

Cisco IOS/CCP — 使用Cisco CP配置DMVPN

目錄

[簡介](#)

[必要條件](#)

[需求](#)

[採用元件](#)

[慣例](#)

[背景資訊](#)

[設定](#)

[網路圖表](#)

[使用Cisco CP的分支配置](#)

[分支的CLI配置](#)

[使用Cisco CP的集線器配置](#)

[集線器的CLI配置](#)

[使用CCP編輯DMVPN配置](#)

[更多資訊](#)

[驗證](#)

[相關資訊](#)

簡介

本文檔提供使用Cisco Configuration Professional(Cisco CP)在中心路由器與分支路由器之間配置動態多點VPN(DMVPN)隧道的示例。動態多點VPN技術整合了GRE、IPSec加密、NHRP和路由等不同概念，可提供複雜的解決方案，使終端使用者能夠通過動態建立的輻條到輻條IPSec隧道進行有效通訊。

必要條件

需求

要獲得最佳DMVPN功能，建議您運行Cisco IOS®軟體版本12.4 mainline、12.4T及更高版本。

採用元件

本文中的資訊係根據以下軟體和硬體版本：

- 採用軟體版本12.4(22)的Cisco IOS路由器3800系列
- 採用軟體版本12.3(8)的Cisco IOS路由器1800系列
- 思科組態專業版2.5

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設

) 的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

慣例

請參閱[思科技術提示慣例](#)以瞭解更多有關文件慣例的資訊。

背景資訊

本文檔提供有關如何使用Cisco CP將路由器配置為分支路由器並將另一路由器配置為集線器的資訊。最初顯示輻條配置，但稍後在文檔中會詳細顯示與集線器相關的配置，以便更好地理解。也可使用類似的方法配置其它輻條以連線到集線器。當前方案使用以下引數：

- 集線器路由器公共網路 — 209.165.201.0
- 隧道網路 — 192.168.10.0
- 使用的路由協定 — OSPF

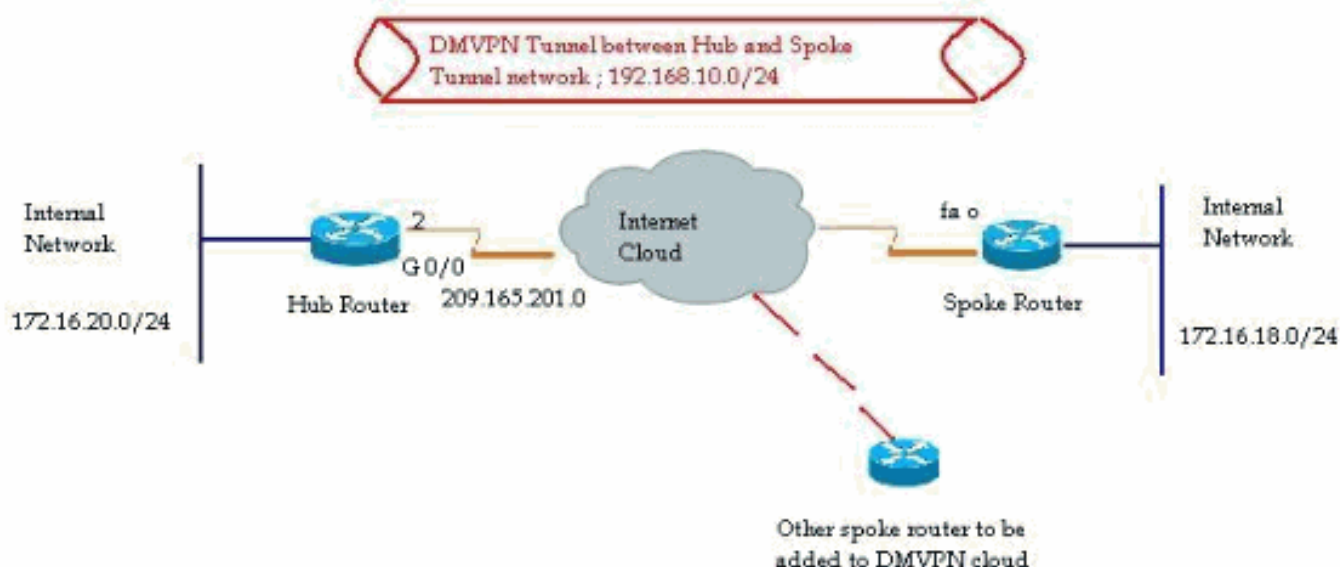
設定

本節提供用於設定本文件中所述功能的資訊。

註：使用[Command Lookup Tool](#)([僅供已註冊客戶使用](#))可獲取本節中使用的命令的詳細資訊。

網路圖表

本檔案會使用以下網路設定：



使用Cisco CP的分支配置

本節介紹如何使用Cisco Configuration Professional中的分步DMVPN嚮導將路由器配置為分支。

1. 要啟動Cisco CP應用並啟動DMVPN嚮導，請轉至 *Configure > Security > VPN > Dynamic Multipoint VPN*。然後，選擇在DMVPN中建立輻條選項，然後單擊Launch the selected

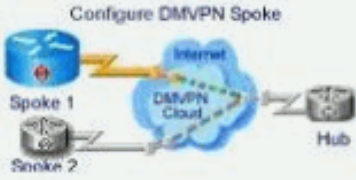
task.

Configure > Security > VPN > Dynamic Multipoint VPN

VPN

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

Configure DMVPN Spoke



The diagram illustrates a DMVPN network topology. It features two spokes, Spoke 1 and Spoke 2, connected to a central DMVPN Cloud. The cloud is connected to the Internet and a Hub. Spoke 1 is shown as a blue router icon, Spoke 2 as a grey router icon, and the Hub as a grey router icon. The Internet is represented by a blue cloud icon.

Create a spoke (client) in a DMVPN

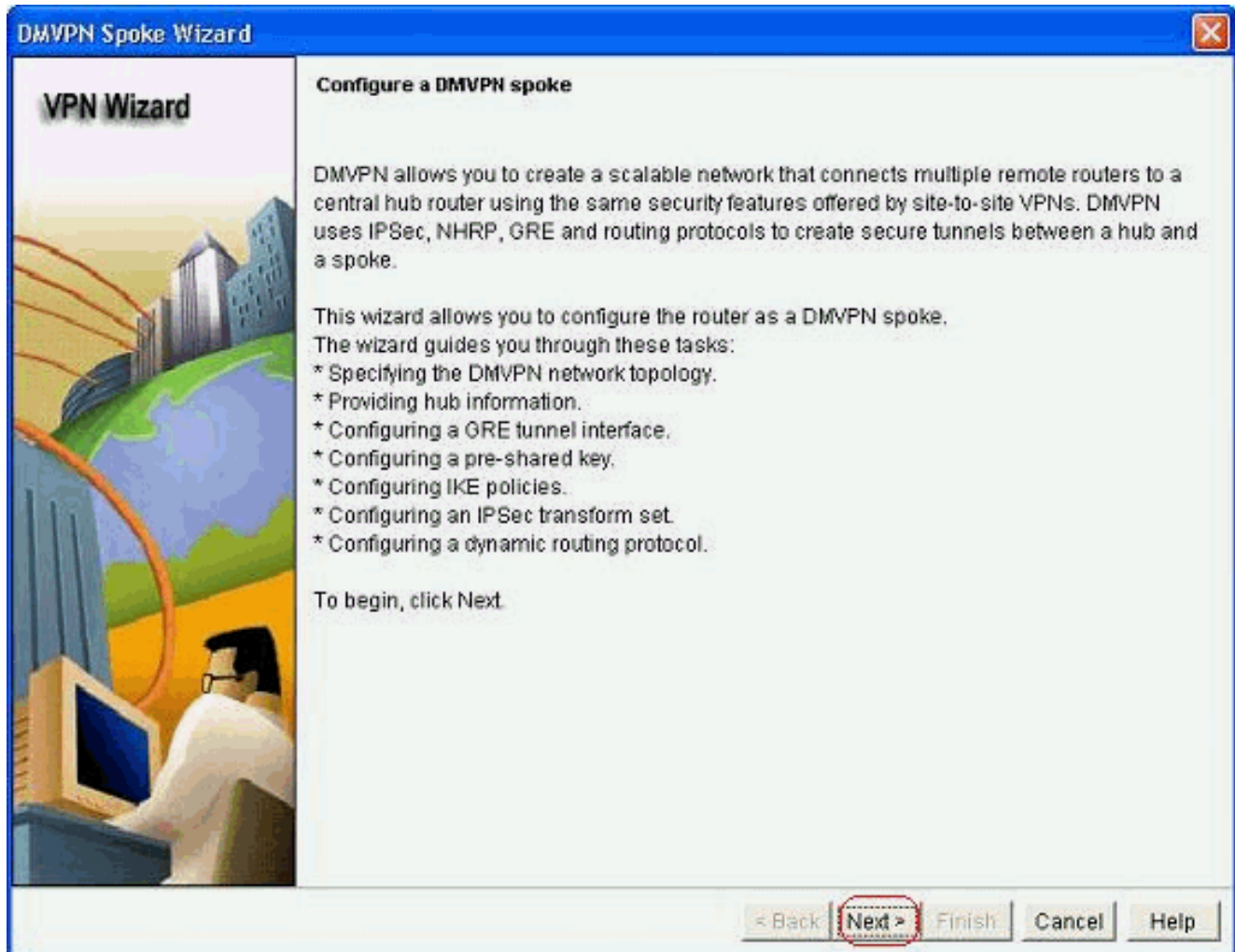
Use this option to configure the router as a spoke in a full mesh or hub and spoke network topology. To complete this configuration, you must know the hub's IP address, NHRP information, pre-shared key, IKE policy, IPSec Transform set and dynamic routing protocol information.

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. 按一下Next開始。



3. 選擇 *Hub and Spoke network* 選項，然後按一下 *Next*。

VPN Wizard



DMVPN Network Topology

Select the DMVPN network topology.

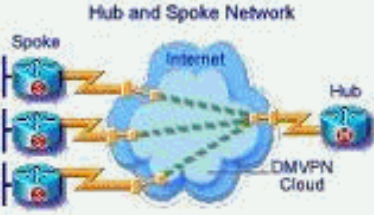
Hub and Spoke network

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. 指定與集線器相關的資訊，例如集線器路由器的公共介面和集線器路由器的隧道介面。

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.

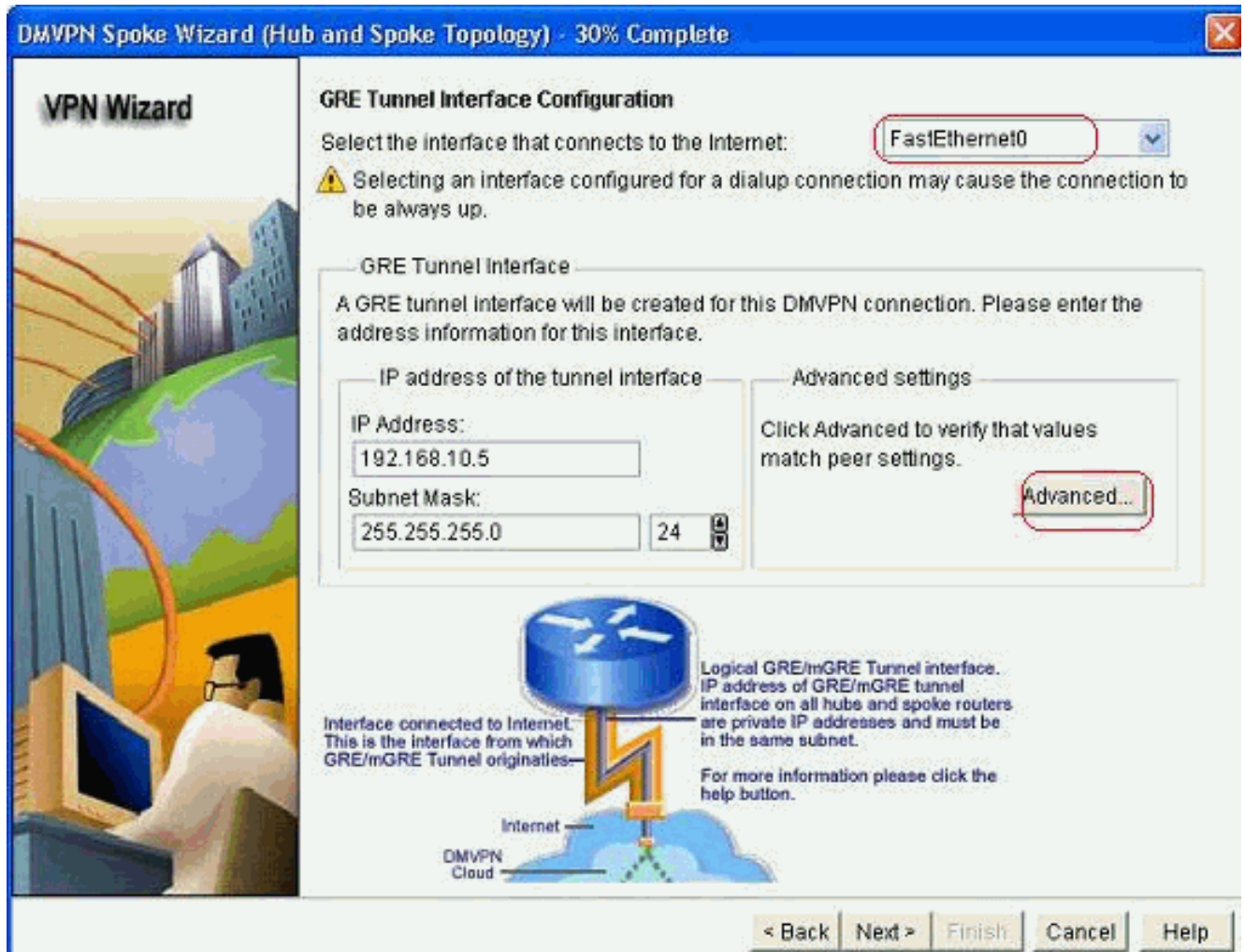
Hub Information

IP address of hub's physical interface:

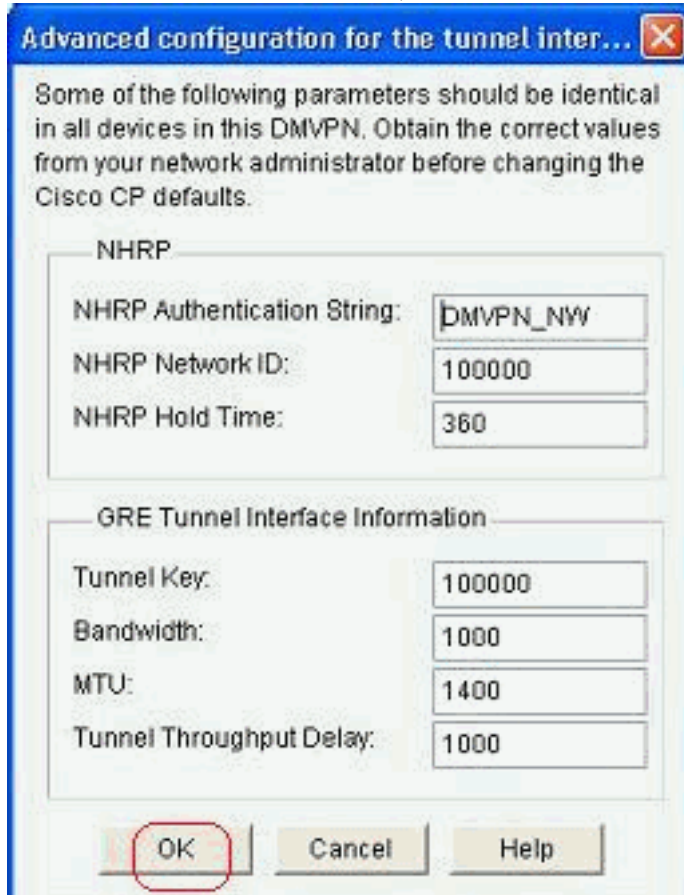
IP address of hub's mGRE tunnel interface:

< Back **Next >** Finish Cancel Help

5. 指定分支的隧道介面詳細資訊和分支的公共介面。然後按一下 *Advanced*。



6. 驗證隧道引數和NHRP引數，並確保它們與Hub引數完全匹配。



7. 指定預共用金鑰並按一下下一步。



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

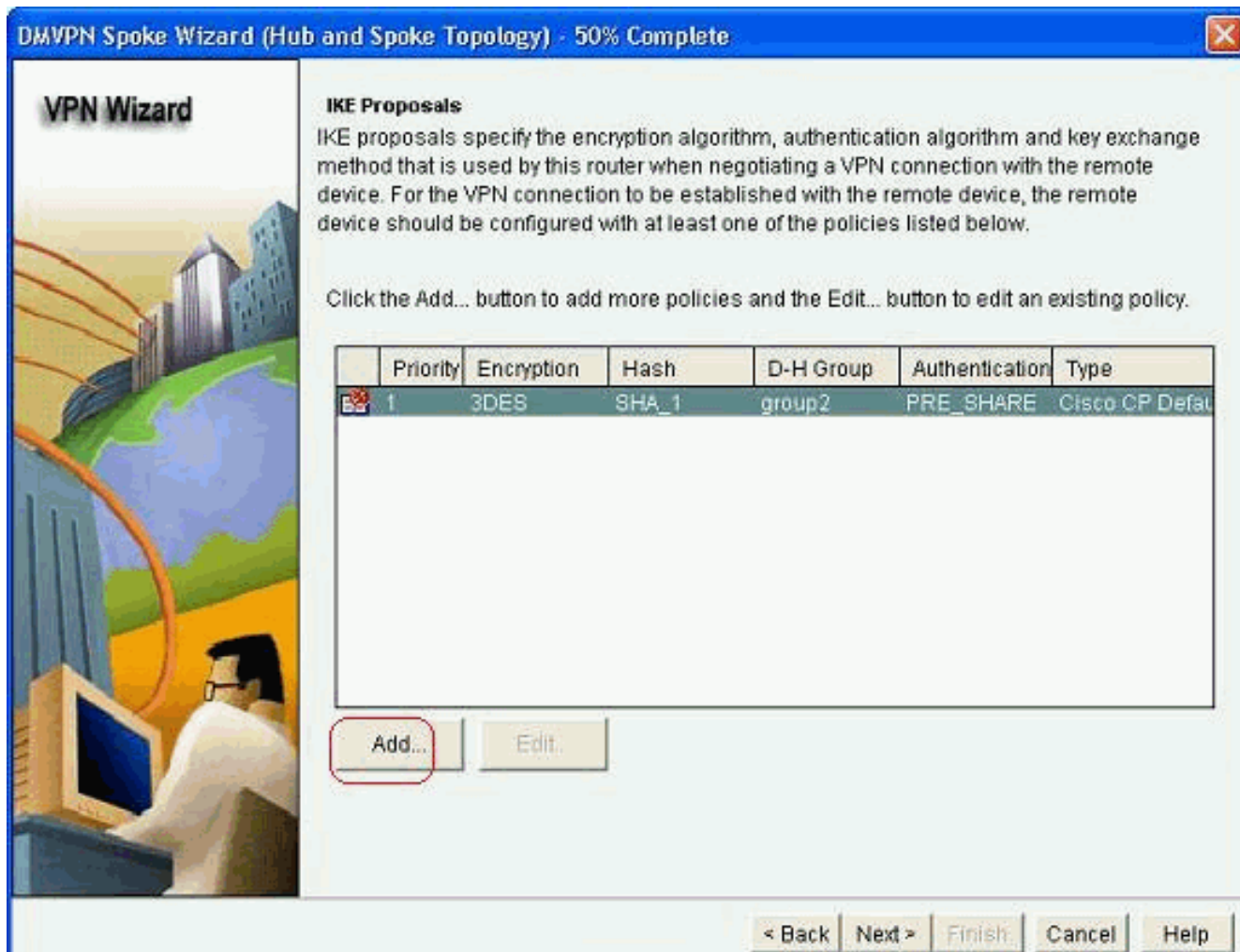
Pre-shared Keys

pre-shared key:

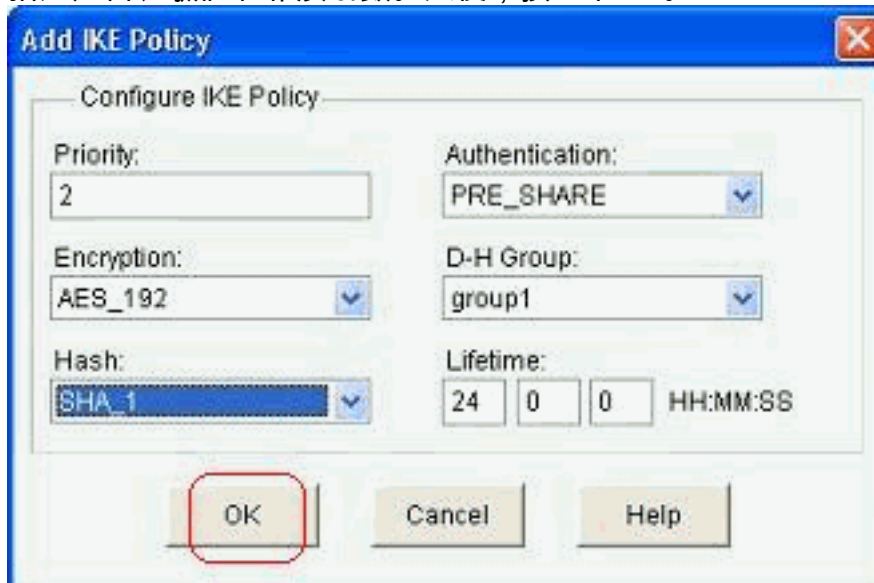
Reenter key:

< Back **Next** > Finish Cancel Help

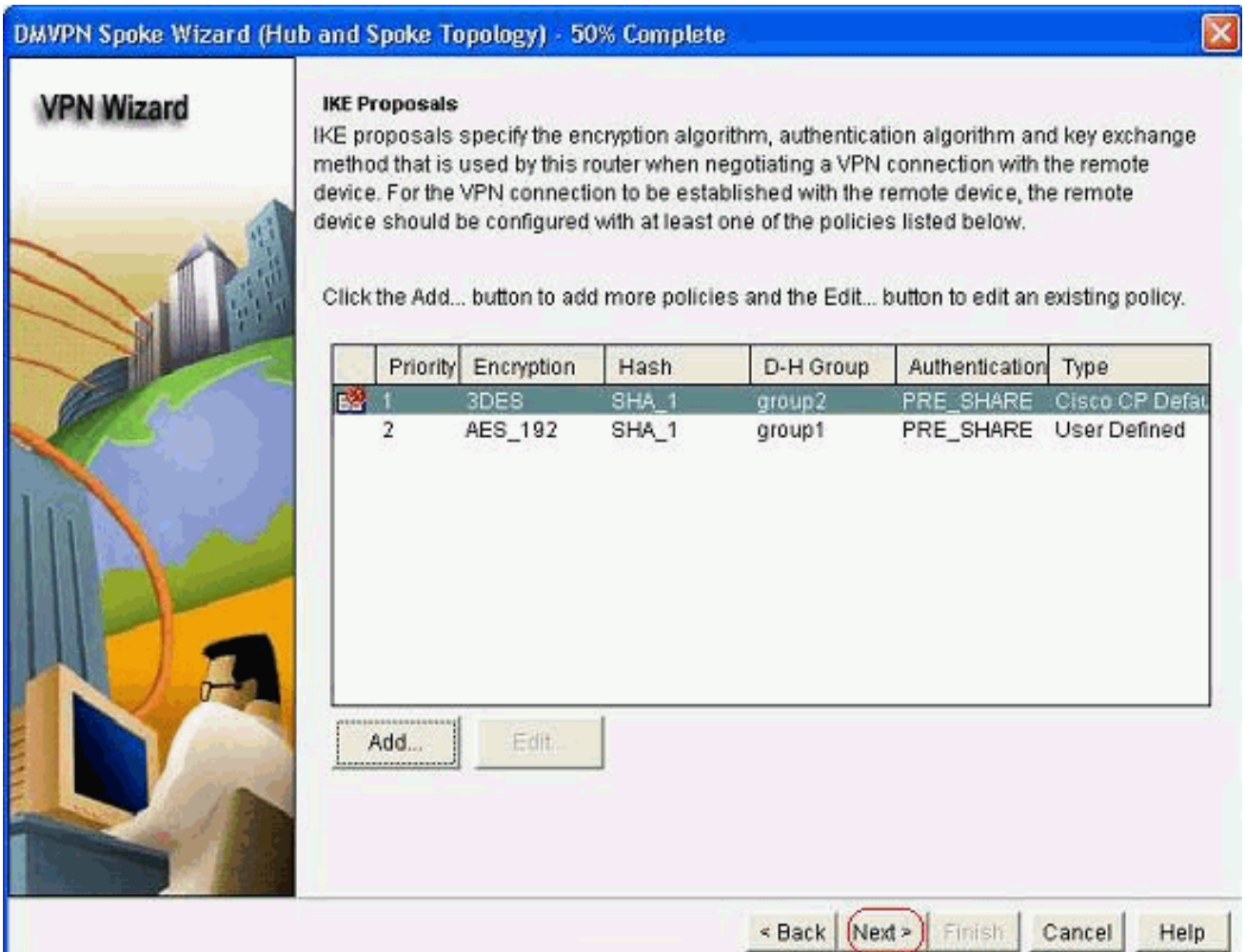
8. 按一下 *Add* 以新增單獨的IKE提議。



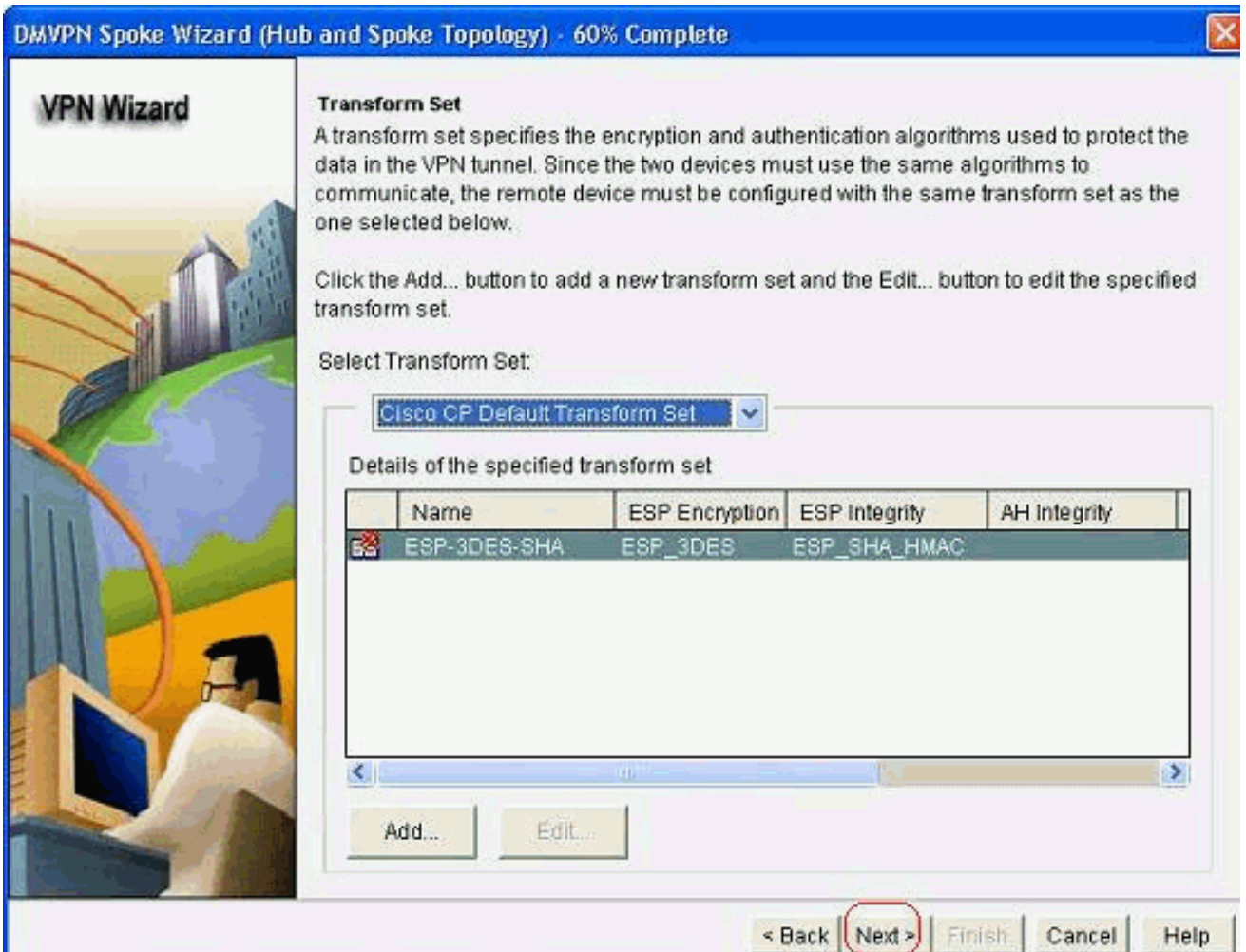
9. 指定加密、驗證和雜湊引數。然後，按一下OK。



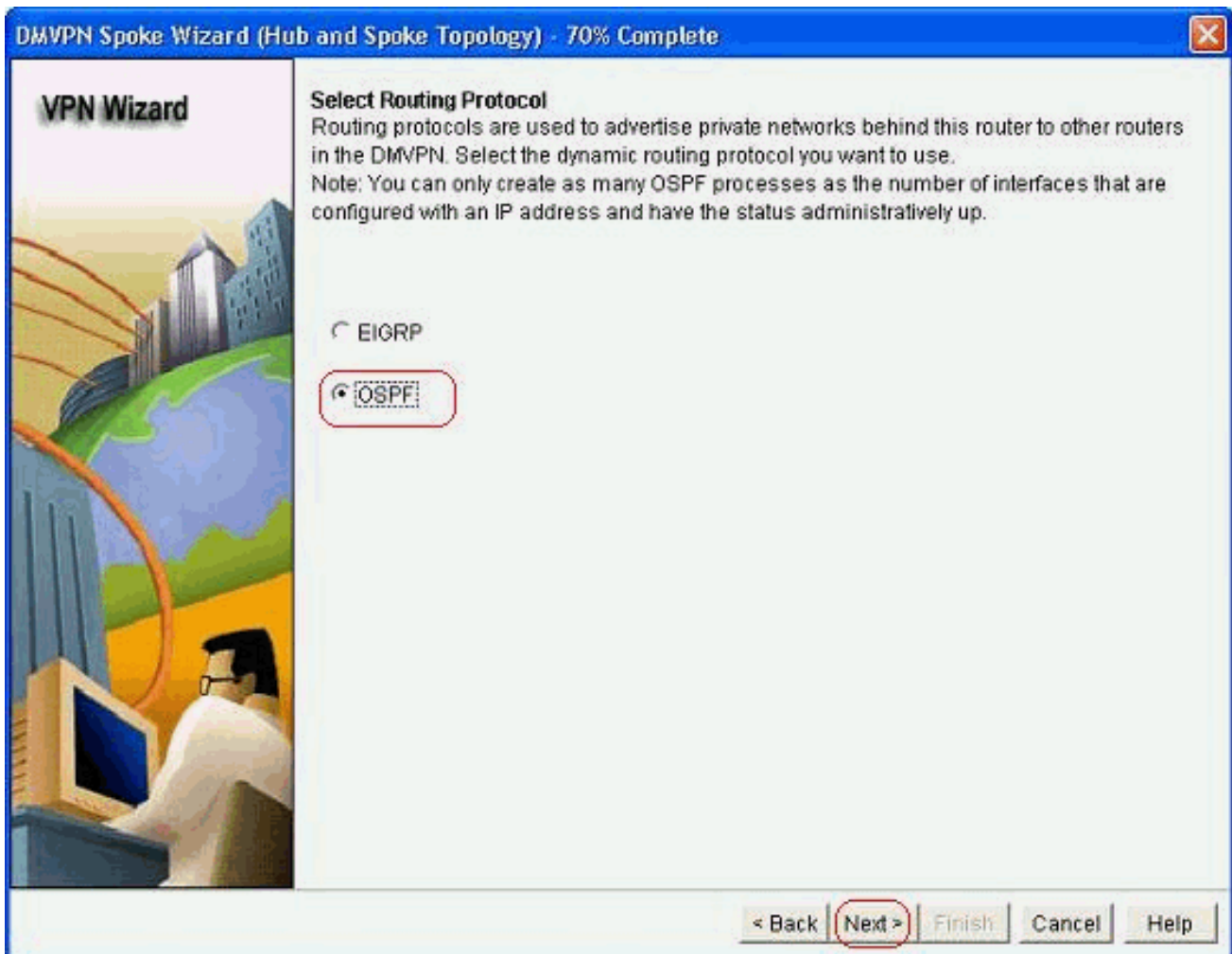
10. 此處可以看到新建立的IKE策略。按「Next」（下一步）。



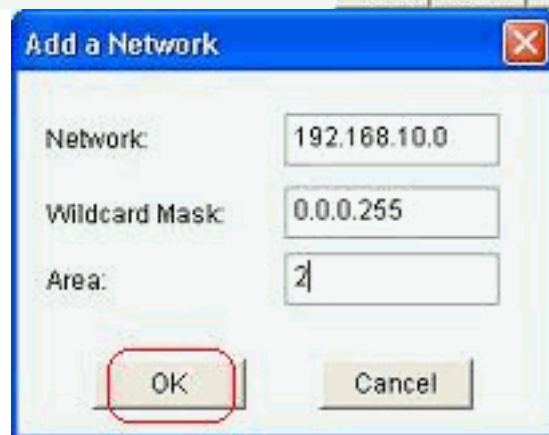
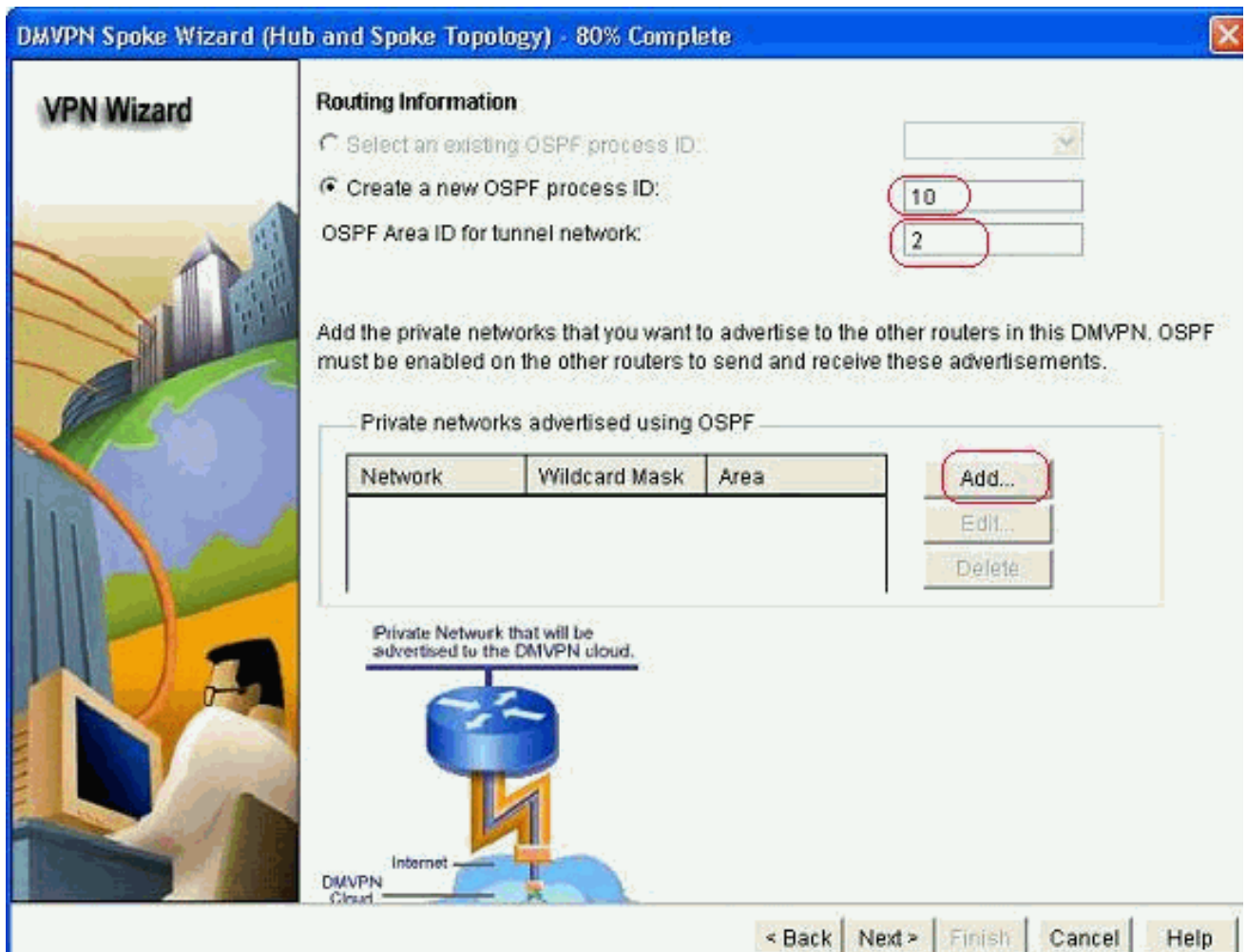
11. 按一下下一步繼續使用預設轉換集。



12. 選擇所需的路由協定。此處選擇了OSPF。

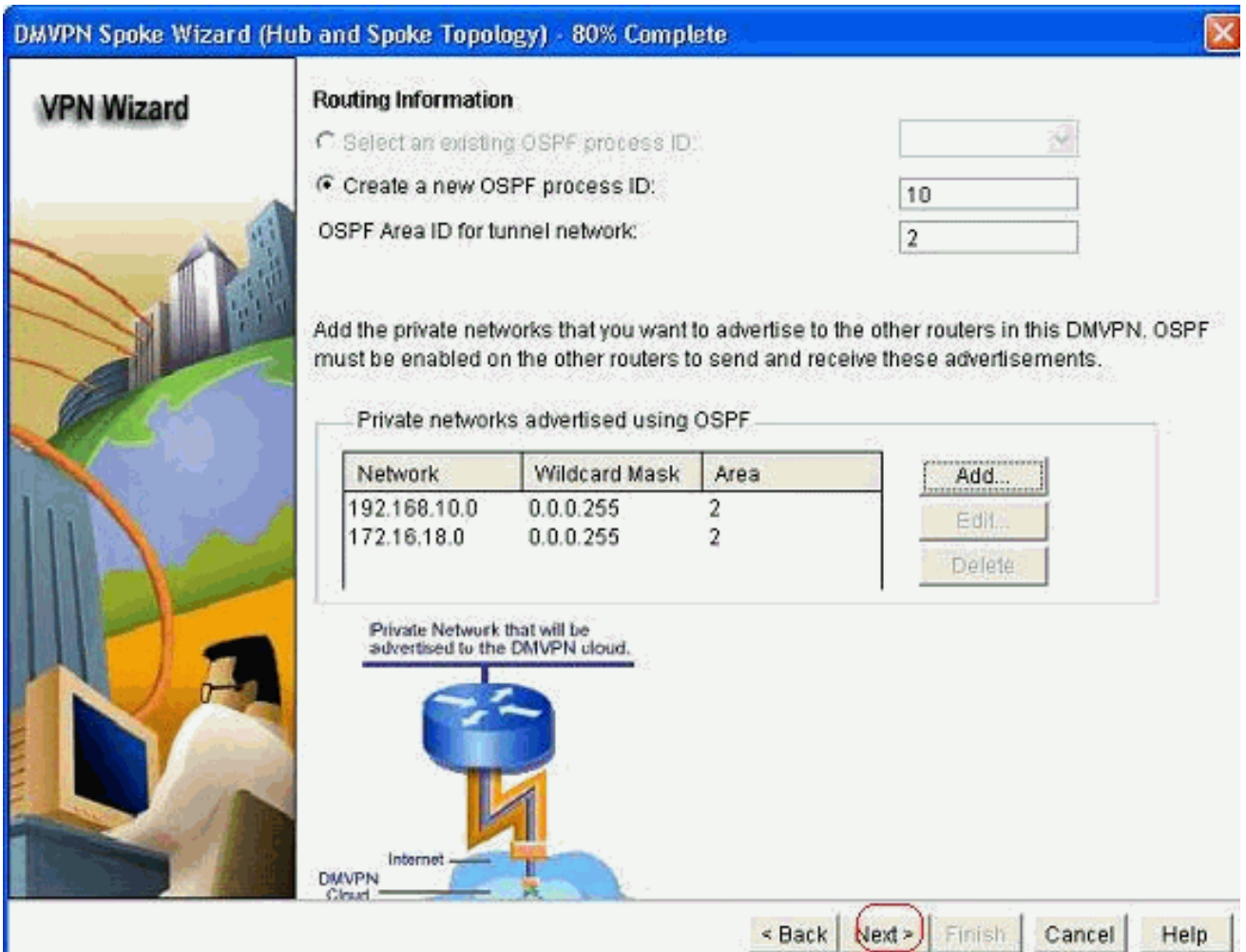


13. 指定OSPF進程ID和區域ID。按一下Add以新增要由OSPF通告的網路。

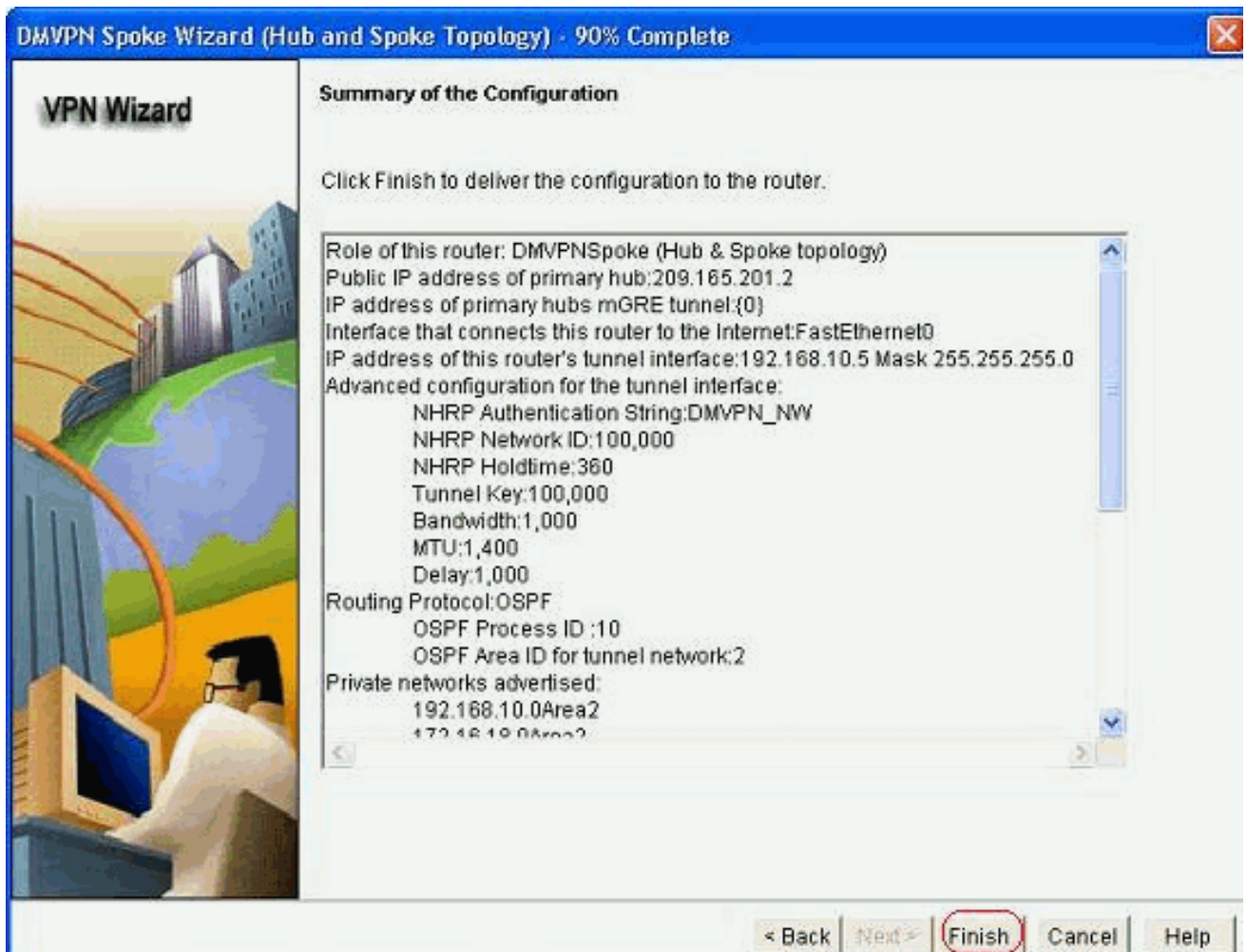


14. 新增隧道網路，然後按一下OK。

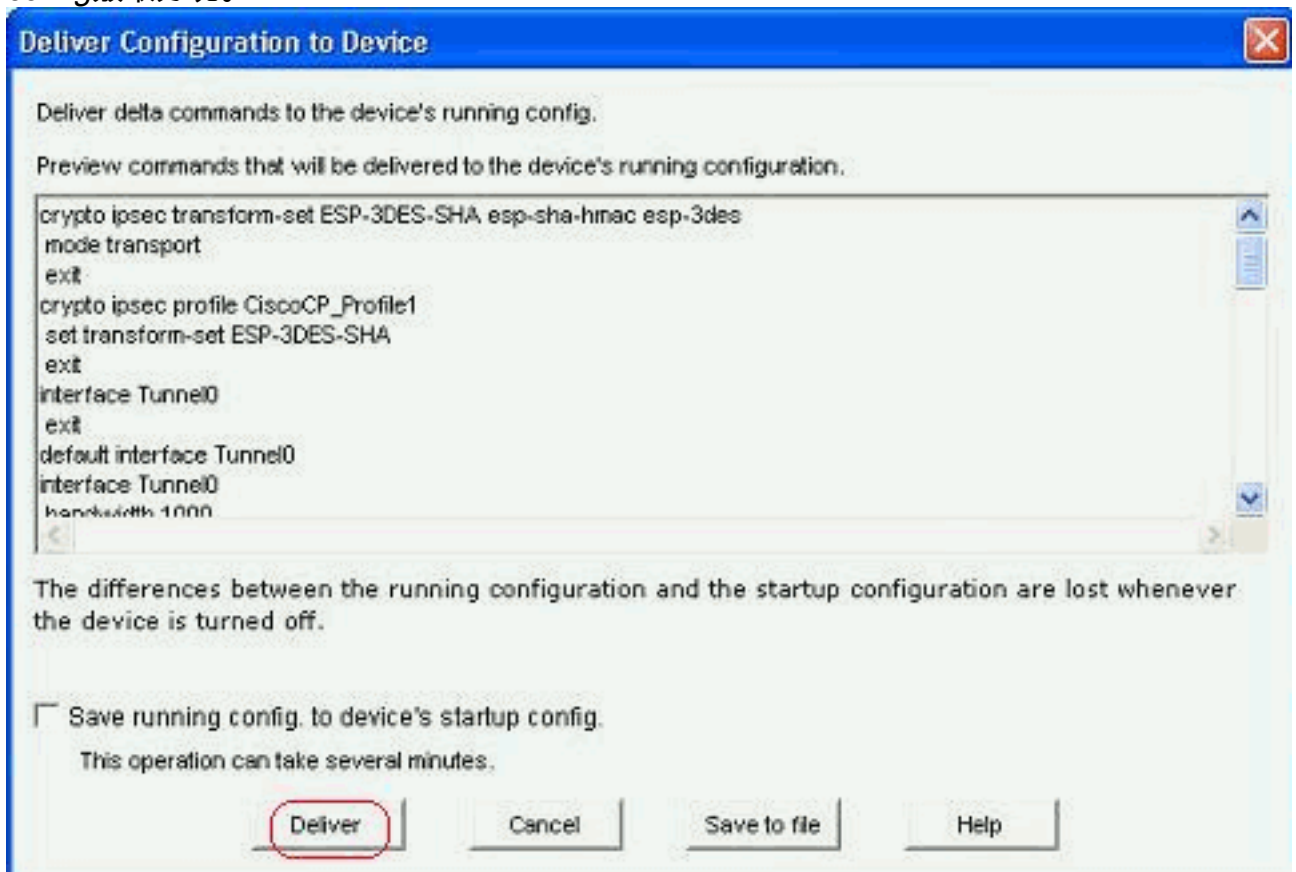
15. 在分支路由器後面新增專用網路。然後，按一下下一步。



16. 按一下完成完成嚮導配置。



17. 按一下 *Deliver* 執行命令。如果要儲存配置，請選中 *Save running config to device's startup config* 覈取方塊。



相關CLI配置如下所示：

分支路由器

```
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
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
```

使用Cisco CP的集線器配置

本節介紹了如何為DMVPN配置中心路由器的逐步方法。

1. 轉至 *Configure > Security > VPN > Dynamic Multipoint VPN*，然後選擇 *Create a hub in a DMVPN* 選項。，按一下 *Launch the selected task*。



Create Dynamic Multipoint VPN (DMVPN)

Edit Dynamic Multipoint VPN (DMVPN)

 Create a spoke (client) in a DMVPN

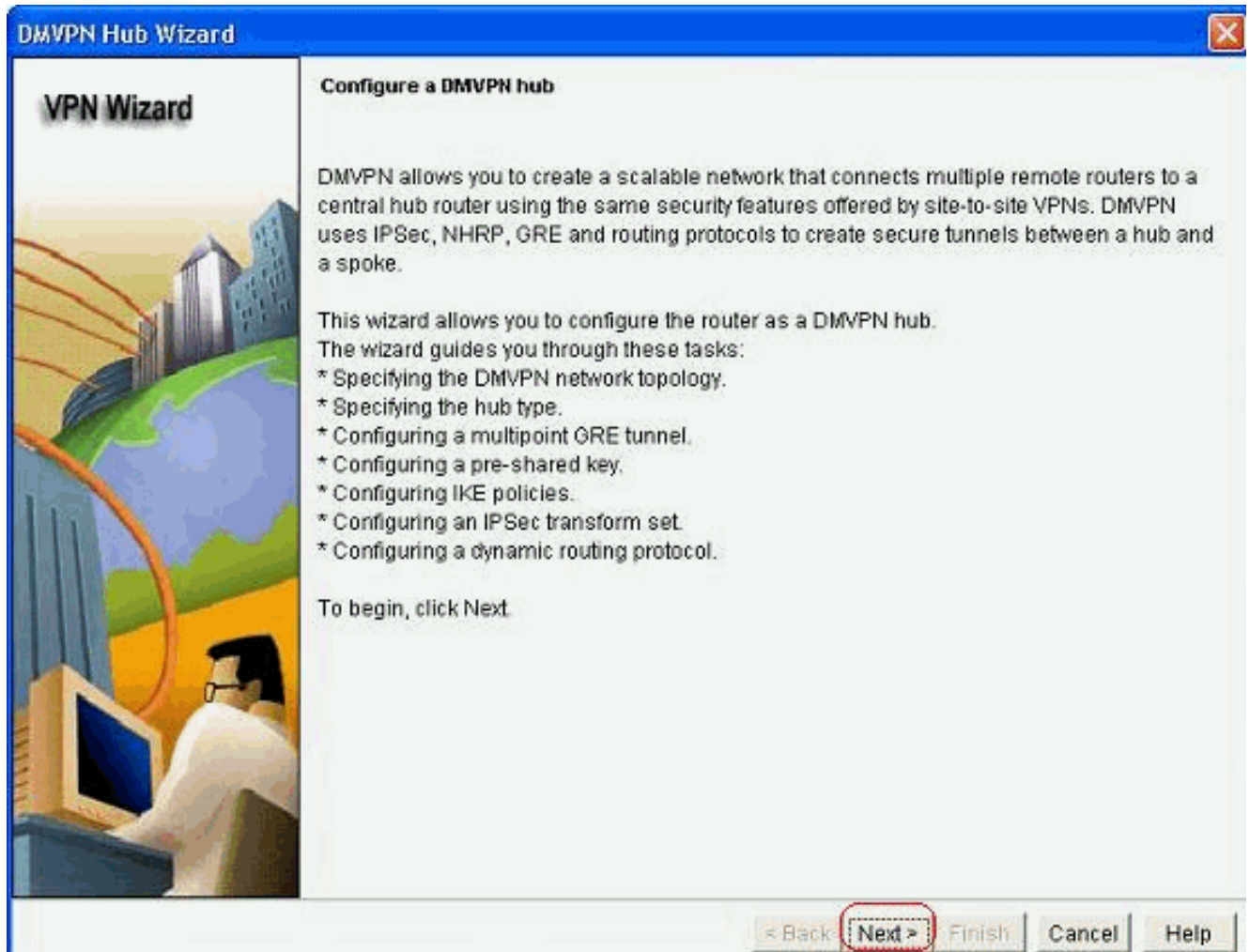
Use this option to configure the router as a spoke in a full mesh or hub and spoke network topology. To complete this configuration, you must know the hub's IP address, NHRP information, pre-shared key, IKE policy, IPsec Transform set and dynamic routing protocol information.

 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. 按「Next」(下一步)。



3. 選擇 *Hub and Spoke network* 選項，然後按一下 *Next*。

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. 選擇 *Primary Hub*。然後，按一下下一步。

VPN Wizard



Type of Hub
In a DMVPN network there will be a hub router and multiple spoke routers connecting to the hub. You can also configure multiple routers as hubs. The additional routers will act as backups. Select the type of hub you want to configure this router as.


Primary hub

Backup Hub (Cisco CP does not support backup hub configuration on this router)

< Back **Next >** Finish Cancel Help

5. 指定Tunnel介面引數，然後按一下*Advanced*。

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...



Interface connected to Internet. This is the interface from which GRE/mGRE Tunnel originates.

Logical GRE/mGRE Tunnel interface. IP address of GRE/mGRE tunnel interface on all hubs and spoke routers are private IP addresses and must be in the same subnet.

For more information please click the help button.

6. 指定隧道引數和NHRP引數。然後，按一下OK。

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:

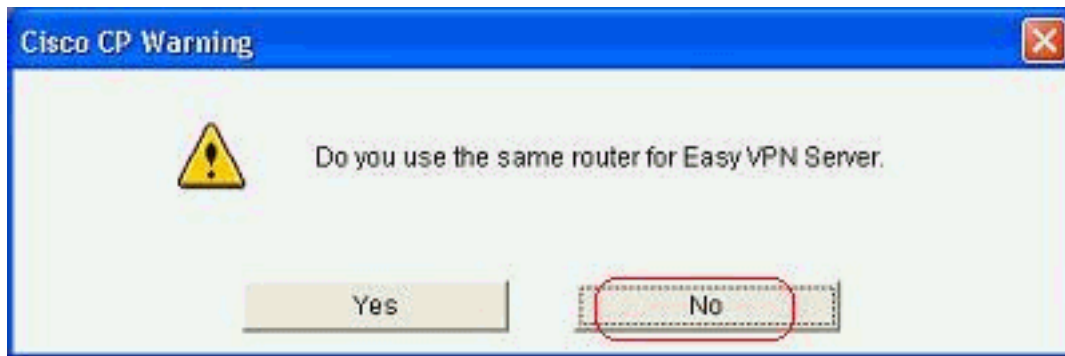
Bandwidth:

MTU:

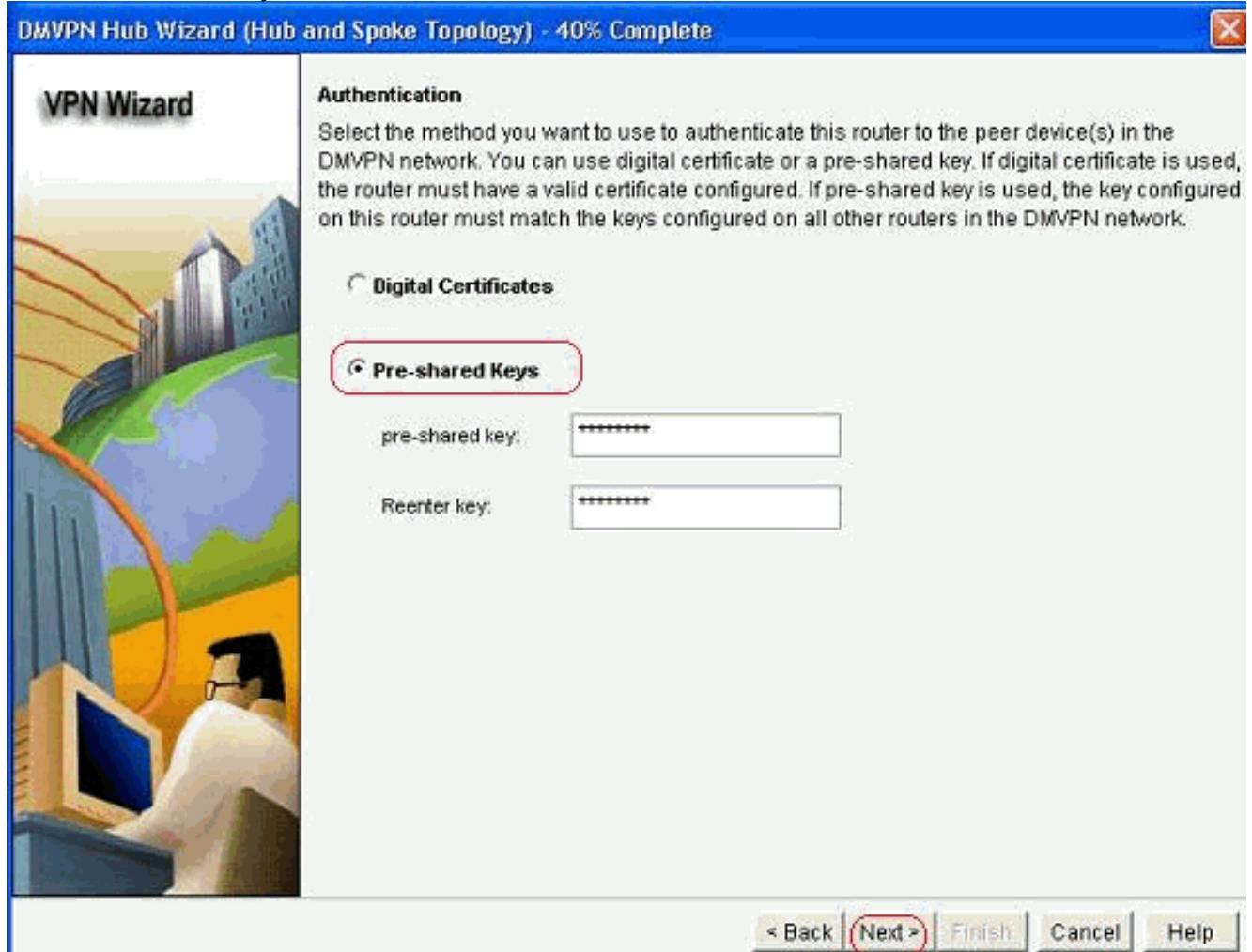
Tunnel Throughput Delay:

OK
Cancel
Help

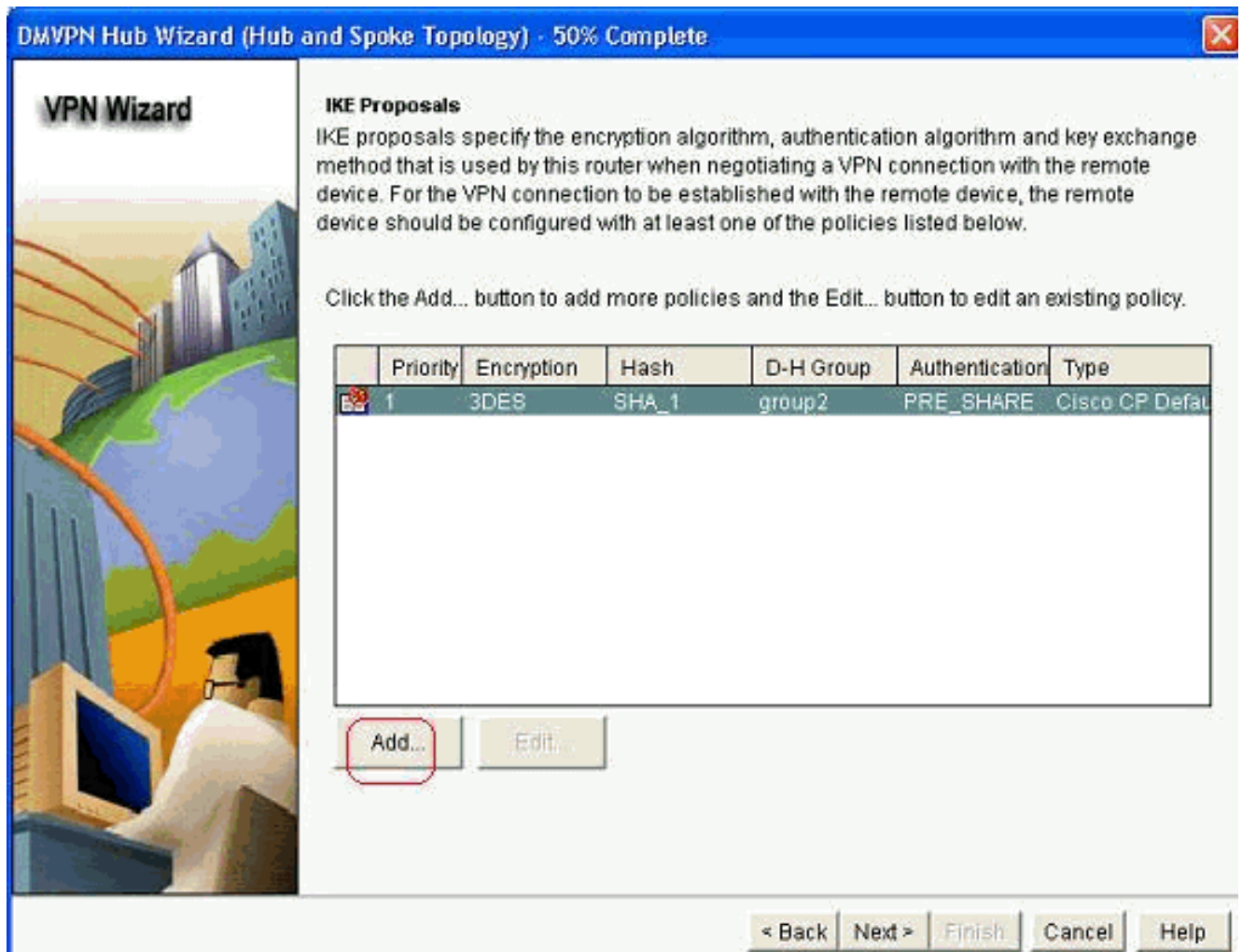
7. 根據您的網路設定指定選項。



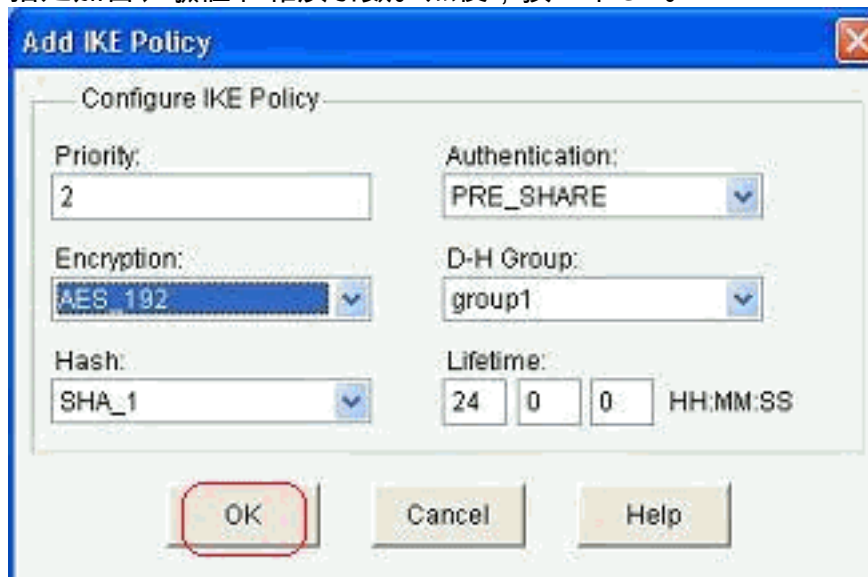
8. 選擇 *Pre-shared Keys* 並指定預共用金鑰。然後，按一下下一步。



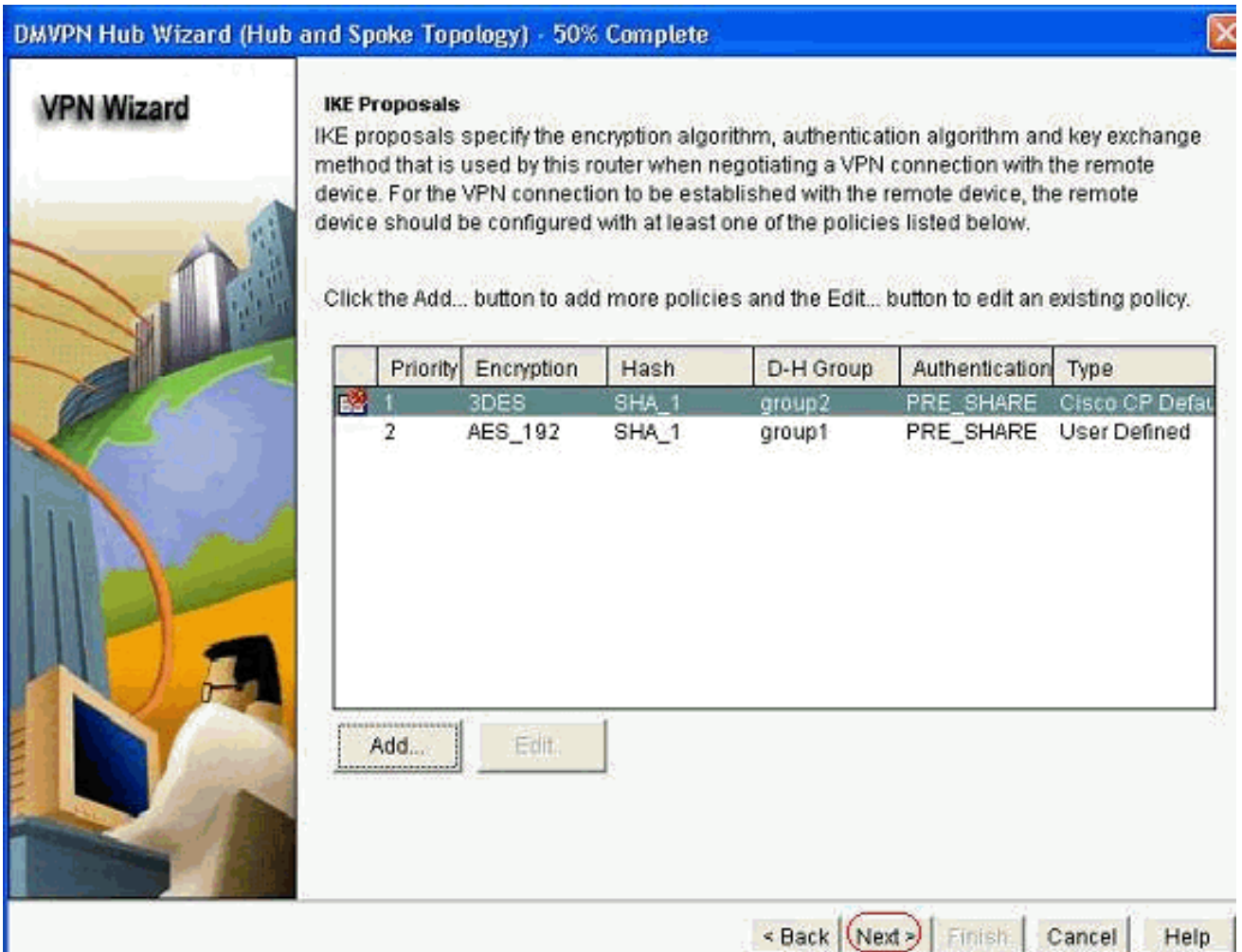
9. 按一下 *Add* 以新增單獨的IKE提議。



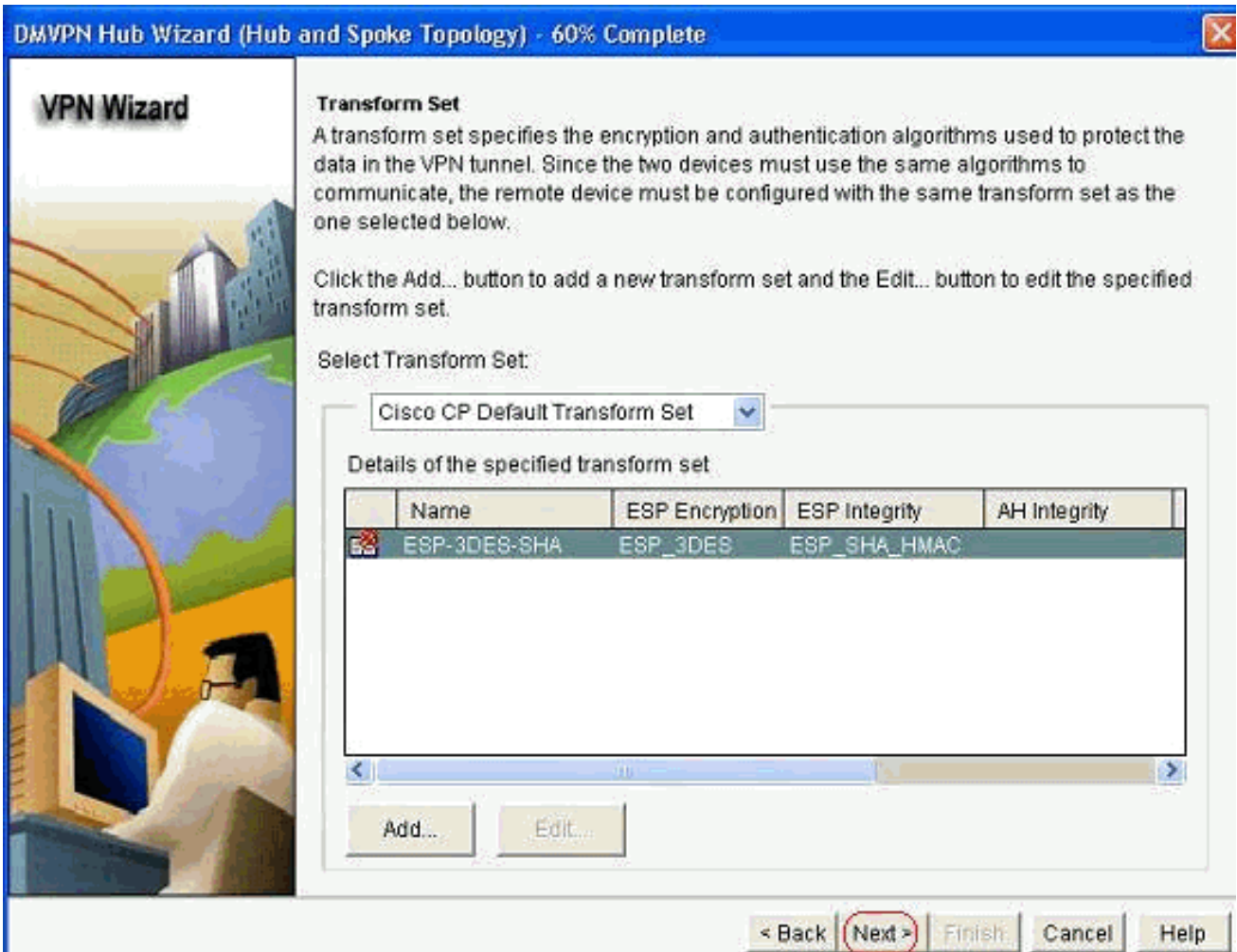
10. 指定加密、驗證和雜湊引數。然後，按一下OK。



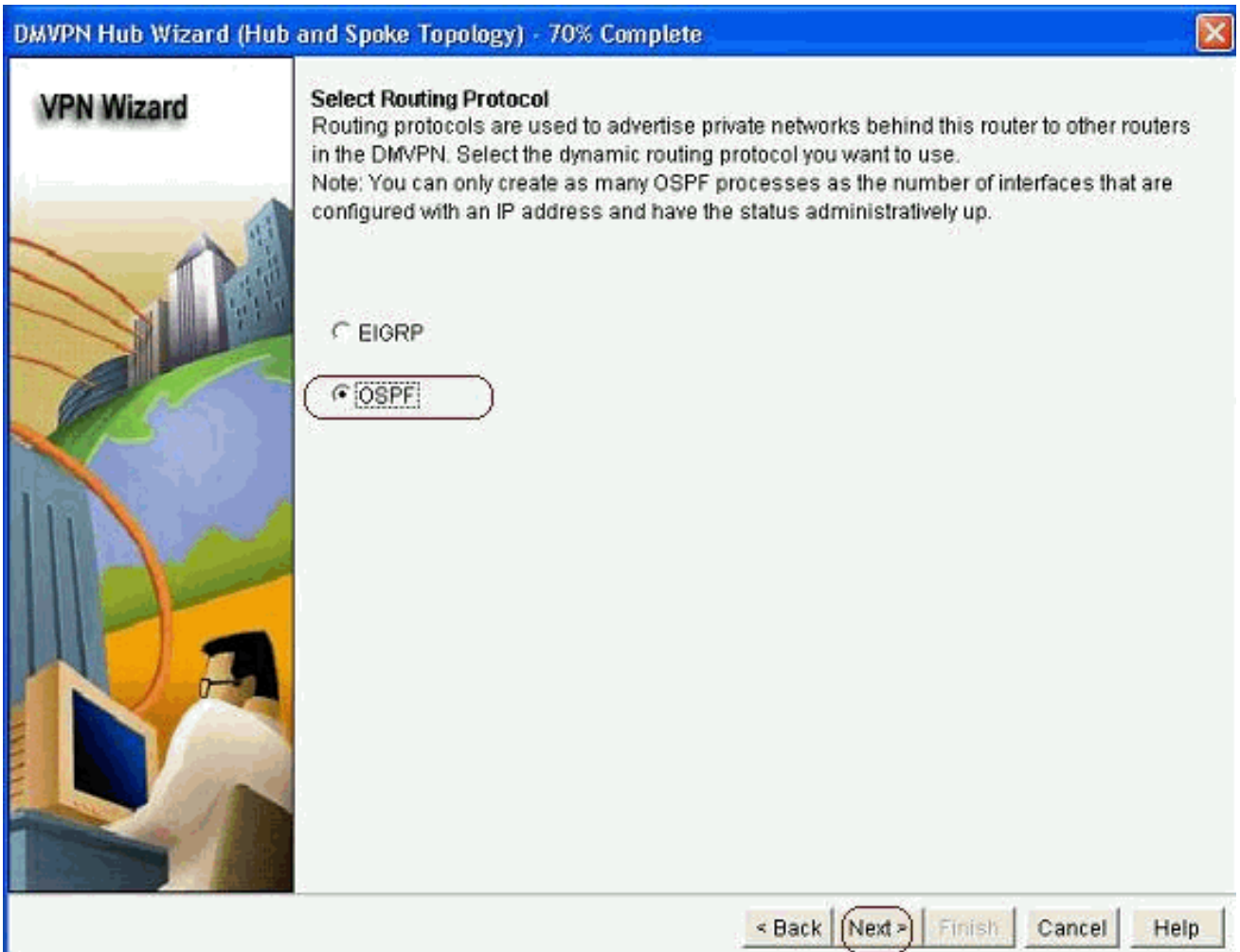
11. 此處可以看到新建立的IKE策略。按「Next」（下一步）。



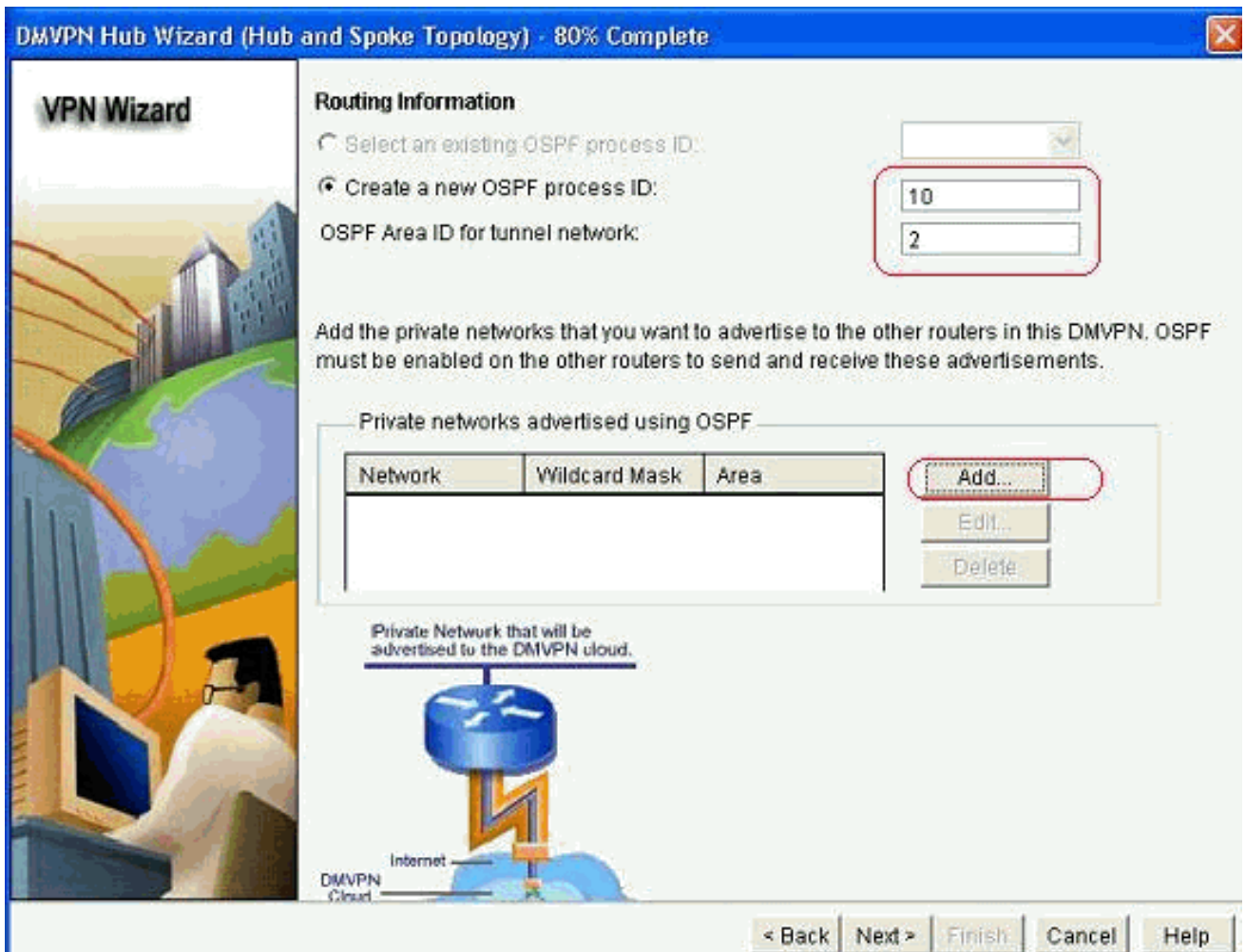
12. 按一下下一步繼續使用預設轉換集。



13. 選擇所需的路由協定。此處選擇了OSPF。

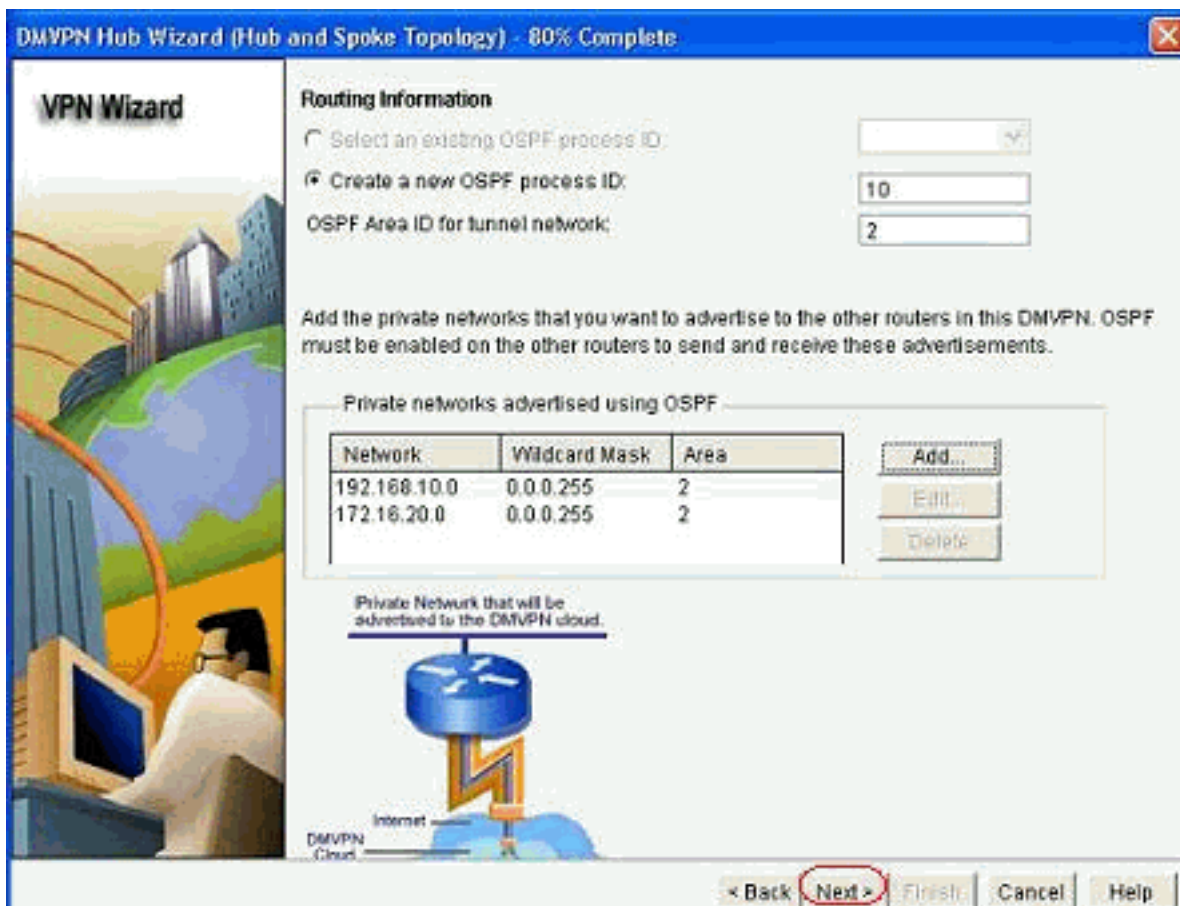


14. 指定OSPF進程ID和區域ID。按一下Add以新增要由OSPF通告的網路。

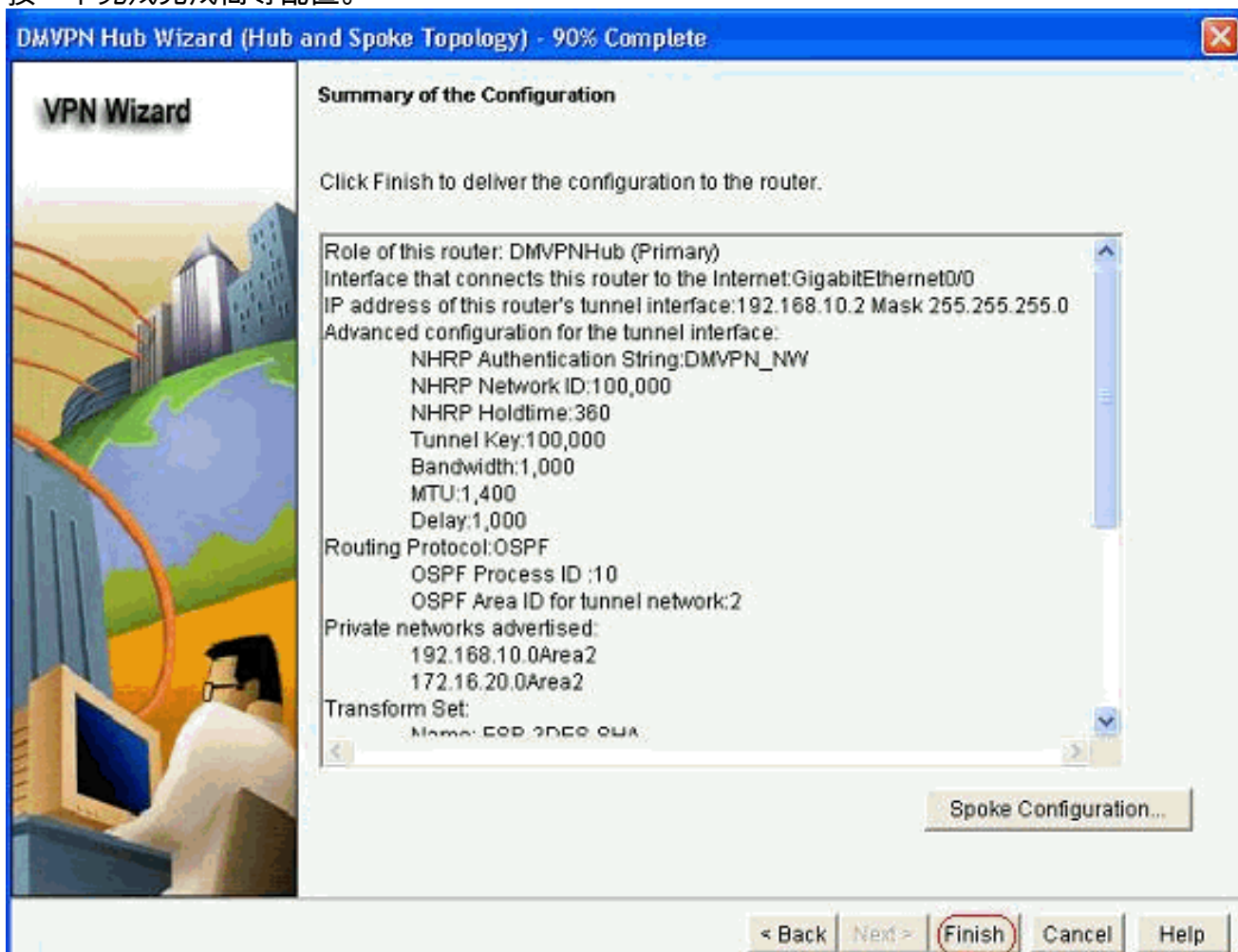


15. 新增隧道網路，然後按一下OK。

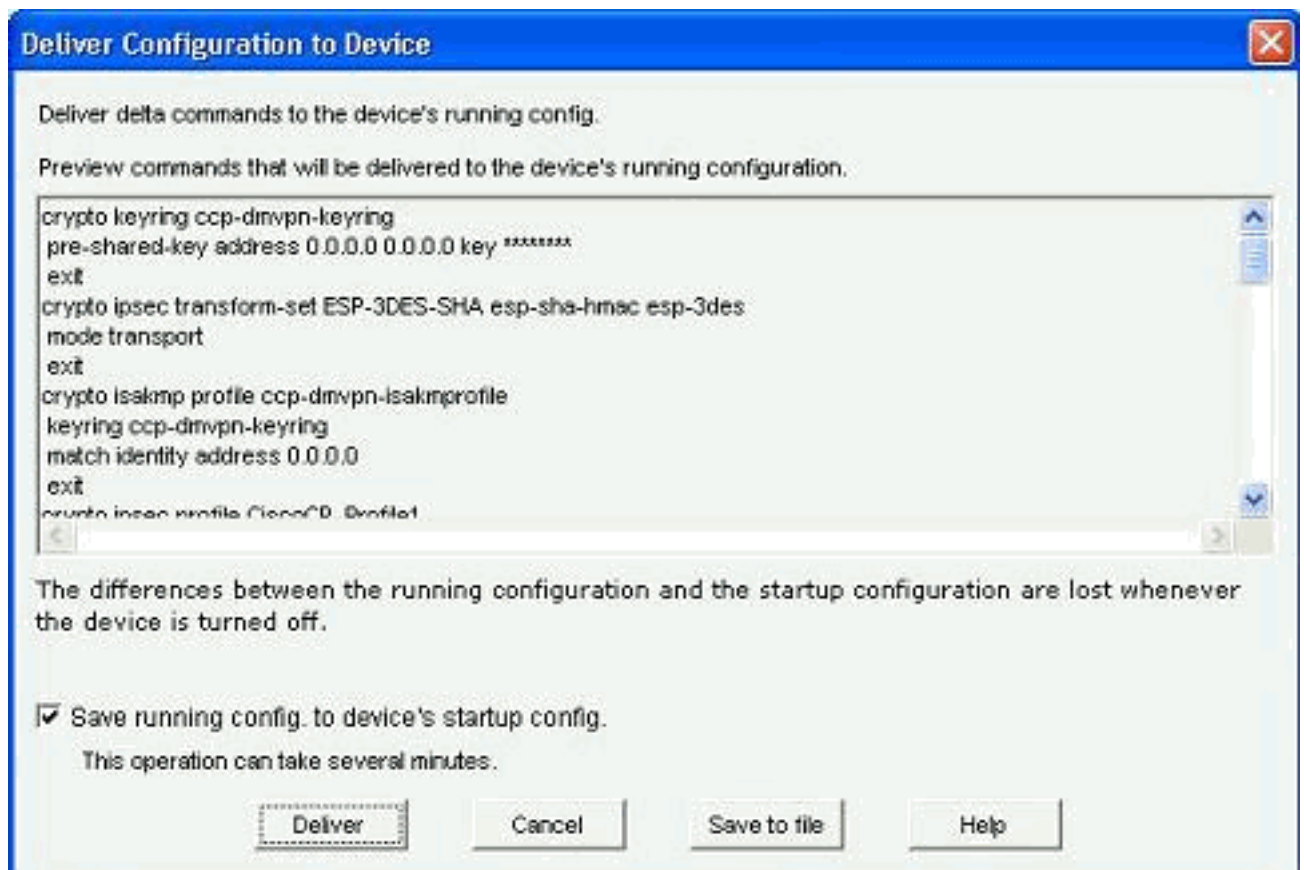
16. 在中心路由器後面新增專用網路，然後按一下下一步。



17. 按一下完成嚮導配置。



18. 按一下 Deliver 執行命令。



集線器的CLI配置

相關CLI配置如下所示：

集線器路由器
<pre> ! 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 </pre>

```

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
!

```

使用CCP編輯DMVPN配置

選擇隧道介面並按一下 *Edit* 時，可以手動編輯現有的DMVPN隧道引數。

Configure > Security > VPN > Dynamic Multipoint VPN

VPN

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

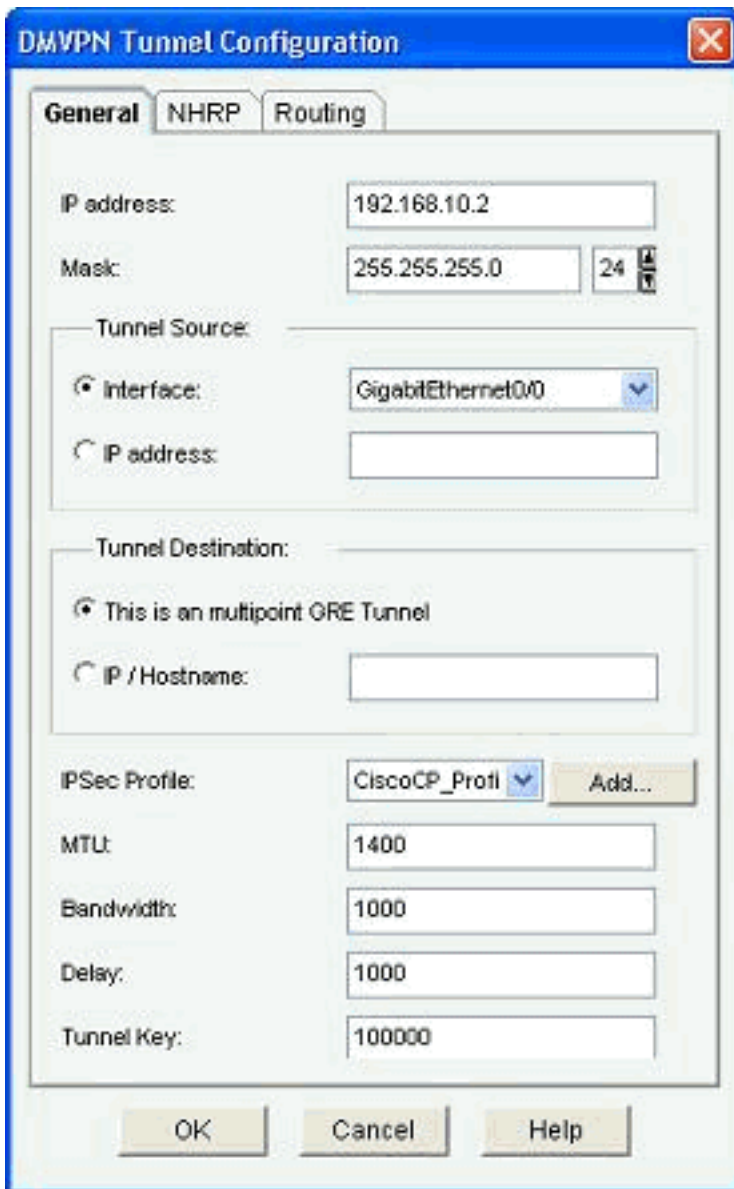
Add... Edit... Delete

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

通道介面引數（例如MTU和通道金鑰）在 *General* 索引標籤下修改。

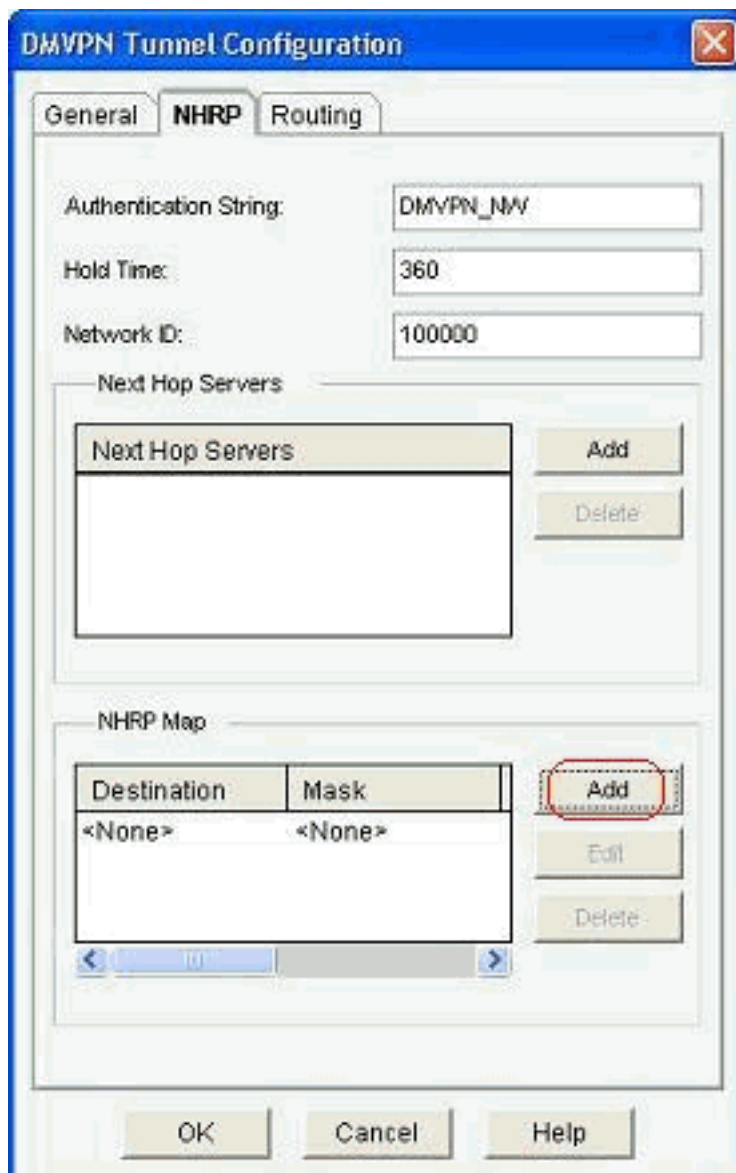


The image shows a 'DMVPN Tunnel Configuration' dialog box with three tabs: 'General', 'NHRP', and 'Routing'. The 'General' tab is active. It contains the following fields and options:

- IP address:** 192.168.10.2
- Mask:** 255.255.255.0, with a dropdown menu set to 24.
- Tunnel Source:**
 - Interface:** GigabitEthernet0/0
 - IP address:** (empty field)
- Tunnel Destination:**
 - This is an multipoint GRE Tunnel**
 - IP / Hostname:** (empty field)
- IPSec Profile:** CiscoCP_Profi (dropdown menu) 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. 根據NHRP頁籤下的要求找到並修改NHRP相關引數。對於分支路由器，您應該能夠將NHS作為中心路由器的IP地址檢視。在NHRP對映部分中按一下Add以新增NHRP對映。



2. 根據網路設定，可以如下所示配置NHRP對映引數

NHRP Map Configuration ✕

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

Destination reachable through NBMA network

IP Address:

Mask (Optional): Y

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

在「工藝路線」(Routing)頁籤下檢視和修改與工藝路線相關的引數。



更多資訊

DMVPN隧道通過以下兩種方式配置：

- 通過中心點進行輻射到輻射通訊
- 無中心點的分支對分支通訊

本文只討論第一種方法。為了允許建立輻射點到輻射點動態IPSec隧道，使用此方法將輻射點新增到DMVPN雲：

1. 啟動DMVPN嚮導並選擇分支配置選項。
2. 在DMVPN Network Topology視窗中，選擇Full meshed network選項，而不是Hub and Spoke network選項。

DMVPN Spoke Wizard - 10% Complete

VPN Wizard

DMVPN Network Topology

Select the DMVPN network topology.

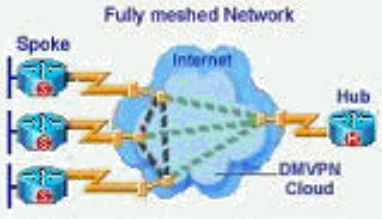
Hub and Spoke network

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

3. 使用與本文檔中的其他配置相同的步驟完成其餘配置。

驗證

目前沒有適用於此組態的驗證程序。

相關資訊

- [Cisco動態多點VPN:簡單、安全的分支機構到分支機構通訊](#)
- [IOS 12.2動態多點VPN\(DMVPN\)](#)
- [技術支援與文件 - Cisco Systems](#)