

IOS/CCP: Dynamisches Multipoint-VPN mit Konfigurationsbeispiel für Cisco Configuration Professional

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Spoke-Konfiguration mit Cisco CP](#)

[CLI-Konfiguration für Spoke](#)

[Hub-Konfiguration mit Cisco CP](#)

[CLI-Konfiguration für Hub](#)

[Bearbeiten der DMVPN-Konfiguration mithilfe von CCP](#)

[Weitere Informationen](#)

[Überprüfung](#)

[Zugehörige Informationen](#)

[Einleitung](#)

Dieses Dokument enthält eine Beispielkonfiguration für einen DMVPN-Tunnel (Dynamic Multipoint VPN) zwischen Hub-and-Spoke-Routern mithilfe von Cisco Configuration Professional (Cisco CP). Dynamic Multipoint VPN ist eine Technologie, die verschiedene Konzepte wie GRE, IPSec-Verschlüsselung, NHRP und Routing integriert, um eine fortschrittliche Lösung bereitzustellen, die es Endbenutzern ermöglicht, effektiv über die dynamisch erstellten Spoke-to-Spoke-IPSec-Tunnel zu kommunizieren.

[Voraussetzungen](#)

[Anforderungen](#)

Für eine optimale DMVPN-Funktionalität wird empfohlen, die Cisco IOS® Software Release 12.4 Mainline, 12.4T und höher auszuführen.

[Verwendete Komponenten](#)

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

- Cisco IOS Router der Serie 3800 mit Softwareversion 12.4 (22)
- Cisco IOS Router der Serie 1800 mit Softwareversion 12.3 (8)
- Cisco Configuration Professional Version 2.5

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 Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

[Konventionen](#)

Weitere Informationen zu Dokumentkonventionen finden Sie in den [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

[Hintergrundinformationen](#)

Dieses Dokument enthält Informationen zum Konfigurieren eines Routers als Spoke-Router und eines anderen Routers als Hub mit Cisco CP. Die erste Spoke-Konfiguration wird angezeigt, später wird jedoch im Dokument die Hub-bezogene Konfiguration detailliert dargestellt, um ein besseres Verständnis zu ermöglichen. Andere Stationen können ebenfalls mit dem gleichen Ansatz für die Verbindung mit dem Hub konfiguriert werden. Im aktuellen Szenario werden folgende Parameter verwendet:

- Öffentliches Hub-Router-Netzwerk - 209.165.201.0
- Tunnel Network - 192.168.10.0
- Verwendetes Routing-Protokoll - OSPF

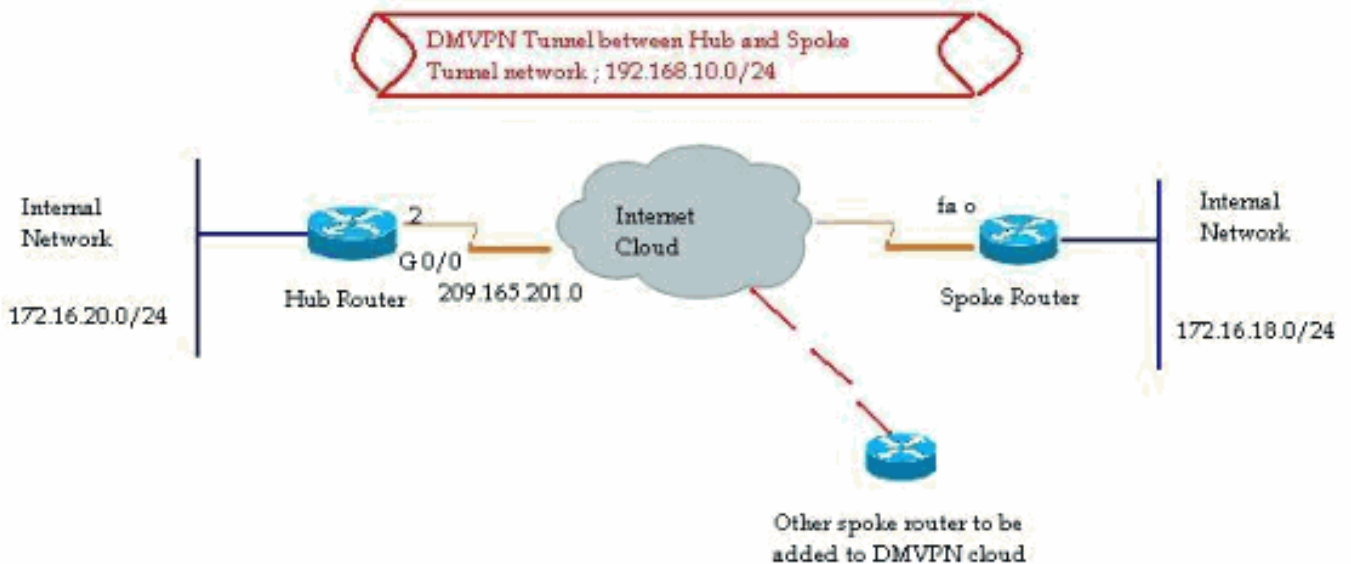
[Konfigurieren](#)

In diesem Abschnitt erfahren Sie, wie Sie die in diesem Dokument beschriebenen Funktionen konfigurieren können.

Hinweis: Verwenden Sie das [Command Lookup Tool](#) (nur [registrierte](#) Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

[Netzwerkdiagramm](#)

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Spoke-Konfiguration mit Cisco CP

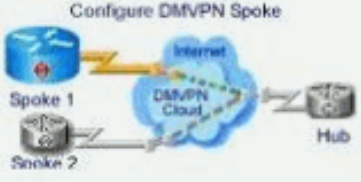
In diesem Abschnitt wird die Konfiguration eines Routers als Spoke mit dem Schritt-für-Schritt-DMVPN-Assistenten im Cisco Configuration Professional beschrieben.

1. Um die Cisco CP-Anwendung zu starten und den DMVPN-Assistenten zu starten, gehen Sie zu *Konfigurieren > Sicherheit > VPN > Dynamic Multipoint VPN*. Wählen Sie dann die Option *Create a Spoke in a DMVPN (Spoke in einem DMVPN erstellen) aus* und klicken Sie auf *Launch the selected task (Ausgewählte Aufgabe starten)*.

VPN

Create Dynamic Multipoint VPN (DMVPN) Edit Dynamic Multipoint VPN (DMVPN)

Configure DMVPN Spoke



Create a spoke (client) in a DMVPN

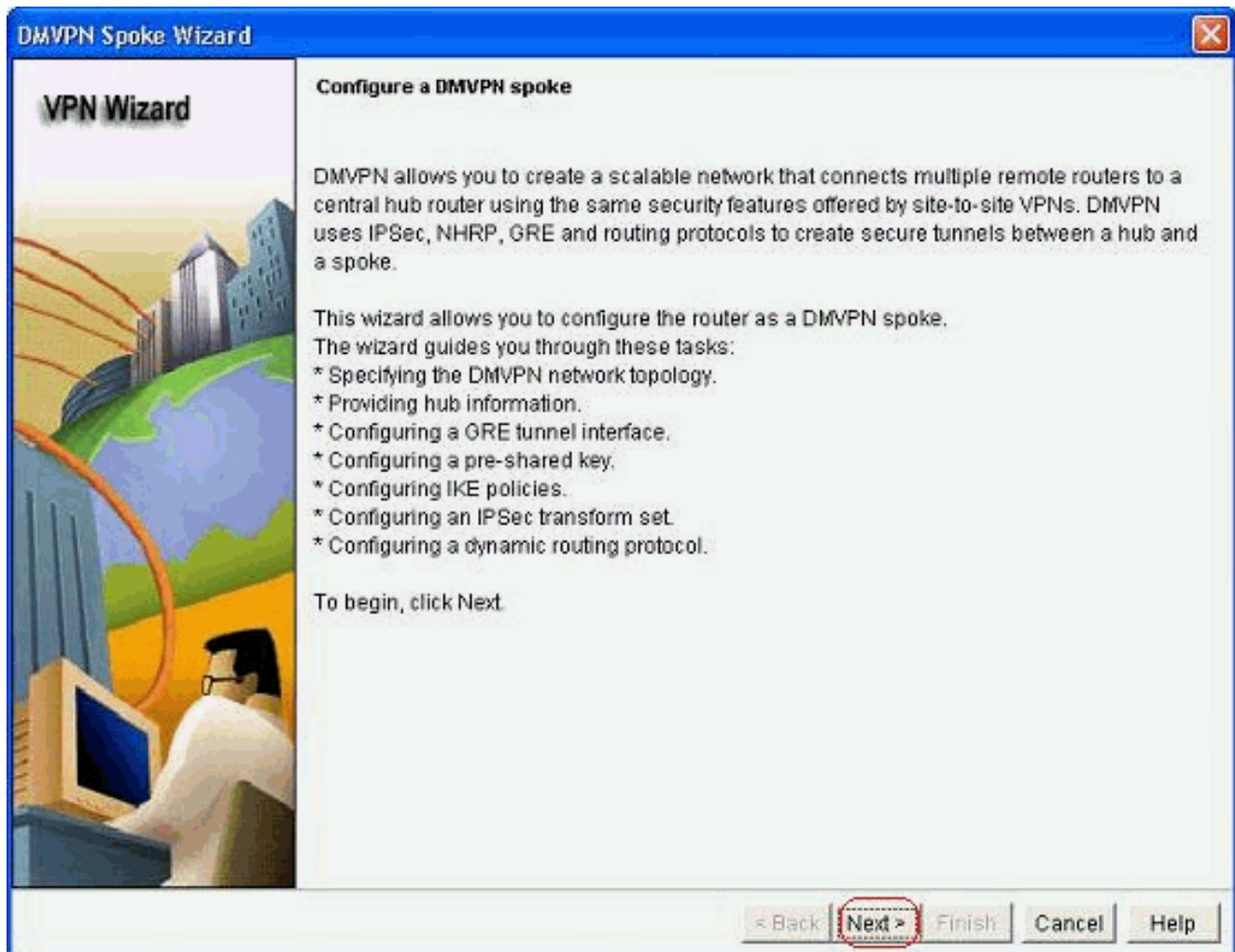
Use this option to configure the router as a spoke in a full mesh or hub and spoke network topology. To complete this configuration, you must know the hub's IP address, NHRP information, pre-shared key, IKE policy, IPSec Transform set and dynamic routing protocol information.

Create a hub (server or head-end) in a DMVPN

Use this option to configure the router as a primary or backup hub. If you are configuring a backup hub, you must know the primary hub's NHRP information, pre-shared key, IKE policy, IPSec Transform set and dynamic routing protocol information.

Launch the selected task

2. Klicken Sie zum Starten auf *Weiter*.



3. Wählen Sie die Option *Hub-and-Spoke-Netzwerk* aus, und klicken Sie auf *Weiter*.

VPN Wizard

DMVPN Network Topology

Select the DMVPN network topology.

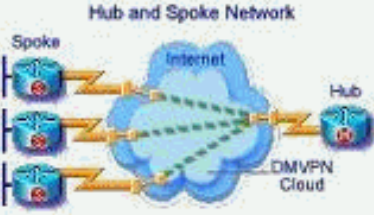
Hub and Spoke network

In this topology, all DMVPN traffic is routed through the hub. A point-to-point GRE interface will be configured on the spoke, and the spoke will use it to create a tunnel to the hub which will remain up. Spokes do not create GRE tunnels to other spokes in this topology.

Fully meshed network

In this topology, the spoke dynamically establishes a direct tunnel to another spoke device, and sends DMVPN traffic directly to it. A multipoint GRE tunnel interface is configured on the spoke to support this functionality.

Note: Cisco supports fully meshed DMVPN networks only in the following Cisco IOS images: 12.3(8)T1 and 12.3(9) or later.



< Back **Next >** Finish Cancel Help

4. Geben Sie die Hub-bezogenen Informationen an, z. B. die öffentliche Schnittstelle des Hub-Routers und die Tunnelschnittstelle des Hub-Routers.

DMVPN Spoke Wizard (Hub and Spoke Topology) - 20% Complete

VPN Wizard

Specify Hub Information
Enter the IP address of the hub and the IP address of the hub's mGRE tunnel interface. Contact your network administrator to get this information.

Hub Information

IP address of hub's physical interface:

IP address of hub's mGRE tunnel interface:

Spoke
You are configuring this spoke router

Internet
DMVPN Cloud

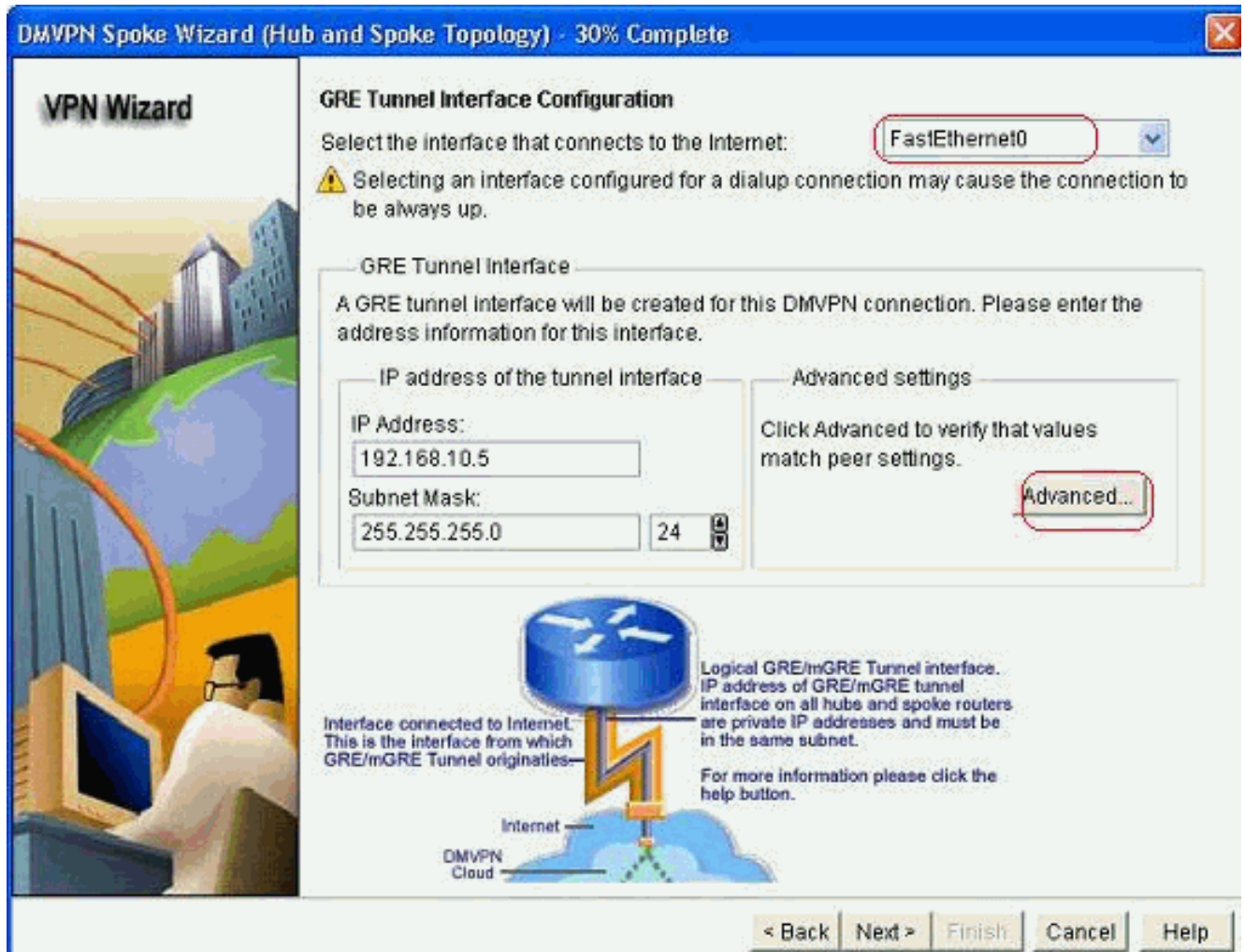
Hub

Public IP address to be entered above

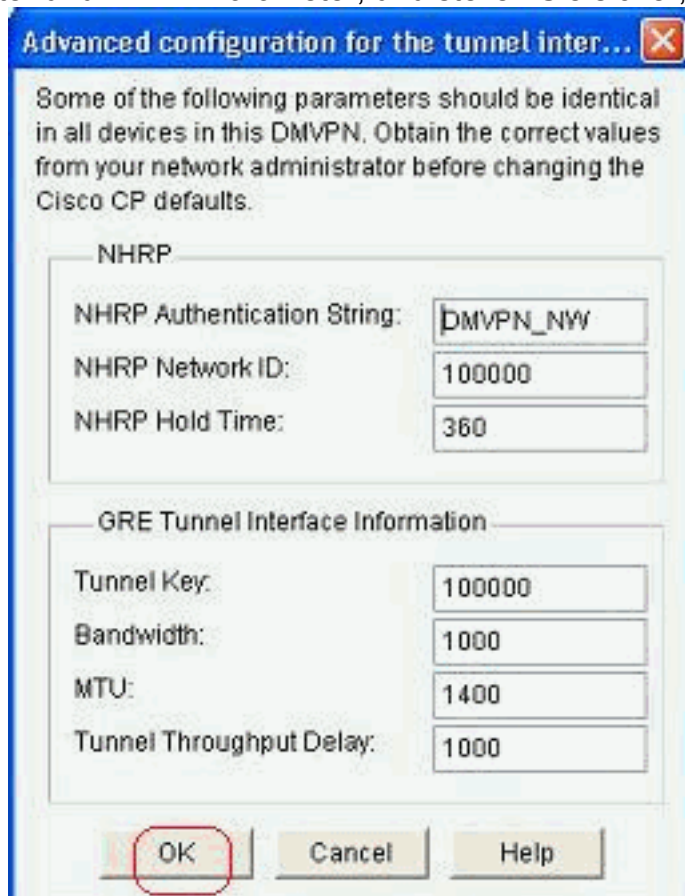
IP address of the mGRE tunnel to be entered above

< Back | **Next >** | Finish | Cancel | Help

5. Geben Sie die Details der Tunnelschnittstelle für das Spoke und die öffentliche Schnittstelle des Spokes an. Klicken Sie anschließend auf *Erweitert*.



6. Überprüfen Sie die Tunnelparameter und NHRP-Parameter, und stellen Sie sicher, dass sie



den Hub-Parametern entsprechen.

7. Geben Sie den vorinstallierten Schlüssel an, und klicken Sie auf

Weiter.

VPN Wizard

Authentication

Select the method you want to use to authenticate this router to the peer device(s) in the DMVPN network. You can use digital certificate or a pre-shared key. If digital certificate is used, the router must have a valid certificate configured. If pre-shared key is used, the key configured on this router must match the keys configured on all other routers in the DMVPN network.

Digital Certificates

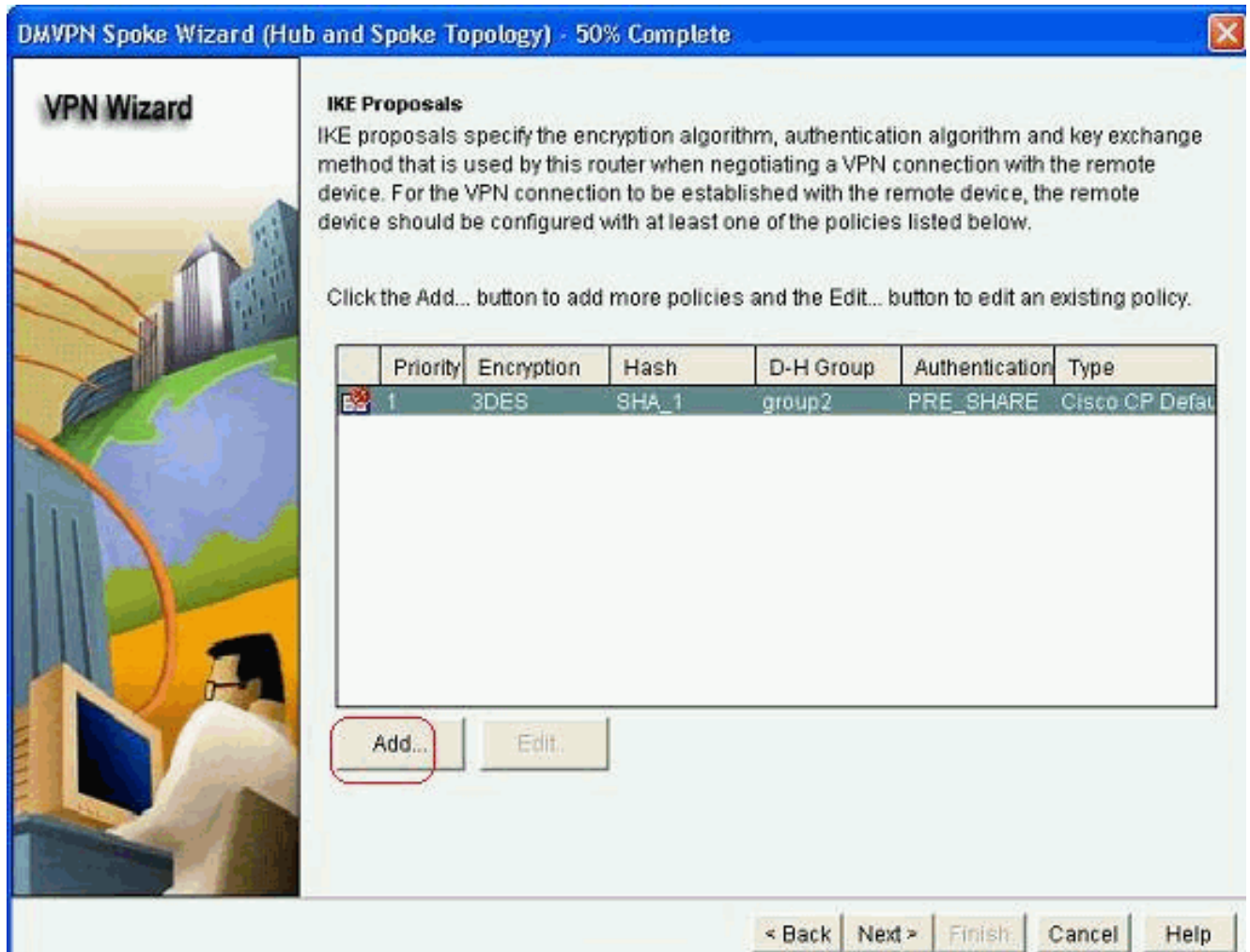
Pre-shared Keys

pre-shared key:

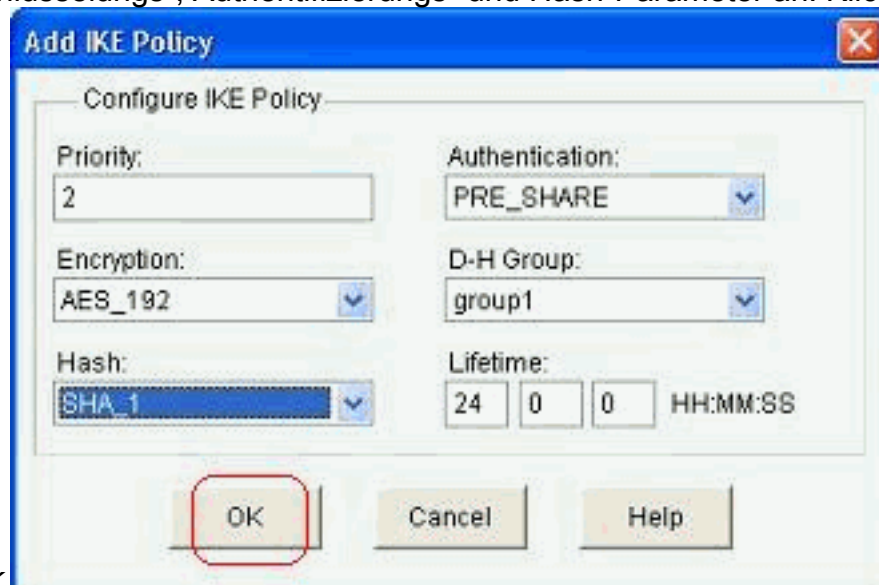
Reenter key:

< Back **Next** > Finish Cancel Help

8. Klicken Sie auf *Hinzufügen*, um ein separates IKE-Angebot hinzuzufügen.

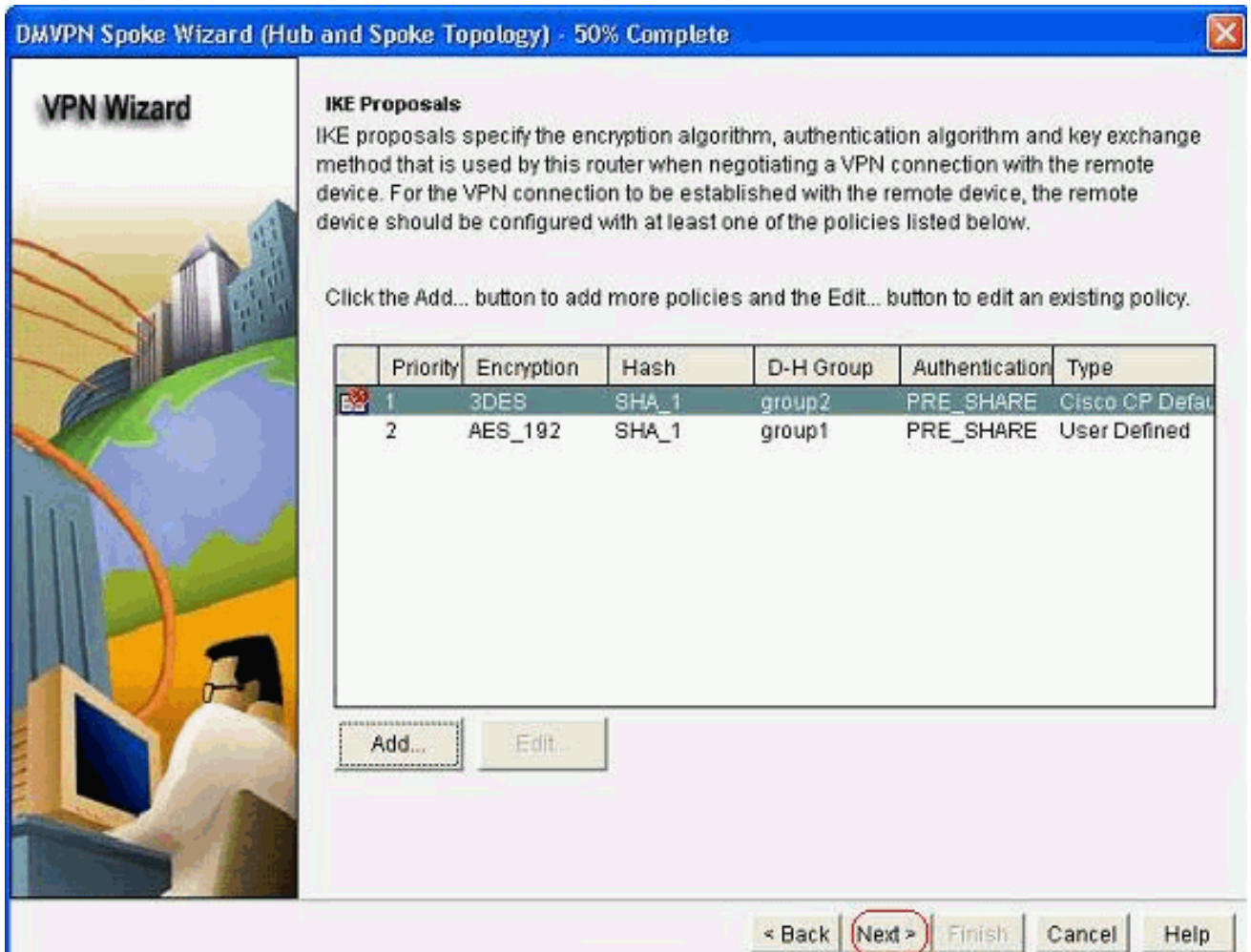


9. Geben Sie die Verschlüsselungs-, Authentifizierungs- und Hash-Parameter an. Klicken Sie

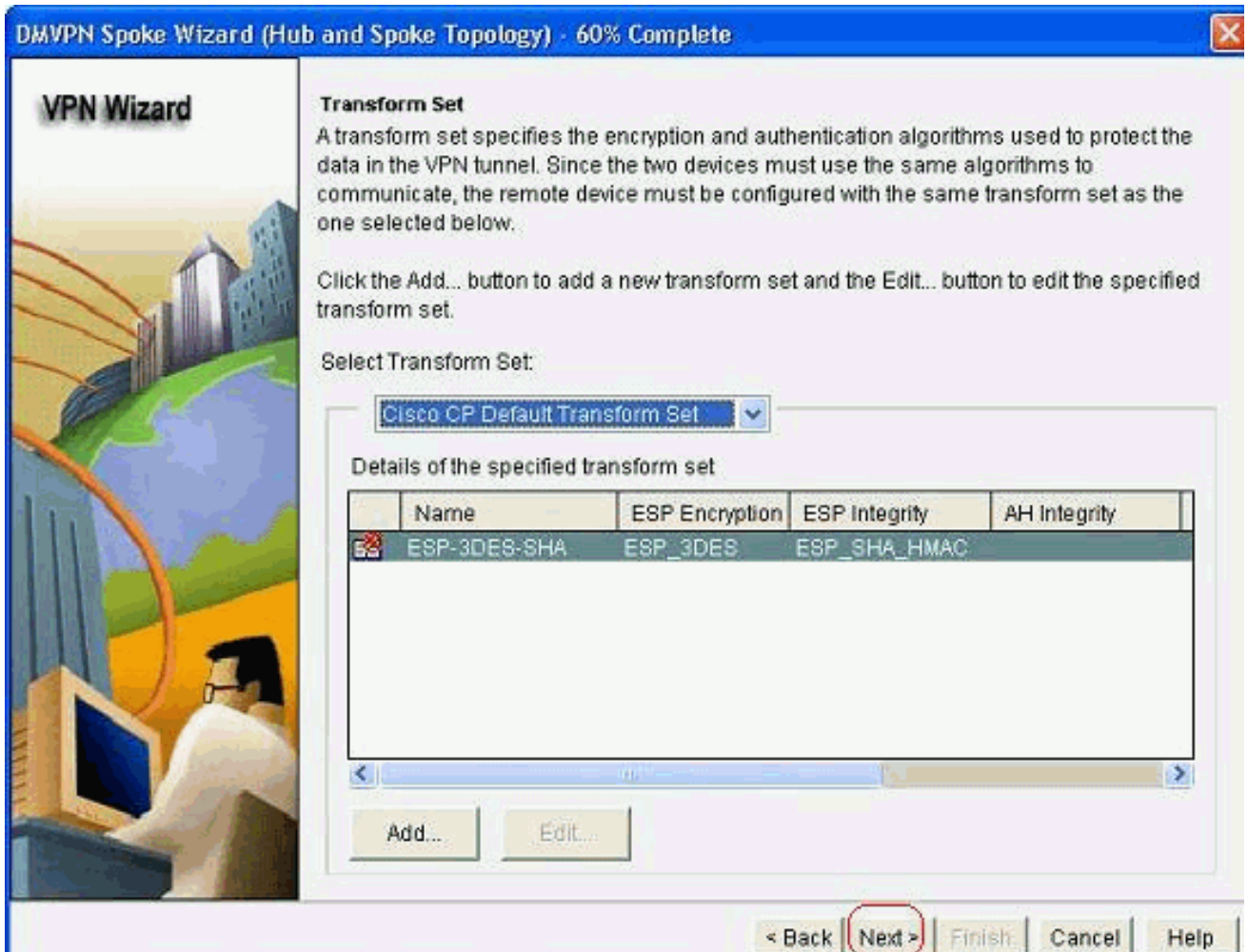


anschließend auf *OK*.

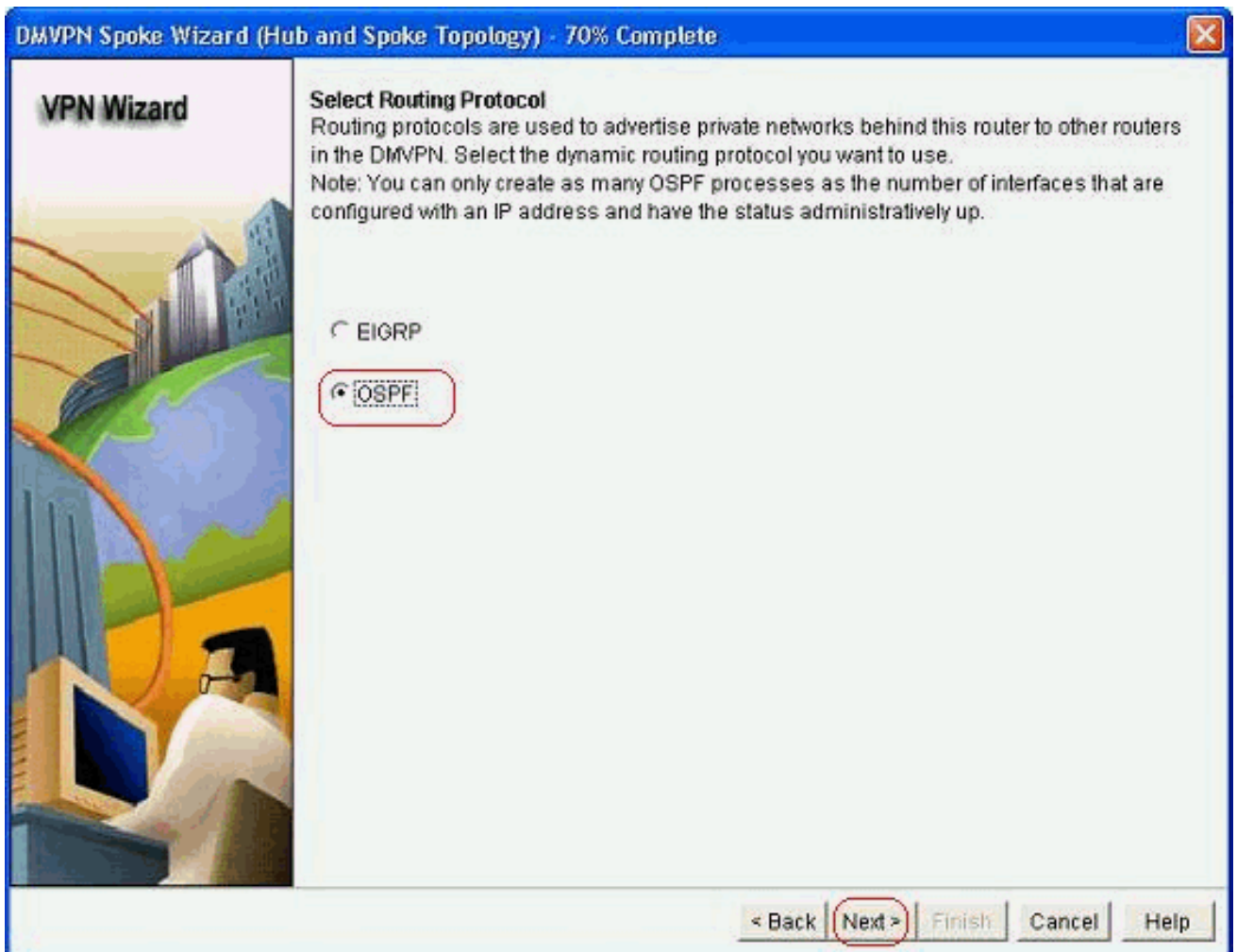
10. Die neu erstellte IKE-Richtlinie ist hier zu sehen. Klicken Sie auf *Weiter*.



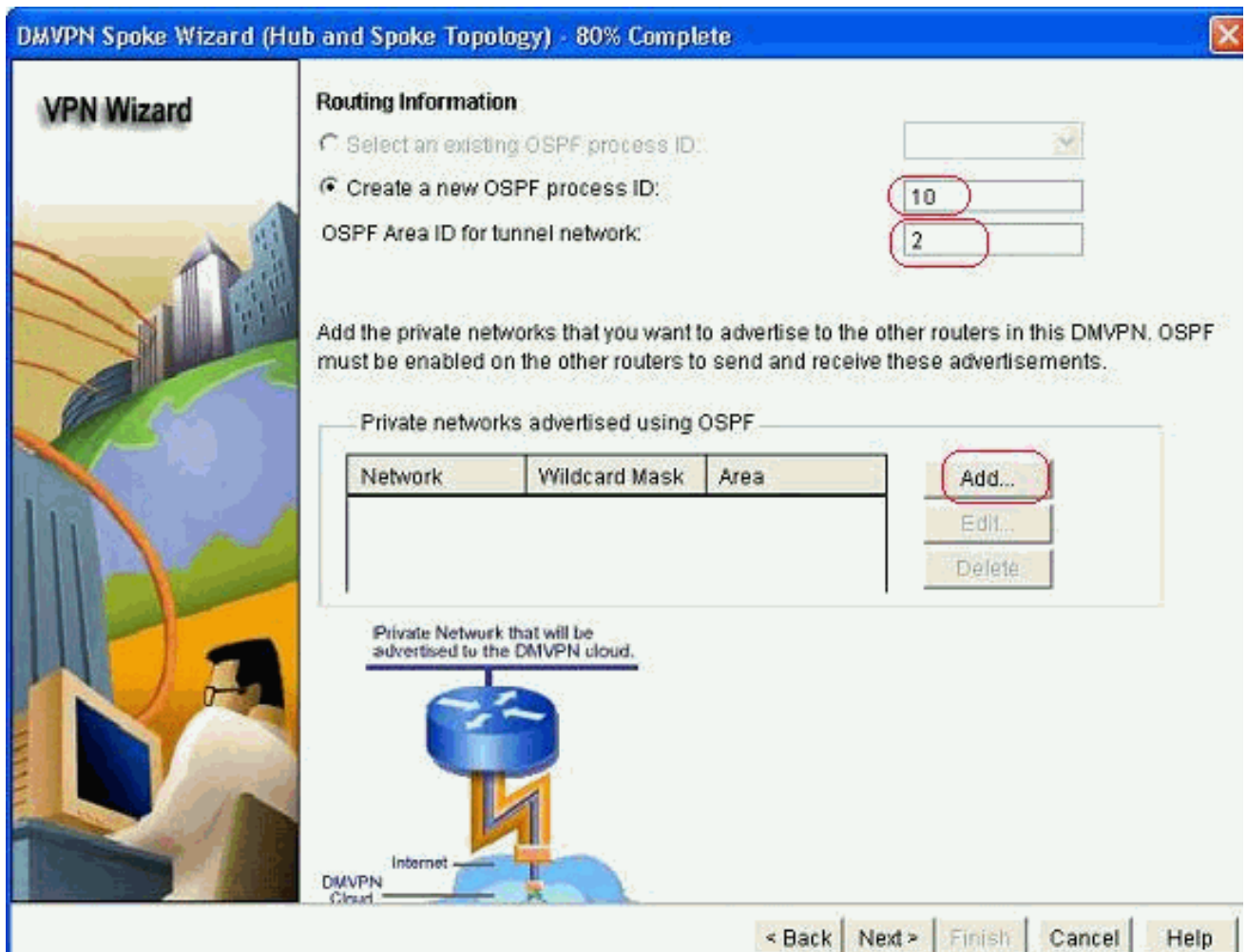
11. Klicken Sie auf *Weiter*, um mit dem standardmäßigen Umwandlungssatz fortzufahren.



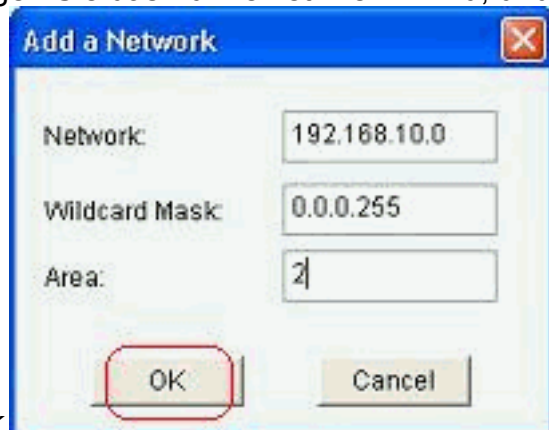
12. Wählen Sie das gewünschte Routing-Protokoll aus. Hier wird *OSPF* ausgewählt.



13. Geben Sie die OSPF-Prozess-ID und die Area-ID an. Klicken Sie auf *Hinzufügen*, um die Netzwerke hinzuzufügen, die von OSPF angekündigt werden sollen.

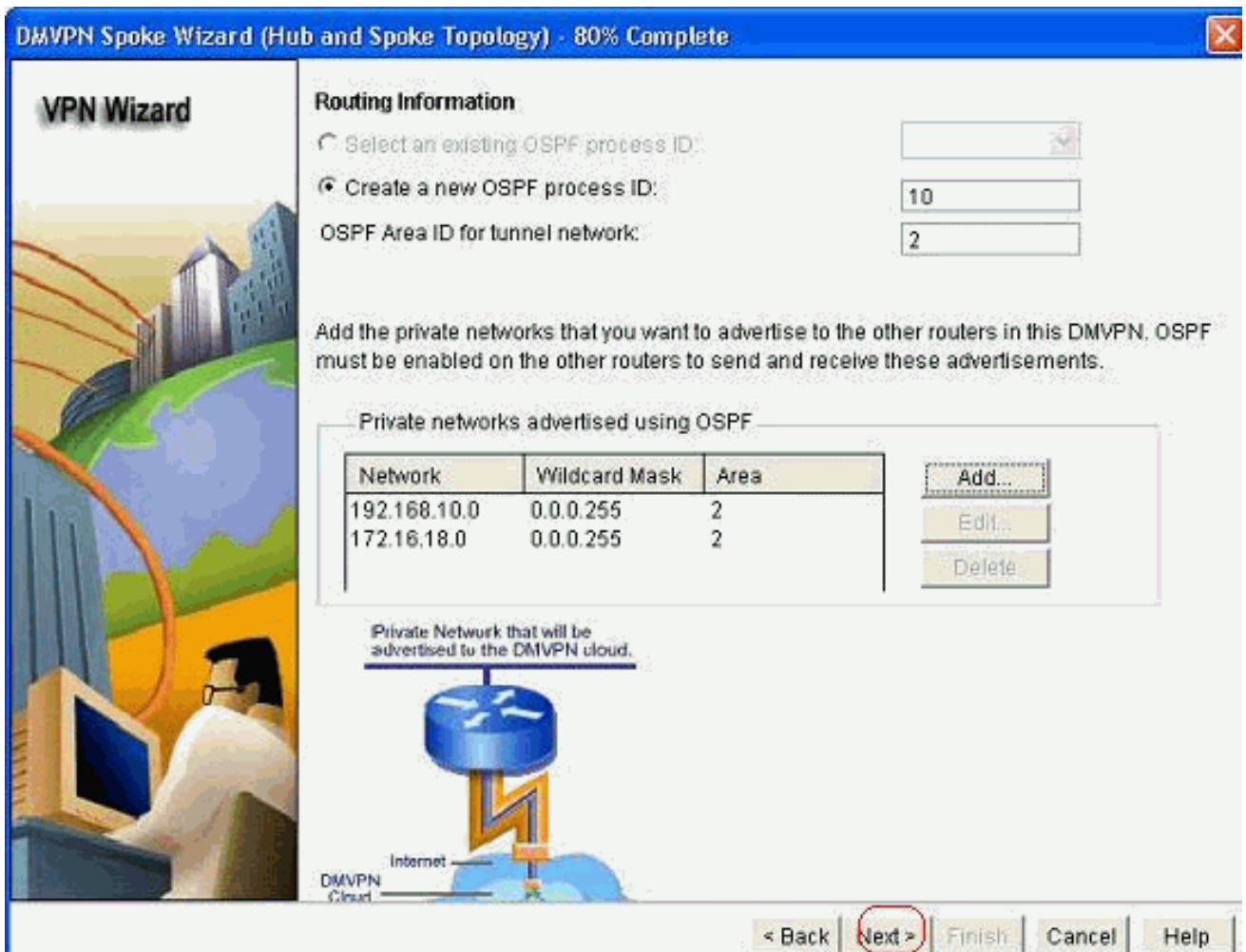


14. Fügen Sie das Tunnelnetzwerk hinzu, und klicken Sie auf

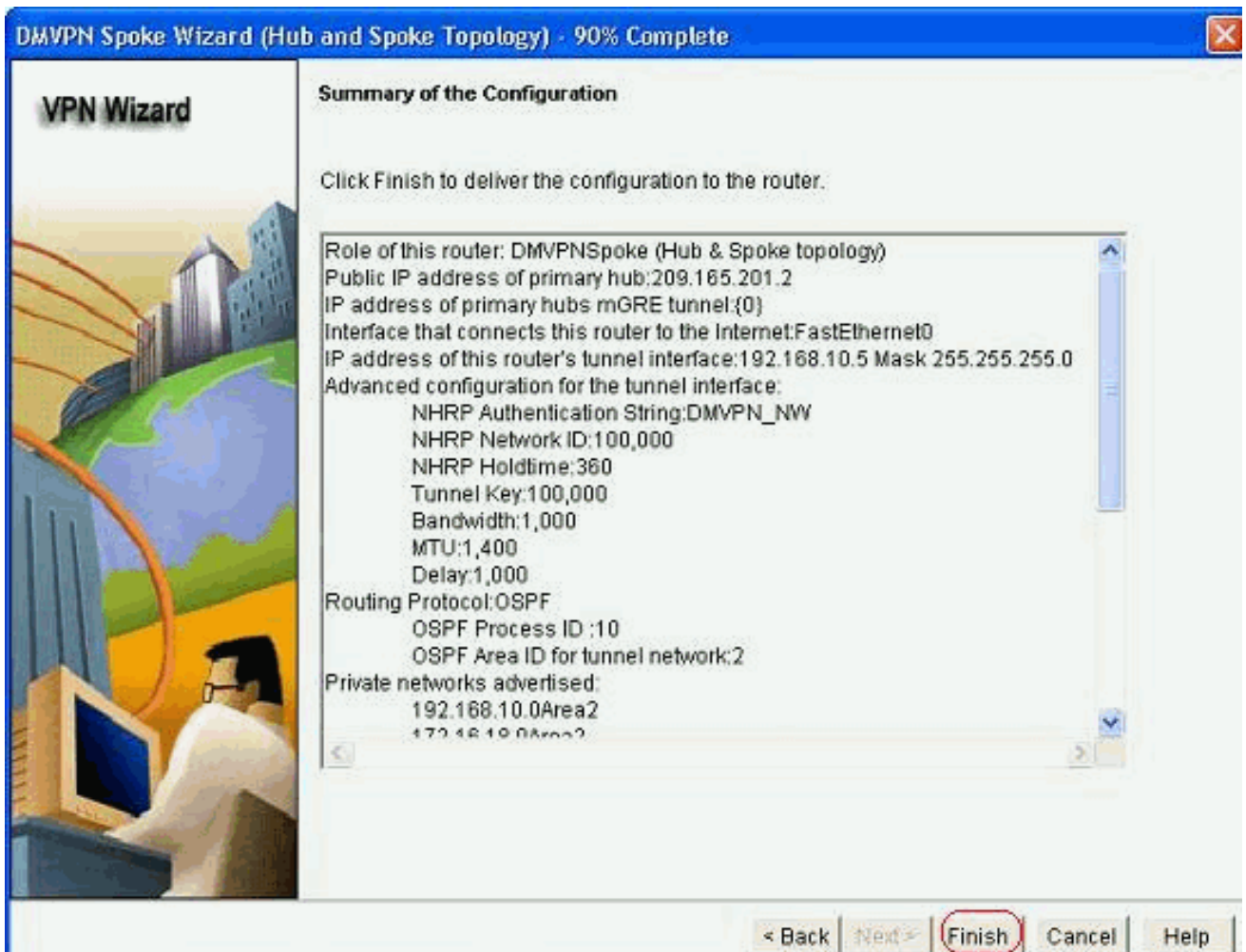


OK.

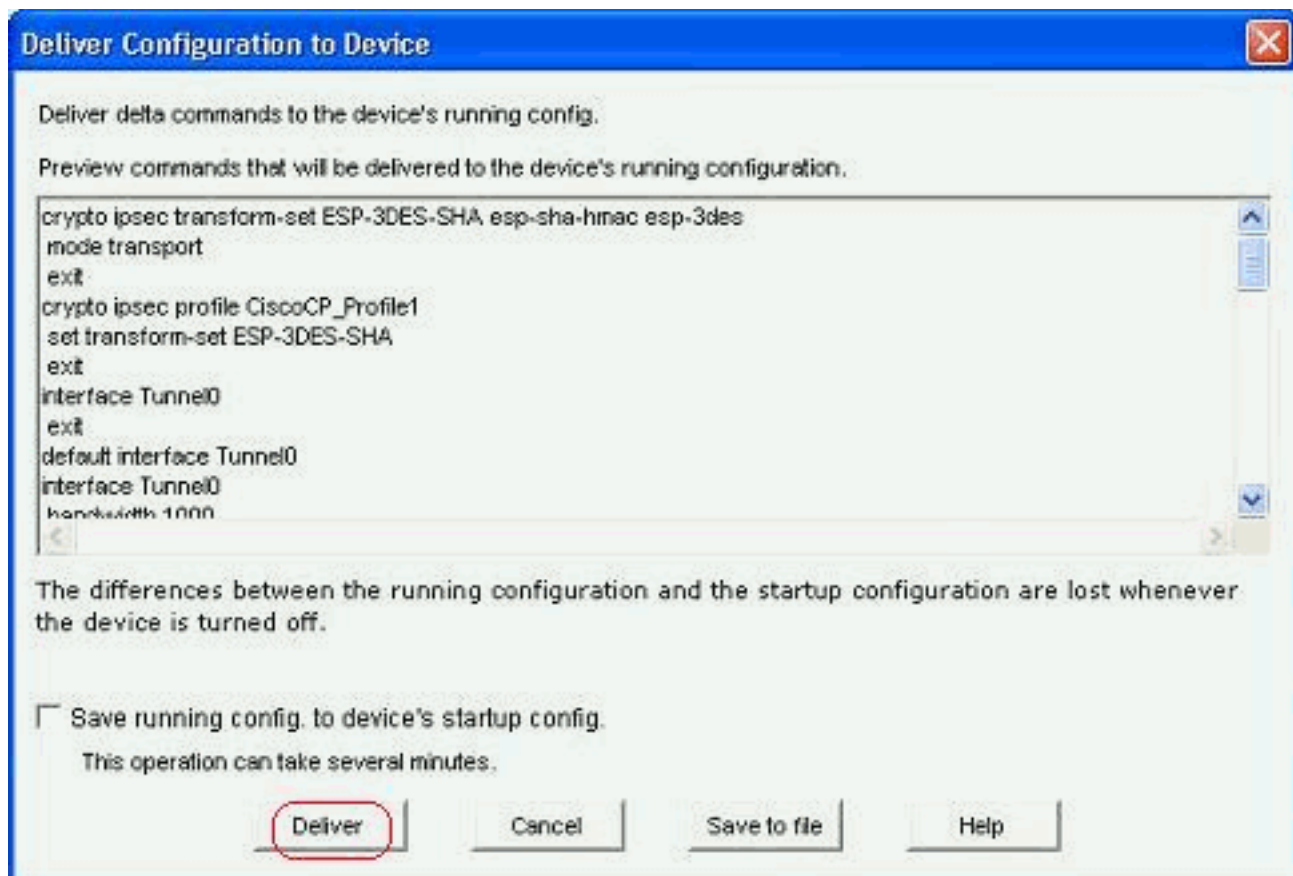
15. Fügen Sie das private Netzwerk hinter dem Spoke-Router hinzu. Klicken Sie anschließend auf *Weiter*.



16. Klicken Sie auf *Fertig stellen*, um die Assistentenkonfiguration abzuschließen.



17. Klicken Sie auf *Deliver*, um die Befehle auszuführen. Aktivieren Sie das Kontrollkästchen *Aktuelle Konfiguration in der Startkonfiguration des Geräts speichern*, wenn Sie die Konfiguration speichern möchten.



CLI-Konfiguration für Spoke

Die entsprechende CLI-Konfiguration wird hier angezeigt:

Spoke-Router
<pre>crypto ipsec transform-set ESP-3DES-SHA esp-sha-hmac esp-3des mode transport exit crypto ipsec profile CiscoCP_Profile1 set transform-set ESP-3DES-SHA exit interface Tunnel0 exit default interface Tunnel0 interface Tunnel0 bandwidth 1000 delay 1000 ip nhrp holdtime 360 ip nhrp network-id 100000 ip nhrp authentication DMVPN_NW ip ospf network point-to-multipoint ip mtu 1400 no shutdown ip address 192.168.10.5 255.255.255.0 ip tcp adjust-mss 1360 ip nhrp nhs 192.168.10.2 ip nhrp map 192.168.10.2 209.165.201.2 tunnel source FastEthernet0 tunnel destination 209.165.201.2 tunnel protection ipsec profile CiscoCP_Profile1 tunnel key 100000</pre>

```

exit
router ospf 10
 network 192.168.10.0 0.0.0.255 area 2
 network 172.16.18.0 0.0.0.255 area 2
exit
crypto isakmp key ***** address 209.165.201.2
crypto isakmp policy 2
 authentication pre-share
 encr aes 192
 hash sha
 group 1
 lifetime 86400
exit
crypto isakmp policy 1
 authentication pre-share
 encr 3des
 hash sha
 group 2
 lifetime 86400
exit

```

[Hub-Konfiguration mit Cisco CP](#)


In diesem Abschnitt wird ein schrittweiser Ansatz zur Konfiguration des Hub-Routers für das DMVPN beschrieben.

1. Gehen Sie zu *Configure > Security > VPN > Dynamic Multipoint VPN*, und wählen Sie die Option *Create a Hub in a DMVPN* aus. Klicken Sie auf *Ausgewählte Aufgabe starten*.

Configure > Security > VPN > Dynamic Multipoint VPN

VPN

Create Dynamic Multipoint VPN (DMVPN) Edit Dynamic Multipoint VPN (DMVPN)



Create a spoke (client) in a DMVPN

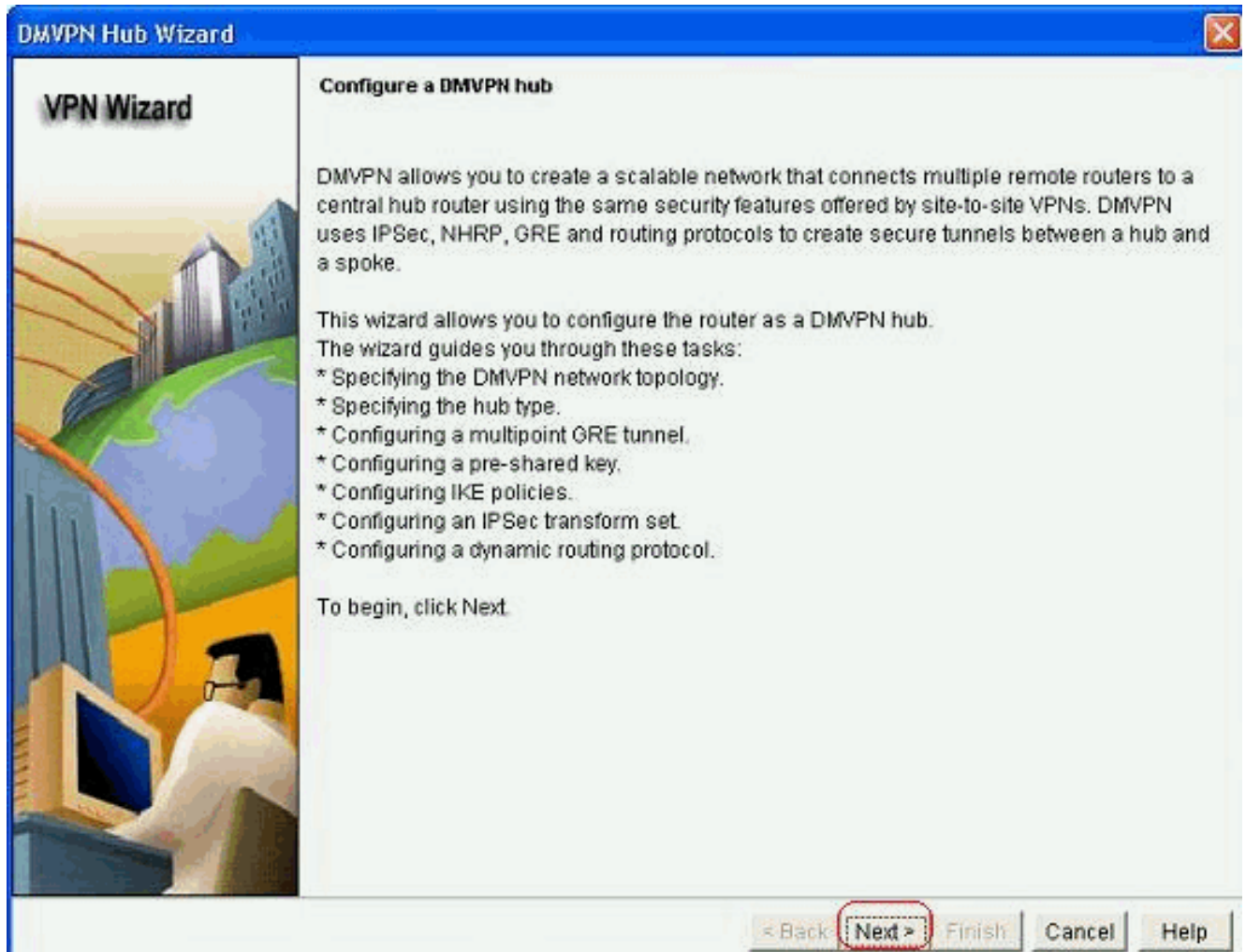
Use this option to configure the router as a spoke in a full mesh or hub and spoke network topology. To complete this configuration, you must know the hub's IP address, NHRP information, pre-shared key, IKE policy, IPsec Transform set and dynamic routing protocol information.

Create a hub (server or head-end) in a DMVPN:

Use this option to configure the router as a primary or backup hub. If you are configuring a backup hub, you must know the primary hub's NHRP information, pre-shared key, IKE policy, IPsec Transform set and dynamic routing protocol information.

Launch the selected task

2. Klicken Sie auf *Weiter*.



3. Wählen Sie die Option *Hub-and-Spoke-Netzwerk* aus, und klicken Sie auf *Weiter*.

VPN Wizard

DMVPN Network Topology

Select the DMVPN network topology.

Hub and Spoke network

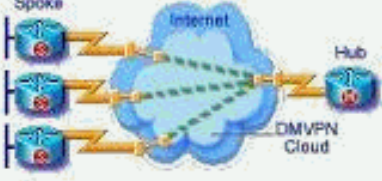
In this topology, all DMVPN traffic is routed through the hub. A point-to-point GRE interface will be configured on the spoke, and the spoke will use it to create a tunnel to the hub which will remain up. Spokes do not create GRE tunnels to other spokes in this topology.

Fully meshed network

In this topology, the spoke dynamically establishes a direct tunnel to another spoke device, and sends DMVPN traffic directly to it. A multipoint GRE tunnel interface is configured on the spoke to support this functionality.

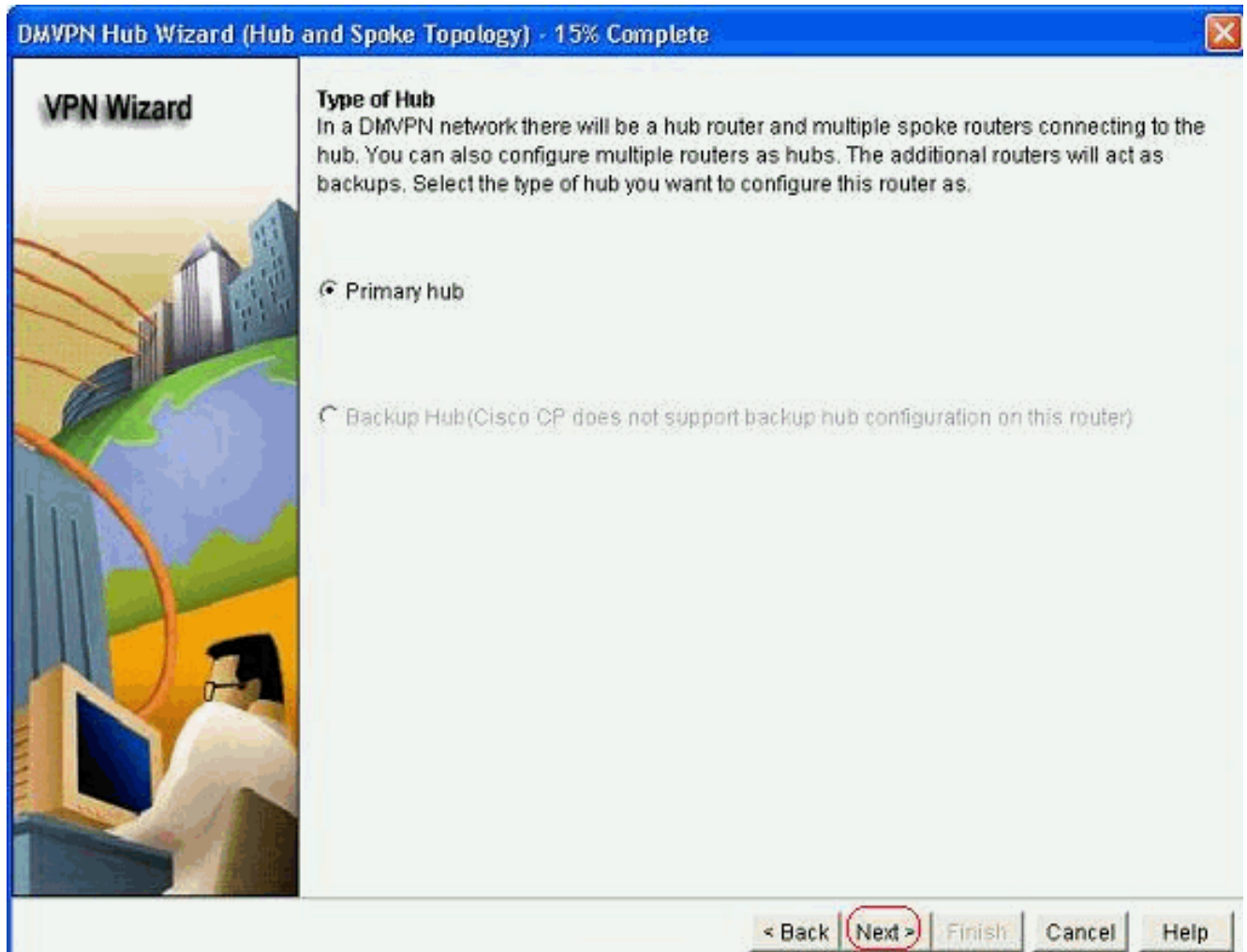
Note: Cisco supports fully meshed DMVPN networks only in the following Cisco IOS images: 12.3(8)T1 and 12.3(9) or later.

Hub and Spoke Network




< Back **Next >** Finish Cancel Help

4. Wählen Sie *Primary Hub (Primärer Hub)*. Klicken Sie anschließend auf *Weiter*.



5. Geben Sie die Tunnel-Schnittstellenparameter an, und klicken Sie auf *Erweitert*.

VPN Wizard



Multipoint GRE Tunnel Interface Configuration

Select the interface that connects to the Internet: GigabitEthernet0/0

⚠ Selecting an interface configured for a dialup connection may cause the connection to be always up.

Multi point GRE (mGRE) Tunnel Interface

A GRE tunnel interface will be created for this DMVPN connection. Please enter the address information for this interface.

IP address of the tunnel interface


IP Address:

Subnet Mask:

Advanced settings

Click Advanced to verify that values match peer settings.

Advanced...



6. Geben Sie die Tunnel-Parameter und NHRP-Parameter an. Klicken Sie anschließend auf

Advanced configuration for the tunnel inter... ✖

Some of the following parameters should be identical in all devices in this DMVPN. Obtain the correct values from your network administrator before changing the Cisco CP defaults.

NHRP

NHRP Authentication String:

NHRP Network ID:

NHRP Hold Time:

GRE Tunnel Interface Information

Tunnel Key:

Bandwidth:

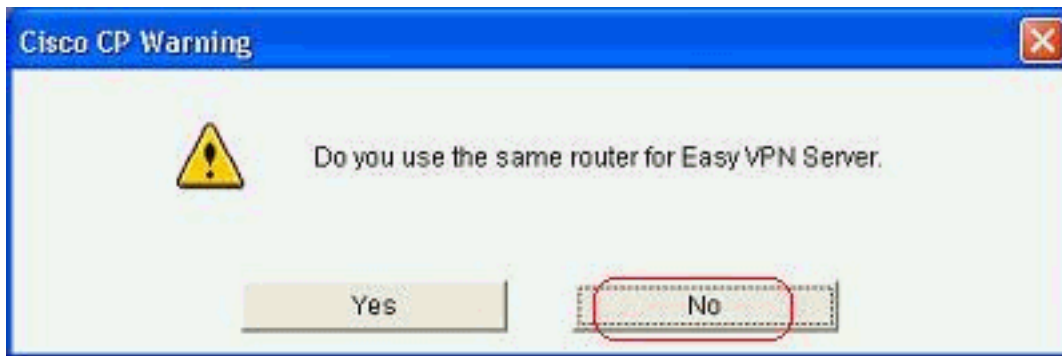
MTU:

Tunnel Throughput Delay:

OK
Cancel
Help

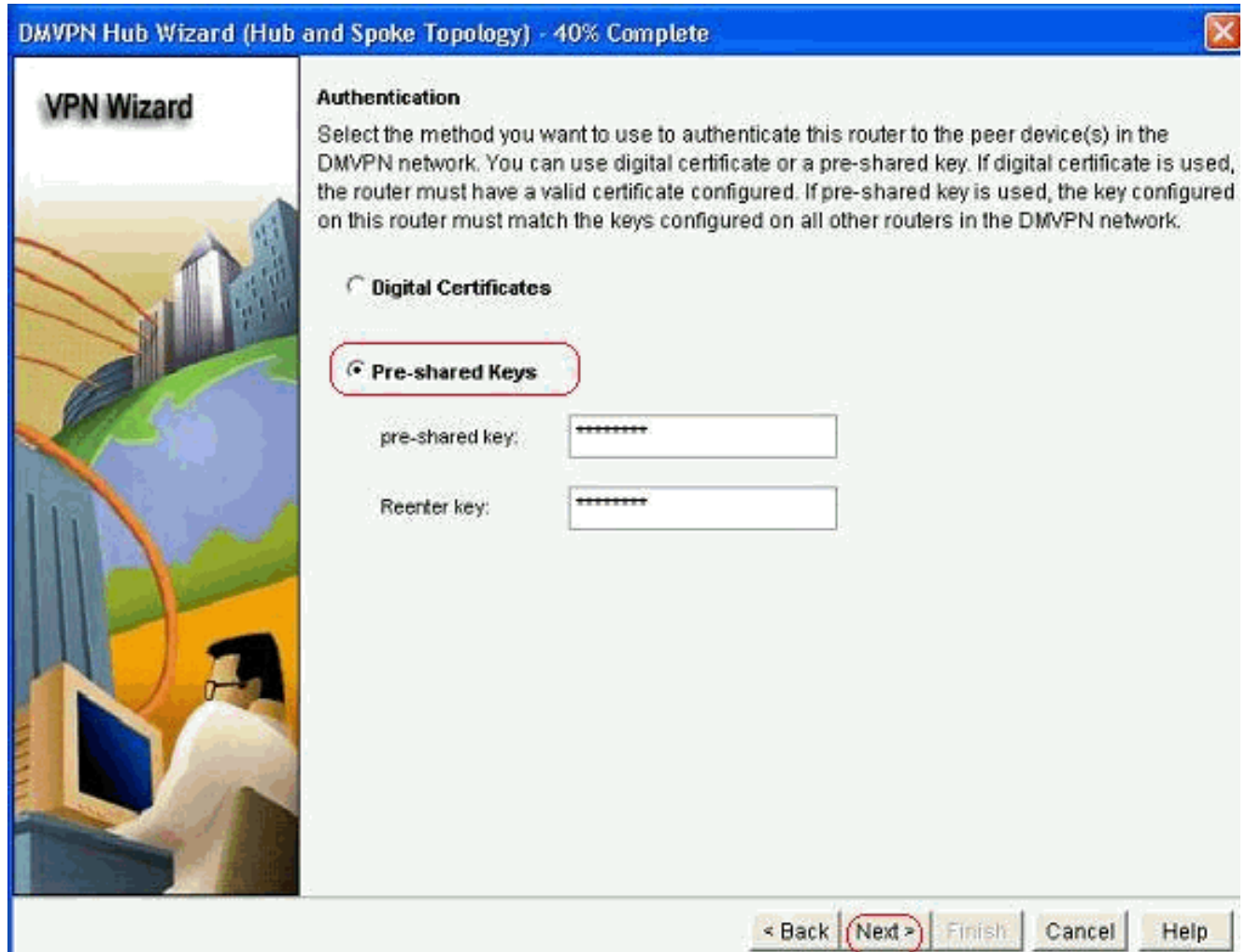
OK.

7. Geben Sie die Option basierend auf Ihrer Netzwerkeinrichtung

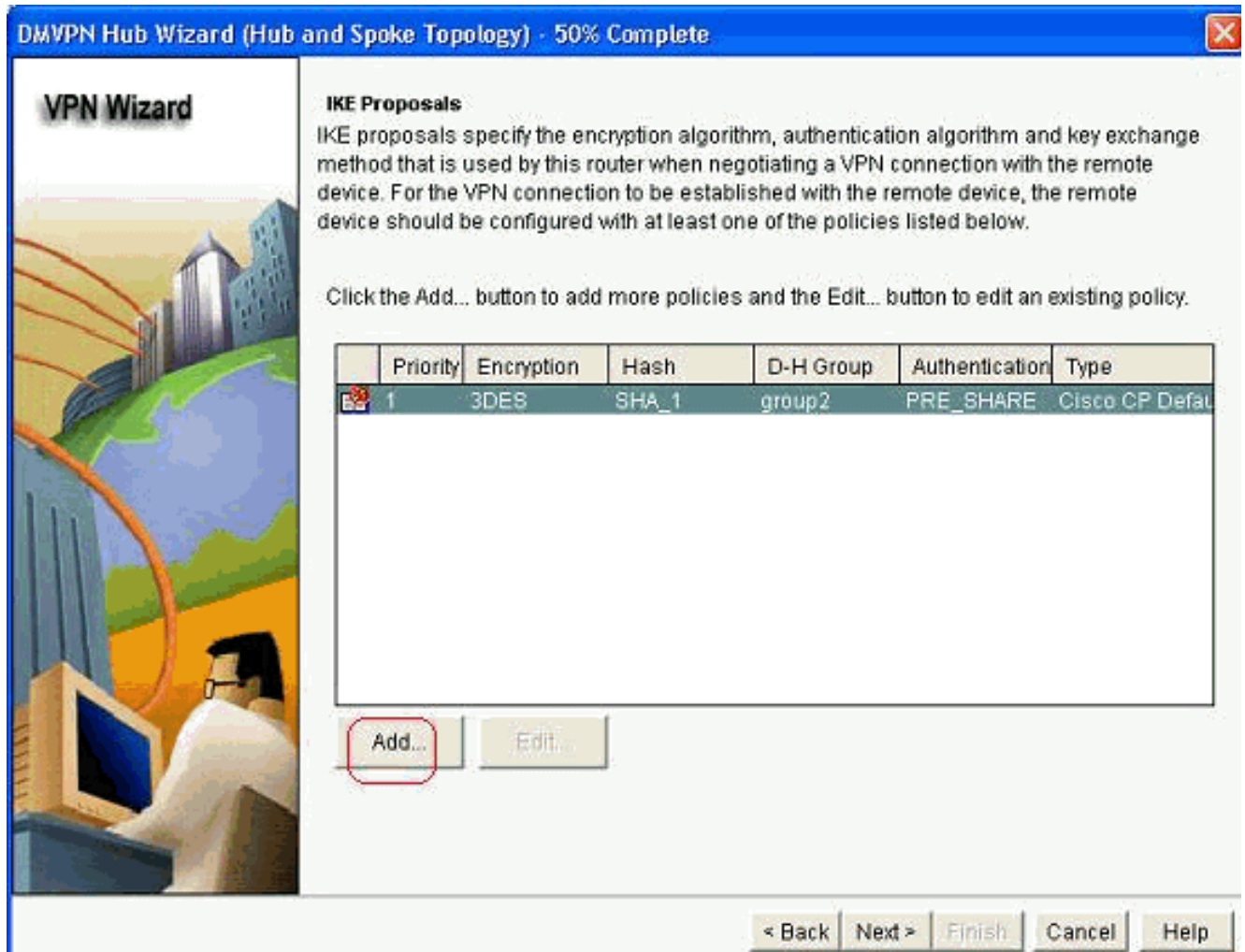


an.

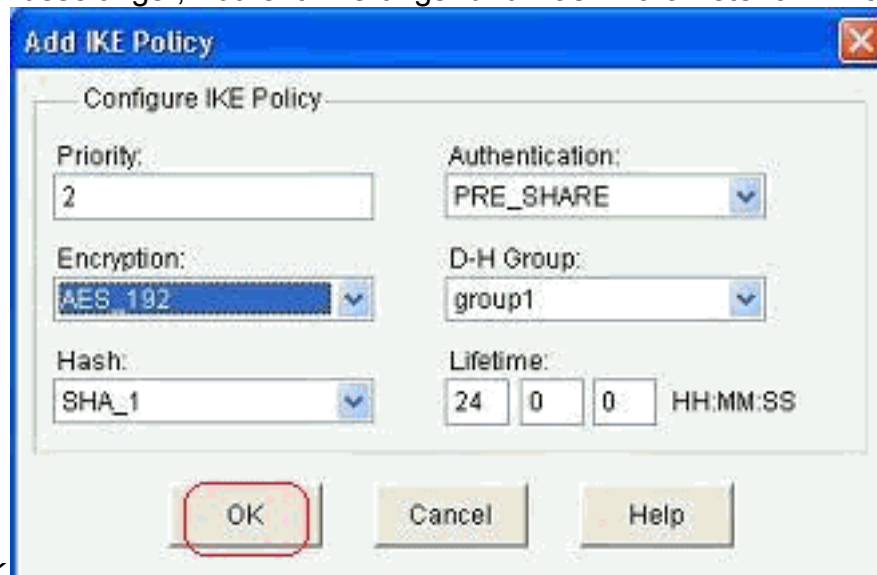
8. Wählen Sie *Pre-shared Keys (Vorinstallierte Schlüssel)* aus, und geben Sie die vorinstallierten Schlüssel an. Klicken Sie anschließend auf *Weiter*.



9. Klicken Sie auf *Hinzufügen*, um ein separates IKE-Angebot hinzuzufügen.

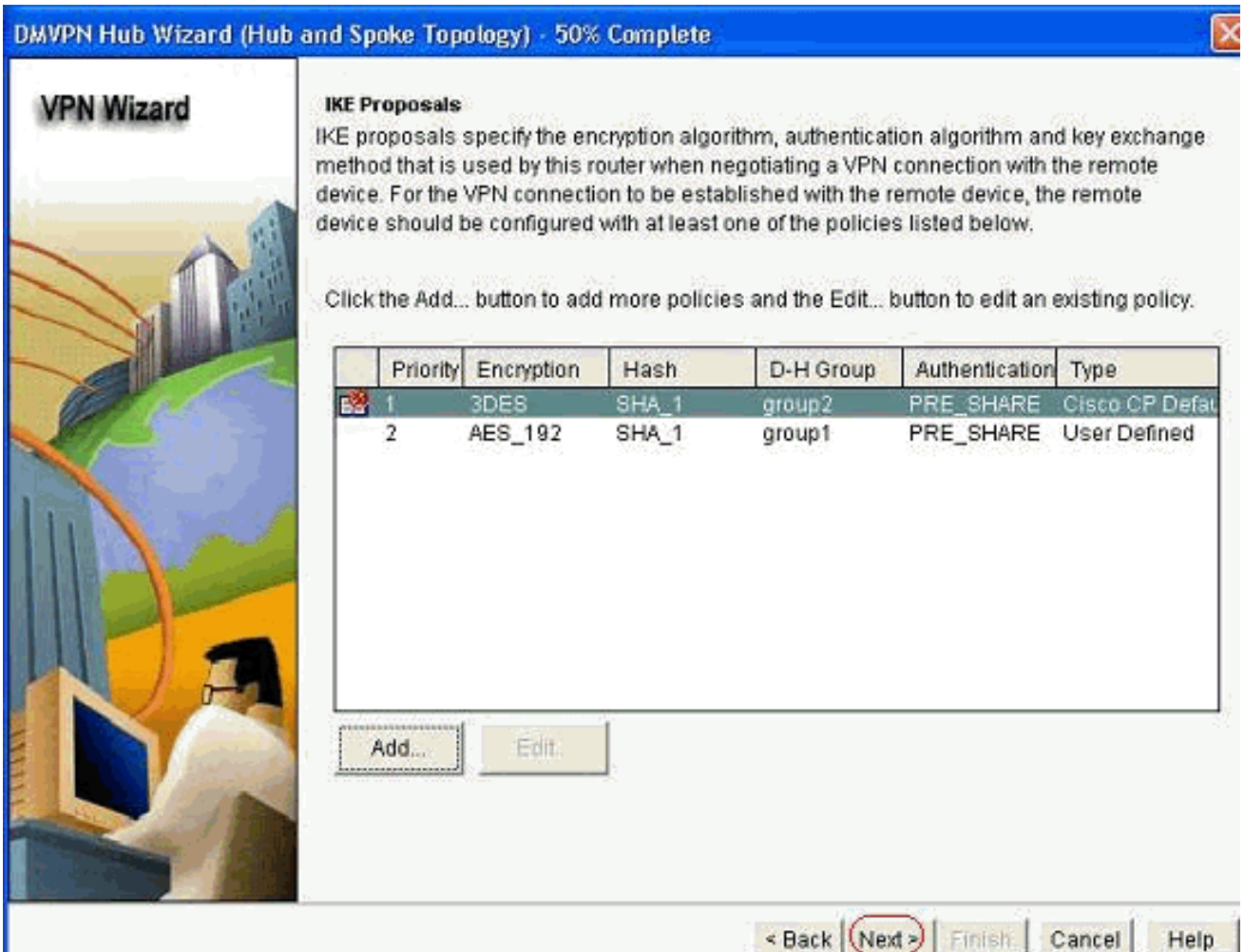


10. Geben Sie die Verschlüsselungs-, Authentifizierungs- und Hash-Parameter an. Klicken Sie

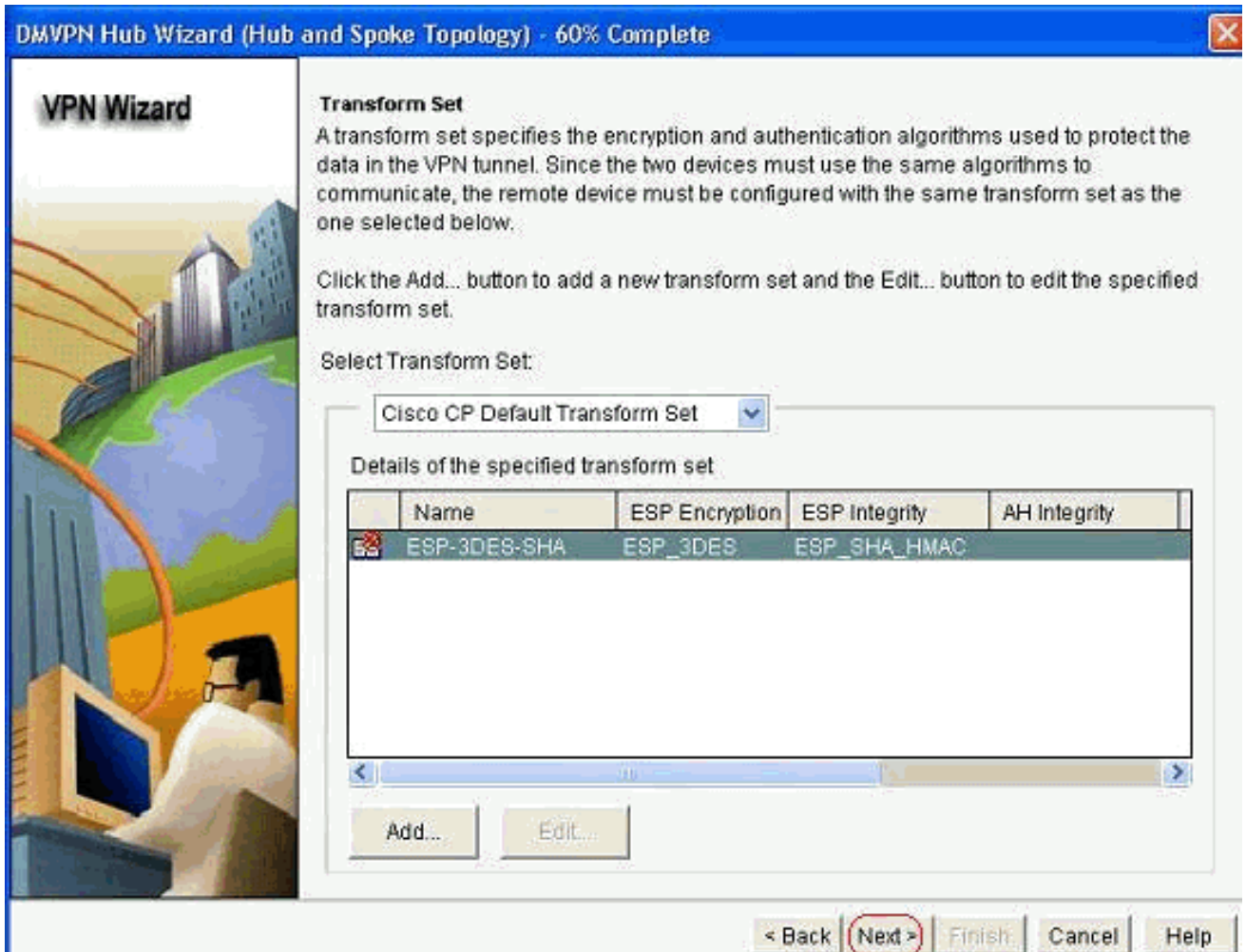


anschließend auf *OK*.

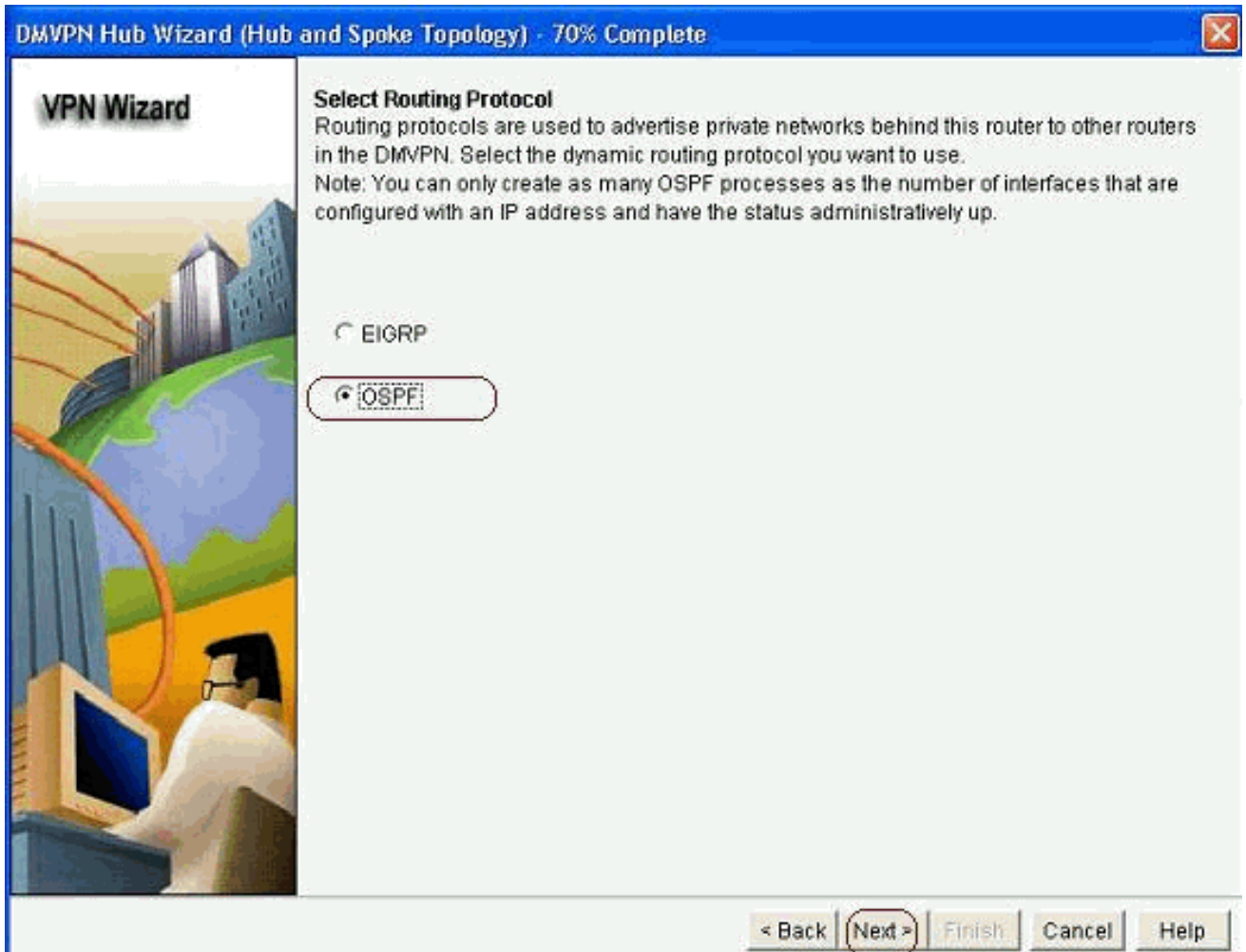
11. Die neu erstellte IKE-Richtlinie ist hier zu sehen. Klicken Sie auf *Weiter*.



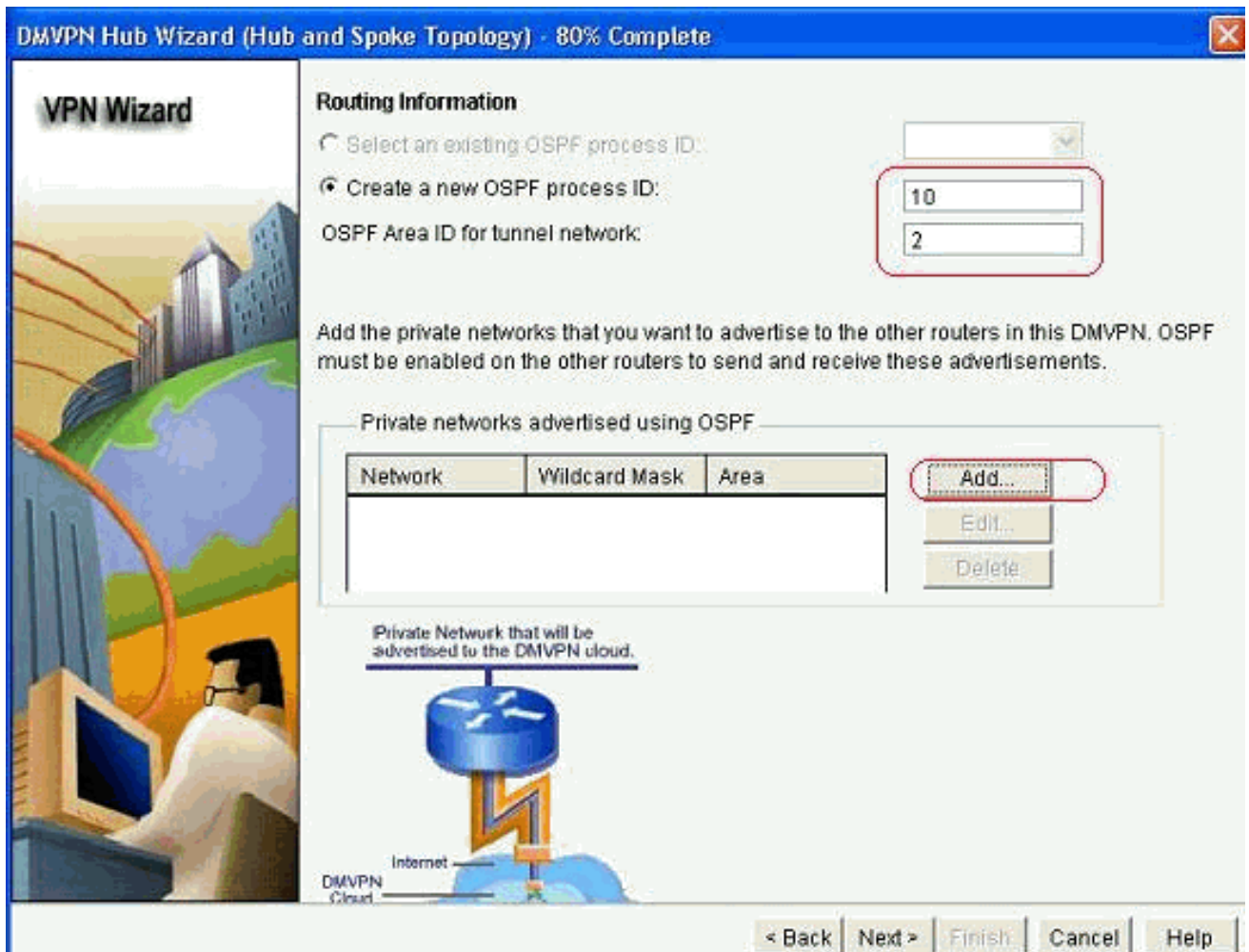
12. Klicken Sie auf *Weiter*, um mit dem standardmäßigen Umwandlungssatz fortzufahren.



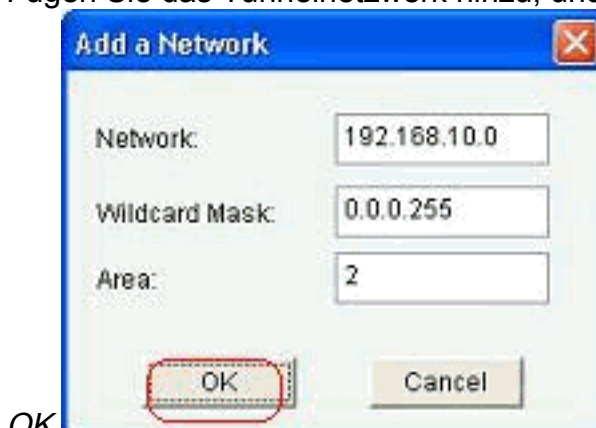
13. Wählen Sie das gewünschte Routing-Protokoll aus. Hier wird *OSPF* ausgewählt.



14. Geben Sie die OSPF-Prozess-ID und die Area-ID an. Klicken Sie auf *Hinzufügen*, um die Netzwerke hinzuzufügen, die von OSPF angekündigt werden sollen.

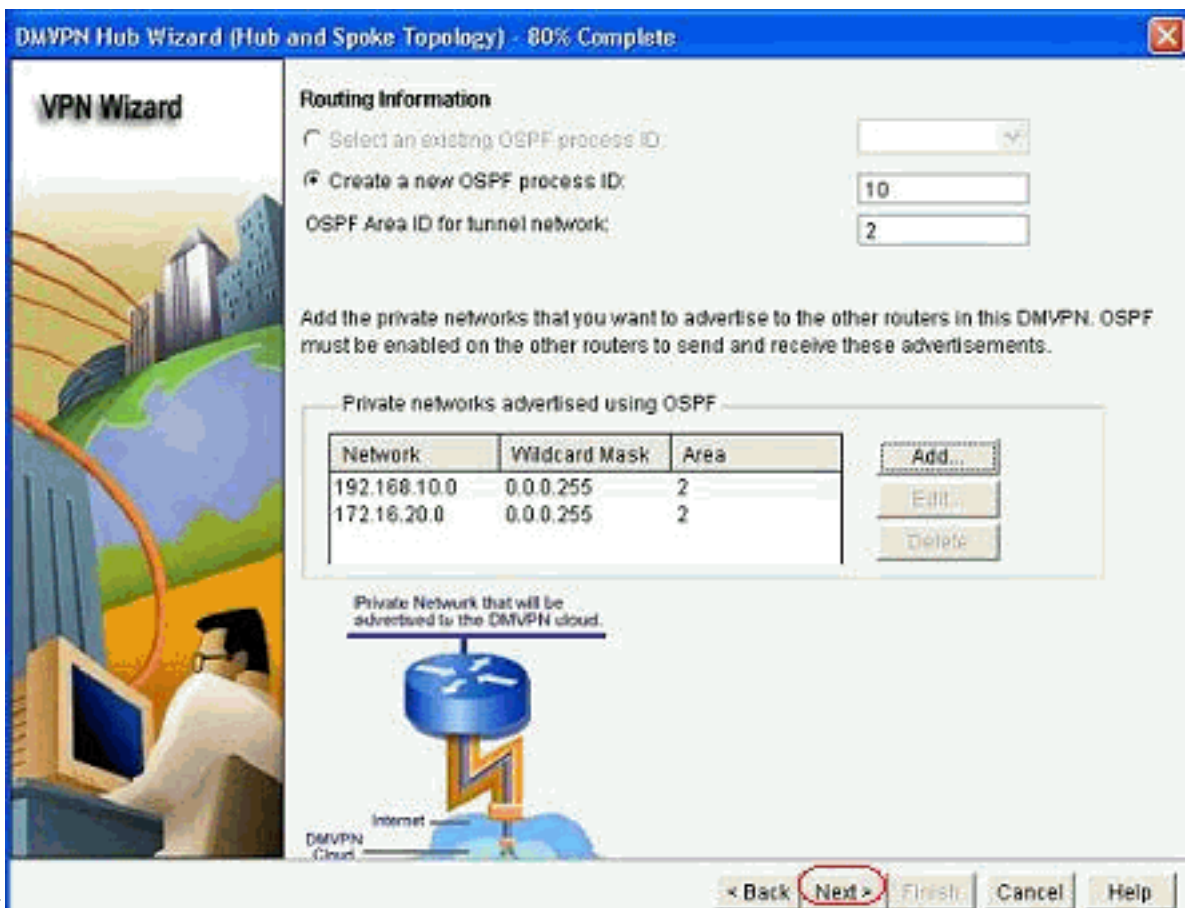


15. Fügen Sie das Tunnelnetzwerk hinzu, und klicken Sie auf



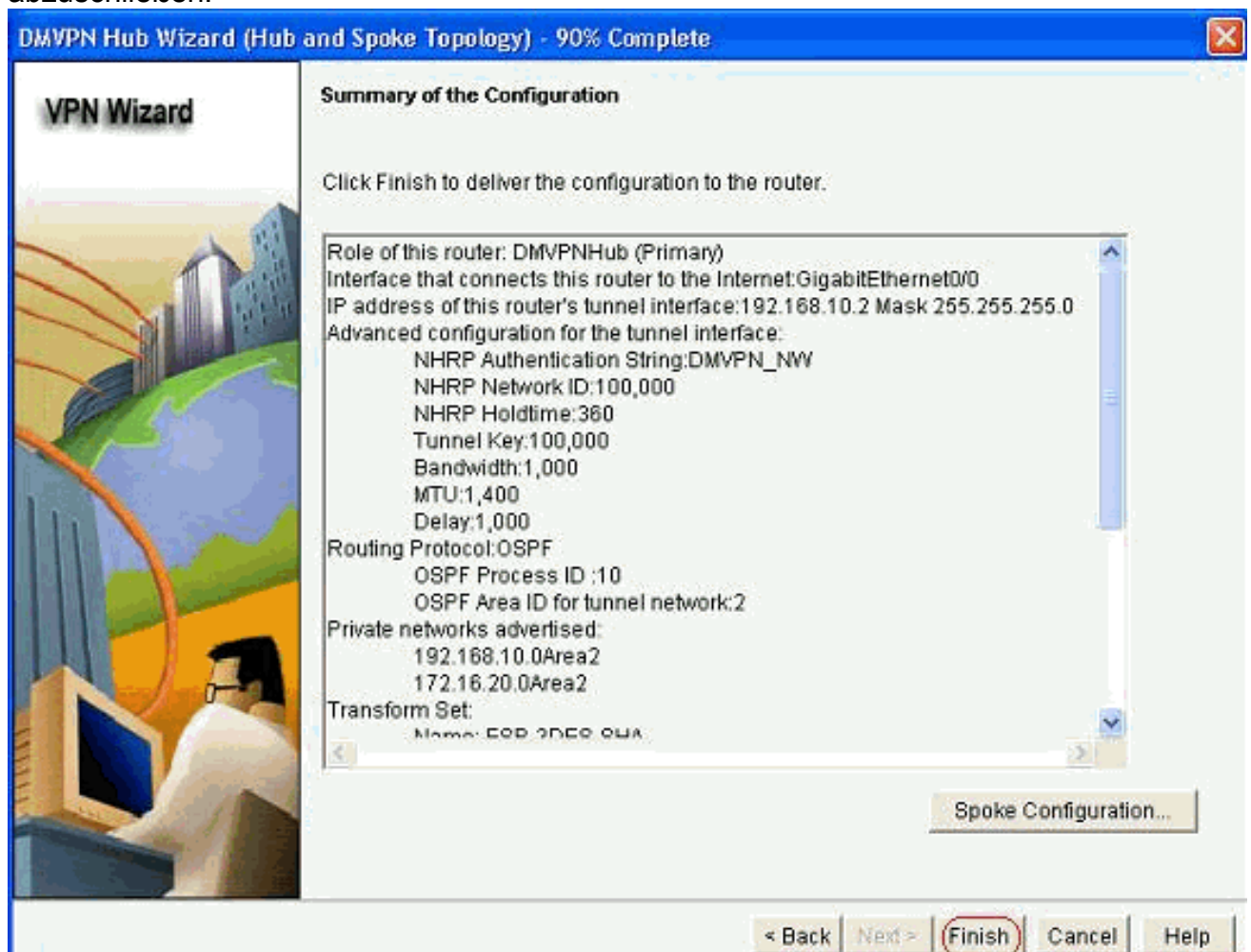
OK.

16. Fügen Sie das private Netzwerk hinter dem Hub-Router hinzu, und klicken Sie auf



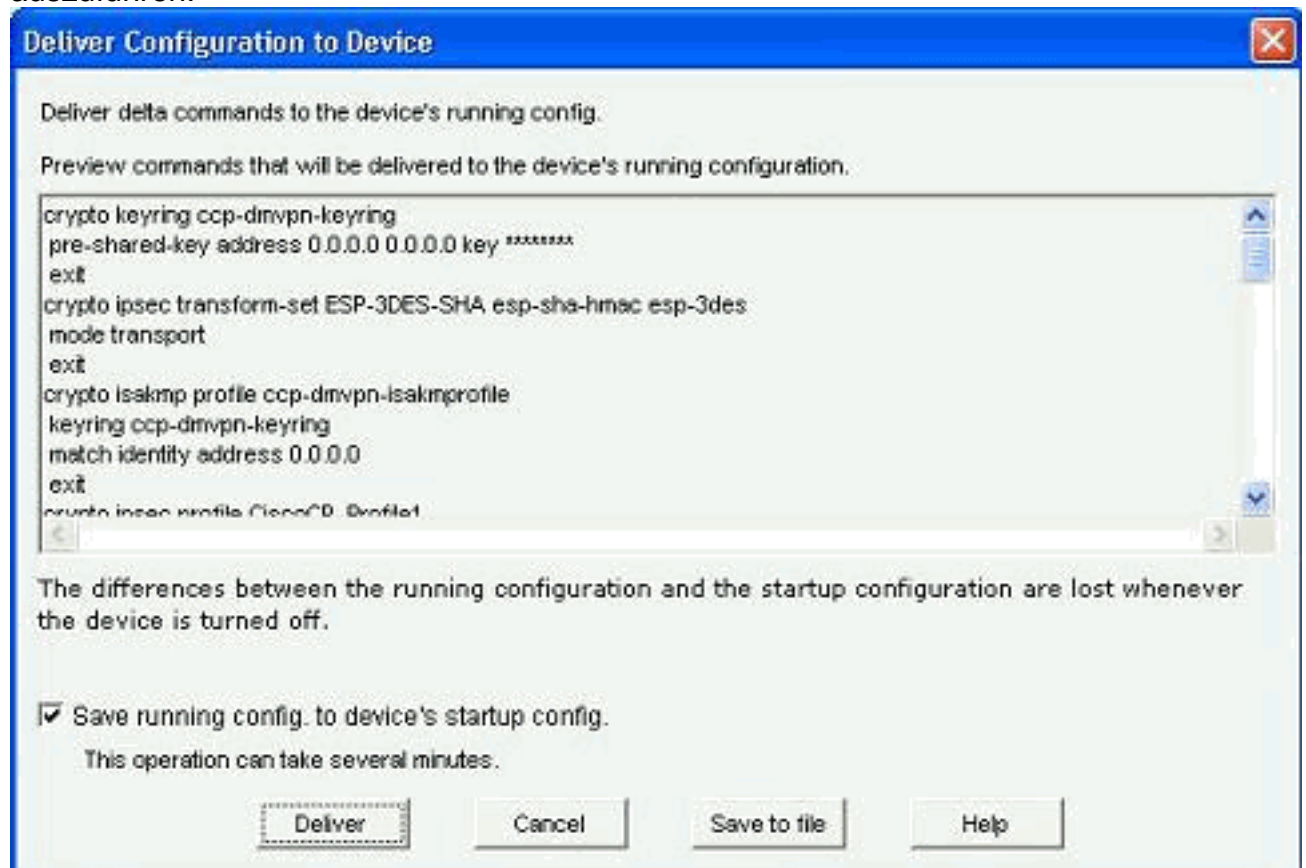
Weiter.

17. Klicken Sie auf *Fertig stellen*, um die Assistentenkonfiguration abzuschließen.



18. Klicken Sie auf *Deliver*, um die Befehle

auszuführen.



CLI-Konfiguration für Hub

Die entsprechende CLI-Konfiguration wird hier angezeigt:

```
Hub-Router
!
crypto isakmp policy 1
  encr 3des
  authentication pre-share
  group 2
!
crypto isakmp policy 2
  encr aes 192
  authentication pre-share
crypto isakmp key abcd123 address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-
sha-hmac
  mode transport
!
crypto ipsec profile CiscoCP_Profile1
  set transform-set ESP-3DES-SHA
!
interface Tunnel0
  bandwidth 1000
  ip address 192.168.10.2 255.255.255.0
  no ip redirects
  ip mtu 1400
  ip nhrp authentication DMVPN_NW
  ip nhrp map multicast dynamic
  ip nhrp network-id 100000
```



```

ip nhrp holdtime 360
ip tcp adjust-mss 1360
ip ospf network point-to-multipoint
delay 1000
tunnel source GigabitEthernet0/0
tunnel mode gre multipoint
tunnel key 100000
tunnel protection ipsec profile CiscoCP_Profile1
!
router ospf 10
 log-adjacency-changes
 network 172.16.20.0 0.0.0.255 area 2
 network 192.168.10.0 0.0.0.255 area 2
!

```

Bearbeiten der DMVPN-Konfiguration mithilfe von CCP

Sie können die vorhandenen DMVPN-Tunnelparameter manuell bearbeiten, wenn Sie die Tunnelschnittstelle auswählen und auf *Bearbeiten* klicken.

Configure > Security > VPN > Dynamic Multipoint VPN

VPN

Create Dynamic Multipoint VPN (DMVPN) **Edit Dynamic Multipoint VPN (DMVPN)**

Add... **Edit...** Delete

Interface	IPSec Profile	IP Address	Description
Tunnel0	CiscoCP_Profile1	192.168.10.2	<None>

Details for interface Tunnel0:

Item Name	Item Value
Interface	Tunnel0
IPSec Profile	CiscoCP_Profile1
IP Address	192.168.10.2
Description	<None>
Tunnel Bandwidth	1000
MTU	1400
NHRP Authentication	DMVPN_NW
NHRP Network ID	100000
NHRP Hold Time	360
Delay{0}	1000

Tunnel-Schnittstellenparameter wie MTU und Tunnel-Schlüssel werden auf der Registerkarte *Allgemein* geändert.

The image shows a screenshot of the "DMVPN Tunnel Configuration" dialog box. The "General" tab is selected, and the "NHRP" sub-tab is active. The configuration fields are as follows:

- IP address: 192.168.10.2
- Mask: 255.255.255.0, with a dropdown set to 24
- Tunnel Source:
 - Interface: GigabitEthernet0/0
 - IP address: (empty)
- Tunnel Destination:
 - This is an multipoint GRE Tunnel
 - IP / Hostname: (empty)
- IPSec Profile: CiscoCP_Profi (dropdown), with an "Add..." button
- MTU: 1400
- Bandwidth: 1000
- Delay: 1000
- Tunnel Key: 100000

At the bottom, there are three buttons: "OK", "Cancel", and "Help".

1. NHRP-bezogene Parameter werden gemäß den Anforderungen auf der Registerkarte *NHRP* gefunden und geändert. Bei einem Spoke-Router sollten Sie den NHS als IP-Adresse des Hub-Routers anzeigen können. Klicken Sie im Abschnitt NHRP-Karte auf *Hinzufügen*, um die

DMVPN Tunnel Configuration

General **NHRP** Routing

Authentication String: DMVPN_MV

Hold Time: 360

Network ID: 100000

Next Hop Servers

Next Hop Servers

Add

Delete

NHRP Map

Destination	Mask
<None>	<None>

Add

Edit

Delete

< 0 >

OK Cancel Help

NHRP-Zuordnung hinzuzufügen.

2. Je nach Netzwerkeinrichtung können die NHRP-Zuordnungsparameter wie folgt konfiguriert

NHRP Map Configuration

Statically configure the IP-to-NBMA address mapping of IP destinations connected to a NBMA network.

Destination reachable through NBMA network

IP Address:

Mask (Optional):

NBMA address directly reachable

IP Address:

Configure NBMA addresses used as destinations for broadcast or multicast packets to be sent over a tunnel network.

Dynamically add spokes' IP addresses to hub's multicast cache

IP address of NBMA address directly reachable

OK Cancel Help

werden:

Die Routingparameter werden auf der Registerkarte *Routing* angezeigt und geändert.



Weitere Informationen

Die DMVPN-Tunnel werden auf zwei Arten konfiguriert:

- Spoke-to-Spoke-Kommunikation über den Hub
- Spoke-to-Spoke-Kommunikation ohne Hub

In diesem Dokument wird nur die erste Methode behandelt. Um die Einrichtung von Spoke-to-Spoke-dynamischen IPSec-Tunneln zu ermöglichen, wird dieser Ansatz verwendet, um die Spoke-to-Spoke-Topologie der DMVPN-Cloud hinzuzufügen:

1. Starten Sie den DMVPN-Assistenten, und wählen Sie die Option *Spoke-Konfiguration aus*.
2. Wählen Sie im Fenster *DMVPN-Netzwerktopologie* die Option *Full Meshed Network* (Vollvernetztes Netzwerk) anstelle der Option *Hub and Spoke* (Hub- und Spoke-Netzwerk) *aus*.

DMVPN Spoke Wizard - 10% Complete

VPN Wizard

DMVPN Network Topology

Select the DMVPN network topology.

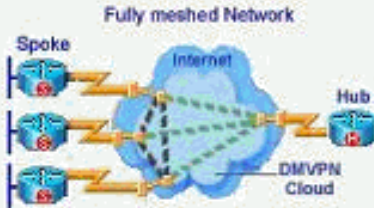
Hub and Spoke network

In this topology, all DMVPN traffic is routed through the hub. A point-to-point GRE interface will be configured on the spoke, and the spoke will use it to create a tunnel to the hub which will remain up. Spokes do not create GRE tunnels to other spokes in this topology.

Fully meshed network

In this topology, the spoke dynamically establishes a direct tunnel to another spoke device, and sends DMVPN traffic directly to it. A multipoint GRE tunnel interface is configured on the spoke to support this functionality.

Note: Cisco supports fully meshed DMVPN networks only in the following Cisco IOS images: 12.3(8)T1 and 12.3(9) or later.



< Back Next > Finish Cancel Help

- Schließen Sie die restliche Konfiguration mit den gleichen Schritten wie die anderen Konfigurationen in diesem Dokument ab.

Überprüfung

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Zugehörige Informationen

- [Cisco Dynamic Multipoint VPN: Einfache und sichere Kommunikation zwischen Zweigstellen](#)
- [IOS 12.2 Dynamic Multipoint VPN \(DMVPN\)](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)