

# 在IOS XE EVPN/VXLAN中配置DHCP

## 目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[网络图](#)

[配置](#)

[服务器配置](#)

[Win2012 R2配置选项1 — 每个VNI/SVI每个VTEP的唯一中继IP](#)

[Win2012 R2配置选项2 — 匹配代理电路ID字段](#)

[Windows Server 2016配置](#)

[Linux DHCP 服务器](#)

[交换机配置](#)

[DHCP客户端位于租户VRF中，而DHCP服务器位于第3层默认VRF中](#)

[DHCP客户端和DHCP服务器位于同一租户VRF中](#)

[一个租户VRF中的DHCP客户端和另一个租户VRF中的DHCP服务器](#)

[一个租户VRF中的DHCP客户端和另一个非VXLAN VRF中的DHCP服务器](#)

[相关信息](#)

## 简介

本文档介绍不同场景中的以太网VPN(EVPN)虚拟可扩展LAN(VXLAN)的动态主机配置协议(DHCP)配置，以及Win2012和Win2016 DHCP服务器的特定方面。

## 先决条件

### 要求

Cisco建议您了解EVPN/VXLAN和DHCP。

### 使用的组件

本文档中的信息基于以下软件和硬件版本：

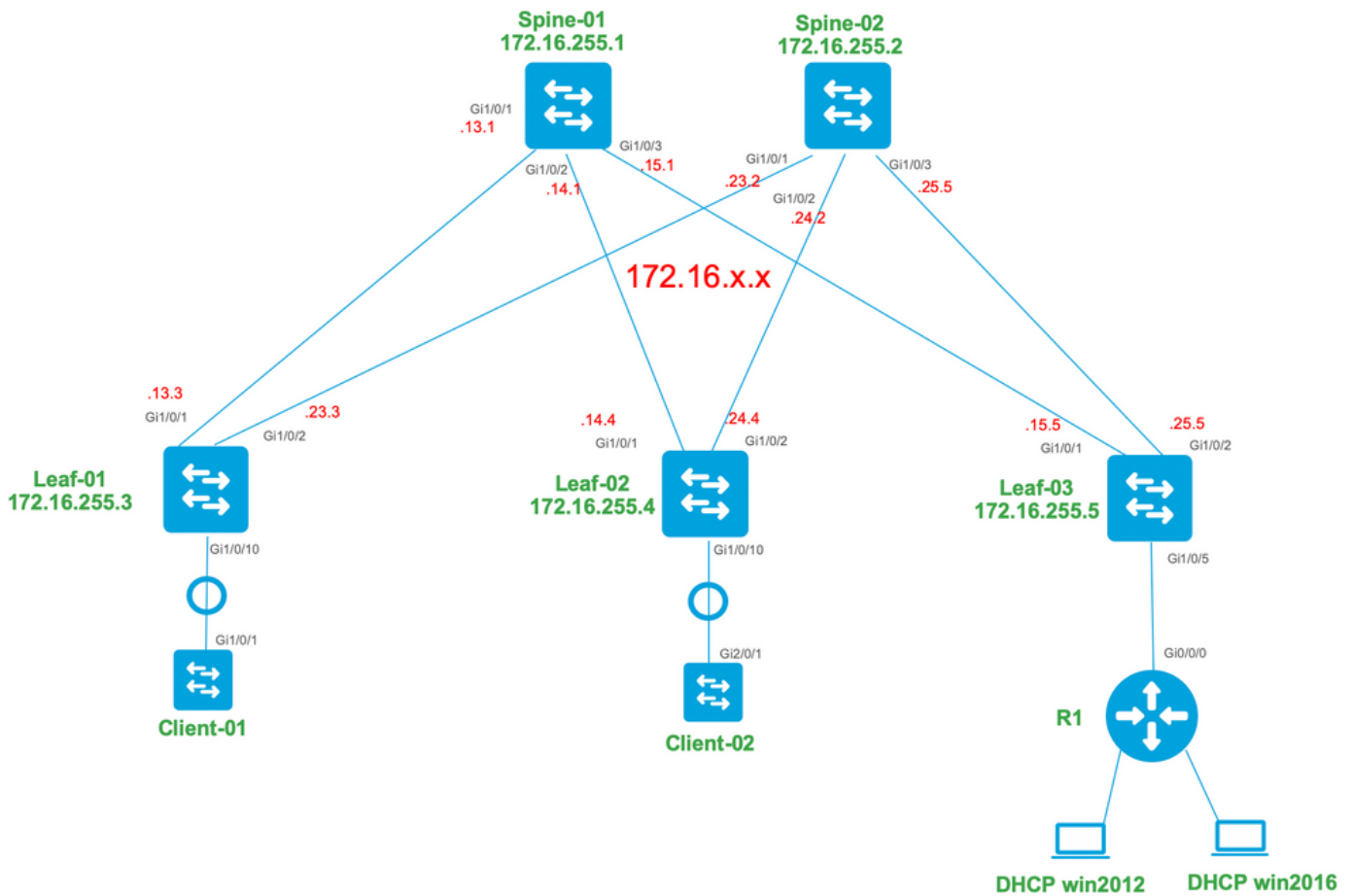
- C9300
- C9400
- C9500
- C9600
- MSFT Windows Server 2012 R2
- MSFT Windows Server 2016

- Cisco IOS XE 16.9.x或更高版本上可用的功能

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

## 配置

### 网络图

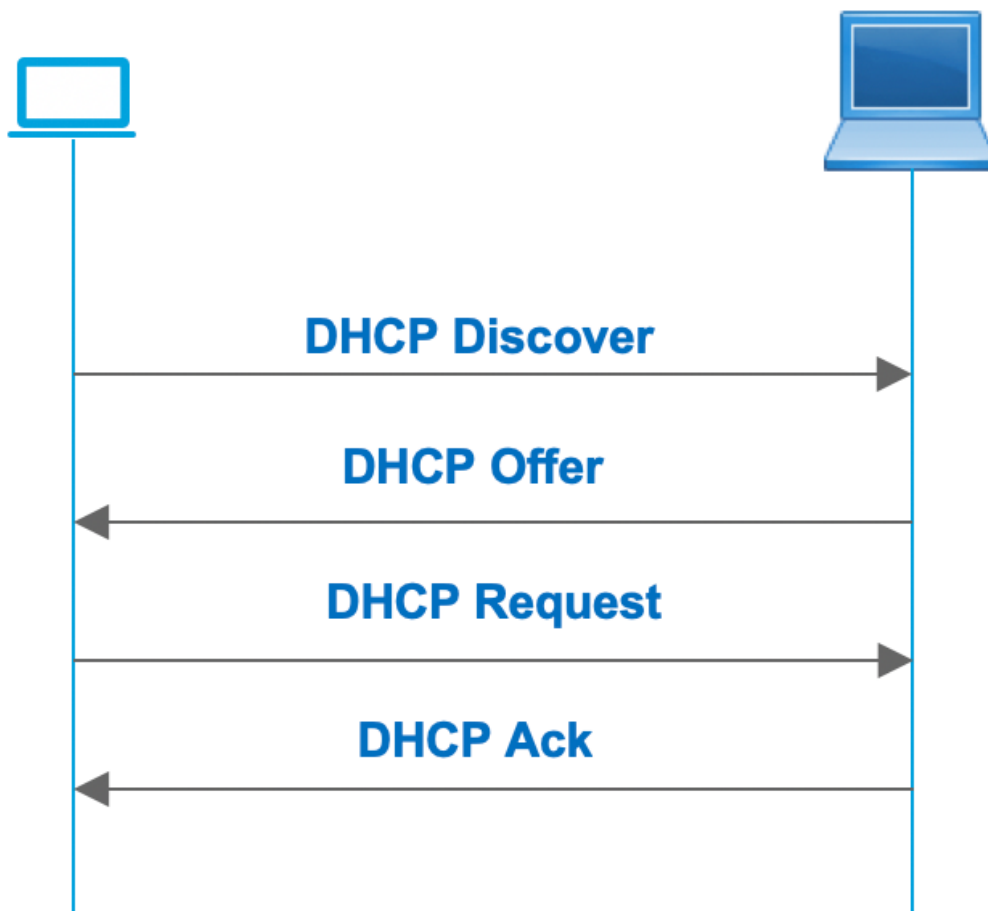


## 配置

现在，让我们复习DHCP客户端和服务端之间的消息流。共有四个阶段：

# DHCP client

# DHCP server



这适用于客户端和服务端位于同一子网的情况，但通常情况并非如此。在大多数情况下，DHCP服务器与客户端不在同一个子网中，并且必须通过第3层路由路径而不是第2层到达。在这种情况下，需要DHCP中继功能。DHCP中继（交换机或路由器）功能将广播转换为可路由的udp封装单播，并将其发送到DHCP服务器。它是当今网络中广泛使用的配置。

DHCP和EVPN/VXLAN交换矩阵的挑战：

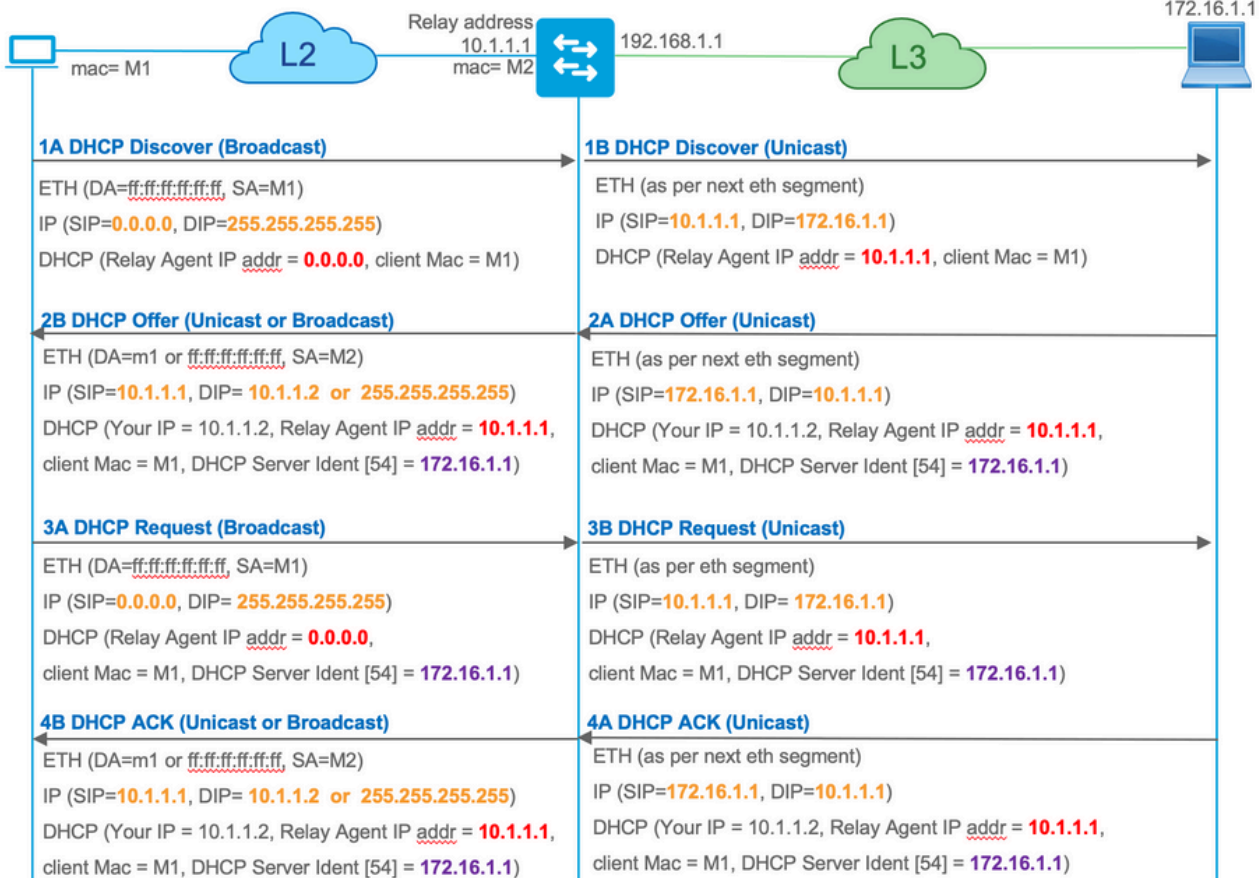
通常，DHCP服务器通过L3网络连接到EVPN交换矩阵。这意味着您必须使用DHCP中继功能将第2层DHCP广播数据包转换为第3层单播可路由数据包。

使用DHCP中继功能时，客户端、中继和服务端之间的DHCP呼叫流的工作方式与以下类似：

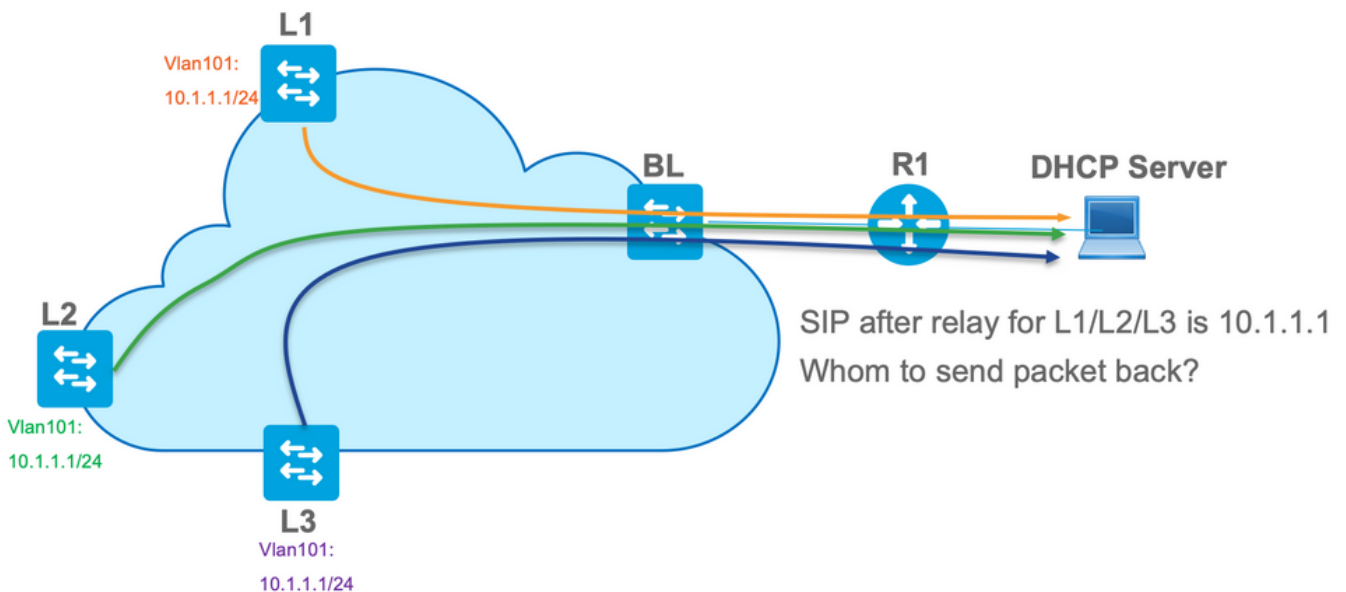
## DHCP client

## DHCP relay

## DHCP server



中继后，数据包的源IP是中介IP。但是，这会在VXLAN/EVPN部署中产生问题，因为由于使用分布式任播GW(DAG)，通常的源IP不是唯一的。由于所有VTEP SVI源IP都相同，这会导致来自DHCP服务器的应答数据包转发到最近的枝叶。



为了解决非唯一源问题，您必须能够为每个枝叶使用唯一IP地址进行中继的DHCP数据包。另一个问题与GIADDR更换有关。在DHCP服务器上，您必须选择正确的池来分配IP地址。它从池中完成，池包含网关IP地址(giaddr)。对于EVPN交换矩阵，它必须是SVI的IP地址，但在中继之后，giaddr会被中介IP地址取代，在本例中，中介IP地址是唯一的环回。



如何通知DHCP服务器，它必须使用哪些池？

为了解决此问题，使用选项82。主要有以下重要的子选项：

- 1 — 座席电路ID。对于VXLAN/EVPN，此子选项传输VNI ID
- 5 — (或150表示思科专有)。具有实际子网的Link selection子选项，DHCP数据包来自该子网
- 11 -(或152 (思科专有)。具有DHCP服务器地址的Server Identifier Override子选项
- 151 - VRF名称/VPN ID。此子选项具有VRF名称/VPN ID

在从DHCP中继到DHCP服务器的数据包捕获中，您可以看到DHCP数据包中的这些不同选项，如图所示。

| 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      |

```
> Ethernet II, Src: a0:b4:39:21:92:3f (a0:b4:39:21:92:3f), Dst: Vmware_a8:0a:e4 (00:50:56:a8:0a:e4)
> Internet Protocol Version 4, Src: 10.1.251.1, Dst: 192.168.20.12
> User Datagram Protocol, Src Port: 67, Dst Port: 67
v Bootstrap Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 1
  Transaction ID: 0x000019a3
  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
  v Option: (82) Agent Information Option
    Length: 44
    v Option 82 Suboption: (1) Agent Circuit ID
      Length: 12
      Agent Circuit ID: 010a000000002775010a0000
    > Option 82 Suboption: (2) Agent Remote ID
    > Option 82 Suboption: (151) VRF name/VPN ID
    v Option 82 Suboption: (150) Link selection (Cisco proprietary)
      Length: 4
      Link selection (Cisco proprietary): 10.1.101.0
    v Option 82 Suboption: (152) Server ID Override (Cisco proprietary)
      Length: 4
      Server ID Override (Cisco proprietary): 10.1.101.1
  > Option: (255) End
```

交换机配置:

- 选项82具有选择正确的DHCP池并将数据包从服务器返回到正确的枝叶所需的所有必要信息。
- 这仅在DHCP服务器可以处理选项82信息时有效，尽管并非所有服务器都完全支持它（例如win2012 r2）。

```
ip dhcp relay information option vpn <<< adds the VRF name/VPN ID to the option 82
ip dhcp relay information remote id <<< 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

```

## 服务器配置

### Win2012 R2配置选项1 — 每个VNI/SVI每个VTEP的唯一中继IP

win2012的主要问题是选项82不完全支持，因此“链路选择”子选项（5或Cisco专有 — 150）不能用于选择DHCP服务器上的正确池。

要解决此类问题，可以使用以下方法：

- 必须创建RELAY IP地址的作用域，否则DHCP找不到与DHCP GIADDR匹配的池并忽略数据包。必须从DHCP中排除完整的IP范围，以防止从中继IP池分配。我们称此池为RELAY\_POOL
- 必须创建要分配的IP范围的范围。我们称此池IP\_POOL
- 必须创建超级作用域，并且必须同时包含两个作用域 — RELAY\_POOL和IP\_POOL

让我们看看如何在服务器上处理DHCP数据包。

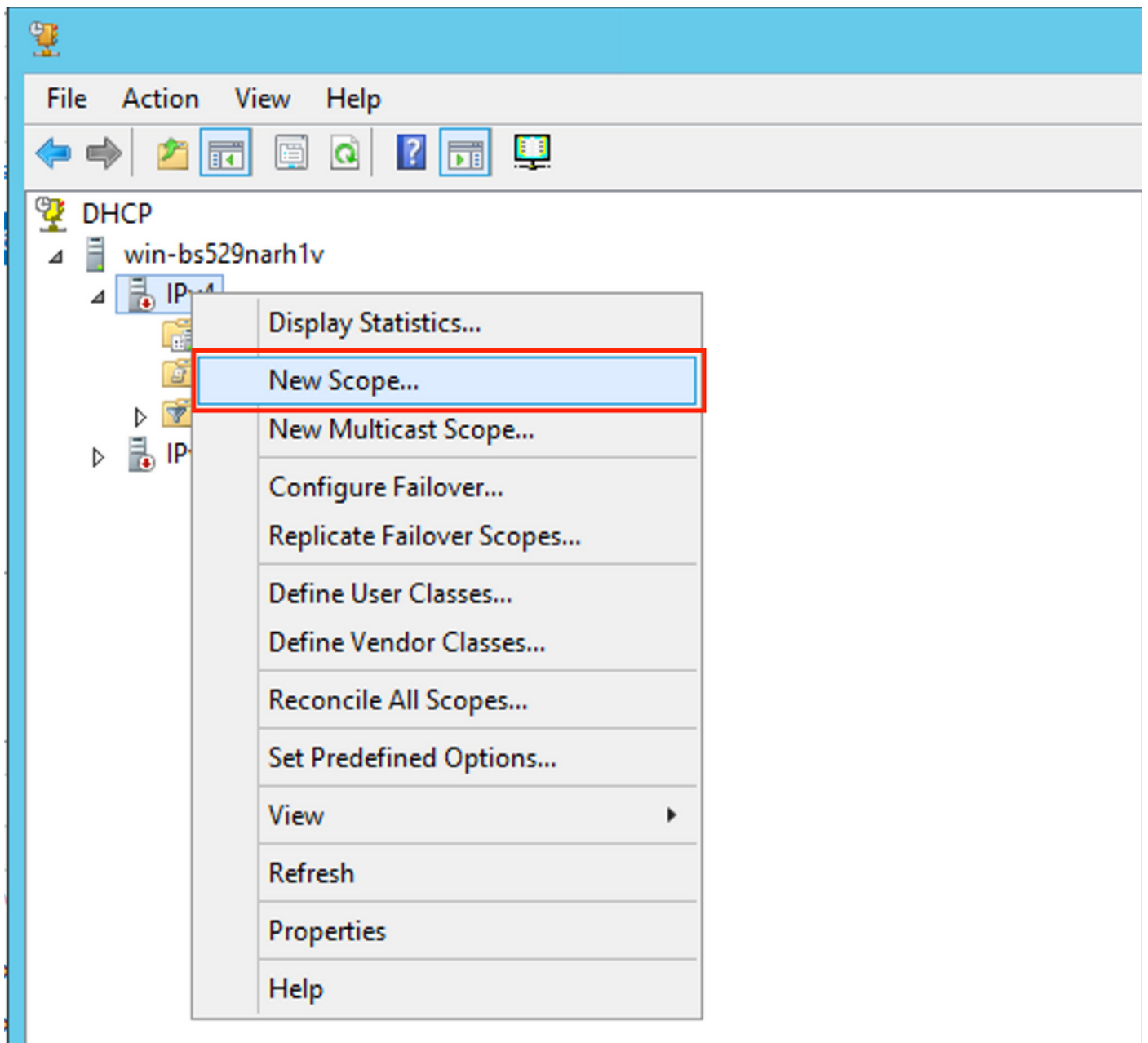
1. 服务器收到DHCP数据包。
2. 基于GIADDR。在适当的超级作用域中选择相应的池RELAY\_POOL。
3. 由于RELAY\_POOL中没有可用的IP地址（是否记得已排除整个范围？），因此它在同一超级作用域中回退到IP\_POOL。
4. 地址从各自的超级池分配，并发送回中继。

此方法的一个重大缺点是，由于根据中继地址选择DHCP池，因此每个VLAN/VNI每个vtep必须具有唯一的环回。

此选项会让我们使用大的IP范围作为中继IP地址。

选项1.有关如何配置win2012 r2的逐步说明。

为中介地址创建DHCP范围。右键单击并选择**New Scope**，如图所示。



选择**Next**，如图所示。

## 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

填写一个有意义的名称、说明，然后选择下一步，如图所示。

## 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

填写中继池的IP地址信息。在本示例中，网络掩码是/24，但可以大于或小于（取决于网络大小），如图所示。

## 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

从池中排除所有范围。这很重要，否则，可以从此池分配IP地址。

## 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

配置租用时间（默认值为8天），如图所示。

## 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

您可以配置DHCP选项参数，如DNS/WINS（在本示例中跳过）。



## 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

激活范围，如图所示。

## 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

如图所示完成配置。

## 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.

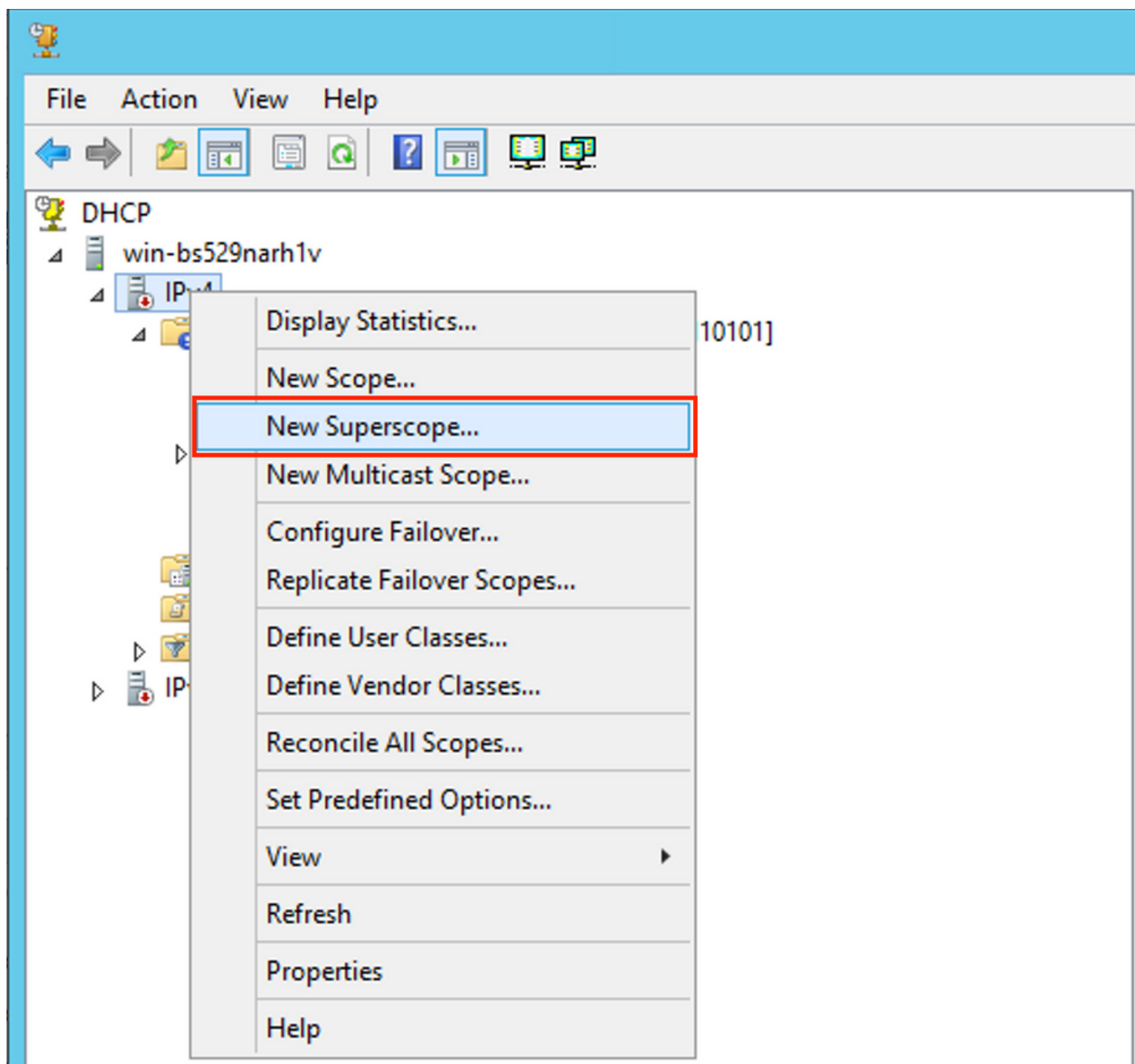
To close this wizard, click Finish.

< Back

Finish

Cancel

现在创建超级作用域。右键单击并选择**新建超级作用域**，如图所示。



选择下一步，如图所示。

## 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

为**超级作用域**选择一个有意义的名称，如图所示。

## New Superscope Wizard

### Superscope Name

You have to provide an identifying superscope name.



Name:

< Back

Next >

Cancel

选择要添加到超级作用域的作用域。

## 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:

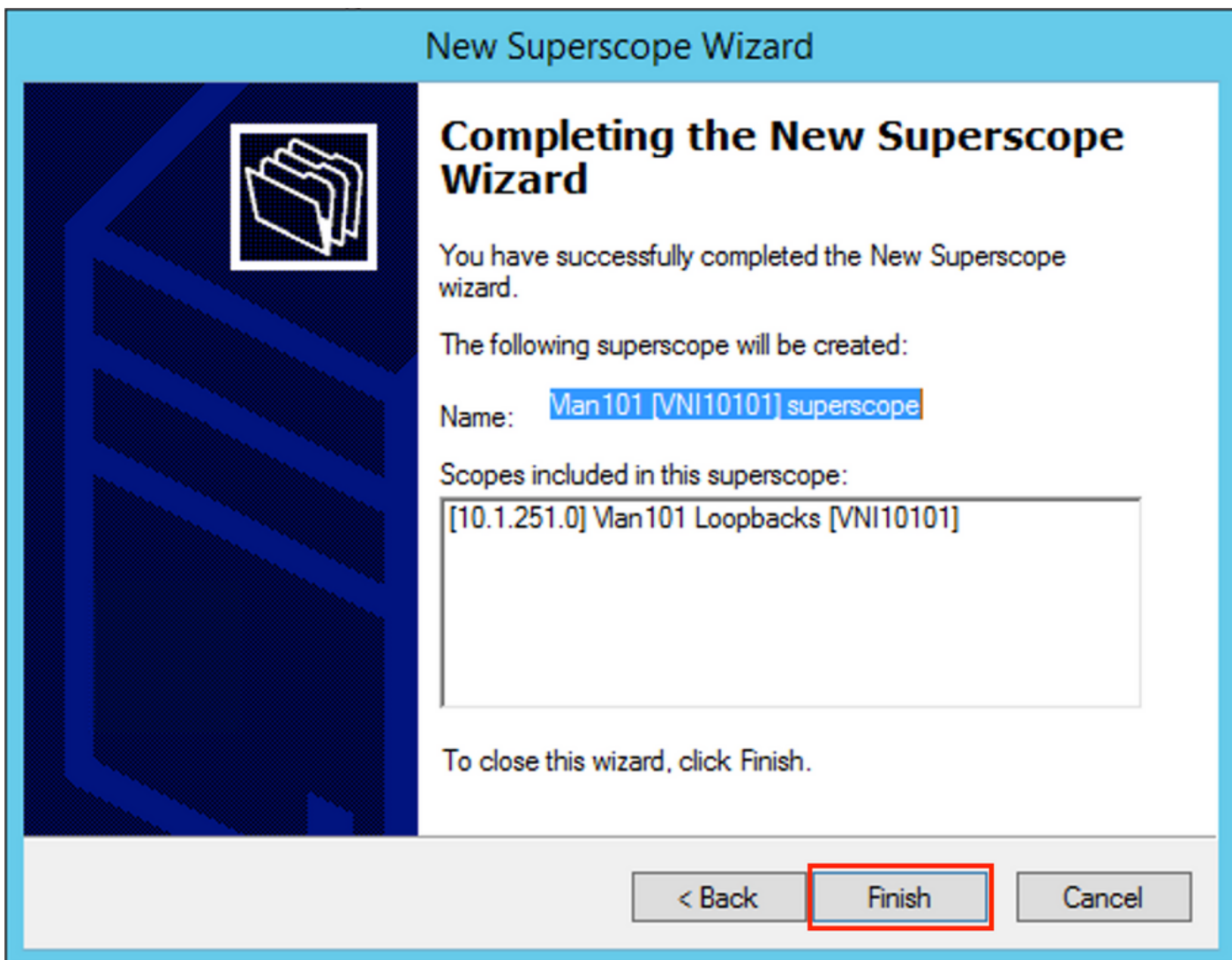
[10.1.251.0] Man101 Loopbacks [VNI10101]

< Back

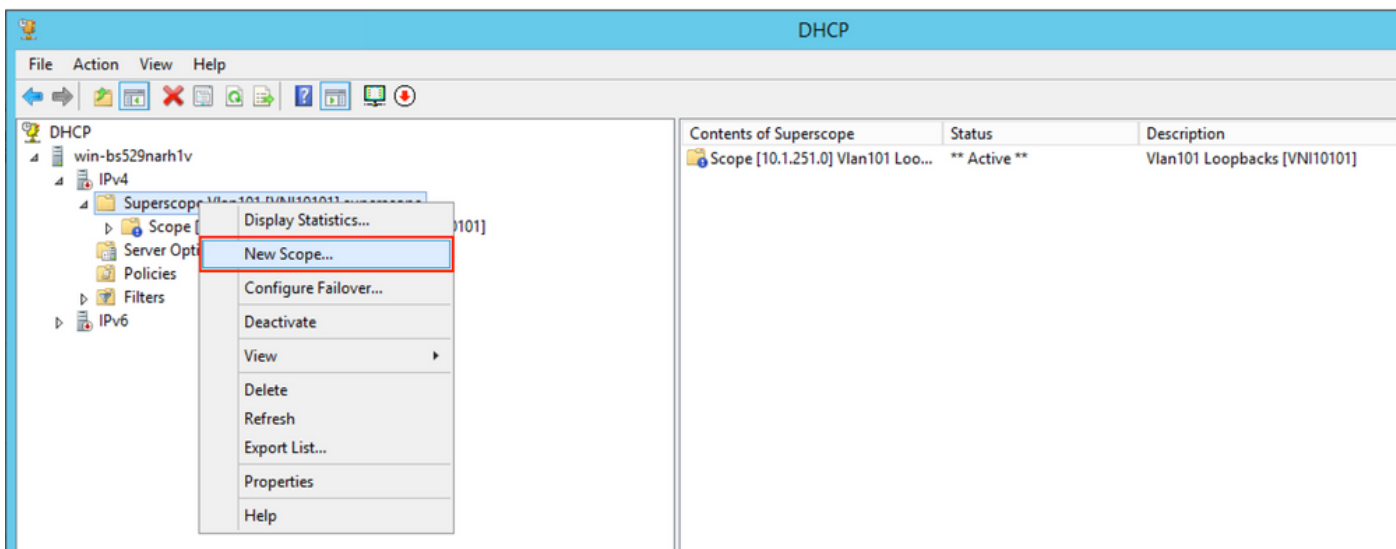
Next >

Cancel

如图所示完成设置。



创建从中分配IP地址的DHCP池。右键单击并选择**新建范围.....** 如图所示。



选择下一步，如图所示。



## 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

选择有意义的名称和说明，如图所示。

## 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

如图所示，为要向其客户端分配IP地址的池指定网络和掩码。

## 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

从池中排除默认网关的IP地址（在本例中为10.1.101.1），如图所示。

## 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

指定租用计时器，如图所示。

## 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

或者，您可以指定DNS/WINS（在本示例中跳过）。

## 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

如图所示完成配置。



创建池后，必须为池创建策略。

- 策略中的代理电路ID [1]匹配
- 如果您有多个Vlan/VNI，则必须创建包含中继IP地址子池和每个VLAN/VNI分配的实际IP范围的超级池
- 本示例使用VNI 10101和10102

交换机配置:

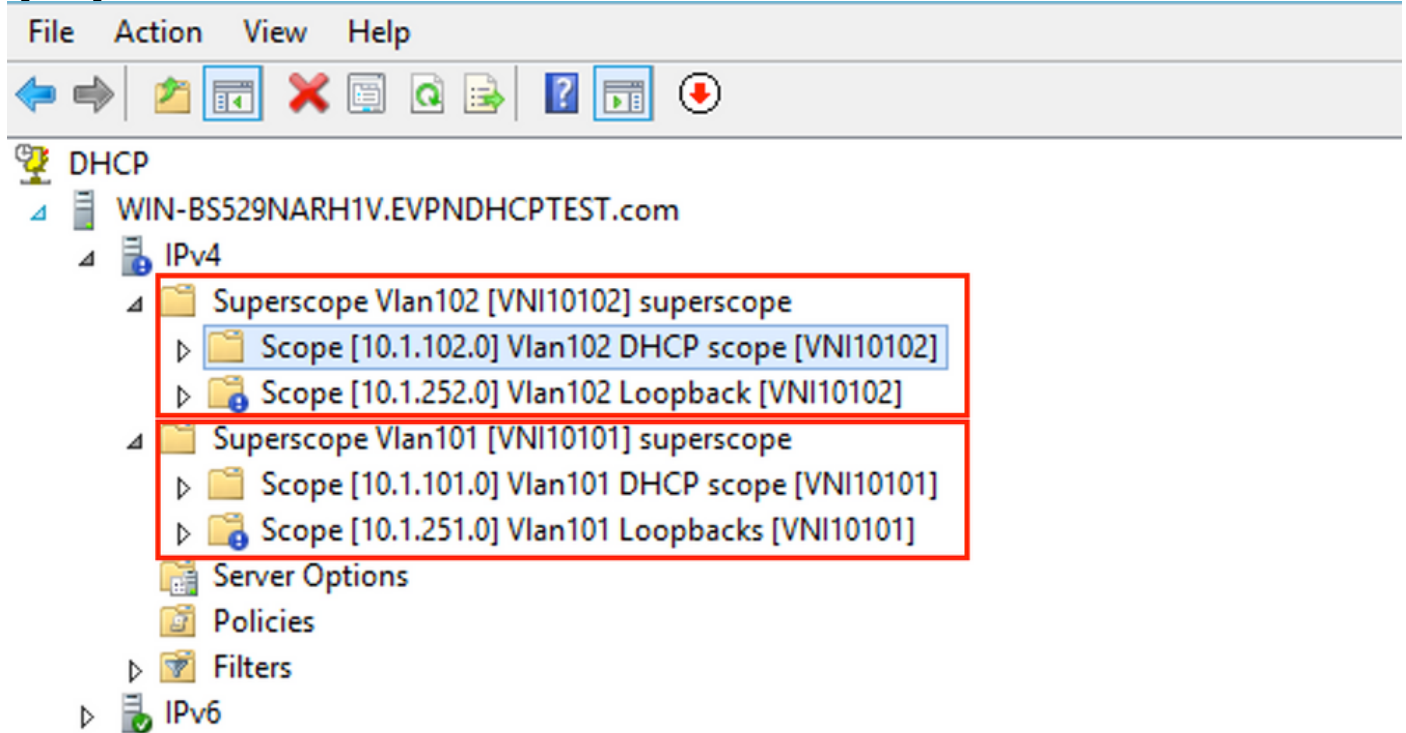
```
ip dhcp relay information option vpn <<< add the VRF name/VPN ID to the option 82
ip dhcp relay information option <<< enables option 82
!
ip dhcp snooping vlan 101-102,201-202
ip dhcp snooping
!
vlan configuration 101
member evpn-instance 101 vni 10101
!
interface Loopback101
 vrf forwarding green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

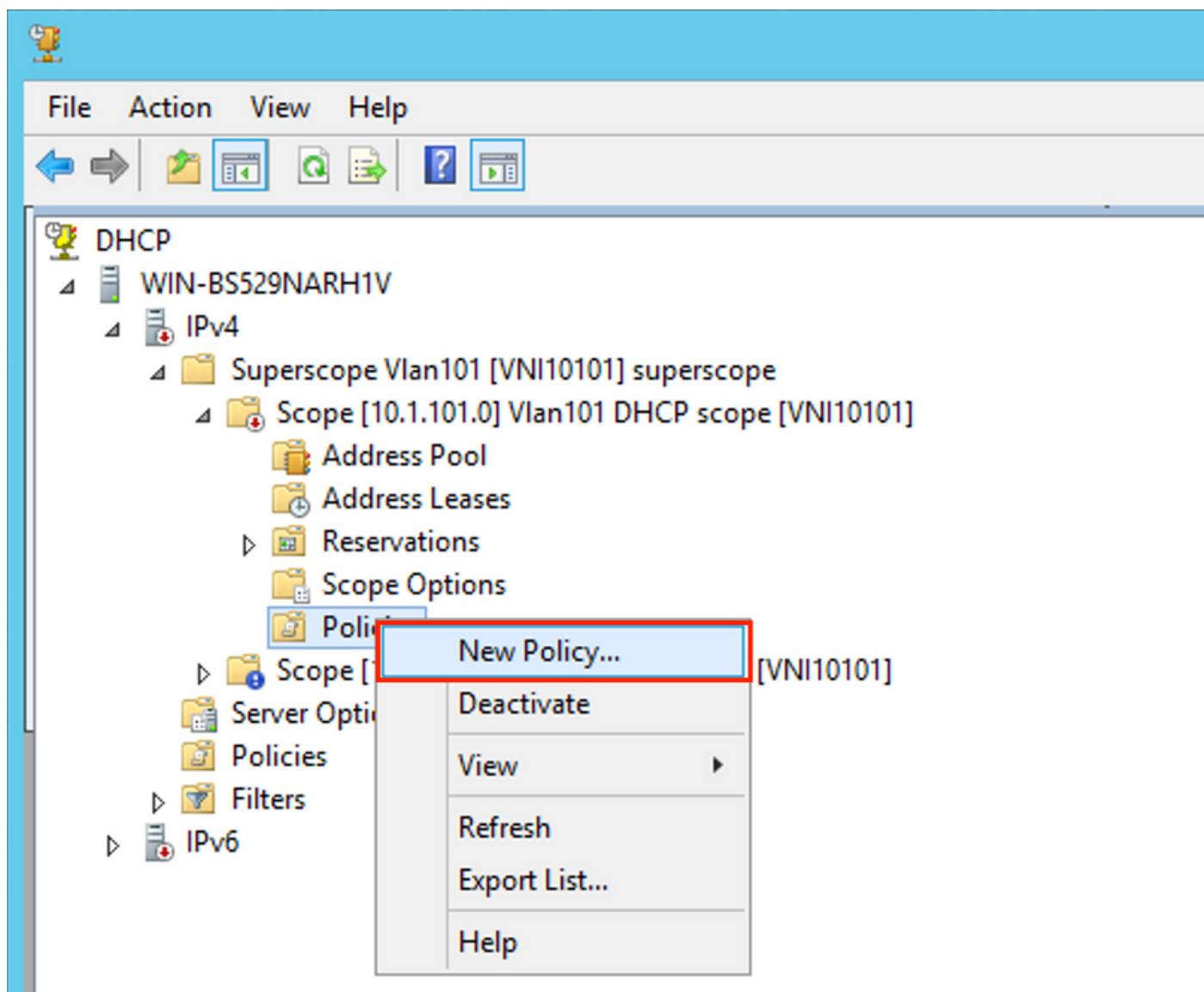
```



## Win2012 R2配置选项2 — 匹配代理电路ID字段

- 最后一种方法的缺点是唯一的环回的利用率很高，因此另一种方法是匹配代理电路ID字段。
- 步骤相同，但您为范围选择添加的策略不是基于Agent Circuit ID字段而是Relay IP。策略创建。右键单击池并选择**New Policy**，如图所示。





为策略选择有意义的名称和说明，如图所示。

## 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

如图所示添加新条件。

## 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...

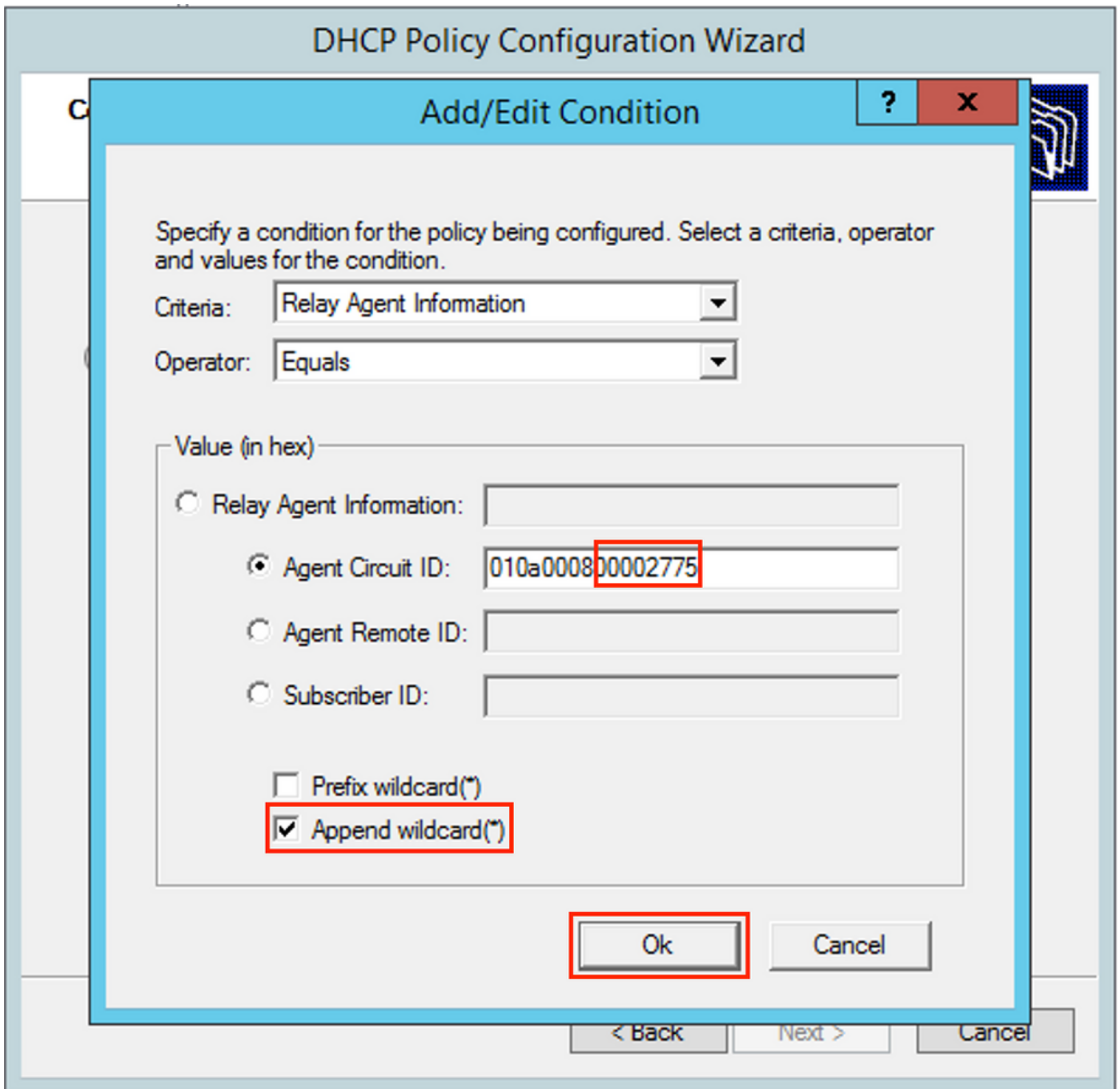
Remove

< Back

Next >

Cancel

输入正确的电路ID(不要忘记附加通配符(\*)框), 如图所示。



澄清为什么选择此编号：

在Wireshark中，可以看到代理电路ID等于010a000800002775010a000，该值是从这里派生的 (00002775十六进制= 10101十进制等于为VLAN 101配置的VNI 10101)。

- ▼ 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

VXLAN VN的代理电路ID子选项采用以下格式编码：

| 子选项类型 | 长度    | 电路ID类型 | 长度    | VNI      | mod   | 端口    |
|-------|-------|--------|-------|----------|-------|-------|
| 1 个字节 | 1 个字节 | 1 个字节  | 1 个字节 | 4 个字节    | 2 个字节 | 2 个字节 |
| 01    | 0a    | 00     | 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

配置从中分配IP地址的IP范围。如果没有此配置，则无法分配当前范围。

## 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

您也可以选择标准DHCP选项，如图所示。

## 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

选择完成，如图所示。



## 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:

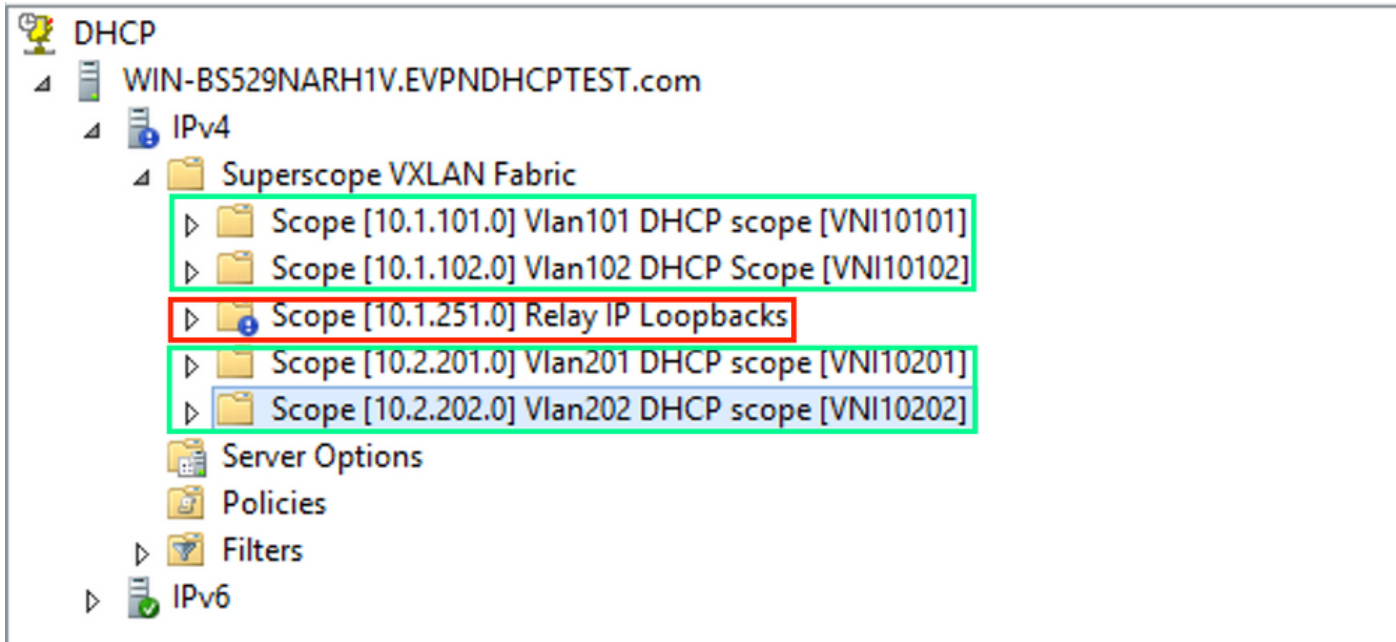
| Option Name | Vendor Class | Value |
|-------------|--------------|-------|
|-------------|--------------|-------|

< Back

Finish

Cancel

对于图中所示的其它范围，必须执行类似的配置。



在此方案中，对于多个SVI，每个VTEP只能使用一个唯一的IP地址，对于每个VTEP，不能使用一个唯一环回。

交换机配置:

```

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

```

## Windows Server 2016配置

- Windows Server 2016支持选项82子选项5 ( Cisco专有的150 ) “链路选择”，这意味着您不会使用唯一的中继IP地址进行池选择。而是使用“链路选择”子选项，从而显着简化配置。
  - 最好您仍然有一个中继IP地址池，否则DHCP数据包与任何范围都不匹配且不会被处理。
- 此示例演示了“链路选择”选项的用法。

启动中继IP地址的IP地址池，如图所示。

DHCP

File Action View Help



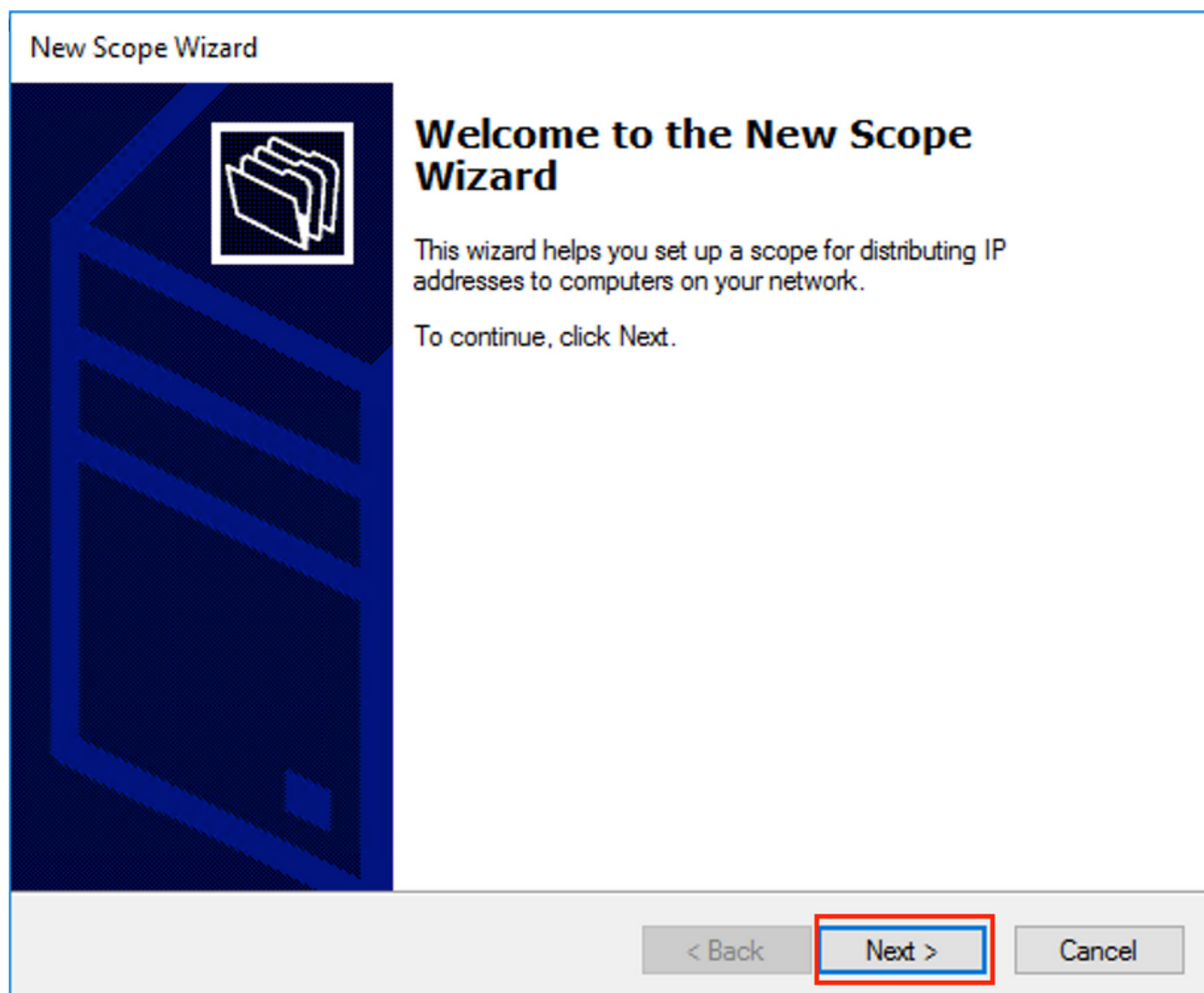
DHCP

WIN-IC90QQIUTE8.EVPNDHCPTTEST2016.com

IP

- 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

选择下一步，如图所示。



为范围选择有意义的名称和说明，如图所示。

## 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

输入用于IP中继的IP地址空间，如图所示。

## 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

从范围中排除所有范围，以阻止从此范围中进行分配，如图所示。

## 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

您还可以选择选项DNS/WINS等参数（在本示例中跳过），如图所示。

## 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

选择完成，如图所示。



## 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.

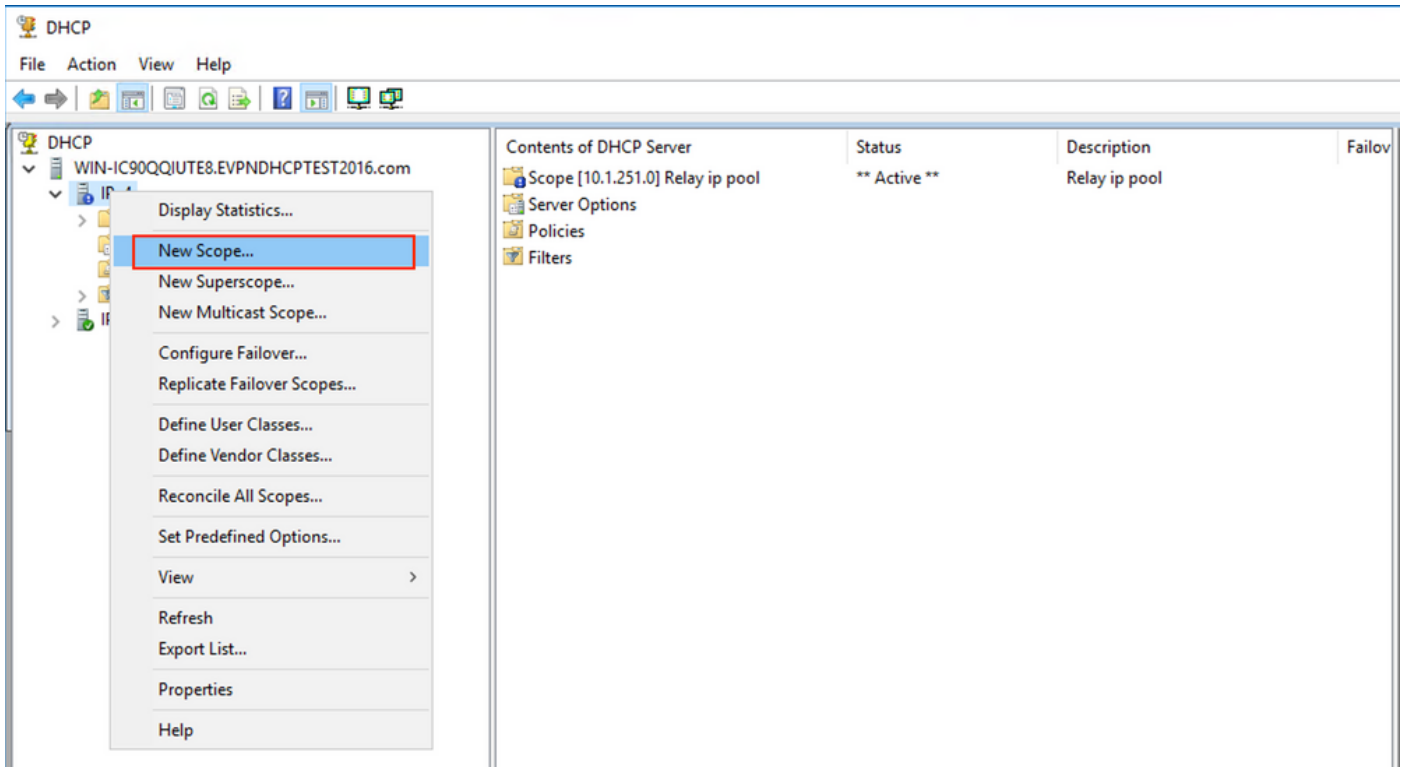
< Back

Finish

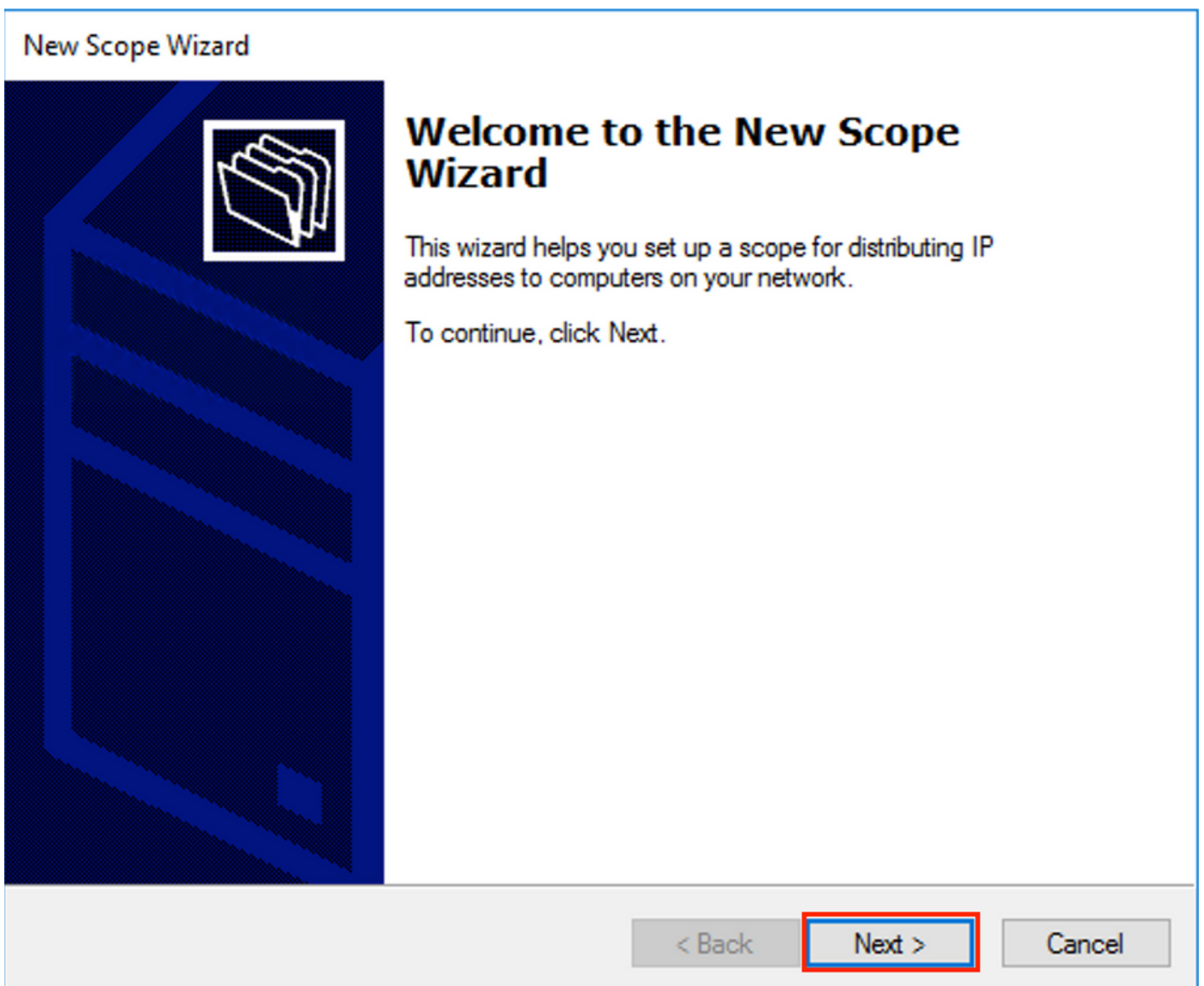
Cancel

继电器的范围现已就绪。

- 接下来，创建客户端从中获取IP地址的池。
- 右键单击并选择**New Scope**，如图所示。



选择下一步，如图所示。



选择有意义的池名称和说明，如图所示。

## 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

输入要在vlan101中分配的IP地址空间，如图所示。

## 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

如图所示，从作用域中排除默认网关IP。

## 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

如图所示设置租用时间。

## 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

如图所示，可以配置（在本例中跳过）其他参数（如DNS/WINS等）。

## 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

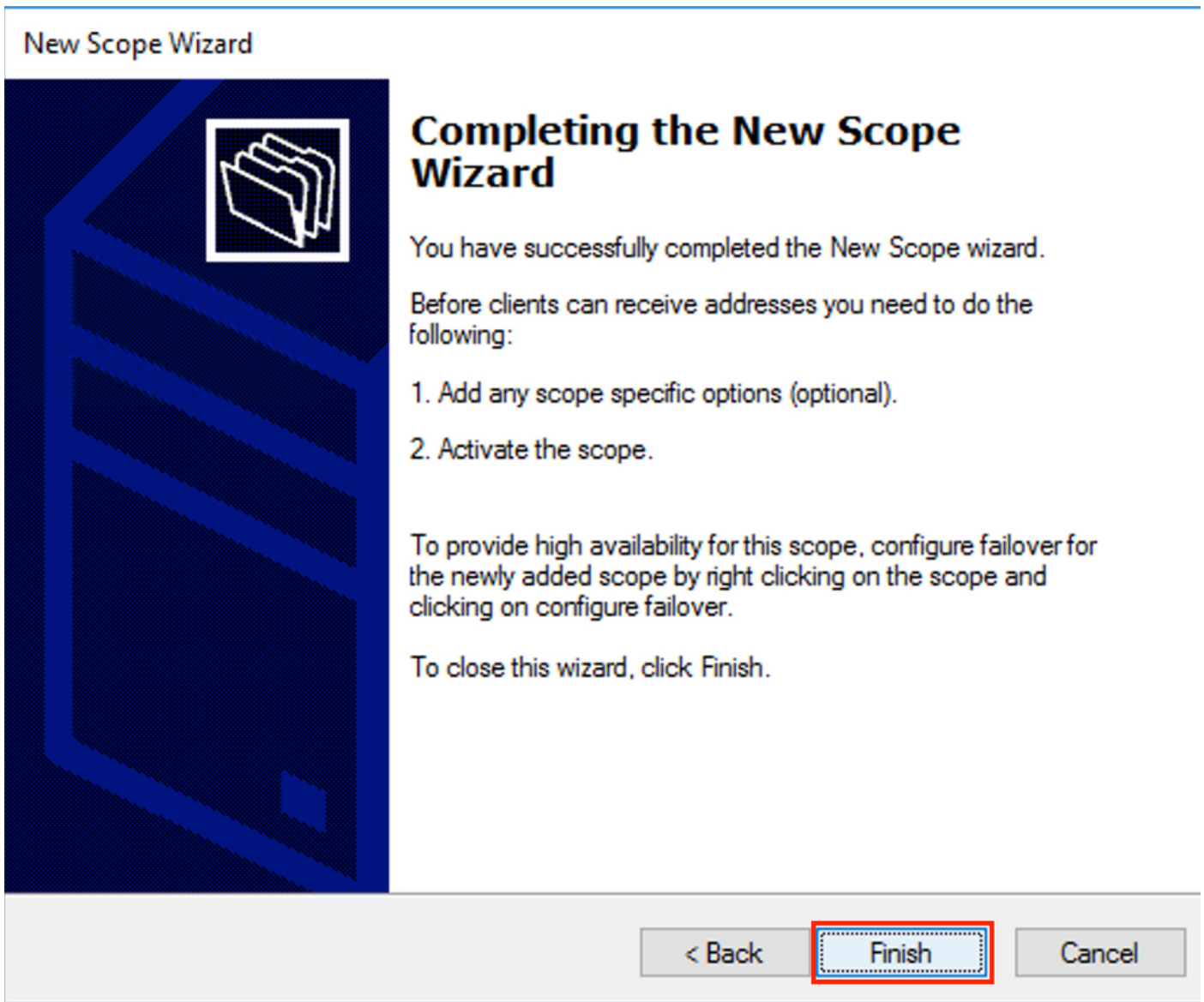
< Back

Next >

Cancel

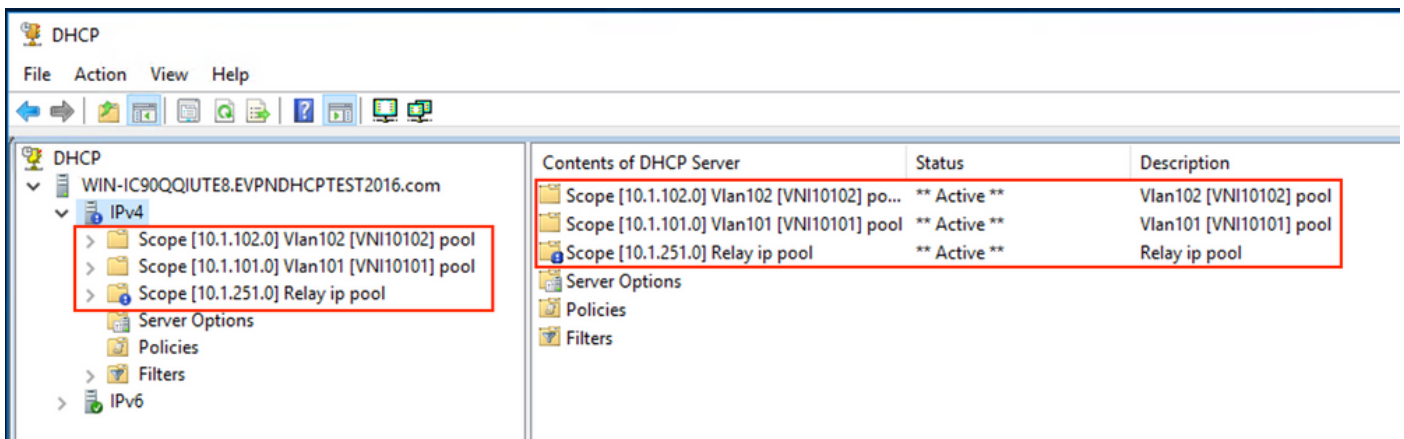
选择完成以完成设置，如图所示。





每个中继IP地址的池未配置，且未在HEX中匹配。池选择基于子选项**Link selection**。

可以添加新池，并且不需要额外配置，如映像所示。



## Linux DHCP 服务器

检查Linux上isc-dhcp-server的配置。

- 它支持中继选项82。在这里，最重要的选项是链路选择子选项。您仍然可以处理特定字段的座



席电路ID信息和十六进制掩码/匹配 ( 与win2012相同 )。从实用角度来看，使用82[5]比直接使用代理电路ID信息容易得多。

- 链路选择子选项的配置在子网定义下完成。

在本示例中，ISC服务器用于Ubuntu Linux。

安装DHCP服务器：

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

要配置DHCP服务器，请编辑/etc/dhcp/dhcpd.conf。（示例中使用Vim编辑器）

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

配置片段（省略常规配置）：

```
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;  
}
```

## 交换机配置

此处将查看一般支持的方案。

1. DHCP客户端位于租户VRF中，DHCP服务器位于第3层默认VRF中
  2. DHCP客户端位于租户VRF中，而DHCP服务器位于同一租户VRF中
  3. DHCP客户端位于租户VRF中，而DHCP服务器位于不同的租户VRF中
  4. DHCP客户端位于租户VRF中，而DHCP服务器位于非默认非VXLAN VRF中
- 对于上述任何一种情况，交换机端都需要DHCP中继配置。

最简单选项2的DHCP配置。

```
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]
```

默认情况下，选项82子选项**Link Selection**和**Server ID Override**是思科专有选项（分别为150和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)

如果DHCP服务器出于任何原因不理解Cisco专有选项，您可以将其更改为标准选项。

```
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

必须为必要的VLAN启用DHCP监听。

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

您可以使用DHCP-relay source-interface全局配置。

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

也可以逐个接口配置它（接口配置会覆盖全局配置）。

```

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

```

检查两个方向上都存在IP连接b/w中继IP地址和DHCP服务器。

```

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

```

在接口配置下，配置DHCP服务器的地址。此命令可以有3个选项。客户端和服务端位于同一VRF中：

```

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

```

客户端和服务端位于不同的VRF中（在本例中，客户端显示为绿色，服务器显示为红色）：

```

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

```

VRF中的客户端和全局路由表(GRT)中的服务器：

```

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

```

现在，此处查看所有选项的典型配置。

**DHCP客户端位于租户VRF中，而DHCP服务器位于第3层默认VRF中**

在本例中，GRT中的Lo0是中继源。某些接口的DHCP中继已全局配置+。

例如，对于vlan101命令“IP DHCP relay source-interface Loopback0”丢失，但使用全局配置。

```

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
```

因此，使用相同的SRC IP/DST IP但使用不同的子选项通过GRT发送DHCP中继数据包。

对于vlan101:

The screenshot displays a network traffic capture for a DHCP Discover packet. The packet list at the top shows three frames, with the second frame selected. The details pane below shows the following structure:

- 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

- 对于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

```

对于Vlan201 (为vrf红色，与VLAN 101和102不同，不是绿色)：

```

▶ 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

```

数据包捕获在Spine-01上从接口捕获到枝叶-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

```

核心层中的DHCP数据包是IP，无任何VXLAN封装：

```
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...>

```

此方法的一大优势是，您可以为不同的租户VRF使用相同的中继IP地址，而不会导致不同VRF和全局之间的路由泄漏。

## DHCP客户端和DHCP服务器位于同一租户VRF中

在这种情况下，租户VRF中具有中继IP地址是合理的。

交换机配置:

```
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
```

对于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
```

对于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

```

主干-01到枝叶-01接口的数据包捕获：

```

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

```

核心中的DHCP数据包采用VXLAN封装：

```

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

```

从Spine-01到Leaf-01接口的数据包捕获：

```

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

```

在本示例中，核心中的数据包包采用VXLAN封装。

```

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...>

```

## 一个租户VRF中的DHCP客户端和另一个非VXLAN VRF中的DHCP服务器

这个例子和上次非常相似。主要区别是数据包没有VXLAN封装 — 纯IP或其他 ( MPLS/GRE/等 )，但从配置角度而言是相同的。

在本示例中，客户端为vrf红色，服务器为vrf绿色。

您有两种选择：

- 中继IP位于客户端vrf中，并配置路由泄漏，这会增加复杂性
- 中继IP位于服务器vrf中 ( 类似于第一种情况下对GRT执行的操作 )

由于支持大量客户端VRF且不需要路由泄漏，因此选择第二种方法更简单。

交换机配置:

```

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

```

## 相关信息

- [RFC 3046](#)
- [RFC 3527](#)
- <https://docs.microsoft.com>
- [技术支持和文档 - Cisco Systems](#)