

UF1865: Operación y supervisión
de los equipos y servicios

Elaborado por: Francisco Castro Báez

Edición: 5.1

EDITORIAL ELEARNING

ISBN: 978-84-16492-39-8

No está permitida la reproducción total o parcial de esta obra bajo cualquiera de sus formas gráficas o audiovisuales sin la autorización previa y por escrito de los titulares del depósito legal.

Impreso en España - Printed in Spain

Presentación

Identificación de la Unidad Formativa

Bienvenidos a la Unidad Formativa **UF1865: Operación y supervisión de los equipos y servicios**. Esta unidad formativa pertenece al Módulo Formativo **MF0960_2: Implementación de equipos de acceso a redes de comunicaciones**, que forma parte del certificado de profesionalidad **IFCM0110: Operación en sistemas de comunicaciones de voz y datos**, de la familia profesional de **Informática y comunicaciones**.

Presentación de los contenidos

La finalidad de esta unidad formativa es enseñar al alumno a gestionar y atender las incidencias en el servicio de los dispositivos de acceso a redes externas a la organización, para corregirlas o informar de ellas según los protocolos establecidos y los procedimientos de actuación predefinidos.

Para ello, se analizarán las incidencias en dispositivo de acceso a redes públicas.

Objetivos del módulo o Unidad Formativa

Al finalizar este módulo formativo aprenderás a Resolver las incidencias detectadas en dispositivos de acceso a redes públicas de comunicaciones, siguiendo unas especificaciones dadas.

Área: informática y comunicaciones

Índice

UD1. Incidencias en dispositivo de acceso a redes públicas.....	7
1.1. Incidencias habituales	9
1.1.1. Incidencias internas.....	12
1.1.1.1. Fallos Hardware	17
1.1.1.2. Fallos Software	94
1.1.1.3. Fallos de configuración interna/interfaces de interconexión	113
1.1.2. Incidencias Externas (atribuibles al proveedor de servicios).....	161
1.1.2.1. Caídas de servicios por parte del proveedor de servicios	163
1.2. Gestión de incidencias en equipos de acceso a redes públicas	173
1.2.1. Sistemas de gestión/monitorización de equipos	175
1.2.1.1. Descripción general. Principios de funcio- namiento. Alarmas	179
1.2.1.2. Bloques funcionales. Procedimientos de análisis e identificación de fallos.....	202
1.2.1.3. Procedimientos de recuperación de fallos. Ejemplos y casos prácticos	209
1.2.1.4. Escalados. Eventuales planes de contingencia/ business continuity	219
1.2.2. Herramientas de gestión de incidencias	233
1.2.2.1. Descripción general. Funcionalidades	235
1.2.2.2. Procedimientos de gestión/documentación de incidencias	239

1.2.2.3. Notificaciones y escalados (internos y/o a proveedor de servicios)	243
1.2.2.4. Procedimiento de escalado (y seguimiento) de problemas no resueltos. Documentación y seguimiento	244
1.3. Herramientas de monitorización de equipos para la localización y notificación de incidencias	246
Glosario	259
Soluciones	263

UD1

Incidencias en
dispositivo de acceso
a redes públicas

- 1.1. Incidencias habituales
 - 1.1.1. Incidencias internas
 - 1.1.1.1. Fallos Hardware
 - 1.1.1.2. Fallos Software
 - 1.1.1.3. Fallos de configuración interna/interfaces de interconexión
 - 1.1.2. Incidencias Externas (atribuibles al proveedor de servicios).
 - 1.1.2.1. Caídas de servicios por parte del proveedor de servicios
- 1.2. Gestión de incidencias en equipos de acceso a redes públicas
 - 1.2.1. Sistemas de gestión/monitorización de equipos
 - 1.2.1.1. Descripción general. Principios de funcionamiento. Alarmas
 - 1.2.1.2. Bloques funcionales. Procedimientos de análisis e identificación de fallos
 - 1.2.1.3. Procedimientos de recuperación de fallos. Ejemplos y casos prácticos
 - 1.2.1.4. Escalados. Eventuales planes de contingencia/business continuity
 - 1.2.2. Herramientas de gestión de incidencias
 - 1.2.2.1. Descripción general. Funcionalidades
 - 1.2.2.2. Procedimientos de gestión/documentación de incidencias
 - 1.2.2.3. Notificaciones y escalados (internos y/o a proveedor de servicios)
 - 1.2.2.4. Procedimiento de escalado (y seguimiento) de problemas no resueltos. Documentación y seguimiento
- 1.3. Herramientas de monitorización de equipos para la localización y notificación de incidencias

1.1. Incidencias habituales

Los problemas de conectividad en redes pueden tener múltiples causas. La solución al problema una vez identificado el fallo, no debe de ser muy difícil.

A continuación se presentan algunos problemas más comunes:

- No se puede conectar con un servidor de acceso remoto.
- Al intentar conectar, aparece un mensaje que indica que el servidor de acceso remoto no responde.
- Se corta continuamente la sesión con el servidor
- Las conexiones se desconectan de forma anormal.
- Al intentar conectar, se recibe un mensaje de error del hardware.
- Al intentar conectar mediante una ISDN recibimos el mensaje «Sin respuesta».
- Las conexiones configuradas usando TCP/IP generan errores.
- Las conexiones establecidas mediante conexión compartida a Internet (ICS) generan errores.
- No hay respuesta en una conexión de red de área local.
- Los clientes de conexiones entrantes no pueden ver ningún recurso excepto el equipo de conexión entrante.
- La tarjeta inteligente no funciona.
- Al intentar establecer una conexión de acceso remoto mediante una tarjeta inteligente, recibe un mensaje de error.

- Hay conflictos de direcciones IP.
- Hay problemas en la conexión de fibra óptica.
- El proveedor de servicios de internet no funciona correctamente.
- Hay conflictos en los canales Wi-Fi.
- Los cables trenzados no están correctamente grimpados.
- Los servidores DNS no funcionan correctamente.
- Problemas de conectividad achacables a los proveedores de servicios de internet (ISP).
- Problemas de enrutamiento.
- Problemas con las subredes.
- Problemas de alimentación eléctrica.
- Sobrecalentamientos, etc.

Hay problemas con Internet ¿qué hago?

Si se pierde la conexión a Internet debemos comprobar si el Router está encendido y en funcionamiento. En caso afirmativo, puede que se haya perdido la conexión con el servidor. En este caso deberíamos reiniciar el Router. Debemos esperar dos o tres minutos a que se establezca correctamente la sincronización. Si sigue sin funcionar, el problema no está en el Router y debemos de buscar a buscar otras causas.

Para empezar, identificaremos si el problema se limita a un equipo, al navegador o recae en toda la conexión.

En primer lugar deberíamos comprobar si se produce la misma incidencia en más de un navegador, si es así lo mejor sería reiniciar el equipo. También el problema puede estar en el cortafuegos de nuestro software de seguridad.

También deberíamos de comprobar si la incidencia afecta más de un equipo de la red.

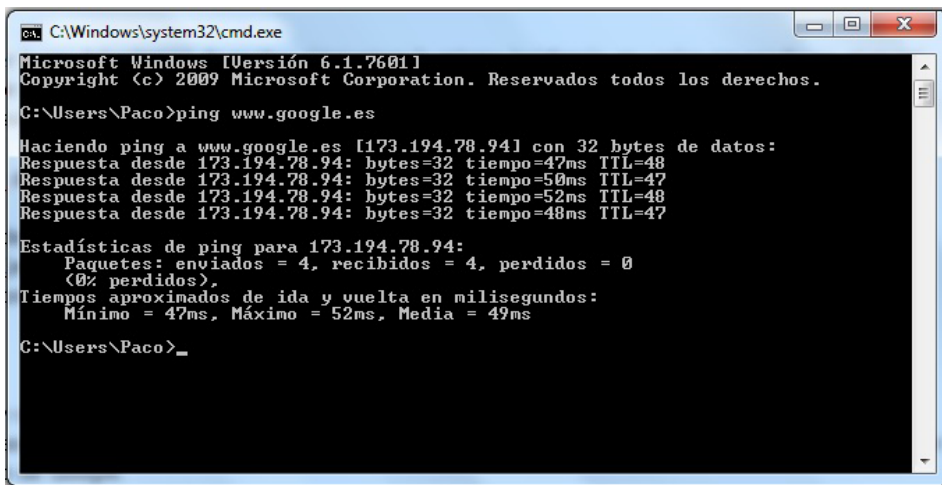
Si el problema persiste, podemos acceder al intérprete de comando del Windows pulsando la combinación de teclas de Windows más la tecla R.

Ahí escribiremos **cmd** y pincharemos en Aceptar.

Una vez en el intérprete de comandos, tecleamos el comando ping de la siguiente forma:

ping www.google.es

Si todo funciona correctamente se nos informará del tiempo en milisegundos que tardan en llegar los paquetes al servidor de la web, en este caso a Google:



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\Paco>ping www.google.es

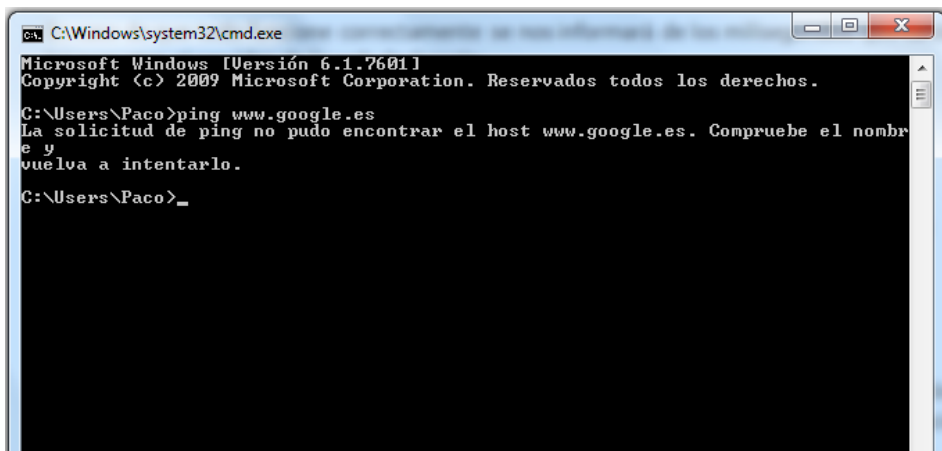
Haciendo ping a www.google.es [173.194.78.94] con 32 bytes de datos:
Respuesta desde 173.194.78.94: bytes=32 tiempo=47ms TTL=48
Respuesta desde 173.194.78.94: bytes=32 tiempo=50ms TTL=47
Respuesta desde 173.194.78.94: bytes=32 tiempo=52ms TTL=48
Respuesta desde 173.194.78.94: bytes=32 tiempo=48ms TTL=47

Estadísticas de ping para 173.194.78.94:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 47ms, Máximo = 52ms, Media = 49ms

C:\Users\Paco>_
```

Ping www.google.es con éxito

Si no hay conexión, se nos indicará que no se puede acceder al host de destino:



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

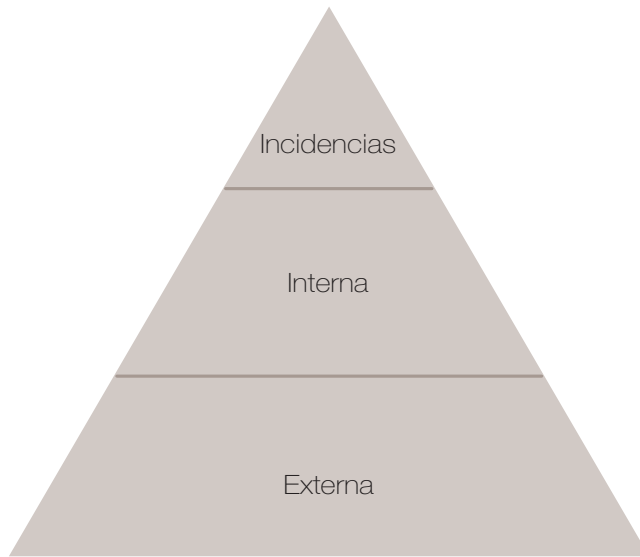
C:\Users\Paco>ping www.google.es
La solicitud de ping no pudo encontrar el host www.google.es. Compruebe el nombre y vuelva a intentarlo.

C:\Users\Paco>_
```

Ping www.google.es con fallo

Si no tenemos conexión, probablemente haya algún conflicto en la línea ADSL, algún problema con la conexión interna de la red hasta el Router, o incluso errores en las DNS o con la configuración del equipo, etc.

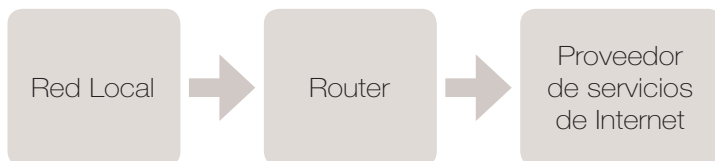
Las incidencias pueden ser muy variadas.



Tipos de Incidencias

1.1.1. Incidencias internas

Las incidencias internas, son aquellas que afectan desde el Router hacia dentro de la red.



Incidencias Internas

Problemas de ADSL y Router

Muchos de los errores de acceso Internet se deben al cable telefónico que trae la señal ADSL desde el servidor. También el propio Router suele generar muchos problemas.

Si el Router no puede sincronizar con la línea, la luz indicadora de ADSL parpadea lentamente o está apagada.

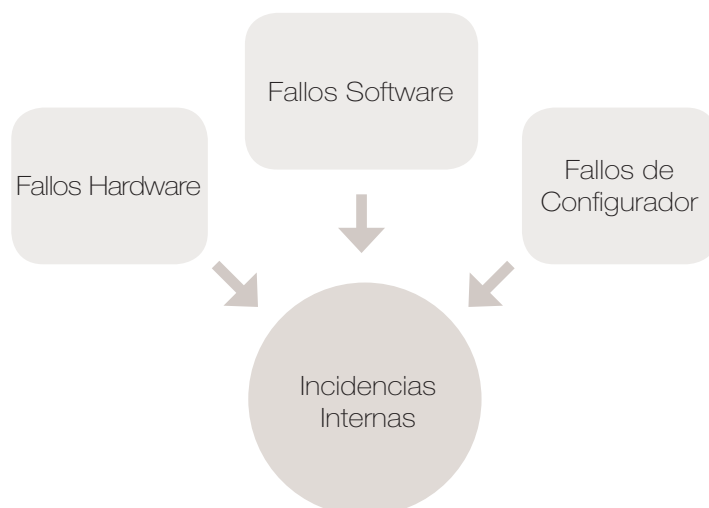
Si después de haber reiniciado el Router, no podemos sincronizar con el servidor, posiblemente el fallo esté en el cableado que trae la señal.

Si tenemos sincronización con el servidor, pero Internet no funciona, podemos restaurar la configuración completa del Router con los parámetros de originales de fábrica.

Si tras restaurar el Router a sus valores originales, las cosas siguen igual, podría ser debido a un problema de enrutado en la infraestructura del operador, algo sobre lo que no podemos actuar nosotros mismos.

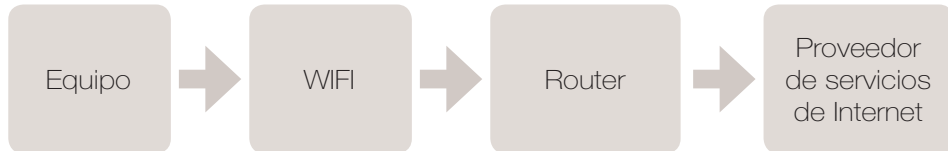
Las incidencias Internas podemos dividir las en tres categorías:

- Fallos HW.
- Fallos SW.
- Fallos de configuración interna o de los interfaces de interconexión.



Errores en la conexión Wi-Fi

Si el equipo ha dejado de conectarse a la red Wi-Fi y no hay forma de que recupere la conexión, puede haber diversas causas.



En primer lugar reiniciamos el equipo y el Router Wi-Fi. Esto suele resolver el problema en el 80% de los casos, ya que una vez hecho esto, se suele solucionar y todo vuelve a funcionar correctamente otra vez.

En caso de que siga habiendo problemas, deberíamos de asegurarnos de que esté activada la señal Wi-Fi en el Router (cada el fabricante es diferente pero lo normal es mediante un interruptor, una combinación de teclas o un software instalado en el equipo).

Después hemos de pinchar sobre el icono de la barra de tareas en forma de escala de señal, para ver la lista con las redes Wi-Fi detectadas.

Ahora debemos comprobar que nuestra red aparece en la lista de redes Wi-Fi disponibles. En caso de que aparezca, intentaremos conectarnos a ella. Si tampoco hay conexión, tendremos que asegurarnos de que la clave de seguridad que hemos introducido es correcta (muchos errores de conectividad se derivan de errores en las claves).

Si la red no aparece entre las redes disponibles o si aparece, no podemos conectar, habrá que revisar el punto de acceso.

También puede pasar que a pesar de tener conectado el equipo al Router Wi-Fi, no hay de tráfico entre el ordenador y la red. Esto se puede deber a muchas razones. Como hemos dicho con anterioridad, lo primero va a ser siempre reiniciar el equipo y el Router Wi-Fi.

Si tras haber reiniciado, seguimos con problemas, habrá que comprobar que el Router está asignando la dirección IP correctamente.

Para ello, seguimos los siguientes pasos:

- Inicio
- Panel de Control

- Redes e Internet
- Centro de redes y recursos compartidos
- Conexión de red inalámbrica, lo que nos mostrará los detalles del adaptador.
- Detalles podremos ver si se nos está asignando una IP automática por DHCP o es automática.
- En el caso de la IP automática, habrá que revisar el Router, pero también el portátil.

Buscaremos la última actualización disponible para el controlador de la tarjeta Wi-Fi.



Para poder ver los elementos hardware del equipo, incluido el adaptador Wi-Fi, hemos de acceder al administrador de dispositivos de Windows. Para ello, debemos pulsar la combinación de la Tecla de Windows y la Tecla Pausa. Ello nos dará acceso a la opción propiedades del sistema. Dentro de esta ventana, debemos pinchar sobre la opción Administrador de dispositivos.

Aquí aparecerán todos los elementos hardware del equipo. En la categoría adaptadores de Red, debe aparecer el adaptador Wi-Fi. Deber doble clic sobre él, se debe mostrar una ventana en la que aparecerán se mostrarán todos los detalles del dispositivo. Accedemos a la pestaña controlador y ahí podremos actualizar el controlador del dispositivo.

Si tenemos instalado algún software de seguridad instalado (antivirus, cortafuegos, etc.), sería bueno desactivarlo temporalmente para averiguar si causante del problema fuese puede ser este. Hay que tener en cuenta que la función principal del cortafuegos es bloquear accesos desde y hacia la red..

Router Wi-Fi

En lo referente a los Router Wi-Fi, hay muchos tipos de ellos atendiendo a factores como:

- **Estándares** Wi-Fi: 802.11b/g/a/n
- **Seguridad**: WEP, WPA o WPA2
- **Frecuencias de trabajo**: entre 2,4 y 5 GHz

A esto hay que añadir las propias tecnologías de algunos fabricantes que cada uno ha desarrollado con la idea de acelerar y mejorar la transmisión de datos.

Una de las primera cuestiones de debemos hacer si el Router Wi-Fi falla es actualizar su firmware a la última versión disponible en la web del fabricante.

Una vez hecho eso, lo más prudente sería, reiniciar el Router Wi-Fi y a continuación restablecer la configuración de fábrica del Router. Ahora podríamos ir modificando ciertos parámetros empezando por lo más sencillo y después configurando lo más complejo.

Podríamos desactivar la seguridad, ajustamos la banda en 2,4 GHz y seleccionamos el estándar más antiguo (802.11b u 802.11g). Esta sería la configuración mas básica, menos problemática, pero también la menos eficiente.

Si todo funciona, ahora podríamos empezar aumentando la seguridad a WEP y después a WPA, también iremos cambiando la cambiando la banda de emisión y después el estándar de transmisión.

Interferencias inalámbricas

Los problema también pueden deberse a interferencias que dificulten la comunicación inalámbrica entre el equipo y el Router. Hay teléfonos inalámbricos DECT que funcionan en la banda de 2,4 GHz, n el área de cobertura demasiadas redes Wi-Fi, que operen a en el mismo canal o incluso puede haber en zonas próximas a edificios sensibles inhibidores de señal.

Para solucionar esto, podemos cambiar el canal de emisión. También podemos cambiar el Router Wi-Fi e instalar otro que funcione a 5 GHz. Esta es una banda muy poco utilizada aún y seguro que apenas tendremos interferencias.

Los servidores DNS, muy importantes

Algunos problemas como la velocidad lenta, los derivados de la propia dificultad de acceder a Internet o el no poder acceder a determinadas direcciones, pueden estar causados por la configuración de los servidores DNS que tenemos en la configuración de red.

Los operadores de Internet cuentan con sus propios servidores DNS que, en muchos casos, pueden estar sobrecargados, caídos o no ser de mucha calidad. Esto provoca malos funcionamientos.

A veces es necesario cambiar la configuración de los servidores DNS que asigna por defecto el Router. Esto puede mejorar la conexión y sobre todo la velocidad a la hora de acceder a muchas páginas.

Más adelante trataremos el problema de los servidores DNS en profundidad. Decir ahora que servidores DNS como el de Google, OpenDNS o incluso los de Norton, además de gran disponibilidad, aportan seguridad a la conexión al bloquear el acceso a páginas malware o phishing.

1.1.1.1. Fallos Hardware

Los fallos hardware, los podemos clasificar conforme al siguiente esquema:

Fallos Hardware

- Organización
 - Rack
 - Paneles de distribución
- Medios de transmisión
 - Cableado estructurado
 - Medios inalámbrico
- Equipos eléctricos
 - Regletas
 - S.A.I.

- Equipos de conexión
 - Hub
 - Switch
 - Modem
 - Router

Los equipos de distribución



Los **equipos de distribución** se encargan de controlar y repartir el flujo de datos en la red local. Los más utilizados son los concentradores (Switch) y los encaminadores (Routers).

Para conectar los equipos de distribución y los equipos (ordenadores, portátiles, TPV, etc.) entre sí se utiliza lo que llamamos el cableado estructurado. Este se compone de elementos pasivos como rosetas, los conectores, el cable cables de par trenzado coaxial o de fibra optica, los armarios Rack, los paneles de parcheo, etc.

Electrónica de red

Para establecer la conexión entre los distintos equipos de la red es necesario instalar unos dispositivos electrónicos:

- Switch: Centralizan las comunicaciones y distribuyen la información.
- Router: proporcionan acceso a internet
- Router Wi-Fi: proporcionan acceso a internet para redes inalámbricas.

Rack



Un **armario rack** se utiliza para alojar en su interior todos los elementos de distribución de la electrónica de la red y centralizar en su interior todas conexiones de la red.

Dentro de un rack podemos incluir:

- Los Hub's.
- Los Switch.
- El Router.
- Los ordenadores que hacen las veces de servidores de red.
- Los sistemas físicos de copias de seguridad automáticas, etc.

La principal función del rack es la de la organización de los distintos elementos necesarios para la conexión de la red. Dentro de ellos se colocan los paneles (meros intermediarios entre los cables de par trenzado que vienen de los ordenadores y los latiguillos que llevarán la conexión hasta los puertos de los Hub's o Switch's). También, como dijimos antes se, colocan los elementos de la electrónica de la red (Switch, Hub y por supuesto el Router).

Hay armarios rack de tamaños diferentes. Hay algunos pequeños para alojar un solo panel y un solo Switch o Hub. En el otro extremo los hay de tamaño bastante grande que incluyen prestaciones adicionales como puede ser la climatización, fuente de alimentación, etc.

En el interior del rack se concentran las señales de voz y datos y desde ahí se reparten por toda la red de área local.

Los racks se componen de un armazón metálico con unas medidas normalizadas (el ancho suele ser de 19 pulgadas). La altura y el fondo varían según el fabricante y las necesidades que tengamos.

Tienen unos bastidores con unas guías horizontales. En estos bastidores se atornillan los elementos que se van a fijar en su interior. También tienen otras guías verticales para fijarlos en la pared.

Podemos clasificar los armarios rack de varias formas:

- **Accesibilidad:** Algunos modelos tienen en los paneles laterales algunas aberturas que facilitan las labores de mantenimiento y de conexión de nuevos elementos.
- **Tamaño.** Hay rack de tipo columna diseñados para grandes redes. Los hay pensados para redes más pequeñas, estos son de fijación mural. El ancho normalizado es de 19 pulgadas pero también los hay de 10 pulgadas.
- **Unidades de rack («U»).** Es una unidad de medida que define la capacidad de almacenamiento del rack. Un rack («U») equivale a 1,75 pulgadas (44,45 mm) de alto.

Paneles de distribución de cableado



Los **patch panel**, paneles de distribución de cableados, se utilizan para conectar los distintos cables de red. Las líneas de entrada y salida de los equipos se conectan a estos elementos. Forman parte de estas conexiones ordenadores, impresoras, servidores...

Los patch suelen estar colocados en el rack, armarios de distribución.
