

# Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Configure](#)

[Network Diagram](#)

[Configurations](#)

[Verify](#)

[Related Cisco Support Community Discussions](#)

## Introduction

Since the introduction of Virtual Extensible LAN (VXLAN) and Cisco One Fabric (formerly Dynamic Fabric Automation (DFA)) providing DHCP services has begun to rely on DHCP Option 82 to inform the server of the proper address to provide to the client. This document shows how to configure Microsoft Windows Server 2012 to identify the information in the Option 82 fields to provide the proper address to the client

## Prerequisites

### Requirements

Cisco recommends you have a basic understanding of the following concepts before reading this article:

- VXLAN Ethernet VPN (EVPN) Configuration
- DHCP Relay Configuration
- Basic understanding of DHCP Services
- Configuring DHCP Services on Microsoft Windows Server 2012

### Components Used

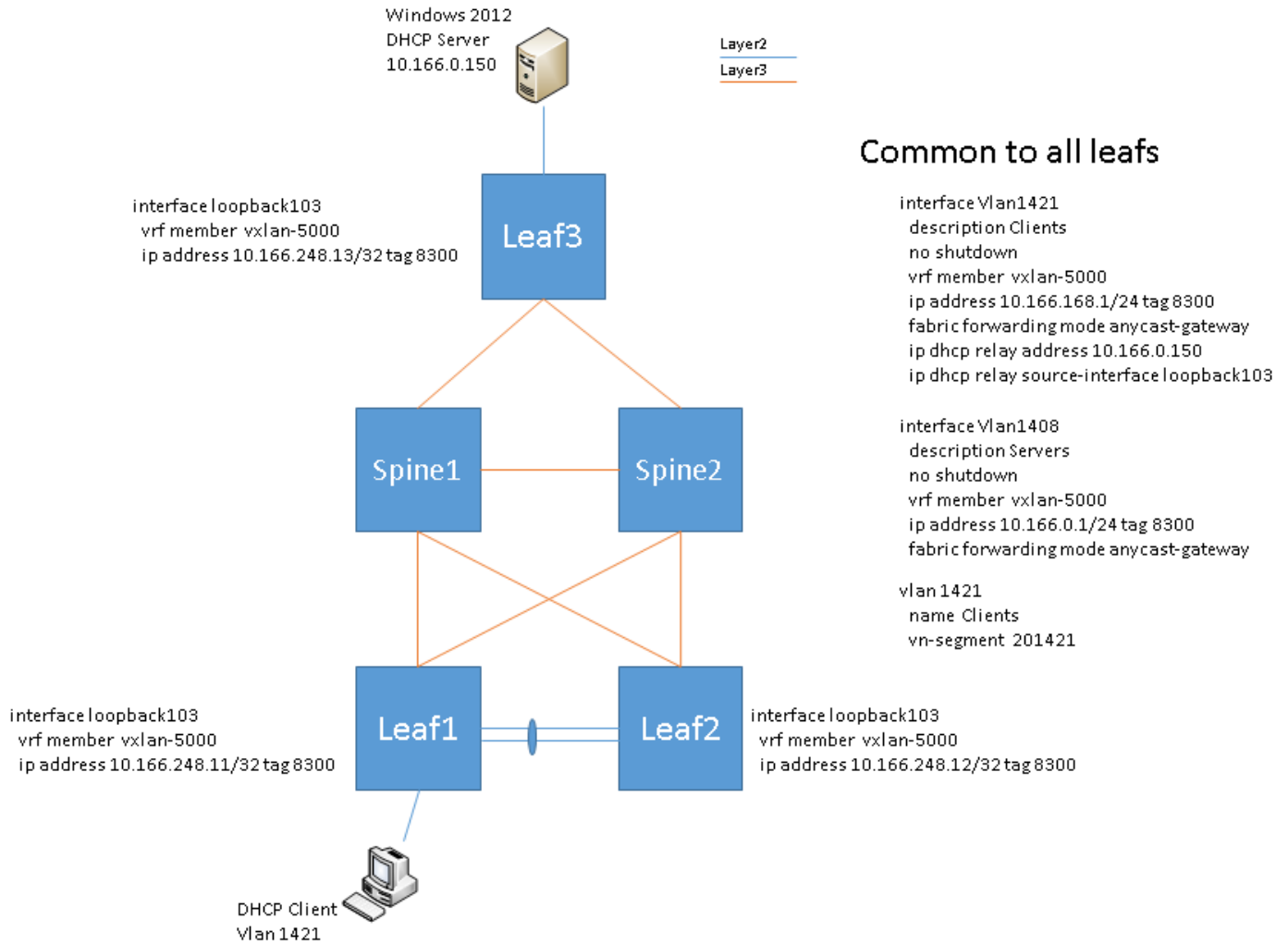
The information in this document is based on these software and hardware versions:

- Nexus 9300 and 9500 switches running 7.0(3)I1(2)
- Microsoft Windows Server 2012 R2

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Configure

# Network Diagram



The challenge here is that since every leaf switch shares the same vlan interface address in the client vlan a unique ip address is needed to be used to source the dhcp packets from. Hence we use the loopback address (103 in this case) to source the dhcp frames from.

From this image you can see that two fields are highlighted, the source and destination ip address of the frame and the relay agent ip address (also known as the gateway address or giaddress). This is the field that the Microsoft Windows Server uses to identify the scope/address pool to assign an address to the client. Since every vlan will be sourced from this loopback something else needs to be done to differentiate the subnets.

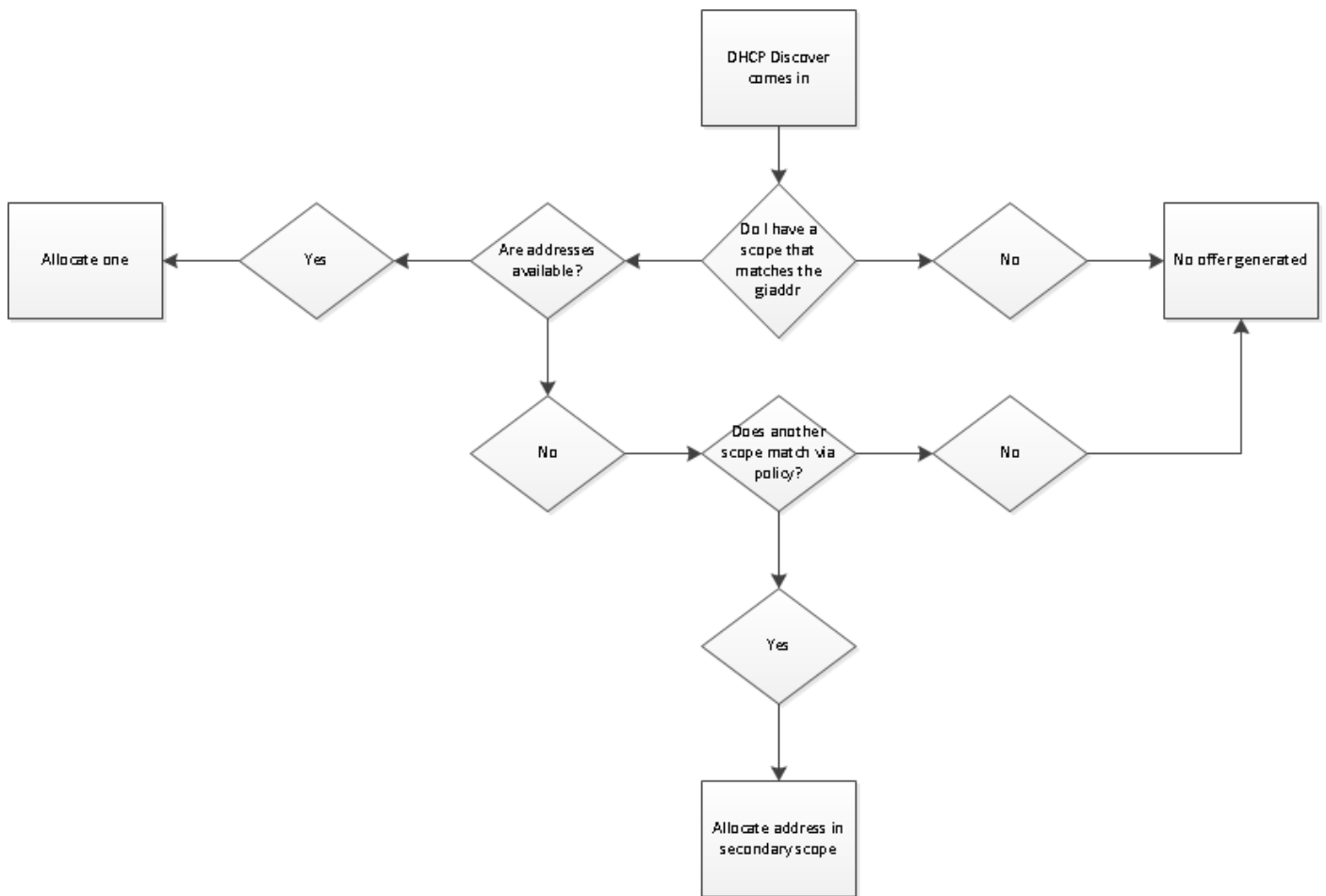
```
1084 366.051393 10.166.248.11 10.166.0.150 DHCP 390 DHCP Discover - Transaction ID 0x9290d377
1163 366.046936 10.166.0.150 10.166.248.11 DHCP 375 DHCP Offer - Transaction ID 0x9290d377
1165 366.048158 10.166.248.11 10.166.0.150 DHCP 416 DHCP Request - Transaction ID 0x9290d377
1166 366.048471 10.166.0.150 10.166.248.11 DHCP 380 DHCP ACK - Transaction ID 0x9290d377
```

```

# Frame 1084: 390 bytes on wire (3120 bits), 390 bytes captured (3120 bits) on interface 0
# Ethernet II, Src: Cisco_Ca:fi:777 (7c:0a:ce:ca:fi:777), Dst: Vmware_bc:51:a3 (00:50:56:bc:51:a3)
# Internet Protocol Version 4, Src: 10.166.248.11 (10.166.248.11), Dst: 10.166.0.150 (10.166.0.150)
# User Datagram Protocol, Src Port: 67 (67), Dst Port: 67 (67)
# Bootstrap Protocol (Discover)
  Message type: Boot Request (1)
  Hardware type: Ethernet (0x01)
  Hardware address length: 6
  Hops: 1
  Transaction ID: 0x9290d377
  Seconds elapsed: 0
# Bootp flags: 0x0000 (unicast)
  Client IP address: 0.0.0.0 (0.0.0.0)
  Your (client) IP address: 0.0.0.0 (0.0.0.0)
  Next server IP address: 0.0.0.0 (0.0.0.0)
  Relay agent IP address: 10.166.248.11 (10.166.248.11)
  Client MAC address: Vmware_bc:33:66 (00:50:56:bc:33:66)
  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: (61) Client identifier
# option: (50) Requested IP Address
# option: (12) Host Name
# option: (60) Vendor class identifier
# option: (55) Parameter Request List
# option: (82) Agent Information Option
# option: (255) End

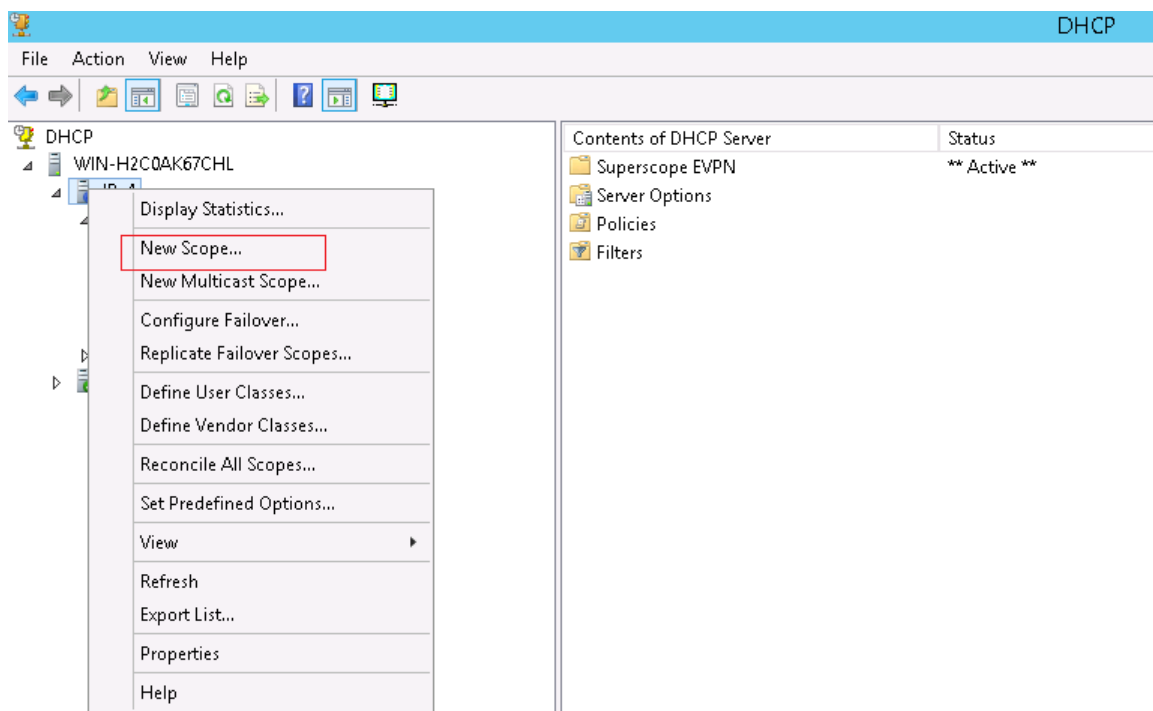
```

Here is the logic that Microsoft Windows 2012 uses to determine if an address is allocated.

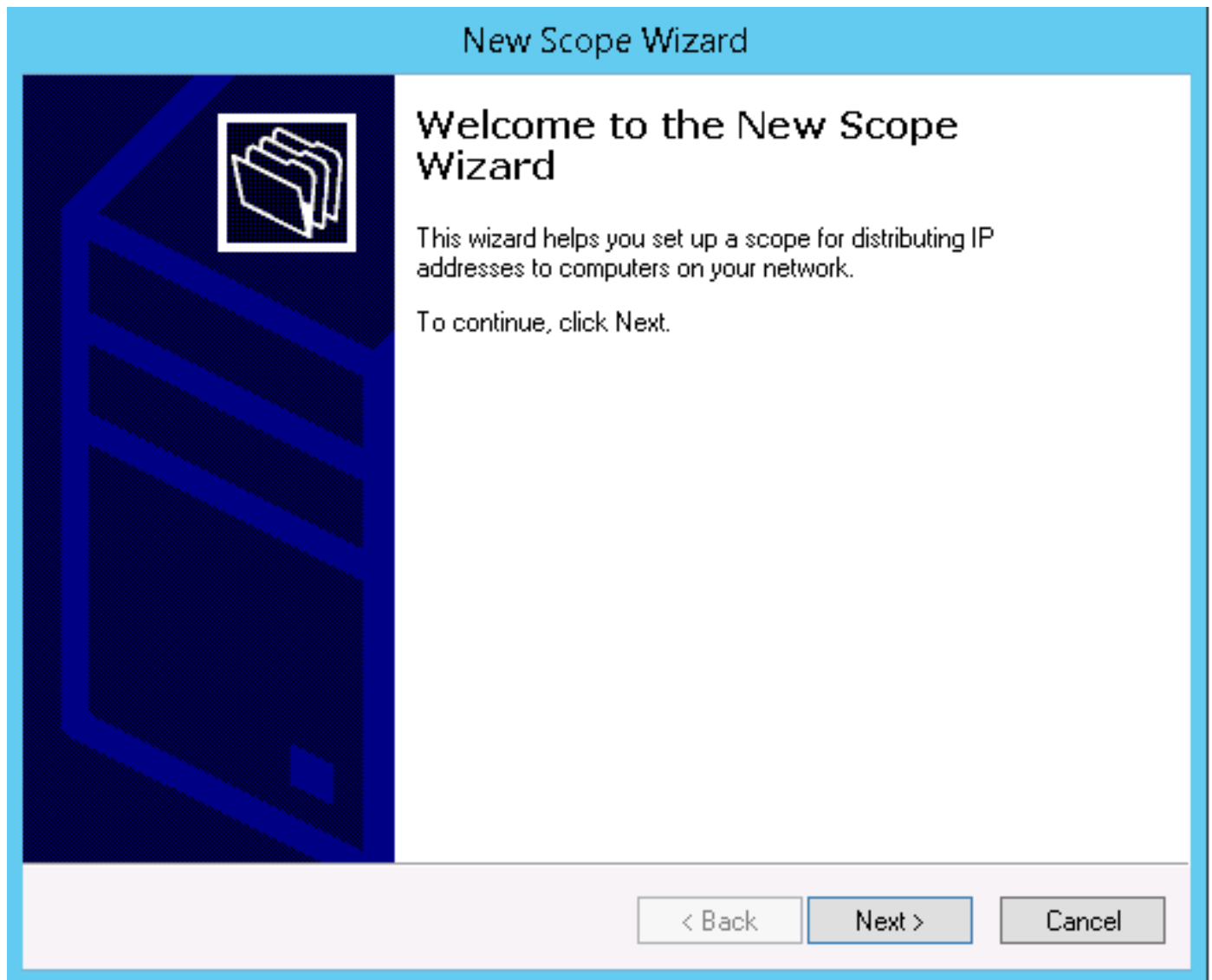


## Configurations

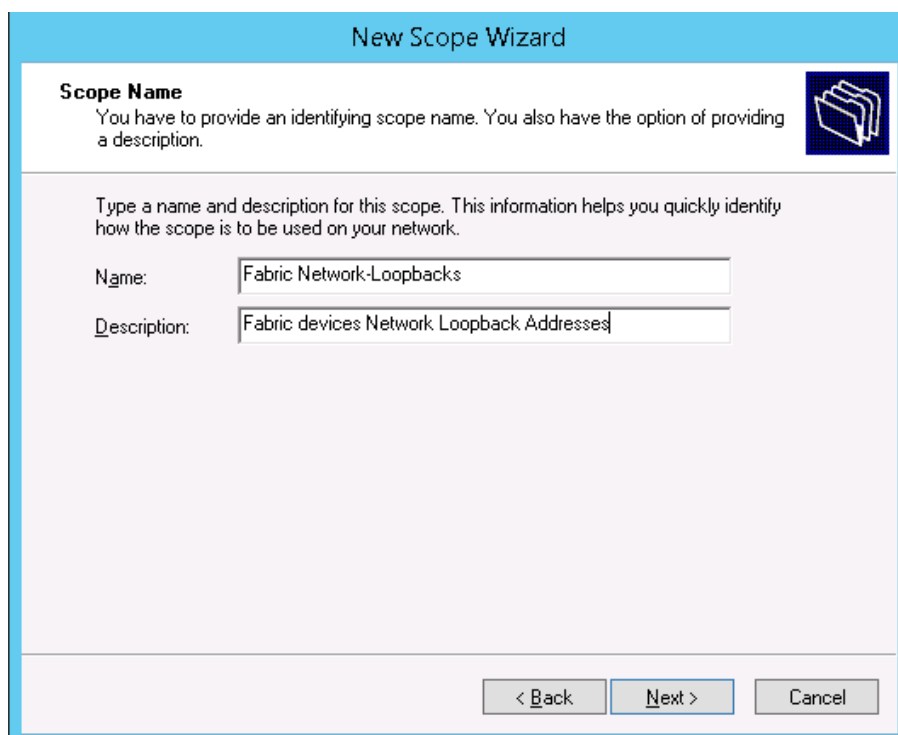
On the Microsoft Windows Server 2012 you first need to define a scope that covers the relay agent address. This is the only method the server uses to determine whether or not it can service this DHCP discover packet. If there's no address pool that matches the relay agent address then the server will not respond. So first you need to create the following scope:



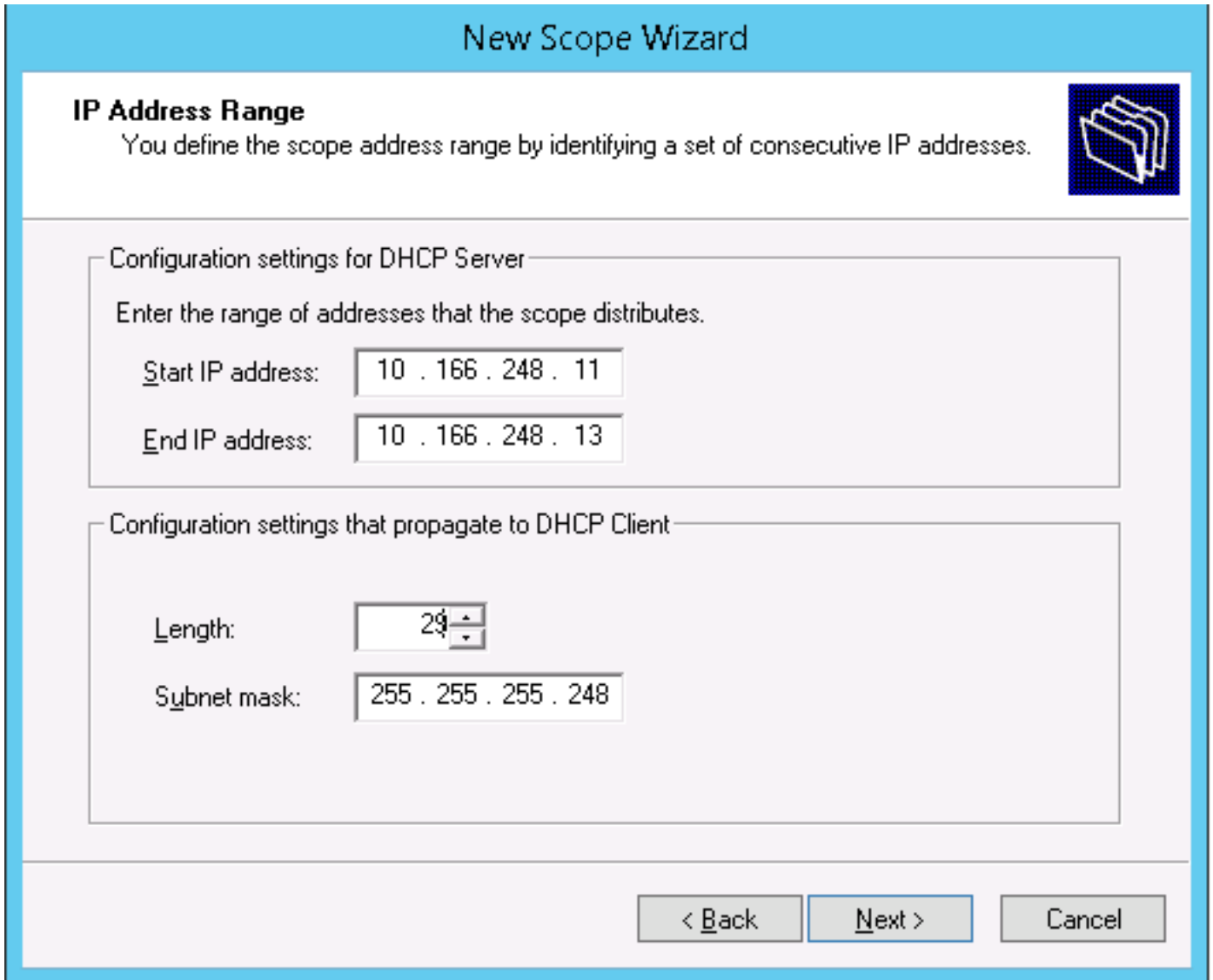
## Start creating the scope



## Name it appropriately



Choose an address range that will include the loopbacks of the switches which will be performing DHCP relay.



**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: 10 . 166 . 248 . 11

End IP address: 10 . 166 . 248 . 13

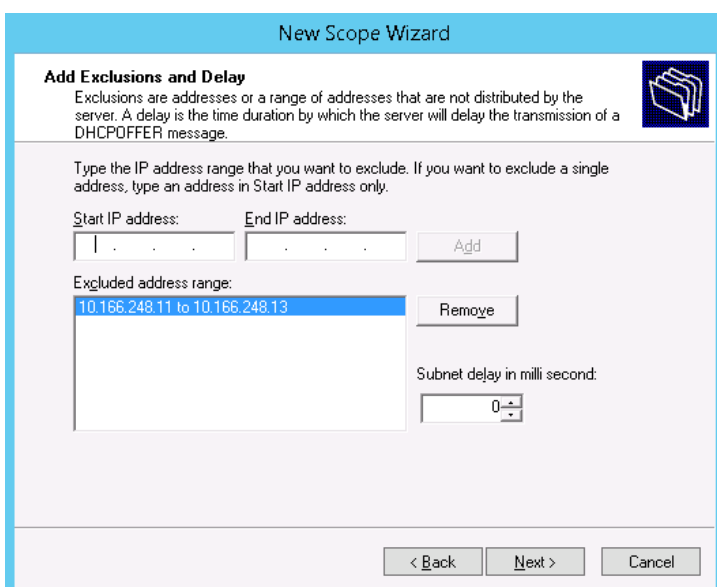
Configuration settings that propagate to DHCP Client

Length: 29

Subnet mask: 255 . 255 . 255 . 248

< Back   Next >   Cancel

Next be sure to exclude the addresses in this scope. It is important that there are no addresses available for the server to give out in this scope. If there are no addresses available in this scope this allows the server to look at other scopes and rules to service this dhcp request. This is one of the most important steps to make this work.



**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.

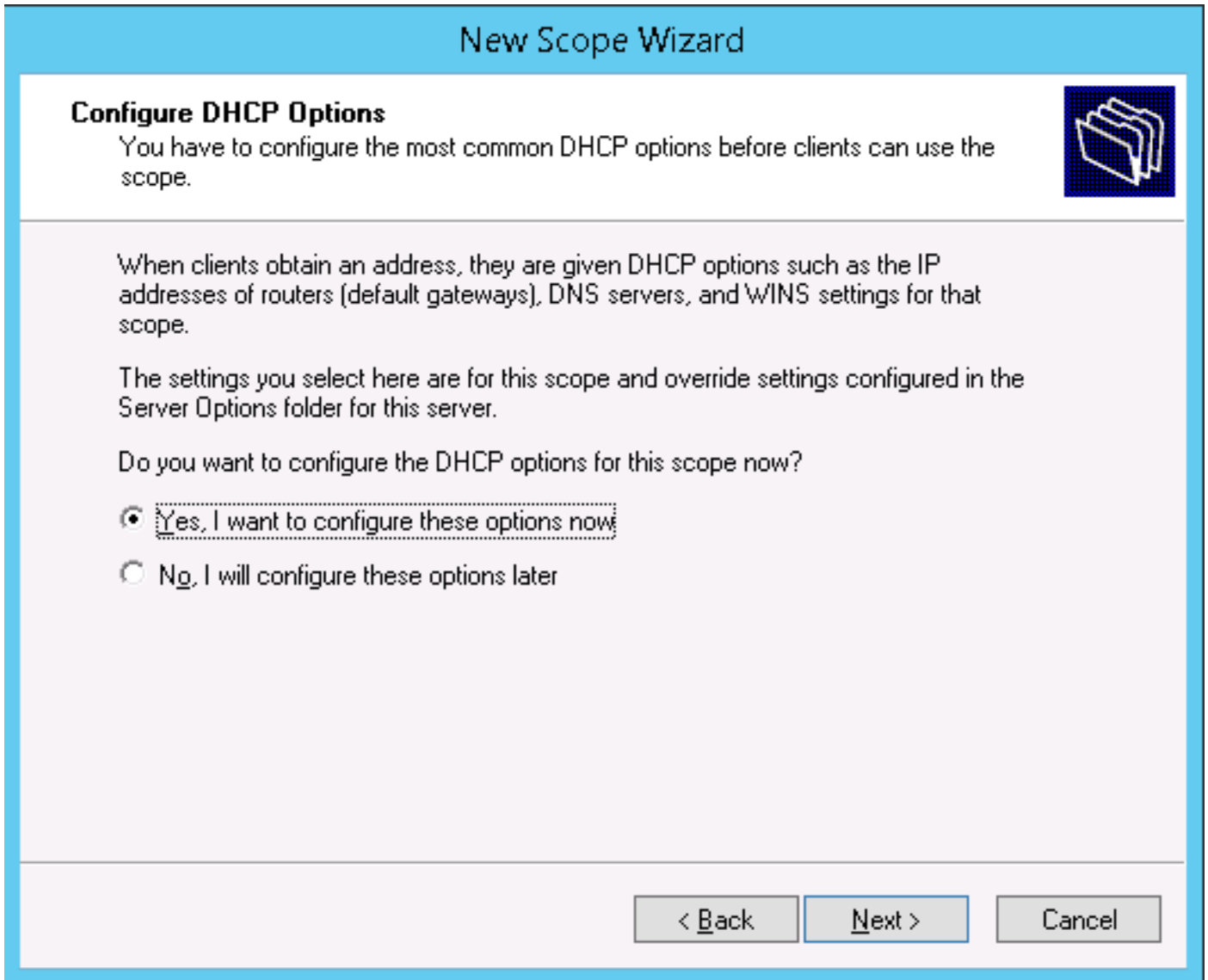
Start IP address: . . .   End IP address: . . .   Add

Excluded address range:  
10.166.248.11 to 10.166.248.13   Remove

Subnet delay in milli second: 0

< Back   Next >   Cancel

Click next until you get this screen. We need to configure one option in order to activate the scope.



**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.

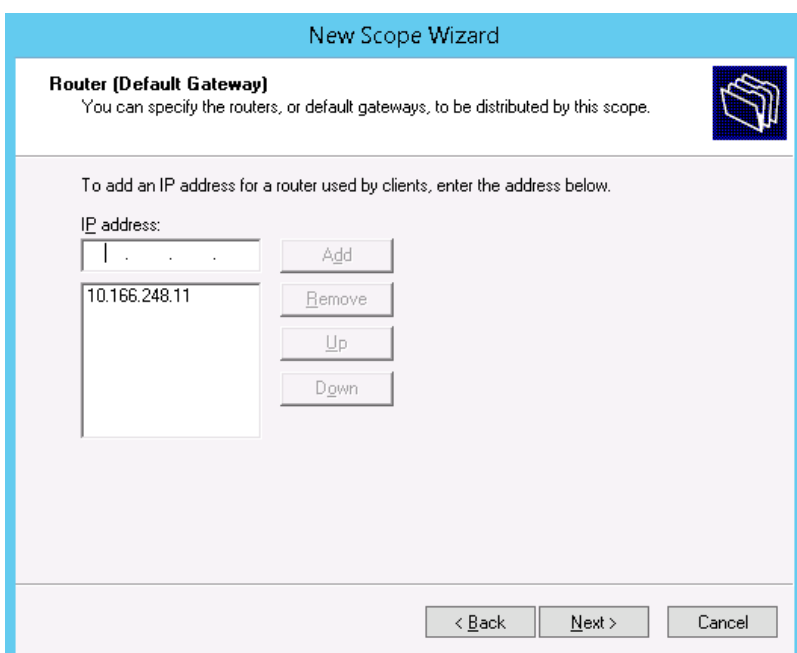
Do you want to configure the DHCP options for this scope now?

Yes, I want to configure these options now

No, I will configure these options later

< Back   Next >   Cancel

Add in any address inside the subnet to be the router. Without a default gateway the server won't let you activate the scope.



**New Scope Wizard**

**Router (Default Gateway)**  
You can specify the routers, or default gateways, to be distributed by this scope.

To add an IP address for a router used by clients, enter the address below.


IP address:

< Back   Next >   Cancel

Click next until you get to this screen and choose Yes and click next.

### 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

All done! Click finish.

### New Scope Wizard

**Completing the New Scope Wizard**



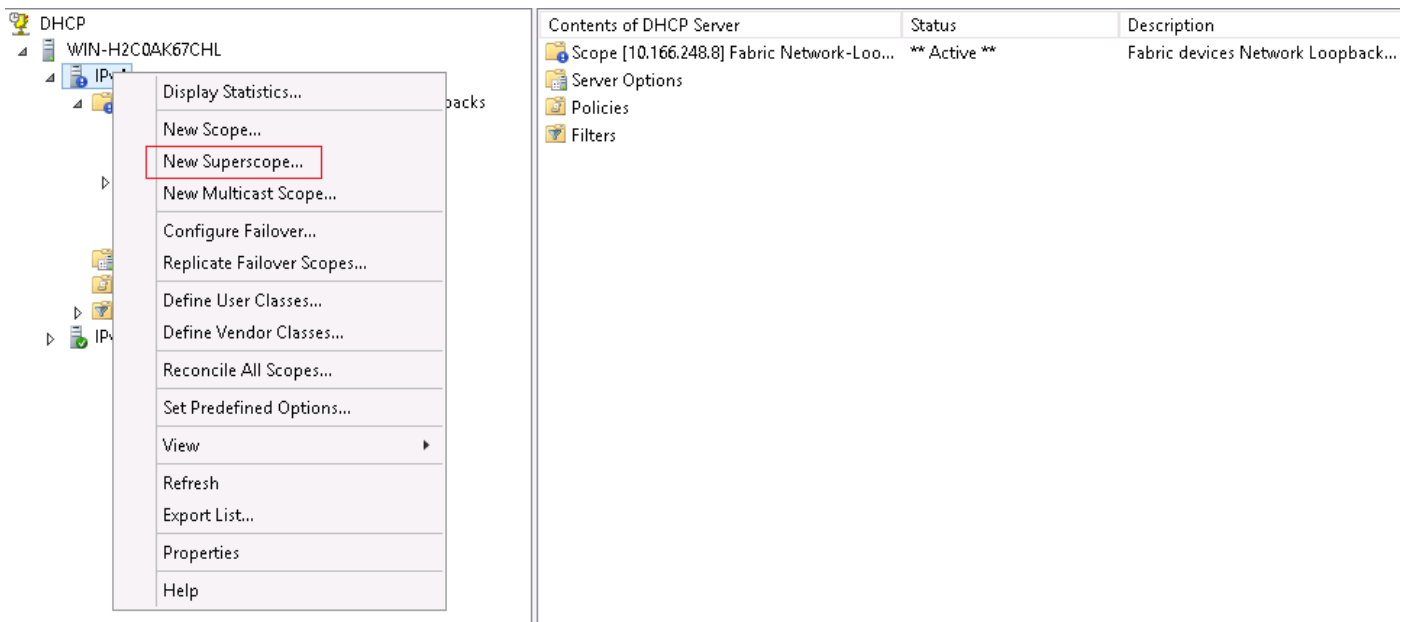
You have successfully completed the New Scope wizard.

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.

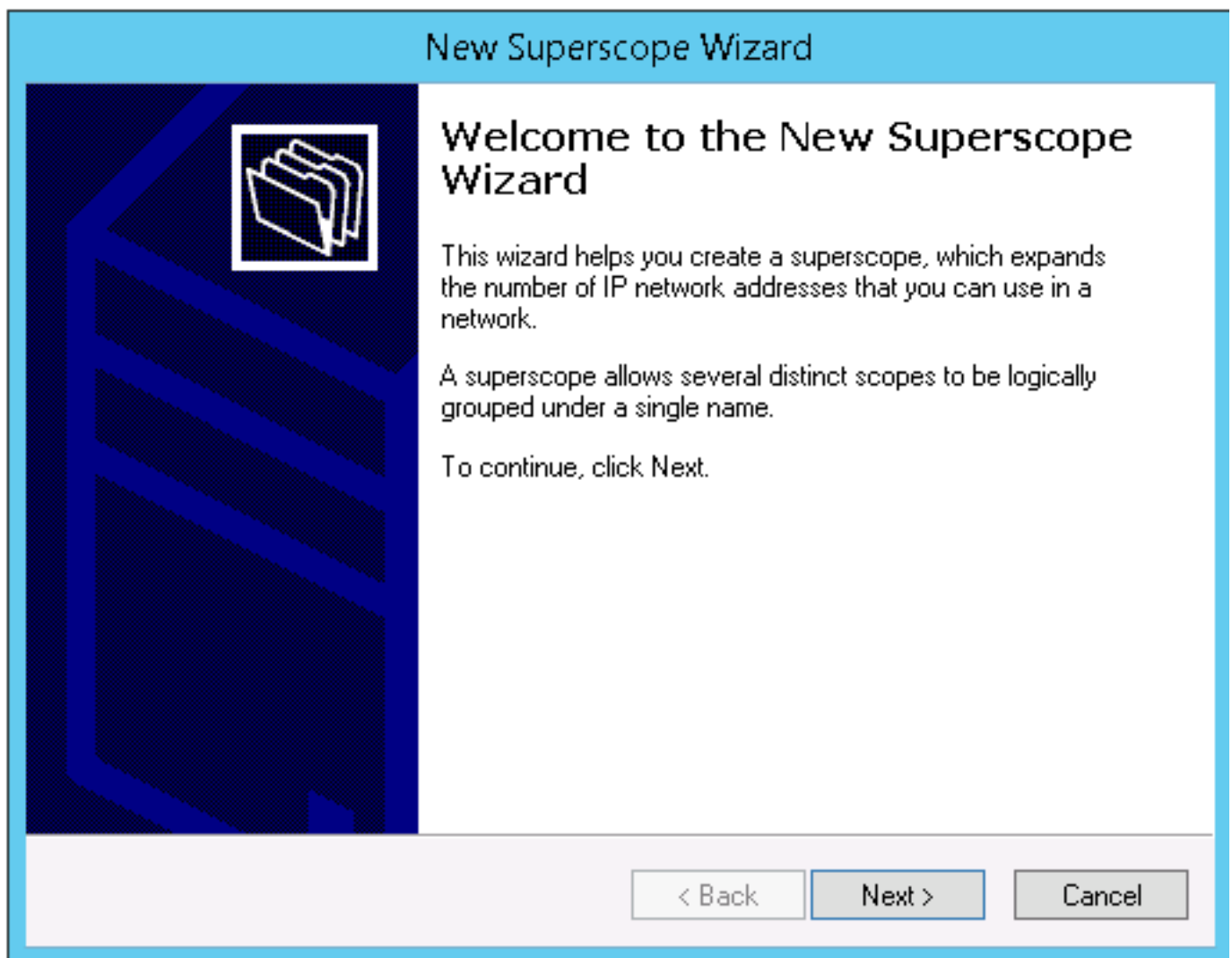
To close this wizard, click Finish.

< Back   Finish   Cancel

Now you need to create a superscope and add this scope to it.



Click Next to get started

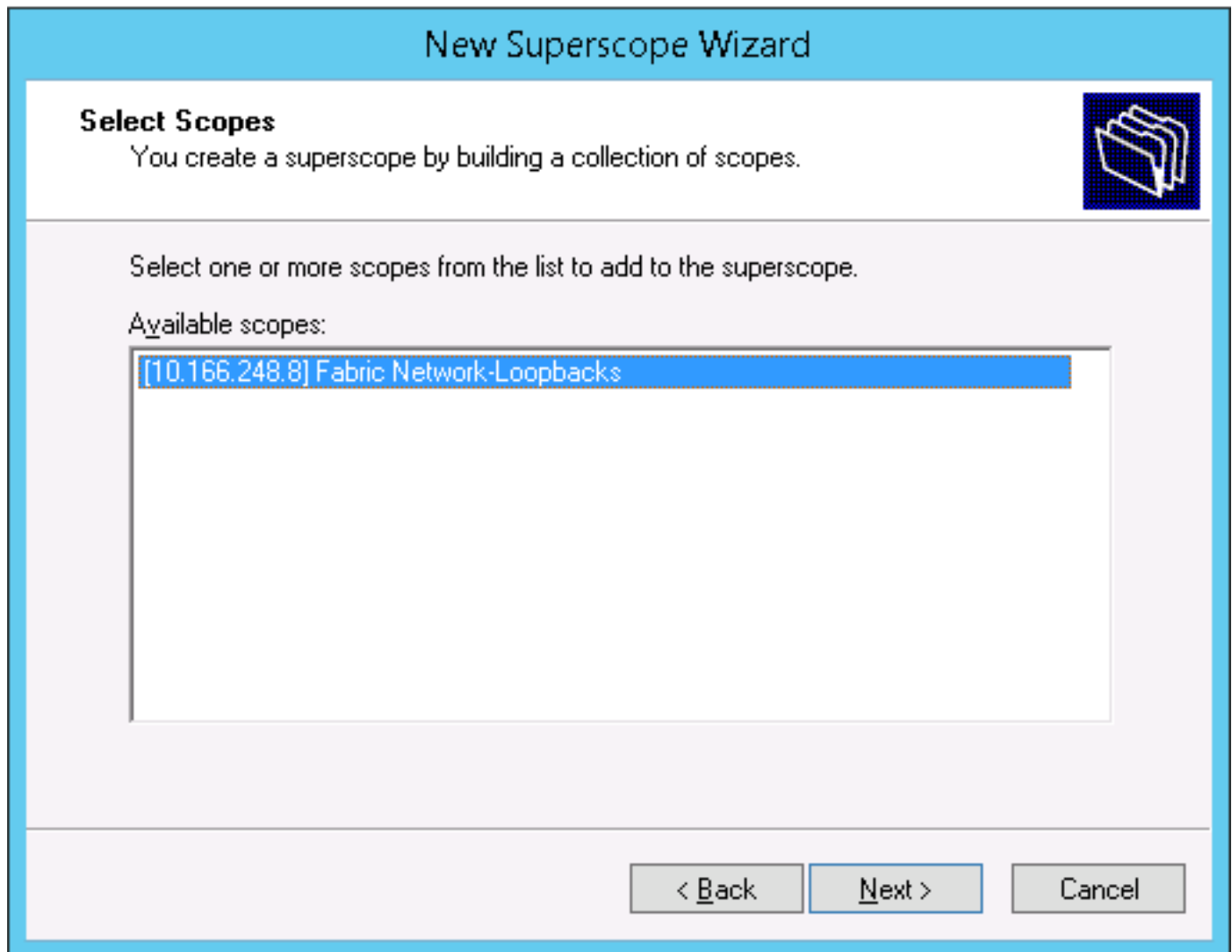


Name it appropriately



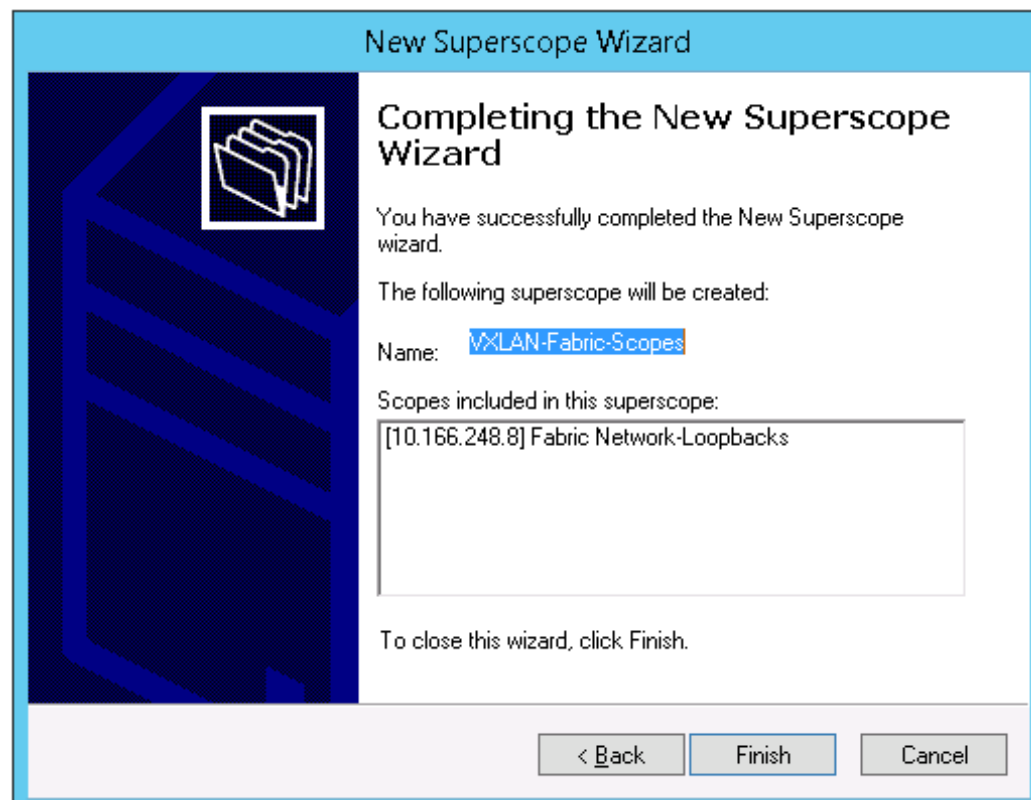


Select your newly created loopback scope to include in the new superscope.



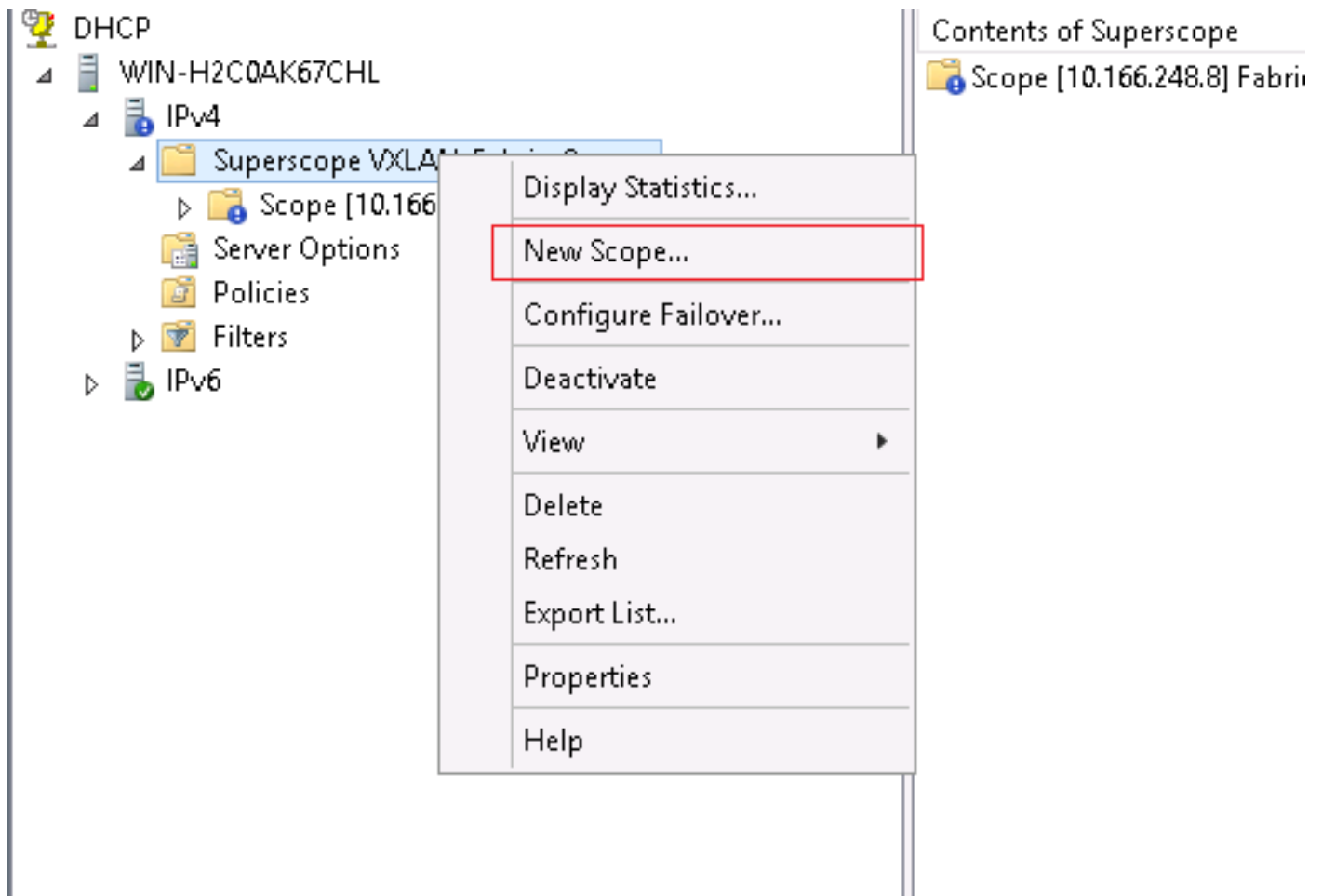
The screenshot shows the 'New Superscope Wizard' window. The title bar reads 'New Superscope Wizard'. The main heading is 'Select Scopes'. Below the heading is the instruction: 'You create a superscope by building a collection of scopes.' To the right of this text is a folder icon. Below the instruction, it says 'Select one or more scopes from the list to add to the superscope.' Underneath, it says 'Available scopes:' followed by a list box containing one item: '[10.166.248.8] Fabric Network-Loopbacks'. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

You're done. Click Finish.

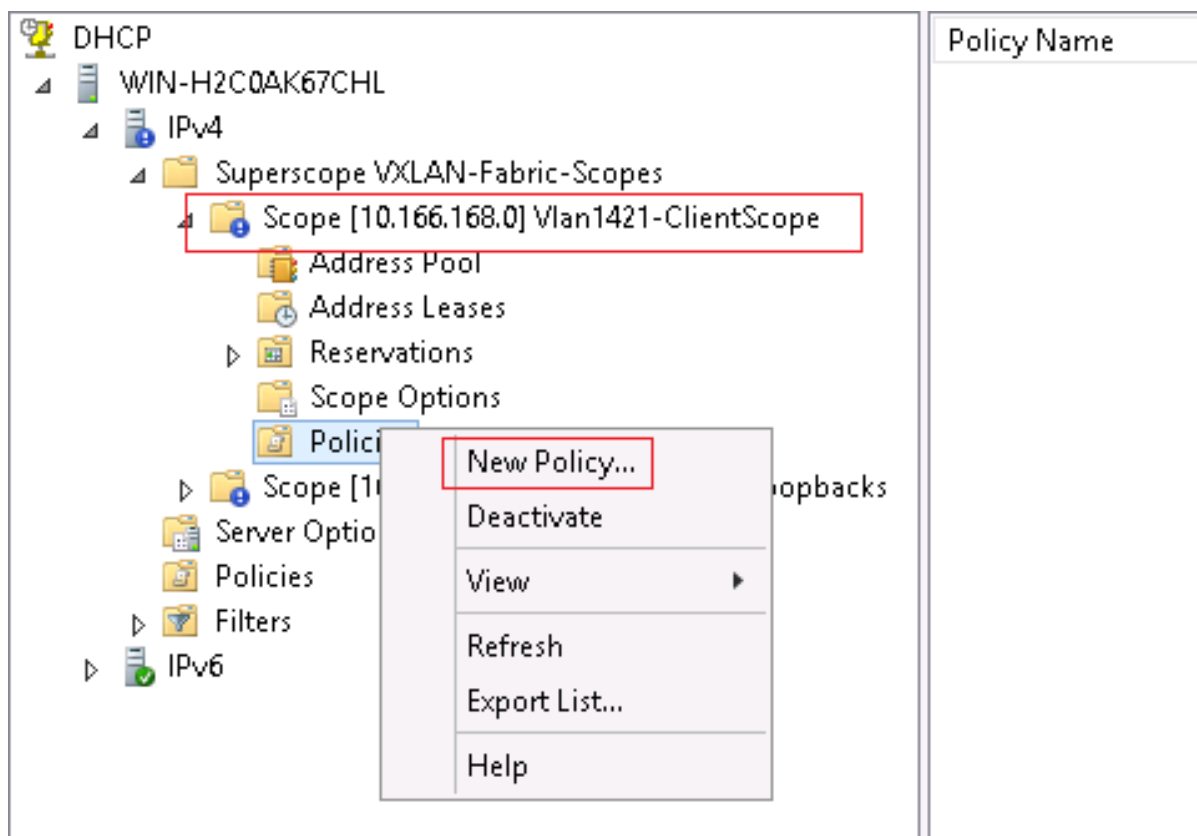


The screenshot shows the 'New Superscope Wizard' window at the completion stage. The title bar reads 'New Superscope Wizard'. The main heading is 'Completing the New Superscope Wizard'. To the left of the text is a large blue graphic with a folder icon. The text says: 'You have successfully completed the New Superscope wizard.' Below that, it says: 'The following superscope will be created:'. Then, 'Name: VXLAN-Fabric-Scopes'. Below that, it says: 'Scopes included in this superscope:' followed by a list box containing one item: '[10.166.248.8] Fabric Network-Loopbacks'. At the bottom, it says: 'To close this wizard, click Finish.' At the bottom of the window are three buttons: '< Back', 'Finish', and 'Cancel'.

Next you need to create a client scope. Create this scope normally as you would create any client scope except be sure to include it in the superscope like this:



After your scope is created now add the Option 82 information that allows the server to identify the correct scope. Expand your scope and go to policies and create a new policy.



Name it appropriately.

## 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:

Click Add to create your policy

## 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

**Choose Relay Agent Information and Equals. Then add the circuit ID as described below. This is how the server will determine the correct vlan to give the ip address to the client. Each vlan will have a unique circuit id as derived from the VN Segment ID. Click OK when finished.**

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

Criteria: Relay Agent Information

Operator: Equals

Value (in hex)

Relay Agent Information:

Agent Circuit ID: 01080006000312CD

Agent Remote ID:

Subscriber ID:

Prefix wildcard(\*)

Append wildcard(\*)

Ok Cancel

< Back Next > Cancel

## Leaf Configuration

```

vlan 1421
 name Clients
 vn-segment 201421
  
```

The Agent Circuit ID is derived from "0108000600" plus XXXXXX where XXXXXX is the six digit VN segment ID converted to hex.

201421 = 312CD. Since the number needs to always be six digits it becomes 0312CD for a total circuit ID of 01080006000312CD

Be sure to check the append wildcard box

**Click Next to move forward to custom options.**

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.

**i** 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	01080006000312CD*

AND  OR

Add... Edit... Remove

< Back Next > Cancel

You can configure a custom IP range by checking Yes and choosing a range of addresses or selecting No and letting it give any eligible address in the scope. For this scope I have chosen No to let it give the client any address in the scope.

The screenshot shows the 'Configure settings for the policy' step of the DHCP Policy Configuration Wizard. The title bar reads 'DHCP Policy Configuration Wizard'. Below the title, the section is titled 'Configure settings for the policy' with a sub-header: 'If the conditions specified in the policy match a client request, the settings will be applied.' A folder icon is visible in the top right corner. The main text explains that a scope can be subdivided into multiple IP address ranges and that clients matching the policy conditions will be issued an IP address from the specified range. It instructs the user to configure the start and end IP addresses for the range, noting they must be within the scope's boundaries. The current scope IP address range is shown as 10.166.168.1 - 10.166.168.254. It states that if an IP address range is not configured, policy clients will be issued an IP address from the scope range. A question asks 'Do you want to configure an IP address range for the policy:' with radio buttons for 'Yes' and 'No'. The 'No' option is selected. Below this are input fields for 'Start IP address:' and 'End IP address:', both containing three dots. A 'Percentage of IP address range:' field shows 'No valid range specified'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

You can also choose to override the options in the main scope for this policy if you wish. For this example there are no custom options.

This screenshot shows the 'Configure settings for the policy' step of the DHCP Policy Configuration Wizard, focusing on the 'Available Options' section. The title bar reads 'DHCP Policy Configuration Wizard'. The section is titled 'Configure settings for the policy' with a sub-header: 'If the conditions specified in the policy match a client request, the settings will be applied.' A folder icon is visible in the top right corner. The 'Vendor class' is set to 'DHCP Standard Options'. The 'Available Options' table is as follows:


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

Below the table is a 'Data entry' section with a 'Long' field containing the value '0x0'. At the bottom, there are three buttons: '< Back', 'Next >', and 'Cancel'.

Verify and click finish to create the policy.

### 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: Vlan1421 - Option 82 Policy  
Description: Vlan1421 - Option 82 Policy  
Conditions: OR of

Conditions	Operator	Value
Relay Agent Information - A...	Equals	01080006000312CD*

Settings:

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

< BackFinishCancel

Now you should see the clients start receiving IP addresses in the newly created scope.

If multiple DHCP Scopes are required for multiple subnets, you need to create one LoopbackX per subnet/vlan on all LEAFS and create a superscope with a loopbackX range scope and actual client IP subnet scope per vlan.

This is due to that MSFT DHCP server only assigns IP from secondary sub-scope after DHCP server found that there is no available IP in Loopback scoper under superscope.

So, if you have have VLAX X and VLAN Y and you need to two super-scopes, one with subnet X and loopback X and another one with subnet Y with loopback Y.

For example, there are two subnets, vlan 1601 and vlan 1602.

You need to create two Loopback with different address in same VRF and advertised into

## BGP.

```
interface loopback601
vrf member evpn-tenant-kk1
ip address 192.168.0.43/32
ip router ospf 1 area 0.0.0.4
```

```
interface loopback602
vrf member evpn-tenant-kk1
ip address 192.168.10.43/32
ip router ospf 1 area 0.0.0.41
```

```
router bgp 2
vrf evpn-tenant-kk1
address-family ipv4 unicast
network 192.168.0.43/32
network 192.168.10.43/32
advertise l2vpn evpn
```

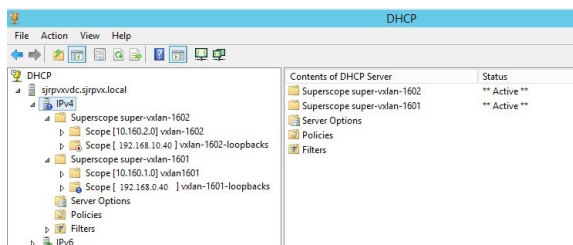
**Each VLAN uses different Loopback as DHCP relay source.**

```
interface Vlan1601
no shutdown
vrf member evpn-tenant-kk1
no ip redirects
ip address 10.160.1.254/24
no ipv6 redirects
fabric forwarding mode anycast-gateway
ip dhcp relay address 10.160.2.253
ip dhcp relay source-interface loopback601
```

```
interface Vlan1602
no shutdown
vrf member evpn-tenant-kk1
no ip redirects
ip address 10.160.2.254/24
no ipv6 redirects
fabric forwarding mode anycast-gateway
ip dhcp relay address 10.160.2.253
ip dhcp relay source-interface loopback602
```

**Then, I have to create two superscopes for vlan 1601 and vlan 1602 with different loopback IP ranges.**

**Without these config, HOSTs in vlan 1601 and 1602 always get IP from one scope.**



# Verify

Running Wireshark on our server we can see that offer is being given out on the correct subnet.

No.	Time	Source	Destination	Protocol	Length	Info
1779	5180.63275	10.166.248.11	10.166.0.150	DHCP	390	DHCP Discover - Transaction ID 0x9cf43ca7
1780	5182.07221	10.166.0.150	10.166.248.11	DHCP	375	DHCP offer - Transaction ID 0x9cf43ca7
1781	5182.07375	10.166.248.11	10.166.0.150	DHCP	416	DHCP Request - Transaction ID 0x9cf43ca7
1783	5182.07485	10.166.0.150	10.166.248.11	DHCP	380	DHCP ACK - Transaction ID 0x9cf43ca7

Frame 1780: 375 bytes on wire (3000 bits), 375 bytes captured (3000 bits) on interface 0	
Ethernet II, Src: Vmware_bc:51:a3 (00:50:56:bc:51:a3), Dst: 02:00:69:69:96:96 (02:00:69:69:96:96)	
Internet Protocol Version 4, Src: 10.166.0.150 (10.166.0.150), Dst: 10.166.248.11 (10.166.248.11)	
User Datagram Protocol, Src Port: 67 (67), Dst Port: 67 (67)	
Bootstrap Protocol (offer)	
Message type: Boot Reply (2)	
Hardware type: Ethernet (0x01)	
Hardware address length: 6	
Hops: 0	
Transaction ID: 0x9cf43ca7	
Seconds elapsed: 0	
Bootp flags: 0x0000 (Unicast)	
Client IP address: 0.0.0.0 (0.0.0.0)	
Your (client) IP address: 10.166.168.3 (10.166.168.3)	
Next server IP address: 10.166.0.150 (10.166.0.150)	
Relay agent IP address: 10.166.248.11 (10.166.248.11)	
Client MAC address: Vmware_bc:33:66 (00:50:56:bc:33:66)	
Client hardware address padding: 00000000000000000000	
Server host name not given	
Boot file name not given	
Magic cookie: DHCP	
Option: (53) DHCP Message Type (offer)	
Option: (1) Subnet Mask	
Option: (58) Renewal Time Value	
Option: (59) Rebinding Time value	
Option: (51) IP Address Lease Time	
Option: (54) DHCP Server Identifier	
Option: (3) Router	
Option: (6) Domain Name Server	
Option: (82) Agent Information option	
Length: 45	
Option 82 Suboption: (1) Agent Circuit ID	
Length: 10	
Agent Circuit ID: 01080006000312cd000b	
Option 82 Suboption: (2) Agent Remote ID	
Length: 6	
Agent Remote ID: 7c0ecec177	
Option 82 Suboption: (151) VRF name/VPN ID	
Length: 11	
VRF name:	
Option 82 Suboption: (11) Server ID override	
Length: 4	
Server ID override: 10.166.168.1 (10.166.168.1)	
Option 82 Suboption: (5) Link selection	
Length: 4	
Link selection: 10.166.168.0 (10.166.168.0)	
Option: (255) End	

Client's IP address from client subnet

Agent Circuit ID