Understanding the Service Operation and Configuration

The system provides wireless carriers with a flexible solution that can support both Simple IP and Mobile IP applications (independently or simultaneously) within a single scalable platform. Simple IP and Mobile IP applications are described in detail in the *System Overview Guide*.

When supporting Simple IP data applications, the system is configured to perform the role of a Packet Data Serving Node (PDSN) within the carrier's 3G CDMA2000 data network. The PDSN terminates the mobile subscriber's Point-to-Point Protocol (PPP) session and then routes data to and from the packet data network (PDN) on behalf of the subscriber. The PDN could consist of Wireless Application Protocol (WAP) servers or it could be the Internet.

When supporting Mobile IP data applications, the system can be configured to perform the role of the PDSN/Foreign Agent (FA) and/or the Home Agent (HA) within the carrier's 3G CDMA2000 data network. When functioning as an HA, the system can either be located within the carrier's 3G network or in an external enterprise or ISP network. Regardless, the PDSN/FA terminates the mobile subscriber's PPP session, and then routes data to and from the appropriate HA on behalf of the subscriber.

Prior to connecting to the command line interface (CLI) and beginning the system's configuration, there are important things to understand about how the system supports these applications. This chapter provides terminology and background information that must be considered before attempting to configure the system.

The following topics are included:

- Terminology, on page 1
- How the System Selects Contexts, on page 9

Terminology

This section defines some of the terms used in this manual.

Contexts

A context is a logical grouping or mapping of configuration parameters that pertain to various physical ports, logical IP interfaces, and services. A context can be thought of as a virtual private network (VPN).

The system supports the configuration of multiple contexts. Each is configured and operates independently from the others. Once a context has been created, administrative users can then configure services, logical IP

interfaces, subscribers, etc.for that context. Administrative users would then bind the logical interfaces to physical ports.

Contexts can also be assigned domain aliases, wherein if a subscriber's domain name matches one of the configured alias names for that context, then that context is used.

Contexts on the system can be categorized as follows:

- Source context: Also referred to as the "ingress" context, this context provides the subscriber's point-of-entry in the system. It is also the context in which services are configured. For example, in a CDMA2000 network, the radio network containing the packet control functions (PCFs) would communicate with the system via R-P interfaces configured within the source context as part of the PDSN service.
- Destination context: Also referred to as the "egress" context, this context is where a subscriber is provided services (such as access to the Internet). Destination contexts are typically named after particular domains. For example, the system's destination context would be configured with the interfaces facilitating subscriber data traffic to/from the Internet, a VPN, or other PDN.
- AAA context: This context provides authorization, authentication, and accounting (AAA) functionality for subscriber and/or administrative user sessions. The AAA context contains context-specific AAA policies, the logical interfaces for communicating with AAA servers, and records for locally configured subscribers and/or administrative users.

Important It is important to note that "source," "destination," and AAA functionality can optionally be configured within the same context or be configured as separate contexts. As a general rule, however, if the carrier owns and operates the AAA server, it is recommended that AAA functionality be configured within the source context. Conversely, if a home network other than the carrier's own operates the AAA server, it is recommended that AAA functionality be configured within the destination context.

To ensure scalability, AAA functionality for subscriber sessions should not be configured in the local out-of-band context.

AAA Realms

A AAA realm is the location within the AAA context where subscriber-specific templates can be defined that are applied to subscribers who match that realm. A AAA realm is considered part of the AAA context; and the AAA context itself is also considered to be a realm. There may be many different AAA realms defined within a single AAA context.

An example of a realm would be that within a source context named ingress, there could be a domain alias of nova.com, another domain alias of bigco.com, and a single AAA configuration that is used by the entire system. In this example, the source context is also serving as a AAA context. There would be three specific AAA realms in this case; ingress, nova.com, and bigco.com, since all three could have their own subscriber templates defined.

The primary purpose of a AAA realm is to host a subscriber template for each realm that provides AAA attributes that may be used in the event that an authenticated subscriber's access-accept message from RADIUS fails to contain certain attributes. In this case, the default attributes contained in the realm-based subscriber template would be used. However, if the RADIUS authentication message contains an attribute from that subscriber's RADIUS user profile, then that information will be used to overwrite any default attribute parameters that are contained in the subscriber template.

More information about subscriber templates will be provided later in this chapter when subscribers are discussed.

Realms must be globally unique in their naming convention in that each realm name can only be used in one context in one system.

Ports

Ports are the physical interfaces that reside upon the system's line cards (Ethernet 10/100, Gigabit Ethernet 1000 Line Cards and the four-port Quad Gigabit Ethernet Line Card otherwise known as the Quad Gig-E or QGLC). Ethernet Port configuration addresses traffic profiles, data encapsulation methods, media type, and other information needed to allow physical connectivity between the system and the rest of the network. Ports are identified by the chassis slot number in which the line card resides, followed by the number of the physical connector on the line card. For example, Port 24/1 identifies connector number 1 on the card in slot 24.

Ports are associated with contexts through bindings. Additional information on bindings can be found in the Bindings section. Each physical port can be configured to support multiple logical IP interfaces each with up to 17 IP addresses (one primary and up to 16 secondaries).

Logical Interfaces

Prior to allowing the flow of user data, the port must be associated with a virtual circuit or tunnel called a logical interface. A logical interface within the system is defined as the logical assignment of a virtual router instance that provides higher-layer protocol transport, such as Layer 3 IP addressing. Interfaces are configured as part of the VPN context and are independent from the physical port that will be used to bridge the virtual interfaces to the network.

Logical interfaces are assigned to IP addresses and are bound to a specific port during the configuration process. Logical interfaces are also associated with services through bindings. Services are bound to an IP address that is configured for a particular logical interface. When associated, the interface takes on the characteristics of the functions enabled by the service. For example, if an interface is bound to a PDSN service, it will function as an R-P interface between the PDSN service and the PCF. Services are defined later in this section.

There are several types of logical interfaces that must be configured to support Simple and Mobile IP data applications as described below:

- Management interface: This interface provides the system's point of attachment to the management network. The interface supports remote access to the system CLI, Common Object Request Broker Architecture (CORBA)-based management via the Web Element Manager application, and event notification via the Simple Network Management Protocol (SNMP).

  The system defaults to a Local context which should not be deleted. Management interfaces are defined in the Local management context and should only be bound to the ports on the Switch Processor Input/Output (SPIO) cards port on the Virtual Management Card.

- R-P interface: Also referred to as the A10/A11 interface, this interface is the communications path between the Radio Node (also referred to as a PCF) and the PDSN.

  The A10/A11 interface carries traffic signaling (A11) and user data traffic (A10). The A10/A11 interface is implemented in accordance with IS-835.

  R-P interfaces are bound to ports on either the Ethernet 10/100 or Ethernet 1000/QGLC Line Cards.

- Pi interface: The packet interface (Pi) is the communications path between the PDSN/Foreign Agent (PDSN/FA) and the Home Agent (HA) for Mobile IP applications.

  Pi interfaces are bound to ports on either the Ethernet 10/100 or Ethernet 1000/QGLC Line Cards.

- PDN interface: The interface to the packet data network (PDN). For Simple IP applications, this is the communications path between the PDSN and the PDN. For Mobile IP applications, this is the communications path between the HA and the PDN.

  PDN interfaces are bound to Ethernet ports.

- AAA interface: The AAA interface is the connection between the PDSN and/or HA and the network servers that perform AAA functions. With this release of the system, the Remote Authentication Dial-In User Service (RADIUS) Protocol is used for communication on this interface.

  AAA interfaces are bound to Ethernet ports. However, AAA interfaces can also be bound to the Local management context and to virtual management ports on the SPIO to provide AAA functions for subscribers, and for context-level administrative users.

- ICC interface: Inter-context communication (ICC) interfaces are only required when multiple services are configured in the same context. As mentioned previously, services are bound to interfaces. Creating an ICC interface provides a communication path between the services. For example, if an FA and HA service were configured in the same context, the FA service would need to be bound to an address assigned to the ICC interface and the HA service would need to be bound to a secondary address on the same ICC interface to provide a communications path between the two services.

  The ICC interface must be configured with multiple addresses (one per service that it is facilitating) and bound to a physical port.

Bindings

A binding is an association between "elements" within the system. There are two types of bindings: static and dynamic.

Static binding is accomplished through the configuration of the system. Static bindings are used to associate:

- A specific logical interface (configured within a particular context) to a physical port. Once the interface is bound to the physical port, traffic can flow through the context just as if it were any physically defined circuit. Static bindings support any encapsulation method over any interface and port type.
- A service to an IP address assigned to a logical interface within the same context. This allows the interface to take on the characteristics (i.e., support the protocols) required by the service. For example, a PDSN service bound to a logical interface will cause the logical interface to take on the characteristics of an R-P interface within a 3G CDMA2000 network.

Dynamic binding associates a subscriber to a specific egress context based on the configuration of their profile or system parameters. This provides a higher degree of deployment flexibility as it allows a wireless carrier to support multiple services and facilitates seamless connections to multiple networks.

Services

Services are configured within a context and enable certain functionality. The following services can be configured on the system:

- PDSN services: Required for both Simple IP and Mobile IP applications, PDSN services define PDSN functionality for the system. The PDSN service must be bound to a logical interface within the same context. Once bound, the interface takes on the characteristics of an R-P interface. Multiple services can be bound to the same logical interface. Therefore, a single physical port can facilitate multiple R-P interfaces.

  The system treats the connection between the PCF and the PDSN service as a VPN (referred to as an RP-VPN). Individual R-P sessions are identified on this RP-VPN using the PCF address, the PDSN interface address, and the R-P Session ID.

- FA services: Currently supported only for use in CDMA 2000 networks, FA services are configured to support Mobile IP and define FA functionality on the system.

  The system supports multiple Mobile IP configurations. A single system can perform the function of a FA only, an HA only, or a combined PDSN/FA/HA. Depending on your configuration, the FA service can create and maintain the Pi interface between the PDSN/FA and the HA or it can communicate with an HA service configured within the same context.

  The FA service should be configured in a different context from the PDSN service. However, if the FA service will be communicating with an HA that is a separate network element, it must be configured within the same context as and be bound to the Pi interfaces that allow it to communicate with the HA.

- HA services: Currently supported only for use in CDMA 2000 networks, HA services are configured to support Mobile IP and define HA functionality on the system. Depending on your configuration, the HA service can be used to terminate the Pi interface from the FA or it can communicate with an FA service configured in the same context.

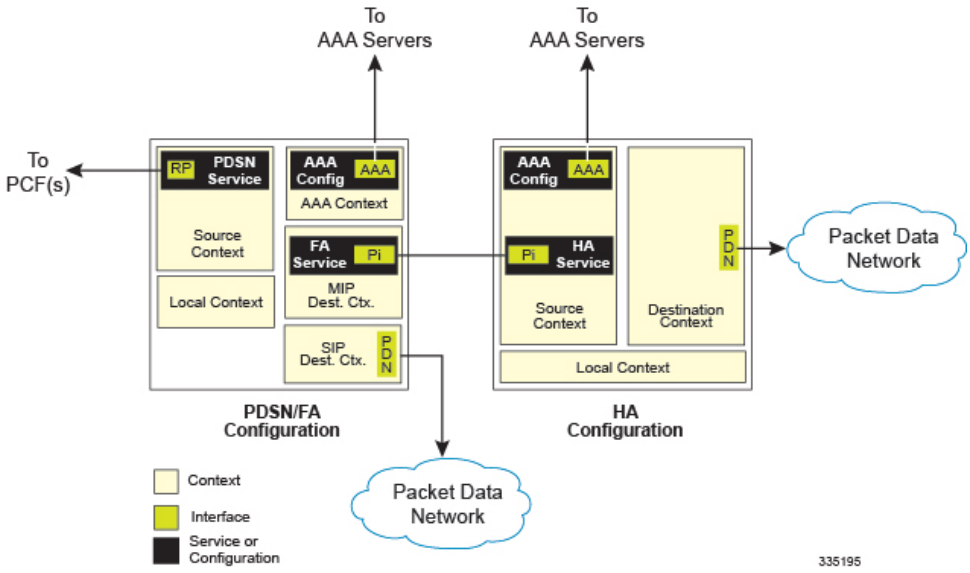
  If the HA service is configured within the same system as the PDSN/FA, then it should be configured within the same context as the FA service. This context, then, would also facilitate the PDSN interfaces to the data network.

  If the HA service is configured in a separate system, it should be configured in the same context as and bound to the Pi interfaces that allow it to communicate with the FA.

- LAC services: LAC services are configured on the system to provide Layer 2 Tunneling Protocol (L2TP) access concentrator (LAC) functionality. LAC services can be configured and used within either CDMA 2000 or GPRS/UMTS networks to provide secure tunneling to an L2TP network server (LNS) on a remote PDN.

The following figure diagrams the relationship between services, interfaces, and contexts within the system for CDMA 2000 networks.

Figure 1: Service, Interface, and Context Relationship Within the System for CDMA 2000 Networks



AAA Servers

For most configurations, AAA servers will be used to store profiles, perform authentication, and maintain accounting records for each mobile data subscriber. The AAA servers communicate with the system over the AAA interface. The system supports the configuration of up to 128 AAA servers with which to communicate.

It is important to note that for Mobile IP, there can be foreign AAA (FAAA) and home AAA (HAAA) servers. The FAAA server(s) typically resides in the carrier's network. The HAAA server(s) could be owned and controlled by either the carrier or the home network. If the HAAA server is owned and controlled by the home network, accounting data can be transferred to the carrier via a AAA proxy server.

For most configurations, AAA servers will be used to store subscriber profiles and perform authentication. In addition, RADIUS AAA servers may be used to maintain accounting records for each mobile data subscriber as opposed to a GTPP-based Charging Gateway Function (CGF). The AAA servers communicate with the system over the AAA interface. The system supports the configuration of up to 128 AAA servers with which to communicate.

Subscribers

Subscribers are the end-users of the service who gain access to the Internet, their home network, or a public network through the system. There are three primary types of subscribers/users:

- RADIUS-based Subscribers: The most common type of subscriber, these users are identified by their International Mobile Subscriber Identity (IMSI) number, an Electronic Serial Number (ESN), or by their domain name or user name and are configured on and authenticated by a RADIUS AAA server.

  Upon successful authentication various attributes (contained in the subscriber profile) are returned that dictate such things as session parameter settings (e.g. protocol settings, IP address assignment method, etc.), and what privileges the subscriber has (e.g. Simple IP, Mobile IP, etc.).

  Attribute settings received by the system from a RADIUS AAA server take precedence over local-subscriber attributes and parameters configured on the system.

- Local Subscribers: These are subscribers, primarily used for testing purposes, that are configured and authenticated within a specific context. Unlike RADIUS-based subscribers, the local subscriber's user profile (containing attributes like those used by RADIUS-based subscribers) is configured within the context where they are created.

  When local subscriber profiles are first created, attributes for that subscriber are set to the system's default settings. The same default settings are applied to all subscriber profiles including the subscriber named default (created automatically by the system for each system context; refer to the Default Subscribers and Realm-based Subscriber Templates section for more information). When configuring local profile attributes, the changes are made on a subscriber-by-subscriber basis.

  Attributes configured for local subscribers take precedence over context-level parameters. However, they could be over-ridden by attributes returned from a RADIUS AAA server.

- Management Subscribers: A management user is an authorized user who can monitor, control, and configure the system through its command line interface (CLI) or Web Element Manager application. This management can be performed either locally, through the system's console port, or remotely through the use of the Telnet or secure shell (SSH) protocols. Management users are typically configured as a local subscriber within the localout-of-band management context, which is used exclusively for system management and administration. Like a local subscriber, the management subscriber's user profile is configured within the context where they are created (in this case the localout-of-band management context). However, management subscribers may also be authenticated remotely via RADIUS, if a AAA configuration exists within the localout-of-band management context.

Default Subscribers and Realm-based Subscriber Templates

Used for RADIUS-based subscribers, default subscribers – created on a per context basis, and subscriber templates – optionally created on per realm basis, contain default AAA attributes that can be used by subscribers who are remotely authenticated within a specific context or domain alias (AAA realm) when needed.

Default Subscriber

When each context is created, the system automatically creates a subscriber named default. There is only one default subscriber per context. The profile for the subscriber named default provides a configuration template of attribute values for subscribers who are remotely authenticated in that context. Any subscriber information that is not included in a RADIUS-based subscriber's user profile is configured according to the defaults defined for the default subscriber.

No matter where created all default subscribers initially have the same attributes set. The attributes for the default subscriber in each context and be changed from the CLI on a context by context basis.

Important Local subscribers, who are authenticated locally within the context where they were created, cannot use any attributes that are defined for subscriber default. Rather, each local subscriber must have any attributes configured for them individually.

Realm-based Subscriber Templates

As defined earlier, a context can have numerous domain aliases that allows a single context to serve numerous different subscribers who have different domain names. When assigned, these domain aliases become AAA realms within the context.

Since each realm is used for a specific group of subscribers (e.g. corporate subscribers who may only have access to a specific corporate network that is protected by a virtual private network), each realm must have the ability to define what AAA attributes should be applied to these different subscriber groups. This is achieved through the use of realm-based subscriber templates.

A subscriber template contains defined attributes that are specific to a select subscriber who belongs to that realm. Like the default subscriber (subscriber named default) who has a context-level set of configuration attributes, the subscriber template is used to provide default attribute values that may be used should a RADIUS user profile for a subscriber belonging to the specific realm fail to contain a needed attribute.

Important If a realm-based subscriber template is not created for a specified realm, then the system will use the attributes configured for default subscriber (named default) within the context where the AAA realm exists.

Below is an example of how realm-based subscriber templates may be used.

As depicted above, a context named "ingress" contains:

- a PDSN service named "PDSN".
- a AAA configuration that is used to communicate with an external RADIUS server. A default subscriber for the context named "default". This default subscriber has an idle timeout attribute value of 45000 seconds.
- three additional realms, based on the following domain alias names:
  - "mega.com", which has a realm-based subscriber template named "megauser". This template contains an idle timeout attribute value of 36000 seconds.
  - "bigco.com", which has a realm-based subscriber template named "bigco". This template contains an idle timeout attribute value of 3600 seconds.
  - "smallco.com", which has no realm-based subscriber template defined.

For this example, we will assume that all subscribers enter the system through the PDSN service defined in the [ingress] context. Configuration procedures and context selection methods will be provided in other sections in this document.

If a subscriber enters the system with a domain name that matches the context name "ingress" (example: user1@ingress), then the [ingress] context would be used for authentication. If the RADIUS server authenticates the subscriber and returns no value for the idle-timeout attribute, then this subscriber would be assigned the value contained in the subscriber default configuration. If a subscriber named user@mega.com enters the system with a domain name that matches a configured domain alias within the [ingress] context, in this case "mega.com", then the [ingress] context would be used for authentication. However, since a realm-based subscriber template named "megauser" is defined within this AAA realm, then should the RADIUS server return no value for the idle-timeout attribute, then this subscriber would be assigned the value contained in the "megauser" subscriber template.

If a subscriber named user@bigco.com enters the system with a domain name that matches a configured domain alias within the [ingress] context, in this case "bigco.com", then the [ingress] context would be used for authentication. However, since a realm-based subscriber template name "bigco" is defined within this AAA realm, any attributes not returned could be assigned from this subscriber template. In this example, the RADIUS server returns an idle-timeout of 18000 seconds. Because the RADIUS user profile contained a value for this attribute, the system would use that value (18000) rather than the value defined in the subscriber template.

If a subscriber name user@smallco.org enters the system with a domain name that matches a configured domain alias within the [ingress] context, in this case "smallco.org", then the [ingress] context would be used for authentication. Note that the "smallco.org" domain alias does not have a realm-based subscriber template defined. In this case, the system would obtain any attribute values not returned from the RADIUS server from the subscriber default configuration. So if no attribute value was returned from RADIUS, user@smallco.org would be assigned an idle-timeout value of 45000 seconds.

How the System Selects Contexts

The previous section of this chapter defined what a context is and how it is used within the system. This section provides details about the process that is used to determine which context to use for context-level administrative user and/or subscriber sessions. Understanding this process allows you to better plan your configuration in terms of how many contexts and interfaces need to be configured.

Context Selection for Context-level Administrative User Sessions

The system comes configured with a context called local management context that should be used specifically for management purposes. The context selection process for context-level administrative users (those configured within a context) is simplified because the management interface(s) on the SPIO are only associated with the localout-of-band management context. Therefore, the source and destination contexts for a context-level administrative user responsible for managing the entire system should always be the local management context.

Although this is not commonly done, a context-level administrative user can also connect through other interfaces on the system and still have full system management privileges.A context-level administrative user can be created in a non-local management context. These management accounts only have privileges in the context where they are created. This type of management account can connect directly to a port in the context in which they belong, if local connectivity is enabled (SSHD for example) in that context.For all FTP or SFTP connections, you must connect through a SPIO interface. If you SFTP or FTP as a non-local management context account you must use the username syntax of usernamecontextname.

The context selection process becomes more involved depending on whether or not you will be configuring the system to provide local authentication or work with a AAA server to authenticate the context-level administrative user.

The system provides the flexibility to configure context-level administrative users locally (meaning that their profile will be configured and stored in its own memory) or remotely on an AAA server. If the user is configured locally, when he/she attempts to log onto the system, the system performs the authentication. If the user profile is configured on a AAA server, the system must determine how to contact the AAA server in order to perform authentication. It does this by determining the AAA context for the session.

The following table and figure describe the process that the system uses to select an AAA context for a context-level administrative user.

Table 1: Context-level Administrative User AAA Context Selection

Item	Description
1	During authentication, the system determines if local authentication is enabled in the local management context. If it is, the system attempts to authenticate the administrative user in the localout-of-band management context. If it is not, proceed to item 2 in this table. If the administrative user's username is configured, authentication is performed using the AAA configuration within the local management context. If not, proceed to item 2 in this table.
2	If local authentication is disabled on the system or if the administrative user's username is not configured in the local management context, then the system determines if a domain was received as part of the username. If there is a domain and it matches the name of a configured context or domain, then the AAA configuration within that context is used. If there is a domain and it does not match the name of a configured context or domain, go to item 4 in this table. If there is no domain as part of the username, go to item 3 in this table.
3	If there was no domain specified in the username or the domain is not recognized, the system determines if an AAA Administrator Default Domain is configured. If the default domain is configured and it matches a configured context, then the AAA configuration within the AAA Administrator Default Domain context is used. If the default domain is not configured or does not match a configured context or domain, go to item 4 item this table

Item	Description
4	If a domain was specified as part of the username but it did not match a configured context, or if a domain was not specified as part of the username, the system determines if the AAA Administrator Last Resort context parameter is configured. If a last resort context is configured and it matches a configured context, then the AAA configuration within that context is used. If a last resort context is not configured or does not match a configured context or domain, then the AAA configuration within the local management context is used.

Context Selection for Subscriber Sessions

The context selection process for a subscriber session is more involved than that for the administrative users.

The source context used to service a subscriber session is mostly dependant on the mapping of PCFs to PDSNs. Depending on this mapping and the subscribers' location in the network, the same subscriber may initiate several different data sessions throughout the day and have their session serviced by several different source contexts.

The AAA and destination context selection is determined based on what services are provided to the subscriber. For example, a carrier may only offer wireless Internet access and therefore be responsible for performing AAA functions for a subscriber session and for providing the network interfaces to the Internet. In this example, the carrier may choose to combine the source and AAA contexts into one and provide a separate destination context. Another carrier may choose to provide both wireless Internet access and VPN service to a corporate or Internet Service Provider (ISP) network. The system is flexible enough to simultaneously support these services because of the unique way in which it determines how to provide AAA functionality and route the session to the appropriate destination.

The following two sections provide details on the system's process in determining the correct AAA and destination contexts for a subscriber session.

AAA Context Selection for Subscriber Sessions

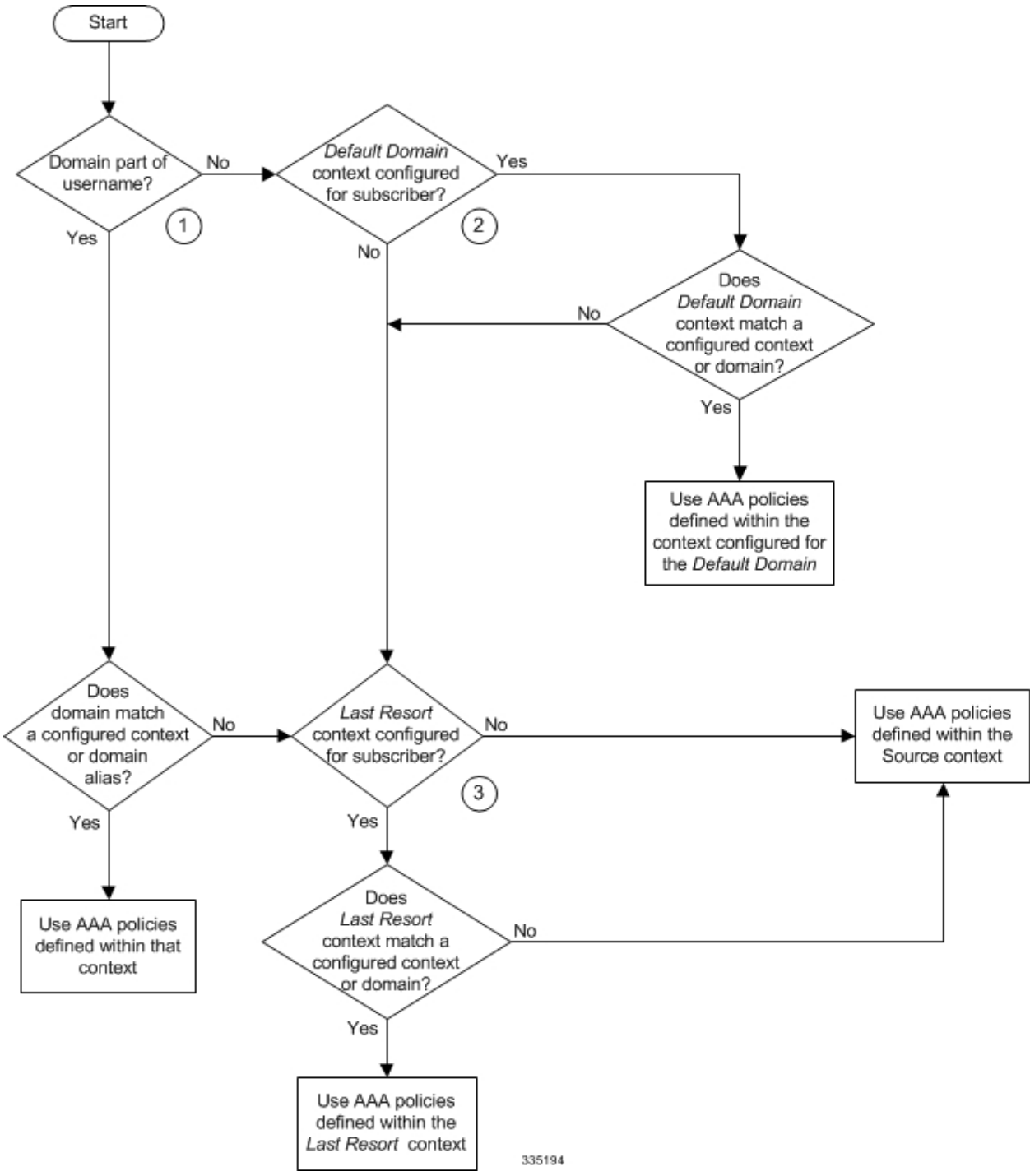
The following table and figure describe the process that the system uses to select an AAA context for a subscriber.

Table 2: Subscriber AAA Context Selection

Item	Description
1	During authentication, the system determines if a domain was received as part of the username. If there is a domain and it matches the name of a configured context or domain alias, then the AAA configuration within that context is used.

Item	Description
2	If there was no domain specified in the username, the system determines if an AAA Subscriber Default Domain was configured. The AAA Subscriber Default Domain parameter is a system-wide AAA parameter that provides the system with the name of a context or domain that can provide AAA functions. If the AAA Subscriber Default Domain is configured and it matches a configured context or domain, then the AAA configuration within the AAA Subscriber Default Domain context is used. If the AAA Subscriber Default Domain is not configured or does not match a configured context or domain, then the system determines if an AAA Subscriber Last Resort is configured.

Figure 2: Subscriber AAA Context Selection



Destination Context Selection For Subscriber Sessions

This section provides information on how a destination context is selected for subscribers whose profiles are configured on a RADIUS AAA server and for those whose profiles are locally configured. Note that the destination context for context-level administrative users is always the local management context.

The following table describes the process that the system uses to select a destination context for a RADIUS-based subscriber whose profile is configured on a RADIUS AAA server and for a subscriber whose profile is configured within a specific context.

Table 3: Subscriber Destination Context Selection

Item	Description
1	The system supports a RADIUS attribute called SN1-VPN-name (or SN-VPN-name in some dictionaries). This attribute specifies the name of the subscriber's destination context. If configured in the subscriber's RADIUS user profile, it will be returned as part of the Access Accept message.If the SN1-VPN-Name attribute is returned, and it matches a configured context, then that context is used as the destination context. If the SN1-VPN-Name attribute is returned, and it does not match a configured context, the call is rejected. If the SN1-VPN-Name attribute is not returned with a value, go to item 2 in this table.
2	The system attempts to use the ip context name parameter configuration for the realm-based subscriber template or context-level default subscriber configured within the AAA context.If a realm-based subscriber template does not exist, go to item 3 in this table.If a realm-based subscriber template exists, the system checks to see if ip context-name is configured in the template. If ip context-name is not configured in the template, the AAA context is used for the destination context. If ip context-name is configured in the template, a check is made to see if it matches the name of a configured context. If ip context-name is configured in the template, but does not match the name of a configured context, the call is rejected. If ip context-name is configured in the template, and matches the name of a configured context, the destination context is set to the ip name-context f or the default subscriber.

Item	Description
3	The local default subscriber profile contains an attribute called ip context-name. This attribute specifies the destination context to use for a local subscriber. If ip context-name is not configured, the AAA context is used for the destination context.If ip context-name is configured, a check is made to see if it matches the name of a configured context. If ip context-name is configured, but does not match the name of a configured context, the AAA context is used for the destination context. If ip context-name is configured, and matches the name of a configured context, the destination context is set to the ip name-context for the default subscriber.

Figure 3: Subscriber Destination Context Selection