



## CHAPTER 4

# HA でのホーム アドレス割り当て

この章では、Cisco Mobile Wireless Home Agent がモバイル ノードにホーム アドレスを割り当てる方法、各種アドレス タイプについて説明し、設定の詳細および設定例を示します。

この章は、次の内容で構成されています。

- 「ホーム アドレス割り当て」 (P.4-1)
- 「アドレス割り当て機能」 (P.4-1)
- 「スタティック IP アドレス」 (P.4-5)
- 「ダイナミック HA 割り当て」 (P.4-7)
- 「ダイナミック IP アドレス」 (P.4-7)
- 「設定例」 (P.4-9)

## ホーム アドレス割り当て

Home Agent (HA) は、モバイル IP 登録時に受信したユーザ NAI に基づいて、モバイル ノードにホーム アドレスを割り当てます。モバイル ステーションには、スタティックまたはダイナミックに IP アドレスを割り当てることができます。HA は、スタティック割り当てかダイナミック割り当てかを問わず、同じ IP アドレスで異なる NAI を同時に登録することを認めません。

## アドレス割り当て機能

セッション上書き機能を備えたアドレス割り当て機能により、古いセッションを削除して、デバイスに新しいセッションを確立できます。デバイスの MAC アドレスは変更されませんが、NAI (外側の EAP ID から取得される可能性あり) と Home Address (HoA; ホーム アドレス) は変更されることがあります。

NAI レルム (つまり、Registration Request (RRQ; 登録要求) の [Home Address] フィールドではない) が、スタティック IP プールまたはダイナミック IP プールのアドレス管理が使用されているかどうかを判別します。

Home Agent Release 5.0 では、CMIPv4 および PMIPv4 がサポートされます。アドレス管理は、登録内の MAC アドレスに基づいて実行されます。

MACアドレスを持つRRQとMACアドレスを持たないRRQに適用される条件を次に示します (PMIPv4 デバイス ID 拡張機能で提供される)。

- RRQにMACアドレス (CMIP) が含まれない場合、セッションはR4.0マトリクスに基づいて管理されます。
- RRQにMACアドレス (PMIP) が含まれている場合、セッションはR5.0マトリクスに基づいて管理されます。
- CMIPおよびPMIP間にハンドオフはありません。
- CMIPユーザとPMIPユーザのドメインは同じではありません。
- CMIPユーザとPMIPユーザのホームアドレスは同じではありません。VPN Routing and Forwarding (VRF; VPNルーティングおよびフォワーディング) が使用されていて、CMIPユーザとPMIPユーザが異なるVRF内にある場合、HoAアドレスが同じである場合があります。

### クライアントベースのモバイルIPv4

CMIPv4はHA Release 4.0のアドレス割り当て方法に基づいています。次に設定例を示します。

#### スタティックIPプール:

```
ip mobile host nai @domain static-address local-pool pool_001
```

authentication, authorization, and accounting (AAA; 認証、認可、アカウントリング)はHoAを割り当て、HoAは初回登録時はMIP RRQで設定されます。

#### スタティックアクセスを許可するダイナミックIPプール:

```
ip mobile host nai @domain static-address local-pool pool_002 address pool local pool_002
```

HoAは初回登録時はMIP RRQで送信され、HAはHoAを使用してセッションを確立します。HoAが初回登録時にMIP RRQで送信されない場合、HAはHoAを割り当てて、セッションを確立します。

#### ダイナミックIPプール:

```
ip mobile host nai @domain address pool local pool_003
```

HAはHoAを割り当てます。HoAは初回登録時はMIP RRQで設定されません (0.0.0.0)。次に示すプールタイプを使用した既存のアドレス管理について以降で説明します。

### プロキシモバイルIPv4

PMIPv4はHA Release 5.0のアドレス割り当て方法に基づいています。HoA上書き機能を備えたアドレス割り当て機能により、古いセッションを削除して、デバイスに新しいセッションを確立できます。デバイスのMACアドレスは変更されませんが、NAI (外側のEAP IDから取得される可能性あり)とHoAは変更されることがあります。

NAIレルム (RRQの[Home Address]フィールドではない)が、スタティックIPプールまたはダイナミックIPプールのアドレス管理が使用されているかどうかを判別します。次に設定例を示します。

#### スタティックIPプール:

```
ip mobile host nai @domain static-address local-pool pool_001
```

AAAはHoAを割り当てます。HoAは初回登録時はMIP RRQで設定されません。

**ダイナミック IP プール :**

```
ip mobile host nai @domain address pool local pool_003
```

HA は HoA を割り当てます。HoA は初回登録時は MIP RRQ で設定されるか、または設定されません (0.0.0.0)。

古いバインディングの削除をイネーブルにするには、次の作業を実行します。

	コマンド	目的
ステップ1	Router(config)# <b>ip mobile home-agent binding-overwrite</b>	HA、MAC アドレス、および登録要求の NAI 情報によって識別される古いバインディングの削除をイネーブルまたはディセーブルにします。
ステップ2	router# <b>debug ip mobile host mac H.H.H</b>	MAC アドレスベースのデバッグをイネーブルにします。



(注) VRF サポートに複数の HA IP アドレスが使用されていないため、失効メッセージに NAI 拡張機能を含める必要はありません。

アドレス割り当て機能の使用方法を示す 3 つの設定例を次に示します。

**スタティック IP プールの HA 設定を使用した MAC ベースのセッション****HA Config**

```
ip local pool cisco-static-pool 5.1.0.1 5.1.1.0

ip mobile host nai @cisco.com static-address local-pool
cisco-static-pool interface Null0 aaa load-sa
```

**FA Config**

```
simulator mip mn profile 1
  description ctc-mac-static
  registration lifetime 65535
  registration retries 0
  registration flags 42
  revocation flags 00
  home-agent 81.81.81.81
  home-address 5.1.0.1
  secure home-agent spi 100 key ascii cisco
  nai cisco-%f@cisco.com
  pmip skip subtype 2 idtype mac
  no extension fa-challenge
  no extension mn-fa
  no extension nat traversal
  extension revocation
```

**ダイナミック IP プールを使用した MAC ベースのセッション****HA Config**

```
ip local pool cisco-pool 5.1.0.1 5.1.1.0

ip mobile host nai @cisco.com address pool local cisco-pool
interface Null0 aaa load-sa
```

**FA Config**

```

simulator mip mn profile 1
  description ctc-mac-static
  registration lifetime 65535
  registration retries 0
  registration flags 42
  revocation flags 00
  home-agent 81.81.81.81
  home-address 5.1.0.1
  secure home-agent spi 100 key ascii cisco
  nai cisco-%f@cisco.com
  pmip skip subtype 2 idtype mac
  no extension fa-challenge
  no extension mn-fa
  no extension nat traversal
  extension revocation

```

**既存のバインディングの上書き****HA Config**

```

ip mobile home-agent binding-overwrite

ip local pool cisco-pool 5.1.0.1 5.1.1.0

ip mobile host nai @cisco.com address pool local cisco-pool
interface Null0 aaa load-sa

```

**FA Config**

```

simulator mip mn profile 3
  registration lifetime 65535
  registration retries 0
  registration flags 42
  revocation flags 00
  home-agent 81.81.81.81
  secure home-agent spi 100 key ascii cisco
  secure aaa spi 2 key ascii cisco
  nai cisco-%f@cisco.com
  pmip skip subtype 2 idtype mac
  no extension mn-aaa
  no extension mn-fa
  no extension nat traversal
  extension revocation

simulator mip mn profile 4
  registration lifetime 65535
  registration retries 0
  registration flags 42
  revocation flags 00
  home-agent 81.81.81.81
  home-address 5.0.0.2 0
  secure home-agent spi 100 key ascii cisco
  secure aaa spi 2 key ascii cisco
  nai pepsi-%f@cisco.com
  pmip skip subtype 2 idtype mac
  no extension mn-aaa
  no extension mn-fa
  no extension nat traversal
  extension revocation

```

```
simulator mip scenario 3
mn profile 3
fa 2.2.2.200
mn id 20

simulator mip scenario 4
mn profile 4
fa 2.2.2.200
mn id 21
```

## スタティック IP アドレス

スタティック IP アドレスは、モバイルステーションに前もって割り当てられたアドレスであり、モバイルデバイスにすでに設定されていることもあります。HA はパブリック IP アドレスでも、プライベートドメインのアドレスでも、スタティックアドレスをサポートします。



(注) モバイル IP サービスにプライベートアドレスを使用するには、PDSN/FA と HA 間にリバーストンネリングが必要です。

モバイルユーザは登録要求メッセージで、設定済みアドレスまたは使用可能アドレスを非ゼロのホームアドレスとして提案します。HA は、このアドレスを受け付けることもあれば、登録応答メッセージで別のアドレスを返すこともあります。HA は、ホーム AAA サーバまたは Dynamic Host Configuration Protocol (DHCP) サーバにアクセスすることによって、IP アドレスを取得できます。ホーム AAA サーバは、ローカルプール名を返すこともあれば、単一の IP アドレスを返すこともあります。モバイル IP 登録が成功すると、ユーザはモバイル IP ベースのサービスを利用できるようになります。

## NAI を使用しないスタティック ホーム アドレッシング

最初のモバイル IP 仕様でサポートしていたのは、モバイルノードのスタティックアドレッシングだけでした。ホーム IP アドレスが認証の「ユーザ名」の部分として使用されていました。スタティックアドレッシングは、各デバイスがどこからネットワークに接続しようと、常に同じアドレスが維持されるので、便利な場合があります。この場合、ユーザは DNS をアップデートしたり、他の形式のアドレス形式を使用しなくても、モバイル終端サービスを実行できます。また、スタティックアドレッシングではホームアドレスと HA が常に同じなので、Mobile Node (MN; モバイルノード) の管理が容易です。しかし、スタティックアドレッシングの場合、アドレス割り当てを手動で処理し、HA と MN の両方をアップデートしなければならないので、プロビジョニングとメンテナンスははるかに困難になります。設定例を示します。

```
router (config)# ip mobile host 10.0.0.5 interface FastEthernet0/0
router (config)# ip mobile host 10.0.0.10 10.0.0.15 interface FastEthernet0/0
router (config)# ip mobile secure host 10.0.0.12 spi 100 key ascii secret
```

## NAI を使用するスタティック ホーム アドレッシング

スタティック ホーム アドレッシングを NAI と組み合わせて使用することによって、NAI ベースの認証およびその他のサービスをサポートすることもできます。また、単一ユーザに同一デバイスまたは複数のデバイス上で複数のスタティック IP アドレスを使用させながら、なおかつ 1 つの AAA レコードとセキュリティ アソシエーションを維持することもできます。ユーザがアドレスを使用して認可を受けてからでなければ、登録は受け付けられません。アドレスはローカルで認可することも、AAA サーバを使用して認可することもできます。異なる NAI のバインディングとすでに関連付けられているアドレスを MN が要求した場合、HA はコマンドが設定されていない限り、プールに含まれている別のアドレスを返そうとします。

設定例を示します。

```
router (config)# ip mobile home-agent reject-static-addr
```

## ローカル認可

スタティック アドレスの認可は、コンフィギュレーション コマンドを使用して MN ベースで、またはレルム ベースで行うことができます。MN ベースの設定には、*user* または *user@realm* の形式で具体的な NAI を定義する必要があります。レルム ベースの設定には、*@realm* の形式で総称 NAI を定義する必要があります。ローカル プールの指定だけが認められます。

設定例を示します。

```
router (config)# ip local pool static-pool 10.0.0.5 10.0.0.10
router (config)# ip mobile host nai user@staticuser.com static-address 10.0.0.1 10.0.0.2
interface FastEthernet0/0
router (config)# ip mobile host nai user@staticuser.com static-address local-pool
static-pool interface FastEthernet0/0
router (config)# ip mobile host nai @static.com static-address local-pool static-pool
interface FastEthernet0/0
```

## AAA の認可

認可されたアドレスまたはローカル プール名を AAA サーバに保管することもできます。各ユーザには、AAA サーバで設定された **static-ip-addresses** アトリビュートまたは **static-ip-pool** アトリビュートが必要です。コマンドラインでスタティック アドレスを設定する場合と異なり、**static-ip-addresses** アトリビュートは返すことのできるアドレスの数に制限がありません。

設定例を示します。

HA の設定

```
router (config)# ip local pool static-pool 10.0.0.5 10.0.0.10
router (config)# ip mobile host nai user@staticuser.com interface FastEthernet0/0 aaa
router (config)# ip mobile host nai @static.com interface FastEthernet0/0 aaa
```

Remote Authentication Dial-In User Service (RADIUS) のアトリビュート

Cisco-AVPair = "mobileip:static-ip-addresses=10.0.0.1 10.0.0.2 10.0.0.3"

Cisco-AVPair = "mobileip:static-ip-pool=static-pool"

## ダイナミック HA 割り当て

次の条件が存在する場合、CDMA2000 ネットワークでは HA のダイナミック割り当てが可能です。

最初の条件は、HA が HA フィールドに 0.0.0.0 の値が指定されたモバイル IP 登録要求を受信することです。認証/認可時に、PDSN が HA の IP アドレスを取得します。PDSN はさらに、このアドレスを使用して HA に登録要求を転送します。ただし、登録要求の実際の HA アドレス フィールドはアップデートされません。

HA は登録応答を送信し、HA フィールドに専用の IP アドレスを格納します。この時点で受信する再登録要求は、HA フィールドに HA の IP アドレスが入ります。

第2の条件は、PDSN/FA の機能であり、それがここで含まれていないと完全ではありません。この場合、AAA サーバを使用してダイナミック HA 割り当て機能を実行します。ネットワーク トポロジに応じて、ローカル AAA サーバまたはホーム AAA サーバがこの機能を実行します。アクセス サービス プロバイダーが ISP でもある場合、HA はアクセス プロバイダーのネットワークに配置されます。このサービス環境では、ローカル AAA サーバが HA の割り当て機能を実行します。AAA サーバはアクセス要求メッセージで受け取ったユーザ NAI に基づいて、PDSN へのアクセス応答メッセージで選択した HA のアドレスを返します。

HA アドレス プールは通常、AAA サーバで設定されます。アクセス プロバイダーが ISP として機能する場合、ローカル AAA サーバで複数の HA プールを設定できますが、これはモバイル IP サービスまたはプロキシ モバイル IP サービスのサポート対象となるドメインのある SLA に依存します。ユーザ NAI 選択条件としてラウンドロビンまたはハッシュ アルゴリズムを使用すると、AAA サーバで HA 選択手順を設定できます。

PDSN/FA は HA に登録要求を送信しますが、MIP RRQ の HA フィールドに IP アドレスは含まれません (0.0.0.0)。PDSN は AAA から IP アドレスを受け取った時点で、MIP RRQ を更新せず、その RRQ を取得した HA アドレスに転送します。PDSN は MN-HA SPI およびキー値 ([Home Agent] フィールドで指定された HA の IP アドレスが含まれる) が不明なので、MIP RRQ を変更できません。ネットワーク トポロジに応じて、ローカル AAA サーバまたはホーム AAA サーバがこの機能を実行します。HA がアクセス プロバイダーのネットワークに配置されている場合、ローカル AAA サーバが HA の割り当て機能を実行します。さらに、モバイル IP サービスまたはプロキシ モバイル IP サービスのサポート対象となるドメインのある SLA に応じて、ローカル AAA サーバで複数の HA プールを設定できます。

## ダイナミック IP アドレス

パケット データ サービスにアクセスするモバイル ステーションで、ホーム IP アドレスを設定する必要はありません。モバイル ユーザは、登録要求メッセージですべてゼロのホーム アドレスを提出することによって、ダイナミック割り当てのアドレスを要求できます。HA がホーム アドレスを割り当て、登録応答メッセージで MN に返します。HA はホーム AAA サーバにアクセスすることによって IP アドレスを取得します。AAA サーバは、ローカル プール名または単一の IP アドレスを返します。登録が成功すると、ユーザはモバイル IP ベースのサービスを利用できるようになります。

## 固定アドレッシング

各 NAI に固定アドレスを指定して HA を設定できます。固定アドレスは、登録するたびに MN に割り当てられます。この場合、ユーザはスタティック アドレッシングのすべての利点を生かしながら、MN の設定を簡素化できます。固定アドレッシングは、大規模展開には推奨できません。全ユーザ メンテナンスを実行するために、HA 設定をアップデートしなければならないからです。

設定例を示します。

```
router# ip mobile host nai user@realm.com address 10.0.0.1 interface FastEthernet0/0
```

## ローカルプール割り当て

ローカルプールを割り当てるには、HA上で1つまたは複数のアドレスプールを設定する必要があります。HAは先着順方式で、プールからアドレスを割り当てます。MNはHAにアクティブバインディングがある限り、アドレスを維持します。MNは割り当てられたアドレスまたは0.0.0.0をホームアドレスとしたRRQを送信することによって、バインディングをアップデートできます。バインディングが期限切れになると、ただちにアドレスがプールに返されます。



(注)

現在、ピアツーピアHA冗長モデルでローカルプール割り当てを使用することはできません。設定できるローカルプール数を制限するものは、ルータ上で使用できるメモリだけです。

設定例を示します。

```
router (config)# ip local pool mipool 10.0.0.5 10.0.0.250
router (config)# ip mobile host nai @localpool.com address pool local mipool
virtual-network 10.0.0.0 255.255.255.0
```

## DHCP割り当て

DHCPは、デスクトップコンピュータのIPアドレス割り当てにすでに広く用いられている方式です。IOSモバイルIPは、IOSにすでにあるDHCPプロキシクライアントを活用して、DHCPサーバにホームアドレスを割り当てさせます。NAIはClient-IDオプションで送信され、ダイナミックDNSサービスの提供に使用できます。

設定例を示します。

```
router (config)# ip mobile host nai @dhcppool.com address pool dhcp-proxy-client
dhcp-server 10.1.2.3 interface FastEthernet 0/0
```



(注)

現在、ピアツーピアHA冗長モデルでDHCPを使用することはできません。

## AAAからのダイナミックアドレッシング

AAAからのダイナミックアドレッシングを使用すると、MNまたはHAでアドレッシングを維持する手間をかけなくても、MNの固定アドレッシング、セッション単位のアドレッシング、またはその両方をサポートできます。AAAサーバは特定のアドレス、ローカルプール名、またはDHCPサーバアドレスを返すことができます。AAAサーバを使用して特定のアドレスを返す場合は、RADIUSデータベースのNAIエントリでアトリビュートとしてホームアドレスを設定することも、または使用するAAAサーバの機能によっては、プールからホームアドレスを割り当てることもできます。AAAサーバは、HAで設定されているローカルプールの名前またはDHCPサーバのIPアドレスを返すこともできます。

設定例を示します。

HA上:

```
router (config)# ip local pool dynamic-pool 10.0.0.5 10.0.0.10
router (config)# ip mobile host nai user@staticuser.com interface FastEthernet0/0 aaa
router (config)# ip mobile host nai @static.com interface FastEthernet0/0 aaa
```

AAAアドレス割り当て:

```
Cisco-AVPair = "mobileip:ip-address=65.0.0.71"
```

AAAローカルプールアトリビュート:

```
Cisco-AVPair = "mobileip:ip-pool=dynamic-pool"
```



```
AAA DHCP サーバ アトリビュート :  
Cisco-AVPair = "mobileip:dhcp-server=10.1.5.10"
```



(注) Framed-IP-Address アトリビュートもサポートされます。

## 同一 NAI に複数のスタティック アドレスを使用する場合のアドレス割り当て

Cisco HA は、同じ NAI に複数のスタティック アドレスを使用する、マルチ モバイル IP 登録をサポートします。これは、ホーム AAA サーバまたは DHCP サーバで static-ip-address pool (複数可) を設定することによって実現されます。モバイル ユーザから登録要求メッセージを受信すると、HA はホーム AAA にアクセスして認証を行い、さらに通常は、IP アドレスを割り当てます。モバイル ユーザが提供した NAI はホーム AAA に送信されます。ホーム AAA サーバは、その NAI に対応するスタティック IP アドレスまたはスタティック IP プール名のリストを返します。

## 同一 NAI に異なるモバイル端末を使用する場合のアドレス割り当て

2つの異なるモバイルから同じ NAI を使用して登録を行う場合、動作は次のようになります。

- 両方のケースでスタティック アドレス割り当てを使用する場合、それぞれ独立したケースと見なされます。
- 両方のケースでダイナミック アドレス割り当てを使用する場合、2番目の登録が最初の登録に取って代わります。
- 最初の登録にスタティックを使用し、2番目の登録にダイナミックを使用する場合、ダイナミック アドレス割り当てがスタティック アドレス割り当てに取って代わります。
- 最初の登録にダイナミックを使用し、2番目にスタティックを使用する場合は、それぞれ独立したケースと見なされます。

さらに、2つの異なる HA ながら、同じ NAI を使用する同じモバイルから発生した2つのフローは、別々のケースと見なされます。

# 設定例

## DHCP プロキシ クライアント設定

### アクティブ HA の設定

```
no service pad  
service timestamps debug uptime  
service timestamps log uptime  
no service password-encryption  
!  
hostname mwt10-7206b  
!  
aaa new-model  
!  
aaa authentication ppp default local group radius  
aaa authorization config-commands  
aaa authorization ipmobile default group radius  
aaa authorization network default group radius
```

```
aaa session-id common
!
ip subnet-zero
ip cef
!
interface Loopback0
ip address 10.0.0.1 255.255.255.255
interface Ethernet2/0
description to PDSN/FA
ip address 10.0.0.2 255.0.0.0
no ip route-cache
no ip mroute-cache
duplex half
standby ip 10.0.0.4
standby priority 110
standby preempt delay sync 100
standby name cisco
!
interface Ethernet2/2
description to AAA
ip address 172.16.1.8 255.255.0.0
no ip route-cache
no ip mroute-cache
duplex half
!
router mobile
!
ip classless
no ip http server
ip pim bidir-enable
ip mobile home-agent
ip mobile home-agent redundancy
ip mobile virtual-network 10.0.0.0 255.0.0.0
ip mobile host nai user01@cisco.com address pool dhcp-proxy-client
dhcp-server 10.0.0.101 virtual-network 10.0.0.0 255.0.0.0
ip mobile secure home-agent 10.0.0.3 spi 100 key ascii redundancy
algorithm md5 mode
prefix-suffix
!
ip mobile virtual-network 10.0.0.0 255.0.0.0
ip mobile host nai user01@cisco.com address pool dhcp-proxy-client
dhcp-server 10.0.0.101 virtual-network 10.0.0.0 255.0.0.0
radius-server host 172.16.0.2 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key cisco
call rsvp-sync
!
mgcp profile default
!
dial-peer cor custom
!
gatekeeper
shutdown
!
line con 0
line aux 0
line vty 0 4
!
end
```

## スタンバイ HA の設定

```
no service pad
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
!
hostname mwt10-7206b
!
aaa new-model
!
aaa authentication ppp default local group radius
aaa authorization config-commands
aaa authorization ipmobile default group radius
aaa authorization network default group radius
aaa session-id common
!
ip subnet-zero
ip cef
!
interface Loopback0
ip address 10.0.0.2 255.255.255.255
interface Ethernet2/0
description to PDSN/FA
ip address 10.0.0.3 255.0.0.0
no ip route-cache
no ip mroute-cache
duplex half
standby ip 10.0.0.4
standby name cisco
!
interface Ethernet2/2
description to AAA
ip address 172.16.1.7 255.255.0.0
no ip route-cache
no ip mroute-cache
duplex half
!
router mobile
!
ip local pool ha-pool 10.0.0.1 10.0.0.255
ip classless
no ip http server
ip pim bidir-enable
ip mobile home-agent
ip mobile home-agent redundancy
ip mobile secure home-agent 10.0.0.2 spi 100 key ascii redundancy
algorithm md5 mode
prefix-suffix
ip mobile virtual-network 10.0.0.0 255.0.0.0
ip mobile host nai user01@cisco.com address pool dhcp-proxy-client
dhcp-server 10.0.0.101 virtual-network 10.0.0.0 255.0.0.0
!
radius-server host 150.2.0.2 auth-port 1645 acct-port 1646
radius-server retransmit 3
radius-server key cisco
call rsvp-sync
!
mgcp profile default
!
dial-peer cor custom
!
gatekeeper
```

```
shutdown
!  
line con 0  
line aux 0  
line vty 0 4  
!  
end
```