

PRÁCTICA SERVIDOR DNS CON WINDOWS SERVER 2019

Antes de empezar la práctica vamos a ver algunos conceptos que hemos visto durante la explicación teórica del tema en clase y vamos a ver en que consiste la búsqueda de zona directa e inversa usando nuestro ordenador en modo terminal. Durante la práctica vamos a usar el comando ping que ya todos conocemos como el comando nslookup que os paso link de su uso por si queréis ampliar vuestro conocimientos.

(<https://www.redeszone.net/tutoriales/internet/nslookup-resolucion-dns-windows/>)

Ejemplo 1 de búsqueda zona directa y en zona inversa

```
C:\Users\USER>ping www.telefonica.es
```

Haciendo ping a www.telefonica.es [141.101.90.97] con 32 bytes de datos:
Respuesta desde 141.101.90.97: bytes=32 tiempo=23ms TTL=57

Respuesta desde 141.101.90.97: bytes=32 tiempo=43ms TTL=57

Respuesta desde 141.101.90.97: bytes=32 tiempo=23ms TTL=57

Respuesta desde 141.101.90.97: bytes=32 tiempo=30ms TTL=57

Estadísticas de ping para 141.101.90.97:

Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),

Tiempos aproximados de ida y vuelta en milisegundos:

Mínimo = 23ms, Máximo = 43ms, Media = 29ms

```
C:\Users\USER>nslookup 141.101.90.97
```

Servidor: Unknown

Address: 192.168.215.40

*** Unknown no encuentra 141.101.90.97: Non-existent domain

```
C:\Users\USER>
```

```
C:\Users\USER>ping www.mercadona.es
```

Haciendo ping a e127230.dsca.akamaiedge.net [96.16.88.150] con 32 bytes de datos:
Respuesta desde 96.16.88.150: bytes=32 tiempo=20ms TTL=56

Respuesta desde 96.16.88.150: bytes=32 tiempo=30ms TTL=56

Respuesta desde 96.16.88.150: bytes=32 tiempo=28ms TTL=56

Respuesta desde 96.16.88.150: bytes=32 tiempo=30ms TTL=56

Estadísticas de ping para 96.16.88.150:

Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),

Tiempos aproximados de ida y vuelta en milisegundos:

Mínimo = 20ms, Máximo = 30ms, Media = 27ms

```
C:\Users\USER>nslookup 96.16.88.150
```

Servidor: Unknown

Address: 192.168.215.40

Nombre: a96-16-88-150.deploy.static.akamaitechnologies.com

Address: 96.16.88.150

Nota: Vamos a refrescar algunos conceptos cuando hago un ping estamos haciendo una búsqueda en zona directa ya que sabemos el nombre de la página web a dónde queremos ir y lo que nos muestra es la información de la dirección IP de a dónde vamos. Cuando usamos el comando nslookup [dirección IP 141.101.90.97] hacemos el proceso contrario por lo que estamos haciendo la búsqueda en zona inversa. Aprovecho para recordar que es el tiempo de vida (TTL) hace referencia a la cantidad de tiempo o "saltos" que se ha establecido que un paquete debe existir dentro de una red antes de ser descartado por un enrutador.

Ejemplo 2 de otra búsqueda en zona inversa y directa / Gráfico de lo que está sucediendo

```
C:\Users\USER>ping www.granada.org
```

Haciendo ping a www.granada.org [85.62.209.9] con 32 bytes de datos:

Respuesta desde 85.62.209.9: bytes=32 tiempo=61ms TTL=115

Respuesta desde 85.62.209.9: bytes=32 tiempo=66ms TTL=115

Respuesta desde 85.62.209.9: bytes=32 tiempo=41ms TTL=115

Respuesta desde 85.62.209.9: bytes=32 tiempo=59ms TTL=115

Estadísticas de ping para 85.62.209.9:

Paquetes: enviados = 4, recibidos = 4, perdidos = 0

(0% perdidos),

Tiempos aproximados de ida y vuelta en milisegundos:

Mínimo = 41ms, Máximo = 66ms, Media = 56ms

```
C:\Users\USER>nslookup www.granada.org
```

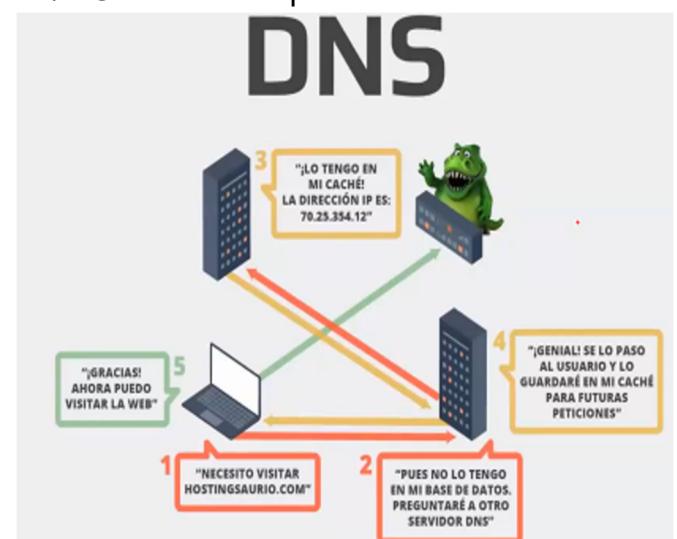
Servidor: Unknown

Address: 192.168.215.40

Respuesta no autoritativa:

Nombre: www.granada.org

Address: 85.62.209.9

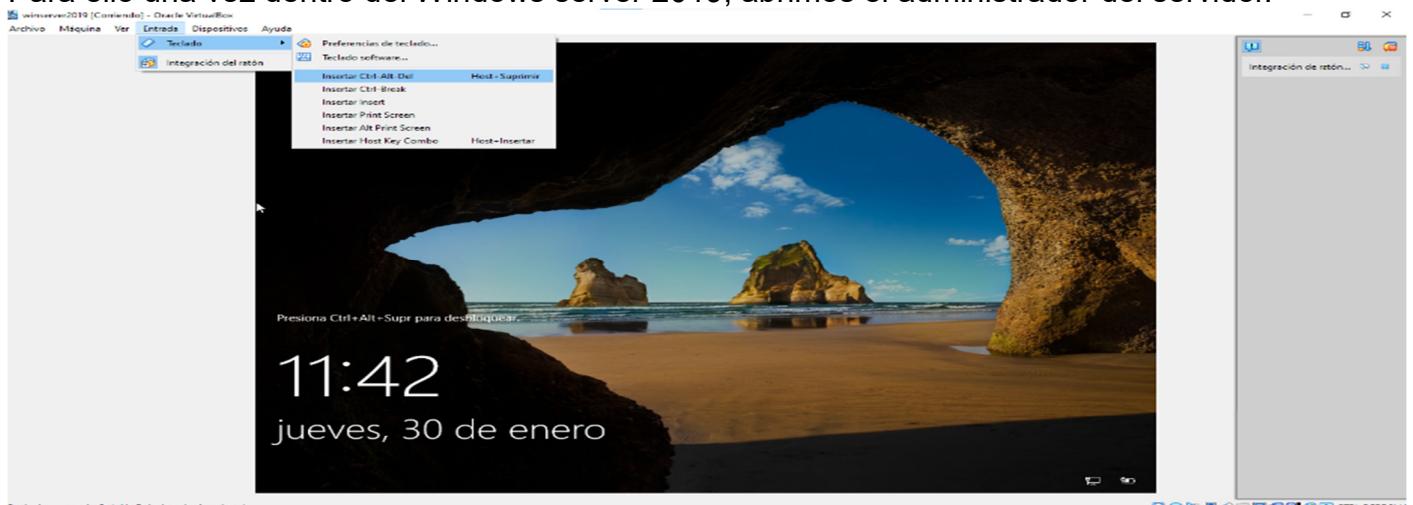


Nota: si veis la respuesta es no autoritativa eso indica que el servidor DNS no tenía la información solicitada y ha tenido que consultarla a otro servidor DNS

Ahora vamos a abrir nuestra máquina virtual donde tenemos instalado el Windows Server 2019 y una vez dentro vamos a abrir el administrador del servidor y vamos a instalar y configurar un servidor DNS para que luego nuestro ordenador anfitrión (El físico) lo use como su servidor DNS. El objetivo es:

1. Saber montar y configurar un servidor DNS en mi máquina virtual con Windows Server 2019.
2. Hacer que ese servidor DNS de mi máquina virtual sea el servidor DNS de mi ordenador anfitrión (el físico)
3. Saber tratar las zonas de búsqueda directa e inversa, como crear host, punteros y la configuración y uso de los reenviadores

Dicho esto y una vez instalado nuestro servidor DNS, vamos a crear una asociación dentro de mi servidor DNS de mi máquina virtual a una página Web, yo he elegido: www.despliegue.com, (pero puedes elegir la que quieras). Actualmente dicha página Web pertenece a otra persona y tiene asignada una dirección IP X (luego la veremos) y lo que vamos a hacer es introducir dicha página Web en mi servidor DNS y asociarlo a una dirección IP distinta. Para que cuando yo pregunte por dicha página y haga mi búsqueda directa e inversa me salga los datos que yo quiero y no los reales. Para ello una vez dentro del Windows server 2019, abrimos el administrador del servidor.



Captura del acceso a Windows server 2019 usando VirtualBox

Una vez dentro abrimos el administrador del servidor. Y vamos a instalar el Servidor DNS haciendo una instalación basada en roles y características

Pero antes vamos a ver entrando en "cmd" en tanto de la máquina anfitrión (el físico) como en la máquina virtual con Windows server 2019 sus direcciones IP

Captura del ordenador anfitrión

```
Adaptador de LAN inalámbrica Wi-Fi:
Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : Intel(R) Centrino(R) Advanced-N 6235
Dirección física. . . . . : C8-F7-33-BE-8C-46
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . . . : sí
Vínculo: dirección IPv6 local. . . . . : fe80::20c8:f09e:94ac:2e85%15(Preferido)
Dirección IPv4. . . . . : 192.168.215.130(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : jueves, 30 de enero de 2025 10:06:31
La concesión expira . . . . . : jueves, 30 de enero de 2025 12:36:26
Puerta de enlace predeterminada . . . . . : 192.168.215.40
Servidor DHCP . . . . . : 192.168.215.40
IAID DHCPv6 . . . . . : 264828723
DUID de cliente DHCPv6. . . . . : 00-01-00-01-23-7C-B0-24-74-28-62-7C-7D-C6
Servidores DNS. . . . . : 192.168.215.40
NetBIOS sobre TCP/IP. . . . . : habilitado
```

Captura máquina virtual Server 2019

```
Adaptador de Ethernet Ethernet:
Sufijo DNS específico para la conexión. . . :
Descripción . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
Dirección física. . . . . : 08-00-27-F7-B9-B4
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . . . : sí
Vínculo: dirección IPv6 local. . . . . : fe80::723b:948b:a7c5:7b38%3(Preferido)
Dirección IPv4. . . . . : 192.168.215.147(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : jueves, 30 de enero de 2025 13:43:57
La concesión expira . . . . . : jueves, 30 de enero de 2025 14:43:55
Puerta de enlace predeterminada . . . . . : 192.168.215.40
Servidor DHCP . . . . . : 192.168.215.40
IAID DHCPv6 . . . . . : 50855975
DUID de cliente DHCPv6. . . . . : 00-01-00-01-2F-20-2B-A8-08-00-27-F7-B9-B4
Servidores DNS. . . . . : 192.168.215.40
NetBIOS sobre TCP/IP. . . . . : habilitado
```

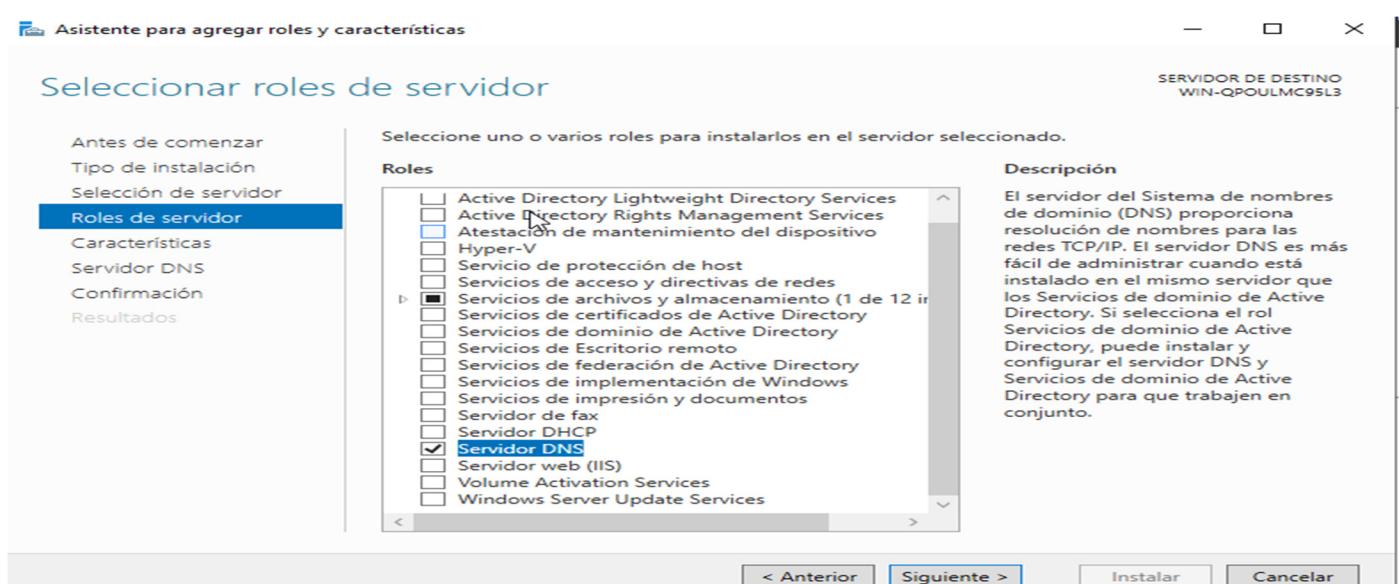
Una vez hecho el paso anterior ahora si, muestro Las capturas con los pasos y el proceso para instalar un servidor DNS por medio de roles y características

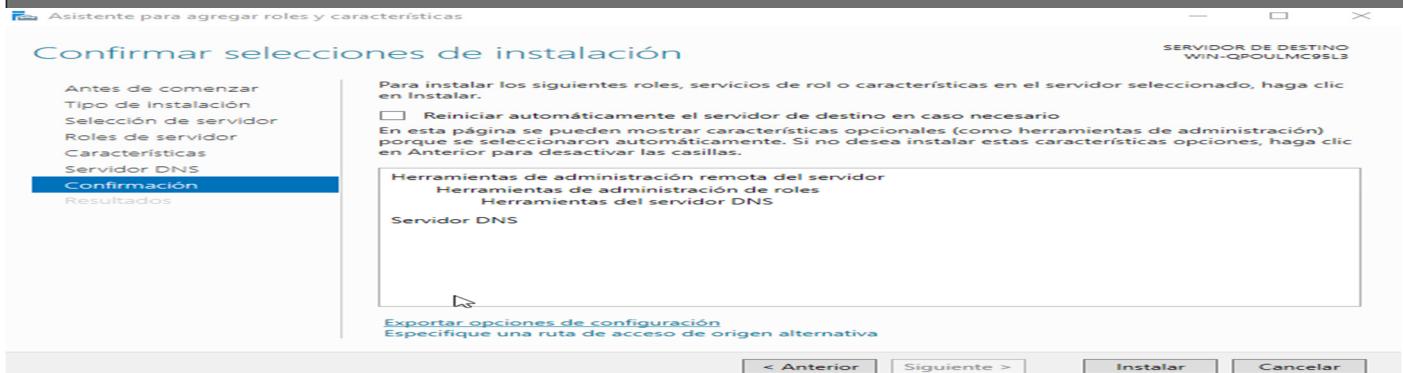
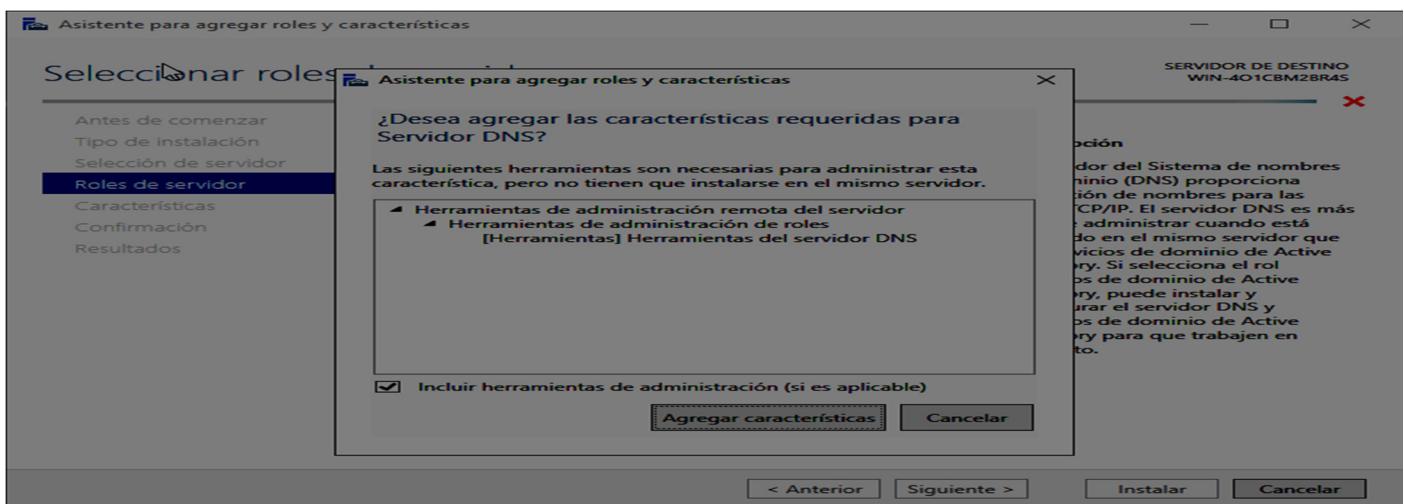


Seleccionamos el servidor y nos fijamos que nuestra dirección IP es 192.168.215.147



Ahora seleccionamos los servicios DNS

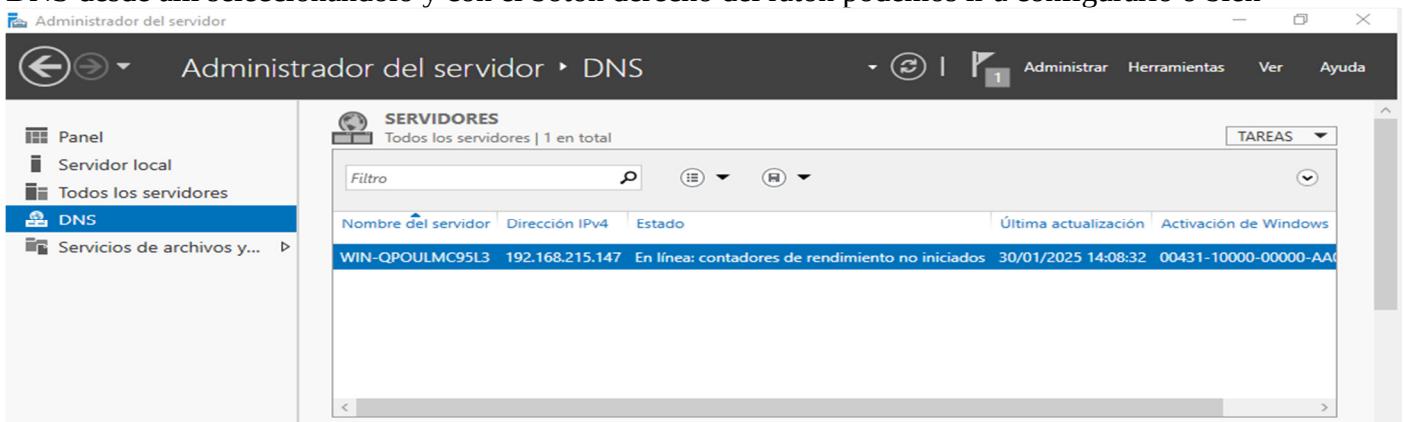




Le damos a instalar y esperamos a que se instalen los roles de DNS esperamos a que se instalen



y una vez que lo hagan nos debería salirnos en la página principal el rol de DNS y vemos nuestro servidor DNS desde allí seleccionándolo y con el botón derecho del ratón podemos ir a configurarlo o bien



Nos vamos a herramientas y pinchamos en DNS para la configuración del servidor DNS



Y ahora vamos a configurar la zonas de búsqueda directa e inversa vamos primero por la zona directa, para lo que vamos a crear una nueva, seleccionamos nuestro servidor luego pinchamos en zona de búsqueda directa y le damos a zona nueva luego le damos a siguiente y seleccionamos zona de tipo principal y le ponemos el nombre en mi caso he puesto despliegue.com, le digo que no admite actualizaciones dinámicas y listo después me saldrá un resumen de la zona directa que acabamos de crear le damos a finalizar y ya por último podemos ver la zona creada

1 Administrador de DNS

2 Asistente para nueva zona

3 Asistente para nueva zona

4 Asistente para nueva zona

5 Asistente para nueva zona

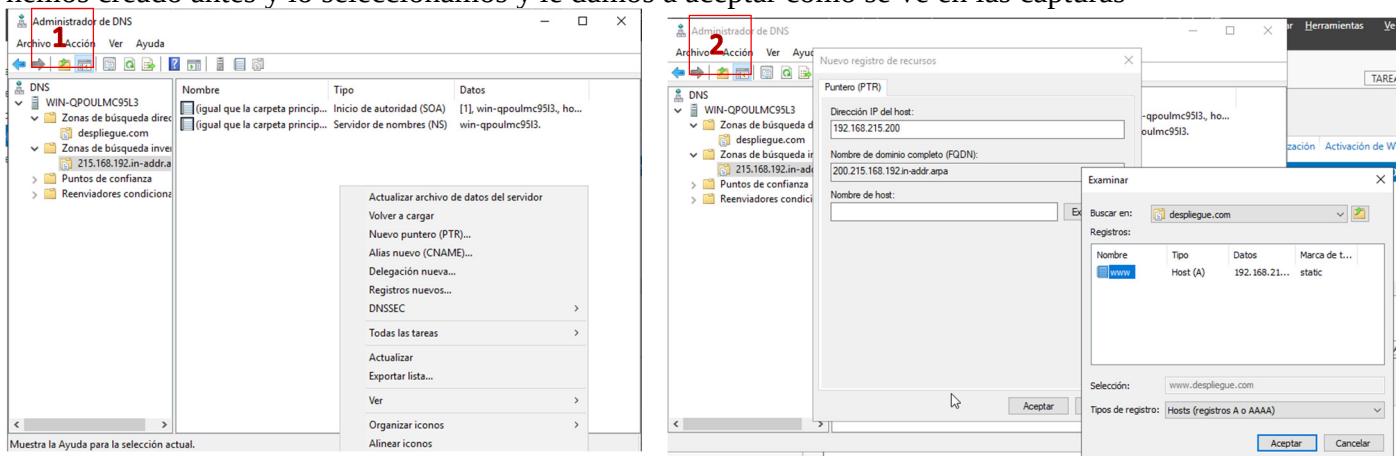
6 Finalización del Asistente para nueva zona

7 Administrador de DNS

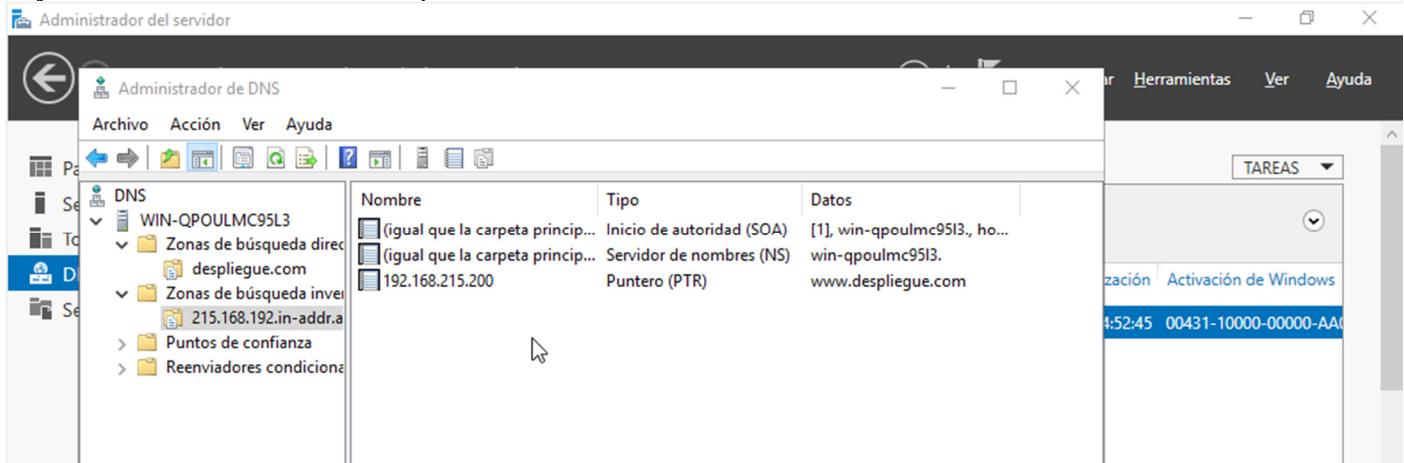
Una vez hecho todos los pasos anteriores nos vamos a la zona de búsqueda inversa seleccionamos zona principal, seleccionamos zona inversa ipv4 y le ponemos la id de nuestra red. Creamos la carpeta, no permitimos las actualizaciones dinámicas y finalizamos. Tal y como vemos en las siguientes capturas

Ahora vamos a crear un Host nuevo pinchamos dentro donde queramos como en la captura y le asignamos los valores de nuestra dirección y agregamos el host fíjate en la dirección IP que le asigno tiene que estar dentro de la subred nuestra y no puedes darle ningún valor que ya esté asignado o reservado(véase captura)

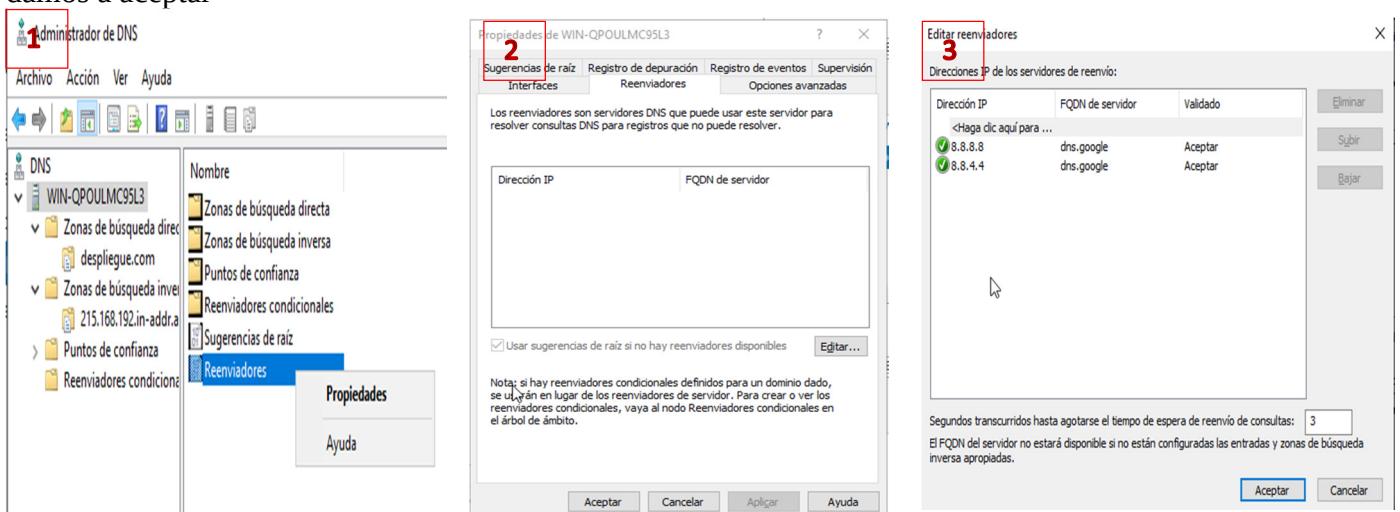
Yo le he puesto la 192.168.215.200, le damos a agregar y listo ya lo tendríamos configurado el host. Ahora vamos a la zona de búsqueda inversa y hacemos nuevo puntero. (vamos a hacerlo al revés que me relacione esta IP del Host con el nombre del host). Para ello nos vamos a la zona inversa pinchamos en la zona ya creada anteriormente y le damos al botón derecho para crear el puntero le ponemos la dirección IP del host que hemos creado antes y lo seleccionamos y le damos a aceptar como se ve en las capturas



Y ya tendríamos creado nuestro puntero



Dicho esto ahora nos tendríamos que ir a nuestro anfitrión es decir a nuestro ordenador física y cambiarle la DNS para que se conecte a nuestro servidor DNS. Ahora tenemos que decirle que si no sabe donde está la ip que la busque en otro sitio ya que la única información que tiene es la de www.despliegue.com. Para eso nos vamos a los reenviadores y lo configuraremos le damos a editar y ponemos las dns de google 8.8.8.8 y 8.8.4.4, le damos a aceptar y listo ya tenemos configurado los reenviadores luego le damos a aplicar y por último le damos a aceptar



De esta forma cuando cambie el adaptador de red vamos a poder seguir trabajando y tener acceso a todo.

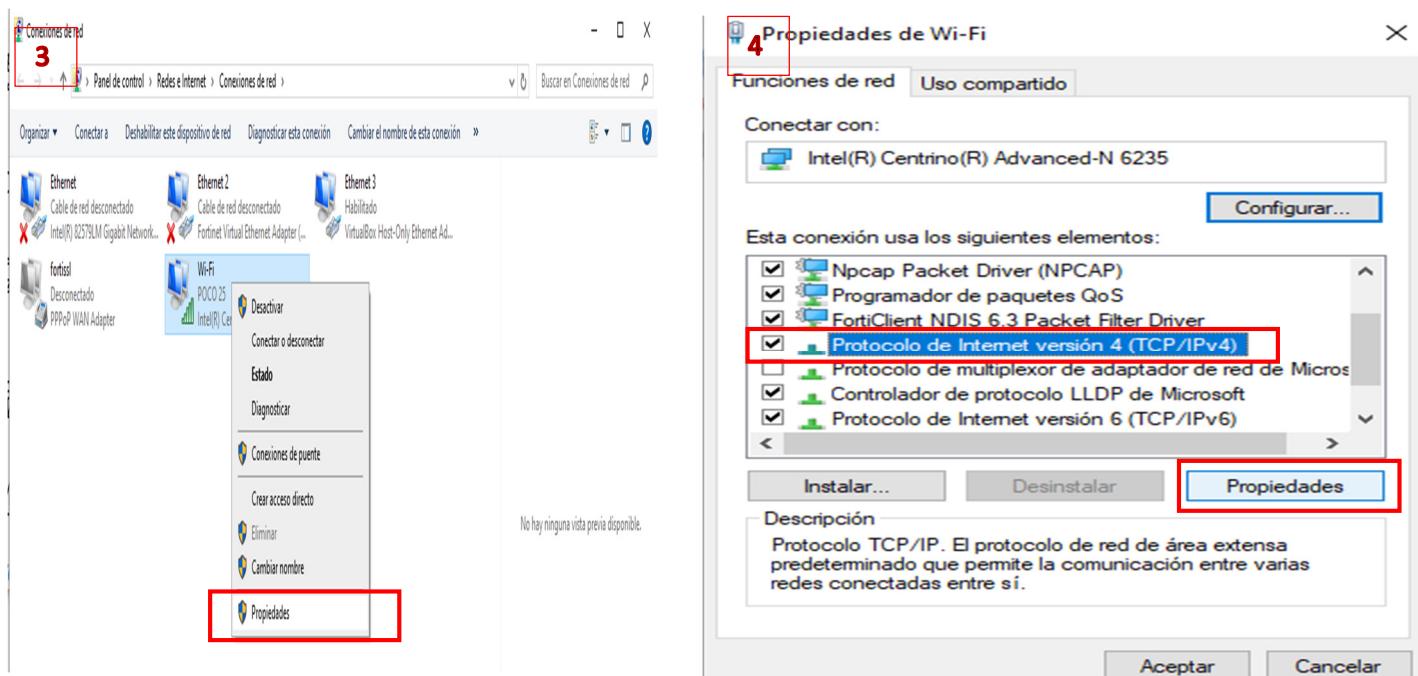
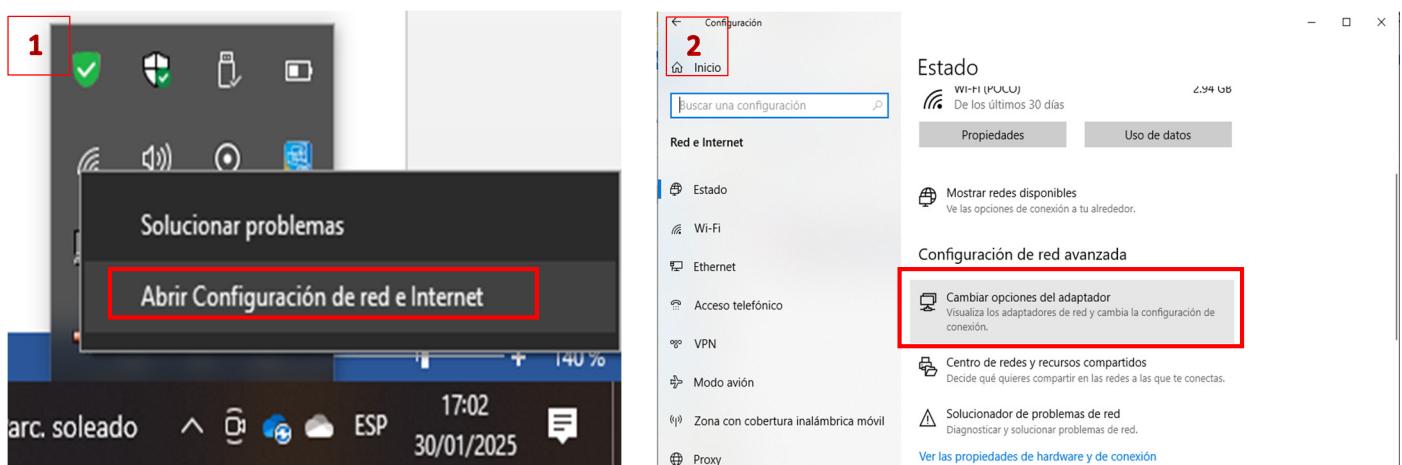
Antes de irnos a nuestro ordenador anfitrión (el Físico) nos vamos al modo terminal y hacemos una búsqueda directa e inversa y vemos las direcciones ip que nos da

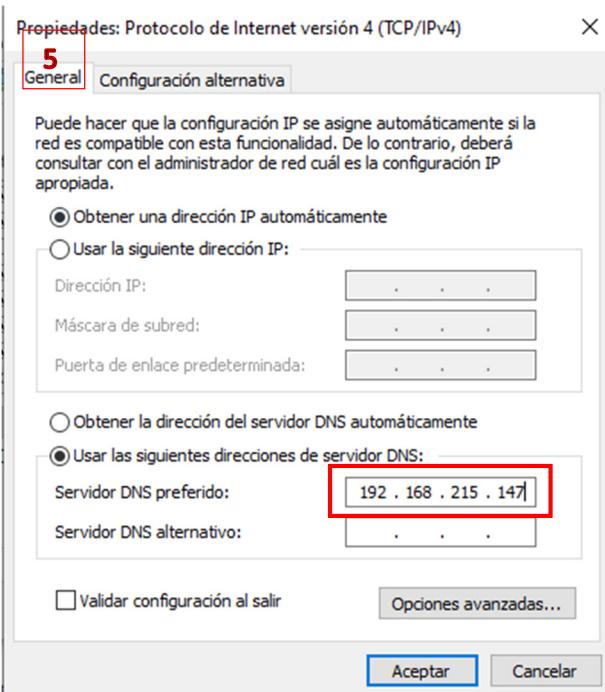
```
C:\Users\USER>ping www.despliegue.com

Haciendo ping a despliegue.com [13.248.243.5] con 32 bytes de datos:
Respuesta desde 13.248.243.5: bytes=32 tiempo=146ms TTL=241
Respuesta desde 13.248.243.5: bytes=32 tiempo=118ms TTL=241
Respuesta desde 13.248.243.5: bytes=32 tiempo=151ms TTL=241
Respuesta desde 13.248.243.5: bytes=32 tiempo=54ms TTL=241

Estadísticas de ping para 13.248.243.5:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 54ms, Máximo = 151ms, Media = 117ms
```

Ahora nos vamos a nuestro ordenador físico y a nuestra conexión de red y en propiedades nos vamos a nuestro protocolo ipv4 y en propiedades ponemos que no use las direcciones automáticas de DNS sino que use la dirección IPv4 de nuestro servidor DNS que acabamos de configurar en nuestro caso la dirección 192.168.215.147, tal y como podemos ver en las siguientes capturas





Nota: recuerda volver a ponerlo de forma dinámica cuando termine la práctica que sino cuando apagues la máquina virtual te vas a quedar sin internet. Porque va a intentar usar el servidor DNS de nuestro Windows Server 2019 y al estar apagado los reenviadores que hemos configurado en nuestro servidor DNS (los de google) no van a funcionar

Ahora comprobamos que sigamos teniendo internet podemos comprobarlo de muchas maneras como por ejemplo abriendo el navegador, después nos volvemos a meter en nuestro cmd de nuestro ordenador anfitrión (el Físico) y hacemos de nuevo la búsqueda directa e inversa y vemos las direcciones que nos da ahora.

Captura mostrando que tengo internet



En la siguiente captura muestro el resultado de la búsqueda en zona directa e inversa tanto usando ping como nslookup y podemos apreciar cómo han cambiado la información que nos muestran dichos comandos apuntando ahora a la dirección que hemos configurado de forma manual en nuestro servidor DNS de nuestra máquina virtual. También podemos comprobar como sólo se ha cambiado la de www.despliegue.com (ver 2)

```
C:\Users\USER>ping www.despliegue.com 1
Haciendo ping a www.despliegue.com [192.168.215.200] con 32 bytes de datos:
Respuesta desde 192.168.215.130: Host de destino inaccesible.

Estadísticas de ping para 192.168.215.200:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
```

```
C:\Users\USER>nslookup 192.168.215.200
Servidor: Unknown
Address: 192.168.215.147

Nombre: www.despliegue.com
Address: 192.168.215.200

2
C:\WINDOWS\system32>nslookup www.despliegue.com
Servidor: Unknown
Address: 192.168.215.147

Nombre: www.despliegue.com
Address: 192.168.215.200

C:\WINDOWS\system32>nslookup 192.158.215.200
Servidor: Unknown
Address: 192.168.215.147

*** Unknown no encuentra 192.158.215.200: Non-existent domain

C:\WINDOWS\system32>nslookup www.telefonica.es
Servidor: Unknown
Address: 192.168.215.147

Respuesta no autoritativa:
Nombre: www.telefonica.es
Addresses: 141.101.90.97
          141.101.90.99
          141.101.90.96
          141.101.90.98

C:\WINDOWS\system32>nslookup 141.101.9097
Servidor: Unknown
Address: 192.168.215.147

*** Unknown no encuentra 141.101.9097: Non-existent domain

C:\WINDOWS\system32>nslookup 141.101.90.97
Servidor: Unknown
Address: 192.168.215.147
```

Aquí ahora muestro aunque quede repetitivo las salidas de las búsquedas de zona directas e inversas de los resultados anteriores con la salida última para que os sea más fácil la comparación. Vemos que sólo se ha modificado la que hemos creado que las otras siguen igual y de paso hemos demostrado que hemos configurado bien los reenviadores y que tenemos conectividad entre nuestro ordenador y la máquina virtual

```
C:\Users\USER>ping www.despliegue.com
```

1

Haciendo ping a despliegue.com [13.248.243.5] con 32 bytes de datos:

Respuesta desde 13.248.243.5: bytes=32 tiempo=146ms TTL=241

Respuesta desde 13.248.243.5: bytes=32 tiempo=118ms TTL=241

Respuesta desde 13.248.243.5: bytes=32 tiempo=151ms TTL=241

Respuesta desde 13.248.243.5: bytes=32 tiempo=54ms TTL=241

Estadísticas de ping para 13.248.243.5:

Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),

Tiempos aproximados de ida y vuelta en milisegundos:

Mínimo = 54ms, Máximo = 151ms, Media = 117ms

```
C:\Users\USER>nslookup 13.248.243.5
```

Servidor: UnKnown

Address: 192.168.215.40

Nombre: a16e665f42988324c.awsglobalaccelerator.com

Address: 13.248.243.5

```
C:\Users\USER>ping www.despliegue.com
```

Haciendo ping a www.despliegue.com [192.168.215.200] con 32 bytes de datos:

Respuesta desde 192.168.215.130: Host de destino inaccesible.

Estadísticas de ping para 192.168.215.200:

Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),

```
C:\Users\USER>nslookup 192.168.215.200
```

Servidor: UnKnown

Address: 192.168.215.147

Nombre: www.despliegue.com

Address: 192.168.215.200

```
Paquetes: enviados = 4, recibidos = 4, perdidos = 0  
(0% perdidos),
```

Tiempos aproximados de ida y vuelta en milisegundos:

Mínimo = 54ms, Máximo = 151ms, Media = 117ms

```
C:\Users\USER>nslookup 13.248.243.5
```

Servidor: UnKnown

Address: 192.168.215.40

Nombre: a16e665f42988324c.awsglobalaccelerator.com

Address: 13.248.243.5

```
C:\Users\USER>ping www.despliegue.com
```

Haciendo ping a www.despliegue.com [192.168.215.200] con 32 bytes de datos:

Respuesta desde 192.168.215.130: Host de destino inaccesible.

Estadísticas de ping para 192.168.215.200:

Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),

```
C:\Users\USER>nslookup 192.168.215.200
```

Servidor: UnKnown

Address: 192.168.215.147

Nombre: www.despliegue.com

Address: 192.168.215.200

```
C:\Users\USER>ping www.telefonica.es
```

Haciendo ping a www.telefonica.es [141.101.90.98] con 32 bytes de datos:

Respuesta desde 141.101.90.98: bytes=32 tiempo=40ms TTL=53

Respuesta desde 141.101.90.98: bytes=32 tiempo=51ms TTL=53

Respuesta desde 141.101.90.98: bytes=32 tiempo=44ms TTL=53

Respuesta desde 141.101.90.98: bytes=32 tiempo=44ms TTL=53

Estadísticas de ping para 141.101.90.98:

Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),

Tiempos aproximados de ida y vuelta en milisegundos:

Mínimo = 40ms, Máximo = 51ms, Media = 44ms

```
C:\Users\USER>nslookup 141.101.90.98
```

Servidor: UnKnown

Address: 192.168.215.147

Nota: Recordar que en la práctica donde montamos el servidor FTP aprendimos o refrescamos como poner una dirección estática en las máquinas

Aprovechando esta práctica vamos a aprender o a refrescar como verificar la conectividad entre la máquina anfitrión y las máquinas virtuales o entre distintos equipos conectados a una red. Si bien, si miráis por internet en muchos sitios para ello desactiva directamente el cortafuegos, el Defender en caso de Windows o el UFW o similar en caso de distribuciones Linux.

¡¡¡ ANTES DE CONTINUAR LEER EL RESTO DE LA PRÁCTICA DE FORMA COMPLETA Y LLEGANDO HASTA EL FINAL Y LUEGO REPLICAR LOS PASOS INDICANDO EL ANTES Y EL DESPUÉS !!!

Nosotros en lugar de eso nos vamos a ir a dicho cortafuegos y dentro de su configuración avanzada vamos a activar las reglas de entrada y salida que nos afecta y no nos permite que podamos ver dicha conectividad usando el comando ping ya que por normal general tenemos desactivada esa función. Para ello nos vamos a nuestras diferentes máquinas y buscamos nuestros cortafuegos, pinchamos en opciones avanzadas y después no vamos a nuestras reglas de entrada y salida y habilitamos la opción que os marco en las capturas. Sólo muestro las captura en una de nuestros equipos tendríamos que hacerlo en los equipos que les afecte y activar las reglas de entrada o de salida o ambas según los resultados al hacer la comprobaciones de conectividad.

Screenshot 1: Firewall de Windows Defender main window. A red box highlights the 'Configuración' section on the left sidebar.

Screenshot 2: Firewall de Windows Defender settings page. A red box highlights the 'Configuración avanzada' link under 'Solución de problemas de red'.

Screenshot 3: Windows Defender Firewall with advanced security window. A red box highlights the 'Reglas de entrada' section on the left sidebar.

Después de hacerlo en ambas máquinas vamos a identificar los distintos equipos usando el comando hostname después vemos la conectividad a ellos mismos (Nota: si nos devuelve una salida de tipo IPv6 y queremos que sea de tipo IPv4 sólo poner al final de hacer el ping [.....] -4, como podemos ver en las capturas. Para probar la conectividad tocaría probar la conexión con las distintas puertas de enlace de los distintos equipos y que ya teníamos desde el principio de la práctica cuando hicimos nuestro ipconfig /all en ambos equipos y después entre los dos equipos/máquinas.

```
C:\ Administrador: Símbolo del sistema
(100% perdidos),
Control-C
^C
C:\Users\Administrador>ping DESKTOP-Q2685J6 -4

Haciendo ping a DESKTOP-Q2685J6.local [192.168.215.130] con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 192.168.215.130:
Paquetes: enviados = 4, recibidos = 0, perdidos = 4
(100% perdidos),

C:\Users\Administrador>ping DESKTOP-Q2685J6 -4

Haciendo ping a DESKTOP-Q2685J6.local [192.168.215.130] con 32 bytes de datos:
Respuesta desde 192.168.215.130: bytes=32 tiempo<1ms TTL=128
Respuesta desde 192.168.215.130: bytes=32 tiempo=1ms TTL=128
Respuesta desde 192.168.215.130: bytes=32 tiempo<1ms TTL=128
Respuesta desde 192.168.215.130: bytes=32 tiempo<1ms TTL=128

Estadísticas de ping para 192.168.215.130:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 0ms, Máximo = 1ms, Media = 0ms

C:\Users\Administrador>
```

En esta captura vemos lo que pasa cuando intentamos hacer ping a nuestro propio equipo antes y después de activar las reglas de nuestro firewall

```
C:\ Símbolo del sistema
(100% perdidos),
Control-C
^C
C:\Users\USER>PING win-qpouulmc95l3 -4

Haciendo ping a WIN-QPOULMC95L3.local [192.168.215.147] con 32 bytes de datos:
Tiempo de espera agotado para esta solicitud.

Estadísticas de ping para 192.168.215.147:
Paquetes: enviados = 4, recibidos = 0, perdidos = 4
(100% perdidos),

C:\Users\USER>PING win-qpouulmc95l3 -4

Haciendo ping a win-qpouulmc95l3 [192.168.215.147] con 32 bytes de datos:
Respuesta desde 192.168.215.147: bytes=32 tiempo<1ms TTL=128

Estadísticas de ping para 192.168.215.147:
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\USER>
```

En esta captura vemos lo que pasa cuando intentamos hacer ping a nuestro propio equipo antes y después de activar las reglas de nuestro firewall

Nota: Dado que no hice capturas verificando conectividades puesto que creo que todo el mundo sabe hacerlo muestro un ejemplo de cómo se haría pero con otros valores de ip, eso sí muestro sólo las salidas una vez ya habiendo habilitado las reglas del cortafuegos.

Captura 1: muestra dirección ip y puerta de enlace (server2019)

```
C:\Users\Administrador>ipconfig /all

Configuración IP de Windows

Nombre de host . . . . . : WIN-QPOULMC95L3
Sufijo DNS principal . . . . . :
Tipo de nodo. . . . . : híbrido
Enrutamiento IP habilitado. . . . . : no
Proxy WINS habilitado . . . . . : no

Adaptador de Ethernet Ethernet:

    Sufijo DNS específico para la conexión. . . . . :
    Descripción . . . . . . . . . . . . . . . . . . . . . . : Intel(R) PRO/1000 MT Desktop Adapter
    Dirección física. . . . . . . . . . . . . . . . . . . . . . : 08-00-27-BC-44-C5
    DHCP habilitado . . . . . . . . . . . . . . . . . . . . . . : sí
    Configuración automática habilitada . . . . . . . . . . . . . . : sí
    Dirección IPv4. . . . . . . . . . . . . . . . . . . . . . . . . : 192.168.89.244(Preferido)
    Máscara de subred . . . . . . . . . . . . . . . . . . . . . . . : 255.255.255.0
    Concesión obtenida. . . . . . . . . . . . . . . . . . . . . . . : miércoles, 5 de febrero de 2025 15:09:57
    La concesión expira . . . . . . . . . . . . . . . . . . . . . . . : miércoles, 5 de febrero de 2025 16:09:59
    Puerta de enlace predeterminada . . . . . . . . . . . . . . . . . : 192.168.89.236
    Servidor DHCP . . . . . . . . . . . . . . . . . . . . . . . . . : 192.168.89.236
    Servidores DNS. . . . . . . . . . . . . . . . . . . . . . . . . : 192.168.89.236
    NetBIOS sobre TCP/IP. . . . . . . . . . . . . . . . . . . . . . . : habilitado
```

Captura 2: muestra conectividad consigo mismo, puerta de enlace y el nombre del equipo (server2019) en la captura supletoria muestro la conectividad con el anfitrión

```
C:\Users\Administrador>hostname
WIN-QPOULMC95L3

C:\Users\Administrador>ping WIN-QPOULMC95L3

Haciendo ping a WIN-QPOULMC95L3 [::1] con 32 bytes de datos:
Respuesta desde ::1: tiempo<1m
Respuesta desde ::1: tiempo<1m
Respuesta desde ::1: tiempo<1m
Respuesta desde ::1: tiempo<1m

Estadísticas de ping para ::1:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Administrador>ping WIN-QPOULMC95L3 -4

Haciendo ping a WIN-QPOULMC95L3 [192.168.89.244] con 32 bytes de datos:
Respuesta desde 192.168.89.244: bytes=32 tiempo<1m TTL=128

Estadísticas de ping para 192.168.89.244:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Administrador>ping 192.168.89.236

Haciendo ping a 192.168.89.236 con 32 bytes de datos:
Respuesta desde 192.168.89.236: bytes=32 tiempo=5ms TTL=64
Respuesta desde 192.168.89.236: bytes=32 tiempo=5ms TTL=64
Respuesta desde 192.168.89.236: bytes=32 tiempo=6ms TTL=64
Respuesta desde 192.168.89.236: bytes=32 tiempo=4ms TTL=64

Estadísticas de ping para 192.168.89.236:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 4ms, Máximo = 6ms, Media = 5ms
```

```
C:\Users\Administrador>hostname
WIN-QPOULMC95L3

C:\Users\Administrador>ping 192.168.89.130

Haciendo ping a 192.168.89.130 con 32 bytes de datos:
Respuesta desde 192.168.89.130: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.89.130: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.89.130: bytes=32 tiempo<1m TTL=128
Respuesta desde 192.168.89.130: bytes=32 tiempo=1ms TTL=128

Estadísticas de ping para 192.168.89.130:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
    (0% perdidos),
Tiempos aproximados de ida y vuelta en milisegundos:
    Mínimo = 0ms, Máximo = 1ms, Media = 0ms
```

Ahora nos vamos al otro equipo en mi caso el anfitrión y repetimos el proceso

Captura 1: salida ipconfig /all ordenador anfitrión

Adaptador de LAN inalámbrica Wi-Fi:

```
Sufijo DNS específico para la conexión. . . . . : 
Descripción . . . . . : Intel(R) Centrino(R) Advanced-N 6235
Dirección física. . . . . : C8-F7-33-BE-8C-46
DHCP habilitado . . . . . : sí
Configuración automática habilitada . . . . . : sí
Vínculo: dirección IPv6 local. . . . . : fe80::20c0:f09e:94ac:2e85%17(Preferido)
Dirección IPv4. . . . . : 192.168.89.130(Preferido)
Máscara de subred . . . . . : 255.255.255.0
Concesión obtenida. . . . . : miércoles, 5 de febrero de 2025 14:50:16
La concesión expira . . . . . : miércoles, 5 de febrero de 2025 16:24:21
Puerta de enlace predeterminada . . . . . : 192.168.89.236
Servidor DHCP . . . . . : 192.168.89.236
IAID DHCPv6 . . . . . : 264828723
DUID de cliente DHCPv6. . . . . : 00-01-00-01-23-7C-BD-24-74-2B-62-7C-7D-C6
Servidores DNS. . . . . : 192.168.89.236
NetBIOS sobre TCP/IP. . . . . : habilitado
```

Captura 2: conectividad ip, puerta enlace, máquina virtual Server2019 y nombre de mi equipo físico

C:\Users\USER>ping 192.168.89.130

```
Haciendo ping a 192.168.89.130 con 32 bytes de datos:
Respuesta desde 192.168.89.130: bytes=32 tiempo<1m TTL=128
```

Estadísticas de ping para 192.168.89.130:

```
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
```

Tiempos aproximados de ida y vuelta en milisegundos:

```
Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

C:\Users\USER>ping 192.168.89.236

```
Haciendo ping a 192.168.89.236 con 32 bytes de datos:
Respuesta desde 192.168.89.236: bytes=32 tiempo=6ms TTL=64
Respuesta desde 192.168.89.236: bytes=32 tiempo=4ms TTL=64
Respuesta desde 192.168.89.236: bytes=32 tiempo=8ms TTL=64
Respuesta desde 192.168.89.236: bytes=32 tiempo=4ms TTL=64
```

Estadísticas de ping para 192.168.89.236:

```
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
```

Tiempos aproximados de ida y vuelta en milisegundos:

```
Mínimo = 4ms, Máximo = 8ms, Media = 5ms
```

C:\Users\USER>ping 192.168.89.244

```
Haciendo ping a 192.168.89.244 con 32 bytes de datos:
Respuesta desde 192.168.89.244: bytes=32 tiempo<1m TTL=128
```

Estadísticas de ping para 192.168.89.244:

```
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
```

Tiempos aproximados de ida y vuelta en milisegundos:

```
Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

C:\Users\USER>hostname

DESKTOP-Q2685J6

C:\Users\USER>ping 192.168.89.244

```
Haciendo ping a 192.168.89.244 con 32 bytes de datos:
Respuesta desde 192.168.89.244: bytes=32 tiempo<1m TTL=128
```

Estadísticas de ping para 192.168.89.244:

```
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
```

Tiempos aproximados de ida y vuelta en milisegundos:

```
Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

C:\Users\USER>hostname

DESKTOP-Q2685J6

C:\Users\USER>ping win-qpoulm95l3 -4

```
Haciendo ping a win-qpoulm95l3 [192.168.89.244] con 32 bytes de datos:
Respuesta desde 192.168.89.244: bytes=32 tiempo<1m TTL=128
```

Estadísticas de ping para 192.168.89.244:

```
Paquetes: enviados = 4, recibidos = 4, perdidos = 0
(0% perdidos),
```

Tiempos aproximados de ida y vuelta en milisegundos:

```
Mínimo = 0ms, Máximo = 0ms, Media = 0ms
```

C:\Users\USER>

Nota: Para ver la diferencia lo suyo sería probar la conectividad entre equipos antes de configurar el cortafuegos y después (Espero que haya quedado claro)