



CHAPTER 10

Home Agent Security

Security

This chapter discusses the concepts that comprise the Security features in Cisco IOS Mobile Wireless Home Agent software.

This chapter includes the following sections:

- [3 DES Encryption, page 10-1](#)
- [Mobile IP IPSec, page 10-2](#)
- [IPSec Support on Catalyst 6500/7600 with 5 CPUs of MWAM, page 10-6](#)
- [Restrictions, page 10-7](#)
- [Configuration Examples, page 10-9](#)

3 DES Encryption

The Cisco Home Agent includes 3DES encryption, which supports IPSec on the HA. To accomplish this on the Cisco 7200 Internet router platform, Cisco supplies an SA-ISA card for hardware provided IPsec. On the Cisco 7600 and Cisco 6500 Catalyst switch platforms, the MWAM utilizes the Cisco IPSec Acceleration Card.

The HA requires you to configure the parameters for each PDSN before a mobile IP data traffic tunnel is established between the PDSN and the HA.



Note

This feature is only available with hardware support.

Mobile IP IPSec

The Internet Engineering Task Force (IETF) has developed a framework of open standards called IP Security (IPSec) that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer; it uses Internet Key Exchange (IKE) to handle negotiation of protocols and algorithms based on local policy, and to generate the encryption and authentication keys to be used by IPSec. IPSec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host.

The HA uses any statically configured shared secret(s) when processing authentication extension(s) present in mobile IP registration messages.

The HA supports IPSec, IKE, Authentication Header (AH) and IP Encapsulating Security Payload (ESP) as required in IS-835-B.

IS835-B specifies three mechanisms for providing IPSec security:

- Certificates
- Dynamically distributed pre-shared secret
- Statically configured pre-shared secret.



Note

IS835B Static IPSec feature is available only on the Cisco 7200 Internet router platform. The Cisco IOS IPSec feature is available on the Cisco 7200 Internet router, Cisco 6500 Catalyst switch, and Cisco 7600 switch platforms. The HA 2.0 (and above) Release only supports statically configured, pre-shared secret for IPSec IKE.

As per IS-835-B, The HA and AAA should be configured with same security level for a PDSN. The PDSN receives a security level from AAA server and initiates IKE, and the HA responds to the IKE request for establishing security policy.

The PDSN receives a security level from the AAA server and initiates IKE, and the HA responds to the IKE request for establishing a security policy. All traffic specified by the access-list of the crypto configuration is protected by the IPSec tunnel. The access-list is configured to protect all traffic between the PDSN and HA, and all bindings belonging to a given PDSN-HA pair are protected.

IPSec is not applicable to mobiles using Co-located COA



Note

Cisco Mobile Wireless Home Agent Release 2.0 (and above) on the Cisco 7600 and Cisco 6500 Catalyst platforms requires the support of the Cisco IPSec Services Module (VPNSM), a blade that runs on the Catalyst 6500 or 7600 router. VPNSM does not have any physical WAN or LAN interfaces, and utilizes VLAN selectors for its VPN policy.

For more information on Catalyst 6500 Security Modules visit <http://www.cisco.com/en/US/products/hw/switches/ps708/index.html>.

For more information on the Cisco 7600 Internet Router visit <http://www.cisco.com/en/US/products/hw/routers/ps368/index.html>.

IPSec-based security may be applied on tunnels between the PDSN and the HA depending on parameters received from the Home AAA server. A single tunnel may be established between each PDSN-HA pair. It is possible for a single tunnel between the PDSN-HA pair to have three types of traffic streams: Control Messages, Data with IP-in-IP encapsulation, and Data with GRE-in-IP encapsulation. All traffic carried in the tunnel has the same level of protection provided by IPSec.

IS835 defines MobileIP service as described in RFC 2002; the Cisco Mobile Wireless HA provides Mobile IP service and Proxy Mobile IP service.

In Proxy Mobile service, the Mobile-Node is connected to the PDSN/FA through Simple IP, and the PDSN/FA acts as Mobile IP Proxy for the MN to the HA.

Once Security Associations (SAs or tunnels) are established, they remain active until there is traffic on the tunnel, or the lifetime of the SAs expire.

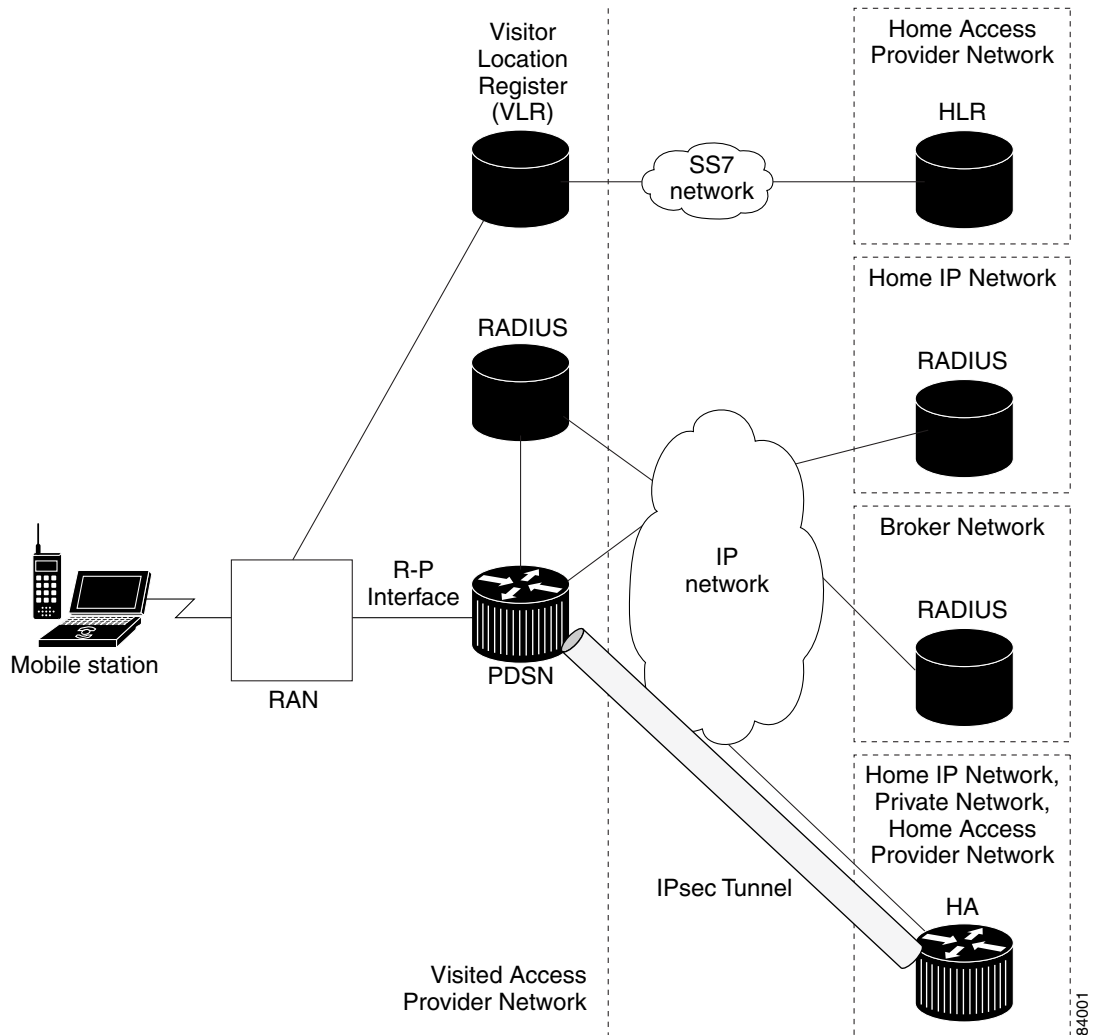


Note

IPSec does not work with HA redundancy, since the IPSec security associations are not replicated to the standby during failover.

Figure 10-1 illustrates the IS835 IPSec network topology.

Figure 10-1 IS835 IPSec Network



84001

IPSec Interoperability Between the PDSN and HA (IS-835-C)

IPSec rules under IS-835C mandates that connections are always initiated from the PDSN to the Home Agent IP address. Certain PDSNs may not be flexible in their approach to IPSec configuration. These PDSNs do not allow any configuration for Remote IPSec termination points, and expect that the remote IPSec termination point is always the Home Agent IP address.

The following section illustrates how to handle IPSec Interoperability between such PDSNs and the HA with Home Agent.

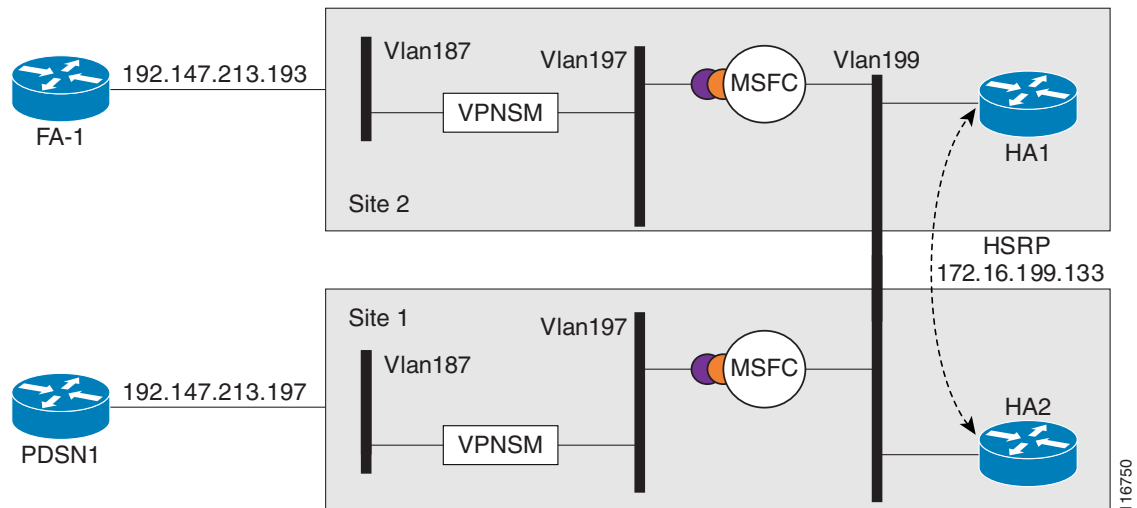
The change in the configuration allows for IPSec connections for the Home Agent IP address that are still terminated by the VPNISM.

Handling Single Home Agent Instance

This solution is achieved by letting SUP IOS own the same Home Agent IP address. Traffic to the Home Agent is then policy routed to the correct Home Agent.

Figure 10-2 illustrates a possible configuration:

Figure 10-2 Single HA Interoperability



Here is a sample configuration for the Supervisor. The PDSN IP Address is 14.0.0.1, HA3 address is 13.0.0.50, and HA4 is 13.0.0.51

Single HA Instance - Interoperability

```
crypto isakmp policy 1
  hash md5
  authentication pre-share
  lifetime 60000
crypto isakmp key cisco address 10.0.0.0 0.0.0.0
!
crypto ipsec transform-set mobile-set1 esp-3des

# Comment: testmap is used for HA3

crypto map testmap local-address Loopback21
crypto map testmap 20 ipsec-isakmp
  set peer 10.0.0.1
```

```
set transform-set mobile-set1
match address 131
!

interface Loopback21
description corresponds to ha-on-proc3
ip address 10.0.0.50 255.255.255.255
!

interface GigabitEthernet4/1
description encrypt traffic from vlan 151 to vlan 201& 136 to 139
no ip address
flowcontrol receive on
flowcontrol send off
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,136,146,151,1002-1005
switchport mode trunk
cdp enable
!
interface GigabitEthernet4/2
description decrypts traffic from vlan 201 to 151, 139 to 136
no ip address
flowcontrol receive on
flowcontrol send off
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 1,139,149,201,1002-1005
switchport mode trunk
cdp enable

interface Vlan136
description secure vlan
ip address 10.0.0.1 255.255.255.0
no ip redirects
no ip unreachableables
ip policy route-map RRQ-HA3
no mop enabled
crypto map testmap
!
interface Vlan137
description internal vlan to HA3
ip address 10.0.0.1 255.255.0.0
!
interface Vlan139
no ip address
crypto connect vlan 136
!

access-list 131 permit ip host 10.0.0.1 host 10.0.0.50
access-list 131 permit ip host 10.0.0.50 host 10.0.0.1
access-list 131 permit ip 10.0.0.0 0.0.0.255 10.0.0.0 0.0.0.255

access-list 2000 permit udp any any eq mobile-ip
access-list 2000 permit ipinip any any

route-map RRQ-HA3 permit 10
match ip address 2000
set ip next-hop 10.0.0.2
!
```

IPSec Support on Catalyst 6500/7600 with 5 CPUs of MWAM

You may require an IPSec tunnel be established over the mobile IP tunnel between the PDSN and the HA. The PDSN resides in the foreign network and the HA in the home network. As per IS-835B specification, IPSec connections are always initiated from the PDSN towards the HA, so the IPSec tunnel endpoints are the PDSN IP address and the HA IP address.

In Cisco's 6500 Catalyst and 7600 HA solution, IPSec is terminated at the Supervisor (SUP), while the actual HA application resides on the MWAM card(s). Each MWAM card has 5 CPUs, each running one HA instance. Each HA has its own IP address. If different IP addresses are used in the SUP as IPSec endpoints, and in the MWAM for HA endpoints, IKE messages generated from the PDSN with HA IP addresses are dropped at the SUP.

To avoid this issue, the above requirement is achieved by letting the SUP own the same IP address that is configured as the HA IP address on the MWAM. The requirement is to split the IPSec traffic for different HA IP addresses across separate IPSec VLANs so that each PDSN-HA pair is handled appropriately. This configuration allows the SUP to support all 5 CPUs on the MWAM card running the HA application, each owning an IP address that is the IPSec endpoint.

In this case, the VRF IPSec feature on the SUP720 is used. All traffic coming from the PDSN is put on different VLANs based on the HA IP address. Each VLAN corresponds to one VRF and one VRF exists per HA instance on the SUP. In this situation, the VRF mode of IPSec is used to split traffic between the 5 different HA instances present on the MWAM. Once the packets are decrypted by the crypto VLAN, packets are then policy routed using an internal VLAN that corresponds to the particular HA to the correct HA CPU on the MWAM.

IPSec redundancy across chassis and within a single chassis is supported for this environment.

The following call flow describes this behavior:

1. An IPSec security association (SA) is opened between each PDSN and HA IP address pair on the SUP. IKE messages are sent from the PDSN with its IP address and peer IP address as the particular HA IP address. Based on the PDSN IP address and the HA IP address in the IKE message, the correct ISAKMP profile is selected for the PDSN-HA pair that indicates the VRF for the pair. This establishes different SPIs corresponding to the PDSN-HA pair.
 2. One VLAN per HA IP address is defined, and it belongs to a VRF that is defined for that IP address on the SUP. Thus, the SUP owns the HA IP address, and it is the IPSec terminating point for PDSN.
 3. Once an IPSec SA is established between each PDSN-HA IP address pair, encrypted packets are put on to the correct VRF based on the SPI of the incoming packet.
 4. Once the encrypted packets are decrypted at the IPSec VLAN corresponding to the HA address, the packets are policy routed to the corresponding CPU on the MWAM card that hosts the HA IP address (using the internal VLAN present between SUP and the HA instance on the MWAM).
 5. In the return path, packets from HA instances on the MWAM are placed on the internal VLAN and put on to the corresponding IPSec VLAN for the HA. This enables the packet to be encrypted and sent out to the PDSN using the outgoing interface.
-

Restrictions

Simultaneous Bindings

The Cisco Home Agent does not support simultaneous bindings. When multiple flows are established for the same NAI, a different IP address is assigned to each flow. This means that simultaneous binding is not required, because it is used to maintain more than one flow to the same IP address.

Security

The HA supports IPSec, IKE, IPSec Authentication Header (AH) and IP Encapsulating Security Payload (ESP) as required in IS-835-B. The Home Agent does not support security for control or user traffic independently. Either both are secured, or neither.

The Home Agent does not support dynamically assigned keys or shared secrets as defined in IS-835-B.

Configuring Mobile IP Security Associations

To configure security associations for mobile hosts, FAs, and HAs, use one of the following commands in global configuration mode:

	Command	Purpose
Step 1	<pre>Router(config)# ip mobile secure {host visitor home-agent foreign-agent proxy-host} {lower-address [upper-address] nai string} {inbound-spi spi-in outbound-spi spi-out spi spi} key {hex ascii} string [replay timestamp [number] algorithm md5 mode prefix-suffix]</pre>	Specifies the security associations for IP mobile users.

Configuring IPsec for the HA

To configure IPsec for the HA, use the following commands in global configuration mode:

	Command	Purpose
Step 1	<pre>Router(config)# crypto map map-name seq-num ipsec-isakmp set peer ip address of ha set transform-set transform-set-name match address acl name crypto map map name local-address interface</pre>	<p>Creates a a crypto map entry for one HA in one Crypto-map set.</p> <p>The Crypto Map definition is not complete until:</p> <ol style="list-style-type: none"> 1. ACL associated with it is defined, and 2. The Crypto-Map is applied on the interface. You can configure Crypto MAP for different HAs by using a different sequence number for each HA in one crypto-map set. <p>Specifies and names an identifying interface to be used by the crypto map for IPsec traffic.</p>
Step 2	<pre>Router# access-list acl-name deny udp host HA IP addr eq mobile-ip host PDSN IP addr eq mobile-ip access-list acl-name permit ip host PDSN IP addr host HA IP addr access-list acl-name deny ip any any</pre>	<p>Defines the access list.</p> <p>The ACL name “acl-name” is same as in the crypto-map configuration.</p>
Step 3	<pre>Router# Interface Physical-Interface of PI interface crypto map Crypto-Map set</pre>	<p>Applies the Crypto-Map on Pi Interface, as the HA sends/receives Mobile IP traffic to/from PDSN on this interface.</p>

Creating Active Standby Home Agent Security Associations

The following IOS command displays active standby Home Agent security associations:

	Command	Purpose
Step 1	<pre>Router(config)#show ip mobile secure ? foreign-agent home-agent host summary</pre>	<p>Displays the active and standby Home Agent Security associations.</p> <p>Displays Foreign agent security associations.</p> <p>Displays Home agent security associations. Displays Mobile host security associations. Displays a summary of security associations.</p>

Here is an example of the command:

```
Router# show ip mobile secure home-agent
Security Associations (algorithm,mode,replay protection,key):
30.0.0.30:
  SPI 100, MD5, Prefix-suffix, Timestamp +/- 7,
  Key 'red'
HA#
```

Configuration Examples

Home Agent IPsec Configuration


Note

Once you permit the hosts/subnets you want encrypted, ensure that you put in an explicit deny statement. The deny statement states do not encrypt any other packets.


Note

The following example is for IPsec on the Cisco 7200 router only. IPsec on the Cisco Catalyst 6500 and the 7600 is configured on the Supervisor, rather than on the Home Agent.

```

access-list 101 deny ip any any
access-list 103 deny ip any any

-----

!
! No configuration change since last restart
!
version 12.2
service timestamps debug datetime
service timestamps log datetime
service password-encryption
!
hostname 7206f1
!
aaa new-model
!
!
aaa authentication login CONSOLE none
aaa authentication login NO_AUTHENT none
aaa authentication ppp default group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa session-id common
enable password 7 151E0A0E
!
username xxx privilege 15 nopassword
ip subnet-zero
ip cef
!
!
no ip domain-lookup
!
!
crypto isakmp policy 1
 authentication pre-share
crypto isakmp key cisco address 10.1.1.4
crypto isakmp key cisco address 172.16.60.30
!
!
crypto ipsec transform-set esp-des-sha-transport esp-des esp-sha-hmac
 mode transport
!
crypto map tosim 10 ipsec-isakmp

```

```

set peer 10.1.1.4
set transform-set esp-des-sha-transport
match address 101
!
crypto map tosim3 10 ipsec-isakmp
set peer 172.16.60.30
set transform-set esp-des-sha-transport
match address 103
!
!
interface Loopback0
ip address 10.0.0.1 255.0.0.0
!
interface Loopback1
ip address 10.0.0.9 255.0.0.0
!
interface Loopback10
ip address 10.1.1.1 255.255.255.0
!
interface FastEthernet0/0
ip address 10.1.1.9 255.255.255.0
load-interval 30
duplex full
speed 100
crypto map tosim
!
interface FastEthernet0/1
ip address 10.1.1.1 255.0.0.0
load-interval 30
duplex full
speed 100
!
interface FastEthernet1/0
ip address 10.1.1.9 255.255.255.0
load-interval 30
duplex full
!
interface FastEthernet2/0
ip address 172.16.60.10 255.255.255.0
load-interval 30
duplex full
crypto map tosim3
!
router mobile
!
ip local pool ispabc-pool1 10.0.0.2 12.1.0.1
ip local pool ispabc-pool1 10.1.0.8 12.2.0.1
ip local pool ispxyz-pool1 10.0.0.2 9.1.0.1
ip local pool ispxyz-pool1 10.1.0.8 9.2.0.1
ip classless
ip route 172.16.49.48 255.255.255.255 172.16.60.1
no ip http server
ip pim bidir-enable
ip mobile home-agent address 10.1.1.1
ip mobile host nai @ispabc.com address pool local ispabc-pool1 virtual-network 10.0.0.0
255.0.0.0 aaa load-sa lifetime 65535
ip mobile host nai @ispxyz.com address pool local ispxyz-pool1 virtual-network 10.0.0.9
255.0.0.0 aaa load-sa lifetime 65535
!
!
access-list 101 permit ip host 10.1.1.1 host 1.1.1.4
access-list 101 deny ip any any
access-list 103 permit ip host 10.1.1.1 host 172.16.60.30
access-list 103 deny ip any any

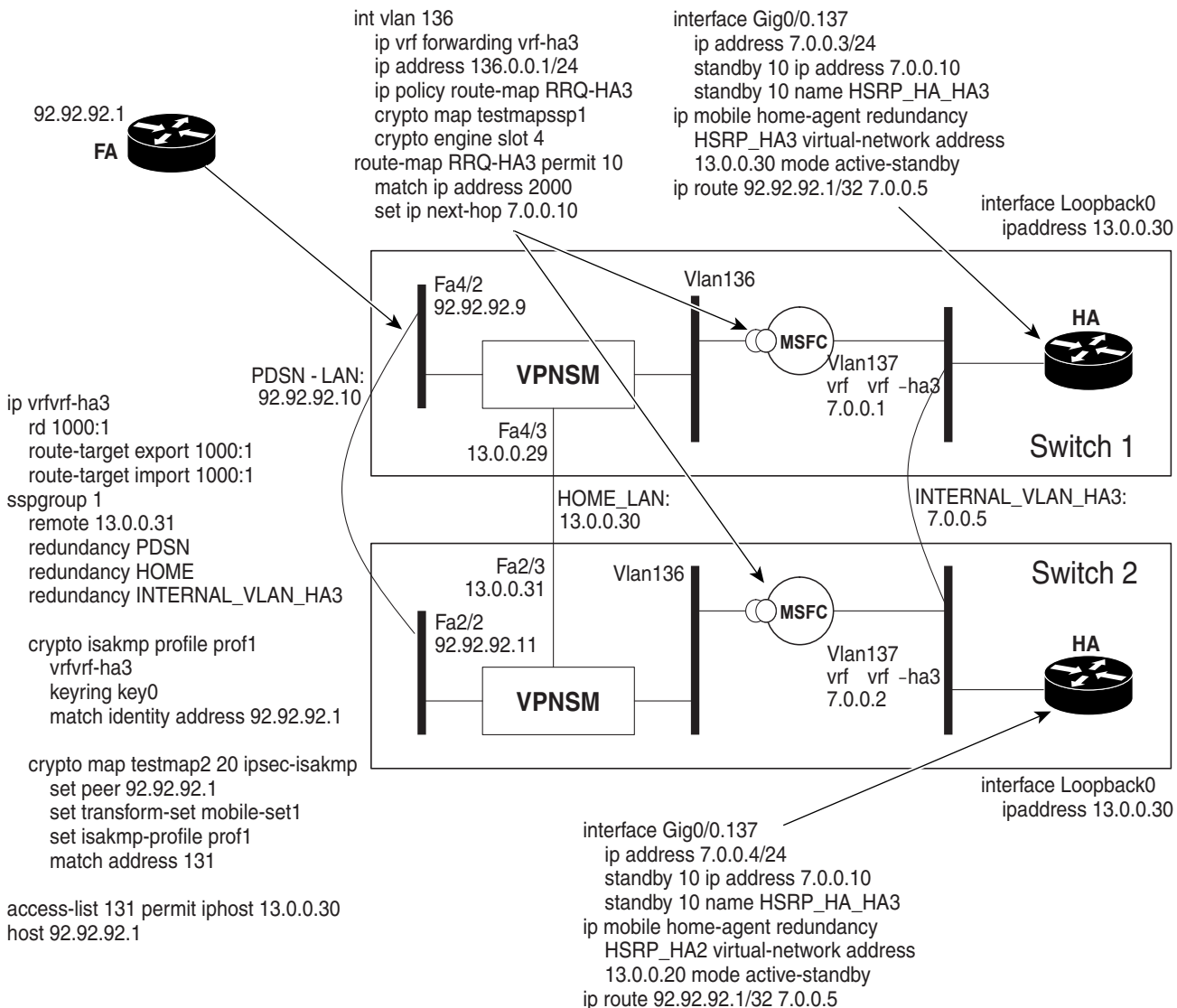
```

```
!  
!  
radius-server host 172.16.49.48 auth-port 1645 acct-port 1646 key 7 094F471A1A0A  
radius-server retransmit 3  
radius-server key 7 02050D480809  
call rsvp-sync  
!  
!  
mgcp profile default  
!  
dial-peer cor custom  
!  
!  
gatekeeper  
  shutdown  
!  
!  
line con 0  
  exec-timeout 0 0  
line aux 0  
line vty 0 4  
  exec-timeout 0 0  
!  
exception protocol ftp  
exception dump 64.102.16.25  
exception memory minimum 1000000  
ntp clock-period 17179878  
ntp server 172.16.60.1  
!  
end
```

Configuration - SUP720 / VRF-IPSec for 5 HA Instances

The following example provides detail of the SUP720 / VRF-IPSec configuration, as illustrated in Figure 10-3.

Figure 10-3 SUP720 / VRF-IPSec Configuration



1411654

SUP Configuration - Switch 1:

```
ip vrf vrf-ha2
 rd 2000:1
 route-target export 2000:1
 route-target import 2000:1
!
ip vrf vrf-ha3
 rd 1000:1
 route-target export 1000:1
 route-target import 1000:1
!
ip vrf vrf-ha4
 rd 4000:1
 route-target export 4000:1
 route-target import 4000:1
!
ip vrf vrf-ha5
 rd 5000:1
 route-target export 5000:1
 route-target import 5000:1
!
ip vrf vrf-ha6
 rd 6000:1
 route-target export 6000:1
 route-target import 6000:1
!
ssp group 1
 remote 13.0.0.31
 redundancy PDSN-LAN
 redundancy HOME-LAN
 redundancy INTERNAL_VLAN_HA3
 redundancy HOME-LAN-2
 redundancy INTERNAL_VLAN_HA2
 redundancy HOME-LAN-4
 redundancy HOME-LAN-5
 redundancy HOME-LAN-6
 redundancy INTERNAL_VLAN_HA4
 redundancy INTERNAL_VLAN_HA5
 redundancy INTERNAL_VLAN_HA6
 port 4098
!
crypto keyring key0
 pre-shared-key address 92.92.92.1 key cisco
!
crypto isakmp policy 1
 authentication pre-share
 lifetime 60000
crypto isakmp ssp 1
!
crypto isakmp profile prof1
 vrf vrf-ha2
 keyring key0
 match identity address 92.92.92.1 255.255.255.255
 local-address 12.0.0.30
crypto isakmp profile prof2
 vrf vrf-ha3
 keyring key0
 match identity address 92.92.92.1 255.255.255.255
 local-address 13.0.0.30
crypto isakmp profile prof4
 vrf vrf-ha4
```

```

    keyring key0
    match identity address 92.92.92.1 255.255.255.255
    local-address 14.0.0.30
crypto isakmp profile prof5
    vrf vrf-ha5
    keyring key0
    match identity address 92.92.92.1 255.255.255.255
    local-address 15.0.0.30
crypto isakmp profile prof6
    vrf vrf-ha6
    keyring key0
    match identity address 92.92.92.1 255.255.255.255
    local-address 16.0.0.30
!
crypto ipsec transform-set mobile-set1 esp-des esp-sha-hmac
!
crypto map testmap local-address FastEthernet4/3
crypto map testmap 20 ipsec-isakmp
    set peer 92.92.92.1
    set transform-set mobile-set1
    set isakmp-profile prof2
    match address 131
!
crypto map testmap1 local-address FastEthernet4/4
crypto map testmap1 20 ipsec-isakmp
    set peer 92.92.92.1
    set transform-set mobile-set1
    set isakmp-profile prof1
    match address 121
!
crypto map testmap4 local-address FastEthernet4/7
crypto map testmap4 20 ipsec-isakmp
    set peer 92.92.92.1
    set transform-set mobile-set1
    set isakmp-profile prof4
    match address 141
!
crypto map testmap5 local-address FastEthernet4/9
crypto map testmap5 20 ipsec-isakmp
    set peer 92.92.92.1
    set transform-set mobile-set1
    set isakmp-profile prof5
    match address 151
!
crypto map testmap6 local-address FastEthernet4/11
crypto map testmap6 20 ipsec-isakmp
    set peer 92.92.92.1
    set transform-set mobile-set1
    set isakmp-profile prof6
    match address 161
!
crypto engine mode vrf
!
interface FastEthernet4/2
ip address 92.92.92.9 255.255.0.0
ip policy route-map RRQ-HA10
speed 100
duplex half
standby delay minimum 30 reload 60
standby 1 ip 92.92.92.10
standby 1 preempt
standby 1 name PDSN-LAN
standby 1 track FastEthernet4/2
standby 1 track FastEthernet4/3

```

```
standby 1 track FastEthernet4/4
standby 1 track FastEthernet4/7
standby 1 track FastEthernet4/9
standby 1 track FastEthernet4/11
standby 1 track GigabitEthernet6/1
standby 1 track Vlan136
standby 1 track Vlan137
standby 1 track Vlan127
standby 1 track Vlan126
standby 1 track Vlan146
standby 1 track Vlan147
standby 1 track Vlan156
standby 1 track Vlan157
standby 1 track Vlan166
standby 1 track Vlan167
standby 1 track Vlan200
crypto engine slot 6
!
interface FastEthernet4/3
ip address 13.0.0.29 255.255.0.0
standby delay minimum 30 reload 60
standby 3 ip 13.0.0.30
standby 3 preempt
standby 3 name HOME-LAN
standby 3 track FastEthernet4/2
standby 3 track FastEthernet4/3
standby 3 track FastEthernet4/4
standby 3 track FastEthernet4/7
standby 3 track FastEthernet4/9
standby 3 track FastEthernet4/11
standby 3 track GigabitEthernet6/1
standby 3 track Vlan136
standby 3 track Vlan137
standby 3 track Vlan127
standby 3 track Vlan126
standby 3 track Vlan146
standby 3 track Vlan147
standby 3 track Vlan156
standby 3 track Vlan157
standby 3 track Vlan166
standby 3 track Vlan167
standby 3 track Vlan200
crypto engine slot 6
!
interface FastEthernet4/4
ip address 12.0.0.29 255.255.255.0
duplex half
standby delay minimum 30 reload 60
standby 2 ip 12.0.0.30
standby 2 preempt
standby 2 name HOME-LAN-2
standby 2 track FastEthernet4/2
standby 2 track FastEthernet4/3
standby 2 track FastEthernet4/4
standby 2 track FastEthernet4/7
standby 2 track FastEthernet4/9
standby 2 track FastEthernet4/11
standby 2 track GigabitEthernet6/1
standby 2 track Vlan136
standby 2 track Vlan137
standby 2 track Vlan127
standby 2 track Vlan126
standby 2 track Vlan146
standby 2 track Vlan147
```

```

standby 2 track Vlan156
standby 2 track Vlan157
standby 2 track Vlan166
standby 2 track Vlan167
standby 2 track Vlan200
crypto engine slot 6
!
interface FastEthernet4/5
switchport
switchport access vlan 137
switchport mode access
no ip address
!
interface FastEthernet4/6
switchport
switchport access vlan 127
switchport mode access
no ip address
speed 100
duplex half
!
interface FastEthernet4/7
ip address 14.0.0.29 255.255.255.0
standby delay minimum 30 reload 60
standby 4 ip 14.0.0.30
standby 4 preempt
standby 4 name HOME-LAN-4
standby 4 track FastEthernet4/2
standby 4 track FastEthernet4/3
standby 4 track FastEthernet4/4
standby 4 track FastEthernet4/7
standby 4 track FastEthernet4/9
standby 4 track FastEthernet4/11
standby 4 track Vlan136
standby 4 track Vlan137
standby 4 track Vlan127
standby 4 track Vlan126
standby 4 track GigabitEthernet6/1
standby 4 track Vlan146
standby 4 track Vlan147
standby 4 track Vlan156
standby 4 track Vlan157
standby 4 track Vlan166
standby 4 track Vlan167
standby 4 track Vlan200
crypto engine slot 6
!
interface FastEthernet4/8
switchport
switchport access vlan 147
switchport mode access
no ip address
!
interface FastEthernet4/9
ip address 15.0.0.29 255.255.255.0
standby delay minimum 30 reload 60
standby 5 ip 15.0.0.30
standby 5 preempt
standby 5 name HOME-LAN-5
standby 5 track FastEthernet4/2
standby 5 track FastEthernet4/3
standby 5 track FastEthernet4/4
standby 5 track FastEthernet4/7
standby 5 track FastEthernet4/9

```

```
standby 5 track FastEthernet4/11
standby 5 track Vlan136
standby 5 track Vlan137
standby 5 track Vlan127
standby 5 track Vlan126
standby 5 track GigabitEthernet6/1
standby 5 track Vlan146
standby 5 track Vlan147
standby 5 track Vlan156
standby 5 track Vlan157
standby 5 track Vlan166
standby 5 track Vlan167
standby 5 track Vlan200
crypto engine slot 6
!
interface FastEthernet4/10
switchport
switchport access vlan 157
switchport mode access
no ip address
!
interface FastEthernet4/11
ip address 16.0.0.29 255.255.255.0
standby delay minimum 30 reload 60
standby 6 ip 16.0.0.30
standby 6 preempt
standby 6 name HOME-LAN-6
standby 6 track FastEthernet4/2
standby 6 track FastEthernet4/3
standby 6 track FastEthernet4/4
standby 6 track FastEthernet4/7
standby 6 track FastEthernet4/9
standby 6 track FastEthernet4/11
standby 6 track Vlan136
standby 6 track Vlan137
standby 6 track Vlan127
standby 6 track Vlan126
standby 6 track GigabitEthernet6/1
standby 6 track Vlan146
standby 6 track Vlan147
standby 6 track Vlan156
standby 6 track Vlan157
standby 6 track Vlan166
standby 6 track Vlan167
standby 6 track Vlan200
crypto engine slot 6
!
interface FastEthernet4/12
switchport
switchport access vlan 167
switchport mode access
no ip address
!
interface GigabitEthernet6/1
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 126,136,146,156,166
switchport mode trunk
no ip address
flowcontrol receive on
flowcontrol send off
spanning-tree portfast trunk
!
interface GigabitEthernet6/2
```

```

switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan none
switchport mode trunk
no ip address
flowcontrol receive on
flowcontrol send off
spanning-tree portfast trunk
!
interface Vlan126
description secure vlan
ethernet point-to-point
ip vrf forwarding vrf-ha2
ip address 126.0.0.1 255.255.255.0
no ip redirects
no ip unreachable
ip policy route-map RRQ-HA2
no mop enabled
crypto map testmap1 ssp 1
crypto engine slot 6
!
interface Vlan127
description internal vlan to HA2
ip vrf forwarding vrf-ha2
ip address 6.0.0.1 255.255.0.0
standby 12 ip 6.0.0.5
standby 12 preempt
standby 12 name INTERNAL_VLAN_HA2
standby 12 track FastEthernet4/2
standby 12 track FastEthernet4/3
standby 12 track FastEthernet4/4
standby 12 track FastEthernet4/7
standby 12 track FastEthernet4/9
standby 12 track FastEthernet4/11
standby 12 track Vlan136
standby 12 track Vlan137
standby 12 track Vlan127
standby 12 track Vlan126
standby 12 track GigabitEthernet6/1
standby 12 track Vlan146
standby 12 track Vlan147
standby 12 track Vlan156
standby 12 track Vlan157
standby 12 track Vlan166
standby 12 track Vlan167
standby 12 track Vlan200
!
interface Vlan136
description secure vlan
ethernet point-to-point
ip vrf forwarding vrf-ha3
ip address 136.0.0.1 255.255.255.0
no ip redirects
no ip unreachable
ip policy route-map RRQ-HA3
no mop enabled
crypto map testmap ssp 1
crypto engine slot 6
!
interface Vlan137
description internal vlan to HA3
ip vrf forwarding vrf-ha3
ip address 7.0.0.1 255.255.0.0
standby 13 ip 7.0.0.5

```

```
standby 13 preempt
standby 13 name INTERNAL_VLAN_HA3
standby 13 track FastEthernet4/2
standby 13 track FastEthernet4/3
standby 13 track FastEthernet4/4
standby 13 track FastEthernet4/7
standby 13 track FastEthernet4/9
standby 13 track FastEthernet4/11
standby 13 track Vlan136
standby 13 track Vlan137
standby 13 track Vlan127
standby 13 track Vlan126
standby 13 track GigabitEthernet6/1
standby 13 track Vlan146
standby 13 track Vlan147
standby 13 track Vlan156
standby 13 track Vlan157
standby 13 track Vlan166
standby 13 track Vlan167
standby 13 track Vlan200
!
interface Vlan146
description secure vlan
ethernet point-to-point
ip vrf forwarding vrf-ha4
ip address 146.0.0.1 255.255.255.0
no ip redirects
no ip unreachablees
ip policy route-map RRQ-HA4
no mop enabled
crypto map testmap4 ssp 1
crypto engine slot 6
!
interface Vlan147
description internal vlan to HA4
ip vrf forwarding vrf-ha4
ip address 8.0.0.1 255.255.0.0
standby 14 ip 8.0.0.5
standby 14 preempt
standby 14 name INTERNAL_VLAN_HA4
standby 14 track FastEthernet4/2
standby 14 track FastEthernet4/3
standby 14 track FastEthernet4/4
standby 14 track FastEthernet4/7
standby 14 track FastEthernet4/9
standby 14 track FastEthernet4/11
standby 14 track Vlan136
standby 14 track Vlan137
standby 14 track Vlan127
standby 14 track Vlan126
standby 14 track GigabitEthernet6/1
standby 14 track Vlan146
standby 14 track Vlan147
standby 14 track Vlan156
standby 14 track Vlan157
standby 14 track Vlan166
standby 14 track Vlan167
standby 14 track Vlan200
!
interface Vlan156
description secure vlan
ethernet point-to-point
ip vrf forwarding vrf-ha5
ip address 156.0.0.1 255.255.255.0
```

```

no ip redirects
no ip unreachable
ip policy route-map RRQ-HA5
no mop enabled
crypto map testmap5 ssp 1
crypto engine slot 6
!
interface Vlan157
description internal vlan to HA5
ip vrf forwarding vrf-ha5
ip address 9.0.0.1 255.255.0.0
standby 15 ip 9.0.0.5
standby 15 preempt
standby 15 name INTERNAL_VLAN_HA5
standby 15 track FastEthernet4/2
standby 15 track FastEthernet4/3
standby 15 track FastEthernet4/4
standby 15 track FastEthernet4/7
standby 15 track FastEthernet4/9
standby 15 track FastEthernet4/11
standby 15 track Vlan136
standby 15 track Vlan137
standby 15 track Vlan127
standby 15 track Vlan126
standby 15 track GigabitEthernet6/1
standby 15 track Vlan146
standby 15 track Vlan147
standby 15 track Vlan156
standby 15 track Vlan157
standby 15 track Vlan166
standby 15 track Vlan167
standby 15 track Vlan200
!
interface Vlan166
description secure vlan
ethernet point-to-point
ip vrf forwarding vrf-ha6
ip address 166.0.0.1 255.255.255.0
no ip redirects
no ip unreachable
ip policy route-map RRQ-HA6
no mop enabled
crypto map testmap6 ssp 1
crypto engine slot 6
!
interface Vlan167
description internal vlan to HA6
ip vrf forwarding vrf-ha6
ip address 10.0.0.1 255.255.0.0
standby 16 ip 10.0.0.5
standby 16 preempt
standby 16 name INTERNAL_VLAN_HA6
standby 16 track FastEthernet4/2
standby 16 track FastEthernet4/3
standby 16 track FastEthernet4/4
standby 16 track FastEthernet4/7
standby 16 track FastEthernet4/9
standby 16 track FastEthernet4/11
standby 16 track Vlan136
standby 16 track Vlan137
standby 16 track Vlan127
standby 16 track Vlan126
standby 16 track GigabitEthernet6/1
standby 16 track Vlan146

```

```

standby 16 track Vlan147
standby 16 track Vlan156
standby 16 track Vlan157
standby 16 track Vlan166
standby 16 track Vlan167
standby 16 track Vlan200
!
interface vlan 200
 ip address 200.0.0.2 255.0.0.0
 standby 250 ip 200.0.0.3
 standby 250 preempt
 standby 250 name NON_IPSEC_VLAN
 standby 250 track FastEthernet4/2
 standby 250 track FastEthernet4/3
 standby 250 track FastEthernet4/4
 standby 250 track FastEthernet4/7
 standby 250 track FastEthernet4/9
 standby 250 track FastEthernet4/11
 standby 250 track Vlan136
 standby 250 track Vlan137
 standby 250 track Vlan127
 standby 250 track Vlan126
 standby 250 track GigabitEthernet6/1
 standby 250 track Vlan146
 standby 250 track Vlan147
 standby 250 track Vlan156
 standby 250 track Vlan157
 standby 250 track Vlan166
 standby 250 track Vlan167
!
ip route vrf vrf-ha2 92.92.92.0 255.255.255.0 Vlan126 92.92.92.1 global
ip route vrf vrf-ha3 92.92.92.0 255.255.255.0 Vlan136 92.92.92.1 global
ip route vrf vrf-ha4 92.92.92.0 255.255.255.0 Vlan146 92.92.92.1 global
ip route vrf vrf-ha5 92.92.92.0 255.255.255.0 Vlan156 92.92.92.1 global
ip route vrf vrf-ha6 92.92.92.0 255.255.255.0 Vlan166 92.92.92.1 global
!
access-list 121 permit ip host 12.0.0.30 host 92.92.92.1
access-list 121 remark Access List for HA2
access-list 131 permit ip host 13.0.0.30 host 92.92.92.1
access-list 131 remark Access List for HA3
access-list 141 permit ip host 14.0.0.30 host 92.92.92.1
access-list 141 remark Access List for HA4
access-list 151 permit ip host 15.0.0.30 host 92.92.92.1
access-list 151 remark Access List for HA5
access-list 161 permit ip host 16.0.0.30 host 92.92.92.1
access-list 161 remark Access List for HA6
access-list 2000 permit udp any any eq mobile-ip
access-list 2000 permit ipinip any any
access-list 2001 permit ip 95.95.95.0 0.0.0.255 host 120.0.0.30
access-list 2002 permit ip 96.96.96.0 0.0.0.255 host 130.0.0.30
access-list 2003 permit ip 97.97.97.0 0.0.0.255 host 140.0.0.30
access-list 2004 permit ip 98.98.98.0 0.0.0.255 host 150.0.0.30
access-list 2005 permit ip 99.99.99.0 0.0.0.255 host 160.0.0.30
!
arp vrf vrf-ha6 10.0.0.10 0000.0c07.ac32 ARPA
arp vrf vrf-ha4 8.0.0.10 0000.0c07.ac1e ARPA
arp vrf vrf-ha5 9.0.0.10 0000.0c07.ac28 ARPA
arp vrf vrf-ha2 6.0.0.10 0000.0c07.ac0a ARPA
arp vrf vrf-ha3 7.0.0.10 0000.0c07.ac14 ARPA
!
route-map RRQ-HA5 permit 10
 match ip address 2000
 set ip next-hop 9.0.0.10
!

```

```

route-map RRQ-HA4 permit 10
  match ip address 2000
  set ip next-hop 8.0.0.10
!
route-map RRQ-HA6 permit 10
  match ip address 2000
  set ip next-hop 10.0.0.10
!
route-map RRQ-HA3 permit 10
  match ip address 2000
  set ip next-hop 7.0.0.10
!
route-map RRQ-HA2 permit 10
  match ip address 2000
  set ip next-hop 6.0.0.10
!
route-map RRQ-HA10 permit 10
  match ip address 2001
  continue 11
  set ip next-hop 200.0.0.5
!
route-map RRQ-HA10 permit 11
  match ip address 2002
  continue 12
  set ip next-hop 200.0.0.15
!
route-map RRQ-HA10 permit 12
  match ip address 2003
  continue 13
  set ip next-hop 200.0.0.25
!
route-map RRQ-HA10 permit 13
  match ip address 2004
  continue 14
  set ip next-hop 200.0.0.35
!
route-map RRQ-HA10 permit 14
  match ip address 2005
  set ip next-hop 200.0.0.45

```

SUP Configuration - Switch 2:

```

ip vrf vrf-ha2
  rd 2000:1
  route-target export 2000:1
  route-target import 2000:1
!
ip vrf vrf-ha3
  rd 1000:1
  route-target export 1000:1
  route-target import 1000:1
!
ip vrf vrf-ha4
  rd 4000:1
  route-target export 4000:1
  route-target import 4000:1
!
ip vrf vrf-ha5
  rd 5000:1
  route-target export 5000:1
  route-target import 5000:1
!

```

```
ip vrf vrf-ha6
 rd 6000:1
  route-target export 6000:1
  route-target import 6000:1
!
ssp group 1
 remote 13.0.0.29
 redundancy PDSN-LAN
 redundancy HOME-LAN
 redundancy INTERNAL_VLAN_HA3
 redundancy HOME-LAN-2
 redundancy INTERNAL_VLAN_HA2
 redundancy HOME-LAN-4
 redundancy HOME-LAN-5
 redundancy HOME-LAN-6
 redundancy INTERNAL_VLAN_HA4
 redundancy INTERNAL_VLAN_HA5
 redundancy INTERNAL_VLAN_HA6
 port 4098
!
crypto keyring key0
 pre-shared-key address 92.92.92.1 key cisco
!
crypto isakmp policy 1
 authentication pre-share
 lifetime 60000
crypto isakmp ssp 1
!
crypto isakmp profile prof1
 vrf vrf-ha2
 keyring key0
 match identity address 92.92.92.1 255.255.255.255
 local-address 12.0.0.30
crypto isakmp profile prof2
 vrf vrf-ha3
 keyring key0
 match identity address 92.92.92.1 255.255.255.255
 local-address 13.0.0.30
crypto isakmp profile prof4
 vrf vrf-ha4
 keyring key0
 match identity address 92.92.92.1 255.255.255.255
 local-address 14.0.0.30
crypto isakmp profile prof5
 vrf vrf-ha5
 keyring key0
 match identity address 92.92.92.1 255.255.255.255
 local-address 15.0.0.30
crypto isakmp profile prof6
 vrf vrf-ha6
 keyring key0
 match identity address 92.92.92.1 255.255.255.255
 local-address 16.0.0.30
!
crypto ipsec transform-set mobile-set1 esp-des esp-sha-hmac
!
crypto map testmap local-address FastEthernet2/3
crypto map testmap 20 ipsec-isakmp
 set peer 92.92.92.1
 set transform-set mobile-set1
 set isakmp-profile prof2
 match address 131
!
crypto map testmap1 local-address FastEthernet2/5
```

```

crypto map testmap1 20 ipsec-isakmp
  set peer 92.92.92.1
  set transform-set mobile-set1
  set isakmp-profile prof1
  match address 121
!
crypto map testmap4 local-address FastEthernet2/7
crypto map testmap4 20 ipsec-isakmp
  set peer 92.92.92.1
  set transform-set mobile-set1
  set isakmp-profile prof4
  match address 141
!
crypto map testmap5 local-address FastEthernet2/9
crypto map testmap5 20 ipsec-isakmp
  set peer 92.92.92.1
  set transform-set mobile-set1
  set isakmp-profile prof5
  match address 151
!
crypto map testmap6 local-address FastEthernet2/11
crypto map testmap6 20 ipsec-isakmp
  set peer 92.92.92.1
  set transform-set mobile-set1
  set isakmp-profile prof6
  match address 161
!
crypto engine mode vrf
!
interface FastEthernet2/2
  ip address 92.92.92.11 255.255.0.0
  ip policy route-map RRQ-HA10
  speed 100
  duplex full
  standby delay minimum 30 reload 60
  standby 1 ip 92.92.92.10
  standby 1 preempt
  standby 1 name PDSN-LAN
  standby 1 track FastEthernet2/2
  standby 1 track FastEthernet2/3
  standby 1 track FastEthernet2/5
  standby 1 track FastEthernet2/7
  standby 1 track FastEthernet2/9
  standby 1 track FastEthernet2/11
  standby 1 track GigabitEthernet4/1
  standby 1 track Vlan136
  standby 1 track Vlan137
  standby 1 track Vlan127
  standby 1 track Vlan126
  standby 1 track Vlan146
  standby 1 track Vlan156
  standby 1 track Vlan157
  standby 1 track Vlan166
  standby 1 track Vlan167
  standby 1 track Vlan147
  standby 1 track Vlan200
  crypto engine slot 4
!
interface FastEthernet2/3
  ip address 13.0.0.31 255.255.0.0
  standby delay minimum 30 reload 60
  standby 3 ip 13.0.0.30
  standby 3 preempt
  standby 3 name HOME-LAN

```

```
standby 3 track FastEthernet2/2
standby 3 track FastEthernet2/3
standby 3 track FastEthernet2/5
standby 3 track FastEthernet2/7
standby 3 track FastEthernet2/9
standby 3 track FastEthernet2/11
standby 3 track GigabitEthernet4/1
standby 3 track Vlan136
standby 3 track Vlan137
standby 3 track Vlan127
standby 3 track Vlan126
standby 3 track Vlan146
standby 3 track Vlan156
standby 3 track Vlan157
standby 3 track Vlan166
standby 3 track Vlan167
standby 3 track Vlan147
standby 3 track Vlan200
crypto engine slot 4
!
interface FastEthernet2/4
  switchport
  switchport access vlan 137
  switchport mode access
  no ip address
!
interface FastEthernet2/5
  ip address 12.0.0.31 255.255.0.0
  standby delay minimum 30 reload 60
  standby 2 ip 12.0.0.30
  standby 2 preempt
  standby 2 name HOME-LAN-2
  standby 2 track FastEthernet2/2
  standby 2 track FastEthernet2/3
  standby 2 track FastEthernet2/5
  standby 2 track FastEthernet2/7
  standby 2 track FastEthernet2/9
  standby 2 track FastEthernet2/11
  standby 2 track GigabitEthernet4/1
  standby 2 track Vlan136
  standby 2 track Vlan137
  standby 2 track Vlan127
  standby 2 track Vlan126
  standby 2 track Vlan146
  standby 2 track Vlan156
  standby 2 track Vlan157
  standby 2 track Vlan166
  standby 2 track Vlan167
  standby 2 track Vlan147
  standby 2 track Vlan200
  crypto engine slot 4
!
interface FastEthernet2/6
  switchport
  switchport access vlan 127
  switchport mode access
  no ip address
!
interface FastEthernet2/7
  ip address 14.0.0.31 255.255.0.0
  standby delay minimum 30 reload 60
  standby 4 ip 14.0.0.30
  standby 4 preempt
  standby 4 name HOME-LAN-4
```

```

standby 4 track FastEthernet2/2
standby 4 track FastEthernet2/3
standby 4 track FastEthernet2/5
standby 4 track FastEthernet2/7
standby 4 track FastEthernet2/9
standby 4 track FastEthernet2/11
standby 4 track Vlan136
standby 4 track Vlan137
standby 4 track Vlan127
standby 4 track Vlan126
standby 4 track GigabitEthernet4/1
standby 4 track Vlan146
standby 4 track Vlan156
standby 4 track Vlan157
standby 4 track Vlan166
standby 4 track Vlan167
standby 4 track Vlan147
standby 4 track Vlan200
crypto engine slot 4
!
interface FastEthernet2/8
switchport
switchport access vlan 147
switchport mode access
no ip address
!
interface FastEthernet2/9
ip address 15.0.0.31 255.255.0.0
standby delay minimum 30 reload 60
standby 5 ip 15.0.0.30
standby 5 preempt
standby 5 name HOME-LAN-5
standby 5 track FastEthernet2/2
standby 5 track FastEthernet2/3
standby 5 track FastEthernet2/5
standby 5 track FastEthernet2/7
standby 5 track FastEthernet2/9
standby 5 track FastEthernet2/11
standby 5 track Vlan136
standby 5 track Vlan137
standby 5 track Vlan127
standby 5 track Vlan126
standby 5 track GigabitEthernet4/1
standby 5 track Vlan146
standby 5 track Vlan156
standby 5 track Vlan157
standby 5 track Vlan166
standby 5 track Vlan167
standby 5 track Vlan147
standby 5 track Vlan200
crypto engine slot 4
!
interface FastEthernet2/10
switchport
switchport access vlan 157
switchport mode access
no ip address
!
interface FastEthernet2/11
ip address 16.0.0.31 255.255.0.0
standby delay minimum 30 reload 60
standby 6 ip 16.0.0.30
standby 6 preempt
standby 6 name HOME-LAN-6

```

```
standby 6 track FastEthernet2/2
standby 6 track FastEthernet2/3
standby 6 track FastEthernet2/5
standby 6 track FastEthernet2/7
standby 6 track FastEthernet2/9
standby 6 track FastEthernet2/11
standby 6 track Vlan136
standby 6 track Vlan137
standby 6 track Vlan127
standby 6 track Vlan126
standby 6 track GigabitEthernet4/1
standby 6 track Vlan146
standby 6 track Vlan156
standby 6 track Vlan157
standby 6 track Vlan166
standby 6 track Vlan167
standby 6 track Vlan147
standby 6 track Vlan200
crypto engine slot 4
!
interface FastEthernet2/12
switchport
switchport access vlan 167
switchport mode access
no ip address
!
interface GigabitEthernet4/1
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan 126,136,146,156,166
switchport mode trunk
no ip address
flowcontrol receive on
flowcontrol send off
spanning-tree portfast trunk
!
interface GigabitEthernet4/2
switchport
switchport trunk encapsulation dot1q
switchport trunk allowed vlan none
switchport mode trunk
no ip address
flowcontrol receive on
flowcontrol send off
spanning-tree portfast trunk
!
interface Vlan126
description secure vlan
ethernet point-to-point
ip vrf forwarding vrf-ha2
ip address 126.0.0.2 255.255.255.0
no ip redirects
no ip unreachablees
ip policy route-map RRQ-HA2
no mop enabled
crypto map testmap1 ssp 1
crypto engine slot 4
!
interface Vlan127
description internal vlan to HA2
ip vrf forwarding vrf-ha2
ip address 6.0.0.2 255.255.0.0
standby 12 ip 6.0.0.5
standby 12 preempt
```

```

standby 12 name INTERNAL_VLAN_HA2
standby 12 track FastEthernet2/2
standby 12 track FastEthernet2/3
standby 12 track FastEthernet2/5
standby 12 track FastEthernet2/7
standby 12 track FastEthernet2/9
standby 12 track FastEthernet2/11
standby 12 track Vlan136
standby 12 track Vlan137
standby 12 track Vlan127
standby 12 track Vlan126
standby 12 track GigabitEthernet4/1
standby 12 track Vlan146
standby 12 track Vlan156
standby 12 track Vlan157
standby 12 track Vlan166
standby 12 track Vlan167
standby 12 track Vlan147
standby 12 track Vlan200
!
interface Vlan136
description secure vlan
ethernet point-to-point
ip vrf forwarding vrf-ha3
ip address 136.0.0.2 255.255.255.0
no ip redirects
no ip unreachable
ip policy route-map RRQ-HA3
no mop enabled
crypto map testmap ssp 1
crypto engine slot 4
!
interface Vlan137
description internal vlan to HA3
ip vrf forwarding vrf-ha3
ip address 7.0.0.2 255.255.0.0
standby 13 ip 7.0.0.5
standby 13 preempt
standby 13 name INTERNAL_VLAN_HA3
standby 13 track FastEthernet2/2
standby 13 track FastEthernet2/3
standby 13 track FastEthernet2/5
standby 13 track FastEthernet2/7
standby 13 track FastEthernet2/9
standby 13 track FastEthernet2/11
standby 13 track Vlan136
standby 13 track Vlan137
standby 13 track Vlan127
standby 13 track Vlan126
standby 13 track GigabitEthernet4/1
standby 13 track Vlan146
standby 13 track Vlan156
standby 13 track Vlan157
standby 13 track Vlan166
standby 13 track Vlan167
standby 13 track Vlan147
standby 13 track Vlan200
!
interface Vlan146
description secure vlan
ethernet point-to-point
ip vrf forwarding vrf-ha4
ip address 146.0.0.2 255.0.0.0
no ip redirects

```

```
no ip unreachable
ip policy route-map RRQ-HA4
no mop enabled
crypto map testmap4 ssp 1
crypto engine slot 4
!
interface Vlan147
description internal vlan to HA4
ip vrf forwarding vrf-ha4
ip address 8.0.0.2 255.255.0.0
standby 14 ip 8.0.0.5
standby 14 preempt
standby 14 name INTERNAL_VLAN_HA4
standby 14 track FastEthernet2/2
standby 14 track FastEthernet2/3
standby 14 track FastEthernet2/5
standby 14 track FastEthernet2/7
standby 14 track FastEthernet2/9
standby 14 track FastEthernet2/11
standby 14 track Vlan136
standby 14 track Vlan137
standby 14 track Vlan127
standby 14 track Vlan126
standby 14 track GigabitEthernet4/1
standby 14 track Vlan146
standby 14 track Vlan156
standby 14 track Vlan157
standby 14 track Vlan166
standby 14 track Vlan167
standby 14 track Vlan147
standby 14 track Vlan200
!
interface Vlan156
description secure vlan
ethernet point-to-point
ip vrf forwarding vrf-ha5
ip address 156.0.0.2 255.255.255.0
no ip redirects
no ip unreachable
ip policy route-map RRQ-HA5
no mop enabled
crypto map testmap5 ssp 1
crypto engine slot 4
!
interface Vlan157
description internal vlan to HA5
ip vrf forwarding vrf-ha5
ip address 9.0.0.2 255.255.0.0
standby 15 ip 9.0.0.5
standby 15 preempt
standby 15 name INTERNAL_VLAN_HA5
standby 15 track FastEthernet2/2
standby 15 track FastEthernet2/3
standby 15 track FastEthernet2/5
standby 15 track FastEthernet2/7
standby 15 track FastEthernet2/9
standby 15 track FastEthernet2/11
standby 15 track Vlan136
standby 15 track Vlan137
standby 15 track Vlan127
standby 15 track Vlan126
standby 15 track GigabitEthernet4/1
standby 15 track Vlan146
standby 15 track Vlan156
```

```

standby 15 track Vlan157
standby 15 track Vlan166
standby 15 track Vlan167
standby 15 track Vlan147
standby 15 track Vlan200
!
interface Vlan166
description secure vlan
ethernet point-to-point
ip vrf forwarding vrf-ha6
ip address 166.0.0.2 255.255.255.0
no ip redirects
no ip unreachable
ip policy route-map RRQ-HA6
no mop enabled
crypto map testmap6 ssp 1
crypto engine slot 4
!
interface Vlan167
description internal vlan to HA2
ip vrf forwarding vrf-ha6
ip address 10.0.0.2 255.255.0.0
standby 16 ip 10.0.0.5
standby 16 preempt
standby 16 name INTERNAL_VLAN_HA6
standby 16 track FastEthernet2/2
standby 16 track FastEthernet2/3
standby 16 track FastEthernet2/5
standby 16 track FastEthernet2/7
standby 16 track FastEthernet2/9
standby 16 track FastEthernet2/11
standby 16 track Vlan136
standby 16 track Vlan137
standby 16 track Vlan127
standby 16 track Vlan126
standby 16 track GigabitEthernet4/1
standby 16 track Vlan146
standby 16 track Vlan156
standby 16 track Vlan157
standby 16 track Vlan166
standby 16 track Vlan167
standby 16 track Vlan147
standby 16 track Vlan200
!
interface vlan 200
ip address 200.0.0.1 255.0.0.0
standby 250 ip 200.0.0.3
standby 250 preempt
standby 250 name NON_IPSEC_VLAN
standby 250 track FastEthernet2/2
standby 250 track FastEthernet2/3
standby 250 track FastEthernet2/5
standby 250 track FastEthernet2/7
standby 250 track FastEthernet2/9
standby 250 track FastEthernet2/11
standby 250 track Vlan136
standby 250 track Vlan137
standby 250 track Vlan127
standby 250 track Vlan126
standby 250 track GigabitEthernet4/1
standby 250 track Vlan146
standby 250 track Vlan156
standby 250 track Vlan157
standby 250 track Vlan166

```

```
standby 250 track Vlan167
standby 250 track Vlan147

ip route vrf vrf-ha2 92.92.92.0 255.255.255.0 Vlan126 92.92.92.1 global
ip route vrf vrf-ha3 92.92.92.0 255.255.255.0 Vlan136 92.92.92.1 global
ip route vrf vrf-ha4 92.92.92.0 255.255.255.0 Vlan146 92.92.92.1 global
ip route vrf vrf-ha5 92.92.92.0 255.255.255.0 Vlan156 92.92.92.1 global
ip route vrf vrf-ha6 92.92.92.0 255.255.255.0 Vlan166 92.92.92.1 global
!
access-list 121 permit ip host 12.0.0.30 host 92.92.92.1
access-list 121 remark Access List for HA2
access-list 131 permit ip host 13.0.0.30 host 92.92.92.1
access-list 131 remark Access List for HA3
access-list 141 permit ip host 14.0.0.30 host 92.92.92.1
access-list 141 remark Access List for HA4
access-list 151 permit ip host 15.0.0.30 host 92.92.92.1
access-list 151 remark Access List for HA5
access-list 161 permit ip host 16.0.0.30 host 92.92.92.1
access-list 161 remark Access List for HA6
access-list 2000 permit udp any any eq mobile-ip
access-list 2000 permit ipinip any any
access-list 2001 permit ip 95.95.95.0 0.0.0.255 host 120.0.0.30
access-list 2002 permit ip 96.96.96.0 0.0.0.255 host 130.0.0.30
access-list 2003 permit ip 97.97.97.0 0.0.0.255 host 140.0.0.30
access-list 2004 permit ip 98.98.98.0 0.0.0.255 host 150.0.0.30
access-list 2005 permit ip 99.99.99.0 0.0.0.255 host 160.0.0.30
!
arp vrf vrf-ha6 10.0.0.10 0000.0c07.ac32 ARPA
arp vrf vrf-ha4 8.0.0.10 0000.0c07.ac1e ARPA
arp vrf vrf-ha5 9.0.0.10 0000.0c07.ac28 ARPA
arp vrf vrf-ha2 6.0.0.10 0000.0c07.ac0a ARPA
arp vrf vrf-ha3 7.0.0.10 0000.0c07.ac14 ARPA
!
route-map RRQ-HA5 permit 10
  match ip address 2000
  set ip next-hop 9.0.0.10
!
route-map RRQ-HA4 permit 10
  match ip address 2000
  set ip next-hop 8.0.0.10
!
route-map RRQ-HA6 permit 10
  match ip address 2000
  set ip next-hop 10.0.0.10
!
route-map RRQ-HA3 permit 10
  match ip address 2000
  set ip next-hop 7.0.0.10
!
route-map RRQ-HA2 permit 10
  match ip address 2000
  set ip next-hop 6.0.0.10
!
route-map RRQ-HA10 permit 10
  match ip address 2001
  continue 11
  set ip next-hop 200.0.0.5
!
route-map RRQ-HA10 permit 11
  match ip address 2002
  continue 12
  set ip next-hop 200.0.0.15
!
route-map RRQ-HA10 permit 12
```

```

match ip address 2003
continue 13
set ip next-hop 200.0.0.25
!
route-map RRQ-HA10 permit 13
match ip address 2004
continue 14
set ip next-hop 200.0.0.35
!
route-map RRQ-HA10 permit 14
match ip address 2005
set ip next-hop 200.0.0.45

```

HA Configuration - Switch 1:

HA1:

```

interface Loopback0
description Advertised Home Agent Virtual IP Address
ip address 12.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.126
encapsulation dot1Q 126
ip address 126.0.0.82 255.255.255.0
!
interface GigabitEthernet0/0.127
description MWAM Processor interface to SUP (Private HSRP VLAN)
encapsulation dot1Q 127
ip address 6.0.0.3 255.255.255.0
standby 10 ip 6.0.0.10
standby 10 preempt
standby 10 name HSRP_HA_HA2
standby 10 track GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
description interface for non-ipsec pkts
encapsulation dot1Q 200
ip address 200.0.0.4 255.0.0.0
no snmp trap link-status
standby 200 ip 200.0.0.5
standby 200 preempt
standby 200 track GigabitEthernet0/0.127
!
router mobile
!
ip local pool ha-pool2 10.1.2.1 10.1.2.255
ip route 92.92.92.1 255.255.255.255 6.0.0.5
ip route 95.95.95.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA2 virtual-network address 12.0.0.30 mode
active-standby
ip mobile virtual-network 12.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool2 virtual-network 12.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 6.0.0.4 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix

```

HA2:

```

interface Loopback0
  description Advertised Home Agent Virtual IP Address
  ip address 13.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.136
  encapsulation dot1Q 136
  ip address 136.0.0.83 255.255.255.0
!
interface GigabitEthernet0/0.137
  description MWAM Processor interface to SUP (Private HSRP VLAN)
  encapsulation dot1Q 137
  ip address 7.0.0.3 255.255.255.0
  standby 20 ip 7.0.0.10
  standby 20 preempt
  standby 20 name HSRP_HA_HA3
  standby 20 name GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
  description interface for non-ipsec pkts
  encapsulation dot1Q 200
  ip address 200.0.0.14 255.0.0.0
  no snmp trap link-status
  standby 201 ip 200.0.0.15
  standby 201 preempt
  standby 201 track GigabitEthernet0/0.137
!
router mobile
!
ip local pool ha-pool3 10.1.3.1 10.1.3.255
ip route 92.92.92.1 255.255.255.255 7.0.0.5
ip route 96.96.96.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA3 virtual-network address 13.0.0.30 mode
active-standby
ip mobile virtual-network 13.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool3 virtual-network 13.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 7.0.0.4 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix

```

HA3:

```

interface Loopback0
  description Advertised Home Agent Virtual IP Address
  ip address 14.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.146
  encapsulation dot1Q 146
  ip address 146.0.0.82 255.255.255.0
!
interface GigabitEthernet0/0.147
  description MWAM Processor interface to SUP (Private HSRP VLAN)
  encapsulation dot1Q 147
  ip address 8.0.0.3 255.255.255.0
  standby 30 ip 8.0.0.10
  standby 30 preempt
  standby 30 name HSRP_HA_HA4

```

```

standby 30 name GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
description interface for non-ipsec pkts
encapsulation dot1Q 200
ip address 200.0.0.24 255.0.0.0
no snmp trap link-status
standby 202 ip 200.0.0.25
standby 202 preempt
standby 202 track GigabitEthernet0/0.147
!
router mobile
!
ip local pool ha-pool4 10.1.4.1 10.1.4.255
ip route 92.92.92.1 255.255.255.255 8.0.0.5
ip route 97.97.97.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA4 virtual-network address 14.0.0.30 mode
active-standby
ip mobile virtual-network 13.0.0.10 255.255.255.255
ip mobile virtual-network 14.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool4 virtual-network 14.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 8.0.0.4 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix

```

HA4:

```

interface Loopback0
description Advertised Home Agent Virtual IP Address
ip address 15.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.156
encapsulation dot1Q 156
ip address 156.0.0.82 255.255.255.0
!
interface GigabitEthernet0/0.157
description MWAM Processor interface to SUP (Private HSRP VLAN)
encapsulation dot1Q 157
ip address 9.0.0.3 255.255.255.0
standby 40 ip 9.0.0.10
standby 40 preempt
standby 40 name HSRP_HA_HA5
standby 40 name GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
description interface for non-ipsec pkts
encapsulation dot1Q 200
ip address 200.0.0.34 255.0.0.0
no snmp trap link-status
standby 203 ip 200.0.0.35
standby 203 preempt
standby 203 track GigabitEthernet0/0.157
!
router mobile
!
ip local pool ha-pool5 10.1.5.1 10.1.5.255
ip route 92.92.92.1 255.255.255.255 9.0.0.5
ip route 98.98.98.0 255.255.255.0 200.0.0.3
!

```

```

ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA5 virtual-network address 15.0.0.30 mode
active-standby
ip mobile virtual-network 15.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool5 virtual-network 15.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 9.0.0.4 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix

```

HA5:

```

interface Loopback0
  description Advertised Home Agent Virtual IP Address
  ip address 16.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.166
  encapsulation dot1Q 166
  ip address 166.0.0.82 255.255.255.0
!
interface GigabitEthernet0/0.167
  description MWAM Processor interface to SUP (Private HSRP VLAN)
  encapsulation dot1Q 167
  ip address 10.0.0.3 255.255.255.0
  standby 50 ip 10.0.0.10
  standby 50 preempt
  standby 50 name HSRP_HA_HA6
  standby 50 GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
  description interface for non-ipsec pkts
  encapsulation dot1Q 200
  ip address 200.0.0.44 255.0.0.0
  no snmp trap link-status
  standby 204 ip 200.0.0.45
  standby 204 preempt
  standby 204 track GigabitEthernet0/0.167
!
router mobile
!
ip local pool ha-pool6 10.1.6.1 10.1.6.255
ip route 92.92.92.1 255.255.255.255 10.0.0.5
ip route 99.99.99.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA6 virtual-network address 16.0.0.30 mode
active-standby
ip mobile virtual-network 16.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool6 virtual-network 16.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 10.0.0.4 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix

```

HA Configuration - Switch 2:**HA1:**

```

interface Loopback0
  description Advertised Home Agent Virtual IP Address
  ip address 12.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.126
  encapsulation dot1Q 126
  ip address 126.0.0.32 255.255.255.0
!
interface GigabitEthernet0/0.127
  description MWAM Processor interface to SUP (Private HSRP VLAN)
  encapsulation dot1Q 127
  ip address 6.0.0.4 255.255.255.0
  standby 10 ip 6.0.0.10
  standby 10 preempt
  standby 10 name HSRP_HA_HA2
  standby 10 GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
  description interface for non-ipsec pkts
  encapsulation dot1Q 200
  ip address 200.0.0.6 255.0.0.0
  no snmp trap link-status
  standby 200 ip 200.0.0.5
  standby 200 preempt
  standby 200 track GigabitEthernet0/0.127
!
router mobile
!
ip local pool ha-pool2 10.1.2.1 10.1.2.255
ip route 92.92.92.1 255.255.255.255 6.0.0.5
ip route 95.95.95.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA2 virtual-network address 12.0.0.30 mode
active-standby
ip mobile virtual-network 12.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool2 virtual-network 12.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 6.0.0.3 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix

```

HA2:

```

interface Loopback0
  description Advertised Home Agent Virtual IP Address
  ip address 13.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.136
  encapsulation dot1Q 136
  ip address 136.0.0.33 255.255.255.0
!
interface GigabitEthernet0/0.137
  description MWAM Processor interface to SUP (Private HSRP VLAN)
  encapsulation dot1Q 137
  ip address 7.0.0.4 255.255.255.0
  standby 20 ip 7.0.0.10
  standby 20 preempt

```

```

standby 20 name HSRP_HA_HA3
standby 20 GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
description interface for non-ipsec pkts
encapsulation dot1Q 200
ip address 200.0.0.16 255.0.0.0
no snmp trap link-status
standby 201 ip 200.0.0.15
standby 201 preempt
standby 201 track GigabitEthernet0/0.137
!
router mobile
!
ip local pool ha-pool3 10.1.3.1 10.1.3.255
ip route 92.92.92.1 255.255.255.255 7.0.0.5
ip route 96.96.96.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA3 virtual-network address 13.0.0.30 mode
active-standby
ip mobile virtual-network 13.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool3 virtual-network 13.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 7.0.0.3 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix

```

HA3:

```

interface Loopback0
description Advertised Home Agent Virtual IP Address
ip address 14.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.146
encapsulation dot1Q 146
ip address 146.0.0.32 255.255.255.0
!
interface GigabitEthernet0/0.147
description MWAM Processor interface to SUP (Private HSRP VLAN)
encapsulation dot1Q 147
ip address 8.0.0.4 255.255.255.0
standby 30 ip 8.0.0.10
standby 30 preempt
standby 30 name HSRP_HA_HA4
standby 30 GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
description interface for non-ipsec pkts
encapsulation dot1Q 200
ip address 200.0.0.26 255.0.0.0
no snmp trap link-status
standby 202 ip 200.0.0.25
standby 202 preempt
standby 202 track GigabitEthernet0/0.147
!
router mobile
!
ip local pool ha-pool4 10.1.4.1 10.1.4.255
ip route 92.92.92.1 255.255.255.255 8.0.0.5
ip route 97.97.97.0 255.255.255.0 200.0.0.3
!

```

```

ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA4 virtual-network address 14.0.0.30 mode
active-standby
ip mobile virtual-network 14.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool4 virtual-network 14.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 8.0.0.3 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix

```

HA4:

```

interface Loopback0
  description Advertised Home Agent Virtual IP Address
  ip address 15.0.0.30 255.255.255.255
!
interface GigabitEthernet0/0.156
  encapsulation dot1Q 156
  ip address 156.0.0.32 255.255.255.0
!
interface GigabitEthernet0/0.157
  description MWAM Processor interface to SUP (Private HSRP VLAN)
  encapsulation dot1Q 157
  ip address 9.0.0.4 255.255.255.0
  standby 40 ip 9.0.0.10
  standby 40 preempt
  standby 40 name HSRP_HA_HA5
  standby 40 GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
  description interface for non-ipsec pkts
  encapsulation dot1Q 200
  ip address 200.0.0.36 255.0.0.0
  no snmp trap link-status
  standby 203 ip 200.0.0.35
  standby 203 preempt
  standby 203 track GigabitEthernet0/0.157
!
router mobile
!
ip local pool ha-pool15 10.1.5.1 10.1.5.255
ip route 92.92.92.1 255.255.255.255 9.0.0.5
ip route 98.98.98.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA5 virtual-network address 15.0.0.30 mode
active-standby
ip mobile virtual-network 15.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool15 virtual-network 15.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 9.0.0.3 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix

```

HA5:

```

interface Loopback0
  description Advertised Home Agent Virtual IP Address
  ip address 16.0.0.30 255.255.255.255
!

```

```
interface GigabitEthernet0/0.166
 encapsulation dot1Q 166
 ip address 166.0.0.32 255.255.255.0
!
interface GigabitEthernet0/0.167
 description MWAM Processor interface to SUP (Private HSRP VLAN)
 encapsulation dot1Q 167
 ip address 10.0.0.4 255.255.255.0
 standby 50 ip 10.0.0.10
 standby 50 preempt
 standby 50 name HSRP_HA_HA6
 standby 50 GigabitEthernet0/0.200
!
interface GigabitEthernet0/0.200
 description interface for non-ipsec pkts
 encapsulation dot1Q 200
 ip address 200.0.0.46 255.0.0.0
 no snmp trap link-status
 standby 204 ip 200.0.0.45
 standby 204 preempt
 standby 204 track GigabitEthernet0/0.167
!
router mobile
!
ip local pool ha-pool6 10.1.6.1 10.1.6.255
ip route 92.92.92.1 255.255.255.255 10.0.0.5
ip route 98.98.98.0 255.255.255.0 200.0.0.3
!
ip mobile home-agent unknown-ha accept
ip mobile home-agent redundancy HSRP_HA_HA6 virtual-network address 16.0.0.30 mode
active-standby
ip mobile virtual-network 16.0.0.10 255.255.255.255
ip mobile host nai @cisco.com address pool local ha-pool6 virtual-network 16.0.0.10
255.255.255.255
ip mobile secure host nai @cisco.com spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 10.0.0.3 spi 100 key ascii cisco algorithm md5 mode
prefix-suffix
```

