# UNIS 防火墙产品

## 二层技术-广域网接入配置指导(V7)

北京紫光恒越网络科技有限公司
http://www.unis-hy.com

资料版本：5P100-20160616

# 前 言

UNIS 防火墙产品配置指导(V7)介绍了防火墙产品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 PPP 和 L2TP 相关的特性。

前言部分包含如下内容：



## 适用款型

防火墙产品款型较多，形态丰富，本手册所描述的内容适用于如下产品款型：

**表1 手册适用的产品款型**

| 款型 | 形态 |
| --- | --- |
| UNIS F5000-M06防火墙 | 分布式设备，可以运行在：<br>• 独立运行模式<br>• IRF 模式 |
| UNIS F5000-G20防火墙 | 集中式IRF设备 |
| UNIS F1000-G20/G50/G60/G80防火墙 | 集中式IRF设备 |

## 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. 端口编号示例约定

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。

## 技术支持

用户支持邮箱：zgsm_service@thunis.com

技术支持热线电话：400-910-9998（手机、固话均可拨打）

网址：http://www.unis-hy.com

## 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：zgsm_info@thunis.com

感谢您的反馈，让我们做得更好！

# 目 录

# 1 PPP

设备各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

| 型号 | 特性 | 描述 |
| --- | --- | --- |
| F5000-M06 | PPP | 不支持 |
| F5000-G20 | | 支持 |
| F1000-G20/G50/G60/G80 | | 支持 |

## 1.1 PPP简介

PPP（Point-to-Point Protocol，点对点协议）是一种点对点的链路层协议。它能够提供用户认证，易于扩充，并且支持同/异步通信。

PPP 定义了一整套协议，包括：

- 链路控制协议（Link Control Protocol，LCP）：用来建立、拆除和监控数据链路。
- 网络控制协议（Network Control Protocol，NCP）：用来协商在数据链路上所传输的网络层报文的一些属性和类型。
- 认证协议：用来对用户进行认证，包括 PAP（Password Authentication Protocol，密码认证协议）、CHAP（Challenge Handshake Authentication Protocol，质询握手认证协议）、MSCHAP（Microsoft CHAP，微软 CHAP 协议）和 MSCHAPv2（微软 CHAP 协议版本 2）。

### 1. PPP链路建立过程

PPP链路建立过程如 图 1-1 所示：

(1) PPP 初始状态为不活动（Dead）状态，当物理层 Up 后，PPP 会进入链路建立（Establish）阶段。

(2) PPP 在 Establish 阶段主要进行 LCP 协商。LCP 协商内容包括：Authentication-Protocol（认证协议类型）、MRU（Maximum-Receive-Unit，最大接收单元）、Magic-Number（魔术字）、PFC（Protocol-Field-Compression，协议字段压缩）、ACFC（Address-and-Control-Field-Compression，地址控制字段压缩）、MP 等选项。如果 LCP 协商失败，LCP 会上报 Fail 事件，PPP 回到 Dead 状态；如果 LCP 协商成功，LCP 进入 Opened 状态，LCP 会上报 Up 事件，表示链路已经建立（此时对于网络层而言 PPP 链路还没有建立，还不能够在上面成功传输网络层报文）。

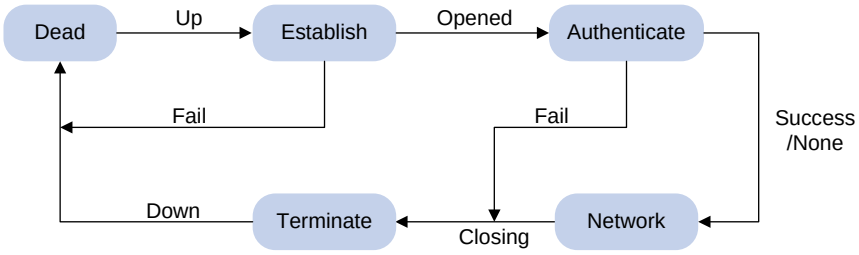
(3) 如果配置了认证，则进入 Authenticate 阶段，开始 PAP、CHAP、MSCHAP 或 MSCHAPv2 认证。如果认证失败，LCP 会上报 Fail 事件，进入 Terminate 阶段，拆除链路，LCP 状态转为 Down，PPP 回到 Dead 状态；如果认证成功，LCP 会上报 Success 事件。

(4) 如果配置了网络层协议，则进入 Network 协商阶段，进行 NCP 协商（如 IPCP 协商、IPv6CP 协商）。如果 NCP 协商成功，链路就会 UP，就可以开始承载协商指定的网络层报文；如果 NCP 协商失败，NCP 会上报 Down 事件，进入 Terminate 阶段。（对于 IPCP 协商，如果接

口配置了 IP 地址，则进行 IPCP 协商，IPCP 协商通过后，PPP 才可以承载 IP 报文。IPCP 协商内容包括：IP 地址、DNS 服务器地址等。）

(5) 到此，PPP 链路将一直保持通信，直至有明确的 LCP 或 NCP 消息关闭这条链路，或发生了某些外部事件（例如用户的干预）。

图1-1 PPP 链路建立过程




有关 PPP 的详细介绍请参考 RFC 1661。

### 2. PPP认证

PPP 提供了在其链路上进行安全认证的手段，使得在 PPP 链路上实施 AAA 变的切实可行。将 PPP 与 AAA 结合，可在 PPP 链路上对对端用户进行认证、计费。

PPP 支持如下认证方式：PAP、CHAP、MSCHAP、MSCHAPv2。

(1) PAP 认证

PAP 为两次握手协议，它通过用户名和密码来对用户进行认证。

PAP 在网络上以明文的方式传递用户名和密码，认证报文如果在传输过程中被截获，便有可能对网络安全造成威胁。因此，它适用于对网络安全要求相对较低的环境。

(2) CHAP 认证

CHAP 为三次握手协议。

CHAP 认证过程分为两种方式：认证方配置了用户名、认证方没有配置用户名。推荐使用认证方配置用户名的方式，这样被认证方可以对认证方的身份进行确认。

CHAP 只在网络上传输用户名，并不传输用户密码（准确的讲，它不直接传输用户密码，传输的是用 MD5 算法将用户密码与一个随机报文 ID 一起计算的结果），因此它的安全性要比 PAP 高。

(3) MSCHAP 认证

MSCHAP 为三次握手协议，认证过程与 CHAP 类似，MSCHAP 与 CHAP 的不同之处在于：

- MSCHAP 采用的加密算法是 0x80。
- MSCHAP 支持重传机制。在被认证方认证失败的情况下，如果认证方允许被认证方进行重传，被认证方会将认证相关信息重新发回认证方，认证方根据此信息重新对被认证方进行认证。认证方最多允许被认证方重传 3 次。

(4) MSCHAPv2 认证

MSCHAPv2 为三次握手协议，认证过程与 CHAP 类似，MSCHAPv2 与 CHAP 的不同之处在于：

- MSCHAPv2 采用的加密算法是 0x81。
- MSCHAPv2 通过报文捎带的方式实现了认证方和被认证方的双向认证。

- MSCHAPv2 支持重传机制。在被认证方认证失败的情况下，如果认证方允许被认证方进行重传，被认证方会将认证相关信息重新发回认证方，认证方根据此信息重新对被认证方进行认证。认证方最多允许被认证方重传 3 次。
- MSCHAPv2 支持修改密码机制。被认证方由于密码过期导致认证失败时，被认证方会将用户输入的新密码信息发回认证方，认证方根据新密码信息重新进行认证。

### 3. PPP支持IPv4

在 IPv4 网络中，PPP 进行 IPCP 协商过程中可以进行 IP 地址、DNS 服务器地址的协商。

(1) IP 地址协商

PPP 在进行 IPCP 协商的过程中可以进行 IP 地址的协商，即一端给另一端分配 IP 地址。

在 PPP 协商 IP 地址的过程中，设备可以分为两种角色：

- Client 端：若本端接口封装的链路层协议为 PPP 但还未配置 IP 地址，而对端已有 IP 地址时，用户可为本端接口配置 IP 地址可协商属性，使本端接口作为 Client 端接受由对端（Server 端）分配的 IP 地址。该方式主要用于设备在通过 ISP 访问 Internet 时，由 ISP 分配 IP 地址。
- Server 端：若设备作为 Server 端为 Client 端分配 IP 地址，则应先配置地址池（可以是 PPP 地址池或者 DHCP 地址池），然后在 ISP 域下关联地址池，或者在接口下指定为 Client 端分配的 IP 地址或者地址池，最后再配置 Server 端的 IP 地址，开始进行 IPCP 协商。

当 Client 端配置了 IP 地址可协商属性后，Server 端根据 AAA 认证结果（关于 AAA 的介绍请参见“安全配置指导”中的“AAA”）和接口下的配置，按照如下顺序给 Client 端分配 IP 地址：

- 如果 AAA 认证服务器为 Client 端设置了 IP 地址或者地址池信息，则 Server 端将采用此信息为 Client 端分配 IP 地址（这种情况下，为 Client 端分配的 IP 地址或者分配 IP 地址所采用的地址池信息是在 AAA 认证服务器上进行配置的，Server 端不需要进行特殊配置）。
- 如果 Client 端认证时使用的 ISP 域下设置了为 Client 端分配 IP 地址的地址池，则 Server 端将采用此地址池为 Client 端分配 IP 地址。
- 如果 Server 端的接口下指定了为 Client 端分配的 IP 地址或者地址池，则 Server 端将采用此信息为 Client 端分配 IP 地址。

(2) DNS 服务器地址协商

设备在进行 IPCP 协商的过程中可以进行 DNS 服务器地址协商。设备既可以作为 Client 端接收其它设备分配的 DNS 服务器地址，也可以作为 Server 端向其它设备提供 DNS 服务器地址。通常情况下：

- 当主机与设备通过 PPP 协议相连时，设备应配置为 Server 端，为对端主机指定 DNS 服务器地址，这样主机就可以通过域名直接访问 Internet；
- 当设备通过 PPP 协议连接运营商的接入服务器时，设备应配置为 Client 端，被动接收或主动请求接入服务器指定 DNS 服务器地址，这样设备就可以使用接入服务器分配的 DNS 来解析域名。

### 4. PPP支持IPv6

在 IPv6 网络中，PPP 进行 IPv6CP 协商过程中，只协商出 IPv6 接口标识，不能协商出 IPv6 地址、IPv6 DNS 服务器地址。

(1) IPv6 地址分配

PPP 进行 IPv6CP 协商过程中，只协商出 IPv6 接口标识，不能直接协商出 IPv6 地址。

客户端可以通过如下三种方式分配到 IPv6 全球单播地址：

- 方式 1：客户端通过 ND 协议中的 RA 报文获得 IPv6 地址前缀。客户端采用 RA 报文中携带的前缀和 IPv6CP 协商的 IPv6 接口标识一起组合生成 IPv6 全球单播地址。RA 报文中携带的 IPv6 地址前缀的来源有三种：AAA 授权的 IPv6 前缀、接口下配置的 RA 前缀、接口下配置的 IPv6 全球单播地址的前缀。三种来源的优先级依次降低，AAA 授权的优先级最高。关于 ND 协议的详细介绍请参见“三层技术-IP 业务配置指导”中的“IPv6 基础”。
- 方式 2：客户端通过 DHCPv6 协议申请 IPv6 全球单播地址。在服务器端可以通过 AAA 授权为每个客户端分配不同的地址池，当授权了地址池后，DHCPv6 在分配 IPv6 地址时会从地址池中获取 IPv6 地址分配给客户端。如果 AAA 未授权地址池，DHCPv6 会根据服务器端的 IPv6 地址查找匹配的地址池为客户端分配地址。关于 DHCPv6 协议的详细介绍请参见“三层技术-IP 业务配置指导”中的“DHCPv6”。
- 方式 3：客户端通过 DHCPv6 协议申请代理前缀，客户端通过代理前缀为下面的主机分配 IPv6 全球单播地址。代理前缀分配方式中地址池的选择原则和通过 DHCPv6 协议分配 IPv6 全球单播地址方式中地址池的选择原则一致。

根据组网不同，主机获取 IPv6 地址的方式如下：

- 当主机通过桥设备或者直连接入设备时，设备可以采用上述的方式 1 或方式 2 直接为主机分配 IPv6 全球单播地址。
- 当主机通过路由器接入设备时，设备可以采用方式 3 为路由器分配 IPv6 前缀，路由器把这些 IPv6 前缀分配给主机来生成 IPv6 全球单播地址。

(2) IPv6 DNS 服务器地址分配

在 IPv6 网络中，IPv6 DNS 服务器地址的分配有如下两种方式：

- AAA 授权 IPv6 DNS 服务器地址，通过 ND 协议中的 RA 报文将此 IPv6 DNS 服务器地址分配给主机。
- DHCPv6 客户端向 DHCPv6 服务器申请 IPv6 DNS 服务器地址。

# 1.2 配置PPP

## 1.2.1 PPP配置任务简介

**表1-1 PPP 配置任务简介**

| 配置任务 | 说明 | 详细配置 |
|---|---|---|
| 配置PPP认证方式 | 可选 | 1.2.2 |
| 配置轮询功能 | 可选 | 1.2.3 |
| 配置PPP协商参数 | 可选 | 1.2.4 |
| 配置PPP IPHC压缩功能 | 可选 | 1.2.5 |
| 配置PPP链路质量监测功能 | 可选 | 1.2.6 |
| 配置PPP计费统计功能 | 可选 | 1.2.7 |
| 配置PPP用户的nas-port-type属性 | 可选 | 1.2.8 |

### 1.2.2 配置PPP认证方式

PPP 支持如下认证方式：PAP、CHAP、MSCHAP、MSCHAPv2。用户可以同时配置多种认证方式，在 LCP 协商过程中，认证方根据用户配置的认证方式顺序逐一与被认证方进行协商，直到协商通过。如果协商过程中，被认证方回应的协商报文中携带了建议使用的认证方式，认证方查找配置中存在该认证方式，则直接使用该认证方式进行认证。

#### 1. 配置PAP认证

(1) 配置认证方

**表1-2 配置认证方**

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 配置本地认证对端的方式为PAP | **ppp authentication-mode pap** [ [ **call-in** ] **domain** *isp-name* ] | 缺省情况下，PPP协议不进行认证 |
| 配置本地AAA认证或者远程AAA认证 | 请参见“安全配置指导”中的“AAA”<br>• 若采用本地 AAA 认证，则认证方必须为被认证方配置本地用户的用户名和密码<br>• 若采用远程 AAA 认证，则远程 AAA 服务器上需要配置被认证方的用户名和密码 | 为被认证方配置的用户名和密码必须与被认证方上的配置一致 |

(2) 配置被认证方

**表1-3 配置被认证方**

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 配置本地被对端以PAP方式认证时本地发送的PAP用户名和密码 | **ppp pap local-user** *username* **password** { **cipher** \| **simple** } *string* | 缺省情况下，被对端以PAP方式认证时，本地设备发送的用户名和密码均为空<br>查看加密方式时，无论采用明文或密文加密，默认显示密文方式 |

#### 2. 配置CHAP认证

CHAP 认证分为两种：认证方配置了用户名和认证方没有配置用户名。

(1) 认证方配置了用户名

- 配置认证方

表1-4 配置认证方

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 配置本地认证对端的方式为CHAP | **ppp authentication-mode chap** [ [ **call-in** ] **domain** *isp-name* ] | 缺省情况下，PPP协议不进行认证 |
| 配置采用CHAP认证时认证方的用户名 | **ppp chap user** *username* | 缺省情况下，CHAP认证的用户名为空<br>在被认证方上为认证方配置的用户名必须跟此处配置的一致 |
| 配置本地AAA认证或者远程AAA认证 | 请参见“安全配置指导”中的“AAA”<br>• 若采用本地 AAA 认证，则认证方必须为被认证方配置本地用户的用户名和密码<br>• 若采用远程 AAA 认证，则远程 AAA 服务器上需要配置被认证方的用户名和密码 | 为被认证方配置的用户名必须与被认证方上的配置一致<br>认证方用户的密码和被认证方用户的密码要配置成相同的 |

- 配置被认证方

表1-5 配置被认证方

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 配置采用CHAP认证时被认证方的用户名 | **ppp chap user** *username* | 缺省情况下，CHAP认证的用户名为空<br>在认证方上为被认证方配置的用户名必须跟此处配置的一致 |
| 配置本地AAA认证或者远程AAA认证 | 请参见“安全配置指导”中的“AAA”<br>• 若采用本地 AAA 认证，则被认证方必须为认证方配置本地用户的用户名和密码<br>• 若采用远程 AAA 认证，则远程 AAA 服务器上需要配置认证方的用户名和密码 | 为认证方配置的用户名必须与认证方上的配置一致<br>认证方用户的密码和被认证方用户的密码要配置成相同的 |

(2) 认证方没有配置用户名

- 配置认证方

表1-6 配置认证方

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 配置本地认证对端的方式为CHAP | **ppp authentication-mode chap** [ [ **call-in** ] **domain** *isp-name* ] | 缺省情况下，PPP协议不进行认证 |

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 配置本地AAA认证或者远程AAA认证 | 请参见“安全配置指导”中的“AAA”<br>• 若采用本地 AAA 认证，则认证方必须为被认证方配置本地用户的用户名和密码<br>• 若采用远程 AAA 认证，则远程 AAA 服务器上需要配置被认证方的用户名和密码 | 为被认证方配置的用户名必须与被认证方上的配置一致<br>为被认证方配置的密码必须与被认证方上配置的CHAP认证密码一致 |

- 配置被认证方

**表1-7 配置被认证方**

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 配置采用CHAP认证时被认证方的用户名 | **ppp chap user** *username* | 缺省情况下，CHAP认证的用户名为空<br>在认证方上为被认证方配置的用户名必须跟此处配置的一致 |
| 设置CHAP认证密码 | **ppp chap password** { **cipher** \| **simple** } *password* | 缺省情况下，没有配置进行CHAP认证时采用的密码<br>在认证方上为被认证方配置的密码必须跟此处配置的一致<br>查看加密方式时，无论采用明文或密文加密，默认显示密文方式 |

### 3. 配置MSCHAP或MSCHAPv2 认证

与 CHAP 认证相同，MSCHAP 和 MSCHAPv2 认证也分为两种：认证方配置了用户名和认证方没有配置用户名。

配置 MSCHAP 或 MSCHAPv2 认证时需注意：

- 设备只能作为 MSCHAP 和 MSCHAPv2 的认证方来对其它设备进行认证。
- L2TP 环境下仅支持 MSCHAP 认证，不支持 MSCHAPv2 认证。
- MSCHAPv2 认证只有在 RADIUS 认证的方式下，才能支持修改密码机制。

**表1-8 配置 MSCHAP 或 MSCHAPv2 认证的认证方（认证方配置了用户名）**

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 配置本地认证对端的方式为MSCHAP或MSCHAPv2 | **ppp authentication-mode** { **ms-chap** \| **ms-chap-v2** } [ [ **call-in** ] **domain** *isp-name* ] | 缺省情况下，PPP协议不进行认证 |
| 配置采用MSCHAP或MSCHAPv2认证时认证方的用户名 | **ppp chap user** *username* | 在被认证方上为认证方配置的用户名必须跟此处配置的一致 |

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 配置本地AAA认证或者远程AAA认证 | 请参见“安全配置指导”中的“AAA”<br>• 若采用本地 AAA 认证，则认证方必须为被认证方配置本地用户的用户名和密码<br>• 若采用远程 AAA 认证，则远程 AAA 服务器上需要配置被认证方的用户名和密码 | 为被认证方配置的用户名和密码必须与被认证方上的配置一致 |

表1-9 配置 MSCHAP 或 MSCHAPv2 认证的认证方（认证方没有配置用户名）

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 配置本地认证对端的方式为MSCHAP或MSCHAPv2 | **ppp authentication-mode** { **ms-chap** \| **ms-chap-v2** } [ [ **call-in** ] **domain** *isp-name* ] | 缺省情况下，PPP协议不进行认证 |
| 配置本地AAA认证或者远程AAA认证 | 请参见“安全配置指导”中的“AAA”<br>• 若采用本地 AAA 认证，则认证方必须为被认证方配置本地用户的用户名和密码<br>• 若采用远程 AAA 认证，则远程 AAA 服务器上需要配置被认证方的用户名和密码 | 为被认证方配置的用户名和密码必须与被认证方上的配置一致 |

### 1.2.3 配置轮询功能

PPP 协议使用轮询机制来确认链路状态是否正常。

当接口上封装的链路层协议为 PPP 时，链路层会周期性地向对端发送 keepalive 报文（可以通过 **timer-hold** 命令修改 keepalive 报文的发送周期）。如果接口在 *retry* 个（可以通过 **timer-hold retry** 命令修改该个数）keepalive 周期内无法收到对端发来的 keepalive 报文，链路层会认为对端故障，上报链路层 Down。

如果将 keepalive 报文的发送周期配置为 0 秒，则不发送 keepalive 报文。

在速率非常低的链路上，keepalive 周期和 *retry* 值不能配置过小。因为在低速链路上，大报文可能会需要很长的时间才能传送完毕，这样就会延迟 keepalive 报文的发送与接收。而接口如果在 *retry* 个 keepalive 周期之后仍然无法收到对端的 keepalive 报文，它就会认为链路发生故障。如果 keepalive 报文被延迟的时间超过接口的这个限制，链路就会被认为发生故障而被关闭。

轮询时间间隔设置应小于协商超时时间间隔，否则无法轮询。

表1-10 配置轮询功能

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 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 |

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 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 |

### 1.2.4 配置PPP协商参数

可以配置的 PPP 协商参数包括：

- 协商超时时间间隔
- 协商 IP 地址
- 协商接口 IP 网段
- 协商 DNS 服务器地址
- 协商 ACFC（Address-and-Control-Field-Compression，地址控制字段压缩）
- 协商 PFC（Protocol-Field-Compression，协议字段压缩）

#### 1. 配置协商超时时间间隔

在 PPP 协商过程中，如果在这个时间间隔内没有收到对端的应答报文，则 PPP 将会重发前一次发送的报文。超时时间间隔的取值范围为 1～10 秒。

在 PPP 链路两端设备对 LCP 协商报文的处理速度差异较大的情况下，为避免因一端无法及时处理对端发送的 LCP 协商报文而导致对端重传，可在对协商报文处理速度较快的设备上配置 LCP 协商的延迟时间。配置 LCP 协商的延时时间后，当接口物理层 UP 时 PPP 将在延时时间超时后才会主动进行 LCP 协商；如果在延时时间内本端设备收到对端设备发送的 LCP 协商报文，则本端设备将不再等待延时时间超时，而是直接进行 LCP 协商。

**表1-11 配置协商超时时间间隔**

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 配置协商超时时间间隔 | **ppp timer negotiate** *seconds* | 缺省情况下，协商超时时间间隔为3秒 |
| （可选）配置LCP协商的延迟时间 | **ppp lcp delay** *milliseconds* | 缺省情况下，接口物理层UP后，PPP立即进行LCP协商 |

#### 2. 配置PPP协商IP地址

(1) 配置 Client 端

**表1-12 配置 Client 端**

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 进入接口视图 | **interface** *interface-type interface-number* | - |

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 为接口配置IP地址可协商属性 | **ip address ppp-negotiate** | 缺省情况下，接口没有配置IP地址可协商属性<br>本命令和**ip address**命令互斥，二者不能同时配置。关于**ip address**命令的详细介绍，请参见“三层技术-IP业务命令参考”中的“IP地址” |

(2) 配置 Server 端

在下列三种 Server 端分配 IP 地址的方式下 Server 端需要进行配置：

- 在接口下指定为 Client 端分配的 IP 地址。
- 从接口下指定的地址池中分配 IP 地址。
- 从 ISP 域下关联的地址池中分配 IP 地址。

这三种方式中，不同 PPP 用户可以采用的方式如下：

- 不需要进行 PPP 认证的 PPP 用户可以使用两种方式：在接口下指定为 Client 端分配的 IP 地址和从接口下指定的地址池中分配 IP 地址。这两种方式不能同时使用。
- 需要进行PPP认证的PPP用户可以使用全部的三种方式。用户可以同时配置多种方式。同时配置多种方式时，以 ISP 域下关联的地址池优先，然后是接口下指定为 Client 端分配的 IP 地址或者地址池（接口下的这两种方式不能同时使用）。

PPP 可以使用两类地址池为对端分配 IP 地址：PPP 地址池、DHCP 地址池，优先采用 PPP 地址池。如果用户配置了名称相同的 PPP 地址池和 DHCP 地址池，并采用该名称的地址池来分配 IP 地址，则系统只会使用 PPP 地址池来分配 IP 地址。

表1-13 配置 Server 端（在接口下指定为 Client 端分配的 IP 地址）

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 配置接口为Client端分配的IP地址 | **remote address** *ip-address* | 缺省情况下，接口不为Client端分配IP地址 |
| 配置Server端的IP地址 | **ip address** *ip-address* | 缺省情况下，接口没有配置IP地址 |

表1-14 配置 Server 端（从接口下指定的 PPP 地址池中分配 IP 地址）

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 配置PPP地址池 | **ip pool** *pool-name start-ip-address* [ *end-ip-address* ] [ **group** *group-name* ] | 缺省情况下，没有配置PPP地址池 |
| （可选）配置PPP地址池的网关地址 | **ip pool** *pool-name* **gateway** *ip-address* [ **vpn-instance** *vpn-instance-name* ] | 缺省情况下，没有为PPP地址池配置网关地址 |

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| （可选）配置PPP地址池路由 | **ppp ip-pool route** *ip-address* { *mask-length* \| *mask* } [ **vpn-instance** *vpn-instance-name* ] | 缺省情况下，没有配置PPP地址池路由<br>用户需要保证配置的PPP地址池路由网段覆盖PPP地址池网段范围 |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 使用PPP地址池为Client端分配IP地址 | **remote address pool** *pool-name* | 缺省情况下，接口不为Client端分配IP地址 |
| （可选）配置Server端的IP地址 | **ip address** *ip-address* | 缺省情况下，接口没有配置IP地址<br>配置了PPP地址池的网关地址后，可以不用配置本命令 |

表1-15 配置 Server 端（从接口下指定的 DHCP 地址池中分配 IP 地址）

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 配置DHCP功能 | • 如果 Server 端同时作为 DHCP 服务器，则在 Server 端上配置 DHCP 服务器、DHCP 地址池相关内容<br>• 如果 Server 端作为 DHCP 中继，则在 Server 端上配置 DHCP 中继相关内容（必须配置 DHCP 中继用户地址表项记录功能、DHCP 中继地址池），并在远端 DHCP 服务器上配置 DHCP 地址池 | DHCP的具体配置介绍请参见“三层技术-IP业务配置指导”中的“DHCP” |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 使用DHCP地址池为Client端分配IP地址 | **remote address pool** *pool-name* | 缺省情况下，接口不为Client端分配IP地址 |
| 配置Server端的IP地址 | **ip address** *ip-address* | 缺省情况下，接口没有配置IP地址 |
| （可选）配置使用PPP用户名作为DHCP客户端ID | **remote address dhcp client-identifier username** | 缺省情况下，未使用PPP用户名作为DHCP客户端ID |

表1-16 配置 Server 端（从 ISP 域下关联的 PPP 地址池中分配 IP 地址）

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 配置PPP地址池 | **ip pool** *pool-name start-ip-address* [ *end-ip-address* ] **group** *group-name* | 缺省情况下，没有配置PPP地址池 |
| （可选）配置PPP地址池的网关地址 | **ip pool** *pool-name* **gateway** *ip-address* [ **vpn-instance** *vpn-instance-name* ] | 缺省情况下，没有为PPP地址池配置网关地址 |

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| （可选）配置PPP地址池路由 | **ppp ip-pool route** *ip-address* { *mask-length* \| *mask* } [ **vpn-instance** *vpn-instance-name* ] [ **vsrp-instance** *vsrp-instance-name* ] | 缺省情况下，没有配置PPP地址池路由<br>用户需要保证配置的PPP地址池路由网段覆盖PPP地址池网段范围 |
| 进入ISP域视图 | **domain** *isp-name* | - |
| 在ISP域下关联PPP地址池为Client端分配IP地址 | **authorization-attribute ip-pool** *pool-name* | 缺省情况下，ISP域下没有关联PPP地址池<br>本命令的详细介绍请参见“安全命令参考”中的“AAA” |
| 退回系统视图 | **quit** | - |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| （可选）配置Server端的IP地址 | **ip address** *ip-address* | 缺省情况下，接口没有配置IP地址<br>配置了PPP地址池的网关地址后，可以不用配置本命令 |

表1-17 配置 Server 端（从 ISP 域下关联的 DHCP 地址池中分配 IP 地址）

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 配置DHCP功能 | • 如果 Server 端同时作为 DHCP 服务器，则在 Server 端上配置 DHCP 服务器、DHCP 地址池相关内容<br>• 如果 Server 端作为 DHCP 中继，则在 Server 端上配置 DHCP 中继相关内容（必须配置 DHCP 中继用户地址表项记录功能、DHCP 中继地址池），并在远端 DHCP 服务器上配置 DHCP 地址池 | DHCP的具体配置介绍请参见“三层技术-IP业务配置指导”中的“DHCP” |
| 进入ISP域视图 | **domain** *isp-name* | - |
| 在ISP域下关联DHCP地址池为Client端分配IP地址 | **authorization-attribute ip-pool** *pool-name* | 缺省情况下，ISP域下没有关联DHCP地址池<br>本命令的详细介绍请参见“安全命令参考”中的“AAA” |
| 退回系统视图 | **quit** | - |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 配置Server端的IP地址 | **ip address** *ip-address* | 缺省情况下，接口没有配置IP地址 |
| （可选）配置使用PPP用户名作为DHCP客户端ID | **remote address dhcp client-identifier username** | 缺省情况下，未使用PPP用户名作为DHCP客户端ID |

### 3. 配置接口IP网段检查

使能接口的 IP 网段检查功能后，当 IPCP 协商时，本地会检查对端的 IP 地址与本端接口的 IP 地址是否在同一网段，如果不在同一网段，则 IPCP 协商失败。

如果接口的 IP 网段检查功能处于关闭状态，则在 IPCP 协商阶段不进行接口 IP 网段检查。

表1-18 配置接口 IP 网段检查

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 使能接口的IP网段检查功能 | **ppp ipcp remote-address match** | 缺省情况下，接口的IP网段检查功能处于关闭状态 |

### 4. 配置DNS服务器地址协商

(1) 配置 Client 端

正常情况下，Client 端配置了 **ppp ipcp dns request** 命令，Server 端才会为本端指定 DNS 服务器地址。但是有一些特殊的设备，Client 端并未请求，Server 端却要强制为 Client 端指定 DNS 服务器地址，从而导致协商不通过，为了适应这种情况，Client 端可以配置 **ppp ipcp dns admit-any** 命令。

表1-19 配置 Client 端

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 配置设备主动请求对端指定DNS服务器地址 | **ppp ipcp dns request** | 缺省情况下，禁止设备主动向对端请求DNS服务器地址 |
| 配置设备可以被动地接收对端指定的DNS服务器地址，即设备不发送DNS请求，也能接收对端设备分配的DNS服务器地址 | **ppp ipcp dns admit-any** | 缺省情况下，设备不会被动地接收对端设备指定的DNS服务器的IP地址<br>在配置了**ppp ipcp dns request**命令的情况下不用配置本命令 |

(2) 配置 Server 端

表1-20 配置 Server 端

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 进入接口视图 | **interface** *interface-type interface-number* | - |

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 配置设备为对端设备指定DNS服务器地址 | **ppp ipcp dns** *primary-dns-address* [ *secondary-dns-address* ] | 缺省情况下，设备不为对端设备指定DNS服务器的IP地址<br>收到Client端的请求后，Server端才会为对端指定DNS服务器地址 |

### 5. 配置ACFC协商

缺省情况下，PPP 报文中的地址字段的值固定为 0xFF，控制字段的值固定为 0x03，既然这两个字段的值是固定的，就可以对这两个字段进行压缩。

ACFC 协商选项字段用来通知对端，本端可以接收地址和控制字段被压缩的报文。

ACFC 协商在 LCP 协商阶段进行，当协商通过后，对于发送的非 LCP 报文将进行地址控制字段压缩，不再添加地址控制字段，以增加链路的有效载荷；对于 LCP 报文不进行地址控制字段压缩，以确保 LCP 协商过程顺利进行。

建议在低速链路上配置本功能。

(1) 配置本地发送 ACFC 协商请求

**表1-21 配置本地发送 ACFC 协商请求**

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 配置本地发送ACFC协商请求，即LCP协商时本地发送的协商请求携带ACFC协商选项 | **ppp acfc local-request** | 缺省情况下，LCP协商时本地发送的协商请求不携带ACFC协商选项 |

(2) 配置拒绝对端的 ACFC 协商请求

**表1-22 配置拒绝对端的 ACFC 协商请求**

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 配置拒绝对端的ACFC协商请求，即LCP协商时拒绝对端携带的ACFC协商选项 | **ppp acfc remote-reject** | 缺省情况下，接受对端的ACFC协商请求，即LCP协商时接受对端携带的ACFC协商选项，并且发送的报文进行地址控制字段压缩 |

### 6. 配置PFC协商

缺省情况下，PPP 报文中的协议字段长度为 2 字节，然而，目前典型的协议字段取值都小于 256，所以可以压缩成一个字节来区分协议类型。

PFC 协商选项字段用来通知对端，本端可以接收协议字段被压缩成一个字节的报文。

PFC 协商在 LCP 协商阶段进行，当协商通过后，对于发送的非 LCP 报文将进行协议字段压缩，如果协议字段的头 8 比特为全零，则不添加此 8 比特，以增加链路的有效载荷；对于 LCP 报文不进行协议字段压缩，以确保 LCP 协商过程顺利进行。

建议在低速链路上配置本功能。

(1) 配置本地发送 PFC 协商请求

**表1-23 配置本地发送 PFC 协商请求**

| 操作 | 命令 | 说明 |
|---|---|---|
| 进入系统视图 | **system-view** | - |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 配置本地发送PFC协商请求，即LCP协商时本地发送的协商请求携带PFC协商选项 | **ppp pfc local-request** | 缺省情况下，LCP协商时本地发送的协商请求不携带PFC协商选项 |

(2) 配置拒绝对端的 PFC 协商请求

**表1-24 配置拒绝对端的 PFC 协商请求**

| 操作 | 命令 | 说明 |
|---|---|---|
| 进入系统视图 | **system-view** | - |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 配置拒绝对端的PFC协商请求，即LCP协商时拒绝对端携带的PFC协商选项 | **ppp pfc remote-reject** | 缺省情况下，接受对端的PFC协商请求，即LCP协商时接受对端携带的PFC协商选项，并且发送的报文进行协议字段压缩 |

### 1.2.5 配置PPP IPHC压缩功能

IPHC（IP Header Compression，IP 报文头压缩）协议主要应用于低速链路上的语音通信。

在低速链路上，每个语音报文中报文头消耗大部分的带宽。比如，G.729 编码 20ms 打包时长 PPP 链路，每秒传送 1000/20=50 个语音报文，每个语音报文中都包含 46 字节的报文头（6 字节 PPP 头、20 字节 IP 头、8 字节 UDP 头、12 字节 RTP 头），这样每一路语音数据所占的带宽为：（6+20+8+12）*8*50+8000（语音净荷所占带宽）=26.4kbps，传送 RTP/UDP/IP 头所花的带宽开销还是很大的，为（20+8+12）*8*50=16kbps，占语音数据总带宽的百分比为 16k/26.4k=60.1%，网络带宽利用率很差。为了减少报文头对带宽的消耗，可以在 PPP 链路上使用 IPHC 压缩功能，对报文头进行压缩。

IPHC 压缩分为如下两种：

- RTP 头压缩：对报文中的 RTP/UDP/IP 头（长度共 40 字节）进行压缩。
- TCP 头压缩：对报文中的 TCP/IP 头（长度共 40 字节）进行压缩。

IPHC 压缩机制的总体思想是：在一次连接过程中，IP 头、UDP 头、RTP 头以及 TCP 头中的一些字段是固定不变的，还有一些字段是有规律变化的，这样在压缩端和解压端分别维护一个压缩表项和解压缩表项来保存固定不变的字段和有规律变化的字段，在传输过程中，压缩端不需要发送完整

的报文头，只发送报文头中有变化的信息，减少了报文头信息的长度，从而降低了报文头所占的带宽。

(1) 在压缩过程中，压缩端会将变化的字段编码到报文中；对于有规律变化的字段，其二次差分值为零时则不需要携带，其二次差分值不为零时，则其标志位置 1，并将其一次差分值和标志位字段编码到报文中。

(2) 在解压过程中，解压端跟据解压缩表项还原固定不变的字段，对于有规律变化的字段，若其标志位为 0，则按其变化规律做相应计算还原；若其标志位为 1，则根据报文中携带的该字段的一次差分值和解压缩表项中该字段的信息进行计算还原。

举例说明：在压缩 TCP 头时，Destination Port 为固定不变的字段，在报文中不用携带；URG 为变化的字段，在报文中携带；Sequence Number 为有规律变化的字段（一般情况下是每次增加 1），压缩端首先计算被压缩报文的 Sequence Number 字段和压缩表项中的 Sequence Number 字段的差值，即一次差分值，如果一次差分值为 1，那么其二次差分值为 1-1=0，则这个字段就不用携带，解压端会自动加 1 还原；如果其一次差分值不为 1，比如为 2，那么二次差分值就为 2-1=1，这时就会置位 Sequence Number 的标志位，并将一次差分值 2 编码到报文中，解压端会在解压缩表项中的 Sequence Number 字段上加 2 还原。

配置本功能时需要注意：

- 用户必须在链路的两端同时开启 IPHC 压缩功能，该功能才生效。
- 在虚拟模板接口、Dialer 接口、ISDN 接口上开启/关闭 IPHC 压缩功能时，配置不会立即生效，只有对此接口或者其绑定的物理接口进行 **shutdown/undo shutdown** 操作后，配置才能生效。
- 只有在开启 IPHC 压缩功能后，才能配置接口上允许进行 RTP 头/TCP 头压缩的最大连接数，并且需要对接口进行 **shutdown/undo shutdown** 操作后，配置才能生效。在关闭 IPHC 压缩功能后，配置将被清除。

表1-25 配置 PPP IPHC 压缩功能

| 操作 | 命令 | 说明 |
|---|---|---|
| 进入系统视图 | **system-view** | - |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 开启PPP IPHC压缩功能 | **ppp compression iphc enable** [ **nonstandard** ] | 缺省情况下，IPHC压缩功能处于关闭状态<br>与友商设备互通时需要配置**nonstandard**参数 |
| 配置接口上允许进行RTP头压缩的最大连接数 | **ppp compression iphc rtp-connections** *number* | 缺省情况下，接口上允许进行RTP头压缩的最大连接数为16 |
| 配置接口上允许进行TCP头压缩的最大连接数 | **ppp compression iphc tcp-connections** *number* | 缺省情况下，接口上允许进行TCP头压缩的最大连接数为16 |

### 1.2.6 配置PPP链路质量监测功能

PPP 链路质量监测功能可以实时对 PPP 链路的通信质量（丢包率和错包率）进行监测。

在没有配置 PPP 链路质量监测功能之前，PPP 接口（封装 PPP 协议的接口）会每隔一段时间向对端发送 keepalive 报文；在配置此功能之后，PPP 接口会用 LQR（Link Quality Reports，链路质量报告）报文代替 keepalive 报文，即每隔一段时间向对端发送 LQR 报文，用以对链路情况进行监测。

当链路质量正常时，系统对每个 LQR 报文进行链路质量计算，如果连续两次链路质量低于用户设置的禁用链路质量百分比，链路会被禁用。当链路被禁用后，系统每隔十个 LQR 报文进行一次链路质量计算，只有连续三次链路质量高于用户设置的恢复链路质量百分比，链路才会被恢复。因此，当链路被禁用后，至少要在 30 个 keepalive 周期后才能恢复。如果 keepalive 周期设置过大，可能会导致链路长时间无法恢复。

配置本功能时需要注意：

- 当在 PPP 链路两端同时开启链路质量监测功能时，两端设备的参数必须相等。一般来说，不建议在链路两端同时开启链路质量监测功能。
- 不建议在拨号线路上开启 PPP 链路质量监测功能。当在拨号线路上开启链路质量监测功能后，由于拨号线路的特点，一旦链路被禁用，DDR 模块就会把拨号线路挂断，因此链路质量监测就不能正常的运行。只有当有数据需要传输时，DDR 模块把拨号线路重新呼起，链路质量监测功能才能恢复正常。

表1-26 配置 PPP 链路质量监测功能

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 开启PPP链路质量监测功能 | **ppp lqm close-percentage** *close-percentage* [ **resume-percentage** *resume-percentage* ] | 缺省情况下，PPP链路质量监测功能处于关闭状态。设备支持情况请参考命令参考中的相关描述 |
| 配置当链路质量监测功能监测到链路质量低时向对端发送LCP echo报文 | **ppp lqm lcp-echo** [ **packet** *size* ] [ **interval** *interval* ] | 缺省情况下，当链路质量监测功能监测到链路质量低时不向对端发送LCP echo报文。设备支持情况请参考命令参考中的相关描述 |

## 1.2.7 配置PPP计费统计功能

PPP 协议可以为每条 PPP 链路提供基于流量的计费统计功能，具体统计内容包括出入两个方向上流经本链路的报文数和字节数。AAA 可以获取这些流量统计信息用于计费控制。关于 AAA 计费的详细介绍请参见“安全配置指导”中的“AAA”。

表1-27 配置 PPP 计费统计功能

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 进入接口视图 | **interface** *interface-type interface-number* | - |
| 开启PPP计费统计功能 | **ppp account-statistics enable** [ **acl** { *acl-number* \| **name** *acl-name* } ] | 缺省情况下，PPP计费统计功能处于关闭状态 |

### 1.2.8 配置PPP用户的nas-port-type属性

本特性用来配置 RADIUS 认证计费时所携带的 nas-port-type 属性。关于 nas-port-type 属性的详细介绍请参见 RFC 2865。

表1-28 配置 PPP 用户的 nas-port-type 属性

| 操作 | 命令 | 说明 |
|---|---|---|
| 进入系统视图 | **system-view** | - |
| 进入虚拟模板接口视图 | **interface virtual-template** *number* | - |
| 配置接口的nas-port-type属性 | **nas-port-type** { **802.11** \| **adsl-cap** \| **adsl-dmt** \| **async** \| **cable** \| **ethernet** \| **g.3-fax** \| **hdlc** \| **idsl** \| **isdn-async-v110** \| **isdn-async-v120** \| **isdn-sync** \| **piafs** \| **sdsl** \| **sync** \| **virtual** \| **wireless-other** \| **x.25** \| **x.75** \| **xdsl** } | 缺省情况下，nas-port-type属性由PPP用户的业务类型和承载链路类型决定：<br>• 如果是 PPPoE 业务，当承载链路类型为三层虚拟以太网接口时，nas-port-type 属性为 **xdsl**，否则 nas-port-type 属性为 **ethernet**<br>• 如果是 PPPoA 业务，nas-port-type 属性为 **xdsl**<br>• 如果是 L2TP 业务，nas-port-type 属性为 **virtual** |

## 1.3 PPP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 PPP 配置后的运行情况，通过查看显示信息验证配置的效果。

在用户视图下执行 **reset** 命令可以清除相应接口的统计信息。

表1-29 PPP 显示和维护

| 操作 | 命令 |
|---|---|
| 显示PPP接入用户的信息 | **display ppp access-user** { **interface** *interface-type interface-number* [ **count** ] \| **ip-address** *ip-address* \| **ipv6-address** *ipv6-address* \| **username** *user-name* \| **user-type** { **lac** \| **lns** \| **pppoa** \| **pppoe** } [ **count** ] } |
| 显示PPP地址池的信息 | **display ip pool** [ *pool-name* \| **group** *group-name* ] |
| 显示IPHC压缩的统计信息 | **display ppp compression iphc** { **rtp** \| **tcp** } [ **interface** *interface-type interface-number* ] |
| 显示虚拟模板接口的相关信息 | **display interface** [ **virtual-template** [ *interface-number* ] ] [ **brief** [ **description** \| **down** ] ] |
| 显示虚拟访问接口的相关信息 | **display interface** [ **virtual-access** [ *interface-number* ] ] [ **brief** [ **description** \| **down** ] ] |
| 清除IPHC压缩的统计信息 | **reset ppp compression iphc** [ **rtp** \| **tcp** ] [ **interface** *interface-type interface-number* ] |
| 强制PPP用户下线 | **reset ppp access-user** { **ip-address** *ip-address* [ **vpn-instance** *ipv4-vpn-instance-name* ] \| **ipv6-address** *ipv6-address* [ **vpn-instance** *ipv6-vpn-instance-name* ] \| **username** *user-name* } |

| 操作 | 命令 |
| --- | --- |
| 清除VA接口的统计信息 | **reset counters interface** [ **virtual-access** [ *interface-number* ] ] |

# 2 PPPoE

设备各款型对于本节所描述的特性支持情况有所不同，详细差异信息如下：

| 型号 | 特性 | 描述 |
| --- | --- | --- |
| F5000-M06 | PPPoE | 不支持 |
| F5000-G20 | | 支持 |
| F1000-G20/G50/G60/G80 | | 支持 |

## 2.1 PPPoE简介

PPPoE（Point-to-Point Protocol over Ethernet，在以太网上承载 PPP 协议）的提出，解决了 PPP 无法应用于以太网的问题，是对 PPP 协议的扩展。

### 2.1.1 PPPoE概述

PPPoE 描述了在以太网上建立 PPPoE 会话及封装 PPP 报文的方法。要求通信双方建立的是点到点关系，而不是在以太网中所出现的点到多点关系。

PPPoE 利用以太网将大量主机组成网络，然后通过一个远端接入设备为以太网上的主机提供互联网接入服务，并对接入的每台主机实现控制、认证、计费功能。由于很好地结合了以太网的经济性及 PPP 良好的可扩展性与管理控制功能，PPPoE 被广泛应用于小区接入组网等环境中。

PPPoE 协议将 PPP 报文封装在以太网帧之内，在以太网上提供点对点的连接。

关于 PPPoE 的详细介绍，可以参考 RFC 2516。

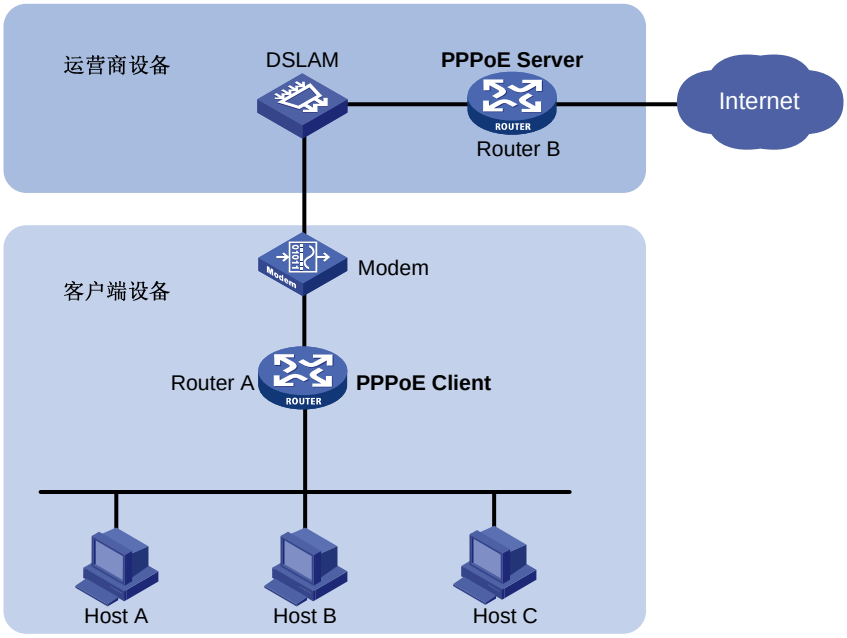
### 2.1.2 PPPoE组网结构

PPPoE 使用 Client/Server 模型。PPPoE Client 向 PPPoE Server 发起连接请求，两者之间会话协商通过后，就建立 PPPoE 会话，此后 PPPoE Server 向 PPPoE Client 提供接入控制、认证、计费等功能。

根据 PPPoE 会话的起点所在位置的不同，有两种组网结构：

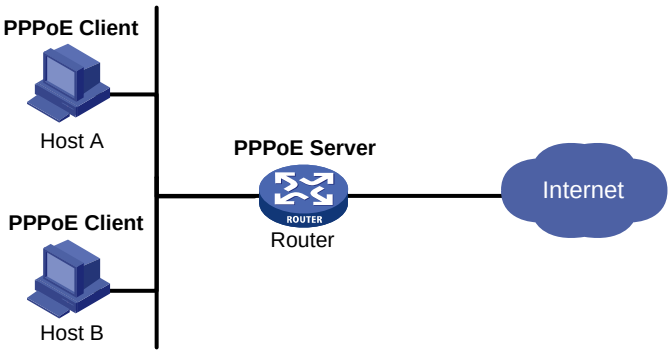
- 第一种方式是在两台路由器之间建立 PPPoE 会话，所有主机通过同一个 PPPoE 会话传送数据，主机上不用安装 PPPoE 客户端拨号软件，一般是一个企业共用一个账号接入网络（图中 PPPoE Client 位于企业/公司内部，PPPoE Server 是运营商的设备）。

图2-1 PPPoE 组网结构图 1




- 第二种方式是将 PPPoE 会话建立在 Host 和运营商的路由器之间，为每一个 Host 建立一个 PPPoE 会话，每个 Host 都是 PPPoE Client，每个 Host 使用一个帐号，方便运营商对用户进行计费和控制。Host 上必须安装 PPPoE 客户端拨号软件。

图2-2 PPPoE 组网结构图 2




## 2.2 配置PPPoE

设备作为PPPoE Client时，配置过程请参见“2.2.1 配置PPPoE Client。

### 2.2.1 配置PPPoE Client

PPPoE Client 的配置包括配置拨号接口和配置 PPPoE 会话。

PPPoE 会话有三种工作模式：永久在线模式、按需拨号模式、诊断模式。

- 永久在线模式：当物理线路 up 后，设备会立即发起 PPPoE 呼叫，建立 PPPoE 会话。除非用户删除 PPPoE 会话，否则此 PPPoE 会话将一直存在。
- 按需拨号模式：当物理线路 up 后，设备不会立即发起 PPPoE 呼叫，只有当有数据需要传送时，设备才会发起 PPPoE 呼叫，建立 PPPoE 会话。如果 PPPoE 链路的空闲时间超过用户配置的值，设备会自动中止 PPPoE 会话。
- 诊断模式：设备在配置完成后立即发起 PPPoE 呼叫，建立 PPPoE 会话。每隔用户配置的重建时间间隔，设备会自动断开该会话、并重新发起呼叫建立会话。通过定期建立、删除 PPPoE 会话，可以监控 PPPoE 链路是否处于正常工作状态。

PPPoE 会话的工作模式由对应的拨号接口的配置决定：

- 当 Dialer 接口的链路空闲时间（通过 **dialer timer idle** 命令配置）配置为 0，且 Dialer 接口上没有配置 **dialer diagnose** 命令时，PPPoE 会话将工作在永久在线模式。
- 当 Dialer 接口的链路空闲时间（通过 **dialer timer idle** 命令配置）配置不为 0，且 Dialer 接口上没有配置 **dialer diagnose** 命令时，PPPoE 会话将工作在按需拨号模式。
- 当 Dialer 接口上配置了 **dialer diagnose** 命令时，PPPoE 会话将工作在诊断模式。

### 1. 配置拨号接口

在配置 PPPoE 会话之前，需要先配置一个 Dialer 接口，并在接口上使能共享 DDR。每个 PPPoE 会话唯一对应一个 Dialer bundle，而每个 Dialer bundle 又唯一对应一个 Dialer 接口。这样就相当于通过一个 Dialer 接口可以创建一个 PPPoE 会话。

配置拨号接口

| 操作 | 命令 | 说明 |
|---|---|---|
| 进入系统视图 | **system-view** | - |
| 创建拨号访问组，并配置拨号控制规则 | **dialer-group** *group-number* **rule** { *protocol-name* { **deny** \| **permit** } \| **acl** { *acl-number* \| **name** *acl-name* } } | 缺省情况下，不存在拨号访问组 |
| 创建Dialer接口，并进入该Dialer接口视图 | **interface dialer** *number* | - |
| 配置接口IP地址 | **ip address** { *address mask* \| **ppp-negotiate** } | 缺省情况下，接口没有配置IP地址 |
| 使能共享DDR | **dialer bundle enable** | 缺省情况下，接口上不使能任何类型的DDR |
| 配置该拨号接口关联的拨号访问组，将该接口与拨号控制规则关联起来 | **dialer-group** *group-number* | 缺省情况下，接口不与任何拨号访问组相关联 |
| 配置链路空闲时间 | **dialer timer idle** *idle* [ **in** \| **in-out** ] | 缺省情况下，链路空闲时间为120秒<br>当*idle*配置为0时，PPPoE会话工作在永久在线模式下，否则工作在按需拨号模式下 |
| 配置DDR应用工作在诊断模式 | **dialer diagnose** [ **interval** *interval* ] | 缺省情况下，工作在非诊断模式<br>当工作在诊断模式时，链路空闲时间无效 |

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 配置DDR自动拨号的间隔时间 | **dialer timer autodial** *autodial-interval* | 缺省情况下，DDR自动拨号的间隔时间为300秒<br>当工作在永久在线模式或者诊断模式情况下，链路断开后将启动自动拨号定时器，等待自动拨号定时器超时后再重新发起呼叫<br>为了在链路断开时可以尽快自动重新拨号，建议将自动拨号的时间间隔配置的小一些 |
| 配置Dialer接口的MTU值 | **mtu** *size* | 缺省情况下，Dialer接口的MTU值为1500字节<br>对于PPPoE Client应用的Dialer接口，应修改其MTU值，保证分片后的报文加上2个字节的PPP头和6个字节的PPPoE头之后的总长度不超过对应PPPoE会话所在接口的MTU值 |

### 2. 配置PPPoE会话

表2-1 配置 PPPoE 会话

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入系统视图 | **system-view** | - |
| 进入三层以太网接口视图/三层以太网子接口视图/VLAN接口视图 | **interface** *interface-type interface-number* | - |
| 建立一个PPPoE会话，并且指定该会话所对应的Dialer bundle | **pppoe-client dial-bundle-number** *number* [ **no-hostuniq** ] | 缺省情况下，没有配置PPPoE会话<br>该Dialer bundle的序号*number*与Dialer接口的编号相同 |

### 3. 复位PPPoE会话

当 PPPoE 会话工作在永久在线模式时，如果使用 **reset pppoe-client** 命令复位 PPPoE 会话，设备会在自动拨号定时器超时后自动重新建立 PPPoE 会话。

当 PPPoE 会话工作在按需拨号模式时，如果使用 **reset pppoe-client** 命令复位 PPPoE 会话，设备会在有数据需要传送时，才重新建立 PPPoE 会话。

表2-2 复位 PPPoE 会话

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 复位PPPoE会话 | **reset pppoe-client** { **all** \| **dial-bundle-number** *number* } | 请在用户视图下进行该操作 |

## 2.3 PPPoE显示和维护

### 2.3.1 PPPoE Client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 PPPoE Client 配置后的运行情况，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 PPPoE 会话的协议报文统计信息。

表2-3 PPPoE Client 显示和维护

| 操作 | 命令 |
| --- | --- |
| 显示PPPoE会话的概要信息 | **display pppoe-client session summary** [ **dial-bundle-number** *number* ] |
| 显示PPPoE会话的协议报文统计信息 | **display pppoe-client session packet** [ **dial-bundle-number** *number* ] |
| 清除PPPoE会话的协议报文统计信息 | **reset pppoe-client session packet** [ **dial-bundle-number** *number* ] |

# 目 录

# 1 L2TP

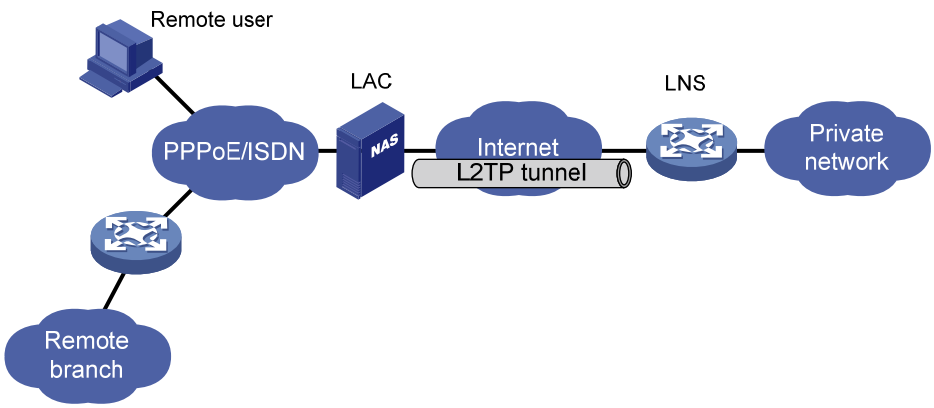
## 1.1 L2TP简介

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。

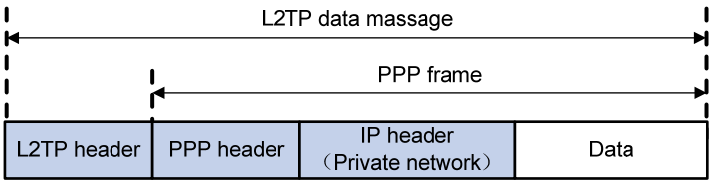
LNS 作为 L2TP 隧道的另一侧端点，是 LAC 通过隧道传输的 PPP 会话的逻辑终点。L2TP 通过在公共网络中建立 L2TP 隧道，将远端系统的 PPP 连接由原来的 NAS 延伸到了企业内部网络的 LNS 设备。

### 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。

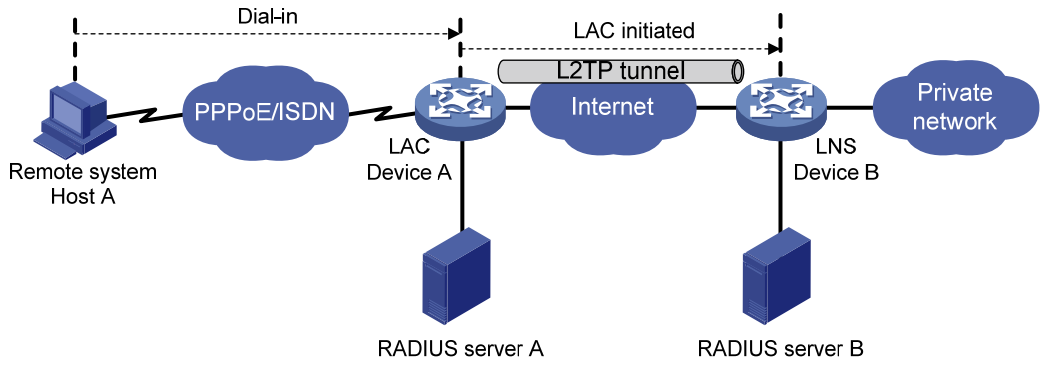
### 1.1.4 L2TP隧道模式及隧道建立过程

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。

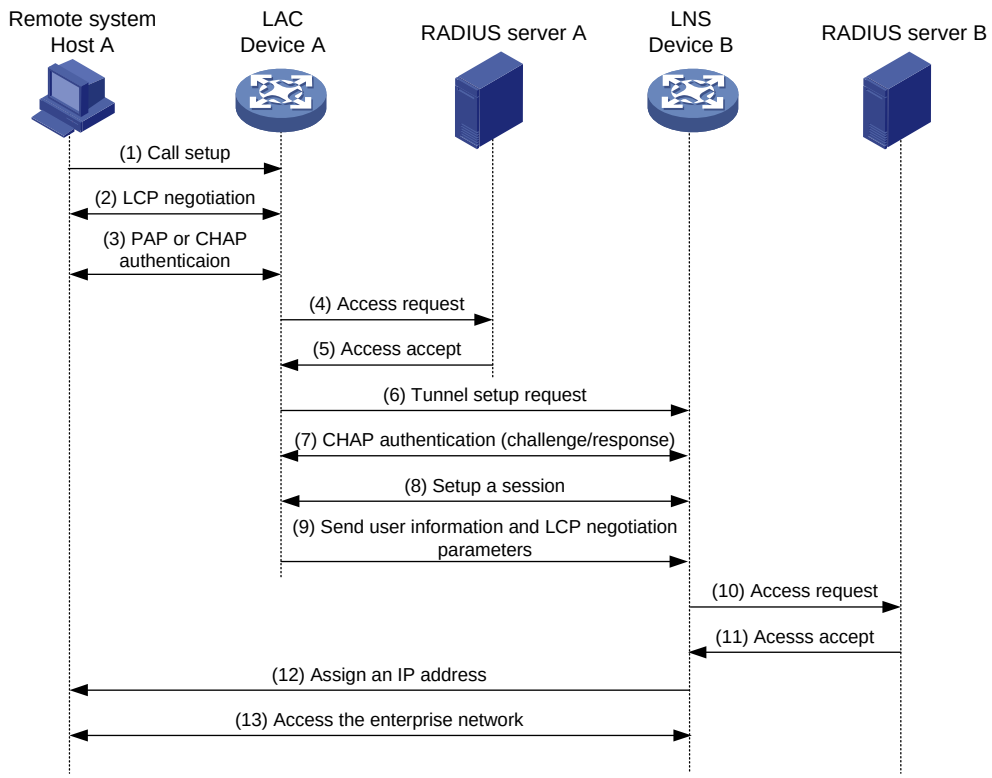
图1-4 NAS-Initiated 模式 L2TP 隧道示意图




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，LNS 为 Host A 分配一个企业网内部的 IP 地址。

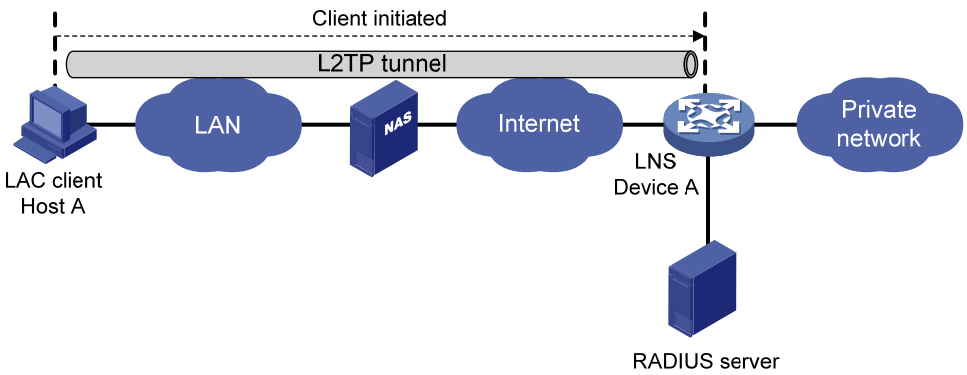
(13) 获得 IP 地址后，PPP 用户可以通过 Host A 访问企业内部资源。

在步骤(12)和(13)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

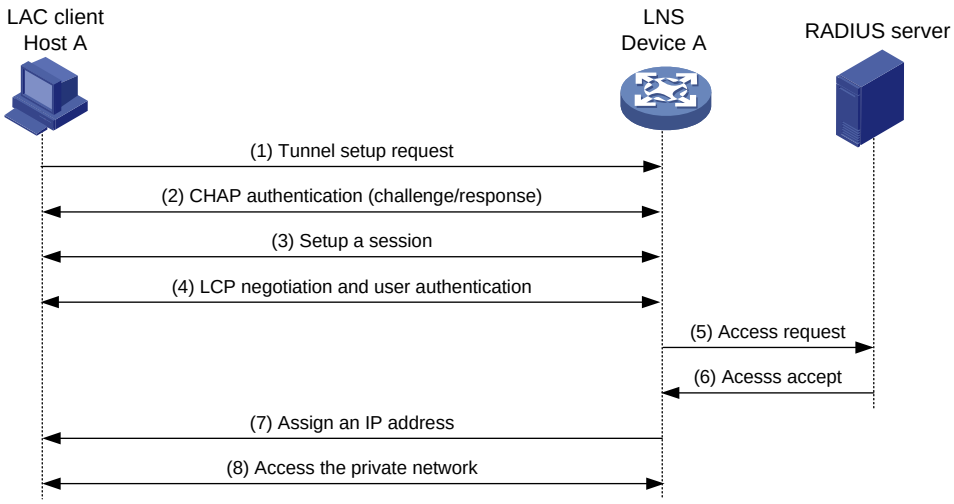



Client-Initiated 模式 L2TP 隧道具有如下特点：

- 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

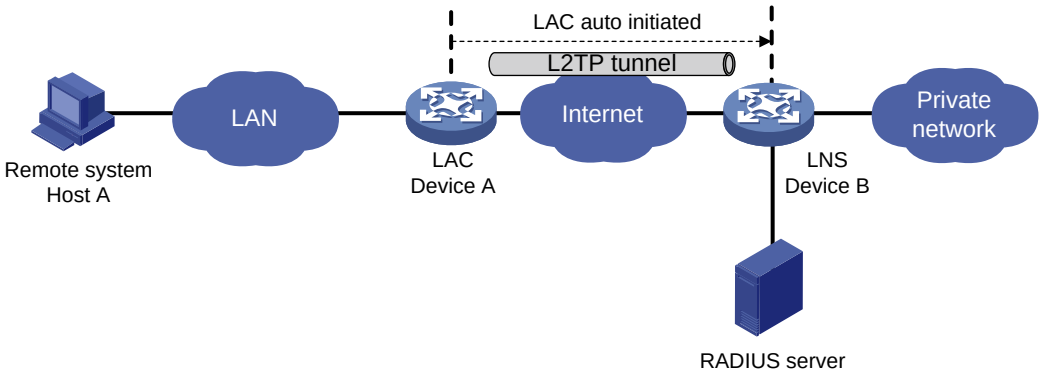



### 3. LAC-Auto-Initiated模式

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

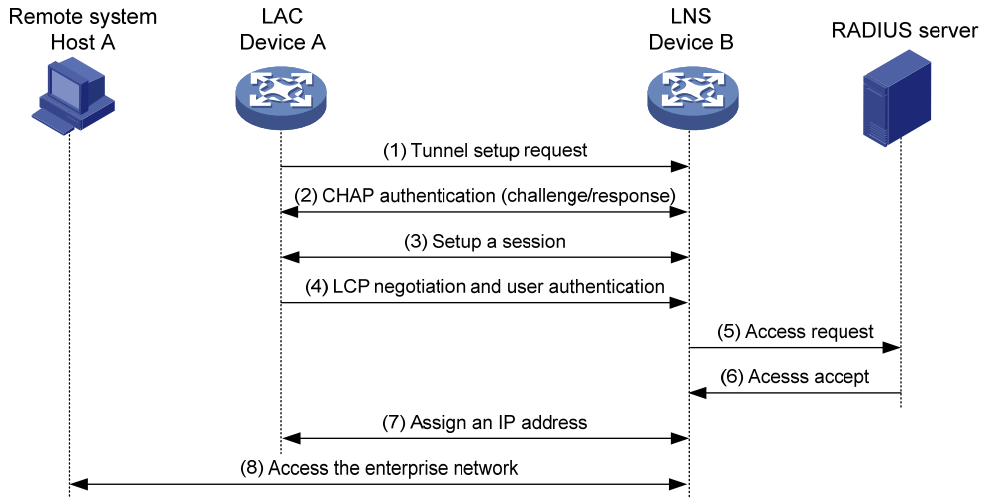



LAC-Auto-Initiated 模式 L2TP 隧道具有如下特点：

- 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<br>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<br>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<br>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。

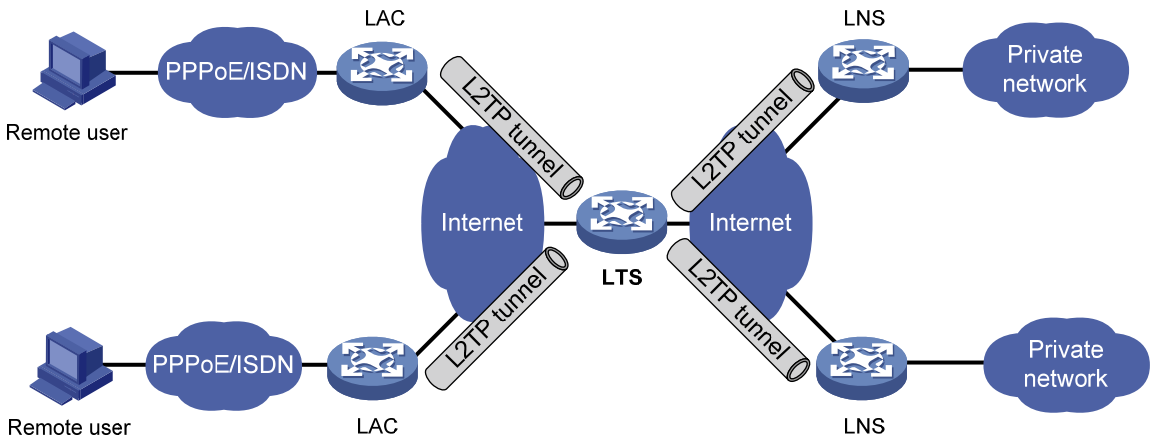
### 8. 支持L2TP隧道交换

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 |
| | 配置隧道对端所属的VPN | | 1.6.5 |
| | 配置LTS设备的TSA ID | | 1.6.6 |

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 |
| | 配置隧道对端所属的VPN | | 1.6.5 |
| | 配置LTS设备的TSA ID | | 1.6.6 |

## 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，设备上未配置任何L2TP组<br>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<br>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。但当 LAC 和 LNS 之间存在等价路由时，必须将 L2TP 隧道的源端地址通过 source-ip 命令配置或通过 RADIUS 服务器授权为设备上某 LoopBack 接口的 IP 地址。

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** | - |

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 进入LAC模式的L2TP组视图 | **l2tp-group** *group-number* [ **mode lac** ] | - |
| 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，设备上未配置任何虚拟PPP接口 |
| 配置虚拟PPP接口的IP地址 | **ip address** *address mask* | 二者选其一<br>缺省情况下，未配置接口的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” | - |

| 操作 | 命令 | 说明 |
| --- | --- | --- |
| 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<br>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 |
| （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** *retries* | 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）配置处理接口流量的主用slot | **service slot** *slot-number* | 缺省情况下，未配置处理接口流量的主用slot<br>本命令的支持情况与设备的型号有关，请参见命令参考中的介绍 |
| （可选）配置处理接口流量的备用slot | **service standby slot** *slot-number* | 缺省情况下，未配置处理接口流量的备用slot<br>本命令的支持情况与设备的型号有关，请参见命令参考中的介绍 |
| （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”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，设备上未配置任何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 | L2TP组号不为1 | **allow l2tp virtual-template** *virtual-template-number* **remote** *remote-name* | 二者选其一<br>缺省情况下，LNS不接受任何LAC的隧 |

| 操作 | | 命令 | 说明 |
| --- | --- | --- | --- |
| 定建立隧道时使用的虚拟模板接口 | L2TP组号为1 | **allow l2tp virtual-template** *virtual-template-number* [ **remote** *remote-name* ] | 道建立请求<br>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<br>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** ] | - |
| 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<br>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。

如果 LAC 和 LNS 两端都开启了隧道验证功能，则两端密钥（通过 **tunnel password** 命令配置）不为空并且完全一致的情况下，二者之间才能成功建立 L2TP 隧道。

如果 LAC 和 LNS 中的一端开启了隧道验证功能，则另一端可不开启隧道验证功能，但需要两端密钥（通过 **tunnel password** 命令配置）不为空并且完全一致，二者之间才能成功建立 L2TP 隧道。

如果 LAC 和 LNS 两端都禁用隧道验证功能，则无论两端是否配置密钥、密钥是否相同，都不影响隧道建立。

需要注意的是：

- 为了保证隧道安全，建议用户不要禁用隧道验证功能。
- 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，未配置隧道验证密钥 |

## 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** } ] | - |
| 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 配置隧道对端所属的VPN

缺省情况下，设备在公网上发送 L2TP 控制消息和数据消息。通过本配置指定隧道对端所属的 VPN 后，设备将在指定的 VPN 内发送 L2TP 控制消息和数据消息，即在指定 VPN 内查找到达控制消息和数据消息目的地址的路由，根据指定 VPN 的路由转发控制消息和数据消息。

当 L2TP 隧道的一个端点位于某个 VPN 中时，需要在 L2TP 隧道的另一个端点上通过本配置指定隧道对端属于该 VPN，以便正确地在 L2TP 隧道端点之间转发报文。

执行本配置时需要注意，隧道对端所属的 VPN 应该与本端设备连接 L2TP 隧道对端的物理接口所属的 VPN（通过 **ip binding vpn-instance** 命令配置）相同。

表1-18 配置隧道对端所属的 VPN

| 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** } ] | - |
| 配置隧道对端所属的VPN | **vpn-instance** *vpn-instance-name* | 缺省情况下，L2TP隧道对端属于公网 |

### 1.6.6 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1-19 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1-20 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** ] |
| 显示当前L2TP非稳态会话的信息 | **display l2tp session temporary** |
| 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

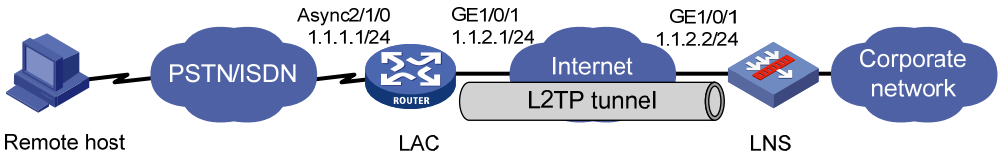
## 1.8.1 NAS-Initiated模式L2TP隧道配置举例

### 1. 组网需求

PPP 用户通过 LAC 接入 LNS，在 LAC 和 LNS 之间建立 L2TP 隧道，以便用户通过该 L2TP 隧道访问公司总部。

### 2. 组网图

图1-11 NAS-Initiated 模式 L2TP 隧道组网图




### 3. 配置步骤

(1) LAC 侧的配置

# 配置各接口的 IP 地址（略）。

# 创建本地 PPP 用户 vpdnuser，设置密码为 Hello。

```
<LAC> system-view
[LAC] local-user vpdnuser class network
[LAC-luser-network-vpdnuser] password simple Hello
[LAC-luser-network-vpdnuser] service-type ppp
[LAC-luser-network-vpdnuser] quit
```

# 配置 ISP 域 system 对 PPP 用户采用本地验证。

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

# 在 Async2/1/0 接口上配置 PPP 认证方式为 CHAP。

```
[LAC] interface async 2/1/0
[LAC-Async2/1/0] ppp authentication-mode chap
[LAC-Async2/1/0] quit
```

# 开启 L2TP 功能。

```
[LAC] l2tp enable
```

# 创建LAC模式的L2TP组1，配置隧道本端名称为LAC，指定接入的PPP用户的用户名为vpdnuser时 LAC 向 LNS 发起隧道建立请求，并指定 LNS 地址为 1.1.2.2。

```
[LAC] l2tp-group 1 mode lac
[LAC-l2tp1] tunnel name LAC
[LAC-l2tp1] user fullusername vpdnuser
[LAC-l2tp1] lns-ip 1.1.2.2
```

# 启用隧道验证功能，并设置隧道验证密钥为 aabbcc。

```
[LAC-l2tp1] tunnel authentication
[LAC-l2tp1] tunnel password simple aabbcc
[LAC-l2tp1] quit
```

(2) LNS 侧的配置

# 配置各接口的 IP 地址。（略）

# 创建本地 PPP 用户 vpdnuser，设置密码为 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
```

# 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
```

#配置 PPP 地址池。

```
[LNS] ip pool aaa 192.168.0.10 192.168.0.20
[LNS] ip pool aaa gateway 192.168.0.1
```

# 创建接口 Virtual-Template1，PPP 认证方式为 CHAP，并使用地址池 aaa 为 Client 端分配 IP 地址。

```
[LNS] interface virtual-template 1
 [LNS-virtual-template1] ppp authentication-mode chap domain system
[LNS-virtual-template1] remote address pool aaa
[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，并配置隧道对端名称为 LAC。

```
[LNS] l2tp-group 1 mode lns
[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
```

(3) Remote host 侧的配置

在 Remote host 上配置拨号连接，在拨号网络窗口中输入用户名 vpdnuser 和密码 Hello 进行拨号。

### 4. 验证配置

# 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 tunnel** 可查看建立的 L2TP 隧道。

```
[LNS] display l2tp tunnel
LocalTID RemoteTID State         Sessions RemoteAddress    RemotePort RemoteName
196      3542      Established   1        1.1.2.1          1701       LAC
```

# 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
```

```
2041          64              196           Established
```

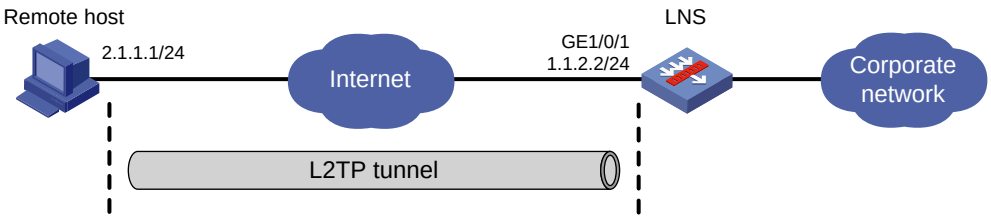
## 1.8.2 Client-Initiated模式L2TP隧道配置举例

### 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1-12 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
```

#配置 PPP 地址池。

```
[LNS] ip pool aaa 192.168.0.10 192.168.0.20
[LNS] ip pool aaa gateway 192.168.0.1
```

# 创建接口 Virtual-Template1，PPP 认证方式为 CHAP，并使用地址池 aaa 为 Client 端分配 IP 地址。

```
[LNS] interface virtual-template 1
 [LNS-virtual-template1] ppp authentication-mode chap domain system
[LNS-virtual-template1] remote address pool aaa
[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
```

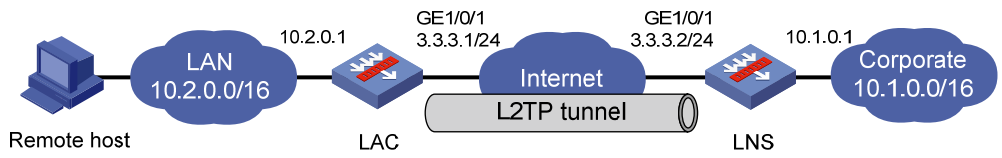
## 1.8.3 LAC-Auto-Initiated模式L2TP隧道配置举例

### 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1-13 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
```
#配置 PPP 地址池。
```
[LNS] ip pool aaa 192.168.0.10 192.168.0.20
[LNS] ip pool aaa gateway 192.168.0.1
```
# 创建接口 Virtual-Template1，PPP 认证方式为 PAP，并使用地址池 aaa 为 Client 端分配 IP 地址。
```
[LNS] interface virtual-template 1
[LNS-virtual-template1] ppp authentication-mode pap
[LNS-virtual-template1] remote address pool aaa
[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. 10
```
(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 MSCHAP，如果对端不支持 MSCHAP，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。