Ejercicio 1: DHCP

a) Para entender el funcionamiento interno del protocolo DHCP y cómo se comunican clientes y servidores, vas a capturar paquetes DHCP empleando Wireshark. En primer lugar, recuerda que, como ahora tienes conexión a la red y dirección IP, el proceso DHCP ya ha finalizado, por lo que debemos forzar al ordenador para que solicite de nuevo una IP al servidor. **Ten en cuenta que durante la ejecución de esta práctica, vas a perder la conexión a la red momentáneamente.**

Abre Wireshark e inicia una captura de paquetes. Mientras capturas, desde la consola de Windows (comando cmd) teclea `ipconfig /release`. Este comando fuerza al equipo a liberarse de su IP, pasando entonces a tener la dirección especial 0.0.0.0. A continuación teclea el comando `ipconfig /renew` para pedir de nuevo una IP al servidor DHCP. Comprueba que vuelves a tener una dirección IP y que ya has recuperado la conexión. Puedes parar de capturar con Wireshark. Deberían haberte aparecido, entre otros, los cuatro paquetes básicos de DHCP: DISCOVER, OFFER, REQUEST y ACK.

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	0.0.0.0	255.255.255.255	DHCP	314	DHCP Discover - Transaction ID 0x3d1d
2	0.000295	192.168.0.1	192.168.0.10	DHCP	342	DHCP Offer - Transaction ID 0x3d1d
3	0.070031	0.0.0.0	255.255.255.255	DHCP	314	DHCP Request - Transaction ID 0x3d1e
4	0.070345	192.168.0.1	192.168.0.10	DHCP	342	DHCP ACK - Transaction ID 0x3d1e

(En Linux, puedes simular la liberación de IP y la petición de dirección desactivando y activando temporalmente la conexión haciendo clic en el icono correspondiente, cuya ubicación puede variar según la distribución Linux empleada)

Si lo prefieres, en lugar de capturar por tu cuenta, también puedes usar la captura de prueba **dhcp.pcap** disponible en el aula virtual, que ya incluye los cuatro paquetes.

b) Completa la tabla analizando las cabeceras de los niveles de enlace (Ethernet), red (IP) y transporte (UDP) de los cuatro mensajes DHCP:

Mensaje	***MAC origen***	***MAC destino***	***IP origen***	***IP destino***	***Puerto origen***	***Puerto destino***
DISCOVER	Mi MAC	Broadcast	0.0.0.0	Broadcast	68	67
OFFER	MAC del Router	Mi MAC	IP del Router	Mi IP ofrecida	67	68
REQUEST	Mi MAC	Broadcast	0.0.0.0	Broadcast	68	67
ACK	MAC del Router	Mi MAC	IP del Router	Mi IP	67	68

c) Completa también esta tabla analizando el contenido del nivel de aplicación de los mensajes DHCP:

Mensaje	*Message Type*	*HW type*	*HW address length*	*Hops*	*Transaction ID*	*Your (client) IP address*	*Server IP address*	*Client MAC address*
DISC	Boot Request (1)	Ethernet (0x01)	6	0	0x383e9742	0.0.0.0	0.0.0.0	Mi MAC
OFFER	Boot Reply (2)	Ethernet (0x01)	6	0	0x383e9742	Mi IP ofrecida	IP del Servidor	Mi MAC
REQ	Boot Request (1)	Ethernet (0x01)	6	0	0x383e9742	0.0.0.0	0.0.0.0	Mi MAC
ACK	Boot Reply (2)	Ethernet (0x01)	6	0	0x383e9742	Mi IP	IP del Servidor	Mi MAC

d) Contesta las siguientes preguntas sobre los campos de los mensajes DHCP:

- ¿Cuál es el valor del campo “Message Type” en los mensajes DISCOVER y REQUEST?
  Boot Request (1) = 0x01
- ¿Cuál es el valor del campo “Message Type” en los mensajes OFFER y ACK?
  Boot Reply (2) = 0x02
- ¿Cuál es el valor de “HW type”? ¿Qué tecnología de LAN está asociada a dicho valor?
  Ethernet (0x01).
  Ethernet 802.3
- ¿Cuál es el valor de “HW address length”? ¿Por qué?
  6
  Es por los 6 bytes que representa el tamaño de una dirección MAC (nivel de enlace)

e) Asocia cada nombre de campo con su longitud en bytes y la letra (A, B o C) correspondiente a su definición:

- Message type (1 bytes): definición B
- Hardware type (1 bytes): definición C
- Hardware address length (1 bytes): definición A

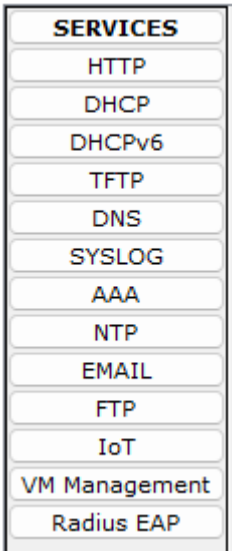
Definiciones: *A) “Es el tamaño de la dirección usada en el nivel de enlace. En redes Ethernet, cada MAC ocupa 6 bytes”, B) “Es el tipo de mensaje DHCP. Es 1 para los mensajes enviados por el cliente y 2 para los mensajes enviados por el servidor”, C) “Representa el tipo de tecnología usada en la LAN. Si es 1, indica que estamos usando Ethernet”*

f) Selecciona el mensaje ACK, inspecciona su contenido e indica qué datos (además de la IP) son proporcionados por el servidor.

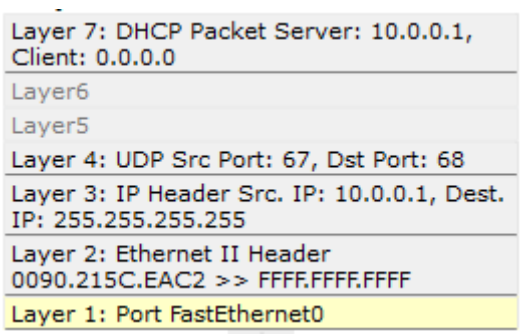
g) Para cada uno de estos filtros de Wireshark, indica cuál o cuáles de los 4 mensajes DHCP básicos son recogidos por cada filtro:

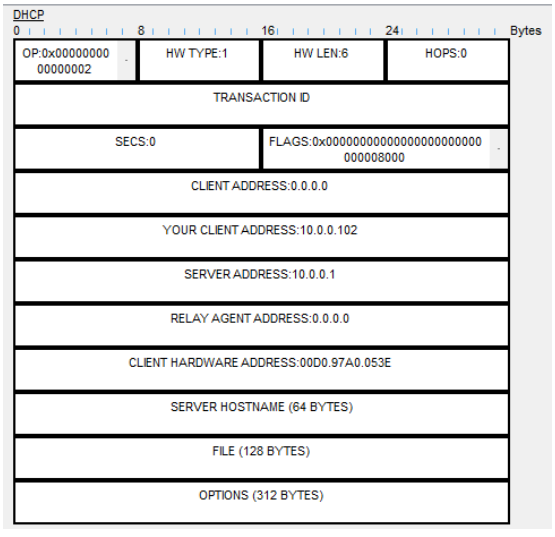
- (eth.src==”tu MAC”) && (udp.srcport==68) → **DISCOVER y REQUEST**
- (ip.src==”IP del servidor DHCP”) && (udp.srcport==67) → **OFFER y ACK**
- (eth.src==”tu MAC”) && (eth.dst==ff:ff:ff:ff:ff:ff) → **DISCOVER y REQUEST**
- (udp.port==67) || (udp.port==68) → **DISCOVER, OFFER, REQUEST y ACK**
- ip.dst==”IP del servidor DHCP” → **NO ES VÁLIDO**, ip.dst==broadcast o mi ip
- (udp.dstport==68)&&(ip.src==0.0.0.0) → **NO ES VÁLIDO**, ip.src==IP servidor
- (ip.dst!=255.255.255.255) → **OFFER y ACK**

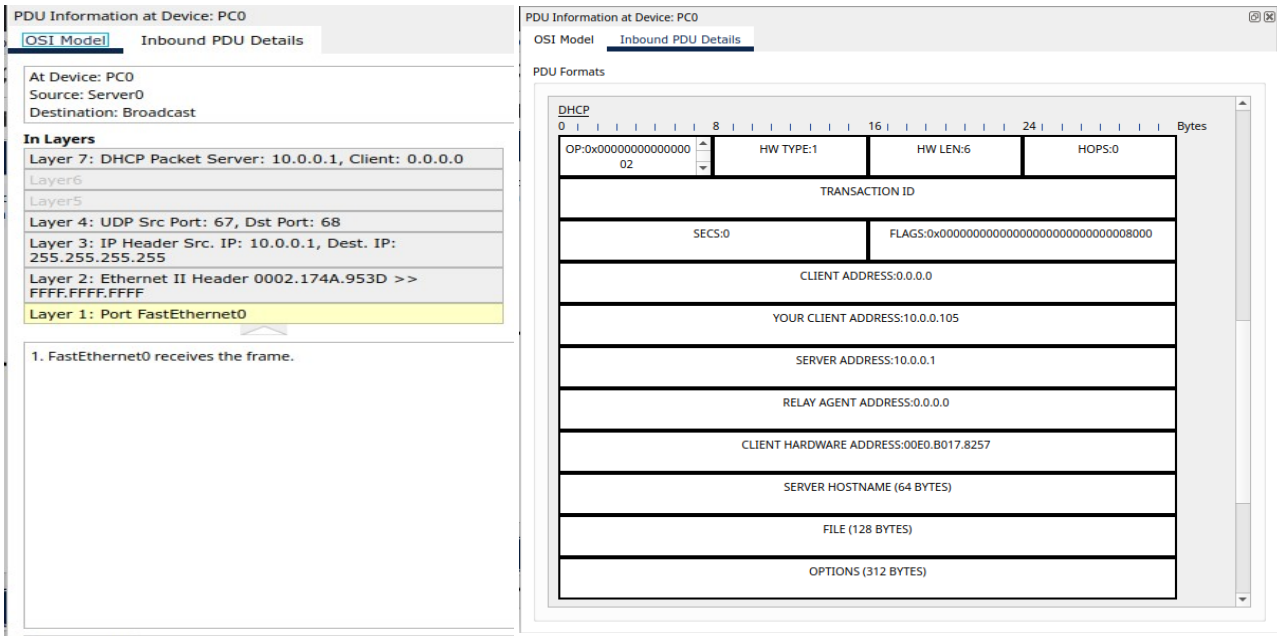
h) Crea en Packet Tracer una LAN con un servidor y 4 PC, todos conectados por cable a un switch 2960. Ve a la configuración del servidor y asígnale la IP estática 10.0.0.1, y a los PC asígnales IP dinámicas. De nuevo en el servidor DHCP, ve a la pestaña Services, y configura el servicio DHCP para que reparta en el pool que tiene por defecto desde la IP 10.0.0.101 hasta la 10.0.0.200 y que también reparta la máscara por defecto (sin subredes).



Usando el modo Simulación (ver Unidad 6, ejercicio 7, parte 2), pega aquí dos pantallazos: uno con el contenido de todas las cabeceras OSI del ACKNOWLEDGMENT, y otro con el contenido de la zona de datos, del mismo mensaje ACKNOWLEDGMENT. En las dos siguientes imágenes se muestra lo mismo pero para un DISCOVER. Recuerda aplicar un filtro antes de simular, para que solo se muestren los mensajes DHCP y no todos los mensajes de todos los protocolos. Para forzar el uso de DHCP en los PC, deberás cambiar la IP a estática y a continuación a dinámica (o teclear `ipconfig /release` y después `ipconfig /renew` en la consola de un PC).

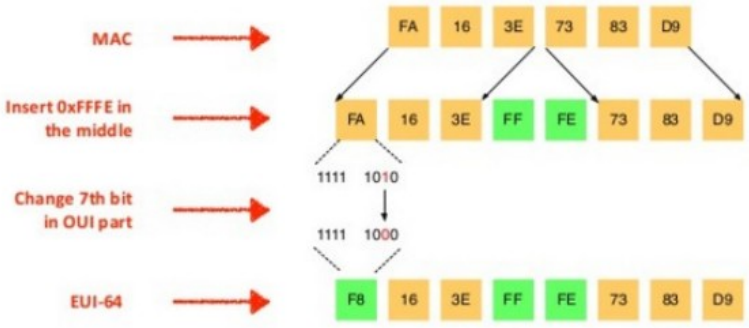






i) DHCPv6 es la adaptación del protocolo DHCP tradicional para que reparta IPv6. Uno de los nuevos tipos de reparto introducidos en DHCPv6 se denomina SLAAC, que consiste en obtener una IPv6 sin pedírsela al servidor DHCP, para ahorrar difusiones. Para obtener una IPv6 sin interactuar con el servidor, el proceso es el siguiente:

Paso 1. Obtener la MAC del equipo.
Paso 2. Insertar en medio de la MAC “FFFE”
Paso 3. En el primer byte, cambiar el séptimo bit (si es 0, cambiarlo a 1, y si es 1, cambiarlo a 0).
Paso 4. Traducir a hexadecimal el resultado obtenido.



Así se obtiene el EUI64, que correspondería a los últimos 64 bits de una IPv6. Respecto a los primeros 64 bits (recuerda que una IPv6 tiene 128 bits en total), también llamados “prefijo”, se puede obtener de dos formas: o bien el prefijo es difundido por el router de vez en cuando por toda la red, o bien se usa el prefijo local FE80:: que está reservado para uso interno en una LAN (de forma parecida a las IP privadas en IPv4, cuyo ámbito de actuación es únicamente la red local). La unión del prefijo y el EUI64 formarán la IPv6 completa.

A partir de tu MAC, obtén cuál sería tu IPv6 usando el prefijo local, siguiendo los cuatro pasos del proceso SLAAC:

- Dirección MAC: **3c:91:80:2e:09:77**
- IPv6 local: **3e:91:80:ff:fe:2e:09:77**
  3c = 0011 1100
  3e = 0011 1110

Ejercicio 2: DNS

a) Busca en Google el significado de los siguientes dominios gTLD:

.aero: aeronautics, Industria de la aviación.
.biz: negocios, Empresas.
.info: información, páginas web informativas (sitios de información)

b) Busca en Google a qué países pertenecen los siguientes dominios geográficos ccTLD:

.mt: Malta
.tr: Turquía
.za: Sudáfrica
.kr: Corea

c) Busca en Google los dominios correspondientes a los siguientes países:

Dinamarca: .dk
Marruecos: .ma
Rusia: .ru

d) Ve a https://root-servers.org/ y contesta estas preguntas:

¿Cuál es la IPv4 de k.root-servers.org? 193.0.14.129
¿Y la IPv6? 2001:7fd::1
¿Cuántas "copias" de f.root-servers.org existen en el mundo? 336
¿Cuántos servidores raíz hay en total en España? 7
¿En qué ciudades? Madrid, Barcelona y Malaga

e) Averigua la/s IP de tu/s servidor/es DNS (por ejemplo, con `ipconfig /all`).

Mi/s servidor/es DNS: **192.168.0.1**
Averiguada desde el comando **cat /etc/resolv.conf**

f) Captura paquetes DNS con Wireshark. Para ello, inicia una captura y visita varias webs que no hayas visitado recientemente, para forzar que haya nuevas consultas DNS (si las visitaste hace poco, no se usará DNS ya que las respuestas recientes se guardan en la caché DNS para ahorrar consultas). Cuando hayas capturado varios paquetes DNS, termina de capturar. También puedes usar el fichero **dns.pcap**, disponible en el aula virtual, con varios paquetes DNS capturados de prueba.

Escoge una pregunta DNS (también llamada "query") y una respuesta DNS ("response") y completa la siguiente tabla analizando las cabeceras correspondientes:

	IP origen	***IP destino***	***Puerto origen***	***Puerto destino***
Pregunta DNS	Mi IP	IP Servidor	Mi puerto	53
Respuesta DNS	IP Servidor	Mi IP	53	Mi puerto

g) Ahora responde estas preguntas analizando el interior de los mensajes DNS (capa de aplicación):

- ¿Cuánto mide (en bytes) el campo “Transaction ID”? **2**
- ¿Qué valor tiene el flag “Response” en las preguntas? **0**
- ¿Y en las respuestas? **1**
- Abre el campo Query de varias consultas DNS. ¿Qué tipo (“type”) suele aparecer más frecuentemente? En mi captura solo aparece:
  A (Host Address) (1) o **AAA (IPv6 addres) (28)**
- Abre el campo Answer de una respuesta DNS. ¿Cuál es el “data length” asociado a una dirección? ¿Por qué?
  En mi captura con **A (Host Address) (1)** es 4 y con **AAA (IPv6 addres) (28)** no tiene. Me imagino que hara referencia a que la ip es versión 4.

h) Escribe un filtro Wireshark para que aparezcan:
En el filtro puse el primer dns porque solo con dns.flags.response == 0 me salian tambien consultas MDNS.

- Solo las consultas DNS: dns && dns.flags.response == 0
- Solo las respuestas DNS: dns && dns.flags.response == 1

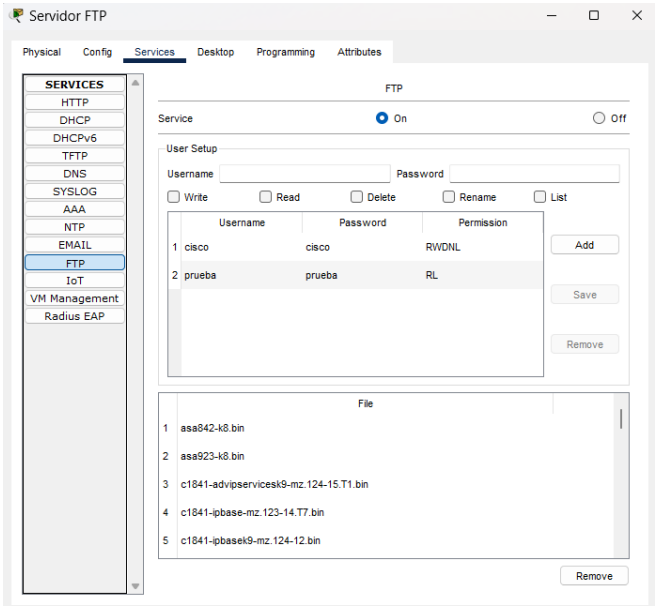
i) Añade a la LAN que creaste con Packet Tracer en el ejercicio anterior otro servidor, también conectado al switch, que usaremos como servidor DNS. Asígnale la IP estática 10.0.0.2. Modifica el pool del servidor DHCP para que el servidor DNS repartido a todos los clientes sea el 10.0.0.2. Haz que los clientes soliciten de nuevo IP para que se les reparta ahora también el nuevo servidor DNS.

En el servidor DNS, configura el servicio para añadir tres registros de tipo A: www.ejemplo.com con la IP 10.0.0.51, www.pruebas.es con la IP 10.0.0.61 y www.paginaweb.es con la IP 10.0.0.71.

Desde cualquier PC de la LAN, en su consola haz ping usando el nombre (por ejemplo, `ping www.pruebas.es`) y debería aparecerte la IP resuelta. Es normal que los pings no respondan, ya que esos equipos no existen en la red y por tanto no hay conexión con ellos, pero sí que debería traducirse el nombre a IP (eso indica que el servidor DNS funciona).

Ejercicio 3: FTP

a) Añade un servidor más a la red de PT, conéctalo al switch y asígnale la IP estática 10.0.0.81. Configura en el servidor el servicio FTP, creando una cuenta de usuario (login “prueba” y password “prueba”), con permisos de lectura y listar.



Ahora desde cualquier PC, abre una consola y conéctate al servidor FTP tecleando "`ftp 10.0.0.81`". Introduce el login y el password de la cuenta que acabas de crear. Lista el contenido del directorio home del servidor con el comando "`dir`". Aparecerá un listado de ficheros y su tamaño en bytes. Para descargarte uno desde el servidor FTP al PC, teclea "`get nombre_de_fichero`". Dependiendo del tamaño del fichero escogido, la transferencia puede tardar bastante tiempo. Cuando termine, desconéctate del servidor tecleando "`quit`". Una vez desconectado, teclea "`dir`" en la consola y aparecerá el fichero descargado, indicando que la transferencia FTP ha funcionado.

b) Modifica la configuración del servidor DNS para que se pueda acceder al servidor mediante el nombre "ftp.servidor.es" además de con su IP (10.0.0.81). Compruébalo desde un PC.

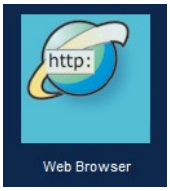
c) Crea un nuevo usuario en el servidor FTP llamado "prueba2" con la contraseña que quieras, y otórgale permisos de lectura, escritura y listado. Desde cualquier PC de la LAN, crea un fichero de texto con cualquier contenido, desde el editor de textos:

Al cerrar el editor, te preguntará el nombre del fichero de texto que quieres crear (ejemplo.txt). Abre la consola de ese PC y, tras ejecutar "`dir`" comprueba que aparece el fichero recién creado. Ahora conéctate al servidor FTP usando el nombre del servidor (no su IP) y con la cuenta "prueba2". Sube el fichero del cliente al servidor mediante el comando "`put ejemplo.txt`". Tras subirlo, haz un "`dir`" para verificar que se ha subido el fichero al servidor FTP. Desconéctate del servidor con "`quit`" para acabar.

Ejercicio 4: HTTPS

a) Añade a la red tres servidores más, con IP estáticas 10.0.0.51, 10.0.0.61 y 10.0.0.71 y nombres www.ejemplo.com, www.pruebas.es y www.paginaweb.es, respectivamente. Deberás configurar el servidor DNS para que se resuelvan los nombres. Asegúrate de que los tres servidores tienen activado tanto el servicio HTTP como HTTPS.

b) Ve a cualquier PC y abre su navegador:



Accede a www.ejemplo.com para ver la página web que Cisco pone por defecto en un servidor HTTPS.

c) Ve al servidor www.ejemplo.com y configura su servicio HTTP para añadir un nuevo fichero llamado prueba.html con el siguiente contenido:

```
<html><head><title>Prueba</title></head>
<body bgcolor=red>Ejemplo</body></html>
```

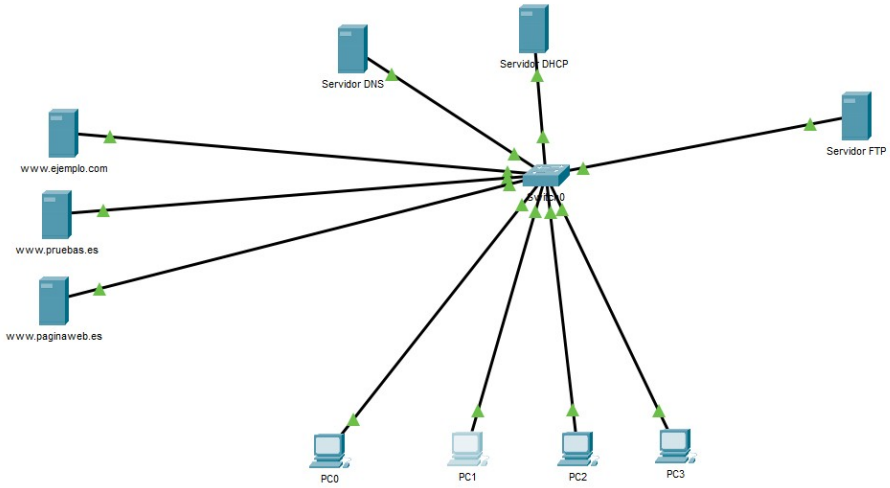
Graba el fichero, ve a un PC y desde su navegador accede a www.ejemplo.com/prueba.html. Deberías ver una página web con fondo rojo.

d) Crea dos páginas web más:

www.pruebas.es/pagina.html, donde ponga "hola" con fondo amarillo
www.paginaweb.es/redes.html donde ponga "Redes" con fondo verde

Comprueba desde cualquier PC de la LAN que puedes ver las webs accediendo a su URL desde el navegador.

Después de haber añadido todos los servidores (DHCP, DNS, FTP y HTTPS), tu LAN debería haber quedado así:



Adjunta a tu entrega el fichero .pkt obtenido.