

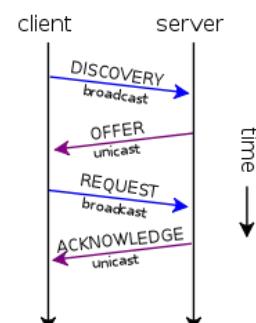
# Protocolo de configuración dinámica de host (DHCP)

Autores: Pineda y Schaab

Teniendo en cuenta que la definición de protocolo es “Conjunto de reglas que rigen el funcionamiento de un sistema”, podemos entender que **DHCP** es un protocolo de red del tipo que *relaciona al cliente con el servidor*. Es un protocolo que se encarga de asignar una IP a cada dispositivo dentro de una red, además de otros parámetros de configuración de red (tales como nombres DNS, servidores NTP, entre otros). Aquel que comprende el protocolo puede supervisar y distribuir desde un mismo punto las direcciones IP, y de forma automática, reasignar nuevas IPs si se diera el caso de que un dispositivo se conecte desde un lugar distinto en la red.

DHCP nace debido a que se utilizaba el protocolo RARP (Reverse Address Resolution Protocol), pero éste era un protocolo de la capa de enlace de datos que hacía que fuese muy tedioso de utilizar en múltiples plataformas de servidores, entonces se reemplazó por BOOTP, siendo uno de los primeros métodos para asignar direcciones IP de forma dinámica. A su vez, BOOTP, que requería intervención manual para completar la información de configuración de cada cliente y no se podían recuperar las direcciones IP en desuso, fue extendido con DHCP, que si entregaba una gran variedad de parámetros de configuración extra a los clientes IP y además tenía la capacidad de asignar muchas más IPs en las redes actuales, que cada vez eran más grandes. Finalmente en 2003 se documentó DHCPv6 y más tarde se complementó con otros RFC (documentación extensa sobre el funcionamiento de Internet y redes, englobando protocolos, procedimientos, entre otros).

El protocolo DHCP tiene tres formas de asignación de direcciones IP: **asignación manual o estática** (nos permite crear un listado de direcciones IP y MAC como par, con el objetivo de que a una determinada dirección física siempre se le proporcione la misma dirección IP y así poder controlar el flujo de clientes), **asignación automática** (le asigna una dirección IP a una máquina cliente la primera vez que ésta realiza una solicitud al servidor DHCP hasta que el cliente la libera. Se suele utilizar cuando el número de clientes no varía demasiado) y **asignación dinámica** (es el único método que permite la reutilización dinámica de las direcciones IP. El administrador asigna un rango de direcciones y todos los dispositivos que se conecten pueden pedirle al servidor una dirección cuando su tarjeta de red se inicializa). El funcionamiento del protocolo DHCP consta de cuatro procesos principales, **Discovery**, **Offer**, **Request** y **Acknowledge**. La comunicación entre servidor y cliente suele darse a través de, del lado servidor, el protocolo UDP puerto 67, y del lado cliente, se utiliza también UDP pero en el puerto 68. En la **primera instancia**, **Discovery**, el cliente no cuenta con una dirección IP asignada, por lo que va a intentar encontrar una, enviando un mensaje a la red. Para ello envía una dirección IP de origen 0.0.0.0, junto a una dirección IP de destino 255.255.255.255, esta es la IP de broadcast global, dentro de un datagrama a la vez que otros datos a completar por el servidor. Un datagrama es un conjunto de información hecha por el protocolo UDP, contiene IP de origen y destino, a la vez que otros datos relevantes para los protocolos que la utilizan. De existir y encontrar,



dentro de la misma red, un servidor funcional, le enviará una respuesta al cliente, llamada **Offer**. Esta respuesta, en forma de datagrama y de tipo unicast, contiene una IP de origen propio del servidor, y de destino la IP es 255.255.255.255, con los respectivos puertos 67 y 68, sin sumarle otro tipo de información más que la dirección IP que el servidor puede otorgar junto a la dirección MAC a asociar. Cuando el cliente recibe la respuesta, envía un **Request**. Vuelve a enviar de forma broadcast la solicitud de IP que el servidor le ofreció junto a la configuración ofrecida. Como situación final, el servidor envía un **Acknowledge**, confirmando que recibió correctamente la información que se configuró, duración de la conexión, información de los servidores DNS, servidor NTP, entre otros datos. Una vez el servidor termine de configurarse correctamente dada la nueva información, el cliente comenzará a recibir información del protocolo ARP, junto a los otros equipos que pertenecen a la red local. Esto evita conflictos entre direcciones IP o superposición de grupos de direcciones en los servidores. En caso de error, el servidor genera un mensaje de **Decline** indicando que la dirección IP ya está en uso.

El sistema no es perfecto y cuenta con una falla importante en cuanto a seguridad. Los servidores DHCP no cuentan con autenticación por parte del servidor, lo cual termina por permitir que en una red con un DHCP legítimo, surja otro servidor DHCP malicioso. Si el hecho mencionado llegara a ocurrir, como el cliente tiende a mandar el mensaje a todas las direcciones de la red, en caso de que la primera en contestar su Discovery fuera la maliciosa, ésta podría proveerle datos que, más adelante, podría aprovechar. Con éste tipo de ataque, llamado “Rogue DHCP Server”, el atacante podría cortar la conexión a Internet de los usuarios que estuvieran en su red, a la vez que podría reenviarle a los dispositivos involucrados resultados maliciosos, ya que él controlaría el DNS y por lo tanto el flujo de datos. La forma de evitar que surjan, o por lo menos que no afecten, los servidores Rogue es implementando la tecnología de los switches, DHCP Snooping, que bloquea los DHCP Offer y DHCP Acknowledge de los puertos donde no esté permitido. Otro ataque más común es aquel en el que se envían demasiadas solicitudes de IP al servidor, consiguiendo que este colapse debido al flujo excesivo de datos y por lo tanto genera que toda la red caiga al no poder otorgar más direccionamientos en la red.

## Implementación.

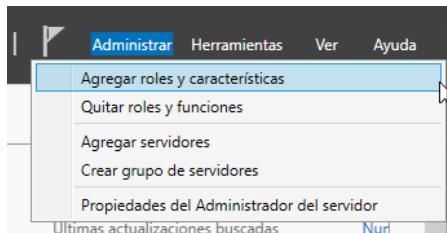
El método de implementación del protocolo DHCP que elegimos fue, dentro de un servidor, modificar algunos parámetros del propio protocolo. Para ello decidimos utilizar “VirtualBox” de Oracle para emular un sistema operativo de Windows Server, específicamente la versión de 2019. Al momento de conseguir el ISO para emular este sistema operativo, nos encontramos con la dificultad de que Microsoft había eliminado de su página oficial la posibilidad de descargar de forma gratuita una extensión de prueba de Windows Server 2019. Debido a esto, recurrimos a obtenerlo por otros medios. Cercano a la fecha de entrega, el link de la página de Microsoft ya se encontraba funcional, por lo que se puede conseguir de forma oficial el ISO, asegurando la confiabilidad del sistema debido a no ser de terceros sino de una empresa importante que no tomaría el riesgo de difundir ISOs maliciosos. Una vez instalado y levantado el sistema operativo, debemos configurar el propio servidor con lo justo y necesario para poder aplicar cambios al protocolo en cuestión. Dentro de la aplicación “Administrador del servidor”, dentro del servidor local, debíamos definir que tipo de características iba a tener el servidor, por lo cual instalamos únicamente la opción de “Servidor DHCP”, para poder acceder a la instalación de características se entra en “Administrar”>“Agregar roles y características” y allí podremos elegir sobre que servidor queremos instalar las características<sup>1</sup>. Tras haber instalado la característica de DHCP<sup>2</sup>, cambiamos de “Adaptador de puente” a “Red interna”, con tal de cambiar nuestra IP. Para ello accedemos al símbolo de la barra que refiere a las redes, click derecho y accedemos a preferencias de red que es donde podremos modificar el tipo de red en la que queremos estar<sup>3</sup>. Para cambiar la IP accedemos a la propiedad de Ethernet de nuestro servidor local, e ir adentrandonos en las propiedades hasta llegar a las mismas de “Protocolo de Internet versión 4 (TCP/IPv4)”, donde podremos configurar la IP propia y la máscara de red a la vez que las direcciones de servidor DNS<sup>5</sup>. Una vez realizado el proceso previo podemos empezar a modificar algunos parámetros de DHCP.

En un primer momento nos dirigimos a Herramientas>DHCP<sup>6</sup> y allí en nuestro servidor en la sección de IPv4 hacemos click derecho y generamos un ámbito nuevo<sup>7</sup> con tal de poder aplicar las normas de DHCP al servidor. Nombramos al ámbito y continuamos con definir el rango de IPs que contempla este ámbito, poniendo la propia IP que pusimos en el servidor como la primera pero empezando el rango después de la nuestra, el último número<sup>8</sup>. Luego podemos configurar aquellas direcciones IPs que queremos excluir del rango contemplado, de no querer restringir ninguna, simplemente no se llenan los campos<sup>9</sup>. Luego se define el intervalo de tiempo en el que un cliente puede usar una IP de ese ámbito hasta volver a cambiarla, tiempos más largos tienden a utilizarse para redes con equipos de escritorio fijos mientras que con redes con clientes móviles con equipos portátiles o de acceso telefónico es conveniente utilizar intervalos cortos<sup>10</sup>. Lo siguiente es una consulta de si se quiere implementar el ámbito ahora o más tarde pero la siguiente es más relevante. Podemos definir la puerta de enlace predeterminada, utilizando la IP propia del servidor aunque se pueden agregar una lista de estas y ordenarlas por prioridad<sup>11</sup>. En la siguiente sección podemos agregar un dominio predeterminado para la parte del DNS, pero como no contamos con ella no modificamos ningún parámetro de esta sección<sup>12</sup>. Otra opción a poder configurar es sobre los servidores WINS, una sección propia de Windows que se trata de un convertidor de IPs en base a los nombres de equipos NetBIOS, otro parámetro más que es posible configurar pero no vamos a modificar<sup>13</sup>. Se vuelve a consultar si se quiere implementar el ámbito ahora o más tarde, siendo esta la última consulta que el asistente

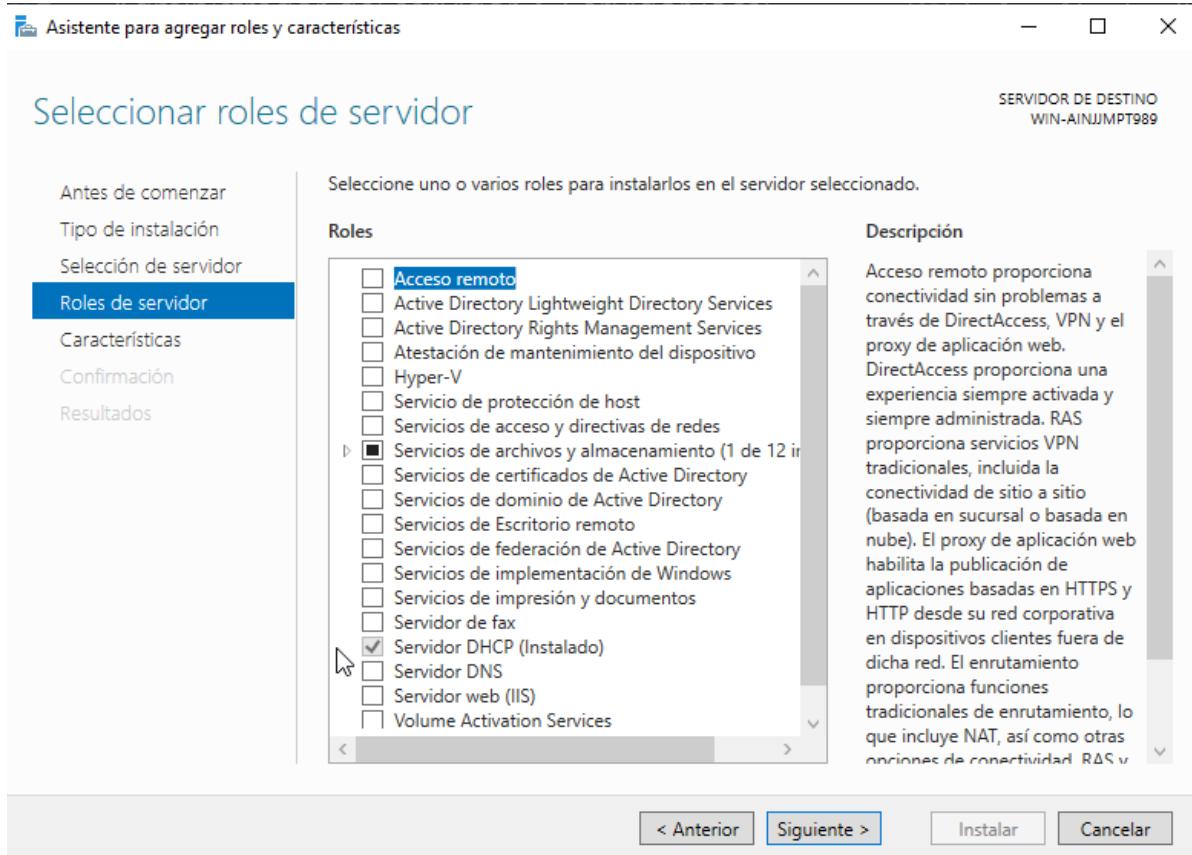
hace antes de crear el nuevo ámbito. Una vez finalizado podemos ver que se generó una carpeta dentro de IPv4 con el nombre del ámbito que definimos en un principio, y si accedemos a las propiedades de este podemos ver los parámetros que definimos e inclusive modificarlos<sup>14</sup>.

## Preparación para la implementación

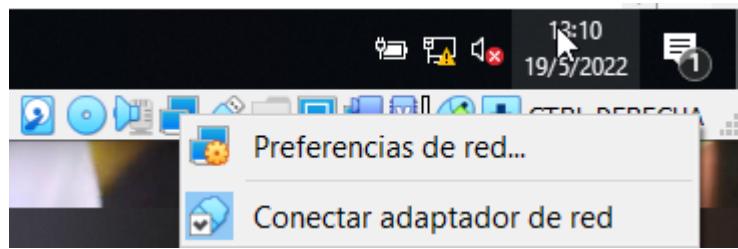
1-



2-



3-



4-

PROPIEDADES		TAREAS	
Nombre de equipo	WIN-AINJJMPT989	Últimas actualizaciones instaladas	Nunca
Grupo de trabajo	WORKGROUP	Últimas actualizaciones buscadas	Nunca
Firewall de Windows Defender	Público: Activado	Antivirus de Windows Defender	Protegido
Administración remota	Habilitado	Comentarios y diagnósticos	Conectado
Escrivtorio remoto	Deshabilitado	Configuración de seguridad mejorada de IE	Activada
Formación de equipos de NIC	Deshabilitado	Zona horaria	(UTC+00:00)
Ethernet	<a href="#">190.129.1.10 IPv6</a> [Habilitado]	Id. del producto	004
versión del sistema operativo	Microsoft Windows Server 2019 Standard Evaluation	Procesadores	Intel
Información de hardware	innotek GmbH VirtualBox	Memoria instalada (RAM)	2 GiB
		Espacio total en disco	24,4

5-

Propiedades: Protocolo de Internet versión 4 (TCP/IPv4) X

General

Puede hacer que la configuración IP se asigne automáticamente si la red es compatible con esta funcionalidad. De lo contrario, deberá consultar con el administrador de red cuál es la configuración IP apropiada.

Obtener una dirección IP automáticamente

Usar la siguiente dirección IP:

Dirección IP:	190 . 129 . 1 . 10
Máscara de subred:	255 . 255 . 255 . 0
Puerta de enlace predeterminada:	190 . 129 . 1 . 0

Obtener la dirección del servidor DNS automáticamente

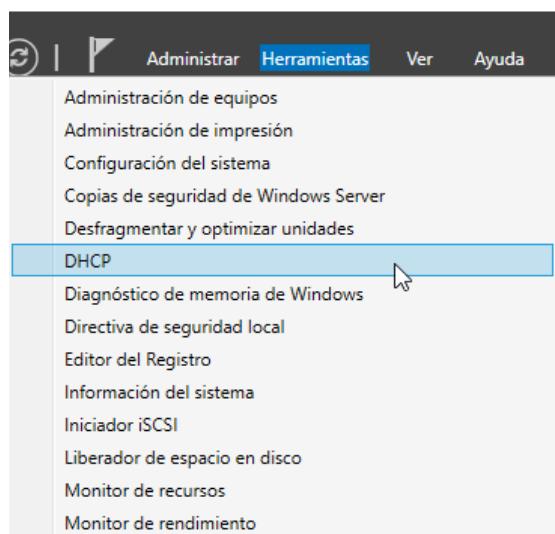
Usar las siguientes direcciones de servidor DNS:

Servidor DNS preferido:	190 . 129 . 1 . 10
Servidor DNS alternativo:	8 . 8 . 8 . 8

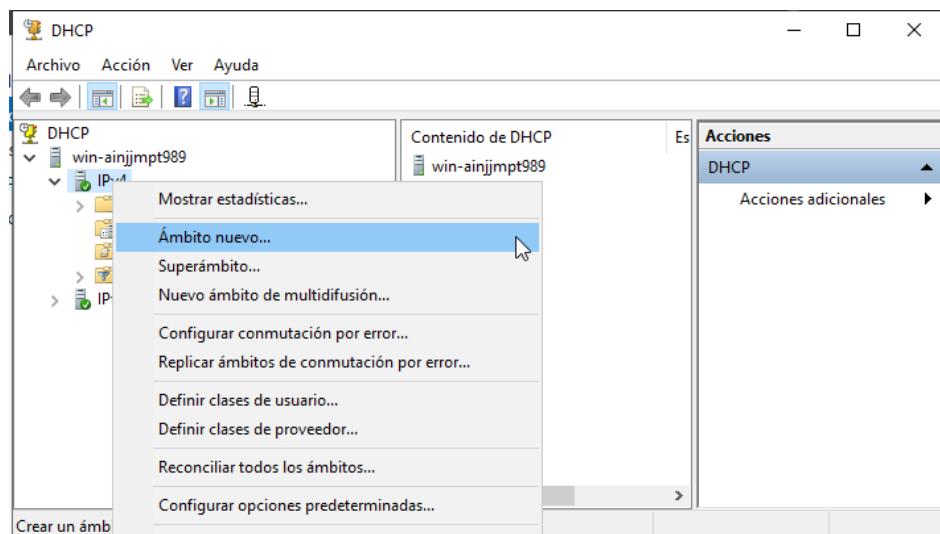
Validar configuración al salir

## Inicio de la implementación

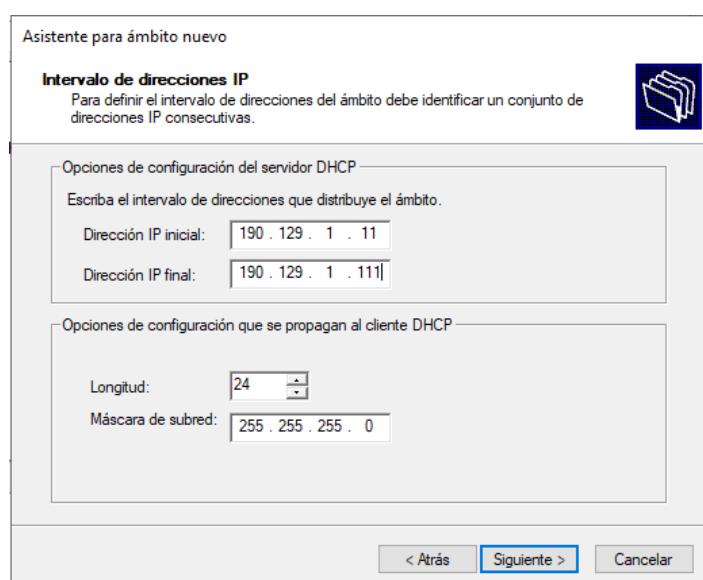
6-



7-



8-



9-

Asistente para ámbito nuevo

**Agregar exclusiones y retraso**

Exclusiones son direcciones o intervalos de direcciones que no son distribuidas por el servidor. Retraso es el tiempo que retrasará el servidor la transmisión de un mensaje DHCPOFFER.



Escriba el intervalo de direcciones IP que desea excluir. Si desea excluir una sola dirección, escriba solo una dirección en Dirección IP inicial.

Dirección IP inicial:      Dirección IP final:

Agregar

Intervalo de direcciones excluido:

Quitar

Retraso de subred en milisegundos:

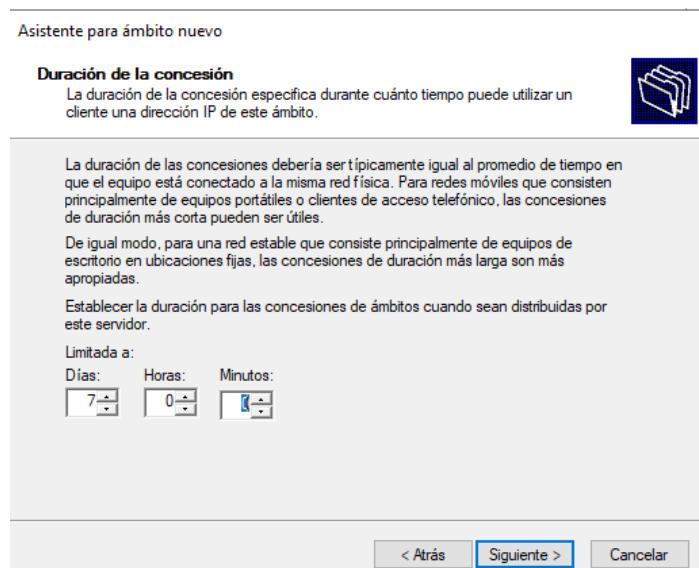
 0

< Atrás

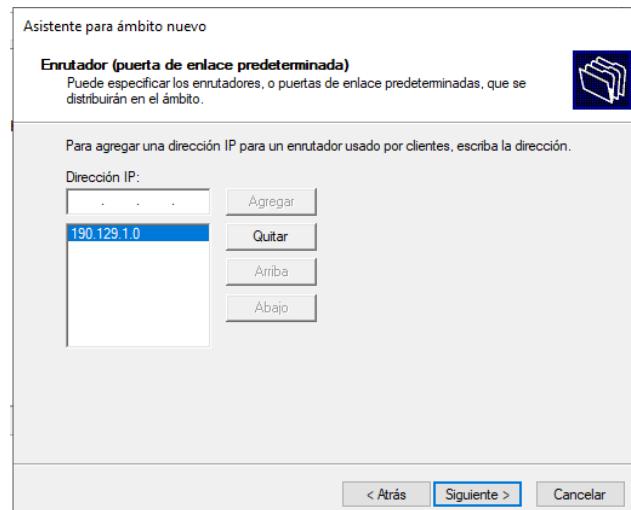
Siguiente >

Cancelar

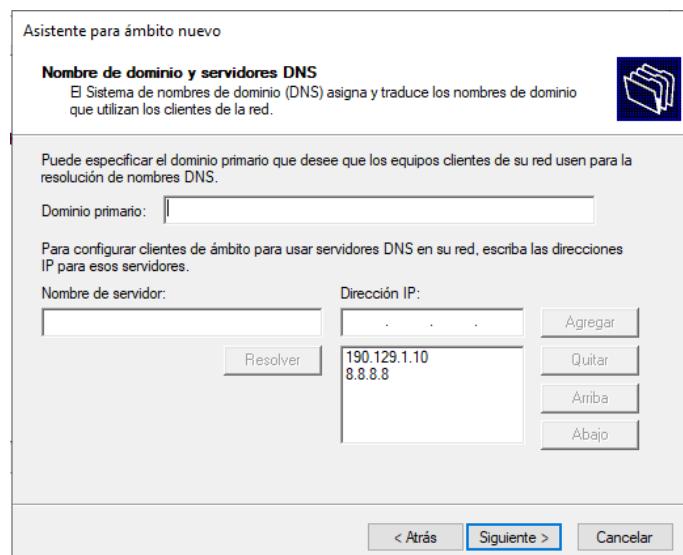
10-



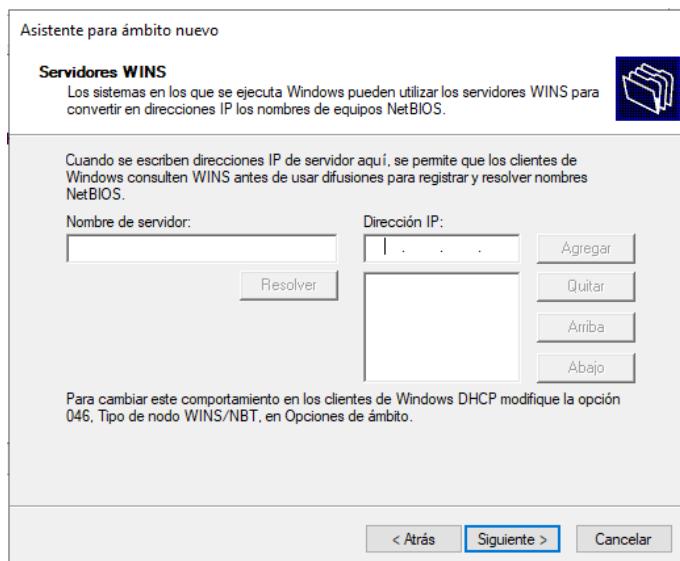
11-



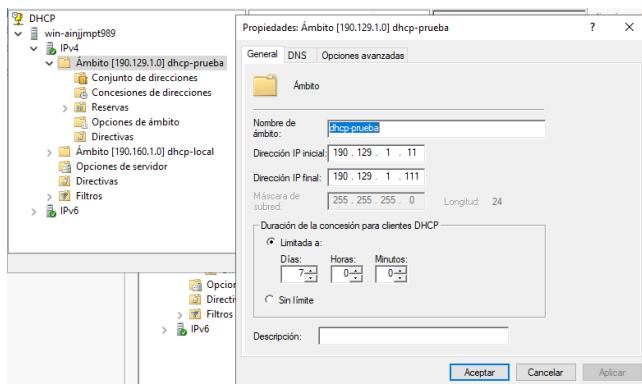
12-



13-



14-



## Bibliografía

<https://www.youtube.com/watch?v=fUK6d3s1Im4>

<https://www.youtube.com/watch?v=cwSKZReA0gQ>

<https://www.redeszone.net/tutoriales/internet/que-es-protocolo-dhcp/>

[https://es.wikipedia.org/wiki/Protocolo\\_de\\_configuraci%C3%B3n\\_din%C3%A1mica\\_de\\_host](https://es.wikipedia.org/wiki/Protocolo_de_configuraci%C3%B3n_din%C3%A1mica_de_host)

<https://datatracker.ietf.org/doc/html/rfc2132>

<https://www.ionos.es/digitalguide/servidores/know-how/unicast/>

[https://es.wikipedia.org/wiki/Protocolo\\_de\\_datagramas\\_de\\_usuario](https://es.wikipedia.org/wiki/Protocolo_de_datagramas_de_usuario)

<https://www.ugr.es/~fernala/Untitled.pdf>

ISO de Windows Server 2019:

1. <https://web.archive.org/web/20210612190353/https://www.microsoft.com/es-es/evalcenter/evaluate-windows-server-2019-essentials>
  - a. <https://www.microsoft.com/es-es/evalcenter/evaluate-windows-server-2019-essentials>
2. <https://web.archive.org/web/20211215124551/https://www.microsoft.com/es-es/evalcenter/evaluate-windows-server-2019>
  - a. <https://www.microsoft.com/es-es/evalcenter/evaluate-windows-server-2019>
3. <https://www.microsoft.com/es-es/evalcenter/download-windows-server-2019>

Tanto el primer link como el segundo muestran cómo eran las páginas de descarga del ISO de Windows Server 2019 en los últimos dos años, al momento de realizar la búsqueda e intentar realizar la implementación del protocolo, ambos links dirigían a "<https://www.microsoft.com/en-us/download>". Actualmente dirigen al tercer link, ahora funcional, que si tiene el ISO del sistema operativo. Si uno intenta encontrar la fecha que otorga Google de una página (agregando &as\_qdr=y15 en el link de búsqueda de Google), ninguno de los tres links aparecen pero si aparecen varios links de microsoft.com con el subíndice /evalcenter que fueron modificados o agregados hace menos de una semana.

Link de como conocer las fechas de aparición de una página web:

<https://david.mu/experimentos/indexacion/como-saber-la-fecha-de-publicacion-de-una-pagina-web>