



## Mobile IP Configuration Examples

This chapter provides information for several configuration examples that can be implemented on the system to support Mobile IP (MIP) data services.



### Important

This chapter does not discuss the configuration of the local context. Information about the local context can be found in *Command Line Reference*.



### Important

When configuring Mobile IP take into account the MIP timing considerations discussed in *Mobile-IP and Proxy-MIP Timer Considerations* appendix.

- [Example 1: Mobile IP Support Using the System as a GGSN/FA, on page 1](#)
- [Example 2: Mobile IP Support Using the System as an HA, on page 17](#)
- [Example 3: HA Using a Single Source Context and Multiple Outsourced Destination Contexts, on page 27](#)

## Example 1: Mobile IP Support Using the System as a GGSN/FA

For Mobile IP applications, the system can be configured to perform the function of a Gateway GPRS Support Node/Foreign Agent (GGSN/FA) and/or a Home Agent (HA). This example describes what is needed for and how the system performs the role of the GGSN/FA. Examples 2 and 3 provide information on using the system to provide HA functionality.

The system's GGSN/FA configuration for Mobile IP applications is best addressed with three contexts (one source, one AAA, and one Mobile IP destination) configured as shown in the figure that follows.



### Important

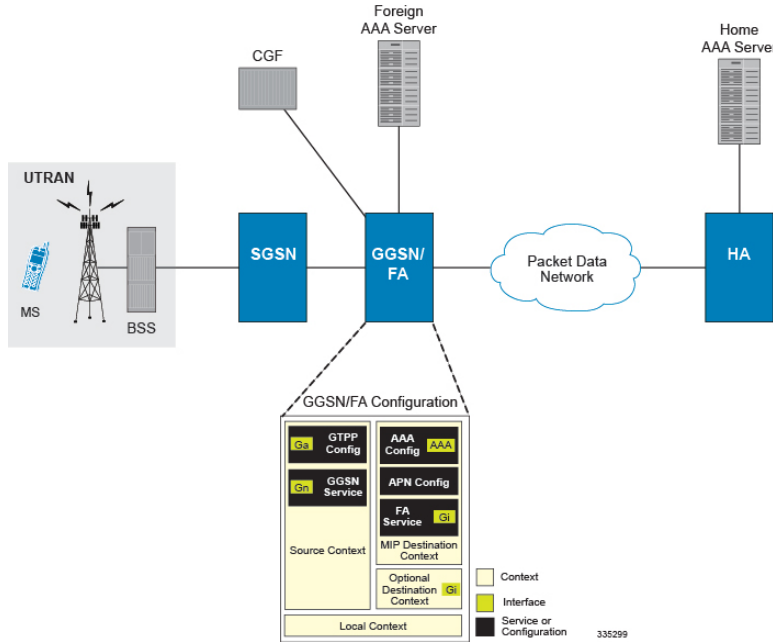
A fourth context that serves as a destination context must also be configured if Reverse Tunneling is disabled in the FA service configuration. Reverse Tunneling is enabled by default.

The source context will facilitate the GGSN service(s), and the Ga and Gn interfaces. The AAA context will be configured to provide foreign AAA functionality for subscriber PDP contexts and facilitate the AAA interfaces. The MIP destination context will facilitate the FA service(s) and the Gi interface(s) from the GGSN/FA to the HA.

Information Required

The optional destination context will allow the routing of data from the mobile node to the packet data network by facilitating a packet data network (PDN) interface. This context will be used only if reverse tunneling is disabled.

Figure 1: Mobile IP Support using the system as a GGSN/FA



## Information Required

Prior to configuring the system as shown in this example, there is a minimum amount of information required. The following sections describe the information required to configure the source and destination contexts.

### Source Context Configuration

The following table lists the information that is required to configure the source context.

Table 1: Required Information for Source Context Configuration

| Required Information       | Description   |
|----------------------------|---|
| Source context name        | An identification string from 1 to 79 characters (alpha and/or numeric) by which the source context will be recognized by the system.<br><br><b>Important</b> The name of the source context should be the same as the name of the context in which the FA-context is configured if a separate system is being used to provide GGSN/FA functionality. |
| Gn Interface Configuration |   |

| Required Information              | Description   |
|-----------------------------------|---|
| Gn interface name                 | <p>An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system.</p> <p>Multiple names are needed if multiple interfaces will be configured.</p>   |
| IP address and subnet             | <p>These will be assigned to the Gn interface.</p> <p>Multiple addresses and/or subnets are needed if multiple interfaces will be configured.</p>   |
| Physical port number              | <p>The physical port to which the interface will be bound.</p> <p>Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card.</p> <p>For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.</p> |
| Physical port description         | <p>An identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system.</p> <p>Multiple descriptions are needed if multiple ports will be used.</p> <p>Physical ports are configured within the source context and are used to bind logical Gn interfaces.</p>  |
| Gateway IP address                | <p>Used when configuring static routes from the Gn interface(s) to a specific network.</p>  |
| <b>GGSN service Configuration</b> |   |
| GGSN service name                 | <p>An identification string from 1 to 63 characters (alpha and/or numeric) by which the GGSN service will be recognized by the system.</p> <p>Multiple names are needed if multiple GGSN services will be used.</p>   |
| Accounting context                | <p>The name of the context configured on the system in which the processing of GTPP accounting records is performed.</p> <p>The context name is an identification string from 1 to 79 characters (alpha and/or numeric).</p> <p>By default, the system attempts to use the same context as the one in which the GGSN service is configured.</p>                         |

| Required Information                          | Description   |
|---|---|
| UDP port number for GTPC traffic              | <p>The port used by the GGSN service and the SGSN for communicating GTPC sockets for GTPv1.</p> <p>The UDP port number and can be any integer value from 1 to 65535. The default value is 2123.</p>   |
| Public Land Mobile Network (PLMN) Identifiers | <p><b>Mobile Country Code (MCC):</b> The MCC can be configured to any integer value from 0 to 999.</p>  |
|   | <p><b>Mobile Network Code (MNC):</b> The MNC can be configured to any integer value from 0 to 999.</p>  |
| SGSN information (optional)                   | <p>The GGSN can be configured with information about the SGSN(s) that it is to communicate with.</p> <p>This includes the SGSN's IP address and subnet mask and whether or not the SGSN is on a foreign PLMN. Multiple SGSNs can be configured.</p> |

| Required Information                          | Description   |
|---|---|
| GGSN charging characteristics (CC) (optional) | <p><b>Behavior Bits:</b> If charging characteristics will be configured on the GGSN, behavior bits for the following conditions can be configured:</p> <ul style="list-style-type: none"> <li>• GGSN use of the accounting server specified by the profile index</li> <li>• GGSN rejection of Create PDP Context Request messages</li> <li>• GGSN ceases sending accounting records</li> </ul> <p>Each value must be a unique bit from 1 to 12 to represent the 12 possible behavior bits allowed for in the standards. The default configuration is disabled (0).</p> <p><b>Profile Index:</b> If the GGSN's charging characteristics will be used for subscriber PDP contexts, profile indexes can be modified/configured for one or more of the following conditions:</p> <ul style="list-style-type: none"> <li>• The number of statistics container changes is met or exceeded causing an accounting record to be closed. The number can be configured from 1 to 15. The default is 4.</li> <li>• The up and/or downlink traffic volume limits are met or exceeded within a specific time interval causing a partial record to be generated. The up and downlink volumes can be configured from 0 to 1000000 octets. The interval can be configured from 60 to 4000000 seconds.</li> <li>• The up and/or downlink traffic volume limits are met or exceeded causing an accounting record to be closed. The up and downlink volumes can be configured from 100000 to 4000000000 octets.</li> <li>• The number of SGSN switchovers is met or exceeded causing an accounting record to be closed. The number can be configured from 1 to 15. The default is 4.</li> <li>• Specific tariff times within a day are reached causing an accounting record to be closed. Up to four times can be configured using the hour of the day (1-24) and the minute (1-60).</li> </ul> <p>The system supports the configuration of up to 16 profile indexes numbered 0 through 15.</p> |

| Required Information       | Description  |
|----------------------------|--|
| PLMN policy                | <p>The GGSN can be configured treat communications from unconfigured SGSNs in one of the following ways:</p> <ul style="list-style-type: none"> <li>• Treat the SGSN as if it is on a foreign PLMN</li> <li>• Treat the SGSN as if it is on a home PLMN</li> <li>• Reject communications from unconfigured SGSNs (default)</li> </ul>                            |
| Ga Interface Configuration |  |
| Ga interface name          | <p>An identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system.</p> <p>Multiple names are needed if multiple interfaces will be configured.</p>  |
| IP address and subnet      | <p>These will be assigned to the Ga interface.</p> <p>Multiple addresses and/or subnets are needed if multiple interfaces will be configured.</p>  |
| Physical port number       | <p>The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17.</p> <p>A single physical port can facilitate multiple interfaces.</p> |
| Physical port description  | <p>An identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system.</p> <p>Multiple descriptions are needed if multiple ports will be used.</p> <p>Physical ports are configured within the source context and are used to bind logical Ga interfaces.</p>                               |
| Gateway IP address         | Used when configuring static routes from the Ga interface(s) to a specific network.  |
| GTPP Configuration         |  |
| Charging gateway address   | The IP address of the system's GGSN interface.   |

| Required Information   | Description   |
|------------------------|---|
| CGF server information | <p><b>IP address:</b> The IP address of the CGF server to which the GGSN will send accounting information</p> <p>.Multiple CGFs can be configured.</p>  |
|                        | <p><b>Priority:</b> If more than on CGF is configured, this is the server's priority. It is used to determine the rotation order of the CGFs when sending accounting information.</p> <p>The priority can be configured to any integer value from 1 to 1000. The default is 1.</p>  |
|                        | <p><b>Maximum number of messages:</b> The maximum number of outstanding or unacknowledged GTPP messages allowed for the CGF.</p> <p>The maximum number can be configured to any integer value from 1 to 256. The default is 256.</p>  |
| GCDR optional fields   | <p>The following optional fields can be specified/configured in CDRs generated by the GGSN:</p> <ul style="list-style-type: none"> <li>• diagnostics</li> <li>• duration-ms: the time specified in the mandatory Duration field is reported in milliseconds</li> <li>• local-record-sequence-number</li> <li>• plmn-id</li> </ul> |

## AAA Context Configuration

*Table 2: Required Information for AAA Context Configuration*

| Required Information | Description   |
|----------------------|---|
| AAA context name     | <p>An identification string from 1 to 79 characters (alpha and/or numeric) by which the AAA context will be recognized by the system.</p> <p><b>Important</b> If a separate system is used to provide HA functionality, the AAA context name should match the name of the context in which the AAA functionality is configured on the HA machine.</p> |
| APN Configuration    |   |

| Required Information                             | Description   |
|--|---|
| APN name   | <p>An identification string by which the APN will be recognized by the system. The name can be from 1 to 62 alpha and/or numeric characters and is not case sensitive. It may also contain dots ( . ) and/or dashes ( - ).</p> <p>Multiple names are needed if multiple APNs will be used.</p>  |
| Accounting mode                                  | <p>Selects the accounting protocol. GTPP or RADIUS are supported. In addition, accounting can be completely disabled. The default is to perform accounting using GTPP.</p> <p><b>Important</b> The examples discussed in this chapter assumes GTPP is used.</p>   |
| Authentication protocols used                    | <p>Specifies how the system handles authentication: using a protocol (such as CHAP, PAP, or MSCHAP), or not requiring any authentication.</p>   |
| APN charging characteristics (CC) (optional)     | <p>Specifies whether or not the GGSN accepts the CC from the SGSN for home, visiting, and roaming subscribers.</p> <p>By default the GGSN accepts the CC from the SGSN for all three scenarios.</p> <p>If the GGSN is to use its own CC for any of these scenarios, then each scenario requires the specification of behavior bits and a profile index to use.</p> <p><b>Important</b> The profile index parameters are configured as part of the GGSN service.</p> |
| Domain Name Service (DNS) information (optional) | <p>If DNS will be used for the APN, IP addresses can be configured for primary and secondary DNS servers.</p>   |
| IP destination context name                      | <p>The name of the system destination context to use for subscribers accessing the APN. If no name is specified, the system automatically uses the system context in which the APN is configured.</p>   |
| Maximum number of PDP contexts                   | <p>The maximum number of PDP contexts that are supported for the APN.</p> <p>The maximum number can be configured to any integer value from 1 to 1500000. The default is 1000000.</p>   |
| PDP type   | <p>The type of PDP contexts supported by the APN. The type can be IPv4, IPv6, both IPv4 and IPv6, or PPP. IPv4 support is enabled by default.</p>   |



| Required Information        | Description   |
|-----------------------------|---|
| Verification selection mode | <p>The level of verification that will be used to ensure a MS's subscription to use the APN. The GGSN uses any of the following methods:</p> <ul style="list-style-type: none"> <li>• No verification and MS supplies APN</li> <li>• No verification and SGSN supplies APN</li> <li>• Verified by SGSN (default)</li> </ul>   |
| Mobile IP Configuration     | <p><b>Home Agent IP Address:</b> The IP address of an HA with which the system will tunnel subscriber Mobile IP sessions.</p> <p>Configuring this information tunnels all subscriber Mobile IP PDP contexts facilitated by the APN to the same HA unless an individual subscriber profile provides an alternate HA address.</p> <p>Parameters stored in individual profiles supersede parameters provided by the APN.</p> <p><b>Mobile IP Requirement:</b> The APN can be configured to require Mobile IP for all sessions it facilitates. Incoming PDP contexts that do/can not use Mobile IP are dropped.</p> |
| AAA Interface Configuration |   |
| AAA interface name          | <p>This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system.</p> <p>Multiple names are needed if multiple interfaces will be configured.</p>   |
| IP address and subnet       | <p>These will be assigned to the AAA interface.</p> <p>Multiple addresses and/or subnets are needed if multiple interfaces will be configured.</p>  |
| Physical port number        | <p>This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17.</p> <p>A single physical port can facilitate multiple interfaces.</p>   |

| Required Information                 | Description  |
|--------------------------------------|--|
| Physical port description            | <p>This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system.</p> <p>Multiple descriptions are needed if multiple ports will be used.</p> <p>Physical ports are used to bind logical AAA interfaces.</p>   |
| Gateway IP address                   | Used when configuring static routes from the AAA interface(s) to a specific network.   |
| Foreign RADIUS Server Configuration  |  |
| Foreign RADIUS Authentication server | <p><b>IP Address:</b> Specifies the IP address of the Foreign RADIUS authentication server the system will communicate with to provide subscriber authentication functions.</p> <p>Multiple addresses are needed if multiple RADIUS servers.</p> <p>Foreign RADIUS servers are configured with in the source context. Multiple servers can be configured and each can be assigned a priority.</p> <p><b>Shared Secret:</b> The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS authentication server and the source context.</p> <p>A shared secret is needed for each configured RADIUS server.</p> <p><b>UDP Port Number:</b> Specifies the port used by the source context and the RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.</p> |

| Required Information                        | Description   |
|---|---|
| Foreign RADIUS Accounting server (optional) | <p><b>IP Address:</b> Specifies the IP address of the foreign RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions.</p> <p>Multiple addresses are needed if multiple RADIUS servers will be configured. RADIUS accounting servers are configured within the source context.</p> <p>Multiple servers can be configured and each assigned a priority.</p> <p><b>Shared Secret:</b> The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the foreign RADIUS accounting server and the source context.</p> <p>A shared secret is needed for each configured RADIUS server.</p> <p><b>UDP Port Number:</b> Specifies the port used by the source context and the foreign RADIUS Accounting server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1813.</p> |
| RADIUS attribute NAS Identifier             | Specifies the name by which the source context will be identified in the Access-Request message(s) it sends to the RADIUS server. The name must be from 1 to 32 alpha and/or numeric characters and is case sensitive.  |
| RADIUS NAS IP address                       | Specifies the IP address of the system's AAA interface. A secondary address can be optionally configured.   |

## Mobile IP Destination Context Configuration

*Table 3: Required Information for Mobile IP Destination Context Configuration*

| Required Information               | Description  |
|------------------------------------|--|
| Mobile IP Destination context name | <p>This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the Mobile IP destination context will be recognized by the system.</p> <p><b>Important</b> For this configuration, the destination context name should <b>not</b> match the domain name of a specific domain. It should, however, match the name of the context in which the HA service is configured if a separate system is used to provide HA functionality.</p> |
| Gi Interface Configuration         |  |
| Gi interface name                  | <p>This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system.</p> <p>Multiple names are needed if multiple interfaces will be configured.</p> <p>Gi interfaces are configured in the destination context.</p>  |
| IP address and subnet              | <p>These will be assigned to the Gi interface.</p> <p>Multiple addresses and/or subnets are needed if multiple interfaces will be configured.</p>  |
| Physical port number               | <p>This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17.</p> <p>A single physical port can facilitate multiple interfaces.</p>  |
| Physical port description(s)       | <p>This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system.</p> <p>Multiple descriptions will be needed if multiple ports will be used.</p> <p>Physical ports are configured within the destination context and are used to bind logical Gi interfaces.</p>  |
| Gateway IP address(es)             | <p>Used when configuring static routes from the Gi interface(s) to a specific network.</p>   |

| Required Information                             | Description  |
|--|--|
| FA Service Configuration                         |  |
| FA service name                                  | <p>This is an identification string between 1 and 63 characters (alpha and/or numeric) by which the FA service will be recognized by the system</p> <p>.Multiple names are needed if multiple FA services will be used.</p> <p>FA services are configured in the destination context.</p>  |
| UDP port number for Mobile IP traffic            | <p>Specifies the port used by the FA service and the HA for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 434.</p>  |
| Security Parameter Index (indices) Information   | <p><b>HA IP address:</b> Specifies the IP address of the HAs with which the FA service communicates. The FA service allows the creation of a security profile that can be associated with a particular HA.</p> <p><b>Index:</b> Specifies the shared SPI between the FA service and a particular HA. The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the FA service is to communicate with multiple HAs.</p> <p><b>Secrets:</b> Specifies the shared SPI secret between the FA service and the HA. The secret can be between 1 and 127 characters (alpha and/or numeric). An SPI secret is required for each SPI configured.</p> <p><b>Hash-algorithm:</b> Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default is hmac-md5. A hash-algorithm is required for each SPI configured.</p> |
| FA agent advertisement lifetime                  | <p>Specifies the time (in seconds) that an FA agent advertisement remains valid in the absence of further advertisements.</p> <p>The time can be configured to any integer value between 1 and 65535. The default is 9000.</p>   |
| Number of allowable unanswered FA advertisements | <p>Specifies the number of unanswered agent advertisements that the FA service will allow during call setup before it will reject the session.</p> <p>The number can be any integer value between 1 and 65535. The default is 5.</p>   |

| Required Information                                   | Description   |
|--|---|
| Maximum mobile-requested registration lifetime allowed | <p>Specifies the longest registration lifetime that the FA service will allow in any Registration Request message from the mobile node.</p> <p>The lifetime is expressed in seconds and can be configured between 1 and 65534. An infinite registration lifetime can be configured by disabling the timer. The default is 600 seconds.</p>              |
| Registration reply timeout                             | <p>Specifies the amount of time that the FA service will wait for a Registration Reply from an HA.</p> <p>The time is measured in seconds and can be configured to any integer value between 1 and 65535. The default is 7.</p>   |
| Number of simultaneous registrations                   | <p>Specifies the number of simultaneous Mobile IP sessions that will be supported for a single subscriber.</p> <p>The maximum number of sessions is 3. The default is 1.</p> <p><b>NOTE:</b> The system will only support multiple Mobile IP sessions per subscriber if the subscriber's mobile node has a static IP address.</p>                       |
| Mobile node re-registration requirements               | <p>Specifies how the system should handle authentication for mobile node re-registrations.</p> <p>The FA service can be configured to always require authentication or not. If not, the initial registration and de-registration will still be handled normally.</p>  |
| Maximum registration lifetime                          | <p>Specifies the longest registration lifetime that the HA service will allow in any Registration Request message from the mobile node.</p> <p>The time is measured in seconds and can be configured to any integer value between 1 and 65535. An infinite registration lifetime can also be configured by disabling the timer. The default is 600.</p> |
| Maximum number of simultaneous bindings                | <p>Specifies the maximum number of "care-of" addresses that can simultaneously be bound for the same user as identified by NAI and Home address.</p> <p>The number can be configured to any integer value between 1 and 5. The default is 3.</p>  |

## Optional Destination Context Configuration

The following table lists the information required to configure the optional destination context. As discussed previously, this context is required if: 1) reverse tunneling is disabled in the FA service, or 2) if access control lists (ACLs) are used

**Important**

If ACLs are used, the destination context would only consist of the ACL configuration. Interface configuration would not be required.

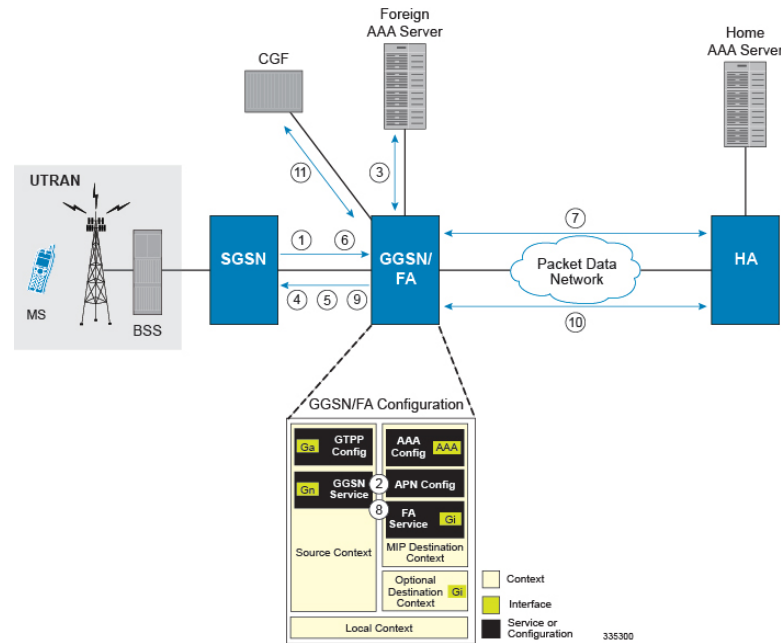
**Table 4: Required Information for Destination Context Configuration**

| Required Information        | Description   |
|-----------------------------|---|
| Destination context name    | <p>This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the destination context will be recognized by the system.</p> <p><b>Important</b> For this configuration, the destination context name should <b>not</b> match the domain name of a specific domain.</p>  |
| PDN Interface Configuration |   |
| PDN interface name          | <p>This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system.</p> <p>Multiple names are needed if multiple interfaces will be configured. PDN interfaces are configured in the destination context.</p>   |
| IP address and subnet       | <p>These will be assigned to the PDN interface.</p> <p>Multiple addresses and/or subnets are needed if multiple interfaces will be configured.</p>  |
| Physical port number        | <p>This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17.</p> <p>A single physical port can facilitate multiple interfaces.</p> |
| Physical port description   | <p>This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used.</p> <p>Physical ports are configured within the destination context and are used to bind logical PDN interfaces.</p>                                       |
| Gateway IP address(es)      | <p>Used when configuring static routes from the PDN interface(s) to a specific network.</p>   |

## How This Configuration Works

The following figure and the text that follows describe how this configuration with a single source and destination context would be used by the system to process a Mobile IP data call.

**Figure 2: Call Processing When Using the system as a GGSN/FA**



1. A Create PDP Context Request message for a subscriber session is sent from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.
2. The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN. In this case, it is determined that Mobile IP must be used. From the APM configuration, the system also determines the context in which the FA service is configured.
3. If subscriber authentication is required, the GGSN authenticates the subscriber by communicating with a RADIUS server over the AAA interface.
4. The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface. The home address assigned to the mobile as part of the response is 0.0.0.0 indicating that it will be reset with a Home address after the PDP context activation procedure.
5. The FA component of the GGSN sends a Agent Advertisement message to the MS. The message contains the FA parameters needed by the mobile such as one or more care-of addresses. The message is sent as an IP limited broadcast message (i.e. destination address 255.255.255.255), however only on the requesting MS's TEID to avoid broadcast over the radio interface.
6. The MS sends a Mobile IP Registration request to the GGSN/FA. This message includes either the MS's static home address or it can request a temporary address by sending 0.0.0.0 as its home address. Additionally, the request must always include the Network Access Identifier (NAI) in a Mobile-Node-NAI Extension.



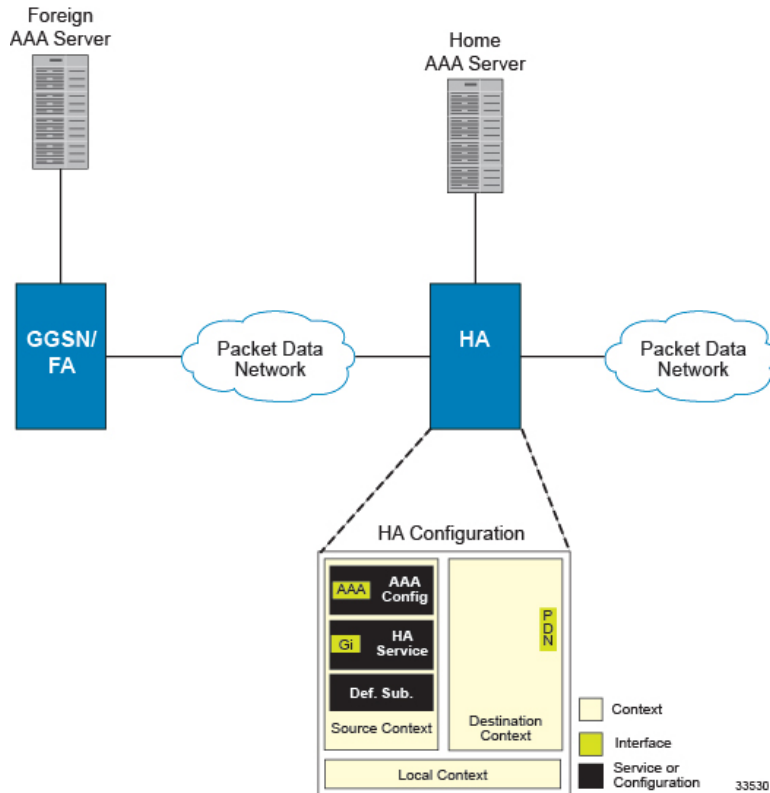
7. The FA forwards the registration request from the MS to the HA while the MS's home address or NAI and TEID are stored by the GGSN. In response the HA sends a registration response to the FA containing the address assigned to the MS.
8. The FA extracts the home address assigned to the MS by the HA from the response and the GGSN updates the associated PDP context. The FA then forwards it to the MS (identified by either the home address or the NAI and TEID).
9. The GGSN issues a PDP context modification procedure to the SGSN in order to update the PDP address for the MS.
10. The MS sends/receives data to/from the packet data network over the GGSN's PDN interface.
11. Upon termination of the subscriber session, the GGSN sends GGSN charging detail records to the CGF using GTPP over the Ga interface.

## Example 2: Mobile IP Support Using the System as an HA

The system supports both Simple and Mobile IP. For Mobile IP applications, the system can be configured to perform the function of a GGSN/FA and/or a HA. This example describes what is needed for and how the system performs the role of the HA. Example number 1 provides information on using the system to provide GGSN/FA functionality.

The system's HA configuration for Mobile IP applications requires that at least two contexts (one source and one destination) be configured as shown in the following figure.

Figure 3: Mobile IP Support Using the system as an HA



The source context will facilitate the HA service(s), the Gi interfaces from the FA, and the AAA interfaces. The source context will also be configured to provide Home AAA functionality for subscriber sessions. The destination context will facilitate the PDN interface(s).

## Information Required

Prior to configuring the system as shown in this example, there is a minimum amount of information required. The following sections describe the information required to configure the source and destination contexts.

### Source Context Configuration

The following table lists the information that is required to configure the source context.

Table 5: Required Information for Source Context Configuration

| Required Information       | Description   |
|----------------------------|---|
| Source context name        | An identification string from 1 to 79 characters (alpha and/or numeric) by which the source context will be recognized by the system. |
| Gi Interface Configuration |   |

| Required Information                  | Description   |
|---------------------------------------|---|
| Gi interface name                     | <p>This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system.</p> <p>Multiple names are needed if multiple interfaces will be configured.</p> <p>Gi interfaces are configured in the destination context.</p>   |
| IP address and subnet                 | <p>These will be assigned to the Gi interface.</p> <p>Multiple addresses and/or subnets are needed if multiple interfaces will be configured.</p>   |
| Physical port number                  | <p>This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17.</p> <p>A single physical port can facilitate multiple interfaces.</p> |
| Physical port description(s)          | <p>This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system.</p> <p>Multiple descriptions will be needed if multiple ports will be used.</p> <p>Physical ports are configured within the destination context and are used to bind logical Gi interfaces.</p>                             |
| Gateway IP address                    | <p>Used when configuring static routes from the Gi interface(s) to a specific network.</p>  |
| <b>HA service Configuration</b>       |   |
| HA service name                       | <p>An identification string from 1 to 63 characters (alpha and/or numeric) by which the HA service will be recognized by the system.</p> <p>Multiple names are needed if multiple HA services will be used.</p> <p>HA services are configured in the destination context.</p>   |
| UDP port number for Mobile IP traffic | <p>The port used by the HA service and the FA for communications. The UDP port number can be any integer value from 1 to 65535. The default value is 434.</p>   |

| Required Information                          | Description   |
|---|---|
| Mobile node re-registration requirements      | <p>Specifies how the system should handle authentication for mobile node re-registrations. The HA service can be configured as follows:</p> <ul style="list-style-type: none"> <li>• Always require authentication</li> <li>• Never require authentication</li> </ul> <p><b>Important</b> The initial registration and de-registration will still be handled normally)</p> <ul style="list-style-type: none"> <li>• Never look for mn-aaa extension</li> <li>• Not require authentication but will authenticate if mn-aaa extension present.</li> </ul>   |
| FA-to-HA Security Parameter Index Information | <p><b>FA IP address:</b> The HA service allows the creation of a security profile that can be associated with a particular FA.</p> <p>This specifies the IP address of the FA that the HA service will be communicating with.</p> <p>Multiple FA addresses are needed if the HA will be communicating with multiple FAs.</p> <p><b>Index:</b> Specifies the shared SPI between the HA service and a particular FA. The SPI can be configured to any integer value between 256 and 4294967295.</p> <p>Multiple SPIs can be configured if the HA service is to communicate with multiple FAs.</p> <p><b>Secret:</b> Specifies the shared SPI secret between the HA service and the FA. The secret can be between 1 and 127 characters (alpha and/or numeric).</p> <p>An SPI secret is required for each SPI configured.</p> <p><b>Hash-algorithm:</b> Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is <b>hmac-md5</b>.</p> <p>A hash-algorithm is required for each SPI configured.</p> |

| Required Information                             | Description  |
|--|--|
| Mobile Node Security Parameter Index Information | <p><b>Index:</b> Specifies the shared SPI between the HA service and a particular FA. The SPI can be configured to any integer value between 256 and 4294967295.</p> <p>Multiple SPIs can be configured if the HA service is to communicate with multiple FAs.</p> <p><b>Secret:</b> Specifies the shared SPI secret between the HA service and the FA. The secret can be between 1 and 127 characters (alpha and/or numeric).</p> <p>An SPI secret is required for each SPI configured.</p> <p><b>Hash-algorithm:</b> Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is <b>hmac-md5</b>.</p> <p>A hash-algorithm is required for each SPI configured.</p> <p><b>Replay-protection process:</b> Specifies how protection against replay-attacks is implemented. The possible processes are nonce and timestamp. The default is timestamp with a tolerance of 60 seconds.</p> <p>A replay-protection process is required for each mobile node-to-HA SPI configured.</p> |
| Maximum registration lifetime                    | <p>Specifies the longest registration lifetime that the HA service will allow in any Registration Request message from the mobile node.</p> <p>The time is measured in seconds and can be configured to any integer value between 1 and 65535. An infinite registration lifetime can also be configured by disabling the timer. The default is 600.</p>  |
| Maximum number of simultaneous bindings          | <p>Specifies the maximum number of "care-of" addresses that can simultaneously be bound for the same user as identified by NAI and Home address.</p> <p>The number can be configured to any integer value between 1 and 5. The default is 3.</p>   |
| AAA Interface Configuration                      |  |

| Required Information             | Description   |
|----------------------------------|---|
| AAA interface name               | <p>This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system.</p> <p>Multiple names are needed if multiple interfaces will be configured.</p> <p>AAA interfaces will be configured in the source context.</p>   |
| IP address and subnet            | <p>These will be assigned to the AAA interface.</p> <p>Multiple addresses and/or subnets are needed if multiple interfaces will be configured.</p>  |
| Physical port number             | <p>This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17.</p> <p>A single physical port can facilitate multiple interfaces.</p> |
| Physical port description        | <p>This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system.</p> <p>Multiple descriptions are needed if multiple ports will be used.</p> <p>Physical ports are used to bind logical AAA interfaces.</p>  |
| Gateway IP address               | <p>Used when configuring static routes from the AAA interface(s) to a specific network.</p>   |
| Home RADIUS Server Configuration |   |

| Required Information                     | Description  |
|--|--|
| Home RADIUS Authentication server        | <p><b>IP Address:</b> Specifies the IP address of the home RADIUS authentication server the system will communicate with to provide subscriber authentication functions.</p> <p>Multiple addresses are needed if multiple RADIUS servers.</p> <p>Home RADIUS servers are configured with in the source context. Multiple servers can be configured and each can be assigned a priority.</p> <hr/> <p><b>Shared Secret:</b> The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS authentication server and the source context.</p> <p>A shared secret is needed for each configured RADIUS server.</p> <hr/> <p><b>UDP Port Number:</b> Specifies the port used by the source context and the RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.</p>                         |
| Home RADIUS Accounting server (optional) | <p><b>IP Address:</b> Specifies the IP address of the home RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions.</p> <p>Multiple addresses are needed if multiple RADIUS servers will be configured. RADIUS accounting servers are configured within the source context.</p> <p>Multiple servers can be configured and each assigned a priority.</p> <hr/> <p><b>Shared Secret:</b> The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the home RADIUS accounting server and the source context.</p> <p>A shared secret is needed for each configured RADIUS server.</p> <hr/> <p><b>UDP Port Number:</b> Specifies the port used by the source context and the home RADIUS Accounting server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1813.</p> |

| Required Information                   | Description  |
|--|--|
| RADIUS attribute NAS Identifier        | Specifies the name by which the source context will be identified in the Access-Request message(s) it sends to the RADIUS server. The name must be from 1 to 32 alpha and/or numeric characters and is case sensitive.     |
| RADIUS NAS IP address                  | Specifies the IP address of the system's AAA interface. A secondary address can be optionally configured.  |
| Default Subscriber Configuration       |  |
| "Default" subscriber's IP context name | Specifies the name of the egress context on the system that facilitates the Gi interfaces.<br><br><b>Important</b> For this configuration, the IP context name should be identical to the name of the destination context. |

## Destination Context Configuration

The following table lists the information required to configure the destination context.

**Table 6: Required Information for Destination Context Configuration 3**

| Required Information        | Description   |
|-----------------------------|---|
| Destination context name    | This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the destination context will be recognized by the system.<br><br><b>Important</b> For this configuration, the destination context name should <b>not</b> match the domain name of a specific domain. |
| PDN Interface Configuration |   |
| PDN interface name          | This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system.<br><br>Multiple names are needed if multiple interfaces will be configured.<br><br>PDN interfaces are configured in the destination context.         |
| IP address and subnet       | These will be assigned to the PDN interface.<br><br>Multiple addresses and/or subnets are needed if multiple interfaces will be configured.   |

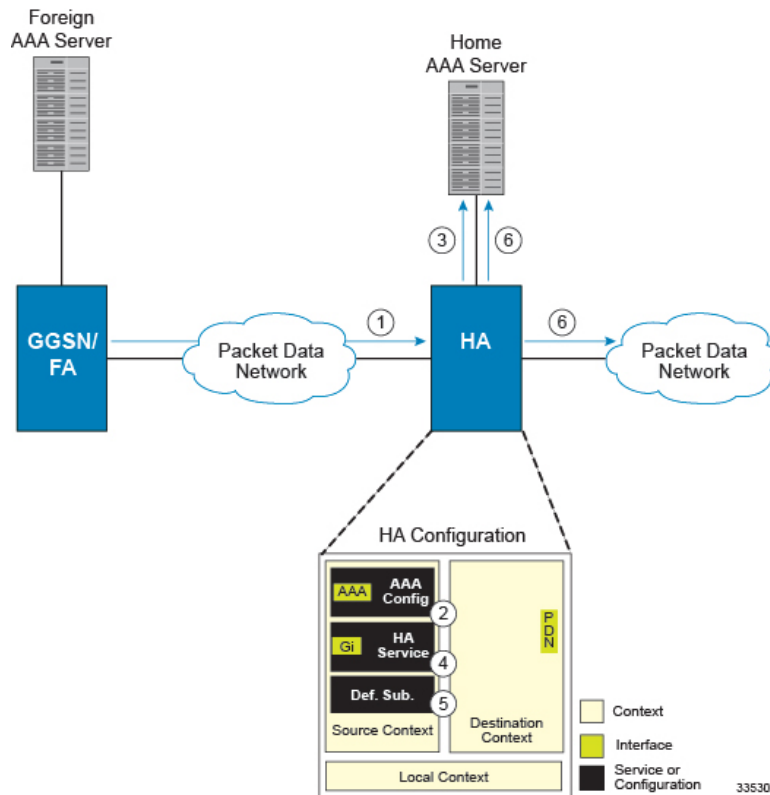


| Required Information          | Description   |
|-------------------------------|---|
| Physical port number          | <p>This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17.</p> <p>A single physical port can facilitate multiple interfaces.</p> |
| Physical port description     | <p>This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used.</p> <p>Physical ports are configured within the destination context and are used to bind logical PDN interfaces.</p>                                       |
| Gateway IP address(es)        | Used when configuring static routes from the PDN interface(s) to a specific network.  |
| IP Address Pool Configuration |   |
| IP address pool name          | <p>Each IP address pool is identified by a name. The pool name can be between 1 and 31 alpha and/or numeric characters and is case sensitive.</p> <p>IP address pools are configured in the destination context(s). Multiple address pools can be configured within a single context.</p>   |
| IP pool addresses             | <p>An initial address and a subnet, or a starting address and an ending address, are required for each configured pool. The pool will then consist of every possible address within the subnet, or all addresses from the starting address to the ending address.</p> <p>The pool can be configured as public, private, or static.</p>  |

## How This Configuration Works

The following figure and the text that follows describe how this configuration with a single source and destination context would be used by the system to process a Mobile IP data call.

Figure 4: Call Processing When Using the system as an HA



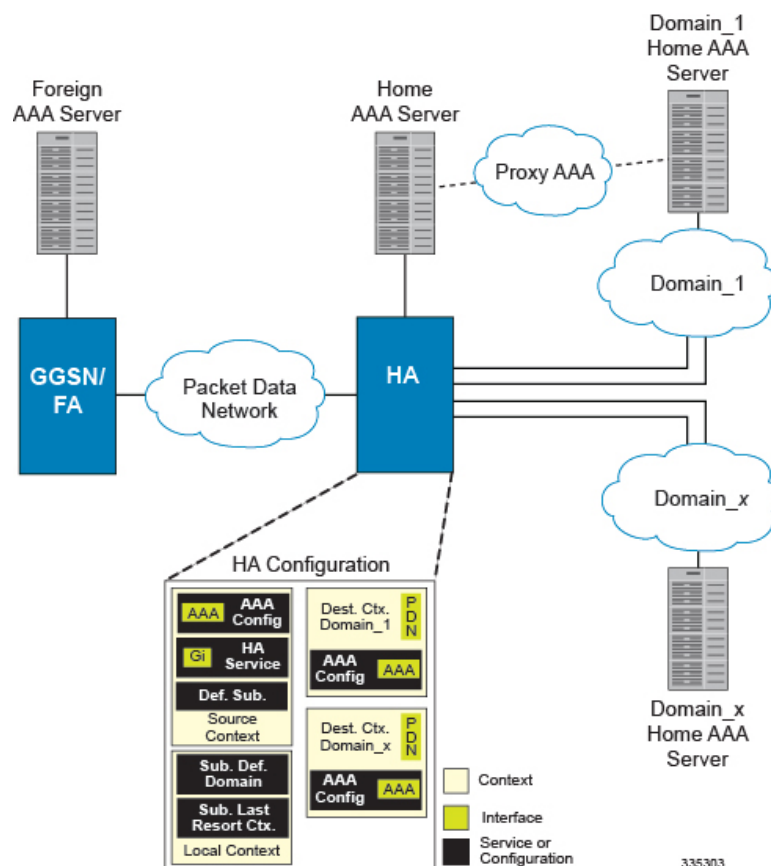
1. A subscriber session from the FA is received by the HA service over the Gi interface.
2. The HA service determines which context to use to provide AAA functionality for the session. This process is described in the *How the System Selects Contexts* section located in the *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*.  
For this example, the result of this process is that the HA service determined that AAA functionality should be provided by the *Source* context.
3. The system then communicates with the Home AAA server specified in the Source context's AAA configuration to authenticate the subscriber.
4. Upon successful authentication, the *Source* context determines which egress context to use for the subscriber session. This process is described in the *How the System Selects Contexts* section located in the *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*.  
For this example, the system determines that the egress context is the *Destination* context based on the configuration of the *Default* subscriber.
5. An IP address is assigned to the subscriber's mobile node from an IP address pool configured in the destination context. This IP address is used for the duration of the session and then be returned to the pool.
6. Data traffic for the subscriber session is then routed through the PDN interface in the *Destination* context.
7. Accounting messages for the session are sent to the AAA server over the AAA interface.

## Example 3: HA Using a Single Source Context and Multiple Outsourced Destination Contexts

The system allows the wireless carrier to easily generate additional revenue by providing the ability to configure separate contexts that can then be leased or outsourced to various enterprises or ISPs, each having a specific domain.

In order to perform the role of an HA and support multiple outsourced domains, the system must be configured with at least one source context and multiple destination contexts as shown in the following figure. The AAA servers could be owned/maintained by either the carrier or the domain. If they are owned by the domain, the carrier will have to receive the AAA information via proxy.

**Figure 5: The system as an HA Using a Single Source Context and Multiple Outsourced Destination Contexts**



The source context will facilitate the HA service(s), and the Gi interface(s) to the FA(s). The source context will also be configured with AAA interface(s) and to provide Home AAA functionality for subscriber sessions. The destination contexts will each be configured to facilitate PDN interfaces. In addition, because each of the destination contexts can be outsourced to different domains, they will also be configured with AAA interface(s) and to provide AAA functionality for that domain.

In addition to the source and destination contexts, there are additional system-level AAA parameters that must be configured.

## Information Required

Prior to configuring the system as shown in this example, there is a minimum amount of information required. The following sections describe the information required to configure the source and destination contexts.

### Source Context Configuration

The following table lists the information that is required to configure the source context.

**Table 7: Required Information for Source Context Configuration**

| Required Information       | Description   |
|----------------------------|---|
| Source context name        | An identification string from 1 to 79 characters (alpha and/or numeric) by which the source context will be recognized by the system.   |
| Gi Interface Configuration |   |
| Gi interface name          | An identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system.<br><br>Multiple names are needed if multiple interfaces will be configured.<br><br>Gi interfaces are configured in the destination context.  |
| IP address and subnet      | These will be assigned to the Gi interface.<br><br>Multiple addresses and/or subnets are needed if multiple interfaces will be configured.  |
| Physical port number       | The physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17.<br><br>A single physical port can facilitate multiple interfaces. |
| Physical port description  | An identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system.<br><br>Multiple descriptions are needed if multiple ports will be used.<br><br>Physical ports are configured within the source context and are used to bind logical Gn interfaces.                                   |
| Gateway IP address         | Used when configuring static routes from the Gi interface(s) to a specific network.   |
| HA service Configuration   |   |

| Required Information                     | Description   |
|--|---|
| HA service name                          | <p>An identification string from 1 to 63 characters (alpha and/or numeric) by which the HA service will be recognized by the system.</p> <p>Multiple names are needed if multiple HA services will be used.</p> <p>HA services are configured in the destination context.</p>   |
| UDP port number for Mobile IP traffic    | <p>The port used by the HA service and the FA for communications. The UDP port number can be any integer value from 1 to 65535. The default value is 434.</p>   |
| Mobile node re-registration requirements | <p>Specifies how the system should handle authentication for mobile node re-registrations. The HA service can be configured as follows:</p> <ul style="list-style-type: none"><li>• Always require authentication</li><li>• Never require authentication</li></ul> <p><b>Important</b> The initial registration and de-registration will still be handled normally)</p> <ul style="list-style-type: none"><li>• Never look for mn-aaa extension</li><li>• Not require authentication but will authenticate if mn-aaa extension present.</li></ul> |

| Required Information                          | Description  |
|---|--|
| FA-to-HA Security Parameter Index Information | <p><b>FA IP address:</b> The HA service allows the creation of a security profile that can be associated with a particular FA.</p> <p>This specifies the IP address of the FA that the HA service will be communicating with.</p> <p>Multiple FA addresses are needed if the HA will be communicating with multiple FAs.</p> |
|   | <p><b>Index:</b> Specifies the shared SPI between the HA service and a particular FA. The SPI can be configured to any integer value between 256 and 4294967295.</p> <p>Multiple SPIs can be configured if the HA service is to communicate with multiple FAs.</p>   |
|   | <p><b>Secret:</b> Specifies the shared SPI secret between the HA service and the FA. The secret can be between 1 and 127 characters (alpha and/or numeric).</p> <p>An SPI secret is required for each SPI configured.</p>  |
|   | <p><b>Hash-algorithm:</b> Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is <b>hmac-md5</b>.</p> <p>A hash-algorithm is required for each SPI configured.</p>                            |

| Required Information                             | Description  |
|--|--|
| Mobile Node Security Parameter Index Information | <p><b>Index:</b> Specifies the shared SPI between the HA service and a particular FA. The SPI can be configured to any integer value between 256 and 4294967295.</p> <p>Multiple SPIs can be configured if the HA service is to communicate with multiple FAs.</p> <p><b>Secret:</b> Specifies the shared SPI secret between the HA service and the FA. The secret can be between 1 and 127 characters (alpha and/or numeric).</p> <p>An SPI secret is required for each SPI configured.</p> <p><b>Hash-algorithm:</b> Specifies the algorithm used to hash the SPI and SPI secret. The possible algorithms that can be configured are MD5 per RFC 1321 and keyed-MD5 per RFC 2002. The default algorithm is <b>hmac-md5</b>.</p> <p>A hash-algorithm is required for each SPI configured.</p> <p><b>Replay-protection process:</b> Specifies how protection against replay-attacks is implemented. The possible processes are nonce and timestamp. The default is timestamp with a tolerance of 60 seconds.</p> <p>A replay-protection process is required for each mobile node-to-HA SPI configured.</p> |
| Maximum registration lifetime                    | <p>Specifies the longest registration lifetime that the HA service will allow in any Registration Request message from the mobile node.</p> <p>The time is measured in seconds and can be configured to any integer value between 1 and 65535. An infinite registration lifetime can also be configured by disabling the timer. The default is 600.</p>  |
| Maximum number of simultaneous bindings          | <p>Specifies the maximum number of "care-of" addresses that can simultaneously be bound for the same user as identified by NAI and Home address.</p> <p>The number can be configured to any integer value between 1 and 5. The default is 3.</p>   |
| AAA Interface Configuration                      |  |

| Required Information             | Description   |
|----------------------------------|---|
| AAA interface name               | <p>This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system.</p> <p>Multiple names are needed if multiple interfaces will be configured.</p> <p>AAA interfaces will be configured in the source context.</p>   |
| IP address and subnet            | <p>These will be assigned to the AAA interface.</p> <p>Multiple addresses and/or subnets are needed if multiple interfaces will be configured.</p>  |
| Physical port number             | <p>This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17.</p> <p>A single physical port can facilitate multiple interfaces.</p> |
| Physical port description        | <p>This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system.</p> <p>Multiple descriptions are needed if multiple ports will be used.</p> <p>Physical ports are used to bind logical AAA interfaces.</p>  |
| Gateway IP address               | <p>Used when configuring static routes from the AAA interface(s) to a specific network.</p>   |
| Home RADIUS Server Configuration |   |



| Required Information                     | Description  |
|--|--|
| Home RADIUS Authentication server        | <p><b>IP Address:</b> Specifies the IP address of the home RADIUS authentication server the system will communicate with to provide subscriber authentication functions.</p> <p>Multiple addresses are needed if multiple RADIUS servers.</p> <p>Home RADIUS servers are configured with in the source context. Multiple servers can be configured and each can be assigned a priority.</p> <hr/> <p><b>Shared Secret:</b> The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS authentication server and the source context.</p> <p>A shared secret is needed for each configured RADIUS server.</p> <hr/> <p><b>UDP Port Number:</b> Specifies the port used by the source context and the RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.</p>                         |
| Home RADIUS Accounting server (optional) | <p><b>IP Address:</b> Specifies the IP address of the home RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions.</p> <p>Multiple addresses are needed if multiple RADIUS servers will be configured. RADIUS accounting servers are configured within the source context.</p> <p>Multiple servers can be configured and each assigned a priority.</p> <hr/> <p><b>Shared Secret:</b> The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the home RADIUS accounting server and the source context.</p> <p>A shared secret is needed for each configured RADIUS server.</p> <hr/> <p><b>UDP Port Number:</b> Specifies the port used by the source context and the home RADIUS Accounting server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1813.</p> |

| Required Information                   | Description  |
|--|--|
| RADIUS attribute NAS Identifier        | Specifies the name by which the source context will be identified in the Access-Request message(s) it sends to the RADIUS server. The name must be from 1 to 32 alpha and/or numeric characters and is case sensitive.     |
| RADIUS NAS IP address                  | Specifies the IP address of the system's AAA interface. A secondary address can be optionally configured.  |
| Default Subscriber Configuration       |  |
| "Default" subscriber's IP context name | Specifies the name of the egress context on the system that facilitates the Gi interfaces.<br><br><b>Important</b> For this configuration, the IP context name should be identical to the name of the destination context. |

## Destination Context Configuration

The following table lists the information required to configure the destination context. This information will be required for each domain.

**Table 8: Required Information for Destination Context Configuration 11**

| Required Information        | Description  |
|-----------------------------|--|
| Destination context name    | This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the destination context will be recognized by the system. <b>NOTE:</b> For this configuration, the destination context name should <b>not</b> match the domain name of a specific domain. |
| PDN Interface Configuration |  |
| PDN interface name          | This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. PDN interfaces are configured in the destination context.            |
| IP address and subnet       | These will be assigned to the PDN interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.   |

| Required Information                     | Description   |
|--|---|
| Physical port number                     | This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces. |
| Physical port description                | This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical PDN interfaces.                                       |
| Gateway IP address(es)                   | Used when configuring static routes from the PDN interface(s) to a specific network.  |
| IP Address Pool Configuration (optional) |   |
| IP address pool name                     | <p>Each IP address pool is identified by a name. The pool name can be between 1 and 31 alpha and/or numeric characters and is case sensitive.</p> <p>IP address pools are configured in the destination context(s). Multiple address pools can be configured within a single context.</p>   |
| IP pool addresses                        | <p>An initial address and a subnet, or a starting address and an ending address, are required for each configured pool. The pool will then consist of every possible address within the subnet, or all addresses from the starting address to the ending address.</p> <p>The pool can be configured as public, private, or static.</p>                            |
| AAA Interface Configuration              |   |
| AAA interface name                       | <p>This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the interface will be recognized by the system.</p> <p>Multiple names are needed if multiple interfaces will be configured.</p>   |
| IP address and subnet                    | <p>These will be assigned to the AAA interface.</p> <p>Multiple addresses and/or subnets are needed if multiple interfaces will be configured.</p>  |

| Required Information               | Description  |
|------------------------------------|--|
| Physical port number               | <p>This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17.</p> <p>A single physical port can facilitate multiple interfaces.</p>  |
| Physical port description          | <p>This is an identification string from 1 to 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system.</p> <p>Multiple descriptions are needed if multiple ports will be used.</p> <p>Physical ports are used to bind logical AAA interfaces.</p>   |
| Gateway IP address                 | Used when configuring static routes from the AAA interface(s) to a specific network.   |
| <b>RADIUS Server Configuration</b> |  |
| RADIUS Authentication server       | <p><b>IP Address:</b> Specifies the IP address of the RADIUS authentication server the system will communicate with to provide subscriber authentication functions.</p> <p>Multiple addresses are needed if multiple RADIUS servers.</p> <p>Foreign RADIUS servers are configured with in the source context. Multiple servers can be configured and each can be assigned a priority.</p> <p><b>Shared Secret:</b> The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS authentication server and the source context.</p> <p>A shared secret is needed for each configured RADIUS server.</p> <p><b>UDP Port Number:</b> Specifies the port used by the source context and the RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.</p> |

| Required Information                | Description   |
|-------------------------------------|---|
| RADIUS Accounting server (optional) | <p><b>IP Address:</b> Specifies the IP address of the RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions.</p> <p>Multiple addresses are needed if multiple RADIUS servers will be configured. RADIUS accounting servers are configured within the source context.</p> <p>Multiple servers can be configured and each assigned a priority.</p> <p><b>Shared Secret:</b> The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS accounting server and the source context.</p> <p>A shared secret is needed for each configured RADIUS server.</p> <p><b>UDP Port Number:</b> Specifies the port used by the source context and the RADIUS Accounting server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1813.</p> |
| RADIUS attribute NAS Identifier     | Specifies the name by which the source context will be identified in the Access-Request message(s) it sends to the RADIUS server. The name must be from 1 to 32 alpha and/or numeric characters and is case sensitive.  |
| RADIUS NAS IP address               | Specifies the IP address of the system's AAA interface. A secondary address can be optionally configured.   |

## System-Level AAA Configuration

The following table lists the information that is required to configure the system-level AAA parameters.

Table 9: Required Information for System-Level AAA Configuration

| Required Information           | Description  |
|--------------------------------|--|
| Subscriber default domain name | <p>Specifies the name of a context that can provide AAA functions in the event that the domain-part of the username is missing or poorly formed.</p> <p>This parameter will be applied to all subscribers if their domain can not be determined from their username regardless of what domain they are trying to access.</p> <p><b>Important</b> The default domain name can be the same as the source context.</p>  |
| Subscriber Last-resort context | <p>Specifies the name of a context that can provide AAA functions in the event that the domain-part of the username was present but does not match the name of a configured destination context</p> <p>.This parameter will be applied to all subscribers if their specified domain does not match a configured destination context regardless of what domain they are trying to access.</p> <p><b>Important</b> The last-resort context name can be the same as the source context.</p>   |
| Subscriber username format     | <p>Specifies the format of subscriber usernames as to whether or not the username or domain is specified first and the character that separates them. The possible separator characters are:</p> <ul style="list-style-type: none"> <li>• @</li> <li>• %</li> <li>• -</li> <li>• \</li> <li>• #</li> <li>• /</li> </ul> <p>Up to six username formats can be specified. The default is <i>username</i> .</p> <p><b>Important</b> The username string is searched from right to left for the separator character. Therefore, if there is one or more separator characters in the string, only the first one that is recognized is considered the actual separator. For example, if the default username format was used, then for the username string <i>user1enterpriseisp1</i>, the system resolves to the username <i>user1enterprise</i> with domain <i>isp1</i>.</p> |



- For *subscriber2*, the HA service determines that no domain name is present.
  - For *subscriber3*, the HA service determines that a domain name is present and is *Domain37*.
5. The HA service determines which context to use to provide AAA functionality for the session. This process is described in the *How the System Selects Contexts* section located in the *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*.
    - For *subscriber1*, the HA service determines that a context was configured with a name (*Domain1*) that matches the domain name specified in the username string. Therefore, *Domain1* is used.
    - For *subscriber2*, the HA service determines that *Domainx* is configured as the default domain name. Therefore, *Domainx* is used.
    - For *subscriber3*, the HA service determines that no context is configured that matches the domain name (*Domain37*) specified in the username string. Because no **last-resort** context name was configured, the *Source* context is used.
  6. The system then communicates with the Home AAA server specified in the Source context's AAA configuration to authenticate the subscriber.
  7. Upon successful authentication of all three subscribers, the HA service determines which destination context to use for each of the subscriber sessions. This process is described in the *How the System Selects Contexts* section located in the *Understanding the System Operation and Configuration* chapter of the *System Administration Guide*.
    - For *subscriber1*, the HA service receives the *SN-VPN-NAME* or *SNI-VPN-NAME* attribute equal to *Domain1* as part of the Authentication Accept message from the AAA server on *Domain1*'s network. Therefore, *Domain1* is used as the destination context.
    - For *subscriber2*, the HA service determines that the *SN-VPN-NAME* or *SNI-VPN-NAME* attribute was not returned with the Authentication Accept response, and determines the subscriber IP context name configured within the *Domainx* context. Therefore, the *Domainx* context is used as the destination context.
    - For *subscriber3*, the HA service determines that the *SN-VPN-NAME* or *SNI-VPN-NAME* attribute was not returned with the Authentication Accept response, and determines the subscriber IP context name configured within the *Source* context. Therefore, the *Source* context is used as the destination context.
  8. Data traffic for the subscriber session is then routed through the PDN interface in the each subscriber's destination context.
  9. Accounting messages for the session are sent to the AAA server over the appropriate AAA interface.