Práctica 0
Introducción a GNS3. Pruebas controladas.

Informe

Dorian Boleslaw Wozniak (817570@unizar.es)

Lunes, 18 de septiembre de 2023

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.

¿Cómo funciona la configuración DHCP?

La configuración mediante DHCP consta de dos pasos: **descubrimiento** y **diálogo**. Este proceso se puede observar en la captura de red `DAR2324_Pr0_g1_P1_captura.pcapng`.

El primer paso se puede observar en las tramas nº 1 y 7 de la captura. Si un equipo nuevo se conecta a la red sin tener una configuración válida, enviará un mensaje de difusión (*broadcast*) a todos los equipos de la red local (255.255.255.255), con una IP de arranque no específica (0.0.0.0) para encontrar un servidor DHCP (**DHCP Discover**). El servidor contestará con una dirección IP disponible (**DHCP Offer**), mediante *unicast* o *broadcast*, dependiendo si el cliente soporta recibir comunicaciones *unicast* sin configuración. En este caso, un servidor localizado en 192.168.79.254 (el servidor DHCP de la red de VMWare) envía una respuesta a la IP 192.168.79.146, pero hay que tener en cuenta que aún no se ha confirmado la IP del cliente.

El segundo paso se puede observar en las tramas 8 y 9. Una vez el cliente recibe el mensaje, volverá a difundir una solicitud desde una IP no especificada, esta vez para confirmar la reserva de la dirección IP (**DHCP Request**). En la opción 50 se encuentra la IP solicitada. Si al recibir el servidor la solicitud comprueba que es la IP que envió, mandará un mensaje de acuse al cliente (**DHCP ACK**). En caso contrario, enviaría un mensaje **DHCP NOACK** y habría que repetir el proceso.

¿En qué interfaz se captura?

En la red `vmnet8`. La máquina virtual del servidor de GNS3 está conectada a la red interna de VMWare, un *software* de virtualización. El tráfico entre las máquinas virtuales se realiza sobre una interfaz virtual dentro de la máquina real.

¿Para qué sirve una configuración DHCP y cuando hay que comunicarse con el servidor?

DHCP sirve para configurar automáticamente dispositivos dentro de una red, negociando con ellos una dirección IP, ya sea una dirección estática o una dinámica que puede cambiar con el tiempo.

Las direcciones IP otorgadas por DHCP no lo son de forma indefinida. Además de tener que comunicarse con el servidor para la configuración inicial, al negociar la dirección también se ha enviado un tiempo de “alquiler” (*lease*). Antes de agotarse este tiempo, el cliente enviará un mensaje **DHCP Release** al servidor, y tendrá que obtener una nueva dirección con el protocolo anterior. También existe un tiempo de expiración (*timeout*) en caso de perderse la comunicación con el cliente durante un tiempo.

En la trama 8 (DHCP ACK), se puede observar el tiempo de cesión de en la opción 51. En este caso, el préstamo es de 30 minutos, tras los cuales hay que renegociar la dirección.

Por otro lado, el paquete IP tiene un tiempo de vida (**TTL**) de 16.

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.

¿En qué interfaces se capturará el tráfico?

Se capturan dos interfaces: la interfaz correspondiente al tráfico interno del equipo real (*loopback*/127.0.0.1) y la interfaz definida por la conexión entre los dos VPCs del escenario de GNS3. GNS permite tener múltiples servidores simultáneamente, tanto sobre la máquina real, como es el caso de los VPCs, como sobre una máquina virtual (GNS3 VM), donde permite ejecutar entornos de virtualización como Docker con mejor rendimiento. Al ejecutarse los VPCs sobre la máquina real, el tráfico real se dirigirá a través del propio ordenador.

¿Qué protocolos y puertos se utilizan en la comunicación?

Los siguientes protocolos se pueden observar en las capturas `DAR2324_Pr0_g1_P2_real.pcapng` y `DAR2324_Pr0_g1_P2_virtual.pcapng`

En la interacción entre los dos equipos VPC, se utilizan una serie de protocolos. El más importante en el contexto del envío de *pings* es **ICMP**. Este protocolo se utiliza para comunicar situaciones de error e inusuales entre equipos. Uno de estas situaciones es la realización de solicitudes *echo*, es decir, un test de alcanzabilidad.

ICMP no utiliza el concepto de puertos. En la captura del tráfico virtual, se puede observar el intercambio de pings entre las máquinas 192.168.100.1 y .2, ambos VPCs, a partir de la trama 3.

Otro protocolo utilizado es **ARP**. Este protocolo sirve para generar una tabla de encaminamiento hacia distintos equipos alcanzables por la máquina origen, almacenando durante un tiempo su dirección IP y MAC.

En la captura virtual, antes de ejecutarse el ping, en las tramas 1 y 2 se puede observar una consulta ARP. El equipo .1 envía un mensaje de difusión a todos los equipos de la red preguntando cual es el equipo .2. El equipo .2 responde a continuación al equipo .1 con su dirección MAC. Hay que destacar que el encaminamiento corresponde al intercambio de tráfico entre interfaces de red y no equipos, por lo que el origen y destino se identifican por su dirección MAC, no su IP. Por la misma razón no utiliza puertos.

Finalmente, **UDP** es, junto a TCP, uno de los protocolos básicos de transmisión de información junto a TCP. A diferencia de este, UDP realiza el envío de datagramas sin conexión, es decir, sin garantías de que un mensaje llegue y en que orden.

¿Cómo se comparan las capturas de la máquina real con el escenario?

La interfaz virtual informará del tráfico de paquetes ICMP y ARP entre las dos máquinas. Sin embargo, las comunicaciones reales se realizan realmente mediante túneles UDP entre las dos máquinas.

En este caso, todo el tráfico entre ambos equipos VPC realmente se realizan sobre la interfaz *loopback*, es decir, sobre la máquina real. Este queda encapsulado en paquetes UDP y los envíos se realizan en los puertos 10000-10005. Además, los paquetes se expiden múltiples veces desde múltiples direcciones de una máquina a otra (.1 tiene asociados los puertos 10000, 10003 y 10004, y .2 los puertos 10001, 10002 y 10005). Se puede observar el tráfico ARP entre las tramas 189-194. La forma mas fácil de distinguirlo es porque la sección de datos del paquete es de 64 bytes, igual al tamaño de la trama ARP. Lo mismo con los mensajes ICMP, que pesan 98 bytes, y se puede observar en los paquetes UDP de 195 a 509.

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.

¿Por qué no se puede hacer *ping* a GNS3 VM?

De forma similar al escenario anterior, el equipo VPC se ejecuta sobre el servidor GNS sobre la máquina real. El elemento *cloud* permite asociar uno de los puertos reales de la máquina a uno de los dispositivos del escenario. Por otro lado, GNS3 VM se ejecuta en la red local de VMWare, que se ejecuta de forma aislada a la red interna del ordenador. Por tanto, los dos servidores GNS3 no están directamente comunicados y no se pueden “ver”.

En cuanto al tráfico, se puede observar en `DAR2324_Pr0_g1_P3_captura`, entre las tramas 49 y 72. Se observa peticiones y respuestas entre un equipo localizado en .101 y un router localizado en .254.

¿Seguro que no son los equipos del escenario anterior?

No. En caso de ser necesario, la dirección MAC se puede observar en el *frame* del protocolo Ethernet que encapsula el paquete ICMP. En este caso, el MAC del VPC es uno privado (00:50:79:66:68:00) y el del router se identifica como Routerboard/MikroTik (cc:2d:e0:02:e6:aa).

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.

El elemento OpenVSwitch es un *software* para poder convertir un ordenador en un *switch* controlable remotamente desde otra máquina. Esta máquina se ejecuta sobre GNS3 VM como un contenedor Docker. La configuración se realiza con el comando `ifconfig`.

Se puede observar el tráfico ICMP entre las tramas 17 a 74 en la captura `DAR2324_Pr0_g1_P4_captura`, entre el vSwitch (.101) y el router del laboratorio (.254).

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 qué interfaz se captura el tráfico?

Sobre la interfaz real Ethernet 1, como en los escenarios anteriores donde estaban conectados los equipos al elemento *cloud*. En la captura `DAR2324_Pr0_g1_P5_captura.pcapng`, se puede observar los envíos y respuestas ICMP entre el equipo Virtualbox, en la IP .102, y el router del laboratorio en .254 (no había otro equipo disponible en el momento); en las tramas entre la 74 y la 102.

¿Por qué no utilizar *cloud* con la máquina de Virtualbox?

La red de Virtualbox, de forma similar a VMWare y QEMU, ya dispone de una red interna que ofrece funcionalidades para asociar direcciones de máquinas virtuales a puertos de la máquina real, así como servicios como NAT. Por tanto, no es necesario utilizar cloud.