HA Redundancy for Dynamic Home Agent Assignment

The product administration guides provide examples and procedures for configuration of basic services on the system. It is recommended that you select the configuration example that best meets your service model, and configure the required elements for that model before using the procedures in this chapter.

This chapter includes the following topics:

Feature Description

This feature provides a mechanism for a system functioning as a Home Agent (HA) to communicate status information to a properly configured RADIUS server. The status information is used by the RADIUS server to determine the availability and readiness of the HA to accept Mobile IP (MIP) subscriber sessions. The RADIUS server\'s awareness of the HA status allows it to dynamically assign immediately available HAs to subscriber sessions.

When a RADIUS server assigns an HA to a Mobile Node (MN), it is very important that only active, or accessible, HAs are selected for the assignment. Therefore, it is necessary for the RADIUS server to detect the availability of each HA before assigning it to an MN. This feature allows the RADIUS server to gather and maintain a list of available HAs through a detection mechanism that provides frequent updates.

With this feature, bogus authentication messages, called probe authentication messages, are exchanged between the RADIUS server and the HA. The HA periodically sends Access-Request messages to the RADIUS server. The RADIUS server distinguishes the probe authentication request from other regular subscriber authentication messages, validates them, and sends proper response.

The probe Access-Request contains the following attributes and expects an Access-Accept from the RADIUS server.

```
User-Name = Probe-User
User-Password = 18 7F 88 02 82 1D B6 F6 70 48 B9 A1 4C 92 C3 3E
NAS-IP-Address = 182.168.65.2
Service-Type = Authenticate_Only
Event-Timestamp = 1255598429
```

User-Name and User-Password are configurable in the system.

If an Access-Accept message is sent in response to the probe authentication request, the RADIUS server updates the status of the HA as active. If an Access-Reject message is sent, the RADIUS server updates only the statistics without any further action. If the RADIUS server misses receiving a configured number of probe authentication requests, the HA, and all of its associated IP addresses, is marked as down, or inaccessible. When an HA is marked as down, a backup HA and its associated IP addresses are made active and used for assignment in the place of the inaccessible HA.

Supported Implementations

This feature is supported on system installations that are configured as Home Agents and are configured to communicate with a AAA Service Controller that supports the configuration of Active and Backup HAs. For more information on a compatible AAA Service Controller, contact your designated customer support engineer.

Configuring HA Redundancy for Dynamic Home Agent Assignment

Before you begin

Important The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

Step 1 Configure the AAA Service Controller as described in the AAA Service Controller documentation.

Step 2 Configure RADIUS support on the HA as described in the Configuring RADIUS Support on the HA, on page 3 section.

Step 3 Save the configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

What to do next

Important Commands used in the configuration examples in this section provide base functionality to the extent that the most common or likely commands and/or keyword options are presented. In many cases, other optional commands and/or keyword options are available. Refer to the *Command Line Interface Reference* for complete information regarding all commands.

Configuring the AAA Service Controller

The AAA Service Controller should be configured with the following parameters. For configuration information refer to the AAA Service Controller documentation.

- Authentication-Probe User profile:

  - Probe Username
  - Probe Password
- HA Client information:
  - HA Client IPv4 address (NAS-IP-Address attribute)
  - HA client secret (authenticator)
  - Whether the HA client is a Primary or Backup HA client
- One or more HA Service addresses for each HA client address.
- The number of missed probe authentication requests before the HA Client is marked as down.
- The number of seconds to wait for a probe authentication request from the HA client (timeout period).
- The number of seconds to wait for a backup HA server to be in the active state after a reboot, known as backup-hold-timeout.

Configuring RADIUS Support on the HA

Use the following example to configure RADIUS support on the HA:

```
configure
 context <context_name>
 radius server <ip_address> [ encrypted ] key <value>
 radius probe-interval <seconds>
 radius probe-max-retries <retries>
 radius probe-timeout <idle_seconds>
 end
```

Notes:

- <context_name> must be the name of the AAA context that the HA service uses for authentication.
- A number of optional keywords and variables are available for the **radius server** command. Refer to the *Command Line Interface Reference* for more information regarding this command.
- Option: To configure HA redundancy with AAA server group, in the Context Configuration Mode, use the following command:

  aaa group *<group_name>*

  <*group_name*> must be the name of the AAA group designated for AAA functionality within the context. A total of 400 server groups can be configured system-wide including the default server-group unless **aaa large-configuration** is enabled. For information on configuring context-level AAA functionality, refer to the AAA Interface Administration and Reference.

Important After you configure the **aaa large-configuration** CLI command, you must save the configuration and then reload the chassis for the command to take effect. For information on saving the configuration file and reloading the chassis, refer to the *System Administration Guide* for your deployment.

Verifying RADIUS Server Configurations

This section provides information to verify connectivity to the RADIUS server, and information to view counters and statistics that can be useful in troubleshooting issues.

Step 1 Verify connectivity to the RADIUS server by sending a test probe message to the RADIUS server by entering the following command:

radius test probe authentication server <*ip_address*> **port** <*port_number*> [**username** <*username*> **password** <*password*>]

Important Any response, including **Access-Reject** and **Access-Accept** from the AAA server, is considered to mean that the AAA server is alive.

The following is a sample of the output of a successful probe authentication test.

```
[local]host_name radius test probe authentication server 192.168.20.1 port 1812
Authentication from authentication server 192.168.20.1, port 1812
Authentication Success: Access-Accept received
Round-trip time for response was 714.2 ms
```

Step 2 View the RADIUS counters by entering the following command:

show radius counters { all | server <*ip_address*> [**port** <*port_number*>] } [| { **grep** <*grep_options*> | **more** }]

The following is a sample output of the command displaying RADIUS Probe counters.

```
Server-specific Probing Counters
   --------------------------------
     State: Down
     Number of transactions issued:3
     Number of successful transactions:2
     Number of failed transactions:1
     Last successful transaction time: Thu Aug 26 17:40:32 2004
     Last failed transaction time:Thu Aug 26 17:40:39 2004
     Last roundtrip time:3.2 ms
```

Step 3 View AAA Manager statistics by entering the following command:

show session subsystem [full | facility *aaamgr* [**all | instance** <*id*>]] [**verbose**] [| { **grep** <*grep_options*> | **more** }]

The following is a sample output of the command displaying authentication probe statistics in the output.

```
AAAMgr:  Instance 261
       4 Total aaa requests                 0 Current aaa requests
       3 Total aaa auth requests            0 Current aaa auth requests
       0 Total aaa auth probes              0 Current aaa auth probes
       1 Total aaa acct requests            0 Current aaa acct requests
```