83w	En este video podrás ver una iniciación a los ajustes básicos de una maquina fusionadora y a los mantenimientos mínimos que puede requerir. No olvides leer los manuales del fabricante de la que utilices, te ahorrará mucho tiempo y alargará el tiempo útil de la herramienta.
11. https://www.youtube.com/watch?v=Dv2ePLjZpw	En este video podremos ver, como es el despliegue dentro de un edificio y la forma de actuar en cajas preconectorizadas para llegar al domicilio del cliente.
12. https://www.youtube.com/watch?v=2fOi0Y6088w	En este video, seguimos en el edificio de cliente, pero vamos a ver un tipo de despliegue diferente. Son cajas sin preconectarizar, donde las fibras tendremos que fusionarlas, en todos los puntos del despliegue de cliente. Concretamente vamos a ver el manejo de las fibras del divisor y del "Riser", en la Caja Terminal Optica.
13. https://www.youtube.com/watch?v=RZHdp18jlgw	En este video terminaremos la instalación empezada en el video anterior. Concretamente veremos la caja de derivación, que se instala en las diferentes plantas del edificio, para poder dar el servicio de fibra de una manera más sencilla para el instalador, acercando la fibra, al domicilio de cliente.
14. https://www.youtube.com/watch?v=BBkPLBtNTTl	En este video, podremos ver la instalación de equipos en el domicilio de cliente y las diferentes opciones que nos pueden ofrecer las operadoras.
15. https://www.youtube.com/watch?v=WLILwAw6Cpk	En este video podremos ver la importancia de la limpieza en los conectores de fibra óptica y las diferencias con las redes fusionadas.
16. https://www.youtube.com/watch?v=kspS_XyDqws	Para la detección de incidencias en la fibra óptica, tenemos tres herramientas que nos facilitan tanto la instalación como su posterior mantenimiento. Veremos una breve introducción y su funcionamiento.

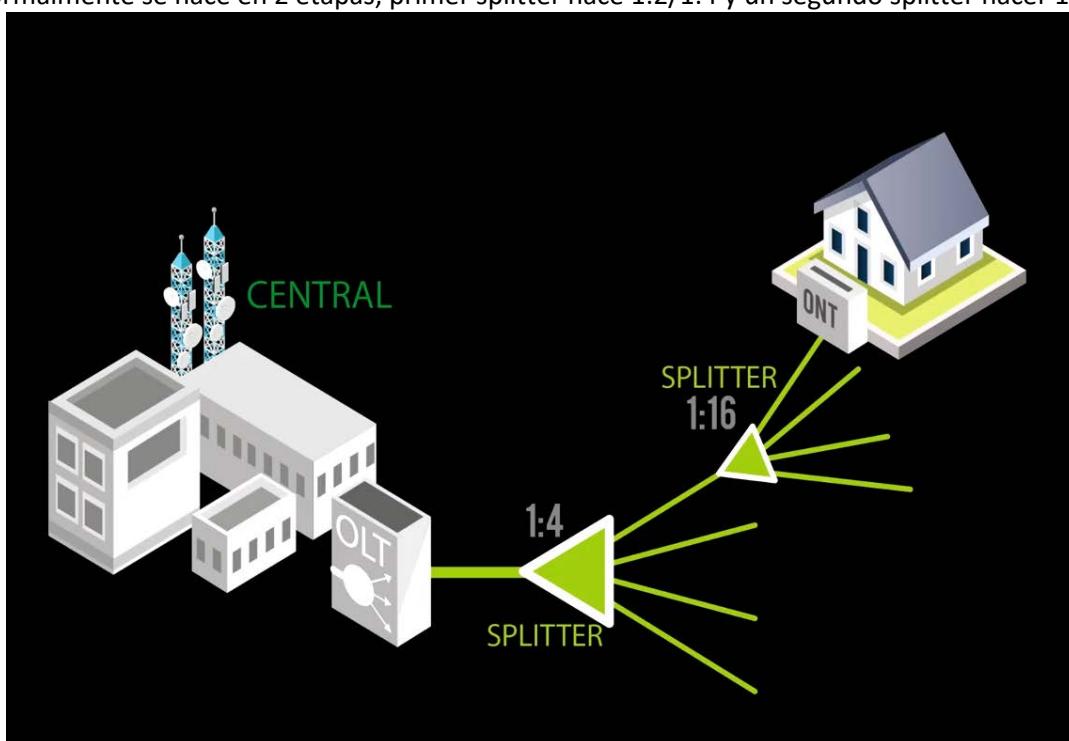
Resumen de los Vídeos:

Queremos ver como esta montada la estructura de la red, desde la distribuidora hasta los hogares:

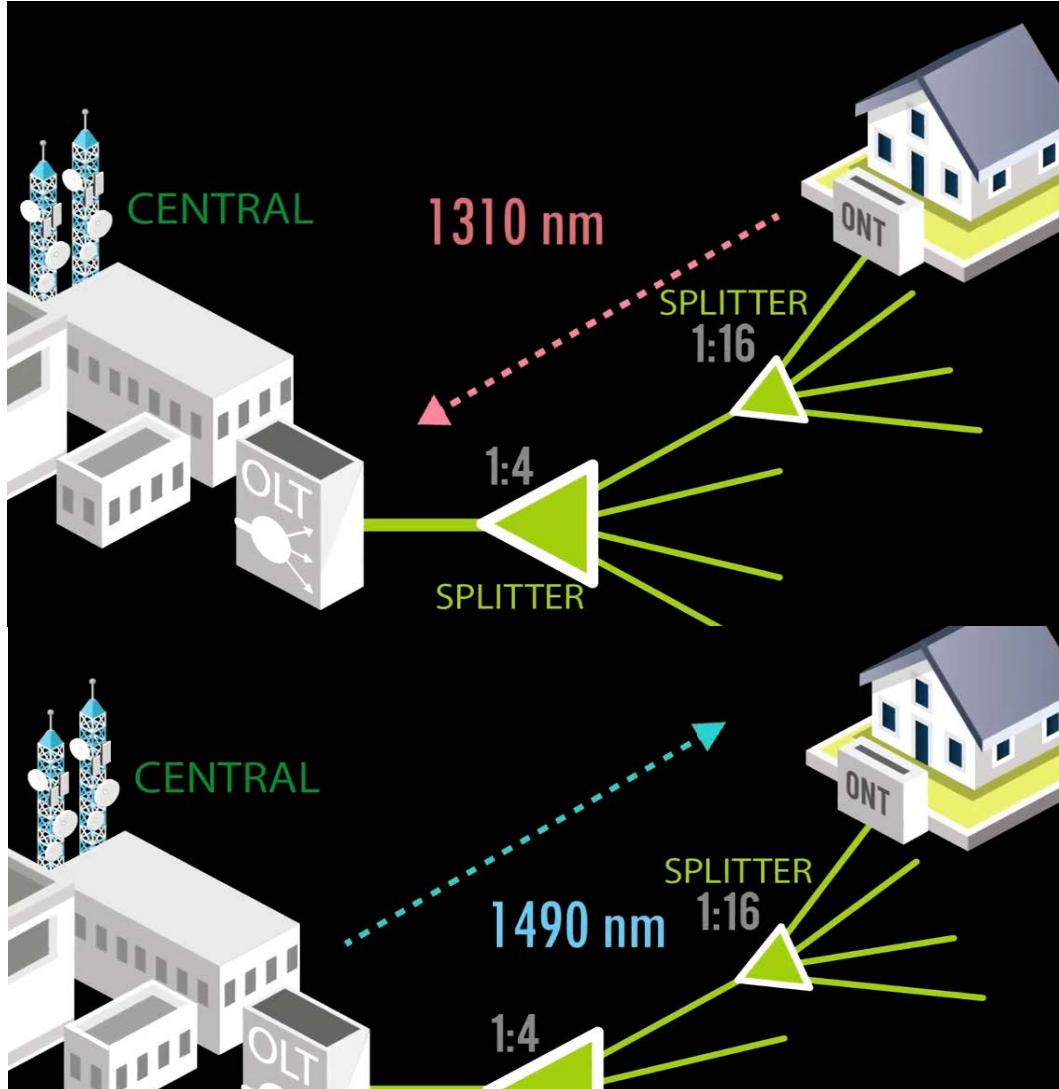
- ⇒ Red FTTH (Fiber To The Home)
- ⇒ 3 ventanas de longitudes de onda (no visibles): 850nm, 1300nm, 1550nm



- ⇒ GPON: Gigabit Passive Optical Network
- ⇒ Punto/Multipunto: De una fibra que sale de central llega a varias fibras de clientes
- ⇒ Fibra bidireccional: con una sola fibra hace transmisión y recepción
- ⇒ ONT: Convierte la señal de óptico a eléctrico en el domicilio del cliente (activo)
- ⇒ OLT: Dispositivo de oficina central
- ⇒ Splitter: Divisor Óptico (Pasivo) El laser llega por una de las entradas y sale por varias salidas.
- ⇒ Normalmente se hace en 2 etapas, primer splitter hace 1:2/1:4 y un segundo splitter hacer 1:8/1:16

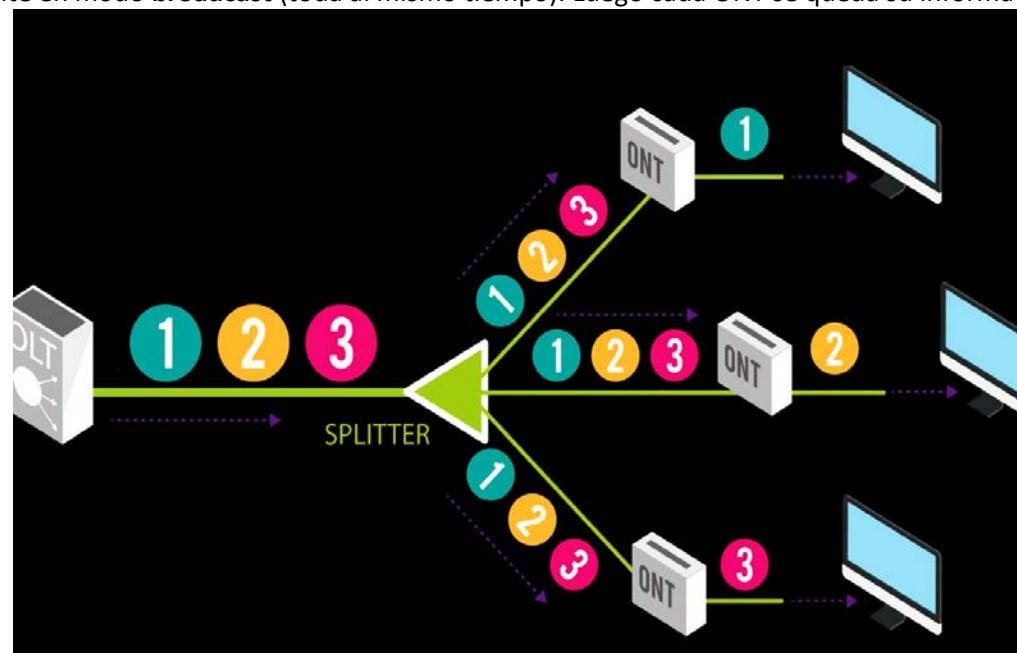


Señal **bidireccional**: landa (onda) de 1490 de la OLT a la ONT y 1310nm de la ONT a la OLT de bajada:

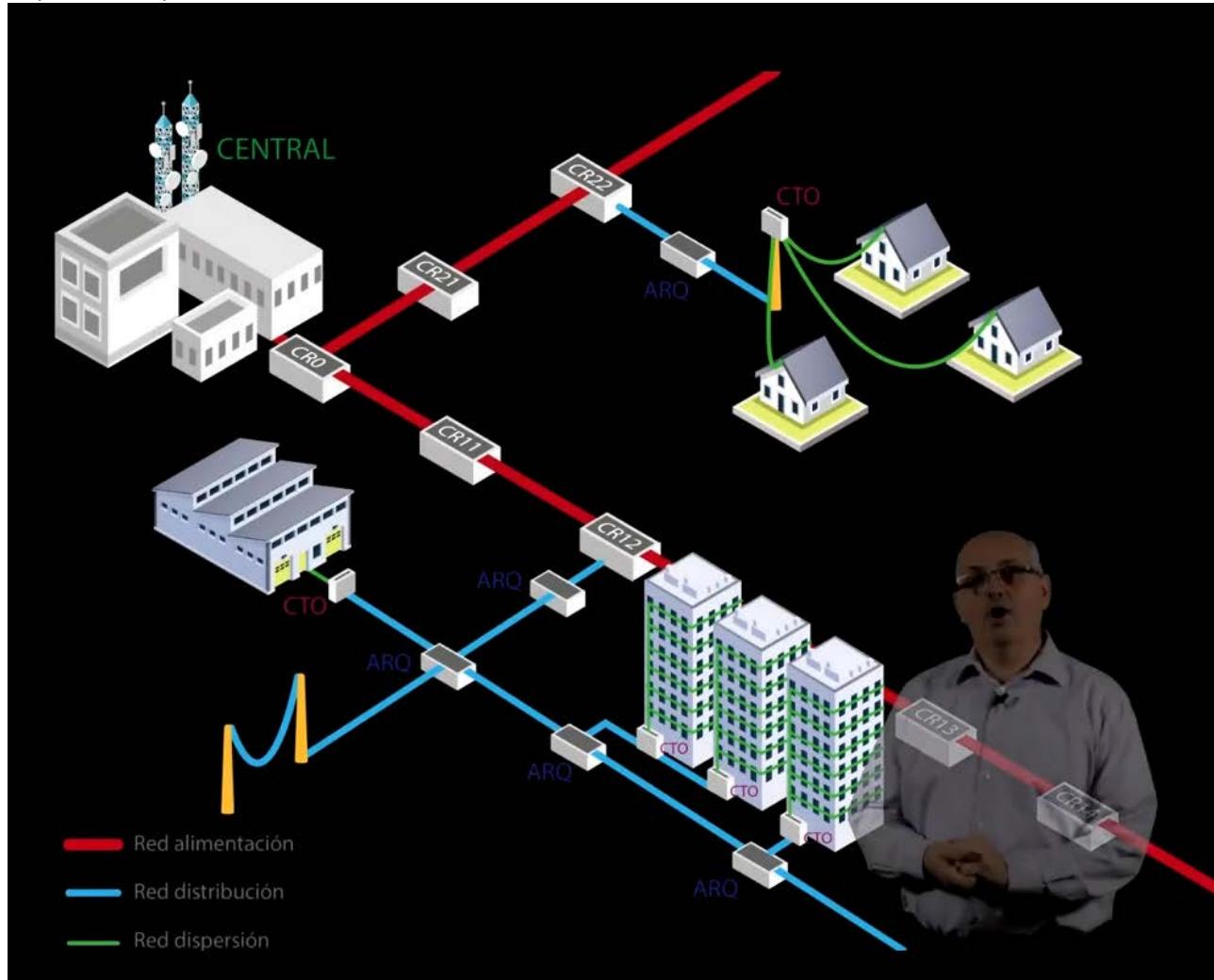


Mediante login y password, número de serie u otro sistema de autenticación se autentica y se le asigna un SLOT temporal. Que se le asigna por TDMA (Time Division Multiple Access).

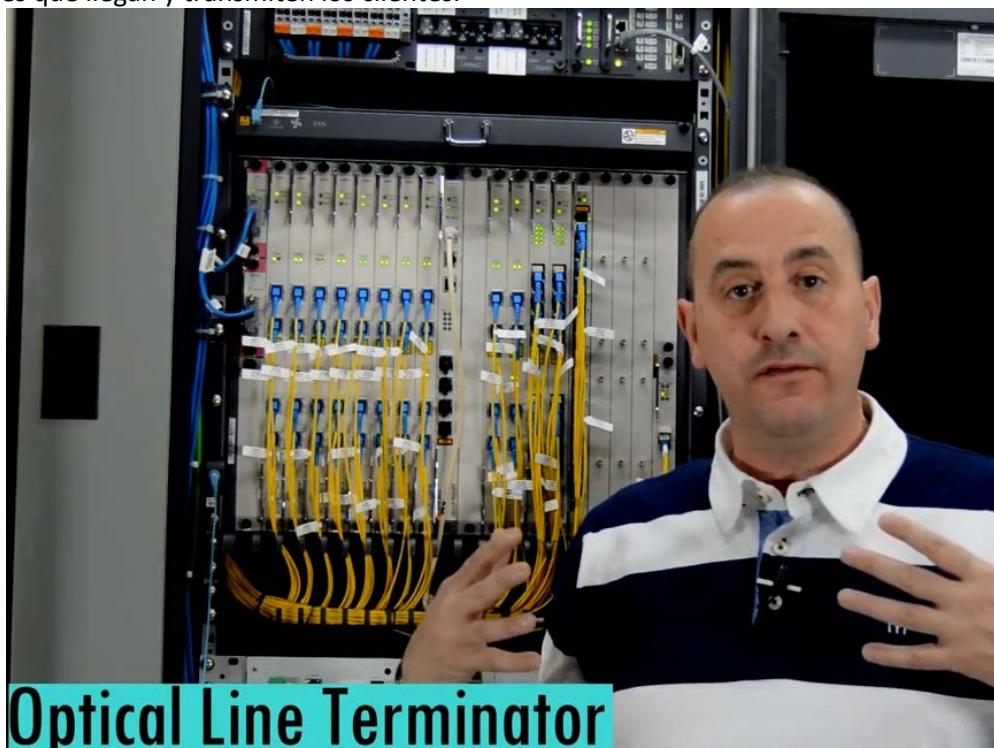
Y transmite en modo **broadcast** (toda al mismo tiempo). Luego cada ONT se queda su información:



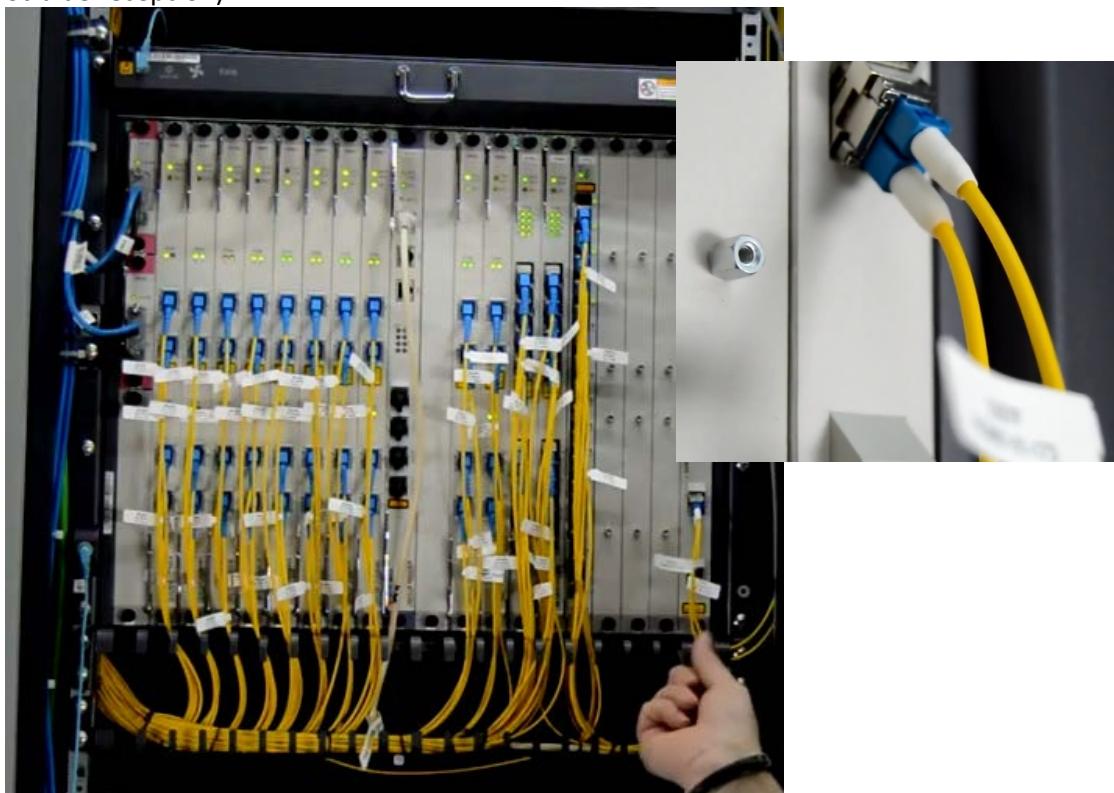
Esquema completo:



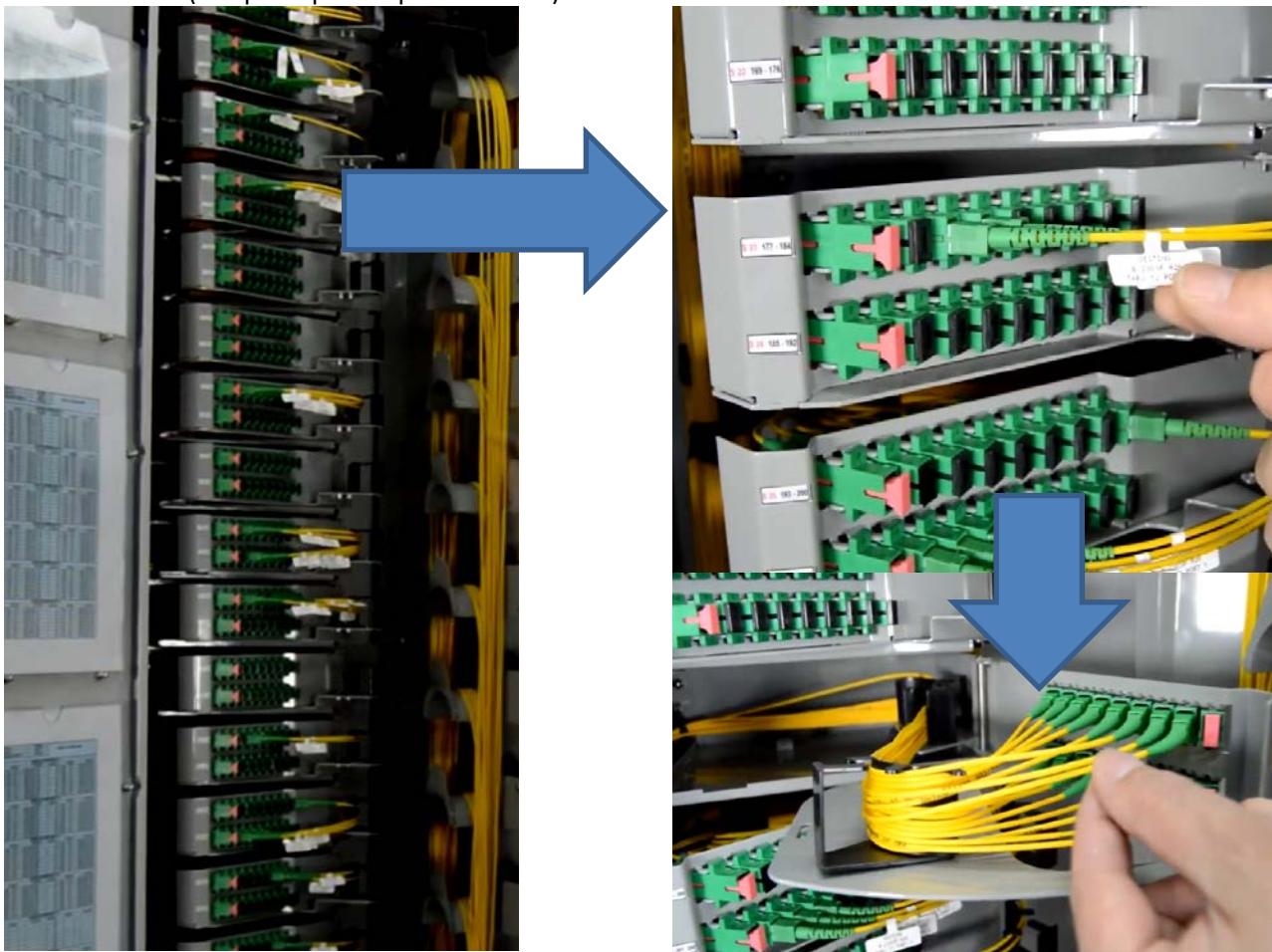
En la central nos encontramos con la OLT (Optical Line Terminator), concentrador que llegan todas las informaciones que llegan y transmiten los clientes.



A cada OLT llega una fibra (bidireccional) y luego de todas las OLT juntas salen 2 fibras una de transmisión y otra de recepción)



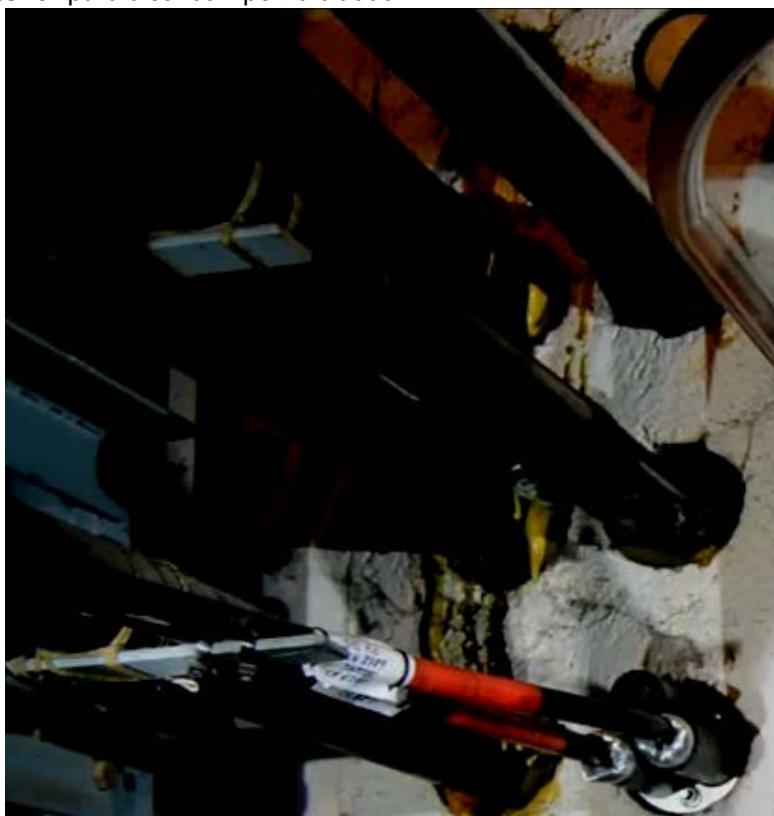
ROM: Repartidor Optico Modular. Llegan las fibras de la OLT o de otros equipos de transmisión con las fibras de alimentación (las que reparten por la ciudad)





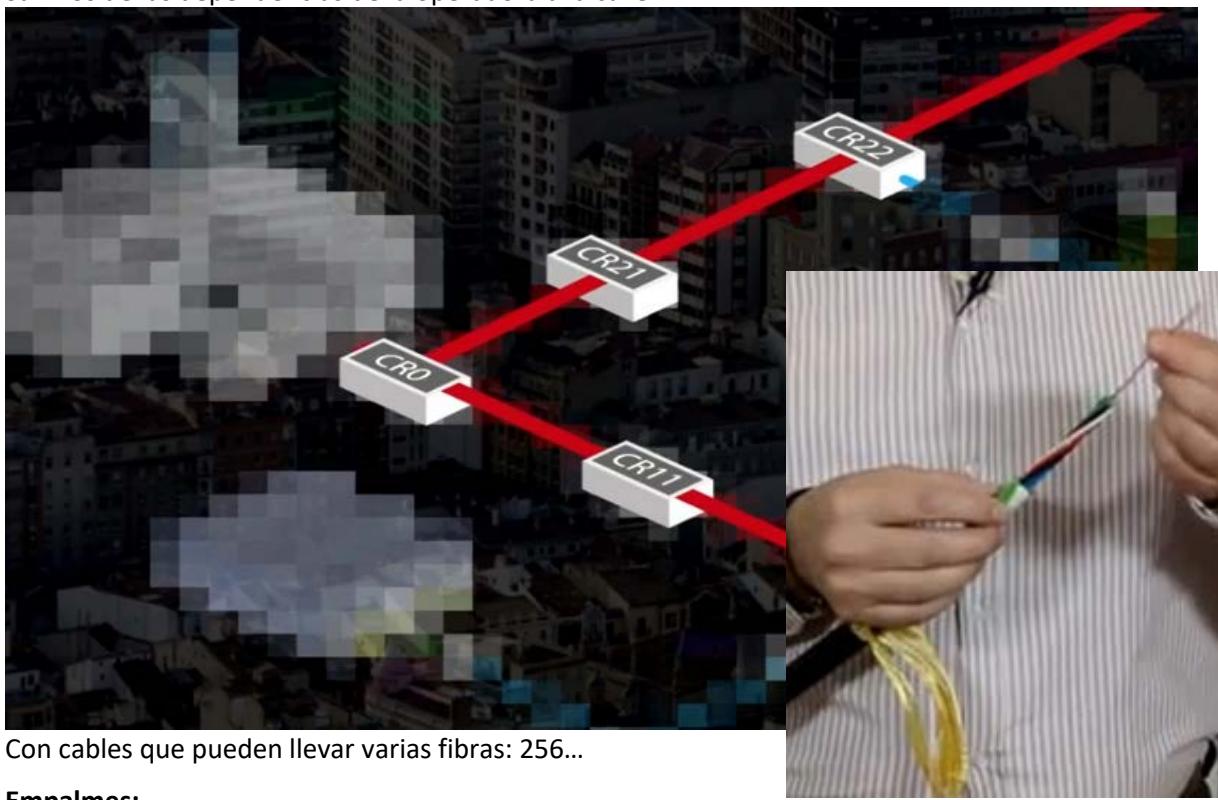
Del ROM baja a la sala de cables:

Los cables van de la OLT al ROM y luego bajan a la sala de cables van a los conductos que son donde salen los cables hacia el exterior para distribuir por la ciudad:



Video 5:

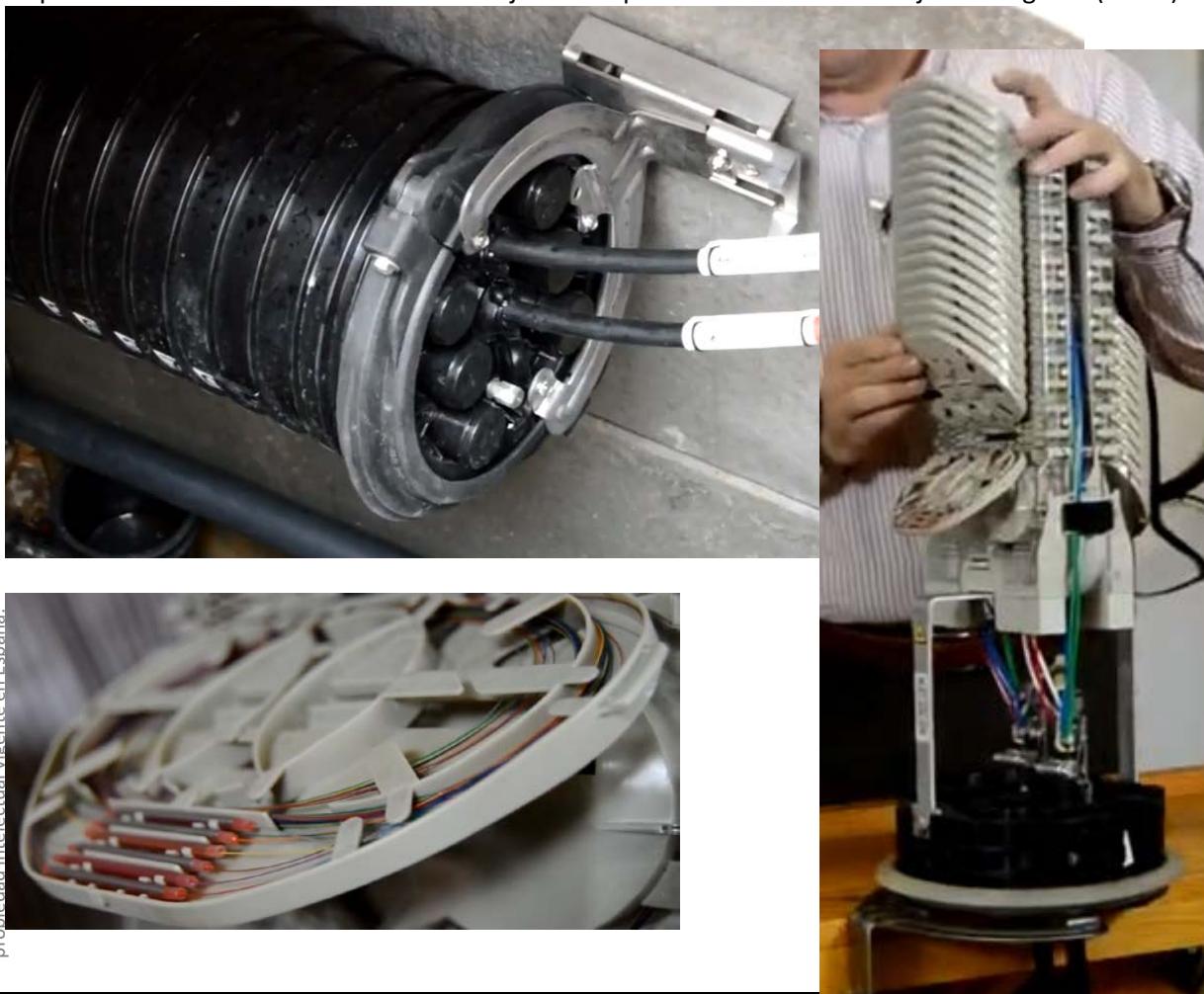
Salimos de las dependencias de la operadora a la calle:



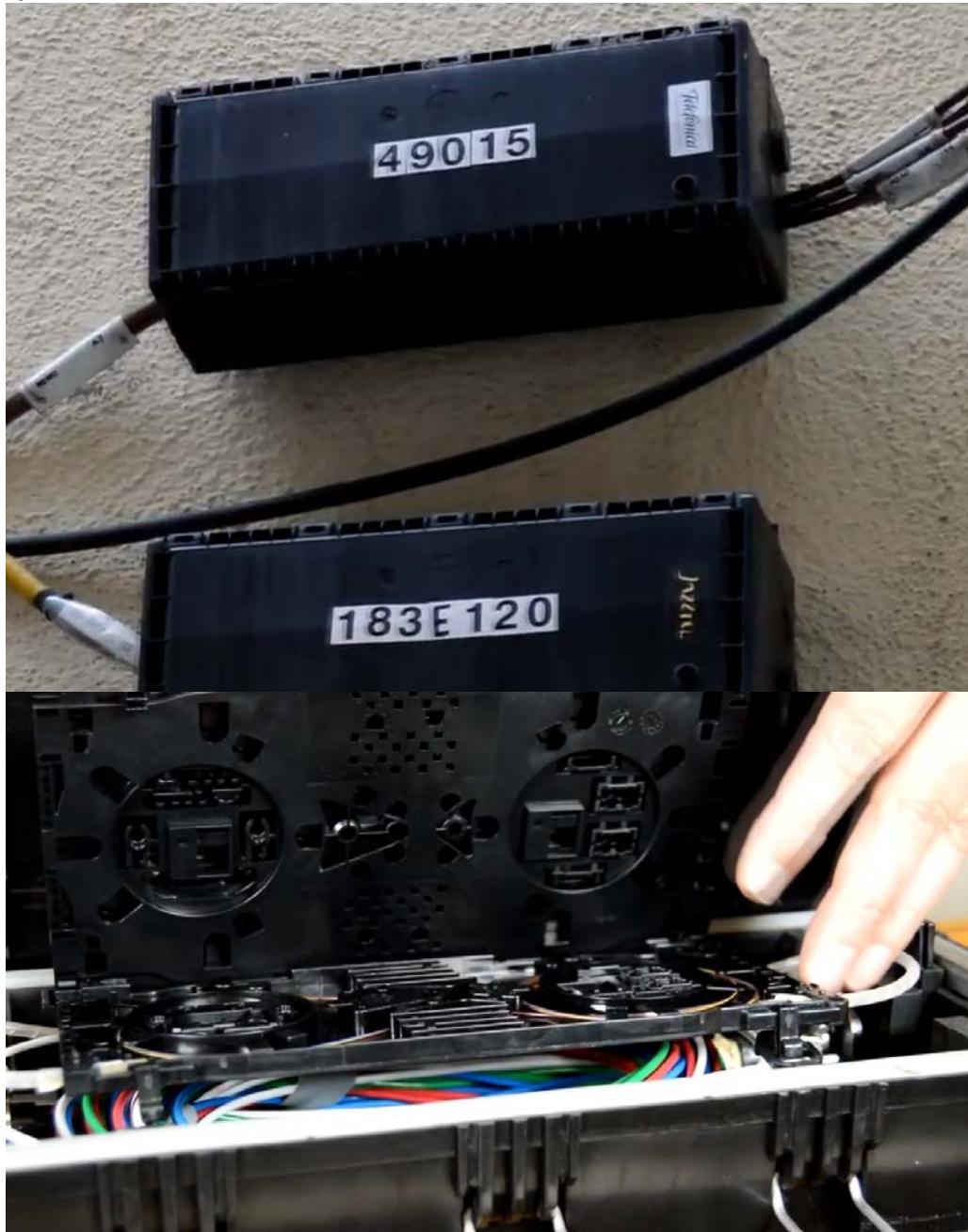
Con cables que pueden llevar varias fibras: 256...

Empalmes:

Se pueden hacer en el **Subsuelo** usando Cajas de empalme ubicadas en las Cajas de Registro (CR0...):

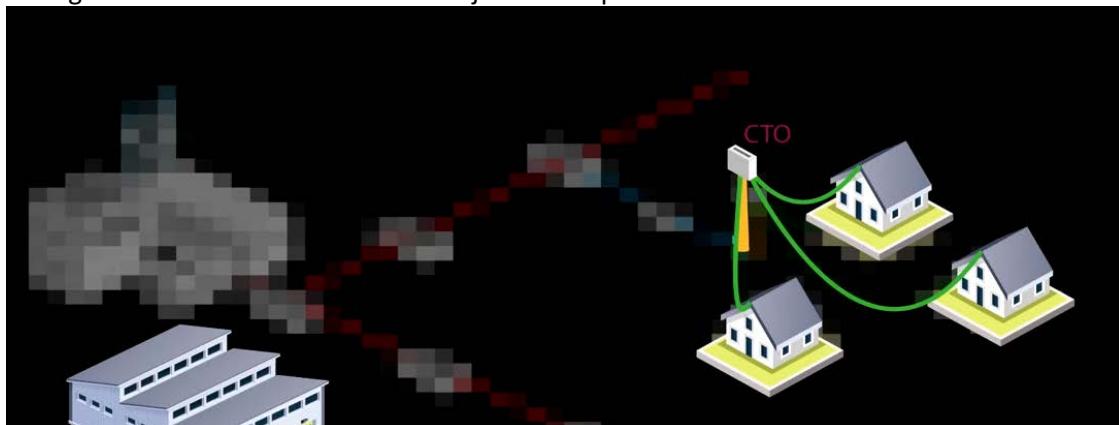


De fachada-poste



Video 6:

Ya hemos llegado de la calle al cliente a una caja exterior preconectorizada:



CTO: Caja Terminal Óptica (La caja negra de la imagen)

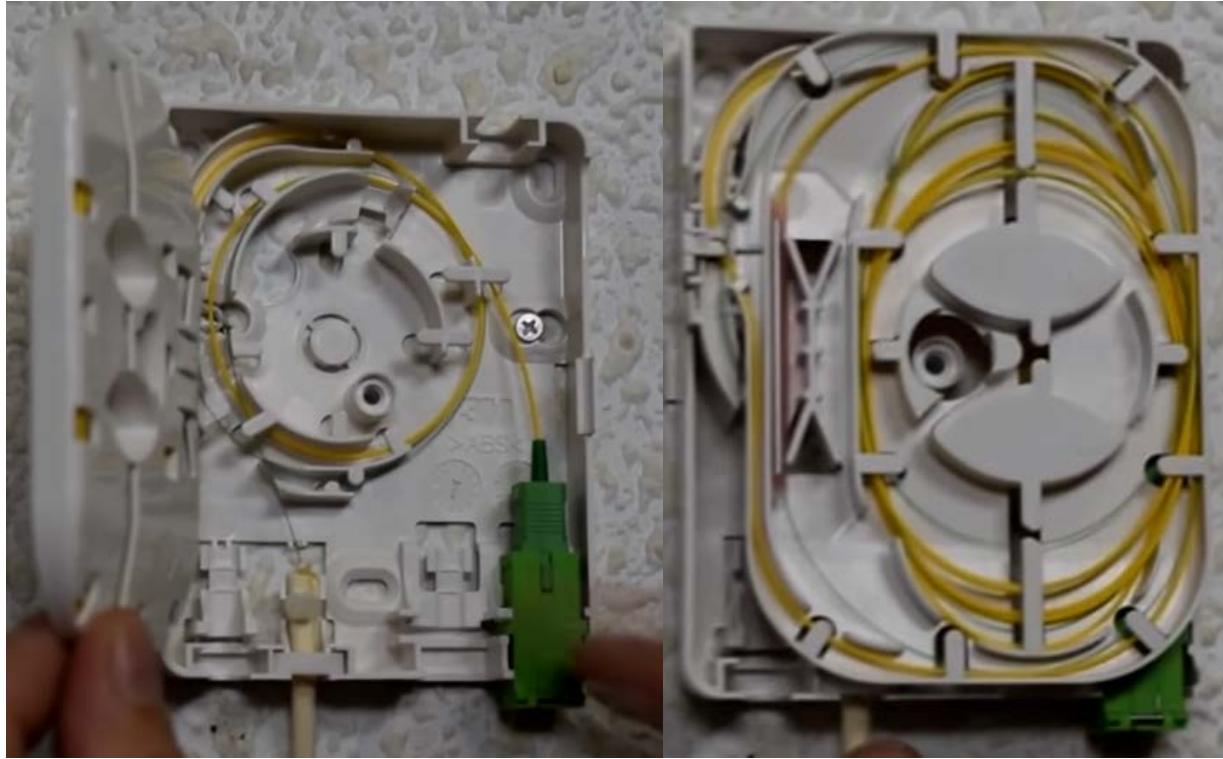


Llegamos hasta la Roseta en paso



Se Fusionan la fibra negra y la blanca

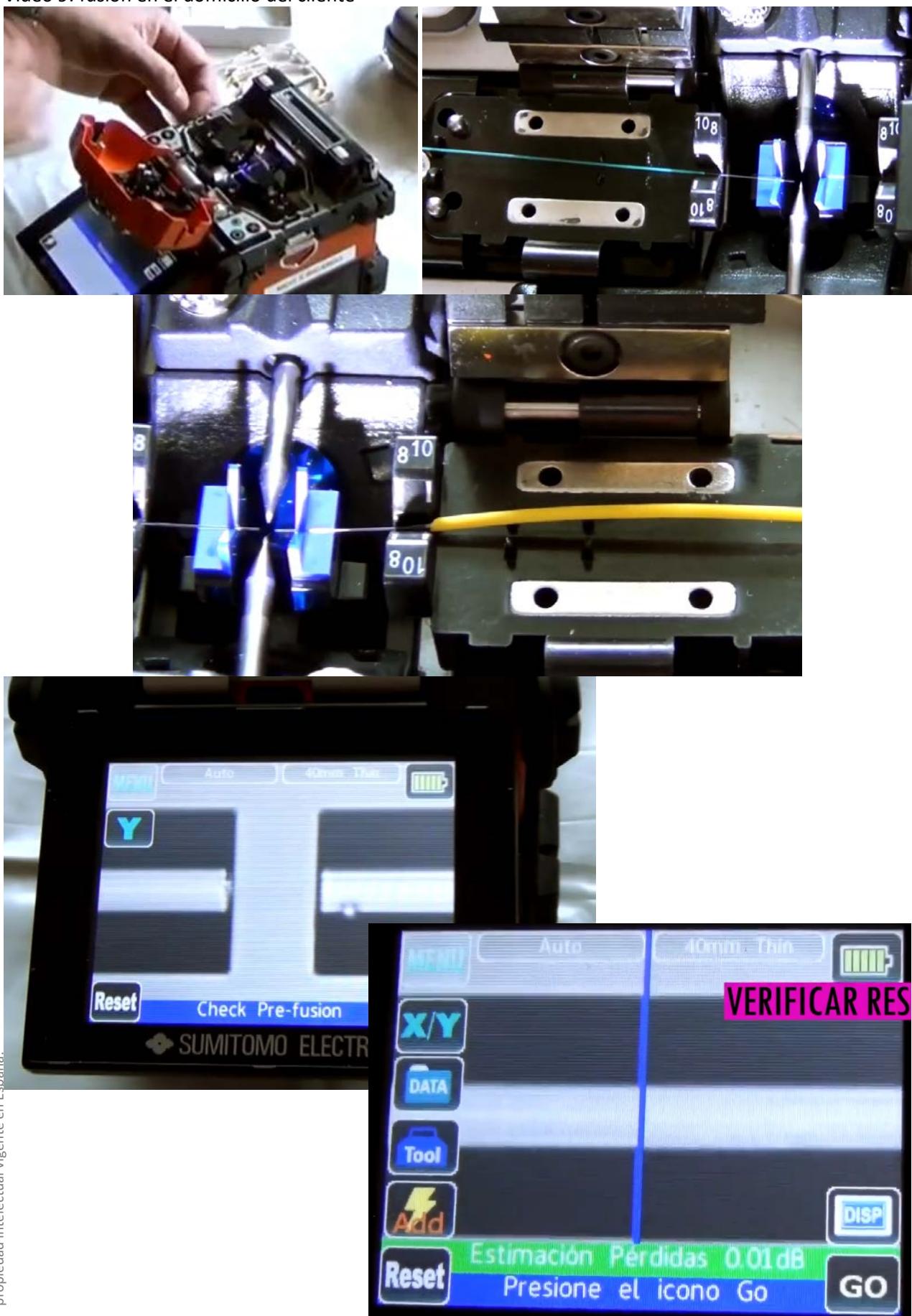
Roseta final: fusión de la fibra blanca al latiguillo (pig-tail)



En las viviendas unifamiliares también se puede llegar con una Caja de Empalme en pedestal:



Video 9: fusión en el domicilio del cliente



Luego le ponemos la funda protectora, la cual metemos al horno:



Video 10:

Configuración de la fusionadora: Tipo de Fibra:



Tipo de funda protectora-tipo de calefactor:



Video 11:

Instalación en edificios modernos -> RITI: Armario de telecomunicaciones del edificio



Cable de la operadora: indica las fibras en este caso 16



El cable de cliente es el mas pequeño que se ve en la imagen inferior.

Abrimos el módulo del operador:



Y abrimos el módulo del cliente:

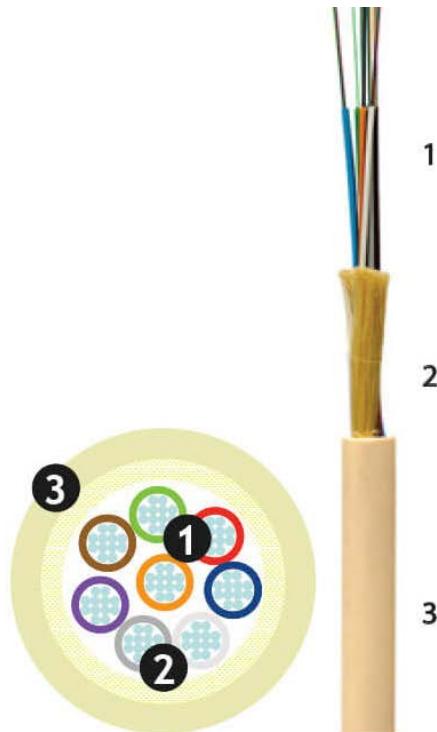


El cable que se usa se llama Cable RISER:

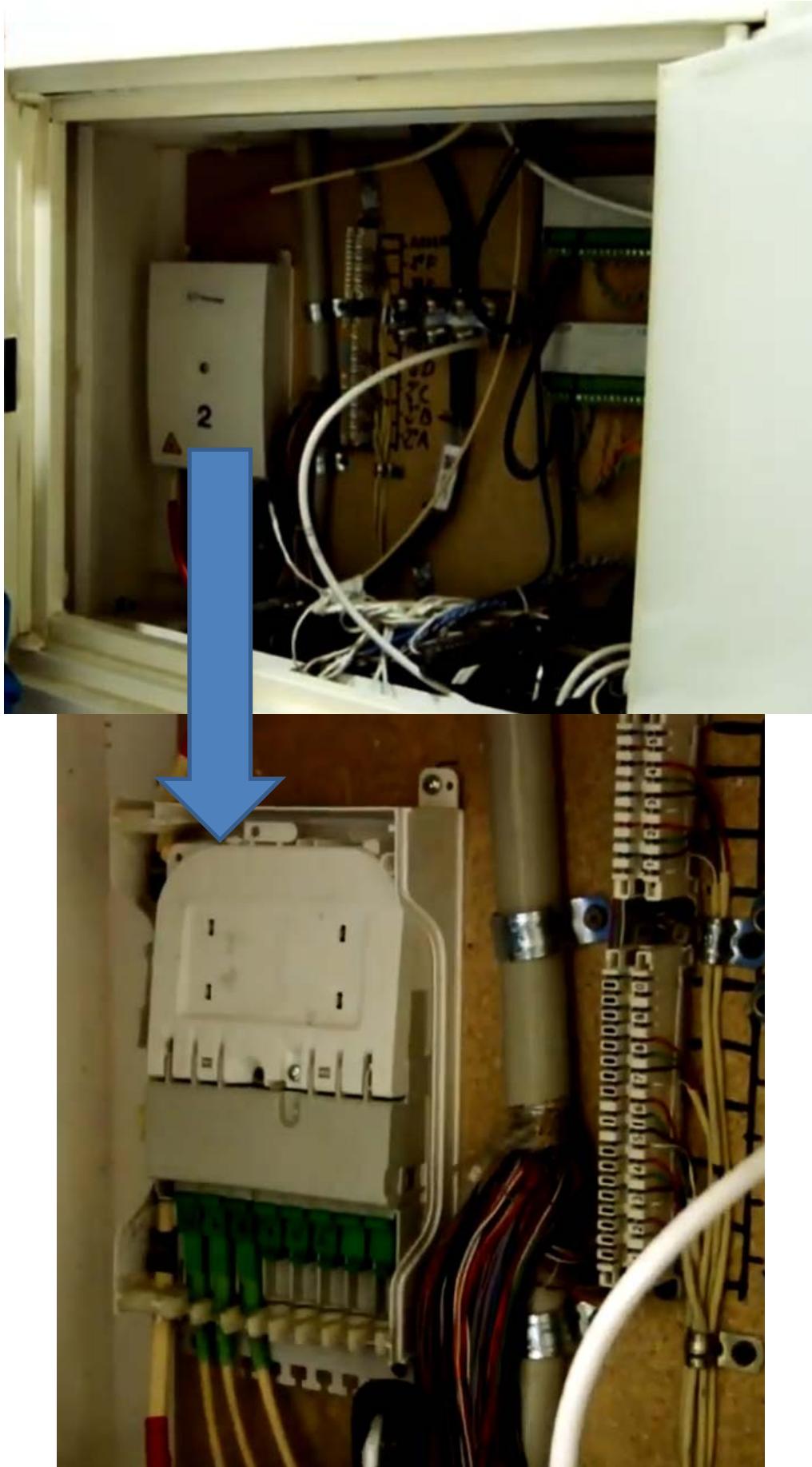
Cable RISER 16 FIBRAS (multitubo 4x4)

Detalle de construcción

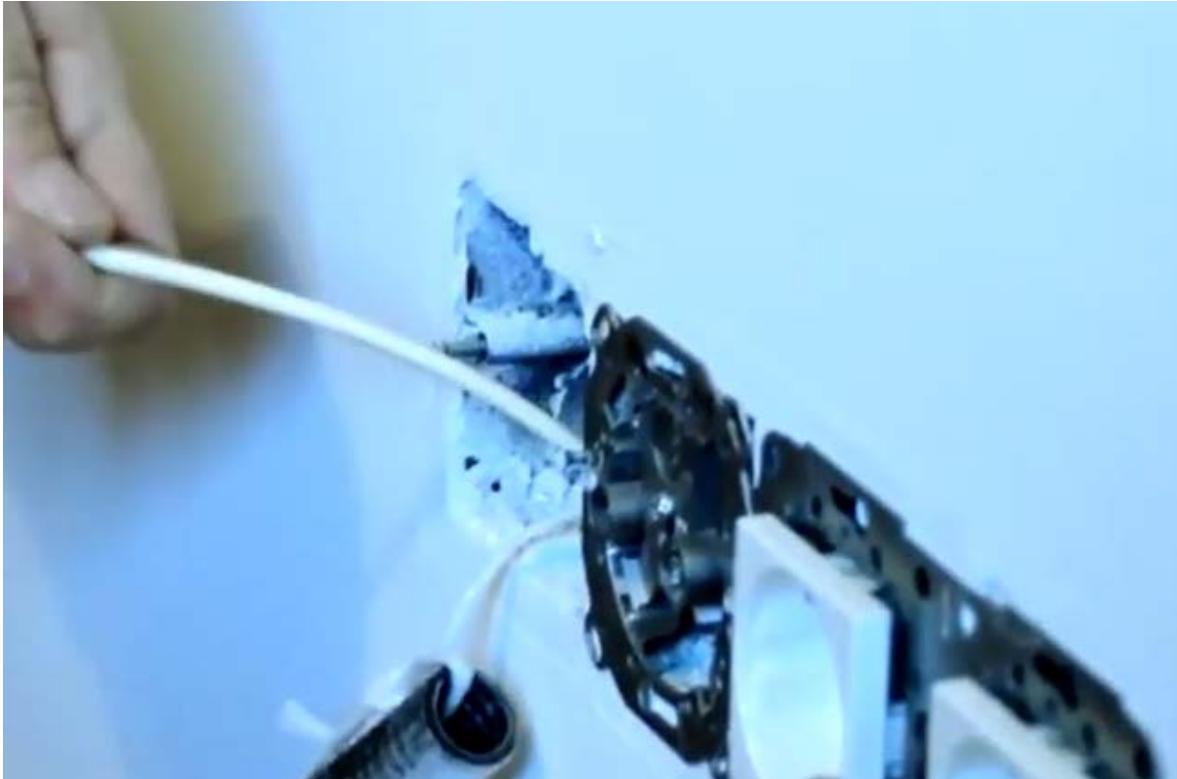
1. Micromódulos que contienen fibras ópticas
2. Cabos de aramida como elemento de refuerzo a la tracción
3. Cubierta de termoplástico retardante de llama, de baja emisión de humos y cero halógenos (LSZH)



Y desde el RITI llegamos a la caja de Derivación en la planta del cliente



Y desde la caja de derivación se llega a los enchufes de la casa del cliente:

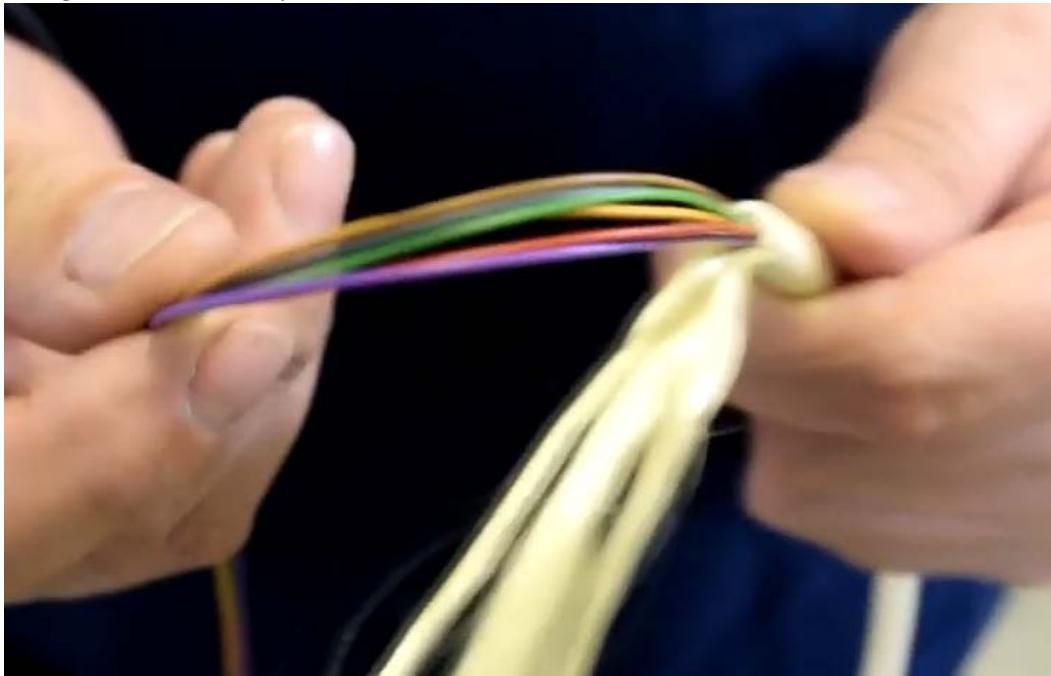


Video 12:

Cajas de interior fusionadas, dónde no hay cuarto para el RITI (por ejemplo en garajes)



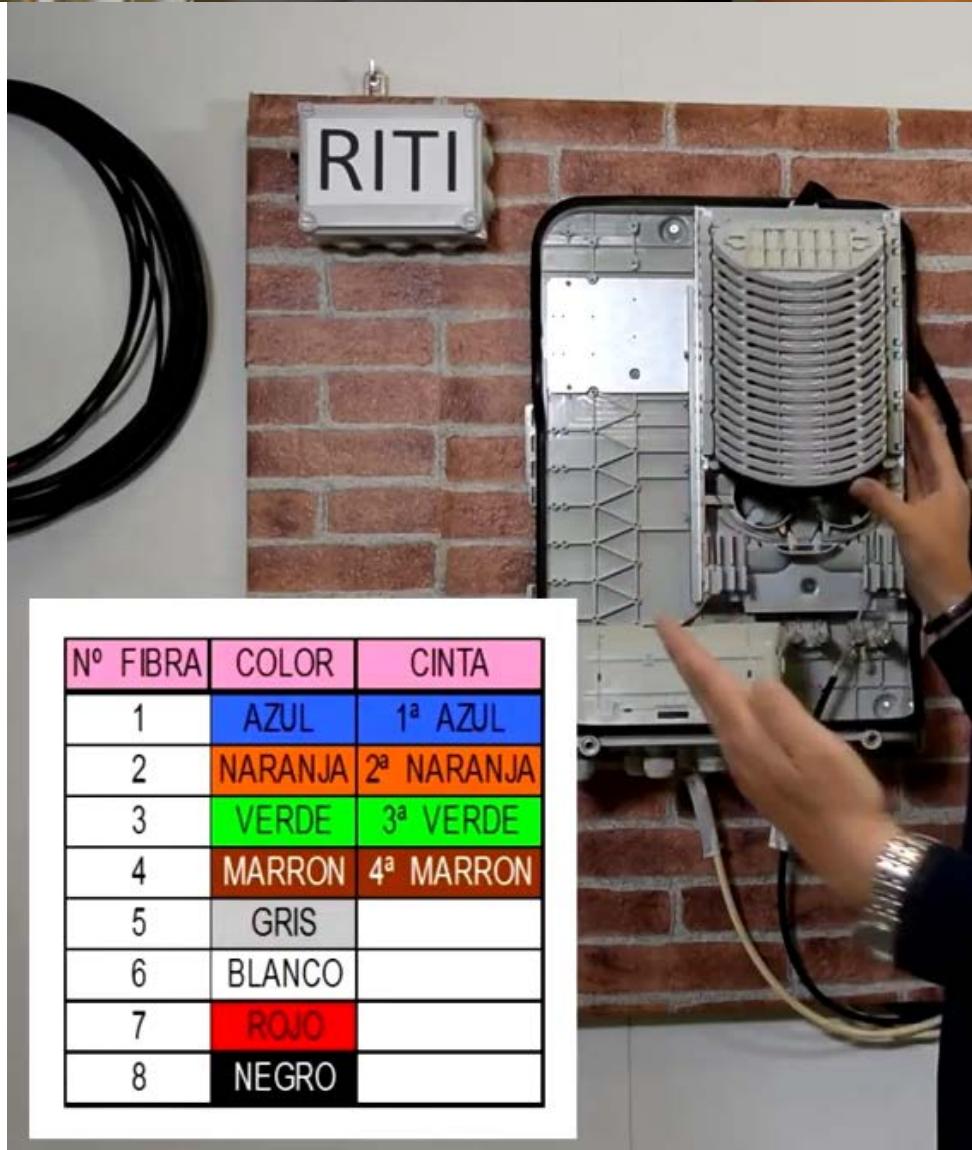
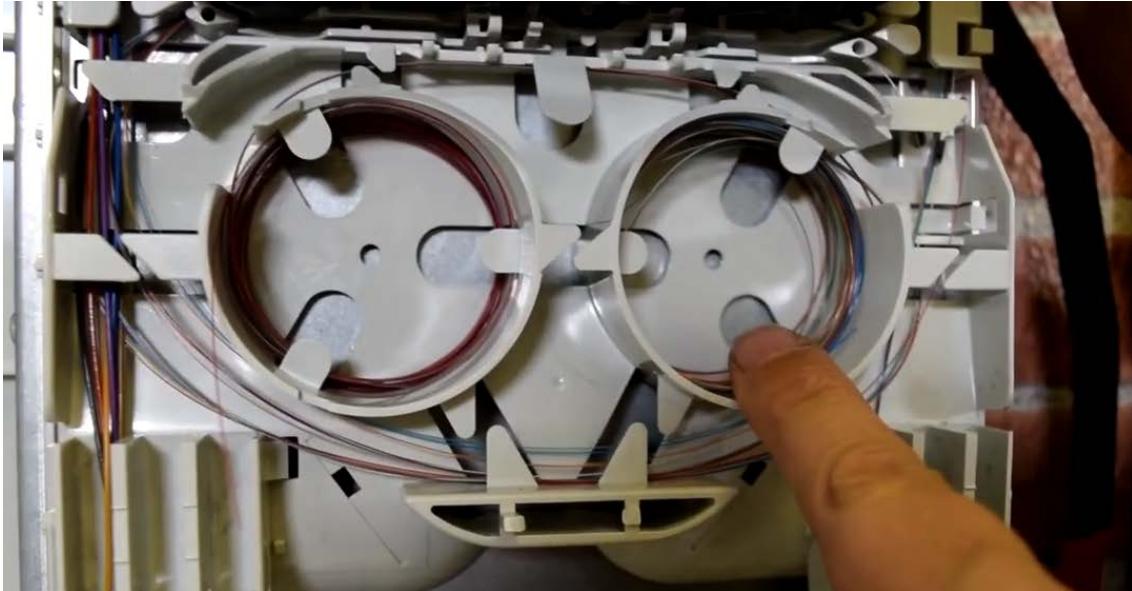
El Riser que llega al módulo del operador:



Usando el separador (negro) dividimos el RISER en:

Cinta de color azul del 1-8 y la cinta de color naranja del 9-16

Y luego conectamos en la bandeja que llega hasta el cliente:

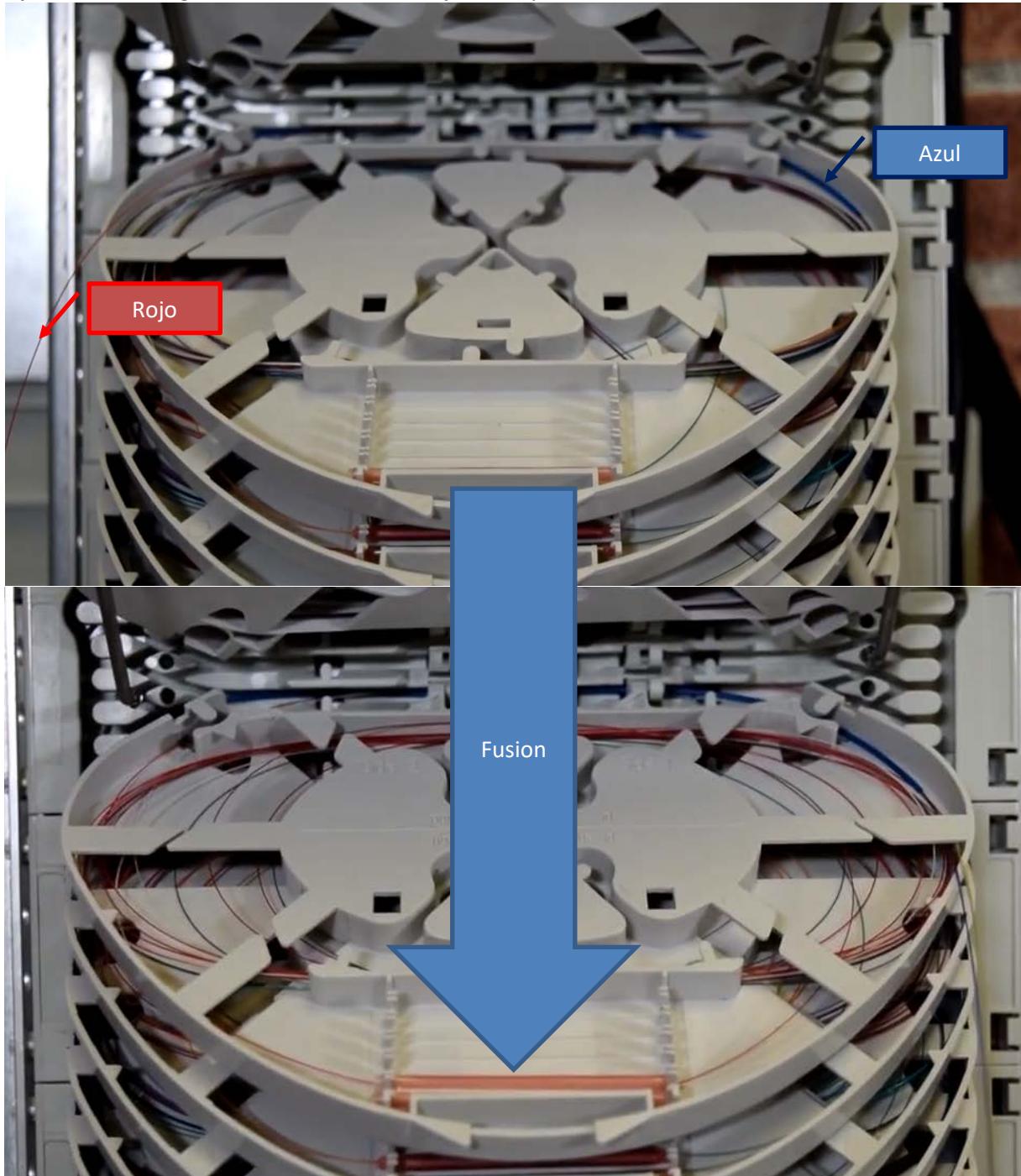


Nº FIBRA	COLOR	CINTA
1	AZUL	1 ^a AZUL
2	NARANJA	2 ^a NARANJA
3	VERDE	3 ^a VERDE
4	MARRON	4 ^a MARRON
5	GRIS	
6	BLANCO	
7	ROJO	
8	NEGRO	

El siguiente documento está creado con fines únicamente docentes y corresponde al registro diario de cada una de las jornadas de los cursos de formación impartidos por Luis Orlando Lázaro Medrano, y por lo tanto sólo se autoriza la lectura del mismo a los alumnos dados de alta en las plataformas de formación, cuyo acceso está restringido con nombre de usuario y contraseña. Y en ningún caso se autoriza la reproducción o difusión de este documento a terceros sin la aprobación expresa y por escrito de Luis Orlando Lázaro Medrano. El objetivo de este documento es únicamente ilustrar la actividad educativa en el aula, sin ninguna finalidad comercial, y siempre que sea posible, y la jornada educativa lo permita, se incluirá el nombre del autor y la fuente, adecuándose a los artículos 32.1 y 32.2. de la Ley de Propiedad Intelectual vigente en España.

Seleccionamos el color en el divisor (bandeja negra) por ejemplo el Rojo y luego en la toma del cliente, por ejemplo en el piso 4º miramos el color: en este caso azul. Buscamos ese color en las bandejas de la caja de la operadora y solo faltaría fusionarlas.

La roja del divisor negro con el azul de la bandeja correspondiente:



Video 14:

Instalación de equipos en la casa del cliente: ONT, ONT+Router y Equipo integrado. Ejemplos:

- ⇒ Solo ONT: (Optical Node Terminal) Conversor óptico – eléctrico y entonces el router suele estar virtualizado



⇒ ONT+Router:

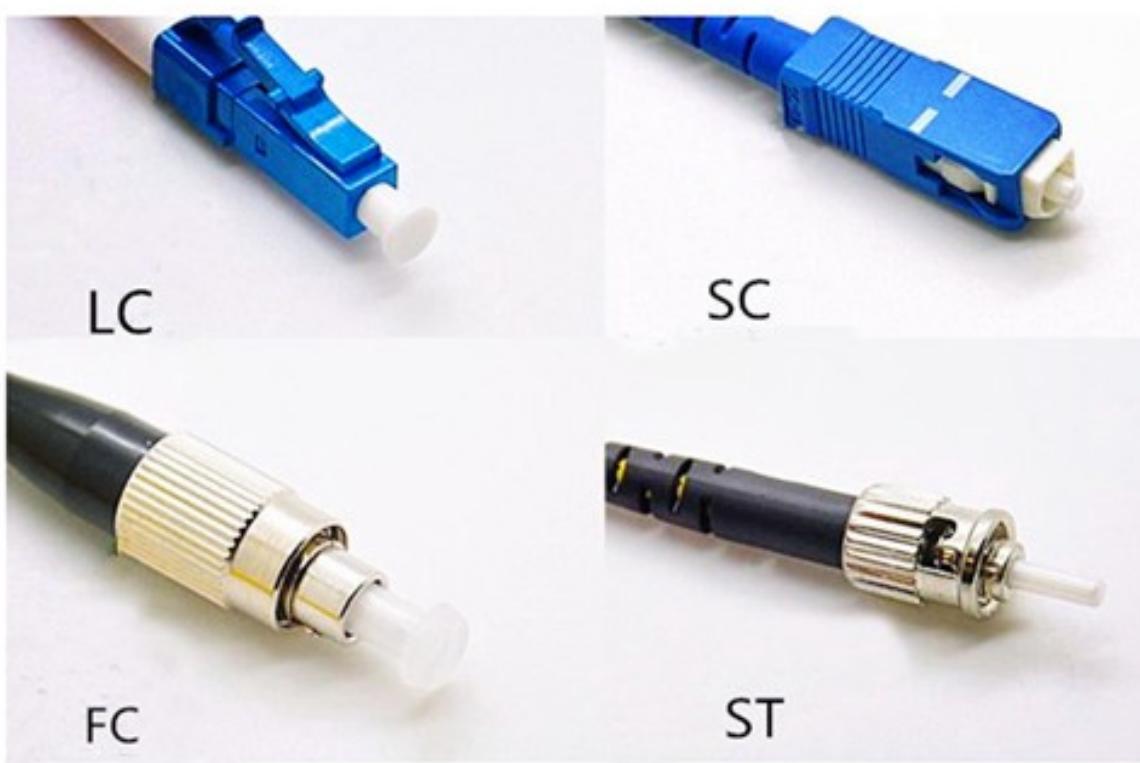


⇒ Equipo integrado:



Video 15:

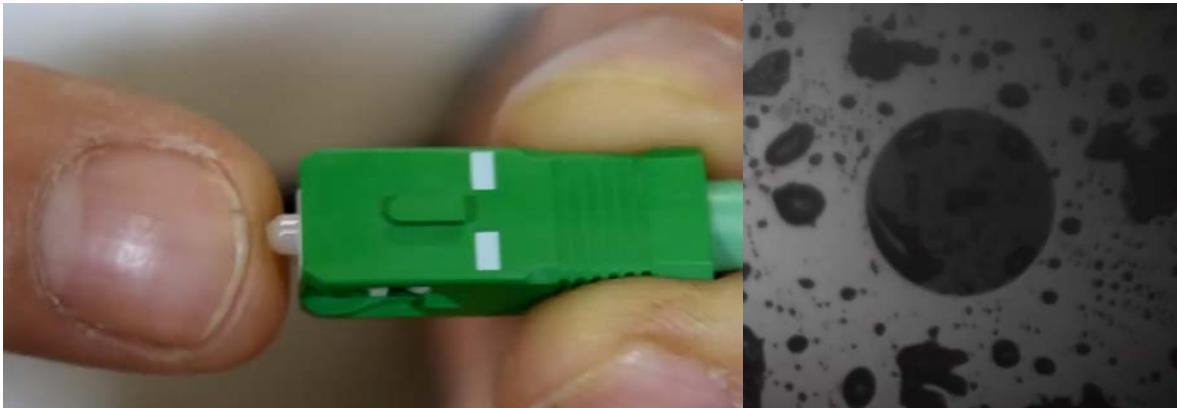
Fusión o Conectores:



Vista al microscopio:



Si toca con las manos el conector SC, mirar como se ve al microscopio:



Video 16:

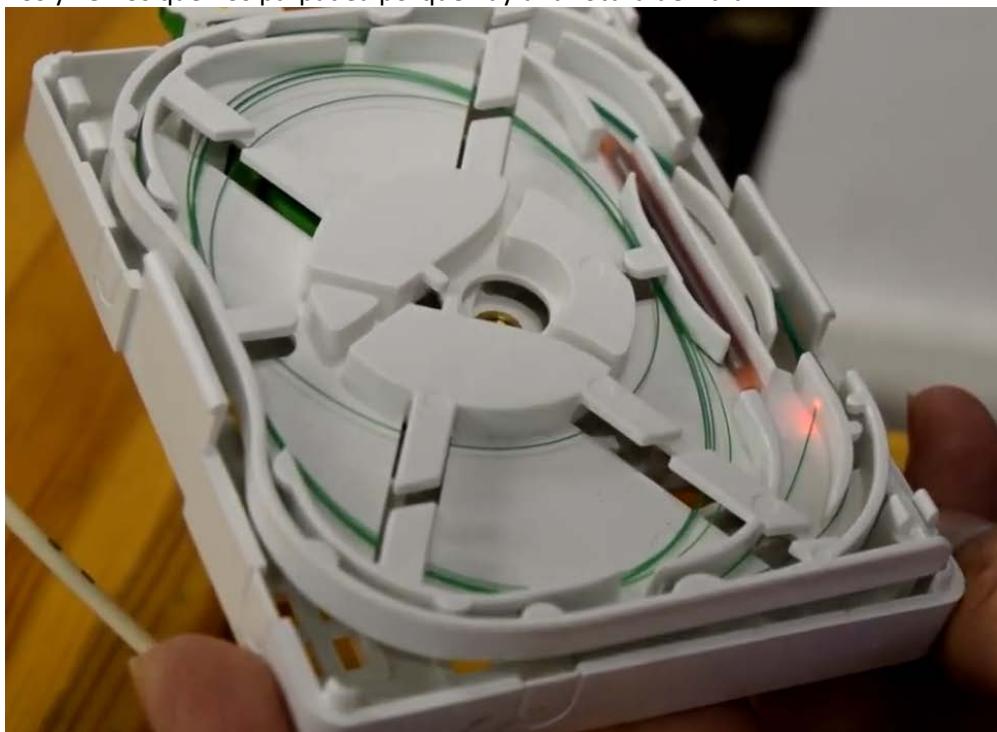
Test de fibra (Medidor de potencia GPON): nos marca la Landa (nm) y la potencia óptica (dbm) sabiendo que la ONT sincroniza a una valor entre -18 y -23 dbm



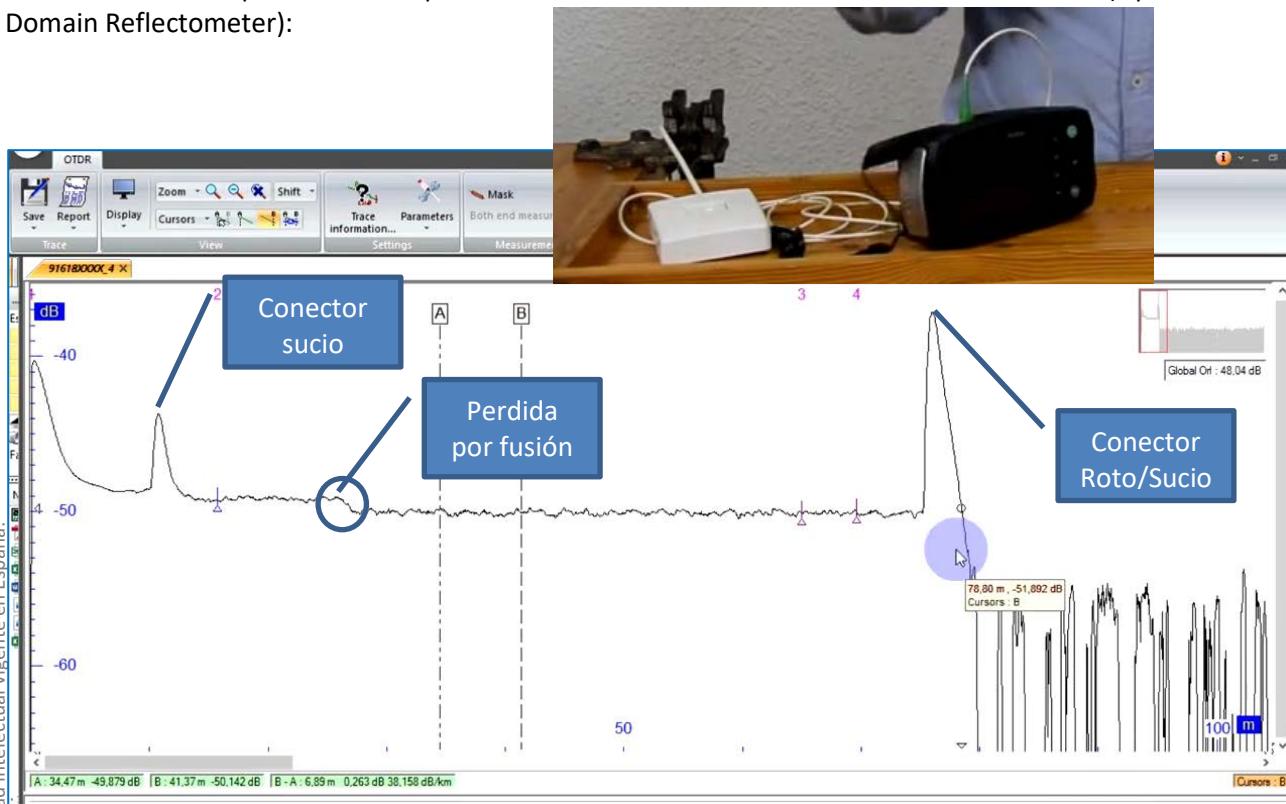
Localizador Visual de fallos:



Lo encendemos y vemos que nos parpadea porque hay una rotura de fibra:



Para hacer una comprobación más precisa usamos la Gráfica Reflecto-métrica usando OTDR (Optical Time Domain Reflectometer):



Web sobre Cómo es el despliegue de la red de fibra FTTH GPON de Movistar:

<https://bandaancha.eu/articulos/como-despliegue-red-fibra-ftth-gpon-9852>

1.2.1. Red de acceso

La red de acceso, como ya se ha descrito anteriormente, constituye el nivel funcional de la red que **hace llegar los servicios de telecomunicaciones a los usuarios finales**, así como atender a las peticiones que estos solicitan.

Estas redes de acceso se pueden implementar de varias formas, dando lugar a tres tipos de redes de acceso:

Redes de acceso vía cobre

Son las que usan como medio de transmisión el cobre. Destaca entre ellas las tecnologías **xDSL** (base de las tecnologías ADSL, vDSL...).

Redes de acceso vía fibra óptica

Son las que usan la fibra óptica como medio de transmisión, dando lugar a las redes **PON** (Red Óptica Pasiva), **CWDM** (Coarse wavelength Division Multiplexing - Multiplexación por división aproximada de longitud de onda) y redes **HFC** (redes híbridas coaxial-fibra).

Redes de acceso inalámbricas

Son aquellas que usan la transmisión por radiofrecuencia para la transmisión de la información. Destacan principalmente las tecnologías **WLL** (Wireless Local Loop" o bucle de abonado sin hilos) y **LMDS** (Sistema de Distribución Local Multipunto - Local Multipoint Distribution Service - despliegue de servicios fijos de voz, acceso a Internet, comunicaciones de datos en redes privadas, y video bajo demanda).

1.2.2. Red troncal de transporte

La red de transporte es el nivel funcional de una red de comunicaciones que **hace llegar los servicios de telecomunicaciones a la red de acceso** y que agrupa la mayor parte del tráfico de un conjunto de usuarios. Se denomina habitualmente el **backbone** de la red.

La mayor parte de esta red se implementa sobre fibra óptica debido a la gran cantidad de tráfico que debe soportar.

Los motivos que llevan a usar la fibra óptica para este nivel de red son los siguientes:

- ⇒ Baja atenuación.
- ⇒ Gran ancho de banda.
- ⇒ Fácil instalación.
- ⇒ Inmunidad ante interferencias electromagnéticas.
- ⇒ Alta seguridad.
- ⇒ Integración con cualquier tipo de red.

El tipo de **fibra óptica habitualmente** utilizado es la fibra **monomodo**, ya que es la que cumple los anteriores requisitos.

En este nivel de red han aparecido las siguientes tecnologías:

- ⇒ Tecnología PDH (jerarquía digital plesioícrona - Plesiochronous Digital Hierarchy) permite enviar varios canales telefónicos sobre un mismo medio usando técnicas de multiplexación por división de tiempo y equipos digitales
- ⇒ Tecnología SDH (jerarquía digital síncrona- Synchronous Digital Hierarchy) dispositivo digital que trabaja realizando multiplexación por división el tiempo)
- ⇒ Tecnología DWDM (Dense Wavelength Division Multiplexing) multiplexado denso por división en longitudes de onda

1.2.3. Red de distribución

La red de distribución es el nivel funcional de una red de comunicaciones que **se encarga de realizar las tareas de conmutación y multiplexación de la información procedentes de los proveedores de servicio y adaptarlas y entregarlas al siguiente nivel de la red de telecomunicaciones**, es decir, a la red troncal.

Es misión de esta red de distribución realizar el establecimiento y liberación de las conexiones con los diferentes bucles de abonado, además de **gestionar el ancho de banda de la información transmitida entre los proveedores de servicios y los usuarios**.

En este nivel de red es donde se **instalan y configuran los siguientes elementos**:

Comutadores

Son dispositivos que **permiten realizar conexiones de varios usuarios e interconectarlos empleando un mismo enlace físico**, optimizando así los recursos de la red.

Multiplexores

Son dispositivos que **permiten transmitir por el mismo canal diferentes fuentes de información de diferentes usuarios (multiplexación)**, haciendo que cada una de ellas se transmita sin interferir con el resto.

Para ello se emplea la **multiplexación en frecuencia, en el tiempo y la multiplexación estadística**.

1.3. Multiplexación

En una red de comunicaciones se transmite mucha información de diferentes usuarios y a diferentes puntos.

Es por ello que se basa en una arquitectura e infraestructuras compartidas que son usadas por muchos usuarios y equipos.

Para que sobre un mismo soporte pueda transmitirse información de diferentes usuarios es preciso emplear técnicas como la **multiplexación**, que permite que cada información llegue a su destino correcto y no se solape con el resto de información de otros usuarios.

A continuación, veremos estas técnicas y en especial la multiplexación como la técnica más usada en las modernas redes de comunicaciones.

En un **enlace de comunicaciones** entre dos o más equipos siempre se busca maximizar la capacidad del canal, es decir, **se busca el máximo rendimiento de las comunicaciones**.

Ello se consigue utilizando el mismo canal para transmitir varias comunicaciones independientes a la vez.

Una de las técnicas más empleadas para esto es la citada multiplexación.

Se define la multiplexación como la técnica que permite la transmisión por el mismo canal de diferentes comunicaciones independientes entre sí y de diferentes dispositivos o equipos asegurando que la transmisión de cada una de ellas sea fiable, segura y que no interfieran entre ellas consiguiendo con ello la máxima eficiencia de transmisión del canal.

La multiplexación es una técnica empleada en el tratamiento de señales que permite por el mismo canal enviar varias comunicaciones a la vez sin que interfieran unas con otras. Con ello se mejora la eficiencia de los canales de transmisión.

1.3.1. Multiplexores

Los multiplexores son dispositivos electrónicos encargados de realizar la multiplexación de los canales de información en las redes de comunicaciones.

Su **ubicación** se realiza, como ya se ha descrito anteriormente, en la red de distribución junto con otros dispositivos como los comutadores.

Existen diferentes tipos de multiplexores:

- Multiplexores terminales.
- Multiplexores de inserción y extracción.
- Multiplexores de distribución o DXC.

Son estos últimos los más empleados en la red de distribución.

El multiplexor dispone de varias entradas de datos y una única salida por donde se transmite el conjunto de canales de entrada ya multiplexadas.



Los multiplexores **basan su funcionamiento en circuitos combinacionales capaces de seleccionar una entrada entre varias posibles y cortocircuitar entrada con salida**, de forma que la información de esa entrada vaya a la salida.

Con una **comutación temporal de varias entradas** podemos ir enviando a la salida la información de varias entradas y con ello realizar la **multiplexación de los canales de entrada**.

Uno de los parámetros a definir en un multiplexor es el **número de entradas** de los que dispone.

Existen diferentes tipos de multiplexores en función del tipo de multiplexación a realizar y sobre el tipo de medio de transmisión que conmuta.

Así existen multiplexores para:

- ⇒ Redes de pares trenzados.
- ⇒ Redes de fibra óptica.
- ⇒ Redes de coaxiales.
- ⇒ Redes inalámbricas.

Existen además numerosos fabricantes en el mercado que suministran este tipo de equipos con diferentes modelos. En su hoja de especificaciones o datasheet figuran las características de cada uno de ellos.

1.3.2. Técnicas de multiplexación

Existen tres tipos de **técnicas de multiplexación** claramente diferenciadas:

- ⇒ Multiplexación **por división en frecuencia** (FDM).
- ⇒ Multiplexación **por división en el tiempo** (TDM).
- ⇒ Multiplexación **por división en la longitud de onda** (WDM).

Cada una de ellas presenta sus ventajas e inconvenientes, que veremos a continuación.

Dependiendo del tipo de multiplexación a realizar se deberá emplear un equipo u otro de multiplexación.

No obstante, **existen determinados modelos de multiplexados que pueden aplicar varias técnicas de multiplexación**.

La **multiplexación** se puede aplicar para cualquier tipo de red tanto cableada (par trenzado, fibra óptica) como inalámbrica.

1.3.2.1. Multiplexación por división en frecuencias (FDM)

La multiplexación por división en frecuencias o FDM (Frequency Division Multiplexing) tiene sus orígenes en las transmisiones analógicas.

Se basa en transmitir cada comunicación en diferentes ventanas de frecuencias no solapadas entre sí y con **ventanas de guardas**.

De este modo, aprovechamos al máximo todo el **ancho de banda de canal** dividiendo dicho ancho de banda en canales. En cada uno de ellos **transmitimos un canal de comunicación independiente del otro**.

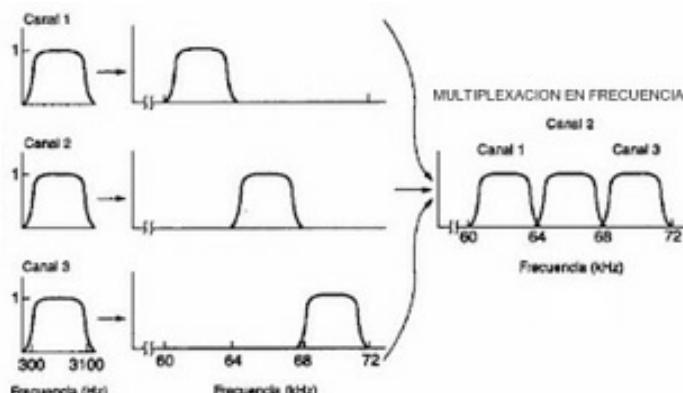
La capacidad del canal está limitada por el propio ancho de banda del canal.

La multiplexación por división en frecuencias presenta las siguientes **ventajas**:

- **Bajo coste**, es una tecnología ya **muy madura**.
- **Posibilidad de conectarse en cascada** entre varios equipos.

Las **desventajas** que ofrece son las siguientes:

- Presenta un **número limitado de canales** a transmitir en función del **ancho de banda** del canal.
- Presenta **baja eficiencia** al precisar **bandas de guarda**.
- **Necesidad de mantener el sincronismo** en las **frecuencias** de funcionamiento.
- Necesidad de utilizar **filtros** en los equipos.



1.3.2.2. Multiplexación por división en el tiempo (TDM)

La multiplexación por división en el tiempo o TDM (Time Division Multiplexing) surge a partir de las transmisiones digitales, cuando se emplea la transmisión de datos binarios (bits).

Se basa en dividir el tiempo en intervalos. En cada intervalo se envía una trama de bits de una comunicación.

De este modo, aprovechamos al máximo todo el ancho de banda de canal dividiendo dicho ancho de banda en canales donde transmitimos un canal de comunicación independiente del otro.

La capacidad del canal está limitada por el propio ancho de banda del canal.

1.3.2.3. Multiplexado estadístico o asíncrono

La multiplexación estadística **consiste en asignar intervalos de tiempos a cada canal en función del tráfico existente y demandado por el canal y no de forma fija como en la multiplexación por división en el tiempo (TDM)**.

De esta forma **a aquellos canales con tráfico crítico o con mucho tráfico se le asignan más intervalos y a aquellos con menos tráfico o tráfico no crítico se le asignan menos canales**.

Por **tráfico crítico** se entienden servicios de telecomunicaciones con QoS (quality of service) como VoIP, TVIP, streaming de vídeo, etc.

Este multiplexado (aunque más complejo) **es el más eficiente, ya que reparte los recursos de la red en función de cada tipo de tráfico y su carga, con lo que se consigue optimizar el canal portador**.

1.3.2.4. Multiplexación por División de Longitud de Ondas o WDM

Existe otro tipo de multiplexación también muy empleada que es la multiplexación por división de longitud de ondas o WDM (WaveLength Division Multiplexing).

Es un tipo de multiplexación **similar a la multiplexación por división de frecuencias, pero en vez de hablar de frecuencias hablamos de longitud de ondas (λ)**.

Como ya sabemos, frecuencia (f) y longitud de onda (λ) están relacionadas mediante la siguiente expresión:

$$\lambda = c/f$$

Este tipo de multiplexación se emplea en transmisiones por infrarrojos, en las que el canal de transmisión se divide en ventanas de longitud de onda y cada canal de comunicación se envía en una determinada ventana de transmisión.

De este modo somos capaces de enviar **n** comunicaciones simultáneamente, cada una de ellas en una ventana o longitud de onda diferente.

El número de ventanas o canales que se pueden transmitir dependerá de la longitud de la ventana de cada canal y de la longitud de la ventana total del medio de transmisión, es decir:

$$\text{Nº canales} = (\text{Longitud de la ventana del medio de transmisión}) / (\text{Longitud de la ventana de un canal})$$

La multiplexación por división de longitud de onda cada vez se emplea más en las transmisiones, ya que suelen ofrecer un gran ancho de banda para los nuevos servicios de telecomunicaciones.

En el emisor requiere de un multiplexor óptico y en el receptor de un demultiplexor óptico.

1.4. Funciones de conmutación, transporte y señalización

La conmutación es una **técnica** ampliamente utilizada en comunicaciones **consistente en poner en contacto un equipo con otro empleando una infraestructura común de comunicaciones** para la transmisión de los datos.

Con ello **se pretende dar eficiencia al sistema, ya que varios equipos pueden emplear la misma infraestructura para enviar datos y no crear redes y recursos individuales para cada transmisión**, lo que encarecería enormemente la infraestructura.

Esta **técnica**, por tanto, **permite que en un momento dado el equipo emisor y el equipo receptor estén conectados para la transferencia de la información. Cuando termina la transferencia, se liberan los recursos para que puedan ser usados para otra transmisión de otros equipos**.

Existen dos tipos o técnicas de conmutación:

Conmutación de circuitos

Es una técnica de conmutación **basada en el establecimiento de una conexión física entre los dos extremos** (emisor y receptor), empleando para ello y conectando todos los elementos y nodos intermedios para que durante la transferencia exista ese camino físico para el intercambio de la información.

Cuando se termina la transferencia, se liberan todas las conexiones intermedias y quedan a disposición de la red para otra comunicación del mismo o de diferentes equipos.

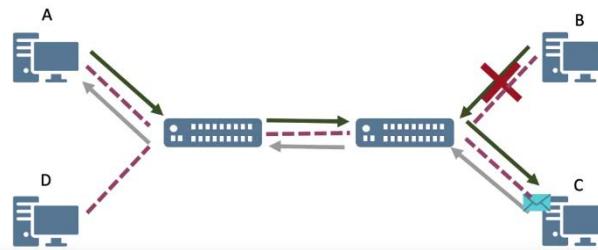
Esta conmutación de circuitos permite ser implementada de dos formas:

⇒ **Comutación de circuitos espacial:**

Es aquella en la que durante la transferencia el circuito establecido está permanente y en exclusiva para el emisor y el receptor y sólo se libera cuando haya finalizado la transferencia.

⇒ **Comutación de circuitos temporal:**

En esta **se crean espacios temporales de transmisión**, de forma que cada comunicación emplea una serie de intervalos de tiempo para transmitir, pero todas las comunicaciones emplean el mismo circuito o enlace físico.



En la conmutación de circuitos se establece una conexión física a través de varios enlaces y nodos intermedios para unir emisor y receptor.

En la conmutación de circuitos temporal, en cambio, se establecen slots temporales.

Cada slot temporal es utilizado por un canal de comunicaciones, pero todas ellos usan el mismo enlace o circuito de conexión.

Este tipo de conmutación es el empleado por el servicio telefónico RTC (red telefónica conmutada).

Comutación de paquetes

La conmutación de paquetes es una técnica que **'trocea'** la información en paquetes de longitud fija y envía cada paquete desde el emisor al receptor.

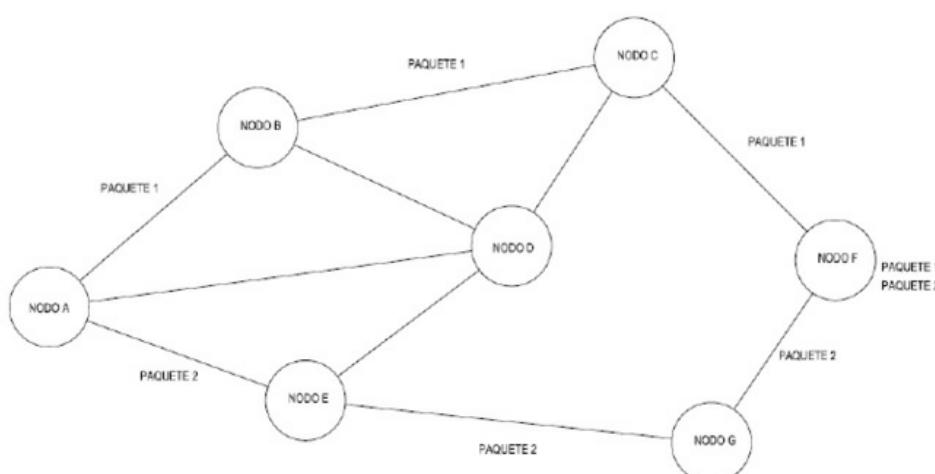
Cada paquete puede utilizar una ruta diferente para llegar al destino y para poder llegar a ese destino cada paquete incluye una cabecera (además de la información) que contiene la dirección de origen y destino del paquete.

Cada nodo de la red analiza la cabecera del paquete y decide si es para él o si debe enrutarlo a otro nodo para hacerlo llegar a su destino.

Este tipo de conmutación es más eficiente que la conmutación de circuito, ya que aprovecha mejor los recursos del sistema.

Internet utiliza para la transmisión de los datos la conmutación de paquetes.

Uno de los problemas de este tipo de conmutación es el retardo sufrido por los paquetes (al tener que pasar por muchos nodos), las pérdidas de paquetes y la llegada desordenada de paquetes del mismo mensaje al receptor (ya que llegan por rutas diferentes). Estos dos últimos problemas implican que el sistema debe incluir técnicas de detección y corrección de paquetes.



La conmutación de paquetes admite dos implementaciones:

Modo circuito virtual u orientado a conexión

En este tipo de conmutación de paquetes, **todos los paquetes pertenecientes al mismo mensaje siguen la misma ruta**, por lo que previamente se debe establecer un circuito virtual entre emisor y receptor.

Así, cada paquete además de la dirección origen y destino incluye el número de conexión por el que va dirigido.

La ventaja es que evita la llegada desordenada de paquetes, aunque incluye más retardo debido al tiempo de establecimiento del circuito virtual.

Modo datagrama u orientado a no conexión

En este tipo de conmutación de paquetes, **cada paquete puede ir por rutas diferentes dependiendo del estado de la red y de cada uno de los enlaces**.

Esto implica que los paquetes puedan llegar desordenados y serán aplicaciones de niveles superiores a nivel de red quienes deban aplicar técnicas de detección y corrección de paquetes.

La ventaja es que hay menos retardo que en el modo circuito virtual u orientado a conexión.

Señalización

La **señalización** es un **procedimiento de gestión y control** que incluyen las redes de comunicaciones y que se emplea como medio para establecer, mantener y finalizar las diferentes conexiones y/o llamadas.

Gestiona por tanto los conmutadores para que puedan realizar sus funciones adecuadamente en función de las necesidades del tráfico en la red.

Esta señalización cobra especial relevancia en las redes de conmutación telefónica (RTC).

En este caso, la señalización realiza las siguientes funciones:

- ⇒ Establecer la comunicación con el abonado incluyendo los tonos de marcado, tono de llamada, señal de ocupado, etc.
- ⇒ intermedios de la red.
- ⇒ Transmisión de la información por la red.
- ⇒ Conexión con el abonado destino.
- ⇒ Realizar las funciones de tarificación.
- ⇒ Liberar la conexión una vez finalizada.
- ⇒ Control y gestión del sistema.

Existen dos procedimientos para realizar la señalización:

- Señalización por canal común.
Esta señalización se caracteriza por enviar los mensajes de señalización por el mismo canal donde se transmite la información.
- Señalización por canal asociado.
Esta señalización se caracteriza por enviar los mensajes de señalización por un canal dedicado especialmente a este fin e independiente del canal donde se envía la información.

La función de transporte de la información en las redes de comunicaciones se encarga de hacer llegar al destinatario la información enviada por el emisor de forma correcta, ordenada y sin errores.

Además, deberá asegurar que dicha información sea entregada en los plazos establecidos en la QoS de cada servicio, algunos muy críticos como pueden ser:

- ⇒ Servicio de VoIP.
- ⇒ Servicio de TvIP.
- ⇒ Servicio de streaming de vídeo.

2. Arquitectura de redes de voz y datos

2.1. Redes de acceso: guiadas y no guiadas

Para que los servicios de telecomunicaciones lleguen a los usuarios y equipos finales es necesaria una red que distribuya dichos servicios desde donde se generan hasta la ubicación donde están estos usuarios y equipos finales.

Es por ello que las redes de comunicaciones están estructuradas en diferentes niveles, que son: nivel de acceso, nivel troncal o de transporte y nivel de distribución.

El nivel o red de acceso es la parte de la red que permite que los servicios de telecomunicaciones lleguen hasta los hogares, usuarios y empresas. Representa el último tramo de la red y proporciona por eso el 'acceso' de los servicios.

Esta parte de la red, debido a que debe hacer llegar los servicios a todos los usuarios y ubicaciones, es la que presenta mayor capilaridad y por ello la más costosa y en numerosas ocasiones las más difícil de implementar.

En numerosas bibliografías a este tramo de la red se le conoce como 'la última milla'.

Las redes de acceso pueden implementarse de dos formas:

Redes de acceso guiadas

Son aquellas que usan un cable (medio guiado) como medio de transmisión.

En este caso existen dos variantes fundamentalmente:

- ⇒ Redes de acceso basado en el **cobre**: son las que usan como medio de transmisión el cobre, destacando entre ellas las tecnologías **xDSL**.
- ⇒ Redes de acceso basado en la **fibra óptica**: son las que usan la fibra óptica como medio de transmisión, dando lugar a las redes **PON** (Red Óptica Pasiva), **CWDM** (Coarse wavelength Division Multiplexing - Multiplexación por división aproximada de longitud de onda) y redes **HFC** (redes híbridas coaxial-fibra).

Redes de acceso no guiadas

Son las redes inalámbricas que emplean la radiofrecuencia para la transmisión de la información.

Destacan principalmente las tecnologías **WLL** (Wireless Local Loop" o bucle de abonado sin hilos) y **LMDS** (Sistema de Distribución Local Multipunto - Local Multipoint Distribution Service - despliegue de servicios fijos de voz, acceso a Internet, comunicaciones de datos en redes privadas, y video bajo demanda)

Las redes de acceso (también denominadas la última milla) constituyen la última parte de la red que hace llegar los servicios de telecomunicación a los usuarios.

Las redes basadas en el cable, como las tecnologías xDSL y la fibra óptica, presentan una serie de ventajas como:

- ⇒ Son altamente fiables y seguras.
- ⇒ Ofrecen en general un gran ancho de banda.
- ⇒ Permiten adaptarse a las nuevas tecnologías.

Por el contrario, presentan el gran inconveniente del alto coste de instalación, ya que su alta capilaridad exige habitualmente apertura de zanjas, permisos, tendidos de cables, servidumbres, etc.

En cambio, las redes inalámbricas en sus diferentes implementaciones presentan las siguientes ventajas:

- ⇒ Su despliegue es mucho más rápido que las redes cableadas.
- ⇒ Son muy aptas para zonas u orografías accidentadas o complicadas.
- ⇒ Su coste es sensiblemente menor que las redes cableadas.

Por el contrario, presentan ciertos inconvenientes como:

- ⇒ En general, su ancho de banda es menor que las redes cableadas.
- ⇒ Su nivel de seguridad es menor que las redes cableadas (cada vez menos).

2.1.1. Redes de acceso vía cobre: xDSL

Ya hemos visto que las redes de acceso se pueden implementar mediante redes cableadas y guiadas, siendo las más utilizadas las redes con tecnologías xDSL, que son redes basadas en el cable de cobre.

Las tecnologías xDSL surgieron al aprovechar el hilo telefónico ya instalado en la mayoría de los hogares y edificios (su sustitución por otro tipo de cable era muy costoso) para ofrecer servicios de telecomunicaciones de banda ancha y de alta velocidad.

xDSL representa una tecnología que admite diversas variantes o **modalidades** como:

- ⇒ ADSL.
- ⇒ HDSL.
- ⇒ SDSL.
- ⇒ RADSL.
- ⇒ VDSL.
- ⇒ Etc.

Cada una de ellas tiene unas características y prestaciones diferentes que la hacen adecuada para un determinado servicio u otro.

La más conocida, por ser la más ampliamente utilizada, es la tecnología **ADSL** (Asymmetric Digital Subscriber Line). Se emplea habitualmente en el bucle de abonado.

Proporciona un gran ancho de banda, con una alta velocidad y conexión permanente. Además, se realiza individualmente sobre cada línea, sin tener que afectar al resto de líneas de otros usuarios.

Esto último da gran facilidad y operatividad al **operador**, que puede activar este tipo de tecnología individualmente a cada cliente que lo solicite. Además, no requiere un acondicionamiento especial en la central telefónica que sostiene a la línea en cuestión.

El **ADSL** basa su funcionamiento en crear dos canales de datos de ancho de banda asimétricos (uno de subida y otro de bajada). El canal de bajada (de central al usuario) es mucho mayor que el de subida (de usuario a central), que se adapta perfectamente al servicio de datos de Internet, ya que habitualmente el flujo de información de descarga es mucho mayor que el de subida.

Es por ello que el **ADSL** se emplea para el acceso a datos de Internet, dado que ofrece gran ancho de banda gracias a esta asimetría de los canales.

Además de los canales de datos, el **ADSL** incorpora un tercer canal destinado al servicio de voz, es decir, al servicio telefónico básico.

Esta estructura de tres canales obliga a poner dispositivos denominados **splitter** (que son básicamente **filtros**) que permitan separar en el usuario cada canal para que pueda emplearse simultáneamente el servicio de voz telefónico habitual con el servicio de datos en el mismo PTR del usuario.

Un **inconveniente** de esta tecnología es su fuerte dependencia con la distancia entre el usuario y la central. A mayor distancia, la velocidad y ancho de banda operativa se reduce debido a las interferencias y a la atenuación que aumenta en los cables. Es por ello que la distancia máxima permitida para ofrecer **ADSL** de buen ancho de banda se ha establecido en 6 km.

No obstante, esta tecnología ha evolucionado a versiones como **ADSL2** y **ADSL2+** que permiten alcanzar mayores distancias y mayores velocidades que el **ADSL** original.

En la siguiente tabla puede verse cómo ha evolucionado esta tecnología y con ello ha aumentado sus prestaciones en cuanto a ancho de banda y velocidades de transmisión.

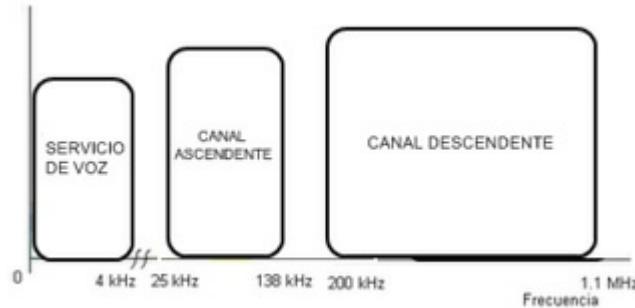
Nombre Comercial	Velocidad de bajada máxima	Velocidad de subida máxima
ADSL	8 Mbit/s	1,0 Mbit/s
ADSL (G.DMT)	12 Mbit/s	1,3 Mbit/s
ADSL2	12 Mbit/s	1,0 Mbit/s
ADSL2+	24 Mbit/s	1,0 Mbit/s
ADSL2+M	24 Mbit/s	3,5 Mbit/s

El funcionamiento del **ADSL** consiste en utilizar parte del espectro de frecuencia del hilo telefónico y que no empleaba el servicio telefónico básico de voz, cuya banda cubría desde los 300 Hz hasta los 3.400 Hz.

El servicio de datos que incluye el **ADSL** usa la banda de frecuencias desde los 24 KHz hasta los 1,1 Mhz, y mediante multiplexación y demultiplexación permite al usuario tener ambos servicios en el mismo PTR.

Esta multiplexación realizada en la central se consigue con unos dispositivos (habitualmente modems) que luego son concentrados en los llamados **DSLAM**, mientras que en el usuario se instala otro módem o set-top-box que debe incluir unos filtros (splitters) para separar ambas bandas y dar por un lado el servicio de voz (que se conecta al terminal telefónico) y el servicio de datos (conectado habitualmente a un router).

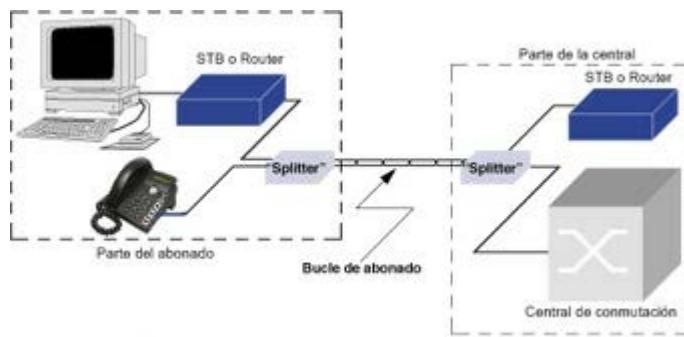
En la siguiente figura podemos ver el espectro de frecuencias asignados a cada banda del ADSL:



Los **splitters o filtros** anteriormente mencionados **realizan dos funciones**:

- ⇒ Separar o combinar **bandas de trabajos de diferentes servicios**.
- ⇒ Eliminar **interferencias entre ambas bandas**, es decir, que las señales del servicio telefónico de voz no se acoplen en la banda del servicio de datos y viceversa.

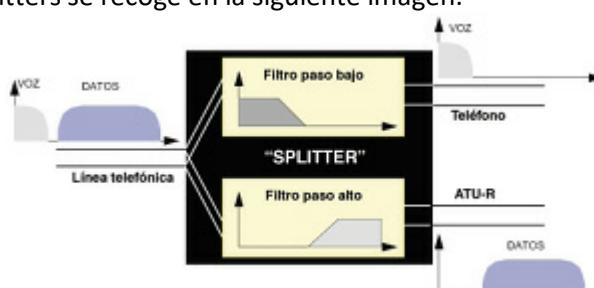
En la siguiente figura podemos ver cómo es el esquema y los elementos que componen esta estructura del ADSL.



En la figura anterior puede comprobarse la presencia del splitter como un conjunto de filtros paso bajo y paso alto que separa la banda del servicio telefónico básico y entrega su salida a un terminal telefónico y la banda del servicio de datos que entrega su salida a un router o un set-top-box.

En la parte de la central ocurre lo mismo ya que el servicio telefónico se conecta a la matriz de conmutación del operador de telefonía (RTC) y el servicio de datos se conecta a un proveedor de servicios de Internet (ISP).

El funcionamiento de los splitters se recoge en la siguiente imagen:



Como se aprecia en la anterior imagen, el **splitter es un conjunto de dos filtros**:

- ⇒ **Filtro paso bajo**: que deja pasar solo las **frecuencias bajas**, es decir, el servicio **telefónico básico**.
- ⇒ **Filtro paso alto**: que deja pasar solo las **frecuencias altas**, es decir, el servicio de **datos**.

Las **frecuencias de corte** de ambos filtros están ajustados al ancho de banda de cada una de las bandas que se quiere dejar pasar.

Además, **este filtrado evita las interferencias de unas bandas con otras, con lo que la señal es más ' limpia' e inmune y eso se traduce en una mayor velocidad de transmisión**.

Aunque el ADSL es una tecnología muy utilizada, existen otras tecnologías que forman parte de este grupo de sistemas xDSL.

Entre ellas destacan las variantes siguientes:

HDSL (High Data Rate Digital Subscriber Line)

Se trata de una tecnología con **anchos de banda y caudales simétricos** en el enlace ascendente y descendente pero de alta velocidad.

No se permiten distancias superiores a 3,6 Km desde el usuario a la central.

SDSL (Symmetric Digital Subscriber Line)

Se trata de una versión comercial y mejorada del HDSL con ancho de banda y caudales también simétricos en el enlace ascendente y descendente, pero con mayores tasas de velocidad.

IDS (ISDN Digital Subscriber Line)

Se trata de una tecnología xDSL empleada habitualmente sobre redes **RDSI**. Cada vez está más en **desuso**.

RADSL (Rate Adaptive Digital Subscriber Line)

Es una **tecnología similar al ADSL** pero que permite el **ajuste de los valores de transmisión en función de la longitud y otros parámetros de transmisión sobre el par de cobre**.

Esto permite adaptar diferentes velocidades de transmisión en función del estado y propiedades del cobre instalado.

VDSL y VDSL2 (Very High Speed Digital Subscriber Line)

La **tecnología VDSL** es la que ofrece mayores tasas de transferencia con caudales que oscilan entre 13 y 52 Mbps en el canal descendente y de 1,5 a 2,3 Mbps en el canal ascendente.

Su principal inconveniente es que limita la distancia entre el usuario y la central a 1,5 km.

VDSL2 es una mejora de la VDSL que permite mayores tasas de transferencia en función de la distancia usuario-central.

Esta tecnología es capaz de soportar servicios de telecomunicaciones de altas requerimientos de transmisión como Vídeo bajo demanda (VoD), streaming de vídeo, etc

2.1.2. Redes de acceso vía radio: WLL, MMDS, LMDS

Como ya se ha descrito anteriormente la red de acceso también puede implementarse mediante tecnologías inalámbricas, es decir, **por radiofrecuencias**.

Entre ellas destacan principalmente **las tres tecnologías más utilizadas**:

Tecnología WLL

WLL son las siglas de Wireless Local Loop, es decir, **bucle local inalámbrico**. Se trata de una tecnología vía radio para **ofrecer servicios de banda ancha** (fundamentalmente telefonía e Internet) **a los usuarios en la última parte de la red**, es decir, la conocida como la **última milla**.

Trabajan en las **frecuencias licenciadas**, por lo que está asignado habitualmente a operadores de telecomunicaciones privadas que proporcionan los servicios de telefonía y de Internet a sus clientes.

La **estructura** de esta tecnología se basa en la **instalación de un conjunto de estaciones base interconectadas entre sí por radiofrecuencia** que **concentran todo el tráfico de datos** y que transmiten dicha información a **los terminales de los usuarios** mediante radioenlace.

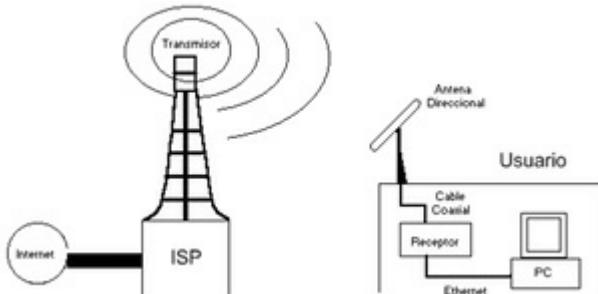
Como toda tecnología por radioenlace, **precisa de visibilidad directa entre las estaciones base**, por lo que su ubicación debe realizarse en **lugares altos como edificios, torretas, montes, etc.**

La **gran ventaja** de esta tecnología es su **rápida implementación** (no requiere cable), un ancho de banda alto para los usuarios (del orden de **Mbps**) y fácilmente escalable.

Como **desventaja** tiene que es más **sensible a la orografía del terreno y a las interferencias con otras señales de radiofrecuencia**.

La transmisión se puede realizar siguiendo una **estructura punto-punto o punto-multipunto**.

En la siguiente figura podemos ver el esquema de funcionamiento de la tecnología WLL:



En la figura anterior se puede observar que el sistema se basa en una antena transmisora que da servicio por radio a los abonados que requiere de una antena receptora en sus tejados, la cual con la electrónica necesaria se conecta al PTR (Punto de terminación de red) de la vivienda.

Esta antena transmisora puede dar **cobertura** a una zona de **varios kilómetros** y a una horquilla de entre **50 y 200 usuarios**, dependiendo de la orografía de la zona de cobertura.

Esta antena se conecta a la red de telefonía conmutada (RTC) o a los proveedores de servicios de Internet (ISP) generalmente por cable, ya sea por par trenzado o fibra óptica.

Es imprescindible en esta arquitectura la visibilidad entre antena transmisora y receptora.

Esta tecnología se ha empleado con mucha frecuencia para dar servicio telefónico y de Internet a zonas rurales o de difícil acceso.

Tecnología MMDS

MMDS son las siglas de Microwave Multipoint Distribution System, es decir, **Sistema de distribución multipunto por microondas**.

Se trata de una tecnología que se creó para dar servicio de vídeo y televisión por radio a zonas con orografía complicada y zonas alejadas (entornos rurales, polígonos industriales, etc.).

Las **velocidades de transmisión rondan los 2-5 Mbps para alcances de hasta 20 km, y aunque se empleó originariamente para vídeo luego se amplió para el servicio de datos**.

La banda de MMDS utiliza la frecuencia de microondas, es decir, de los **2 Ghz a 3 Ghz en banda L**. Es por ello que requiere antenas cuya banda de trabajo esté en estas frecuencias, así como un decodificador para la recepción en el abonado.

En la siguiente imagen puede verse el ejemplo de una antena receptora para esta tecnología de MMDS.



Esta tecnología ha sido sustituida por su sucesor, el LMDS, cuyo funcionamiento es similar pero ofrecía mayores velocidades de transmisión.

Tecnología LMDS

LMDS son las siglas de Local Multipoint Distribution System, es decir, **Sistema de distribución multipunto local**.

Se trata de una tecnología inalámbrica para la distribución de servicios de datos y/o telefónico en la frecuencia de los **26 Ghz**.

Requiere, al igual que la tecnología MMDS, de un conjunto de estaciones base interconectadas entre sí (bien por radioenlace o de forma cableada) y donde cada una de ellas da cobertura inalámbrica a un conjunto de usuarios que precisará una antena receptora junto con su decodificador.

La distancia entre antenas no debe superar los 3 km (menor que MMDS) pero se alcanzan mayores velocidades de transmisión que oscilan entre los 50 a 622 Mbps.

Esta tecnología ha sido ampliamente utilizada en entornos rurales y en zonas con orografía complicada para sustituir los antiguos TRAC (servicio telefónico básico por radio), ofreciendo con ello este servicio de voz además de servicio de Internet.

La tecnología LMDS es una tecnología inalámbrica muy utilizada para dotar de servicios de banda ancha a zonas aisladas (rurales) y de difícil orografía donde los costes de dotarlo con redes cableadas los hacen inviables.

WIMAX

WiMAX (Worldwide Interoperability for Microwave Access - interoperabilidad mundial para acceso por microondas), es una norma de transmisión de datos que utiliza las ondas de radio en las frecuencias de 2,5 a 5,8 GHz y puede tener una cobertura hasta de 70 km.

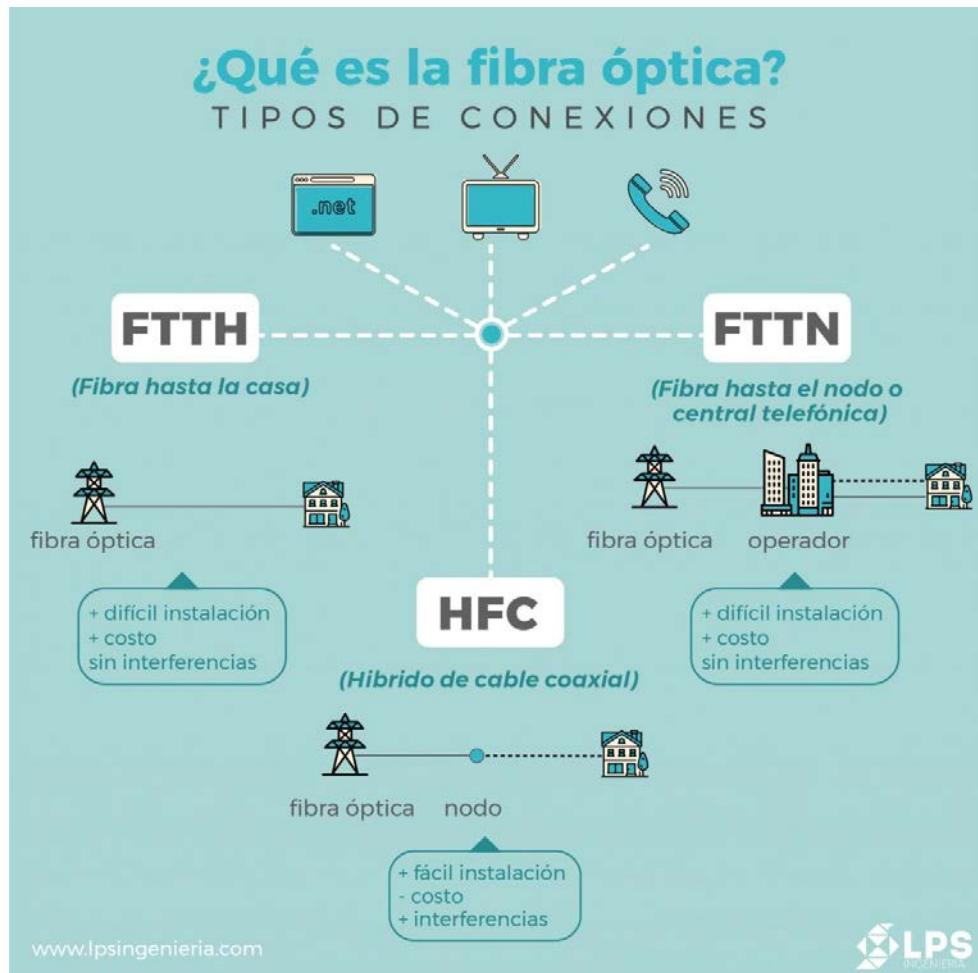
Es una tecnología dentro de las conocidas como tecnologías de última milla, también conocidas como bucle local que permite la recepción de datos por microondas y retransmisión por ondas de radio



Simulador WIMAX: <https://airlink.ui.com/#/ptp>

2.1.3. Redes de acceso vía fibra óptica: HFC, PON y CWDM

Las redes de acceso también se pueden implementar con redes de fibra óptica como medio de transmisión cableada.



En este caso, dan lugar a diferentes tecnologías, como son:

- ⇒ Tecnología HFC.
- ⇒ Tecnología PON.
- ⇒ Tecnología CWDM.

A continuación, veremos con más detalles cada una de ellas.

Tecnología HFC

HFC son las siglas de Hybrid Fiber Coaxial, es decir, redes híbridas de fibra y coaxial.

Se trata de una red de acceso que **aprovecha parte del coaxial ya instalado** (**la parte más capilarizada**, es decir, el último tramo del abonado) **y lo conecta a redes de fibra óptica** (**la parte troncal de la red**) para con ello ofrecer mayores velocidades de transmisión al usuario.

Esto se realiza porque **la velocidad de transmisión tiene una fuerte dependencia con la distancia desde la central al nodo de conmutación**. Es por ello que **se intenta minimizar el tramo de coaxial** (que supone el cuello de botella de la red) empleando el otro tramo con fibra óptica, cuya atenuación y ancho de banda es mucho más elevado.

De esta forma se consigue aumentar sensiblemente las prestaciones de red sin suponer altos costes de instalación.

Estas redes HFC presentan **dos niveles jerárquicos**:

- ⇒ **Un primer nivel con topología en estrella que parte del nodo o central y que llega a nodos secundarios distribuidos en una ciudad** con armarios tipo muxfin (MULTipleXor Flexible de Interfaces Normalizadas) o similar y **que realiza la conversión óptico-eléctrica y su distribución por coaxial**.



⇒ Un segundo nivel con topología en bus que partiendo desde los nodos secundarios llega a todos los abonados mediante coaxial.

Con las redes HFC se han podido distribuir servicios de voz, vídeo y datos a alta velocidad bajo la denominación **Triple play**.

Cada nivel de la red es la responsable de unas determinadas funciones con una gestión propia, es decir:

Red de transporte

Corresponde a la parte de **fibra** y suele estar formada por **un anillo de fibra primaria** al que se conectan **diversos anillos de fibra secundarios** también en fibra.

Concentra el tráfico troncal y sus velocidades de transferencia son muy altas.

Cada nodo secundario puede alimentar a unos 500 abonados y un nodo primario a unos 10.000 abonados.

Red de distribución

Corresponde a la parte de coaxial que, **partiendo del nodo secundario óptico y siguiendo una topología en bus, llega hasta los abonados**.

En el abonado **es necesario un elemento adaptador** que se ubica generalmente en fachada y que realiza **además la conversión a cobre**.

En esta tecnología HFC han aparecido dos estándares que definen sus especificaciones:

- **DOCSIS**: es un estándar que surgió en 1997 por los principales operadores de cable de Estados Unidos y que ha tenido gran implementación.
- **DAVIC**: es un estándar definido por la DVB (Digital Video Broadcast) pero que no ha tenido tanta implantación como la anterior.

Tecnología PON

PON son las siglas de Passive Optical Network. Representa una tecnología de red de acceso basada en una **red óptica pasiva**, es decir, **no incluyendo elementos activos (amplificadores) en la red de distribución desde la central hasta el abonado**.

Este tipo de tecnología es ampliamente **utilizada en las redes FTTH**.

Su alta expansión se debe a las continuas demandas de ancho de banda y prestaciones que requieren los nuevos servicios de telecomunicaciones y en especial los servicios **Triple play**.

Las redes de cable y de ADSL (aunque cubría gran parte de estas redes) tienen el problema de que están limitadas en prestaciones, ya que a lo sumo pueden ofrecer 100 Mbps en el canal descendente y 50 en el canal ascendente, además de su fuerte dependencia con la distancia entre la central y el abonado (máximo 6 km).

Es por ello que la fibra óptica es la solución alternativa que permite superar estos obstáculos, ya que sus **ventajas** son:

- ⇒ **Gran ancho de banda.**
- ⇒ **Descenso** continuo del **precio** de sus elementos y en especial de la fibra y de los láseres ópticos.
- ⇒ Aumento de la **distancia** hasta 20 Km entre la central y los abonados.
- ⇒ **Inmunidad** ante las **interferencias electromagnéticas**.
- ⇒ Posibilidad de incorporar **nuevos servicios de telecomunicación con QoS**.

Una red PON la forman los siguientes **elementos**:

- ⇒ Un módulo **OLT** (Optical Line Terminal), que es un dispositivo óptico ubicado en la central.
- ⇒ Un divisor óptico denominado **splitter**.
- ⇒ Numerosos **ONTs** (Optical Network Terminal), que son dispositivos ópticos situados en el domicilio del abonado.

La red PON se comporta de dos maneras:

- ⇒ Como red **Punto-Multipunto** en la dirección **Central-Abonado**, es decir, en la dirección **OLT-ONT** (**canal descendente**).
- ⇒ Como red **Punto-Punto** en la dirección **Abonado-Central**, es decir, en la dirección **ONT-OLT** (**canal ascendente**).

El esquema de una red PON se puede ver en la siguiente figura:



En ella se aprecia cómo el módulo OLT se conecta a un splitter (divisor óptico) que da acceso a las unidades ONT ubicadas en cada abonado.

Todos los tramos se realizan con fibra óptica. En el tramo **OLT-Splitter** se emplea habitualmente **fibra multimodo** y en el tramo **Splitter-ONT** es más habitual usar **fibra monomodo**.

Las redes **PON** emplean la **multiplexación por longitud de onda (WDM)** para los canales **ascendente y descendente**.

Bajo esta tecnología y arquitectura PON se han definido diversas variantes o **estándares** entre las que destacan las siguientes:

Redes APON (ATM PON)

Se trata de una red **PON** que emplea la **tecnología ATM (modo de transferencia asíncrono)** para el canal descendente y que consigue con ello velocidades de transferencia de 622 Mbps de salida del OLT (debe repartirse entre todas las ONTs conectadas).

Redes BPON (Broadband PON)

Se trata de una red **APON mejorada** para ofrecer servicios de gran ancho de banda. En ella se pueden **configurar los canales ascendente y descendente a diferentes velocidades**.

Así, podemos conseguir las siguientes velocidades en cada canal:

- ⇒ Canal ascendente con velocidades de 155 Mbps y 622 Mbps.
- ⇒ Canal descendente con velocidades de 155 Mbps, 622 Mbps y 1,25 Gbps.

Sus especificaciones quedan definidas en la normativa ITU-T G.983.x.

Redes GPON (Gigabit PON)

Son redes PON con velocidades de transferencia de **Gigabit Ethernet**.

Así, podemos obtener las siguientes velocidades en cada canal:

- ⇒ Canal ascendente con velocidades de 155 Mbps, 622 Mbps, 1,25 Gbps y 2,5 Gbps.
- ⇒ Canal descendente con velocidades de 1,25 Gbps y 2,5 Gbps.

Sus especificaciones quedan definidas en la normativa ITU-T G.984.x.

Redes EPON (Ethernet PON)

Son redes PON que emplean la fibra óptica para crear redes Ethernet.

Por ello siguen las especificaciones del 802.3 y su gran ventaja es que trabajan con tramas Ethernet, por lo que reducen los costes en su implementación.

Con esta tecnología se consiguen las siguientes velocidades de transferencia en cada canal:

- ⇒ Canal ascendente con velocidad de 1,25 Gbps.
- ⇒ Canal descendente con velocidad de 1,25 Gbps.

Redes 10GPON (10 Gigabit PON)

Son redes PON que consiguen velocidades de transferencia del orden de los **10Gbps**.

Son las redes PON más avanzadas que existen en estos momentos y son capaces de admitir grandes flujos de datos.

Con esta tecnología se consiguen las siguientes velocidades de transferencia en cada canal:

- ⇒ Canal ascendente con velocidad de 1,25 Gbps o 10 Gbps.
- ⇒ Canal descendente con velocidad de 10 Gbps.

En la siguiente tabla recogemos una comparativa de todos estos estándares.

Tecnología	APON	BPON	GPON	EPON	10GPON
Estándar	ITU-T.G983x	ITU-T.G983x	ITU-T.G984x	802.3ah	802.3ah
Velocidades de transmisión (Mbps)	Canal ascendente: 155, 622 Canal descendente: 155 y 622	Canal ascendente: 155, 622 Canal descendente: 155, 622 y 1244	Canal ascendente: 155, 622, 1244, 2488 Canal descendente: 1244 y 2488	Canal ascendente: 1244 Canal descendente: 1244	Canal ascendente: 1244 y 10000 Canal descendente: 10000
Tipo de fibra empleada	Monomodo	Monomodo	Monomodo	Monomodo	Monomodo
Máxima distancia entre OLT y ONU	20 km	20 km	10-20 km	10 km	20 km
Arquitectura de transmisión	Asimétrica o simétrica	Asimétrica o simétrica	Asimétrica o simétrica	Simétrica	Asimétrica o simétrica

A continuación describiremos con más detalle cada uno de los elementos que forman parte de una red PON.

OLT

El OLT es un dispositivo óptico activo **ubicado en la central del proveedor y que se conecta al splitter o divisor óptico mediante fibra**.

Su función principal es la de **hacer de router para gestionar el tráfico demandado por los abonados**. Es capaz de gestionar cientos de abonados, además de permitir la conectividad con otras redes externas.

En resumen, las funciones del OLT son:

- ⇒ **Gestionar y enrutar el tráfico de las ONTs.**
- ⇒ **Conectar la red PON con otras redes.**

El OLT actúa como concentrador de redes externas que ofrecen los servicios de voz, datos y vídeo. Es por ello que su cabecera **permite la conectividad con**:

- ⇒ La red **RTC** para los servicios de voz **telefónica básica**.
- ⇒ Proveedores **ISP** para los **servicios de datos a través de un Gateway**.
- ⇒ Proveedores de **Vídeo (VoD)** a través de un **Gateway**.

El OLT como dispositivo hardware está formado por varios **módulos**:

- ⇒ **Módulo P-OLT (Provider OLT)**

Es el **módulo** encargado de **recoger las tramas de las redes de voz y datos procedentes del exterior (red RTC e ISP) y de inyectarlas a la red PON mediante multiplexación TDM**. Emplea la ventana de los **1490 nm**.

Además, recoge las tramas de datos y voz procedentes de la red PON y las dirige a la red RTC o ISP donde corresponda en la ventana de 1310 nm.

⇒ **Módulo V-OLT (Vídeo OLT)**

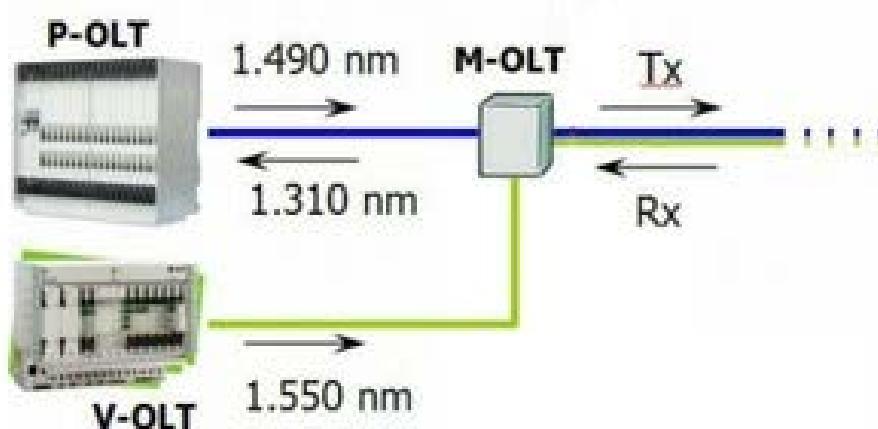
Es el módulo encargado de recoger las tramas del red de vídeo exterior (VoD) y de inyectarlas en la red PON, empleando para ello la ventana de los 1550 nm.

También recoge las tramas de vídeo de la red PON y las dirige a la red exterior de vídeo también en la misma ventana de los 1550 nm.

⇒ **Módulo M-OLT (Multiplexer OLT)**

Es el encargado de realizar la multiplexación de ambos servicios suministrados por el P-OLT y V-OLT bajo una multiplexación WDM.

En la siguiente figura podemos ver los módulos que componen el OLT y las ventanas de trabajo que emplea para cada canal.



ONT

El ONT es un dispositivo óptico ubicado en el domicilio del cliente capaz de recibir y filtrar la información recibida por el OLT para entregársela al abonado. A su vez, recoge la información y petición del abonado para encapsularla y entregársela al OLT para que pueda procesarla.

Existen dos tipos de ONT:

- ⇒ H-ONT (Home ONT): es un dispositivo que se coloca en el hogar. Es el empleado en las redes FTTH.
- ⇒ B-ONT (Building ONT): es un dispositivo que se coloca en el RITI o RITU del edificio. Es el empleado para redes FTTB.

El ONT en definitiva realiza un filtrado de la información separando los servicios de voz, datos y vídeo.

Para ello incorpora dos filtros ópticos:

- ⇒ Filtro OAF (Optical Analogic Filter): es quien se encarga de obtener la señal de vídeo a la longitud de onda de los 1550 nm y la entrega al fotodiodo APD (Fotodiodo De Avalanche) para realizar la conversión de frecuencia.
- ⇒ Filtro ODF (Optical Digital Filter): es quien se encarga de obtener la señal de voz y datos a la longitud de onda de los 1490 nm y la entrega al fotodiodo digital DPD (Dinámicos).

Splitter Óptico

Se trata de un dispositivo pasivo óptico que actúa como divisor de señales, ya que recibe las señales procedentes del OLT y las entrega a las diferentes ONT conectados a él.

Sus funciones son las de:

- ⇒ Multiplexar las señales recibidas.
- ⇒ Dividir la señal de entrada entre un número de salida.
- ⇒ Combinar las señales recibidas y entregarlas por una única salida.

Además, al tratarse de un elemento pasivo no requiere alimentación.

El inconveniente principal del splitter es la pérdida de potencia óptica debido a la división de señal en múltiples salidas. Esta atenuación de la señal de salida viene dada por la siguiente expresión.

$$\text{Atenuación}_{\text{salida}} = 10 \times \log (1 / N)$$

Siendo N el número de salidas del divisor.

Existen divisores ópticos o splitters de 2, 4, 8, 16, 32 y 64 salidas.

Las redes PON son redes pasivas de fibra óptica que permiten altas tasas de transferencia para los usuarios y con ello ofrecer los nuevos servicios de Triple Play (voz, datos y televisión).

Tecnología CWDM

CWDM son las siglas de Coarse WDM, es decir, una tecnología basada en la transmisión óptica empleando multiplexación por división en longitud de onda.

CWDM emplea la fibra óptica multimodo para la transmisión de datos, y se emplea para transmisiones de corta distancia a diferencia de la tecnología DWDM para largas distancias.

CWDM tuvo sus orígenes en la transmisión de vídeo (CATV). Su característica principal era que sus componentes ópticos (sobre todo láseres) eran de menor complejidad, ya que se permitía obtener un ancho de banda menor que en la tecnología DWDM y con ello su coste era menor.

Es por ello que CWDM tuvo tanta implantación para redes de corta distancia, pues su coste era menor a pesar de tener un ancho de banda alto (aunque inferior al DWDM).

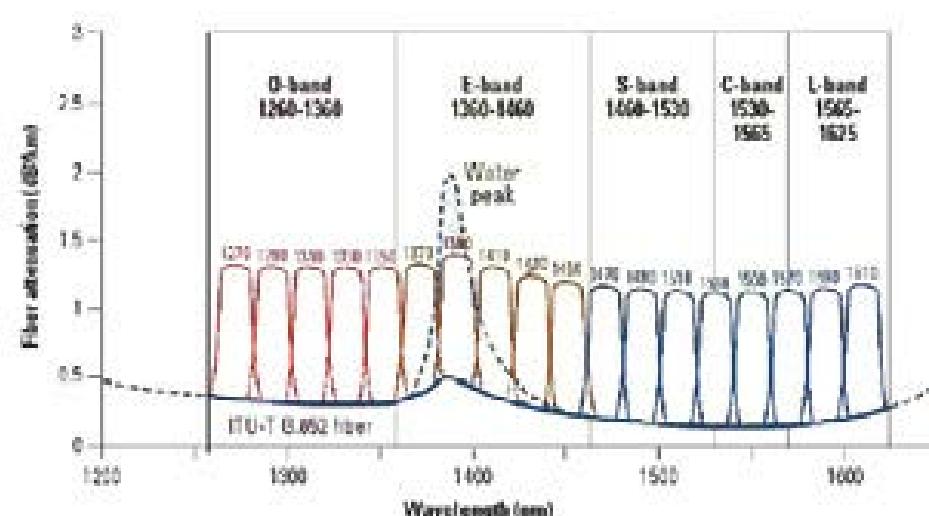
CWDM se transmite en 18 canales o longitudes de onda, con un ancho de banda de 20 nm en el intervalo de 1270 a 1610 nm en las bandas O, E, S, C y L.

Es por ello que dispone de gran ancho de banda para distancias máximas de 120 km.

Esta tecnología emplea Laser DBF, es decir, láseres de realimentación distribuidos, cuyos costes de fabricación son sensiblemente menores que los empleados en las redes DWDM.

CWDM se emplea en tecnología PON, FTTH, CATV y ATM, entre otros.

En la siguiente figura podemos ver los canales o longitudes de onda en los que trabaja la tecnología CWDM.



En la anterior figura se pueden observar los 18 canales de 20 nm que emplea la tecnología CWDM. A destacar el 'pico de agua' en la longitud de los 1390 nm que provoca una alta atenuación en este canal y que por ello a menudo este canal no se emplea para las largas distancias usando esta tecnología.

2.2. Redes troncales

Las redes troncales o de transporte constituyen el segundo nivel y constituyen la parte de la red que tiene la mayor capacidad de tráfico que luego se capilariza en los niveles de acceso.

También es denominado habitualmente 'backbone'. Se encarga en definitiva de que los servicios puedan llegar a cualquier situación geográfica.

La misión última de la red troncal es concentrar y distribuir todo el tráfico generado entre los diferentes usuarios que proceden de las diferentes redes de acceso.

La mayor parte de esta red se implementa sobre fibra óptica debido a la gran cantidad de tráfico que debe soportar este nivel de red.

Los motivos que llevan a usar la fibra óptica para este nivel de red son los siguientes:

- ⇒ Baja atenuación.
- ⇒ Gran ancho de banda.
- ⇒ Fácil instalación.
- ⇒ Inmunidad ante interferencias electromagnéticas.
- ⇒ Alta seguridad.
- ⇒ Integración con cualquier tipo de red.

El tipo de fibra óptica habitualmente utilizado es la fibra monomodo, ya que es la que cumple los anteriores requisitos.

En este nivel de red han aparecido las siguientes tecnologías:

- ⇒ Tecnología PDH.
- ⇒ Tecnología SDH.
- ⇒ Tecnología ATM.

Veremos a continuación y con más detalle cada una de estas tecnologías.

Las redes troncales constituyen la parte de la red del operador que concentra todo el tráfico de las diferentes redes de acceso. Constituye el backbone del operador con un gran ancho de banda y altas tasas de transferencia. Suele estar implementado con fibra óptica monomodo.

2.2.1. MTA (Modo de transferencia asíncrono – ATM)

ATM son las siglas de [Asynchronous Transfer Mode](#). Representa una tecnología de [multiplexación y conmutación de celdas o pequeños paquetes de longitud fija aprovechando las ventajas de la conmutación de circuitos y la conmutación de paquetes](#).

Proporciona un ancho de banda variable y ajustable según las necesidades que van [desde los 2 Mbps hasta los 10 Gbps](#).

Las [ventajas](#) del ATM son las siguientes:

- ⇒ [Capacidad garantizada y retardo de transmisión constante](#).
Esto lo obtiene de la [conmutación de circuitos](#).
- ⇒ [Flexibilidad y eficiencia para el tráfico rafagueado](#).
Esto lo obtiene de la conmutación de paquetes.
- ⇒ [Permite integrar diferentes servicios con QoS diferentes](#).

ATM se caracteriza por ser asíncrona y es por ello que lo hace más eficiente que otras tecnologías como TDM, que son síncronas.

Esto [caracteriza](#) a ATM en el sentido de que:

- ⇒ [No hay control del flujo y corrección de errores nodo a nodo](#).
- ⇒ Trabajo en [modo orientado a conexión](#).
- ⇒ Tiene una [cabecera eficiente](#).
- ⇒ El [campo de información](#) es relativamente [pequeño](#), lo que favorece una [comutación rápida](#).
- ⇒ [Utiliza paquetes o slots de longitud fija](#).

Una red ATM está formada principalmente por los siguientes elementos:

- ⇒ **Conmutadores o switches ATM**

Son dispositivos encargados del tránsito de celdas ATM dentro de la red.

Leen la cabecera de la celda ATM y en función de esta la comuta a uno u otro nodo.

- ⇒ **Puntos finales ATM**

Actúan como interfaz de entrada o salida a la red ATM.

Leen el contenido de la celda ATM (además de su cabecera) y en función de ello lo entrega a un destinatario final que puede ser un servidor, conmutador LAN, router, etc.

Dentro de los conmutadores ATM existen dos tipos:

- [Conmutador UNI \(User Network Interface\)](#): conecta destinatarios finales como router, servidores, etc., a un conmutador ATM.
- [Conmutador NNI \(Network to Network Interface\)](#): conecta dos conmutadores ATM.

Estos conmutadores, tanto UNI como NNI pueden ser privados o públicos. En el primer caso su propiedad y ubicación están en el cliente final (es privado) y en el segundo caso su propiedad está ubicada en el operador ATM.

La celda ATM es una trama de formato fijo de 53 octetos o bytes de donde los primeros 5 bytes se corresponden a la cabecera (cabecera pequeña para rápida conmutación) y los 48 bytes restantes es información del usuario.

En la siguiente figura podemos ver el formato de trama de la celda ATM.

Cabecera	Información
5 bytes	48 bytes

El formato de cabecera de la celda ATM puede admitir dos formatos:

- ⇒ Formato UNI: que es el empleado por los conmutadores UNI.
- ⇒ Formato NNI: que es el empleado por los conmutadores NNI.

El formato de cabecera de celda ATM UNI es el que se muestra en la siguiente figura:

----- 8 bits -----		
Campo de Control de flujo (GFC)	Identificador de Camino virtual (VPI)	
Identificador de Camino virtual (VPI)	Identificador de Canal virtual (VCI)	
Identificador de Canal virtual (VCI)		
Identificador de Canal virtual (VCI)	Identificador de tipo de carga (PTI)	Prioridad de pérdida de celda (CLP)
Campo de control de errores (HEC)		

En ATM se define lo que se denomina canal virtual (VC) o camino virtual (VP).

Un canal virtual (VC) es la multiplexación de varios flujos de información entre dos nodos ATM.

Un camino virtual (VP) es la multiplexación de varios canales virtuales en la red ATM.

Por tanto, un camino virtual (VP) es un conjunto de canales virtuales (VC).

Es por ello que en la cabecera ATM existen los campos de identificación del canal virtual (VCI) y el identificador de camino virtual (VPI) para que el conmutador pueda saber a qué nodo debe dirigir la celda ATM.

El campo de control de flujo (GFC) es un campo encargado del control y gestión del tráfico, aunque en la práctica apenas se emplea.

El campo de identificador de tipo de carga (PTI) indica si la celda contiene datos de usuarios y datos de control.

El campo de prioridad de pérdida de celda indica si dicha celda ATM puede ser descartada en caso de congestión de la red.

El campo de control de errores (HFC) es un campo checksum.

En cambio el formato de la cabecera de celda ATM NNI tiene un formato ligeramente diferente al anterior.

----- 8 bits -----		
Identificador de Camino virtual (VPI)		
Identificador de Camino virtual (VPI)	Identificador de Canal virtual (VCI)	
Identificador de Canal virtual (VCI)		
Identificador de Canal virtual (VCI)	Identificador de tipo de carga (PTI)	Prioridad de pérdida de celda (CLP)
Campo de control de errores (HEC)		

Es decir, en este caso solo varía los primeros bits de la cabecera, eliminando el campo de control de flujo (GFC) y ampliando el del identificador de camino virtual (VPI).

2.2.2. JDP (Jerarquía Digital Plesióncrona – PDH)

PDH son las siglas de Plesiosynchronous Digital Hierarchy y representa [unas de las primeras tecnologías troncales que aparecieron en la década de los 70](#).

[Esta tecnología se empleaba en aquella época para la transmisión de las señales telefónicas de voz que se digitalizaban según la técnica de muestreo PCM](#) (modulación por impulsos codificados - Pulse Code Modulation).

PDH se caracterizaba por emplear transmisiones digitales que permitían tasas de transferencia hasta 565 Mbps fraccionados en múltiplos de 2 Mbps.

Esta tecnología creaba canales múltiples de 2 Mbps porque un canal de 2 Mbps era lo que cabía por transmitir 30 canales de voz telefónico muestreado con PCM.

Esta tecnología se basaba en un entrelazado de bit que obligaba a sincronizar las distintas fuentes de información a transmitir.

Como las diferentes fuentes no tenían por qué transmitir a las mismas tasas de transferencia sobre este sistema se crearon diferentes mecanismos de control para absorber esas asincronías de las fuentes (de ahí el término de plesícrona que indica casi síncrona).

Este fue uno de los motivos por los que esta tecnología **fue sustituida por otras como la SDH, que no presentaba este problema y en la que además las redes cada vez más eran más digitales.**

Veamos un ejemplo.

Justifique mediante cálculos el número de canales de voz digitalizadas (30) que permitía transmitir un canal de 2 Mbps empleando la tecnología PDH.

Solución:

El servicio telefónico básico tiene un ancho de banda que va desde los 300 Hz hasta los 3.400 Hz. Es por ello que su ancho de banda es:

$$\text{Ancho de banda} = 3.400 - 300 = 3.100 \text{ Hz.}$$

Si digitalizamos la señal y con objeto de no perder información, aplicamos el teorema de muestreo que nos dice que:

$$F_{\text{muestreo}} \geq 2 \times \text{ancho de banda.}$$

Es decir, en nuestro caso particular quedaría como:

$$F_{\text{muestreo}} \geq 2 \times 3.100 \text{ Hz} = 6.200 \text{ Hz.}$$

Redondeamos y aplicamos una frecuencia de muestro de 8 KHz.

Para la cuantificación usaremos 8 bits, es decir, 256 valores. Con ello, la tasa binaria para un canal de voz es:

$$\text{Tasa binaria} = F_{\text{muestreo}} \times \text{Nº bits cuantificación} = 8 \text{ KHz} \times 8 = 64 \text{ Kbps.}$$

Si multiplicamos esa tasa binaria por 30 canales de voz, nos sale que:

$$\text{Caudal de 30 canales de voz digitalizada} = 30 \times 64 \text{ Kbps} = 1920 \text{ Mbps} \approx 2 \text{ Mbps.}$$

Aquí está la justificación de cómo en un canal de 2 Mbps podemos transmitir 30 canales de voz de señal de voz telefónico digitalizada.

Veamos otro ejemplo.

En Estados Unidos y Japón también se empleó la tecnología PDH para la transmisión de caudales de señal de voz telefónica digitalizada, pero con canales de 1,5 Mbps.

Indique y justifique cuántos canales de voz digitalizada podemos transmitir por ese canal de 1,5 Mbps.

Solución:

Partimos del mismo punto de que el servicio telefónico tiene el mismo ancho de banda y se digitaliza con el mismo número de bits de cuantificación, es decir:

$$\text{Ancho de banda} = 3.400 - 300 = 3.100 \text{ Hz.}$$

Muestreamos aplicando el teorema de muestreo.

$$F_{\text{muestreo}} \geq 2 \times 3.100 \text{ Hz} = 6.200 \text{ Hz} \approx 8 \text{ KHz.}$$

Para la cuantificación usaremos 8 bits, es decir, 256 valores, luego con ello, la tasa binaria para un canal de voz es:

$$\text{Tasa binaria} = F_{\text{muestreo}} \times \text{Nº bits cuantificación} = 8 \text{ KHz} \times 8 = 64 \text{ Kbps.}$$

Si disponemos de un caudal de 1,5 Mbps, el número de canales de voz telefónica digitalizada es de:

$$\text{Número de canales de voz} = (1,5 \text{ Mbps}) / (64 \text{ kbps}) = (1536 \text{ Kbps}) / (64 \text{ kbps}) = 24 \text{ canales}$$

Luego para el caso de EEUU y Japón para un canal de 1,5 Mbps sólo podemos transmitir 24 canales de señal de voz telefónica digitalizada.

Veamos un ejemplo más.

Sobre el ejemplo anterior, en comunicaciones militares es admisible pérdida de calidad de la información telefónica transmitida (sobre todo timbre) a cambio de obtener un mayor número de canales a transmitir por el caudal siempre y cuando la comunicación sea audible e interpretable.

Es por ello que se admite un menor nivel de cuantificación en la digitalización de la señal.

Si sobre el canal de transmisión de 1,5 Mbps, aplicamos un nivel de cuantificación de 4 niveles, indique y calcule cuantos canales de voz telefónica digitalizada podemos transmitir.

Solución:

Partimos del mismo punto de que el servicio telefónico tiene el mismo ancho de banda y donde se le aplica el teorema de muestreo.

$$\text{Ancho de banda} = 3.400 - 300 = 3.100 \text{ Hz.}$$

$$F_{\text{muestreo}} \geq 2 \times 3.100 \text{ Hz} = 6.200 \text{ Hz} = 8 \text{ KHz.}$$

Dado que cuantificamos con 4 niveles, eso indica que necesitamos sólo 2 bits para cuantificar cada muestra de la señal, es decir:

$$2x = 4 \text{ niveles} \Rightarrow x = 2 \text{ bits para cuantificar.}$$

Luego la tasa binaria de cada canal de voz digitalizada queda en:

$$\text{Tasa binaria} = F_{\text{muestreo}} \times \text{Nº bits cuantificación} = 8 \text{ KHz} \times 2 = 16 \text{ Kbps.}$$

Si disponemos de un caudal de 1,5 Mbps, el número de canales de voz telefónica digitalizada es de:

$$\text{Número de canales de voz} = (1,5 \text{ Mbps}) / (16 \text{ kbps}) = (1536 \text{ Kbps}) / (16 \text{ kbps}) = 96 \text{ canales}$$

Es decir, hemos multiplicado por 4 el número de señales de voz telefónica digitalizada que podemos transmitir por un canal de 1,5 Mbps.

Eso sí, se ha perdido parte de calidad de cada señal

2.2.3. JDS (Jerarquía Digital Síncrona – SDH)

SDH son las siglas de Synchronous Digital Hierachy. Representa a una tecnología troncal de transporte que surgió de la evolución de su antecesora, la tecnología PDH, corrigiendo los problemas que presentaba este último.

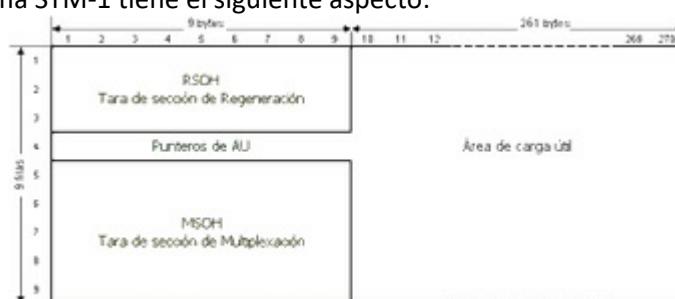
Esta tecnología tuvo gran expansión a raíz de la digitalización de todas las comunicaciones de voz y de datos ya que alcanzaban tasas de transferencia desde los 155 Mbps hasta los 40 Gbps con canales de 2 Mbps.

La gran ventaja de SDH es su compatibilidad con diferentes tecnologías incluidas PDH y ATM, lo que permitía una gran interoperabilidad de equipos y con ello soportaba una amplia variedad de servicios desde voz, datos, redes alquiladas, redes de televisión, etc.

2.2.3.1. Estructura de la trama

SDH basa su funcionamiento en una estructura fija denominada trama STM-1, que es un slot de tiempo con una duración de 125 µseg y se corresponde con una matriz de 9 filas y 270 columnas cuyos elementos son octetos de 8 bits. La velocidad de esta trama es de 155 Kbps.

La estructura de una trama STM-1 tiene el siguiente aspecto:



Puede observarse cómo la trama se dispone en 9 filas por 270 columnas.

Esta trama presenta las siguientes partes:

- ⇒ Los primeros 9 bytes de cada fila se denominan tara de cabecera u Overhead.
- ⇒ Los restantes bytes de cada fila se denominan carga útil.

La tara de cabecera se divide en tres partes:

- ⇒ El R-SOH que contiene información de gestión y control entre los repetidores de la tecnología SDH y cuyas funciones son, entre otras, las de:
 - Señal de alineamiento.
 - Monitorización de errores.
 - Señalización de conmutación automática.

Estado de sincronización.

- ⇒ Puntero de unidad administrativa que contiene información de gestión de la red.
- ⇒ El M-SOH que contiene información de la monitorización de la calidad de transmisión. Se compone del Contenedor Virtual (VC) que es la carga útil que viaja sin cambios en la red y de algunos bytes que se añaden en los puntos de terminación del servicio.

La transmisión de la trama se realiza fila a fila hasta completar las 9 filas que componen la trama con una orientación de izquierda a derecha y de arriba abajo.

2.2.3.2. Velocidades

PDH está basado en una trama básica denominada SMT-1, que es la descrita anteriormente.

Pero admite diferentes modos de transmisión de esta trama dando lugar a diferentes modalidades de SMT, que vienen recogidas en la siguiente tabla:

Tipo de SMT	Tasa de transferencia
SMT-1	155 Mbps
SMT-4	622 Mbps
SMT-16	2,5 Gbps
SMT-64	10 Gbps
SMT-256	40 Gbps

El valor que se adjunta junto al SMT indica el factor de múltiplo sobre la trama SMT que se aplica y que da lugar a las diferentes tasas de transferencia.

2.2.3.3. Ventajas y desventajas respecto a PDH

La SDH surgió como evolución de la PDH que corregía los problemas que este último presentaba.

En este sentido las ventajas de SDH frente a PDH son las siguientes:

- ⇒ La multiplexación en SDH es mucho más rápida y eficiente que en PDH.
- ⇒ Gracias a lo anterior, se obtienen tasas de transferencia mucho más altas.
- ⇒ Permite transmitir tráfico de numerosos formatos, caudal y tipos, por lo que se hace flexible a cualquier tipo de servicio de telecomunicación.
- ⇒ Es perfectamente compatible e interoperable con otras tecnologías como ATM o PDH.
- ⇒ Permite su integración con tecnologías ópticas.
- ⇒ Pero SDH presenta algunas desventajas como:
- ⇒ Precisa de un exacto sincronismo con todos los nodos SDH. Esto encarece enormemente la tecnología al precisar de un reloj de sincronismo altamente estable.
- ⇒ La cabecera de la trama es mayor que en PDH y esto implica una mayor ineficiencia en la tasa binaria de datos a transmitir.

2.3. Mecanismos de codificación y cifrado de la información

La codificación es una técnica usada en comunicaciones que consiste en la conversión de un sistema de datos en otro sistema de datos.

Cuando queremos transmitir datos por un medio de transmisión no podemos transmitirlo tal cual, sino que debemos convertirlo en otro formato adaptado al medio de transmisión para que pueda ser transmitido. Esto es codificar los datos.

La codificación la realizan unos dispositivos denominados CODEC (Codificación- Decodificación) que se encargan (antes del envío del datos) de codificarlos (en la parte del emisor) y de decodificarlos (en la parte del receptor).

Evidentemente emisor y receptor deben emplear el mismo código de codificación para codificar y decodificar la información transmitida.

Dado que existen dos tipos de transmisión: analógica y digital, se emplean técnicas de codificación diferentes para cada una de ellas.

Así encontramos:

- ⇒ Técnicas de codificación de datos digitales.
Para una transmisión digital.
- ⇒ Técnicas de codificación de datos analógicos.
Para una transmisión analógica.

Veremos a continuación con más detalle cada una de estas técnicas.

La codificación es una técnica de tratamiento de señales que consiste en convertir la señal de un formato a otro con objeto de adaptarla al canal, mejorar su transmisión, aumentar la eficiencia de las infraestructuras, etc.

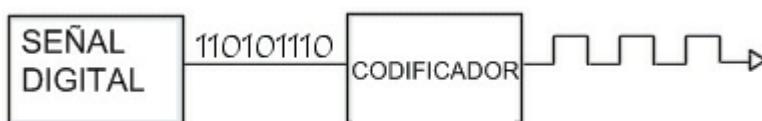
En una transmisión digital lo que se transmite son 0 y 1.

Pero estos 0 y 1 no se pueden transmitir tal cual sino que deben ser codificados (traducidos) a estados de una señal, como por ejemplo:

- ⇒ Ausencia o presencia de señal.
- ⇒ Cambio del voltaje de una señal.
- ⇒ Diferencias de voltajes con respecto a una señal de referencia.

Esta traducción de 0 y 1 a estados de una señal es lo que realiza un CODEC. Emplea para ello diferentes técnicas de codificación de datos digitales.

Lo vemos en la siguiente figura:



En la anterior figura podemos ver cómo el flujo de bits tras pasar por el códec se ha transformado en flujo de estados de una señal, que es lo que realmente se transmite.

El receptor detectará estos cambios de señal y, empleando la misma técnica de codificación, será capaz de traducirlo en señales binarias de 0 y 1 tal y como se enviaron por parte del emisor.

Existen numerosas técnicas de codificación de señales digitales, destacando las siguientes:

- ⇒ Codificación NRZ.
- ⇒ Codificación NRZI.
- ⇒ Codificación Manchester.
- ⇒ Codificación de Miller.
- ⇒ Codificación bipolar.

A continuación veremos con más detalle el funcionamiento de cada una de ellas.

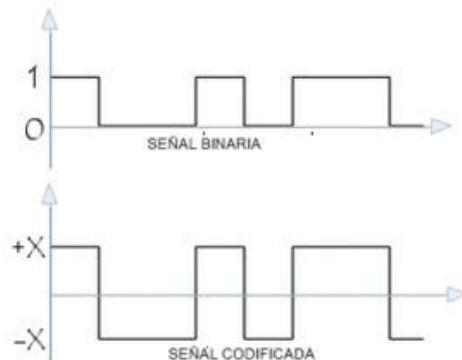
Codificación NRZ

Se trata de una de las técnicas de codificación de señales digitales más sencillas y simples, ya que fue de las primeras que aparecieron.

Se trata de una codificación de no retorno a cero (Not Return zero) y consiste en transmitir un valor de amplitud de señal X cuando queremos transmitir un 1 y un valor de amplitud de señal negativo $-X$ cuando queremos transmitir un 0.

Nunca hay un valor 0 voltaje de señal en el canal (por eso lo de no retorno a cero).

En la siguiente figura puede verse cómo funciona esta codificación:



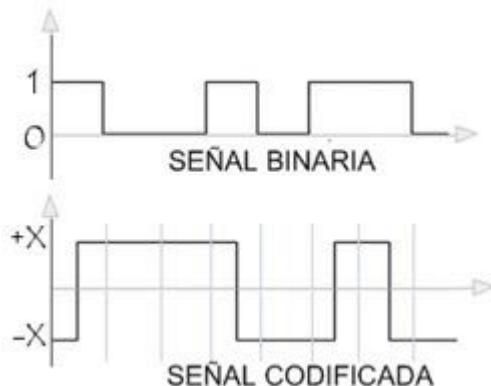
La figura de arriba representa el flujo de bits a transmitir y cuando queremos transmitir un 1 enviamos una señal con voltaje X y cuando queremos transmitir un 0 enviamos la misma señal y con el mismo voltaje pero en negativo.

Así el receptor en función del voltaje recibido (X o $-X$) decodificará si se ha enviado un 1 o un 0.

Codificación NRZI

Se trata de una codificación de datos digitales en la cual la señal que se transmite por el canal cambia de estado cuando queremos transmitir un 1 y permanece en el mismo estado cuando transmitimos un 0.

Lo vemos en la siguiente figura:



La figura de arriba representa el flujo de bits a transmitir. Cuando queremos transmitir un 1 provocamos un cambio de estado en la señal. Si en cambio queremos enviar un 0 no cambiamos el estado de la señal transmitida.

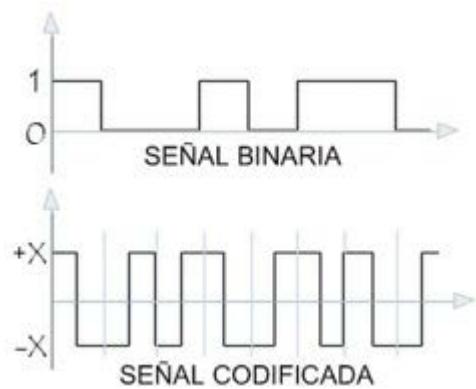
Así, el receptor, en función de los cambios de estado de la señal recibida, va decodificando si el emisor ha enviado un 0 o un 1.

Codificación de Manchester

Se trata de una codificación de datos digitales en la cual se introduce una transición del estado cada vez que transmitimos un bit. Es por ello que también se le denomina codificación en dos fases.

Esta codificación podría equivaler a realizar una OR exclusiva (XOR) con la señal de reloj de la transmisión digital.

En la siguiente figura podemos ver cómo funciona esta codificación:



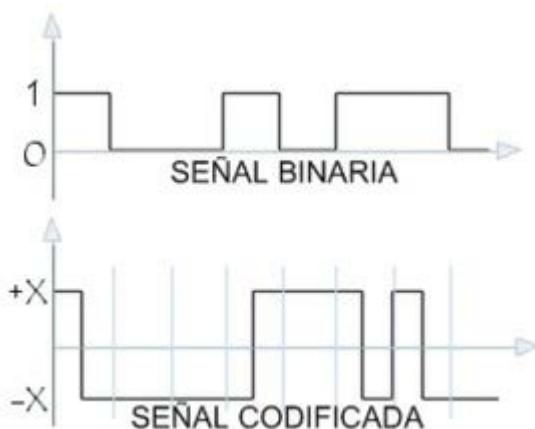
La figura de arriba representa el flujo de bits a transmitir y cuando queremos transmitir un 1 enviamos un pulso con una transmisión de X a $-X$. En cambio, cuando queremos enviar un 0 enviamos un pulso con una transición de $-X$ a X .

Así, el receptor, en función de estos pulsos y sus transiciones, va decodificando si el emisor ha enviado un 0 o un 1.

Codificación de Miller

Se trata de una codificación de datos digitales muy similar al código Manchester, pero en este caso la transición en medio del intervalo solo se produce cuando se transmite un 1.

Lo vemos en la siguiente figura:



La figura de arriba representa el flujo de bits a transmitir. Cuando queremos transmitir un 1 la señal incluye una transición en medio del intervalo. En cambio, cuando queremos enviar un 0 no provocamos ningún cambio de la señal.

Esta técnica permite un mayor índice de datos a transmitir.

Codificación Bipolar

Se trata de una codificación de datos digitales que, a diferencia de los anteriores, presenta tres estados (los anteriores solo 2).

En esta codificación, cuando se quiere transmitir un 0, se envía una señal con valor 0 y cuando se quiere enviar un 1 se envía la misma señal con valor X y -X alternativamente.

En la siguiente figura se puede ver cómo funciona esta técnica de codificación:



La figura de arriba representa el flujo de bits a transmitir. Cuando queremos transmitir un 1 la señal incluye una transición en medio del intervalo. En cambio, cuando queremos enviar un 0 no provocamos ningún cambio de la señal.

Esta técnica permite un mayor índice de datos a transmitir.

Ejemplo:

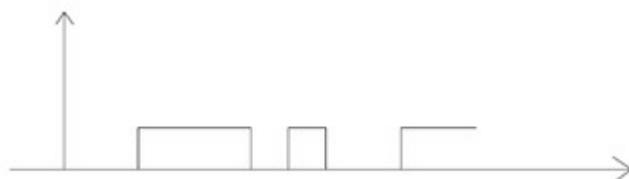
Queremos transmitir la siguiente secuencia de bits por un medio digital en la cual se va emplear la codificación NRZ.



Dibuje la secuencia de bits codificada que se envía al canal.

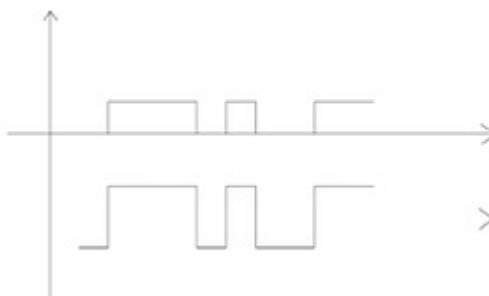
Solución:

Dibujemos en primer lugar en un diagrama de tiempos los bits originales que se quieren enviar, es decir:



La codificación NRZ consiste en transmitir un pulso con amplitud $-X$ cuando se quiere transmitir un 0 y un pulso con amplitud $+X$ cuando se quiere transmitir un 1.

Superponemos en el mismo diagrama de tiempo los bits originales a enviar y la señal codificada según codificación NRZ.



El hecho de que siempre se envíe una señal (negativa o positiva) favorece que el canal tenga siempre señal y sea más inmune al ruido.

Por otro lado, su espectro es mayor, por lo que requiere más ancho de banda.

Veamos otro **ejemplo**.

Queremos transmitir la misma secuencia de bits del ejemplo anterior pero ahora empleando la codificación bipolar.



Dibuje la secuencia de bits codificada que se envía al canal.

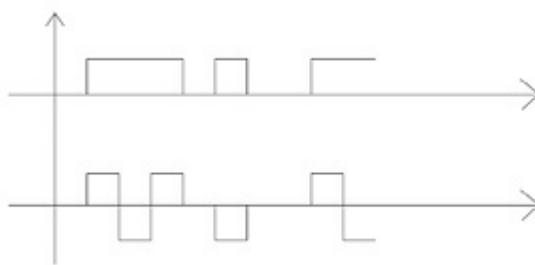
Solución:

Al igual que en el ejemplo anterior, debemos dibujar en un diagrama temporal los bits originales que se quieren enviar:



En la codificación bipolar, cuando se quiere enviar un 0 no se transmite señal y cuando se quiere enviar un 1 se envía alternativamente una señal con amplitud X y $-X$.

Superponemos en el mismo diagrama de tiempo los bits originales a enviar y la señal codificada según codificación bipolar.



Esta es una de las codificaciones que se caracteriza por tener tres estados: ausencia de señal, señal positiva y señal negativa.

Los datos analógicos se caracterizan porque pueden adoptar un número infinito de valores.

Los datos analógicos pueden ser transmitidos por medios analógicos o digitales, ya que el formato que tenga el dato es independiente del medio de transmisión por el que se quiere transmitir.

Para ello, se emplean técnicas de codificación que permiten traducir estos datos analógicos a estados de una señal adaptada al medio de transmisión (analógica o digital) y así poder transmitir los datos analógicos.

Existen diferentes técnicas de codificación para datos analógicos. Depende de si lo transmitimos por un canal digital o por un canal analógico.

Si lo queremos transmitir por un canal digital, lo primero que se realiza es una digitalización de la señal (pasamos el dato de analógico a digital) y obtenemos un flujo de bits sobre el cual podemos emplear cualquiera de las técnicas de codificación de datos digitales descritas anteriormente.

También podemos transmitir dichos datos analógicos empleando un medio analógico (transmisión analógica) y para ello existen, entre otras, las siguientes técnicas de codificación:

- ⇒ Modulación en amplitud.
- ⇒ Modulación en frecuencia.
- ⇒ Modulación en fase.

Técnicas de modulación existen muchas, aunque las tres anteriores son las más sencillas y básicas, ya que el resto suelen ser combinaciones de las tres anteriores.

Veremos a continuación cómo funciona cada una de estas técnicas de codificación de datos analógicos.

Hemos comentado anteriormente que los datos analógicos los podemos transmitir por un canal digital empleando la digitalización de la señal.

Veamos en qué consiste esta técnica.

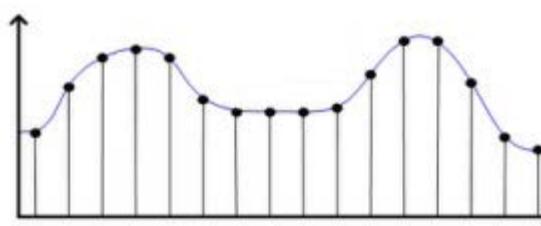
La digitalización consiste en ir tomando muestras de la señal analógica en intervalos regulares y cuantificando la amplitud en cada una de las muestras tomadas.

El intervalo con que se toman las muestras sigue el Teorema de Muestreo o Teorema de Nyquist, que establece que muestreando a una frecuencia al menos el doble que la máxima frecuencia de la señal original se puede obtener una señal digitalizada sin pérdida de la información.

Teorema del Muestreo Frecuencia_{muestreo} ≥ 2 x frecuencia_{máxima señal}

Si cuantificamos (tomamos valores discretos de la amplitud de cada muestra), obtenemos así un flujo de bits que representa la digitalización en cada tiempo de la señal analógica y con ello ya podemos enviarlo por un canal digital empleando cualquiera de las técnicas de codificación digital.

En la siguiente figura podemos ver cómo funciona la digitalización de una señal analógica:

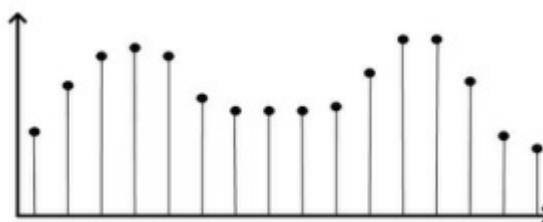


En la figura de arriba podemos ver el ejemplo de una señal analógica, la cual puede adoptar cualquier tipo de valor de amplitud.

Con la digitalización tomamos valores a intervalos regulares a frecuencias f_1 , $2 \times f_1$, $3 \times f_1$, $4 \times f_1$, etc. y en cada uno de ellos tomamos el valor que le corresponde en la señal analógica.

Si luego dibujamos la señal a partir de sus muestras podemos obtener una representación digitalizada de la señal analógica.

Lo vemos en la siguiente figura:



Pero la digitalización implica también una cuantificación de los valores de la señal muestreada, ya que el valor tomado puede ser infinito.

Para ello, cuantificamos la señal, es decir, tomamos el valor máximo y mínimo de la señal analógica y podemos cuantificarlo en un número discreto de valores, por ejemplo, 2, 4, 8, 16, etc.

Si, por ejemplo, tomamos un número discreto de 4 valores, eso indica que la señal digitalizada solo podrá tener uno de esos posibles valores y el valor tomado es el valor más cercano al valor de la señal analógica.

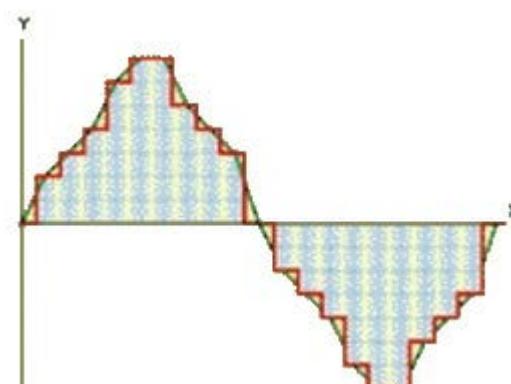
En cada una de las muestras se toman los valores de la señal analógica, pero la cuantificación implica que debemos ajustarnos a uno de los 4 valores discretos posibles y esos valores son los que se transmiten.

Esos cuatro valores posibles se pueden representar mediante 2 bits ($2^2=4$ valores).

A partir de estos cuatro valores a intervalos regulares podemos obtener la señal digitalizada.

Si en vez de cuatro valores cuantificamos 8 valores ello implica que podemos obtener una señal digitalizada más fiel a la señal analógica original pero ello implica transmitir más bits. Ocho valores implican tres bits ($2^3=8$ valores).

Lo vemos en la siguiente figura.

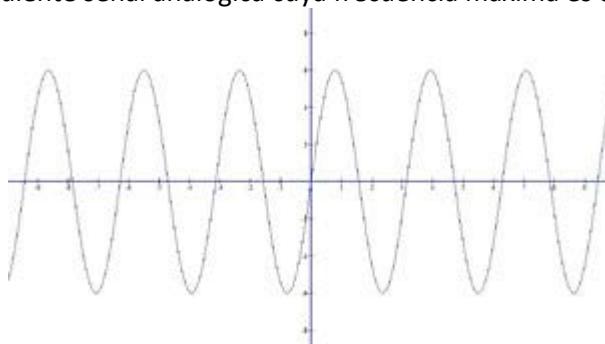


Lo mismo ocurre si muestreamos a intervalos de mayor frecuencia. Obtenemos una señal digitalizada más fiel a la señal analógica original, pero ello implica un mayor número de bits a transmitir.

El teorema del Muestreo nos indica que con una frecuencia de muestreo de al menos el doble de la frecuencia máxima de la señal analógica es suficiente para no perder información.

Vemos un **ejemplo**.

Si queremos digitalizar la siguiente señal analógica cuya frecuencia máxima es de 1 Mhz.



Calcula:

- ⇒ Frecuencia mínima de muestreo para no perder información.
- ⇒ Número de bits de cuantificación necesarios si tomamos un valor de 16 posibles.
- ⇒ Cuántos bits se deben transmitir si tomamos un total de 10 muestras con el nivel de cuantificación anterior.

Solución:

Resolvemos cada uno de los apartados:

–Dado que la frecuencia máxima de la señal analógica es de 1 Mhz, por el Teorema del muestreo la frecuencia del muestreo debe ser:

$$\text{Frecuencia}_{\text{muestreo}} \geq 2 \times \text{frecuencia}_{\text{máxima señal}}$$

Por lo que si tomamos el mínimo, será de:

$$\text{Frecuencia}_{\text{muestreo}} = 2 \times \text{frecuencia}_{\text{máxima señal}} = 2 \text{ Mhz}$$

–Si la señal cuantificada solo puede adoptar uno de los 16 valores posibles, el número de bits necesarios será de:

$$2^x = 16 \text{ bits } x = 4$$

–Si se envían 10 muestras de la señal donde cada una precisa de 4 bits por la cuantificación, el flujo de bits que se transmite será de:

$$\text{Flujo de bits} = 10 \text{ muestras} \times 4 \text{ bits} = 40 \text{ bits.}$$

Es decir, en total se envían 40 bits. En realidad se suelen enviar más bits, ya que en una transmisión se suelen incluir bits de redundancia y control de errores.

Vemos otro **ejemplo**.

Dada la anterior señal analógica la cual se quiere digitalizar empleando una frecuencia de muestreo de 5 Mhz y 3 bits de cuantificación, se pide lo siguiente:

–Dibuje la señal digitalizada.

–¿Se pierde información por la digitalización?

–¿Cuántos valores son posibles en la cuantificación?

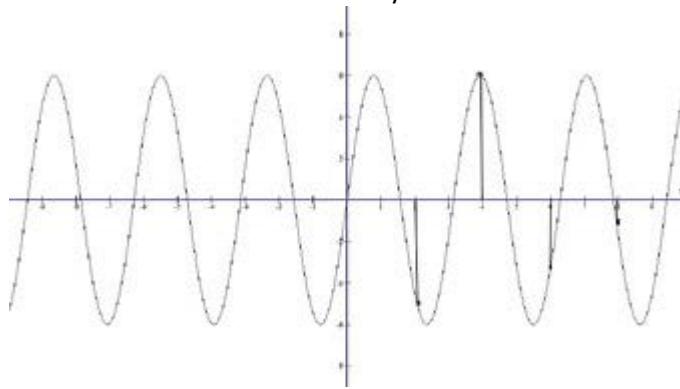
Solución:

Resolvemos cada uno de los apartados:

–La digitalización consiste en formar muestras a intervalos de 2 Mhz, 4 Mhz, 6 Mhz, etc. y donde con tres bits de cuantificación nos dan $2^3 = 8$ valores posibles.

Dado que la máxima y mínima amplitud de la señal es de 16 V, los valores posibles serán de -16, -12, -8, -4, 4, 8, 12 y 16.

Dibujamos la señal digitalizada con esos valores discretos y muestreada a esas frecuencias.



–El que se pierda información o no depende de si cumple el Teorema del Muestreo.

$$\text{Frecuencia}_{\text{muestreo}} \geq 2 \times \text{frecuencia}_{\text{máxima señal}}$$

Dado que la frecuencia de la señal es de 1 Mhz y muestreamos a 5 Mhz, cumple el teorema, luego no se pierde información en la digitalización.

–El número de posibles valores en la cuantificación es:

$$2^3 = 8 \text{ valores}$$

Y cuyos valores posibles son los indicados anteriormente en función del valor máximo y mínimo de pico de la señal analógica: -16, -12, -8, -4, 4, 8, 12 y 16.

Si ahora queremos transmitir un dato o señal analógica por un canal analógico, empleamos otras técnicas de codificación.

En este caso se emplea la técnica de modulación, que consiste en transformar una señal de mayor frecuencia (señal portadora) en función de la señal analógica a transmitir (señal moduladora).

El resultado es una señal modulada de mayor frecuencia con la que se consigue dos cosas:

–Adaptar la señal transmitida al canal.

–Permitir la multiplexación de canales en el medio de transmisión.

Con los dos logros anteriores se obtiene una mayor eficiencia en la transmisión.

La modulación puede ser de tres tipos:

–Modulación en amplitud.

–Modulación en frecuencia.

–Modulación en fase.

Vemos cada uno de ellas con más detalle a continuación.

Son muchos los tipos de modulación existentes en comunicaciones. Todas son variantes y combinaciones de las tres modulaciones básicas: modulación en amplitud, en frecuencia y en fase.

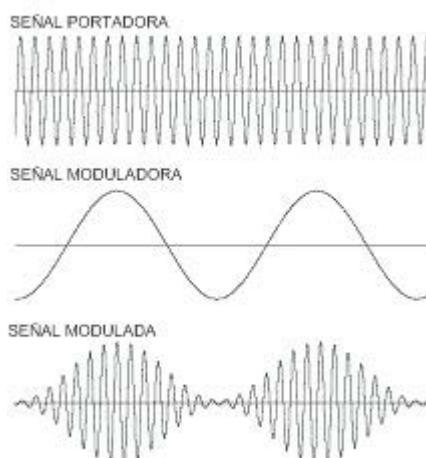
Modulación en amplitud

Es una técnica de codificación de señales analógicas basada en modular (transformar) la amplitud de la señal portadora en relación a la señal a transmitir (moduladora).

El resultado es una señal modulada en amplitud que mantiene la misma forma que la señal moduladora pero es de mayor frecuencia.

La frecuencia de la señal portadora es aquella que está adaptada al medio de transmisión (generalmente una frecuencia mucho mayor que la señal moduladora).

Lo vemos en la siguiente figura:



La operación que permite la modulación en amplitud es una operación de multiplicación de señal moduladora y señal portadora.

Las expresiones matemáticas que representan la modulación en amplitud se basan en la multiplicación de señales sinusoidales.

Así si, por ejemplo, tenemos una señal moduladora expresada por la siguiente ecuación:

$$S_{\text{moduladora}}(t) = A_{\text{moduladora}} \times \cos(w_{\text{moduladora}} \times t)$$

Siendo $A_{\text{moduladora}}$ la amplitud de la señal moduladora y $w_{\text{moduladora}}$ la frecuencia de la señal moduladora (téngase en cuenta que $S_{\text{moduladora}}(t)$ es la señal analógica a transmitir).

Y la señal portadora expresada por la siguiente expresión:

$$S_{\text{portadora}}(t) = A_{\text{portadora}} \times \cos(w_{\text{portadora}} \times t)$$

La señal moduladora viene dada por la multiplicación de ambas señales, es decir:

$$S_{\text{modulada}}(t) = S_{\text{moduladora}}(t) \times S_{\text{portadora}}(t) = A_{\text{moduladora}} \times \cos(w_{\text{moduladora}} \times t) \times A_{\text{portadora}} \times \cos(w_{\text{portadora}} \times t)$$

La modulación en amplitud es una de las modulaciones más sencillas y básicas de las existentes.

Su principal problema es que es sensible al ruido, ya que ésta se acopla a la amplitud de la señal modulada y puede provocar errores en la recepción.

La radio AM (Amplitud Modulada) es un ejemplo del uso de esta técnica de modulación.

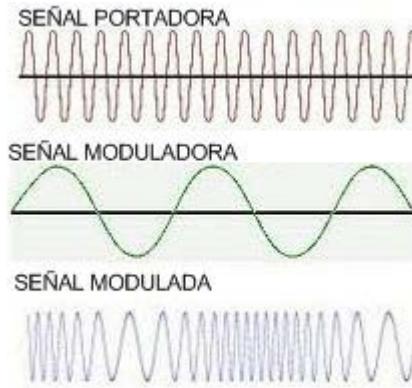
Modulación en frecuencia

Es una técnica de codificación de señales analógicas basada en modular (transformar) la frecuencia de la señal portadora en relación a la señal a transmitir (moduladora).

El resultado es una señal modulada en frecuencia en función de la amplitud de la señal moduladora.

Así, a mayor amplitud de la señal moduladora, más frecuencia en la señal modulada y a menor amplitud de la señal moduladora, menos frecuencia en la señal modulada.

Lo vemos en la siguiente figura:



A diferencia de la modulación en amplitud, la señal modulada mantiene la misma amplitud.

Al igual que la modulación en frecuencia, se basa en la multiplicación de una señal portadora con una señal moduladora, es decir:

$$S_{\text{moduladora}}(t) = A_{\text{moduladora}} \times \cos(\omega_{\text{moduladora}} \times t)$$

$$S_{\text{portadora}}(t) = A_{\text{portadora}} \times \cos(\omega_{\text{portadora}} \times t)$$

$$S_{\text{modulada}}(t) = S_{\text{moduladora}}(t) \times S_{\text{portadora}}(t) = A_{\text{moduladora}} \times \cos(\omega_{\text{moduladora}} \times t) \times A_{\text{portadora}} \times \cos(\omega_{\text{portadora}} \times t)$$

Y donde aplicando operaciones de cosenos podemos obtener una señal modulada con una frecuencia que varía en función de la amplitud de la señal moduladora.

Un ejemplo de aplicación de este tipo de modulación es la radio FM (Frequency Modulation).

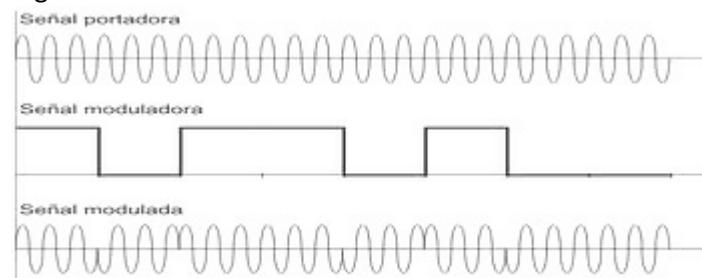
Modulación en fase

Es una técnica de codificación de señales analógicas basada en modular (transformar) la fase de la señal portadora en relación a la señal a transmitir (moduladora).

El resultado es una señal modulada en fase en función de la amplitud de la señal moduladora.

Así, cada vez que hay un cambio en la amplitud de la señal moduladora hay un cambio de fase en la señal portadora.

Lo vemos en la siguiente figura:



La amplitud y frecuencia de la señal modulada, a diferencia de las modulaciones anteriores, no varía.

Al igual que las modulaciones anteriores, se basa en la multiplicación de una señal portadora con una señal moduladora, es decir:

$$S_{\text{moduladora}}(t) = A_{\text{moduladora}} \times \cos(\omega_{\text{moduladora}} \times t + \phi_{\text{moduladora}})$$

$$S_{\text{portadora}}(t) = A_{\text{portadora}} \times \cos(\omega_{\text{portadora}} \times t + \phi_{\text{moduladora}})$$

$$S_{\text{modulada}}(t) = S_{\text{moduladora}}(t) \times S_{\text{portadora}}(t) = A_{\text{moduladora}} \times \cos(\omega_{\text{moduladora}} \times t + \phi_{\text{moduladora}}) \times A_{\text{portadora}} \times \cos(\omega_{\text{portadora}} \times t + \phi_{\text{moduladora}})$$

Y donde aplicando operaciones de cosenos podemos obtener una señal modulada con una fase que varía en función de la amplitud de la señal moduladora.

Existen numerosas técnicas de modulación, pero la gran mayoría suelen ser combinaciones de las anteriormente descritas.

Veamos un **ejemplo**.

Dadas las siguientes señales moduladas recibidas en un receptor, indique qué tipo de modulación se ha empleado en cada una de ellas.

Solución:

En el análisis de las señales moduladas podemos observar que en la figura 1 la señal mantiene su amplitud y fase constante, variando únicamente su frecuencia, por lo que podemos concluir que en la Figura 1 se ha empleado modulación en frecuencia.

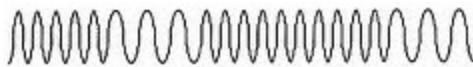


Figura 1 = Modulación en frecuencia.

En la figura 2 podemos observar, en cambio, que la amplitud de la señal va variando constantemente manteniendo invariable su frecuencia y su fase, por lo que podemos deducir que la modulación empleada en el emisor ha sido de una modulación en amplitud.



Figura 2 = Modulación en amplitud.

Por último, en la figura 3 podemos observar que la fase de la señal va dando 'saltos' en el tiempo manteniendo constante su frecuencia y amplitud, por lo que la modulación empleada para esta señal es una modulación en fase.



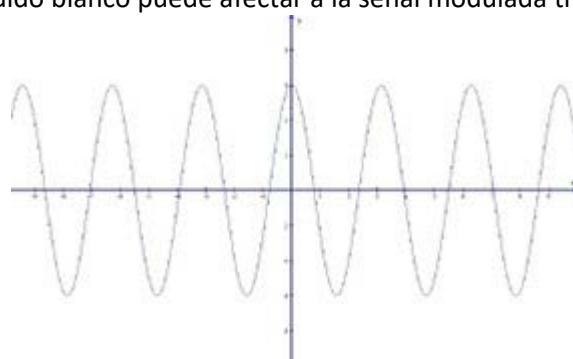
Figura 3 = Modulación en fase.

Veamos otro ejemplo.

Dada la siguiente señal analógica que se quiere transmitir con una amplitud de A voltios y $-A$ voltios y frecuencia 1 KHz, se emplea una modulación en fase de forma que la señal portadora de 1 Mhz, emplea un cambio de fase 180° en cada cambio de ciclo de la señal moduladora.

Dibuje en base a lo anterior la señal modulada correspondiente.

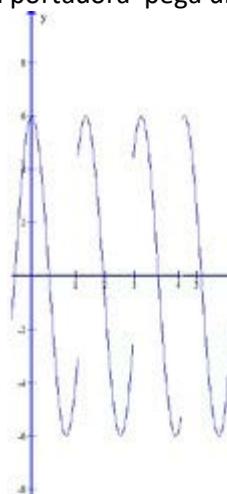
A continuación, razoné si el ruido blanco puede afectar a la señal modulada transmitida.



Solución:

La modulación en fase se caracteriza por modular la fase de la señal portadora en función de la amplitud de la señal moduladora.

Dado que en este caso la señal moduladora solo presenta dos estados de amplitud (A voltios y $-A$ voltios), luego solo habrá dos estados de fase y donde cada vez que hay un cambio de ciclo en la señal moduladora (hay un cambio en la amplitud) la fase de la portadora 'pega un salto' de 180° .



Por último, el ruido blanco (siempre presente en todo medio de transmisión) afecta a cualquier tipo de modulación pero afecta mucho más a una modulación en amplitud (por interferencias en suma de señales) que a una modulación en fase.

El ruido impulsivo, en cambio, sería más perturbador a este tipo de modulación en fase (puede crear un salto de fase) que el ruido blanco

2.4. Sistemas de seguridad en el transporte de datos

La seguridad en las redes es un concepto que cada vez más se tiene en cuenta en este mundo hiperconectado.

Hasta hace poco las redes solo eran utilizadas por determinadas multinacionales y organizaciones por lo que su seguridad también estaba acotada a ellos.

Hoy día, todo el mundo (empresas, organizaciones, particulares e incluso objetos) están conectados a la red (generalmente a Internet) y es por ello que cada vez surge más el concepto de seguridad en la redes como aquel que permite que su conectividad y acceso se realicen de forma segura.

Todos queremos estar interconectados con todos. Están conectados a las redes (Internet) las personas, los equipos, las aplicaciones, etc.

Gracias a las redes podemos comunicarnos con todos, en cualquier parte del mundo y a cualquier hora.

Pero esto hace también que seamos vulnerables a intrusiones y ataques no deseados de personas (hackers o crackers) o aplicaciones (virus, rootkit, códigos maliciosos, etc.).

En base a esto surgió la seguridad informática como conjunto de técnicas o mecanismos que intentan proteger el almacenamiento, procesamiento y transmisión de la información que circula por las redes y en particular por Internet.

Con la seguridad informática conseguimos que nuestras conversaciones telefónicas y nuestros mensajes sean privados y confidenciales y que, por ejemplo, nuestros mensajes lleguen al destinatario deseado y no a otros y que además lleguen sin alteración ni manipulación.

En una red constantemente están transmitiéndose datos de un equipo a otro. Es por ello que debemos asegurar que dichas transmisiones sean seguras y de ello se encarga la seguridad informática. Es decir, debemos proteger la información que se transmite con objeto de que llegue a su destino de forma segura, no sea alterada ni manipulada, ni sea leída por terceros no deseados.

Para conseguir una comunicación segura se emplea como técnica de seguridad en redes el cifrado de las conexiones, es decir: el mensaje no se transmite tal cual se ha generado, sino que se codifica (según una clave) en un mensaje cifrado que es el que se transmite. El receptor (que conoce la clave) es capaz de descifrar este mensaje cifrado para poder visualizar el mensaje original.

Evidentemente, la clave debe ser conocida sólo por emisor y receptor para que la comunicación sea realmente segura.

Como se ha descrito anteriormente, para conseguir una comunicación segura ciframos nuestros mensajes y documentos antes de enviarlos.

De esto se encarga la criptografía, que es una técnica o ciencia capaz de crear mensajes ocultos.

La criptografía consiste en aplicar un algoritmo matemático sobre un documento original y legible con objeto de obtener otro documento no legible (cifrado) que es el que se transmite.

Este algoritmo matemático emplea una clave denominada clave del algoritmo, que solo es conocida por emisor y receptor y que debe aplicarla sobre el algoritmo para cifrar y descifrar el documento.

El algoritmo es un conjunto de reglas ampliamente conocido, pero la que es privada es la clave del algoritmo que es realmente la fortaleza del sistema.

Los algoritmos criptográficos emplean claves que son necesarias para el cifrado de los mensajes y/o documentos.

Pero estas claves pueden ser descifradas por hackers o crackers con la técnica denominada ataque de fuerza bruta, es decir, probar todas las combinaciones de símbolos posibles hasta dar con la clave buscada.

La constante ciberdelincuencia ha hecho que las empresas, organizaciones y organismos gubernamentales dediquen cada vez más esfuerzos, recursos y personal a la seguridad de los datos con objeto de protegerlo de los hackers, crackers y códigos maliciosos.

Para evitar el descifrado de la clave del algoritmo y con ello dar fortaleza al sistema de cifrado se deben tomar ciertas medidas en la elección de la clave del algoritmo. Entre ellas están:

- La clave de cifrado debe ser de gran longitud: por ejemplo, emplear claves de 512, 1024 o incluso 2048 bytes de forma que el atacante necesite de muchos recursos hardware y software para conseguirlo. Con ello se genera la desmotivación del atacante.
- Cambiar la clave regularmente: con ello se consigue que, en el caso de descifrarla, solo la tiene disponible un corto espacio de tiempo.
- Emplear todo tipo de símbolos disponibles: el uso de caracteres especiales (%,&,#, etc.), junto con valores numéricos y alfanuméricos hace más difícil su descifrado.
- No emplear palabras conocidas o identificables: es decir, fechas de nacimiento, película favorita, etc., que puede el atacante asociar con la persona atacada.
- Detectar intentos fallidos continuos en un intervalo corto de tiempo: Los algoritmos criptográficos existentes pueden ser de dos tipos:
 - Emplean una criptografía simétrica: es decir, emplean la misma clave para cifrar (para el envío del mensaje o documento) que para descifrar (en la recepción del mensaje o documento).
 - Emplean una criptografía asimétrica: es decir, emplean la misma clave para cifrar (para el envío del mensaje o documento) pero emplean otra diferente para descifrar (en la recepción del mensaje o documento).

Veremos a continuación las diferencias existentes entre uno y otro.

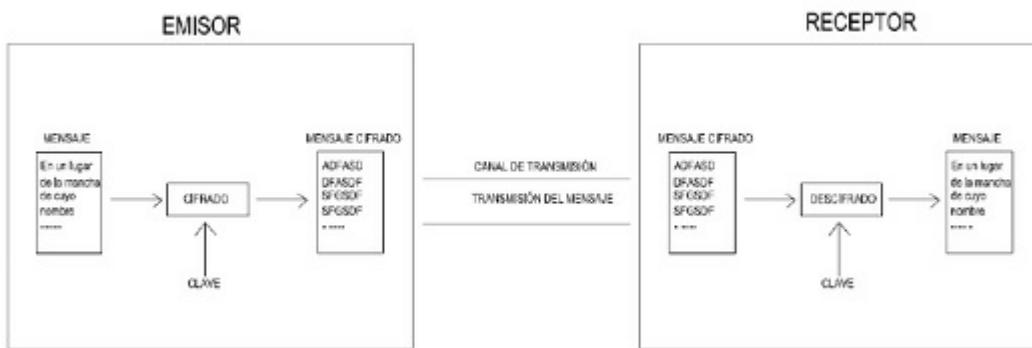
Criptografía simétrica

En la criptografía simétrica **se emplea la misma clave del algoritmo para cifrar que para descifrar**.

Es el tipo de criptografía más sencilla y se ha empleado desde la antigüedad.

En ella el emisor emplea un clave de cifrado antes de enviar el mensaje. El documento cifrado es el que se envía y una vez recibido por el receptor emplea la misma clave para descifrar.

Evidentemente, la clave debe ser la misma para ambos para obtener el documento cifrado y luego obtener el documento descifrado.



La criptografía simétrica presenta varios problemas o **inconvenientes**:

- **La clave del algoritmo debe ser conocida por emisor y receptor** y en algún momento debe ser enviada al 'otro' para poder emplear el algoritmo. Evidentemente, no podemos usar el mismo canal 'inseguro' para enviar la clave.
- Además, debemos tener una clave diferente por cada pareja emisor-receptor, ya que no se puede emplear la misma clave para varios receptores. Por ello, para cada usuario receptor (que puede ser un trabajador de una empresa) debemos disponer de una clave diferente. Esto hace que tengamos que tener almacenadas una gran cantidad de claves, una por cada receptor al que queramos enviar el mensaje.

En base a lo anterior, en los años 70 surgió la criptografía asimétrica, que solucionaba los problemas de la criptografía simétrica y es el método criptográfico más empleado actualmente.

Criptografía asimétrica

La criptografía asimétrica soluciona los problemas de la **criptografía simétrica al emplear una clave de cifrado distinta para cifrar y otra para descifrar**.

El emisor, cuando va a enviar un documento o mensaje, emplea una clave (denominada clave pública) con la que cifrar el documento. Esta clave puede ser conocida por cualquiera, ya que se emplea para cifrar.

Pero el documento solo puede ser cifrado por otra clave (clave privada) que solo conoce el receptor al que va dirigido el mensaje o documento que emplea dicha clave privada para descifrar el documento.

No existe relación matemática entre la clave pública o privada, por lo que conociendo la clave pública con que se cifró el mensaje no se puede descifrar. Solo puede descifrarse con la clave privada que solo conoce el receptor al que va dirigido el mensaje.

Con la criptografía asimétrica hemos resuelto los siguientes problemas:

- No es preciso transmitir la clave de cifrado.
Es una clave que puede ser conocida por cualquiera (por eso se le denomina clave pública), ya que sólo se emplea para cifrar el documento o mensaje.
- No hay problema de almacenamiento de clave.
Por cada documento que se envía a diferentes usuarios solo se emplea una clave de cifrado. Sí aumenta la clave privada para el descifrado, pero esa clave privada la tiene almacenada cada receptor, porque el emisor solo guarda la clave de cifrado (clave pública).

No obstante, la criptografía asimétrica presenta ciertos **problemas** o vulnerabilidades, que son las siguientes:

- Se debe **proteger** la clave privada.
La clave privada empleada por cada receptor debe ser protegida para que nadie pueda emplearla para descifrar el mensaje cifrado recibido.
- La clave privada debe ser **transportada**.
La clave privada, en algún momento, debe ser transportada y para ello se emplea un mecanismo como el llavero de claves.
- Son poco **eficientes**.
Las claves de cifrado y descifrado suelen ser largas. Se tarda tiempo en cifrar y descifrar los documentos, lo que lo hace ineficiente en este sentido.

En seguridad informática, la autenticación se define como la confirmación de que un usuario, equipo o aplicación es quien dice ser y no otro.

Es decir, evitamos la suplantación y al impostor.

Está técnica constituye uno de los pilares básicos en toda comunicación segura. Para conseguir esta autenticación generalmente en la transmisión de un documento o mensaje se debe logear el usuario o máquina, es decir, le exigimos que introduzca su usuario y contraseña con lo cual el sistema confirma que la persona que envía el documento o mensaje es quien dice ser.

Esta técnica de autenticación está plenamente integrada en nuestras vidas cotidianas: nuestro DNI representa la autenticación de que esa persona es quien dice ser; el PIN de nuestro móvil indica al sistema que quien tiene acceso a usar la red móvil es el abonado que dice ser; el código de nuestra tarjeta de crédito indica que la persona que intenta sacar el dinero del cajero es realmente el titular de la cuenta, etc. En seguridad informática, la integridad se define como la seguridad de que los datos almacenados son realmente los datos que se espera almacenar, es decir, que no han sido alterados ni manipulados.

Por tanto, cuando se intentan recuperar dichos datos son los mismos que se almacenaron, ya que no han sufrido alteración alguna en su forma o contenido.

Esto es otro de los pilares básicos en la seguridad de los datos.

Esta técnica, al igual que la autenticación, está plenamente integrada en nuestra vida cotidiana.

Por ejemplo, nuestro DNI lo forman ocho números seguidos de una letra. Existe un algoritmo que comprueba que dicha letra corresponde a esa numeración, ya que la letra se obtiene a través de una combinación aritmética de los números. Cuando se introduce un DNI en un sistema informático, lo primero que se hace es comprobar si dicho DNI es válido, y para ello aplica la combinación aritmética a los números. Si la letra que obtiene es la misma que la introducida en el DNI, el DNI es válido. Con esto se verifica la integridad del DNI introducido y el usuario puede operar con el sistema.

Hemos visto que los algoritmos criptográficos tanto simétricos como asimétricos necesitan una clave privada que ambos, emisor y receptor, deben compartir y que en algún momento debe ser transportada por un canal seguro.

Para transportar esta clave de cifrado (distribuir la clave) existen mecanismos de transporte de claves siendo el más habitual la tarjeta inteligente.

Esta tarjeta es un dispositivo generalmente de plástico y provisto de un chip electrónico en el que se almacena nuestra clave. Antes de usarla nos pedirá un PIN de acceso a la clave.

La implementación de esta tarjeta inteligente puede ser de dos tipos:

- Mediante una tarjeta de memoria flash.
- Mediante una tarjeta preprocesadora.

La primera es más insegura ya que cuando se introduce la tarjeta en el equipo para utilizar la clave se realiza una copia temporal de dicha clave en el equipo. Aquí es donde está la vulnerabilidad.

En cambio, en la segunda, la clave nunca sale de la tarjeta preprocesadora, ya que el proceso matemático de cifrado y descifrado que emplea la clave lo realiza el propio chip de la tarjeta preprocesadora.

Otra clasificación de las tarjetas inteligentes se puede realizar en función del interfaz de comunicación que emplea. Así encontramos:

- Tarjetas de contacto:
Son aquellas en las que debe existir un contacto (generalmente metálico) entre el equipo y la tarjeta inteligente para poder operar. Es el caso más habitual y más seguro.
- Tarjeta sin contacto:
Es aquella en que no existe contacto físico entre la tarjeta inteligente y el equipo. Generalmente la transmisión se realiza por radiofrecuencia. Es más inseguro (utiliza un canal como el aire, que es inseguro) pero es más rápido y por ello se emplea en lugares donde se busca gran rapidez, como por ejemplo en estaciones de tren, aeropuertos, etc.

Las aplicaciones en red son realmente los puntos críticos en la seguridad de las redes.

Son numerosas las aplicaciones que presentan vulnerabilidades y el hecho de que se empleen en red hace más fácil que códigos maliciosos puedan propagarse de un equipo a otro de manera muy rápida.

Es por ello que en el transporte de datos existen mecanismos que deben estar centrados en aquellas aplicaciones que más se utilizan en las redes para detectar sus vulnerabilidades y crear parches a dichos programas para asegurar su integridad.

A continuación, veremos aquellas aplicaciones y sus protocolos asociados que más se emplean en red, donde se describirá su funcionamiento y cómo la seguridad informática actúa sobre ellos para conseguir unas transmisiones fiables y seguras.

SSL representa un protocolo que trabaja en el nivel de transporte del modelo OSI o TCP/IP y que asegura una transmisión segura de la información entre los equipos, generalmente entre un equipo cliente y un servidor.

Que trabaje a nivel de transporte lo hace transparente de la arquitectura de los elementos de interconexión o encaminadores que trabajan a nivel 3 o nivel de red.

SSL surgió para proteger las conexiones existentes entre clientes y servidores web con el protocolo http que se empleaban para el comercio electrónico. Esta protección debía asegurar al cliente que se había conectado al servidor auténtico, y enviarle en consecuencia datos confidenciales, como por ejemplo los datos de su número de tarjeta de crédito.

El protocolo se encarga de encapsular el trabajo de los elementos de la capa superior, construyendo un canal de comunicaciones entre los dos extremos objeto de la comunicación. Esto lo realiza empleando la técnica de Handshake, encargada de intercambiar la clave que se utilizará para crear un canal seguro mediante un algoritmo eficiente de cifrado simétrico.

SSH representa un protocolo en el que se definen una serie de reglas que permiten una transmisión segura de un equipo a otro al cifrar la información que transmite de extremo a extremo.

Es muy empleado para configuración remota de equipos (sustituyendo al TELNET), para transferencia de archivos (sustituyendo al FTP), crear canales seguros de comunicaciones, etc.

En la actualidad existen dos versiones de este sistema SSH: SSH1 y SSH2, siendo esta última la más usada al tener mejoras sobre la primera.

Una de las aplicaciones más usadas que emplea dicho protocolo es el OpenSSH.

SSH constituye un protocolo seguro de transferencia de información de un equipo a otro. Esta seguridad la proporciona porque la información intercambiada va cifrada de un equipo a otro. Muchos programas TELNET, como Putty, integran este protocolo para gestionar equipos en modo remoto y con comunicaciones seguras.

IPsec es un protocolo que define una serie de reglas que, trabajando a nivel de red (a diferencia de SSL que trabaja a nivel de transporte), permiten una comunicación segura y fiable entre extremos o dicho de otro modo entre equipos.

Para ello este protocolo usa técnicas criptográficas además de la autenticación para la transmisión segura de los datos.



Un cortafuegos o firewall es una aplicación software especializada que se intercala entre las aplicaciones y la tarjeta de red para realizar un filtrado de los paquetes.

El objetivo no es más que controlar los paquetes que entran y salen del equipo por la red con objeto de actuar correctamente ante paquetes sospechosos.

Es una herramienta básica para la seguridad de las redes y todos los equipos siempre deberían tenerla instalada y activada.

El **firewall** se puede instalar tanto en equipos clientes como en equipos servidores actuando de forma diferente aunque empleando las mismas técnicas.

Veremos a continuación cómo trabaja según sea un equipo cliente o un equipo servidor.

Cortafuegos en un equipo cliente

En un equipo cliente el cortafuegos actúa aplicando un filtrado de paquetes.

En el tráfico saliente, es decir, de paquetes que salen del equipo hacia la red, el cortafuegos o firewall analiza la cabecera de cada paquete y, en función de las reglas que tenga definidas en el cortafuegos, realiza una acción u otra. Por ejemplo, si detecta que la máquina cliente hace spam, bloquea el puerto 25 (puerto de correo electrónico).

En el tráfico entrante, es decir, de paquetes que entran al equipo cliente, analiza la cabecera de cada paquete y en función de las reglas de configuración actúa de una forma u otra.

Cortafuegos en un equipo servidor

En un equipo servidor el cortafuegos también actúa aplicando un filtrado de paquetes.

En el tráfico saliente, es decir, de paquetes que salen del equipo hacia la red, el cortafuegos o firewall analiza la cabecera de cada paquete y en función de las reglas que tenga definidas en el cortafuegos realiza una acción u otra. En este tráfico es donde generalmente actúa el cortafuegos puesto que en un servidor la mayor parte del tráfico es saliente.

En el tráfico entrante, en cambio, el firewall analiza qué paquetes quieren acceder a qué puertos del servidor para bloquear en el caso de un ataque al servidor si así lo tiene en las reglas de configuración.

3. Servicios de comunicaciones

3.1. Servicios de voz

Las redes de comunicaciones son instaladas, montadas y configuradas para prestar servicios de comunicaciones a los usuarios o equipos.

Son muchos los servicios de telecomunicaciones que demandan los usuarios: servicios de voz, de datos, servicios de televisión, etc.

Uno de los servicios más demandados históricamente es el servicio telefónico, es decir, el servicio de voz. El servicio de voz sobre redes de comunicaciones consiste en el inicio, mantenimiento y finalización de una conversación bidireccional entre dos usuarios separados geográficamente, a través de una red de comunicaciones.

El servicio telefónico tiene como objetivo la transmisión de la voz humana mediante recursos técnicos de forma que pueda llegar de un usuario a otro conectado a la red de forma rápida, correcta y audible.

Actualmente, el servicio de voz puede prestarse mediante dos formas:

- ⇒ Servicio de telefonía fija.
Emplea redes fijas de comunicaciones (cableadas o inalámbricas) pero los terminales están fijados en ubicaciones geográficas concretas.
- ⇒ Servicio de telefonía móvil.
Emplea redes fijas de comunicaciones (cableadas o inalámbricas) pero los terminales no tienen fijada su ubicación. Son terminales móviles.

Ambos servicios de voz, tanto fijos como móviles, son altamente demandados por la sociedad, en especial el servicio de telefonía móvil, que en las últimas décadas ha experimentado un desarrollo exponencial de su demanda.

A continuación se mostrará con más detalles cada uno de ellos.

Servicio de telefonía fija

El servicio de telefonía fija se caracteriza porque los terminales de usuarios tienen sus ubicaciones geográficas fijadas en un sitio concreto (el PTR: punto de terminación de red).

Históricamente ha sido el servicio de voz empleado y con ello el más desarrollado y capilarizado.

Este servicio de voz emplea la red telefónica conmutada (RTC) o también denominada red telefónica básica (RTB), que es una red de conmutación de circuitos diseñada para transmitir señal de voz, aunque también transporta señales de datos.

La red RTC es una red jerárquica basada en centrales de conmutación que pueden ser:

- Central de conmutación local.
- Central de conmutación de tránsito.
- Central de conmutación internacional.

La información pasa por la red a través de estos conmutadores hasta llegar a su destino.

Cuando un usuario quiere llamar, es la central de conmutación local la que establece el mecanismo para tramitar dicha llamada, pasando dicha información por los diferentes conmutadores de tránsito hasta llegar a la central de conmutación local del destinatario.

Si el destinatario está en el extranjero, se emplearán las centrales de conmutación internacionales.

La red RTC utiliza un sistema de numeración específico (cada usuario final tiene un identificador único) y un sistema de señalización propio denominado SS7.

Como red de conmutación de circuitos, la red telefónica precisa para cada llamada de voz crear una conexión entre el equipo emisor de la llamada y el equipo receptor de la llamada.

Es por ello que la red debe crear un circuito virtual o canal lógico que pasando por todos los nodos intermedios conecte emisor con receptor.

La red telefónica conmutada RTC constituye la primera red de telefonía fija basada en hilos de cobre.

Presenta una estructura muy jerárquica basada en nodos primarios, secundarios, etc. Actualmente está siendo actualizada para los nuevos servicios de voz como la VoIP.

Para la creación de este canal virtual o circuito virtual (virtual porque desaparece al finalizar la llamada) hay que seguir los siguientes pasos:

- Establecimiento del circuito virtual:

Es la creación del conjunto de enlaces necesarios entre los nodos intermedios para hacer llegar la llamada desde el emisor hasta el receptor.

La creación de este conjunto de enlaces sigue unos criterios de eficiencia, costes, nivel de saturación de enlaces, etc.

–Transferencia de datos:

Una vez establecido el circuito virtual se transmite la información por este circuito como si emisor y receptor estuvieran 'físicamente' unidos.

–Liberación del circuito virtual:

Una vez finalizada la llamada (bien por emisor o receptor) se liberan los canales y con ellos todos los recursos de la red.

La red RTC incorpora determinadas funciones de gestión y tarificación que son necesarias en todo servicio de voz.

Este sistema de conmutación de circuitos tiene como ventaja de que una vez establecido el circuito virtual la señal viaja sin cortes y sin retardos graves sin más que el retardo del propio establecimiento de la conexión.

No es un sistema muy eficiente, ya que se consumen recursos durante todo el establecimiento de la conexión y no se libera hasta que finaliza (lo hace poco eficiente para tráfico rafagueado).

El servicio de telefonía fija (en la ubicación del abonado) presenta los siguientes elementos:

–Un PTR o PAU.

Que representa el punto de terminación del operador. Representa un punto de corte y prueba para delimitar responsabilidades del operador y del abonado.

–Una roseta o BAT.

Es el punto de conectividad para los terminales telefónicos (teléfono, fax, etc.).

Representa el último punto de la red al que se conecta el latiguillo del terminal del usuario.

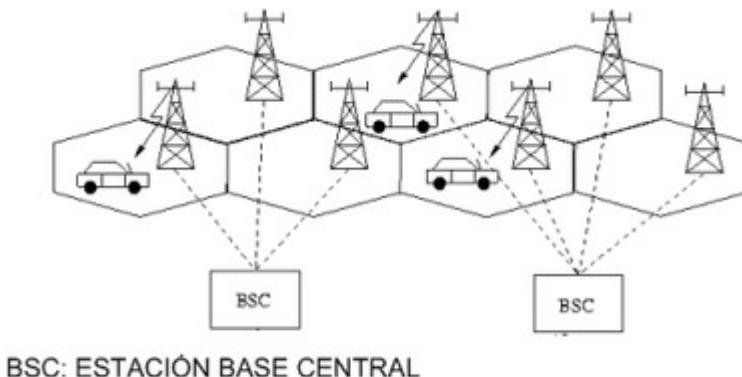
–Hilo telefónico.

Formado por un par de cables de cobre rígido de Ø 0,5 mm.

En la siguiente figura podemos ver el esquema de estos elementos.



A continuación podemos ver ejemplos comerciales de estos elementos.



En la anterior figura podemos observar la estructura interna de un PAU de dos salidas.

Servicio de telefonía móvil

El servicio de telefonía móvil ha experimentado un auge exponencial en las últimas décadas y ha sido motor de parte del mercado de las telecomunicaciones.

Las redes de telefonía móvil permiten transmitir también el servicio de voz, pero a diferencia de la telefonía fija los terminales no tienen ubicación geográfica fija, sino que son terminales móviles.

Esto le da gran ventaja frente a la telefonía fija, ya que permite la movilidad de los usuarios.

La red de telefonía móvil basa su estructura en dividir el territorio o geografía en celdas con forma hexagonal en las que se instala una estación base de telefonía móvil que da cobertura a su celda.

Cualquier terminal móvil está vinculado a la estación móvil que está en su misma celda geográficamente y si el terminal móvil se mueve y cambia de celda, el sistema lo desvincula de la estación base de la celda que deja y lo conecta a la estación base de la nueva celda en la que se halla, todo ello de manera automática y transparente para el usuario.

Este sistema permite la reutilización de frecuencias, ya que las frecuencias pueden ser reutilizadas en cada una las celdas que son independientes entre sí.

Aunque la infraestructura del sistema celular se ha mantenido a lo largo del tiempo, ha ido variando la tecnología que ha soportado sobre ella, evolucionando a sistemas cada vez más eficientes y sobre todo con mayores tasas de transferencias que permiten integrar no solo el servicio de voz sino servicios de datos al alta velocidad.

Así la evolución de las distintas tecnologías en la telefonía móvil ha sido:

–Etacs.

Representa la primera generación de telefonía móvil (1G), que eran analógicos.

–GSM.

Representa la segunda generación de telefonía móvil (2G), que supuso una revolución ya que las transmisiones ya eran digitales.

Con esta tecnología llegó el SIM como tarjeta de identificación del abonado y que era necesario insertar en los terminales móviles para su acceso e identificación en la red.

GSM trabaja en las frecuencias de los 900 Mhz, 1.800 Mhz y 1.900 Mhz.

–GPRS.

Representa la segunda generación y media de telefonía móvil (2.5G) y que permitía la transferencia de datos por la red aunque a muy baja velocidad.

Aquí es donde apareció la tecnología WAP, que suponía una traducción del formato HTML para PC a un formato WAP que pudiera ser visualizado en los terminales móviles.

–UMTS.

Representa la tercera generación de la telefonía móvil (3G), que suponía la consolidación (e inicio) de los servicios de datos por las redes móviles ya que permitía mayores tasas de transferencia.

UMTS utiliza la tecnología CDMA, una tecnología de espectro ensanchado, eficiente y seguro. Opera en la banda de los 2 Ghz (1.800 hasta los 2.200 Mhz) y permite tasas de transferencia de hasta 384 Kbps.

–HSDPA.

Es la evolución del UMTS y representa la 3,5 G.

Permite ya tasas de transferencia de hasta 1,8 Mbps y con ello se generalizó el uso de la telefonía móvil no solo para transmitir voz sino para transmitir datos a alta velocidad.

Permite ya servicios de telecomunicaciones en tiempo real como videotexting, videosharing, etc.

–LTE.

Representa la última generación de telefonía hasta la fecha y se denomina comercialmente como redes 4G.

Permite tasas de velocidad de bajada (downlink) de hasta 100 Mbps y de subida (uplink) de 50 Mbps.

Soporta servicios avanzados de telecomunicación y servicios en tiempo real.

Los actuales operadores de telefonía móvil están realizando grandes esfuerzos en su red de infraestructuras con objeto de mejorar sus prestaciones, sobre todo sus tasas binarias de transferencia. Con ello quieren ser competitivos ante un usuario cada vez más exigente y demandante de nuevos servicios avanzados de telecomunicación en su terminal móvil.

3.2. Servicios corporativos y de red inteligente

Los servicios corporativos representan un tipo de red o servicio ampliamente utilizado en el sector empresarial, que permite interconectar sus equipos, sedes, organizaciones, etc. y dotarlos de servicios de telecomunicaciones.

La RDSI (Red digital de servicios integrados) fue uno de los primeros servicios corporativos que cubría las necesidades de este sector.

La RDSI fue una evolución natural de la RDI (Red digital integral) y proporcionaba una conectividad digital extremo a extremo que permitía un amplio abanico de servicios de telecomunicaciones como voz, datos, facsímil, etc.

Entre los servicios que permite la RDSI destacamos los siguientes:

–Telefonía básica con servicios añadidos.

Se trataba de la telefonía básica de la RTB a la que se añadían servicios avanzados como desvío de llamadas, conferencia a tres, llamada en espera, etc.

–Telefonía a 7 KHz.

Se trataba de ofrecer una telefonía de alta calidad, ya que la telefonía de la RTB era de 4 KHz.

Precisaba de un teléfono RDSI.

–Servicio de Fax.

Permitía la transmisión de imágenes de mejor calidad, ya que la transmisión se realizaba en digital y no como en la RTB que era analógica.

Precisaba de un fax con adaptador para la RDSI.

–Servicio de Fax avanzado.

Se trataba de un servicio de fax de altas prestaciones que mejoraba mucho la velocidad de transmisión consiguiendo reducir drásticamente el tiempo de transmisión.

–Teletex.

Servicio de intercambio de textos.

–Videotex.

Servicio de acceso a recursos de la red como servidores, bases de datos.

–Videotelefonía.

Servicio de transmisión de audio y vídeo entre los interlocutores.

El funcionamiento de la RDSI se basa en dos estructuras:

–Acceso básico.

Consiste en 2 canales independientes de 64 kbps cada uno, denominados canales B y que se emplean para la transmisión de voz y datos, además de un canal denominado D de 16 Kbps para señalización.

En total proporciona una velocidad de 144 kbps.

A la contratación de este servicio se le conoce como 2B + D.

–Acceso primario.

Consiste en 30 canales independientes de 64 kbps cada uno, denominados canales B y que se emplean para la transmisión de voz y datos, además de un canal denominado D de 64 Kbps para señalización.

En total, proporciona una velocidad de 1984 kbps.

La contratación de este servicio se le conoce como 30B + D.

La señalización empleada en la RDSI es la misma que en la RTB, es decir, señalización SS7.

La RDSI, aunque partía de un futuro prometedor, no consiguió los resultados esperados ya que se vio ensombrecida por la aparición de las tecnologías xDSL (sobre todo el ADSL), que ofrecían mejores prestaciones de velocidad a un coste inferior.

Veamos un ejemplo.

Ejemplo:

En Estados Unidos, el acceso primario se basa en 23 canales B de 64 kbps cada uno para voz y datos más un canal D de 64 kbps para señalización.

Calcule entonces, para este acceso primario, la velocidad del acceso primario 23B+D que permite el sistema.

Solución:

Como cada canal B es de 64 kbps y el acceso primario consta de 23 canales, luego la tasa final de transferencia del acceso primario será de:

Tasa acceso primario = tasa transferencia canales B + tasa transferencia canales D =

$$= 23 \times 64 \text{ kbps} + 1 \times 16 \text{ kbps} = 1536 \text{ kbps}$$

3.3. Servicios de datos, servicios IP. Telefonía IP

Las redes de comunicaciones han pasado de transmitir el servicio telefónico de voz a transmitir numerosos otros servicios que son demandados por usuarios, empresas y organizaciones.

Ahora se demandan servicios de datos, Internet, televisión, vídeo, etc., para los cuales han evolucionado, como se ha visto anteriormente, para soportar este gigantesco caudal de tráfico.

Incluso el servicio de telefonía básica de voz ha evolucionado pasando de una transmisión de señales analógicas a un servicio de telefonía digitalizada sobre IP (VoIP).

Las operadoras han puesto especial énfasis y recursos en todos estos servicios de telecomunicaciones demandados ofreciendo paquetes integrados denominados 'Triple play' o 'Cuaduple play' para con ello ofrecer un servicio integral de comunicaciones a sus usuarios que con ello mejoran su fidelidad y amortizan antes sus costes de infraestructuras.

Por 'Triple Play' se entiende un paquete integral de servicios de telecomunicación formado por:

- Servicio telefónico fijo de voz.
- Servicio de datos o Internet.
- Servicio de televisión.

El concepto de 'Cuaduple Play' es una extensión del anterior añadiendo además los mismos servicios pero también el servicio de telefonía móvil.

Estas nuevas redes incluso han hecho evolucionar los servicios de telecomunicaciones ya que el servicio de televisión digital (TDT) o CATV está siendo sustituido por la Televisión sobre IP (TVIP).

Dado que el servicio telefónico ya se ha visto con detalles en capítulos anteriores, ahora nos centraremos en los servicios de datos.

Entre los servicios de datos más empleados nos encontramos con:

- Servicio de navegación web.
- Correo electrónico.
- Servicio FTP.
- Servicio TELNET.
- Servicios de compartición de archivos o P2P.
- Telefonía IP.
- VoIP.
- Televisión sobre IP.

Veremos a continuación con más detalle cada uno de ellos.

Importante:

Los servicios Triple Play (voz, datos y televisión) y Cuaduple Play (voz, datos, televisión y telefonía móvil) son los nuevos servicios cada vez más ofertados por los operadores debido a los grandes ingresos que aportan al ofrecer todo el paquete a un mismo usuario optimizando con ello sus redes de comunicaciones.

Servicio de Navegación Web

Internet se ha convertido en la tecnología soporte para numerosos servicios de datos que son demandados por los usuarios.

Uno de los más usados, conocidos y demandados es el servicio de World Wide Web, es decir, el servicio www, o dicho de otro modo la navegación web.

Este servicio consiste en un conjunto de recursos de textos, imágenes y vídeos estructurados en una página denominada Hipertexto (página web) que están alojados en numerosos servidores en red y que permiten su consulta e interacción con cualquier otro usuario conectado a la red.

En la siguiente figura podemos ver el ejemplo de una página web con numerosos recursos como textos, imágenes, vídeos, etc.

Es por tanto en un servicio de intercambio de información a escala mundial.

A este servicio inicial de intercambio de información se le sumaron otros servicios de valor añadido como el comercio electrónico, la banca electrónica, la formación online, etc.

El servicio www utiliza el estándar HTLM (Hypertext Markup Language), que es un código de programación con el que se diseñan las páginas web y que alojan en ellos los recursos o informaciones del servicio, es decir, los textos, imágenes, vídeos, etc.

Las páginas web además están todas interrelacionadas entre sí mediante los hiperenlaces, que consisten en un vínculo o referencia en una página web que lo conecta a otra página o recurso de la red.

Habitualmente suele estar resaltado en la página web que incluye el hipervínculo y al situar el ratón sobre ella aparece una 'manita'.

Podemos ver a continuación en la siguiente figura como están insertados los hipervínculos.

Los recursos, es decir, páginas web, vídeos, imágenes, están identificados en la red mediante la nomenclatura URL (Uniform Resource Locator).

Esta nomenclatura evita tener que acceder a los recursos mediante su dirección IP (difícil de recordar) y mediante la traducción de los servicios DNS dichas direcciones IP se traducen en una dirección con un formato URL que contiene cuatro campos:

–Método: define el protocolo empleado para acceder al documento o información. Puede ser http, ftp, etc.

–Estación: es la dirección IP del equipo u ordenador que aloja la información solicitada. Habitualmente se emplean los servicios DNS en los cuales esta dirección es sustituida por un alias que comienza por www.

Ejemplo: www.google.es

–Puerto: es un campo opcional y que indica el número del puerto del servidor por el cual se va suministrar la información. Deberá estar habilitado (abierto) por la aplicación servidor.

–Camino: es la ruta del archivo donde se encuentra la información.

Para usar el servicio Web es preciso disponer de aplicaciones de navegación, es decir, de navegadores o browsers.

Son en definitiva aplicaciones software que se conectan con los servidores web, leen las instrucciones HTML y las presentan al usuario según sus peticiones.

Todos los navegadores contienen al menos dos partes:

–Controlador: es la línea de comandos en la que se escribe la dirección URL de la información a solicitar.

–Intérprete: es la 'página' donde se muestra la información de hipertexto solicitada y traducida para que pueda ser visualizada correctamente por el usuario.

Actualmente existen en el mercado numerosos navegadores, siendo los más conocidos Google Chrome, Edge, Firefox y Opera.

En la siguiente imagen podemos ver el ejemplo del navegador Firefox.

Servicio de Correo electrónico

El servicio de correo electrónico o email (electronic mail) es un servicio que permite enviar mensajes de un usuario a otro a través de la red.

Es, después del servicio de navegación web, el servicio de datos más empleado.

La ventaja con respecto a la mensajería tradicional es su inmediatez en la recepción del mensaje.

Además, los mensajes pueden llevar adjuntos archivos, imágenes, vídeos, otros correos, etc., lo que lo hace mucho más versátil.

Hoy día este servicio se ha convertido en imprescindible para particulares, empresas, organizaciones, etc., formando parte de su herramienta habitual de trabajo.

Además, se permiten otras formas de envío como:

–Multienvío del mismo mensaje a múltiples usuarios.

–Responder a un mensaje recibido.

–Reenviar un mensaje recibido a otro usuario.

Para enviar y recibir correos electrónicos es preciso que el usuario tenga una cuenta de correo activa en un servidor de correo electrónico.

Esta cuenta es única, personal e intransferible para su titular.

Dicha cuenta de correo presenta el siguiente formato:

Nombre de la cuenta @ nombre del servidor. dominio de internet

Así, una cuenta de correo válida sería:

antoniofperez@hotmail.es

Siendo:

antoniofperez: el identificador de la cuenta o del usuario.

hotmail: el nombre del servidor de correo que aloja la cuenta de correo electrónico.

es: el dominio al que pertenece el servidor que aloja la cuenta.

El acceso a la cuenta de correo electrónico siempre implica un logueo, es decir, identificar el nombre de la cuenta junto con una contraseña.

Para usar el correo electrónico es preciso tener un cliente de correo electrónico.

Existen numerosos clientes de correo electrónico (la mayoría gratuitos) entre los que destacan Outlook Express, Thunderbird, Pegasus y Eudora Email.

No obstante, hay cuentas de correo electrónico que no precisan de cliente de correo electrónico, ya que son lo que se denomina correo web.

Se trata de cuentas de correo que ofrecen gratuitamente determinados servidores como hotmail, gmail o yahoo a los usuarios pero donde les obliga a usar su cuenta de correo directamente desde su página web (en el vínculo de correo) para que con ello obtengan un mayor número de visitantes y así obtener mayores beneficios en publicidad.

Es por ello que el usuario tan solo necesita acceder a la web del servidor, loguearse y acceder a su cuenta de correo electrónico para operar con ellos.

El correo electrónico basa su funcionamiento en el protocolo SMTP (Simple Mail Transfer Protocol) que además emplea dos protocolos para el envío y recepción de los correos:

–Protocolo POP: es el encargado de la recepción de los correos.

–Protocolo SMTP: es el encargado de la emisión de los correos electrónicos.

Además existe también el protocolo IMAP, que permite un uso compartido del correo electrónico, ya que permite el procesamiento del correo de modo online.

Servicio de FTP

El servicio de FTP (File Transfer Protocol) es un servicio que permite el intercambio de ficheros entre equipos y servidores empleando la red.

Sigue una arquitectura cliente-servidor en la cual precisa de un servidor de FTP donde se alojan los ficheros y de un cliente que solicita los ficheros para su consulta, eliminación, modificación, etc.

Con este servicio se pretende que exista un recopilatorio de archivos, imágenes y vídeos alojado en un servidor y que pueda ser accesible para muchos usuarios (autorizados) para su consulta, modificación, etc.

Es preciso que el usuario disponga de un cliente de FTP para que se conecte al servidor una vez autorizado y logueado.

Existen en el mercado numerosos clientes de FTP (muchos gratuitos) como CuteFTP, WS FTP o Filezilla FTP.

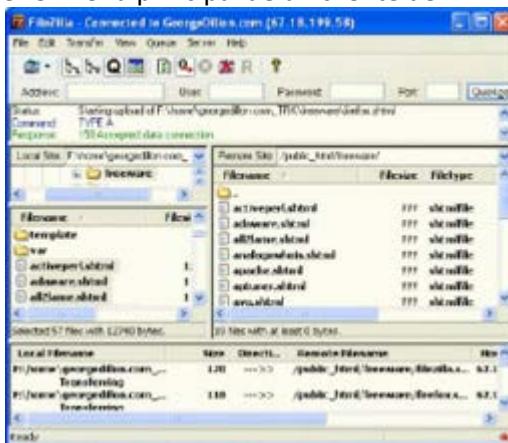
Además, los navegadores permiten también el acceso por FTP a los servidores de FTP con solo escribir en la barra de direcciones el método de acceso de ftp, es decir:

ftp://nombre_servidor.dominio_internet.

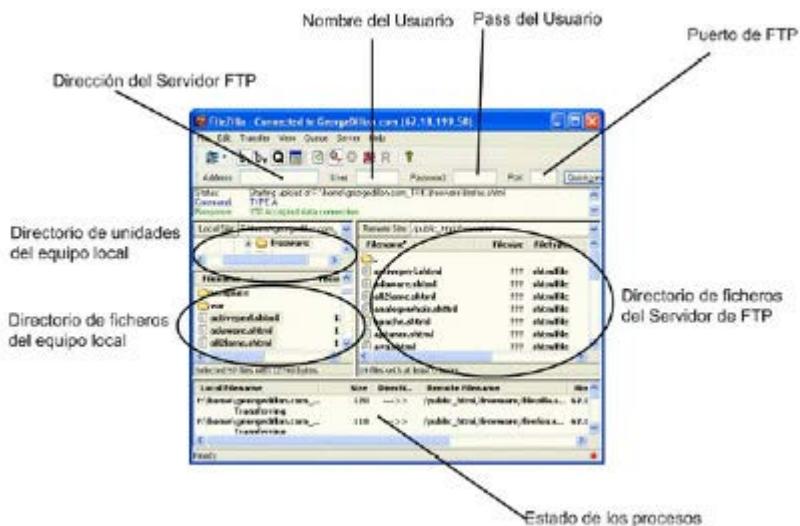
Por ejemplo:

ftp://miservidor.es

En la siguiente figura podemos ver el menú principal de un cliente de FTP:



En él podemos ver las siguientes secciones:



A continuación describimos cada una de estas secciones:

–Dirección del Servidor FTP:

Se trata de la URL o dirección IP del servidor FTP al que queremos acceder.

–User:

Se trata de escribir nuestra cuenta de usuario en el servidor de FTP para loguearnos y tener accesos a los archivos.

–Pass:

Se trata de escribir nuestra clave de usuario en el servidor de FTP para loguearnos y tener accesos a los archivos.

–Port:

Se trata de escribir el puerto de acceso al servidor FTP. Generalmente, si no se escribe nada se toma por defecto el puerto 21.

–Directorio de Unidades del equipo local.

Se muestran las unidades del equipo local que acceden al servidor FTP.

–Directorio de ficheros del equipo local.

Se muestran los ficheros del equipo local que acceden al servidor FTP.

–Directorio de ficheros del Servidor de FTP.

Se muestran las carpetas y archivos del servidor FTP al que queremos acceder.

–Estado de los procesos.

Se muestra el log de las tareas y procesos que se están realizando (connecting, transferring, etc.).

Para pasar ficheros o archivos del equipo local al servidor de FTP tan solo debemos seleccionarlos en el Directorio de ficheros del equipo local y arrastrarlos a la carpeta deseada en el Directorio de ficheros del Servidor de FTP. Para pasar ficheros del servidor local al equipo local el proceso es idéntico.

Servicio TELNET

El servicio de TELNET es el servicio que permite acceder remotamente a otros equipos o máquinas para ejecutar procesos en él aprovechando los recursos o prestaciones de este equipo remoto.

El equipo local actúa como modo terminal, es decir, solo envía órdenes y recibe datos, sin ningún procesamiento en él.

Nuestro teclado y nuestro monitor se portan como si fuesen el monitor y teclado del equipo remoto.

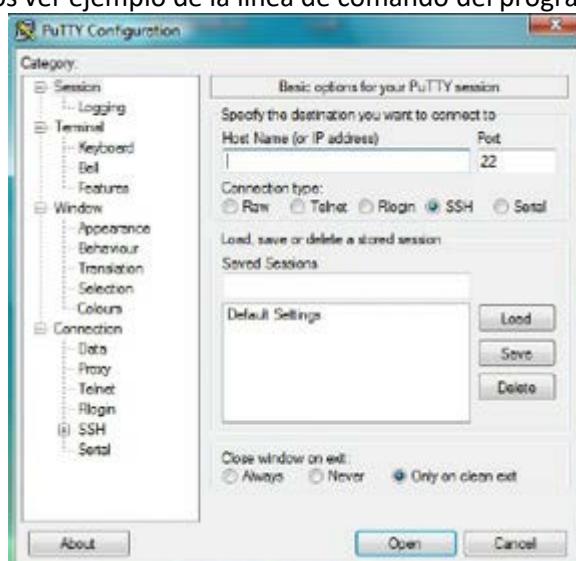
Este servicio precisa de un logueo para que accedan al equipo remoto solo los usuarios autorizados y es por ello que antes de poder usar el servicio debemos introducir nuestro nombre de usuario y nuestra contraseña o clave.

El funcionamiento del servicio TELNET, en muchas ocasiones, es en modo consola, por lo que requiere de conocimientos de comandos y programación.

Este servicio es ampliamente utilizado entre los administradores de red y administradores de sistemas.

Existen determinados programas que facilitan el uso del servicio TELNET entre los que destaca el programa PUTTY.

En la siguiente figura podemos ver ejemplo de la línea de comando del programa PUTTY:



En la imagen anterior, podemos ver varios campos que son necesarios para el servicio TELNET.

–Host Name.

Se trata del campo donde se debe escribir la dirección IP del equipo remoto al que queremos acceder.

–Port.

Se trata del campo donde se debe escribir el puerto del equipo remoto al que queremos acceder.

Si no se especifica nada se tomará por defecto el puerto 22.

La aplicación también permite acceder mediante el servicio SSH, que es un protocolo de comunicación segura para acceder a equipos y máquinas remotas en modo comando.

Con la tecnología SSH (a diferencia de TELNET) la comunicación es segura, ya que SSH aplica técnicas de cifrado en todas las comunicaciones.

Servicio de compartición de archivos o P2P

El sistema P2P (Peer to Peer) es un servicio de intercambio de archivos, sobre todo música y películas, en la que dichos archivos se encuentran alojados entre todos los equipos conectados en la red, actuando simultáneamente como clientes y servidores de archivos.

Todos los usuarios utilizan este sistema P2P instalando sobre sus equipos una aplicación como Edonkey, Emule, Ares, etc., en la cual una vez creada una cuenta de usuario y registrado en ella es posible intercambiar estos archivos con cualquier usuario que esté conectado a la aplicación.

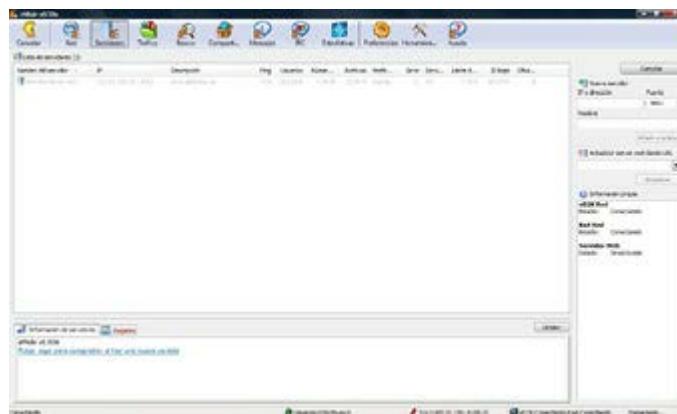
Se trata de una red distribuida con millones de usuarios a escala mundial que intercambian sobre todo música, películas y programas, muchos de ellos protegidos bajo los derechos de autor y que la aplicación 'piratea' prácticamente sin control.

Esto ha generado una gran batalla legal entre los fabricantes y autores contra estas redes P2P a causa de la piratería de estos contenidos.

En algunas ocasiones se han incluso cerrado algunas aplicaciones como BitTorrent o Megaupload por parte de la agencia Estatal de EE.UU. tras numerosas batallas entre casas discográficas y empresas de P2P.

Aún así, todavía siguen funcionando estas aplicaciones, existiendo también numerosas de ellas de forma legal, ya que respetan los derechos de autor (es el caso de aplicaciones como Snocap, imesh, etc.).

En la siguiente figura podemos ver el ejemplo de una aplicación de P2P para la descarga de música, películas y programas.



Telefonía IP

El servicio de telefonía IP es un servicio que permite realizar llamadas telefónicas empleando la red Internet en vez en la red telefónica básica (RTB).

Para ello, la voz debe ser digitalizada y encapsulada en paquetes IP para poder transmitirse por la red Internet que es una red de conmutación de paquetes IP.

El problema principal de la telefonía IP es que dichos paquetes IP viajan junto con otros paquetes de datos (navegación web, servicios Telnet, servicios de P2P, etc.) que pueden crear retardos importantes en la transmisión de los paquetes IP y que hagan que la conversación sufra retardos y la conversación sufra 'cortes' o que incluso se corte la conexión.

Es por ello que a estos servicios de telefonía IP se les dota de un calidad de servicio (QoS) que obliga a que los paquetes no superen un retardo máximo y se minimicen los jitters consiguiendo con ellos una conversación fluida, sin cortes y con una calidad similar a una llamada telefónica convencional.

La ventaja de esta telefonía IP es su bajo coste (a veces gratuita) ya que puede integrarse junto con una tarifa de datos que contrate el usuario.

Existen numerosas aplicaciones que integran el servicio de telefonía IP como pueden ser Skype o Yahoo Messenger.

En numerosas ocasiones estas aplicaciones permiten además realizar videollamadas.

En la

El servicio de VoIP, a diferencia de la telefonía IP, es un protocolo que permite la comunicación telefónica

En este caso no es preciso emplear aplicaciones tipo Skype o Yahoo Messenger, sino que emplean teléfonos

convencionales pero denominados Teléfonos IP. El funcionamiento técnico es similar a la telefonía IP. La voz se digitaliza y paquetiza en formato IP y se transmite por la red Internet. Es por ello que es precisa una conexión de datos.

El sistema introduce en estos paquetes calidad de servicio, es decir, QoS, con lo que asegura un retardo máximo en el flujo de paquetes para garantizar que la conversación es fluida y sin cortes.

Emplea para su funcionamiento protocolos específicos para VoIP como pueden ser los protocolo SIP, IAX, H.323, etc.

Para ser digitalizada la voz emplea los denominados códec. Estos realizan la codificación y compresión del audio (y viceversa en el otro extremo).

Existen numerosos códec (cada uno con un nivel de compresión diferente) como pueden ser:

- Códec G.711
- Códec G.723.1
- Códec G.729
- GSM

A continuación mostramos en la siguiente tabla las tasas binarias que ofrece cada uno de estos códecs.

CÓDEC	TASA BINARIA
G.711	64 Kbps
G.723.1	64 Kbps
G.729	8 Kbps
GSM	13 Kbps

Para el empleo de la VoIP debemos emplear:

- Teléfonos IP.

Que incorporan el códec para la codificación de la señal de voz en IP y permiten su transmisión a la red de datos.

En la siguiente figura podemos ver el ejemplo de un teléfono IP:

En apariencia se trata de un teléfono convencional pero emplea como salida un conector RJ-45 (para conectarse a la red de datos a través de un switch o router) en vez de un conector RJ-11.

Suelen incorporar además numerosos servicios de valor añadido como conferencia a tres, desvío de llamadas, llamadas en espera, etc.

- Teléfonos analógicos convencionales + 1 ATA (Analog Terminal Adapter).

Se trata de un adaptador de analógico a IP para poder seguir utilizando los antiguos teléfonos analógicos en la nueva red de VoIP.

Este dispositivo se coloca entre el teléfono analógico convencional y la red de datos.

Es por ello que incluye un conector RJ-11 para conectarse al teléfono analógico y un conector RJ-45 para conectarse a la red de datos.



En la siguiente figura podemos ver el ejemplo de un adaptador ATA comercial.

- Softphone.

Se trata de aplicaciones que emulan teléfonos IP y con las que empleando el micro y el auricular del PC podemos realizar llamadas telefónicas en VoIP usando la conexión de datos que tengamos contratada.

Como toda aplicación software dispone de un amplio abanico de configuración y fácilmente adaptable a las necesidades del usuario y de los equipos donde están instalados.

Asimismo, existen numerosas aplicaciones para ello y muchas otras que lo incorporan como una funcionalidad más de sus prestaciones.

En las siguientes figuras mostramos algunos de los softphones más empleados comercialmente (algunas son de pago aunque la mayoría son gratuitas).



Tevisión sobre IP

La televisión sobre IP o también denominada TvIP es un servicio que permite visualizar los servicios de televisión usando redes IP como Internet.

Se trata por tanto de ver televisión usando Internet y no por las redes de comunicaciones convencionales como redes de cable (CATV) o servicios de radiodifusión (TDT o TVSAT).

La complejidad de este servicio radica en que se trata de un servicio de una QoS crítico (servicio en tiempo real) que precisa de una conexión de datos de alta velocidad que permite ver la televisión sin cortes, retardos o fluctuaciones.

Es por ello que se han desarrollado protocolos para este servicio de TvIP.

La televisión sobre IP actualmente se comercializa bajo los paquetes de Triple Play (voz, datos y televisión) o Cuaduple Play (voz, datos, televisión y móviles) generando una fuente de ingresos importantes para los operadores.

Este servicio de TvIP revoluciona el concepto de cómo vemos la televisión, ya que permite personalizar los contenidos que el usuario quiere ver, es decir, creamos una televisión a la carta o lo que se conoce como VoD (vídeo bajo demanda).

Lo que caracteriza a la TvIP sobre el resto de servicios de televisión es:

–Da soporte a una televisión interactiva.

Ahora el usuario puede interactuar con los contenidos televisivos al disponer de un canal de retorno el cual permite solicitar determinados contenidos, opinar sobre los espacios televisivos, hacer búsquedas de contenidos, etc.

–Permite el time shifting.

Consiste en realizar la grabación de los contenidos para luego poder reproducirlo cuando el usuario quiere verlos.

–Permite la personalización.

Es decir, el usuario puede configurar qué contenidos quiere ver y cuáles no.

–Mejora la eficiencia del ancho de banda.

Dado que solo se envían al usuario los contenidos que desea enviar, el operador puede adaptar el caudal de la red a los contenidos utilizados mejorando así la eficiencia de la red.

–Permite la integración con otras plataformas como, por ejemplo, dispositivos móviles (Smartphone, portátiles, tablets, etc.).

Para el servicio de TvIP es necesario disponer de unas redes de comunicaciones de alta velocidad o de gran ancho de banda.

Es por ello que este servicio solo es prestado sobre redes que incorporan la fibra óptica como medio de transmisión.

También puede ser implementado sobre redes inalámbricas, pero al igual que las redes cableadas necesitan de un gran ancho de banda para la transmisión de este servicio.

La arquitectura de este servicio de TvIP se basa en los siguientes elementos:

–Fuentes de contenidos.

Son los equipos (servidores, bases de datos, etc.) que contienen los contenidos televisivos que van a visualizar los usuarios.

Proceden de los productores, casas cinematográficas, cadenas de televisión, etc.

–Nodo de servicio de TvIP.

Es el nodo que recibe los contenidos de las fuentes de contenidos y lo entraña con las redes de comunicaciones de los operadores.

Realiza el encapsulado en paquetes IP de los contenidos televisivos.

–Red de distribución.

Es la red de comunicaciones (generalmente de los operadores) en la cual el contenido televisivo llega a toda las ubicaciones.

Suelen ser de fibra óptica por su gran ancho de banda.

–Bucle de abonado.

Es el tramo último de la red de comunicaciones y que llega hasta la ubicación del usuario (hogar, empresa, sede, etc.).

Podrá estar implementado en fibra óptica (FTTH), par trenzado (ADSL) o cable coaxial (CATV).

–Equipo final del cliente.

El servicio de TvIP precisa instalar en la ubicación del abonado un dispositivo set-top-box que realiza la conversión de los paquetes IP en señales de audio y vídeo (A/V) para que pueda ser visualizado en un televisor convencional.

Estos set-top-box también podrán estar integrados en el propio televisor.

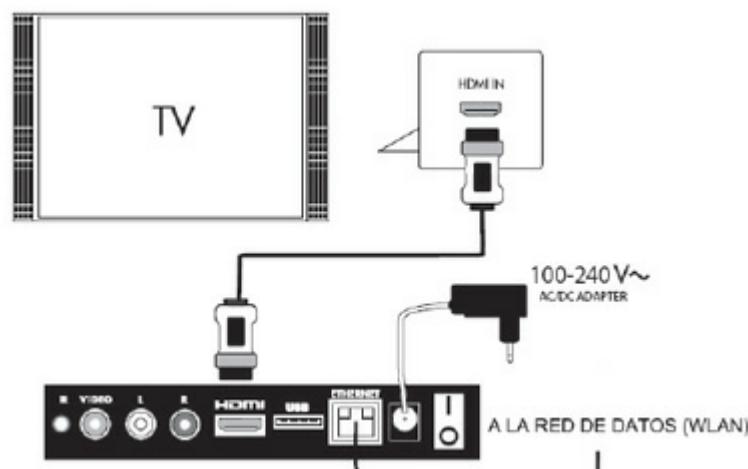
Además, estos dispositivos set-top-box recogen las peticiones del usuario para comunicárselos a los proveedores del servicio de TvIP.



En la siguiente figura podemos ver el ejemplo de un set top box para TvIP.

Este dispositivo dispone de al menos un conector HDMI para su conexión a la televisión convencional y un conector RJ-45 para su conexión a la red de datos.

En la siguiente figura podemos ver los conectores y el conexionado que debe realizarse en la ubicación del abonado.



Con el servicio de TvIP se pueden obtener otros servicios de valor añadido como:

- Servicio de grabación de vídeo digital.
- Vídeo bajo demanda (VoD).
- Guía de programación electrónica (EPG).
- Aplicaciones interactivas a través del televisor.
- E-learning a través del televisor.
- Comunicaciones corporativas.
- Vídeoconferencias.
- Anuncios avanzados.
- Servicios de visualización de contenidos avanzados como PIP (Picture in Picture) mediante el cual podemos visualizar por ejemplo las jugadas de un partido de fútbol desde varios ángulos.

En la siguiente figura podemos ver un ejemplo del servicio de TvIP.

La TvIP viene a ser la nueva revolución en la forma en la que vemos la televisión. Ahora el espectador no será un mero actor pasivo, sino que podrá actuar con su televisor con los nuevos servicios interactivos.

3.4. Servicios telemáticos e interactivos

Las redes de comunicaciones también permiten la transmisión de otros servicios telemáticos, muchos de ellos interactivos, que han tenido gran éxito en el mercado.

Entre estos servicios destacamos los siguientes:

- Chat.
- Servicio de Mensajería.
- Whatsapp.

Describimos a continuación con más detalle cada uno de ellos.

Chat

El chat es un servicio para conversar mediante mensajes de texto con otros usuarios a través de la red.

Es preciso para esta conversación que ambos usuarios estén operativos, es decir, estén 'en línea'.

Se trata de un servicio en tiempo real donde los usuarios conversan entre sí de forma generalmente anónima y que puede estar clasificado por temas o canales como:

- Actualidad.
- Sexo.
- Amigos.
- Provincias.

El tema puede ser cualquiera e incluso los usuarios pueden abrir temas nuevos.

Se trata de un servicio bastante adictivo y que ha experimentado un gran auge en los últimos tiempos, aunque ha sido superado por otros servicios como los de mensajería (Whatsapp).

Para utilizar el servicio es preciso un nick o 'alias' por parte del usuario. El sistema verificará antes que dicho nick no esté siendo utilizado en ese momento por otro usuario.

El servicio permite no solo chatear en un canal con muchos usuarios intercambiando opiniones, sino además abrir un chat privado con otros usuarios en línea.

El protocolo que utiliza este sistema es el denominado IRC (Internet Relay Chat).

Existen numerosos chats en Internet, siendo muchos de ellos los prestados por buscadores como Terra, Yahoo, Msn, etc.

Servicio de mensajería

El servicio de mensajería es un servicio de comunicación entre usuarios de la red que supone un trato más personalizado que los sistemas de chat.

A diferencia del chat, solo nos comunicamos con aquellos usuarios que hayamos autorizado o agregado en nuestra lista de 'amigos'.

Al igual que el chat, se trata de un sistema de comunicación más rápido y fluido que el correo electrónico (ya que esperamos respuesta más o menos inmediata de nuestro interlocutor) pero menos invasivo que una llamada de voz.

Este servicio de mensajería se comercializa bajo programas específicos muy conocidos y en numerosas ocasiones gratuitos como Skype (que absorbió la antigua Messenger) o Yahoo Messenger.

WhatsApp es una aplicación de mensajería multiplataforma que permite enviar mensajes con contenido multimedia entre los usuarios de telefonía móvil empleando una conexión de datos.

Es por ello que si el usuario ya tiene contratada una tarifa de datos para la navegación web en su terminal móvil esta aplicación usa esa línea de datos para el envío de los mensajes, por lo que no supone un coste del servicio al contrario que ocurre con el servicio de SMS y MMS anteriormente visto.

Además permite numerosas funcionalidades como crear grupos, envíos múltiples a diferentes usuarios, etc. Whatsapp se ha convertido en un servicio que recoge las prestaciones y ventajas de servicios de SMS, MMS y de la mensajería instantánea como Skype.

Ha tenido gran éxito sobre todo en el público joven y probablemente acabe sustituyendo o dejando obsoleta el servicio de SMS y MMS.

Esta aplicación solo puede funcionar en los denominados teléfonos inteligentes o smartphones, que permiten la instalación del programa bajo sistemas operativos Android, e iOS.

No obstante, han surgido competidores de este servicio como Line o Viber con unas prestaciones y características similares.

En la siguiente imagen podemos ver el menú principal de este servicio de Whatsapp.

3.5. Otros servicios de valor añadido

Sobre los servicios anteriormente descritos se han generado otro tipo de servicios que son considerados servicios de valor añadido.

Entre ellos destacamos los siguientes:

- Juegos en red.
- Servicios de SMS y MMS.
- Servicio de videostreaming.
- Youtube.

Describimos a continuación con más detalle cada uno de ellos.

Juegos en red

El servicio de juegos en red permite a los usuarios interconectarse y jugar en red con otros usuarios de la red y que participan en el mismo juego.

Se trata de plataformas multiusuarios en las que todos participan en la misma partida, compiten entre ellos y donde pueden chatear y conversar entre ellos.

Se trata de un servicio altamente adictivo que cada vez ofrece más servicios de valor añadido como videojuegos, videoconsolas, etc. y con gran mercado sobre todo entre los más jóvenes.

También se incluyen en este servicio aquellos juegos conocidos como juegos bajo demanda, que permiten al usuario adquirir temporalmente un juego sin necesidad de comprar la aplicación comercial.

Esto último permite disponer de un amplio repertorio de juegos a bajo coste sin necesidad de adquirirlo en soporte de DVD o CD-ROM y supone una importante fuente de ingresos para los fabricantes y desarrolladores de videojuegos.

Las temáticas son amplísimas: desde juegos de Trivial, juegos de mesa, de cartas, de rol, de zombies, etc.

Servicio de SMS y MMS

El servicio de SMS (Short Message Service) surgió como un sistema de intercambio de mensajes en los teléfonos móviles de manera barata, sencilla y rápida.

Como complemento al servicio de telefonía móvil ha supuesto una gran fuente de ingresos para las operadoras y tuvo gran éxito sobre todo entre el público joven.

Este servicio basa su funcionamiento en el envío de un mensaje con una longitud máxima de 160 caracteres desde un terminal móvil a otro, aunque actualmente casi todos los terminales permiten concatenar varios mensajes por lo que no existe en la práctica longitud máxima del mensaje.

Estos mensajes de transmiten por el canal de señalización de la red móvil por lo que se emplea un canal de comunicaciones infrautilizado por los operadores.

Una evolución de los SMS son los MMS (Multimedia Message Service) que son mensajes que permiten incluir recursos multimedia como imágenes, vídeos o audio.

Estos MMS surgieron a partir de la generación 3G de la telefonía móvil, que ya incorporaban más velocidades de transferencia de datos en los terminales.

Estos servicios de SMS y MMS han sido sustituidos actualmente por nuevos servicios de mensajería instantánea como son Whatsapp, Line, Viber, etc.

Estas nuevas aplicaciones han tenido gran penetración en el público (sobre todo en el público joven), ya que incorporan numerosas funcionalidades que no tienen los servicios SMS y MMS. Además, el hecho de que los mensajes sean gratuitos al usar una tarifa de datos contratadas por el usuario ha contribuido al éxito de estos nuevos sistemas de mensajería.

Servicio de videostreaming

El servicio de videostreaming consiste en la visualizar y escuchar vídeos en directo a través de la red sin haberlos descargado previamente.

Es decir, permite ver películas, videoclips o incluso la televisión en directo (en línea) sin descargar ningún archivo.

Esto se realiza porque se produce una descarga temporal de la secuencia de vídeo en el terminal del usuario que lo va reproduciendo a medida de que se va transmitiendo por la red.

Evidentemente precisa de un buen ancho de banda o buena tasa de transferencia de la red de datos para que la transmisión no sufra cortes o latencias excesivas que provoquen que la reproducción se entrecorte.

Dentro de este servicio también se pueden incluir los servicios de e-learning en directo.

El funcionamiento del servicio se basa en la configuración de un buffer en el terminal del usuario donde se va almacenando en la caché la secuencia de tramas del vídeo que se va descargando.

El usuario va reproduciendo el vídeo de este buffer. Evidentemente, este buffer debe ser suficientemente grande para que pueda absorber las fluctuaciones de la red y que el usuario puede visualizar el vídeo de manera totalmente fluida.

Un buffer corto provocaría que dichas fluctuaciones no fueran absorbidas por el buffer y se perdiera calidad en la reproducción.

Tampoco debe ser excesivamente grande para no crear el efecto de una visualización en 'diferido' de los vídeos descargados.

Al final se escoge un tamaño del buffer de compromiso que cumpla ambas prestaciones.

El servicio de videostreaming ha creado en torno a él un gran servicio comercial por parte de las compañías que han creado líneas de negocio en base a cobrar por los vídeos reproducidos o la visualización de los canales de televisión.

Gracias a las modernas y rápidas redes de comunicaciones de hoy día, este servicio puede ser implementado en cualquier terminal bien sea fijo o móvil.

Youtube

Se trata de un servicio de compartición de vídeos a través de la red ampliamente difundido y conocido por los internautas.

En definitiva se trata de un recopilatorio de vídeos subidos por los usuarios (requiere registrarse) y que comparten dichos vídeos con el resto de los usuarios de la red que pueden visualizarlos a través de la página de youtube, es decir, www.youtube.com

Está basado en las técnicas de videostreaming ya que el usuario visualiza el vídeo de forma on line sobre la web sin descargarlo previamente (aunque existen programas que permiten descargar el fichero de audio o vídeo como Atube Catcher).

La web dispone de un buscador de vídeos además de diversos canales y temáticas para la clasificación de los vídeos.

Se ha convertido en una plataforma imprescindible para la búsqueda de información, cursos on-line, vídeos de cualquier contenido, etc.

En la web podemos observar cómo dispone de un buscador de vídeos (en la parte superior) además de las temáticas de los diferentes vídeos (en la parte izquierda).

Además de Youtube existen otras páginas de distribución de vídeo con un funcionamiento similar, como [vimeo](http://www.vimeo.com) (www.vimeo.com).

3.6. Criterios de calidad de servicio (QoS)

La **calidad de servicio o QoS (Quality of Service)** son una serie de **requisitos o condiciones** que deben cumplir las infraestructuras o servicios **con objeto de asegurar la calidad del servicio de telecomunicaciones** que se quiere ofrecer a los usuarios.

Estos **criterios** se refieren en general a parámetros como:

- **Retardo máximo de la señal.**
- **Retardo máximo del paquete IP.**
- **Tiempo de establecimiento de una conexión.**
- **Tiempo de liberación** de una conexión.
- **Tasa binaria de transferencia.**
- **Ancho de banda.**
- **Máximo jitter** permitido.

Los anteriores son criterios de calidad sobre la transmisión de las señales que afectan en definitiva al servicio ofrecido a los usuarios.

Pero además existen **otros criterios de servicios** y/o parámetros que afectan más a los operadores.

Estos pueden **clasificarse** en:

- **Parámetros generales** entre los que encontramos:
 - Tiempo de suministro de accesos a la red fija.
 - Tiempo de suministro de accesos a Internet.
 - Proporción de problemas en los procedimientos de portabilidad numérica.
 - Porcentaje de avisos de averías por línea de acceso fijo.
 - Tiempo de reparación de averías para líneas de acceso fijo.
 - Tiempo de respuesta para consultas sobre asuntos administrativos y de facturación.
 - Frecuencia de reclamaciones de los clientes.
 - Tiempo de resolución de reclamaciones de los clientes.
 - Reclamaciones sobre corrección de facturas.
 - Reclamaciones sobre el saldo de las tarjetas prepago.
 - Tiempo de respuesta para los servicios de consulta de directorio.
- **Parámetros relacionados con las llamadas.**
 - Entre ellos destacan los siguientes:
 - Proporción de llamadas fallidas.
 - Tiempo de establecimiento de llamada.
- **Parámetros específicos de acceso a Internet.**
 - Entre ellos destacan los siguientes:
 - Proporción de accesos de usuario con éxito.
 - Proporción de transmisiones de datos fallidas.
 - Velocidad de transmisión de datos conseguida.

3.7. Control de retardos y congestión

El control de retardos y congestión son parámetros especialmente críticos en determinados servicios de telecomunicaciones y/o datos.

Son críticos en los denominados servicios en tiempo real como pueden ser la VoIP, TvIP, videostreaming, juegos en red, etc.

Es por ello que estos parámetros deben estar acotados para evitar que estos servicios sufran cortes, fluctuaciones o incluso sea imposible realizar la conexión.

Unas redes de comunicaciones de gran ancho de banda (como las que emplean la fibra óptica o redes mesh) facilitan en gran medida el control de retardos y congestión evitando problemas en los servicios de tiempo real como los descritos anteriormente.

Así por ejemplo en la telefonía sobre IP (VoIP), para que el servicio pueda ser empleado con la calidad de servicio aceptable o comparable con la telefonía convencional debemos asegurar que el retardo entre los paquetes no debe superar los 150 mseg.

Pero no solo es imprescindible el control del retardo sino también las pérdidas de paquetes (que están directamente relacionadas con la congestión de la red), que deben estar también acotadas para evitar pérdida de la calidad del servicio.

En este sentido es crucial el empleo de métodos de alta compresión como por ejemplo el MPEG-4 para videostreaming, ya que supone garantizar la tasa de transferencia sobre las redes de comunicaciones que en cualquier caso deben ser de gran ancho de banda.

4. Implementación y configuración de pasarelas

4.1. Tipos y funciones de pasarelas. Servicios que soportan

Una pasarela o gateway es un sistema de hardware/software para conectar dos redes entre sí y que funcionen como un interfaz entre diferentes protocolos de red.

Se trata de un equipamiento que trabaja a nivel de capas superiores del modelo OSI, es decir, a partir de las capas de sesión, presentación y/o aplicación.

Lo vemos en el siguiente esquema.



En el caso del modelo TCP/IP, trabajaría en el nivel de aplicación.

Lo vemos también en el siguiente esquema.



Una pasarela es un dispositivo hardware o aplicación software que permite interconectar redes entre sí a nivel de aplicación del modelo OSI y/o TCP/IP.

Cuando un equipo quiere conectarse a otro equipo que está fuera de su rango de red, debe contactar con la pasarela para que le dé acceso a la red exterior.

Como ambas redes pueden trabajar en protocolos distintos, es función de la pasarela realizar la traducción automática de paquetes y protocolos de manera totalmente transparente para el usuario para que ambos equipos puedan conectarse.

El funcionamiento es el siguiente: cuando un usuario remoto contacta con la pasarela, esta examina su solicitud. Si dicha solicitud coincide con las reglas que el administrador de red ha configurado, la pasarela crea una conexión entre las dos redes. Por lo tanto, la información no se transmite directamente, sino que se traduce para garantizar una continuidad entre los dos protocolos.

El Gateway además ofrece seguridad adicional dado que toda la información se analiza antes de ser enviada. Las pasarelas son por tanto convertidores de protocolos que permiten conectar LANs que utilicen diferentes tecnologías, traduciendo los paquetes y el tráfico de un esquema al otro.

Por ejemplo, una pasarela podría conectar una red Ethernet a otra Token Ring.

Dependiendo de la complejidad de la traducción, pueden operar en cualquier nivel OSI desde el 3 en adelante. En realidad, un router es un caso particular de pasarela en la que ambos extremos usan el mismo protocolo (generalmente Ethernet e IP).

Algunos tipos de gateways existentes son los siguientes:

Gateway asíncrono

Se corresponde a un tipo de gateway que permite a los usuarios de ordenadores personales acceder a grandes ordenadores (mainframes) asíncronos a través de un servidor de comunicaciones, utilizando líneas telefónicas commutadas o punto a punto. Generalmente están diseñados para una infraestructura de transporte muy concreta, por lo que son dependientes de la red.

Gateway SNA

Este tipo de Gateway permite la conexión a grandes ordenadores con arquitectura de comunicaciones SNA (System Network Architecture, Arquitectura de Sistemas de Red), actuando como terminales y pudiendo transferir ficheros o listados de impresión.

Gateway TCP/IP

Estos gateways proporcionan servicios de comunicaciones con el exterior vía RAL o WAN y también funcionan como interfaz de cliente proporcionando los servicios de aplicación estándares de TCP/IP.

Gateway PAD X.25

Son similares a los asíncronos; la diferencia está en que se accede a los servicios a través de redes de conmutación de paquetes X.25.

Gateway FAX

Los servidores de Fax proporcionan la posibilidad de enviar y recibir documentos de fax.

Los gateways o pasarelas habitualmente incluyen o soportan otros servicios además de la conectividad de redes y de traducción de protocolos.

Entre estos servicios que se incluyen destacan los siguientes:

Funciones de firewall

Un firewall o cortafuegos es un dispositivo encargado de monitorizar el tráfico y filtrarlo en función de unas reglas o criterios.

Según el nivel de sofisticación del filtrado, puede operar en diferentes capas OSI, hasta el nivel 7.

Existen dos tipos de firewall:

–Firewall de red.

·Trabaja a nivel 3 o 4 del modelo OSI.

·Se encarga del filtrado del paquete según unas reglas configuradas.

·Permite con ello bloquear el tráfico, redirigir el tráfico, filtrar el tráfico, etc.

·Pueden implementarse tanto en hardware como en software.

–Firewall de aplicación.

Trabaja a nivel 7 del modelo OSI y permite el tráfico a nivel de protocolos como el protocolo http.

El objetivo es filtrar virus y contenidos no deseados en general.

Se suelen implementar en software.

La esencia de los firewall son las reglas que incluyen y su configuración.

Estas reglas pueden ser de dos tipos:

–Reglas positivas.

·Son aquellas en las que se impide el paso de todo el tráfico, excepto aquel que se indica explícitamente mediante reglas que puede circular.

·Es más seguro pero más complejo de configurar.

–Reglas negativas.

·Son aquellas en las que se deja pasar todo el tráfico, excepto aquel que se indica explícitamente que se debe bloquear.

·Es más sencillo de configurar pero más vulnerable.

Funciones de proxy

Un proxy es un dispositivo que permite el acceso a un servicio de red de manera indirecta, permitiendo el procesado del tráfico con diferentes objetivos. Opera en la capa 7 OSI, y generalmente se implementa mediante software.

Con el proxy se persiguen los siguientes objetivos:

–Actuar como caché para conseguir la mayor velocidad y eficiencia.

Con ello se consiguen almacenar temporalmente las peticiones más comunes a un servicio de red para evitar su saturación. Un caso típico es un proxy caché para el acceso a Internet.

–Actuar como filtro.

Se puede filtrar el tráfico que circula por el Gateway actuando como cortafuegos o firewall.

–Permite incluir medidas de seguridad.

Es decir, mediante un proxy es posible asegurar que el acceso a un recurso se hará de forma cifrada, o bien filtrar determinados contenidos que por motivos de seguridad se consideren peligrosos.

–Servidores de dominios de nombres (DNS).

Un Gateway puede ser configurado para que actúe como servidor de DNS y con ello traducir las direcciones IP en direcciones URL consiguiendo actuar de forma más rápida y eficiente que si dicha función se tiene que realizar en un servidor DNS exterior.

Los firewall o cortafuegos son funcionalidades que incluyen los gateways y constituyen mecanismos de seguridad para las redes de datos.

Los gateways o paralelas suelen ser aplicaciones que se instalan en un equipo servidor destinado a tal fin.

También en numerosas ocasiones suelen ser equipos hardware en los cuales ya vienen instaladas y configuradas las aplicaciones que realizan las funciones de pasarela o Gateway.

Pero en definitiva se trata de un equipamiento hardware (un PC) con un software especializado que realiza las funciones de pasarela.

Este equipamiento hardware debe tener unas prestaciones especiales de capacidad de memoria, de capacidad de procesado, de memoria caché, etc. adecuadas para realizar de forma correcta la función de pasarela ya que por él van a pasar mucha información de red que debe de procesarla de una manera rápida y eficiente.

Este equipamiento que actúa como pasarela o Gateway suele ubicarse cercano o próximo al CPD (si existe) o a los servidores o routers de la empresa u organización ya que es un elemento que debe gestionar el administrador de red o administrador de sistemas.

No es habitual y tampoco recomendable instalar la aplicación de pasarela en el servidor principal de la empresa u organización junto con el resto de servicios como servidor de DNS, servidor de DHCP, etc., ya que le resta prestaciones a las funciones y eficiencia de la función de pasarela.



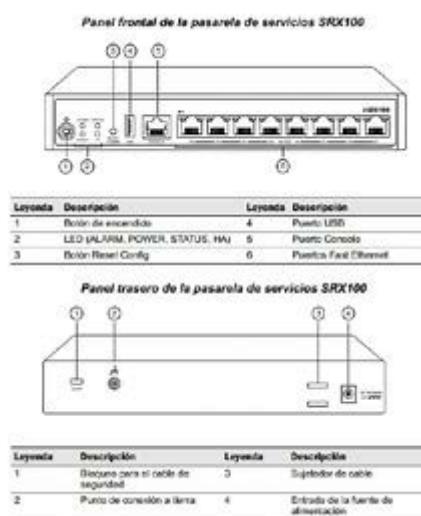
A continuación mostramos el ejemplo de un Gateway para su instalación y configuración (la instalación y configuración de cualquier otro

Gateway tiene un procedimiento similar siempre y cuando se sigan las instrucciones del fabricante).

Este Gateway se caracteriza por tener las siguientes prestaciones:

- 8 puertos RJ-45 10/100 para su conectividad a la red LAN.
- 1 puerto para la consola.
- 2 puertos USB 2.0.
- Indicadores Leds de encendido, alarma, funcionamiento, etc.
- Funciones de seguridad, enrutamiento y cortafuegos hasta 700 Mbps.
- Soporta antivirus, anti SPAM, IPS, etc.

En la siguiente figura indicamos los conectores de este Gateway.



A continuación describimos los pasos para la instalación del hardware del dispositivo:

Paso 1

Conectamos el cable de alimentación del dispositivo a la fuente de alimentación.

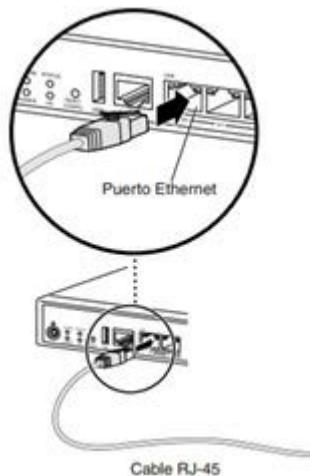
(El fabricante recomienda siempre conectar dicho dispositivo bajo el circuito de protección de sistemas de alimentación ininterrumpida o SAIs).

Una vez conectado el dispositivo a la alimentación eléctrica se debe encender el piloto o Led de POWER.

El encendido del piloto ALARM indica que existe un problema de funcionamiento con el dispositivo. Si es un color ámbar indicar un error leve y si es un color rojo indica un error grave. Debe revisarse entonces el dispositivo y la hoja de características del dispositivo para corregir el problema.

Paso 2

Conectar el dispositivo a la red LAN a través de uno de los conectores RJ-45.



Lo vemos en la siguiente figura.

Hasta aquí ya hemos realizado la conexión hardware del dispositivo.

Ahora realizaremos la instalación y configuración del software del dispositivo.

Paso 1

En primer lugar debemos asignar una dirección IP al dispositivo.

Por defecto está asignada la dirección IP 192.168.1.1.

Si queremos asignar una dirección distinta debemos acceder al menú de configuración del dispositivo a través de la interfaz web que ofrece el dispositivo.

Para ello debemos arrancar la aplicación J-web escribiendo en cualquier navegador la dirección.

<http://192.168.1.1>

Nos saldrá a continuación el acceso a la interfaz en la cual nos pedirá el user y el pass que serán (definidos por fábrica):

User: root

Pass: no tiene

En la siguiente figura podemos ver este logueo al interfaz:



Paso 2

Una vez dentro de la interfaz de configuración del dispositivo podemos configurar los siguientes parámetros:

—Dirección IP del dispositivo de forma manual (si no queremos que sea la dirección IP 192.168.1.1 que viene definida por defecto).

—Host name del dispositivo.

–Clave de acceso al dispositivo.

Estos parámetros se configuran desde el menú principal.

En la siguiente imagen podemos ver este menú principal.



En este punto ya tenemos instalado y configurado el funcionamiento básico del Gateway descrito.

4.3. Condiciones de instalación de la pasarela

Antes de proceder a la instalación y configuración de la pasarela se deben de asegurar unas ciertas condiciones para su correcto funcionamiento y operatividad.

A continuación se describen estas condiciones:

–El dispositivo debe instalarse (en el caso de que no sea enractable) sobre una superficie lisa y horizontal limpia de polvo y suciedad.

–Debe estar ubicado en una zona de temperatura constante y ventilación de aire (a ser posible en un CPD o zona con climatización).

–Debe estar bajo la protección de sistemas de alimentación ininterrumpida o SAIs.

–El cableado debe estar correctamente bridado y fuera de zonas de paso.

En el caso de que la pasarela sea una aplicación o software, debe instalarse sobre un equipo (cuya ubicación debe cumplir con las condiciones anteriormente descritas) y debe reunir al menos las siguientes condiciones:

–Equipo hardware destinado exclusivamente para las funciones de gateway o pasarela.

–Capacidad de procesado de CPU adecuadas para las funciones de pasarela.

–Capacidad de memoria RAM y de discos duros para cubrir las necesidades de la aplicación de Gateway.

–Interfaces o tarjetas de red con capacidad y prestaciones suficientes para las funciones de pasarela que va a cumplir el equipo.

4.3.1. Análisis de los mapas de direcciones IP

A continuación vamos a realizar la configuración de un gateway realizando los ajustes de sus direcciones IP y de los servicios que puede soportar.

Para ello tomaremos como referencia el Gateway modelo GXW-4108 de Grandstream.

En la siguiente figura podemos ver este Gateway.



A continuación describimos sus características:

–Se trata de un gateway para entornos profesionales de pymes que permite resolver la conectividad del servicio telefónico de la red LAN. El Gateway se comporta como un traductor de servicio telefónico VoIP (protocolo SIP) para convertirlas en llamadas telefónicas analógicas y cursarlas a la RTC a la que también se conecta.

–Dispone de 8 conectores RJ-11 para su conexión a la RTC.

–Dispone de 2 puertos RJ-45 10/100 Mbps.

–Permite múltiples cuentas SIP.

–Incluye cancelación de eco.

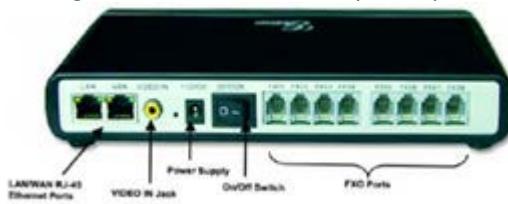
–Configuración mediante entorno Web.

–Configuración para diferentes RTC de diferentes países o áreas.

–Soporta el códec de vídeo H.264.

–Soporta códec de audio G.711 u/a, G.723, G.729, GSM y T.38.

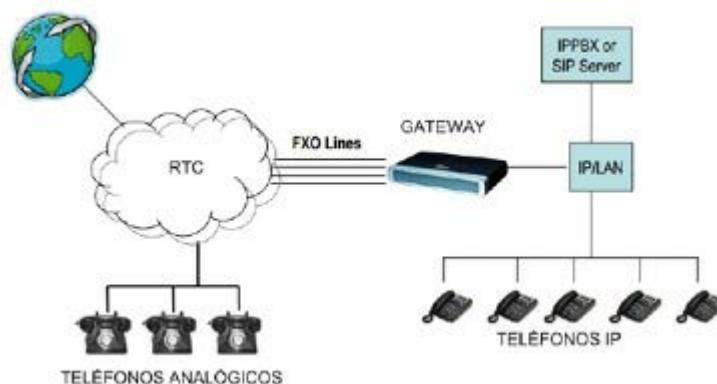
Vemos a continuación en la siguiente figura los conectores de que dispone el gateway.



En ella se pueden observar los siguientes conectores:

- 8 puertos RJ-11 para línea telefónica.
- 2 puertos RJ-45 10/100 Mbps.
- Entrada de vídeo en formato Jack.
- Entrada de alimentación de 12 VDC.
- Botón de encendido y apagado.

A continuación mostramos un esquema de funcionamiento del gateway dentro de una LAN y su conectividad a la RTC.



En el esquema anterior podemos ver cómo el gateway actúa como elemento de conexión entre la red LAN de una oficina o pyme con la red telefónica comutada (RTC). Dicha conexión se realiza mediante las 4 líneas FXO (permite hasta 8) de que dispone el gateway.

El gateway permite por tanto cursar el tráfico de VoIP a través de la RTC realizando la conversión de telefonía IP a telefonía analógica convencional.

La red LAN incorpora entre otros elementos los teléfonos IP mediante los cuales se puede realizar servicio VoIP y la central telefónica IP (IP PBX).

Veamos un **ejemplo**.

Dado el siguiente gateway que se muestra en la siguiente imagen, responda a las siguientes cuestiones.



–Enumere y marque cuántos conectores de FXS para líneas telefónicas analógicas dispone.

–Enumere y marque cuántos conectores para redes Ethernet dispone.

–Indique el conector de alimentación.

–El fabricante especifica que soporta el protocolo PPPoE. Averigüe en qué consiste dicho protocolo.

Solución:

Respondemos a cada uno de los apartados.

–El número de conectores FXS que dispone el gateway es de 24.

En la siguiente figura marcamos dichos conectores.



Se trata de conectores RJ-11 para línea telefónica convencional.

En la propia nomenclatura del gateway ya viene indicado el número de conectores FXS: GXW4224.

–El número de conectores RJ-45 (Ethernet) es 1.

En la siguiente figura marcamos dicho conectores.

Se trata de conectores RJ-45 (se supone de 10/100/1000) para su conexión a la red LAN o red WAN.

–El conector de alimentación viene marcado en la siguiente imagen.



–El protocolo PPPoE es un protocolo punto a punto a través de una red Ethernet (Point to Point Protocol over Ethernet) que permite conectar a Internet muchos usuarios en una red a través de un conexión xDSL.

Se trata de un protocolo que suelen incluir casi todos los gateways actuales.

4.3.2. Análisis de las líneas y nodos de transmisión de voz

A partir del esquema de funcionamiento del gateway mostrado en la imagen vamos a configurar el dispositivo para que cuatro teléfonos IP cursen llamadas por las 4 líneas analógicas de salida del gateway.

Para ello debemos configurar en el dispositivo estas líneas según la siguiente tabla:

Canal	SIP User	Clave SIP
1	101	*****
2	102	*****
3	103	*****
4	104	*****

La tabla anterior lo que configura es que los teléfonos IP identificados con su SIP User y su clave correspondiente van a cursar las llamadas a través de la líneas FXO descritas en la tabla.

A modo de ejemplo, el teléfono IP con SIP User 104 cada vez que va a cursar una llamada saldrá por la línea 4 (línea analógica) del gateway.

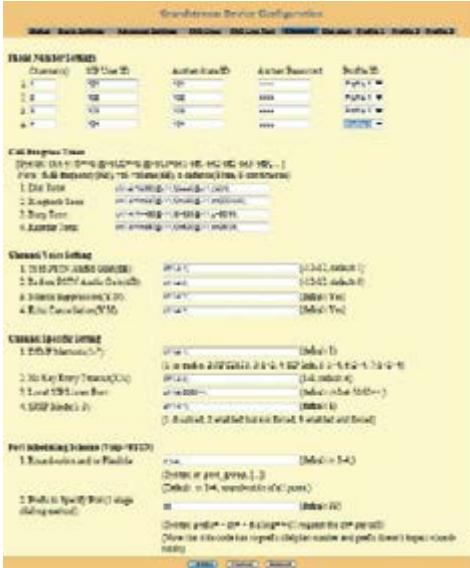
Este se realiza en la configuración del dispositivo a la que se accede mediante interfaz web.

Una vez accedido y logueado, elegimos la pestaña Channels donde configuraremos según la tabla anterior.

En la siguiente imagen podemos ver el panel de configuración.



La opción de profile la dejamos por defecto en profile 1.



Profile se refiere a un conjunto de ajustes preconfigurado que se puede guardar y evitar así realizar la configuración parámetro a parámetro.

Así si elegimos el profile 1 indica al dispositivo que debe configurar los parámetros según lo descrito y guardado en profile 1.

4.4. Parámetros de configuración

Son muchos los parámetros que se pueden configurar en un gateway.

Estos parámetros dependen del modelo de gateway que se escoja ya que cada uno de ellos viene con diferentes prestaciones.

En general los parámetros de configuración se pueden clasificar en:

–Parámetros de configuración de servicios.

–Parámetros de seguridad.

–Parámetros de configuración del operador de servicios.

A continuación veremos con más detalle cada uno de estos parámetros y como configurarlos.

Todos los gateways, así como los routers y switches gestionables, incluyen una interfaz web que permite su configuración remota desde cualquier punto de la red o desde cualquier punto del mundo gracias a las VPN.

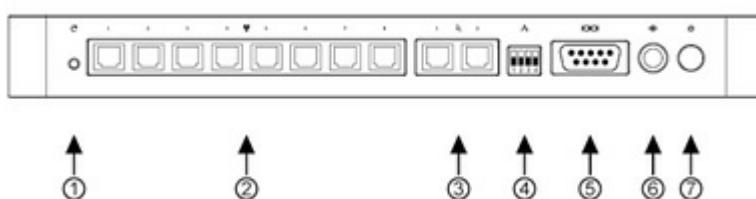
4.4.1. Parámetros de configuración de servicios

Para su configuración emplearemos como ejemplo el gateway Security 360 de Symantec.

En la siguiente figura podemos ver el dispositivo.



En la siguiente figura podemos ver los conectores en la parte trasera.



Los conectores que incluyen son los mostrados en la siguiente tabla:

Referencia	Función
1	Botón de Reset del dispositivo
2	8 puertos RJ-45 10/100 para conectividad a la LAN
3	2 puertos RJ-45 para la conectividad a la WAN
4	Switches de configuración del dispositivo
5	Puerto Serie RS-232 para conectividad a un modem
6	Toma de Alimentación a 220-230/50 Hz
7	Botón de ON/OFF

El dispositivo dispone de una interfaz web para su configuración denominada SGMI (Symantec Gateway Management Interface) a la que se accede a través de un navegador web en la dirección 192.168.0.1 (dirección IP por defecto de fábrica).

Una vez accedido y logueado con las siguientes contraseñas (por defecto de fábrica):

User: admin

Pass: admin

Accedemos al panel de configuración que se muestra en la siguiente imagen.



En la anterior figura podemos observar las siguientes secciones:

- Menú principal: permite la configuración de los diferentes servicios que soporta el gateway.
- Fichas de menú: permiten la gestión del dispositivo.
- Contenidos del panel: permiten la configuración y ajuste de los parámetros de los servicios que soporta el gateway.

Además dispone de un enlace a una ayuda online de la aplicación de gestión y configuración.

A continuación configuraremos el primer menú, es decir, el de gestión que es el que se muestra en la anterior figura.

Este panel es el que permite el ajuste del acceso a la gestión del dispositivo.

En ella configuraremos dos parámetros:

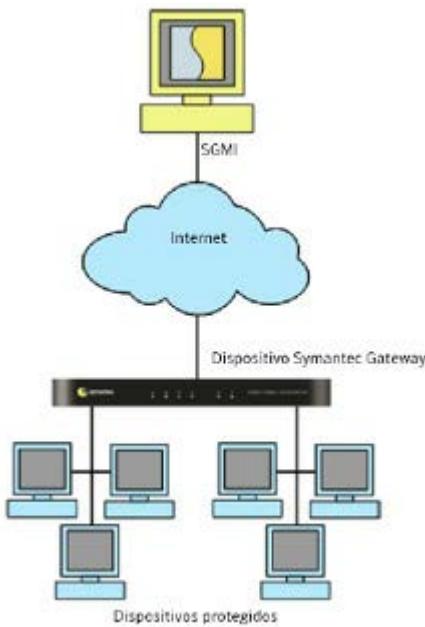
- La clave de acceso a la SGMI (el user es siempre admin).

Se debe cambiar periódicamente esta clave por cuestiones de seguridad.

- Las direcciones IP desde que las que permitiremos acceder a la gestión del dispositivo.

Con este parámetro se asegura que la gestión y configuración del dispositivo solo pueda realizarse desde unos equipos determinados en modo remoto desde la WAN (fijados en la IP que se especifica).

Esto último lo podemos ver en el siguiente esquema.



Si sólo se quiere especificar una dirección IP de un equipo remoto, la dirección IP inicio y la dirección IP final deben coincidir con la dirección IP del equipo desde el cual se quiere acceder.

El acceso al gateway desde un equipo remoto en la red WAN debe realizarse desde un navegador web. En la URL debemos escribir lo siguiente:

`http://<Dirección IP gateway>:8080`

Siendo <dirección IP gateway> la dirección IP pública del gateway.

A continuación nos saldrá el menú de logueo al dispositivo en el cual debemos introducir el user y el pass.

Así por ejemplo, si la dirección IP pública del gateway es 80.95.10.10 debemos escribir en el navegador del equipo remoto lo siguiente:

`http://80.95.10.10:8080`

Y a continuación nos saldrá la página de logueo al dispositivo.

4.4.2. Parámetros de seguridad

Los parámetros de seguridad que generalmente integran los gateways (aunque dependen de los modelos) son los siguientes:

- Firewall.
- Redes privadas (VPN) con encriptación.
- Antivirus.
- Detección de intrusos.
- Prevención de intrusiones.
- Filtrado estático de contenidos.

Todos estos parámetros se configuran habitualmente desde la interfaz web que permite el dispositivo y empleando un navegador tal y como se ha visto en el anterior apartado.

4.4.3. Información sobre la configuración de red del operador

El gateway se puede conectar tanto a una red interna (LAN) como a una red externa (WAN).

En función de esto empleará un tipo de conexión u otro.

El gateway dispone de diferentes parámetros de configuración en función del tipo de conexión que se establece según se conecte a una red interna (LAN) o red externa (WAN).

En función de lo anterior existen diferentes tipos de conexiones:

- Conexión mediante un acceso telefónico.
- Conexión mediante un acceso de banda ancha.

En el caso del acceso telefónico, podría ser de diferentes formatos:

–Módem telefónico xDSL con un conector RJ-11.

–Enlace RDSI.

Y en el caso de acceso de banda ancha tenemos las siguientes variantes:

–Conexión DHCP.

–Conexión PPPoE.

4.5. Herramientas de configuración

Las herramientas para la configuración de los gateways, como ya se ha visto en los apartados anteriores suelen ser una interfaz web a la que se accede desde cualquier navegador web.

Por defecto, los gateways suelen estar configurados para tener la dirección IP 192.168.0.1 (puede variar según los modelos) y sus claves de acceso suelen ser (puede variar según los modelos):

User: admin

Pass: admin

Estos valores en cualquier caso pueden ser cambiados por el administrador de red en el panel de configuración.

En el caso del gateway Security 360 a esta interfaz se le denomina SGMI (Symantec Gateway Management Interface).

4.6. Protocolos de gestión

Uno de los protocolos más empleados en la gestión de red es el protocolo SNMP.

Este protocolo permite gestionar los dispositivos que están conectados en red y que emplean el protocolo TCP/IP con objeto de monitorizar el estado de la red y el mantenimiento de la misma.

En este protocolo se distinguen dos conceptos:

–Gestor: es un dispositivo y/o aplicación que controla y monitoriza un conjunto de agentes.

–Agentes: son dispositivos conectados a la red que realizan determinadas funciones. Generalmente son los elementos de interconexión como router, gateways, switches, etc.

Veremos a continuación con más detalles de cada uno de estos elementos.

Gestor

Un gestor es una máquina que ejecuta un cliente SNMP que se encarga de controlar y monitorizar clientes de la red.

Para ello periódicamente solicita información del estado de cada uno de los agentes para analizar el estado de la red y notificando las incidencias producidas.

El gestor también puede actuar sobre los agentes enviando órdenes y comandos a los agentes para que realicen determinadas tareas para el correcto mantenimiento de la red.

En ocasiones puede incluir el provocar el reinicio de los valores de un agente si así fuese necesario.

Agente

Un agente es un dispositivo o máquina de la red que realiza determinadas funciones de red como por ejemplo encaminar los mensajes, tramas o paquetes.

Por tanto, los agentes suelen ser elementos de interconexión como routers y gateways mayoritariamente.

Un agente (o encaminador) puede almacenar variables como número de paquetes recibidos y enviados y así trasladarlo al gestor.

Los agentes también pueden contribuir en el proceso de gestión. El agente puede comprobar el entorno de la red donde realiza sus funciones y advertir al gestor de posibles problemas para que este último adopte las medidas preventivas y/o correctoras necesarias.

Existen otros protocolos que cooperan con el SNMP para la gestión de la red.

Estos protocolos son los siguientes:

–SMI:

Es un protocolo cuya función es nombrar los objetos de la red, definir el tipo de datos que es capaz de almacenar y cómo mostrarlo y transmitirlo por la red.

–MIB:

Es un protocolo que define la colección o estructura jerárquica de objetos de un agente y que puede manejar un gestor.

El protocolo SNMP define una serie de mensajes para el intercambio de información entre gestor y agentes con objeto de cumplir con las funcionalidades de gestión de la red.

Entre todos los mensajes que se describe en el protocolo destacamos los más importantes:

–GetRequest:

Es un mensaje de petición enviado desde el gestor a un agente para solicitarle el valor de una variable.

–GetResponse:

Es un mensaje de respuesta enviado desde un agente a un gestor (tras un GetRequest) donde se adjunta el valor de la variable solicitada.

–SetRequest:

Es el mensaje enviado desde un gestor a un agente para almacenar un valor en una variable del agente.

–Trap:

Es un mensaje enviado desde un agente a un gestor para informarle de un evento.

4.7. Parámetros de calidad en el servicio

La calidad de servicio o QoS (Quality of Service) es una serie de requisitos o condiciones que deben cumplir los dispositivos con objeto de asegurar la calidad del servicio de telecomunicación que se quiere ofrecer a los usuarios.

Estos criterios se refieren en general a parámetros como:

–Retardo máximo de la señal.

–Retardo máximo del paquete IP.

–Tiempo de establecimiento de una conexión.

–Tiempo de liberación de una conexión.

–Tasa binaria de transferencia.

–Ancho de banda.

–Máximo jitter (fluctuación) permitido.

Lo anterior son criterios de calidad sobre la transmisión de las señales que afectan en definitiva al servicio ofrecido a los usuarios.

Pero además existen otros criterios de servicios y/o parámetros que afectan más a los operadores.

Estos pueden clasificarse en:

Parámetros generales entre los que encontramos

–Tiempo de suministro de accesos a la red fija.

–Tiempo de suministro de accesos a Internet.

–Proporción de problemas en los procedimientos de portabilidad numérica.

–Porcentaje de avisos de averías por línea de acceso fijo.

–Tiempo de reparación de averías para líneas de acceso fijo.

–Tiempo de respuesta para consultas sobre asuntos administrativos y de facturación.

–Frecuencia de reclamaciones de los clientes.

–Tiempo de resolución de reclamaciones de los clientes.

–Reclamaciones sobre corrección de facturas.

–Reclamaciones sobre el saldo de las tarjetas prepago.

–Tiempo de respuesta para los servicios de consulta de directorio.

Parámetros relacionados con las llamadas

Entre ellos destacan los siguientes:

- Proporción de llamadas fallidas.
- Tiempo de establecimiento de llamada.

Parámetros específicos de acceso a Internet

Entre ellos destacan los siguientes:

- Proporción de accesos de usuario con éxito.
- Proporción de transmisiones de datos fallidas.
- Velocidad de transmisión de datos conseguida.

Otra serie de parámetros que influyen también en la calidad del servicio son el control de retardos y congestión.

Son críticos en los denominados servicios en tiempo real como pueden ser la VoIP, TvIP, videostreaming, juegos en red, etc.

Es por ello que estos parámetros deben estar acotados para evitar que estos servicios sufran cortes, fluctuaciones o incluso sea imposible realizar la conexión.

Unas redes de comunicaciones de gran ancho de banda (como las que emplean la fibra óptica o redes imesh) facilitan en gran medida el control de retardos y la congestión evitando problemas en los servicios de tiempo real como los descritos anteriormente.

Así por ejemplo en la telefonía sobre IP (VoIP) para que el servicio pueda ser empleado con la calidad de servicio aceptable o comparable con la telefonía convencional debemos asegurar que el retardo entre los paquetes no debe superar los 150 mseg.

Pero no solo es imprescindible el control del retardo, sino también la pérdidas de paquetes (que están directamente relacionadas con la congestión de la red), que deben estar también acotadas para evitar pérdida de la calidad del servicio.

En este sentido es crucial el empleo de métodos de alta compresión como por ejemplo el MPEG-4 para videostreaming, ya que supone garantizar la tasa de transferencia sobre las redes de comunicaciones que en cualquier caso deben ser de gran ancho de banda.

4.8. Pruebas funcionales y estructurales

Todos los equipos de interconexión de redes (incluidos los gateways o pasarelas) deben superar unas pruebas funcionales y estructurales con objeto de que puedan cumplir las prestaciones para la que fueron diseñados.

Aunque dichas pruebas dependen del modelo del gateway, hay una serie de ellas que se deben siempre verificar en la instalación y configuración de cualquier gateway.

Entre ellas destacamos las siguientes:

- ⇒ Comprobación del nombre y clave del administrador del dispositivo.
- ⇒ Comprobación de la dirección IP del dispositivo.
- ⇒ Comprobación de la conectividad WAN del gateway (si lo hubiera).
- ⇒ Comprobación de cada uno de los puertos que dispone el gateway.
- ⇒ Comprobación de los servicios que soporta el gateway como DHCP, NAT, STUN, PPPoE, etc.

4.9. Comandos para el mantenimiento y resolución de problemas

Aunque la mayoría de los gateways disponen de una interfaz web para su configuración, siempre es posible configurarlo desde la línea de comandos o consola.

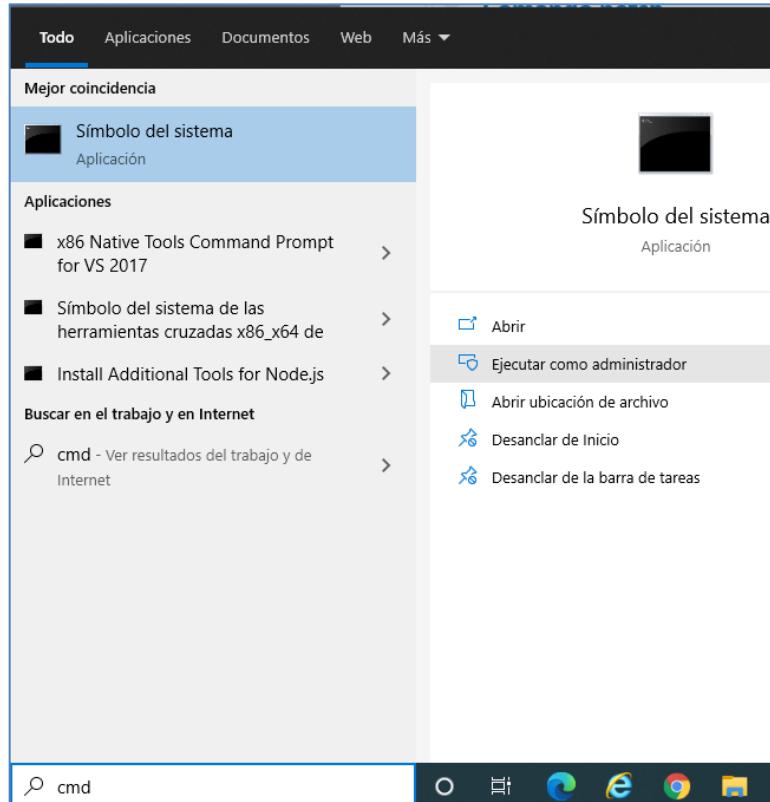
Para ello debemos abrir la ventana de comandos y teclear los diferentes comandos existentes junto con sus parámetros para configurar el dispositivo.

Entre los comandos más habituales encontramos los siguientes:

Comando netsh

Permite cambiar la IP de una interfaz de red...

Para hacerlo tenemos que ejecutar la línea de comandos como administradores, así escribimos **cmd** en buscar programas y elegimos "**Ejecutar como administrador**"



Desde la línea de comandos lo primero que vamos a verificar es las conexiones ipv4 que tenemos y sus nombres, para lo que escribimos: **netsh interface ipv4 show config**

```
Administrator: Símbolo del sistema

C:\WINDOWS\system32>netsh interface ipv4 show config

Configuración para la interfaz "Ethernet"
  DHCP habilitado:           Sí
  Dirección IP:              192.168.1.44
  Prefijo de subred:          192.168.1.0/24 (máscara 255.255.255.0)
  Puerta de enlace predeterminada: 192.168.1.1
  Métrica de puerta de enlace:    0
  Métrica de interfaz:          25
  Servidores DNS configurados a través de DHCP: 192.168.1.1
  Registrar con el sufijo:       Solo el principal
  Servidores WINS configurados a través de DHCP: ninguno

Configuración para la interfaz "Ethernet 3"
```

Vemos que tenemos varios interfaces de red, y el que nos interesa es el primero, el interfaz de red local llamando **Ethernet** y vemos que tiene activado DHCP.

Vamos a ver como podemos cambiar la ip a estática (static), mascara de subred y puerta de enlace, para hacerlo escribimos en la línea de comandos:

```
netsh interface ipv4 set address name="Ethernet" static 192.168.1.51 255.255.255.0 192.168.1.1
```

```
C:\WINDOWS\system32>netsh interface ipv4 set address name="Ethernet" static 192.168.1.51 255.255.255.0 192.168.1.1
C:\WINDOWS\system32>
```

Si escribimos de nuevo **netsh interface ipv4 show config** veremos cómo ha cambiado la dirección IP pero no tenemos ninguna dirección DNS con lo cual no vamos a poder navegar por internet con normalidad:

```
C:\WINDOWS\system32>netsh interface ipv4 set address name="Ethernet" static 192.168.1.51 255.255.255.0 192.168.1.1

C:\WINDOWS\system32>netsh interface ipv4 show config

Configuración para la interfaz "Ethernet"
  DHCP habilitado:          No
  Dirección IP:             192.168.1.51
  Prefijo de subred:        192.168.1.0/24 (máscara 255.255.255.0)
  Puerta de enlace predeterminada: 192.168.1.1
  Métrica de puerta de enlace:    1
  Métrica de interfaz:         25
  Servidores DNS configurados estáticamente: ninguno
  Registrar con el sufijo:      Solo el principal
  Servidores WINS configurados estáticamente: ninguno
```

Por lo tanto tenemos que indicarle también la configuración DNS, en este caso le podemos decir que use la IP de Google **netsh interface ipv4 set dnsservers "Ethernet" source=static 8.8.8.8**

```
C:\WINDOWS\system32>netsh interface ipv4 set dns name="Ethernet" static 8.8.8.8

C:\WINDOWS\system32>netsh interface ipv4 show config

Configuración para la interfaz "Ethernet"
  DHCP habilitado:          No
  Dirección IP:             192.168.1.51
  Prefijo de subred:        192.168.1.0/24 (máscara 255.255.255.0)
  Puerta de enlace predeterminada: 192.168.1.1
  Métrica de puerta de enlace:    1
  Métrica de interfaz:         25
  Servidores DNS configurados estáticamente: 8.8.8.8
  Registrar con el sufijo:      Solo el principal
  Servidores WINS configurados estáticamente: ninguno
```

Configuración de IP

Asignación de IP:	Manual
Dirección IPv4:	192.168.1.51
Longitud del prefijo de subred IPv4	24
Puerta de enlace de IPv4:	192.168.1.1
Servidores DNS IPv4:	8.8.8.8

Editar

También podemos añadir el servidor secundario escribiendo

```
netsh interface ipv4 add dnsservers "Ethernet" 192.168.1.1 index=2
```

Y para cambiar la configuración Ip a automática con DHCP escribimos:

```
netsh interface ipv4 set address name="Ethernet" source=dhcp
```

```
C:\WINDOWS\system32>netsh interface ipv4 set address name="Ethernet" source=dhcp
```

Configuración de IP

Asignación de IP:	Automático (DHCP)
Editar	

Comando ipconfig

Es el comando que permite modificar la interfaz de red de un gateway pero en sistemas operativos Windows.

Su funcionamiento es similar al ifconfig de Linux.

Este comando admite varios parámetros que son los siguientes:

- ⇒ Ipconfig /all: muestra información detallada de todas las interfaces de red.
- ⇒ Ipconfig /renew: solicita al servidor DHCP nueva asignación de dirección IP.
- ⇒ Ipconfig /release: libera las direcciones IP de la tarjeta de red.
- ⇒ Ipconfig /registerdns: registra todos los nombres DNS.
- ⇒ Ipconfig /flushdns: borra todas las entradas DNS.
- ⇒ Ipconfig /displaydns: muestra todas las entradas DNS.

Si se emplea únicamente el comando ipconfig muestra información resumida de todas las interfaces de red del dispositivo.

Comando tracert

Este comando devuelve como salida la ruta seguida por la petición hasta llegar al host de destino.

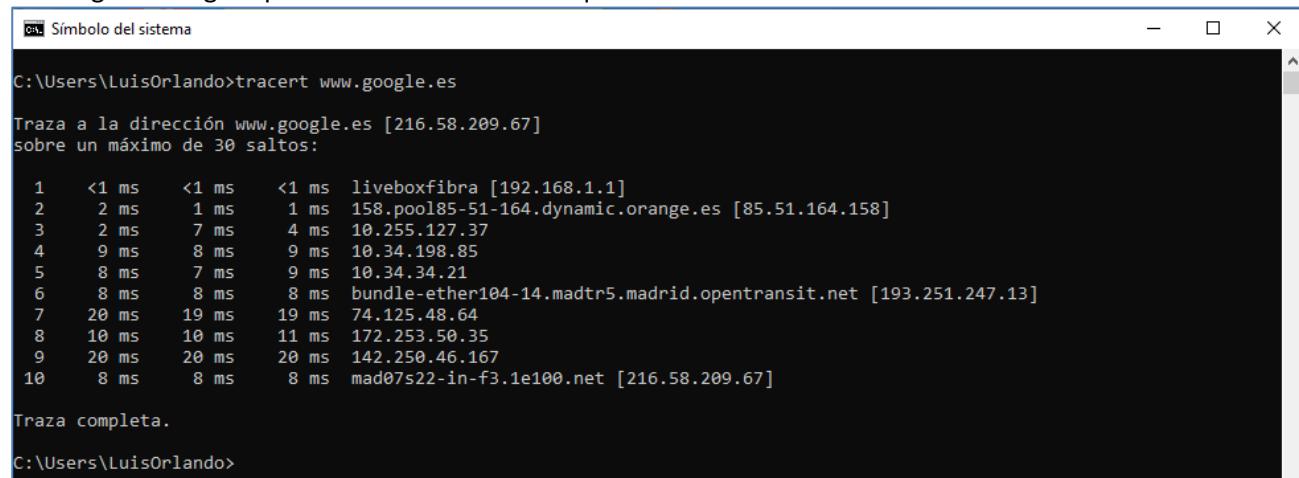
Su sintaxis es:

Tracert <dirección IP>

Así por ejemplo encontramos:

#tracert www.google.es

En la siguiente figura podemos ver el resultado que ofrece:



```
C:\Users\LuisOrlando>tracert www.google.es

Traza a la dirección www.google.es [216.58.209.67]
sobre un máximo de 30 saltos:

 1  <1 ms    <1 ms    <1 ms  liveboxfibra [192.168.1.1]
 2  2 ms     1 ms     1 ms  158.pool85-51-164.dynamic.orange.es [85.51.164.158]
 3  2 ms     7 ms     4 ms  10.255.127.37
 4  9 ms     8 ms     9 ms  10.34.198.85
 5  8 ms     7 ms     9 ms  10.34.34.21
 6  8 ms     8 ms     8 ms  bundle-ether104-14.madtr5.madrid.opentransit.net [193.251.247.13]
 7  20 ms    19 ms    19 ms  74.125.48.64
 8  10 ms    10 ms    11 ms  172.253.50.35
 9  20 ms    20 ms    20 ms  142.250.46.167
10  8 ms     8 ms     8 ms  mad07s22-in-f3.1e100.net [216.58.209.67]

Traza completa.

C:\Users\LuisOrlando>
```

El resultado son los nodos (sus direcciones IP) por lo que ha pasado la petición hasta llegar al destino.

Este comando admite un parámetro que es limitar el número de saltos que salga como resultado.

Su sintaxis sería la siguiente:

Tracert -h <numero> <dirección IP>

Por ejemplo, podemos encontrar el siguiente comando:

#tracert -h 10 www.google.es

Es decir, solo nos devolverá como resultado los diez primeros saltos que ha tenido nuestra solicitud de petición.

Comando ping

Es un comando que permite verificar y comprobar la conectividad de un equipo a nivel de red.

Se emplea para comprobar si un equipo o terminal está conectado, está en funcionamiento o si tiene problemas.

Su sintaxis es:

ping <dirección IP>

Por ejemplo, podemos encontrar el siguiente comando:

#ping 192.168.10.5

El resultado es la devolución del tiempo que ha tardado el mensaje o paquete (un paquete de longitud muy corta) en llegar desde el equipo que lanza el ping hasta el equipo con la dirección IP indicada.

Si el resultado es un valor finito, significa que dicho equipo con la dirección IP indicada está conectado en red y si devuelve un valor no definido o null es que dicho equipo presenta problemas de conectividad.

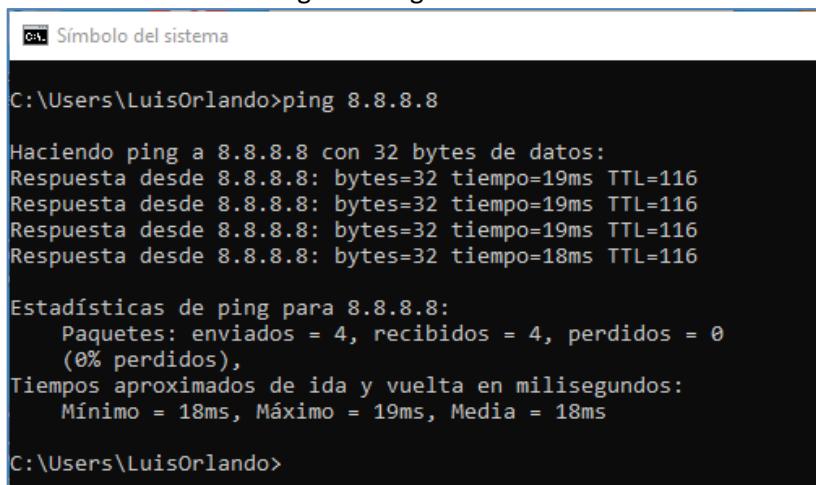
El comando además presenta las siguientes opciones como parámetro:

- ⇒ Ping -t: solicita eco al host hasta ser interrumpido.
- ⇒ Ping -a: resuelve direcciones a nombres de host.
- ⇒ Ping -n cantidad: Cantidad de solicitudes de eco a enviar.
- ⇒ Ping -l tamaño: Tamaño del búfer de envíos en bytes.
- ⇒ Ping -f: No fragmentar el paquete.
- ⇒ Ping -i TTL: Tiempo de vida (TDV).
- ⇒ Ping -v TOS: Tipo de servicio.
- ⇒ Ping -r cantidad: Registrar la ruta para esta cantidad de saltos.
- ⇒ Ping -s cantidad: Registrar horarios para esta cantidad de saltos.
- ⇒ Ping -j lista de hosts: Ruta origen variable en la lista de host.
- ⇒ Ping -k lista de hosts: Ruta origen estricta en la lista de host.

Vemos en el siguiente ejemplo el uso de este comando:

```
#ping 8.8.8.8
```

El resultado obtenido es el mostrado en la siguiente figura:



```
C:\Símbolo del sistema
C:\Users\LuisOrlando>ping 8.8.8.8

Haciendo ping a 8.8.8.8 con 32 bytes de datos:
Respuesta desde 8.8.8.8: bytes=32 tiempo=19ms TTL=116
Respuesta desde 8.8.8.8: bytes=32 tiempo=19ms TTL=116
Respuesta desde 8.8.8.8: bytes=32 tiempo=19ms TTL=116
Respuesta desde 8.8.8.8: bytes=32 tiempo=18ms TTL=116

Estadísticas de ping para 8.8.8.8:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
                (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
                Mínimo = 18ms, Máximo = 19ms, Media = 18ms

C:\Users\LuisOrlando>
```

En la anterior figura podemos ver cómo ha devuelto resultados finitos, es decir, el tiempo de retardo del paquete ping desde el equipo que lanza el ping hasta la dirección 8.8.8.8 indicada.

Luego podemos deducir que dicho equipo está conectado.

De hecho, dicha dirección IP corresponde al servidor dns de google.es

El comando ping admite también indicar dirección DNS en vez de direcciones IP.

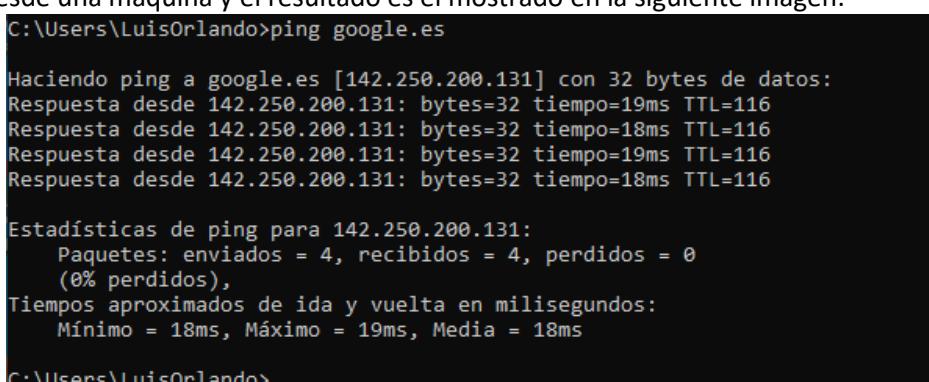
Su sintaxis sería similar a las direcciones IP:

```
ping <dirección DNS>
```

Por ejemplo, podemos encontrar el siguiente comando:

```
#ping Google.es
```

Lo lanzamos desde una máquina y el resultado es el mostrado en la siguiente imagen:



```
C:\Users\LuisOrlando>ping google.es

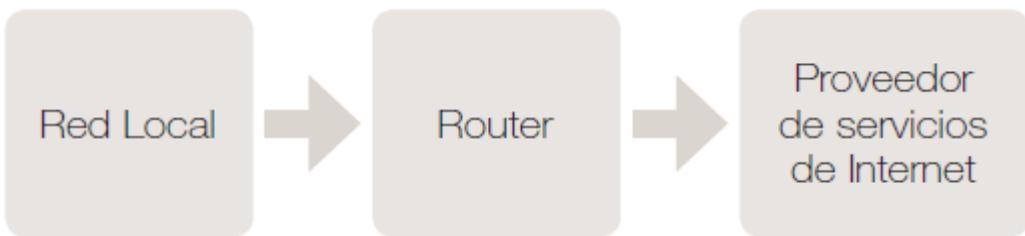
Haciendo ping a google.es [142.250.200.131] con 32 bytes de datos:
Respuesta desde 142.250.200.131: bytes=32 tiempo=19ms TTL=116
Respuesta desde 142.250.200.131: bytes=32 tiempo=18ms TTL=116
Respuesta desde 142.250.200.131: bytes=32 tiempo=19ms TTL=116
Respuesta desde 142.250.200.131: bytes=32 tiempo=18ms TTL=116

Estadísticas de ping para 142.250.200.131:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
                (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
                Mínimo = 18ms, Máximo = 19ms, Media = 18ms

C:\Users\LuisOrlando>
```

Vemos, al igual que en el ejemplo anterior, que devuelve valores finitos. Luego se deduce que dicho equipo está conectado en red.

Problemas de Fibra/ADSL y Router



Muchos de los errores de acceso Internet se deben al cable telefónico que trae la señal ADSL desde el servidor. También el propio Router suele generar muchos problemas.

Si el Router no puede sincronizar con la línea, la luz indicadora de Conexión parpadea lentamente o está apagada.

Si después de haber reiniciado el Router, no podemos sincronizar con el servidor, posiblemente el fallo esté en el cableado que trae la señal.

Si tenemos sincronización con el servidor, pero Internet no funciona, podemos restaurar la configuración completa del Router con los parámetros de originales de fábrica.

Si tras restaurar el Router a sus valores originales, las cosas siguen igual, podría ser debido a un problema de enrutado en la infraestructura del operador, algo sobre lo que no podemos actuar nosotros mismos.

Primeras Verificaciones:

Para averiguar dónde está el problema, en casi todos los casos tenemos que verificar si el problema es:

- ⇒ Interno, de la configuración de nuestro equipo o del propio interfaz de red
- ⇒ De nuestra red Local, puede ser de la configuración de la red o de los elementos hardware internos de la misma: cable, switch, router...
- ⇒ De nuestro proveedor de servicios, puede ser de una mala configuración de nuestro equipo o de la configuración del propio hardware del ISP: router...

Lo primero que debemos comprobar es si funciona nuestra tarjeta de red, luego nuestra red Local, una vez comprobado todo esto, comprobamos si funciona nuestra red WAN.

Usando los comandos:

- Usando ipconfig, vemos nuestra configuración de red
- Hacemos ping a nuestra IP, por ejemplo: ping 192.168.1.44
- Hacemos ping desde la red local a un equipo de la red, por ejemplo: ping 192.168.1.70
- Hacemos ping al router: ping 192.168.1
- Hacemos ping a una URL conocida y fiable: ping google.es
- Y si no funciona hacemos un ping a una ip pública conocida: ping 8.8.8.8

Si falla en alguno de estos pasos ya tendremos una pista de dónde está el problema para solucionarlo.

Errores en la conexión Wi-Fi

Si el equipo ha dejado de conectarse a la red Wi-Fi y no hay forma de que recupere la conexión, puede haber diversas causas.



En primer lugar reiniciamos el equipo y el Router Wi-Fi. Esto suele resolver el problema en el 80% de los casos, ya que una vez hecho esto, se suele solucionar y todo vuelve a funcionar correctamente otra vez.

En caso de que siga habiendo problemas, deberíamos asegurarnos de que esté activada la señal Wi-Fi en el Router (cada fabricante es diferente pero lo normal es mediante un interruptor, una combinación de teclas o un software instalado en el equipo).

Después hemos de pinchar sobre el icono de la barra de tareas en forma de escala de señal, para ver la lista con las redes Wi-Fi detectadas.

Ahora debemos comprobar que nuestra red aparece en la lista de redes Wi-Fi disponibles. En caso de que aparezca, intentaremos conectarnos a ella. Si tampoco hay conexión, tendremos que asegurarnos de que la clave de seguridad que hemos introducido es correcta (muchos errores de conectividad se derivan de errores en las claves).

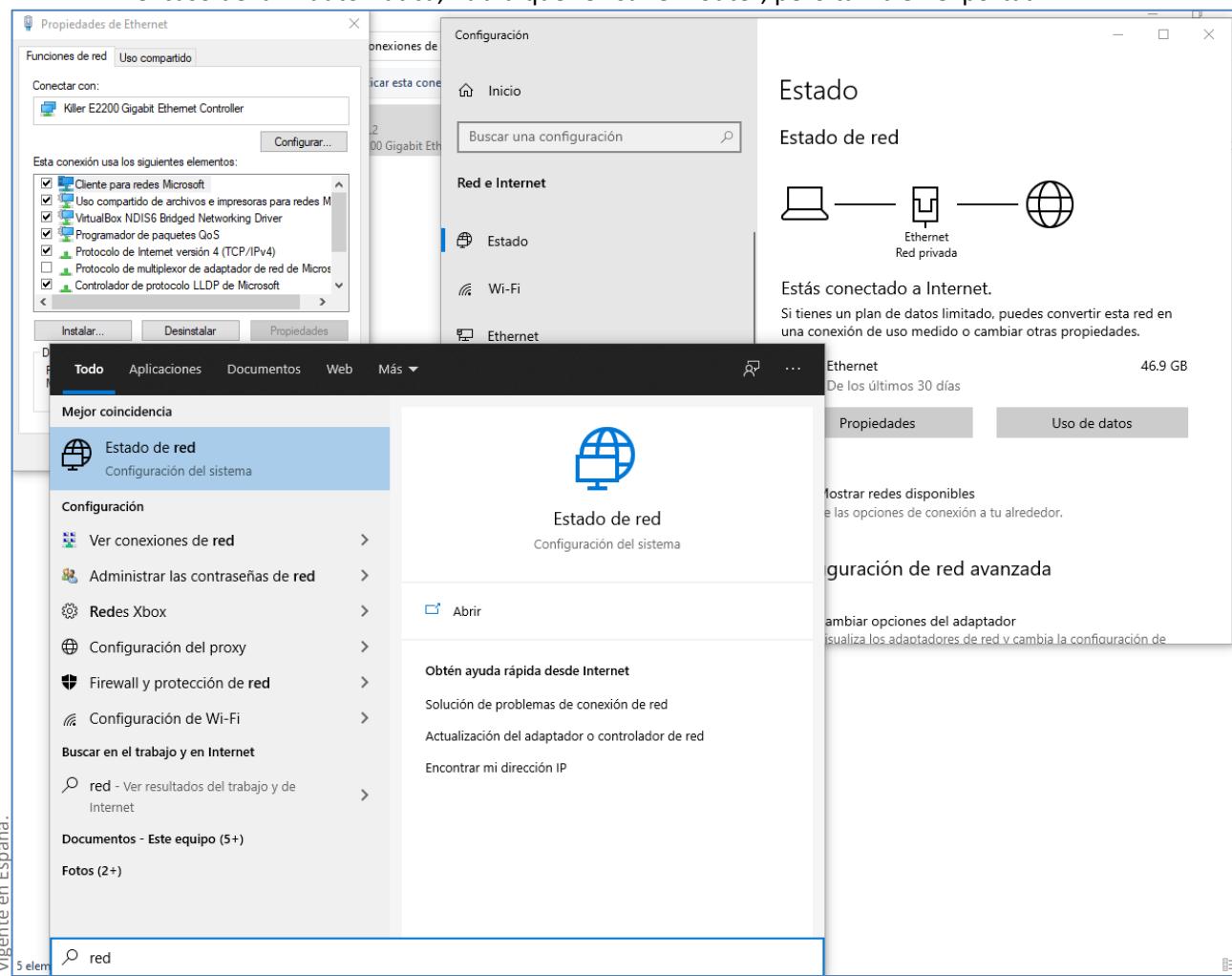
Si la red no aparece entre las redes disponibles o si aparece, no podemos conectar, habrá que revisar el punto de acceso.

También puede pasar que a pesar de tener conectado el equipo al Router Wi-Fi, no hay de tráfico entre el ordenador y la red. Esto se puede deber a muchas razones. Como hemos dicho con anterioridad, lo primero va a ser siempre reiniciar el equipo y el Router Wi-Fi.

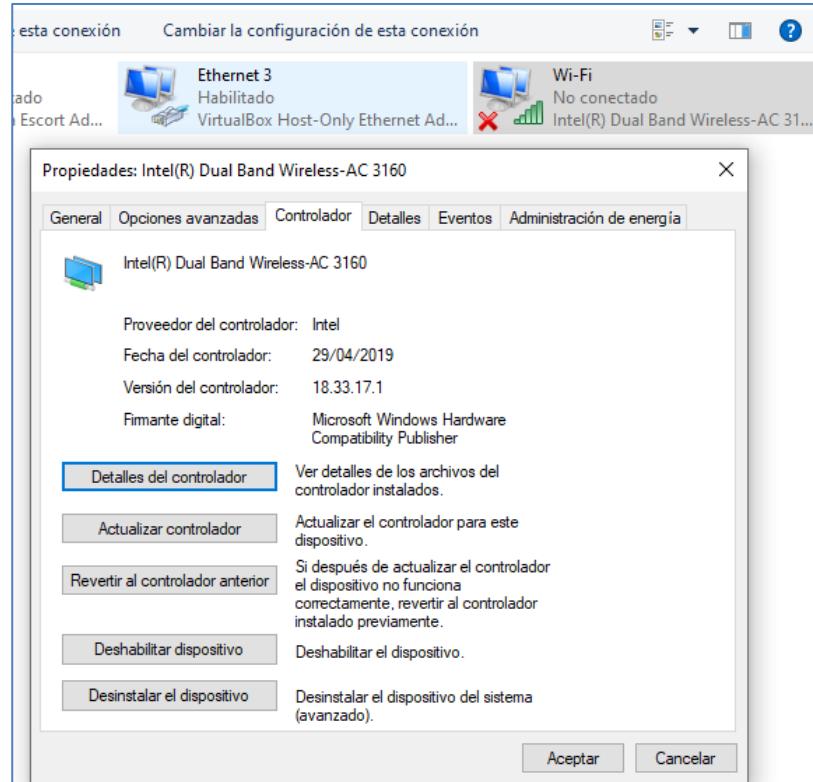
Si tras haber reiniciado, seguimos con problemas, habrá que comprobar que el Router está asignando la dirección IP correctamente.

Para ello:

- ⇒ Buscaremos el texto:
 - Red (y nos saldría **estado de red**) configuración Windows 10
 - Si buscamos conexiones (Ver conexiones de red) configuración Windows 7
- ⇒ Y luego iremos a Centro de redes y recursos compartidos
- ⇒ Conexión de red inalámbrica, lo que nos mostrará los detalles del adaptador.
- ⇒ Detalles podremos ver si se nos está asignando una IP automática por DHCP o es automática.
- ⇒ En el caso de la IP automática, habrá que revisar el Router, pero también el portátil.

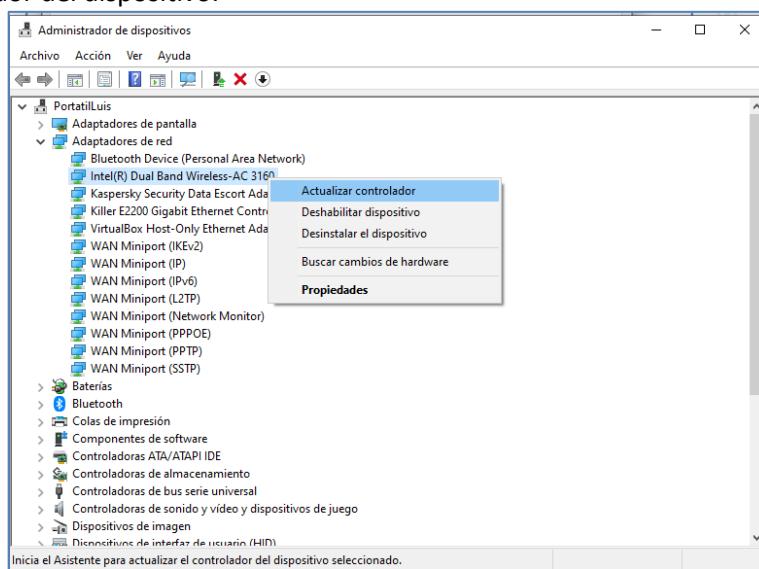


También podemos optar por buscar la última actualización disponible para el controlador de la tarjeta Wi-Fi.

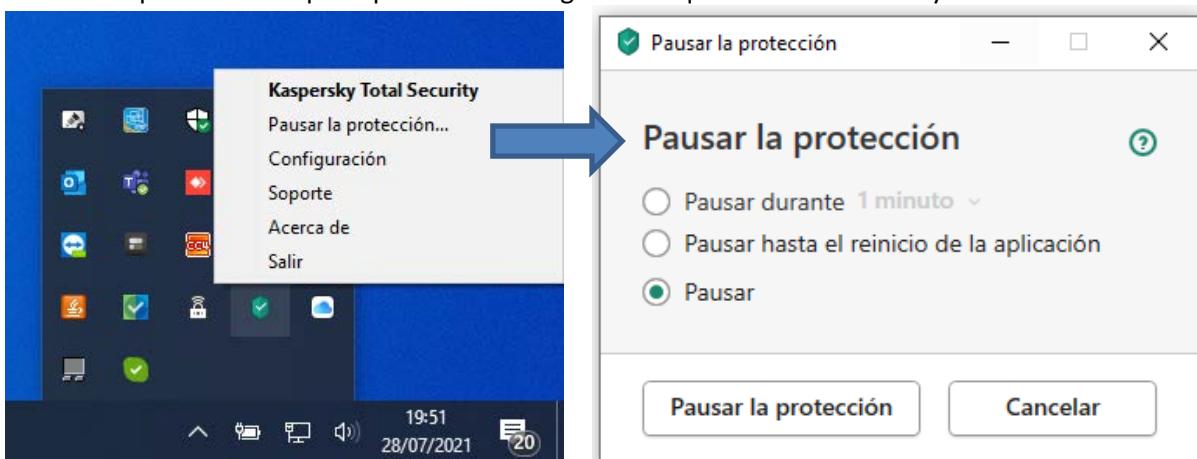


Para poder ver los elementos hardware del equipo, incluido el adaptador Wi-Fi, hemos de acceder al administrador de dispositivos de Windows. Para ello, debemos pulsar la combinación de la Tecla de Windows y la Tecla Pausa. Ello nos dará acceso a la opción propiedades del sistema. Dentro de esta ventana, debemos pinchar sobre la opción Administrador de dispositivos.

Aquí aparecerán todos los elementos hardware del equipo. En la categoría adaptadores de Red, debe aparecer el adaptador Wi-Fi. Deber doble clic sobre él, se debe mostrar una ventana en la que aparecerán se mostrarán todos los detalles del dispositivo. Accedemos a la pestaña controlador y ahí podremos actualizar el controlador del dispositivo.



Si tenemos instalado algún software de seguridad instalado (antivirus, cortafuegos, etc.), sería bueno desactivarlo temporalmente para averiguar si causante del problema fuese puede ser este. Hay que tener en cuenta que la función principal del cortafuegos es bloquear accesos desde y hacia la red.



Router Wi-Fi

En lo referente a los Router Wi-Fi, hay muchos tipos de ellos atendiendo a factores como:

- ⇒ Estándares Wi-Fi: 802.11b/g/a/n
- ⇒ Seguridad: WEP, WPA o WPA2

Frecuencias de trabajo: entre 2,4 y 5 GHz

A esto hay que añadir las propias tecnologías de algunos fabricantes que cada uno ha desarrollado con la idea de acelerar y mejorar la transmisión de datos.

Una de las primeras cuestiones de debemos hacer si el Router Wi-Fi falla es actualizar su firmware a la última versión disponible en la web del fabricante.

Una vez hecho eso, lo más prudente sería, reiniciar el Router Wi-Fi y a continuación restablecer la configuración de fábrica del Router. Ahora podríamos ir modificando ciertos parámetros empezando por lo más sencillo y después configurando lo más complejo.

Podríamos desactivar la seguridad, ajustamos la banda en 2,4 GHz y seleccionamos el estándar más antiguo (802.11b u 802.11g). Esta sería la configuración más básica, menos problemática, pero también la menos eficiente.

Si todo funciona, ahora podríamos empezar aumentando la seguridad a WEP y después a WPA, también iremos cambiando la banda de emisión y después el estándar de transmisión.

Interferencias inalámbricas

Los problemas también pueden deberse a interferencias que dificulten la comunicación inalámbrica entre el equipo y el Router. Hay teléfonos inalámbricos DECT que funcionan en la banda de 2,4 GHz, en el área de cobertura demasiadas redes Wi-Fi, que operen en el mismo canal o incluso puede haber en zonas próximas a edificios sensibles inhibidores de señal.

Para solucionar esto, podemos cambiar el canal de emisión. También podemos cambiar el Router Wi-Fi e instalar otro que funcione a 5 GHz. Esta es una banda muy poco utilizada aún y seguro que apenas tendremos interferencias.

Los servidores DNS, muy importantes

Algunos problemas como la velocidad lenta, los derivados de la propia dificultad de acceder a Internet o el no poder acceder a determinadas direcciones, pueden estar causados por la configuración de los servidores DNS que tenemos en la configuración de red.

Los operadores de Internet cuentan con sus propios servidores DNS que, en muchos casos, pueden estar sobrecargados, caídos o no ser de mucha calidad. Esto provoca malos funcionamientos.

A veces es necesario cambiar la configuración de los servidores DNS que asigna por defecto el Router. Esto puede mejorar la conexión y sobre todo la velocidad a la hora de acceder a muchas páginas.

Más a delante trataremos el problema de los servidores DNS en profundidad. Decir ahora que servidores DNS como el de Google, OpenDNS o incluso los de Norton, además de gran disponibilidad, aportan seguridad a la conexión al bloquear el acceso a páginas malware o phishing.

4.10. Normativa ambiental y estándares de señalización y digitalización

Los dispositivos de interconexión, como todo elemento electrónico, deben cumplir una serie de requerimientos del entorno ambiental con objeto de garantizar su buen funcionamiento.

Estos requerimientos pueden clasificarse en base a dos parámetros:

- Emplazamiento.
- Condiciones del entorno.

En cuanto a las condiciones del emplazamiento, se deben cumplir al menos como mínimo los siguientes requisitos:

- Los equipos deben estar siempre en lugares accesibles para su mantenimiento.
- Deben estar alejados de zona de interferencias eléctricas, de inundación, de humedades, etc.
- Lejos de materiales peligrosos o inflamables.

En cuanto a las condiciones de entorno se deben cumplir al menos los siguientes requisitos:

- Temperatura entre -10º y 40º.
- Humedad relativa entre 30% y 55%.
- Renovación del aire al menos 2 veces/hora.
- Alejado de ruidos impulsivos.
- Alejados de maquinarias vibratorias y mecánicas.

Los fabricantes, en su hoja de características de los dispositivos, indican el rango de funcionamiento en el cual garantiza el correcto funcionamiento del equipo.

Es por ello que es recomendable seguir dichas indicaciones para evitar fallos en los dispositivos de interconexión.

En cuanto a los estándares de señalización y codificación hay muchos a lo largo de la historia de las comunicaciones.

Entre todas ellas destacan al menos la siguientes:

Señalización SS7

Es el estándar de señalización por canal común empleado habitualmente en la red telefónica comutada (RTC).

Fue desarrollada en 1975 por AT&T y estandarizada en 1981.

Señalización H.323

Se trata de un estándar para señalización en VoIP que permite en envío además de otros servicios como videotelefonía, streaming de vídeo, etc.

La señalización SS7 ha sido la más ampliamente utilizada en las redes telefónicas.

A continuación describimos con más detalle su funcionamiento.

La señalización SS7 constituye uno de los protocolos más utilizados al ser el estándar de las redes RTC.

En una red de señalización SS7 se definen dos tipos de componentes:

- Punto de señalización SP.
- Enlace de señalización SL.

Una central digital que use SS7 se conoce como SP y dentro del sistema SS7 se le asigna un número de identificación único conocido como Código del Punto de Señalización SPC (Signalling Point Code).

El camino digital para transferir señales SS7 entre SP's se llama Enlace de Señalización o SL. En la red física esto corresponde a un intervalo de tiempo de la trama PCM (IT16) dedicado, uno en cada dirección de un enlace PCM. La configuración del enlace SS7 lo completa un Terminal de Señalización ST (Signalling Terminal) en cada extremo del enlace.

Los mensajes de señalización están empaquetados en un formato llamado Unidad de Señalización de Mensajes o MSU (Message Signal Unit).

Por razones de confiabilidad y capacidad es necesario tener más de un enlace de señalización o SL entre dos puntos de señalización (SP's) adyacentes. Cuando hay varios SL's en paralelo se denominan Set de Enlaces o LS (Link Set).

A nivel mundial la red de señalización está estructurada en 2 niveles funcionales independientes: el nivel nacional y el nivel internacional.

Esto facilita una clara distribución de la responsabilidad respecto a la señalización en los aspectos de la gestión de red. También permite que los planes de numeración para los SP's en la red internacional y en las diferentes redes nacionales sean independientes entre sí.

En SS7 se definen los puntos de señalización adyacentes como los dos puntos de señalización que están directamente interconectados mediante un enlace de señalización.

En base a lo anterior se distinguen los siguientes tipos de puntos de señalización:

–Punto origen: donde se origina el mensaje.

–Punto destino: donde finaliza el mensaje.

–STP (Punto de Transferencia de Señalización): punto de señalización en el que ni se origina ni termina el mensaje. Recibe un mensaje y lo dirige en forma transparente a otro enlace.

–Rutas de señalización: es el itinerario de SP's y enlaces de señalización interconectados, que toma el mensaje para llegar desde el punto de origen al punto de destino.

–Modos de señalización: es la asociación que hay entre la ruta tomada por el mensaje de señalización y la ruta que toman los canales de voz señalizados (o datos, etc.). Hay tres modos:

›Asociado: mensaje y voz (datos) llevan la misma ruta.

›Cuasi asociado: los mensajes de señalización siguen la misma ruta de la voz (datos) en algunos tramos, separándose en otros.

›Disociado: los mensajes de señalización y el tráfico de voz llevan caminos diferentes en todos los tramos.

Las principales características que hicieron la señalización SS7 como las más empleadas fueron las siguientes:

–Alta flexibilidad, para ser utilizado en distintos servicios de telecomunicaciones.

–Alta capacidad, solo un enlace de señalización soporta cientos de troncales.

–Alta velocidad, solo toma un segundo establecer una llamada a través de varias centrales.

–Alta confiabilidad, contiene una potente funcionalidad para la eliminación de problemas en la red de señalización.

–Economía, puede ser usado por un amplio rango de servicios de telecomunicaciones.

–Requiere de menos hardware que los sistemas anteriores.

Esta señalización es la señalización estándar de las redes RTC.

La aparición de la VoIP ha hecho que hayan surgido otros protocolos y normativas de señalización que serán diferentes a la SS7 pero que en esencia mantiene los mismos objetivos.

5. Equipos de conmutación telefónica. «Call Managers»

5.1. Equipos de conmutación telefónica. «Call managers»

Una central telefónica es un conjunto de equipos que permite la conmutación de diferentes canales telefónicos con objeto de hacer eficiente la infraestructura telefónica.

La conmutación telefónica ha evolucionado a lo largo del tiempo pasando de ser equipos donde la conmutación se realizaba de forma manual (a través de un operador) a ser realizados en la actualidad de forma automática.

La irrupción de la VoIP ha hecho también evolucionar las centrales telefónicas pasando de ser equipos de conmutación de líneas analógicas a equipos de conmutación de paquetes de datos.

En la jerga de la conmutación a las centrales de conmutación manuales se les denomina PBX (Private Branch Exchange) aunque actualmente ya solo se instalan PABX (Private Automatic Branch Exchange), es decir, las centrales de conmutación automática.

Se denomina privado porque el dispositivo suele ser propiedad del cliente (está en la ubicación del cliente) aunque existen modalidades de alquiler, leasing, renting, etc. En cualquier caso, se trata de un dispositivo gestionado por el cliente y no por el operador.

Las PABX actúan como una central de conmutación de un operador, de forma que todos los usuarios conectados a ella se conectan a través del dispositivo PABX que enruta el canal sin necesidad de usar enlace exterior del operador (esta es la razón por la que las llamadas internas son gratuitas).

En cambio si el canal no pertenece a la PABX, entonces saldrá por una línea exterior del operador y se tarificará según la tarifa contratada.

Una central telefónica o Call Manager o también llamados PBX o PABX son dispositivos de conmutación que permiten cursar varias comunicaciones a la vez por las mismas infraestructuras mejorando así su eficiencia y rendimiento.

Es por ello que en una PABX se definen:

Comunicaciones o llamadas internas

Son aquellas en las que se conectan entre los usuarios de una misma empresa u organización conectados a la misma PABX, por lo que no precisa de salida al exterior (del operador).

Estas comunicaciones no tienen coste.

Comunicaciones o llamadas externas

Son aquellas en las que se conectan los usuarios con una extensión no perteneciente a la PABX, y es por ello que sale al exterior usando una línea del operador contratado.

Estas comunicaciones tienen coste según la tarifa contratada.

Las PABX han sufrido una rápida evolución en cuanto a prestaciones y automatización de las mismas, pasando de ser analógicas a ser semi-digitales y luego totalmente digitales.

Actualmente han surgido las PABX IP, herramientas software que se instalan sobre un ordenador convencional y que realizan las funciones de centralitas para teléfonos IP. Es lo que se conoce como un sistema VoIP.

Estas centrales PABX se han convertido por razones de coste en un dispositivo ampliamente empleado en oficinas, empresas y grandes organizaciones. Sobre todo la PABX IP ha hecho aún más esta consolidación irrumpiendo fuertemente en el mercado por sus bajos costes.

A continuación vamos a ver diferentes implementaciones comerciales de PABX tanto analógicas, como digitales y como PABX IP analizando sus prestaciones y funcionalidades más significativas.

Central telefónica PABX analógica KX-TEA308 de Panasonic

Se trata de una central telefónica PABX analógica para 8 terminales y con 3 líneas de teléfonos.

Se emplea habitualmente para pequeñas oficinas y pymes (hasta 8 teléfonos).

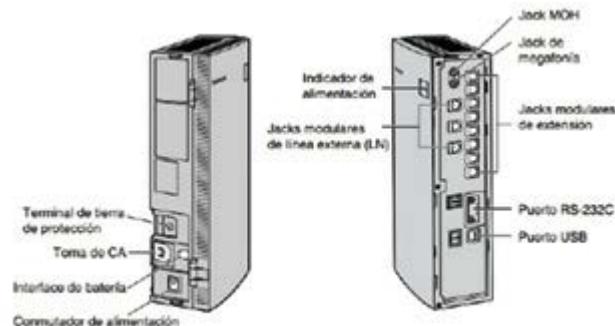


En la siguiente figura podemos ver el dispositivo.

A continuación mostramos sus características y funcionalidades más destacadas:

- Permite conectar hasta 8 teléfonos analógicos convencionales con conectores RJ-11.
- 3 líneas telefónicas de salida con conector RJ-11.
- Incorpora funciones de:
 - Llamada en espera.
 - Llamada de conferencia.
 - Rellamada.
 - Bloqueo de llamadas.
 - Fax automático.
 - Música en espera.

En la siguiente imagen pueden verse los conectores y LEDs que ofrece el PABX.



A continuación describimos los conectores de que dispone:

- 8 conectores para extensiones RJ-11.
- 3 conectores para líneas externas RJ-11.
- Conector para megafonía tipo jack.
- Conector para música en espera tipo jack.
- Puerto RS-232C para configuración.
- Puerto USB para configuración.
- Conector para alimentación.
- LED de encendido.
- Led de batería.

Central OmniPCX Office Compact de Alcatel

Se trata de una central telefónica PABX analógica para 4 terminales y con 3 líneas de teléfonos.

Se emplea habitualmente para pequeñas oficinas y pymes (hasta 4 teléfonos).



En la siguiente figura podemos ver el dispositivo.

A continuación mostramos sus características y funcionalidades más destacadas:

- Permite conectividad de hasta 24 teléfonos analógicos convencionales con conectores RJ-11.
- 2 líneas telefónicas de salida con conector RJ-11.
- Incorpora funciones de:
 - Llamada en espera.
 - Llamada de conferencia.
 - Rellamada.
 - Bloque de llamadas.
 - Fax automático.
- Interfaz web de configuración.

IP PABX modelo UCM6108 de Grandstream

Se trata de una central telefónica PABX IP con 8 terminales FXO y 2 terminales RJ-11 para líneas exteriores.

Se emplea habitualmente para oficinas pequeñas y medianas al permitir hasta 50 cuentas SIP.



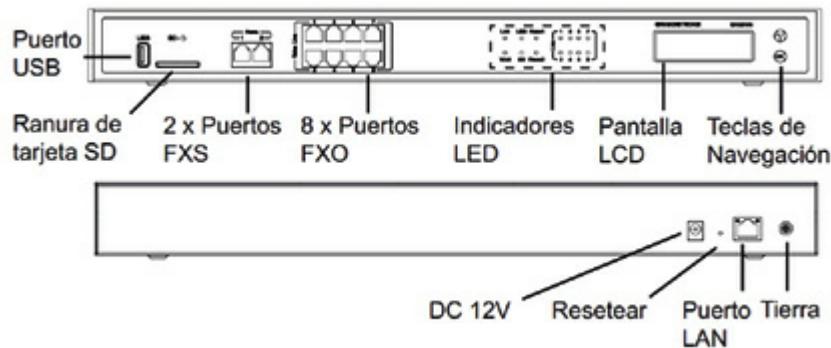
En la siguiente figura podemos ver el dispositivo.

Describimos a continuación los conectores de los que dispone:

- 8 conectores FXO.
- 2 conectores RJ-11 para líneas telefónicas convencionales externas.
- 1 puerto USB 2.0 para configuración.
- 1 puerto RJ-45 con PoE.
- LEDs de indicación de actividad.
- Display de información.

Todos los Call Manager suelen incluir una interfaz web que permite su configuración desde cualquier terminal telefónico o cualquier punto de la red de datos.

En la siguiente figura vemos estos conectores:



A continuación mostramos sus características y funcionalidades más destacadas:

- Permite 50 conversaciones SIP simultáneas y 32 en conferencia.
- Configuración mediante interfaz web.
- Alimentación mediante conector RJ-45 PoE.
- Router NAT integrado.
- Configurables diferentes parámetros de QoS.
- Soporta códecs G.711 Ley a/μ, G.722, G.723, 1, G.726, G.729 (audios) y H.264, H.263 (vídeos) y T.38 (Fax).
- Permite grabación de llamadas.
- Detección automática de teléfonos IP, ATA y teléfonos con vídeos.

La rápida implantación de la VoIP está haciendo migrar todos los PABX a IPPABX, donde ahora son aplicaciones que corren sobre un PC y que realizan todas las funciones de un Call Manager. Destacan entre ellos Call Manager IP de Cisco y Asterisk, este último de libre distribución.

IP PABX modelo UCM6116 de Grandstream

Se trata de una central telefónica PABX IP con 16 terminales FXO y 2 terminales RJ-11 para líneas exteriores.

Se emplea habitualmente para oficinas pequeñas y medianas al permitir hasta 60 cuentas SIP.

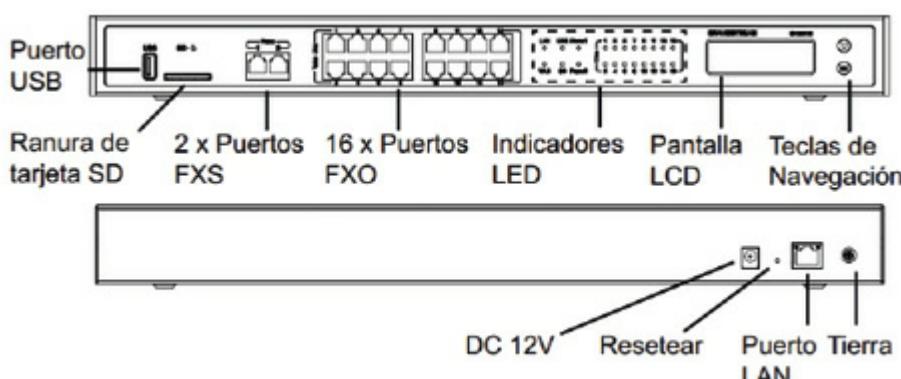


En la siguiente figura podemos ver el dispositivo.

Describimos a continuación los conectores de los que dispone:

- 16 conectores FXO.
- 2 conectores RJ-11 para líneas telefónicas convencionales externas.
- 1 puerto USB 2.0 para configuración.
- 1 puerto RJ-45 con PoE.
- LEDs de indicación de actividad.
- Display de información.

En la siguiente figura vemos estos conectores:



A continuación mostramos sus características y funcionalidades más destacadas:

- Permite 60 conversaciones SIP simultáneas y 32 en conferencia.
- Configuración mediante interfaz web.
- Alimentación mediante conector RJ-45 PoE.
- Router NAT integrado.
- Configurables diferentes parámetros de QoS.
- Soporta códecs G.711 Ley a/μ, G.722, G.723, 1, G.726, G.729 (audios) y H.264, H.263 (vídeos) y T.38 (Fax).
- Permite grabación de llamadas.
- Detección automática de teléfonos IP, ATA y teléfonos con vídeos.
- Una central telefónica o Call Manager es un dispositivo capaz de realizar la conmutación de canales de voz bien de forma manual o automática aumentando la eficiencia de la infraestructura.

- Las Call Manager pueden ser manuales (PAX cada vez más en desuso) o automáticas (PABX). También están aquellas que se implementan mediante una aplicación software (cada vez más extendidas) denominándose IPPABX.
- Existen numerosos fabricantes de Call Managers, destacando entre otros Panasonic, GrandStream, Alcatel-Lucent y Siemens.
- Todas las Call Manager suelen incluir los conectores RJ-11 (para la conectividad con el operador), RJ-45 (para la conectividad con la red de datos), USB, RS-232 (conector de consola), etc. Además suelen ser gestionables vía web.
- Además, la gran mayoría suele incorporar ya actualmente la tecnología PoE que le permite alimentarse por el cable de datos.

6. Mercado de las telecomunicaciones

6.1. Situación de las telecomunicaciones. Marco legal y organismos de normalización

El mercado de las telecomunicaciones ha registrado en los últimos años notables recortes debido a la actual coyuntura económica que también afecta al hipersector de las telecomunicaciones.

Según el informe de la CMT del año 2012 sobre el sector de las telecomunicaciones:

“El último año 2012 fue un año de recesión y de ajustes severos en la Unión Europea (UE). La zona euro registró un crecimiento negativo del 0,5% y la actividad fue desacelerándose a medida que avanzó el año. Las mayores tasas de decrecimiento del producto interior bruto (PIB) se dieron en el sur de Europa, donde los gobiernos aplicaron ajustes fiscales drásticos, una política de saneamiento del sistema bancario y medidas estructurales para mejorar la competitividad de las economías de sus respectivos países. A pesar de que en 2012 se otorgara mayor liquidez al sistema bancario, disminuyó el volumen de créditos concedidos al sector privado.

En España el ejercicio resultó especialmente difícil. La caída del PIB en términos reales fue del 1,4%. La formación bruta de capital disminuyó el 9,2%, el consumo privado también se redujo el 1,4% y el consumo público lo hizo aún en mayor proporción (el 3,7%), como consecuencia del fuerte ajuste fiscal. El único componente positivo de la demanda vino del exterior, debido al aumento de las exportaciones, que junto al descenso en la demanda de bienes extranjeros mejoró la balanza comercial.

Para 2013 se prevén reducciones importantes en la actividad de las economías del sur de Europa y para 2014 se espera un cambio de tendencia con tasas pequeñas pero positivas de crecimiento.”

Todo esto ha afectado notablemente tanto al hipersector de las telecomunicaciones como al resto de los sectores.

La normativa existente en el sector de las telecomunicaciones es amplia en función del tipo de servicio o dispositivo del que hablamos.

En general, existen una serie de normas que con carácter básico regulan a todo el sector.

Entre ellos destacan:

–Ley General de Telecomunicaciones (LGTEL) del año 2003 (Ley 32/2003, de 3 de noviembre).

–Real Decreto 899/2009, de 22 de mayo, por el que se aprueba la carta de derechos del usuario de los servicios de comunicaciones electrónicas.

–Real Decreto 346/2001, de 11 de marzo, por el que se aprueba el Reglamento regulador de las infraestructuras comunes de telecomunicaciones para el acceso a los servicios de telecomunicaciones en el interior de las edificaciones.

Estas leyes están normalizadas y supervisadas por una serie de organismos oficiales encargados de su regulación.

Entre ellos destacamos los siguientes:

Comisión Nacional del Mercado de la Competencia (CNMC)

Es el nuevo superorganismo de regulación que incluye la antigua CMT (Comisión del Mercado de la Telecomunicaciones).

Tiene su sede en Madrid y entre sus funciones está la de regular y normalizar el sector de las telecomunicaciones en el entorno de operadores, suministradores, proveedores, etc.

Su dirección web es www.cnmc.es

Red.es

Entidad pública con sede en Madrid entre cuyas funciones está la supervisión de la red Internet fomentando su potencial, extensión en la sociedad e impulsando su desarrollo.

Su dirección web es www.red.es

Ametic

Organización privada que engloba a empresas de la electrónica, las tecnologías de la información, las telecomunicaciones y los contenidos digitales impulsando su normalización, extensión de la sociedad y defensa de sus intereses.

Su dirección web es www.ametic.es

El organismo actual que regula el sector de las telecomunicaciones está integrado en la CNMC. Es quien se encarga de la supervisión y normalización del sector tanto para operadores, proveedores, distribuidores, etc.

6.2. Principales servicios de telecomunicaciones

Son muchos los servicios de telecomunicaciones existentes actualmente en el mercado y demandados por la sociedad.

Estos servicios de telecomunicación vienen englobados en una primera clasificación que sería la siguiente:

- Servicio de telefonía.
- Servicio de televisión.
- Servicio de datos.
- Servicios de geolocalización.

Cada uno de estos servicios a su vez incluye toda una serie de modalidades que se describen a continuación.

Servicio de telefonía

Por el servicio de telefonía se entiende como el conjunto de infraestructuras y capacidades técnicas que permite la transmisión en tiempo real o en diferido de una conversación de voz entre un punto a otro.

Junto a esta conversación de voz existen lo que se denominan servicios de valor añadido como videotelefonía, llamadas a tres, llamadas en espera, etc.

Este servicio de telefonía es implementado en el actual mercado de las telecomunicaciones de diversas formas:

Red telefónica conmutada (RTC)

Se trata de la tradicional red telefónica fija analógica (actualmente digitalizada) en la que empleando la red capilarizada de cobre (actualmente cada vez más con fibra óptica) se proporciona el servicio telefónico fijo. Ha sido el servicio de telecomunicaciones por excelencia desde sus inicios en el siglo XIX con Graham Bell. Esta red está basada en un conjunto de nodos de conmutación que permiten maximizar las infraestructuras haciendo llegar el servicio hasta los puntos de terminación de red (las comunes PTR o rosetas) en el interior de los hogares, oficinas o locales.

Red Digital de Servicios Integrados (RDSI)

Surgió como una red digital que pretendía integrar un conjunto de servicios, incluido el servicio telefónico, empleando canales digitales (denominados primarios) que proporcionaban mayores velocidades y numerosos servicios de valor añadido.

No tuvo gran éxito debido a que fue eclipsada por nuevos servicios emergentes como el ADSL.

Redes de telefonía móvil

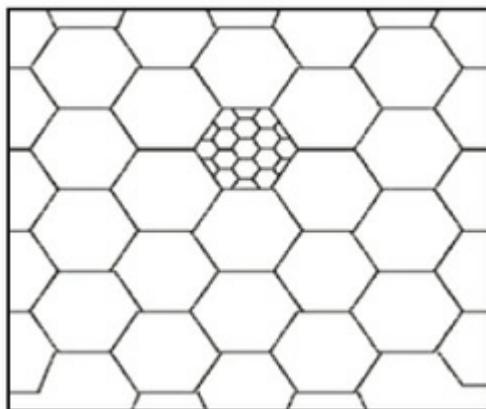
En las últimas décadas la telefonía ha sufrido una gran revolución con la aparición y estandarización de la denominada telefonía móvil, que permitía el servicio telefónico pero ahora en movilidad, es decir, el usuario no tiene por qué 'estar pegado' a un terminal fijo, sino que disponía de un terminal móvil con el servicio telefónico.

Aunque en sus inicios fue una tecnología analógica (Moviline) pronto se digitalizó convirtiéndose en una red móvil digital (GSM) que evolucionó rápidamente añadiendo nuevos servicios como red de datos.

Aparecieron así las diferentes tecnologías que se muestran en la siguiente tabla.

GENERACIÓN	TECNOLOGÍA
1G	Tecnología TACS (comercialmente Moviline)
2G	Tecnología GSM
2.5G	Tecnología GPRS y EDGE Aparición de protocolo WAP
3G	Tecnología UMTS
4G	Tecnología HSDPA y HSUPA

La infraestructura de la telefonía se basa en una estructura celular de forma hexagonal.



VoIP

La VoIP se denomina como el servicio telefónico que emplea como infraestructuras las redes IP, es decir, Internet.

Ahora la voz se digitaliza y se paquetiza en paquetes IP que se transmiten por una red de datos como es Internet y con los terminales adecuados (teléfonos IP o softphone) permiten el servicio telefónico entre dos puntos.

Es el futuro de la telefonía, que pasa a dejar de usar una red propia para convertirse en un servicio más de una red de servicios integrados.

Servicio de televisión

Por servicio de televisión se entiende el conjunto de infraestructuras y capacidades técnicas que permiten la transmisión de audio y vídeo en tiempo real de un punto a otro.

La televisión, desde sus inicios, ha supuesto una gran revolución en sector de las comunicaciones al ser un servicio de comunicación de masas.

El servicio de televisión, aun siendo un servicio bastante conservador, ha sufrido también un gran evolución (sobre todos en los últimos años con la TDT), aumentando sus prestaciones de calidad, de oferta televisiva, etc.

A continuación se muestra la evolución de la televisión de los últimos años:

Televisión analógica terrestre

Consistía en la distribución del servicio de televisión empleando transmisores y reemisores analógicos terrestres (y receptores de televisión analógicos). El servicio se distribuía en los canales de las frecuencias VHF y UHF (sobre todo este último).

Era un servicio con una calidad relativamente buena aunque presentaba numerosos problemas de interferencias, ruido, alta sensibilidad a las inclemencias meteorológicas, etc.

Televisión digital terrestre (TDT)

Consiste en la distribución del servicio de televisión de forma digital empleando transmisores y reemisores terrestres. Ahora los televisores deberán disponer de un receptor de TDT para poder decodificar la señal digital. Emplea canales de RF en la banda de UHF.

A nivel nacional se creó un mapa de canales de TDT de carácter nacional, autonómico y local (esto último por demarcaciones).

El servicio, a diferencia de la televisión analógica, era de mayor calidad, con una amplia oferta televisiva, más inmune al ruido e interferencias y optimiza enormemente el espectro radioeléctrico.

Permitía además incorporar servicios interactivos con la tecnología MHP.

Televisión sobre IP (TvIP)

La televisión sobre IP es un nuevo concepto de televisión en el cual dicho servicio se distribuye por redes IP, es decir, por Internet.

La flexibilidad de las redes IP permite agregar numerosos servicios de valor añadido como la televisión a la carta (VoD), streaming de vídeo, etc.

Con la televisión sobre IP se permite integrar en una única conectividad todos los servicios de telecomunicaciones (voz, datos, televisión) bajo un único acceso a Internet.

La exigencia de la televisión sobre IP exige gran ancho de banda y de caudal de la conexión para evitar retardos y cortes en un servicio con una calidad de servicio (QoS) crítico.

La televisión por Internet (TvIP) viene a ser la próxima gran revolución del sector audiovisual. La integración en el televisor de los nuevos servicios de datos es el próximo salto en el sector de las telecomunicaciones

Servicio de datos

Por servicio de datos se entiende el conjunto de infraestructuras y las capacidades técnicas que permiten la transmisión de información (audio, vídeo, archivos, etc) de un punto a otro.

Es el servicio de comunicación entendido en su versión más amplia.

Estos servicios de datos emplean infraestructuras de redes de comunicaciones, siendo el más utilizado Internet, ya que su ámbito es mundial.

Entre los servicios de datos más demandados por los usuarios destacamos:

- Servicio de navegación web.
- Correo electrónico.
- Servicio FTP.
- Servicio TELNET.
- Servicios de compartición de archivos o P2P.
- Chat.
- Servicio de Mensajería.
- Whatsapp.
- Juegos en red.
- Servicios de SMS y MMS.
- Servicio de videostreaming.
- Youtube.

6.3. Agentes en el mercado de las telecomunicaciones

En el hipersector de las telecomunicaciones, donde hay agentes que producen servicios y agentes que usan esos servicios, se definen una serie de agentes (además de los ya indicados) que actúan como intermediarios o distribuidores para que esos servicios lleguen desde los que los producen hasta aquellos que los consumen.

Así, en este hipersector de las telecomunicaciones distinguimos los siguientes agentes:

Fabricantes y suministradores.

Son aquellos agentes que planean, diseñan y fabrican productos de comunicaciones para ser consumidos bien como producto final o como producto intermedio.

Proveedores de servicios

Son los agentes que diseñan y ponen en funcionamiento servicios de comunicaciones destinados a un usuario final.

Suelen desarrollar servicios de comunicaciones en los cuales el agente proporciona la conectividad y el soporte para el uso del servicio.

Operadores

Son los agentes encargados de la distribución de los servicios de telecomunicaciones desde su origen hasta los usuarios finales que los consumen.

Los operadores se pueden clasificar en función de la infraestructura utilizada para la distribución de estos servicios.

Así encontramos:

- Operadores fijos.
- Operadores móviles.
- Operadores vía satélite.

También suelen coexistir diversos niveles de operadores (operadores de primer nivel o troncales, operadores de segundo nivel o distribuidores, etc.).

Usuarios

Son los agentes que consumen o usan los servicios y/o productos de comunicaciones.

Estos usuarios pueden ser empresas, organizaciones, administraciones públicas o particulares.

El mercado suele proporcionar diferentes productos y servicios para cada tipo de usuario en función de las necesidades de comunicaciones que precisa cada tipo de usuario.

6.3.1. Fabricantes y suministradores

Como ya se ha descrito anteriormente, son los agentes encargados de la planificación, diseño y fabricantes de productos de comunicaciones.

Estos productos pueden tener un destino final de consumo o servir como producto intermedio para otro producto como destino final.

En el mercado existen numerosos fabricantes y suministradores catalogados en función del producto que diseñan y fabrican.

En una primera clasificación (extensible por supuesto) encontramos:

Fabricantes de equipos de redes de comunicaciones

En ellos encontramos fabricantes que diseñan y fabrican productos como hub, switches, routers, gateways, etc.

Entre los principales fabricantes encontramos: Cisco, TP-Link, Netgear, Linksys, etc.

Fabricantes de cableados para comunicaciones

Son aquellos que fabrican componentes y sistemas de cableados para redes de comunicaciones.

Entre los principales fabricantes encontramos: Systimax, Nordix, 3M, Alcad, Televés, Ikusi, etc.

Fabricantes de terminales para telefonía móvil o fija

Son aquellos que diseñan y fabrican terminales para el servicio telefónico fijo o móvil.

Entre los principales fabricantes encontramos: Alcatel, Samsung, Nokia, ZTE, Panasonic, Sony, etc.

Fabricantes de receptores para el servicio de televisión

Son aquellos que diseñan y fabrican terminales para el servicio de televisión.

Entre los principales fabricantes encontramos: LG, Samsung, Panasonic, etc.

Fabricantes de componentes de equipos informáticos

Son aquellos que diseñan y fabrican componentes y equipamiento informático.

Entre los principales fabricantes encontramos: Asus, Logitech, Sony, HP, Olivetti, Acer.

Fabricantes de componentes electrónicos

Son aquellos que diseñan y fabrican componentes electrónicos de consumo. Muchos de ellos destinados a sistemas de comunicaciones.

Entre los principales fabricantes encontramos: TP-Link, GrandStream, General Electric, AT&T., etc.

6.3.2. Proveedores de servicio

Los proveedores de servicios son los agentes que diseñan y ponen en funcionamiento servicios de comunicaciones destinados a un usuario final que pueden ser empresas, organizaciones o particulares.

Suelen desarrollar servicios de comunicaciones en los cuales el agente proporciona la conectividad y el soporte para el uso del servicio.

Existen numerosos proveedores de servicios, pero destacan sobre todo los siguientes:

Proveedores de servicios de Internet (ISP)

Son empresas que proporcionan a sus usuarios el acceso a Internet.

Son muy numerosas en España y en el mundo y cada una de ellas ofrece diferentes tipos de conexiones y por supuesto tarifas.

Proveedores de Alojamiento Web y hosting

Son empresas que alquilan sus equipos hardware (almacenamiento de disco duro sobre todo) a terceros (empresas, organizaciones y particulares) a cambio de un coste económico.

Este alquiler supone que la información almacenada siempre va a estar disponible (desde cualquier punto del planeta), es confidencial y no se va a perder (incluyen copias de seguridad).

Además incluyen el hosting del correo electrónico de forma que la información de dichas cuentas también está asegurada con las copias de seguridad y disponible 24 horas, 365 días.

Proveedores de servicios hay muchos en España y en el mundo. Destacan entre otros los siguientes:

- Gmail: proveedor de hosting y de correo electrónico.
- Yahoo: proveedor de hosting y de correo electrónico.
- Ibercom: proveedor de internet (ISP), hosting y correo electrónico.
- Orange: proveedor de internet (ISP), hosting y correo electrónico.
- Movistar: proveedor de Internet (ISP), hosting y correo electrónico.
- Vodafone: proveedor de Internet (ISP), hosting y correo electrónico.

6.3.3. Operadores

Son los agentes encargados de la distribución de los servicios de telecomunicaciones desde su origen hasta los usuarios finales que lo consumen.

Los operadores se pueden clasificar en función de la infraestructura utilizada para la distribución de estos servicios.

Así encontramos:

- Operadores fijos.
- Operadores móviles.
- Operadores vía satélite.

También suelen coexistir diversos niveles de operadores (operadores de primer nivel o troncales, operadores de segundo nivel o distribuidores, etc.).

Entre los operadores nacionales más importantes y destacables citamos los siguientes:

Movistar

Operador global de telecomunicaciones con sede en España y fuerte presencia internacional, sobre todo en Sudamérica.

Ofrece y proporciona servicios de telefonía fija, telefonía móvil y servicio de datos como ISP.

Orange

Operador global de telecomunicaciones con sede en Francia y fuerte presencia internacional comercializándose en España bajo este nombre.

Ofrece y proporciona servicios de telefonía fija, telefonía móvil y servicio de datos como ISP.

Vodafone

Operador global de telecomunicaciones con sede en Reino Unido y fuerte presencia internacional, sobre todo en Europa.

En España en sus inicios se comercializó con el nombre de Airtel, aunque luego adquirió el nombre de su matriz Vodafone España.

Ofrece y proporciona servicios de telefonía fija, telefonía móvil y servicio de datos como ISP.

Yoigo

Operador global de telecomunicaciones con sede en Suecia con el nombre de Teliosonera y fuerte presencia internacional sobre todo en Europa.

En España en sus inicios se comercializó con el nombre de Xfera aunque luego adquirió el nombre de Yoigo Móviles.

Ofrece y proporciona servicios de telefonía fija, telefonía móvil y servicio de datos como ISP.

Los anteriores operadores son operadores troncales, es decir, disponen de infraestructuras propias para proporcionar los servicios descritos.

Existen además los operadores virtuales (los denominados OMV) que son operadores que alquilan las líneas a los anteriores operadores y los venden a sus clientes.

Dentro de estos operadores virtuales el número es mucho mayor, destacando entre ellos los siguientes:

- Eroski Móvil.
- Carrefour Móvil.

- Masmóvil.
- Lycamobile.
- Simyo.
- Pepephone.
- Happymóvil.
- Tuenti.
- Orbitel.
- Lebara móvil.

El sector de las OMV es bastante dinámico, produciéndose constantes fusiones y nuevas operadores en función de las necesidades del mercado.

Existen también los operadores de servicios vía SAT (por satélite).

Entre ellos encontramos o destacamos los siguientes:

SES Astra

Operador global de telecomunicaciones con sede en Luxemburgo que ofrece servicios de radio, televisión y datos vía satélite.

Dispone de una amplia oferta de ocio y entretenimiento en el mundo audiovisual.

Hispasat.

Operador global de telecomunicaciones con sede en España que ofrece servicios de radio, televisión y datos vía satélite.

Dispone también de una amplia oferta de ocio y entretenimiento en el mundo audiovisual.

Amazon

Operador global de telecomunicaciones con sede en Estados Unidos que ofrece una amplia variedad de servicios de radio, televisión y datos vía satélite.

Dispone también de una amplia oferta de ocio y entretenimiento en el mundo audiovisual.

6.3.4. Perfiles de las operadoras

Como ya se ha comentado anteriormente, los operadores son los agentes que se encargan de la distribución de los servicios de telecomunicaciones desde su creación en origen hasta su acceso final a los usuarios, empresas u organizaciones que la consumen.

Estas operadoras, en función del tipo de servicio que ofrecen se clasifican en:

- Operadores de servicio telefónico fijo.
- Operadores de servicio telefónico móvil.
- Operadores de servicios de televisión terrestre.
- Operadores de servicios de televisión vía satélite.
- Operadores de servicios de radio terrestre.
- Operadores de servicios de radio vía satélite.
- Operadores de servicios de datos vía cable.
- Operadores de servicios de datos vía inalámbricas.

No obstante, es habitual que existan operadores globales que ofrezcan a la vez y de forma simultánea servicios de voz, datos y televisión (servicios Triple Play) de forma cableada o incluso también de forma inalámbrica (Cuaduple play).

Esta tendencia hacia operadores globales facilita la integración y la eficiencia de costes por parte de los operadores.

6.3.5. Usuarios. Derechos de los usuarios de telecomunicaciones

Los usuarios de servicios de telecomunicaciones disponen de una serie de derechos y obligaciones como usuarios finales de cualquier tipo de producto o servicio.

En el hipersector de las telecomunicaciones se ha regulado lo que se denomina 'Carta de los derechos de los usuarios de telecomunicaciones', que recoge de manera particular aquellos derechos y obligaciones de los usuarios cuando emplean, usan o consumen productos o servicios de telecomunicación.

Estos usuarios finales de servicios de comunicaciones electrónicas serán titulares además de los derechos establecidos en el artículo 8 del texto refundido de la Ley General para la Defensa de los Consumidores y

Usuarios y otras leyes complementarias, aprobado por el Real Decreto Legislativo 1/2007, de 16 de noviembre:

- Derecho a obtener una conexión a la red telefónica pública desde una ubicación fija que posibilite el acceso funcional a Internet, y acceder a la prestación del servicio telefónico, así como al resto de prestaciones incluidas en el servicio universal, con independencia de su localización geográfica, a un precio asequible y con una calidad determinada.
- Derecho a celebrar contratos y a rescindirlos, así como a cambiar de operador de forma segura y rápida, con conservación del número telefónico. En particular, incluye el derecho a resolver el contrato anticipadamente, sin penalización, en supuestos de modificación del mismo por el operador por motivos válidos especificados en aquel y sin perjuicio de otras causas de resolución unilateral.
- Derecho a la información veraz, eficaz, suficiente, transparente y actualizada sobre las condiciones ofrecidas por los operadores y las garantías legales.
- Derecho a recibir servicios de comunicaciones electrónicas con garantías de calidad, así como a recibir información comparable, pertinente y actualizada sobre la calidad de los servicios de comunicaciones electrónicas disponibles al público.
- Derecho a la continuidad del servicio y a una indemnización en caso de interrupciones.
- Derecho a una facturación desglosada, a la desconexión de determinados servicios y a elegir el medio de pago de los servicios entre los comúnmente utilizados en el tráfico comercial.
- Derecho a una atención eficaz por el operador.
- Derecho a unas vías rápidas y eficaces para reclamar.
- Derecho a prestaciones especiales para personas con discapacidad y de renta baja.
- Derecho a una especial protección en la utilización de servicios de tarificación adicional.
- Derecho a la protección de los datos de carácter personal.

Asimismo, los usuarios finales de servicios de comunicaciones electrónicas tendrán derecho a celebrar contratos con los operadores y a recibir el servicio en las condiciones pactadas con ellos.

La formalización y entrega del contrato se regirán por lo dispuesto en el texto refundido de la Ley General para la Defensa de los Consumidores y Usuarios y otras leyes complementarias, aprobado por el Real Decreto Legislativo 1/2007, de 16 de noviembre, sin perjuicio de otras formalidades adicionales que, en su caso, se establezcan en la regulación de la portabilidad y la preselección.

Los operadores no podrán acceder a la línea de un usuario final sin su consentimiento expreso e inequívoco. En relación con el servicio de banda ancha para acceder a Internet, el operador no podrá aplicar al usuario final una oferta cuya velocidad máxima publicitada sea superior a la velocidad máxima que admite la tecnología utilizada sobre su bucle local o en el enlace de acceso.

El operador deberá informar al usuario final, antes de su contratación, de los factores relevantes que limitan la velocidad efectiva que puede experimentar el usuario, diferenciando aquellos sobre los que tiene control el operador de los ajenos al mismo.

A efectos de lo establecido en el párrafo anterior, mediante resolución de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, se podrá establecer el contenido mínimo y demás condiciones que los operadores deben cumplir al informar a los usuarios, con carácter previo a la contratación.

RESUMEN

1. Niveles funcionales de una red de comunicaciones:

- Nivel de acceso:

Redes Guiadas:

Cobre (xDSL -> ADSL)

Fibra (PON)

Redes No Guiadas Inalámbricas

- Nivel troncal de transporte: backbone

- Nivel de distribución:

Comutación:

Circuitos (ocupamos todo el canal)

y de Paquetes (troceamos):

Orientado a la Conexión (Todos los paquetes siguen el mismo) - TCP

No Orientado a la Conexión (Cada paquete sigue su propio camino) - UDP

Multiplexación:

FDM (Multiplexación por División de Frecuencias)

TDM (Multiplexación por División de Tiempos)

WDM (Multiplexación por División de Longitudes de Onda)

2. Arquitectura de redes de voz y datos

Redes de Cobre xDSL:

ADSL (Asymmetric Digital Subscriber Line) Línea de Abono Digital Asimétrica

Crea dos canales de datos de ancho de banda asimétricos (uno de subida y otro de bajada). El canal de bajada (de central al usuario) es mucho mayor que el de subida (de usuario a central)

Un tercer canal destinado al servicio de voz, es decir, al servicio telefónico básico

Con el Splitter separamos los canales de voz (300 Hz hasta los 3.400 Hz) y de datos (24 KHz hasta los 1,1 Mhz)

Redes inalámbricas:

Problemas:

Necesitas Visibilidad directa

Interferencias por otras señales, por tormentas... muy sensible a la orografía del terreno

WLL (Radiofrecuencias Licenciadas)

MMDS (Distribución Multipunto por Microondas)

LMDS (Sistema de Distribución Multipunto Local)

WIMAX (Interoperabilidad Mundial para Acceso por Microondas)

Redes de Fibra:

- ⇒ HFC: Fibra en la operador y coaxial en el hogar
 - Primer Nivel: topología estrella del Nodo central a los nodos secundarios conversión óptico-coaxial
 - Segundo Nivel: topología bus del nodo secundario al abonado con coaxial
 - Nivel Transporte: backbone – anillo fibra primaria a anillos fibra secundaria
 - Nivel distribución: viene del nodo secundario óptico y en bus hasta el abonado
- ⇒ Tecnología PON: Red Óptica Pasiva, sin elementos activos (amplificadores)
 - OLT: ubicado en la central.

Funciones:

- Gestionar y enrutar el tráfico de las ONTs.
- Conectar la red PON con otras redes

Permite conectividad con:

- La red telefónica básica.
- Proveedores ISP para datos a través de un Gateway.
- Proveedores de Vídeo a través de un Gateway

- Splitter: entre el abonado y la central
- ONT: ubicado en el domicilio del abonado

- Utiliza multiplexación por longitud de onda
 - Estándares: APON, BPON, GPON, EPON, 10GPON
- ⇒ Tecnología CWDM: Se usa en PON, FTTH y se basa en dividir la longitudes de onda ancho de banda de 20 nm
- 2.3. Mecanismos de codificación y cifrado de la información**
Existen técnicas para codificación de señales, entre ellas: Codificación NRZ, Codificación NRZI, Codificación Manchester, Codificación de Miller, Codificación bipolar
- 2.4. Sistemas de seguridad en el transporte de datos**
Criptografía simétrica: se emplea la misma clave del algoritmo para cifrar que para descifrar
Criptografía asimétrica: emplear una clave de cifrado distinta para cifrar y otra para descifrar
- 3. Servicios de comunicaciones:**
Servicio de telefonía fija
Servicio de telefonía móvil
- 3.3. Servicios de datos, servicios IP. Telefonía IP**
Web, Correo electrónico, FTP, TELNET
Telefonía IP
Televisión IP
- 3.4. Servicios telemáticos e interactivos**
Whatsapp, Chat, mensajería
- 3.6. Criterios de calidad de servicio (QoS)**
- 4. Implementación y configuración de pasarelas:**
Funciones de una pasarela o Gateway.
- 5. Equipos de conmutación telefónica. «Call Managers»**
El Concepto de central telefónica o Call Manager
- 6. Mercado de las telecomunicaciones**
Agentes en el mercado de las telecomunicaciones:
 - Fabricantes y suministradores.
 - Operadores:
Tipos de Servicio que nos van a dar: ISP, Hosting, Telefonía, Satelite
 - Usuarios