

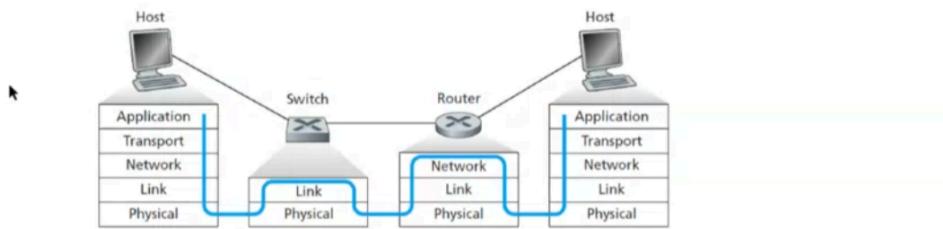
**Pregunta 1 (0,5 puntos):** En el siguiente esquema donde se representa como las diferentes capas SW encapsulan y desencapsulan la información, ¿qué campos podemos encontrar en la cabecera TCP y en la cabecera IP?



Respuesta:

- A. Cabecera TCP: TTL, puerto origen, puerto destino, flags (SYN, ACK, etc.) y en la cabecera IP: IP origen, MAC destino.
- B. Cabecera TCP: puerto origen, MAC destino y en la cabecera IP: IP origen, IP destino, TTL, checksum.
- C. Cabecera TCP: puerto origen, puerto destino, flags (SYN, ACK, etc.), checksum y en la cabecera IP: IP origen, IP destino, TTL, checksum.**
- D. Cabecera TCP: puerto origen, puerto destino, flags (SYN, ACK, etc.), checksum y en la cabecera IP: MAC origen, MAC destino, TTL.

**Pregunta 2 (0,5 puntos):** Del siguiente esquema donde se representa la estructura SW de una red de ordenadores, ¿qué afirmaciones son correctas?



Respuesta:

- A. En el nivel de aplicación existen protocolos como DNS, DHCP y HTTP y en el nivel de transporte IP e ICMP.
- B. Una identidad del nivel de red puede ser IP=10.20.15.10 y una del nivel de aplicación pepito@hotmail.com.**
- C. El switch de la figura tiene dos direcciones IP, una en la conexión con el host y otra en la conexión con el router.
- D. Para que la comunicación pueda llevarse a cabo, falta implementar los niveles de transporte y aplicación en el router.

**Pregunta 3 (0,5 puntos):** Tenemos dos máquinas virtuales Ubuntu en el sistema VirtualBox configuradas como NAT, en la primera tenemos un servidor WEB y en la segunda usamos el navegador Firefox para acceder a la página WEB de la primera. ¿La conectividad NAT definida permite que ambas máquinas se puedan conectar entre sí para intercambiarse la página WEB?

Respuesta:

- A. Si, ya que las máquinas virtuales siempre pueden verse entre sí independientemente de su configuración de red.
- B. Si, ya que en adaptador puente como en NAT, se permite la conectividad entre máquinas virtuales.
- C. No, porque las máquinas virtuales configuradas como NAT solo permiten conectividad hacia Internet y no entre ellas.**
- D. Si, porque la configuración NAT permite conectividad entre máquinas virtuales.

**Pregunta 4 (0,5 puntos):** Las funcionalidades de filtrado de Wireshark son muy potentes y nos permiten p.e. filtrar por IP. ¿Qué tráfico capturaría el siguiente filtro ip.src==192.168.20.4 && ip.src==192.168.20.5 ?

Respuesta:

- A. Los paquetes cuyas IP origen sea 192.168.20.4 y los paquetes cuya IP origen sea 192.168.20.5
- B. Ningún paquete porque no hay ningún paquete que cumpla la condición de tener dos IP origen**
- C. Los paquetes cuyas IP destino sea 192.168.20.4 y los paquetes cuya IP destino sea 192.168.20.5
- D. Los paquetes cuya IP origen sea 192.168.20.4 y cuya IP destino sea 192.168.20.5

**Pregunta 5 (0,5 puntos):** El servicio o demonio INETD lo utilizan los sistemas Linux para...

Respuesta:

- A. ...los demonios INETD y Stand Alone son exactamente lo mismo, es decir, son aplicaciones servidoras. La diferencia es que Linux los llama INETD y Widows Stand Alone.
- B. ...el demonio INETD los utiliza Linux para instalar las aplicaciones clientes, en cambio usa los Stand Alone para las servidoras.
- C. ...hacer óptima la ejecución de las aplicaciones servidoras, arrancando los servicios sólo cuando hay peticiones de los clientes.**
- D. Son correctas todas las anteriores.

**Pregunta 6 (0,5 puntos):** En la siguiente conexión HTTP/TCP, ¿cuáles son los paquetes del cierre de la conexión o TearDown?

No.	Time	Source	Destination	Protocol	Length	Info
727	2023-11-28 14:47:30,00000000	19.1.207.41	10.1.207.38	TCP	74	SYN [SYN] Seq=0 Win=65168 Len=40 SACK_PERM=1 TSeq=130453
728	2023-11-28 14:47:30,0000453	10.1.207.38	10.1.207.41	TCP	66	SYN [ACK] Seq=1 Win=65168 Len=40 SACK_PERM=1 TSeq=130453
729	2023-11-28 14:47:30,6999397	10.1.207.38	10.1.209.41	HTTP	522	GUTT / HTTP/1.1
730	2023-11-28 14:47:30,6405931	10.1.203.41	10.1.207.38	TCP	66	HTTP/1.1 200 OK (text/html)
731	2023-11-28 14:47:30,64138962	10.1.203.41	10.1.207.38	HTTP	3926	HTTP/1.1 200 OK (text/html)
732	2023-11-28 14:47:30,64191812	10.1.207.38	10.1.206.41	TCP	66	SYN [SYN] Seq=0 Win=62592 Len=40 SACK_PERM=1 TSeq=130457
733	2023-11-28 14:47:30,64246	10.1.206.41	10.1.207.38	TCP	66	SYN [ACK] Seq=1 Win=62592 Len=40 SACK_PERM=1 TSeq=130457
1329	2023-11-28 14:47:35,6451034	10.1.207.38	10.1.203.41	TCP	66	SYN [SYN] Seq=0 Win=64128 Len=40 SACK_PERM=1 TSeq=130457
1330	2023-11-28 14:47:35,6409691	10.1.203.41	10.1.207.38	TCP	66	SYN [ACK] Seq=1 Win=64128 Len=40 SACK_PERM=1 TSeq=130457
1331	2023-11-28 14:47:35,6481102	10.1.207.38	10.1.203.41	TCP	66	SYN [SYN] Seq=0 Win=64128 Len=40 SACK_PERM=1 TSeq=130457
					58	SYN [ACK] Seq=1 Win=64128 Len=40 SACK_PERM=1 TSeq=130457

Respuesta:

- A. Paquetes No. 1329 y 1330.
- B. Paquete No. 731.
- C. Paquetes No. 1329, 1330 y 1331.**
- D. Paquetes No. 732, 1329, 1330 y 1331.

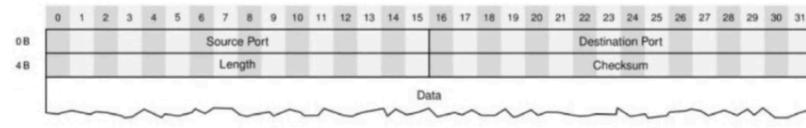
**Pregunta 7 (0,5 puntos):** En el siguiente mensaje TCP están activos los flags SYN y ACK. ¿Qué significa que estos flags estén activos?

```
[TCP Segment Len: 0]
Sequence Number: 0 (relative sequence number)
Sequence Number (raw): 1287326401
[Next Sequence Number: 1 (relative sequence number)]
Acknowledgment Number: 1 (relative ack number)
Acknowledgment number (raw): 1019374685
1010 .... = Header Length: 40 bytes (10)
Flags: 8x012 (SYN, ACK)
    000. .... .... = Reserved: Not set
    ...0.... .... = Nonce: Not set
    ....0.... .... = Congestion Window Reduced (CWR): Not set
    ....0.... .... = ECN-Echo: Not set
    ....0.... .... = Urgent: Not set
    ....1.... .... = Acknowledgment: Set
    ....0.... .... = Push: Not set
    ....0.... .... = Reset: Not set
    ....1.... .... = Syn: Set
    ....0.... .... = Fin: Not set
```

Respuesta:

- A. Tener activo SYN y ACK significa que se recibió una petición de conexión TCP, a lo que se contesta pidiendo conectarme también (SYN) además de aceptarle su conexión (ACK).
- B. Que se han recibido los paquetes correctamente (SYN) y se están confirmando (ACK).
- C. En todos los paquetes TCP van activos para indicar que es una conexión orientada a la conexión.
- D. Se utilizan para cerrar la conexión, este procedimiento se denomina Tear Down.

**Pregunta 8 (0,5 puntos):** Sabemos por teoría que el protocolo de transporte TCP es más confiable que el UDP porque tiene la capacidad de recuperar paquetes perdidos y eliminar los duplicados gracias a los números de secuencia. El UDP no tiene esas capacidades, pero si es capaz de saber si un paquete ha llegado corrupto (la información que se ha enviado es diferente a la recibida). Analizando la cabecera UDP que se muestra a continuación, ¿en qué campos se apoya UDP para hacer esa comprobación?



Fuente: <https://www.edx.org/es/course/lab-the-internet-masterclass>

Respuesta:

- A. Si la diferencia entre el puerto origen y el puerto destino es igual al checksum el paquete ha llegado bien.
- B. Si el campo Data tiene un número de bytes igual al que indica el campo Length, el paquete ha llegado correctamente.
- C. Hace una suma de verificación con la información recibida y el campo checksum, en función de su resultado puede determinar si el paquete ha llegado corrupto o no.
- D. UDP es muy sencillo y no tiene la capacidad de detectar si un paquete ha llegado corrupto.

**Pregunta 9 (0,5 puntos):** Si realizamos una conexión WEB entre nuestro navegador (en una máquina virtual) y un servidor WEB (que está en una máquina virtual diferente) que tiene actualmente sus puertos HTTP y HTTPS cerrados, si traceamos el intercambio de mensajes con el Wireshark, ¿qué esperamos ver?

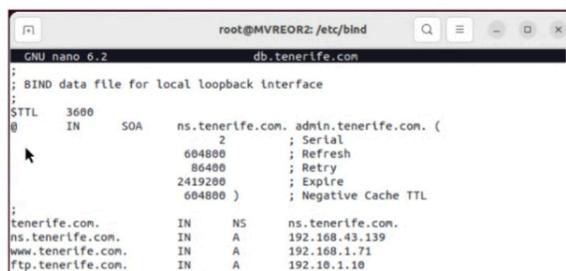
-:-

---

Respuesta:

- A. Todo el proceso de intercambio de paquetes esperado, es decir, conexión (three way handshake), intercambio de información y cierre de la conexión (four way handshake) ya que cuando llega la petición del cliente, aunque el puerto esté cerrado el servidor al ver la petición lo abre.
- B.** Un paquete de intento de conexión SYN del cliente al servidor y un mensaje de rechazo RST del servidor al cliente.
- C. No se ve ningún paquete porque al estar el puerto cerrado no se genera ningún tráfico.
- D. Solo se ve el proceso de cierre de conexión o Tear Down al estar el puerto cerrado.

**Pregunta 10 (0,5 puntos):** Tenemos un DNS cuyo fichero zona incluye la configuración que se muestra en la imagen. Si quiero incluir un nuevo subdominio denominado **ssh.tenerife.com** que apunte a la IPv4 **80.27.30.10**. ¿Qué línea tengo que incluir en dicho fichero?



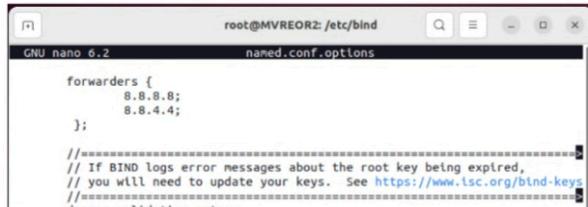
```
root@MVREORZ:/etc/bind
GNU nano 6.2          db.tenerife.com
;
; BIND data file for local loopback interface
;
$TTL    3600
@      IN      SOA     ns.tenerife.com. admin.tenerife.com. (
                      2                   ; Serial
                      604800              ; Refresh
                      86400               ; Retry
                      2419200              ; Expire
                      604800 )              ; Negative Cache TTL
;
tenerife.com.        IN      NS      ns.tenerife.com.
ns.tenerife.com.    IN      A       192.168.43.139
www.tenerife.com.   IN      A       192.168.1.71
ftp.tenerife.com.   IN      A       192.168.1.10
```

---

Respuesta:

- A. ssh.tenerife.com IN A 80.27.30.10
- B. ssh.tenerife.com. IN AAAA 80.27.30.10
- C. ssh.tenerife.com. IN NS 80.27.30.10
- D.** ssh.tenerife.com. IN A 80.27.30.10

**Pregunta 11 (0,5 puntos):** En el fichero de configuración `named.conf.options` de nuestro servidor de DNS se ha definido el parámetro `forwarders` con los valores 8.8.8.8 y 8.8.4.4 (ver figura adjunta). ¿Qué función tienen estas dos IP?



```
root@MVREOR2: /etc/bind
GNU nano 6.2          named.conf.options

forwarders {
    8.8.8.8;
    8.8.4.4;
};

//=====
// If BIND logs error messages about the root key being expired,
// you will need to update your keys. See https://www.lsc.org/bind-keys
=====
```

---

Respuesta:

- A. Son los DNS a los que nuestro servidor enviará todas aquellas consultas que él no sepa resolver.
- B. Son los DNS de Google y con esta configuración hacemos que nuestro servidor los utilice para todas sus resoluciones de DNS.
- C. Están solo por seguridad, si nuestro servidor deja de funcionar enviará todas las consultas a estos dos DNS.
- D. No tienen ningún impacto, ya que nuestro DNS siempre resolverá las consultas con los datos que tiene en el fichero de zona.

**Pregunta 12 (0,5 puntos):** Ejecutamos dos consultas a nuestro DNS (192.168.43.139) mediante el comando nslookup. Una a la URL [www.tenerife.com](http://www.tenerife.com) y otra a [www.tenerife.es](http://www.tenerife.es) (ver figura adjunta). ¿Por qué en la segunda consulta se devuelve el mensaje *Non-authoritative answer*?



```
root@MVREOR2: /etc/bind#
root@MVREOR2: /etc/bind# nslookup www.tenerife.com 192.168.43.139
Server:      192.168.43.139
Address:   192.168.43.139#53

Name: www.tenerife.com
Address: 192.168.1.71

root@MVREOR2: /etc/bind#
root@MVREOR2: /etc/bind# nslookup www.tenerife.es 192.168.43.139
Server:      192.168.43.139
Address:   192.168.43.139#53

Non-authoritative answer:
www.tenerife.es canonical name = pxpyro.tenerife.es.
Name: pxpyro.tenerife.es
Address: 212.170.134.107

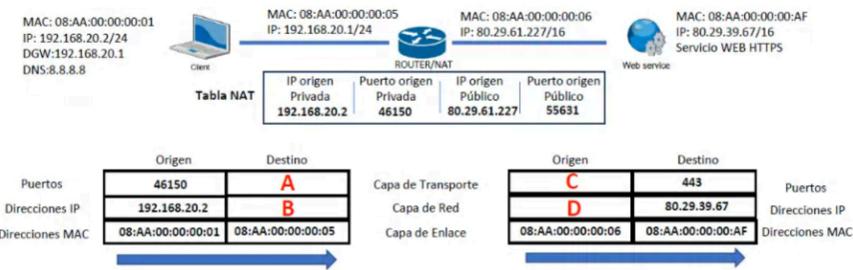
root@MVREOR2: /etc/bind#
```

---

Respuesta:

- A. Significa que no estamos autorizados a realizar esa consulta.
- B.** Indica que nuestro DNS (192.168.43.139) no tiene definido ese dominio y tiene que preguntarlo a otro DNS.
- C. Significa que la IP que nos devuelve no estamos autorizados a utilizarla.
- D. Indica que la IP que nos devuelve de la resolución es una IP pública.

**Pregunta 13 (0,5 puntos):** En el esquema de red que se muestra a continuación el portátil está navegando por HTTPS hacia el servidor WEB. Si consideramos los paquetes de red que van en sentido Cliente → Servidor, elija los campos (A, B, C y D: puertos e IP) que faltan en dichos paquetes apoyándose en la información facilitada en la figura. (**Ojo que el router hace NAT, traduciendo tanto direcciones como puertos, para salir a Internet.**)



Respuesta:

- A. A=443, B=80.29.61.227, C=55631, D=80.29.61.227
- B.** A=443, B=80.29.39.67, C=55631, D=80.29.61.227
- C. A=55631, B=80.29.61.227, C=55631, D=80.29.39.67
- D. A=4150, B=192.168.20.2, C=443, D=80.29.39.67

**Pregunta 14 (0,5 puntos):** En la figura adjunta, se presenta el proceso DORA (Discover, Offer, Request y Ack) que utiliza el protocolo DHCP para asignar IP y otros parámetros de conectividad. Analizando dicha figura, ¿qué IP se asigna al cliente y qué IP tiene el servidor de DHCP?

dhcp.id == 0x40815b0d						
No.	Time	Source	Destination	Protocol	Length	Info
2152	2023-11-28 15:05:30,1578386	0.0.0.0	255.255.255.255	DHCP	333	DHCP Discover - Transaction ID 0x40815b0d
2153	2023-11-28 15:05:30,1580694	10.0.2.2	10.0.2.15	DHCP	590	DHCP Offer - Transaction ID 0x40815b0d
2154	2023-11-28 15:05:30,1581761	0.0.0.0	255.255.255.255	DHCP	339	DHCP Request - Transaction ID 0x40815b0d
2155	2023-11-28 15:05:30,1583970	10.0.2.2	10.0.2.15	DHCP	590	DHCP ACK - Transaction ID 0x40815b0d

Respuesta:

- A. Se asigna al cliente la IP=10.0.2.2 y el servidor tiene la IP=255.255.255.255
- B. Se asigna al cliente la IP=0.0.0.0 y el servidor tiene la IP=255.255.255.255
- C.** Se asigna al cliente la IP=10.0.2.15 y el servidor tiene la IP=10.0.2.2
- D. Se asigna al cliente la IP=10.0.2.2 y el servidor tiene la IP=10.0.2.15

**Pregunta 15 (0,5 puntos):** Analizando el mensaje DHCP ACK que se presenta a continuación. ¿Qué IP, qué máscara y qué servidores de DNS se asignan al cliente?

```
Client IP address: 10.0.2.15
Your (client) IP address: 10.0.2.15
Next server IP address: 10.0.2.4
Relay agent IP address: 0.0.0.0
Client MAC address: PcsCompu_AC:19:af (08:00:27:ac:19:af)
Client hardware address padding: 000000000000000000000000
Server host name not given
Boot file name: MV_REOR_1.pxe
Magic cookie: DHCP
> Option: (53) DHCP Message Type (ACK)
> Option: (1) Subnet Mask (255.255.255.0)
> Option: (3) Router
    Length: 4
    Router: 10.0.2.2
> Option: (6) Domain Name Server
    Length: 8
    Domain Name Server: 10.5.0.225
    Domain Name Server: 10.5.0.220
> Option: (15) Domain Name
> Option: (51) IP Address Lease Time
> Option: (54) DHCP Server Identifier (10.0.2.2)
```

Respuesta:

- A. IP cliente=10.0.2.15, mascara=/24, DNS=10.5.0.255 y 10.5.0.220
- B. IP cliente=10.0.2.15, mascara=255.255.0.0, DNS=10.5.0.255 y 10.5.0.220
- C. IP cliente=10.0.2.15, mascara=0.0.0.0, DNS=10.0.2.2
- D. IP cliente=10.0.2.15, mascara=0.0.0.0, DNS=10.5.0.255 y 10.5.0.220

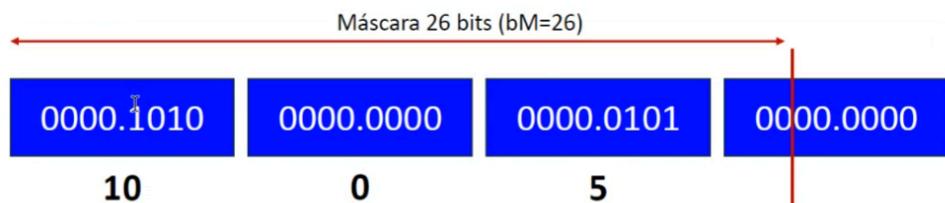
**Pregunta 16 (0,5 puntos):** Desde el equipo 10.1.207.38 estamos haciendo un scan TCP al puerto 80 del equipo 10.1.203.41 mediante el comando nmap. Analizando los mensajes que presentan en la figura siguiente, ¿qué tipo de escaneo estamos haciendo?

ip.addr==10.1.203.41					
No.	Time	Source	Destination	Protocol	Length Info
160	4.236670649	10.1.207.38	10.1.203.41	TCP	74 59618 - 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
161	4.237998664	10.1.203.41	10.1.207.38	TCP	74 80 - 59618 [SYN, ACK] Seq=0 Ack=1 Win=65168 Len=0 MSS=1460 SACK_PERM=1
162	4.238188941	10.1.207.38	10.1.203.41	TCP	66 59618 - 80 [ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=324010360 TStamp=324010360
163	4.238819719	10.1.207.38	10.1.203.41	TCP	66 59618 - 80 [RST, ACK] Seq=1 Ack=1 Win=64256 Len=0 TSval=324010360 TStamp=324010360

Respuesta:

- A. UDP scan mediante el comando nmap -p80 -sU 10.1.203.41
- B. Full scan mediante el comando nmap -p80 -sT 10.1.203.41
- C. Half scan mediante el comando nmap -p80 -sS 10.1.203.41
- D. Full scan mediante el comando nmap -p80 -sT 10.1.207.38

**Pregunta 17 (0,5 puntos):** Si nos asignan el rango de direcciones IP 10.0.5.0/24 (**solo podemos utilizar este rango**) y elegimos una máscara de 26 bits. ¿Cuántas redes diferentes podemos construir y cuantos hosts podemos conectar en cada una de ellas?



---

Respuesta:

- A. Podemos construir  $2^2=4$  redes y conectar  $2^{(32-bM)}=2^6=64$  hosts.
- B. Podemos construir 1 red y conectar  $2^{(32-bM)}-2=2^6-2=64-2=62$  hosts.
- C. Podemos construir  $2^2=4$  redes y conectar  $2^{(32-bM)}-2=2^6-2=64-2=62$  hosts.
- D. Podemos construir  $2^{26}=67.108.864$  redes y conectar  $2^{(32-bM)}-2=2^6-2=64-2=62$  hosts.

**Pregunta 18 (0,5 puntos):** Al realizar un ping desde nuestro equipo cuya dirección IP es 192.168.1.14 a otro cuya dirección es 8.8.8.8 (DNS de Google) recibimos un mensaje ICMP de “time to live exceeded”. Explique qué puede estar pasando para que recibamos esa respuesta. **Ayuda:** Recuerde que los paquetes IP llevan un campo denominado TTL (normalmente se generan con valor 64) que va disminuyendo su valor a medida que este paquete va atravesando los diferentes *routers* de Internet.

---

Respuesta:

- A. Al hacer una consulta al DNS, éste en su fichero de zona no tiene definido el parámetro TTL.
- B. Son mensajes de control que envía el protocolo ICMP para indicar que los nodos están operativos.
- C. Que el paquete ha llegado al límite de saltos indicado en el campo TTL de la cabecera IP y ha sido descartado.
- D. Google suele enviar estos mensajes de vez en cuando para indicar que están sondeándote.

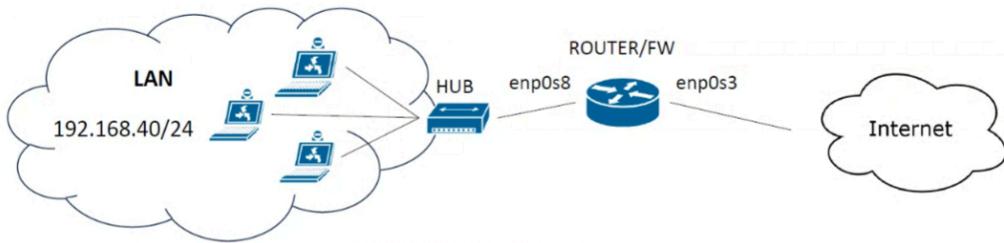
**Pregunta 19 (0,5 puntos):** El protocolo ARP se usa dentro de las LAN para resolver las direcciones IP, es decir, saber que MAC le corresponde a un IP determinada. Analizando la siguiente figura, ¿por qué se una MAC de broadcast en el mensaje de solicitud y qué MAC tiene el nodo cuya IP es 10.0.0.21?

No.	Time	Source	Destination	Protocol	Length	Info
5	16.565972...	00:00:00_aa:00:00	Broadcast	ARP	42	Who has 10.0.0.21? Tell 10.0.0.20
6	16.565993...	00:00:00_aa:00:01	00:00:00_aa:00:00	ARP	42	10.0.0.21 is at 00:00:00:aa:00:01

Respuesta:

- A. Se usa una MAC de broadcast para que solo vaya al nodo objetivo dentro de la LAN. A la IP 10.0.0.21 le corresponde la MAC 00:00:00:aa:00:00.
- B. Se usa una MAC de broadcast para poder consultar a todos los nodos de la LAN. A la IP 10.0.0.21 le corresponde la MAC Broadcast.
- C. Se usa una MAC de broadcast para solo vaya al nodo objetivo dentro de la LAN. A la IP 10.0.0.21 le corresponde la MAC 00:00:00:aa:00:01.
- D. Se usa una MAC de broadcast para poder consultar a todos los nodos de la LAN. A la IP 10.0.0.21 le corresponde la MAC 00:00:00:aa:00:01.

**Pregunta 20 (0,5 puntos):** Suponiendo que el router/firewall de la figura tienen definida la política por defecto de la cadena FORWARD (**iptables -t filter -P FORWARD DROP**), ¿qué reglas tendrá que definir para que los equipos de la LAN puedan navegar con protocolo HTTPS en Internet (browser en la LAN y Servidor WEB en Internet)?



Respuesta:

- A. 

```
iptables -t filter -A FORWARD -s 192.168.40/24 -o enp0s3 -p tcp --dport 443 -j ACCEPT
iptables -t filter -A FORWARD -i enp0s3 -d 192.168.40/24 -p tcp --sport 443 -j ACCEPT
```
- B. 

```
iptables -t filter -A FORWARD -i enp0s3 -d 192.168.40/24 -p tcp --dport 443 -j ACCEPT
iptables -t filter -A FORWARD -s 192.168.40/24 -o enp0s3 -p tcp --sport 443 -j ACCEPT
```
- C. 

```
iptables -t filter -A FORWARD -s 192.168.40/24 -o enp0s3 -p udp --dport 53 -j ACCEPT
iptables -t filter -A FORWARD -i enp0s3 -d 192.168.40/24 -p udp --sport 53 -j ACCEPT
```
- D. 

```
iptables -t filter -A FORWARD -s 192.168.40/24 -o enp0s3 -p tcp --dport 22 -j ACCEPT
iptables -t filter -A FORWARD -i enp0s3 -d 192.168.40/24 -p tcp --sport 22 -j ACCEPT
```

