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 <u>分支的CLI配置</u> 使用Cisco CP的集線器配置 <u>集線器的CLI配置</u> 使用CCP編輯DMVPN配置 更多資訊 驗證 相關資訊

<u>簡介</u>

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。

<u>必要條件</u>

<u>需求</u>

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。

<u>採用元件</u>

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。

<u>慣例</u>

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。

<u>背景資訊</u>

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

<u>設定</u>

本節提供用於設定本文件中所述功能的資訊。

註:使用<u>Command Lookup Tool</u>(僅<u>供</u>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

tasko Configure > Security > VPN > Dynamic Multipoint VPN

VPN		
Create Dynamic Multipoint VPN (DMVPN	B Edit Dynamic Multipoint VPN (DMVPN)	
Configure DMVPN Spoke		
Senter 2	outer as a spoke in a full mesh or hub complete this configuration, you must P information, pre-shared key, IKE temamic routing protocol information	
Create a hub (server or head-end)	in a DMVPN	
Use this option to configure the re are configuring a backup hub, you information, pre-shared key, IKE (dynamic routing protocol information)	outer as a primary or backup hub. If you u must know the primary hub's NHRP policy, IPSec Transform set and tion.	
	aunch the selected task	

2. 按一下*Next*開始。

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 an IPSec transform set. * Configuring a dynamic routing protocol. To begin, click Next.
	< Back Next > Finish Cancel Help

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



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。

DMVPN Spoke Wizard (Hu	b and Spoke Topology) - 20% Complete		×
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.	
$\sim h$	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 P address of the mG to be entered above	iblic IP address be entered above Hub RE tunnel	
	<	Back Next > Finish Cancel Hel	p

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。

PN Wizard	GRE Tunnel Interface Configuration	ion -	
an rinn - aith Manual - aite	Select the interface that connects to	to the Internet: (FastEthernet0)	~
	Selecting an interface configured be always up. GRE Tunnel Interface A GRE tunnel Interface will be created of the second of the	reated for a dialup connection may cause the connection may cause the connection reated for this DMVPN connection. Please enter inface. erface Advanced settings Click Advanced to verify that values match peer settings.	the
	Interface connected to Internet. This is the interface from which GRE/mGRE Tunnel originaties-	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. 驗證隧道引數和NHRP引數,並確保它們與Hub引數完全匹配。

ome of the following parameter a all devices in this DMVPN. Obt om your network administrator t isco CP defaults.	s should be identica ain the correct value: 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

7. 指定預共用金鑰並按一下下一步。

VPN Wizard	Authentication		
	Select the method you w DMVPN network. You ca the router must have a v on this router must mate	vant to use to authenticate this n use digital certificate or a pr alid certificate configured. If pr th the keys configured on all c	router to the peer device(s) in the e-shared key. If digital certificate is used e-shared key is used, the key configured ther routers in the DMVPN network.
	O Digital Certificates O Pre-shared Keys		
	pre-shared key:		
B	Reenter key:		
		< Back	Next Finish Cancel Help

8. 按一下Add以新增單獨的IKE提議。

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

VPN Wizard

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.

and a second		Priority	Encryption	Hash	D-H Group	Authentication	Туре
		1	3DES	SHA_1	group2	PRE_SHARE	Cisco CP Defa
17							
214							
pril.							
Care and							
AL.							
	-		1	1			
and the second	F	Add	Edit				
100	-	_					
14							
					1		122

9. 指定加密、驗證和雜湊引數。然後,按一下OK。

Priority:	Authentication:
2	PRE_SHARE
Encryption:	D-H Group:
AES_192 🛃	group1 😪
Hash:	Lifetime:
SHA_1	24 0 0 HH:MM:SS

10. 此處可以看到新建立的IKE策略。按「Next」(下一步)。

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

VPN Wizard

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.

1.0	Priority	Encryption	Hash	D-H Group	Authentication	Туре
1	1	3DES	SHA_1	group2	PRE_SHARE	Cisco CP Defa
	2	AES_192	SHA_1	group1	PRE_SHARE	User Defined
			1			
	Add	Edit]			
	Add	Edit				

11. 按一下下一步繼續使用預設轉換集。

	and the second second			
VPN Wizard	A transform set specifies th data in the VPN tunnel. Sinc communicate, the remote d	e encryption and auti te the two devices mi evice must be config	hentication algorit ust use the same ured with the sam	hms used to protect the algorithms to e transform set as the
	Click the Add button to add transform set. Select Transform Set:	d a new transform se insform Set 💽 💌 –	t and the Edit bu	tton to edit the specifie
	Details of the specified t	ransform set		
	Name	ESP Encryption	ESP Integrity	AH Integrity
A	SE ESP-3DES-SHA	ESP_3DES	ESP_SHA_HMAC	
	<			>

12. 選擇所需的路由協定。此處選擇了OSPF。

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.
	< Back Next > Finish Cancel Help

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。

and the second second	routing mormation		
	C Select an existing OSPF proce	ss ID	4
	Create a new OSPF process II). (10)	
	OSPF Area ID for tunnel network:	2	
	Add the private networks that you must be enabled on the other rou	want to advertise to the other routers in ters to send and receive these advertis using OSPF	this DMVPN. (ements.
	Network Wildcard M	fask Årea	
	DMVPN Cloud		
	(and the second se	< Back Next > Finish	Cancel
	Add a Network		
	Network:	192.168.10.0	
	Network: Wildcard Mask	192.168.10.0 0.0.0.255	
	Network: Wildcard Mask Area:	192.168.10.0 0.0.0.255 2	
	DMVPN Internet	< Back Next > Finish	Canci

lizard Rot	ting Information	n;;		
ം റ	Select an existin	g OSPF process ID		
(* (Create a new OS	SPF process ID:		10
OS OS	PF Area ID for tu	innel network:		2
Ado	I the private netv st be enabled of Private network	vorks that you want n the other routers t ks advertised using	to advertise to o send and rec OSPF	the other routers in this DM eive these advertisements
	Network	Wildcard Mask	Area	Add
a see p	192.168.10.0	0.0.0.255	2	Field
1000	172.16;18.0	0.0.0.255	2	Delete
	Private Network advertised to the	that will be • DMVPN cloud.		
		1		

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。

Deliver Configuration to Device	
Deliver delta commands to the device's running config. Preview commands that will be delivered to the device's running configuration.	
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 Interface 1000	~
	2.
The differences between the running configuration and the startup configuration are the device is turned off. Save running config. to device's startup config. This operation can take several minutes. Deliver Cancel Save to file Help	e lost whenever



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*。



2. 按「*Next*」(下一步)。

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 hub type. * Configuring a multipoint GRE tunnel. * Configuring a pre-shared key. * Configuring an IPSec transform set. * Configuring a dynamic routing protocol. To begin, click Next.
	< Back Next > Finish Cancel Help

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



4. 選擇Primary Hub。然後,按一下下一步。

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

5. 指定Tunnel介面引數,然後按一下Advanced。

VPN Wizard	Multipoint GRE Tunnel Inter	face Configura	tion
ne na na nativaliti na	Select the interface that con	nects to the Inte	emet: (GigabitEthemet0/0) 💌
	A Selecting an interface co be always up.	nfigured for a c	lialup connection may cause the connection
	A GRE tunnel interface will address information for th	l be created for is interface. iel interface —	this DMVPN connection. Please enter the Advanced settings
Cast Chan	IP Address:		Click Advanced to varify that values
	192.168.10.2		match peer settings.
	Subnet Mask	17.5	Advanced
	255.255.255.0	24	
	Interface connected to Internet. This is the interface from which GRE/mGRE Tunnel originaties-	Logi IP as inter are of in the For 1 help	cal GRE/mGRE Tunnel interface. ddress of GRE/mGRE tunnel face on all hubs and spoke routers sivate IP addresses and must be a same subnet. more information please click the button.

and here been been been been

6. 指定隧道引數和NHRP引數。然後,按一下*OK*。 Advanced configuration for the tunnel inter... 🕅

JISCO CP defaults.	efore changing th
NHRP	
NHRP Authentication String:	DMVPN_NW
NHRP Network ID:	100000
NHRP Hold Time:	360
	nation
GRE Tunnel Interface Inform Tunnel Key:	nation
GRE Tunnel Interface Inform Tunnel Key: Bandwidth:	100000
GRE Tunnel Interface Inform Tunnel Key: Bandwidth: MTU:	100000 1000 1000

7. 根據您的網路設定指定選項。

Cisco CP Warning		
	Do you use the same router for Easy VPN Server.	
	Yes	

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

UMVPN HUO WIZATO (HI	uo and spoke Topology) -	40% Complete		A
VPN Wizard	Authentication Select the method you w DMVPN network. You ca the router must have a w on this router must mat C Digital Certificates Pre-shared Keys	vant to use to authe an use digital certifi /alid certificate conf ch the keys configu	enticate this router to the p cate or a pre-shared key igured. If pre-shared key red on all other routers in	peer device(s) in the If digital certificate is used, is used, the key configured the DMVPN network.
	pre-shared key: Reenter key:			
			Sack Next >	ish Cancel Help

9. 按一下Add以新增單獨的IKE提議。

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

VPN Wizard

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.

A LUNA		Priority	Encryption	Hash	D-H Group	Authentication	Туре
	1	1	3DES	SHA_1	group2	PRE_SHARE	Cisco CP Defa
1							
Specify -							
and the second second							
	5			f			
		4dd	Edit				
1100	É						
100							
							11

- <Back Next> Finish Cancel Help
- 10. 指定加密、驗證和雜湊引數。然後,按一下OK。

Priority:	Authentication:
2	PRE_SHARE
Incryption:	D-H Group:
NES_192 🛛 💙	group1 🛛 👻
lash:	Lifetime:
SHA_1 😽	24 0 0 HH:MM:SS

11. 此處可以看到新建立的IKE策略。按「Next」(下一步)。

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

1.00		14.4		
VP	AL.	MAX	17.9	20
10.00		11	140	

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
2	AES_192	SHA_1	group1	PRE_SHARE	User Defined
 	10 T	1			
Add	Edit.				
Add	Edit]			
Add	Edit.]			

12. 按一下下一步繼續使用預設轉換集。

VPN Wizard	Transform Set	4. 33. 3. 4		6 - 245 - 556.55
	A transform set specifies	the encryption and aut	hentication algorit	hms used to protect the
	communicate the remot	e device must be confic	ust use the same	algorithms to transform set as the
	one selected below.	e dente mastre com	area marine our	te nonstoriti serus inc
	Click the Add button to	add a new transform se	et and the Edit bu	itton to edit the specifie
	transform set.			
	Select Transform Set:			
The second second				
MARCON 3	Cisco CP Default	Transform Set		
	Details of the specifie	ed transform set		
	Name	ESP Encryption	ESP Integrity	AH Integrity
	ESP-3DES-SH	A ESP 3DES	ESP SHA HMAC	(at the gray
1 Section				2
	Add	üt		
A DECEMBER OF A				

13. 選擇所需的路由協定。此處選擇了*OSPF*。

DMVPN Hub Wizard (H	lub and Spoke Topology) - 70% Complete 📃 🗧
VPN Wizard	Select Routing Protocol Routing protocols are used to advertise private networks behind this router to other routers. About DMVPN. Select the dynamic routing protocol you want to use. About DMVPN. Select the dynamic routing protocol you want to use. About DMVPN. Select the dynamic routing protocol you want to use. About DMVPN. Select the dynamic routing protocol you want to use. About DMVPN. Select the dynamic routing protocol you want to use. About DMVPN. Select the dynamic routing protocol you want to use. About DMVPN. Select the dynamic routing protocol you want to use. About DMVPN. Select the dynamic routing protocol you want to use. About DMVPN. Select the dynamic routing protocol you want to use. About DMVPN. Select the dynamic routing protocol you want to use. About DMVPN. Select the dynamic routing protocol you want to use. About DMVPN. Select the dynamic routing protocol you want to use. About DMVPN. Select the dynamic routing protocol you want to use. About DMVPN. Select the dynamic routing protocol you want to use. About DMVPN. Select the dynamic routing protocol you want to use. About DMVPN. Select the dynamic routing protocol you want to use. About DMVPN. Select the dynamic routing protocol you want to use. About DMVPN. Select the dynamic routing protocol you want to use. About DMVPN. Select the dyna
	< Back Next > Finish Cancel Help

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。

VPN Wizard	Routing Information		
	C Select an existing OSPF process ID.	×	
	Create a new OSPF process ID:		
	OSPF Area ID for tunnel network:	j	
	Add the private networks that you want to advertise to the other must be enabled on the other routers to send and receive thes	routers in this DMVPN e advertisements.	
	Network Wildcard Mask Area	bhA	
NA			
	DMVPN DMVPN		
	DMVPN Closed & Different Under Back Next >	Finish Cancel	
	Add a Network	Finish Cancel	
	Add a Network: 192.168.10.0	Finish Cancel	
	Add a Network: Network: 192.168.10.0 Wildcard Mask: 0.0.255	Finish Cancel	
	Add a Network 192168.10.0 Wildcard Mask 0.0.255 Area: 2	Finish Cancel	
	Add a Network: Network: Network: Network: Network: Network: 192.168.10.0 Wildcard Mask: Area: 2	Finish Cancel	

Vizard	Routing Informatio	n		
	C Select an existen	g OSPF process ID		35
	(F Create a new Os	SPF process ID:		10
1	OSPF Area ID for tu	innel network:		2
	Private network	is advertised using	OSPF	rene mese auvenisements.
	Network	Wildcard Mask	Area	Add
	102169100	0.0.0.255	2	Provide and
S. and	132.100.10.0	330.0.0	2	一 馬田田 小
	172.16.20.0	0.0.0.255	2	Defete
	Private Network	0.0.0.255 that will be DMVPN about.	2	Defete

17. 按一下 完成完成嚮導配置。



18. 按一下Deliver執行命令。

Preview commands that will be delivered to the device's running confi	guration.
crypto keyring ccp-dinvpn-keyring	2
pre-shared-key address 0.0.0.0 0.0.0.0 key *******	
exte exurte issee transform out ESD 2DES, Skit een ake kmee een 2dee	
in you gaed a ansionin-set con-opeo-one esp-sha-ninad esp-odes mode transport	
ext	
crypto isakmp profile ccp-dmvpn-isakmprofile	
keyring ccp-dmvpn-keyring	
match identity address 0.0.0.0	
exit exuste insee weatle Ciece/CB, Destiled	
	2
The differences between the running configuration and the the device is turned off.	startup configuration are lost whenever
Save running config. to device's startup config.	

集線器的CLI配置

相關CLI配置如下所示:

集線器路由器
!
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-
mode transport
crvpto 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
```

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。

VPN			
reate Dynamic Multip	oint VPN (DMVPN) Edit Dynam	ic Multipoint VPN (DMVPN)	
			Add
Interface	IPSec Profile	IP Address	Description
FunnelO	CiscoCP_Profile1	192.168.10.2	<none></none>
Details for interface Tu	unnel0:		
Details for interface Tu Item Name	unnel0:	Item Value	
Details for interface Tu Item Name Iterface	unnel0:	Item Value Tunnel0	
Petails for interface Tu Item Name Interface PSec Profile	unnel0:	Item Value Tunnel0 CiscoCP_Profile1	
Details for interface Tu Item Name Interface PSec Profile P Address	unnel0:	Item Value Tunnel0 CiscoCP_Profile1 192.168.10.2	
Details for interface Tu Item Name Iterface PSec Profile P Address Description	unnel0:	Item Value Tunnel0 CiscoCP_Profile1 192.168.10.2 <none></none>	
Details for interface Tu Item Name Iterface PSec Profile P Address Description Tunnel Bandwidth	unnel0:	Item Value Tunnel0 CiscoCP_Profile1 192.168.10.2 <none> 1000</none>	
Details for interface Tu Item Name Interface PSec Profile P Address Description Tunnel Bandwidth ATU	unnel0:	Item Value Tunnel0 CiscoCP_Profile1 192.168.10.2 <none> 1000 1400 DM/RN NW/</none>	
Details for interface Tu Item Name PSec Profile P Address Description Funnel Bandwidth VTU NHRP Authentication	unnel0:	Item Value Tunnel0 CiscoCP_Profile1 192.168.10.2 «None» 1000 1400 DMVPN_NW 100000	
Details for interface Tu Item Name nterface PSec Profile P Address Description Funnel Bandwidth ATU VHRP Authentication VHRP Network ID VHRP Hold Time	unnel0:	Item Value Tunnel0 CiscoCP_Profile1 192.168.10.2 <none> 1000 1400 DMVPN_NW 100000 360</none>	

通道介面引數(例如MTU和通道金鑰)在*General*索引標籤下修改。

eneral NHRP	Routing
P address:	192.168.10.2
Masic	255.255.255.0 24
Tunnel Source:	
Interface:	GigabitEthernet0/0
C IP address:	
Tunnel Destinatio	on:
Tunnel Destinatio	on: oint GRE Tunnel
Tunnel Destination This is an multip IP / Hostname: IPSec Profile: MTU:	on: oint GRE Tunnel CiscoCP_Proti M Add
Tunnel Destination This is an multip IP / Hostname: IPSec Profile: MTU: Bandwidth:	on: oint GRE Tunnel CiscoCP_Proti Add 1400 1000
Tunnel Destination This is an multip IP / Hostname: PSec Profile: MTU: Bandwidth: Delay:	on: cint GRE Tunnel CiscoCP_Proti Add 1400 1000 1000

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。

neral NHKP	Routing		
uthentication Strin	g: DMVPh	NWV_	
lold Time:	360		
letwork ID:	100000	100000	
-Next Hop Server	's		
Next Hop Serve	ers	Add	
		Delete	
NHRP Map	Mast		
NHRP Map Destination <none></none>	Mask <none></none>	Add	
NHRP Map Destination <none></none>	Mask «None»	Add	

2. 根據網路設定,可以如下所示配置NHRP對映引數

· oraneany connigun	e the IP-to-NMBA address mapping
of IP destinations	s connected to a NBMA network.
Destination re	eachable through NBMA network
ID Enderson	
IP ADDIESS.	
Mask (Optiona	0
NBMA addres	s directly reachable
IP Address.	
Configure NBMA a	addresses used as destinations for br
	ts to be sent over a tunnel network.
or multicast packet	
or multicast packer	dd spokes' IP addresses to hub's mul
or multicast packet	dd spokes' IP addresses to hub's mul
or multicast packer © Dynamically a C IP address of	dd spokes' IP addresses to hub's mul NBMA address directly reachable
or multicast packer	dd spokes' IP addresses to hub's mul NBMA address directly reachable

General NHRP Routin	9
Routing Protocol:	OSPF
Ø OSPF	
OSPF Network Type:	point-to-multipoint
OSPF Priority:	
Hello Interval:	-
Dead Interval:	

<u>更多資訊</u>

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



DMVPN Network Topology

Select the DMVPN network topology.

C 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。

<u>驗證</u>

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

X