

IOS XE EVPN/VXLANでのDHCPの設定

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[設定](#)

[サーバの設定](#)

[Win2012 R2設定オプション1 - VNIごとの一意のリレーIP/VTEPごとのSVI](#)

[Win2012 R2設定オプション2 - \[Agent Circuit ID\]フィールドの照合](#)

[Windows Server 2016の構成](#)

[Linux DHCP サーバ](#)

[スイッチの設定](#)

[DHCPクライアントはテナントVRFにあり、DHCPサーバはレイヤ3デフォルトVRFにあります](#)

[DHCPクライアントとDHCPサーバが同じテナントVRFにある](#)

[あるテナントVRFのDHCPクライアントと別のテナントVRFのDHCPサーバ](#)

[1つのテナントVRF内のDHCPクライアントと別の非VXLAN VRF内のDHCPサーバ](#)

[関連情報](#)

概要

このドキュメントでは、さまざまなシナリオでのイーサネットVPN(EVPN)仮想拡張LAN(VXLAN)のダイナミックホストコンフィギュレーションプロトコル(DHCP)の設定と、Win2012およびWin2016 DHCPサーバの特定の側面について説明します。

前提条件

要件

EVPN/VXLANおよびDHCPに関する知識があることが推奨されます。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

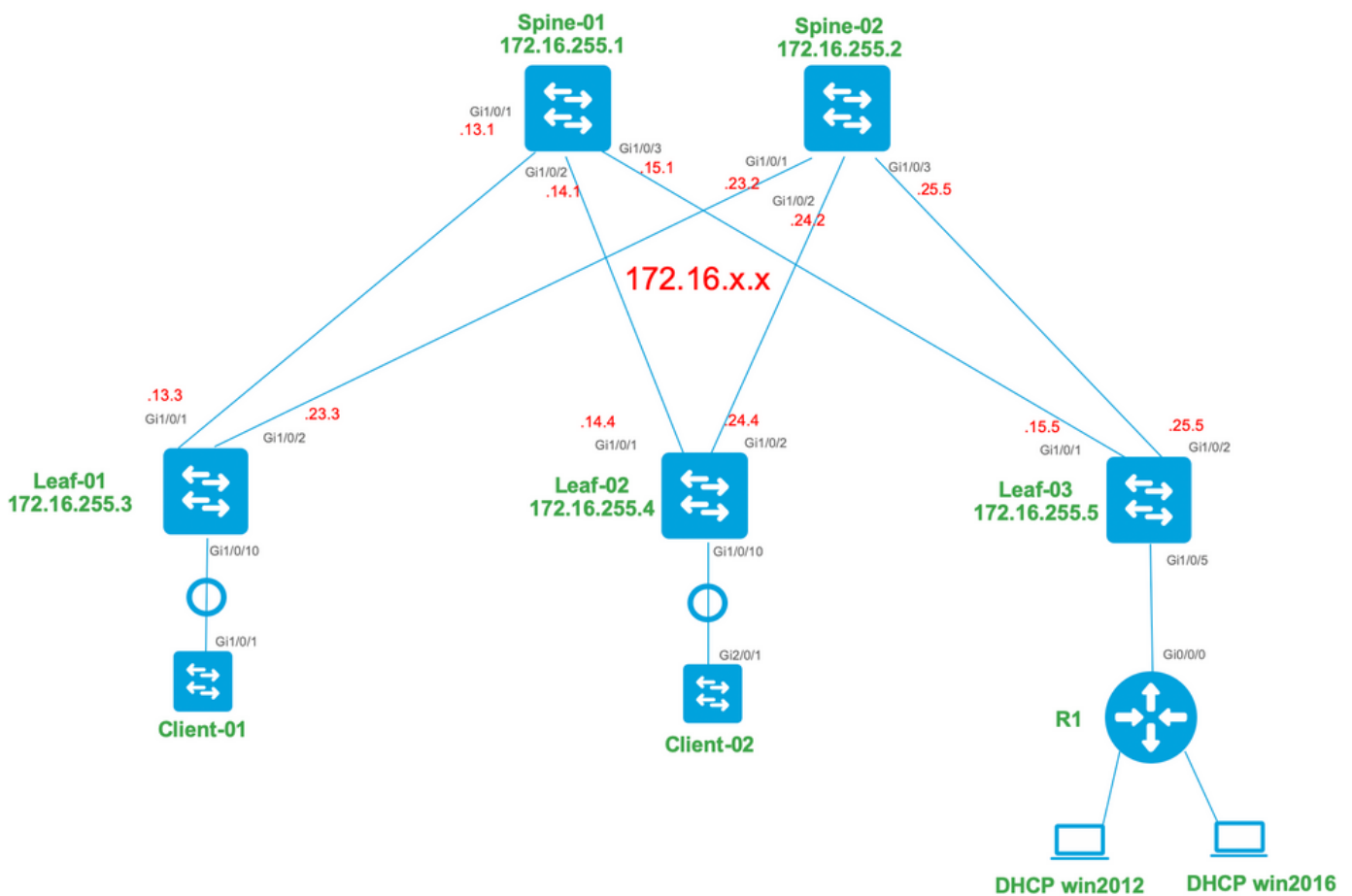
- C9300
- C9400
- C9500
- C9600
- MSFT Windows Server 2012 R2
- MSFT Windows Server 2016

- Cisco IOS XE 16.9.x以降で使用可能な機能

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

ネットワーク図

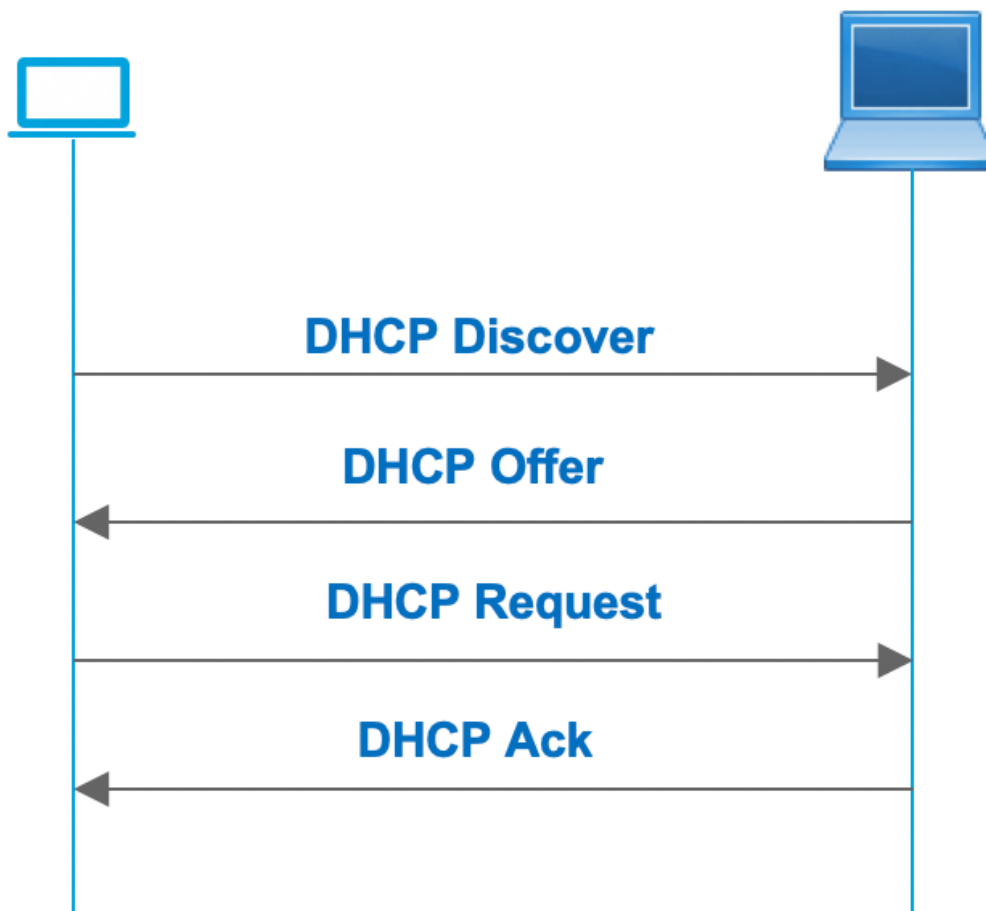


設定

次に、DHCPクライアントとサーバ間のメッセージフローを確認します。次の4つのフェーズがあります。

DHCP client

DHCP server



これは、クライアントとサーバが同じサブネットにある場合に機能しますが、通常はそうではありません。ほとんどの場合、DHCPサーバはクライアントと同じサブネットになく、レイヤ3ルーテッドパスとレイヤ2を介して到達可能である必要があります。この場合、DHCPリレー機能が必要です。DHCPリレー（スイッチまたはルータ）機能は、ブロードキャストをルーティング可能なudpカプセル化ユニキャストに変換し、DHCPサーバに送信します。最近のネットワークで広く使用されている設定です。

DHCPおよびEVPN/VXLANファブリックの課題：

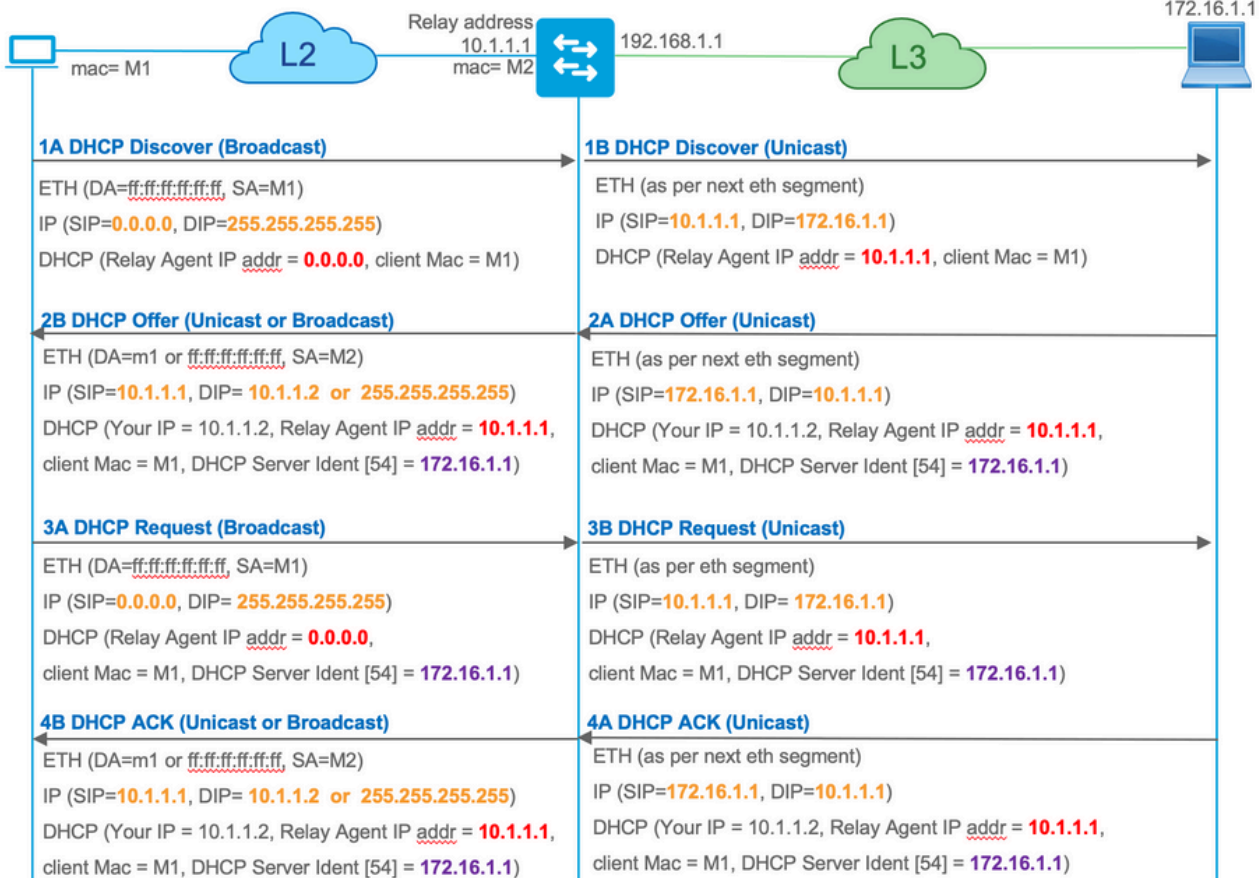
通常、DHCPサーバはL3ネットワーク経由でEVPNファブリックに接続されます。つまり、DHCPリレー機能を使用して、レイヤ2 DHCPブロードキャストパケットをレイヤ3ユニキャストのルーティング可能なパケットに変換する必要があります。

DHCPリレー機能では、クライアント、リレー、およびサーバ間のDHCPコールフローは次のように動作します。

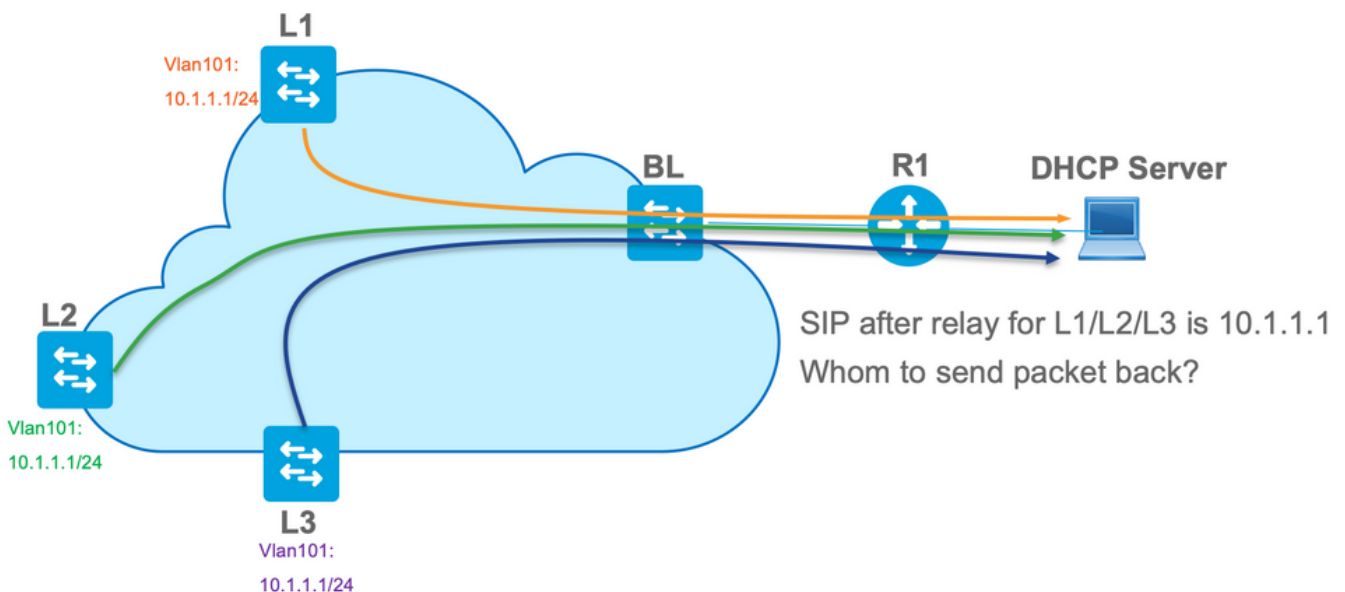
DHCP client

DHCP relay

DHCP server



リレーされた後、パケットの送信元IPはリレーIPになります。ただし、分散工二一キャストゲートウェイ(DAG)の使用により、通常の送信元IPは一意ではないため、VXLAN/EVPN展開では問題が発生します。すべてのVTEP SVI送信元IPが同じであるため、DHCPサーバからの応答パケットが最も近いリーフに転送される可能性があります。



一意でない送信元の問題を解決するには、リーフごとにリレーされるDHCPパケットに一意的IPアドレスを使用できる必要があります。GIADDRの交換に関連する別の問題もあります。DHCPサーバで、IPアドレスを割り当てる正しいプールを選択する必要があります。これは、ゲートウェイIPアドレス(giaddr)をカバーするプールから実行されます。EVPNファブリックの場合

は、SVIのIPアドレスである必要がありますが、リレーの後、giaddrはリレーIPアドレス（この場合は一意のループバック）に置き換えられます。

使用する必要があるプールをDHCPサーバに通知するには、どうすればよいですか。

この問題を解決するには、オプション82を使用します。主に、次の重要なサブオプションがあります。

- 1:エージェント回線ID。VXLAN/EVPNの場合、このサブオプションはVNI IDを転送します
- 5 - (またはシスコ独自の150)。DHCPパケットの送信元である実際のサブネットを持つ **Link selection**サブオプション
- 11 - (またはシスコ独自の場合は152)。DHCPサーバのアドレスを持つ **Server Identifier Override**サブオプション
- 151:VRF名/VPN ID。このサブオプションにはVRF名/VPN IDがあります

DHCPリレーからDHCPサーバへのパケットのネットワークキャプチャでは、次の図に示すように、DHCPパケットに次のようなさまざまなオプションが存在することを確認できます。

The screenshot shows a packet capture of a DHCP Discover message. Key fields are highlighted with red boxes and labeled with red arrows:

- Relay Agent/Giaddr:** Points to the 'Relay agent IP address: 10.1.251.1' field.
- Agent Circuit ID (VNI encoded):** Points to the 'Agent Circuit ID: 010a00080002775010a0000' field.
- Link Selection (pool from which ip_address should be assigned):** Points to the 'Link selection (Cisco proprietary): 10.1.101.0' field.
- Server ID override (used for redirecting DHCP renew over relay):** Points to the 'Server ID Override (Cisco proprietary): 10.1.101.1' field.

スイッチの設定：

- オプション82には、正しいDHCPプールを選択し、サーバから正しいリーフにパケットを戻すために必要なすべての情報が含まれています。
- これは、DHCPサーバがオプション82情報を処理できる場合にのみ機能しますが、すべてのサーバが完全にサポートしているわけではありません（win2012 r2など）。

`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

```

サーバの設定

Win2012 R2設定オプション1 - VNIごとの一意のリレーIP/VTEPごとのSVI

win2012の主な問題は、オプション82が完全にはサポートされないので、「Link selection」サブオプション（5またはCisco独自 - 150）を使用してDHCPサーバ上の適切なプールを選択できないことです。

このような問題を解決するには、次のアプローチを使用できます。

- リレーIPアドレスのスコープを作成する必要があります。作成しない場合、DHCPはDHCP GIADDRに一致するプールを見つけず、パケットを無視します。リレーIPプールからの割り当てを防ぐために、DHCPから完全なIP範囲を除外する必要があります。このプールをRELAY_POOLと呼びます
- 割り当てるIP範囲のスコープを作成する必要があります。このプールをIP_POOLと呼びます
- スーパースコープを作成し、両方のスコープ - RELAY_POOLとIP_POOLを含める必要があります

DHCPパケットがサーバでどのように処理されるかを見てみましょう。

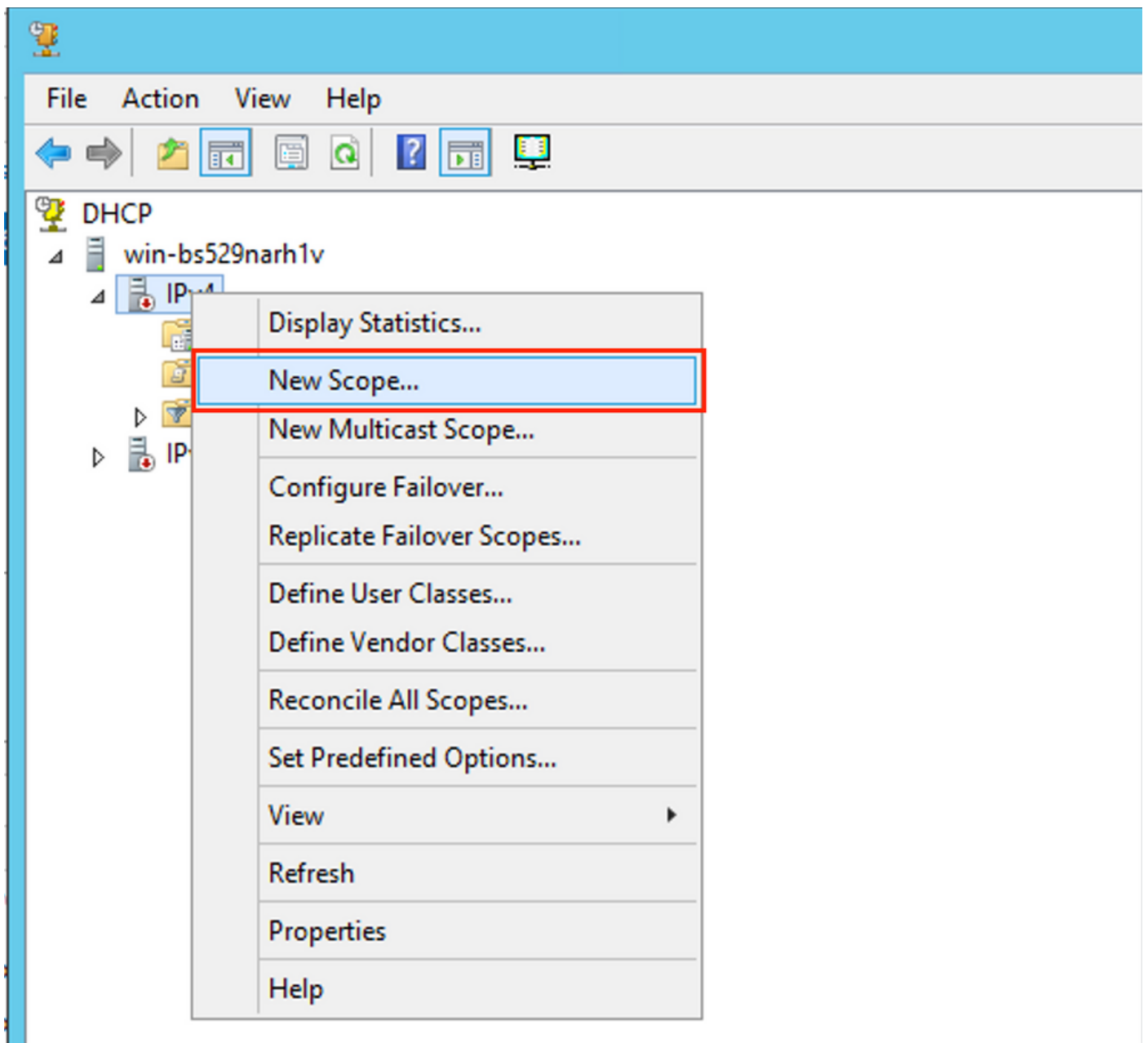
1. DHCPパケットがサーバによって受信されます。
2. GIADDRに基づいて、適切なスーパースコープで各プールRELAY_POOLが選択されます。
3. RELAY_POOLには空きIPアドレスがないため（フルスコープが除外されていることに注意してください）、同じスーパースコープ内のIP_POOLにフォールバックします。
4. アドレスはそれぞれのスーパースコープから割り当てられ、リレーに送り返されます。

この方法の大きな欠点は、DHCPプールがリレーアドレスに基づいて選択されるため、VLAN単位またはVTEP単位で一意のループバックを設定する必要があることです。

このオプションを使用すると、リレーIPアドレスに大きなIP範囲を使用できます。

オプション1. win2012 r2を設定する手順の説明。

リレーアドレスのDHCPスコープを作成します。右クリックし、図に示すように[New Scope]を選択します。



図に示すように、[Next] を選択します。

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

意味のある名前と説明を入力し、図に示すように[Next] を選択します。

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

リレープールのIPアドレス情報を入力します。この例では、ネットマスクは/24ですが、図に示すように大きくすることも小さくすることもできます（ネットワークのサイズによって異なります）。

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

プールからすべての範囲を除外します。これは重要です。そうしないと、このプールからIPアドレスを割り当てることができます。

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

図に示すように、リース時間（デフォルトでは8日）を設定します。

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

DNS/WINS (この例では省略)などのDHCPオプションパラメータを設定できます。

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

図に示すように、スコープをアクティブにします。

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

図に示すように、設定を終了します。

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.

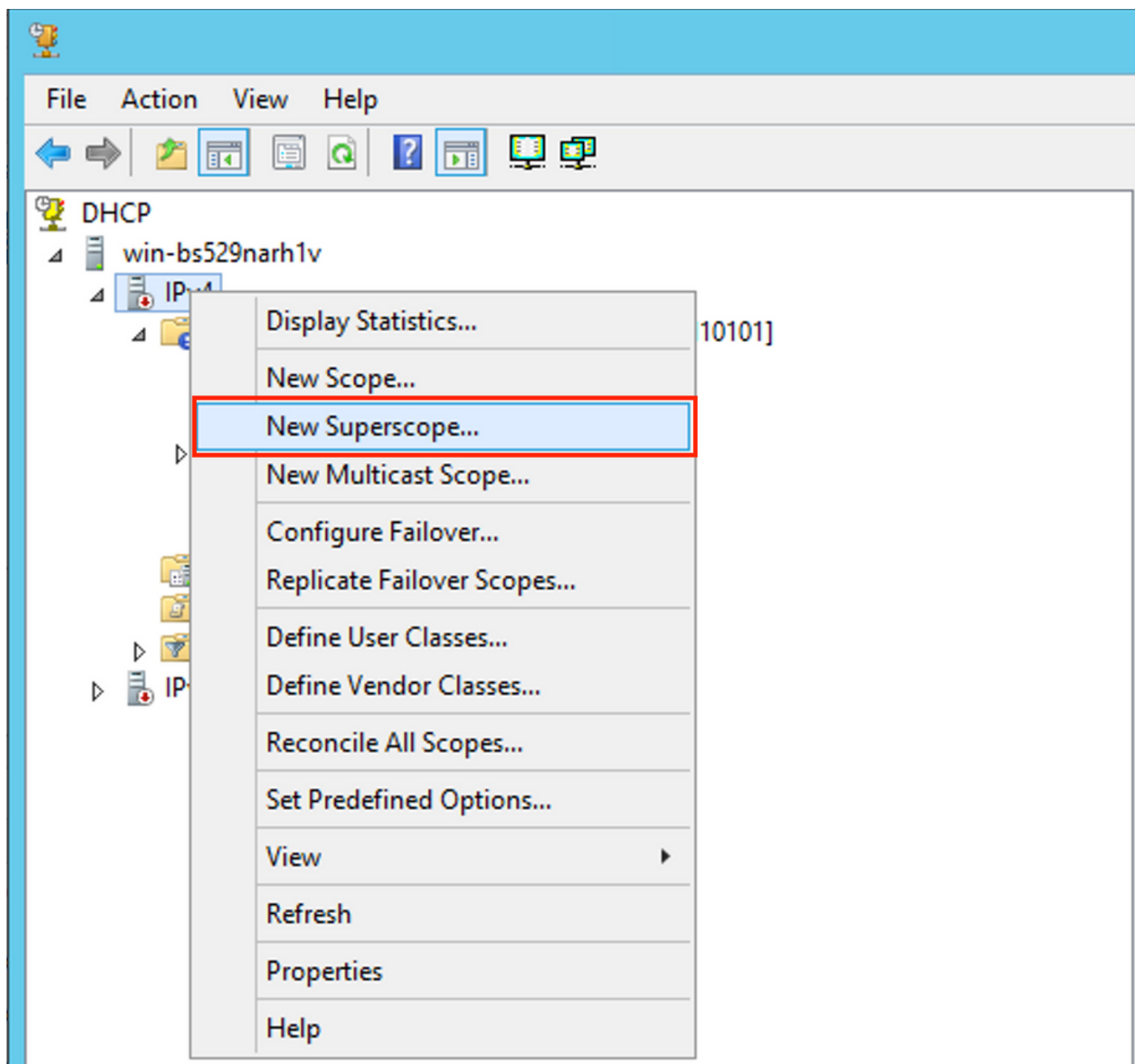
To close this wizard, click Finish.

< Back

Finish

Cancel

次に、スーパースコープを作成します。右クリックし、図に示すように[New Superscope] を選択します。



図に示すように、[Next] を選択します。

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

図に示すように、スーパースコープに意味のある名前を選択します。

New Superscope Wizard

Superscope Name

You have to provide an identifying superscope name.



Name:

< Back

Next >

Cancel

スーパースコープに追加するスコープを選択します。

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:

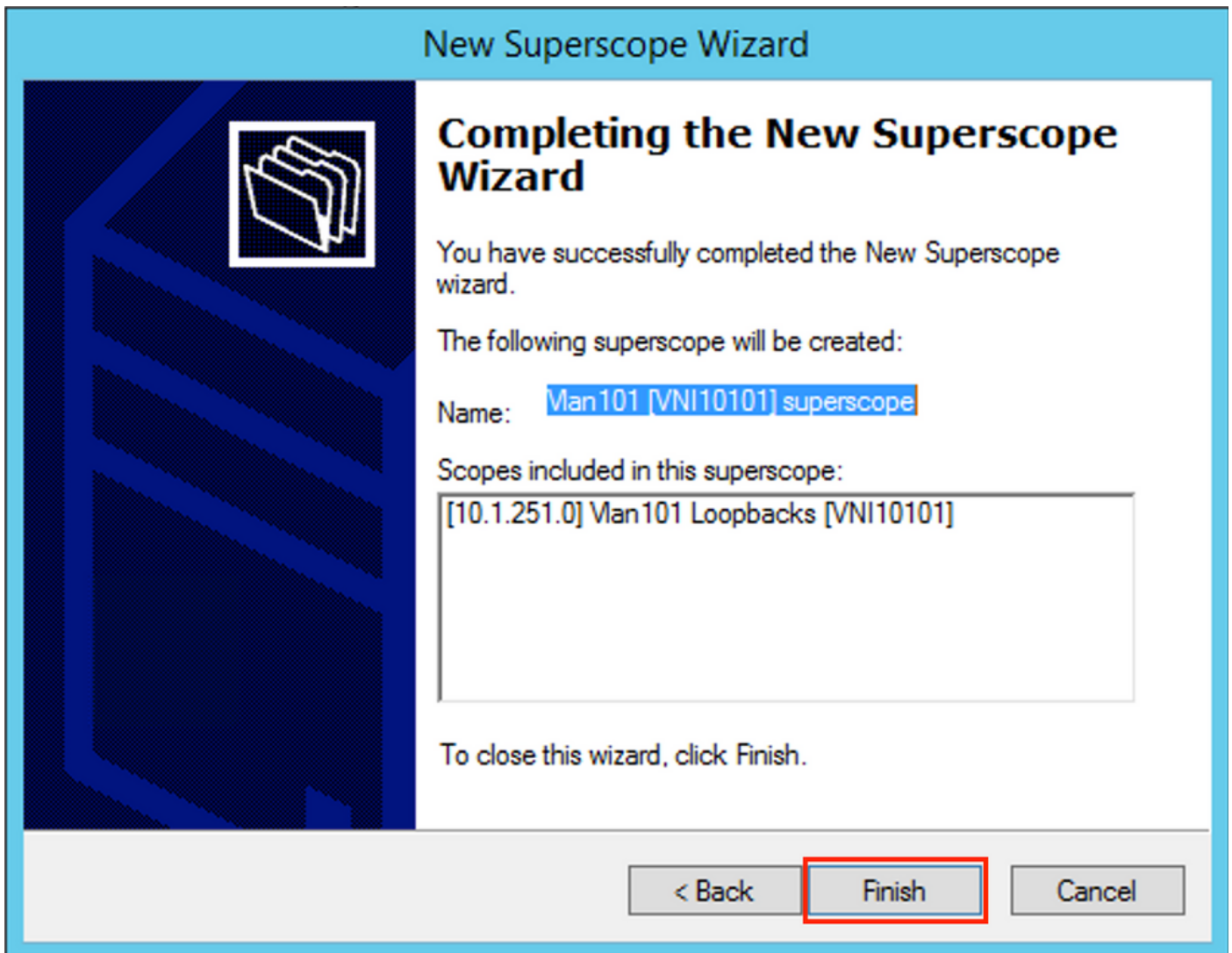
[10.1.251.0] Man101 Loopbacks [VNI10101]

< Back

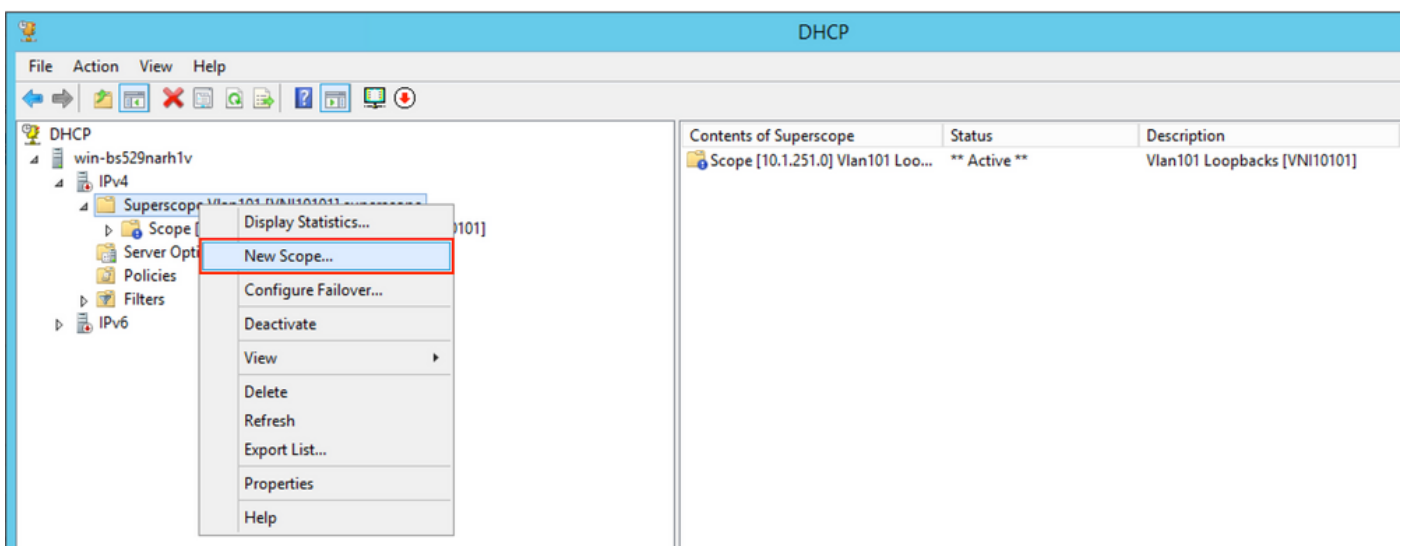
Next >

Cancel

図に示すように、セットアップを終了します。



IPアドレスを割り当てるDHCPプールを作成します。右クリックして[New Scope...]を選択します。を参照してください。



図に示すように、[Next] を選択します。

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

図に示すように、意味のある名前と説明を選択します。

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

図に示すように、クライアントにIPアドレスを割り当てるプールのネットワークとマスクを指定します。

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

図に示すように、デフォルトゲートウェイのIPアドレス（この例では10.1.101.1）をプールから除外します。

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

図に示すように、リースタイマーを指定します。

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

必要に応じて、DNS/WINS (この例では省略) を指定できます。

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

図に示すように、設定を終了します。



プールを作成した後、プールのポリシーを作成する必要があります。

- Agent Circuit ID [1]が一致するポリシー内
- 複数のVlan/VNIがある場合は、リレーIPアドレス用のサブプールと、各VLAN/VNIごとの割り当て用の実際のIP範囲を使用してスーパープールを作成する必要があります
- この例では、VNI 10101および10102を使用しています

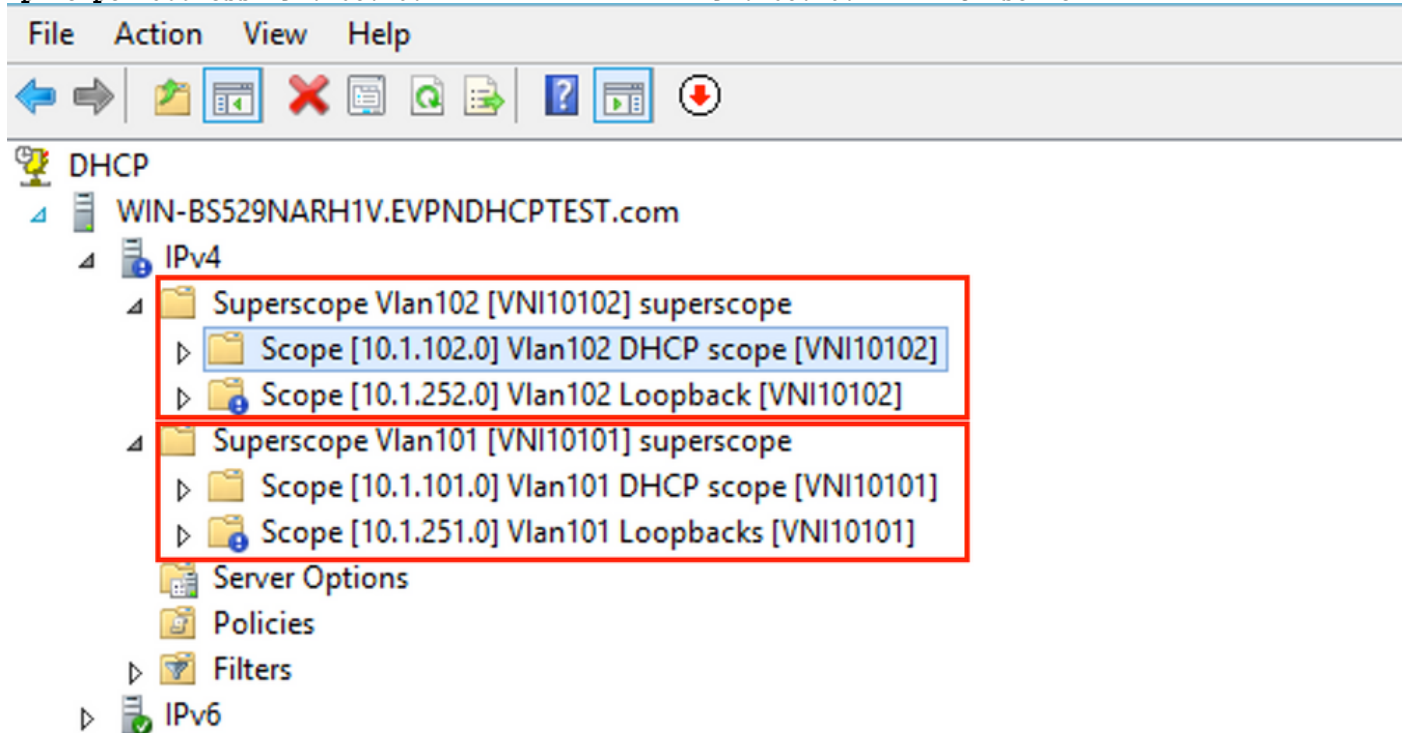
スイッチの設定：

```
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

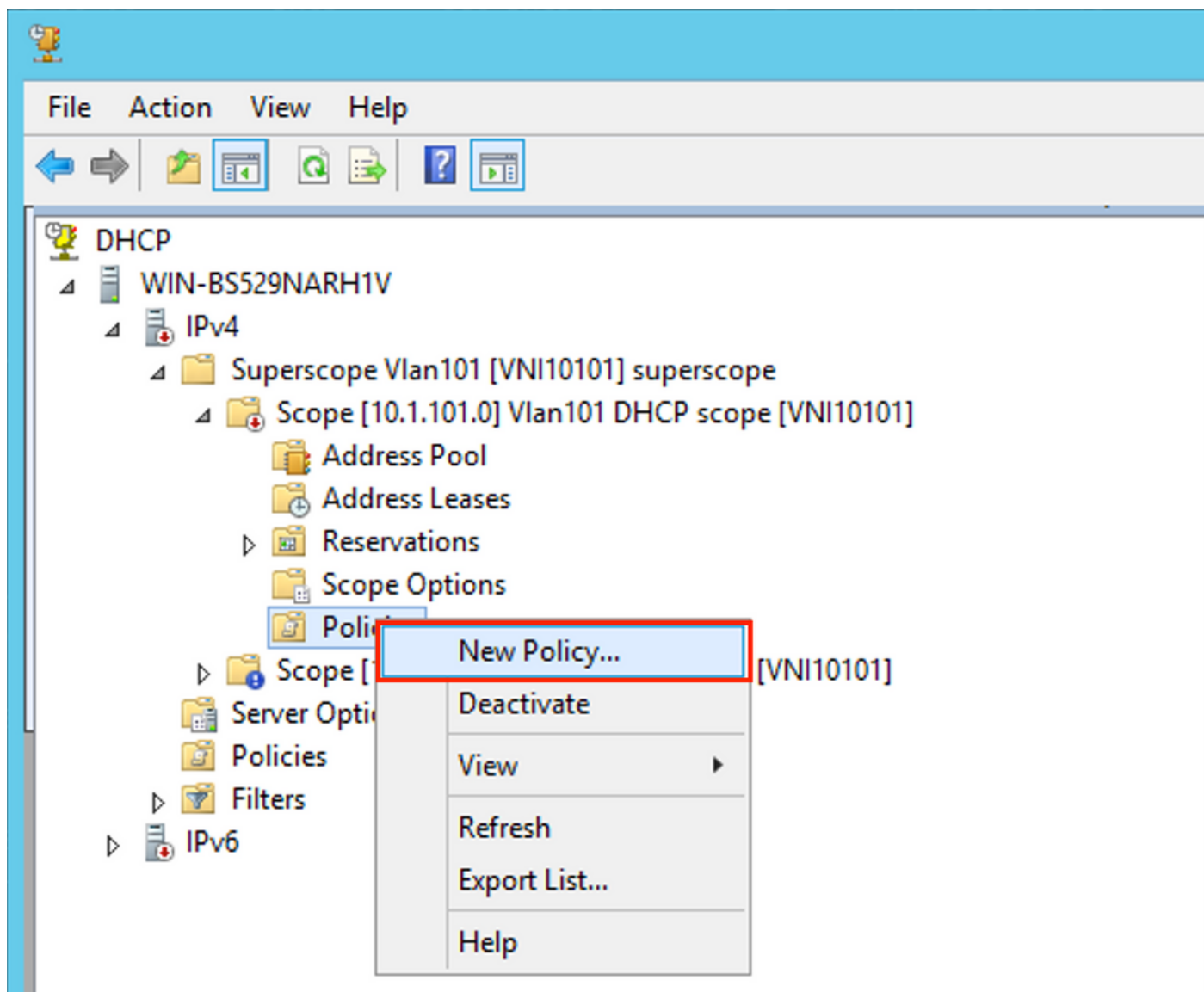
```



Win2012 R2設定オプション2 - [Agent Circuit ID]フィールドの照合

- 最後のアプローチの欠点は、一意のループバックの使用率が高いことです。そのため、別のオプションとして、エージェント回線IDフィールドを照合する方法があります。
- 手順は同じですが、Relay IPではなくAgent Circuit IDフィールドに基づかないスコープ選択のポリシー作成を追加します。

ポリシーの作成次の図に示すように、[pool]を右クリックし、[New Policy] を選択します。



図に示すように、ポリシーの意味のある名前と説明を選択します。

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

図に示すように、新しい条件を追加します。

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

図に示すように、適切な回線IDを入力します([Append Wildcard (*)]ボックスを忘れないでください)。

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(*)

この番号が選択された理由の説明：

Wiresharkでは、010a000800002775010a0000と等しいエージェント回線IDを確認できます。この場合、この値は(00002775 hex = 10101 decimal is equal to configured VNI 10101 for the VLAN 101)から算出されます。

- ▼ 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

Agent Circuit IDサブオプションは、VXLAN VNに対して次の形式でエンコードされます。


サブオプションタイプ	長さ	回線IDタイプ	長さ	VNI	mod	port
01	1バイト	0a	1バイト	00	1バイト	4バイト
					2バイト	2バイト
					*	*

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

IPアドレスが割り当てられるIP範囲を設定します。この設定を行わないと、現在のスコープの割り当ては行えなくなります。

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

図に示すように、この段階で標準のDHCPオプションを選択することもできます。

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	∨

Data entry

Long:

0x0

< Back

Next >

Cancel

図に示すように、[Finish] を選択します。

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:

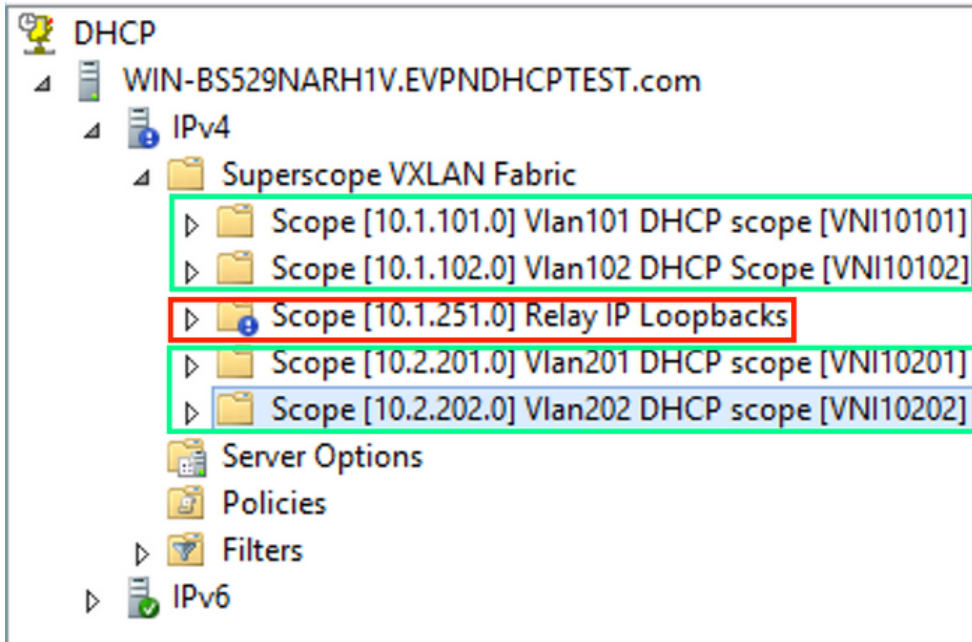
Option Name	Vendor Class	Value
-------------	--------------	-------

< Back

Finish

Cancel

図に示すように、他の範囲でも同様の設定を行う必要があります。



このシナリオでは、SVIの数に対してVTEPごとに1つの一意のIPアドレスのみを使用でき、VTEPごとにVNI/SVIごとに1つの一意のループバックを使用することはできません。

スイッチの設定：

```

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の構成

- Windows Server 2016は、オプション82サブオプション5 (Cisco独自の150) 「リンク選択」をサポートしています。これは、プール選択に一意のリレーIPアドレスを使用しないことを意味します。代わりに、「リンク選択」サブオプションを使用して、設定を大幅に簡素化します。
- リレーIPアドレス用のプールがまだある場合に最適です。そうでない場合、DHCPパケットはどのスコープとも一致せず、処理されません。

この例では、「link selection」オプションの使用方法を示します。

図に示すように、リレーIPアドレスのIPアドレスプールを開始します。

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

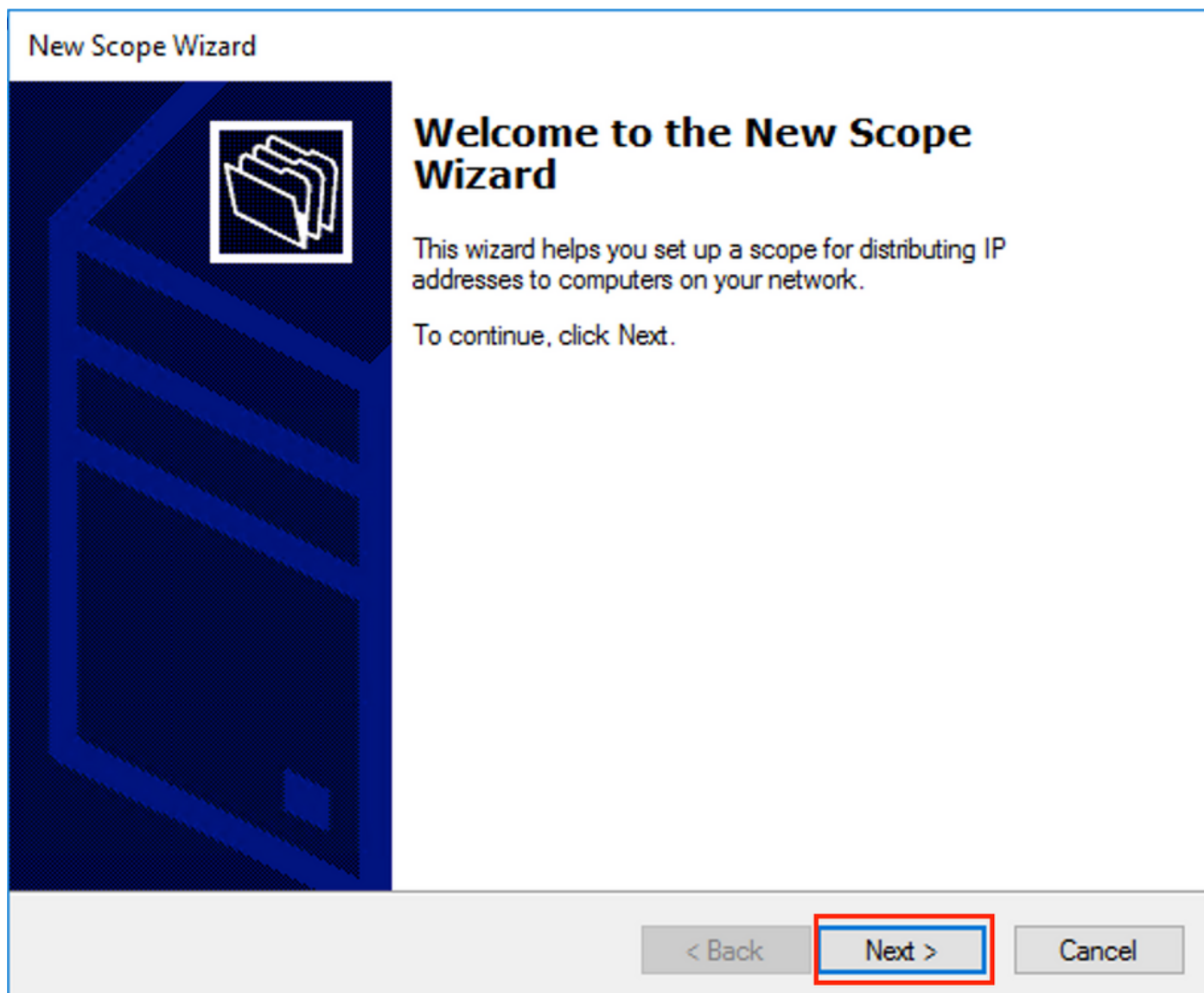


Refresh

Properties

Help

図に示すように、[Next] を選択します。



図に示すように、スコープの意味のある名前と説明を選択します。

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

図に示すように、IPリレーに使用されるIPアドレス空間を入力します。

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

図に示すように、スコープからすべての範囲を除外して、この範囲からの割り当てを防ぎます。

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

図に示すように、オプションDNS/WINSなどのパラメータ（この例では省略）を選択することもできます。

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

図に示すように、[Finish] を選択します。



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.

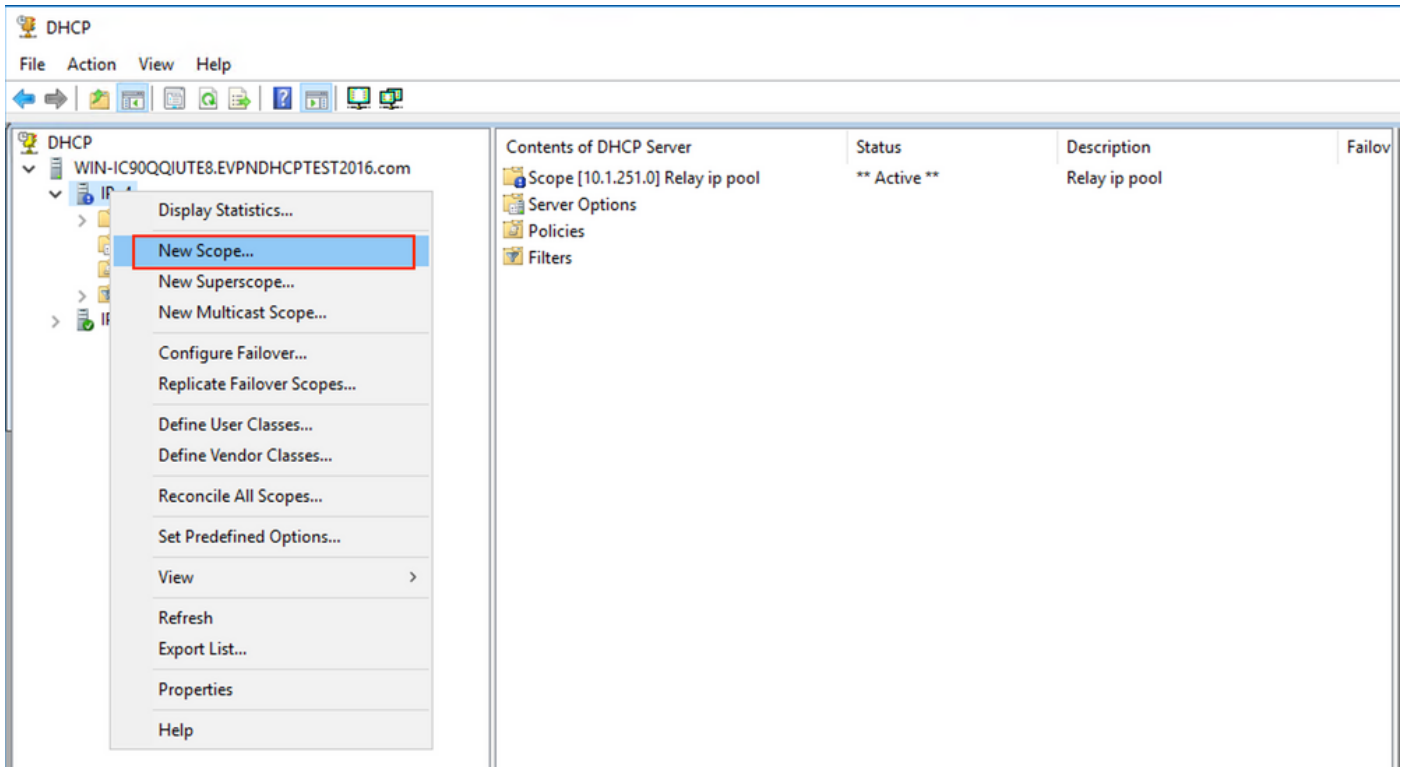
< Back

Finish

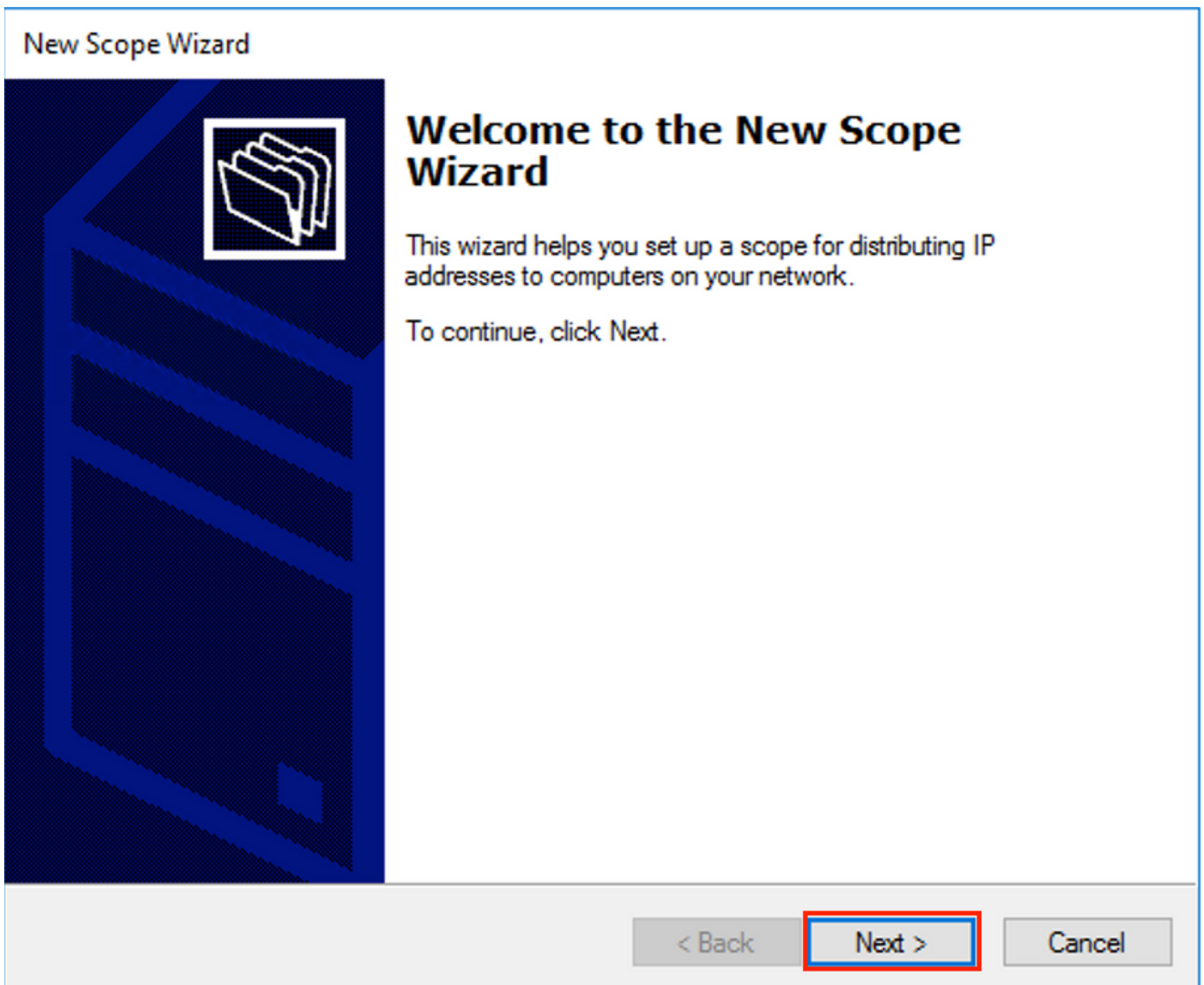
Cancel

リレーのスキープの準備ができました。

- 次に、クライアントがIPアドレスを取得するプールを作成します。
- 右クリックし、図に示すように[New Scope] を選択します。



図に示すように、[Next] を選択します。



図に示すように、プールの意味のある名前と説明を選択します。

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:

図に示すように、vlan101に割り当てるIPアドレス空間を入力します。

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

図に示すように、スコープからデフォルトゲートウェイIPを除外します。

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

図に示すように、リース時間を設定します。

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

図に示すように、DNS/WINSなどの追加パラメータを設定できます（この例では省略します）。

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

Finishを選択して、図に示すように設定を完了します。

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

リレーIPアドレスごとのプールは設定されておらず、16進数では一致しません。プールの選択は、サブオプション[Link selection]に基づきます。

新しいプールを追加でき、図に示すように追加の設定は必要ありません。

Contents of DHCP Server	Status	Description
Scope [10.1.102.0] Vlan102 [VNI10102] po...	** Active **	Vlan102 [VNI10102] pool
Scope [10.1.101.0] Vlan101 [VNI10101] pool	** Active **	Vlan101 [VNI10101] pool
Scope [10.1.251.0] Relay ip pool	** Active **	Relay ip pool
Server Options		
Policies		
Filters		

Linux DHCP サーバ

Linuxのisc-dhcp-serverの設定を確認します。

- リレーオプション82をサポートしています。ここで最も重要なものはリンク選択サブオプションです。エージェント回線ID情報と16進数のマスク一致は、特定のフィールドに対して引き続き使用できます (win2012に対して行われたように)。実用的な観点から、エージェント回線ID情報を直接操作するよりも、82[5]を使用する方がはるかに簡単です。
- リンク選択サブオプションの設定は、サブネット定義の下で行われます。

この例では、ISCサーバはUbuntu Linuxで使用されます。

DHCPサーバをインストールします。

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

DHCPサーバを設定するには、`/etc/dhcp/dhcpd.conf`を編集します。(例ではVimエディタを使用します)。

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

設定の省略 (一般的な設定は省略):

```
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;  
}
```

スイッチの設定

ここでは、一般的にサポートされているシナリオを確認します。

1. DHCPクライアントはテナントVRFにあり、DHCPサーバはレイヤ3のデフォルトVRFにあります
2. DHCPクライアントはテナントVRFにあり、DHCPサーバは同じテナントVRFにあります
3. DHCPクライアントはテナントVRFにあり、DHCPサーバは別のテナントVRFにあります
4. DHCPクライアントはテナントVRFにあり、DHCPサーバはデフォルト以外の非VXLAN VRFにあります

これらのシナリオでは、スイッチ側でDHCPリレーの設定が必要です。

最も単純なオプション番号2のDHCP設定。

```
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]
```

デフォルトでは、オプション82のサブオプションLink SelectionとServer ID Overrideはシスコ独自のオプションです (それぞれ150と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)

何らかの理由でDHCPサーバがシスコ独自のオプションを理解できない場合は、標準のオプションに変更できます。

```
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

必要なVLANに対してDHCPスヌーピングを有効にする必要があります。

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

DHCP-relay source-interfaceグローバルコンフィギュレーションを使用できます。

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

または、インターフェイス単位で設定することもできます (インターフェイス設定はグローバル設定よりも優先されます)。

```
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
```

双方向にリレーIPアドレスとDHCPサーバによるIP接続があることを確認します。

```
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

インターフェイス設定では、DHCPサーバのアドレスが設定されます。このコマンドには3つのオプションがあります。クライアントとサーバは同じVRF内にあります。

```
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
```

クライアントとサーバは異なるVRFにあります (この例では、クライアントは緑、サーバは赤)。

```
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内のクライアント、およびグローバルルーティングテーブル(GRT)内のサーバ :

```
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
```

ここでは、すべてのオプションの一般的な設定を確認します。

DHCPクライアントはテナントVRFにあり、DHCPサーバはレイヤ3デフォルトVRFにあります

この場合、GRTのLo0はリレーソースです。DHCPリレーは、一部のインターフェイスに対してグローバル+に設定されます。

たとえば、vlan101コマンド「IP DHCP relay source-interface Loopback0」が欠落していても、グローバルコンフィギュレーションが使用されています。

```
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
```

その結果、DHCPリレーパケットは同じSRC IP/DST IPを使用してGRT経由で送信されますが、サブオプションは異なります。

vlan101の場合：

dhcpcd

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

• Vlan102の場合 :

```
▶ 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
```

Vlan201 (VLAN 101と102のように緑色ではなく、vrf redで表示) の場合 :

```

▶ 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

```

Spine-01で、インターフェイスからLeaf-01へのパケットキャプチャが実行されました。

```
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

```

コア内のDHCPパケットは、VXLANカプセル化のないIPです。

```
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...>

```

このアプローチの大きな利点は、異なるVRFとグローバル間でルートが漏出することなく、異なるテナントVRFに同じリレーIPアドレスを使用できることです。

DHCPクライアントとDHCPサーバが同じテナントVRFにある

この場合は、テナントVRFにリレーIPアドレスを設定するのが適切です。

スイッチの設定：

```
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
```

vlan101の場合：

```
▶ 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
```

vlan102の場合 :

```

▶ 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

```

Spine-01からLeaf-01インターフェイスへのパケットキャプチャ :

```

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

```

コア内のDHCPパケットにはVXLANカプセル化があります。

```

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

```

```

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

```

あるテナントVRFのDHCPクライアントと別のテナントVRFのDHCPサーバ

この例では、クライアントはvrf redで、サーバはvrf greenです。

次の2つのオプションがあります。

- クライアントvrfでリレーIPを維持し、より複雑なルート漏出を設定する
- サーバvrfにリレーIPを保持する (最初のケースではGRTに対して行ったのと同様)

多くのクライアントvrfがサポートされており、ルート漏出が不要であるため、2番目のアプローチを選択する方が簡単です。

スイッチの設定 :

```

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

```

vlan201の場合 :


```

▶ 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

```

Spine-01からLeaf-01インターフェイスへのパケットキャプチャ :

```

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

```

この例では、コア内のパケットはVXLANカプセル化されます。

```

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...>

```

1つのテナントVRF内のDHCPクライアントと別の非VXLAN VRF内のDHCPサーバ

この事件は前の事件とたいへん似ている。主な違いは、パケットにはVXLANカプセル化(純粋なIP(MPLS/GRE/ETC)など)がないことですが、設定の観点からは同じです。

この例では、クライアントはvrf redで、サーバはvrf greenです。

次の2つのオプションがあります。

- リレーIPはクライアントvrfにあり、ルート漏出を設定するため、複雑さが増す
 - リレーIPはサーバvrf内にあります (最初のケースではGRTに対して行われたものと同様)。
- 多くのクライアントvrfがサポートされ、ルート漏出が不要なため、2番目のアプローチを選択する方が簡単です。

スイッチの設定 :

```

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

```

関連情報

- [RFC 3046](#)
- [RFC 3527](#)
- <https://docs.microsoft.com>
- [テクニカル サポートとドキュメント - Cisco Systems](#)