CHAPTER 13

Home Agent（HA）でのマルチ VPN ルーティングおよびフォワーディング（VRF）

この章では、マルチ VPN Routing and Forwarding（VRF; VPN ルーティングおよびフォワーディング）Customer Edge（CE; カスタマー エッジ）ネットワーク アーキテクチャの機能要素、および Cisco IOS Mobile Wireless Home Agent ソフトウェアでの実装について説明します。

この章は、次の内容で構成されています。

- 「HA での VRF サポート」（P.13-1）
- 「モバイル IP トンネルの確立」（P.13-3）
- 「RADIUS サーバ上の VRF マッピング」（P.13-3）
- 「VRF 機能の制約事項」（P.13-4）
- 「レルム単位の認証およびアカウンティング サーバ グループ」（P.13-4）
- 「HA の VRF の設定」（P.13-4）
- 「VRF の設定例」（P.13-5）
- 「HA 冗長性を使用した VRF の設定例」（P.13-7）

HA での VRF サポート

Home Agent（HA）は、異なるレルムで開かれたモバイル IP フローのモバイル ノードについて、オーバーラップ IP アドレスをサポートします。この機能は、マルチ VPN VRF CE ネットワーク アーキテクチャを基盤とし、単一の CE デバイスで複数の VPN（つまり複数のカスタマー）をサポートできるように、BGP/MPLS VPN アーキテクチャに拡張したものです。これにより、必要な機器数を削減し、管理を簡素化しながら、CE ネットワーク内でオーバーラップ IP アドレス スペースを使用できます。

マルチ VRF CE は、これらの問題に対応している Cisco IOS Release 12.2(4)T で導入された新機能です。マルチ VRF CE は、VRF-Lite とも呼ばれ、MPLS-VPN モデル内の CE に、限定された Provider Edge（PE; プロバイダー エッジ）機能を提供します。CE ルータで個別の VRF テーブルを保持できるので、MPLS-VPN のプライバシーおよびセキュリティを、PE ルータ ノードだけでなく、ブランチ オフィスにも拡張して適用できます。CE は、カスタマー ネットワーク間、または単一カスタマー ネットワーク内のエンティティ間のトラフィック分離をサポートしています。CE ルータ上の各 VRF は、PE ルータ上の対応する VRF にマッピングされます。

マルチ VRF CE ネットワーク アーキテクチャの詳細については、次の URL にある Cisco Product Bulletin 1575 を参照してください。
http://www.cisco.com/warp/public/cc/pd/rt/2600/prodlit/1575_pp.pdf.

図 13-1　Cisco パケット データ サービス ノード（PDSN）/HA アーキテクチャの VRF-Lite

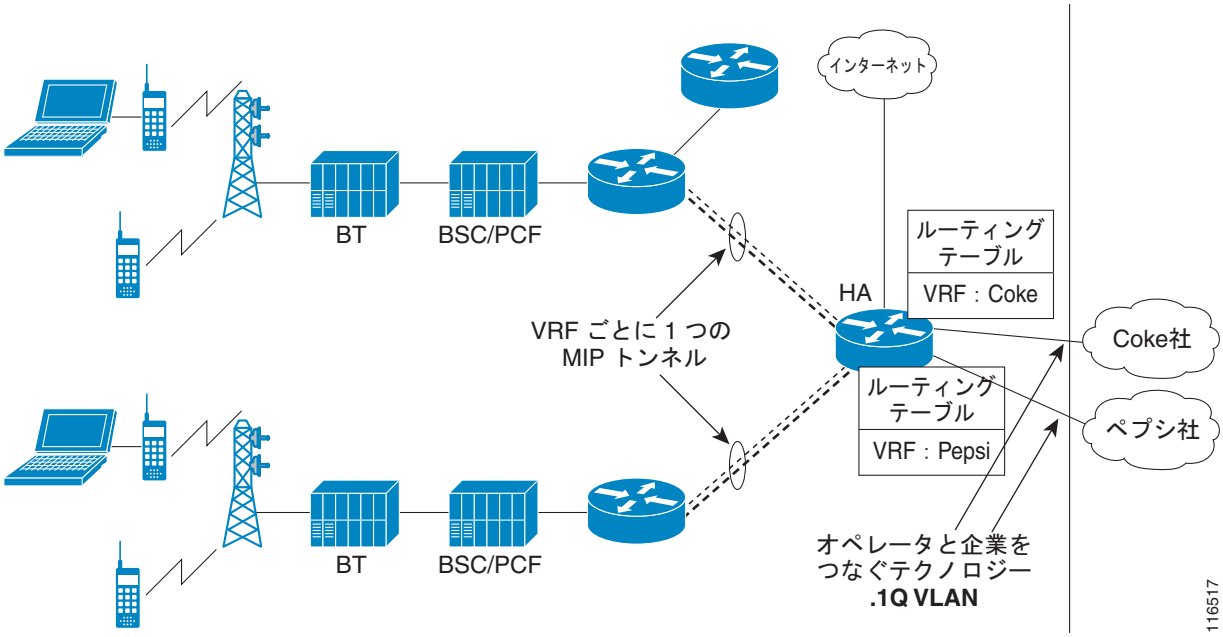

図 13-1 は、Packet Data Serving Node（PDSN; パケット データ サービス ノード）アーキテクチャ、および複数の異なるレルムおよび企業の HA への VRF-Lite ソリューションの適用方法、つまり、企業間のデータの分離方法を示しています。

VRF ソリューションの要点は、次のとおりです。

- ユーザのドメインまたはレルムに基づいて、ユーザの VRF を識別できます。
- 異なる企業に属している異なるモバイルが同じオーバーラップ IP アドレスを共有している場合、PDSN 経由で、モバイルにパケットを確実に配信できます。
- VRF 単位で IP アドレスおよびルーティング テーブルを管理できます。
- 企業またはドメイン単位で VRF を管理できます。
- VRF 単位で Authentication, Authorization and Accounting（AAA; 認証、許可、アカウンティング）認証およびアカウンティング グループをサポートできます。

レルムは、企業ネットワークを識別するために使用します。各レルムに 1 つの仮想 HA が設定されます。Network Access Identifier（NAI; ネットワーク アクセス識別子）は、モバイル IP Registration Request（RRQ; 登録要求）の一部で、PDSN および HA におけるモバイル IP ユーザの主要識別名です。仮想 HA の識別には、NAI のレルム部分が使用されます。モバイル ノードは、*username@company* の NAI 表記を使用し、*company* にサブスクライバのコミュニティを示すレルム名を識別します。

HA では、PDSN への異なる企業接続または VRF を示すために、複数の IP アドレスが使用されます。したがって、各レルムまたは VRF に、PDSN と HA 間の 1 つのモバイル IP トンネルが設定されます。

HA が 2 つの企業、"abc.com" および "xyz.com" に接続している場合、HA に 2 つの固有 IP アドレスが設定されます（通常、ループバック インターフェイスに設定されます）。PDSN には、"abc.com" に到達するアドレス LA1 への MoIP トンネル、および "xyz.com" に到達するアドレス LA2 へのもう 1 つの MoIP トンネルが設定されます。LA1 および LA2 は、ループバック インターフェイスに設定された IP アドレスです。

ホーム AAA Remote Authentication Dial-In User Service（RADIUS）サーバでは、NAI/ ドメイン コンフィギュレーションにより、PDSN は、FA-CHAP または HA-CHAP（MN-AAA 認証）のアクセス応答の一部として、LA1 を "xyz.com" 企業の HA の IP アドレスとして受信し、LA2 を "mnp.com" 企業の HA の IP アドレスとして受信します。

この機能は、HA ロード バランシングを提供する HA Server Load Balancing（HA-SLB; HA サーバ ロード バランシング）ソリューションと併用できます。

モバイル IP トンネルの確立

HA-SLB および VRF をイネーブルにした場合、モバイル IP フローが確立されるまでの手順は、次のとおりです。このコール フローには、2 つのモバイル ノード（MN-1 および MN-2）が存在し、それぞれ ENT-1 および ENT-2 の企業に属しています。

ステップ 1　モバイル IP RRQ が HA に到達すると、HA は入力 RRQ の NAI フィールドを読み取り、設定済み IP アドレスを選択し、この IP アドレスをトンネルの送信元アドレスとして使用して、PDSN に戻すモバイル IP トンネルを形成します。

ステップ 2　PDSN に送信される RRP の "Home-Agent address" フィールドが、上記の IP アドレスに変更されます。

ステップ 3　HA は、レルムに定義された VRF に対応するルーティング テーブルに、モバイルに割り当てられた IP アドレスに対応するホスト ルートを追加します。

ステップ 4　HA のトンネル エンドポイントも、VRF ルーティング テーブルに挿入されます。これにより、モバイルは、同じ HA 上の異なるレルム間で共通 IP アドレスを共有できます。

ステップ 5　MN-1 が、R-P セッションにより、HA アドレスを 0.0.0.0（ダイナミック HA）に設定したモバイル IP RRQ を、PDSN に送信します。

ステップ 6　PDSN は FA-CHAP を開始し、AAA にアクセス要求を送信します。

ステップ 7　AAA は、アクセス応答を戻します。戻される HA アドレスは、HA-SLB の IP アドレスです。

ステップ 8　PDSN は、MIP RRQ を HA-SLB に転送します。

ステップ 9　HA-SLB は、ロードに基づいて実 HA を判別し、HA1 に RRQ を転送します。

ステップ 10　HA-1 が MIP RRQ を受信します。HA-1 は、メッセージ内の NAI を解析し、ユーザのレルム（Ent-1 企業）に基づいてユーザの VRF を判別します。さらに、HA-CHAP（MN-AAA 認証）を実行して、モバイルに Ent-1 の IP アドレスを割り当てます。モバイルのバインディングを作成して、VRF、FIB などのルート テーブル内のルート エントリなど、VRF 特定のデータ構造を読み込みます。

ステップ 11　HA1 は PDSN に MIP RRP を送信し、PDSN と HA 間にモバイル IP トンネルを確立します。HA 上のトンネルのエンド ポイントは、LI-IP-1 になります（MIP RRQ の入力インターフェイスの IP アドレスではありません）。

RADIUS サーバ上の VRF マッピング

Release 3.0 では、VRF 機能が拡張され、RADIUS サーバ上で NAI から VRF へのマッピングを設定できます。この拡張により、モバイルから VRF へのマッピングは、次のように学習されます。HA は、モバイル IP 登録要求を受信すると、RADIUS アクセス要求を送信します。AAA サーバは、アクセス受諾により、RADIUS アトリビュート "cisco-avpair = mobileip:ip-vrf" 内の VRF 名、および RADIUS アトリビュート "cisco-avpair = mobileip-vrf-ha-addr" 内の対応する HA アドレスを、HA に送信します。HA は、この情報を使用し、バインディングを開いて、正しい VRF に関連付けます。これらのアトリビュートが AAA サーバからダウンロードされない場合は、ローカル設定の VRF（存在する場合）が使用されます。

また、HA が PDSN/FA により要求されたアドレスとは異なるアドレスを割り当てる必要がある場合には、コード 136 および新しい HA アドレスで登録応答を送信できるオプションがあります。コード 136 の登録応答を受信すると、モバイルは新しいアドレスを使用して、もう 1 つの登録要求を送信します。HA は、この要求を処理し、バインディングを開き、登録応答（success）を送信することにより、登録プロセスを完了します。

VRF 機能の制約事項

VRF 機能には、次の制約事項があります。

- HA 単位でサポートされる VRF 数は、最大 130 です。
- HA MIB は、VRF 情報ではアップデートされません。

レルム単位の認証およびアカウンティング サーバ グループ

各レルムに、個別の認証およびアカウンティング グループを指定できます。HA は、ユーザのレルムに基づいて、HA 上のそのレルムに指定された認証グループに基づく AAA 認証サーバを選択します。同様に、レルムにアカウンティング グループが指定されている場合、ユーザのレルムに基づいて、AAA アカウンティング サーバが選択されます。

（注）　この機能は、VRF 機能と併用できます。

HA の VRF の設定

HA 上に VRF を設定するには、次の作業を実行します。

	コマンド	目的
ステップ 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*]]	ドメイン *@xyz.com* の VRF を定義します。 また、VRF に対応する HA の IP アドレスを、MOIP トンネルの終端ポイントに定義します。 HA の IP アドレスは、ボックス上のルーティング可能な IP アドレスにする必要があります。 オプションで、VRF 単位の AAA アカウンティングおよび認証サーバ グループを定義できます。 AAA アカウンティング サーバ グループを定義すると、レルムのユーザのすべてのアカウンティング レコードが、指定したグループに送信されます。 AAA 認証サーバ グループを定義すると、HA-CHAP（MN-AAA 認証）が、そのグループに定義されているサーバに送信されます。

	コマンド	目的
ステップ 2	Router(config)# **ip vrf** *vrf-name* description VRF for domain1 rd 10:1	ボックス上に VRF を定義します。 VRF の説明。 VRF のルータ記述子。ルート識別子を指定して、VRF テーブル作成します。 **（注）** 各 HA CPU 上で、各ドメインに 1 つの VRF を設定する必要があります。
ステップ 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	各 VRF の IP アドレスを設定するループバック インターフェイスを定義します。これらのアドレスは、レルムのモバイル IP トンネルの送信元 IP アドレスとして使用されます。 IP アドレスに設定するマスクは、VRF ルーティング テーブルで使用されます。ホスト マスク（255.255.255.255）またはブロードキャスト マスク（0.0.0.0）は、設定しないでください。

次に、VRF のユーザ プロファイルを設定する例を示します。

```
[ //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 の設定例

次に、MWAM HA 上での VRF サポートの設定例を示します。

```
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
```

HA 冗長性を使用した VRF の設定例

次に、HA 冗長性と VRF を使用した Cisco HA の設定例を示します。次の手順が必要です。

ステップ 1　パブリッシュした HA IP アドレスについて、標準 Hot Standby Routing Protocol（HSRP; ホット スタンバイ ルーティング プロトコル）および HA 冗長性を設定します。

ステップ 2　ループバック上の IP アドレス（またはトンネル エンド ポイントの任意の他のインターフェイス IP アドレス）を設定するのではなく、HSRP インターフェイス上に、セカンダリのスタンバイ IP アドレスとして設定します。

ステップ 3　IP モバイルを冗長設定するために、VRF トンネル ポイント サブネットに仮想ネットワークを追加します。

ステップ 4　VRF 関連コマンドを設定します。

ステップ 5　アクティブ HA からスタンバイ HA へのバインディング アップデート メッセージには NAI が含まれているので、スタンバイ HA は、メッセージ内の NAI のドメインに基づいて、適切な VRF を使用したバインディングを作成できます。

アクティブ 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
```

スタンバイ 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
```