

LNS Service Configuration Mode Commands

The LNS Service Configuration Mode is used to create and manage L2TP services within contexts on the system. L2TP Network Server (LNS) services facilitate tunneling with peer L2TP Access Concentrators (LACs).

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lns-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.

- aaa accounting, on page 2
- authentication, on page 3
- avp map called-number apn, on page 5
- bind, on page 5
- data sequence-number, on page 6
- default, on page 7
- ip source-violation, on page 9
- keepalive-interval, on page 11
- local-receive-window, on page 12
- max-retransmission, on page 13
- max-session-per-tunnel, on page 13
- max-tunnel-challenge-length, on page 14
- max-tunnels, on page 15
- nai-construction domain, on page 15
- newcall, on page 16

- peer-lac, on page 17
- proxy-lcp-authentication, on page 18
- retransmission-timeout-first, on page 19
- retransmission-timeout-max, on page 20
- setup-timeout, on page 21
- single-port-mode, on page 21
- trap, on page 22
- tunnel-authentication, on page 23
- tunnel-switching, on page 23

aaa accounting

Enables the sending of authentication, authorization, and accounting (AAA) accounting information by the LNS.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
aaa accounting [ roaming ]
[ no ] aaa accounting
```

no

Disables this option.

roaming

Enables the sending of AAA accounting information by the LNS only for roaming subscribers.

Usage Guidelines

Use this command to enable the sending of AAA accounting information by the LNS. By default this is enabled.

Example

The following command enables the sending of AAA accounting information by the LNS:

```
aaa accounting
```

authentication

Configures the type of subscriber authentication for PPP sessions terminated at the current LNS.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

`authentication { { [ allow-noauth ] [ chap` *`chap_priority`* **`] [ mschap`** *`mschap_priority`* **`] [ pap`** *`pap_priority`* **`] } | msid-auth }`**

allow-noauth

Default: Disabled

Configures the LNS to allow PPP sessions access even though they have not been authenticated. This command issued by itself causes the LNS not to attempt authentication for any PPP sessions.

When the **allow-noauth** option is used in conjunction with commands specifying other authentication protocols and priorities to use, then if attempts to use those protocols fail, the system treats the **allow-noauth** option as the lowest priority.

If no authentication is allowed, the system constructs an Network Access Identifier (NAI) to provide accounting records for the PPP session.

chap *chap_priority*

Default: 1

Configures the LNS to attempt to use Challenge Handshake Authentication Protocol (CHAP) to authenticate the PPP session.

A *chap_priority* must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on.

chap_priority must be an integer from 1 through 1000. The lower the integer, the higher the preference. CHAP is enabled by default as the highest preference.

mschap *mschap_priority*

Default: Disabled

Configures the LNS to attempt to use the Microsoft Challenge Handshake Authentication Protocol (MSCHAP) to authenticate the PPP session.

A *mschap_priority* must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on.

mschap_priority must be an integer from 1 through 1000. The lower the integer, the higher the preference.

pap *pap_priority*

Default: 2

This option configures the LNS to attempt to use the Password Authentication Protocol (PAP) to authenticate the PPP session.

A *pap_priority* must be specified in conjunction with this option. Priorities specify which authentication protocol should be attempted first, second, third and so on.

pap_priority must be an integer from 1 through 1000. The lower the integer, the higher the preference. PAP is enabled by default as the second highest preference.

msid-auth

Default: Disabled

This option configures the LNS to attempt to authenticate the PPP session based on the Mobile Station Identity (MSID).

Usage Guidelines

Use to specify how the LNS service should handle authentication and what protocols to use. The flexibility is given to configure this option to accommodate the fact that not every mobile will implement the same authentication protocols.

By default LNS authentication options are set as follows:

- allow-noauth disabled
- chap enabled with a priority of 1
- mschap disabled
- msid-auth disabled
- pap enabled with a priority of 2

Important At least one of the keywords must be used to complete the command.

Example

The following command configures the LNS service to allow no authentication for PPP sessions and would perform accounting using the default NAI-construct of username@domain:

```
authentication allow-noauth
```

The following command configures the system to attempt authentication first using CHAP, then MSCHAP, and finally PAP. If the allow-noauth command was also issued, when all attempts to authenticate the subscriber using these protocols failed, then the subscriber would be allowed access:

```
authentication chap 1 mschap 2 pap 3
```

avp map called-number apn

This command maps an incoming Attribute Value Pair (AVP) to a GGSN Access Point Name (APN) for authentication and authorization of the call.

Product

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ default | no ] avp map called-number apn`

default

Disables mapping.

no

Disables mapping.

Usage Guidelines

For LNS calls received through a LAC, the ICRQ message includes an APN name in the Called Number AVP. This mapping function enables a GGSN system to provide RADIUS authentication/authorization via a defined APN in place of an LNS configuration. If the mapped APN has not been defined within the GGSN configuration then the call will be rejected.

Example

Enter the following command to enable mapping:

`avp map called-number apn`

Enter the following command to disable mapping:

`no avp map called-number apn`

bind

This command assigns the IP address of an interface in the current context to the LNS service.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

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

no

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

ip_address

Specifies the IP address of an interface in the current context. This must be a valid IP address entered using IPV4 dotted-decimal notation.

max-subscribers *max_value*

Default: 10000

Specifies the maximum number of subscribers that can be connected to this service at any time. *max_value* must be an integer from 1 through 2500000.

Usage Guidelines

Use this command to bind the IP address of an interface in the current context to the LNS service.

Example

The following command binds the current context interface IP address *209.165.200.234* to the current LNS service:

```
bind 209.165.200.234
```

The following command removes the binding of the IP address from the LNS service:

```
no bind
```

data sequence-number

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

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

```
[context_name]host_name(config-lns-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

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

default { authentication | data sequence-number | ip source-violation | 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 | setup-timeout| single-port-mode | subscriber| trap all tunnel-authentication}

authentication

Sets the authentication parameters for PPP sessions to the following defaults:

- allow-noauth disabled

- chap enabled with a priority of 1
- mschap disabled
- msid-auth disabled
- pap enabled with a priority of 2

data sequence-number

Enables data sequence numbering for sessions.

ip source-violation

Sets the IP source violation parameters to the following defaults:

- drop-limit 10
- period 120 seconds
- reneg-limit 5

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.

local-receive-window

Sets the window size to be used for the local side for the reliable control transport to the default of 4.

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 65535.

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.

setup-timeout

Sets the maximum time allowed for session setup to the default of 60 seconds.

single-port-mode

Disables assignment of only port 1107 for incoming tunnels and allows dynamic assignment of ports.

subscriber

Sets the name of the default subscriber configuration to use.

tunnel-authentication

Sets tunnel authentication to the default state of enabled.

trap all

Generates all supported SNMP traps.

tunnel-switching

Sets the ability of the LNS to create subsequent tunnels to the default 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 keepalive 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
```

ip source-violation

This command configures settings related to IP source-violation detection.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
ip source-violation { clear-on-valid-packet | drop-limit num | period secs
 | reneg-limit num }
no ip source-violation clear-on-valid-packet
```

clear-on-valid-packet

Default: disabled

Configures the service to reset the reneg-limit and drop-limit counters after receipt of a properly addressed packet.

drop-limit *num*

Default: 10

Sets the number of allowed source violations within a detection period before forcing a call disconnect. If *num* is not specified, the value is set to the default.

num can be an integer from 1 through 1000000.

period *secs*

Default: 120

The length of time (in seconds) for a source violation detection period to last. drop-limit and reneg-limit counters are decremented each time this value is reached.

The counters are decremented in this manner: reneg-limit counter is reduced by one (1) each time the period value is reached until the counter is zero (0); drop-limit counter is halved each time the period value is reached until the counter is zero (0). If *secs* is not specified, the value is set to the default.

secs can be an integer from 1 through 1000000.

reneg-limit *num*

Default: 5

Sets the number of allowed source violations within a detection period before forcing a PPP renegotiation. If *num* is not specified, the value is set to the default.

num can be an integer from 1 through 1000000.

Usage Guidelines

This function allows the operator to configure a network to prevent problems such as when a user gets handed back and forth between two PDSNs a number of times during a handoff scenario.

When a subscriber packet is received with a source address violation, the system increments both the IP source-violation reneg-limit and drop-limit counters and starts the timer for the IP-source violation period. Every subsequent packet received with a bad source address during the IP-source violation period causes the reneg-limit and drop-limit counters to increment.

For example, if reneg-limit is set to 5, the system allows five packets with a bad source address (source violations), but on the fifth packet, it re-negotiates PPP.

If the drop-limit is set to 10, the above process of receiving five source violations and renegotiating PPP occurs only once. After the second 5-source violation, the call is dropped. The period timer continues to count throughout this process.

If at any time before the call is dropped, the configured source-violation period is exceeded, the counters for drop-limit is decremented by half and reneg-limit is decremented by 1. See period definition above.

Example

To set the maximum number of source violations before dropping a call to 100, enter the following command:

```
ip source-violation drop-limit 100
```

keepalive-interval

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

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

keepalive-interval *seconds*
no keepalive-interval

no

Disables the generation of Hello keepalive messages on the tunnel.

seconds

Default: 60

Specifies the number of seconds to wait before sending a Hello keepalive message as an integer from 30 through 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 keepalive 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
```

local-receive-window

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

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

local-receive-window *integer*

integer

Default: 4

Specifies the number of control messages to send before waiting for an acknowledgement as an integer from 1 through 256.

Usage Guidelines

Use this command to set the size of the control message receive window being offered to the remote peer LAC. The remote peer LAC 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

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

max-retransmission *integer*

integer

Default: 5

Specifies the maximum number of retransmissions of a control message to a peer as an integer from 1 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 tunnel at any time.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

max-sessions-per-tunnel *integer*

integer

Default: 512

Specifies the maximum number of sessions 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 authentication purposes during tunnel creation.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

max-tunnel-challenge-length *bytes*

bytes

Default: 16

Specifies the number of bytes to set the maximum length of the tunnel challenge as 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 LNS service can support.

Product PDSN

GGSN

Privilege Security Administrator, Administrator

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

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

Entering the above command sequence results in the following prompt:

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

Syntax Description **max-tunnels** *integer*

integer

Default: 32000

Specifies the maximum number of tunnels as an integer from 1 through 32000.

Usage Guidelines Use this command to set the maximum number tunnels that this LNS service can support at any one time.

Example

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

```
max-tunnels 20000
```

nai-construction domain

Designates the alias domain name to use for Network Access Identifier (NAI) construction.

Product PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

`nai-construction domain` *`domain_name`* **`{ @ | % | - | \ | # | / }`**
`no nai-construction domain`

no

Deletes the NAI construction domain alias.

domain_name **{ @ | % | - |\| # | / }**

Specifies the desired domain name alias followed immediately by a separator from the valid list. *domain_name* must be an alphanumeric string of from 1 through 79 characters.

Usage Guidelines

Use this command to specify the domain alias and separator to use for NAI construction. The specified domain name must be followed by a valid separator (@ | % | - | \ | # | /).

Example

To specify a domain alias of *mydomain@* with a separator of @, enter the following command:

`nai-construction domain mydomain@`

To delete the current setting for the NAI construction domain alias, enter the following command:

`no nai-construction domain`

newcall

Configures new call related behavior.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

`newcall duplicate-subscriber-requested-address { accept | reject }`
`default newcall duplicate-subscriber-requested-address`

default

Sets or restores default value assigned for specified parameter

duplicate-subscriber-requested-address

Configures how duplicate sessions with same address request are handled.

Example

The following command configures new call with duplicate address request to accept:

```
newcall duplicate-subscriber-requested-address accept
```

peer-lac

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

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

```
peer-lac { ip_address | ip_address/mask } [ encrypted ] secret secret [
description text ]
no peer-lac ip_address
```

no peer-lac *ip_address*

Deletes the peer LAC IP address specified by *ip_address*. *ip_address* must be entered using IPv4 dotted-decimal notation.

ip_address

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

ip_address/mask

A network prefix and mask enabling communication with a group of peer LACs. *ip_address* is the network prefix expressed in IPv4 dotted-decimal notation.

mask is the number of bits that defines the prefix.

encrypted

Specifies the encrypted shared key between the LAC and the LNS service.

This keyword is intended only for use by the system while saving configuration scripts. The system displays the encrypted keyword in the configuration file as a flag that the variable following the secret keyword is the encrypted version of the plain text secret. Only the encrypted secret is saved as part of the configuration file.

secret *secret*

Designates the secret which is shared between the current LNS service and the peer LAC. *secret* must ben alphanumeric string of 1 through 127 characters that is case sensitive.

description *text*

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

Usage Guidelines

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

Specific peer LACs can be configured by specifying their individual IP addresses. In addition, to simplify configuration, communication with a group of peer LACs can be enabled by specifying a network prefix and a mask.

Example

The following command adds a peer LAC to the current LNS service with the IP address of *209.165.200.234*, and specifies the shared secret to be *1b34nnf5d*:

```
peer-lac 209.165.200.234 secret 1b34nnf5d
```

The following command enables communication with up to 16 peer LACs on the 192.168.1.0 network each having a secret of *abc123*:

```
peer-lac 209.165.200.224/27 secret abc123
```

The following command removes the peer LAC with the IP address of *209.165.200.244* for the current LNS service:

```
no peer-lac 209.165.200.244
```

proxy-lcp-authentication

Enables/disables proxy LCP authentication.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] proxy-lcp-authentication`

no

Disables the processing of proxy LCP authentication parameters from the LAC.

proxy-lcp-authentication

Default: Enabled

Enables the processing proxy LCP authentication parameters from the LAC.

Usage Guidelines

When enabled, if proxy LCP authentication parameters are received from the LAC and are acceptable, the LNS resumes the PPP session from the authentication phase and goes to the IPCP phase.

When disabled, PPP is always started from the LCP phase, ignoring and discarding any proxy LCP authentication parameters received from the LAC. Disable this feature in situations where accept proxy LCP Auth AVPs that the peer LAC sends should not be expected.

Example

Use the following command to disable the processing of proxy LCP authentication parameters from the LAC:

`no proxy-lcp-authentication`

Use the following command to re-enable the processing of proxy LCP authentication parameters from the LAC:

`proxy-lcp-authentication`

retransmission-timeout-first

Configures the initial timeout for the retransmission of control messages to the peer LAC.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

`retransmission-timeout-first` *`integer`*

integer

Default: 1

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

Usage Guidelines

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.

Example

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

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

retransmission-timeout-max

Configures the maximum amount of time that can elapse before retransmitting control messages to the peer LAC.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

retransmission-timeout-max *integer*

integer

Default: 8

Specifies the maximum time (in seconds) to wait before retransmitting control messages. If this limit is reached, the tunnel, and all sessions within it, is cleared. This value is an integer from 1 through 100.

Usage Guidelines

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. 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. This continues until the limit set by this command is reached. If this limit is reached, the tunnel, and all sessions within it, is cleared.

Example

Use the following command to set the maximum retransmission time-out to *10* seconds:

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

setup-timeout

Configures the maximum amount of time, in seconds, allowed for session setup.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

setup-timeout *seconds*

seconds

Default: 60

Specifies the maximum time (in seconds) to wait for the setup of a session. *seconds* must be an integer from 1 through 1000000.

Usage Guidelines

This command controls the amount of time allowed for tunnel establishment with a peer LAC. If this timer is exceeded the tunnel setup is aborted.

Example

The following command configures a maximum setup time of *120* seconds:

```
setup-timeout 120
```

single-port-mode

When enabled, this command sets the LNS to use only the default local UDP port (port 1701) for the life of a tunnel.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[default | no] single-port-mode

no

Disable single port mode

Usage Guidelines

Use this command to control the L2TP LNS tunnel local UDP port assignment mode. If single-port-mode is enabled, the LNS-service uses the standard UDP port (port 1701) for the life of the incoming tunnel. Otherwise, it assigns a new local UDP port number for a tunnel when it responds to a tunnel create request received on the standard port number. This is done for load distributing the tunnel processing between multiple tasks within the system to increase the capacity and performance. Even though all L2TP LACs are required to support such dynamic port assignments during tunnel establishments, there exist some LACs that do not support port assignment other than port 1701. This single-port-mode feature can be enabled to support such LAC peers. This configuration must be applied for the LNS-Service before the **bind** command is executed.

Example

The following command enables single port mode for the current LNS service:

single-port-mode

trap

This command generates SNMP traps.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

[no] trap all

no

Disables SNMP traps.

Usage Guidelines

Use this command to enable/disable all supported SNMP traps.

Example

To enable all supported SNMP traps, enter the following command;

```
trap all
```

tunnel-authentication

Enables/disables L2TP tunnel authentication for the LNS service.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

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

no

Disables tunnel authentication

Tunnel authentication is enabled by default.

Usage Guidelines

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

Example

To disable tunnel authentication, use the following command:

```
no tunnel-authentication
```

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

```
tunnel-authentication
```

tunnel-switching

Enables or disables the LNS service from creating tunnels to another LAC for an existing tunnel.

Product

PDSN

GGSN

Privilege

Security Administrator, Administrator

Command Modes

Exec > Global Configuration > Context Configuration > LNS Service Configuration

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

Entering the above command sequence results in the following prompt:

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

Syntax Description

`[ no ] tunnel-switching`

`no`

Disable tunnel switching.

Tunnel switching is enabled by default.

Usage Guidelines

Tunnel switching is when the LNS has a tunnel connected to a LAC and creates a tunnel to a different LAC and routes the data from the original LAC through the new tunnel to the other LAC.

Example

To disable tunnel switching in the LNS, enter the following command;

`no tunnel-switching`