H3C LA 系列无线网关

二层技术-广域网接入配置指导(V7)

新华三技术有限公司
http://www.h3c.com

资料版本：6W101-20180328

前 言

H3C LA 系列无线网关 配置指导(V7)介绍了 LA 系列无线网关各软件特性的原理及其配置方法，包含原理简介、配置任务描述和配置举例。《二层技术-广域网接入配置指导》主要介绍广域网协议的原理及配置，包括 L2TP、4G Modem 等。

前言部分包含如下内容：

读者对象

本手册主要适用于如下工程师：

- 网络规划人员
- 现场技术支持与维护人员
- 负责网络配置和维护的网络管理员

本书约定

1. 命令行格式约定

格　式	意　义
粗体	命令行关键字（命令中保持不变、必须照输的部分）采用**加粗**字体表示。
斜体	命令行参数（命令中必须由实际值进行替代的部分）采用*斜体*表示。
[ ]	表示用“[ ]”括起来的部分在命令配置时是可选的。
{ x | y | ... }	表示从多个选项中仅选取一个。
[x | y | ...]	表示从多个选项中选取一个或者不选。
{ x | y | ... } *	表示从多个选项中至少选取一个。
[x | y | ...] *	表示从多个选项中选取一个、多个或者不选。
&<1-n>	表示符号&前面的参数可以重复输入1～n次。
#	由“#”号开始的行表示为注释行。

2. 图形界面格式约定

格　式	意　义
< >	带尖括号“< >”表示按钮名，如“单击<确定>按钮”。
[ ]	带方括号“[ ]”表示窗口名、菜单名和数据表，如“弹出[新建用户]窗口”。
/	多级菜单用“/”隔开。如[文件/新建/文件夹]多级菜单表示[文件]菜单下的[新建]子菜单下

格　式	意　义
	的[文件夹]菜单项。

3. 各类标志

本书还采用各种醒目标志来表示在操作过程中应该特别注意的地方，这些标志的意义如下：

 警告	该标志后的注释需给予格外关注，不当的操作可能会对人身造成伤害。
 注意	提醒操作中应注意的事项，不当的操作可能会导致数据丢失或者设备损坏。
 提示	为确保设备配置成功或者正常工作而需要特别关注的操作或信息。
 说明	对操作内容的描述进行必要的补充和说明。
 窍门	配置、操作、或使用设备的技巧、小窍门。

4. 图标约定

本书使用的图标及其含义如下：

	该图标及其相关描述文字代表一般网络设备，如路由器、交换机、防火墙等。
	该图标及其相关描述文字代表一般意义下的路由器，以及其他运行了路由协议的设备。
	该图标及其相关描述文字代表二、三层以太网交换机，以及运行了二层协议的设备。
	该图标及其相关描述文字代表无线控制器、无线控制器业务板和有线无线一体化交换机的无线控制引擎设备。
	该图标及其相关描述文字代表无线接入点设备。
	该图标及其相关描述文字代表无线终结单元。
	该图标及其相关描述文字代表无线终结者。
	该图标及其相关描述文字代表无线Mesh设备。
	该图标代表发散的无线射频信号。
	该图标代表点到点的无线射频信号。
	该图标及其相关描述文字代表防火墙、UTM、多业务安全网关、负载均衡等安全设备。

	该图标及其相关描述文字代表防火墙插卡、负载均衡插卡、NetStream插卡、SSL VPN插卡、IPS插卡、ACG插卡等安全插卡。

5. 示例约定

由于设备型号不同、配置不同、版本升级等原因，可能造成本手册中的内容与用户使用的设备显示信息不一致。实际使用中请以设备显示的内容为准。

本手册中出现的端口编号仅作示例，并不代表设备上实际具有此编号的端口，实际使用中请以设备上存在的端口编号为准。

资料意见反馈

如果您在使用过程中发现产品资料的任何问题，可以通过以下方式反馈：

E-mail：info@h3c.com

感谢您的反馈，让我们做得更好！

目 录

1 L2TP

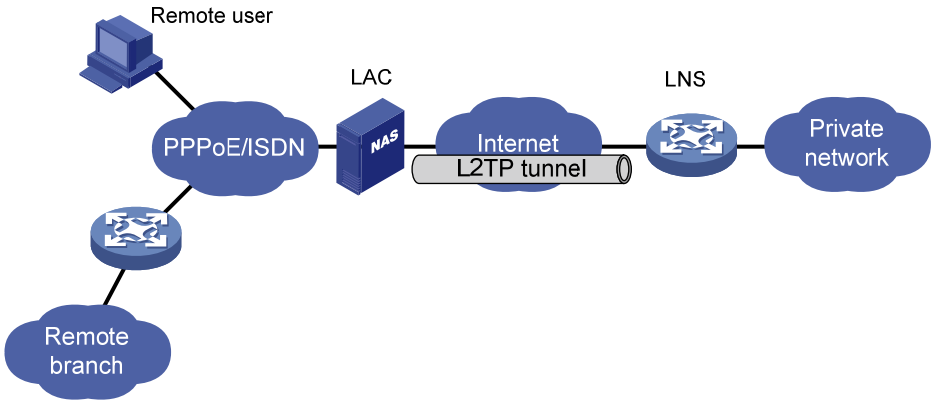
1.1 L2TP简介

L2TP（Layer 2 Tunneling Protocol，二层隧道协议）是目前使用最为广泛的 VPDN（Virtual Private Dial-up Network，虚拟专用拨号网络）隧道协议。L2TP 通过在公共网络（如 Internet）上建立点到点的 L2TP 隧道，将 PPP（Point-to-Point Protocol，点对点协议）数据帧封装后通过 L2TP 隧道传输，使得远端用户（如企业驻外机构和出差人员）利用 PPP 接入公共网络后，能够通过 L2TP 隧道与企业内部网络通信，访问企业内部网络资源。

L2TP 是一种二层 VPN（Virtual Private Network，虚拟专用网络）技术，为远端用户接入私有的企业网络提供了一种安全、经济且有效的方式。

1.1.1 L2TP典型组网

图1-1 L2TP 典型组网



如 图 1-1 所示，L2TP的典型组网中包括以下三个部分：

- 远端系统

远端系统是要接入企业内部网络的远端用户和远端分支机构，通常是一个拨号用户的主机或私有网络中的一台设备。

- LAC（L2TP Access Concentrator，L2TP 访问集中器）

LAC 是具有 PPP 和 L2TP 协议处理能力的设备，通常是一个当地 ISP 的 NAS（Network Access Server，网络接入服务器），主要用于为 PPP 类型的用户提供接入服务。

LAC 作为 L2TP 隧道的端点，位于 LNS 和远端系统之间，用于在 LNS 和远端系统之间传递报文。它把从远端系统收到的报文按照 L2TP 协议进行封装并送往 LNS，同时也将从 LNS 收到的报文进行解封装并送往远端系统。

- LNS（L2TP Network Server，L2TP 网络服务器）

LNS 是具有 PPP 和 L2TP 协议处理能力的设备，通常位于企业内部网络的边缘。

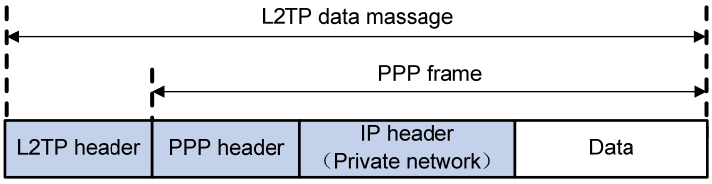
LNS 作为 L2TP 隧道的另一侧端点，是 LAC 通过隧道传输的 PPP 会话的逻辑终点。L2TP 通过在公共网络中建立 L2TP 隧道，将远端系统的 PPP 连接由原来的 NAS 延伸到了企业内部网络的 LNS 设备。

1.1.2 L2TP消息类型及封装结构

L2TP 协议定义了两种消息：

- 控制消息：用于 L2TP 隧道和 L2TP 会话的建立、维护和拆除。控制消息的传输是可靠的，并且支持流量控制和拥塞控制。
- 数据消息：用于封装PPP帧，其格式如 图 1-2 所示。数据消息的传输是不可靠的，若数据消息丢失，不予重传。数据消息支持流量控制，即支持对乱序的数据消息进行排序。

图1-2 L2TP 数据消息格式



如 图 1-3 所示，L2TP控制消息和L2TP数据消息均封装在UDP报文中。

图1-3 L2TP 消息封装结构图

1.1.3 L2TP隧道和会话

L2TP 隧道是 LAC 和 LNS 之间的一条虚拟点到点连接。控制消息和数据消息都在 L2TP 隧道上传输。在同一对 LAC 和 LNS 之间可以建立多条 L2TP 隧道。每条隧道可以承载一个或多个 L2TP 会话。

L2TP 会话复用在 L2TP 隧道之上，每个 L2TP 会话对应于一个 PPP 会话。当远端系统和 LNS 之间建立 PPP 会话时，LAC 和 LNS 之间将建立与其对应的 L2TP 会话。属于该 PPP 会话的数据帧通过该 L2TP 会话所在的 L2TP 隧道传输。

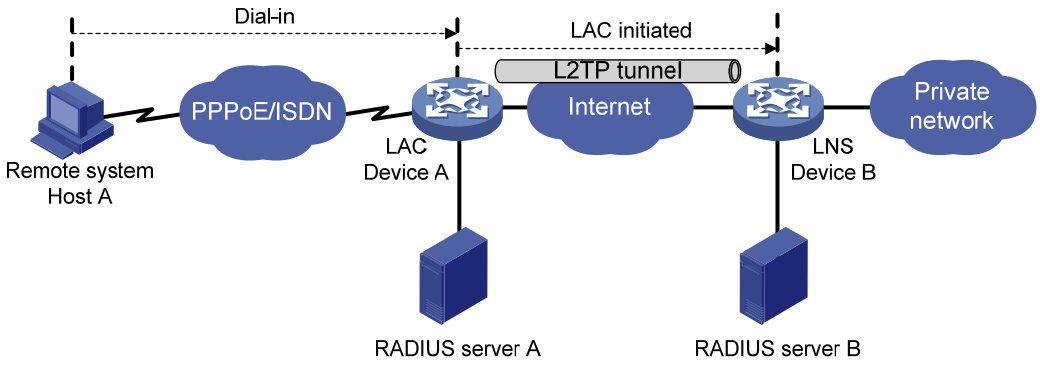
1.1.4 L2TP隧道模式及隧道建立过程

L2TP 隧道包括 NAS-Initiated、Client-Initiated 和 LAC-Auto-Initiated 三种模式。

1. NAS-Initiated模式

如 图 1-4 所示，NAS-Initiated模式L2TP隧道的建立由LAC（即NAS）发起。远端系统的拨号用户通过PPPoE/ISDN拨入LAC后，由LAC向LNS发起建立L2TP隧道的请求。

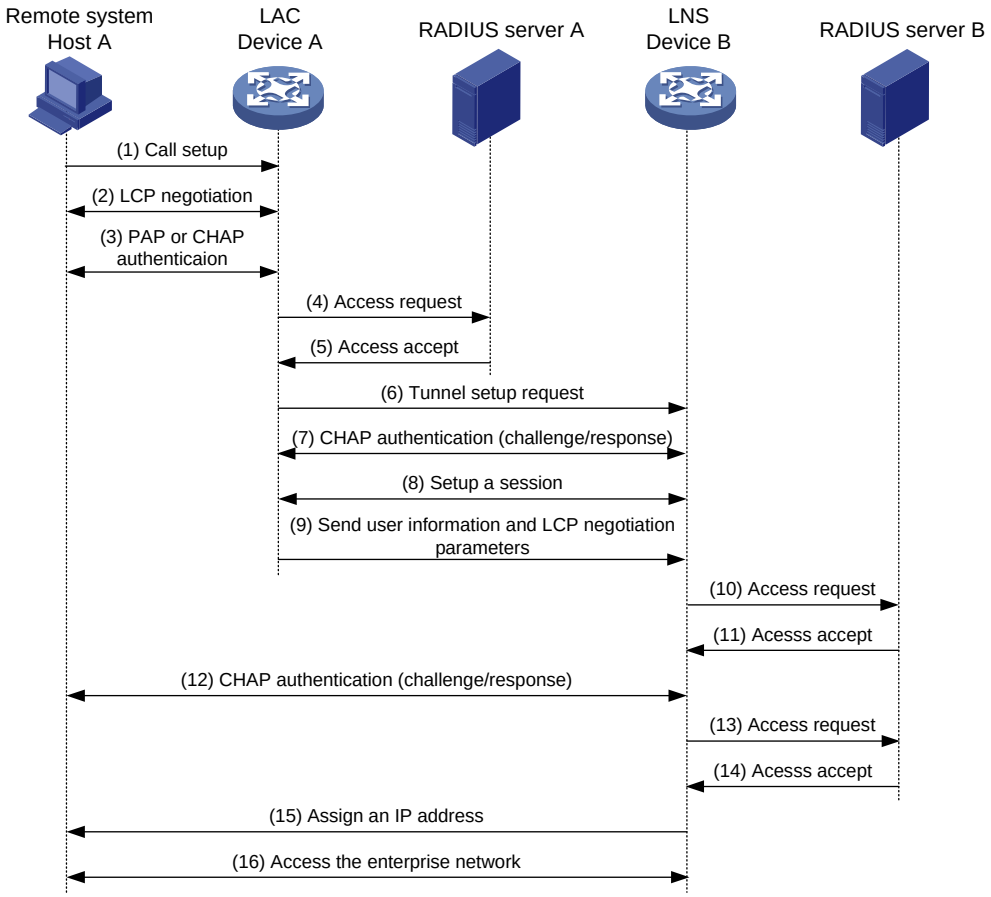
图1-4 NAS-Initiated 模式 L2TP 隧道示意图



NAS-Initiated 模式 L2TP 隧道具有如下特点：

- 远端系统只需支持 PPP 协议，不需要支持 L2TP。
- 对远端拨号用户的身份认证与计费既可由 LAC 代理完成，也可由 LNS 完成。

图1-5 NAS-Initiated 模式 L2TP 隧道的建立流程



如 图 1-5 所示，NAS-Initiated模式L2TP隧道的建立过程为：

(1) 远端系统 Host A 发起呼叫，请求建立连接。

(2) Host A 和 LAC（Device A）进行 PPP LCP 协商。

(3) LAC 对 Host A 提供的 PPP 用户信息进行 PAP 或 CHAP 认证。

(4) LAC 将认证信息（用户名、密码）发送给 RADIUS 服务器进行认证。

(5) RADIUS 服务器认证该用户，并返回认证结果。

(6) 如果认证通过，且根据用户名或用户所属 ISP 域判断该用户为 L2TP 用户，则 LAC 向 LNS（Device B）发起 L2TP 隧道建立请求。

(7) 在需要对隧道进行认证的情况下，LAC 和 LNS 分别发送 CHAP challenge 信息，以验证对方身份。隧道验证通过后，LAC 和 LNS 之间成功建立了 L2TP 隧道。

(8) LAC 和 LNS 在 L2TP 隧道上协商建立 L2TP 会话。

(9) LAC 将 PPP 用户信息和 PPP 协商参数等传送给 LNS。

(10) LNS 将认证信息发送给 RADIUS 服务器进行认证。

(11) RADIUS 服务器认证该用户，并返回认证结果。

(12) 认证通过后，若 LNS 上配置了强制 CHAP 验证，则 LNS 对 PPP 用户进行认证，发送 CHAP challenge，PPP 用户回应 CHAP response。

(13) LNS 再次将认证信息发送给 RADIUS 服务器。

(14) RADIUS 服务器认证该用户，并返回认证结果。

(15) 认证通过后，LNS 为 Host A 分配一个企业网内部的 IP 地址。

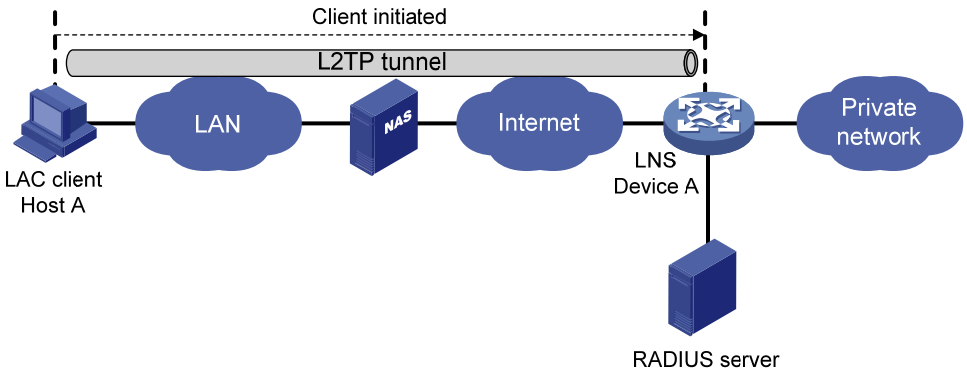
(16) 获得 IP 地址后，PPP 用户可以通过 Host A 访问企业内部资源。

在步骤(12)、(15)和(16)中，LAC 负责在 Host A 和 LNS 之间转发报文。Host A 和 LAC 之间交互的是 PPP 数据帧，LAC 和 LNS 之间交互的是 L2TP 数据报文。

2. Client-Initiated模式

如 图 1-6 所示，Client-Initiated模式L2TP隧道的建立直接由LAC client（指本地支持L2TP协议的远端系统）发起。LAC client具有公网地址，并能够通过Internet与LNS通信后，如果在LAC client上触发L2TP拨号，则LAC client直接向LNS发起L2TP隧道建立请求，无需经过LAC设备建立隧道。

图1-6 Client-Initiated 模式 L2TP 隧道示意图

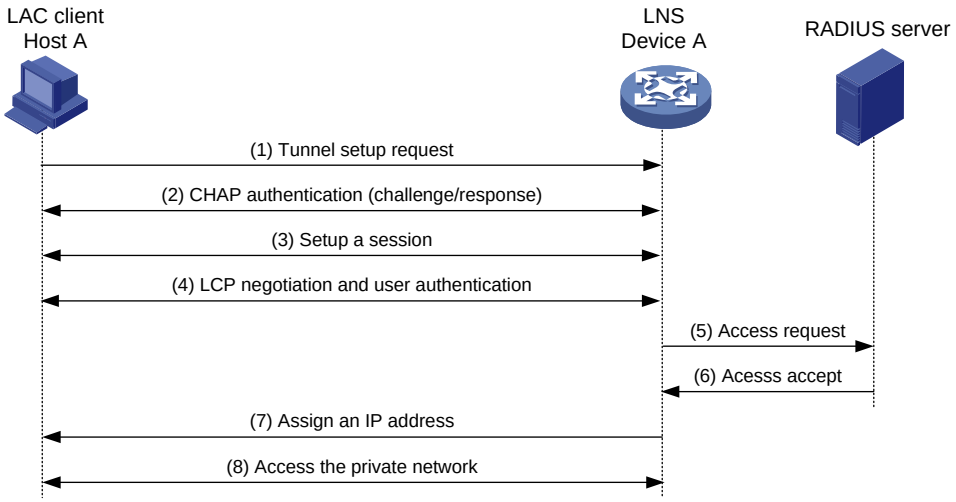


Client-Initiated 模式 L2TP 隧道具有如下特点：

- L2TP 隧道在远端系统和 LNS 之间建立，具有较高的安全性。
- Client-Initiated 模式 L2TP 隧道对远端系统要求较高（远端系统必须是支持 L2TP 协议的 LAC client，且能够与 LNS 通信），因此它的扩展性较差。

如 图 1-7 所示，Client-Initiated模式L2TP隧道的建立过程与NAS-Initiated模式类似，此处不再赘述。

图1-7 Client-Initiated 模式 L2TP 隧道的建立流程

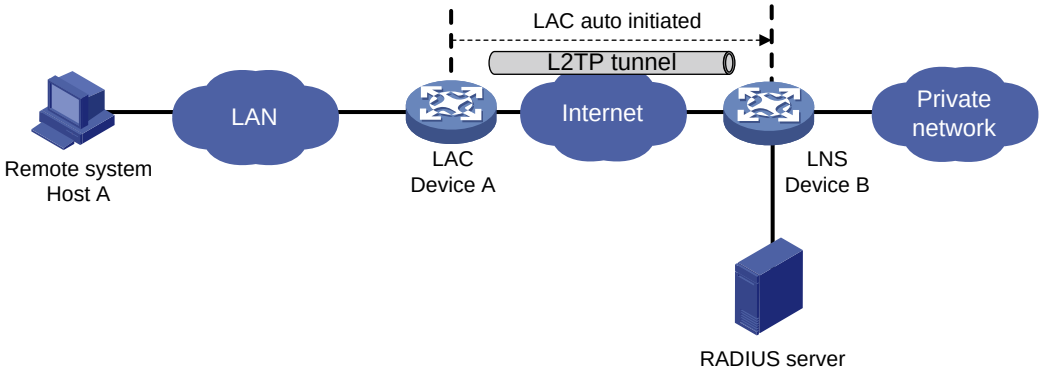


3. LAC-Auto-Initiated模式

采用 NAS-Initiated 方式建立 L2TP 隧道时，要求远端系统必须通过 PPPoE/ISDN 等拨号方式拨入 LAC，且只有远端系统拨入 LAC 后，才能触发 LAC 向 LNS 发起建立隧道的请求。

如 图 1-8 所示，在LAC-Auto-Initiated模式下，不需要远端系统拨号触发，在LAC上通过执行**l2tp-auto-client**命令即可触发LAC建立L2TP隧道。远端系统访问LNS连接的内部网络时，LAC将通过L2TP隧道转发这些访问数据。

图1-8 LAC-Auto-Initiated 模式 L2TP 隧道示意图

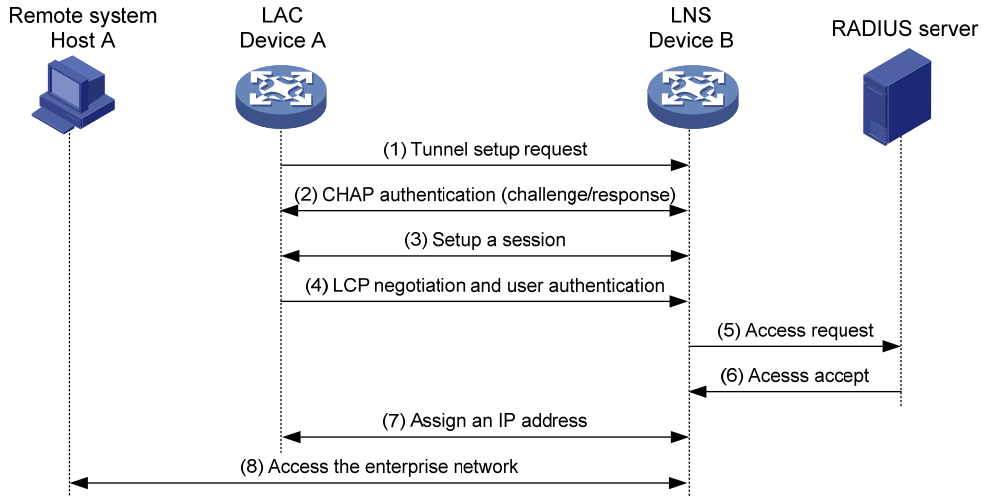


LAC-Auto-Initiated 模式 L2TP 隧道具有如下特点：

- 远端系统和 LAC 之间可以是任何基于 IP 的连接，不局限于拨号连接。
- 不需要远端系统上的拨号接入来触发建立 L2TP 隧道。
- L2TP 隧道创建成功后立即建立 L2TP 会话，然后在 LAC 和 LNS 之间进行 PPP 协商，LAC 和 LNS 分别作为 PPP 客户端和 PPP 服务器端。
- 一条 L2TP 隧道上只承载一个 L2TP 会话。
- LNS 为 LAC 分配企业网内部的 IP 地址，而不是为远端系统分配。

如 图 1-9 所示，LAC-Auto-Initiated模式L2TP隧道的建立过程与NAS-Initiated模式类似，此处不再赘述。

图1-9 LAC-Auto-Initiated 模式 L2TP 隧道的建立流程



1.1.5 L2TP协议的特点

1. 灵活的身份验证机制以及高度的安全性

L2TP 协议本身并不提供连接的安全性，但它可依赖于 PPP 提供的认证（比如 CHAP、PAP 等），因此具有 PPP 所具有的所有安全特性。

L2TP 还可以与 IPsec 结合起来实现数据安全，使得通过 L2TP 所传输的数据更难被攻击。

2. 多协议传输

L2TP 传输 PPP 数据包，在 PPP 数据包内可以封装多种协议。

3. 支持RADIUS服务器的认证

LAC 和 LNS 可以将用户名和密码发往 RADIUS 服务器，由 RADIUS 服务器对用户身份进行认证。

4. 支持内部地址分配

LNS 可以对远端系统的地址进行动态的分配和管理，可支持私有地址应用（RFC 1918）。为远端系统分配企业内部的私有地址，可以方便地址的管理并增加安全性。

5. 网络计费的灵活性

可在 LAC 和 LNS 两处同时计费，即 ISP 处（用于产生帐单）及企业网关（用于付费及审计）。L2TP 能够提供数据传输的出/入包数、字节数以及连接的起始、结束时间等计费数据，AAA 服务器可根据这些数据方便地进行网络计费。

6. 可靠性

L2TP 协议支持备份 LNS，当主 LNS 不可达之后，LAC 可以与备份 LNS 建立连接，增加了 L2TP 服务的可靠性。

7. 支持由RADIUS服务器为LAC下发隧道属性

L2TP 隧道采用 NAS-Initiated 模式时，LAC 上的 L2TP 隧道属性可以通过 RADIUS 服务器来下发。此时，在 LAC 上只需开启 L2TP 服务，并配置采用 AAA 远程认证方式对 PPP 用户进行身份验证，无需进行其他 L2TP 配置。

当 L2TP 用户拨入 LAC 时，LAC 作为 RADIUS 客户端将用户的身份信息发送给 RADIUS 服务器。RADIUS 服务器对 L2TP 用户的身份进行验证。RADIUS 服务器将验证结果返回给 LAC，并将该用户对应的 L2TP 隧道属性下发给 LAC。LAC 根据下发的隧道属性，创建 L2TP 隧道和会话。

目前，RADIUS服务器可以为LAC下发的属性如 表 1-1 所示。

表1-1 RADIUS 服务器为 LAC 下发的属性列表

属性编号	属性名称	描述
64	Tunnel-Type	隧道类型，目前只支持L2TP隧道类型
65	Tunnel-Medium-Type	隧道的传输媒介类型，目前只支持IPv4
67	Tunnel-Server-Endpoint	LNS的IP地址
69	Tunnel-Password	隧道验证密钥
81	Tunnel-Private-Group-ID	隧道的Group ID LAC将该值发送给LNS，以便LNS根据该值进行相应的处理
82	Tunnel-Assignment-ID	隧道的Assignment ID 用来标识会话承载在哪条隧道上，具有相同Tunnel-Assignment-ID、Tunnel-Server_Endpoint和Tunnel-Password的L2TP用户共用同一条L2TP隧道
90	Tunnel-Client-Auth-ID	隧道的名称 用来标识本端隧道

目前，仅支持通过 RADIUS 服务器下发一组 L2TP 隧道属性，不支持同时下发多组隧道属性。

如果既通过RADIUS服务器为LAC下发了隧道属性，又在LAC上通过命令行手工配置了隧道属性，则以 RADIUS 服务器下发的属性为准。

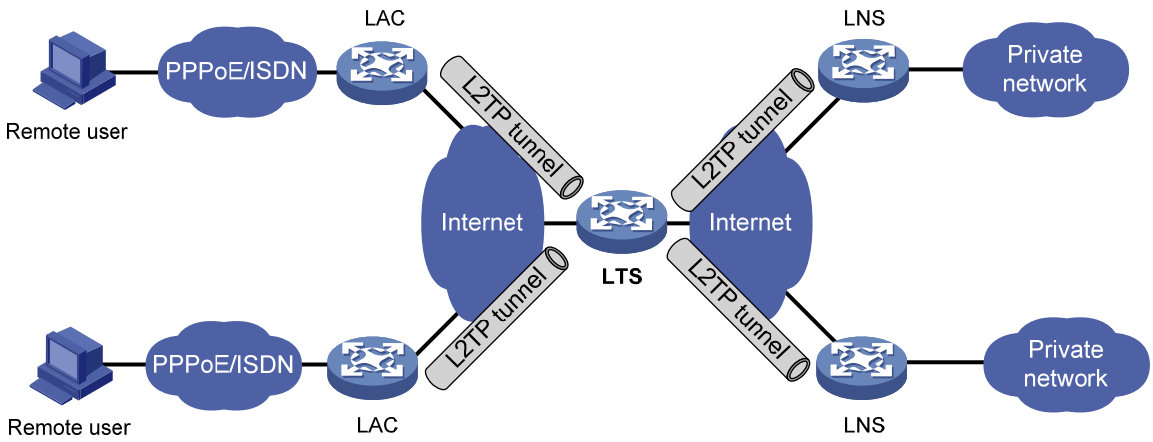
8. 支持L2TP隧道交换

如 图 1-10 所示，设备可以同时作为LNS和LAC，终结来自LAC的L2TP报文后，再将其通过L2TP隧道发送给最终的LNS，实现L2TP隧道的交换，即多跳L2TP隧道。同时作为LNS和LAC的设备称为LTS（L2TP Tunnel Switch，L2TP隧道交换）设备。

L2TP 隧道交换功能具有如下作用：

- LAC 和 LNS 位于不同的管理域时，可以简化 LAC 和 LNS 的配置与部署。所有的 LAC 都将 LTS 当作 LNS，不需要感知网络中是否存在多个 LNS，不需要区分 LNS；所有 LNS 都将 LTS 当作 LAC，不需要感知 LAC 的新增和删除。
- 不同用户可以共用 LAC 和 LTS 之间的 L2TP 隧道，由 LTS 将不同用户的数据分发给不同的 LNS。

图1-10 L2TP 隧道交换组网图



1.1.6 协议规范

与 L2TP 相关的协议规范有：

- RFC 1661：The Point-to-Point Protocol (PPP)
- RFC 1918：Address Allocation for Private Internets
- RFC 2661：Layer Two Tunneling Protocol "L2TP"
- RFC 2868：RADIUS Attributes for Tunnel Protocol Support

1.2 L2TP配置任务简介

配置 L2TP 时，需要执行以下操作：

(1) 根据实际组网环境，判断需要的网络设备。对于 NAS-Initiated 和 LAC-Auto-Initiated 模式，需要配置 LAC 和 LNS 两台网络设备；对于 Client-Initiated 模式，只需要配置 LNS 一台网络设备。

(2) 根据设备在网络中的角色，分别进行 LAC 或 LNS 端的相关配置，使设备具有 LAC 或 LNS 端功能。

表1-2 LAC 端配置任务简介（NAS-Initiated 和 LAC-Auto-Initiated 模式）

操作		说明	详细配置
配置L2TP基本功能		必选	1.3
配置LAC端	配置向LNS发起隧道建立请求的触发条件	对于NAS-Initiated模式，为必选； LAC-Auto-Initiated模式下无需配置	1.4.1
	配置LNS的IP地址	必选	1.4.2
	配置隧道的源端地址	可选	1.4.3
	配置AVP数据的隐藏传输	可选	1.4.4

操作		说明	详细配置
	配置LAC侧的AAA认证	对于NAS-Initiated模式，为必选；LAC-Auto-Initiated模式下无需配置	1.4.5
	配置LAC自动建立L2TP隧道	对于LAC-Auto-Initiated模式，为必选；NAS-Initiated模式下无需配置	1.4.6
配置L2TP可选参数	配置隧道验证	可选	1.6.1
	配置隧道Hello报文发送时间间隔		1.6.2
	开启L2TP会话的流控功能		1.6.3
	配置隧道报文的DSCP优先级		1.6.4
	配置LTS设备的TSA ID		1.6.5

表1-3 LNS 配置任务简介（NAS-Initiated、Client-Initiated 和 LAC-Auto-Initiated 模式）

操作		说明	详细配置
配置L2TP基本功能		必选	1.3
配置LNS端	配置虚拟模板接口	必选	1.5.1
	配置VA池	可选	1.5.2
	配置LNS接受L2TP隧道建立请求	必选	1.5.3
	配置LNS侧的用户验证	可选	1.5.4
	配置LNS侧的AAA认证	可选	1.5.5
配置L2TP可选参数	配置隧道验证	可选	1.6.1
	配置隧道Hello报文发送时间间隔		1.6.2
	开启L2TP会话的流控功能		1.6.3
	配置隧道报文的DSCP优先级		1.6.4
	配置LTS设备的TSA ID		1.6.5

1.3 配置L2TP基本功能

L2TP 基本功能的配置包括如下内容：

- 启用 L2TP 功能：只有启用 L2TP 后，设备上的 L2TP 功能才能正常发挥作用。
- 创建 L2TP 组：L2TP 组用于配置 L2TP 的相关参数，它不仅增加了 L2TP 配置的灵活性，还方便地实现了 LAC 和 LNS 之间一对一、一对多的组网应用。L2TP 组在 LAC 和 LNS 上独立编号，只需要保证 LAC 和 LNS 之间关联的 L2TP 组的相关配置（如隧道对端名称、LNS 地址等）保持对应关系即可。

- 配置隧道本端的名称：隧道本端的名称在 LAC 和 LNS 进行隧道协商时使用，它用来标识本端隧道，以供对端识别。

表1-4 配置 L2TP 基本功能

操作	命令	说明
进入系统视图	**system-view**	-
开启L2TP功能	**l2tp enable**	缺省情况下，L2TP功能处于关闭状态
创建L2TP组，指定L2TP组的模式，并进入L2TP组视图	**l2tp-group** *group-number* **mode** { **lac** | **lns** }	缺省情况下，设备上不存在任何L2TP组 在LAC侧需要指定L2TP组的模式为**lac**；在LNS侧需要指定L2TP组的模式为**lns**
配置隧道本端的名称	**tunnel name** *name*	缺省情况下，隧道本端的名称为设备的名称 LAC侧配置的隧道本端名称要与LNS侧配置的允许接受的L2TP隧道请求的隧道对端名称保持一致

1.4 配置LAC端

LAC 负责和相应的 LNS 建立 L2TP 隧道，并负责在远端系统和 LNS 之间转发报文。

1.4.1 配置向LNS发起隧道建立请求的触发条件

本配置用来指定 LAC 向 LNS 发起隧道建立请求的触发条件。只有 PPP 用户的信息与指定的触发条件匹配时，LAC 才认为该 PPP 用户为 L2TP 用户，向 LNS 发起 L2TP 隧道建立请求。

触发条件分为如下两种：

- 完整的用户名（**fullusername**）：只有 PPP 用户的用户名与配置的完整用户名匹配时，才会向 LNS 发起 L2TP 隧道建立请求。
- 带特定域名的用户名（**domain**）：PPP 用户的 ISP 域名与配置的域名匹配时，即向 LNS 发起 L2TP 隧道建立请求。

表1-5 配置向 LNS 发起隧道建立请求的触发条件

操作	命令	说明
进入系统视图	**system-view**	-
进入LAC模式的L2TP组视图	**l2tp-group** *group-number* [**mode lac**]	-
配置向LNS发起隧道建立请求的触发条件	**user** { **domain** *domain-name* | **fullusername** *user-name* }	缺省情况下，没有指定本端作为LAC端时向LNS发起隧道建立请求的触发条件

1.4.2 配置LNS的IP地址

LAC 上最多可以配置五个 LNS 地址，即允许存在备用 LNS。LAC 按照 LNS 配置的先后顺序依次向每个 LNS 发送建立 L2TP 隧道的请求。LAC 接收到某个 LNS 的接受应答后，该 LNS 就作为隧道的对端；否则，LAC 向下一个 LNS 发起隧道建立请求。

表1-6 配置 LNS 的 IP 地址

操作	命令	说明
进入系统视图	**system-view**	-
进入LAC模式的L2TP组视图	**l2tp-group** *group-number* [**mode lac**]	-
配置LNS的IP地址	**lns-ip** { *ip-address* }&<1-5>	缺省情况下，没有指定LNS的IP地址

1.4.3 配置隧道的源端地址

在 LAC 上配置了 L2TP 隧道的源端地址后，LAC 会将该地址作为封装后 L2TP 隧道报文的源 IP 地址。

建议将 L2TP 隧道的源端地址配置为设备上某 LoopBack 接口的 IP 地址，以减小物理接口故障对 L2TP 业务造成的影响。

表1-7 配置隧道的源端地址

操作	命令	说明
进入系统视图	**system-view**	-
进入LAC模式的L2TP组视图	**l2tp-group** *group-number* [**mode lac**]	-
配置L2TP隧道的源端地址	**source-ip** *ip-address*	缺省情况下，L2TP隧道的源端地址为本端隧道出接口的IP地址

1.4.4 配置AVP数据的隐藏传输

L2TP 协议通过 AVP（Attribute Value Pair，属性值对）来传输隧道协商参数、会话协商参数和用户认证信息等。如果用户不希望这些信息（如用户密码）被窃取，则可以使用本配置将 AVP 数据的传输方式配置成为隐藏传输，即利用隧道验证密钥（通过 **tunnel password** 命令配置）对 AVP 数据进行加密传输。

只有使能了隧道验证功能，本配置才会生效。隧道验证功能的详细配置，请参见“1.6.1 配置隧道验证”。

表1-8 配置 AVP 数据的隐藏传输

操作	命令	说明
进入系统视图	**system-view**	-
进入LAC模式的L2TP组视图	**l2tp-group** *group-number* [**mode lac**]	-

操作	命令	说明
配置隧道采用隐藏方式传输AVP数据	**tunnel avp-hidden**	缺省情况下，隧道采用明文方式传输AVP数据

1.4.5 配置LAC侧的AAA认证

本配置用来通过 AAA 对远端拨入用户的身份信息（用户名、密码）进行认证。用户身份认证通过后，LAC 才能发起建立隧道的请求，否则不会为用户建立隧道。

设备支持的 AAA 认证包括本地和远程两种认证方式：

- 如果选择本地认证方式，则需要在 LAC 侧配置本地用户名和密码。LAC 通过检查拨入用户的用户名/密码是否与本地配置的用户名/密码相符来验证用户身份。
- 如果选择远程认证方式，则需要在 RADIUS/HWTACACS 服务器上配置用户名和密码。LAC 将拨入用户的用户名和密码发往服务器，由服务器对用户身份进行认证。

AAA 相关的配置请参见“安全配置指导”中的“AAA”。

配置 LAC 侧的 AAA 认证时，接入用户的接口上需要配置 PPP 用户的验证方式为 PAP 或 CHAP，配置方法请参见“二层技术-广域网接入配置指导”中的“PPP”。

1.4.6 配置LAC自动建立L2TP隧道

配置 LAC 自动建立 L2TP 隧道，需要进行以下操作：

- 创建虚拟 PPP 接口，并配置该接口的 IP 地址。
- 在虚拟 PPP 接口下，配置 PPP 验证的被验证方，即通过 **ppp pap** 或 **ppp chap** 命令指定 PPP 用户支持的验证方法、PPP 用户的用户名和密码，LNS 对该 PPP 用户进行身份验证。详细介绍请参见“二层技术-广域网接入命令参考”中的“PPP”。
- 触发 LAC 建立 L2TP 隧道。

表1-9 配置 LAC 自动建立 L2TP 隧道

操作	命令	说明
进入系统视图	**system-view**	-
创建虚拟PPP接口，并进入虚拟PPP接口视图	**interface virtual-ppp** *interface-number*	缺省情况下，设备上不存在任何虚拟PPP接口
配置虚拟PPP接口的IP地址	**ip address** *address mask*	二者选其一 缺省情况下，没有配置接口的IP地址
配置虚拟PPP接口的IP地址可协商属性，使该接口接受PPP协商产生的由对端分配的IP地址	**ip address ppp-negotiate**	
配置PPP验证的被验证方	配置方法请参见“二层技术-广域网接入命令参考”中的“PPP”	-
触发LAC自动建立L2TP隧道	**l2tp-auto-client l2tp-group** *group-number*	缺省情况下，LAC没有建立L2TP隧道 触发LAC建立L2TP隧道后，该隧道将始终存在，直到通过**undo l2tp-auto-client**或**undo l2tp-group** *group-number*命令拆除该隧道

操作	命令	说明
（可选）配置当前接口的描述信息	**description** *text*	缺省情况下，接口的描述信息为“*该接口的接口名* Interface”，比如：Virtual-PPP254 Interface
配置接口的MTU值	**mtu** *size*	缺省情况下，虚拟PPP接口的MTU值为1500字节
（可选）配置接口发送keepalive报文的周期	**timer-hold** *seconds*	缺省情况下，接口发送keepalive报文的周期为10秒
（可选）配置接口在多少个keepalive周期内没有收到keepalive报文的应答就拆除链路	**timer-hold retry** *retry*	缺省情况下，接口在5个keepalive周期内没有收到keepalive报文的应答就拆除链路
（可选）配置接口的期望带宽	**bandwidth** *bandwidth-value*	缺省情况下，接口的期望带宽＝接口的波特率÷1000（kbit/s）
（可选）恢复当前接口的缺省配置	**default**	-
（可选）打开当前接口	**undo shutdown**	缺省情况下，接口处于打开状态

1.5 配置LNS端

LNS 响应 LAC 的隧道建立请求，负责对用户进行认证，并为用户分配 IP 地址。

1.5.1 配置虚拟模板接口

L2TP 会话建立之后，LNS 需要创建一个 VA（Virtual Access，虚拟访问）接口用于和 LAC 交换数据。VA 接口基于 VT（Virtual Template，虚拟模板）接口上配置的参数动态创建。因此，配置 LNS 时需要首先创建 VT 接口，并配置该接口的参数。

VT 接口的参数主要包括：

- 接口的 IP 地址
- 对 PPP 用户的验证方式
- LNS 为 PPP 用户分配的 IP 地址

关于 VT 接口配置的详细介绍，请参见“二层技术-广域网接入配置指导”中的“PPP 和 MP”以及“三层技术-IP 业务配置指导”中的“IP 地址”。

1.5.2 配置VA池

VA 池是在建立 L2TP 连接前事先创建的 VA 接口的集合。VA 池可以用来解决大量用户同时上线/下线，无法及时创建/删除 VA 接口，以至于影响 L2TP 连接建立和拆除性能的问题。

创建 VA 池后，当需要创建 VA 接口时，直接从 VA 池中获取一个 VA 接口，加快了 L2TP 连接的建立速度。当用户下线后，直接把 VA 接口放入 VA 池中，不需要删除 VA 接口，加快了 L2TP 连接的拆除速度。当 VA 池中的 VA 接口耗光后，仍需在建立 L2TP 连接时再创建 VA 接口，在用户下线后删除 VA 接口。

配置 VA 池时需要注意：

- 每个虚拟模板接口只能关联一个 VA 池。如果想要修改使用的 VA 池的大小，只能先删除原来的配置，然后重新配置 VA 池。
- 创建/删除 VA 池需要花费一定的时间，请用户耐心等待。在 VA 池创建/删除过程中（还没创建/删除完成）允许用户上线/下线，但正在创建/删除的 VA 池不生效。
- 系统可能由于资源不足不能创建用户指定容量的 VA 池，用户可以通过 **display l2tp va-pool** 命令查看实际可用的 VA 池的容量以及 VA 池的状态。
- VA 池会占用较多的系统内存，请用户根据实际情况创建大小合适的 VA 池。
- 删除 VA 池时，如果已有在线用户使用该 VA 池中的 VA 接口，不会导致这些用户下线。

表1-10 配置 VA 池

操作	命令	说明
进入系统视图	**system-view**	-
配置VA池	**l2tp virtual-template** *template-number* **va-pool** *va-volume*	缺省情况下，设备上不存在任何VA池

1.5.3 配置LNS接受L2TP隧道建立请求

接收到 LAC 发来的隧道建立请求后，LNS 需要检查 LAC 的隧道本端名称是否与本地配置的隧道对端名称相符合，从而决定是否与对端建立隧道，并确定创建 VA 接口时使用的 VT 接口。

表1-11 配置 LNS 接受 L2TP 隧道建立请求

操作		命令	说明
进入系统视图		**system-view**	-
进入LNS模式的L2TP组视图		**l2tp-group** *group-number* [**mode lns**]	-
配置LNS接受来自指定LAC的隧道建立请求，并指定建立隧道时使用的虚拟模板接口	L2TP组号不为1	**allow l2tp virtual-template** *virtual-template-number* **remote** *remote-name*	二者选其一 缺省情况下，LNS不接受任何LAC的隧道建立请求
	L2TP组号为1	**allow l2tp virtual-template** *virtual-template-number* [**remote** *remote-name*]	使用L2TP组号1时，可以不指定隧道对端名，即在组1下LNS可以接受任何名称的隧道对端的隧道建立请求

1.5.4 配置LNS侧的用户验证

当 LAC 对用户进行验证后，为了增强安全性，LNS 可以再次对用户进行验证。在这种情况下，将对用户进行两次验证，第一次发生在 LAC 侧，第二次发生在 LNS 侧，只有两次验证全部成功后，L2TP 隧道才能建立。

在 L2TP 组网中，LNS 侧对用户的验证方式有三种：

- 代理验证：由 LAC 代替 LNS 对用户进行验证，并将用户的所有验证信息及 LAC 端本身配置的验证方式发送给 LNS。LNS 根据接收到的信息及本端配置的验证方式，判断用户是否合法。
- 强制 CHAP 验证：强制在 LAC 代理验证成功后，LNS 再次对用户进行 CHAP 验证。

- LCP 重协商：忽略 LAC 侧的代理验证信息，强制 LNS 与用户间重新进行 LCP（Link Control Protocol，链路控制协议）协商。

验证方式的优先级从高到底依次为：LCP 重协商、强制 CHAP 验证和代理验证。

- 如果在 LNS 上同时配置 LCP 重协商和强制 CHAP 验证，L2TP 将使用 LCP 重协商。
- 如果只配置强制 CHAP 验证，则在 LAC 代理验证成功后，LNS 再次对用户进行 CHAP 验证。
- 如果既不配置 LCP 重协商，也不配置强制 CHAP 验证，则对用户进行代理验证。

1. 配置强制CHAP验证

配置强制 CHAP 验证后，对于 NAS-Initiated 模式 L2TP 隧道的用户来说，会经过两次验证：一次是在 NAS 端的验证，另一次是在 LNS 端的验证。一些用户可能不支持进行第二次验证，这时，LNS 端的 CHAP 重新验证会失败。在这种情况下，建议不要开启 LNS 的强制 CHAP 验证功能。

配置强制 CHAP 验证时，需要在 LNS 的 VT 接口下配置 PPP 用户的验证方式为 CHAP 认证。

表1-12 配置强制 CHAP 验证

操作	命令	说明
进入系统视图	**system-view**	-
进入LNS模式的L2TP组视图	**l2tp-group** *group-number* [**mode lns**]	-
强制LNS重新对用户进行CHAP验证	**mandatory-chap**	缺省情况下，LNS不会重新对用户进行CHAP验证 本命令只对NAS-Initiated模式的L2TP隧道有效，对Client-Initiated模式和LAC-Auto-Initiated模式的隧道无效

2. 配置强制LCP重新协商

对于 NAS-Initiated 模式 L2TP 隧道的 PPP 用户，在 PPP 会话开始时，先和 NAS 进行 PPP 协商。若协商通过，则由 NAS 触发建立 L2TP 隧道，并将用户信息传递给 LNS，由 LNS 根据收到的代理验证信息，判断用户是否合法。

但在某些特定的情况下（如 LNS 不接受 LAC 的 LCP 协商参数，希望和用户重新进行参数协商），需要强制 LNS 与用户重新进行 LCP 协商，并采用相应的虚拟模板接口上配置的验证方式对用户进行验证。

启用 LCP 重协商后，如果相应的虚拟模板接口上没有配置验证，则 LNS 将不对用户进行二次验证（这时用户只在 LAC 侧接受一次验证）。

表1-13 配置强制本端 LCP 重新协商

操作	命令	说明
进入系统视图	**system-view**	-
进入LNS模式的L2TP组视图	**l2tp-group** *group-number* [**mode lns**]	-

操作	命令	说明
配置强制LNS与用户重新进行LCP协商	**mandatory-lcp**	缺省情况下，LNS不会与用户重新进行LCP协商 本命令只对NAS-Initiated模式的L2TP隧道有效，对Client-Initiated模式和LAC-Auto-Initiated模式的隧道无效

1.5.5 配置LNS侧的AAA认证

本配置用来通过 AAA 对远端拨入用户的身份信息（用户名、密码）进行认证。认证通过后，远端系统可以通过 LNS 访问企业内部网络。

对于 NAS-Initiated 隧道模式，当 LNS 侧没有配置强制 LCP 重新协商时，必须在 LNS 侧配置 AAA 认证；或者当 LNS 侧配置了强制 LCP 重新协商，并且虚拟模板接口上配置了需要对 PPP 用户进行验证时，也必须在 LNS 侧配置 AAA 认证。对于 Client-Initiated 和 LAC-Auto-Initiated 隧道模式，当虚拟模板接口上配置了需要对 PPP 用户进行验证时，必须在 LNS 侧配置 AAA 认证。其他情况下无需在 LNS 侧配置 AAA 认证。

LNS侧支持的AAA配置与LAC侧的相同，具体介绍及配置方法请参见“1.4.5 配置LAC侧的AAA认证”。

1.6 配置L2TP可选参数

本节中的配置既可以在 LAC 上执行，也可以在 LNS 上执行。

1.6.1 配置隧道验证

用户可根据实际需要，决定是否在创建隧道之前进行隧道验证。

隧道验证请求可由 LAC 或 LNS 任何一侧发起。只要本端启用了隧道验证，则只有在对端也启用了隧道验证，两端密钥不为空并且完全一致的情况下，隧道才能建立；否则本端将自动断开隧道。

若隧道两端都配置了禁止隧道验证，隧道验证的密钥一致与否将不影响隧道建立。

为了保证隧道安全，建议用户最好不要禁用隧道验证的功能。如果用户需要修改隧道验证的密钥，请在隧道开始协商前进行，否则修改的密钥不生效。

表1-14 配置隧道验证

操作	命令	说明
进入系统视图	**system-view**	-
进入L2TP组视图	**l2tp-group** *group-number* [**mode** { **lac** | **lns** }]	-
开启L2TP的隧道验证功能	**tunnel authentication**	缺省情况下，L2TP隧道验证功能处于开启状态
配置隧道验证密钥	**tunnel password** { **cipher** | **simple** } *password*	缺省情况下，没有配置隧道验证密钥

1.6.2 配置隧道Hello报文发送时间间隔

为了检测 LAC 和 LNS 之间隧道的连通性，LAC 和 LNS 会定期向对端发送 Hello 报文，接收方接收到 Hello 报文后会进行响应。当 LAC 或 LNS 在指定时间间隔内未收到对端的 Hello 响应报文时，重复发送，如果重复发送 5 次仍没有收到对端的响应信息则认为 L2TP 隧道已经断开。

表1-15 配置隧道 Hello 报文发送时间间隔

操作	命令	说明
进入系统视图	**system-view**	-
进入L2TP组视图	**l2tp-group** *group-number* [**mode** { **lac** | **lns** }]	-
配置隧道中Hello报文的发送时间间隔	**tunnel timer hello** *hello-interval*	缺省情况下，隧道中Hello报文的发送时间间隔为60秒

1.6.3 配置L2TP会话的流控功能

L2TP 会话的流控功能是指在 L2TP 会话上传递的报文中携带序列号，通过序列号检测是否丢包，并根据序列号对乱序报文进行排序。

L2TP 会话的流控功能应用在 L2TP 数据报文的接收与发送过程中。只要 LAC 和 LNS 中的一端开启了流控功能，二者之间建立的 L2TP 会话就支持流控功能。

表1-16 开启 L2TP 会话的流控功能

操作	命令	说明
进入系统视图	**system-view**	-
进入L2TP组视图	**l2tp-group** *group-number* [**mode** { **lac** | **lns** }]	-
开启L2TP会话的流控功能	**tunnel flow-control**	缺省情况下，L2TP会话的流控功能处于关闭状态

1.6.4 配置隧道报文的DSCP优先级

DSCP（Differentiated Services Code Point，区分服务编码点）携带在 IP 报文中的 ToS 字段，用来体现报文自身的优先等级，决定报文传输的优先程度。

通过本配置指定隧道报文的 DSCP 优先级后，当流量经过 L2TP 隧道转发时，L2TP 将其封装为 IP 报文并将 IP 报文头中的 DSCP 优先级设置为指定的值。

表1-17 配置隧道报文的 DSCP 优先级

操作	命令	说明
进入系统视图	**system-view**	-
进入L2TP组视图	**l2tp-group** *group-number* [**mode** { **lac** | **lns** }]	-

操作	命令	说明
配置隧道报文的DSCP优先级	**ip dscp** *dscp-value*	缺省情况下，L2TP隧道报文的DSCP优先级为0

1.6.5 配置LTS设备的TSA ID

在 L2TP 隧道交换组网中，LTS 通过 ICRQ（Incoming Call Request，入呼叫请求）报文中的 TSA（Tunnel Switching Aggregator，隧道交换聚合） ID AVP 来避免环路。

LTS 接收到 ICRQ 报文后，将报文中携带的所有 TSA ID AVP 中的 TSA ID 逐一与本地配置的 TSA ID 进行比较。如果 TSA ID AVP 中存在与本地相同的 TSA ID，则表示存在环路，LTS 立即拆除会话。否则，LTS 将自己的 TSA ID 封装到新的 TSA ID AVP 中，LTS 向它的下一跳 LTS 发送 ICRQ 报文时携带接收到的所有 TSA ID AVP 及本地封装的 TSA ID AVP。

为不同 LTS 设备配置的 TSA ID 不能相同，否则会导致环路检测错误。

表1-18 配置 LTS 设备的 TSA ID

操作	命令	说明
进入系统视图	**system-view**	-
配置LTS设备的TSA ID，并开启LTS设备的L2TP环路检测功能	**l2tp tsa-id** *tsa-id*	缺省情况下，未指定LTS设备的TSA ID，且LTS设备的L2TP环路检测功能处于关闭状态

1.7 L2TP显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 L2TP 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以强制断开指定的 L2TP 隧道。

表1-19 L2TP 显示和维护

操作	命令
显示当前L2TP隧道的信息	**display l2tp tunnel** [**statistics**]
显示当前L2TP会话的信息	**display l2tp session** [**statistics**]
显示虚拟PPP接口的相关信息	**display interface** [**virtual-ppp** [*interface-number*]] [**brief** [**description** | **down**]]
显示L2TP的VA池信息	**display l2tp va-pool**
强制断开指定的L2TP隧道	**reset l2tp tunnel** { **id** *tunnel-id* | **name** *remote-name* }
清除虚拟PPP接口的统计信息	**reset counters interface** [**virtual-ppp** [*interface-number*]]

1.8 L2TP典型配置举例

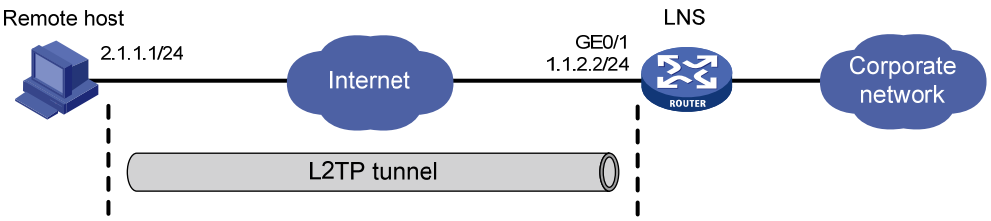
1.8.1 Client-Initiated模式L2TP隧道配置举例

1. 组网需求

PPP 用户直接与 LNS 建立 L2TP 隧道，通过 L2TP 隧道访问公司总部。

2. 组网图

图1-11 Client-Initiated 模式 L2TP 隧道组网图



3. 配置步骤

(1) LNS 侧的配置

配置接口的 IP 地址。（略）

配置路由，使得 LNS 与用户侧主机之间路由可达。（略）

创建本地 PPP 用户 vpdnuser，设置密码为 Hello。

```
[LNS] local-user vpdnuser class network
[LNS-luser-network-vpdnuser] password simple Hello
[LNS-luser-network-vpdnuser] service-type ppp
[LNS-luser-network-vpdnuser] quit
```

配置 ISP 域 system 对 PPP 用户采用本地验证。

```
[LNS] domain system
[LNS-isp-system] authentication ppp local
[LNS-isp-system] quit
```

开启 L2TP 功能。

```
[LNS] l2tp enable
```

创建接口 Virtual-Template1，配置接口的 IP 地址为 192.168.0.1/24，PPP 认证方式为 CHAP，并指定为 PPP 用户分配的 IP 地址为 192.168.0.2。

```
[LNS] interface virtual-template 1
[LNS-virtual-template1] ip address 192.168.0.1 255.255.255.0
[LNS-virtual-template1] ppp authentication-mode chap domain system
[LNS-virtual-template1] remote address 192.168.0.2
[LNS-virtual-template1] quit
```

创建 LNS 模式的 L2TP 组 1，配置隧道本端名称为 LNS，指定接收呼叫的虚拟模板接口为 VT1。

```
[LNS] l2tp-group 1 mode lns
[LNS-l2tp1] tunnel name LNS
[LNS-l2tp1] allow l2tp virtual-template 1
```

关闭 L2TP 隧道验证功能。

```
[LNS-l2tp1] undo tunnel authentication
```

(2) Remote host 侧的配置

配置 IP 地址为 2.1.1.1，并配置路由，使得 Remote host 与 LNS（IP 地址为 1.1.2.2）之间路由可达。

利用 Windows 系统创建虚拟专用网络连接，或安装 L2TP 客户端软件，如 WinVPN Client。

在 Remote host 上进行如下 L2TP 配置(设置的过程与相应的客户端软件有关,以下为设置的内容)：

- 设置 PPP 用户名为 vpdnuser，密码为 Hello。
- 将 LNS 的 IP 地址设为安全网关的 Internet 接口地址（本例中 LNS 侧与隧道相连接的以太网接口的 IP 地址为 1.1.2.2）。
- 修改连接属性，将采用的协议设置为 L2TP，将加密属性设为自定义，并选择 CHAP 验证。

4. 验证配置

在 Remote host 上触发 L2TP 拨号。拨号连接成功后，Remote host 获取到 IP 地址 192.168.0.2，并可以 Ping 通 LNS 的私网地址 192.168.0.1。

在 LNS 侧，通过命令 **display l2tp session** 可查看建立的 L2TP 会话。

```
[LNS-l2tp1] display l2tp session
LocalSID      RemoteSID      LocalTID      State
89            36245          10878         Established
```

在 LNS 侧，通过命令 **display l2tp tunnel** 可查看建立的 L2TP 隧道。

```
[LNS-l2tp1] display l2tp tunnel
LocalTID RemoteTID State         Sessions RemoteAddress    RemotePort RemoteName
10878    21        Established   1        2.1.1.1          1701       PC
```

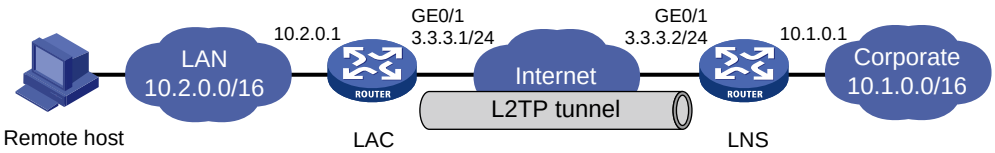
1.8.2 LAC-Auto-Initiated模式L2TP隧道配置举例

1. 组网需求

PPP 用户接入之前，在 LAC 和 LNS 之间采用 LAC-Auto-Initiated 模式建立 L2TP 隧道。PPP 用户接入后，通过已经建立的 L2TP 隧道访问公司总部。

2. 组网图

图1-12 LAC-Auto-Initiated 模式 L2TP 隧道组网图



3. 配置步骤

(1) LNS 侧的配置

配置各接口的 IP 地址（略）。

创建本地 PPP 用户 vpdnuser，配置密码为 Hello。

```
<LNS> system-view
[LNS] local-user vpdnuser class network
[LNS-luser-network-vpdnuser] password simple Hello
```

```
[LNS-luser-network-vpdnuser] service-type ppp
[LNS-luser-network-vpdnuser] quit
```
创建接口 Virtual-Template1，配置接口的 IP 地址为 192.168.0.20/24，PPP 认证方式为 PAP，并指定为 PPP 用户分配的 IP 地址为 192.168.0.2。
```
[LNS] interface virtual-template 1
[LNS-virtual-template1] ip address 192.168.0.20 255.255.255.0
[LNS-virtual-template1] ppp authentication-mode pap
[LNS-virtual-template1] remote address 192.168.0.2
[LNS-virtual-template1] quit
```
配置 ISP 域 system 对 PPP 用户采用本地验证。
```
[LNS] domain system
[LNS-isp-system] authentication ppp local
[LNS-isp-system] quit
```
开启 L2TP 功能，并创建 LNS 模式的 L2TP 组 1。
```
[LNS] l2tp enable
[LNS] l2tp-group 1 mode lns
```
配置 LNS 侧本端名称为 LNS，指定接收呼叫的虚拟模板接口为 VT1，并配置隧道对端名称为 LAC。
```
[LNS-l2tp1] tunnel name LNS
[LNS-l2tp1] allow l2tp virtual-template 1 remote LAC
```
启用隧道验证功能，并设置隧道验证密钥为 aabbcc。
```
[LNS-l2tp1] tunnel authentication
[LNS-l2tp1] tunnel password simple aabbcc
[LNS-l2tp1] quit
```
配置私网路由，使得访问 PPP 用户的报文将通过 L2TP 隧道转发。
```
[LNS] ip route-static 10.2.0.0 16 192.168.0.2
```
(2)　LAC 侧的配置

配置各接口的 IP 地址（略）。

开启 L2TP 功能。
```
<LAC> system-view
[LAC] l2tp enable
```
创建 LAC 模式的 L2TP 组 1。
```
[LAC] l2tp-group 1 mode lac
```
配置 LAC 侧本端名称为 LAC，并指定 LNS 的 IP 地址为 3.3.3.2。
```
[LAC-l2tp1] tunnel name LAC
[LAC-l2tp1] lns-ip 3.3.3.2
```
开启隧道验证功能，并设置隧道验证密钥为 aabbcc。
```
[LAC-l2tp1] tunnel authentication
[LAC-l2tp1] tunnel password simple aabbcc
[LAC-l2tp1] quit
```
创建虚拟 PPP 接口 Virtual-PPP 1，配置 PPP 用户的用户名为 vpdnuser、密码为 Hello，并配置 PPP 验证方式为 PAP。
```
[LAC] interface virtual-ppp 1
[LAC-Virtual-PPP1] ip address ppp-negotiate
[LAC-Virtual-PPP1] ppp pap local-user vpdnuser password simple Hello
[LAC-Virtual-PPP1] quit
```

配置私网路由，访问公司总部的报文将通过 L2TP 隧道转发。

```
[LAC] ip route-static 10.1.0.0 16 virtual-ppp 1
```

触发 LAC 发起 L2TP 隧道建立请求。

```
[LAC] interface virtual-ppp 1
[LAC-Virtual-PPP1] l2tp-auto-client l2tp-group 1
```

(3) Remote host 侧的配置

Remote host 上应将 LAC 设置为网关。

4. 验证配置

在 LNS 侧，通过命令 **display l2tp session** 可查看建立的 L2TP 会话。

```
[LNS] display l2tp session
LocalSID      RemoteSID      LocalTID      State
21409         3395           4501          Established
```

在 LNS 侧，通过命令 **display l2tp tunnel** 可查看建立的 L2TP 隧道。

```
[LNS] display l2tp tunnel
LocalTID RemoteTID State         Sessions RemoteAddress    RemotePort RemoteName
4501     524       Established   1        3.3.3.1          1701       LAC
```

在 LNS 侧，可以 Ping 通 LAC 的私网地址 10.2.0.1，说明 10.2.0.0/16 和 10.1.0.0/16 网络内的主机可以通过 L2TP 隧道通信。

```
[LNS] ping -a 10.1.0.1 10.2.0.1
Ping 10.2.0.1 (10.2.0.1): 56 data bytes, press CTRL_C to break
56 bytes from 10.2.0.1: icmp_seq=0 ttl=128 time=1.000 ms
56 bytes from 10.2.0.1: icmp_seq=1 ttl=128 time=1.000 ms
56 bytes from 10.2.0.1: icmp_seq=2 ttl=128 time=1.000 ms
56 bytes from 10.2.0.1: icmp_seq=3 ttl=128 time=1.000 ms
56 bytes from 10.2.0.1: icmp_seq=4 ttl=128 time=1.000 ms

--- Ping statistics for 10.2.0.1 ---
5 packet(s) transmitted, 5 packet(s) received, 0.0% packet loss
round-trip min/avg/max/std-dev = 1.000/1.000/1.000/0.000 ms
```

1.9 常见配置错误举例

1.9.1 错误之一

1. 错误现象

远端系统无法访问企业内部网络。

2. 错误排除

主要有以下几种原因：

(1) Tunnel 建立失败，原因可能是：

- 在 LAC 端，LNS 的地址设置不正确，具体可以查看 **lns-ip** 命令的说明。
- LNS 端没有设置可以接收该隧道对端的 L2TP 组，具体可以查看 **allow** 命令的说明。
- Tunnel 验证不通过，如果配置了验证，应该保证双方都启用了隧道验证并且配置相同的验证密钥。

(2) PPP 协商不通过，可能原因有：

- LAC 端设置的用户名与密码有误，或者是 LNS 端没有设置相应的用户。
- LNS 端不能分配地址，请检查远端系统和 LNS 对 IP 地址协商相关的配置是否正确。
- 密码验证类型不一致。例如，Windows 2000 所创建的 VPN 连接缺省的验证类型为 MS-CHAP，如果对端不支持 MS-CHAP，建议改为 CHAP。

1.9.2 错误之二

1. 错误现象

数据传输失败，在隧道建立后数据不能传输，如 Ping 不通对端。

2. 错误排除

可能有如下原因：

(1) 路由问题：LAC 和 LNS 上需要存在到达对端私网的路由，否则会导致数据传输失败。在 LAC 和 LNS 上执行 **display ip routing-table** 命令，查看设备上是否存在到达对端私网的路由。若不存在，则需要配置静态路由或动态路由协议，在设备上添加该路由。

(2) 网络拥挤：Internet 主干网产生拥挤，丢包现象严重。L2TP 是基于 UDP 进行传输的，UDP 不对报文进行差错控制。如果是在线路质量不稳定的情况下进行 L2TP 应用，有可能会产生 Ping 不通对端的情况。

目 录

1 4G Modem管理

说明

本节所指的 4G Modem 为设备内置的 4G modem 模块。

1.1 4G Modem管理配置任务简介

表1-1 4G Modem 管理配置任务简介

配置任务	说明	详细配置
配置4G Modem模块Cellular接口基本参数	必选	1.2
配置4G Modem模块以太网通道接口基本参数	必选	1.3
配置4G Modem模块以太网通道接口的IP地址	必选	1.4
配置4G Modem无线网络	必选	1.5
配置4G Modem参数模板	必选	1.6
配置4G Modem PIN码认证功能	可选	1.7
配置4G Modem调试功能	可选	1.8
通过配置指令配置4G Modem	可选	1.9
配置4G Modem自动重启功能	可选	1.10
手动重启4G Modem	可选	1.11

说明

根据实际组网需要，在 4G Modem 模块对应的 Cellular 接口派生出来的 Eth-channel 接口上可能要配置 DDR 参数、IP 地址等。

1.2 配置4G Modem模块Cellular接口基本参数

表1-2 配置 4G Modem 模块 Cellular 接口基本参数

操作	命令	说明
进入系统视图	**system-view**	-
进入Cellular接口视图	**controller cellular** *cellular-number*	-
配置Cellular接口的描述信息	**description** *text*	缺省情况下，Cellular接口的描述信息为“*该接口的接口名* Interface”，比如：Cellular2/0 Interface

操作	命令	说明
将Cellular接口通道化出以太网通道接口	**eth-channel** *channel-number*	Cellular接口在配置该命令后通道化出一个以太网通道接口，接口名是**eth-channel** *cellular-number*:*channel-number*
打开Cellular接口	**undo shutdown**	缺省情况下，Cellular接口处于打开状态

1.3 配置4G Modem模块以太网通道接口基本参数

表1-3 配置 4G Modem 模块以太网通道接口基本参数

操作	命令	说明
进入系统视图	**system-view**	-
进入以太网通道接口视图	**interface eth-channel** *interface-number*	-
配置接口的描述信息	**description** *text*	缺省情况下，以太网通道接口的描述信息为“*该接口的接口名* Interface”，比如“Echannel2/0:0 Interface”
配置接口的MTU值	**mtu** *size*	缺省情况下，以太网通道接口的MTU值为1500字节
配置接口的期望带宽	**bandwidth** *bandwidth-value*	缺省情况下，接口的期望带宽＝接口的波特率÷1000（kbit/s） 以太网通道接口的波特率为100Mbps
恢复接口的缺省配置	**default**	-
打开以太网通道接口	**undo shutdown**	缺省情况下，以太网通道接口处于打开状态

1.4 配置4G Modem模块以太网通道接口的IP地址

以太网通道接口有了 IP 地址后才可以与其它主机进行 IP 通信。以太网通道接口获取 IP 地址的方式有以下几种：

- 通过 Modem 私有协议获取 IP 地址：部分 Modem 支持以厂商自己的私有协议从 Modem 处获取 IP 地址，Modem 的 IP 地址由运营商自动分配。
- 手动指定 IP 地址：部分情况下，如果不能从 Modem 处获得 IP 地址，则必须手动配置接口 IP 地址。

上述几种方式是互斥的，通过新的配置方式获取的 IP 地址会覆盖通过原有方式获取的 IP 地址。例如，首先通过手动指定了 IP 地址，然后使用 Modem 私有协议获取 IP 地址，那么手动指定的 IP 地址会被删除，接口使用的是通过 Modem 私有协议获取到的 IP 地址。

提示

改变以太网通道接口的 IP 地址配置会导致拨号断开，部分运营商不支持断开后马上进行拨号。

表1-4 配置 4G Modem 模块以太网通道接口的 IP 地址

操作		命令	说明
进入系统视图		**system-view**	-
进入以太网通道接口视图		**interface eth-cahnnel** *interface-number*	-
配置以太网通道接口的IP地址（三者选其一）	配置接口通过DHCP协议获取IP地址	**ip address dhcp-alloc**	缺省情况下，接口不通过DHCP协议获取IP地址 关于本命令的详细介绍请参见“三层技术-IP业务命令参考”中的“DHCP”
	配置接口通过Modem私有协议获取IP地址	**ip address cellular-alloc**	缺省情况下，接口不通过Modem私有协议获取IP地址
	手动指定接口IP地址	**ip address** *ip-address* { *mask-length* | *mask* } [**sub**]	缺省情况下，没有为接口配置IP地址

1.5 配置4G Modem无线网络

无线网络按照使用的标准可以分为：GSM 网络、CDMA2000 网络、TD-SCDMA 网络、WCDMA 网络和 LTE 网络，其中 CDMA2000 网络又分为两种：CDMA-1x RTT 网络和 CDMA-EVDO 网络。特定的 4G Modem 模块，只能接入其中的一种或多种网络。其中，4G Modem 可以接入 GSM 网络、CDMA2000 网络、TD-SCDMA 网络、WCDMA 网络和 LTE 网络。

使用 4G Modem 时，需要在 PLMN（Public Land Mobile Network，公共陆地移动网络）中选择接入的移动网络。每个 PLMN 由 MCC（Mobile Country Code，移动国家编码）和 MNC（Mobile Network Code，移动网络编码）唯一标识。有的 4G Modem 能自动选择接入合适的网络。如果用户需要手工指定接入的移动网络，则需要先搜索移动网络，获取当前区域内有信号的移动网络列表。

表1-5 配置 4G Modem 搜索和选择无线网络功能

操作	命令	说明
进入系统视图	**system-view**	-
进入Cellular接口视图	**controller cellular** *interface-number*	-
（可选）搜索移动网络	**plmn search**	-
配置选择移动网络的方式	**plmn select** { **auto** | **manual** *mcc mnc* }	本命令的缺省情况与4G Modem设备的型号有关，请以设备的实际情况为准
选择网络连接方式	**mode** { **1xrtt** | **auto** | **evdo** | **gsm** | **gsm-precedence** | **hybrid** | **lte** | **td** | **td-precedence** | **wcdma** | **wcdma-precedence** }	本命令的缺省情况以及各参数的支持情况与4G Modem设备的型号有关，请以设备的实际情况为准
选择LTE模块所工作的频段	**lte band** *band-number*	本命令的缺省情况以及各参数的支持情况与4G Modem设备的型号有关，请以设备的实际情况为准

1.6 配置4G Modem参数模板

1.6.1 创建/删除参数模板

4G Modem 参数模板用于配置 4G Modem 的接入点和认证方式， 4G Modem 会根据配置的接入点和认证方式，来和对应的服务商进行认证：

- 当选用 None 方式时，不需要输入用户名和密码。
- 当选用 CHAP 或 PAP 方式时，需要根据运营商的要求，选择配置用户名和密码。

表1-6 创建/删除参数模板

操作	命令	说明
进入系统视图	**system-view**	-
进入Cellular接口视图	**controller cellular** *interface-number*	-
创建参数模板	**profile create** *profile-number* { **dynamic** | **static** *apn* } **authentication-mode** { **none** | { **chap** | **pap** } **user** *username* [**password** *password*] }	本命令的缺省情况与4G Modem设备的型号有关，请以设备的实际情况为准

1.6.2 配置 4G Modem拨号使用的参数模板

缺省情况下， 4G Modem 使用参数模板 1 进行拨号。如果参数模板 1 不存在，则拨号失败。

用户也可以通过下面的命令配置 4G Modem 拨号使用的主备参数模板。配置该命令后，4G Modem 每次拨号都优先选择主参数模板，如果主参数模板拨号失败，将使用备份参数模板进行拨号。无论备份参数模板拨号是否成功，下次拨号时都使用主参数模板拨号。需要注意的是，使用的主备参数模板的用户名和密码必须配成一样的。

表1-7 配置 4G Modem 拨号使用的主备参数模板

操作	命令	说明
进入系统视图	**system-view**	-
进入Cellular接口视图	**controller cellular** *interface-number*	-
配置4G Modem拨号使用的主备参数模板	**profile main** *main-profile-number* **backup** *backup-profile-number*	缺省情况下，4G Modem使用参数模板1进行拨号

1.7 配置4G Modem PIN码认证功能

每个 SIM/UIM 卡（UIM 卡用于 CDMA 网络，SIM 卡用于其它网络）都有 PIN（Personal Identification Number，个人识别号码）码。PIN 码认证功能可以防止 SIM/UIM 卡在未授权的情况下被使用。

如果开启了 4G Modem 的 PIN 码认证功能，当 4G Modem 插入或重启时，会使用 **pin verify** 命令配置的 PIN 码进行认证，否则 4G Modem 的数据通信功能不可用。重启 4G Modem 的途径包括：重启设备、使用 **modem reboot** 命令重启 4G Modem。用户可以在需要 PIN 码认证时配置 **pin verify**

命令，也可以提前配置 **pin verify** 命令，只要配置一次 **pin verify** 命令，PIN 码就会保存在设备上，在需要认证时，自动完成 PIN 码认证。

在进行 PIN 码认证时，如果 PIN 码连续输入错误达到一定次数（该次数与 4G Modem 的设备型号有关）时，SIM/UIM 卡会被锁。此时，必须使用 SIM/UIM 卡的 PUK（PIN Unlocking Key，PIN 码解锁码）码才能解锁。

表1-8 配置 4G Modem PIN 码认证功能

操作	命令	说明
进入系统视图	**system-view**	-
进入Cellular接口视图	**controller cellular** *interface-number*	-
开启4G Modem的PIN码认证功能	**pin verification enable** [*pin*]	本命令的缺省情况与4G Modem设备的型号有关，请以设备的实际情况为准 配置本功能时，可能要求输入当前的PIN码。该要求与4G Modem设备的型号有关，请以设备的实际情况为准
配置4G Modem进行认证的PIN码	**pin verify** { **cipher** *ciphered-pin* | **simple** *pin* }	缺省情况下，未配置4G Modem进行认证的PIN码 该配置保存在设备上，而不是保存在4G Modem上
（可选）使用PUK码解锁PIN码	**pin unlock** *puk new-pin*	如果开启了4G Modem的PIN码认证功能，解锁PIN码后，需要配置**pin verify**命令以保持和重新设置的PIN码一致
（可选）修改SIM/UIM卡的PIN码	**pin modify** *current-pin new-pin*	修改后的PIN码保存在SIM/UIM卡上 如果开启了4G Modem的PIN码认证功能，修改PIN码后，需要配置**pin verify**命令以保持和修改后的PIN码一致

1.8 配置4G Modem的DM功能

DM（Diagnostic and Monitoring，诊断和监控），指某些类型的 4G Modem 支持通过 4G Modem 上的调试信息输出接口输出调试信息功能，用于连接第三方的调试工具（如高通 QXDM 软件）进行诊断和监控。

表1-9 配置 4G Modem 的 DM 功能

操作	命令	说明
进入系统视图	**system-view**	-
进入Cellular接口视图	**controller cellular** *interface-number*	-
打开4G Modem的DM功能	**dm-port open**	本命令的缺省情况与4G Modem设备的型号有关，请以设备的实际情况为准

1.9 通过配置指令配置4G Modem

注意

通过配置指令配置 4G Modem 后， 4G Modem 的工作状态会被改变，有可能导致 4G Modem 的状态混乱从而影响到拨号等基本功能，请慎重使用本功能。

表1-10 通过配置指令配置 4G Modem

操作	命令	说明
进入系统视图	**system-view**	-
进入Cellular接口视图	**controller cellular** *interface-number*	-
手工向4G Modem发送配置指令	**sendat** *at-string*	**sendat**命令一次只能配置一条配置指令

1.10 配置自动重启4G Modem功能

4G 无线网络的不稳定运行或应用环境变化可能导致 4G Modem 功能故障，无法自动拨号并连接网络。设备提供自动重启 4G Modem 功能，尽可能减少需要用户手工重启 4G Modem 的情况。

开启自动重启 4G Modem 功能后，如果连续多次下发配置指令失败或配置指令响应超时，系统将自动重启 4G Modem。为避免因配置错误引起的多次拨号失败，而导致的反复自动重启 4G Modem 的情况，系统仅在上次自动重启 4G Modem 后有过至少一次拨号成功记录，并且多次发配置指令失败或配置指令响应超时的情况下才会自动重启 4G Modem。

表1-11 配置自动重启 4G Modem 功能

操作	命令	说明
进入系统视图	**system-view**	-
进入Cellular接口视图	**controller cellular** *interface-number*	-
配置系统向4G Modem下发配置指令后，等待其回复的时间间隔，以及4G Modem连续不响应系统配置指令（配置指令失败或配置指令响应超时）次数的阈值，达到系统配置的阈值后，自动重启4G Modem	**modem response timer** *time* **auto-recovery** *threshold*	缺省情况下，系统等待4G Modem回复的时间间隔为10秒，连续不响应系统配置指令次数的阈值为3次 该配置保存在设备上，而不是保存在4G Modem上

1.11 手动重启4G Modem

4G Modem 在运行过程中能够自动检测异常，并实施自动重启。如果无法自动重启，用户可以通过本配置手动重启 4G Modem。

表1-12 手动重启 4G Modem

操作	命令	说明
进入系统视图	**system-view**	-
进入Cellular接口视图	**controller cellular** *interface-number*	-
手动重启4G Modem	**modem reboot**	-

1.12 4G Modem管理显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 4G Modem 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除相关接口的统计信息。

表1-13 4G Modem 管理显示和维护

操作	命令
显示4G Modem的呼叫连接信息	**display cellular** [*interface-number*]
显示Cellular接口的相关信息	**display controller** [**cellular** [*interface-number*]]
显示以太网通道接口的相关信息	**display interface** [**eth-channel** [*channel-id*]] [**brief** [**description** | **down**]]
清除Cellular接口的统计信息	**reset counters controller** [**cellular** [*interface-number*]]
清除以太网通道接口的统计信息	**reset counters interface** [**eth-channel** [*channel-id*]]

1.13 4G Modem管理常见故障的诊断与排除

1.13.1 4G Modem状态不正常

1. 故障现象

4G Modem 状态不正常（如搜不到信号或不能连接到运营商网络）。

2. 故障排除

可以按照如下步骤进行：

- 在 4G Modem 对应的 Cellular 接口上执行 **shutdown** 和 **undo shutdown** 命令，检查 4G Modem 状态是否恢复正常；
- 若 4G Modem 状态仍不正常，则在 4G Modem 对应的 Cellular 接口上执行 **modem reboot**。