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 management context. Information about the local management context can be found in Chapter 1 of Command Line Reference. Additionally, when configuring Mobile IP take into account the MIP timing considerations discussed in *MIP Timer Considerations*.

This chapter contains the following topics:

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

The system supports both Simple and Mobile IP. For Mobile IP applications, the system can be configured to perform the function of a Packet Data Serving Node/Foreign Agent (PDSN/FA) and/or a Home Agent (HA). This example describes what is needed for and how the system performs the role of the PDSN/FA. Examples 2 and 3 provide information on using the system to provide HA functionality.

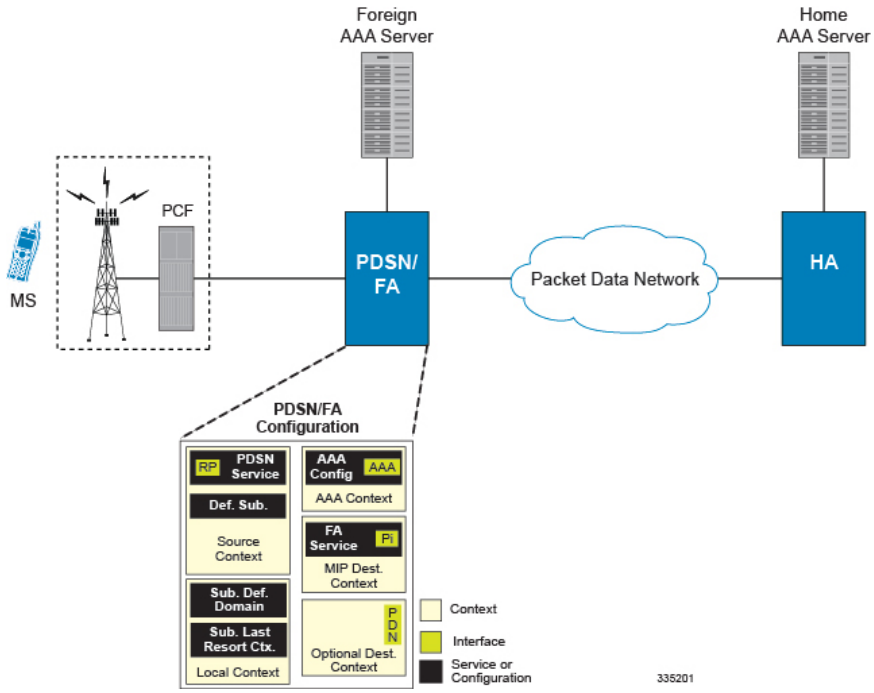
The system's PDSN/FA configuration for Mobile IP applications is best addressed with three contexts (one source, one AAA, and one Mobile IP destination) configured as shown in the figure below.

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 PDSN service(s), and the R-P interfaces. The AAA context will be configured to provide foreign AAA functionality for subscriber sessions and facilitate the AAA interfaces. The MIP destination context will facilitate the FA service(s) and the Pi interface(s) from the PDSN/FA to the HA.

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 was disabled.

Figure 1: Mobile IP Support using the system as a PDSN/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	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the source context will be recognized by the system.
R-P Interface Configuration	

Required Information	Description
R-P 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. R-P interfaces are configured in the source context.
IP address and subnet	These will be assigned to the R-P interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
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 using multiple ports. Physical ports are configured within the source context and are used to bind logical R-P interfaces.
Gateway IP address	Used when configuring static routes from the R-P interface(s) to a specific network.
PDSN service Configuration	
PDSN service name	This is an identification string between 1 and 63 characters (alpha and/or numeric) by which the PDSN service will be recognized by the system. Multiple names are needed if using multiple PDSN services. PDSN services are configured in the source context.
UDP port number for R-P traffic	Specifies the port used by the PDSN service and the PCF for communications. The UDP port number and can be any integer value between 1 and 65535. The default value is 699.

Required Information	Description
Authentication protocols used	Specifies how the system handles authentication: using a protocol (such as CHAP, PAP, or MSCHAP), or not requiring any authentication.
Domain alias for NAI-construction	Specifies a context name for the system to use to provide accounting functionality for a subscriber session. This parameter is needed only if the system is configured to support no authentication.
Security Parameter Index Information	**PCF IP address:** Specifies the IP address of the PCF that the PDSN service will be communicating with. The PDSN service allows the creation of a security profile that can be associated with a particular PCF. Multiple IP addresses are needed if the PDSN service is to communicate with multiple PCFs.
	Index: Specifies the shared SPI between the PDSN service and a particular PCF. The SPI can be configured to any integer value between 256 and 4294967295. Configure multiple SPIs if the PDSN service is to communicate with multiple PCFs.
	Secret: Specifies the shared SPI secret between the PDSN service and the PCF. The secret can be between 1 and 127 characters (alpha and/or numeric). An SPI secret is required for each SPI configured.
	Hash-algorithm: 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 MD5. A hash-algorithm is required for each SPI configured.
	Replay-protection process: 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. A replay-protection process is required for each SPI configured.

Required Information	Description
Subscriber session lifetime	Specifies the time in seconds that an A10 connection can exist before its registration is considered expired. The time is expressed in seconds and can be configured to any integer value between 1 and 65534, or the timer can be disabled to set an infinite lifetime. The default value is 1800 seconds.
Mobile IP FA context name	Specifies the name of the context in which the FA service is configured.

AAA Context Configuration

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

Table 2: Required Information for AAA Context Configuration

Required Information	Description
AAA context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the AAA context will be recognized by the system. **Important** 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.
AAA Interface Configuration	
AAA 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. AAA interfaces will be configured in the source context.
IP address and subnet	These will be assigned to the AAA 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 AAA interfaces.
Gateway IP address(es)	Used when configuring static routes from the AAA interface(s) to a specific network.
Foreign RADIUS Server Configuration	

Required Information	Description
Foreign RADIUS Authentication server	**IP Address**: Specifies the IP address of the foreign RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions. Multiple addresses are needed if configuring multiple RADIUS servers. Foreign RADIUS accounting servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key exchanged between the RADIUS accounting server and the source context. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: 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 1812.

Required Information	Description
Foreign RADIUS Accounting server	**IP Address**: Specifies the IP address of the foreign RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions. Multiple addresses are needed if configuring multiple RADIUS servers. Foreign RADIUS accounting servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key exchanged between the RADIUS accounting server and the source context. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: 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.
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 foreign RADIUS server. The name must be between 1 and 32 alpha and/or numeric characters and is case sensitive.
RADIUS NAS IP address	Specifies the IP address of the source context's AAA interface. A secondary address can be optionally configured.

Mobile IP Destination Context Configuration

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

Table 3: Required Information for Destination Context Configuration

Required Information	Description
Mobile IP 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. **Important** For this configuration, the destination context name should **not** 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.
Pi Interface Configuration	
Pi 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. Pi interfaces are configured in the destination context.
IP address and subnet	These will be assigned to the Pi interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
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 Pi interfaces.
Gateway IP address(es)	Used when configuring static routes from the Pi interface(s) to a specific network.
FA Service Configuration	

Required Information	Description
FA service name	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. Multiple names are needed if multiple FA services will be used. FA services are configured in the destination context.
UDP port number for Mobile IP traffic	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.
Security Parameter Index (indices) Information	HA IP address: 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.
	Index: 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.
	Secrets: 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.
	Hash-algorithm: 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.
FA agent advertisement lifetime	Specifies the time (in seconds) that an FA agent advertisement remains valid in the absence of further advertisements. The time can be configured to any integer value between 1 and 65535. The default is 9000.

Required Information	Description
Number of allowable unanswered FA advertisements	Specifies the number of unanswered agent advertisements that the FA service will allow during call setup before it will reject the session. The number can be any integer value between 1 and 65535. The default is 5.
Maximum mobile-requested registration lifetime allowed	Specifies the longest registration lifetime that the FA service will allow in any Registration Request message from the mobile node. 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.
Registration reply timeout	Specifies the amount of time that the FA service will wait for a Registration Reply from an HA. The time is measured in seconds and can be configured to any integer value between 1 and 65535. The default is 7.
Number of simultaneous registrations	Specifies the number of simultaneous Mobile IP sessions that will be supported for a single subscriber. The maximum number of sessions is 3. The default is 1. **Important** The system will only support multiple Mobile IP sessions per subscriber if the subscriber's mobile node has a static IP address.
Mobile node re-registration requirements	Specifies how the system should handle authentication for mobile node re-registrations. 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.

System-Level AAA Configuration

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

Table 4: Required Information for System-Level AAA Configuration

Required Information	Description
Subscriber default domain name	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. 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. **Important** The default domain name can be the same as the source context.
Subscriber Last-resort context	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. 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. **Important** The last-resort context name can be the same as the source context.

Required Information	Description
Subscriber username format	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: • @ • % • - • \ • # • / Up to six username formats can be specified. The default is *username* @. **Important** 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 *user1@enterprise@isp1*, the system resolves to the username *user1@enterprise* with domain *isp1*.

Optional Destination Context

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 5: Required Information for Destination Context Configuration 0

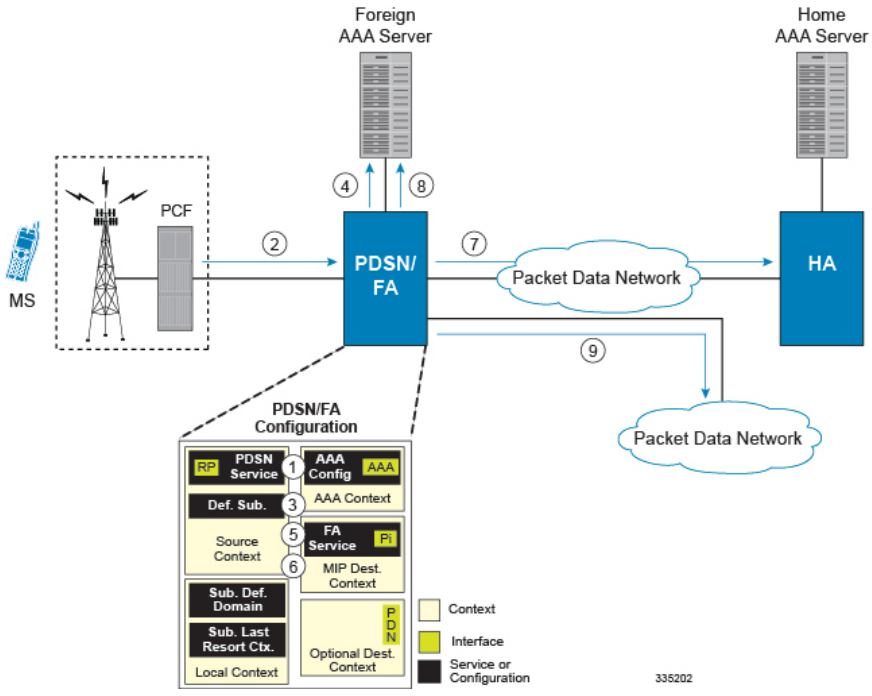
Required Information	Description
Destination context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the destination context will be recognized by the system. **Important** For this configuration, the destination context name should not match the domain 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.
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	

Required Information	Description
IP address pool name	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. IP address pools are configured in the destination context(s). Multiple address pools can be configured within a single context.
IP pool addresses	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. The pool can be configured as public, private, or static. If this IP pool is being used for Interchassis Session Recovery, it must be a static and srp-activated.

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 PDSN/FA



1. The system-level AAA settings were configured as follows:
   - Subscriber default domain name = *AAA context*

- Subscriber username format = *username @*
- Subscriber last-resort context name = *AAA context*

2. A subscriber session from the PCF is received by the PDSN service over the R-P interface.
3. The PDSN service determines which context to use to provide foreign 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 PDSN service determined that foreign AAA functionality should be provided by the *AAA context*.
4. The system then communicates with the foreign AAA server specified in the AAA context's AAA configuration to authenticate the subscriber.
5. Upon successful authentication, the PDSN service determines the IP address of the subscriber's HA using either an attribute returned in the Access Accept message, or the address specified by the mobile.

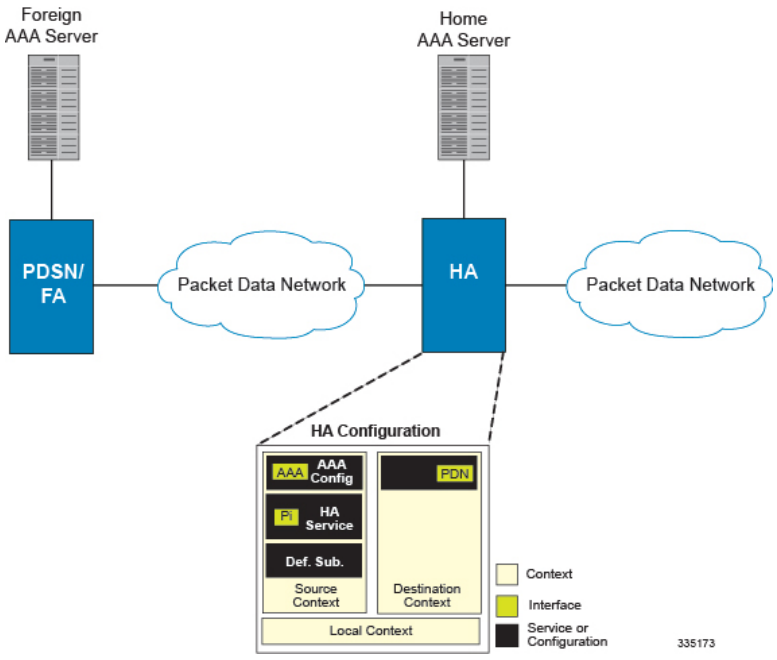
   The PDSN service uses the Mobile IP FA context name to determine what destination context is facilitating the FA service. In this example, it determines that it must use the *MIP Destination* context.
6. The PDSN service passes the HA IP address to the FA service.
7. The FA service then establishes a connection to the specified HA over the Pi interface.
8. Accounting messages for the session are sent to the Foreign AAA server over the AAA interface.
9. If reverse tunneling is disabled, then subscriber data traffic would have been routed over the PDN interface configured in the *Optional Destination* context.

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 PDSN/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 PDSN/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 Pi 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 6: Required Information for Source Context Configuration

Required Information	Description
Source context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the source context will be recognized by the system. **Important** 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 PDSN/FA functionality.
Pi Interface Configuration	

Required Information	Description
Pi 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. Pi interfaces are configured in the source context. If this interface is being used for Interchassis Session Recovery, you must specify a loopback interface type after the interface_name.
IP address and subnet	These will be assigned to the Pi interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
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 using multiple ports. Physical ports are configured within the source context and are used to bind logical Pi interfaces.
Gateway IP address	Used when configuring static routes from the R-P interface(s) to a specific network.
HA service Configuration	
HA service name	This is an identification string between 1 and 63 characters (alpha and/or numeric) by which the HA service will be recognized by the system. Multiple names are needed if multiple HA services will be used. HA services are configured in the destination context.
UDP port number for Mobile IP traffic	Specifies the port used by the HA service and the FA for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 434.

Required Information	Description
Mobile node re-registration requirements	Specifies how the system should handle authentication for mobile node re-registrations. The HA service can be configured as follows:Always require authentication Never require authentication (NOTE: the initial registration and de-registration will still be handled normally) Never look for mn-aaa extension Not require authentication but will authenticate if mn-aaa extension present
FA-to-HA Security Parameter Index Information	FA IP address: The HA service allows the creation of a security profile that can be associated with a particular FA. This specifies the IP address of the FA that the HA service will be communicating with. Multiple FA addresses are needed if the HA will be communicating with multiple FAs.
	Index: 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. Multiple SPIs can be configured if the HA service is to communicate with multiple FAs.
	Secret: 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). An SPI secret is required for each SPI configured.
	Hash-algorithm: 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 hmac-md5. A hash-algorithm is required for each SPI configured.

Required Information	Description
Mobile Node Security Parameter Index Information	Index: Specifies the shared SPI between the HA service and the mobile node(s). The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the HA service is to communicate with multiple mobile nodes.
	Secret(s): Specifies the shared SPI secret between the HA service and the mobile node. The secret can be between 1 and 127 characters (alpha and/or numeric). An SPI secret is required for each SPI configured.
	Hash-algorithm: 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 hmac-md5. A hash-algorithm is required for each SPI configured.
	Replay-protection process: 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. A replay-protection process is required for each mobile node-to-HA SPI configured.
Maximum registration lifetime	Specifies the longest registration lifetime that the HA service will allow in any Registration Request message from the mobile node. The time is measured in seconds and can be configured to any integer value between 1 and 65534. An infinite registration lifetime can also be configured by disabling the timer. The default is 600.
Maximum number of simultaneous bindings	Specifies the maximum number of "care-of" addresses that can simultaneously be bound for the same user as identified by NAI and Home address. The number can be configured to any integer value between 1 and 5. The default is 3.
AAA Interface Configuration	

Required Information	Description
AAA 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. AAA interfaces will be configured in the source context.
IP address and subnet	These will be assigned to the AAA interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
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 source context and are used to bind logical AAA interfaces.
Gateway IP address	Used when configuring static routes from the AAA interface(s) to a specific network.
Home RADIUS Server Configuration	
Home RADIUS Authentication server	IP Address:Specifies the IP address of the home RADIUS authentication server the source context will communicate with to provide subscriber authentication functions. Multiple addresses are needed if multiple RADIUS servers will be configured. Home RADIUS authentication servers are configured within the source context. Multiple servers can be configured and each assigned a priority.

Required Information	Description
	Shared Secret: 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. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the home RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.
Home RADIUS Accounting server	IP Address: Specifies the IP address of the home RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions. Multiple addresses are needed if multiple RADIUS servers will be configured.Home RADIUS accounting servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	Shared Secret: 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. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: 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.
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 home RADIUS server. The name must be between 1 and 32 alpha and/or numeric characters and is case sensitive.

Required Information	Description
RADIUS NAS IP address	Specifies the IP address of the source context'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 PDN ports. **Important** 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 7: Required Information for Destination Context Configuration 1

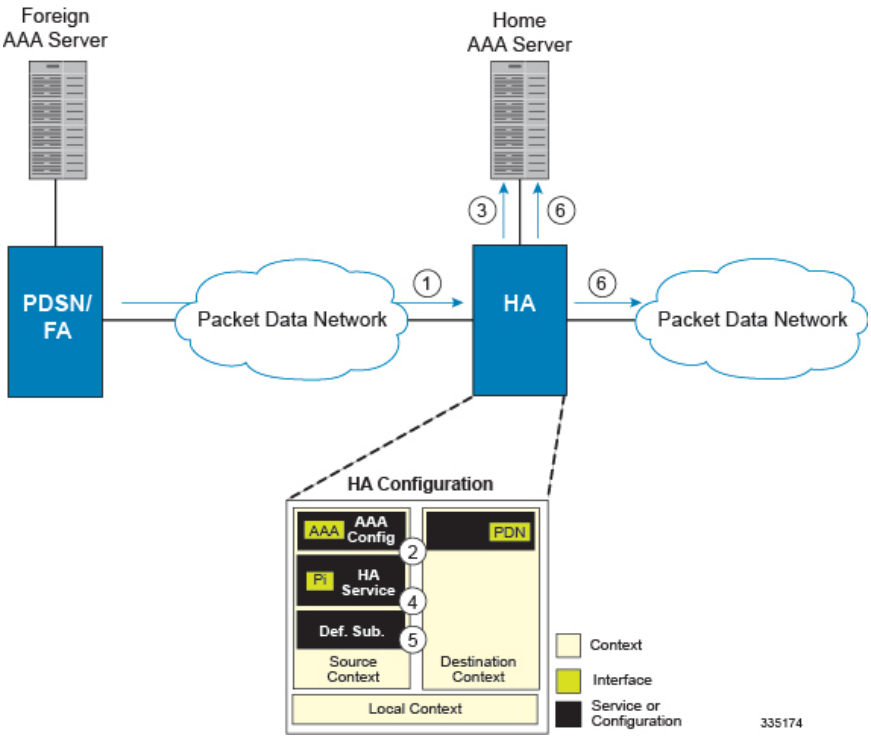
Required Information	Description
Destination context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the destination context will be recognized by the system. **Important** For this configuration, the destination context name should **not** match the 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	
IP address pool name	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. IP address pools are configured in the destination context(s). Multiple address pools can be configured within a single context.
IP pool addresses	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. The pool can be configured as public, private, or static. If this IP pool is being used for Interchassis Session Recovery, it must be a static and srp-activated.

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 a PDSN/FA



1. The system-level AAA settings were configured as follows:
   - Subscriber default domain name = *AAA context*
   - Subscriber username format = *username @*
   - Subscriber last-resort context name = *AAA context*
2. A subscriber session from the PCF is received by the PDSN service over the R-P interface.
3. The PDSN service determines which context to use to provide foreign 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 PDSN service determined that foreign AAA functionality should be provided by the *AAA context*.
4. The system then communicates with the foreign AAA server specified in the AAA context's AAA configuration to authenticate the subscriber.
5. Upon successful authentication, the PDSN service determines the IP address of the subscriber's HA using either an attribute returned in the Access Accept message, or the address specified by the mobile.

   The PDSN service uses the Mobile IP FA context name to determine what destination context is facilitating the FA service. In this example, it determines that it must use the *MIP Destination* context.
6. The PDSN service passes the HA IP address to the FA service.
7. The FA service then establishes a connection to the specified HA over the Pi interface.

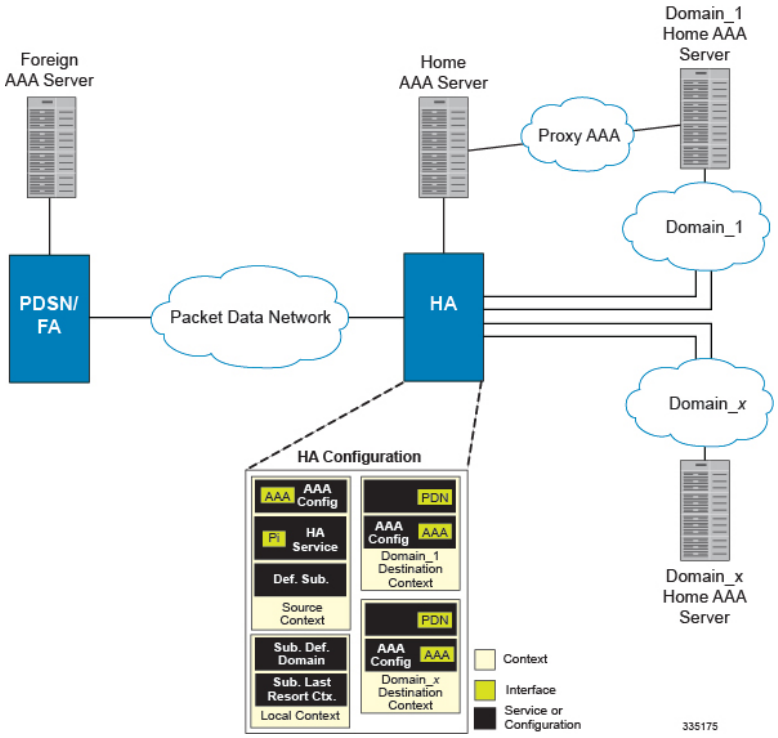
8. Accounting messages for the session are sent to the Foreign AAA server over the AAA interface.
9. If reverse tunneling is disabled, then subscriber data traffic would have been routed over the PDN interface configured in the *Optional Destination* context.

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 by 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 Pi 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 8: Required Information for Source Context Configuration 4

Required Information	Description
Source context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the source context will be recognized by the system.
Pi Interface Configuration	
Piinterface 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. Pi interfaces are configured in the source context.
IP address and subnet	These will be assigned to the Pi interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
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 using multiple ports. Physical ports are configured within the source context and are used to bind logical Pi interfaces.
Gateway IP address	Used when configuring static routes from the Pi interface(s) to a specific network.

Required Information	Description
HA service Configuration	
HA service name	This is an identification string between 1 and 63 characters (alpha and/or numeric) by which the PDSN service will be recognized by the system. Multiple names are needed if using multiple HA services. HA services are configured in the source context.
UDP port number for Mobile IP traffic	Specifies the port used by the HA service and the FA for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 434.
Mobile node re-registration requirements	Specifies how the system should handle authentication for mobile node re-registrations. The HA service can be configured as follows: Always require authentication Never require authentication (NOTE: the initial registration and de-registration will still be handled normally) Never look for mn-aaa extension Not require authentication but will authenticate if mn-aaa extension present

Required Information	Description
FA-to-HA Security Parameter Index Information	**FA IP address:** The HA service allows the creation of a security profile that can be associated with a particular FA. This specifies the IP address of the FA that the HA service will be communicating with. Multiple FA addresses are needed if the HA will be communicating with multiple FAs.
	Index: 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. Multiple SPIs can be configured if the HA service is to communicate with multiple FAs.
	Secret: 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). An SPI secret is required for each SPI configured.
	Hash-algorithm: 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 hmac-md5. A hash-algorithm is required for each SPI configured.

Required Information	Description
Mobile Node Security Parameter Index Information	**Index**: Specifies the shared SPI between the HA service and the mobile node(s). The SPI can be configured to any integer value between 256 and 4294967295. Multiple SPIs can be configured if the HA service is to communicate with multiple mobile nodes.
	Secret(s): Specifies the shared SPI secret between the HA service and the mobile node. The secret can be between 1 and 127 characters (alpha and/or numeric). An SPI secret is required for each SPI configured.
	Hash-algorithm: 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 hmac-md5. A hash-algorithm is required for each SPI configured.
	Replay-protection process: 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. A replay-protection process is required for each mobile node-to-HA SPI configured.
Maximum registration lifetime	Specifies the longest registration lifetime that the HA service will allow in any Registration Request message from the mobile node. 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.
Maximum number of simultaneous bindings	Specifies the maximum number of "care-of" addresses that can simultaneously be bound for the same user as identified by NAI and Home address. The number can be configured to any integer value between 1 and 5. The default is 3.
AAA Interface Configuration	

Required Information	Description
AAA 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. AAA interfaces will be configured in the source context.
IP address and subnet	These will be assigned to the AAA interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
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 source context and are used to bind logical AAA interfaces.
Gateway IP address	Used when configuring static routes from the AAA interface(s) to a specific network.
Home RADIUS Server Configuration	

Required Information	Description
Home RADIUS Authentication server	IP Address: Specifies the IP address of the home RADIUS authentication server the source context will communicate with to provide subscriber authentication functions. Multiple addresses are needed if multiple RADIUS servers will be configured. Home RADIUS authentication servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	Shared Secret: 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. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the home RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.

Required Information	Description
Home RADIUS Accounting server	IP Address: Specifies the IP address of the home RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions. Multiple addresses are needed if multiple RADIUS servers will be configured. Home RADIUS accounting servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	Shared Secret: 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. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: 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.
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 home RADIUS server. The name must be between 1 and 32 alpha and/or numeric characters and is case sensitive.
RADIUS NAS IP address	Specifies the IP address of the source context'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 PDN ports. **Important** 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 9: Required Information for Destination Context Configuration 6

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. **Important** For this configuration, the destination context name should **not** 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.
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	

Required Information	Description
IP address pool name	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. IP address pools are configured in the destination context(s). Multiple address pools can be configured within a single context.
IP pool addresses	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. The pool can be configured as public, private, or static. If this IP pool is being used for Interchassis Session Recovery, it must be a static and srp-activated.
AAA Interface Configuration	
AAA 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. AAA interfaces will be configured in the source context.
IP address and subnet	These will be assigned to the AAA interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
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 source context and are used to bind logical AAA interfaces.

Required Information	Description
Gateway IP address	Used when configuring static routes from the AAA interface(s) to a specific network.
Home RADIUS Server Configuration	
Home RADIUS Authentication server	IP Address: Specifies the IP address of the home RADIUS authentication server the source context will communicate with to provide subscriber authentication functions. Multiple addresses are needed if multiple RADIUS servers will be configured. Home RADIUS authentication servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	Shared Secret: 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. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the home RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.

Required Information	Description
Home RADIUS Accounting server	IP Address: Specifies the IP address of the home RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions. Multiple addresses are needed if multiple RADIUS servers will be configured. Home RADIUS accounting servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	Shared Secret: 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. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: 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.
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 home RADIUS server. The name must be between 1 and 32 alpha and/or numeric characters and is case sensitive.
RADIUS NAS IP address	Specifies the IP address of the source context'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 10: Required Information for System-Level AAA Configuration

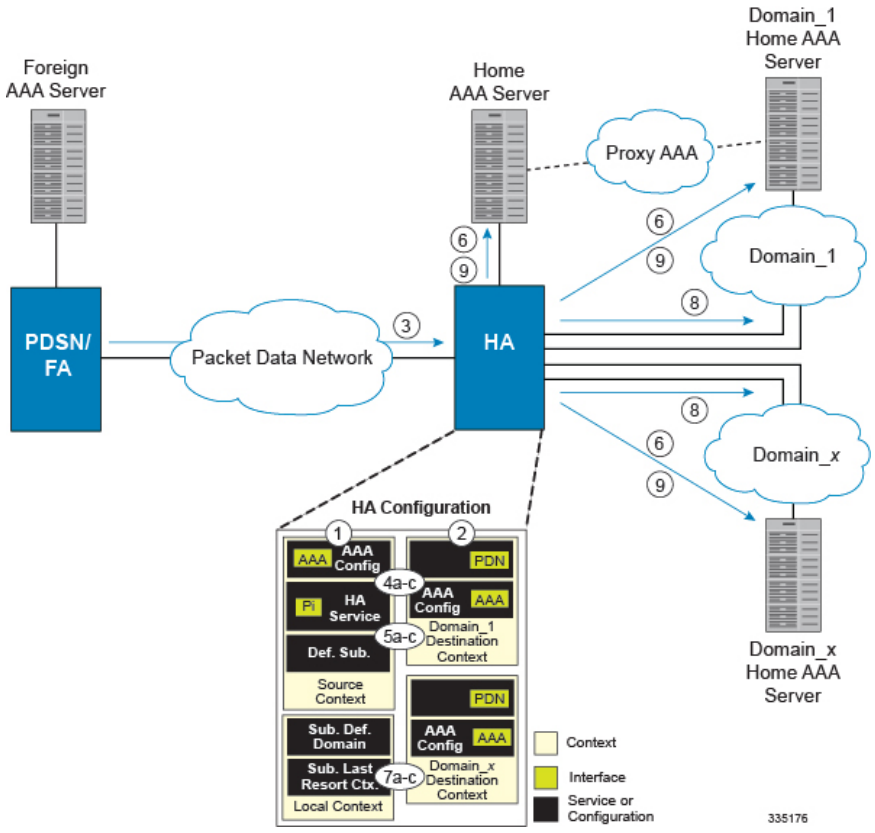
Required Information	Description
Subscriber default domain name	Specifies the name of a context that can provide AAA functions in the event that the domain-part of the username is missing or poorly formed. This parameter will be applied to all subscribers if their domain can not be determined from their username regardless of what domain they are trying to access. **Important** The default domain name can be the same as the source context.
Subscriber Last-resort context	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. 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. **Important** The last-resort context name can be the same as the source context.

Required Information	Description
Subscriber username format	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: • @ • % • - • \ • # • / Up to six username formats can be specified. The default is *username* @. **Important** 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 *user1@enterprise@isp1*, the system resolves to the username *user1@enterprise* with domain *isp1*.

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 6: Call Processing When Using the system as a PDSN/FA



1. The system-level AAA settings were configured as follows:
   - Subscriber default domain name = *AAA context*
   - Subscriber username format = *username @*
   - Subscriber last-resort context name = *AAA context*
2. A subscriber session from the PCF is received by the PDSN service over the R-P interface.
3. The PDSN service determines which context to use to provide foreign 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 PDSN service determined that foreign AAA functionality should be provided by the *AAA context*.
4. The system then communicates with the foreign AAA server specified in the AAA context's AAA configuration to authenticate the subscriber.
5. Upon successful authentication, the PDSN service determines the IP address of the subscriber's HA using either an attribute returned in the Access Accept message, or the address specified by the mobile.

   The PDSN service uses the Mobile IP FA context name to determine what destination context is facilitating the FA service. In this example, it determines that it must use the *MIP Destination* context.
6. The PDSN service passes the HA IP address to the FA service.

7. The FA service then establishes a connection to the specified HA over the Pi interface.
8. Accounting messages for the session are sent to the Foreign AAA server over the AAA interface.