L2TP Network Server

This chapter describes the support for Layer 2 Tunneling Protocol (L2TP) Network Server (LNS) functionality 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 Layer 2 Tunneling Protocol (L2TP) Network Server (LNS) 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, LNS functionality is configured as context-level services on the system. LNS services support the termination of L2TP encapsulated tunnels from L2TP Access Concentrators (LACs) in accordance with RFC 2661.

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.

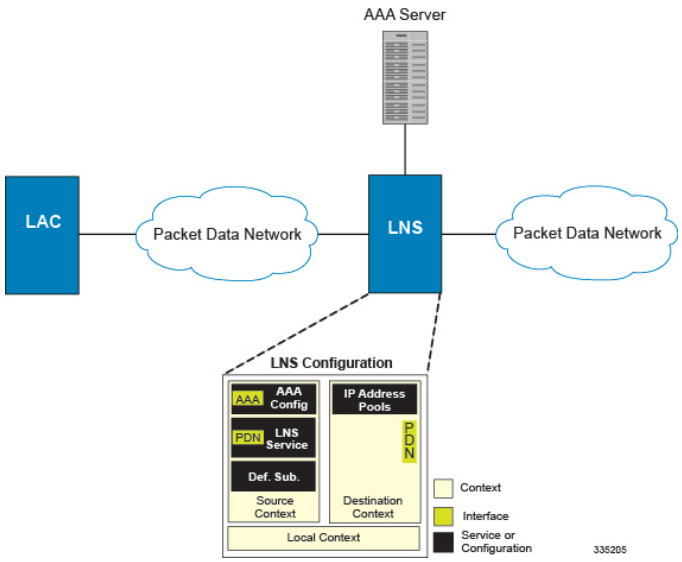
Important The LNS service uses UDP ports 13660 through 13668 as the source port for receiving packets from the LAC. You can force the LNS to only use the standard L2TP port (UDP Port 1701) with the **single-port-mode** LNS service configuration mode command. Refer to the *Command Line Interface Reference* for more information on this command.

LNS Service Operation

As mentioned previously, LNS functionality on the system is configured via context-level services. LNS services can be configured in the same context as other services supported on the system or in its own context. Each context can support multiple LNS services.

One of the most simple configuration that can be implemented on the system to support Simple IP data applications requires that two contexts (one source and one destination) be configured on the system as shown in the following figure.

Figure 1: LNS Configuration Example



The source context facilitates the LNS service(s) and the PDN and AAA interfaces. The PDN interface is bound to the LNS service and connects L2TP tunnels and sessions from one or more peer LACs. The source context is also be configured to provide AAA functionality for subscriber sessions. The destination context facilitates the packet data network interface(s) and can optionally be configured with pools of IP addresses for assignment to subscriber sessions.

In this configuration, the LNS service in the source context terminates L2TP tunnels from peer LACs and routes the subscriber session data through the destination context to and from a packet data network such as the Internet or a home network.

Information Required

Prior to configuring the system as shown in figure above, a minimum amount of information is required. The following sections describe the information required to configure the source and destination contexts.

Source Context Configuration

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

Table 1: Required Information for Source Context Configuration

Required Information	Description
Source context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the source context will be recognized by the system.
PDN Interface Configuration	
PDN interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. These PDN interfaces facilitates the L2TP tunnels/sessions from the LAC and are configured in the source context.
IP address and subnet	These will be assigned to the PDN interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	This specifies the physical port to which the interface will be bound. Ports are identified by the chassis slot number where the line card resides in, followed by the number of the physical connector on the line card. For example, port 17/1 identifies connector number 1 on the card in slot 17. A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical PDN interfaces.
Gateway IP address	Used when configuring static routes from the PDN interface(s) to a specific network.
LNS service Configuration	

Required Information	Description
LNS service name	This is an identification string between 1 and 63 characters (alpha and/or numeric) by which the LNS service will be recognized by the system. Multiple names are needed if multiple LNS services will be used. LNS services are configured in the source context.
Authentication protocols used	Specifies how the system handles authentication: using a protocol (such as CHAP, PAP, or MSCHAP), or not requiring any authentication.
Domain alias for NAI-construction	Specifies a context name for the system to use to provide accounting functionality for a subscriber session. This parameter is needed only if the system is configured to support no authentication.
Maximum number of sessions per tunnel	This defines the maximum number of sessions supported by each tunnel facilitated by the LNS service. The number can be configured to any integer value from 1 to 65535. The default is 65535.
Maximum number of tunnels	This defines the maximum number of tunnels supported by the LNS service. The number can be configured to any integer value from 1 to 32000. The default is 32000.
Peer LAC	IP address or network prefix and mask: The IP address of a specific peer LAC for which the LNS service terminates L2TP tunnels. The IP address must be expressed in dotted decimal notation. Multiple peer LACs can be configured. Alternately, to simplify configuration, a group of peer LACs can be specified by entering a network prefix and a mask.
	Secret: The shared secret used by the LNS to authenticate the peer LAC. The secret can be from 1 to 256 alpha and/or numeric characters and is case sensitive.
AAA Interface Configuration	

Required Information	Description
AAA interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. AAA interfaces will be configured in the source context.
IP address and subnet	These will be assigned to the AAA interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	A single physical port can facilitate multiple interfaces.
Physical port description	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions are needed if multiple ports will be used. Physical ports are configured within the source context and are used to bind logical AAA interfaces.
Gateway IP address	Used when configuring static routes from the AAA interface(s) to a specific network.
RADIUS Server Configuration	

Required Information	Description
RADIUS Authentication server	IP Address: Specifies the IP address of the RADIUS authentication server the source context will communicate with to provide subscriber authentication functions. Multiple addresses are needed if multiple RADIUS servers will be configured. RADIUS authentication servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS authentication server and the source context. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the RADIUS authentication server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1812.

Required Information	Description
RADIUS Accounting server	IP Address: Specifies the IP address of the RADIUS accounting server that the source context will communicate with to provide subscriber accounting functions. Multiple addresses are needed if multiple RADIUS servers will be configured. RADIUS accounting servers are configured within the source context. Multiple servers can be configured and each assigned a priority.
	Shared Secret: The shared secret is a string between 1 and 15 characters (alpha and/or numeric) that specifies the key that is exchanged between the RADIUS accounting server and the source context. A shared secret is needed for each configured RADIUS server.
	UDP Port Number: Specifies the port used by the source context and the RADIUS Accounting server for communications. The UDP port number can be any integer value between 1 and 65535. The default value is 1813.
RADIUS attribute NAS Identifier	Specifies the name by which the source context will be identified in the Access-Request message(s) it sends to the RADIUS server. The name must be between 1 and 32 alpha and/or numeric characters and is case sensitive.
RADIUS NAS IP address	Specifies the IP address of the source context's AAA interface. A secondary IP address interface can optionally be configured.
Default Subscriber Configuration	
"Default" subscriber's IP context name	Specifies the name of the egress context on the system that facilitates the PDN ports. **Important** For this configuration, the IP context name should be identical to the name of the destination context.

Destination Context Configuration

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

Table 2: Required Information for Destination Context Configuration

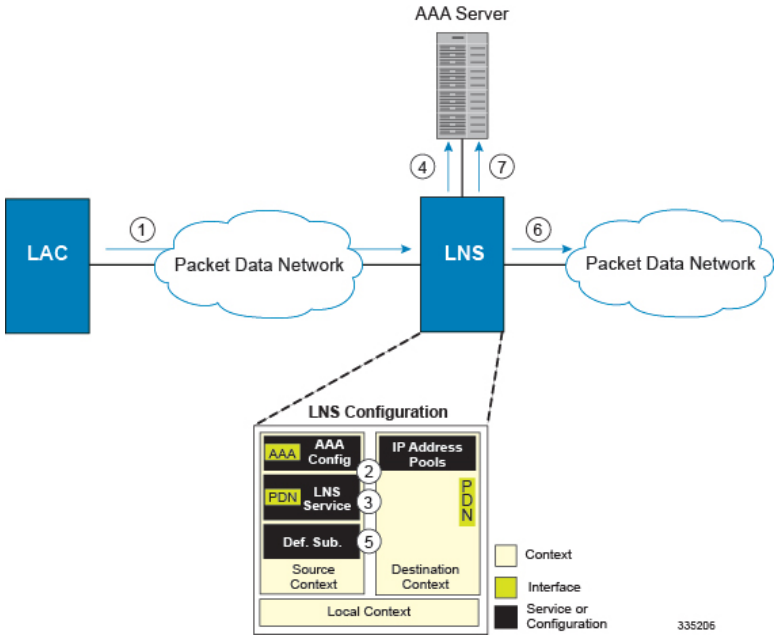
Required Information	Description
Destination context name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the destination context will be recognized by the system. **Important** For this configuration, the destination context name should **not** match the domain name of a specific domain.
PDN Interface Configuration	
PDN interface name	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the interface will be recognized by the system. Multiple names are needed if multiple interfaces will be configured. PDN interfaces are used to connect to a packet network and are configured in the destination context.
IP address and subnet	These will be assigned to the PDN interface. Multiple addresses and/or subnets are needed if multiple interfaces will be configured.
Physical port number	A single physical port can facilitate multiple interfaces.
Physical port description(s)	This is an identification string between 1 and 79 characters (alpha and/or numeric) by which the physical port will be recognized by the system. Multiple descriptions will be needed if multiple ports will be used. Physical ports are configured within the destination context and are used to bind logical PDN interfaces.
Gateway IP address(es)	Used when configuring static routes from the PDN interface(s) to a specific network.
IP Address Pool Configuration (optional)	
IP address pool name(s)	If IP address pools will be configured in the destination context(s), names or identifiers will be needed for them. The pool name can be between 1 and 31 alpha and/or numeric characters and is case sensitive.

Required Information	Description
IP pool addresses	An initial address and a subnet, or a starting address and an ending address, are required for each configured pool. The pool will then consist of every possible address within the subnet, or all addresses from the starting address to the ending address. The pool can be configured as public, private, or static.

How This Configuration Works

The following figure and the text that follows describe how this LNS service configuration with a single source and destination context would be used by the system to terminate an L2TP tunnel.

Figure 2: Call Processing Using a Single Source and Destination Context



1. An L2TP tunnel request from a peer LAC is received by the LNS service. The tunnel is to facilitate a subscriber session.
2. The LAC and LNS establish the L2TP tunnel according to the procedures defined in RFC 2661.

   Once the L2TP tunnel is established, subscriber L2TP sessions can be established.
3. The LNS service determines which context to use in providing AAA functionality for the subscriber session if authentication is enabled for the LNS service. For more information on this process, refer How the System Selects Contexts in System Administration Guide.

   For this example, the result of this process is that LNS service determined that AAA functionality should be provided by the Source context.
4. The system communicates with the AAA server specified in the Source context's AAA configuration to authenticate the subscriber.

5. Upon successful authentication, the LNS service terminates the subscriber's PPP datagrams from the L2TP session and the system determines which egress context to use for the subscriber session. For more information on egress context selection process, refer How the System Selects Contexts in System Administration Guide.

   The system determines that the egress context is the destination context based on the configuration of either the Default subscriber's ip-context name or from the SN-VPN-NAME or SN1-VPN-NAME attributes that is configured in the subscriber's RADIUS profile.

6. Data traffic for the subscriber session is routed through the PDN interface in the Destination context.
7. Accounting information for the session is sent to the AAA server over the AAA interface.

Configuring the System to Support LNS Functionality

Many of the procedures required to configure the system to support LNS functionality are provided in the System Administration Guide. The System Administration Guide provides information and procedures for configuring contexts, interfaces and ports, AAA functionality, and IP address pools on the system.

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

Important This section provides the minimum instruction set for configuring an LNS service allowing the system to terminate L2TP tunnels and process data sessions. For more information on commands that configure additional LNS service properties, refer LNS Configuration Mode Commands chapter in *Command Line Interface Reference*.

To configure the system to provide access control list facility to subscribers:

Step 1 Create the LNS service and bind it to an interface IP address by applying the example configuration in the *Creating and Binding LNS Service* section.

Step 2 Specify the authentication parameters for LNS service by applying the example configuration in the *Configuring Authentication Parameters for LNS Service* section.

Step 3 Configure the maximum number of tunnels supported by the LNS service and maximum number of sessions supported per tunnel by applying the example configuration in the *Configuring Tunnel and Session Parameters for LNS Service* section.

Step 4 Configure peer LACs for the LNS service by applying the example configuration in the *Configuring Tunnel and Session Parameters for LNS Service* section.

Step 5 *Optional*. Specify the domain alias designated for the context which the LNS service uses for AAA functionality by applying the example configuration in the *Configuring Domain Alias for AAA Subscribers* section.

Step 6 Verify your LNS service configuration by following the steps in the *Verifying the LNS Service Configuration* section.

Step 7 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*.

Creating and Binding LNS Service

Use the following example to create the LNS service and bind the IP address to it:

```
configure
    context <dest_ctxt_name> -noconfirm
        lns-service <lns_svc_name> -noconfirm
            bind address <ip_address> [ max-subscribers <max_subscriber> ]
            end
```

Notes:

- LNS service has to be configured in destination context.
- Bind address is the interface address that is to serve as an L2TP PDN interface.
- Multiple addresses on the same IP interface can be bound to different LNS services. However, each address can be bound to only one LNS service. In addition, the LNS service can not be bound to the same interface as other services such as a LAC service.

Configuring Authentication Parameters for LNS Service

Use the following example to authentication parameters for LNS service:

```
configure
    context <dest_ctxt_name>
        lns-service <lns_svc_name>
            authentication { { [ allow-noauth | chap <pref> | mschap <pref>
 | | pap <pref> ] } | msid-auth }
            end
```

Note:

- For more information on authentication procedure and priorities, refer **authentication** command section in LNS Configuration Mode Commands chapter of the *Command Line Interface Reference*.

Configuring Tunnel and Session Parameters for LNS Service

Use the following example to configure the tunnel and session parameters for LNS service:

```
configure
    context <dest_ctxt_name>
        lns-service <lns_svc_name>
            max-tunnel <max_tunnels>
            max-session-per-tunnel <max_sessions>
            end
```

Note:

- For more information on tunnel and session related parameters, refer LNS Configuration Mode Commands chapter of the *Command Line Interface Reference*.

Configuring Peer LAC servers for LNS Service

Use the following example to configure the peer LAC servers for LNS service:

```
configure
    context <dest_ctxt_name>
        lns-service <lns_svc_name>
            peer-lac { <lac_ip_address> | <ip_address>/<mask> } [ encrypted ] secret
 <secret_string> [ description <desc_text> ]
            end
```

Note:

- Multiple LACs can be configured with this command. For more information, refer LNS Configuration Mode Commands chapter of the *Command Line Interface Reference*.

Configuring Domain Alias for AAA Subscribers

Use the following example to create the LNS service and bind the IP address to it:

```
configure
    context <dest_ctxt_name> -noconfirm
        lns-service <lns_svc_name> -noconfirm
            nai-construct domain <domain_alias>
            end
```

Notes:

- If this command is enabled, an NAI is constructed for the subscriber in the event that their mobile node does not negotiate CHAP, PAP, or MSCHAP.
- If this option is selected, no further attempts are made to authenticate the user. Instead, the constructed NAI is used for accounting purposes.

Important This command should only be used if the LNS service is configured to allow "no authentication" using the **authentication allow-noauth** command.

Verifying the LNS Service Configuration

These instructions are used to verify the LNS service configuration.

Verify that your LNS service configuration by entering the following command in Exec Mode:

show lns-service name *service_name*

The output of this command displays the configuration of the LNS service and should appear similar to that shown below.

```
Service name: testlns
    Context:                                        test
    Bind:                                               Not Done
    Local IP Address:                       0.0.0.0
    First Retransmission Timeout:    1 (secs)
```

```
Max Retransmission Timeout:        8 (secs)
Max Retransmissions:                    5
Setup Timeout:                                60 (secs)
Max Sessions:                                   500000                Max Tunnels:
        32000
Max Sessions Per Tunnel:             65535
Keep-alive Interval:                    60                        Control Receive Window: 16
Data Sequence Numbers:                Enabled
Tunnel Authentication:                Enabled
Tunnel Switching:                           Enabled
Max Tunnel Challenge Length:     16
PPP Authentication:                      CHAP 1 PAP 2
Allow Noauthentication:               Disabled            MSID Authentication:        Disabled
No NAI Construct Domain defined
No Default Subscriber defined
IP Src Violation Reneg Limit:    5
IP Src Violation Drop Limit:     10
IP Src Violation Period:             120 (secs)
Service Status:                             Not started
Newcall Policy:                             None
```

L2TP Network Server