LAC Service Configuration Mode Commands

The LAC Service Configuration Mode is used to create and manage L2TP services within contexts on the system. L2TP Access Concentrator (LAC) services facilitate tunneling to peer L2TP Network Servers (LNSs).

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

configure > context *context_name* **> lac-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lac-service)#
```

Important The commands or keywords/variables that are available are dependent on platform type, product version, and installed license(s).

Important For information on common commands available in this configuration mode, refer to the Common Commands chapter.

allow

This command configure the system to allow different attributes in the LAC Hostname Attribute Value Pair (AVP) and Called-Number AVP for L2TP messages exchanged between LAC and LNS.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

configure > **context** *context_name* > **lac-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lac-service)#
```

Syntax Description

```
allow { aaa-assigned-hostname | called-number value apn | calling-number
 value imsi }
default allow { aaa-assigned-hostname | called-number value apn }
no allow { aaa-assigned-hostname | called-number value apn | calling-number
 }
```

no

Disable the configured attribute and returns to the behavior that uses the LAC-Service name as the HostName AVP.

aaa-assigned-hostname

When enabled if AAA assigns a valid Tunnel-Client-Auth-ID attribute for the tunnel, it is used as the HostName AVP in the L2TP tunnel setup message.

This keyword works in conjunction with the **local-hostname** *hostname* keyword applied via the **tunnel l2tp** command in APN Configuration mode.

When Tunnel parameters are not received from the RADIUS Server, Tunnel parameters configured in an APN are considered for the LNS peer selection. When APN configuration is selected, the local-hostname configured with the **tunnel l2tp** command in the APN for the LNS peer will be used as an LAC Hostname.

called-number value apn

Configures the system to send the APN name in the Called-Number AVP as a part of ICRQ message sent to the LNS. If this keyword is not configured, Called-Number AVP will not be included in ICRQ message sent to the LNS.

calling-number value imsi

Configures the system to allow the IMSI to be used as Calling-Number as a part of ICRQ message sent to the LNS. If this keyword is not configured, then MSISDN will be used as Calling-Number.

Important This is a customer-specific keyword available for PDSN. Please contact your local Cisco sales representative for more information.

Usage Guidelines

Use this command to configure the attribute for the HostName AVP for L2TP messages exchanged between LAC and LNS.

LAC Hostname will be different for the subscribers corresponding to the different corporate APNs. In the absence of a AAA assigned HostName, the LAC-Service name is used as HostName. By default the LAC-Service name is used as the HostName AVP.

Example

The following command enables the use of the value of Tunnel-Client-Auth-ID attribute for the HostName AVP:

```
allow aaa-assigned-hostname
```

Use the following command to reset the behavior so that the LAC-Service uses the LAC-Service name as the HostName AVP:

```
no allow aaa-assigned-hostname
```

bind

This command assigns a local end point address to the LAC service in the current context.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

configure > context *context_name* **> lac-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lac-service)#
```

Syntax Description

bind *ip_address* **[max-subscribers]**
no bind *ip_address*

no

Unassign, or unbind, the local end point to the LAC service.

ip_address

This must be a valid IP address entered using IPv4 dotted-decimal notation.

max-subscribers

The maximum number of subscribers that can use the endpoint for this LAC service. Must be an integer from 1 to 2500000.

Usage Guidelines

Use this command to bind a local end point IP address to the LAC service.

Example

The following command binds the local end point IP address *10.10.10.100* to the LAC service in the current context:

```
bind 10.10.10.100
```

The following command removes the binding of the local end point to the LAC service:

```
no bind
```

data sequence-number

Enables data sequence numbering for sessions that use the current LAC service. Data sequence numbering is enabled by default.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

configure > **context** *context_name* > **lac-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lac-service)#
```

Syntax Description

```
[ no ] data sequence-number
```

no

Disables data sequence numbering for sessions.

Usage Guidelines

An L2TP data packet header has an optional data sequence numbers field. The data sequence number may be used to ensure ordered delivery of data packets. This command is used to re-enable or disable the use of the data sequence numbers for data packets.

Example

Use the following command to disable the use of data sequence numbering:

```
no data sequence-number
```

Use the following command to re-enable data sequence numbering:

```
data sequence-number
```

default

This command sets the specified LAC service parameter to its default value or setting.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

configure > **context** *context_name* > **lac-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lac-service)#
```

Syntax Description

```
default { data sequence-number | hide-attributes | keepalive-interval |
load-balancing | local-receive-window | max-retransmission |
max-session-per-tunnel | max-tunnel-challenge-length | max-tunnels |
proxy-lcp-authentication | retransmission-timeout-first |
retransmission-timeout-max | trap all | tunnel-authentication }
```

data sequence-number

Enables data sequence numbering for sessions.

hide-attributes

Disables hiding attributes in control messages sent from the LAC to the LNS.

keepalive-interval

Sets the interval for send L2TP Hello keepalive if there is no control or data transactions to the default value of 60 seconds.

load-balancing

Sets the load balancing algorithm to be used when many LNS peers have been configured to the default of round robin.

local-receive-window

Sets the window size to be used for the local side for the reliable control transport to the default of 16.

max-retransmission

Sets the maximum number of retransmissions to the default of 5.

max-session-per-tunnel

Sets the maximum number of sessions per tunnel at any point in time to the default of 512.

max-tunnel-challenge-length

Sets the maximum length of the tunnel challenge to the default of 16 bytes.

max-tunnels

Sets the maximum number of tunnels for this service to the default of 32000.

proxy-lcp-authentication

Sets sending of proxy LCP authentication parameters to the LNS to the default state of enabled.

retransmission-timeout-first

Sets the first retransmit interval to the default of 1 second.

retransmission-timeout-max

Sets the maximum retransmit interval to the default of 8 seconds.

trap all

Generates all supported SNMP traps.

tunnel-authentication

Sets tunnel authentication to the default state of enabled.

Usage Guidelines

Use the default command to set LAC service parameters to their default states.

Example

Use the following command to set the keep alive interval to the default value of 60 seconds:

```
default
keepalive-interval
```

Use the following command to set the maximum number of sessions per tunnel to the default value of 512:

```
default max-session-per-tunnel
```

hide-attributes

Enables hiding certain attributes (such as proxy-auth-name and proxy-auth-rsp) in control messages sent from the LAC to the LNS. The LAC hides such attributes only if tunnel authentication is enabled between the LAC and the LNS.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

configure > context *context_name* **> lac-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lac-service)#
```

Syntax Description

```
[ no ] hide-attributes
```

no

Disable hiding attributes.

Usage Guidelines

Use this command to hide certain attributes from control messages when tunnel authentication is enabled between the LAC and the LNS.

Example

The following command enables hiding attributes:

```
hide-attributes
```

keepalive-interval

This command specifies the amount of time to wait before sending a Hello keep alive message.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

configure > context *context_name* **> lac-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lac-service)#
```

Syntax Description

keepalive-interval *seconds*
no keepalive-interval

no

Disables the generation of Hello keepalive messages on the tunnel.

seconds

Default: 60

The number of seconds to wait before sending a Hello keepalive message. The number can be configured to an integer from 30 to 2147483648.

Usage Guidelines

Use this command to set the amount of time to wait before sending a Hello keepalive message or disable the generation of Hello keep alive messages completely. A keepalive mechanism is employed by L2TP in order to differentiate tunnel outages from extended periods of no control or data activity on a tunnel. This is accomplished by injecting Hello control messages after a specified period of time has elapsed since the last data or control message was received on a tunnel. As for any other control message, if the Hello message is not reliably delivered then the tunnel is declared down and is reset. The transport reset mechanism along with the injection of Hello messages ensures that a connectivity failure between the LNS and the LAC is detected at both ends of a tunnel.

Example

Use the following command to set the Hello keepalive message interval to *120* seconds:

```
keepalive-interval 120
```

Use the following command to disable the generation of Hello keepalive messages:

```
no keepalive-interval
```

load-balancing

Configures how LNSs are selected for this LAC service.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

configure > context *context_name* **> lac-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-lac-service)#`

Syntax Description

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

balanced

LNS selection is made without regard to prioritization, but in a sequential order that balances the load across the total number of LNS nodes available.

prioritized

LNS selection is made based on the priority assigned in the Tunnel-Preference attribute. An example of this method is three LNS nodes, with preferences of 1, 2, and 3 respectively. In this example, the RADIUS server always tries the tunnel with a preference of 1 before using any of the other LNS nodes.

random

Default: Enabled

LNS selection is random in order, wherein the RADIUS server does not use the Tunnel-Preference attribute in determining which LNS to select.

Usage Guidelines

Use this command to configure the load-balancing algorithm that defines how the LNS node is selected by the LAC when there are multiple peer LNSs configured in the LAC service.

Example

The following command sets the LAC service to connect to LNSs in a sequential order;

`load-balancing balanced`

The following command sets the LAC service to connect to LNSs according to the priority assigned through the Tunnel-Preference attribute:

`load-balancing prioritized`

local-receive-window

Specifies the number of control messages the remote peer LNS can send before waiting for an acknowledgement.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

configure > context *context_name* **> lac-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lac-service)#
```

Syntax Description

local-receive-window *integer*

integer

Default: 4

Specifies the number of control messages to send before waiting for an acknowledgement. The number can be configured to an integer from 1 to 256.

Usage Guidelines

Use this command to set the size of the control message receive window being offered to the remote peer LNS. The remote peer LNS may send the specified number of control messages before it must wait for an acknowledgment.

Example

The following command sets the local receive window to *10* control messages:

```
local-receive-window 10
```

max-retransmission

Sets the maximum number of retransmissions of a control message to a peer before the tunnel and all sessions within it are cleared.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

configure > context *context_name* **> lac-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lac-service)#
```

Syntax Description

max-retransmission *integer*

integer

Default: 5

Specifies the maximum number of retransmissions of a control message to a peer. This value must be an integer from1 through 10.

Usage Guidelines

Each tunnel maintains a queue of control messages to be transmitted to its peer. After a period of time passes without acknowledgement, a message is retransmitted. Each subsequent retransmission of a message employs an exponential backoff interval. For example; if the first retransmission occurs after 1 second, the next retransmission occurs after 2 seconds has elapsed, then the next after 4 seconds. If no peer response is detected after the number of retransmissions set by this command, the tunnel and all sessions within are cleared.

Use this command to set the maximum number of retransmissions that the LAC service sends before closing the tunnel and all sessions within. it.

Example

The following command sets the maximum number of retransmissions of a control message to a peer to *7*:

```
max-retransmissions 7
```

max-session-per-tunnel

Sets the maximum number of sessions that can be facilitated by a single a tunnel at any time.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

configure > context *context_name* **> lac-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lac-service)#
```

Syntax Description

max-sessions-per-tunnel *integer*

integer

Default: 512

The maximum number of sessions expressed as an integer from 1 through 65535.

Usage Guidelines

Use this command to set the maximum number of sessions you want to allow in a tunnel.

Example

The following command sets the maximum number of sessions in a tunnel to *5000*:

```
max-sessions-per-tunnel 5000
```

max-tunnel-challenge-length

Sets the maximum length of the tunnel challenge in bytes.The challenge is used for tunnel authentication purposes during tunnel creation.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

configure > **context** *context_name* > **lac-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lac-service)#
```

Syntax Description

max-tunnel-challenge-length *bytes*

bytes

Default: 16

Specifies the maximum length (in bytes of the tunnel challenge. This must be an integer from 4 through 32.

Usage Guidelines

Use this command to set the maximum length (in bytes) for the tunnel challenge that is used during tunnel creation.

Example

The following command sets the maximum length of the tunnel challenge to *32* bytes:

```
max-tunnel-challenge-length 32
```

max-tunnels

The maximum number of tunnels that the current LAC service can support.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

configure > context *context_name* **> lac-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lac-service)#
```

Syntax Description

max-tunnels *integer*

integer

Default: 32000

The maximum number of tunnels expressed as an integer from 1 through 32000.

Usage Guidelines

Use this command to set the maximum number tunnels that this LAC service can support at any on time.

Example

Use the following command to set the maximum number of tunnels for the current LAC service to *20000*:

```
max-tunnels 20000
```

peer-lns

Adds a peer LNS address for the current LAC service. Up to eight peer LNSs can be configured for each LAC service.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

configure > context *context_name* **> lac-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lac-service)#
```

Syntax Description

peer-lns *ip_address* **[encrypted] secret** *secret* **[crypto-map** *map_name* **{ [encrypted] isakmp-secret** *secret* **}] [description** *text* **] [preference** *integer* **]**
no peer-lns *ip_address*

no peer-lns *ip_address*

Deletes the peer LNS at the IP address specified by *ip_address*. *ip_address* must be entered in IPv4 dotted-decimal notation.

ip_address

The IP address of the peer LNS for the current LAC service. *ip_address* must be entered in IPv4 dotted-decimal notation.

[encrypted] secret *secret*

Designates the secret which is shared between the current LAC service and the peer LNS. *secret* must be an alphanumeric string of 1 through 256 characters that is case sensitive.

encrypted secret *secret*: Specifies that encryption should be used when communicating the secret with the peer LNS.

crypto-map *map_name* { [encrypted] isakmp-secret *secret* }

map_name is the name of a crypto map that has been configured in the current context. *map_name* must be an alphanumeric string of 1 through 127 characters that is case sensitive.

isakmp-secret *secret*: The pre-shared key for IKE. *secret* must be an alphanumeric string of 1 through 127 characters that is case sensitive.

encrypted isakmp-secret *secret*: The pre-shared key for IKE. Encryption must be used when sending the key. *secret* must be an alphanumeric string of 1 through 127 characters.

description *text*

Specifies the descriptive text to use to describe the specified peer LNS. *text* must be an alphanumeric string of 0 through 79 characters.

preference *integer*

This sets the priority of the peer LNS if multiple peer LNSs are configured. *integer* must be an integer from 1 through 128.

Usage Guidelines

Use this command to add a peer LNS address for the current LAC service.

Example

The following command adds a peer LNS to the current LAC service with the IP address of *10.10.10.100*, sets encryption on, specifies the shared secret to be *1b34nnf5d*, and sets the preference to *3*:

```
peer-lns 10.10.10.100 encrypted secret 1b34nnf5d preference 3
```

The following command removes the peer LNS with the IP address of *10.10.10.200* for the current LAC service:

```
no peer-lns 10.10.10.200
```

proxy-lcp-authentication

Enables and disables the sending of proxy LCP authentication parameters to the LNS.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

configure > **context** *context_name* > **lac-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lac-service)#
```

Syntax Description

```
[ no ] proxy-lcp-authentication
```

no

Disables the sending of proxy LCP authentication parameters to the LNS.

proxy-lcp-authentication

Default: Enabled

Enables the sending of proxy LCP authentication parameters to the LNS.

Usage Guidelines Use this feature in situations where the peer LNS does not understand the proxy LCP Auth AVPs that the system sends and does not do an LCP renegotiation and tears down the call.

Example

Use the following command to disable the sending of proxy LCP authentication parameters to the LNS;

```
no proxy-lcp-authentication
```

Use the following command to re-enable the sending of proxy LCP authentication parameters to the LNS:

```
proxy-lcp-authentication
```

retransmission-timeout-first

Each tunnel maintains a queue of control messages to transmit to its peer. After a period of time passes without acknowledgement, a message is retransmitted. This command sets the initial timeout for retransmission of control messages.

Product GGSN

PDSN

P-GW

SAEGW

Privilege Security Administrator, Administrator

Command Modes Exec > Global Configuration > Context Configuration > LAC Service Configuration

configure > **context** *context_name* > **lac-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lac-service)#
```

Syntax Description **retransmission-timeout-first** *integer*

integer

Default: 1

The amount of time to wait (in seconds) before sending the first control message retransmission. This must be an integer from 1 through 100.

Usage Guidelines Use this command to set the initial timeout before retransmitting control messages to the peer.

Example

The following command sets the initial retransmission timeout to *3* seconds:

```
retransmission-timeout-first 3
```

retransmission-timeout-max

Configures maximum amount of time between two retransmission of control messages.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

configure > context *context_name* **> lac-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-lac-service)#`

Syntax Description

`retransmission-timeout-max` *`integer`*

integer

Default: 8

integer is the maximum time (in seconds) to wait before retransmitting control messages expressed as e an integer from 1 through 100.

Usage Guidelines

Use this command to set the maximum amount of time that can elapse before retransmitting control messages.

Each tunnel maintains a queue of control messages to transmit to its peer. After a period of time passes without acknowledgement, a message is retransmitted. Each subsequent retransmission of a message employs an exponential backoff interval.

Example

The following command sets the maximum retransmission time-out to *10* seconds:

```
retransmission-timeout-max 10
```

single-port-mode

This command enables/disables the L2TP LAC service always to use standard L2TP port 1701 as source port for all L2TP control and data packets originated from LAC node.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

configure > context *context_name* **> lac-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lac-service)#
```

Syntax Description

[default | no] single-port-mode

default

Default: Enabled

Sets this command to its default state of disabled. By default single source port configuration for L2TP LAC packets is disabled.

no

Disables the configured single source port configuration from this LAC service.

Usage Guidelines

Use this command to enable or disable the single port mode for L2TP LAC service.

If this feature is enabled, then L2TP LAC service will always use standard L2TP port 1701 as source port for all L2TP control/data packets originated from LAC (instead of the default scheme in which each L2TPMgr uses a dynamic source port). L2TPMgr instance 1 will handle all L2TP calls for the service.

Caution Changing this configuration, while the service is already running, will cause restart of the service.

Example

The following command enables the LAC service to use port 1701 as source port for all L2TP control and data packets:

single-port-mode

snoop framed-ip-address

When enabled, this feature allows the LAC to detect IP Control Protocol (IPCP) packets exchanged between the mobile node and the LNS and extract the framed-ip-address assigned to the mobile node. The address will be reported in accounting start/stop messages and displayed for subscriber sessions.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

configure > context *context_name* **> lac-service** *service_name*

Entering the above command sequence results in the following prompt:

`[context_name]host_name(config-lac-service)#`

Syntax Description

`[ default | no ] snoop framed-ip-address`

default

Disabled.

no

Disables the feature. Accounting start/stop will occur before the PPP session is established and the framed IP address field will be reported as 0.0.0.0.

Usage Guidelines

This feature is available to address simple IP roaming scenarios. If this feature is enabled, the Accounting Start will be sent only after the framed-ip-address is detected. If the framed-ip-address is not detected within 16 seconds, an Accounting Start will be sent for the session with the 0.0.0.0 address. If the session is disconnected during the detection attempt, Accounting Start/Stop will be sent for the session. If the session renegotiates IPCP, an Accounting Stop will be generated with a framed-ip-address from the old session, and an Accounting Start will be generated with an IP address for the new session. IPv6 address detection is not supported.

Important

When this feature is enabled and the show subscribers all command is invoked, the framed-IP-address is displayed for the PDSN Simple IP subscriber in the output display.

tunnel selection-key

Enables the creation of tunnels between an L2TP service and an LNS server on the basis of a key received from AAA server.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

configure > context *context_name* **> lac-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lac-service)#
```

Syntax Description

```
tunnel selection-key { none | tunnel-client-auth-id | tunnel-server-auth-id
 }
default tunnel selection-key
```

default

Disables the creation of tunnel between LAC service and LNS based on a key value received from AAA server.

none

Default: Enabled

This keyword disables the creation of multiple tunnels between a pair of LAC service and LNS server. LAC will not make use of the key to choose a tunnel with LNS in this setup.

tunnel-client-auth-id

Default: Disabled

This keyword enables the creation of tunnels between LAC service and an LNS server on the basis of domain attribute "Tunnel-Client-Auth-ID" value received from AAA server.

tunnel-server-auth-id

Default: Disabled

This keyword enables the creation of tunnels between LAC service and an LNS server on the basis of domain attribute "Tunnel-Server-Auth-ID" value received from AAA server.

Usage Guidelines

Use this command to enable or disable the creation of additional L2TP tunnels between LAC service and LNS server on the basis of "Tunnel-Client-Auth-ID" or "Tunnel-Server-Auth-ID" attribute value received from AAA Server in Access-Accept message. This value of attribute is treated as a key for tunnel selection and creation.

When the LAC needs to establish a new L2TP session, it first checks for an existing L2TP tunnel with the peer LNS based on the value of the key configured. If no such tunnel exists for the key, it will create a new tunnel with the LNS.

The default configuration has the selection-key as **none**. Hence, LAC will not make use of key to choose a tunnel with LNS in default setup.

The maximum number of sessions, as configured via the **max-sessions-per-tunnel** command, is applicable for each tunnel created through this command. By default, each tunnel supports 512 sessions.

If the LAC service needs to establish a new tunnel for a 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 for the APN/subscriber. If all available peer-LNS are exhausted, LAC service will reject the call.

Example

The following command enables the use of "Tunnel-Server-Auth-ID" attribute value received from AAA Server in Access-Accept message as a key for tunnel selection and creation:

```
tunnel selection-key tunnel-server-auth-id
```

tunnel-authentication

Enables tunnel authentication. When tunnel authentication is enabled, a configured shared secret is used to ensure that the LAC service is communicating with an authorized peer LNS. The shared secret is configured by the **peer-lns** command in the LAC Service Configuration mode, the **tunnel l2tp** command in the Subscriber Configuration mode, or the **Tunnel-Password** attribute in the subscribers RADIUS profile.

Product

GGSN

PDSN

P-GW

SAEGW

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LAC Service Configuration

configure > context *context_name* **> lac-service** *service_name*

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lac-service)#
```

Syntax Description

```
[ no ] tunnel-authentication
```

no

Disables tunnel authentication.

Tunnel authentication is enabled by default.

Usage Guidelines

Disable or enable the usage of secrets to authenticate a peer LNS when setting up a tunnel.

Example

To disable tunnel authentication, use the following command:

```
no tunnel-authentication
```

To re-enable tunnel authentication, use the following command:

```
tunnel-authentication
```