

Configuración de DHCP en EVPN/VXLAN IOS XE

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de la red](#)

[Configuraciones](#)

[Configuración del servidor](#)

[Opción 1 de configuración de Win2012 R2: IP de retransmisión única por VNI/SVI por VTEP](#)

[Opción 2 de configuración de Win2012 R2: haga coincidir el campo ID del circuito del agente](#)

[Configuración de Windows Server 2016](#)

[Servidor DHCP de Linux](#)

[Configuración del switch](#)

[El cliente DHCP se encuentra en el VRF del arrendatario y el servidor DHCP se encuentra en el VRF predeterminado de la Capa 3](#)

[El cliente DHCP y el servidor DHCP se encuentran en el mismo VRF de arrendatario](#)

[Cliente DHCP en un VRF arrendatario y servidor DHCP en otro VRF arrendatario](#)

[Cliente DHCP en un VRF arrendatario y servidor DHCP en otro VRF no VXLAN](#)

[Información Relacionada](#)

Introducción

Este documento describe la configuración del protocolo de configuración dinámica de host (DHCP) para la LAN extensible virtual (VXLAN) Ethernet VPN (EVPN) en diferentes escenarios y aspectos específicos para los servidores DHCP Win2012 y Win2016.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento de EVPN/VXLAN y DHCP.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

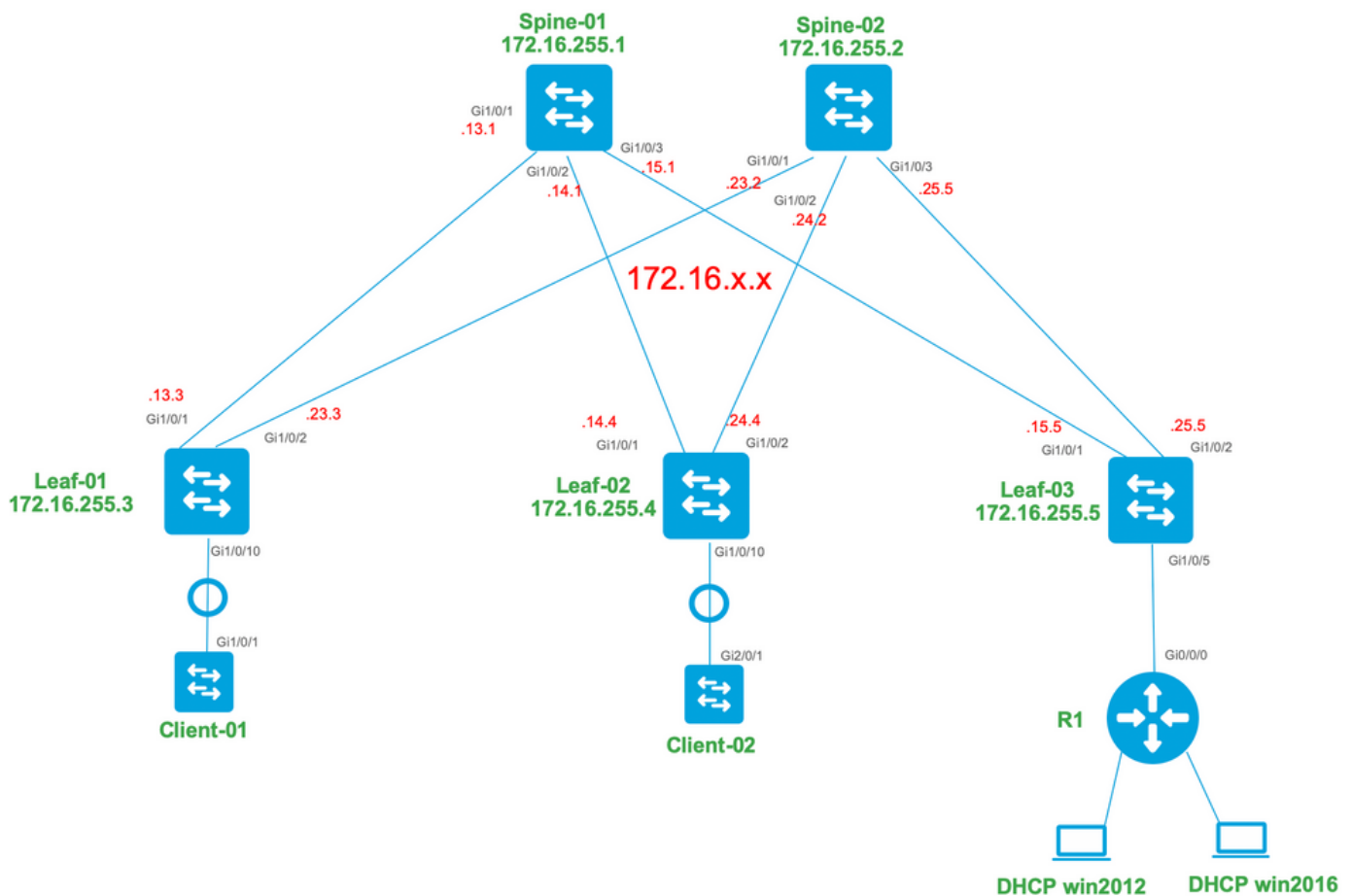
- C9300
- C9400

- C9500
- C9600
- MSFT Windows Server 2012 R2
- MSFT Windows Server 2016
- Funciones disponibles en Cisco IOS XE 16.9.x o posterior

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Configurar

Diagrama de la red

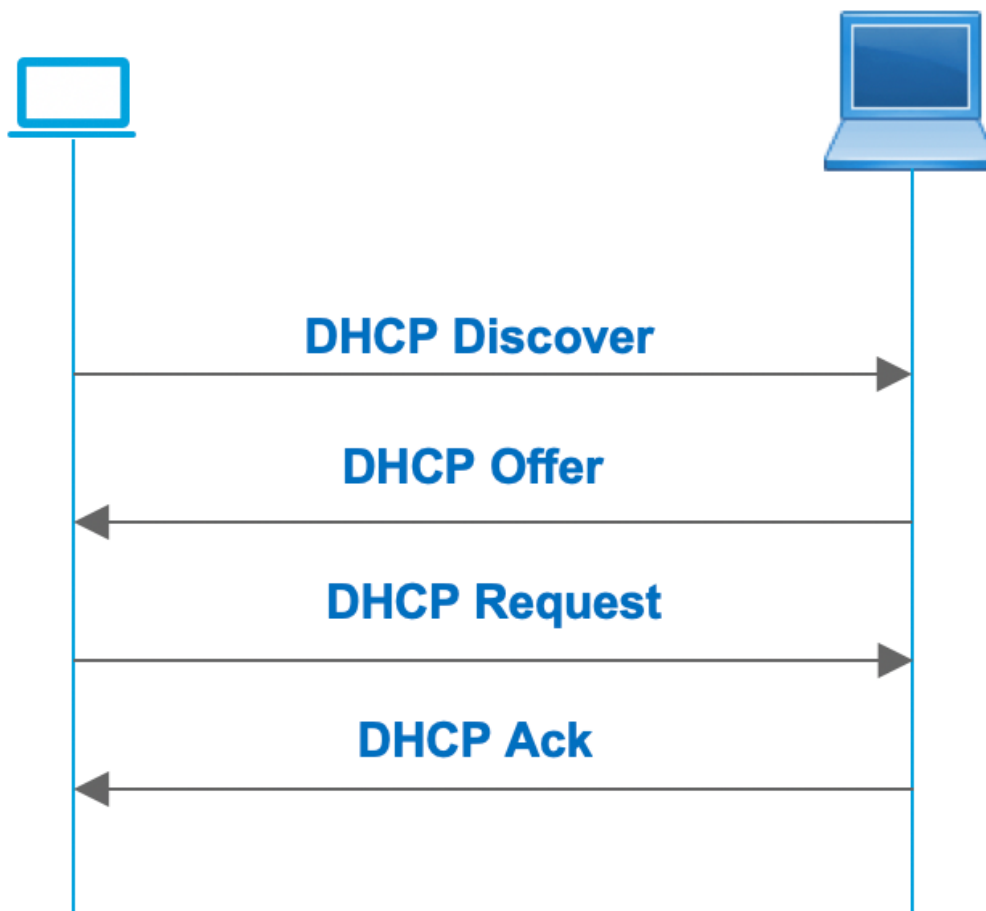


Configuraciones

Ahora, revisemos el flujo de mensajes entre el cliente DHCP y el servidor. Hay 4 fases:

DHCP client

DHCP server



Esto funciona para los casos en los que el cliente y el servidor se encuentran en la misma subred, sin embargo, normalmente, este no es el caso. En la mayoría de los casos, el servidor DHCP no está en la misma subred con el cliente y debe ser accesible a través de una trayectoria enrutada de capa 3 frente a la capa 2. En este caso, se requiere la funcionalidad de relé DHCP. La función DHCP relay (switch o router) convierte la difusión en unicast encapsulado por udp que es enrutable y la envía al servidor DHCP. En la actualidad, se trata de una configuración muy utilizada en las redes.

Retos con el fabric DHCP y EVPN/VXLAN:

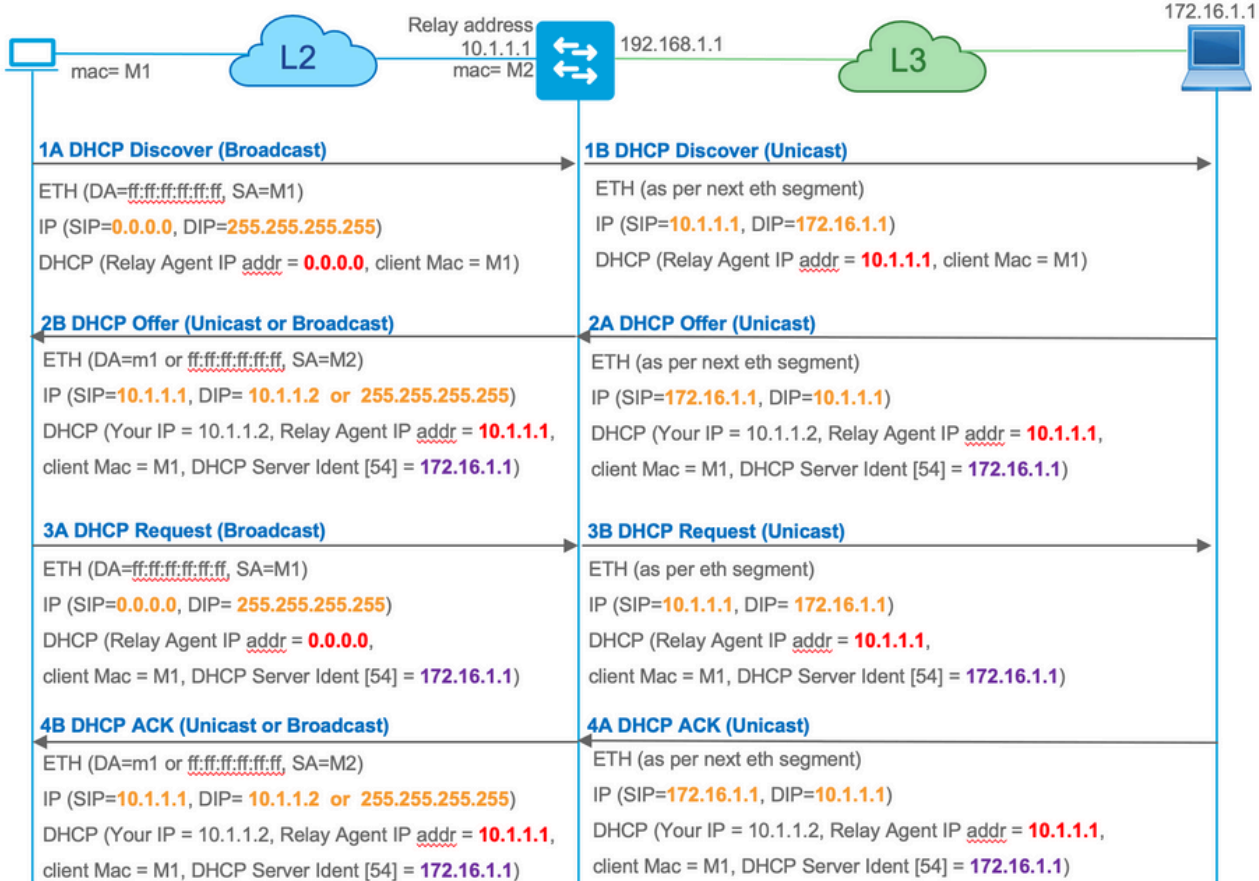
Normalmente, el servidor DHCP se conecta al fabric EVPN a través de la red L3. Esto significa que debe utilizar la funcionalidad de relé DHCP para convertir un paquete de broadcast DHCP de capa 2 en un paquete enrutable unicast de capa 3.

Con la función DHCP relay, el flujo de llamadas DHCP entre el cliente, relay y el servidor funciona de manera similar a esto:

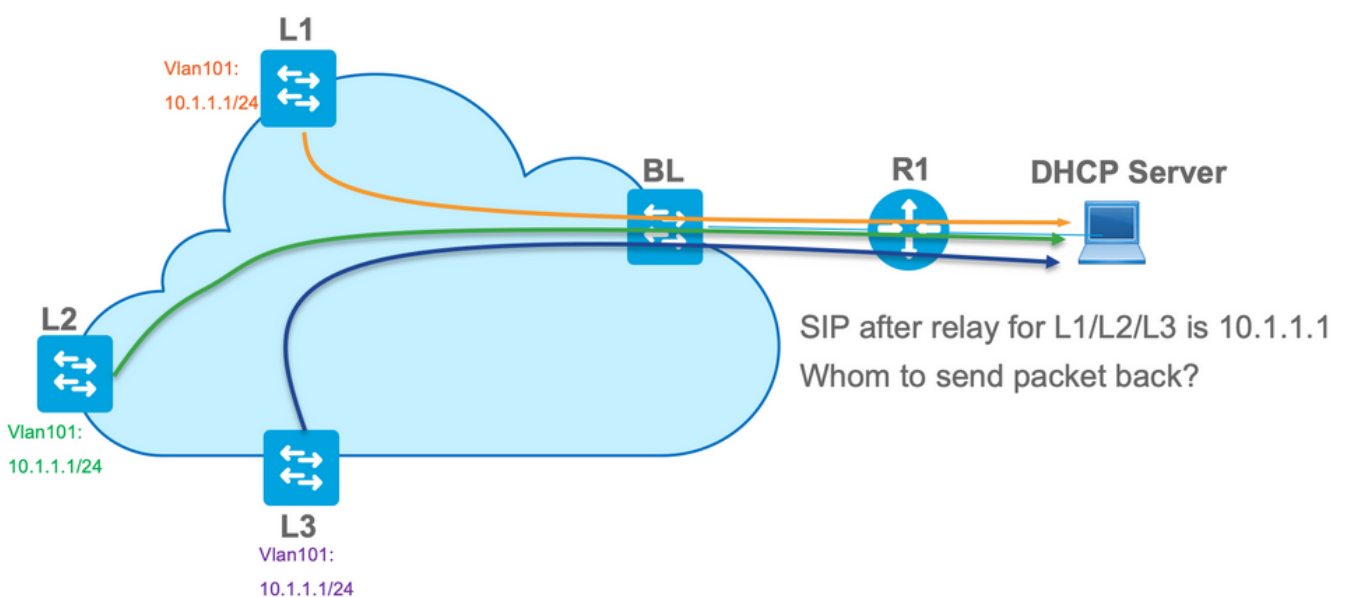
DHCP client

DHCP relay

DHCP server



Una vez retransmitida, la IP de origen del paquete es la IP de retransmisión. Sin embargo, esto crea un problema en la implementación de VXLAN/EVPN, ya que la IP de origen habitual no es única debido al uso de GW de difusión distribuida (DAG). Debido a que todas las IP de origen VTEP SVI son iguales, esto puede hacer que los paquetes de respuesta del servidor DHCP se reenvíen a la hoja más cercana.



Para resolver el problema de origen no único, debe poder utilizar una dirección IP única para los paquetes DHCP retransmitidos por hoja. Otro problema está relacionado con la sustitución de GIADDR. En el servidor DHCP, debe elegir el conjunto correcto para asignar la dirección IP. Se

realiza desde el conjunto, que cubre la dirección IP (giaddr) de la puerta de enlace. Para el entramado EVPN, debe ser una dirección IP de SVI, pero después del relay, el giaddr se reemplaza por una dirección IP relay que en este caso es un loopback único.

¿Cómo puede informar al servidor DHCP, qué agrupamientos debe utilizar?

Para resolver este problema, se utiliza la opción 82. Principalmente, estas son las subopciones importantes:

- 1 - La **ID del circuito del agente**. En el caso de VXLAN/EVPN, esta subopción transfiere la ID de VNI
- 5 - (o 150 para cisco owner). Las subopciones de **selección de link** que tienen una subred real, de la cual proviene el paquete DHCP
- 11 - (o 152 para cisco owner). La subopción **Server Identifier Override** que tiene la **dirección del servidor DHCP**
- 151 - El **nombre VRF/ID de VPN**. Esta subopción tiene el nombre de VRF/ID de VPN

En una captura de paquetes del paquete desde el relé DHCP al servidor DHCP, puede ver estas diversas opciones presentes en el paquete DHCP como se muestra en la imagen.

The screenshot shows a DHCP Discover packet with the following details:

- Transaction ID: 0x00019a3
- Relay agent IP address: 10.1.251.1 (highlighted as Relay Agent/Giaddr)
- Option 82 (Agent Information Option):
 - Suboption (1) Agent Circuit ID: 010a00000002775010a0000 (highlighted as Agent Circuit ID (VNI encoded))
 - Suboption (151) VRF name/VPN ID
 - Suboption (150) Link selection (Cisco proprietary): 10.1.101.0 (highlighted as Link Selection (pool from which ip_address should be assigned))
 - Suboption (152) Server ID Override (Cisco proprietary): 10.1.101.1 (highlighted as Server ID override (used for redirecting DHCP renew over relay))

Configuración del switch:

- La opción 82 tiene toda la información necesaria para elegir el conjunto DHCP correcto y devolver el paquete del servidor a la hoja correcta.
- Esto sólo funciona si el servidor DHCP puede procesar la información de la opción 82, aunque no todos los servidores la soportan completamente (como win2012 r2).

```

ip dhcp relay information option vpn          <<< adds the VRF name/VPN ID to the option 82
ip dhcp relay information option            <<< enables option 82
!
ip dhcp snooping vlan 101-102,201-202
ip dhcp snooping
!
vlan configuration 101
member evpn-instance 101 vni 10101
!
interface Loopback101
 vrf forwarding green
 ip address 10.1.251.1 255.255.255.255
!
interface Vlan101
 vrf forwarding green
ip dhcp relay source-interface Loopback101  <<< DHCP relay source is unique Loopback
 ip address 10.1.101.1 255.255.255.0
 ip helper-address 192.168.20.12          <<< 192.168.20.12 - DHCP server

```

Configuración del servidor

Opción 1 de configuración de Win2012 R2: IP de retransmisión única por VNI/SVI por VTEP

El problema principal con win2012 es que la opción 82 no está totalmente admitida, por lo que la subopción "Selección de enlaces" (5 o propietaria de Cisco - 150) no se puede utilizar para seleccionar el conjunto derecho en el servidor DHCP.

Para resolver este problema, se puede utilizar este enfoque:

- Se debe crear un alcance para las direcciones IP RELAY; de lo contrario, DHCP no encuentra un conjunto que coincida con DHCP GIADDR e ignore el paquete. El rango IP completo debe excluirse del DHCP para evitar la asignación del conjunto IP RELAY. Llamamos a este pool RELAY_POOL
- Se debe crear el alcance del intervalo IP que desea asignar. Llamamos a este pool IP_POOL
- Se debe crear el superscopio y se deben incluir ambos ámbitos: RELAY_POOL e IP_POOL

Veamos cómo se procesa el paquete DHCP en el servidor.

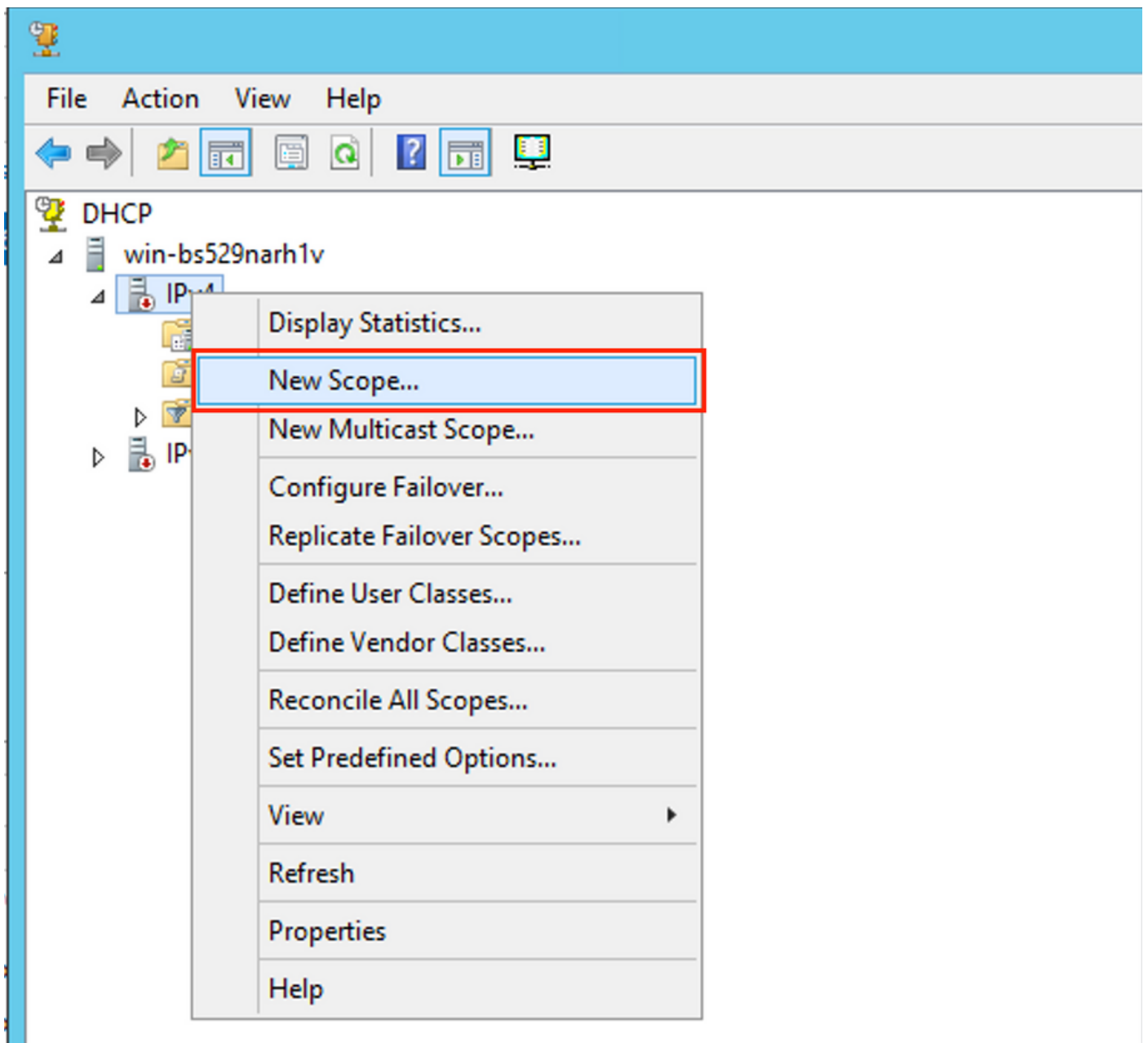
1. El servidor recibe el paquete DHCP.
2. Basado en GIADDR, el grupo correspondiente RELAY_POOL se elige en el superscopio adecuado.
3. Dado que no hay direcciones IP libres en RELAY_POOL (¿recuerda que se excluye el ámbito completo?), se repliega a IP_POOL en el mismo superscopio.
4. La dirección se asigna desde el superconjunto respectivo y se envía de vuelta a la retransmisión.

Una gran desventaja de este método es que debe tener un loopback único por VLAN/VNI por vtep ya que el conjunto DHCP se selecciona en función de la dirección Relay.

Esta opción nos lleva a la utilización de un rango IP grande para las direcciones IP de los relés.

Opción 1. Instrucciones paso a paso sobre cómo configurar win2012 r2.

Cree el alcance DHCP para las direcciones de retransmisión. Haga clic con el botón derecho del ratón y elija **Nuevo alcance** como se muestra en la imagen.



Seleccione **Next** como se muestra en la imagen.

New Scope Wizard



Welcome to the New Scope Wizard

This wizard helps you set up a scope for distributing IP addresses to computers on your network.

To continue, click Next.

< Back

Next >

Cancel

Rellene un nombre significativo, una descripción y, a continuación, seleccione **Siguiente** como se muestra en la imagen.

New Scope Wizard

Scope Name

You have to provide an identifying scope name. You also have the option of providing a description.



Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name:

Description:

< Back

Next >

Cancel

Complete la información de la dirección IP para el conjunto de retransmisión. En este ejemplo, la máscara de red es /24 pero puede ser más grande o más pequeña (depende del tamaño de la red), como se muestra en la imagen.

New Scope Wizard

IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.



Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address:

End IP address:

Configuration settings that propagate to DHCP Client

Length:

Subnet mask:

< Back

Next >

Cancel

Excluya todos los rangos de la piscina. Esto es importante, de lo contrario, las direcciones IP se pueden asignar desde este conjunto.

New Scope Wizard

Add Exclusions and Delay

Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCP OFFER message.



Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address:

End IP address:

Add

Excluded address range:

10.1.251.1 to 10.1.251.254

Remove

Subnet delay in milli second:

< Back

Next >

Cancel

Configure el tiempo de concesión (de forma predeterminada es de 8 días) como se muestra en la imagen.

New Scope Wizard

Lease Duration

The lease duration specifies how long a client can use an IP address from this scope.



Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

Days:

Hours:

Minutes:

< Back

Next >

Cancel

Puede configurar los parámetros de la opción DHCP como DNS/WINS (omitidos en este ejemplo).

New Scope Wizard

Configure DHCP Options

You have to configure the most common DHCP options before clients can use the scope.



When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

- Yes, I want to configure these options now
- No, I will configure these options later

< Back

Next >

Cancel

Active el alcance como se muestra en la imagen.

New Scope Wizard

Activate Scope

Clients can obtain address leases only if a scope is activated.



Do you want to activate this scope now?

- Yes, I want to activate this scope now
- No, I will activate this scope later

< Back

Next >

Cancel

Finalizar la configuración como se muestra en la imagen.

New Scope Wizard



Completing the New Scope Wizard

You have successfully completed the New Scope wizard.

To provide high availability for this scope, configure failover for the newly added scope by right clicking on the scope and clicking on configure failover.

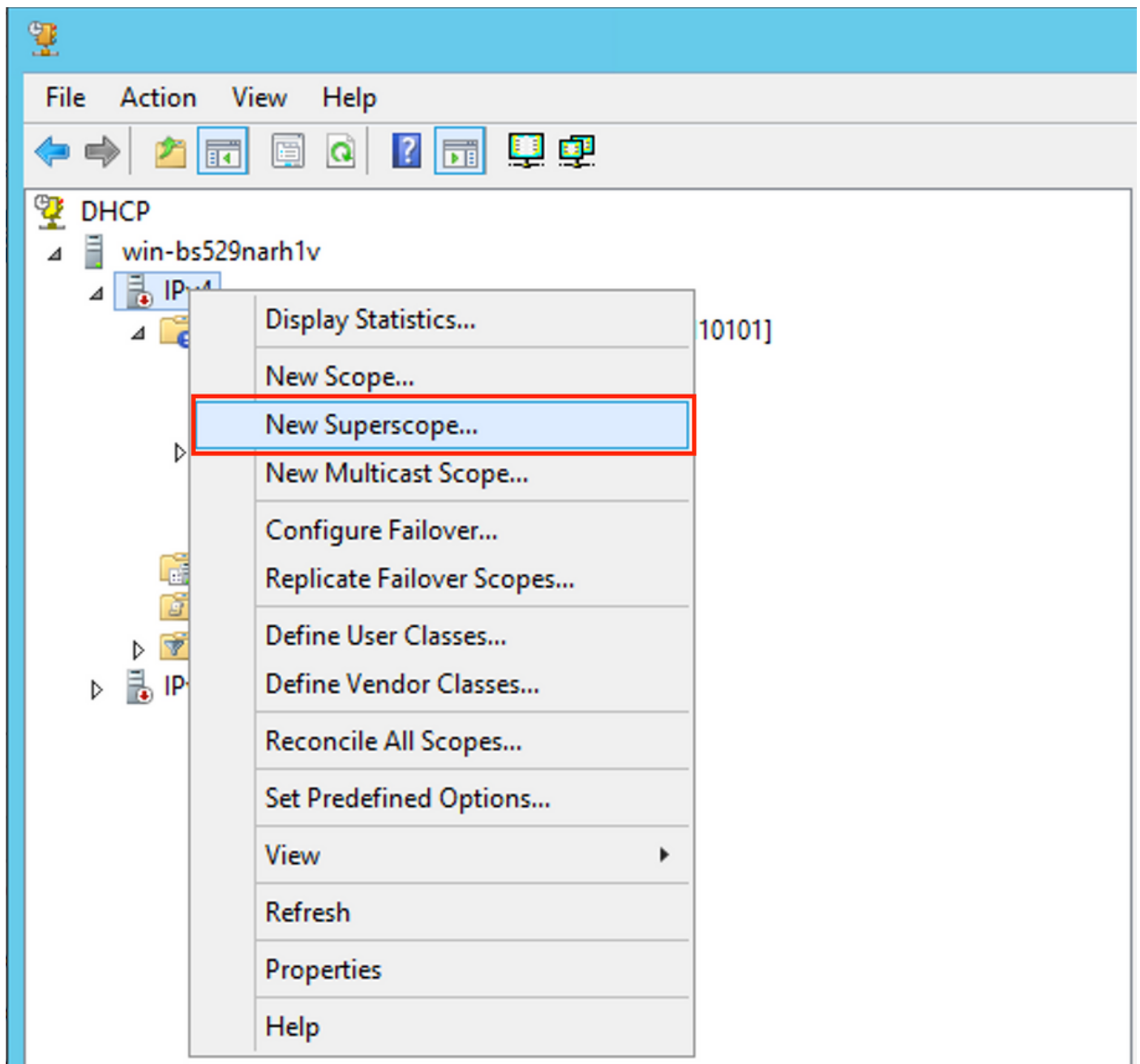
To close this wizard, click Finish.

< Back

Finish

Cancel

Ahora, cree un superscopio. Seleccione el botón derecho y elija **Nuevo superámbito** como se muestra en la imagen.



Seleccione **Next** como se muestra en la imagen.

New Superscope Wizard



Welcome to the New Superscope Wizard

This wizard helps you create a superscope, which expands the number of IP network addresses that you can use in a network.

A superscope allows several distinct scopes to be logically grouped under a single name.

To continue, click Next.

< Back

Next >

Cancel

Elija un nombre significativo para el **superámbito** como se muestra en la imagen.

New Superscope Wizard

Superscope Name

You have to provide an identifying superscope name.



Name:

< Back

Next >

Cancel

Elija el alcance que se agregará al superámbito.

New Superscope Wizard

Select Scopes

You create a superscope by building a collection of scopes.



Select one or more scopes from the list to add to the superscope.

Available scopes:

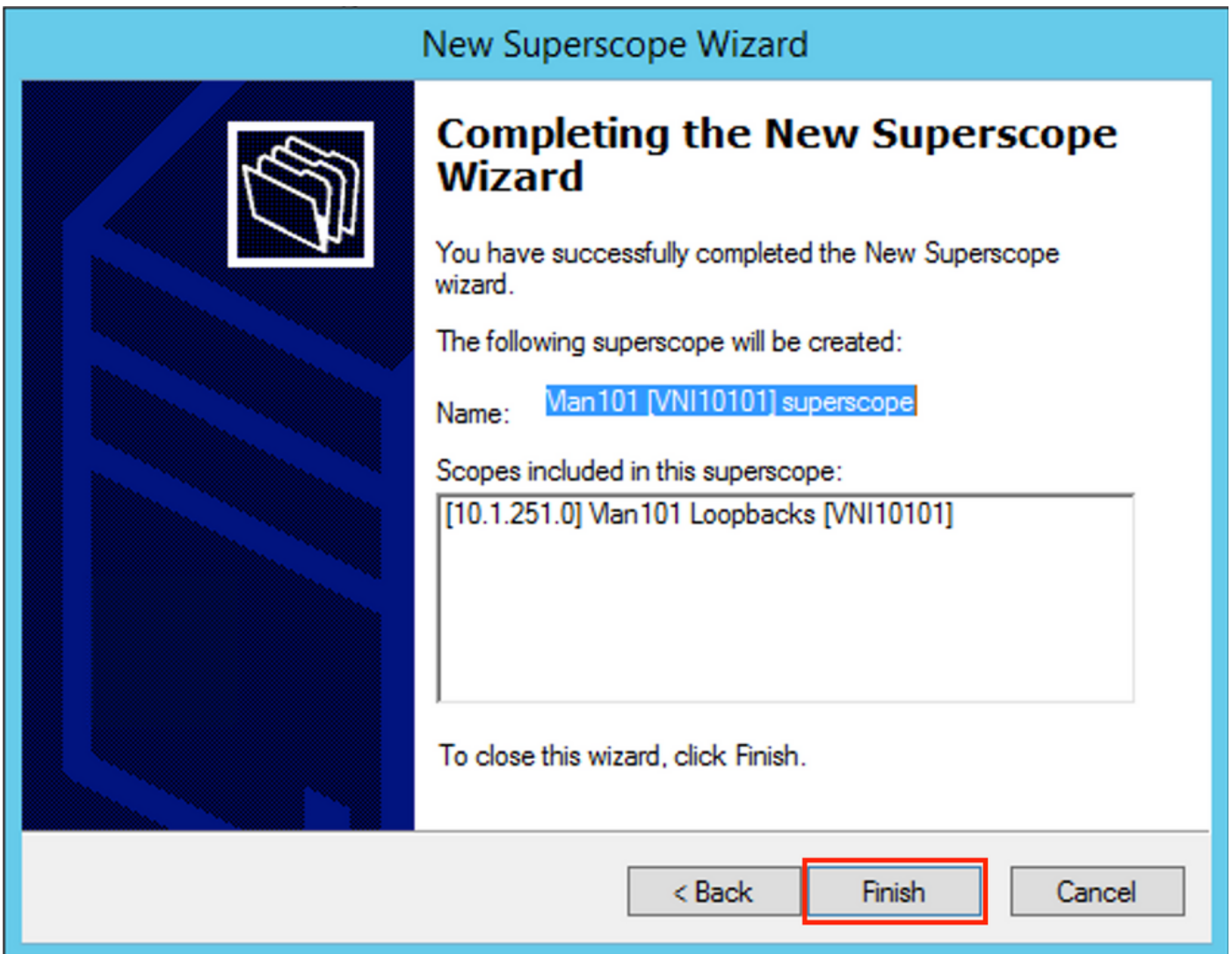
[10.1.251.0] Man101 Loopbacks [VNI10101]

< Back

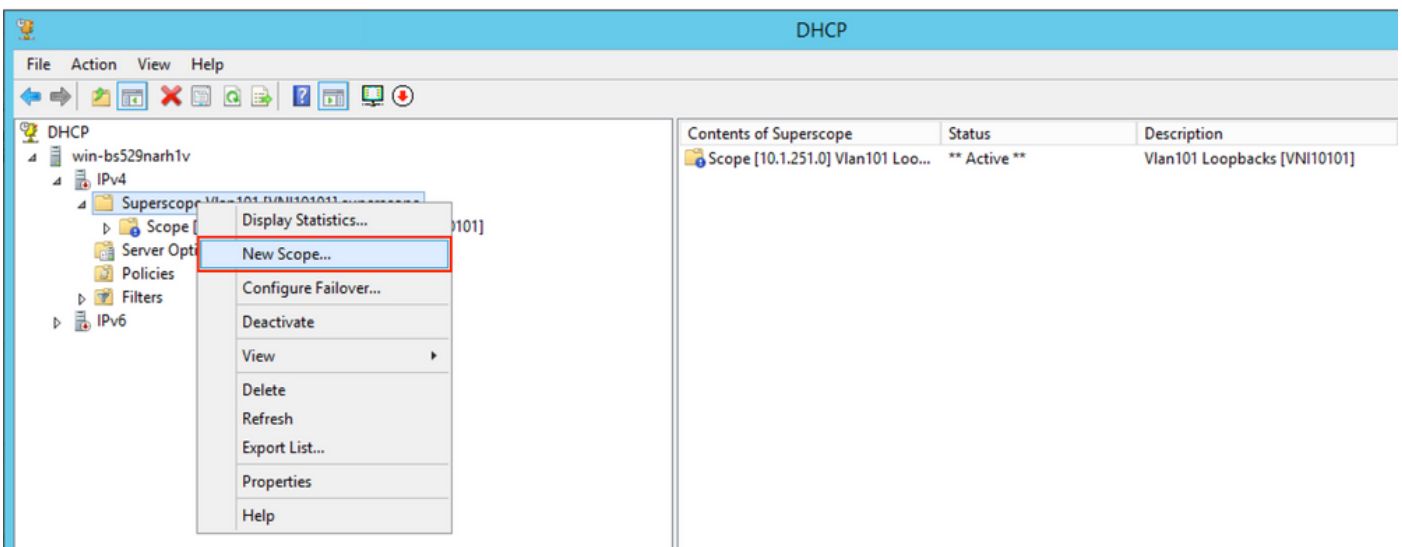
Next >

Cancel

Finalizar la configuración como se muestra en la imagen.



Cree un conjunto DHCP desde el cual se asignan las direcciones IP. Haga clic con el botón derecho y seleccione **Nuevo alcance...** como se muestra en la imagen.



Seleccione **Next** como se muestra en la imagen.

New Scope Wizard



Welcome to the New Scope Wizard

This wizard helps you set up a scope for distributing IP addresses to computers on your network.

To continue, click Next.

< Back

Next >

Cancel

Elija un nombre y una descripción significativos como se muestra en la imagen.

New Scope Wizard

Scope Name

You have to provide an identifying scope name. You also have the option of providing a description.



Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name:

Description:

< Back

Next >

Cancel

Especifique la red y la máscara para el conjunto del que desea asignar las direcciones IP a los clientes como se muestra en la imagen.

New Scope Wizard

IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.



Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address:

End IP address:

Configuration settings that propagate to DHCP Client

Length:

Subnet mask:

< Back

Next >

Cancel

Excluya la dirección IP de la puerta de enlace PREDETERMINADA del conjunto (en este ejemplo es 10.1.101.1) como se muestra en la imagen.

New Scope Wizard

Add Exclusions and Delay

Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCP OFFER message.



Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address:

End IP address:

Add

Excluded address range:

Address 10.1.101.1

Remove

< Back

Next >

Cancel

Especifique el temporizador de arrendamiento como se muestra en la imagen.

New Scope Wizard

Lease Duration

The lease duration specifies how long a client can use an IP address from this scope.



Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

Days: Hours: Minutes:

< Back

Next >

Cancel

Opcionalmente, puede especificar DNS/WINS (omitido en este ejemplo).

New Scope Wizard

Configure DHCP Options

You have to configure the most common DHCP options before clients can use the scope.



When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

- Yes, I want to configure these options now
- No, I will configure these options later

< Back

Next >

Cancel

Finalizar la configuración como se muestra en la imagen.



Después de la creación del conjunto, se debe crear una política para el conjunto.

- En la política ID del circuito del agente [1] se coincide
- Si tiene varias VLAN/VNI, debe crear superpool con subconjuntos para las direcciones IP de retransmisión y el rango de IP real para la asignación por cada VLAN/VNI
- Este ejemplo utiliza VNI 10101 y 10102

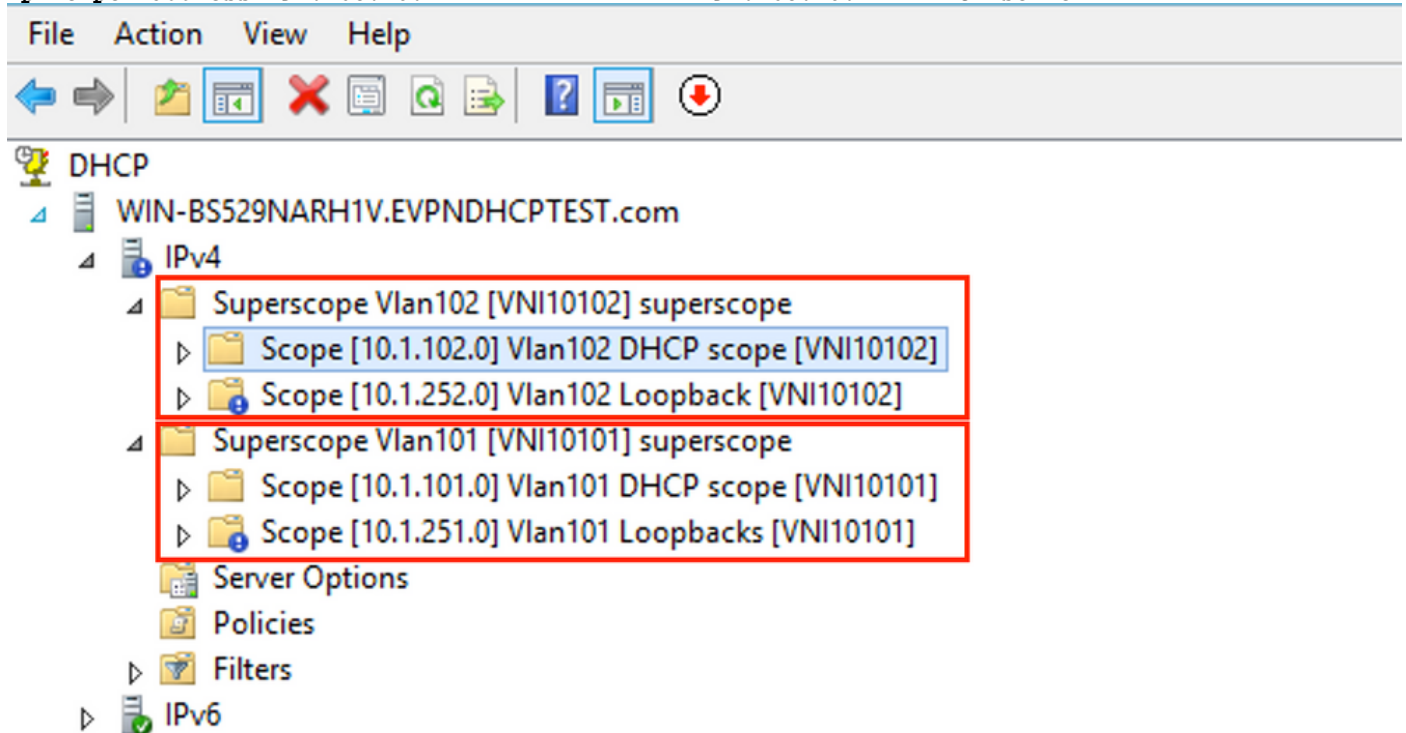
Configuración del switch:

```
ip dhcp relay information option vpn <<< add the VRF name/VPN ID to the option 82
ip dhcp relay information option <<< enables option 82
!
ip dhcp snooping vlan 101-102,201-202
ip dhcp snooping
!
vlan configuration 101
member evpn-instance 101 vni 10101
!
interface Loopback101
 vrf forwarding green
 ip address 10.1.251.1 255.255.255.255
!
interface Loopback102
 vrf forwarding green
 ip address 10.1.251.2 255.255.255.255
```

```

!
interface Vlan101
 vrf forwarding green
 ip dhcp relay source-interface Loopback101 <<< DHCP relay source is unique Loopback101
 ip address 10.1.101.1 255.255.255.0
 ip helper-address 192.168.20.12 <<< 192.168.20.12 - DHCP server
!
interface Vlan102
 vrf forwarding green
 ip dhcp relay source-interface Loopback102 <<< DHCP relay source is unique Loopback102
 ip address 10.1.101.1 255.255.255.0
 ip helper-address 192.168.20.12 <<< 192.168.20.12 - DHCP server

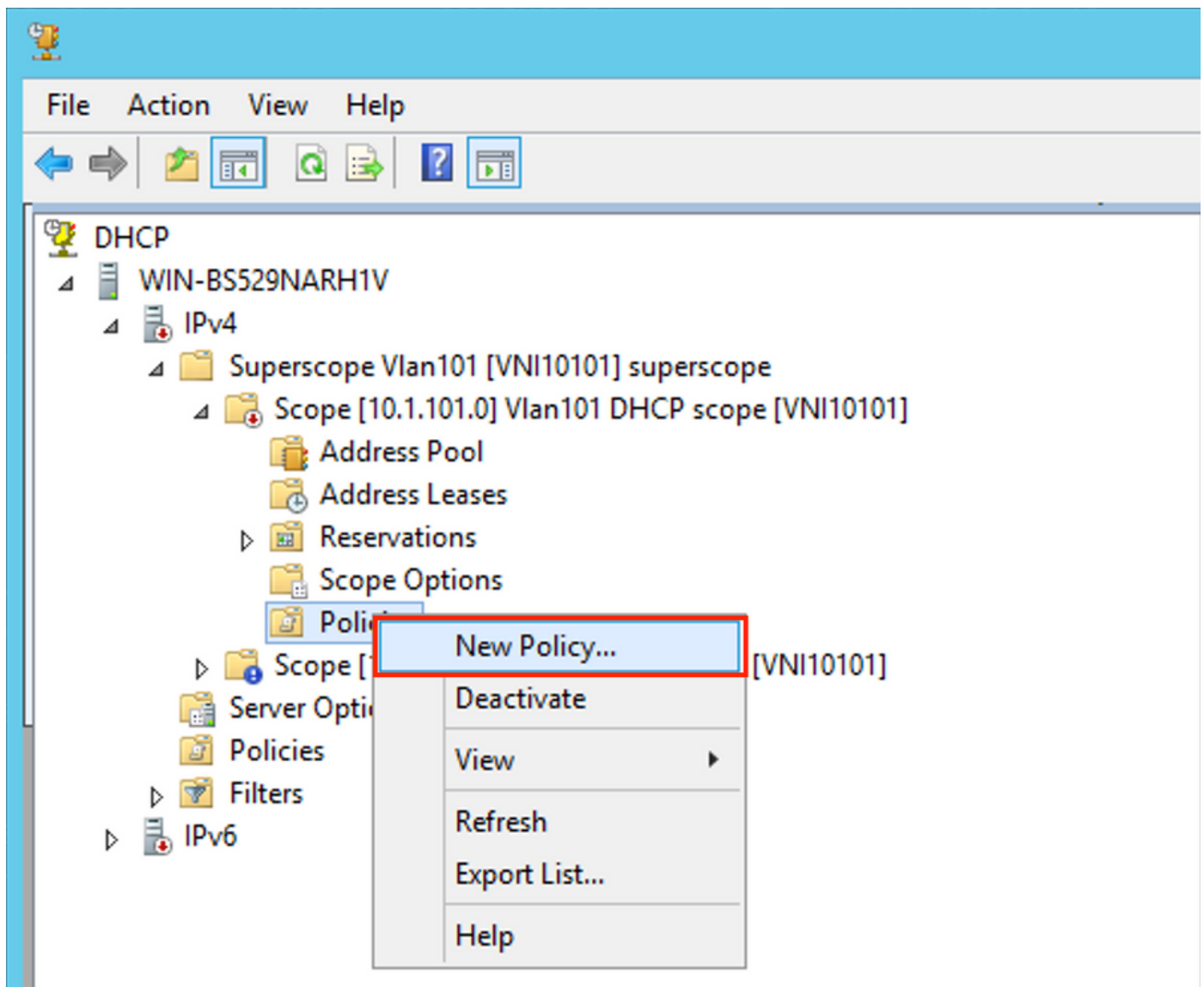
```



Opción 2 de configuración de Win2012 R2: haga coincidir el campo ID del circuito del agente

- La desventaja del último enfoque es la alta utilización de loopback único, por lo que otra opción es hacer coincidir el campo ID del circuito del agente.
- Los pasos son los mismos, pero agrega la creación de la política para la selección de alcance que no se basa en el campo ID del circuito del agente en lugar de IP de retransmisión.

Creación de políticas. Haga clic con el botón derecho en pool y seleccione **New Policy** como se muestra en la imagen.



Elija un nombre y una descripción significativos para la política como se muestra en la imagen.

DHCP Policy Configuration Wizard

Policy based IP Address and Option Assignment



This feature allows you to distribute configurable settings (IP address, DHCP options) to clients based on certain conditions (e.g. vendor class, user class, MAC address, etc.).

This wizard will guide you setting up a new policy. Provide a name (e.g. VoIP Phone Configuration Policy) and description (e.g. NTP Server option for VoIP Phones) for your policy.

Policy Name:

Description:

< Back

Next >

Cancel

Agregue la nueva condición como se muestra en la imagen.

DHCP Policy Configuration Wizard

Configure Conditions for the policy



A policy consists of one or more conditions and a set of configuration settings (options, IP Address) that are distributed to the client. The DHCP server delivers these specific settings to clients that match these conditions.

- ! A policy with conditions based on fully qualified domain name can have configuration settings for DNS but not for options or IP address ranges.

Conditions	Operator	Value
------------	----------	-------

AND

OR

Add...

Edit...

Remove

< Back

Next >

Cancel

Introduzca la ID de circuito adecuada (no olvide el cuadro **Agregar comodín (*)** como se muestra en la imagen.

DHCP Policy Configuration Wizard

Add/Edit Condition ? X

Specify a condition for the policy being configured. Select a criteria, operator and values for the condition.

Criteria:

Operator:

Value (in hex)

Relay Agent Information:

Agent Circuit ID:

Agent Remote ID:

Subscriber ID:

Prefix wildcard(*)

Append wildcard(*)

Aclaración de por qué se eligió este número:

En Wireshark, puede ver el ID de circuito del agente igual a **010a000800002775010a0000**, que es donde este valor deriva de (00002775 hex = 10100 La cifra decimal es igual a la VNI 10101 configurada para la VLAN 101).

- ▼ Option: (82) Agent Information Option
 - Length: 44
 - ▼ Option 82 Suboption: (1) Agent Circuit ID
 - Length: 12
 - Agent Circuit ID: 010a000800002775010a0000
 - ▶ Option 82 Suboption: (2) Agent Remote ID
 - ▶ Option 82 Suboption: (151) VRF name/VPN ID
 - ▼ Option 82 Suboption: (150) Link selection (Cisco proprietary)
 - Length: 4
 - Link selection (Cisco proprietary): 10.1.101.0
 - ▼ Option 82 Suboption: (152) Server ID Override (Cisco proprietary)
 - Length: 4
 - Server ID Override (Cisco proprietary): 10.1.101.1

La subopción ID del circuito del agente se codifica en este formato para VXLAN VN:


Tipo de subopción	Longitud	Tipo de ID de circuito	Longitud	VNI	mod	puerto		
01	1 byte	0 a	1 byte	00	1 byte	4 bytes	2 byte	2 byte
				08	00002775	*	*	

DHCP Policy Configuration Wizard

Configure Conditions for the policy



A policy consists of one or more conditions and a set of configuration settings (options, IP Address) that are distributed to the client. The DHCP server delivers these specific settings to clients that match these conditions.

 A policy with conditions based on fully qualified domain name can have configuration settings for DNS but not for options or IP address ranges.

Conditions	Operator	Value
Relay Agent Information - A...	Equals	010A000800002775*

AND

OR

Add...

Edit...

Remove

< Back

Next >

Cancel

Configure el rango IP desde el que se asignan las direcciones IP. Sin esta configuración no es posible asignar ninguna asignación para el **ámbito actual**.

DHCP Policy Configuration Wizard

Configure settings for the policy

If the conditions specified in the policy match a client request, the settings will be applied.



A scope can be subdivided into multiple IP address ranges. Clients that match the conditions defined in a policy will be issued an IP Address from the specified range.

Configure the start and end IP address for the range. The start and end IP addresses for the range must be within the start and end IP addresses of the scope.

The current scope IP address range is 10.1.101.1 - 10.1.101.254

If an IP address range is not configured for the policy, policy clients will be issued an IP address from the scope range.

Do you want to configure an IP address range for the policy:

Yes No

Start IP address: 10 . 1 . 101 . 1

End IP address: 10 . 1 . 101 . 254

Percentage of IP address range: 100.0

< Back

Next >

Cancel

También puede seleccionar opciones DHCP estándar en esta etapa, como se muestra en la imagen.

DHCP Policy Configuration Wizard

Configure settings for the policy

If the conditions specified in the policy match a client request, the settings will be applied.



Vendor class:

DHCP Standard Options

Available Options	Description	
<input type="checkbox"/> 002 Time Offset	UTC offset in seconds	^
<input type="checkbox"/> 003 Router	Array of router addresses order	
<input type="checkbox"/> 004 Time Server	Array of time server addresses	v

Data entry

Long:

0x0

< Back

Next >

Cancel

Seleccione **Finalizar** como se muestra en la imagen.

DHCP Policy Configuration Wizard

Summary



A new policy will be created with the following properties. To configure DNS settings, view properties of the policy and click the DNS tab.

Name: Man101 [VNI10101] Option 82

Description: Man101 [VNI10101] Option 82

Conditions: OR of

Conditions	Operator	Value
Relay Agent Information - A...	Equals	010A000800002775*

Settings:

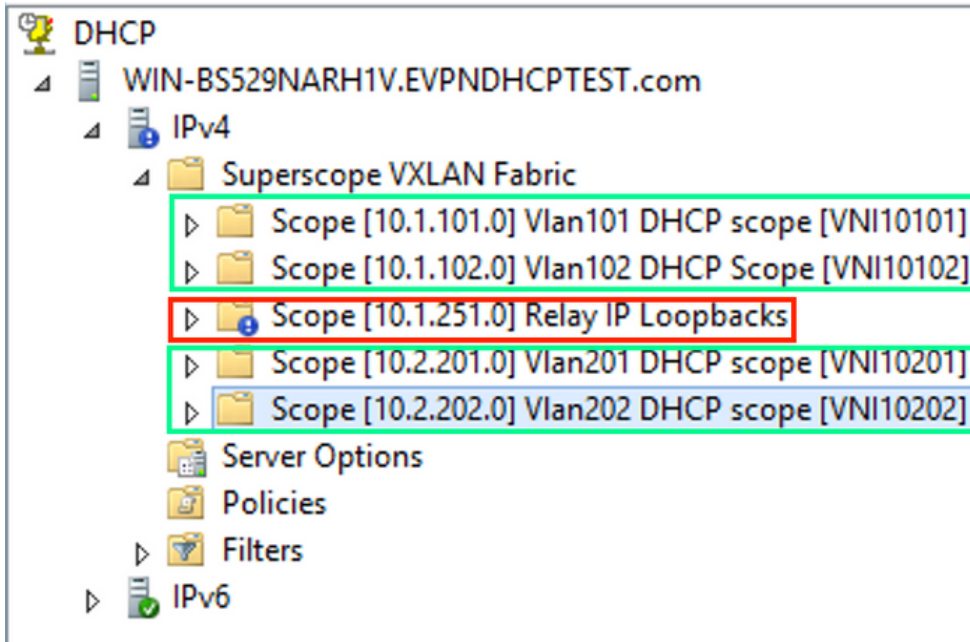
Option Name	Vendor Class	Value
-------------	--------------	-------

< Back

Finish

Cancel

Se debe realizar una configuración similar para otros rangos como se muestra en la imagen.



En esta situación, puede utilizar sólo una dirección IP única por VTEP para números de SVI, no un loopback único por VNI/SVI por VTEP.

Configuración del switch:

```

ip dhcp relay information option vpn          <<< adds the VRF name/VPN ID to the option 82
ip dhcp relay information option            <<< enables option 82
!
ip dhcp snooping vlan 101-102,201-202
ip dhcp snooping
!
vlan configuration 101
member evpn-instance 101 vni 10101
!
interface Loopback101
 vrf forwarding green
 ip address 10.1.251.1 255.255.255.255
!
interface Vlan101
 vrf forwarding green
 ip dhcp relay source-interface Loopback101 <<< DHCP relay source
 ip address 10.1.101.1 255.255.255.0
 ip helper-address 192.168.20.12          <<< 192.168.20.12 - DHCP server
!
interface Vlan102
 vrf forwarding green
 ip dhcp relay source-interface Loopback101 <<< DHCP relay source
 ip address 10.1.101.1 255.255.255.0
 ip helper-address 192.168.20.12          <<< 192.168.20.12 - DHCP server

```

Configuración de Windows Server 2016

- Windows Server 2016 admite la opción 82 subopciones 5 (Cisco propietario 150) "Selección de enlaces", lo que significa que no utiliza una dirección IP de retransmisión única para la selección de grupos. En su lugar, se utiliza la subopción "Selección de enlace", que simplifica significativamente la configuración.
- Sería mejor si todavía tuviera un conjunto para las direcciones IP de retransmisión, de lo contrario el paquete DHCP no coincide con ningún alcance y no se procesa.

Este ejemplo muestra el uso de la opción "selección de enlaces".

Inicie el conjunto de direcciones IP para las direcciones IP de retransmisión como se muestra en la imagen.

DHCP

File Action View Help



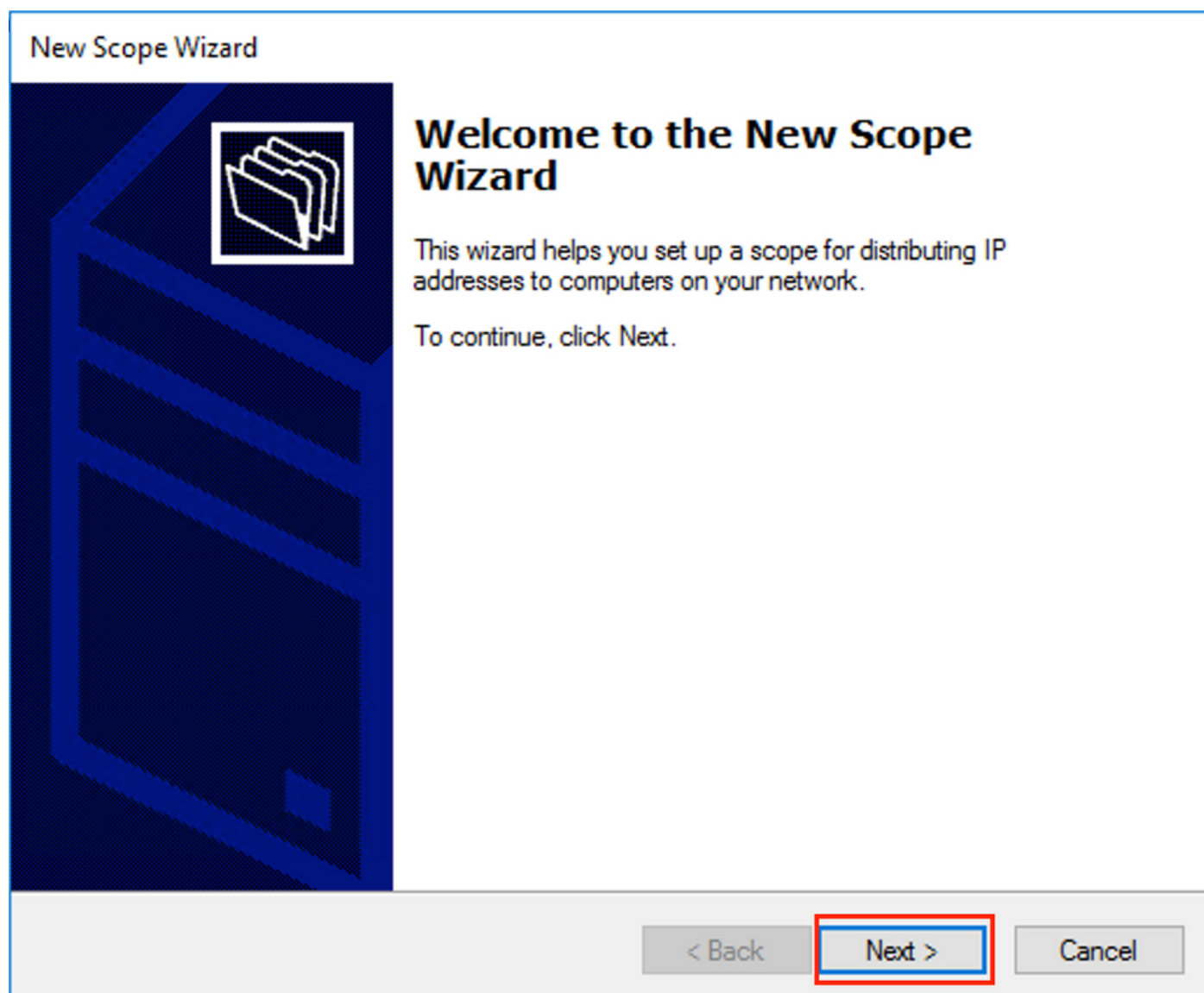
DHCP

WIN-IC90QQIUTE8.EVPNDHCPTTEST2016.com

IP v4

- Display Statistics...
- New Scope...**
- New Multicast Scope...
- Configure Failover...
- Replicate Failover Scopes...
- Define User Classes...
- Define Vendor Classes...
- Reconcile All Scopes...
- Set Predefined Options...
- View >
- Refresh
- Properties
- Help

Seleccione **Next** como se muestra en la imagen.



Elija un nombre y una descripción significativos para el ámbito como se muestra en la imagen.

New Scope Wizard

Scope Name

You have to provide an identifying scope name. You also have the option of providing a description.



Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name:

Description:

< Back

Next >

Cancel

Introduzca el espacio de dirección IP que se utiliza para los relés IP, como se muestra en la imagen.

New Scope Wizard

IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.



Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address:

End IP address:

Configuration settings that propagate to DHCP Client

Length:

Subnet mask:

< Back

Next >

Cancel

Excluir todos los intervalos del ámbito para evitar la asignación desde este rango, como se muestra en la imagen.

New Scope Wizard

Add Exclusions and Delay

Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCP OFFER message.



Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address:

End IP address:

Add

Excluded address range:

10.1.251.1 to 10.1.251.254

Remove

Subnet delay in milli second:

< Back

Next >

Cancel

También puede elegir la opción DNS/WINS, etc parámetros (omitidos en este ejemplo) como se muestra en la imagen.

New Scope Wizard

Configure DHCP Options

You have to configure the most common DHCP options before clients can use the scope.



When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

- Yes, I want to configure these options now
- No, I will configure these options later

< Back

Next >

Cancel

Seleccione **Finalizar** como se muestra en la imagen.

New Scope Wizard



Completing the New Scope Wizard

You have successfully completed the New Scope wizard.

Before clients can receive addresses you need to do the following:

1. Add any scope specific options (optional).
2. Activate the scope.

To provide high availability for this scope, configure failover for the newly added scope by right clicking on the scope and clicking on configure failover.

To close this wizard, click Finish.

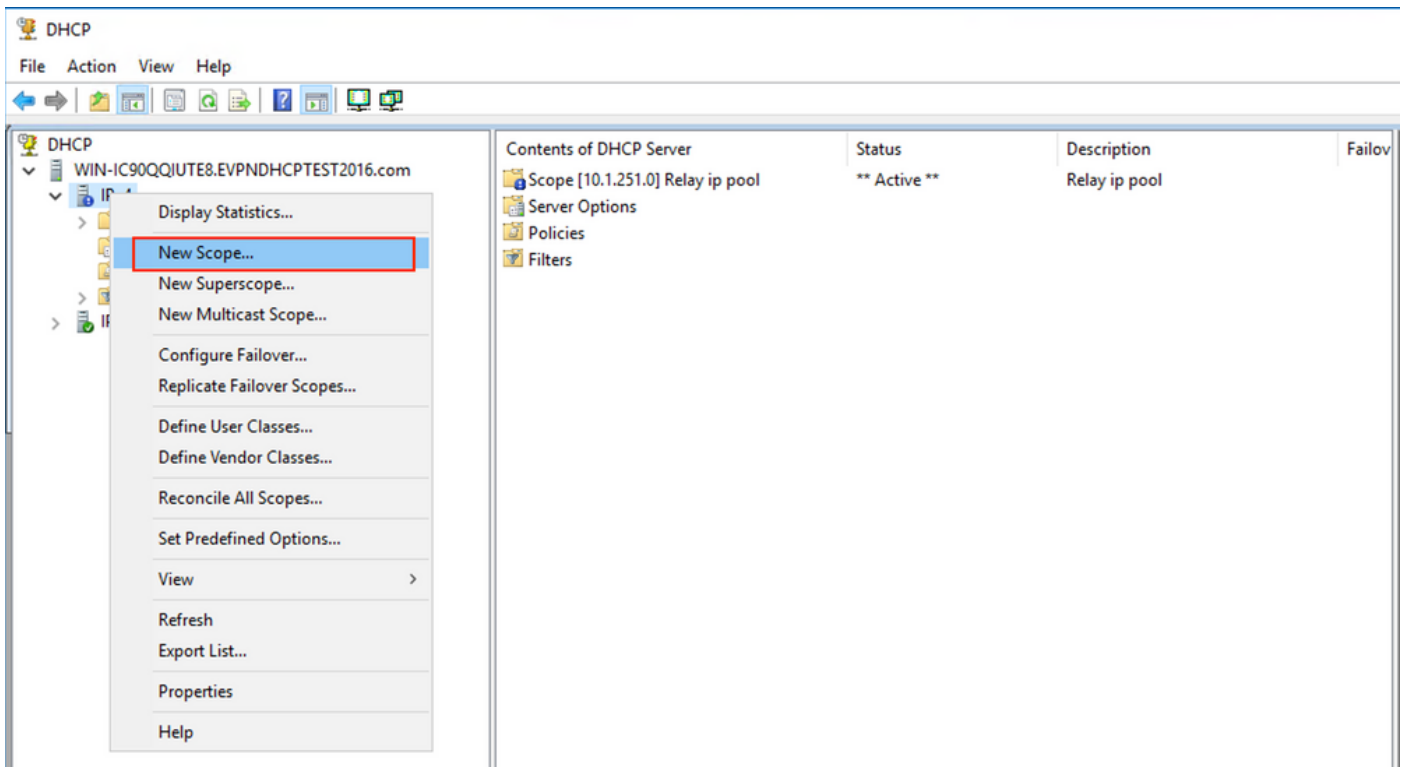
< Back

Finish

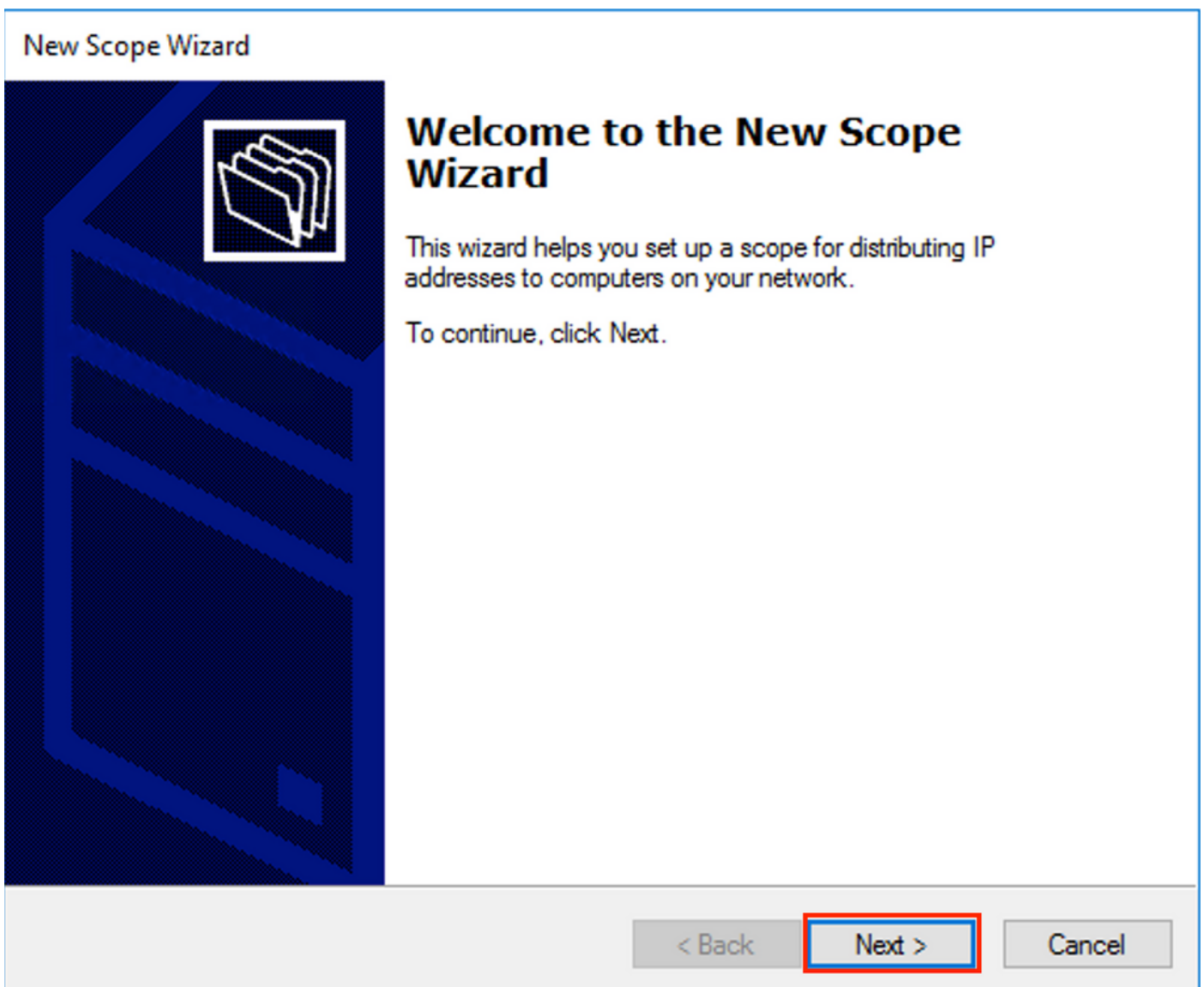
Cancel

El alcance de los relés ya está listo.

- A continuación, se crea el conjunto desde el cual los clientes obtienen direcciones IP.
- Haga clic con el botón derecho del ratón y elija **Nuevo alcance** como se muestra en la imagen.



Seleccione **Next** como se muestra en la imagen.



Elija un nombre y una descripción significativos para el conjunto como se muestra en la imagen.

New Scope Wizard

Scope Name

You have to provide an identifying scope name. You also have the option of providing a description.



Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name:

Description:

Introduzca el espacio de dirección IP para la asignación en vlan101, como se muestra en la imagen.

New Scope Wizard

IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.



Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address:

End IP address:

Configuration settings that propagate to DHCP Client

Length:

Subnet mask:

< Back

Next >

Cancel

Excluya la IP de gateway predeterminada del ámbito como se muestra en la imagen.

New Scope Wizard

Add Exclusions and Delay

Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCP OFFER message.



Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.

Start IP address:

End IP address:

Add

Excluded address range:

Address 10.1.101.1

Remove

Subnet delay in milli second:

< Back

Next >

Cancel

Establezca un tiempo de concesión como se muestra en la imagen.

New Scope Wizard

Lease Duration

The lease duration specifies how long a client can use an IP address from this scope.



Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

Set the duration for scope leases when distributed by this server.

Limited to:

Days:

Hours:

Minutes:

< Back

Next >

Cancel

Se pueden configurar parámetros adicionales como DNS/WINS y más (se omite en este ejemplo), como se muestra en la imagen.

New Scope Wizard

Configure DHCP Options

You have to configure the most common DHCP options before clients can use the scope.



When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

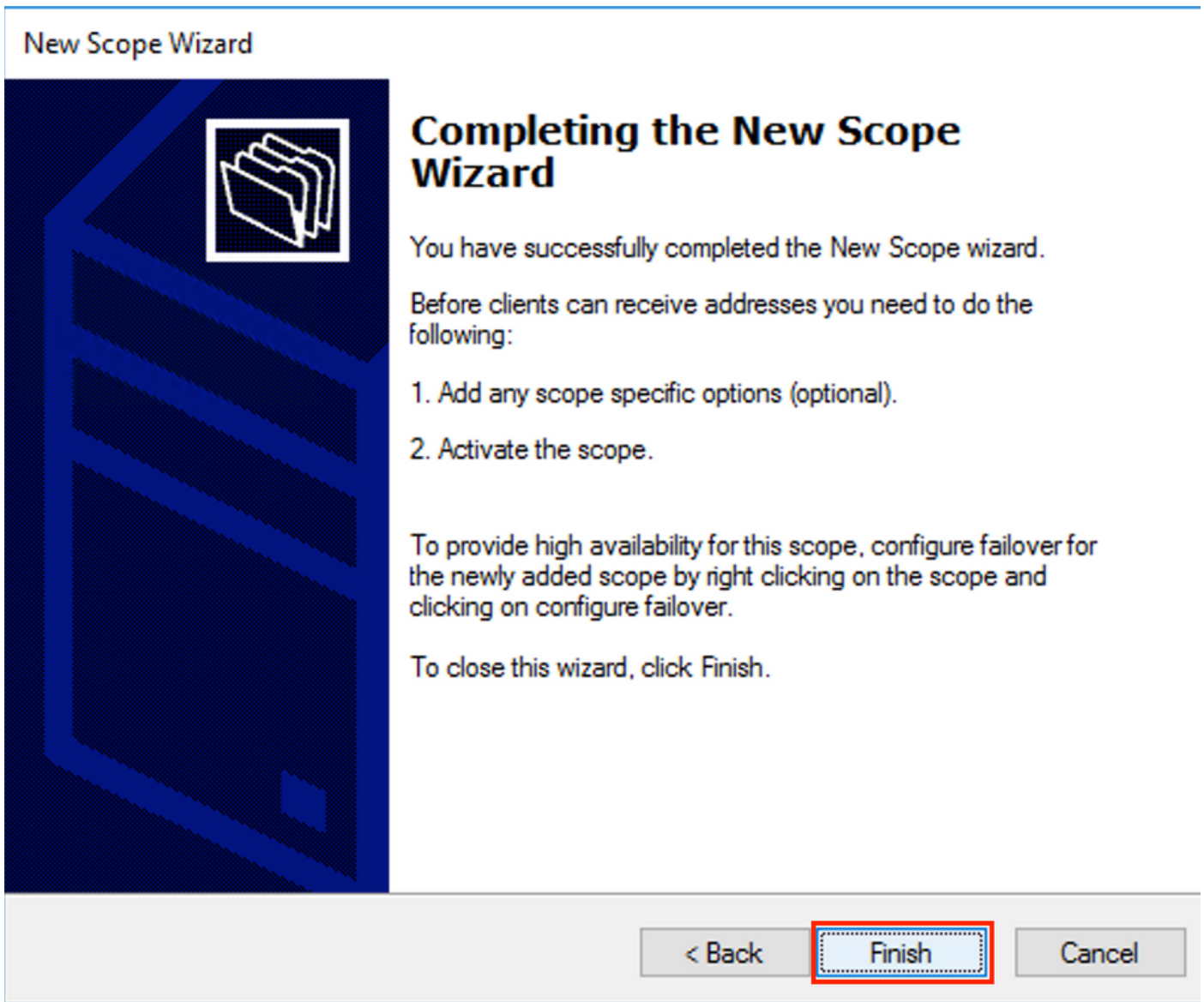
- Yes, I want to configure these options now
- No, I will configure these options later

< Back

Next >

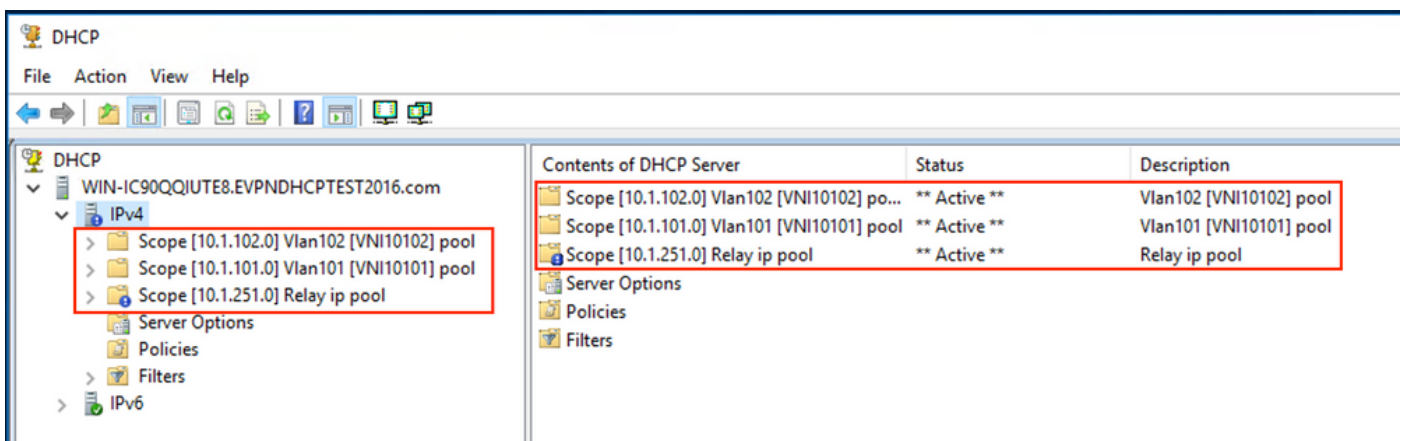
Cancel

Seleccione **Finish** para completar la configuración como se muestra en la imagen.



El conjunto por dirección IP de relay no está configurado y no coincide en HEX. La selección del conjunto se basa en la **selección** de subopción **Link**.

Se puede agregar un nuevo conjunto y no se necesita ninguna configuración adicional como se muestra en la imagen.



Servidor DHCP de Linux

Revise la configuración para isc-dhcp-server en Linux.

- Admite la opción Relay 82. Aquí, el más importante es la subopción de selección de enlaces. Todavía puede trabajar con la información de ID del circuito del agente y la máscara hexadecimal/coincidencia para el campo específico (como se hizo para el win2012). Desde una perspectiva práctica, es mucho más fácil utilizar 82[5] que trabajar directamente con la información de ID del circuito de agentes.
- La configuración de la subopción de selección de link se realiza bajo la definición de subred.

En este ejemplo, el servidor ISC se utiliza en Ubuntu Linux.

Instale el servidor DHCP:

```
apt-get install isc-dhcp-server
```

Para configurar el servidor DHCP edite `/etc/dhcp/dhcpd.conf`. (El editor Vim se utiliza en un ejemplo)

```
vim /etc/dhcp/dhcpd.conf
```

Fragmento de configuración (se omiten las configuraciones generales):

```
subnet 10.1.101.0 netmask 255.255.255.0 {
    option agent.link-selection 10.1.101.0; <<< suboption 82[5] definition

    option routers 10.1.101.1;
    option subnet-mask 255.255.255.0;

    range 10.1.101.16 10.1.101.254;
}

subnet 10.1.102.0 netmask 255.255.255.0 {
    option agent.link-selection 10.1.102.0; <<< suboption 82[5] definition

    option routers 10.1.102.1;
    option subnet-mask 255.255.255.0;

    range 10.1.102.16 10.1.102.254;
}

subnet 10.2.201.0 netmask 255.255.255.0 {
    option agent.link-selection 10.2.201.0; <<< suboption 82[5] definition

    option routers 10.2.201.1;
    option subnet-mask 255.255.255.0;

    range 10.2.201.16 10.2.201.254;
}

subnet 10.2.202.0 netmask 255.255.255.0 {
    option agent.link-selection 10.2.202.0; <<< suboption 82[5] definition

    option routers 10.2.202.1;
    option subnet-mask 255.255.255.0;

    range 10.2.202.16 10.2.202.254;
}
```

Configuración del switch

Los escenarios que se admiten en general se revisan aquí.

1. El cliente DHCP se encuentra en el VRF de arrendatario y el servidor DHCP se encuentra en el VRF predeterminado de Capa 3
2. El cliente DHCP está en el VRF de arrendatario y el servidor DHCP está en el mismo VRF de arrendatario
3. El cliente DHCP está en el VRF de arrendatario y el servidor DHCP está en un VRF de arrendatario diferente
4. El cliente DHCP está en el VRF arrendatario y el servidor DHCP está en un VRF no VXLAN no predeterminado

Para cualquiera de estos escenarios se necesita la configuración de relé DHCP en el lado del switch.

La configuración DHCP para la opción más simple número 2.

```
ip dhcp relay information option <<< Enables insertion of option 82 into the packet
ip dhcp relay information option vpn <<< Enables insertion of vpn name/id to the packet - option
82[151]
```

De forma predeterminada, las subopciones de la opción 82 **Selección de enlaces** y **Anulación de ID de servidor** son propiedad de Cisco de forma predeterminada (150 y 152, respectivamente).

- ▼ Option: (82) Agent Information Option
 - Length: 44
 - ▶ Option 82 Suboption: (1) Agent Circuit ID
 - ▶ Option 82 Suboption: (2) Agent Remote ID
 - ▶ Option 82 Suboption: (151) VRF name/VPN ID
 - ▶ Option 82 Suboption: (150) Link selection (Cisco proprietary)
 - ▶ Option 82 Suboption: (152) Server ID Override (Cisco proprietary)

Si por alguna razón el servidor DHCP no **comprende** las opciones propietarias de Cisco, puede cambiarlo por el estándar.

```
ip dhcp compatibility suboption link-selection standard <<< "Link Selection" suboption
ip dhcp compatibility suboption server-override standard <<< "Server ID Override" suboption
```

- ▼ Option: (82) Agent Information Option
 - Length: 44
 - ▶ Option 82 Suboption: (1) Agent Circuit ID
 - ▶ Option 82 Suboption: (2) Agent Remote ID
 - ▶ Option 82 Suboption: (151) VRF name/VPN ID
 - ▶ Option 82 Suboption: (5) Link selection
 - ▶ Option 82 Suboption: (11) Server ID Override

El snooping DHCP debe estar habilitado para las VLAN necesarias.

```
ip dhcp snooping vlan 101-102,201-202
ip dhcp snooping
```

Puede utilizar la configuración global de la interfaz de origen DHCP-relay.

```
ip dhcp-relay source-interface Loopback101
```

O puede configurarlo por interfaz (la configuración de la interfaz invalida la global).

```
interface Vlan101
vrf forwarding green
ip dhcp relay source-interface Loopback101 <<< DHCP source-interface
ip address 10.1.101.1 255.255.255.0
ip helper-address 192.168.20.20
```

Verifique que haya conectividad IP por dirección IP de relé y servidor DHCP en ambas direcciones.

```
Leaf-01#ping vrf green 192.168.20.20 source lo101
```

Type escape sequence to abort.

Sending 5, 100-byte ICMP Echos to 192.168.20.20, timeout is 2 seconds:

Packet sent with a source address of 10.1.251.1

!!!!

Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/1 ms

En la configuración de la interfaz, se configura la dirección del servidor DHCP. Puede ser 3 opciones para este comando. El cliente y el servidor están en el mismo VRF:

```
interface Vlan101
vrf forwarding green
ip dhcp relay source-interface Loopback101
ip address 10.1.101.1 255.255.255.0
ip helper-address 192.168.20.20 <<< DHCP server ip address
```

El cliente y el servidor se encuentran en los diferentes VRF (cliente en verde, servidor en rojo en este ejemplo):

```
interface Vlan101
vrf forwarding green
ip dhcp relay source-interface Loopback101
ip address 10.1.101.1 255.255.255.0
ip helper-address vrf red 192.168.20.20 <<< DHCP server is reachable over vrf RED
end
```

Cliente en un VRF y servidor en la tabla de routing global (GRT):

```
interface Vlan101
vrf forwarding green
ip dhcp relay source-interface Loopback101
ip address 10.1.101.1 255.255.255.0
ip helper-address global 192.168.20.20 <<< DHCP server is reachable over global routing table
end
```

Aquí se revisa una configuración típica de todas las opciones.

El cliente DHCP se encuentra en el VRF del arrendatario y el servidor DHCP se encuentra en el VRF predeterminado de la Capa 3

En este caso, Lo0 en GRT es una fuente de relé. El relé DHCP se configura globalmente + para algunas interfaces.

Por ejemplo, para el comando vlan101 "IP DHCP relay source-interface Loopback0" se pierde, pero utiliza la configuración global.

```
ip dhcp-relay source-interface Loopback0          <<< DHCP relay source interface is Lo0
ip dhcp relay information option vpn              <<< adds the vpn suboption to option 82
ip dhcp relay information option                 <<< enables DHCP option 82
ip dhcp compatibility suboption link-selection standard <<< switch to standard option 82[5]
ip dhcp compatibility suboption server-override standard <<< switch to standard option 82[11]
ip dhcp snooping vlan 101-102,201-202           <<< enables dhcp snooping for vlans
ip dhcp snooping                                <<< enables dhcp snooping globally
!
interface Loopback0
 ip address 172.16.255.3 255.255.255.255
 ip ospf 1 area 0
!
interface Vlan101
 vrf forwarding green
 ip address 10.1.101.1 255.255.255.0
 ip helper-address global 192.168.20.20          <<< DHCP is reachable over GRT
!
interface Vlan102
 vrf forwarding green
 ip dhcp relay source-interface Loopback0
 ip address 10.1.102.1 255.255.255.0
 ip helper-address global 192.168.20.20          <<< DHCP is reachable over GRT
!
interface Vlan201
 vrf forwarding red
 ip dhcp relay source-interface Loopback0
 ip address 10.2.201.1 255.255.255.0
 ip helper-address global 192.168.20.20          <<< DHCP is reachable over GRT
```

Como resultado, el paquete de relé DHCP se envía sobre GRT con la misma IP de SRC/DST, pero con diferentes subopciones.

Para vlan101:

The screenshot displays a network traffic capture in a tool named 'bootp'. The main window shows a table of captured packets with columns for No., delta, ip.id, Time, Source, and Destination. Packet 2 is highlighted, showing a source IP of 192.168.20.20 and a destination IP of 172.16.255.3.

Below the table, the details of the selected packet are shown. The packet is identified as an Internet Protocol Version 4 (IPV4) packet with source 172.16.255.3 and destination 192.168.20.20. It is a User Datagram Protocol (UDP) packet with source port 67 and destination port 67. The protocol is identified as Bootstrap Protocol (Discover).

The DHCP Discover message details are as follows:

- Message type: Boot Request (1)
- Hardware type: Ethernet (0x01)
- Hardware address length: 6
- Hops: 1
- Transaction ID: 0x000007f3
- Seconds elapsed: 0
- Bootp flags: 0x8000, Broadcast flag (Broadcast)
- Client IP address: 0.0.0.0
- Your (client) IP address: 0.0.0.0
- Next server IP address: 0.0.0.0
- Relay agent IP address: 172.16.255.3
- Client MAC address: Cisco_43:34:c1 (f4:cf:e2:43:34:c1)
- Client hardware address padding: 00000000000000000000
- Server host name not given
- Boot file name not given
- Magic cookie: DHCP

The DHCP Discover message options are listed below:

- Option: (53) DHCP Message Type (Discover)
 - Length: 1
- DHCP: Discover (1)
 - Option: (57) Maximum DHCP Message Size
 - Option: (61) Client identifier
 - Option: (12) Host Name
 - Option: (55) Parameter Request List
 - Option: (60) Vendor class identifier
 - Option: (82) Agent Information Option
 - Length: 44
 - Option 82 Suboption: (1) Agent Circuit ID
 - Option 82 Suboption: (2) Agent Remote ID
 - Option 82 Suboption: (151) VRF name/VPN ID
 - Option 82 Suboption: (5) Link selection
 - Length: 4
 - Link selection: 10.1.101.0
 - Option 82 Suboption: (11) Server ID Override
 - Option: (255) End

- Para Vlan102:

```

▶ Frame 8: 396 bytes on wire (3168 bits), 396 bytes captured (3168 bits)
▶ Ethernet II, Src: a0:b4:39:21:92:3f (a0:b4:39:21:92:3f), Dst: Vmware_a8:b8:b4 (00:50:56:a8:b8:b4)
▶ Internet Protocol Version 4, Src: 172.16.255.3, Dst: 192.168.20.20
▶ User Datagram Protocol, Src Port: 67, Dst Port: 67
▼ Bootstrap Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 1
  Transaction ID: 0x000007f4
  Seconds elapsed: 0
▶ Bootp flags: 0x8000, Broadcast flag (Broadcast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 0.0.0.0
  Next server IP address: 0.0.0.0
  Relay agent IP address: 172.16.255.3
  Client MAC address: Cisco_43:34:c3 (f4:cf:e2:43:34:c3)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
▶ Option: (53) DHCP Message Type (Discover)
▶ Option: (57) Maximum DHCP Message Size
▶ Option: (61) Client identifier
▶ Option: (12) Host Name
▶ Option: (55) Parameter Request List
▼ Option: (60) Vendor class identifier
  Length: 8
  Vendor class identifier: ciscopnp
▼ Option: (82) Agent Information Option
  Length: 44
  ▶ Option 82 Suboption: (1) Agent Circuit ID
  ▶ Option 82 Suboption: (2) Agent Remote ID
  ▶ Option 82 Suboption: (151) VRF name/VPN ID
  ▼ Option 82 Suboption: (5) Link selection
    Length: 4
    Link selection: 10.1.102.0
  ▶ Option 82 Suboption: (11) Server ID Override
▼ Option: (255) End
  Option End: 255

```

Para Vlan201 (que está en rojo vrf, no en verde como VLAN 101 y 102):

```

▶ Frame 19: 394 bytes on wire (3152 bits), 394 bytes captured (3152 bits)
▶ Ethernet II, Src: a0:b4:39:21:92:3f (a0:b4:39:21:92:3f), Dst: Vmware_a8:b8:b4 (00:50:56:a8:b8:b4)
▶ Internet Protocol Version 4, Src: 172.16.255.3, Dst: 192.168.20.20
▶ User Datagram Protocol, Src Port: 67, Dst Port: 67
▼ Bootstrap Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 1
  Transaction ID: 0x0000ccb
  Seconds elapsed: 0
  ▶ Bootp flags: 0x8000, Broadcast flag (Broadcast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 0.0.0.0
  Next server IP address: 0.0.0.0
  Relay agent IP address: 172.16.255.3
  Client MAC address: Cisco_43:34:c4 (f4:cf:e2:43:34:c4)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  ▶ Option: (53) DHCP Message Type (Discover)
  ▶ Option: (57) Maximum DHCP Message Size
  ▶ Option: (61) Client identifier
  ▶ Option: (12) Host Name
  ▶ Option: (55) Parameter Request List
  ▶ Option: (60) Vendor class identifier
  ▼ Option: (82) Agent Information Option
    Length: 42
    ▶ Option 82 Suboption: (1) Agent Circuit ID
    ▶ Option 82 Suboption: (2) Agent Remote ID
    ▶ Option 82 Suboption: (151) VRF name/VPN ID
    ▼ Option 82 Suboption: (5) Link selection
      Length: 4
      Link selection: 10.2.201.0
    ▶ Option 82 Suboption: (11) Server ID Override
  ▶ Option: (255) End

```

La captura de paquetes se realizó en Spine-01 desde la interfaz hasta la hoja 01:

```
Spine-01#sh mon cap TAC buff br | i DHCP
```

```

5401 4.402431 172.16.255.3 b^F^R 192.168.20.20 DHCP 396 DHCP Discover - Transaction ID 0x1feb
5403 4.403134 192.168.20.20 b^F^R 172.16.255.3 DHCP 362 DHCP Offer - Transaction ID 0x1feb
5416 4.418117 172.16.255.3 b^F^R 192.168.20.20 DHCP 414 DHCP Request - Transaction ID 0x1feb
5418 4.418608 192.168.20.20 b^F^R 172.16.255.3 DHCP 362 DHCP ACK - Transaction ID 0x1feb

```

El paquete DHCP en el núcleo es IP sin encapsulación VXLAN:

```
Spine-01#sh mon cap TAC buff det | b Frame 5401:
```

```

Frame 5401: 396 bytes on wire (3168 bits), 396 bytes captured (3168 bits) on interface 0
<...skip...>
[Protocols in frame: eth:ethertype:ip:udp:dhcp]
Ethernet II, Src: 10:b3:d5:6a:8f:e4 (10:b3:d5:6a:8f:e4), Dst: 7c:21:0d:92:b2:e4
(7c:21:0d:92:b2:e4)
<...skip...>
Internet Protocol Version 4, Src: 172.16.255.3, Dst: 192.168.20.20
<...skip...>
User Datagram Protocol, Src Port: 67, Dst Port: 67
<...skip...>
Dynamic Host Configuration Protocol (Discover)
<...skip...>

```

Una gran ventaja de este enfoque es que puede utilizar la misma dirección IP de retransmisión para diferentes VRF de arrendatarios sin que se produzcan fugas de ruta entre diferentes VRF y globales.

El cliente DHCP y el servidor DHCP se encuentran en el mismo VRF de arrendatario

En este caso, tiene sentido tener la dirección IP de retransmisión en el VRF del arrendatario.

Configuración del switch:

```
ip dhcp relay information option vpn <<< adds the vpn suboption to option 82
ip dhcp relay information option <<< enables DHCP option 82
ip dhcp compatibility suboption link-selection standard <<< switch to standard option 82[5]
ip dhcp compatibility suboption server-override standard <<< switch to standard option 82[11]
ip dhcp snooping vlan 101-102,201-202 <<< enables dhcp snooping for vlans
ip dhcp snooping <<< enables dhcp snooping globally
!
interface Loopback101
vrf forwarding green
ip address 10.1.251.1 255.255.255.255
!
interface Vlan101
vrf forwarding green
ip dhcp relay source-interface Loopback101
ip address 10.1.101.1 255.255.255.0
ip helper-address 192.168.20.20 <<< DHCP is reachable over vrf green
!
interface Vlan102
vrf forwarding green
ip dhcp relay source-interface Loopback101
ip address 10.1.102.1 255.255.255.0
ip helper-address 192.168.20.20 <<< DHCP is reachable over vrf green
```

Para vlan101:

```

▶ Frame 1: 396 bytes on wire (3168 bits), 396 bytes captured (3168 bits)
▶ Ethernet II, Src: a0:b4:39:21:92:3f (a0:b4:39:21:92:3f), Dst: Vmware_a8:b8:b4 (00:50:56:a8:b8:b4)
▶ Internet Protocol Version 4, Src: 10.1.251.1, Dst: 192.168.20.20
▶ User Datagram Protocol, Src Port: 67, Dst Port: 67
▼ Bootstrap Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 1
  Transaction ID: 0x000016cc
  Seconds elapsed: 0
▶ Bootp flags: 0x8000, Broadcast flag (Broadcast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 0.0.0.0
  Next server IP address: 0.0.0.0
  Relay agent IP address: 10.1.251.1
  Client MAC address: Cisco_43:34:c1 (f4:cf:e2:43:34:c1)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
▶ Option: (53) DHCP Message Type (Discover)
▶ Option: (57) Maximum DHCP Message Size
▶ Option: (61) Client identifier
▶ Option: (12) Host Name
▶ Option: (55) Parameter Request List
▶ Option: (60) Vendor class identifier
▼ Option: (82) Agent Information Option
  Length: 44
  ▶ Option 82 Suboption: (1) Agent Circuit ID
  ▶ Option 82 Suboption: (2) Agent Remote ID
  ▶ Option 82 Suboption: (151) VRF name/VPN ID
  ▼ Option 82 Suboption: (5) Link selection
    Length: 4
    Link selection: 10.1.101.0
  ▶ Option 82 Suboption: (11) Server ID Override
▶ Option: (255) End

```

Para vlan102:

```

▶ Frame 5: 396 bytes on wire (3168 bits), 396 bytes captured (3168 bits)
▶ Ethernet II, Src: a0:b4:39:21:92:3f (a0:b4:39:21:92:3f), Dst: Vmware_a8:b8:b4 (00:50:56:a8:b8:b4)
▶ Internet Protocol Version 4, Src: 10.1.251.1, Dst: 192.168.20.20
▶ User Datagram Protocol, Src Port: 67, Dst Port: 67
▼ Bootstrap Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 1
  Transaction ID: 0x000016cd
  Seconds elapsed: 0
  ▶ Bootp flags: 0x8000, Broadcast flag (Broadcast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 0.0.0.0
  Next server IP address: 0.0.0.0
  Relay agent IP address: 10.1.251.1
  Client MAC address: Cisco_43:34:c3 (f4:cf:e2:43:34:c3)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  ▶ Option: (53) DHCP Message Type (Discover)
  ▶ Option: (57) Maximum DHCP Message Size
  ▶ Option: (61) Client identifier
  ▶ Option: (12) Host Name
  ▶ Option: (55) Parameter Request List
  ▼ Option: (60) Vendor class identifier
    Length: 8
    Vendor class identifier: ciscopnp
  ▼ Option: (82) Agent Information Option
    Length: 44
    ▶ Option 82 Suboption: (1) Agent Circuit ID
    ▶ Option 82 Suboption: (2) Agent Remote ID
    ▶ Option 82 Suboption: (151) VRF name/VPN ID
    ▼ Option 82 Suboption: (5) Link selection
      Length: 4
      Link selection: 10.1.102.0
    ▶ Option 82 Suboption: (11) Server ID Override
  ▼ Option: (255) End
    Option End: 255

```

Captura de paquetes de la interfaz Spine-01 a Leaf-01:

```

Spine-01#sh monitor capture TAC buffer brief | i DHCP
2 4.287466 10.1.251.1 b^F^R 192.168.20.20 DHCP 446 DHCP Discover - Transaction ID 0x1894
3 4.288258 192.168.20.20 b^F^R 10.1.251.1 DHCP 412 DHCP Offer - Transaction ID 0x1894
4 4.307550 10.1.251.1 b^F^R 192.168.20.20 DHCP 464 DHCP Request - Transaction ID 0x1894
5 4.308385 192.168.20.20 b^F^R 10.1.251.1 DHCP 412 DHCP ACK - Transaction ID 0x1894

```

El paquete DHCP en el núcleo tiene encapsulación VXLAN:

```

Frame 2: 446 bytes on wire (3568 bits), 446 bytes captured (3568 bits) on interface 0
<...skip...>
[Protocols in frame: eth:ethertype:ip:udp:vxlan:eth:ethertype:ip:udp:dhcp]
Ethernet II, Src: 10:b3:d5:6a:8f:e4 (10:b3:d5:6a:8f:e4), Dst: 7c:21:0d:92:b2:e4
(7c:21:0d:92:b2:e4)
<...skip...>
Internet Protocol Version 4, Src: 172.16.254.3, Dst: 172.16.254.5 <<< VTEP IP addresses
<...skip...>
User Datagram Protocol, Src Port: 65283, Dst Port: 4789
<...skip...>

```

```

Virtual eXtensible Local Area Network
Flags: 0x0800, VXLAN Network ID (VNI)
0... .. = GBP Extension: Not defined
.... .0.. = Don't Learn: False
.... 1... = VXLAN Network ID (VNI): True
.... .0... = Policy Applied: False
.000 .000 0.00 .000 = Reserved(R): 0x0000
Group Policy ID: 0
VXLAN Network Identifier (VNI): 50901 <<<<<<<<<< L3VNI for VRF green
Reserved: 0
<--- Inner header started --->
Ethernet II, Src: 10:b3:d5:6a:00:00 (10:b3:d5:6a:00:00), Dst: 7c:21:0d:bd:27:48
(7c:21:0d:bd:27:48)
<...skip...>
Internet Protocol Version 4, Src: 10.1.251.1, Dst: 192.168.20.20
<...skip...>
User Datagram Protocol, Src Port: 67, Dst Port: 67
<...skip...>
Dynamic Host Configuration Protocol (Discover)
<...skip...>

```

Cliente DHCP en un VRF arrendatario y servidor DHCP en otro VRF arrendatario

En este ejemplo, el cliente está en rojo vrf y el servidor está en verde vrf.

Tiene dos opciones:

- Mantenga Relay IP en el vrf del cliente y configure la fuga de ruta, lo que añade más complejidad
- Mantenga Relay IP en el servidor vrf (similar a lo que hizo con GRT en el primer caso)

Es más sencillo elegir el segundo enfoque, ya que se admiten muchos vrfs de cliente y no se necesita fuga de ruta.

Configuración del switch:

```

ip dhcp relay information option vpn           <<< adds the vpn suboption to option 82
ip dhcp relay information option             <<< enables DHCP option 82
ip dhcp compatibility suboption link-selection standard <<< switch to standard option 82[5]
ip dhcp compatibility suboption server-override standard <<< switch to standard option 82[11]
ip dhcp snooping vlan 101-102,201-202       <<< enables dhcp snooping for vlans
ip dhcp snooping                            <<< enables dhcp snooping globally
!
interface Loopback101
vrf forwarding green
ip address 10.1.251.1 255.255.255.255
!
interface Vlan201
vrf forwarding red
ip dhcp relay source-interface Loopback101
ip address 10.2.201.1 255.255.255.0
ip helper-address vrf green 192.168.20.20           <<< DHCP is reachable over vrf green

```

Para vlan201:


```

▶ Frame 7: 394 bytes on wire (3152 bits), 394 bytes captured (3152 bits)
▶ Ethernet II, Src: a0:b4:39:21:92:3f (a0:b4:39:21:92:3f), Dst: Vmware_a8:b8:b4 (00:50:56:a8:b8:b4)
▶ Internet Protocol Version 4, Src: 10.1.251.1, Dst: 192.168.20.20
▶ User Datagram Protocol, Src Port: 67, Dst Port: 67
▼ Bootstrap Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 1
  Transaction ID: 0x000016ce
  Seconds elapsed: 0
  ▶ Bootp flags: 0x8000, Broadcast flag (Broadcast)
  Client IP address: 0.0.0.0
  Your (client) IP address: 0.0.0.0
  Next server IP address: 0.0.0.0
  Relay agent IP address: 10.1.251.1
  Client MAC address: Cisco_43:34:c4 (f4:cf:e2:43:34:c4)
  Client hardware address padding: 00000000000000000000
  Server host name not given
  Boot file name not given
  Magic cookie: DHCP
  ▶ Option: (53) DHCP Message Type (Discover)
  ▶ Option: (57) Maximum DHCP Message Size
  ▶ Option: (61) Client identifier
  ▶ Option: (12) Host Name
  ▶ Option: (55) Parameter Request List
  ▶ Option: (60) Vendor class identifier
  ▼ Option: (82) Agent Information Option
    Length: 42
    ▶ Option 82 Suboption: (1) Agent Circuit ID
    ▶ Option 82 Suboption: (2) Agent Remote ID
    ▶ Option 82 Suboption: (151) VRF name/VPN ID
    ▼ Option 82 Suboption: (5) Link selection
      Length: 4
      Link selection: 10.2.201.0
    ▶ Option 82 Suboption: (11) Server ID Override
  ▶ Option: (255) End

```

Captura de paquetes en la interfaz Spine-01 a Leaf-01:

```

Spine-01#sh mon cap TAC buff br | i DHCP
2 0.168829 10.1.251.1 b^F^R 192.168.20.20 DHCP 444 DHCP Discover - Transaction ID 0x10db
3 0.169450 192.168.20.20 b^F^R 10.1.251.1 DHCP 410 DHCP Offer - Transaction ID 0x10db
4 0.933121 10.1.251.1 b^F^R 192.168.20.20 DHCP 462 DHCP Request - Transaction ID 0x10db
5 0.933970 192.168.20.20 b^F^R 10.1.251.1 DHCP 410 DHCP ACK - Transaction ID 0x10db

```

En este ejemplo, el paquete en el núcleo está encapsulado VXLAN.

```

Frame 2: 446 bytes on wire (3552 bits), 444 bytes captured (3552 bits) on interface 0
<...skip...>
[Protocols in frame: eth:ethertype:ip:udp:vxlan:eth:ethertype:ip:udp:dhcp]
Ethernet II, Src: 10:b3:d5:6a:8f:e4 (10:b3:d5:6a:8f:e4), Dst: 7c:21:0d:92:b2:e4
(7c:21:0d:92:b2:e4)
<...skip...>
Internet Protocol Version 4, Src: 172.16.254.3, Dst: 172.16.254.5 <<< VTEP IP addresses
<...skip...>
User Datagram Protocol, Src Port: 65283, Dst Port: 4789
<...skip...>
Virtual eXtensible Local Area Network
Flags: 0x0800, VXLAN Network ID (VNI)
0... .. = GBP Extension: Not defined

```

```

.... .0.. .... = Don't Learn: False
.... 1... .... = VXLAN Network ID (VNI): True
.... .... 0... = Policy Applied: False
.000 .000 0.00 .000 = Reserved(R): 0x0000
Group Policy ID: 0
VXLAN Network Identifier (VNI): 50901 <<< L3VNI for VRF green
Reserved: 0
<--- Inner header started --->
Ethernet II, Src: 10:b3:d5:6a:00:00 (10:b3:d5:6a:00:00), Dst: 7c:21:0d:bd:27:48
(7c:21:0d:bd:27:48)
<...skip...>
Internet Protocol Version 4, Src: 10.1.251.1, Dst: 192.168.20.20
<...skip...>
User Datagram Protocol, Src Port: 67, Dst Port: 67
<...skip...>
Dynamic Host Configuration Protocol (Discover)
<...skip...>

```

Cliente DHCP en un VRF arrendatario y servidor DHCP en otro VRF no VXLAN

Este caso es muy similar al anterior. La diferencia clave es que los paquetes no tienen encapsulación VXLAN - IP pura o algo más (MPLS/GRE/etc), pero es lo mismo desde la perspectiva de la configuración.

En este ejemplo, el cliente está en rojo vrf y el servidor está en verde vrf.

Tiene dos opciones:

- La IP de retransmisión se encuentra en el vrf del cliente y configura la fuga de ruta, lo que aumenta la complejidad
- La IP de retransmisión está en el vrf del servidor (similar a lo que se hizo para GRT en el primer caso)

Es más sencillo elegir el segundo enfoque, ya que se admiten muchos vrfs de cliente y no se necesita fuga de ruta.

Configuración del switch:

```

ip dhcp relay information option vpn <<< adds the vpn suboption to option 82
ip dhcp relay information option <<< enables DHCP option 82
ip dhcp compatibility suboption link-selection standard <<< switch to standard option 82[5]
ip dhcp compatibility suboption server-override standard <<< switch to standard option 82[11]
ip dhcp snooping vlan 101-102,201-202 <<< enable dhcp snooping for vlans
ip dhcp snooping <<< enable dhcp snooping globally
!
interface Loopback101
vrf forwarding green
ip address 10.1.251.1 255.255.255.255
!
interface Vlan201
vrf forwarding red
ip dhcp relay source-interface Loopback101
ip address 10.2.201.1 255.255.255.0
ip helper-address vrf green 192.168.20.20 <<< DHCP is reachable over vrf green

```

Información Relacionada

- [RFC 3046](#)

- [RFC 3527](#)
- <https://docs.microsoft.com>
- [Soporte Técnico y Documentación - Cisco Systems](#)