6AOSCG0071-29B
October 2015

ADTRAN

Configuration Guide

DMVPN in AOS

This configuration guide describes the configuration steps for Dynamic Multipoint Virtual Private Networking (DMVPN) components in ADTRAN Operating System (AOS) products. This configuration guide includes an overview of DMVPN functionality, its configuration in AOS products, and troubleshooting steps for DMVPN configurations.

This guide contains the following sections:

- *DMVPN Overview on page 2*
- *Hardware and Software Requirements and Limitations on page 4*
- *Configuring NHRP, NHC, and Per-host IPsec SAs for Phase 1 DMVPN on page 5*
- *Configuring mGRE, NHC, and IPsec for Phase 2 DMVPN on page 8*
- *DMVPN Component Configuration Examples on page 13*
- *DMVPN Configuration Command Summary on page 19*
- *Troubleshooting on page 24*
- *Additional Resources on page 27*

DMVPN Overview

DMVPN is a feature set of various protocols that provides easier configuration, implementation, and scalability of traditional hub-and-spoke VPN networks. A DMVPN network can be used in college campuses, retail settings, or for remote connections in a corporate setting, providing connectivity between several spokes and a centralized hub within the VPN framework. DMVPN offers several improvements over traditional VPN networks, because it allows dynamic assignment of IP addresses to the network spokes, provides dynamic tunnel creation and tear down, and assists in streamlining configuration and management of a large number of low-bandwidth spokes. DMVPN can be used with or without Internet Protocol security (IPsec), and operates using Generic Routing Encapsulation (GRE) tunnels for communication between the spokes and the hub. In addition, Next Hop Resolution Protocol (NHRP) is used to register spokes with the network hub, which simplifies configuration of the hub itself.

DMVPN in AOS

In AOS, DMVPN is implemented in a hub-and-spoke network with multiple implementation phases. In the first phase, spokes communicate with each other through a centralized hub. In the second phase, spokes can communicate directly. The difference between DMVPN operation in these phases is detailed in the following sections.

DMVPN Phase 1 in AOS

In AOS, DMVPN is implemented in a hub-and-spoke network. In a hub-and-spoke phase 1 DMVPN layout, multiple spokes communicate with a centralized hub in order to talk to each other (rather than communicating directly). Communication is facilitated by NHRP and the creation of GRE tunnels between the spokes and the hub. The GRE tunnels from the spoke to hub operate in point-to-point mode, whereas GRE tunnels created on the hub operate in multipoint mode. In AOS, the AOS router is configured to operate as a spoke in the network, as a next hop client (NHC), therefore configuration is done on the spoke, not the hub. As an NHRP client, the AOS router uses NHRP to register its own address mappings. When configured, the AOS product operates as an NHRP client and exchanges NHRP registration requests and registration responses between itself and the hub, which operates as a next hop server (NHS). The hub uses the registration information to make forwarding decisions in its multipoint GRE tunnel, and no local routing decisions are made based on NHRP. *Figure 1 on page 3* describes packet flow through a hub-and-spoke DMVPN network, as the packets flow from the host 192.168.1.101 to 192.168.2.101. In this example, only the hub and spoke exchange NHRP messages, and the only messages exchanged are registration requests from the spoke to the hub and registration responses from the hub to the spoke. The hub uses the information from the registrations to make forwarding decisions in its multipoint GRE tunnel.

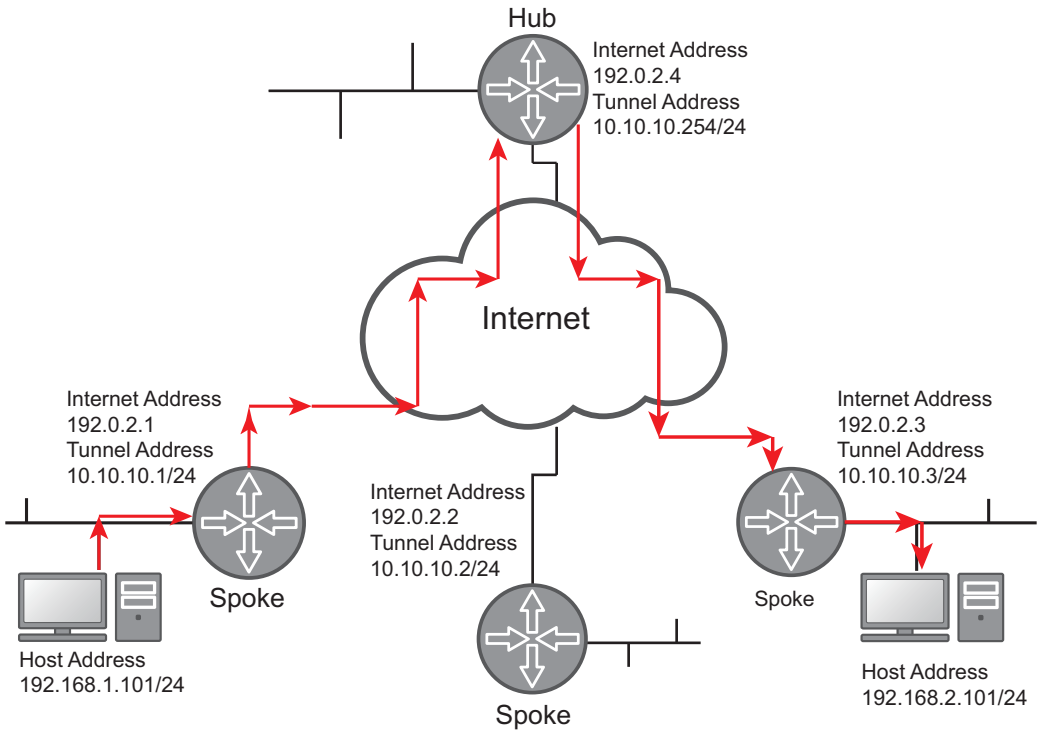

Figure 1. Packet Flow in a Phase 1 Hub-and-Spoke DMVPN Network

To configure the AOS product as a spoke in a phase 1 DMVPN network, you must configure it as an NHC. You have the option to implement IPsec on the GRE tunnels created within the network, but it is not required. The configuration steps necessary for implementing phase 1 DMVPN are described in *Configuring NHRP, NHC, and Per-host IPsec SAs for Phase 1 DMVPN on page 5*.

DMVPN Phase 2 in AOS

In AOS, DMVPN phase 2 is implemented in a hub-and-spoke network, where support for spoke-to-spoke communications is incorporated. In this type of DMVPN topology, spokes can send traffic directly to each other, rather than relying on the hub for spoke-to-spoke communication. *Figure 2 on page 4* describes the packet flow through a hub-and-spoke DMVPN network in which spoke-to-spoke communication is configured. In this example, messages can be exchanged between the hub and the spoke, or they can be exchanged between spokes directly, as traffic flows from host 192.168.1.101 to 192.168.2.101. When traffic from host 192.168.1.101 reaches the spoke (10.10.10.1), the spoke's routing table resolves the next hop as 10.10.10.3 (the tunnel address of the destination spoke). Since the source spoke does not immediately know how to reach 10.10.10.3 directly, it forwards the packet to the hub which then passes it to the destination spoke. This functionality is like a phase 1 DMVPN network. Simultaneously, the source spoke (10.10.10.1) generates an NHRP resolution request for the destination spoke's Internet address and forwards this request to the hub. The hub then forwards this request to the destination spoke (10.10.10.3). The destination spoke (10.10.10.3) generates a response with its Internet address, sends it to the hub, and the hub then forwards the response to the source spoke (10.10.10.1). Once the source spoke receives the response, traffic switches from being forwarded to the destination by the hub, and the spokes at 10.10.10.1 and 10.10.10.3 begin to communicate directly.

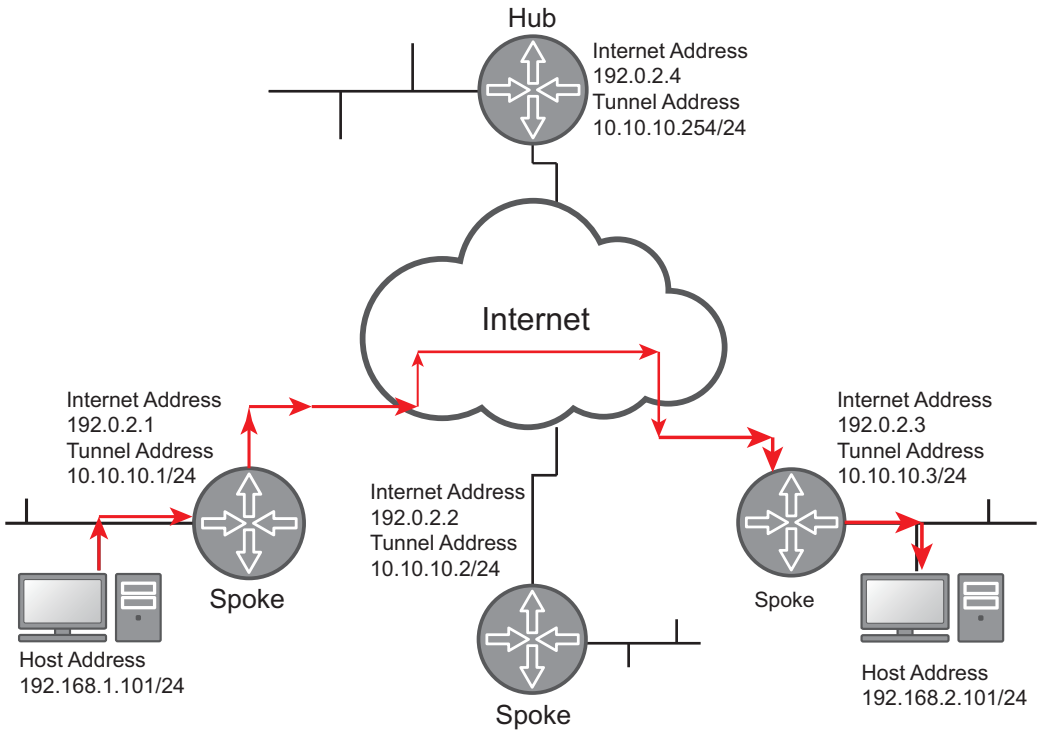

Figure 2. Packet Flow in a Phase 2 Hub-and-Spoke DMVPN Network

To configure the AOS product as a spoke in a phase 2 DMVPN network, configure phase 2 NHC options, Multipoint GRE (mGRE) tunnels, and IPsec profiles. The configuration steps necessary for implementing DMVPN phase 2 are described in *Configuring mGRE, NHC, and IPsec for Phase 2 DMVPN on page 8*.

Hardware and Software Requirements and Limitations

The DMVPN phase 1 networking, NHRP client, and per-host mode for IPsec security association (SA) features are supported on AOS products running AOS firmware R11.7.0 and later, as described in the *AOS Feature Matrix*, available online at https://supportforums.adtran.com.

The DMVPN phase 2 networking, NHRP client, mGRE tunnels, and IPsec profile features are supported on AOS products running AOS firmware R11.9.0 and later, as described in the *AOS Feature Matrix*, available online at https://supportforums.adtran.com.

To configure DMVPN, you should be familiar with VPN, GRE tunnel, IPsec, and crypto map configuration and operation. Additional documentation covering these subjects is listed in *Additional Resources on page 27*. The features described in this guide were introduced in R11.7.0 for DMVPN implementation and familiarity with older features is assumed.

In its initial release, AOS DMVPN support is implemented by configuring the AOS router as an NHRP client. The router is configured as a spoke in a hub-and-spoke DMVPN network topology. In its second release, AOS DMVPN support is implemented by configuring the AOS router as an NHRP client, configuring mGRE tunnels on the router, and configuring IPsec profiles to facilitate spoke-to-spoke communication.

NHRP Configuration Considerations

The following are NHRP functionality and configuration considerations when configuring NHRP on an AOS router:

- When NHRP is operating on a point-to-point GRE tunnel, only NHRP registration requests and error indication messages are sent, while only NHRP registration and error indication replies are processed.
- NHRP authentication extensions are present in AOS generated packets only if NHRP authentication is configured on the tunnel interface.
- If an NHRP registration request has not been answered with a corresponding reply, the NHC retransmits the request at the following intervals: 1s, 2s, 4s, 8s, 16s, 32s, 64s. After the final interval (64s), the unanswered request is retransmitted every 64 seconds until it answered or until the NHC's NHS configuration is changed. If an NHS has not positively acknowledged any of the previous three NHRP registration requests, it is placed in a DOWN state.

IPsec and NAT

If one or more GRE endpoints are behind a network address translation (NAT) device, and IPsec profiles are being used, the GRE endpoint behind NAT may not be able to communicate with other GRE endpoints that are not behind NAT. This occurs only when GRE is used with IPsec. There are no interoperability issues with non-IPsec GRE and NAT.

Configuring NHRP, NHC, and Per-host IPsec SAs for Phase 1 DMVPN

To configure the components for phase 1 DMVPN, you will configure the AOS router as an NHC, specify its NHRP settings, and optionally configure per-host IPsec SAs. The configurations for these components are discussed in the following sections.

Configuring the AOS Router as an NHC

An NHC serves as the spoke in a hub-and-spoke DMVPN network. By default, each AOS router running AOS firmware R11.7.0 or later has the ability to function as an NHC that uses NHRP for communication in the phase 1 DMVPN network. To configure the NHRP settings on the AOS router, follow these steps:

1. Specify the address used by the router (NHC) to communicate with the hub (NHS). This address is the private tunnel address used in the GRE tunnel between the spoke and the hub. Only a single address can be configured for the point-to-point GRE tunnel. Specify this address using the **ip nhrp nhs** <*ip address*> command from the Tunnel Interface Configuration mode. The <*ip address*> is the private tunnel address on the NHS. Specify IP addresses in dotted decimal notation; for example, **10.10.10.1**. Use the **no** form of this command to remove the address from the tunnel's configuration. Enter the command as follows:

(config)**#interface tunnel 1 gre ip**
(config-tunnel 1)**#ip nhrp nhs 10.10.10.1**

2. Optionally specify the authentication string used on the router for NHRP communications using the command **ip nhrp authentication** <*string*>. This authentication type used for NHRP communication is not encrypted. All routers communicating with NHRP must have the same authentication string. The <*string*> parameter is a text string of no more than **8** characters. By default, the NHRP authentication is disabled. Use the **no** form of this command to return to the default setting. To enable NHRP authentication and specify an authentication string, enter the command from the Tunnel Interface Configuration mode as follows:

   (config-tunnel 1)**#ip nhrp authentication STRINGX**

3. Specify how often the router sends NHRP registration requests to the NHS using the **ip nhrp holdtime** <*value*> command. The <*value*> parameter is the time (in seconds) between requests. Valid range is **1** to **65535** seconds. By default, this value is set to **7200** seconds. In addition, by default, the NHRP registration requests are sent at intervals of one third the hold time value; for example, if the hold time is set to 7200 seconds (default), then the registration requests are sent every 2400 seconds. Use the **no** form of this command to return to the default setting. To change the NHRP hold time for NHRP registration requests, enter the command from the Tunnel Interface Configuration mode as follows:

   (config-tunnel 1)**#ip nhrp holdtime 800**

4. Optionally specify how often the router sends NHRP registration requests to the NHS independent of the hold time setting using the **ip nhrp registration timeout** <*value*> command. The <*value*> parameter is the time, in seconds, between requests. This value must be less than or equal to the hold time value. Valid range is **1** to **65535** seconds. By default, this option is not configured and the registration requests are sent at intervals of one third the value of the hold time. Use the **no** form of this command to return to the default value. To optionally configure that requests are sent independently from the hold time value, enter the command from the Tunnel Interface Configuration mode as follows:

   (config-tunnel 1)**#ip nhrp registration timeout 300**

The NHRP parameters are now configured on the AOS router and the router can act as an NHC.

Configuring Per-host IPsec Security Associations for DMVPN

When the spoke communicates with the hub in a phase 1 DMVPN network, it uses a GRE tunnel. You can optionally choose to configure IPsec for the purposes of tunnel security. When IPsec is configured for the tunnel, secure traffic flows between the public IP addresses of the hub and spokes. Secure traffic in the tunnel is facilitated by IPsec SAs. SAs define the rules for providing IPsec protection for packets traversing a VPN tunnel. Included in these rules are information about outer IP headers, encryption and hash algorithms, secret-derived keys, a unique identifier for the SA, the selectors defining the traffic to be protected, SA lifetimes, and the traffic direction (outbound for encryption and inbound for decryption). SAs use VPN selectors to define the traffic protected by IPsec. Typically these VPN selectors are defined using an access control list (ACL). Typically, the IP addresses of the spokes are assigned dynamically from the Internet service provide. In this case, the ACL entry used as a VPN selector for the IPsec SA would appear as follows:

(config)**#ip access-list extended VPN-10**
(config-ex-nacl)**#permit gre any host** <*hub's public IP address*>

When using DMVPN, however, this type of ACL entry allows the hub to have multiple outbound IPsec SAs at the same time with **any** as the destination traffic selector, making it impossible for the hub to able to select the appropriate outbound IPsec SA for traffic protection. To avoid this issue, when using DMVPN, you can configure a per-host IPsec SA on the AOS router. The per-host IPsec SA provides the VPN selectors with the source and destination IP address of the packet requiring IPsec protection. *Figure 3* and *Figure 4* describe the differences in the network traffic flow when per-host IPsec SAs are configured.

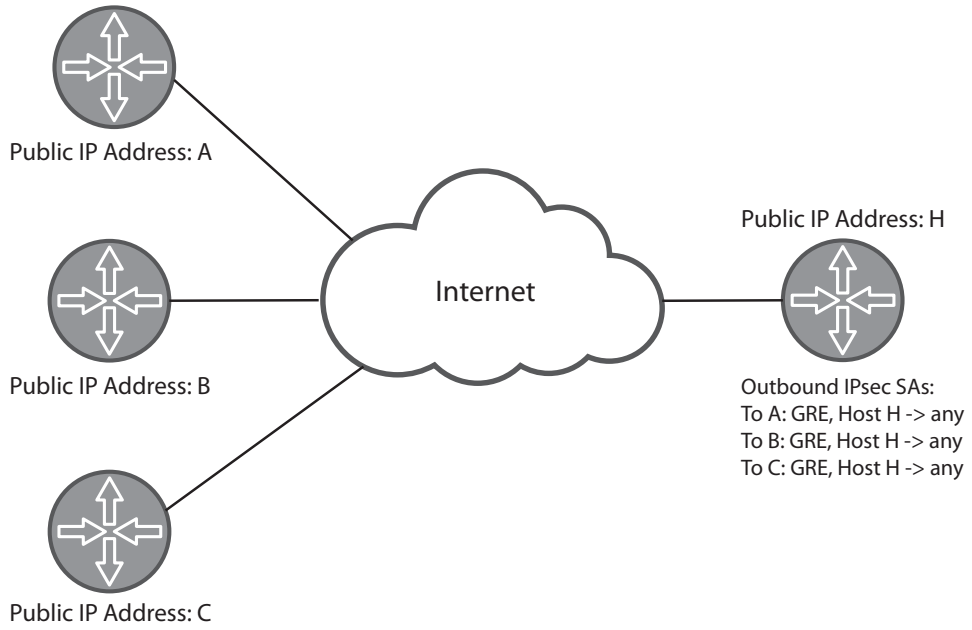

Figure 3. Outbound IPsec SAs without Per-Host Mode

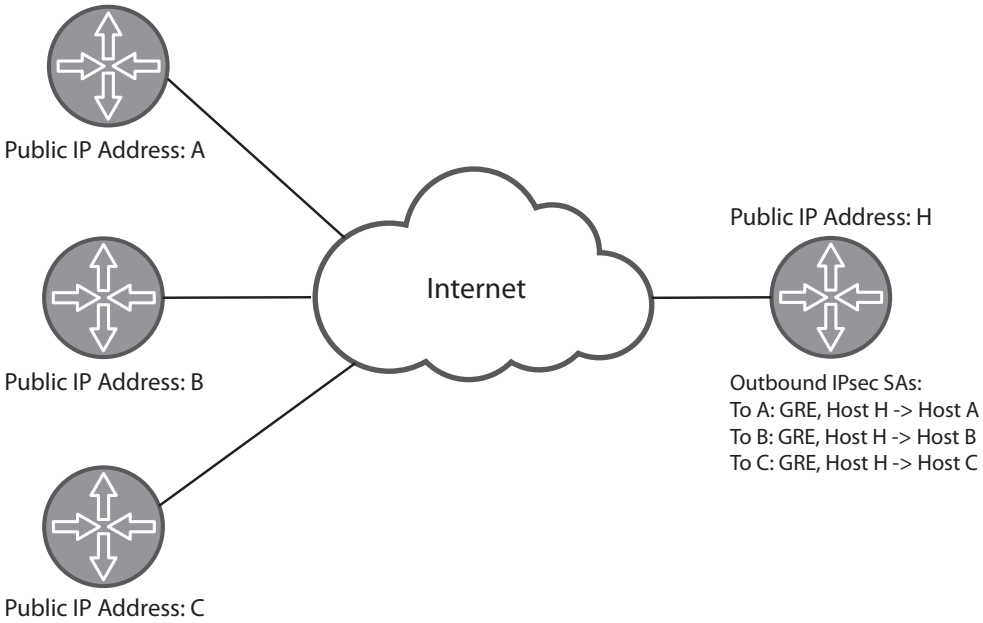

Figure 4. Outbound IPsec SAs with Per-Host Mode

To configure per-host mode for the IPsec SA, enter the **set security-association level per-host** command on the crypto map entry that will generate the SA. When enabled, per-host mode specifies that the source and destination IP addresses of the packet requiring IPsec protection are placed in the VPN selectors used in Quick Mode IPsec SA generation. Use the **no** form of this command to disable the per-host mode. Per-host mode applies only to crypto map entries keyed by Internet Key Exchange (IKE). This feature is not available in crypto maps keyed manually. By default, per-host mode is disabled. To enable per-host mode in the crypto map, enter the command in the crypto map's configuration as follows:

(config)**#crypto map MYMAP 100 ipsec-ike**
(config-crypto-map)**#set security-association level per-host**

Exercise caution when enabling the set security-association level per-host command. If many host-to-host conversations are being protected by the crypto map entry, a large number of IPsec SAs can be created, which can consume significant memory and processor resources on the device.

Configuring mGRE, NHC, and IPsec for Phase 2 DMVPN

In phase 2 DMVPN, spoke-to-spoke communication is supported. This communication is possible because of mGRE tunnels created on the spoke, which learn tunnel destinations dynamically and can have multiple endpoints, NHC configurations that capitalize on mGRE functionality, and IPsec profiles which simplify the configuration of VPN tunnels by eliminating the need to define a crypto map entry and ACL for each peer. The configuration of each of these components are described in the following sections.

Creating an mGRE Tunnel

The first step for phase 2 DMVPN configuration is to configure an mGRE tunnel on the spoke. To accomplish this, enter the **interface tunnel** <*number*> **multipoint-gre ip** command from the Global Configuration mode. The <*number*> parameter is the tunnel interface number; valid range is **1** to **1024**. Use the **no** form of this command to remove the interface.

To create an mGRE tunnel interface, enter the command as follows:

(config)**#interface tunnel 1 multipoint-gre ip**
(config-tunnel 1)#

Once the mGRE tunnel interface is created, you can configure the necessary NHC settings for phase 2 DMVPN.

Configuring the NHC for Phase 2 DMVPN

In DMVPN phase 2, additional NHRP settings are available for configuring the router as an NHC. To configure the additional settings, follow these steps:

1. Use the **ip nhrp map** <*destination ipv4 address*> <*nbma address*> command from the tunnel interface's configuration mode to statically create an NHRP mapping between the IPv4 address and the nonbroadcast multiaccess (NBMA) address of the NHS. Use the **no** form of this command to remove the mapping. The IPv4 destination address is the private tunnel address, and the NBMA address is the tunnel's public facing address. IP addresses are expressed in dotted decimal notation; for example,

10.10.10.1. By default, no mapping exists between the private and public tunnel addresses. To statically create a mapping between the IPv4 destination address **10.10.10.254** and the NBMA address **192.0.2.4**, enter the command as follows:

(config)**#interface tunnel 1 multipoint-gre ip**
(config-tunnel 1)**#ip nhrp map 10.10.10.254 192.0.2.4**

2. Use the **ip nhrp map multicast** <*nbma address*> command to statically add an NHRP mapping for multicast and broadcast traffic to a NMBA address. The NHS is typically used as the NBMA address. The <*nbma address*> parameter specifies the NBMA address that will receive multicast and broadcast traffic. Express NBMA addresses in dotted decimal notation; for example, **192.168.1.101**. By default, no mapping is configured. Use the **no** form of this command to remove the mapping. The following example enables multicast and broadcast traffic to the NMBA address **192.0.2.4**:

   (config)**#interface tunnel 1 multipoint-gre ip**
   (config-tunnel 1)**#ip nhrp map multicast 192.0.2.4**

3. Use the **ip nhrp record** command to specify whether NHRP requests and replies should include forward and backward record extensions. Use the **no** form of this command to disable the addition of these extensions. By default, these extensions are included in NHRP requests and replies. To disable these extensions, enter the command as follows:

   (config)**#interface tunnel 1 multipoint-gre ip**
   (config-tunnel 1)**#no ip nhrp record**

4. Use the **ip nhrp registration non-unique** command to specify whether the Unique flag is set in the NHRP registration packet. This feature is disabled by default; however, because the GRE tunnel source is used in NHRP registration, and when the source IP address changes, a new registration with the NHS occurs, ADTRAN recommends enabling the feature on interfaces where the IP addresses can change. Once enabled, you can use the **no** form of this command to remove the Unique flag. To enable the feature, enter the command as follows:

   (config)**#interface tunnel 1 multipoint-gre ip**
   (config-tunnel 1)**#ip nhrp registration non-unique**

The NHRP configuration for a phase 2 DMVPN NHC is now complete. The next step is to configure IPsec profiles for traffic security within the mGRE tunnels.

Configuring IPsec Profiles for Phase 2 DMVPN

IPsec profiles are used to simplify the configuration of VPN tunnels in a spoke-to-spoke or partial mesh DMVPN network by eliminating the need to define a crypto map entry and ACL for each peer, as well as the traffic selectors in the ACLs for each remote or local network combination that requires IPsec protection. Instead, the profile provides protection to traffic traversing an mGRE tunnel interface by inferring a VPN peer address from the tunnel destination, the traffic selectors from the tunnel type, and the source and destination addresses of the tunnel interface. Once these parameters are known by the profile, protection is granted to traffic routed through the tunnel interface with the IPsec profile applied.

An mGRE tunnel configured to be protected with an IPsec profile negotiates its SAs on demand. The first packets traveling the tunnel are dropped, as the SA is created. Once the SA is established, all subsequent packets use the protected tunnel. In phase 2 DMVPN, the tunnel interface can have multiple destinations, each of which requires a set of SAs for the GRE encapsulated traffic to be protected by IPsec.

When NHRP is configured on the tunnel interface, the spoke knows of one tunnel destination. In order for NHRP registration to occur, a set of SAs must be created so that NHRP can take place over a protected tunnel. These SAs have the tunnel source address and the NHS's mapped address as their selectors. When another tunnel destination becomes necessary, such as in spoke-to-spoke communication, the NHC makes a request to the NHS over these SAs to get the tunnel destination of another subnet in the network. The NHC is then able to use the learned destination address to negotiate a new set of SAs to the destination spoke so that traffic is protected.

A single IPsec profile can be applied to multiple tunnel interfaces because the peer identifying information is configured on the tunnel interface, and not specific to the IPsec profile. When a single profile is applied to multiple tunnel interfaces, support for dual-hub DMVPN architecture is allowed. *Figure 5* describes this type of topology. In this example, a single pair of SAs protects traffic for multiple tunnel interfaces, which may have the same source and destination (this occurs when a spoke-to-spoke tunnel is initiated). Because the tunnels have the same source and destination, traffic over either tunnel can match the same set of SAs. Using an IPsec profile uses the tunnel interface's GRE key to differentiate between the two tunnel pairs.

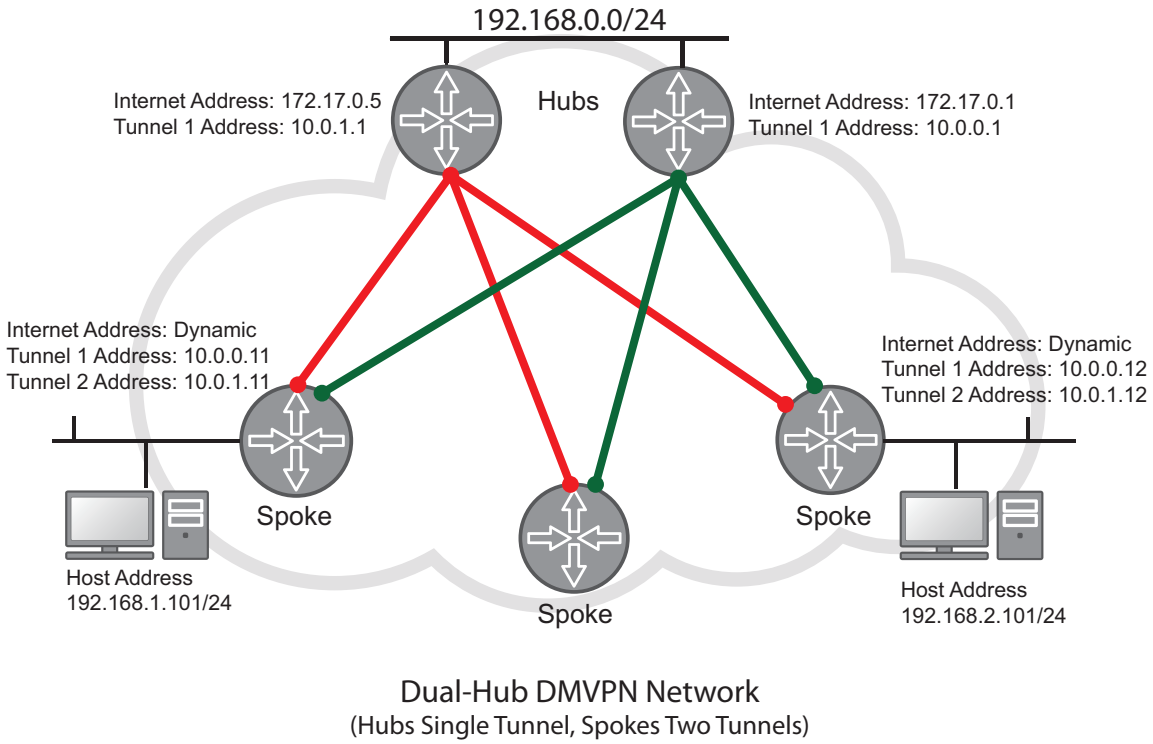

Figure 5. DMVPN Phase 2 Dual-Hub Topology

To configure an IPsec profile, follow these steps:

1. Create the IPsec profile using the **ip crypto ipsec profile** <*name*> command from the Global Configuration mode. This command creates the profile and enters the profile's configuration mode. Use the **no** form of this command to remove the profile from the unit's configuration. To create an IPsec profile, and enter its configuration mode, enter the command as follows:

   (config)**#ip crypto ipsec profile PROFILE1**
   (config-crypto-profile)#

2. Use the **description** <*text*> command to configure a textual description of up to **80** characters for the profile. Use the **no** form of this command to remove the description from the profile's configuration. By default, no description is configured. To create a textual description of the profile, enter the command as follows:

   (config-crypto-profile)**#description SPOKEATOSPOKEB**

3. Use the **ike-policy** <*number*> command to ensure that only a specified Internet key exchange (IKE) policy is used to establish the IPsec tunnel for this profile. This prevents any mobile VPN policies from using IPsec policies that are configured for static VPN peer policies. Use the **no** form of this command to remove a configured policy. The <*number*> parameter specifies the number of the policy to assign to this IPsec profile; valid range is **1** to **10000**. By default, an IKE policy is not assigned to the profile. If no IKE policy is defined in the profile, SA negotiation attempts to use existing IKE policies (starting with the lowest number) until a match is found. If no match is found, negotiation fails. To assign an IKE policy to the IPsec profile, enter the command as follows:

   (config-crypto-policy)**#ike-policy 10**

   
   The IKE policy applied in this command should be previously configured. If an IKE policy is removed, references to that IKE policy in the IPsec profile must be removed manually to prevent an invalid configuration. When this setting is modified, all IPsec SAs created from this IPsec profile are deleted, and delete payloads are sent to the peer(s) so that new IPsec SAs are negotiated using the modified setting.

4. Use the **set security-association idle-time** <*value*> command to set the receive idle timeout in seconds. This is the maximum amount of time for which an SA pair associated with this IPsec profile can be idle. Once the timeout has occurred, the SA pair is removed. Use the **no** form of this command to disable the timeout feature. The <*value*> parameter is the time, in seconds, that the SA pair can be idle. Valid range is **20** to **1209600** seconds. By default, the idle timeout is not specified. To specify an SA idle timeout value, enter the command as follows:

   (config-crypto-policy)**#set security-association idle-time 150000**

   
   When this setting is modified, all IPsec SAs created from this IPsec profile are deleted, and delete payloads are sent to the peer(s) so that new IPsec SAs are negotiated using the modified setting.

5. Use the **set security-association lifetime** <**kilobytes** <*value*> | **seconds** <*value*>> command to define the lifetime (in kilobytes and/or seconds) of the IPsec SAs associated to this IPsec profile. Valid range for kilobytes is **2560** to **536870911** kilobytes, and valid range for seconds is **120** to **1209600** seconds. By default, SA lifetime is set to **28800** seconds. Use the **no** form of this command to return to the default setting. The following example sets the SA lifetime to **300** kilobytes and 2 hours (**7200** seconds) for SAs associated with the IPsec profile:

   (config-crypto-profile)**#set security-association lifetime kilobytes 300**
   (config-crypto-profile)**#set security-association lifetime seconds 7200**

   
   Values can be entered for this command in both kilobytes and seconds. Whichever limit is reached first will end the SA. When this setting is modified, all IPsec SAs created from this IPsec profile are deleted, and delete payloads are sent to the peer(s) so that new IPsec SAs are negotiated using the modified setting.

6. Use the **set pfs** <**group1** | **group2** | **group5**> command to choose the type of perfect forward secrecy (PFS), if any, that will be required during the IPsec negotiation of SAs for this IPsec profile. Specifying **group1** requires IPsec to use Diffie-Hellman Group 1 (768-bit modulus) exchange, specifying **group2** requires IPsec to use Diffie-Hellman Group 2 (1024-bit modulus) exchange, and specifying **group5** requires IPsec to use Diffie-Hellman Group 5 (1536-bit modulus) exchange during IPsec SA key generation. By default, no PFS is used during IPsec SA key generation. If left at the default setting, no PFS will be used during IPsec SA key generation. If PFS is specified, then the specified Diffie-Hellman Group exchange will be used for the initial and all subsequent key generation, thus providing no data link between prior keys and future keys. Use the **no** form of this command to return to the default setting. To configure the PFS for the IPsec profile, enter the command as follows:

   (config-crypto-profile)**#set pfs group1**

   NOTE *When this setting is modified, all IPsec SAs created from this IPsec profile are deleted, and delete payloads are sent to the peer(s) so that new IPsec SAs are negotiated using the modified setting.*

7. Use the **set transform-set** <*name*> command to associate up to six transform sets to the IPsec profile. Separate multiple set names with a space; for example, **set transform-set SET1 SET2 SET3**. By default, no transform set is associated with the IPsec profile. However, transform sets MUST be configured and associated with the profile for it to function. IPsec profiles do not directly contain the transform configuration for securing data. Instead, the profile is associated with transform sets that contain specific security algorithms (set with the command **ip crypto ipsec transform-set** <*name*> <*parameters*>). The parameters defined in one or more of the transform sets' peer(s) must match. Use the **no** form of this command to remove the association between the IPsec profile and the transform set. To associate a transform set with the profile, enter the command as follows:

   (config-crypto-profile)**#set transform-set SET1**

   NOTE *The transform set applied in this command should be previously configured. In addition, the transform set must be defined in the IPsec profile for the profile to function. When this setting is modified, all IPsec SAs created from this IPsec profile are deleted, and delete payloads are sent to the peer(s) so that new IPsec SAs are negotiated using the modified setting.*

8. Use the **rpf-check** command to enable reverse path forward (RPF) checking on the IPsec profile. This check refuses traffic on the tunnel if the tunnel's source and destination indicate the source of the traffic can be reached through a different tunnel or interface. By default, this feature is enabled. Use the **no** form of this command to disable RFP checking on the profile. To disable the feature, enter the command as follows:

   (config-crypto-profile)**#no rpf-check**

   NOTE *When this setting is modified, all IPsec SAs created from this IPsec profile are deleted, and delete payloads are sent to the peer(s) so that new IPsec SAs are negotiated using the modified setting.*

9. Use the **antireplay [**<*value*>**]** command to enable anti-replay sequence number checking for all SAs using this profile. The optional <*value*> parameter specifies the anti-replay window size in bytes. Select from **64**, **128**, **256**, **512**, or **1024** bytes. By default, antireplay is set to **64** bytes. Use the **no** form of this command to disable this feature. To change the anti-replay window size, enter the command as follows:

   (config-crypto-profile)**#antireplay 128**

   > NOTE *When this setting is modified, all IPsec SAs created from this IPsec profile are deleted, and delete payloads are sent to the peer(s) so that new IPsec SAs are negotiated using the modified setting.*

10. Use the **commit-bit** command to set the commit-bit in the Internet Security Association and Key Management Protocol (ISAKMP) header when sending the second message of quick mode on an IPsec tunnel negotiation. This feature verifies that encrypted payloads are not received until an SA is completely established. As an extra security measure, the commit-bit can be set by the responder of a quick mode negotiation to force the initiator to wait for the fourth message of quick mode before bringing up its IPsec SAs. By default, this feature is enabled on all AOS products with VPN capabilities. Use the **no** form of this command to disable this feature. To disable this feature, enter the command as follows:

    (config-crypto-profile)**#no commit-bit**

    > NOTE *When this setting is modified, all IPsec SAs created from this IPsec profile are deleted, and delete payloads are sent to the peer(s) so that new IPsec SAs are negotiated using the modified setting.*

11. Once the IPsec profile settings have been configured, the profile must be applied to the tunnel interface using the **tunnel protection ipsec profile** <*name*> command. The <*name*> parameter is the name of the profile you are applying to the tunnel interface. By default, no IPsec profile is created or associated with the tunnel interface. Use the **no** form of this command to remove the profile from the interface. To associate an IPsec profile with the tunnel interface, enter the command from the tunnel's configuration mode as follows:

    (config)**#interface tunnel 1 multipoint-gre ip**
    (config-tunnel 1)**#tunnel protection ipsec profile PROFILE1**

You have now completed the IPsec profile configuration, applied it to the tunnel interface, and specified the mGRE and NHRP settings for the phase 2 DMVPN network.

DMVPN Component Configuration Examples

The following configuration examples display the NHRP configurations for the AOS router as an NHC and the configuration of a per-host IPsec SA. The configuration parameters entered in these examples are sample configurations only. You should configure these applications in a manner consistent with the needs of your particular network. Command line interface (CLI) prompts have been removed from the configuration examples to provide you with a method of copying and pasting directly from this guide into the CLI. You should make the necessary adjustments to these configurations before adding them to your configuration to ensure they will function properly in your network.

Example 1: DMVPN Router Configuration with OSPF

The following is a sample configuration for a router acting as an NHC with the Open Shortest Path First (OSPF) routing protocol configured. *Figure 6* describes the network topology.

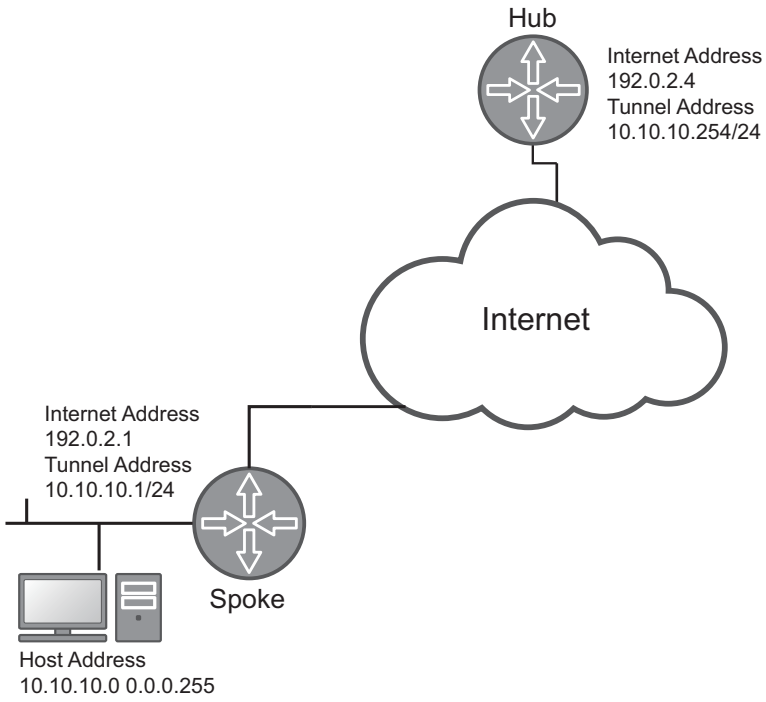

Figure 6. DMVPN Router with OSPF

```
interface tunnel 1 gre ip
    ip address 10.10.10.1 255.255.255.0
    tunnel source 192.0.2.1
    tunnel destination 192.0.2.4
    ip nhrp nhs 10.10.10.254
    ip ospf 1 network broadcast
    ip ospf 1 priority 0
    no shutdown
!
router ospf 1
    network 10.10.10.0 0.0.0.255 area 0
!
```


Example 2: DMVPN Router Configuration with IPsec

In this example, traffic between the private network at the DMVPN spoke and the private network at the DMVPN hub is encapsulated in GRE, and the GRE traffic is protected by IPsec. *Figure 7* describes the network topology. The spoke receives its public IP address on Ethernet 0/1 from the service provider using Dynamic Host Control Protocol (DHCP). The GRE tunnel interface uses this address as the source IP address. The IKE crypto maps are configured in aggressive mode (main mode cannot be used in this application).

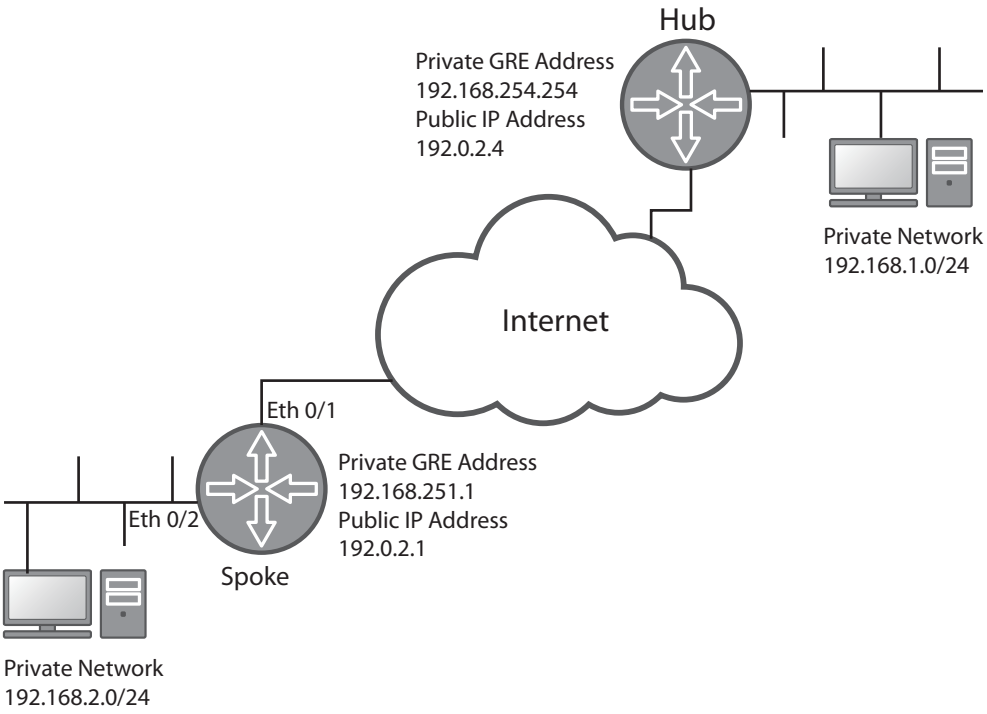

Figure 7. DMVPN with GRE Tunnel over IPsec

The following is sample configuration for the spoke in this example:

```
!
ip crypto
!
crypto ike policy 100
    initiate aggressive
    respond anymode
    local-id fqdn test-spoke.adtran.com
    peer 192.0.2.4
    attribute 10
            encryption aes-256-cbc
            authentication pre-share
!
crypto ike remote-id fqdn test-hub.adtran.com preshared-key MY-PRESHARED-KEY
!
```



```
ip crypto ipsec transform-set ESP-AES-256-SHA-1 esp-aes-256-cbc esp-sha-hmac
    mode tunnel
!
ip crypto map VPN 10 ipsec-ike
    match address ip VPN-10
    set peer 192.0.2.4
    set transform-set ESP-AES-256-SHA-1
    set security-association level per-host
!
ip access-list extend VPN-10
    permit gre any host 192.0.2.4
!
interface ethernet 0/1
    ip address dhcp
    ip crypto map VPN
    no shutdown
!
interface ethernet 0/2
    ip address 192.168.2.254 255.255.255.0
    no shutdown
!
interface tunnel 1 gre ip
    ip address 192.168.254.1 255.255.255.0
    ip nhrp nhs 192.168.254.254
    tunnel source ethernet 0/1
    tunnel destination 192.0.2.4
    no shutdown
!
ip route 192.168.1.0 255.255.255.0 tunnel 1
!
```

Example 3: DMVPN Phase 2 Spoke Configuration with mGRE, OSPF, and IPsec Profile

In this example, a phase 2 DMVPN network spoke is configured to send OSPF traffic over an IPsec-protected mGRE tunnel to the hub. *Figure 8* describes the network topology. Important considerations in this type of configuration include the following:

- mGRE is configured for broadcast mode to facilitate operation with OSPF
- OSPF configuration must not allow spokes to be elected as an OSPF designated router
- NHRP configuration connects the spoke to the hub and causes OSPF traffic to be sent to the hub
- IPsec profile is applied to the mGRE interface instead of a crypto map

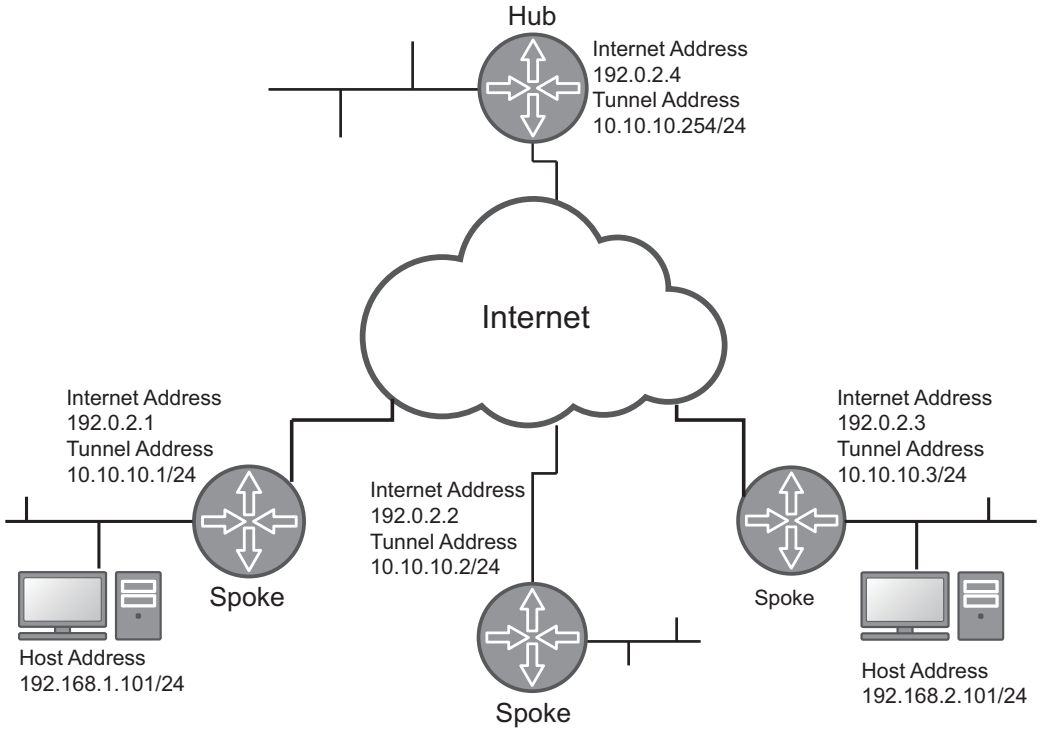

Figure 8. DMVPN Phase 2 Spoke Configuration with mGRE, OSPF, and IPsec Profiles

The following is sample configuration for the spoke in this example:

```
ip crypto
!
crypto ike policy 100
     initiate aggressive
     respond anymode
     local-id fqdn test-spoke.adtran.com
     peer 192.0.2.4
     attribute 10
       encryption aes-256-cbc
       authentication pre-share
!
crypto ike remote-id fqdn test-hub.adtran.com preshared-key MY-PRESHARED-KEY
!
ip crypto ipsec transform-set ESP-AES-256-SHA-1 esp-aes-256-cbc esp-sha-hmac mode tunnel
!
ip crypto ipsec profile VPN
     set transform-set ESP-AES-256-SHA-1
!
!
```



```
interface ethernet 0/1
    description WAN interface
    ip address 192.0.2.1 255.255.255.0
    no shutdown
!
interface vlan 100
    description LAN interface
    ip address 192.168.1.254 255.255.255.0
    no shutdown
!
interface tunnel 1 multipoint-gre ip
    ip address 10.10.10.1 255.255.255.0
    tunnel source eth 0/1
    ip ospf 1 priority 0
    ip nhrp nhs 10.10.10.254
    ip nhrp map 10.10.10.254 192.0.2.4
    ip nhrp map multicast 192.0.2.4
    tunnel protection ipsec profile VPN
    no shutdown
!
router ospf 1
    network 192.168.1.0 0.0.0.255 area 0
    network 10.10.10.0 0.0.0.255 area 0
!
```


DMVPN Configuration Command Summary

The following tables describe the commands used to configure both phase 1 and phase 2 DMVPN in AOS.

Phase 1 DMVPN Configuration Commands

The following table outlines the commands used to configure the tunnel interface on an NHC and to specify a per-host SA used in phase 1 DMVPN configurations.

Table 1. DMVPN Phase 1 Configuration Command Summary

Prompt	Command	Description
(config-tunnel 1)#	**[no] ip nhrp nhs** <*ip address*>	Specifies the private tunnel address on the NHS that the NHC uses for communication with the NHS. Specify IP addresses in dotted decimal notation (**10.10.10.1**). The **no** form of this command removes the address from the tunnel's configuration.
(config-tunnel 1)#	**[no] ip nhrp authentication** <*string*>	Specifies the authentication string used by all routers communicating with NHRP. By default, NHRP authentication is disabled. The <*string*> parameter is a text string of no more than **8** characters. The **no** form of this command disables NHRP authentication.
(config-tunnel 1)#	**[no] ip nhrp holdtime** <*value*>	Specifies how often the router sends NHRP registration requests to the NHS. The <*value*> parameter is the time (in seconds) between requests. Valid range is **1 to 65535** seconds, with a default value of **7200** seconds. The **no** form of this command returns to the default setting.
(config-tunnel 1)#	**[no] ip nhrp registration timeout** <*value*>	Optional. Specifies how often the router sends NHRP registration requests to the NHS independent of the hold time setting. The <*value*> parameter is the time (in seconds) between requests. Valid range is **1** to **65535** seconds. The timeout value must be less than or equal to the hold time value. By default, this option is not configured and registration requests are sent at intervals of one third the value of the hold time. The **no** form of this command returns to the default value.

Table 1. DMVPN Phase 1 Configuration Command Summary *(Continued)*

Prompt	Command	Description
(config-crypto-map)#	**[no] set security-association level per-host**	Enables per-host mode for the SA. When enabled, per-host mode specifies that the source and destination IP addresses of the packet requiring IPsec protection are placed in the VPN selectors used in Quick Mode IPsec SA generation. By default, this feature is disabled. The **no** form of this command disables the feature.

DMVPN Phase 2 Configuration Commands

The following tables outline the configuration commands used to configure the NHC, mGRE tunnel interface, and IPsec profile for use in phase 2 DMVPN networks.

Table 2. mGRE Tunnel Interface Configuration Commands for Phase 2 DMVPN

Prompt	Command	Description
(config)#	**[no] interface tunnel** <*number*> **multipoint-gre ip**	Creates an mGRE tunnel interface. Valid <*number*> range is **1** to **1024**. By default, no mGRE tunnel exists. Use the **no** form of the command to remove the interface.

Table 3. NHC/NHRP Configuration Commands for Phase 2 DMVPN

Prompt	Command	Description
(config-tunnel 1)#	**[no] ip nhrp map** <*destination ipv4 address*> <*nbma address*>	Statically creates an NHRP mapping between the IPv4 address and the NBMA address of the NHS. Use the **no** form of this command to remove the mapping. The IPv4 destination address is the private tunnel address, and the NBMA address is the tunnel's public facing address. IP addresses are expressed in dotted decimal notation; for example, **10.10.10.1**. By default, no mapping exists between the private and public tunnel addresses.

Table 3. NHC/NHRP Configuration Commands for Phase 2 DMVPN

Prompt	Command	Description
(config-tunnel 1)#	**[no] ip nhrp map multicast** *<nbma address>*	Statically adds an NHRP mapping for multicast and broadcast traffic to an NMBA address. The NHS is typically used as the NBMA address. The *<nbma address>* parameter specifies the NBMA address that will receive multicast and broadcast traffic. Express NBMA addresses in dotted decimal notation; for example, **192.168.1.101**. By default, no mapping is configured. Use the **no** form of this command to remove the mapping.
(config-tunnel 1)#	**[no] ip nhrp record**	Specifies whether NHRP requests and replies should include forward and backward record extensions. Use the **no** form of this command to disable the addition of these extensions. By default, these extensions are included in NHRP requests and replies.
(config-tunnel 1)#	**[no] ip nhrp registration non-unique**	Specifies whether the Unique flag is set in the NHRP registration packet. This feature is disabled by default; however, ADTRAN recommends it is enabled on interfaces where the IP address can change. Once enabled, use the **no** form of the command to disable the feature.

Table 4. IPsec Profile Configuration Commands for Phase 2 DMVPN

Prompt	Command	Description
(config)#	**[no] ip crypto ipsec profile** *<name>*	Creates an IPsec profile and enters the profile's configuration mode. By default, no IPsec profile is configured. Use the **no** form of this command to remove the profile.
(config-crypto-profile)#	**[no] description** *<text>*	Specifies a textual description of up to 80 characters for the profile. By default, no description exists. Use the **no** form of this command to remove the description.

Table 4. IPsec Profile Configuration Commands for Phase 2 DMVPN

Prompt	Command	Description
(config-crypto-profile)#	**[no] ike-policy** <*number*>	Ensures that only a specified IKE policy is used to establish the IPsec tunnel for this profile. The <*number*> parameter specifies the policy number of the IKE policy to assign to this IPsec profile; valid range is **1** to **10000**. By default, no IKE policy is associated with the profile. Use the **no** form of the command to remove the policy from the profile configuration.
(config-crypto-profile)#	**[no] set security-association idle-time** <*value*>	Sets the receive idle timeout in seconds. This is the maximum amount of time for which an SA pair associated with this IPsec profile can be idle. Valid range is **20** to **1209600** seconds. The idle time is not set by default. Use the **no** form of this command to disable the feature.
(config-crypto-profile)#	**[no] set security-association lifetime** <**kilobytes** <*kilobytes* | **seconds** <*seconds*>>	Defines the lifetime (in kilobytes and/or seconds) of the IPsec SAs associated to this IPsec profile. Valid range for kilobytes is **2560** to **536870911** kilobytes, and valid range for seconds is **120** to **1209600** seconds. By default, SA lifetime is set to **28800** seconds. Use the **no** form of this command to return to the default setting.
(config-crypto-profile)#	**[no] set pfs** <**group1** | **group2** | **group5**>	Specifies the type of PFS, if any, that will be required during the IPsec negotiation of SAs for this IPsec profile. By default, no PFS is used during IPsec SA key generation. Use the **no** form of this command to disable PFS for the profile.
(config-crypto-profile)#	**[no] set transform-set** <*name*>	Associates up to six transform sets to the IPsec profile. Separate multiple set names with a space; for example, **set transform-set SET1 SET2 SET3**. By default, no transform set is associated with the IPsec profile. However, transform sets MUST be configured and associated with the profile for it to function. Use the **no** form of this command to remove the set from the profile.

Table 4. IPsec Profile Configuration Commands for Phase 2 DMVPN

Prompt	Command	Description
(config-crypto-profile)#	**[no] rpf-check**	Enables RPF checking on the IPsec profile. This check refuses traffic on the tunnel if the tunnel's source and destination indicate the source of the traffic can be reached through a different tunnel or interface. By default, this feature is enabled. Use the **no** form of this command to disable RFP checking on the profile.
(config-crypto-profile)#	**[no] antireplay [**<*value*>**]**	Enables anti-replay sequence number checking for all SAs using this profile. The optional <*value*> parameter specifies the anti-replay window size in bytes. Select from **64**,**128**, **256**, **512**, or **1024** bytes. By default, antireplay is set to **64** bytes. Use the **no** form of this command to disable this feature.
(config-crypto-profile)#	**[no] commit-bit**	Sets the commit-bit in the ISAKMP header when sending the second message of quick mode on an IPsec tunnel negotiation.By default, this feature is enabled on all AOS products with VPN capabilities. Use the **no** form of this command to disable this feature.
(config-tunnel 1)#	**[no] tunnel protection ipsec profile** <*name*>	Assigns the specified IPsec profile to the tunnel interface. By default, no IPsec profile is created or associated with the tunnel interface. Use the **no** form of this command to remove the profile from the interface.

Troubleshooting

Troubleshooting the configuration of DMVPN can be done by using various **clear**, **show**, and **debug** commands from the CLI. All commands are entered from the Enable mode prompt.

Clear Commands

Use the **clear counters tunnel** <*number*> command to clear the NHRP counters for the specified tunnel interface. The <*number*> parameter is the tunnel interface number. To clear the NHRP counters on tunnel interface **1**, enter the command as follows:

```
>enable
#clear counters tunnel 1
```

Use the **clear ip nhrp [**<*destination ipv4 address*> **| tunnel** <*number*>**]** command to clear all NHRP cache entries. The optional <*destination ipv4 address*> parameter specifies that only cache entries matching this address are cleared. Express IPv4 addresses in dotted decimal notation; for example, **10.10.10.1**. The optional **tunnel** <*number*> parameter specifies that only cache entries matching the GRE multipoint tunnel interface number are cleared. Valid range is **1** to **1024**. To clear all NHRP cache entries, enter the command as follows:

```
>enable
#clear ip nhrp
```

Use the **clear ip crypto ipsec sa profile** <*name*> command to clear the SAs created in association with the specified IPsec profile name. To clear the SAs for IPsec profile **PROFILE1**, enter the command as follows:

```
>enable
#clear ip crypto ipsec sa profile PROFILE1
```

Show Commands

Various **show** commands can be used to show the configuration information for NHRP and IPsec SAs. These commands are outlined in the following section.

Use the **show ip nhrp [interface tunnel** <*number*>**] traffic** command to display the NHRP traffic for all tunnel interfaces. To limit the output to a single interface, optionally enter the **interface tunnel** <*number*> parameter, where <*number*> is the tunnel interface number. To view the NHRP traffic statistics on a single tunnel interface, enter the command as follows:

```
>enable
#show ip nhrp interface tunnel 1 traffic
Interface tunnel 1:
    Sent: 1234567890 Total
            1234567890 Resolution Requests Resolution Replies:
            1234567890 Total, 1234567890 Acknowledged,
            1234567890 Prohibited, 1234567890 Insufficient Resources,
            1234567890 No Binding, 1234567890 Not Unique
            1234567890 Registration Requests Registration Replies:
            1234567890 Total, 1234567890 Acknowledged,
            1234567890 Prohibited, 1234567890 Insufficient Resources,
```



```
        1234567890 Already Registered
        1234567890 Purge Requests
        1234567890 Purge Replies Error Indications:
        1234567890 Total, 1234567890 Unrecognized Extension,
        1234567890 Loop Detected, 1234567890 Protocol Address Unreachable,
        1234567890 Protocol Error, 1234567890 SDU Size Exceeded,
        1234567890 Invalid Extension, 1234567890 Authentication Failure,
        1234567890 Hop Count Exceeded

    Received: 1234567890 Total
        1234567890 Resolution Requests Resolution Replies:
        1234567890 Total, 1234567890 Acknowledged,
        1234567890 Prohibited, 1234567890 Insufficient Resources,
        1234567890 No Binding, 1234567890 Not Unique
        1234567890 Registration Requests
        Registration Replies:
            1234567890 Total, 1234567890 Acknowledged,
            1234567890 Prohibited, 1234567890 Insufficient Resources,
            1234567890 Already Registered
            1234567890 Purge Requests
            1234567890 Purge Replies
        Error Indications:
            1234567890 Total, 1234567890 Unrecognized Extension,
            1234567890 Loop Detected, 1234567890 Protocol Address Unreachable,
            1234567890 Protocol Error, 1234567890 SDU Size Exceeded,
            1234567890 Invalid Extension, 1234567890 Authentication Failure,
            1234567890 Hop Count Exceeded
```

Use the **show ip nhrp [interface tunnel** <*number*>**] nhs** command to display a list of NHS servers and their statuses for each NHRP interface. You can optionally specify that only entries for a single tunnel interface are displayed using the **interface tunnel** <*number*> parameter, where <*number*> is the tunnel interface number. To display NHS servers and their statuses for all configured tunnel interfaces, enter the command as follows:

```
>enable
#show ip nhrp nhs
INTERFACE                NHS              STATUS
tunnel 4                 1.1.1.2          UP
tunnel 5                 5.5.5.5          DOWN
```

Use the **show ip nhrp [interface tunnel** <*number*>**] [**<*ip address*>**] [brief]** command to display NHRP cache entries. The optional **interface tunnel** <*number*> parameter limits entries to only those that correspond to the specified interface. The optional <*ip address*> parameter limits entries to those with the specified private tunnel IP address. The optional **brief** keyword shortens the output for each entry to fit on a single line. To display all NHRP cache entries, enter the command as follows:

```
>enable
#show ip nhrp
```



```
Interface tunnel 1:
    Protocol address: 10.10.10.1/32,
    Type: static, Flags: unique,
    NBMA Address: 1.1.1.1
    Created: 33:44:55, Expires: Never
```

Use the **show ip crypto map [**<*name*>**] [**<*number*>**]** command to display the IPsec SA configuration information. You can optionally limit the output to information about a single crypto map using the <*name*> and <*number*> parameters. To display the IPsec SA information for the crypto map **VPN 10**, enter the command as follows:

```
>enable
#show ip crypto map VPN 10
Crypto Map “VPN” 10 ipsec-ike
    Extended IP access list VPN-10
    Peers:
        10.10.10.2
    Transform sets:
        ESP-AES-256-SHA-1
    Security-association lifetimes:
        0 kilobytes
        28800 seconds
    No PFS group configured
    Anti-replay checking enabled, window size: 64
    Commit bit in use
    Idle Timeout: disabled
    Per-host selector negotiation: enabled
    Reverse Route Inject disabled
    Interfaces using crypto map VPN:
        eth 0/1.3158
```

Use the **show ip crypto ipsec sa profile** <*name*> command to display all IPsec SAs associated with the specified IPsec profile. Enter the command as follows to display the SAs associated with **PROFILE1**:

```
>enable
#show ip crypto ipsec sa profile PROFILE1
```

Debug Commands

You can use the **debug ip nhrp [events | packet]** command to enable debug messages for NHRP. Optionally view only event messages by entering the **event** keyword, or view only packet information by entering the **packet** keyword. To view debug messages for NHRP configuration, enter the command as follows:

```
>enable
#debug ip nhrp
18:21:32 NHRP tunnel 1: No reply for registration request to 10.10.10.254 after 16s, resending
18:21:33 NHRP tunnel 1: Error indication received from 10.10.10.254
```


Additional Resources

The following table outlines additional resources you may find useful in configuring the various aspects of DMVPN.

Table 5. Additional Resources for DMVPN Configuration

Subject	Resource
NHRP	*RFC 2332*
GRE	*Configuring GRE in AOS*
IPsec	*Configuring GRE over an IPsec VPN Tunnel in AOS*
VPN	*Configuring VPN Using Aggressive Mode in AOS*