شكلت DHCP في IOS XE EVPN/VXLAN

المحتويات

المقدمة

يصف هذا المستند تكوين بروتوكول التكوين الديناميكي للمضيف (DHCP) لشبكة Ethernet VPN (EVPN) شبكة LAN الموسعة الظاهرية (VXLAN) في سيناريوهات مختلفة، وجوانب محددة لخوادم Win2012 و Win2016 DHCP.

المتطلبات الأساسية

المتطلبات

cisco يوصي أن يتلقى أنت معرفة من EVPN/VXLAN و DHCP.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

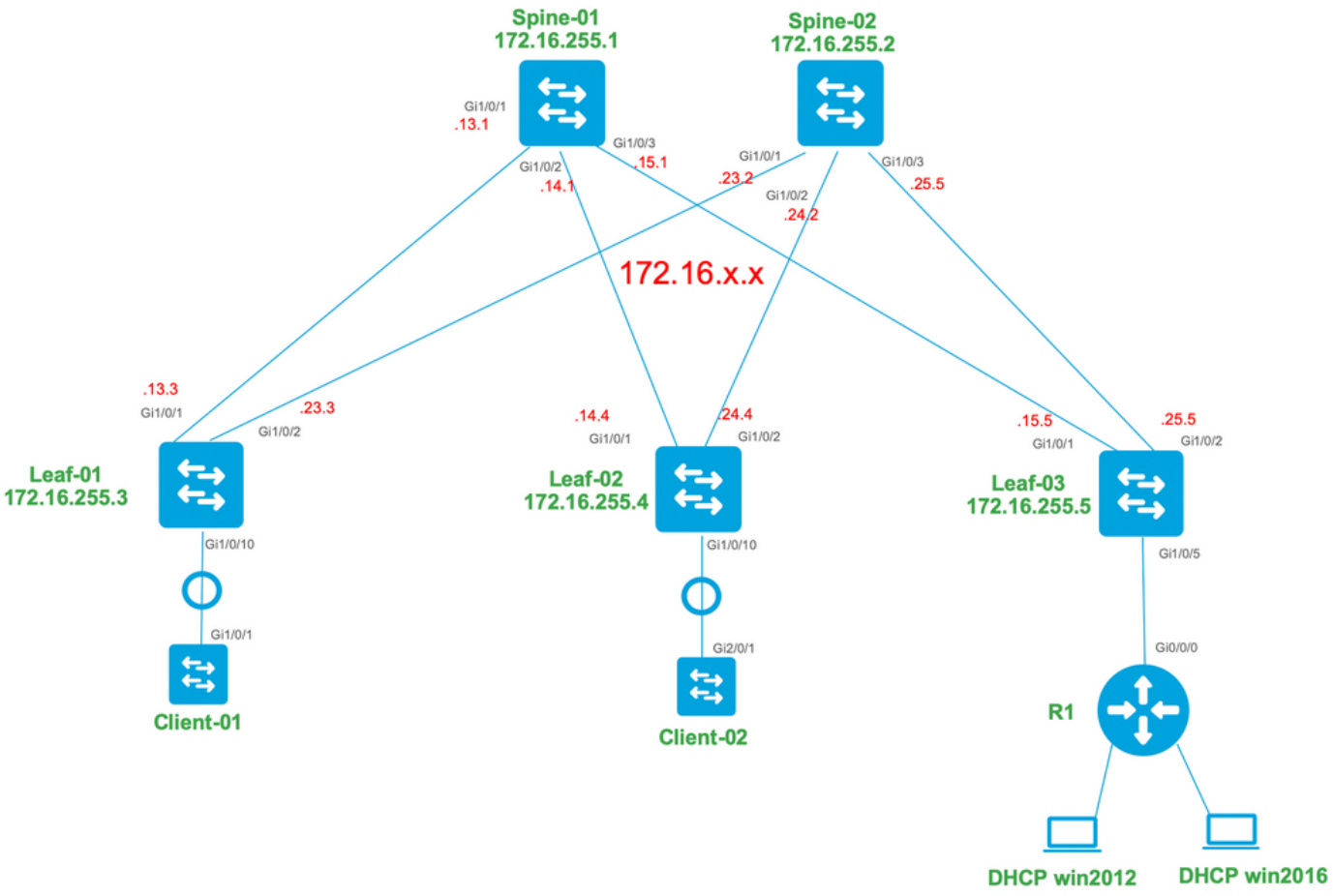
- C9300
- C9400
- C9500
- C9600
- نظام التشغيل Windows Server 2012 R2 من MSFT
- نظام التشغيل MSFT Windows Server 2016

- الميزات المتوفرة على Cisco IOS XE 16.9.x أو إصدار أحدث

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك قيد التشغيل، فتأكد من فهمك للتأثير المحتمل لأي أمر.

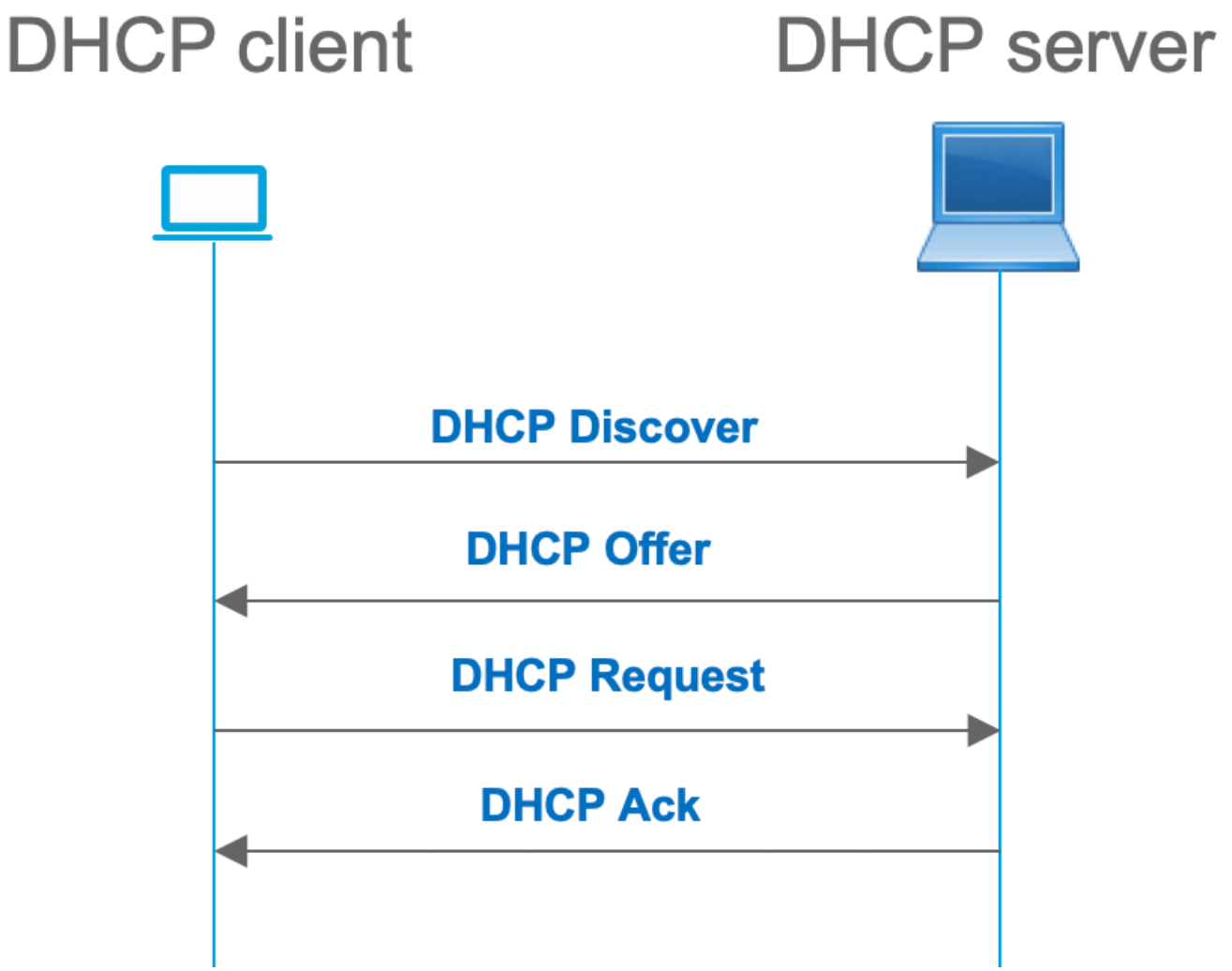
التكوين

الرسم التخطيطي للشبكة



التكوينات

الآن، دعنا نراجع تدفق الرسالة بين عميل DHCP والخادم. هناك أربع مراحل:

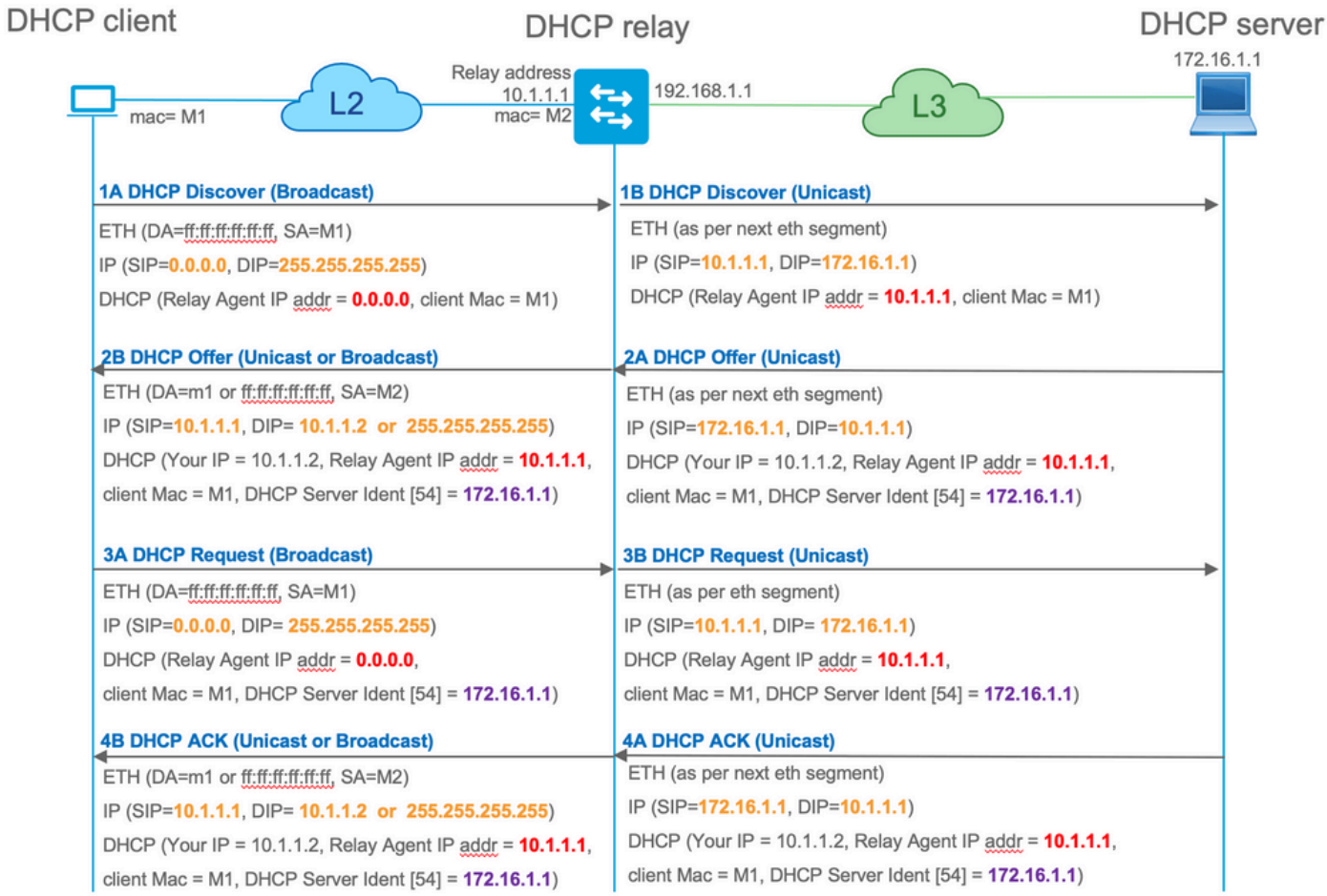


وهذا يعمل في الحالات التي يكون فيها العميل والخادم في الشبكة الفرعية نفسها، ومع ذلك، عادة، ال يكون هذا هو الحال. في معظم الحالات، ال يكون خادم DHCP في الشبكة الفرعية نفسها مع العميل ويجب أن يكون قابال للوصول إليه عبر مسار موجه من الطبقة 3 مقابل الطبقة 2. في هذه الحالة، يلزم توفر وظيفة ترحيل DHCP. تحول ميزة ترحيل DHCP (المحول أو الموجه) البث إلى البث الأحادي المغلف ل UDP والذي يكون قابال للتوجيه وإرساله إلى خادم DHCP. وهو تكوين مستخدم بشكل واسع في الشبكات هذه الأيام.

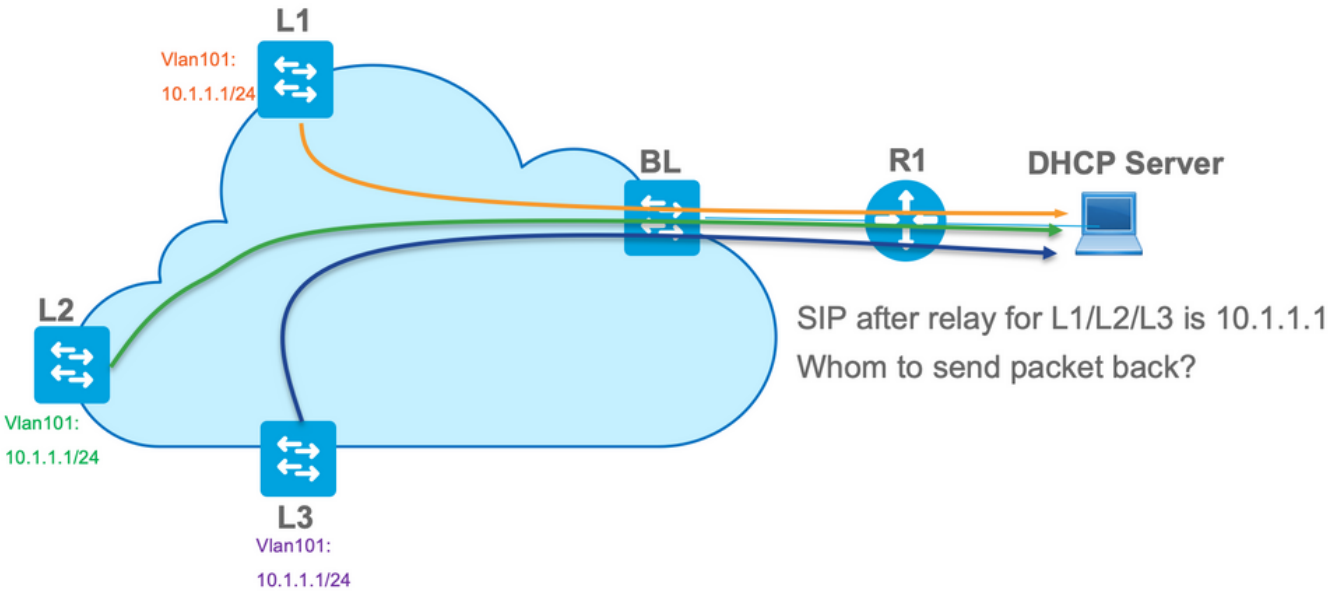
تحديات مع بنية DHCP و EVPN/VXLAN:

عادة، يتم توصيل خادم DHCP بنسيج EVPN عبر شبكة L3. هذا يعني أنه يجب عليك إستخدام وظيفة ترحيل DHCP لتحويل حزمة بث DHCP للطبقة 2 إلى حزمة توجيه أحادية البث للطبقة 3.

باستخدام ميزة ترحيل DHCP، يعمل تدفق مكالمات DHCP بين العميل والترحيل والخادم بشكل مماثل ل:



بعد إعادة التوجيه، يكون IP المصدر للحزمة هو IP للترحيل. مهما، يخلق هذا مشكلة في VXLAN/EVPN نشر بما أن المصدر المعتاد IP ليس فريد بسبب الإستعمالموزع AnyCast GW (DAG). لأن جميع بروتوكولات VTEP SVI المصدر هي نفسها، فإن ذلك يمكن أن يتسبب في إعادة توجيه حزم الرد من خادم DHCP إلى أقرب بوقة.



لحل مشكلة المصدر غير الفريدة، يجب أن تكون قادرا على إستخدام عنوان IP فريد لحزم DHCP المنقولة لكل بوقة. وثمة مسألة أخرى تتعلق باستبدال GIADDR. على خادم DHCP، يجب عليك إختيار التجمع الصحيح لتعيين عنوان IP. يتم ذلك من التجمع، والذي يغطي عنوان IP للعبارة (giaddr). ل EVPN بناء، وه ينبغي أن يكون عنوان IP من SVI، غير أن بعد

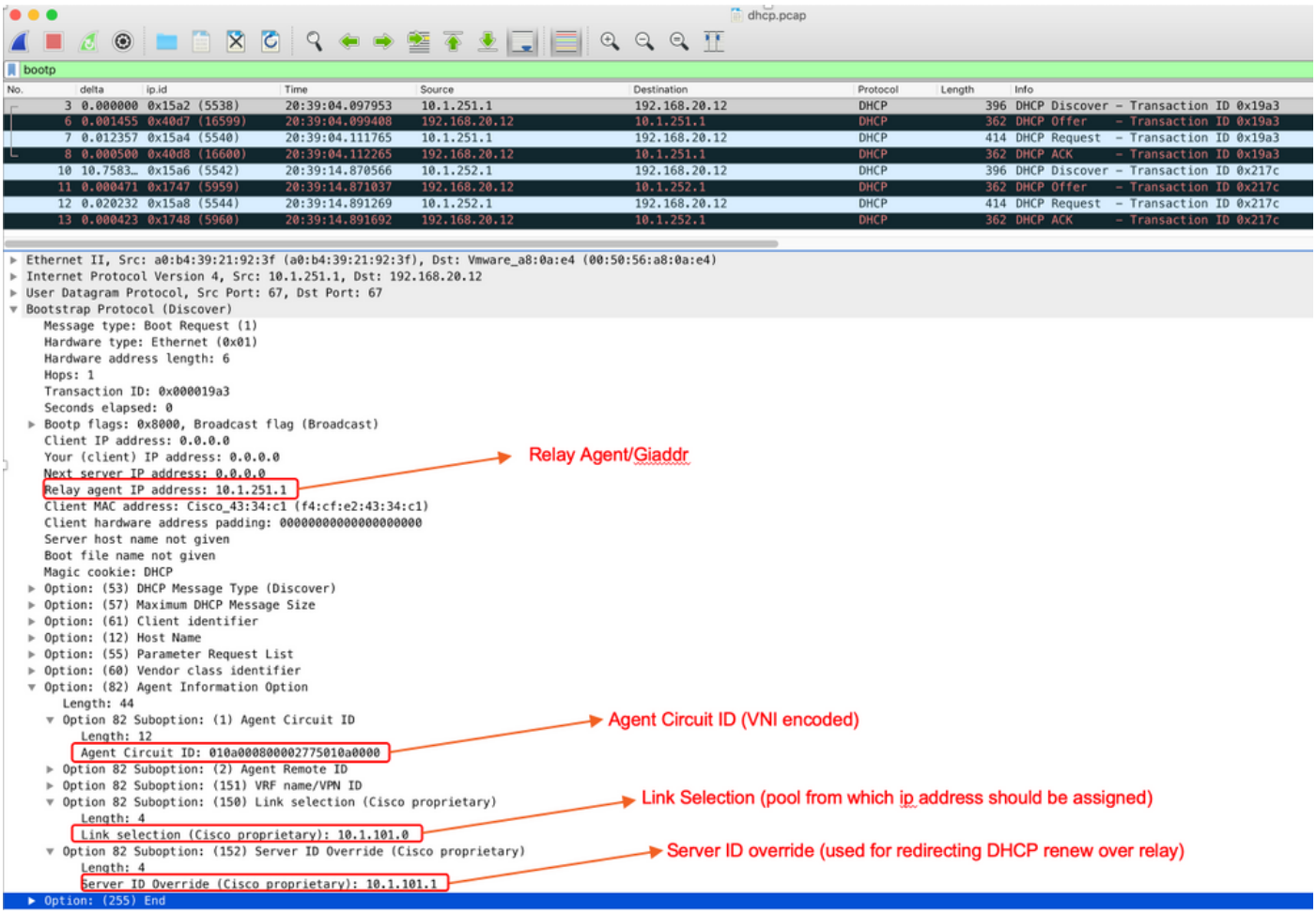
الترحيل، استبدلت الـ giaddr بـ ترحيل عنوان أي يكون في هذه الحالة إسترجاع فريد.

كيف يمكنك إعلام خادم DHCP، بالمجموعات التي يجب إستخدامها؟

in order to حللت هذا إصدار، استعملت خيار 82. وبشكل أساسي، هذه هي الخيارات الفرعية المهمة:

- 1 - **معرف دائرة الوكيل**. في حالة شبكة VXLAN/EVPN، يقوم هذا الخيار الفرعي بنقل معرف VNI
- 5 - (أو 150 لشركة Cisco الخاصة). الخيارات الفرعية **تحديد** الارتباط التي تحتوي على شبكة فرعية فعلية، والتي انطلقت منها حزمة DHCP
- 11 - (أو 152 لشركة Cisco الخاصة). الخيار الفرعي **تجاوز معرف الخادم** الذي يحتوي على عنوان خادم DHCP
- 151 - **اسم VRF/معرف VPN**. يحتوي هذا الخيار الفرعي على اسم VRF/معرف VPN

في حزمة التقاط من الربط من ترحيل DHCP إلى خادم DHCP، يمكنك رؤية هذه الخيارات المختلفة الموجودة في حزمة DHCP كما هو موضح في الصورة.



تكوين المحول:

- يحتوي الخيار 82 على كل المعلومات الضرورية الضرورية لاختيار تجمع DHCP الصحيح وإرجاع الحزمة من الخادم إلى الصفحة الصحيحة.
- يعمل هذا فقط إذا كان خادم DHCP يستطيع معالجة معلومات الخيار 82، رغم عدم دعم كل الخوادم له بالكامل (مثل 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
```

تكوين الخادم

الخيار Win2012 R2 Configuration 1 - IP توزيع ديناميكي لكل VNI/SVI لكل VTEP

المشكلة الرئيسية مع WIN2012 هي أن الخيار 82 غير مدعوم بالكامل لذلك لا يمكن استخدام الخيار الفرعي "تحديد الارتباط" (5 أو Cisco مالك - 150) لتحديد التجمع الصحيح على خادم DHCP.

لحل هذه المسألة، يمكن إستخدام هذا النهج:

- يجب إنشاء نطاق عناوين IP للتوزيع الذي تجمع ياطاق DHCP. يجب إستبعاد نطاق IP الكامل من DHCP لمنع التخصيص من GIADDR وتجاهل الحزمة. نسمي هذا التجمع relay_pool. تجمع IP للتوزيع.
- يجب إنشاء نطاق نطاق IP الذي تريد توزيعه. نسمي هذا التجمع IP_POOL
- يجب إنشاء Superscope ويجب تضمين كل النطاقين - relay_pool و ip_pool

دعنا نرى كيفية معالجة حزمة DHCP على الخادم.

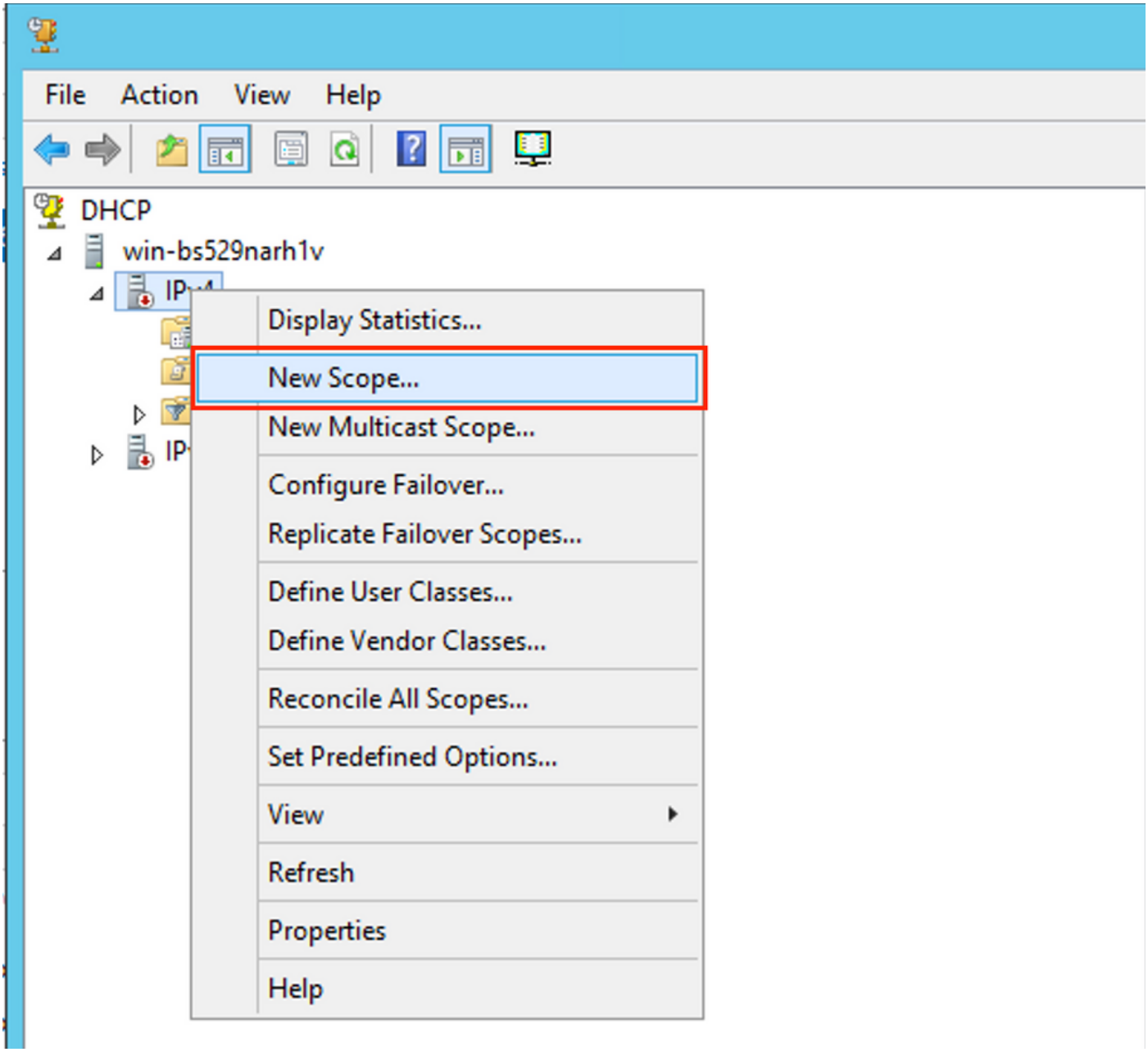
1. تم تلقي حزمة DHCP بواسطة الخادم.
2. استنادا إلى GIADDR. يتم إختيار التجمع المناسب relay_pool في المرتفع المناسب.
3. نظرا لعدم وجود عنوان IP حرة في relay_pool (هل تذكر أن النطاق الكامل مستبعد؟)، يرجع إلى IP_POOL في نفس النطاق الفائق.
4. يتم تخصيص العنوان من المجموعة الفائقة المقابلة وإرساله مرة أخرى إلى الترحيل.

من أكبر عيوب هذه الطريقة أنه يجب أن يكون لديك إستراجاع فريد لكل شبكة VLAN/VNI لكل VTEP حيث يتم تحديد تجمع DHCP استنادا إلى عنوان الترحيل.

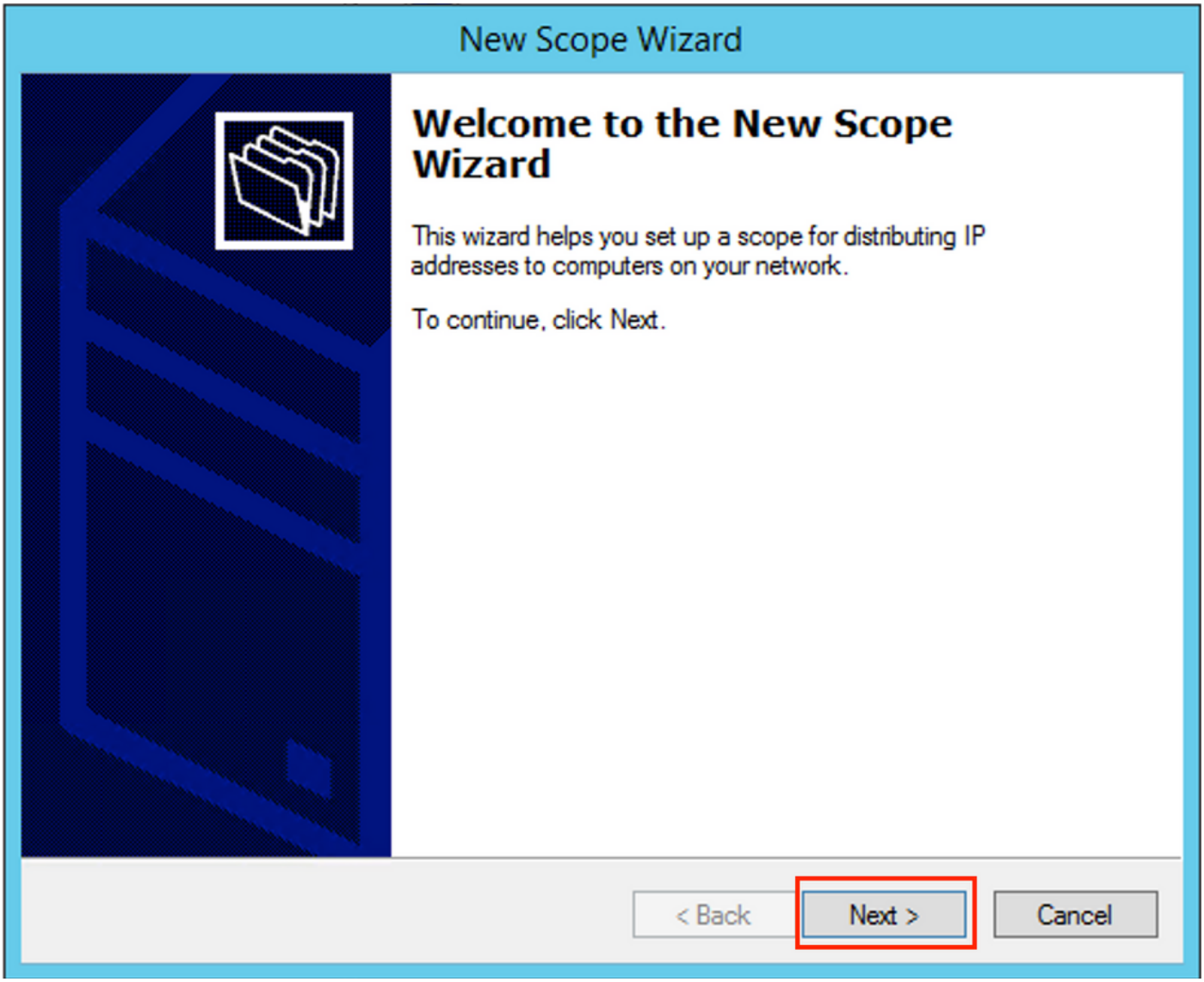
يقودنا هذا الخيار إلى إستخدام نطاق IP كبير لعناوين IP للاسترسال.

الخيار 1. إرشادات خطوة بخطوة حول كيفية تكوين Win2012 R2.

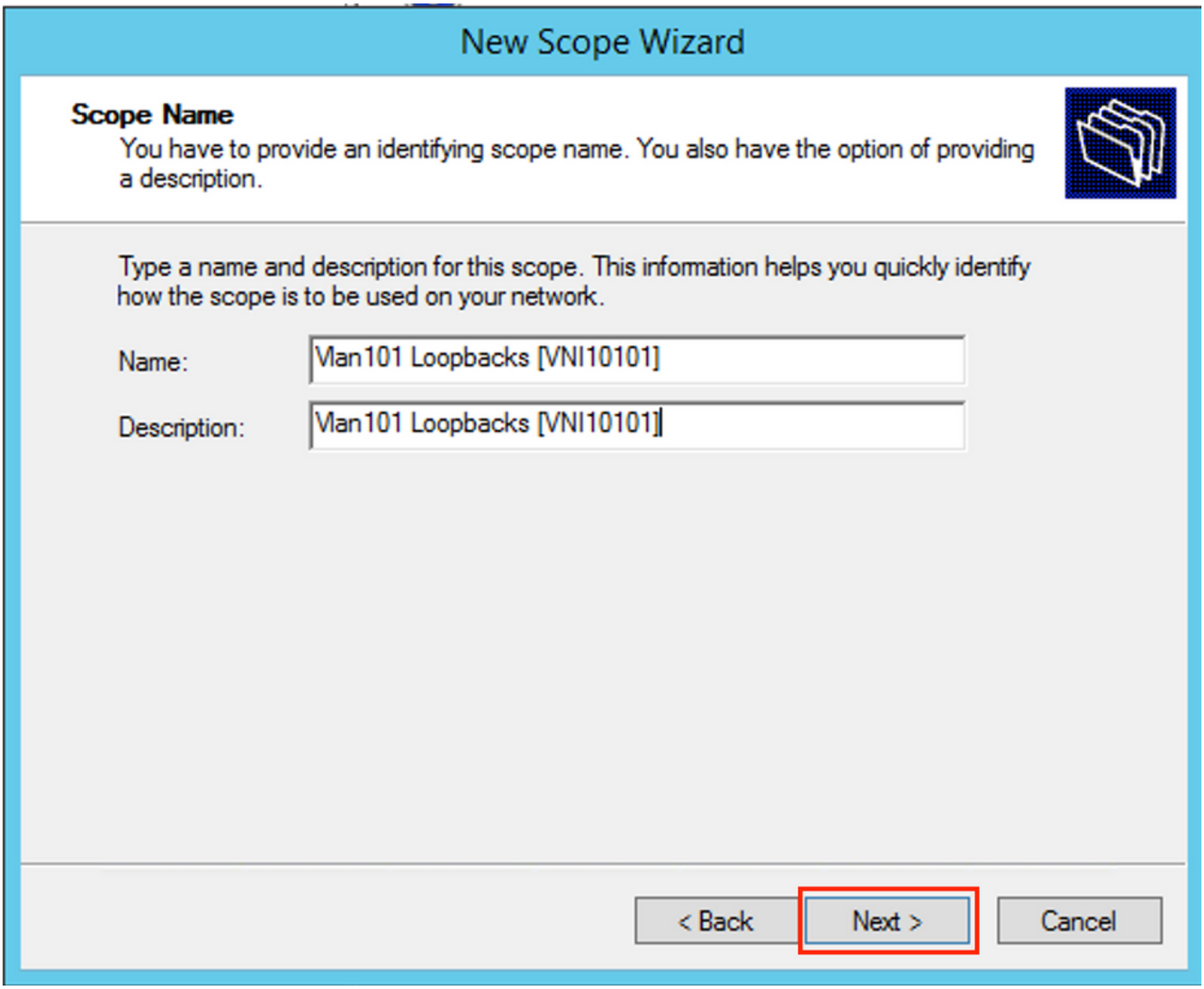
قم بإنشاء نطاق DHCP لعناوين الترحيل. انقر بزر الماوس الأيمن واختر **جديد نطاق** كما هو موضح في الصورة.



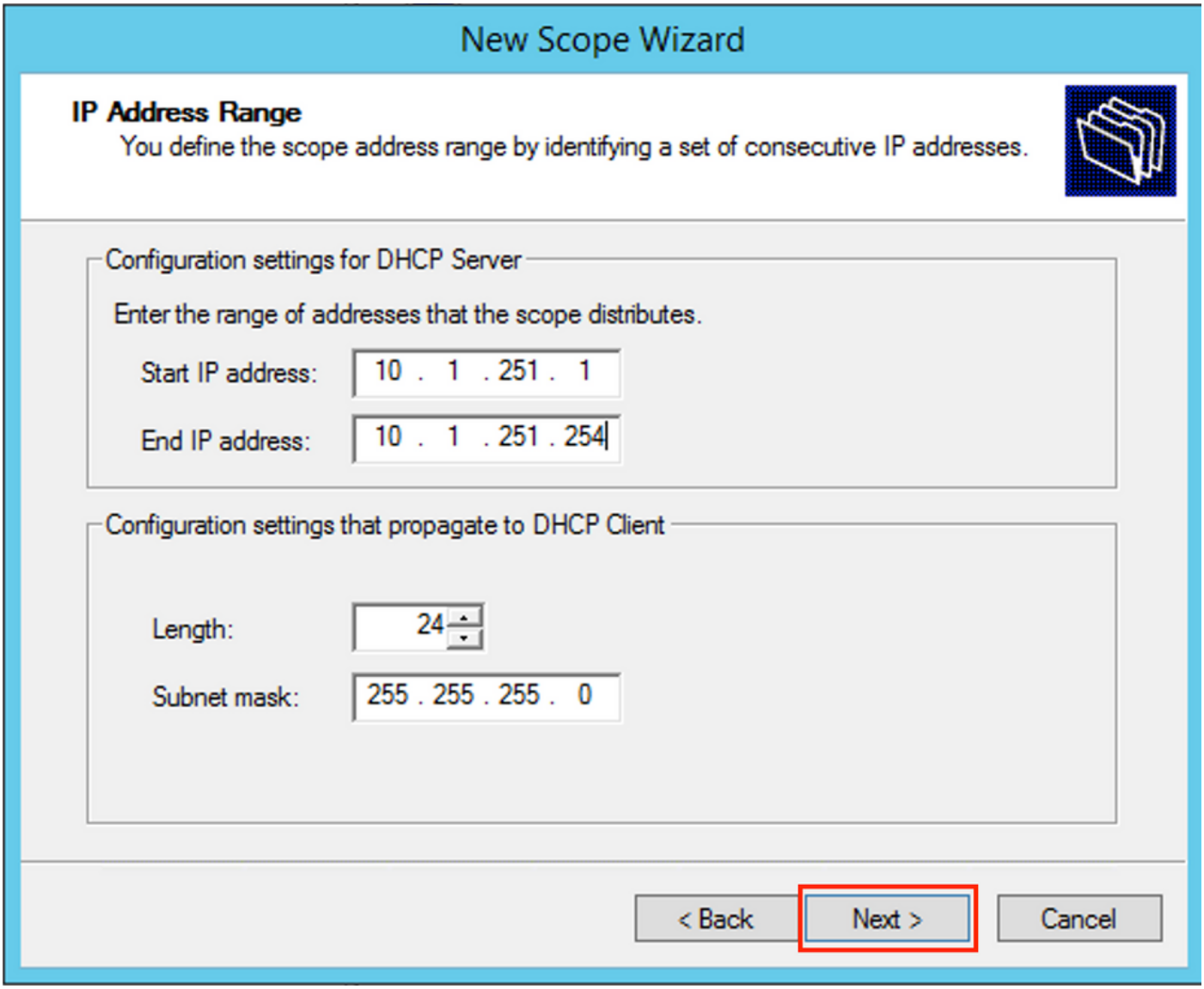
حدد **التالي** كما هو موضح في الصورة.



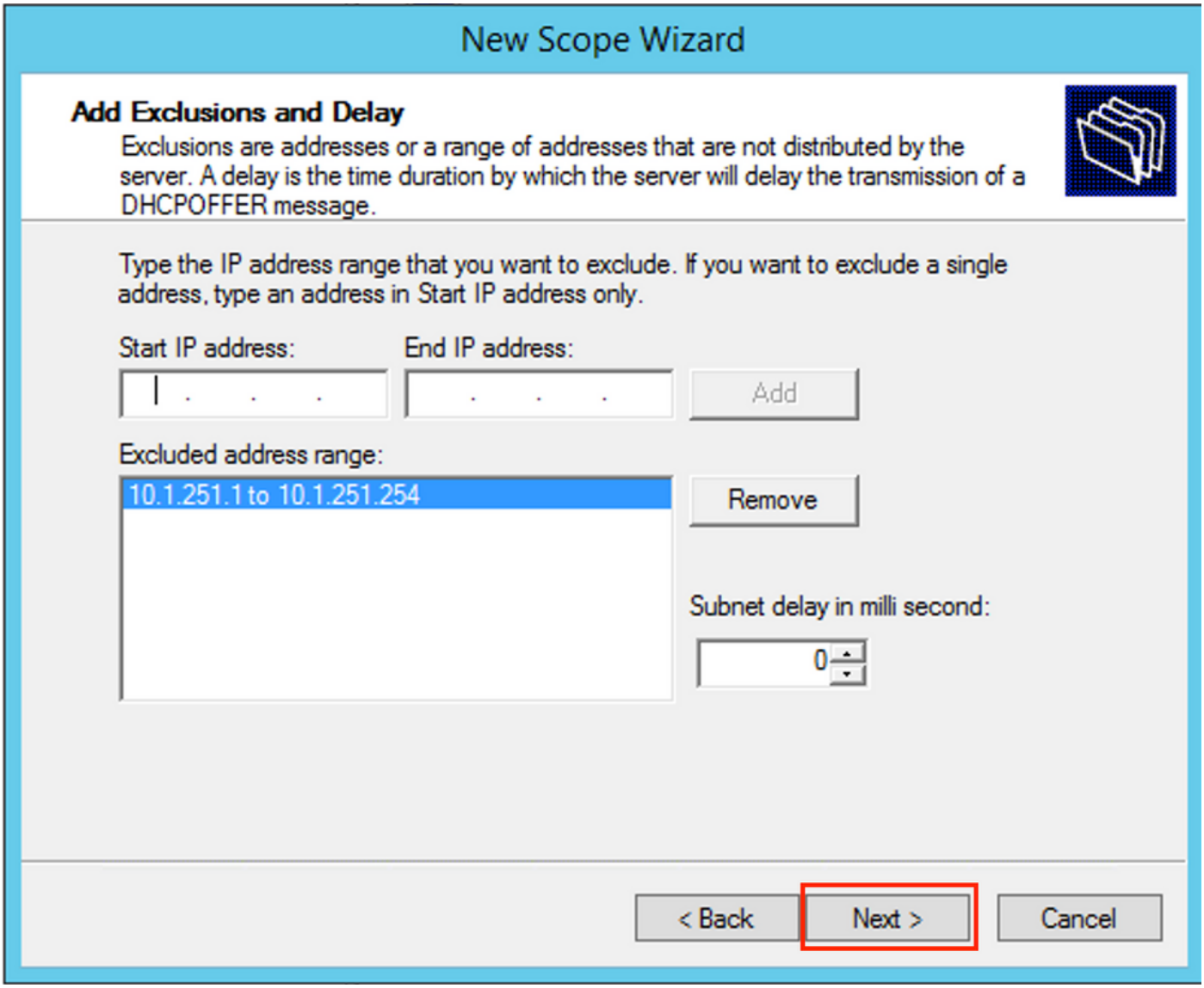
قم بتعبئة اسم ذو معنى، وصف، ثم حدد **التالي** كما هو موضح في الصورة.



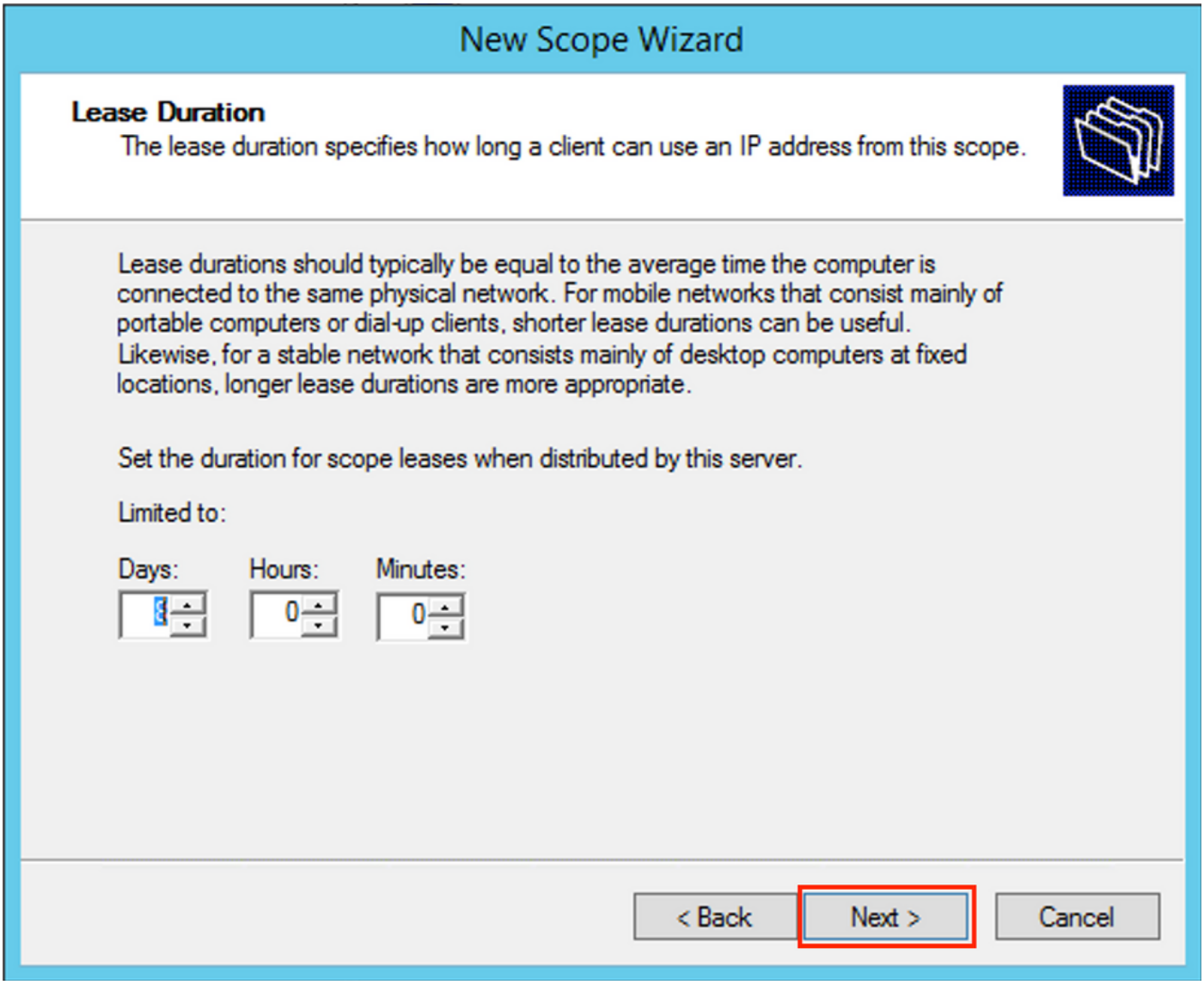
المألم معلومات عنوان IP لتجمع الترحيل. في هذا المثال، يكون قناع الشبكة هو /24 ولكن يمكن أن يكون أكبر أو أصغر (يعتمد على حجم الشبكة) كما هو موضح في الصورة.



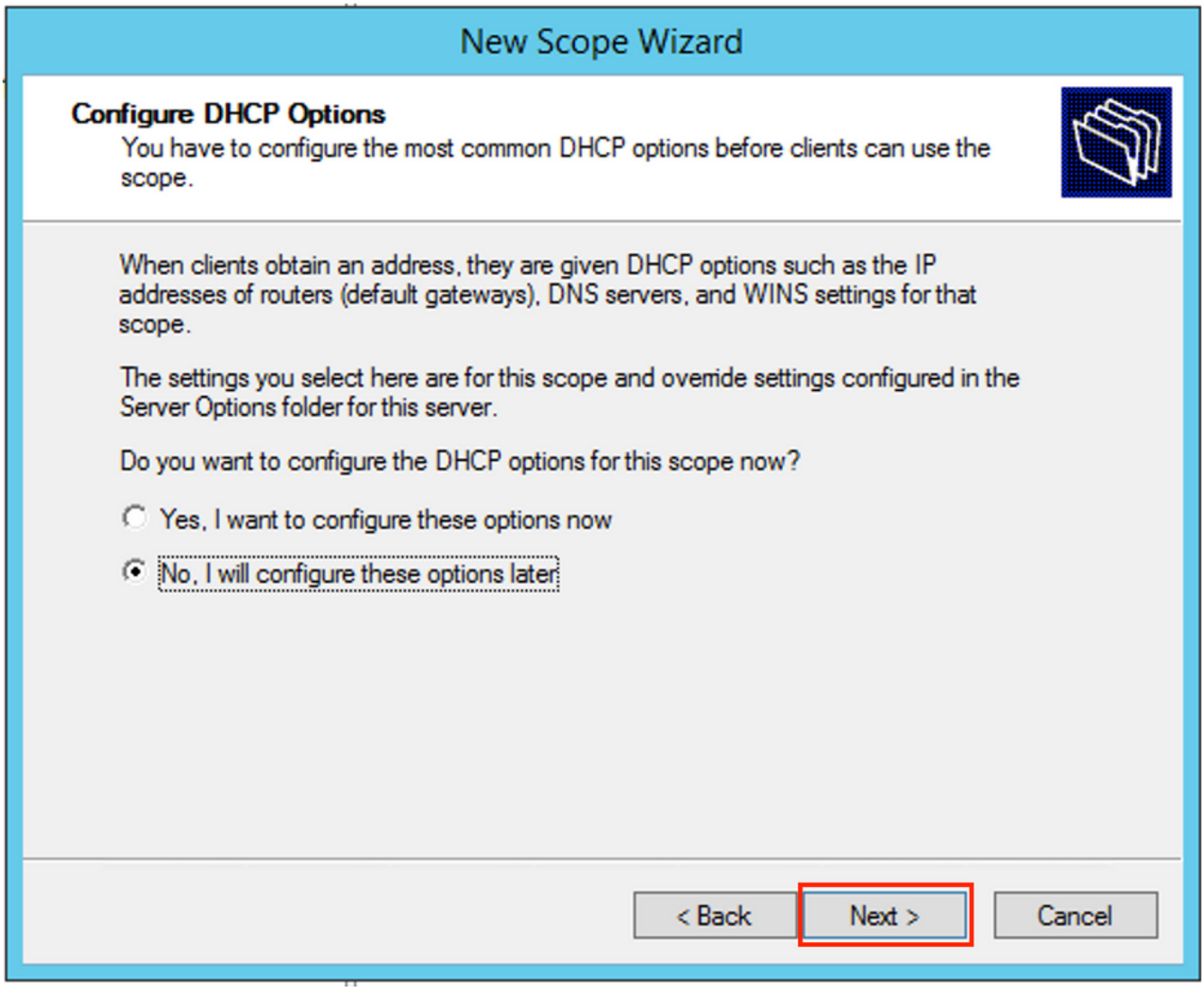
إستثناء كافة النطاقات من التجمع. هذا مهم، وإلا، يمكن تخصيص عناوين IP من هذا التجمع.



قم بتكوين وقت التأجير (افتراضيا يكون 8 أيام) كما هو موضح في الصورة.

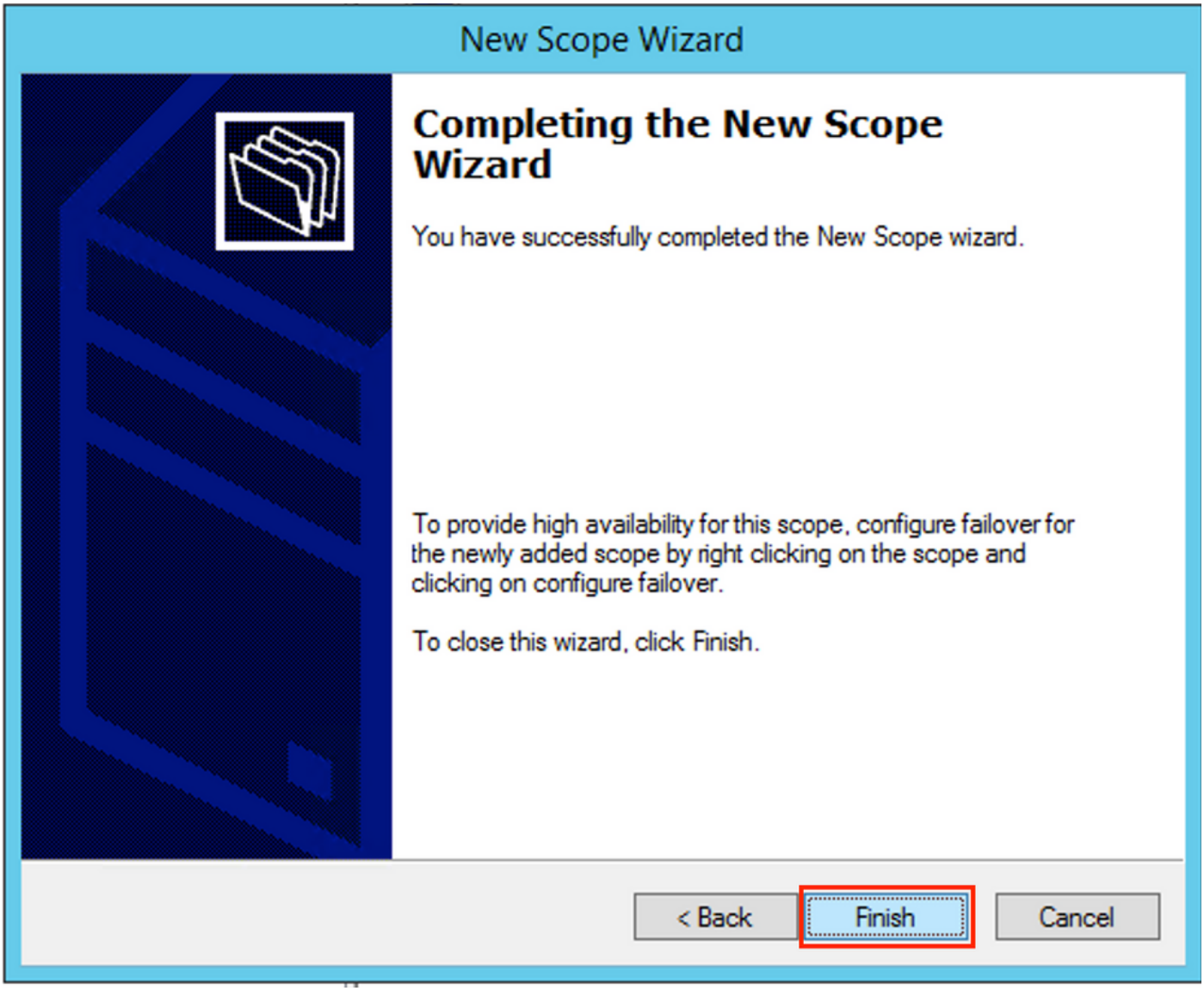


يمكنك تكوين معلمات خيار DHCP مثل DNS/WINS (تم تخطيه في هذا المثال).

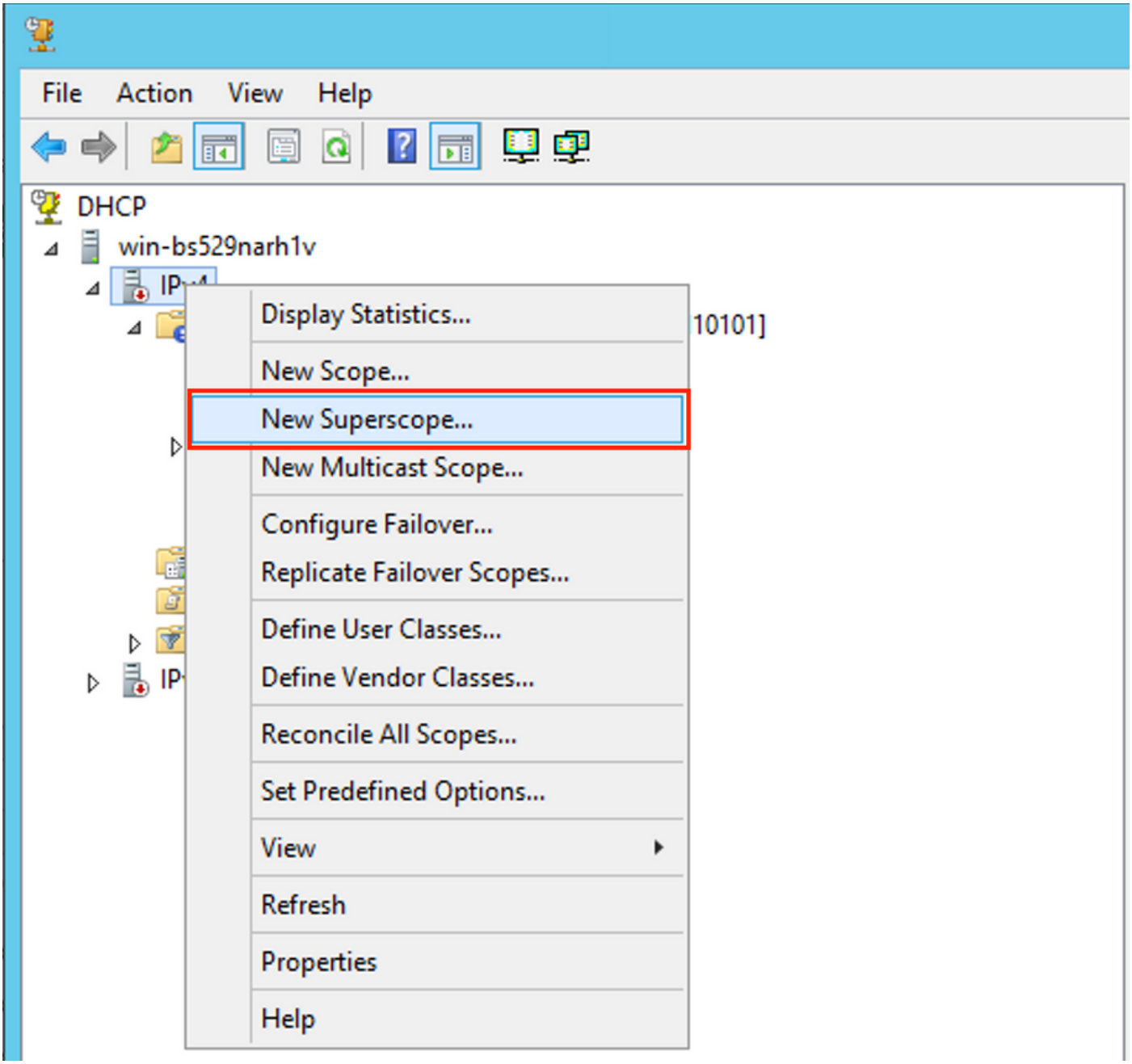


قم بتنشيط النطاق كما هو موضح في الصورة.

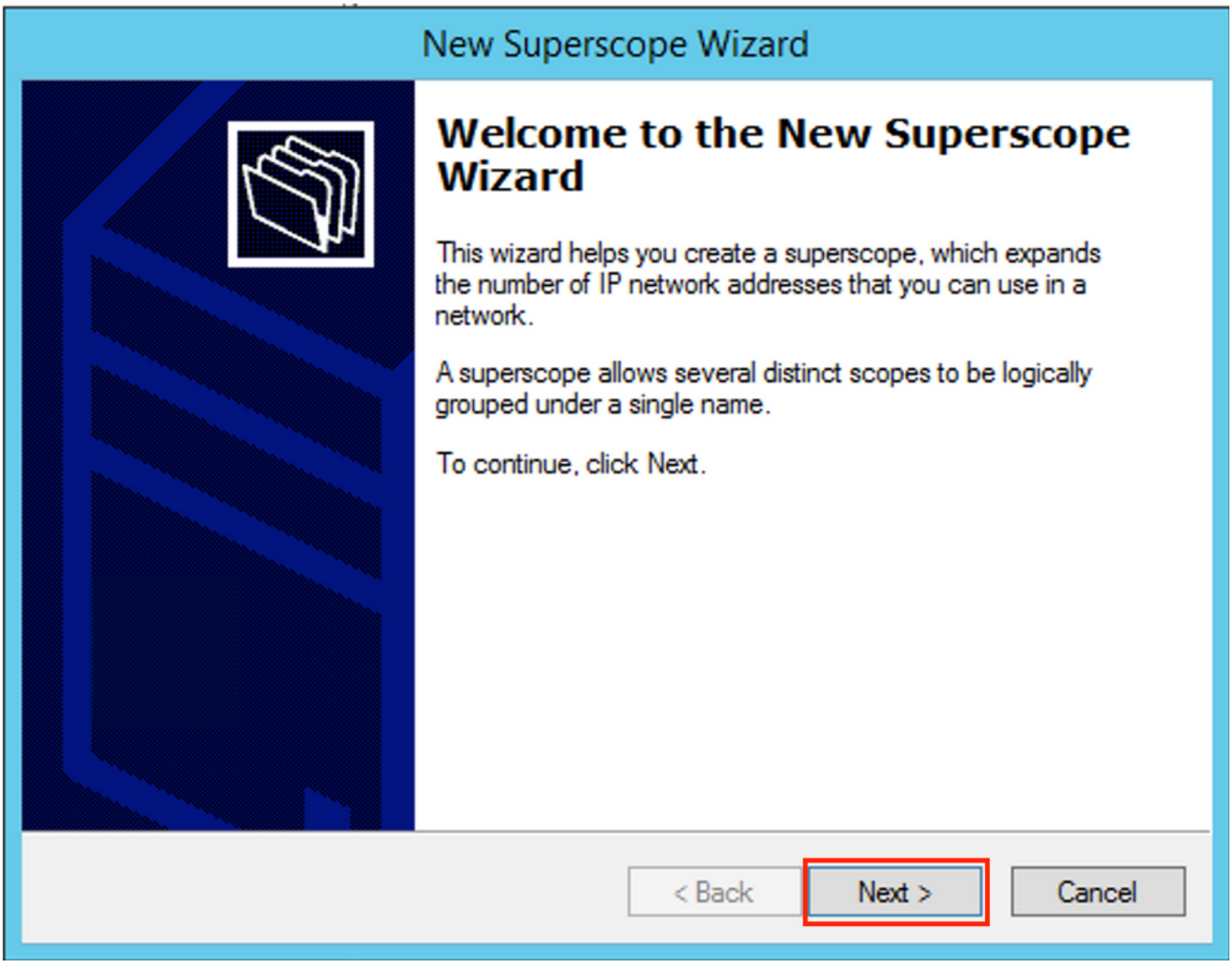
قم بإنهاء التكوين كما هو موضح في الصورة.



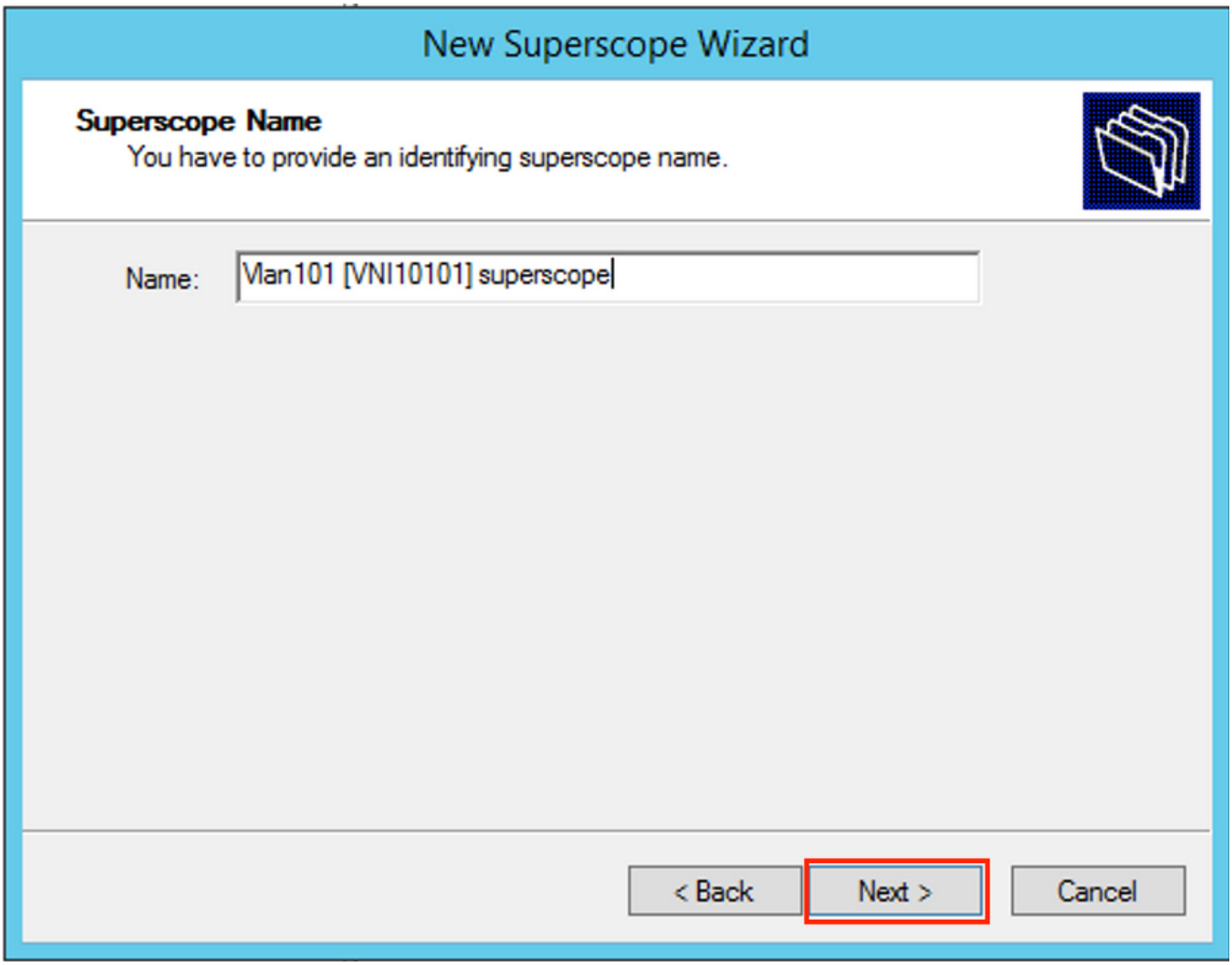
الآن قم بإنشاء أعلى درجة. قم بالتحديد بزر الماوس الأيمن واختر **المرتفع الجديد** كما هو موضح في الصورة.



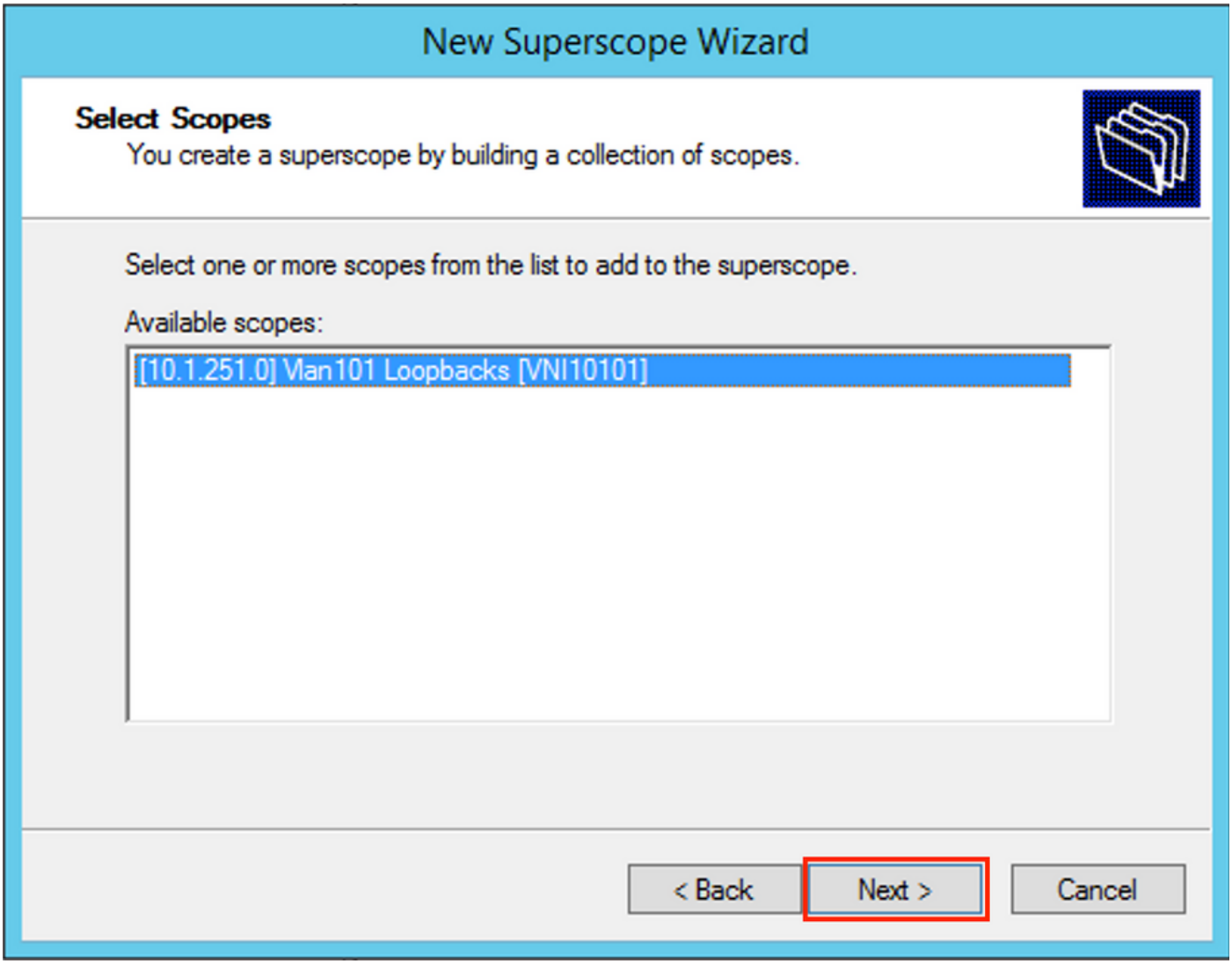
حدد **التالي** كما هو موضح في الصورة.



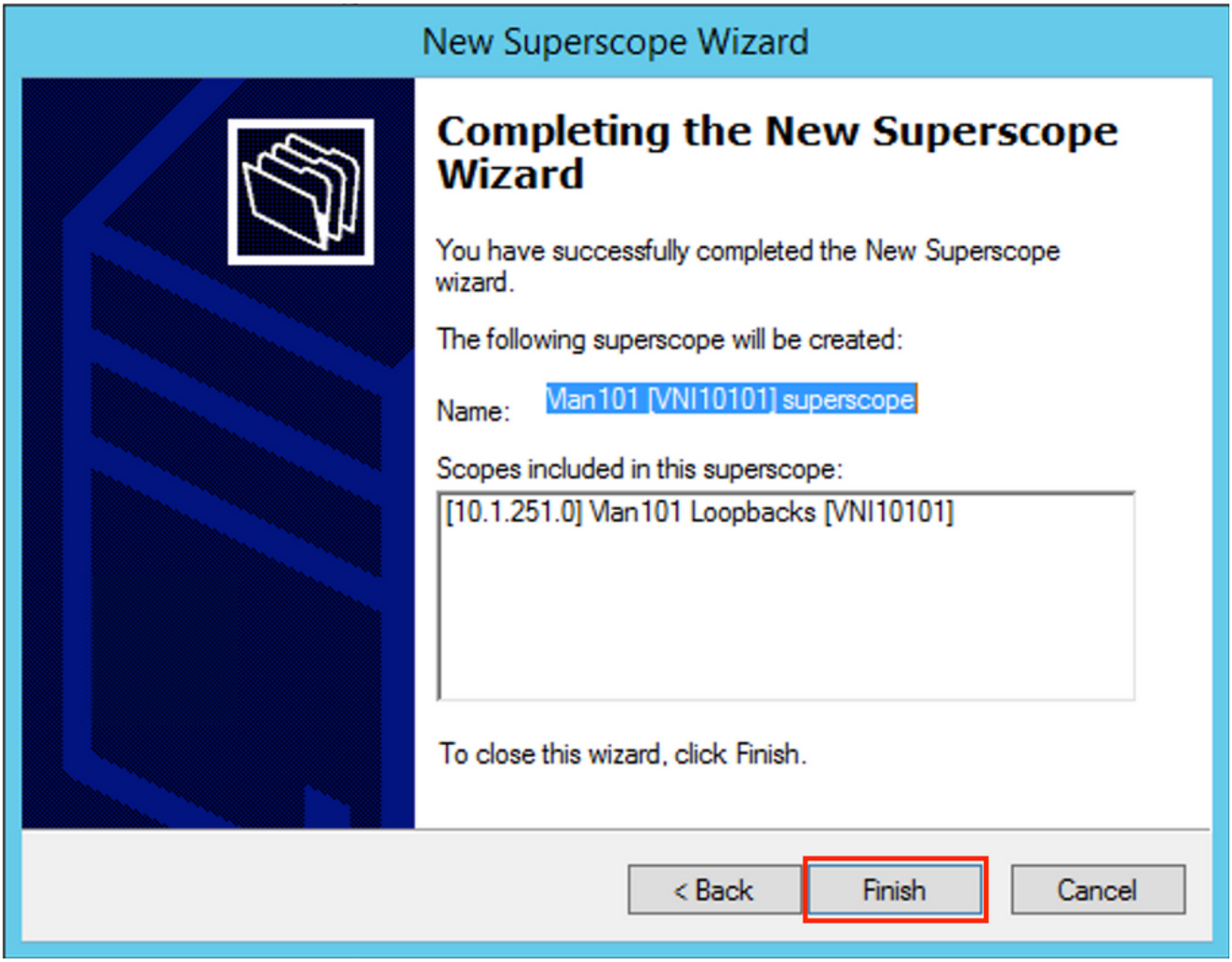
أختر اسم ذو معنى للمنطار **العالي** كما هو موضح في الصورة.



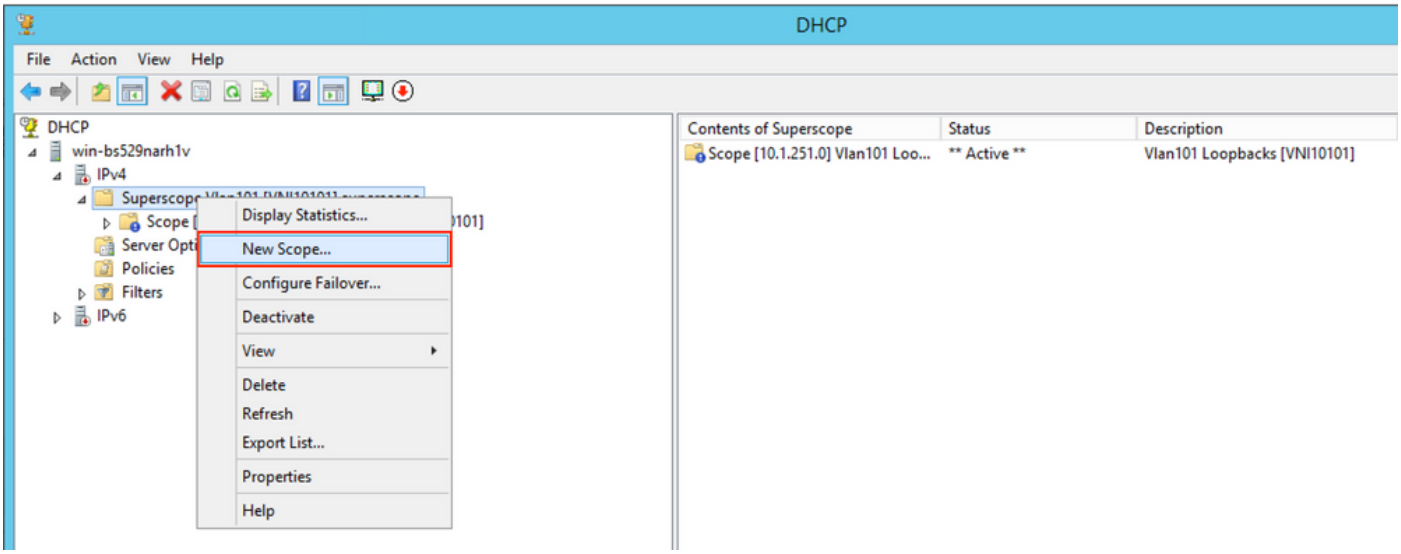
أختر النطاق الذي تريد إضافته إلى النطاق الفائق.



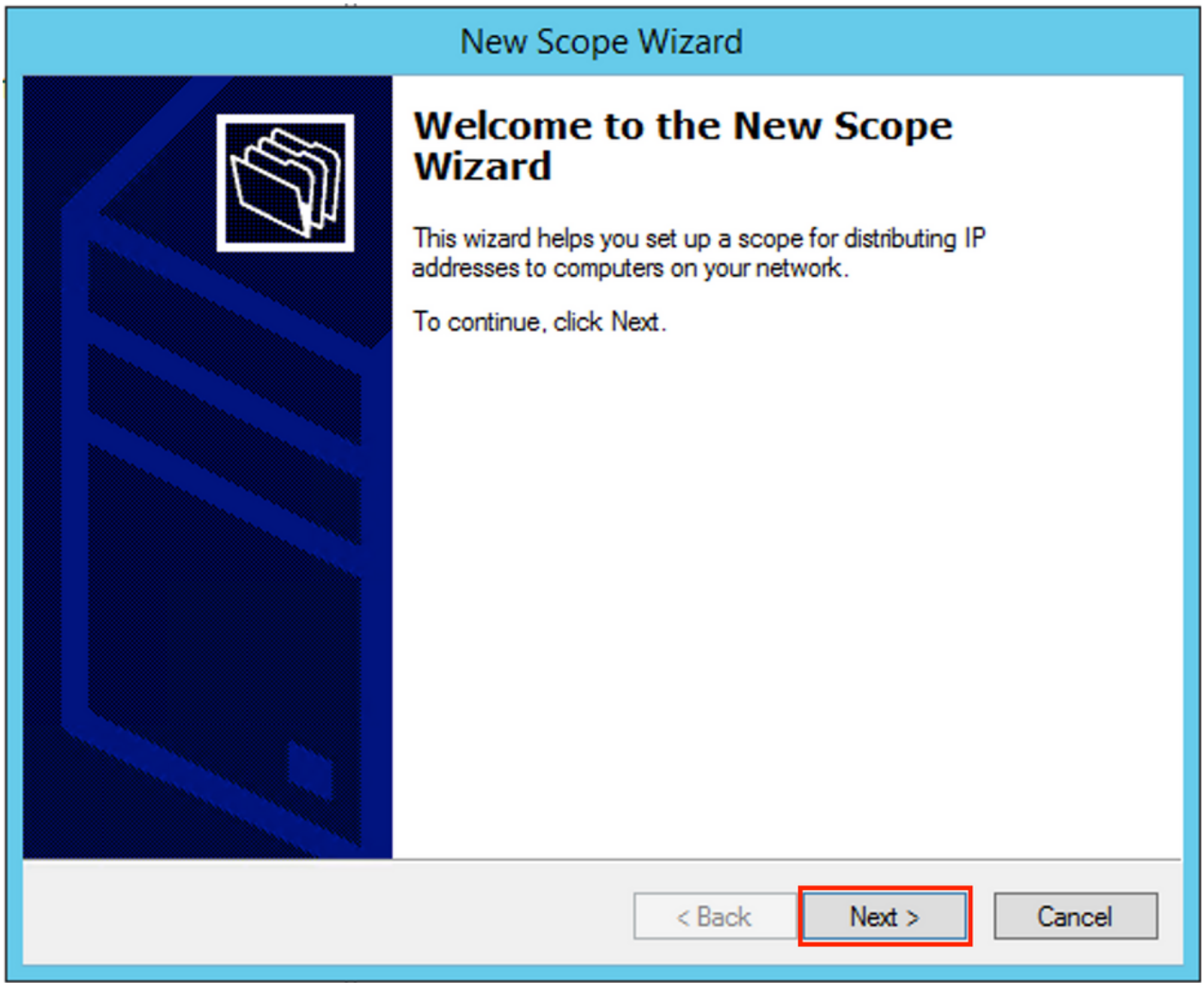
قم بإنهاء الإعداد كما هو موضح في الصورة.



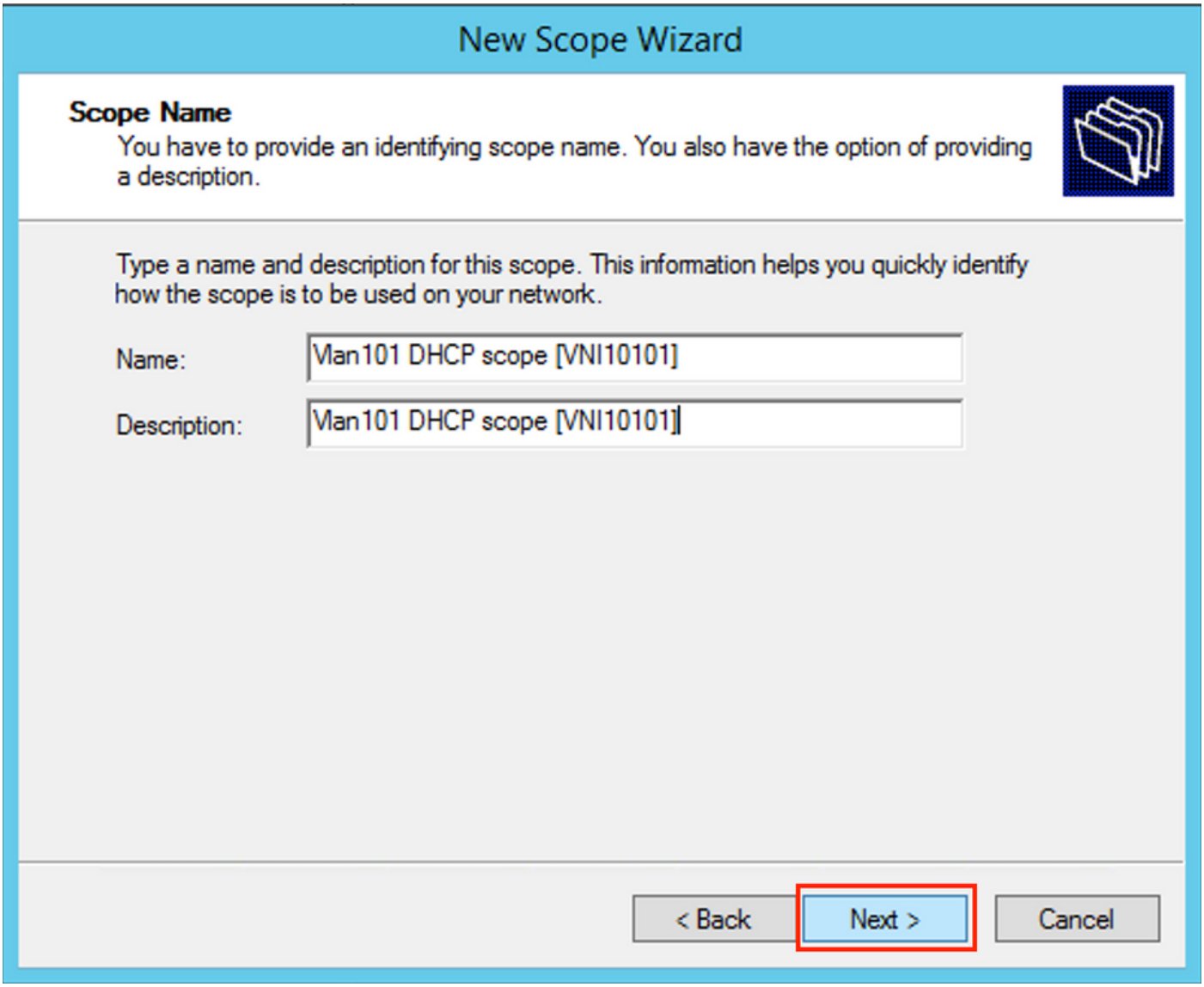
قم بإنشاء تجمع DHCP يتم من خلاله تخصيص عناوين IP. انقر بزر الماوس الأيمن وحدد **نطاق جديد...** كما هو موضح في الصورة.



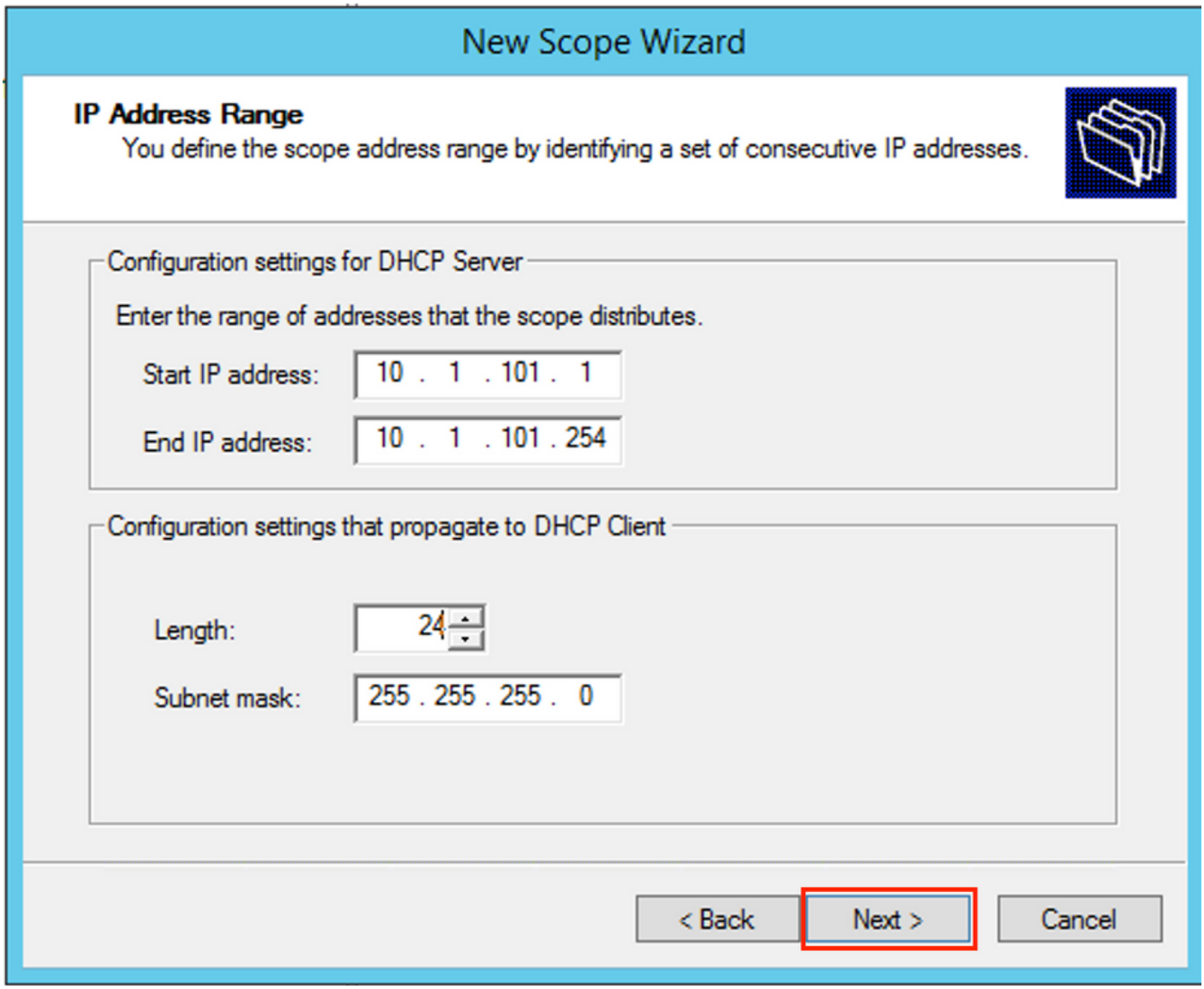
حدد **التالي** كما هو موضح في الصورة.



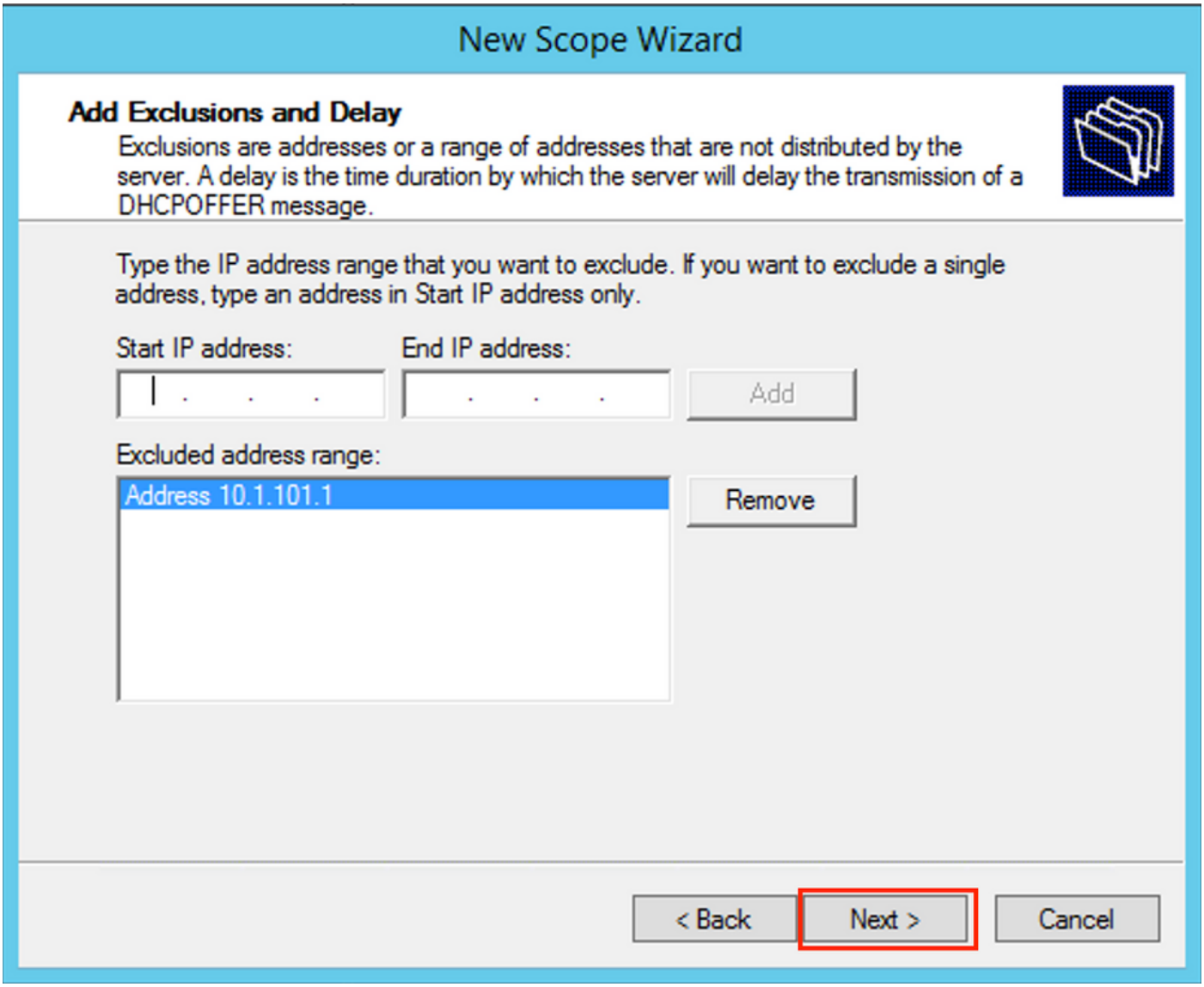
أختر اسم ذو معنى ووصف كما هو موضح في الصورة.



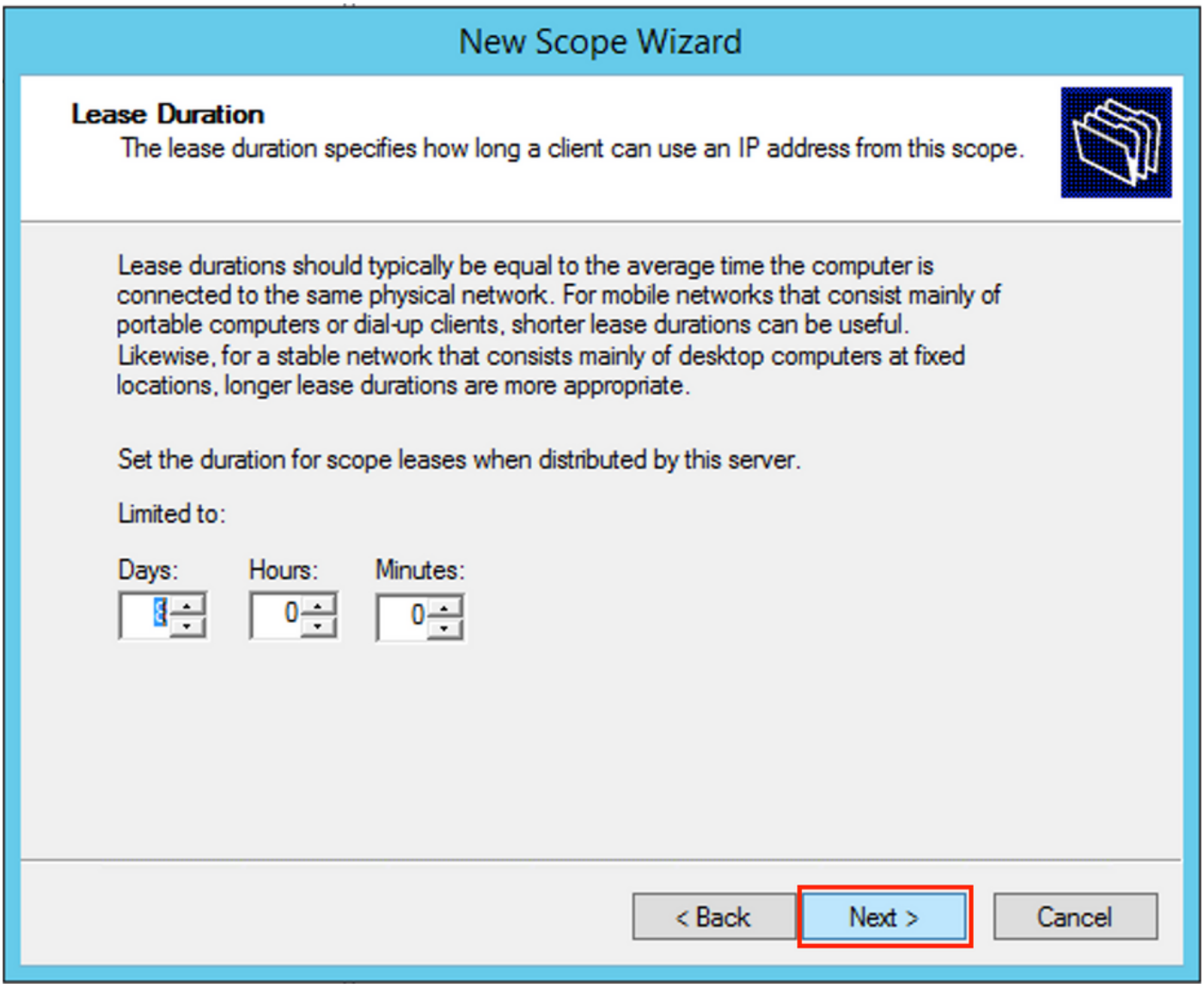
حدد الشبكة والقناع للتجمع الذي تريد تخصيص عناوين IP له للعملاء كما هو موضح في الصورة.



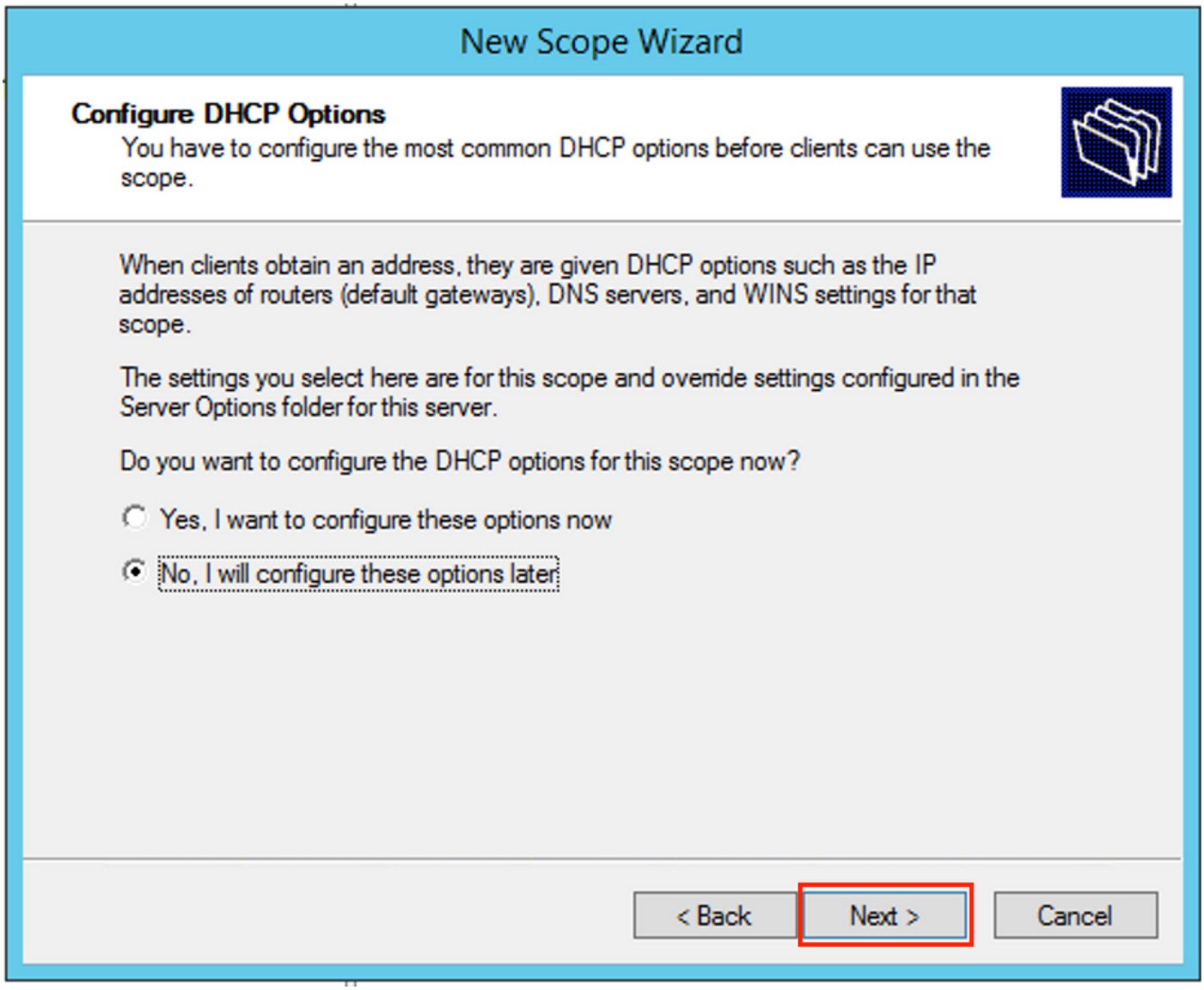
استثنيت العنوان من التقصير مدخل من البركة (في هذا مثال وه 10.1.101.1) كما وه موضح في الصورة.



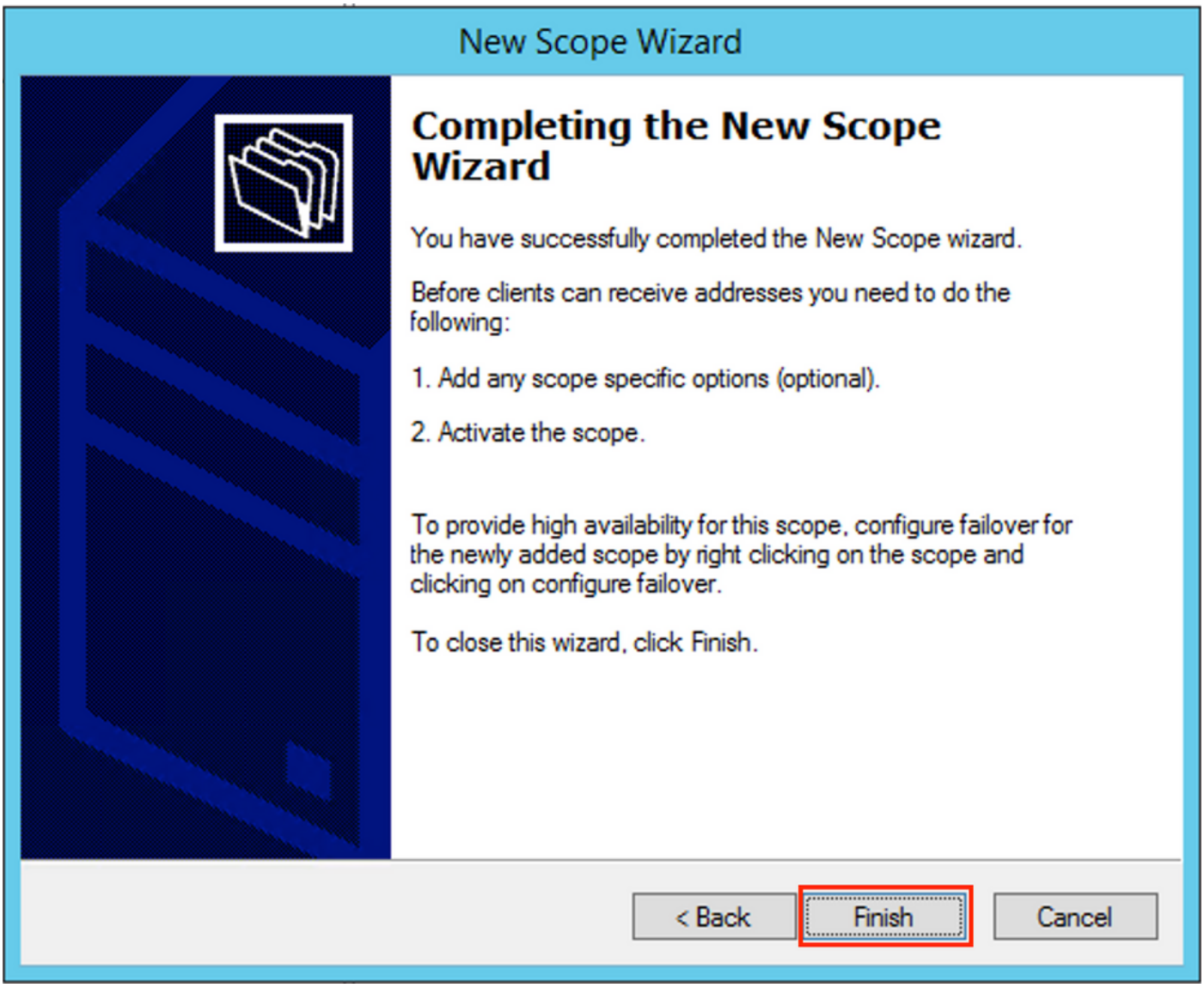
حدد مؤقت التأجير كما هو موضح في الصورة.



يمكنك إختياريا تحديد DNS/WINS (تم تخطيه في هذا المثال).



قم بإنهاء التكوين كما هو موضح في الصورة.



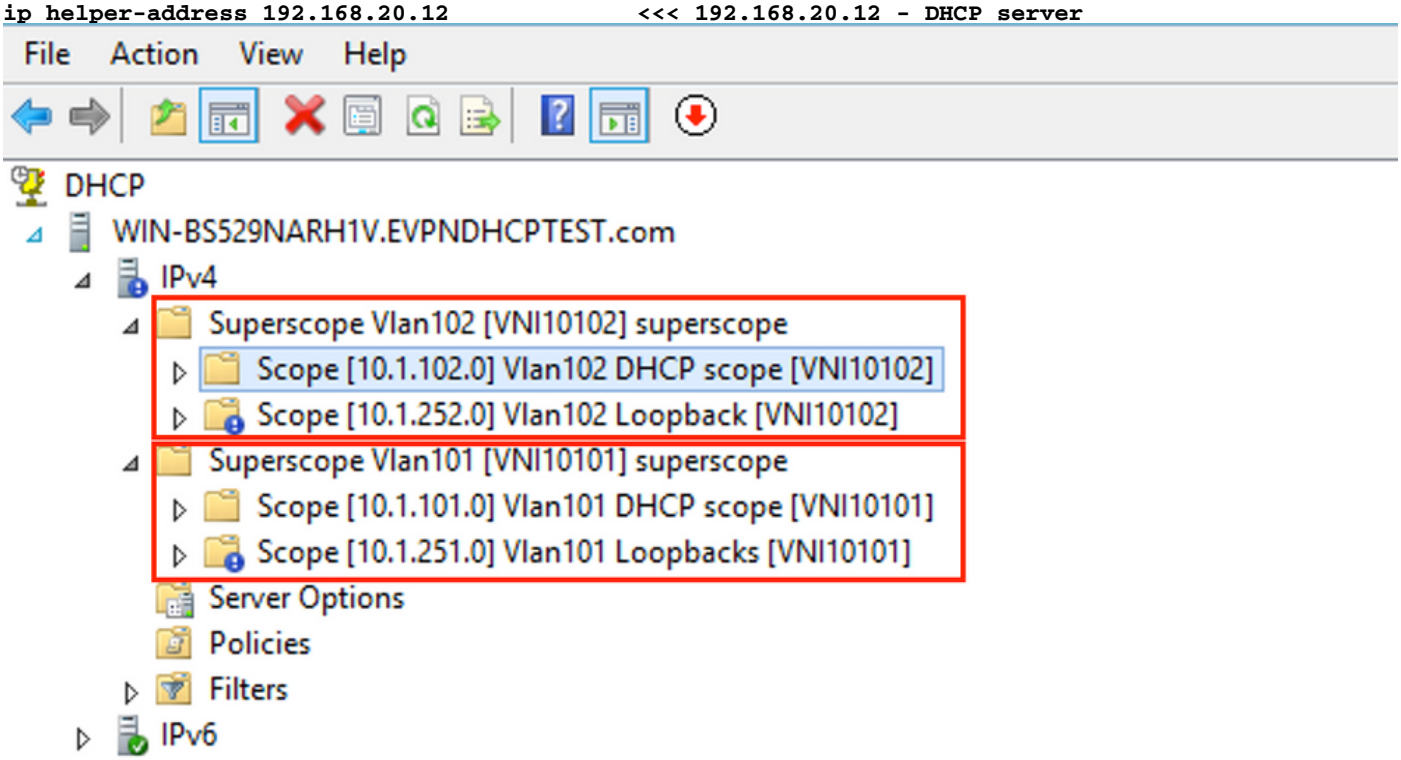
بعد إنشاء التجمع، يجب إنشاء سياسة للتجمع.

- في معرف دائرة وكيل النهج [1] مطابق
- إن يتلقى أنت عدة VLANs/VNIs أنت يضطر أن يخلق سوبر بركة مع subpool ل ترحيل عنوان وال حقيقي IP مدى لتخصيص لكل VLAN/VNI
- يستعمل هذه مثال VNIs 10101 و 10102

تكوين المحول:

```
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
```

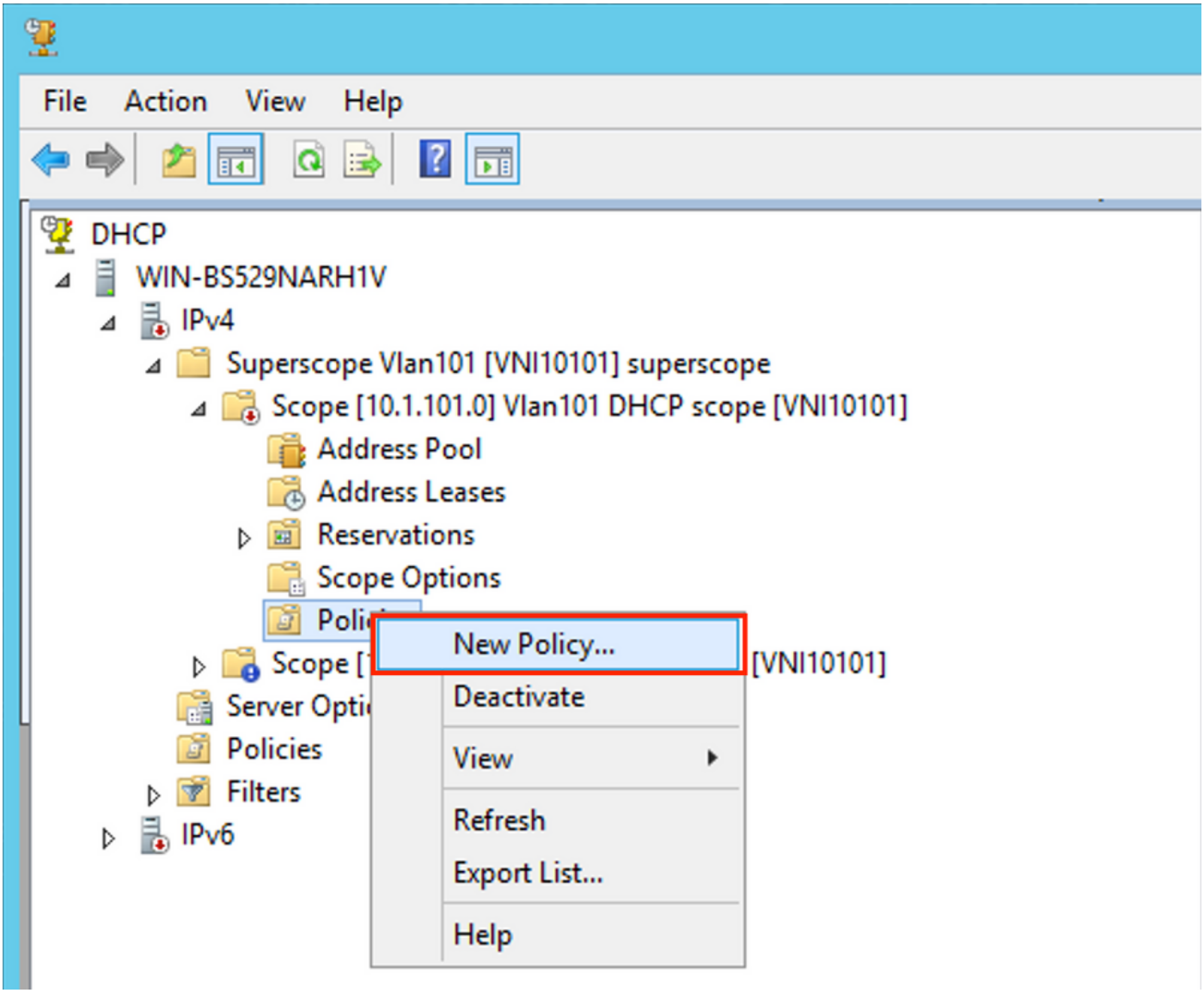
```
!
interface Vlan101
 vrf forwarding green
 ip dhcp relay source-interface Loopback101  <<< DHCP relay source is unique Loopback101
 ip address 10.1.101.1 255.255.255.0
ip helper-address 192.168.20.12              <<< 192.168.20.12 - DHCP server
!
interface Vlan102
 vrf forwarding green
 ip dhcp relay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



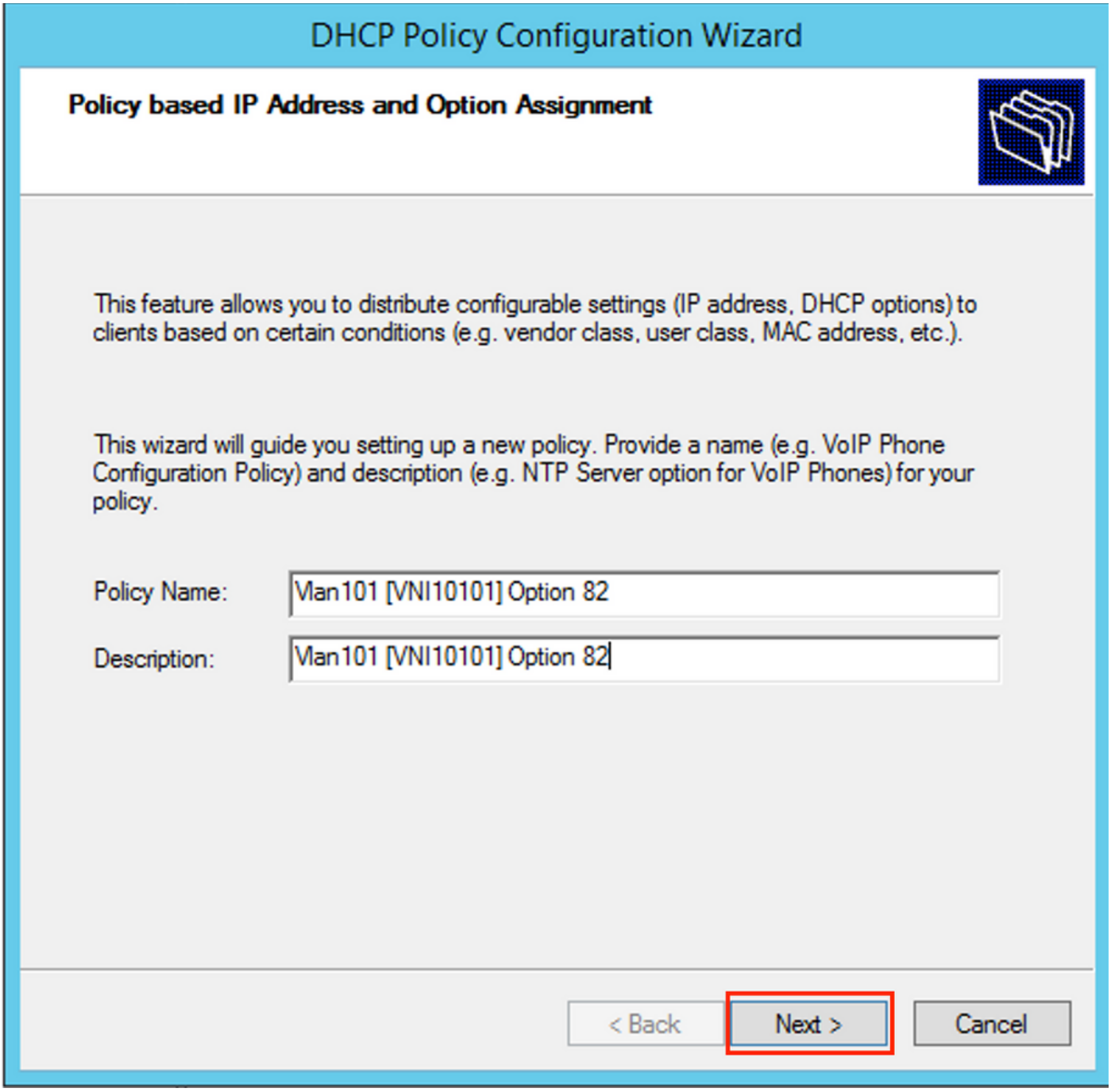
خيار التكوين WIN2012 R2 2 - مطابقة حقل معرف دائرة الوكيل

- أما عيوب النهج الأخير فتتمثل في الاستخدام العالي لميزة الاسترجاع الفريدة، لذلك يتمثل خيار آخر في مطابقة حقل معرف دائرة الوكيل.
- الخطوات هي نفسها، ولكن يمكنك إضافة إنشاء نهج لتحديد النطاق ال يستند إلى حقل معرف دائرة الوكيل بدلا من IP الترحيل.

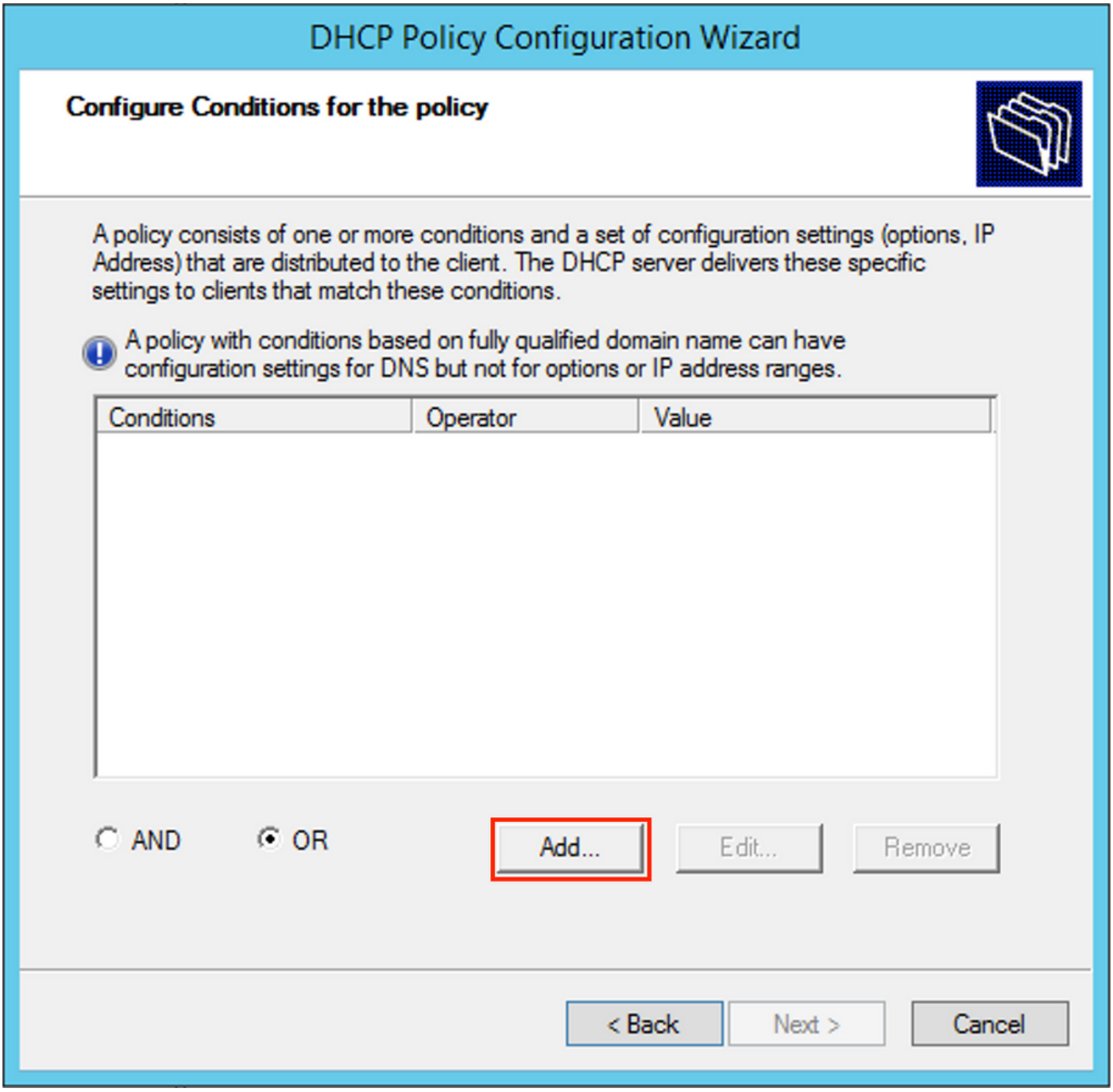
وضع السياسات. انقر بزر الماوس الأيمن فوق التجمع وحدد **نهج جديد** كما هو موضح في الصورة.



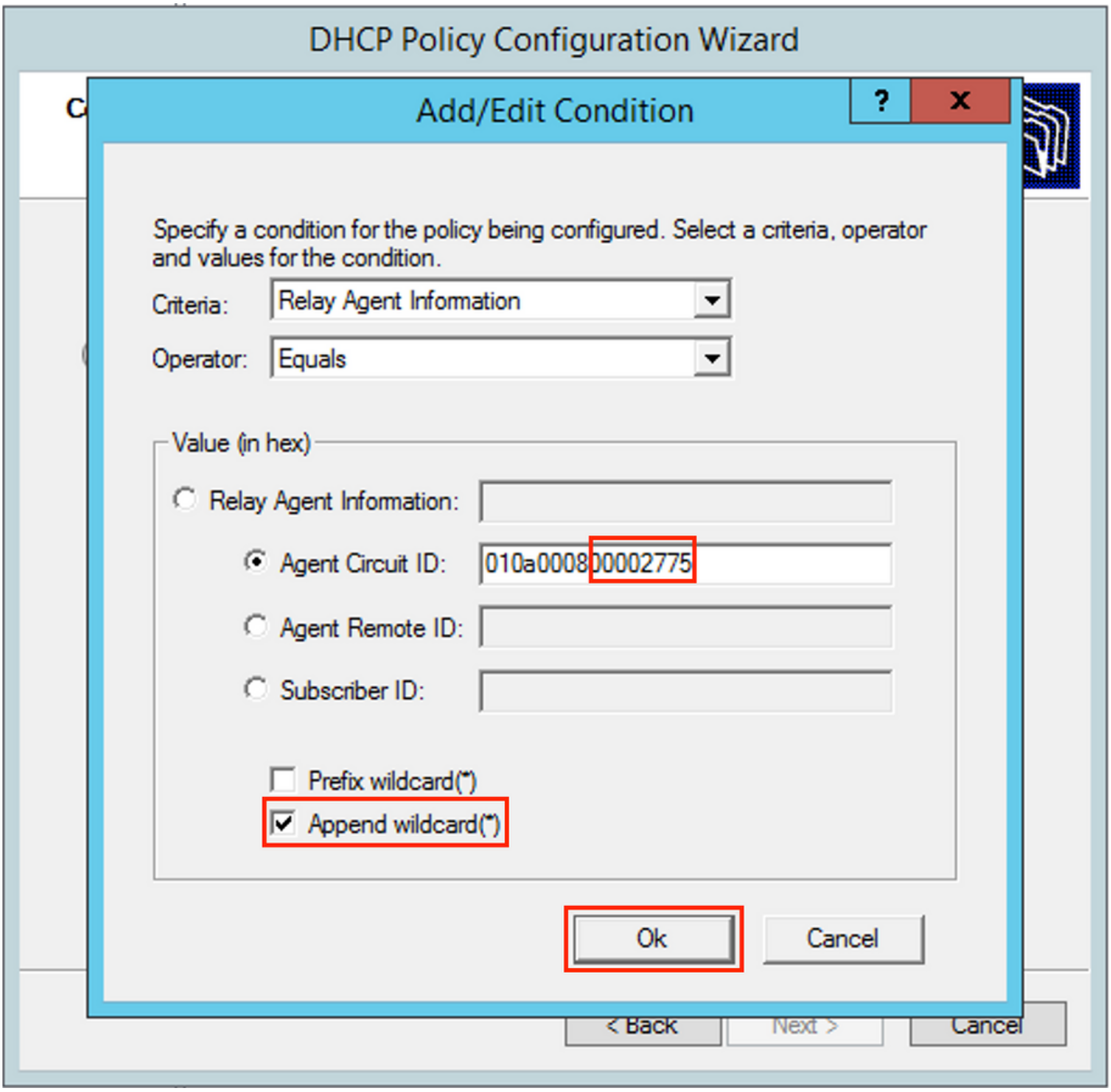
أختر اسم ذو معنى ووصف للنهج كما هو موضح في الصورة.



قم بإضافة الشرط الجديد كما هو موضح في الصورة.



أدخل معرف الدائرة المناسب (لا تنس مربع **إضافة حرف بدل (*)**) كما هو موضح في الصورة.



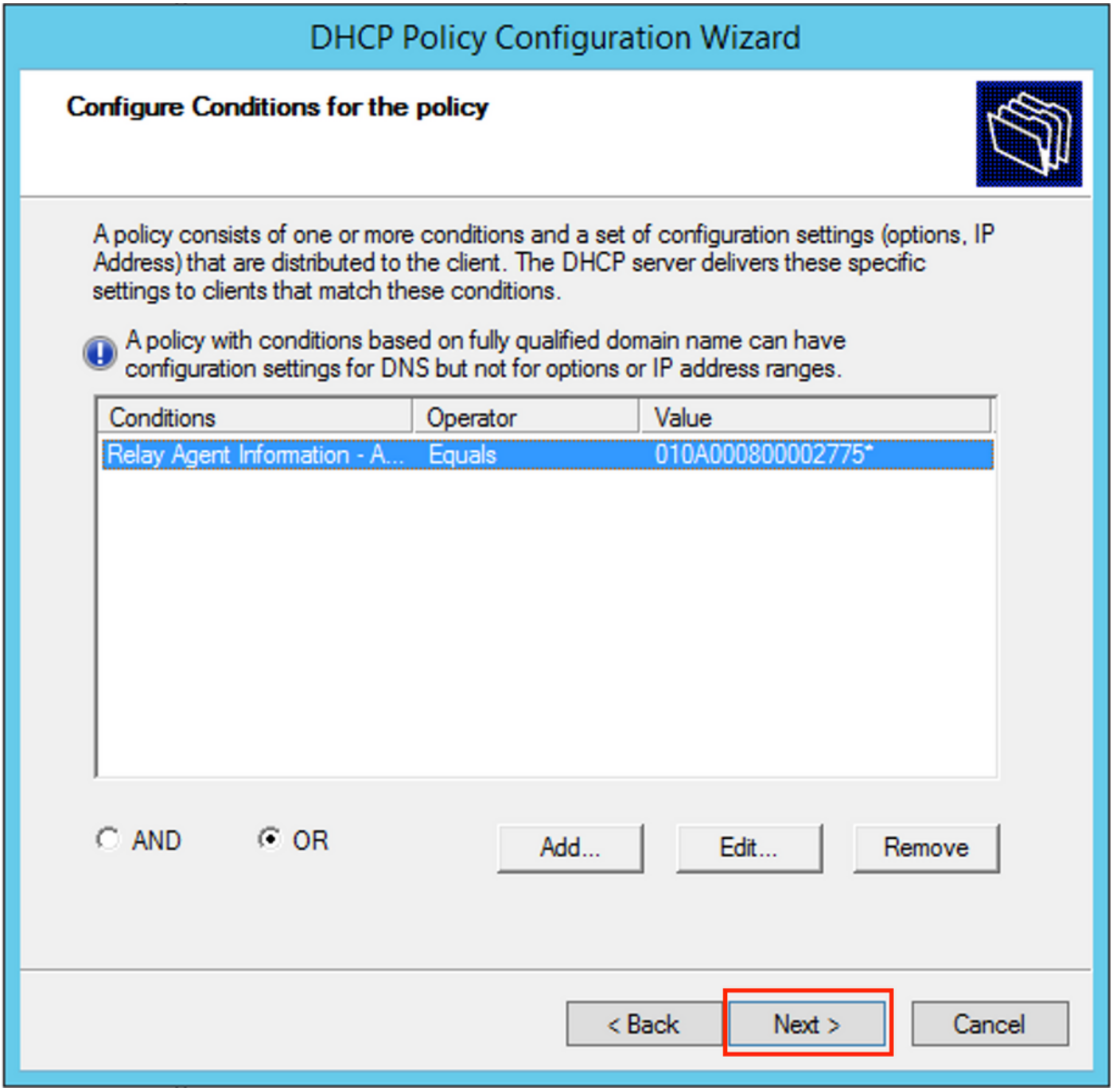
توضيح حول سبب إختيار هذا الرقم:

في Wireshark، أنت يستطيع رأيت وكيل دائرة id **يساوي 010a00800002775010a000**، أي يكون هذا قيمة مشتقة من (00002775 hex = 10101 decimal يكون مساوي إلى شكل VNI 10101 ل VLAN 101).

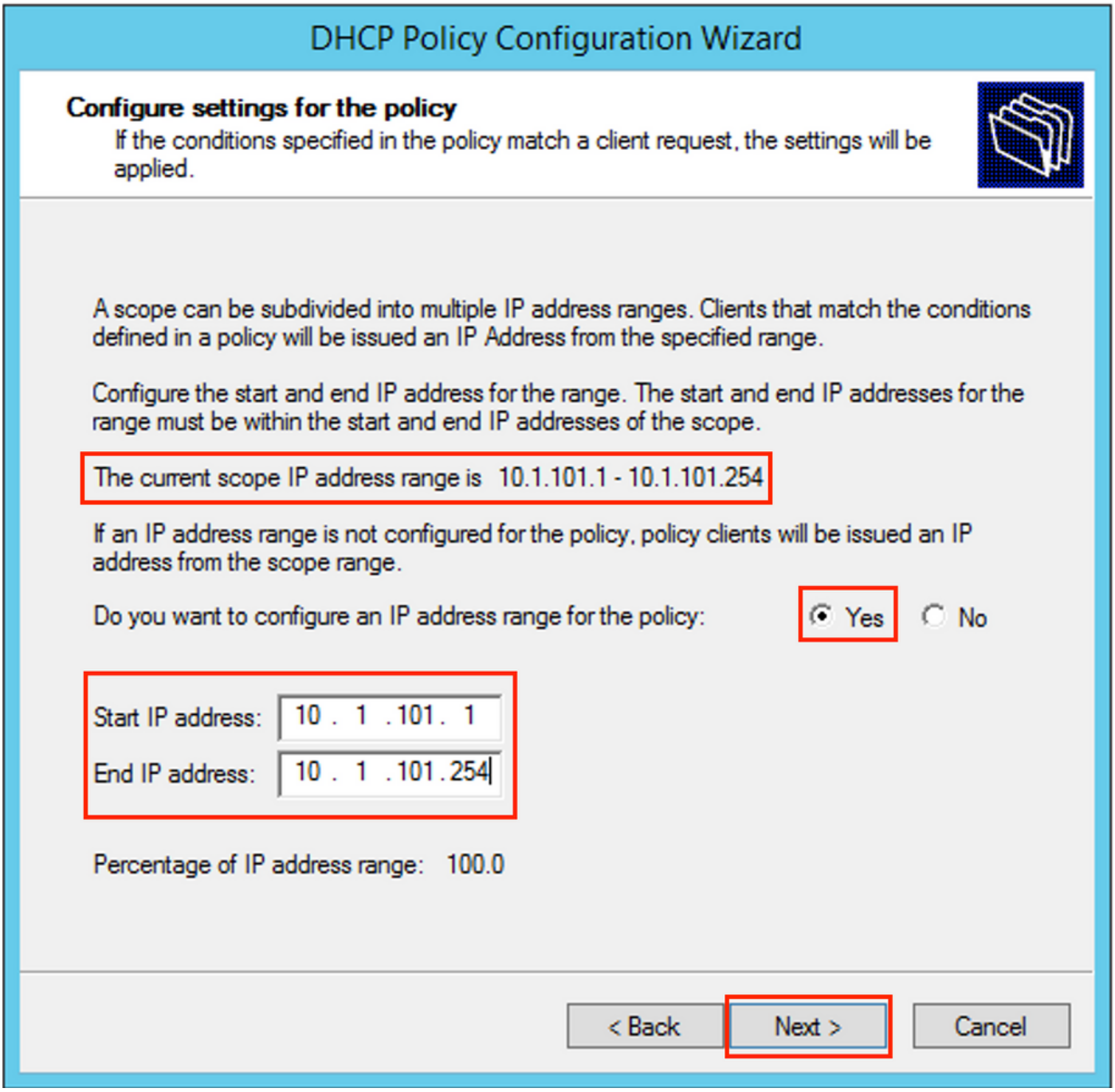
```
▼ Option: (82) Agent Information Option
    Length: 44
  ▼ Option 82 Suboption: (1) Agent Circuit ID
      Length: 12
      Agent Circuit ID: 010a000800002775010a0000
  ▶ Option 82 Suboption: (2) Agent Remote ID
  ▶ Option 82 Suboption: (151) VRF name/VPN ID
  ▼ Option 82 Suboption: (150) Link selection (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
```

تم تشفير الخيار الفرعي لمعرف دائرة الوكيل بهذا التنسيق ل VXLAN VN:

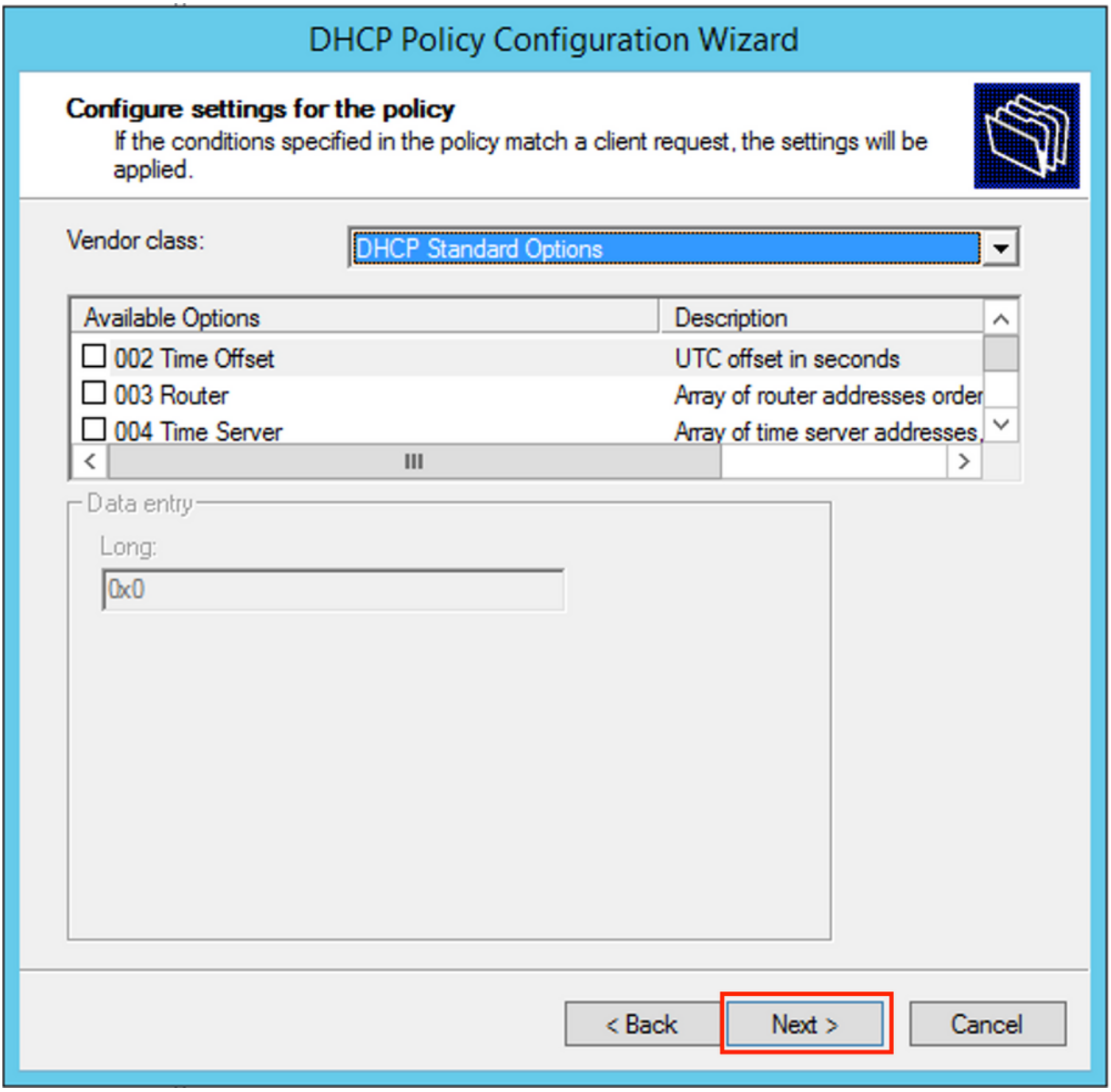
نوع الخيار الفرعي	طول	نوع معرف الدائرة	طول	VNI	mod	المنفذ
1 بايت	1 بايت	1 بايت	1 بايت	4 بايت	2 بايت	2 بايت
01	0a	00	08	00002775	*	*



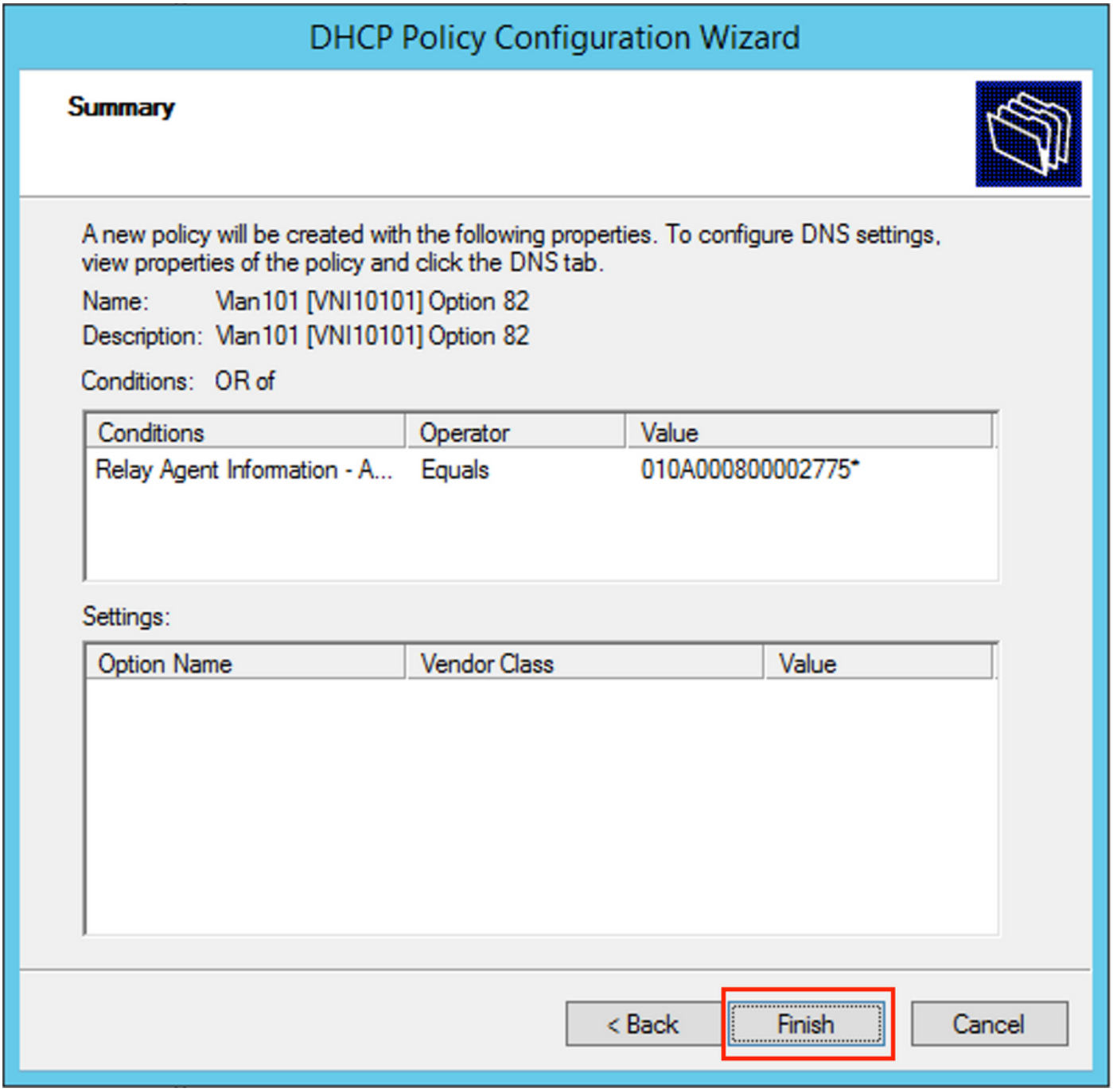
قم بتكوين نطاق IP الذي يتم تخصيص عناوين IP منه. بدون هذا التكوين، لا يمكن تخصيص **النطاق الحالي**.



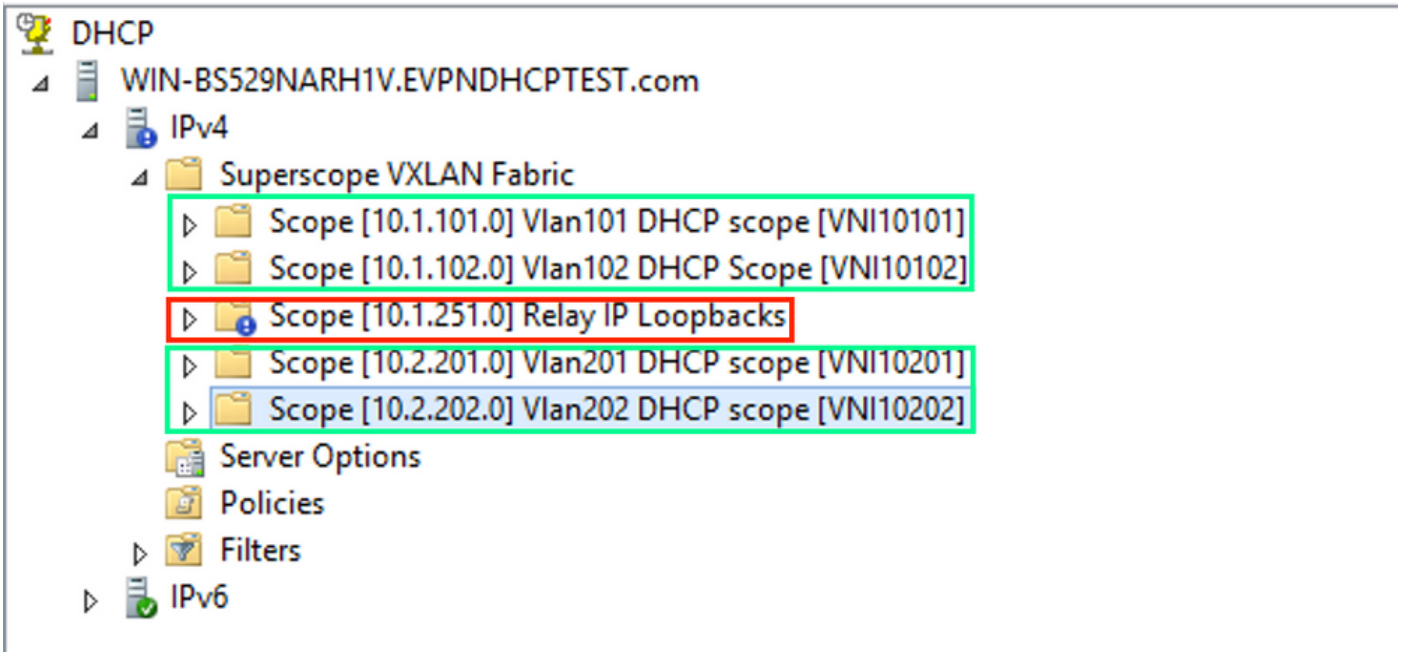
يمكنك أيضا تحديد خيارات DHCP القياسية في هذه المرحلة كما هو موضح في الصورة.



حدد **إنهاء** كما هو موضح في الصورة.



يجب إجراء تكوين مماثل للنطاقات الأخرى كما هو موضح في الصورة.



في هذا السيناريو، يمكنك إستخدام عنوان IP فريد واحد فقط لكل VTEP لأرقام SVIs، وليس إستجاع واحد فريد لكل VNI/SVI لكل VTEP.

تكوين الحول:

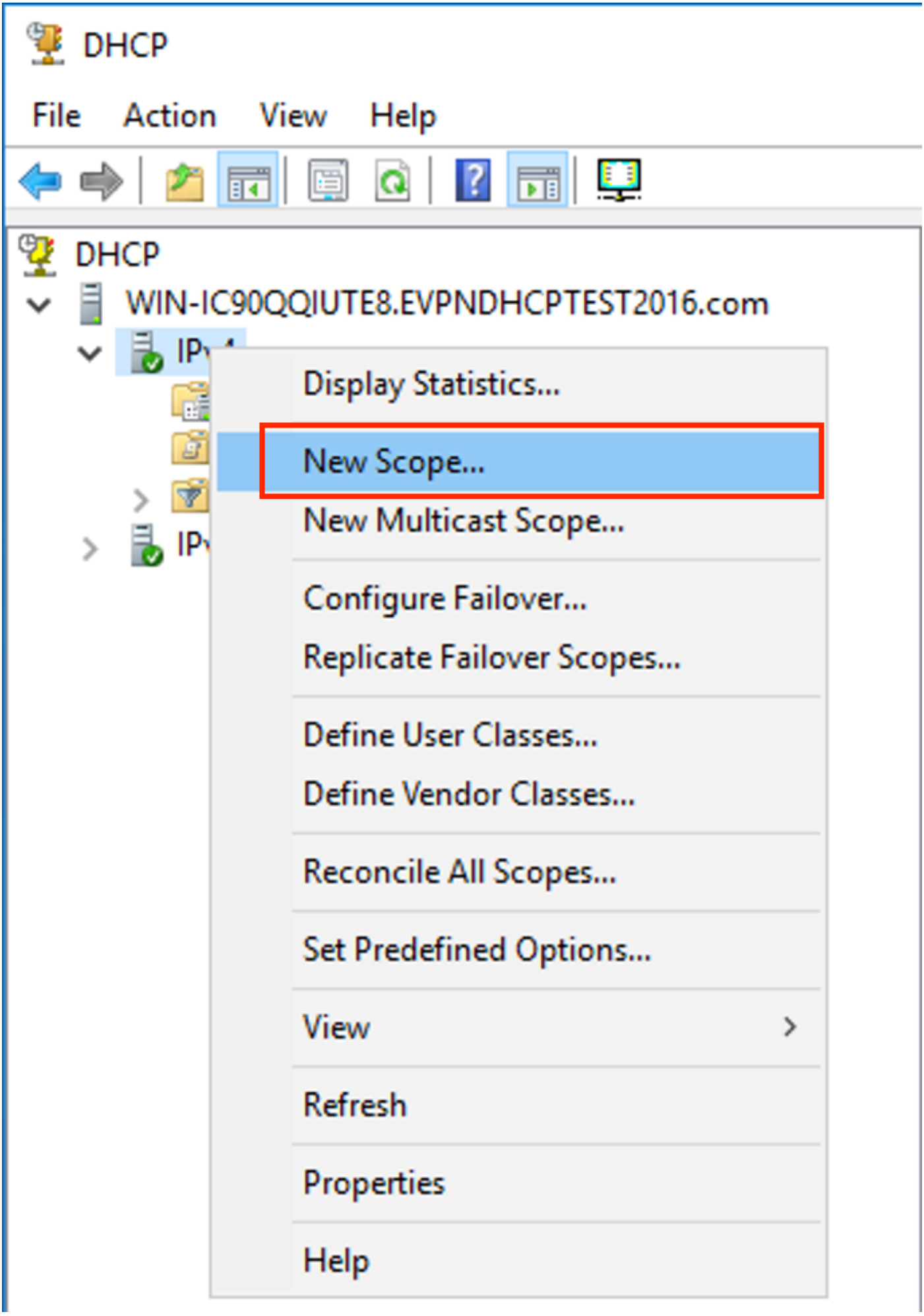
```
ip dhcp relay information option vpn     <<<  adds the VRF name/VPN ID to the option 82
ip dhcp relay information option         <<< enables option 82
!
ip dhcp snooping vlan 101-102,201-202
ip dhcp snooping
!
vlan configuration 101
member evpn-instance 101 vni 10101
!
interface Loopback101
 vrf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

تكوين Windows Server 2016

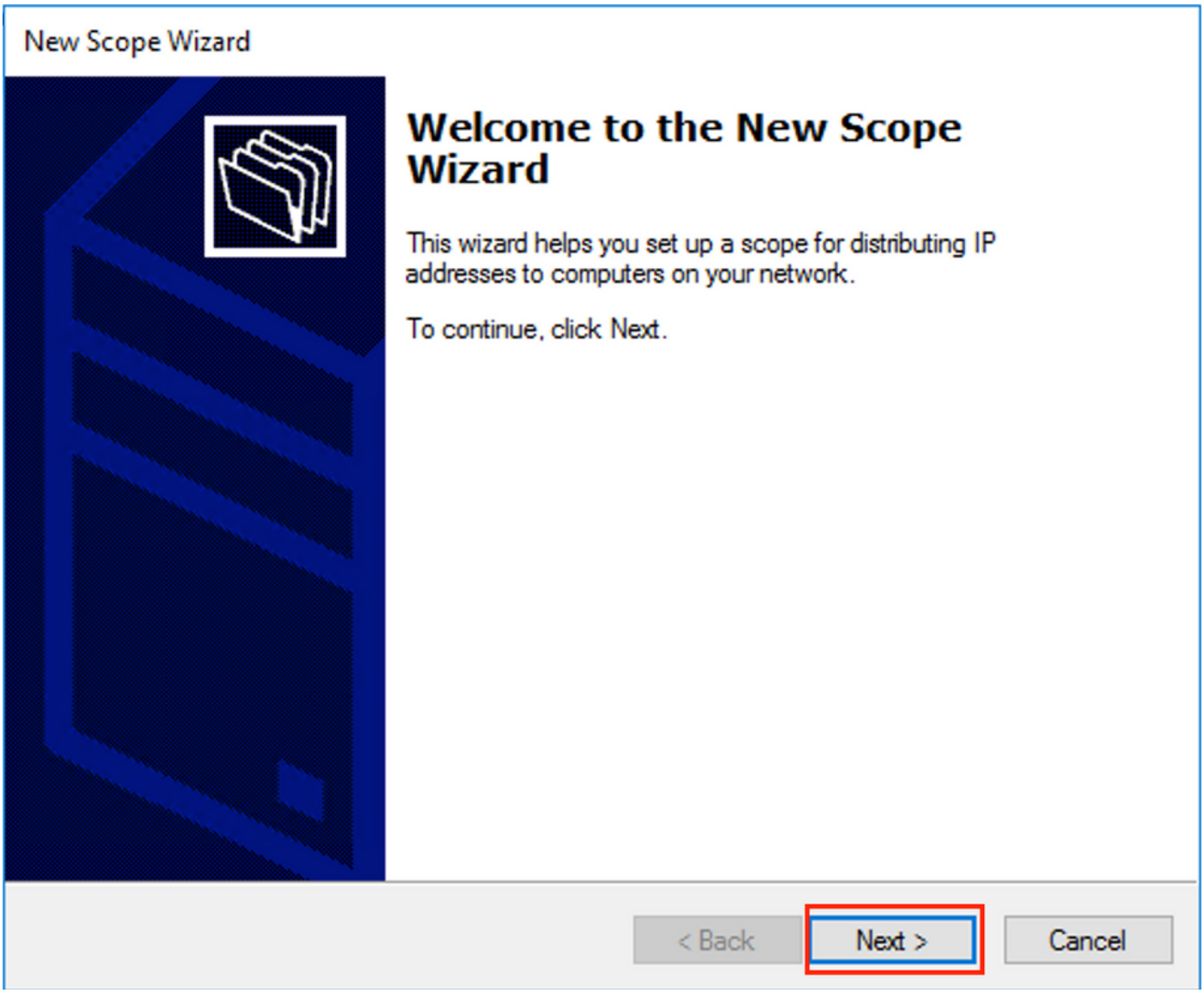
- يدعم Windows Server 2016 الخيار 82 الخيارات الفرعية 5 (Cisco Private 150) "تحديد الارتباط" الذي يعني أنك ال تستخدم عنوان IP ترحيل فريد لتحديد المجموعة. وبدال من ذلك، يتم إستخدام الخيار الفرعي "تحديد الارتباط" الذي يبسط التكوين بشكل كبير.
- سيكون من الأفضل إذا كان لديك بعد تجمع لعناوين IP للترحيل وإال فإن حزمة DHCP ال تطابق أي نطاق والى تتم معالجتها.

يوضح هذا المثال إستخدام خيار "تحديد الارتباط".

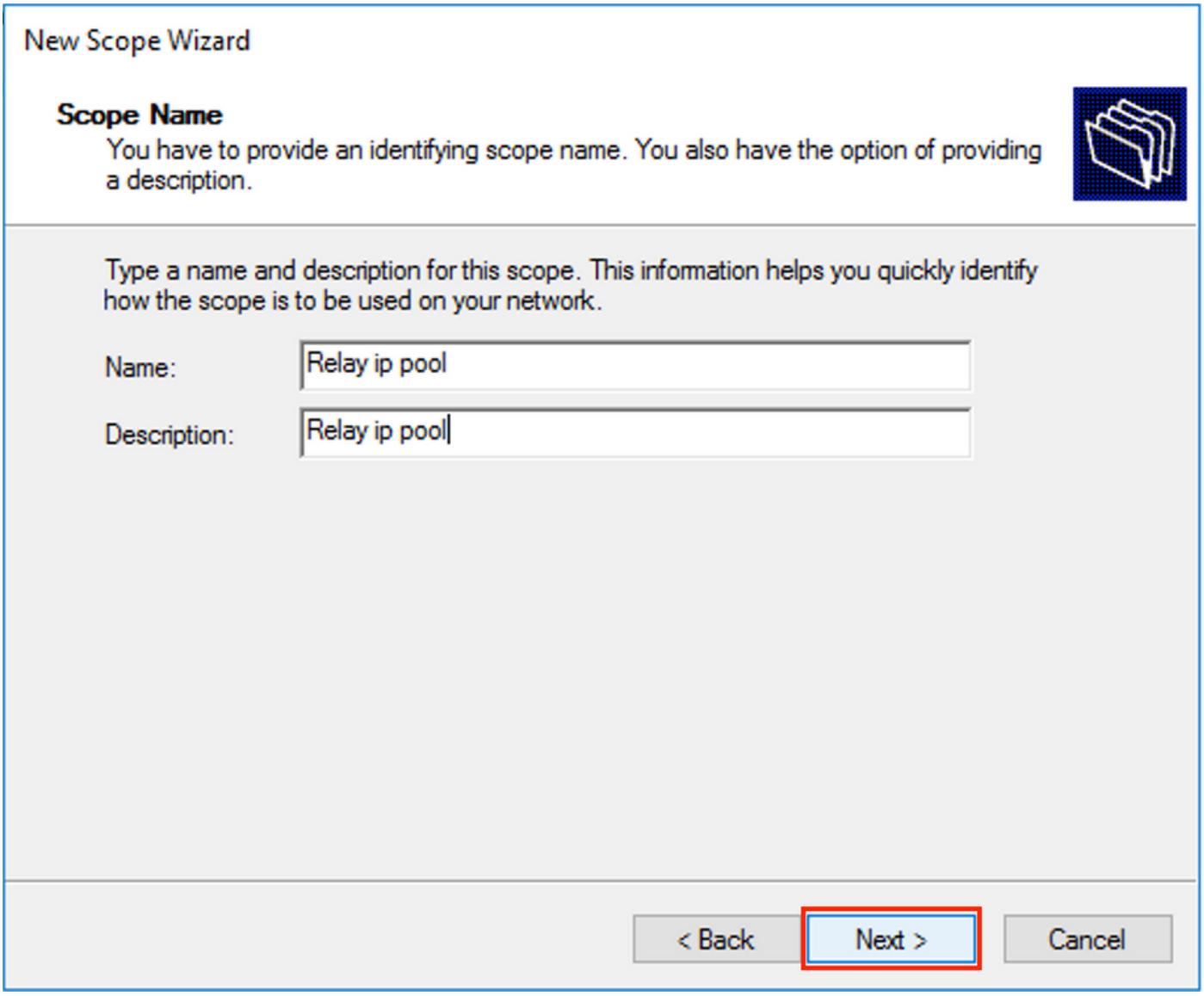
ابدأ تجمع عناوين IP لعناوين IP للترحيل كما هو موضح في الصورة.


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

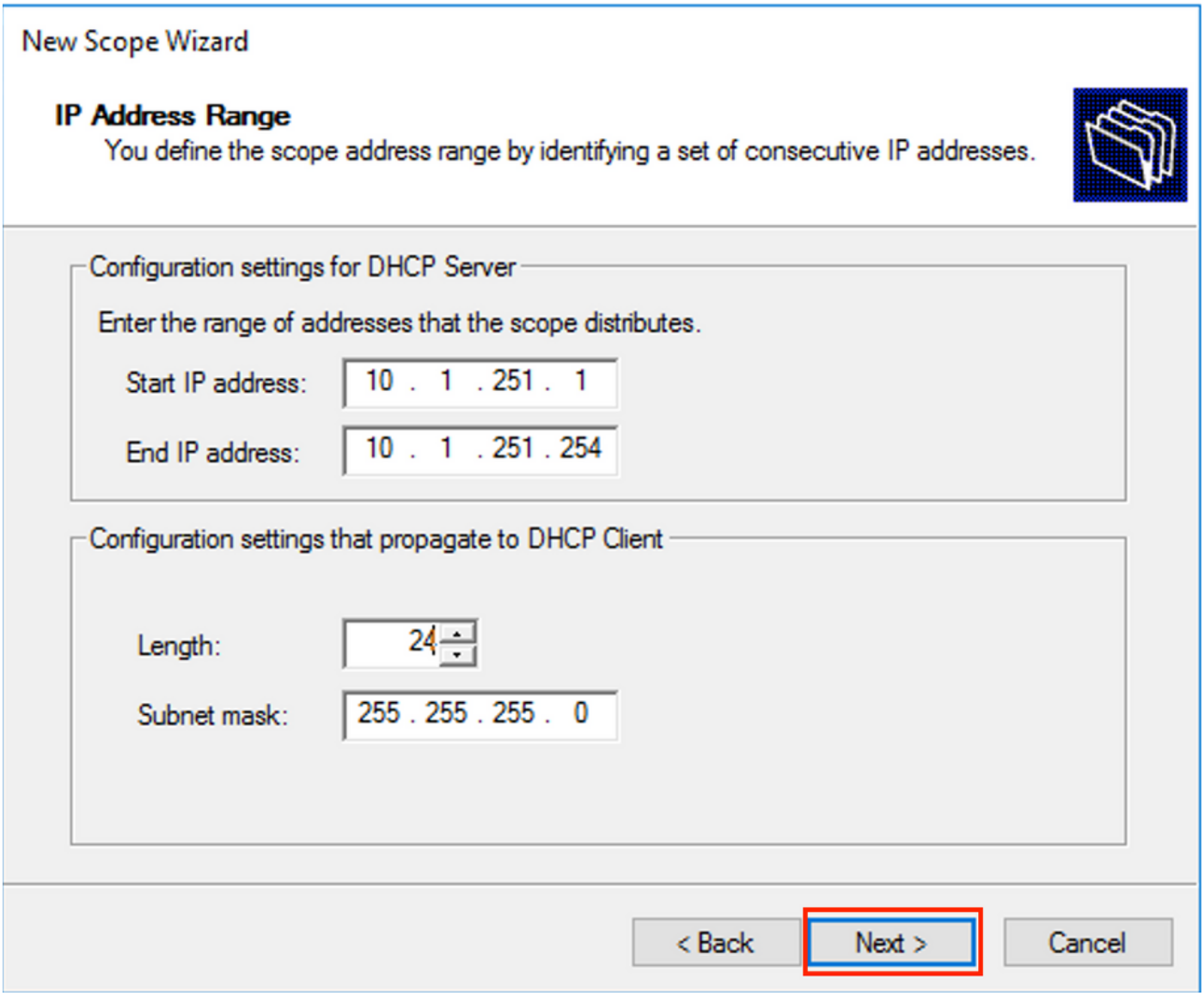
حدد **التالي** كما هو موضح في الصورة.



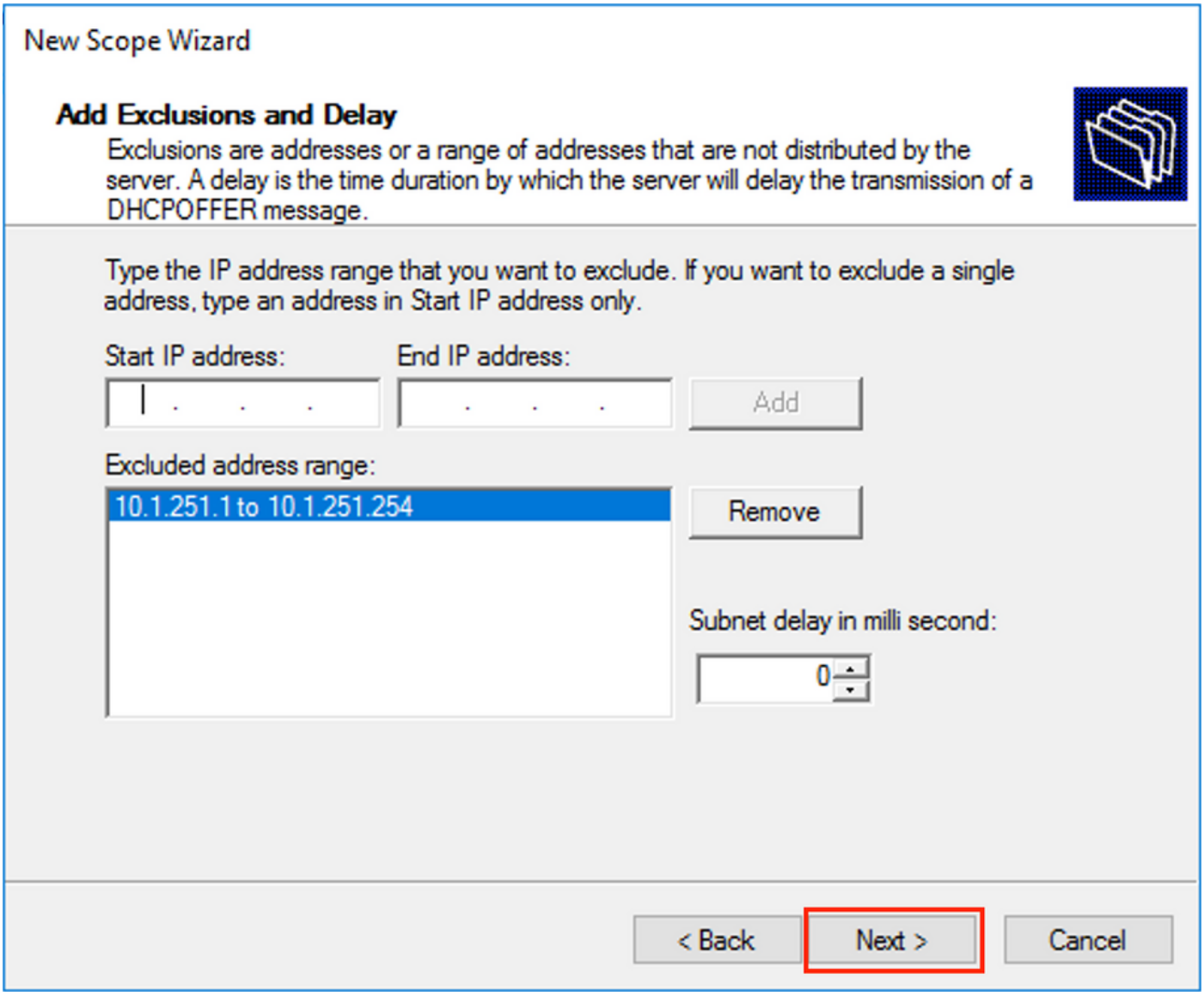
أختر اسم ووصف ذو معنى للنطاق كما هو موضح في الصورة.



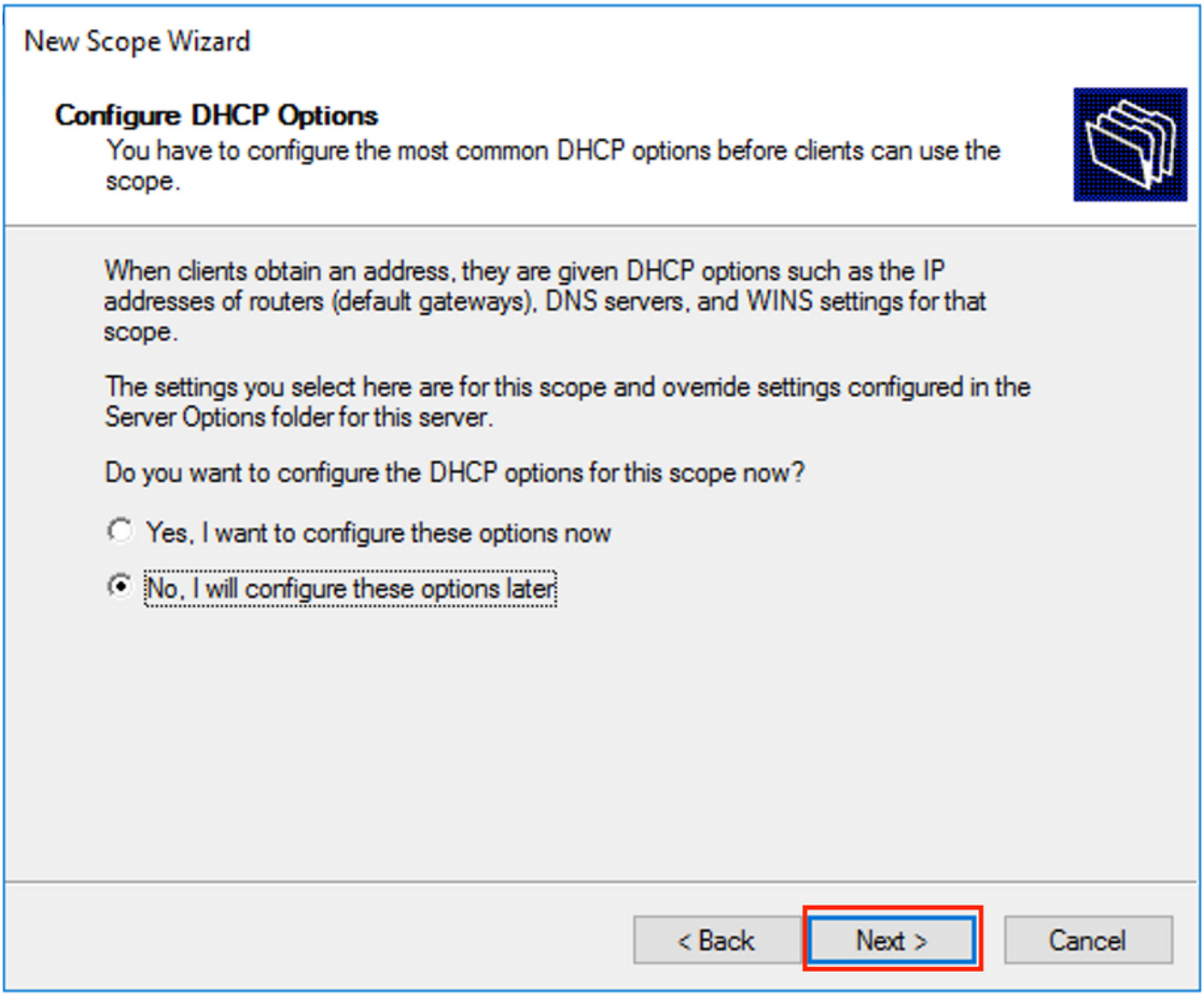
أدخل مساحة عنوان IP التي يتم إستخدامها لترحيل IP كما هو موضح في الصورة.



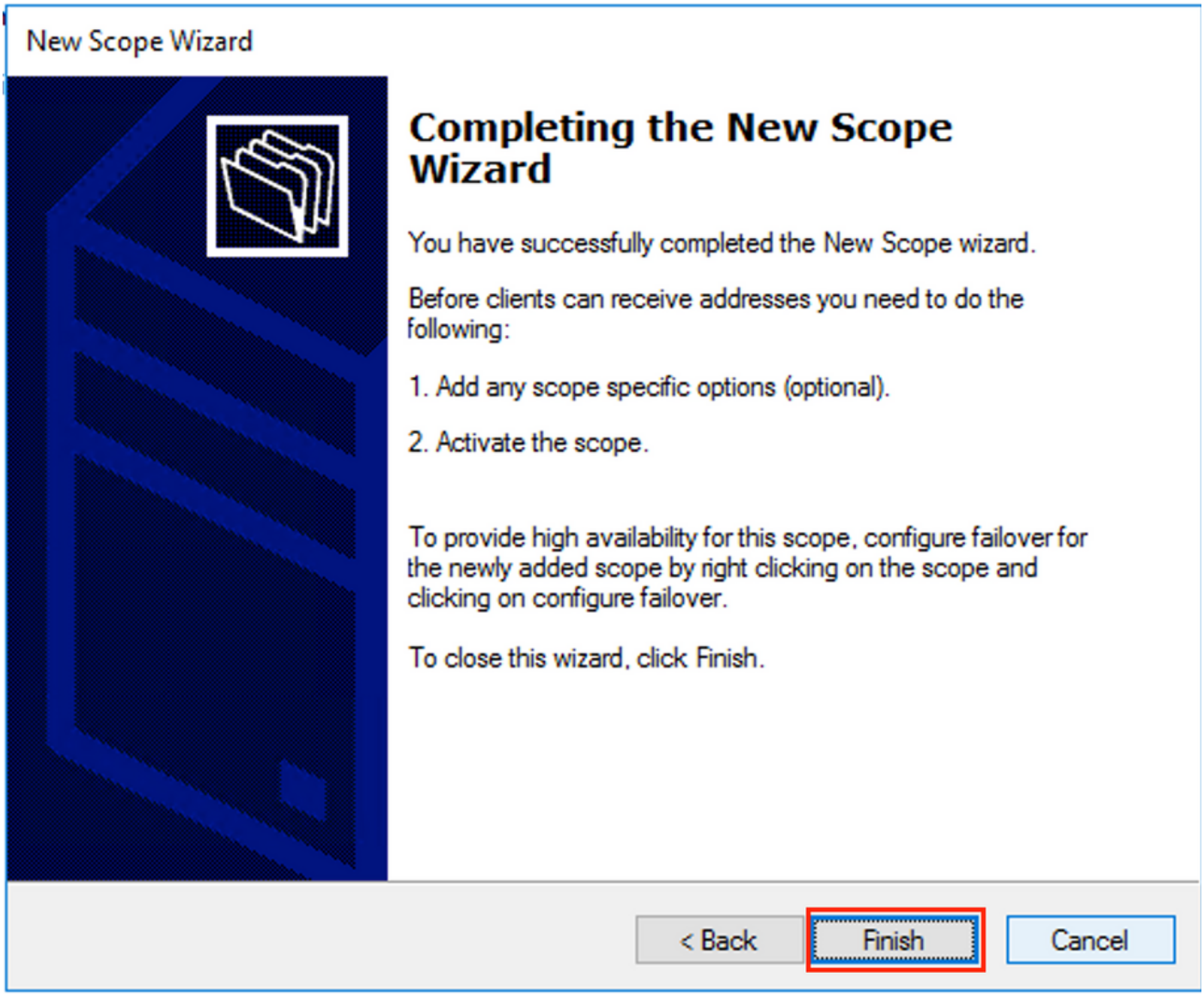
إستثناء كافة النطاقات من النطاق لمنع التخصيص من هذا النطاق كما هو موضح في الصورة.



يمكنك أيضا إختيار معلمات DNS/WINS وغير ذلك للخيار (تم تخطيها في هذا المثال) كما هو موضح في الصورة.

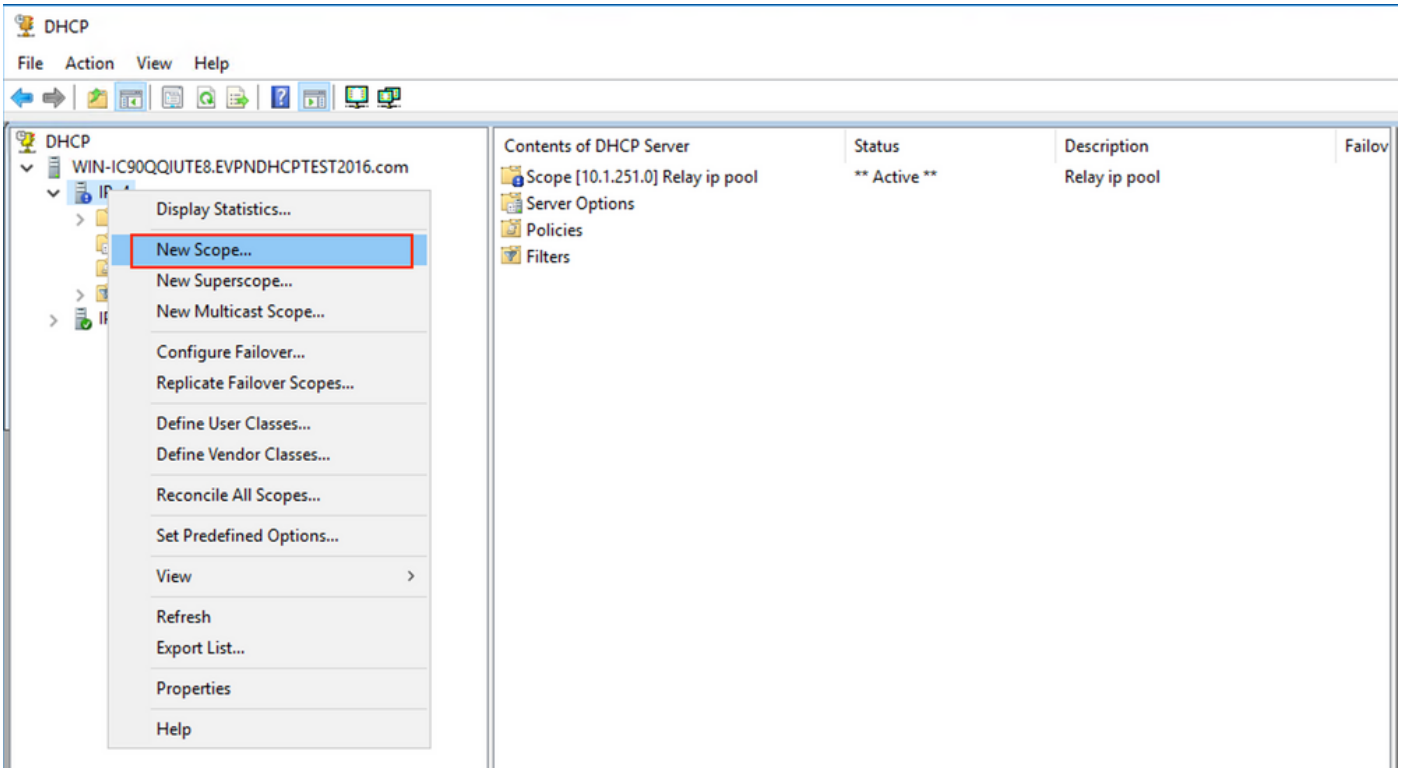


حدد **إنهاء** كما هو موضح في الصورة.

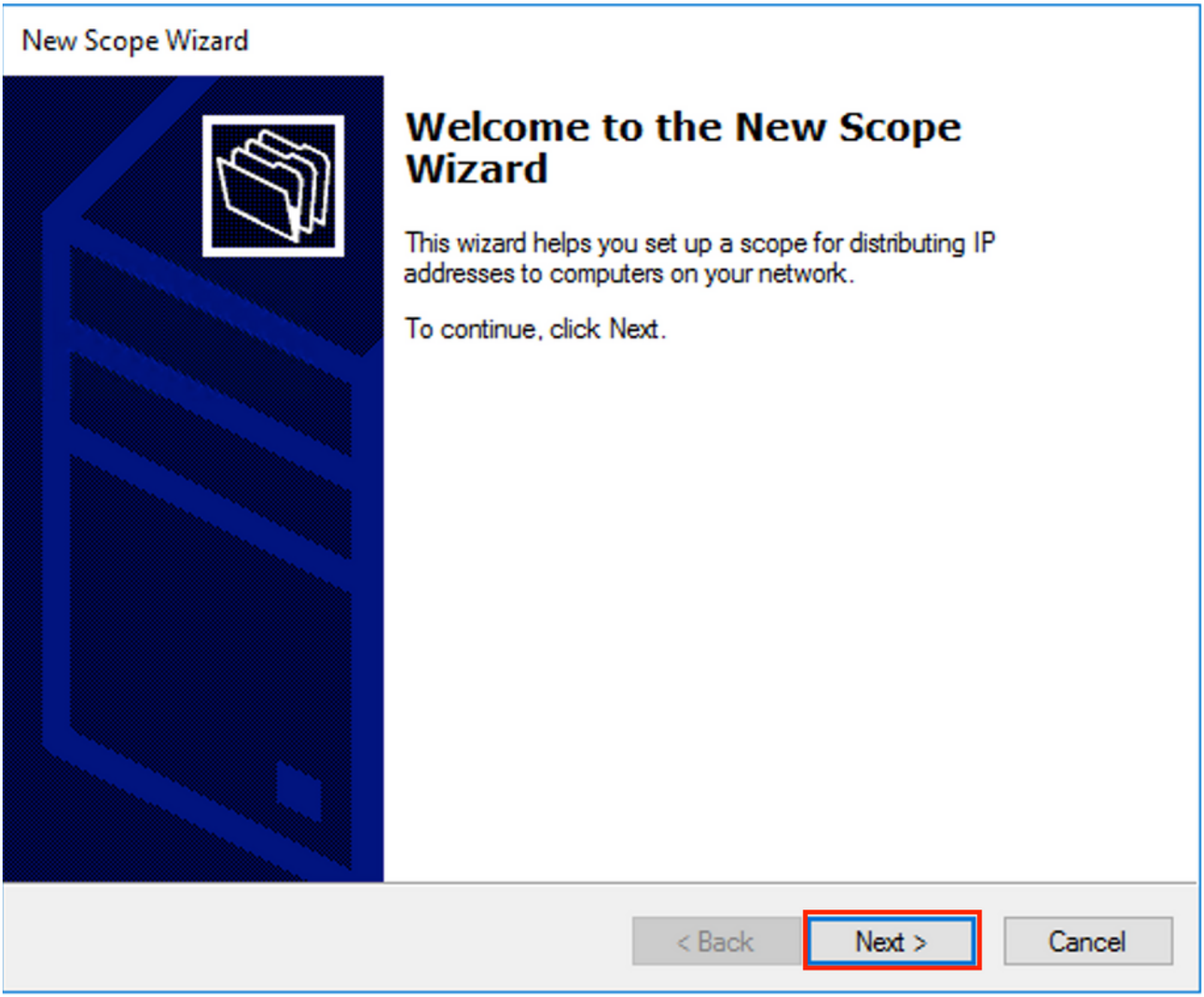


أصبح مجال الارتحال جاهزا الآن.

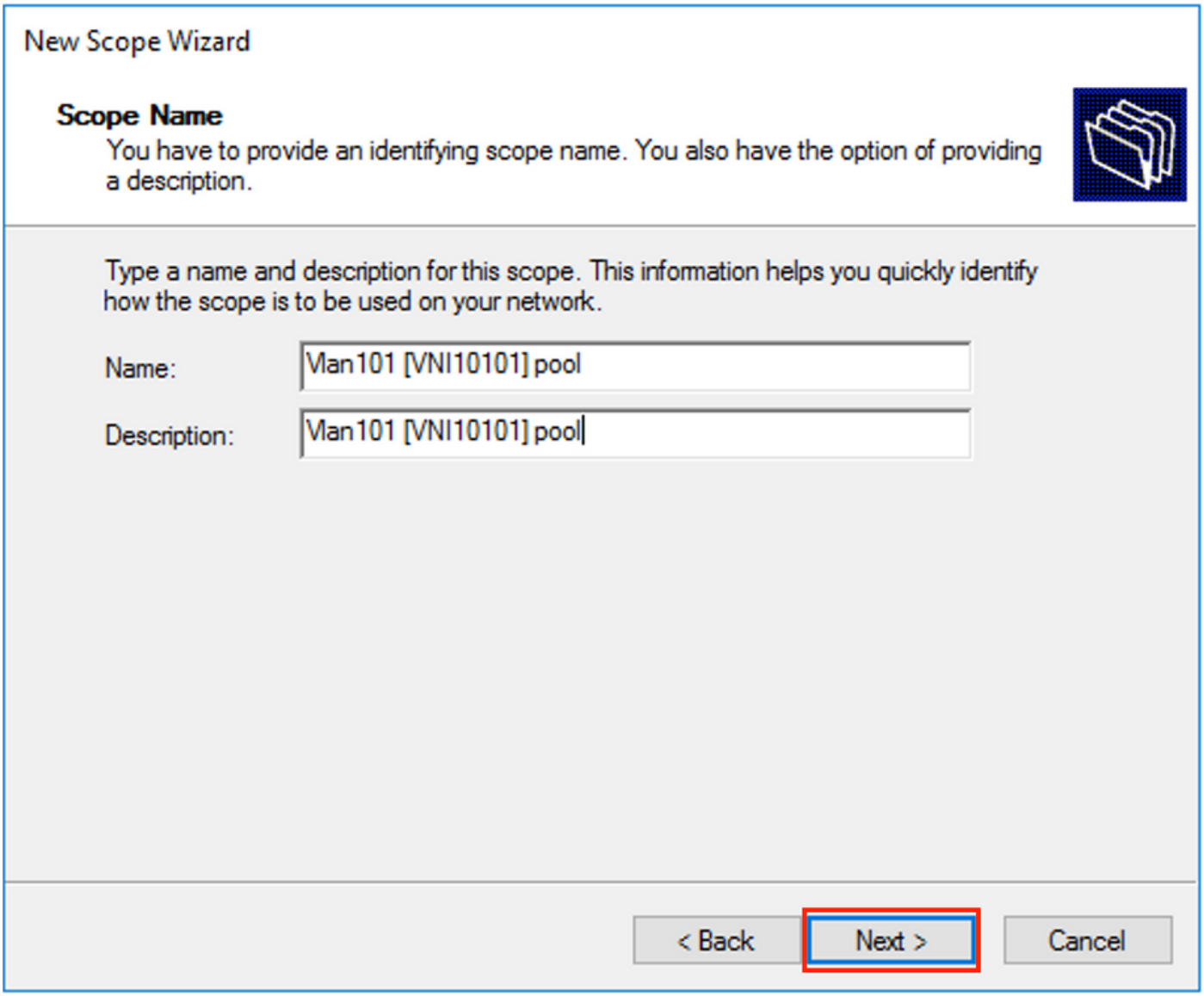
- بعد ذلك، قم بإنشاء التجمع الذي يحصل العملاء من خلاله على عناوين IP.
- انقر بزر الماوس الأيمن واختر **نطاق جديد** كما هو موضح في الصورة.



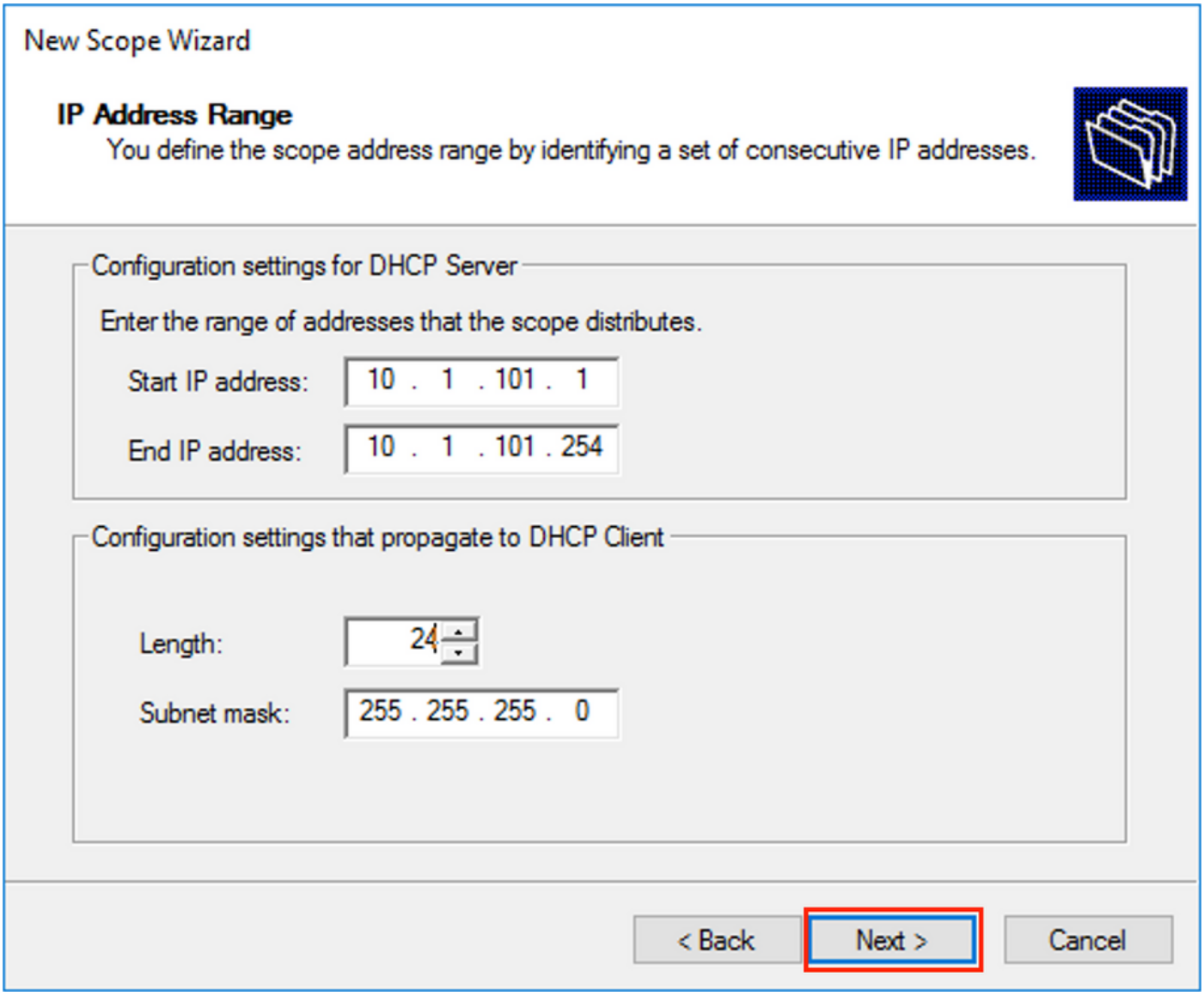
حدد **التالي** كما هو موضح في الصورة.



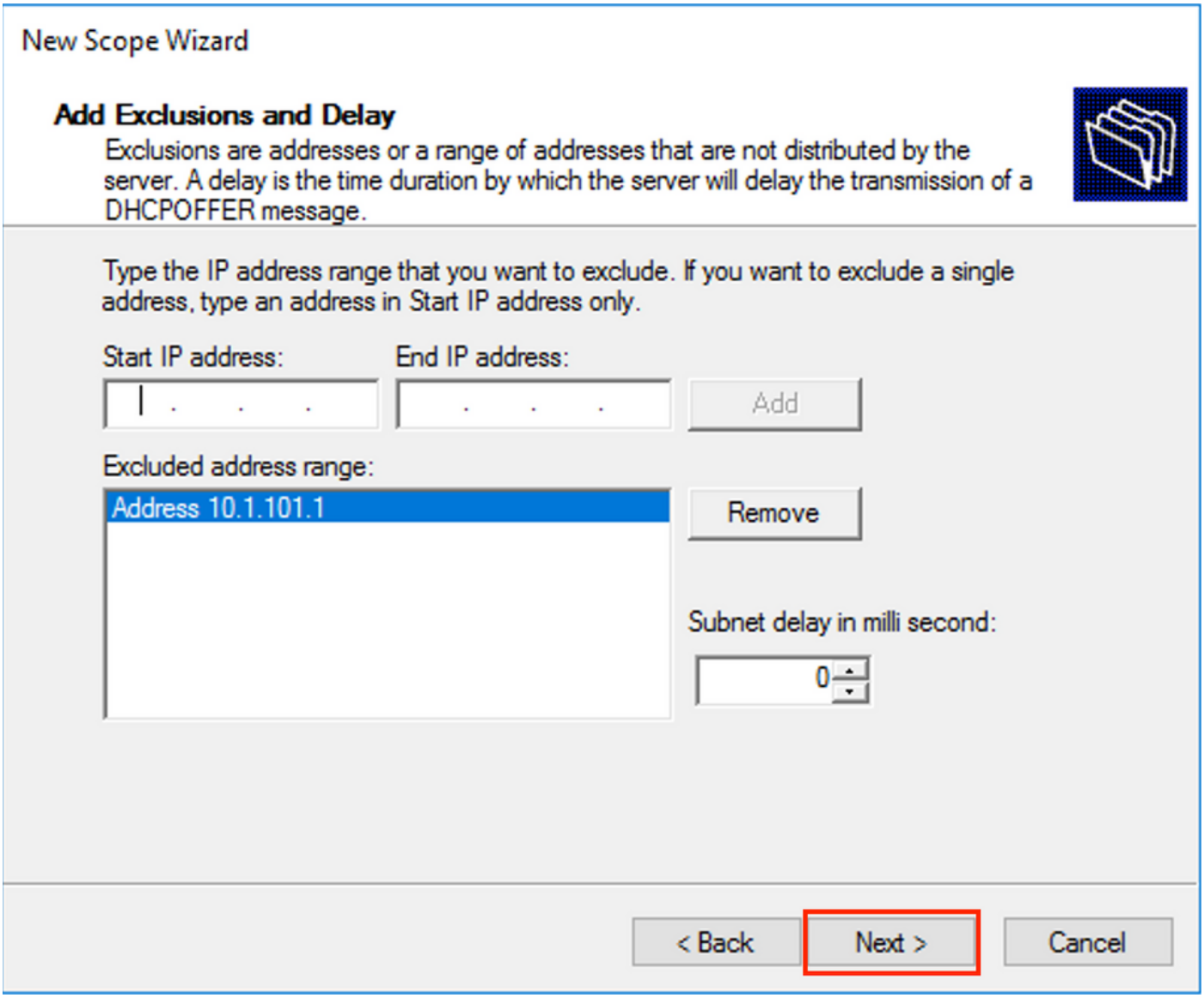
أختر اسم ذو معنى ووصف للتجمع كما هو موضح في الصورة.



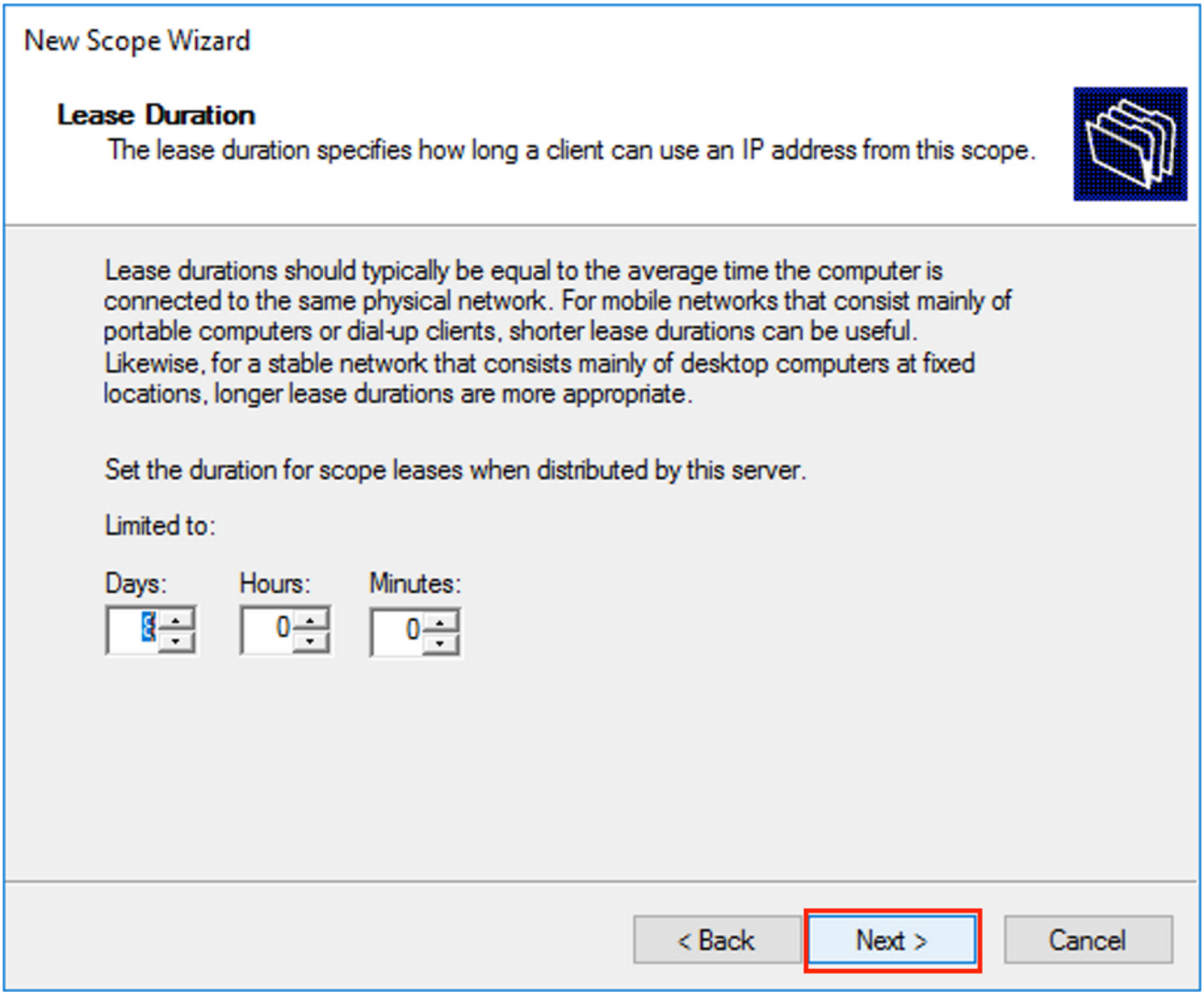
دخلت العنوان مساحة للتخصيص في VLAN101 كما هو موضح في الصورة.



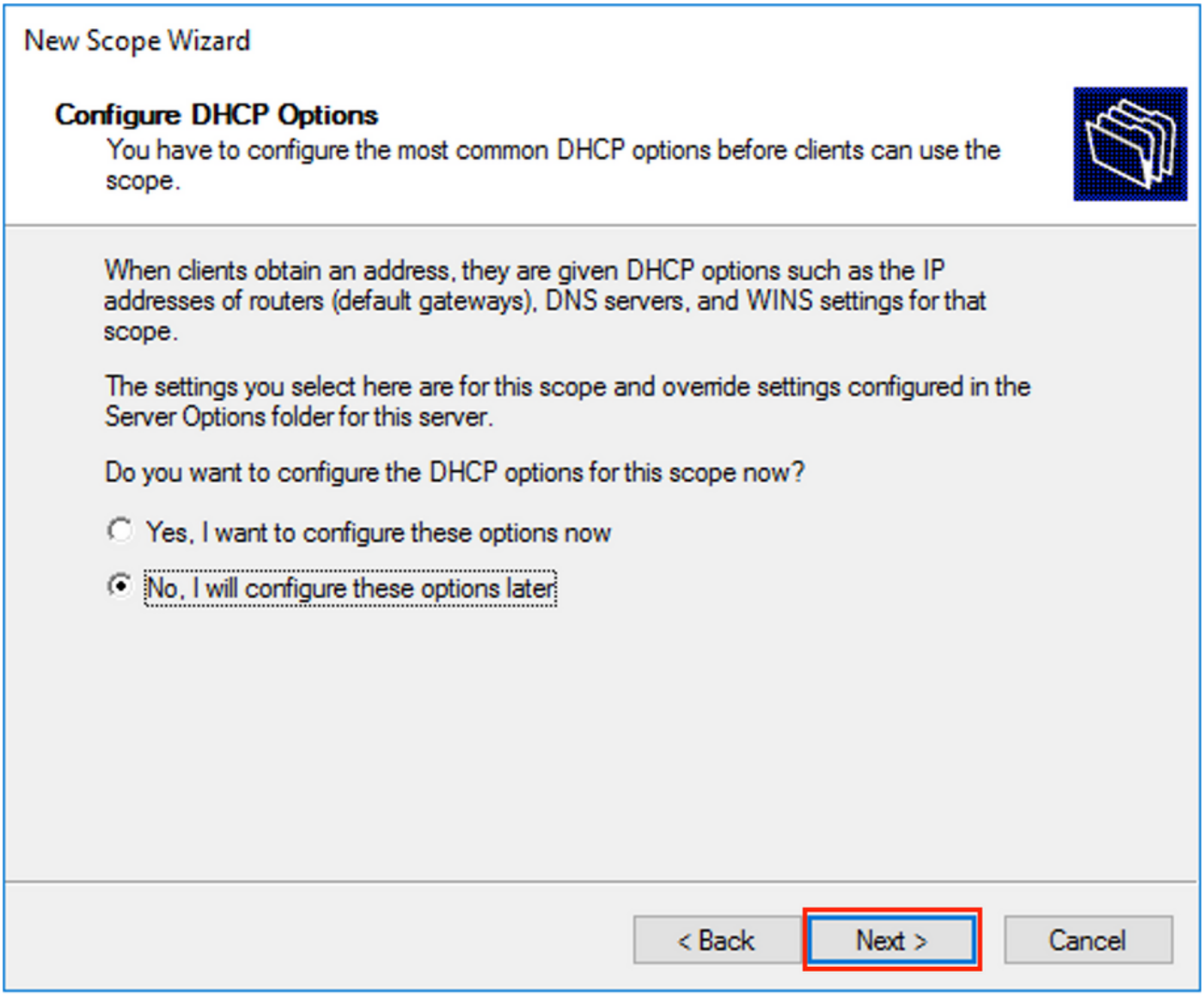
إستثناء عنوان IP للعبارة الافتراضية من النطاق كما هو موضح في الصورة.



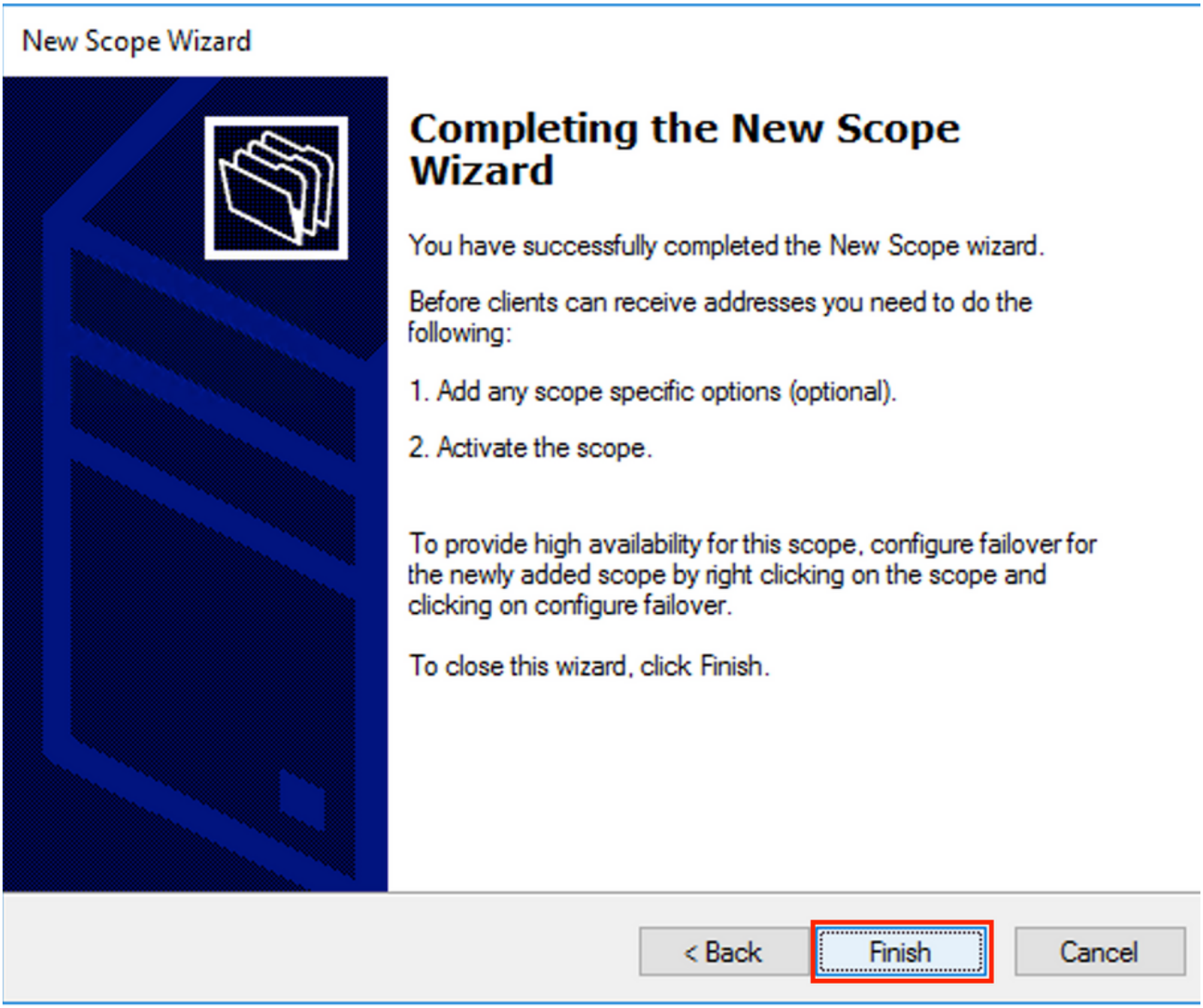
قم بتعيين وقت التأجير كما هو موضح في الصورة.



يمكن تكوين معلمات إضافية مثل DNS/WINS والمزيد (تم تخطيها في هذا المثال) كما هو موضح في الصورة.

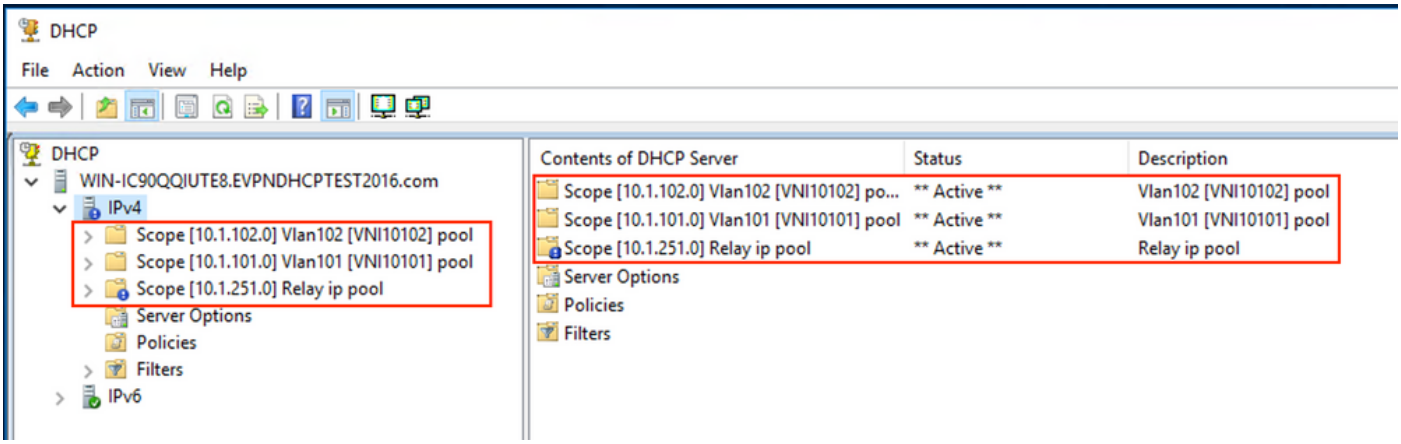


حدد **إنهاء** لإكمال الإعداد كما هو موضح في الصورة.



لم يتم تكوين التجمع لكل عنوان IP لترحيل والا تمت مطابقته في HEX. يستند تحديد التجمع إلى **تحديد إرتباط** الخيار الفرعي.

يمكن إضافة تجمع جديد، والا يلزم تكوين إضافي كما هو موضح في الصورة.



خادم Linux DHCP

راجع تكوين خادم isc-dhcp على Linux.

- إنه يدعم خيار الترحيل 82. هنا، الأمر الأكثر أهمية هو الخيار الفرعي لتحديد الارتباط. ال الزي بإمكانك العمل بمعلومات فرعية دائرة الوكيل والقناع السداسي العشري/التطابق للحقل المحدد (كما تم بالنسبة إلى Win2012). من الناحية العملية، من الأسهل بكثير إستخدام الرقم 82[5] مقارنة بالعمل مباشرة مع معلومات فرعية دائرة الوكيل.
- يتم تكوين الخيار الفرعي لتحديد الارتباط ضمن تعريف الشبكة الفرعية.

في هذا المثال، يتم إستخدام خادم ISC على نظام التشغيل Ubuntu Linux.

قم بتثبيت خادم DHCP:

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

شكلت ال DHCP لدان يحرر **/etc/dhcp/dhcpd.conf**. (يتم إستخدام محرر VIM في المثال)

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

snip التكوين (يتم حذف التكوينات العامة):

```
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;
}
```

تكوين المبدّل

يتم إستعراض السيناريوهات التي يتم دعمها بشكل عام هنا.

1. DHCP زبون في المستأجر VRF والـ DHCP ندال في الطبقة 3 تقصير VRF
2. DHCP زبون في المستأجر VRF والـ DHCP ندال في ال نفس مستأجر VRF
3. عميل DHCP في VRF المستأجر وخادم DHCP في VRF مستأجر مختلف
4. عميل DHCP في VRF المستأجر وخادم DHCP في VRF غير افتراضي غير VXLAN

لأي من هذه السيناريوهات، يلزم تكوين ترحيل DHCP على جانب المحول.

الـ DHCP تشكيل ل بسيط خيار رقم 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]
```

بشكل افتراضي، الخيار 82 خيار فرعي **تحديد الارتباط وتجاوز معرف الخادم** هما cisco خاص بشكل افتراضي (150 و 152 على التوالي).

```
▼ 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)
```

إذا لم **يفه** خادم DHCP خيارات Cisco الخاصة لأي سبب، فيمكنك تغييرها إلى الخيار القياسي.

```
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
```

يجب تمكين التطفل على بروتوكول DHCP لشبكات VLAN الضرورية.

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

أنت يستطيع استعملت الـ DHCP-relay source-interface تشكيل شامل.

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

أو يمكنك تكوين الواجهة التكوين العام (تكوين الواجهة لكل واجهة).

```
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
```

تحقق من وجود عنوان IP لترحيل IP وخادم DHCP الاتصال IP في الكل الاتجاهين.

```
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
```

رمز أذه ل راي خ 3 تنك عيطتسي وه .DHCP خادم ناونع نيوكت متي ،ةهجاولا نيوكت نمضم
العميلاو لخادم في نفس 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
```

العميلاو لخادم في VRFs مختلفة (عميل باألخضر، خادم باألحمر في هذا المثال):

```
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
```

العميل في VRF والخادم في جدول التوجيه العام (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
```

الآن، تمت مراجعة تكوين نموذجي لجميع الخيارات هنا.

VRF تصيرق 3 ةقبطلا في الدان DHCP لاو VRF رأجتسملا في نبوز DHCP

في هذه الحالة، Lo0 في GRT وهو مصدر ترحيل DHCP. تم تكوين ترحيل DHCP بشكل عام + لبعض الواجهات.

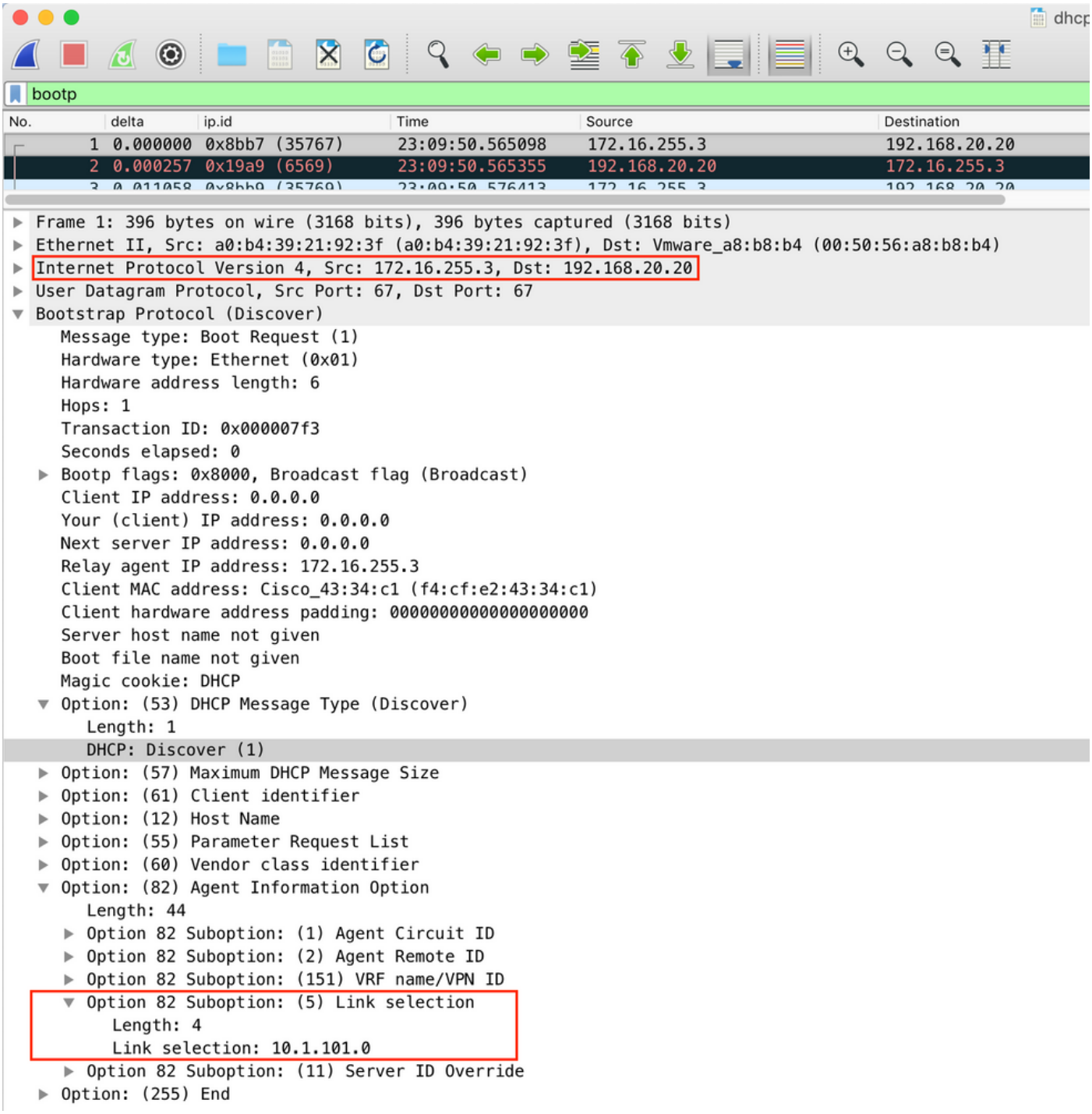
على سبيل المثال، بالنسبة إلى الرأمز vlan101، تم فقد "ip dhcp relay source-interface loopback0"، ولكنه يستخدم التكوين العام.

```
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
```

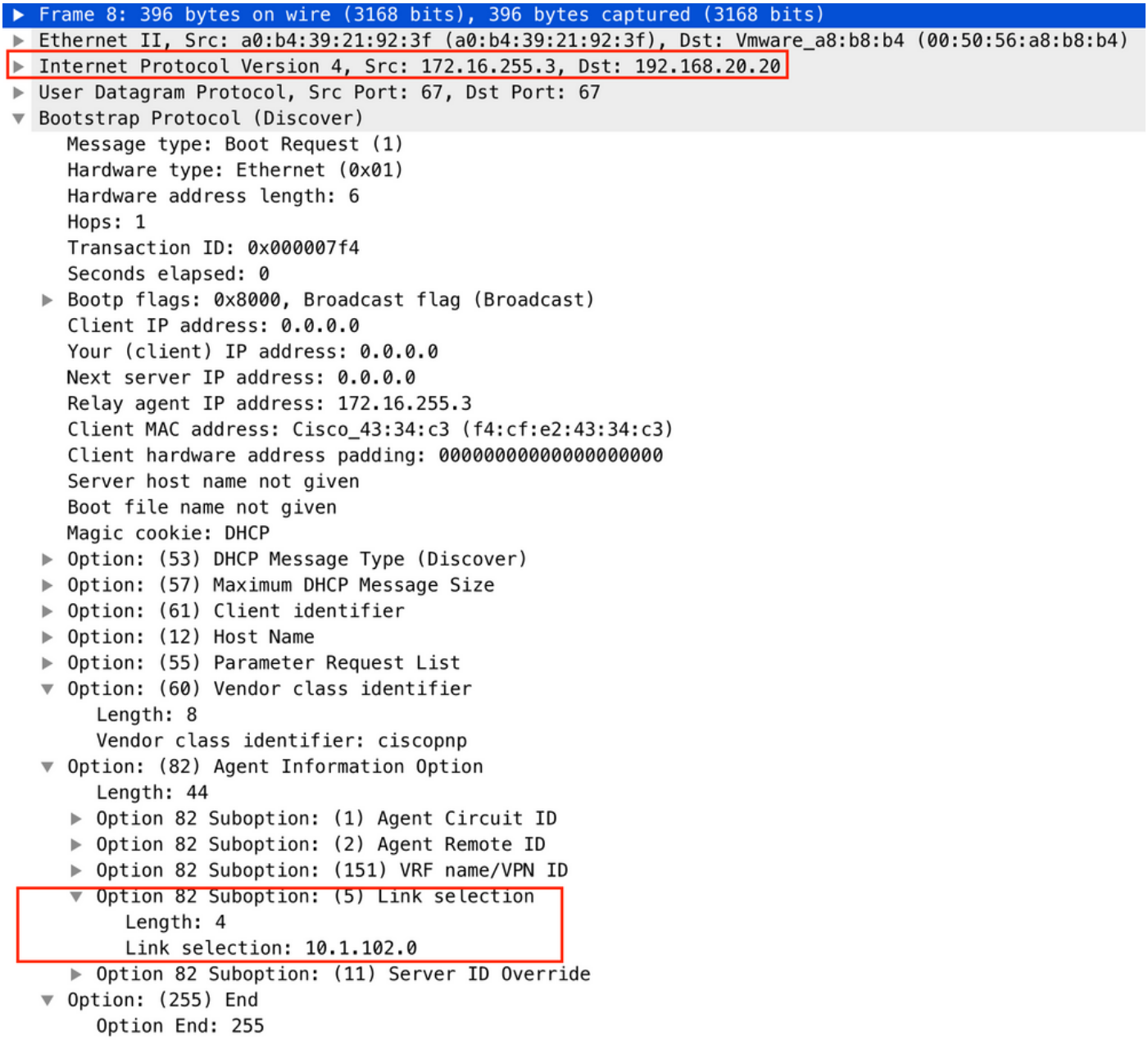
```
ip dhcp relay information option                          <<< enables DHCP option 82
ip dhcp compatibility suboption link-selection standard  <<< switch to standard option 82[5]
ip dhcp compatibility suboption server-override standard <<< switch to standard option 82[11]
ip dhcp snooping vlan 101-102,201-202                     <<< 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
```

ونتيجة لذلك، يتم إرسال حزمة ترحيل DHCP عبر GRT باستخدام SRC IP/DST IP نفسه، ولكن باستخدام خيارات فرعية مختلفة.

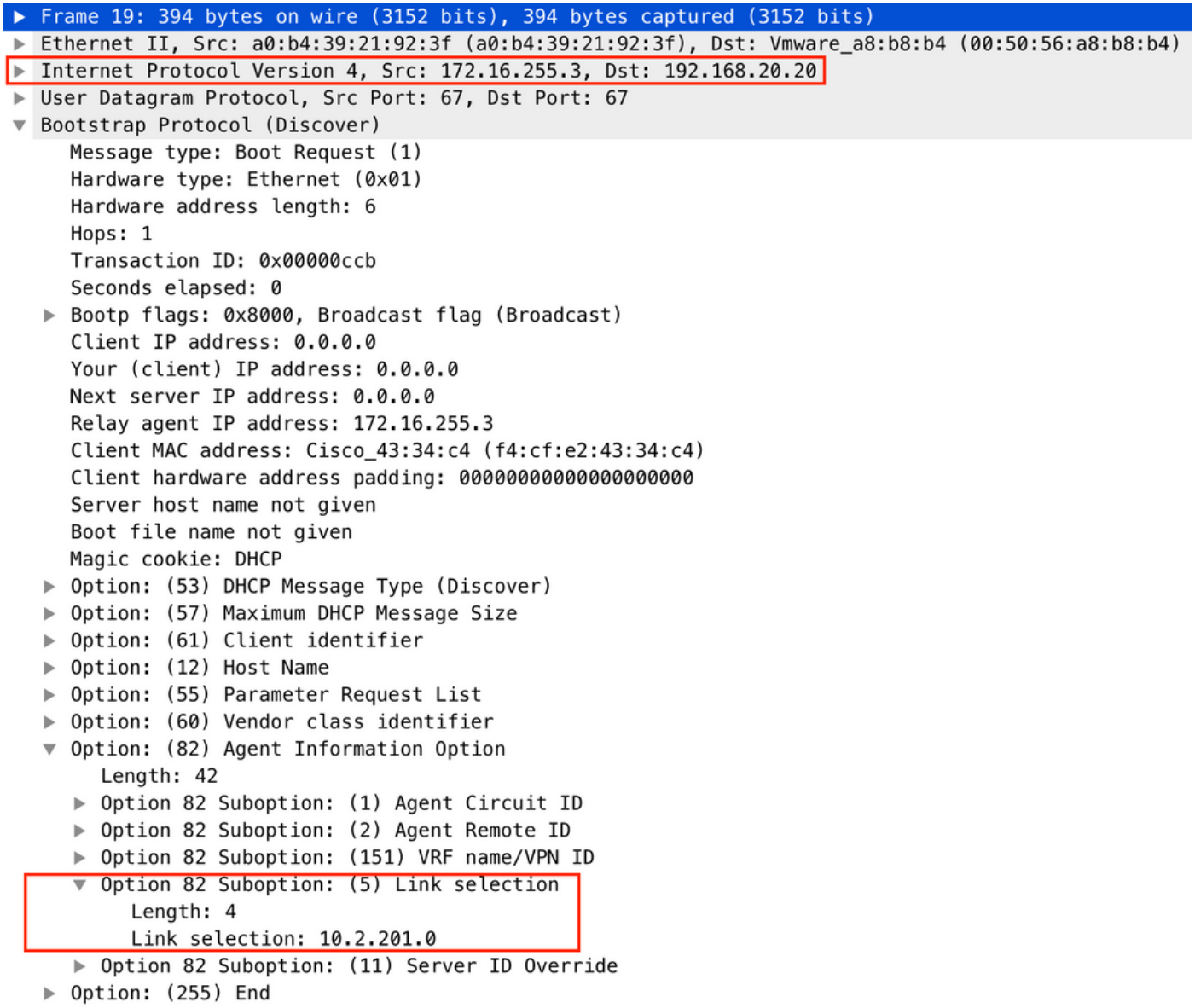
ل VLAN101:


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

- J VLAN102:



ل VLAN201 (والذي يكون في VRF أحمر، ليس أخضر مثل VLANs 101 و 102):



تم التقاط الحزمة على العامود الرئيسي-01 من الواجهة إلى الورقة-01:

```
Spine-01#sh mon cap TAC buff br | i DHCP
5401 4.402431 172.16.255.3 b^F^R 192.168.20.20 DHCP 396 DHCP Discover - Transaction ID 0x1feb
5403 4.403134 192.168.20.20 b^F^R 172.16.255.3 DHCP 362 DHCP Offer - Transaction ID 0x1feb
5416 4.418117 172.16.255.3 b^F^R 192.168.20.20 DHCP 414 DHCP Request - Transaction ID 0x1feb
5418 4.418608 192.168.20.20 b^F^R 172.16.255.3 DHCP 362 DHCP ACK - Transaction ID 0x1feb
```

لا DHCP ربط في لب ip دون أي VXLAN عملية كبسلة:

```
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...>
```

فائدة كبيرة من هذا النهج هو أنه يمكنك إستخدام نفس عنوان IP للترحيل لشبكات VRF المستأجر المختلفة بدون تسرب المسار بين شبكات VRF المختلفة وشبكات VRF العالمية.

DHCP زبون و DHCP لدان في ال نفسه مستأجر VRF

في هذه الحالة، من المنطقي أن يكون لديك عنوان IP للترحيل في VRF المستأجر.

تكوين المحول:

```
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
```

ل 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
```

J VLAN102:

```
▶ Frame 5: 396 bytes on wire (3168 bits), 396 bytes captured (3168 bits)
▶ Ethernet II, Src: a0:b4:39:21:92:3f (a0:b4:39:21:92:3f), Dst: Vmware_a8:b8:b4 (00:50:56:a8:b8:b4)
▶ Internet Protocol Version 4, Src: 10.1.251.1, Dst: 192.168.20.20
▶ User Datagram Protocol, Src Port: 67, Dst Port: 67
▼ Bootstrap Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 1
    Transaction ID: 0x000016cd
    Seconds elapsed: 0
  ▶ Bootp flags: 0x8000, Broadcast flag (Broadcast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 10.1.251.1
    Client MAC address: Cisco_43:34:c3 (f4:cf:e2:43:34:c3)
    Client hardware address padding: 00000000000000000000
    Server host name not given
    Boot file name not given
    Magic cookie: DHCP
  ▶ Option: (53) DHCP Message Type (Discover)
  ▶ Option: (57) Maximum DHCP Message Size
  ▶ Option: (61) Client identifier
  ▶ Option: (12) Host Name
  ▶ Option: (55) Parameter Request List
  ▼ Option: (60) Vendor class identifier
      Length: 8
      Vendor class identifier: ciscopnp
  ▼ Option: (82) Agent Information Option
      Length: 44
    ▶ Option 82 Suboption: (1) Agent Circuit ID
    ▶ Option 82 Suboption: (2) Agent Remote ID
    ▶ Option 82 Suboption: (151) VRF name/VPN ID
    ▼ Option 82 Suboption: (5) Link selection
        Length: 4
        Link selection: 10.1.102.0
    ▶ Option 82 Suboption: (11) Server ID Override
  ▼ Option: (255) End
      Option End: 255
```

التقاط حزمة من واجهة SPINE-01 إلى 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
```

تتضمن حزمة DHCP في المركز تضمين VXLAN:

```
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 زبون في واحد مستأجر VRF و DHCP دان ل في آخر مستأجر VRF

في هذا المثال، يكون العميل باللون الأحمر VRF والخادم باألخضر VRF.

لديك خياران:

- الاحتفاظ ب IP للترحيل في VRF العميل وتكوين تسريب المسار الذي يضيف مزيدا من التعقيد
- الاحتفاظ ب IP للترحيل في VRF الخاص بالخادم (يشبه ما قمت به ل GRT في الحالة الأولى)

من الأبسط إختيار النهج الثاني نظرا لأن الكثير من بروتوكولات تكرار الخطوة الأولى من تسريب المسار إلى حاجة ولا مجموعة العملاء الخاصة (VRFS).

تكوين المحول:

```
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
```

ل VLAN201:

```
▶ 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
```

التقاط الحزمة على واجهة SPINE-01 إلى Leaf-01:

```
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
```

في هذا مثال، الربط في لب VXLAN يغلف.

```
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...>
```

VXLAN VRF غير آخر في لدان DHCP و VRF مستأجر واحد في زبون DHCP

هذه الحالة مشابهة جدا للحالة الأخيرة. الفرق الرئيسي هو أن الجزم لا تحتوي على تضمين VXLAN - IP نقي أو أي شيء آخر (MPLS/GRE/وما إلى ذلك)، ولكنها نفسها من منظور التكوين.

في هذا المثال، يكون العميل باللون الأحمر VRF والخادم باألخضر VRF.

لديك خياران:

- يوجد بروتوكول Relay IP في ملف VRF الخاص بالعميل ويقوم بتكوين تسجيل المسار الذي يضيف مزيدا من التعقيد
- يوجد Relay IP في VRF الخاص بالخادم (مماثل لما تم القيام به ل GRT في الحالة الأولى)

من الأبسط إختيار النهج الثاني نظرا لأن الكثير من بروتوكولات تكرار الخطوة الأولى من (VRFS) الخاصة بالعمالء مدعومة ولا حاجة إلى تسريب المسار.

تكوين الموجل:

```
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
```

معلومات ذات صلة

- المعيار RFC 3046
- المعيار RFC 3527
- https://docs.microsoft.com

- الدعم التقني والمستندات - Cisco Systems

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).