Rejection/Redirection of HA Sessions on Network Failures

This chapter provides information on configuring an enhanced, or extended, service. 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, as described in the respective product Administration Guide, before using the procedures in this chapter.

This chapter contains the following topics:

- Overview, on page 1
- Configuring HA Session Redirection, on page 2
- RADIUS Attributes, on page 5

Overview

This feature enables the HA service to either reject new calls or redirect them to another HA when a destination network connection failure is detected. When network connectivity is re-established, the HA service begins to accept calls again in the normal manner.

The way this is implemented in the system is as follows:

- A policy is configured in the HA service that tells the service what action to take when network connectivity is lost. New calls are either directed to one of up to 16 different IP addresses or all new calls are rejected until network connectivity is restored.
- In the destination context, a network reachability server is configured. This is a device on the destination network to which ping packets are periodically sent to determine if the network is reachable. As soon as a network reachability server is configured, pinging of the server commences whether or not the server name is bound to a subscriber or an IP pool.
- The name of the network reachability server configured in the destination context is bound to either a local subscriber profile or an IP pool. If the subscriber is authenticated by an AAA server, RADIUS attributes may specify the network reachability server for the subscriber. (If an IP pool has a network reachability server name bound to it, that takes precedence over both the RADIUS attributes and the local subscriber configuration.)

Configuring HA Session Redirection

This section provides instructions for configuring rejection or redirection of HA sessions on the event of a network failure. These instructions assume that there is a destination context. and HA service, an IP pool, and a subscriber already configured and that you are at the root prompt for the Exec mode:

```
[local]host_name
```

Step 1 Enter the global configuration mode by entering the following command:

configure

The following prompt appears:

```
[local]host_name(config)
```

Step 2 Enter context configuration mode by entering the following command:

context <*context_name*>

context_name is the name of the destination context where the HA service is configured. The name must be from 1 to 63 alpha and/or numeric characters and is case sensitive.The following prompt appears:

```
[<context_name>]host_name(config-ctx)
```

Step 3 Enter the HA service configuration mode by entering the following command:

ha-service <*ha_service_name*>

ha_service_name is the name of the HA service. The name must be from 1 to 63 alpha and/or numeric characters and is case sensitive.The following prompt appears:

```
[<context_name>]host_name(config-ha-service)
```

Step 4 Configure the action for the HA service to take when network connectivity is lost by entering the following command:

policy nw-reachability-fail { reject [use-reject-code { admin-prohibited | insufficient-resources }] | redirect <*ip_addr1*> [**weight** <*value*>] [<*ip_addr2*> [**weight** <*value*>]] ... [<*ip_addr16*> [**weight** <*value*>]] }

Keyword/Variable	Description
reject	Upon network reachability failure reject all new calls for this context.
use-reject-code { admin-prohibited | insufficient-resources }	When rejecting calls send the specified reject code. If this keyword is not specified the admin-prohibited reject code is sent by default.

Keyword/Variable	Description
redirect <*ip_addr1*> [**weight** <*value*>] [<*ip_addr2*> [**weight** <*value*>]] ... [<*ip_addr16*> [**weight** <*value*>]]	Upon network reachability failure redirect all calls to the specified IP address. <*ip_addr*>: This must be an IPv4 address. Up to 16 IP addresses and optional weight values can be entered on one command line. **weight** <*value*>: When multiple addresses are specified, they are selected in a weighted round-robin scheme. If a weight is not specified, the entry is automatically assigned a weight of 1. <*value*> must be an integer from 1 through 10.

Step 5 Enter the following command to return to the context configuration mode:

exit

The following prompt appears:

[<*context_name*>]*host_name***(config-ctx)**

Step 6 Specify the network device on the destination network to which ping packets should be sent to test for network reachability, by entering the following command:

nw-reachability server <*server_name*> [**interval** <*seconds*>] [**local-addr** <*ip_addr*>] [**num-retry** <*num*>] [**remote-addr** <*ip_addr*>] [**timeout** < *seconds*>]

Keyword/Variable	Description
server_name	A name for the network device that is sent ping packets to test for network reachability.
interval <*seconds*>	Default: 60 seconds Specifies the frequency in seconds for sending ping requests.<*seconds*> must be an integer from 1 through 3600.
local-addr <*ip_addr*>	Specifies the IP address to be used as the source address of the ping packets; If this is unspecified, an arbitrary IP address that is configured in the context is used. <*ip_addr*> must be an IP v4 address.
num-retry <*num*>	Default: 5 Specifies the number of retries before deciding that there is a network-failure. <*num*> must be an integer from 0 through 100.
remote-addr <*ip_addr*>	Specifies the IP address of a network element to use as the destination to send the ping packets for detecting network failure or reachability. <*ip_addr*> must be an IPv4 address.

Keyword/Variable	Description
timeout < *seconds*>	Default: 3 seconds Specifies how long to wait, in seconds, before retransmitting a ping request to the remote address. <*seconds*> must be an integer from 1 through 10.

Step 7 Repeat *step 6* to configure additional network reachability servers.

Step 8 To bind a network reachability server to an IP pool, continue with *step 9*. To bind a network reachability server to a local subscriber profile, skip to *step 11*.

Step 9 To bind a network reachability server name to an IP pool, enter the following command:

ip pool <*pool_name*> **nw-reachability server** <*server_name*>

<*pool_name*>	The name of an existing IP pool in the current context.
nw-reachability server <*server_name*>	Bind the name of a configured network reachability server to the IP pool and enable network reachability detection for the IP pool. This takes precedence over any network reachability server settings in a subscriber configuration or RADIUS attribute. <*server_name*>: The name of a network reachability server that has been defined in the current context. This is a string of from 1 through 16 characters.

Step 10 Repeat *step 9* for additional IP pools in the current context then skip to *step 13*.

Step 11 Enter the subscriber configuration mode by entering the following command:

subscriber { default | name <*subs_name*> }

Where **default** is the default subscriber for the current context and *subs_name* is the name of the subscriber profile that you want to configure for network reachability.The following prompt appears:

[<*context_name*>]*host_name***(config-subscriber)**

Step 12 To bind a network reachability server name to the current subscriber in the current context, enter the following command:

nw-reachability server <*server_name*>

Where *server_name* is the name of a network reachability server that has been defined in the current context.

Step 13 Return to the executive mode by entering the following command:

end

The following prompt appears:

[local]*host_name*

Step 14 Enter the executive mode for the destination context for which you configured network reachability by entering the following command:

context <*context_name*>

Where *context_name* is the name of the destination context for which you configured network reachability.The following prompt appears:

```
[context_name]host_name
```

Step 15 Check the network reachability server configuration by entering the following command

show nw-reachability server all

The output of this command appears similar to the following:

```
  Server           remote-addr     local-addr      state
 ---------------  --------------- --------------- ---------------
 nw-server1       192.168.100.20  192.168.1.10    Down
  Total Network Reachability Servers: 1 Up: 0
```

Ensure that the remote and local addresses are correct. The state column indicates whether or not the server is reachable (Up) or unreachable (Down).

Step 16 Check the HA service policy by entering the following command:

show ha-service name *<ha_service_name>*

Where <*ha_service_name*> is the name of the HA service in the current context for which you configured a network reachability policy.The output of this command includes information about the network reachability policy that looks similar to the following:

```
NW-Reachability Policy:  Reject    (Reject code: Admin Prohibited)
```

Step 17 Check the network reachability server name bound to an IP pool by entering the following command:

show ip pool pool-name *<pool_name>*

Where <*pool_name*> is the name of the IP pool to which you bound a network reachability server name.The output of this command includes information about the network reachability server name that looks similar to the following:

```
Network Reachability Detection Server: nw-server1
```

Step 18 Check the network reachability server name bound to a local subscriber profile by entering the following command:

show subscribers configuration username *<subscriber_name>*

Where <*subscriber_name*> is the name of the local subscriber to which you bound a network reachability server name.The output of this command includes information about the network reachability server name that looks similar to the following:

```
network reachability detection server name: nw-server1
```

Step 19 Save your 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*.

RADIUS Attributes

Attributes defined in a subscriber profile stored remotely on a RADIUS server can be used to bind the network reachability server to a subscriber session. Use the following attributes to bind a network reachability server to a subscriber session;

- **SN-Nw-Reachability-Server-Name**
- **SN1-Nw-Reachability-Server-Name**

The attributes have one possible value, which is a variable that is a string of from 1 to 15 characters in length. This should be the name of the configured network reachability server.

The **SN-Nw-Reachability-Server-Name** attribute is contained in the following dictionaries:

- starent
- starent-835

The **SN1-Nw-Reachability-Server-Name** attribute is contained in the following dictionaries:

- starent-vsa1
- starent-vsa1-835

Refer to the *AAA Interface Administration and Reference* for more details.