Spoke-to-Spoke NHRP Summary Maps

The Spoke-to-Spoke NHRP Summary Maps feature summarizes and reduces the NHRP resolution traffic on the network.

- Information About Spoke-to-Spoke NHRP Summary Maps, on page 1
- Information About NHRP Default Maps, on page 3
- How to Configure Spoke-to-Spoke NHRP Summary Maps, on page 3
- Configuration Examples for Spoke-to-Spoke NHRP Summary Maps, on page 7
- How to Configure NHRP for Tunnel Setup, on page 9
- Configuration Examples for Spoke-to-Spoke NHRP Summary Maps, on page 21
- Deploying Dual Data Centers, on page 21
- Additional References for Spoke-to-Spoke NHRP Summary Maps, on page 23
- Feature Information for Spoke-to-Spoke NHRP Summary Maps, on page 24

Information About Spoke-to-Spoke NHRP Summary Maps

Spoke-to-Spoke NHRP Summary Maps

In DMVPN phase 3, route summarization is performed at a hub. The hub is the next-hop for any spoke to reach any network behind a spoke. On receiving a packet, the hub sends a redirect message to a local spoke and indicates the local spoke to send Next Hop Resolution Protocol (NHRP) resolution request for the destination network. The resolution request is forwarded by the hub to a remote spoke with the destination LAN network. The remote spoke responds to the resolution request and initiates a tunnel with the local spoke.

When a spoke answers an NHRP resolution request for a local host, it uses the explicit IP address network and subnet mask from the Routing Information Base (RIB) in response. Multiple networks behind a local spoke require similar NHRP messages for a host behind remote spoke to exchange packets with the hosts in these networks. It is difficult to handle NHRP messages for a huge number of spokes and large networks behind each spoke.

The number of NHRP messages between spokes can be limited when the first NHRP resolution reply provides information about the network behind a local spoke instead of a specific network. The spoke-to-spoke NHRP summary map uses the configured IP address network and subnet mask in the NHRP resolution response instead of the IP address network and subnet mask from RIB. If RIB has more number of IP address networks (lesser subnet mask length) than the configured IP address network and subnet mask, the spoke still uses the configured IP address network and subnet mask for NHRP resolution response thereby summarizing and

Spoke-to-Spoke NHRP Summary Maps

reducing the NHRP resolution traffic on the network. Use the **ip nhrp summary-map** command to configure NHRP summary map on a spoke.

Note In DMVPN, it is recommended to configure a Rendezvous Point (RP) at or behind the hub. If there is an IP multicast source behind a spoke, the **ip pim spt-threshold infinity** command must be configured on spokes to avoid multicast traffic going through spoke-to-spoke tunnels.

How Spoke-to-Spoke NHRP Summary Maps Works

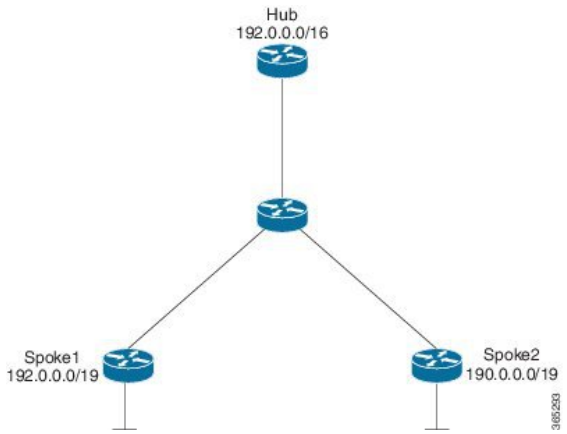
On receiving the resolution request, the spoke

1. Looks into the RIB for the IP address and subnet mask and returns.
2. Checks the IP address and subnet mask against the configured NHRP summary map and verifies if the destination IP address is covered.
3. Sends the summary map in the NHRP resolution reply to the remote spoke and NHRP on the remote spoke adds the IP address and subnet mask with the next-hop of the local spoke to the RIB.

The entire network behind the local spoke is identified to the remote spoke with one NHRP resolution request.

The following figure shows the working of spoke-to-spoke NHRP summary maps.

Figure 1: Spoke-to-Spoke NHRP Summary Maps



A local spoke with the address space 192.0.0.0/19 on its local LAN has all 32-24 RIB entries – 192.0.0.0/24,….192.0.31.0/24. When a routing protocol like EIGRP is used to advertise this local address space, the routing protocol is configured to summarize the networks to 192.0.0.0/19 and advertise that to the hub. The hub summarizes this further, to 192.0.0.0/16, when it advertises it to the other spokes. The other spokes starts with only a 192.0.0.0/16 routing table entry with the next-hop of the hub in the RIB.

If a remote host communicates with 192.0.12.1, the local spoke receives the NHRP resolution request for 192.0.12.1/32. it looks into the RIB and return 192.0.12.0/24 in NHRP resolution reply.

If the local spoke is configured with NHRP summary map for eg. "ip nhrp summary-map 192.0.0.0/19", the local spoke upon receing the resolution request for 192.0.12.1 checks the RIB which return 192.0.12.0/24. the local spoke then check for summary map configuration 192.0.0.0/19 and verifies if the destination 192.0.12.1/32 is covered and returns 192.0.0.0/19 in NHRP resolution reply.

NHRP Summary Map Support for IPv6 Overlay

Spoke-to-spoke NHRP summary maps feature is supported on IPv6 and is configured using **ipv6 nhrp summary-map** command.

Information About NHRP Default Maps

NHRP Default Maps

A default-map specifies the default forwarding and encapsulation that is used in the absence of a better match. When you send a registration request, ror easy provisioning, an NHRP default-map is pushed as a special summary map from the hub (NHS) as part of the registration reply. This is specified by configuring the **ip nhrp summary-map <Prefix> <IPv4/IPv6 NBMA Address>** command on the NHS. The prefix is the network for which default-maps have to be pushed to the NHCs and the NBMA address is the address of the data plane hub (same as the control plane hub for collocated case).

Also, as a part of the registration reply, you can configure the NHCs as neighbors **neighbor nhc Tunnel<number>**'). In addition, you can push any network that is configured locally or the networks imported from other protocols as part of redistribution to subscribing spokes. This allows the sytem to monitor these networks and notify the spokes when there is any change in the NHSs LAN side networks.

When you use NHCs as neighbors instead of summary-map along with redistribution from another routing protocol on the LAN side (OSPF), it is recommended to use route filters while redistributing into NHRP(e.g. from OSPF). NHRP routes use a default tag of the network-id of the interface to learn the route/mapping. You can filter the in-bound route redistribution into NHRP based on these or any other tag that is configuredexplicitly when the network was originally redistributed from NHRP (e.g. into OSPF). Also, you can use other redistribution filtering mechanisms to avoid a loop where another routing protocol imports routes from NHRP and exports them back to NHRP.

Alternatively, the NHS may choose not to specify any NBMA address for a specific prefix or network. In this case, the NHCs is expected to resolve addresses covered by the prefix. This becomes a hub-less model (no data plane hub) and can be set up by using the **resolve** keyword in the summary-map configuration **ip nhrp summary-map <Prefix> resolve**. An NHS may use a mix of both kinds of summary and default maps to provide a default forwarding path for some subnets (till more specific mapping information is learnt, often through resolution), while forcing a resolution for other subnets.

How to Configure Spoke-to-Spoke NHRP Summary Maps

Configuring Spoke-to-Spoke NHRP Summary Maps on Spoke

Note The following task can be performed to configure the spoke device.

SUMMARY STEPS

1. **enable**

2. **configure terminal**
3. **interface tunnel** *number*
4. **ip address** *ip-address mask secondary ip-address mask*
5. **ip nhrp authentication** *string*
6. **ip nhrp summary-map** {*ip-address* | *mask*}
7. **ip nhrp network-id** *number*
8. **ip nhrp nhs** [*hub-tunnel-ip-address*] **nbma** [*hub-wan--ip*] **multicast**
9. **ip nhrp shortcut**
10. **tunnel source** {*ip-address* | *type number*}
11. **tunnel mode gre multipoint**
12. **tunnel key** *key-number*
13. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface tunnel** *number* **Example:** `Device(config)# interface tunnel 5`	Configures a tunnel interface and enters interface configuration mode. • *number*—Specifies the number of the tunnel interface that you want to create or configure. There is no limit on the number of tunnel interfaces you can create.
Step 4	**ip address** *ip-address mask secondary ip-address mask* **Example:** `Device(config-if)# ip address 10.0.0.2 255.255.255.0`	Sets a primary or secondary IP address for the tunnel interface. **Note** All hubs and spokes that are in the same DMVPN network must be addressed in the same IP subnet.
Step 5	**ip nhrp authentication** *string* **Example:** `Device(config-if)# ip nhrp authentication donttell`	Configures an authentication string for an interface using NHRP.
Step 6	**ip nhrp summary-map** {*ip-address*	*mask*} **Example:**	Summarizes and reduces the NHRP resolution traffic on the network.

	Command or Action	Purpose
	`Device(config-if)# ip nhrp summary-map 10.0.0.0/24`	
Step 7	**ip nhrp network-id** *number* **Example:** `Device(config-if)# ip nhrp network-id 99`	Enables NHRP on an interface. • *number*—Specifies a globally unique 32-bit network identifier from a nonbroadcast multiaccess (NBMA) network.
Step 8	**ip nhrp nhs** [*hub-tunnel-ip-address*] **nbma** [*hub-wan--ip*] **multicast** **Example:** `Device(config-if)# ip nhrp nhs 10.0.0.1 nbma 172.17.0.1 multicast`	Configures the hub router as the NHRP next-hop server.
Step 9	**ip nhrp shortcut** **Example:** `Device(config-if)# ip nhrp shortcut`	Enables NHRP shortcut switching.
Step 10	**tunnel source** {*ip-address* | *type number*} **Example:** `Device(config-if)# tunnel source Gigabitethernet 0/0/0`	Sets the source address for a tunnel interface.
Step 11	**tunnel mode gre multipoint** **Example:** `Device(config-if)# tunnel mode gre multipoint`	Sets the encapsulation mode to Multiple Generic Routing Encapsulation (mGRE) for the tunnel interface. • Use this command if data traffic can use dynamic spoke-to-spoke traffic.
Step 12	**tunnel key** *key-number* **Example:** `Device(config-if)# tunnel key 100000`	(Optional) Enables an ID key for a tunnel interface. • *key-number*—Specifies a number to identify a tunnel key. This must be set to the same value on all hubs and spokes that are in the same DMVPN network.
Step 13	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Verifying Spoke-to Spoke NHRP Summary Maps

SUMMARY STEPS

1. **enable**

2. **show ip nhrp**

DETAILED STEPS

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **show ip nhrp**

Example:

The following is an example of show command output on spoke.

```
Device# show ip nhrp

15.0.0.1/32 (vrf1) via 15.0.0.1
   Tunnel3 created 09:09:00, never expire
   Type: static, Flags: used
   NBMA address: 123.0.0.1
15.0.0.20/32 (vrf1) via 15.0.0.20
   Tunnel3 created 00:00:54, expire 00:04:05
   Type: dynamic, Flags: router nhop rib
   NBMA address: 42.0.0.1
190.0.0.0/22 (vrf1) via 15.0.0.10
   Tunnel3 created 09:09:00, never expire
   Type: static, Flags: local
   NBMA address: 121.0.0.1
    (no-socket)
201.0.0.0/22 (vrf1) via 15.0.0.20
   Tunnel3 created 00:00:54, expire 00:04:05
   Type: dynamic, Flags: router rib nho
   NBMA address: 42.0.0.1
```

Displays Next Hop Resolution Protocol (NHRP) mapping information.

Troubleshooting Spoke-to-Spoke NHRP Summary Maps

SUMMARY STEPS

1. **debug dmvpn all nhrp**

DETAILED STEPS

debug dmvpn all nhrp

Checks the IP address and subnet mask received by the spoke for a resolution request.

Example:

```
Device# debug dmvpn all nhrp

NHRP-RT: Attempting to create instance PDB for vrf global(0x0)(0x0)
NHRP-CACHE: Tunnel0: Cache add for target 67.0.0.1/32 vrf global(0x0) label none next-hop 67.0.0.1

NHRP-CACHE: Tunnel0: Cache add for target 67.0.0.0/24 vrf global(0x0) label none next-hop 15.0.0.30
            80.0.0.1
NHRP-CACHE: Inserted subblock node(2 now) for cache: Target 67.0.0.0/24 nhop 15.0.0.30
NHRP-CACHE: Converted internal dynamic cache entry for 67.0.0.0/24 interface Tunnel0 vrf global(0x0)
 to external
NHRP-RT: Adding route entry for 67.0.0.0/24 (Tunnel0 vrf:global(0x0)) to RIB
NHRP-RT: Route addition to RIB Successful
NHRP-RT: Route watch started for 67.0.0.0/23
NHRP-CACHE: Updating label on Tunnel0 for 15.0.0.30 vrf global(0x0), old none new none nhop 15.0.0.30
NHRP-CACHE: Tunnel0: Cache update for target 15.0.0.30/32 vrf global(0x0) label none next-hop 15.0.0.30

            80.0.0.1
NHRP-CACHE: Deleting incomplete entry for 67.0.0.1/32 interface Tunnel0 vrf global(0x0)
NHRP-CACHE: Still other cache entries with same overlay nhop 67.0.0.1
NHRP-RT: Received route watch notification for  67.0.0.0/24
NHRP-RT: Covering prefix is 67.0.0.0/22
NHRP-RT: Received route watch notification for  67.0.0.0/24
NHRP-RT: (0x0):NHRP RIB entry for  67.0.0.0/24  is unreachable
```

Configuration Examples for Spoke-to-Spoke NHRP Summary Maps

Example: Spoke-to-Spoke NHRP Summary Maps

Example: Spoke-to-Spoke NHRP Summary Maps

The following is an example of configuring DMVPN phase 3 on hub for summary map .

```
interface Tunnel0
 ip address 15.0.0.1 255.255.255.0
 no ip redirects
 no ip split-horizon eigrp 2
 ip nhrp authentication cisco123
 ip nhrp network-id 23
 ip nhrp redirect
 ip summary-address eigrp 2 190.0.0.0 255.255.252.0
 ip summary-address eigrp 2 201.0.0.0 255.255.252.0
 tunnel source GigabitEthernet1/0/0
 tunnel mode gre multipoint
 tunnel key 6
end
```

The following example shows how to configure spoke-to-spoke NHRP summary maps on spoke 1.

```
interface Tunnel0
 vrf forwarding vrf1
 ip address 15.0.0.10 255.255.255.0
 ip nhrp authentication cisco123
 ip nhrp summary-map 190.0.0.0/22
 ip nhrp network-id 5
 ip nhrp nhs 15.0.0.1 nbma 123.0.0.1 multicast
 ip nhrp shortcut
 tunnel source GigabitEthernet0/1/0
 tunnel mode gre multipoint
 tunnel key 6
end
```

The following example shows how to configure spoke-to-spoke NHRP summary maps on spoke 2.

```
interface Tunnel0
 ip address 15.0.0.20 255.255.255.0
 ip nhrp authentication cisco123
 ip nhrp summary-map 201.0.0.0/22
 ip nhrp network-id 5
 ip nhrp nhs 15.0.0.1 nbma 123.0.0.1 multicast
 ip nhrp shortcut
 tunnel source GigabitEthernet0/0/0
 tunnel mode gre multipoint
 tunnel key 6
end
```

The following is a sample output of the show ip nhrp command on the hub.

```
Device# show ip nhrp

15.0.0.10/32 via 15.0.0.10
   Tunnel0 created 00:22:26, expire 00:07:35
   Type: dynamic, Flags: registered used nhop
   NBMA address: 41.0.0.1
15.0.0.20/32 via 15.0.0.20
   Tunnel0 created 00:13:43, expire 00:09:36
   Type: dynamic, Flags: registered used nhop
   NBMA address: 42.0.0.1
```

The following is a sample output of the show ip nhrp command on spoke 1.

```
Device# show ip nhrp

15.0.0.1/32 (vrf1) via 15.0.0.1
   Tunnel3 created 09:09:00, never expire
   Type: static, Flags: used
   NBMA address: 123.0.0.1
15.0.0.20/32 (vrf1) via 15.0.0.20
   Tunnel3 created 00:00:54, expire 00:04:05
   Type: dynamic, Flags: router nhop rib
   NBMA address: 42.0.0.1
190.0.0.0/22 (vrf1) via 15.0.0.10
   Tunnel3 created 09:09:00, never expire
```

```
   Type: static, Flags: local
   NBMA address: 121.0.0.1
    (no-socket)
201.0.0.0/22 (vrf1) via 15.0.0.20
   Tunnel3 created 00:00:54, expire 00:04:05
   Type: dynamic, Flags: router rib nho
   NBMA address: 42.0.0.1
```

The following is a sample output of the show ip nhrp command on spoke 2.

```
Device# show ip nhrp

15.0.0.1/32 via 15.0.0.1
   Tunnel0 created 09:08:16, never expire
   Type: static, Flags: used
   NBMA address: 123.0.0.1
15.0.0.10/32 via 15.0.0.10
   Tunnel0 created 00:00:04, expire 01:59:55
   Type: dynamic, Flags: router nhop rib
   NBMA address: 121.0.0.1
190.0.0.0/22 via 15.0.0.10
   Tunnel0 created 00:00:04, expire 01:59:55
   Type: dynamic, Flags: router rib nho
   NBMA address: 121.0.0.1
201.0.0.0/22 via 15.0.0.20
   Tunnel0 created 09:08:16, never expire
   Type: static, Flags: local
   NBMA address: 42.0.0.1
    (no-socket)
```

How to Configure NHRP for Tunnel Setup

Configure NHRP for Tunnel Setup

To set up the tunnel for configuring NHRP:

- Configuring NHRP for Tunnel on Hub1
- Configuring NHRP for Tunnel on Hub2
- Configuring NHRP for Tunnel on a Spoke

Configuring NHRP for Tunnel on Hub1

Note The following task can be performed to configure the NHRP for tunnel on a hub.

SUMMARY STEPS

1. **enable**
2. **configure terminal**

3. **interface tunnel** *number*
4. **ip address** *ip-address mask secondary ip-address mask*
5. **ip nhrp network-id** *number*
6. **ip nhrp redirect interest** <*acl_num/acl_name*>
7. **tunnel source** {*ip-address* | *type number*}
8. **tunnel mode gre multipoint**
9. **tunnel key** *key-number*
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface tunnel** *number* **Example:** `Device(config)# interface tunnel 0`	Configures a tunnel interface and enters interface configuration mode. • *number*—Specifies the number of the tunnel interface that you want to create or configure. There is no limit on the number of tunnel interfaces you can create.
Step 4	**ip address** *ip-address mask secondary ip-address mask* **Example:** `Device(config-if)# ip address 10.0.0.99 255.255.255.0`	Sets a primary or secondary IP address for the tunnel interface. **Note** All hubs and spokes that are in the same DMVPN network must be addressed in the same IP subnet.
Step 5	**ip nhrp network-id** *number* **Example:** `Device(config-if)# ip nhrp network-id 1`	Enables NHRP on an interface. • *number*—Specifies a globally unique 32-bit network identifier from a nonbroadcast multiaccess (NBMA) network.
Step 6	**ip nhrp redirect interest** <*acl_num/acl_name*> **Example:** `Device(config-if)# ip nhrp redirect`	Enables redirect traffic indication if traffic is forwarded with the NHRP network. From Cisco IOS XE 17.11.1a, a new keyword **interest** is introduced to configure the interest ACL in AF VRF, if the traffic VRF matches the AF VRF.

	Command or Action	Purpose
Step 7	**tunnel source** {*ip-address* | *type number*} **Example:** `Device(config-if)# tunnel source Ethernet 0/0`	Sets the source address for a tunnel interface.
Step 8	**tunnel mode gre multipoint** **Example:** `Device(config-if)# tunnel mode gre multipoint`	Sets the encapsulation mode to Multiple Generic Routing Encapsulation (mGRE) for the tunnel interface. • Use this command if data traffic can use dynamic spoke-to-spoke traffic.
Step 9	**tunnel key** *key-number* **Example:** `Device(config-if)# tunnel key 1`	(Optional) Enables an ID key for a tunnel interface. • *key-number*—Specifies a number to identify a tunnel key. This must be set to the same value on all hubs and spokes that are in the same DMVPN network.
Step 10	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring NHRP for Tunnel on Hub2

Note The following task can be performed to configure the NHRP for tunnel on a hub.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **ip address** *ip-address mask secondary ip-address mask*
5. **ip nhrp network-id** *number*
6. **ip nhrp redirect interest** <*acl_num/acl_name*>
7. **tunnel source** {*ip-address* | *type number*}
8. **tunnel mode gre multipoint**
9. **tunnel key** *key-number*
10. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:**	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
	`Device> enable`	
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface tunnel** *number* **Example:** `Device(config)# interface tunnel 1`	Configures a tunnel interface and enters interface configuration mode. • *number*—Specifies the number of the tunnel interface that you want to create or configure. There is no limit on the number of tunnel interfaces you can create.
Step 4	**ip address** *ip-address mask secondary ip-address mask* **Example:** `Device(config-if)# ip address 10.0.0.98 255.255.255.0`	Sets a primary or secondary IP address for the tunnel interface. **Note** All hubs and spokes that are in the same DMVPN network must be addressed in the same IP subnet.
Step 5	**ip nhrp network-id** *number* **Example:** `Device(config-if)# ip nhrp network-id 2`	Enables NHRP on an interface. • *number*—Specifies a globally unique 32-bit network identifier from a nonbroadcast multiaccess (NBMA) network.
Step 6	**ip nhrp redirect interest** <*acl_num/acl_name*> **Example:** `Device(config-if)# ip nhrp redirect`	Enables redirect traffic indication if traffic is forwarded with the NHRP network. From Cisco IOS XE 17.11.1a, a new keyword **interest** is introduced to configure the interest ACL in AF VRF, if the traffic VRF matches the AF VRF.
Step 7	**tunnel source** {*ip-address* | *type number*} **Example:** `Device(config-if)# tunnel source Ethernet 0/0`	Sets the source address for a tunnel interface.
Step 8	**tunnel mode gre multipoint** **Example:** `Device(config-if)# tunnel mode gre multipoint`	Sets the encapsulation mode to Multiple Generic Routing Encapsulation (mGRE) for the tunnel interface. • Use this command if data traffic can use dynamic spoke-to-spoke traffic.
Step 9	**tunnel key** *key-number* **Example:** `Device(config-if)# tunnel key 2`	(Optional) Enables an ID key for a tunnel interface. • *key-number*—Specifies a number to identify a tunnel key. This must be set to the same value on all hubs and spokes that are in the same DMVPN network.

	Command or Action	Purpose
Step 10	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring NHRP for Tunnel on a Spoke

Note The following task can be performed to configure the NHRP for tunnel on a spoke.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **ip address** *ip-address mask secondary ip-address mask*
5. **ip nhrp network-id** *number*
6. **ip nhrp nhs dynamic nbma** {*nbma-address* | *FQDN-string*} [**multicast**] [**priority** *value*] [**cluster** *value*]
7. **ip nhrp path preference** *value*
8. **tunnel source** {*ip-address* | *type number*}
9. **tunnel mode gre multipoint**
10. **tunnel key** *key-number*
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface tunnel** *number* **Example:** `Device(config)# interface tunnel 10`	Configures a tunnel interface and enters interface configuration mode. • *number*—Specifies the number of the tunnel interface that you want to create or configure. There is no limit on the number of tunnel interfaces you can create.

	Command or Action	Purpose
Step 4	**ip address** *ip-address mask secondary ip-address mask* **Example:** `Device(config-if)# ip address 10.0.0.n 255.0.0.0`	Sets a primary or secondary IP address for the tunnel interface. **Note** All hubs and spokes that are in the same DMVPN network must be addressed in the same IP subnet.
Step 5	**ip nhrp network-id** *number* **Example:** `Device(config-if)# ip nhrp network-id 1`	Enables NHRP on an interface. • *number*—Specifies a globally unique 32-bit network identifier from a nonbroadcast multiaccess (NBMA) network.
Step 6	**ip nhrp nhs dynamic nbma** {*nbma-address* | *FQDN-string*} [**multicast**] [**priority** *value*] [**cluster** *value*] **Example:** `Router(config-if)# ip nhrp nhs 10.0.0.99 nbma 1.1.1.99 multicast`	Registers a spoke to a hub. • The NHS protocol address is dynamically fetched by the spoke. • **ip nhrp nhs dynamic nbma** *nbma-address*--Use this command to register a spoke to a hub using the NHS NBMA IP address. **Note** You can use the **ipv6 nhrp nhs dynamic nbma** {*nbma-address* | *FQDN-string*} [**multicast**] [**priority** *value*] [**cluster** *value*] command for registering IPv6 address.
Step 7	**ip nhrp path preference** *value* **Example:** `Device(config-if)# ip nhrp path preference 192`	
Step 8	**tunnel source** {*ip-address* | *type number*} **Example:** `Device(config-if)# tunnel source Ethernet 0/0`	Sets the source address for a tunnel interface.
Step 9	**tunnel mode gre multipoint** **Example:** `Device(config-if)# tunnel mode gre multipoint`	Sets the encapsulation mode to Multiple Generic Routing Encapsulation (mGRE) for the tunnel interface. • Use this command if data traffic can use dynamic spoke-to-spoke traffic.
Step 10	**tunnel key** *key-number* **Example:** `Device(config-if)# tunnel key 1`	(Optional) Enables an ID key for a tunnel interface. • *key-number*—Specifies a number to identify a tunnel key. This must be set to the same value on all hubs and spokes that are in the same DMVPN network.

	Command or Action	Purpose
Step 11	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring NHRP for Tunnel on a Spoke2

Note The following task can be performed to configure the NHRP for tunnel on a spoke2.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **ip address** *ip-address mask secondary ip-address mask*
5. **ip nhrp network-id** *number*
6. **ip nhrp nhs dynamic nbma** {*nbma-address* | *FQDN-string*} [**multicast**] [**priority** *value*] [**cluster** *value*]
7. **ip nhrp path preference** *value*
8. **tunnel source** {*ip-address* | *type number*}
9. **tunnel mode gre multipoint**
10. **tunnel key** *key-number*
11. **end**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface tunnel** *number* **Example:** `Device(config)# interface tunnel 11`	Configures a tunnel interface and enters interface configuration mode. • *number*—Specifies the number of the tunnel interface that you want to create or configure. There is no limit on the number of tunnel interfaces you can create.

	Command or Action	Purpose
Step 4	**ip address** *ip-address mask secondary ip-address mask* **Example:** `Device(config-if)# ip address 11.0.0.n 255.0.0.0`	Sets a primary or secondary IP address for the tunnel interface. **Note** All hubs and spokes that are in the same DMVPN network must be addressed in the same IP subnet.
Step 5	**ip nhrp network-id** *number* **Example:** `Device(config-if)# ip nhrp network-id 1`	Enables NHRP on an interface. • *number*—Specifies a globally unique 32-bit network identifier from a nonbroadcast multiaccess (NBMA) network.
Step 6	**ip nhrp nhs dynamic nbma** {*nbma-address* | *FQDN-string*} [**multicast**] [**priority** *value*] [**cluster** *value*] **Example:** `Router(config-if)# ip nhrp nhs 11.0.0.98 nbma 1.1.1.98 multicast`	Registers a spoke to a hub. • The NHS protocol address is dynamically fetched by the spoke. • **ip nhrp nhs dynamic nbma** *nbma-address*--Use this command to register a spoke to a hub using the NHS NBMA IP address. **Note** You can use the **ipv6 nhrp nhs dynamic nbma** {*nbma-address* | *FQDN-string*} [**multicast**] [**priority** *value*] [**cluster** *value*] command for registering IPv6 address.
Step 7	**ip nhrp path preference** *value* **Example:** `Device(config-if)# ip nhrp path preference 64`	
Step 8	**tunnel source** {*ip-address* | *type number*} **Example:** `Device(config-if)# tunnel source Ethernet 0/0`	Sets the source address for a tunnel interface.
Step 9	**tunnel mode gre multipoint** **Example:** `Device(config-if)# tunnel mode gre multipoint`	Sets the encapsulation mode to Multiple Generic Routing Encapsulation (mGRE) for the tunnel interface. • Use this command if data traffic can use dynamic spoke-to-spoke traffic.
Step 10	**tunnel key** *key-number* **Example:** `Device(config-if)# tunnel key 2`	(Optional) Enables an ID key for a tunnel interface. • *key-number*—Specifies a number to identify a tunnel key. This must be set to the same value on all hubs and spokes that are in the same DMVPN network.

	Command or Action	Purpose
Step 11	**end** **Example:** `Device(config-if)# end`	Exits interface configuration mode and returns to privileged EXEC mode.

Configuring Network Registration and Redistribution

You can configure the networks to be registered as part of the router block (global or address-family). These netwroks can also be learnt as redistributed from another routing process.

Configuring Spoke for Network Registration and Redistribution

To register and redistribute the spoke network:

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **router nhrp** *number*
4. **neighbor nhs tunnel** *number*
5. **neighbor nhs tunnel** *number*
6. (Optional) **router ospf** *process id*
7. (Optional) **redistribute nhrp** *number* **tag** *number*
8. (Optional) **network** *ip-address wildcard-mask* **area** *area-id*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**router nhrp** *number* **Example:** `Device(config-if)# router nhrp 5`	Enables NHRP on an interface.
Step 4	**neighbor nhs tunnel** *number* **Example:**	

	Command or Action	Purpose
	`Device(config-if)# neighbor nhs Tunnel0`	
Step 5	**neighbor nhs tunnel** *number* **Example:** `Device(config-if)# neighbor nhs Tunnel1`	
Step 6	(Optional) **router ospf** *process id* **Example:** `Device(config-if)# router nhrp 5`	Enables OSPF routing and enters router configuration mode..
Step 7	(Optional) **redistribute nhrp** *number* **tag** *number* **Example:** `Device(config-router)# redistribute nhrp 5 tag 55`	
Step 8	(Optional) **network** *ip-address wildcard-mask* **area** *area-id* **Example:** `Device(config-router)# network 192.168.2.0 0.0.0.255 area 0`	Defines an interface on which OSPF runs and defines the area ID for that interface.

Configuring Hub for Network Registration and Redistribution

You can configure the hub with just advertising one or more summary mapping information or instruct the spokes to resolve all networks (in the later case, it degenerates into a hub-less model!) using the standard summary-map command.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **interface tunnel** *number*
4. **IP nhrp summary-map** *ip-address ? preference?*
5. **IP nhrp summary-map** *ip-address ? preference?*
6. **IP nhrp summary-map** *ip-address ? preference?*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**interface tunnel** *number* **Example:** `Device(config-if)# interface Tunnel0`	Configures an interface and enters interface configuration mode.
Step 4	**IP nhrp summary-map** *ip-address ? preference?* **Example:** `Device(config-router)# ip nhrp summary-map 192.168.0.0/16 1.1.1.99 preference 1`	Summarizes and reduces the NHRP resolution traffic on the network.
Step 5	**IP nhrp summary-map** *ip-address ? preference?* **Example:** `Device(config-router)# ip nhrp summary-map 192.168.0.0/20 1.1.1.99 preference 16`	Summarizes and reduces the NHRP resolution traffic on the network.
Step 6	**IP nhrp summary-map** *ip-address ? preference?* **Example:** `Device(config-router)# ip nhrp summary-map 192.168.128.0/20 1.1.1.99 preference 32`	Summarizes and reduces the NHRP resolution traffic on the network.

Verifying NHRP Configuration?

SUMMARY STEPS

1. **enable**
2. **show ip routenhrp | begin Gateway**

DETAILED STEPS

Step 1 **enable**

Example:

```
Device> enable
```

Enables privileged EXEC mode.

- Enter your password if prompted.

Step 2 **show ip routenhrp | begin Gateway**

Example:

The following is an example of show command output on hub.

```
Device# show sh ip route nhrp | begin Gateway

00.0.0.0/32 is subnetted, 1 subnets
H G  100.100.100.100 [15/338] via 11.0.0.2, 09:53:20, Tunnel1
H G  192.168.1.0/24 [15/1016] via 11.0.0.1, 09:50:27, Tunnel1
H G  192.168.2.0/24 [15/338] via 11.0.0.2, 09:53:20, Tunnel1
H G  192.168.11.0/24 [15/1016] via 11.0.0.1, 09:50:27, Tunnel1
H G  192.168.12.0/24 [15/338] via 11.0.0.2, 09:53:20, Tunnel1
 192.169.1.0/32 is subnetted, 1 subnets
H G  192.169.1.1 [15/1016] via 11.0.0.1, 09:50:27, Tunnel1
 195.168.1.0/32 is subnetted, 1 subnets
H G  195.168.1.1 [15/1016] via 11.0.0.1, 09:50:27, Tunnel1
H G  195.168.2.0/24 [15/338] via 11.0.0.2, 09:53:20, Tunnel1
H G  199.1.1.0/24 [15/338] via 11.0.0.2, 09:53:20, Tunnel1
Hub-2#sh ip route 192.168.1.0 255.255.255.0
Routing entry for 192.168.1.0/24
 Known via "nhrp 5", distance 15, metric 1016
 Tag 2, type registered
 Last update from 11.0.0.1 on Tunnel1, 09:51:17 ago
 Routing Descriptor Blocks:
 * 11.0.0.1, from 11.0.0.1, 09:51:17 ago, via Tunnel1
 Route metric is 1016, traffic share count is 1
 Route tag 2
Hub-2#
```

Example:

The following is an example of show command output on spoke.

```
Device# sh ip protocols | sec nhrp

Routing Protocol is "nhrp 5"
 Redistributing: connected, static, rip
 Maximum path: 32
 Routing for Networks:
   192.168.12.0
 Publishing Routes over Interfaces:
   Tunnel0
   Tunnel1
 Imported Networks:
   Network                Pref          Tag      Route Source
   100.100.100.100/32      255   4294967295      connected
   192.168.2.0/24          255   4294967295      connected
   199.1.1.0/24            255            0      static
   195.168.2.0/24          255           11      rip
 Routing Information Sources:
   Gateway            Distance     Last Update
   11.0.0.98                16     09:55:59
   10.0.0.99                16     09:55:59
 Distance: (default is 250)
Spoke-2#
Spoke-2#sh ip route nhrp | begin Gateway
Gateway of last resort is not set
H g  192.0.0.0/8 [16/255], 00:00:03, Tunnel1
                 [16/255], 00:00:03, Tunnel0
H g  192.168.0.0/16 [16/4064] via 11.0.0.98, 10:02:37, Tunnel1
```

```
                    [16/4064] via 10.0.0.99, 10:02:37, Tunnel0
H g  192.168.0.0/20 [16/2032] via 11.0.0.98, 10:02:37, Tunnel1
                    [16/4064] via 10.0.0.99, 10:02:37, Tunnel0
H    192.168.1.0/24 [250/1016] via 11.0.0.1, 00:00:01, Tunnel1
H g  192.168.128.0/20 [16/4064] via 11.0.0.98, 10:02:37, Tunnel1
                      [16/2032] via 10.0.0.99, 10:02:37, Tunnel0
Spoke-2#
```

Displays Next Hop Resolution Protocol (NHRP) mapping information.

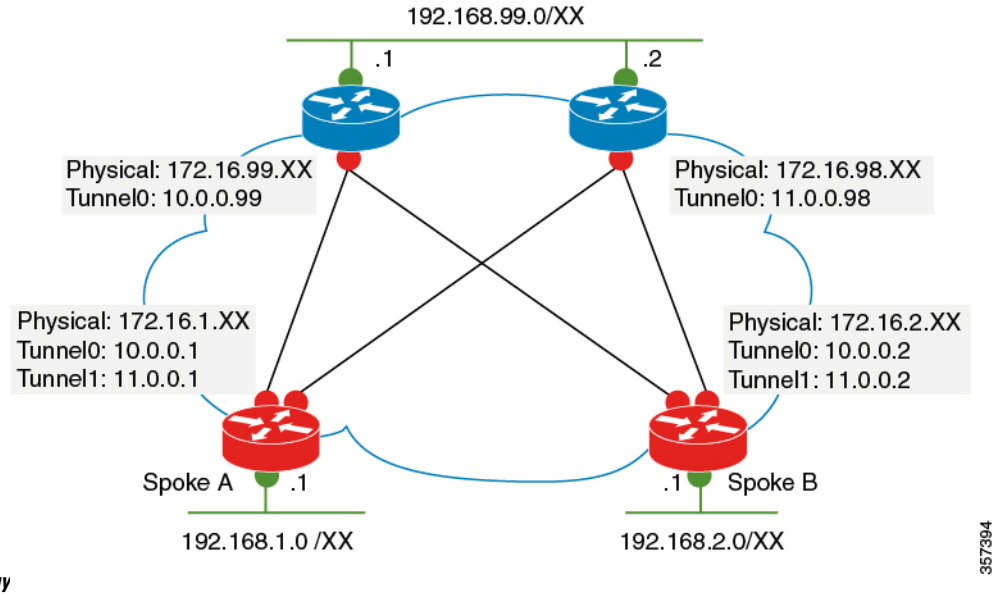
Configuration Examples for Spoke-to-Spoke NHRP Summary Maps

Example: Dual Hub and Dual DMVPN Design

Deploying Dual Data Centers

In this topologgy, the tunnel configuration is a standard DMVPN tunnel configuration with the hub Datacenter (DC) tunnel which is a multipoint. This DMVPN tunnel configuration is without a routing protocol. The spoke (branch) tunnel can be either point-to-point or multipoint. The spoke and branch routers register their LAN networks (either configured or redistributed from connected or static or another routing protocol) with the hub DC router. The hub router sends back one or more summary routes (configured using summary-map) as a part of the registration reply. These routes can be active-active (ECMP/UCMP) or active-passive and the ratio of preferences governs the load sharing ratio (flow based). This provides both egress load-balancing and ingress traffic engineering behaviour (if all nodes respect the preference). Also, a router can override to use active-passive even if the source says active-active by using the **traffic-share** command in the router mode. In such a case, egress load distribution is governed by local configuration overriding ingress traffic engineering. The common standard routing operations of redistribution,admin distance, filtering(in/out), tagging(local) and so on are available.

Figure 2: Deploying Dual Datacenter



Topology

This sample configuration example shows how to configure the dual datacenters.

```
Example Datacenter 1
crypto ikev2 profile default
 match identity remote any
 authentication remote pre-share key CISCO
 authentication local pre-share key CISCO
 dpd 10 2 periodic
!
crypto ipsec transform-set default esp-gcm 256
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Tunnel0
 ip address 10.0.0.99 255.0.0.0
 ip nhrp summary-map 192.168.0.0/16 172.16.99.1 preference 96
 ip nhrp summary-map 192.169.0.0/16 172.16.99.1 preference 96
 ip nhrp network-id 1
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel key 1
 tunnel protection ipsec profile default
!

Example Datacenter 2

crypto ikev2 profile default
 match identity remote any
 authentication remote pre-share key CISCO
 authentication local pre-share key CISCO
 dpd 10 2 periodic
!
crypto ipsec transform-set default esp-gcm 256
!
crypto ipsec profile default
 set ikev2-profile default
!
interface Tunnel1
```

```
 ip address 11.0.0.98 255.0.0.0
 ip nhrp summary-map 192.168.0.0/16 172.16.98.1 preference 32
 ip nhrp summary-map 192.169.0.0/16 172.16.98.1 preference 32
 ip nhrp network-id 2
 ip nhrp path preference 64
 tunnel source Ethernet0/0
 tunnel mode gre multipoint
 tunnel key 2
 tunnel protection ipsec profile default
!
```

Note Note: The summary-map on the hub is relatively static from hub's LAN perspective. For exmaple, spokes may not learn if the LAN side link is down unless there is an inter-router path at the DC. However, it tracks the hub reachability and can be unreachable (on the spokes) when the hub is unreachable. If it is dynamically tracked similar to regular routing, then redistribution along with neighbour command can be used(newer releases) on the hub router. **router nhrp 5 redistribute bgp 99 <<<<< LAN side protocol at DC neighbor nhc Tunnel0!** However, this is not meant to be used for distributing a large number of subnets to the spokes. Also, like any other protocol, care has to be taken while redistributing routes cyclically NHRP >OSPF> NHRP. For example, tag routes while redistributing from NHRP to OSPF so that we can filter them while redistributing back from OSPF to NHRP. For ease of use, NHRP routes are auto-tagged with a value which is the network-id on the interface on which they are learnt.

Additional References for Spoke-to-Spoke NHRP Summary Maps

Related Documents

Related Topic	Document Title
Cisco IOS security commands	• Cisco IOS Security Command Reference: Commands A to C • Cisco IOS Security Command Reference: Commands D to L • Cisco IOS Security Command Reference: Commands M to R • Cisco IOS Security Command Reference: Commands S to Z

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for Spoke-to-Spoke NHRP Summary Maps

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature Information for Spoke-to-Spoke NHRP Summary Maps

Feature Name	Releases	Feature Information
Spoke-to-Spoke NHRP Summary Maps		The Spoke-to-Spoke Next Hop Resolution Protocol (NHRP) Summary Maps feature summarizes and reduces the NHRP resolution traffic on the network. The following commands were introduced or modified by this feature: **ip nhrp summary-map, ipv6 summary-map**.