Escuela de
Ingeniería y Arquitectura
Universidad Zaragoza

dar-pr-0

Diseño y administración de redes

Autor 1:	Toral Pallás, Héctor - 798095
Autor 2:	Martínez Lahoz, Sergio - 801621
Grado:	Ingeniería Informática
Curso:	2022-2023

18 de septiembre de 2023

Índice

01

Pregunta 1

Deberemos entregar la captura (obtenida mediante wireshark) correspondiente a la configuración DHCP del servidor GNS3 VM y dar una breve descripción de su funcionamiento. Para ello debemos escoger convenientemente en qué interfaz capturar y justificarlo adecuadamente en el informe. También deberemos explicar para qué sirve esta configuración DHCP y en qué situaciones prevemos que se use una comunicación a dicho servidor. Es necesario apoyar las explicaciones con una captura de ejemplo de uso.

En esta pregunta, hemos tenido la oportunidad de analizar el tráfico que ocurre cuando se realiza una solicitud DHCP, donde hemos podido observar cómo el router asigna una dirección IP a una máquina.

En la captura "DAR2324_Pr0_g2_P1_virt.pcapng", se pueden identificar los paquetes [90, 91, 97, 98, 99], que representan todo el proceso para alcanzar este objetivo.

90	258.153536	0.0.0.0	255.255.255.255	DHCP	320	DHCP Discover - Transaction ID 0x4368014a
91	258.153600	192.168.79.254	192.168.79.145	ICMP	62	Echo (ping) request id=0xd47a, seq=0/0, ttl=16 (no response found!)
92	258.153622	VMware_f3:a4:94	Broadcast	ARP	42	Who has 192.168.79.145? Tell 192.168.79.2
93	258.163555	::	ff02::16	ICMPv6	130	Multicast Listener Report Message v2
94	258.729283	::	ff02::16	ICMPv6	130	Multicast Listener Report Message v2
95	258.761210	::	ff02::1:ff59:2be6	ICMPv6	86	Neighbor Solicitation for fe80::20c:29ff:fe59:2be6
96	259.153994	VMware_f3:a4:94	Broadcast	ARP	42	Who has 192.168.79.145? Tell 192.168.79.2
97	259.154072	192.168.79.254	192.168.79.145	DHCP	342	DHCP Offer - Transaction ID 0x4368014a
98	259.154318	0.0.0.0	255.255.255.255	DHCP	332	DHCP Request - Transaction ID 0x4368014a
99	259.154409	192.168.79.254	192.168.79.145	DHCP	342	DHCP ACK - Transaction ID 0x4368014a

Figura 1: Secuencia DHCP

En el paquete número 90, se aprecia que una máquina sin dirección IP previamente asignada realiza una solicitud broadcast mediante el protocolo DHCP con el mensaje "discover". A continuación, el router emite un ping para verificar si la dirección 192.168.79.145 está ocupada o en uso. Dado que no se recibe respuesta, el router ofrece la dirección 192.168.79.145 a través del protocolo DHCP en el paquete 97. Luego, en los dos paquetes siguientes, se muestra cómo la máquina sin dirección IP realiza una solicitud broadcast, y finalmente, se observa cómo el router le asigna la dirección disponible mediante un mensaje "ACK".

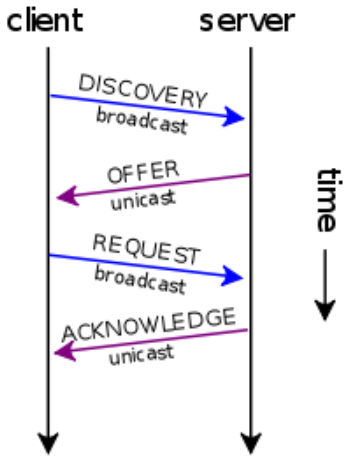

Figura 2: Diagrama DHCP

La configuración DHCP se utiliza para asignar automáticamente direcciones IP a dispositivos en una red. Esta configuración es útil en situaciones donde se necesite una gestión eficiente de direcciones IP, como en redes locales, para evitar conflictos de direcciones IP y simplificar la administración de dispositivos.

[1]

[1] Figura 4: https://www.zonasystem.com/2018/05/nmap-dhcp-discover-conocer-servidores-dhcp.html

02

Pregunta 2

Vamos a configurar un escenario simple compuesto por dos VPC conectados entre sí. Ejecutamos un ping entre los VPC mientras capturamos con wireshark, tanto en el interfaz adecuado de la máquina real como en el propio escenario. La captura deberá ir acompañada del correspondiente informe en el que se expliquen los protocolos y puertos utilizados en la comunicación y también la comparación de la captura del ping cuando lo capturamos en la máquina real y en el escenario GNS3.

Escenario 1: GNS3

La captura almacenada en el archivo denominado "DAR2324_Pr0_g2_P2_virt_eth0.pcapng" corresponde a la captura realizada desde el entorno virtual. En dicho archivo, es posible observar de manera directa cada uno de los paquetes generados al ejecutar el comando 'ping'. En esta captura, se pueden identificar claramente todos los paquetes de solicitud y respuesta del protocolo ICMP (Internet Control Message Protocol).

Además, es relevante destacar que en el paquete número 3 de la captura, al explorar el menú desplegable correspondiente al protocolo ICMP, se puede observar que el campo 'type' tiene un valor de 8. Este valor indica que se trata de una solicitud 'echo ping request', de acuerdo con la especificación del protocolo ICMP.

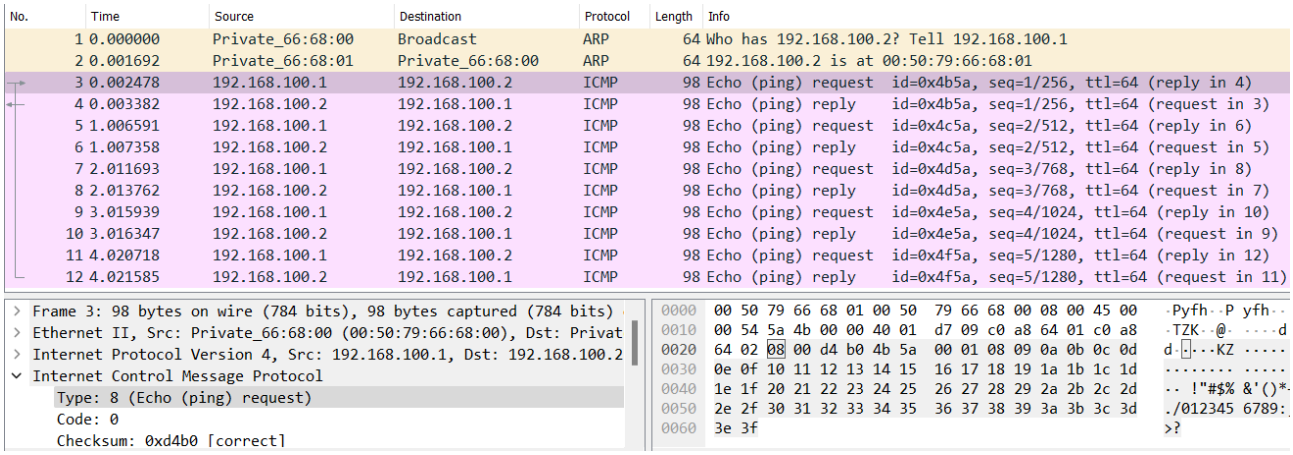

Figura 3: Captura escenario 1: GNS3

Escenario 2: Máquina Real

En este segundo escenario, tenemos la captura almacenada en el archivo denominado "DAR2324_Pr0_g2_P2_virt_lo.pcapng", en esta notamos la ausencia de tráfico ICMP, en su lugar, la gran mayoría del tráfico corresponde a los protocolos UDP y TCP. Con el objetivo de depurar la trama y concentrarnos en los paquetes de interés, hemos aplicado el siguiente filtro: (ip.addr eq 127.0.0.1 and ip.addr eq 127.0.0.1) and (udp.port eq 10002 and udp.port eq 10003). Es importante destacar que este filtro fue aplicado de manera similar en la captura del escenario anterior al momento de guardarla, por lo que solo se presentan estos datos filtrados.

Al analizar los resultados, observamos varias conclusiones, algunas más evidentes que otras. En primer lugar, debido a nuestro conocimiento previo de que GNS3 utiliza el protocolo UDP para la comunicación con sus máquinas virtuales, podemos confirmar que el tráfico actual es de tipo UDP. Además, al considerar que este tráfico está encapsulado, podemos inferir que el tamaño del paquete será igual al tamaño del tráfico detectado en el escenario anterior más un valor adicional debido a la encapsulación en UDP.

Por último, al inspeccionar el campo 'data', nuevamente podemos identificar el campo 'type' del paquete ICMP, que en el caso del paquete 151, por ejemplo, se identifica como una solicitud 'echo ping request'.

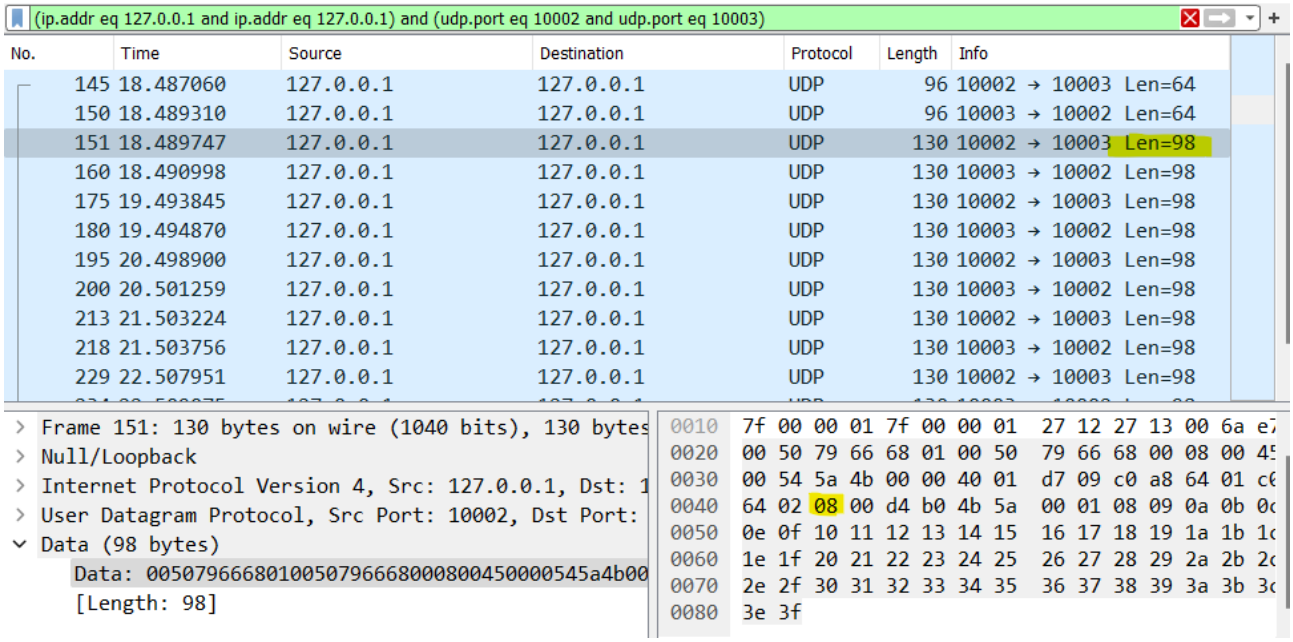

Figura 4: Captura escenario 2: Máquina Real

03

Pregunta 3

Vamos a configurar un escenario simple compuesto por un VPC con una dirección IP pública que sea la reservada a la máquina virtual (usando la del interfaz físico de la máquina real pero sumándole 4 al último campo de la IP) conectado al cloud que nos permite conexión al exterior. Ejecutamos un ping a la IP de una máquina real (por ejemplo del router por defecto de la red del laboratorio) mientras capturamos, en la máquina real, con wireshark, en el interfaz adecuado y comprobamos que funciona. Sin embargo, no podemos hacer un ping desde VPC a la dirección IP del servidor GNS3 VM. Justifica teóricamente por qué y explica qué sucede en base a una captura de tráfico que hagamos mientras se ejecuta el ping. Será conveniente comprobar la dirección MAC de cada VPC para asegurarnos de que no son la misma en los VPC de escenarios en PCs diferentes.

En la configuración de este escenario, se ha asignado una dirección IP (IP pública pc + 4) utilizando el siguiente comando para que la máquina VPC disponga de una dirección pública: "ip 155.210.157.134/24". Después de realizar un ping al router del laboratorio mediante el comando "ping 155.210.157.254", hemos confirmado que funciona correctamente. Esto es apreciable en el paquete 3330 de la captura "DAR2324_Pr0_g2_p3_real.pcapng".

```
3330 589.004705   155.210.157.134   155.210.157.254   ICMP   98 Echo (ping) request   id=0xbd15, seq=1/256, ttl=64 (reply in 3334)
3334 589.006605   155.210.157.254   155.210.157.134   ICMP   98 Echo (ping) reply     id=0xbd15, seq=1/256, ttl=64 (request in 3330)
```

Figura 5: Ping

No obstante, al intentar ejecutar un comando ping hacia la máquina GNS3 VM, hemos observado que no recibimos respuesta. De esta manera, deducimos que el comando ping envía un paquete ICMP de ida, pero no recibe uno de vuelta, lo que indica que el host es inalcanzable. Esta situación se debe a la incapacidad de acceder desde una red pública a una red privada a través de una configuración de NAT estática.

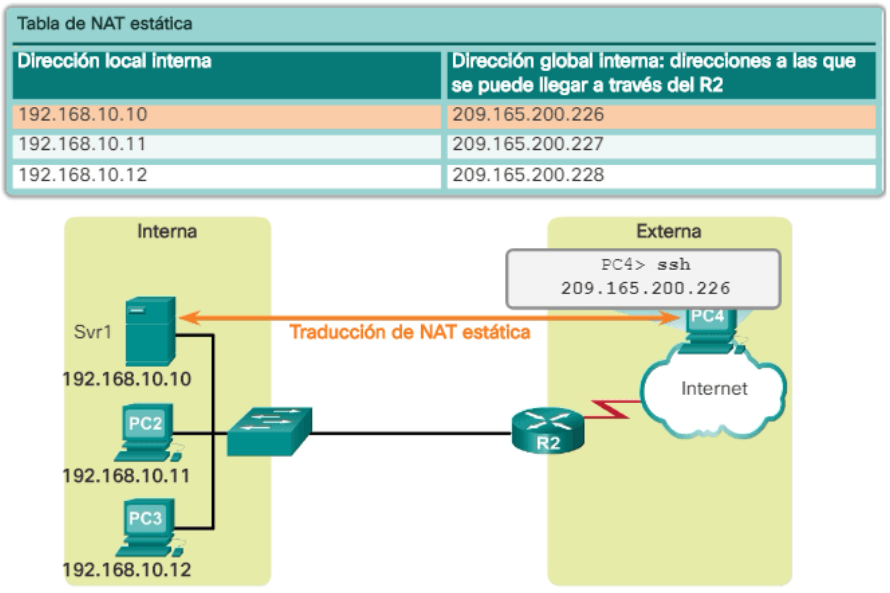

Figura 6: Ejemplo de NAT estático

[2]

[2]Figura 6: https://ccnadesdecero.es/tipos-ventajas-desventajas-de-nat/

04

Pregunta 4

Creamos a continuación un nuevo escenario sustituyendo VPC por OvS, fijándonos en qué servidor se lanza OvS y comprobando el correcto funcionamiento del escenario. Si vamos apurados de tiempo, no será necesaria la comprobación del funcionamiento.

En esta sección, comenzamos reemplazando la máquina VPC por Open vSwitch (OvS) y lo implementamos dentro de un contenedor de Docker. Durante el proceso de descarga de la imagen, es importante destacar que se muestran las credenciales de acceso que permiten la entrada.

Una vez dentro del servidor, configuramos la dirección IP utilizando el comando “ip addr add 155.210.157.134/24 dev eth1”. Finalmente, para verificar el correcto funcionamiento de la configuración, realizamos un ping hacia la máquina de un compañero, lo que nos permitió confirmar que todo estaba operando según lo previsto.

05

Pregunta 5

Vamos a configurar un escenario simple compuesto por un PC virtualBox con una dirección IP (que sea la reservada a la máquina virtual; la misma de la máquina real pero sumándole 4 al último campo de la IP) en un interfaz que esté conectado al exterior mediante la configuración virtualBox. Ejecutamos un ping a la IP del PC virtualBox del escenario del compañero mientras capturamos, en la máquina real, con wireshark, en el interfaz adecuado. ¿Por qué, ahora, no usamos el cloud para conectarnos al exterior? Razona la respuesta.

En primer lugar, para configurar el escenario, hemos realizado los siguientes pasos:

- Asignamos una dirección IP estática a la máquina virtual VBox utilizando el siguiente comando: "ip addr add 155.210.157.134/24 dev eth1". De esta manera, hemos establecido la dirección IP "155.210.157.134" en la interfaz de red "eth1" de la máquina virtual.
- A continuación, iniciamos una captura de paquetes en la interfaz de red eth0 en el fichero "DAR2324_Pr0_g2_P5_real.pcap y ejecutamos un comando "ping" hacia la dirección IP del PC virtualBox de nuestro compañero, como parte de la prueba de conectividad.

Es importante destacar que en este escenario no estamos utilizando recursos en la nube, ya que VirtualBox está configurado con una tarjeta de red definida como "adaptador puente", lo que permite la comunicación directa entre la máquina virtual y la red física, realizando la traducción de direcciones necesaria de forma automática.

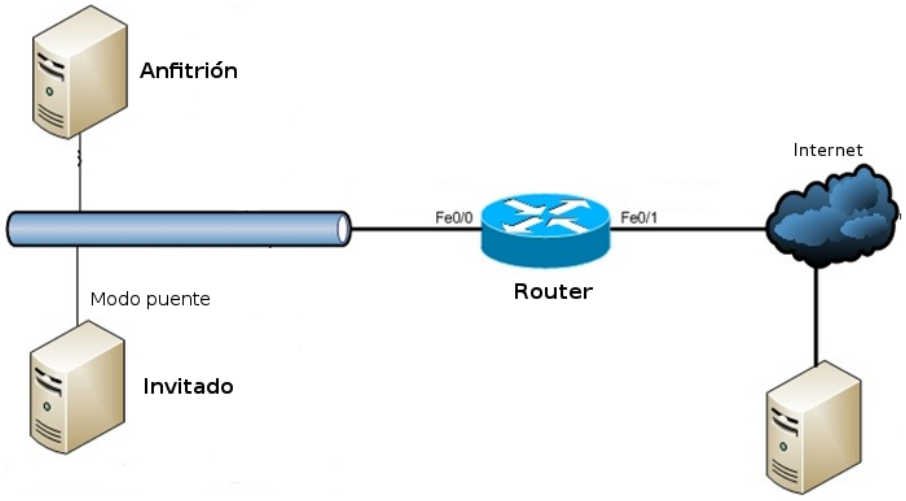

Figura 7: Adaptador puente

[3]

[3]Figura 7: https://www.fpgenred.es/VirtualBox/modo$_a daptador_p uente.html$

06

Vocabulario

- **Hub** Es un hub Ethernet que viene con el propio GNS3. Dispone de 8 conexiones Ethernet a las que podemos conectar los diferentes elementos de nuestro escenario.
- **Switch** Es un switch Ethernet que viene con el propio GNS3 y tiene las funciones básicas de conmutación Ethernet, además de la posibilidad de utilizar VLAN. Dispone, por defecto, de 8 conexiones Ethernet
- **VPC** Es un PC virtual muy simple que lo usaremos para conectividad IPv4.
- **Cloud** Es el dispositivo que va a permitir que nuestro escenario tenga conexión al exterior mediante la utilización de las interfaces Ethernet fijas del ordenador donde está instalado GNS3.
- **OpenvSwitch-management** Es un software que puede instalarse sobre diferentes sistemas operativos y permite el uso de funciones avanzadas de LAN-switch controladas desde un equipo externo llamado controlador.
- **Adaptador puente** Es una de las configuraciones posibles que define Virtual Box y que simula que la tarjeta virtual está conectada al mismo switch que la tarjeta física del anfitrión, por lo tanto, la MV se va a comportar como si fuese un equipo más dentro de la misma red física en la que está el equipo anfitrión.