

Unidad 2



Redes locales

Planificación y Administración de Redes



Índice



2.1. Proyecto IEEE 802

2.2. La familia Ethernet (IEEE 802.3)

2.2.1. Ethernet → Tasa de transferencia 10 Mbps

2.2.2. Fast Ethernet → Tasa de transferencia 100 Mbps

2.2.3. Gigabit Ethernet → Tasa de transferencia 1 Gbps

2.2.4. 10 Gigabit Ethernet → Tasa de transferencia 10 Gbps

2.3. Token Bus (IEEE 802.4)

2.4. Token Ring (IEEE 802.5)

2.5. FDDI (ANSI y IEEE 802.8)

2.6. WLAN. Wireless LAN (IEEE 802.11)

2.7. Espacios y recorridos para telecomunicaciones en edificios comerciales (ANSI/TIA/EIA 569-B)

2.7.1. Espacios de las redes locales

2.7.2. Canalizaciones

2.8. Cableado de telecomunicaciones en edificios comerciales (ANSI/TIA/EIA 568-C)

2.8.1. Herramientas para trabajar con cableado y conectores

3.1.2. Cable coaxial

3.1.3. Fibra óptica

2.8.2. Fabricación de cables

2.8.3. Conexión de tomas y paneles de parcheo

2.8.4. Recomendaciones en la instalación del cableado



Introducción

Una LAN o Red de Área Local se trata de un sistema que nos va a permitir el compartir recursos y comunicar distintos dispositivos ubicados en una determinada área geográfica.

Sus **características principales** son:

- > Máxima distancia total de la red: 4km.
- > Mínima tasa de velocidad: 1 Mbps.
- > Topología física: bus, anillo, estrella (los más habituales).
- > Baja tasa de error: $10^{-11} < \text{Tasa} < 10^{-8}$.
- > Titularidad: privada.
- > Configuración de la línea: difusión.
- > Estándares: Ethernet, FDDI, Wifi, etc.

Ventajas:

- > Compartir recursos: nos facilitan el poder compartir ciertos recursos que si los pusieramos para cada equipo en particular nos saldría mucho peor económicamente hablando.
- > Mayor Fiabilidad: las funciones se van a repartir entre los distintos integrantes de la red y habrá una redundancia controlada respecto a los datos para poder recuperarlos en caso de error.

- > Administración eficiente: toda la gestión se lleva desde un punto de administración central. Nos referimos a gestión de usuarios, grupos, directivas, etc....
- > Flexibilidad: si cambiamos la situación física de los dispositivos no afecta a su funcionamiento.
- > Automatización de tareas: de la mano con la gestión centralizada va este punto, que trata de automatizar tareas como copias de seguridad, los apagados automáticos, y otros mecanismos.

Inconvenientes:

- > Es posible la opción de que haya pérdidas en cuanto a seguridad y privacidad de los datos nos referimos.
- > Los datos y los recursos están dispersos y no conjuntos.
- > Es más difícil de gestionar que un equipo solamente,

No obstante, todos estos inconvenientes y ventajas tienen distintas aplicaciones como iremos viendo a la largo de esta unidad.

Al finalizar esta unidad

- + Conoceremos en que consiste el proyecto IEEE 802.
- + Sabremos diferenciar las distintas implementaciones del estándar Ethernet IEEE 802.3.
- + Podremos conocer el funcionamiento de las dos implementaciones posteriores a IEEE 802.3 como son IEEE 802.4 e IEEE 802.5.
- + Identificaremos en que consiste el estándar dedicado a FDDI.
- + Sabremos cómo funcionan las diferentes redes inalámbricas y sus implementaciones con respecto a la seguridad.
- + Seremos capaces de estructurar un edificio entero de telecomunicaciones y de crear el cableado necesario para su implantación.



2.1.

Proyecto IEEE 802

IEEE es el acrónimo de Institute of Electrical and Electronics Engineer. Las redes Ethernet en bus se rigen por el estándar IEEE 802.3.

IEEE se utiliza mucho en las redes de área local, normalmente IEEE 802. Es un proyecto del instituto de ingenieros eléctricos y electrónicos en el que se definen las normativas que deben seguir los fabricantes de productos de redes LAN y MAN para que si queremos montar una red LAN podremos utilizar el producto del fabricante que queramos y no tendremos problemas de incompatibilidad con estos. Esto se debe gracias a que todos los fabricantes han seguido las normas establecidas en IEEE 802.

Las que más se utilizan son:

- > **IEEE 802.1:** Normativa para las interfaces y modelo de referencia para la interconexión de sistemas abiertos.
- > **IEEE 802.1D:** Normativa para el protocolo de árbol en expansión.
- > **IEEE 802.1Q:** Normativa para las VLAN.
- > **IEEE 802.2:** Normativa para el control de enlace lógico.
- > **IEEE 802.3:** Normativa de Ethernet.
- > **IEEE 802.11:** Normativa para WLAN.
- > **IEEE 802.16:** Normativa para WIMAX.

2.2.

La familia Ethernet (IEEE 802.3)

La familia ethernet referida en el estándar IEE 802.3 fue desarrollada en primera instancia por el grupo formado por Digital, Intel y Xerox que se hacían llamar grupo DIX; fue ya en 1985 cuando el IEE decidió estandarizarlo con el objetico de que creará una compatibilidad con el modelo OSI que vimos en la primera unidad.

Ethernet es un conjunto de redes de área local donde se definen:

- > **Protocolos a nivel de enlace.**
- > **Tecnologías a nivel físico.**

Es por esto por lo que podemos decir que Ethernet engloba el primer nivel del modelo OSI y el subnivel MAC del nivel de enlace.



Imagen 2. Niveles OSI de Ethernet



Características físicas

Las redes LAN usan señales digitales, varias codificaciones como pueden ser por ejemplo 4B5B, 8B6T o PAM-5. También usa comunicación Full Dúplex, en ambas direcciones, pero al mismo tiempo no existe multiplexación porque hay un único canal de datos. Para terminar, hay que comentar que también se usan repetidores, hubs y switches con la intención de reconstruir la señal.

La topología usada actualmente es en estrella y los costes a la hora de implementar dicha red son relativamente bajos.

Método de acceso al medio: CSMA/CD

Ya vimos en la unidad anterior que es posible que se quiera enviar mucha información de muchos sitios al mismo tiempo y se pueda llevar a cabo una colisión que terminaría en una pérdida de información.

En las LAN existe un mecanismo, que en realidad es perteneciente a Ethernet, que nos regula el envío de esta información o de estas señales con el fin de que no haya colisiones: CSMA/CD (Acceso Múltiple con Detección de Portadora y Detección de Colisiones).

Direccionamiento físico

Cada conector de red por ethernet existe porque hay una tarjeta o adaptador de red, también llamados NIC. Estas tarjetas van ligadas a una dirección física llamada MAC que consiste en 12 dígitos hexadecimales,

Dos comandos para poder conocer las direcciones MAC de las tarjetas de red de un equipo son:

- > En el CMD o Powershell de Windows: `ipconfig /all`.
- > En el terminal de Linux: `ip a s`.

```

adaptador de Ethernet Ethernet:
.
.
.
Sufrido DNS específico para la conexión. . . :
Descripción . . . . . : Realtek PCIe GbE Family Controller
Dirección física. . . . . : 04-42-1A-26-FC-47
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::b45a:3718:267b:32df%4(Preferido)
Dirección IPv4. . . . . : 10.10.30.151(Preferido)
Máscara de subred . . . . . : 255.255.0.0
Concesión obtenida. . . . . : jueves, 30 de diciembre de 2021 6:56:19
La concesión expira . . . . . : jueves, 30 de diciembre de 2021 12:51:18
Puerta de enlace predeterminada . . . . . : 10.10.10.1
Servidor DHCP . . . . . : 10.10.10.1
IAID DHCPv6 . . . . . : 100942362
DUID de cliente DHCPv6. . . . . : 00-01-00-01-29-46-19-F0-04-42-1A-26-FC-47
Servidores DNS. . . . . : 8.8.8.8
NetBIOS sobre TCP/IP. . . . . : habilitado

```

Imagen 3. Ejemplo de salida de `ipconfig /all`, se puede observar la dirección física



Implementaciones

Con las implementaciones queremos hacer referencia a las distintas versiones de Ethernet que coexisten.

La implementación se representa del siguiente modo: tiene un número al principio que hace referencia a la tasa de transferencia en Mbps, es decir, cuantos megabits por segundo es capaz de transmitir; en segunda posición está el tipo de transmisión, que puede ser Base (lo más común), o Broad y por último tiene la longitud del segmento (máxima longitud del cable sin regeneración de señal) o el tipo de cable, incluso los dos.

Una imagen explicativa:



Imagen 4. Código para implementaciones Ethernet

Las implementaciones más conocidas:

> Ethernet (IEEE 802.3)

- » **10Base5** (10 Mbps y coaxial 500 m)
- » **10Base2** (10 Mbps y coaxial 185 m)
- » **10BaseT** (10 Mbps y par trenzado 100 m)
- » **10BaseF** (10 Mbps y fibra óptica 2000 m)

> Fast Ethernet (IEEE 802.3u)

- » **100BaseTX** (100 Mbps y par trenzado de 2 pares 100 m)
- » **100BaseT4** (100 Mbps y par trenzado de 4 pares 100 m)
- » **100BaseFX** (10 Mbps y fibra óptica 2000 m)
- » **Gigabit Ethernet** (IEEE 802.3ab)
- » **1000BaseX** (1 Gbps y fibra óptica)
- » **1000BaseT** (1 Gbps y par trenzado 100 m)

> 10 Gigabit Ethernet (IEEE 802.3ae)

- » **10GBaseSR, 10GBaseLR, 10GBaseCX4** (10 Gbps y fibra óptica)
- » **10GBaseT** (10 Gbps y par trenzado 100 m)



2.2.1. Ethernet → Tasa de transferencia 10 Mbps

10Base5

En 1983 se crea el primer estándar definido en el IEEE 802.3 al que denominan Ethernet de cable grueso.

Como su topología es en bus, tienen una transmisión en banda base y su longitud máxima por segmento es de 500 metros. Teniendo todo esto en cuenta sacamos en claro que la longitud máxima total de la red es de 2500 metros.

Mínimo debe haber una distancia de 2.5m entre cada puesto, permitiendo que haya 1024 estaciones en total.

El cable que se usa es un coaxial grueso RG-8 de un centímetro de diámetro y que no se puede curvar debido a la rigidez que tiene, hoy en día está en desuso.

10Base2

Esta fue la segunda implementación desarrollada para el estándar IEEE 802.3 a la que llamaban Ethernet de cable fino.

Conseguía la misma velocidad que el anterior, pero ahorrando costes, lo que la hacía una opción más asequible.

Usaba una topología física en bus y tenía un tamaño de segmento máximo de 185 metros.

Su estructura física es la siguiente: tarjeta de red interna, un cable coaxial fino RG-59 que tiene 5 milímetros de grosor y sus conectores son BNC.

El que la topología física fuera en bus creaba problemas conforme la red LAN crecía debido a que un fallo de cualquiera de los cables causaba el apagado de toda la red. Es por esto por lo que todas las implementaciones de 10Base2 que había han desaparecido del mundo de las redes.

10BaseT

La topología usada es la de estrella y se ayuda de un hub en el centro que tiene un puerto para cada una de las estaciones, con las que se conecta con un cable par trenzado UTP.

En cambio, como el hub transmite todas las tramas a todas y cada una de las estaciones y es cada tarjeta de red la encargada de saber si es la suya o no, la topología lógica usada es en bus.

Se pueden tener hasta 1024 equipos con un tamaño máximo de 100m por segmento.

El dominio de colisión, es decir, el ámbito en el que es posible que suceda una colisión entre distintos envíos de información, está formado por los equipos que están conectados al hub. Esto se traduce en que cuanto más hubs tengamos, mayor es el dominio de colisión.

Los hubs nos ayudan a tener más equipos interconectados unos a otros, pero la tasa de transferencia es repartida entre todos los equipos conectados al mismo tiempo que crece la probabilidad de colisión, lo que hace que el rendimiento se vea afectado por esto.

Aunque el tener una topología en estrella nos ayuda a que si hay un fallo concreto en la red esta no se desconecte al completo, el número de colisiones sigue siendo muy alto y su ancho de banda se reduce más a cada nuevo equipo conectado.

Esta problemática se resolvió con la aparición del switch. Este dispositivo no permite las colisiones y mantiene la misma tasa de transferencia para cada uno de los puertos.

El único problema que seguía latente era que solo 10 Mbps es una velocidad bastante lenta para las necesidades de una LAN, por lo que surgieron nuevas implementaciones.



2.2.2. Fast Ethernet → Tasa de transferencia 100 Mbps

Fue ya en los 90 cuando se implementó un nuevo estándar que se apoyaba en el uso de unos sistemas de codificación lo suficientemente eficientes como para posibilitar una tasa de transferencia de 100 Mbps. Esto, unido a que gracias al switch y a su capacidad para enviar la información al destinatario concreto de cada mensaje hace que el estándar Fast Ethernet sea el más usado en todo el mundo.

Otra característica que lo hacía tan usado era que cuando teníamos una instalación previa realizada no era necesario que se cambiara entera, simplemente se cambiaban las tarjetas de red y el nodo central para que se pudiera transmitir hasta 100 Mbps. Esto era posible en la gran mayoría de los casos, pero no siempre.

Las implementaciones más extendidas a lo largo del tiempo han sido: 100BaseT4, 100BaseTX, 100BaseFX.

100BaseT4

Este estándar usa cuatro pares de hilos trenzados UTP categoría 3 o superior en los que dos pares son bidireccionales y los otros son unidireccionales.

Si traducimos esto, llegamos a la conclusión de que para cada dirección hay 3 pares en cada momento, si dividimos, vemos que los 100 Mbps se reparten en 33.6 Mbps por par.

Su longitud máxima para cada segmento es de 100 metros.

100BaseTX

En este caso son dos los pares que se usan, y son de hilos trenzados UTP o STP, categoría 5 o superior.

Mientras que uno de los pares envía la información, el otro la recibe. Esto es implementado porque su modo de transmisión es Full-Dúplex con un switch de intermediario.

La longitud máxima para cada segmento sigue siendo de 100 metros.

100BaseFX

Este estándar es el primero que usa fibra óptica de todos, dos hilos multimodo. La primera es usada para transmitir tramas mientras que la segunda las recibe al mismo tiempo que intenta detectar colisiones.

Su modo de transmisión es Half-Dúplex simétrico con el código de bloque de 4B/5B.

La longitud máxima por segmento en 100BaseFX es de 2000 metros, es decir, 2 kilómetros.

Implementaciones Fast Ethernet			
Implementación	Medio	Características	Segmento máximo
100BaseFX	Fibra óptica Multimodo	Láser onda 1300 nm	2 km
100BaseTX	Par trenzado	Categoría 5	100 m
100BaseT4	Par trenzado	Categoría 3	100 m



2.2.3. Gigabit Ethernet → Tasa de transferencia 1 Gbps

Aunque en un principio su diseño iba orientado a fibra óptica, se admite el uso del par trenzado.

Su codificación es 8B/10B y sus implementaciones son: 1000BaseZX, 1000BaseLX, 1000BaseSX y 1000BaseT.

1000BaseT

Es la única de las implementaciones de GigaBit Ethernet que funciona con cable de par trenzado, y la diferencia de las anteriores que lo usaba es que emplea los cuatro pares de hilos de cable para transmitir de manera simultánea en ambos sentidos. Esto consigue que la velocidad se multiplique por 8 gracias también a que se aplica un sistema electrónico que cancela el eco. Es soportado por cables UTP de categoría 5e o superior.

Una de las características a tener más en cuenta con el estándar 1000BaseT es que también es interoperable con los otros estándares que usan par trenzado.

Implementaciones de Gigabit Ethernet			
Implementación	Medio	Señal	Segmento Máximo
1000BaseZX	Fibra Monomodo	Láser 1550 nm	80 km
1000BaseLX	Fibra Monomodo	Láser 1310 nm	5 km
1000BaseSX	Fibra Multimodo 50/125 micras	Láser 850nm	550 m
1000BaseT	UTP	Eléctrica	100 m

2.2.4. 10 Gigabit Ethernet → Tasa de transferencia 10 Gbps

Fue publicada en un nuevo estándar en 2002, en el estándar IEEE 802.3ae, y su uso principal debido a su gran potencia es para MAN o WAN, pero se puede aplicar a una LAN, aunque no es lo común.

Sus implementaciones, que vamos a describir más abajo son sobre fibra óptica y sobre par trenzado categoría 6 y 7.

Implementaciones de 10 Gigabit Ethernet			
Implementación	Medio	Señal	Segmento máximo
10GBaseER	Fibra monomodo	Láser 1550 nm	80 km
10GBaseLR	Fibra Monomodo	Láser 1310 nm	5 km
10GBaseSR	Fibra Multimodo 50/125 micras	Láser 850 nm	300 m
10GBaseT	FTP/STP	Eléctrica	100 m



2.3.

Token Bus (IEEE 802.4)

Este estándar define una topología física en bus que a su vez usa una topología lógica en anillo.

La primera estación empezando por arriba es la encargada de empezar con el envío de la información. Acto seguido, pasa a su estación contigua el permiso para transmitir la trama, esto lo realiza mediante una trama de control a la que llamamos testigo (token). Este testigo va a ir de estación en estación hasta el destino del mensaje y únicamente las máquinas que tengan este testigo tienen la capacidad de transmitir la trama con la información. Token bus lo que nos permite es que añadamos y quitemos estaciones del anillo.

Este es un protocolo bastante complejo debió a que cada una de las estaciones debe mantener 10 temporizadores y más de 24 variables de estado.

El medio de transmisión es un cable coaxial de antena con 75 ohmios de potencia. Su tasa de transmisión va a ser variable, entre 1 y 10 Mbps.

Realmente, este estándar no se usa en los puestos informáticos de una empresa común, se suele usar en otros como por ejemplo una fábrica de coches moderna en la que todo vaya automatizado y los nodos de los equipos se encargan de los procesos de elaboración de un vehículo. Este es el caso de algunas fábricas de Toyota en china que ya están totalmente automatizadas.

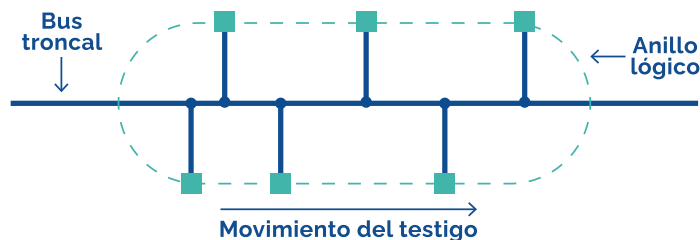


Imagen 5. Red local Token Bus



2.4.

Token Ring (IEEE 802.5)

Como se ha ido viendo a lo largo de los distintos estándares, cuando se usa una red ethernet es muy fácil que se sufran colisiones entre las tramas de envío de información. Esto se traduce en retrasos de tiempo indefinido a la hora de la entrega de los datos al destinatario, y más se acentuará el problema conforme más crezca la red.

La solución que se propone para estos problemas es la red en anillo con paso de testigo ya que les exige que las estaciones manden la información por turnos.

Método de acceso: paso de testigo

El testigo se trata de una trama con la función puramente de controlar que va a ir pasando de manera consecutiva por todas las estaciones del anillo. Solo las estaciones que esté en posesión de ese testigo podrán enviar información, pero no interviene a la hora de recibir.

Implementación

Su organización es la siguiente, su topología lógica es en anillo, mientras que, aunque la física suele ser en anillo, también nos la podemos encontrar en estrella. Independientemente de esto último, la codificación que usa es Manchester diferencial y su velocidad puede llegar hasta los 16 Mbps.

Cada sección va a conectar dos estaciones vecinas, y la última con la primera para que así se cierre el círculo. Esto último siempre que la topología sea en anillo, que es lo más común.



2.5.

FDDI (ANSI y IEEE 802.8)

FDDI se trata de un estándar que se basa en la transmisión de datos entre equipos ubicados en redes locales mediante fibra óptica. Esta es la principal, pero existe otro estándar que aplica las mismas normas para el trenzado, al que llamamos TP-DDI.

Sus características básicas son:

- > Tasa de transferencia de datos de 100 Mbps.
- > Topología en anillo doble, física y lógica.
- > Distancia máxima de 200 Km
- > Máximo 1000 estaciones interconectadas.

Método de acceso: paso de testigo

El acceso al medio de las tramas con información se regula del mismo modo que el definido en el punto anteriormente visto, Token Bus.

Implementación

La implementación de FDDI como hemos dicho antes se implementa con una topología de anillo doble que se basa en que el primero es el que funciona a pleno rendimiento y el segundo se tiene de respaldo en caso de fallo del primero. En algunas ocasiones se podrían usar ambos anillos al mismo tiempo para que la tasa de transferencia llegase a los 200 Mbps, pero perderíamos el respaldo, que es la base de esta topología.

Hay tres tipos de nodos para FDDI:

- > Estación dual (DAS).
- > Estación simple (SAS).
- > Concentrador de conexión (DAC).

La estación dual consta de dos conectores para que se pueda estar conectado a los dos anillos al mismo tiempo.

En general, son equipos normales los que están conectados al anillo, de manera que si falla su tarjeta de red, como es sencilla, se desconectará de la red sin que el anillo sufra.

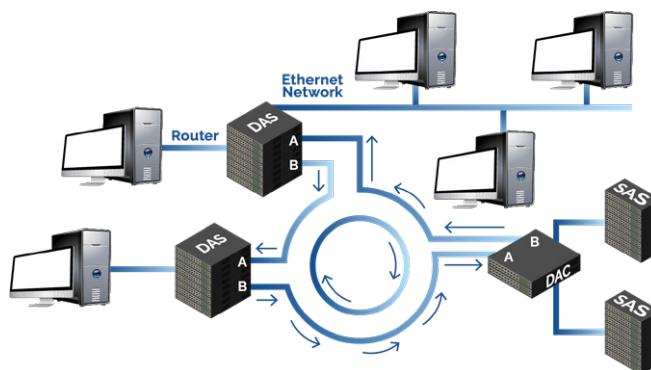


Imagen 6. Red local FDDI

Actualmente esta LAN se encuentra en desuso ya que El estándar Gigabit Ethernet es más rápido y económico.



2.6.

WLAN. Wireless LAN (IEEE 802.11)

Una WLAN, acrónimo de Wireless Local área Network, o Red inalámbrica de área local, es una red local en la que se da servicio a varios dispositivos, pero sin la necesidad de que estén conectados de manera física. En este caso la información se envía mediante ondas electromagnéticas y su medio de transmisión es el aire.

Una WLAN siempre se va a referir a una red local que es inalámbrica, cuyo propósito es que una serie de dispositivos se conecte al mismo router o punto de acceso con la intención de compartir información. No se debe confundir esto con las redes móviles de los teléfonos modernos como es el 5G, esto se trataría de una WWAN.

Además, la red WLAN también suele propiciar el acceso a internet y necesita de un cortafuegos que la asile del exterior.

Por último, como dato de interés, hoy en día los smartphones son capaces de crear puntos de acceso a los que se les denomina Wifi Direct. Todos los dispositivos que se conecten a este punto de acceso pensarán que se encuentren conectados a una WLAN normal y corriente, ya que es invisible.

Implementaciones

IEEE 802.11a

Nació de manera oficial en 1999 y usando los mismos protocolos base que el estándar IEEE 802.11, se mueve en la banda de 5 GHz con una velocidad capaz de llegar a los 54 Mbps, pero medianamente establecida en 20 Mbps. Su distancia máxima es de 200 metros y no puede interoperar con equipos del estándar siguiente.

IEEE 802.11b

Al igual que el anterior, fue creado en 1999 pero este opera en la banda de 2.4 GHz. Su velocidad es de unos 5.5 Mbps aproximadamente sobre TCP, en UDP aumenta a más o menos unos 7 Mbps.

Aunque dentro de un mismo edificio la distancia máxima de las ondas va a ser 50m, existen ciertas antenas que producen ondas capaces de alcanzar los 10 Km de distancia.

IEEE 802.11g

Se trata de una evolución del estándar anterior que se aprobó en junio de 2003.

Muy similar en cuanto a velocidad con el estándar 802.11a, opera en la banda de 2,4 GHz con una velocidad media de 22 Mbps y máxima de 54 Mbps.

Sí que es compatible con el estándar b y usa las mismas frecuencias.

Su distancia máxima es de hasta 50 km si los equipos usados son apropiados. Hay una variante que se llama 802.11g+ con el que se pueden alcanzar hasta los 108 Mbps.



IEEE 802.11n

Este estándar, que se aprobó en 2009, tiene el principal avance de que su tasa de transferencia máxima es de 600 Mbps y la tasa real suele estar en torno a los 300 Mbps.

Aunque se basa en los protocolos anteriores, se añaden numerosas mejoras:

- > Opera en 2,4GHz, pero también es capaz de operar en 5GHz, lo que lo hace compatible con todos los anteriores.
- > Se mejora la modulación OFDM, obteniendo una mayor tasa de datos.
- > Se usa la técnica MIMO, la cual consiste en que se usen múltiples antenas emisoras y otras tantas receptoras.
- > Se realiza Channel bonding con dos canales de 20 MHz en cada uno de ellos. Esta técnica se trata de la agregación de canales que estarán transmitiendo datos de manera simultánea en diferentes frecuencias, no se solapan.

IEEE 802.11ac

Evoluciona directamente del estándar IEEE 802.11n y su creación se llevó a cabo en 2014.

Su principal objetivo es que se aumente la tasa de transferencia máxima hasta los 1,3 Gbps. Esta implementación se mueve en una frecuencia de 5 GHz, su ancho de banda es de 160 MHz y tiene una modulación 256-QAM. Una de las principales ventajas es que consume una energía menor que las anteriores, lo que la hace muy útil en el uso de dispositivos móviles.

Seguridad en redes Wifi

La primera implementación de seguridad en redes inalámbricas nace en 1999 con el sistema WEP.

El sistema WEP (Wired Equivalent Privacy) usa un cifrado que en principio se incluyó solamente para redes 802.11. Este sistema se basa en un algoritmo que usa claves de 64 o 128 bits y es llamado RC4. Más tarde se ha ido viendo que este sistema tenía una cantidad asombrosa de fallos y debilidades gracias al análisis de su criptografía. De hecho, hoy en día ya no se usa el sistema clave WEP porque se ha demostrado que puede ser descifrada en pocos minutos mediante ataques estadísticos.

Fue ya en 2003 cuando el organismo encargado de certificar las redes WLAN, la Alianza Wi-Fi anunció oficialmente que el sistema WPA (Wifi Protected Access) sustituiría al sistema WEP.

El funcionamiento de WPA se basaba en que en, normalmente, un servidor RADIUS de autenticación, se distribuían distintas claves para cada usuario.

Existe la opción de cifrar de manera menos segura la red con WPA usando una clave precompartida entre el dispositivo inalámbrico y el punto de acceso al que desea conectarse, normalmente esto es de uso cotidiano en casas o pequeñas empresas. Este tipo de sistema recibe el nombre de WPA-PSK.

**Mejoras que introduce WPA:**

- > Se sigue usando el mismo algoritmo que en el sistema WEP, RC4, pero esta vez se añade una clave precompartida de hasta 63 caracteres ASCII.
- > Esta clave cambia de manera automática cada cierto tiempo gracias a la implementación del protocolo TKIP (Temporal Key Integrity Protocol).
- > Además, también se integra el código de integridad del mensaje MIC (Message Integrity Code), que es más seguro que el CRC.
- > Tiene un contador de tramas que nos ayuda a tener protección frente a ataques de repetición.
- > En 2004 el estándar se ratifica y sufre una evolución hasta el estándar WPA2.

Mejoras que introduce WPA2:

- > Se cambia el algoritmo de cifrado por AES (Advanced Encryption Standard), que estaba aprobado por el gobierno de Estados Unidos como un mecanismo dedicado al cifrado de información clasificada.
- > El código de integridad del mensaje MIC es mejorado.
- > Se descubrió en 2017 que había un exploit que se encargaba de reconocer las claves de encriptación para poder penetrar en la red, conocido como KRACK. Este se solucionó aplicando un parche de seguridad.
- > En enero de 2018 obtuvo una tercera evolución hacia el estándar WPA3.

Mejoras que introduce WPA3:

- > Su cifrado es de 192 bits.
- > La clave precompartida es sustituida por un sistema de autenticación simultánea entre iguales.
- > Es más sencilla su configuración para dispositivos sin pantalla.



2.7.

Espacios y recorridos para telecomunicaciones en edificios comerciales (ANSI/TIA/EIA 569-B)

2.7.1. Espacios de las redes locales

Podemos diferenciar los siguientes espacios importantes en una red según los siguientes elementos:

1. **Las salas donde se encuentran los ordenadores.** Todo el cableado que sea necesario para que se conecten los equipos que están en la misma red de la sala suele ser denominado cableado horizontal. Aquí hay que añadir las rosetas y los latiguillos que usamos para darle al equipo conexión.
2. **Los armarios** (en algunos casos dependiendo del tamaño de la organización pueden ser cuartillos) donde se almacenan los dispositivos de red como son switches o routers. El cableado presente en todos estos armarios o cuartillos es denominado cableado vertical o backbone.
3. **CPD o Centro Procesal de Datos** es una sala donde se almacenan los servidores y otros elementos de la red. Esta sala debe encontrarse con una temperatura baja debido al riesgo de incendio.
4. **El cuarto de entrada de servicios** es como su nombre indica, donde se da entrada a los servicios externos contratados de internet o electricidad. En el caso de grandes empresas se aconsejan que estos dos vayan por separado para evitar que problemas en la empresa nos dejen sin ambas conexiones.

Al conjunto de todos los cables, conectores, canalizaciones, etiquetas, dispositivos y espacios necesarios para montar la red se le denomina cableado estructurado.

Cuartos de comunicaciones

En algunas ocasiones un armario no es suficiente para albergar todos nuestros dispositivos de red y cuando esto sucede los albergamos en un cuarto específico llamado cuarto de comunicaciones. Los cuartos de comunicaciones pueden ser de diferentes tamaños dependiendo del tamaño de la red que tengamos, desde una pequeña habitación hasta un almacén entero solo dedicado a esto. Si un cuarto de comunicaciones es de un tamaño muy extenso, pasa a denominarse CPD o Centro de procesamiento de datos.

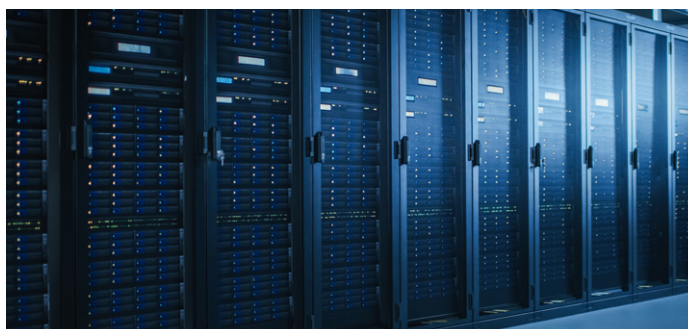


Imagen 7. CPD moderno



Debido a la importancia de los elementos que aloja un CPD, existen una serie de medidas de seguridad a la hora de elegir esta sala:

- > Se debe de controlar el acceso a dichas salas de comunicaciones de manera estricta, otorgando solo acceso al personal necesario como el administrador de la red o el encargado de su mantenimiento. Hoy en día se controla dicho acceso de muchas maneras, entre las que destaca el acceso biométrico.
- > La sala siempre debe de encontrarse en unas condiciones de temperatura mínimas y esta debe de ser controlada de manera constante. Un buen sistema de refrigeración es fundamental.
- > La humedad nunca debe de ser excesiva ya que podría favorecer al mal funcionamiento de la estructura.
- > Las puertas de esta sala siempre deben de abrirse hacia fuera y solo se debe de restringir su apertura desde fuera, nunca desde dentro.
- > Es aconsejable que la ubicación de esta sala no sea pública para poder evitar posibles ataques.
- > Los pasillos o caminos hasta este deben de ser anchos para que se pueda manejar fácilmente la maquinaria grande.
- > Todo el mobiliario y hasta la pintura de estas habitaciones debería ser ignífuga para que en caso de incendio se proteja.
- > Siempre debe de contar con un sistema antincendios provisto de extintores, detectores de humos y alarmas.
- > La sala no debe de encontrarse en sitios bajos como un sótano, las paredes deben de ser gruesas y tampoco debe de tener ventanas u otros elementos que den al exterior de manera abierta. Todo esto se realiza para evitar inundaciones o filtraciones de agua.
- > Cuanto más alejada esté de sitios con mucho ruido o interferencias, mejor.
- > La insonorización también es importante ya que este cuarto por lo general creará ruido en exceso debido a todas las máquinas que se encuentran en él.
- > **SIEMPRE** debe de contar con un **SAI** para que, en caso de fallo de la red eléctrica, todos los dispositivos sigan en funcionamiento.



Armarios de comunicaciones. Paneles de parcheo

Los armarios de comunicaciones suelen encontrarse dentro del CPD y albergan los elementos más específicos de una red (también suelen ser los más caros). Hay distintos tipos de tamaños para los armarios de comunicaciones, desde pequeños de 30 cm hasta algunos de 2 m.

La altura de los armarios suele medirse en U. Una U equivale a 1,75 pulgadas (4,445 cm). Dentro de estos armarios no solemos encontrar elementos superiores a 1 o 2 U. Hablamos de elementos como patch panels, servidores, SAI, etc.

Los armarios de comunicaciones también reciben la denominación de rack de comunicaciones.

Los paneles de parcheo (a.k.a patch panels) se componen de una estructura, generalmente metálica, que sirve de conexión entre los distintos cables. Estos nos hacen sencilla la manera de cambiar o alterar las conexiones entre distintos cables sin necesidad de mover todos los equipos. Existen paneles de parcheo para todo tipo de cables de red, desde UTP hasta fibra óptica. El número de puertos de estos paneles puede ser muy variado: 12, 24 64, pero siempre será una potencia de dos.

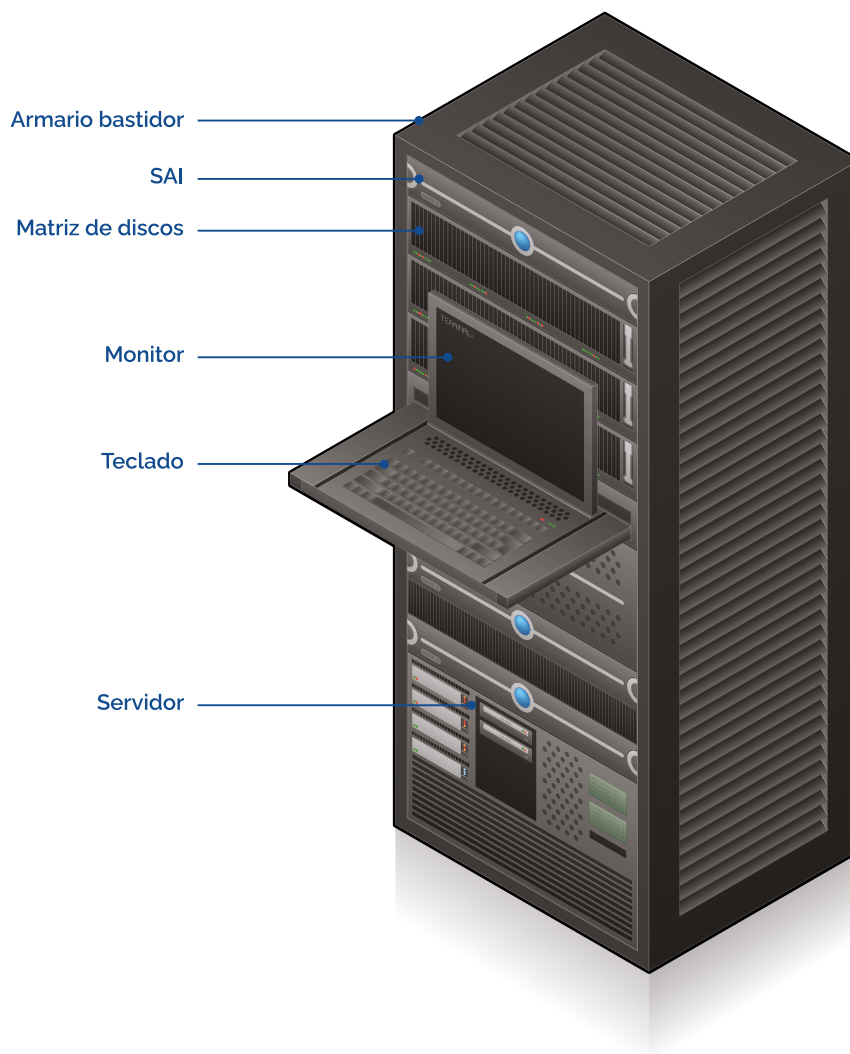


Imagen 8. Ejemplo de distribución de un armario de comunicaciones



2.7.2. Canalizaciones

Al hablar de canalizaciones, nos referimos al espacio por donde circulan los cables.

Los tipos más comunes de canaletas vienen explicados en el siguiente cuadro:

Tipos de canalizaciones

Las canalizaciones suelen clasificarse en tres tipos:

- > **Por pared.** Debido a la facilidad de su montaje y su precio reducido suelen ser las más utilizadas. Se trata de pequeñas canaletas o tuberías de plástico que se sujetan a la pared mediante tornillos. Debemos fijarnos en que los cables no queden por el suelo ya que podría ocasionar caídas, o el deterioro de los conectores, provocando así una posible pérdida del servicio de Internet. Será necesario disponer de materiales como taladros, tacos, herramientas de nivelación y bridas para realizar la instalación.
- > **Por techo.** Menos problemática que la anterior ya que es muy complicado que un usuario tenga contacto con ella. Se ponen por encima de un llamado falso techo, lo que las hace también muy estéticas.
- > **Por suelo.** El inverso al anterior, también necesita un falso suelo y es poco problemática. La gran diferencia con el falso techo es que aquí sí que necesitaremos unas canaletas de aluminio por el suelo, lo que hace de esta instalación menos estética y algo más propensa al deterioro, aunque es más barata.

En entornos domésticos es común que se usen canaletas de plástico y adhesivas a la pared o al suelo. Lógicamente son mucho más inseguras.

Hay varios materiales de canalización (al igual que en los cuadros eléctricos), el cual lo elegiremos en base al tipo de canalización que queramos realizar. Al igual que con el material, el tamaño también es diverso, desde 2 cm hasta más de 30cm. En cuanto al largo suelen estar estandarizadas en los 1.8 m de longitud.

Tipos de canaletas		
Tipo de canaleta	Imagen	Descripción
Escalera	 <p>Fuente: direct-industries</p>	Fáciles de instalar, se suelen usar en techo debido a su flexibilidad. El material más común es el acero galvanizado.
Cerrada	 <p>Fuente: perlex.com</p>	Con forma de U y sin necesidad de tener tapa. Suelen ser usadas en falso techo o en pared.
Especiales	 <p>Fuente: rarelabs.io</p>	Las más comunes para fijar a la pared. Cuentan con agujeros para fijar las rosetas.
Plásticas	 <p>Fuente: importadoraorbea.com</p>	Las más versátiles, con uso en cualquier sitio.
Salvacables	 <p>Fuente: feb.ee</p>	Las más decorativas y estéticas, se suelen usar en el suelo.



Instalación de canaletas

Independientemente del tipo de canalización elegido, es importante seguir una serie de recomendaciones:

- > Para evitar averías no deben estar cerca de otras canalizaciones (como las eléctricas o las de agua).
- > No deben estar cerca de aparatos eléctricos con el fin de minimizar el riesgo de interferencias.
- > Debemos evitar doblar en exceso los cables.
- > Las aristas de las propias canaletas no deben estar afiladas o con rebordes para no estropear los cables a la hora de pasarlos.
- > La canaleta no puede ir sobrecargada, se deberá poner una canaleta de la anchura necesaria para el cable que queramos instalar de manera que no estén amontonados ni a presión, deben estar holgados.

Los pasos para instalar una canaleta en la pared son los siguientes:

1. Debemos prestar atención a las medidas de seguridad en el entorno en el que vamos a trabajar, debemos usar guantes para evitar cortes u otro tipo de daños, y gafas protectoras para evitar que nos entre en los ojos cualquier elemento o partícula que se pueda desprender al taladrar la pared.
2. Mediremos la pared y la canaleta que vayamos a utilizar, y en caso de ser necesario, cortaremos la canaleta al tamaño adecuado para la pared.
3. Separar los dos componentes de la canaleta, deslizando uno sobre otro.
4. Marcar en la pared con un lápiz los agujeros para los tornillos que se harán en la canaleta. Utilizar nivel para que la canaleta quede recta.
5. Debemos tener en cuenta que no pase ninguna tubería por donde vamos a taladrar, por lo que es conveniente consultar los planos previos a la instalación. También existen herramientas que nos pueden indicar si hay alguna tubería de paso en el punto donde trabajaremos.
6. Ahora taladraremos en el lugar previamente marcado con una broca del tamaño preciso para que pasen los tornillos que usaremos.
7. Retiramos el polvo de los agujeros.
8. Se colocan los tacos en los agujeros ayudándonos de un martillo.
9. Situamos la canaleta e introducimos los tornillos por los agujeros para que se quede fija.
10. Pasamos el cable de datos por dentro de la canaleta.
11. Con mucho cuidado de no pinzar los cables (si hay varios podemos agruparlos con bridas), iremos poniendo la tapa de la canaleta hasta escuchar un clic, que significa que ha quedado fijada.
12. Tener en cuenta las esquinas y demás obstáculos usando elementos esquineros.
13. Si es necesario, al final de la canaleta pondremos una caja donde irán una o varias rosetas.
14. Recogemos el espacio de trabajo dejándolo limpio de restos y residuos para evitar cualquier riesgo laboral.



2.8.

Cableado de telecomunicaciones en edificios comerciales (ANSI/TIA/EIA 568-C)

2.8.1. Herramientas para trabajar con cableado y conectores

Como se ha visto en la unidad anterior, para conectar los conectores a los cables usamos los tres tipos de cables: de pares, coaxial y fibra óptica.

Cable de pares

Las principales herramientas para trabajar con el cable de par trenzado procederemos a estudiarlas a continuación.

Crimpadora

Con esta utilidad específica, lo que se persigue es que los hilos de cobre atravesados por los pines metálicos del conector RJ45 macho de modo que queden fijos. Para usarla hacemos lo siguiente: colocamos los hilos (en su orden, esto como veremos más adelante es fundamental) dentro del conector, introducimos el conector en la cavidad de la crimpadora y cerramos con una presión media.

Este procedimiento debe ser suficiente para que se queden fijados los pines a los hilos.



Imagen 1. Crimpadora RJ45

Ponchadora

Esta herramienta es la que nos ayuda a que introduzcamos los hilos de cobre del cable de pares en el conector RJ45 hembra (roseta).

Se usa de manera muy sencilla, colocamos los cables en el conector y vamos uno a uno empujando con cierta suavidad hasta que queden los hilos en su posición correcta.

La ponchadora, al mismo tiempo que inserta el hilo, corta el sobrante por el otro extremo, por eso es muy importante que no nos equivoquemos de lado, o cortaremos este hilo.



Imagen 2. Ponchadora RJ45.
Fuente: ferretronica.com



Pelacables

La única herramienta que es prescindible entre todas las nombradas porque este trabajo se puede hacer con un cúter, pero, además de ser más peligroso, el resultado no sería el mismo.

Esta herramienta lo que hace es ayudarnos a retirar la funda protectora del cable, siempre con cuidado de no cortar los hilos de cobre que se encuentran en su interior.



Imagen 3. Pelacables. Fuente: coupang.com

Tester

El tester es la herramienta que nos dirá si se ha realizado bien el cableado, es decir, comprueba la calidad de este. Lo que hace este tester es lo siguiente: el emisor manda una señal que recorrerá el latiguillo de red y se nos mostrará en la pantalla del tester si los pares están estructurados de manera correcta o no. De hecho, los tester modernos muestran los pares en los que nos hemos equivocado y por qué.



Imagen 4. Tester para RJ45 y RJ11



3.1.2. Cable coaxial

Crimpadora para cable coaxial

La crimpadora del cable coaxial se usa de manera similar a la del par trenzado salvo porque en este caso sujetaremos el conducto metálico al vivo. Es por esto por lo que se debe de llevar un cuidado minucioso con esta crimpadora, si se aprieta en exceso, podemos propiciar que el elemento metálico quede en la crimpadora y necesitaríamos un conector nuevo.



Imagen 5. Crimpadora de cable coaxial

Pelacables

En este tipo de cables sí que no se debe usar bajo ningún concepto otro método para pelar el cable, porque este pelacables corta de un solo movimiento todos los elementos en la medida deseada. Su uso consiste en colocar el pelacables en la medida exacta que queremos y hacer que, de una vuelta completa, con esto sería suficiente.



Imagen 6. Pelacables para cable coaxial o rotativo. Fuente: walmart.com



3.1.3. Fibra óptica

Estas herramientas se caracterizan porque son mucho más caras que las anteriores. Además, son necesarios muchos elementos para trabajar con cables de fibra óptica. Los más comunes son los siguientes:

- > **Pegamento o epoxy.** Es un pegamento que se crea a partir de dos líquidos distintos que se unen. Lo usaremos para que la fibra se pegue al conector.
- > **Jeringuillas.** Se usa para que podamos introducir el pegamento dentro del conector.
- > **Lijas.** A la hora de construir algunos conectores es necesario pulir algo la fibra con estas lijas.
- > **Alcohol isopropílico.** Se usa para limpiar la fibra.
- > **Toallitas.** En ellas depositaremos el alcohol con el que se limpia la fibra.
- > **Gautes.** La fibra es muy fina y cortante, con lo que sería fácil clavárnosla, además, sería imperceptible en muchos casos.
- > **Microscopio.** Este elemento es por si queremos ver el estado de la fibra.
- > **Emisor de luz.** Como este cable funciona por luz, podemos comprobar si la luz se transmite de un extremo a otro.
- > **Herramienta para pelar la fibra.** Con un aspecto similar al de la crimpadora, le quitamos a la fibra el revestimiento que tiene. Además, tiene la forma de manera que se hará progresivamente. También hay que llevar mucho cuidado en este paso para no cortar la fibra.
- > **Metro, regla, o escalímetro de precisión.** Esto es necesario para calcular en que punto hemos de cortar la fibra.
- > **Holders.** Se usan para sujetar el cable de fibra y que no se parta ni se vaya desde que se ha tratado hasta que procedemos a su función. Se cierran de manera magnética.
- > **Cortadora de precisión o de diamante.** Esta cortadora da un golpe seco con su cuchilla para cortar con total precisión en el punto que hayamos elegido la fibra.
- > **Fusionadora.** Se colocan ambos extremos de la fibra en esta y mediante la fusión, une dichos cables. Esta unión es muy débil, por lo que hay que llevar un cuidado extremo.
- > **Termoretráctiles.** Los macarrones termoretráctiles se colocan justo donde se ha realizado la fusión y se calientan en la misma fusionadora a una temperatura alta para que este se compacte y proteja la unión.
- > **Gafas.** Durante todo el proceso hemos de llevar gafas para que nos protejan en caso de que algún trozo de fibra salte disparado.

Como veremos más adelante, la fibra óptica es el cable más complicado de realizar porque es tremendamente delicado y con suma facilidad podemos romperlo o deteriorarlo, lo que nos hará tener que empezar desde el principio.



2.8.2. Fabricación de cables

Aunque en el mercado se pueden encontrar los cables ya hechos, puede que haya ocasiones en las que se necesite hacerlo de urgencia o que simplemente porque nos resulta más útil en alguna tarea específica.

Siempre debemos de usar el material adecuado que hemos visto antes, o si no, en gran probabilidad el cable no funcionará.

Cable de pares

Se deben de seguir los pasos descritos a continuación para este tipo de cables:

15. Lo primero que se debe de hacer es ver la longitud deseada del cable y cortar por ese extremo, siempre dejando algo de margen para errores.
16. En segunda instancia, cogeremos el pelacables y aproximadamente a unos 15 milímetros del extremo, retiraremos con cuidado la cobertura de plástico del cable.
17. Destrenzamos los pares de hilos y los intentamos colocar lo más rectos posible.
18. Ahora tenemos que poner los hilos por orden según normativa. Actualmente existen dos normativas. La T-568A o la T-568B. Dentro de esto, tenemos también dos tipos de cable que crear, y lo elegiremos ahora:
 - » **Directo o recto:** independientemente de que normativa se use, los dos extremos deben de seguir la misma normativa, que suele ser la T-568B.
 - » **Cruzado:** en este caso, cada extremo usará una normativa diferente.
19. Si ya tenemos los hilos ordenados como los queremos, los dejamos todos al ras con unas tijeras.
20. Se colocan los hilos en el conector con la pestaña de este siempre mirando hacia abajo.
21. Se coloca el conector con los hilos ya bien posicionados en la crimpadora y procedemos a ejercer una leve presión en ella para que se queden fijos.
22. Se repite el mismo proceso con el conector hembra, pero al introducir los hilos, esta vez los fijamos con el puncher en las rosetas.

Par 1	+ Azul-blanco - Azul	Par 3	+ Verde-blanco - Verde
Par 2	+ Naranja-blanco - Naranja	Par 4	+ Café-blanco - Café

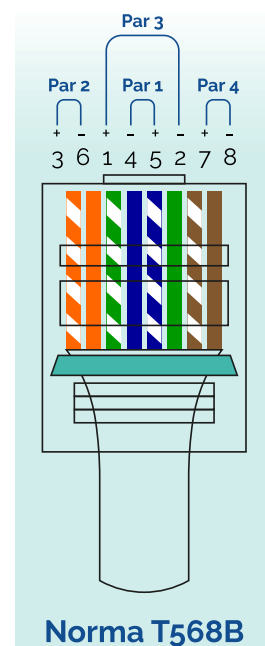
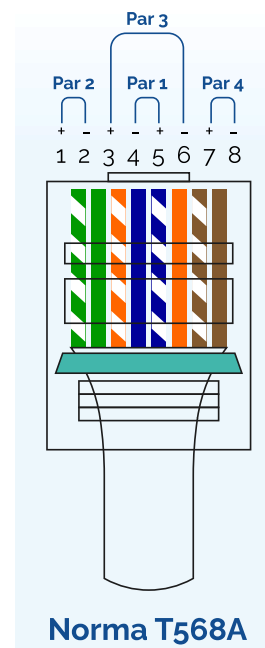


Imagen 7. Códigos de color en los cables de par trenzado



Cable coaxial

Para construir un cable coaxial, debemos de seguir los siguientes pasos:

1. Insertar la anilla.
2. Se retiran todos los elementos que recubren el conductor con el pelacables por la medida deseada.
3. Retiramos hacia atrás un poco la malla metálica.
4. Se introduce el conductor central en la cánula que tiene el conector.
5. Crimpamos de manera muy suave el conductor central.
6. Se colocan todos los elementos en su sitio de nuevo y una vez puesta la anilla, recortamos los hilos que sobre con respecto a la malla.
7. Se introduce el conector en la crimpadora intentando no mover nada de manera que el elemento anteriormente crimpado quede a la altura del borde externo del conector.
8. Crimpamos muy suavemente.
9. Sacamos el conector de la crimpadora con mucho cuidado también.

Fibra óptica

Cuando vayamos a hacer fibra óptica, siempre es recomendable comprar los cables ya hechos, puesto que es un proceso muy tedioso y complicado. Por si en alguna ocasión necesitamos realizarlo nosotros, los pasos son los siguientes:

1. Medimos las distancias por las que debemos de cortar la fibra.
2. Con la herramienta específica para esto, retiramos la funda que protege a la fibra con mucho cuidado de no partirla.
3. Se impregna una toallita en el alcohol isopropílico y con mucho cuidado limpiamos la fibra de posibles restos que hayan quedado. Se limpia la fibra hasta que escuchamos como chirría, lo que quiere decir que está limpia.
4. Se coloca la fibra justo por la distancia que deseamos en la cortadora de diamante y se acciona el mecanismo.
5. Se le introduce a cualquiera de los extremos de la fibra el macarrón termoretráctil.
6. Colocamos ambos lados de la fibra en los holders para sujetarla.
7. Se coloca la fibra en posición de fusión. En este punto es muy importante que las dos queden lo más pares posibles o si no, la fusión fallará.
8. Se acciona la fusión.
9. Una vez terminada, con extremo cuidado se coloca el termoretráctil justo en el punto de la fusión y se procede a calentarlo.
10. Cuando se haya calentado este, procedemos a introducir la fibra en el conector con el pegamento.
11. Pulimos la fibra.
12. Testeamos y revisamos la fibra en búsqueda de fallos.



2.8.3. Conexión de tomas y paneles de parcheo

La conexión de tomas trata de instalar los conectores hembra de los distintos tipos de cables usados para las redes LAN.

El conector RJ45 se explicó anteriormente en la unidad organizativa 2 a la hora de realizar el cableado de un habitáculo.

El conector RG58 hembra se instala de manera muy parecida a la que se realiza el macho, como hemos visto antes, la única diferencia es que no es necesario crimpar el conductor central.

Por último, en temas de fibra óptica, los paneles de parcheo se usan para que los cables estén organizados y conectados entre ellos como nosotros deseamos. Al introducir en los paneles de parcheo la fibra es muy importante que esta se enrolle en forma de bovina y no muestre giros bruscos o dejará de funcionar.

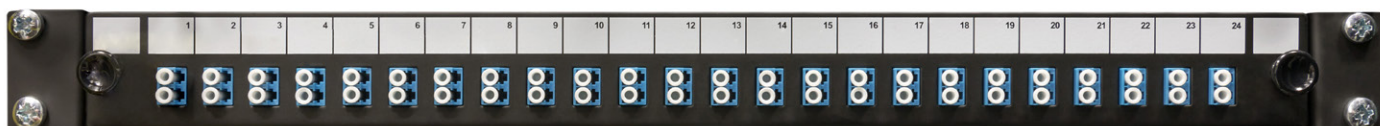


Imagen 7. Panel de parcheo para fibra óptica

2.8.4. Recomendaciones en la instalación del cableado

Siempre que vamos a proceder con la instalación completa de un cableado, debemos de tener en cuenta una serie de recomendaciones:

- > Lo primero es comprobar si podemos trazar una red cableada o si nos conviene más poner una red wifi inalámbrica. Por ejemplo, si es un castillo histórico pero muy turístico, normalmente habrá red, pero no agujeros y cables pasando.
- > Se dibuja en un plano el trazado que llevarán los cables.
- > Dependiendo de lo necesario, hay que decidir previamente el tipo de cable y dispositivos que se van a usar.
- > Se debe de medir todo de la manera más exacta posible para que no nos falte cable y que tampoco nos obre muchísimo, sino lo justo para errores.
- > En primera instancia se recomienda montar las rosetas, después los cables que van desde estas hasta los dispositivos y en última instancia los cables que salen de las rosetas y van directamente al equipo.
- > En el caso de la fibra óptica, siempre hay que seguir las recomendaciones específicas para esta ya que las curvaturas y demás degradaciones durante el recorrido puede que perturbe el funcionamiento de esta.
- > Se debe de ir comprobando que estén bien hechos y el funcionamiento de los cables conforme los vamos haciendo.
- > Los cables de deben de etiquetar para distinguir las conexiones.
- > Se debe etiquetar cada roseta con el punto exacto en el panel de parcheo o en dispositivo de red al que enlaza.
- > Siempre debemos de documentar toda esta estructura de red especificando todos los cables con sus extremos, todos los dispositivos y todos los paneles de parcheo que haya en nuestra red. Esto se suele hacer a modo de diagrama.
- > Debemos seguir las normas de seguridad estipuladas en todo momento para evitar accidentes.
- > Para que todo funcione correctamente, se han de seguir las normativas y estándares para cada cable o dispositivo.



 www.universae.com

