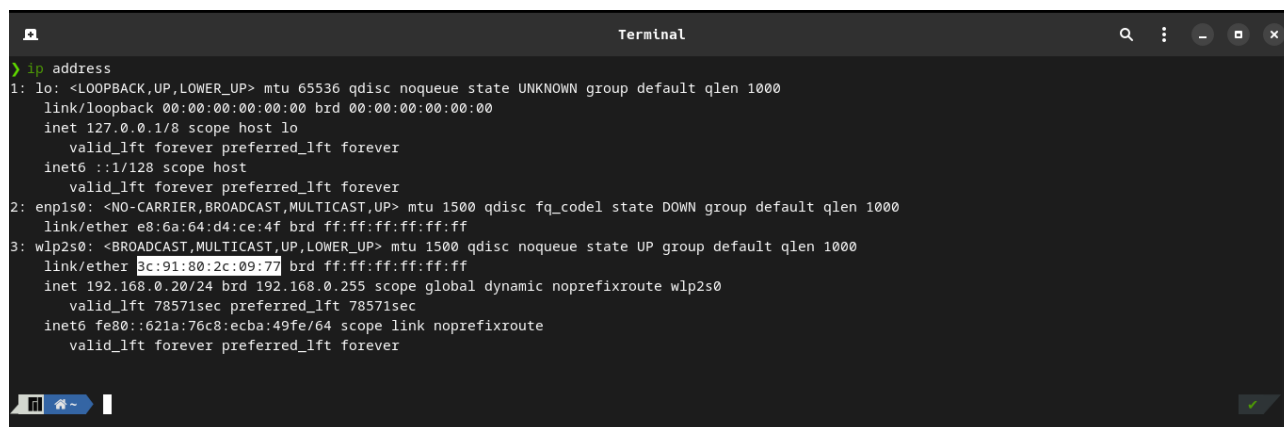


**Ejercicio 1: Direcciones MAC.** Obtén la dirección MAC del equipo que usas habitualmente. Recuerda usar tu MAC real, no las posibles MAC virtuales de máquinas virtuales creadas por programas como VirtualBox o VMware. Adjunta una captura de la pantalla donde hayas obtenido las respuestas (bien sea por comando o de manera gráfica).



```
Terminal
> ip address
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp1s0: <NO-CARRIER,BROADCAST,MULTICAST,UP> mtu 1500 qdisc fq_codel state DOWN group default qlen 1000
    link/ether e8:6a:64:d4:ce:4f brd ff:ff:ff:ff:ff:ff
3: wlp2s0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 3c:91:80:2c:09:77 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.20/24 brd 192.168.0.255 scope global dynamic noprefixroute wlp2s0
        valid_lft 78571sec preferred_lft 78571sec
    inet6 fe80::621a:76c8:ecba:49fe/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
```

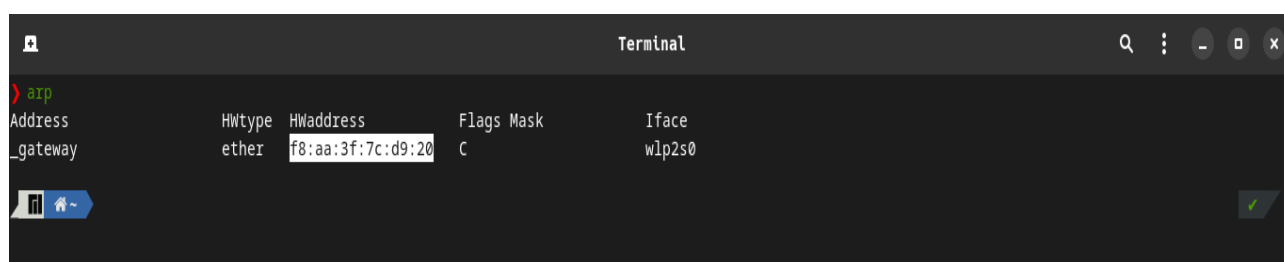
- Mi dirección MAC es: 3c:91:80:2c:09:77
- La longitud de la dirección MAC es 6 bytes y 48 bits
- El OUI de la dirección MAC es: 3c:91:80

Averigua también la dirección IP de tu router. Como el router es la puerta de enlace, la dirección IP del router será la dirección que aparece como puerta de enlace o gateway predeterminado en cualquier equipo conectado a la red. Adjunta un pantallazo.

Lo he sacado de la misma imagen de pregunta anterior.

- La dirección IP del router es: 192.168.0.20
- Mi dirección IP es: 127.0.0.1

Sabiendo la IP del router, consulta la caché ARP de tu equipo y anota la dirección MAC de tu router. Adjunta un pantallazo.



```
Terminal
> arp
Address      Hwtype  Hwaddress      Flags Mask      Iface
_gateway     ether   f8:aa:3f:7c:d9:20 C                wlp2s0
```

- La dirección MAC del router es: f8:aa:3f:7c:d9:20
- Su OUI es: f8:aa:3f

(Como actividad complementaria, puedes averiguar también la MAC de tu móvil buscando en los Ajustes, así como la IP de tu móvil y la IP de la puerta de enlace que usa)

**Ejercicio 2: Cabecera Ethernet.** Utilizando los datos del ejercicio anterior, escribe en hexadecimal el contenido de cada cabecera Ethernet que se te pide:

- Cabecera Ethernet de un paquete enviado por tu equipo solicitando ver [www.google.es](http://www.google.es):

<i>MAC destino (6)</i> f8:aa:3f:7c:d9:20	<i>MAC origen(6)</i> 3c:91:80:2c:09:77	<i>Tipo (2)</i> 0x0800
---------------------------------------------	-------------------------------------------	---------------------------

- Cabecera Ethernet de un paquete broadcast enviado por tu equipo:

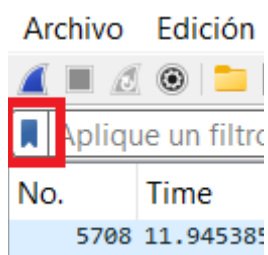
<i>MAC destino (6)</i> ff:ff:ff:ff:ff:ff	<i>MAC origen (6)</i> 3c:91:80:2c:09:77	<i>Tipo (2)</i> 0x0800
---------------------------------------------	--------------------------------------------	---------------------------

### Ejercicio 3. Práctica: Filtros en Wireshark.

(Realiza primero una captura con Wireshark durante unos instantes para poder trabajar con varios paquetes a lo largo de esta sección. No olvides detener la captura)

El listado de paquetes de Wireshark (zona superior) muestra siempre los paquetes capturados, tanto los enviados como los recibidos. En ocasiones es preferible que se muestren solamente los paquetes que cumplan ciertas condiciones. Para conseguir esto, lo que se hace es seleccionar un filtro y aplicarlo, para visualizar únicamente los paquetes que cumplan las condiciones especificadas en el filtro. Tenemos dos maneras de trabajar con filtros: usando algún filtro que Wireshark proporcione por defecto (apartado a) o escribir nuestro propio filtro (apartado c).

a) **Filtros predefinidos.** Para ver los filtros por defecto que tiene Wireshark deberás hacer clic aquí:



Cada filtro tiene dos partes: un texto descriptivo y el filtro en sí.

```
Ethernet address 00:00:5e:00:53:00: eth.addr == 00:00:5e:00:53:00
Ethernet type 0x0806 (ARP): eth.type == 0x0806
Ethernet broadcast: eth.addr == ff:ff:ff:ff:ff:ff
No ARP: not arp
IPv4 only: ip
```

Selecciona el filtro con el nombre “Ethernet broadcast” para que te muestre únicamente los paquetes Ethernet enviados por difusión. Al aplicar el filtro, verás que se muestran solamente aquellos paquetes cuya MAC destino es FF:FF:FF:FF:FF:FF. Compruébalo, seleccionando alguno de los paquetes que se muestran, e inspeccionando la dirección destino de la cabecera Ethernet.

Para dejar de aplicar un filtro y que vuelvan a aparecer de nuevo todos los paquetes capturados, haz clic en el siguiente botón, situado en la zona superior derecha de la pantalla:



Rellena la siguiente tabla inspeccionando la lista de filtros por defecto de Wireshark:

Condición	Nombre del filtro	Filtro
Mostrar paquetes de difusión	Ethernet broadcast	eth.addr == ff: ff: ff: ff: ff: ff
Mostrar paquetes TCP	TCP only	tcp
Mostrar paquetes IPv6	IPv6 only	ipv6
Mostrar paquetes ARP	ARP	arp
Mostrar paquetes que usen el puerto 80	TCP or UDP port is 80 (HTTP)	tcp.port == 80    udp.port == 80

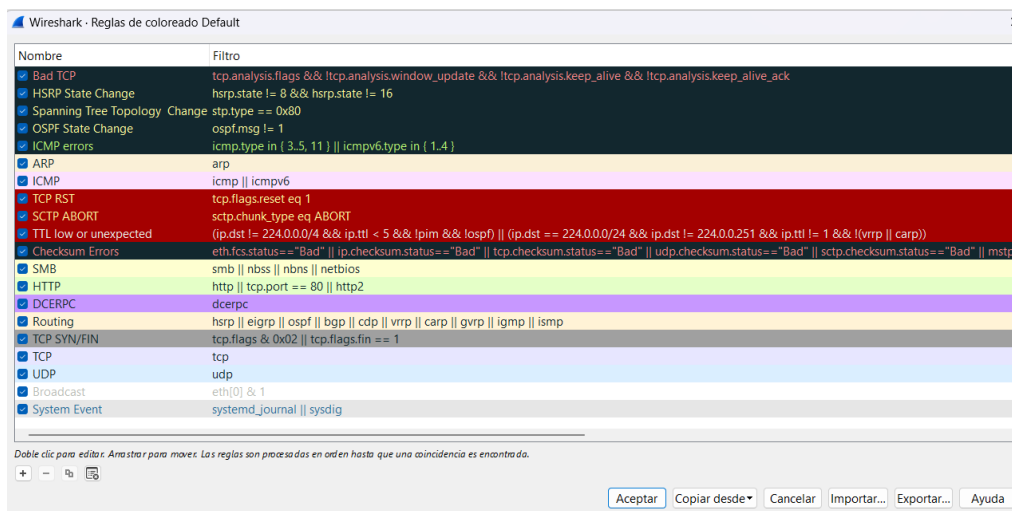
Los filtros por defecto se pueden gestionar en el menú Analizar, Mostrar filtros. Ahí podemos añadir o eliminar filtros de la lista por defecto con los botones + y -, o editar un filtro existente haciendo doble clic en la zona que queramos cambiar. Por ejemplo, cambia el nombre del filtro para mostrar los paquetes por difusión para que a partir de ahora se llame “Paquetes de difusión Ethernet”.

Los filtros son muy útiles en Wireshark ya que permiten mostrar los paquetes realmente necesarios, y no todos. De hecho, no es necesario que primero captures y cuando hayas detenido la captura apliques un filtro. Puede aplicarse un filtro directamente antes de capturar, para que solo se capturen directamente los paquetes que tú especifiques, y no todo lo que pase por la tarjeta de red. Para ello, hay que ir a las Opciones de la captura (cuarto botón de la barra superior) y seleccionar el filtro:



No es necesario que lo uses en esta práctica, aunque en posteriores unidades puede ser útil que lo apliques.

b) **Reglas de coloreado.** Como sabes, el listado de paquetes muestra los paquetes con colores diferentes dependiendo del tipo de paquete que sea (TCP, UDP, DNS, etc). Esto es así porque Wireshark tiene asociadas combinaciones de colores con filtros. De este modo, a todos los paquetes que cumplen un filtro se les aplica una regla de coloreado. Puedes ver las reglas de coloreado existentes en el menú Visualización, Reglas de coloreado.



Como ves, cada combinación de colores va asociada a un nombre y a un filtro. Desde esta pantalla podemos realizar varias opciones:

- Marcar/desmarcar los filtros que queremos que se apliquen o no.
- Editar el nombre, el filtro o los colores de texto y fondo de cada regla.
- Arrastrar una regla de coloreado para cambiar su posición. El orden de las reglas es especialmente importante, ya que las reglas se aplican de arriba a abajo, y en cuanto se cumple una, se aplica su coloreado y Wireshark ya no comprobará las inferiores. Por eso los errores, que aparecen con fondo negro, están en las primeras posiciones, para que se coloreen de manera destacada antes que ningún otro paquete.
- Añadir o eliminar reglas con los botones + y -.
- Importar o exportar un fichero con reglas de coloreado para poder aplicar los mismos colores personalizados en diferentes equipos que tengan Wireshark instalado.

Prueba a cambiar la regla que colorea en azul los paquetes TCP para que los coloree en naranja a partir de ahora. Comprueba qué sucede en el listado de paquetes.

Recuerda que hay un botón en la barra de herramientas para que aplique o no las reglas de coloreado.

c) **Creación de filtros.** Si ninguno de los filtros que provee Wireshark se ajusta a lo que quieres ver, puedes crear tu propio filtro escribiéndolo directamente en la barra de filtros:



Para especificar un filtro, Wireshark sigue un formato concreto. Y ese formato está directamente relacionado con los contenidos de las cabeceras de cada paquete, de ahí la importancia de conocer protocolos, cabeceras y campos. En esta unidad has aprendido qué contiene exactamente una cabecera Ethernet, y son los siguientes 3 campos y en este orden: MAC destino, MAC origen y tipo.

Para escribir filtros, el formato general es el siguiente:

cabecera.campo operador valor

- Las **cabeceras** son los nombres que Wireshark le da a los protocolos: eth para la cabecera Ethernet, ip para IPv4, ipv6 para IPv6, etc. Si no conoces exactamente alguno, puedes escribir su inicio en la barra de filtros y Wireshark irá completando el nombre.
- Los **campos** son las secciones dentro de cada cabecera, y de nuevo reciben un nombre muy parecido a aquello que representan. Por ejemplo, en la cabecera Ethernet el campo con la MAC destino se llama dst, para la MAC origen tenemos src, y para el tipo está type. El campo va separado de la cabecera por un punto para indicar que ese campo está dentro de la cabecera especificada.
- El **operador** representa qué condición queremos expresar. Solo aquellos paquetes que cumplan la condición del filtro serán mostrados cuando éste se aplique. Los operadores principales son: == (igual), != (diferente), < (menor que), > (mayor que), <= (menor o igual que), >= (mayor o igual que).
- Finalmente, el **valor** indica el número concreto que queremos buscar. Puede ser una longitud, una dirección, un n.º de puerto, etc.

Veamos todo esto con un ejemplo:

```
eth.dst==11:33:e2:00:23:5a
```

En este filtro, la cabecera es eth, el campo es dst, el operador es == y el valor es 11:33:e2:00:23:5a. Este filtro seleccionará aquellos paquetes cuya MAC destino dentro de la cabecera Ethernet sea exactamente igual a la dirección 11:33:e2:00:23:5a.

Si escribimos mal un filtro, o nos dejamos un símbolo, Wireshark nos avisará poniendo el fondo del filtro en rojo, y no nos dejará aplicarlo hasta que sea correcto y aparezca en verde. Tanto para los nombres de protocolo como para los nombres de campo, Wireshark nos muestra sugerencias a medida que los vamos escribiendo.

Aquí tienes otro ejemplo de filtro:

```
eth.type==0x0800
```

Con este filtro, se mostrarán todos los paquetes que tengan en el campo tipo de la cabecera Ethernet el valor 800 (se añade 0x porque es un número hexadecimal), que corresponde al código numérico para IPv4. En resumen, ese filtro muestra los paquetes IPv4.

Varios filtros sencillos pueden combinarse para crear filtros más complejos intercalando los operadores && (and) y || (or) entre dos filtros simples. Por ejemplo, si unimos los dos filtros anteriores con el operador and...

```
eth.dst==11:33:e2:00:23:5a && eth.type==0x0800
```

...tendremos un filtro que selecciona aquellos paquetes que cumplen la primera condición y que también cumplen a la vez la segunda.

Wireshark proporciona mucha ayuda a la hora de elaborar filtros, hasta el punto de que sugiere el uso de campos que no están realmente incluidos en las cabeceras, pero que puede ser útil que los usemos. Por ejemplo, en la cabecera Ethernet no existe un campo que nos indique la longitud del paquete, pero Wireshark permite usar `eth.len` para hacer referencia al tamaño. También existe `eth.addr` para hacer referencia a una MAC sin importarnos si está como origen o como destino.

Ayudándote de los datos obtenidos en el ejercicio 1, rellena la siguiente tabla con el filtro adecuado. Ve aplicando también cada filtro en tu captura de Wireshark para comprobar y analizar los resultados obtenidos. No es necesario que adjuntes pantallazos.

Condición	Filtro
Paquetes enviados por tu tarjeta de red	<code>eth.src == 3c:91:80:2c:09:77</code>
Paquetes enviados a tu tarjeta de red	<code>eth.dst == 3c:91:80:2c:09:77</code>
Paquetes enviados a una tarjeta de red <b>que no sea la tuya</b>	<code>eth.dst != 3c:91:80:2c:09:77</code>
Paquetes con tipo 0x800	<code>eth.type == 0x800</code>
Paquetes con un tipo que no sea 0x800 enviados por tu tarjeta de red	<code>eth.type != 0x800</code>
Paquetes que superen los 1500 bytes de tamaño	<code>eth.len &gt; 1500</code>
Paquetes enviados o recibidos por tu tarjeta de red	<code>eth.addr == 3c:91:80:2c:09:77</code>
Paquetes enviados por tu tarjeta de red a todos los equipos de la LAN y cuyo tamaño supere los 300 bytes	<code>eth.src == ff:ff:ff:ff:ff:ff &amp;&amp; eth.len &gt; 300</code>
Paquetes enviados por tu tarjeta de red al exterior de la LAN y cuyo tamaño sea inferior a 100 bytes	<code>eth.src == 3c:91:80:2c:09:77 &amp;&amp; eth.len &gt; 100</code>

Recuerda usar a partir de ahora filtros en Wireshark para no tener que navegar entre miles de paquetes en el listado y acceder rápidamente a la información deseada.

**Ejercicio 4: Tarjetas de red.** En el siguiente enlace tienes el manual de una placa base que tiene una tarjeta de red Ethernet integrada:

[https://download.gigabyte.com/FileList/Manual/mb\\_manual\\_z490m\\_e.pdf](https://download.gigabyte.com/FileList/Manual/mb_manual_z490m_e.pdf)

Responde a las siguientes preguntas buscando en el manual. **Indica también el n.º de página del manual donde has encontrado cada respuesta.**

- ¿Qué tipo de tarjeta de red tiene la placa (Ethernet, Fast Ethernet, etc)? Ethernet, Fast Ethernet y Giga Ethernet.
- ¿A qué velocidad máxima puede funcionar? 1000 Mbps.
- ¿Qué subestándar 802.3 soporta la tarjeta? 802.3i, 802.3u, 802.3ab y 802.3z.

- ¿Cuántos puertos LAN tiene la placa?  
1.
- ¿Cuántos LED tiene la tarjeta de red?  
2.
- Sobre el LED izquierdo, ¿qué quiere decir si está en naranja?  
Que está transmitiendo a 1Gbps.
- Sobre el LED derecho, ¿qué quiere decir si está parpadeando?  
Que está transmitiendo datos.
- Si instalamos otra tarjeta de red en una ranura PCI Express de la placa, ¿a qué sección de Settings dentro de la BIOS tendremos que ir para deshabilitar la tarjeta de red integrada?  
IO Ports > PCH LAN Controller.
- ¿La tarjeta integrada soporta Wake On LAN?  
Si.

**Ejercicio 5: Características de los switches.** En el siguiente enlace tienes las especificaciones de una serie de switches:

[https://eu.dlink.com/es/es/-/media/business\\_products/dgs/dgs-1210/datasheet/dgs\\_1210\\_series\\_f1\\_datasheet\\_en\\_eu.pdf](https://eu.dlink.com/es/es/-/media/business_products/dgs/dgs-1210/datasheet/dgs_1210_series_f1_datasheet_en_eu.pdf)

Responde a las siguientes preguntas sobre el modelo de switch DGS1210-10:

- ¿Número de puertos Ethernet del switch?  
8 de Fast Ethernet y 2 de Gigabit Ethernet.
- ¿Número de puertos SFP (para fibra óptica)?  
2.
- ¿Subestándares 802.3 soportados?  
802.3, 802.3u, 802.3ab, 802.3z, 802.3az y 802.3x.
- ¿Categorías y tipo de par trenzado soportados?  
UTP Cat. 5, Cat. 5e (100 m max.).
- ¿Tamaño máximo permitido del cable?  
280 x 126 x 44 mm.
- ¿Qué quiere decir que todos los puertos soportan AUTO MDI/MDIX (ver unidad 4)?  
Que las conexiones pueden ser directas o cruzadas, ya que el interface cambia su estado de MDI a MDIX automáticamente.
- ¿Cuántas direcciones MAC caben en la tabla del switch?  
8.000.
- ¿Cuánta RAM tiene la CPU del switch?  
128MB.
- ¿Cuántos LEDs tiene **en total** el switch?  
31.
- ¿En qué rango de temperaturas puede funcionar correctamente?  
-5 to 50°C.
- ¿En qué rango de humedades puede almacenarse sin ser usado?  
• 0% to 95%.
- ¿Cuánto pesa el switch?  
0,98 kg.
- ¿Cuál es el tiempo medio entre fallos del switch (Mean Time Between Failures, MTBF)?  
1.380.058 horas.

**Ejercicio 6: Configuración de switches.** En el siguiente enlace tienes emuladores online de dispositivos de red, para que puedas examinar sus opciones:

<https://www.tp-link.com/en/support/emulator/>

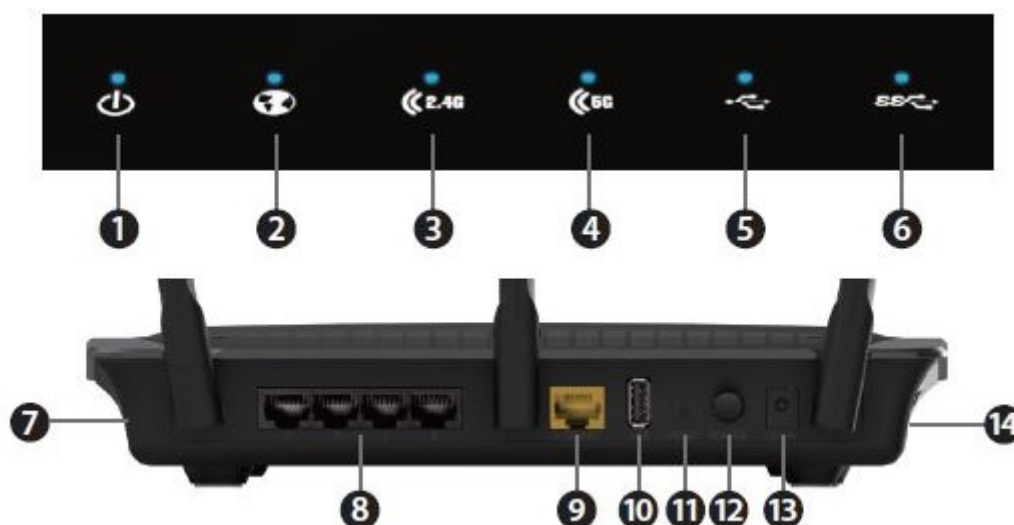
Baja hasta la sección Business, Switches, Managed Switches y haz clic en el switch TL-SL5428E. Accede a la versión 3 del firmware del switch. El firmware de un dispositivo es el programa que nos permite gestionar la configuración del mismo, similar a una versión reducida de un SO. Busca las opciones de la tabla siguiente y para cada una de ellas indica dónde la encontrarías. Puedes cambiar las opciones del switch que quieras sin miedo, ya que no son dispositivos reales, son emuladores para aprender a configurar un switch y poder ver todas sus opciones y menús como si estuvieran en tu red. Todas las opciones que se te piden en este ejercicio están en una de las siguientes tres categorías del panel izquierdo: System, Switching o Maintenance.

Opción a buscar	Categoría del panel izquierdo	Subcategoría del panel izquierdo	Sección del panel superior
<i>Versión actual del firmware instalado en el switch</i>	System	System Info	System Summary
<i>Deshabilitar el puerto 4</i>	Switching	Port	Port Config
<i>Hacer un backup (copia de seguridad) de la configuración</i>	System	System Tools	Config Backup
<i>Ver el contenido de la tabla con todas las direcciones MAC</i>	Switching	MAC Address	Address Table
<i>Averiguar la dirección MAC del switch</i>	System	System Info	System Summary
<i>Hallar el número de paquetes de difusión recibidos por el switch</i>	Switching	Traffic Monitor	Traffic Statistics
<i>Agregar otra cuenta de administrador para configurar el switch</i>	System	User Management	User Config
<i>Actualizar el firmware</i>	System	System Tools	Firmware Upgrade
<i>Restaurar la configuración por defecto</i>	System	System Tools	Config Restore
<i>Ver el log(*)</i>	Maintenance	Log	Log Table
<i>Averiguar el n.º de paquetes recibidos por el puerto 3</i>	Switching	Traffic Monitor	Traffic Summary

(\*) El log o fichero de registro es un fichero de texto interno donde se guardan todas las operaciones realizadas en el switch junto con la fecha y hora en la que se hicieron.



**Ejercicio 7: Características de routers inalámbricos.** Aquí tienes una foto de los LED de la parte frontal de un router inalámbrico y otra foto de la parte trasera del mismo router:



Completa la tabla con el número adecuado:

Nº	Elemento	Definición
14	Puerto USB 3.0	Para conectar dispositivos USB compatibles con v3.0
	LED SS USB	Luz azul cuando un dispositivo Super Speed (USB v3.0) está conectado
	Puerto USB 2.0	Para conectar dispositivos USB compatibles con v2.0
	LED 5G	Luz azul cuando el router está emitiendo a frecuencia de 5 GHz. Además, durante la conexión por WPS, parpadeará
	LED Internet	Luz azul cuando el router está conectado a Internet. Luz naranja cuando el router tiene conexión local, pero no puede conectarse a Internet
	Puertos LAN (1 a 4)	Puertos para conectar dispositivos usando cable de red
	Puerto Internet o WAN	Puerto para la conexión con el ISP (ADSL, fibra óptica...)
	LED Power	Luz azul cuando recibe corriente. Luz naranja durante el arranque
	Botón Reset	Mantener pulsado durante 6 segundos para cargar los valores de fábrica en el router. Se perderá toda la configuración anterior
	Clavija de alimentación	Para conectar el router a la corriente eléctrica
	LED 2.4G	Luz azul cuando el router está emitiendo a frecuencia de 2.4 GHz. Además, durante la conexión por WPS, parpadeará
7	Botón WPS	Pulsar para iniciar el proceso WPS (WiFi Protected Setup). Una vez pulsado, el router detectará el nuevo dispositivo que pide conectarse temporalmente a la WLAN. El usuario

		deberá introducir el PIN en la ventana que aparecerá en su dispositivo móvil. El PIN está en la pegatina del router. Después, el dispositivo móvil podrá conectarse a la WLAN
	LED USB	Luz azul cuando un dispositivo USB v2.0 está conectado
	Botón de encendido	Pulsar para encender/apagar el router

(Como actividad complementaria, identifica todos los LED y conexiones de un router inalámbrico que uses habitualmente)

**Ejercicio 8: Configuración de routers inalámbricos.** Accede de nuevo a la web que usaste en el ejercicio 6. Busca la sección “Wi-Fi Routers” y selecciona el router inalámbrico TL-WR1043ND, firmware v4. Haz clic en Advanced para ver la configuración completa. Completa la tabla buscando la opción correspondiente. Las categorías donde están todas las opciones que debes buscar son: Status, Network, Wireless, DHCP, USB Settings, Advanced Routing o System Tools.

Opción a buscar	Categoría del panel izquierdo	Subcategoría
<i>Cambiar el SSID de la WLAN</i>	Wireless	Wireless Settings
<i>Ver el log del router</i>	System Tools	System Log
<i>Habilitar/deshabilitar la difusión del SSID</i>	Wireless	Wireless Settings
<i>Averiguar la MAC del router</i>	Status	Wireless
<i>Actualizar el firmware</i>	System Tools	Firmware Upgrade
<i>Cambiar el canal por defecto de la WLAN</i>	Network	WAN
<i>Averiguar la IP que tiene el router en la LAN</i>	Status	LAN
<i>Cambiar la IP que tiene el router en la LAN</i>	Network	LAN
<i>Cambiar la contraseña del administrador</i>	System Tools	Password
<i>Seleccionar el tipo de seguridad (WPA, WPA2...) y establecer la contraseña de la WLAN</i>	Wireless	Wireless Security
<i>Crear/restaurar un backup de la configuración del router</i>	System Tools	Backup & Restore
<i>Añadir un nuevo dispositivo por WPS</i>	Wireless	WPS
<i>Ver la tabla de enrutamiento del router</i>	Advanced Routing	System Routing Table
<i>Lista “negra” con las MAC que no pueden conectarse a la WLAN (todas las demás tienen acceso)</i>	Wireless	Wireless MAC Filtering
<i>Especificar el rango de IP que repartirá el servidor DHCP</i>	DHCP	DHCP Settings
<i>Ver los dispositivos conectados al puerto USB del router</i>	USB Settings	Storage Sharing

<i>Reiniciar el router (similar a apagar y encender con el botón externo)</i>	System Tools	Reboot
<i>Lista “blanca” con las MAC que sí pueden conectarse a la WLAN (todas las demás no tienen acceso)</i>	Advanced Routing	Static Routing list
<i>Ver las IP asignadas en este momento por el servidor DHCP</i>	DHCP	DHCP Client List
<i>Resetear toda la configuración del router (cargar los valores de fábrica)</i>	System Tools	Factory Defaults
<i>Hacer que el servidor DHCP reparta siempre la misma IP a la misma MAC</i>	DHCP	Address Recervation

(Como actividad complementaria, busca las mismas opciones en un router inalámbrico que uses habitualmente)

### **Ejercicio 9: Práctica: Configuración de switches y routers en Packet Tracer.**

Realiza las prácticas 3 y 4 de Packet Tracer (los PDF con el manual de CISCO están en el aula virtual):

- *Práctica 3. Configure End Devices*
  - Lo más importante de esta práctica es que sepas asignar una dirección IP a un PC, usar el comando ping en los PC para enviar datos de un equipo a otro y así probar que entre ellos hay conectividad, y configurar switches de Cisco con comandos empleando la CLI (Command Line Interface, Interfaz de Línea de Comandos)
- *Práctica 4. Create a Simple Network*
  - *Esta práctica empieza mostrándote primero el resultado final que deberás obtener. Después, el enunciado te va guiando paso a paso para conseguirlo*
  - *Lo más importante es configurar un router Cisco inalámbrico, instalar una tarjeta de red inalámbrica en un portátil y conectar un portátil al router por WiFi*
  - *A partir del paso 3 de la página 6, la realización de la práctica es opcional*
  - *El PDF de esta práctica contiene algunos errores. Consulta el aula virtual para corregir los errores del enunciado*

Como ejercicio, tras hacer las dos prácticas crea el diseño lógico de una WLAN con PT que incluya 5 portátiles conectados por WiFi a un router inalámbrico. Las IP de los equipos deberán ser desde la 192.168.0.31 hasta la 35, y las repartirá el servidor DHCP del router. El SSID de la red será ENLACE. Deberá poder hacerse ping entre dos portátiles cualesquiera. **Envía en la entrega el fichero .pkt con la red creada. No olvides añadir una etiqueta con nombre y fecha al fondo.**

**Ejercicio 10: Protocolo ARP.** En la unidad 5 has aprendido el funcionamiento del protocolo ARP (para traducir direcciones IP del nivel de red a direcciones MAC del nivel de enlace). Ahora vas a verlo en acción, analizando el formato exacto que tienen los mensajes que envía el protocolo por la red.

En Redes y en Seguridad es sumamente importante que conozcas muy bien el funcionamiento de los protocolos y el contenido de las diversas cabeceras, ya que la gran mayoría de ataques que suceden en una red consisten en alterar los valores típicos de las cabeceras y los pasos que deberían seguir los protocolos para que el resultado sea diferente, y como consecuencia, la red tenga agujeros de seguridad y quede desprotegida.

En primer lugar, observa el contenido de la caché ARP de tu equipo usando el comando correspondiente. Adjunta un pantallazo con los resultados y rellena la siguiente tabla con tres filas cualesquiera.



```
> arp
Address                HWtype  HWaddress      Flags Mask    Iface
192.168.0.18           ether    ec:be:5f:45:f6:fe  C             wlp2s0
_gateway              ether    ac:3b:77:8d:91:6c  C             wlp2s0
192.168.0.10          ether    ac:3b:77:8d:91:6d  C             wlp2s0
> ip n show
192.168.0.18 dev wlp2s0 lladdr ec:be:5f:45:f6:fe REACHABLE
192.168.0.1 dev wlp2s0 lladdr ac:3b:77:8d:91:6c STALE
192.168.0.10 dev wlp2s0 lladdr ac:3b:77:8d:91:6d STALE
```

Dirección IP	Dirección MAC
192.168.0.18	ec:be:5f:45:f6:fe
192.168.0.1	ac:3b:77:8d:91:6c
192.168.0.10	ac:3b:77:7d:91:6d

Longitud de cada IP: 4 bytes.

Longitud de cada MAC: 6 bytes.

Ahora vamos a borrar el contenido de la caché ARP. Así forzaremos a que el equipo no conozca la MAC de ningún otro equipo y envíe mensajes ARP por difusión. Para borrar la caché ARP, en Windows usa `arp -d *` y en Linux usa `ip -s -s neigh flush all`. Deberás ser administrador en ambos casos para poder ejecutar el comando correspondiente. En Windows, puedes abrir una terminal en modo administrador buscando el comando `cmd`, haciendo clic con el botón derecho y seleccionar “Ejecutar como administrador”. En Linux, bastará que pongas “`sudo`” y a continuación en la misma línea el comando antes citado.

Ahora deberás abrir Wireshark y capturar paquetes. Sin detener la captura, **deberás mandar un ping a otro equipo de tu red del cual sepas su IP y no sepas su MAC**, tecleando el comando `ping` y la IP (el comando es el mismo para Windows y Linux). Después, puedes detener la captura. Deberías poder ver varios paquetes ARP capturados en Wireshark.

Por ejemplo, en este equipo con la IP 192.168.1.25...

```

C:\Windows\System32>arp -d *

C:\Windows\System32>arp -a

Interfaz: 192.168.56.1 --- 0x8
Dirección de Internet      Dirección física      Tipo
224.0.0.22                01-00-5e-00-00-16    estático

Interfaz: 192.168.1.25 --- 0x9
Dirección de Internet      Dirección física      Tipo
192.168.1.1                60-8d-26-b9-88-     dinámico
224.0.0.2                  01-00-5e-00-00-     estático
224.0.0.22                 01-00-5e-00-00-     estático

C:\Windows\System32>ping 192.168.1.10

Haciendo ping a 192.168.1.10 con 32 bytes de datos:
Respuesta desde 192.168.1.10: bytes=32 tiempo=921ms TTL=64
Respuesta desde 192.168.1.10: bytes=32 tiempo=7ms TTL=64
Respuesta desde 192.168.1.10: bytes=32 tiempo=16ms TTL=64
Respuesta desde 192.168.1.10: bytes=32 tiempo=8ms TTL=64

Estadísticas de ping para 192.168.1.10:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 7ms, Máximo = 921ms, Media = 238ms

```

...borramos primero la caché ARP, miramos de nuevo su contenido y comprobamos que otro equipo de la misma red con la IP 192.168.1.10 no está en la caché. Le enviamos un ping (para forzar a pedir su MAC usando ARP) y a partir de entonces se habrá realizado el proceso por difusión y ya debería aparecer en caché:

```

Dirección de Internet      Dirección física      Tipo
192.168.1.1                60-8d-26-b9-88-     dinámico
192.168.1.10               18-70-3b-65-f8-     dinámico

```

Y además en Wireshark habrán aparecido mensajes ARP del 25 preguntando por la MAC del 10:

42	2.987796	Arcadyan_b9:88	Chongqin_91:d4	ARP	52	Who has 192.168.1.25? Tell 192.168.1.1
43	2.987837	Chongqin_91:d4	Arcadyan_b9:88	ARP	42	192.168.1.25 is at 4c:d5:77:91:d4
44	3.063846	Chongqin_91:d4	Broadcast	ARP	42	Who has 192.168.1.10? Tell 192.168.1.25
45	3.068411	Arcadyan_b9:88	Broadcast	ARP	60	Who has 192.168.1.13? Tell 192.168.1.1
46	3.069243	Arcadyan_b9:88	Broadcast	ARP	60	Who has 192.168.1.14? Tell 192.168.1.1
49	3.951411	Chongqin_91:d4	Broadcast	ARP	42	Who has 192.168.1.10? Tell 192.168.1.25
50	3.978048	HuaweiDe_65:f8	Chongqin_91:d4	ARP	52	192.168.1.10 is at 18:70:3b:65:f8

Wireshark resume los mensajes ARP de **consulta** con frases como “¿Quién tiene la 10? Respóndele al 25” (paquetes 44 y 49, enviados por difusión o broadcast). Si te fijas, el paquete 50 es la **respuesta** esperada: “El 10 tiene la MAC 18:70:etc”, que como puedes comprobar en la caché ARP, es justamente esa.

Recuerda que no tienes por qué buscar los paquetes ARP en el listado, puedes darle a la columna Protocol para que agrupe los paquetes según el mismo protocolo... o aplicar un filtro (Wireshark viene con un filtro por defecto para mostrar sólo los paquetes ARP, ver ejercicio 3a de esta misma unidad).

¿Qué filtro muestra los paquetes ARP? arp

Haz clic en un mensaje ARP de consulta (o pregunta, petición o request).

¿Cuál es la longitud de una pregunta ARP (sin contar la cabecera Ethernet)? 28 bytes  
 ¿Qué valor aparece en el campo tipo de la cabecera Ethernet de este paquete? 0x0806

Completa esta tabla analizando el contenido de las cabeceras Ethernet de una pregunta y su respuesta ARP asociada:

	MAC origen	MAC destino	Tipo
<i>Pregunta ARP</i>	3c:91:80:2c:09:77	ac:3b:77:8d:91:6c	0x0806
<i>Respuesta ARP</i>	ac:3b:77:8d:91:6c	3c:91:80:2c:09:77	0x0806

¿Qué filtro mostraría **solamente las preguntas ARP**? arp.opcode == 1

Abre el contenido de una pregunta ARP...

```
> Frame 44: 42 bytes on wire (336
> Ethernet II, Src: Chongqin_91:d
v Address Resolution Protocol (re
  Hardware type: Ethernet (1)
  Protocol type: IPv4 (0x0800)
  Hardware size: 6
```

... y completa esta tabla con los campos que aparecen en el interior de la zona de ARP:

	Nombre	Valor	Longitud en bytes
<i>Campo #1</i>	Hardware type	1	2
<i>Campo #2</i>	Protocol type	0x0800	2
<i>Campo #3</i>	Hardware size	6	1
<i>Campo #4</i>	Protocol size	4	1
<i>Campo #5</i>	Opcode	1	2
<i>Campo #6</i>	Sender MAC address	3c:91:80:2c:09:77	6
<i>Campo #7</i>	Sender IP address	192.168.0.21	4
<i>Campo #8</i>	Targer MAC address	00:00:00:00:00:00	6
<i>Campo #9</i>	Targer IP address	192.168.0.1	4

Y ahora repite lo mismo, pero con la respuesta ARP asociada a la pregunta:

	Nombre	Valor	Longitud en bytes
<i>Campo #1</i>	Hardware type	1	2
<i>Campo #2</i>	Protocol type	0x0800	2
<i>Campo #3</i>	Hardware size	6	1
<i>Campo #4</i>	Protocol size	4	1
<i>Campo #5</i>	Opcode	2	2
<i>Campo #6</i>	Sender MAC address	ac:3b:77:8d:91:6c	6
<i>Campo #7</i>	Sender IP address	192.168.0.1	4

<b>Campo #8</b>	Targer MAC address	3c:91:80:2c:09:77	6
<b>Campo #9</b>	Targer IP address	192.168.0.21	4

Como ves, tanto las preguntas como las respuestas ARP tienen un formato muy parecido, aunque no idéntico.

De los 9 campos, ¿cuáles tienen idénticos valores en las preguntas y en las respuestas?  
1, 2, 3 y 4.

¿Y cuáles tienen valores diferentes?  
5, 6, 7, 8, y 9.

Asocia cada uno de los 9 campos del interior de un mensaje ARP con su significado, rellorando la tabla que encontrarás abajo:

1. Hardware type
2. Protocol type
3. Hardware size
4. Protocol size
5. Opcode
6. Sender MAC address
7. Sender IP address
8. Target MAC address
9. Target IP address

- a. Indica la longitud de las direcciones del nivel de enlace (por lo general, direcciones MAC, de 6 bytes cada una)
- b. Indica la MAC del emisor
- c. Indica si el mensaje es una pregunta (valor 1) o una respuesta (valor 2)
- d. Indica el tipo de direcciones del nivel de enlace (por lo general, Ethernet, código 1)
- e. Indica la MAC del receptor (o todo a ceros si no conocemos su MAC)
- f. Indica la longitud de las direcciones del nivel de red (por lo general, direcciones IP, de 4 bytes cada una)
- g. Indica el tipo de direcciones del nivel de red (por lo general, IPv4, código 0x0800)
- h. Indica la IP del receptor
- i. Indica la IP del emisor

Nº	Definición
1	d
2	g
3	a
4	f
5	c
6	b
7	i
8	e
9	h

Aquí tienes un paquete entero capturado en otra red, en cuyo interior hay un mensaje ARP:

0000	ff ff ff ff ff ff 00 07 0d af f4 54 08 06 00 01
0010	08 00 06 04 00 01 00 07 0d af f4 54 45 4c d8 01
0020	00 00 00 00 00 00 45 4c de 10

¿Es una pregunta o una respuesta? Pregunta

¿De qué dos formas puedes demostrarlo?

1. Por la MAC ff:ff:ff:ff:ff:ff
2. Opcode que es 00 01, en la fila 0010 el quinto y sexto byte.