

Cisco IOS/CCP - Configurazione di DMVPN con Cisco CCP

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Convenzioni](#)

[Premesse](#)

[Configurazione](#)

[Esempio di rete](#)

[Configurazione spoke con Cisco CP](#)

[Configurazione CLI per spoke](#)

[Configurazione hub con Cisco CP](#)

[Configurazione CLI per hub](#)

[Modificare la configurazione DMVPN utilizzando CCP](#)

[Ulteriori informazioni](#)

[Verifica](#)

[Informazioni correlate](#)

[Introduzione](#)

In questo documento viene fornita una configurazione di esempio per il tunnel DMVPN (Dynamic Multipoint VPN) tra router hub e spoke tramite Cisco Configuration Professional (Cisco CP). Dynamic Multipoint VPN è una tecnologia che integra diversi concetti, quali GRE, crittografia IPsec, NHRP e routing, per fornire una soluzione sofisticata che consente agli utenti finali di comunicare in modo efficace tramite i tunnel IPsec spoke creati in modo dinamico.

[Prerequisiti](#)

[Requisiti](#)

Per ottenere le migliori funzionalità di DMVPN, è consigliabile eseguire il software Cisco IOS® versione 12.4 mainline, 12.4T e successive.

[Componenti usati](#)

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Cisco IOS Router serie 3800 con software versione 12.4 (22)
- Cisco IOS Router serie 1800 con software release 12.3 (8)
- Cisco Configuration Professional versione 2.5

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a [Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti](#).

Premesse

Questo documento offre informazioni su come configurare un router come spoke e un altro router come hub con Cisco CP. Inizialmente viene mostrata la configurazione spoke, ma più avanti nel documento, viene mostrata in dettaglio anche la configurazione relativa all'hub per fornire una migliore comprensione. È possibile configurare anche altri raggi utilizzando un approccio simile per la connessione all'hub. Lo scenario corrente utilizza i parametri seguenti:

- Rete pubblica router hub - 209.165.201.0
- Rete tunnel - 192.168.10.0
- Protocollo di routing utilizzato - OSPF

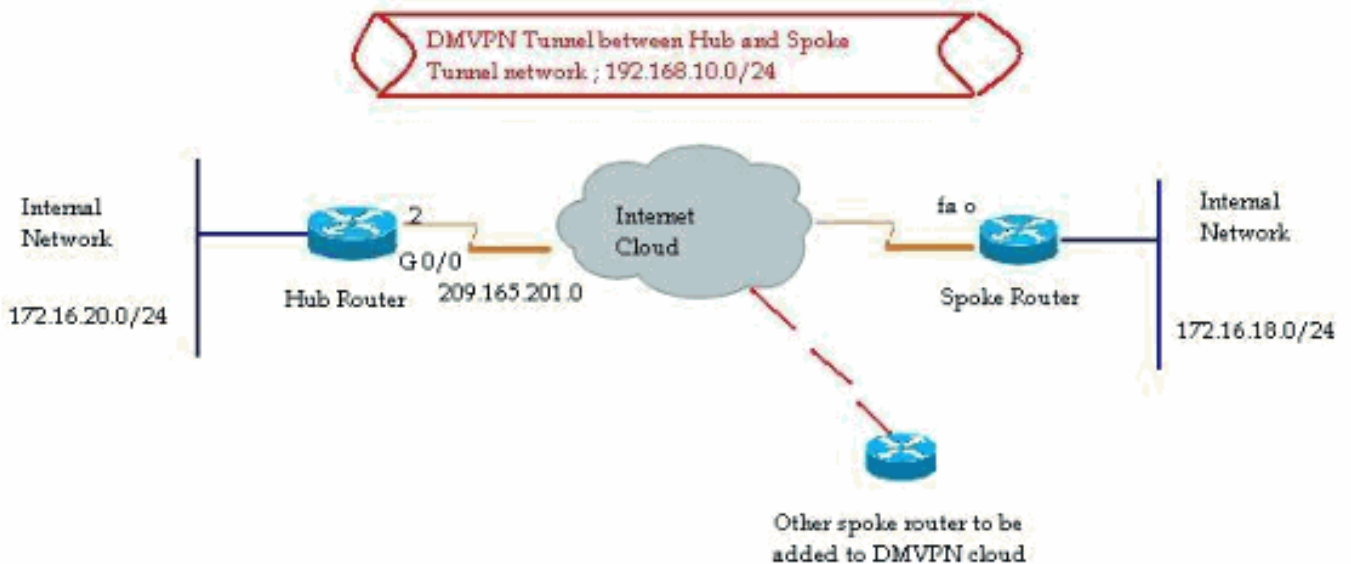
Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo [strumento di ricerca](#) dei comandi (solo utenti [registrati](#)).

Esempio di rete

Nel documento viene usata questa impostazione di rete:



[Configurazione spoke con Cisco CP](#)

Questa sezione illustra come configurare un router come spoke utilizzando la procedura guidata DMVPN in Cisco Configuration Professional.

1. Per avviare l'applicazione Cisco TCP e avviare la procedura guidata DMVPN, andare a *Configurazione > Sicurezza > VPN > Dynamic Multipoint VPN*. Quindi, selezionare l'opzione *Crea un raggio in una VPN DMVPN* e fare clic su *Avvia l'attività selezionata*.

Configure > Security > VPN > Dynamic Multipoint VPN

VPN

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

Configure DMVPN Spoke

Spoke 1

Spoke 2

DMVPN Cloud

Hub

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. Fare clic su *Next* (Avanti) per iniziare.



3. Selezionare l'opzione *Rete Hub e Spoke* e fare clic su *Avanti*.

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.

Hub and Spoke Network

< Back **Next >** Finish Cancel Help

4. Specificare le informazioni relative all'hub, ad esempio l'interfaccia pubblica del router hub e l'interfaccia del tunnel del router hub.

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: 209.165.201.2

IP address of hub's mGRE tunnel interface: 192.168.10.2

Spoke
You are configuring this spoke router

Internet
DMVPN Cloud

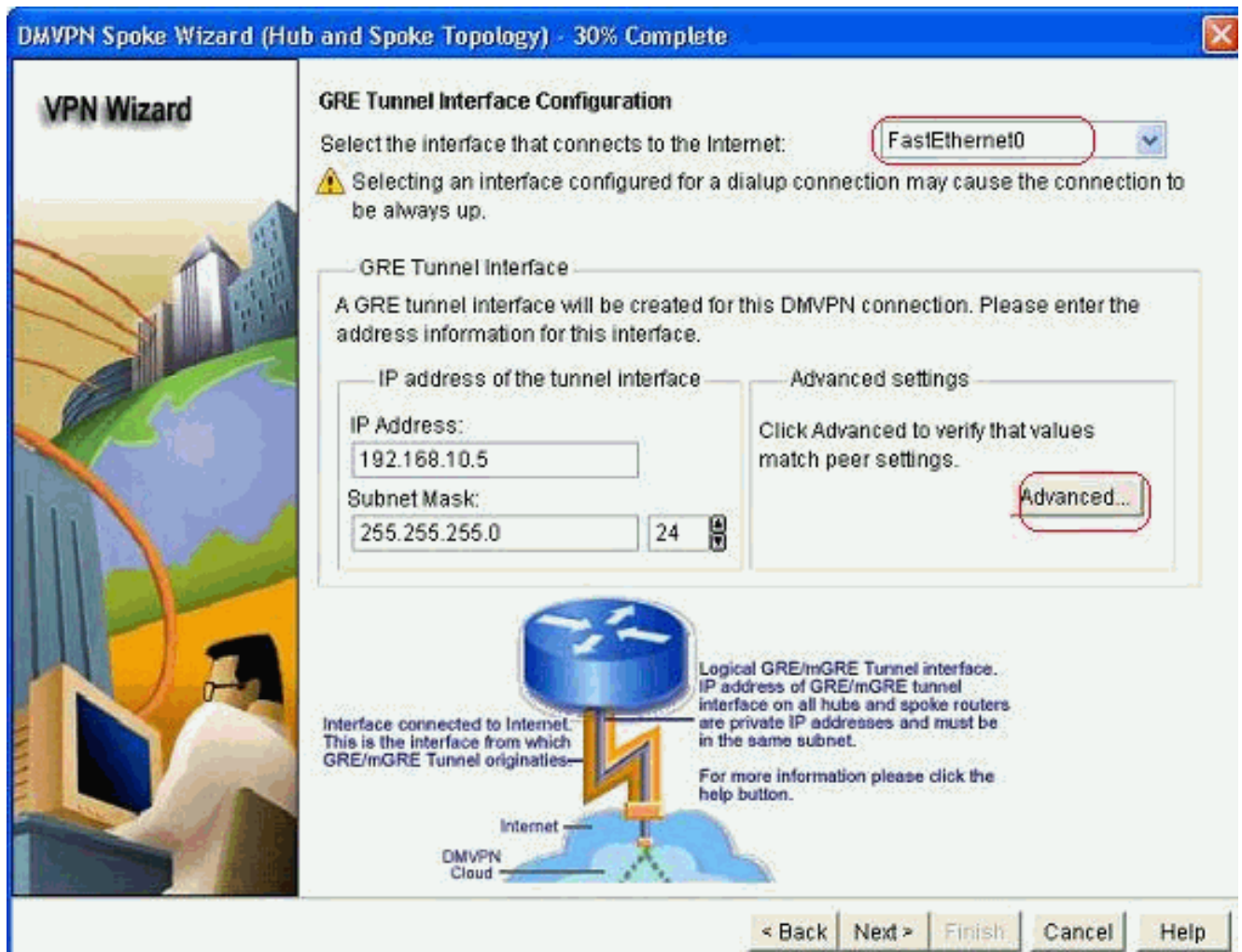
Hub

Public IP address to be entered above

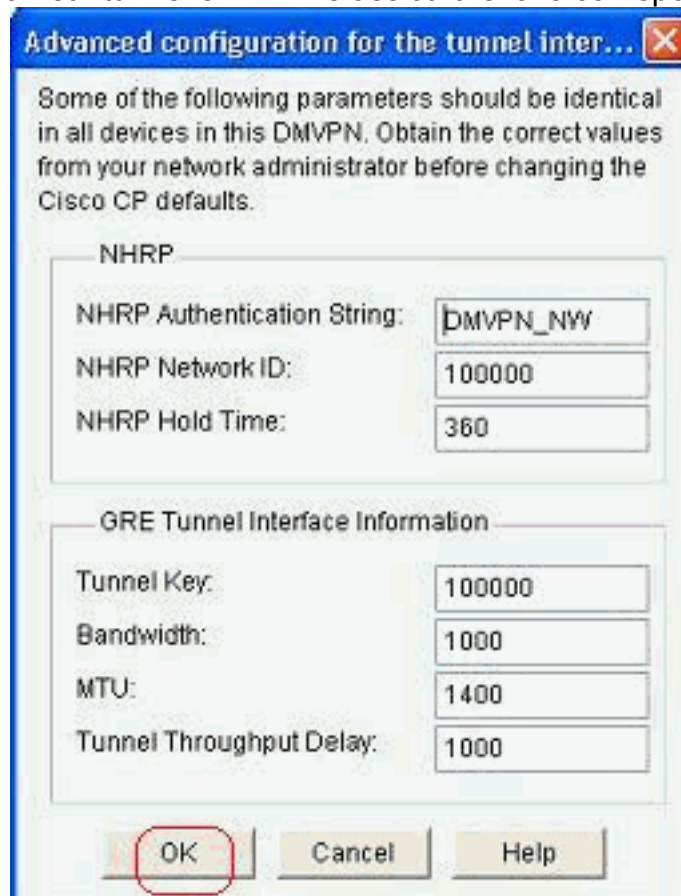
IP address of the mGRE tunnel to be entered above

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

5. Specificare i dettagli dell'interfaccia tunnel dello spoke e l'interfaccia pubblica dello spoke. Quindi fare clic su *Avanzate*.



6. Verificare i parametri tunnel e NHRP e assicurarsi che corrispondano perfettamente ai



parametri Hub.

7. Specificare la chiave già condivisa e fare clic su

Avanti.

DMVPN Spoke Wizard (Hub and Spoke Topology) - 40% Complete

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

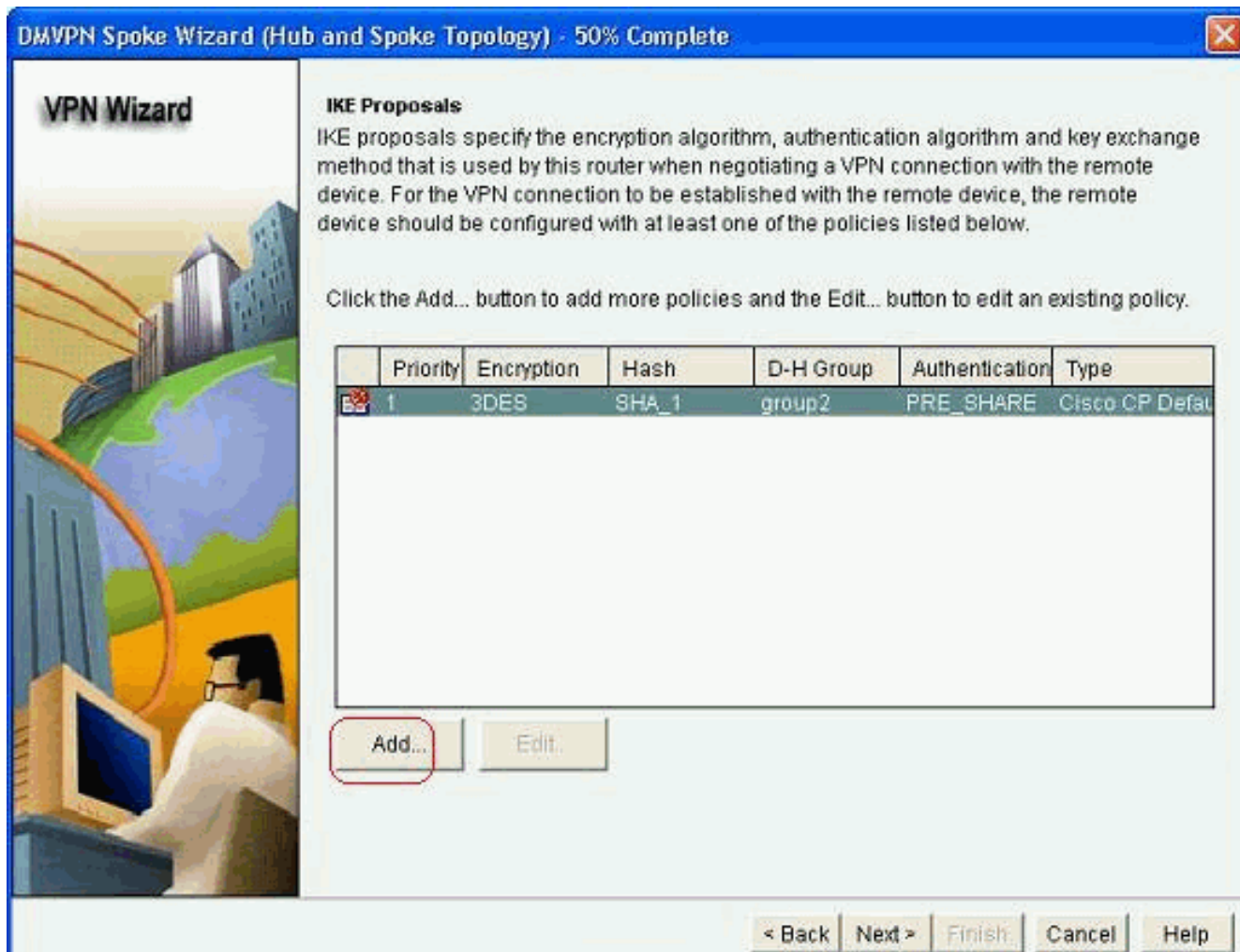
Pre-shared Keys

pre-shared key:

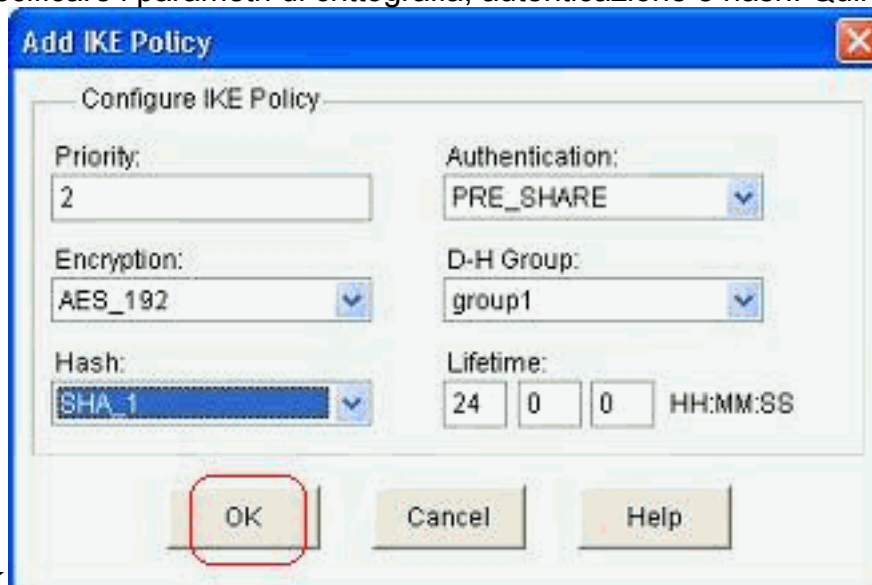
Reenter key:

< Back **Next >** Finish Cancel Help

8. Per aggiungere una proposta IKE separata, fare clic su *Add* (Aggiungi).

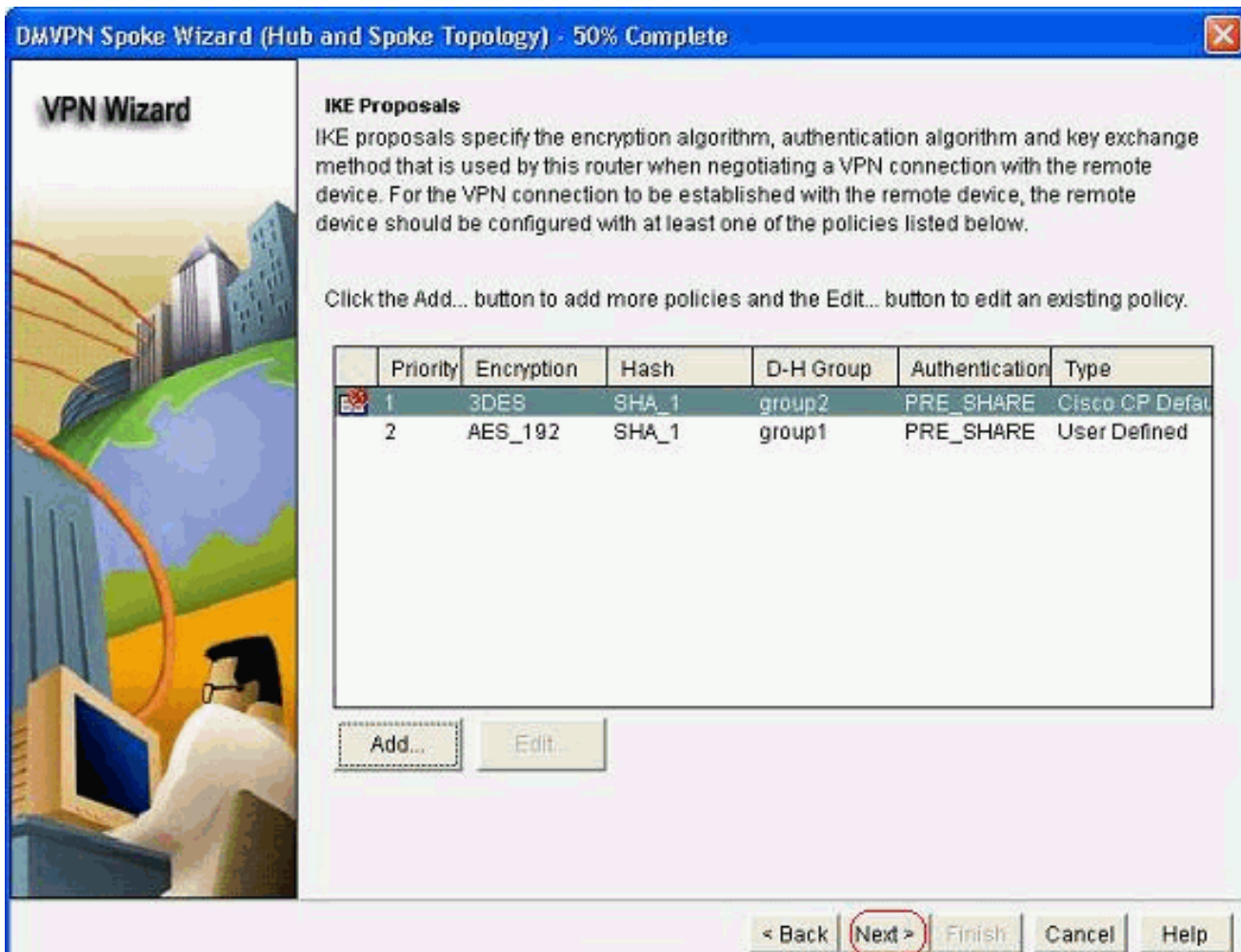


9. Specificare i parametri di crittografia, autenticazione e hash. Quindi fare clic su

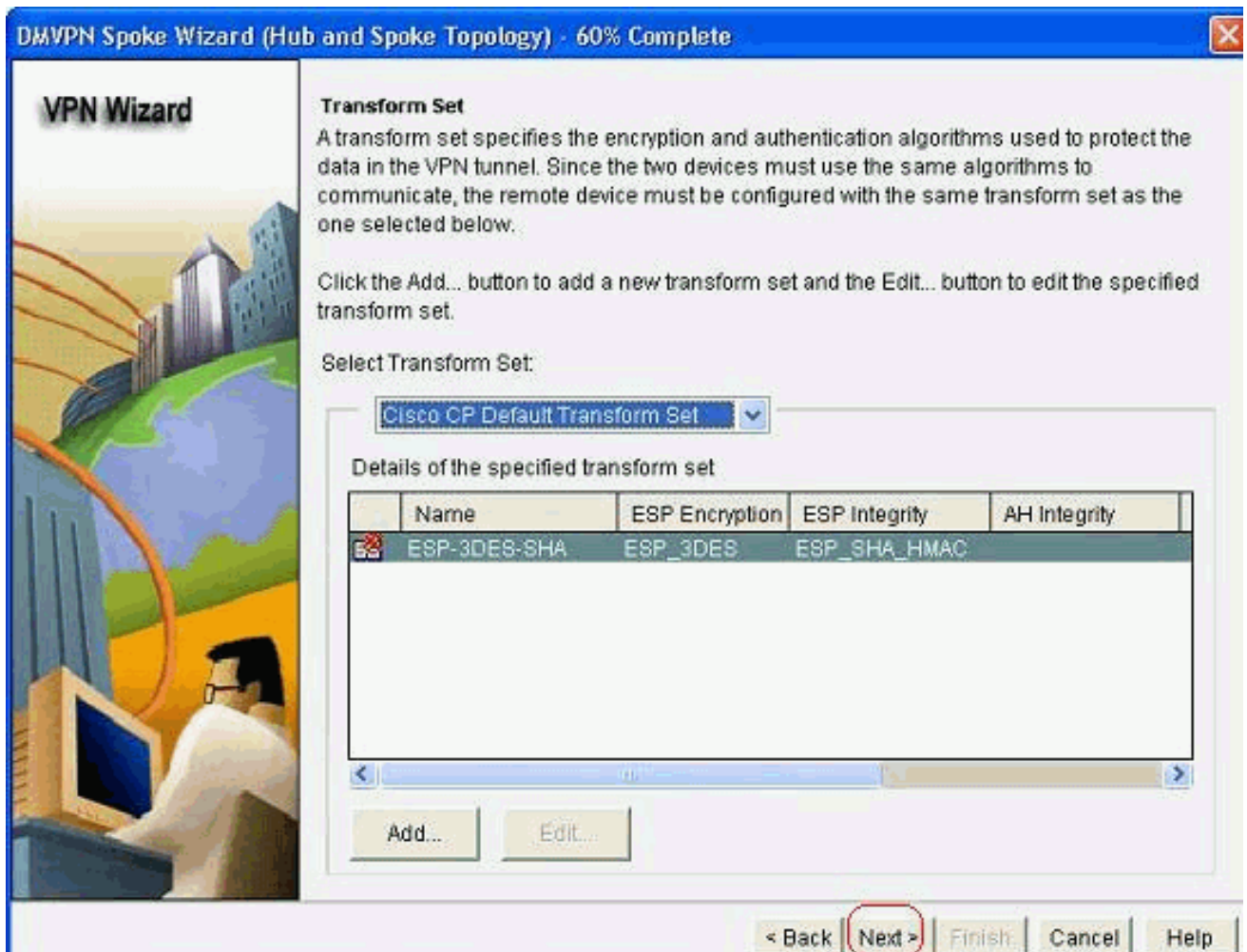


OK.

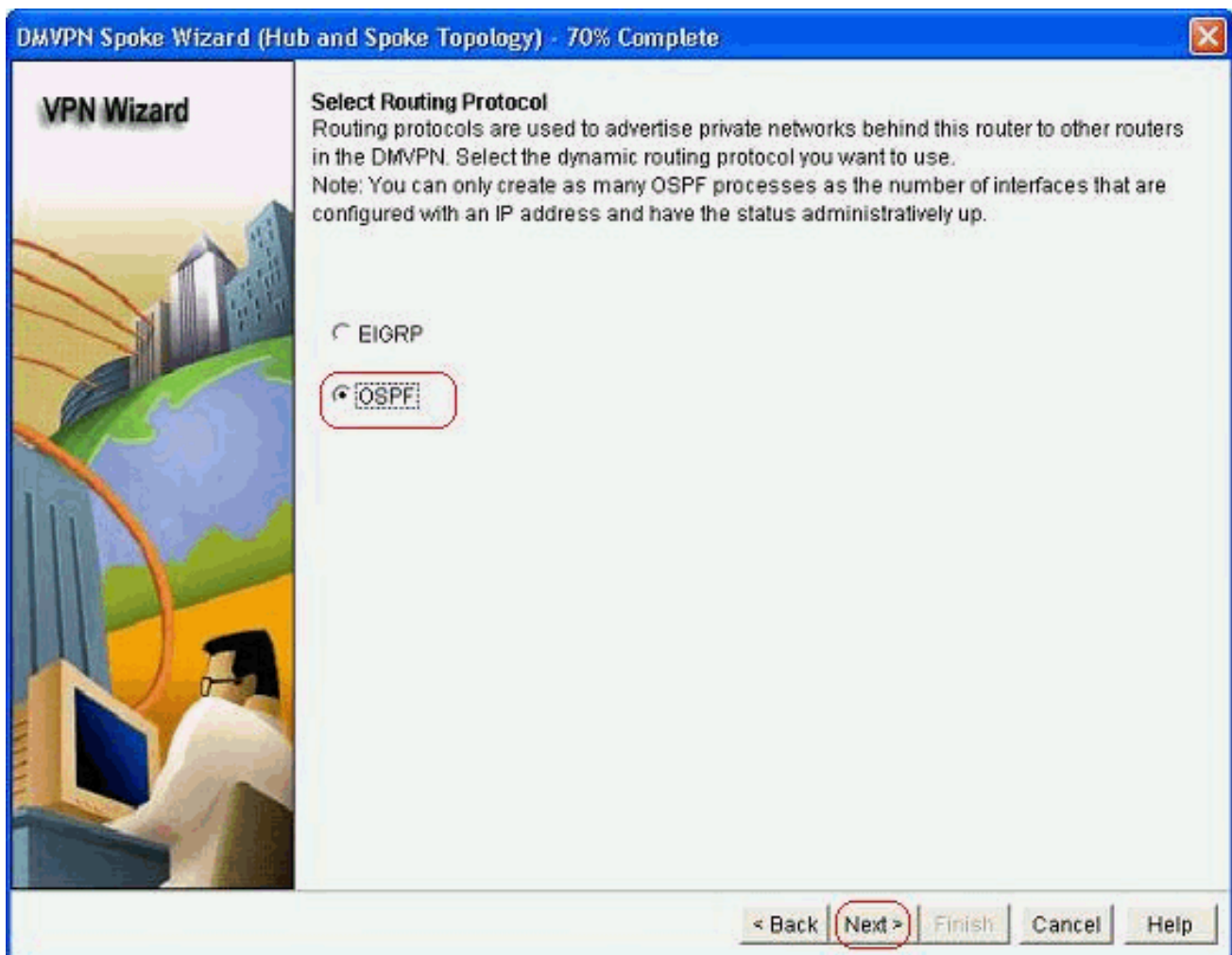
10. I nuovi criteri IKE possono essere visualizzati qui. Fare clic su Next (Avanti).



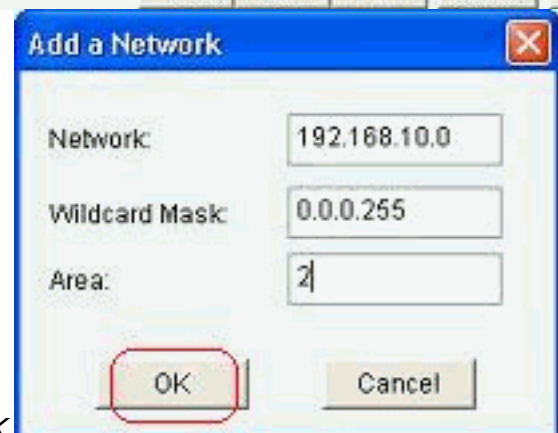
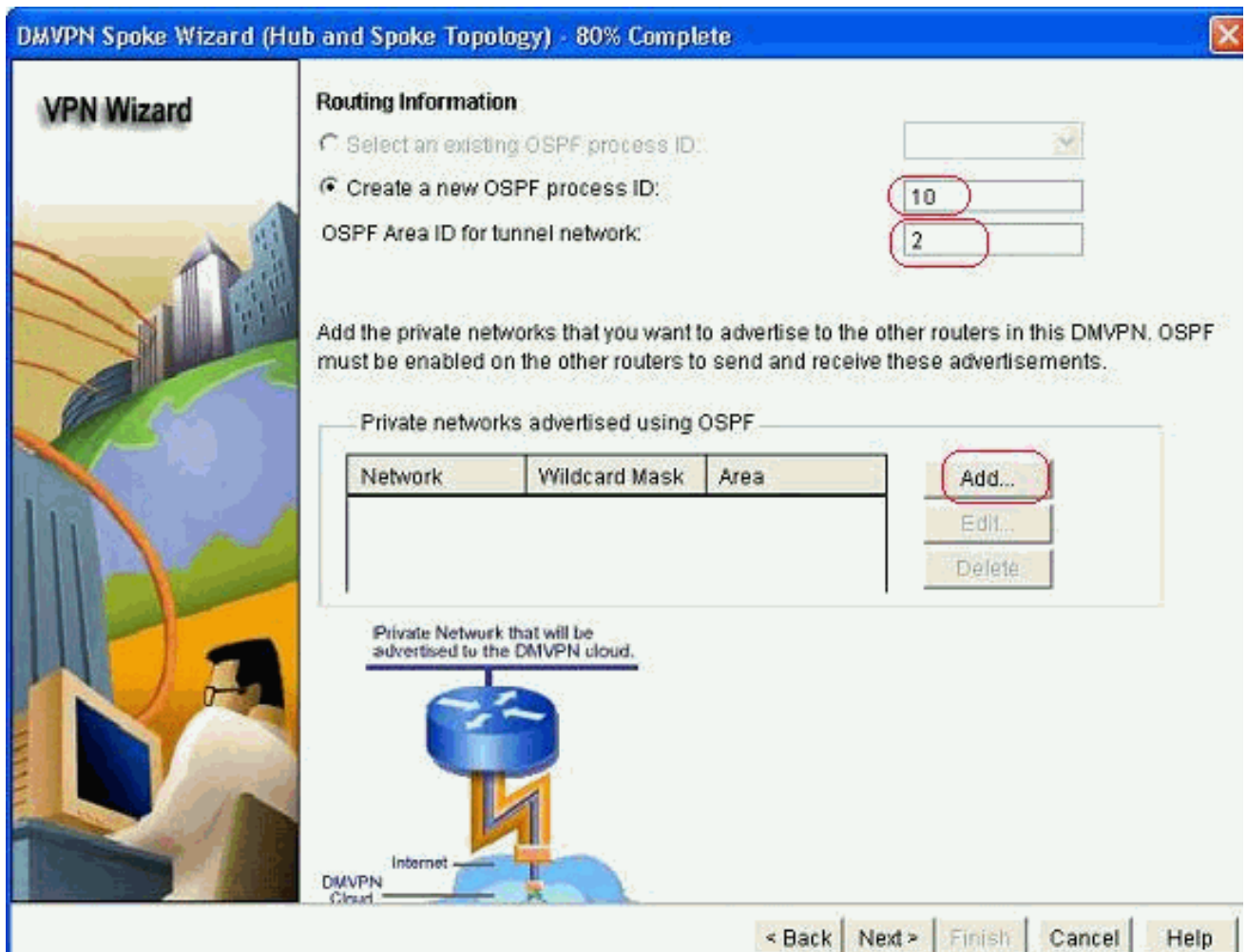
11. Fare clic su *Avanti* per continuare con il set di trasformazioni predefinito.



12. Selezionare il protocollo di routing desiderato. In questo caso, è selezionato *OSPF*.

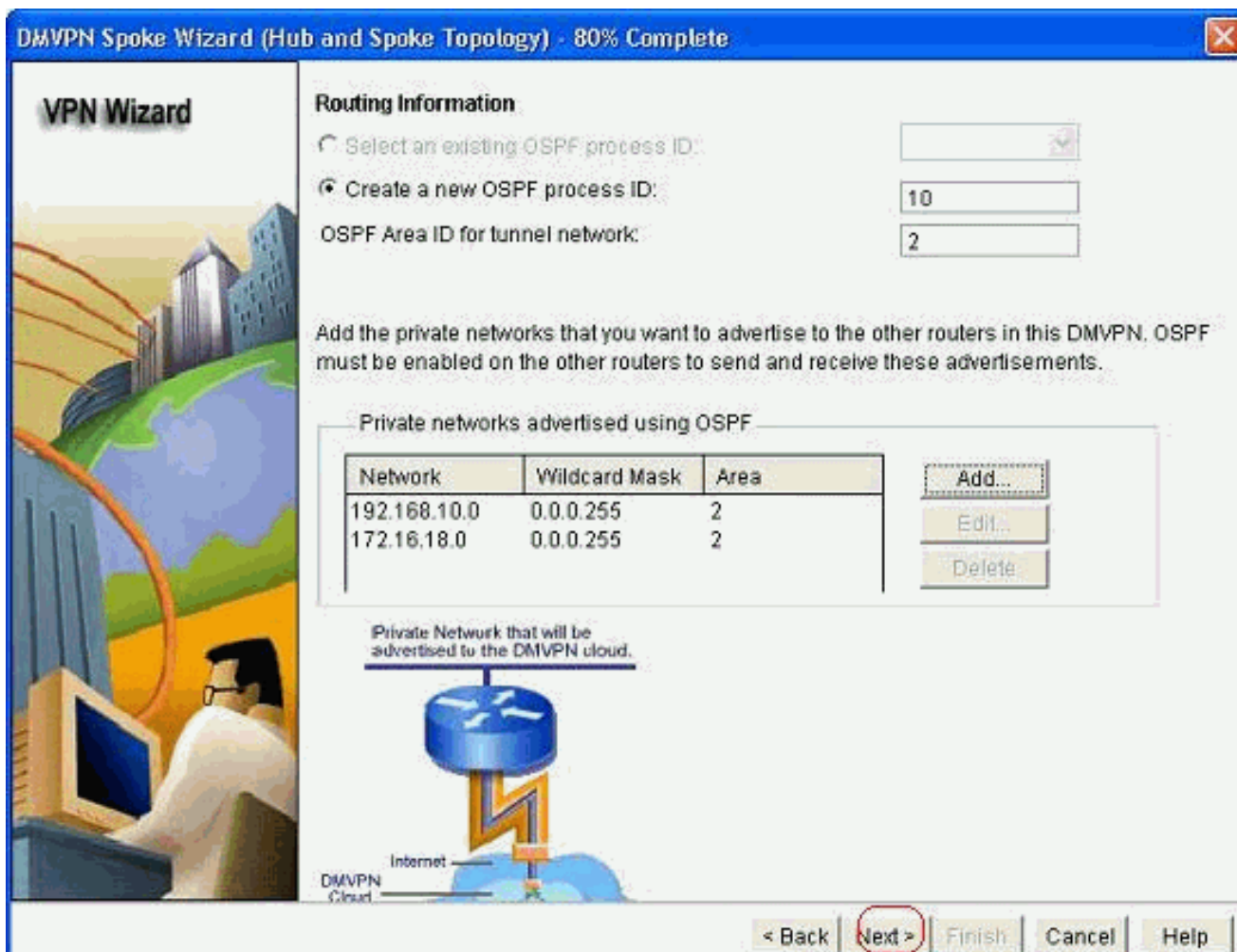


13. Specificare l'ID processo OSPF e l'ID area. Per aggiungere le reti che devono essere annunciate da OSPF, fare clic su *Add* (Aggiungi).

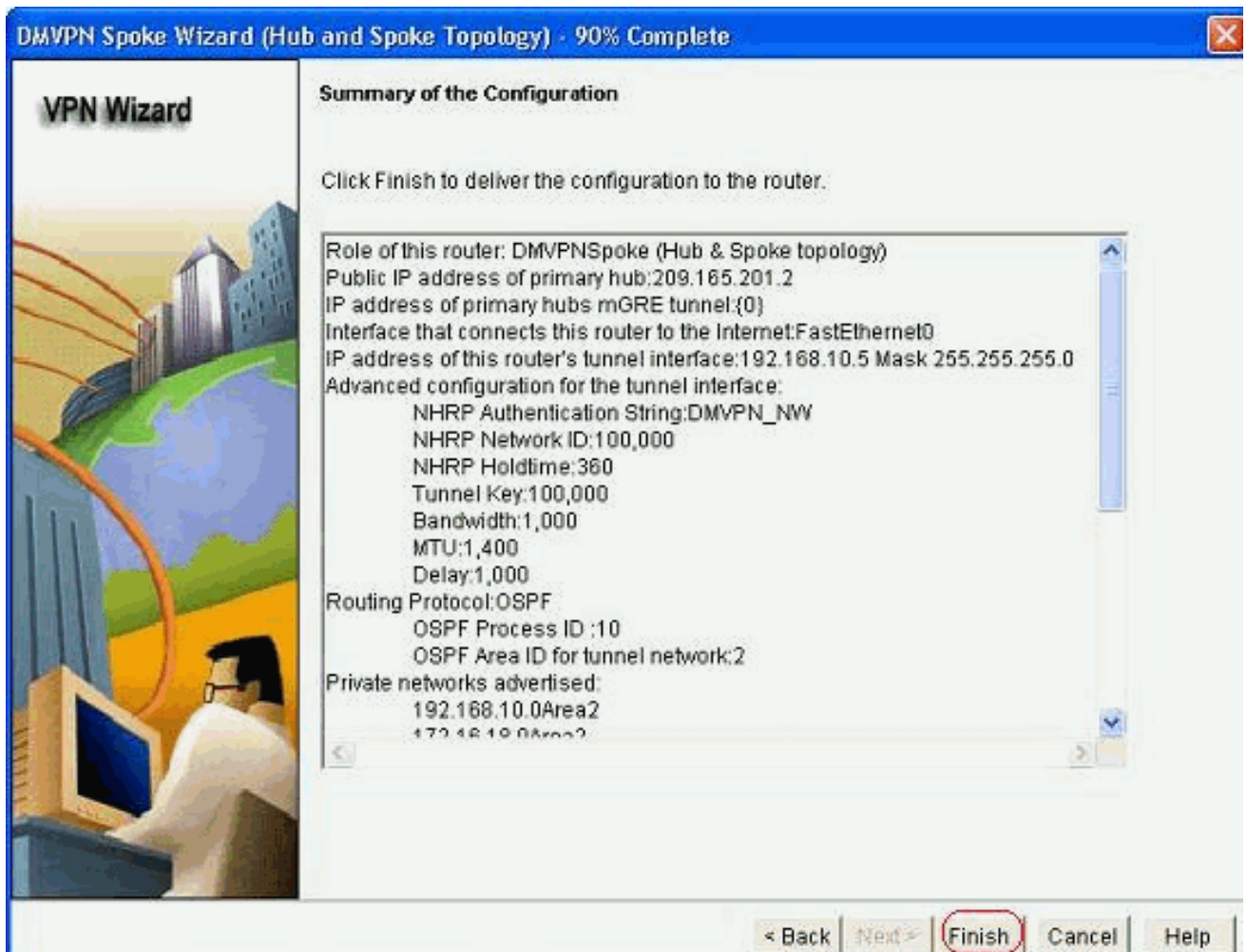


14. Aggiungere la rete del tunnel e fare clic su *OK*.

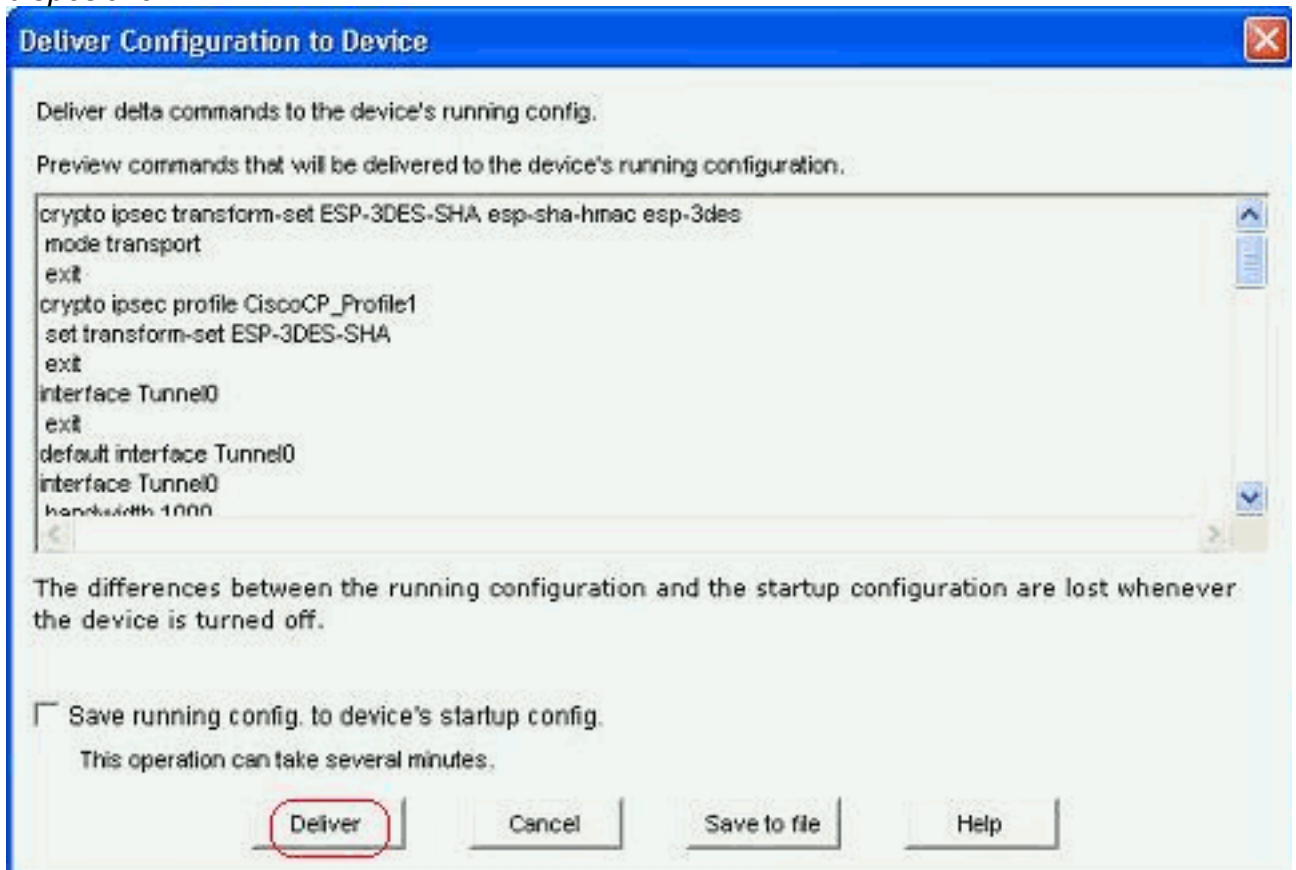
15. Aggiungere la rete privata dietro il router spoke. Fare quindi clic su *Avanti*.



16. Fare clic su *Fine* per completare la configurazione della procedura guidata.



17. Fare clic su *Consegna* per eseguire i comandi. Per salvare la configurazione, selezionare la casella di controllo *Salva configurazione in esecuzione nella configurazione di avvio del dispositivo*.



Configurazione CLI per spoke

La configurazione CLI correlata è mostrata di seguito:

Router Spoke

```
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
```

Configurazione hub con Cisco CP


In questa sezione viene mostrato un approccio graduale su come configurare il router hub per la VPN DMVPN.

1. Selezionare *Configura > Sicurezza > VPN > Dynamic Multipoint VPN* e selezionare l'opzione *Crea un hub in una VPN DPM*. Fare clic su *Avvia l'attività selezionata*.

Configure > Security > VPN > Dynamic Multipoint VPN

VPN

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



Create a spoke (client) in a DMVPN

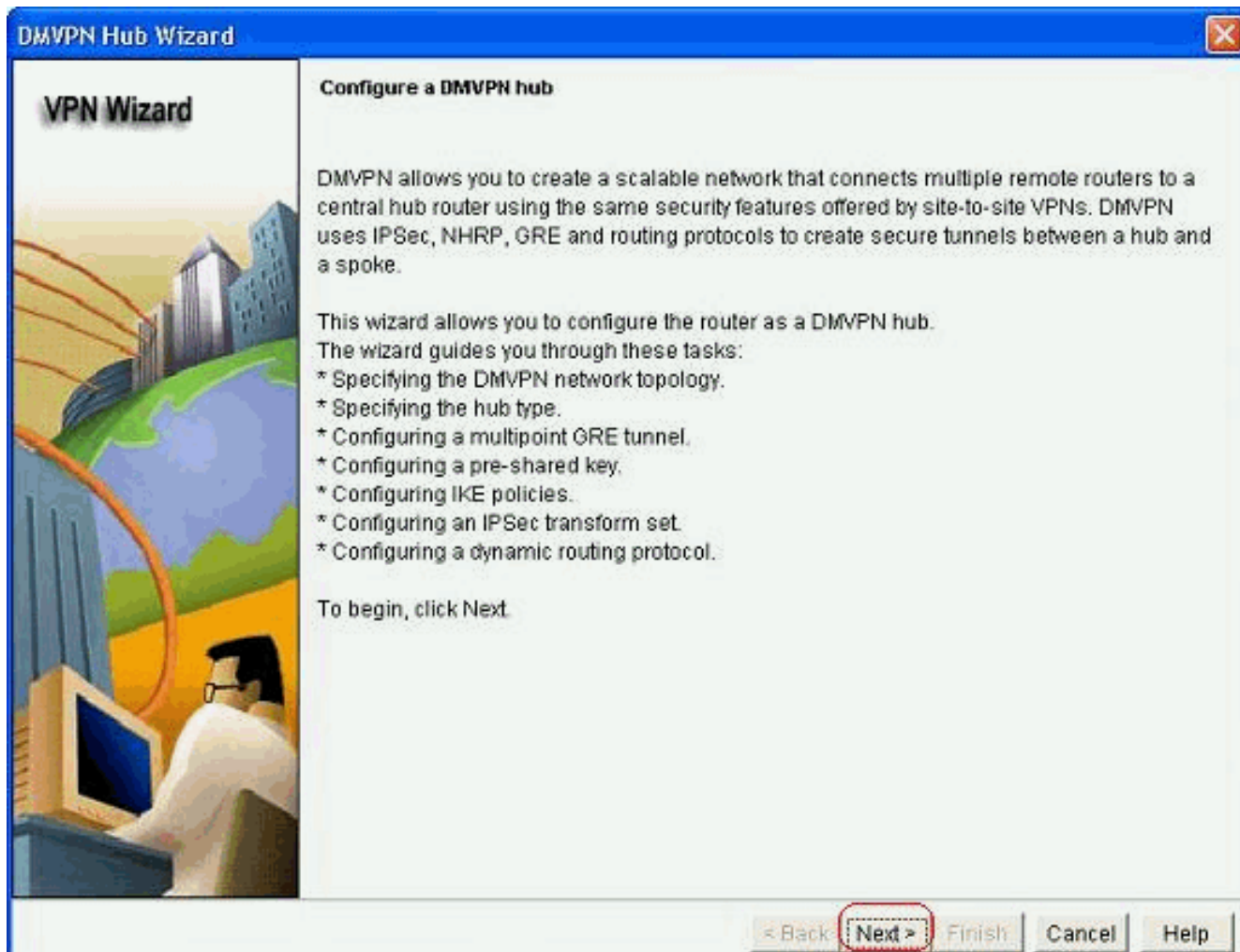
Use this option to configure the router as a spoke in a full mesh or hub and spoke network topology. To complete this configuration, you must know the hub's IP address, NHRP information, pre-shared key, IKE policy, IPsec Transform set and dynamic routing protocol information.

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. Fare clic su *Next* (Avanti).



3. Selezionare l'opzione *Rete Hub e Spoke* e fare clic su *Avanti*.

VPN Wizard



DMVPN Network Topology

Select the DMVPN network topology.

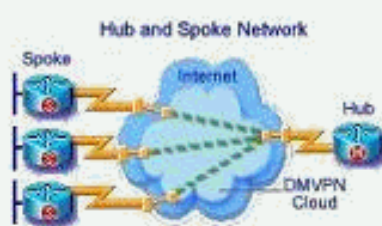
Hub and Spoke network

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

Spoke

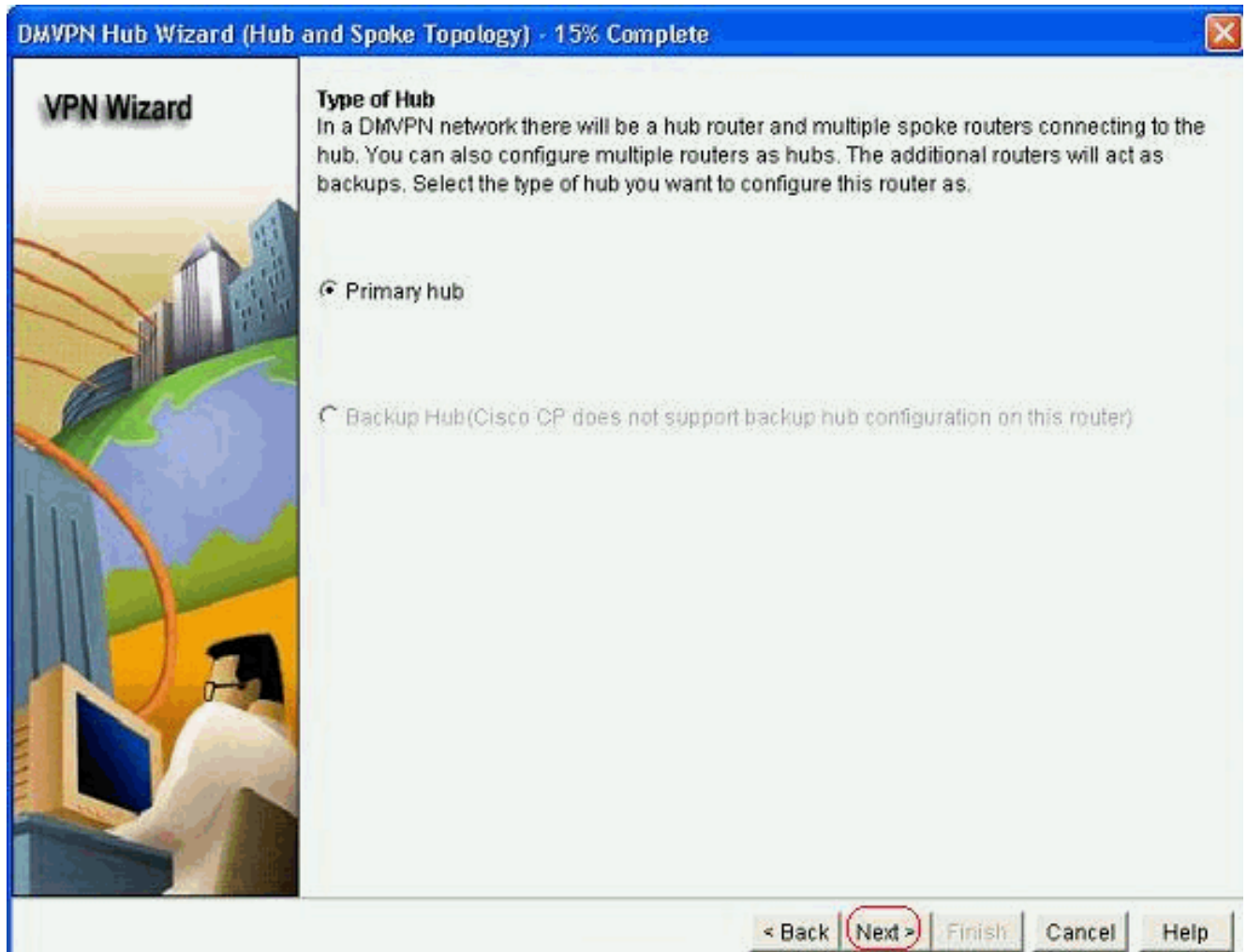
Internet

Hub

DMVPN Cloud


< Back **Next >** Finish Cancel Help

4. Selezionare *Hub primario*. Fare quindi clic su *Avanti*.



5. Specificare i parametri dell'interfaccia del tunnel e fare clic su *Avanzate*.

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. Specificare i parametri Tunnel e NHRP. Quindi fare clic su

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:

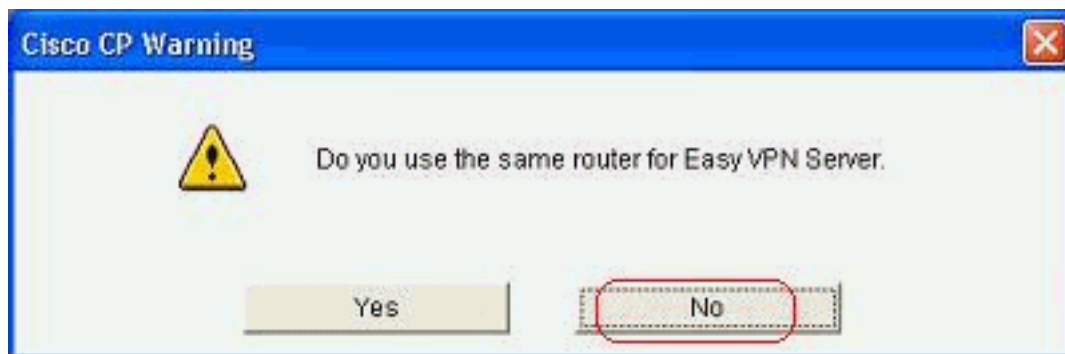
MTU:

Tunnel Throughput Delay:

OK
Cancel
Help

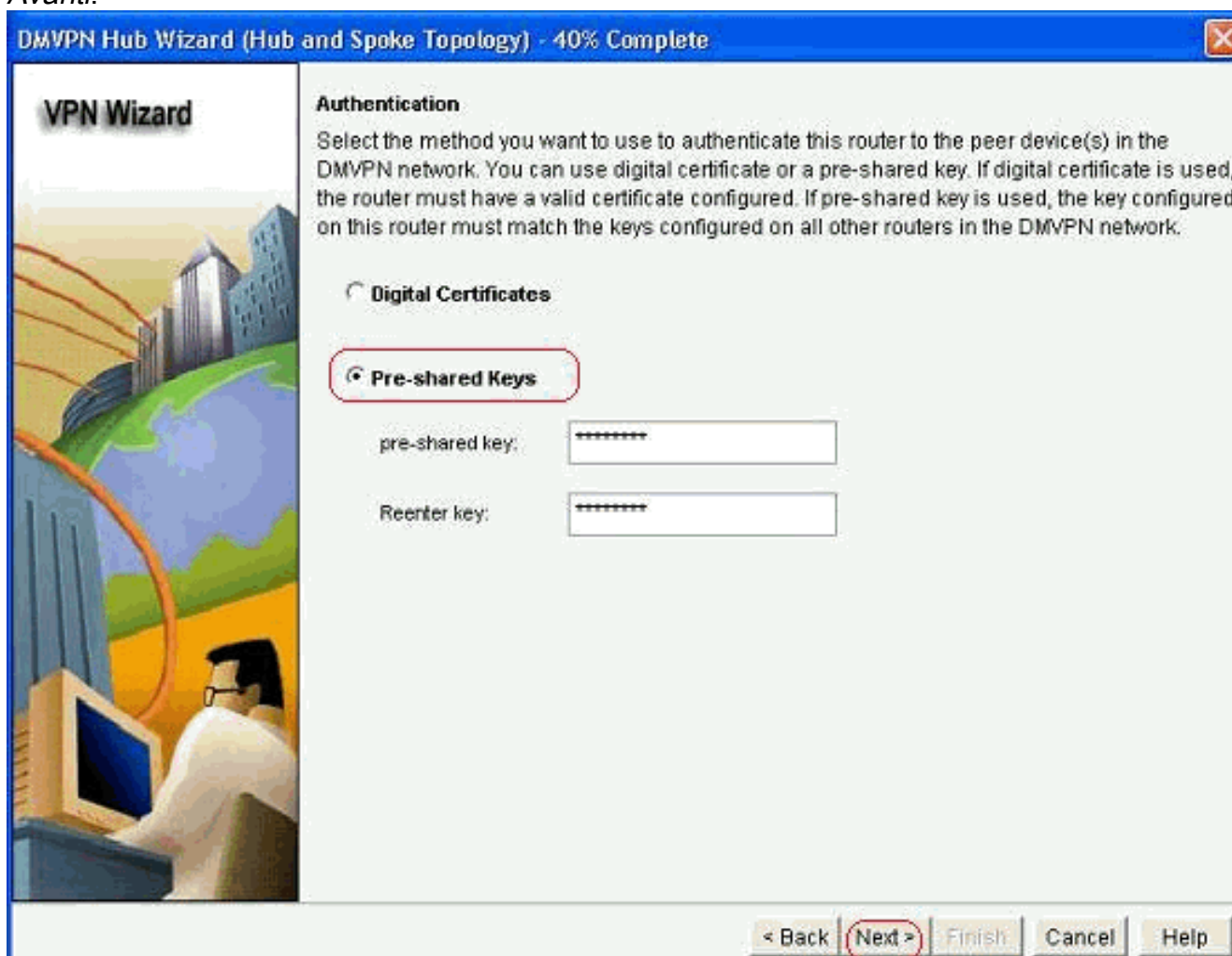
OK.

7. Specificare l'opzione in base alla configurazione della

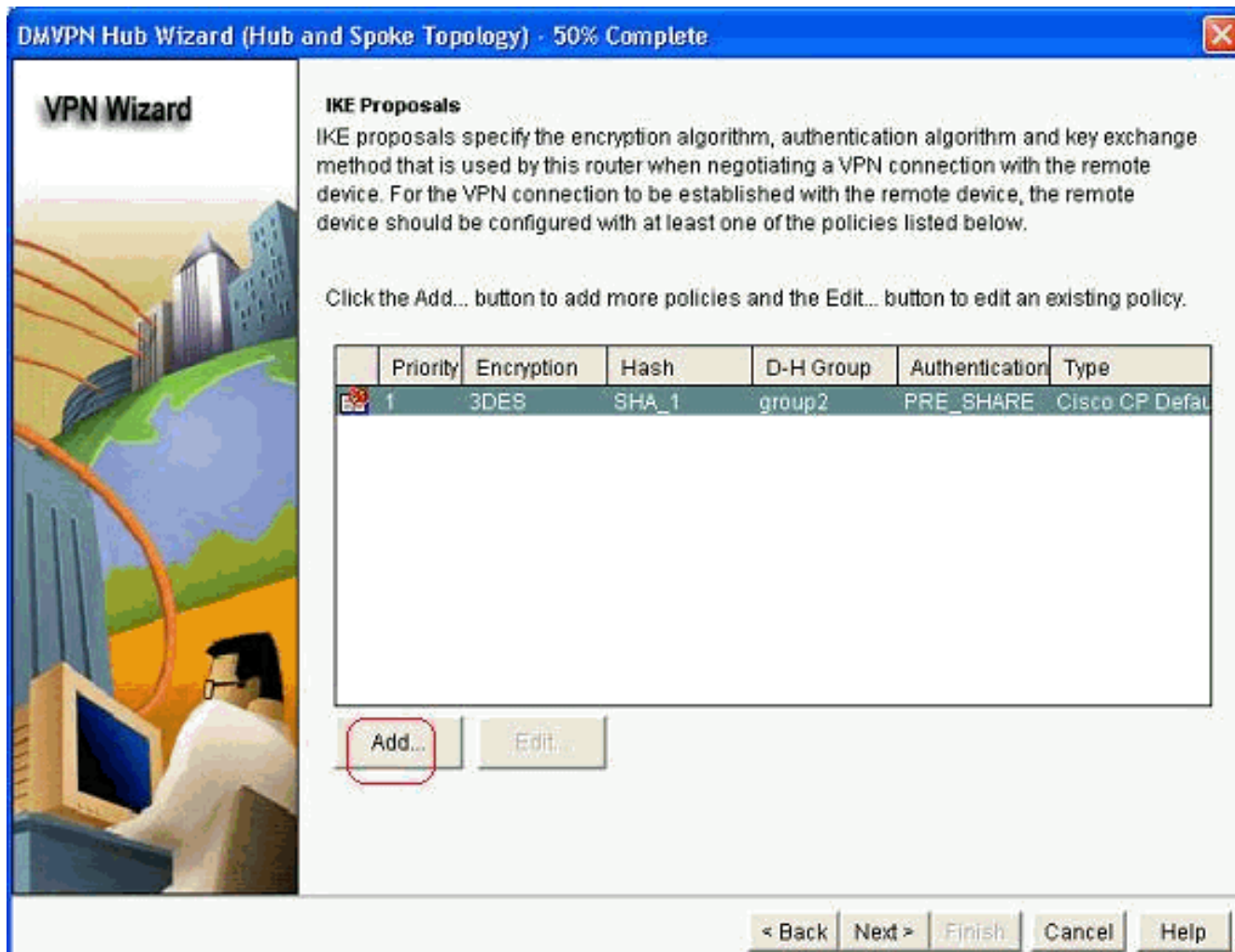


rete.

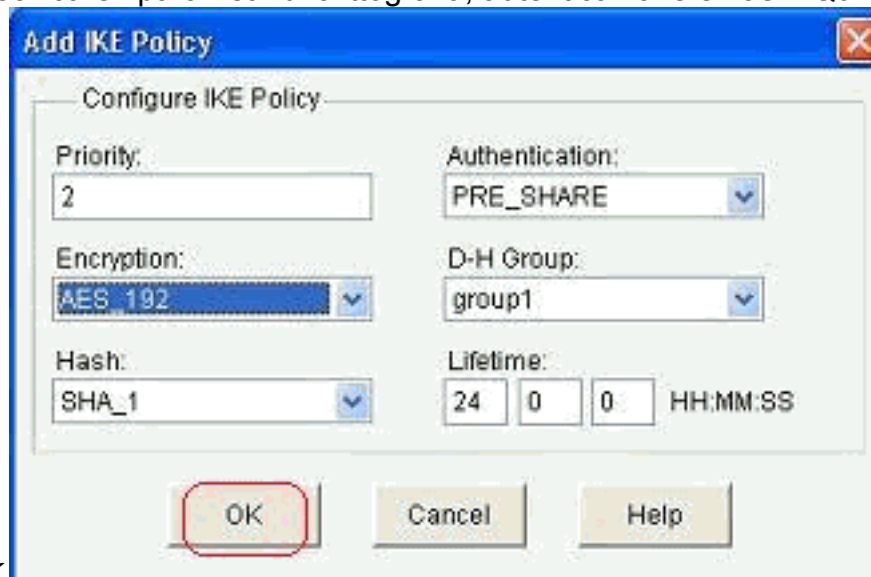
8. Selezionare *Chiavi già condivise* e specificare le chiavi già condivise. Fare quindi clic su *Avanti*.



9. Per aggiungere una proposta IKE separata, fare clic su *Add* (Aggiungi).

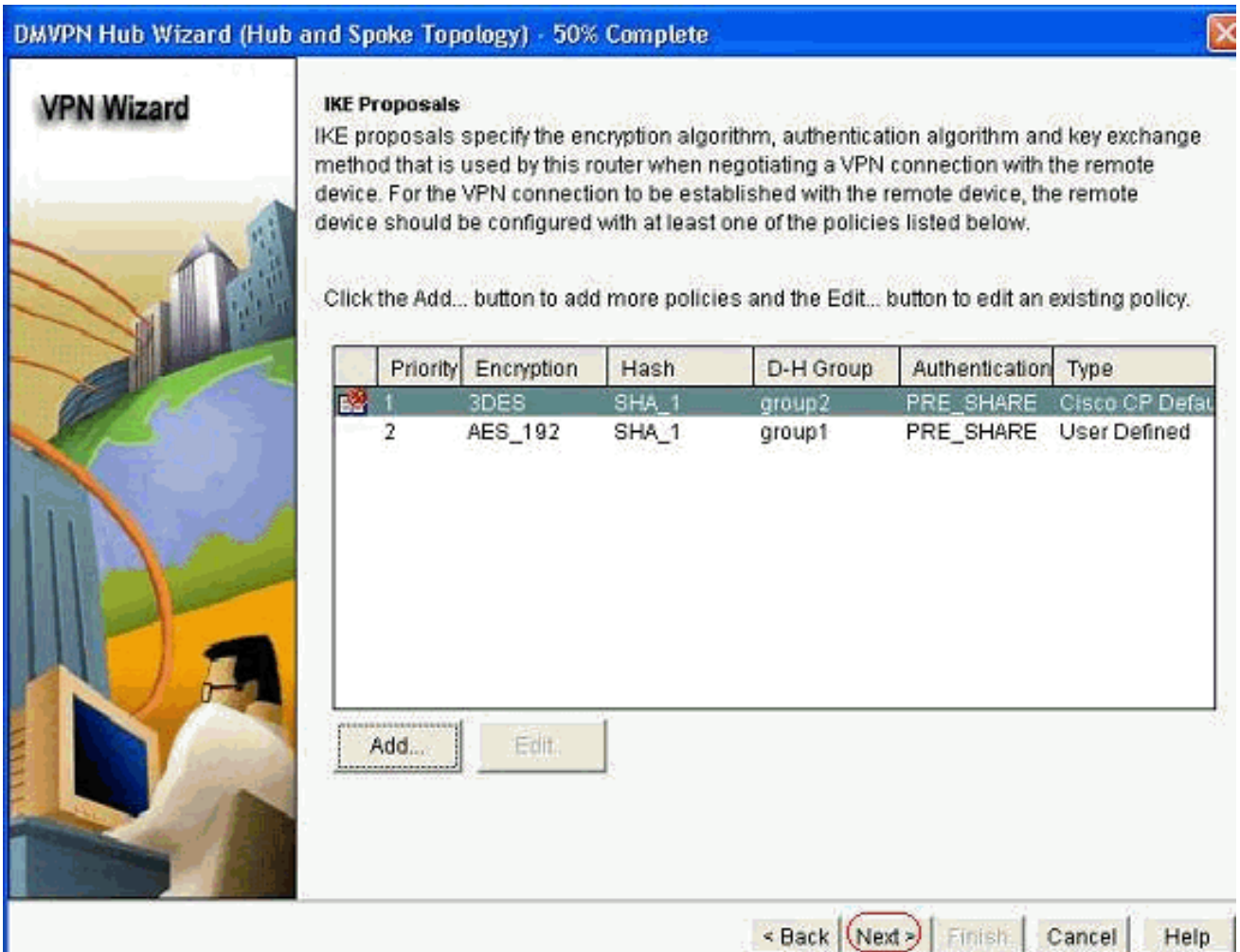


10. Specificare i parametri di crittografia, autenticazione e hash. Quindi fare clic su

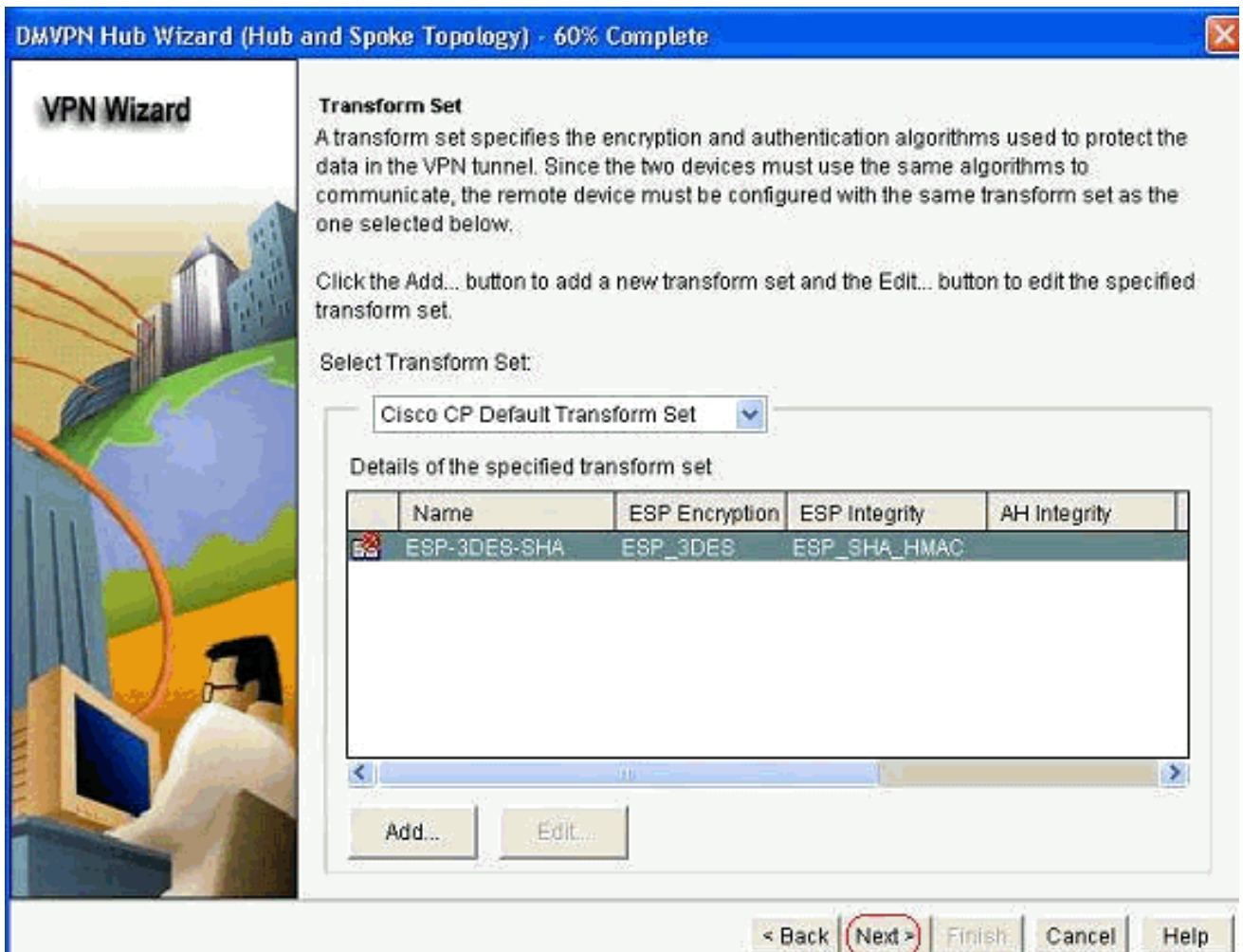


OK.

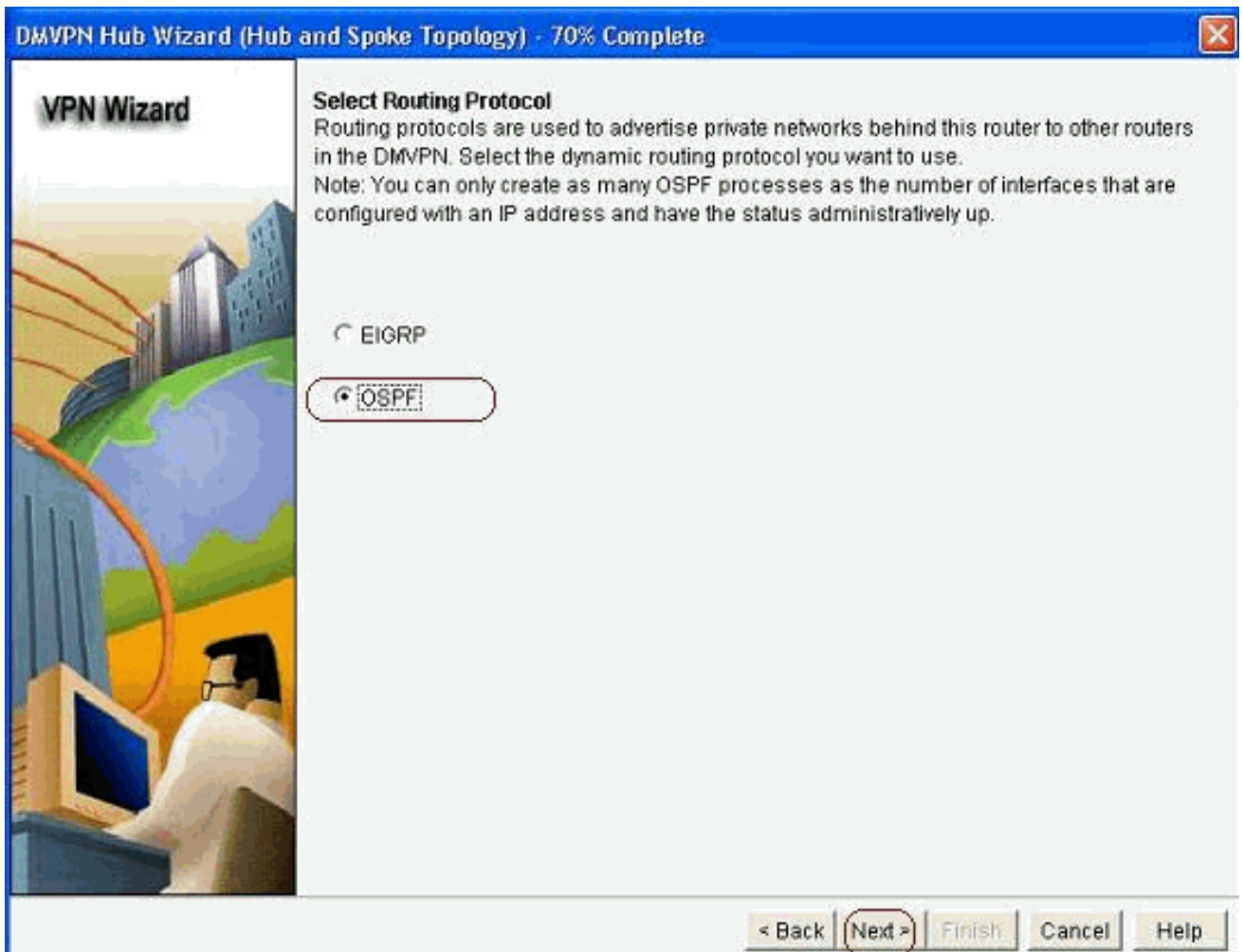
11. I nuovi criteri IKE possono essere visualizzati qui. Fare clic su Next (Avanti).



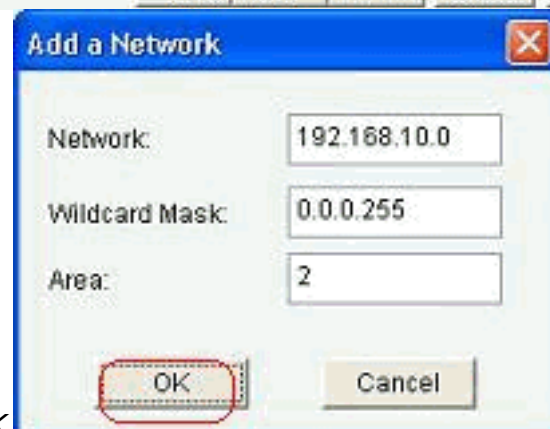
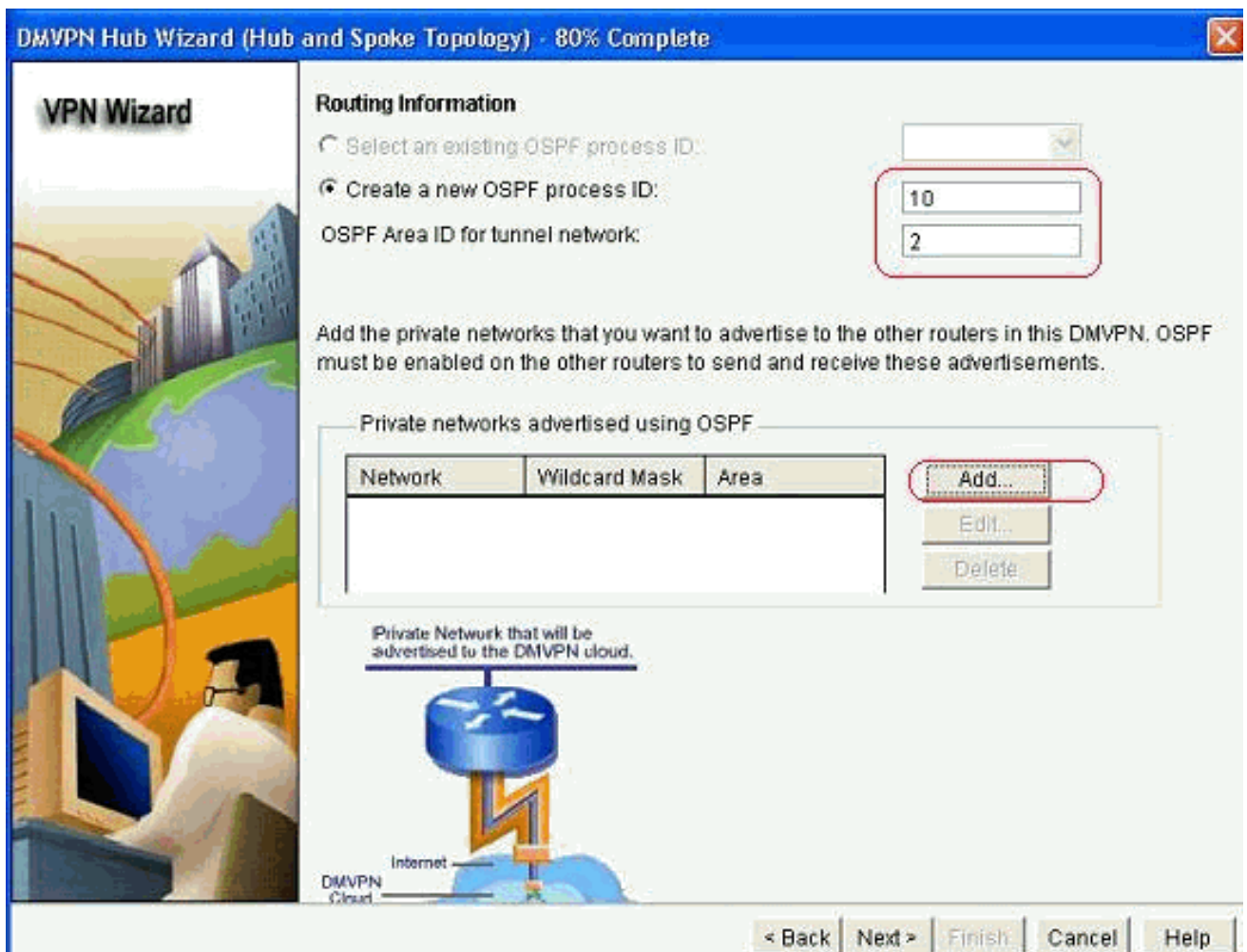
12. Fare clic su *Avanti* per continuare con il set di trasformazioni predefinito.



13. Selezionare il protocollo di routing desiderato. In questo caso, è selezionato *OSPF*.

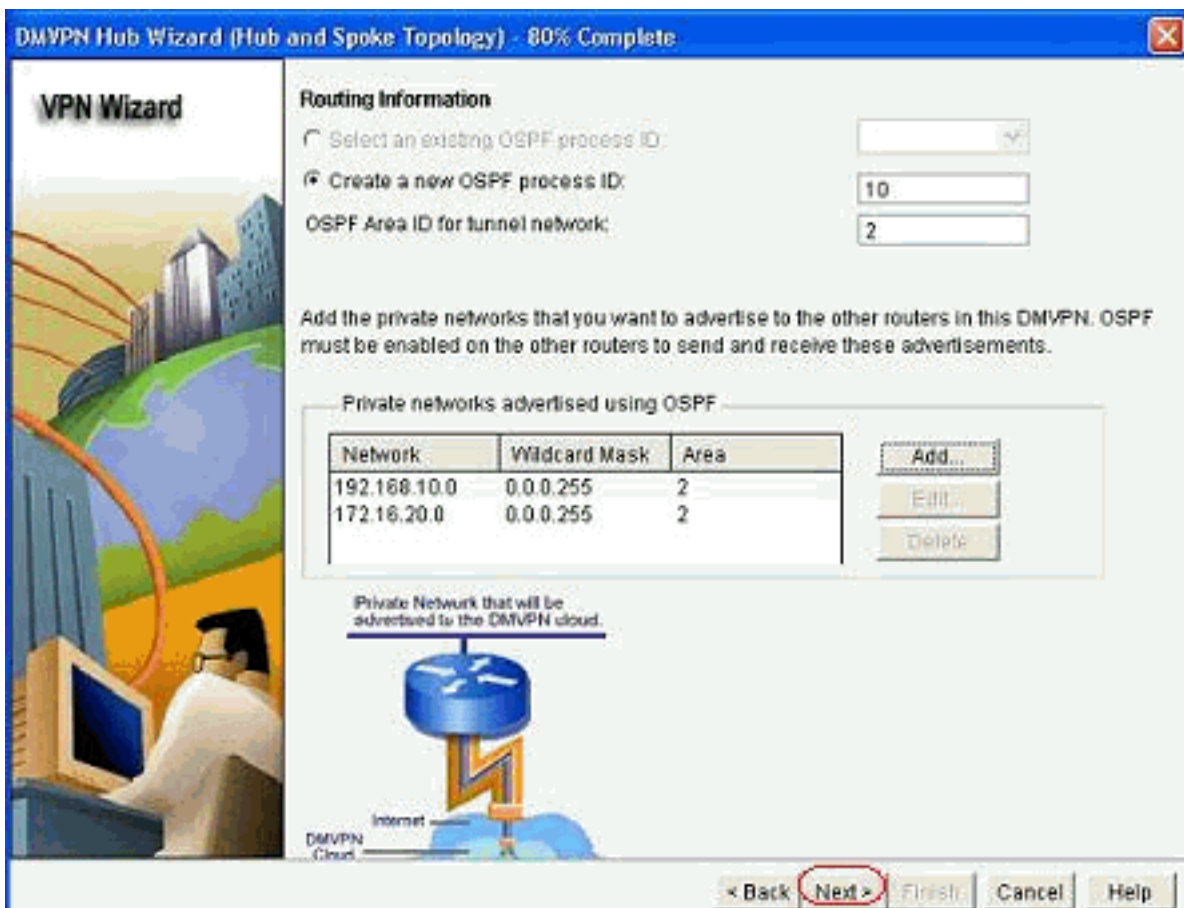


14. Specificare l'ID processo OSPF e l'ID area. Per aggiungere le reti che devono essere annunciate da OSPF, fare clic su *Add* (Aggiungi).



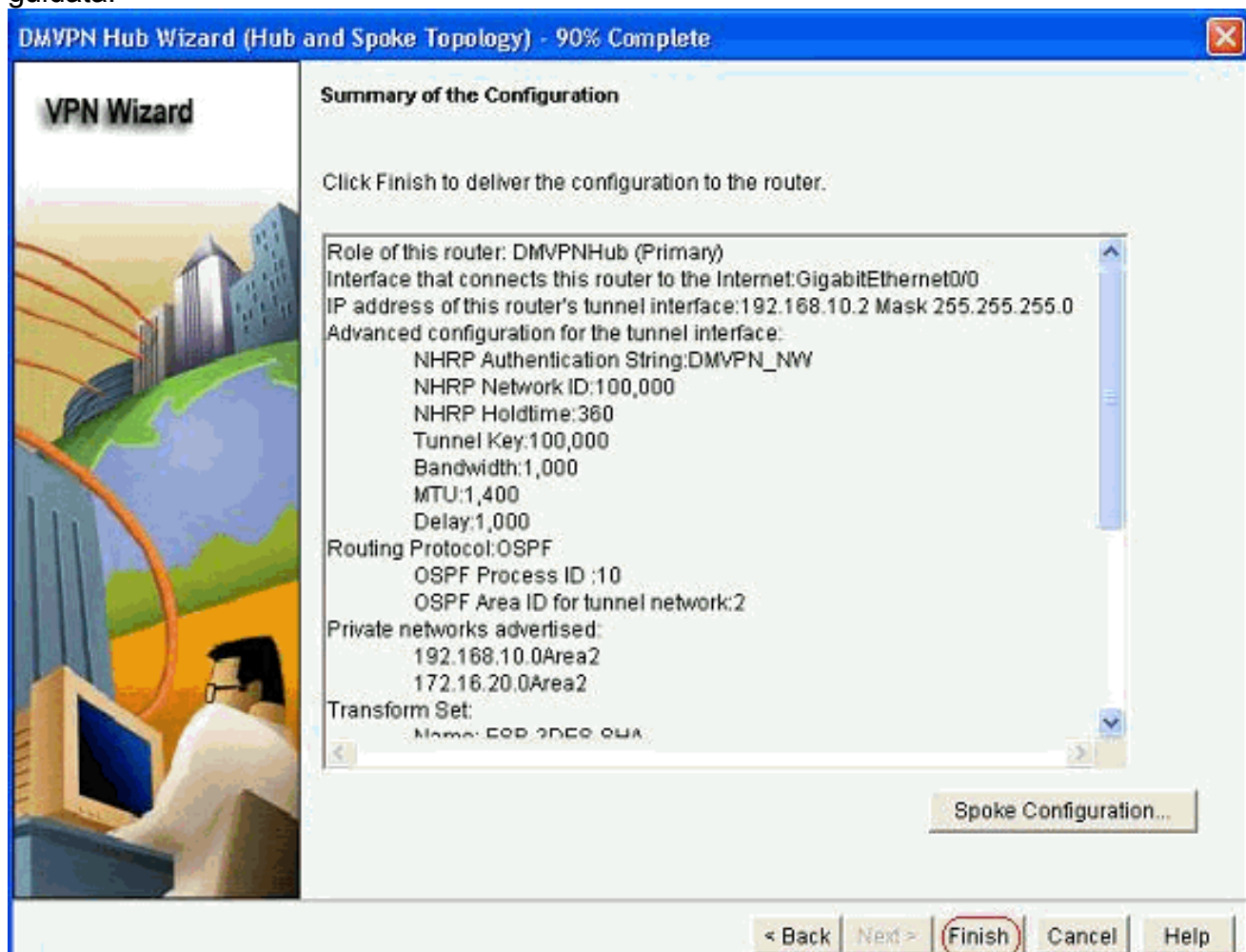
15. Aggiungere la rete del tunnel e fare clic su **OK**.

16. Aggiungere la rete privata dietro il router hub e fare clic su



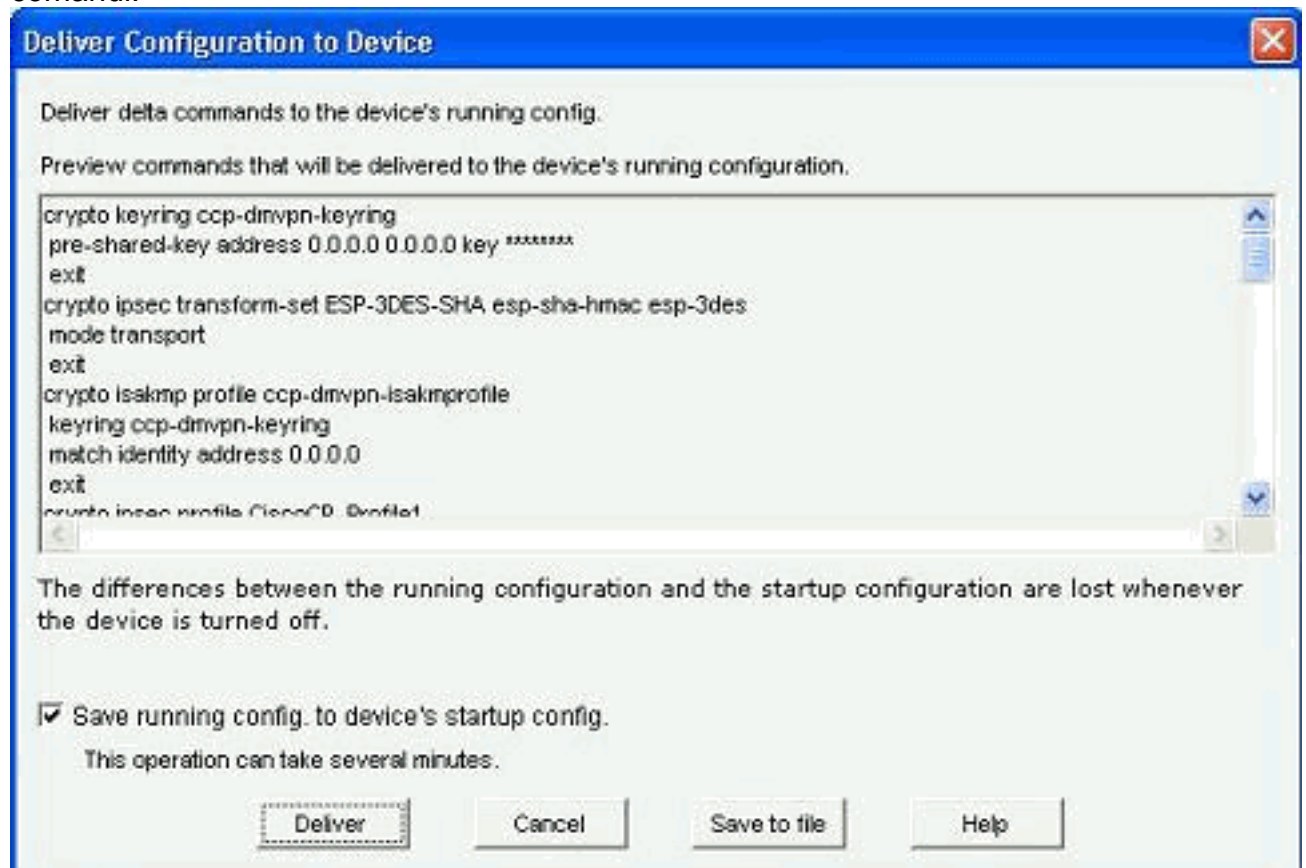
Avanti.

- Fare clic su *Fine* per completare la configurazione della procedura guidata.



- Fare clic su *Consegna* per eseguire i

comandi.



Configurazione CLI per hub

Di seguito è illustrata la configurazione CLI correlata:

```
Router hub
!
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
!

```

Modificare la configurazione DMVPN utilizzando CCP

È possibile modificare manualmente i parametri del tunnel DMVPN esistenti quando si seleziona l'interfaccia del tunnel e si fa clic su *Modifica*.

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

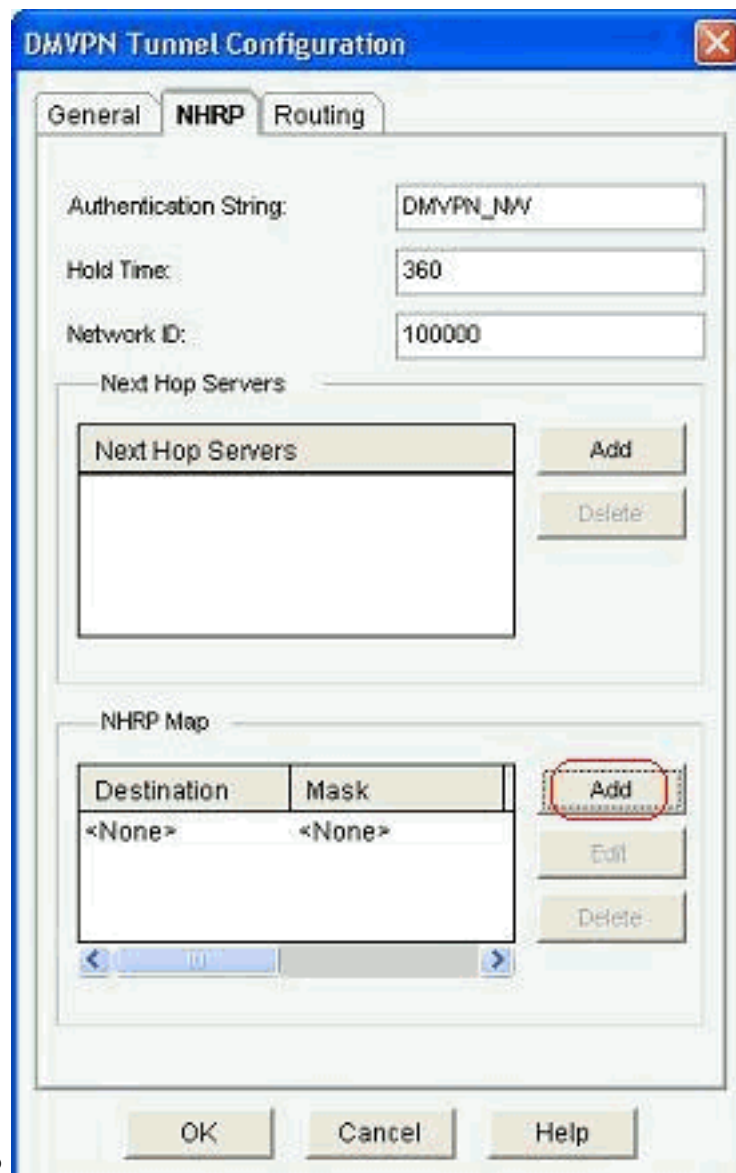
I parametri dell'interfaccia del tunnel, come MTU e chiave del tunnel, vengono modificati nella scheda *Generale*.

The image shows a screenshot of the 'DMVPN Tunnel Configuration' dialog box, specifically the 'NHRP' tab. The dialog has a blue title bar with a close button. It contains several sections for configuring the tunnel and NHRP parameters.

- General:** IP address: 192.168.10.2; Mask: 255.255.255.0 (with a dropdown for 24 bits).
- 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) 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. I parametri correlati a NHRP vengono individuati e modificati in base al requisito nella scheda *NHRP*. Nel caso di un router spoke, dovrebbe essere possibile visualizzare il servizio NHS come indirizzo IP del router hub. Per aggiungere il mapping NHRP, fare clic su *Aggiungi*



nella sezione Mappa NHRP.

2. A seconda dell'impostazione della rete, è possibile configurare i parametri di mapping NHRP

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):

— 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

come illustrato di seguito:

I parametri relativi al ciclo vengono visualizzati e modificati nella scheda *Ciclo*.



[Ulteriori informazioni](#)

I tunnel DMVPN sono configurati nei due modi seguenti:

- Comunicazione Spoke-to-Spoke attraverso l'hub
- Comunicazione spoke-to-spoke senza hub

In questo documento viene illustrato solo il primo metodo. Per consentire la creazione di tunnel IPsec dinamici spoke-to-spoke, questo approccio viene utilizzato per aggiungere spoke al cloud DMVPN:

1. Avviare la procedura guidata DMVPN e selezionare l'opzione di *configurazione Spoke*.
2. Dalla finestra *Topologia di rete DMVPN*, selezionare l'opzione *Rete a mesh completa* anziché l'opzione *Rete hub e spoke*.

DMVPN Spoke Wizard - 10% Complete

VPN Wizard

DMVPN Network Topology

Select the DMVPN network topology.

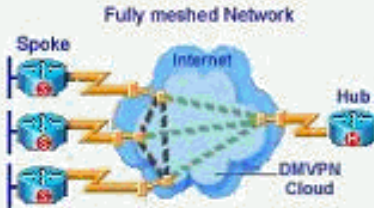
Hub and Spoke network

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. Completare il resto della configurazione seguendo la stessa procedura delle altre configurazioni descritte in questo documento.

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Informazioni correlate

- [Cisco Dynamic Multipoint VPN: Comunicazioni Branch-to-Branch semplici e sicure](#)
- [IOS 12.2 Dynamic Multipoint VPN \(DMVPN\)](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)