TECNOLOGÍA DE REDES
(Grado en Ingeniería Informática)

(francisco.arguello@usc.es)
Departamento de Electrónica y Computación
Universidad de Santiago de Compostela

28 de enero de 2020

Índice general

Capítulo 1

Calidad de Servicio (QoS)

En este capítulo veremos la calidad de servicio, dos protocolos que dependen fuertemente de la calidad de servicio (RTP y VoIP) y el multicast.

1.1. Modelos de QoS

La calidad de servicio (QoS, Quality of Service) es el rendimiento de la red tal como lo percibe el usuario final. Los parámetros de QoS comprenden todos los aspectos de una conexión, siendo particularmente importantes:

tasa de transmisión (ancho de banda)
retardo (latencia)
variación del retardo (jitter)
pérdida de paquetes

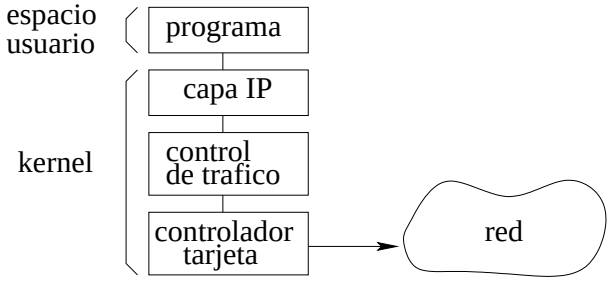
La QoS es imprescindible en aplicaciones tales como el audio y vídeo en tiempo real (telefonía y videoconferencia IP), aplicaciones interactivas (conexiones remotas por ssh), los juegos en red y el pago por visión (streaming). Para proporcionar QoS es necesario asignar diferentes prioridades a diferentes aplicaciones, usuarios o flujos de datos. A las aplicaciones que tienen unos requerimientos de QoS se les asigna la máxima prioridad de transmisión y se les reservan recursos en los routers y enlaces. Este beneficio se consigue a costa penalizar a otro tipo de transmisiones tales como la transferencia de ficheros, envío de correos, etc, que no son tan sensibles a la QoS. Las garantías de QoS son especialmente importantes si la capacidad de la red es limitada.

Las redes IP fueron diseñadas para maximizar el número de paquetes transmitidos por la red, sin tener en cuenta los retardos ni la pérdida de paquetes. Sin embargo, a las redes IP actualmente se les pide que soporten una mezcla de tráfico que engloba tanto a las transferencias masivas de datos como a las aplicaciones anteriormente citadas que requieren QoS. Afortunadamente la QoS se puede introducir con mecanismos y protocolos adicionales sobre la base de la arquitectura IP.

1.1.1. Calidad de servicio en la red local

Cuando en una red local tenemos más de un ordenador conectado a Internet compartiendo la misma conexión puede pasar que una aplicación empiece a consumir mucho ancho de banda (una descarga grande, p2p, etc), acaparando la conexión y haciendo que las demás transmisiones casi no tengan ancho de banda y los retardos sean muy grandes. Esto se ve agravado en las aplicaciones interactivas o que requieran bajo retardo, como las conexiones ssh.

El subsistema de transmisión de un sistema operativo tiene la siguiente estructura simplificada:



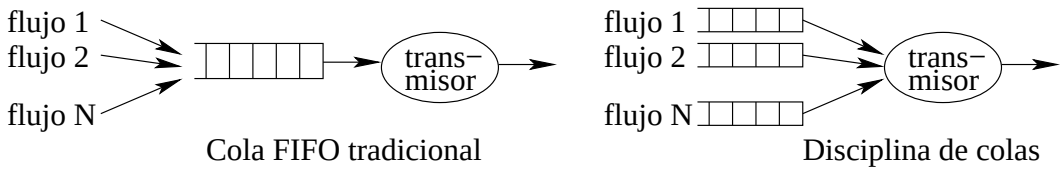
El programa del usuario genera los datos y solicita las transmisiones, la capa IP construye los paquetes y el módulo de control del tráfico gestiona cómo y cuándo los paquetes son transmitidos, por último, la tarjeta de red se limita a poner los paquetes en el enlace en el mismo orden que los recibe.

El módulo de control de tráfico puede limitarse a multiplexar los paquetes que le llegan de las diferentes aplicaciones pero también puede utilizarse para proporcionar QoS implementando las siguientes medidas:

1. **Reordenamiento de la secuencia de paquetes**. El módulo de control de tráfico puede reordenar la secuencia de paquetes dando más prioridad a determinadas aplicaciones.

2. **Reducción de la tasa de transmisión**. El módulo de control de tráfico puede retrasar el envío de paquetes, con lo que reduce de forma directa el tráfico de salida. También puede retrasar el envío de asentimientos en TCP, con lo que se reduce indirectamente el tráfico de entrada.

Teniendo en cuesta esto, se implementa un control de tráfico basado en las denominadas **disciplinas de colas**. Así, el comando `tc` de Linux permite organizar un sistema de colas que clasifique, reordene o retrase el envío de los paquetes según los criterios del administrador.



Como criterio de clasificación puede utilizarse: usuario, IP o puerto origen o destino, aplicación, flujo, etc. Se puede definir un ancho de banda de transmisión total máximo, repartirlo equitativamente o no entre cada flujo, tipo de transmisión o usuario, definir prioridades, etc.

1.1.2. Calidad de servicio en IP

Tradicionalmente, las redes IP proporcionan un tipo de servicio denominado de *mejor esfuerzo*, que significa que todos los usuarios reciben el mejor servicio posible en ese momento, repartiendo los recursos entre todas las transmisiones, pero sin ninguna garantía con respecto a los retardos, ancho de banda y paquetes perdidos. De entre los elementos que caracterizan al protocolo IP, hay algunos que podrían aprovecharse para proporcionar cierta QoS:

1. **Tipo de Servicio**. En la cabecera IP hay un campo denominado *tipo de Servicio* (TOS) pensado para que la aplicación indique qué tipo de ruta prefiere: de gran capacidad, de bajo retardo o más confiable. Este parámetro se diseñó para aprovechar los algoritmos de encaminamiento que generan rutas alternativas para un mismo destino, como por ejemplo OSPF. Aunque este campo tradicionalmente ha sido ignorado por los routers, podría utilizarse para distinguir los diferentes tipos de tráfico y proporcionar QoS.

2. **Descarte de paquetes**. Para evitar la congestión en los routers, cuando la memoria de un router se satura, éste descarta algunos paquetes, usualmente los últimos en llegar. Esta característica podría aprovecharse para proporcionar QoS si se seleccionaran los paquetes a descartar.

3. **Control de congestión en TCP**. Cuando TCP detecta pérdida de paquetes procede a reducir la tasa de envío. UDP, sin embargo, no dispone de ningún tipo de control de congestión. Esta característica de TCP podría aprovecharse para la QoS si la reducción de la tasa de envío estuviera supeditada al tipo de tráfico.

Para añadir QoS a las redes IP se han definido dos mecanismos complementarios: servicios integrados *IntServ* y servicios diferenciados *DiffServ*.

1.1.3. Modelo de Servicios Integrados

El modelo de *Servicios Integrados* (IntServ) especifica un mecanismo de extremo a extremo para proporcionar QoS en Internet. Requiere de un módulo en cada router IP a lo largo de la trayectoria, que reserva recursos para cada transmisión y entonces se asegura que cada paquete de datos en tránsito sea chequeado para ver qué recursos le corresponden recibir.

Estas reservas son pedidas usando un protocolo de reserva de recursos conocido como RSVP. Si la solicitud de RSVP falla, entonces la sesión no se inicia.

Para implementar este modelo los routers incluirán lo siguiente:

1. **Control de admisión**. Los hosts TCP/IP podrán enviar los datagramas en la forma usual, pero si desean que la transmisión haga uso de las nuevas técnicas de QoS deberán hacer una reserva para el nuevo flujo. Si los routers determinan de manera colectiva que los recursos son insuficientes para garantizar la QoS solicitada, entonces el flujo no se admite.

2. **Identificador de flujo**. En este modelo cada paquete IP se hace corresponder a un flujo, que es una secuencia de paquetes IP que tiene como origen la actividad única de un usuario y que requiere una misma QoS. Por tanto, los routers han de identificar el flujo al que pertenece cada paquete. Para ello puede utilizarse el identificador de flujo de la cabecera IPv6, mientras que en IPv4 un flujo podría identificarse como una transmisión con el mismo origen y destino y con la misma conexión de transporte o por las cabeceras de la capa de aplicación si son estándar.

3. **Routers con disciplina de colas**. Los routers tradicionalmente implementan una cola FIFO: rutan en primer lugar los paquetes que ha llegado antes. En este modelo se utilizarán diversas colas para tener en cuenta los distintos requisitos de los distintos flujos.

El modelo *IntServ* define tres categorías de servicio:

- **Mejor esfuerzo**. Es el servicio tradicional de las redes IP

- **Garantizado**. La red garantiza a la aplicación una cierta tasa de transmisión, un cierto retardo de los paquetes y que no habrá pérdidas de paquetes por desbordamiento de la memoria en routers. Los paquetes sólo se perderán por fallos en la red.

- **Carga controlada**. No hay un límite superior para el retardo de los paquetes en la red, aunque se asegura que la mayor parte de los paquetes llegarán con poco retardo. El número de paquetes que se descarten por desbordamiento de la memoria en los routers será pequeño.

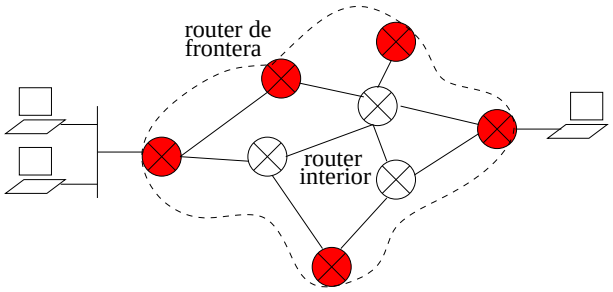
Este modelo presenta como desventajas ser complejo, necesitar de nuevo software tanto en los hosts como en todos routers a lo largo del camino y ser poco escalable, pues si fuera implementado en todas las transmisiones podría degradar el rendimiento de la red.

1.1.4. Modelo de Servicios Diferenciados

El modelo *Servicios Diferenciados* (DiffServ) usa un mecanismo alternativo a *IntServ*, más simple, fácil de implementar y con menos requerimientos. La QoS no es global como en modelo anterior, sino que queda limitada al dominio de un ISP (Proveedor de Servicios de Internet) y con un acuerdo previo entre proveedor y cliente. Los clientes pueden elegir entre distintas clases de servicio, por ejemplo, a un centro de datos puede interesarle mayor ancho de banda, mientras que a una empresa de juegos en red, menores retardos.

El modelo incorpora los siguientes elementos:

1. **Routers**. Dentro del dominio del ISP se distinguen dos tipos de routers: de frontera e interiores. Los routers de frontera son típicamente los encargados de realizar el control de tráfico y constan de 4 elementos:



   Clasificador. Clasifica los paquetes de acuerdo a los campos de la cabecera IP. Por ejemplo, con las direcciones IP de origen y destino puede identificar a los clientes.

   Medidor. Comprueba que el tráfico de cada cliente respecta las condiciones del contrato.

   Marcador. Escribe las marcas en los paquetes.

   Conformado/descarte. Retrasa el envío de algunos paquetes para ajustarse a la tasa de transmisión contratada por cada cliente. Si la capacidad de las colas de espera se sobrepasa se empieza a descartar paquetes.

2. **Marcas**. A la entrada de la red del proveedor se marcan los paquetes de acuerdo al tipo de servicio contratado. En respuesta a estas marcas, los enrutadores y switches proporcionan diferentes prioridades y con ello QoS. Se le da la misma marca a los paquetes de distintos clientes que requieran la misma clase de servicio. De esta forma se evita la creación de información de estado en los routers para cada flujo individual. Las marcas se introducen modificando el campo TOS de los paquetes IPv4 o el identificador de flujo de los paquetes IPV6, con lo que se evita introducir nuevas cabeceras o protocolos.

3. **Tipos de servicio**. Las características de las distintas clases de servicio las puede definir cada ISP, aunque hay algunas recomendadas. La única clase requerida es la de mejor esfuerzo por compatibilidad con las redes IP tradicionales. Es decir, el modelo en vez de especificar clases de servicio, provee los componentes necesarios para que puedan construirse.

1.1.5. Protocolos y redes que incorporan QoS

Muchos otros protocolos y modelos de red incorporan por sí mismos QoS, entre ellos veremos más adelante:

1. VoIP (Voz IP), un protocolo de telefonía usando las redes IP.
2. VLAN (Virtual LAN), un mecanimo para crear LANs virtuales.
3. WiFi Multimedia (WMM), una extensión a las redes WiFi.
4. WiMAX (Wireless MAN), un modelo de red inalámbrica MAN.
5. ATM (Asynchronous Transfer Mode), un modelo de red WAN.
6. MPLS (Multiprotocol Label Switching), un mecanismo para definir circuitos virtuales en las redes IP.

1.2. RTP

El Protocolo de Transporte en Tiempo Real (RTP) se ha diseñado especificamente para aplicaciones distribuidas que requieren tiempo real. Ejemplos de tales aplicaciones son la telefonía, la videoconferencia, la reproducción de vídeo, juegos en red, entornos de trabajo compartidos, monitorización en tiempo real, etc. El protocolo de transporte UDP es adecuado para estas aplicaciones, sin embargo, le faltan algunas características que proporciona RTP. RTP se implementa por encima de UDP (en una capa adicional) y proporciona las características siguientes:

- **Información de tiempos**. RTP posee un mecanismo para asociar tiempos a los datagramas, que es una de las exigencias del tiempo real. Con ello el receptor puede recrear la temporización correcta de la información.
- **Mayor control de la aplicación sobre la transmisión**. Es recomendable informar a la aplicación sobre la calidad de la entrega, más que solicitar retransmisiones. Si se están perdiendo demasiados paquetes, la fuente

podría reducir la calidad de la aplicación, por ejemplo, disminuyendo el nivel de resolución del audio o del vídeo. En todo caso, es preferible que se sea la aplicación, más que la capa de transporte, la que proporcione los datos para la retransmisión, suministrando valores revisados para la situación actual.

En el caso de RTP, se proporcionan informes de recepción que informan al emisor de los problemas encontrados por los receptores, incluyendo las pérdidas de paquetes y el exceso de fluctuaciones.

- **Multidifusión**. RTP soporta la transferencia en tiempo real entre varios participantes. Existen campos para indicar el identificador de una sesión y las direcciones IP de los participantes en dicha sesión.

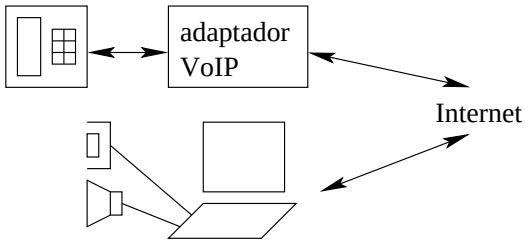
- **Retransmisores**. Supongamos que un sistema A desea enviar datos a un sistema B, pero que no puede hacerlo porque entre ambos hay un cortafuegos que lo impide. En tal caso, A puede transmitir los datos a un retransmisor intermedio con permiso para atravesar el cortafuegos. Este retransmisor transmite luego los datos a B. Además, dos tipos especiales de retransmisores son los mezcladores y traductores.

  Un *mezclador* es un retransmisor RTP que recibe flujos de paquetes RTP de dos o más fuentes, combina esos flujos y envía el flujo combinado a uno o más destinos.

  Un *traductor* es un dispositivo más sencillo que simplemente produce uno más paquetes RTP de salida por cada paquete RTP entrante, después de realizar un cierto procesamiento.

1.3. VoIP

Voz sobre IP (VoIP) es una tecnología que permite hacer llamadas telefónicas sobre las redes IP, obteniendo la convergencia entre las redes de voz y datos. VoIP en el origen convierte la señal de voz en paquetes IP y en el destino se vuelve a reconstruir la señal de voz. Cuando se usan teléfonos normales con adaptadores de VoIP, el usuario oirá los tonos de señalización telefónica usuales. También se puede utilizar directamente un ordenador que disponga de tarjeta de sonido.



Su principal ventaja es el abaratamiento de las comunicaciones telefónicas. Entre sus características destacan las siguientes:

- Es completamente compatible con todo tipo de red, aunque se necesita una conexión de banda ancha. Se puede utilizar desde una línea ADSL, red Ethernet, etc. También se puede utilizar desde redes Wi-Fi.

  Además, se puede cambiar la ubicación del adaptador de VoIP (y del teléfono) en cualquier lugar de Internet.

  Se puede implementar tanto en software como en hardware y admite el cifrado de las transmisiones.

- Permite el control del tráfico de la red, por lo que se disminuyen las posibilidades de que se produzcan caídas importantes en el rendimiento de las redes de datos.

- Se puede implementar sin ningún tipo de contrato, aunque en este caso sólo se podrá llamar a otros teléfonos VoIP.[1]

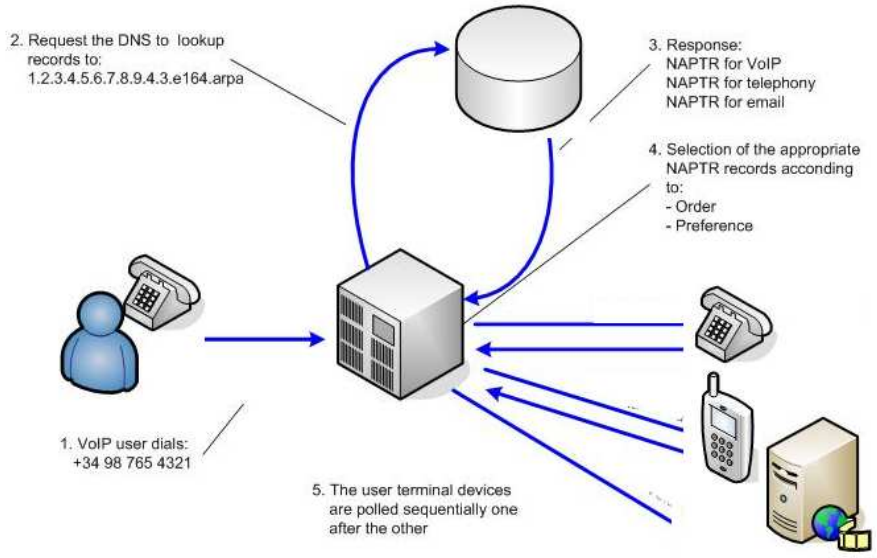
  Alternativamente, se puede contratar con alguna compañía proveedora de servicios VoIP y en este caso se podrá hacer llamadas a cualquier teléfono fijo, móvil, etc, a precios muy reducidos, pues la transmisión se realizará en su mayor parte por Internet. Solo en el tramo final se pasará a la red telefónica, con lo cual todas las llamadas se cobrarán como locales.[2]

- La localización de los teléfonos puede realizarse de varias formas. Lo más usual es que la compañías de VoIP mantengan un base de datos en la que se dan de alta los usuarios que desean usar el servicio. Cuando se realiza una llamada a un determinado usuario se consulta esta base de datos que devuelve la localización (dirección IP y otros datos) del usuario solicitado.

- El estándar ENUM (E.164) proporciona la forma de mapear los números de teléfono del sistema telefónico tradicional sobre VoIP usando el DNS. A cualquier número de teléfono, tal como 1 555 42 42, se le puede asignar un nombre de host invirtiendo los dígitos, separándolos por puntos y añadiendo el sufijo *e164.arpa*, como por ejemplo, 2.4.2.4.5.5.5.1.e164.arpa.

  Cuando se realiza una llamada usando ENUM el DNS responde con una lista de recursos, que se pueden ir probando secuencialmente. Por ejemplo, puede responder con datos para una comunicación VoIP, para una llamada teléfónica convencional o una dirección de correo-e.

[1] Por ejemplo, *spyke* y *google talk*.
[2] Véase por ejemplo, http://www.telsome.es, http://www.virtucall.es.



La arquitectura de red de VoIP define tres elementos fundamentales:

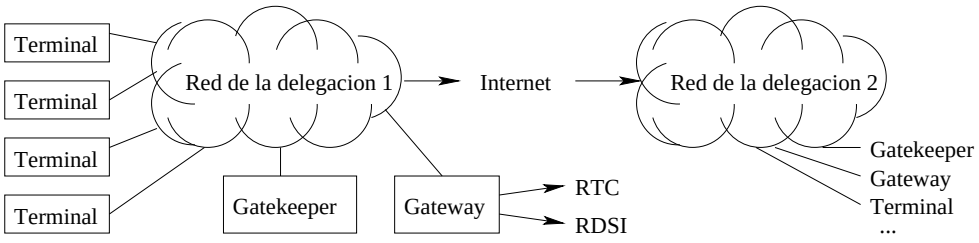
1. **Terminal**. Es el sustituto del teléfono actual. Se puede implementar tanto en software como en hardware.

2. **Centralita (gatekeeper)**. En caso de existir será el centro de toda la organización VoIP y el sustituto de las actuales centralitas. Todas las comunicaciones pasarán por ella y proporcionará traducción de direcciones, control de admisiones y control de QoS. Se puede implementar en software.

   En general, a la centralita telefónica privada de una empresa se le denomina PBX (Private Branch Exchange).

3. **Pasarela (gateway)**. Se trata del enlace con la red telefónica tradicional, actuando de forma transparente para el usuario.

En la siguiente figura se muestra la conexión entre dos delegaciones de una misma empresa conectadas mediante VoIP. La ventaja es inmediata: todas las comunicaciones entre las delegaciones son completamente gratuitas.



VoIP emplea diversos protocolos dependiendo de la aplicación y del proveedor, algunos de los cuales se basan en RTP. Algunos de los protocolos, por orden de antigüedad son: H.323, SIP, IAX, Skype e IAX2.

1.4. Multicast

Dependiendo de los destinatarios, se distinguen los siguientes tipos de transmisión en una red:

1. **Unicast**. Es la transmisión normal, en donde el datagrama se envía al destino identificado por la dirección IP del paquete.

2. **Broadcast**. Es el envío de un datagrama a todos los hosts de una red. El broadcast se utiliza para funciones de administración, para la localización de servidores, etc.

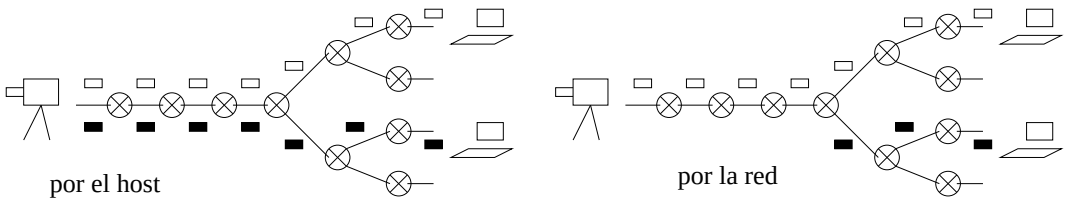
3. **Multicast**. Permite hacer hacer grupos de hosts e identificarlos por una dirección de multicast, de tal forma que un datagrama enviado a dicha dirección de multicast sea recibido por todos los hosts del grupo.

4. **Anycast**. Es el envío de un datagrama a uno cualquiera de los hosts de un grupo identificado por una dirección anycast, usualmente al más cercano. Por ejemplo, puede utilizarse para enviar una petición HTTP a cualquiera de los servidores web que contengan un determinado documento.

El multicast tiene múltiples aplicaciones, entre las que están los juegos en red, la telefonía con varios participantes, la distribución de software (por ejemplo, las actualizaciones de seguridad), el envío noticias a grupos, la difusión de audio/vídeo hacia múltiples abonados, etc. El multicast puede hacerse de dos formas:

- Por el host. En este esquema, el host emisor envía una copia del datagrama para cada uno de los destinos. Obviamente este esquema es muy ineficiente.

- Por la red. El emisor envía un único datagrama a una dirección de multicast y es la red la que se encarga de replicar los paquetes en los routers precisos. Este es el esquema más adecuado dado el elevado volumen de datos que suelen enviar las aplicaciones multicast.



a) Direcciones multicast IPv4

En primer lugar, revisemos las antiguas clases de direcciones IPv4:

- Las direcciones IPv4 unicast son las antiguas clases A, B y C, que actualmente se han transformado en las direcciones sin clases. Estas direcciones contienen una parte de red y otra de host.
- En IPv4 las direcciones de broadcast se obtienen a partir de la dirección de una red poniendo todos los bits del campo de host a 1 (por ejemplo, para la red 193.144.84.0/24, la dirección de broadcast es 193.144.84.255). También puede usarse la dirección genérica 255.255.255.255.
- Las direcciones de clase D (cuyo primer byte comienza por 1110) se usan para multicast.
- En IPv4 no hay direcciones anycast.

Restringiéndonos a las direcciones IPv4, dentro de esta clase D se distinguen tres rangos de direcciones multicast:

- **Reservadas**. Este rango de direcciones se reserva para los protocolos de rutado y de administración de la red (224.0.0.0-224.0.0.255). Por ejemplo, 224.0.0.1 es el grupo de todos los dispositivos de una red, 224.0.0.2 es el grupo de todos los routers, 224.0.0.5 es el conjunto de todos los routers OSPF, etc.
- **Globales**. Este rango es gestionado directamente por el organismo de asignación de direcciones de Internet (224.0.1.0-238.255.255.255). Las direcciones se asignan mediante petición y hacen posible el multicast en el global de Internet. Aunque no todos los routers de Internet soportan el multicast, siempre es posible la tunelización en las zonas en las que no haya soporte.
- **Privadas**. Este rango puede utilizarse libremente por el administrador de una red local (o de un sistema autónomo), pero las transmisiones quedan restringidas localmente (239.0.0.0-239.255.255.255).

El tiempo de vida de los paquetes (TTL) en el multicast IPv4 tiene un doble significado. Por un lado controla el tiempo de vida de un datagrama en la red, pero si además estamos trabajando con multicast, el TTL define el ámbito del datagrama, es decir, cómo de lejos llegará.

Ámbito	TTL	Direcciones
Nodo. No saldrá por interface de red.	0	
Enlace. No será encaminado por router.	1	224.0.0.0-224.0.0.255
Departamento.	2-31	239.255.0.0-239.255.255.255
Organización.	32-63	239.192.0.0-239.195.255.255
Global. Sin restricción.	64-255	224.0.1.0-238.255.255.255

b) Direcciones multicast IPv6

Las direcciones IPv6 que comienzan por el byte `FF` son multicast y el resto son direcciones unicast. Las direcciones anycast se obtienen a partir de las direcciones unicast poniendo a 0 el campo de host. En IPv6 no existe el broadcast, en su lugar ha de usarse el multicast. Más en concreto para el multicast:

Ámbito	Direcciones (prefijo)
Nodo	`FFx1:`
Enlace	`FFx2:`
Departamento	`FFx3`
Organización	`FFx8:`
Global	`FFxE:`

Por ejemplo, `3FFE:FFFF:128:1:2:3:4:5/48` es una dirección unicast, pero `3FFE:FFFF:128:0:0:0:0:0/48` es una dirección anycast y `FF01:0:0:0:0:0:0:1` es una dirección multicast.

c) Direcciones multicast Ethernet

Las direcciones Ethernet cuyo primer byte es par son direcciones unicast, `FF:FF:FF:FF:FF:FF` es la dirección de broadcast y el resto son direcciones multicast. Por ejemplo, `32:11:22:33:44:55` es una dirección unicast, mientras que `01:11:22:33:44:55` es una dirección multicast.

En una red Ethernet, si el host se ha unido a un grupo multicast, el interface de red deberá reconocer también como tramas destinadas a él, todas aquellas cuya dirección de destino sea la correspondiente al grupo de multicast al cual se haya unido el host. Por ejemplo, si un host de una red tiene un interface cuya dirección física es `80:C0:F6:A0:4A:B1` y además se ha unido al grupo 224.0.1.9, se le autoasigna la dirección multicast `01:00:5E:00:01:09`. Esta dirección se obtiene de la siguiente forma (la relación no es biunívoca):

- Los tres primeros bytes son siempre el prefijo `01:00:5E`.
- El siguiente bit es siempre 0.
- Los tres siguientes bytes (excepto el primer bit que se puso a 0 en el punto anterior) se igualan a los tres bytes de menor peso de la dirección multicast IPv4 (224.0.1.9 → `00:01:09`).

Uso del multicast

El uso del multicast implica la necesidad de incorporar lo siguiente:

1. *En el host* hay que informar a la tarjeta de red de los grupos de multicast en los que estamos interesados, para que ésta acepte las transmisiones con

las correspondientes direcciones multicast. Normalmente esto lo harán las aplicaciones que hacen uso del multicast, como por ejemplo las aplicaciones multimedia.

2. *En la red* hay que informar a los routers de qué hosts forman en cada momento parte de cada grupo multicast. Para ello, se ha diseñado un protocolo que permite la unión o abandono de un host a un grupo, la consulta de los miembros de un grupo, etc. Este protocolo se denomina IGMP (Protocolo de Gestión de Grupos de Internet).

3. *Protocolo de rutado.* Además, se han diseñado los protocolos de rutado específicos para multicast, entre los cuales se encuentra PIM (Multicast Independiente del Protocolo). Este protocolo crea una estructura de árbol de distribución entre los clientes multicast.

Capítulo 2

Redes de área local y metropolitanas

Las redes se pueden clasificar como redes de área amplia (WAN, Wide Area Network), redes de área metropolitana (MAN, Metropolitan Area Network) y redes de área local (LAN, Local Area, Network). En este capítulo nos ocuparemos de las redes de área local y metropolitanas.

Las *redes área local (LAN)* ocupan un área de unos pocos km y suelen ser propiedad de una organización que las usa para conectar sus equipos dentro de un mismo edificio.

Las *redes metropolitanas (MAN)* típicamente funcionan como troncales (*backbone*) interconectando redes situadas en varios edificios dentro de la misma ciudad, pero usan una tecnología muy similar a las LAN y las veremos también en este capítulo.

2.1. Clasificación de las redes de área local

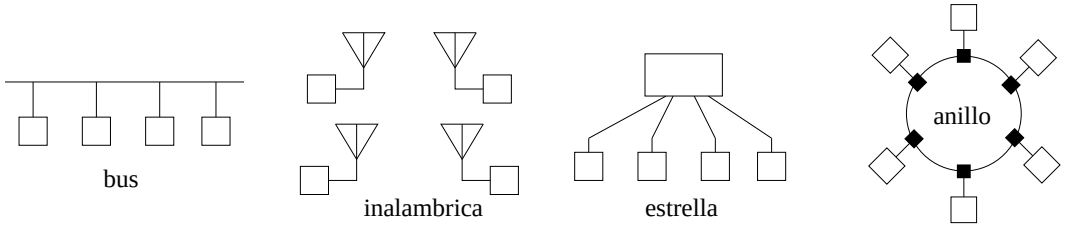
Las redes local se pueden clasificar atendiendo a diferentes criterios.

a) Clasificación según la tecnología: conmutación, difusión, híbrida

En una *red de conmutación* para cada transmisión se genera un ruta que tiene como destino único el host destino. La ruta se genera conmutando routers. En una *red de difusión* el medio de transmisión es compartido por todas las transmisiones, por lo que todas las transmisiones las reciben todos los hosts, aunque sólo el host destino es el que atiende a la recepción, ignorándola el resto.

El tipo de red *híbrida difusión-conmutación* es la más extendida actualmente para las LANs. Por ejemplo, en una Ethernet conmutada, el switch difunde las transmisiones cuando desconoce la localización del destino, pero realiza conmutaciones una vez que aprende la localización de los hosts. En todas las redes de difusión e híbridas es necesario un protocolo de Control de Acceso al Medio (MAC).

b) Clasificación según la topología

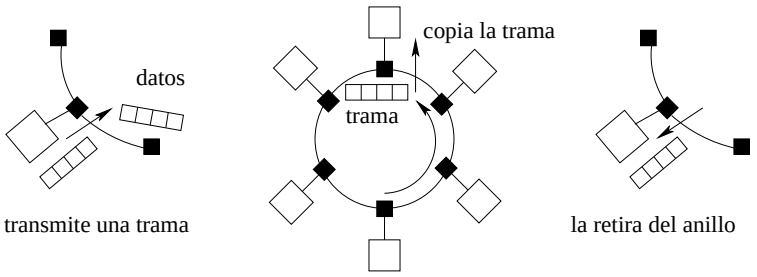


- **Bus**. La topología clásica (obsoleta) es un bus de cable coaxial en el que se insertan las tarjetas de red de los hosts mediante conectores T (cortando cable). Una LAN de topología bus es siempre una red de difusión. Una transmisión desde cualquier host se propaga a través del cable en ambos sentidos y es recibida por el resto de los hosts.

- **Inalámbrica**. Las transmisiones pueden realizarse con infrarrojos, en cuyo caso el alcance se limita a una habitación, o con microondas, que son capaces de atravesar las paredes (aunque con cierta atenuación). En cualquier caso, son redes de difusión.

- **Estrella**. En la actualidad la topología más empleada para las LAN es la estrella con un centro (hub o switch) y par trenzado o fibra óptica. El centro puede ser un hub (concentrador) funcionando en este caso como una red de difusión pura. En el caso en el que centro sea un conmutador (switch), comienza realizando difusiones cuando no conoce la localización de los hosts, pero una vez que los ha aprendido realiza conmutaciones. Es, por tanto, una red híbrida difusión-conmutación.

- **Anillo**. En la topología en anillo, la red consta de un conjunto de nodos unidos por enlaces punto a punto formando un bucle cerrado. Los nodos actúan como repetidores copiando bit a bit lo que viene por uno de los lados en el lado opuesto. De esta forma los datos van girando en el anillo en un determinado sentido. Mientras pasan por el nodo, este puede examinar los datos para determinar quién es el destino, y si es el mismo, pasar un copia al host al que está conectado. Típicamente el host origen de una trama es el encargado de retirarla del anillo una vez que esta ha dado una vuelta completa. La red de topología en anillo es, por tanto, una red de difusión.



c) Clasificación según el protocolo MAC

En una red de difusión el medio de transmisión es compartido por todos los hosts. El principal problema es decidir quién puede en cada momento utilizarlo. Por ejemplo, considérese una conversación de N personas, en N teléfonos todas conectadas todas entre sí. Es muy probable que cuando una deje de hablar, varias personas comenzarán a hablar a la vez.

De esto se ocupa la capa de acceso al medio o MAC (*Medium Access Control*). Hay dos tipos de protocolos MAC:

1. **Protocolos de contienda** (contención). Basados en el principio de que el primer host que decide transmitir es el que lo hace. El ejemplo típico es Ethernet.

2. **Basados en turnos** (rotación circular). A cada host se le da la oportunidad de transmitir en el turno que le corresponde. Típicamente los turnos se dan en secuencia, de ahí el nombre de rotación circular. Un ejemplo es WiMAX.

Para evaluar los dos tipos de protocolos hay dos parámetros principales, que tienen relevancia según lo cargada que esté la red:

- **Red en carga baja**. El parámetro a tener en cuenta es el retardo de transmisión promedio. Es decir el tiempo desde que un host solicita transmitir hasta que puede hacerlo.

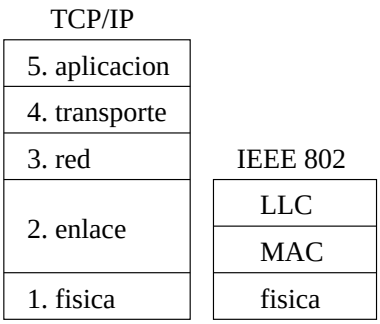
- **Red en carga alta**. El parámetro a tener en cuenta es la eficiencia (número de transmisiones).

En general, los protocolos de contienda generan un retardo de transmisión menor en situaciones de carga baja, puesto que cuando un host decide transmitir simplemente lo hace y el retardo es prácticamente 0, mientras que con un protocolo basado en turnos el host ha de esperar su turno.

En cambio, en condiciones de carga alta, los protocolos de contienda generan muchas colisiones y su eficiencia es baja, lo que no ocurre con los protocolos basados en turnos.

El modelo de referencia IEEE 802

El modelo IEEE 802 considera que los protocolos LAN que se integran en la arquitectura TCP/IP corresponden a las capas física y de enlace y que esta última se divide en dos subcapas:



La subcapa LLC (Control Lógico del Enlace) es común a todos los modelos de LAN y proporciona control de flujo y control de errores a nivel de la capa de enlace. Sin embargo la red Ethernet usualmente no la incluye porque los errores son raros en la redes de cable y los paquetes con errores simplemente se descartan. En la LAN inalambrica los errores son frecuentes, pero su gestión forma parte de la subcapa MAC, así que estas redes tampoco usan LLC.

A continuación mostramos la lista de estándares del modelo IEEE 802. El estándar IEEE 802.2 especifica la subcapa LLC, mientras que los restantes, en su mayoría, describen los distintos modelos de la subcapa MAC.

IEEE 802.1	Higher layer LAN protocols (por ejemplo, **Bridges**, **Virtual LANs**, **Spanning Tree Protocol**)
IEEE 802.2	Logical Link Control
IEEE 802.3	**Ethernet**
IEEE 802.4	Token Bus
IEEE 802.5	Token Ring
IEEE 802.6	Metropolitan Area Networks
IEEE 802.7	Broadband LAN using Coaxial Cable
IEEE 802.8	Fiber Optic TAG
IEEE 802.9	Integrated Services LAN
IEEE 802.10	Interoperable LAN Security
IEEE 802.11	**Wireless LAN (WiFi)**
IEEE 802.12	Demand priority
IEEE 802.13	Se ha evitado su uso por superstición
IEEE 802.14	Cable modems
IEEE 802.15	**Wireless PAN (Bluetooth)**
IEEE 802.16	**Broadband wireless access (WiMAX)**
IEEE 802.17	Resilient Packet Ring
IEEE 802.18	Radio Regulatory TAG
IEEE 802.19	Coexistence TAG
IEEE 802.20	Mobile Broadband Wireless Access
IEEE 802.21	Media Independent Handoff
IEEE 802.22	Wireless Regional Area Network

Vamos a tratar los protocolos MAC de Ethernet, LAN inalámbrica y WiMAX.

2.2. Ethernet

2.2.1. Protocolo MAC

El protocolo de acceso al medio utilizado por Ethernet es de contienda y del tipo CSMA/CD (*Acceso Múltiple por Detección de Portadora con Detección de Colisión, Carrier Sense Multiple Access with Collision Detection*) 1-persistente.

Transmisión

Cuando los hosts están próximos entre sí, por ejemplo en una LAN, es posible comprobar si el medio está libre antes de transmitir (si las distancias fueran muy grandes, habría grandes retardos de propagación y se desconocería a priori lo que están haciendo los demás hosts en este momento). Cuando un host desea transmitir escucha el cable (de ahí el nombre de CSMA, *Acceso Múltiple por Detección de Portadora*) y si el medio está libre transmite.

Si el medio estuviera ocupado, el host espera a que se desocupe y a continuación transmite de inmediato (el protocolo oficial de Ethernet especifica un espacio intertrama de 96 tiempos de bit, que en la práctica ha sido ignorado por los fabricantes con el objetivo de conseguir en los tests mejores resultados para sus productos), de ahí el nombre de *1-persistente*.

El problema es que si dos hosts quieren emitir cuando otro está a mitad de una transmisión, esperarán tranquilamente hasta que termine, y entonces ambos comenzarán a emitir a la vez, provocando una colisión. Si no fueran tan impacientes, se tendría un número menor de colisiones. Pero aunque este protocolo de contienda no es el mejor en términos de eficiencia, garantiza retardos pequeños.

Colisión

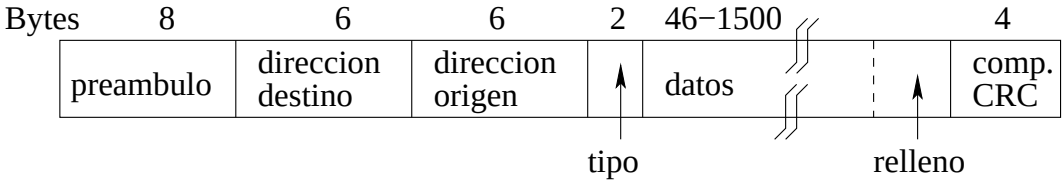
Si dos o más hosts de forma simultánea empiezan a emitir, generarán una colisión. Ambos detectarán inmediatamente la colisión y emitirán una ráfaga de aviso (*jam*) de 4 bytes para avisar al resto de los hosts que ha habido una colisión. La rapidez con que se efectúe la parada de las transmisiones disminuye el tiempo perdido en la colisión. Este protocolo añade la parte CD (*Detección de colisión*) al nombre de CSMA/CD. El protocolo CSMA/CD se usa extensivamente en las redes Ethernet de cable. No se incluye en la LAN inalámbrica, puesto que no resulta práctica en las transmisiones de radio. La señales radiadas se atenúan rápidamente y además el ruido del medio es elevado, por lo que es muy difícil detectar una colisión.

La pérdida de eficiencia del protocolo CSMA 1-persistente se ve minimizada por el hecho de que si la colisión se detecta pronto el tiempo perdido será muy pequeño.

Espera después de colisión

Después de una colisión los hosts esperarán un tiempo aleatorio antes de retransmitir. Para la elección del tiempo aleatorio se usa un algoritmo de *espera exponencial binaria* que a cada colisión sucesiva genera tiempos cada vez mayores. Después de la primera colisión, los hosts elegirán 0 o 1 y esperan ese número de ranuras de tiempo. Si se produjese una segunda colisión, elegirán aleatoriamente esperar 0, 1, 2 o 3 ranuras de tiempo. Después de la i-ésima colisión los hosts elegirán entre 0 y $2^i - 1$ ranuras. Después de la décima colisión el número de ranuras se congela a 1024 y si se produjesen 16 colisiones consecutivas se aborta el intento de transmisión y se reporta un fallo.

2.2.2. Formato de las tramas



1. Comienza con un *preámbulo* de 8 bytes, cada uno de los 7 primeros con los bits 10101010. Este patrón genera una onda cuadrada con objeto de permitir que el reloj del receptor se sincronice con el reloj del emisor. El octavo byte contiene el patrón 10101011.

2. Después vienen dos direcciones, una de ellas para el destino y otra para la fuente, de 6 bytes cada una.

3. El campo *tipo*[1] indica a qué protocolo de la capa de red hay que entregar los datos. Usualmente se entregarán al IP (otras alternativas son ARP, AppleTalk, etc).

4. El campo datos es de longitud variable. El máximo son 1500 bytes y el mínimo son 46. Si la información no llega al mínimo, se introduce un relleno. El relleno se introduce para que las tramas duren lo suficiente para que la detección de las colisiones se realice fácilmente.

   Sumando el resto de los campos menos el preámbulo, 6+6+2+4, la longitud de la trama estará comprendida entre 64 bytes (512 bits) y 1518 bytes.

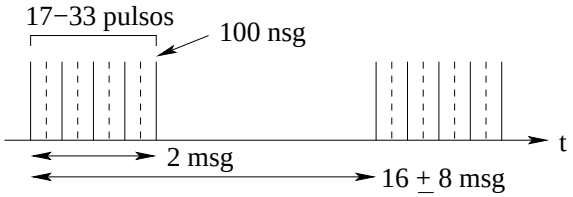
5. El campo *comprobación CRC* (código de redundancia cíclica) es un código de 4 bytes para detección de errores, calculado sobre los datos.

[1]Usualmente, por ejemplo en Linux y Windows, este campo de 2 bytes funciona como tipo. En otros sistemas operativos este campo puede indicar la longitud del campo datos.

Direcciones. Las direcciones Ethernet constan de 6 bytes (48 bits), de las cuales las direcciones ordinarias (unicast) que identifican a hosts individuales tienen el primer byte par, mientras que las direcciones multicast tienen el primer byte impar. La dirección `FF:FF:FF:FF:FF:FF` es de broadcast. Los tres primeros bytes identifican al vendedor, por ejemplo[2]: `00:E0:4C` (realtek), `00:E0:63` (cabletron), `00:50:BF` (mototech), etc.

La tarjeta de red de un ordenador usualmente atiende a las transmisiones con destino la dirección de la tarjeta y las direcciones de difusión, aunque puede programarse para que atienda a todas las transmisiones (modo promiscuo).

Pulsos. Adicionalmente, cuando no se transmiten tramas, los hosts transmiten pulsos (FLP, Fast Link Pulses) para detectar la presencia de otros dispositivos y para autonegociar la velocidad de transmisión y otros parámetros como half/full duplex. Son pulsos de tensión positiva, de duración 100 nsg, y hay 33 posiciones de pulso, de las cuales las 17 posiciones impares son para pulsos de sincronización y la presencia o ausencia de pulsos en las 16 restantes establecen el código.

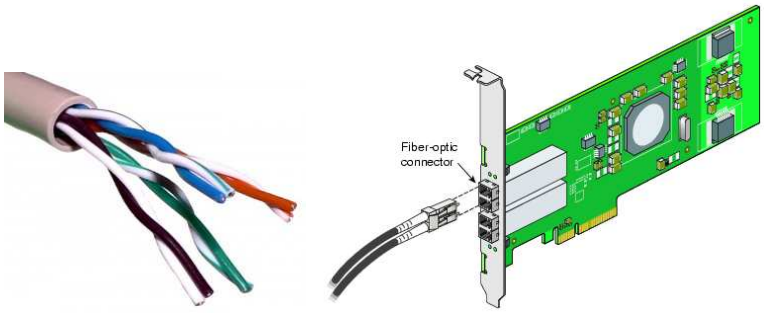


2.2.3. Ethernet conmutada

En la actualidad las redes Ethernet suelen utilizar una topología en estrella con un switch en el centro y con cable par trenzado o fibra óptica para realizar las conexiones. Aunque el par trenzado es peor que el coaxial tiene la ventaja que es simplemente cable telefónico y los edificios de oficinas suelen tener una preinstalación desde cada despacho a un armario de interconexión, en donde se instala el switch.

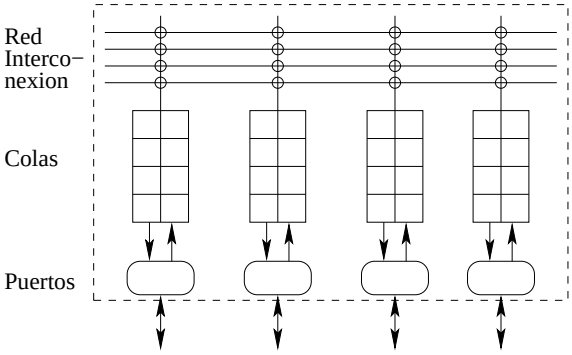
[2]Pueden consultarse en `http://www.coffer.com/mac_find/`.

Cableado. Los conectores RJ45 incluyen 8 hilos (4 pares trenzados) y la longitud del cable está limitada a 100 m. Como alternativa se puede utilizar fibra óptica en cuyo caso la distancia máxima puede ser de 400 m o más dependiendo del modelo. Como las fibras suelen ser unidireccionales, se suele usar un par de ellas, una para cada sentido de transmisión.



Switch (conmutador). Este es un dispositivo de capa 2 (enlace) que opera directamente con tramas Ethernet, es decir, que puede examinar y procesar los distintos campos de las tramas Ethernet. Por ejemplo, puede extraer la dirección destino de las tramas y redirigirlas por el puerto correspondiente. Además, puede detectar si la trama tiene errores usando el campo de comprobación CRC y en este caso descartarla. El switch realiza difusiones cuando no conoce la localización de los destinos, pero con el paso del tiempo aprende la localización de cada host en función de las direcciones Ethernet y a partir de entonces las transmisiones sólo se envían al host destino.

Los switches disponen de colas en los interfaces en las que pueden almacenar tramas y con ello evitar colisiones, aunque pueden perderse tramas por desbordamientos de las colas. Puesto que las transmisiones originadas en diferentes puertos no pueden colisionar entre sí, se dice que los switches segmentan los dominios de colisión.



Comercialmente existen dos tipos de switches:

- **Switch de almacenamiento y reenvío**. El switch almacena las tramas que llegan en una memoria donde se examinan y después las reenvía por el correspondiente puerto de salida. Por tanto, se introduce un pequeño retardo.

- **Switch rápido o de corte** (cut-through). El switch empieza a reenviar la trama por el puerto de salida (corte a través) tan pronto como sabe la dirección destino. Proporciona un mayor rendimiento a costa de no poder comprobar la integridad de la trama, pues esta se empieza a reenviar antes de que el switch la haya recibida completa.

2.2.4. Modelos

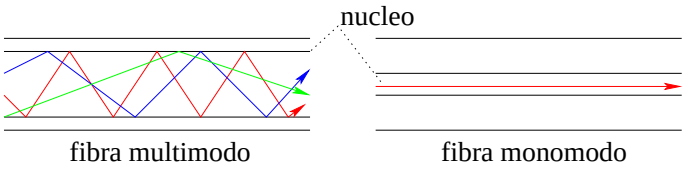
Existen varias configuraciones de red Ethernet con topología estrella. En la nomenclatura T indica par trenzado y F (fibra), S (short), L (long), E (extended) indican fibra óptica.

- *10base-T*: 10 Mbps, dos pares trenzados UTP de categorías 3 o 5: un par para emisión y otro par para recepción, longitud 100 m.
- *100base-TX* (Fast Ethernet de par trenzado): 100 Mbps, dos pares trenzados UTP de categoría 5: uno de emisión y otro de recepción, longitud 100 m.
- *100base-FX* (Fast Ethernet de fibra óptica): 100 Mbps, dos fibras ópticas, una para emitir y otra para recibir, longitud 400 m. Es más cara que el modelo anterior, pero tiene la ventaja de que la longitud es mayor.
- *1000base-T* (Gigabit Ethernet de par trenzado): 1 Gbps, 4 pares trenzados de categoría 5e o 6 funcionando en paralelo, longitud 100 m.

  El par trenzado de categoría 5e puede transmitir de forma fiable hasta 125 Mbps. Usando cancelación de eco las transmisiones full-duplex sobre el mismo par obtienen 250 Mbps, que multiplicado por 4 pares da el total de 1 Gbps.
- *1000base-SX* y *1000base-LX* (Gigabit Ethernet de fibra óptica): 1 Gbps con distancias máximas de 550 m y 10 km, utilizadas como troncales para conexión de LANs y en MANs. Las letras S y L indican longitud: Short y Long.

  El modelo S (Short) utiliza fibra multimodo, que es aquella en la que durante una transmisión la luz se dispersa por más de un modo de propagación o camino (puede haber más de mil modos). Esto supone que no llegan todos a la vez y las interferencias que se producen limitan las transmisiones a corta distancia (menores a 2 km), pero es simple de diseñar y económico.

  El modelo L (Large) utiliza fibra monomodo, en la que sólo se propaga un modo de luz. Esto se logra reduciendo el diámetro del núcleo de la fibra hasta un tamaño del orden de la longitud de onda de la señal (sobre 10 micras). Esto implica que la señal solo se puede propagar de un solo modo, paralelo al eje de la fibra. Estas fibras permiten alcanzar grandes distancias (hasta 400 km) mediante un láser de alta intensidad.



- *10Gbase-SR*, *10Gbase-LR* y *10Gbase-ER* (10 Gigabit Ethernet): 10 Gbps sobre dos fibras ópticas (una para emitir y otra para recibir) y con distancias máximas de 300 m, 10 km y 40 km, respectivamente. Aunque sigue siendo completamente compatible con el resto de las tecnologías Ethernet, pues el formato de la trama sigue siendo el mismo, abandona el protocolo CSMA/CD (las colisiones son muy raras por el uso de switches y las pueden gestionar las capas superiores, por ejemplo, TCP).

  Con esta tecnología Ethernet entra de lleno en el terreno de las MAN (40 km) y su velocidad la hace compatible con la jerarquía SONET/SDH. Y con la ventaja de poder usar las tramas Ethernet de extremo a extremo.

- *40Gbase-SR4*, *40Gbase-LR4* y *40Gbase-ER4* (40 Gigabit Ethernet). Similar a los anteriores modelos, con distancias de 100 m, 10 km y 40 km, respectivamente. La transmisión se realiza usando 4 haces láser de diferentes longitudes de onda a 10 Gbps cada uno.

- *100Gbase-SR10*, *100Gbase-LR4* y *100Gbase-ER4* (100 Gigabit Ethernet). Similar a los anteriores modelos, con distancias menores a 100 m, 10 km y 40 km, respectivamente. La transmisión se realiza usando 4 haces láser de diferentes longitudes de onda a 25 Gbps cada uno.

  En la actualidad están en estudio los modelos de 400 Gbps y 1 Tbps.

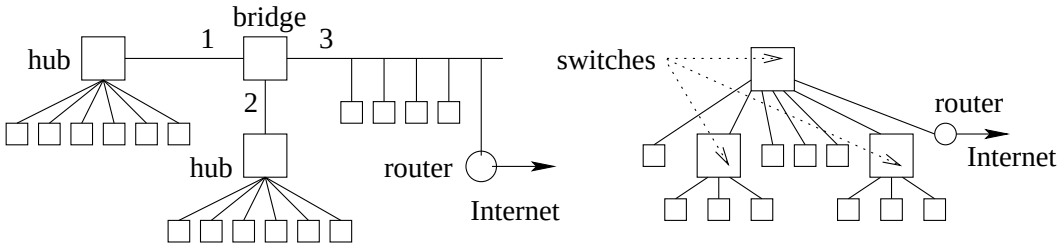
Duplex La topología en estrella con switch admite las configuraciones *half-duplex* (envíos y recepciones no simultáneos) o *full-duplex* (envíos y recepciones simultáneos). La configuración full-duplex permite duplicar la capacidad total en algunas configuraciones (200 Mbps en 100baseTX) y es útil sobre todo en servidores.

Autonegociación Ethernet. Es un procedimiento que permite hacer compatibles los modelos Ethernet de 10, 100 y 1000 Mbps en velocidades y configuración half-duplex y full-duplex. Su implementación es opcional por parte de los fabricantes. La autonegociación permite a dos tarjetas negociar para fijar la configuración que ofrezca el mejor rendimiento común. Involucra el envío de pulsos que realizan las tarjetas cuando no están ocupadas transmitiendo tramas.

2.2.5. Interconexión de LANs

Varias LANs pueden interconectarse entre sí mediante dispositivos de capa 1: concentradores (hubs), dispositivos de capa 2: switches (conmutadores) y bridges (puentes) o dispositivos de capa 3: routers.

En realidad un switch es básicamente un bridge con un número de puertos mayor. Un brigde suele tener de dos a cuatro puertos y su función es la de interconectar LANs. Un switch puede tener docenas de puertos, típicamente uno por cada host conectado. Sin embargo, además de interconectar hosts, los switches pueden interconectar LANs, por lo que han reemplazado a los bridges. Por otro lado, pueden encadenarse todos los bridges y switches que se deseen con tal que se respecten las limitaciones de distancia de los cables.



Autoaprendizaje

Los dispositivos de capa 2 (switches y bridges) con el paso del tiempo aprenden la localización de los hosts. Inicialmente realizan *difusión* de las tramas, pero cuando han aprendido la localización de un host ponen la trama sólo en el puerto de salida que lleva a dicho host.

Esto se realiza con una *tabla del switch* (o del bridge). Dicha tabla contiene entradas para algunos de los hosts de la LAN. Una entrada de la tabla contiene: (1) la dirección Ethernet de un host (2) la localización del host, es decir, el puerto del dispositivo que lleva al host y (3) el instante en que se creó esta entrada. Por ejemplo:

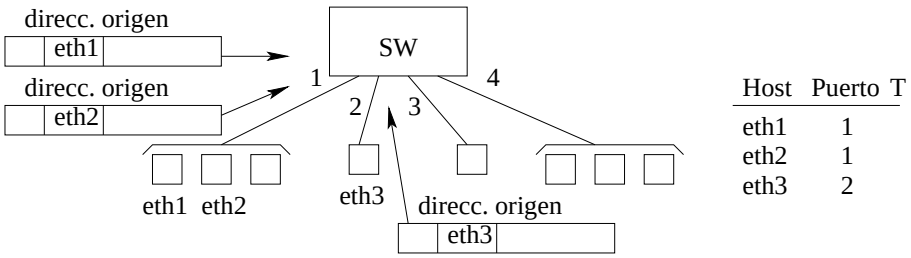
Host	Puerto	Tiempo
`00:01:03:4C:C6:39`	1	9.32
`00:E0:63:93:26:E5`	1	9.50
`00:03:BA:16:E1:70`	2	9.55

Además, switches y bridges tienen la útil característica de que su tabla se construye automáticamente.

1. Cuando el dispositivo, switch o brigde, se enchufa por primera vez, su tabla se encuentra vacía y no sabe dónde se encuentra ningún host.

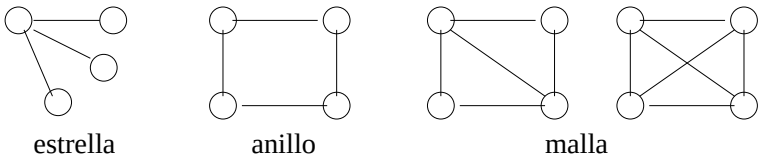
2. El aprendizaje se realiza examinando las tramas que llegan al dispositivo. La dirección Ethernet origen de la trama proporciona la identidad del host y el puerto de entrada su localización. Por último, se añade a la tabla el instante de tiempo de llegada.

3. Periódicamente se revisa la tabla y se borran las anotaciones que tienen una antigüedad mayor que unos cuantos minutos. De esta forma si un host se cambia de lugar, al cabo de unos minutos el dispositivo lo encontrará.



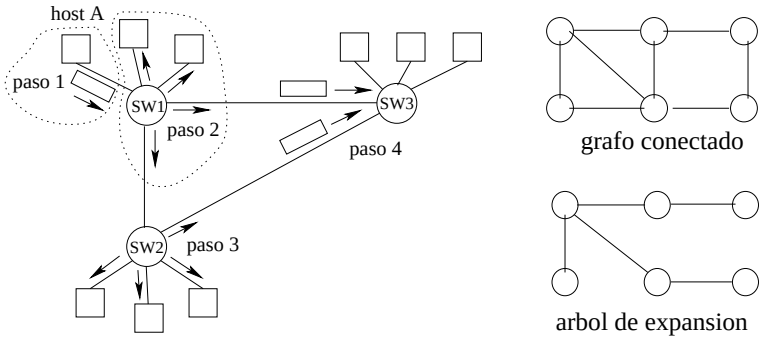
Árbol de expansión

Cuando se utilizan líneas troncales para interconectar LANs, además de la topología estrella suelen utilizarse las topologías anillo y malla. Estas tienen la ventaja de que existe más de un camino alternativo para llegar a un destino.



El algoritmo de aprendizaje del switch es efectivo si la topología de interconexión es un árbol, es decir no existe más de un camino para llegar a un destino. La existencia de caminos alternativos ocasiona inestabilidades.

Por ejemplo, en la figura de abajo, una transmisión del host A ocasiona que el switch de la derecha reciba dos copias de la trama por dos enlaces y que no sea capaz de fijar la localización del host A. Esto puede producir bucles de envío infinitos y degradar el rendimiento de la red, hasta al extremo de quedar inutilizable.



La solución a este problema es la construcción de un árbol de expansión: aunque la estructura física de las conexiones es un grafo conectado, los dispositivos pueden seleccionar un árbol lógico usando sólo una parte de los enlaces. Como el algoritmo es dinámico, si uno de los enlaces seleccionados falla, el árbol se puede reconfigurar. Los bridges y switches de gama alta incluyen un protocolo para construir el árbol de expansión.

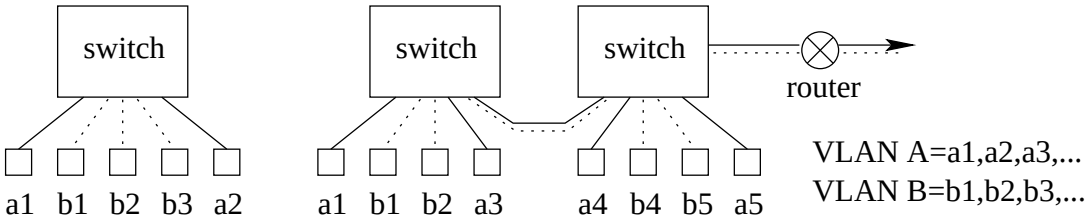
Diferencia con los routers

Los bridges y switches trabajan en la capa 2, de enlace (con cabeceras Ethernet), mientras que los routers trabajan con la capa 3, de red (con cabeceras IP). Pueden utilizarse routers para interconectar LANs, aunque suelen ser más caros que los switches. Los routers realizan un encaminamiento más flexible (protocolos RIP, OSPF, etc) y sus interfaces aíslan los *dominios de difusión* de las LANs (los broadcast Ethernet no atraviesan los routers).

Aunque los switches funcionan en la capa 2 (de enlace), existen modelos de gama alta y de nivel corporativo, denominados *switches de capa 3*, que sin llegar a ser routers incorporan alguna funcionalidad de la capa 3, por ejemplo, pueden trabajar con direcciones IP.

2.2.6. LANs virtuales (VLANs)

Las VLANs son una técnica que permite separar los hosts conectados al mismo switch en varias LANs o incluso construir LANs con hosts situados en distintas redes. Es decir, las VLANs se construyen de forma lógica, independientemente de la localización física de los hosts. En la siguiente figura mostramos dos ejemplos. En la parte de izquierda usamos un solo switch con capacidad VLAN para separar los hosts (de tipos a y b) en dos VLANs, mientras que en la parte de de la derecha asignamos los hosts a dos VLANs independientemente de su posición física en la red. Para ello todos los dispositivos de conexión de la red (switches y routers) implicados deben tener capacidad VLAN.



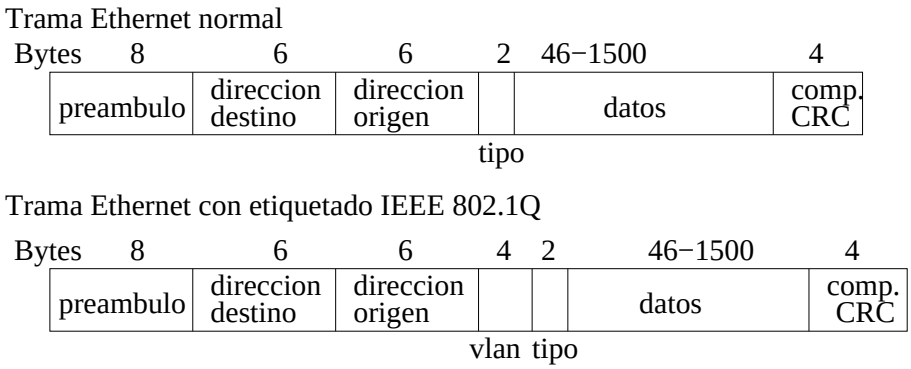
La asignación de los hosts a las VLANs puede hacerse de dos formas:

- *Estática*. Simplemente se asignan los puertos del switch a una de las VLANs y los hosts conectados a ese puerto pasan a ser automáticamente miembros de la VLAN. Los puertos de un switch se pueden configurar para pertenecer a una de las VLANs, pertenecer a todas o no pertenecer a ninguna. En la figura de arriba, los puertos que interconectan hosts han sido asignados a una VLAN concreta, mientras que los puertos que interconectan switches y routers pertenecen a todas las VLANs.

- *Dinámica*. La asignación de los puertos a las VLANs se realiza en función del host o del usuario conectado a ese puerto. Se utilizan parámetros tales como la dirección MAC o IP del host, claves de acceso, el nombre del usuario que se conecta, etc.

Después de que un puerto haya sido asignado a una VLAN, a través de ese puerto no se puede enviar ni recibir datos desde dispositivos incluidos en otra VLAN sin la intervención de algún dispositivo de capa 3. Los hosts que se conectan a los puertos no tienen que realizar ninguna operación en particular y probablemente no sean conscientes de su pertenencia a un VLAN, aparte de la capacidad de realizar o no ciertas conexiones. Las VLANs proporcionan un alto nivel de seguridad al implementar la mayor parte de las operaciones en hardware. Al igual que con los routers, el *dominio de difusión* (es decir, el broadcast Ethernet) queda limitado al interior de la VLAN.

Para la comunicación de switches y routers con capacidad VLAN se han definidos los correspondientes protocolos. Algunos de esos protocolos son propietarios (por ejemplo, el propuesto por CISCO), y otros estándar. El protocolo de etiquetado IEEE 802.1Q es el más común para la formación de las VLANs. Se caracteriza por modificar las tramas Ethernet de forma que se añaden 4 bytes a continuación de las direcciones MAC para incorporar la información del protocolo (además de modificar el campo *tipo* y recalcular el CRC). Estos 4 bytes incluyen entre otros el identificador de la VLAN y la prioridad de la trama (que puede ser utilizada para proporcionar calidad de servicio). El tamaño máximo de la trama pasa de 1518 a 1522 bytes.



2.3. LAN inalámbrica

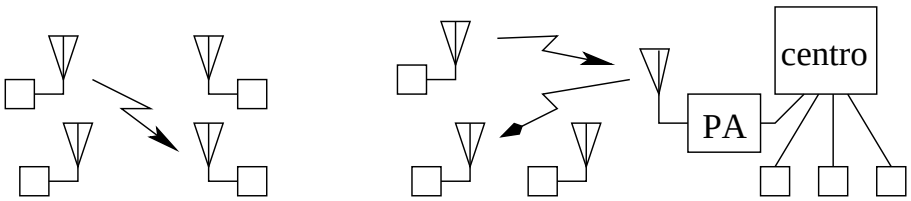
Una red Ethernet puede gestionar tanto transmisiones de cable como inalámbricas. La ventaja de la redes inalámbricas es que no necesitan infraestructura de ningún tipo, mientras que su principal desventaja es una velocidad de transmisión menor que las redes de cable conmutadas, sobre todo cuando el número de hosts es elevado. A las LAN inalámbricas se les denomina comúnmente Wi-Fi (Wireless Fidelity) o WLAN y corresponden a la especificación IEEE 802.11, siendo los modelos actuales 802.11af (Wi-Fi 5) y 802.11ax (Wi-Fi 6), que suponen un gran avance con repecto a los modelos anteriores.

Generación	Años	Modelo	Velocidad máxima teórica
1	1987-1988	802.11a	2 Mbps
2	1999-2001	802.11b	11 Mbps
3	2002-2006	802.11g	54 Mbps
4	2007-2016	802.11n	450 Mbps
5	Actual	802.11af	7 Gbps
6	2020-	802.11ax	10 Gbps

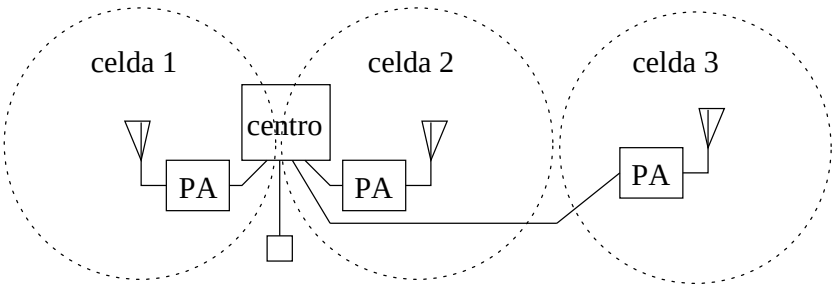
Configuraciones

Una WLAN admite dos tipos de configuración básica:

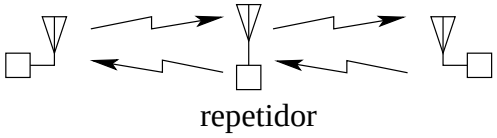
- **Ad-hoc**. Es una red de iguales con varios hosts que pueden transmitir entre sí y sin conexión con el exterior.
- **Con punto de acceso** (o de *acceso nómada*, *infraestructura* o *managed*). Se dispone de una estación base o punto de acceso (PA) por la que pasan todas las transmisiones inalámbricas (aquí no hay conexión de radio directa entre hosts) y que enlaza con la red de cable.



Una WLAN de **celdas múltiples** consta de una troncal cableada que conecta los servidores y los puntos de acceso (PA, *access point*). Cada PA da servicio a un número de hosts móviles, distribuyendo el espacio en celdas. Aunque el solapamiento de celdas en necesario para permitir el tránsito de celdas sin interrupciones, es deseable que este sea sólo del 20 o el 30 %.

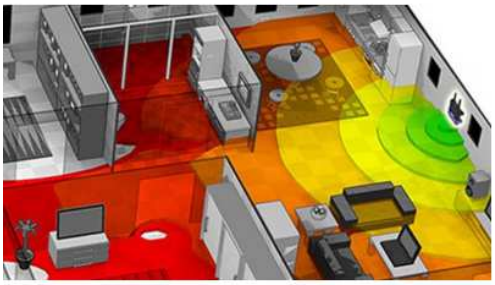


Por último, existen también **repetidores** (wireless range extender) que se limitan a retransmitir todo lo que reciben. Permiten realizar transmisiones a mayor distancia pero con la desventaja de que el tráfico se duplica.



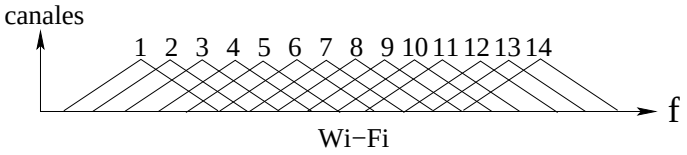
2.3.1. Capa física

Bandas de frecuencia. Es posible la transmisión por infrarrojos o microondas. Las microondas pueden atravesar las paredes, si bien sufren bastante atenuación cuando lo hacen. Los infrarrojos no pueden hacerlo.



Las bandas de frecuencia de microondas típicas son dos: las de 2,4 GHz y 5 GHz, ambas de transmisión sin licencia.[3] Todas las redes inalámbricas usan estas bandas de frecuencia por lo que puede haber solapamiento de redes en algunos lugares. Además, estas bandas se comparten con otros muchos dispositivos inalámbricos con lo que se producen interferencias, sobre todo la banda de 2,4 GHz que está muy saturada y por lo tanto es muy ruidosa. La banda de 5 GHz es menos usada y además tiene un mayor ancho de frecuencia.

La banda de 2,4 GHz se divide en 14 canales que se solapan en gran parte, por lo que canales próximos se producen interferencias entre ellos. En Europa, los canales más óptimos a usar en puntos de acceso cercanos o adyacentes para eliminar el solapamiento entre canales y minimizar las interferencias son tres: el 1, el 7 y el 13 (el 14 está prohibido en España).[4] La selección del canal de transmisión se hace desde el PA.



Alcance. El alcance de la comunicación inalámbrica depende del entorno. En el exterior, es de 100 a 300 m, mientras que en el interior va de 35 a 100 m dependiendo de la estructura del edificio, material de construcción, densidad de objetos, etc. Las condiciones de propagación en el interior son bastante malas por la absorción de las superficies y la interferencia causada por los ecos. Puede también haber zonas de sombra en las que no se pueda alcanzar el PA.

Los modelos 802.11ac y 802.11ax permiten focalizar las señales, de forma que el dispositivo es capaz de determinar la dirección en la que se encuentra el

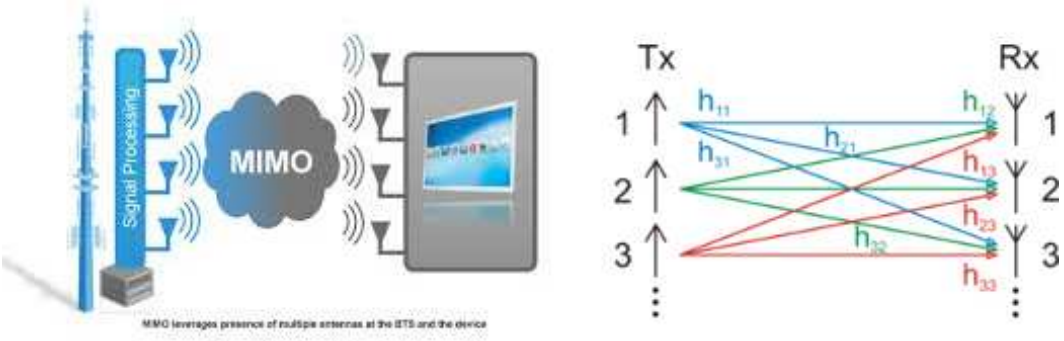
[3]La banda de 2,4 MHz abarca en Europa el rango 2400-2483,5 MHz, mientras que la de 5 GHz abarca 5150-5350 MHz y 5470-5725 MHz.

[4]Por su parte, en la banda de 5 GHz se permite el uso de los canales 36-64 y 100-140.

destinatario y focalizar la señal justo en esa dirección, al contrario que los modelos anteriores, que radían en todas direcciones.

Velocidad. La velocidad máxima fijada para el modelo 802.11ax (que también se denomina Wi-Fi 6 o Wi-Fi Gigabit) es de 10 Gbps. Pero esta velocidad sólo se puede alcanzar en condiciones ideales: cuando no hay interferencias y para distancias cortas entre antenas. Las velocidades conseguibles en la práctica para el modelo 802.11ax están en torno a 1 Gbps. Si no puede conseguirse la velocidad máxima, automáticamente se reduce la tasa de transmisión, pudiendo bajar incluso a 1 Mbps.

Para obtener esta velocidad usa el agregado de ocho flujos de datos independientes de 1,25 Gbps cada uno, que se transmiten con la correspondiente antena (ocho antenas en total). Está técnica se conoce como MIMO (multiple entrada, múltiple salida). Los dispositivos más pequeños como los móviles suelen tener una sola antena, pero pueden verse beneficiados los tablets (que pueden tener de dos a cuatro antenas) y los portátiles, televisores y routers 802.11ax (que pueden llegar a tener de cuatro a ocho).



2.3.2. Capa de enlace

Escaneo. La subcapa MAC incluye la búsqueda de un PA o de otros hosts. El PA periódicamente envía tramas *baliza* para anunciar su presencia y otros parámetros como su identidad (ESSID), temporización, velocidad, etc. Estas tramas son enviadas a la dirección de broadcast (FF:FF:FF:FF:FF:FF) usualmente cada 100 msg y a la velocidad de 1 Mbps para asegurar que pueden recibirse incluso en las condiciones más ruidosas. Los hosts están continuamente escuchando

todos los canales de radio y las balizas para elegir el mejor PA con el asociarse. Dos métodos son válidos y los hosts eligen el que más les conviene:

- *Escaneo pasivo*. Los hosts esperan justo a recibir las balizas.
- *Escaneo activo*. Implica dos fases:

  (a) El host envía una trama *prueba*.

  (b) Todos los PAs a su alcance responden con una trama *respuesta a prueba*.

El escaneo pasivo es un proceso continuo y los hosts pueden asociarse o separarse de los PA por cambios en la intensidad de la señal producidos, por ejemplo, por el movimiento. Si un host se asocia a un nuevo PA, este PA le indica el cambio al antiguo a través de la red de cable.

En las redes Ad-hoc no hay punto de acceso y parte de su funcionalidad tienen que realizarla los hosts. Por ejemplo, el primer host que se activa comienza a enviar balizas y cualquier otro host puede unirse si acepta los parámetros establecios por el primero. En el caso de que este host deje de enviar balizas, cualquier otro host deberá ocupar su lugar.

Asociación. El acuerdo implica dos fases: (a) El host selecciona uno de los PA y le envía una trama *solicitud de asociación* (association request). (b) El PA responde con una trama *respuesta a asociación* (association response).

Autentificación. El acceso de un host a la red puede ser libre, en función de la dirección Ethernet del host o mediante claves, que pueden ser iguales o diferentes para cada uno de los hosts. El protocolo de autentificación más utilizado es WPA2 (*Wi-Fi Protected Access*), usando claves PSK (Pre-Shared Key) en el caso de las redes personales y un servidor RADIUS en el caso empresarial. Para gestionarla se emplean tramas especiales de *autentification*.

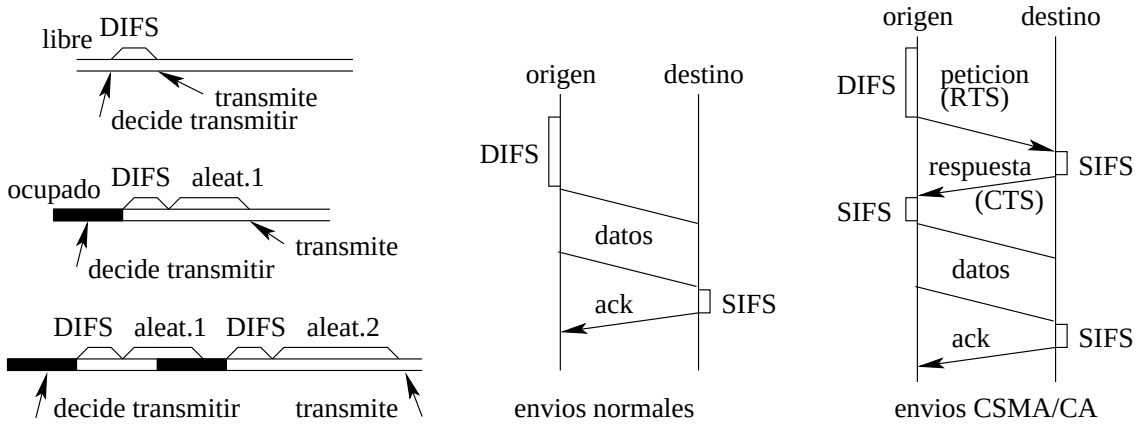
Protocolo de contienda. El protocolo de contienda de la red inalámbrica es CSMA, aunque algo distinto al de una Ethernet de cable, puesto que las condiciones de propagación en el espacio son bastante peores que en un cable, debido a mayores niveles de atenuación, ruido e interferencias.

- **Transmisión**. Un host que quiere transmitir sondea el medio durante una tiempo de ranura grande (DIFS, en la figura) y si durante todo este tiempo el medio permanece libre a continuación transmite.

  Si el medio está ocupado (bien porque el host lo encontraba inicialmente así o porque este hecho sucede durante la ranura) espera hasta que se desocupe más una nueva ranura y una cantidad aleatoria de tiempo. Si el medio continúa libre, el host puede transmitir.

  Si, por el contrario, el medio es ocupado durante el periodo de espera, el contador se para comenzando una nueva espera cuando el medio quede

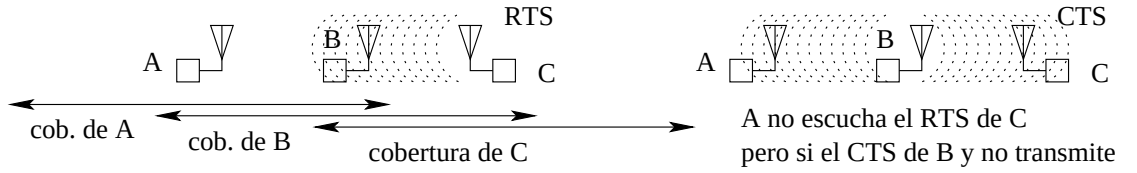
libre. Para la elección del tiempo aleatorio se usa un algoritmo de *espera exponencial binaria* que genera tiempos cada vez mayores.



- **Asentimientos**. No se incluye la detección de colisiones, puesto que ésta no resulta práctica en las transmisiones de radio. La señales radiadas se atenúan rápidamente y además el ruido del medio es elevado, por lo que es muy difícil detectar una colisión. En su lugar, se utilizan los asentimientos (ACK) para comunicar que el envío se completó satisfactoriamente. Antes de enviar el ACK se espera una ranura corta (SIFS en la figura). Al ser menor el tiempo de espera para los asentimientos que para las tramas de datos, se asegura que los primeros tengan una mayor prioridad.

- **CSMA/CA** (Acceso múltiple por detección de portadora/con evitación de colisiones, *Collision Avoidance*). Con esta técnica, un host puede asegurar que su trama de datos se transmitirá enviando primero una trama de petición de envío (denominada RTS, Request To Send). El host destino deberá responder si está o no dispuesta a la transmisión (con una trama denominada CTS, Clear To Send). Todos los demás hosts deberán esperar hasta que la transmisión de datos pedida se complete.

  Esta técnica resuelve el problema del **host oculto**. En la siguiente figura, el host C está oculto para el host A, pues no recibe sus transmisiones y podría interrumpirlas con las suyas propias. Para evitar esto, cuando el host C desea transmitir al host B, envía un RTS. El hosts B le devuelve un CTS, el cual es también recibido por el host A, que queda informado que va ha realizarse una transmisión entre C y B.

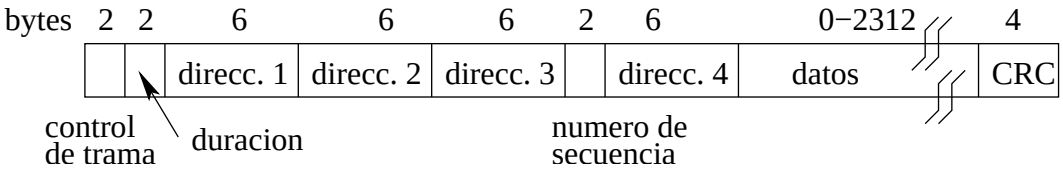


Wi-Fi multimedia. Este protocolo opcional se denomina Wi-Fi Multimedia

(WMM) o Wireless Multimedia Extensions (WME), del standard IEEE 802.11e. Este protocolo permite configurar la red para que parte de los hosts tengan aseguradas una ranuras de tiempo para transmitir, mientras que el resto compite por las ranuras libres usando el protocolo CSMA. Proporciona una QoS básica y permite prioriorizar el tráfico de acuerdo a 4 categorías: voz, vídeo, best effort y background. Es un modo opcional y muchas tarjetas no lo implementan.

Ahorro de energía y fragmentación. Opcionalmente se establecen protocolos para gestionar el ahorro de energía. Por ejemplo, el punto de acceso puede guardar las tramas en una memoria temporal para los hosts que se encuentren en el modo de ahorro de energía. También se establecen procedimientos para la fragmentación de tramas, pues puede que en el cable se acepten longitudes de trama mayores a las que permite el acceso inalámbrico.

Tramas. Existen tres tipos de tramas: *gestión* (prueba, respuesta a prueba, solicitud de asociación, respuesta a asociación, baliza y autentificación), *control* (petición de envío y respuesta de envío) y *datos*, que pueden llevar o no asentimientos superpuestos. El formato de la trama se muestra a continuación (no se han incluido los preámbulos):

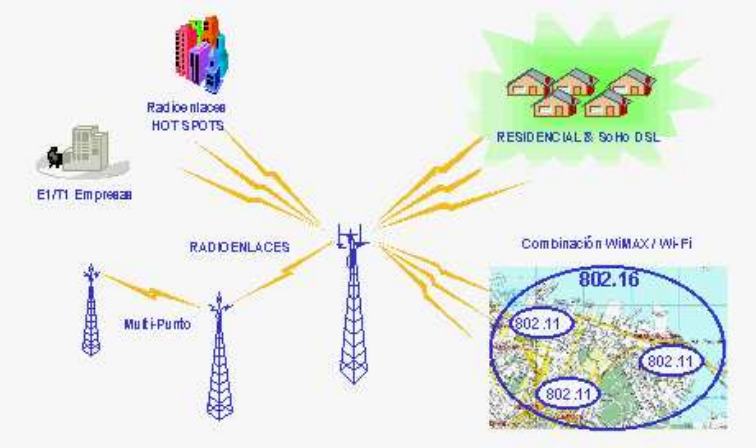


La trama contiene 4 direcciones MAC (Ethernet): dos de ellas son las direcciones origen y destino como es usual. Las dos restantes se usan si hay transmisiones hacia puntos de acceso. Si la transmisión incluye un punto de acceso, se añade como tercera dirección la del punto de acceso, y si se incluyen dos puntos de acceso, entonces se añade una cuarta.

El caso de 4 direcciones Ethernet puede explicarse como sigue: el host de dirección *eth1* realiza una transmisión por ondas de radio usando un PA de dirección *eth2*. Este PA está conectado a través de una red Ethernet de cable a un segundo PA de dirección *eth3*. Finalmente, este PA retransmite la trama por ondas de radio al host destino de dirección *eth4*.

2.4. MAN inalámbrica

El estándar IEEE 802.16 o WiMAX (Worldwide Interoperability for Microwave Access) especifica un interface inalámbrico de banda ancha para las redes metropolitanas. La versión 802.16a proporciona accesos concurrentes en áreas de hasta 50 kilómetros de radio. Las transmisiones están optimizadas para enlaces de gran distancia por lo que puede tolerar retrasos más largos y variaciones de retraso.



La velocidad máxima es de 1 Gbps, pero sólo para distancias cortas y con línea de vista (sin obstáculos). Al igual que ocurre con el ADSL, al aumentar la distancia la velocidad se reduce y para distancias de 50 km la velocidad proporcionada es menor de 70 Mbps.[5] Las antenas son muy direccionales, por lo que se pueden tener accesos de radio independientes a distintos puntos; en caso contrario la tasa de transmisión ha de repartirse.

Los usos de WiMAX incluyen configuraciones punto a punto y multipunto (como se muestra en la figura). Se usa para la interconexión de redes y para proporcionar acceso a Internet inalámbrico a cientos de hogares, sustituyendo al ADSL. En este caso requiere únicamente del despliegue de estaciones base capaces de dar acceso a Internet a unos 200 hosts. En la actualidad en España existen despliegues comerciales, por ejemplo, en zonas de Galicia y Asturias. WiMax se ha incorporado recientemente a la cuarta generación de comunicaciones móviles (4G) y existe una versión que permite el desplazamiento del usuario. Existen además tarjetas que se pueden insertar en ordenadores portátiles para permitir la conexión a una red WiMax donde haya señal.

En cuanto al protocolo de acceso al medio, mientras que en Wi-Fi los hosts compiten entre sí para acceder al punto de acceso, en WiMAX una vez que los hosts se ponen en contacto con la estación base, ésta les asigna una ranura de tiempo reservada para las transmisiones. La ranura de tiempo puede aumentar o disminuir, pero siempre está disponible. Este mecanismo permite al punto de acceso ofrecer QoS.

[5]WiMAX puede utilizar varias bandas en el rango 2-11 GHz (bandas de 2,4 y 5 GHz sin licencia y bandas 3,5 GHz y 10,5 GHz con licencia.

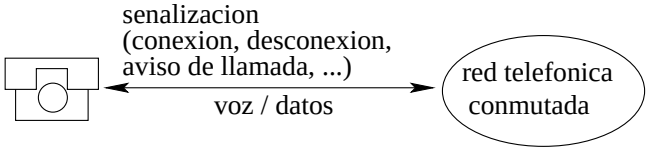
Capítulo 3

Redes de área amplia

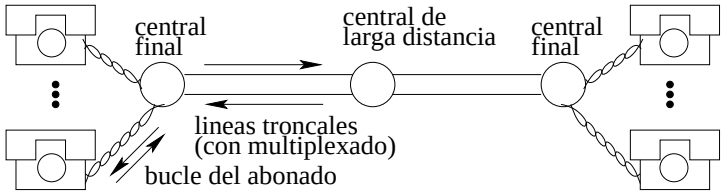
Las redes se pueden clasificar como redes de área amplia (WAN, Wide Area Network), redes de área metropolitana (MAN, Metropolitan Area Network) y redes de área local (LAN, Local Area, Network). En este capítulo nos ocuparemos de las redes de área amplia.

3.1. Red telefónica conmutada

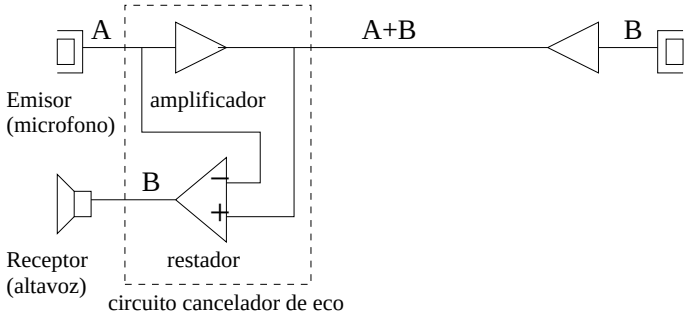
La Red Telefónica Conmutada (RTC) o Public Switched Telephone Network (PSTN) es el conjunto mundial de las redes telefónicas de conmutación de circuitos. Por el sistema telefónico se transmiten tanto las señales de control (señalización) como la información del usuario (voz o datos). Para conectar un teléfono con otro, mediante señalización la llamada se enruta a través de numerosos interruptores en las centrales telefónicas que operan a nivel local, regional, nacional o internacional. La conexión que se establece entre los dos teléfonos, denominada circuito, permanece activa hasta el momento de la desconexión.



Dentro de la red telefónica pueden distinguirse dos partes: el bucle del abonado (subscriber loop) y las líneas de larga distancia o troncales. El bucle del abonado es la parte de la red telefónica que conecta al abonado con la central telefónica más cercana. Vamos a distinguir entre el bucle del abonado clásico de par trenzado y el más moderno que incluye fibra óptica. En la siguiente figura se muestra el esquema clásico.



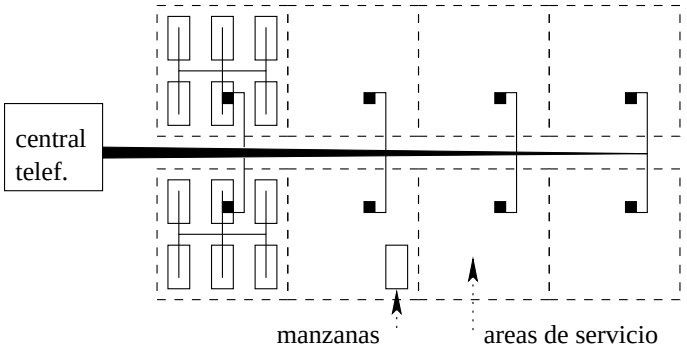
Cancelación de eco. Es una técnica que se usa para emitir y recibir a la vez en el bucle del abonado sobre el mismo par trenzado (dos hilos). Se emplea también en Gigabit Ethernet.



En el circuito emisor tenemos la señal a emitir (A), que conocemos puesto que se genera en el dispositivo. En la línea tenemos las dos señales sumadas (A+B). Por tanto solo quedará restar las señales de la línea con la señal emitida, obteniéndose la señal recibida completamente separada (B). Para que esto funcione bien, la circuitería deberá estar bien ajustada, pues en caso contrario se producirán los molestos ecos.

3.1.1. Bucle del abonado de par trenzado

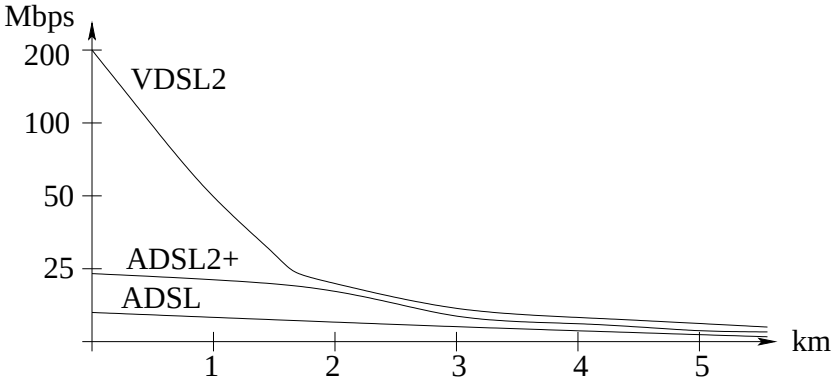
En la telefonía fija cada aparato telefónico está conectado a una central mediante un par trenzado sin apantallar (cable UTP de 0,4 o 0,5 mm) independiente. Por el mismo cable por el que se transmite la voz y se envía el número marcado se recibe también la alimentación, las distintas señales de estado (tono dial o invitación a marcar, llamando, comunica, línea saturada, etc) y la señal de timbre. Cada central suele gestionar unos 10 000 teléfonos. A cada hogar se dirige un par trenzado, los cuales se agrupan en mazos que se hacen más gruesos al acercarse a la central telefónica. En las aceras de algunas calles se colocan una cajas denominadas *interfaces de áreas de servicio* (repartidores de barrio) que agrupan unos 500 pares trenzados.



La mayoría de los pares trenzados que conectan las centralitas locales de las compañías telefónicas con sus clientes fueron instaladas hace ya algunas décadas y no han sido sustituidas desde entonces. Estos pares hacen bien la función para

la cual estaban inicialmente diseñados, llevar las señales de voz. La situación no es tan buena cuando se utilizan para transmitir datos. El principal efecto es la reducción de la velocidad de transmisión conforme aumenta la longitud del cable.

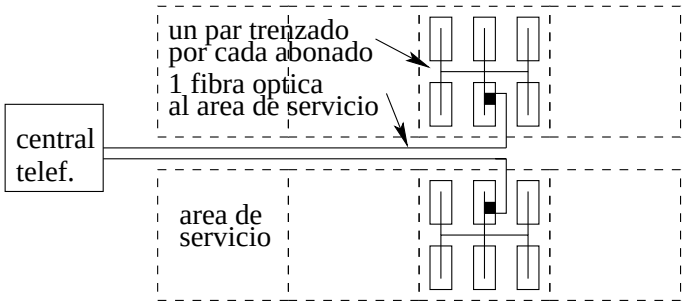
En la siguiente figura se muestra la velocidad alcanzable en ADSL/VDSL en función de la distancia a la central. Por ejemplo, a 3 km de la central la velocidad máxima alcanzable es de unos 10 Mbps.



3.1.2. Bucle del abonado FTTx

FTTx (Fiber To The x) es un término genérico que designa la incorporación de fibra óptica al bucle del abonado que sustituya total o parcialmente al par trenzado. La fibra óptica resuelve todos los problemas de atenuación, distorsión y ruido y permite velocidades mucho más altas de transmisión. FTTx puede ser de los siguientes tipos:

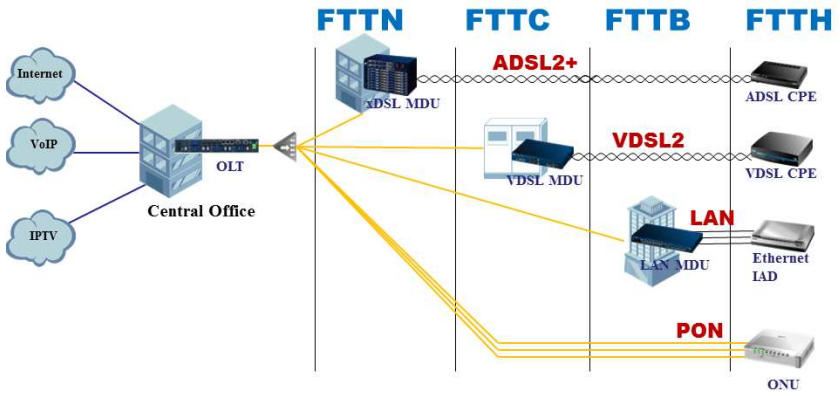
1. FTTN (Fiber To The Node). La fibra óptica llega hasta el interface del área de servicio, a partir del cual y hasta hogar se continúa con cable de cobre. Puesto que la capacidad de transmisión de una fibra óptica es muy superior a la del par trenzado, una sola fibra puede multiplexar la transmisiones de un gran número de abonados. Usando este esquema la conversión del bucle del abonado clásico es bastante sencilla puesto que solo hay que sustituir la parte que comunica la central con el interface del área de servicio por una fibra óptica, dejando intactos los pares trenzados que llegan hasta los abonados. Permite ADSL2+ en muy buenas condiciones.



2. FTTC (Fiber To The Cabinet). Similar al anterior, pero la cabina o armario de telecomunicaciones se coloca más cerca del usuario, normalmente a menos de 300 metros. Permite velocidades de VDSL2.

3. FTTB (Fiber To The Building). En este caso la fibra óptica termina en la base del edifico y se continúa hasta los hogares con cable de cobre (par trenzado o coaxial).

4. FTTH (Fiber To The Home). La fibra óptica llega hasta el interior de la casa del abonado.



Por el precio de instalación FTTx solo es rentable para el Triple Play: telefonía, internet de banda ancha y televisión de pago. Mediante splitters se multiplexa el tráfico telefónico, de datos y de televisión de los diferentes usuarios. En España, tenemos los proveedores de fibra: Movistar, Vodafone/Ono, Orange/Jazztel, MásMóvil y Euskaltel/R, entre otros.

Red Óptica Pasiva Gigabit (GPON)

Es una red óptica pasiva (esto es, sin necesidad de alimentación) que permite eliminar todos los componentes activos. La utilización de sistemas pasivos, incluidos los splitters, reduce considerablemente los costes de las redes FTTH, pues no son necesarios cables de alimentación. GPON soporta todo tipo de servicios (voz, Ethernet, ATM), distancias de 20 km y velocidades superiores a 1 Gbps.

Los elementos de GPON son los siguientes:

1. Módulo OLT (Terminal de la Línea Óptica, Optical Line Terminal) que se encuentra en el nodo central.

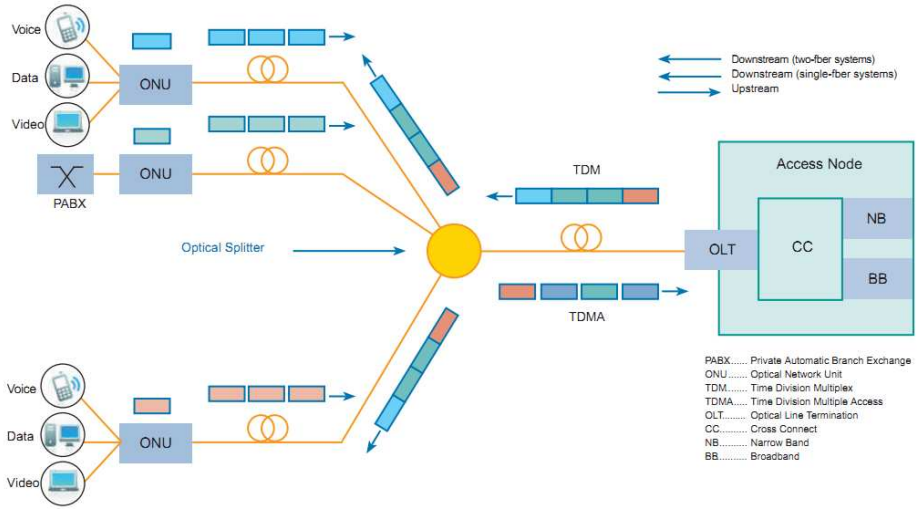
2. Divisor óptico (splitter), que divide un haz de luz en copias idénticas o bien suma varios haces de luz en uno.

3. Módulo ONU (Unidad de Red Óptica, Optical Network Unit), ubicado en cada domicilio de usuario.

Para multiplexar las distintas transmisiones y los distintos usuarios se utiliza TDM (Time Division Multiplexing) y TDMA (Time Division Multiplexing Access).

- En el canal descendente el modulo OLT de la central telefónica envía una serie de contenidos multiplexados en tiempo (TDM) que son recibidos por todos los usuarios, cada uno de los cuales selecciona los que son destinados a el.
- En el canal ascendente los diferentes usuarios transmiten contenidos a la central telefónica. Por este motivo es necesario sincronizar los envíos para que no colisionen entre ellos. Por ello se usa TDMA controlados por la unidad OLT, la cual indica a las diferentes ONUs que envíen la información en diferentes ranuras (TDM Access). Esta sincronización de todos los dispositivos no es necesaria en el canal descendente.

Para operar simultámente en los canales ascendente y descendente se utilizan longitudes de onda diferentes en los dos sentidos de la misma fibra. Esto se denomina WDM (Wavelength Division Multiplexing) o multiplexado por división de la longitud de onda.



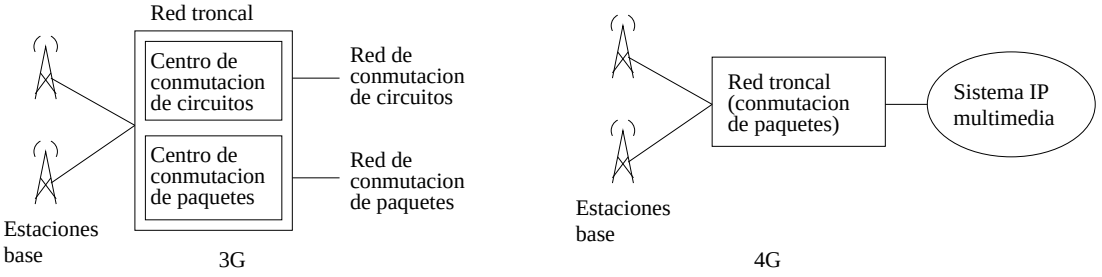
Protocolo de Inicio de Sesión (SIP)

El protocolo de inicio de sesión (SIP) es un protocolo de comunicaciones para señalizar y controlar sesiones de comunicación multimedia, tales como llamadas de voz y vídeo. La aplicación más común de SIP es la realización de llamadas telefónicas convencionales usando la red de datos y el protocolo VoIP. De esta forma en el lazo de abonado solo es necesario instalar la red de datos que será usada también por el teléfono fijo. Las troncales SIP (SIP trunking) sustituyen a la anterior red telefónica digital (RDSI).

3.2. Telefonía móvil

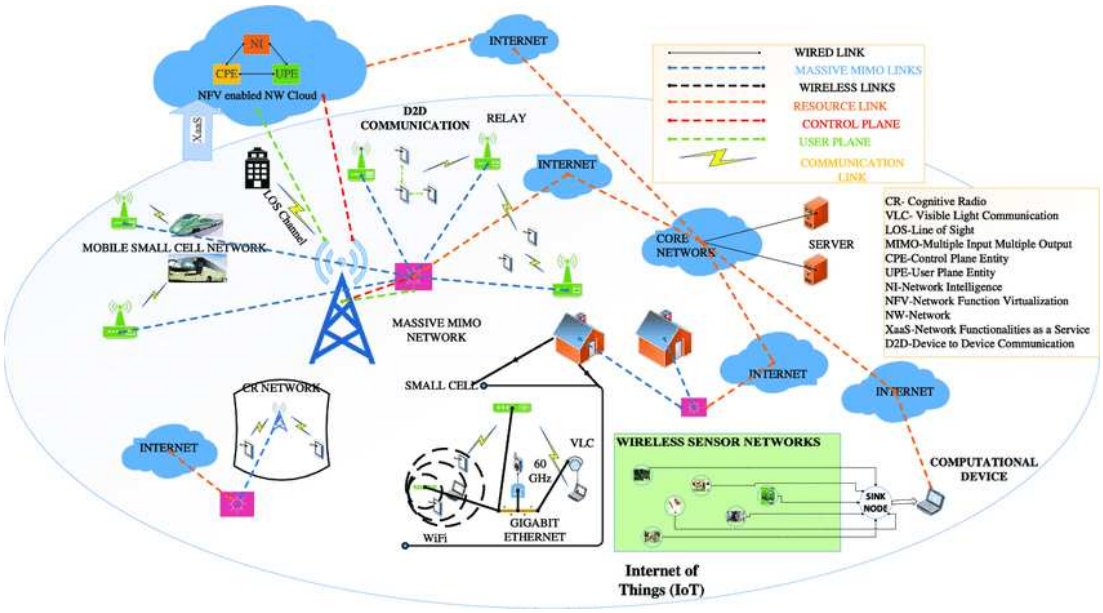
3.2.1. Acceso móvil de quinta generación (5G)

- La **primera generación** de móviles proporcionó servicios de voz analógicos a los usuarios, como por ejemplo el estándar TACS (Moviline, en España).
- La **segunda generación** proporcionó servicios de telefonía digital y de transmisión de datos a baja velocidad, siendo el estándar europeo GSM, *Sistema General de Móviles* (Movistar, Vodafone y Amena en España). La velocidad de transmisión de datos estándar de GSM es de 9,6 kbps, pero puede ampliarse con la extensión GPRS que consiste en la agregación de los canales GSM disponibles proporcionando velocidades del orden de 56 kbps.
- La **tercera generación** (3G) de móviles tuvo como objetivo la introducción de capacidades multimedia en las comunicaciones móviles con el estándar UMTS (Telefónica, Vodafone, Orange y Yoigo en España, además de otras empresas revendedoras de servicios sin red propia). Introdujo un acceso a Internet de calidad a los usuarios móviles. Se caracteriza por incorporar dos subsistemas separados, uno dedicado a las transmisiones telefónicas (que funciona con una red de conmutación de circuitos) y otro dedicado a la transmisión de datos (que funciona con una red de conmutación de paquetes IP).
- La **cuarta generación** (4G) de telefonía móvil se basa en el estándar LTE (Long Term Evolution) y utiliza como base el protocolo IP para todo tipo de transmisiones, añadiendo calidad de servicio para la transmisión multimedia y en tiempo real. Es decir, tanto las transmisiones telefónicas como los datos se gestionan con un único sistema unificado de transmisión de paquetes IP.



- La **quinta generación** (5G), introducida en 2020, da un paso más hacia la conexión universal de todo tipo de dispositivos. Se basa en los conceptos de *todo en la nube* (all cloud) y en la *virtualización de la red* (network slices) en la que la infraestructura hardware y de control puede configurarse para proporcionar redes virtuales con la funcionalidad requerida para cada tipo de

conexión (muticonectividad). Por otro lado, incorpora una arquitectura de seguridad nativa. Además de tráfico telefónico, conexión a Internet y contenido multimedia, proporciona la infraestructura que necesita la internet de las cosas, por ejemplo, *smart cities* con todo tipo de sensores recopilando información (cámaras de vigilancia, control de semáforos, iluminación, etc), posicionamiento, conducción autónoma, domótica, control de máquinas en fábricas, etc.



3.2.2. Telefonía celular

Las consideraciones que hay que tener en cuenta para diseñar un sistema de telefonía móvil son las siguientes:

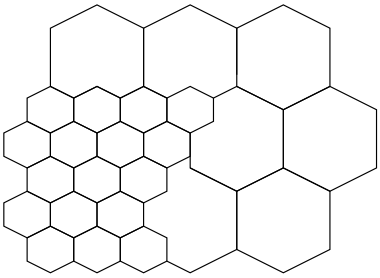
1. No es posible asignar una frecuencia distinta a cada uno de los teléfonos móviles. En España hay unos 55 millones de líneas de telefonía móvil, más que habitantes.

2. El alcance de un móvil es limitado. Debemos tener estaciones base que atiendan a los teléfonos móviles cada pocos km.

3. El móvil puede cambiar de posición. En este caso puede cambiar también la estación base que atiende al móvil.

Teniendo en cuenta estos requerimientos se diseña el sistema de telefonía móvil. El área cubierta por el sistema de telefonía se divide en celdas, teóricamente de forma hexagonal, aunque en la práctica de forma más irregular (en las autopistas, por ejemplo, las celdas serán alargadas). El tamaño de una celda corresponde al área cubierta por una estación base.

De aquí se desprende que cuanto más pequeñas sean las celdas a más teléfonos móviles puede atender el sistema. Por esta razón las celdas son más pequeñas en zonas de gran aglomeración: aeropuertos, espectáculos, etc (radio 100 m), medianas en zonas urbanas (radio 1 km), y más grandes en las zonas rurales (radio 20 km). Adicionalmente en 4G la estación base puede radiar señales a subzonas de la celda y en 5G se utiliza la tecnología MIMO.



- **Ubicación**. En cada celda hay una estación base que se comunica con todos los teléfonos móviles localizados en esa celda. Cada estación base tiene asignada una frecuencia de identificación en la cual emite continuamente. Cuando un móvil se enciende busca la frecuencia de identificación de la estación base más cercana (teóricamente la de mayor intensidad) y le transmite un mensaje anunciando su número telefónico.

- **Emisión**. Cuando un móvil desea hacer una llamada envía un mensaje de petición de llamada a la estación base, la cual entonces le asigna una frecuencia de transmisión disponible.

- **Recepción**. La estación base difunde las llamadas por toda la celda y todos los teléfonos móviles están escuchando continuamente para ver si les corresponde alguna.

- **Movimiento**. Por otro lado, mientras el móvil está encendido escucha periódicamente la frecuencia de identificación de la estación base que la atiende. También testea todas las frecuencias de identificación posibles y mide sus intensidades. Si el teléfono cambia de celda, obviamente ahora estará más cerca de una nueva estación base y la frecuencia de identificación de la nueva estación base será de mayor intensidad que la de la celda antigua. Entonces el teléfono deduce que ha cambiado de celda y anuncia su presencia a la nueva estación base.

- **Encaminamiento**. Es importante conocer la ubicación de todos los teléfonos móviles, de manera que las llamadas puedan encaminarse cuando se llame a un móvil. Para ello la localización de cada móvil se traza continuamente mediante el uso de ordenadores y bases de datos, a los cuales tienen acceso todas las estaciones base.

3.2.3. Gestión de la movilidad

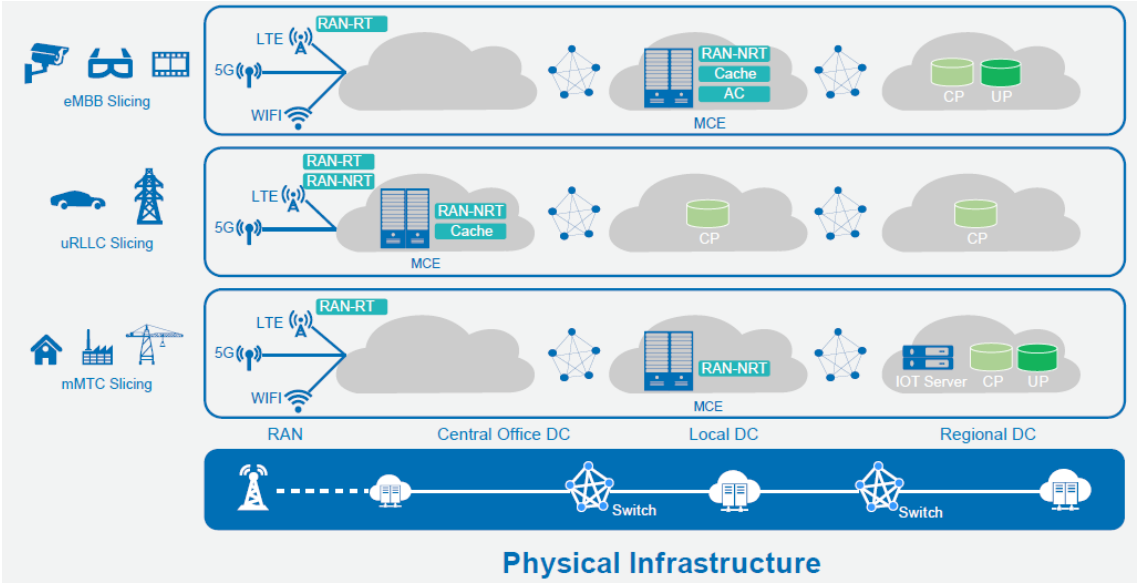
Alta. Por cada área geográfica (y compañía) existen dos registros de usuarios: el registro de propios y el de visitantes. El usuario está incluido permanentemente en el registro de propios del área geográfica en la que se dio de alta. Cuando el móvil se desplaza a un área geográfica distinta a la propia, sus datos se copian desde el registro de propios al registro de visitantes del área visitada. Para que sea posible la localización del móvil, su posición se anota en el registro de propios en el que está suscrito el usuario.

Encaminamiento de una llamada. Lo primero que hace la red cuando recibe una llamada para un móvil es dirigirse al registro de propios en el que está suscrito el usuario, el cual localiza los datos del abonado móvil, así como el registro de visitantes en el que está incluido en ese momento. A continuación la llamada se reencaminará al registro de visitantes.

Cobertura. La cobertura ofrecida por el operador a un abonado incluye aquellos países en los cuales este operador ha establecido acuerdos de itinerancia internacional con otros operadores.

3.2.4. Arquitectura

La arquitectura de un sistema 5G se muestra en la siguiente figura.



La infraestructura física consta de 3 tipos de elementos:

1. **Red de acceso de radio** (Radio Access Network, RAN). Está constituida por la estaciones base que controlan la realización, encaminamiento y mantenimiento de las transmisiones con los móviles. Por una parte es un transmisor de radiofrecuencia constituido por el equipo de modulación, amplificación y antenas. Por otra realiza la asignación y gestión de los canales

de radiofrecuencia, cifra las señales, envía información de control a los móviles, etc. Estas funciones tienen una carga computacional elevada y deben ser realizadas en tiempo real. Soporta los protocolos 4G, 5G y Wi-Fi.

2. **Red troncal** (Switches). Es la parte de la red que realiza el tráfico de los paquetes IP a través de la red de cable.

3. **Centros de datos** (Data Center). Son los elementos que proporcionan los servicios a los usuarios, con una arquitectura descentralizada de tipo nube (cloud). Por ejemplo, contienen las bases de datos de abonados, contenidos multimedia, etc.

Estos elementos hardware se configuran mediante virtualización para proporcionar tres tipos de redes diferentes (network slices). De esta forma se consigue que una única infraestructura de red soporte diferentes escenarios. En concreto, se definen los tres siguientes:

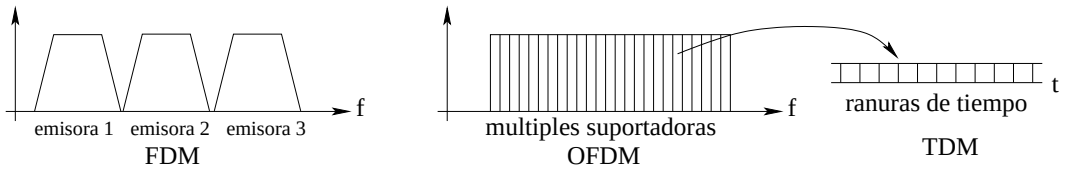
1. *Ancho de banda móvil mejorado* (Enhanced Mobile Broadband, eMBB). Proporciona conexiones digitales de gran capacidad a los usuarios móviles, incluyendo llamadas telefónicas, acceso a Internet, vídeos de alta definición, realidad aumentada, etc.

2. *Comunicaciones confiables de baja lantencia* (Ultra-Reliable and Low Latency Communications, URLLC). Están orientadas a las aplicaciones de la industria que requieren operaciones rápidas en tiempo real, como por ejemplo, la conducción asistida y el control remoto.

3. *Comunicaciones masivas de máquinas* (Massive Machine Type Communications, mMTC). Centrados en servicios D2D (dispositivo a dispositivo) con altos requerimientos de densidad, por ejemplo ciudades inteligentes (smart cities) y agricultura inteligente (smart agriculture).

3.2.5. Tecnología

Debido a que las aplicaciones están orientadas a la conmutación de paquetes es necesario optimizar este tipo de transmisiones. Esto implica una gestión eficiente de las variaciones en las tasas de transmisión. Como consecuencia de ello se modifica el rígido esquema de asignación de canales de multiplexión en el tiempo y en frecuencia. Se sigue utilizando multiplexión en frecuencia, pero cada portadora se divide en un elevado número de subportadoras que pueden repartirse y reasignarse entre distintas transmisiones, ajustando dinámicamente las tasas de transmisión. Este tipo de modulación se denomina OFDM (Orthogonal Frequency Division Multiplexing). Adicionalmente las diferentes ranuras de tiempo que lleva cada subportadora también se reparten entre varias transmisiones.



Por otro lado, se añade tecnología de antenas múltiples (MIMO, Multi-Input Multi-Output). Este sistema permite múltiples enlaces de radio entre las estaciones base y los móviles.

3.2.6. Canales

Usando los enlaces proporcionados por las capas física y de transporte se construyen los distintos canales lógicos. Estos pueden ser de control o de tráfico (es decir, de información, voz o datos). Se distinguen los dos siguientes canales de tráfico:

1. Canales para servicios dedicados, esto es, para las transmisiones de un usuario individual (DTCH, Dedicated Traffic Channel).

2. Canales para los servicios multicast de la estación base, como por ejemplo, para la transmisión de TV móvil o radiodifusión (MTCH, Multicast Traffic Channel).

En cuanto a los canales de control, se utilizan los siguientes:

1. La estación base dispone de un canal para difundir periódicamente la *información específica de la celda*, como por ejemplo, su identificación y la configuración de los demás canales de control (BCCH, Broadcast Control Channel).

2. El móvil y la estación base disponen de un canal para transmitir un cierto número de mensajes no programados de antemano, tales como *anuncio de presencia*, *peticiones de establecimiento de llamada*, etc. Este canal es compartido por todos los móviles (CCCH: Common Control Channel).

3. La estación base dispone de un canal para avisar a los móviles de la *recepción de llamadas* cuando se desconoce la posición del móvil en la celda (PCCH: Paging Control Channel).

4. Además, cada canal de tráfico dispone para su gestión un canal de *control asociado* para operaciones sobre una transmisión en curso de un usuario. Lo utilizan tanto los móviles como la estación base (DCCH, Dedicated Control Channel).

5. De forma similar al anterior canal, la estación base dispone de un canal de *control asociado* para transmisión multicast (MCCH: Multicast Control Channel).

3.2.7. Medidas de ahorro de energía en la operación del móvil

Control de potencia. Con el fin de prolongar la duración de las baterías de los teléfonos móviles, así como reducir las interferencias se establece que la potencia de emisión se mantenga al valor mínimo posible con el que se pueda asegurar una calidad de transmisión aceptable.

En el acceso inicial, el móvil utilizará la potencia máxima admitida en la celda (difundida por la estación base). Tras el acceso, la estación base calcula la potencia que debe usar el móvil y le ordena el ajuste de potencia mediante un número transmitido a través de un canal de control asociado.

Transmisión discontinua. En todos los sistemas de telefonía de voz sólo se envía información en un sólo sentido de cada vez (mientras un lado habla, el otro escucha), y además hay pausas en la conversación. En término medio, un canal sólo está activo menos del 50 % del tiempo. El sistema se aprovecha de esto utilizando el sistema de transmisión discontinua (DTX), que consiste en que sólo hay transmisión cuando hay muestras de voz presentes, cesando la transmisión en los periodos de silencio. Como consecuencia, se prolonga la duración de los teléfonos móviles y se limitan las interferencias.

La realización de la DTX implica el uso de un *detector de actividad vocal* para distinguir la voz del ruido ambiente. La aplicación de este sistema le supone un problema al usuario receptor. Como habitualmente se percibe cierto ruido, su inexistencia produce una sensación de irrealidad. Para evitar esto, el receptor sintetiza un *ruido de conveniencia*.

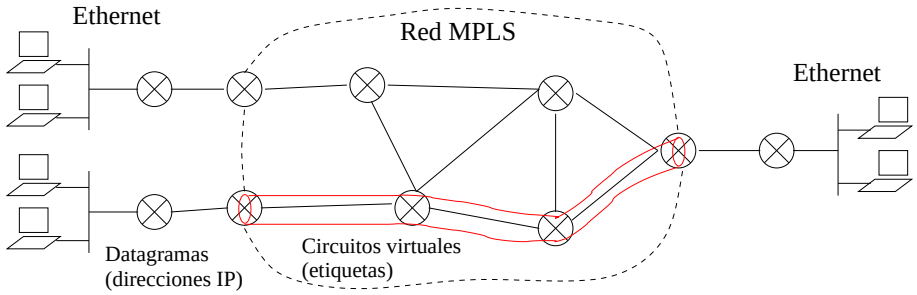
Recepción discontinua. Para aumentar la duración de las baterías del móvil en el tiempo en que el teléfono está en espera, la escucha del canal de control no es permanente, sino conmutada. El móvil sólo tiene que escuchar las transmisiones de control cada cierto tiempo. En consecuencia, cuando no hay necesidad de escucha, su receptor puede estar desconectado. Esta modalidad de funcionamiento se llama *recepción discontinua* (DRX).

3.3. MPLS

MPLS (Conmutación MultiProtocolo mediante Etiquetas o Multiprotocol Label Switching) es un modelo de red simple, ideal para WAN, diseñada para operar a alta velocidad y que puede transmitir tráfico telefónico además de datos usando el protocolo IP. El sector de las telecomunicaciones se encuentra actualmente inmerso en un proceso de transformación de sus infraestructuras tomando como base el protocolo IP, con el objetivo de incorporar los beneficios de esta tecnología. MPLS utiliza una tecnología de conmutación basada en etiquetas que permite generar circuitos virtuales sobre las redes IP y con ello proporcionar QoS

a los diferentes tipos de tráfico. El objetivo es adaptar las redes IP a las nuevas aplicaciones multimedia con altas necesidades de ancho de banda y calidad de servicio.

Las redes MPLS se pueden usar en redes privadas, pero lo más normal es que las compañías telefónicas o los ISP (Proveedores de Servicios de Internet) las alquilen como troncales (backbone) a las empresas que necesitan interconectar diferentes sedes. Las compañías telefónicas, además de los tradicionales servicios de voz, han ofrecido a las empresas servicios de transmisión de datos desde hace bastante tiempo. Previamente ofrecían el modelo ATM (Modo de Transferencia Asíncrono), que ha sido sustituido en la actualidad por MPLS. Los clientes pueden conectar sus routers Ethernet directamente a los routers MPLS de los proveedores, en un esquema de red WAN que se denomina *Metro Ethernet*.



Las principales características de MPLS, son pues, las siguientes:

- Presenta un diseño sencillo que transmite los paquetes IP a través de circuitos virtuales con mínima sobrecarga.
- Soporta QoS, por lo que es adecuado para cualquier tipo de tráfico.
- Es compatible con cualquier capa de enlace (Ethernet, ATM, etc). Además, se integra a la perfección en los modelos de servicios integrados (IntServ) y diferenciados (DiffServ).

Además, MPLS presenta otras dos características interesantes:

- La versión denominada GMPLS (Generalized MPLS) soporta también el multiplexado TDM, por lo que es compatible con las redes ópticas actuales SONET y está preparada para aprovechar las ventajas de las redes ópticas de nueva generación.
- MPLS puede utilizarse también para crear VPNs (Virtual Public Networks). Una VPN simula la operación de una WAN privada sobre la Internet pública utilizando túneles en Internet en vez de enlaces dedicados. Los túneles mediante cifrado y restricciones de conexión aislan el tráfico de la WAN virtual del resto de las conexiones en Internet. Los circuitos virtuales de MPLS son especialmente adecuados para la construcción de los túneles. Una generalización de las VPN son las SD-WAN (WAN definida por software).

3.3.1. Circuitos virtuales

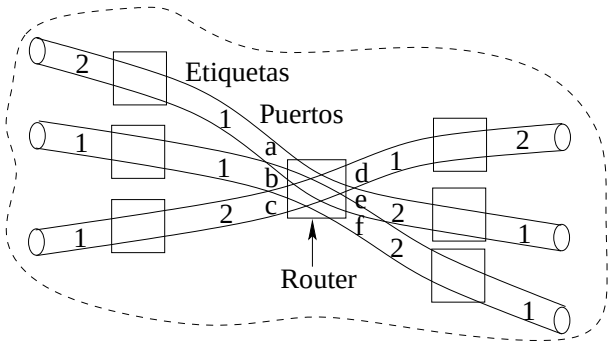
En el encaminamiento IP tradicional cuando un paquete llega a un router se le examina la dirección destino junto a otros parámetros de la cabecera y de acuerdo con la tabla del router se coloca en una de las líneas de salida. Como la ruta que va a seguir el paquete no se conoce a priori, es difícil reservar recursos que garanticen la calidad de servicio.

MPLS es una red de circuitos virtuales por lo que antes de transmitir un paquete de datos hay que generar un circuito virtual a través de la red MPLS. Cuando un router MPLS de frontera acepta un paquete desde una red externa no MPLS, lee la dirección del destino y negocia con otros routers MPLS la creación de un circuito virtual a través de la red. En MPLS a cada paquete que entra en la red se le asigna una etiqueta que identifica el ciruito virtual. Las etiquetas se asignan en base a la dirección destino del paquete, los parámetros de tipo de servicio, la pertenencia a una VPN o por cualquier otro criterio. Las etiquetas permiten identificar a un conjunto de paquetes que siguen el mismo camino a través de la red, incluso aunque sus destinos finales (fuera ya de la red MPLS) sean diferentes. Las etiquetas se escriben en un campo añadido a los paquetes cuando entran en la red MPLS y se eliminan cuando salen de ella. Los routers añaden esta etiqueta a sus tablas y se la comunican a sus vecinos.

Para optimizar el uso de las tablas de rutas se utilizan las dos siguientes estrategias:

1. Dos niveles de direccionamiento. Como hemos visto, las etiquetas solo tienen que codificar la parte de la ruta dentro de la red MPLS, por lo que el tamaño del campo puede ser pequeño. La ruta fuera de la red MPLS la determinarán las direcciones IP, que no se utilizan dentro de la red MPLS. Además, a todas las transmisiones con el mismo origen y destino dentro de la red MPLS se le asigna la misma etiqueta, con lo que las tablas de los routers tienen un tamaño reducido y su consulta es muy rápida.

2. Las etiquetas pueden variar a lo largo de la ruta.



El cambio de etiquetas en los paquetes se realiza a la vez que se encamina el paquete, de acuerdo con las tablas que disponen los routers MPLS. El

formato de las tablas es el siguiente:

Entradas		Salidas	
puerto entrada	etiqueta entrada	puerto salida	etiqueta salida
a	1	e	2
b	1	f	2
c	2	d	1

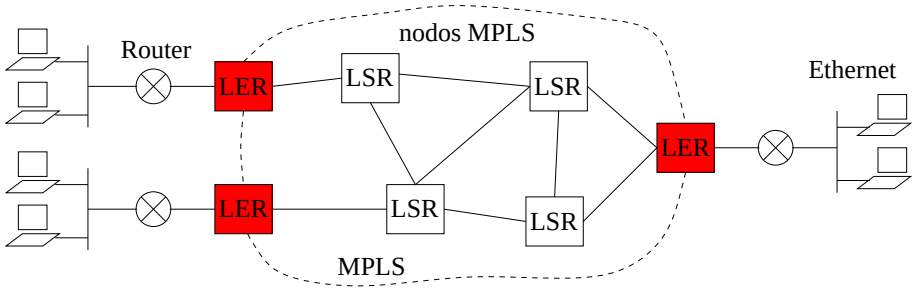
Esto tiene dos ventajas:

1. Al poder reutilizar las mismas etiquetas en distintos routers, el tamaño del campo será menor.

2. No se necesita una coordinación global entre todos los routers para evitar que diferentes transmisiones tengan las mismas etiquetas, pues los conmutadores las pueden ajustar en las partes de la ruta que se solapen.

3.3.2. Routers

Los nodos MPLS son routers o switches de red troncal que incorporan el software MPLS. Se distinguen dos tipos de nodos, físicamente el mismo dispositivo pero configurados por el administrador para uno u otro modo de trabajo:



- *Router de Etiquetado de Frontera* (LER: Label Edge Router). Opera en la periferia de la red MPLS y se encarga de recoger a los paquetes procedentes de otras redes, por lo que soporta múltiples protocolos para poder comunicarse con diferentes modelos de red. Este router analiza y clasifica el paquete IP entrante leyendo las cabeceras hasta el nivel 3 (nivel de red), es decir, considerando la dirección IP de destino y la QoS demandada. A continuación, decide el camino entero a lo largo de la red que el paquete debe seguir (un router IP normal solo decidiría el siguiente salto). Por último, inserta en el paquete la etiqueta MPLS y la clase de servicio en función del campo TOS de la cabecera IP u otros parámetros.

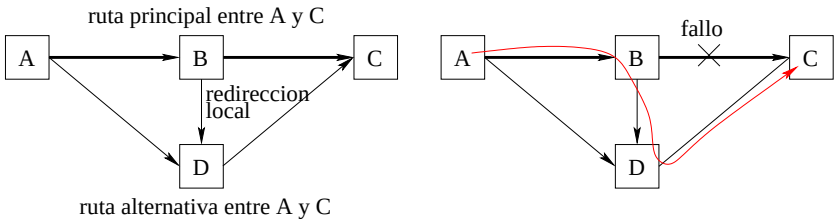
- *Router de Conmutación por Etiquetas* (LSR: Label Switched Router). Es un router de alta velocidad situado en el interior de la red MPLS que realiza el encaminamiento exclusivamente en base a las etiquetas. Las etiquetas tienen significado local, por lo que pueden variar a lo largo de la ruta, como hemos indicado en el ejemplo anterior.

Protocolos. Los nodos MPLS trabajan con dos tipos de protocolo de rutado:

- Al igual que los routers IP normales, los nodos MPLS utilizan los protocolos de rutado estándar, tales como OSPF (Open Shortest Path First), RIP (Routing Information Protocol) y BGP (Border Gateway Protocol), para intercambiar información sobre la topología de la red y construtruir las tablas de rutado basándose principalmente en la distancia a las redes IP destino.

- Adicionalmente se utilizan los Protocolos de Distribución de Etiquetas (LDP, Label Distribution Protocols), que facilitan a los nodos MPLS descubrirse, intercambiar información entre ellos y construir las tablas de conmutación. De esta forma pueden negociar determinados parámetros y reservar los recursos físicos necesarios para satisfacer los requerimientos de calidad de servicio que pueden ofrecen en cada ruta.

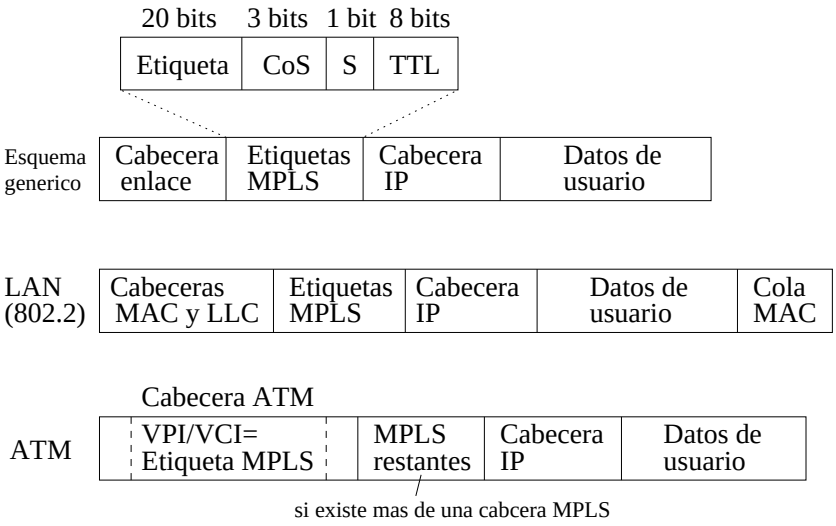
Recuperación rápida. Una característica muy importante de estos protocolos es que permiten una recuperación rápida en caso de fallos en la red, en menos de 50 ms, lo cual es imprescindible para aplicaciones en tiempo real. La recuperación de los fallos se basa en la existencia de rutas alternativas y en redirecciones locales.



El nodo que detecta un fallo, usando la redirección local redirige automáticamente los paquetes por la ruta alternativa, sin necesidad de informar antes a ningún otro nodo. La notificación a los demás nodos de que se ha producido un corte en la red se realiza a posteriori y a partir de entonces todos usarán la ruta alternativa.

3.3.3. Cabeceras

Las etiquetas MPLS son pequeñas y de tamaño fijo (4 bytes), se insertan entre las cabeceras de enlace y de red del paquete y constan de los siguientes campos:



- Etiqueta (20 bits). Es el identificador del circuito virtual.

- Clase de Servicio (CoS) (3 bits). Este campo se usa para indicar la prioridad, QoS y notificación de la congestión. Mediante este campo es posible diferenciar distintos tipos de tráfico y mejorar el rendimiento de algunas transmisiones frente a otras.

- Stack (1 bit). Permite apilar varias cabeceras MPLS, por ejemplo, cuando una red MPLS tiene que atravesar una segunda red MPLS perteneciente a otra organización. Cuando el paquete entra en esta segunda red se le añade una nueva cabecera MPLS y al salir de ella se elimina y se continúa trabajando con la cabecera MPLS original. El campo se pone a 1 en la primera cabecera introducida y 0 en las restantes.

- TTL (8 bits). Tiempo de vida, que reemplaza al correspondiente campo existente en la cabecera IP mientras el paquete viaja por la red MPLS.

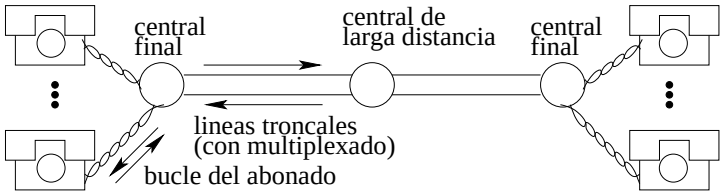
En ATM no es necesario añadir una cabecera nueva, pues pueden reutilizarse algunos de los campos que ya tiene la cabecera ATM.

3.4. Troncales

Las líneas troncales son las que interconectan los niveles superiores de la red, por ejemplo, las conexiones entre centrales telefónicas o el backbone (columna vertebral) de Internet. Vamos a ver tres tipos de líneas troncales en orden de antigüedad.

3.4.1. Sistemas portadora-E/T

Constituyen el esquema clásico para la transmisión de canales telefónicos de 64 kbps utilizando TDM (multiplexión por división del tiempo).



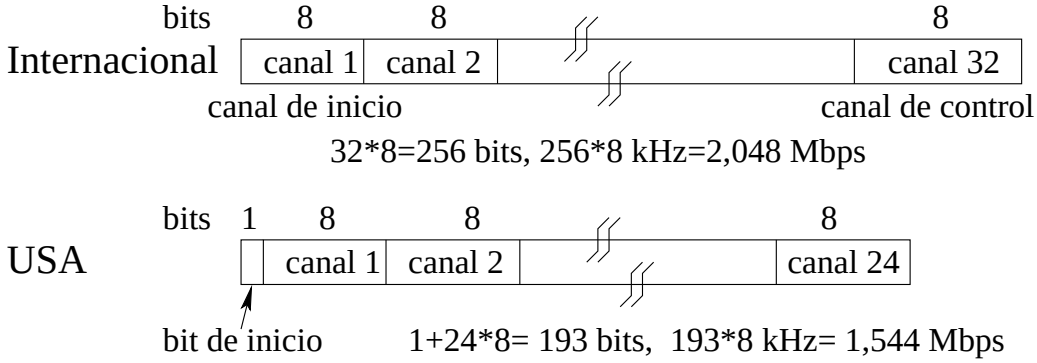
Según el país se distinguen dos sistemas:

- **Sistema portadora-E (E-carrier)** (europeo o internacional). El sistema básico E1 multiplexa 32 canales de 64 kbps, resultando una tasa de transmisión total de $64 \times 32 = 2,048$ Mbps que se puede transmitir por un par trenzado.

  Cada conjunto de 32 palabras se denomina cuadro. La primera y la última palabra de cada cuadro no llevan voz, sino que se usan para inicio (sincronización) y para llevar información de control (señalización).

- **Sistema portadora-T (T-carrier)** (USA, desarrollado por ATT) también denominado DS (*digital stream*). El sistema básico T1 multiplexa un bit de inicio de cuadro y 24 canales de voz ($1 + 24 \times 8 = 193$ bits). La tasa de transmisión de los 24 canales es $r = 193$ bits $\times$ 8 kHz $= 1,544$ Mbps.

  La sincronización se realiza mediante el bit de inicio de cuadro, que genera el patrón 0101010... entre cuadros sucesivos. El receptor verifica continuamente el valor de este bit para tener la seguridad de que está sincronizado con el comienzo del cuadro y en caso de pérdida de sincronismo debe buscar este patrón en la secuencia. La señalización se consigue mediante el "robo de bits" a los canales de voz, es decir, que cada cierto número de palabras se roban bits al usuario para emplearlos en la señalización.



Jerarquía. El sistema internacional E1 de 32 canales (30 canales útiles) y el USA T1 de 24 canales constituyen el sistema básico y pueden transmitirse

a través de un par trenzado para corta distancia en áreas metropolitanas. En la práctica los sistemas E1 y T1 son utilizados como base de una jerarquía de multiplexión de canales[1]:

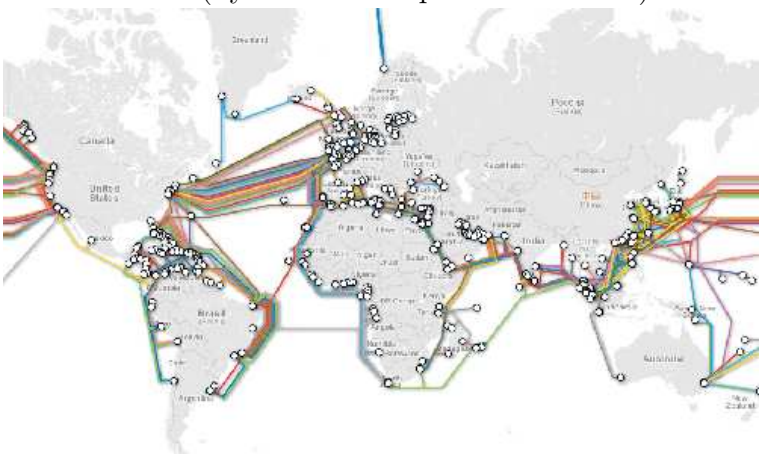
Internacional			
nivel	canales	MUX	Mbps
E1	30	-	2,048
E2	120	4 E1	8,448
E3	480	4 E2	34,368
E4	1920	4 E3	139,264
E5	7680	4 E4	565,148

USA			
nivel	canales	MUX	Mbps
T1	24	-	1,544
T2	96	4 T1	6,312
T3	672	7 T2	44,736
T4	4032	6 T3	274,176
T5	8064	2 T4	560,160

Alquiler de capacidad. Las empresas pueden contratar cierta capacidad de las líneas telefónicas para construir su infraestructura de red con la interconectar las sucursales situadas en distintas ciudades. La capacidad que se suele contratar en un múltiplo de E1 o T1.

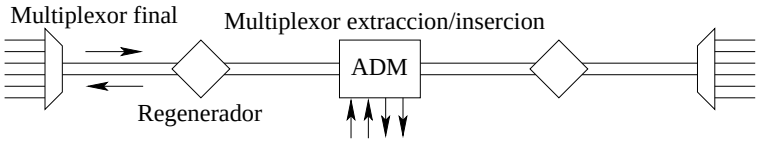
3.4.2. Red Óptica Síncrona (SONET)

Las líneas troncales de Internet están construidas con cables que contienen un gran número de fibras ópticas agrupadas para aumentar la capacidad. La capacidad de cada fibra es típicamente de 100 Gbps (por longitud de onda). La capacidad agregada de todas las fibras de un cable puede sumar miles de Tbps. En la actualidad el tráfico IP en Internet o en WANs es ampliamente transmitido a través de líneas SONET (Synchronous Optical NETwork).



Los dispositivos utilizados en SONET son los siguientes: un *multiplexor final* multiplexa los diferentes canales, un *regenerador* permite aumentar la distancia de transmisión decodificando la señal y volviéndola a generar (se colocan cada 100 km), por último, un *multiplexor de extracción-inserción* (ADM, Multiplexor Add/Drop) es un dispositivo que permite en un punto intermedio de una ruta extraer parte del tráfico o inyectar nuevo tráfico.

[1]Cuando se trata de velocidades, 1k=10^3 y 1M=10^6 (en vez de 1k=2^{10}=1024 y 1M=2^{20}).



La jerarquía de multiplexión de SONET es similar a la de los sistemas portadora. La capacidad útil cuenta solo la capacidad de datos mientras que la bruta cuenta también la información que llevan las cabeceras de control.

Nomenclatura SONET	Nomenclatura CCITT	velocidad bruta (Mbps)	velocidad útil (Mbps)
STS-1/OC-1		51,840	50,112
STS-3/OC-3	STM-1	155,52	150,336
STS-9/OC-9	STM-3	466,56	451,008
STS-12/OC-12	STM-4	622,08	601,344
STS-18/OC-18	STM-6	933,12	902,016
STS-24/OC-24	STM-8	1244,12	1202,688
STS-36/OC-36	STM-12	1866,24	1804,032
STS-48/OC-48	STM-16	2488,32	2405,376
STS-192/OC-192	STM-64	9953,28	9621,504
STS-768/OC-768	STM-256	39.813,12	38.486,016
STS-1536/OC-1536	STM-512	79.626,12	76.972,032
STS-3072/OC-3072	STM-1024	159.252,24	153.944,064

3.4.3. Red de Transporte Óptica (OTN)

La Red de Transporte Optica (OTN, Optical Transport Network) es un entorno diseñado recientemente para explotar las capacidades de las redes ópticas de nueva generación. Estas redes transmiten paquetes IP a través de fibra óptica DWDM usando el protocolo GMPLS.

Esquema clásico:

Datos
IP
ATM
SONET
Fibra

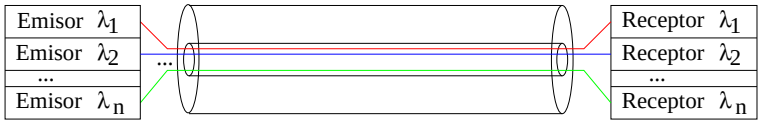
Red de Transporte Óptica:

Datos
IP
GMPLS
DWDM

Las dos capas nuevas de la arquitectura OTN son las siguientes:

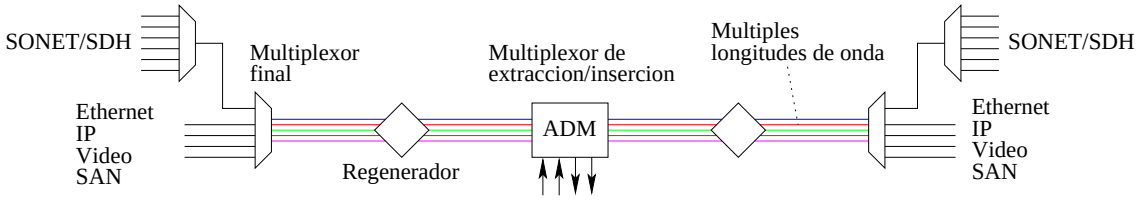
- **DWDM** (Multiplexión por división en longitudes de onda densas) es una técnica de transmisión de señales a través de fibra óptica muy similar a la multiplexión por división de frecuencia (FDM) que se utiliza con las señales electromagnéticas. DWDM multiplexa centenares de señales portadoras ópticas utilizando distintas longitudes de onda proporcionadas por diferentes haces láser. La capacidad típica es de 100 Gbps por cada longitud

de onda, lo que da unos 10 Tbps por fibra, que finalmente hay que multiplicar por el número de fibras que lleva el cable. Debe tenerse en cuenta que todavía queda mucho margen de mejora.

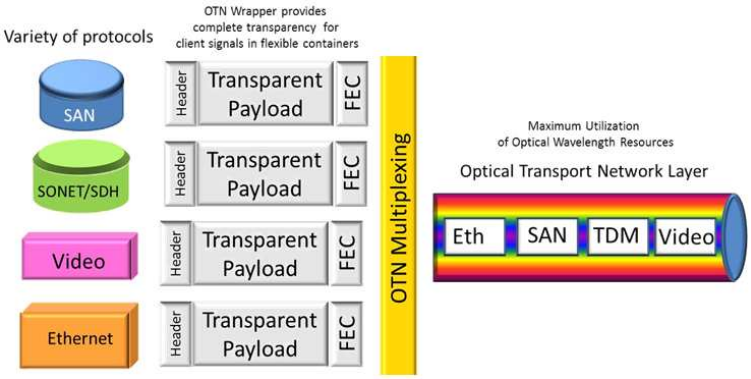


- **GMPLS (Generalized MPLS)** es un protocolo MPLS compatible con las transmisiones TDM y DWTM. Además de soportar el tráfico incluye la parte de control para provisionar los recursos de la red de forma dinámica. Es de hecho un protocolo de control de las redes ópticas. Por tanto se establece la integración total de las redes IP con las redes ópticas SONET y DWDM incluyendo la parte de control de las mismas dando lugar a las redes ópticas inteligentes de nueva generación.

La red de transporte óptica es compatible con casi todas las tecnologías de red. Integra la jerarquía de multiplexión SONET con los servicios de datos, por ejemplo Ethernet, IP, SAN (Storage Area Network), etc. El control de la red se realiza mediante el protocolo GMPLS.



El multiplexado de los distintos tipos de datos es totalmente transparente, esto es, el transporte se realiza automáticamente (de ahí su nombre). A cada paquete de datos se le añade una cabecera de control y un código corrector de errores (FEC, Forward Error Correction).



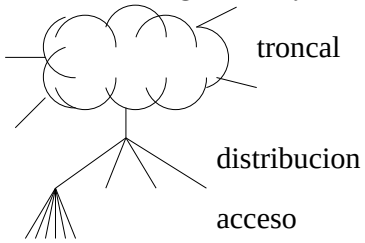
Capítulo 4

Diseño de redes

Para el diseño de una red es conveniente usar una metodología de diseño de arriba a abajo (top-down), es decir, partir de las aplicaciones que se deben ejecutar y terminar con la estructura física. Los pasos de esta metodología son los siguientes:

1. **Análisis de los requerimientos**. Primero, estudiar el tipo de empresa y el tráfico que genera. A continuación, estudiar las limitaciones de la red actual. Por último, establecer los criterios de diseño.

2. **Desarrollo del diseño lógico**. Seleccionar la estructura de la red (red troncal, red de distribución y red de acceso), seleccionar los protocolos de rutado y de conmutación, establecer la política de direcciones y nombres y realizar una planificación de la seguridad y de la gestión de la red.



3. **Desarrollo del diseño físico**. Seleccionar el cableado y las tecnologías (Ethernet, MPLS, etc) y también los productos comerciales y los proveedores de servicios.

4. **Test, optimización y documentación de la red**.

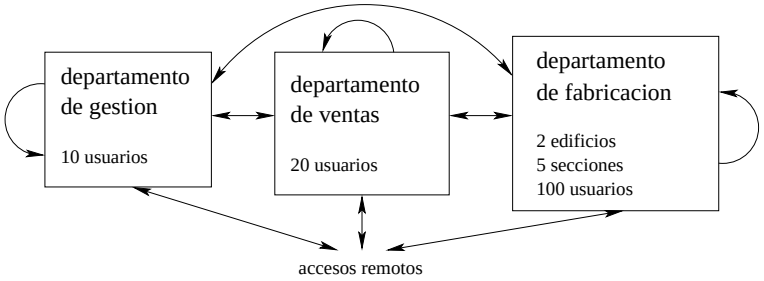
4.1. Análisis de los requerimientos

4.1.1. Tipo de empresa y tráfico

Hay que realizar el siguiente estudio:

1. Estudiar el tipo de negocio de la compañía y su organización, es decir, cómo está estructurada la empresa en departamentos, oficinas, grupos de trabajo, etc. Esto permite saber dónde están los empleados y cómo fluye el tráfico.

   Comprobar si la mayoría del tráfico es interno a los departamentos o exterior. Durante años se ha hecho un diseño de redes 80/20: 80 % para tráfico interno en una LAN y 20 % para otros departamentos o externo. En la actualidad esto ya no es así por el uso de granjas de servidores centralizados y redes troncales, accesos web, etc.



2. Estudiar los tipos de aplicaciones que generan tráfico de red: correo-e, transferencia de ficheros, acceso a bases de datos, navegación web, etc. A partir de aquí se pueden obtener las velocidades de transferencia requeridas, por ejemplo, si se desea transferir una página web típica de 50 kbytes en 1 sg, se requiere una velocidad de 50 kbytes $\times$ 8 bits/byte / 1 sg $\approx$ 400 kbps.

   Para el cálculo del tráfico total en la red interna se puede hacer una suposición del caso peor (así no habrá quejas por parte del cliente):

   - Todos los usuarios trabajan simultáneamente.
   - Las sesiones de un usuario duran todo el tiempo.
   - Todas las aplicaciones son utilizadas permanentemente.

4.1.2. Caracterización de la red actual

Antes de diseñar una nueva red, es conveniente estudiar la red de la que dispone actualmente el cliente. En concreto ha de realizarse:

- Caracterización de la arquitectura lógica (red troncal, red de distribución y red de acceso), del cableado y de las instalaciones inalámbricas.
- Caracterización de tipo de tráfico: terminal/host, cliente/servidor, servidor/servidor, P2P, computación distribuida, etc.
- Análisis de la utilización de la red, de los retardos y del tiempo de respuesta. Testeo del estado de routers, switches y firewalls (estadísticas). Si la utilización promedio de una red es del 70 % la actualización es necesaria siempre.

Esto dará una idea de lo que falla en la red actual y dónde ha de ponerse el énfasis en el diseño de la nueva red.

4.1.3. Criterios diseño

Existen diversos criterios para realizar el diseño de la red, algunos de los cuales son contrapuestos, por lo que habrá que llegar a una solución de compromiso.

- **Prestaciones**. El principal parámetro para medir las prestaciones (desde el punto de vista del usuario) es el tiempo de respuesta. Los usuarios se sienten frustrados cuando el tiempo de respuesta es mayor que 0,1 sg en aplicaciones interactivas. Para descarga de páginas web grandes los usuarios admiten tiempos de hasta 10 sg.

  Para conseguir tiempos de respuesta más rápidos hay que aumentar la capacidad (ancho de banda) de la red.

- **Disponibilidad**. Hay que determinar cuánto tiempo es admisible que la red esté parada. Las causas de parada de la red incluyen fallos de tensión, fallos hardware y software en los routers, fallos humanos, incrementos de tráfico, fallos de seguridad, etc.

  Una disponibilidad del 99,70 significa que la red puede estar parada 30 minutos por semana, lo cual implica que es factible hacer paradas en la red. Una disponibilidad del 99,95 significa 5 minutos de paro por semana, lo que implica sustitución en caliente de los equipos. Una disponibilidad del 99,999 (conocido como 5 nueves) implica hardware de doble o triple redundancia y software prácticamente libre de fallos.

- **Escalabilidad**. Por lo menos, ha de hacerse un diseño de red que le sirva a la empresa para los próximos 2 años. Hay que tener en cuenta la posible incorporación de nuevas oficinas, usuarios, servidores, etc.

  Optativamente pueden hacerse diseños escalables a más largo plazo. El problema es que muchas compañías no tienen una visión clara de cómo será su futuro en plazos tales como 5 años.

  Para ello pueden elegirse routers y conmutadores modulares y cableado con capacidad suficiente, lo cual, obviamente tiene un coste. En general, los diseños jerárquicos (de varios niveles) son más escalables.

- **Adaptabilidad**. Facilidad de acomodarse a cambios: incorporación de nuevos protocolos, de nuevas tecnologías, nuevos requerimientos, etc. Por ejemplo, reutilizar una red de datos para transmitir VoIP.

- **Seguridad**. El aumento de la seguridad de un sistema tiene costos, tanto económicos como de productividad de los usuarios. Hay que protegerse tanto

de los accesos externos como de empleados no autorizados. Una medida útil de cuánto debe invertirse en seguridad es el punto en el que el costo de implementar la seguridad supera al costo de un incidente de intrusión.

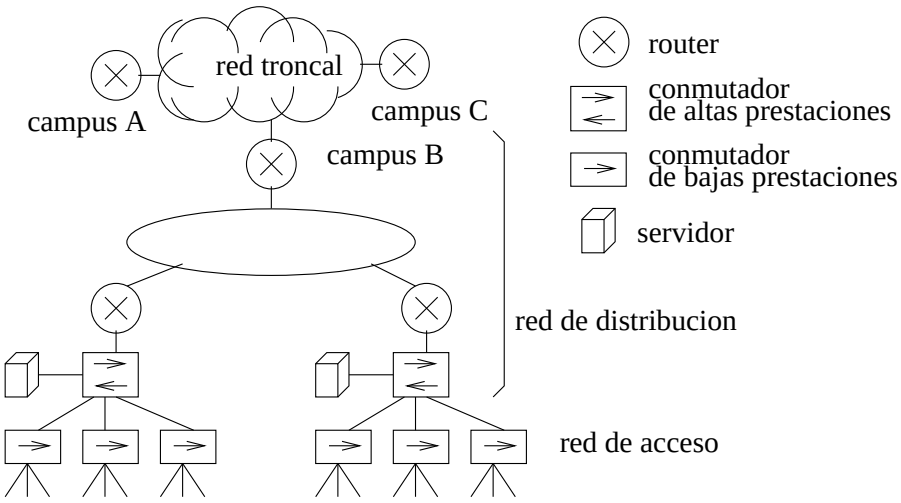
- **Usabilidad**. Es la facilidad de acceso de los usuarios a los servicios: bases de datos, impresión, etc. Suele ser inversamente proporcional a la seguridad.
- **Gestión**. Deben incluirse facilidades para reconfigurar la red, analizar el tráfico, detectar fallos, gestionar la seguridad, etc.
- **Coste**.

El cliente debe establecer su prioridad para cada uno de estos criterios. Una forma es hacer un reparto en %, por ejemplo, 15/30/20/5/5/5/5/15 (total 100).

4.2. Desarrollo del diseño lógico

4.2.1. Estructura de la red

Lo ideal es una estructura jerárquica de tres niveles:



1. **Una red troncal**. Es el nivel superior que interconecta los distintos campus de la empresa. Puesto que la empresa no puede tender cable entre los distintos campus (los ayuntamientos no suelen dar permiso), la red troncal puede construirse con líneas alquiladas a las compañías telefónicas, con una WAN alquilada a un proveedor de servicios o puede ser una *red privada virtual*, es decir, construida sobre la Internet pública.

2. **Una red de distribución**. Es la parte de la red que interconecta los edificios y departamentos dentro de un mismo campus. Suele constar de routers

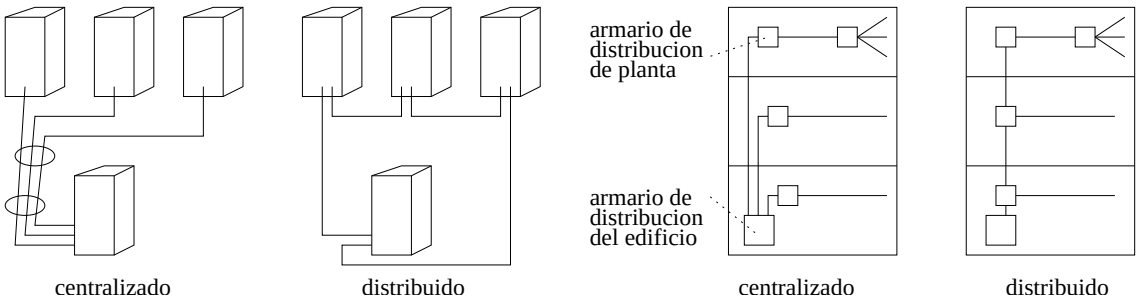
y switches de altas prestaciones que implementan políticas (seguridad, rutado entre VLANs, etc).

3. **Una red de acceso**. Es la parte de la red que proporciona acceso a los usuarios. Está compuesta de switches de altas o bajas prestaciones y puntos de acceso inalámbricos. En esta etapa de diseño, la red de acceso puede especificarse a nivel de VLANs.

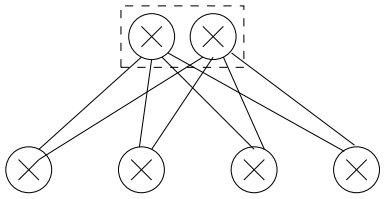
Topología. Cualquier nivel de la red puede tener una topología centralizada (estrella) o distribuida (lineal, anillo o malla).

En el campus los cables que realizan la interconexión suelen estar expuestos a mayores peligros: cortes, cortocircuitos, inundaciones, etc. El esquema distribuido con topología malla ofrece una ligera ventaja frente a los desastres que el centralizado.

Dentro de un edificio, si este es pequeño es preferible usar un esquema centralizado, pues la gestión de la red es más sencilla. Un esquema distribuido lineal es más barato y sencillo de instalar.



Redundancia. Puede introducirse redundancia a cualquier nivel de la red incorporando componentes replicados. Estos incluyen routers, switches, enlaces, fuentes de alimentación, etc. Por ejemplo, una estructura jerárquica redundante en el nivel superior se muestra en la siguiente figura:



Existe también la posibilidad de implementar una redundancia en la que el camino alternativo sea de menos prestaciones que el principal.

4.2.2. Selección de los protocolos de rutado y de conmutación

1. Como algoritmo de rutado podría usarse RIP, OSPF o algún algoritmo propietario. RIP es el algoritmo más simple y compatible con cualquier

equipamiento, si bien sus capacidades son limitadas. Si se desean más prestaciones, por ejemplo, rutas múltiples o soporte para jerarquías debería usarse OSPF u otro similar.

2. Para las redes Ethernet se deberían usar bridges y switches, y no hubs. Es muy importante que estos dispositivos incluyan el algoritmo del árbol de expansión (para evitar bucles) y un protocolo para la construcción de VLANs.

4.2.3. Asignación de direcciones y nombres

A continuación, debe establecerse la política de asignación de direcciones y nombres. Hay que asignar direcciones IP a routers y hosts. Una serie de reglas para asignar direcciones:

1. Diseñar un esquema estructurado para la asignación de direcciones. Usar direcciones sin clases y hacer un uso extensivo de las máscaras. Hacer una correspondencia entre los niveles de red y los niveles de direccionamiento.
2. Dejar márgenes para poder aumentar las direcciones en cada nivel.
3. Asignar los bloques de direcciones en función de la red física, no de los usuarios (eso ya se hará con VLANs).
4. Elegir direccionamiento estático o dinámico (DHCP) de los hosts. Para maximizar la flexibilidad y minimizar el trabajo de configuración, usar DHCP.
5. Para maximizar la seguridad y adaptabilidad, usar direcciones privadas y realizar la traducción de direcciones de red (NAT).
6. Si el nivel de los administradores de la red de la empresa es alta, se puede delegar el detalle del direccionamiento a las oficinas regionales, administradores de las subredes, etc.

Pasamos a la asignación de nombres. Hay que tomar las siguientes decisiones:

1. A qué dispositivos se les van a asignar nombres: servidores, routers, hosts, impresoras, etc. Hay que recordar que la asignación de nombres no es obligatoria, en principio basta con asignar direcciones IP.
2. Cómo se estructuran los nombres, tanto los subdominios como las distintas porciones de un nombre. Como siempre, es preferible un esquema jerárquico.
3. Cómo se mapea un nombre a una dirección. Se realizará por asignación estática o dinámica junto a las direcciones IP.
4. Qué nombres se usarán localmente y cuáles se darán de alta en el DNS. En este último caso, existe la alternativa de implementar los servidores de nombres en la empresa o bien utilizar los proporcionados por el ISP.

4.2.4. Estrategias de seguridad

Desde el punto de vista de la red, pueden establecerse las siguientes medidas de seguridad:

1. **Seguridad física**. Esto es, limitar el acceso a los dispositivos de la red mediante su localización en habitaciones cerradas.

2. **Cifrado**. Deberían usarse protocolos cifrados (ssh, sftp, https) frente a los que transmiten en claro (telnet, ftp, http), sobre todo si se realizan conexiones desde el exterior. En las WLAN debería habilitarse la opción de cifrado.

3. **Autentificación y autorización**. Aunque usualmente se refieren a los usuarios, también pueden aplicarse a los equipos. Muchos protocolos de red admiten autentificación y autorización de equipos (VLANs, WLANs, PPP, etc). Routers y cortafuegos pueden aceptar o denegar paquetes dependiendo del origen o del tipo de servicio solicitado.

4. **Deshabilitación de servicios**. Los servicios que no se usen deberían deshabilitarse, por ejemplo, algunos de los protocolos de rutado en los routers, devolución de ecos, etc.

5. **Puntos de entrada bien definidos**. Para las conexiones remotas desde Internet es una buena práctica el sólo aceptar conexiones en un determinado punto de la red. Esto permite evitar el escaneo de hosts desde el exterior y permite una fácil monitorización de los accesos externos. Los servidores públicos (web, ftp, etc) deberían estar separados del resto de la red mediante cortafuegos.

6. **Auditorías**. Routers y hosts pueden almacenar información de todos los intentos de conexión. El examen de dicha información debería ser parte de la política de seguridad de la red.

Una política de seguridad debería informar a los usuarios y administradores de lo que se permite o no y de sus obligaciones para la protección de la información y de la seguridad.

4.2.5. Estrategias de gestión

La gestión de una red implica la realización de tareas tales como la configuración de la red, la detección de fallos, la gestión de la seguridad y la medida de las prestaciones.

1. **Configuración**. Los protocolos de configuración dinámica (DHCP, NAT, etc), simplifican mucho la tarea de configuración.

2. **Detección de fallos**. Para ello existen múltiples herramientas, desde las más sencillas como *traceroute* y los capturadores de paquetes a herramientas más complejas como SNMP (Simple Network Management Protocol), RMON (Remote Monitoring) y otras propietarias. Estas últimas son imprescindibles en redes muy grandes.

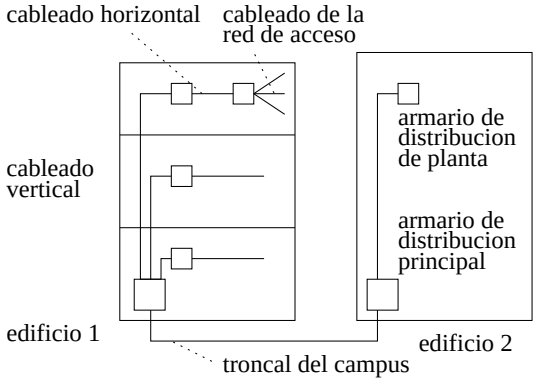
3. **Medida de prestaciones**. Las herramientas van desde el simple *ping* para medir los retardos a medidas de tráfico realizadas por herramientas tales como SNMP y RMON.

4.3. Desarrollo del diseño físico

Una vez que tenemos el diseño lógico de la red es la hora de concretar el diseño seleccionado tecnologías de red concretas para implementar las LANs y WANs.

4.3.1. Tecnologías y dispositivos para las redes campus

Una red campus, como su nombre indica, es aquella que se localiza en un conjunto de edificios localizados no demasiado dispersos.



1. **Tipos de cables**. Se puede elegir entre UTP, STP, coaxial y fibra óptica. El cableado UTP puede ser de categoría 5 (permite Ethernet 100 Mbps), 5e o 6 (con ciertas limitaciones permite Gigabit Ethernet y ATM).

   La fibra óptica por su dificultad de instalación y por el precio de los dispositivos suele limitarse a la interconexión de edificios y de plantas. (Nota: comprobar lo que cuesta poner en cada PC una tarjeta de red de fibra óptica frente a las típicas tarjetas Gigabit Ethernet de par trenzado). No obstante, en el futuro se espera que se use fibra óptica también para las LANs.

2. **Tecnologías de red**. Para una LAN, la tecnología recomendada es Gigabit Ethernet.

Para la red del campus se puede elegir entre Gigabit Ethernet o MPLS. Esta última es más cara y compleja que Gigabit Ethernet, pero ofrece más flexibilidad y garantías de calidad de servicio. Es una buena elección para redes que mezclan datos, voz y vídeo. También se puede utilizar Ethernet sobre MPLS (MPLS en los niveles inferiores y Ethernet en los superiores).

3. **Dispositivos de interconexión**. Esto es, bridges, switches y routers.

Los criterios de selección para estos dispositivos en general, son:

Diseño modular	Facilidad de configuración
Número de puertos	Tipo de gestión (SNMP, RMON)
Velocidad de procesamiento	Filtrado de paquetes y seguridad
Retardo introducido	Instalación de componentes en caliente
Cantidad de memoria	Fuentes de alimentación redundantes
Tecnologías LAN y WAN soportadas	Soporte de calidad de servicio
Autodetección de velocidad	Calidad (tiempo de fallo)
Autodetección de half/full duplex	Coste
Cableado que soporta	

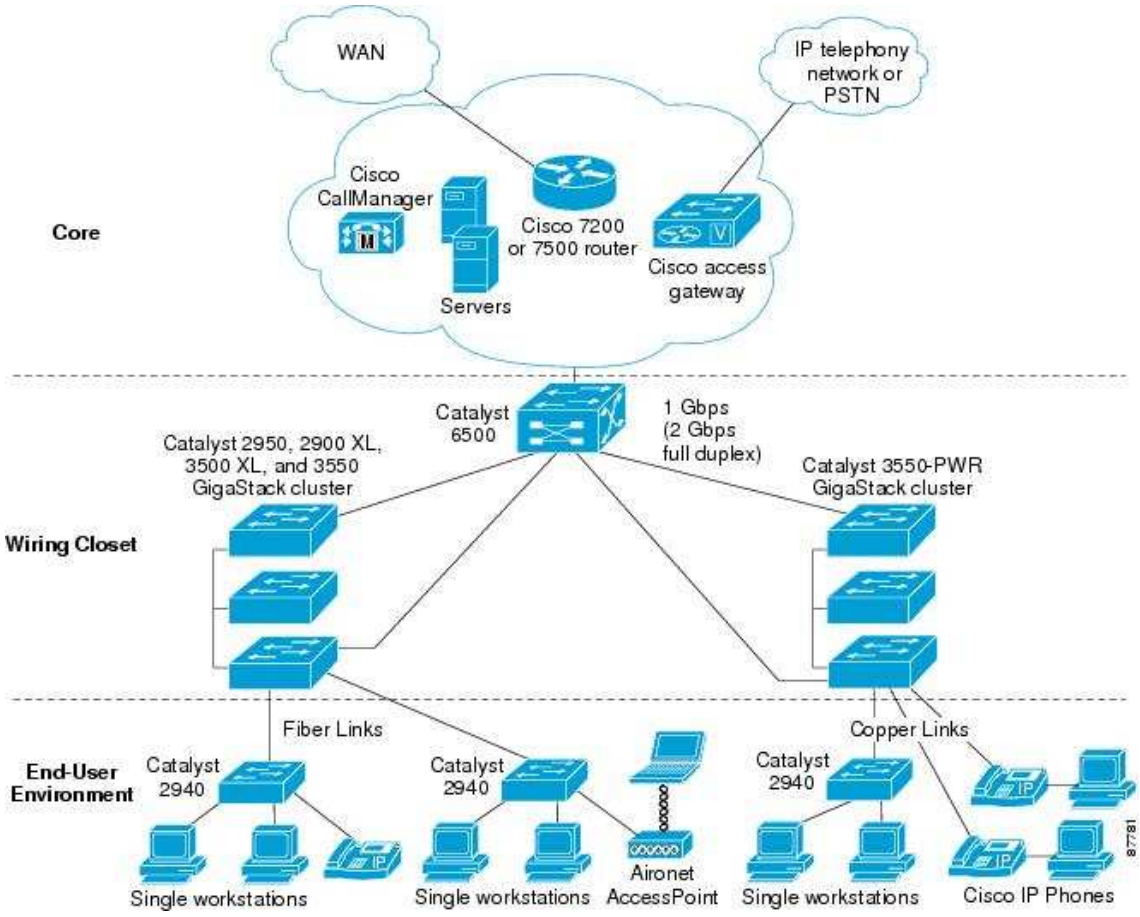
Para bridges y switches:	Para routers:
Número de direcciones que puede aprender	Protocolos de red soportados
Algoritmos de árbol de expansión	Protocolos de rutado soportados
Soporte para seguridad de puertos	Soporte para multicast
Conmutación rápida	Soporte para conmutación rápida
Algoritmos VLAN soportados	Soporte para compresión
Soporte para multicast	Soporte para cifrado

Para los puntos de acceso inalámbricos:

Velocidades soportadas	Sensibilidad en la recepción
Velocidad del puerto Ethernet	Posibilidad de uso exterior
Soporte para DHCP, NAT y rutado IP	Autentificación por direcciones MAC
Soporte para VLANs	Autentificación de usuarios
Alcance de la antena	Algoritmos de cifrado
Potencia de emisión	Medidas de seguridad del 802.11i

A continuación se muestra un ejemplo de red campus con dispositivos de la empresa CISCO[1]

[1] `http://www.cisco.com/c/en/us/td/docs/switches/lan/catalyst2940/software/release/12-1_19_ea1/configuration/guide/2940scg_1.html`.

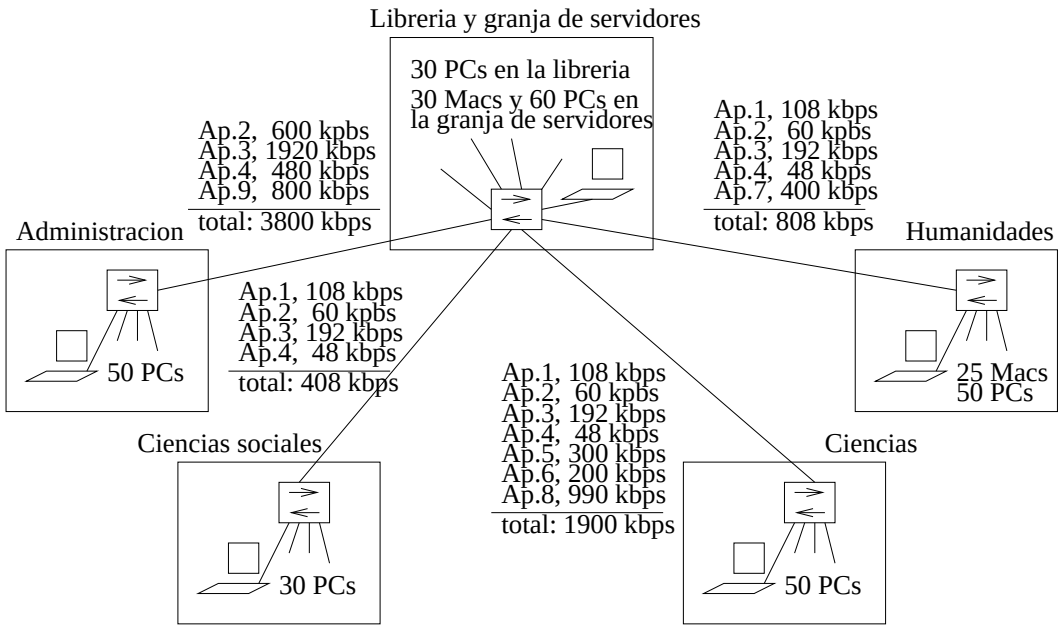


4.3.2. Ejemplo de diseño de una red campus

Consideraremos el caso del diseño de la red para un pequeño instituto de unos 600 estudiantes (que pueden aumentar a 1000 en los próximos años), 50 profesores y 25 administrativos. Se desea también proporcionar acceso remoto y acceso inalámbrico a todos los estudiantes[2].

La etapa de análisis de los requerimientos ha proporcionado el esquema:

[2]Véase el artículo *Administrar la red en un IES*, `http://recursostic.educacion.es/observatorio/web/ca/equipamiento-tecnologico/redes/694-administrar-la-red-en-un-ies` y el ejemplo `http://www.juntadeandalucia.es/averroes/centros-tic/11700123/helvia/sitio/index.cgi?wid_seccion=1&wid_item=160`.

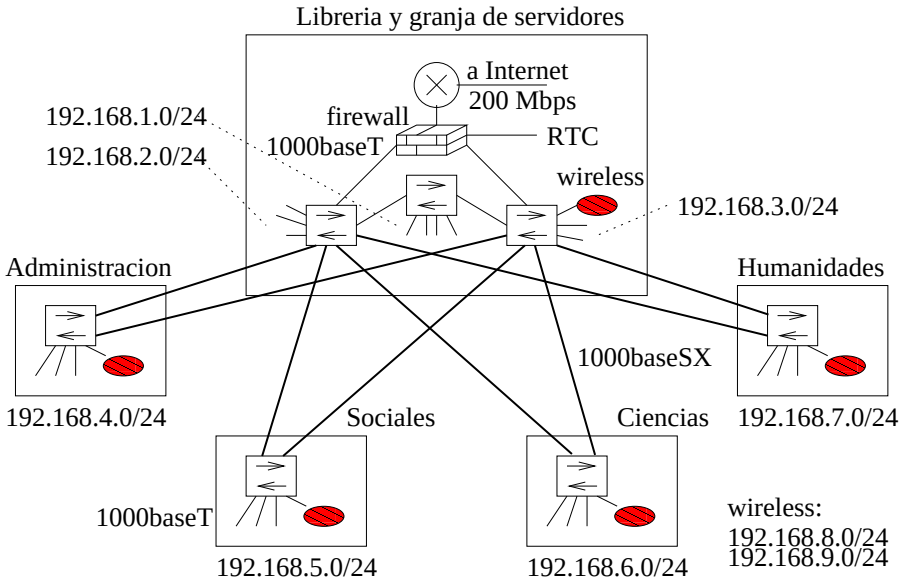


En esta etapa de análisis de los requerimientos se ha determinado que la capacidad de los enlaces individuales debe ser al menos 3,8 Mbps y la de los compartidos al menos $50 \times 3{,}8$ Mbps $= 190$ Mbps (realmente un poco más debido a los puntos de acceso inalámbrico). En la etapa del desarrollo del diseño lógico se ha elegido una topología en estrella con redundancia, direcciones IP privadas y accesos centralizados.

En la etapa de desarrollo del diseño físico se han determinado que los requerimientos mínimos para los enlaces individuales los proporciona la tecnología Ethernet 10 Mbps y para los enlaces troncales Gigabit Ethernet (1000baseT para distancias menores de 100 m usando par trenzado y 1000baseSX para distancias de hasta 550 m usando fibra óptica) para los enlaces compartidos. No obstante se ha decido instalar la tecnología Ethernet 1000baseT también para los enlaces individuales, puesto que la diferencia de precio es insignificante y garantizará la adaptabilidad de la red durante algunos años.

Los accesos desde Internet se realizan mediante ADSL, cable o fibra (se puede contratar un paquete de varias líneas) proporcionados por un ISP[3] y se centralizan en un sólo punto protegido por un firewall. Aquí también se realiza la traducción NAT.

[3]La Xunta saca a concurso la dotación de 100 megas a los colegios públicos. El plan afecta a 820 centros de primaria y secundaria, 450 con más de 100 alumnos. La empresa adjudicataria del servicio podrá combinar fibra y red móvil para atender los diferentes centros (18/06/2016), `http://www.lavozdegalicia.es/noticia/sociedad/2016/06/18/xunta-saca-concurso-dotacion-100-megas-colegios-publicos/0003_201606G18P38991.htm`.



4.3.3. Tecnologías y dispositivos para redes corporativas

En este apartado veremos el diseño físico de la parte de la red empresarial constituida por la red de área extensa (WAN) y por el acceso remoto.

Tecnologías WAN

Son utilizadas por la empresa para interconectar las redes locales dispersas geográficamente. La interconexión puede realizarse alquilando líneas a una compañía telefónica, alquilando parte de la capacidad de una WAN a un proveedor de servicios, construyendo una *red privada virtual* (VPN) sobre la infraestructura de red pública, como el sistema telefónico o Internet, o mezclando varios tipos de conexiones en una *WAN definida por software* (SD-WAN).

1. **Las líneas alquiladas** permiten reservar una cierta capacidad con la seguridad de que no será compartida con nadie. La capacidad puede seleccionarse usando las distintas jerarquías digitales, como el sistema portadora-E o la red óptica síncrona (SONET), etc. Suelen emplearse en conexiones síncronas manteniendo constante la utilización del ancho de banda. Son las líneas más costosas económicamente hablando. Las capacidades van desde 64 kbps a 10 Gbps.

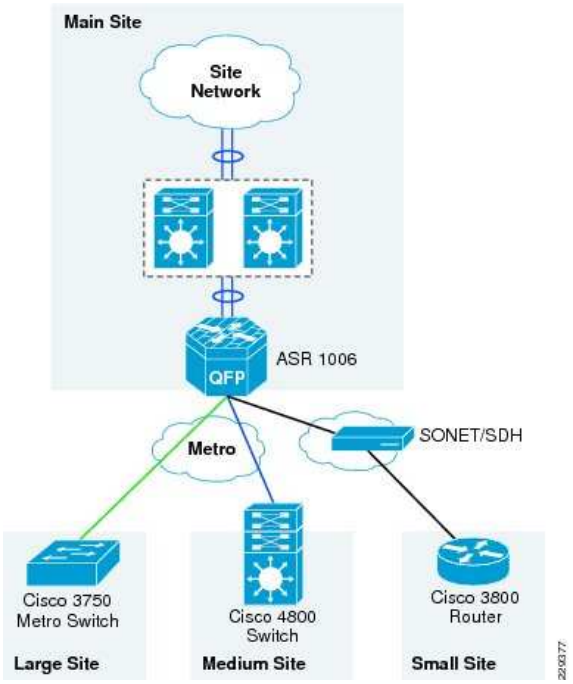
2. A un proveedor de servicios se le puede **alquilar parte de la capacidad de una WAN**, típicamente de una red MPLS. En ambos casos se puede usar Ethernet sobre MPLS, que tiene la ventaja de que el cliente usa routers Ethernet (más baratos y de más fácil gestión) sobre la red del proveedor. *Metro Ethernet* es un entorno tecnológico destinado a suministrar servicios

de conectividad MAN/WAN a través de Ethernet. La elección del proveedor se basará en criterios tales como coste, fiabilidad (mediante redundancia), seguridad, etc.

3. Una **red privada virtual** (VPN) típicamente usa la conexión a Internet de banda ancha de la empresa para interconectar las distintas redes locales de las sucursales. Esta solución es más barata y el costo no se incrementa con la distancia, también es más flexible. Sin embargo, no garantiza una capacidad de transmisión y es menos fiable. Las VPNs deben usar fuerte autentificación y cifrado (un protocolo estándar es IPsec). En la empresa pueden utilizarse routers y cortafuegos genéricos o bien dispositivos especializados denominados *concentradores VPN*.

4. Una **WAN definida por software** (SD-WAN) es una generalización de una VPN con dos principales características añadidas. En primer lugar permite gestionar eficientemente y de forma centralizada miles de puntos de conexión, seleccionando las rutas dinámicamente, añadiendo redundancia si es necesario y evitando la congestión y los cortes en la red. Además, si disponemos de varios tipos de conexiones (MPLS, 5G, Internet, etc) permite gestionarlas unificadamente, seleccionando en cada momento la más apropiada.

A continuación se muestra un ejemplo de la empresa CISCO[4]



[4] http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Medium_Enterprise_Design_Profile/MEDP.html.

Tecnologías de acceso remoto

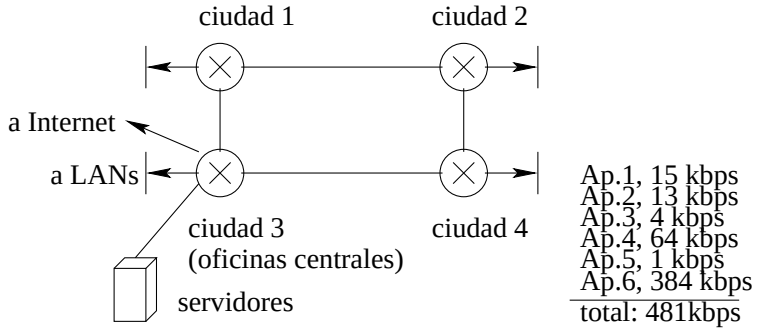
El acceso remoto proporciona acceso a los empleados desde su domicilio, de viaje, en sucursales remotas, etc. Típicamente, estos usuarios usan aplicaciones tales como correo-e, web, gestión de ventas, videoconferencia, intercambio de ficheros, demostraciones de productos, etc. Algunas de esas aplicaciones requieren bastante velocidad.

El acceso remoto se construye típicamente también como una *red privada virtual*, es decir usando el sistema telefónico o la Internet pública. El usuario normalmente usará una conexión a Internet de banda ancha (ADSL, cable o fibra), pero también se pueden usar los módems de telefonía móvil. La velocidad va desde 56 kbps hasta unos 300 Mbps.

4.3.4. Ejemplo de diseño de una red corporativa

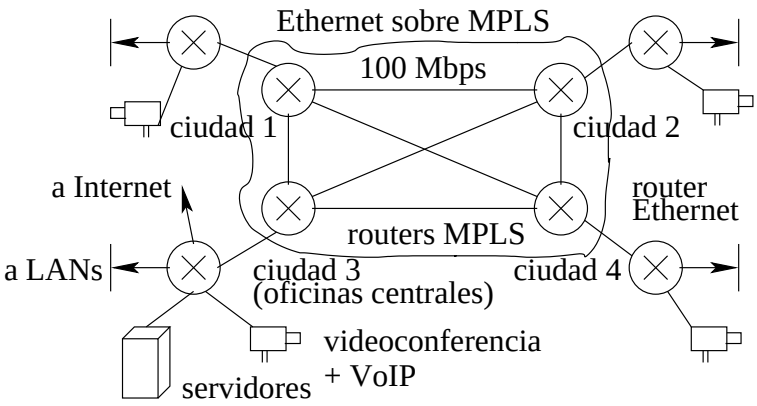
Consideraremos el caso de una empresa que posee 4 localizaciones principales, otras 11 secundarias nacionales, sucursales en todo el mundo y alrededor de 1500 empleados (400 empleados en la sede principal y 200 en las otras tres localizaciones principales). La red se utilizará para transmitir datos, audio y vídeo (tasas estándar de videoconferencia son 128, 256 y 384 kbps).

La etapa de análisis de los requerimientos ha proporcionado el siguiente esquema, donde las 4 oficinas principales estarán conectadas mediante una WAN alquilada a un ISP y el resto de oficinas y compradores utilizarán accesos remotos.



Durante la etapa de desarrollo del diseño lógico se ha elegido una topología malla. En la etapa de desarrollo del diseño físico se ha elegido una red MPLS pues permite proporcionar calidad de servicio a las transmisiones de audio y vídeo. Para los enlaces de las oficinas principales se requiere una capacidad de 200×481 kbps ≈ 100 Mbps. Como los enlaces alquilados dedicados son bastante caros, se ha decido contratar justo esta capacidad. Cuando sea necesario actualizar a una velocidad mayor bastará cambiar el contrato con la empresa telefónica o con el ISP[5].

[5]En España, las compañías telefónicas y los ISPs proporcionan a las empresas líneas dedicadas con capacidades comprendidas entre 2 Mbps y 10 Gbps, por ejemplo, `http://jazztelempresas.com/gran_empresa/gran_empresa_circuito`.



4.4. La red de la Universidad de Santiago

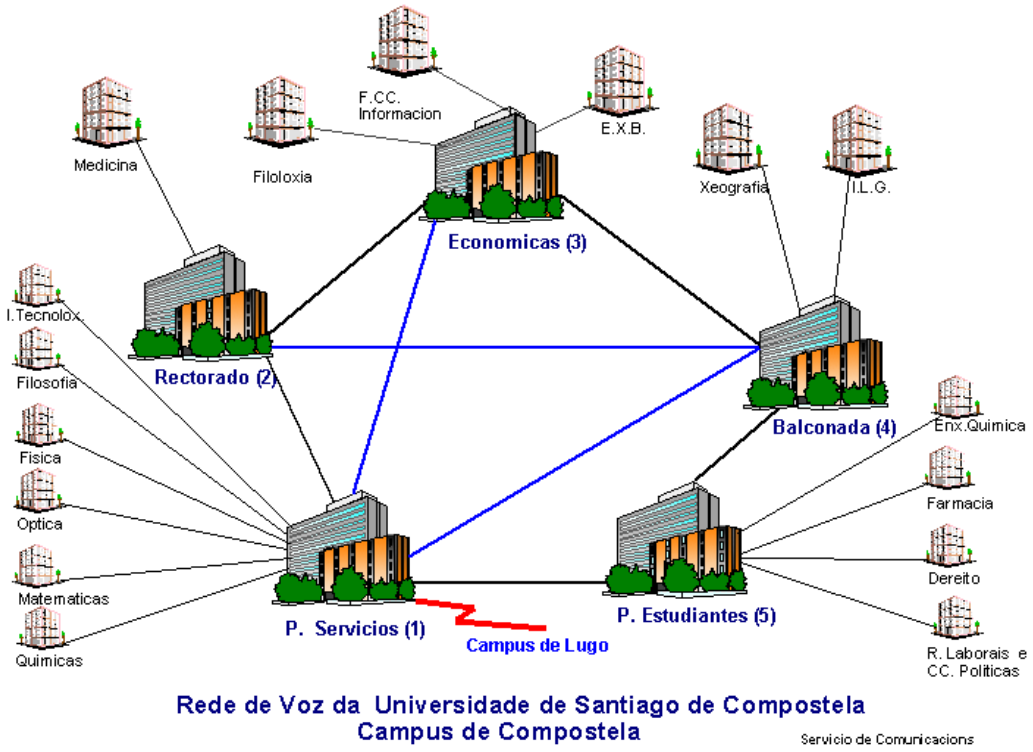
La Universidad de Santiago[6] (USC) posee dos redes de comunicaciones propias que dan servicio, respectivamente, a las transmisiones de voz y datos.

4.4.1. Red de telefonía

La red de telefonía del Campus de Santiago está dotada de 5 nodos centrales formando una red completamente mallada que garantiza la comunicación ante cualquier adversidad, 13 módulos remotos dan servicio al resto de edificios, 6 puestos de vídeo-operadora con directorio distribuido atienden las llamadas y se dispone de aproximadamente 2700 extensiones analógicas, 140 digitales, 200 enlaces urbanos analógicos, y acceso primario RDSI para marcación directa entrante.

Las 5 centrales digitales que componen el cuerpo se comportan como una única central con gestión centralizada y disponen de las modernas facilidades y servicios de las centrales digitales de última generación (desvío de llamadas, buzón de voz, multifrecuencia, redirección de destinos, creación de grupos de usuarios, control de accesos, etc). La topología esquemática la podemos ver en la figura siguiente:

[6] `http://www.usc.es`.



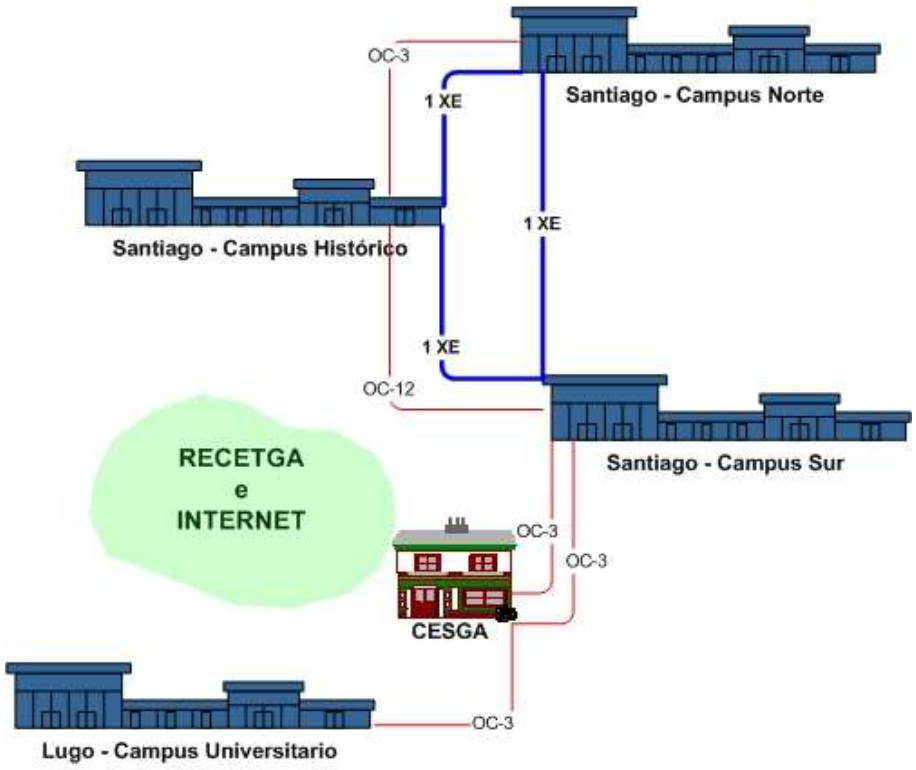
4.4.2. Red de datos

La red de datos está constituida por una red troncal de fibra óptica Ethernet Gigabit que une los edificios y que luego se bifurca en redes Fast Ethernet en los centros en base a switches y cableado estructurado UTP de categoría 5. Sus características son las siguientes:

- La velocidad de la conexión de los usuarios es de 100 Mbps mientras que la conexión entre los distintos edificios es una malla a 1 Gbps.
- Flexibilidad en la definición de servicios y funcionalidades, tanto en lo referido a la implantación de VLANs que separan los diferentes usuarios de la red, como a la utilización de múltiples encaminadores IP por edificios descargando los encaminadores centrales.
- Permite la instalación de filtros con objeto de definir las correspondientes políticas de seguridad.
- Esquema redundante en consideración de que se trata de un servicio estratégico para la USC y en la necesidad de garantizar un servicio estable.

La red troncal consta de 4 nodos centrales, 3 en Santiago y 1 en Lugo, dotados con equipos SSR8600 de Enterasys, enlaces Gigabit con interfaces multimodo

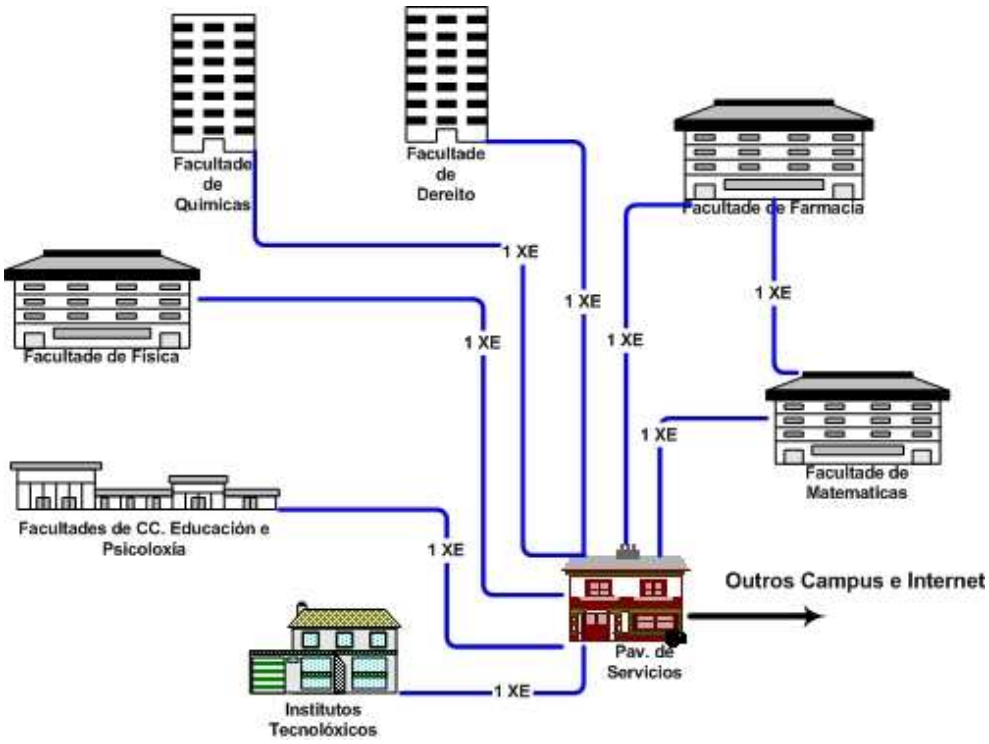
para las propias plantas y edificios próximos, y monomodo para los edificios más alejados.



En la ciudad de Santiago se unen los 3 nodos mediante un triángulo de enlaces Gigabit Ethernet (XE), garantizando caminos alternativos. Las dos ciudades se unen a través de la Autopista Gallega de la Información (AGI) y de la Red Científica y Tecnolóxica de Galicia (RECETGA) actualmente a una velocidad de 1 Gbps. Existe otro enlace de 1 Gbps al Centro de Supercomputación de Galicia (CESGA) que proporciona la conexión a RedIRIS y por lo tanto a Internet.

En un segundo nivel, el servicio se extiende a 80 edificios con segmentos Gigabit Ethernet conectados a los 4 nodos centrales, por tanto se trata de la tecnología de Ethernet conmutada en backbone. El sistema da soporte a dos redes independientes, a la red de Gestión y a la red de Investigación con un número de equipos conectados superior a 7000.

En este segundo nivel, los nodos de edificio están dotados también de equipamiento Enterasys: Matrix E7 o SS600 con una tarjeta de routing SSR-2, y numerosos puertos tanto a 1 Gigabit Ethernet en fibra, como Fast Ethernet en cobre (UTP categoría 5). La topología esquemática es la siguiente:



4.4.3. Cableado de un edificio de la USC

Diremos por tanto que la red del Campus de Santiago consta de una red de fibra óptica que sirve de troncal de la red de datos y cableado estructurado en más de 80 edificios. En el cableado interior de los edificios se emplea fibra óptica en los tendidos verticales y cable UTP de categoría 5 para todos los puntos de conexión de usuario, tanto de voz como de datos. Así el número de equipos instalados asciende a más de 7000.

El cableado utilizado es estructurado en el que se integra tanto voz como datos. Consta de los siguientes elementos:

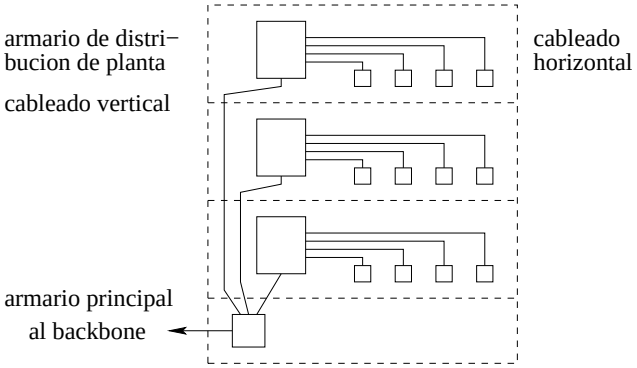
1. **Interconexión de usuarios**. Se utilizan rosetas RJ45/RJ14 para datos y para voz. Desde estos puntos se conectan los dispositivos del usuario.

2. **Cableado horizontal**. Se utiliza cable UTP de categoría 5, no pudiendo sobrepasar los 90 m ya que se utilizará unos 6 m para la conexión en el armario de distribución de planta y unos 3 m en el latiguillo de usuario. Este cableado va canalizado por las canaletas.

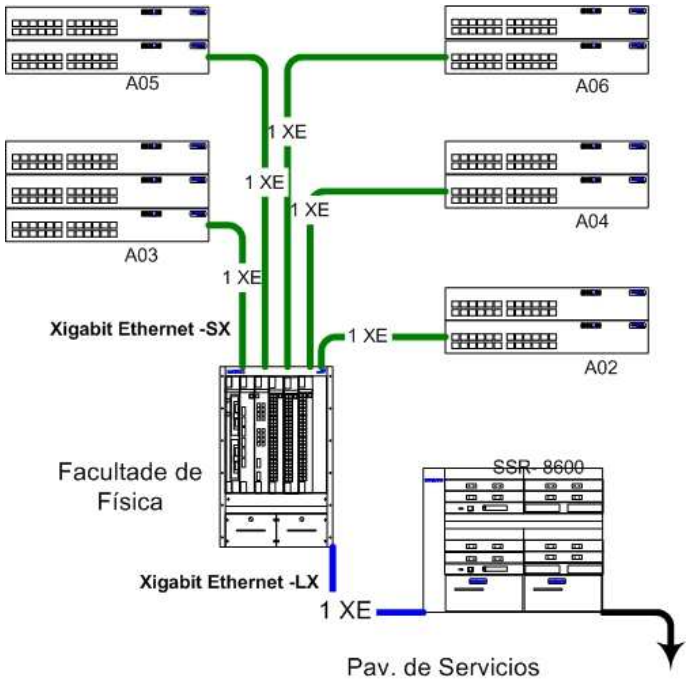
3. **Armario de distribución de planta**. Es el armario al que llegan los cables procedentes de las rosetas con una topología de estrella. A estos armarios llegan los cables que van a un bastidor de rosetas que luego se utilizará para conectarlos al switch de planta. Este dispositivo se inserta en una serie de de raíles que hay en los armarios.

4. **Cableado vertical**. Se utiliza fibra óptica para conectar los diferentes armarios de distribución de planta.

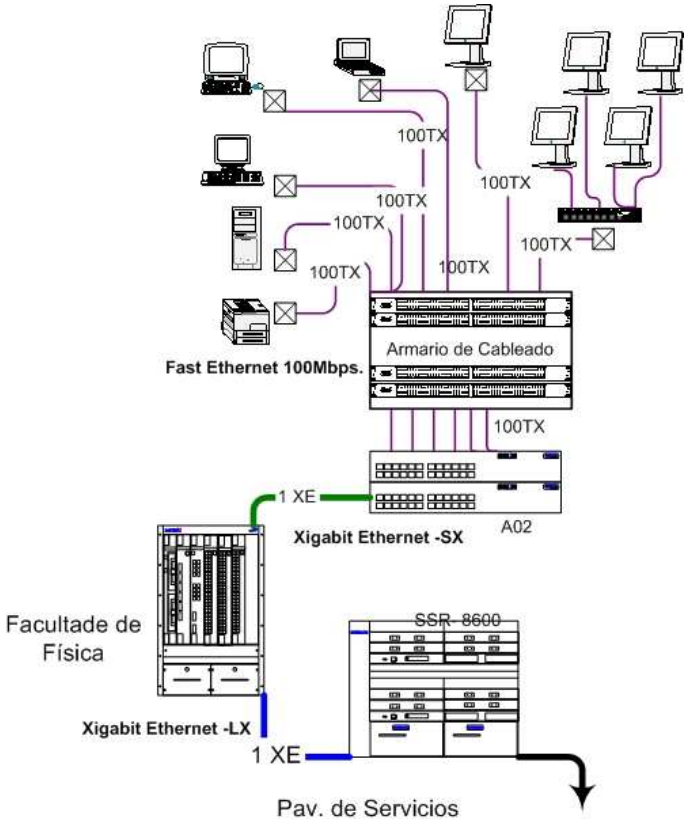
5. **Armario de distribución principal**. Existe un armario principal que suele estar en el sótano, planta baja o donde sea más fácil el acceso para la conexión con la red backbone exterior de fibra óptica.



Más en detalle, en las plantas tenemos uno o varios Vertical Horizon en configuraciones de 24, 48, 72, ... hasta 168 puertos Fast Ethernet configurados mediante una pila de switches y con una conexión Ethernet Gigabit como mínimo.



Por último, encontramos el cableado estructurado de planta y los equipos de usuarios (ordenadores personales, servidores, impresoras de red, ...). En algunos laboratorios o aulas de informática podemos encontrar concentradores de menor capacidad, aunque están siendo sustituidos progresivamente.



La USC dispone también de una red inalámbrica proporcionada por más de 400 puntos de acceso. La cobertura prevista en cada uno de los edificios está aproximadamente entre el 80 % y el 90 % del espacio útil del edificio, priorizándose las zonas comunes: bibliotecas, salas de lecturas, corredores con zonas de trabajo, aulas magnas, salas de juntas, así como los espacios de docencia e investigación. En resumen:

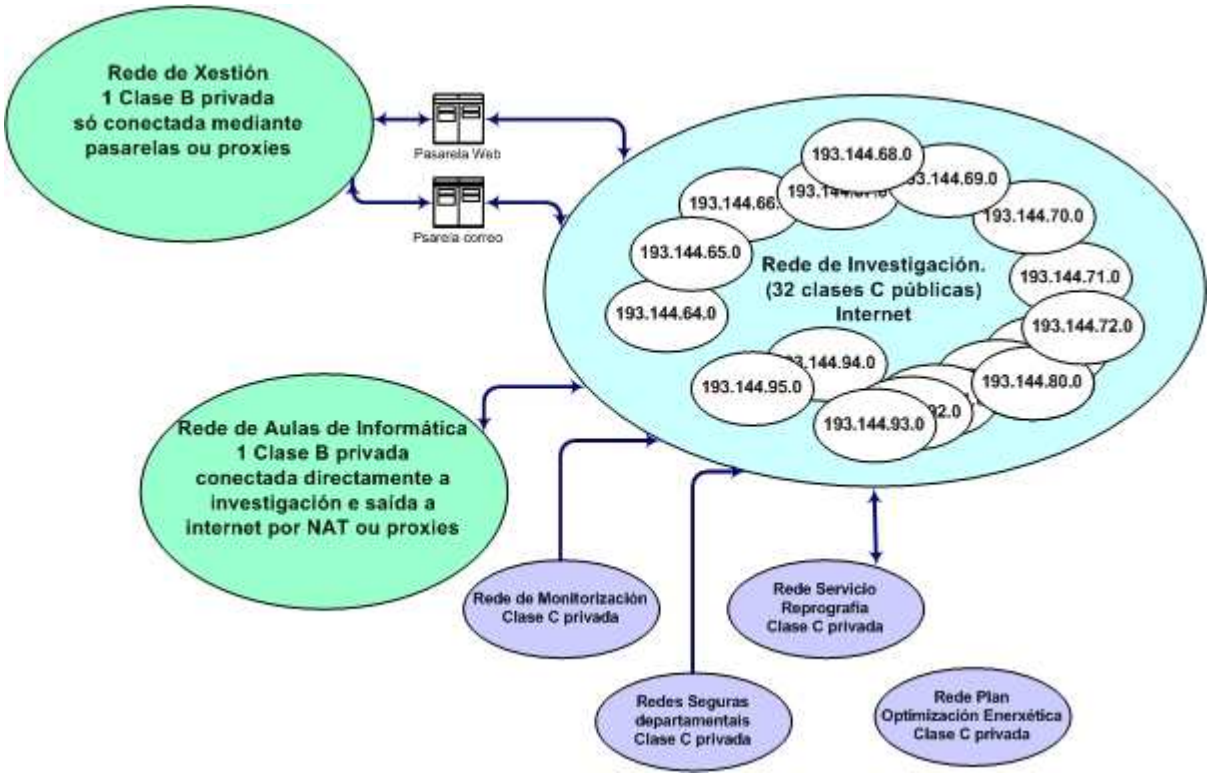
Fibra óptica:	+30 km
Par trenzado:	+450 km
Edificios interconectados:	80
VLANs:	100
Armarios de distribución:	160
Ordenadores:	+7000
Puntos de acceso inalámbrico:	444

4.4.4. Topología lógica de la red

Sobre esta infraestructura tenemos definidos un conjunto complejo de Redes Virtuales (VLANs) cuya topología depende tanto de factores históricos, disponibilidad de direcciones IP legales, necesidades de los distintos grupos de usuarios, seguridad, etc, respondiendo en cada caso a alguna o varias de estas características.

Redes generales definidas:

- **Red de Gestión:** 1 clase B privada, aislada del resto de las redes mediante filtros, sólo tiene conexión exterior mediante pasarelas web y correo electrónico.
- **Red de Aulas de Informática (RAI):** 1 clase B privada, conexión al resto de las redes de la USC, pero utilizan NAT o Proxies para la salida a Internet.
- **Redes de Investigación:** 32 Clases C legales, actualmente algunas están fraccionadas mediante subredes.
- **Redes privadas departamentales:** muchos departamentos solicitan mayor seguridad por lo que son movidos a una red privada virtual que está conectada al resto mediante un cortafuegos o conjunto de lista de acceso (ACLs) utilizando NAT para la traducción de direcciones. Las soluciones son muy variadas: cortafuegos comerciales (CISCO PIX), cortafuegos software (Linux), o ACL´s de los propios encaminadores Enterasys.
- **Red de monitorización, telefonía, Reprografía, POE, ...:** cada una de estas redes especiales tiene un cometido muy concreto y en función des ellos tienen distintas características.



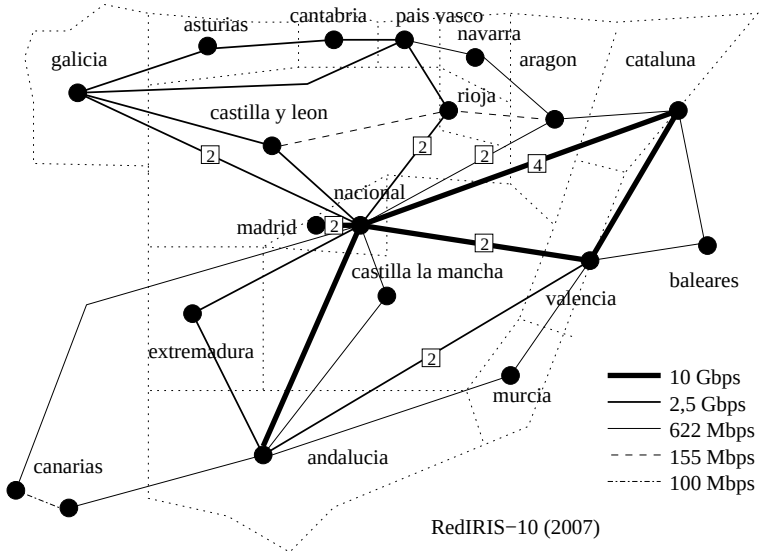
4.5. La red nacional de investigación

4.5.1. RedIRIS

RedIRIS[7] es la red académica y de investigación nacional española que interconecta las universidades y centros de investigación. Es una red propia que da acceso, de forma directa o indirecta, a más de 260 organizaciones. Está constituida por una red troncal de topología malla con enlaces a 2,5 y 10 Gbps que une los 18 los nodos existentes, uno en cada Comunidad Autónoma, excepto en las Islas Canarias, donde hay dos nodos.

RedIris está conectada a otras redes de investigación europeas y mundiales. Así, RedIRIS participa en el Proyecto GEANT que constituye una red IP paneuropea académica y de investigación. GEANT posee una red troncal de 10 Gbps y accesos de hasta 2,5 Gbps. El nodo de RedIRIS está Madrid esta conectado con Suiza por un enlace de "fibra oscura" (que provee múltiples longitudes de onda a 10 Gbps) con Francia por un enlace de 10 Gbps y con Portugal a 2,5 Gbps. GEANT también provee la conexión de RedIRIS con Internet2 (Abilene, ESnet).

Para el tráfico con la Internet global comercial RedIRIS dispone de un punto neutro de interconexión para el intercambio de tráfico IP entre los proveedores de tránsito internacional a Internet existentes en España (EspaNIX). RedIRIS se conecta a este punto neutro mediante dos enlaces Gigabit Ethernet.

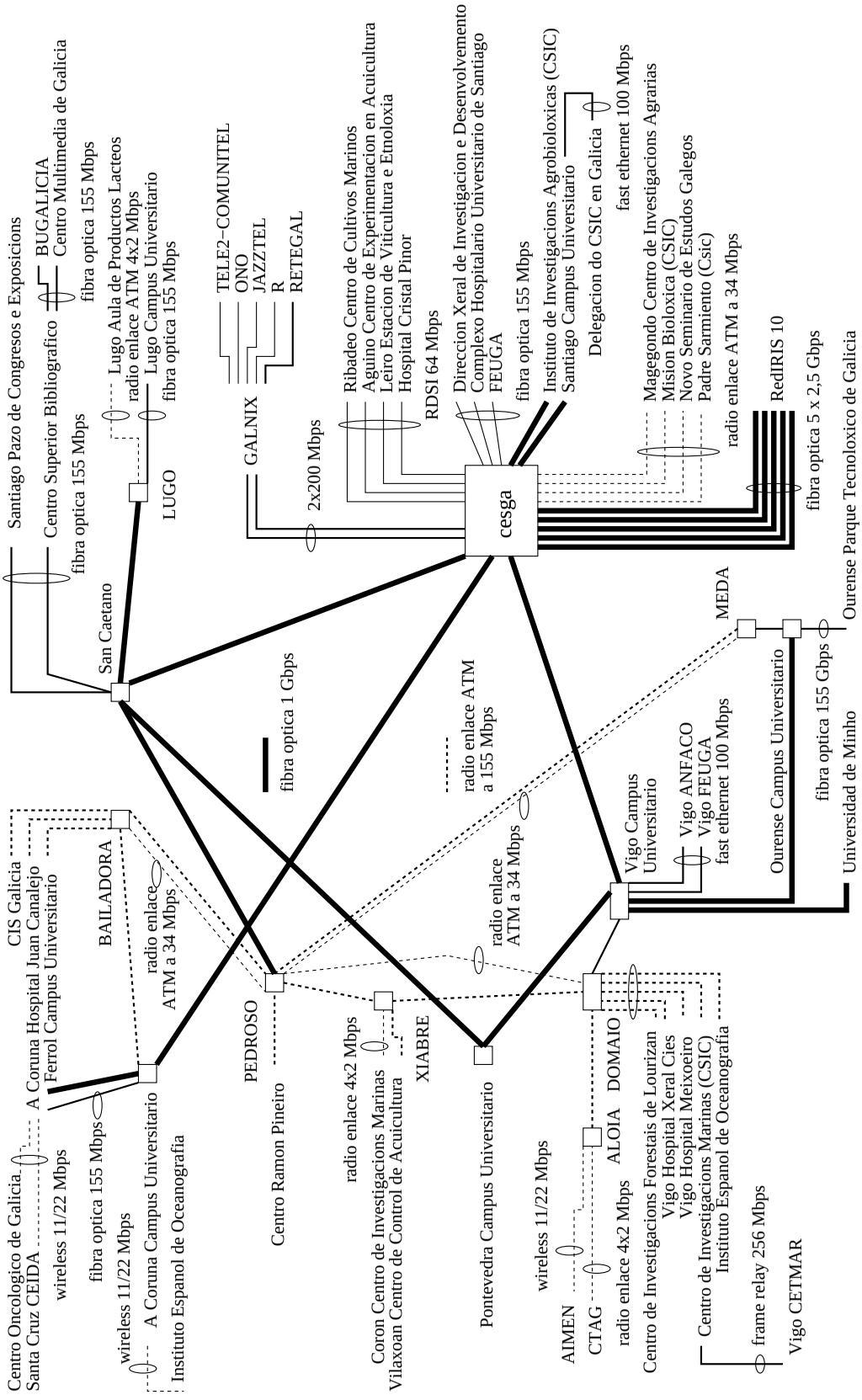


4.5.2. RECETGA

En Galicia la gestión de la red académica y de investigación la realiza RECETGA[8].

[7] `http://www.rediris.es`.

[8] `http://www.cesga.es`.


Santiago Pazo de Congresos e Exposicions
Centro Superior Bibliografico
fibra optica 155 Mbps
BUGALICIA
Centro Multimedia de Galicia
fibra optica 155 Mbps
Lugo Aula de Productos Lacteos
radio enlace ATM 4x2 Mbps
Lugo Campus Universitario
fibra optica 155 Mbps
LUGO
TELE2−COMUNITEL
ONO
JAZZTEL
R
RETEGAL
GALNIX
2x200 Mbps
Ribadeo Centro de Cultivos Marinos
Aguiño Centro de Experimentacion en Acuicultura
Leiro Estacion de Viticultura e Etnoloxia
Hospital Cristal Pinor
RDSI 64 Mbps
Direccion Xeral de Investigacion e Desenvolvemento
Complexo Hospitalario Universitario de Santiago
FEUGA
fibra optica 155 Mbps
Instituto de Investigacions Agrobioloxicas (CSIC)
Santiago Campus Universitario
Delegacion do CSIC en Galicia
fast ethernet 100 Mbps
Magegondo Centro de Investigacions Agrarias
Mision Bioloxica (CSIC)
Novo Seminario de Estudos Galegos
Padre Sarmiento (Csic)
radio enlace ATM a 34 Mbps
RedIRIS 10
fibra optica 5 x 2,5 Gbps
Ourense Parque Tecnoloxico de Galicia
cesga
San Caetano
fibra optica 1 Gbps
radio enlace ATM
a 155 Mbps
MEDA
Vigo Campus
Universitario
Vigo ANFACO
Vigo FEUGA
fast ethernet 100 Mbps
Ourense Campus Universitario
fibra optica 155 Gbps
Universidad de Minho
CIS Galicia
A Coruna Hospital Juan Canalejo
Ferrol Campus Universitario
wireless 11/22 Mbps
BAILADORA
fibra optica 155 Mbps
wireless 11/22 Mbps
A Coruna Campus Universitario
Instituto Espanol de Oceanografia
radio enlace
ATM a 34 Mbps
PEDROSO
Centro Ramon Pineiro
radio enlace 4x2 Mbps
Coron Centro de Investigacions Marinas
Vilaxoan Centro de Control de Acuicultura
XIABRE
Pontevedra Campus Universitario
radio enlace
ATM a 34 Mbps
wireless 11/22 Mbps
AIMEN
CTAG
radio enlace 4x2 Mbps
ALOIA
DOMAIO
Centro de Investigacions Forestais de Lourizan
Vigo Hospital Xeral Cies
Vigo Hospital Meixoeiro
Centro de Investigacions Marinas (CSIC)
Instituto Espanol de Oceanografia
frame relay 256 Mbps
Vigo CETMAR
Centro Oncologico de Galicia
Santa Cruz CEIDA

Actualmente RECETGA da servicio de comunicaciones a los siete Campus Universitarios gallegos, Centros Tecnológicos y de Investigación dependientes de la Xunta de Galicia, Consejo Superior de Investigaciones Científicas (CSIC), Instituto Español de Oceanografía, Laboratorios de Investigación de Complejos Hospitalarios y más de veinte instituciones y empresas que trabajan en I+D+I. El número de usuarios de la red se cifra entorno a los 100.000, incluyendo, docentes, investigadores, estudiantes, etc.

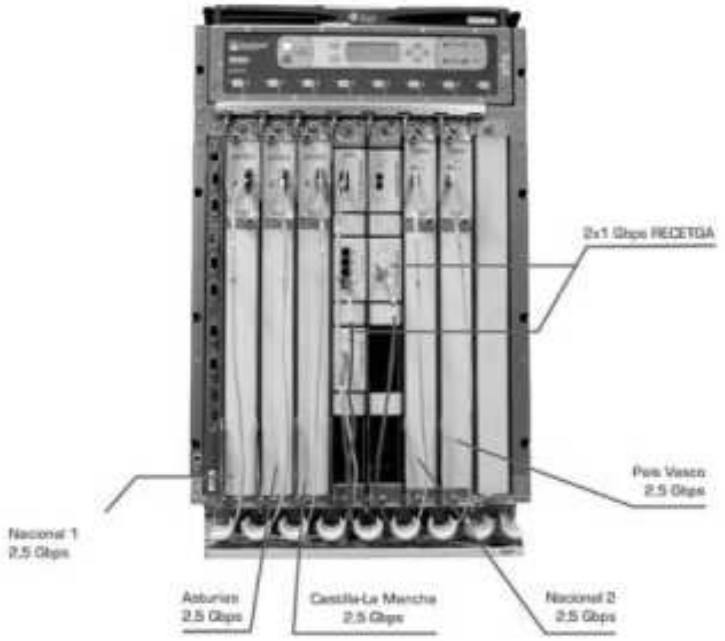
RECETGA es una red ATM soportada sobre fibra óptica y radioenlaces, con un ancho de banda en la troncal de hasta 1 Gbps. La topología es mixta, presentando una troncal mallada en su mayor parte y el resto en estrella, con un nodo central situado en Santiago de Compostela. Más en concreto, está formada por los siguiente elementos:

1. Red troncal. Basada en fibra óptica a 1 Gbps y radioenlaces de SDH a 155 Mbps. Además dispone de dos anillos de radioenlaces (norte y sur) al que se conectan los enlaces de distribución. El equipo consta de conmutadores ATM de modelos FORE y Marconi ASX-1000 y routers Gigabit Ethernet/ATM de modelos Juniper M-Series (M20, M10 y M10i). Transmite tráfico CBR, ABR, VBR y UBR.

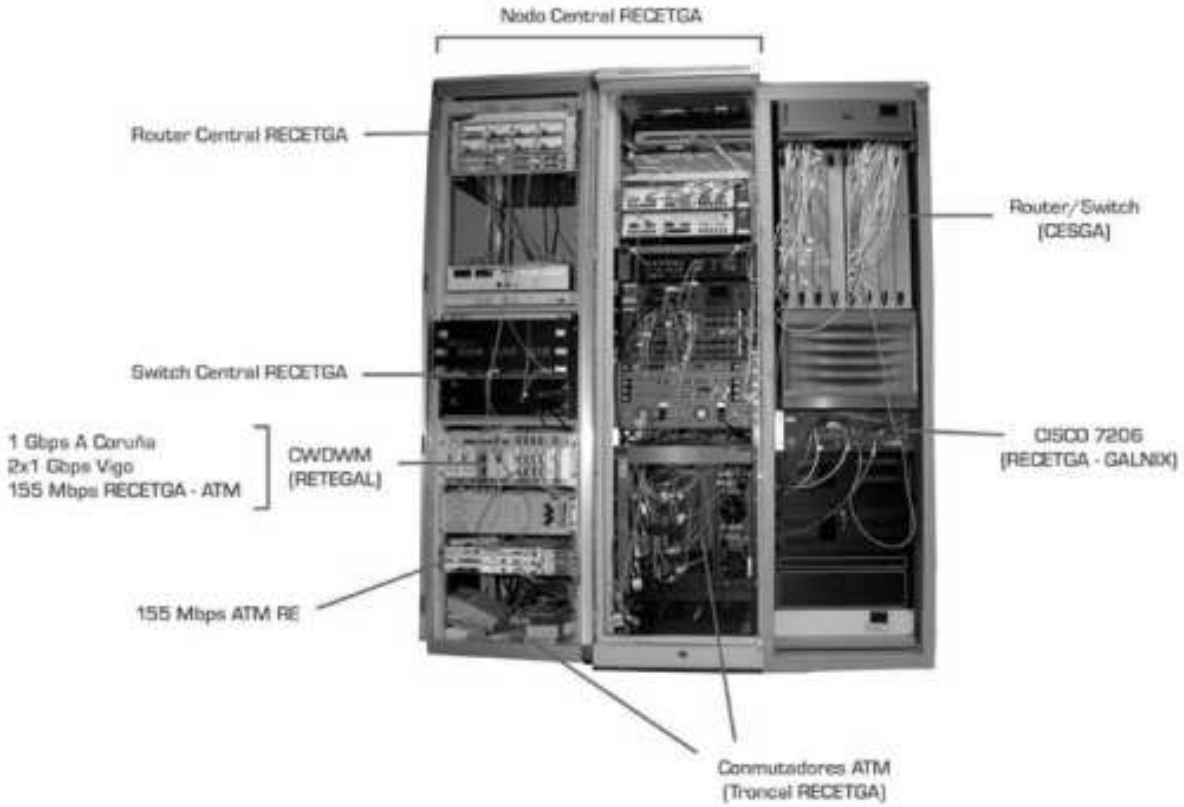
2. Red de distribución. Basada en fibra óptica a 1 Gbps y 155 Mbps y radioenlaces SONET/SDH a 155 Mbps. En casos puntuales, enlaces Frame Relay, RDSI, Ethernet o Wireless. Los equipos son conmutadores ASX200, FORE, CISCO, LAX-20, PowerHUB 6000 y 7000, ENTERASYS XP-2400 y Juniper M10.

3. Conexiones exteriores. Se conecta con RedIRIS a través de 5 enlaces de fibra óptica de 2,5 Gbps. También se conecta a Galnix (punto neutro de intercambio de Internet en Galicia) a través de Gigabit Ethernet.

A continuación se muestra un nodo Juniper M40e de RedIRIS en Galicia.



Y en la siguiente figura el nodo central de RECETGA instalado en el Cesga.



Bibliografía

[1] W. Stallings, *Comunicaciones y redes de computadores*, ISBN 8420541109, 2004, Pearson.

[2] P. Oppenhaeimer, *Top-down network design*, ISBN 1587051524, 2004, Cisco Press.

[3] Cisco Systems, *Small Enterprise Design Profile Reference Guide*. Disponible para descarga: `http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Small_Enterprise_Design_Profile/SEDP.html`

[4] Cisco Systems, *Medium Enterprise Design Profile Reference Guide* . Disponible para descarga: `http://www.cisco.com/c/en/us/td/docs/solutions/Enterprise/Medium_Enterprise_Design_Profile/MEDP.html`

[5] Cisco Systems, *Academia de networking de Cisco Systems: guía del primer año*", ISBN 842054079X, 2004, Pearson.

[6] J.F. Kurose y K.W. Ross, *Redes de Computadores. Un enfoque Descendente Basado en Internet*, ISBN 8478290613, 2010, Pearson Addison Wesley.

[7] E. Magaña, E. Izme Mendi, M. Prieto Minguez y J. Villadangos Alonso, *Comunicación y Redes de Computadores. Problemas y Ejercicios Resueltos*, ISBN 8420539201, 2003, Pearson Prentice-Hall.

[8] N. Barcia Vázquez y otros, *Redes de computadores y arquitecturas de comunicaciones: supuestos práticos*, ISBN 8420546070, 2005 Pearson.

[9] E. Tittel, *Redes de computadores*, ISBN 8448142802, 2004, McGraw-Hill.