



Large Scale DMVPN Deployment: 7200 Server Farm Behind 7600

Cisco Confidential

1. OVERVIEW

This document provides configuration guidance for users of Cisco® Dynamic Multipoint VPN (DMVPN) technology on Cisco 7200 and 7600 series routers. The testing was performed on Cisco 7200 Series Network Processing Engine G1s (NPE-G1s) running Cisco IOS® Software Release 12.3(11)T6 and Cisco 7600 Series routers with the Supervisor Engine 720 (SUP-720-3BXL) and the VPN Services Module (VPNSM), running Cisco IOS Software Release 12.2(18)SXE. The objective of the testing was to configure and test DMVPN on a Cisco 7600/7200 series router combination when configured as a large-scale DMVPN hub.

Advantage: The advantage of using a server farm design is to split the DMVPN function onto different devices. The Cisco 7600 Series router can perform encryption and decryption functions while the Cisco 7200 Series router can handle all tasks related to Next-Hop Resolution Protocol (NHRP) and multipoint generic routing encapsulation (MGRE). While the NPE-G1 is a faster processor than the Multilayer Switch Feature Card (MSFC), encryption/decryption can slow it down considerably. Secondly, the VPN Acceleration Module 2+ (VAM2+), with 250 Mbps maximum throughput, is no match for the VPNSM or shared port adapter (SPA), with Gbps throughput. By taking the burden of encryption/decryption off of the Cisco 7200 Series processor, we allow it to perform better in routing protocol and NHRP handling. To increase the scalability of routing protocols hubs can be configured in daisy chains. The traffic between hubs is configured to traverse a backend LAN for added bandwidth.

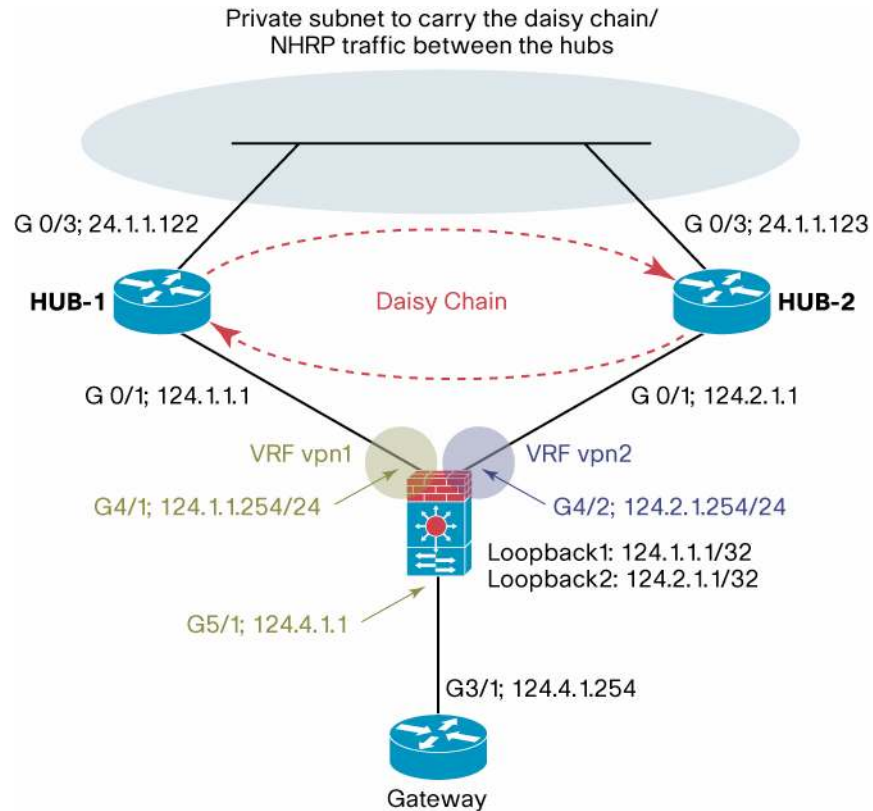
What makes it work: The Cisco 7600 Series router is configured with virtual routing and forwarding (VRF)-aware IPSec. The IP addresses on the hubs are configured as the global loopback interfaces on the Cisco 7600 Series router. These loopbacks are used as crypto endpoints. The 7600 is configured with dynamic crypto to accept any spoke with any proxies. After decryption, the GRE packet comes out in appropriate VRF and is forwarded to the hub in that VRF. Therefore, even with overlapping addresses, we are using VRFs to separate the routing tables. To use different pre-shared keys for different VRFs (hence different hubs), recently introduced “local-address <interface>” command on Cisco IOS Software is used to tie a crypto endpoint to a keyring as well as an ISAKMP profile.

2. AUDIENCE

This configuration guide is targeted for Cisco systems engineers and customer support engineers to provide configuration guidelines and best practices for large-scale DMVPN customer deployments.

3. NETWORK TOPOLOGY

Figure 1. DMVPN Topology



4. SYSTEM COMPONENTS

4.1 7600 Hardware Requirements

- 7600 Enhanced Chassis with enough power to support VPNSM (or SPA) and SUP-720
- SUP-720-3BXL (3B shall work too) with a minimum of 512 MB RAM; 1024 MB preferred
- VPNSM

4.2 7200 Hardware Requirements

- 7200 VXR NPE-G1 (can use 7301)
- Minimum of 512 MB RAM

4.3 7600 Software Requirements

- Feature set: ADVENTERPRISEK9 Release: 12.2(18)SXE

4.4 7200 Software Requirements

- Release: 12.3(11)T6 or later

4.5 Spoke Software Requirements

- Release: 12.3(11)T6 or later

5. CONFIGURATION ON THE 7600

5.1 VRF Configuration

```
ip vrf vpn1
  rd 100:1
!
ip vrf vpn2
  rd 100:2
```

5.2 Loopback Configuration

```
!
! The addresses defined here will reside on the 7200 HUBs (in VRFs)
!
interface Loopback1
  ip address 124.1.1.1 255.255.255.255
!
interface Loopback2
  ip address 124.2.1.1 255.255.255.255
```

5.3 IPsec Configuration

5.3.1 ISAKMP Policy

```
crypto isakmp policy 10
  encr 3des
  authentication pre-share
  group 2
  lifetime 14400
!
```

5.3.2 ISAKMP Keepalive (DPD)

```
crypto isakmp keepalive 60
!
```

5.3.3 IPsec Transform Set

```
crypto ipsec transform-set gre esp-3des esp-sha-hmac
  mode transport
!
```

5.3.4 ISAKMP Keyrings

! Using the local-address command we are tying all the spoke connections coming in
! to Loopback1's address with keyring vpn1 and Loopback2's address with keyring vpn2

```
crypto keyring vpn1
  local-address Loopback1
pre-shared-key address 0.0.0.0 0.0.0.0 key Cisco123
!
crypto keyring vpn1
  local-address Loopback2
pre-shared-key address 0.0.0.0 0.0.0.0 key Cisco456
!
```

5.3.5 ISAKMP Profiles

! Using local-address command, we are tying all the spokes with destination pointing
! to different Loopbacks' addresses together.
!

```
crypto isakmp profile vpn1
  vrf vpn1
  keyring vpn1
  match identity address 0.0.0.0
  local-address Loopback1
crypto isakmp profile vpn2
  vrf vpn2
  keyring vpn2
  match identity address 0.0.0.0
  local-address Loopback2
!
```

5.3.6 Dynamic Crypto Maps

! RRI is turned on to install routes for remote endpoints in VRFs. The addresses can
! be advertised to the HUB by redistributing into any routing protocol running
! between 7600 and HUBs. Another alternative would be to define default routes on
! HUBs pointing back to 7600.
!

```
crypto dynamic-map vpn1-dyna 10
  set transform-set gre
  set isakmp-profile vpn1
  reverse-route remote-peer
!
crypto dynamic-map vpn2-dyna 10
  set transform-set gre
```

```
set isakmp-profile vpn2  
reverse-route remote-peer
```

```
!
```

5.3.7 Crypto Maps

```
!
```

! Each crypto map is tied to different Loopback to define separate VPN termination
! addresses

```
!
```

```
crypto map vpn1 local-address Loopback1  
crypto map vpn1 10 ipsec-isakmp dynamic vpn1-dyna
```

```
!
```

```
crypto map vpn2 local-address Loopback2  
crypto map vpn2 10 ipsec-isakmp dynamic vpn2-dyna
```

```
!
```

5.3.8 Crypto Engine Mode

```
crypto engine mode vrf
```

5.3.9 Crypto Interface Configuration

```
interface GigabitEthernet5/1  
description T0 Internet Gateway  
ip address 124.4.1.1 255.255.255.0  
speed negotiate  
crypto engine slot 1
```

```
!
```

! VLANs with dummy addresses for applying crypto maps

```
!
```

```
interface Vlan101  
ip vrf forwarding vpn1  
ip address 192.70.1.1 255.255.255.0  
crypto map vpn1  
crypto engine slot 1
```

```
!
```

```
interface Vlan102  
ip vrf forwarding vpn2  
ip address 192.70.2.1 255.255.255.0  
crypto map vpn2  
crypto engine slot 1
```

```
!
```

5.4 Uplinks to Hubs

```
interface GigabitEthernet4/1
  description TO G0/1 DMVPN1-G1-1
  ip vrf forwarding vpn1
  ip address 124.1.1.254 255.255.255.0
  speed nonegotiate
!
interface GigabitEthernet4/2
  description TO G0/1 DMVPN1-G1-2
  ip vrf forwarding vpn2
  ip address 124.2.1.254 255.255.255.0
  speed nonegotiate
!
```

5.5 VPNSM Interfaces

! The interfaces appear when we insert VPNSM in the chassis. The VLANs get added
! automatically due to crypto engine slot and crypto connect commands.

```
interface GigabitEthernet1/1
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1,101-102,1002-1005
  switchport mode trunk
  mtu 4500
  no ip address
  flowcontrol receive on
  flowcontrol send off
  spanning-tree portfast trunk
!
interface GigabitEthernet1/2
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1,1002-1005
  switchport mode trunk
  mtu 4500
  no ip address
  flowcontrol receive on
  flowcontrol send off
  spanning-tree portfast trunk
!
```

5.6 Routing Protocol Configuration

```
!  
! OSPF running in different VRFs to advertise IPSec endpoints routes, learnt via RRI  
! to hubs  
!  
router ospf 10 vrf vpn1  
  log-adjacency-changes  
  redistribute static metric 100 subnets  
  network 124.1.1.0 0.0.0.255 area 0  
!  
router ospf 20 vrf vpn2  
  log-adjacency-changes  
  redistribute static metric 100 subnets  
  network 124.2.1.0 0.0.0.255 area 0  
!
```

6. CONFIGURATION ON THE 7200

6.1 DMVPN Tunnel Configuraiton

```
! Multipoint GRE interface. Bandwidth set to a value more than the aggregate  
! bandwidth defined on the spoke GRE interfaces. IP MTU set to 1400 for  
! fragmentation before encryption. Hold-Queues are increased to a value more than  
! the number of neighbors.
```

```
interface Tunnel1  
  bandwidth 10000000  
  ip address 172.20.1.254 255.255.0.0  
  no ip redirects  
  ip mtu 1440  
  no ip next-hop-self eigrp 10  
  ip nhrp authentication nsite  
  ip nhrp map multicast dynamic  
  ip nhrp map 172.20.2.254 124.2.1.1  
  ip nhrp map multicast 124.2.1.1  
  ip nhrp network-id 101  
  ip nhrp holdtime 600  
  ip nhrp nhs 172.20.2.254  
  no ip split-horizon eigrp 10  
  tunnel source GigabitEthernet0/1  
  tunnel mode gre multipoint  
  hold-queue 500 in  
  hold-queue 500 out  
!
```

6.2 Interface Configuration

! Gig5/1 interface connects 7600 to Internet. "crypto connect vlan 2" command ties
! this interface to VLAN 2, which is the source of MGRE tunnel.

```
interface GigabitEthernet0/1
  description to 7600
  ip address 124.1.1.1 255.255.255.0
  duplex full
  speed 1000
  media-type gbic
  no negotiation auto
  hold-queue 500 in
  hold-queue 500 out
!
interface GigabitEthernet0/2
  description Private Network on corporate side
  ip address 192.24.1.1 255.255.255.0
  duplex auto
  speed auto
  media-type rj45
  no negotiation auto
  no keepalive
!
interface GigabitEthernet0/3
  description Private Subnet for NHRP traffic
  ip address 24.1.1.122 255.255.255.0
  duplex auto
  speed auto
  media-type rj45
  no negotiation auto
!
```

6.3 Routing Protocol Configuration

```
!
! EIGRP running over the MGRE tunnel
!
router eigrp 10
  network 172.20.0.0
  network 192.24.1.0
  no auto-summary
!
```



```

! OSPF running to 7600 for learning public IP addresses of the spokes
!
router ospf 254
 log-adjacency-changes
 network 124.1.1.0 0.0.0.255 area 0
!
! Static Route to force NHRP/daisy-chained traffic over G0/3
!
ip route 124.2.1.1 255.255.255.255 24.1.1.123
!

```

7. 7600 CONFIGURATION VERIFICATION

7.1 Modules

Show module

Mod	Ports	Card Type	Model	Serial No.
1	2	IPSec VPN Accelerator	WS-SVC-IPSEC-1	SAD0626000D
4	24	CEF720 24 port 1000mb SFP	WS-X6724-SFP	SAD084700TJ
5	2	Supervisor Engine 720 (Active)	WS-SUP720-3BXL	SAL09137GMT

Mod	MAC addresses	Hw	Fw	Sw	Status
1	0030.f271.d5d9 to 0030.f271.d5dc	1.0	7.2(1)	8.5(0.46)R0C	Ok
4	0011.9299.af44 to 0011.9299.af5b	2.1	12.2(14r)S5	12.2(ROCKIES	Ok
5	0013.7f0b.507c to 0013.7f0b.507f	4.3	8.1(3)	12.2(ROCKIES	Ok

Mod	Sub-Module	Model	Serial	Hw	Status
4	Centralized Forwarding Card	WS-F6700-CFC	SAL08435709	2.0	Ok
5	Policy Feature Card 3	WS-F6K-PFC3BXL	SAL09159788	1.6	Ok
5	MSFC3 Daughterboard	WS-SUP720	SAL09137EC4	2.3	Ok

Mod Online Diag Status

```

-----
1 Pass
4 Pass
5 Pass

```

7.2 VLANs

Show vlan

VLAN	Name	Status	Ports
1	default	active	
3	INSIDE	active	
24	MGMT_VLAN	active	
101	vpn1_crypto_vlan	active	
102	vpn2_crypto_vlan	active	
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

7.3 RRI Installed Routes

show ip route vrf vpn1

```
112.0.0.0/32 is subnetted, 1 subnets
S      112.1.1.1 [1/0] via 0.0.0.0, Vlan101
124.0.0.0/24 is subnetted, 1 subnets
C      124.1.1.0 is directly connected, GigabitEthernet4/1
C      192.70.1.0/24 is directly connected, Vlan101
105.0.0.0/32 is subnetted, 500 subnets
S      105.4.1.100 [1/0] via 0.0.0.0, Vlan101
S      105.3.1.99 [1/0] via 0.0.0.0, Vlan101
```

7.4 ISAKMP SAs

show crypto isakmp sa

124.1.1.1	112.1.1.1	QM_IDLE	211	0
124.1.1.1	105.11.1.28	QM_IDLE	1120	0
124.2.1.1	105.15.1.100	QM_IDLE	1124	0

7.5 IPSec SAs

show crypto eli

Hardware Encryption Layer : **ACTIVE**
Number of crypto engines = **1** .

CryptoEngine-**VPNSM**(1) (slot-1) details.

Capability-IPSec : No-IPPCP, **3DES**, NoAES, RSA

```
IKE-Session   :      5 active, 10921 max, 0 failed
DH-Key        :      0 active,  9999 max, 0 failed
IPSec-Session :     10 active, 21842 max, 0 failed
```

7.6 IPSec SAs

show crypto ipsec sa peer 112.1.1.1

interface: Vlan101

Crypto map tag: vpn1, local addr. 124.1.1.1

protected vrf: vpn1

local ident (addr/mask/prot/port): (124.1.1.1/255.255.255.255/47/0)

remote ident (addr/mask/prot/port): (112.1.1.1/255.255.255.255/47/0)

current_peer: 112.1.1.1:500

PERMIT, flags={}

#pkts encaps: 6591, #pkts encrypt: 6591, #pkts digest: 6591

#pkts decaps: 3908, #pkts decrypt: 3908, #pkts verify: 3908

#pkts compressed: 0, #pkts decompressed: 0

#pkts not compressed: 0, #pkts compr. failed: 0

#pkts not decompressed: 0, #pkts decompress failed: 0

#send errors 0, #recv errors 0

local crypto endpt.: 124.1.1.1, remote crypto endpt.: 112.1.1.1

path mtu 1500, media mtu 1500

current outbound spi: F4989EFF

inbound esp sas:

spi: 0xEC50D6E3(3964720867)

transform: esp-3des esp-sha-hmac ,

in use settings ={Transport, }

slot: 1, conn id: 12395, flow_id: 1469, crypto map: vpn1

crypto engine type: Hardware, engine_id: 2

sa timing: remaining key lifetime (k/sec): (330301/2270)

ike_cookies: 5EB3B2E8 2BC1457F DFA91869 2F20321A

IV size: 8 bytes

replay detection support: Y

inbound ah sas:

inbound pcp sas:

outbound esp sas:

```
spi: 0xF4989EFF(4103642879)
  transform: esp-3des esp-sha-hmac ,
  in use settings ={Transport, }
  slot: 1, conn id: 12396, flow_id: 1470, crypto map: vpn1
  crypto engine type: Hardware, engine_id: 2
  sa timing: remaining key lifetime (k/sec): (330245/2270)
  ike_cookies: 5EB3B2E8 2BC1457F DFA91869 2F20321A
  IV size: 8 bytes
  replay detection support: Y
```

outbound ah sas:

outbound pcg sas:

8. 7200 CONFIGURATION VERIFICATION

8.1 Routes

Show ip route ospf

```
124.0.0.0/8 is variably subnetted, 6 subnets, 2 masks
S      124.2.1.1/32 [1/0] via 24.1.1.123
112.0.0.0/32 is subnetted, 1 subnets
O E2    112.1.1.1 [110/100] via 124.1.1.254, 04:46:03, GigabitEthernet0/1
105.0.0.0/32 is subnetted, 404 subnets
O E2    105.4.1.100 [110/100] via 124.1.1.254, 04:46:03, GigabitEthernet0/1
O E2    105.3.1.99 [110/100] via 124.1.1.254, 04:46:03, GigabitEthernet0/1
```

8.2 NHRP

Show ip NHRP dynamic

```
172.20.112.1/32 via 172.20.112.1, Tunnel1 created 04:23:16, expire 00:06:41
  Type: dynamic, Flags: authoritative unique registered
NBMA address: 112.1.1.1
172.20.1.1/32 via 172.20.1.1, Tunnel1 created 00:01:16, expire 00:13:43
  Type: dynamic, Flags: authoritative unique registered
NBMA address: 105.1.1.1
172.20.1.2/32 via 172.20.1.2, Tunnel1 created 00:01:16, expire 00:13:43
  Type: dynamic, Flags: authoritative unique registered
NBMA address: 105.1.1.2
```

9. LIMITATIONS/CAVEATS/INTEGRATION ISSUES/GUIDELINES

- Hold queues need to be increased to avoid routing protocol and NHRP packet drops in large networks.
- Buffer tuning is generally not required but if buffer failures are seen in a large network, appropriate buffer tuning must be performed, especially on the hubs.
- Reverse Route Injection (RRI) and routing protocol are not required and a default route can be configured on the hub. If the hub already has a default route pointing to some other interface, then the RRI/RP combination will be helpful.

10. RELATED DOCUMENTS

Cisco.com documentation: <http://www.cisco.com/warp/public/732/Tech/security/ipsec/dmvpn/>

11. APPENDIX A

11.1 7600 Configuration

```
version 12.2
service timestamps debug uptime
service timestamps log datetime msec localtime
no service password-encryption
service counters max age 10
!
hostname DMVPN1-7600
!
!
no aaa new-model
clock timezone EST -5
clock summer-time edt recurring
ip subnet-zero
!
!
!
ip vrf vpn1
    rd 100:1
!
ip vrf vpn2
    rd 100:2
!
ipv6 mfib hardware-switching replication-mode ingress
mls ip multicast flow-stat-timer 9
no mls flow ip
no mls flow ipv6
no mls acl tcam share-global
mls cef error action freeze
no scripting tcl init
no scripting tcl encdir
```

```

!
!
!
crypto keyring vpn1
  local-address Loopback1
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco123
crypto keyring vpn2
  local-address Loopback2
  pre-shared-key address 0.0.0.0 0.0.0.0 key cisco456
!
crypto isakmp policy 10
  encr 3des
  authentication pre-share
  group 2
  lifetime 14400
crypto isakmp keepalive 60
crypto isakmp profile vpn1
  vrf vpn1
  keyring vpn1
  match identity address 0.0.0.0
  local-address Loopback1
crypto isakmp profile vpn2
  vrf vpn2
  keyring vpn2
  match identity address 0.0.0.0
  local-address Loopback2
!
crypto ipsec transform-set gre esp-3des esp-sha-hmac
  mode transport
!
crypto dynamic-map vpn1-dyna 10
  set transform-set gre
  set isakmp-profile vpn1
  reverse-route remote-peer
!
crypto dynamic-map vpn2-dyna 10
  set transform-set gre
  set isakmp-profile vpn2
  reverse-route remote-peer
!
!
crypto map vpn1 local-address Loopback1
crypto map vpn1 10 ipsec-isakmp dynamic vpn1-dyna

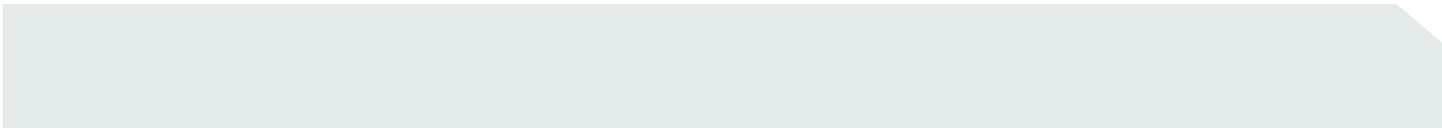
```

```
!  
crypto map vpn2 local-address Loopback2  
crypto map vpn2 10 ipsec-isakmp dynamic vpn2-dyna  
!  
!  
crypto engine mode vrf  
!  
!  
!  
!  
!  
!  
redundancy  
  mode sso  
  main-cpu  
    auto-sync running-config  
spanning-tree mode pvst  
no spanning-tree optimize bpdu transmission  
diagnostic cns publish cisco.cns.device.diag_results  
diagnostic cns subscribe cisco.cns.device.diag_commands  
!  
vlan internal allocation policy ascending  
vlan access-log ratelimit 2000  
!  
!  
interface Loopback1  
  ip address 124.1.1.1 255.255.255.255  
!  
interface Loopback2  
  ip vrf forwarding vpn2-out  
  ip address 124.2.1.1 255.255.255.255  
!  
interface GigabitEthernet1/1  
  switchport  
  switchport trunk encapsulation dot1q  
  switchport trunk allowed vlan 1,101-102,1002-1005  
  switchport mode trunk  
  mtu 4500  
  no ip address  
  flowcontrol receive on  
  flowcontrol send off  
  spanning-tree portfast trunk  
!
```

```
interface GigabitEthernet1/2
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 1,1002-1005
  switchport mode trunk
  mtu 4500
  no ip address
  flowcontrol receive on
  flowcontrol send off
  spanning-tree portfast trunk
!
interface GigabitEthernet4/1
  description TO G0/1 DMVPN1-G1-1
  ip vrf forwarding vpn1
  ip address 124.1.1.254 255.255.255.0
  speed nonegotiate
!
interface GigabitEthernet4/2
  description TO G0/1 DMVPN1-G1-2
  ip vrf forwarding vpn2
  ip address 124.2.1.254 255.255.255.0
  speed nonegotiate
!
!
interface GigabitEthernet5/1
  description TO GW
  ip address 124.4.1.1 255.255.255.0
  load-interval 30
  speed nonegotiate
  crypto engine slot 1
!
interface GigabitEthernet5/2
  description TO DMVPN-AGG-1 GIG 5/1 FOR MGMT
  switchport
  switchport trunk encapsulation dot1q
  switchport trunk allowed vlan 24
  switchport mode trunk
  no ip address
  load-interval 30
!
interface Vlan1
  no ip address
  shutdown
```



```
!  
interface Vlan24  
  ip address 24.1.1.125 255.255.255.0  
!  
interface Vlan101  
  ip vrf forwarding vpn1  
  ip address 192.70.1.1 255.255.255.0  
  crypto map vpn1  
  crypto engine slot 1  
!  
interface Vlan102  
  ip vrf forwarding vpn2  
  ip address 192.70.2.1 255.255.255.0  
  crypto map vpn2  
  crypto engine slot 1  
!  
router ospf 10 vrf vpn1  
  log-adjacency-changes  
  redistribute static metric 100 subnets  
  network 124.1.1.0 0.0.0.255 area 0  
!  
router ospf 20 vrf vpn2  
  log-adjacency-changes  
  redistribute static metric 100 subnets  
  network 124.2.1.0 0.0.0.255 area 0  
!  
ip classless  
ip route 0.0.0.0 0.0.0.0 124.4.1.254  
!  
no ip http server  
!  
logging 24.1.1.192  
!  
line con 0  
  exec-timeout 0 0  
  stopbits 1  
line vty 0 4  
  exec-timeout 0 0  
  password lab  
  login  
!  
!  
monitor event-trace timestamps
```



```
no cns aaa enable
end
```

12. APPENDIX B

12.1 HUB1 Configuration

```
version 12.3
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
!
hostname HUB-1
!
enable password lab
!
clock timezone EST -5
clock summer-time edt recurring
no aaa new-model
ip subnet-zero
!
!
ip cef
no ip domain lookup
!
!
no crypto isakmp enable
!
buffers small permanent 1000
buffers small max-free 1500
buffers small min-free 500
buffers middle permanent 1000
buffers middle max-free 1500
buffers middle min-free 500
buffers big permanent 250
buffers big max-free 500
buffers big min-free 150
!
!
!
interface Tunnel1
    bandwidth 100000000
    ip address 172.20.1.254 255.255.0.0
    no ip redirects
```

```
ip mtu 1440
no ip next-hop-self eigrp 10
ip nhrp authentication nsite
ip nhrp map multicast dynamic
ip nhrp map 172.20.2.254 124.2.1.1
ip nhrp map multicast 124.2.1.1
ip nhrp network-id 101
ip nhrp holdtime 600
ip nhrp nhs 172.20.2.254
no ip split-horizon eigrp 10
load-interval 30
tunnel source GigabitEthernet0/1
tunnel mode gre multipoint
hold-queue 500 in
hold-queue 500 out
!
interface GigabitEthernet0/1
ip address 124.1.1.1 255.255.255.0
duplex full
speed 1000
media-type gbic
no negotiation auto
hold-queue 500 in
hold-queue 500 out
!
interface GigabitEthernet0/2
ip address 192.24.1.1 255.255.255.0
duplex auto
speed auto
media-type rj45
no negotiation auto
no keepalive
!
interface GigabitEthernet0/3
description T0 NHRP Private NET
ip address 24.1.1.122 255.255.255.0
duplex auto
speed auto
media-type rj45
no negotiation auto
!
router eigrp 10
network 172.20.0.0
```

```
network 192.24.1.0
no auto-summary
!
router ospf 254
log-adjacency-changes
network 124.1.1.0 0.0.0.255 area 0
!
ip classless
ip route 124.2.1.1 255.255.255.255 24.1.1.123
!
!
line con 0
exec-timeout 0 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
exec-timeout 0 0
password lab
login
!
!
end
```

13. APPENDIX C

13.1 HUB2 Configuration

```
version 12.3
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
!
hostname HUB-2
!
enable password lab
!
no aaa new-model
ip subnet-zero
!
ip cef
no ip domain lookup
!
no crypto isakmp enable
```

```
!
buffers small permanent 1000
buffers small max-free 1500
buffers small min-free 500
buffers middle permanent 1000
buffers middle max-free 1500
buffers middle min-free 500
buffers big permanent 250
buffers big max-free 500
buffers big min-free 150
!
!
!
interface Tunnel1
 bandwidth 10000000
 ip address 172.20.2.254 255.255.0.0
 no ip redirects
 ip mtu 1440
 no ip next-hop-self eigrp 10
 ip nhrp authentication nsite
 ip nhrp map multicast dynamic
 ip nhrp map multicast 124.1.1.1
 ip nhrp map 172.20.1.254 124.1.1.1
 ip nhrp network-id 101
 ip nhrp holdtime 1800
 ip nhrp nhs 172.20.1.254
 no ip split-horizon eigrp 10
 load-interval 30
 tunnel source GigabitEthernet0/1
 tunnel mode gre multipoint
 hold-queue 500 in
 hold-queue 500 out
!
interface GigabitEthernet0/1
 ip address 124.2.1.1 255.255.255.0
 load-interval 30
 duplex full
 speed 1000
 media-type gbic
 no negotiation auto
 hold-queue 500 in
 hold-queue 500 out
!
```

```
interface GigabitEthernet0/2
  description Inside traffic vlan
  ip address 192.24.2.1 255.255.255.0
  load-interval 30
  duplex full
  speed 1000
  media-type gbic
  no negotiation auto
  no keepalive
!
interface GigabitEthernet0/3
  description FOR NHRP Traffic Private NET
  ip address 24.1.1.123 255.255.255.0
  duplex auto
  speed auto
  media-type rj45
  no negotiation auto
!
router eigrp 10
  passive-interface GigabitEthernet0/2
  network 172.20.0.0
  network 192.24.2.0
  no auto-summary
!
router ospf 254
  log-adjacency-changes
  network 124.2.1.0 0.0.0.255 area 0
!
ip classless
ip route 124.1.1.1 255.255.255.255 24.1.1.122
!
no ip http server
no ip http secure-server
!
line con 0
  exec-timeout 0 0
  stopbits 1
line aux 0
  stopbits 1
line vty 0 4
  exec-timeout 0 0
  password lab
  login
```

!
end

14. APPENDIX D

14.1 Spoke Configuration

```
version 12.3
service timestamps debug datetime msec localtime
service timestamps log datetime msec localtime
no service password-encryption
!
hostname SPOKE
!
!
no aaa new-model
ip subnet-zero
ip cef
!
no ip domain lookup
!
crypto isakmp policy 10
  encr 3des
  authentication pre-share
  group 2
  lifetime 14400
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
crypto isakmp keepalive 60
!
crypto ipsec transform-set gre_set esp-3des esp-sha-hmac
  mode transport
!
crypto ipsec profile gre_prof
  set transform-set gre_set
!
interface Tunnel1
  bandwidth 128
  ip address 172.20.112.1 255.255.0.0
  no ip redirects
  ip mtu 1440
  ip nhrp authentication nsite
  ip nhrp map multicast 124.1.1.1
  ip nhrp map 172.20.1.254 124.1.1.1
  ip nhrp network-id 101
```

```
ip nhrp holdtime 600
ip nhrp nhs 172.20.1.254
load-interval 30
tunnel source FastEthernet0/0
tunnel mode gre multipoint
tunnel protection ipsec profile gre_prof
!
interface FastEthernet0/0
ip address 112.1.1.1 255.255.255.0
load-interval 30
speed 100
full-duplex
!
interface FastEthernet0/1
description dmvpn interface
no ip address
load-interval 30
duplex auto
speed auto
!
interface FastEthernet0/1.11
description traffic interface
encapsulation dot1Q 11
ip address 12.1.1.1 255.255.255.0
!
interface FastEthernet0/1.24
description mgmt net
encapsulation dot1Q 24
ip address 24.1.1.161 255.255.255.0
!
router eigrp 10
passive-interface FastEthernet0/1.11
network 12.1.1.0 0.0.0.255
network 172.20.0.0
no auto-summary
!
router ospf 254
log-adjacency-changes
network 112.1.1.0 0.0.0.255 area 0
!
ip classless
!
line con 0
```



```
exec-timeout 0 0
stopbits 1
line aux 0
stopbits 1
line vty 0 4
exec-timeout 0 0
password lab
login
end
```

**Corporate Headquarters**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

European Headquarters

Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters

Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries and regions. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus
Czech Republic • Denmark • Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel
Italy • Japan • Korea • Luxembourg • Malaysia • Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal Puerto
Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore • Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan
Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam • Zimbabwe

Copyright © 2006 Cisco Systems, Inc. All rights reserved. CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0601R)

