

# Configurazione di DHCP in IOS XE EVPN/VXLAN

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazioni](#)

[Configurazione server](#)

[Opzione di configurazione 1 per Win2012 R2 - Unique Relay IP per VNI/SVI per VTEP](#)

[Opzione di configurazione 2 di Win2012 R2 - Corrispondenza con il campo ID circuito agente](#)

[Configurazione di Windows Server 2016](#)

[Server DHCP Linux](#)

[Configurazione degli switch](#)

[Il client DHCP è nel VRF tenant e il server DHCP è nel VRF predefinito di layer 3](#)

[Il client DHCP e il server DHCP si trovano nello stesso VRF tenant](#)

[Client DHCP in un VRF tenant e server DHCP in un altro VRF tenant](#)

[Client DHCP in un VRF tenant e server DHCP in un altro VRF non VXLAN](#)

[Informazioni correlate](#)

## Introduzione

In questo documento viene descritta la configurazione del protocollo DHCP (Dynamic Host Configuration Protocol) per la VXLAN (Virtual Extensible LAN) Ethernet VPN (EVPN) in diversi scenari e gli aspetti specifici per i server DHCP Win2012 e Win2016.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza di VPN/VXLAN e DHCP.

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

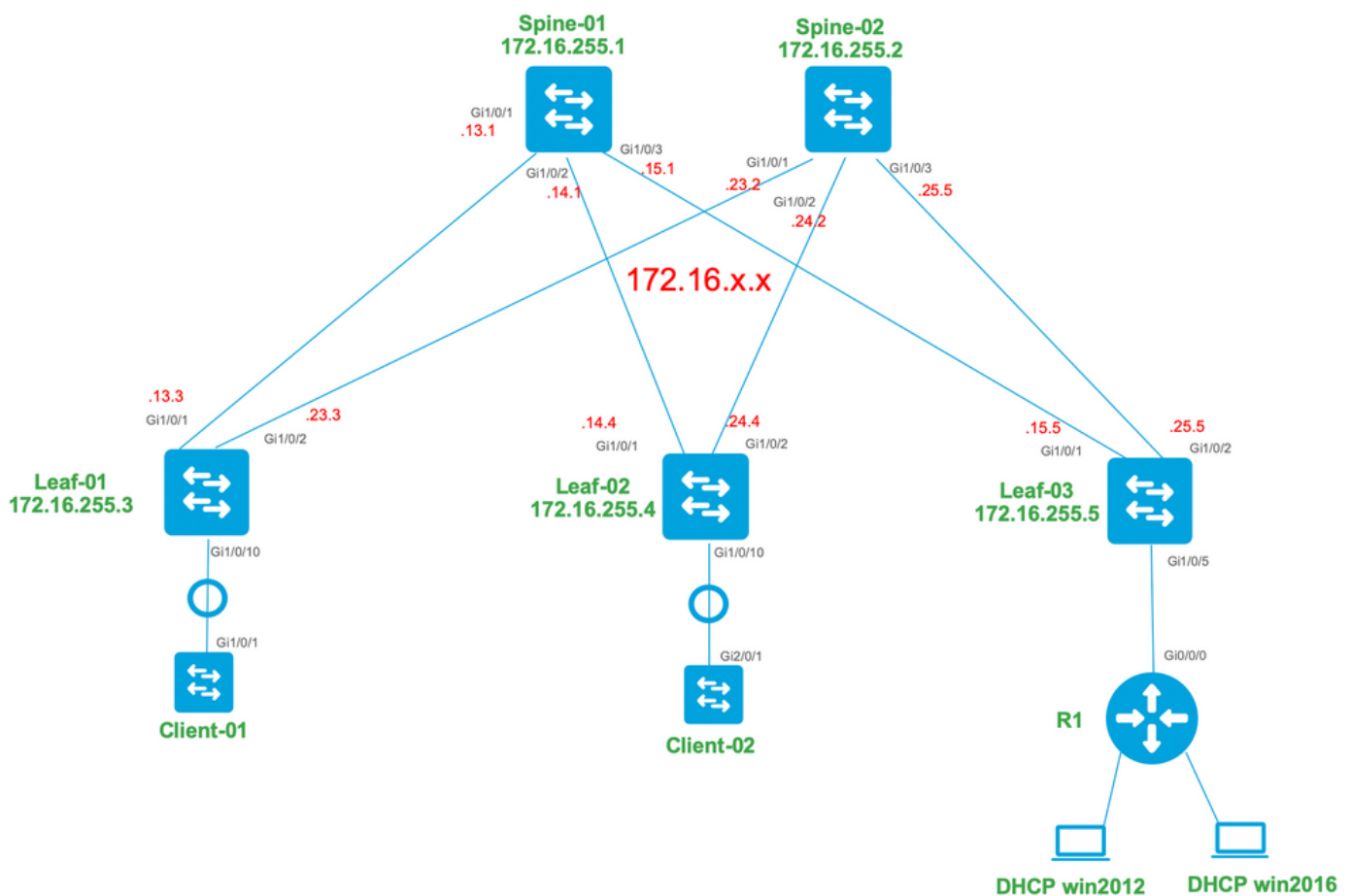
- C9300
- C9400
- C9500

- C9600
- MSFT Windows Server 2012 R2
- MSFT Windows Server 2016
- Funzioni disponibili su Cisco IOS XE 16.9.x o versioni successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

## Configurazione

### Esempio di rete

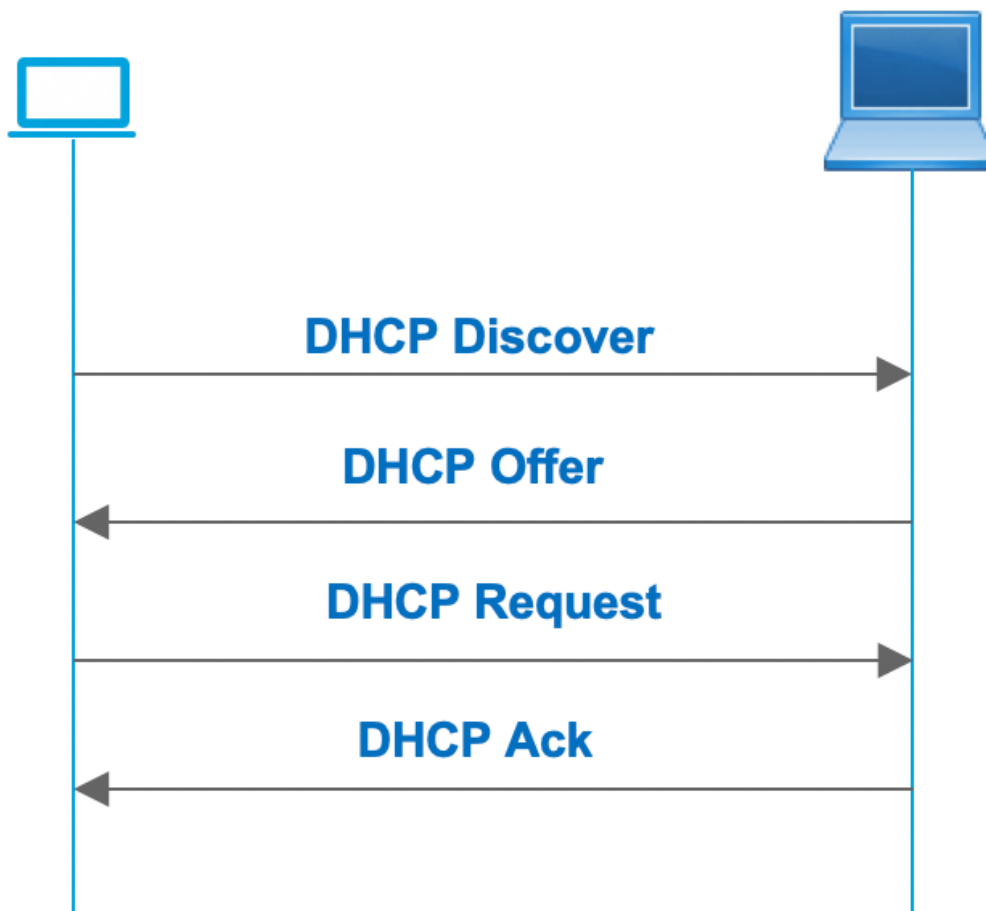


## Configurazioni

Esaminiamo ora il flusso dei messaggi tra il client DHCP e il server. Sono previste 4 fasi:

# DHCP client

# DHCP server



Questa procedura è valida nei casi in cui il client e il server si trovano nella stessa subnet, ma in genere non è così. Nella maggior parte dei casi, il server DHCP non si trova nella stessa subnet del client e deve essere raggiungibile tramite un percorso di routing di layer 3 rispetto al layer 2. In questo caso, è necessaria la funzionalità di inoltra DHCP. La funzionalità di inoltra DHCP (switch o router) converte la trasmissione in un unicast incapsulato da UDP che può essere instradato e inviato al server DHCP. Attualmente è una configurazione molto utilizzata nelle reti.

Problemi con DHCP e VPN/VXLAN Fabric:

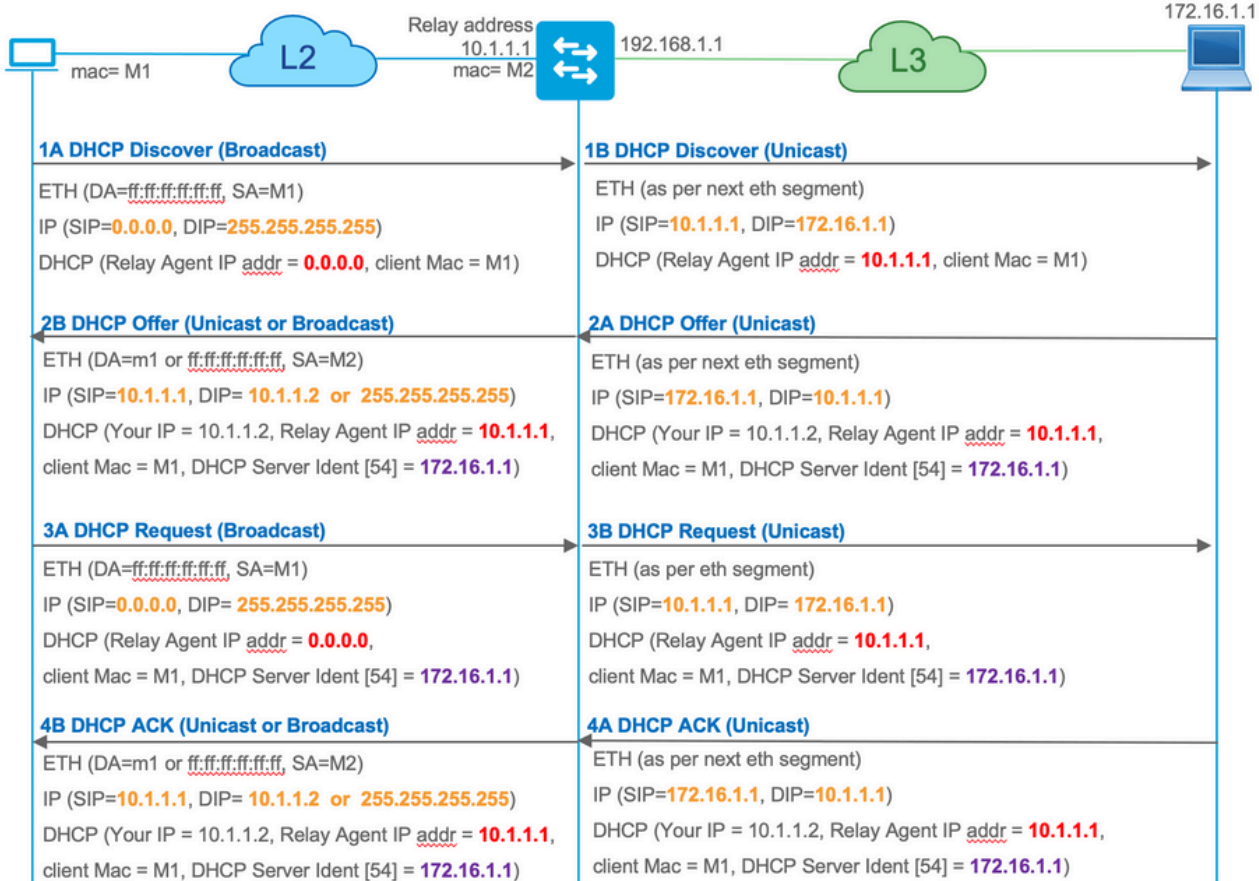
In genere, il server DHCP è connesso all'infrastruttura EVPN tramite la rete L3. Ciò significa che è necessario utilizzare la funzionalità di inoltra DHCP per convertire un pacchetto di trasmissione DHCP di livello 2 in un pacchetto indirizzabile unicast di livello 3.

Con la funzione di inoltra DHCP, il flusso di chiamate DHCP tra client, inoltra e server funziona in modo simile al seguente:

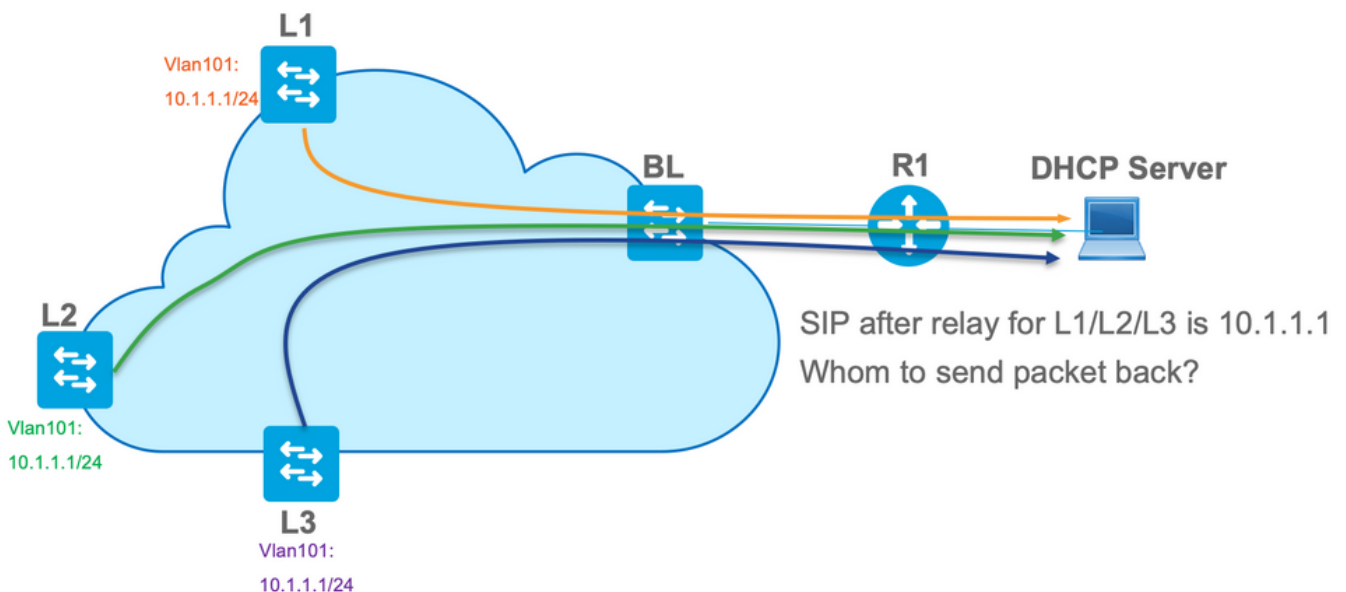
DHCP client

DHCP relay

DHCP server



Dopo l'inoltro, l'IP di origine del pacchetto è l'IP di inoltro. Tuttavia, ciò crea un problema nell'implementazione di VXLAN/EVPN poiché l'IP di origine abituale non è univoco a causa dell'uso di DAG (Distributed Anycast GW). Poiché tutti gli IP di origine VTEP SVI sono uguali, i pacchetti Reply dal server DHCP possono essere inoltrati alla foglia più vicina.



Per risolvere il problema dell'origine non univoca, è necessario essere in grado di utilizzare un indirizzo IP univoco per i pacchetti DHCP inoltrati per foglia. Un altro problema riguarda la sostituzione di GIADDR. Sul server DHCP, è necessario scegliere il pool corretto per assegnare l'indirizzo IP. Viene eseguita dal pool, che copre l'indirizzo IP del gateway (giaddr). Per il fabric



EVPN, deve essere un indirizzo IP di SVI, ma dopo il relay, il giaddr viene sostituito con un indirizzo IP di relay che in questo caso è un loopback univoco.

Come è possibile informare il server DHCP sui pool da utilizzare?

Per risolvere questo problema, viene utilizzata l'opzione 82. Principalmente, queste sono le opzioni secondarie importanti:

- 1 - **ID circuito agente**. Nel caso di VXLAN/EVPN, questa opzione secondaria trasferisce l'ID VNI
- 5 - (o 150 per cisco proprietaria). Le opzioni secondarie di **selezione collegamento** che hanno una subnet effettiva da cui proviene il pacchetto DHCP
- 11 - (o 152 per cisco proprietaria ). L'opzione secondaria **Server Identifier Override** che ha l'indirizzo del server DHCP
- 151 - **Nome VRF/ID VPN**. Questa opzione secondaria ha nome VRF/ID VPN

In un'acquisizione del pacchetto dal relay DHCP al server DHCP, è possibile visualizzare queste diverse opzioni presenti nel pacchetto DHCP, come mostrato nell'immagine.

No.	delta	ip.id	Time	Source	Destination	Protocol	Length	Info
3	0.000000	0x15a2 (5538)	20:39:04.097953	10.1.251.1	192.168.20.12	DHCP	396	DHCP Discover - Transaction ID 0x19a3
6	0.001455	0x40d7 (16599)	20:39:04.099408	192.168.20.12	10.1.251.1	DHCP	362	DHCP Offer - Transaction ID 0x19a3
7	0.012357	0x15a4 (5540)	20:39:04.111765	10.1.251.1	192.168.20.12	DHCP	414	DHCP Request - Transaction ID 0x19a3
8	0.000500	0x40d8 (16600)	20:39:04.112265	192.168.20.12	10.1.251.1	DHCP	362	DHCP ACK - Transaction ID 0x19a3
10	10.7583...	0x15a6 (5542)	20:39:14.870566	10.1.252.1	192.168.20.12	DHCP	396	DHCP Discover - Transaction ID 0x217c
11	0.000471	0x1747 (5959)	20:39:14.871037	192.168.20.12	10.1.252.1	DHCP	362	DHCP Offer - Transaction ID 0x217c
12	0.020232	0x15a8 (5544)	20:39:14.891269	10.1.252.1	192.168.20.12	DHCP	414	DHCP Request - Transaction ID 0x217c
13	0.000423	0x1748 (5960)	20:39:14.891692	192.168.20.12	10.1.252.1	DHCP	362	DHCP ACK - Transaction ID 0x217c

Relay Agent/Giaddr

Agent Circuit ID (VNI encoded)

Link Selection (pool from which ip address should be assigned)

Server ID override (used for redirecting DHCP renew over relay)

Configurazione degli switch:

- L'opzione 82 contiene tutte le informazioni necessarie per scegliere il pool DHCP corretto e restituire il pacchetto dal server alla foglia corretta.
- Questa procedura funziona solo se il server DHCP è in grado di elaborare le informazioni dell'opzione 82, sebbene non tutti i server le supportino completamente (ad esempio 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

```

## Configurazione server

### Opzione di configurazione 1 per Win2012 R2 - Unique Relay IP per VNI/SVI per VTEP

Il problema principale di win2012 è che l'opzione 82 non è completamente supportata, quindi la sottopopzione "Link selection" (5 o proprietaria di Cisco - 150) non può essere utilizzata per selezionare il pool corretto sul server DHCP.

Per risolvere questo problema, è possibile utilizzare questo approccio:

- È necessario creare un ambito per gli indirizzi IP RELAY. In caso contrario, DHCP non troverà un pool corrispondente a DHCP GIADDR e ignorerà il pacchetto. L'intervallo IP completo deve essere escluso da DHCP per impedire l'allocazione dal pool di indirizzi IP RELAY. Questo pool viene chiamato RELAY\_POOL
- È necessario creare l'ambito dell'intervallo IP da allocare. Questo pool viene chiamato IP\_POOL
- È necessario creare l'ambito esteso e includere entrambi gli ambiti: RELAY\_POOL e IP\_POOL

Scopri come viene elaborato il pacchetto DHCP sul server.

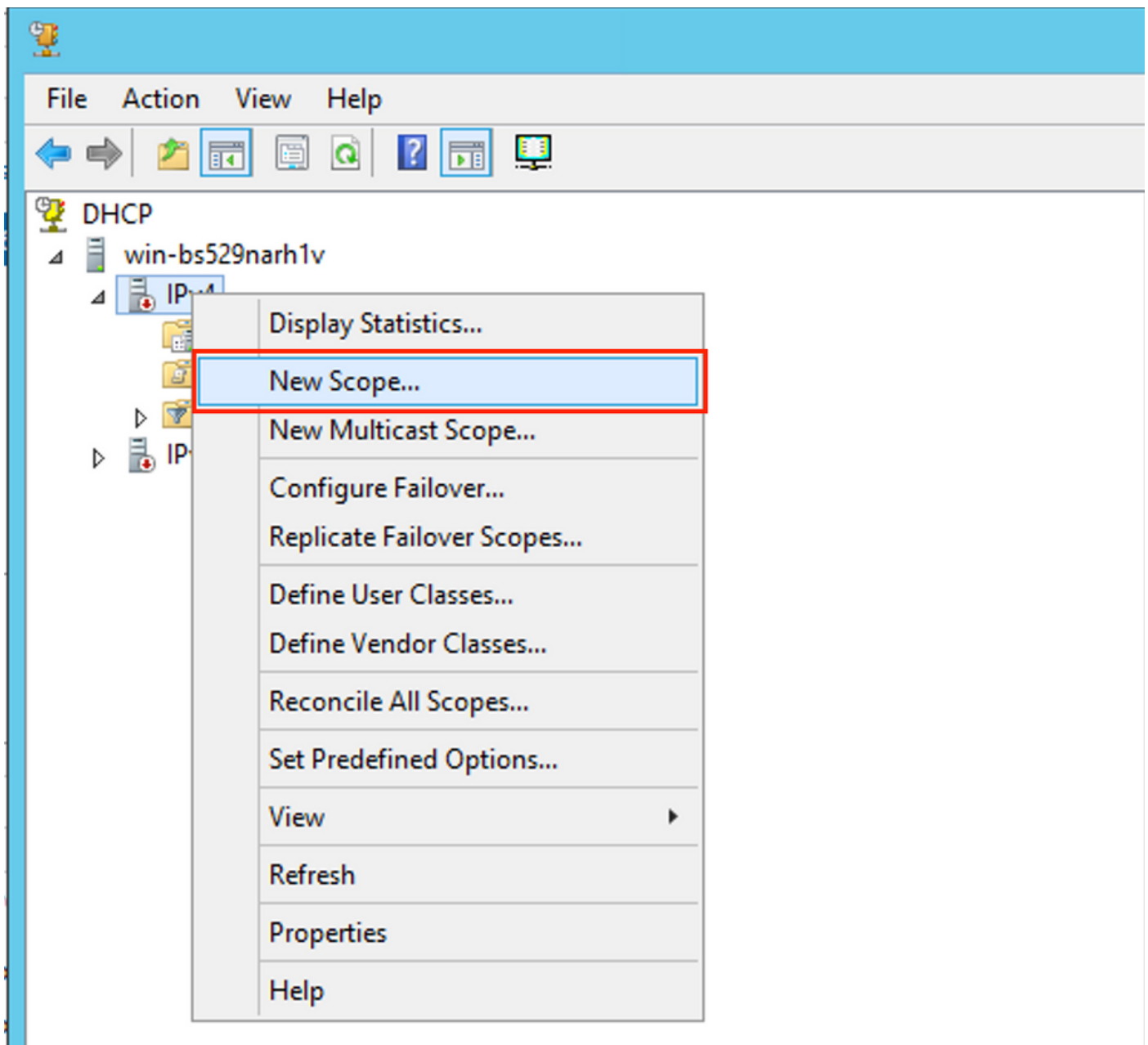
1. Il pacchetto DHCP viene ricevuto dal server.
2. In base a GIADDR, nell'ambito esteso appropriato viene scelto RELAY\_POOL.
3. Poiché in RELAY\_POOL non sono presenti indirizzi IP liberi (si ricorda che l'ambito completo è escluso?), viene eseguito il fallback a IP\_POOL nello stesso ambito esteso.
4. L'indirizzo viene allocato dal superpool corrispondente e rinviato al Relay Server.

Uno dei principali svantaggi di questo metodo è la necessità di disporre di un loopback univoco per VLAN/VNI per VTEP, in quanto il pool DHCP viene selezionato in base all'indirizzo del relay.

Questa opzione consente di utilizzare un ampio intervallo IP per gli indirizzi IP dei relè.

Opzione 1. Istruzioni dettagliate su come configurare win2012 r2.

Creare l'ambito DHCP per gli indirizzi di inoltro. Fare clic con il pulsante destro del mouse e scegliere **Nuovo ambito** come mostrato nell'immagine.



Selezionate **Succ (Next)** come mostrato nell'immagine.

## 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

Immettere un nome e una descrizione significativi, quindi selezionare **Avanti** come illustrato nell'immagine.

## 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:

Immettere le informazioni sull'indirizzo IP del pool di server Relay Server. Nell'esempio, la netmask è /24, ma può essere maggiore o minore (dipende dalle dimensioni della rete), come mostrato nell'immagine.

## 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

Esclude tutti gli intervalli dal pool. È importante, altrimenti è possibile allocare gli indirizzi IP da questo 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

Configurare la durata del lease (per impostazione predefinita è di 8 giorni) come illustrato nell'immagine.

## 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

È possibile configurare i parametri dell'opzione DHCP come DNS/WINS (ignorati in questo esempio).



## 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

Attivate l'ambito come mostrato nell'immagine.

## 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

Complete la configurazione come mostrato nell'immagine.

## 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.

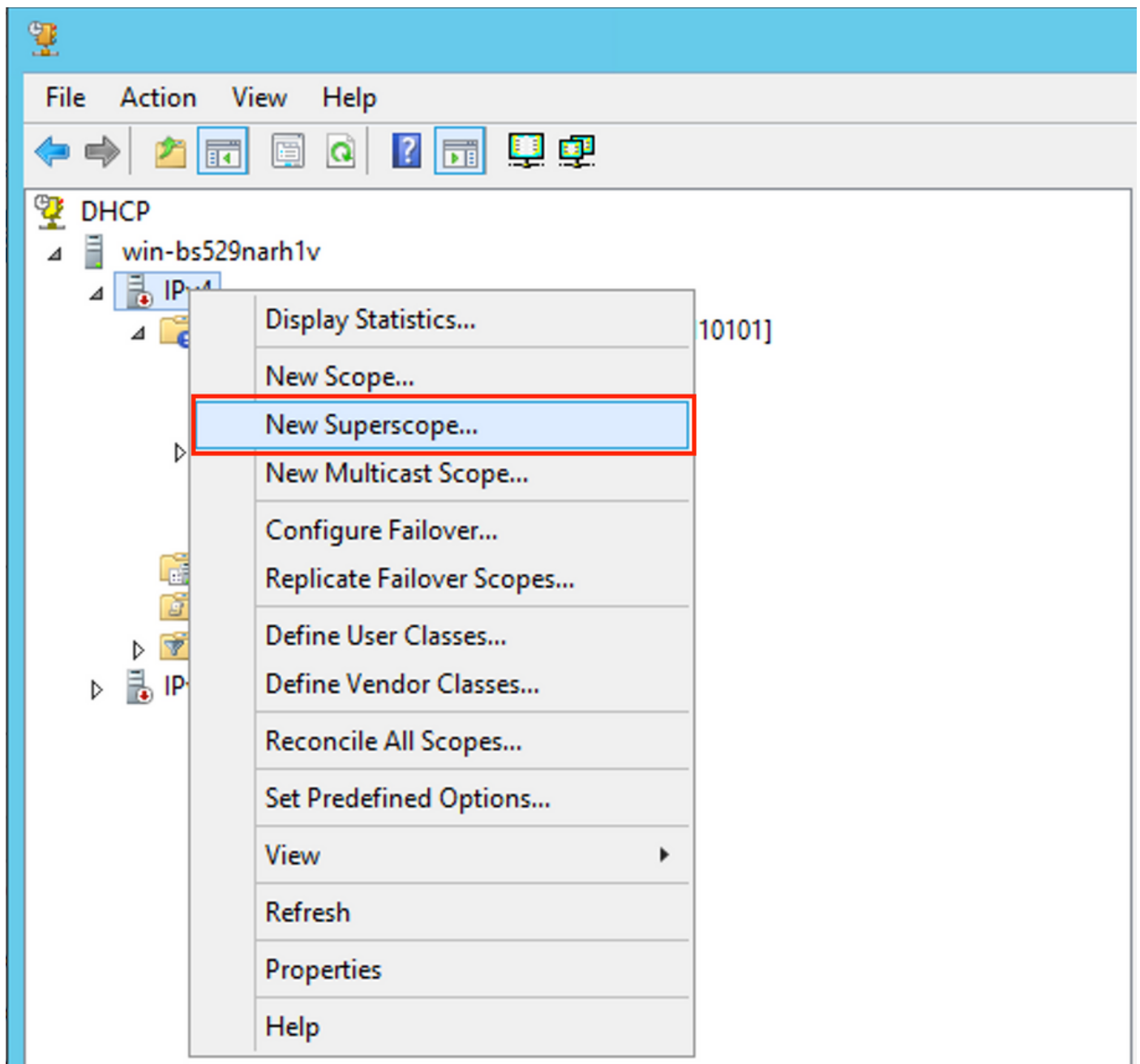
To close this wizard, click Finish.

< Back

Finish

Cancel

Creare un ambito esteso. Fare clic con il pulsante destro del mouse e scegliere **Nuovo ambito esteso** come mostrato nell'immagine.



Selezionare **Next** (Avanti) come mostrato nell'immagine.

## 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

Scegliere un nome significativo per l'**ambito esteso**, come mostrato nell'immagine.

## New Superscope Wizard

### Superscope Name

You have to provide an identifying superscope name.



Name:

< Back

Next >

Cancel

Scegliere l'ambito da aggiungere all'ambito esteso.

## 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]

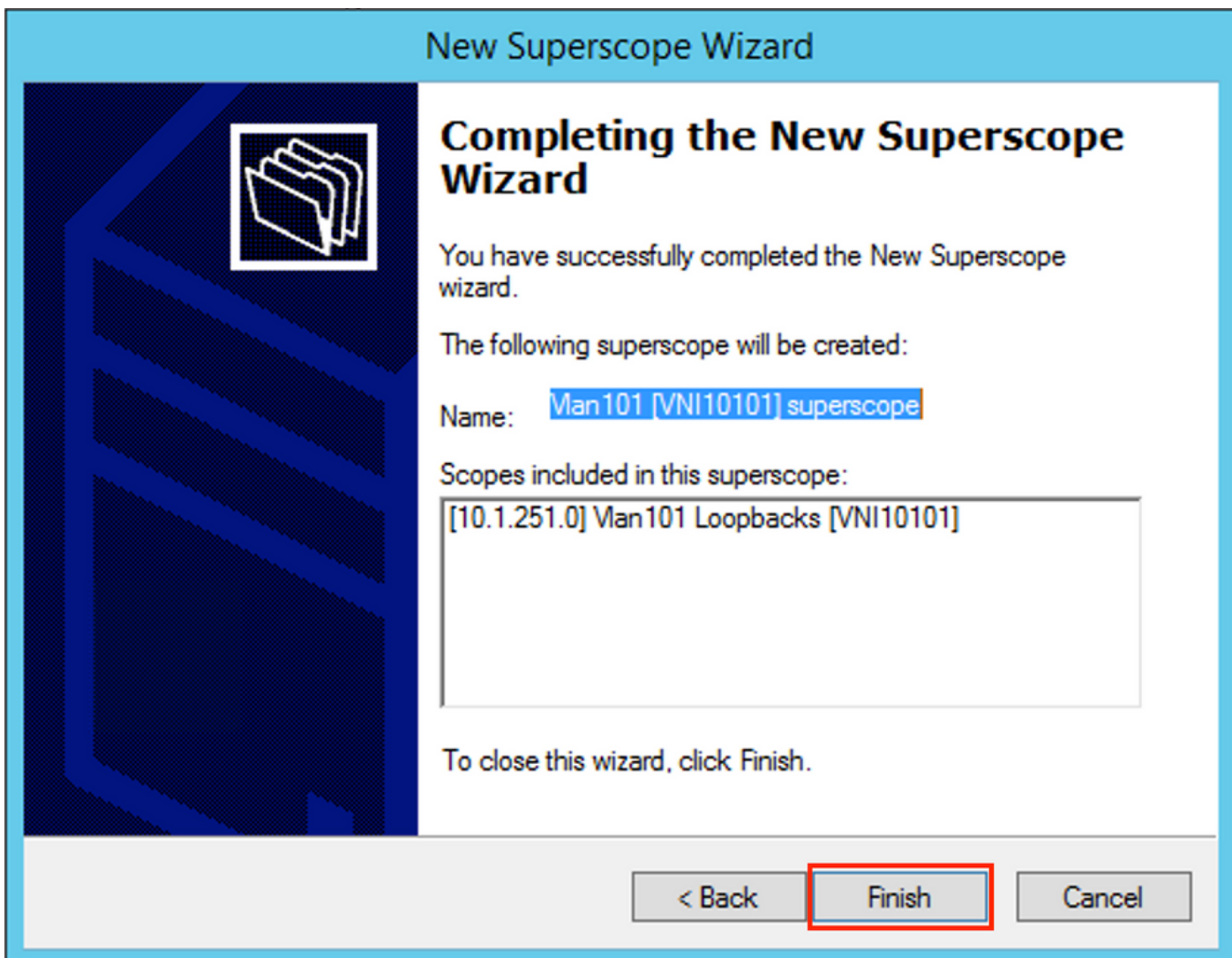
< Back

Next >

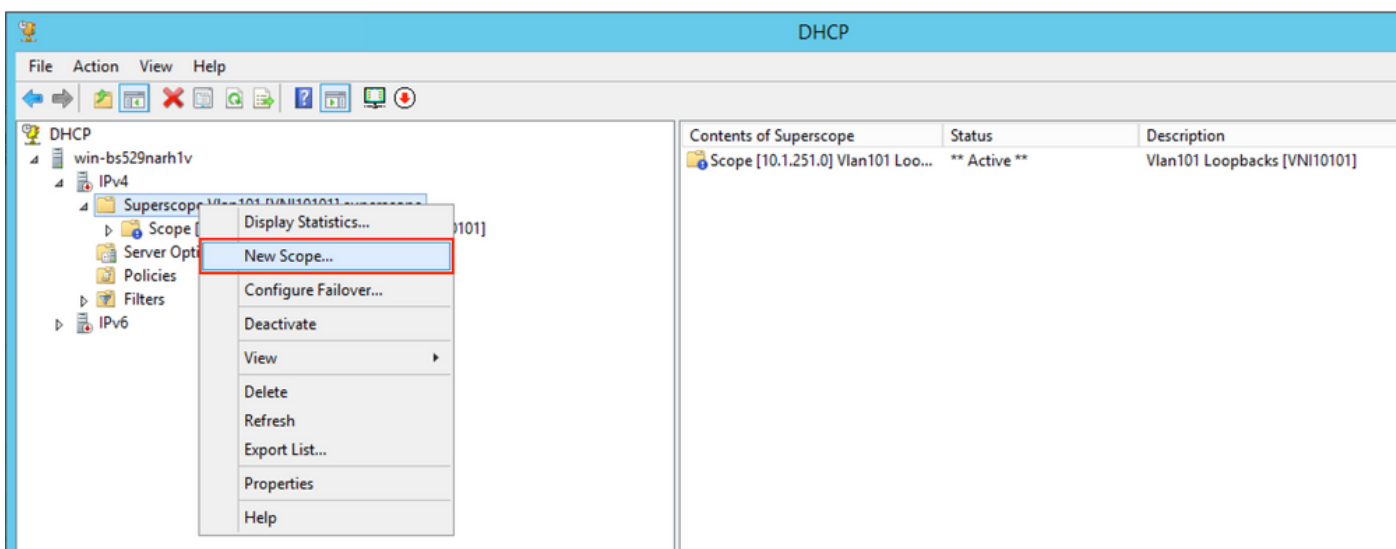
Cancel

Complete l'installazione come mostrato nell'immagine.





Creare un pool DHCP da cui allocare gli indirizzi IP. Fare clic con il pulsante destro del mouse e selezionare **Nuovo ambito...** come mostrato nell'immagine.



Selezionare **Next** (Avanti) come mostrato nell'immagine.



## 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

Scegliere un nome significativo e una descrizione come illustrato nell'immagine.

## 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

Specificare la rete e la maschera per il pool di cui si desidera allocare gli indirizzi IP ai client, come mostrato nell'immagine.

## 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

Escludere l'indirizzo IP del gateway PREDEFINITO dal pool (nell'esempio riportato è 10.1.101.1), come mostrato nell'immagine.

## 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

Specificare il timer di lease come mostrato nell'immagine.

## 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

Facoltativamente è possibile specificare DNS/WINS (ignorato in questo esempio).

## 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

Complete la configurazione come mostrato nell'immagine.



Dopo la creazione del pool, è necessario creare un criterio per il pool.

- Nel criterio l'ID circuito agente [1] corrisponde
- Se si hanno più VLAN/VNI, è necessario creare un superpool con subpool per gli indirizzi IP del relay e l'intervallo IP effettivo per l'allocazione per ciascuna VLAN/VNI
- In questo esempio vengono utilizzati VNI 10101 e 10102

Configurazione degli switch:

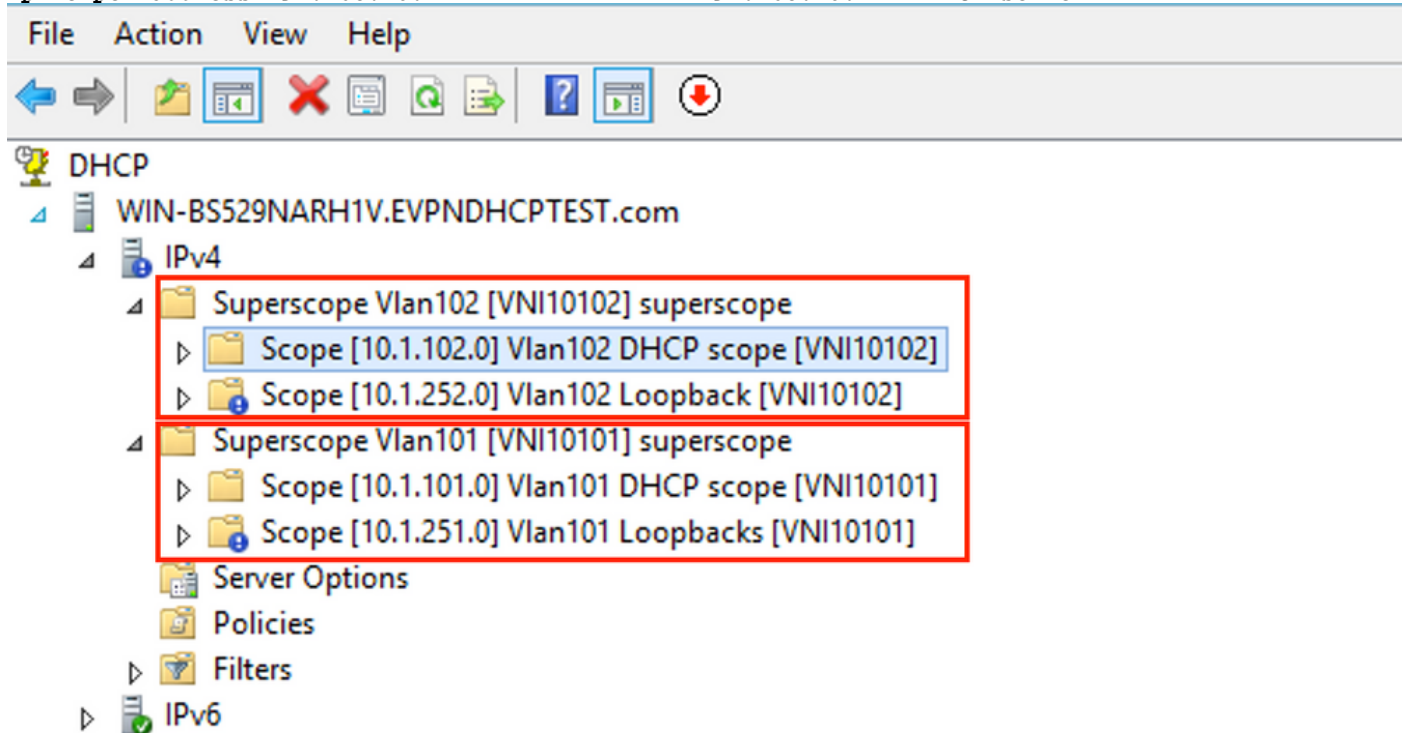
```
ip dhcp relay information option vpn <<< add the VRF name/VPN ID to the option 82
ip dhcp relay information option <<< enables option 82
!
ip dhcp snooping vlan 101-102,201-202
ip dhcp snooping
!
vlan configuration 101
member evpn-instance 101 vni 10101
!
interface Loopback101
 vrf forwarding green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

```

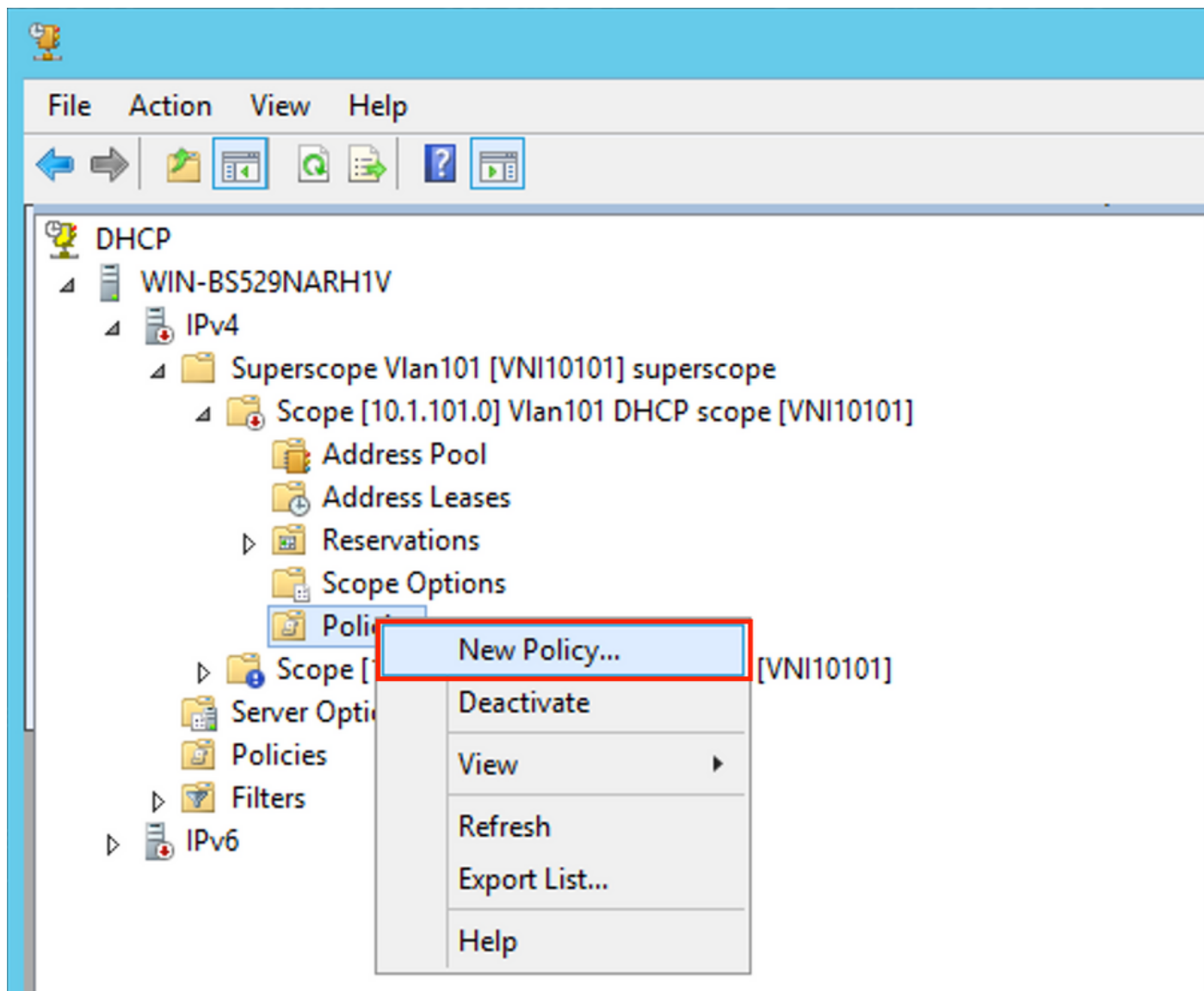


## Opzione di configurazione 2 di Win2012 R2 - Corrispondenza con il campo ID circuito agente

- Lo svantaggio dell'ultimo approccio è l'elevato utilizzo di loopback univoci, quindi un'altra opzione è quella di far corrispondere il campo ID circuito agente.
- I passaggi sono gli stessi, ma è possibile aggiungere la creazione di criteri per la selezione dell'ambito non basati sul campo ID circuito agente anziché su Inoltra IP.

Creazione di criteri. Fare clic con il pulsante destro del mouse sul pool e selezionare **Nuovo criterio**, come mostrato nell'immagine.





Scegliere un nome significativo e una descrizione per il criterio, come illustrato nell'immagine.

## 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


Aggiungete la nuova condizione come mostrato nell'immagine.

## 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

Immettere l'ID del circuito corretto (non dimenticare la casella **Aggiungi carattere jolly (\*)**) come mostrato nell'immagine.

**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(\*)

Chiarimento sul motivo della scelta di questo numero:

In Wireshark, è possibile vedere l'ID del circuito agente uguale a **010a000800002775010a00000**, da cui deriva questo valore (0002775 hex = 10101 decimale è uguale alla VNI 10101 configurata per 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

L'opzione secondaria ID circuito agente è codificata nel seguente formato per la VXLAN VN:


Tipo di opzione secondaria	Lunghezza	Tipo ID circuito	Lunghezza	VNI	mod	port
01	1 byte	0a	1 byte	00	1 byte	1 byte
				08	4 byte	2 byte
				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

Configurare l'intervallo IP da cui vengono allocati gli indirizzi IP. Senza questa configurazione non è possibile allocare l'**ambito corrente**.

## 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

In questa fase è possibile anche selezionare le opzioni DHCP standard, come mostrato nell'immagine.

## 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

Selezionare **Finish** (Fine) come mostrato nell'immagine.



## 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:

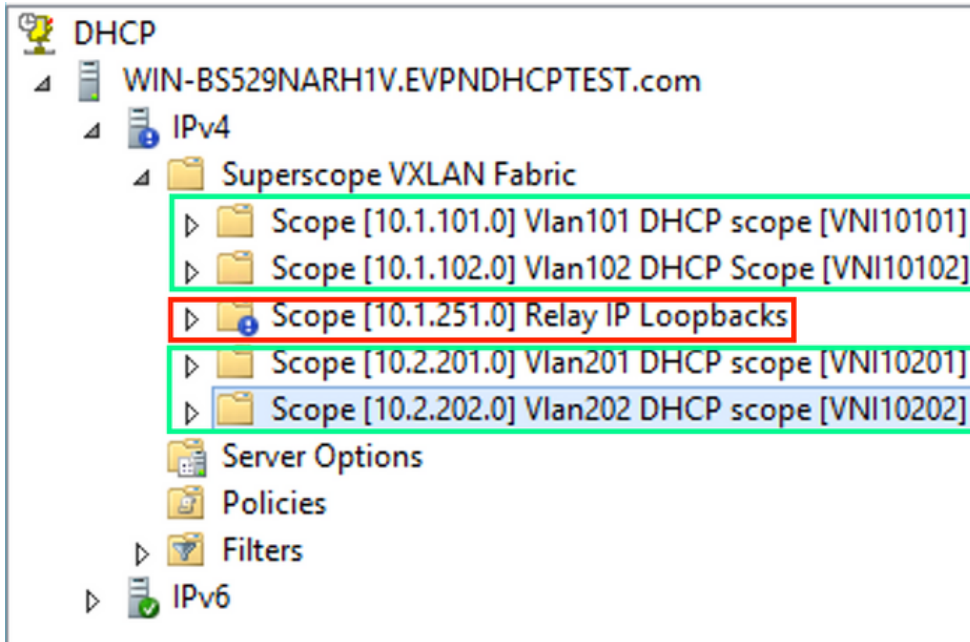
Option Name	Vendor Class	Value
-------------	--------------	-------

< Back

Finish

Cancel

Una configurazione simile deve essere eseguita per altri intervalli, come mostrato nell'immagine.



In questo scenario, è possibile utilizzare un solo indirizzo IP univoco per VTEP per il numero di SVI, non un unico loopback per VNI/SVI per VTEP.

Configurazione degli 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

```

### Configurazione di Windows Server 2016

- Windows Server 2016 supporta l'opzione 82 delle opzioni secondarie 5 (Cisco proprietary 150) "Selezione collegamento", ossia non si utilizza un indirizzo IP di inoltro univoco per la selezione del pool. Viene invece utilizzata l'opzione secondaria "Link selection", che semplifica notevolmente la configurazione.
- È consigliabile disporre ancora di un pool per gli indirizzi IP di inoltro, altrimenti il pacchetto DHCP non corrisponde ad alcun ambito e non viene elaborato.

Nell'esempio viene mostrato come usare l'opzione "link selection".

Avviare il pool di indirizzi IP per gli indirizzi IP Relay come mostrato nell'immagine.

DHCP

File Action View Help



DHCP

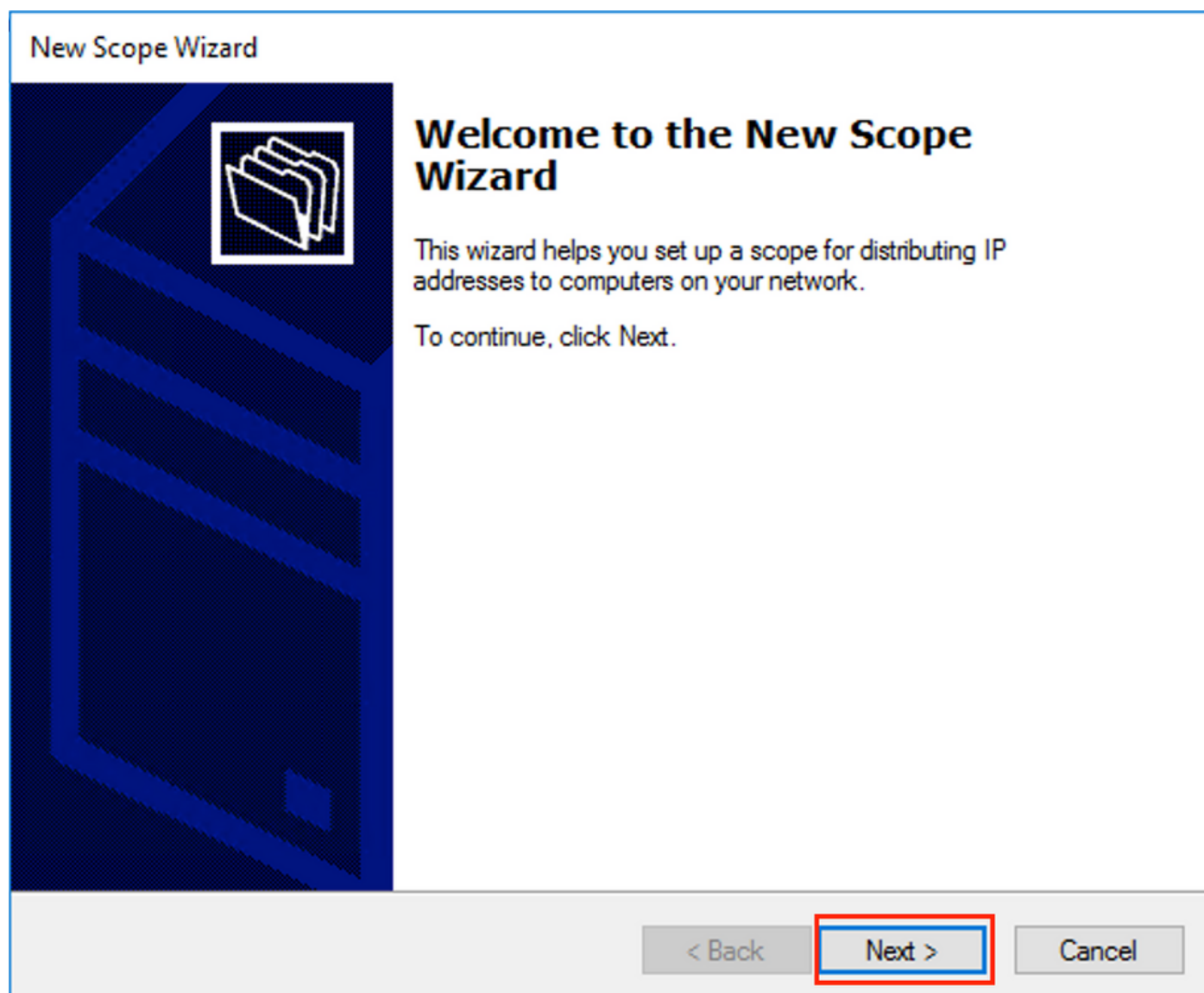
WIN-IC90QQIUTE8.EVPNDHCPTTEST2016.com

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

IP v6

Selezionare **Next** (Avanti) come mostrato nell'immagine.



Scegliere un nome significativo e una descrizione per l'ambito, come illustrato nell'immagine.

## 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

Immettere lo spazio degli indirizzi IP utilizzato per i relè IP, come mostrato nell'immagine.

## 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

Escludere tutti gli intervalli dall'ambito per impedire l'allocazione da questo intervallo, come mostrato nell'immagine.

## 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

È inoltre possibile scegliere l'opzione DNS/WINS e altri parametri (ignorati in questo esempio) come illustrato nell'immagine.



## 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

Selezionare **Finish** (Fine) come mostrato nell'immagine.

## 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.

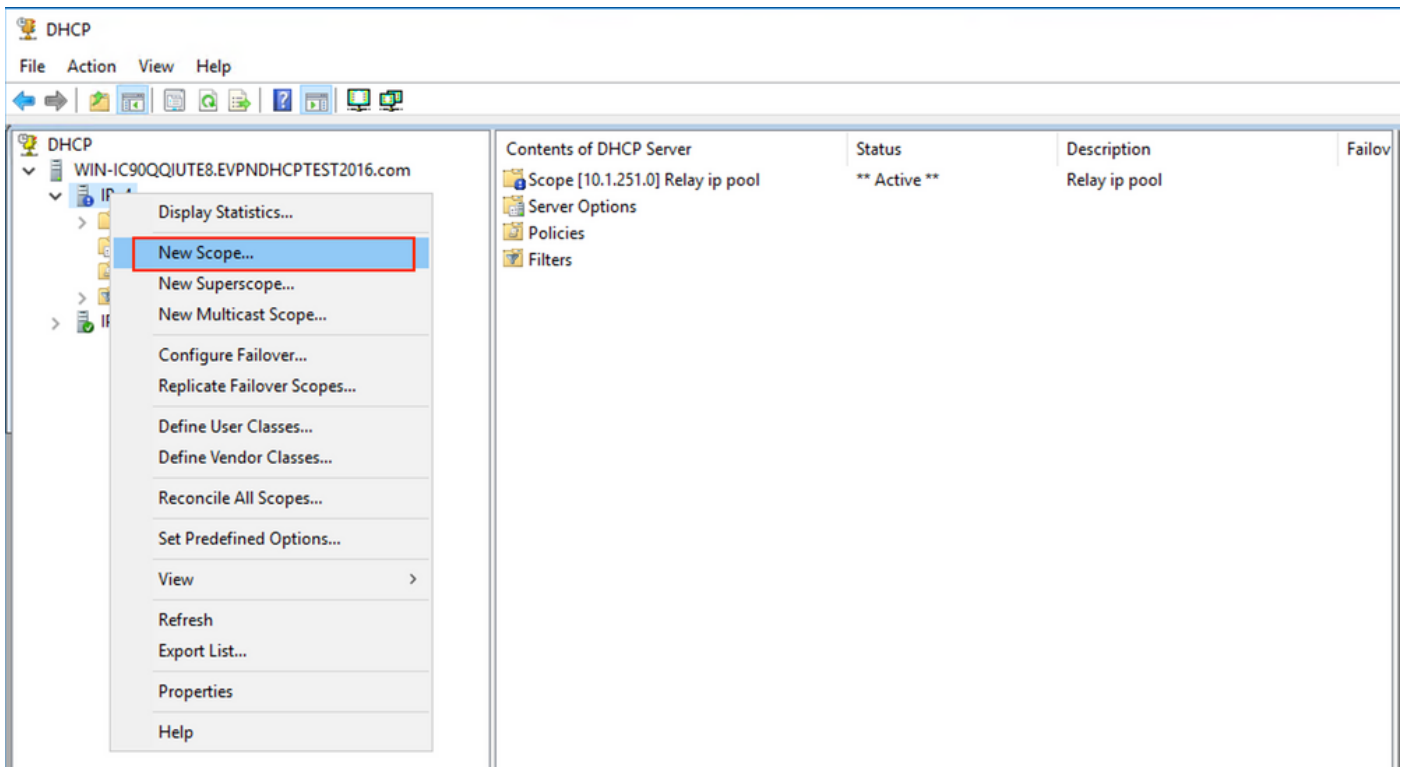
< Back

Finish

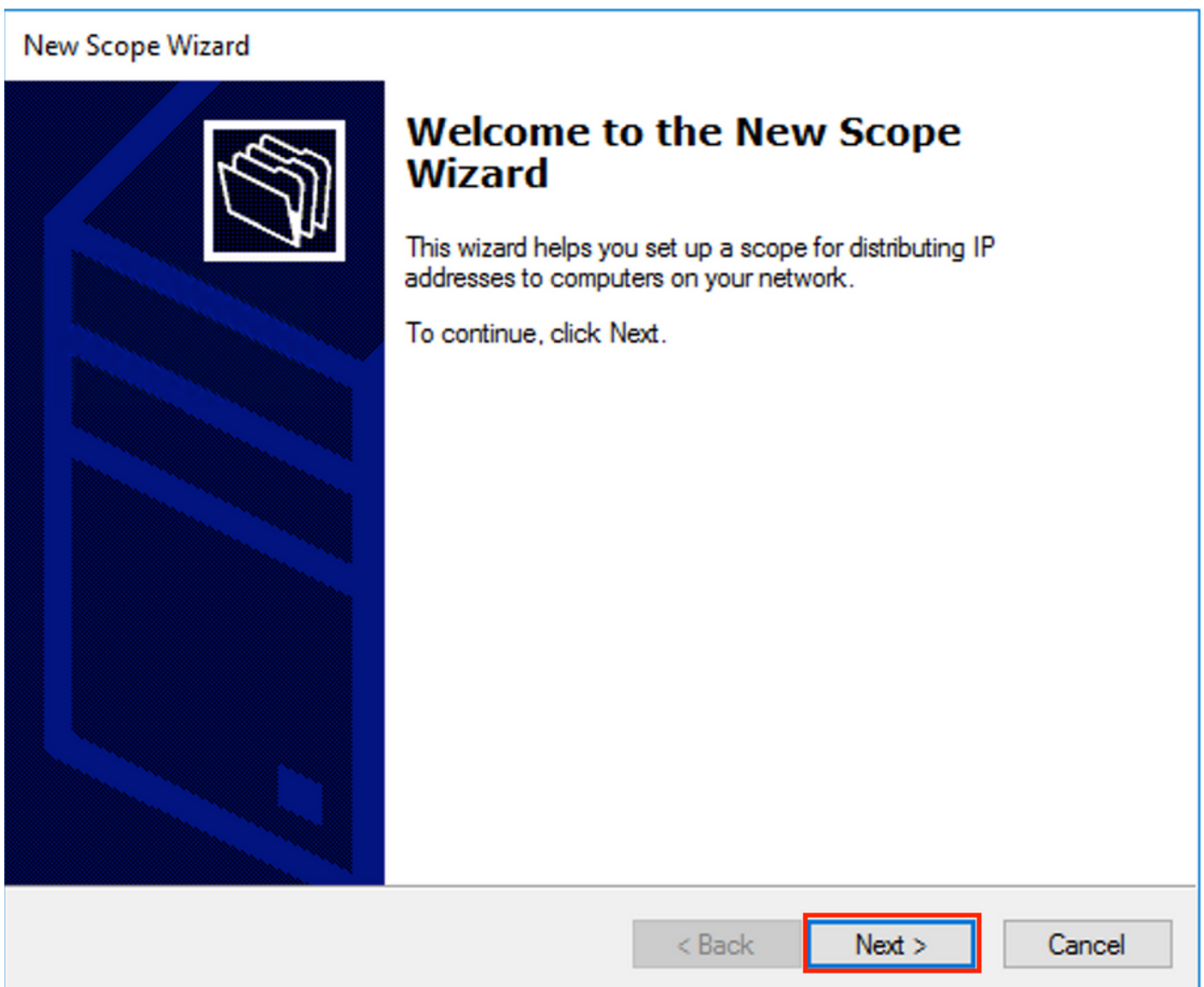
Cancel

L'ambito degli inoltri è pronto.

- Creare quindi il pool da cui i client ottengono gli indirizzi IP.
- Fare clic con il pulsante destro del mouse e scegliere **Nuovo ambito** come mostrato nell'immagine.



Selezionate **Succ (Next)** come mostrato nell'immagine.



Scegliere un nome significativo e una descrizione per il pool, come illustrato nell'immagine.

## 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

Immettere lo spazio degli indirizzi IP da allocare alla vlan101, come mostrato nell'immagine.

## 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

Escludere l'IP del gateway predefinito dall'ambito come mostrato nell'immagine.

## 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

Impostate una Durata lease come mostrato nell'immagine.

## 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

È possibile configurare (ignorare in questo esempio) parametri aggiuntivi quali DNS/WINS e altri, come illustrato nell'immagine.



## 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

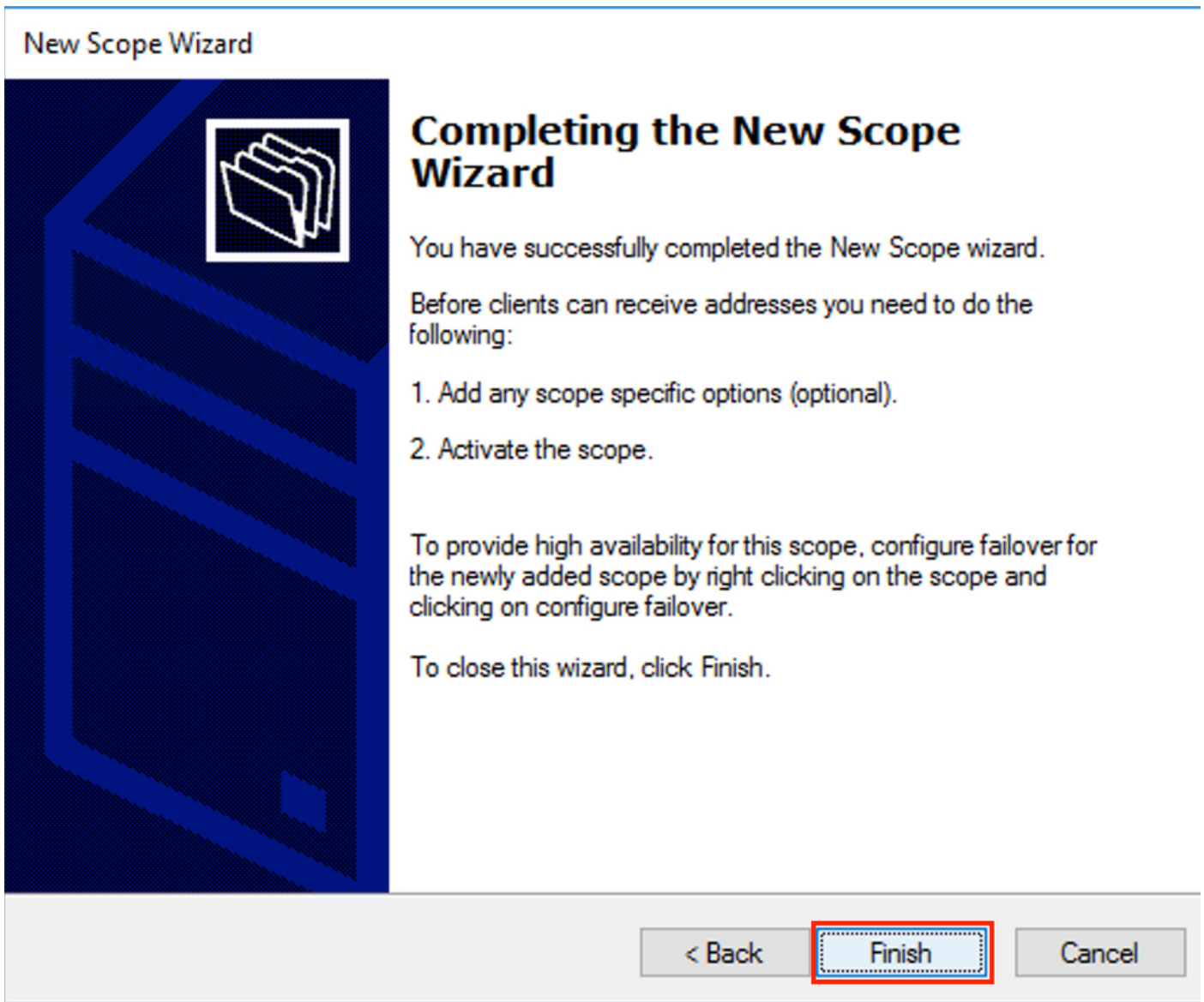
< Back

Next >

Cancel

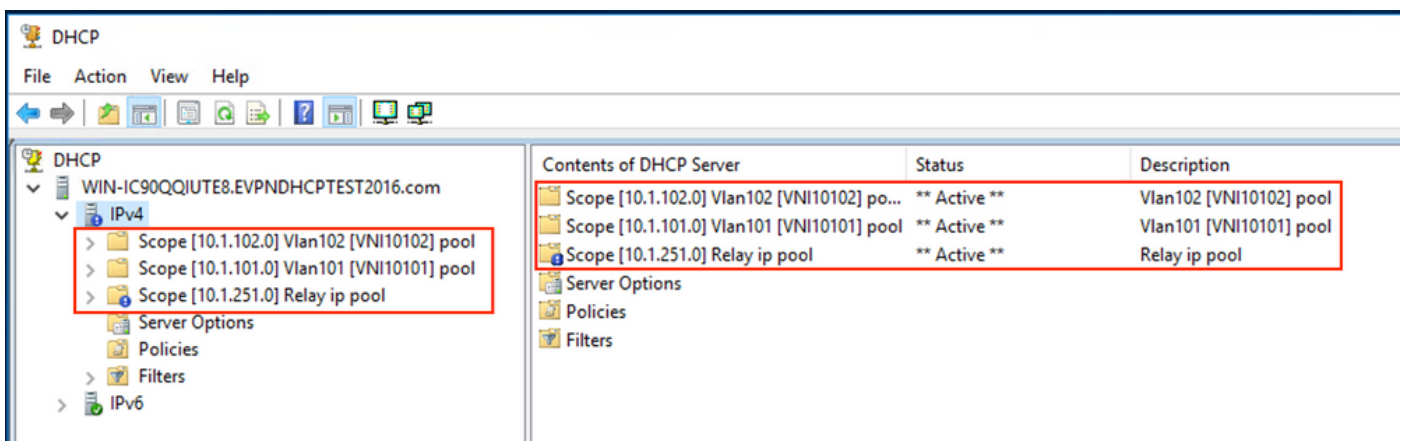
Selezionare **Finish** (Fine) per completare l'impostazione come mostrato nell'immagine.





Il pool per l'indirizzo IP del relay non è configurato e non corrisponde in formato esadecimale. La selezione del pool si basa sull'opzione secondaria **Link selection**.

È possibile aggiungere un nuovo pool e non è necessaria alcuna configurazione aggiuntiva, come mostrato nell'immagine.



## Server DHCP Linux

Esaminare la configurazione del server isc-dhcp su Linux.

- Supporta l'opzione Relay 82. La più importante è l'opzione secondaria di selezione dei collegamenti. È comunque possibile utilizzare le informazioni sull'ID circuito agente e la maschera esadecimale/corrispondenza per il campo specifico (come è stato fatto per win2012). Da un punto di vista pratico, è molto più facile utilizzare 82[5] che lavorare direttamente con le informazioni sull'ID del circuito agente.
- La configurazione dell'opzione secondaria di selezione del collegamento viene eseguita nella definizione della subnet.

In questo esempio, il server ISC viene utilizzato su Ubuntu Linux.

Installare il server DHCP:

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

Per configurare il server DHCP, modificare `/etc/dhcp/dhcpd.conf`. (in un esempio viene utilizzato l'editor Vim)

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

Elemento di cattura configurazione (le configurazioni generali sono omesse):

```

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;
}
```

## Configurazione degli switch

Gli scenari supportati in generale vengono esaminati di seguito.

1. Il client DHCP è nel VRF tenant e il server DHCP è nel VRF predefinito di layer 3
2. Il client DHCP è nel VRF tenant e il server DHCP è nello stesso VRF tenant
3. Il client DHCP è nel VRF tenant e il server DHCP è in un VRF tenant diverso
4. Il client DHCP è nel VRF tenant e il server DHCP è in una VXLAN non predefinita

In uno di questi scenari, è necessario configurare il relay DHCP sul lato switch.

La configurazione DHCP per l'opzione più semplice numero 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]
```

Per impostazione predefinita, le opzioni secondarie dell'opzione 82 **Selezione collegamento e Sostituzione ID server** sono proprietarie di Cisco per impostazione predefinita (rispettivamente 150 e 152).

- ▼ 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)

Se per qualche motivo il server DHCP non **comprende** le opzioni proprietarie Cisco, è possibile modificarlo in uno 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

Lo snooping DHCP deve essere abilitato per le VLAN necessarie.

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

```
ip dhcp snooping
```

È possibile utilizzare la configurazione globale dell'interfaccia di origine dell'inoltro DHCP.

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

In alternativa, è possibile configurarla per interfaccia (la configurazione dell'interfaccia ha la precedenza su quella 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
```

Verificare che esista una connettività IP con indirizzo IP di inoltro in bianco e nero e server DHCP in entrambe le direzioni.

```
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
```

In configurazione interfaccia, viene configurato l'indirizzo del server DHCP. Per questo comando sono disponibili 3 opzioni. Il client e il server si trovano nello stesso 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
```

Il client e il server si trovano in VRF diverse (client in verde, server in rosso in questo esempio):

```
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 in un VRF e server nella tabella di routing 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
```

In questa sezione viene esaminata una configurazione tipica per tutte le opzioni.

**Il client DHCP è nel VRF tenant e il server DHCP è nel VRF predefinito di layer 3**

In questo caso, Lo0 in GRT è una sorgente relè. L'inoltro DHCP è configurato globalmente + per alcune interfacce.

Ad esempio, per il comando `vlan101 "IP DHCP relay source-interface Loopback0"` non è presente, ma viene utilizzata la configurazione 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
```

Di conseguenza, il pacchetto dell'inoltro DHCP viene inviato su GRT con lo stesso IP/DST SRC IP, ma con opzioni secondarie diverse.

Per vlan101:

The screenshot displays a network traffic capture in a tool named 'bootp'. The main window shows a table of captured packets and a detailed view of the selected packet (Frame 1).

No.	delta	ip.id	Time	Source	Destination
1	0.000000	0x8bb7 (35767)	23:09:50.565098	172.16.255.3	192.168.20.20
2	0.000257	0x19a9 (6569)	23:09:50.565355	192.168.20.20	172.16.255.3
3	0.011058	0x8bb0 (35760)	23:09:50.576413	172.16.255.3	192.168.20.20

**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

- Per 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

```

Per la Vlan201 (che è in rosso vrf, non verde come le VLAN 101 e 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

```

L'acquisizione dei pacchetti è stata effettuata sulla Spine-01 dall'interfaccia alla 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

```

Il pacchetto DHCP nel core è IP senza alcun incapsulamento 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...>

```



Un grande vantaggio di questo approccio è che è possibile utilizzare lo stesso indirizzo IP di inoltro per VRF tenant diversi senza perdite di route tra VRF diverse e globali.

## Il client DHCP e il server DHCP si trovano nello stesso VRF tenant

In questo caso, ha senso avere l'indirizzo IP Relay nel VRF tenant.

Configurazione degli 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
```

Per 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

```

Per 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

```

Packet capture dell'interfaccia da 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

```

Il pacchetto DHCP nel core ha un incapsulamento 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

```

Packet capture sull'interfaccia da 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

```

Nell'esempio, il pacchetto nel core è incapsulato in 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 in un VRF tenant e server DHCP in un altro VRF non VXLAN

Questo caso è molto simile all'ultimo. La differenza chiave è che i pacchetti non hanno l'incapsulamento VXLAN - IP puro o qualcos'altro (MPLS/GRE/ecc.), ma è lo stesso dal punto di vista della configurazione.

In questo esempio, il client è in rosso vrf e il server è in verde vrf.

Sono disponibili due opzioni:

- L'indirizzo IP di inoltro si trova nel file vrf del client e configura la perdita di route, aumentando la complessità
- L'indirizzo IP di inoltro si trova nel file vrf del server (come nel primo caso per la tecnologia GRT)

La scelta del secondo approccio è più semplice in quanto vengono supportati molti VFR client e non sono necessarie perdite di percorso.

Configurazione degli 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

```

## Informazioni correlate

- [RFC 3046](#)

- [RFC 3527](#)
- <https://docs.microsoft.com>
- [Documentazione e supporto tecnico – Cisco Systems](#)