

# Configurer DHCP dans IOS XE EVPN/VXLAN

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Configuration](#)

[Diagramme du réseau](#)

[Configurations](#)

[Configuration du serveur](#)

[Option de configuration 1 de Win2012 R2 - IP de relais unique par VNI/SVI par VTEP](#)

[Option 2 de configuration de Win2012 R2 - Correspondance du champ ID de circuit de l'agent](#)

[Configuration de Windows Server 2016](#)

[Serveur DHCP Linux](#)

[Configuration du commutateur](#)

[Le client DHCP se trouve dans le VRF du client et le serveur DHCP dans le VRF par défaut de couche 3](#)

[Le client DHCP et le serveur DHCP se trouvent dans le même VRF locataire](#)

[Client DHCP dans un serveur VRF et DHCP locataire dans un autre VRF locataire](#)

[Client DHCP dans un serveur VRF et DHCP locataire dans un autre VRF non-VXLAN](#)

[Informations connexes](#)

## Introduction

Ce document décrit la configuration du protocole DHCP (Dynamic Host Configuration Protocol) pour un réseau local virtuel extensible Ethernet VPN (EVPN) (VXLAN) dans différents scénarios, ainsi que des aspects spécifiques pour les serveurs DHCP Win2012 et Win2016.

## Conditions préalables

### Conditions requises

Cisco vous recommande de connaître EVPN/VXLAN et DHCP.

### Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

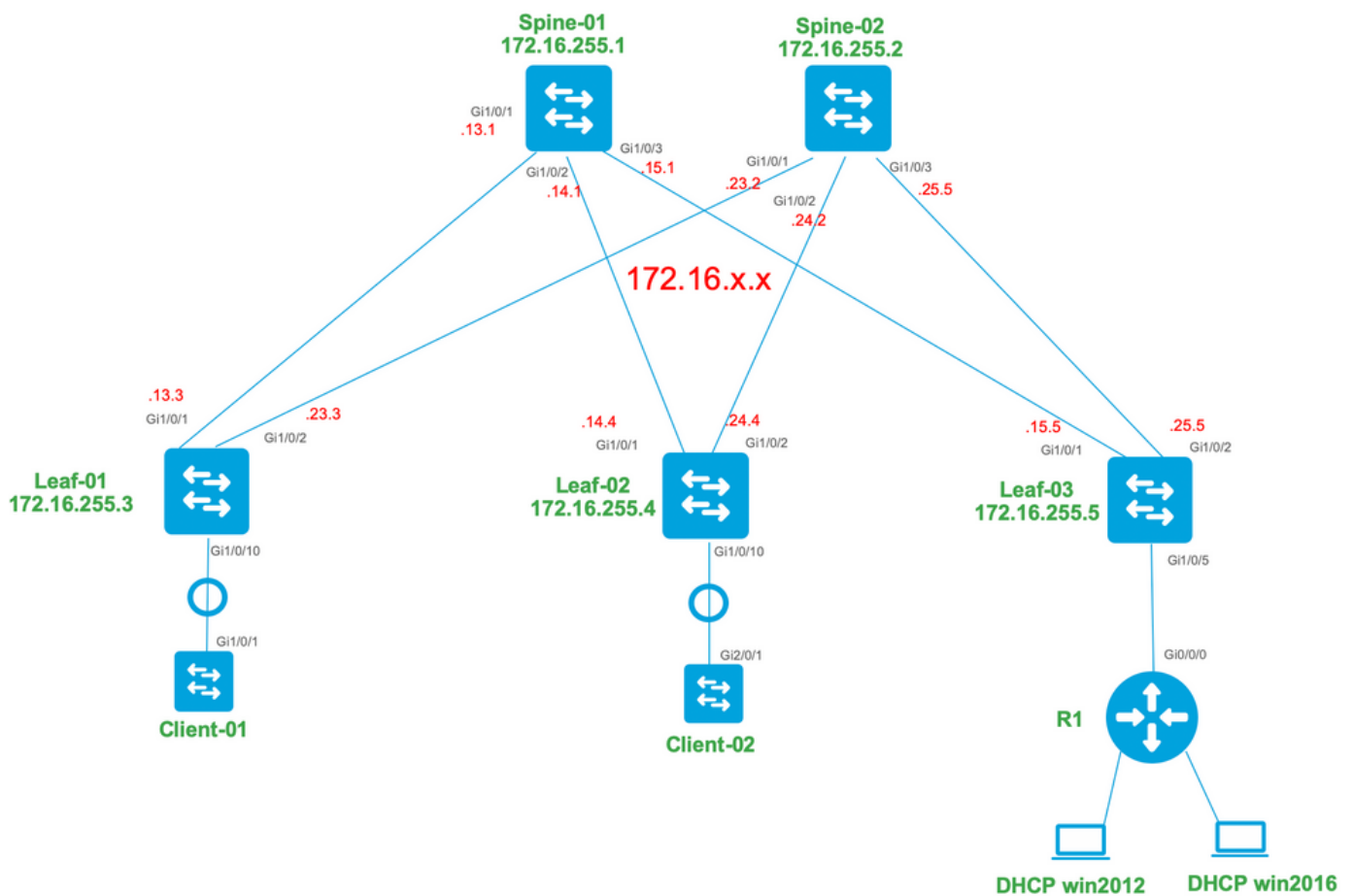
- C9300
- C9400
- C9500
- C9600

- MSFT Windows Server 2012 R2
- MSFT Windows Server 2016
- Fonctionnalités disponibles sur Cisco IOS XE 16.9.x ou version ultérieure

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 votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

## Configuration

### Diagramme du réseau

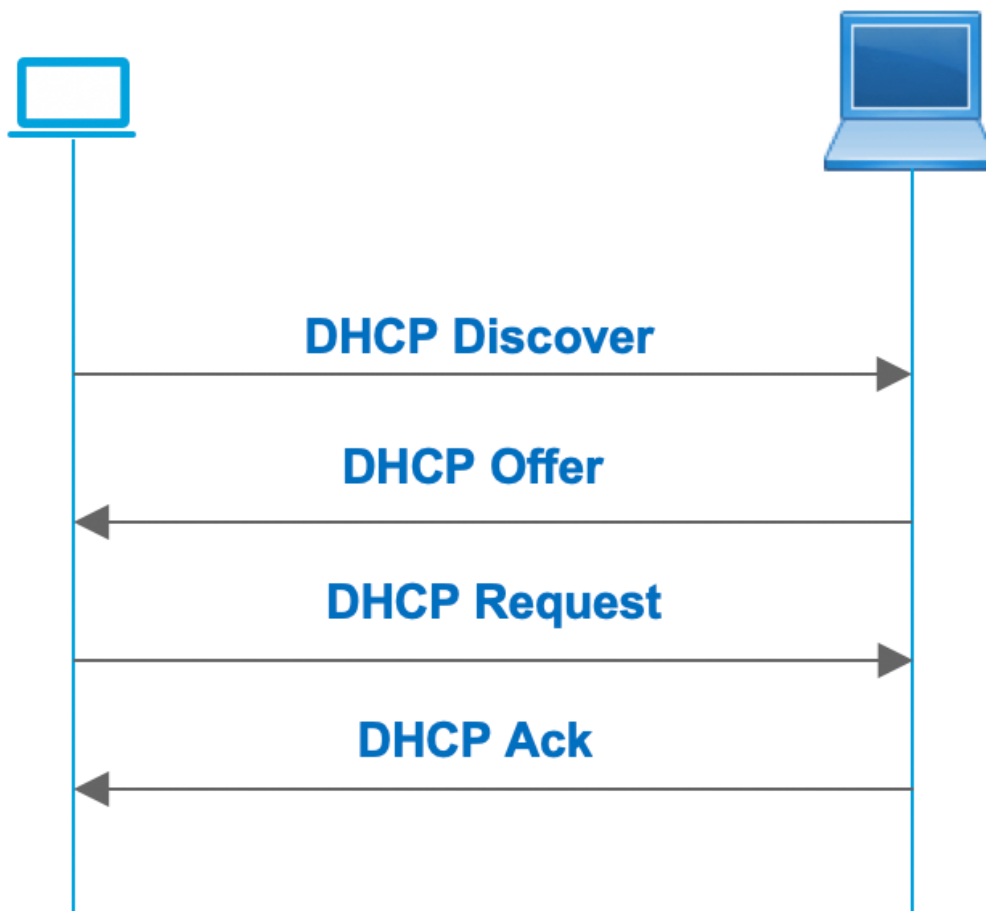


## Configurations

Examinons maintenant le flux de messages entre le client et le serveur DHCP. Il y a 4 phases :

# DHCP client

# DHCP server



Cela fonctionne pour les cas où le client et le serveur se trouvent dans le même sous-réseau, mais généralement, ce n'est pas le cas. Dans la plupart des cas, le serveur DHCP ne se trouve pas dans le même sous-réseau que le client et doit être accessible via un chemin routé de couche 3 par rapport à la couche 2. Dans ce cas, la fonctionnalité de relais DHCP est requise. La fonction de relais DHCP (commutateur ou routeur) convertit la diffusion en monodiffusion encapsulée udp qui est routable et l'envoie au serveur DHCP. Il s'agit d'une configuration couramment utilisée dans les réseaux de nos jours.

Défis liés au fabric DHCP et EVPN/VXLAN :

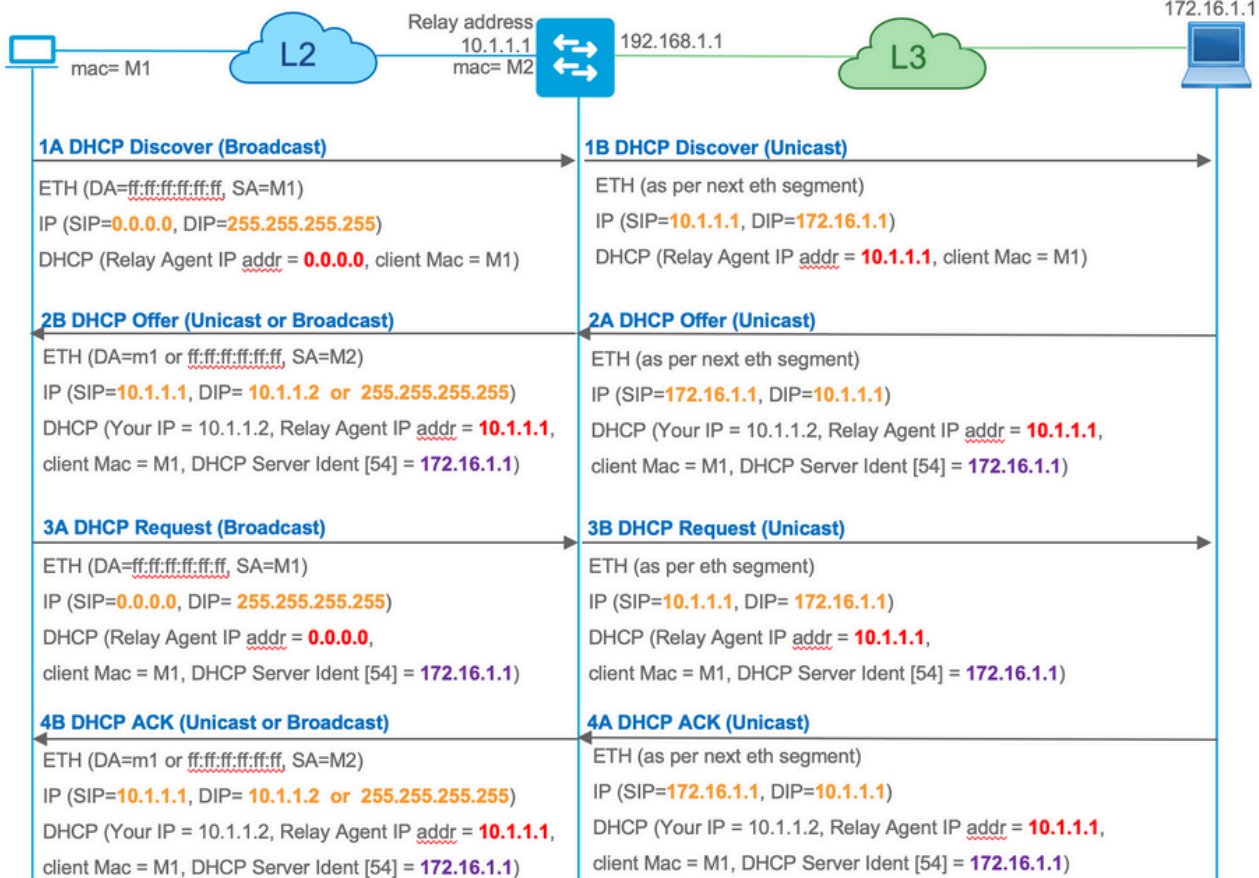
Généralement, le serveur DHCP est connecté au fabric EVPN sur le réseau L3. Cela signifie que vous devez utiliser la fonctionnalité de relais DHCP pour convertir un paquet de diffusion DHCP de couche 2 en un paquet routable de monodiffusion de couche 3.

Avec la fonction de relais DHCP, le flux d'appels DHCP entre le client, le relais et le serveur fonctionne comme suit :

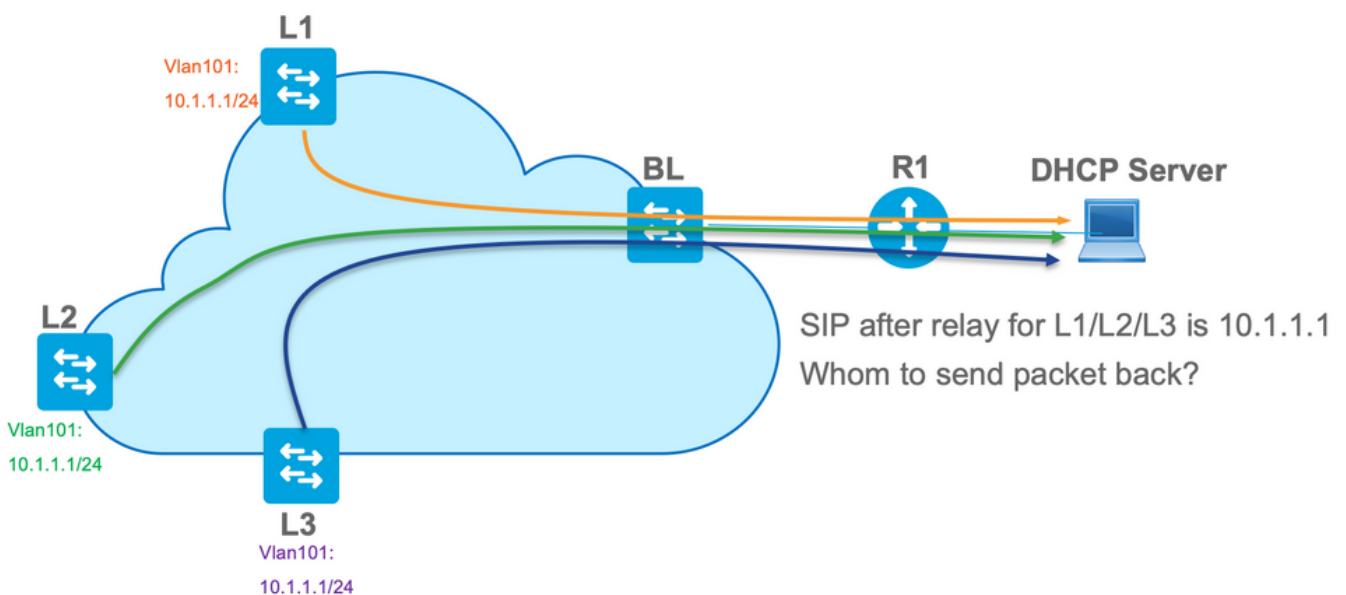
## DHCP client

## DHCP relay

## DHCP server



Une fois relayé, l'adresse IP source du paquet est l'adresse IP de relais. Cependant, cela crée un problème dans le déploiement VXLAN/EVPN, car l'adresse IP source habituelle n'est pas unique en raison de l'utilisation de Distributed Anycast GW (DAG). Comme toutes les adresses IP source VTEP SVI sont identiques, cela peut entraîner le transfert des paquets de réponse du serveur DHCP vers le leaf le plus proche.



Afin de résoudre le problème de source non unique, vous devez pouvoir utiliser une adresse IP unique pour les paquets DHCP relayés par leaf. Un autre problème concerne le remplacement du GIADDR. Sur le serveur DHCP, vous devez choisir le pool approprié pour attribuer l'adresse IP. II

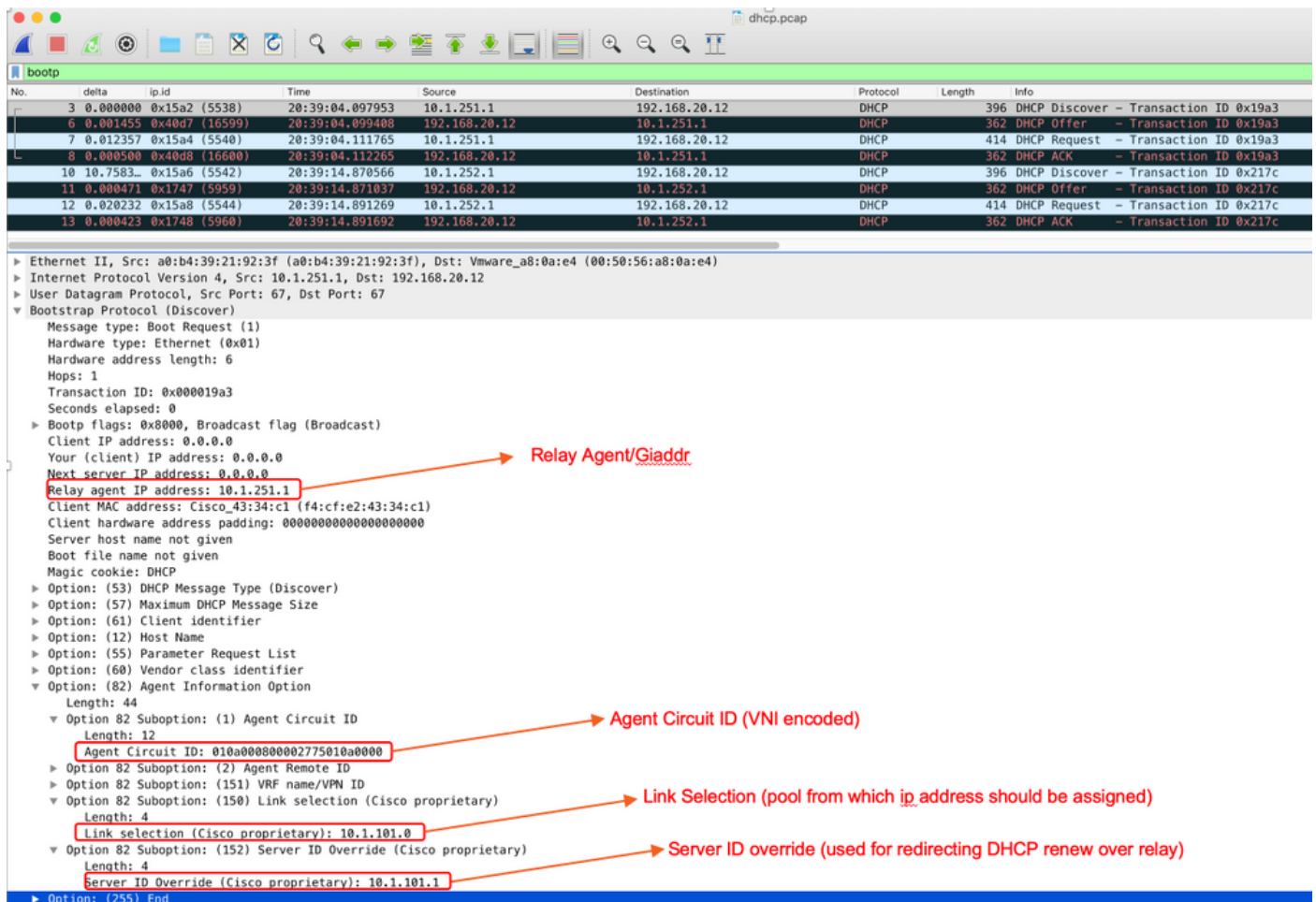
est effectué à partir du pool, qui couvre l'adresse IP de la passerelle (giaddr). Pour le fabric EVPN, il doit s'agir d'une adresse IP de SVI, mais après le relais, la giaddr est remplacée par une adresse IP de relais qui est dans ce cas un bouclage unique.

Comment pouvez-vous informer le serveur DHCP, quels pools il doit utiliser ?

Pour résoudre ce problème, l'option 82 est utilisée. Il s'agit principalement des principales sous-options :

- 1 - L'ID de circuit de l'agent. Dans le cas de VXLAN/EVPN, cette sous-option transfère l'ID VNI
- 5 - (ou 150 pour cisco propriétaire). Les sous-options de sélection de liaison qui ont un sous-réseau réel, d'où provient le paquet DHCP
- 11 - (ou 152 pour cisco propriétaire). La sous-option Server Identifier Override qui a l'adresse du serveur DHCP
- 151 - Nom VRF/ID VPN. Cette sous-option a un nom VRF/ID VPN

Dans une capture de paquet du paquet du relais DHCP au serveur DHCP, vous pouvez voir ces différentes options présentes dans le paquet DHCP comme l'illustre l'image.



Configuration du commutateur:

- L'option 82 dispose de toutes les informations nécessaires pour choisir le pool DHCP approprié et renvoyer le paquet du serveur vers le noeud leaf approprié.
- Cela ne fonctionne que si le serveur DHCP peut traiter les informations de l'option 82, bien que tous les serveurs ne le prennent pas entièrement en charge (comme 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

```

## Configuration du serveur

### Option de configuration 1 de Win2012 R2 - IP de relais unique par VNI/SVI par VTEP

Le problème principal avec win2012 est que l'option 82 n'est pas entièrement prise en charge, de sorte que la sous-option « Sélection de lien » (5 ou propriétaire Cisco - 150) ne peut pas être utilisée pour sélectionner le pool approprié sur le serveur DHCP.

Pour résoudre un tel problème, cette approche peut être utilisée :

- Une étendue pour les adresses IP RELAY doit être créée sinon DHCP ne trouve pas de pool correspondant à DHCP GIADDR et ignore le paquet. La plage d'adresses IP complète doit être exclue de DHCP pour empêcher l'allocation du pool d'adresses IP RELAY. Nous appelons ce pool RELAY\_POOL
- L'étendue de la plage d'adresses IP que vous souhaitez allouer doit être créée. Nous appelons ce pool IP\_POOL
- L'étendue globale doit être créée et les deux étendues : RELAY\_POOL et IP\_POOL doivent être incluses

Voyons comment le paquet DHCP est traité sur le serveur.

1. Le paquet DHCP est reçu par le serveur.
2. Basé sur GIADDR, le pool respectif RELAY\_POOL est choisi dans l'étendue globale appropriée.
3. Comme il n'y a aucune adresse IP libre dans RELAY\_POOL (vous souvenez-vous que l'étendue complète est exclue ?), il revient à IP\_POOL dans la même étendue globale.
4. L'adresse est attribuée à partir du super-pool respectif et renvoyée au relais.

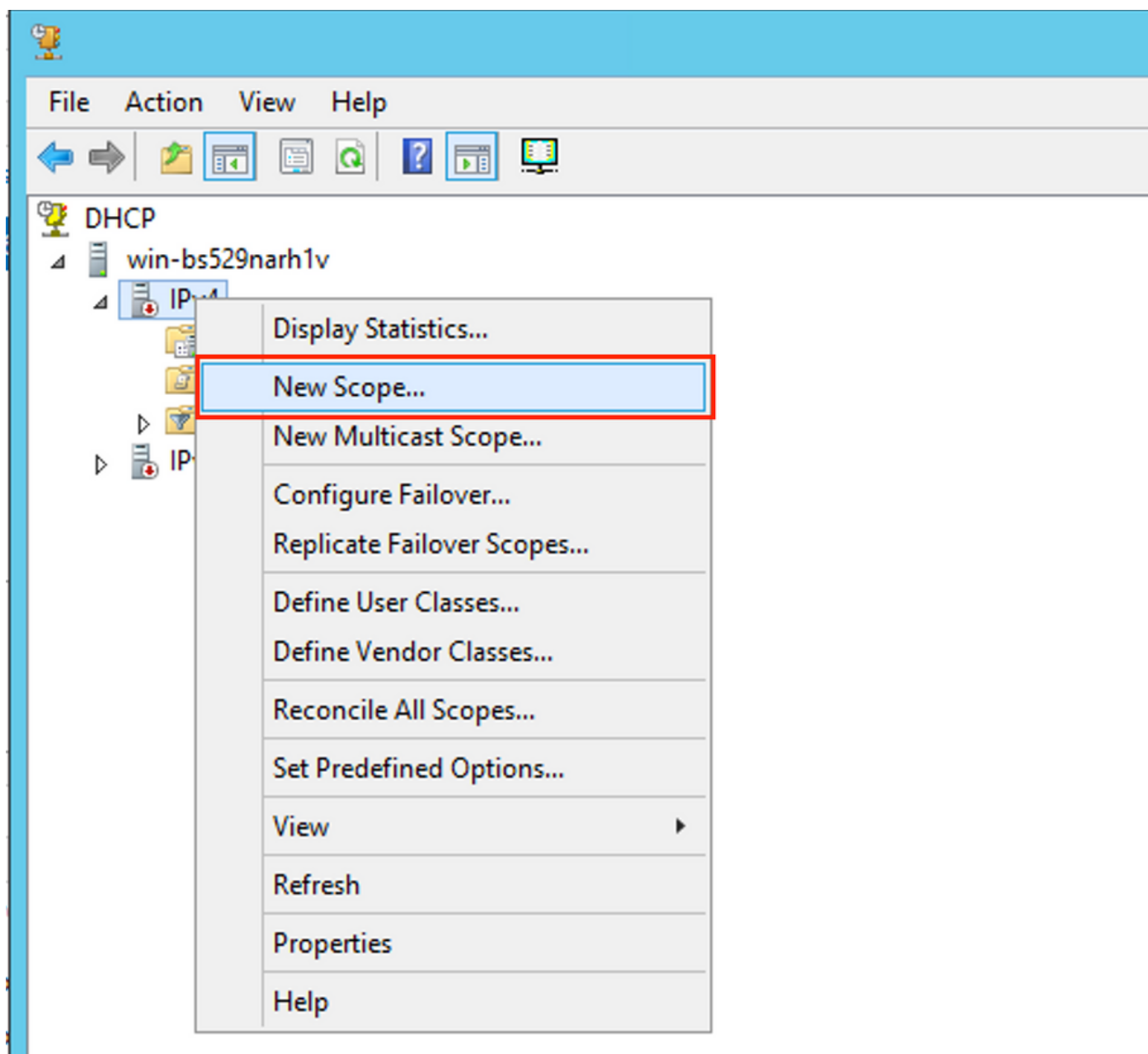
Un gros inconvénient de cette méthode est que vous devez avoir un bouclage unique par VLAN/VNI par vtep, car le pool DHCP est sélectionné en fonction de l'adresse de relais.

Cette option nous conduit à l'utilisation d'une grande plage IP pour les adresses IP de relais.

Option 1. Instructions pas à pas sur la configuration de win2012 r2.

Créez l'étendue DHCP pour les adresses de relais. Cliquez avec le bouton droit de la souris et

sélectionnez **Nouvelle étendue** comme indiqué dans l'image.



Sélectionnez **Suivant** comme indiqué dans l'image.

## 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

Complétez un nom significatif, Description, puis sélectionnez **Suivant** comme indiqué dans l'image.



## 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

Complétez les informations d'adresse IP du pool de relais. Dans cet exemple, le masque de réseau est /24, mais il peut être plus grand ou plus petit (il dépend de la taille du réseau) comme le montre l'image.

## 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

Excluez toutes les plages du pool. Ceci est important, sinon, les adresses IP peuvent être attribuées à partir de ce pool.

## 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

Configurez la durée du bail (par défaut, elle est de 8 jours) comme indiqué dans l'image.

## 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:
<input type="text" value="3"/>	<input type="text" value="0"/>	<input type="text" value="0"/>

< Back

Next >

Cancel

Vous pouvez configurer les paramètres d'option DHCP tels que DNS/WINS (ignorés dans cet exemple).

## 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

Activez l'étendue comme indiqué dans l'image.

## 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

Terminez la configuration comme indiqué dans l'image.

## 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.

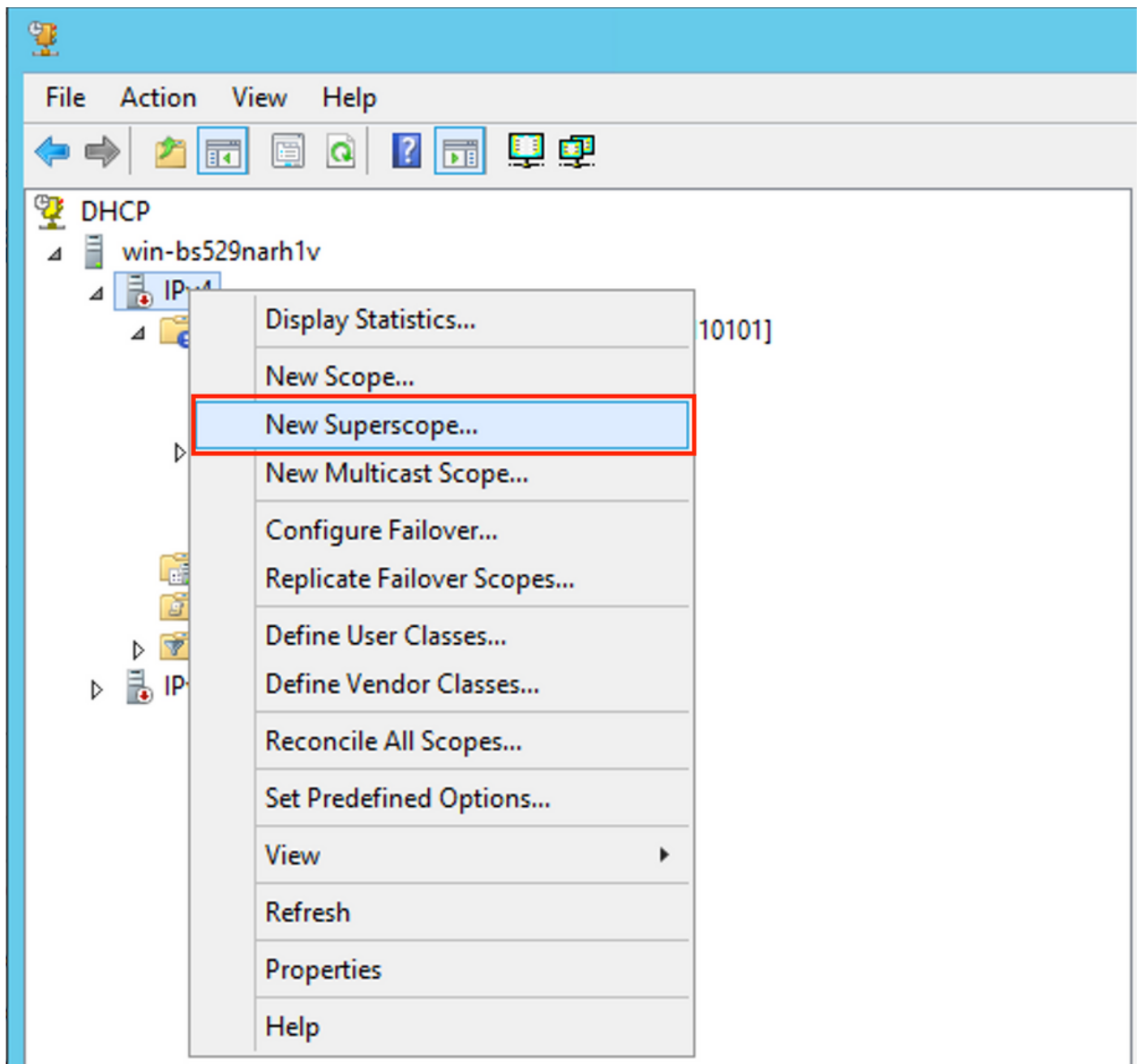
To close this wizard, click Finish.

< Back

Finish

Cancel

Maintenant, créez une étendue globale. Sélectionnez avec le bouton droit et choisissez **Nouvelle étendue globale** comme indiqué dans l'image.



Sélectionnez **Suivant** comme indiqué dans l'image.



## 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

Choisissez un nom significatif pour l'**étendue globale** comme indiqué dans l'image.

## New Superscope Wizard

### Superscope Name

You have to provide an identifying superscope name.



Name:

< Back

Next >

Cancel

Sélectionnez l'étendue à ajouter à l'étendue globale.

## 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:

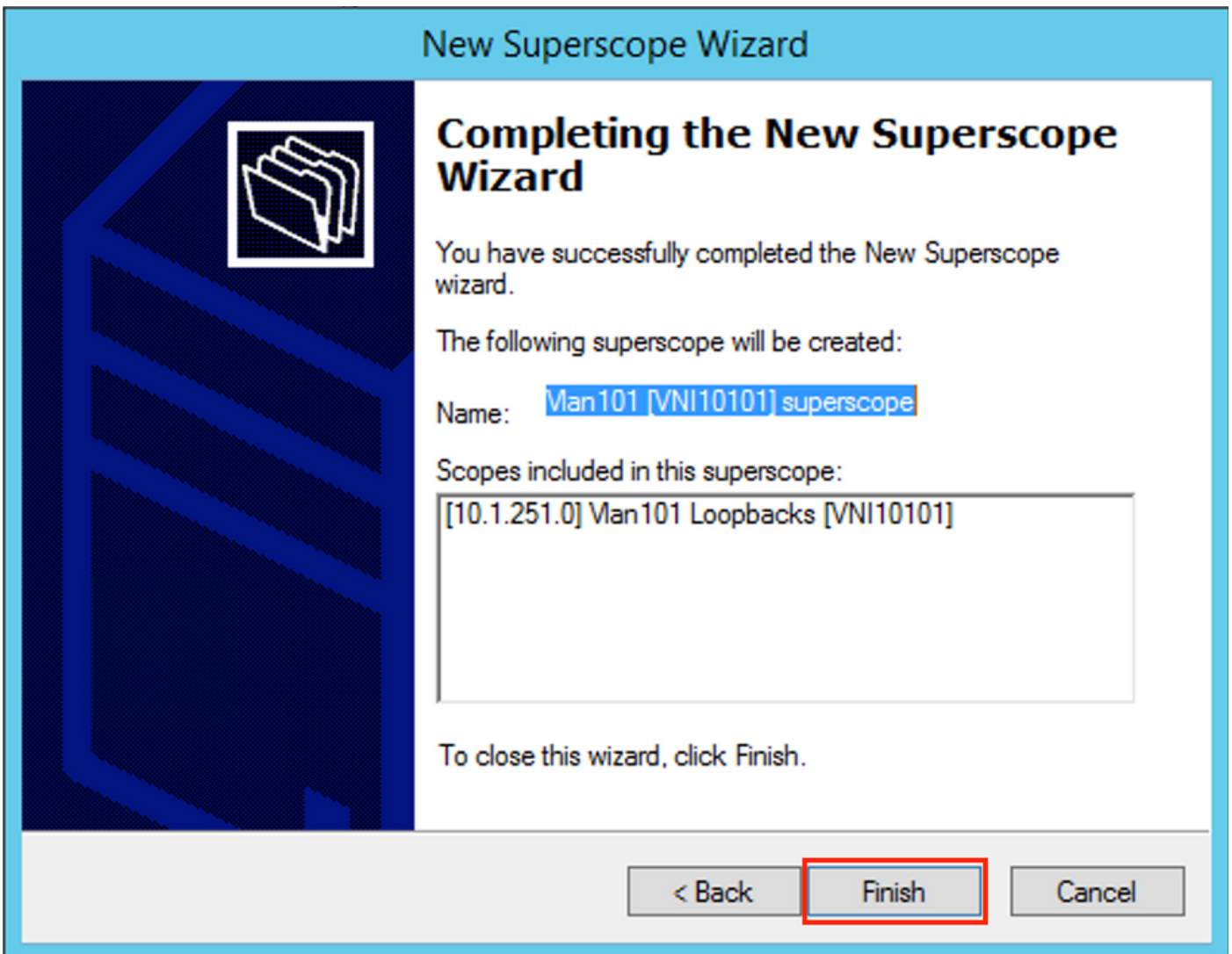
[10.1.251.0] Man101 Loopbacks [VNI10101]

< Back

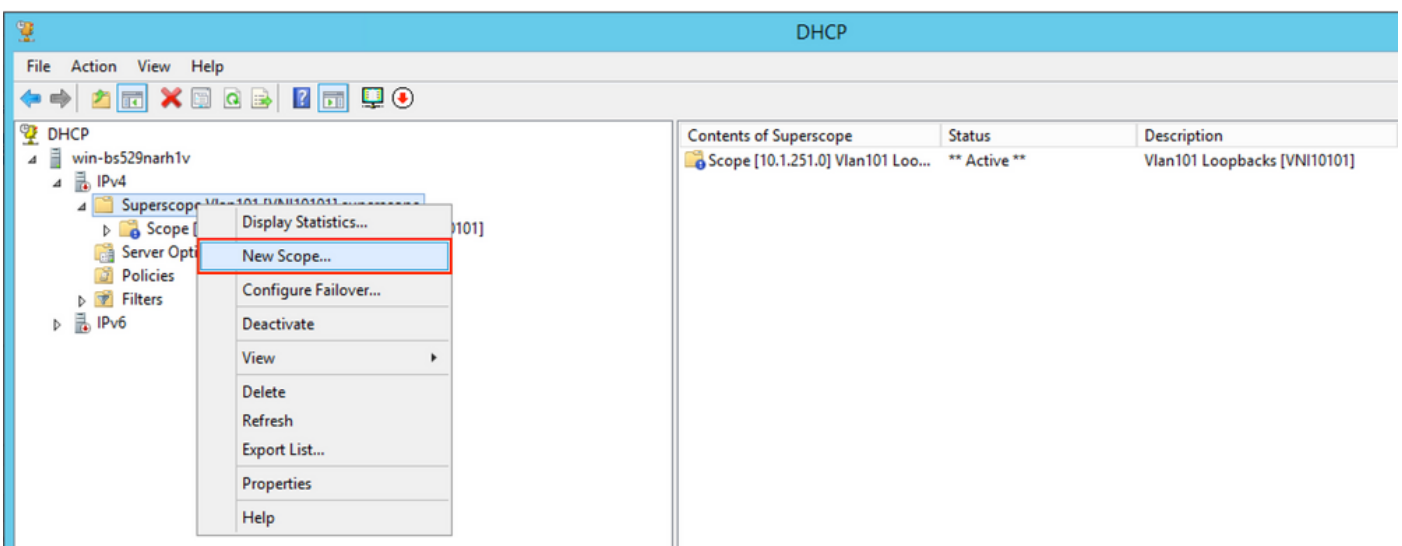
Next >

Cancel

Terminez la configuration comme indiqué dans l'image.



Créez un pool DHCP à partir duquel les adresses IP sont attribuées. Cliquez avec le bouton droit de la souris et sélectionnez **Nouvelle étendue...** comme le montre l'image.



Sélectionnez **Suivant** comme indiqué dans l'image.

## 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

Choisissez un nom et une description significatifs comme indiqué dans l'image.

## 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

Spécifiez le réseau et le masque du pool dont vous voulez allouer les adresses IP aux clients, comme l'illustre l'image.

## 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

Exclure l'adresse IP de la passerelle par défaut du pool (dans cet exemple, il s'agit de 10.1.101.1) comme indiqué dans l'image.

## 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

Spécifiez le temporisateur de bail comme indiqué dans l'image.



## 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

Vous pouvez éventuellement spécifier DNS/WINS (ignoré dans cet exemple).

## 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

Terminez la configuration comme indiqué dans l'image.



Après la création du pool, une stratégie doit être créée pour le pool.

- Dans la stratégie, l'ID de circuit de l'agent [1] correspond
- Si vous avez plusieurs VLAN/VNI, vous devez créer un super-pool avec des sous-pools pour les adresses IP de relais et la plage IP réelle pour l'allocation par chaque VLAN/VNI
- Cet exemple utilise les VNI 10101 et 10102

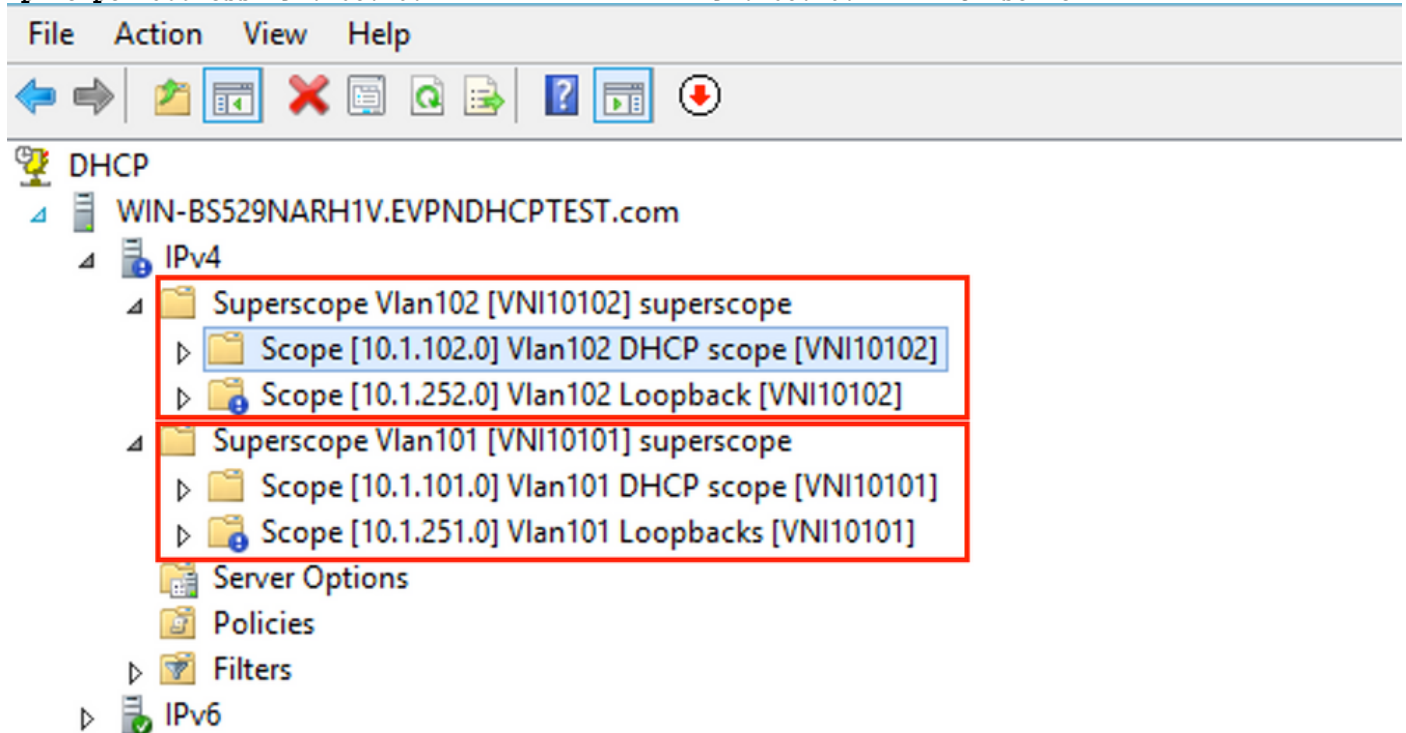
Configuration du commutateur:

```
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

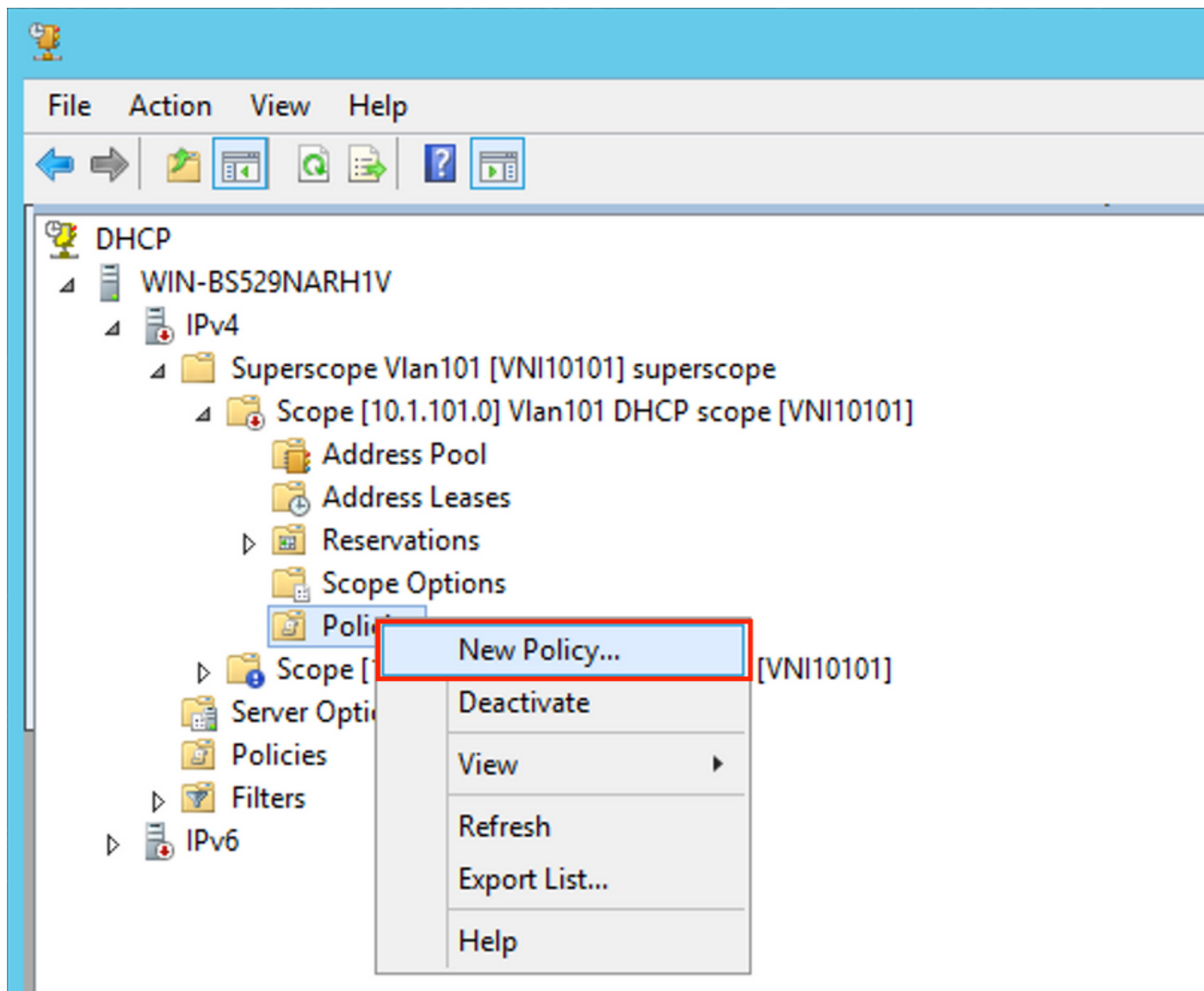
```



## Option 2 de configuration de Win2012 R2 - Correspondance du champ ID de circuit de l'agent

- L'inconvénient de la dernière approche est l'utilisation élevée du bouclage unique. Une autre option consiste donc à faire correspondre le champ ID de circuit de l'agent.
- Les étapes sont identiques, mais vous ajoutez la création de stratégie pour la sélection de l'étendue, non basée sur le champ ID de circuit de l'agent plutôt que sur IP de relais.

Création de stratégie. Cliquez avec le bouton droit sur le pool et sélectionnez **Nouvelle stratégie** comme indiqué dans l'image.



Choisissez un nom et une description significatifs pour la stratégie comme indiqué dans l'image.

## 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


Ajoutez la nouvelle condition comme l'illustre l'image.

## 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

Entrez l'ID de circuit approprié (n'oubliez pas la zone **Ajouter un caractère générique (\*)**) comme indiqué dans l'image.

**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(\*)

Précisions sur les raisons du choix de ce nombre :

Dans Wireshark, l'ID de circuit d'agent est égal à **010a000800002775010a0000**, d'où provient cette valeur (00002775 hex = 10100 La valeur décimale 1 est égale à la valeur VNI 10101 configurée pour le 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 sous-option ID de circuit de l'agent est codée dans ce format pour VXLAN VN :


Type de sous-option	Longueur	Type d'ID de circuit	Longueur	VNI	mod	port
01	1 octet	0 a	1 octet	00	4 bytes	2 octets
			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

Configurez la plage IP à partir de laquelle les adresses IP sont attribuées. Sans cette configuration, aucune allocation pour l'**étendue actuelle** n'est possible.

## 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

Vous pouvez également sélectionner des options DHCP standard à ce stade, comme l'illustre l'image.

## 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

Sélectionnez **Terminer** comme indiqué dans l'image.

## 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:

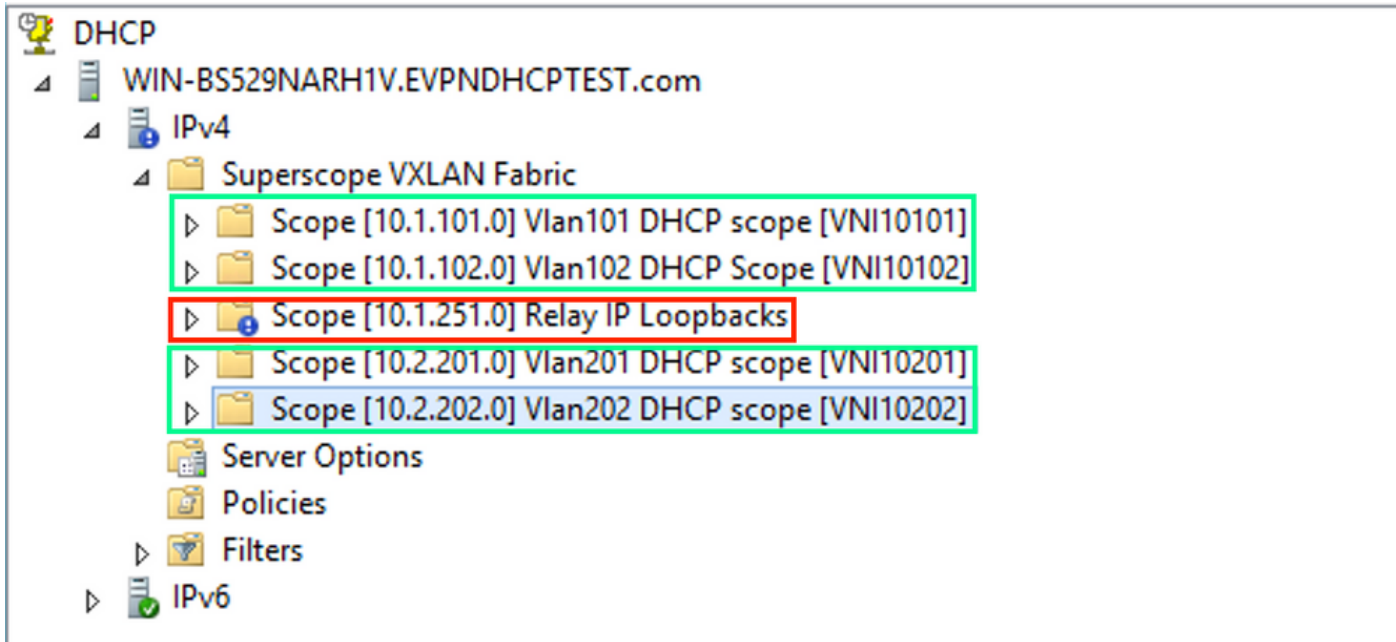
Option Name	Vendor Class	Value
-------------	--------------	-------

< Back

Finish

Cancel

Une configuration similaire doit être effectuée pour d'autres pages, comme illustré dans l'image.



Dans ce scénario, vous ne pouvez utiliser qu'une seule adresse IP unique par VTEP pour le nombre d'interfaces SVI, pas un seul bouclage par VNI/SVI par VTEP.

Configuration du commutateur:

```

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

```

Configuration de Windows Server 2016

- Windows Server 2016 prend en charge l'option 82 sous-options 5 (Cisco propriétaire 150) « Sélection de liaison », ce qui signifie que vous n'utilisez pas une adresse IP de relais unique pour la sélection du pool. La sous-option « Sélection de lien » est utilisée, ce qui simplifie considérablement la configuration.
- Il serait préférable que vous disposiez encore d'un pool d'adresses IP de relais, sinon le paquet DHCP ne correspond à aucune étendue et n'est pas traité.

Cet exemple illustre l'utilisation de l'option de sélection de lien.

Lancez un pool d'adresses IP pour les adresses IP de relais, comme illustré dans l'image.

DHCP

File Action View Help



DHCP

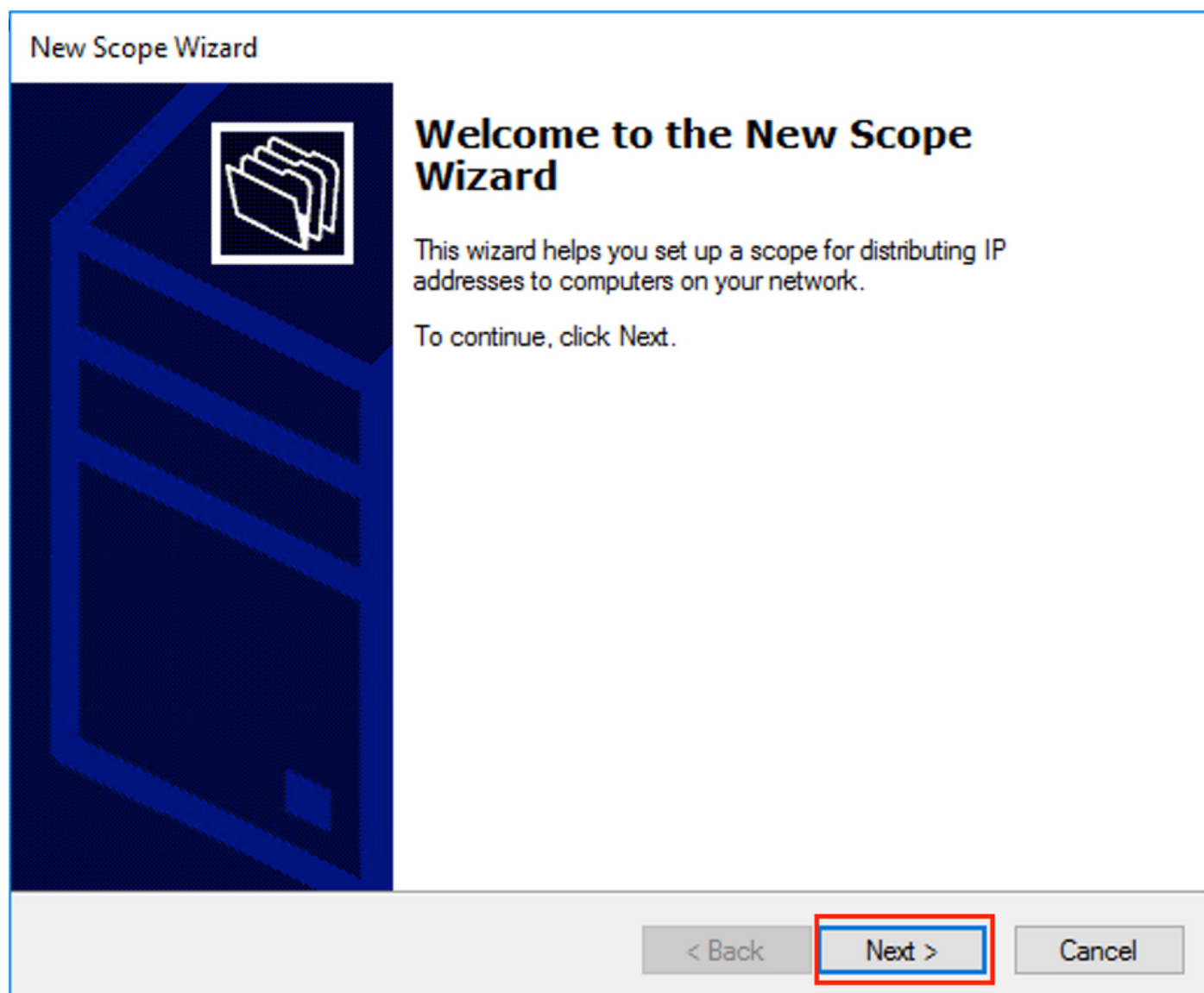
WIN-IC90QQIUTE8.EVPNDHCPTTEST2016.com

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



Sélectionnez **Suivant** comme indiqué dans l'image.



Choisissez un nom et une description significatifs pour l'étendue comme indiqué dans l'image.

## 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:

Saisissez l'espace d'adressage IP utilisé pour les relais IP, comme illustré dans l'image.

## 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

Exclure toutes les plages de l'étendue pour empêcher l'allocation de cette plage comme l'illustre l'image.

## 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

Vous pouvez également choisir l'option DNS/WINS etc paramètres (ignorés dans cet exemple) comme indiqué dans l'image.

## 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

Sélectionnez **Terminer** comme indiqué dans l'image.

## 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.

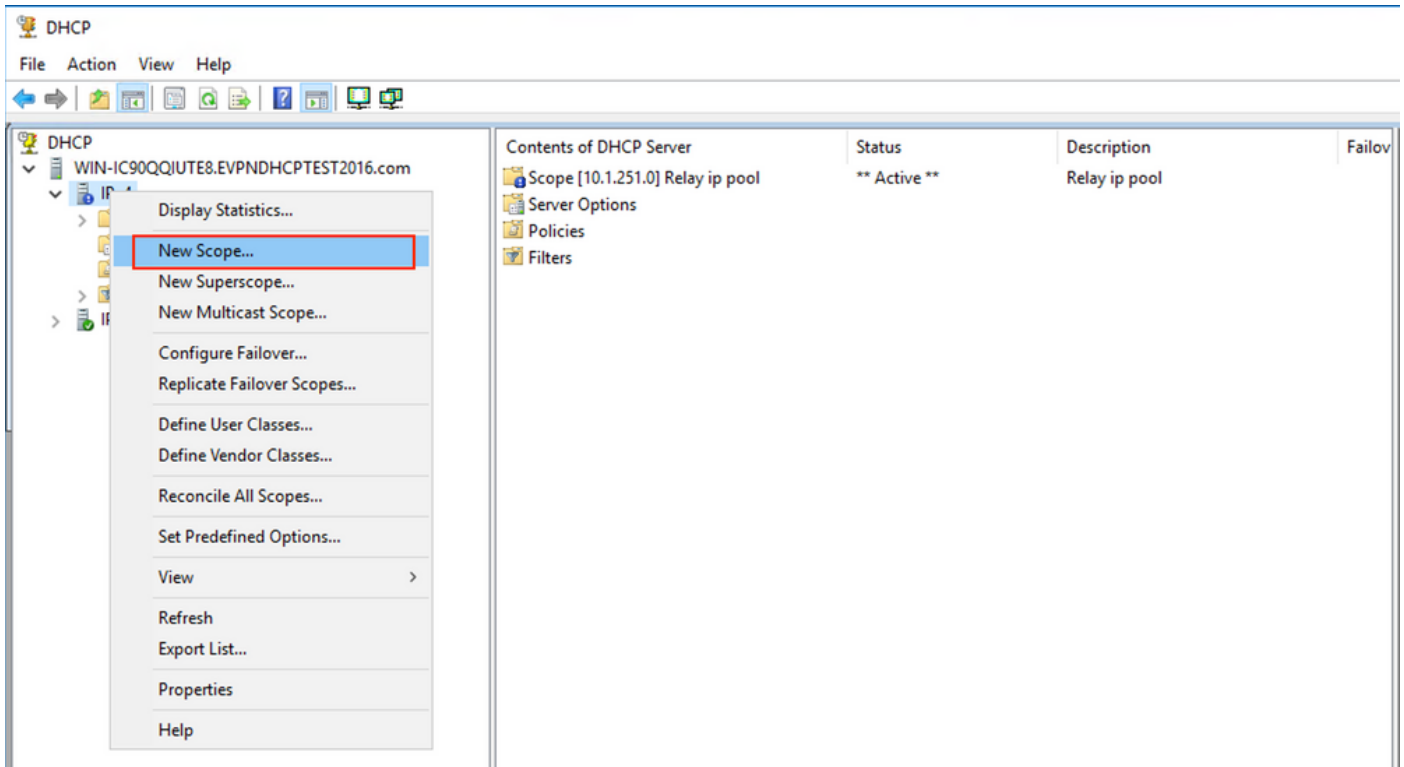
< Back

Finish

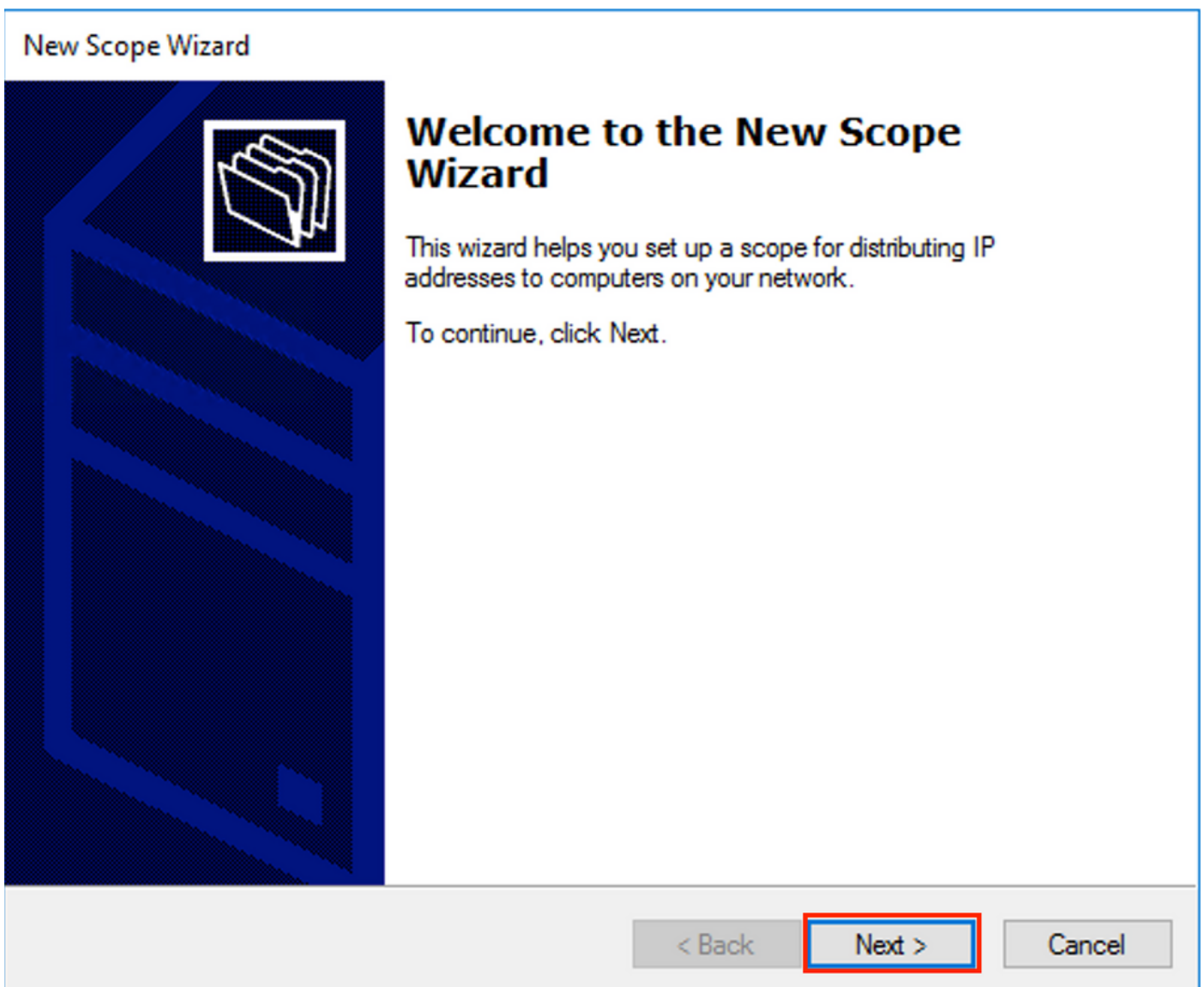
Cancel

La portée des relais est maintenant prête.

- Ensuite, vous créez le pool à partir duquel les clients obtiennent des adresses IP.
- Cliquez avec le bouton droit de la souris et sélectionnez **Nouvelle étendue** comme indiqué dans l'image.



Sélectionnez **Suivant** comme indiqué dans l'image.



Choisissez un nom et une description significatifs pour le pool, comme indiqué dans l'image.

## 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

Saisissez l'espace d'adressage IP à allouer dans vlan101, comme illustré dans l'image.



## 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

Exclure l'adresse IP de la passerelle par défaut de l'étendue comme illustré dans l'image.

## 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

Définissez une durée de bail comme indiqué dans l'image.

## 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

D'autres paramètres tels que DNS/WINS et d'autres peuvent être configurés (ignorés dans cet exemple) comme l'illustre l'image.

## 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?

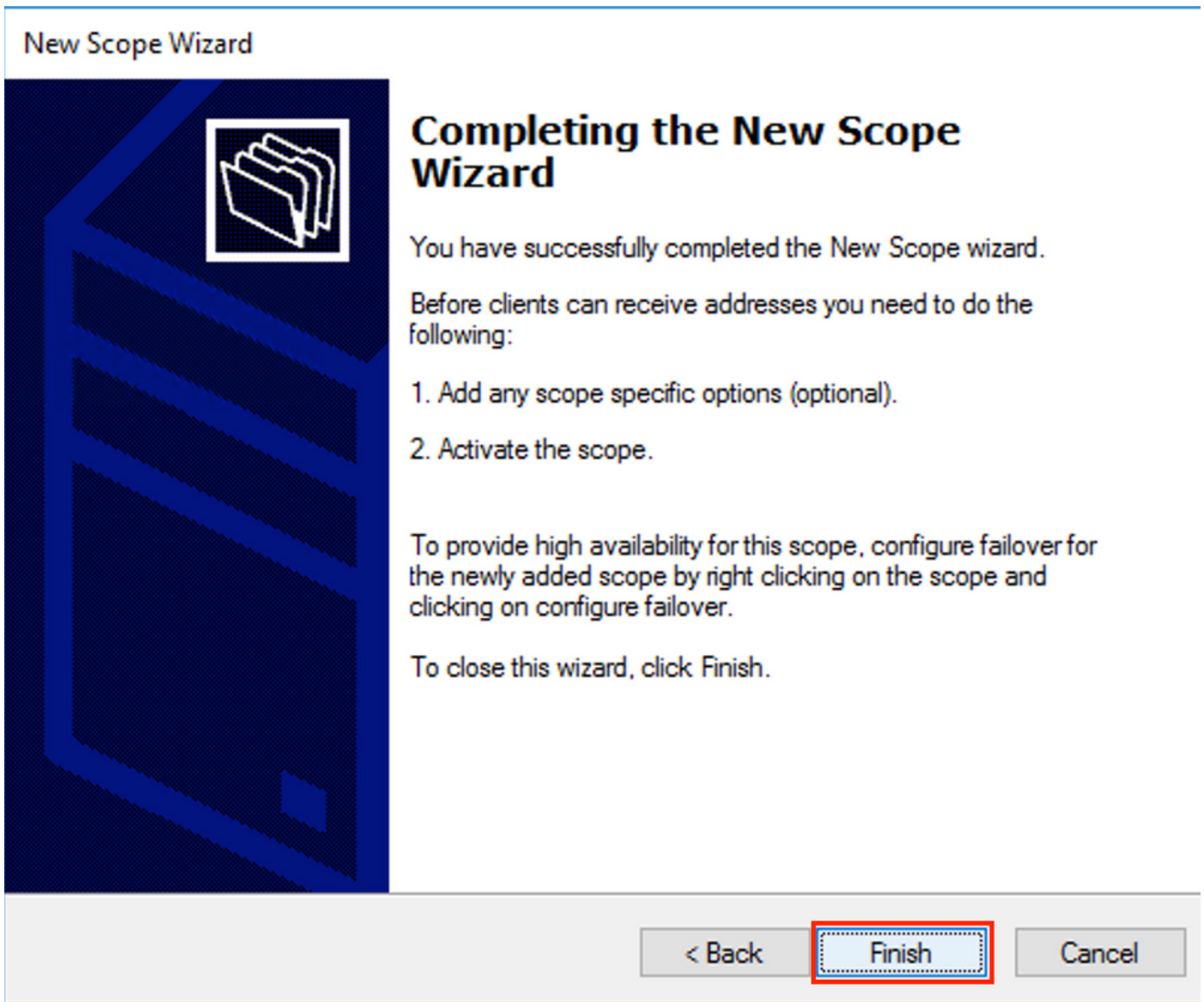
- Yes, I want to configure these options now
- No, I will configure these options later

< Back

Next >

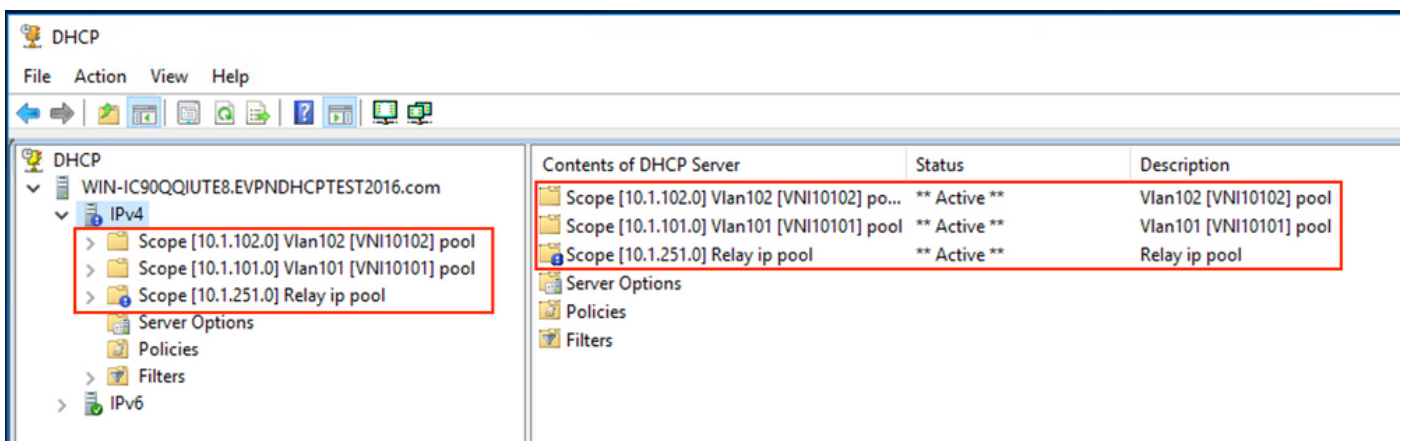
Cancel

Sélectionnez **Terminer** pour terminer l'installation comme indiqué dans l'image.



Le pool par adresse IP de relais n'est pas configuré et ne correspond pas dans HEX. La sélection du pool est basée sur la **sélection** de la sous-option **Lien**.

Un nouveau pool peut être ajouté et aucune configuration supplémentaire n'est nécessaire, comme l'illustre l'image.



## Serveur DHCP Linux

Examinez la configuration du serveur isc-dhcp sous Linux.

- Il prend en charge l'option de relais 82. Ici, la plus importante est la sous-option de sélection de liens. Vous pouvez toujours utiliser les informations d'ID de circuit d'agent et le masque/correspondance hexadécimal pour le champ spécifique (comme pour win2012). D'un point de vue pratique, il est beaucoup plus facile d'utiliser 82[5] que de travailler directement avec les informations d'ID de circuit d'agent.
- La configuration de la sous-option de sélection de liaison est effectuée sous la définition de sous-réseau.

Dans cet exemple, le serveur ISC est utilisé sur Ubuntu Linux.

Installez le serveur DHCP :

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

Afin de configurer le serveur DHCP modifier `/etc/dhcp/dhcpd.conf`. (L'éditeur Vim est utilisé dans un exemple)

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

Extrait de configuration (les configurations générales sont omises) :

```

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;
}
```

## Configuration du commutateur

Les scénarios pris en charge en général sont examinés ici.

1. Le client DHCP se trouve dans le VRF du client et le serveur DHCP dans le VRF par défaut de couche 3
2. Le client DHCP se trouve dans le VRF du locataire et le serveur DHCP est dans le même VRF du locataire
3. Le client DHCP se trouve dans le VRF du locataire et le serveur DHCP dans un VRF du locataire différent
4. Le client DHCP se trouve dans le VRF du client et le serveur DHCP dans un VRF non VXLAN par défaut

Pour l'un de ces scénarios, la configuration du relais DHCP est nécessaire côté commutateur.

Configuration DHCP pour l'option la plus simple numéro 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]
```

Par défaut, l'option 82 **Sélection de liaison et Remplacement d'ID de serveur** sont propriétaires de Cisco par défaut (150 et 152 respectivement).

- ▼ 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, pour une raison quelconque, le serveur DHCP ne **comprend** pas les options propriétaires de Cisco, vous pouvez les remplacer par les options standard.

```
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

La surveillance DHCP doit être activée pour les VLAN nécessaires.

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

Vous pouvez utiliser la configuration globale de l'interface source de relais DHCP.

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

Vous pouvez également le configurer par interface (la configuration de l'interface remplace la configuration globale).

```
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
```

Vérifiez qu'il existe une adresse IP de relais b/w de connectivité IP et un serveur DHCP dans les deux directions.

```
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
```

Dans la configuration d'interface, l'adresse du serveur DHCP est configurée. Cette commande peut comporter 3 options. Le client et le serveur se trouvent dans le même 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
```

Le client et le serveur se trouvent dans les différents VRF (client en vert, serveur en rouge dans cet exemple) :

```
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
```

Client dans un VRF et serveur dans la table de routage globale (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
```

Maintenant, une configuration type pour toutes les options est examinée ici.



Le client DHCP se trouve dans le VRF du client et le serveur DHCP dans le VRF par défaut de couche 3

Dans ce cas, Lo0 dans GRT est une source de relais. Le relais DHCP est configuré globalement + pour certaines interfaces.

Par exemple, pour la commande vlan101 « IP DHCP relay source-interface Loopback0 » est manquée, mais il utilise la configuration globale.

```
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
```

Par conséquent, le paquet de relais DHCP est envoyé sur GRT avec la même adresse IP SRC/DST, mais avec différentes sous-options.

Pour 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 a DHCP Discover message. The details are as follows:

- 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: 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: 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
  - 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

- Pour 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

```

Pour Vlan201 (qui est en rouge VRF, pas vert comme les VLAN 101 et 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 capture de paquets a été effectuée sur Spine-01 depuis l'interface vers Leaf-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

```

Le paquet DHCP du coeur est IP sans encapsulation 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...>

```

L'un des grands avantages de cette approche est que vous pouvez utiliser la même adresse IP de relais pour différents VRF de locataire sans fuite de route entre différents VRF et global.

## Le client DHCP et le serveur DHCP se trouvent dans le même VRF locataire

Dans ce cas, il est logique d'avoir l'adresse IP de relais dans le VRF du locataire.

Configuration du commutateur:

```
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
```

Pour 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

```

Pour 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

```

Capture de paquets de l'interface Spine-01 à 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

```

Le paquet DHCP dans le coeur a une encapsulation 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...>

```





```

▶ 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

```

Capture de paquets sur l'interface Spine-01 à 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

```

Dans cet exemple, le paquet du coeur est encapsulé 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...>

```

## Client DHCP dans un serveur VRF et DHCP locataire dans un autre VRF non-VXLAN

Cette affaire est très similaire à la précédente. La principale différence est que les paquets n'ont pas d'encapsulation VXLAN - IP pur ou autre (MPLS/GRE/etc), mais c'est la même chose du point de vue de la configuration.

Dans cet exemple, le client est en rouge VRF et le serveur en vert VRF.

Vous avez deux options :

- Le relais IP se trouve dans la VRF du client et configure les fuites de route, ce qui ajoute de la complexité
- L'IP de relais se trouve dans la VRF du serveur (similaire à ce qui a été fait pour GRT dans le premier cas)

Il est plus simple de choisir la deuxième approche car de nombreux VRF clients sont pris en charge et les fuites de route ne sont pas nécessaires.

Configuration du commutateur:

```

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

```

## Informations connexes

- [RFC 3046](#)

- [RFC 3527](#)
- <https://docs.microsoft.com>
- [Support et documentation techniques - Cisco Systems](#)