CHAPTER 13

Multi-VPN Routing and Forwarding on the Home Agent

This chapter discusses the functional elements of the Multi-VPN Routing and Forwarding (VRF) CE network architecture, and their implementation in Cisco IOS Mobile Wireless Home Agent software.

This chapter includes the following sections:

- VRF Support on HA, page 13-1
- Mobile IP Tunnel Establishment, page 13-3
- VRF Mapping on the RADIUS Server, page 13-4
- VRF Feature Restrictions, page 13-4
- Authentication and Accounting Server Groups Per Realm, page 13-4
- Configuring VRF for the HA, page 13-5
- VRF Configuration Example, page 13-6
- VRF Configuration with HA Redundancy Example, page 13-7

VRF Support on HA

The HA supports overlapping IP addresses for mobile nodes for the mobile IP flows that are opened for different realms. This feature is based on the Multi-VPN Routing and Forwarding (VRF) CE network architecture, and expands the BGP/MPLS VPN architecture to support multiple VPNs (and therefore multiple customers) per Customer Edge (CE) device. This reduces the amount of equipment required, and simplifies administration, while allowing the use of overlapping IP address spaces within the CE network.

Multi-VRF CE is a new feature, introduced in Cisco IOS release 12.2(4)T, that addresses these issues. Multi-VRF CE, also known as VRF-Lite, extends limited PE functionality to a Customer Edge (CE) router in an MPLS-VPN model. A CE router now has the ability to maintain separate VRF tables in order to extend the privacy and security of an MPLS-VPN down to a branch office rather than just at the PE router node. The CE can support traffic separation between customer networks, or between entities within a single customer network. Each VRF on the CE router is mapped to a corresponding VRF on the PE router.

For more information on Multi-VRF CE network architecture, please refer to Cisco Product Bulletin 1575 at the following URL: http://www.cisco.com/warp/public/cc/pd/rt/2600/prodlit/1575_pp.pdf.

Figure 13-1 VRF-Lite in the Cisco PDSN/Home Agent Architecture

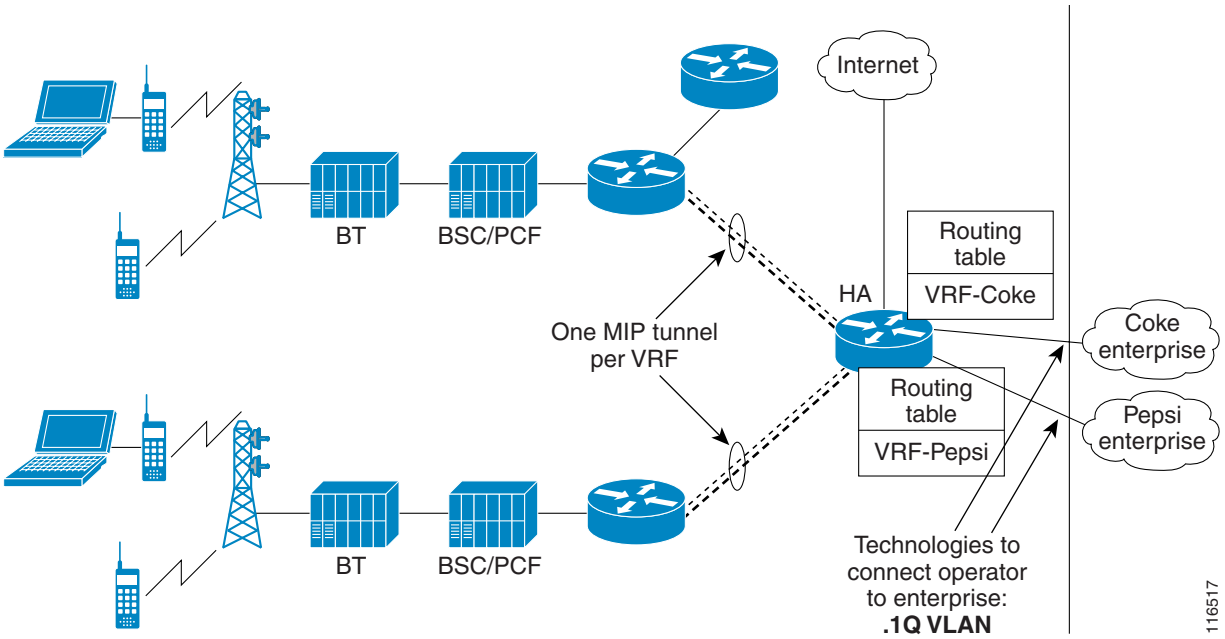

Figure 13-1 illustrates the PDSN architecture and how the VRF-lite solution is applied to the Home Agent for different realms/enterprises, thus segregating data between the enterprises.

Highlights of the VRF solution include the following:

- Provides a method to identify VRF of the user that is based on domain/realm of the user.
- Provides a method to ensure delivery of packets to the mobile through the PDSN, when different mobiles belonging to different enterprises share the same overlapping IP address.
- Supports IP address and routing table management per VRF.
- Supports management of VRF per enterprise/domain.
- Supports AAA authentication and accounting group per VRF.

The realm is used to identify an enterprise network. One virtual Home Agent is configured per realm. NAI is part of Mobile IP RRQ, and is the main identifier of mobile IP users in the PDSN and HA. The realm part of NAI will be used to identify the virtual Home Agent. Mobile nodes follow the NAI convention of *username@company*, where *company* identifies a realm name that indicates a subscriber community.

Multiple IP addresses are used at the HA to indicate different enterprise connections or VRFs to the PDSN. Thus, there will be one mobile IP tunnel between the PDSN and the HA per realm/VRF.

For an HA that is connected to two enterprises, “abc.com” and “xyz.com,” the HA will be configured with two unique IP addresses (typically configured under a loopback interface). The PDSN will have a MoIP tunnel to an address LA1 to reach “abc.com,” and will have another MoIP tunnel to address LA2 to reach “xyz.com,” where LA1 and LA2 are IP addresses configured under a Loopback interface.

On the home AAA RADIUS server, the NAI/domain configuration ensures that the PDSN receives LA1 as the IP address of the Home Agent of enterprise “xyz.com” as part of the Access Response during FA-CHAP or HA-CHAP (MN-AAA authentication); and LA2 as the IP address of Home Agent of enterprise “mnp.com”.

This feature will work with HA-SLB solution for HA load balancing.

Mobile IP Tunnel Establishment

The following procedure describes a mobile IP flow establishment with HA-SLB and VRF enabled. Elements in this call flow are two Mobile nodes (MN-1 and MN-2) belonging to enterprise ENT-1 & ENT-2 respectively:

Step 1 When a Mobile IP RRQ arrives at the HA, the HA will read the NAI field of the incoming RRQ, and select a pre-configured IP address to form a Mobile IP tunnel back to the PDSN using this IP address as the source address of the tunnel.

Step 2 The “Home-Agent address” field in the RRP that is being sent to the PDSN is modified to the IP address as described above.

Step 3 The Home Agent adds a host route corresponding to the IP address assigned for the mobile in the routing table corresponding to the VRF defined for the realm.

Step 4 The tunnel end-point at HA is also inserted in the VRF routing table. This enables the mobiles to share common IP address across different realms on the same Home Agent.

Step 5 MN-1 sends Mobile IP RRQ with Home Agent address set to 0.0.0.0 (dynamic Home Agent) to PDSN over its R-P session.

Step 6 PDSN initiates FA-CHAP and sends an Access Request to AAA.

Step 7 AAA responds with Access Response, Home Agent address returned is the IP address of HA-SLB.

Step 8 PDSN forwards MIP RRQ to HA-SLB.

Step 9 HA-SLB determines real HA based on load, and forwards the RRQ to HA1.

Step 10 HA-1 receives the MIP RRQ. It parses the NAI inside the message and determines the VRF of the user based on its realm - enterprise Ent-1. It performs HA-CHAP (MN-AAA authentication), allocates IP address to mobile for Ent-1. It creates a binding for the mobile and populates VRF specific data structures like route entry in route-table of VRF, FIB, etc.

Step 11 HA1 sends MIP RRP to PDSN, and also establishes mobile IP tunnel between PDSN and HA. End point of the tunnel on HA is L1-IP-1 (rather than IP address of ingress interface in the MIP RRQ).

VRF Mapping on the RADIUS Server

In Release 3.0, the VRF feature is enhanced to configure the NAI to VRF mapping on the RADIUS server. Mobile to VRF mapping will be learned as follows with this enhancement. When a mobileip registration request is received, the HA sends a radius access request. The AAA server sends access accept with VRF name, in radius attribute “cisco-avpair = mobileip:ip-vrf”, and the corresponding home-agent address in RADIUS attribute “cisco-avpair = mobileip-vrf-ha-addr” to the HA. The Home Agent uses this information to open the binding and associates it with the correct VRF. If the above attributes are not downloaded from AAA server, then the locally configured VRF, if any, is used.

Additionally, an option is provided to send a registration reply with code 136 and a new home agent address, if the HA has to assign a different address than requested by the PDSN/FA. Upon receiving a registration reply with code 136, the mobile sends one more registration request with a new address. The HA will process the request, open a binding, and send a registration reply (success) thus completing the registration process

VRF Feature Restrictions

The following list identifies restrictions for the VRF feature:

- A maximum of 130 VRFs per Home Agent is supported.
- The Home Agent MIB is not updated with the VRF information.

Authentication and Accounting Server Groups Per Realm

Separate authentication and accounting groups can be specified across different realms. Based on the realm of the user, the HA will choose the AAA authentication server based on the authentication group specified for the realm on the HA. Similarly, the HA will choose a AAA accounting server based on the realm of the user if the accounting group is specified for the realm.

Note This feature will work in conjunction with the VRF feature.

Configuring VRF for the HA

To configure VRF on the HA, perform the following tasks:

	Command	Purpose
Step 1	`Router(config)#`**`ip mobile realm`** *`@xyz.com`* **`vrf`** *`vrf-name`* **`ha-addr`** *`ip-address`* [**`aaa-group`** [**`accounting`** *`aaa-acct-group`* | **`authentication`** *`aaa-auth-group`*]]	Defines the VRF for the domain *@xyz.com*. The IP address of the Home Agent that corresponds to the VRF is also defined at the point that the MOIP tunnel will terminate. The IP address of the Home Agent should be a routable IP address on the box. Optionally, the AAA accounting and/or authentication server groups can be defined per VRF. If AAA accounting server group is defined, all accounting records for the users of the realm will be sent to the specified group. If AAA authentication server group is defined, HA-CHAP (MN-AAA authentication) is sent to the server(s) defined in the group.

Step 2	`Router(config)#` **`ip vrf`** *`vrf-name`*
	`description VRF for domain1`
	`rd 10:1`
		Defines the VRF on the box.
		Description of the VRF.
		Router descriptor for VRF. Creates a VRF table by specifying a route distinguisher.
		Note One VRF per domain should be configured on each HA CPU.

Step 3	`router#` **`interface Loopback1`**
	`ip address 192.168.11.1 255.255.255.0 secondary`
	`ip address 192.168.10.1 255.255.255.0`
		Defines the loopback interface under which the IP addresses for each VRF are configured. These addresses are used as the Mobile IP tunnel source IP addresses for the realm.
		The mask that is configured for the IP address will be used in the VRF routing table. Host mask (255.255.255.255) or broadcast mask (0.0.0.0) should not be configured.

Here is an example of how to configure the User profile for VRF:

```
[ //localhost/Radius/Profiles/mwts-mip-r20sit-haslb1-prof/Attributes ]
    CDMA-HA-IP-Addr = 20.20.225.1
    CDMA-MN-HA-Shared-Key = ciscociscociscoc
    CDMA-MN-HA-SPI = 00:00:10:01
    CDMA-Reverse-Tunnel-Spec = "Reverse tunneling is required"
    cisco-avpair = mobileip-vrf-ha-addr=20.20.204.2
    cisco-avpair = ip:ip-vrf#0=ispxyz-vrf1
    class = "Entering the World of Mobile IP-3"
    Service-Type = Framed
```

VRF Configuration Example

The following is a sample configuration on an MWAM HA with VRF support:

```
CiscoHA#show running-config
Building configuration...

Current configuration : 3366 bytes
!
...
!
aaa new-model
!
!
aaa group server radius vrf-auth-grp1
 server 9.15.100.1 auth-port 1645 acct-port 1646
!
aaa group server radius vrf-auth-grp2
 server 10.76.86.8 auth-port 1645 acct-port 1646
!
aaa authentication ppp vrf-auth-grp1 group vrf-auth-grp1
aaa authentication ppp vrf-auth-grp2 group vrf-auth-grp2
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network vrf-auth-grp1 group vrf-auth-grp1
aaa authorization network vrf-auth-grp2 group vrf-auth-grp2
aaa authorization configuration default group radius
aaa accounting network default start-stop group radius
aaa accounting network vrf-auth-grp1 start-stop group vrf-auth-grp1
aaa accounting network vrf-auth-grp2 start-stop group vrf-auth-grp2
aaa session-id common
ip subnet-zero
no ip gratuitous-arps
ip cef
no ip domain lookup
!
!
ip vrf moip-vrf-grp1
 rd 100:1
!
ip vrf moip-vrf-grp2
 rd 100:2
!
no virtual-template snmp
!
!
!
interface Loopback1
 ip address 172.16.11.1 255.255.255.0 secondary
 ip address 172.16.10.1 255.255.255.0
!
interface GigabitEthernet0/0
 no ip address
!
interface GigabitEthernet0/0.11
 encapsulation dot1Q 11
 ip address 9.15.42.111 255.255.0.0
 no cdp enable
!
interface GigabitEthernet0/0.82
 description Interface towards PDSN
 encapsulation dot1Q 82
 ip address 10.82.82.2 255.255.0.0
```

```
!
router mobile
!
ip local pool vrf-pool1 10.5.5.1 5.5.5.254 group vrf-pool-grp1
ip local pool vrf-pool2 10.5.5.1 5.5.5.254 group vrf-pool-grp2
ip classless
ip route 10.15.47.80 255.255.255.255 GigabitEthernet0/1
ip route 10.76.86.8 255.255.255.255 9.15.0.1
ip route 10.1.0.0 255.255.0.0 GigabitEthernet0/0.82
no ip http server
!
ip mobile home-agent
ip mobile host nai @xyz.com address pool local vrf-pool2 interface GigabitEthernet0/0.82
aaa
ip mobile host nai @cisco.com address pool local vrf-pool1 interface GigabitEthernet0/0.82
aaa
ip mobile realm @xyz.com vrf moip-vrf-grp2 ha 172.16.11.1 aaa-group accounting
vrf-auth-grp1 authentication vrf-auth-grp2
ip mobile realm @cisco.com vrf moip-vrf-grp1 ha 172.16.10.1 aaa-group accounting
vrf-auth-grp2 authentication vrf-auth-grp1
!
!
!
radius-server host 10.15.100.1 auth-port 1645 acct-port 1646 key cisco
radius-server host 10.76.86.8 auth-port 1645 acct-port 1646 key cisco
!
control-plane
!
...
!
end
```

VRF Configuration with HA Redundancy Example

The following is a sample configuration on a Cisco HA with HA redundancy and VRF. The following steps are required:

Step 1 Configure normal HSRP and HA redundancy for the published HA IP address.

Step 2 Rather than configuring IP addresses on the Loopback (or any other interface IP addresses for tunnel end-point), configure them on the HSRP interface as a secondary standby IP address.

Step 3 For ip mobile redundancy, add virtual network for VRF tunnel point subnet.

Step 4 Configure the VRF related commands.

Step 5 Because the binding update message from active to the standby HA contains the NAI, the standby is able to create the binding using appropriate VRF using the domain of the NAI in the message.

Active HA:

```
HA1#sh run
...
aaa new-model
!
!
aaa group server radius vrf-auth-grp1
 server 9.15.100.1 auth-port 1645 acct-port 1646
!
```

```
aaa group server radius vrf-auth-grp2
 server 10.76.86.8 auth-port 1645 acct-port 1646
!
aaa authentication ppp default local group radius
aaa authentication ppp vrf-auth-grp1 group vrf-auth-grp1
aaa authentication ppp vrf-auth-grp2 group vrf-auth-grp2
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa authorization network vrf-auth-grp1 group vrf-auth-grp1
aaa authorization network vrf-auth-grp2 group vrf-auth-grp2
aaa authorization configuration default group radius
aaa session-id common
ip subnet-zero
ip gratuitous-arps
!
!
ip cef
no ip domain lookup
!
!
ip vrf moip-vrf
 rd 100:1
!
ip vrf moip-vrf1
 rd 100:2
!
...
!
interface FastEthernet1/0
 ip address 10.92.92.2 255.255.0.0
 duplex auto
 speed auto
 no cdp enable
 standby 10 ip 10.92.92.12
 standby 10 ip 172.16.11.1 secondary
 standby 10 ip 172.16.12.1 secondary
 standby 10 priority 130
 standby 10 preempt delay sync 10
 standby 10 name cisco
!
!
router mobile
!
ip local pool vrf-pool1 10.5.5.5 5.5.5.55 group vrf-pool-grp1
ip local pool vrf-pool2 10.5.5.5 5.5.5.55 group vrf-pool-grp2
ip classless
ip mobile home-agent address 10.92.92.12
ip mobile home-agent ip mobile home-agent redundancy
ip mobile host nai @cisco.com address pool local vrf-pool1 interface FastEthernet1/0 aaa
ip mobile host nai @xyz.com address pool local vrf-pool2 interface FastEthernet1/0 aaa
ip mobile realm @cisco.com vrf moip-vrf home-agent-address 192.168.11.1 aaa-group
authentication vrf-auth-grp1
ip mobile realm @xyz.com vrf moip-vrf1 home-agent-address 192.168.12.1 aaa-group
authentication vrf-auth-grp2
ip mobile secure home-agent 10.92.92.3 spi 101 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 172.16.11.1 spi 101 key ascii cisco algorithm md5 mode
prefix-suffix
...
```

```
radius-server host 10.76.86.8 auth-port 1645 acct-port 1646 key cisco
radius-server host 10.15.100.1 auth-port 1645 acct-port 1646 key cisco
!
...
end
```

Standby HA:

```
HA2#sh run
...
!
aaa new-model
!
aaa group server radius vrf-auth-grp1
 server 10.15.100.1 auth-port 1645 acct-port 1646
!
aaa group server radius vrf-auth-grp2
 server 10.76.86.8 auth-port 1645 acct-port 1646
!
aaa authentication ppp default group radius
aaa authentication ppp vrf-auth-grp1 group vrf-auth-grp1
aaa authentication ppp vrf-auth-grp2 group vrf-auth-grp2
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa authorization network vrf-auth-grp1 group vrf-auth-grp1
aaa authorization network vrf-auth-grp2 group vrf-auth-grp2
aaa session-id common
ip subnet-zero
!
!
ip cef
!
!
ip vrf moip-vrf
 rd 100:1
!
ip vrf moip-vrf1
 rd 100:2
!
...
!
interface FastEthernet1/0
 ip address 10.92.92.3 255.255.255.0
 duplex auto
 speed auto
 standby 10 ip 10.92.92.12
 standby 10 ip 172.16.11.1 secondary
 standby 10 ip 172.16.12.1 secondary
 standby 10 preempt delay sync 10
 standby 10 name cisco
!
...
!
router mobile
!
ip local pool vrf-pool1 10.5.5.5 5.5.5.55 group vrf-pool-grp1
ip local pool vrf-pool2 10.5.5.5 5.5.5.55 group vrf-pool-grp2
ip mobile home-agent address 10.92.92.12
ip mobile home-agent ip mobile home-agent redundancy
ip mobile host nai @cisco.com address pool local vrf-pool1 interface FastEthernet1/0 aaa
ip mobile host nai @xyz.com address pool local vrf-pool2 interface FastEthernet1/0 aaa
```

```
ip mobile realm @cisco.com vrf moip-vrf home-agent-address 192.168.11.1 aaa-group
authentication vrf-auth-grp1
ip mobile realm @xyz.com vrf moip-vrf1 home-agent-address 192.168.12.1 aaa-group
authentication vrf-auth-grp2
ip mobile secure home-agent 10.92.92.2 spi 101 key ascii cisco algorithm md5 mode
prefix-suffix
ip mobile secure home-agent 172.16.11.1 spi 101 key ascii cisco algorithm md5 mode
prefix-suffix ignore-spi
ip mobile secure home-agent 172.16.12.1 spi 101 key ascii cisco algorithm md5 mode
prefix-suffix
no ip http server
!
...
radius-server host 10.76.86.8 auth-port 1645 acct-port 1646 key cisco
radius-server host 10.15.100.1 auth-port 1645 acct-port 1646 key cisco
...
end
```