EJERCICIO DE ENRUTAMIENTO CON NAT ESTÁTICO EN *WINDOWS SERVER 2022* 34

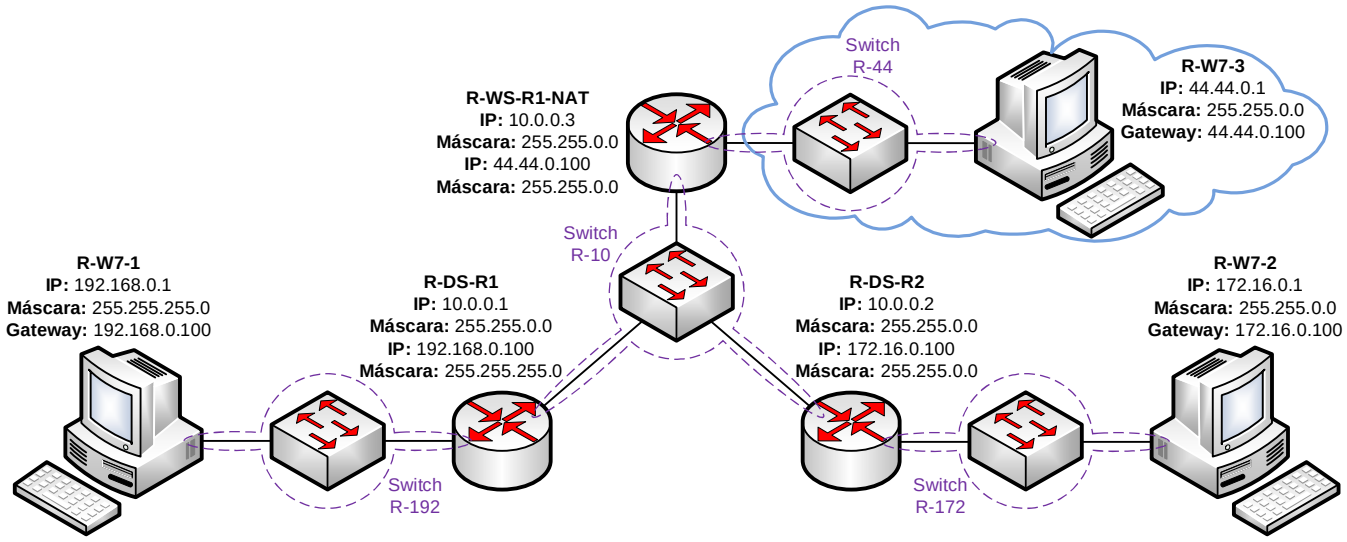


Figura 1

1.- CONFIGURACIÓN DE R-W7-1, R-W7-2 Y R-W7-3.

La configuración de las tres máquinas será la que se muestra en la Figura 1 y se recoge en la siguiente tabla:

	R-W7-1	**R-W7-2**	**R-W7-3**
Red interna (*VirtualBox*)	R-192	R-172	R-44
IP	192.168.0.1	172.16.0.1	44.44.0.1
Máscara de subred	255.255.255.0	255.255.0.0	255.255.0.0
Puerta de enlace	192.168.0.100	172.16.0.100	44.44.0.100

2.- R-DS-R1 (RÚTER INTERIOR DE LA LAN).

Con la finalidad de hacer las rutas persistentes se incorporan en el fichero */etc/network/interfaces*, quedando como (comprobar, en cada caso, que interfaces "ve" el equipo con ***ip a l***):

Opción 1

```
auto lo
   iface lo inet loopback
auto enp0s3
   iface enp0s3 inet static
   address 10.0.0.1
   netmask 255.255.0.0
auto enp0s8
   iface enp0s8 inet static
   address 192.168.0.100
   netmask 255.255.255.0
```

Opción 2

```
auto lo
   iface lo inet loopback
auto enp0s3
   iface enp0s3 inet static
   address 10.0.0.1/16
auto enp0s8
   iface enp0s8 inet static
   address 192.168.0.100/24
```

```
#Reglas de enrutado
   up ip route add 172.16.0.0/16 via 10.0.0.2 dev enp0s3
   up ip route add default via 10.0.0.3 dev enp0s3
```

Recuérdese que, una vez concluida la edición del fichero, debe reiniciarse la infraestructura de red:

sudo /etc/init.d/networking restart o ***sudo systemctl restart networking.service***

En coherencia con la configuración de las interfaces, `enp0s3` debe encontrarse en la red interna R-10 y `enp0s8` en R-192

Si no se deseara que las reglas fueran permanentes, podrían incorporarse directamente desde la línea de comandos como:

sudo ip route add 172.16.0.0/16 via 10.0.0.2

sudo ip route add default via 10.0.0.3

Recuérdese que, en todos los casos, el parámetro ***dev*** (*device*, dispositivo) es opcional, aunque se recomienda su uso, por cuestiones de documentación, cuando las reglas de enrutado se incorporan en el fichero */etc/network/interfaces*.

Recordar que para activar el enrutamiento en sistemas *GNU/Linux* es necesario que el fichero */proc/sys/net/ipv4/ip_forward* guarde el valor 1 (por defecto guarda el valor 0), para lo cual editaremos el fichero */etc/sysctl.conf* utilizando el editor de texto *nano*, en la forma siguiente:

sudo nano /etc/sysctl.conf

y acudiremos a la sección correspondiente al enrutamiento IPv4, quedando como:

```
# Uncomment the next line to enable packet forwarding for IPv4
net.ipv4.ip_forward=1
```

Una vez realizado el cambio en el fichero, bastará con reiniciar el equipo (***sudo reboot***) o ejecutar el comando ***sudo sysctl -p*** para que sea efectiva la nueva configuración y dispongamos del servicio de enrutamiento habilitado.

Para verificar que el servicio de enrutamiento se encuentra habilitado, bastará con ejecutar un ***cat /proc/sys/net/ipv4/ip_forward*** y comprobar que devuelve el valor 1.

3.- R-DS-R2 (RÚTER INTERIOR DE LA LAN).

Con la finalidad de hacer las rutas persistentes se incorporan en el fichero */etc/network/interfaces*, quedando como (comprobar, en cada caso, que interfaces "ve" la máquina con ***ip a l***):

Opción 1

```
auto lo
   iface lo inet loopback
auto enp0s3
   iface enp0s3 inet static
   address 10.0.0.2
   netmask 255.255.0.0
auto enp0s8
   iface enp0s8 inet static
   address 172.16.0.100
   netmask 255.255.0.0
```

Opción 2

```
auto lo
   iface lo inet loopback
auto enp0s3
   iface enp0s3 inet static
   address 10.0.0.2/16
auto enp0s8
   iface enp0s8 inet static
   address 172.16.0.100/16
```

```
#Reglas de enrutado
   up ip route add 192.168.0.0/24 via 10.0.0.1 dev enp0s3
   up ip route add default via 10.0.0.3 dev enp0s3
```

Recuérdese que, una vez concluido el fichero, debe reiniciarse la infraestructura de red:

sudo /etc/init.d/networking restart o ***sudo systemctl restart networking.service***

En coherencia con la configuración de las interfaces, `enp0s3` debe encontrarse en la red interna R-10 y `enp0s8` en R-172

Si no se deseara que las reglas fueran permanentes, podrían incorporarse directamente desde la línea de comandos como:

sudo ip route add 192.168.0.0/24 via 10.0.0.1 dev enp0s3

sudo ip route add default via 10.0.0.3 dev enp0s3

Recuérdese que, en todos los casos, el parámetro ***dev*** (*device*, dispositivo) es opcional, aunque se recomienda su uso, por cuestiones de documentación, cuando las reglas de enrutado se incorporan en el fichero */etc/network/interfaces*.

No olvide activar el enrutamiento, utilizando el procedimiento descrito para el R-DS-R1.

4.- R-WS-R1-NAT (RÚTER FRONTERA LAN/WAN).

Empezaremos por darle la configuración TCP/IP a ambas interfaces, tal y como se muestra en la Figura 2. Se asume que la primera de las interfaces se encuentra en la red interna R-10 y que la segunda se encuentra en R-44.

Para incorporar las reglas de enrutado en la tabla, de forma permanente, deben ejecutarse las siguientes órdenes en una consola, recuerde que se requiere elevación:

route -p add 172.16.0.0 mask 255.255.0.0 10.0.0.2

route -p add 192.168.0.0 mask 255.255.255.0 10.0.0.1

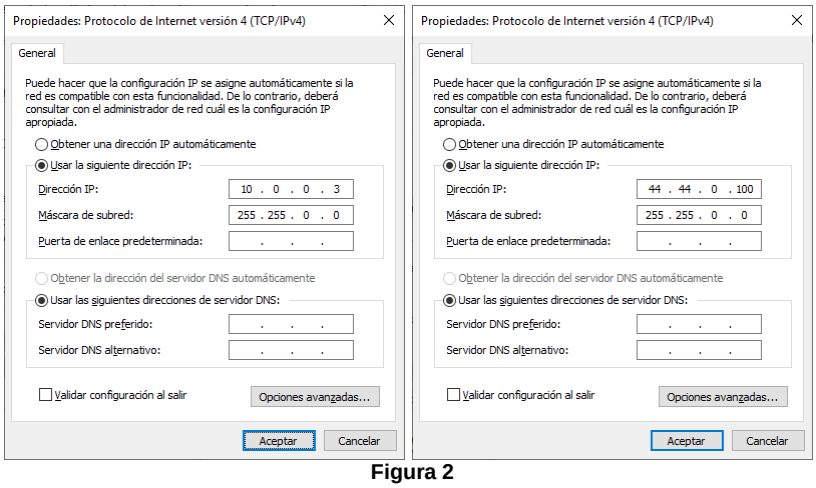


Figura 2

Para instalar el servicio de enrutamiento, en el supuesto de que no lo estuviera:

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-NAT, 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.

Antes de instalar y configurar el enrutamiento NAT, levantaremos el enrutamiento convencional (denominado, en el *Windows Server 2022*, “Enrutamiento LAN”) para comprobar que todo funciona según lo esperado. Para ello:

Inicio ➔ Herramientas administrativas ➔ Enrutamiento y acceso remoto ➔ Seleccionamos el servidor (en nuestro caso, R-WS-R1-NAT), 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 del 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.

Como ya se conoce, la herramienta de administración del servicio de enrutamiento, instala una opción para incorporar reglas de enrutamiento de forma gráfica. Por ejemplo, si no hubiéramos incorporado las reglas en el R-WS-R1-NAT podríamos hacerlo, ahora, de la siguiente forma:

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 el ítem “Rutas estáticas” ➔ Botón derecho ➔ Seleccionar “Ruta estática nueva” ➔ Para las dos rutas que debemos incorporar seleccionaremos, en el combo interfaz (Figura 3), la conexión correspondiente a la IP 10.0.0.3, ya que ambas rutas son internas. Para saber que conexión de área local corresponde a esa IP, puede verse en la opción “General”, de IPv4, tal y como muestra la Figura 4.

Una vez hecha esta selección, cubrimos el resto de los campos con la información correspondiente a cada regla, según puede verse en la Figura 3.

Quedando las rutas, tal y como se muestran en la Figura 5.

Las rutas así establecidas aparecen en la tabla de enrutado (***route print***) como no permanentes, aunque en realidad lo son, ya que se cargan cada vez que se arranca el sistema y se levanta el servicio de enrutamiento. Recuerde que una regla de enrutado incorporada a través de la herramienta gráfica, solo se puede eliminar usando esa misma herramienta.

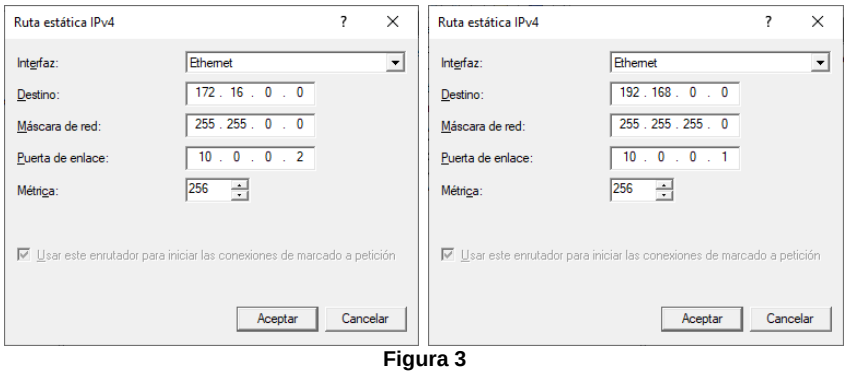


Figura 3

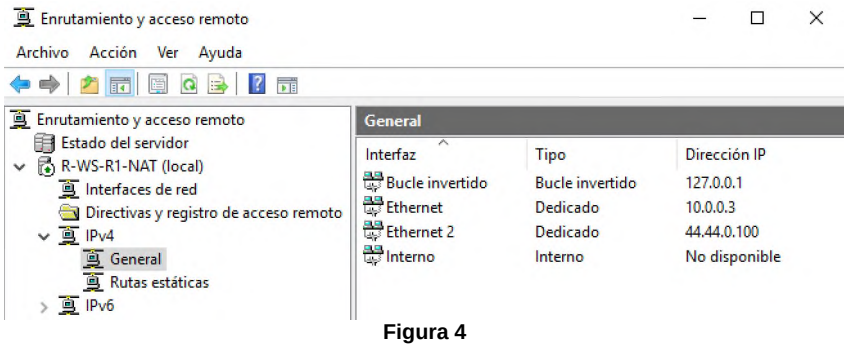


Figura 4

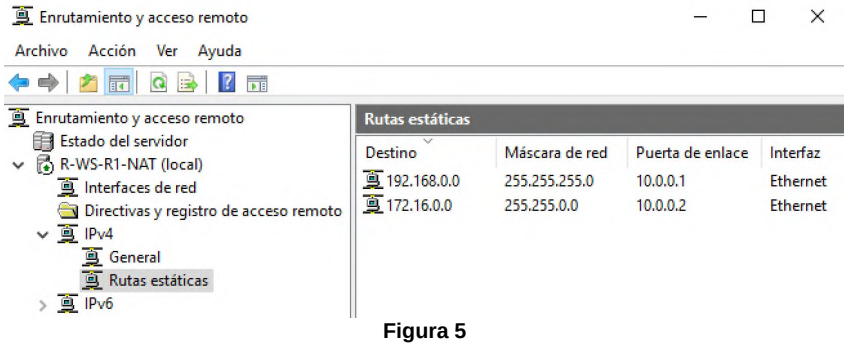


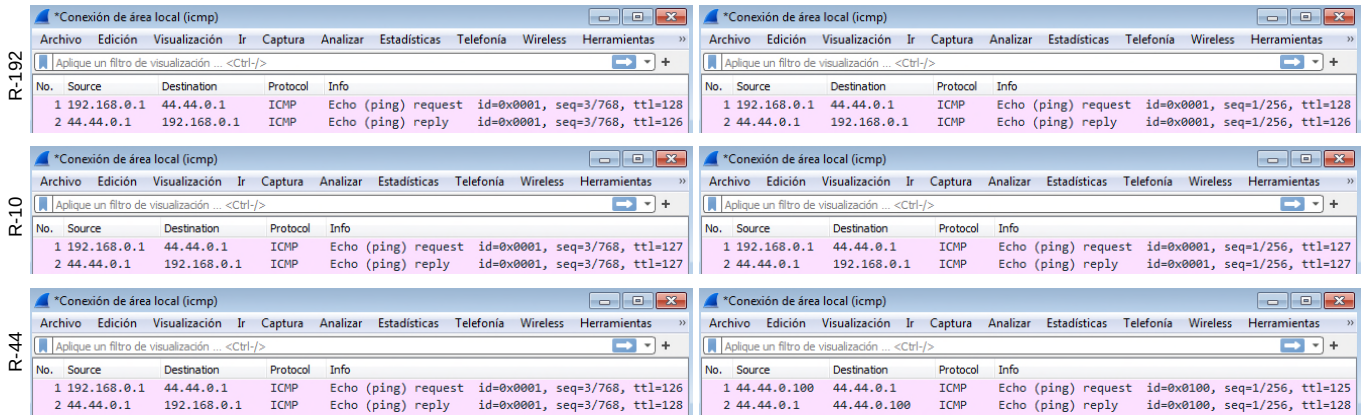
Figura 5

Antes de probar las nuevas rutas es muy conveniente reiniciar el servicio para garantizar que acepta los cambios de forma estable y fiable. Pare ello:

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

En la Figura 6a pueden verse las capturas realizadas en las subredes R-192, R-10 y R-44, utilizando el filtro de captura: *icmp*, correspondientes a la petición de un eco *ICMP* desde R-W7-1 a R-W7-3 (***ping -n 1 44.44.0.1***), en ellas puede comprobarse como la respuesta de R-W7-3 llega sin problema a R-W7-1 y como, a lo largo del camino, las direcciones IP de origen y destino no

cambian en ninguno de los paquetes que transportan las tramas capturadas, independientemente de que correspondan a la petición del eco o al propio eco.

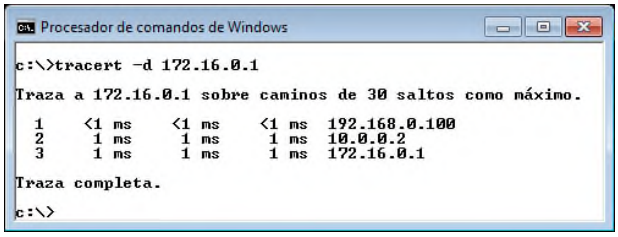


a) Enrutamiento convencional **b)** Enrutamiento con NAT

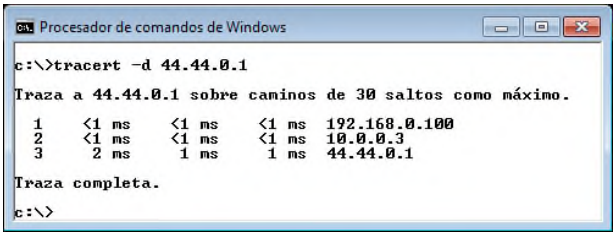
Figura 6. Capturas, realizadas en las distintas subredes, correspondientes a un ***ping -n 1 44.44.0.1*** (R-W7-3) desde R-W7-1.

Acudiendo al comando ***tracert***, ya conocido, podemos comprobar, de forma muy visual, que todo funciona tal y como lo habíamos previsto.

a) Desde R-W7-1 (192.168.0.1).

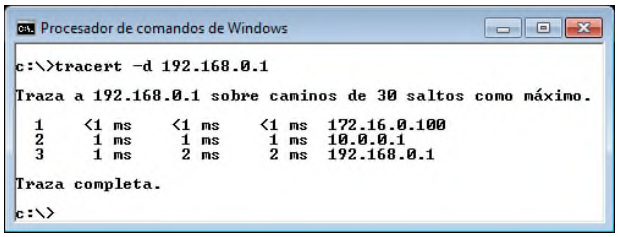


tracert a R-W7-2

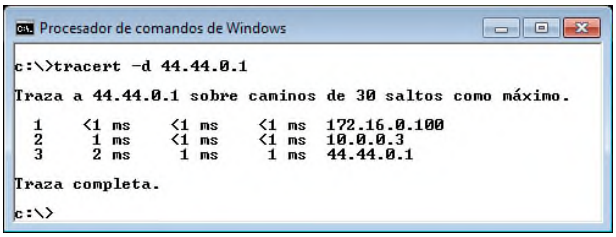


tracert a R-W7-3

b) Desde R-W7-2 (172.16.0.1).



tracert a R-W7-1



tracert a R-W7-3

Una vez comprobado que todo funciona según se esperab, es el momento de incorporar y configurar el NAT.

4.1.- Instalación de la herramienta de administración del NAT y configuración del NAT.

Para instalar y configurar la herramienta de administración del NAT (***N**etwork **A**ddress **T**ranslation*, traducción de dirección de red), dado que ya tenemos habilitado el enrutamiento convencional, procederemos de la forma siguiente:

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 el ítem “General” ➔ Botón derecho, opción “Protocolo de enrutamiento nuevo...” ➔ En el formulario que se presenta, hacer doble clic sobre la opción NAT.

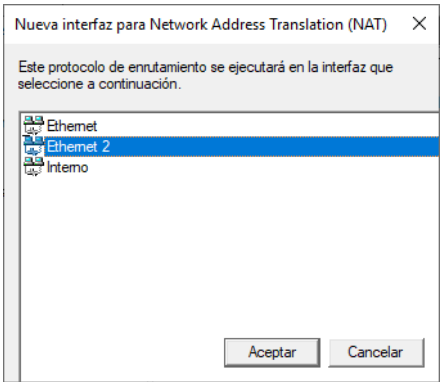


Figura 7

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 procederemos de la forma siguiente:

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

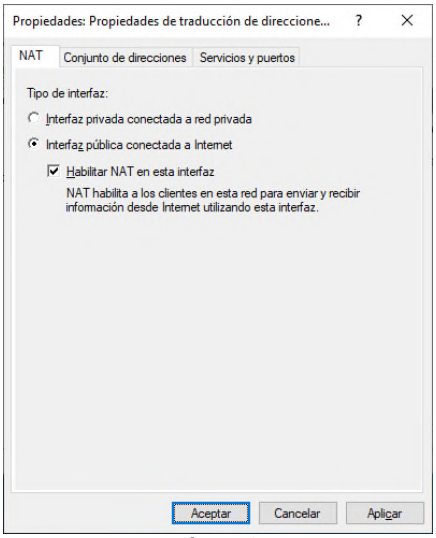


Figura 8

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, 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 sobre la interfaz "Ethernet 2", Figura 7 → 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 8 → Botón "Aceptar".

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", ya que es la interfaz que corresponde a la subred 10.0.0.0/8, Figura 9 → 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 Figura 10 → Botón "Aceptar".

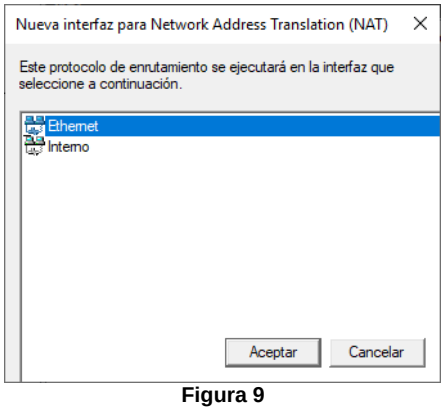


Figura 9

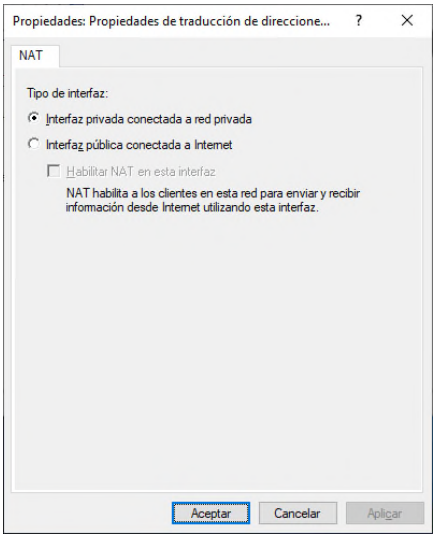


Figura 10

Una vez 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.

Ahora ya se podrá probar el funcionamiento del NAT. Lanzando un ***ping*** desde R-W7-1 a R-W7-3, con una única petición de eco se obtiene las capturas mostradas en la Figura 6b, en la que puede apreciarse el efecto del NAT sobre las correspondientes a la subred 44.44.0.0/16 (R-44), en la que aparece la IP 44.44.0.100, perteneciente a R-WS-R1-NAT, como IP origen (NAT origen, SNAT), en el caso de la petición de eco, y como IP destino, en el de la respuesta desde R-W7-3. Dando la impresión de tratarse de un diálogo entre R-WS-R1-NAT y R-W7-3 exclusivamente.

Tal y como es normal, la única etapa afectada, por el NAT, es la correspondiente al segmento de la subred 44.44.0.0/16, ya que las otras dos etapas corresponden a la parte privada de la red. Obsérvese la evolución de los TTL, tanto en los *request* como en los *reply*.

Recuerde que, por alguna razón desconocida, *Windows Server 2022*, cuando tiene habilitado el NAT, le resta 2 al valor del TTL del paquete saliente, provocando que las peticiones de eco lleguen al R-W7-3 con un valor del campo TTL de 125, Figura 6b captura en R-44, en lugar del correcto de 126, tal y como puede verse en las capturas del enrutamiento sin NAT, Figura 6a captura en R-44. En principio, tal comportamiento es incorrecto y, probablemente, debido a un error (*bug*). Adviértase que el eco, sí llega con el TTL correcto, 126, a R-W7-1, captura correspondiente a la subred R-192 de la Figura 6b.

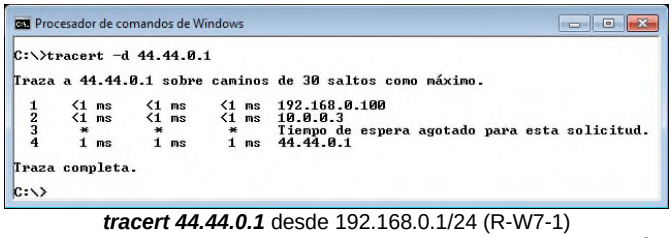
No olvide, que una vez instalado el enrutamiento NAT, en *Windows Server 2022*, se incluyen, automáticamente, unas reglas en el *firewall* del sistema que impiden conexiones de entrada, desde el exterior, que no sean esperadas.

De forma paralela a lo hecho con el R-W7-1, podríamos lanzar idéntico ***ping*** (***ping -n 1 44.44.0.1***) desde el R-W7-2 y se comprobará que sus paquetes también salen de la LAN con la IP pública del rúter (IP 44.44.0.100/16), ya que el NAT se realiza sobre todo paquete que salga de la LAN, hacía la WAN, independientemente del equipo origen de los mismos.

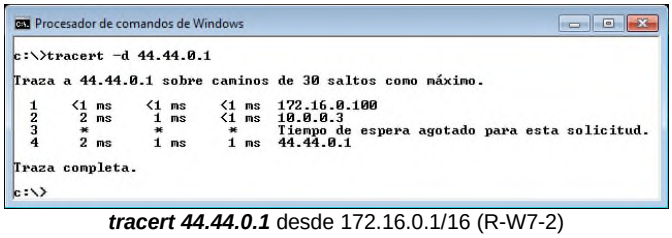
4.2.- Resultados de los *tracert* con el NAT activado.

En principio no deberían variar, en nada, con respecto a los obtenidos antes de activar el NAT, y de hecho los resultados obtenidos para los ***tracert*** entre R-W7-1 y R-W7-2 son idénticos a los mostrados anteriormente, R-W7-1 pasará por 192.168.0.100 → 10.0.0.2 → 172.16.0.1 y R-W7-2 por 172.16.0.100 → 10.0.0.1 → 192.168.0.1. Ya que en su camino no se encuentra el R-WS-R1-NAT.

Pero la sorpresa surge al hacer un ***tracert*** a 44.44.0.1 desde R-W7-1 (192.168.0.1) o desde R-W7-2 (172.16.0.1), obteniéndose los resultados que se muestran en la Figura 11.



tracert 44.44.0.1 desde 192.168.0.1/24 (R-W7-1)

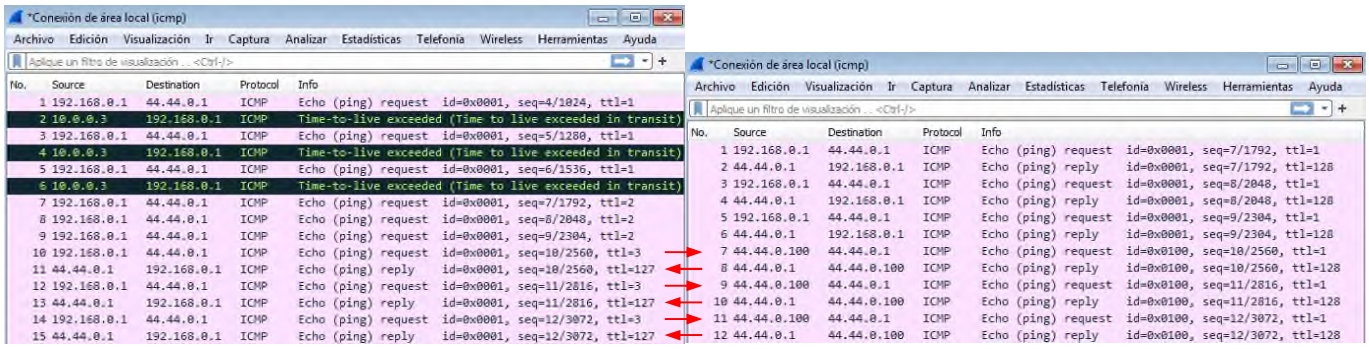


tracert 44.44.0.1 desde 172.16.0.1/16 (R-W7-2)

Figura 11

Y que no dejan de sorprender, pues no coinciden con el resultado esperado. Aparentemente aparece una etapa de enrutado (tercera traza de las capturas), cuyo origen no es fácil de explicar.

Para poder resolver el enigma del resultado de esos ***tracert***, capturaremos las tramas correspondientes en las subredes 10.0.0.0/8 (R-10) y 44.44.0.0/16 (R-44), filtrando las capturas por el protocolo ICMP (*icmp*). Los resultados obtenidos, para el ***tracert 44.44.0.1*** desde 192.168.0.1 (R-W7-1), son los mostrados en la Figura 12.



Captura en la subred 10.0.0.0/8 (R-10) Captura en la subred 44.44.0.0/16 (R-44)

Figura 12

Lo primero será identificar cada trama y conocer su origen y su destino.

Empezando por la captura de la subred 10.0.0.0/8, es fácil identificar las tramas 1 a 6 como aquellas que llegan a R-WS-R1-NAT con TTL 1 (tramas 1, 3 y 5) y por lo tanto él hace su TTL 0 y lo notifica al origen (tramas 2, 4 y 6), según esto, las tramas comentadas, 1 a 6, son las causantes de la segunda línea de los ***tracert*** en R-W7-1 y R-W7-2.

A continuación, aparecen las tramas 7 a 9, que llegan a R-WS-R1-NAT con un TTL 2 y, por lo tanto, debería enrutarlas con un TTL 1, para ser respondidas por R-W7-3. Sin embargo, ninguna de estas tramas 7 a 9 (*request*) recibe respuesta alguna, lo que permite afirmar que son el origen de la tercera línea de los ***tracert*** obtenidos por R-W7-1 y R-W7-2.

Para averiguar el por qué, de esta falta de respuesta a las tramas 7 a 9, vamos a la captura de la subred 44.44.0.1/16 y nos fijamos en las tramas 1 a 6, que son las que se corresponden. Lo primero es constatar que efectivamente R-WS-R1-NAT las enruta con un TTL de 1, tal y como se esperaba (tramas 1, 3 y 5, *request*). Lo que realmente es singular es que NO hace NAT, obsérvese que las envía hacia R-W7-3 con la IP origen 192.168.0.1. Este fallo es característica del *Windows Server 2022* cuando hace NAT, por alguna razón desconocida cuando le llega una trama con TTL 2, le disminuye el valor del TTL, pero no hace el cambio de dirección origen (SNAT), de manera que las pone en circulación con la IP privada como IP de origen. Esto provoca que cuando R-W7-3 las reciba y las intente responder (tramas 2, 4 y 6, *reply*, de la captura en R-44) lo haga poniendo como IP de destino la 192.168.0.1, lo que hace que cuando R-WS-R1-NAT las reciba las bloquee, sin enrutarlas a la subred privada, de acuerdo con las restricciones de su cortafuegos. Razón por la cual, a pesar de obtener la respuesta de R-W7-3, ésta nunca llega ni a R-W7-1 ni a R-W7-2, originando la tercera línea de cada resultado del ***tracert***.

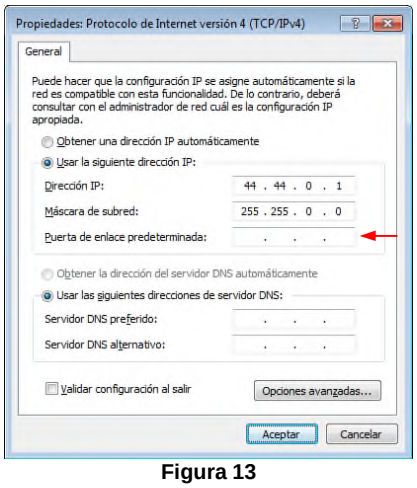


Figura 13

Dado que el ***tracert*** no obtiene respuesta, lanza una nueva serie de *request* con un TTL inicial de 4, con lo cual llegan a R-WS-R1-NAT con un TTL de 3 (tramas 10, 12 y 14 de la captura en R-10), que enruta con un TTL de 1 (tramas 7, 9 y 11 de la captura en R-44, recuerde que, debido a un *bug* a los paquetes que les hace NAT les resta 2 al TTL) y además, en esta ocasión, SÍ les hace NAT, con lo cual el R-W7-3 las recibe con la IP de origen 44.44.0.100. Inmediatamente R-W7-3 las responde, dirigiéndolas a la IP 44.44.0.100 (tramas 8, 10 y 12 de la captura en R-44), que llegan a R-WS-R1-NAT y las enruta hacia R-W7-1 (tramas 11, 13 y 15 de la captura en R-10), que cuando son recibidas por R-W7-1 originan la última línea del resultado del ***tracert***. Obsérvese que las tramas de petición de eco del R-W7-1 le llegan a R-W7-3 con un TTL de 1, cuando deberían llegar con valor de 2. *Windows Server 2022* le resta dos, al campo TTL de los paquetes de salida, cuando las enruta, debido al *bug* ya conocido.

Como queda demostrado, el original comportamiento obtenido para el ***tracert*** se debe a otro error (*bug*) del *Windows Server 2022* cuando tiene habilitado el NAT.

Una vez configurado el NAT, hay un cambio que podemos hacer en R-W7-3, ya que será posible prescindir de la puerta de enlace que tiene configurada, pues solo recibirá paquetes de su propia subred. Según esto, le eliminaremos de la configuración la puerta de enlace, quedando tal y como se muestra en la Figura 13; y comprobaremos que todo sigue funcionando de la manera ya comentada.

5.- INSTALACIÓN INICIAL DEL ENRUTAMIENTO NAT.

Es posible instalar el enrutamiento NAT sin instalar previamente el enrutamiento convencional, enrutamiento LAN. Para ello, una vez instalado el servicio de enrutamiento, procederemos de la forma siguiente:

Inicio ➔ Herramientas administrativas ➔ Enrutamiento y acceso remoto ➔ Seleccionar el servidor correspondiente (R-WS-R1-NAT) ➔ Botón derecho, opción “Configurar y habilitar Enrutamiento y acceso remoto” ➔ Botón “Siguiente” ➔ En el formulario que se abre, Figura 14, seleccionar la opción “Traducción de direcciones de red (NAT)” ➔ Botón “Siguiente” ➔ En el

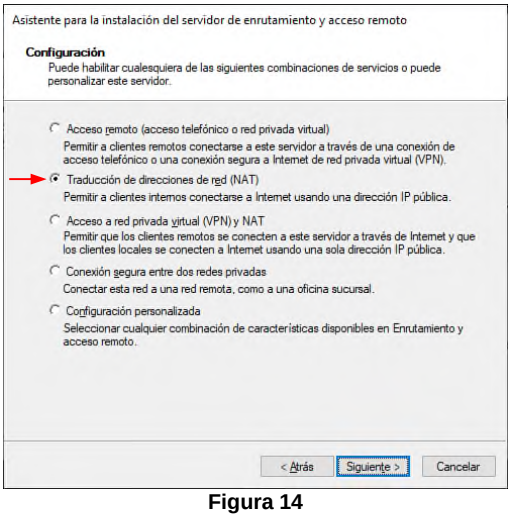


Figura 14

formulario que se abre, seleccionar la interfaz con la IP pública (en este caso, la configurada con la IP 44.44.0.100, “Ethernet 2”), Figura 15 ➔ Botón “Siguiente” ➔ En el nuevo formulario, seleccionar la opción “Configurar más adelante los servicios de nombres y direcciones”, Figura 16 ➔ Botón “Siguiente” ➔ Botón “Finalizar”.

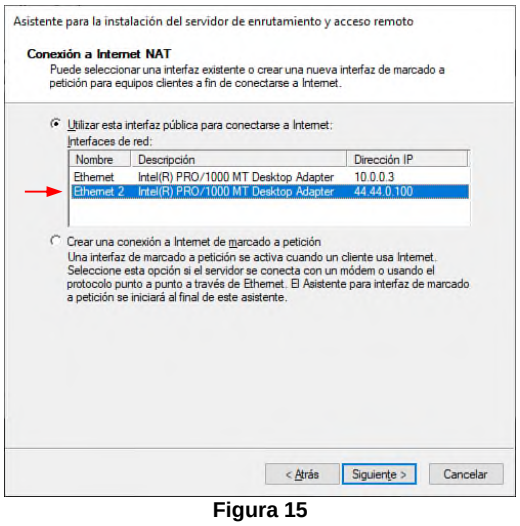


Figura 15

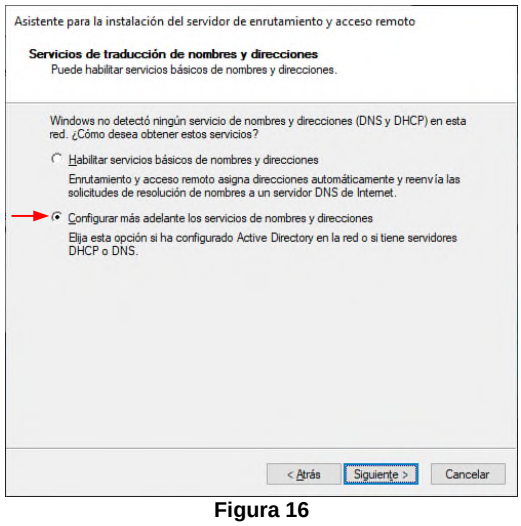


Figura 16

De esta forma tenemos instalado y configurado el servicio de enrutamiento NAT. No olvide cambiar el tipo de inicio del servicio de “Enrutamiento y acceso remoto” de “Automático (Inicio retrasado)” a “Automático”, mediante el procedimiento ya conocido.

Indicar, por último, que utilizando este método de instalación y configuración del servicio NAT, también se instala el protocolo IGMP[1] (***Internet Group Management Protocol***, protocolo de administración de grupos de Internet. Nivel de red) al que, de momento, no prestaremos atención. La instalación del IGMP se pone de manifiesto por la aparición del ítem “IGMP” al mismo nivel, del árbol IPv4, que el “NAT”, tal y como se muestra en la Figura 17.

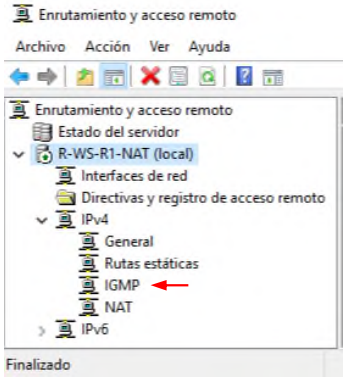


Figura 17

También se instala el protocolo IGMP, si el NAT se selecciona en el formulario de configuración personalizada.

Recuerde que, como principio general de seguridad, no suele ser buena idea el instalar protocolo y/o servicios que no se vayan a utilizar, pues la tendencia general es a desatender su configuración pudiendo crear agujeros de seguridad para el propio sistema. De acuerdo con esto, si una vez instalado el protocolo IGMP se desea eliminarlo, tan solo debemos seleccionarlo y en el menú contextual, botón derecho del ratón, seleccionar la opción eliminar.

6.- NOTA FINALES.

[1] Para IGMP, véase: https://es.wikipedia.org/wiki/Internet_Group_Management_Protocol