

**TAREA ONLINE UNIDAD 1 .-  
CARACTERÍSTICAS GENERALES DE LAS  
REDES LOCALES**

IES CASTILLO DE LUNA, ROTA (CÁDIZ)  
GRADO MEDIO SEMIPRESENCIAL SISTEMA MICROINFORMÁTICOS Y REDES  
MODULO: REDES LOCALES  
CURSO ACADEMICO: 2021/2022  
ALUMNO: ANTONIO NAVAS BERNAL  
OCTUBRE 2021

## INDICE

	<b>PÁGINA</b>
<u>Tarea 1.1-Comunicación entre ordenadores</u>	<u>3</u>
<u>Tarea 1.2-CMD</u>	<u>9</u>
<u>Tarea 1.3-Tipos de redes</u>	<u>19</u>
<u>Tarea 1.4-Topologías</u>	<u>33</u>
<u>Tarea 1.5-Conexión entre dos empresas</u>	<u>44</u>
<u>Tarea 1.6-Modelo OSI/TCP-IP</u>	<u>55</u>
<u>Webgrafía.</u>	<u>61</u>

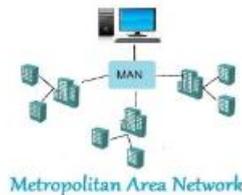
## Tarea 1.1-Comunicación entre ordenadores

Explica con tus palabras como se haría una comunicación entre dos ordenadores, es decir, cómo se hace la transferencia de datos entre dos ordenadores interconectados en dos partes del mundo distintas.

La comunicación entre ordenadores es la transmisión de datos e información a través de un canal de comunicaciones entre dos ordenadores, se logra mediante la utilización de la utilización de redes. La red más sencilla es una conexión directa entre dos ordenadores. Sin embargo, también pueden conectarse a través de grandes redes que permiten a los usuarios intercambiar datos, comunicarse mediante correo electrónico y compartir recursos, por ejemplo, impresoras.

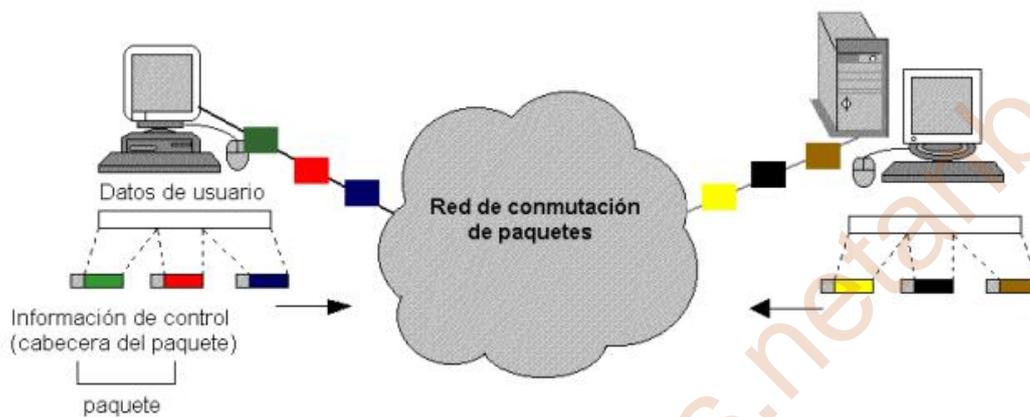
En función de ubicación de cada uno de estos dos ordenadores podemos clasificar las redes por el tipo de red por la distancia entre ellos, es decir, si necesitamos comunicarnos en otra parte del mundo, podemos partir de una red local (LAN), una red metropolitana (MAN) y por último una red de área extensa (WAN) y viceversa hasta llevar al usuario o destino final. La siguiente tabla se define cada uno de estos tipos de red y distancias:

Distancia hasta	Ejemplo	Tipo red
10 m	Bluetooth, USB, Ethernet corto alcance	PAN (Personal)
100 m	WiFi, Ethernet en cobre y fibra óptica	LAN (Edificio)
2 Km	Ethernet en fibra óptica	LAN (Campus)
80 Km	Redes CATV, ADSL, FTTH, WiMAX, servicios fibra oscura	MAN (Metropolitan)
20.000 Km	Enlaces telefónicos, fibra óptica, telefonía celular, satélite	WAN
> 20.000 Km	Transmisiones de datos con sondas espaciales	Internet interplanetaria



De la misma forma que dos personas que hablan idiomas distintos podrían comunicarse entre sí, si ambas aprendieran un tercer idioma común, dos ordenadores deberán utilizar el mismo protocolo al mismo tiempo para interconectarse. Para Internet este idioma es el modelo de referencia OSI (Interconexión de Sistemas abiertos) y a posteriori y más utilizado fue la arquitectura TCP/IP (Protocolo de Control de Transmisión/Protocolo de Internet). Este es el idioma que debe hablar cualquier ordenador que se desee comunicar a través de Internet.

## USO DE PAQUETES



OSI (Interconexión de Sistemas abiertos) o TCP/IP divide la información en forma de paquetes, cada uno de ellos contiene una parte del documento o la información junto con etiquetas identificadoras que indican las direcciones de las computadoras que reciben y envían esa información. Estos paquetes pueden llegar desordenados al destino pero no importa pues contienen toda la información necesaria para que sean agrupados correctamente, siendo todo este proceso transparente para el usuario. Al mismo se lo denomina sistema de conmutación por lotes.

El modelo de referencia OSI está definido como un modelo teórico que no se aplica realmente a la práctica, ya que ISO definió solamente la función general que debe realizar cada capa, pero no mencionó en absoluto los servicios y protocolos que se deben usar en cada una de ellas. Además cuando apareció OSI ya otros modelos se habían implantado de forma generalizada a causa de Internet, como es la pila de protocolos TCP/IP. No obstante, en el estudio y el diseño de las redes, el modelo de referencia OSI juega un papel importante para conocer y entender mejor su funcionamiento.

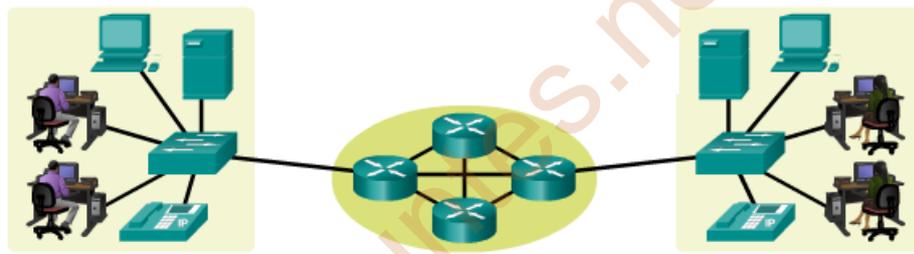
Es decir, una arquitectura de redes es formada por:

- Un modelo de capas, detallando las funciones que desempeña cada una.
- Un conjunto de protocolos propios de cada capa, denominadas familia, pila de protocolos o 'protocol stack'. Una capa puede tener varios protocolos.

Ejemplos de arquitecturas de redes: SNA (IBM), DNA(DEC), OSI, TCP/IP.

La comunicación entre dos capas adyacentes (en una misma entidad) se realiza a través de la interfaz. La interfaz es local a esa entidad y no forma parte de la arquitectura de redes, es decir, existen las interfaces que son las comunicaciones verticales entre capas y que son propios de cada entidad y no tienen que acordarlas con nadie, y existen los protocolos que son las comunicaciones horizontales y este si es fundamental que estén todos de acuerdo en utilizar los mismos.

Los modelos TCP/IP y OSI son los modelos principales que se utilizan al hablar de funcionalidad de red. Representan el tipo básico de modelos de red en capas:



	Modelo OSI	Conjunto del protocolo TCP/IP	Modelo TCP/IP
<b>Capa 7</b>	Aplicación	HTTP, DNS, DHCP, FTP	Aplicación
<b>Capa 6</b>	Presentación		
<b>Capa 5</b>	Sesión		
<b>Capa 4</b>	Transporte	TCP, UDP	Transporte
<b>Capa 3</b>	Red	IPv4, IPv6, ICMPv4, ICMPv6	Internet
<b>Capa 2</b>	Enlace de datos	PPP, retransmisión de tramas, Ethernet	Acceso a la red
<b>Capa 1</b>	Física		

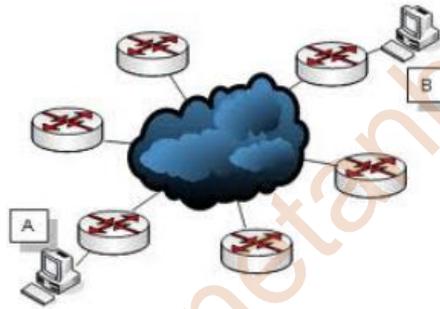
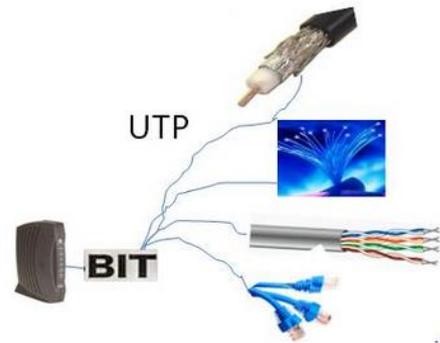
**Capa 1 Física:** Configura las características físicas necesarias para la transmisión y recepción de datos en forma de bits.

La capa física, en última instancia, será la encargada de pasar a señal eléctrica, luminica o de radio, los datos que reciba en forma digital a través de cable (coaxial, par trenzado, fibra óptica), el medio inalámbrico que utilizamos, voltaje para repesnar un 1 o un 0, microsegundos que dura cada digito, frecuencia de radio se va a transmitir, tipos de conectores.

**Capa 2 De enlace:** Se responsabiliza de la integridad de la transmisión de los datos entre dos nodos.

La capa de enlace de datos existe como una capa de conexión entre los procesos de software de las capas por encima de ella y la capa física debajo de ella. Como tal, prepara los paquetes de capa de red para la transmisión a través de alguna forma de medio, ya sea cobre, fibra o entornos /medios inalámbricos.

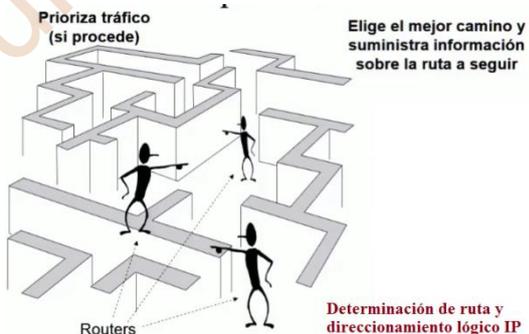
En muchos casos, la Capa de enlace de datos está incorporada en una entidad física como tarjeta de interfaz de red (NIC) de Ethernet, que se inserta dentro del bus del sistema de un ordenador, switch o router y hace la conexión entre los procesos de software que se ejecutan en los dispositivos finales y los medios físicos. Sin embargo, la NIC no es solamente una entidad física. El software asociado con la NIC permite que la NIC realice sus funciones de intermediara preparando los datos para la transmisión y codificando los datos como señales que deben enviarse sobre los medios asociados.



**Capa 3 De red:** Define la ruta entre las unidades de emisión y las de recepción de datos, haciendo las veces de conmutador.

Se ocupa de determinar cuál es el mejor camino para enviar información entre el origen y el destino, pudiendo pasar por tantas redes intermedias como sea necesario. Es en este nivel de red donde los datos se fragmentan en paquetes, enviándose cada uno de ellos de forma independiente.

Estos paquetes irán por el camino más adecuado de forma que lleguen en el menor tiempo posible (camino más corto, el más rápido, el que tenga menor tráfico, etc). Esta capa debe controlar también la congestión de la red, intentando repartir la carga lo más equilibrada posible entre las distintas rutas. La unidad mínima de información que se transfiere a este nivel se llama paquete o datagrama.



**Capa 4 De transporte:** Su función es verificar la validez de la integridad de la transmisión utilizando algoritmos de la corrección de errores.

Permite asegurar que los datos lleguen correctamente de un extremo a otro de la comunicación al nivel de sesión. Para ello establece mecanismos fiables para el intercambio de datos, realizando servicios de detección de errores. Además el nivel de transporte será el encargado de recomponer la información, eliminando las tramas repetidas y colocándolas en el orden correcto.

### Conexión de extremo a extremo y control de flujo de datos



Internet se representa como una nube. La capa de transporte envía los paquetes de datos desde la fuente transmisora hacia el destino receptor a través de la nube. La nube maneja los aspectos tales como la determinación de la mejor ruta.

**Capa 5 De sesión:** Se encarga de la coordinación de las comunicaciones en forma ordenada y del control de la sesión.

Esto incluye un control a nivel de la contabilidad y la conversación, es decir, determinar quién debe hablar y en qué momento y negociaciones relativas a los parámetros de sesión. Además se describe de qué manera la capa de sesión coordina las peticiones y las respuestas de servicio. Esto ocurre cuando las aplicaciones se comunican entre diferentes hosts.

Se incluye el control de diálogo y la separación de diálogo que permite a las aplicaciones comunicarse entre el origen y el destino.

La capa de sesión establece, administra y termina las sesiones entre las aplicaciones. Esto incluye el inicio, la terminación y la resincronización de dos ordenadores que están manteniendo una sesión; La capa de sesión coordina las aplicaciones mientras interactúan en dos hosts que se comunican entre sí.

Las comunicaciones de datos se transportan a través de redes conmutadas por paquetes, al contrario de lo que ocurre con las llamadas telefónicas que se transportan a través de redes conmutadas por circuitos.



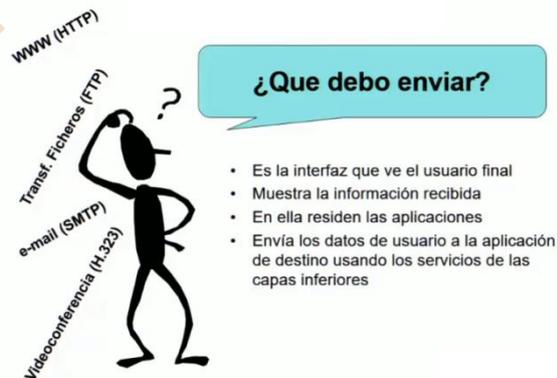
**Capa 6 De presentación:** Organiza la transferencia de datos entre los sistemas para representarlos y codificarlos de una manera uniforme.

Esta capa tiene la misión de coger los datos que han sido entregados por la capa de aplicación, y convertirlos en un formático estándar que otras capas puedan entender. En esta capa tenemos como ejemplo los formatos MP3, MPG, GIF, etc.



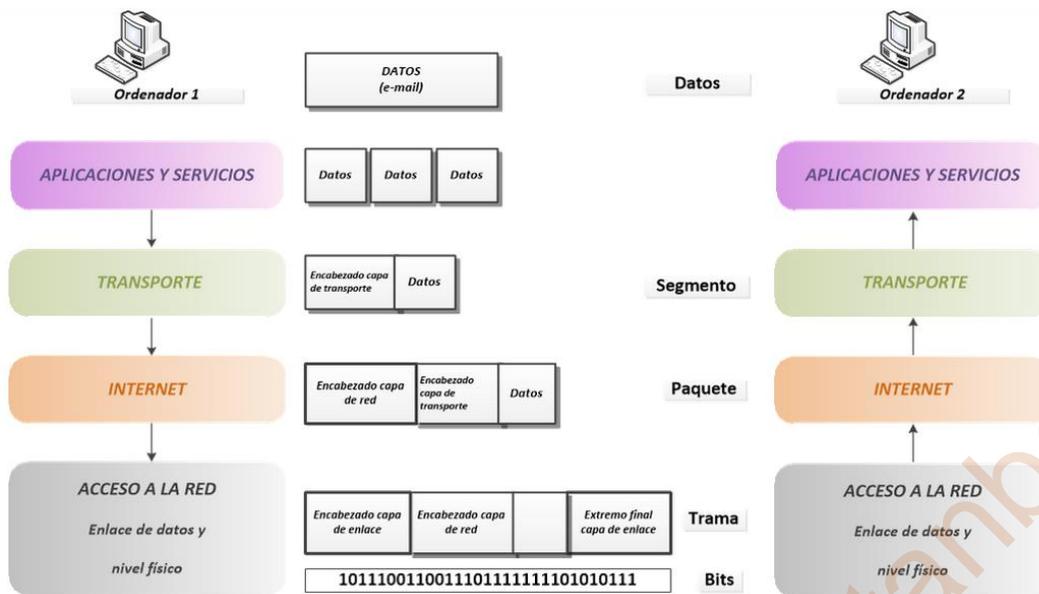
**Capa 7 De aplicación:** Define las reglas de comunicación o programas y la red (correo electrónico, transferencia de archivos, base de datos, etcétera.).

Esta es la capa que interactúa con el sistema operativo o aplicación cuando el usuario decide transferir archivos, leer mensajes, o realizar otras actividades de red. Por ello, en esta capa se incluyen tecnologías tales como http, DNS, SMTP, SSH, Telnet, etc.



**TCP/IP** se suele confundir muchas veces con un protocolo de comunicaciones concreto, cuando, en realidad, es una compleja arquitectura de red que incluye varios de ellos, apilados por capas. Es, sin lugar a dudas, *la más utilizada del mundo*, ya que es la base de comunicación de Internet y también se utiliza ampliamente en las distintas versiones de los sistemas operativos Unix y Linux y (aunque debido a su gran utilización ha sido también implantado en otros sistemas como Windows).

La arquitectura de TCP/IP se construyó diseñando inicialmente los protocolos para, posteriormente, integrarlos por capas en la arquitectura. Por esta razón, a TCP/IP muchas veces se la califica como pila de protocolos. Su modelo por niveles es algo diferente a OSI de ISO, como demuestra la tabla siguiente pasando a 4 capas:



Y por último la arquitectura de redes locales, la cual existen estándares y protocolos como Ethernet, WIFI, FDDI y las redes Token Ring, éstas dos últimas ya en desuso. La arquitectura de las redes locales sigue un esquema parecido que la arquitectura OSI de ISO, con pequeñas diferencias que afecta principalmente a la capa de enlace de datos.

En la siguiente imagen muestra las funciones de cada capa de cada una de las arquitecturas:



## Tarea 1.2-CMD

### Objetivo

- Determinar la dirección MAC de una computadora con Windows 10 conectada a una red Ethernet mediante el comando **ipconfig /all**.
- Acceder al comando **Ejecutar. / cmd**

### Información básica/Preparación

Cada computadora de una red local Ethernet tiene una dirección de control de acceso al medio (MAC, Media Access Control) grabada en la tarjeta de interfaz de red (NIC, Network Interface Card). Por lo general las direcciones MAC de las computadoras aparecen como seis conjuntos de dos números hexadecimales separados por guiones o por dos puntos, y a veces sin separador. (por ejemplo: 15-EF-A3-45-9B-57). El comando **ipconfig /all** muestra la dirección MAC de la computadora. Podrá trabajar de forma individual o en equipo.

### Se necesitan los siguientes recursos:

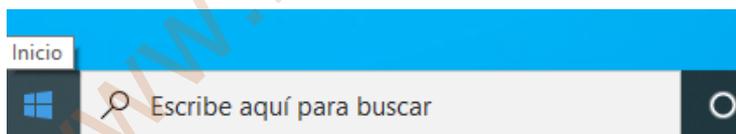
- Estación de trabajo con Windows 10, por lo menos, con una tarjeta de interfaz de red Ethernet (NIC).

### Se necesitan los siguientes recursos:

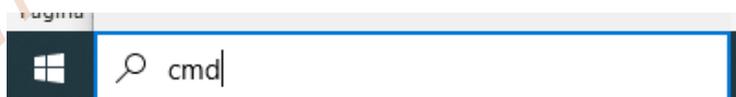
- Estación de trabajo con Windows 10, por lo menos, con una tarjeta de interfaz de red Ethernet (NIC).

### Paso 1: Abra una ventana de intérprete de comandos de Windows (A través del portátil HP compact)

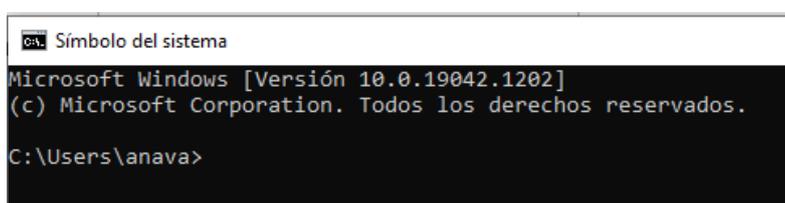
1. En el escritorio de Windows haga clic en **Inicio** y luego en



2. Escriba **cmd** en el cuadro de diálogo Ejecutar y luego haga clic en



3. Se abre una ventana de intérprete de comandos de Windows.



## Paso 2: Utilice el comando `ipconfig /all`

1. Escriba el comando `ipconfig /all` en la ventana de intérprete de comandos.

```
CA. Símbolo del sistema
Microsoft Windows [Versión 10.0.19042.1202]
(c) Microsoft Corporation. Todos los derechos reservados.
C:\Users\anava>ipconfig/all_
```

2. Presione

```
CA. Símbolo del sistema
Microsoft Windows [Versión 10.0.19042.1202]
(c) Microsoft Corporation. Todos los derechos reservados.
C:\Users\anava>ipconfig/all

Configuración IP de Windows

Nombre de host. . . . . : DESKTOP-FNP172T
Sufijo DNS principal . . . . . :
Tipo de nodo. . . . . : híbrido
Enrutamiento IP habilitado. . . : no
Proxy WINS habilitado . . . . . : no

Adaptador de Ethernet Ethernet:

Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : Realtek RTL8139/810x Family Fast Ethernet NIC
Dirección física. . . . . : 00-1E-EC-27-6C-40
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::65fd:e8ef:da8e:2d0%15(Preferido)
Dirección IPv4. . . . . : 192.168.0.42(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : viernes, 1 de octubre de 2021 19:09:43
La concesión expira . . . . . : sábado, 2 de octubre de 2021 19:25:42
Puerta de enlace predeterminada . . . . . : 192.168.0.1
Servidor DHCP . . . . . : 192.168.0.1
IAID DHCPv6 . . . . . : 201334508
DUID de cliente DHCPv6. . . . . : 00-01-00-01-27-C5-A7-99-00-1E-EC-27-6C-40
Servidores DNS. . . . . : 212.166.211.23
                          212.166.132.104
NetBIOS sobre TCP/IP. . . . . : habilitado

Adaptador de LAN inalámbrica Conexión de área local* 10:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : Microsoft Hosted Network Virtual Adapter
Dirección física. . . . . : 22-1F-3A-B4-FC-05
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí

Adaptador de LAN inalámbrica Wi-Fi:

Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : Qualcomm Atheros AR5007 802.11b|g WiFi Adapter
Dirección física. . . . . : 00-1F-3A-B4-FC-05
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::3d60:db9:dc4:5763%9(Preferido)
Dirección IPv4. . . . . : 192.168.0.35(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : viernes, 1 de octubre de 2021 19:21:01
La concesión expira . . . . . : sábado, 2 de octubre de 2021 19:37:08
Puerta de enlace predeterminada . . . . . : 192.168.0.1
Servidor DHCP . . . . . : 192.168.0.1
IAID DHCPv6 . . . . . : 151002938
DUID de cliente DHCPv6. . . . . : 00-01-00-01-27-C5-A7-99-00-1E-EC-27-6C-40
Servidores DNS. . . . . : 212.166.211.23
                          212.166.132.104
NetBIOS sobre TCP/IP. . . . . : habilitado

C:\Users\anava>
```

**Paso 3: Ubique una dirección MAC (física) en el resultado obtenido mediante el comando `ipconfig /all`**

3.1 Utilice la siguiente tabla para completar la descripción del **adaptador Ethernet** y la dirección física (MAC):

```
Adaptador de Ethernet Ethernet:

  Sufijo DNS específico para la conexión. . . :
  Descripción . . . . . : Realtek RTL8139/810x Family Fast Ethernet NIC
  Dirección física. . . . . : 00-1E-EC-27-6C-40
  DHCP habilitado . . . . . : sí
  Configuración automática habilitada . . . : sí
```

3.2 **Descripción:** Realt RTL8139/810x Family Fast Ethernet NIC

3.3 **Dirección física:** 00 – 1E – EC – 27 – 6C -40

3.4 **¿Cuál es la dirección física del adaptador inalámbrico?**

```
Adaptador de LAN inalámbrica Wi-Fi:

  Sufijo DNS específico para la conexión. . . :
  Descripción . . . . . : Qualcomm Atheros AR5007 802.11b|g WiFi Adapter
  Dirección física. . . . . : 00-1F-3A-B4-FC-05
  DHCP habilitado . . . . . : sí
  Configuración automática habilitada . . . : sí
  Vínculo: dirección IPv6 local. . . : fe80::3d60:db9:dc4:5763%9(Preferido)
  Dirección IPv4. . . . . : 192.168.0.35(Preferido)
  Máscara de subred . . . . . : 255.255.255.0
  Concesión obtenida. . . . . : viernes, 1 de octubre de 2021 19:21:01
  La concesión expira . . . . . : sábado, 2 de octubre de 2021 19:37:08
  Puerta de enlace predeterminada . . . . . : 192.168.0.1
  Servidor DHCP . . . . . : 192.168.0.1
  IAID DHCPv6 . . . . . : 151002938
  DUID de cliente DHCPv6. . . . . : 00-01-00-01-27-C5-A7-99-00-1E-EC-27-6C-40
  Servidores DNS. . . . . : 212.166.211.23
  . . . . . : 212.166.132.104
  NetBIOS sobre TCP/IP. . . . . : habilitado
```

**Descripción:** Qualcomm Atheros AR5007 802.11b|g Wifi adapter

**Dirección física:** 00 - 1F - 3A – B4 – FC - 05

## Paso 4: Reflexión

### 4.1 ¿Por qué una computadora puede tener más de una dirección MAC?

Porque cada ordenador puede tener más de una tarjeta de red y cada tarjeta de red tendría su propia dirección física o MAC.

### 4.2 El ejemplo que se muestra a continuación sobre el resultado del comando **ipconfig /all** tenemos una dirección MAC.

```
C:\>ipconfig /all

Configuración IP de Windows

Nombre del host . . . . . : CBROWN
Sufijo DNS principal . . . . . :
Tipo de nodo . . . . . : híbrido
Enrutamiento IP habilitado. . . . . : Sí
Proxy WINS habilitado. . . . . : No
Lista de búsqueda de sufijo DNS: netdev.sourcehill.net

Adaptador Ethernet Conexión de área local :

Sufijo de conexión específica DNS : sourcehill.net
Descripción. . . . . : Adaptador Fast Ethernet D-Link DFE-5
30TX PCI (rev. A)
Dirección física. . . . . : 00-05-5D-03-49-48
DHCP habilitado. . . . . : No
Autoconfiguración habilitada. . . . . : Sí
Dirección IP. . . . . : 192.168.1.30
Máscara de subred . . . . . : 255.255.255.0
Puerta de enlace predeterminada : 192.168.1.2
Servidor DHCP . . . . . : 192.168.1.2
Servidores DNS . . . . . : 192.168.1.2
Servidor WINS principal . . . . . : 172.16.8.25
172.16.9.25
Concesión obtenida . . . . . : viernes, 23 de noviembre de 2007 12:
51:16
Concesión expira . . . . . : sábado, 01 de diciembre de 2007 12:5
1:16
```

La dirección física o MAC es el 00 - 05 - 5D - 03 - 49 - 48

### 4.3 Supón que el resultado es el de una computadora que también tiene capacidad de conexión inalámbrica Ethernet. ¿En qué cambiaría el resultado?

Que se contempla también la activación de la tarjeta inalámbrica con una dirección física MAC, que en mi ordenador es la siguiente dirección física 00 - 1F - 3A - B4 - FC - 05

```
Adaptador de LAN inalámbrica Wi-Fi:

Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : Qualcomm Atheros AR5007 802.11b|g WiFi Adapter
Dirección física. . . . . : 00-1F-3A-B4-FC-05
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . : fe80::3d60:db9:dc4:5763%9(Preferido)
Dirección IPv4. . . . . : 192.168.0.35(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : viernes, 1 de octubre de 2021 19:21:01
La concesión expira . . . . . : sábado, 2 de octubre de 2021 19:37:08
Puerta de enlace predeterminada . . . . . : 192.168.0.1
Servidor DHCP . . . . . : 192.168.0.1
IAID DHCPv6 . . . . . : 151002938
DUID de cliente DHCPv6. . . . . : 00-01-00-01-27-C5-A7-99-00-1E-EC-27-6C-40
Servidores DNS. . . . . : 212.166.211.23
212.166.132.104
NetBIOS sobre TCP/IP. . . . . : habilitado
```

4.4 Desactiva el adaptador de tu red wifi y vuelve a utilizar el comando **ipconfig /all**. ¿Qué cambios puede ver? ¿Sigue apareciendo la dirección MAC? ¿Cambiará la dirección MAC?

```

Adaptador de LAN inalámbrica Wi-Fi:

Estado de los medios. . . . . : medios desconectados
Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : Qualcomm Atheros AR5007 802.11b|g WiFi Adapter
Dirección física. . . . . : 00-1F-3A-B4-FC-05
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí

C:\Users\anava>_
  
```

Que el adaptador de LAN inalámbrico Wi-Fi en estado de los medios esta desconectado.

Si sigue viéndose la dirección MAC y no cambiará nunca la dirección MAC al permanecer inamovible dicha dirección física a dicha tarjeta Wifi.

4.5 ¿Cuántos dígitos tiene la dirección MAC?¿Cuántos bits?¿Investiga y explica la diferencia entre el número de bits y número de dígitos?

La dirección física tiene 12 dígitos y 48 bits.

Por ejemplo, la dirección física de mi adaptador inalámbrico o MAC es el 00 – 05 – 5D – 03 – 49 – 48. Esta expresado en Hexadecimal porque esta expresado en números y letras desde la A a la F, que son los dígitos que se representa en ese sistema de numeración.

Entiendo que se representa de esta forma para evitar disponer de 48 bits siendo más fácil su expresión en hexadecimal con 12 dígitos en vez de 48, independiente del sistema de bus que disponga la tarjeta de red para la transferencia de los datos o conversión del sistema de una numeración a otra, y con esta dirección MAC posibilita tener 229.044.593.815.315 de combinaciones más que suficientes de los 7.896.915.473 personas de la población mundial actual en el año 2021.

En el caso de mi adaptador inalámbrico o MAC es el 00 – 05 – 5D – 03 – 49 – 48 al pasar esas parejas de dígitos hexadecimal a binarios tenemos:

Hexadec.	00	05	5D	03	49	48
Binario	00000000	00000101	01011101	00000011	01001001	01001000

4.6 ¿Con qué otro nombre se conoce la dirección MAC?

Se conoce también como dirección física.

4.7 ¿Qué identifican los seis primeros dígitos de la dirección MAC?

Los seis primeros dígitos hexadecimales de la dirección MAC es el identificador Único Organizacional (OUI) que se utiliza para identificar a los fabricantes en los dispositivos que hacen como Ethernet, Bluetooth o dispositivos Wifi de comunicación.

#### 4.8 ¿Puede haber dos direcciones MAC iguales en el mundo?

No puede haber dos direcciones MAC iguales en el mundo. La **dirección MAC** es un identificador único que los fabricantes asignan a una tarjeta o dispositivo de red. También es conocida como **dirección física** y está formada por 48 bits, representados por dígitos hexadecimales. Cada **dirección MAC** es única a nivel mundial y, en teoría, son fijas para cada dispositivo.

#### 4.9 Investiga como podrías asegurar la red en tu casa o cualquier red que se conecten a ella solo los ordenadores/dispositivos de tus familiares.

El método más sencillo de expulsar intrusos del WiFi doméstico es descargándonos e instalando un programa totalmente gratuito para nuestro ordenador que se llama Avances IP Scanner, con el que podremos conocer diferentes datos de los dispositivos que están conectados a nuestra conexión WiFi.

Una vez accedemos al programa, debemos pulsar en el **botón Explorador**, lo que comenzará a trabajar y a generar una **lista de dispositivos conectados** a nuestra red WiFi. Para hacerla más sencilla y práctica, el propio programa es capaz de identificar la marca de los dispositivos, sobre todo los smartphones, gadgets y productos de domótica.

Estado	Nombre	IP	Fabricante	Dirección MAC	Comentarios
▶	TC7230.O	192.168.0.1	Technicolor CH USA Inc.	10:62:D0:8D:77:9D	<b>PUERTA DE ENLACE</b>
▶	Equipo-PC	192.168.0.10	GIGA-BYTE TECHNOLOGY CO.,LTD.	FC:AA:14:28:22:77	<b>ORDENADOR SOBREMESA</b>
	192.168.0.12	192.168.0.12	Sony Interactive Entertainment Inc.	BC:60:A7:A6:8C:49	<b>CONSOLA PS4</b>
	192.168.0.13	192.168.0.13	Samsung Electronics Co.,Ltd	C4:57:6E:AE:1A:40	<b>TV SAMSUNG SALON</b>
	192.168.0.25	192.168.0.25	Xiaomi Communications Co Ltd	D8:CE:3A:90:01:4D	<b>MOVIL</b>
	192.168.0.26	192.168.0.26		F0:67:28:5D:47:23	<b>MOVIL OPPO-A91</b>
	192.168.0.27	192.168.0.27			
	192.168.0.30	192.168.0.30			
	192.168.0.42	192.168.0.42	COMPAL INFORMATION (KUNSHAN) CO., LTD.	00:1E:EC:27:6C:40	<b>ORD. PORTATIL</b>
▶	192.168.0.254	192.168.0.254	Technicolor CH USA Inc.	10:62:D0:8D:77:9F	<b>ROUTER</b>
▶	Equipo-PC	192.168.56.1		0A:00:27:00:00:12	

Estado	Nombre	IP	Fabricante	Dirección MAC	Comentarios
▶	TC7230.O	192.168.0.1	Technicolor CH USA Inc.	10:62:D0:8D:77:9D	<b>ROUTER. PUERTA ENLACE</b>
▶	Equipo-PC	192.168.0.10	GIGA-BYTE TECHNOLOGY CO.,LTD.	FC:AA:14:28:22:77	<b>ORDENADOR SOBREMESA</b>
	192.168.0.12	192.168.0.12	Sony Interactive Entertainment Inc.	BC:60:A7:A6:8C:49	<b>CONSOLA PS4</b>
	192.168.0.26	192.168.0.26		F0:67:28:5D:47:23	<b>MOVIL OPPO-A91</b>
	192.168.0.30	192.168.0.30	SAMSUNG ELECTRO-MECHANICS(THAILAND)	08:C5:E1:A2:9C:E5	<b>MOVIL SAMSUNG S8</b>
	192.168.0.42	192.168.0.42	COMPAL INFORMATION (KUNSHAN) CO., LTD.	00:1E:EC:27:6C:40	<b>PORTATIL</b>
▶	Equipo-PC	192.168.56.1		0A:00:27:00:00:12	

Ahora que ya conocemos los diferentes productos que están conectados a nuestra red WiFi, podemos dar el siguiente paso, identificar qué dispositivo queremos dejar sin acceso a nuestra conexión WiFi. Esta misión se basa en el descarte, si nosotros solo tenemos un dispositivo Xiaomi, y si disponemos por ejemplo de otro dispositivo Xiaomi que no es de la familia es que se trata de otra persona que no debería tener acceso. Para asegurarnos de cuál de ellos es nuestro dispositivo, tenemos que coger nuestro

smartphone Xiaomi y dirigirnos a los ajustes, en el buscador podemos introducir la palabra MAC y desde ahí podremos conocer cuál es la nuestra, para pasar al siguiente paso.

Una vez conocemos el dispositivo que queremos eliminar, debemos **copiar la dirección MAC**, para pasar al siguiente paso, donde le impediremos el acceso a nuestra conexión. Para esto debemos escribir en el navegador la siguiente dirección: **192.168.0.1** de acuerdo a la puerta de enlace al entrar en comando de órdenes y ejecutar **ipconfig**.

```
Microsoft Windows [Versión 10.0.19042.1202]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\anava>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . . . : fe80::65fd:e8ef:da8e:2d0%15
    Dirección IPv4. . . . . : 192.168.0.42
    Máscara de subred. . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.0.1

Adaptador de LAN inalámbrica Wi-Fi:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . :

Adaptador de LAN inalámbrica Conexión de área local* 10:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . :

C:\Users\anava>
```

En el navegador accedemos con el siguiente enlace <http://192.168.0.1/> al menú de bienvenido del Router Vodafone introduciendo el nombre de usuario y contraseña que se encuentra en la etiqueta del router:

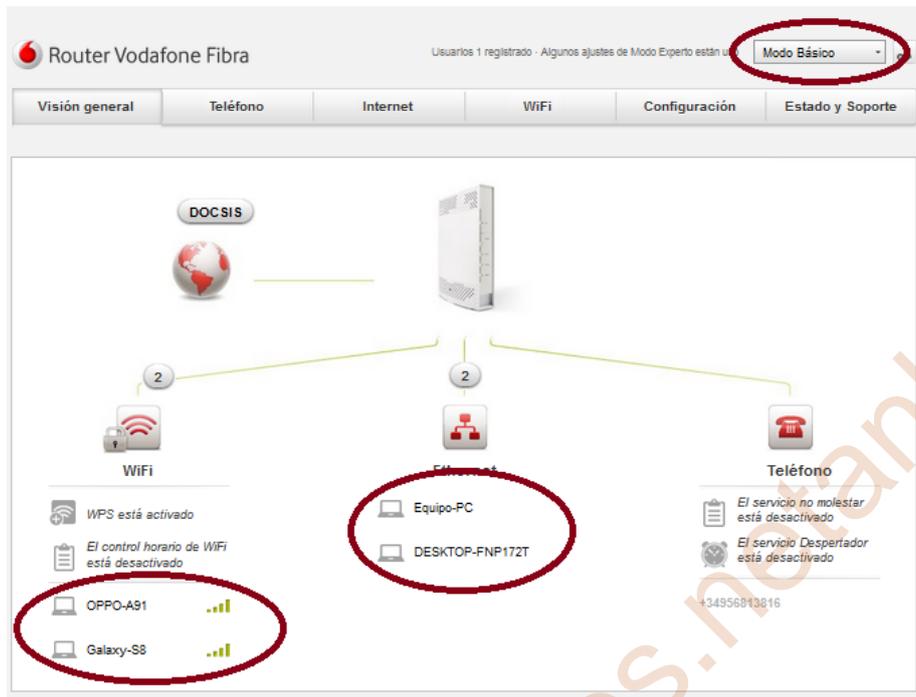
## Bienvenido al Router Vodafone Fibra



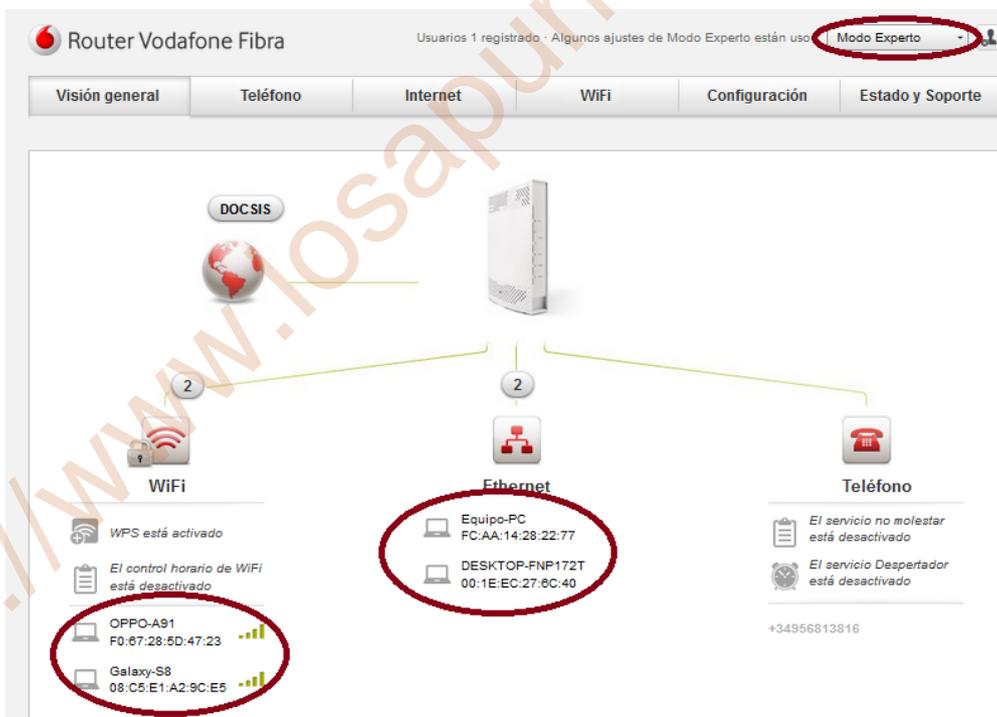
Introduzca la contraseña para acceder a las opciones de configuración.

Iniciar la sesión

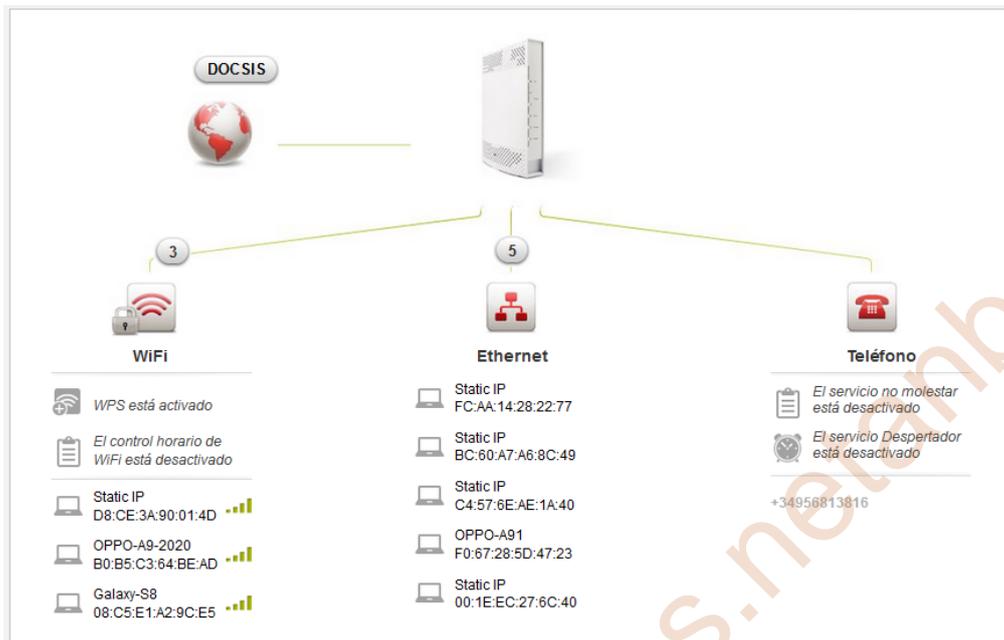
En el modo básico tenemos la siguiente información de equipos conectado tanto al internet como a la red wifi:



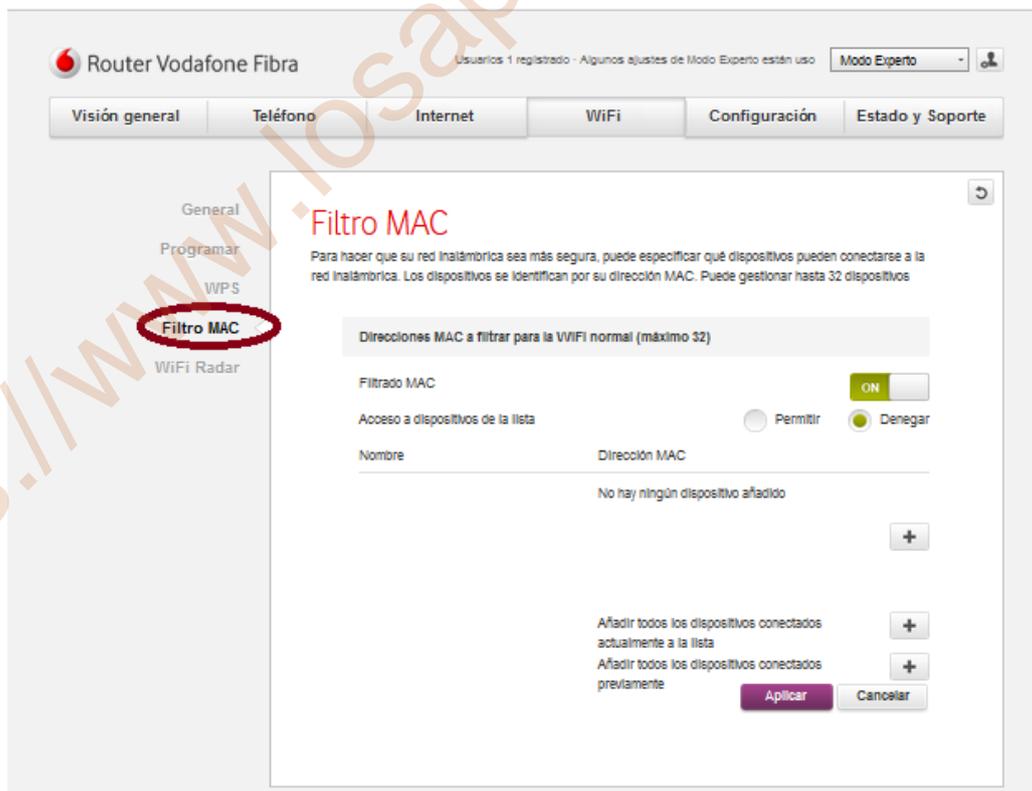
Pasamos del modo básico al modo experto para una configuración del sistema más completa:



En el modo experto conecto más dispositivos a mi red doméstica, tales como ordenador de sobremesa, portátil, móviles, consola, etc. y en este modo experto se muestra la dirección MAC de cada dispositivo:



Clic en el icono de WIFI podemos seleccionar mediante Filtro MAC aquellos dispositivos que le permitiríamos el acceso a nuestra red WIFI mediante la dirección MAC de cada dispositivo, no dejando acceso a nuestra red aquellos dispositivos que no estén identificados en nuestra router;



Otros datos a tener en cuenta para proteger nuestra red WIFI es la siguiente:

- 1) Cambiar la contraseña predefinido del router y pasar protección wifi en WPA + WPA2 que es de mayor protección. (Imagen marcado con el color rojo y azul).
- 2) Cambiar el nombre de usuario de la red wifi (SSID) con otro que sea más persuasivo como virus alerta, no pasar por aquí o soy abogado. (Imagen marcado con el color verde).
- 3) Ocultar el nombre de la red – Hide Access Point. Dado que no está visible se tiene que conocer el nombre del usuario exacto con mayúsculas y minúsculas de la red wifi (SSID) para poder acceder a él y la contraseña (Imagen marcado con el color amarillo).

## General

2.4 GHz

Su router soporta los estándares WLAN con velocidades de transmisión de hasta 300 Mbit / s (802.11b/g/n), que facilita la conexión inalámbrica de los dispositivos.

Red WiFi  ON

Canal 6

Velocidad Máxima 300 Mbit/s

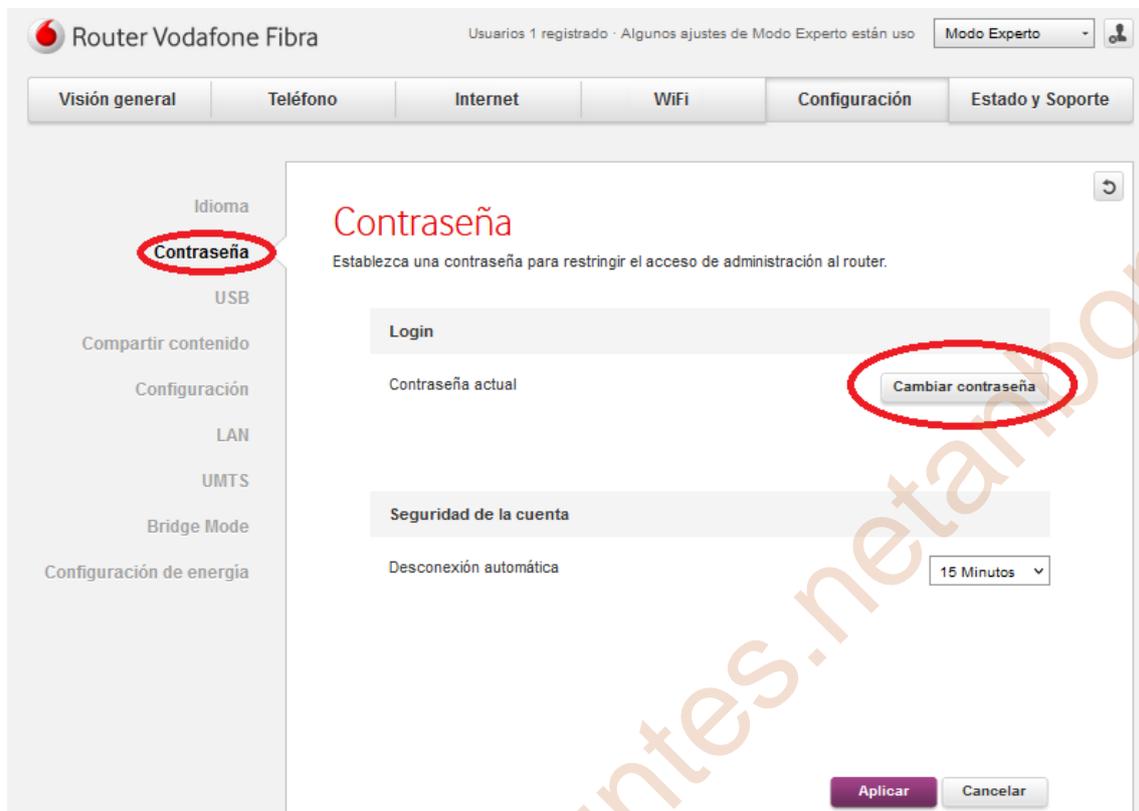
### Configuración

#### WiFi

Red WiFi (SSID)	vodafone7799
Bandwidth	20 Mhz
Canal	Auto
Emitir SSID	<input checked="" type="checkbox"/> ON
Frecuencia	2.4 GHz
Protección WiFi	WPA + WPA2
Clave de red	.....

Mostrar los caracteres

- 4) Cambiar el nombre de usuario y contraseña del router para que nadie puede vulnerar nuestro dispositivo y pueda acceder al router.



- 5) Apagar el dispositivo router cuando no lo estemos utilizando.

# Tarea 1.3- Tipos de redes

## Tipos de Redes

1) Busca en Internet periféricos de red, periféricos IP y otros dispositivos susceptibles de compartir en red. En un procesador de texto haz una tabla que contenga su foto y las funciones básicas que realizan.

### Periféricos de red

Los periféricos de red son los dispositivos que permiten la comunicación entre ordenadores. Para establecer esta comunicación podremos usar:

<p><b>Adaptador de red o Tarjetas de red (NIC).</b> Es el dispositivo que actúa de interface entre otros dispositivos. En este periférico encontramos la dirección MAC, único para cada adaptador y muy importante en el proceso de comunicación. Podemos encontrar adaptadores de red por cable y inalámbrico.</p>	
<p><b>Módem.</b> El módem recibe en tu casa la información proveniente del ISP a través de la línea de teléfono, fibra óptica o un cable coaxial (dependiendo del ISP) y a continuación la convierte de una señal eléctrica de tipo sinusoidal a una señal digital tipo cuadrada y viceversa.</p>	
<p><b>Router ó encaminador.</b> Va dirigiendo los paquetes de datos a distintas redes hasta alcanzar su destino. El trabajo del router es el de canalizar esta señal a los dispositivos conectados, ya sea por cables Ethernet o por Wi-Fi, para que todos sus dispositivos puedan tener acceso a internet. El router y el ISP no se pueden comunicar directamente porque emplean lenguajes distintos, o mejor dicho, transmiten distintos tipos de señales. De ahí que el papel del módem como intérprete sea tan relevante.</p>	
<p><b>Hub ó concentrador.</b> Su misión es la de concentrar muchas entradas en una única salida ó una única entrada, además regenera la señal. La señal recogida es repartida por todos los puertos que tiene el hub. El <b>HUB Ethernet trabaja en la capa física</b> de este modelo, o en la <b>capa de acceso al medio</b> si hablamos del <b>modelo TCP/IP</b>. Es decir, un Concentrador se encarga de recibir una señal de datos y repetirla para enviarla por sus diferentes puertos. Entonces, básicamente estamos hablando de un repetidor.</p>	
<p><b>Switch ó conmutador.</b> Su misión es la de ser selectivo a diferencia del hub. Concentra y regenera la señal también, pero además la señal recogida solamente será mandada al equipo al que va dirigida. Los Switch operan en la <b>capa de enlace o capa 2 del modelo OSI</b> (Open System Interconnection), un modelo de referencia utilizado para los protocolos de red y su definición. Esta se ocupa del <b>direccionamiento físico</b> de los paquetes que viajan por la red de acuerdo con la dirección MAC asociada a cada dispositivo en él conectado.</p>	

## Periféricos IP

La **dirección IP** es un conjunto de números que identifica, de manera lógica y jerárquica, a una interfaz en la red (elemento de comunicación/conexión) de un dispositivo (computadora, laptop, teléfono inteligente) que utilice el protocolo (*Internet Protocol*) o que corresponde al nivel de red del modelo TCP/IP.<sup>1</sup> La dirección IP no debe confundirse con la dirección MAC, que es un identificador de 48 bits expresado en código hexadecimal, para identificar de forma única la tarjeta de red y no depende del protocolo de conexión utilizado en la red.

**Teclado IP** para VideoXpert, Endura y Digital Sentry, con Joystick, teclas numéricas y Jog-Shuttle



EZVIZ **Cámara** de Vigilancia Visión Nocturna Colorida, **Wi-Fi IP** Cámara de Seguridad 1080p



El GXP1610/GXP1615 es un **teléfono IP** simple de usar para pequeñas y medianas empresas (PyMEs) y oficinas en casa. Puertos dobles conmutados de 10/100 Mbps, soporte multilinguaje, llamada en espera y conferencia de 3 vías



## Otros dispositivos

**Impresoras:** Prácticamente cualquier **impresora** que podamos comprar, salvo los modelos más básicos, permite conectarla a nuestro router por cable o por Wi-Fi de manera que cualquier usuario conectado al router dentro de la misma red pueda utilizarla para imprimir documentos. Esto es muy práctico y nos evita tener que obligar a los usuarios a llevar sus documentos en un pendrive a otros ordenadores para poder imprimirlos, aunque también complica bastante la configuración de la impresora, impresora que se tiene que configurar individualmente en cada ordenador y que en más de una ocasión se complica sobre todo por la dificultad para obtener la IP de la misma.



**Escáner:** Se trata de dispositivos que **permiten el rastreo de imágenes o documentos impresos**, los cuales se procesan con un programa de reconocimiento óptico de caracteres (OCR) y se genera el texto original en formato de los editores de texto más habituales.



2) Busca en Internet las fotografías de los terminales que pueden conectarse a Internet (PC, portátil, PDA, móvil, consolas, frigoríficos, ascensores, etc.).



**Ordenador** de sobremesa conectado a red con cable RJ45



**Portátil** conectado a red con cable RJ45



Conexión **PDA** a internet mediante tarjeta SIM



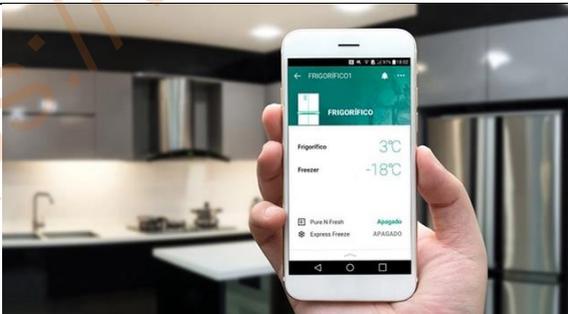
**Móvil** conexión internet mediante la operadora con la tarjeta SIM o mediante Wifi.



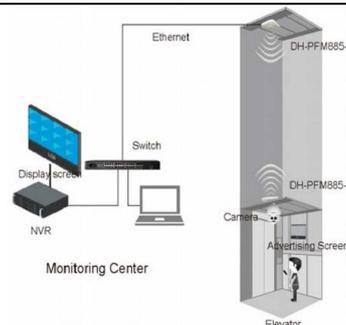
**Consola PS4** conectado a internet con el cable RJ45.



**Tablet:** Compartir internet WIFI desde móvil a otros dispositivos.



Los **frigoríficos** conectados disponen de una **conexión wifi** que, a través del router de la casa, les permite acceder a internet.



Tecnología IP/WIFI para facilitar la instalación de cámaras de seguridad en el interior de las cabinas de **ascensores**.

### 3. Clasifica las siguientes redes PAN, LAN, CAN, MAN, WAN:

- Conexión a Internet con un Módem-Splitter-Router ADSL. → **Redes LAN si está dentro de la red privada antes del módem y red pública MAN acceso a internet con ADSL.**
- CaTV (Internet, telefonía y televisión por cable). → **Redes MAN**
- Compartir dos impresoras, un escáner y un plotter. → **Redes LAN**
- Un teclado inalámbrico. → **Redes PAN**
- Una red en un campus universitario, que conecta el CPD con un cuartel militar cercano. → **Redes CAN**

#### Clasificación de las redes atendiendo al tamaño:

- **Red de área personal o Personal Área Network (PAN):** Incluye el entorno de usuario (PC, PDA, Pocket PC, Móvil, Ipod, portátiles, Tablets, Palms, etc). Normalmente son redes inalámbricas que utilizan tecnologías bluetooth o infrarojos...
- **Redes LAN (*Local Area Network*).** Su nombre consiste las siglas en inglés de Red de Área Local, y son aquellas que limitan su alcance a un área bien definida y de pequeñas envergaduras, como puede ser un departamento, una oficina, un avión, incluso un mismo edificio. Desprovistas de medios de interconexión públicos, se manejan como una sola red de localización, a pesar de que pueden servir a numerosos usuarios a la vez.
- **Red CAN de Campus:** Se extiende entre varios edificios dentro de un mismo polígono industrial que se conectan generalmente a un tendido de cable principal. Normalmente, la empresa es propietaria del terreno por el que se extiende el cable y tiene libertad para poner cuantos cables sean necesarios sin tener que solicitar permisos especiales.
- **Redes MAN (*Metropolitan Area Network*).** Su nombre consiste en las siglas en inglés de Red de Área Metropolitana, ya que se trata de una red de alta velocidad que brinda cobertura a un área geográfica más extensa que una LAN (de hecho contiene varias de ellas), pero aun así concreta y definida, como una porción de una ciudad.
- **Redes WAN (*Wide Area Network*).** Su nombre consiste en las siglas en inglés de Red de Área Amplia, y en esta ocasión se trata de redes de amplio alcance y alta velocidad, que echan mano a satélites, cableados, microondas y nuevas tecnologías para cubrir una extensa porción geográfica. Internet, sin duda alguna, es una WAN de proporciones globales.

### ¿Qué es un splitter en ADSL?

Un filtro **ADSL**, también llamado filtro separador o **splitter**, es un dispositivo que actúa como un filtro de frecuencias, ya que separa la señal de datos y voz en conexiones **ADSL**, de tal modo que permite hablar por teléfono y navegar por Internet simultáneamente con una sola línea.



#### 4. Busca en Internet programas que funcionen como servidor y otros como cliente.

### COMO SERVIDOR

Un «**Servidor Web**» puede ser tanto un **Ordenador (hardware)** que presta funcionalidades de alojamiento y funcionamiento a **páginas o servicios de Internet**, como un **Programa o Conjunto de programas (Software)** que hacen posible que dichas páginas o servicios de Internet existan y funcionen.

A nivel de Software, para lograr la implementación de un «**Servidor Web**», hoy en día, existen muchas **soluciones exitosas de software libre y código abierto** disponibles, como **alternativas a las soluciones comerciales, privativas y cerradas** de las grandes empresas de categoría mundial.

En lo individual, un programa de «**Servidor Web**» gestiona el «**Protocolo de Transferencia de Hipertextos (Hypertext Transfer Protocol o HTTP)**», para hacer posible que los archivos que forman una página web esté disponible (en línea) para los usuarios, mediante un **navegador web**.

En lo grupal, un «**Servidor Web**» también puede verse o definirse como un conjunto de programas relacionados con conexiones a **internet o una intranet**, abarcando para ello desde la gestión de los correos electrónicos, la descarga de archivos, la navegación de sitios web, y/o las simples o complejas consulta de informaciones alojadas en bases de datos (BD) dentro de sí mismas o conectadas a él.

Un Servidor Web básico suele estar integrado por 3 tipos fundamentales de programas que son:

- **Servidor Web**
- **Base de Datos**
- **Lenguaje de Programación, Scripting y Marcado**

**Servidores Web. Principales libres, abiertos y gratuitos:**

- Apache
- NGINX

## Bases de Datos. Principales libres, abiertos y gratuitos:

- Postgresql
- Mysql (Community)
- MariaDB

## Lenguajes de Programación, Scripting y Marcado. Principales libres, abiertos y gratuitos:

- PHP
- PERL
- Python

## COMO CLIENTE

Un cliente es todo proceso que reclama servicios de otro. Una definición un poco más elaborada podría ser la siguiente: cliente es el proceso que permite al usuario formular los requerimientos y pasarlos al servidor. Se lo conoce con el término front-end.

Las funciones que lleva a cabo el proceso cliente se resumen en los siguientes puntos:

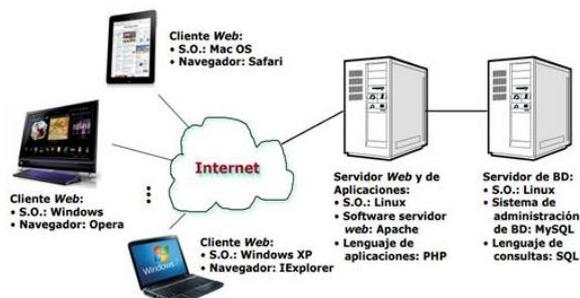
- Administrar la interfaz de usuario.
- Interactuar con el usuario.
- Procesar la lógica de la aplicación y hacer validaciones locales.
- Generar requerimientos de bases de datos.
- Recibir resultados del servidor.
- Formatear resultados.

De este modo el cliente se puede clasificar en:

- **Cliente basado en aplicación de usuario.** Si los datos son de baja interacción y están fuertemente relacionados con la actividad de los usuarios de esos clientes.
- **Cliente basado en lógica de negocio.** Toma datos suministrados por el usuario y/o la base de datos y efectúa los cálculos necesarios según los requerimientos del usuario.

Los programas que funcionan como clientes son los navegadores Safari, Opera, Internet Explorer, Mozilla Firefox, Chrome....

### Ejemplo de arquitectura Cliente/Servidor:



## 5. Busca sistemas operativos específicos para servidores.

### Microsoft Windows Server

Para trabajo en grupo (Windows for Workgroups) fue el primer sistema operativo de servidores de Microsoft. En esa versión, ciertos ordenadores podían configurarse para compartir recursos y responder a las solicitudes de los clientes, lo que los convertía en servidores, por definición. El primer sistema operativo de servidores de verdad de Microsoft fue Windows NT. Sus versiones 3.5 y 3.51 podían encontrarse en muchas redes comerciales hasta que Microsoft lanzó su línea Windows Server, que continúa existiendo a día de hoy. La versión más actual es Windows Server 2016, que admite numerosas aplicaciones y bases de datos, así como un hipervisor que permite servidores virtuales.

### Servidores Linux/Unix

El otro actor principal de los sistemas operativos de servidores es Linux/Unix. Podemos encontrarlo en múltiples versiones y de todos los colores, como Red Hat Enterprise Linux, Debian y CentOS como algunos de los más famosos. Al ser un sistema operativo de código abierto, Linux es muy popular como servidor web, generalmente con una instalación del servidor web Apache.

## 6. Busca equipos hardware que sirvan especialmente de servidores.

Las características de un servidor web a nivel de hardware son:

**Rack:** La palabra «rack» viene del inglés y se refiere al lugar donde se alojan los servidores físicamente. Es una jaula metálica o armario donde se colocan muchos servidores junto con otros dispositivos de red como routers, switch, etc.

**Gabinete:** El gabinete, también conocido como «torre», es el armazón que sostiene los componentes de hardware de una computadora. Existen diferentes tipos de gabinetes o armazones para equipos informáticos, cuanto más chicos sean los componentes también lo será el gabinete.

**CPU:** Es el centro de procesamiento de datos del servidor, la unidad central de procesamiento (CPU en inglés) desde donde se realizan todos los cálculos lógicos y matemáticos para que el usuario pueda manipular y acceder a los datos como necesita.

Los procesadores / CPU utilizados hoy en día en servidores son sobre todo AMD e Intel. Estos últimos en particular son los que usamos en Infranetworking y permiten lograr un rendimiento excelente en cualquier ámbito de servidores web como lo son:

- Servidores de Hosting Compartido
- Servidores dedicados
- Sitios de alto tráfico
- Análisis de Datos
- BigData

**Memoria RAM:** La RAM es otro de los componentes y características de un servidor web más esenciales. Se utiliza para almacenar información y datos de forma temporal dependiendo de la demanda del usuario a través del sistema operativo.

Es un tipo de memoria rápida. Cuando la memoria RAM se termina o usa por completo, el servidor intentará utilizar la memoria SWAP, que es una memoria basada en disco y suele ser más lenta.

**Placa madre:** La placa madre, también conocida como motherboard es una tarjeta o placa base de circuitos integrados que se utilizan para conectar los dispositivos y partes internas de la computadora. Poseen diversos puertos, ranuras y conectores para poder comunicarse con otros componentes de hardware como disco duro SSD, SATA o bien tarjetas de video, entre otras.

**Unidades de disco óptico:** Los servidores enterprise generalmente no utilizan este tipo de unidades de CD o DVD, sino que instalan los sistemas operativos por red en forma de imágenes ISO.

En otras épocas era muy común que los data centers guardaran la información en medios como cintas de almacenamiento.

**Unidades de almacenamiento:** El almacenamiento de servidores web se hace en discos duros, los cuales permiten almacenar la información del sistema operativo, los servicios de sistema, y en última instancia los datos cargados por el usuario.

Los que fueron durante muchas décadas un estándar fueron: IDE, SCSI y SATA.

También con la aparición de los discos SSD incorporaron tecnología digital que les permite leer y escribir más rápido que los tradicionales SATA.

Esto los ha hecho ubicarse como las unidades de almacenamiento más características de los servidores web ya que aseguran una excelente performance en lo que respecta a lectura y escritura, ideal para aplicaciones demandantes hechas en PHP-MYSQL por ejemplo.

**Puerto de red:** El puerto de red, también conocido como uplink, es en simples palabras el ancho de banda del que dispone tu servidor.

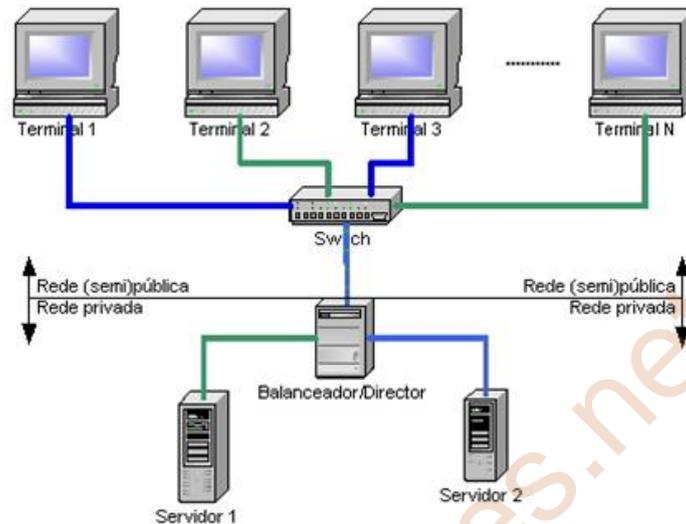
En el mundo de los servidores web existen puertos de red con velocidades de:

- 10mbps
- 100mbps
- 1gbps
- 10gbps
- 40gbps
- 100gbps

El ancho de banda es el que te permite tener un volumen suficiente para transmitir información de ida y vuelta hacia y desde tu servidor web.

## 7. Google tiene millones de equipos en Internet, averigua qué tipo de topología y tipo de red usan.

Usan este tipo de topología:



Cuando alguien intenta conectarse a Google, los servidores DNS (Sistema de nombre de dominio) traducen la dirección `www.google.com` a varias IP's distintas permitiendo que se distribuya la carga (balanceo de carga) entre varios clusters. Cuando un dominio tiene varias IP's, como en el caso de Google, el orden en que los servidores DNS traducen las direcciones IP se calcula mediante el sistema de planificación Round-robin.

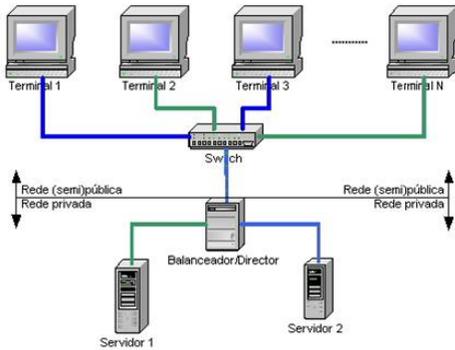
Cada cluster de Google tiene miles de servidores, por lo que cuando alguien se conecta a un cluster, se distribuye la carga de nuevo mediante el hardware del cluster para enviar la consulta al servidor web que esté menos ocupado en ese momento.

Los racks de Google están hechos a medida y pueden contener entre 40 y 80 servidores. Cada rack tiene una conexión ethernet a un router local que a su vez se conecta al router central utilizando una conexión de 1 Gigabit.

Es decir, el balanceo de carga se asegura de que un servidor no se vea sobrecargado por una gran afluencia de tráfico y que este tráfico cause una caída del sistema evitando su acceso para los usuarios. Este procedimiento es esencial ya que no se sabe el momento exacto en que las peticiones a un servidor serán altas, por ejemplo si se posee un servidor dedicado a procesar transacciones de banco, y de pronto ocurre un evento externo el cual obliga a las personas a realizar el triple de transacciones de lo habitual, este servidor sin un correcto balanceo de carga colapsara en menos de 15 minutos.

**Cluster:** Es un grupo de ordenadores unidos a una red de alta velocidad, de tal forma que el conjunto es visto como un único ordenador.

La tipología que utiliza Google es una **topología mixta o híbrida** al utilizar varias tipologías diferentes, en este caso la topología de acceso a Internet que es una colección interconectada de muchas redes pública y topología estrella a la red privada.



**La tipología** de acceso a la red pública que es una colección interconectada de muchas redes a través de la **red MAN** y la **red WAN** para acceder a los principales centros de Google que se encuentran en Mountain View (California), Virginia, Memphis Atlanta y Dublín, etc. y la **tipología en estrella** al estar dentro de una **red privada LAN** de Google tanto el balanceador y servidores.

**La red de Google:** Se trata de todos los lugares donde se pueden mostrar sus anuncios de Google, como los sitios de Google, los sitios web asociados con Google y otras ubicaciones, como las aplicaciones para móviles.

La red de Google se divide en grupos para proporcionarle un mayor control sobre dónde quiere que se muestre su anuncio.

- La **Red de Búsqueda:** las páginas de resultados de búsqueda de Google, otros sitios web de Google, como Maps y Shopping, y los sitios web de búsqueda asociados con Google para mostrar anuncios.
- La **Red de Display:** sitios web de Google, como YouTube, Blogger y Gmail, además de miles de sitios web asociados en Internet.

## 8. Busca programas P2P, indica su uso y explica por qué se usan para cometer delitos.

Los cinco mejores programas de intercambio de archivos P2P son:

### 1- uTorrent, el campeón absoluto y por KO

En la cúspide, el número uno no es otro que uTorrent, el cliente de Bit Torrent preferido por la gran mayoría de los usuarios. Una maravilla extremadamente **liviana, potente y rápida**, y todo ello empaquetado en un exquisito diseño.

La información, ya sea del archivo descargado o del progreso de descarga, es pormenorizada y ofrece esa agradable sensación de tenerlo todo bajo control.

También te sigue fuera de casa: uTorrent cuenta con una **versión portable** y la opción de controlar tus descargas **de forma remota**. Tus opciones extras y extensiones son numerosas y lo convierten en el programa P2P más completo.

### 2- Vuze, el P2P más elegante

El segundo de la lista se llama Vuze, y aunque no es el más conocido, su **ligereza, potencia y mejor diseño** lo convierten en un programa P2P más que notable. No solo es fulminante en la búsqueda, sino que es uno de los programas más veloces en encontrar archivos.

Si a esto le sumamos su extensa colección de *plugins* y servicios extra, como el **asistente de grabación de DVD**, el reproductor HD o su lector RSS, no hay duda de que merece este segundo puesto.

### 3- Ares, el coloso de las descargas

En el número tres el gigantesco Ares, el P2P más descargado en Softonic y el preferido por millones de personas.

Su **inmenso catálogo** y **facilidad de uso**, así como algunas de sus características avanzadas, como la posibilidad de previsualizar los archivos antes de descargarlos por completo, hacen que su gran comunidad de usuarios se mantenga fiel, lo que al mismo tiempo repercute en una mejor experiencia de usuario. Si no lo has probado ya, deberías hacerlo.

### 4- BitTorrent, porque los clásicos nunca mueren

En el cuarto escalón hemos situado a BitTorrent, porque dan igual las alternativas que vayan apareciendo, como el loable aunque frustrado Tribler: el clásico sigue dando caña. Es el cliente oficial de BitTorrent, utiliza **muy pocos recursos de tu ordenador**, es un programa P2P **potentísimo** y cuenta con funciones como el control remoto de las descargas.

## 5- eMule, el clásico que nunca muere

El puesto número cinco es para **eMule**, el P2P que en sus tiempos supuso toda una revolución, extendiendo el uso de esta tecnología entre millones de usuarios gracias a su facilidad de uso y el salto cualitativo que suponía respecto a **eDonkey**.

En la actualidad ha visto reducir mucho sus servidores, no es el más rápido y ha quedado un poco desfasado. Aun así, sigue contando con un **gran número de usuarios** que siguen compartiendo sus archivos de forma activa.

### ¿Cuál es su uso?

Una red P2P o 'peer to peer' es un tipo de conexión con una arquitectura destinada a la comunicación entre aplicaciones. Esto permite a las personas o a los ordenadores compartir información y archivos de uno a otro sin necesidad de intermediarios, es decir, **P2P (Peer to Peer)** significa de colega a colega, y son aquellos programas **que** permiten a los usuarios de Internet conectarse entre sí y compartir archivos que están en sus ordenadores.

Las redes P2P se pueden utilizar para muchos propósitos. La más habitual es la opción de **compartir archivos de cualquier tipo**, como audio, vídeo, imágenes o software variado, pero también se utiliza en **telefonía VoIP** (voz sobre protocolo de Internet) como Skype para que el 'streaming' en tiempo real funcione de manera más correcta, para hacer **enrutamientos anónimos** (Tor), para crear sistemas de ficheros distribuidos para hacer cálculos científicos o para hacer **transacciones mediante moneda virtual** (Bitcoin), entre otras cosas.

El origen de esta red tal y como la conocemos hoy en día se remonta a 1999, cuando Internet comenzaba su expansión y aterrizaba en los hogares. En mayo de ese año, un programador estadounidense que tenía problemas para encontrar la música que quería, **Shawn Fanning**, creó Napster, una aplicación virtual para compartir archivos .mp3 entre usuario totalmente independiente de una red física.

A pesar de que ese 'intercambio de archivos' lo más común en la red P2P, esta conexión no solo sirve para eso, sino que también tiene otras funciones, una serie de beneficios y también algunas desventajas.

Por ello, la principal ventaja de estas redes es **que administran y optimizan el ancho de banda** de todos los usuarios gracias a la arquitectura de comunicación que poseen, obteniendo una mayor eficiencia de las transferencias sin necesitar nada más.

De este modo se evita que los posibles **servidores intermediarios formen un cuello de botella** que no consiga funcionar de manera correcta y dejar que las transmisiones de archivos sean óptimas. Al no existir una autoridad única que pueda colapsarse, la red tiene una **capacidad innata para sobrevivir por sí misma**, además de tratarse de una conexión fuerte y muy versátil.

## ¿Por qué se puede cometer delitos?

Ese consumo de ancho de banda puede llegar a ser excesivo, ralentizando otros procedimientos que se hagan con el ordenador que está actuando. Además, se utilizan para **violar los derechos de propiedad intelectual**, es difícil crear protocolos de control de acceso a la red con ellas y si no se tiene cuidado con su uso pueden llegar a ser una fuente importante de 'malware' (se pueden descargar virus de todo tipo en ese intercambio de información).

Uno de sus usos, el relacionado con el **intercambio de información entre dos o más usuarios**, lleva tiempo siendo objeto de controversia. Mucha gente ha aprovechado esta función para traspasar **contenido sujeto a 'copyright'**, es decir, para enviar y recibir archivos con derechos de autor de manera ilegal. El ejemplo actual más importante aquí es **Torrent**, pero también podemos remontarnos a **eMule**, entre otros.

A través de ese servicio se pueden **saltar las leyes de protección de la propiedad intelectual** para intercambiar series, películas, música, videojuegos, etc. Determinados usuarios ponen a disposición del público cierto contenido en sus ordenadores y se conectan a una red P2P; los demás acceden a dicho contenido a través de alguna web, enlace o pequeño archivo y lo van sustrayendo poco a poco, como si se hiciera una **copia de manera 'local'** aunque estén en sitios diferentes.

Hay expertos que señalan que a pesar de esos derechos de autor, al tratarse de una copia privada (no hay intermediarios, es como si alguien le hace una copia de su disco favorito a su pareja) no puede ser ilegal, al menos si no hay ánimo de lucro de por medio.

**Las redes P2P en España**, ni en otros muchos países del mundo, **no son ilegales**, ya que pueden utilizarse para compartir archivos personales, creaciones propias, obras sin derechos, etc. El foco de la atención está puesto sobre las **páginas web que suministran los enlaces** de descarga del contenido, como las famosas The Pirate Bay o Kickass Torrents, ambas perseguidas por la policía. Estos dominios ponen el contenido a disposición de todo el mundo, pero sus páginas cuentan con publicidad, por lo que están obteniendo dinero por ello y por eso en muchos países son consideradas como ilegales.

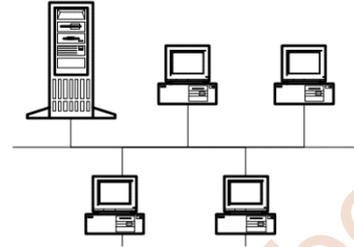
En nuestro país uno de los referentes de los que más se han hecho eco los medios de comunicación es el **caso Sharemula**, una web que suministraba enlaces P2P a los usuarios. En 2007 un juzgado de Madrid declaró que **no había actividad delictiva** en el funcionamiento porque los enlaces como tal no contienen la obra, sino que llevan a otra página diferente para la descarga; el caso acabó llegando a la Audiencia Provincial de la capital en 2008, donde se cerró a favor del dominio por la misma razón.

## Tarea 1.4-Topologías

1. Busca en internet las ventajas e inconvenientes de las diferentes topologías de las redes: Bus, estrella, anillo, mixta.

### Red en bus

Una **red en bus** es aquella topología que se caracteriza por tener un único canal de comunicaciones (denominado bus, troncal o backbone) al cual se conectan los diferentes dispositivos. De esta forma todos los dispositivos comparten el mismo canal para comunicarse entre sí.



### **Ventajas de red en bus**

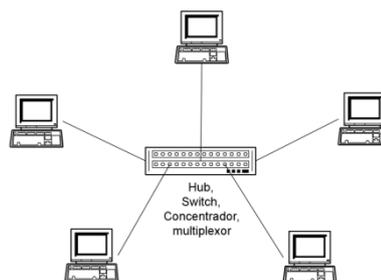
- Facilidad de implementación y crecimiento.
- Simplicidad en la arquitectura.
- Es una red que no ocupa mucho espacio.
- Están constituidas fundamentalmente por elementos pasivos, solo encontrándose elementos activos en las estaciones.
- Por tanto una avería solo afectaría a la estación implicada.
- Presentan una alta modularidad, por lo que es facilísimo añadir o retirar estaciones de la red.
- Su adaptación a la distribución geográfica se realiza con un coste reducido.

### **Desventajas red en bus**

- Hay un límite de equipos dependiendo de la calidad de la señal.
- Puede producirse degradación de la señal.
- Complejidad de reconfiguración y aislamiento de fallos.
- Limitación de las longitudes físicas del canal.
- Un problema en el canal usualmente degrada toda la red.
- El desempeño se disminuye a medida que la red crece.
- El canal requiere ser correctamente cerrado (camino cerrado).
- Altas pérdidas en la transmisión debido a colisiones entre mensajes.
- Una avería en el bus provoca en el mejor de los casos la incomunicación entre los segmentos de red que se generan.

## Red en estrella

Una **red en estrella** es una red de computadoras donde las estaciones están conectadas directamente a un punto central y todas las comunicaciones se hacen necesariamente a través de ese punto (conmutador, repetidor o concentrador).



Los dispositivos no están directamente conectados entre sí, además de que no se permite tanto tráfico de información. Dada su transmisión, una red en estrella activa tiene un nodo central "activo" que normalmente tiene los medios para prevenir problemas relacionados con el eco.

Se utiliza sobre todo para redes locales (LAN). La mayoría de las redes de área local que tienen un conmutador (*switch*) o un concentrador (*hub*) siguen esta topología. El punto o nodo central en estas sería el switch o el hub, por el que pasan todos los paquetes de usuarios.

### **Ventajas de red en estrella**

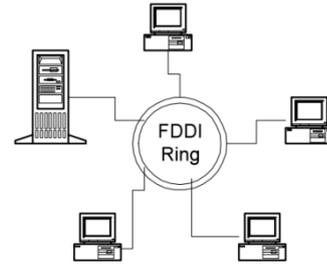
- Posee un sistema que permite agregar nuevos equipos fácilmente.
- Reconfiguración rápida.
- Fácil de prevenir daños y/o conflictos, ya que no afecta a los demás equipos si ocurre algún fallo.
- Centralización de la red.
- Fácil de encontrar fallos
- El acceso está en todo momento bajo el control de la central.
- La configuración de la red y la localización de fallos son fáciles, ya que pueden estar gestionadas por el nodo central.

### **Desventajas red en estrella**

- Si el hub (repetidor) o switch central falla, toda la red deja de transmitir.
- Es costosa, ya que requiere más cables que las topologías en bus o anillo.
- El cable viaja por separado del concentrador a cada computadora.
- En caso de fallo del nodo central se produce el bloqueo de toda la red.
- La longitud de cableado es elevada.

## Red en anillo

Una **red en anillo** es una topología de anillo en la que cada estación tiene una única conexión de entrada y otra de salida de anillo. Cada estación tiene un receptor y un transmisor que hace la función de traductor, pasando la señal a la siguiente estación.



Cada equipo lleva una tarjeta repetidora.

En este tipo de red la comunicación se da por el paso de un *token* o testigo, que se puede conceptualizar como un cartero que pasa recogiendo y entregando paquetes de información, de esta manera se evitan eventuales pérdidas de información debidas a colisiones.

En un anillo doble (*Token Ring*), dos anillos permiten que los datos se envíen en ambas direcciones (*Token passing*). Esta configuración crea redundancia (tolerancia a fallos).

### **Ventajas en anillo**

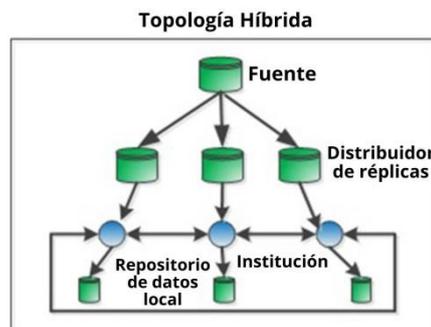
- El sistema provee un acceso equitativo para todas las computadoras.
- El rendimiento no decae cuando muchos usuarios utilizan la red.
- Arquitectura muy sólida.
- Facilidad para la fluidez de datos.
- Sistema operativo caracterizado con un único canal
- El tiempo de respuesta está controlado.
- Facilita la gestión de averías.

### **Desventajas en anillo**

- Longitudes de canales (si una estación desea enviar a otra, los datos tendrán que pasar por todas las estaciones intermedias antes de alcanzar la estación de destino).
- El canal usualmente se degradará a medida que la red crece.
- Difícil de diagnosticar y reparar los problemas.
- Si se encuentra enviando un archivo podrá ser visto por las estaciones intermedias antes de alcanzar la estación de destino.
- La transmisión de datos es más lenta que en las otras topologías (Estrella, Malla, Bus, etc), ya que la información debe pasar por todas las estaciones intermedias antes de llegar al destino.
- Al estar todas las estaciones involucradas en la transferencia de datos, el fallo de un repetidor inutiliza por completo la red.
- Requiere de mecanismos de control sofisticados para detectar informaciones corruptas y evitar un ciclo sin-fin de retransmisiones (en algunos casos de hace uso de una estación monitora).

### Red mixta o híbrida

La **topología mixta** es un tipo de topología de red que utiliza dos o más topologías de red diferentes. Esta topología contiene una combinación de la topología de bus, topología de malla, topología de anillo y topología de estrella.



Esta topología tiene las características y limitaciones de los componentes que la conforman. Comúnmente se utilizan dos tipos de topología mixta: la topología estrella-bus y la topología estrella-anillo.

### **Ventajas en red mixta**

- La topología mixta de red tiene muchas ventajas. Estas topologías son flexibles, confiables y tienen mayor tolerancia a fallas.
- La principal ventaja de la estructura mixta es el grado de flexibilidad que proporciona, ya que hay pocas limitaciones en la estructura de una red como tal que una configuración mixta no pueda adaptar.
- Este tipo de red es capaz de utilizar los aspectos más fuertes de otras redes, tal como la intensidad de la señal.

### **Desventajas en red mixta**

- Cada topología de red tiene sus desventajas particulares. Por tanto, a medida que crezca la complejidad de la red también crecerá el requerimiento de experiencia y conocimientos necesarios por parte de los administradores de la red para que todo funcione de forma excelente.
- Por otro lado, la instalación es difícil y el diseño es complejo, por lo que el mantenimiento es elevado y, por tanto, costoso.
- Igualmente, al implantar una topología de red mixta se debe considerar el costo monetario, incluyendo el requerimiento de equipos de alta gama.

- Ejecuta la instrucción “getmac” en la línea de comandos para averiguar la dirección MAC de tu ordenador. Con los 3 primeros bytes averigua el fabricante de tu tarjeta.

```
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\Equipo>getmac

Dirección física      Nombre de transporte
=====
0A-00-27-00-00-12    \Device\NPF{549E609C-C3C5-400F-9588-3E72D2605F09}
0A-FE-DB-00-27-25    Medios desconectados
FC-AA-14-28-22-77    \Device\NPF{40DABBDA-4B75-4A52-9CD1-E8672E751E98}

C:\Users\Equipo>ipconfig/all

Configuración IP de Windows

Nombre de host. . . . . : Equipo-PC
Sufijo DNS principal . . . . . :
Tipo de nodo. . . . . : híbrido
Enrutamiento IP habilitado. . . . . : no
Proxy WINS habilitado . . . . . : no

Adaptador de Ethernet Conexión de área local 6:
. . . . .
Descripción . . . . . : Realtek PCIe GBE Family Controlle
r #2
Dirección física. . . . . : FC-AA-14-28-22-77
. . . . .
```

Los 3 primeros bytes que son los 6 primeros dígitos de mi tarjeta de red con la dirección física o MAC es: FC-AA-14.

OUI	MAC range	Company
FC-AA-14	FC-AA-14-00-00-00 - FC-AA-14-FF-FF-FF	GIGA-BYTE TECHNOLOGY CO.,LTD.

En un buscador de internet tenemos: El identificador Único Organizacional (OUI) FC-AA-14 le corresponde con el fabricante GIGA-BYTE TECHNOLOGY CO.,LTD.

También mediante la descripción en ipconfig/all tenemos Realtek PCIe GBE Family Controller, en donde GBE significa GIGA-BYTE.

<https://es.adminsub.net/mac-address-finder/FC-AA-14>

- Busca la IP y el DNS de tu ordenador en el instituto y en casa.

El IP y el DNS de mi ordenador de sobremesa:

```
Adaptador de Ethernet Conexión de área local 6:
. . . . .
Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : Realtek PCIe GBE Family Controlle
r #2
Dirección física. . . . . : FC-AA-14-28-22-77
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . : sí
Vínculo: dirección IPv6 local. . . . . : fe80::3df7:5fed:2f5f:620c%17<Preferido>
Dirección IPv4. . . . . : 192.168.0.10<Preferido>
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : miércoles, 06 de octubre de 2021
15:55:42
La concesión expira . . . . . : jueves, 07 de octubre de 2021 15:
55:42
Puerta de enlace predeterminada . . . . . : 192.168.0.1
Servidor DHCP . . . . . : 192.168.0.1
IÁID DHCPv6 . . . . . : 536652308
DUID de cliente DHCPv6. . . . . : 00-01-00-01-1D-91-A0-52-FC-AA-14-
28-22-77
Servidores DNS. . . . . : 212.166.211.23
212.166.132.104
NetBIOS sobre TCP/IP. . . . . : habilitado
```

El IP y el DNS del ordenador del instituto:

```
Microsoft Windows [Versión 10.0.19043.1288]
(c) Microsoft Corporation. Todos los derechos reservados.

C:\Users\usuario>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Ethernet:
    Suftio DNS específico para la conexión. . . : smr1.iescdl.es
    Vínculo: dirección IPv6 local. . . . . : fe80::2d63:e178:81c5:a522%6
    Dirección IPv4. . . . . : 192.168.128.176
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.128.1
```

4. Explica para qué sirven las instrucciones de consola ipconfig, ping, tracert y pon un ejemplo de uso.

### ipconfig

**ipconfig** en Microsoft Windows es una aplicación **de consola** que muestra los valores **de configuración de red de TCP/IP** actuales y actualiza la configuración del protocolo DHCP y el sistema **de nombres de dominio (DNS)**.

### Parámetros de Ipconfig

Parámetro	Descripción
/all	Mostrar la información de configuración completa de TCP/IP para todos los adaptadores de red.
/release	Libera la dirección IPv4 del adaptador especificado.
/release6	Libera la dirección IPv6 del adaptador especificado.
/renew	Renueva la dirección IPv4 para el adaptador especificado.
/renew6	Renueva la dirección IPv6 para el adaptador especificado.
/flushdns	Purga el caché del DNS Resolver.
/registerdns	Refresca todas las concesiones DHCP y vuelve a registrar los nombres del DNS.
/displaydns	Mostrar el contenido del DNS Resolver Cache.
/showclassid	Muestra todas las identificaciones de clase del DHCP permitidas para el adaptador.
/setclassid	Modifica la ID de clase del DHCP.
/showclassid6	Muestra todas las IDs de clase IPv6 DHCP permitidas para el adaptador.
/setclassid6	Modifica el ID de clase IPv6 DHCP.
/?	Muestra información de ayuda.

Para obtener información básica de la red de tu ordenador, escribe ipconfig en la ventana de comandos y luego presiona **Enter**.

El ejemplo de la captura de pantalla que se muestra a continuación es la salida del ipconfig de mi ordenador de sobremesa particular. La salida del resultado del ipconfig

variará dependiendo de la configuración de la red y del tipo de adaptadores de red instalados en el equipo. En nuestro ejemplo de pantalla, muestra la siguiente información de red básica sobre el computador desde el que se ejecutó ipconfig.

```
C:\Users\Equipo>ipconfig

Configuración IP de Windows

Adaptador de Ethernet Conexión de área local 6:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local . . . . . : fe80::3df7:5fed:2f5f:620c%17
    Dirección IPv4. . . . . : 192.168.0.10
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . : 192.168.0.1

Adaptador de Ethernet Conexión de área local 5:

    Estado de los medios. . . . . : medios desconectados
    Sufijo DNS específico para la conexión. . . :

Adaptador de Ethernet VirtualBox Host-Only Network:

    Sufijo DNS específico para la conexión. . . :
    Vínculo: dirección IPv6 local. . . . . : fe80::88c7:7f1a:dadf:b878%18
    Dirección IPv4. . . . . : 192.168.56.1
    Máscara de subred . . . . . : 255.255.255.0
    Puerta de enlace predeterminada . . . . . :

C:\Users\Equipo>
```

Hay que tener en cuenta que a menos que el ordenador esté conectado directamente a Internet (esto es raro), la dirección IP reportada por ipconfig será la IP de mi red local, no tu dirección IP externa pública. Estos tres datos Dirección IPv4, Mascara de subred y Puerta de enlace predeterminada es lo que típicamente se necesita.

### ping

**Ping es un comando o una herramienta de diagnóstico que permite hacer una verificación del estado de una determinada conexión de un host local con al menos un equipo remoto contemplado en una red de tipo TCP/IP. Sirve para determinar si una dirección IP específica o host es accesible desde la red o no.**

**Ping se utiliza comúnmente para comprobar si hay errores de red. El funcionamiento del mecanismo es muy simple y puede ser de mucha ayuda. Trabaja mediante el envío de series de información a una dirección IP, host o servidor. Por medio del tiempo de espera de la respuesta a ese envío de información se determina el retraso o no de esa respuesta, lo que también se conoce como latencia.**

```
Microsoft Windows [Versión 6.1.7601]
Copyright (c) 2009 Microsoft Corporation. Reservados todos los derechos.

C:\Users\Equipo>ping www.google.com

Haciendo ping a www.google.com [172.217.17.4] con 32 bytes de datos:
Respuesta desde 172.217.17.4: bytes=32 tiempo=16ms TTL=117
Respuesta desde 172.217.17.4: bytes=32 tiempo=17ms TTL=117
Respuesta desde 172.217.17.4: bytes=32 tiempo=16ms TTL=117
Respuesta desde 172.217.17.4: bytes=32 tiempo=16ms TTL=117

Estadísticas de ping para 172.217.17.4:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos)
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 16ms, Máximo = 17ms, Media = 16ms

C:\Users\Equipo>
```

En la imagen de ejemplo de mi ordenador de sobremesa, el comando ping ha enviado cuatro paquetes al destino (google.com), que nos ha respondido correctamente. También podemos enviar más paquetes que los cuatro que vienen por defecto, colocando el comando -n al final del destino, junto con el número de resultados que queramos. Por ejemplo: «ping google.com -n 10 » o «ping -n 10 google.com »

```
C:\Users\Equipo>ping www.google.com -n 10

Haciendo ping a www.google.com [172.217.17.4] con 32 bytes de datos:
Respuesta desde 172.217.17.4: bytes=32 tiempo=17ms TTL=117
Respuesta desde 172.217.17.4: bytes=32 tiempo=18ms TTL=117
Respuesta desde 172.217.17.4: bytes=32 tiempo=15ms TTL=117

Estadísticas de ping para 172.217.17.4:
    Paquetes: enviados = 10, recibidos = 10, perdidos = 0
    (0% perdidos).
    Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 15ms, Máximo = 18ms, Media = 17ms
```

### tracert

Es una herramienta de diagnóstico, que igual que ping, envía una serie de paquetes, con la diferencia que nos muestra la ruta que toma hasta el destino. Durante el camino, nos muestra los datos de los hosts por los que va pasando, y el tiempo que toma en cada salto hasta su llegada al destino. Por lo tanto, podemos decir que si tenemos una pérdida de paquetes (identificada en el ping) podemos saber dónde exactamente falla.

```
C:\Users\Equipo>tracert www.google.com

Trazo a la dirección www.google.com [172.217.17.4]
sobre un máximo de 30 saltos:

 1  <1 ms    <1 ms    <1 ms    192.168.0.1
 2  17 ms    11 ms    11 ms    10.194.131.1
 3  8 ms     9 ms     10 ms    10.80.9.181
 4  9 ms     9 ms     8 ms     172.29.184.101
 5  *        *        *        Tiempo de espera agotado para esta solicitud.
 6  18 ms    19 ms    17 ms    212.166.147.222
 7  18 ms    19 ms    19 ms    172.253.50.47
 8  21 ms    19 ms    17 ms    74.125.253.199
 9  17 ms    17 ms    21 ms    mad07s09-in-f4.1e100.net [172.217.17.4]

Trazo completa.
C:\Users\Equipo>
```

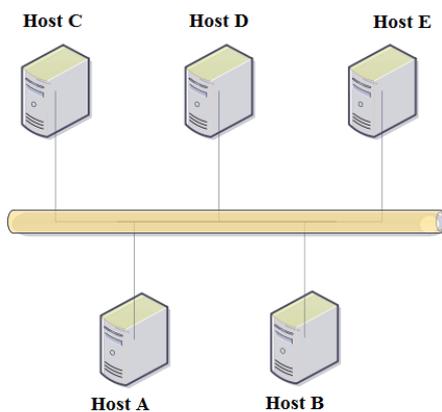
Lo primero que hace el comando al ser ejecutado es mostrar la dirección IP real del dominio de la web que hayas elegido, en este caso www.google.com. Luego, **te irá diciendo uno a uno todos los nodos** y routers por los que pasa el mensaje de prueba que has enviado, sus direcciones IP y la latencia de cada uno de ellos hasta llegar a su destino.

Como puedes ver en nuestra captura, hay veces en las que algunos nodos o routers te pueden devolver el mensaje de *Tiempo de espera agotado*, algo que pasa cuando son equipos que tienen limitada la función de tracert, al formar parte de la red interna de tu operador de Internet. Vamos, una medida interna de seguridad. Pero cuando sale de la red del operador, el último mensaje es siempre el del dominio u ordenador con el que has trazado la ruta.

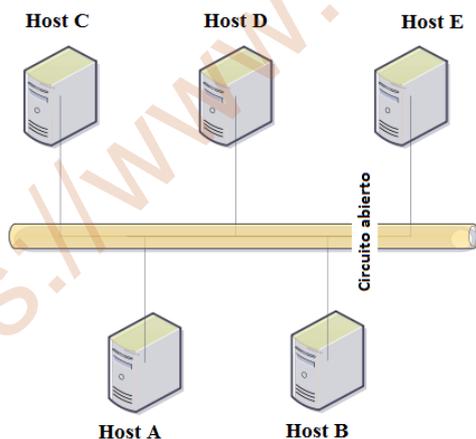
5. Si en una topología en bus se desconecta un fragmento de ella ¿Sigue funcionando? Justifica la respuesta.

La fragmentación IP es una técnica utilizada para dividir los datagramas IP en fragmentos de menor tamaño. Esto es necesario ya que cuando los datagramas IP viajan de un lugar a otro, éstos pueden atravesar diferentes tipos de redes y el tamaño máximo -llamado MTU (unidad máxima de transferencia) de estos paquetes puede variar dependiendo del medio físico utilizado para la transmisión.

Una red en bus es aquella topología que se caracteriza por tener un único canal de comunicaciones (denominado bus, troncal o backbone) al cual se conectan los diferentes dispositivos. De esta forma todos los dispositivos comparten el mismo canal para comunicarse entre sí.



Si se envía un datagrama de información desde el Host A hasta el Host E y este se fragmenta en pequeños paquetes, toda esta información de pequeños paquetes ira a toda la red bus buscando la dirección IP que le corresponda a su destino. Si una parte del paquete o fragmento no llega a su destino dependerá del modo de envío del datagrama. Si el envío es orientado a conexión fiable (TCP) tiene que llegar todos los paquetes a su destino con acuse de recibo, y por lo tanto no sigue funcionando al no llegarle todos los paquetes. Si la conexión es no fiable (UDP) no tiene por qué llegarle todos los paquetes por lo que en este caso si seguiría funcionando.

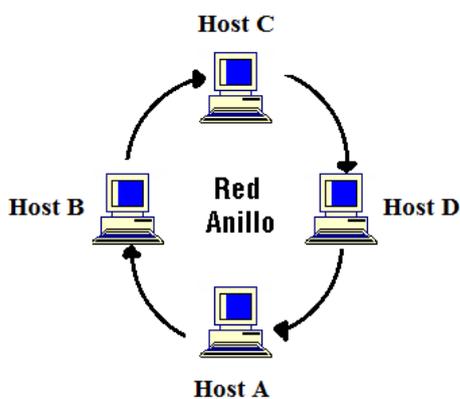


Si ahora se envía un datagrama de información desde el Host A hasta el Host E y este se fragmenta en pequeños paquetes, toda esta información de pequeños paquetes ira a toda la red bus en broadcast (a todos los ordenadores) buscando la dirección IP que le corresponda a su destino. Si esta topología en bus está el circuito abierto o fallo de un nodo hasta el Host E la información o los paquetes no llegarían a su destino, ni tampoco al resto de Host u ordenadores dejando al conjunto de nodos incomunicados entre sí.

6. Si en una topología en anillo se desconecta un fragmento de ella ¿Sigue funcionando? Justifica la respuesta.

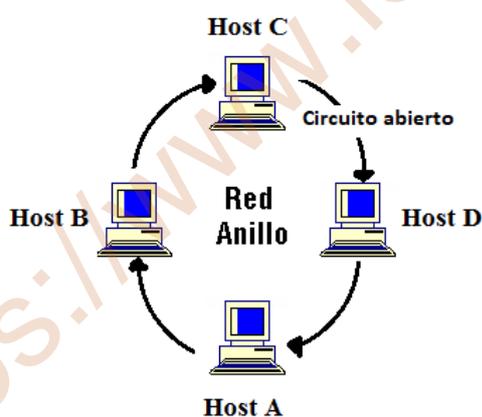
La fragmentación IP es una técnica utilizada para dividir los datagramas IP en fragmentos de menor tamaño. Esto es necesario ya que cuando los datagramas IP viajan de un lugar a otro, éstos pueden atravesar diferentes tipos de redes y el tamaño máximo -llamado MTU (unidad máxima de transferencia) de estos paquetes puede variar dependiendo del medio físico utilizado para la transmisión.

La Topología de redes la que cada estación está conectada a la siguiente y la última está conectada a la primera. Cada estación tiene un receptor y un transmisor que hace la función de repetidor, pasando la señal a la siguiente estación.



Si se envía un datagrama de información desde el Host A hasta el Host D y este se fragmenta en pequeños paquetes, toda esta información de pequeños paquetes ira a la red anillo, en este caso en sentido de las agujas del reloj según la configuración establecida, buscando la dirección IP que le corresponda a su destino. En este caso al enviar los paquetes fragmentados en un mismo anillo en sentido de las agujas del reloj todos los paquetes llegarían a su destino, salvo que falle una de las estaciones en la recepción y transmisión de la información.

Si se desconecta un fragmento con conexión no fiable (UDP) no tiene por qué llegarle todos los paquetes por lo que en este caso si seguiría funcionando. Si el envío es orientado a conexión fiable (TCP) tiene que llegar todos los paquetes a su destino con acuse de recibo, y por lo tanto no sigue funcionando al no llegarle todos los paquetes.

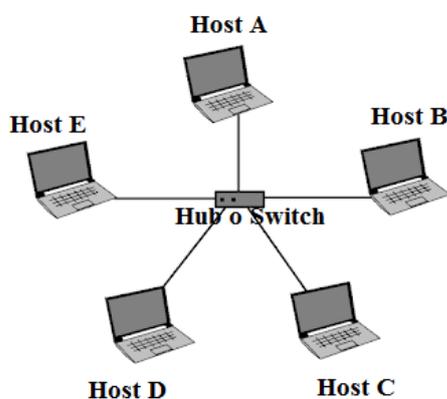


Si ahora se envía un datagrama de información desde el Host A hasta el Host D y este se fragmenta en pequeños paquetes, toda esta información de pequeños paquetes ira a toda la red en anillo buscando la dirección IP que le corresponda a su destino. Si esta topología en anillo está el circuito abierto hasta el Host D la información o los paquetes no llegaría a su destino, ni tampoco al resto de Host u ordenadores dejando de funcionar completamente esta tipología en anillo.

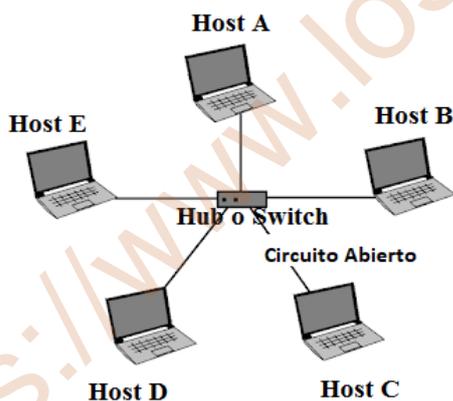
7. Si en una topología en estrella se desconecta un fragmento de ella ¿Sigue funcionando? Justifica la respuesta.

La fragmentación IP es una técnica utilizada para dividir los datagramas IP en fragmentos de menor tamaño. Esto es necesario ya que cuando los datagramas IP viajan de un lugar a otro, éstos pueden atravesar diferentes tipos de redes y el tamaño máximo -llamado MTU (unidad máxima de transferencia) de estos paquetes puede variar dependiendo del medio físico utilizado para la transmisión.

Una red en estrella es una red en la cual las estaciones están conectadas directamente a un punto central y todas las comunicaciones se han de hacer necesariamente a través de este. Los dispositivos no están directamente conectados entre sí, además de que no se permite tanto tráfico de información.



Si se envía un datagrama de información desde el Host A hasta el Host C y este se fragmenta en pequeños paquetes, toda esta información de pequeños paquetes ira al nodo central Switch, y este repartiría directamente a su destino. Si se desconecta un fragmento con conexión no fiable (UDP) no tiene por qué llegarle todos los paquetes por lo que en este caso si seguiría funcionando. Si el envío es orientado a conexión fiable (TCP) tiene que llegar todos los paquetes a su destino con acuse de recibo, y por lo tanto no sigue funcionando al no llegarle todos los paquetes.



Si ahora se envía un datagrama de información desde el Host A hasta el Host C y este se fragmenta en pequeños paquetes, toda esta información de pequeños paquetes ira al nodo central Switch, y este repartiría directamente a su destino. Si esta topología en estrella está el circuito abierto hasta el Host C la información o los paquetes no llegarían a su destino, si llegaría al resto de ordenadores o Host B, Host D y Host E a través del Switch al no estar el circuito abierto.

## Tarea 1.5-Conexión entre dos empresas

Explica todos los elementos necesarios de electrónica de red, de software, servicios y cableado necesarios que se necesitarían para comunicarse dos empresas definiendo el tipo de tecnologías utilizadas, la arquitectura de red a diseñar y estándares utilizados, además de implantar algún método de seguridad. Ambas empresas se dedican al desarrollo de software y tienen más de 50 empleados.

Para la realización de la infraestructura he elegido dos edificios uno situados en la localidad de Rota (Cádiz) como edificio central y otra en la provincia de Málaga. El edificio en Rota será de tres plantas y el edificio de Málaga de dos plantas de oficinas. En cada uno de las plantas se destinará un cuarto de telecomunicaciones y se implementará a través de suelo técnico en el pasillo y por áreas o departamentos por el que irá la bandeja técnica que servirá de base para la tirada de cableado de voz y datos. En el edificio central de un ascensor que servirá de vertical para el paso de las instalaciones cada una de las plantas. El número de usuarios por cada edificio será de más de 50 empleados, sumando las conexiones inalámbricas.

Antes de definir una topología de red para esta empresa, la podemos definir como el mapa físico o lógico de una red para intercambiar datos. En otras palabras, es la forma en que está diseñada la red, sea en el plano físico o lógico. El concepto de red puede definirse como "conjunto de nodos interconectados".

El diseño elegido para ambas ubicaciones, central (Rota) y sucursal (Málaga), es una topología de estrella, ya que este tipo de instalación permite una mayor facilidad en el montaje así como una mayor robustez al conjunto. Si falla un cable, sólo ese equipo se quedará sin servicio, no como sucede en otro tipo de topologías. Por el contrario, serán necesarios muchos más metros de cables, que vayan de cada uno de los equipos al conector correspondiente.

La categoría de los componentes, cableado, switch, Racks, etc., será de categoría **6A**, con vistas a una posible ampliación en el futuro. La instalación soportará **1GbaseT**, con posibilidad de migrar a **10GbaseT**.

### **El número y distribución de las tomas de usuario se detallan a continuación:**

#### Edificio Central en Rota

- Planta baja:
  - Sala de comunicaciones. Dos Tomas
  - Departamento 1. 10 tomas
  - Departamento 2. 10 tomas
- Planta primera:
  - Departamento 3. 10 tomas
  - Departamento 4. 10 tomas
- Planta segunda:
  - Departamento 5. 10 tomas

### Edificio Sucursal en Málaga

Planta baja:

Sala de comunicaciones. Dos Tomas

Departamento 1. 10 tomas

Departamento 2. 10 tomas

Departamento 3. 10 tomas

Planta primera:

Departamento 3. 10 tomas

Departamento 4. 10 tomas

El número total de tomas a instalar en cada uno de los edificios es de 52 tomas.

El cableado vertical encuentra la dificultad de que al tener el distribuidor de planta próximo al hueco del ascensor, acarrea la inserción de posible ruido externo en el cable, con lo que se aconseja una instalación con cableado **SSTP**, ya que por su constitución permite la disminución del ruido, con un coste más elevado que el cableado UTP.

### **La infraestructura física de la instalación tenemos:**

#### Edificio Central en Rota

Planta baja:

En la sala de telecomunicaciones, se instalará el distribuidor de edificio y distribuidor de planta en un mismo Racks. Hasta éste, llegará el cableado de la operadora contratada. El distribuidor de esta planta dará servicio a un total de veintidós tomas.

Planta primera:

En la sala de telecomunicaciones, se instalará un distribuidor de planta que dará servicio a veinte tomas en esta altura. El cableado de entrada, que llega de la planta baja, y el de salida, que sube a la planta superior, se canaliza por el hueco del ascensor mediante cableado SSTP.

Planta segunda:

En la sala de telecomunicaciones, se instalará un distribuidor de planta que dará servicio a diez tomas en esta altura. El cableado de entrada, que llega de la planta primera, se canaliza por el hueco del ascensor mediante cableado SSTP.

#### Edificio Sucursal en Málaga

Planta baja:

En la sala de telecomunicaciones, se instalará el distribuidor de edificio y distribuidor de planta en un mismo Racks. Hasta éste, llegará el cableado de la operadora contratada. El distribuidor de esta planta dará servicio a un total de treinta y dos tomas.

□ Planta primera:

En la sala de telecomunicaciones, se instalará un distribuidor de planta que dará servicio a veinte tomas en esta altura. El cableado de entrada, que llega de la planta baja, se canaliza por el hueco del edificio mediante cableado UTP.

Se utilizará bandeja para suelo técnico para la tirada de cableado a lo largo de las plantas y se usará bandejas pasamuros en aquellos casos que sea necesario. Se instalarán rosetas dobles, con sistema de guardapolvo.

Se instalarán en cada una de los edificios sesenta **rosetas para voz y sesenta rosetas** para datos con conectores hembra RJ-45 (8P8C) de CAT 6A apantallados.

**Cálculo de equipamiento de datos en cada uno de los edificios:**

El **router** se encargará de dirigir el tráfico generado por los equipos informáticos que salgan a la “Nube”. Es el elemento principal de un SCE. Se situará en distribuidor principal, en la planta baja y se encargará de repartir los switch mediante cuatro interfaces. Todos los departamentos de la planta baja pertenecen a una misma red, las tomas de usuario, irán conectadas al switch. Así como en la primera y segunda planta, las tomas ofimáticas irán conectadas a sus respectivos switch, éstos se conectarán al router de la planta baja.

**Switch:** La función básica de un switch es la de **unir o conectar dispositivos en red**. Es importante tener claro que un switch **NO** proporciona por si solo conectividad con otras redes, y obviamente, **TAMPOCO** proporciona conectividad con Internet. Para ello es necesario un router. La función básica que realiza un switch se conoce como conmutación y consiste en transferir datos entre los diferentes dispositivos de la red. Para ello, los switches procesan la información contenida en las cabeceras de la trama Ethernet. Ethernet es una tecnología de transmisión de datos para redes locales cableadas que divide los datos que se tiene que transmitir en **tramas** y a cada trama se le añade una determinada información de control llamada **cabecera**. Dicha cabecera contiene la dirección MAC tanto del emisor como del receptor. Los switches guardan en una tabla las direcciones MAC de todos los dispositivos conectados junto con el puerto en el que están conectados, de forma que cuando llega una trama al switch, dicha trama se envía al puerto correspondiente. Los **switch** comúnmente vienen con 5, 8, 10, 24 y 48 **puertos**.

**Servidor:** En el sentido del hardware, etiqueta modelos de computadora diseñados para hospedar un conjunto de aplicaciones que tiene gran demanda dentro de una red. En esta configuración cliente-servidor, uno o más equipos, lo mismo una computadora que una aplicación informática, comparten información entre ellos de forma que uno actúa como Host de los otros. Equipamiento que almacenará y gestionará el correo electrónico y el servicio Web de la central y la sucursal.

**Punto de acceso wifi:** Están diseñados para establecer o ampliar una red inalámbrica N de alta velocidad escalable o para conectar a una red inalámbrica múltiples dispositivos adaptados a Ethernet.

Un rack es un soporte metálico destinado a alojar equipamiento electrónico, informático y de comunicaciones. Las medidas para la anchura están normalizadas bajo el standard 19" para que sean compatibles con equipamiento de cualquier fabricante. También son llamados bastidores, cabinas o armarios informáticos, rack de comunicaciones, etc.

**Ventilador rack:** Las unidades de ventilación están diseñadas para no ocupar espacio en el interior de los armarios, ya que se fijan directamente en el techo.

Los **patch panel** (paneles parcheo o IPF) harán de conectores intermediarios entre las rosetas y el switch que vayan conectadas. Hay varias ventajas en usar patch pannel, logrando más durabilidad en los switch, ya que se reducirán las conexiones / desconexiones. Además en las instalaciones con patch-pannel se facilita el manejo de los latiguillos. Utilizaremos paneles de conexión de veinticuatro puertos en cada una de las plantas, con posibilidad de conexiones de categoría 6A en una U. Es importante tener buenos paneles de conexión para que no nos limite la calidad y la velocidad de nuestra instalación. Llevan los cables de datos de los diferentes puestos de trabajo para conectorizarlos mediante latiguillos de parcheo directamente al switch.

**Bridge:** Este elemento evitará cualquier zona de sombra de cobertura a lo largo del edificio. Será instalado en el techo de la planta primera y segunda, únicamente condicionado por un punto de fuerza de 12 V para poder estar encendido continuamente.

**SAI'S:** Es importante tener sistemas de alimentación ininterrumpidos para protegerse de posibles caídas de tensión, apagones, o picos de corriente. El sistema de alimentación ininterrumpidos es un dispositivo que posee una serie de baterías u otros elementos almacenadores de energía con el que se puede proporcionar energía eléctrica por un tiempo limitado (depende de la SAI) en casa de no tener corriente, por ejemplo un apagón, a todos los dispositivos que tenga conectados.

**Cortafuegos** o firewall en inglés, en el mundo de la informática es un sistema de seguridad para **bloquear accesos no autorizados a un ordenador** mientras sigue permitiendo la comunicación de tu ordenador con otros servicios autorizados. También se utilizan en redes de ordenadores, especialmente en intranets o redes locales. Se trata de una de las primeras medidas de seguridad que empezó a implementarse en los ordenadores tras el nacimiento de Internet. Los cortafuegos pueden ser de dos tipos, **pueden ser software, de hardware o una combinación de ambos**. Esto quiere decir que pueden ser aplicaciones que instales en tu ordenador o dispositivos que se conecten a él para controlar el tráfico. Los cortafuegos físicos pueden ser productos independientes o venir directamente integrados en un router. Los independientes se suelen situar entre el punto de acceso a Internet y el switch que se encarga de distribuir la conexión entre los ordenadores de una misma red. El hecho de que vaya antes de la

distribución de la red entre los equipos significa que todos los que haya en una red interna quedan protegidos.

#### Edificio Central en Rota

- Planta baja:
  - Armario **rack** principal y distribuidor que da conectividad a todo el edificio, además de conectar la central y sucursal.
  - Ventilador Rack.
  - Patch pannel de 24 puertos
  - Centralita telefónica (PBX)
  - Un **Switch** de 24 puertos.
  - Un **router** y se conectarán los tres switch a él y éste llevará toda la organización del Edificio.
  - El número de **router inalámbrico** será **uno**, con **dos puntos bridge**.
  - Dos **servidores** en la sede central de la empresa, uno de ficheros y otros de correos web.
  - **Cortafuegos** de protección a los servidores para violaciones de seguridad y ataques de malware.
  
- Planta primera:
  - Rack: Se encarga de interconectar el subsistema horizontal de la planta con el subsistema vertical, de forma que todas las plantas puedan acceder al router que se encuentra en el distribuidor de planta.
  - Ventilador Rack.
  - Patch pannel de 24 puertos.
  - Un Switch de 24 puertos (en esta planta dispone de 20 tomas pero selecciona la siguiente para futuras ampliaciones)
  
- Planta segunda:
  - Rack: Se encarga de interconectar el subsistema horizontal de la planta con el subsistema vertical, de forma que todas las plantas puedan acceder al router que se encuentra en el distribuidor de planta.
  - Ventilador Rack.
  - Patch pannel de 24 puertos.
  - Un Switch de 24 puertos (en esta planta dispone de 10 tomas pero selecciona la siguiente para futuras ampliaciones)

#### Edificio Sucursal en Málaga

- Planta baja:
  - Armario **rack** principal y distribuidor que da conectividad a todo el edificio, además de conectar la sucursal y central.
  - Ventilador Rack.

- Un **Switch** de 48 puertos (en esta planta dispone de 32 tomas pero selecciona la siguiente para futuras ampliaciones)
  - Un **router** y se conectarán los dos switch a él y éste llevará toda la organización del Edificio.
  - El número de **router inalámbrico** será **uno**, con un **punto bridge**.
- Planta primera:
- Rack: Se encarga de interconectar el subsistema horizontal de la planta con el subsistema vertical, de forma que todas las plantas puedan acceder al router que se encuentra en el distribuidor de planta.
  - Ventilador Rack.
  - Patch pannel de 24 puertos.
  - Un Switch de 24 puertos (en esta planta dispone de 20 tomas pero selecciona la siguiente para futuras ampliaciones)

El SCE (Subsistema de Cableado Estructurado) soportará prestaciones de enlace de categoría 6A.

**Una instalación de un sistema de cableado estructurado está formado por los siguientes elementos:**

□ **Subsistema horizontal.**

- Se extiende desde el repartidor de planta hasta las tomas de telecomunicaciones conectadas al mismo. Incluye:
  - Cableado de subsistema.
  - La terminación mecánica del cableado horizontal incluyendo las conexiones, tanto en la toma de telecomunicaciones como en el repartidor de planta junto con los latiguillos de parcheo y los puentes en dicho repartidor.
  - Las tomas de telecomunicaciones. Los latiguillos de equipo no se consideran parte del mismo.
- **El cableado horizontal:** se realiza en una sola tirada entre la toma de telecomunicaciones y el panel de conectores del armario repartidor de planta, estando prohibidos los puntos de transición, empalmes o inserción de dispositivos.

Para el subsistema horizontal se tiene que tener en cuenta la distancia más larga entre un repartidor de planta y la última roseta que no sobrepase los noventa metros de la normativa de categoría 6A. La instalación del cableado comenzará por la planta baja, canalizando todo el cableado con precaución, para no dañar ningún elemento del SCE. Los cables se organizarán en bridas, de la forma más ordenada posible, evitando el agrupamiento de cables excesivos, y por supuesto no usando bridas de plástico, ya que éstas presionan muy agresivamente los cables.

- Latiguillos serán utilizados para conectar todas las tomas ofimáticas a las rosetas dobles, así también, para las conexiones interiores en los armarios distribuidores. El cable utilizado es un cable SSTP de categoría 6A protegido por una cubierta de PVC.

#### □ **Subsistema troncal de edificio.**

- Se extiende desde el repartidor del edificio al repartidor de planta. Incluye:
  - El cableado del subsistema.
  - La terminación mecánica de los cables de la vertical del edificio, junto con los latiguillos de parcheo y puentes en el repartidor del edificio. Los latiguillos de equipo no se consideran parte del mismo.
  - Para realizar la instalación del subsistema vertical, se comienza desde la planta segunda y terminaremos en la planta baja, en el caso del edificio de Málaga desde la planta primera hasta la baja ya que es más sencillo hacer el subsistema vertical desde arriba hasta abajo, cableando también el servicio de telefonía básica y luego procederemos al cableado de datos.

#### □ **Subsistema de interconexión con proveedores de servicio.**

- Soporta las acometidas, cableado y equipamiento de los operadores de telecomunicaciones. Es el encargado de conducir hasta el armario principal de comunicaciones o repartidor de interconexión el cableado de cada uno de los proveedores, desde el punto de entrada que éste tenga en el edificio, así como, albergar el equipamiento del cliente, que posibilita el acceso a los servicios de telecomunicaciones.
  - Incorpora, por un lado, infraestructuras de conexión para accesos cableados a la red corporativa, dando lugar a instalaciones que conectan el repartidor de interconexión con la acometida exterior del edificio. Los criterios de dimensionado del repartidor de interconexión hacen referencia a las unidades de armario que tendrán que ser dedicadas a la funcionalidad, para albergar los equipos de red de los proveedores de servicio, como router, etc.
  - Este subsistema evita que tengan que realizarse nuevas instalaciones de tubos y canalizaciones para la provisión de servicio por parte de red corporativa.
  - Los requerimientos que afectan directamente a este subsistema que afectan a las características constructivas del inmueble son de aplicación para el caso de edificios de nueva construcción o grandes reformas.
- o Incluye:
- Las infraestructuras de enlace desde el exterior del edificio y la cubierta hasta el repartidor de interconexión.
  - El repartidor de interconexión, que provee del espacio necesario para alojar los equipos de cliente que instalarán los proveedores de red corporativa.

□ **Subsistema de distribución de Vídeo-Audio.**

- Se encarga de proveer las infraestructuras para dar soporte a la adaptación y distribución de señales de radio y televisión.
- Se instalará en aquellos edificios en los que se desee proporcionar señal audiovisual a tomas de usuario.
- Los requerimientos que afectan directamente a este subsistema que afectan a las características constructivas del inmueble son de aplicación para el caso de edificios de nueva construcción o grandes reformas.

□ **Subsistema de administración y gestión.**

- No está formado por elementos de la arquitectura del sistema de cableado estructurado.
- Es el conjunto de directrices que garantizan la óptima administración y gestión del sistema de cableado.

**Etiquetado y documentación del sistema:**

En el sistema de cableado estructurado, es necesario etiquetar todo el material que pueda causar confusión y permita facilitar el trabajo de una forma más eficaz y eficiente. Además, permitirá mantener ordenada de una forma lógica la instalación. La duración del etiquetado tiene que ser similar al del conexionado. Los elementos que deben ser etiquetados en un sistema de cableado estructurado son:

- Cableado horizontal y vertical. Como mínimo ambos extremos del cable, y si es posible en tramos regulares.
- Repartidores y switch.
- Rosetas o tomas de usuario.
- Espacios donde se localicen terminales.

**Diseño lógico de la red**

Una *VLAN*, acrónimo de virtual LAN (red de área local virtual), es un método para crear redes lógicas independientes dentro de una misma red física.

Una vez desarrollada todo el diseño de la infraestructura física, para el diseño de la infraestructura lógica he utilizado el programa Packet Tracer 8.0 en modo de estudiante para hacer el diseño de la infraestructura lógica.

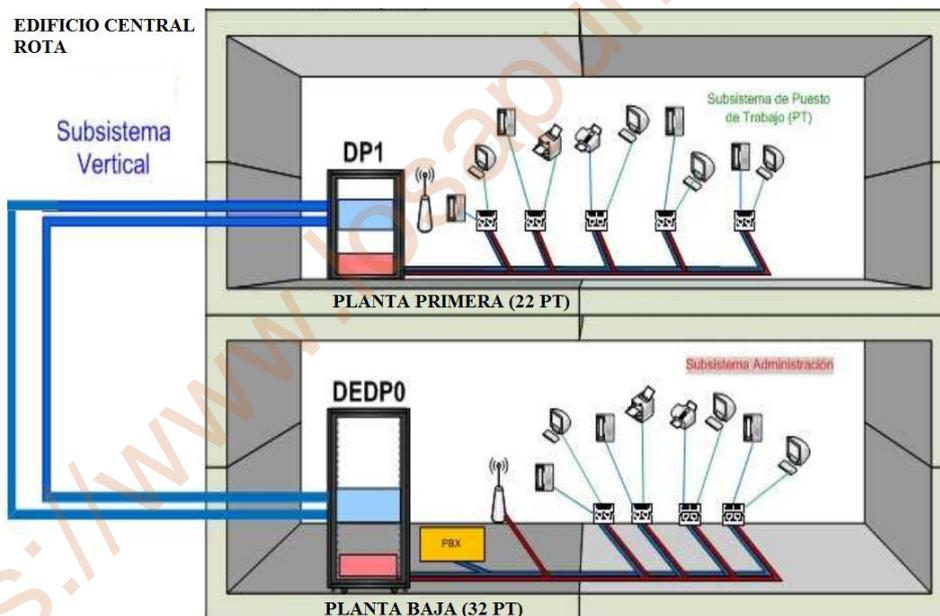
Se implementa en las oficinas Centrales en Rota con IP Privada de red 192.168.1.1 con puerto serial de acceso a la nube IP 10.0.0.1 y en la sucursal de Málaga con IP Privada de red 192.168.1.1 con puerto serial de acceso a la nube IP 10.0.0.2.

Se crean VLAN para diferenciar entre las jerarquías de los diversos departamentos en cada una de las plantas que componen tanto en Rota como en Málaga, permitiendo comunicarse a los departamentos de la misma jerarquía. Se habilita una conexión entre router y switch en modo TRUNK (TRONCAL), para soportar el tráfico de todas las VLAN que transiten por la misma.

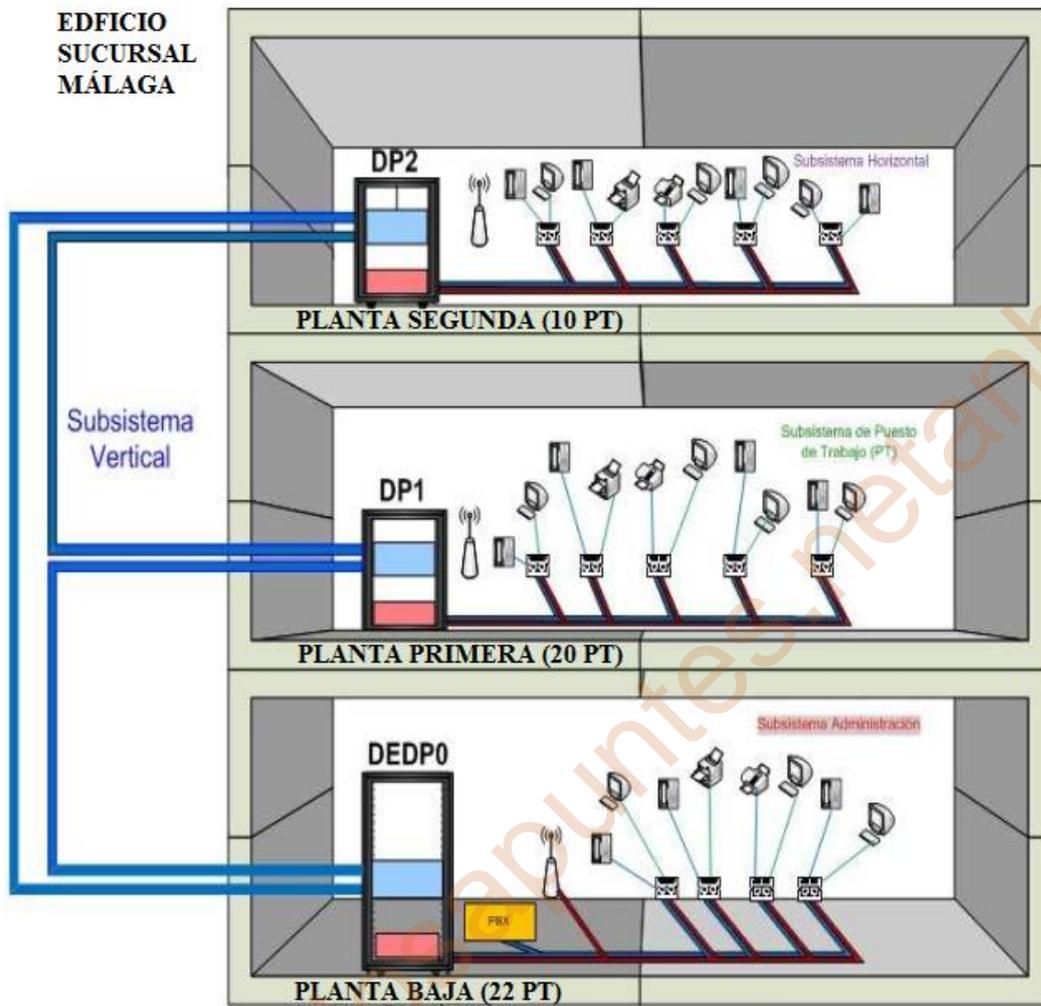
**Planos de Esquema lógico, sistema de cableado (vertical/horizontal):**



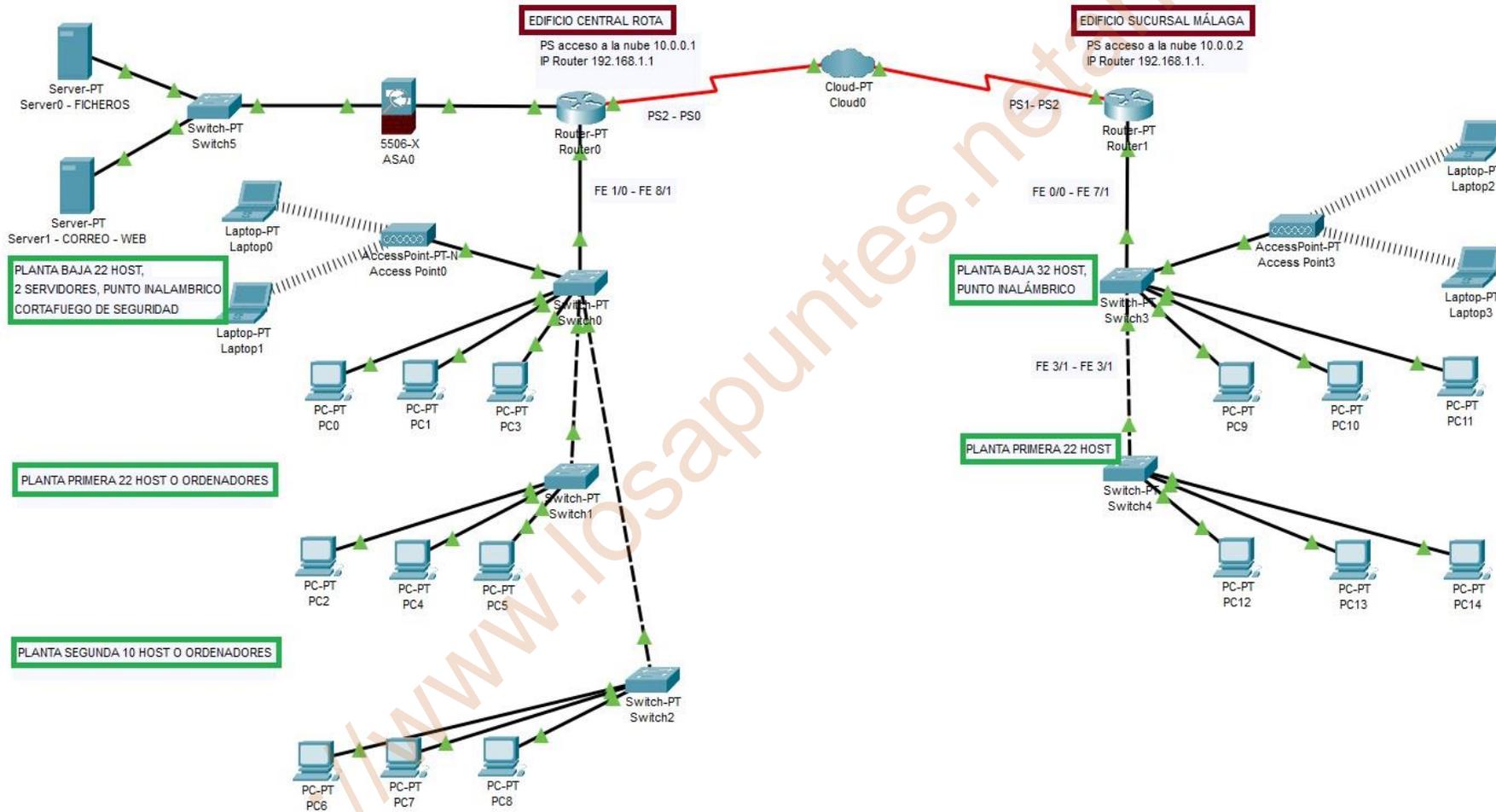
**Edificio Central Rota con planta baja + planta primera.**



Edificio Sucursal Málaga con planta baja + planta primera + planta segunda:



## Pano de diseño lógico de red.



## Tarea 1.6-Modelo OSI/TCP-IP

### Objetivos:

- Relacionar los dispositivos y la terminología con las diversas capas del modelo OSI
- Comparar las capas del modelo OSI con las del modelo TCP/IP
- Identificar las utilidades y los protocolos TCP/IP que operan en cada capa

### Información básica:

Esta práctica de laboratorio sirve como repaso para reforzar la comprensión de las siete capas del modelo OSI y su relación con el modelo TCP/IP. El enfoque se centra en los términos y dispositivos que se adecuan al modelo OSI. Esta práctica de laboratorio se puede organizar como una entretenida actividad competitiva de conocimiento.

### Paso 1 - El modelo OSI y las capas de pila de protocolo TCP/IP asociadas.

**Tarea:** Complete la siguiente tabla basándose en su conocimiento de los modelos OSI y TCP/IP.

**Explicación:** Su comprensión del modelo OSI y su relación con el modelo TCP/IP aumentará considerablemente su capacidad para incorporar y categorizar la información de networking a medida que la aprenda.

## El modelo OSI y la pila de protocolo TCP/IP

Nº de OSI o de capas OSI	Nombre de la capa OSI (y su función)	Nº de TCP/ IP	Nombre de la capa TCP/IP	Protocolos, estándares y utilidades en cada capa TCP/IP	Dispositivos y términos asociados con esta capa
7	NIVEL DE APLICACIÓN.	4 (es la capa 5, 6, y 7 de la OSI)	APLICACIONES Y SERVICIOS	HTTP, DNS, DHCP, FTP, telnet, e-mail	<p><u>Capa 7:</u> Esta es la capa que interactúa con el sistema operativo o aplicación cuando el usuario decide transferir archivos, leer mensajes, o realizar otras actividades de red. Por ello, en esta capa se incluyen tecnologías tales como http, DNS, SMTP, SSH, Telnet, etc.</p>
6	NIVEL DE PRESENTACIÓN				<p><u>Capa 6:</u> Esta capa tiene la misión de coger los datos que han sido entregados por la capa de aplicación, y convertirlos en un formato estándar que otras capas puedan entender. En esta capa tenemos como ejemplo los formatos MP3, MPG, GIF, etc.</p>
5	NIVEL DE SESIÓN				<p><u>Capa 5:</u> La capa de sesión establece, administra y termina las sesiones entre las aplicaciones. Esto incluye el inicio, la terminación y la resincronización de dos ordenadores que están manteniendo una sesión; La capa de sesión coordina las aplicaciones mientras interactúan en dos hosts que se comunican entre sí.</p>
4	NIVEL DE TRANSPORTE	3 (es la capa 4 de la OSI)	TRANSPORTE	TCP, UDP	<p><u>Capa 4:</u> Permite asegurar que los datos lleguen correctamente de un extremo a otro de la comunicación al nivel de sesión. Para ello establece mecanismos fiables para el intercambio de datos, realizando servicios de detección de errores. Además el nivel de transporte será el encargado de recomponer la información, eliminando las tramas repetidas y colocándolas en el orden correcto.</p>
3	NIVEL DE RED	2 (es la capa 3 de la OSI)	INTERNET	IPv4, IPv6, ICMPv4, ICMPv6	<p><u>Capa 3:</u> Se ocupa de determinar cuál es el mejor camino para enviar información entre el origen y el destino, pudiendo pasar por tantas redes intermedias como sea necesario. Es en este nivel de red donde los datos se fragmentan en paquetes, enviándose cada uno de ellos de forma independiente. <u>ROUTER</u></p>
2	NIVEL DE ENLACE DE DATOS	1 (es la capa 1 y 2 de la OSI)	ACCESO A LA RED	PPP, retransmisión de tramas, Ethernet	<p><u>Capa 2:</u> Tarjeta de interfaz de red (NIC) de Ethernet, que se inserta dentro del bus del sistema de un ordenador, <u>Dirección física</u> o MAC - SWITCH.</p>
1	NIVEL FISICA				<p><u>Capa 1:</u> A través de cable (coaxial, par trenzado, fibra óptica), hubs, el medio inalámbricos que utilizamos</p>

## GLOSARIO DE CADA UNA DE LAS CAPAS

**HTTP:** *Hypertext Transfer Protocol (HTTP)* (o *Protocolo de Transferencia de Hipertexto en español*) es un protocolo de la capa de aplicación para la transmisión de documentos hipermedia, como HTML. Fue diseñado para la comunicación entre los navegadores y servidores web, aunque puede ser utilizado para otros propósitos también. Sigue el clásico modelo cliente-servidor, en el que un cliente establece una conexión, realizando una petición a un servidor y espera una respuesta del mismo. Se trata de un protocolo sin estado, lo que significa que el servidor no guarda ningún dato (estado) entre dos peticiones. Aunque en la mayoría de casos se basa en una conexión del tipo TCP/IP, puede ser usado sobre cualquier capa de transporte segura o de confianza, es decir, sobre cualquier protocolo que no pierda mensajes silenciosamente, tal como UDP.

**DNS:** o sistema de nombres de dominio, traduce los nombres de dominios aptos para lectura humana (por ejemplo, www.amazon.com) a direcciones IP aptas para lectura por parte de máquinas de servidores (por ejemplo, 192.0.2.44).

**DHCP:** El Protocolo de configuración dinámica de host (DHCP) es un protocolo cliente/servidor que proporciona automáticamente un host de Protocolo de Internet (IP) con su dirección IP y otra información de configuración relacionada, como la máscara de subred y la puerta de enlace predeterminada. Las RFC 2131 y 2132 definen DHCP como un estándar de Internet Engineering Task Force (IETF) basado en el Protocolo de arranque (BOOTP), un protocolo con el que DHCP comparte muchos detalles de implementación. DHCP permite a los hosts obtener la información de configuración de TCP/IP necesaria de un servidor DHCP.

Todos los dispositivos de una red basada en TCP/IP deben tener una dirección IP de unidifusión única para acceder a la red y sus recursos. Sin DHCP, las direcciones IP de los equipos nuevos que se mueven de una subred a otra deben configurarse manualmente. Las direcciones IP de los equipos que se quitan de la red deben reclamarse manualmente.

Con DHCP, todo este proceso se automatiza y administra de forma centralizada. El servidor DHCP mantiene un grupo de direcciones IP y concede una dirección a cualquier cliente habilitado para DHCP cuando se inicia en la red. Dado que las direcciones IP son dinámicas (concesionadas) en lugar de estáticas (asignadas permanentemente), las direcciones que ya no están en uso se devuelven automáticamente al grupo para su reasignación.

**FTP:** Las siglas de FTP significan *File Transfer Protocol*, que se traduce como *Protocolo de Transferencia de Archivos*. Se trata de un protocolo que **permite transferir archivos directamente de un dispositivo a otro**. Actualmente, es un protocolo que poco a poco va abandonándose, pero ha estado vigente más de 50 años.

El protocolo FTP se empezó a utilizar en abril de 1971, y terminó de definir su estructura en el 73, aunque durante las décadas de los 70 y los 80 del siglo pasado fue perfeccionándose. **Este protocolo nació antes de que existieran Internet o el correo electrónico**, ya que fue uno de los componentes básicos de ARPANET, que fue esa red primigenia que luego dio lugar a Internet.

Este protocolo funciona entre ordenadores que estén conectados a una red TCP, que significa *Transmission Control Protocol* o Protocolo de control de transmisión. Este protocolo TCP da soporte a muchas tecnologías, entre ellas a Internet. La familia de protocolos que forman Internet se llama TCP/IP.

El protocolo FTP tal cual es un protocolo inseguro, ya que su información no viaja cifrada. Sin embargo, en 2001 esto se solucionó con el protocolo FTPS, que le añade una capa SSH para hacerlo más seguro y privado.

El FTP es un protocolo muy útil para el envío de archivos, ya que te permite enviarlos de un equipo a otro a gran velocidad de transferencia, y no hay ningún tipo de límites de tamaño como puede pasar en la descarga directa. También suele utilizarse en contextos como la creación de webs, pudiendo enviar por FTP los ficheros de una web al servidor donde están.

**telnet:** es un protocolo que se concibió para interactuar con ordenadores a distancia. La palabra “Telnet” se refiere también a la utilidad de línea de comando “telnet” que existe para el sistema operativo de Windows y sistemas similares a Unix, entre los que se encuentran Mac, Linux y otros. Telnet permite a sus usuarios comprobar la conectividad a máquinas remotas y enviar comandos a través de un teclado. A pesar de que la mayoría de los usuarios se deciden por utilizar interfaces gráficas, Telnet es una de las maneras más sencillas de comprobar la conectividad en ciertos puertos.

**TCP (Transmisión Control Protocol):** El protocolo TCP es un acuerdo estandarizado de transmisión de datos entre distintos participantes de una red informática. El estado actual de desarrollo del protocolo TCP (Protocolo de Control de Transmisión) permite establecer una conexión entre dos puntos terminales en una red informática común que posibilite un **intercambio mutuo de datos**. En este proceso, cualquier pérdida de datos se detecta y resuelve, por lo que se considera un **protocolo fiable**. Dentro de la familia de protocolos de Internet, el TCP, junto con el UDP y el SCTP forma el grupo de los protocolos de transporte, que, según el modelo OSI, se ubican en la capa de transporte dentro de la arquitectura de red. Como el protocolo TCP se combina casi en todos los casos con el protocolo de Internet (IP) y esta conexión forma la base de la gran mayoría de redes locales y servicios de red, es común hablar del **conjunto de protocolos TCP/IP**, aunque en realidad se haga referencia a la familia de protocolos de Internet.

El protocolo de control de transmisión permite **la transmisión de información en ambas direcciones**. Por lo tanto, los sistemas informáticos que se comunican mediante TCP pueden enviar y recibir datos de forma simultánea, como si se tratase de una llamada telefónica. En este contexto, las unidades de transmisión básicas de las que echa mano el protocolo son segmentos (paquetes) que, aparte de los datos de uso, también pueden contener información de control y están limitados a un tamaño de

1500 bytes. El establecimiento y la interrupción de las conexiones, que se pueden catalogar como conexiones de terminal a terminal, así como la transmisión de datos en sí, la realiza el **software TCP** en la pila de protocolos de red del sistema operativo correspondiente.

El software TCP se activa mediante distintas aplicaciones de red, como los navegadores de red o los servidores, a través de **interfaces específicas**. Cada conexión se debe identificar siempre claramente mediante dos puntos terminales definidos (cliente y servidor). En este contexto, qué lado desempeña el papel de cliente y cuál el de servidor es indiferente. Lo que importa es que el software TCP cuente con una **pareja ordenada** de dirección IP y puerto (también denominada “2-tupla” o “socket”) en cada punto terminal.

**UDP (User Datagram Protocol):** El **Protocolo de datagrama de usuario (UDP)** es un protocolo ligero de transporte de datos que funciona sobre IP.

UDP proporciona un mecanismo para detectar datos corruptos en paquetes, pero *no* intenta resolver otros problemas que surgen con paquetes, como cuando se pierden o llegan fuera de orden. Por eso, a veces UDP es conocido como el **protocolo de datos no confiable**.

UDP es simple pero rápido, al menos en comparación con otros protocolos que funcionan sobre IP. A menudo se usa para aplicaciones sensibles al tiempo (como "streaming" de vídeo en tiempo real) donde la velocidad es más importante que la precisión.

**IP:** Abreviatura de **Internet Protocol**, es un protocolo que ayuda a los ordenadores/dispositivos a comunicarse entre sí a través de una red. Como la «v» del nombre sugiere, hay diferentes versiones del Protocolo de Internet: **IPv4 e IPv6**.

El Protocolo de Internet (IP) es un conjunto de reglas que ayudan a enrutar los paquetes de datos para que estos puedan desplazarse a través de las redes y llegar al destino correcto.

Cuando un ordenador trata de enviar información, esta se descompone en trozos más pequeños, llamados paquetes. Para asegurarse de que todos estos paquetes lleguen al lugar correcto, cada paquete incluye información de IP.

La otra parte del rompecabezas es que a cada dispositivo o **dominio** de Internet se le asigna una dirección IP que lo identifica de manera única de otros dispositivos.

Esta versión 6 del protocolo de Internet incrementa el tamaño de la dirección IP de 32 a 128 bits, eliminando las limitaciones actuales y con pequeñas diferencias entre el protocolo **IPv6** de **IPv4**: la nueva versión tiene mayor flexibilidad y ofrece más seguridad en la autenticación y la confidencialidad.

**ICMP:** El segundo protocolo a nivel de red es el **ICMP (Internet Control Message Protocol - Protocolo de mensajes de control de Internet)**. **ICMP** es una parte necesaria de cada implementación de **IP**. **ICMP** maneja los mensajes de error y control para **IP**. Es considerado como parte de la capa de red IP. **ICMP** es un protocolo empleado por los routers (encaminadores) y por los hosts (clientes, servidores, etc) para comunicar la información de control o de error de la red.

Además de los fallos en las líneas de comunicación, IP tiene fallos en la entrega de datagramas cuando la máquina destino está desconectada, cuando el tiempo de vida se acaba o cuando existe congestión en los encaminadores. El protocolo IP no puede controlar estas situaciones y los diseñadores de TCP/IP crearon ICMP como mecanismo de informe de errores y/o situaciones anómalas en la red. Una consideración a tener en cuenta es que ICMP informa de errores, pero no los corrige.

Los mensajes de ICMP no son obligatorios y, a menudo, no se permiten dentro de una red por razones de seguridad. El protocolo ICMP está disponible tanto para IPv4 como para IPv6. El protocolo de mensajes para IPv4 es **ICMPv4**. **ICMPv6** proporciona estos mismos servicios para IPv6, pero incluye funcionalidad adicional.

Existe una gran variedad de tipos de mensajes de ICMP y de razones para enviarlos. Analizaremos algunos de los mensajes más comunes.

Los mensajes ICMP comunes a ICMPv4 y a ICMPv6 incluyen lo siguiente: Confirmación de host, Destino o servicio inaccesible, Tiempo superado, Redireccionamiento de ruta, Confirmación de host.

**PPP:** La encapsulación PPP (Protocolo Punto a Punto) se diseñó cuidadosamente para conservar la compatibilidad con el hardware más usado que la admite. PPP encapsula tramas de datos para transmitirlos a través de enlaces físicos de capa 2. PPP establece una conexión directa mediante cables seriales, líneas telefónicas, líneas troncales, teléfonos celulares, enlaces de radio especializados o enlaces de fibra óptica.

**Ethernet** es la tecnología tradicional para conectar dispositivos en una red de área local (LAN) o una red de área amplia (WAN) por cable, lo que les permite comunicarse entre sí a través de un protocolo: un conjunto de reglas o lenguaje de red común. Ethernet describe cómo los dispositivos de red pueden formatear y transmitir datos para que otros dispositivos del mismo segmento de red de área local o de campus puedan reconocer, recibir y procesar la información. Un cable Ethernet es el cableado físico, encapsulado, por el que viajan los datos.

## **WEBGRAFÍA**

### **Tarea 1.1-Comunicación entre ordenadores**

<https://www.cavsi.com/preguntasrespuestas/como-se-realiza-la-comunicacion-entre-computadoras/>

<https://prezi.com/llvzmjzctsob/las-computadoras-se-comunican-entre-si-mediante-lenguajes-ii/>

<https://tododeredes.com/modelo-osi/capa-2/>

[https://prezi.com/qv8clvohyj\\_k/capa-de-sesion/](https://prezi.com/qv8clvohyj_k/capa-de-sesion/)

### **Tarea 1.2-CMD**

<https://www.seabrookewindows.com/dwPyRNmQp/>

<https://www.youtube.com/watch?v=fFnojenaWFg>

[https://cincodias.elpais.com/cincodias/2019/10/16/lifestyle/1571221957\\_521769.html](https://cincodias.elpais.com/cincodias/2019/10/16/lifestyle/1571221957_521769.html)

<https://www.youtube.com/watch?v=nIQ774mJWiU>

<https://www.youtube.com/watch?v=iA6SGq4Ro4M>

### **Tarea 1.3- Tipos de redes**

1)

<https://sites.google.com/site/inforbasicaguadalajara/temario/hardware/perifericos/perifericos-de-red>

<https://www.ejemplos.co/10-ejemplos-de-perifericos-de-comunicacion/>

4)

<https://blog.desdelinux.net/servidores-web-mejores-programas-libres-abiertos/>

<https://www.monografias.com/docs114/telecomunicaciones-arquitectura-cliente-servidor/telecomunicaciones-arquitectura-cliente-servidor.shtml>

5)

<https://www.paessler.com/es/it-explained/server>

6)

[https://blog.infranetworking.com/caracteristicas-servidor-web/#Caracteristicas de un servidor web a nivel de hardware](https://blog.infranetworking.com/caracteristicas-servidor-web/#Caracteristicas_de_un_servidor_web_a_nivel_de_hardware)

7)

<https://es.slideshare.net/luzdarysaenzquiroyga/google-y-sus-servidores-31914529>

<https://como-funciona.com/el-balanceo-de-carga/>

<https://blogs.masterhacks.net/geek/interesante/que-es-un-balanceador-de-carga/>

<http://administracionycentrosdecomputo.blogspot.com/2012/10/balanceo-de-carga.html>

<https://support.google.com/google-ads/answer/1752334?hl=es>

[https://es.wikipedia.org/wiki/Plataforma de Google](https://es.wikipedia.org/wiki/Plataforma_de_Google)

8)

<https://www.softonic.com/articulos/mejores-programas-p2p>

[https://es.wikipedia.org/wiki/Peer-to-peer#Controversia legal](https://es.wikipedia.org/wiki/Peer-to-peer#Controversia_legal)

<https://www.xataka.com/legislacion-y-derechos/descargar-archivos-p2p-no-es-delito-y-aunque-pueda-ser-una-infraccion-civil-es-improbable-que-te-demanden>

<https://www.europapress.es/portaltic/internet/noticia-conexion-p2p-utiliza-pirateria-20170420085940.html>

#### **Tarea 1.4-Topologías**

1)

<https://sites.google.com/site/605bredesdecomputadoras/home/6>

<https://docs.google.com/document/edit?id=1AC1mHzAA-D-Px3i31qwiwzq3H9wcO0fIQZMwpWaVEo&hl=es>

<https://sites.google.com/site/tecnocompu32/home/topologias-de-red>

[https://es.wikipedia.org/wiki/Topolog%C3%ADa de red#Red en %C3%A1rbol](https://es.wikipedia.org/wiki/Topolog%C3%ADa_de_red#Red_en_%C3%A1rbol)

<https://apuntesjulio.com/topologias-de-red/> (ventajas y desventajas)

<https://sites.google.com/site/estandaresred/tipos-de-red/topologias-de-red>

<https://www.lifeder.com/topologia-mixta/> (tipología mixta)

<https://ocw.unican.es/pluginfile.php/1357/course/section/1682/Tema%200.pdf>  
(Protocolo interconexión de redes)

4)

<https://comofriki.com/comando-ipconfig-con-ejemplos/>

<https://es.wikipedia.org/wiki/Ipconfig>

<https://computerhoy.com/noticias/internet/que-es-comando-ping-como-funciona-42607>

<https://www.xataka.com/basics/tracert-traceroute-que-como-funciona-como-se-utiliza>

<https://support.microsoft.com/es-es/topic/c%C3%B3mo-usar-tracert-para-solucionar-problemas-de-tcp-ip-en-windows-e643d72b-2f4f-cdd6-09a0-fd2989c7ca8e>

<https://www.mundiserver.com/como-hacer-ping-tracert/>

5)

<https://aprendederedes.com/fragmentacion-ip/>

<https://www.pedrocarrasco.org/fragmentacion-ip/>

[https://es.wikipedia.org/wiki/Fragmentaci%C3%B3n\\_IP](https://es.wikipedia.org/wiki/Fragmentaci%C3%B3n_IP)

6)

<http://enredate602.blogspot.com/2011/03/redes-de-difusion-y-redes-punto-punto.html>

7)

[https://es.wikipedia.org/wiki/Conmutaci%C3%B3n\\_\(redes\\_de\\_comunicaci%C3%B3n\)#Ventajas\\_3](https://es.wikipedia.org/wiki/Conmutaci%C3%B3n_(redes_de_comunicaci%C3%B3n)#Ventajas_3)

<https://dementium2.com/administrador-neto/conmutacion-de-circuitos-vs-conmutacion-de/>

<https://zimbronapps.com/educacion/sistemas-computacionales/telecomunicaciones/conmutacion-paquetes-mensajes/>

<https://zimbronapps.com/educacion/sistemas-computacionales/telecomunicaciones/conmutacion-paquetes-mensajes/>

### **Tarea 1.5-Conexión entre dos empresas**

<http://elcuandernodedaniel.blogspot.com/2018/10/taller-redes.html>

[https://repository.ucc.edu.co/bitstream/20.500.12494/7048/6/2018\\_Dise%C3%B1o\\_Red\\_Lan.pdf](https://repository.ucc.edu.co/bitstream/20.500.12494/7048/6/2018_Dise%C3%B1o_Red_Lan.pdf)

<https://repository.ucc.edu.co/bitstream/20.500.12494/13003/1/2016-Dise%C3%B1o-%20Red-Intel..pdf>

<http://openaccess.uoc.edu/webapps/o2/bitstream/10609/28625/6/aobisTFC0114memoria.pdf>

[https://oa.upm.es/54288/1/TFG\\_PABLO\\_TRUJILLO\\_DIEZ.pdf](https://oa.upm.es/54288/1/TFG_PABLO_TRUJILLO_DIEZ.pdf)

[https://riunet.upv.es/bitstream/handle/10251/125775/Vivas%20-%20Dise%C3%B1o,%20desarrollo%20e%20implementaci%C3%B3n%20de%20una%20red%20de%20%C3%A1rea%20local%20\(LAN\)%20en%20GA-Autotrim.pdf?sequence=1](https://riunet.upv.es/bitstream/handle/10251/125775/Vivas%20-%20Dise%C3%B1o,%20desarrollo%20e%20implementaci%C3%B3n%20de%20una%20red%20de%20%C3%A1rea%20local%20(LAN)%20en%20GA-Autotrim.pdf?sequence=1)

[https://e-archivo.uc3m.es/bitstream/handle/10016/26135/PFC\\_Raul\\_Duran\\_Nieto.pdf](https://e-archivo.uc3m.es/bitstream/handle/10016/26135/PFC_Raul_Duran_Nieto.pdf)

### **Tarea 1.6-Modelo OSI/TCP-IP**

<https://aws.amazon.com/es/route53/what-is-dns/>

<https://docs.microsoft.com/es-es/windows-server/networking/technologies/dhcp/dhcp-top>

<https://www.dropbox.com/es/business/resources/what-is-ftp>

<https://www.ionos.mx/digitalguide/servidores/know-how/que-es-tcp-transport-control-protocol/>

<https://es.khanacademy.org/computing/ap-computer-science-principles/the-internet/x2d2f703b37b450a3:transporting-packets/a/user-datagram-protocol-udp>

<https://interpolados.wordpress.com/2017/03/26/icmpv4-e-icmpv6/>

<https://ccnadesdecero.es/funcionamiento-ppp-protocolo-punto-a-punto/>