# 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 <u>Cisco Technical Tips</u> <u>Conventions</u> (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 <u>Command Lookup Tool</u> (nur <u>registrierte</u> 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.

 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).



2. Klicken Sie zum Starten auf *Weiter*.

DMVPN Spoke Wizard	
VPN Wizard	Configure a DMVPN spoke
	DMVPN allows you to create a scalable network that connects multiple remote routers to a central hub router using the same security features offered by site-to-site VPNs. DMVPN uses IPSec, NHRP, GRE and routing protocols to create secure tunnels between a hub and a spoke. This wizard allows you to configure the router as a DMVPN spoke. The wizard guides you through these tasks: * Specifying the DMVPN network topology. * Providing hub information. * Configuring a GRE tunnel interface. * Configuring a pre-shared key. * Configuring IKE policies. * Configuring an IPSec transform set. * Configuring a dynamic routing protocol. To begin, click Next.
	Reack Next > Finish Cancel Help

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



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 (H	ub and Spoke Topology) · 20% Complete		X
VPN Wizard	Specify Hub Information Enter the IP address of the hub and the IP addre Contact your network administrator to get this in	ess of the hub's mGRE tunnel interface. formation.	
	Hub Information IP address of hub's physical interface: IP address of hub's mGRE tunnel interface:	209.165.201.2	
	Spoke You are configuring this spoke router Padress of the mG to be entered above	Iblic IP address be entered above Hub RE tunnel	
		Back Next > Finish Cancel He	lp

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

VPN Wizard	GRE Tunnel Interface Configuration	
an de mangeliere	Select the interface that connects to the Ir	nternet: (FastEthernet0 🕑
	<ul> <li>Selecting an interface configured for a be always up.</li> <li>GRE Tunnel Interface</li> <li>A GRE tunnel interface will be created for address information for this interface.</li> <li>IP address of the tunnel interface –</li> <li>IP Address:</li> <li>192.168.10.5</li> <li>Subnet Mask:</li> <li>255.255.0</li> </ul>	a dialup connection may cause the connection to or this DMVPN connection. Please enter the 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 originaties	gical GRE/mGRE Tunnel interface. address of GRE/mGRE tunnel terface on all hube and spoke routers e private IP addresses and must be the same subnet. In more information please click the lp button.

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

Some of the following parameter in all devices in this DMVPN. Obt from your network administrator I Cisco CP defaults.	s should be identica ain the correct values before changing the
NHRP NHRP Authentication String:	DMVPN NW
NHRP Network ID:	100000
NHRP Hold Time:	360
GRE Tunnel Interface Inform	nation
Tunnel Key:	100000
Bandwidth:	1000
MTU:	1400
Tunnel Throughput Delay:	1000

den Hub-Parametern entsprechen.

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

	Authentiation		_
VPN Wizard	Authentication Select the method you of DMVPN network. You of the router must have a on this router must man in <b>Digital Certificates</b> in <b>Pre-shared Keys</b> pre-shared key: Reenter key:	want to use to authenticate this router to the peer device(s) in the an use digital certificate or a pre-shared key. If digital certificate is u valid certificate configured. If pre-shared key is used, the key config tch the keys configured on all other routers in the DMVPN network.	sed
		Reck Next Finish Concel He	

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

#### DMVPN Spoke Wizard (Hub and Spoke Topology) - 50% Complete

1.000.01	14.0	
VPN	Miza	<b>F</b> (1)
	TILLO	

#### **IKE Proposals**

IKE proposals specify the encryption algorithm, authentication algorithm and key exchange method that is used by this router when negotiating a VPN connection with the remote device. For the VPN connection to be established with the remote device, the remote device should be configured with at least one of the policies listed below.

Click the Add... button to add more policies and the Edit... button to edit an existing policy.

	Priority	Encryption	Hash	D-H Group	Authentication	Туре
	1	3DES	SHA_1	group2	PRE_SHARE	Cisco CP Defa
N and						
			Ĩ.			
	Add	Edit.				
	Add	Edit.				
	Add	Edit				
	Add	Edit				

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

Configure IKE Policy	
Priority:	Authentication:
2	PRE_SHARE
Encryption:	D-H Group:
AES_192	group1 🔛
Hash:	Lifetime:
SHA_1	24 0 0 HH:MM:SS
OK	Cancel Help

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

IKE F IKE p meth devic devic Click	Proposals roposals : od that is : e. For the ' e should t < the Add	specify the en used by this n VPN connecti be configured button to ado	cryption algo outer when n on to be esta with at least f more polici	rithm, authenticat egotiating a VPN blished with the r one of the policie es and the Edit I	ion algorithm and connection with t emote device, the s listed below. outton to edit an e	d key exchange he remote e remote existing policy.
	Priority	Encryption	Hash	D-H Group	Authentication	Type
	1	3DES	SHA 1	group2	PRE SHARE	Cisco CP Def
	Add	Edit				
	IKE F IKE p meth devic Clici	IKE Proposals method that is o device. For the o device should b Click the Add Priority 2 Add	IKE Proposals IKE proposals specify the en- method that is used by this in device. For the VPN connecti- device should be configured Click the Add button to add Priority Encryption Priority Encryption 2 AES_192	IKE Proposals IKE proposals specify the encryption algo method that is used by this router when n device. For the VPN connection to be esta device should be configured with at least Click the Add button to add more policie Priority Encryption Hash Priority Encryption Hash 2 AES_192 SHA_1 2 AES_192 SHA_1	IKE Proposals IKE proposals specify the encryption algorithm, authenticat method that is used by this router when negotiating a VPN device. For the VPN connection to be established with the r device should be configured with at least one of the policies Click the Add button to add more policies and the Edit I Priority Encryption Hash D-H Group Priority Encryption Hash I - H Group 2 AES_192 SHA_1 group2 2 AES_192 SHA_1 group1	IKE Proposals IKE proposals specify the encryption algorithm, authentication algorithm and method that is used by this router when negotiating a VPN connection with t device. For the VPN connection to be established with the remote device, the device should be configured with at least one of the policies listed below. Click the Add button to add more policies and the Edit button to edit an e Priority Encryption Hash D-H Group Authentication Priority Encryption Hash ID-H Group Authentication 2 AES_192 SHA_1 group1 PRE_SHARE 2 AES_192 SHA_1 group1 PRE_SHARE Add. Edit.

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

VOLUM	Transform Fat			
VPN Wizard	Transform Set I transform set specifies the Jata in the VPN tunnel. Since communicate, the remote de one selected below. Click the Add button to add ransform set. Select Transform Set:	encryption and auti the two devices mo vice must be config a new transform se	hentication algorit ust use the same ured with the sam and the Edit bu	hms used to protect th algorithms to ie transform set as the itton to edit the specifi
	Cisco CP Default Tran	nsform Set 🛛 💌		
	Details of the specified tra	ansform set		
	Name	ESP Encryption	ESP Integrity	AH Integrity
	ESP-3DES-SHA	ESP_3DES	ESP_SHA_HMAC	
	<			
	1 ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) ( ) (	14		

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

DMVPN Spoke Wizard (Hu	b and Spoke Topology) - 70% Complete	×
VPN Wizard	Select Routing Protocol Routing protocols are used to advertise private networks behind this router to other routers in the DMVPN. Select the dynamic routing protocol you want to use. Note: You can only create as many OSPF processes as the number of interfaces that are configured with an IP address and have the status administratively up. C EIGRP COSPF	
	Back Next > Finish Cancel Help	

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



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

Weiter.

zard Routing Information	6			
C Select an existing	<ul> <li>Select an existing OSPF process ID.</li> </ul>			
Create a new OS	Create a new OSPF process ID:			
OSPF Area ID for tur	nnel network:		2	
Add the private networks	orks that you want the other routers t advertised using	to advertise to o send and red OSPF	the other routers in this ceive these advertiseme	
Network	Wildcard Mask	Area	Add	
192.168.10.0	0.0.0.255	2	Edit	
172.16.18.0	0.0.0.255	2	Delete	
Private Network t advertised to the	hat will be DMIVPN cloud.			

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.

Derver della commanda lo tric device	es running config.			
Preview commands that will be delive	ered to the device's	running configuration.		
crypto ipsec transform-set ESP-3DE	S-SHA esp-sha-hma	ic esp-3des		^
node transport				
crypto ipsec profile CiscoCP_Profile1	ř.			1.1
set transform-set ESP-3DES-SHA	53.			
exit				
interface Tunnel0				
exe defective to the second s				
interface Tunnel0				1
handwidth 1000				Y
<				2.
The differences between the ru the device is turned off.	nning configurati	on and the startup c	onfiguration are los	t whenever
Save running config to device	's startup config.			
ouver failing coning. to defice				
Save running config to device	's startup config.			

## **CLI-Konfiguration für Spoke**

Die entsprechende CLI-Konfiguration wird hier angezeigt:

Spoke-Router
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 TunnelO
bandwidth 1000
delay 1000
ip nhrp holdtime 360
ip nhrp network-id 100000
ip nhrp authentication DMVPN_NW
ip ospi network point-to-multipoint
ip mtu 1400
no shutdown
1p address 192.168.10.5 255.255.255.0
ip top adjust-mss 1360
1p nnrp nns 192.168.10.2
ip mirp map 192.168.10.2 209.165.201.2
tunnel doctination 200 165 201 2
tunnel protoction incode profile CiccoCD Profile1
tunnel kov 100000
CULLET VEN TOODOO

```
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*.



### 2. Klicken Sie auf

### Weiter.

DMVPN Hub Wizard	
VPN Wizard	Configure a DMVPN hub
	DMVPN allows you to create a scalable network that connects multiple remote routers to a central hub router using the same security features offered by site-to-site VPNs. DMVPN uses IPSec, NHRP, GRE and routing protocols to create secure tunnels between a hub and a spoke. This wizard allows you to configure the router as a DMVPN hub. The wizard guides you through these tasks: * Specifying the DMVPN network topology. * Specifying the DMVPN network topology. * Configuring a multipoint GRE tunnel. * Configuring a pre-shared key. * Configuring an IPSec transform set. * Configuring an IPSec transform set. * Configuring a dynamic routing protocol. To begin, click Next.
	< Back Next > Finish Cancel Help

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

DMVPN Hub Wizard -	10% Complete	×
VPN Wizard	DMVPN Network Topology Select the DMVPN network topology.	
Lat	(F Hub and Spoke network	
	In this topology, all DMVPN traffic is routed through the hub. A point-to-point GRE interfa will be configured on the spoke, and the spoke will use it to create a tunnel to the hub v will remain up. Spokes do not create GRE tunnels to other spokes in this topology.	ice vhich
	C Fully meshed network	
	In this topology, the spoke dynamically establishes a direct tunnel to another spoke de and sends DMVPN traffic directly to it. A multipoint GRE tunnel interface is configured o spoke to support this functionality.	wice, n the
H) a	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 Hub Hub Hub Hub Hub Hub Hub Hub Hub Hub	
	< Back Next > Finish Cancel	Help

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

DMVPN Hub Wizard (H	ub and Spoke Topology) - 15% Complete	
VPN Wizard	Type of Hub In a DMVPN network there will be a hub router and multiple spoke routers connecting hub. You can also configure multiple routers as hubs. The additional routers will act a backups. Select the type of hub you want to configure this router as.	to the s
	Primary hub	
	C Backup Hub(Cisco CP does not support backup hub configuration on this router)	
	< Back Next > Finish Cancel	Help

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

VPN Wizard	Multipoint GRE Tunnel Interface Configuration							
re- nec nezeranijekovan	Select the interface that cor	Select the interface that connects to the Internet: GigabitEthernet0/0						
	A GRE tunnel interface with the second secon	onfigured for a ( ) Tunnel Interfa Il be created for	lialup coni ce this DMVF	nection may cause the conne PN connection. Please enter	action			
	address information for the tun	address information for this interface.						
	IP Address:		Click Ac	Click Educerand to unit disturburs				
	192.168.10.2		match peer settings.					
	Subnet Mask:	Subnet Mask:			Advanced.			
	255.255.255.0	24						
	Interface connected to Internet. This is the interface from which GRE/mGRE Tunnel originaties-	Log IP a inter are in th For help	cal GRE/mG ddress of GR face on all h private IP ad e same subr more informat button.	RE Turnel interface. RE/mGRE tunnel ubs and spoke routers dresses and must be net. ation please click the				

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

in all devices in this DMVPN. Obt from your network administrator to Cisco CP defaults.	ain the correct va pefore changing
NHRP Authentication String:	DMVPN_NW
NHRP Network ID:	100000
NHRP Hold Time:	360
GRE Tunnel Interface Inform	100000
Bandwidth:	1000
MTU:	1400
Tuppel Throughput Dolor	1000

7. Geben Sie die Option basierend auf Ihrer Netzwerkeinrichtung



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

d Spoke Topology) - uthentication elect the method you w	40% Complete			×
uthentication elect the method you w				
MVPN network. You ca le router must have a v n this router must mate © Digital Certificates Pre-shared Keys pre-shared key: Reenter key:	vant to use to authe in use digital certific ralid certificate confi ch the keys configue 	nticate this router to ti cate or a pre-shared k gured. If pre-shared k red on all other router	he peer device(s) in the ey. If digital certificate is u ey is used, the key config s in the DMVPN network.	ised, ured
		< Back (Next >)	Finish Cancel He	eto 1
	<ul> <li>router must have a v n this router must mate</li> <li>Digital Certificates</li> <li>Pre-shared Keys</li> <li>pre-shared key:</li> <li>Reenter key:</li> </ul>	re router must have a valid certificate configure in this router must match the keys configure in the keys configure in this router must match the keys configure in this router must match the keys configure in this router must match the keys configure in this router in the keys configure in th	refrection for car able angle configured of the shared is     n this router must have a valid certificate configured on all other router     Oigital Certificates     pre-shared Keys     pre-shared key:     Reenter key:	Pre-shared Keys     pre-shared key:     This router was a valid certificate configured on all other routers in the DMVPN network     Pre-shared Keys     pre-shared Keys     Reenter key:     This router key:     Cancel He

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

#### DMVPN Hub Wizard (Hub and Spoke Topology) - 50% Complete

A COM	144	
	MUTOR	

#### **IKE Proposals**

IKE proposals specify the encryption algorithm, authentication algorithm and key exchange method that is used by this router when negotiating a VPN connection with the remote device. For the VPN connection to be established with the remote device, the remote device should be configured with at least one of the policies listed below.

Click the Add... button to add more policies and the Edit... button to edit an existing policy.

1	Priority	Encryption	Hash	D-H Group	Authentication	Туре
	1	3DES	SHA_1	group2	PRE_SHARE	Cisco CP Defa
-			t			
1	\dd	Edit				
0						
				1	i i i	

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

Configure IKE Policy				
Priority:	Authentication:			
2	PRE_SHARE			
Encryption:	D-H Group:			
AES_192 🗸 🗸	group1 😪			
Hash:	Lifetime:			
SHA_1	24 0 0 HH:MM:SS			
OK	Cancel Help			

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

X

· · · · · · · · · · · · · · · · · · ·									
VPN Wizard	IKE Prop IKE prop method t device. F device st	IKE Proposals IKE proposals specify the encryption algorithm, authentication algorithm and key exchange method that is used by this router when negotiating a VPN connection with the remote device. For the VPN connection to be established with the remote device, the remote device should be configured with at least one of the policies listed below.							
	Click the	e Add. Priority	Encryption	d more polici Hash	D-H Group	Authentication	existing policy. Type		
	2		3DES AES_192	SHA_1 SHA_1	group2 group1	PRE_SHARE PRE_SHARE	Cisco CP Defa User Defined		
KA	Adu	d	Edit.						
	1.				< Back Ne	a) Finish   a	Cancel Hel		

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

VDN Wizard	Transform Set			
	A transform set specifies data in the VPN tunnel. S communicate, the remotione selected below. Click the Add button to transform set. Select Transform Set:	s the encryption and aut Since the two devices m le device must be config add a new transform se	hentication algorit ust use the same ured with the sam it and the Edit bu	hms used to protect the algorithms to le transform set as the itton to edit the specifie
Call	Cisco CP Default	Transform Set		
	Details of the specific	ed transform set		
	Name	ESP Encryption	ESP Integrity	AH Integrity
	ESP-3DES-SH	A ESP_3DES	ESP_SHA_HMAC	
KE				2
	Add E	dit		

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

DMVPN Hub Wizard (Hub	and Spoke Topology) - 70% Complete
VPN Wizard	Select Routing Protocol Routing protocols are used to advertise private networks behind this router to other routers in the DMVPN. Select the dynamic routing protocol you want to use. Note: You can only create as many OSPF processes as the number of interfaces that are configured with an IP address and have the status administratively up. C EIGRP COSPF
	<ul> <li>Back Next &gt; Finish Cancel Help</li> </ul>

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.



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

192.168.10.0

Cancel

0.0.0.255

2

Network:

Area:

OK.

Wildcard Mask:

OK

VPN Wizard	Routing Information	n		
	C Select an existen	g OSPF process ID		37
	(* Create a new OSPF process ID:		10	
	OSPF Area ID for tu	innel network:		2
	Add the private network must be enabled or Private network Network 192.168.10.0 172.16.20.0	vorks that you want in the other routers t s advertised using Wildcard Mask 0.0.0.255 0.0.0.255	to advertise to o send and re OSPF Area 2 2	the other routers in this DMVPN. I ceive these advertisements.
Ja	Private Network advertised to the	that will be DMVPN cloud.		

Weiter.

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

VPN Wizard         Summary of the Configuration           Click Finish to deliver the configuration to the router.         Click Finish to deliver the configuration to the router.           Role of this router: DMVPNHub (Primary)         Interface that connects this router to the Internet: GigabitEthernet0/0           IP address of this router's tunnel interface:192.168.10.2 Mask 255.25         Advanced configuration for the tunnel interface:           NHRP Authentication String:DMVPN_NWV         NHRP Network ID:100,000           NHRP Holdtime:360         Tumperel Kow100	~
Click Finish to deliver the configuration to the router. Role of this router: DMVPNHub (Primary) Interface that connects this router to the Internet.GigabitEthernet0/0 IP address of this router's tunnel interface:192.168.10.2 Mask 255.25 Advanced configuration for the tunnel interface: NHRP Authentication String:DMVPN_NW NHRP Network ID:100,000 NHRP Holdtime:300	^
Role of this router: DMVPNHub (Primary) Interface that connects this router to the Internet.GigabitEthernet0/0 IP address of this router's tunnel interface:192.168.10.2 Mask 255.25 Advanced configuration for the tunnel interface: NHRP Authentication String:DMVPN_NW NHRP Network ID:100,000 NHRP Holdtime:360	^
Routing Protocol: OSPF OSPF Process ID :10 OSPF Area ID for tunnel network:2 Private networks advertised: 192.168.10.0Area2 172.16.20.0Area2 Transform Set:	5.255.0
Spok	e Configuration

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 abcdl23 address 0.0.0.0 0.0.0.0
crypto ipsec transform-set ESP-3DES-SHA esp-3des esp-
sna-nmac
mode transport
: ammte ingeg profile diggodD Drofile1
ast transform ast ESD 2DES SUN
Set Clansion-Set ESP-SDES-SHA
: interface Tunnel()
handwidth 1000
in 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.

VPN				
reate Dynamic Multipo	int VPN (DMVPN)	Edit Dynamic	: Multipoint VPN (DMVPN)	Add
Interface	IPSec Pr	ofile	IP Address	Description
Funnel0	CiscoCP_	Profile1	192.168.10.2	<none></none>
Details for interface Tu	nnelO:			
Details for interface Tu Item Name	nnel0:		Item Value	
Details for interface Tu Item Name nterface	nnel0:		Item Value Tunnel0	
Details for interface Tu Item Name nterface PSec Profile	nnel0:		Item Value Tunnel0 CiscoCP_Profile1	
Details for interface Tu Item Name Interface PSec Profile P Address	nnel0:		Item Value Tunnel0 CiscoCP_Profile1 192.168.10.2	
Details for interface Tu Item Name Interface PSec Profile P Address Description Suppel Bandwidth	nnel0:		Item Value Tunnel0 CiscoCP_Profile1 192.168.10.2 <none> 1000</none>	
Details for interface Tu Item Name Interface PSec Profile P Address Description Funnel Bandwidth	nnel0:		Item Value Tunnel0 CiscoCP_Profile1 192.168.10.2 «None» 1000 1400	
Details for interface Tu Item Name nterface PSec Profile P Address Description Funnel Bandwidth I/TU VHRP Authentication	nnel0:		Item Value Tunnel0 CiscoCP_Profile1 192.168.10.2 «None» 1000 1400 DMVPN_NW	
Details for interface Tu Item Name Interface IPSec Profile IP Address Description Tunnel Bandwidth MTU NHRP Authentication NHRP Network ID	nnel0:		Item Value Tunnel0 CiscoCP_Profile1 192.168.10.2 «None» 1000 1400 DMVPN_NW/ 100000	
Details for interface Tu Item Name Interface IPSec Profile IP Address Description Tunnel Bandwidth WTU NHRP Authentication NHRP Network ID NHRP Hold Time	nnel0:		Item Value Tunnel0 CiscoCP_Profile1 192.168.10.2 «None» 1000 1400 DMVPN_NW 100000 360	

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

eneral NHRP R	outing
IP address:	192.168.10.2
Mask:	255.255.255.0 24
Interface:	GigabitEthernet0/0
C P address:	
- Tunnel Destination:	
Tunnel Destination: This is an multipoir P / Hostname:	t GRE Tunnel
Tunnel Destination: This is an multipoir P/Hostname:	t GRE Tunnel
Tunnel Destination: This is an multipoir P / Hostname: PSec Profile: MTU:	t GRE Tunnel CiscoCP_Proti Add 1400
Tunnel Destination: This is an multipoir P / Hostname: PSec Profile: MTU: Bandwidth:	t GRE Tunnel CiscoCP_Proti Add 1400 1000
Tunnel Destination: This is an multipoir P/Hostname: PSec Profile: MTU: Bandwidth: Delay:	t GRE Tunnel  CiscoCP_Proti  Add  1400  1000  1000

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.	,NWV	
fold Time:	360	360	
letwork ID:	100000		
-Next Hop Servers	S		
Next Hop Servers	5	Add	
		Delete	
NHRP Map			
NHRP Map Destination	Mask	Add	

NHRP-Zuordnung hinzuzufügen.

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

C 1	Statically configure th	ne IP-to-NMBA addres	s mapping
	of IP destinations co	onnected to a NBMA i	network.
	Destination read	hable through NBMA	network
	IP Address:		
	Mask (Optional):	-	
	NDM0 address a	live attractions	
	NBINA address t	prectly reachable	
	IP Address		
G	Configure NBMA add	lesses used as des	tinations for broades
	r multicast nackets t	n he sent over a tunn	el network
č	i manifesti pacifeto t		or notwork.
	Dynamically add	spokes' IP addresse	s to hub's multicast
	C IP address of NB	MA address directly r	eachable
		mer address directly i	Cucinable

Die Routingparameter werden auf der Registerkarte Routing angezeigt und geändert.

General NHRP Routin	a 🗌 👘
Routing Protocol:	OSPF N
Ø OSPF	
OSPF Network Type:	point-to-multipoint
OSPF Priority:	
Hello Interval:	
Dead Interval:	

### 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*.



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

# <u>Überprüfung</u>

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

## Zugehörige Informationen

- <u>Cisco Dynamic Multipoint VPN: Einfache und sichere Kommunikation zwischen Zweigstellen</u>
- IOS 12.2 Dynamic Multipoint VPN (DMVPN)
- <u>Technischer Support und Dokumentation für Cisco Systeme</u>