L2TP Access Concentrator

This chapter describes the Layer 2 Tunneling Protocol (L2TP) Access Concentrator (LAC) functionality support on Cisco® ASR 5500 chassis and explains how it is configured.

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

Important The L2TP Access Concentrator is a licensed Cisco feature. A separate feature license may be required. Contact your Cisco account representative for detailed information on specific licensing requirements. For information on installing and verifying licenses, refer to the *Managing License Keys* section of the *Software Management Operations* chapter in the *System Administration Guide*.

When enabled though the session license and feature use key, the system supports L2TP for encapsulation of data packets between it and one or more L2TP Network Server (LNS) nodes. In the system, this optional packet encapsulation, or tunneling, is performed by configuring L2TP Access Concentrator (LAC) services within contexts.

Important While establishing the L2TP session from LAC to LNS, the PPP connection for the user is established. The server uses CHAP authentication protocol to authenticate the connection. While calculating the CHAP response for the CHAP challenge received by the server, the server does not consider the CHAP password.

Important The LAC service uses UDP ports 13660 through 13668 as the source port for sending packets to the LNS.

This chapter contains the following topics:

Applicable Products and Relevant Sections

The LAC feature is supported for various products. The following table indicates the products on which the feature is supported and the relevant sections within the chapter that pertain to that product.

Applicable Product(s)	Refer to Sections

PDSN/FA/HA	• *Supported LAC Service Configurations for PDSN Simple IP*
	• *Supported LAC Service Configuration for Mobile IP*
	• *Configuring Subscriber Profiles for L2TP Support*
	  • *RADIUS and Subscriber Profile Attributes Used*
	  • *Configuring Local Subscriber Profiles for L2TP Support*
	  • *Tunneling All Subscribers in a Specific Context Without Using RADIUS Attributes*
	• *Configuring LAC Services*
	• *Modifying PDSN Services for L2TP Support*

GGSN/SGSN/FA/P-GW	• *Supported LAC Service Configurations for the GGSN*
	• *Supported LAC Service Configuration for Mobile IP*
	• *Configuring Subscriber Profiles for L2TP Support*
	  • *RADIUS and Subscriber Profile Attributes Used*
	  • *Configuring Local Subscriber Profiles for L2TP Support*
	• *Enabling Multicast Services over L2TP*
	• *Configuring LAC Services*
	• *Modifying APN Templates to Support L2TP*

Applicable Product(s)	Refer to Sections

ASN GW	• *Supported LAC Service Configuration for Mobile IP*
	• *Configuring Subscriber Profiles for L2TP Support*
	  • *RADIUS and Subscriber Profile Attributes Used*
	  • *Configuring Local Subscriber Profiles for L2TP Support*
	  • *Tunneling All Subscribers in a Specific Context Without Using RADIUS Attributes*
	• *Configuring LAC Services*

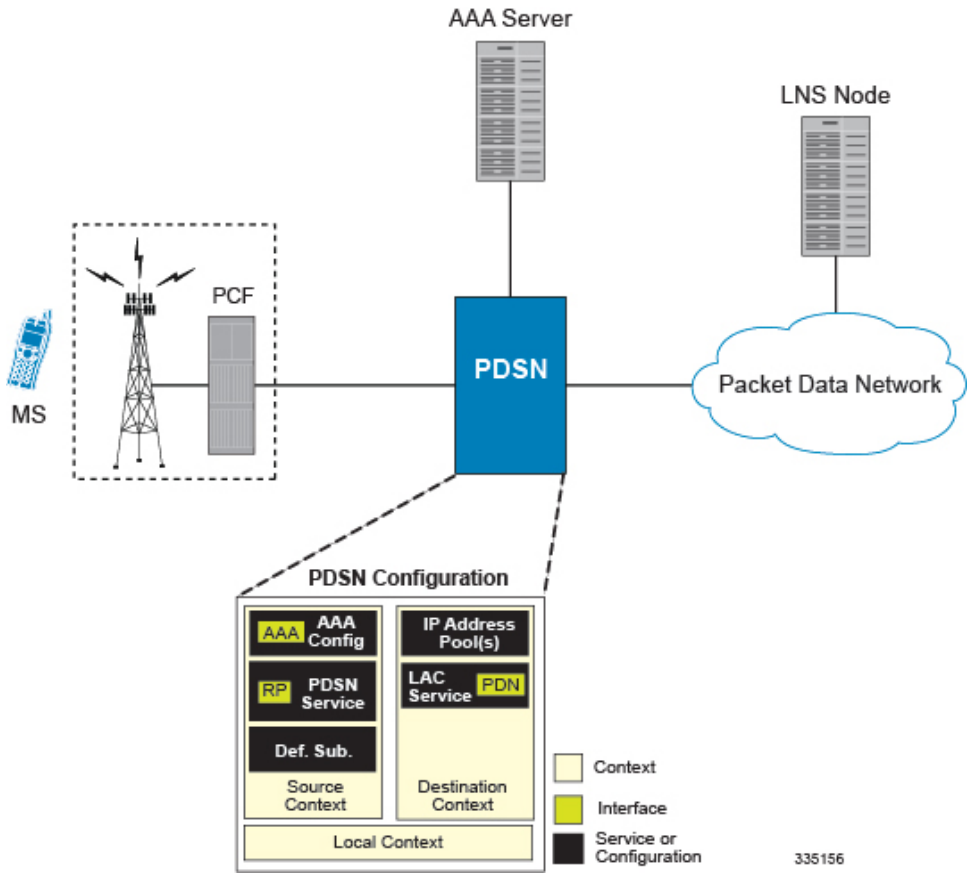
Supported LAC Service Configurations for PDSN Simple IP

LAC services can be applied to incoming PPP sessions using one of the following methods:

- **Attribute-based tunneling:** This method is used to encapsulate PPP packets for only specific users, identified during authentication. In this method, the LAC service parameters and allowed LNS nodes that may be communicated with are controlled by the user profile for the particular subscriber. The user profile can be configured locally on the system or remotely on a RADIUS server.
- **PDSN Service-based compulsory tunneling:** This method of tunneling is used to encapsulate all incoming PPP traffic from the R-P interface coming into a PDSN service, and tunnel it to an LNS peer for authentication. It should be noted that this method does not consider subscriber configurations, since all authentication is performed by the peer LNS.

Each LAC service is bound to a single system interface configured within the same system context. It is recommended that this context be a destination context as displayed in the following figure.

Figure 1: LAC Service Configuration for SIP



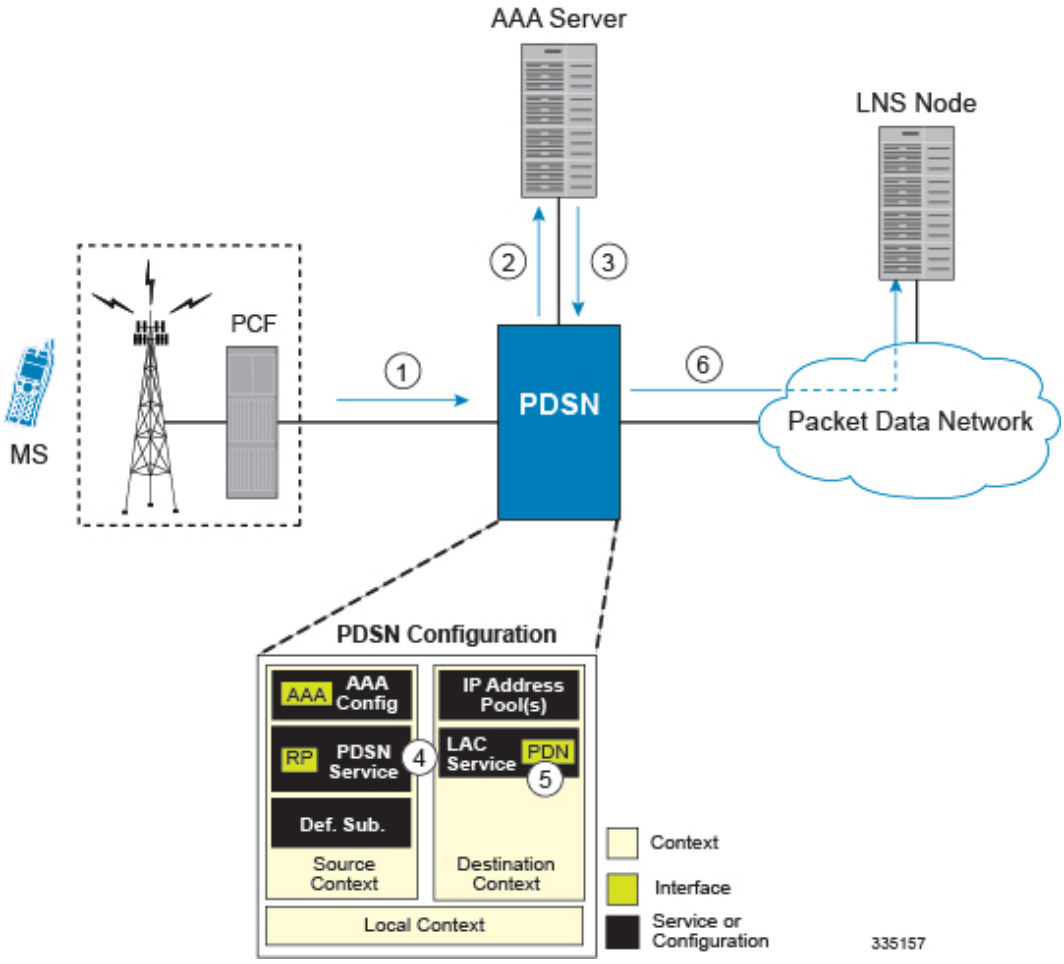
Attribute-based Tunneling

This section describes the working of attribute-based tunneling and its configuration.

How The Attribute-based L2TP Configuration Works

The following figure and the text that follows describe how Attribute-based tunneling is performed using the system.

Figure 2: Attribute-based L2TP Session Processing for SIP



1. A subscriber session from the PCF is received by the PDSN service over the R-P interface.
2. The PDSN service attempts to authenticate the subscriber. The subscriber could be configured either locally or remotely on a RADIUS server. Figure above shows subscriber authentication using a RADIUS AAA server.
3. The RADIUS server returns an Access-Accept message, which includes attributes indicating that session data is to be tunneled using L2TP, and the name and location of the LAC service to use. An attribute could also be provided indicating the LNS peer to connect to.
4. The PDSN service receives the information and then forwards the packets to the LAC service, configured within the Destination context.
5. The LAC service, upon receiving the packets, encapsulates the information and forwards it to the appropriate PDN interface for delivery to the LNS.
6. The encapsulated packets are sent to the peer LNS through the packet data network where they will be un-encapsulated.

Configuring Attribute-based L2TP Support for PDSN Simple IP

This section provides a list of the steps required to configure attribute-based L2TP support for use with PDSN Simple IP applications. Each step listed refers to a different section containing the specific instructions for completing the required procedure.

Important These instructions assume that the system was previously configured to support subscriber data sessions as a PDSN.

Step 1 Configure the subscriber profiles according to the information and instructions located in the *Configuring Subscriber Profiles for L2TP Support* section of this chapter.

Step 2 Configure one or more LAC services according to the information and instructions located in the *Configuring LAC Services* section of this chapter.

Step 3 Configure the PDSN service(s) with the tunnel context location according to the instructions located in the *Modifying PDSN Services for L2TP Support* section of this chapter.

Step 4 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

PDSN Service-based Compulsory Tunneling

This section describes the working of service-based compulsory tunneling and its configuration.

How PDSN Service-based Compulsory Tunneling Works

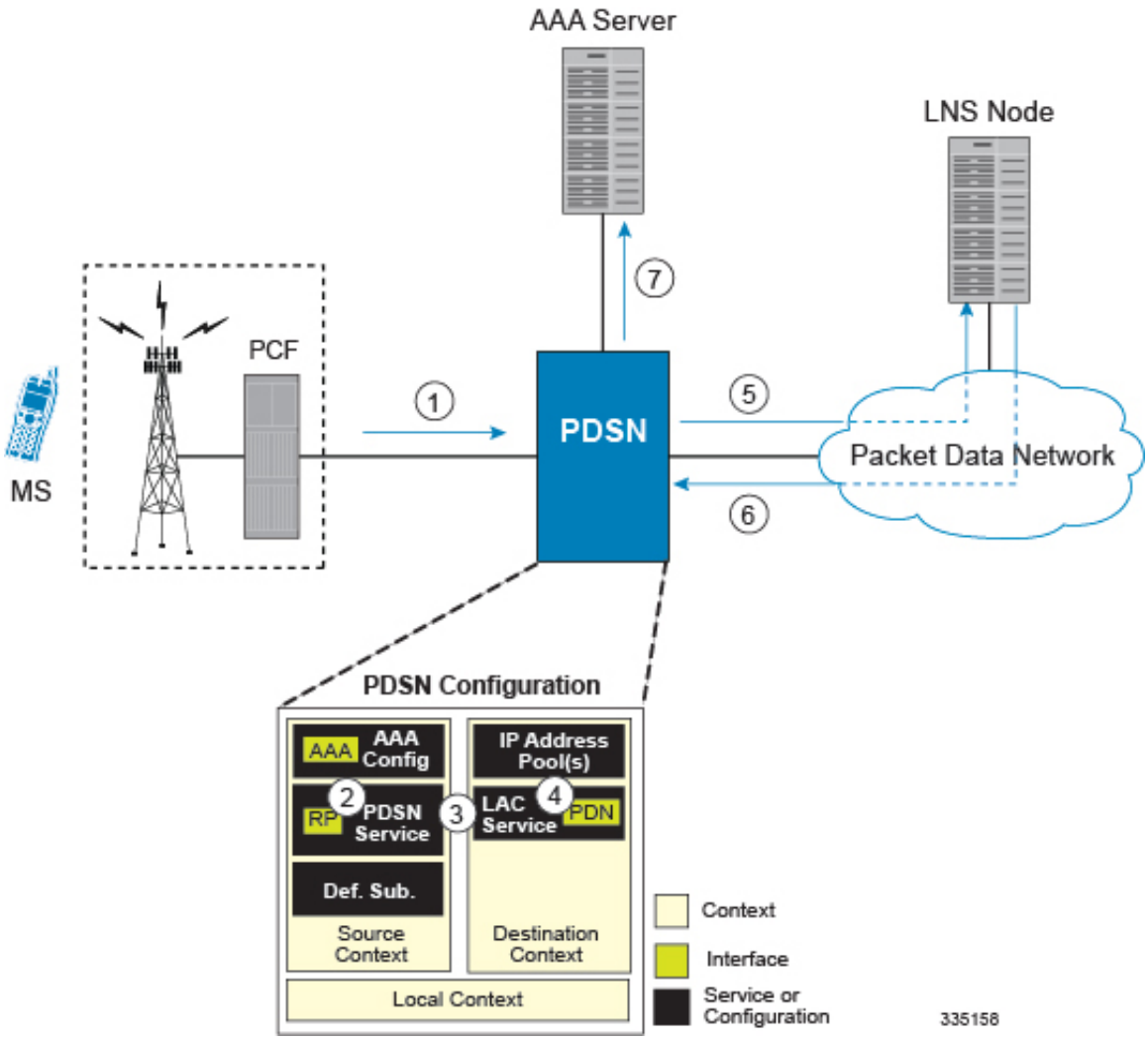
PDSN Service-based compulsory tunneling enables wireless operators to send all PPP traffic to remote LNS peers over an L2TP tunnel for authentication. This means that no PPP authentication is performed by the system.

Accounting start and interim accounting records are still sent to the local RADIUS server configured in the system's AAA Service configuration. When the L2TP session setup is complete, the system starts its call counters and signals the RADIUS server to begin accounting. The subscriber name for accounting records is based on the NAI-constructed name created for each session.

PDSN service-based compulsory tunneling requires the modification of one or more PDSN services and the configuration of one or more LAC services.

The following figure and the text that follows describe how PDSN service-based compulsory tunneling is performed using the system.

Figure 3: PDSN Service-based Compulsory Tunneling Session Processing



1. A subscriber session from the PCF is received by the PDSN service over the R-P interface.
2. The PDSN service detects its **tunnel-type** parameter is configured to L2TP and its **tunnel-context** parameter is configured to the Destination context.
3. The PDSN forwards all packets for the session to a LAC service configured in the Destination context. If multiple LAC services are configured, session traffic will be routed to each using a round-robin algorithm.
4. The LAC service initiates an L2TP tunnel to one of the LNS peers listed as part of its configuration.
5. Session packets are passed to the LNS over a packet data network for authentication.
6. The LNS authenticates the session and returns an Access-Accept to the PDSN.
7. The PDSN service initiates accounting for the session using a constructed NAI.

   Session data traffic is passed over the L2TP tunnel established in step 4.

Configuring L2TP Compulsory Tunneling Support for PDSN Simple IP

This section provides a list of the steps required to configure L2TP compulsory tunneling support for use with PDSN Simple IP applications. Each step listed refers to a different section containing the specific instructions for completing the required procedure.

Important These instructions assume that the system was previously configured to support subscriber data sessions as a PDSN.

Step 1 Configure one or more LAC services according to the information and instructions located in the *Configuring LAC Services* section of this chapter.

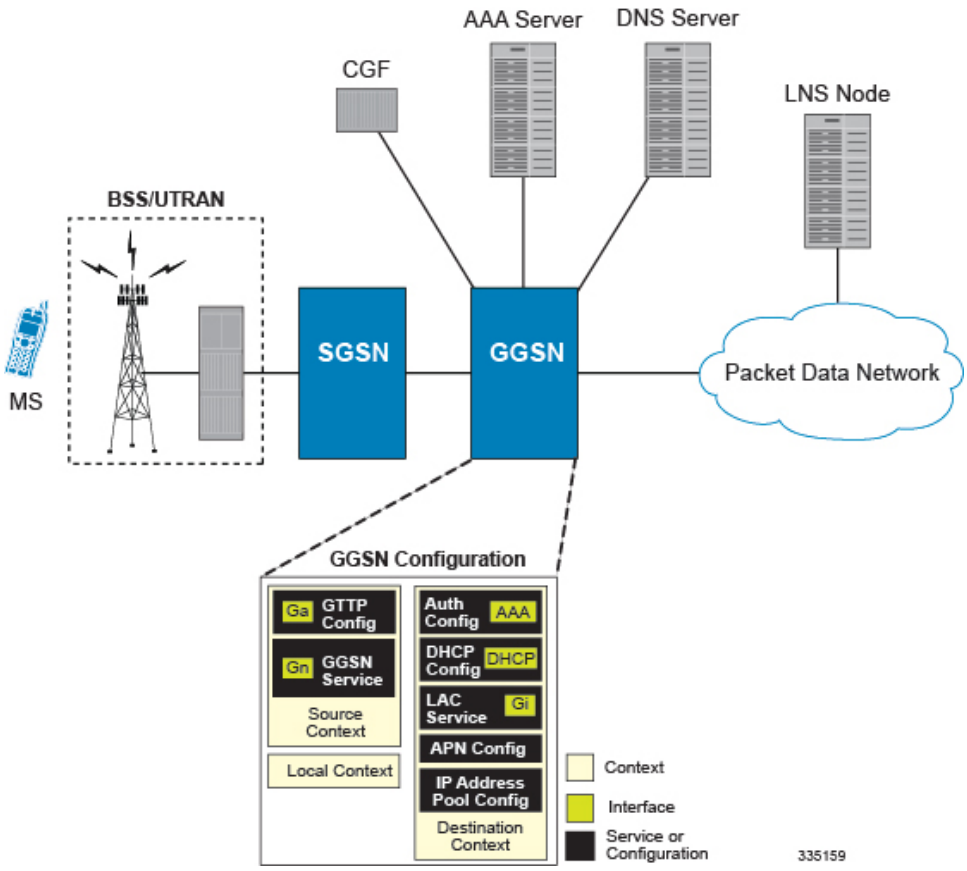
Step 2 Configure the PDSN service(s) according to the instructions located in the *Modifying PDSN Services for L2TP Support* section of this chapter.

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

Supported LAC Service Configurations for the GGSN and P-GW

As mentioned previously, L2TP is supported through the configuration of LAC services on the system. Each LAC service is bound to a single system interface configured within the same system destination context as displayed in following figure.

Figure 4: GGSN LAC Service Configuration



LAC services are applied to incoming subscriber PDP contexts based on the configuration of attributes either in the GGSN's Access Point Name (APN) templates or in the subscriber's profile. Subscriber profiles can be configured locally on the system or remotely on a RADIUS server.

LAC service also supports domain-based L2TP tunneling with LNS. This method is used to create multiple tunnels between LAC and LNS on the basis of values received in "Tunnel-Client-Auth-ID" or "Tunnel-Server-Auth-ID" attribute received from AAA Server in Access-Accept as a key for tunnel selection and creation. When the LAC needs to establish a new L2TP session, it first checks if there is any existing L2TP tunnel with the peer LNS based on the value of key "Tunnel-Client-Auth-ID" or "Tunnel-Server-Auth-ID" attribute. If no such tunnel exists for the key, it will create a new Tunnel with the LNS.

If LAC service needs to establish a new tunnel for new L2TP session with LNS and the tunnel create request fails because maximum tunnel creation limit is reached, LAC will try other LNS addresses received from AAA server in Access-Accept message. If all available peer-LNS are exhausted, LAC service will reject the call

L2TP tunnel parameters are configured within the APN template and are applied to all subscribers accessing the APN. However, L2TP operation will differ depending on the subscriber's PDP context type as described below:

- **Transparent IP:** The APN template's L2TP parameter settings will be applied to the session.
- **Non-transparent IP:** Since authentication is required, L2TP parameter attributes in the subscriber profile (if configured) will take precedence over the settings in the APN template.

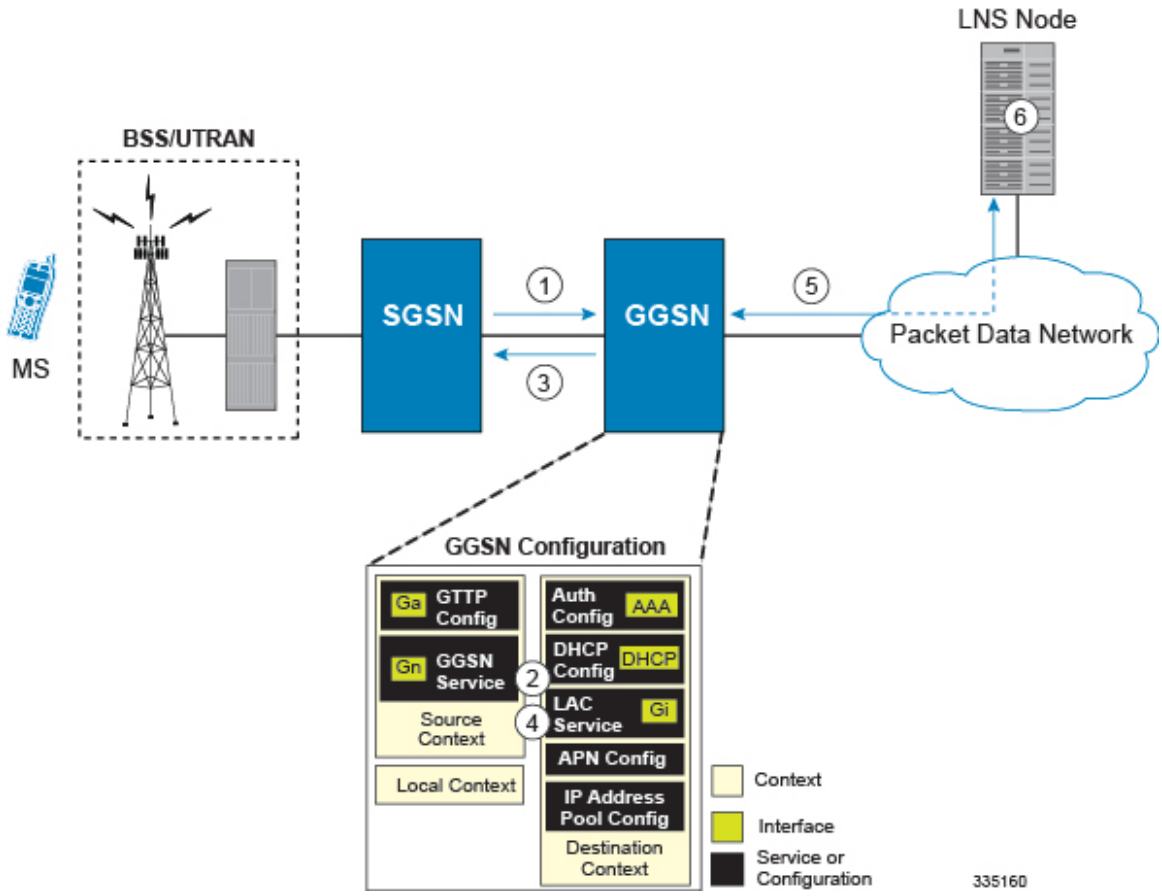
- **PPP:** The APN template's L2TP parameter settings will be applied and all of the subscriber's PPP packets will be forwarded to the specified LNS.

More detailed information is located in the sections that follow.

Transparent IP PDP Context Processing with L2TP Support

The following figure and the text that follows describe how transparent IP PDP contexts are processed when L2TP tunneling is enabled.

Figure 5: Transparent IP PDP Context Call Processing with L2TP Tunneling



1. A Create PDP Context Request message for a subscriber session is sent from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.
2. The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN.

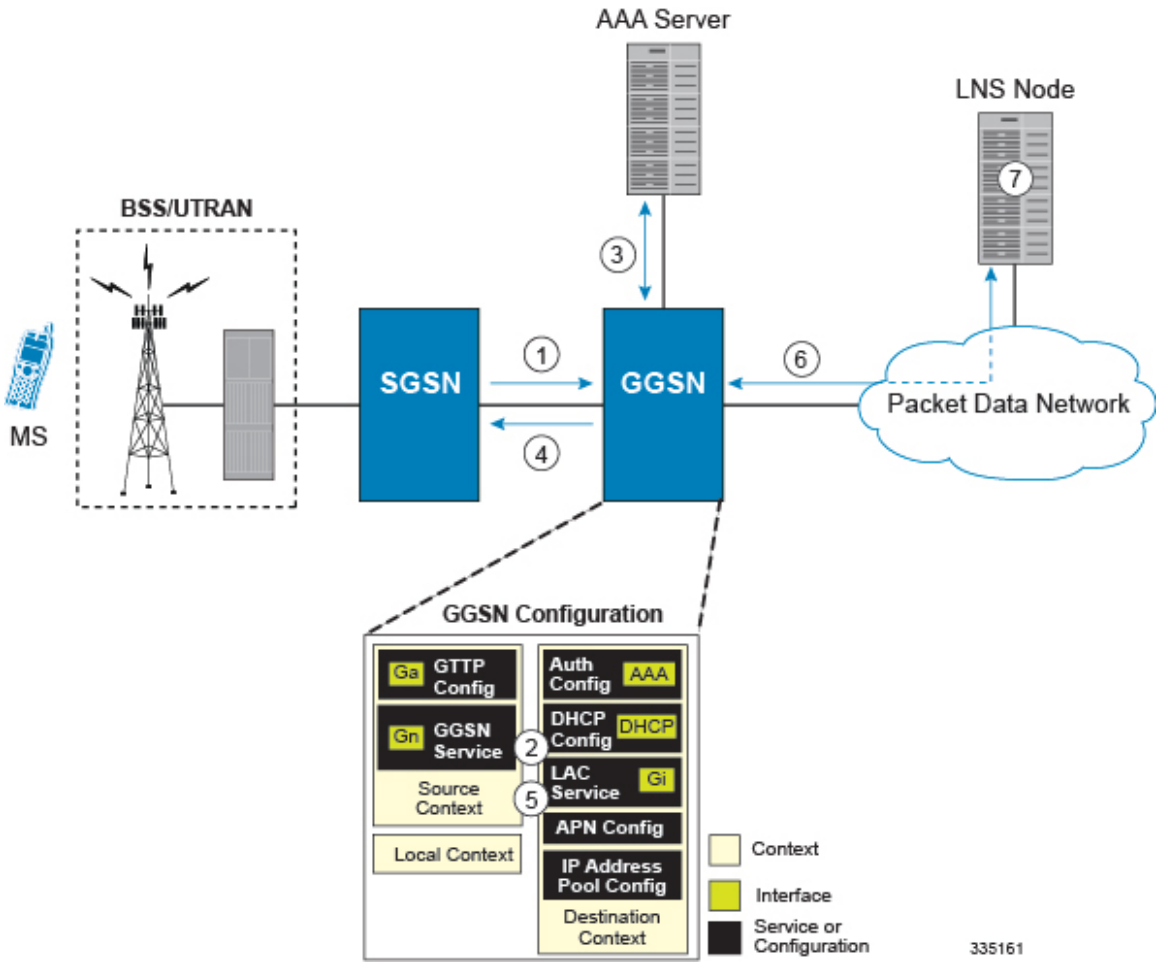
   The APN configuration indicates such things as the IP address of the LNS, the system destination context in which a LAC service is configured, and the outbound username and password that will be used by the LNS to authenticate incoming sessions. If no outbound information is configured, the subscriber's International Mobile Subscriber Identity (IMSI) is used as the username at the peer LNS.

1. The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface.
2. The GGSN passes data received from the MS to a LAC service.
3. The LAC service encapsulates the IP packets and forwards it to the appropriate Gi interface for delivery to the LNS.
4. The LNS un-encapsulates the packets and processes them as needed. The processing includes IP address allocation.

Non-transparent IP PDP Context Processing with L2TP Support

The following figure and the text that follows describe how non-transparent IP PDP contexts are processed when L2TP tunneling is enabled.

Figure 6: Non-transparent IP PDP Context Call Processing with L2TP Tunneling



1. A Create PDP Context Request message for a subscriber session is sent from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.

2. The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN.

   The APN configuration indicates such things as the IP address of the LNS, the system destination context in which a LAC service is configured, and the outbound username and password that will be used by the LNS to authenticate incoming sessions. If no outbound information is configured, the subscriber\'s username is sent to the peer LNS.

3. The GGSN service authenticates the subscriber. The subscriber could be configured either locally or remotely on a RADIUS server. Figure above shows subscriber authentication using a RADIUS AAA server.

   As part of the authentication, the RADIUS server returns an Access-Accept message.

   The message may include attributes indicating that session data is to be tunneled using L2TP, and the name and location of the LAC service to use. An attribute could also be provided indicating the LNS peer to connect to.

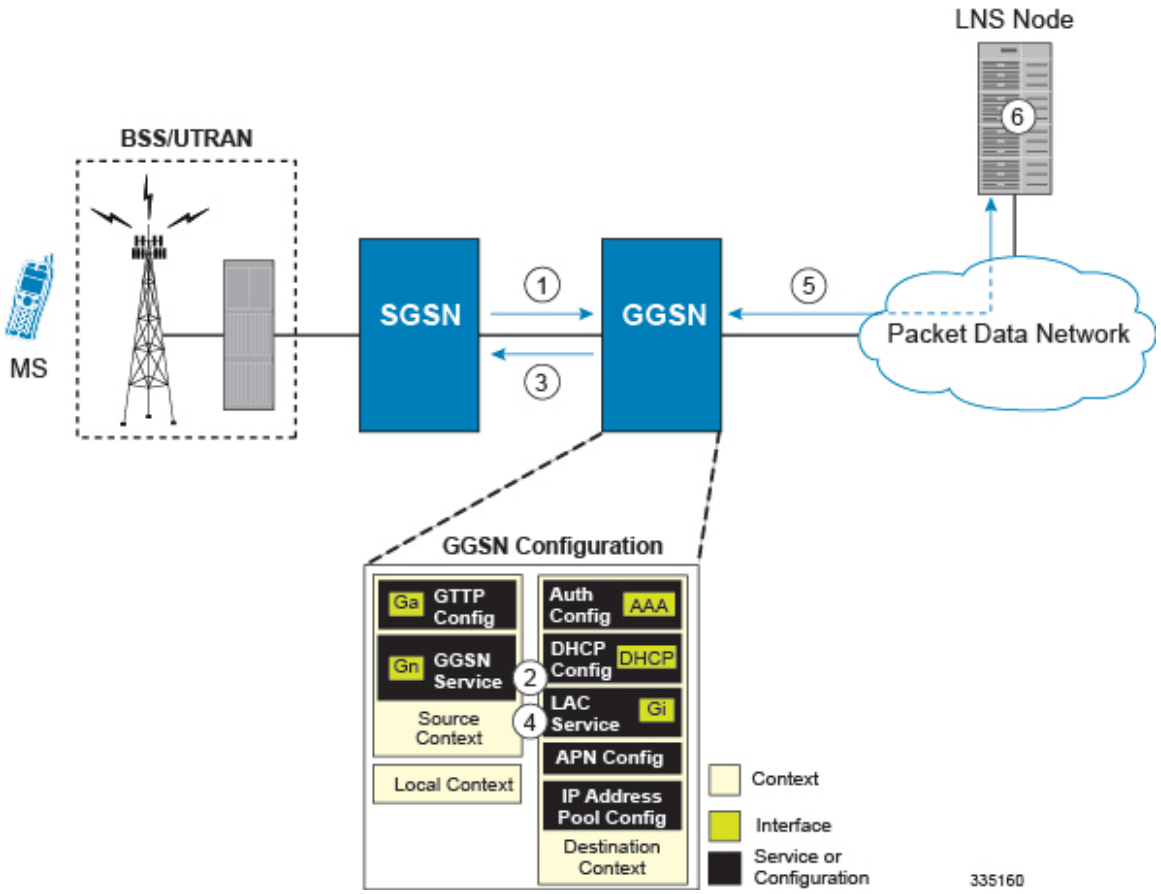
   If these attributes are supplied, they take precedence over those specified in the APN template.

4. The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface.
5. The GGSN passes data received from the MS to a LAC service.
6. The LAC service encapsulates the IP packets and forwards it to the appropriate Gi interface for delivery to the LNS.
7. The LNS un-encapsulates the packets and processes them as needed.The processing includes authentication and IP address allocation.

PPP PDP Context Processing with L2TP Support

The following figure and the text that follows describe how non-transparent IP PDP contexts are processed when L2TP tunneling is enabled.

Figure 7: PPP PDP Context Call Processing with L2TP Tunneling



1. A Create PDP Context Request message for a subscriber session is sent from the SGSN to the GGSN service over the Gn interface. The message contains information such as the PDP Type, APN, and charging characteristics.
2. The GGSN determines whether or not it is configured with an APN identical to the one specified in the message. If so, it determines how to process the session based on the configuration of the APN.

   The APN configuration indicates such things as the IP address of the LNS, the system destination context in which a LAC service is configured.

   Note that L2TP support could also be configured in the subscriber\'s profile. If the APN is not configured for L2TP tunneling, the system will attempt to authenticate the subscriber.The tunneling parameters in the subscriber\'s profile would then be used to determine the peer LNS.
3. The GGSN returns an affirmative Create PDP Context Response to the SGSN over the Gn interface.
4. The GGSN passes the PPP packets received from the MS to a LAC service.
5. The LAC service encapsulates the PPP packets and forwards it to the appropriate Gi interface for delivery to the LNS.
6. The LNS un-encapsulates the packets and processes them as needed. The processing includes PPP termination, authentication (using the username/password provided by the subscriber), and IP address allocation.

Configuring the GGSN or P-GW to Support L2TP

This section provides a list of the steps required to configure the GGSN or P-GW to support L2TP. Each step listed refers to a different section containing the specific instructions for completing the required procedure.

Important These instructions assume that the system was previously configured to support subscriber data sessions as a GGSN or P-GW.

Step 1 Configure the APN template to support L2TP tunneling according to the information and instructions located in the *Modifying APN Templates to Support L2TP* section of this chapter.

Important L2TP tunneling can be configured within individual subscriber profiles as opposed/or in addition to configuring support with an APN template. Subscriber profile configuration is described in the *Configuring Subscriber Profiles for L2TP Support* section of this chapter.

Step 2 Configure one or more LAC services according to the information and instructions located in the *Configuring LAC Services* section of this chapter.

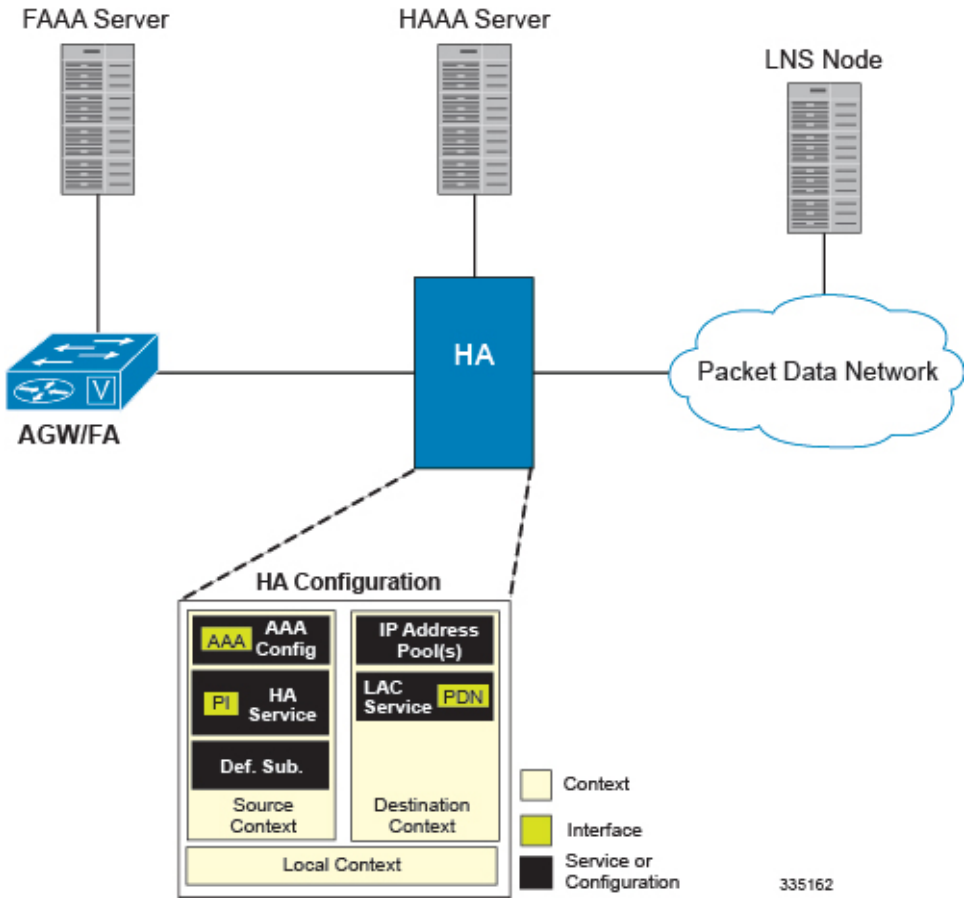
Step 3 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface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

Supported LAC Service Configuration for Mobile IP

LAC services can be applied to incoming MIP sessions using attribute-based tunneling. Attribute-based tunneling is used to encapsulate PPP packets for specific users, identified during authentication. In this method, the LAC service parameters and allowed LNS nodes that may be communicated with are controlled by the user profile for the particular subscriber. The user profile can be configured locally on the system or remotely on a RADIUS server.

Each LAC service is bound to a single system interface within the same system context. It is recommended that this context be a destination context as displayed in figure below.

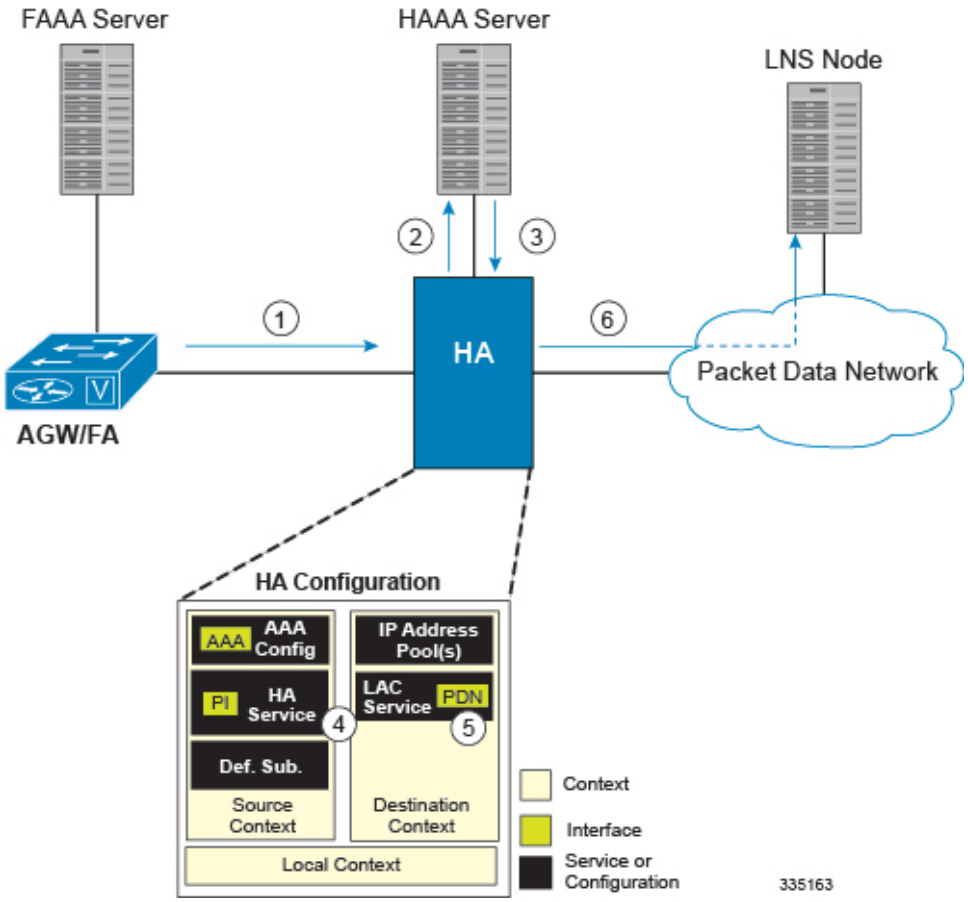
Figure 8: LAC Service Configuration for MIP



How The Attribute-based L2TP Configuration for MIP Works

The following figure and the text that follows describe how Attribute-based tunneling for MIP is performed using the system.

Figure 9: Attribute-based L2TP Session Processing for MIP



1. A subscriber session from the FA is received by the HA service over the Pi interface.
2. The HA service attempts to authenticate the subscriber. The subscriber could be configured either locally or remotely on a RADIUS server. Figure above shows subscriber authentication using a RADIUS AAA server.
3. The RADIUS server returns an Access-Accept message, which includes attributes indicating that session data is to be tunneled using L2TP, and the name and location of the LAC service to use. An attribute could also be provided indicating the LNS peer to connect to.
4. The HA service receives the information and then forwards the packets to the LAC service, configured within the Destination context.
5. The LAC service, upon receiving the packets, encapsulates the information and forwards it to the appropriate PDN interface for delivery to the LNS.
6. The encapsulated packets are sent to the peer LNS through the packet data network where they will be un-encapsulated.

Configuring Attribute-based L2TP Support for HA Mobile IP

This section provides a list of the steps required to configure attribute-based L2TP support for use with HA Mobile IP applications. Each step listed refers to a different section containing the specific instructions for completing the required procedure.

Important These instructions assume that the system was previously configured to support subscriber data sessions as an HA.

Step 1 Configure the subscriber profiles according to the information and instructions located in the *Configuring Subscriber Profiles for L2TP Support* section of this chapter.

Step 2 Configure one or more LAC services according to the information and instructions located in the *Configuring LAC Services* section of this chapter.

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

Configuring Subscriber Profiles for L2TP Support

This section provides information and instructions on the following procedures:

Important Since the instructions for configuring subscribers differ between RADIUS server applications, this section only provides the individual attributes that can be added to the subscriber profile. Refer to the documentation that shipped with your RADIUS server for instructions on configuring subscribers.

RADIUS and Subscriber Profile Attributes Used

Attribute-based L2TP tunneling is supported through the use of attributes configured in subscriber profiles stored either locally on the system or remotely on a RADIUS server. The following table describes the attributes used in support of LAC services. These attributes are contained in the standard and VSA dictionaries.

Table 1: Subscriber Attributes for L2TP Support

RADIUS Attribute	Local Subscriber Attribute	Description	Variable
Tunnel-Type	tunnel l2tp	Specifies the type of tunnel to be used for the subscriber session	L2TP
Tunnel-Server-Endpoint	tunnel l2tp peer-address	Specifies the IP address of the peer LNS to connect tunnel to.	IPv4 address in dotted-decimal format, enclosed in quotation marks

RADIUS Attribute	Local Subscriber Attribute	Description	Variable
Tunnel-Password	tunnel l2tp secret	Specifies the shared secret between the LAC and LNS.	Alpha and or numeric string from 1 to 63 characters, enclosed in quotation marks
Tunnel-Private- Group-ID	tunnel l2tp tunnel-context	Specifies the name of the destination context configured on the system in which the LAC service(s) to be used are located. **Important** If the LAC service and egress interface are configured in the same context as the core service or HA service, this attribute is not needed.	Alpha and or numeric string from 1 to 63 characters, enclosed in quotation marks
Tunnel-Preference	tunnel l2tp preference	Configures the priority of each peer LNS when multiple LNS nodes are configured. **Important** This attribute is only used when the **loadbalance-tunnel-peers** parameter or **SN-Tunnel-Load-Balancing** attribute configured to prioritized.	Integer from 1 to 65535

RADIUS Attribute	Local Subscriber Attribute	Description	Variable
SN-Tunnel-Load-Balancing	loadbalance-tunnel- peer	A vendor-specific attribute (VSA) used to provides a selection algorithm defining how an LNS node is selected by the RADIUS server when multiple LNS peers are configured within the subscriber profile.	• **Random** - Random LNS selection order, the **Tunnel-Preference** attribute is not used in determining which LNS to select. • **Balanced** - LNS selection is sequential balancing the load across all configured LNS nodes, the **Tunnel-Preference** attribute is not used in determining which LNS to select. • **Prioritized** - LNS selection is made based on the priority assigned in the **Tunnel-Preference** attribute.
Client-Endpoint	local-address	Specifies the IP address of a specific LAC service configured on the system that to use to facilitate the subscriber\'s L2TP session. This attribute is used when multiple LAC services are configured.	IPv4 address in dotted decimal notation. (xxx.xxx.xxx.xxx)

RADIUS Tagging Support

The system supports RADIUS attribute tagging for tunnel attributes. These "tags" organize together multiple attributes into different groups when multiple LNS nodes are defined in the user profile. Tagging is useful to ensure that the system groups all the attributes used for a specific server. If attribute tagging is not supported by your specific RADIUS server, the system implicitly organizes the attributes in the order that they are listed in the access accept packet.

Configuring Local Subscriber Profiles for L2TP Support

This section provides information and instructions for configuring local subscriber profiles on the system to support L2TP.

Important The configuration of RADIUS-based subscriber profiles is not discussed in this document. Please refer to the documentation supplied with your RADIUS server for further information.

Important This section provides the minimum instruction set for configuring local subscriber profile for L2TP support on the system. For more information on commands that configure additional parameters and options, refer to the *LAC Service Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

To configure the system to provide L2TP support to subscribers:

Step 1 Configure the "Local" subscriber with L2TP tunnel parameters and the load balancing parameters with action by applying the example configuration in the *Configuring Local Subscriber* section.

Step 2 Verify your L2TP configuration by following the steps in the *Verifying the L2TP Configuration* section.

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

Configuring Local Subscriber

Use the following example to configure the Local subscriber with L2TP tunnel parameters. Optionally you can configure load balancing between multiple LNS servers:

```
configure
   context <ctxt_name> [-noconfirm]
      subscriber name <subs_name>
         tunnel l2tp peer-address <lns_ip_address> [ preference <integer> | [
encrypted ] secret <secret_string> | tunnel-context <context_name> | local-address
 <local_ip_address> }
         load-balancing { random | balanced | prioritized }
         end
```

Notes:

- *<ctxt_name>* is the system context in which you wish to configure the subscriber profile.
- *<lns_ip_address>* is the IP address of LNS server node and *<local_ip_address>* is the IP address of system which is bound to LAC service.

Verifying the L2TP Configuration

These instructions are used to verify the L2TP configuration.

Verify that your L2TP configurations were configured properly by entering the following command in Exec Mode in specific context:

show subscriber configuration username *user_name*

The output of this command is a concise listing of subscriber parameter settings as configured.

Tunneling All Subscribers in a Specific Context Without Using RADIUS Attributes

As with other services supported by the system, values for subscriber profile attributes not returned as part of a RADIUS Access-Accept message can be obtained using the locally configured profile for the subscriber named default. The subscriber profile for default must be configured in the AAA context (i.e. the context in which AAA functionality is configured).

As a time saving feature, L2TP support can be configured for the subscriber named default with no additional configuration for RADIUS-based subscribers. This is especially useful when you have separate source/AAA contexts for specific subscribers.

To configure the profile for the subscriber named default, follow the instructions above for configuring a local subscriber and enter the name default.

Feature Description

When a multicast service is set up for the mobile Customer Premises Equipment (CPE), the APN is configured with L2TP tunnel and P-GW works as L2TP Access Concentrator (LAC). To set up the multicast session, the video client/mobile CPE need to send or receive the PIM (Protocol Independent Multicast) message (with TTL=1) to or from Video headend server over SGi L2TP tunnel.

The P-GW follows the default L2TP LAC to inspect and process the encapsulated IP traffic inside the L2TP tunnel. This process prevents certain applications between CPE and LNS that sends TTL=1 traffic to function. Prior to 21.21.1 release, when an IP packet is sent, the Time to Live (TTL) value (for example, 255) was decremented by 1 at each hop. The P-GW dropped the packet with TTL value 0 or 1, decremented (when TTL > 1) the TTL value and the new checksum for the data packet was calculated. In this release, by enabling multicast session over L2TP feature through CLI:

- P-GW ignores the TTL value and forwards the packet.
- The L2TP and regular packets gets differentiated by L2TP tunnel type at sessmgr_ipv4.c and it verifies the CLI configuration mode enabled.

Configuring LAC Services

Important Not all commands, keywords and functions may be available. Functionality is dependent on platform and license(s).

This section provides information and instructions for configuring LAC services on the system allowing it to communicate with peer LNS nodes.

Important This section provides the minimum instruction set for configuring LAC service support on the system. For more information on commands that configure additional parameters and options, refer to the *LAC Service Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

To configure the LAC services on system:

Step 1 Configure the LAC service on system and bind it to an IP address by applying the example configuration in the *Configuring LAC Service* section.

Step 2 *Optional*. Configure LNS peer information if the Tunnel-Service-Endpoint attribute is not configured in the subscriber profile or PDSN compulsory tunneling is supported by applying the example configuration in the *Configuring LNS Peer* section.

Step 3 Verify your LAC configuration by following the steps in the Verifying the LAC Service Configuration section.

Step 4 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Configuring LAC Service

Use the following example to create the LAC service and bind the service to an IP address:

```
configure
  context <dst_ctxt_name> [-noconfirm]
    lac-service <service_name>
      bind address <ip_address>
      end
```

Notes:

- *<dst_ctxt_name>* is the destination context where you want to configure the LAC service.

Configuring Multicast Services over L2TP

Use the following CLI commands to enable or disable the multicast session over L2TP feature. By default, this feature is disabled.

```
configure
  context context_name
    lac-service service_name
      ttl-ignore
      end
```

Notes:

- **ttl-ignore**: Ignores the TTL value and forwards the packets.

Configuring LNS Peer

Use the following example to configure the LNS peers and load balancing between multiple LNS peers:

```
configure
   context <dst_ctxt_name> [ -noconfirm ]
      lac-service <service_name>
         tunnel selection-key tunnel-server-auth-id
         peer-lns <ip_address> [encrypted] secret <secret> [crypto-map <map_name>
{[encrypted] isakmp-secret <secret> }] [description <text>] [ preference <integer>]

         load-balancing { random | balanced | prioritized }
         end
```

Notes:

- <*dst_ctxt_name*> is the destination context where the LAC service is configured.

Verifying the LAC Service Configuration

These instructions are used to verify the LAC service configuration.

Verify that your LAC service configurations were configured properly by entering the following command in Exec Mode in specific context:

show lac-service name *service_name*

The output given below is a concise listing of LAC service parameter settings as configured.

```
Service name: vpn1
Context:                        isp1
Bind:                           Done
Local IP Address:               192.168.2.1
First Retransmission Timeout:   1 (secs)
Max Retransmission Timeout:     8 (secs)
Max Retransmissions:            5
Max Sessions:                   500000      Max Tunnels: 32000
Max Sessions Per Tunnel:        512
Data Sequence Numbers:          Enabled     Tunnel Authentication:  Enabled
Keep-alive interval:            60          Control receive window: 16
Max Tunnel Challenge Length:    16
Proxy LCP Authentication:       Enabled
Load Balancing:                 Random
Service Status:                 Started
Newcall Policy:                 None
```

Modifying PDSN Services for L2TP Support

PDSN service modification is required for compulsory tunneling and optional for attribute-based tunneling.

For attribute-based tunneling, a configuration error could occur such that upon successful authentication, the system determines that the subscriber session requires L2TP but cannot determine the name of the context in which the appropriate LAC service is configured from the attributes supplied. As a precautionary, a parameter

has been added to the PDSN service configuration options that will dictate the name of the context to use. It is strongly recommended that this parameter be configured.

This section contains instructions for modifying the PDSN service configuration for either compulsory or attribute-based tunneling.

Important This section provides the minimum instruction set for modifying PDSN service for L2TP support on the system. For more information on commands that configure additional parameters and options, refer to the *LAC Service Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

To configure the LAC services on system:

Step 1 Modify the PDSN service to support L2TP by associating LAC context and defining tunnel type by applying the example configuration in the *Modifying PDSN Service* section.

Step 2 Verify your configuration to modify PDSN service by following the steps in the *Verifying the PDSN Service for L2TP Support* section.

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

Modifying PDSN Service

Use the following example to modify the PDSN service to support L2TP by associating LAC context and defining tunnel type:

```
configure
   context <source_ctxt_name> [ -noconfirm ]
      pdsn-service <pdsn_service_name>
         ppp tunnel-context <lac_context_name>
         ppp tunnel-type { l2tp | none }
         end
```

Notes:

- <*source_ctxt_name*> is the name of the source context containing the PDSN service, which you want to modify for L2TP support.
- <*pdsn_service_name*> is the name of the pre-configured PDSN service, which you want to modify for L2TP support.
- <*lac_context_name*> is typically the destination context where the LAC service is configured.

Verifying the PDSN Service for L2TP Support

These instructions are used to verify the PDSN service configuration.

Verify that your PDSN is configured properly by entering the following command in Exec Mode in specific context:

```
show pdsn-service name pdsn_service_name
```

The output of this command is a concise listing of PDSN service parameter settings as configured.

Modifying APN Templates to Support L2TP

This section provides instructions for adding L2TP support for APN templates configured on the system.

Important This section provides the minimum instruction set for configuring LAC service support on the system. For more information on commands that configure additional parameters and options, refer to the *LAC Service Configuration Mode Commands* chapter in the *Command Line Interface Reference*.

To configure the LAC services on system:

Step 1 Modify the APN template to support L2TP with LNS server address and other parameters by applying the example configuration in the *Assigning LNS Peer Address in APN Template* section.

Step 2 Optional. If L2TP will be used to tunnel transparent IP PDP contexts, configure the APN\'s outbound username and password by applying the example configuration in the *Configuring Outbound Authentication* section.

Step 3 Verify your APN configuration by following the steps in the *Verifying the APN Configuration* section.

Step 4 Save your configuration to flash memory, an external memory device, and/or a network location using the Exec mode command **save configuration**. For additional information on how to verify and save configuration files, refer to the *System Administration Guide* and the *Command Line Interface Reference*.

Assigning LNS Peer Address in APN Template

Use following example to assign LNS server address with APN template:

```
configure
   context <dst_ctxt_name> [-noconfirm]
      apn <apn_name>
         tunnel l2tp [ peer-address <lns_address> [ [ encrypted ] secret
<l2tp_secret> ] [ preference <integer> ] [ tunnel-context <l2tp_context_name> ] [
local-address <local_ip_address> ] [ crypto-map <map_name> { [ encrypted ]
isakmp-secret <crypto_secret> } ]
         end
```

Notes:

- <*dst_ctxt_name*> is the name of system destination context in which the APN is configured.
- <*apn_name*> is the name of the pre-configured APN template which you want to modify for the L2TP support.
- <*lns_address*> is the IP address of LNS server node and <*local_ip_address*> is the IP address of system which is bound to LAC service.

Configuring Outbound Authentication

Use the following example to configure the LNS peers and load balancing between multiple LNS peers:

```
configure
   context <dst_ctxt_name> [ -noconfirm ]
      apn <apn_name>
         outbound { [ encrypted ] password <pwd> | username <name> }
         end
```

Notes:

- <*dst_ctxt_name*> is the destination context where APN template is is configured.
- <*apn_name*> is the name of the pre-configured APN template which you want to modify for the L2TP support.

Verifying the APN Configuration

These instructions are used to verify the APN configuration.

Verify that your APN configurations were configured properly by entering the following command in Exec Mode in specific context:

```
show apn name apn_name
```

The output is a concise listing of APN parameter settings as configured.