Konfigurieren von DHCP in IOS XE EVPN/VXLAN

Inhalt

Einleitung

In diesem Dokument wird die DHCP-Konfiguration (Dynamic Host Configuration Protocol) für Ethernet VPN (EVPN) Virtual Extensible LAN (VXLAN) in verschiedenen Szenarien und spezifische Aspekte für Win2012- und Win2016-DHCP-Server beschrieben.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über EVPN/VXLAN und DHCP zu verfügen.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

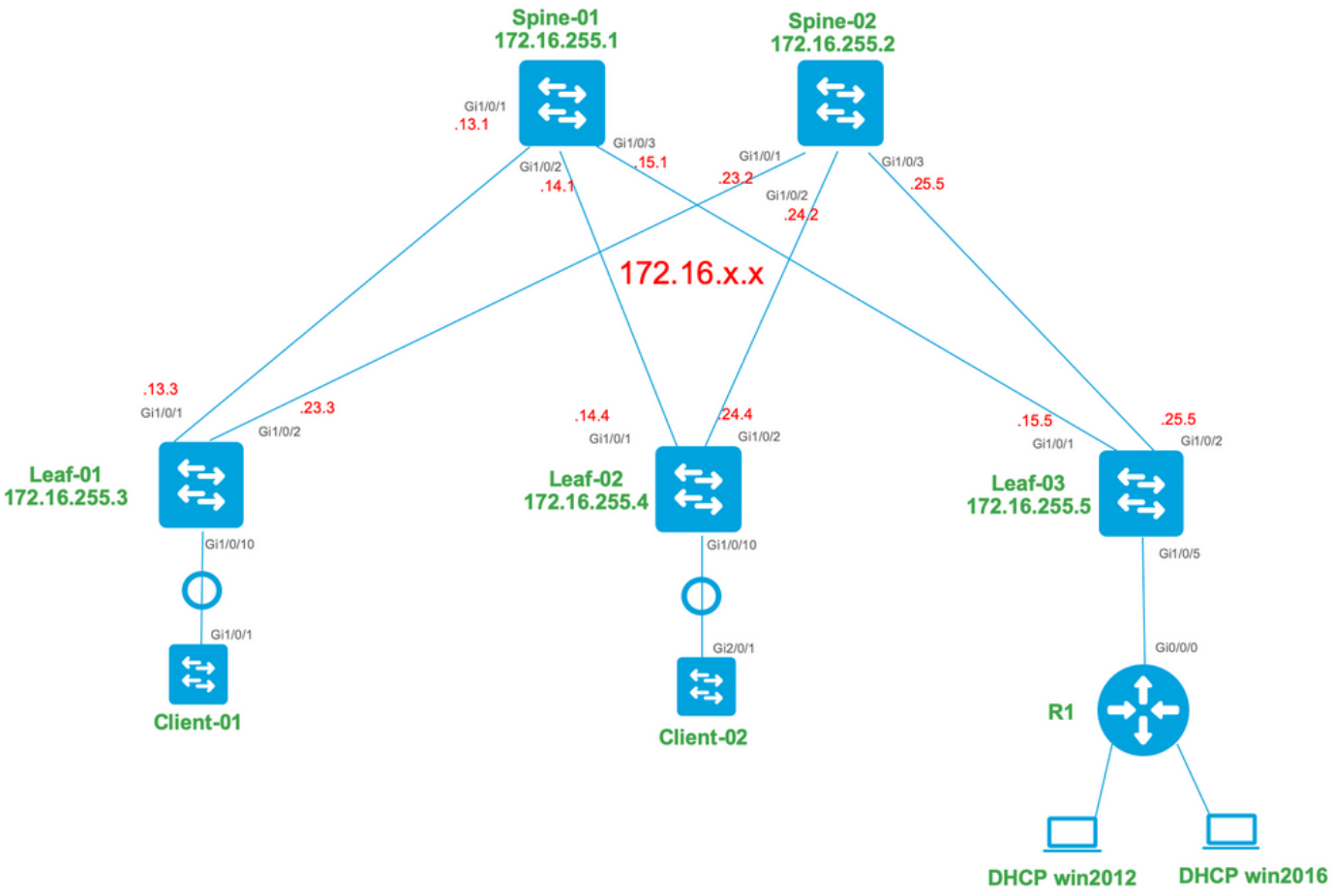
- C9300
- C9400

- C9500
- C9600
- Microsoft Windows Server 2012 R2
- Microsoft Windows Server 2016
- Funktionen ab Cisco IOS XE 16.9.x

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle verstehen.

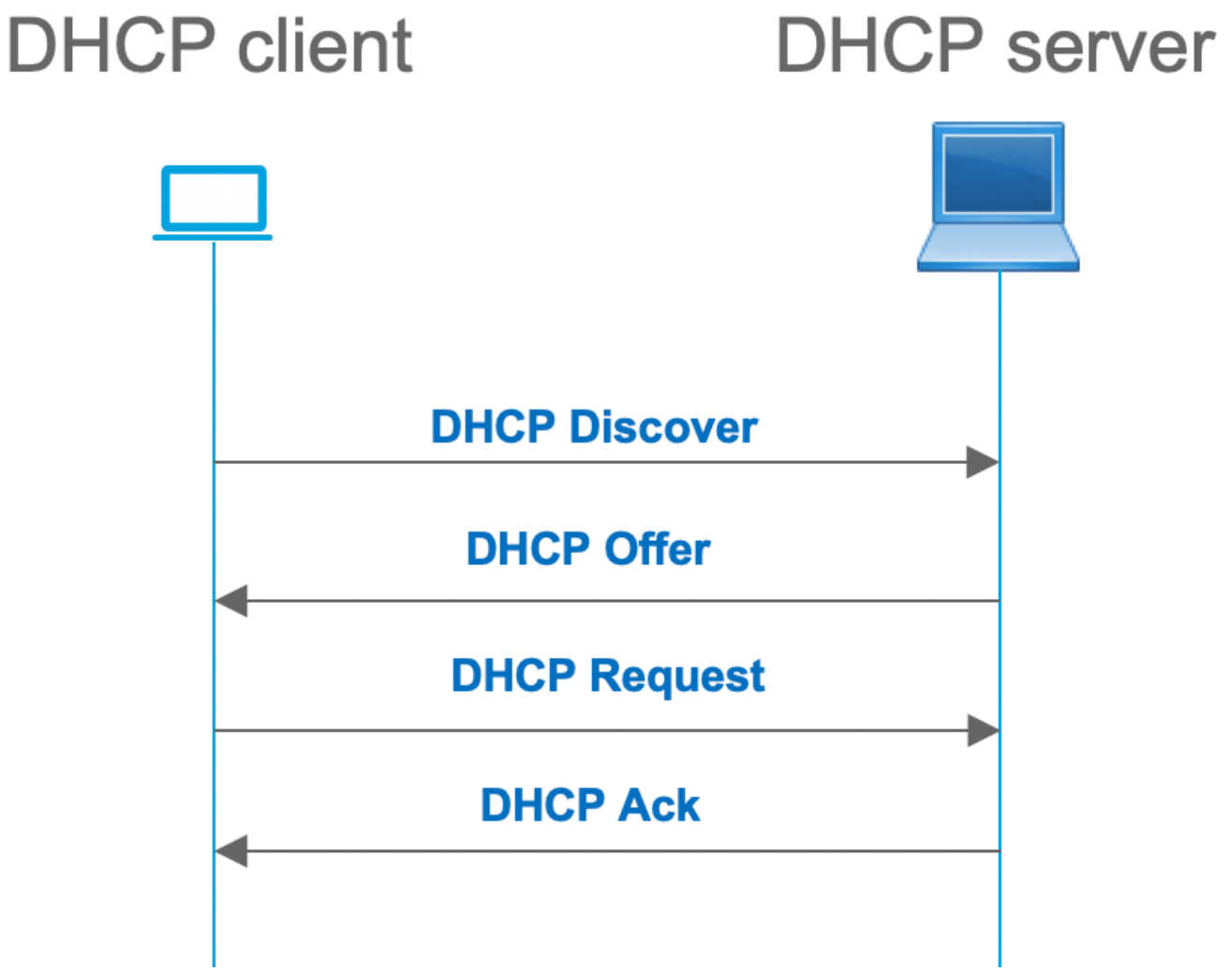
Konfigurieren

Netzwerkdiagramm



Konfigurationen

Lassen Sie uns nun den Nachrichtenfluss zwischen dem DHCP-Client und dem Server überprüfen. Es gibt vier Phasen:

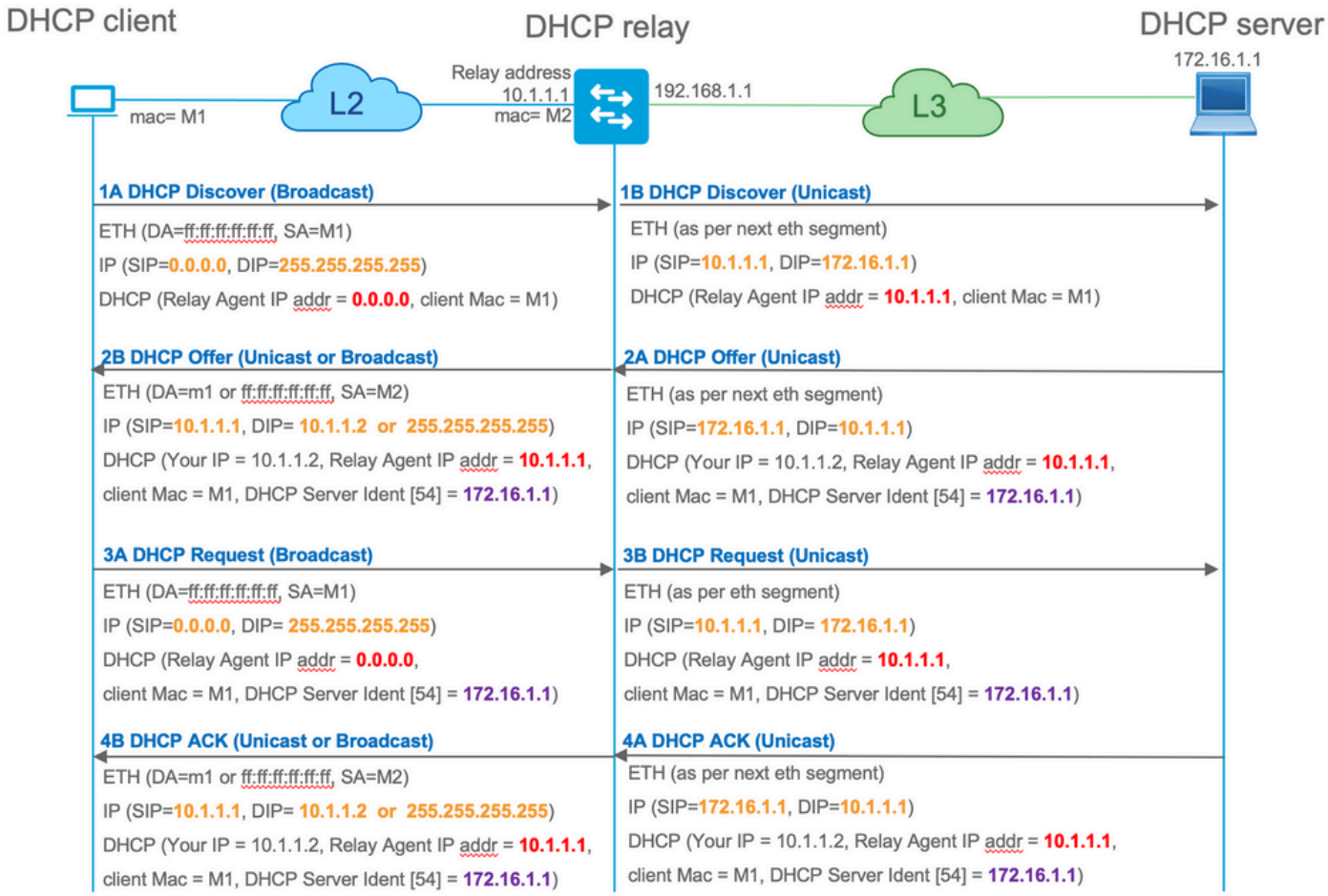


Dies funktioniert in Fällen, in denen sich der Client und der Server im gleichen Subnetz befinden, in der Regel ist dies jedoch nicht der Fall. In den meisten Fällen befindet sich der DHCP-Server nicht im gleichen Subnetz wie der Client und muss über einen gerouteten Layer-3-Pfad im Vergleich zu Layer-2 erreichbar sein. In diesem Fall ist eine DHCP-Relay-Funktion erforderlich. Die DHCP-Relay-Funktion (Switch oder Router) wandelt Broadcast in UDP-gekapseltes Unicast um, das routingfähig ist, und sendet es an den DHCP-Server. Diese Konfiguration wird heutzutage häufig in Netzwerken verwendet.

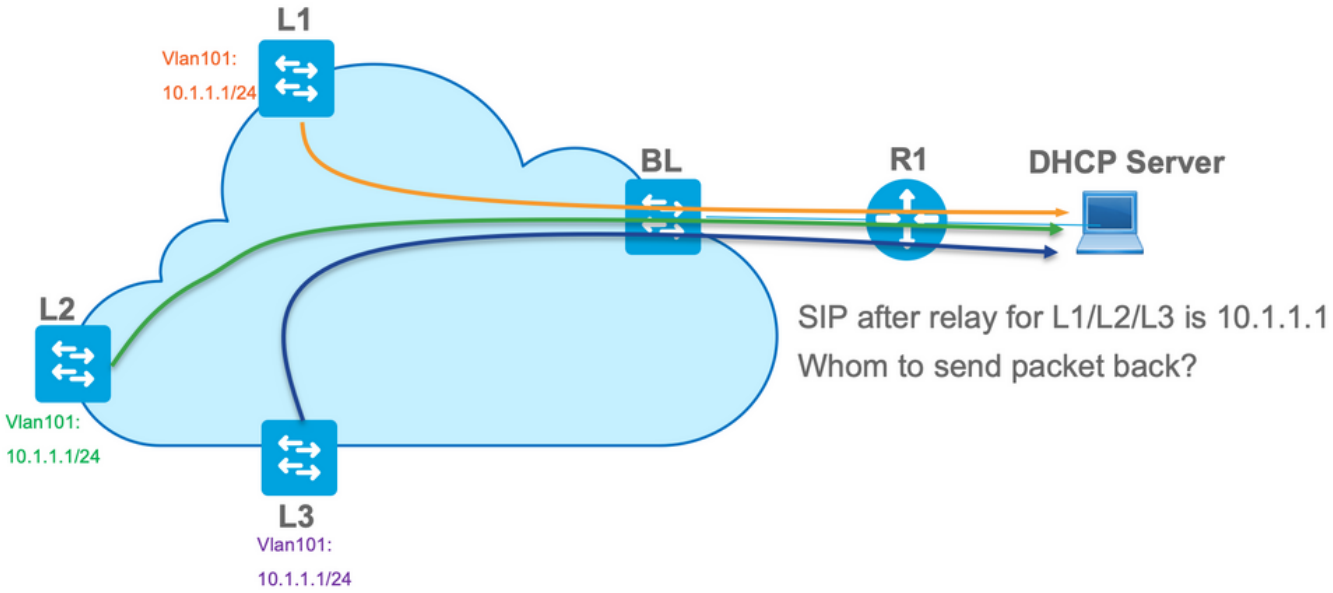
Herausforderungen mit DHCP und EVPN/VXLAN-Fabric:

In der Regel ist der DHCP-Server über das L3-Netzwerk mit der EVPN-Fabric verbunden. Das bedeutet, dass Sie die DHCP-Relay-Funktion verwenden müssen, um ein DHCP-Broadcast-Paket von Layer 2 in ein Unicast-Routingpaket von Layer 3 zu konvertieren.

Mit der DHCP-Relay-Funktion funktioniert der DHCP-Anruffluss zwischen Client, Relay und Server ähnlich:



Nach dem Weiterleiten ist die Quell-IP des Pakets die Relay-IP. Dies wirft jedoch ein Problem bei der VXLAN/EVPN-Bereitstellung auf, da die übliche Quell-IP aufgrund der Verwendung von Distributed Anycast GW (DAG) nicht eindeutig ist. Da alle VTEP SVI-Quell-IPs identisch sind, kann dies dazu führen, dass die Reply-Pakete vom DHCP-Server an den nächstgelegenen Leaf weitergeleitet werden.



Um das Problem der nicht eindeutigen Quelle zu beheben, müssen Sie in der Lage sein, eine eindeutige IP-Adresse für weitergeleitete DHCP-Pakete pro Leaf zu verwenden. Ein weiteres Problem betrifft den Austausch von GIADDR-Geräten. Auf dem DHCP-Server müssen Sie den

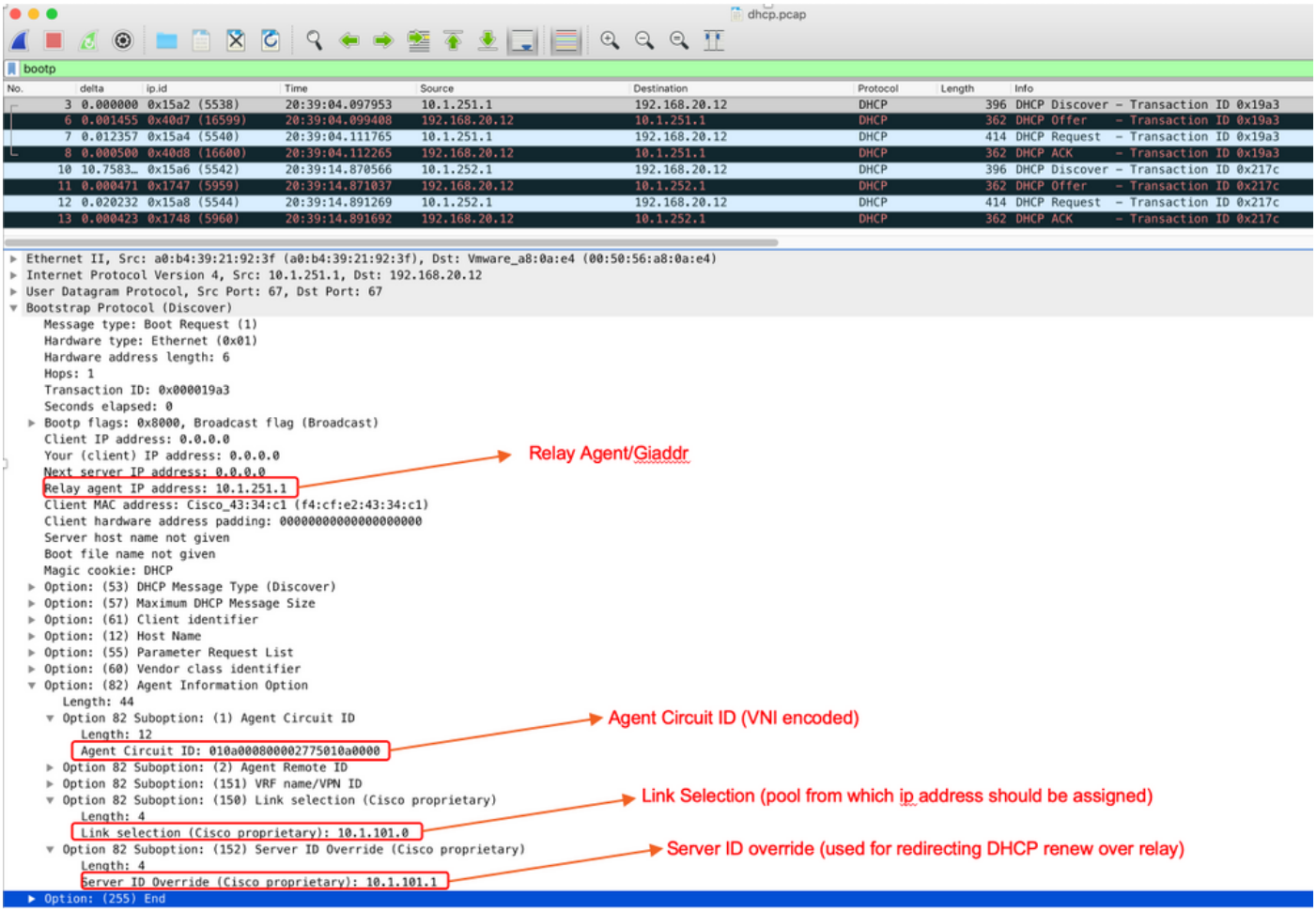
richtigen Pool auswählen, um die IP-Adresse zuzuweisen. Sie erfolgt über den Pool, der die Gateway-IP-Adresse (giaddr) abdeckt. Bei der EVPN-Fabric muss es sich um eine IP-Adresse der SVI handeln. Nach dem Relay wird der Gigat jedoch durch eine Relay-IP-Adresse ersetzt, die in diesem Fall ein eindeutiges Loopback ist.

Wie können Sie den DHCP-Server informieren, welche Pools er verwenden muss?

Zur Lösung dieses Problems wird Option 82 verwendet. Dies sind vor allem die wichtigen Unteroptionen:

- 1 - Die **Agenten-Circuit-ID**. Bei VXLAN/EVPN überträgt diese Unteroption die VNI-ID.
- 5 - (oder 150 für Cisco proprietär). Die Unteroptionen für die **Verbindungsauswahl**, die das tatsächliche Subnetz aufweisen, von dem das DHCP-Paket stammt
- 11 - (oder 152 für Cisco proprietär). Die **Unteroption Server Identifier Override**, die die Adresse des DHCP-Servers enthält.
- 151 - Der **VRF-Name/die VPN-ID**. Diese Unteroption hat einen VRF-Namen/eine VPN-ID

Bei der Paketerfassung des Pakets vom DHCP-Relay zum DHCP-Server werden diese verschiedenen Optionen im DHCP-Paket angezeigt, wie im Bild gezeigt.



Switch-Konfiguration:

- Option 82 enthält alle erforderlichen Informationen, um den richtigen DHCP-Pool auszuwählen und das Paket vom Server an den richtigen Leaf zurückzugeben.
- Dies funktioniert nur, wenn der DHCP-Server die Option 82-Informationen verarbeiten kann, aber nicht alle Server diese vollständig unterstützen (z. B. win2012 r2).

```
ip dhcp relay information option vpn        <<<  adds the VRF name/VPN ID to the option 82
ip dhcp relay information option            <<< enables option 82
!
ip dhcp snooping vlan 101-102,201-202
ip dhcp snooping
!
vlan configuration 101
member evpn-instance 101 vni 10101
!
interface Loopback101
 vrf forwarding green
 ip address 10.1.251.1 255.255.255.255
!
interface Vlan101
 vrf forwarding green
ip dhcp relay source-interface Loopback101    <<< DHCP relay source is unique Loopback
 ip address 10.1.101.1 255.255.255.0
 ip helper-address 192.168.20.12               <<< 192.168.20.12 - DHCP server
```

Serverkonfiguration

Win2012 R2 Konfigurationsoption 1 - Unique Relay IP pro VNI/SVI pro VTEP

Das Hauptproblem bei win2012 besteht darin, dass Option 82 nicht vollständig unterstützt wird, sodass die Unteroption "Verbindungsauswahl" (5 oder Cisco proprietär - 150) nicht zur Auswahl des richtigen Pools auf dem DHCP-Server verwendet werden kann.

Zur Lösung eines solchen Problems kann dieser Ansatz verwendet werden:

- Ein Bereich für RELAY-IP-Adressen muss erstellt werden. Andernfalls findet DHCP keinen Pool, der mit DHCP GIADDR übereinstimmt und das Paket ignoriert. Der gesamte IP-Bereich muss von DHCP ausgeschlossen werden, um eine Zuweisung aus dem RELAY IP-Pool zu verhindern. Dieser Pool wird als RELAY_POOL bezeichnet.
- Der Bereich für den IP-Bereich, den Sie zuweisen möchten, muss erstellt werden. Dieser Pool wird als IP_POOL bezeichnet.
- Superscope muss erstellt und beide Bereiche - RELAY_POOL und IP_POOL - eingeschlossen werden.

Sehen wir uns an, wie das DHCP-Paket auf dem Server verarbeitet wird.

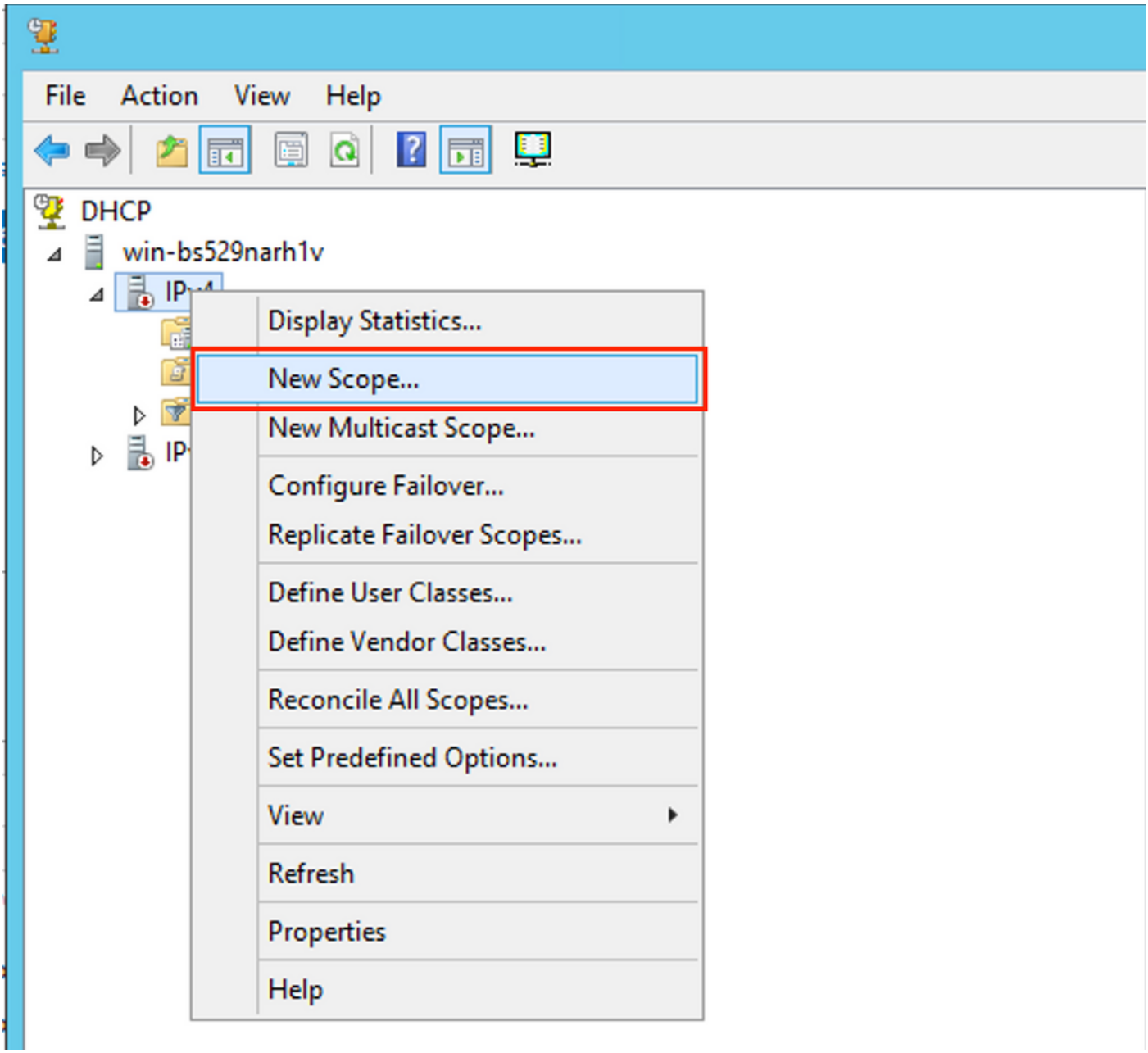
1. Das DHCP-Paket wird vom Server empfangen.
2. Basierend auf GIADDR-Pool wird RELAY_POOL im entsprechenden Superscope ausgewählt.
3. Da es in RELAY_POOL keine freien IP-Adressen gibt (denken Sie daran, dass der vollständige Gültigkeitsbereich ausgeschlossen ist?), wird im selben Superskop IP_POOL zurückgesetzt.
4. Die Adresse wird vom jeweiligen Superpool zugewiesen und an Relay zurückgesendet.

Ein großer Nachteil dieser Methode ist, dass Sie ein eindeutiges Loopback pro VLAN/VNI pro Vtep haben müssen, da der DHCP-Pool auf Basis der Relay-Adresse ausgewählt wird.

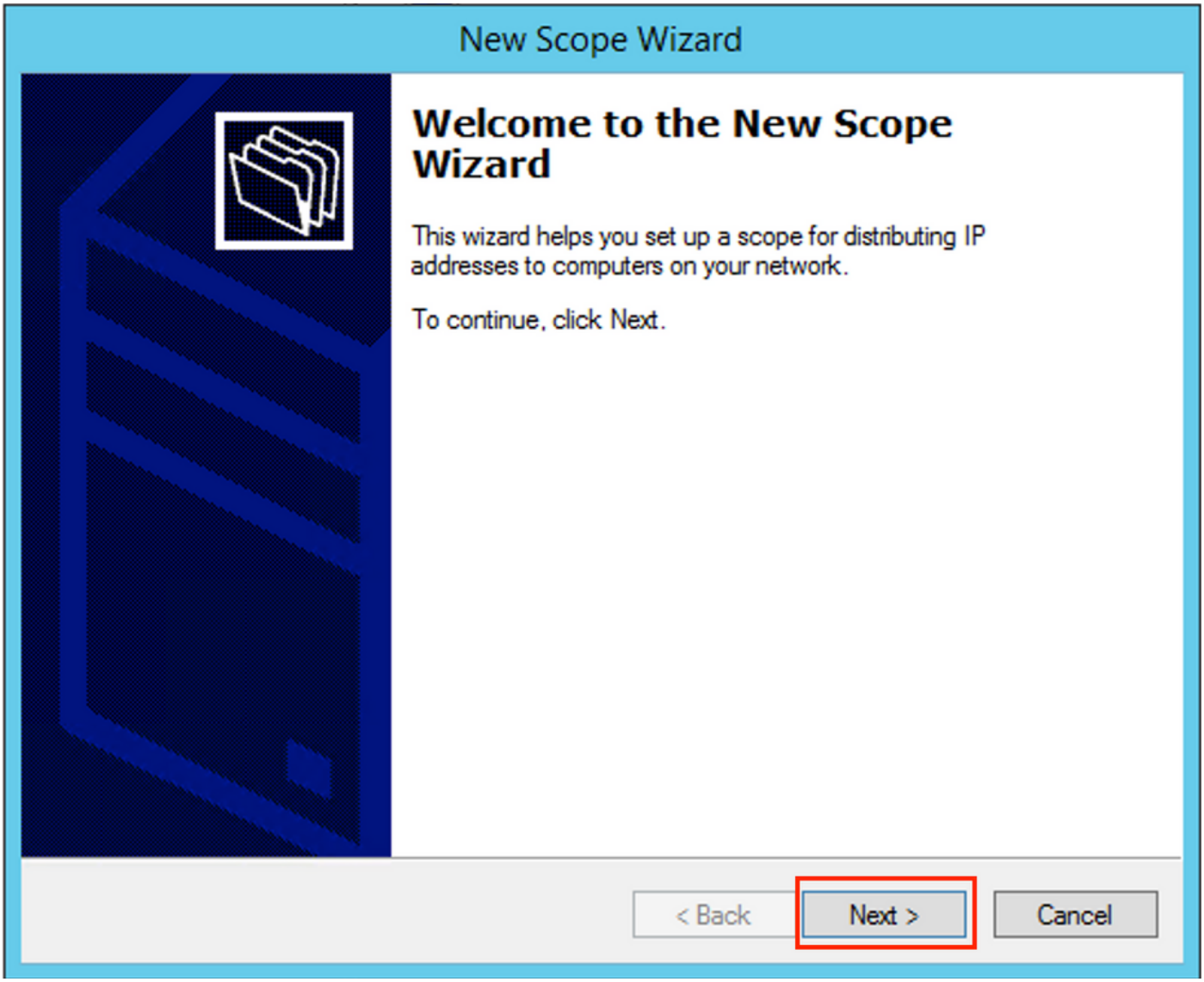
Diese Option führt zur Nutzung eines großen IP-Bereichs für die Relays-IP-Adressen.

Option 1: Schrittweise Anleitung zur Konfiguration von win2012 r2.

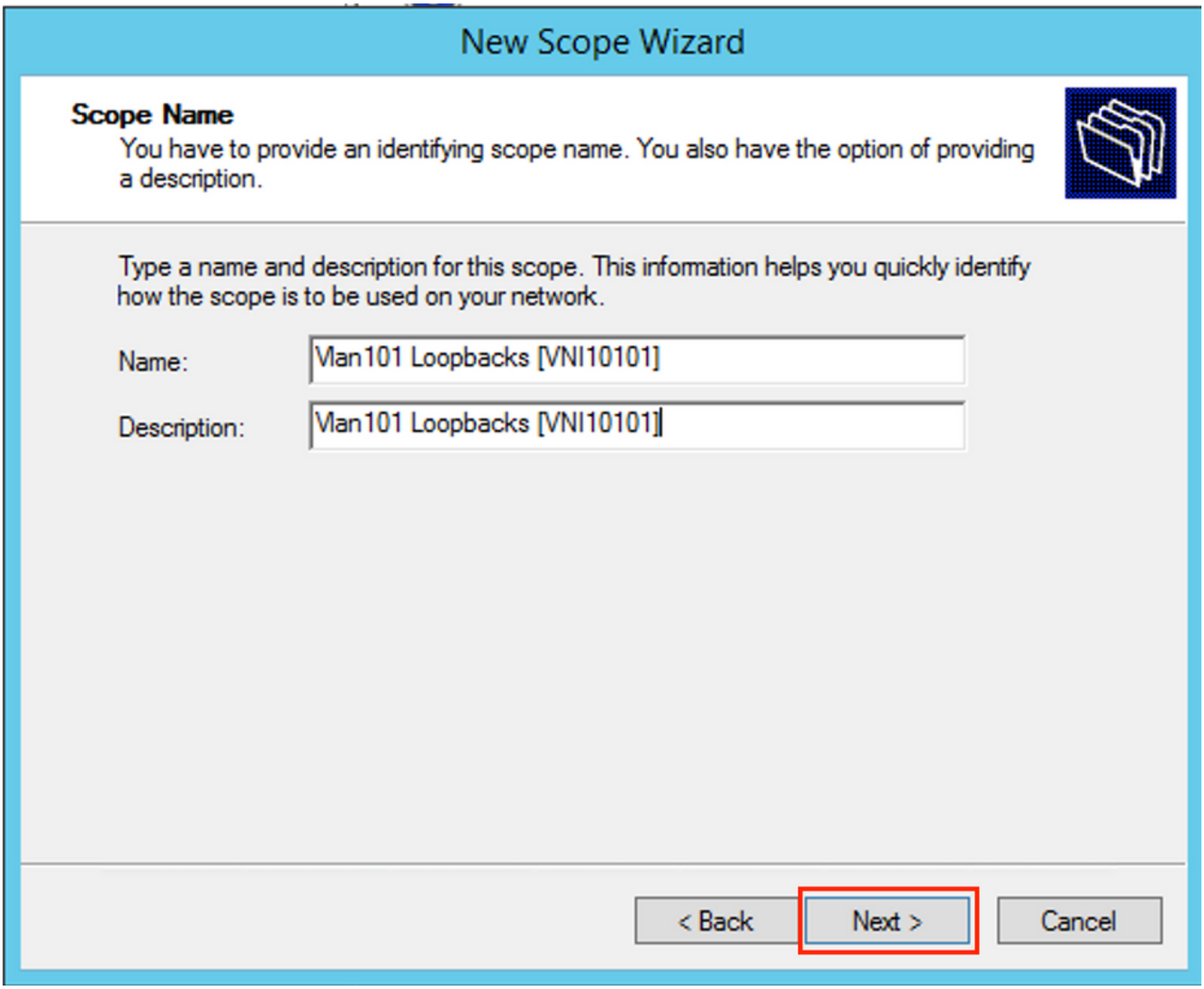
Erstellen Sie den DHCP-Bereich für Relay-Adressen. Klicken Sie mit der rechten Maustaste, und wählen Sie **Neuer Bereich** aus, wie im Bild gezeigt.



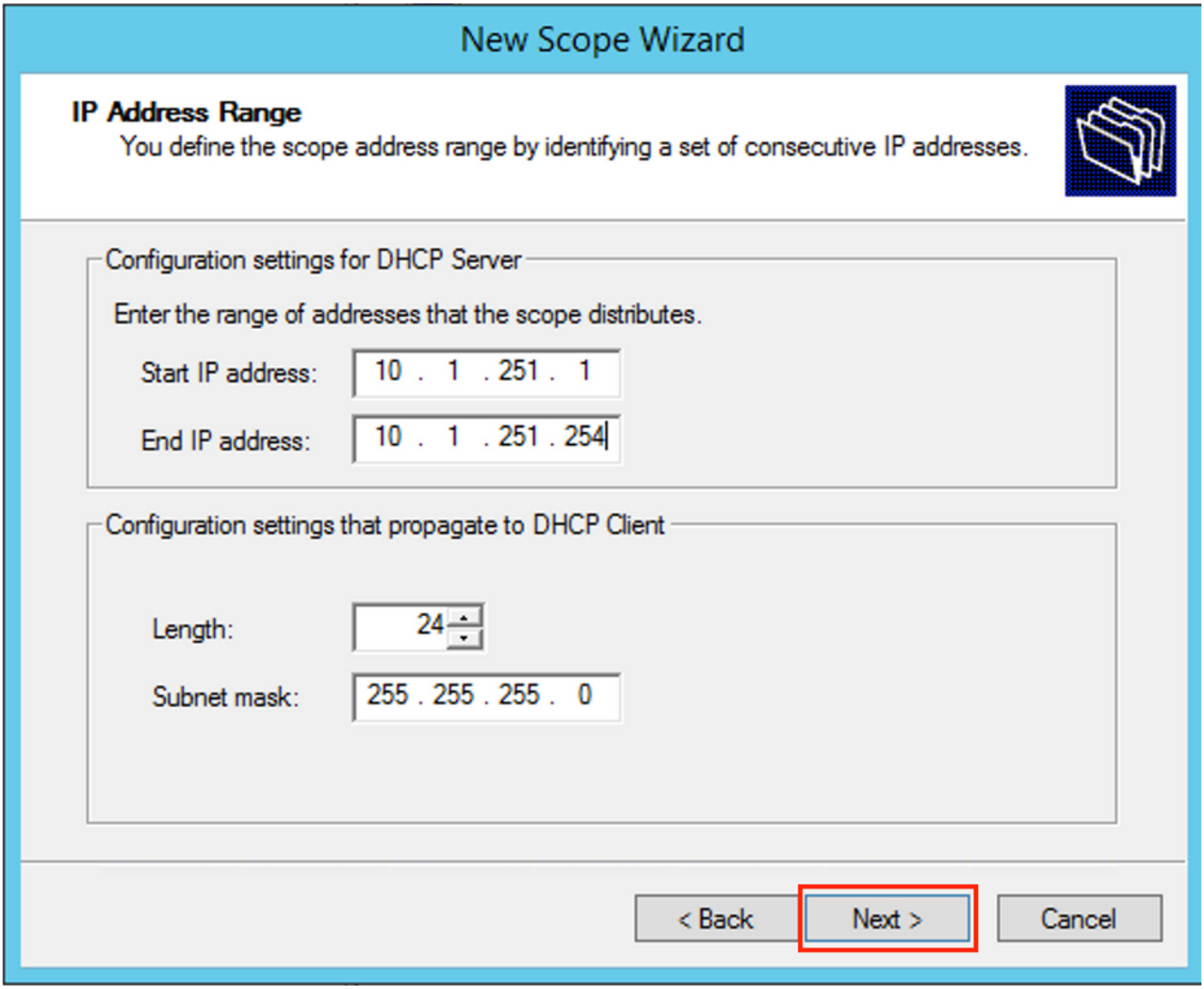
Wählen Sie **Weiter**, wie im Bild gezeigt.



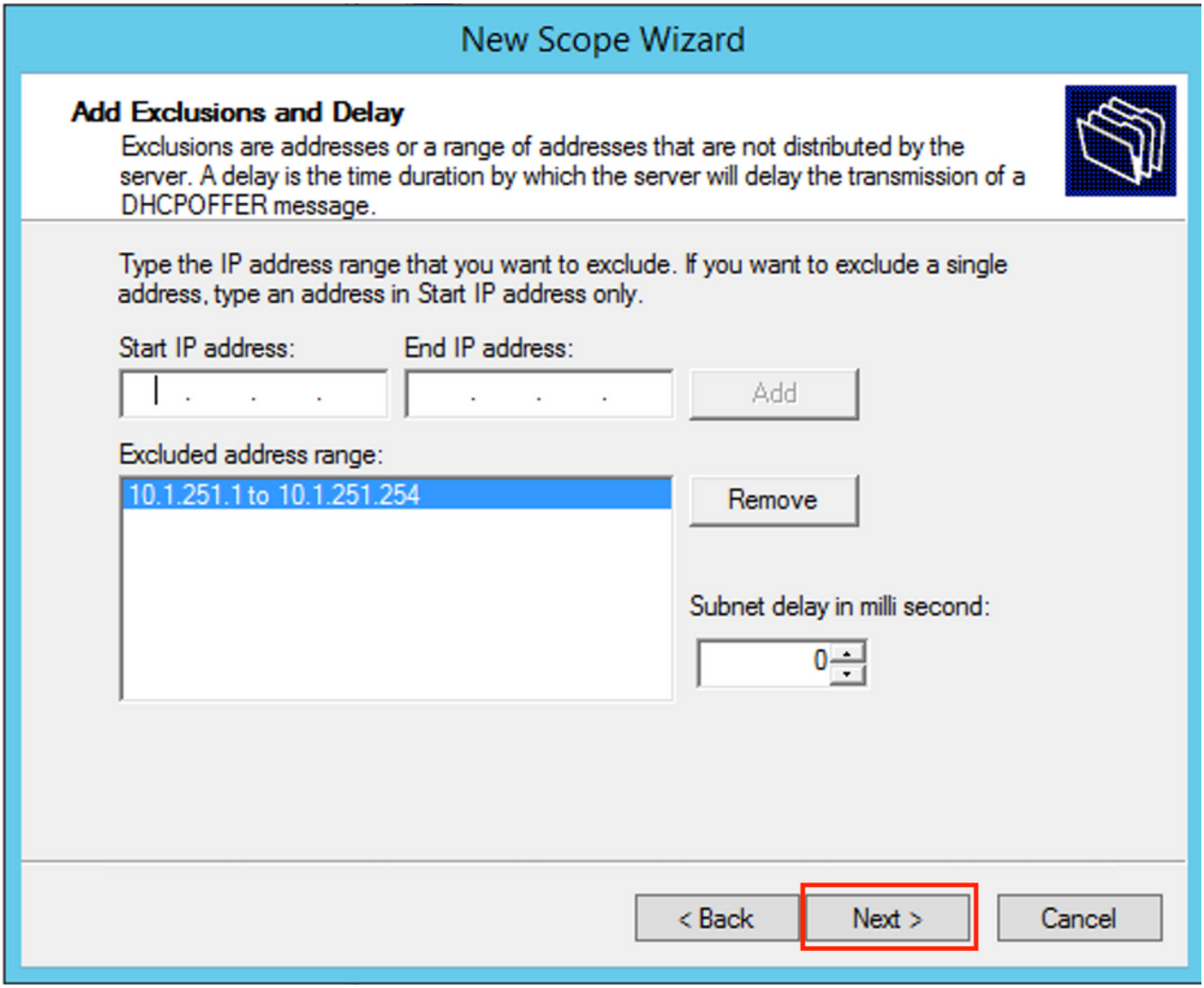
Geben Sie einen aussagekräftigen Namen, eine Beschreibung ein, und wählen Sie dann **Weiter** aus, wie im Bild gezeigt.



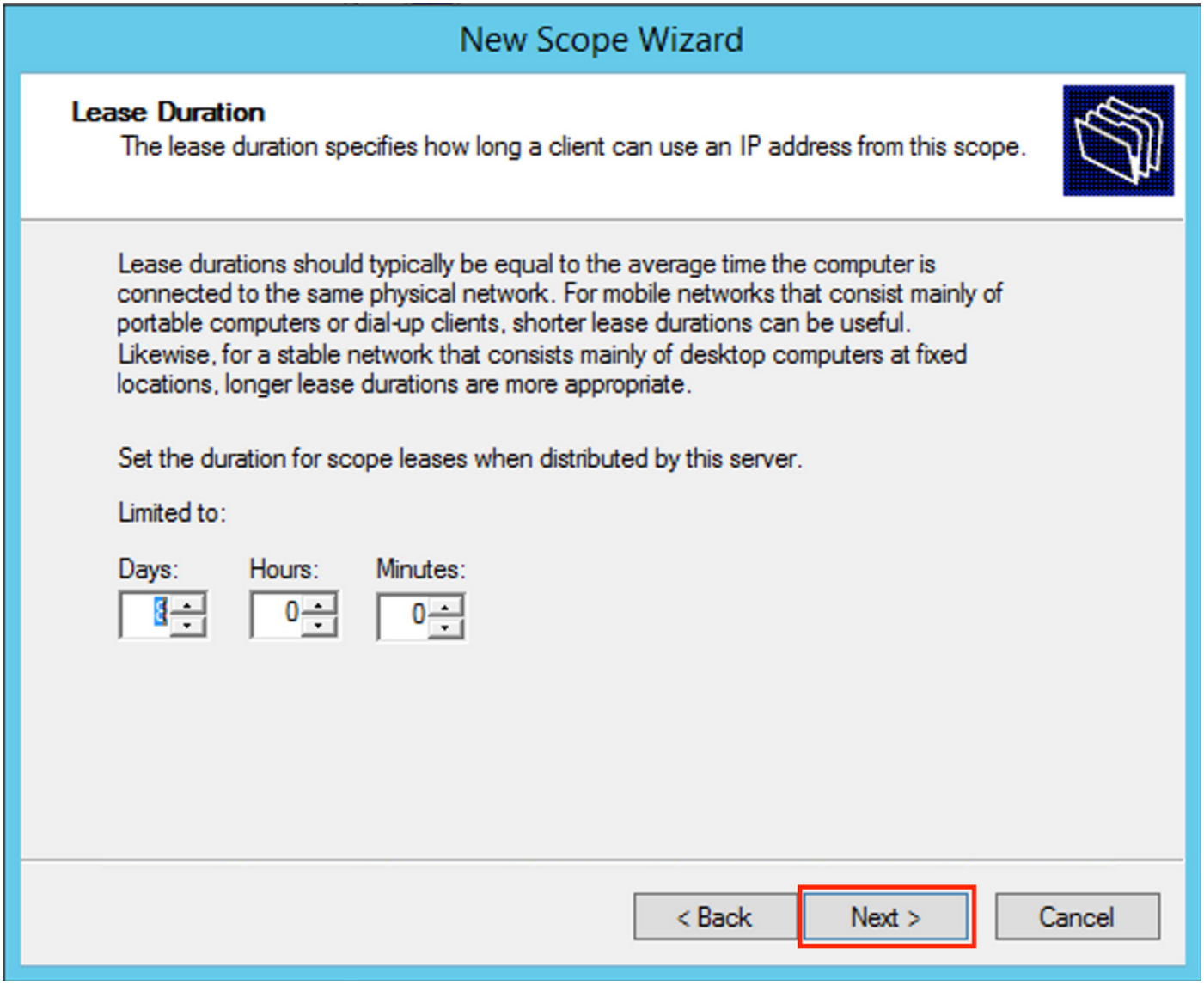
Geben Sie die IP-Adressinformationen für den Relay-Pool ein. In diesem Beispiel ist die Netzmaske "/24", sie kann jedoch größer oder kleiner (abhängig von der Netzwerkgröße) sein, wie im Bild gezeigt.



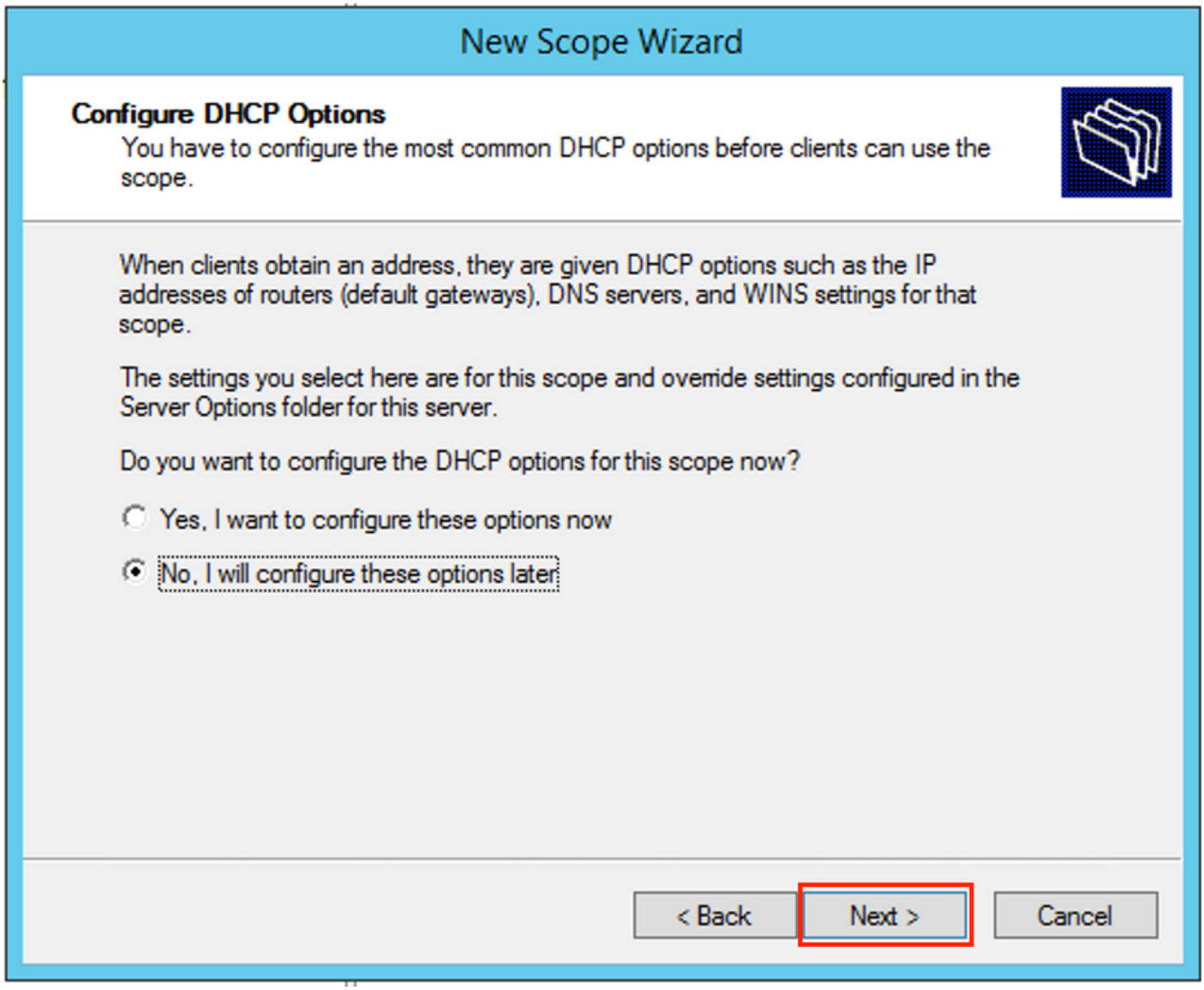
Schließen Sie alle Bereiche aus dem Pool aus. Dies ist wichtig, da andernfalls IP-Adressen aus diesem Pool zugewiesen werden können.



Konfigurieren Sie die Leasing-Zeit (standardmäßig beträgt sie 8 Tage) wie im Bild gezeigt.

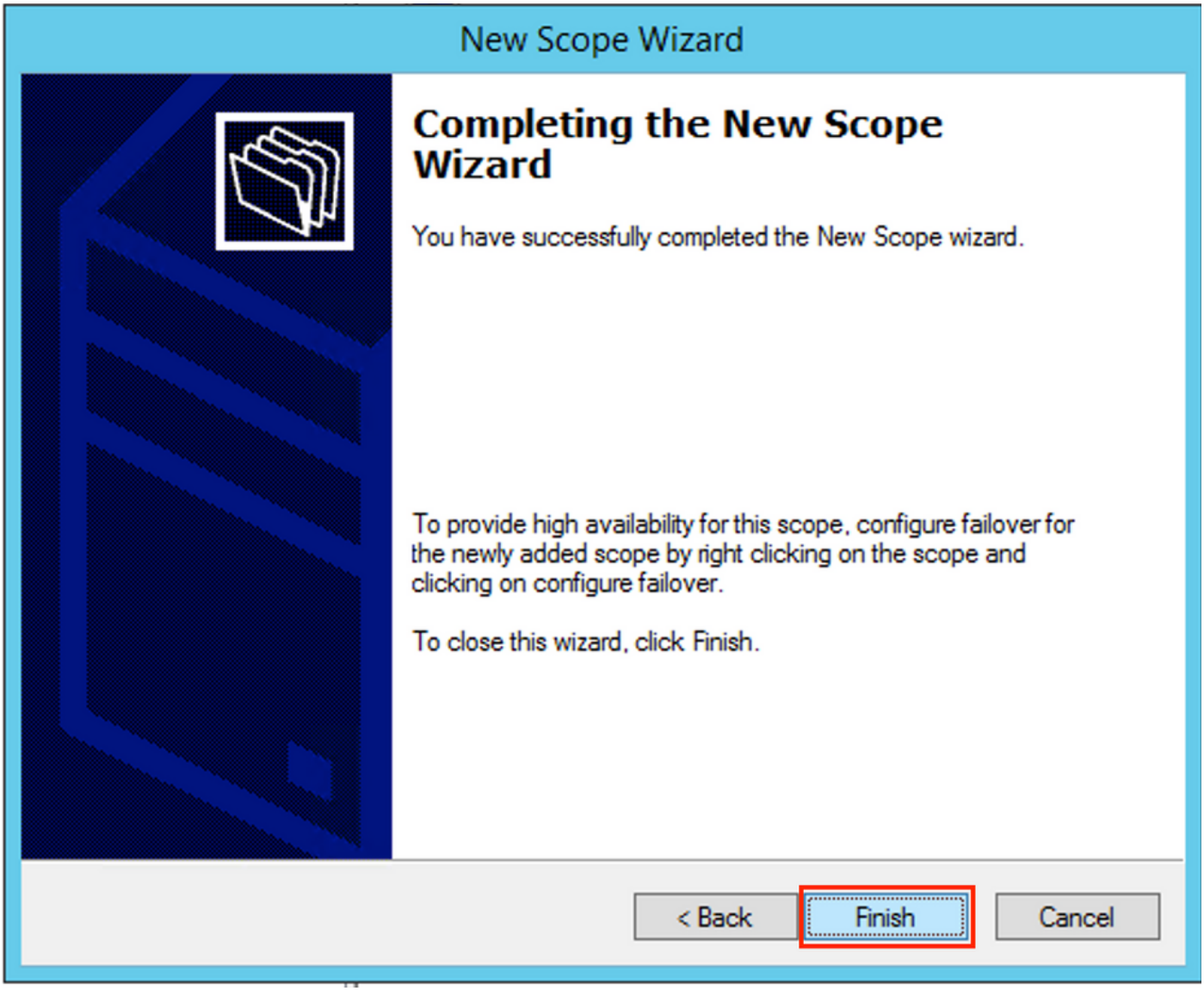


Sie können die DHCP-Optionsparameter wie DNS/WINS konfigurieren (in diesem Beispiel übersprungen).

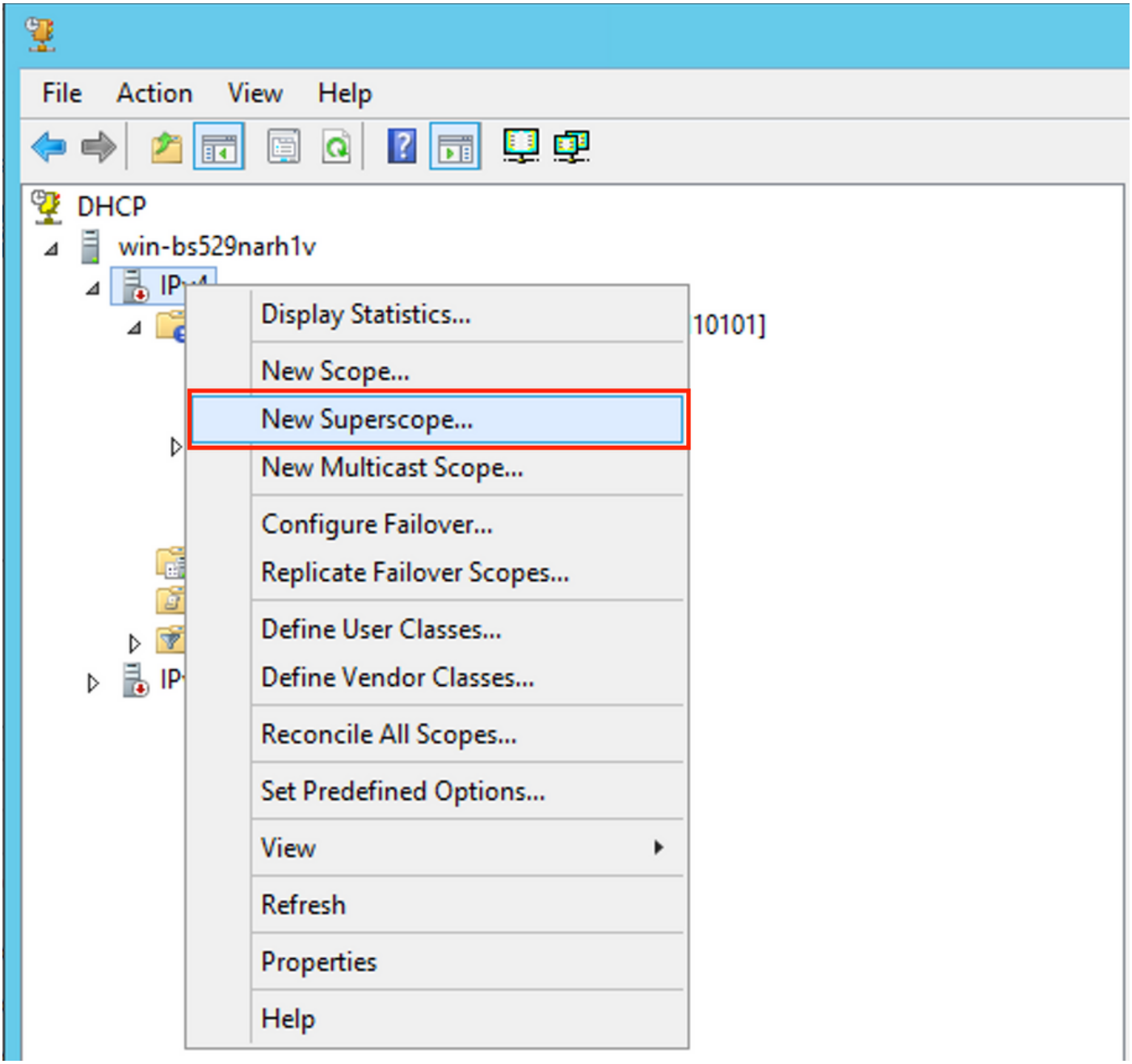


Aktivieren Sie den Bereich, wie im Bild gezeigt.

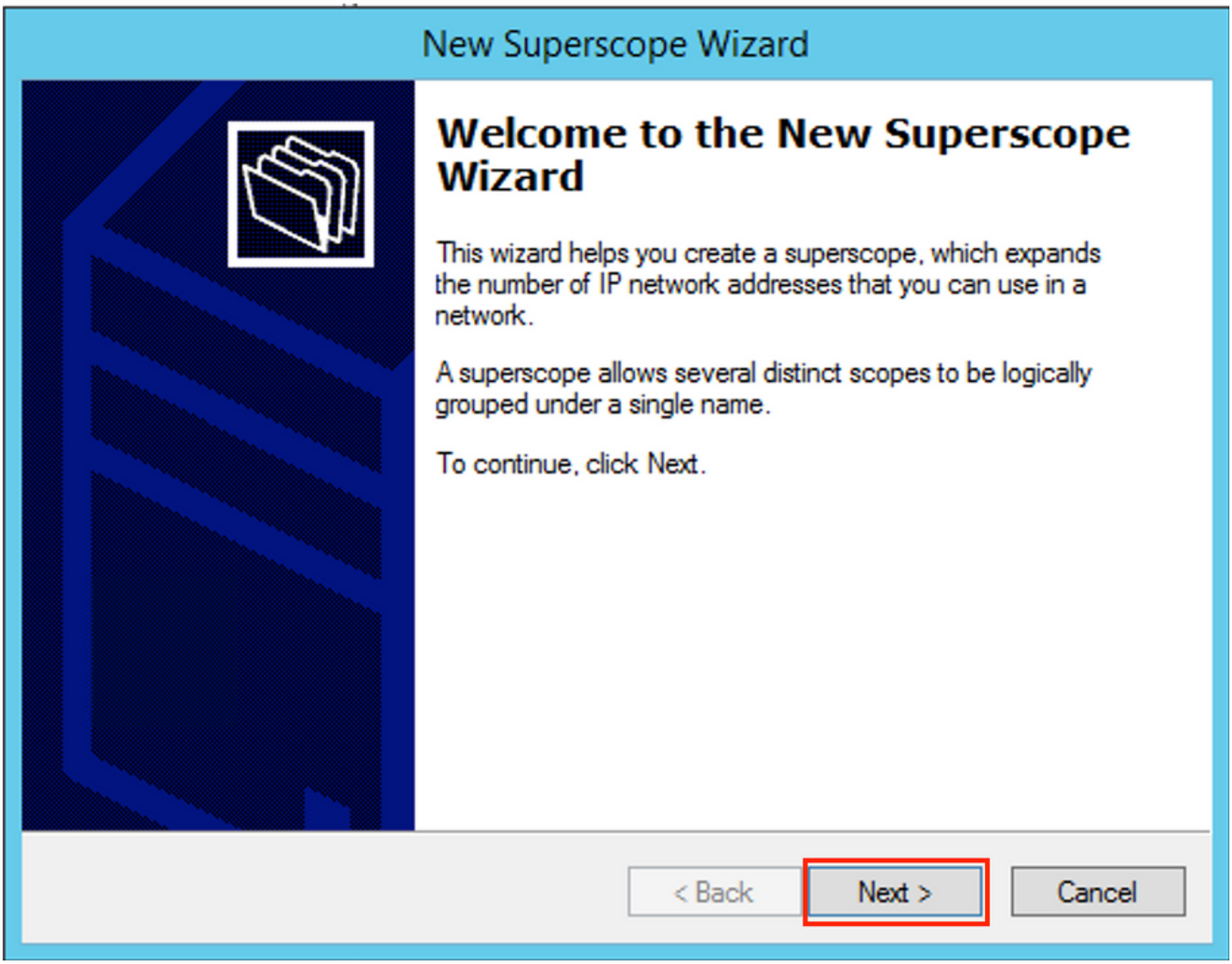
Schließen Sie die Konfiguration wie im Bild gezeigt ab.



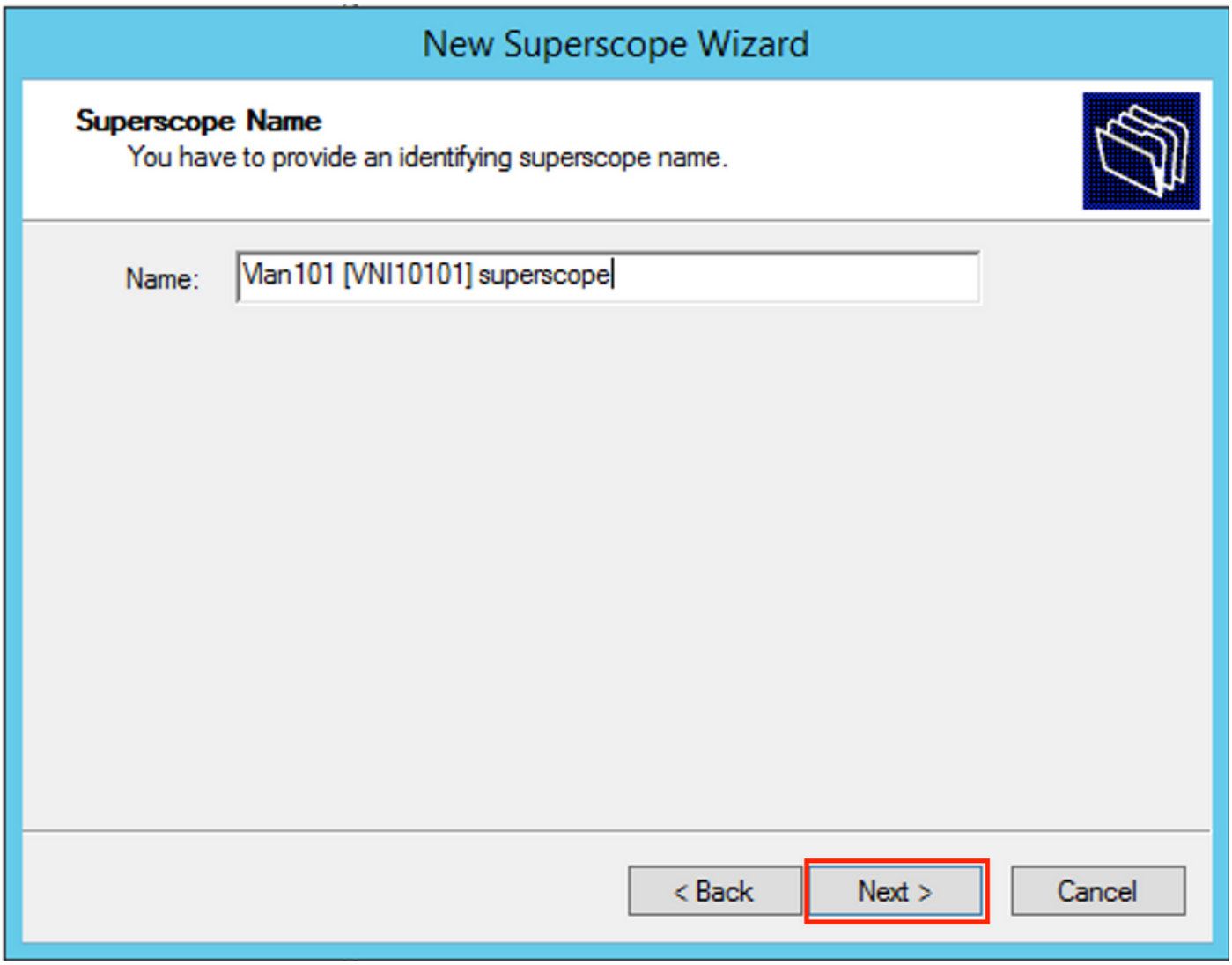
Erstellen Sie jetzt ein Superskop. Wählen Sie mit der rechten Maustaste **New Superscope** aus, wie im Bild gezeigt.



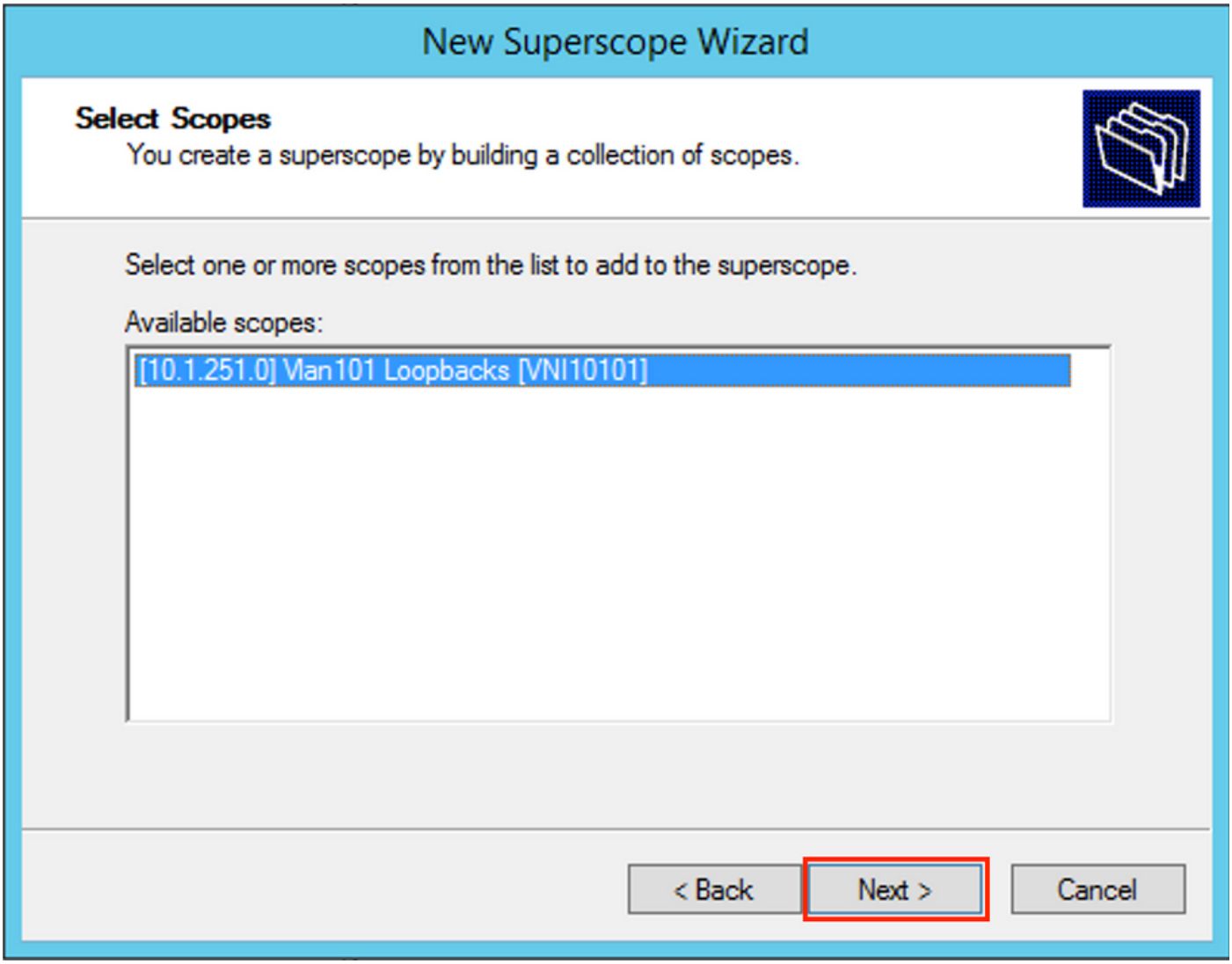
Wählen Sie **Weiter** aus, wie im Bild gezeigt.



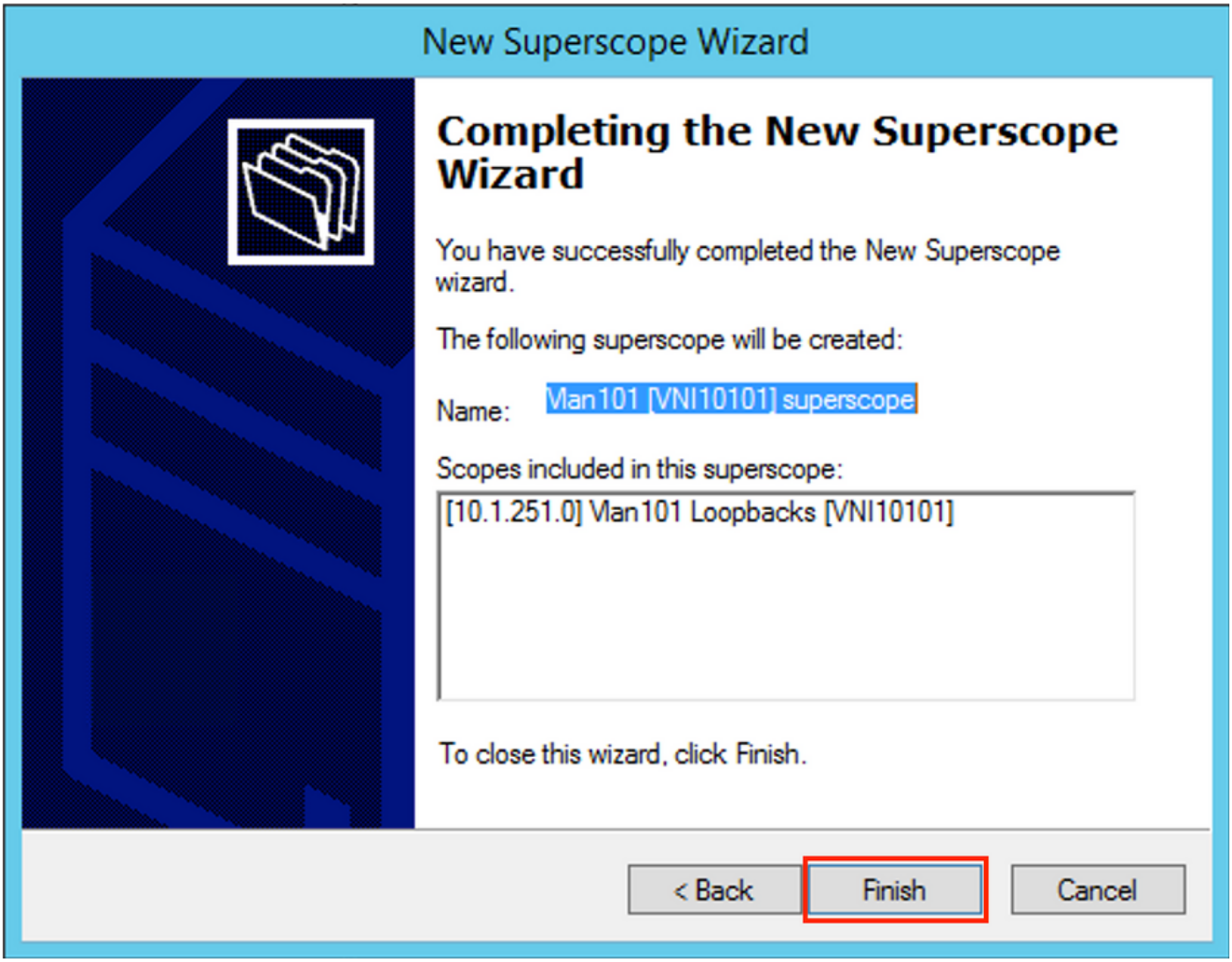
Wählen Sie einen aussagekräftigen Namen für den **Superscope** aus, wie im Bild gezeigt.



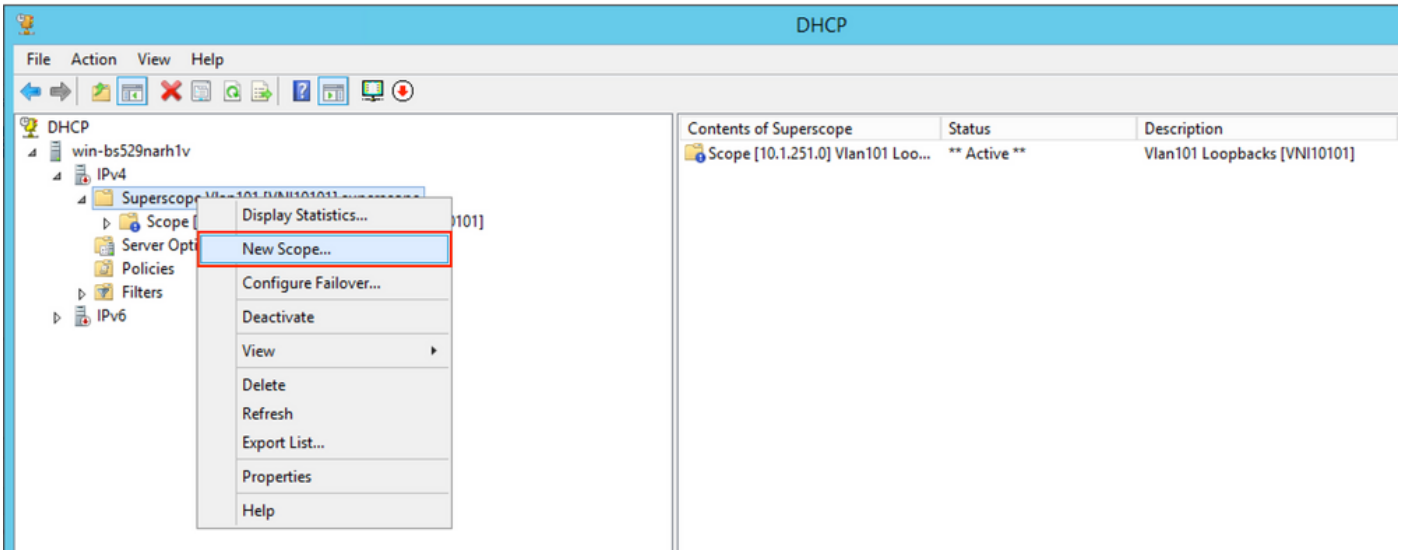
Wählen Sie den Bereich aus, der dem Superscope hinzugefügt werden soll.



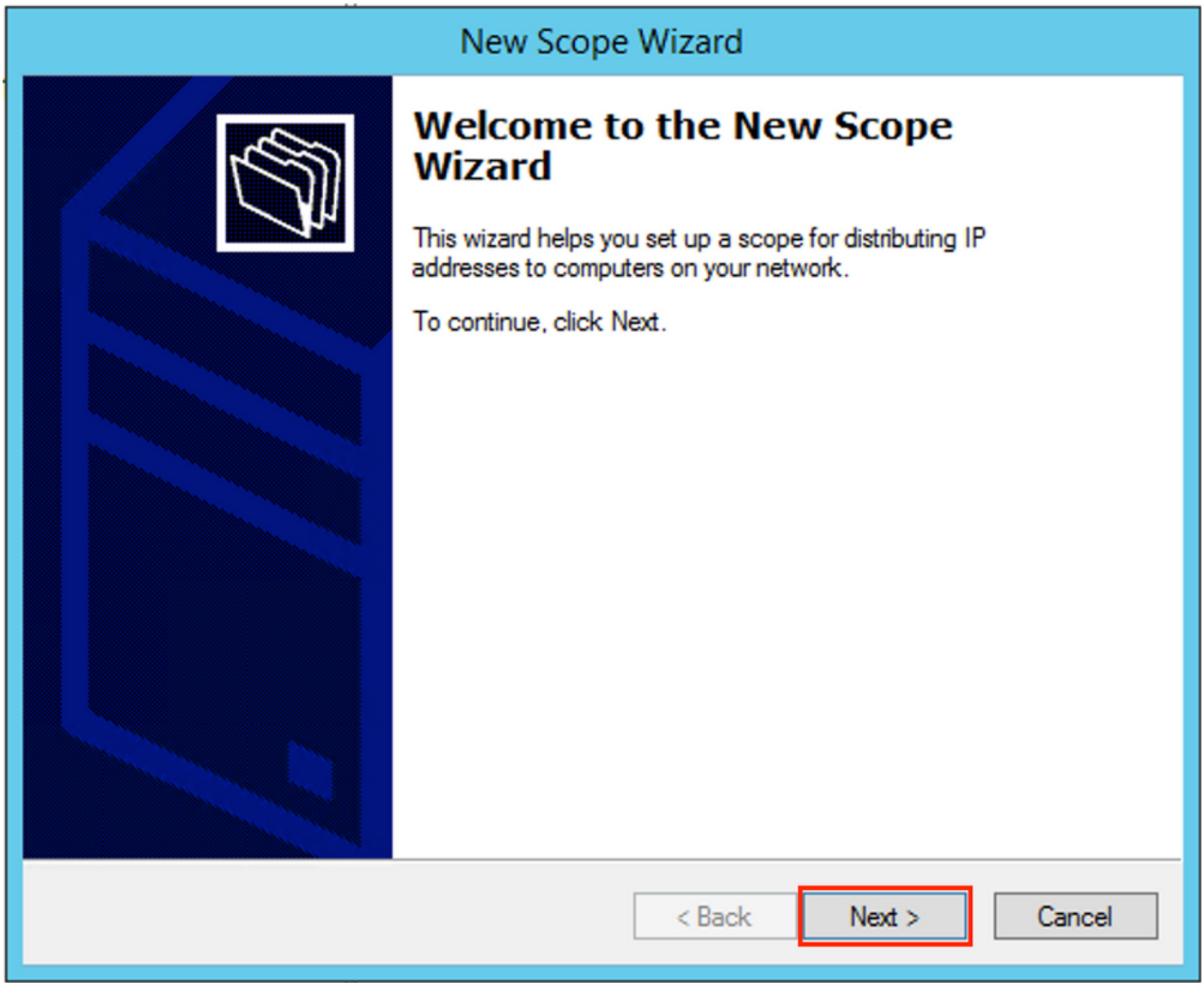
Schließen Sie das Setup wie im Bild gezeigt ab.



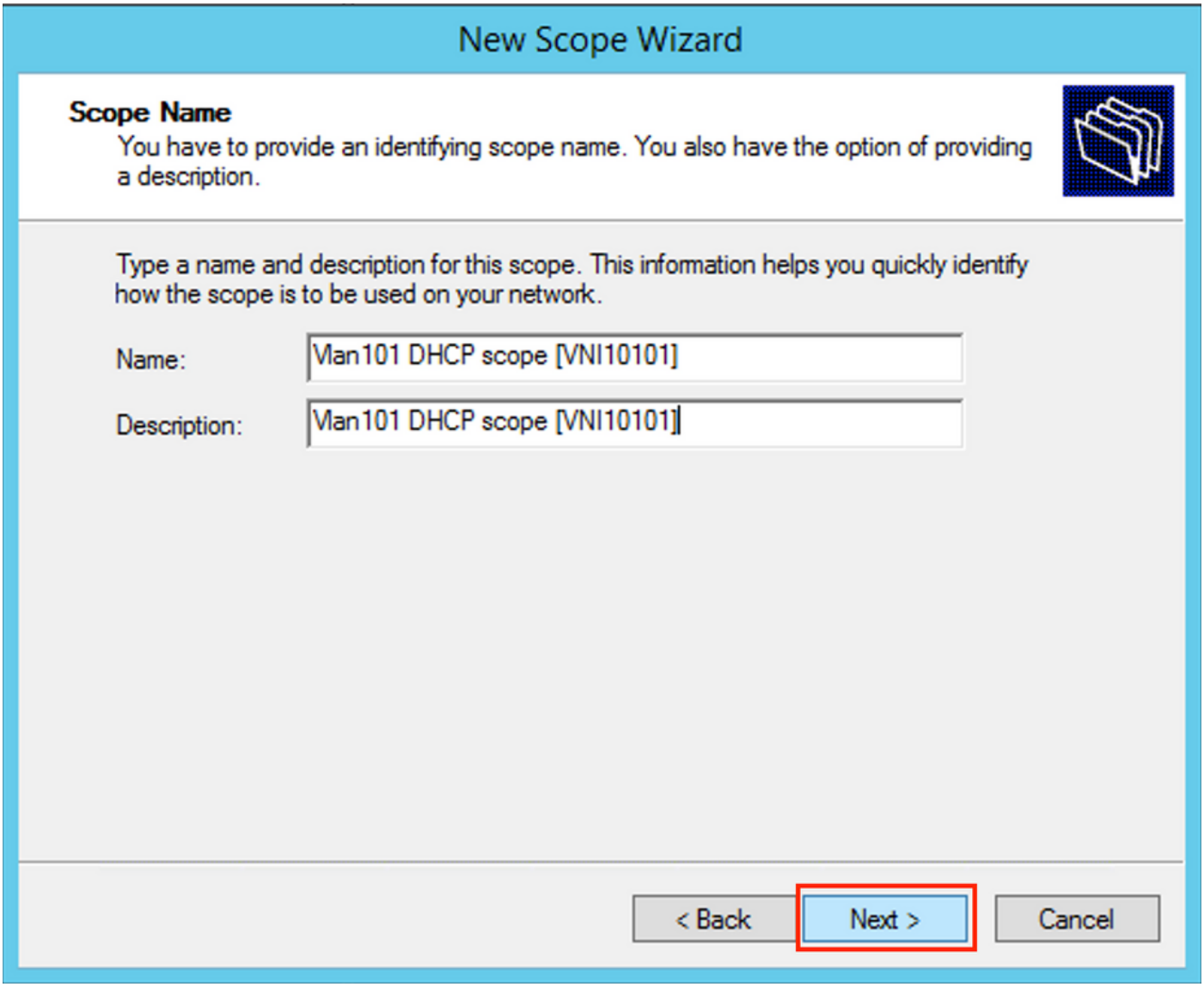
Erstellen Sie einen DHCP-Pool, aus dem IP-Adressen zugewiesen werden. Klicken Sie mit der rechten Maustaste, und wählen Sie **Neuer Bereich aus...** wie im Bild gezeigt.



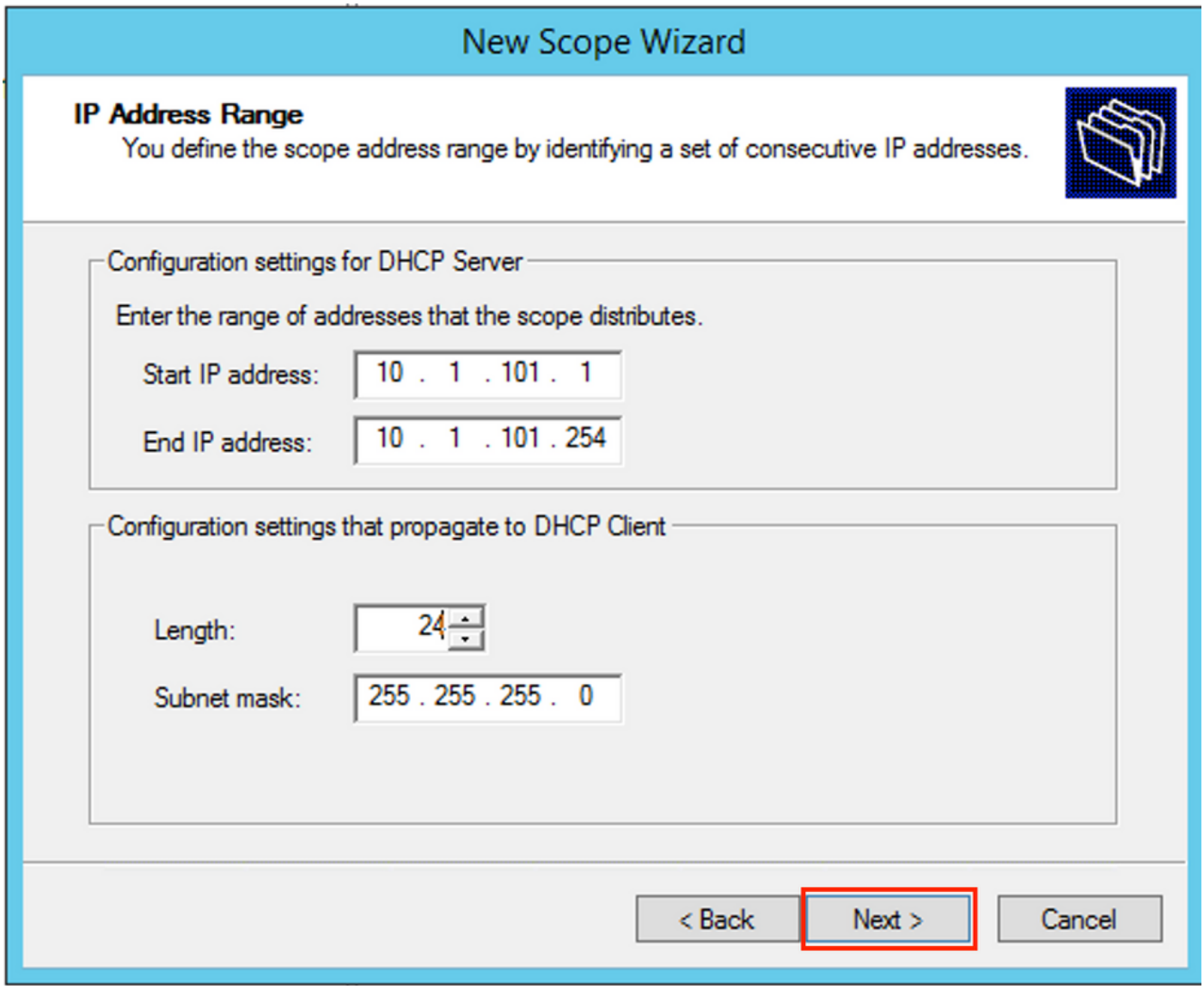
Wählen Sie **Weiter** aus, wie im Bild gezeigt.



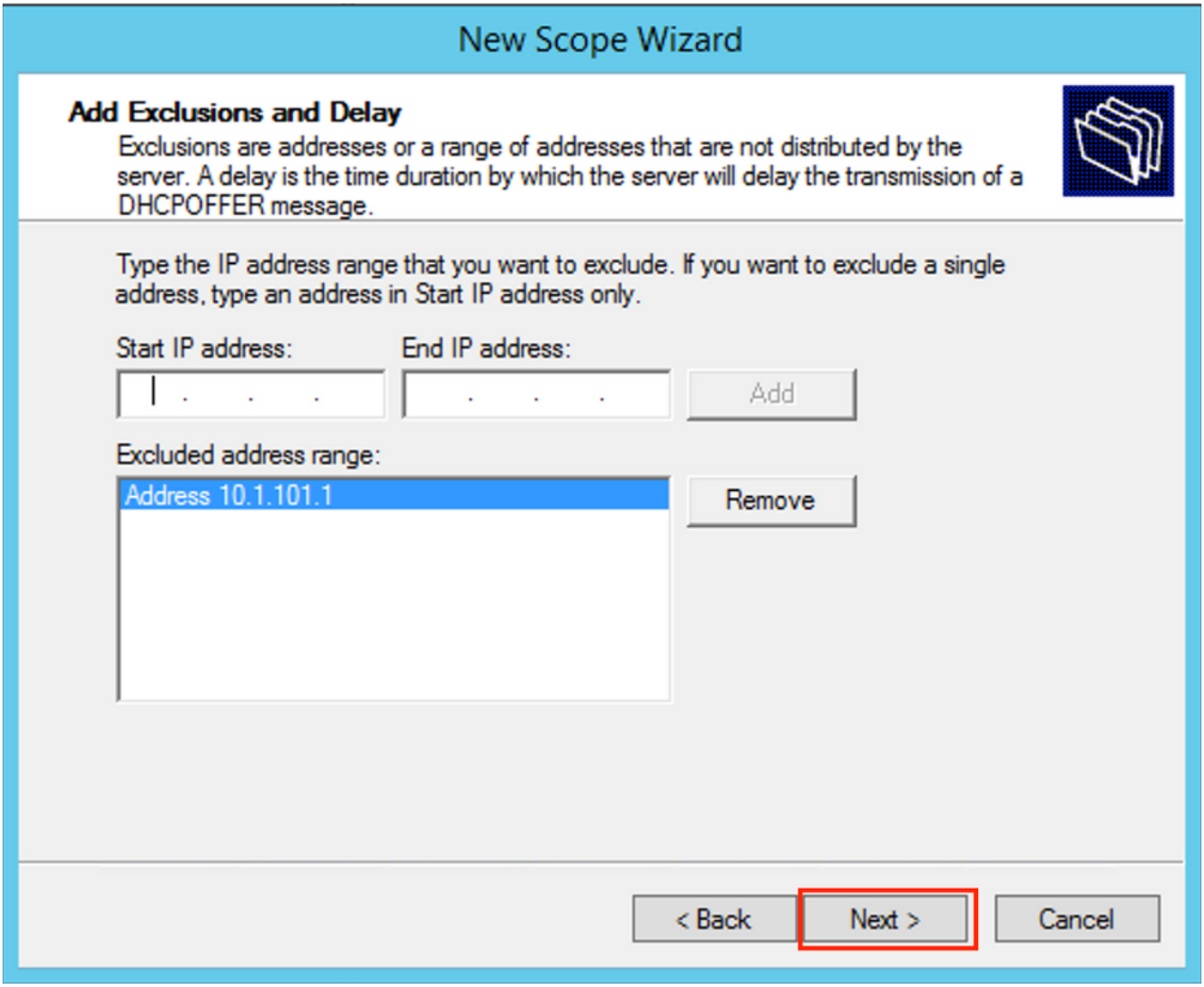
Wählen Sie einen aussagekräftigen Namen und eine Beschreibung aus, wie im Bild gezeigt.



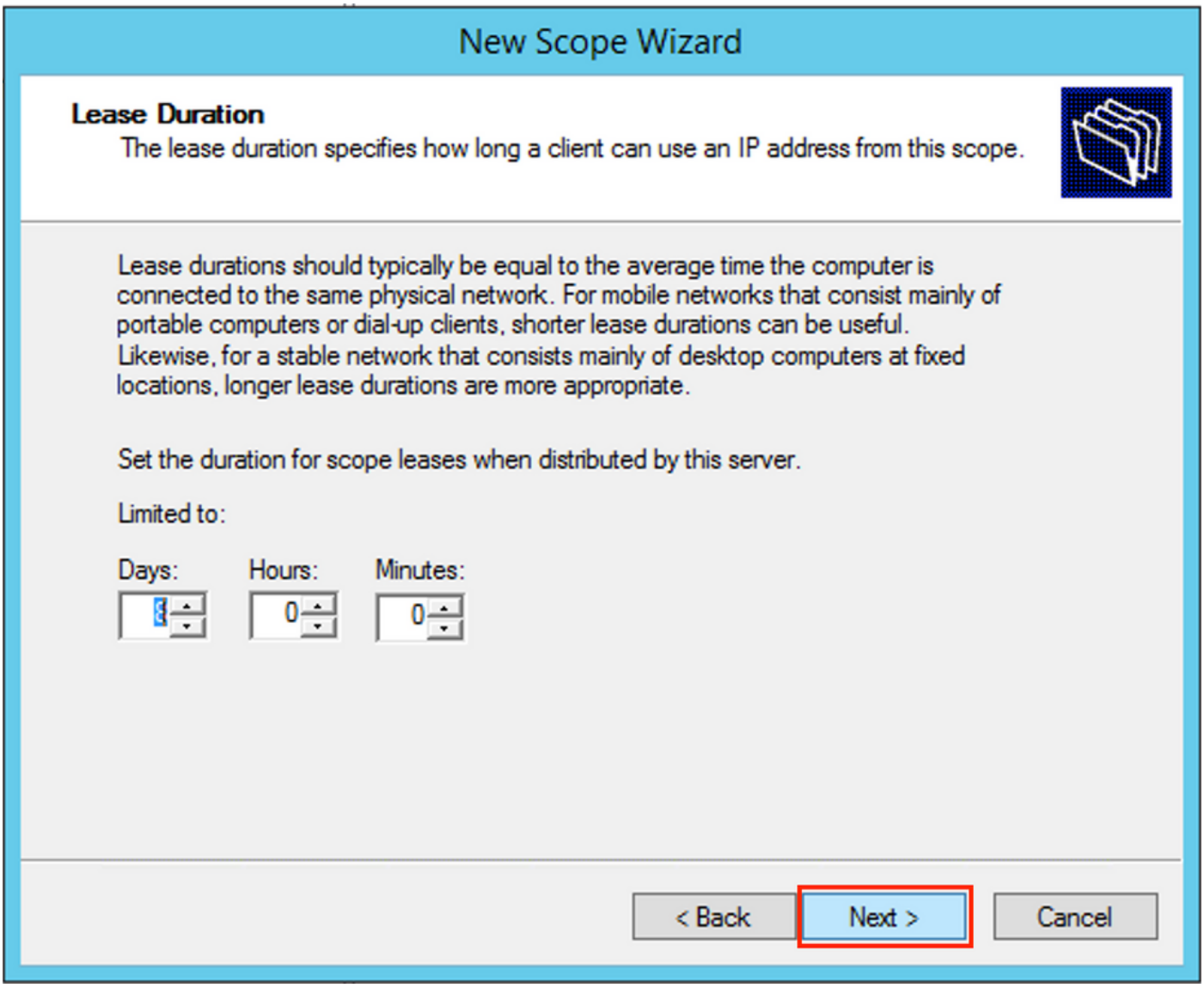
Geben Sie das Netzwerk und die Maske für den Pool an, dessen IP-Adressen Sie den Clients wie im Bild gezeigt zuweisen möchten.



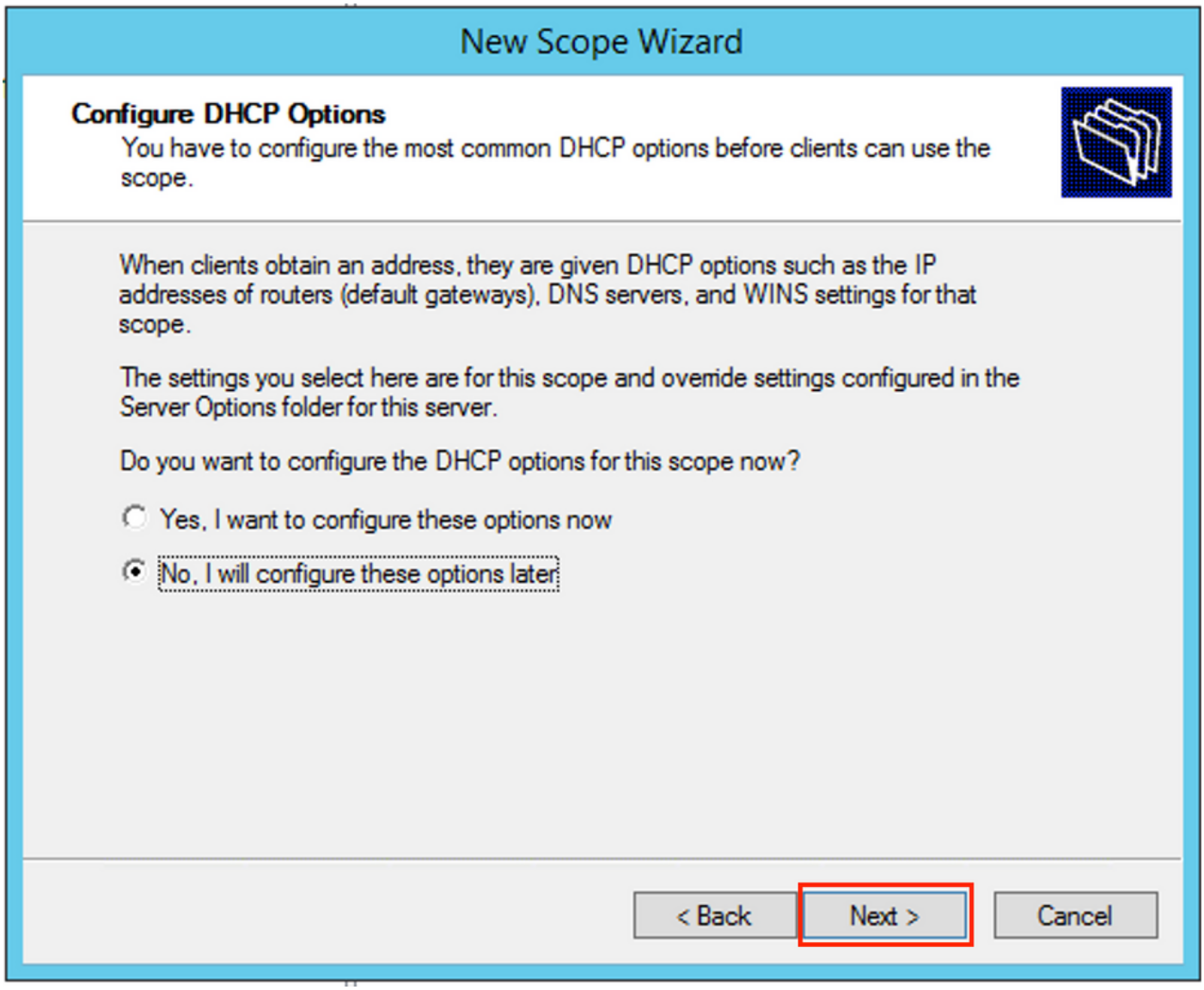
Nehmen Sie die IP-Adresse des DEFAULT-Gateways aus dem Pool (in diesem Beispiel ist es 10.1.101.1) heraus, wie im Bild gezeigt.



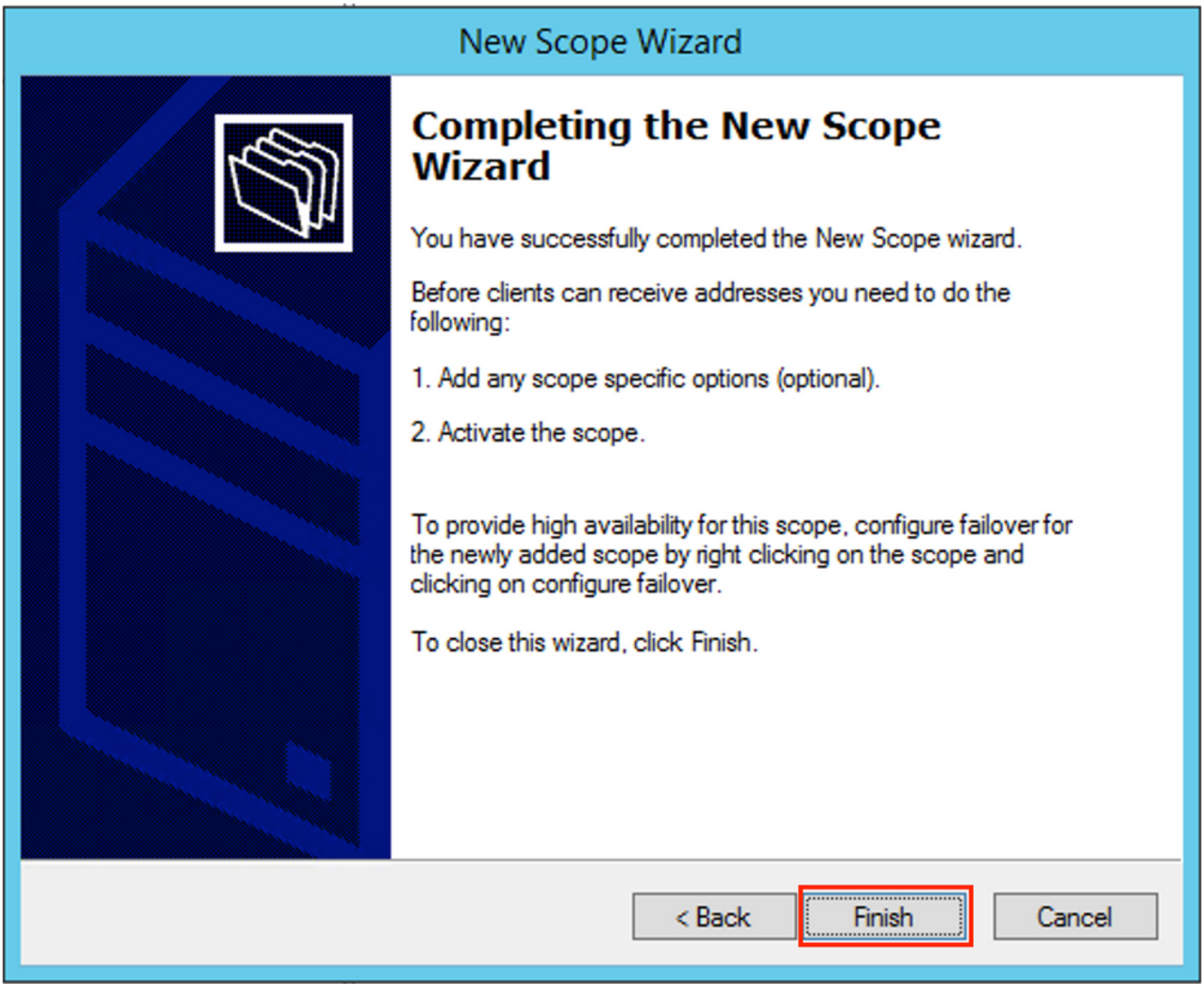
Geben Sie den Lease-Timer wie im Bild gezeigt an.



Optional können Sie DNS/WINS angeben (in diesem Beispiel übersprungen).



Schließen Sie die Konfiguration wie im Bild gezeigt ab.



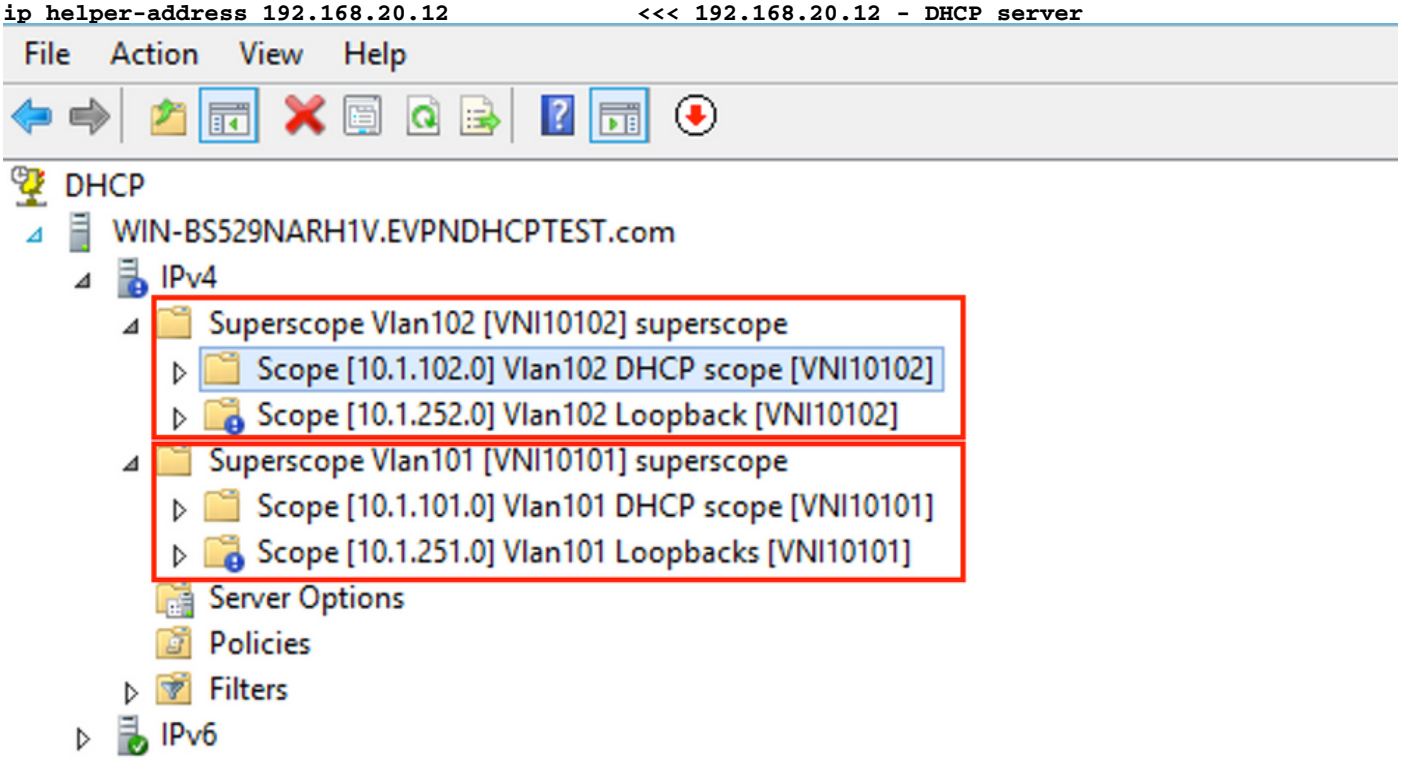
Nach der Erstellung des Pools muss eine Richtlinie für den Pool erstellt werden.

- In der Richtlinie Agent Circuit ID [1] ist zugeordnet
- Wenn Sie über mehrere VLANs/VNIs verfügen, müssen Sie einen Superpool mit Subpools für Relay-IP-Adressen und den tatsächlichen IP-Bereich für die Zuweisung pro VLAN/VNI erstellen.
- In diesem Beispiel werden die VNIs 10101 und 10102 verwendet.

Switch-Konfiguration:

```
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
```

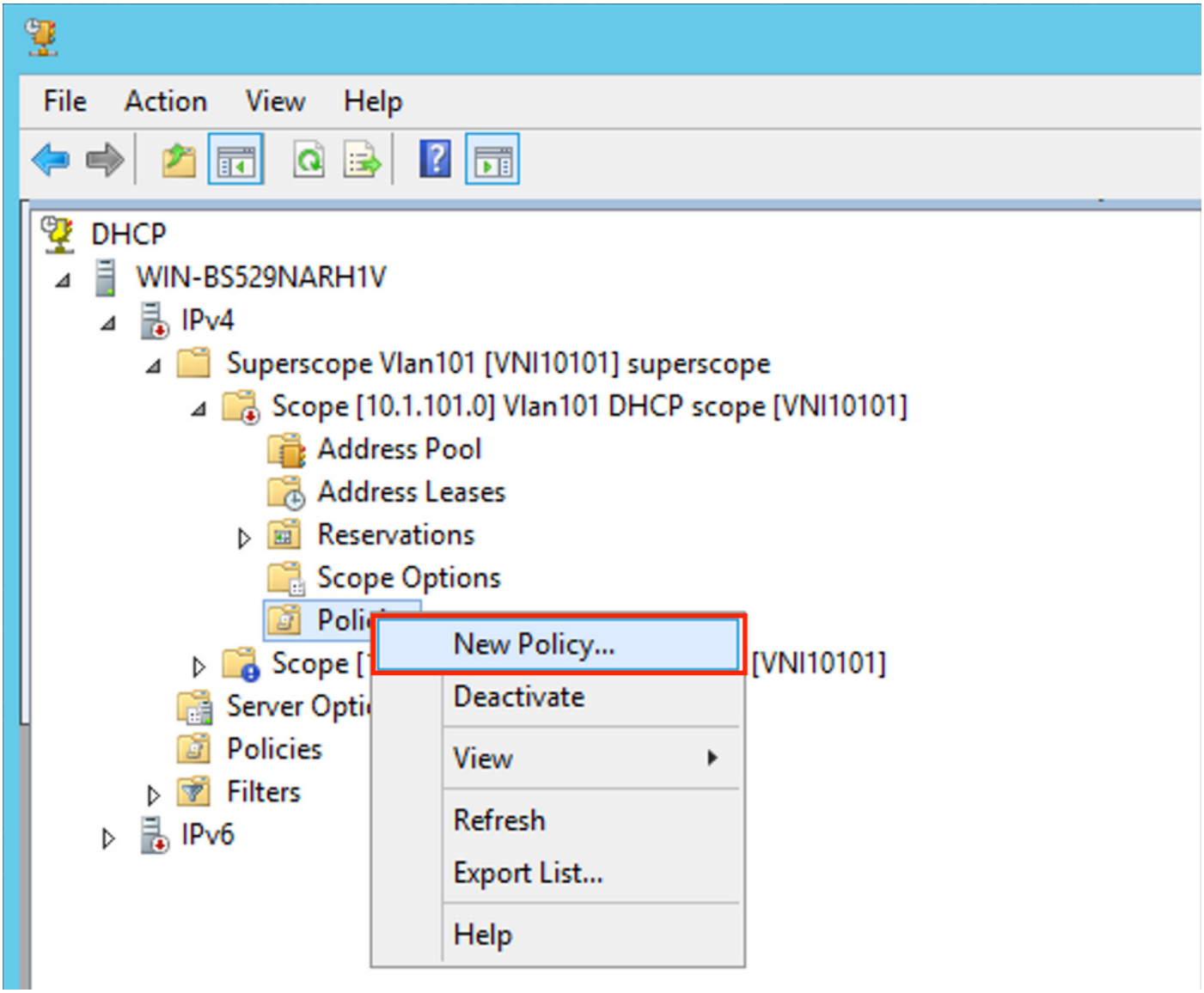
```
 ip address 10.1.251.2 255.255.255.255
!
interface Vlan101
 vrf forwarding green
 ip dhcp relay source-interface Loopback101  <<< DHCP relay source is unique Loopback101
 ip address 10.1.101.1 255.255.255.0
ip helper-address 192.168.20.12             <<< 192.168.20.12 - DHCP server
!
interface Vlan102
 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
```



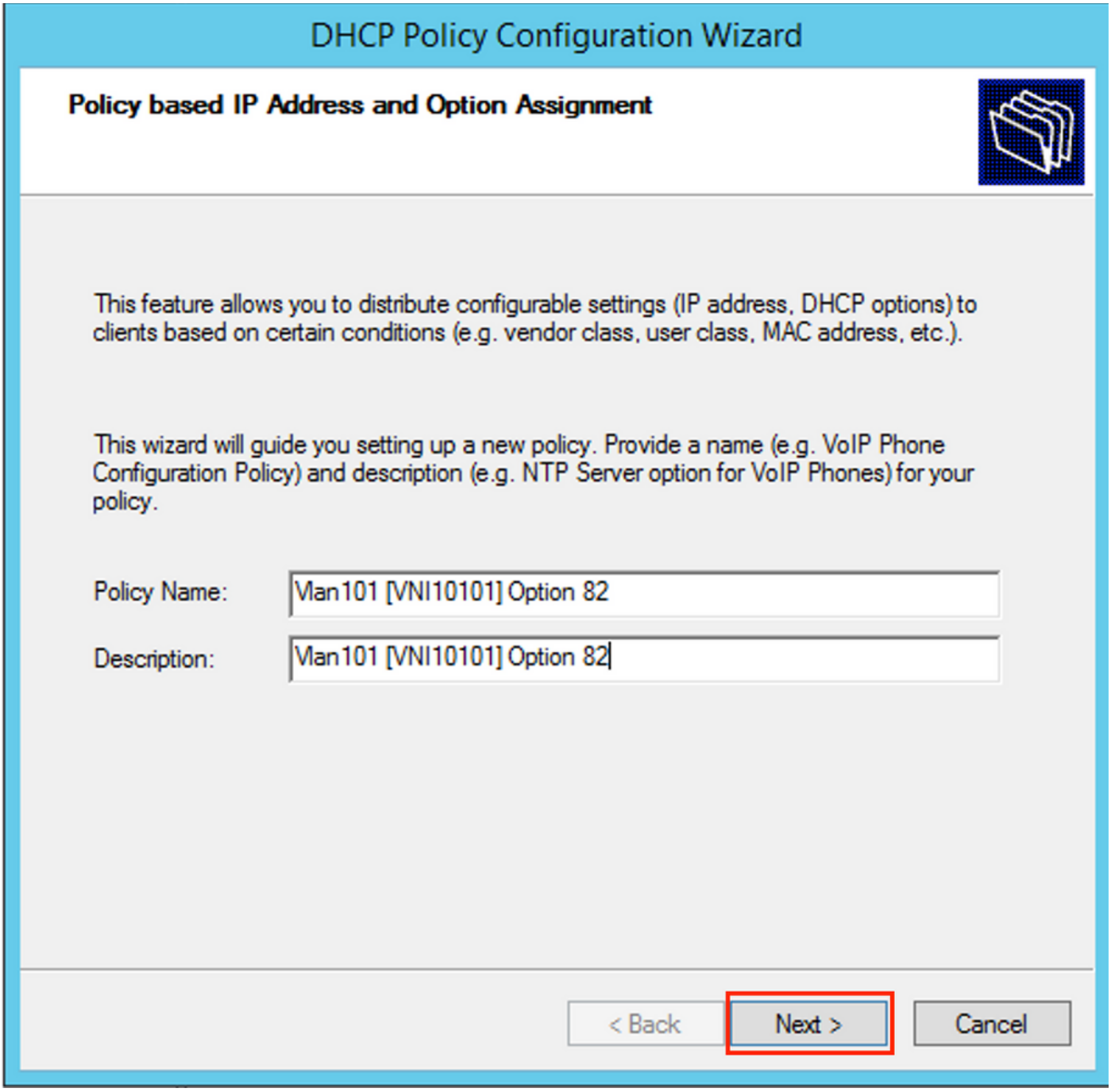
Win2012 R2 Konfigurationsoption 2 - Zuordnen des Agenten-Circuit-ID-Felds

- Der Nachteil des letzten Ansatzes ist die hohe Auslastung des eindeutigen Loopbacks. Eine weitere Option besteht also darin, das Feld "Agent Circuit ID" (Agenten-Circuit-ID) zu verwenden.
- Die Schritte sind identisch, Sie fügen jedoch Richtlinien für die Bereichsauswahl hinzu, die nicht auf dem Agent Circuit-ID-Feld statt auf Relay IP basieren.

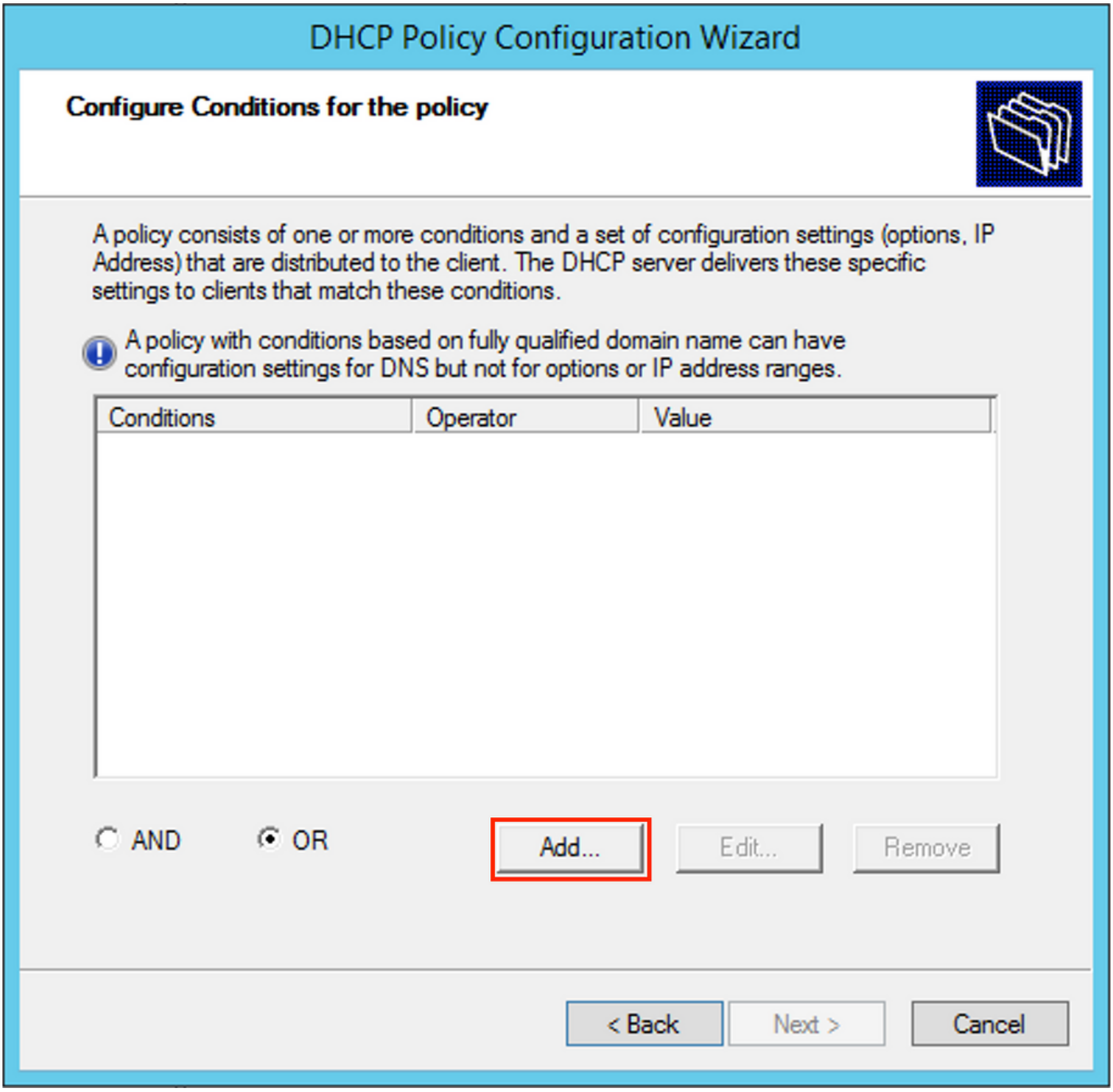
Richtlinienerstellung. Klicken Sie mit der rechten Maustaste auf den Pool, und wählen Sie **Neue Richtlinie** aus, wie im Bild gezeigt.



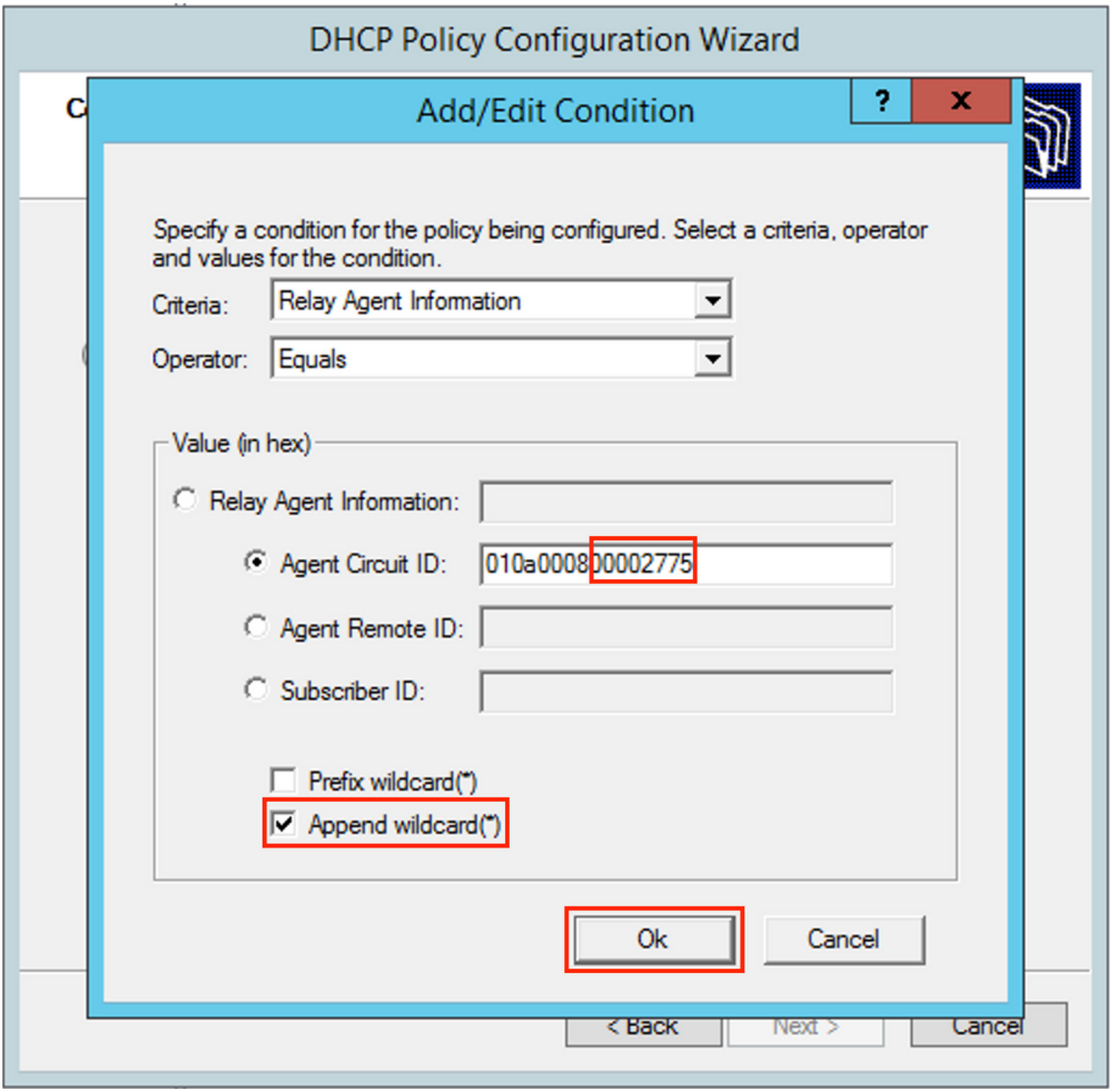
Wählen Sie einen aussagekräftigen Namen und eine Beschreibung für die Richtlinie aus, wie im Bild gezeigt.



Fügen Sie die neue Bedingung hinzu, wie im Bild gezeigt.



Geben Sie die richtige Circuit-ID ein (vergessen Sie nicht das **Append Wildcard (*)** Feld), wie im Bild gezeigt.



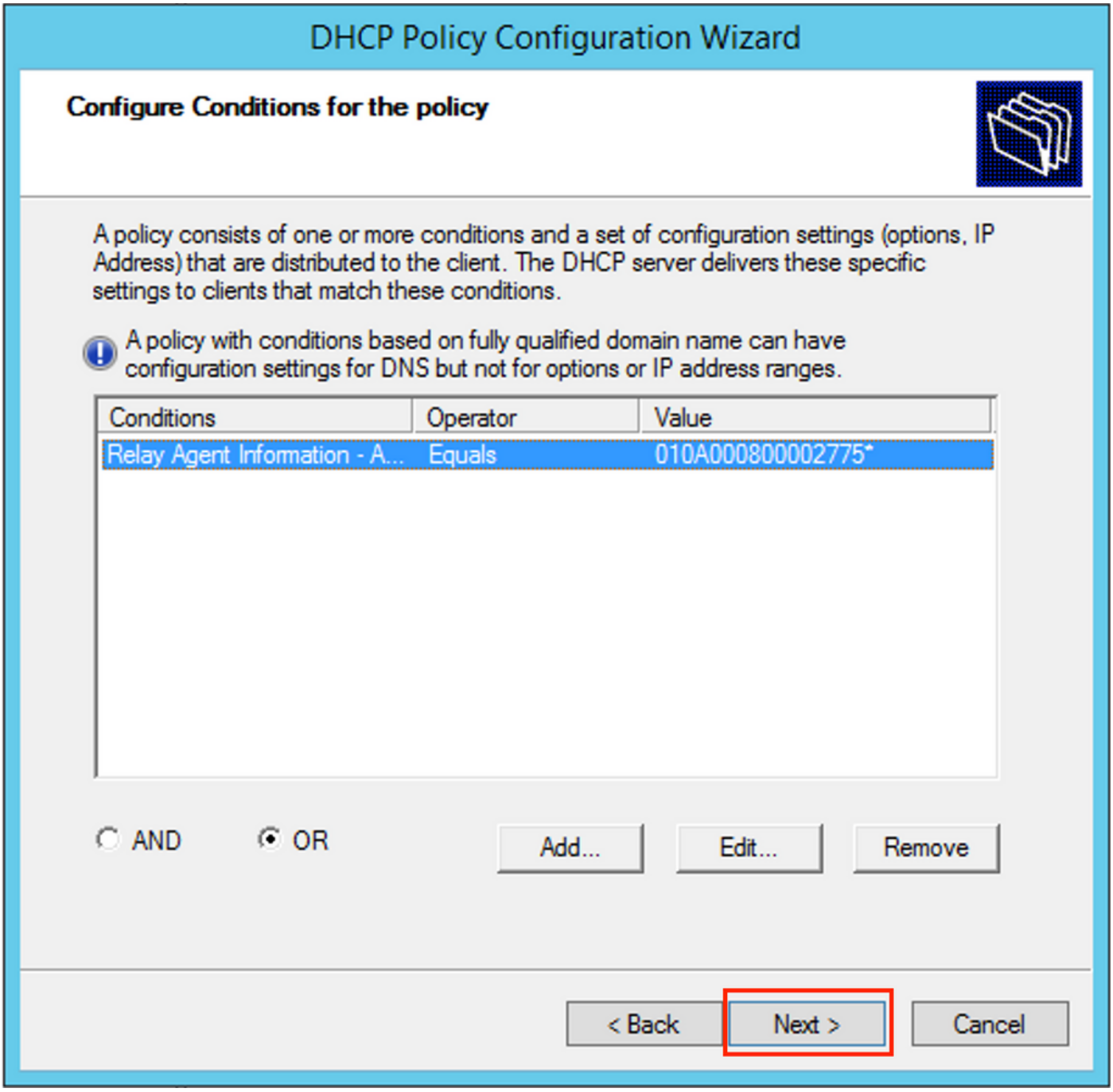
Erläuterung, warum diese Nummer gewählt wurde:

In Wireshark können Sie die Agenten-Circuit-ID gleich **010a00800002775010a0000** sehen, wobei dieser Wert von (00002775 hex = 101 abgeleitet wird. Die Dezimalzahl 01 entspricht der konfigurierten VNI 10101 für VLAN 101).

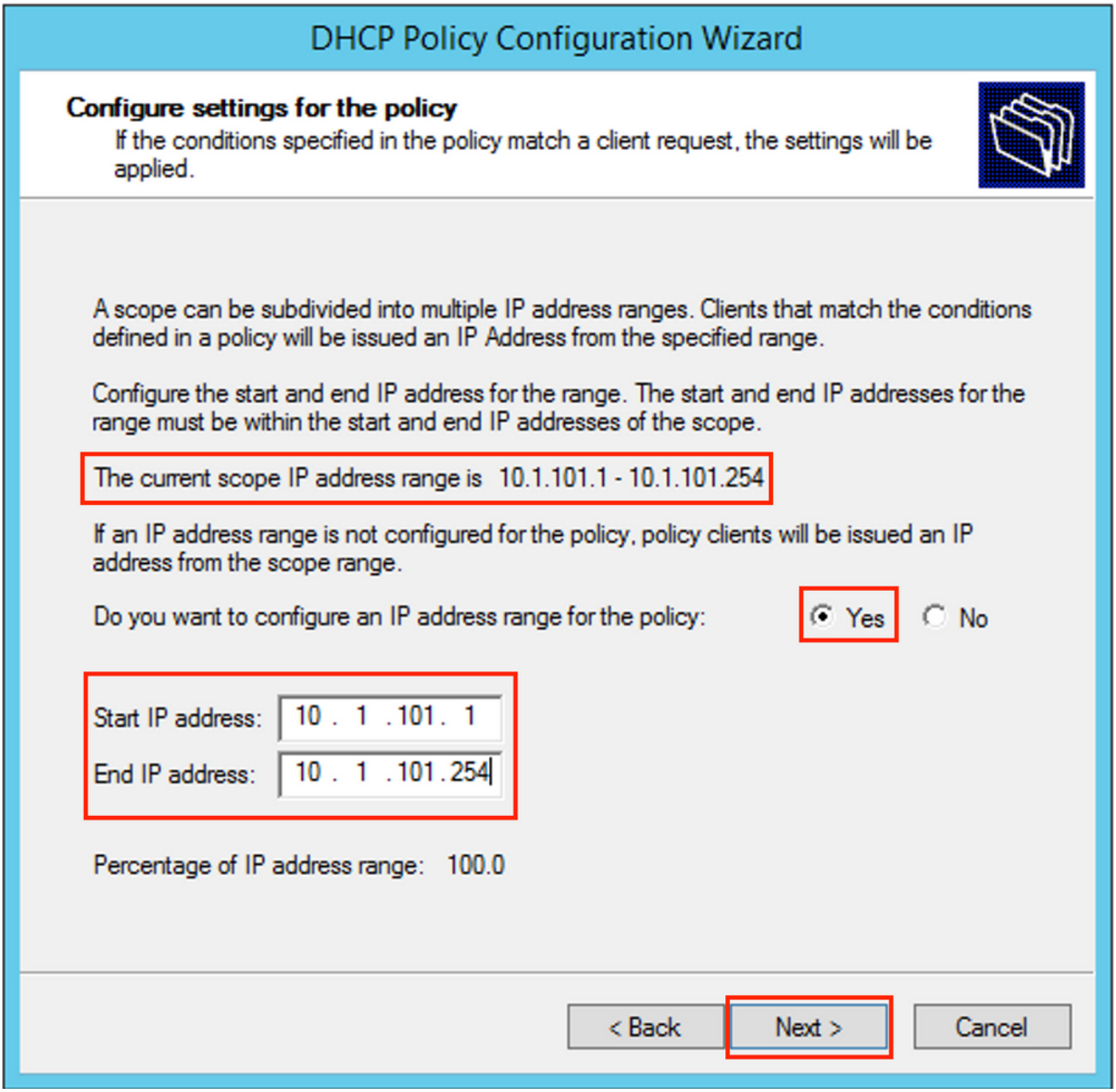
```
▼ Option: (82) Agent Information Option
    Length: 44
  ▼ Option 82 Suboption: (1) Agent Circuit ID
      Length: 12
      Agent Circuit ID: 010a000800002775010a0000
  ▶ Option 82 Suboption: (2) Agent Remote ID
  ▶ Option 82 Suboption: (151) VRF name/VPN ID
  ▼ Option 82 Suboption: (150) Link selection (Cisco proprietary)
      Length: 4
      Link selection (Cisco proprietary): 10.1.101.0
  ▼ Option 82 Suboption: (152) Server ID Override (Cisco proprietary)
      Length: 4
      Server ID Override (Cisco proprietary): 10.1.101.1
```

Agent Circuit ID-Suboption ist in diesem Format für VXLAN VN verschlüsselt:

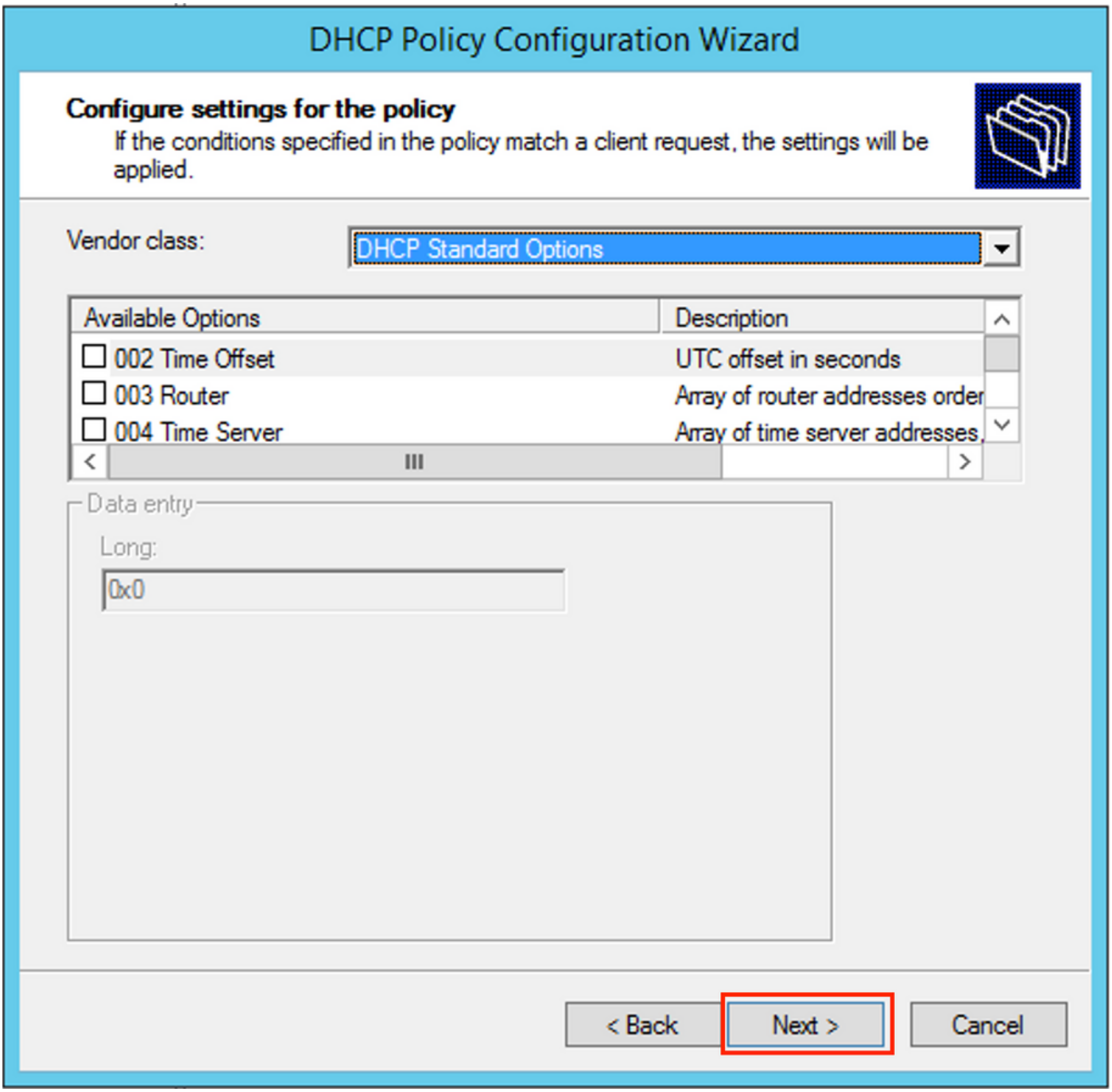
Subtyp	Länge	Circuit-ID-Typ	Länge	VNI	Mod	anschluss
1 Byte	1 Byte	1 Byte	1 Byte	4 Byte	2 Byte	2 Byte
01	0 A	00	08	00002775	*	*



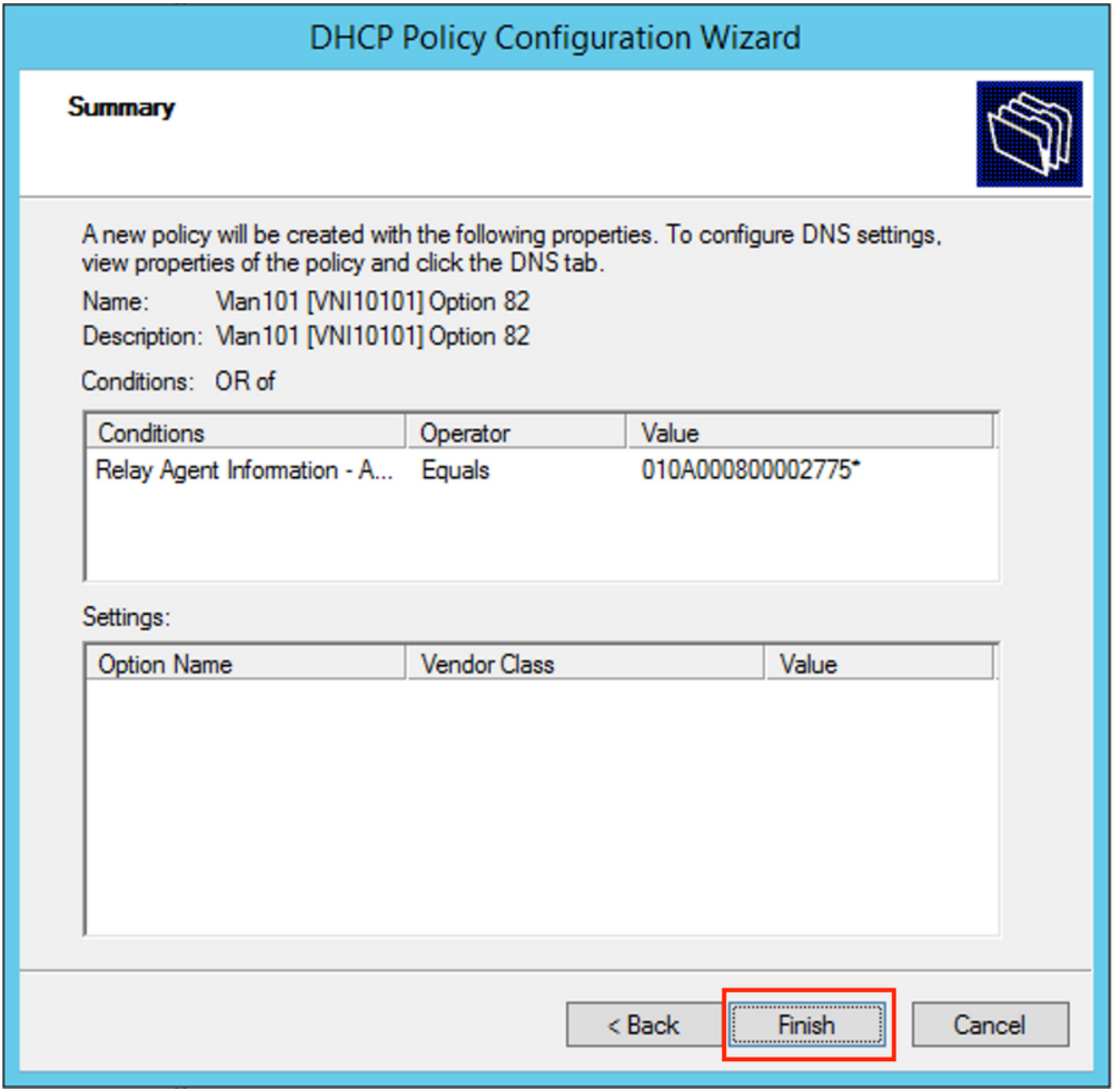
Konfigurieren Sie den IP-Bereich, dem IP-Adressen zugewiesen werden. Ohne diese Konfiguration ist keine Zuweisung für den **aktuellen Umfang** möglich.



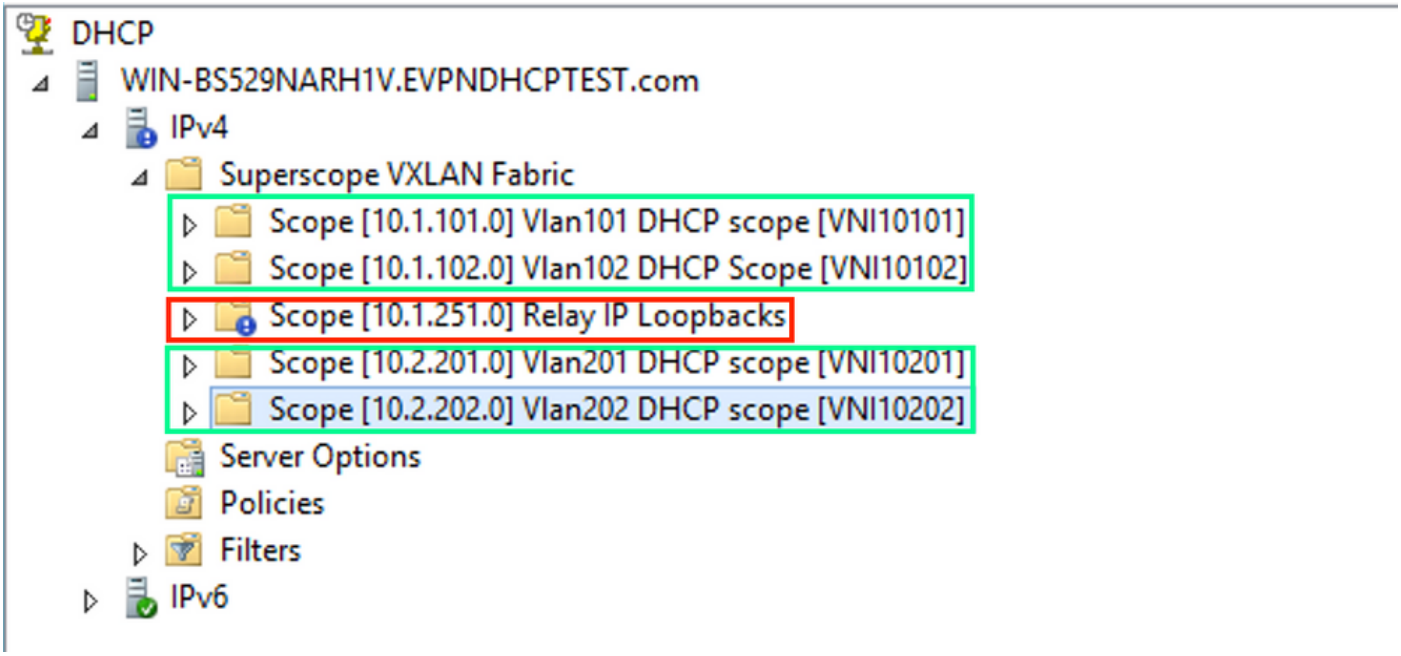
Sie können zu diesem Zeitpunkt auch Standard-DHCP-Optionen auswählen, wie im Bild gezeigt.



Wählen Sie **Fertig stellen** wie im Bild gezeigt.



Eine ähnliche Konfiguration muss für andere Bereiche vorgenommen werden, wie im Bild gezeigt.



In diesem Szenario können Sie für die Anzahl der SVIs nur eine eindeutige IP-Adresse pro VTEP verwenden, nicht einen eindeutigen Loopback pro VNI/SVI pro VTEP.

Switch-Konfiguration:

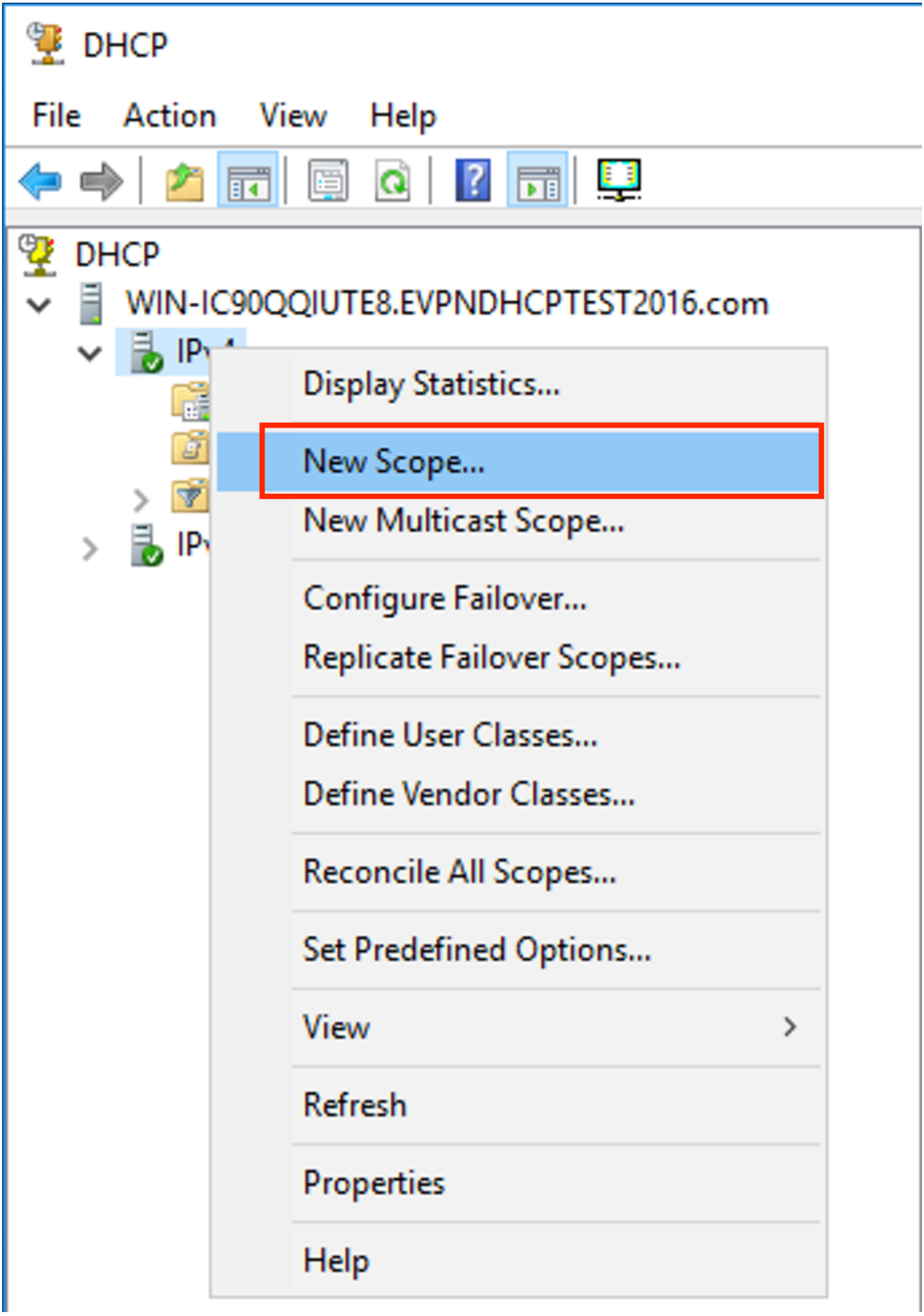
```
ip dhcp relay information option vpn     <<<  adds the VRF name/VPN ID to the option 82
ip dhcp relay information option         <<< enables option 82
!
ip dhcp snooping vlan 101-102,201-202
ip dhcp snooping
!
vlan configuration 101
member evpn-instance 101 vni 10101
!
interface Loopback101
 vrf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

Konfiguration von Windows Server 2016

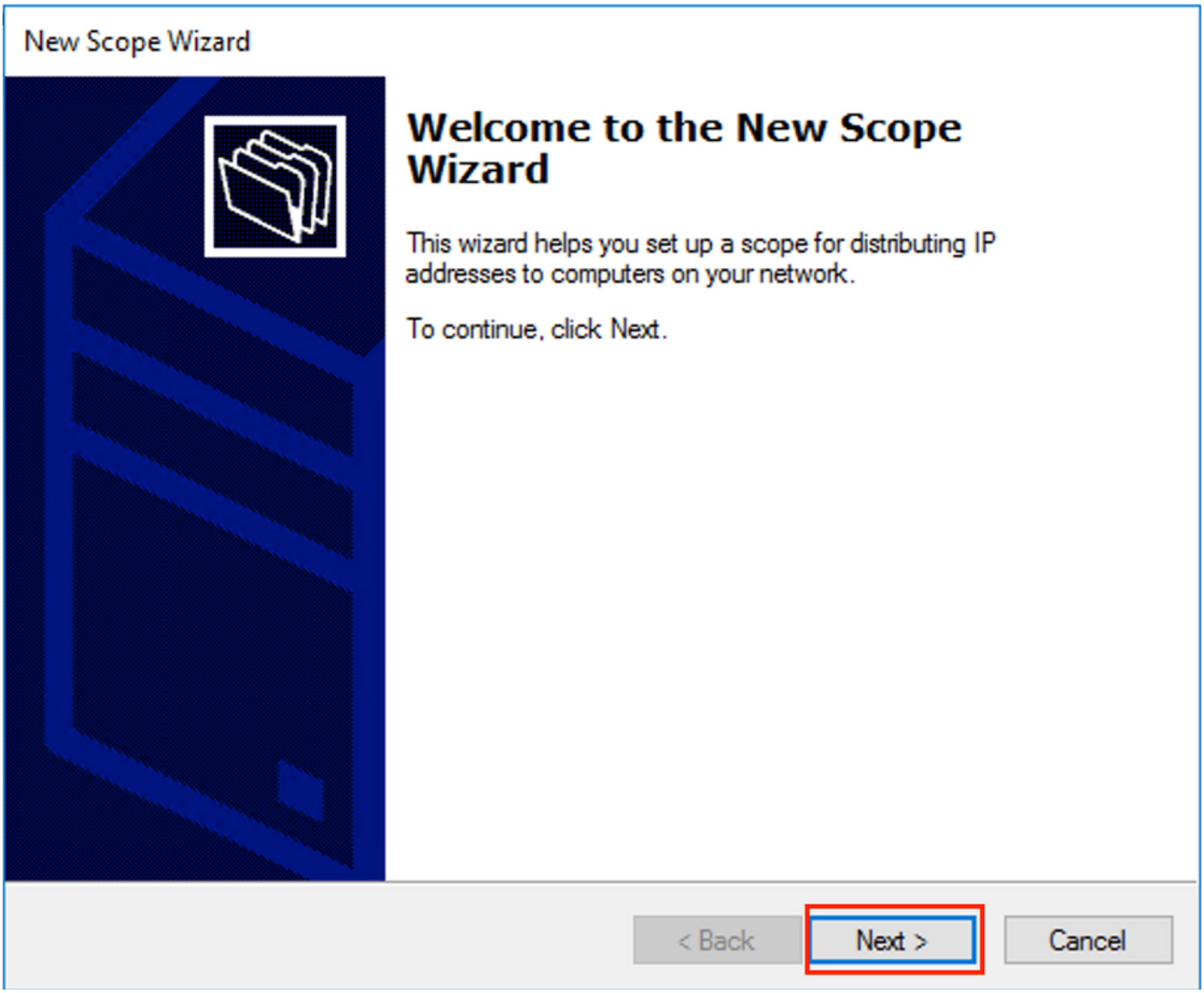
- Windows Server 2016 unterstützt Option 82 Unteroptionen 5 (Cisco proprietär 150) "Verbindungsauswahl". Das bedeutet, dass Sie keine eindeutige Relay-IP-Adresse für die Pool-Auswahl verwenden. Stattdessen wird die Unteroption "Verbindungsauswahl" verwendet, die die Konfiguration deutlich vereinfacht.
- Am besten wäre es, wenn Sie immer noch einen Pool für Relay-IP-Adressen hätten, da DHCP-Pakete ansonsten keinem Bereich entsprechen und nicht verarbeitet werden.

In diesem Beispiel wird die Verwendung der Option "Verbindungsauswahl" veranschaulicht.

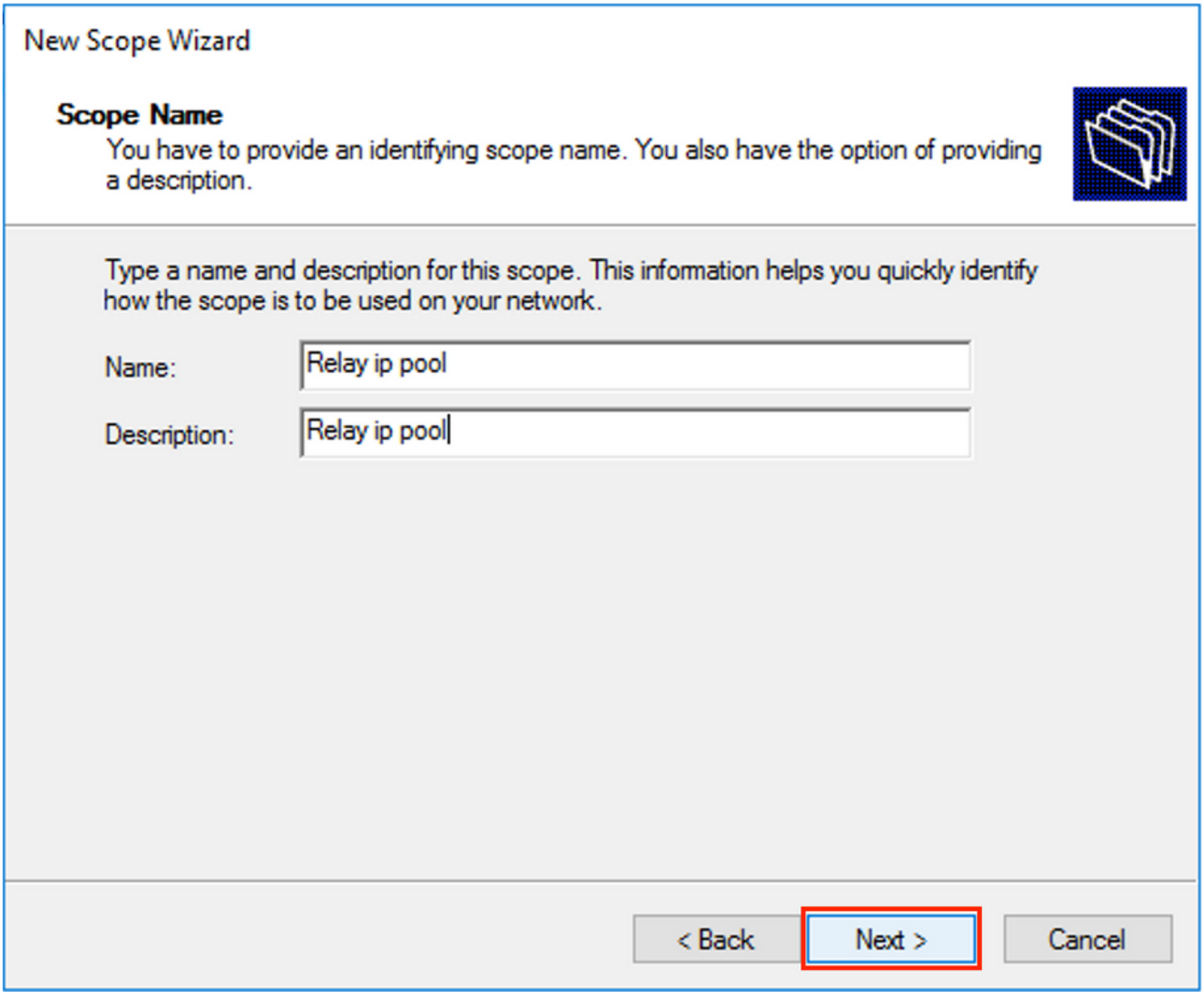
Initiieren Sie einen IP-Adresspool für Relay-IP-Adressen, wie im Bild gezeigt.


DHCP
File
Action
View
Help
DHCP
WIN-IC90QQIUTE8.EVPNDHCPTEST2016.com
IPv
IPv
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

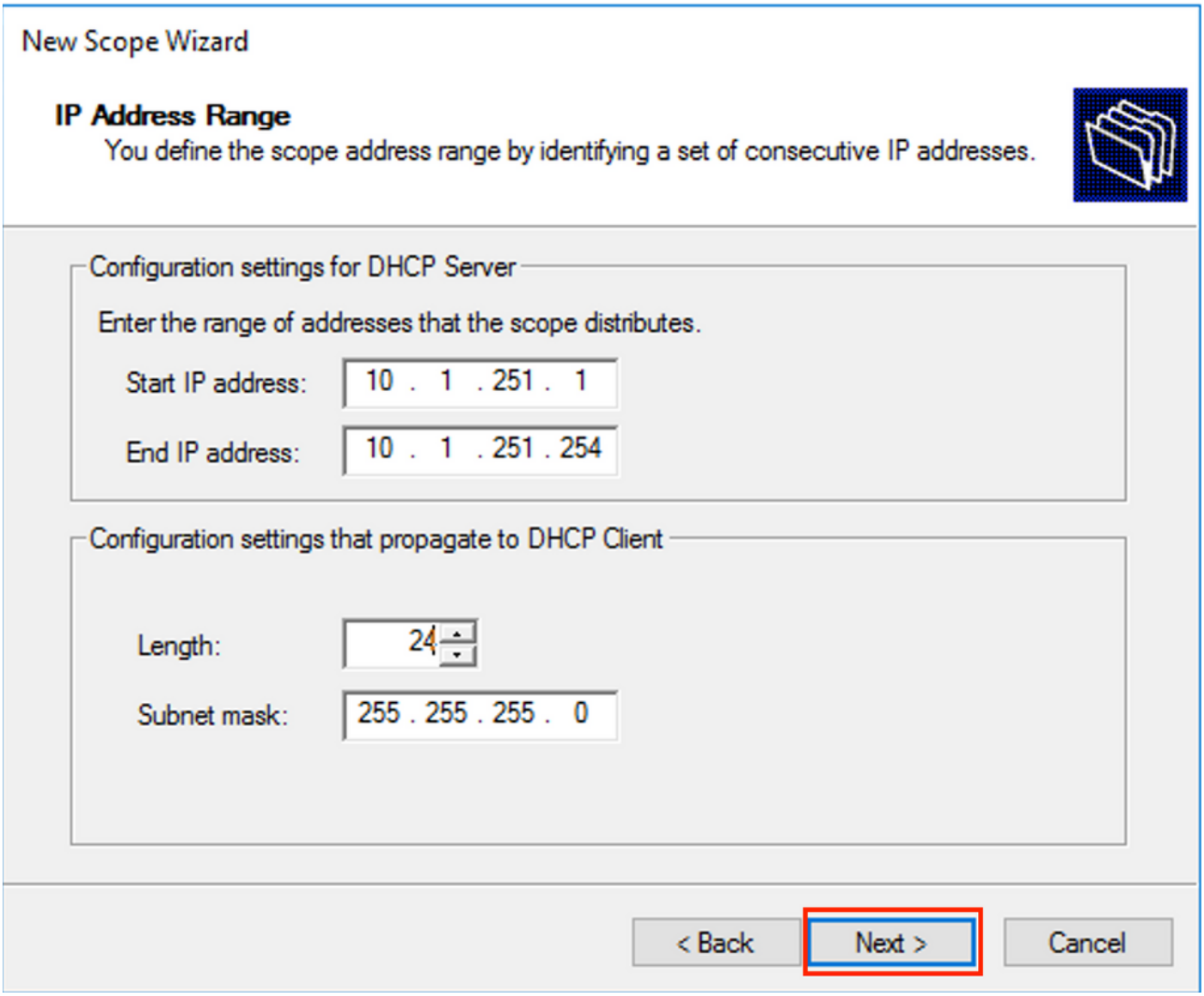
Wählen Sie **Weiter** aus, wie im Bild gezeigt.



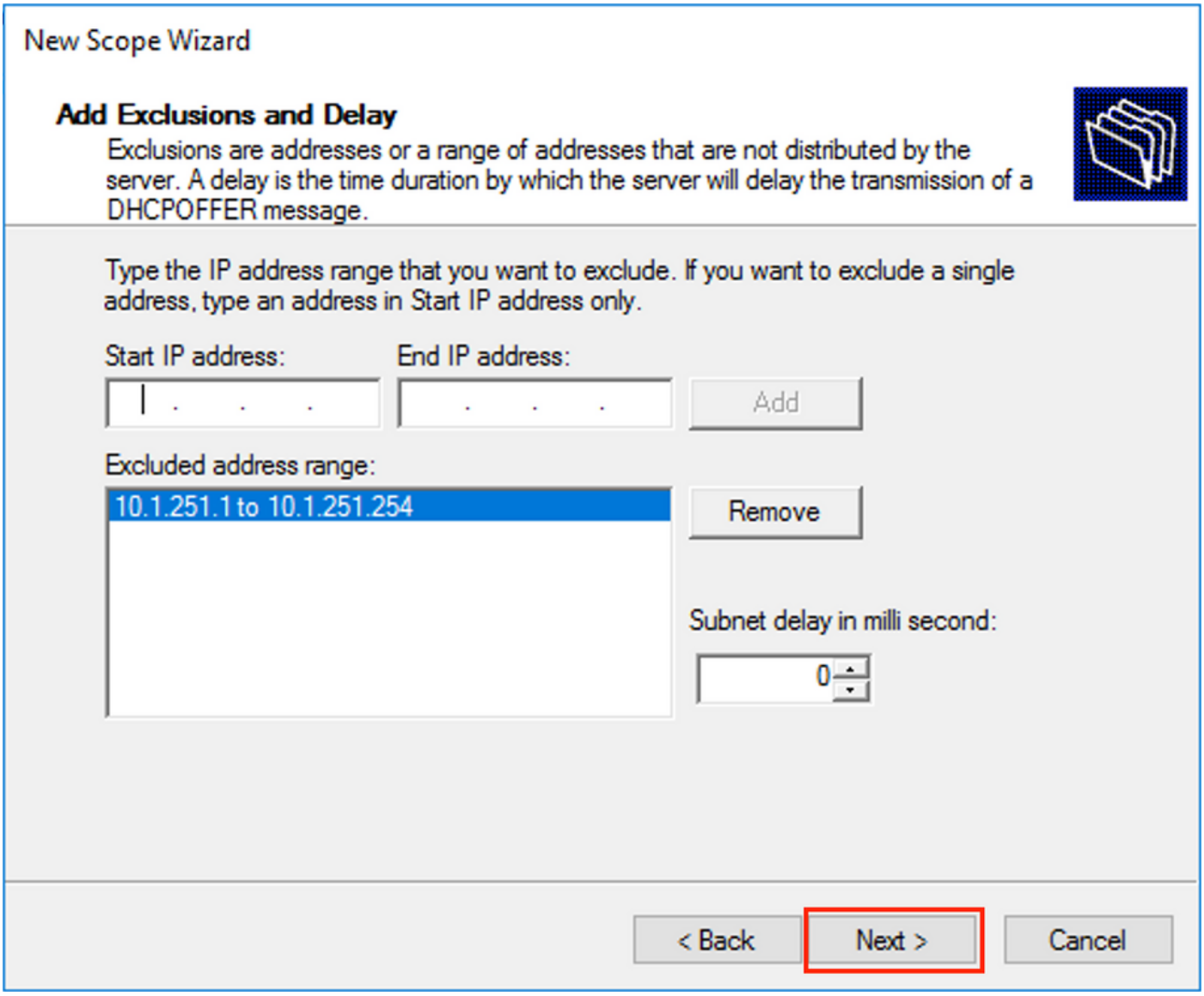
Wählen Sie einen aussagekräftigen Namen und eine Beschreibung für den Bereich, wie im Bild gezeigt.



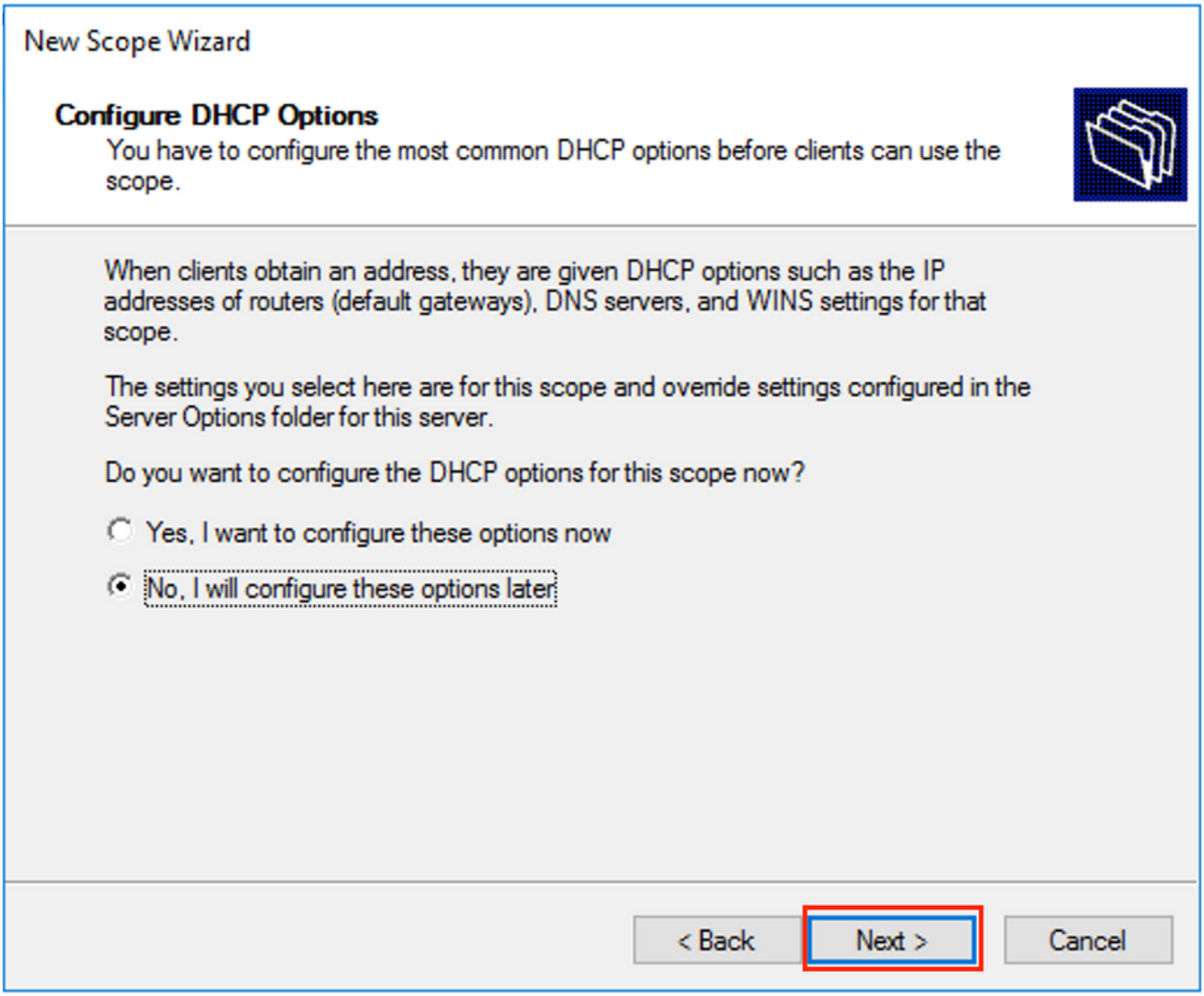
Geben Sie den IP-Adressbereich ein, der für IP-Relays wie im Bild gezeigt verwendet wird.



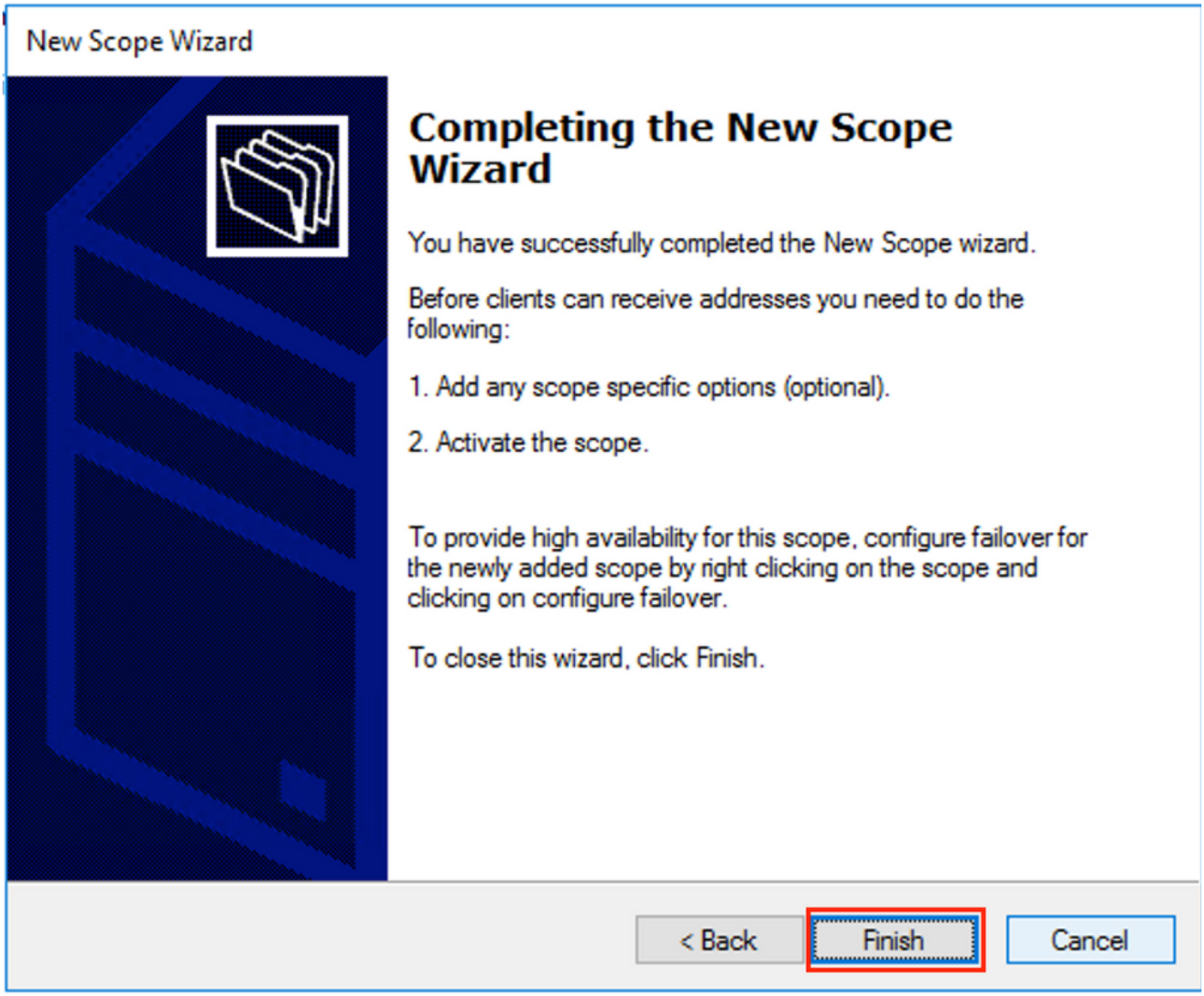
Schließen Sie alle Bereiche aus dem Bereich aus, um die Zuweisung aus diesem Bereich zu verhindern, wie im Bild gezeigt.



Sie können auch die Option DNS/WINS etc Parameter (übersprungen in diesem Beispiel) wählen, wie im Bild gezeigt.

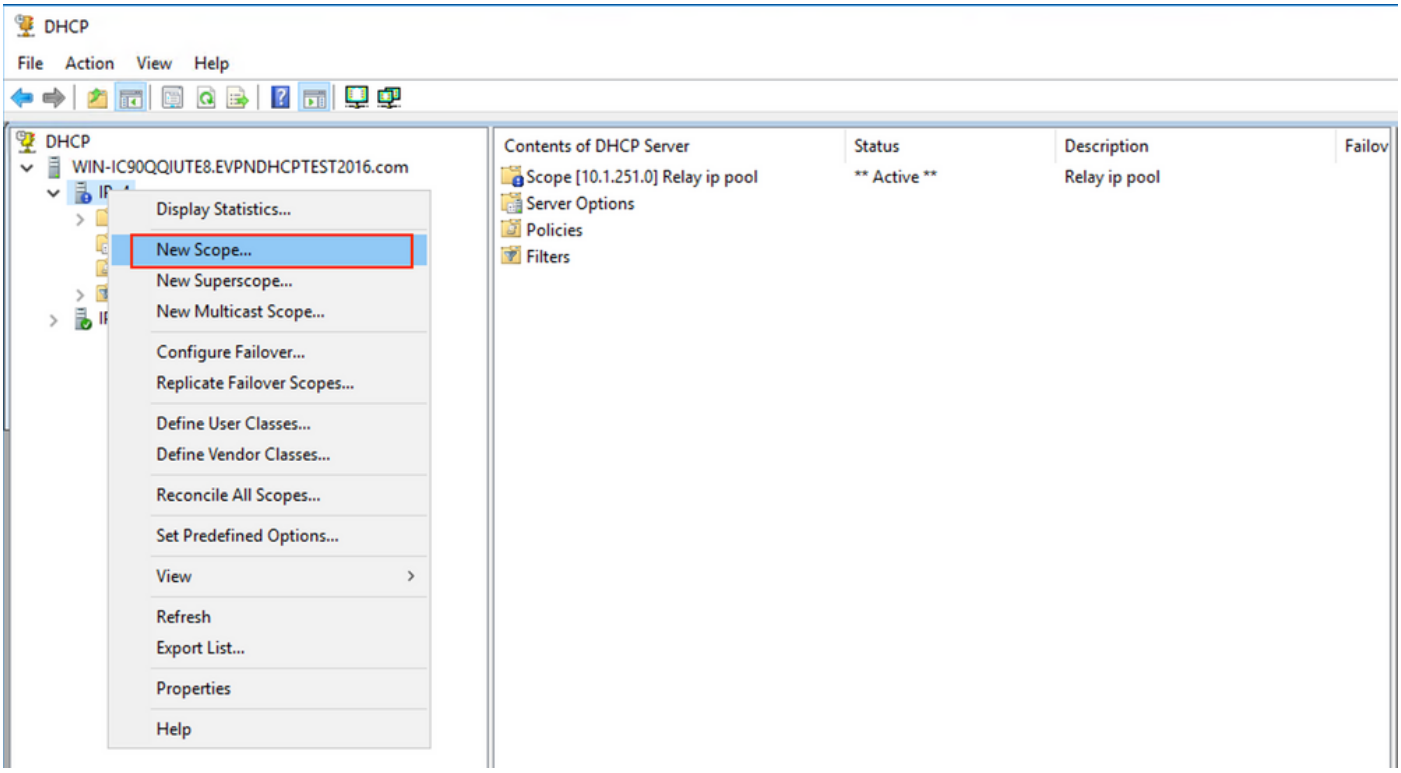


Wählen Sie **Fertig stellen** wie im Bild gezeigt.

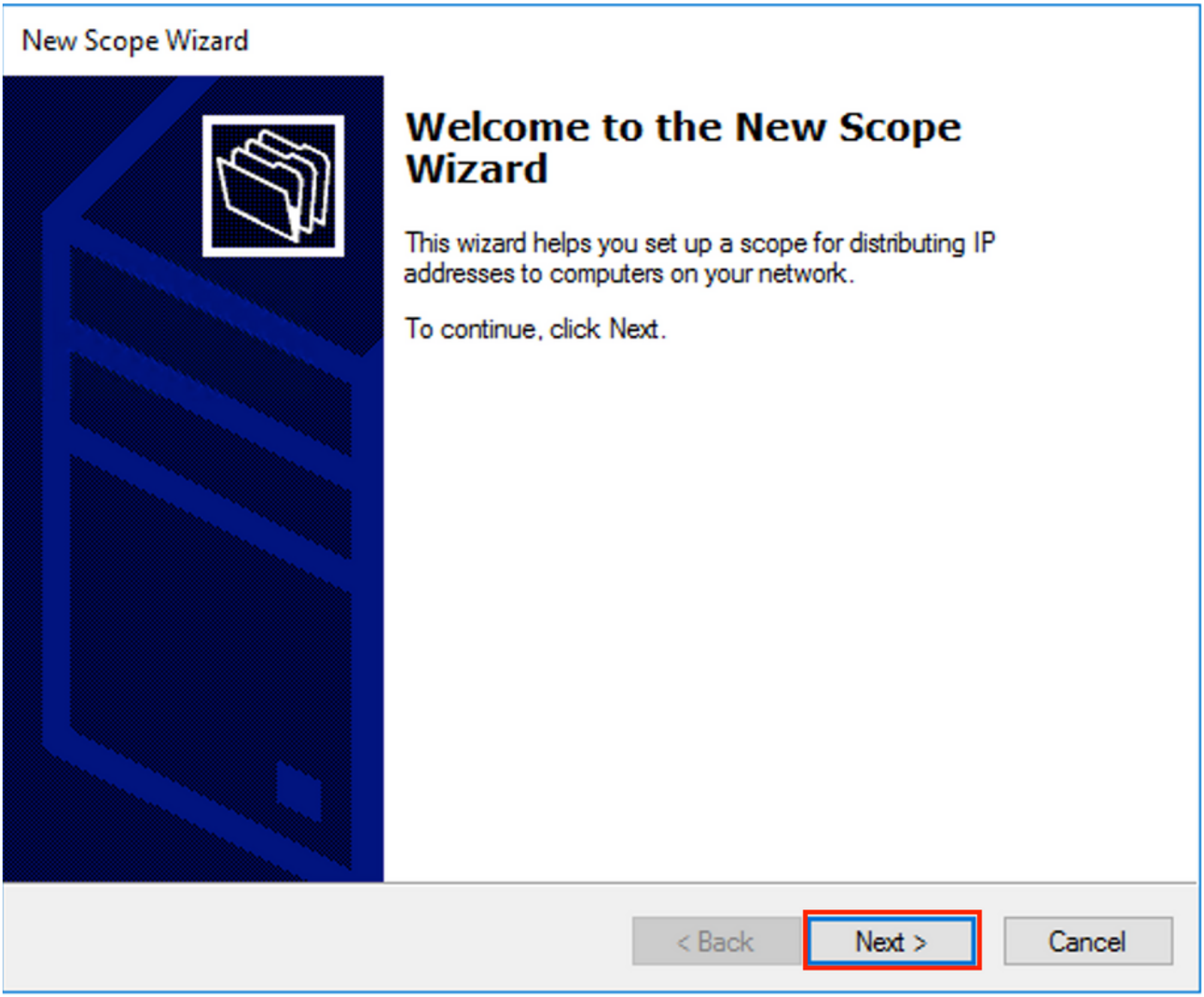


Der Spielraum für Relays ist jetzt bereit.

- Anschließend erstellen Sie den Pool, aus dem Clients IP-Adressen beziehen.
- Klicken Sie mit der rechten Maustaste, und wählen Sie **Neuer Bereich** aus, wie im Bild gezeigt.

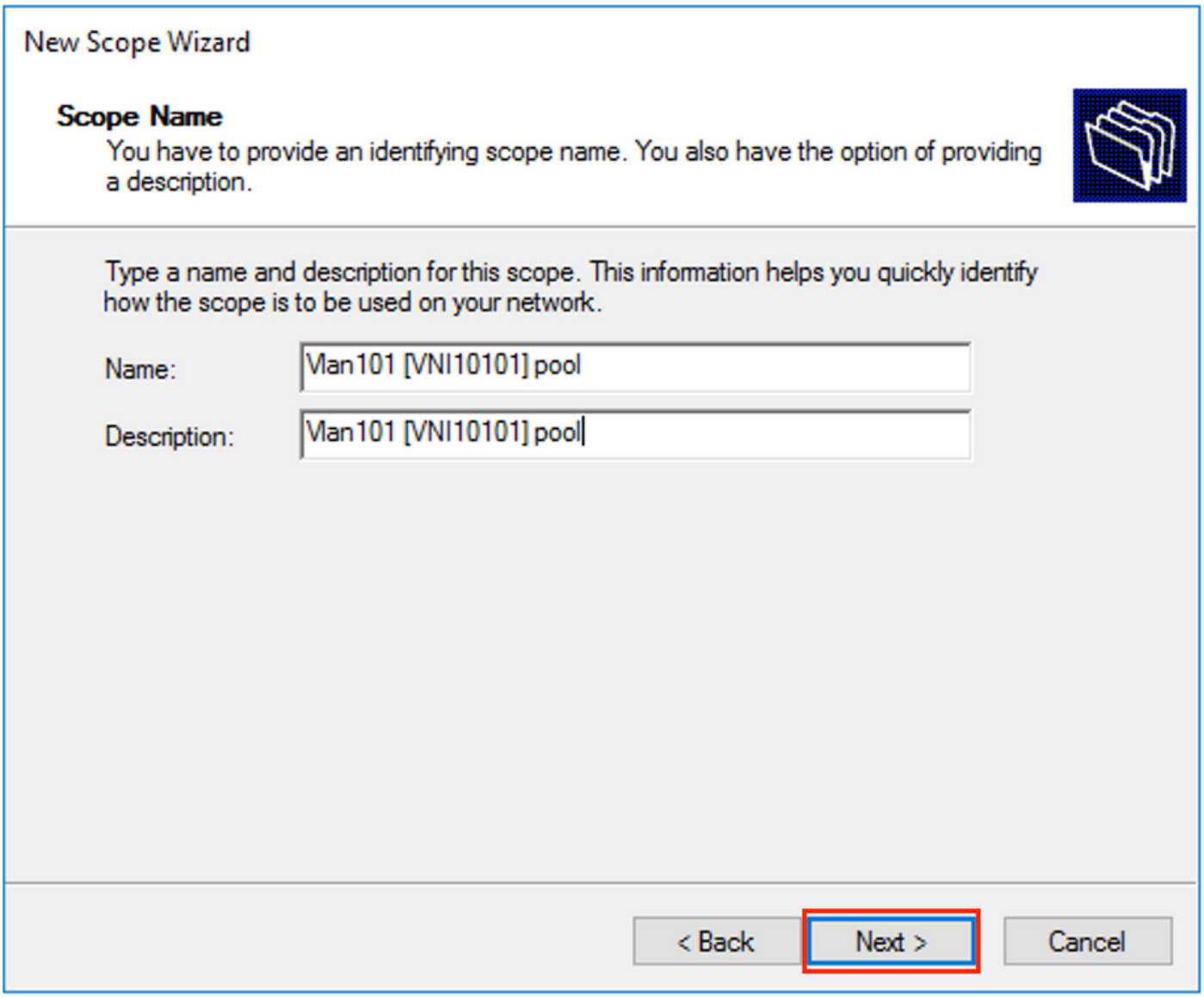


Wählen Sie wie im Bild gezeigt **Weiter** aus.

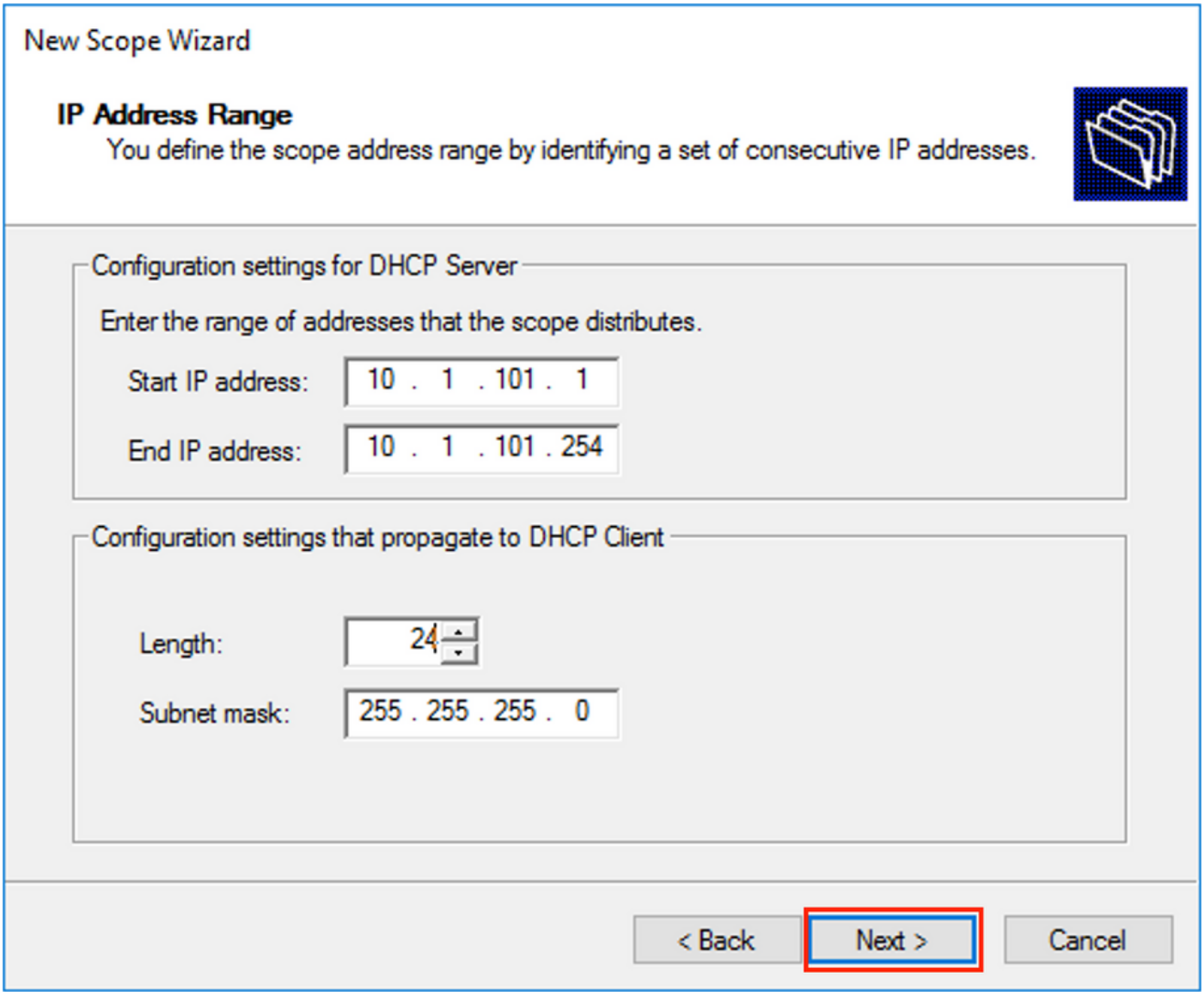


Wählen Sie einen aussagekräftigen Namen und eine Beschreibung für den Pool, wie im Bild

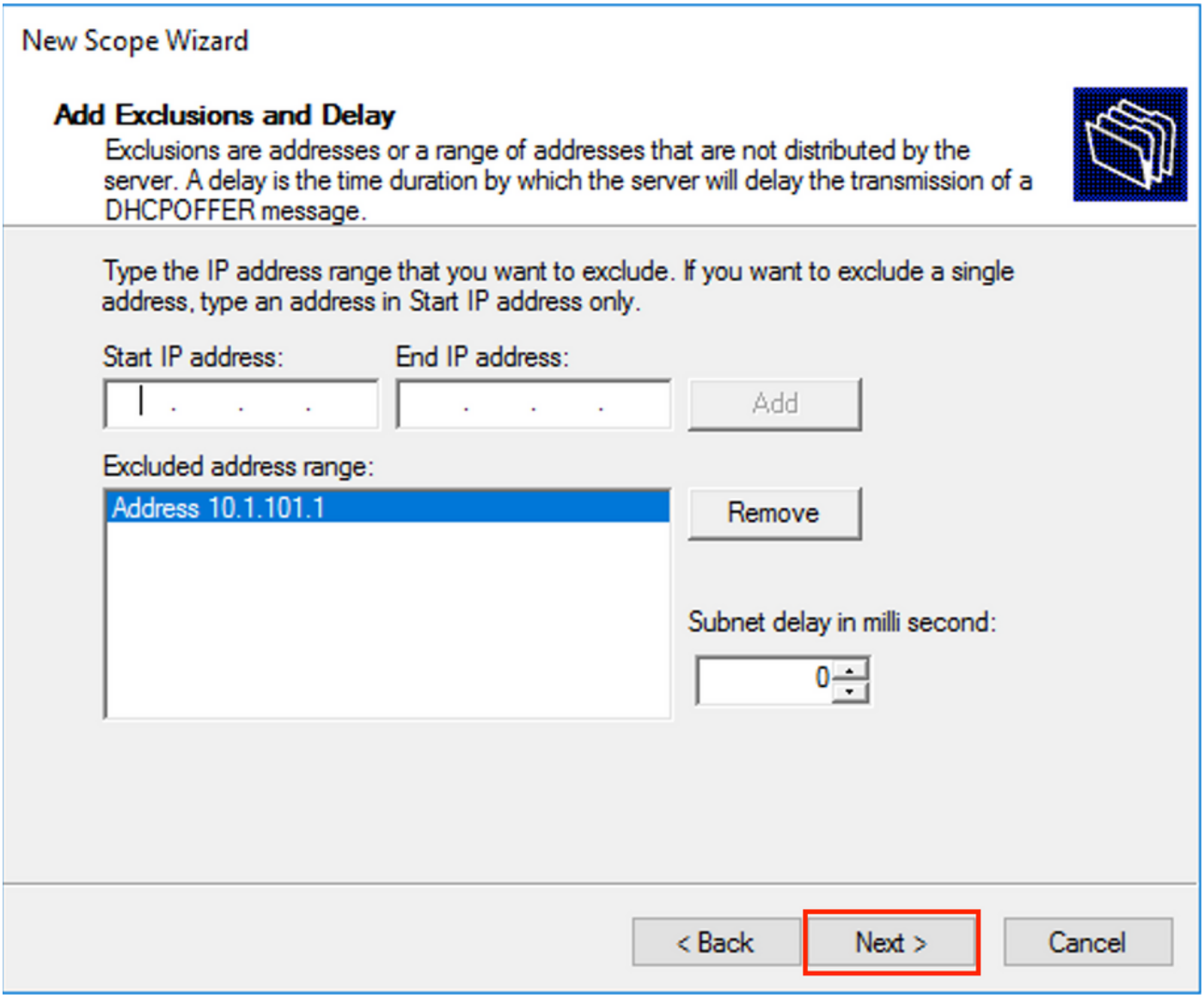
gezeigt.



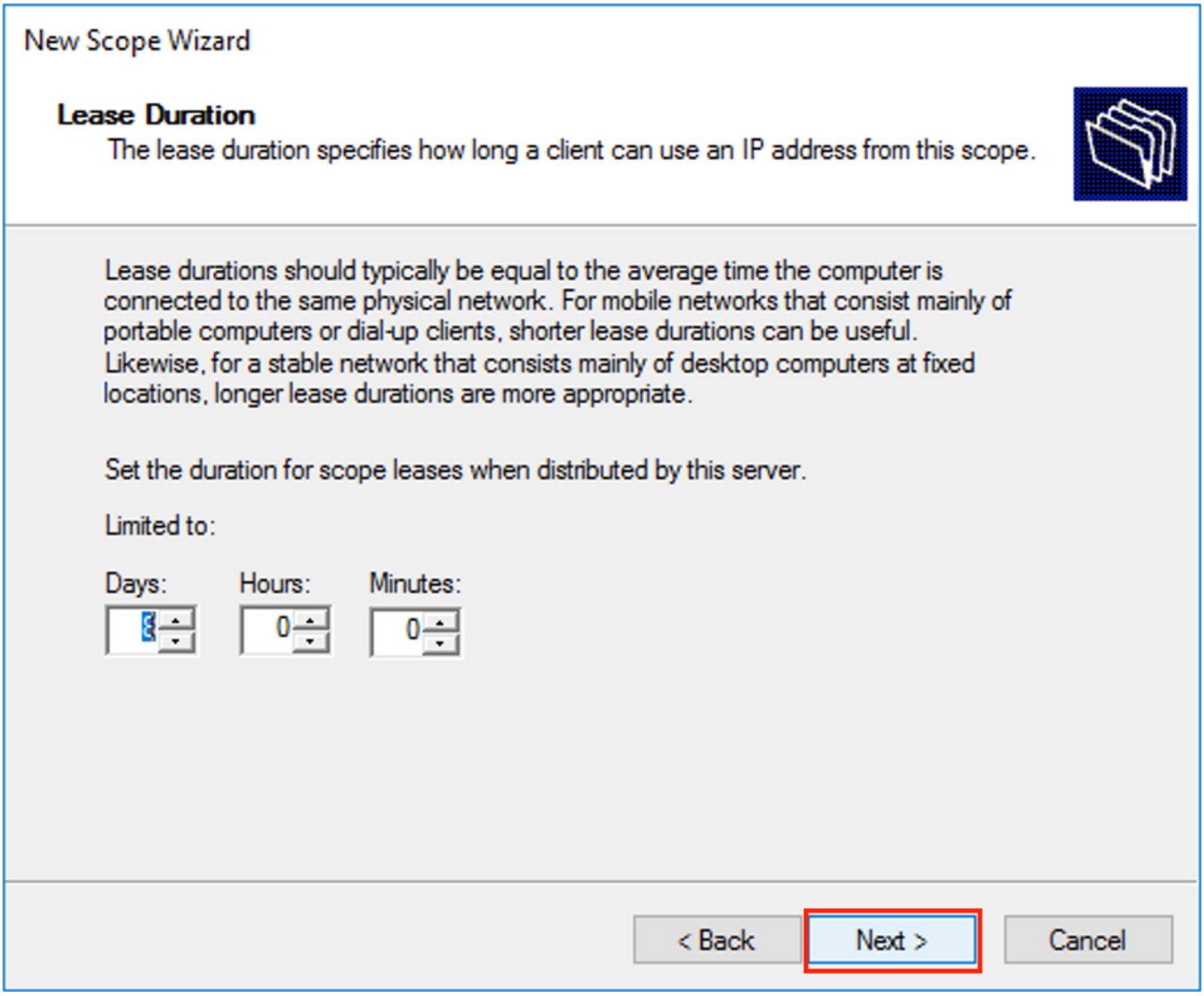
Geben Sie den IP-Adressbereich für die Zuweisung in vlan101 ein, wie im Bild gezeigt.



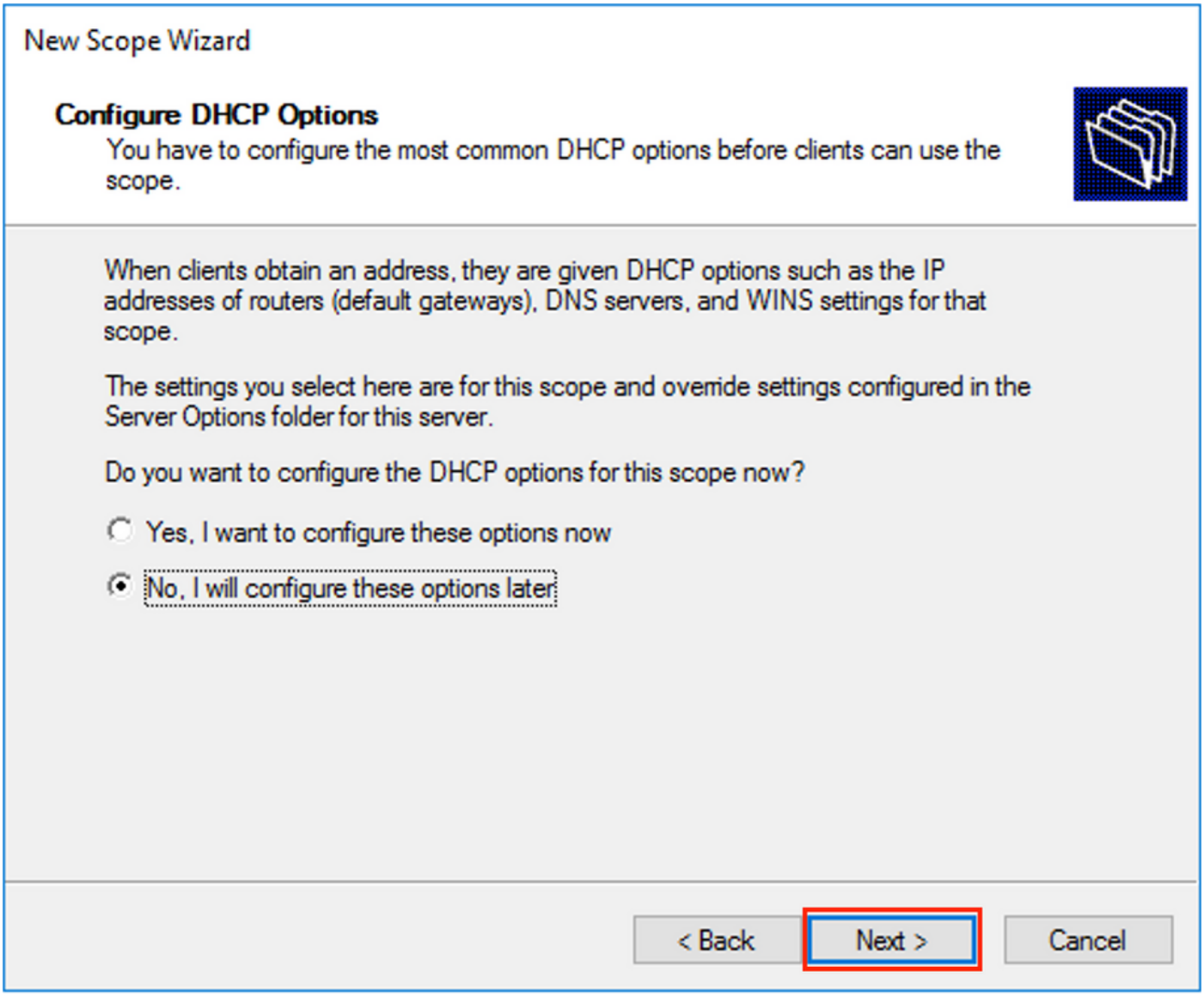
Schließen Sie die Standard-Gateway-IP aus dem Bereich aus, wie im Bild gezeigt.



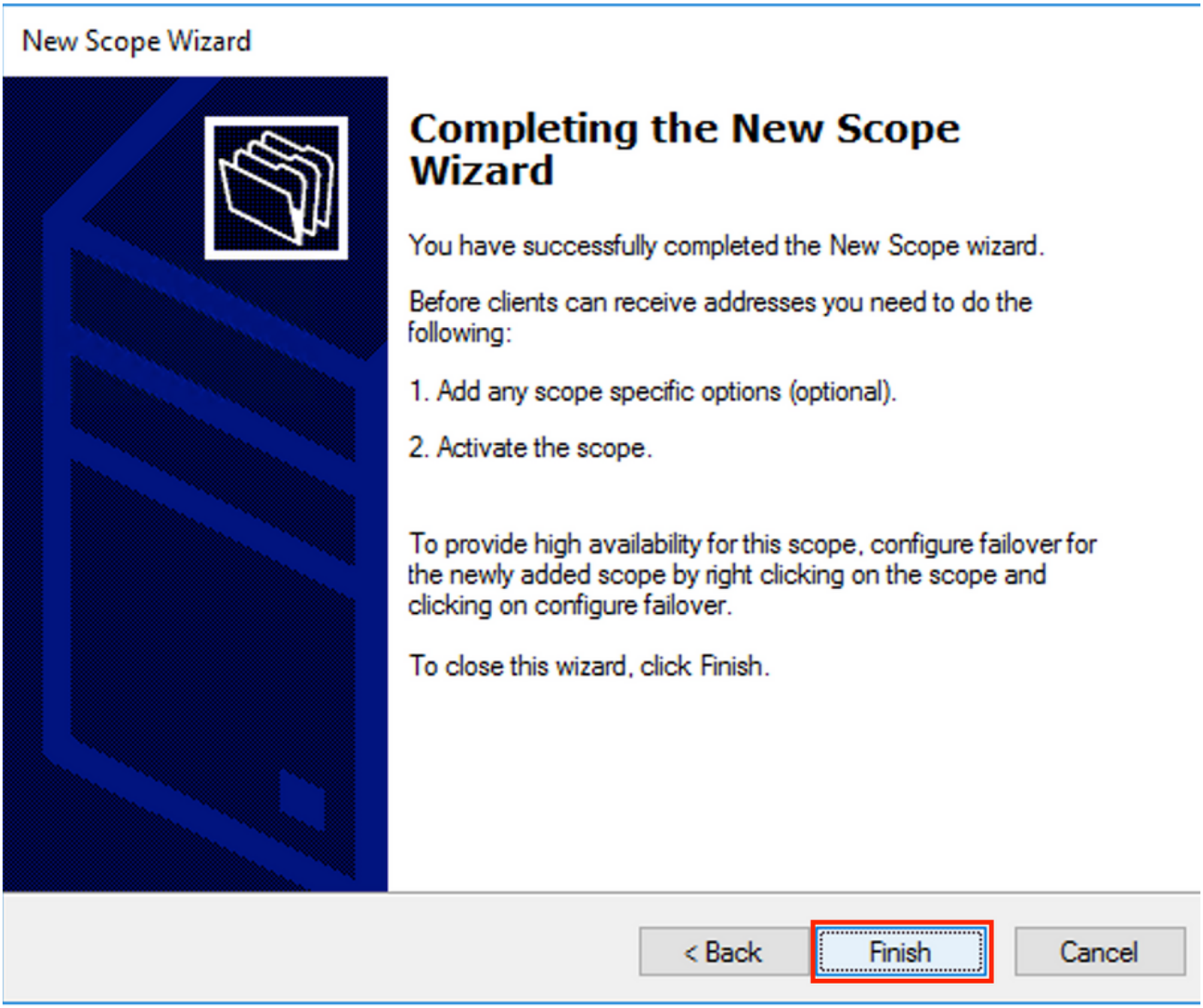
Legen Sie eine Leasingzeit fest, wie im Bild gezeigt.



Zusätzliche Parameter wie DNS/WINS und mehr können konfiguriert (in diesem Beispiel übersprungen) werden, wie im Bild gezeigt.

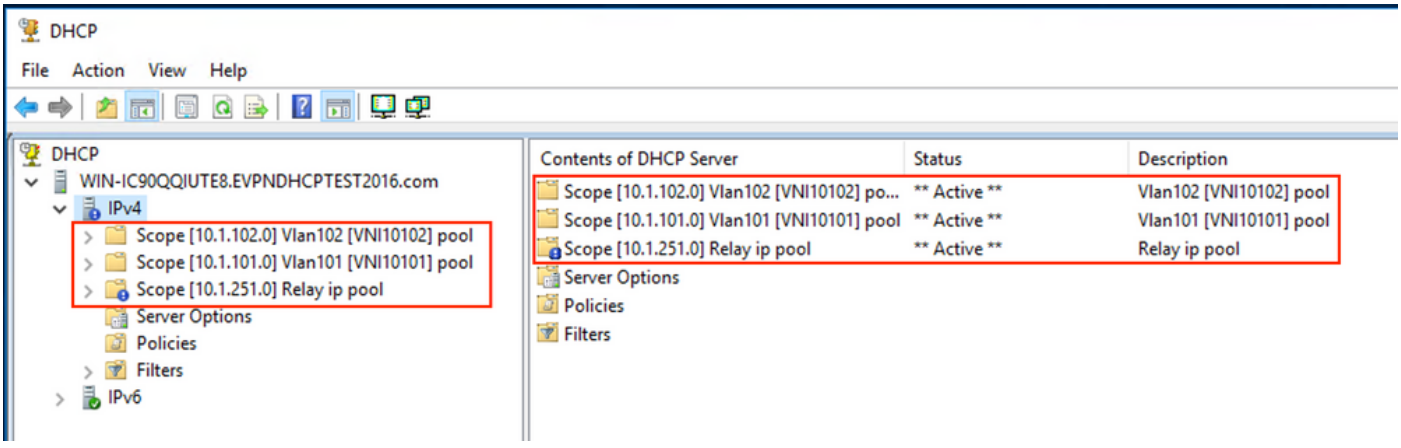


Wählen Sie **Fertig stellen**, um die Einrichtung wie im Bild gezeigt abzuschließen.



Der Pool pro Relay-IP-Adresse ist nicht konfiguriert und in HEX nicht zugeordnet. Die Pool-Auswahl basiert auf der **Auswahl** der Unteroption **Link**.

Ein neuer Pool kann hinzugefügt werden, und es ist keine zusätzliche Konfiguration erforderlich, wie im Bild gezeigt.



Linux-DHCP-Server

Überprüfen Sie die Konfiguration für den isc-dhcp-server unter Linux.

- Es unterstützt Relay Option 82. Hier ist die wichtigste Unteroption die Linkauswahl. Sie können weiterhin Agent Circuit-ID-Informationen und Hexadezimalmaske/Übereinstimmung für das jeweilige Feld (wie beim win2012) bearbeiten. Aus praktischer Sicht ist es viel einfacher, 82[5] zu verwenden, als direkt mit Agent Circuit-ID-Informationen zu arbeiten.
- Die Konfiguration der Unteroption für die Verbindungsauswahl erfolgt unter der Subnetzdefinition.

In diesem Beispiel wird der ISC-Server unter Ubuntu Linux verwendet.

Installieren Sie den DHCP-Server:

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

Um den DHCP-Server zu konfigurieren, bearbeiten Sie **/etc/dhcp/dhcpd.conf**. (In einem Beispiel wird der Vim-Editor verwendet.)

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

Konfigurationsausschnitt (allgemeine Konfigurationen werden weggelassen):

```
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;
}
```

Switch-Konfiguration

Szenarien, die allgemein unterstützt werden, werden hier vorgestellt.

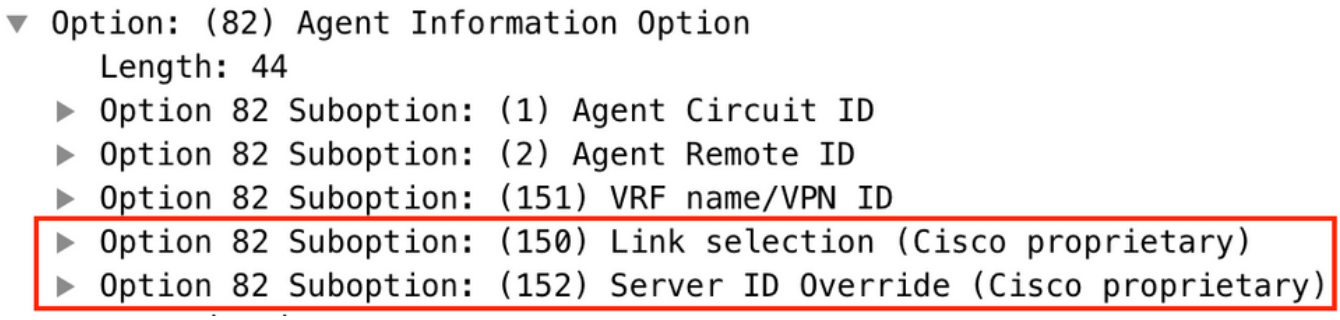
1. Der DHCP-Client befindet sich im Tenant-VRF, und der DHCP-Server befindet sich im Standard-VRF für Layer 3.
2. Der DHCP-Client befindet sich im Tenant-VRF, und der DHCP-Server befindet sich im gleichen Tenant-VRF
3. Der DHCP-Client befindet sich im Tenant-VRF, und der DHCP-Server befindet sich in einer anderen Tenant-VRF-Instanz.
4. Der DHCP-Client befindet sich im Tenant-VRF, und der DHCP-Server befindet sich in einer nicht standardmäßigen VXLAN-VRF-Instanz.

Für jedes dieser Szenarien ist eine DHCP-Relay-Konfiguration auf Switch-Seite erforderlich.

Die DHCP-Konfiguration für die einfachste Option Nr. 2.

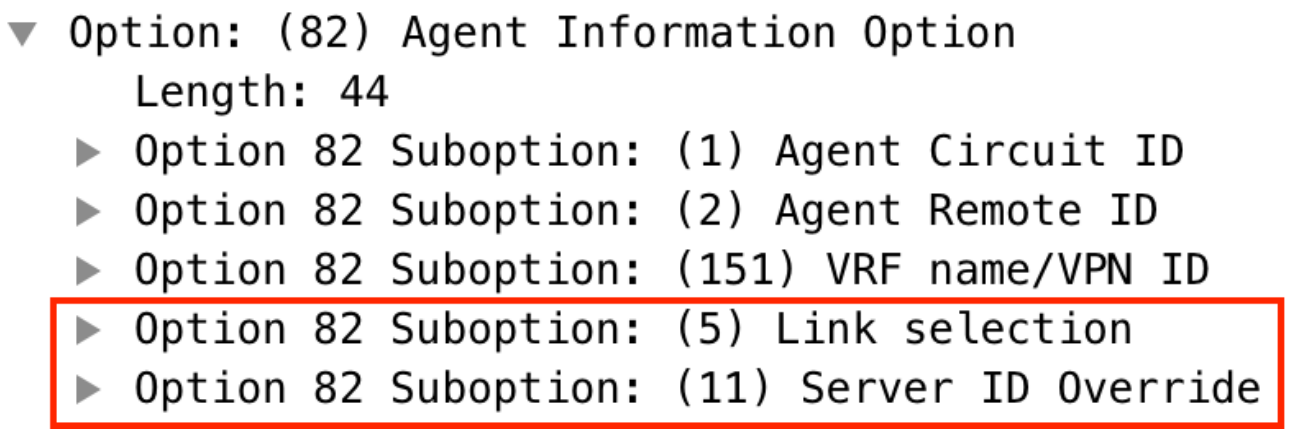
```
ip dhcp relay information option      <<< Enables insertion of option 82 into the packet
ip dhcp relay information option vpn <<< Enables insertion of vpn name/id to the packet - option 82[151]
```

Standardmäßig sind Option 82 Suboptionen **Link Selection** und **Server ID Override** standardmäßig von Cisco proprietär (150 bzw. 152).



Wenn der DHCP-Server proprietäre Optionen von Cisco aus irgendeinem Grund nicht **versteht**, können Sie diese auf die Standardoptionen ändern.

```
ip dhcp compatibility suboption link-selection standard <<< "Link Selection" suboption
ip dhcp compatibility suboption server-override standard <<< "Server ID Override" suboption
```



DHCP-Snooping muss für erforderliche VLANs aktiviert werden.

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

Sie können die globale Konfiguration der DHCP-Relay-Quellschnittstelle verwenden.

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

Sie können es auch pro Schnittstelle konfigurieren (die Schnittstellenkonfiguration setzt die globale außer Kraft).

```
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
```

Überprüfen Sie, ob in beide Richtungen die IP-Konnektivitäts-B/W-Relay-IP-Adresse und der DHCP-Server vorhanden sind.

```
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
```

Unter Schnittstellenkonfiguration wird die Adresse des DHCP-Servers konfiguriert. Dieser Befehl kann aus drei Optionen bestehen. Der Client und der Server befinden sich im gleichen VRF:

```
interface Vlan101
vrf forwarding green
ip dhcp relay source-interface Loopback101
ip address 10.1.101.1 255.255.255.0
  ip helper-address 192.168.20.20         <<< DHCP server ip address
```

Der Client und der Server befinden sich in den verschiedenen VRFs (in diesem Beispiel Client in grün, Server in rot):

```
interface Vlan101
vrf forwarding green
ip dhcp relay source-interface Loopback101
ip address 10.1.101.1 255.255.255.0
ip helper-address vrf red 192.168.20.20   <<< DHCP server is reachable over vrf RED
end
```

Client in einer VRF-Instanz und Server in der globalen Routing-Tabelle (GRT):

```
interface Vlan101
vrf forwarding green
ip dhcp relay source-interface Loopback101
ip address 10.1.101.1 255.255.255.0
ip helper-address global 192.168.20.20  <<< DHCP server is reachable over global routing table
end
```

Eine typische Konfiguration für alle Optionen wird hier überprüft.

Der DHCP-Client befindet sich im Tenant-VRF, und der DHCP-Server befindet sich im Layer-3-

Standard-VRF

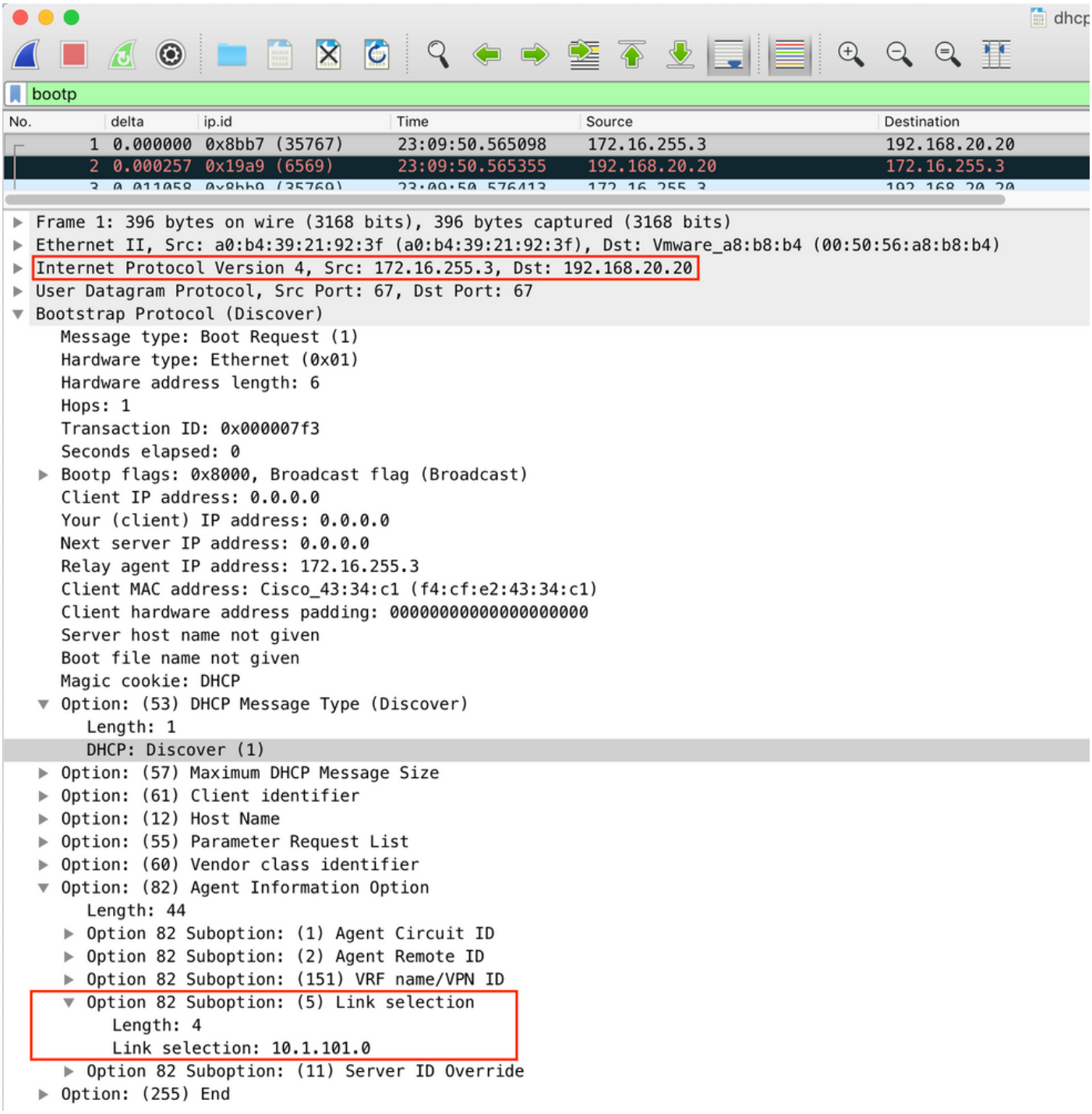
In diesem Fall ist Lo0 in GRT eine Relaisquelle. DHCP-Relay wird global + für einige Schnittstellen konfiguriert.

Für den Befehl vlan101 "IP DHCP Relay Source-Interface Loopback0" wird beispielsweise der Befehl "IP DHCP Relay Source-Interface Loopback0" verpasst, es wird jedoch die globale Konfiguration verwendet.

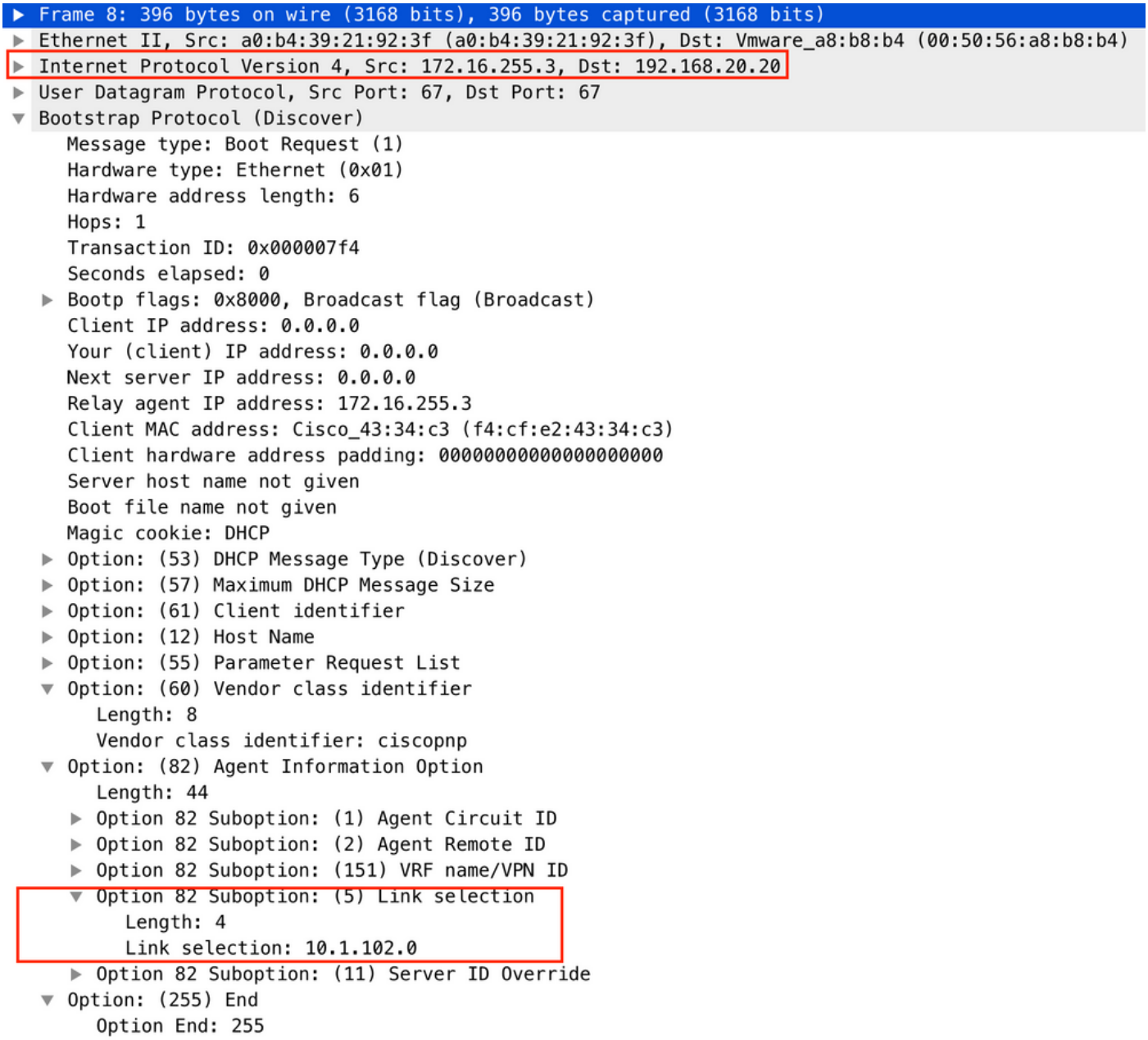
```
ip dhcp-relay source-interface Loopback0                 <<< DHCP relay source interface is Lo0
ip dhcp relay information option vpn                     <<< adds the vpn suboption to option 82
ip dhcp relay information option                         <<< enables DHCP option 82
ip dhcp compatibility 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
```

Das Ergebnis ist, dass das DHCP-Relay-Paket über GRT mit derselben SRC IP/DST IP, aber mit unterschiedlichen Unteroptionen gesendet wird.

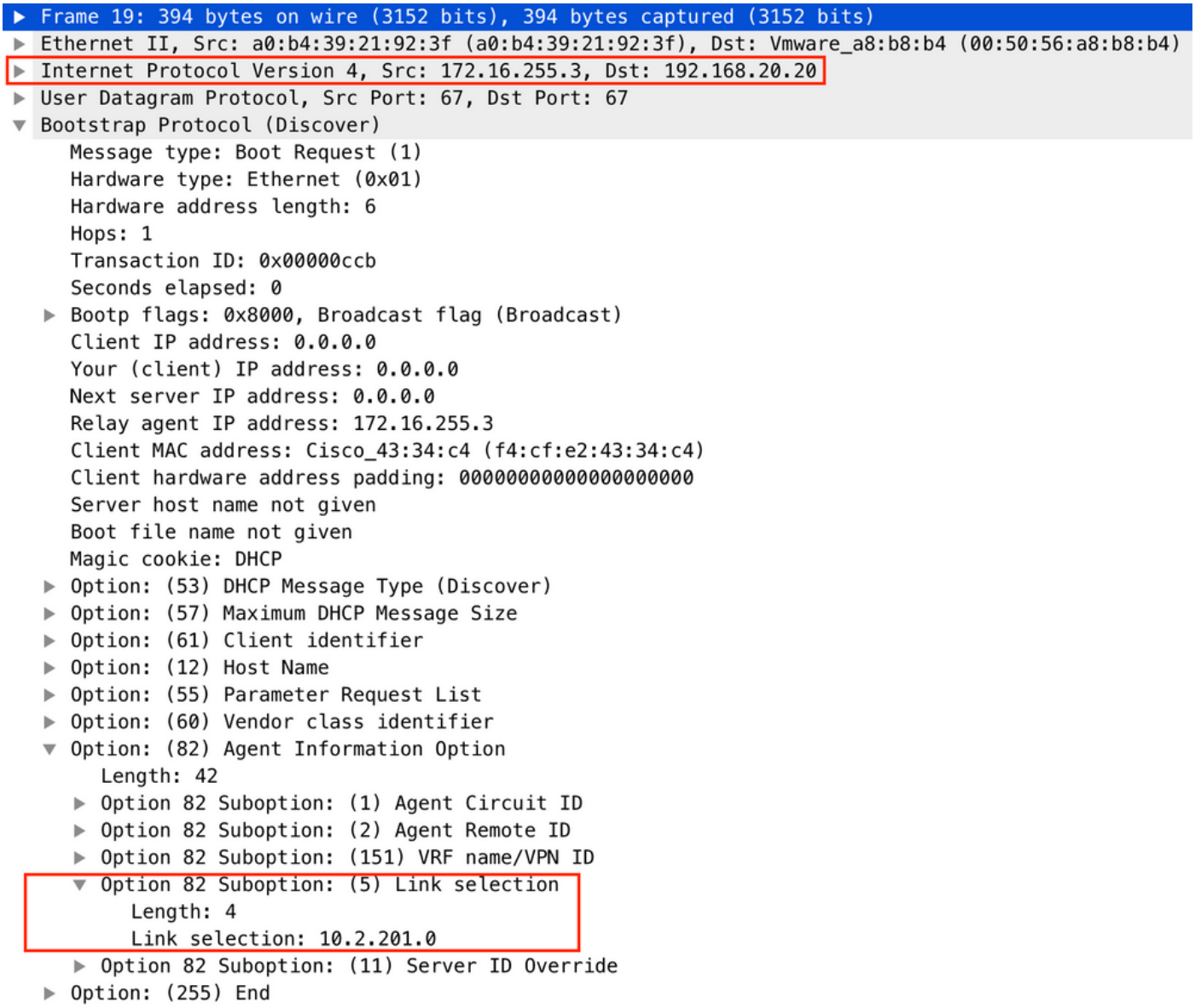
Für VLAN101:


dhcp
bootp
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
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

- Für VLAN102:



Für VLAN201 (VRF rot, nicht grün wie VLANs 101 und 102):



Die Paketerfassung wurde für Spine-01 von der Schnittstelle zum Leaf-01 übernommen:

```
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
```

Das DHCP-Paket im Core ist IP ohne VXLAN-Kapselung:

```
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...>
```

Ein großer Vorteil dieses Ansatzes besteht darin, dass Sie dieselbe Relay-IP-Adresse für verschiedene Tenant-VRFs verwenden können, ohne dass zwischen verschiedenen VRFs und global Route Leaking durchgeführt wird.

DHCP-Client und DHCP-Server befinden sich im selben Tenant-VRF

In diesem Fall ist es sinnvoll, die Relay-IP-Adresse im Tenant-VRF zu haben.

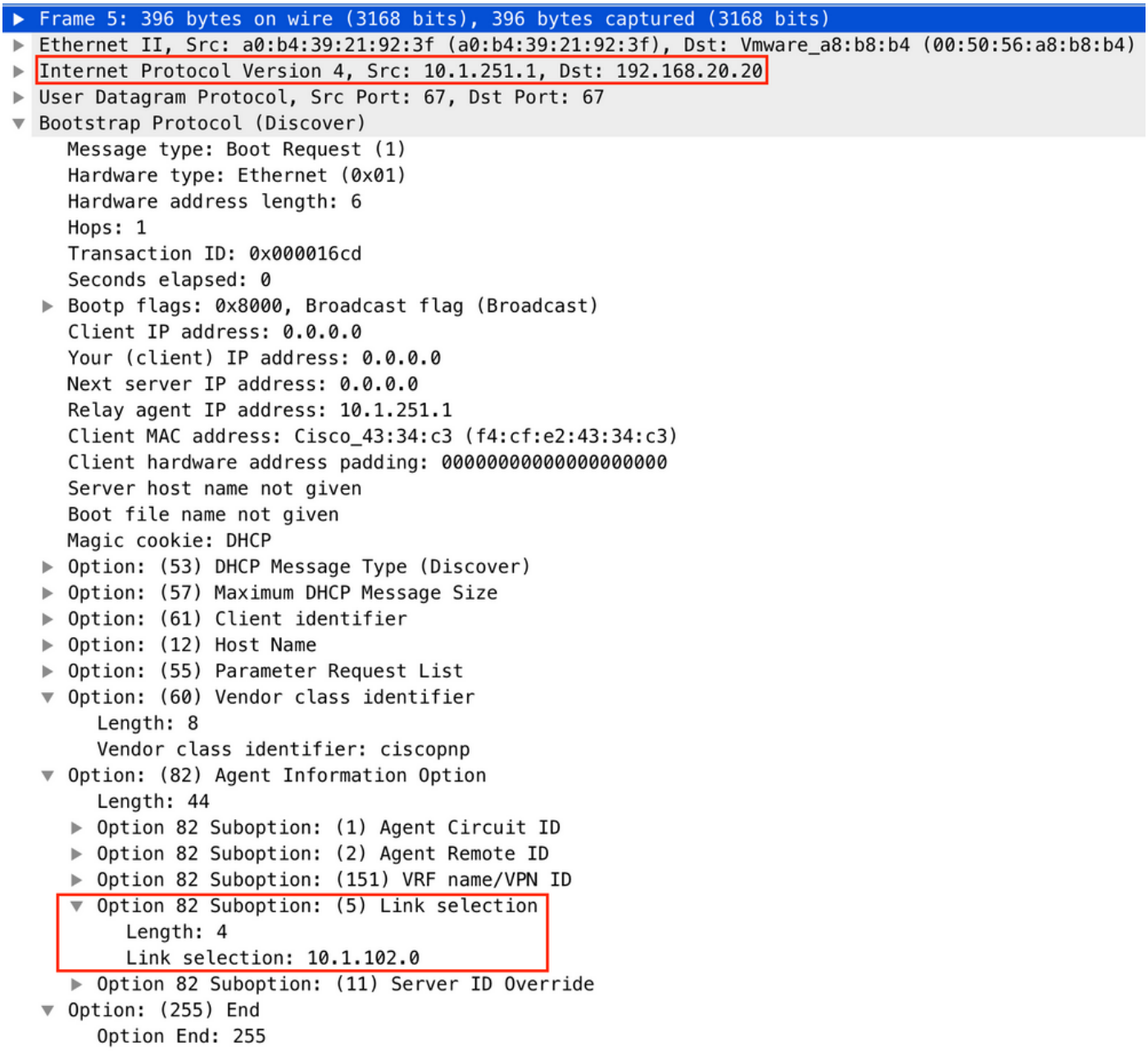
Switch-Konfiguration:

```
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
```

Für 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
```

Für VLAN102:



Paketerfassung der Schnittstelle Spine-01 bis Leaf-01:

```
Spine-01#sh monitor capture TAC buffer brief | i DHCP
2 4.287466 10.1.251.1 b^F^R 192.168.20.20 DHCP 446 DHCP Discover - Transaction ID 0x1894
3 4.288258 192.168.20.20 b^F^R 10.1.251.1 DHCP 412 DHCP Offer - Transaction ID 0x1894
4 4.307550 10.1.251.1 b^F^R 192.168.20.20 DHCP 464 DHCP Request - Transaction ID 0x1894
5 4.308385 192.168.20.20 b^F^R 10.1.251.1 DHCP 412 DHCP ACK - Transaction ID 0x1894
```

Das DHCP-Paket im Core verfügt über VXLAN-Kapselung:

```
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...>
```

DHCP-Client in einem Tenant-VRF und DHCP-Server in einem anderen Tenant-VRF

In diesem Beispiel ist der Client in VRF rot und der Server in VRF grün.

Sie haben zwei Optionen:

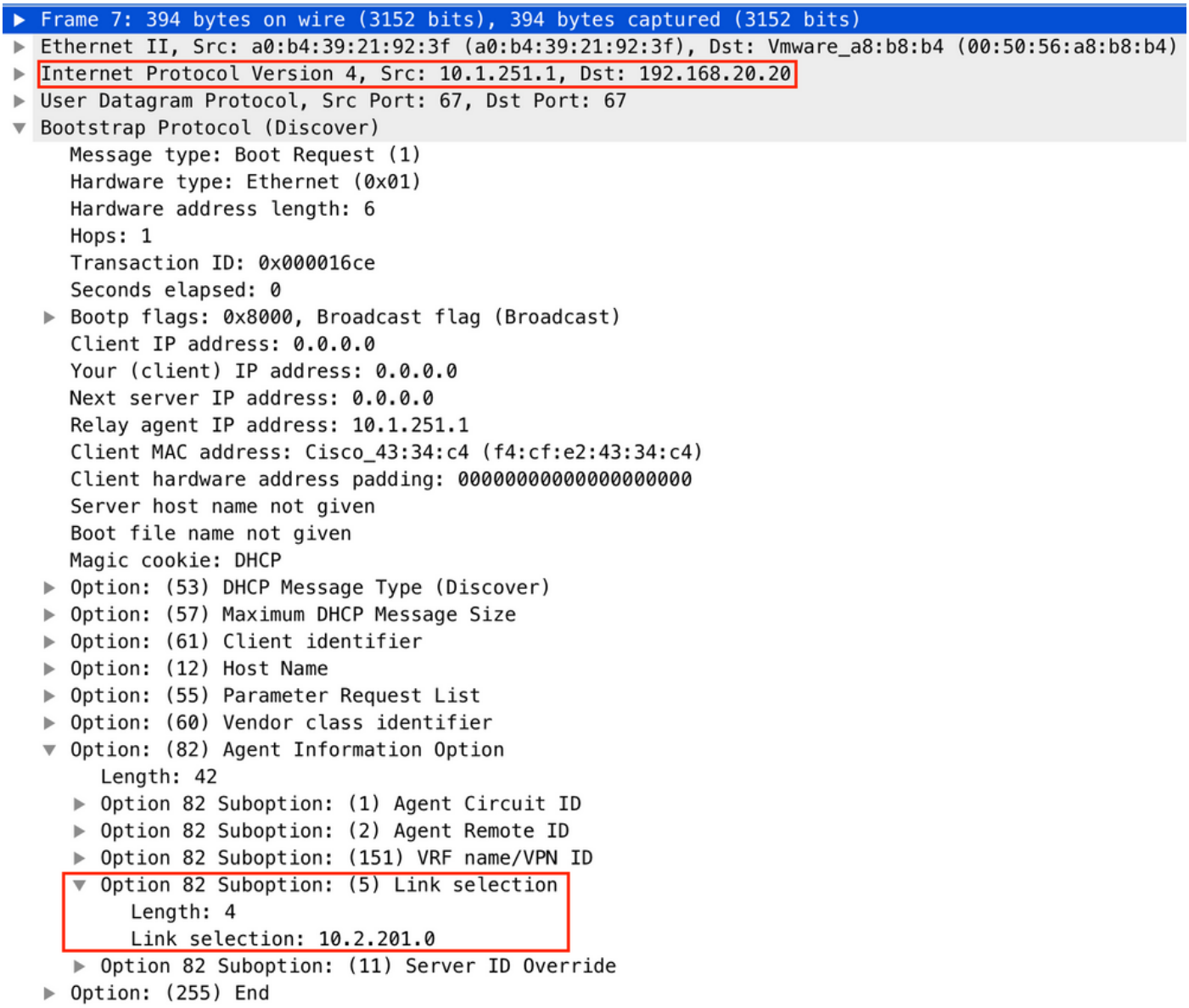
- Bewahren Sie Relay-IP in Client-VRF auf, und konfigurieren Sie Route Leaking, was die Komplexität erhöht.
- Keep Relay IP im Server-VRF (ähnlich wie bei GRT im ersten Fall)

Der zweite Ansatz ist einfacher auszuwählen, da viele Client-VRFs unterstützt werden und kein Route-Leaking erforderlich ist.

Switch-Konfiguration:

```
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
```

Für VLAN201:



Paketerfassung an Spine-01-to-Leaf-01-Schnittstelle:

```
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
```

In diesem Beispiel ist das Paket im Core VXLAN gekapselt.

```
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...>
```

DHCP-Client in einem Tenant-VRF und DHCP-Server in einem anderen Nicht-VXLAN-VRF

Dieser Fall ähnelt dem letzten. Der Hauptunterschied besteht darin, dass Pakete keine VXLAN-Kapselung aufweisen - reine IP-Adresse oder etwas Anderes (MPLS/GRE/etc.), aber aus Konfigurationsperspektive identisch ist.

In diesem Beispiel ist der Client in VRF rot und der Server in VRF grün.

Sie haben zwei Optionen:

- Relay-IP befindet sich im Client-VRF und konfiguriert Route Leaking, was die Komplexität erhöht.
- Relay-IP befindet sich im Server-VRF (ähnlich wie bei GRT im ersten Fall).

Der zweite Ansatz ist einfacher auszuwählen, da viele Client-VRFs unterstützt werden und kein Route Leaking erforderlich ist.

Switch-Konfiguration:

```
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
```

Zugehörige Informationen

- RFC 3046
- RFC 3527

- https://docs.microsoft.com
- Technischer Support und Dokumentation für Cisco Systeme