ENRUTAMIENTO CONVENCIONAL FRENTE A ENRUTAMIENTO CON NAT

33

1.- ENRUTAMIENTO CONVENCIONAL.

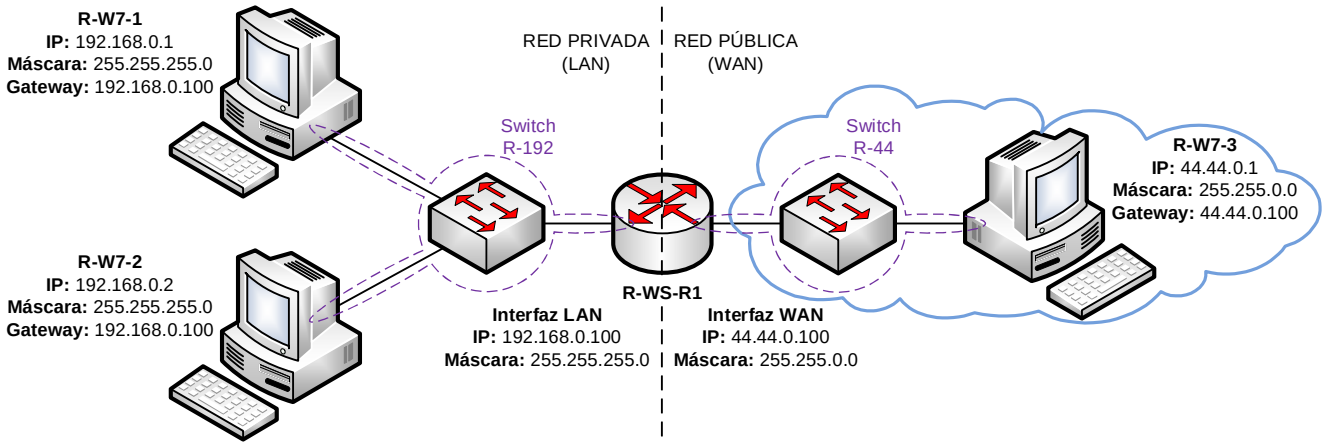


Figura 1

Para instalar el servicio de enrutamiento, en el R-WS-R1, en el supuesto de que no lo estuviera, procederemos de la forma siguiente:

> Inicio → Administrador del servidor [Herramientas administrativas → Administrador del servidor] → Hacer clic en la opción 2, "Agregar roles y características" → Botón "Siguiente" → Seleccionar la opción "Instalación basada en características o en roles" y botón "Siguiente" → Habilitar la opción "Seleccionar un servidor del grupo de servidores" y verificar que está seleccionado, en la lista de servidores, el R-WS-R1, botón "Siguiente" → Habilitar la opción "Acceso remoto", botón "Siguiente" → En el formulario "Seleccionar características", botón "Siguiente", para aceptar las características por defecto → En el formulario de "Acceso Remoto", botón "Siguiente" → En el formulario "Seleccionar servicios de rol" seleccionar "Enrutamiento" → En el formulario que se abre, botón "Agregar características", para aceptar la propuesta por defecto → Nótese que en el formulario "Seleccionar servicios de rol", se habilitó automáticamente la opción "DirectAcces y VPN (RAS)", por ser necesarios para el funcionamiento del servicio de enrutamiento que nos interesa, botón "Siguiente" → En el formulario "Rol del servidor web (IIS)", botón "Siguiente" → En el formulario "Seleccionar servicios de rol", botón "Siguiente", para aceptar las características por defecto → En el nuevo formulario, botón "Instalar" y esperar a que concluya el proceso.

Una vez instalada la herramienta de administración del servicio de enrutamiento, es necesario "levantar" el enrutamiento convencional (denominado, en el *Windows Server 2022*, "Enrutamiento LAN"), para ello:

> Inicio → Herramientas administrativas → Enrutamiento y acceso remoto → Seleccionamos el servidor (en nuestro caso, R-WS-R1), en el panel de la derecha → Sobre el servidor seleccionado, botón derecho, opción "Configurar y habilitar enrutamiento y acceso remoto" → Botón "Siguiente" → Dado que, de momento, solo necesitamos el servicio básico de enrutamiento, seleccionamos la opción "Configuración personalizada" → Botón "Siguiente" → Seleccionamos la opción "Enrutamiento LAN" → Botón "Siguiente" → Botón "Finalizar" → En el formulario que se abre, botón "Iniciar servicio".

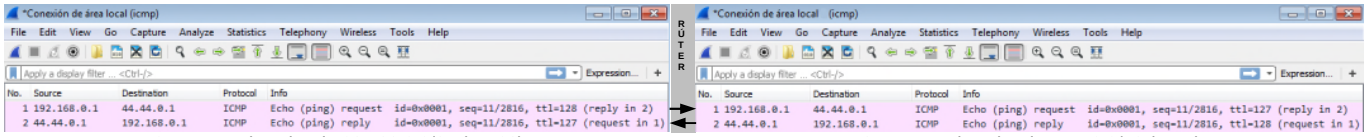
Con respecto al arranque del servicio de enrutamiento, en el *Windows Server 2022*, es necesario hacer una precisión. Al igual que ocurría en el *Windows 7*, el arranque de este servicio se configura, por defecto, con la opción "Automático (inicio retrasado)" con la finalidad de escalonar el arranque de los distintos servicios instalados y mejorar el rendimiento en el arranque del servidor. En la vida real esta es una opción muy interesante, pero en nuestro caso, dado que el arranque del servicio puede retrasarse bastante, tan solo consigue demorar el ejercicio e incluso generar confusión, por creer que algo no funciona en el servidor.

Para evitar esta situación cambiaremos esta opción a "Automático". Para ello acudiremos a: Inicio → Herramientas administrativas → Servicios → Doble clic sobre el servicio "Enrutamiento y acceso remoto" → En el combo "Tipo de inicio", del formulario que se abre, seleccionamos la entrada "Automático" → Botón "Aceptar" → Cerramos la herramienta de administración de servicios.

Una vez instalado el servicio de enrutamiento en el R-WS-R1, y habilitado el enrutamiento convencional, dotaremos a todos los equipos de la configuración TCP/IP indicada en el esquema de la Figura 1, tras lo cual procederemos a analizar el mecanismo del enrutamiento convencional.

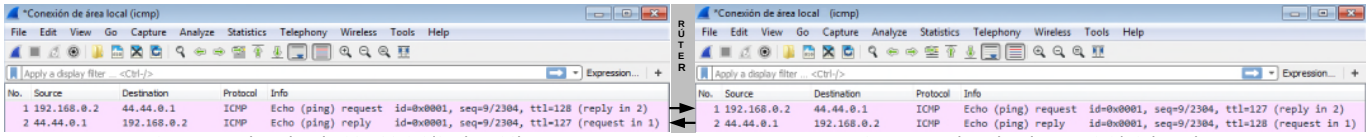
Como ya se conoce, y se muestra en la Figura 2, en los procesos de enrutamiento convencional el direccionamiento del nivel de red (direcciones IP origen y destino) no cambia a lo largo de la ruta seguida por los paquetes IP, independientemente del número de procesos de enrutamiento convencional que sufran esos paquetes.

En la Figura 2 se muestra un ejemplo de enrutamiento convencional, en el cual puede apreciarse como los diálogos, entre las distintas máquinas, tienen lugar, siempre, permaneciendo invariables las direcciones IP de origen y destino, a pesar de que cada uno de los paquetes, transportados por las tramas correspondientes, sufren un proceso de enrutado convencional. Lo cual queda palmariamente de manifiesto siguiendo el valor de los TTL de los distintos paquetes de los diálogos ICMP recogidos en la Figura 2, en donde se constata que, una vez enrutado un paquete, el valor del campo TTL del mismo disminuye en una unidad, pasando, en este caso, de 128 a 127.



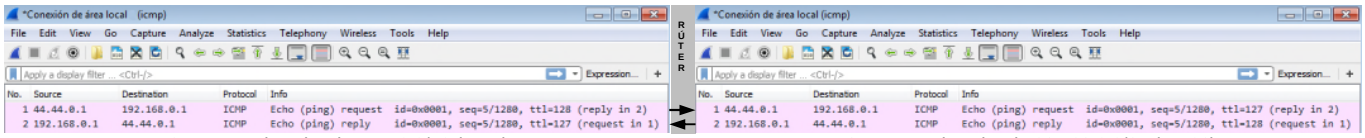
Captura en la subred 192.168.0.0/24 (R-192) | Captura en la subred 44.44.0.0/16 (R-44)

a) ***ping -n 1 44.44.0.1*** desde R-W7-1



Captura en la subred 192.168.0.0/24 (R-192) | Captura en la subred 44.44.0.0/16 (R-44)

b) ***ping -n 1 44.44.0.1*** desde R-W7-2



Captura en la subred 44.44.0.0/16 (R-44) | Captura en la subred 192.168.0.0/24 (R-192)

c) ***ping -n 1 192.168.0.1*** desde R-W7-3

Figura 2

De igual modo, en la Figura 2, se comprueba que cuando se habilita el enrutamiento convencional en el *Windows Server 2022*, es posible la comunicación en ambos sentidos, es decir, los equipos de la LAN privada (R-W7-1 y R-W7-2) pueden iniciar un diálogo con cualquier equipo de la red pública (en este caso R-W7-3) y este le responde sin problemas, Figura 2a y Figura 2b.

Paralelamente, cualquier equipo de la red pública (R-W7-3) puede iniciar un diálogo con cualquiera de los equipos de la LAN privada (R-W7-1 y R-W7-2), obteniendo la respuesta correspondiente, Figura 2c.

Recordar, por último, que el direccionamiento del nivel de enlace de datos, direcciones MAC de las tramas, es absolutamente distinto del comentado para el nivel de red. En el nivel 2, las direcciones MAC cambian en cada segmento, su dominio es la subred. Así, por ejemplo, en una comunicación R-W7-1 → R-W7-3, la trama de la subred R-192 tendrá como MAC origen la asociada a la interfaz de red del R-W7-1 y como MAC destino, la correspondiente a la interfaz del rúter (R-WS-R1) de la subred R-192. Una vez enrutado el paquete, en la nueva trama que circule por R-44, la MAC origen será la de la interfaz de red del R-WS-R1 de esa subred, y la MAC destino la correspondiente a la interfaz de R-W7-3.

La gestión de direcciones MAC, es independiente del tipo de proceso de enrutamiento que sufran los paquetes. Resultando irrelevante que sea un enrutamiento convencional o de cualquier otro tipo.

2.- ENRUTAMIENTO CON NAT (*NETWORK ADDRESS TRANSLATION*).

Para entender la finalidad del NAT (***N**etwork **A**ddress **T**ranslation*, traducción de dirección de red), debemos recordar que, por definición, las IP de subredes privadas (10.0.0.0/8, 172.16.0.0/12, 169.254.0.0/16, 192.168.0.0/16 y sus respectivos subconjuntos) no son enrutadas por los rúteres públicos.

Imaginemos que deseamos salir de la LAN desde el equipo R-W7-1 de la Figura 1. Según esto, todos los paquetes con origen en él tendrán como dirección IP origen la 192.168.0.1/24, estos paquetes llegarán a R-WS-R1 que los enrutará hacia la WAN, a través de un proceso de enrutamiento convencional, sin alterar ni la IP origen ni la IP destino, lo que significa que esos paquetes podrán llegar a cualquier destino con la IP, privada, 192.168.0.1/24 como IP origen. Una vez en el destino, éste procederá a responder; con lo cual generará los paquetes que corresponda indicando como IP destino la misma que recibió en el paquete de entrada como IP origen, es decir la 192.168.0.1/24. Pondrá en circulación los paquetes, y en cuanto lleguen al primer rúter público éste los retirará de la circulación, por carecer de la regla de enrutado que le indique cómo acceder a un equipo destino de una subred privada 192.168.0.0/16. Según esto, R-W7-1 nunca recibirá respuesta alguna desde el exterior de su propia LAN. Como corolario es fácil deducir, que no es útil salir desde una LAN, hacia la WAN, utilizando una IP privada.

Para evitar la situación anterior, se utiliza el mecanismo de enrutamiento NAT a través del cual se traduce, se cambia, la IP origen, privada, de todos los paquetes que abandonan la LAN por la IP de la interfaz pública del rúter frontera, IP pública prestada por el ISP (***I**nternet **S**ervice **P**rovider*, proveedor de servicio de Internet), Figura 3. De esta forma se consigue que todos los paquetes que salgan de la LAN lo hagan con una IP origen a la que se pueda responder desde el exterior. En este caso todas las máquinas de la LAN saldrán, a la WAN, con la misma IP, la única IP pública del rúter, (en la Figura 3 y en la Figura 4 será la 44.44.0.100/16) razón por la cual a esta técnica de traducción se le denomina *NAT estático*. El contrapunto a este *NAT estático* lo constituye el *NAT dinámico*, en el cual el rúter frontera dispone de un

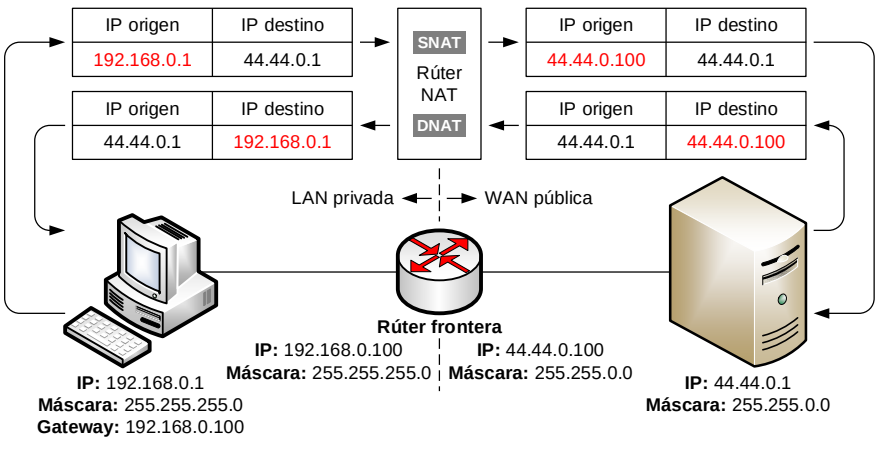


Figura 3

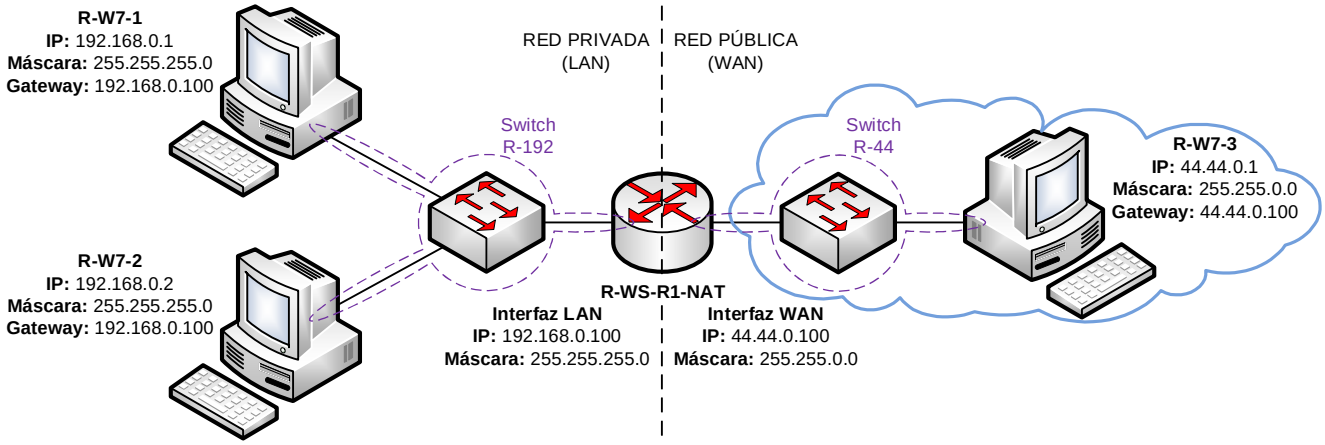


Figura 4

conjunto, más o menos grande, de direcciones IP públicas que asigna, dinámicamente, a los paquetes que salen de la LAN. En este caso, no todos los paquetes de la LAN tendrán la misma IP origen.

Partiendo del R-WS-R1, con el servicio de enrutamiento convencional ya funcionando, para la instalación de la herramienta de administración del enrutamiento NAT (***N**etwork **A**ddress **T**ranslation*, traducción de dirección de red) y la configuración del mismo, procederemos del siguiente modo:

Inicio ➔ Herramientas administrativas ➔ Enrutamiento y acceso remoto ➔ Desplegar las opciones del servidor (haciendo clic en el signo ">" que tiene a su izquierda) ➔ Desplegar las opciones de IPv4 (haciendo clic en el signo ">" que tiene a su izquierda) ➔ Seleccionar ítem "General" ➔ Botón derecho, opción "Protocolo de enrutamiento nuevo..." ➔ En el formulario que se presenta, Figura 5, hacemos doble clic sobre la opción NAT.

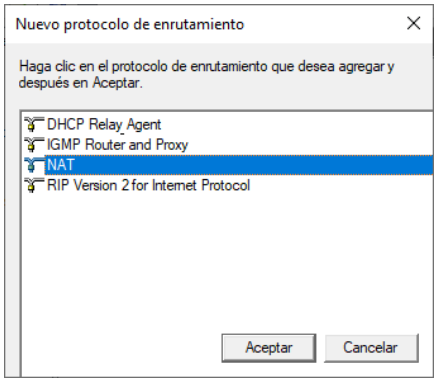


Figura 5

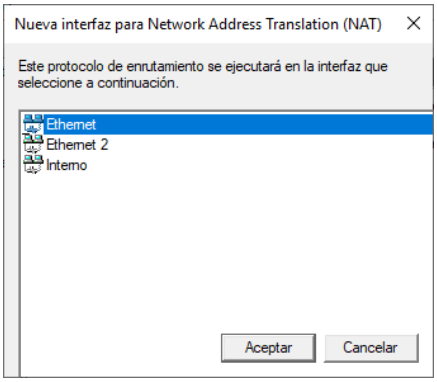


Figura 6

Una vez instalada la herramienta de administración del NAT, será necesario configurarlo. Para ello debemos advertir que se incorporó el ítem "NAT", bajo el epígrafe IPv4. Para configurarlo será necesario indicarle qué interfaz corresponde a la LAN y cuál a la WAN, para lo cual procederemos de la forma siguiente:

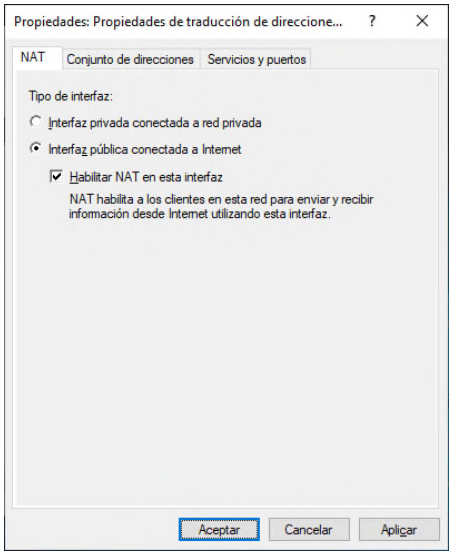


Figura 7

Seleccionar el ítem "NAT" ➔ Botón derecho, opción "Interfaz nueva" ➔ Se abre un formulario en el cual se debe indicar sobre qué interfaz, de las indicadas, se desea ejecutar el nuevo protocolo, en nuestro caso deseamos que se ejecute sobre la interfaz correspondiente a la subred pública, es decir la de IP 44.44.0.100/16, ya que debe ser esa la IP con lo cual los paquetes procedentes de la LAN circulen por las redes públicas. Según esto, haremos doble clic sore la interfaz "Ethernet", Figura 6 ➔ Que nos abre un nuevo formulario a través del cual configuraremos, realmente, el comportamiento del NAT. En él se seleccionará la opción "Interfaz pública conectada a Internet", tras lo cual se activa la opción "Habilitar NAT en esta interfaz", que también seleccionaremos. Quedando tal y como se muestra en la Figura 7 ➔ Botón "Aceptar".

Una vez configurada la interfaz de la WAN, configuraremos la correspondiente a la LAN; para lo cual seleccionaremos, de nuevo, el ítem "NAT" ➔ Botón derecho, opción "Interfaz nueva" ➔ Se abre un formulario en el cual, en esta ocasión, haremos doble clic sobre la correspondiente a la LAN, es decir la interfaz "Ethernet 2", Figura 8 ➔ Que nos abre un nuevo formulario en cual se seleccionará la opción "Interfaz privada conectada a red privada". Quedando tal y como se muestra en la 9 ➔ Botón "Aceptar".

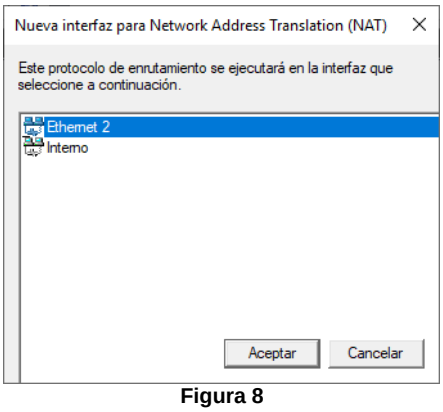


Figura 8

Instalado y configurado el enrutamiento NAT, reiniciaremos el servicio, para lo cual:

Seleccionamos el servidor (R-WS-R1-NAT) ➔ Botón derecho "Todas las tareas" ➔ Reiniciar.

Antes de realizar las pruebas correspondientes, con el enrutamiento NAT, quizá sea interesante hacer hincapié en que el término NAT es un término genérico que incluye, básicamente, dos técnicas distintas de traducción de direcciones de red, el

NAT origen, al que suele hacerse referencia como *SNAT* (siglas de, ***S**ource **N**etwork **A**ddress **T**ranslation*) y el NAT destino, *DNAT* (siglas de, ***D**estination **N**etwork **A**ddress **T**ranslation*), Figura 3. En ambas técnicas se realiza traducción de direcciones IP, cambio de direcciones IP, en los paquetes que recibe el rúter, en el primero de los casos, SNAT, se cambia la dirección IP origen y en el segundo la dirección IP destino.

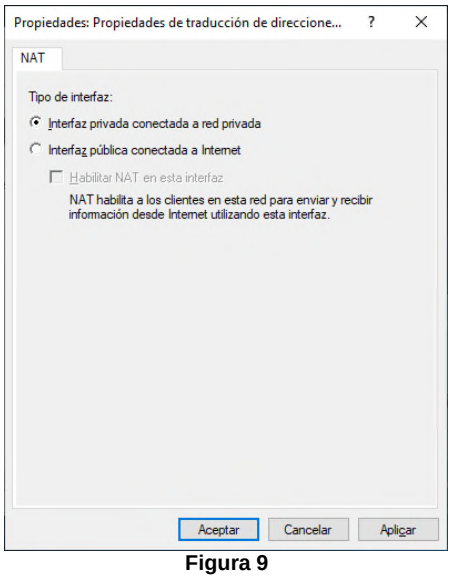


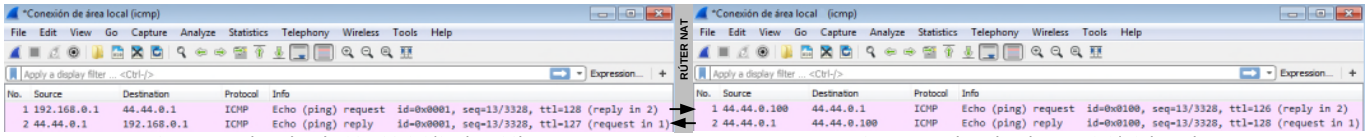
Figura 9

De hecho, ya se verá que en las comunicaciones con enrutamiento NAT se utilizan ambas técnicas, dependiendo del sentido de la comunicación, el SNAT cuando los paquetes salen de la LAN hacia la WAN, y el DNAT cuando el sentido es el inverso, Figura 3.

Una vez configurado el NAT y transformado el R-WS-R1, Figura 1, en el R-WS-R1-NAT de la Figura 4, podremos realizar las pruebas cuyos resultados se muestran en la Figura 10.

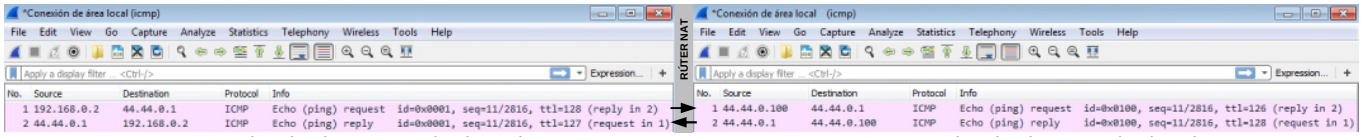
En las capturas realizadas en R-44, de la Figura 10a, se comprueba que al hacer un ***ping*** desde el R-W7-1 hacia el R-W7-3, los paquetes que viajan en las tramas capturadas, correspondientes a las peticiones de eco ICMP (*request*, mensaje ICMP tipo 8), lo hacen con la IP origen 44.44.0.100 tal y como se esperaba de un enrutamiento NAT. Adviértase que, en este caso, se realizó un SNAT, NAT origen, ya que lo que se cambió fue la IP origen de la comunicación.

Lo mismo ocurre, Figura 10b, para el ***ping*** lanzado desde el R-W7-2 hacia idéntico destino. Las peticiones de eco le llegan a R-W7-3 con la IP origen 44.44.0.100/16. Todo ello pone de manifiesto que, efectivamente, todos los equipos de la LAN comparten, al salir de la misma, la única IP pública configurada en el rúter frontera, la 44.44.0.100/16.



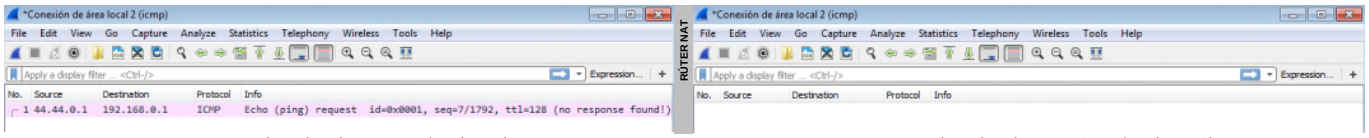
Captura en la subred 192.168.0.0/24 (R-192) | Captura en la subred 44.44.0.0/16 (R-44)

a) ***ping -n 1 44.44.0.1*** desde R-W7-1



Captura en la subred 192.168.0.0/24 (R-192) | Captura en la subred 44.44.0.0/16 (R-44)

b) ***ping -n 1 44.44.0.1*** desde R-W7-2



Captura en la subred 44.44.0.0/16 (R-44) | Captura en la subred 192.168.0.0/24 (R-192)

c) ***ping -n 1 192.168.0.1*** desde R-W7-3

Figura 10

Mención especial merecen los ecos que le llegan a R-W7-1 y R-W7-2 procedentes de R-W7-3. En estos casos puede comprobarse, Figura 10a y Figura 10b, que cuando atraviesan el R-WS-R1-NAT sufren un cambio en la dirección de destino, pasando de la 44.44.0.100/16 (configurada sobre la interfaz de la WAN del rúter) a la correspondiente al equipo concreto. En este caso, el R-WS-R1-NAT realiza un NAT destino (DNAT) ya que lo que cambia es la IP de destino.

Llamar la atención sobre el hecho de que, para los equipos del exterior de la LAN, los diálogos tienen lugar entre ellos y el rúter, nunca sabrán que tras esa IP a la que dirigen sus paquetes, se esconde una subred completa con un número indeterminado de equipos. En estas circunstancias, es el rúter el encargado de redireccionar los paquetes que recibe, desde la WAN, al equipo correspondiente de la LAN, como puede verse en las capturas realizadas en la subred R-192 de la Figura 10, en donde el rúter sustituye su IP pública, que aparecía como IP destino en los paquetes que le llegan, por la IP de los correspondientes equipos de la LAN. Esta gestión la realiza guardando, en una tabla NAT (de referencia obligada en el caso de las *nftables* de *GNU/LINUX*), la información de cada uno de los paquetes que envía a la WAN, de manera que cuando llega la correspondiente respuesta podrá saber a qué equipo, específico, de la LAN debe enviársela.

Es importante señalar que, en el *Windows Server 2022*, cuando se habilita el NAT en el enrutamiento, automáticamente se activan una serie de reglas en el *firewall* que impiden el acceso a la LAN desde el exterior, empleando IP privadas. Esa es la razón por la cual, con el enrutamiento convencional, un ***ping*** lanzado desde R-W7-3 hacia R-W7-1, con IP destino 192.168.0.1/24, obtenía la respuesta correspondiente, Figura 2c, mientras que ese mismo ***ping*** lanzado con el NAT habilitado no obtiene respuesta alguna, ya que es bloqueado en el R-WS-R1-NAT, Figura 10c.

En la Figura 10a y la Figura 10b llama la atención que las peticiones de eco, desde R-W7-1 y R-W7-2, lleguen a R-W7-3 con un valor del campo TTL, del paquete, de 126; como si hubieran sufrido dos procesos de enrutamiento. Este comportamiento se debe a un *bug*[1] (en la jerga informática se traduce por error, aunque su traducción correcta sería bicho) que se introduce al habilitar el NAT en el *Windows Server 2022*. Por alguna razón que se desconoce, le resta dos al campo TTL, de los paquetes entrantes, cuando los enruta, en contra del estándar. Lamentablemente, tal y como se verá más adelante, no es el único *bug* que tiene el NAT en el *Windows Server 2022*.

Una vez habilitado el NAT en el rúter, hay un cambio que se puede hacer en el R-W7-3 y que deja bien a las claras el funcionamiento de ese mecanismo. Si en el R-W7-3 se elimina la puerta de enlace, en su configuración TCP/IP, tal y como se muestra en la Figura 11, podremos comprobar que sigue respondiendo a los ***ping*** lanzados desde el R-W7-1 o el R-W7-2, ya que al funcionar el NAT los recibe desde la IP 44.44.0.100/16 del rúter, que pertenece a su misma subred. Con lo cual estima que no necesita el concurso de ningún rúter para responderlos. De esta forma se evidencia, que la subred privada queda absolutamente oculta, para el exterior, tras el rúter frontera que hace NAT.

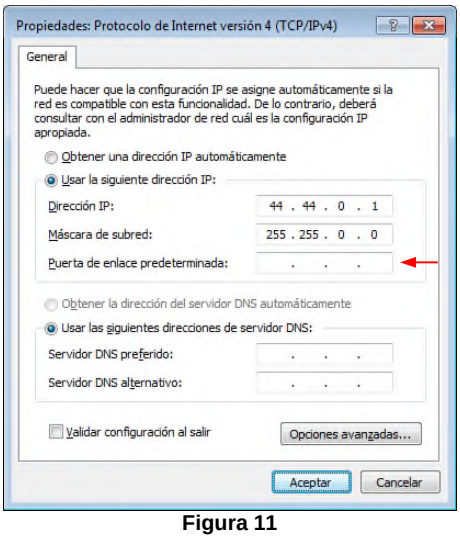


Figura 11

Por último, indicar, que el NAT fue uno de los mecanismos que contribuyeron, de forma decisiva, a hacer posible la universalización del acceso a Internet, ya que sin él ya haría muchos años que se habrían agotado las IP públicas y la mayoría de los usuarios no podrían salir de su LAN por carecer de ellas. Gracias al NAT, entre otras técnicas, este agotamiento de IP públicas no tuvo el efecto demoledor que hubiera tenido, sin ellas, sobre el usuario final.

Adviértase, por otro lado, que es el NAT el que permite que en el mundo existan un número indeterminado de millones de redes privadas (10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16 y sus respectivos subconjuntos) teniendo cada una de ellas, a su vez, un número indeterminado de equipos, de manera tal que todos ellos puedan salir, de su respectiva LAN, sin mayores problemas y utilizando un número muy significativamente menor de IP públicas, que equipos existen en esas subredes.

3.- NOTAS FINALES.

[1] Para *bug*, véase: https://es.wikipedia.org/wiki/Error_de_software