CHAPTER 9

ダイナミック ドメイン ネーム サーバ（DNS）アップデート

この章では、Domain Name Server（DNS; ドメイン ネーム サーバ）アップデートの方法、サーバのアドレス割り当て、およびこれらの機能の設定方法について説明します。

この章の内容は、次のとおりです。

IP 到達可能性

TIA/EIA/IS-835-D には、ホーム AAA サーバと Home Agent（HA）を使用したダイナミック DNS アップデートの方法が説明されています。AAA による DNS アップデートは簡易 IP およびモバイル IP の両方のサービスに適用できますが、HA による DNS アップデートを適用できるのはモバイル IP サービスだけです。次に、HA 上の IP 到達可能性の機能について説明します。

HA は、初回の登録要求を受信すると、ホーム Remote Authentication Dial-In User Service（RADIUS）サーバに RADIUS アクセス要求を送信します。RADIUS サーバが HA ベースの DNS アップデートを要求するように設定されていれば、ホーム RADIUS サーバは、HA に戻す RADIUS Access-Accept メッセージに DNS-Update-Required アトリビュートを付加します。初回のモバイル IP 登録に成功すると、HA は DNS サーバに DNS アップデート メッセージを送信し、MS のリソース レコードを追加します。HA は、DNS アップデート メッセージをプライマリおよびセカンダリ（存在する場合）の DNS サーバに送信します。

HA が、ライフタイム タイマーがゼロに設定された Mobile IP Registration Request（RRQ; 登録要求）を受信すると、モバイル IP のライフタイムが期限切れになった場合、または管理操作によって MS のモビリティ バインディングが無効にされた場合には、HA は DNS サーバに、関連リソース レコードを削除するための DNS アップデート メッセージを送信します。以降のコマンドは、特定のレルムについて、HA 上の IP 到達可能性をイネーブルにします。

（注） 再登録の場合は、その都度、DNS アップデートは送信されません。

（注）　この機能は、プロキシ モバイル IP フローでも同様にサポートされます。

次に、モバイル登録シナリオにおける、HA 上の IP 到達可能性のコール フローを示します。

1. HA が、Packet Data Serving Node（PDSN）/Foreign Agent（FA; 外部エージェント）から登録要求を受信します。
2. HA から RADIUS サーバにアクセス要求が送信されます。HA により、DNS Server Update Capability VSA が付加されます。
3. RADIUS サーバから、DNS Update Required VSA が付加されたアクセス受諾が送信されます。
4. HA から PDSN/FA に登録応答が送信されます。HA が冗長設定されている場合、アクティブ HA とスタンバイ HA のバインディング作成が同期化されます。
5. HA によりバインディングが作成され、DNS サーバに DNS アップデート要求メッセージが送信されます。
6. DNS サーバにより、NAI の DNS エントリが作成され、HA に DNS アップデート応答メッセージが戻されます。

次に、モバイル登録解除シナリオにおける、HA 上の IP 到達可能性のコール フローを示します。

1. HA が、PDSN/FA からライフタイムがゼロの登録要求を受信します。
2. SA がローカルに保管されていない場合、HA から RADIUS サーバにアクセス要求が送信されます（オプション）。
3. RADIUS サーバからアクセス受諾が戻されます（オプション）。
4. HA により、バインディングが削除されます。HA から PDSN/FA に、登録応答が戻されます。HA が冗長設定されている場合、アクティブ HA とスタンバイ HA のバインディング削除が同期化されます。
5. HA から DNS サーバに、DNS エントリを削除するための DNS アップデート要求メッセージが送信されます。
6. DNS サーバにより、NAI の DNS エントリが削除されます。DNS サーバから HA に、DNS アップデート応答メッセージが戻されます。

IP 到達可能性の設定

特定のレルムでこの機能をイネーブルにするには、次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router(config)# ip name-server x.x.x.x`	名前とアドレスの解決に使用する 1 つ以上のネームサーバのアドレスを指定します。
ステップ 2	`Router(config)# ip mobile realm @ispxyz1.com dns dynamic-update method word`	特定のレルムで DNS アップデートの手順をイネーブルにします。*word* に、ダイナミック DNS アップデート方式の名前を入力します。
ステップ 3	`Router(config)# ip mobile realm realm dns server primary dns server address secondary dns server address`	DNS サーバのアドレスをローカルで設定できます。

この機能によるバインディングがイネーブルかどうかを確認するには、次のコマンドを使用します。

	コマンド	目的
ステップ 1	`Router# show ip mobile binding`	モビリティ バインディング テーブルを表示します。

次に、レルムに IP 到達可能性を設定する例を示します。

```
ip ddns update method sit-ha2-ddns2
 DDNS both
ip mobile realm @ispxyz2.com dns dynamic-update method sit-ha2-ddns2
```

DNS サーバのアドレスの割り当て

IS835D に、モバイル IP 登録応答で、ホーム DNS サーバのアドレスを Normal Vendor Specific Extension（NVSE）としてモバイルにプッシュする方法が定義されています。この手順により、モバイル ステーションで、ホーム ドメインのプライマリおよびセカンダリ DNS サーバのアドレスを学習できます。

RADIUS サーバは、モバイル認証中に、HA へのアクセス応答に DNS Server VSA を付加します。HA は、DNS Server VSA から DNS サーバの NVSE を作成し、モバイル IP 登録応答に付加します。認証時に DNS Server VSA を受信しない場合、HA 上で DNS サーバのアドレスがローカルに設定されていれば、ローカル設定から DNS サーバの NVSE が作成され、モバイル IP 登録応答に付加されます。

DNS Server VSA および DNS Server NVSE は、プライマリとセカンダリの DNS IP アドレスを保持します。

HA が冗長モードで配置されている場合、スタンバイ HA に DNS Server VSA が同期化されます。

特定のレルムでこの機能をイネーブルにするには、次のコマンドを使用します。

ip mobile realm *realm* **dns server assign**

ip name-server x.x.x.x

DNS サーバのアドレスをローカルで設定するには、次のコマンドを使用します。

ip mobile realm ***realm*** **dns server** ***primary dns server address secondary dns server address***

この機能によるバインディングがイネーブルかどうかを確認するには、**show ip mobile binding** コマンドを使用します。

（注）　DNS サーバのアドレスがローカルで設定されていて、かつ AAA からもダウンロードされた場合には、HA 上のローカル設定アドレスが優先されます。

HA 上での DNS リマッピングのサポート

Cisco Mobile Wireless Home Agent Release 5.0 で HA は HA でサポートされるサブスクライバの数に調整してステートフル Network Address Translation（NAT; ネットワーク アドレス変換）機能をサポートします。これによって特定のプロトコルとポートが一致するため、ユーザからの DNS 要求を認識できます。認識されると、宛先 IP アドレスが変更されるため、DNS 要求がオペレータによって定義された IP アドレスに送信されます。同様に、応答には要求に応答した DNS サーバのソース IP アドレスが含まれます。これは、その後、サブスクライバによって使用される元のアドレスにマッピングされます。

Mobile Node（MN; モバイル ノード）は、初めに、セッションの設定中にアクセスしたネットワークの DNS サーバ IP アドレスで設定されます。その後、MN はホーム ネットワーク経由で宛先に到達できないこの IP アドレス（つまり、HA へのリバース トンネル）に DNS メッセージを送信して、ホスト名を解決しようとします。この問題に対処するために、HA 5.0 では「DNS リマッピング」機能が追加されました。

モニタリングでの DNS リダイレクション

DNS リマッピングの問題の 1 つは、プライマリ DNS サーバに障害が発生すると、DNS クエリーが HA で設定されたセカンダリ DNS サーバでリダイレクトされないことです。さらに、HA は DNS クエリーの宛先アドレスを HA 上の設定された DNS アドレスにリマッピングするために NAT 設定を使用しません。

既存の DNS リマッピング機能上の DNS リダイレクション機能では、HA は HA でサポートされるサブスクライバの数に調整してステートフル NAT 機能をサポートできます。

この機能サポートの一環として、HA はアベイラビリティのために DNS サーバのモニタリングと同様に宛先アドレスのリマッピングに対処するようになりました。HA は、どちらが使用可能かに応じて、MN からプライマリまたはセカンダリ DNS サーバの設定された IP アドレスへの DNS メッセージの宛先 IP アドレスを書き直します。プライマリとセカンダリの両方の DNS が使用可能な場合、プライマリがアクティブ DNS の役割を果たします。プライマリ DNS サーバが使用できない場合、HA は HA 上で設定されたセカンダリ DNS サーバへの宛先 IP アドレスのリマッピングを開始します。

このソリューションによって、プライマリ DNS サーバに障害が発生した場合の潜在的な問題を解決できます。DNS クエリーは HA 上で設定されたセカンダリ DNS サーバにリダイレクトする必要がありません。

HA は IP SLA の機能を使用して、HA からプライマリとセカンダリの DNS サーバのアベイラビリティを検出します。IP SLA はモニタリングされているノードの接続についての情報を Control Plane（CP; コントロール プレーン）にしか通知しないため、CP は（IPC 経由で）すべての Traffic Plane（TP; トラフィック プレーン）に CP が IP SLA から受信した接続についての情報を通知します。

HA がプライマリ DNS サーバが使用できることを検出した場合は、プライマリ DNS サーバがアクティブ DNS サーバとして使用され、トンネル上の FA から送信される DNS クエリーのリマッピングに使用されます。プライマリ DNS サーバがダウンしている場合、セカンダリ DNS サーバが DNS クエリーのリマッピングのためのアクティブ DNS サーバとして使用されます。プライマリとセカンダリの両方の DNS に HA がアクセスできる場合、プライマリ サーバが DNS リマッピングに使用されます。さらに、セカンダリ DNS サーバがアクティブ DNS サーバで、プライマリ DNS サーバがアップしたり、HA との接続が再開した場合、プライマリ DNS サーバがアクティブ DNS サーバの役割を再度引き継ぎます。

この機能についての重要な考慮事項は次のとおりです。

- スイッチオーバーが行われると、HA で DNS サーバからの応答を待っている保留中の DNS クエリーは新しいアクティブな HA ですべて失われます。このシナリオでは、モバイル ノードは DNS クエリーを再送する必要があります。
- DNS クエリーの宛先アドレスが HA 上で設定された DNS サーバのアドレスと一致すると、DNS リダイレクションが使用されず、HA はこのパケットを通常のデータ パケットとして処理します。
- DNS リダイレクションに NAT 設定を使用する必要はありません。

レルムベースの DNS リダイレクション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)# ip mobile realm` *word* `dns server` *primary DNS ip secondary DNS ip*	レルムのプライマリおよびセカンダリの DNS サーバを設定します。
ステップ 2	`Router(config)# ip mobile realm` *word* `dns server redirect` {all}	このレルムの DNS リダイレクション機能をイネーブルにします。

上記の 2 つのコマンドの動作

- **ip mobile realm** *word* **dns server redirect {all}** が **ip mobile realm** *word* **dns server** *primary DNS ip secondary DNS ip* の前に設定されている場合、HA は次のエラー メッセージを表示します。

エラー メッセージ　`Error: Primary and Secondary DNS not configured for realm`

- DNS リダイレクション機能はレルム ベースであるため、"@" または "@domain" だけが有効なレルムになります。たとえば、xyz@domain、xyz または xyz@ は有効なレルム オプションにはなりません。エラーの場合、HA は次のエラー メッセージを表示します。

エラー メッセージ　`DNS Redirection is allowed for realm only (e.g. @word)`

- プライマリ DNS サーバとセカンダリ DNS サーバを設定解除するコマンドが特定のレルムに対して実行されていない場合、そのレルムに対する DNS リダイレクションは自動的にディセーブルになります。
- **ip mobile realm** *word* **dns server redirect** コマンドの **no** バージョンを使用して DNS リダイレクション機能を設定解除する場合、そのレルムの既存のバインディングは HA から削除されません。DNS リダイレクション機能だけがディセーブルになります。

アベイラビリティをモニタリングしている DNS サーバをイネーブルにするには、次の IP SLA CLI を設定します。この IP SLA コンフィギュレーション コマンド セットは、HA によってモニタリングする必要のあるすべての DNS サーバ ノードに必要です。これらの IP SLA コマンドは 7600 シリーズ ルータすべてで使用できる既存のコマンドです。

	コマンド	目的
ステップ 1	`Router(config)# ip sla` *`ipsla-number`* `icmp-echo` *`ip-addr`* `frequency` *`freq`*	IPSLA 番号を割り当て、モニタリングする必要のある IP アドレスを設定します。
ステップ 2	`Router(config)# ip sla reaction-configuration` *`ipsla-number`* `react timeout threshold-type immediate action-type trapAndTrigger`	上記の設定済みの DNS サーバが使用できないことを通知するために IP SLA を設定します。
ステップ 3	`router(config)#ip sla reaction-configuration` *`ipsla-number`* `react connectionLoss threshold-type immediate action-type trapAndTrigger`	上記の設定済みの DNS サーバが使用できることを通知するために IP SLA を設定します。
ステップ 4	`router(config)#ip sla enable reaction-alerts`	上で設定した DNS サーバのアベイラビリティとアンアベイラビリティの通知を生成するよう IP SLA を設定します。
ステップ 5	`router(config)#ip sla sch` *`ipsla-number`* `start-time now life forever`	上で設定した設定済み DNS サーバのモニタリングを開始するよう IP SLA を設定します。

上記で

- ipsla-number は DNS サーバのチェックのために割り当てられている IP SLA 番号です。
- ip-addr は DNS サーバの IP アドレスです。
- freq は プローブの秒単位での周波数です（デフォルトは 60）。

Proximity Domain Name Server（PDNS; プロキシミティ ドメイン ネーム サーバ）または SDNS に一致する DNS クエリー

ここでは、DNS クエリーが設定済みの PDNS または SDNS に一致する場合のリダイレクション動作について説明します。

PDNS に一致する要求

DNS 要求が PDNS に一致し、PDNS がアクティブの場合、その要求はスキップされます。しかし、PDNS がダウンしている場合、要求は SDNS にリダイレクトされます（SDNS がアクティブの場合）。アクティブでない場合、要求は無視されます（通常のデータ パケットとして処理されます）。

SDNS に一致する要求

SDNS に一致する要求に関する動作は、設定 CLI によって制御されます。DNS のリダイレクトを設定するために使用される CLI は、次のとおりです。

ip mobile realm *@realm* dns server redirect {**all**}

redirect だけが設定されている場合、SDNS に送信される要求はリダイレクトされません（アップしている場合）。これらは SDNS サーバだけに送信されます。その他の DNS 要求は PDNS にリダイレクトされます。

redirect all が設定されている場合、（設定済みの SDNS IP に一致する要求を含む）すべての DNS 要求が PDN にリダイレクトされます。

IP SLA 経由の DNS サーバのモニタリング

IP SLA が設定済みのプライマリおよびセカンダリいずれかの DNS サーバとの接続切断または接続のアップ イベントを検出すると、CP 上でレジストリ API を起動します。CP が通知を受け取ると、このイベントについて IPC 経由ですべての TP に通知します。TP が CP からこの通知を受け取ると、プライマリ DNS とセカンダリ DNS 間にアクティブ DNS を設定します。

DNS リダイレクションは冗長性をサポートします。スイッチオーバー後、HA がアクティブになると、設定済みの DNS サーバのアベイラビリティのモニタリングを開始します。DNS クエリーが受信されると、HA 上の設定済みの DNS サーバにリマッピングされます。

唯一の制限は、スイッチオーバーが行われると、HA で DNS の応答を待っている保留中の DNS クエリーが新しいアクティブな HA ですべて失われることです。このシナリオでは、モバイル ノードは DNS クエリーを再送する必要があります。

例

次に、DNS 用のユーザ 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-DNS-Server-IP-Address = 01:06:0A:4D:9B:0A:02:06:0A:4D:9B:09:03:03:01:04:03:01
    CDMA-DNS-Update-Required = "HA does need to send DNS Update"
    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"
    class = "Entering the World of Mobile IP-3"
    Service-Type = Framed
```

次に、DNS サーバ アドレス割り当てレルムのコンフィギュレーション例を示します。

```
ip mobile realm @ispxyz2.com dns server 10.77.155.10 2.2.2.2
ip mobile realm @ispxyz2.com dns server assign
```

次に、AR ユーザ プロファイルでの同じ設定の例を示します。

```
set  CDMA-DNS-Server-IP-Address 01:06:0A:4D:9B:0A:02:06:0A:4D:9B:09:03:03:01:04:03:01
```

太字の部分が、プライマリおよびセカンダリの DNS サーバ アドレスです。

次に、IP 到達可能性および DNS サーバ アドレス割り当ての両方の設定例を示します。

```
ha2#show run
Building configuration...

Current configuration : 10649 bytes
!
! Last configuration change at 22:45:21 UTC Fri Nov 11 2005
!
version 12.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
service internal
service udp-small-servers
!
hostname tb1-6513-ha2
!
boot-start-marker
boot-end-marker
!
!
aaa new-model
!
!
aaa group server radius MOT
 server 150.2.0.1 auth-port 1645 acct-port 1646
!
aaa authentication ppp default local group MOT
aaa authorization config-commands
aaa authorization ipmobile default group MOT
aaa authorization network default group MOT
aaa authorization configuration default group MOT
aaa accounting session-duration ntp-adjusted
aaa accounting update newinfo periodic 3
aaa accounting network ha start-stop group MOT
aaa accounting system default start-stop group MOT
!
aaa server radius dynamic-author
 client 150.2.0.1
 server-key cisco
!
aaa session-id common
!
resource policy
!
ip subnet-zero
no ip gratuitous-arps
!
!
ip cef
ip dfp agent ipmobile
 port 400
 interval 15
 inservice
!
ip ftp source-interface GigabitEthernet0/0.10
ip ftp username root
ip ftp password pdsnmwg
no ip domain lookup
ip name-server 10.77.155.10
ip name-server 1.1.1.1
ip name-server 6.6.6.6
no ip dhcp use vrf connected
```

```
no ip dhcp conflict logging
ip dhcp ping packets 0
!
ip dhcp pool Subnet-Pool1
   utilization mark high 75
   utilization mark low 25
   origin dhcp subnet size initial /30 autogrow /30
!
!
ip vrf forwarding
!
ip vrf ispxyz
!
ip vrf ispxyz-vrf1
 rd 100:1
!
ip vrf ispxyz-vrf2
 rd 100:2
!
!
ip ddns update method sit-ha2-ddns1
 DDNS both
!
ip ddns update method sit-ha2-ddns2
 DDNS both
!
vpdn enable
vpdn ip udp ignore checksum
!
vpdn-group testsip1-l2tp
! Default L2TP VPDN group
! Default PPTP VPDN group
 accept-dialin
  protocol any
  virtual-template 1
 l2tp tunnel hello 0
!
username user-ha2 password 0 cisco
!
!
!
interface Tunnel10
 no ip address
 ip access-group 150 in
!
interface Loopback0
 ip address 20.20.225.1 255.255.255.0
!
interface Loopback1
 description address of the LNS server
 ip address 20.20.206.20 255.255.255.0
!
interface Loopback2
 ip address 170.12.0.102 255.255.0.0
!
interface GigabitEthernet0/0
 no ip address
 no ip route-cache cef
 no ip route-cache
 no keepalive
 no cdp enable
!
interface GigabitEthernet0/0.10
 description TFTP vlan
```

```
 encapsulation dot1Q 10
 ip address 10.77.155.5 255.255.255.192
 no ip route-cache
 no snmp trap link-status
 no cdp enable
!
interface GigabitEthernet0/0.172
 description HAAA interface
 encapsulation dot1Q 172
 ip address 170.2.0.20 255.255.0.0
 no ip route-cache
 no snmp trap link-status
 no cdp enable
 standby delay minimum 15 reload 15
 standby version 2
 standby 2 ip 170.2.0.102
 standby 2 follow sit-ha2
!
interface GigabitEthernet0/0.202
 description PI interface
 encapsulation dot1Q 202
 ip address 20.20.202.20 255.255.255.0
 no ip route-cache
 no snmp trap link-status
 no cdp enable
 standby delay minimum 15 reload 15
 standby version 2
 standby 2 ip 20.20.202.102
 standby 2 ip 20.20.204.2 secondary
 standby 2 ip 20.20.204.3 secondary
 standby 2 ip 20.20.204.4 secondary
 standby 2 ip 20.20.204.5 secondary
 standby 2 ip 20.20.204.6 secondary
 standby 2 timers msec 750 msec 2250
 standby 2 priority 130
 standby 2 preempt delay minimum 180
 standby 2 name sit-ha2
!
interface GigabitEthernet0/0.205
 description REF interface
 encapsulation dot1Q 205
 ip address 20.20.205.20 255.255.255.0
 no ip route-cache
 no snmp trap link-status
 no cdp enable
 standby delay minimum 15 reload 15
 standby version 2
 standby 2 ip 20.20.205.102
 standby 2 follow sit-ha2
!
interface Virtual-Template1
 description To be used by VPDN for PPP tunnel
 ip unnumbered Loopback1
 peer default ip address pool LNS-pool
 no keepalive
 ppp accm 0
 ppp authentication chap pap optional
 ppp accounting none
!
router mobile
!
ip local pool LNS-pool 7.0.0.1 7.0.0.255
ip local pool ispxyz-vrf1-pool 50.0.0.1 50.0.0.255
ip local pool mobilenodes 40.0.0.1 40.0.100.255
```

```
ip default-gateway 10.77.155.1
ip classless
ip route 0.0.0.0 0.0.0.0 GigabitEthernet0/0.202
ip route 10.77.139.29 255.255.255.255 10.77.155.1
ip route 150.2.0.0 255.255.0.0 170.2.0.1
no ip http server
!
!
ip mobile debug include username
ip mobile home-agent template Tunnel10 address 20.20.202.102
ip mobile home-agent revocation timeout 5 retransmit 4
ip mobile home-agent dynamic-address 20.20.202.102
ip mobile home-agent accounting ha broadcast lifetime 3600 replay 8 suppress-unreachable
unknown-ha deny
ip mobile home-agent redundancy sit-ha2 virtual-network address 20.20.202.102
periodic-sync
ip mobile radius disconnect
ip mobile virtual-network 50.0.0.0 255.0.0.0
ip mobile virtual-network 40.0.0.0 255.0.0.0
ip mobile host nai mwts-pmp-r20sit-base-user1@ispxyz1.com virtual-network 40.0.0.0
255.0.0.0 aaa load-sa lifetime 600
ip mobile host nai @ispxyz2.com address pool local mobilenodes virtual-network 40.0.0.0
255.0.0.0 aaa lifetime 180
ip mobile realm mwts-pmp-r20sit-base-user1@ispxyz1.com dns server 10.77.155.10 1.1.1.1
ip mobile realm mwts-pmp-r20sit-base-user1@ispxyz1.com dns server assign
ip mobile realm mwts-pmp-r20sit-base-user1@ispxyz1.com dns dynamic-update method
sit-ha2-ddns1
ip mobile realm @ispxyz2.com vrf ispxyz-vrf2 ha-addr 20.20.204.6
ip mobile realm @ispxyz2.com dns server 10.77.155.10 2.2.2.2
ip mobile realm @ispxyz2.com dns server assign
ip mobile realm @ispxyz2.com dns dynamic-update method sit-ha2-ddns2
ip mobile secure foreign-agent 20.20.201.10 20.20.201.100 spi 100 key ascii cisco replay
timestamp within 7 algorithm md5 mode prefix-suffix
ip mobile secure foreign-agent 20.20.210.10 20.20.210.100 spi 100 key ascii cisco replay
timestamp within 5 algorithm md5 mode prefix-suffix
ip mobile secure home-agent 20.20.202.10 20.20.202.95 spi 100 key ascii cisco replay
timestamp within 7 algorithm md5 mode prefix-suffix
!
ip radius source-interface Loopback2
no logging trap
logging source-interface GigabitEthernet0/0.201
access-list 150 permit ip host 40.0.0.1 host 20.20.205.220 log
access-list 150 permit ip host 20.20.205.220 host 40.0.0.1 log
access-list 150 deny   ip any any log
snmp-server community public RO
snmp-server community private RW
snmp-server trap-source Loopback0
snmp-server host 150.2.0.100 version 2c private
snmp-server host 150.2.0.100 public
no cdp run
!
!
radius-server attribute 44 include-in-access-req
radius-server attribute 8 include-in-access-req
radius-server attribute 32 include-in-access-req
radius-server attribute 55 access-request include
radius-server host 150.2.0.1 auth-port 1645 acct-port 1646 key 7 121A0C041104
radius-server host 150.2.0.100 auth-port 1645 acct-port 1646 key cisco
radius-server retransmit 4
radius-server timeout 2
radius-server deadtime 5
radius-server key cisco
radius-server vsa send accounting
radius-server vsa send authentication
```

```
radius-server vsa send accounting 3gpp2
radius-server vsa send authentication 3gpp2
!
control-plane
!
alias exec shc sh cdma pdsn
alias exec ua undebug all
alias exec ui undebug ip packet
!
line con 0
 exec-timeout 0 0
line vty 0 4
 exec-timeout 0 0
line vty 5 15
 exec-timeout 0 0
!
!
end

ha2#
```