Contents

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

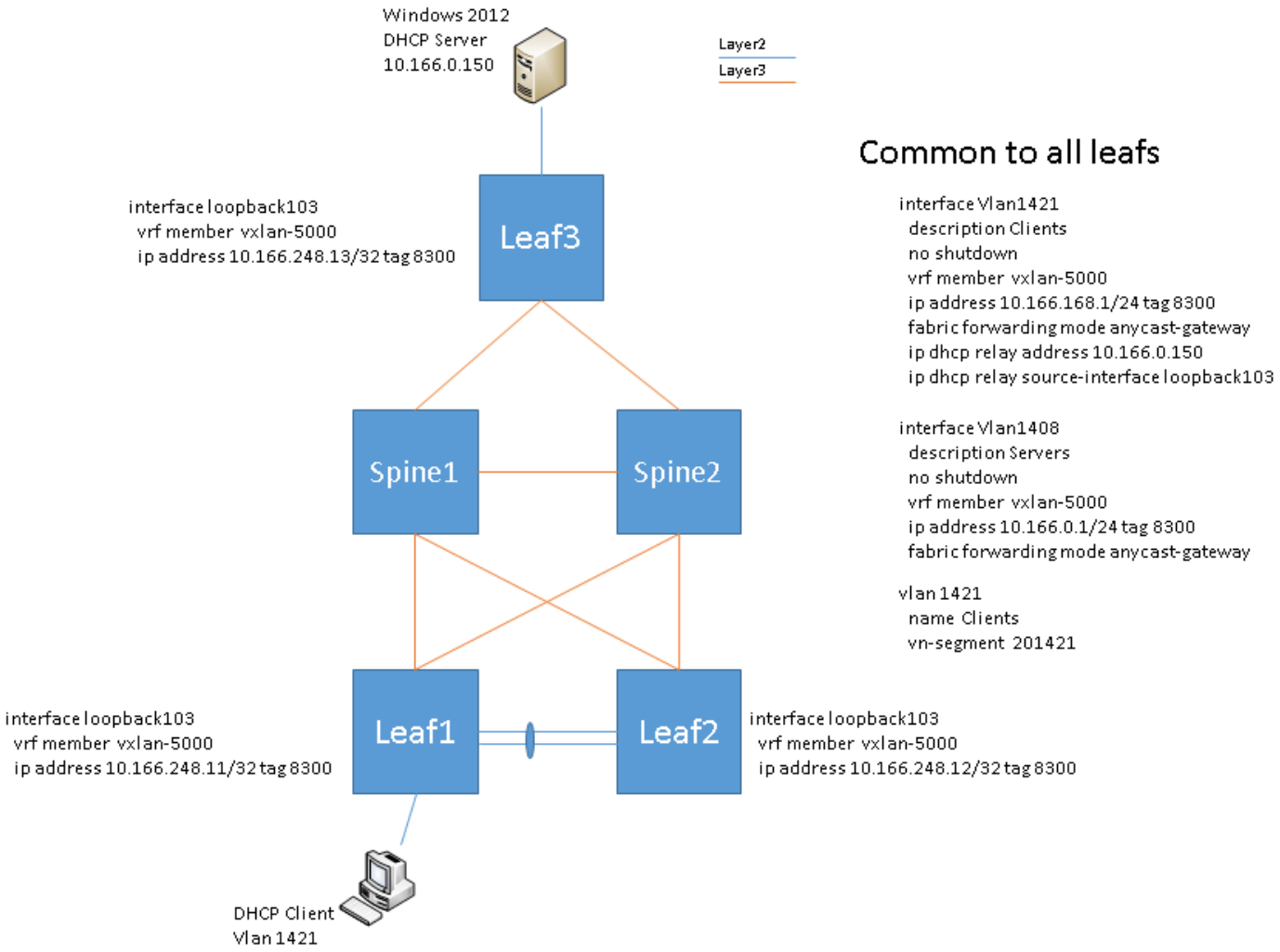
The information in this document is based on these software and hardware versions:

- 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.

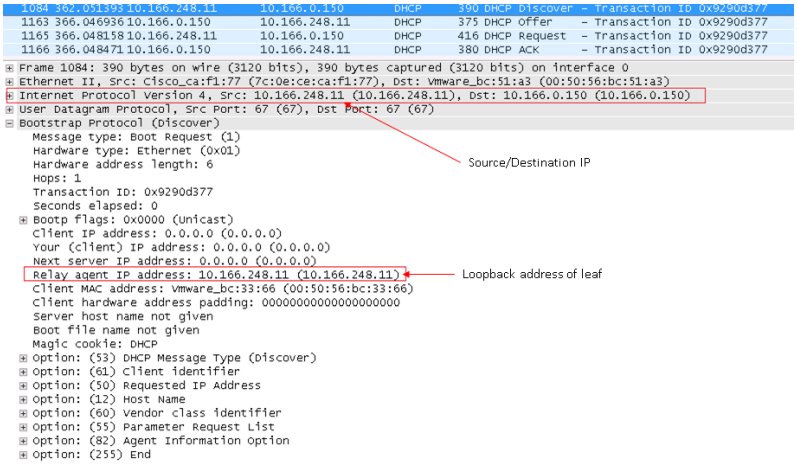
Configure

Network Diagram

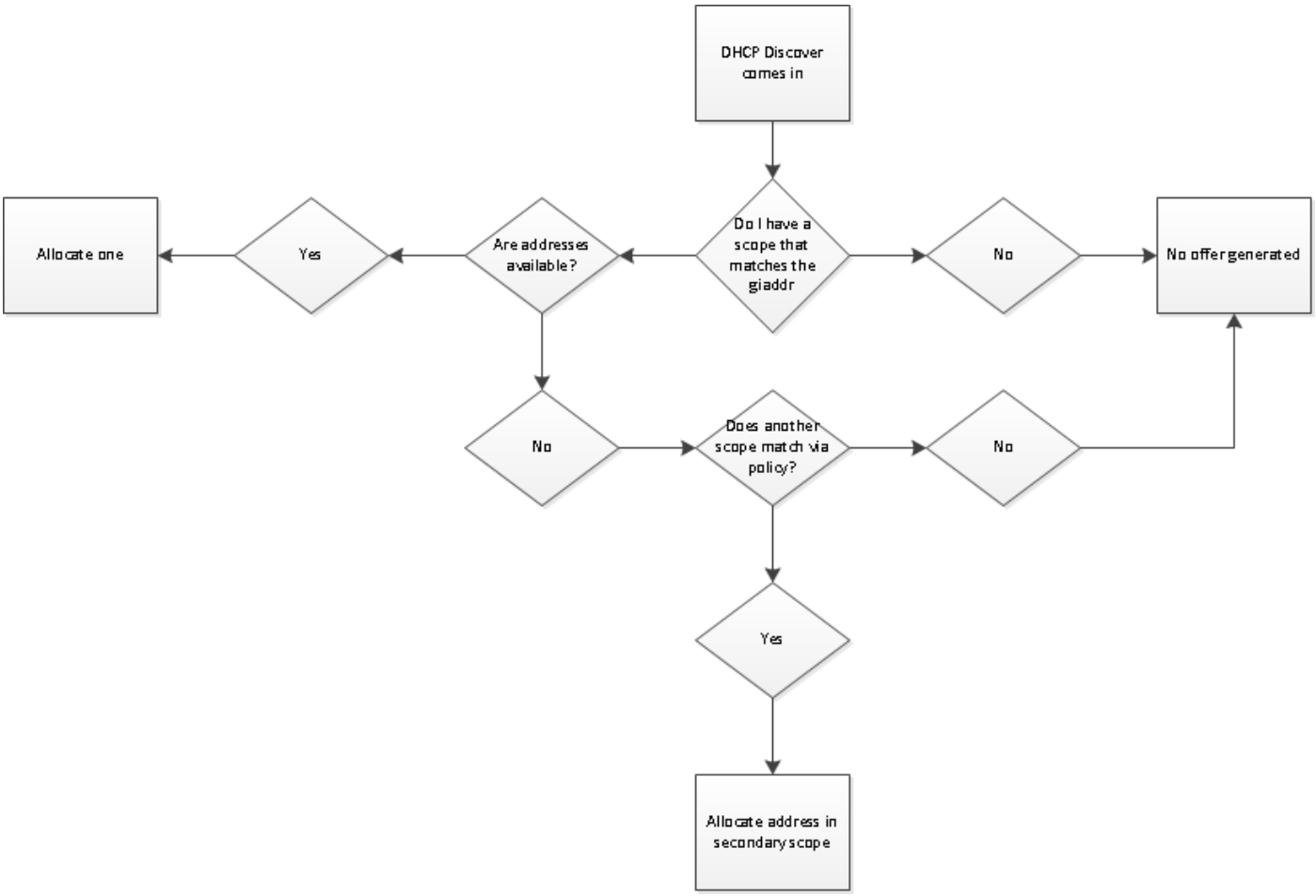


The challenge here is that since every leaf switch shares the same vlan interface address in the client vlan a unique ip address is needed to be used to source the dhcp packets from. Hence we use the loopback address (103 in this case) to source the dhcp relay frames from.

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.

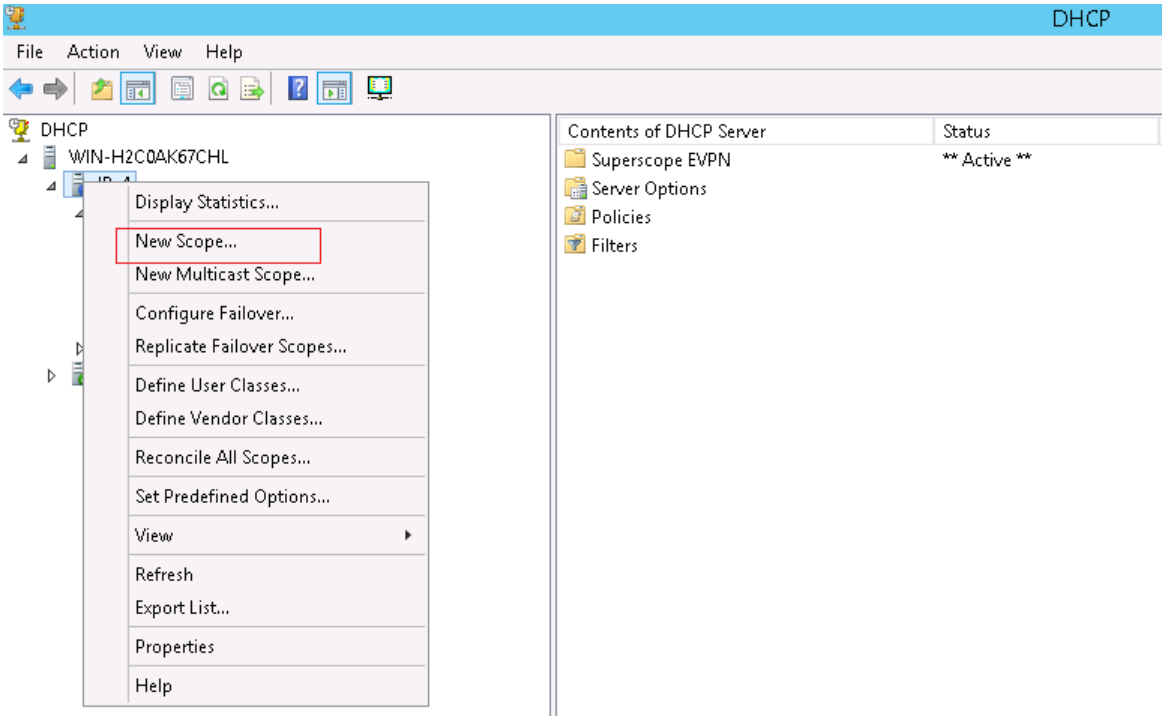


Here is the logic that Microsoft Windows 2012 uses to determine if an address is allocated.

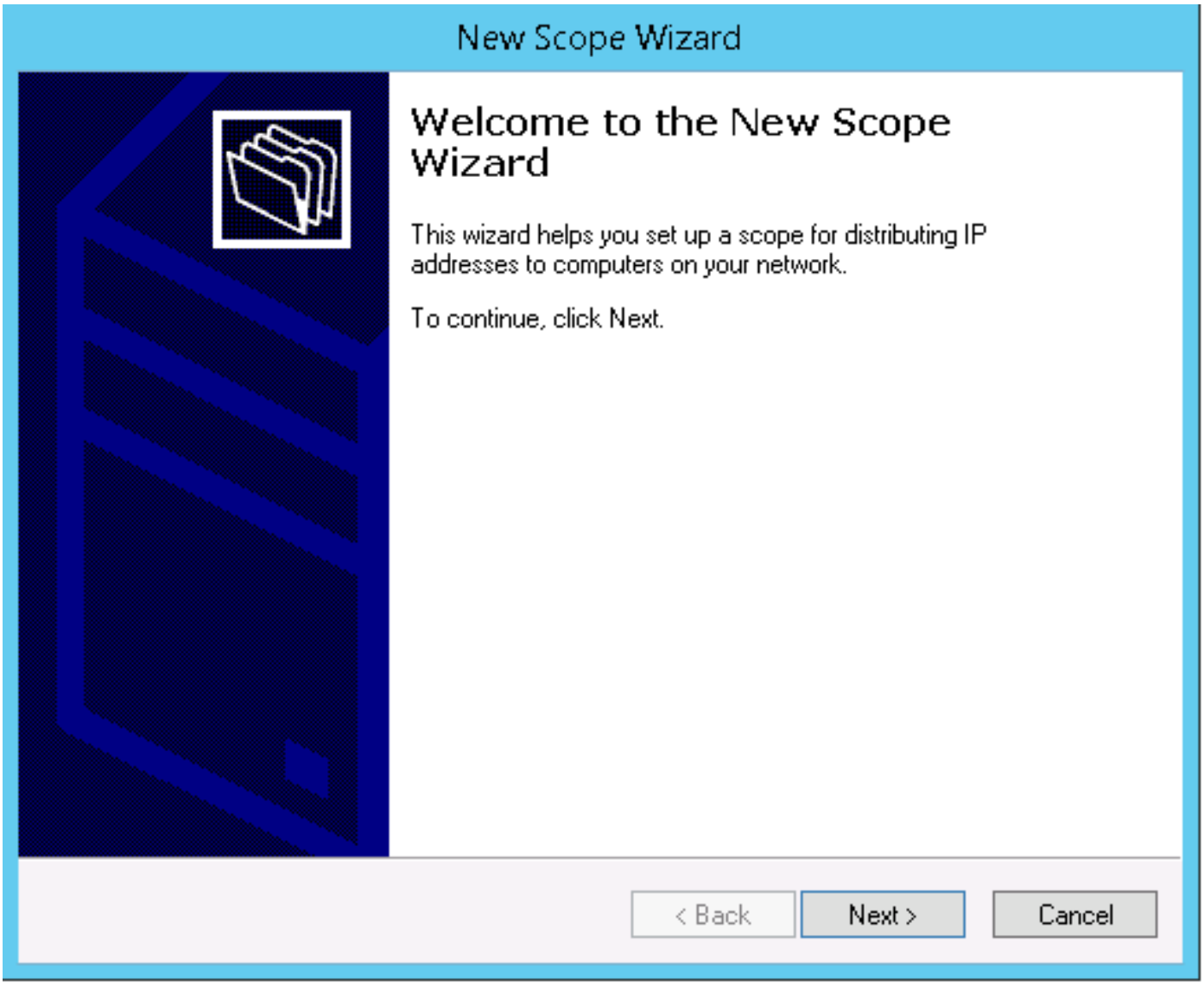


Configurations

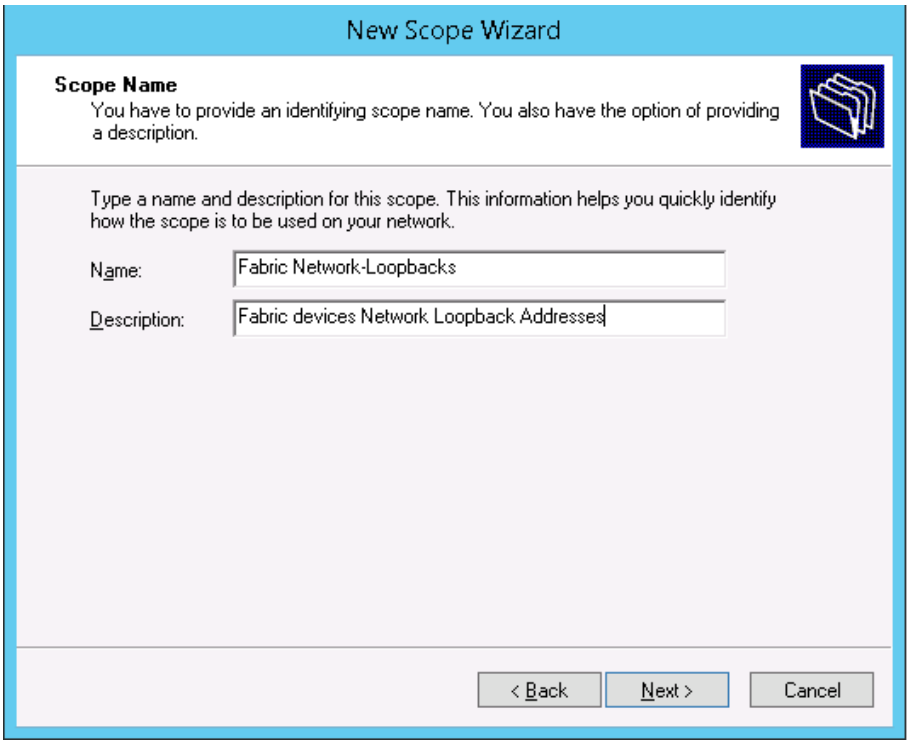
On the Microsoft Windows Server 2012 you first need to define a scope that covers the relay agent address. This is the only method the server uses to determine whether or not it can service this DHCP discover packet. If there's no address pool that matches the relay agent address then the server will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



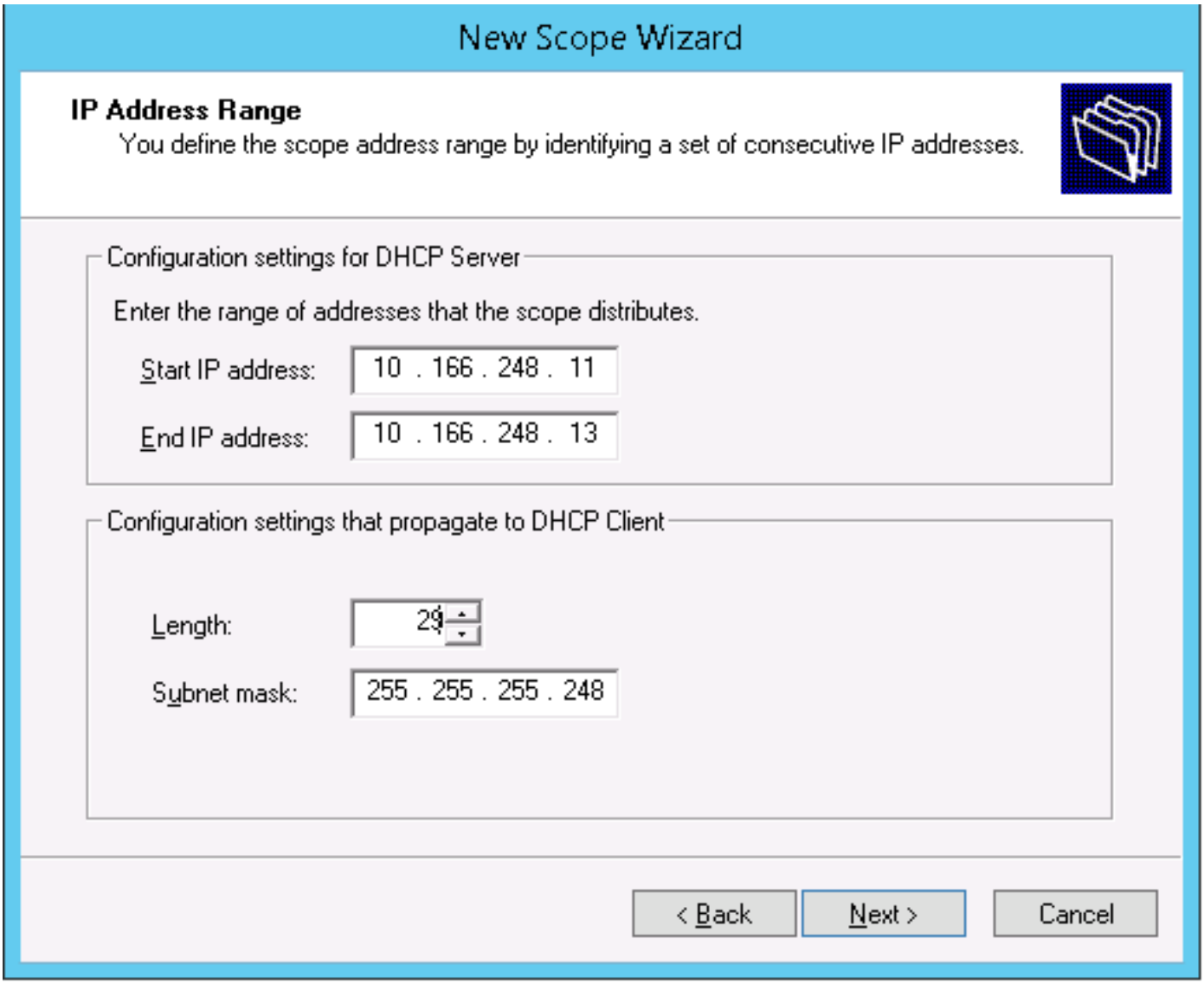
Start creating the scope



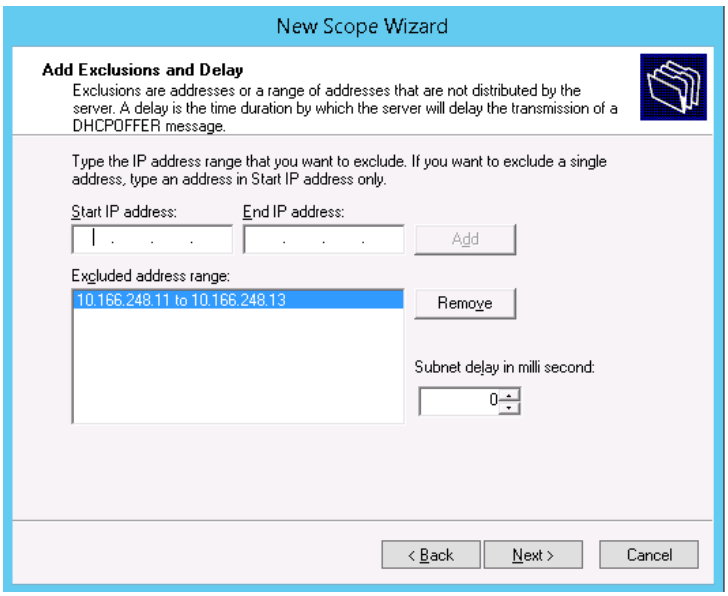
Name it appropriately



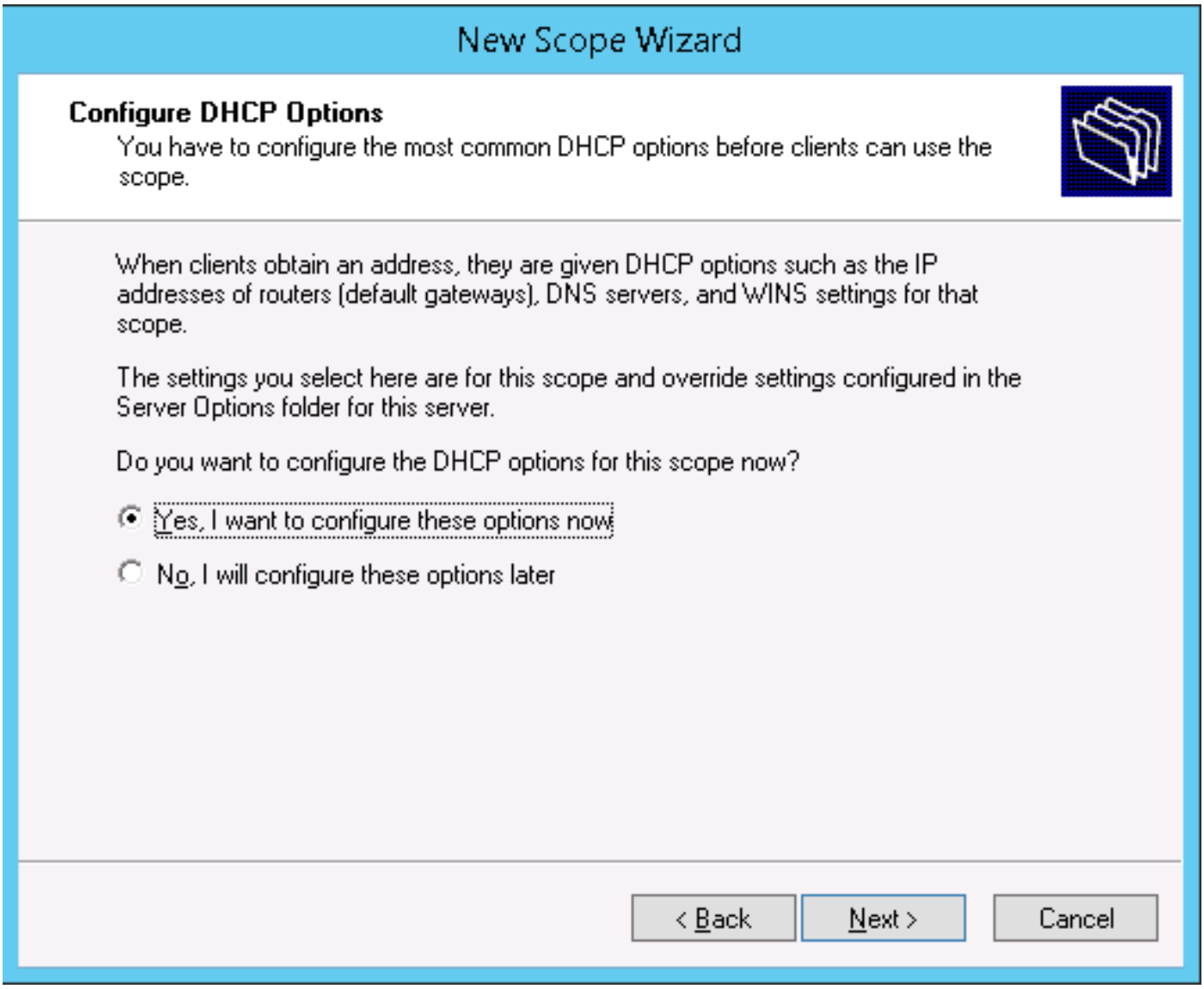
Choose an address range that will include the loopbacks of the switches which will be performing DHCP relay.



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.

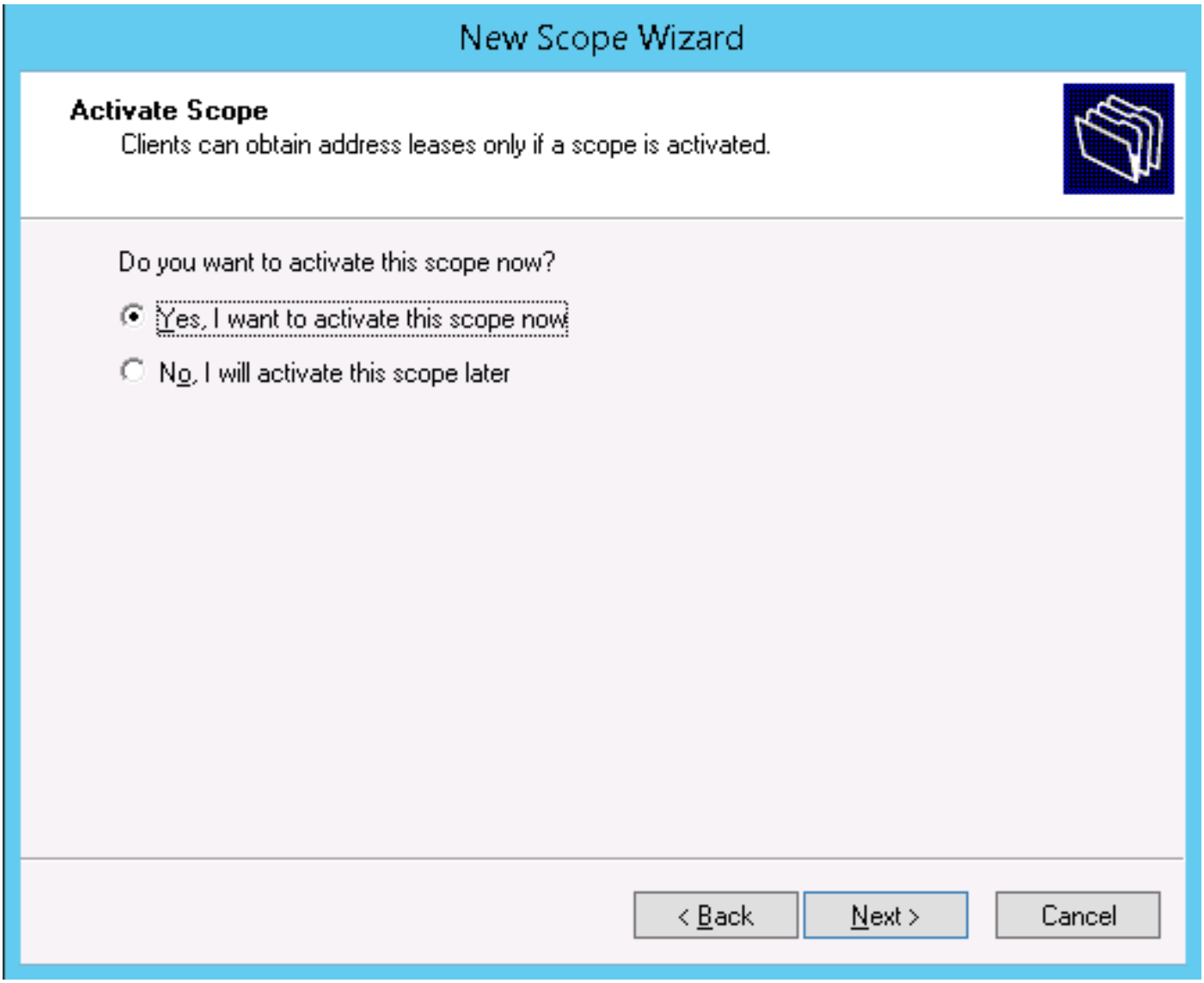


Click next until you get this screen. We need to configure one option in order to activate the scope.

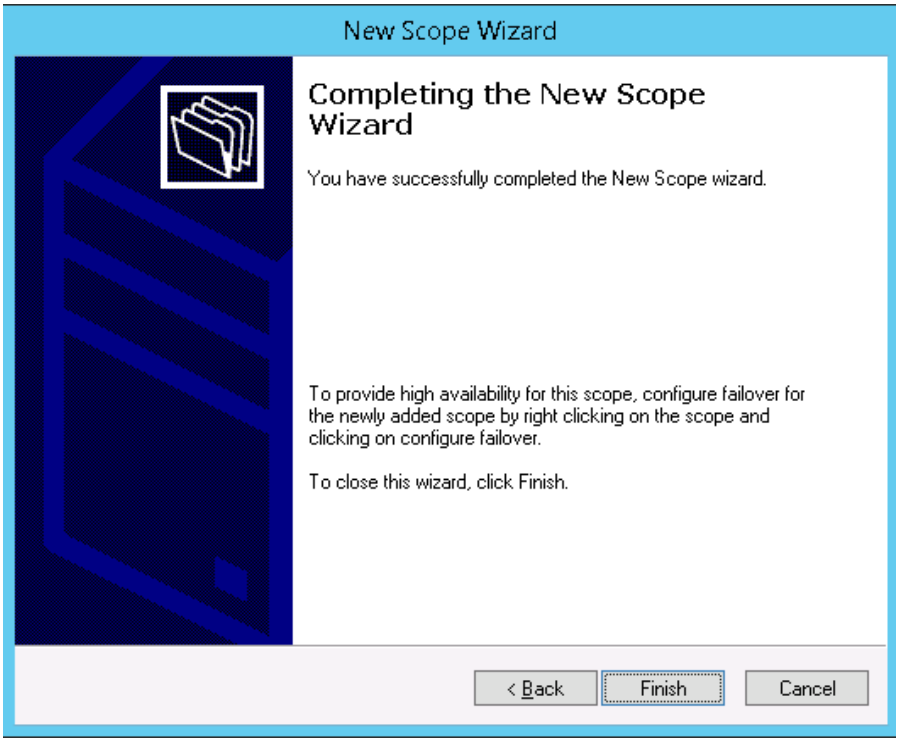


Add in any address inside the subnet to be the router. Without a default gateway the server won't let you activate the scope.

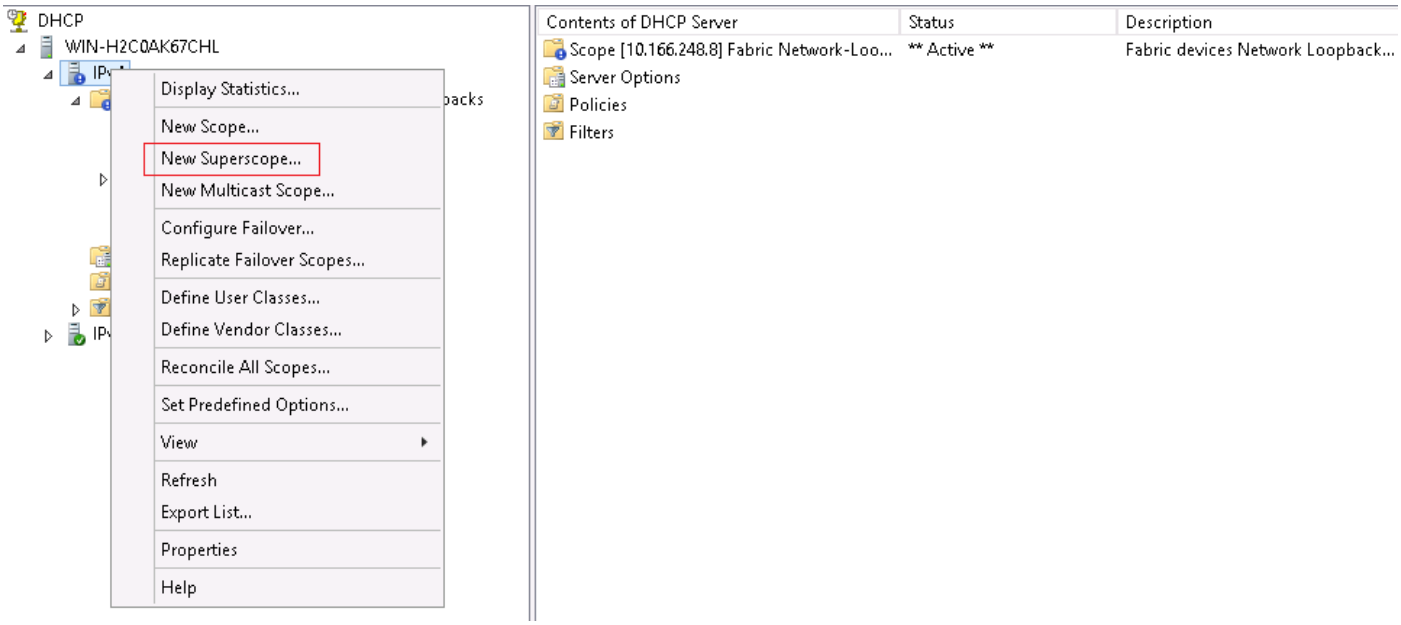
Click next until you get to this screen and choose Yes and click next.



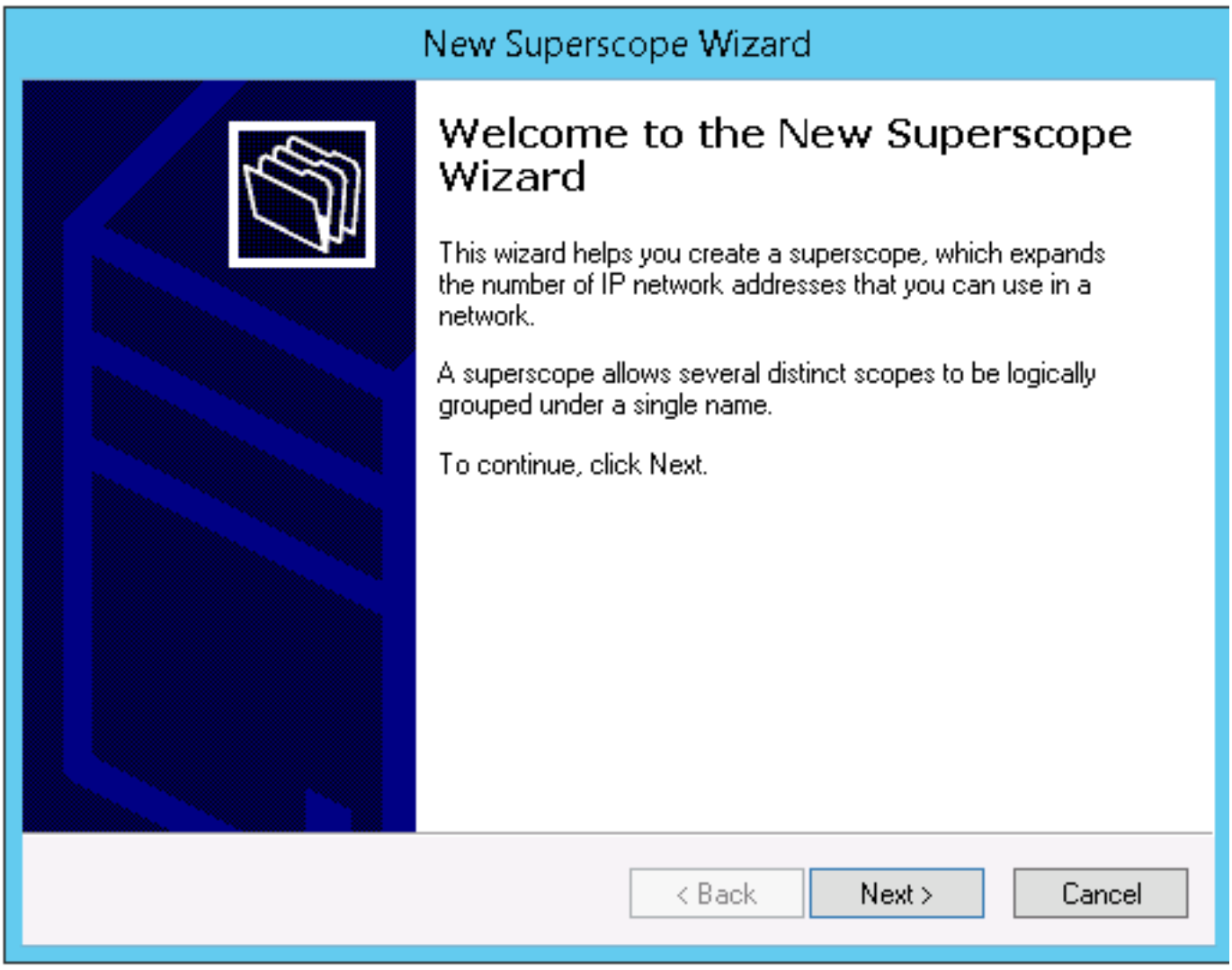
All done! Click finish.



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

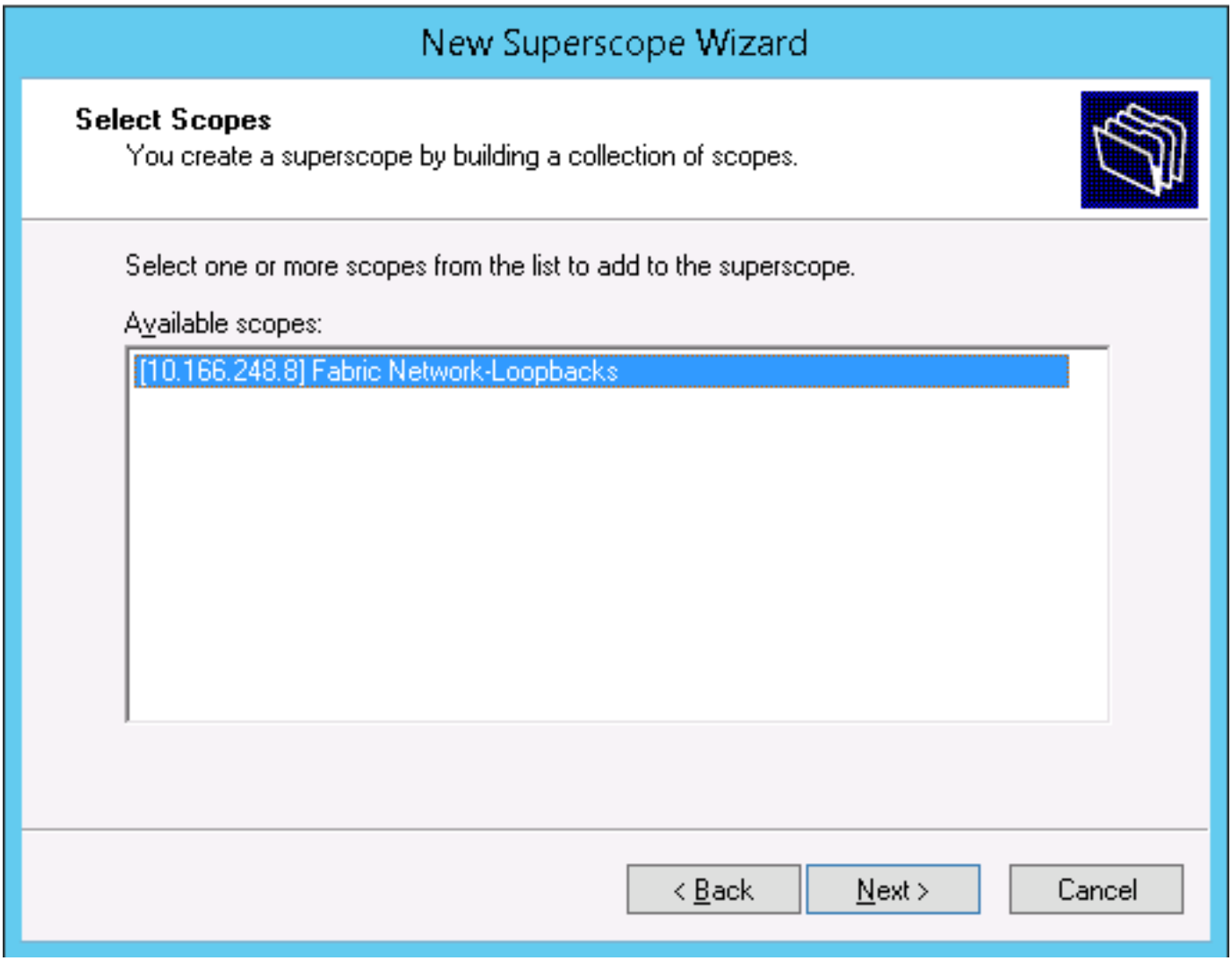


Click Next to get started

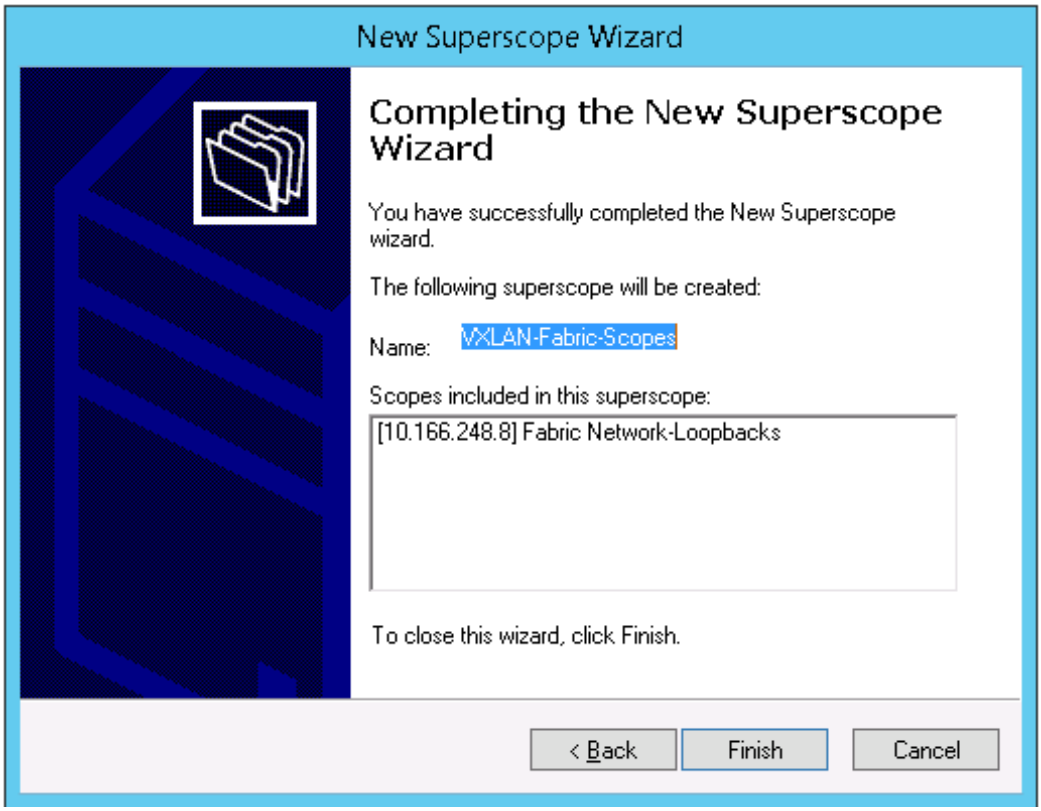


Name it appropriately

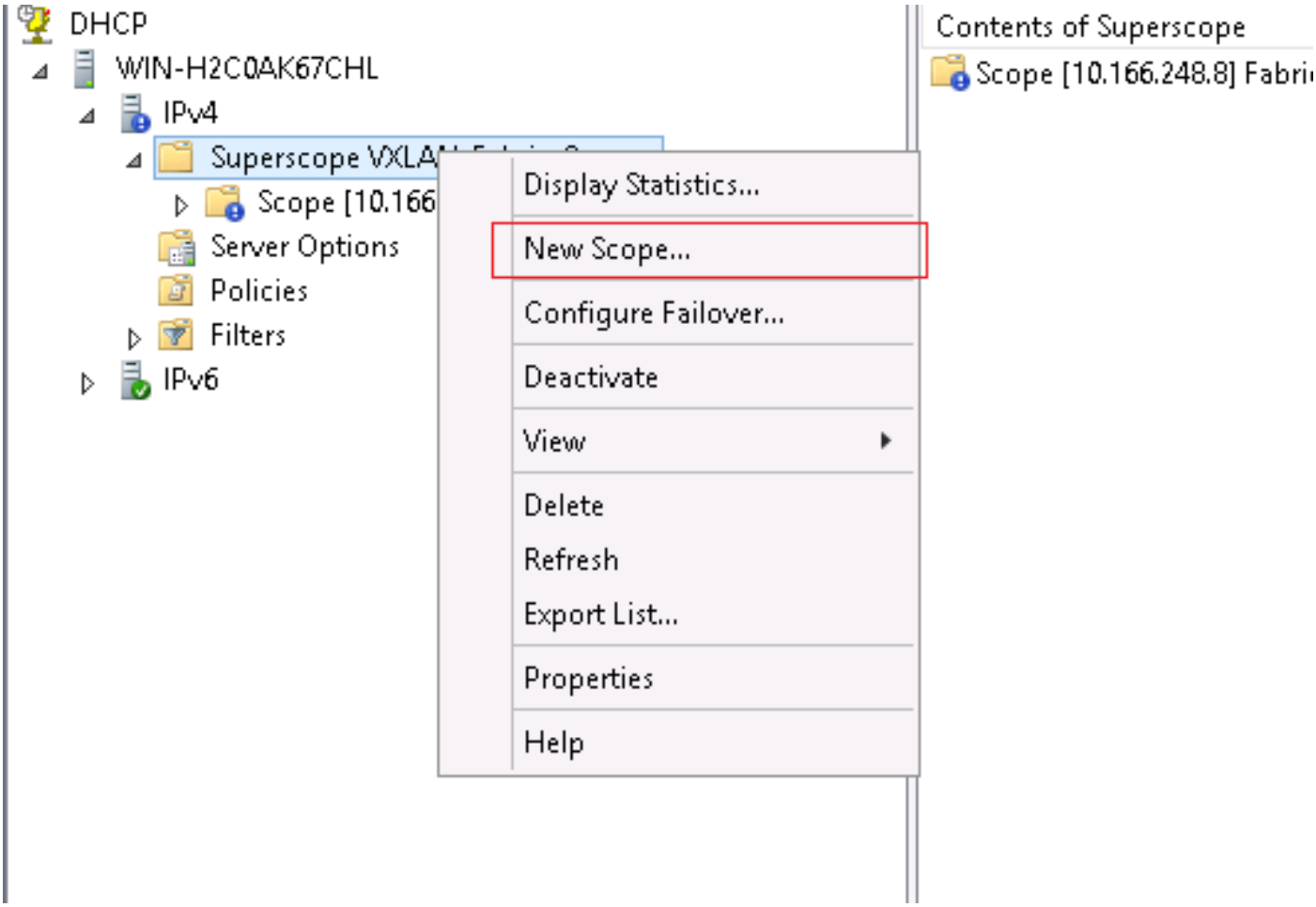
Select your newly created loopback scope to include in the new superscope.



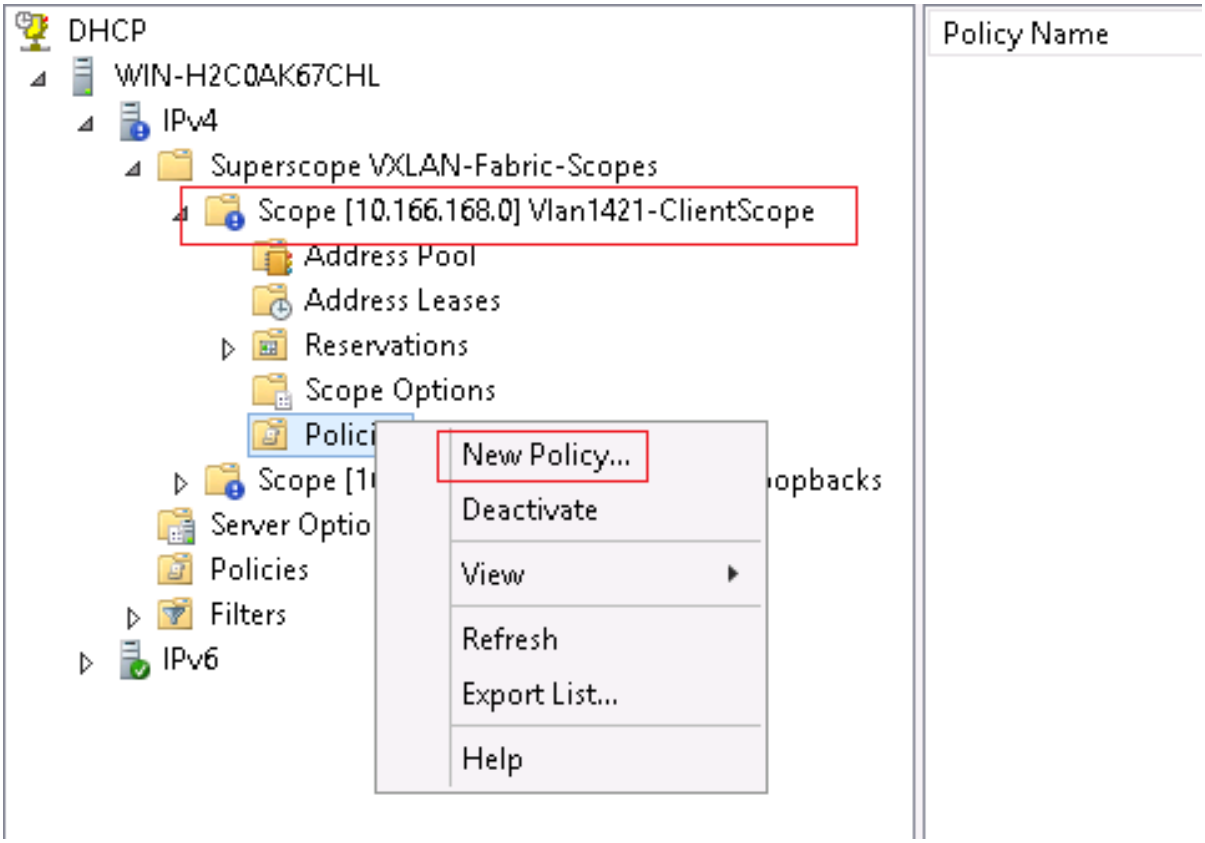
You're done. Click Finish.



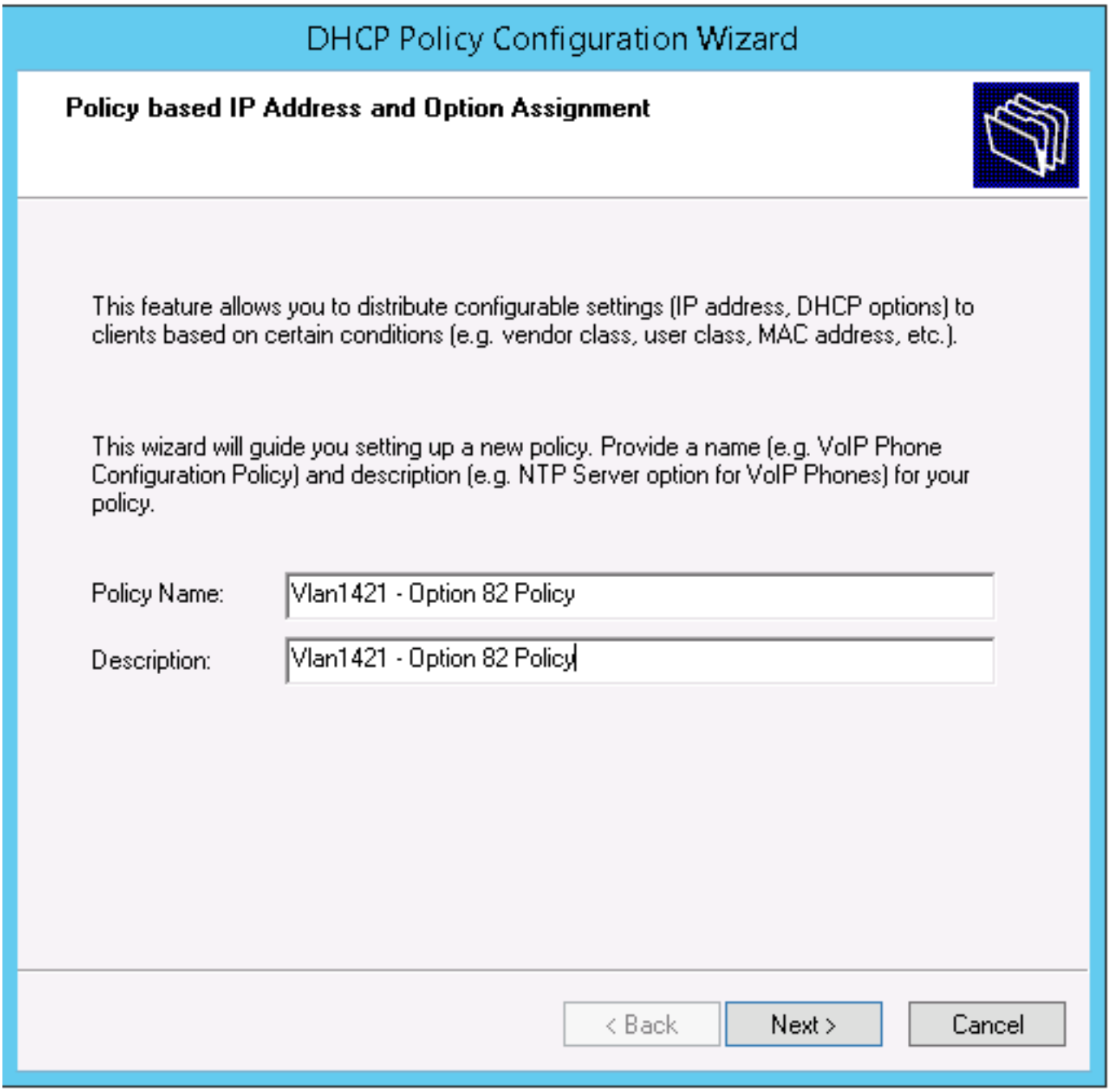
Next you need to create a client scope. Create this scope normally as you would create any client scope except be sure to include it in the superscope like this:



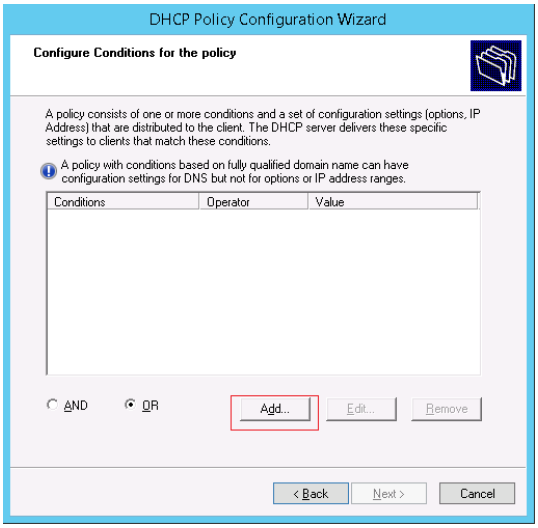
After your scope is created now add the Option 82 information that allows the server to identify the correct scope. Expand your scope and go to policies and create a new policy.



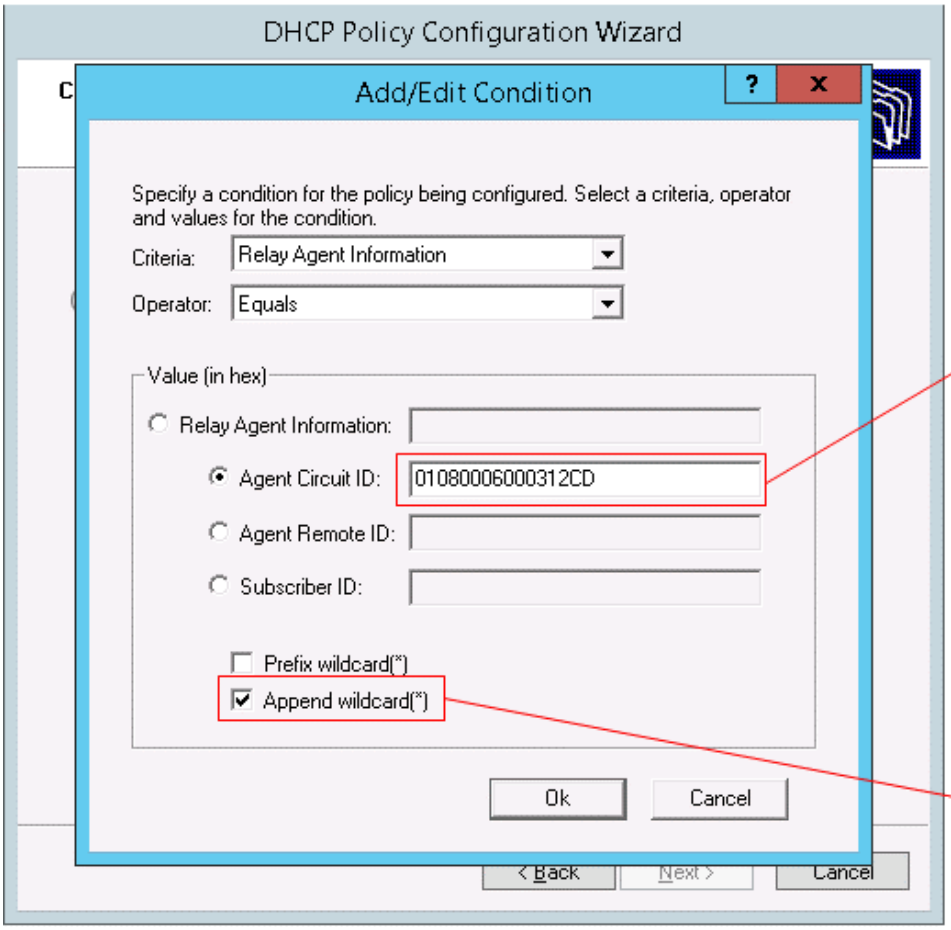
Name it appropriately.



Click Add to create your policy



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.



Leaf Configuration

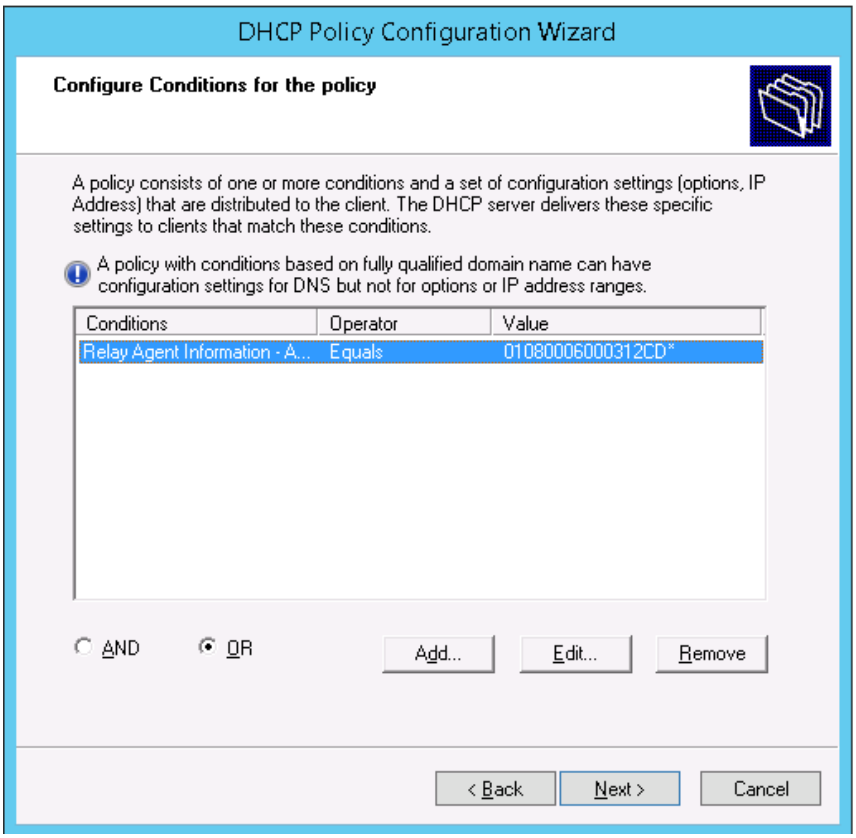
```
vlan 1421
 name Clients
 vn-segment 201421
```

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

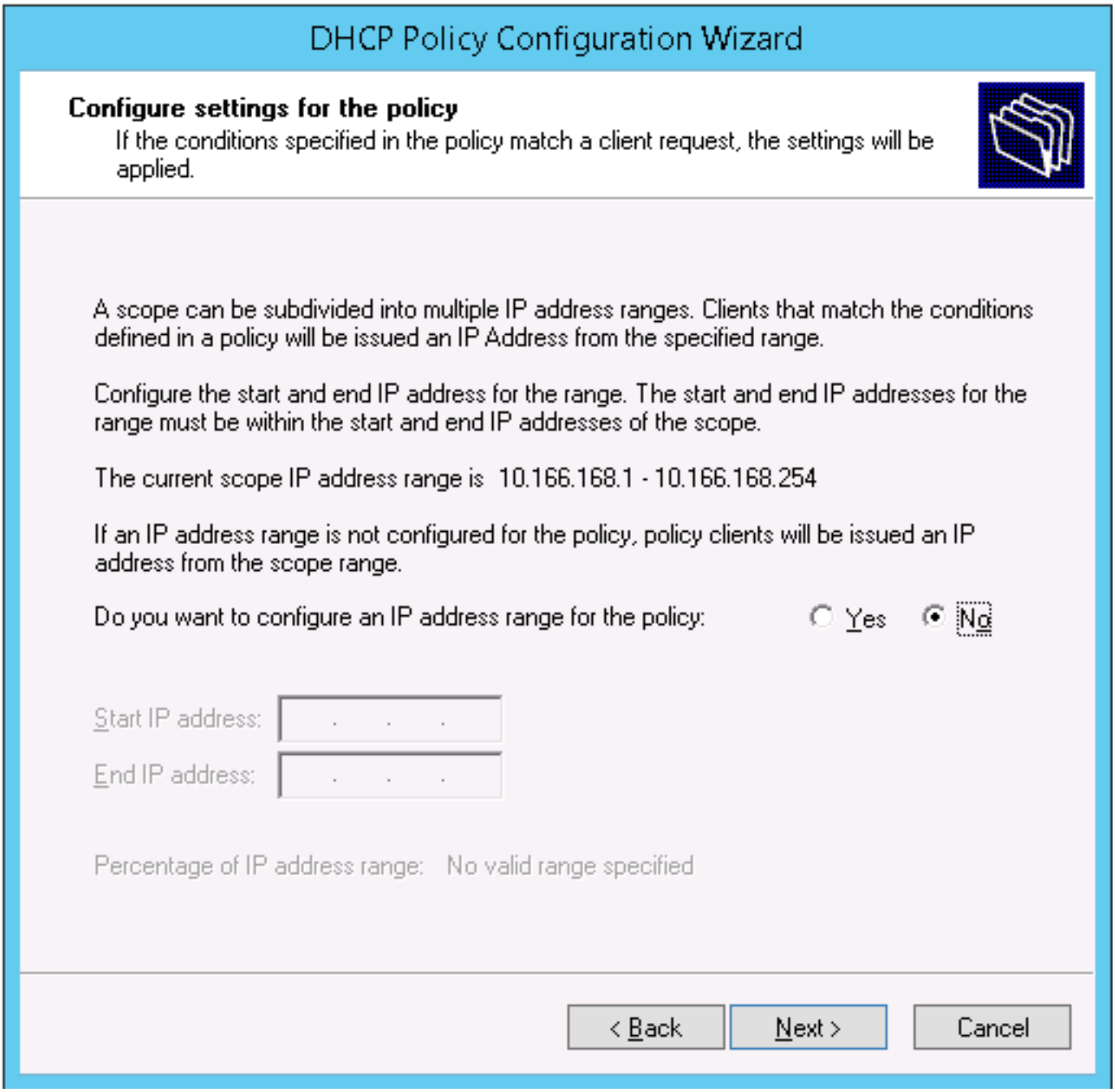
201421 = 312CD. Since the number needs to always be six digits it becomes 0312CD for a total circuit ID of 01080006000312CD

Be sure to check the append wildcard box

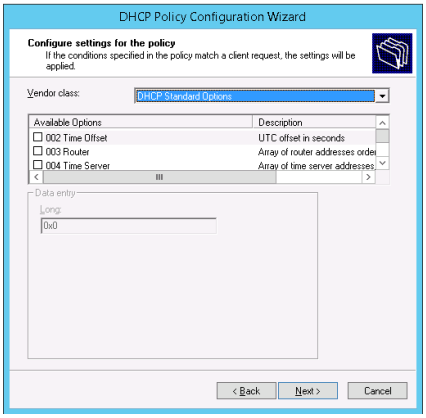
Click Next to move forward to custom options.



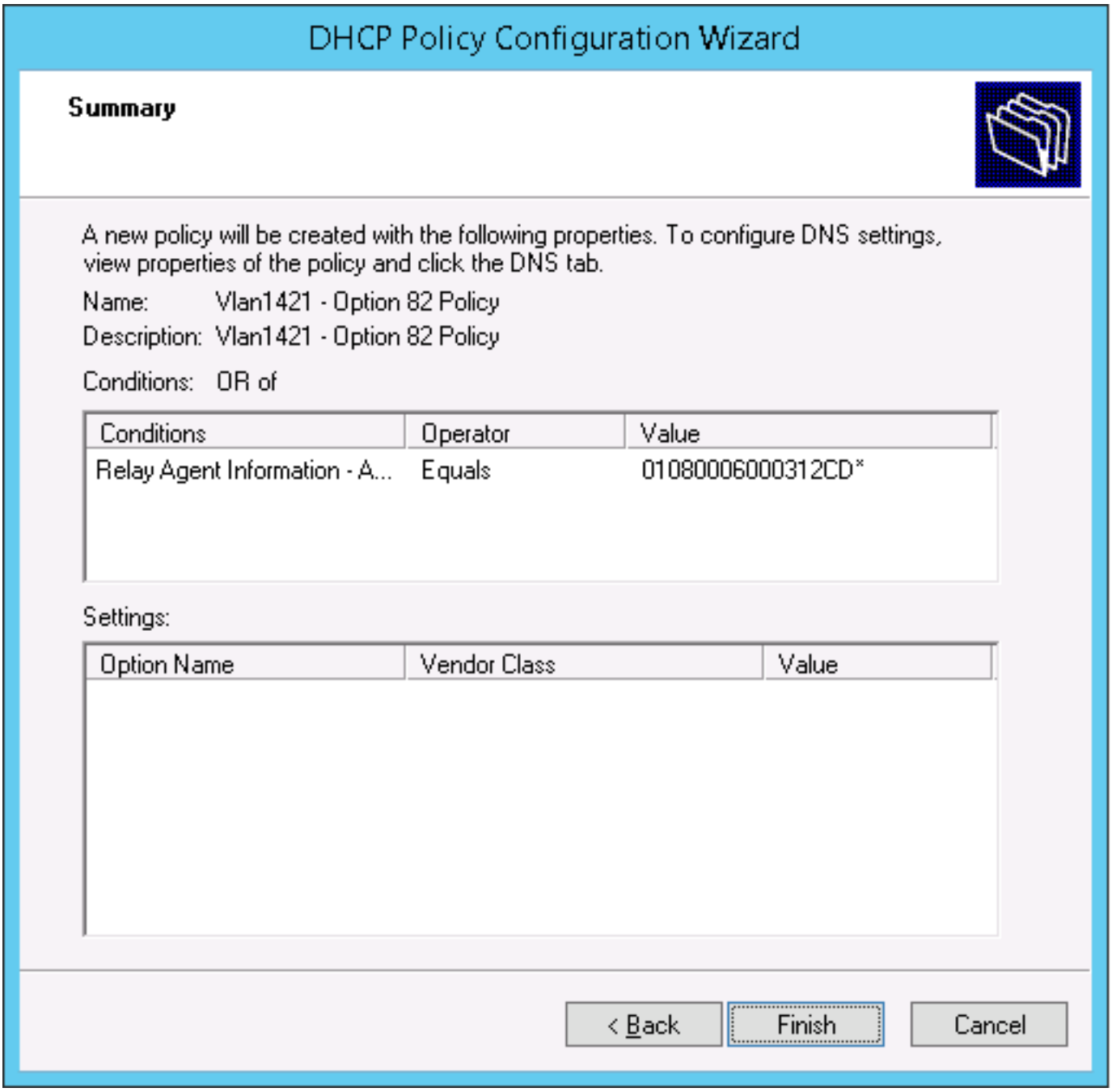
You can configure a custom IP range by checking Yes and choosing a range of addresses or selecting No and letting it give any eligible address in the scope. For this scope I have chosen No to let it give the client any address in the scope.



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.



Verify and click finish to create the policy.



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

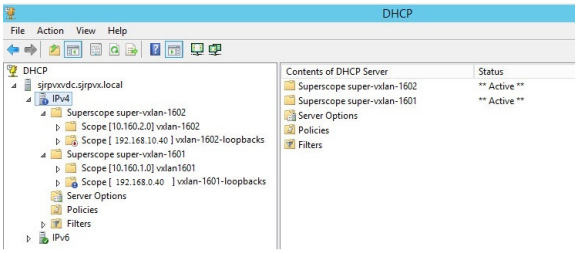
Each VLAN uses different Loopback as DHCP relay source.

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.