Migration Guide

Migrating from Dynamic Multipoint VPN Phase 2 to Phase 3: Why and How to Migrate to the Next Phase

This guide shows how a Dynamic Multipoint VPN (DMVPN) deployment can be migrated to make use of the shortcut switching enhancements for increased network performance and scalability.

Up to Cisco IOS® Software Release 12.4(4)T, Cisco® DMVPN deployments could be Phase 1 (hub-and-spoke only) or Phase 2, which included direct spoke-to-spoke tunnels and "daisy-chaining" of hubs for scaling the network. In Cisco IOS Software Release 12.4(6)T, DMVPN Phase 3 was introduced. It reduces latency during call setup for direct spoke-to-spoke calls, improves resilience to hub failures and allows for hierarchical hub design. These benefits are detailed below.

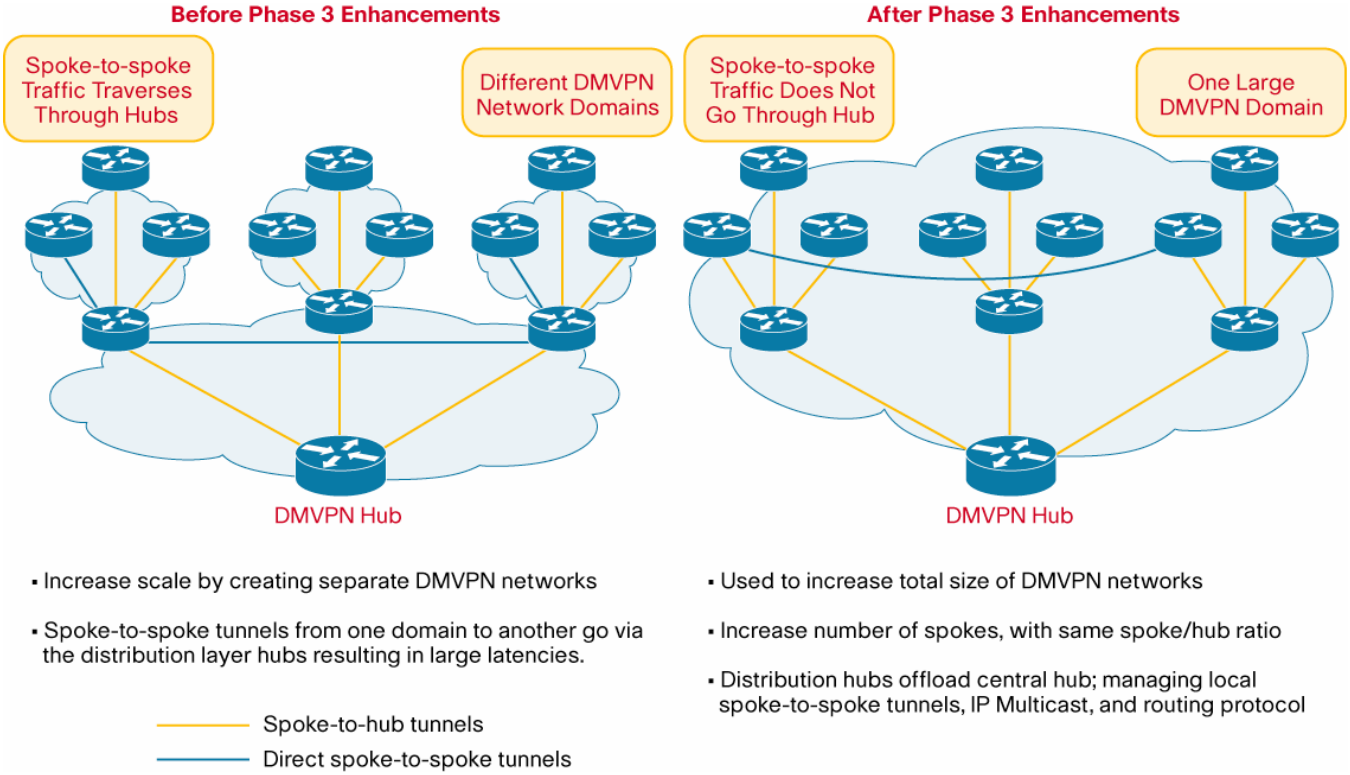
BENEFITS OF NHRP SHORTCUT SWITCHING ENHANCEMENTS

Next Hop Resolution Protocol (NHRP) shortcut switching works in the Cisco Express Forwarding output switching path. In summary, for each data packet that is forwarded out the multipoint Generic Routing Encapsulation (mGRE) interface, NHRP performs a lookup in its mapping table to find an entry for the destination IP address of the data packet. If there is one, it overrides the adjacency determined by Cisco Express Forwarding during the Forwarding Information Base/Adjacency (FIB/ADJ) lookup. This lookup process is how data packets are redirected over the spoke-to-spoke direct tunnel, rather than being forwarded to the hub as the routing table states. Please visit the Shortcut Switching Enhancements for NHRP in DMVPN Networks Website for more information about this feature.

The Shortcut Switching Enhancements for NHRP in DMVPN (DMVPN Phase 3) feature provides a more scalable alternative to the previous NHRP model. This model provides the following advantages over previous DMVPN implementations (DMVPN Phase 2).

Figure 1 shows how the network evolves from Phase 2 to Phase 3. As shown in the figure, we are scaling the DMVPN network by dividing it into regions and creating a separate DMVPN network for each region. The regional hubs are then set up as spokes of a central hub network. In many networks, this layout will follow the general data flow patterns. In a DMVPN Phase 2 network, each DMVPN network is independent and causes traffic between spokes in different regions to have to traverse through the regional hubs (didn't have to go through the central hubs). In a DMVPN Phase 3 network, all the regional DMVPN networks are "glued" together into a single hierarchical DMVPN network (including the central hubs) and spokes in different regions can build direct spoke-to-spoke tunnels with each other, bypassing both the regional and central hubs. When building spoke-to-spoke tunnels within a region, only the regional hubs are involved in the tunnel setup. When building spoke-to-spoke tunnels between regions, the regional and central hubs are involved in the tunnel setup.

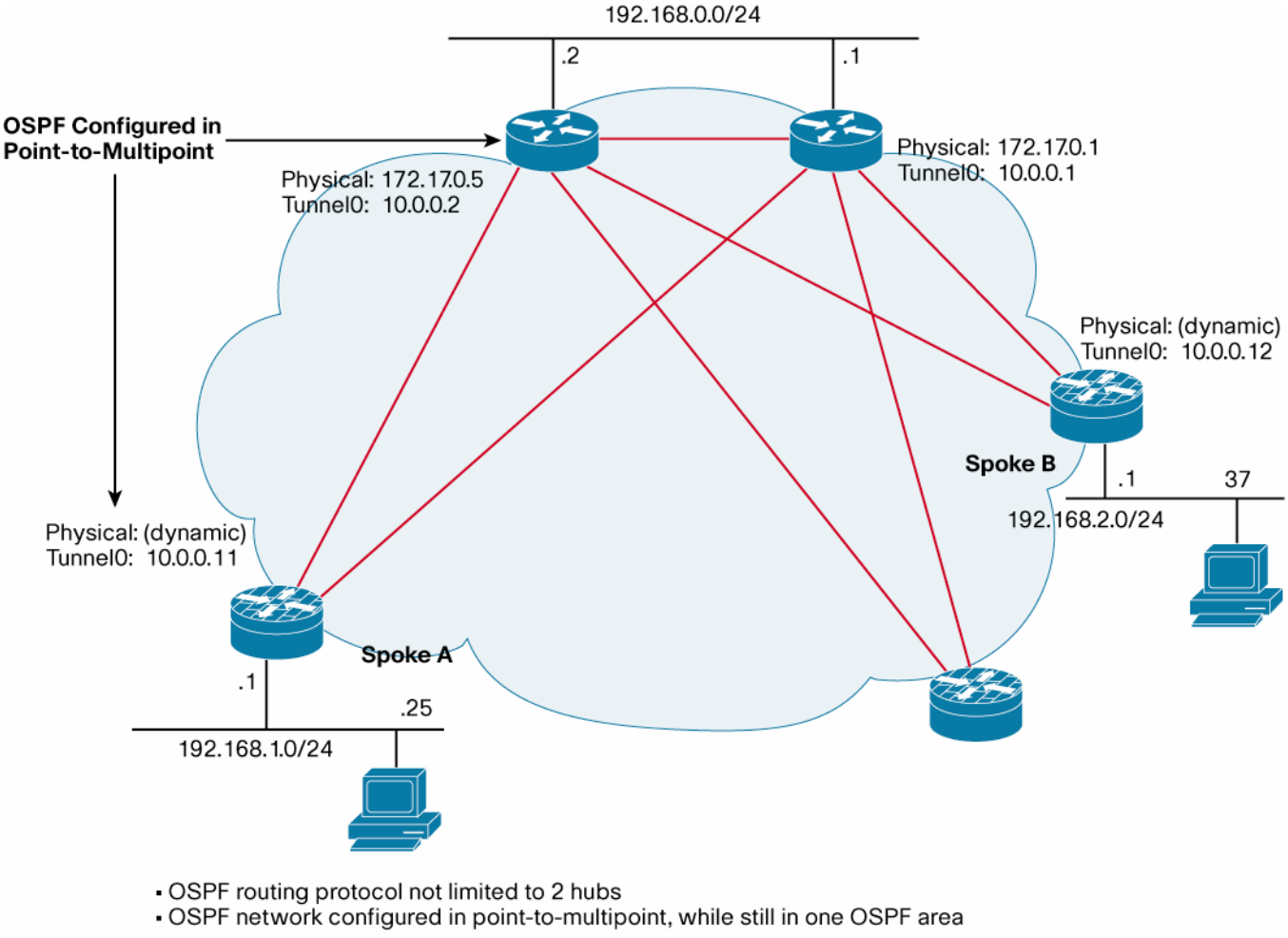
Figure 1. Before and After DMVPN Phase 3 Examples



In more detail, these are the benefits that DMVPN Phase 3 brings:

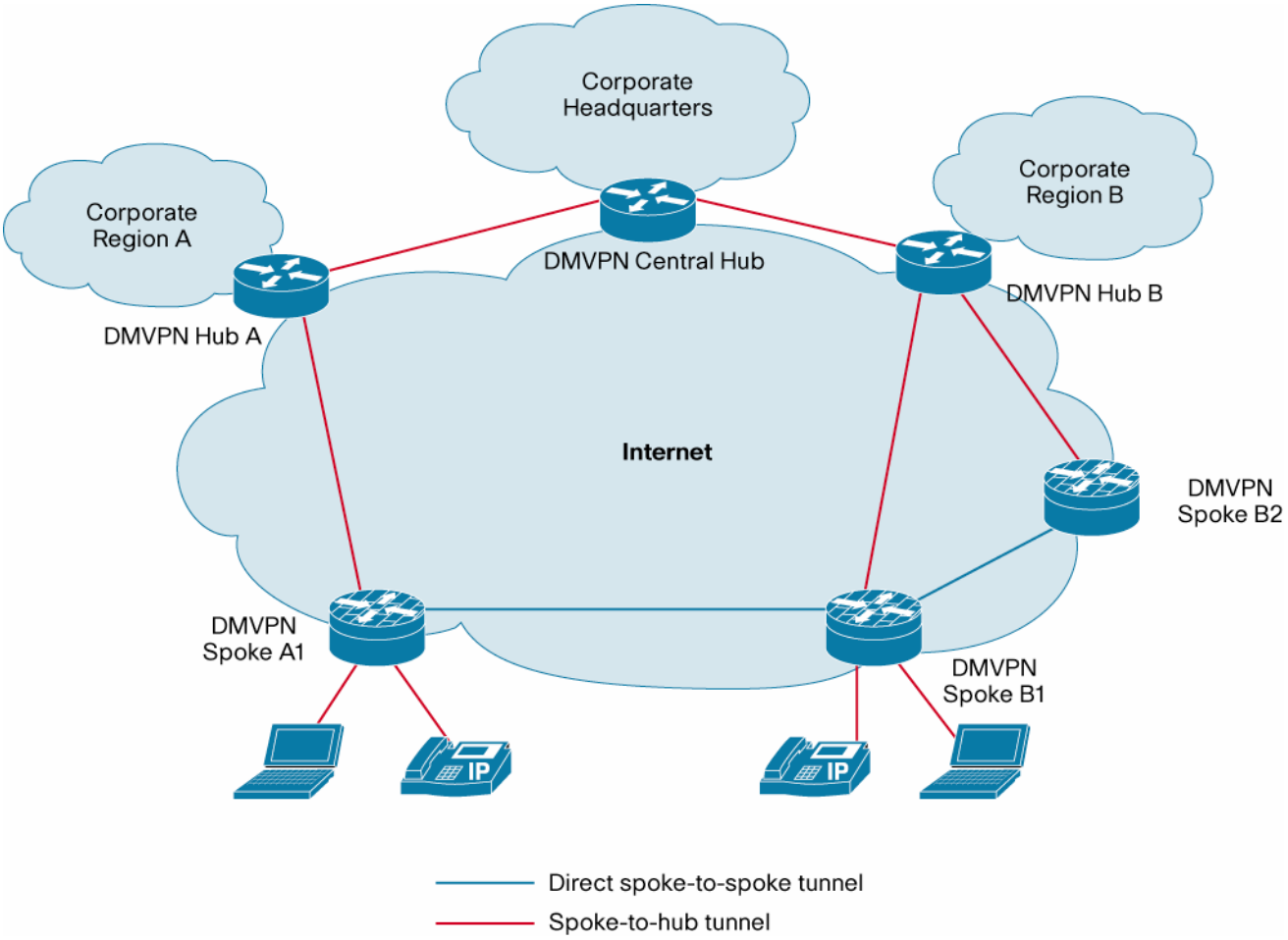
- Allows summarization of routing protocol updates from hub to spokes. The spokes no longer need to have an individual route with an IP next-hop of the tunnel IP address of the remote spoke for the networks behind all the other spokes. The spokes can use summarized routes or specific routes with an IP next-hop of the tunnel IP address of the hub and still be able to build spoke-to-spoke tunnels. This can reduce the load on the routing protocol running on the hub router. You can reduce the load; when you can summarize the networks behind the spokes to a few summary routes or even one summary route, the hub routing protocol only has to advertise the few or one summary route to each spoke rather than all of the individual spoke routes. For example, with 1000 spokes and one route per spoke, the hub receives 1000 routes but only has to advertise one summary route back to each spoke (equivalent to 1000 advertisements, one per spoke) instead of the 1,000,000 advertisements it had to send in the prior implementation of DMVPN (Phase 2).
- Provides better alternatives to complex daisy chaining of hubs for expanding DMVPN spoke-to-spoke networks. The hubs must still be interconnected, but they are not restricted to just a daisy-chain pattern. The hubs may now be interconnected in a dual direction chain, partial or full mesh, or in a hierarchical design. Since the routing table is now used to forward data packets and NHRP control packets between hubs, there is efficient forwarding of packets to the correct hub rather than having request and reply packets traversing around the daisy chain to go through all of the hub routers.
- Allows for expansion of DMVPN spoke-to-spoke networks beyond two hubs with Open Shortest Path First (OSPF) as the routing protocol. Because the spokes use routes with the IP next-hop set to the hub router (not the remote spoke router as before), you can configure OSPF to use point-to-multipoint network mode rather than broadcast network mode. Configuring OSPF to use point-to-multipoint network mode removes the Designated Router (DR) and Backup Designated Router (BDR) requirements that restricted the DMVPN network to just two hubs (Figure 2). When using OSPF, each spoke still has all the individual spoke routes, because the DMVPN network must be in a single OSPF area and you cannot summarize routes within an OSPF area.

Figure 2. OSPF Configured in Point-to-Multipoint Mode



- Allows the ability to build dynamic spoke-to-spoke tunnels when the network is set up for non-split-tunneling or the routing protocol On-Demand Routing (ODR is used. A virtual routing and forwarding “lite” (VRF-lite) configuration is needed in this case.
- Allows for hierarchical (greater than one level) and more complex tree-based DMVPN network topologies (Figure 3). Tree-based topologies allow the capability to build DMVPN networks with regional hubs that are spokes of central hubs. This architecture allows the regional hub to handle the data and NHRP control traffic for its regional spokes, but still allows spoke-to-spoke tunnels to be built between any spokes within the DMVPN network, whether they are in the same region or not. This architecture also allows the DMVPN network layout to more closely match regional or hierarchical data flow patterns.

Figure 3. Hierarchical DMVPN Deployment Example



- Allows data packets to be Cisco Express Forwarding switched along the routed path until a spoke-to-spoke tunnel is established.

One deployment scenario where these DMVPN enhancements have been implemented is in the Cisco Enterprise Class Teleworker (ECT) solution. ECT is a highly scalable Cisco IOS Software-based solution that securely integrates the network infrastructure, management infrastructure, managed services, and applications across the entire enterprise, including LAN, WAN, branch, and teleworker locations. The solution is an integral part of the Cisco Service-Oriented Network Architecture (SONA), a framework that enables enterprise customers to build integrated systems across a fully converged, intelligent network. Using the Cisco SONA framework, the enterprise network can evolve into an Intelligent Information Network: one that offers the kind of end-to-end functions and centralized, unified control that promote true business transparency and agility.

Cisco has successfully deployed the Enterprise Class Teleworker solution within its own organization, increasing productivity and improving efficiency while enabling “zero-touch” deployment, manageability, and low-to-negative total cost of ownership. Enterprises and service providers can use the Cisco ECT solution to offer the benefits of network services to their end users and customers, while maintaining an effective return on investment (ROI).

For the Cisco ECT/SONA Solution Overview, refer to:
http://www.cisco.com/en/US/prod/collateral/iosswrel/ps6537/ps6586/ps6660/prod_brochure0900aecd803fc7ec.html

For the Cisco ECT/SONA solution, services, and applications support, refer to:

http://cisco.com/go/ect/

WHEN AND WHY SHOULD A NETWORK BE MIGRATED TO THE NEXT PHASE OF DMVPN?

DMVPN Phase 3 has improvements over a DMVPN Phase 2 (spoke-to-spoke network). It is expected that all DMVPN Phase 2 networks will be eventually migrated to DMVPN Phase 3. The only disadvantage of DMVPN Phase 3 is that it is not yet available when running DMVPN natively on Cisco 6500 or 7600 routers. For a DMVPN spoke-to-spoke network, the main improvements from Phase 2 are in the increased flexibility in laying out the base DMVPN network (hierarchical and no daisy chain) and the removal of some of the restrictions on the routing protocols required by Phase 2 (OSPF broadcast mode, non-split-tunneling). DMVPN Phase 3 is not expected to change the number of spokes that a single DMVPN hub can support, though it may reduce the CPU load of the routing protocol on the hub.

In Table 1, the term “regional hubs” refers to a DMVPN design where hubs are located in different locations, or regions. With DMVPN Phase 3 they can be interconnected using a central hub into a single, overall DMVPN.

The term “high concentration hub” is used when DMVPN is deployed using a Cisco 6500 or 7600 router that is playing the role of a server load balancer (SLB) and the encryption is performed in a VPN Services Module (VPNSM) module or a VPN shared port adapter (VPN-SPA) in the same chassis. The design includes a server farm of Cisco 7206 or 7301 routers to perform the mGRE, NHRP, and routing protocol tasks. For more information, refer to:
http://www.cisco.com/en/US/products/ps6635/products_white_paper0900aecd803498b1.shtml

Table 1. Migration Gains

Deployment Scenario	Migration Gain	Reasons for Migration
Spoke-to-spoke: **Daisy-chained hubs**	High	With previous DMVPN implementations, we had to daisy-chain the hubs in a ring to be able to pass NHRP resolution requests and replies across the hubs. The daisy chain was also used to forward spoke-to-spoke data packets through the hubs while the spoke-to-spoke tunnel was being built. The chain can only be unidirectional. With a single-level chain, if one hub fails the chain is broken and a resolution request would not be able to be passed on; thus, most of the spokes would not be able to communicate at all, not even through the hubs. In this scenario, a hub failure would be critical. More levels of daisy chain can protect against a single hub failure, but this increases the complexity of the hub configuration. With the NHRP shortcut switching enhancements, the hubs can easily be set up in a partial or full mesh. In this case, the routing table is used by the hubs to select the best path to reach the other hub in the mesh that supports the remote spoke. Also, if one hub fails, it doesn’t block the path to another hub within the hub mesh. OSPF can now be used for more than one pair of hubs and still allow spoke-to-spoke tunnels. With previous DMVPN implementations, all the spoke routers are required to have full routing tables to build spoke-to-spoke tunnels. This means you could need more powerful spoke routers to handle that many routes in a very large DMVPN. With NHRP shortcut switching enhancements, you can advertise summary routes to the spokes and still build spoke-to-spoke tunnels. Data packets are now Cisco Express Forwarding switched at the hubs through the spoke-to-hub-…-hub-to-spoke path while the direct spoke-to-spoke tunnels are being set up. This helps reduce the CPU load and latency of forwarding data packets through the hub routers.

Deployment Scenario	Migration Gain	Reasons for Migration
Spoke-to-spoke: **Regional hubs**	High	Before Phase 3 we could not deploy DMVPN in a regionalized or hierarchical model. The hubs could be daisy-chained, but all would reside at the same logical level. NHRP resolution requests and replies could be passed on from hub to hub from one region to the other, but that would be slow and be sensitive to hub-to-hub failure, as described above. With the NHRP shortcut switching enhancements, we can have a central hub that interconnects regional hubs and can forward data packets and NHRP requests between the regional hubs, reducing the number of hops that an NHRP request has to go through for large-scale deployments, in a multilevel hierarchy (Figure 3). In addition, there is no theoretical limit to the number of layers, but a practical limit is about 3 to 4 layers in the hierarchy. This also allows direct spoke-to-spoke tunnels between spokes in different regions, since all nodes are within the same DMVPN. Also, OSPF can now be used for larger DMVPN deployments because it is no longer limited to one pair of hubs. OSPF is still limited to a single area on the DMVPN; therefore, it cannot summarize routes on the spoke routers.
Spoke-to-spoke: **High-concentration hub**	High	With the NHRP shortcut switching enhancements, we can now have spoke-to-spoke tunnels for the high concentration deployments, where the previous DMVPN implementation did not allow spoke-to-spoke in this scenario. Also, OSPF can now be used for more than one pair of hubs and still allow spoke-to-spoke.

HOW TO MIGRATE TO DMVPN NEXT PHASE

To migrate to the next DMVPN phase, you must first make sure that your Cisco routers are able to run the Cisco IOS Software releases that support NHRP shortcut switching. Use Cisco Feature Navigator to find information about platform support and Cisco IOS Software image support. Access the Cisco Feature Navigator at http://www.cisco.com/go/fn. NHRP shortcut switching is with Cisco IOS Software Release 12.4(6)T and higher.

Note: It is best to run at least Cisco IOS Software Release 12.4(6)T4 or 12.4(9)T1.

Ideally, we would be able to migrate all of the hubs and spokes to DMVPN Phase 3 at the same time. This is an easier scenario, but it might not be possible for some field deployments.

The best way to do the migration, as well as manage the DMVPN Phase 3 deployment, is to use the Cisco Security Manager. With this easy-to-use tool, we have a way to centrally provision and change all aspects of Cisco IOS router configurations at the touch of a button. This allows us to upgrade all the DMVPN hubs and spokes to NHRP shortcut switching. We can also use any other mechanism to connect to all devices and change the configuration, only it will take longer and require more manual work.

Let us analyze the most common migration scenarios:

- **One-time simultaneous migration.** All hubs and spokes are migrated at the same time. In this case, we would follow these steps:

1. Upgrade the Cisco IOS Software for all hubs and spokes.
2. Add the new NHRP commands to hubs, set the routing protocol on the hubs to not preserve the IP next-hop, and add in any route summarization. The Phase 2 DMVPN spokes will no longer be able to build spoke-to-spoke tunnels, but spoke to hub and spoke to spoke traffic via the hub is still supported.
3. Add the new NHRP commands to the spokes. The spokes (now at Phase 3) will again be able to build spoke-to-spoke tunnels.

After the above steps are done, the migration is over.

- **Gradual migration: Coexistence of both implementations.** In this case, we can create a parallel DMVPN domain for the spokes that are migrated and keep the older ones in the older domain.

1. On the hubs, create a second DMVPN domain; new tunnel interface with a different IP subnet (**ip address <address> <mask>**), different NHRP network-id (**ip nhrp network-id <id>**), and different tunnel key (**tunnel key <number>**), if using tunnel keys. An external WAN interface can be shared by both the old and new DMVPN; as long as the same IPsec profile and the **shared** keyword is used in the **tunnel protection ipsec profile <profile-name> shared** command and the DMVPN networks are configured with tunnel keys. If tunnel keys are not configured, you must use a different external address (**tunnel source <interface-name/ip address>**) for the new DMVPN domain.
2. Start moving spokes to the new DMVPN as soon as possible, as spokes connected to separate DMVPNs will not be able to build spoke-to-spoke tunnels with each other. Please note that direct spoke-to-spoke tunnels are not possible between spokes during the migration process when one spoke is in the new DMVPN and the other is part of the original one. In this case, the traffic will flow through the hub. There should be no loss of connectivity.
3. After all spokes have been migrated to the new DMVPN, the old one can be deleted and the "shared" keyword can be removed from the hub tunnel protection command.

Following is the list of configuration changes that need to be done for both hubs and spokes, and for the two main routing protocols: Enhanced Interior Gateway Routing Protocol (EIGRP) and Open Shortest Path First (OSPF), which will have to be applied in any of the migration approaches.

After the Cisco IOS Software is upgraded to a release equal to or greater than 12.4(6)T, nothing happens until we add a few commands. This means that all hubs and spokes will continue to run the same as the original DMVPN Phase 2.

Note: Some older Cisco router series might not have enough memory to run the new Cisco IOS Software releases and the hardware will have to be upgraded first, before the new Cisco IOS Software can be run.

To enable NHRP shortcut switching:

- All spokes need to have the commands **ip nhrp shortcut** and the **ip nhrp redirect** added to their tunnel interfaces. For the hubs use only **ip nhrp redirect**.
- For EIGRP, in the hub side only:
  - Remove: **no ip next-hop-self eigrp <as>** from the hub tunnel configuration
  - Leave: **no ip split-horizon eigrp <as>** in the hub tunnel configuration
  - Add as needed: **ip summary-address eigrp <as> <summary-of-spokes-subnets> 5**
- For OSPF, for all hubs and spokes:
  - Change from **ip ospf network broadcast to ip ospf network point-multipoint.**

1. On all hubs and spokes, change OSPF to point-to-multipoint.

```
interface tunnel <y>
 ...
 ip ospf network point-multipoint
```

2. On all hubs and spokes, remove the OSPF priority; it is no longer needed.

```
interface tunnel <y>
 ...
 no ip ospf priority
```


3. If you need to block the OSPF /32 routes, you can add the following on all hub and spoke routers:

```
router ospf <#>
 ...
 distribute-list prefix-list Block-32 out    (block OSPF/32 connected routes)

ip prefix-list Block-32 deny <tunnel-subnet> <mask> ge 32
ip prefix-list Block-32 permit any le 32
```

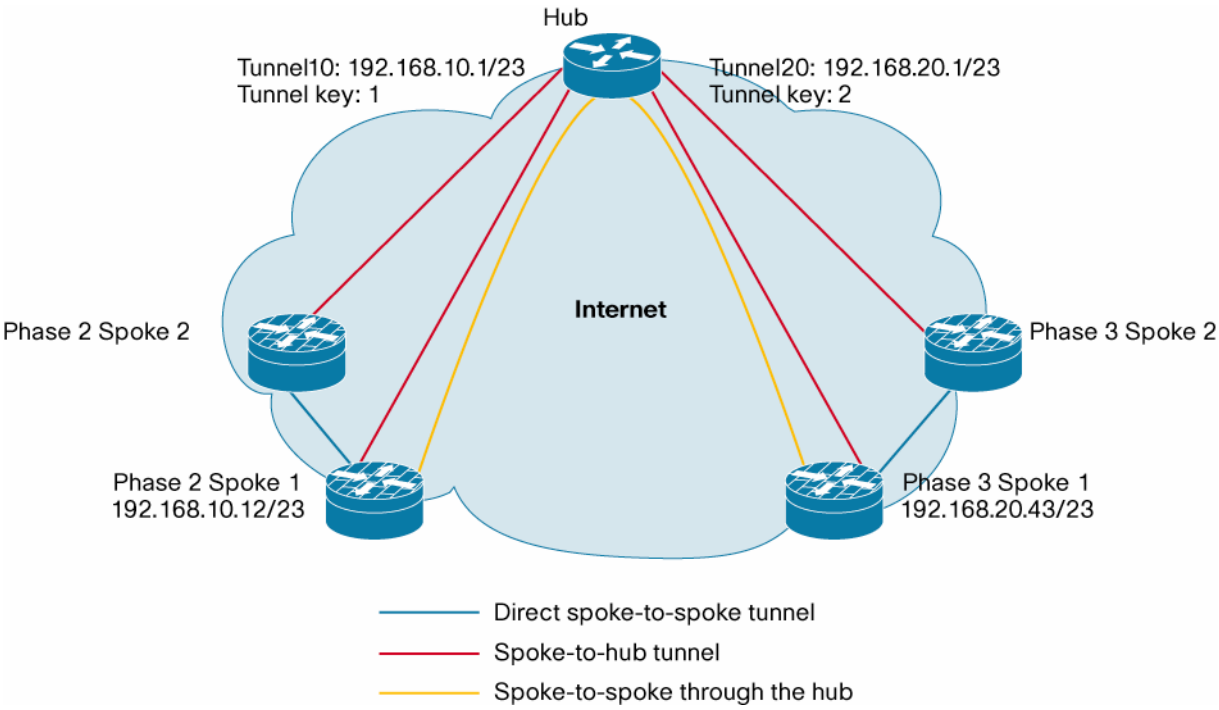
- Use Cisco IOS Software Release 12.4(9)T or later instead of 12.4(6)T. This is because we need to have a fix to NHRP so that it won't be confused by the Cisco IOS OSPF behavior of installing /32 routes for the directly connected routers on the GRE tunnel interface. Otherwise use the technique above to have OSPF block adding these /32 routes to the routing table if you need to run IOS code between 12.4(6)T and 12.4(9)T.

CONFIGURATION SAMPLES

The next sample configuration is for EIGRP with a dual DMVPN implementation in the same hub (Phase 2) and with NHRP shortcut switching (Phase 3). Only the DMVPN part of the configuration is shown. PKI is assumed, although it is not shown in the sample.

Next we show the DMVPN hub configuration while a migration is happening, where two separate DMVPN domains are configured: one to keep the spokes in the existing "old" phase of DMVPN implementation, and one for the migrated spokes, as well as new spokes. "Tunnel 10" is the one used before the migration (where the DMVPN spokes connect to) and "Tunnel 20" is used for spokes after being migrated to DMVPN Phase 3 (Figure 4).

Figure 4. A DMVPN Hub During Migration



DMVPN Hub Router Configuration While Being Migrated: Both DMVPN Phase 2 and Phase 3 Are Configured

```
crypto isakmp policy 1
 encr 3des
crypto isakmp keepalive 30 5
crypto isakmp nat keepalive 30
!
crypto ipsec transform-set ESP-transport esp-3des esp-sha-hmac
 mode transport require
!
crypto ipsec profile DMVPN
 set transform-set ESP-transport
!
interface Tunnel10
 Description original DMVPN domain
 bandwidth 2000
 ip address 192.168.10.1 255.255.254.0
 no ip redirects
 ip mtu 1400
 no ip next-hop-self eigrp 1
 ip nhrp map multicast dynamic
 ip nhrp map multicast 172.16.10.3
 ip nhrp map 192.168.10.3 172.16.10.3
 ip nhrp network-id 1111
 ip nhrp holdtime 360
 ip nhrp nhs 192.168.10.3
 no ip split-horizon eigrp 1
 ip pim sparse-dense-mode
 ip multicast rate-limit out 768
 ip tcp adjust-mss 1360
 load-interval 30
 delay 2000
 qos pre-classify
 tunnel source <wan-side-interface>
 tunnel mode gre multipoint
 tunnel key 111
 tunnel protection ipsec profile DMVPN shared
!
interface Tunnel20
 Description NHRP shortcut switching domain
 bandwidth 2000
 ip address 192.168.20.1 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip nhrp map multicast dynamic
 ip nhrp map multicast 172.16.20.2
```



```
 ip nhrp map 192.168.20.2 172.16.20.2
 ip nhrp network-id 2222
 ip nhrp holdtime 360
 ip nhrp nhs 192.168.20.2
 ip nhrp shortcut
 ip nhrp redirect
 no ip split-horizon eigrp 1
 ip summary-address eigrp 1 10.10.0.0 255.255.128.0 5
 ip summary-address eigrp 1 10.20.0.0 255.255.128.0 5
 ip pim sparse-dense-mode
 ip multicast rate-limit out 768
 ip tcp adjust-mss 1360
 load-interval 30
 delay 2000
 qos pre-classify
 tunnel source <wan-side-interface>
 tunnel mode gre multipoint
 tunnel key 222
 tunnel protection ipsec profile DMVPN shared
!
router eigrp 1
 network 10.10.0.0 0.0.127.255
 network 10.20.0.0 0.0.127.255
 network 192.168.10.0 0.0.1.255
 network 192.168.20.0 0.0.1.255
 no auto-summary
```

DMVPN Phase 2: Not Migrated

```
crypto isakmp policy 1
 encr 3des
crypto isakmp keepalive 30 5
crypto isakmp nat keepalive 30
!
crypto ipsec transform-set ESP-transport esp-3des esp-sha-hmac
 mode transport
!
crypto ipsec profile DMVPN
 set transform-set ESP-transport
!
interface Tunnel0
 Description DMVPN phase2 domain
 bandwidth 2000
 ip address 192.168.10.12 255.255.254.0
 no ip redirects
 ip mtu 1400
 ip nhrp map multicast 172.16.10.1
```



```
 ip nhrp map multicast 172.16.10.2
 ip nhrp map 192.168.10.1 172.16.10.1
 ip nhrp map 192.168.10.2 172.16.10.2
 ip nhrp network-id 1111
 ip nhrp holdtime 360
 ip nhrp nhs 192.168.10.1
 ip nhrp nhs 192.168.10.2
 ip nhrp registration no-unique
 ip pim sparse-dense-mode
 ip multicast rate-limit out 768
 ip tcp adjust-mss 1360
 load-interval 30
 delay 2000
 qos pre-classify
 tunnel source <wan-side-interface>
 tunnel mode gre multipoint
 tunnel key 111
 tunnel protection ipsec profile DMVPN
!
router eigrp 1
 network 192.168.10.0 0.0.1.255
 network 10.10.0.16 0.0.0.15
 distribute-list dmvpn_acl out
 no auto-summary
!
ip access-list standard dmvpn_acl
 permit 10.10.0.16 0.0.0.15
```

DMVPN Phase 3 Spoke: After Migration

```
crypto isakmp policy 1
 encr 3des
crypto isakmp keepalive 30 5
crypto isakmp nat keepalive 30
!
crypto ipsec transform-set ESP-transport esp-3des esp-sha-hmac
 mode transport
!
crypto ipsec profile DMVPN
 set transform-set ESP-transport
!
interface Tunnel0
 Description DMVPN phase3
 bandwidth 2000
 ip address 192.168.20.43 255.255.254.0
 no ip redirects
 ip mtu 1400
```



```
 ip nhrp map multicast 172.16.20.1
 ip nhrp map multicast 172.16.20.2
 ip nhrp map 192.168.20.1 172.16.20.1
 ip nhrp map 192.168.20.2 172.16.20.2
 ip nhrp network-id 2222
 ip nhrp holdtime 360
 ip nhrp nhs 192.168.20.1
 ip nhrp nhs 192.168.20.2
 ip nhrp registration no-unique
 ip nhrp shortcut
 ip nhrp redirect
 ip pim sparse-dense-mode
 ip multicast rate-limit out 768
 ip tcp adjust-mss 1360
 load-interval 30
 delay 2000
 qos pre-classify
 tunnel source <wan-side-interface>
 tunnel mode gre multipoint
 tunnel key 222
 tunnel protection ipsec profile DMVPN
!
router eigrp 1
 network 192.168.20.0 0.0.1.255
 network 10.20.0.16 0.0.0.15
 no auto-summary
!
```

Next, we show the output of some **show** commands for hub and spokes. The DMVPN Phase 3-enabled Cisco IOS routers are running Cisco IOS Software Release 12.4(9)T1. All commands refer to the configuration examples shown above. EIGRP is used as the DMVPN routing protocol.

Also, split-tunneling is configured in the network. This means that only the respective corporate networks are routed through the DMVPN tunnels. All other traffic is sent directly to the Internet.

This next output is from a **show ip route** EIGRP excerpt of the above examples, where two DMVPN domains are configured in the same hub: one for Phase 2 and one for Phase 3.

```
dmvpn-hub1#show ip route
…
 D 10.10.0.32/28 [90/1666560] via 192.168.10.12, 04:10:48, Tun      ←Phase2 spoke
 nel10
 …
 D 10.10.0.0/17 is a summary, 2d10h, Null0
 D 10.20.0.0/17 is a summary, 2d10h, Null0                          ←Phase3 summaries
 D 10.20.0.16/28 [90/1894400] via 192.168.20.43, 5d11h, Tunnel      ←Phase3 spoke
 20
 … [more lines would follow here for all the remaining spokes]
```

This next output is for the DMVPN hub side **show dmvpn** command that shows the two DMVPN domains: one in Phase 2 and one in Phase 3. Tunnel10 is being used for spokes connecting to the Phase 2 domain, and Tunnel20 is used for the spokes already configured for Phase 3.

```
dmvpn-hub1#show dmvpn
Legend: Attrb --> S - Static, D - Dynamic, I - Incompletea
 N - NATed, L - Local, X - No Socket
 # Ent --> Number of NHRP entries with same NBMA peer
Tunnel10, Type:Hub/Spoke, NHRP Peers:90,
 # Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
 1 172.16.0.10 192.168.10.1 UP 5d11h S
 1 172.16.10.1 192.168.10.12 UP 6d09h D
 …
Tunnel20, Type:Hub/Spoke, NHRP Peers:210,
 # Ent Peer NBMA Addr Peer Tunnel Add State UpDn Tm Attrb
 ----- --------------- --------------- ----- -------- -----
 1 172.16.20.1 192.168.20.43 UP 01:46:38 D
…
```

The next sample is from a spoke running DMVPN in Phase 2. We can see that for each spoke, we have a specific route for its advertised protected subnet.

```
 spoke1-phase2-vpn#show ip route eigrp
  192.168.0.0/16 is variably subnetted, 2 subnets, 2
 masks
 D 192.168.10.0/23 [90/2278400] via 192.168.10.1,          ←DMVPN domain for phase2
 5d1h, Tunnel0
 D 192.168.20.0/23 [90/2176000] via 192.168.10.1,          ←DMVPN domain for phase3
 5d1h, Tunnel0
  172.16.0.0.0/16 is variably subnetted, 8 subnets, 3
 masks
```



```
D EX 172.16.0.0/18 [170/2230784] via 192.168.10.1,          ←Corporate subnets
5d1h, Tunnel0

D EX 172.16.2.0/20 [170/2230784] via 192.168.10.1,          ←Corporate subnets
5d1h, Tunnel0

 10.0.0.0/8 is variably subnetted, 158 subnets, 5
masks

D 10.10.0.32/28 [90/2304000] via 192.168.10.13,             ←phase2 spoke3
04:43:02

D 10.10.0.48/28 [90/2304000] via 192.168.10.17, 1d05h       ←phase2 spoke4

D EX 10.0.0.0/8 [170/2230784] via 192.168.10.1, 5d1h,       ←phase3 spokes summary
Tunnel0

D 10.10.0.80/28 [90/2304000] via 192.168.10.21, 5d1h,       ←phase2 spoke5
Tunnel0

D 10.10.0.96/28 [90/2304000] via 192.168.10.111,            ←phase2 spoke6
1d1h, Tunnel0

D 10.10.0.128/28 [90/2304000] via 192.168.10.212,           ←phase2 spoke7
5dh, Tunnel0

… [more lines would follow here for all the remaining
spokes]
```

The next sample is from a spoke running DMVPN in Phase 3. In this case, the spoke sees only the summary routes of all the other spokes' protected subnets.

```
spoke1-phase3-vpn#show ip route eigrp

 192.168.0.0/16 is variably subnetted, 2 subnets, 2 masks

D 192.168.10.0/23 [90/2278400] via 192.168.20.1, 5d1h,          ←DMVPN domain for phase2
Tunnel0

D 192.168.20.0/23 [90/2176000] via 192.168.20.1, 5d1h,          ←DMVPN domain for phase3
Tunnel0

 172.16.0.0.0/16 is variably subnetted, 8 subnets, 3 masks

D EX 172.16.0.0/18 [170/2230784] via 192.168.20.1, 5d1h,        ←Corporate subnets
Tunnel0

D EX 172.16.2.0/20 [170/2230784] via 192.168.20.1, 5d1h,        ←Corporate subnets
Tunnel0

 10.0.0.0/8 is variably subnetted, 2 subnets, 2 masks

D 10.10.0.0/8 [170/2230784] via 192.168.20.1, 5d1h, Tunnel0     ←phase2 all-spokes
                                                                summary

D 10.20.0.0/17 [90/2178560] via 192.168.20.1, 5d03h,            ←phase3 all-spokes
Tunnel0                                                         summary
```

To help the management tasks of a DMVPN, Cisco IOS Software Release 12.4(9)T and later have the **show dmvpn** commands, which greatly facilitate finding information about the nodes in the DMVPN, as well as their dynamically assigned IP addresses and their state.

To debug DMVPN Phase 3, and if Cisco IOS Software Release 12.4(9)T or later is running, new debug commands are available:

```
spoke1-phase3-vpn#debug dmvpn detail all
```


The option “all” includes these, which can also be enabled individually:

```
all Enable NHRP/Tunnel Protection/Crypto debugs
crypto Enable Crypto IKE/IPSec debugs only
nhrp Enable NHRP debugs only
socket Enable Crypto Secure Socket debugs only
tunnel Enable Tunnel Protection debugs
```

ADDITIONAL MIGRATION SCENARIOS

If a DMVPN high-concentration hub is deployed in Phase 2 and needs to be migrated to Phase 3, it is recommended to use the one-time simultaneous migration of all server farm hubs and spokes. This is because a tunnel key is usually **not** recommended for the high-concentration hub design, and thus Phase 2 and Phase 3 simultaneous DMVPN domains in the same real server is not suggested.

REFERENCES

1. **DMVPN Phase 2 Configuration Guide:**
   http://www.cisco.com/en/US/products/ps6350/products_configuration_guide_chapter09186a0080455c71.html
2. **DMVPN Documentation Center:**
   http://cisco.com/go/dmvpn
3. **Large-Scale DMVPN Deployment: Cisco 7200 Server Farm Behind 7600**
   http://www.cisco.com/en/US/products/ps6635/products_white_paper0900aecd803498b1.shtml
4. **Enhanced NHRP shortcut switching:**
   http://www.cisco.com/en/US/products/ps6441/products_feature_guide09186a0080641515.html
5. **Cisco ECT solution guides and information:**
   http://www.cisco.com/go/ect
6. **Cisco Feature Navigator:**
   http://www.cisco.com/go/fn
7. **Cisco Security Manager:**
   http://cisco.com/go/csmanager

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.com 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

Printed in USA C07-374471-00 10/06