HiPER 命令行配置手册

第 4 卷：拨号连接

上海艾泰科技有限公司

http://www.utt.com.cn

版权声明

产品编号（PN）：0900-0041-001

文档编号（DN）：PR-PMMU-1106.05-PPR-CN-1.0A

目 录

导　　读

命令行格式约定

本手册中，讲解命令句法时，英文字体为“ Times New Roman ”字体，中文字体为“ 宋体 ”。相关命令行格式约定的描述如下：

加粗字体：指配置命令时需要原封不动输入的参数。

倾斜字体：指配置命令时必须为之提供实际值的参数。

[ ]：表示用[ ]扩起来的部分，在配置命令时是可选的。

{x｜y｜… }：表示从两个或多个选项中选取一个。

[x｜y｜…]：表示从两个或多个选项中选取一个或者不选。

!：由感叹号！开始的行表示注释行。

_：输入光标位置。

>:命令行参数层次分隔符。

此外，在实际的配置实例和终端输出（Terminal Display）中，使用加粗“ Courier New ”字体表示用户从终端输入的信息；使用普通“ Courier New ”字体表示屏幕输出信息。

键盘操作约定

<>：表示键盘上的按键。例如，<Enter>表示回车。

<键 1+键 2>：表示在键盘上同时按下键 1 和键 2。例如，<Ctrl+H>表示同时按下 Ctrl 键和 H 键。

特殊符号约定

该符号表示提示信息，指出重点注意事项。

适用版本

本手册适用的软件版本为 ReOS 5.0。

第1章 拨号连接介绍

1.1 概述

在 HiPER 中，支持以下三种类型的拨号连接：

- PPPoE（Point-to-Point Protocol over Ethernet）：以太网上的点对点协议。
- L2TP（Layer Two Tunneling Protocol）：第二层隧道协议，已成为 IETF 有关二层隧道协议的工业标准。
- PPTP（Point-to-Point Tunneling Protocol）：点到点隧道协议，属于第二层的协议。

目前，HiPER 不支持 PPPoE 的服务器端，只支持 PPPoE 的客户端；可同时支持 L2TP/PPTP 的客户端和服务器端。在 HiPER 中，无论是 PPPoE 客户端，还是 L2TP/PPTP 客户端、L2TP/PPTP 服务器，都是通过配置拨号连接实例来实现的。

1.2 PPP 协议简介

由于 PPPoE、L2TP/PPTP 协议在很大程度上都是依靠 PPP（Point to Point Protocol）协议的各种特性，因此有必要先介绍一下 PPP 协议。

PPP 协议实现了通过拨号或专线方式建立点对点连接发送数据，属于链路层协议。PPP 协议可将 IP、IPX 和 NETBEUI 包封装在 PPP 帧内通过点对点的链路发送。由于 PPP 协议能够提供用户验证、易于扩充和支持同异步，因此获得了较广泛的应用。

以下仅简要介绍 PPP 协议的组成部分、PPP 链路的建立过程以及 HiPER 支持的几种 PPP 验证协议。有关 PPP 协议的详细说明，请参考 RFC 1661、RFC 1994、RFC 1990、RFC 1974、RFC 1334。

1.2.1 PPP 协议的组成部分

PPP 协议由三个部分组成：

- LCP（Link Control Protocol）：链路控制协议，主要用来建立、拆除和监控数据链路。
- NCP（Network Control Protocol）网络层控制协议，主要用来协商在该数据链路上所传输的数据包的格式与类型。
- 用于网络安全方面的验证协议，比如 PAP、CHAP 等。

1.2.2 PPP 链路的建立过程

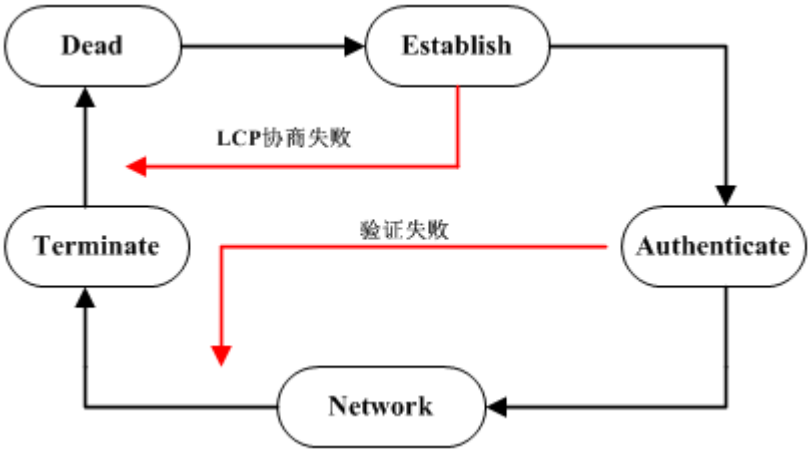

图 1-1 PPP 链路的建立过程

如图 1-1 所示，PPP 链路的建立需要经历以下几个阶段：

- Dead 阶段（链路不可用阶段），也称为物理层不可用阶段，PPP 链路都需从这个阶段开始和结束。当通信双方检测到物理线路激活时，就进入 Establish 阶段。
- Establish 阶段（链路建立阶段）：PPP 链路进行 LCP 协商，协商内容包括工作方式、验证方式和最大传输单元等。LCP 协商成功后，LCP 状态变为 Opened，表示底层链路已经建立。
- Authenticate 阶段（验证阶段）：如果配置了验证，就进入验证阶段，开始 CHAP 或 PAP 验证。如果验证失败，就进入 Terminate 阶段，拆除链路，LCP 状态变为 Down；如果验证成功，就进入 Network 阶段。
- Network 阶段（网络层协商阶段）：PPP 将调用在 Establish 阶段选定的各种网络控制协议。例如，在该阶段 IP 控制协议（IPCP）能为拨入的用户分配动态地址。当相应的网络层协议协商成功后，才能通过这条 PPP 链路发送报文。
- Terminate 阶段（网络终止阶段）：PPP 能在任何时候终止链路。物理线路 Down、链路检测失败和管理员人为关闭链路等情况均会导致链路终止；明确的 LCP 或 NCP 帧都可关闭 PPP 链路。

1.2.3 PPP 的验证协议

在 HiPER 中，目前可支持 PAP、CHAP 以及 MS-CHAP 这三种 PPP 验证协议。

- PAP（Password Authentication Protocol）：口令验证协议；
- CHAP（Challenge Handshake Authentication Protocol）：质询握手验证协议；
- MS-CHAP（Microsoft- Challenge Handshake Authentication Protocol）：微软质询握手验证协议。

1.2.3.1 PAP 验证协议

PAP 是 PPP 协议中对通信双方身份验证的安全性协议之一，是一种简单的明文验证协议。PAP 验证仅在 PPP 连接建立时进行，在数据传输阶段不进行 PAP 验证。

PAP 验证的过程如下：

- 当被验证方（记为 B）拨通验证方（记为 A）后， B 将自己的用户名和密码一起发送给 A；
- A 根据本地配置查看相关的用户名和密码是否正确，然后返回不同的响应。如果用户名和密码正确，则 A 与 B 可继续进行网络层协商，否则 A 将切断线路。

PAP 的特点是在网络上以明文的方式传递用户名及密码，如在传输过程中被截获，便有可能对网络安全造成极大的威胁。因此，它适合于对网络安全要求相对较低的环境。

1.2.3.2 CHAP 验证协议

CHAP 是 PPP 协议中对通信双方身份验证的安全性协议之一，是一种加密的验证方式，能够避免建立连接时传送用户的真实密码。

CHAP 验证为三次握手验证，密码使用密文，验证过程如下：

- 当被验证方（记为 B）拨通验证方（记为 A）后，由 A 将一段随机数据和自身的用户名发送给 B；
- B 根据接收到的名字查找到密钥,并用它对收到的随机数据用 MD5 算法进行加密，然后将加密结果和自身的用户名一起发送给 A；
- A 收到该报文后，首先根据接收到的名字查到 B 的密钥，同样用它对以前发送的随机数据用 MD5 算法进行加密，并将自己算出的加密结果与接收到的加密结果相比较，如果一致，A 与 B 可继续进行网络层协商，否则 A 将切断线路。

由于 CHAP 的特点是只在网络上传输用户名，而并不传输密码，因此它的安全性要比 PAP 高。另外，CHAP 协议不仅在连接建立阶段进行，在以后的数据传输阶段也可以按随机间隔继续进行，但每次验证方发给被验证方的随机数据都应不同，以防被第三方猜出密钥。如果验证方发现机密结果不一致，将立即切断线路。

1.2.3.3 MS-CHAP 验证协议

MS-CHAP 是 PPP 协议中对通信双方身份验证的安全性协议之一，与 CHAP 类似，它也是一种加密的验证方式，能够避免建立连接时传送用户的真实密码。MS-CHAP 使用基于 MPPE（微软点对点加密协议）的数据加密。MS-CHAP 主要用于 HiPER 与 Mircrosoft Windows 设备之间的 CHAP。

1.3 虚端口

1.3.1 虚端口概念

虚端口指在物理上不存在、需要通过配置建立的端口，它必须与某一物理端口相关联。在 HiPER 中，虚端口用于拨号连接，它是基于“ connection ”生成的。

1.3.2 虚端口状态

当配置完拨号连接实例后，系统会使用该配置自动生成一个“ 虚端口 ”用来传输数据。新生成的端口缺省工作在“ 监听 ”（ptpdial）状态下，在该状态下，PPPoE 拨号连接（或

L2TP/PPTP 隧道连接）并未真正建立，以节省系统资源。“ 监听 ” 状态下的端口将一直监听是否有用户的数据包需要传送。

当 PPPoE 拨号连接（或 L2TP/PPTP 隧道连接）建立成功后，虚端口被激活，由“ 监听 ”（ptpdial）状态变为“ 传输 ”（ptp）状态，此时可通过虚端口转发数据包。

由于在系统中维持一条 PPPoE 拨号连接（或 L2TP/PPTP 隧道连接）需要消耗一定的资源，HiPER 采取了一些优化设计。连接可以被配置成：当没有用户数据需要传送的时候，也就是说该连接“ 空闲 ”（此时虚端口也为“ 空闲 ” 状态）一段时间后，系统将主动拆除已经处在“ 传输 ” 状态的连接，虚端口就由“ 空闲 ” 状态变为“ 监听 ” 状态，处在该状态下的连接（虚端口）不能发送用户数据。

由上，从开始配置连接实例、到参数配置完成、到连接建立、再到连接中断整个过程中，相应的虚端口的状态的变化如图 1-2 所示。

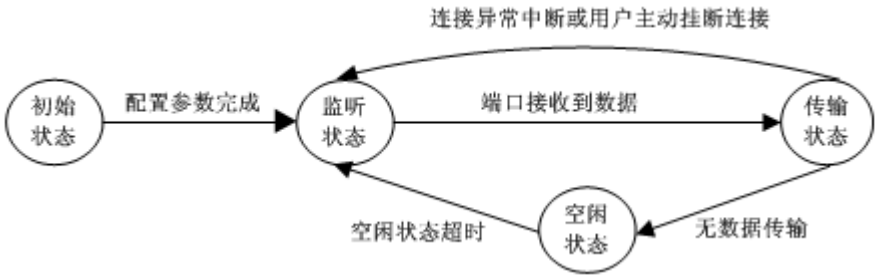

图 1-2 虚端口状态变化图

1.3.3 虚端口和 IP 路由

当配置完拨号连接实例时，系统会自动生成自动生成一个“ 虚端口 ”，同时也会自动生成对应的静态路由：其转发接口即为对应的虚端口；其目的地址由参数“ **ip address remoteip** ”（远端内网 IP 地址）和“ **ip address remotemask** ”（远端内网子网掩码）决定，具体配置可参考 3.3.10 和章节 3.4.6。

注意，对于 PPPoE 拨号连接来说，一般情况下，参数“ **ip address remoteip** ”和“ **ip address remotemask** ” 均使用缺省值（均为 0.0.0.0），因此对应的静态路由即为系统的缺省路由。

虚端口处于“ 监听 ”（ptpdial）状态时，对应的静态路由处于“ 中断 ”（Down）状态；虚端口处于“ 传输 ”（ptp）状态时，对应的静态路由处于“ 激活 ”（Up）状态。在 HiPER 中，可以使用命令 **show ip route table** 来查看虚端口是否建立，以及虚端口的状态，同时也可以查看对应静态路由的状态。

对于 L2TP/PPTP 隧道连接来说，如果隧道连接未建立，对应的静态路由条目中，“ IfId ” 为“ ptpdial0 ”，表示虚端口处于“ 监听 ” 状态；同时，“ Cost ” 和“ Met ” 分别为路由断开优先级和断开跳数，表示该静态路由处于“ 中断 ”状态。当连接建立成功后，“ IfId ”为“ ptpx ”，表示虚端口处于“ 传输 ” 状态；同时，“ Cost ” 和“ Met ” 分别为路由优先级和跳数，表示该静态路由已经“ 激活 ”。如图 1-3 实例中，比较了 L2TP/PPTP 隧道连接成功前后，虚端口及对应静态路由的状态。

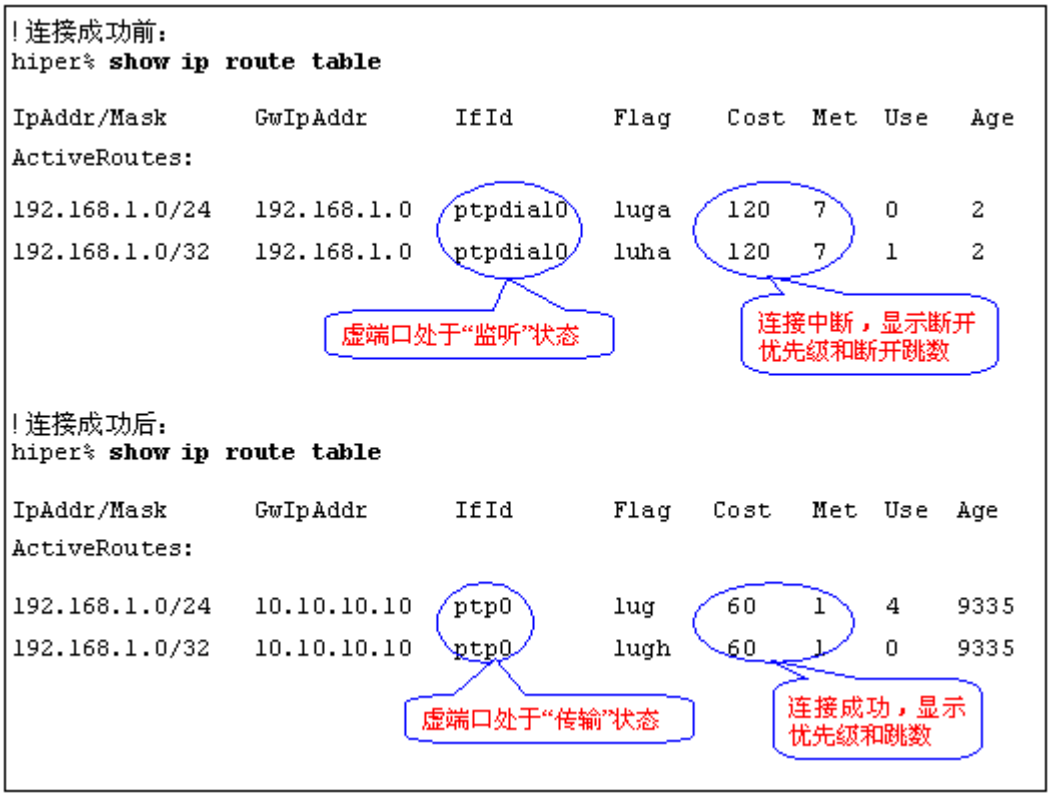

图 1-3 虚端口和 IP 路由的状态——L2TP/PPTP 隧道连接成功前后

对于 PPPoE 拨号连接来说，如果拨号连接未建立，对应的缺省路由条目中，“ IfId ”为“ ptpdial0 ”，表示虚端口处于“ 监听 ”状态；同时，“ Cost ”和“ Met ”分别为路由断开优先级和断开跳数，表示该路由处于“ 中断 ”状态。当连接建立成功后，将新增一条缺省路由，“ IfId ”为“ ptpx ”，表示虚端口处于“ 传输 ”状态；同时，“ Cost ”和“ Met ”分别为路由优先级和跳数，表示该路由已经“ 激活 ”。此时，原先的那条缺省路由的“ Flag ”将增加标记“ * ”，表示该路由目前不生效。如图 1-4 实例中，比较了 PPPoE 拨号连接成功前后，虚端口及对应缺省路由的状态。

提示：如果 PPPoE 拨号实例中，将参数“ **line dialoutSpoof** ”设置为“ **No** ”（参见章节 2.2.9），那么，拨号未成功时，路由表中将不会出现对应的缺省路由；只有当拨号成功后，才会生成一条可转发数据的缺省路由：“ IfId ”为“ ptpx ”，“ Cost ”和“ Met ”分别为路由优先级和跳数，表示虚端口和路由均已激活。

图 1-4 虚端口和 IP 路由的状态——PPPoE 拨号连接成功前后

1.4 HiPER 的拨号机制介绍

1.4.1 首拨号码

HiPER 作为拨号客户端时，无论是 PPPoE 客户端，还是 L2TP/PPTP 客户端，都必须配置首拨号码（**dial first**）。如果没有首拨号码，就无法触发拨号。

1.4.2 呼叫分组（PPPoE）

对于 PPPoE 拨号连接，系统默认从 eth2（WAN）端口呼出，如果希望拨号从指定的物理端口呼出，系统必须启用呼叫分组功能，并为相应的物理端口配置对应的呼叫组号。在 HiPER 中，系统规定：LAN 口、WAN 口、WAN2/DMZ 口对应的呼叫组号的值分别为 4、5、6。相关配置可参考章节 2.2.3.2。

使用呼叫分组功能后，首拨号码由两部分组成：呼叫组号＋呼叫号码，呼叫组号由系统规定，呼叫号码由用户自定义。因此，对于 PPPoE 拨号连接来说，需按照以下方式配置首拨号码：

- 如果要从 eth1 端口（LAN）呼出，那么必须配置以 4 开头的首拨号码；
- 如果要从 eth2 端口（WAN）呼出，那么必须配置以 5 开头的首拨号码；
- 如果要从 eth3 端口（WAN2）呼出，那么必须配置以 6 开头的首拨号码；
- 对于从同一端口呼出的多条 PPPoE 拨号连接，可以使用不同的呼叫号码加以标识。

提示：对于 L2TP/PPTP 客户端，系统是通过 IP 路由触发拨号的，因此无需使用呼

叫分组功能。

1.4.3 拨号类型

HiPER 作为拨号客户端时，无论是 PPPoE 客户端，还是 L2TP/PPTP 客户端，都支持三种拨号类型（即连接方式）。

- 自动拨号：当拨号连接实例的参数配置完成后，或者开启 HiPER 时，或者上一次拨号断线后，HiPER 将自动发起呼叫（建立连接请求）；
- 按需拨号：当拨号连接实例的参数配置完成后，一旦对应虚端口监听到有数据需要传输，HiPER 就发起呼叫（建立连接请求）；
- 手动拨号：只能通过人工进行连接和挂断拨号连接实例。

1.4.4 空闲时间和会话时间

HiPER 作为拨号服务器或者拨号客户端（按需拨号或手动拨号）时，均可设置会话时间和空闲时间。

- 空闲时间（**dial idleTimeout**）：在没有访问流量后自动断线前等待的时长，当拨号连接成功后，如果虚端口空闲（无数据传输）的时间超过了预设的“ 空闲时间 ”，HiPER 将主动断开连接。缺省值为 0，代表不自动断线，即连接空闲不自动挂断。单位：秒。
- 会话时间（**dial sessionTimeout**）：即连接生存时间（一般无需设置），一旦连接建立的时间（从拨号成功开始）超出了预设的“ 会话时间 ”，HiPER 将主动断开连接。缺省值为 0，代表不限制会话时间。单位：秒。

提示：HiPER 作为拨号客户端时，如果拨号类型为自动拨号方式，空闲时间和会话时间是没有意义的，即便设置了空闲时间和会话时间，它们也不会对该连接实例起作用。这是因为，在自动拨号方式下，当连接建立成功后，除非是对方设备主动挂断或者该连接实例所依赖的物理资源不能正常工作，HiPER 是不会主动挂断连接的。

1.4.5 拨号时段和上线时段

HiPER 作为拨号客户端时，无论是 PPPoE 客户端，还是 L2TP/PPTP 客户端，都可设置拨号时段和上线时段。这两个时段的设置可以让管理员控制拨号连接的开始时间和结束时间。

- 拨号时段（**dial dialTimeRange**）：允许拨号客户端拨号的时间段，只有在此时间段范围内才允许拨号客户端触发拨号。不设置代表不对拨号时段进行控制。
- 上线时段（**dial callTimeRange**）：允许拨号客户端（虚端口）处于“ 传输 ”状态的时间段，如果超出这个时间段时，对应连接（虚端口）处于“ 传输 ”状态，HiPER 将会自动断开连接，虚端口变为“ 监听 ”状态。不设置代表不对上线时段进行控制。

1.4.6 LQM 检测

LQM（Link Quality Monitoring），即链路质量监控，它用于 PPP 链路质量的控制。有关 LQM 的详细说明可参考 RFC 1333。

HiPER 作为拨号服务器或者拨号客户端时，均可启用 lqm 检测功能，并通过设置“ lqm 检测间隔 ”和“ lqm 生命周期 ”来控制链路质量。

- lqm 检测间隔（**encaps lqm min**）：发送 lqm 检测包的时间间隔。单位：毫秒。
- lqm 生命周期（**encaps lqm max**）：lqm 检测包的统计周期。单位：毫秒。

在 HiPER 中，如果启用了 lqm 检测，在拨号连接成功后，HiPER 将每隔“ lqm 检测间隔 ”向对端设备发送 lqm 检测包，如果在某个“ lqm 生命周期 ”范围内一直没有收到对方设备的回应包，则断开此连接。

第2章 PPPoE 拨号配置

2.1 PPPoE 简介

2.1.1 PPPoE 介绍

PPPoE（Point-to-Point Protocol over Ethernet），即以太网上的点对点协议，它可以使以太网的主机通过一个简单的桥接设备连到一个远端的接入服务器（Access Concentrator）上。

PPPoE 协议采用 Client/Server（客户端/服务器）方式，它将 PPP 报文封装在以太网帧内，在以太网上提供点对点的连接。关于 PPPoE 协议的详细介绍，请参考 RFC 2516。

2.1.2 PPPoE 拨号过程

PPPoE 拨号有两个阶段：发现（Discovery）阶段和 PPP 会话（PPP Session）阶段。

2.1.2.1 发现阶段

当一个用户主机想开始一个 PPPoE 会话时，首先必须进行发现阶段以识别对方的以太网 MAC 地址，并建立一个 PPPoE 会话标识（Session ID）。在发现阶段，主机以广播方式寻找可以连接的所有接入服务器，一般有多个接入服务器可通信，用户主机可从中选择一个作为自己的接入服务器。

当发现阶段正常结束后，通信的两端都获得会话标识和对方的 MAC 地址，它们一起唯一定义 PPPoE 会话。

2.1.2.2 PPP 会话阶段

进入 PPP 会话阶段后，主机和接入服务器将进行标准的 PPP 协商，PPP 协商通过后，数据通过 PPP 封装发送。PPP 报文作为 PPPoE 帧的净荷被封装在以太网帧内，发送到 PPPoE 链路的对端。注意，此时所有的以太网帧都是单播的。

2.1.2.3 PPPoE 连接的断开

有两种方式可断开 PPPoE 连接：一种是 PPP 协议来结束会话，即 PPP 通信双方使用 PPP 协议自身来结束 PPPoE 会话；另一种是在无法使用 PADT（PPPoE Active Discovery Terminate）数据包来结束 PPPoE 会话，主机或接入服务器均可发送。

2.1.3 PPPoE 客户端介绍

PPPoE 在 ADSL 宽带接入中被广泛使用。通常情况下，一台主机如果要通过 ADSL 接

入 Internet，必须在主机上安装 PPPoE 客户端拨号软件。HiPER 系列产品都支持 PPPoE 客户端功能，用户只需在 HiPER 上完成 PPPoE 拨号的连接，局域网中的计算机即可通过 HiPER 共享一个 ADSL 帐号上网，而无需在 PC 上安装 PPPoE 客户端软件。

提示：在大部分情况下，局域网的计算机共享一个账号和地址上网，需要启用 NAT 功能，并进行相关配置。

2.2 PPPoE 客户端配置

HiPEE 中，PPPoE 客户端配置主要包括以下内容：

- 新建一个 PPPoE 拨号连接实例
- 配置描述信息
- 配置首拨号码、按端口拨号
- 启用 PPP 封装
- 配置 PPP 验证方式及用户名、密码
- 启用/禁用 PPPoE 客户端功能
- 配置 PPPoE 服务名和服务器名
- 配置 MRU 和 MTU
- 配置拨号类型
- 配置拨号时段和上线时段
- 配置空闲时间和会话时间
- 配置 lqm 检测
- 配置路由优先级和断开优先级
- 启用/禁用一个 PPPoE 拨号连接实例
- 删除一个 PPPoE 拨号连接实例

2.2.1 新建一个 PPPoE 拨号连接实例

首先，需要创建一个 PPPoE 拨号连接实例，并为该连接实例自定义一个名字。

配置命令如表 2-1 所示。

操作	命令
新建一个 PPPoE 拨号连接实例	**new connection/***conn-name*
备注：“ *conn-name* ”为自定义的 PPPoE 拨号连接实例的名称。	

表 2-1 新建一个 PPPoE 拨号连接实例

2.2.2 配置描述信息

当系统有多条拨号连接实例存在时，为区别这些连接实例，方便辨别，可以为连接实例增加描述信息。一般情况下，无需设置。

配置命令如表 2-2 所示：

操作	命令
对 PPPoE 拨号连接实例进行描述	**set connection/***conn-name* **description** *description*
备注：“ **description** ”缺省值为空。	

表 2-2 对 PPPoE 拨号连接实例进行描述

2.2.3 配置首拨号码、按端口拨号

2.2.3.1 配置首拨号码

如前所述（参见章节 1.4.1），必须为 PPPoE 拨号连接实例设置首拨号码（**dial first**）。如没有首拨号码，拨号行为就不会发生。

相关配置命令如表 2-3 所示。

操作	命令
配置 PPPoE 拨号连接的首拨号码	**set connection/***conn-name* **dial first** *dial-num*
备注：缺省情况下，“ **dial first** ”的值为空。	

表 2-3 配置 PPPoE 拨号连接实例的首拨号码

2.2.3.2 配置按端口拨号

对于 PPPoE 拨号连接，系统默认从 eth2（WAN）端口呼出，如果希望拨号从指定的物理端口呼出，系统必须启用呼叫分组，并为相应的物理端口配置呼叫组号。并且，系统规定：LAN 口、WAN 口、WAN2/DMZ 口对应的呼叫组号的值分别为 4、5、6。

相关配置命令如表 2-4、2-5 所示。

操作	命令
启用呼叫分组功能	**set system dialerGroup enabled**
禁用呼叫分组功能	**set system dialerGroup disabled**
备注：缺省情况下，“ **dialerGroup** ”的值为“ **disabled** ”，即禁用呼叫分组功能。	

表 2-4 启用/禁用呼叫分组

操作	命令
配置 LAN 口的呼叫组号	**set interface ethernet/1 dialerGroup 4**
配置 WAN 口的呼叫组号	**set interface ethernet/2 dialerGroup 5**
配置 WAN2/DMZ 口的呼叫组号	**set interface ethernet/3 dialerGroup 6**
备注：缺省情况下，各个物理端口的“ **dialerGroup** ”的值都为 0。	

表 2-5 配置物理端口的呼叫组号

使用呼叫分组功能后，首拨号码由两部分组成：呼叫组号＋呼叫号码，呼叫组号由系统规定，呼叫号码由用户自定义。因此，对于 PPPoE 拨号连接来说，需按照以下方式配置首拨号码：

- 如果要从 eth1 端口（LAN）呼出，那么必须配置以 4 开头的首拨号码；
- 如果要从 eth2 端口（WAN）呼出，那么必须配置以 5 开头的首拨号码；
- 如果要从 eth3 端口（WAN2）呼出，那么必须配置以 6 开头的首拨号码；
- 对于从同一端口呼出的多条 PPPoE 拨号连接，可以使用不同的呼叫号码加以标识。

2.2.4 启用 PPP 封装

由于 PPPoE 拨号是建立在 PPP 基础上的，因此，首先需要通过 PPP 协议封装数据包，即在 PPPoE 拨号连接实例上启用 PPP 封装。缺省情况下，为启用 PPP 封装，因此无需修改相关配置。

配置命令如表 2-6 所示。

操作	命令
在 PPPoE 拨号连接实例上启用 PPP 封装	**set connection/***conn-name* **encaps type ppp**
备注：“ **encaps type** ”缺省值为“ **ppp** ”。	

表 2-6 在 PPPoE 拨号连接实例上启用 PPP 封装

2.2.5 配置 PPP 验证方式及用户名、密码

HiPER 作为 PPPoE 客户端与远端 PPPoE 服务器进行拨号连接时，在 PPP 协商过程中支持以下几种身份验证方式：

- **None**：不进行 PPP 验证；
- **PAP**：口令验证协议；
- **CHAP**：质询握手验证协议；
- **MS-CHAP**：微软质询握手验证协议。

如果选择了 PAP、CHAP 以及 MS-CHAP 中的任一种作为 PPP 验证方式，那么，还需设置相关的验证用户名及密码。在 PPP 协商的过程中，验证方（服务器）和被验证方（客户端）的身份验证方式、用户名及密码必须一致。

配置命令如表 2-7 所示。

操作	命令
配置 PPP 验证方式	**set connection/***conn-name* **encaps send authtype** {**None** | **PAP** | **CHAP** | **MS-CHAP** }
配置 PPP 验证时本地发送的用户名	**set connection/***conn-name* **encaps send name** *ppp-name*
配置 PPP 验证时本地发送的密码	**set connection/***conn-name* **encaps send pw** *ppp-password*
备注：缺省情况下，“ **send authtype** ”值为 PAP，“ **send name** ”和“ **send pw** ”的值都为空。	

表 2-7 配置 PPP 验证方式及用户名、密码——PPPoE 拨号连接实例

2.2.6 启用/禁用 PPPoE 客户端功能

缺省情况下，新建的拨号连接是禁用 PPPoE 客户端功能的，此时，它将仅仅向拨号服务器发起 PPP 协商。因此，对于 PPPoE 拨号连接实例来说，必须启用其 PPPoE 客户端功能，它才会向 PPPoE 服务器主动发起 PPPoE 协商。

配置命令如表 2-8 所示。

操作	命令
启用 PPPoE 客户端功能	**set connection/***conn-name* **pppoe type client**
禁用 PPPoE 客户端功能	**set connection/***conn-name* **pppoe type disabled**
备注：缺省情况下，“ **pppoe type”**的值为 “ **disabled** ”。	

表 2-8 启用/禁用 PPPoE 客户端功能

2.2.7 配置 PPPoE 服务名和服务器名

PPPoE 服务名是由 ISP（服务提供商）提供的，它可以是 ISP 的名称，也可以是 PPPoE 服务器上配置的一类服务。一般无需设置该参数；个别情况下，PPPoE 服务器要求协商该参数。如有疑问，请询问相关 ISP。

PPPoE 服务器名即 PPPoE 服务器的名称，也是由 ISP 提供的。一般无需设置该参数；个别情况下，PPPoE 服务器要求协商该参数。如有疑问，请询问相关 ISP。

配置命令如表 2-9 所示。

操作	命令
配置 PPPoE 服务名	**set connection/***conn-name* **pppoe servicename** *servicename*
配置 PPPoE 服务器名	**set connection/***conn-name* **pppoe servername** *servername*
备注：缺省情况下，“ **pppoe servicename** ”和 “ **pppoe servername** ”的值都为空。	

表 2-9 配置 PPPoE 服务名和服务器名

2.2.8 配置 MRU 和 MTU

一般情况下，数据包接收者的最大接收单元（MRU）必须大于等于数据包发送者的最大发送单元（MTU）。HiPER 中，PPPoE 拨号连接实例的 MRU 和 MTU 的缺省值均为 1524 字节，PPPoE 拨号时 HiPER 将自动与对方设备协商，除非特别应用，不要修改。

配置命令如表 2-10 所示。

操作	命令
配置 PPPoE 拨号连接实例的最大接收单元	**set connection/***conn-name* **encaps mru** *mru-size*
配置 PPPoE 拨号连接实例的最大发送单元	**set connection/***conn-name* **encaps mtu** *mtu-size*

备注：缺省情况下，“ **encaps mru** ”和“ **encaps mtu** ”的值都为 1524，单位为字节。

表 2-10 配置 MRU 和 MTU——PPPoE

2.2.9 配置拨号类型

如前所述（参见章节 1.4.3），HiPER 支持三种 PPPoE 拨号类型：

- 自动拨号：当 PPPoE 拨号连接实例的参数配置完成后，或者开启 HiPER 时，或者上一次拨号断线后，HiPER 将自动发起 PPPoE 呼叫；
- 按需拨号：当 PPPoE 拨号连接实例的参数配置完成后，一旦对应虚端口监听到有数据需要传输，HiPER 就发起 PPPoE 呼叫。
- 手动拨号：只能通过人工进行连接和挂断 PPPoE 拨号连接实例。

PPPoE 拨号类型是由拨号连接实例的两个属性来确定的，即“ **line calltype** ”和“ **line dialoutSpoof** ”。各拨号类型下，这两个属性对应的值如表 2-11 所示。

拨号类型 / 相关属性	自动拨号	按需拨号	手动拨号	备注
line calltype	**AO/Switched**	**Switched**	**Switched**	缺省情况下，拨号类型为手动拨号。
line dialoutSpoof	**Yes**	**Yes**	**No**	

表 2-11 PPPoE 拨号类型的相关属性值

相关配置命令如表 2-12 所示。

操作	命令
配置拨号类型为自动拨号	**set connection/***conn-name* **line calltype AO/Switched** **set connection/***conn-name* **line dialoutspoof Yes**
配置拨号类型为按需拨号	**set connection/***conn-name* **line calltype Switched** **set connection/***conn-name* **line dialoutspoof Yes**
配置拨号类型为手动拨号	**set connection/***conn-name* **line calltype Switched** **set connection/***conn-name* **line dialoutspoof No**
备注：缺省情况下，“ **line calltype** ”的值为“ **Switched** ”，“ **line dialoutspoof** ”的值为“ **No** ”，即拨号类型为手动拨号。	

表 2-12 配置 PPPoE 拨号类型

2.2.10 配置空闲时间和会话时间

如前所述（参见章节 1.4.4），对于拨号类型为按需拨号或手动拨号的 PPPoE 拨号连接实例来说，可以设置空闲时间和会话时间。

- 空闲时间（**dial idleTimeout**）：在没有访问流量后自动断线前等待的时长，当 PPPoE 拨号连接成功后，如果 PPPoE 连接（虚端口）空闲的时间超过了预设的“ 空闲时间 ”，HiPER 将主动断开连接。缺省值为 0，代表不自动断线，即连接空闲不自动

挂断。单位：秒。

- 会话时间（**dial sessionTimeout**）：即连接生存时间（一般无需设置），一旦 PPPoE 拨号线路连接的时间（从拨号成功开始）超出了预设的“会话时间”，HiPER 将主动断开连接。缺省值为 0，代表不限制会话时间。单位：秒。

配置命令如表 2-13 所示。

操作	命令
配置 PPPoE 拨号连接的空闲时间	**set connection/***conn-name* **dial idleTimeout** *idle-time*
配置 PPPoE 拨号连接的会话时间	**set connection/***conn-name* **dial sessionTimeout** *session-time*
备注：缺省情况下，“**dial idleTimeout**”的值为 120，“**dial sessionTimeout**”的值为 0。	

表 2-13 配置空闲时间和会话时间——PPPoE

提示：如果 PPPoE 拨号连接实例的拨号类型为自动拨号方式，空闲时间和会话时间是没有意义的，即便设置了空闲时间和会话时间，它们也不会对该连接实例起作用。这是因为，在自动拨号方式下，当 PPPoE 拨号成功后，除非是对方设备主动挂断或者该连接实例所依赖的物理资源不能正常工作，HiPER 是不会主动挂断连接的。

2.2.11 配置拨号时段和上线时段

如前所述（参见章节 1.4.5），可以为 PPPoE 拨号连接实例设置拨号时段和上线时段。

- 拨号时段（**dial dialTimeRange**）：允许 PPPoE 客户端拨号的时间段，只有在此时间段范围内才允许 PPPoE 客户端触发拨号，不设置代表不对拨号时段进行控制。
- 上线时段（**dial callTimeRange**）：允许 PPPoE 客户端保持 PPPoE 线路连接的时间段，如果超出这个时间段时，对应 PPPoE 线路处于连接状态，HiPER 将会自动断开连接，不设置代表不对上线时段进行控制。

配置命令如表 2-14 所示。

操作	命令
配置 PPPoE 拨号连接的拨号时段	**set connection/***conn-name* **dial dialTimeRange** *time-name*
配置 PPPoE 拨号连接的上线时段	**set connection/***conn-name* **dial callTimeRange** *time-name*
备注：缺省情况下，“**dial dialTimeRange**”和“**dial callTimeRange**”的值都为空。	

表 2-14 配置拨号时段和上线时段——PPPoE

提示：“*time-name*”为引用的时间段策略的名称，具体涵义及配置方法请参考手册《HiPER CLI 配置手册——基本配置》中的第 4 章（时间段配置）。

2.2.12 配置 lqm 检测

如前所述（参见章节 1.4.6），在 PPPoE 拨号连接实例上可启用 lqm 检测，并设置“lqm 检测间隔”和“lqm 生命周期”。

- lqm 检测间隔（encaps lqm min）：发送 lqm 检测包的时间间隔。单位：毫秒。

- lqm 生命周期（encaps lqm max）：lqm 检测包的统计周期。单位：毫秒。

如果启用了 lqm 检测，在 PPPoE 拨号连接成功后，HiPER 将每隔“ lqm 检测间隔 ”向 PPPoE 服务器发送 lqm 检测包，如果在某个“ lqm 生命周期 ”范围内一直没有收到对方回应，则断开此连接。

配置命令如表 2-15 所示。

操作	命令
启用/禁用 lqm 检测	**set connection/***conn-name* **encaps lqm active** { **yes**｜**no**}
配置 lqm 检测间隔	**set connection/***conn-name* **encaps lqm min** *lqm-interval*
配置 lqm 生命周期	**set connection/***conn-name* **encaps lqm max** *lqm-period*
备注：缺省情况下，“ **encaps lqm active** ”的值为“ **yes** ”，即启用 lqm 检测； “ **encaps lqm min** ”和“ **encaps lqm max** ”的值分别为 1000、15000，单位为毫秒。	

表 2-15 配置 lqm 检测——PPPoE

2.2.13 配置路由优先级和断开优先级

此处设置的路由优先级和断开优先级就是与 PPPoE 连接实例对应的缺省路由的优先级和断开优先级。

优先级必须比断开优先级高，值越低优先级越高。关于优先级及断开优先级的应用，请参考《HiPER 命令行配置手册——网络层协议》的第 5 章。

配置命令如表 2-16 所示。

操作	命令
配置路由的优先级	**set connection/***conn-name* **ip preference up** *uppref*
配置路由的断开优先级	**set connection/***conn-name* **ip preference down** *downpref*
备注：缺省情况下，“ **ip preference up** ”和“ **ip preference down** ”的值分别为 60 和 120。	

表 2-16 配置路由的优先级和断开优先级——PPPoE

2.2.14 启用/禁用一个 PPPoE 拨号连接实例

允许设置各个 PPPoE 拨号连接实例的使能状态：启用或禁用。启用时，相应的 PPPoE 拨号连接（虚端口）可以根据拨号规则向外发起连接。当禁用时，当前连接实例不能用，仅在 CLI 的配置文件中可见。

如果你暂时不需要使用某个 PPPoE 拨号连接实例，只需禁用该连接实例即可；当需要恢复使用该连接实例时，只需启用该连接实例即可。

配置命令如表 2-17 所示。

操作	命令
启用 PPPoE 拨号连接实例	**set connection**/*conn-name* **enabled yes**
禁用 PPPoE 拨号连接实例	**set connection**/*conn-name* **enabled no**
备注：缺省情况下，“ **enabled** ”的值为“ **yes** ”，即启用 PPPoE 拨号连接实例。	

表 2-17 启用/禁用一个 PPPoE 拨号连接实例

2.2.15 删除一个 PPPoE 拨号连接实例

如果不再需要某 PPPoE 拨号连接实例，则可删除改连接实例。在 HiPER 中，一次只能删除一个 PPPoE 拨号连接实例。

配置命令如表 2-18 所示。

操作	命令
删除一个 PPPoE 拨号连接实例	**delete connection**/*conn-name*
备注：删除某个 PPPoE 拨号连接实例时，输入的“ *conn-name* ”必须与新建该 PPPoE 拨号连接实例时输入的连接实例名完全匹配。	

表 2-18 删除一个 PPPoE 拨号连接实例

2.3 手工连接和挂断 PPPoE

无论是 PPPoE 拨号连接实例配置的是哪一种拨号类型，均可以使用命令进行手工连接和挂断。需要注意的是，在手动拨号方式下，只能通过手工输入命令连接和挂断相关的 PPPoE 拨号连接。

配置命令如表 2-19 所示。

操作	命令
手工建立某个拨号连接	**dial connection**/*conn-name*
手工挂断某个拨号连接	**hangup connection**/*conn-name*
手工挂断当前所有拨号连接	**hangup**

表 2-19 手工连接和挂断 PPPoE

2.4 PPPoE 拨号的显示和调试

2.4.1 PPPoE 拨号的显示

2.4.1.1 显示 PPPoE 拨号历史记录

1. 配置命令

在 HiPER 中，可以查看 PPPoE 拨号的历史记录。在命令行的系统历史记录中，信息按照从旧到新的顺序从上往下排列，最下端的信息最新。

配置命令如表 2-20 所示。

操作	命令
显示 PPPoE 拨号历史记录	**show session history**

表 2-20 显示 PPPoE 拨号历史记录

2. PPPoE 拨号历史记录涵义

如表 2-21 所示，列出了使用命令 show session history 查看时，PPPoE 拨号过程中常见的历史记录及涵义。

历史记录	记录含义
Outgoing Call @61:1-1 Call Connected, on Line1, on Channel 0 PPPoE Up 00:0c:f8:f9:66:c6 Session Up [x]	连接开始呼出，61 为首拨号码 物理层/链路层连接完成，但 IP 不可用 PPPoE 成功和 MAC 地址为 00:0c:f8:f9:66:c6 的设备建立连接 某连接成功建立，[x]为连接名
Outgoing Call @61:1-1 Call Terminated @clearSession: 1	连接开始呼出 呼叫失败
Session down [x]	某连接挂断，[x]为连接名
备注：此命令用于查看系统历史记录，PPPoE 拨号历史记录只是其中的一部分。	

表 2-21 PPPoE 拨号历史记录描述

3. 查看实例

如图 2-1 中所示实例中，显示了 PPPoE 拨号成功时的历史记录。

```
hiper% show session history

21:57:53        Outgoing Call @51:72-7624
21:57:53        Call Connected , on Line  1, on Channel  0
21:57:53        PPPoE Up 00:90:1a:40:3a:55
21:57:53        Session Up PPPOE
```

图 2-1 显示 PPPoE 拨号历史记录——拨号成功实例

2.4.1.2 显示 PPPoE 拨号用户信息

1. 配置命令

在 HiPER 中，可以查看 PPPoE 拨号成功时，PPPoE 拨号用户的相关信息。

配置命令如表 2-22 所示。

操作	命令
显示 PPPoE 拨号用户信息	**show session userinfo**
备注：此命令用于查看系统的 PPPoE、L2TP、PPTP 拨号用户信息。PPPoE 拨号用户信息只是其中的一部分。	

表 2-22 显示 PPPoE 拨号用户信息

2. 查看实例

如图 2-2 中，提供了一个查看 PPPoE 拨号用户信息的实例，并结合该例对 PPPoE 拨号用户信息中各参数进行描述和说明。

```
hiper% show session userinfo

dir  prof/user          callid   port  chan  tx   rx   srv    address
0    PPPOE/ad50069718   1        0:-   2:1   n/a  n/a  PPPoE  222.64.20.124

Total Active users:   1, high  1
```

图 2-2 显示 PPPoE 拨号用户信息——实例

3. 部分参数涵义描述

如图 2-2 所示，PPPoE 拨号用户信息中部分参数涵义如下：

- dir：呼叫的方向。其中，O 表示拨出，I 表示拨入。PPPoE 拨号时，HiPER 作为 PPPoE 客户端，因此一直显示为 O。
- prof/user：prof 为拨号连接名；user 为用户名。
- callid：内部索引号；与 **show session callinfo** 中的 callid 相同。
- srv：使用协议。PPPoE 拨号时，显示为 PPPoE，表示用户正在使用 PPPoE 协议连接。
- address：PPPoE 拨号成功后，由 ISP 分配该拨号连接的 IP 地址。
- Total Active users：系统中当前激活的拨号用户（包括 PPPoE 拨号用户、L2TP 拨号用户、PPTP 用户）的个数。
- high：系统中曾经激活的拨号用户（包括 PPPoE 拨号用户、L2TP 拨号用户、PPTP 用户）的最大个数。

2.4.1.3 显示 PPPoE 拨号呼叫信息

1. 配置命令

在 HiPER 中，可以查看 PPPoE 拨号的呼叫信息。

配置命令如表 2-23 所示。

操作	命令
显示 PPPoE 拨号呼叫信息	**show session callinfo**

表 2-23 显示 PPPoE 拨号呼叫信息

2. 查看实例

如图 2-3 所示实例中，显示了 PPPoE 拨号成功后，PPPoE 拨号呼叫信息。

```
hiper% show session callinfo

callid   dnis      clid       inbytes    outbytes    duration
1        unknown   unknown    29643      2834899     0:04:05:07

Total active calls:    1, high  1
```

图 2-3 显示 PPPoE 拨号呼叫信息——实例

3. 部分参数涵义

如图 2-3 所示，PPPoE 拨号呼叫信息中部分参数涵义如下：

- callid：内部索引号；与 **show session userinfo** 中的 callid 相同。
- inbytes：通过该 PPPoE 拨号连接（虚端口）接收的数据包的统计数量。单位：字节。
- outbytes：通过该 PPPoE 拨号连接（虚端口）发送的数据包的统计数量。单位：字节。
- duration：该 PPPoE 拨号连接成功至查看时刻的时间。单位：天:小时:分钟:秒。
- Total Active calls：系统中当前激活的拨号呼叫（包括 PPPoE 呼叫、L2TP 呼叫、PPTP 呼叫）的数量。
- high：系统中曾经激活的拨号呼叫（包括 PPPoE 拨号用户、L2TP 拨号用户、PPTP 用户）的最大数量。

2.4.1.4 查看对应的缺省路由

对于 PPPoE 拨号连接来说，如果拨号连接未建立，对应的缺省路由条目中，“ IfId ”将显示为“ ptpdial0 ”，表示虚端口处于“ 监听 ”状态；同时，“ Cost ”和“ Met ”分别显示为路由断开优先级和断开跳数的值，表示该路由处于“ 中断 ”状态。

当连接建立成功后，将新增一条缺省路由，“ GwIpAddr ”显示为 ISP 分配的 IP 地址；“ IfId ”显示为“ ptpx ”，表示虚端口处于“ 传输 ”状态；同时，“ Cost ”和“ Met ”分别显示为路由优先级和跳数的值，表示该路由已经“ 激活 ”。此时，原先的那条缺省路由的“ Flag ”有“ * ”标记，表示该路由目前不生效。

如图 2-4 所示实例中，显示了 PPPoE 拨号连接成功前后，所对应的缺省路由。

图 2-4 查看对应的缺省路由——PPPoE 拨号连接成功前后

提示：如果 PPPoE 拨号实例中，将参数“ **line dialoutSpoof** ”设置为“ **No** ”（参见章节 2.2.9），那么，拨号未成功时，路由表中将不会出现对应的缺省路由；只有当拨号成功后，才会生成一条可转发数据的缺省路由：“ IfId ”为“ ptpx ”，“ Cost ”和“ Met ”分别为路由优先级和跳数，表示虚端口和路由均已激活。

2.4.2 PPPoE 拨号的诊断

2.4.2.1 物理线路故障或者兼容性问题

执行命令 **show session history** 后，如果出现如图 2-4 所示信息，则表示对方线路无响应。出现该现象，很可能是因为物理线路故障引起，也有可能是因 ADSL Modem 和 HiPER 的兼容性问题引起。请首先检查你自己的物理接入线路是否完好，然后查看 ISP 的物理线路是否完好。如果物理线路是好的，再检查是否有兼容性问题。

出现这种情况，可以用安装有 Windows XP 的机器代替 HiPER，直接连接到 ADSL Modem 上，配置好 PPPoE 拨号，如果能连接成功，说明是 ADSL Modem 和 HiPER 的连接问题，或者 HiPER 的配置有误。

```
hiper% show session history

13:47:28        Outgoing Call @0:94-4062
13:47:28        Call Terminated @clearSession:94
```

图 2-5 显示 PPPoE 拨号历史记录——拨号失败实例 1

2.4.2.2 验证方式、用户名或者密码输入错误

执行命令 **show session history** 后，如果出现如图 2-5 所示信息，则表示很可能验证用户名或者密码输入错误或者验证方式不正确，这时候需要查看配置的验证用户名、密码以及验证方式是否正确。

```
hiper% show session history

13:49:40        Outgoing Call @0:98-4066
13:49:40        Call Connected , on Line  1, on Channel  0
13:49:40        PPPoE Up 00:90:1a:40:3a:4c
13:50:11        Call Terminated @clearSession:98
```

图 2-6 显示 PPPoE 拨号历史记录——拨号失败实例 2

2.5 PPPoE 典型配置实例

2.5.1 实例 1——单 PPPoE 拨号线路上网

1. 需求：

某网吧使用 HiPER 作为宽带接入路由器，采用单线路上网，接入方式为 PPPoE 拨号。ISP 分配的上网帐号为 ad12345678，密码为 123456，采用 CHAP 验证方式；拨号类型为自动拨号；不限制拨号时段，限制上线时段；不限制会话时间，限制空闲时间为 3600 秒。

2. 配置步骤：

1) PPPoE 上网线路配置

！新建一个 PPPoE 拨号连接实例，自定义连接名为 PPPOE
```
new connection/PPPOE
```
！设置一个首拨号码（任意值）
```
set connection/PPPOE dial first 1
```
！设置 PPP 验证方式、用户名、密码
```
set connection/PPPOE encaps send authtype chap
set connection/PPPOE encaps send name ad12345678
set connection/PPPOE encaps send pw 123456
```
！启用 PPPoE 客户端功能
```
set connection/PPPOE pppoe type client
```
！设置拨号类型为自动拨号
```
set connection/PPPOE line calltype AO/Switched
set connection/PPPOE line dialoutspoof yes
```
！设置空闲时间为 3600 秒
```
set connection/PPPOE dial idletimeout 3600
```
！保存配置
```
write
```

2) NAT 相关配置

此外，要实现局域网计算机通过 HiPER 共享上网，还需启用 NAT 功能，并配置相关的 NAT 规则。相关配置如下，各配置命令的涵义请参考《HiPER 命令行配置手册——NAT 配置》中相关部分。

！启用 NAT 功能
```
set ip nat routing enabled
```

！新建一条 NAT 规则，自定义规则名为 PEBIND
```
new ip nat binding/PEBIND
```

！将 NAT 规则绑定到 PPPoE 拨号线路
```
set ip nat binding/PEBIND profile PPPOE
```

！设置 NAT 规则的类型为 EasyIP
```
set ip nat binding/PEBIND natMethod EasyIP
```

！保存配置
```
write
```

2.5.2 实例 2——双 PPPoE 拨号线路上网

1. 需求：

某公司使用 HiPER 作为宽带接入路由器，采用双线路上网，使用线路备份方式，接入方式都为 PPPoE 拨号。ISP 为主线路（接在 WAN 口的线路）分配的上网帐号为 ad12345678，密码为 123456，采用 CHAP 验证方式；拨号类型为自动拨号；不限制拨号时段和上线时段；不限制会话时间和空闲时间。ISP 为备份线路（接在 WAN2/DMZ 口的线路）分配的上网帐号为 ad11223344，密码为 654321，采用 CHAP 验证方式；拨号类型也为自动拨号；不限制拨号时段和上线时段；不限制会话时间和空闲时间。

2. 分析：

由于双线路为线路备份方式，因此主线路的优先级必须比备份线路的优先级高，主线路的断开优先级也必须比备份线路的断开优先级高。这样的话，主线路可使用系统提供的缺省优先级和断开优先级：分别为 60 和 120；备份线路必须设置较低的优先级和断开优先级：不妨设为 61 和 121。

由于是双线路上网，因此必须配置按端口拨号：主线路从 WAN 端口呼出；备份线路从 WAN2/DMZ 端口呼出。首先需要启用呼叫分组功能，并配置 WAN 口、WAN2/DMZ 口的呼叫组号分别为 5 和 6；然后主线路必须配置以 5 开头的首拨号码，备份线路必须配置以 6 开头的首拨号码。

3. 配置步骤：

1) 配置呼叫分组功能及呼叫组号

！启用呼叫分组功能
```
set system dialergroup enabled
```

！设置 WAN 口的呼叫组号为 5
```
set interface ethernet/2 dialergroup 5
```

！设置 WAN2/DMZ 的呼叫组号为 6

```
set interface ethernet/3 dialergroup 6
```

！保存配置
```
write
```

2) 配置主线路对应的 PPPoE 拨号连接实例

！新建一个 PPPoE 拨号连接实例，自定义连接名为 PPPOE
```
new connection/PPPOE
```

！设置一个首拨号码（从 WAN 口呼出，必须以 5 开头）
```
set connection/PPPOE dial first 51
```

！设置 PPP 验证方式、用户名、密码
```
set connection/PPPOE encaps send authtype chap
set connection/PPPOE encaps send name ad12345678
set connection/PPPOE encaps send pw 123456
```

！启用 PPPoE 客户端功能
```
set connection/PPPOE pppoe type client
```

！设置拨号类型为自动拨号
```
set connection/PPPOE line calltype AO/Switched
set connection/PPPOE line dialoutspoof yes
```

！设置空闲时间为 0（即连接空闲不断线）
```
set connection/PPPOE dial idletimeout 0
```

！保存配置
```
write
```

3) 配置备份线路对应的 PPPoE 拨号连接实例

！新建一个 PPPoE 拨号连接实例，自定义连接名为 PPOE
```
new connection/PPOE
```

！设置一个首拨号码（从 DMZ 口呼出，必须以 6 开头）
```
set connection/PPOE dial first 61
```

！设置 PPP 验证方式、用户名、密码
```
set connection/PPOE encaps send authtype chap
set connection/PPOE encaps send name ad11223344
set connection/PPOE encaps send pw 654321
```

！启用 PPPoE 客户端功能
```
set connection/PPOE pppoe type client
```

！设置拨号类型为自动拨号
```
set connection/PPOE line calltype AO/Switched
set connection/PPOE line dialoutspoof yes
```

！设置空闲时间为 0（即连接空闲不断线）
```
set connection/PPPOE dial idletimeout 0
```

！设置路由优先级和断开优先级分别为 61 和 121
```
set connection/PPOE ip preference up 61
```

```
set connection/PPOE ip preference down 121
```

保存配置

```
write
```

4) NAT 相关配置

此外，要实现局域网计算机通过 HiPER 共享上网，还需启用 NAT 功能，并配置相关的 NAT 规则。相关配置如下，各配置命令的涵义请参考《HiPER 命令行配置手册——NAT 配置》中相关部分。

！启用 NAT 功能

```
set ip nat routing enabled
```

！新建一条主线路 NAT 规则，自定义规则名为 PEBIND

```
new ip nat binding/PEBIND
```

！将主线路 NAT 规则绑定到主线路

```
set ip nat binding/PEBIND profile PPPOE
```

！设置主线路 NAT 规则的类型为 EasyIP

```
set ip nat binding/PEBIND natMethod EasyIP
```

！新建一条备份线路 NAT 规则，自定义规则名为 PBIND

```
new ip nat binding/PBIND
```

！将备份线路 NAT 规则绑定到备份线路

```
set ip nat binding/PBIND profile PPOE
```

！设置备份线路 NAT 规则的类型为 EasyIP

```
set ip nat binding/PBIND natMethod EasyIP
```

！保存配置

```
write
```

第3章 L2TP/PPTP 配置

3.1 L2TP/PPTP 简介

3.1.1 L2TP 简介

L2TP 协议是一种虚拟专用网协议（VPN），该协议可以完成 PPP 封装的数据包在 IP 网络上的传送，L2TP 协议工作在客户端/服务器（Client/Server） 模式下，通信的双方拨出（发起呼叫）的一方叫客户端（Client），拨入（接受呼叫）的一方叫服务器（Server）。使用 L2TP 协议可以在 IP 网（如宽带网）中提供类似于拨号网络（如电话线）的远程接入服务，扩展企业网的范围，实现 VPN 应用。

在 HiPER 中，L2TP 客户端工作在 LAC 模式下，L2TP 服务器工作在 LNS 模式下。关于 HiPER 中 L2TP 的具体实现及应用，请参考《HiPER ReoS 5.0 VPN 配置手册》。

3.1.2 PPTP 简介

PPTP 协议是一种虚拟专用网协议（VPN），该协议可以完成 PPP 封装的数据包在以太网上的传送，PPTP 协议工作在客户端/服务器（Client/Server）模式下，通信的双方拨出（发起呼叫）的一方叫客户端（Client），拨入（接受呼叫）的一方叫服务器（Server）。使用 PPTP 协议可以在 IP 网（如宽带网）中提供类似于拨号网络（如电话线）的远程接入服务，扩展企业网的范围，实现 VPN 应用。

在 HiPER 中，PPTP 客户端工作在 PNS 模式下，PPTP 服务器工作在 PAC 模式下。关于 HiPER 中 PPTP 的具体实现及应用，请参考《HiPER ReoS 5.0 VPN 配置手册》。

3.2 L2TP/PPTP 全局配置

要保证 L2TP/PPTP 隧道能够正常工作，必须进行相关的 L2TP/PPTP 全局配置。L2TP/PPTP 全局配置主要包括以下几个方面的内容。其中，“ 配置 L2TP/PPTP VPN 地址池 ”和“ 允许/禁止客户端手工指定 IP 地址 ” 仅仅是有关 L2TP/PPTP 服务器的全局配置。

- 配置系统启用的第二层隧道协议类型
- 配置系统的工作模式
- 配置 L2TP/PPTP VPN 地址池——L2TP 服务器
- 允许/禁止客户端手工指定 IP 地址——L2TP 服务器
- 相关的 NAT 静态映射配置

3.2.1 配置系统启用的第二层隧道协议类型

缺省情况下，HiPER 是不启用任何第二层隧道协议的。可以将系统配置为仅启用 L2TP 协议，或者仅启用 PPTP 协议，或者同时启用 L2TP 协议和 PPTP 协议。

配置命令如表 3-1 所示。

操作	命令
配置系统不启用第二层隧道协议	**set ip vpn tunnelmode none**
配置系统启用 L2TP 协议	**set ip vpn tunnelmode L2TP**
配置系统启用 PPTP 协议	**set ip vpn tunnelmode PPTP**
配置系统同时启用 L2TP 协议和 PPTP 协议	**set ip vpn tunnelmode any**
备注：“ **ip vpn tunnelmode** ”缺省值为 none，即系统不启用第二层隧道协议。	

表 3-1 配置系统启用的第二层隧道协议类型

3.2.2 配置系统启用的工作模式

HiPER 作为 L2TP 客户端时，工作在 LAC 模式下；作为 L2TP 服务器时，工作在 LNS 模式下。根据需要，可将 HiPER 配置为工作在 LAC 模式下，或者工作在 LNS 模式下，或者同时工作在 LNS 和 LAC 模式下。

配置命令如表 3-2 所示。

操作	命令
配置系统禁用 LAC 和 LNS 工作模式	**set ip vpn l2tpmode none**
配置系统工作在 LAC 模式下	**set ip vpn l2tpmode LAC**
配置系统工作在 LNS 模式下	**set ip vpn l2tpmode LNS**
配置系统同时工作在 LNS 和 LAC 模式下	**set ip vpn l2tpmode Both**
备注：“ **ip vpn l2tpmode** ”缺省值为 none，即系统禁用 LAC 和 LNS 工作模式。	

表 3-2 配置系统启用的 L2TP 工作模式

HiPER 作为 PPTP 客户端时，工作在 PNS 模式下；作为 PPTP 服务器时，工作在 PAC 模式下。根据需要，可将 HiPER 配置为工作在 PNS 模式下，或者工作在 PAC 模式下，或者同时工作在 PNS 和 PAC 模式下。

配置命令如表 3-3 所述。

操作	命令

配置系统禁用 PNS 和 PAC 工作模式	**set ip vpn pptpmode disabled**
配置系统工作在 PNS 模式下	**set ip vpn pptpmode PNS**
配置系统工作在 PAC 模式下	**set ip vpn pptpmode PAC**
配置系统同时工作在 PNS 和 PAC 模式下	**set ip vpn pptpmode Both**
备注：“ **ip vpn l2tpmode** ”缺省值为 none，即系统禁用 LAC 和 LNS 工作模式。	

表 3-3 配置系统启用的 PPTP 工作模式

3.2.3 配置 L2TP/PPTP VPN 地址池——L2TP/PPTP 服务器

在 HiPER 中，所有的 L2TP/PPTP 服务器连接实例是共享 L2TP/PPTP VPN 地址池的。当 L2TP/PPTP 服务器被设置为允许分配 IP 地址时（参见章节 3.4.7），它会从 L2TP/PPTP VPN 地址池中将一个空闲的 IP 地址分配给客户端，作为连接 L2TP/PPTP 隧道两端的路由地址。

在 HiPER 中，最多可允许配置 3 个 L2TP/PPTP VPN 地址池。在实际的应用中，当 HiPER 作为 L2TP/PPTP 服务器为客户端分配 IP 地址时，系统将首先使用第一个地址池；当第一个地址池中的地址分配完了之后，再使用第二个地址池；当第二个地址池中的地址也分配完了之后，才会使用第三个地址池。

当 HiPER 作为 L2TP/PPTP 服务器使用时，如果希望为 L2TP/PPTP 拨入用户自动分配 IP 地址，就必须设置 L2TP/PPTP VPN 地址池。一般情况下，只需设置第一个 L2TP/PPTP VPN 地址池即可满足要求。对于每一个 L2TP/PPTP VPN 地址池来说，允许不设置地址池的名称；地址池中的 IP 地址可以是任意网段的 IP 地址，但是不能和整个 VPN 方案中已有的任何 IP 地址段重复。

配置命令如表 3-4 所示。

操作		命令
配置第一个 L2TP/PPTP VPN 地址池	设置地址池的名称	**set ip pool pooL1name *name***
	设置地址池的起始 IP 地址	**set ip pool pooL1start** *ip-address*
	设置地址池的地址数量	**set ip pool pooL1count** *count*
配置第二个 L2TP/PPTP VPN 地址池	设置地址池的名称	**set ip pool pooL2name *name***
	设置地址池的起始 IP 地址	**set ip pool pooL2start** *ip-address*
	设置地址池的地址数量	**set ip pool pooL2count** *count*
配置第三个 L2TP/PPTP VPN 地址池	设置地址池的名称	**set ip pool pooL3name *name***
	设置地址池的起始 IP 地址	**set ip pool pooL3start** *ip-address*
	设置地址池的地址数量	**set ip pool pooL3count** *count*
备注：缺省情况下，三个地址池的“ ***name*** ”值都为空，“ *ip-address* ”值都为 0.0.0.0，“ *count* ”值都为 0。 此外，配置每个地址池时，允许不设置地址池的名称。		

表 3-4 配置 L2TP/PPTP VPN 地址池——L2TP/PPTP 服务器

3.2.4 允许/禁止客户端手工指定 IP 地址——L2TP/PPTP 服务器

某些应用中，L2TP/PPTP 客户端希望使用固定的 IP 地址作为虚端口地址。这种情况下，如果是 HiPER 作为 L2TP/PPTP 服务器，就必须允许 L2TP/PPTP 客户端使用手工指定的 IP 地址作为虚端口地址。

但是，为安全性起见，某些情况下，可以将系统设置为：禁止 L2TP/PPTP 客户端手工指定 IP 地址，只允许使用系统从 L2TP/PPTP VPN 地址池中自动分配给客户端的 IP 地址作为虚端口地址。

配置命令如表 3-5 所示。

操作	命令
禁止 L2TP/PPTP 客户端手工指定 IP 地址	**set ip pool poolonly yes**
允许 L2TP/PPTP 客户端手工指定 IP 地址	**set ip pool poolonly no**
备注：缺省情况下，允许 L2TP/PPTP 客户端自己指定 IP 地址。	

表 3-5 允许/禁止客户端手工指定 IP 地址——L2TP/PPTP 服务器

3.2.5 相关的 NAT 静态映射配置

L2TP 协议使用 UDP 1701 端口建立连接和传输数据；PPTP 协议使用 TCP 1723 端口建立连接，使用 GRE 协议传输数据。

如果 HiPER 启用了 NAT 功能，当 HiPER 作为 L2TP 服务器或 L2TP 客户端使用时，为保证 L2TP 隧道能够正常连接，在配置完 L2TP 隧道相关参数后，还需配置一条 UDP 1701 端口的 NAT 静态映射；当 HiPER 作为 PPTP 服务器或 PPTP 客户端使用时，为保证 PPTP 隧道能够正常连接，在配置完 PPTP 隧道相关参数后，还需配置一条 TCP 1723 端口以及一条 GRE 协议的 NAT 静态映射。

关于 NAT 静态映射相关命令的具体涵义及用法请参考手册《HiPER 命令行配置手册——NAT 配置》中相关部分，这里不再具体描述。

上述三条 NAT 静态映射的具体配置如下：

1. 配置 UDP 1701 端口的 NAT 静态映射（L2TP 用）

！新建一条 NAT 映射，名字为 l2tp-map
```
new ip nat static/l2tp-map
```
！ 协议为 UDP
```
set ip nat static/l2tp-map protocol udp
```
！ 内部端口和外部端口均为 1701
```
set ip nat static/l2tp-map dstport 1701
set ip nat static/l2tp-map localport 1701
```

！内部地址为 HiPER 的 LAN 口地址
set ip nat static/l2tp-map localaddress *localaddress*

！绑定到主线路上，*binding-name* 为主线路 NAT 规则名
set ip nat static/l2tp-map binding *binding-name*

！设置端口 1701 在 NAT 前后保持不变
set ip nat static/l2tp-map autolocalIP yes

2. 配置 TCP 1723 端口的 NAT 静态映射（PPTP 用）

！新建一条 NAT 映射，名字为 pptp-map
new ip nat static/pptp-map

！协议为 TCP
set ip nat static/pptp-map protocol tcp

！内部端口和外部端口均为 1723
set ip nat static/pptp-map dstport 1723
set ip nat static/pptp-map localport 1723

！内部地址为 HiPER 的 LAN 口地址
set ip nat static/pptp-map localaddress *localaddress*

！绑定到主线路上，*binding-name* 为主线路 NAT 规则名
set ip nat static/l2tp-map binding *binding-name*

！设置端口 1723 在 NAT 前后保持不变
set ip nat static/pptp-map autolocalIP yes

3. 配置 GRE 协议的 NAT 静态映射（PPTP 用）

！新建一条 NAT 映射，名字为 gre-map
new ip nat static/gre-map

！协议为 GRE
set ip nat static/gre-map protocol gre

！内部地址为 HiPER 的 LAN 口地址
set ip nat static/gre-map localaddress *localaddress*

！绑定到主线路上，*binding-name* 为主线路 NAT 规则名
set ip nat static/gre-map binding *binding-name*

3.3 L2TP/PPTP 客户端配置

L2TP/PPTP 客户端配置主要包括以下内容：

- 新建一个 L2TP/PPTP 客户端连接实例
- 配置描述信息
- 配置首拨号码
- 启用 PPP 封装
- 配置 PPP 验证方式及用户名、密码
- 配置 PPP 压缩

- 启用/禁用 L2TP/PPTP 客户端功能
- 配置第二层隧道协商的协议类型
- 配置隧道服务器地址（域名）
- 配置远端内网地址
- 配置虚端口地址
- 配置 MRU 和 MTU
- 配置拨号类型
- 配置拨号时段和上线时段
- 配置空闲时间和会话时间
- 配置 lqm 检测
- 配置路由优先级和断开优先级
- 启用/禁用一个 L2TP/PPTP 客户端连接实例
- 删除一个 L2TP/PPTP 客户端连接实例

3.3.1 新建一个 L2TP/PPTP 客户端连接实例

首先，需要创建一个 L2TP/PPTP 客户端连接实例，并为该连接实例自定义一个名字。

配置命令如表 3-6 所示。

操作	命令
新建一个 L2TP/PPTP 客户端连接实例	**new connection/***conn-name*
备注：“ *conn-name* ”为自定义的 L2TP/PPTP 客户端连接实例的名称。	

表 3-6 新建一个 L2TP/PPTP 客户端连接实例

3.3.2 配置描述信息

当系统有多条连接实例存在时，为区别这些连接实例，方便辨别，可以为连接实例增加描述信息。一般情况下，无需设置。

配置命令如表 3-7 所示：

操作	命令
对 L2TP/PPTP 客户端连接实例进行描述	**set connection/***conn-name* **description** *description*
备注：“ **description** ”缺省值为空。	

表 3-7 对 L2TP/PPTP 客户端连接实例进行描述

3.3.3 配置首拨号码

如前所述（参见章节 1.4.1），必须为 L2TP/PPTP 客户端连接实例设置首拨号码（dial first）。如没有首拨号码，拨号行为就不会发生。

相关配置命令如表 3-8 所示。

操作	命令
配置 L2TP/PPTP 客户端连接实例的首拨号码	**set connection/***conn-name* **dial first** *dial-num*
备注：缺省情况下，“ **dial first** ”的值为空。	

表 3-8 配置 L2TP/PPTP 客户端连接实例的首拨号码

3.3.4 启用 PPP 封装

由于 L2TP/PPTP 隧道是建立在 PPP 基础上的，因此，首先需要通过 PPP 协议封装数据包，即在 L2TP/PPTP 客户端连接实例上启用 PPP 封装。

缺省情况下，L2TP/PPTP 客户端连接实例是启用 PPP 封装的，因此，无需修改相关配置。

配置命令如表 3-9 所示。

操作	命令
在 L2TP/PPTP 客户端连接实例上启用 PPP 封装	**set connection/***conn-name* **encaps type ppp**
备注：“ **encaps type** ”缺省值为“ **ppp** ”。	

表 3-9 在 L2TP/PPTP 客户端连接实例上启用 PPP 封装

3.3.5 配置 PPP 验证方式及用户名、密码

HiPER 作为 L2TP/PPTP 客户端与远端 L2TP/PPTP 服务器进行拨号连接时，在 PPP 协商过程中支持以下几种身份验证方式：

- **None**：不进行 PPP 验证；
- **PAP**：口令验证协议；
- **CHAP**：质询握手验证协议；
- **MS-CHAP**：微软质询握手验证协议。

如果选择了 PAP、CHAP 以及 MS-CHAP 中的任一种作为 PPP 验证方式，那么，还需设置相关的验证用户名及密码。在 PPP 协商的过程中，验证方（服务器）和被验证方（客户端）的身份验证方式、用户名及密码必须一致。

配置命令如表 3-10 所示。

操作	命令
配置 PPP 验证方式	**set connection/***conn-name* **encaps send authtype** {**None	PAP	CHAP	MS-CHAP** }
配置 PPP 验证时本地发送的用户名	**set connection/***conn-name* **encaps send name** *ppp-name*
配置 PPP 验证时本地发送的密码	**set connection/***conn-name* **encaps send pw** *ppp-password*

备注：缺省情况下，“ **send authtype** ”值为 PAP，“ **send name** ”和“ **send pw** ”的值都为空。

表 3-10 配置 PPP 验证方式及用户名、密码——L2TP/PPTP 客户端

3.3.6 配置 PPP 压缩

缺省情况下，PPP 层上不使用数据压缩，但是，HiPER 可支持以下几种数据压缩方法：

- **Stac**：stac 压缩方法；
- **Stac-9**：stac-9 压缩算法；
- **MS-Stac**：微软 stac 压缩算法。

一般情况下，无需配置 PPP 压缩的。但是，如果 L2TP/PPTP 隧道对端设备启用了某种 PPP 压缩方法，那么，在这里必须配置与之相同的压缩方法。

配置命令如表 3-11 所示。

操作	命令
配置 PPP 压缩	**set connection/***conn-name* **encaps comp** {**None | Stac | Stac-9 | MS-Stac** }
备注：缺省情况下，“ **encaps comp** ”值为“ **None** ”，即禁止使用数据压缩。	

表 3-11 配置 PPP 压缩——L2TP/PPTP 客户端

3.3.7 启用/禁用 L2TP/PPTP 客户端功能

缺省情况下，新建的拨号连接是禁用第二层隧道客户端功能的，此时，它将仅仅向拨号服务器发起 PPP 协商。因此，对于 L2TP/PPTP 客户端连接实例来说，必须启用第二层隧道客户端功能，它才会向 L2TP/PPTP 服务器主动发起第二层隧道协商。

配置命令如表 3-12 所示。

操作	命令
启用 L2TP/PPTP 客户端功能	**set connection/***conn-name* **tunnel type client**
禁用 L2TP/PPTP 客户端功能	**set connection/***conn-name* **tunnel type disabled**
备注：缺省情况下，“ **tunnel type”**的值为“ **disabled** ”。	

表 3-12 启用/禁用 L2TP/PPTP 客户端功能

3.3.8 配置第二层隧道协商的协议类型

如果当前连接实例是作为 L2TP 客户端使用的，那么，必须将它设置为向隧道服务器发起 L2TP 协商；如果当前连接实例是作为 PPTP 客户端使用的，那么，必须将它设置为向隧道服务器发起 PPTP 协商。

配置命令如表 3-13 所示。

操作	命令
禁止发起第二层隧道协商	**set connection**/*conn-name* **tunnel protocol disabled**
配置当前客户端向隧道服务器发起 L2TP 协商	**set connection**/*conn-name* **tunnel protocol L2TP**
配置当前客户端向隧道服务器发起 PPTP 协商	**set connection**/*conn-name* **tunnel protocol PPTP**
备注：缺省情况下，“ **tunnel ”**的值为 “ **disabled** ”。	

表 3-13 配置第二层隧道协商的协议类型

3.3.9 配置隧道服务器地址（域名）

对于 L2TP/PPTP 客户端连接实例来说，必须配置隧道服务器的地址或者域名。配置后，系统会向指定的隧道服务器发起第二层隧道协商。

配置命令如表 3-14 所示。

操作	命令
配置隧道服务器的地址（域名）	**set connection**/*conn-name* **tunnel serveraddress** *serveraddress*
备注：缺省情况下，“ **serveraddress”**的值为空。	

表 3-14 配置隧道服务器的地址（域名）

提示：如果配置的是隧道服务器的域名，必须在 HiPER 中配置 DNS 服务器，HiPER 才能与隧道服务器进行协商。

3.3.10 配置远端内网地址

远端内网地址即 L2TP/PPTP 隧道对端局域网的地址，它由参数 “ 远端内网 IP 地址 ” 和 “ 远端内网子网掩码 ” 来设置。其中，“ 远端内网 IP 地址 ” 为远端内网中任意一个合法的 IP 地址，一般可以设置为 L2TP/PPTP 隧道对端设备的 LAN 口 IP 地址，也可以设置为远端内网的子网号。

配置命令如表 3-15 所示。

操作	命令
配置远端内网 IP 地址	**set connection**/*conn-name* **ip address remoteip** *ip-address*
配置远端内网子网掩码	**set connection**/*conn-name* **ip address remotemask** *ip-netmask*
备注：缺省情况下，“ **remoteip”**的值和 “ **remotemask** ” 的值都为 0.0.0.0。	

表 3-15 配置远端内网地址——L2TP/PPTP 客户端

提示：配置完 “ 远端内网 IP 地址 ” 和 “ 远端内网子网掩码 ” 之后，系统会自动生成一条目的地址为预设的 “ *ip-address* ” 的主机路由，其网络掩码为 255.255.255.255；以及一条目的地址也为 “ *ip-address* ” 的子网路由，其网络掩码为预设的 “ *ip-netmask* ”。

3.3.11 配置虚端口地址

当 L2TP/PPTP 隧道两端设备建立连接时，会各用一个虚端口来连接对方。一般情况下，L2TP/PPTP 服务器会从地址池中分配一个 IP 地址作为两个虚端口的路由地址，具体可参见章节 3.4.8。但是，某些 L2TP/PPTP 服务器并没有配置地址池，此时需要为隧道两端设备的虚端口配置 IP 地址作为各自的路由地址。

在 HiPER 中，无论是 L2TP/PPTP 客户端连接实例，还是 L2TP/PPTP 服务器连接实例，都要求本地虚端口和对端虚端口处于同一个子网中；因此，本地虚端口和对端虚端口将使用同一个子网掩码。

配置命令如表 3-16 所示。

操作	命令
配置本地虚端口 IP 地址	**set connection**/*conn-name* **ip address wanif** *ip-address*
配置远端虚端口 IP 地址	**set connection**/*conn-name* **ip address localif** *ip-address*
配置虚端口子网掩码	**set connection**/*conn-name* **ip address localmask** *ip-netmask*
备注：缺省情况下，“ **wanif**”、“ **localif** ”的值和“ **localmask** ”的值都为 0.0.0.0。	

表 3-16 配置虚端口地址——L2TP/PPTP 客户端

3.3.12 配置 MRU 和 MTU

一般情况下，数据包接收者的最大接收单元（MRU）必须大于等于数据包发送者的最大发送单元（MTU）。HiPER 中，L2TP/PPTP 客户端连接实例的 MRU 和 MTU 的缺省值均为 1524 字节，L2TP/PPTP 拨号时 HiPER 将自动与对方设备协商，除非特别应用，不要修改。

配置命令如表 3-17 所示。

操作	命令
配置 L2TP/PPTP 客户端的最大接收单元	**set connection**/*conn-name* **encaps mru** *mru-size*
配置 L2TP/PPTP 客户端的的最大发送单元	**set connection**/*conn-name* **encaps mtu** *mtu-size*
备注：缺省情况下，“ **encaps mru** ”和“ **encaps mtu** ”的值都为 1524，单位为字节。	

表 3-17 配置 MRU 和 MTU——L2TP/PPTP 客户端

3.3.13 配置拨号类型

如前所述（参见章节 1.4.3），HiPER 支持三种 L2TP/PPTP 拨号类型：

- 自动拨号：当 L2TP/PPTP 客户端连接实例的参数配置完成后，或者开启 HiPER 时，或者上一次 L2TP/PPTP 隧道连接中断，L2TP/PPTP 客户端将自动拨号（发起建立隧道请求）；
- 按需拨号：当 L2TP/PPTP 客户端连接实例的参数配置完成后，一旦 L2TP/PPTP 客

户端监听到有数据需要传输，就拨号（发起建立隧道请求）。

- 手动拨号：只能通过人工进行连接和挂断 L2TP/PPTP 隧道。

L2TP/PPTP 拨号类型是由 L2TP/PPTP 客户端连接实例的两个属性来确定的，即“ **line calltype** ”和“ **line dialoutSpoof** ”。各拨号类型下，这两个属性对应的值如表 3-18 所示。

拨号类型 / 相关属性	自动拨号	按需拨号	手动拨号	备注
line calltype	**AO/Switched**	**Switched**	**Switched**	缺省情况下，拨号类型为手动拨号。
line dialoutSpoof	**Yes**	**Yes**	**No**	

表 3-18 L2TP/PPTP 拨号类型的相关属性值

相关配置命令如表 3-19 所示。

操作	命令
配置拨号类型为自动拨号	**set connection/***conn-name* **line calltype AO/Switched** **set connection/***conn-name* **line dialoutspoof Yes**
配置拨号类型为按需拨号	**set connection/***conn-name* **line calltype Switched** **set connection/***conn-name* **line dialoutspoof Yes**
配置拨号类型为手动拨号	**set connection/***conn-name* **line calltype Switched** **set connection/***conn-name* **line dialoutspoof No**
备注：缺省情况下，“ **line calltype** ”的值为“ Switched ”，“ **line dialoutspoof** ”的值为“ no ”，即拨号类型为手动拨号。	

表 3-19 配置 L2TP/PPTP 拨号类型

3.3.14 配置拨号时段和上线时段

如前所述（参见章节 1.4.5），可以为 L2TP/PPTP 客户端连接实例设置拨号时段和上线时段。

- 拨号时段（**dial dialTimeRange**）：允许 L2TP/PPTP 客户端拨号的时间段，只有在此时间段范围内才允许 L2TP/PPTP 客户端触发拨号，不设置代表不对拨号时段进行控制。
- 上线时段（**dial callTimeRange**）：允许 L2TP/PPTP 客户端保持隧道连接的时间段，如果超出这个时间段时，对应 L2TP/PPTP 隧道处于连接状态，HiPER 将会自动断开 L2TP/PPTP 隧道连接，不设置代表不对上线时段进行控制。

配置命令如表 3-20 所示。

操作	命令
配置 L2TP/PPTP 客户端的拨号时段	**set connection/***conn-name* **dial dialTimeRange** *time-name*
配置 L2TP/PPTP 客户端的上线时段	**set connection/***conn-name* **dial callTimeRange** *time-name*

备注：缺省情况下，“ **dial dialTimeRange** ”和“ **dial callTimeRange** ”的值都为空。

表 3-20 配置拨号时段和上线时段——L2TP/PPTP 客户端

提示：“ *time-name* ”为引用的时间段策略的名称，具体涵义及配置方法请参考手册《HiPER CLI 配置手册——基本配置》中的第 4 章（时间段配置）。

3.3.15 配置空闲时间和会话时间

如前所述（参见章节 1.4.4），对于拨号类型为按需拨号或手动拨号的 L2TP/PPTP 客户端来说，可以设置空闲时间和会话时间。

- 空闲时间（**dial idleTimeout**）：在没有访问流量后自动断线前等待的时长，当 L2TP/PPTP 隧道连接成功后，如果隧道空闲（没有数据传输）的时间超过了预设的“ 空闲时间 ”，HiPER 将主动断开连接。缺省值为 0，代表不自动断线，即连接空闲不自动挂断。单位：秒。
- 会话时间（**dial sessionTimeout**）：即连接生存时间（一般无需设置），一旦 L2TP/PPTP 隧道连接的时间（从拨号成功开始）超出了预设的“ 会话时间 ”，HiPER 将主动断开隧道连接。缺省值为 0，代表不限制会话时间。单位：秒。

配置命令如表 3-21 所示。

操作	命令
配置 L2TP/PPTP 客户端的空闲时间	**set connection**/*conn-name* **dial idleTimeout** *idle-time*
配置 L2TP/PPTP 客户端的会话时间	**set connection**/*conn-name* **dial sessionTimeout** *session-time*
备注：缺省情况下，“ **dial idleTimeout** ”的值为 120，“ **dial sessionTimeout** ”的值为 0。	

表 3-21 配置空闲时间和会话时间——L2TP/PPTP 客户端

提示：如果 L2TP/PPTP 客户端的拨号类型为自动拨号方式，空闲时间和会话时间是没有意义的，即便设置了空闲时间和会话时间，它们也不会对该 L2TP/PPTP 客户端起作用。这是因为，在自动拨号方式下，当 L2TP/PPTP 客户端拨号成功后，除非是对方设备主动挂断或者该 L2TP/PPTP 客户端所依赖的物理资源不能正常工作，HiPER 是不会主动挂断隧道连接的。

3.3.16 配置 lqm 检测

如前所述（参见章节 1.4.6），在 L2TP/PPTP 客户端连接实例上可启用 lqm 检测，并设置“ lqm 检测间隔 ”和“ lqm 生命周期 ”。

- lqm 检测间隔（**encaps lqm min**）：发送 lqm 检测包的时间间隔。单位：毫秒。
- lqm 生命周期（**encaps lqm max**）：lqm 检测包的统计周期。单位：毫秒。

如果启用了 lqm 检测，在 L2TP/PPTP 隧道连接成功后，HiPER 将每隔“ lqm 检测间隔 ”向 L2TP/PPTP 隧道对端设备发送 lqm 检测包，如果在某个“ lqm 生命周期 ”范围内一直没有收到对方回应，则断开此连接。

配置命令如表 3-22 所示。

操作	命令
启用/禁用 lqm 检测	**set connection**/*conn-name* **encaps lqm active** { **yes**｜**no**}
配置 lqm 检测间隔	**set connection**/*conn-name* **encaps lqm min** *lqm-interval*
配置 lqm 生命周期	**set connection**/*conn-name* **encaps lqm max** *lqm-period*
备注：缺省情况下，“ **encaps lqm active** ”的值为“ **yes** ”，即启用 lqm 检测； “ **encaps lqm min** ”和“ **encaps lqm max** ”的值分别为 1000、15000，单位为毫秒。	

表 3-22 配置 lqm 检测——L2TP/PPTP 客户端

提示：对于 L2TP/PPTP 客户端来说，一般情况下无需启用 lqm 检测，系统会发送默认的 HELLO 数据包到 L2TP/PPTP 隧道对端设备来探测隧道连接是否正常。

3.3.17 配置路由优先级和断开优先级

如前所属（参见章节 3.3.10），当配置完“ 远端内网 IP 地址 ”和“ 远端内网子网掩码 ”之后，系统会自动生成对应的主机路由和子网路由。此处设置的路由优先级和断开优先级就是这两条路由的优先级和断开优先级。

优先级必须比断开优先级高，值越低优先级越高。关于优先级及断开优先级的应用，请参考《HiPER 命令行配置手册——网络层协议》的第 5 章。

配置命令如表 3-23 所示。

操作	命令
配置路由优先级	**set connection**/*conn-name* **ip preference up** *uppref*
配置路由断开优先级	**set connection**/*conn-name* **ip preference down** *downpref*
备注：缺省情况下，“ **ip preference up** ”和“ **ip preference down** ”的值分别为 60 和 120。	

表 3-23 配置路由优先级和断开优先级——L2TP/PPTP 客户端

3.3.18 启用/禁用一个 L2TP/PPTP 客户端连接实例

允许设置各个 L2TP/PPTP 客户端连接实例的使能状态：启用或禁用。启用时，相应的 L2TP/PPTP 客户端可以根据拨号规则向外发起连接。当禁用时，当前连接实例不能用，仅在 CLI 的配置文件中可见。

如果你暂时不需要使用某个 L2TP/PPTP 客户端连接实例，只需禁用该连接实例即可；当需要恢复使用该连接实例时，只需启用该连接实例即可。

配置命令如表 3-24 所示。

操作	命令
启用 L2TP/PPTP 客户端连接实例	**set connection**/*conn-name* **enabled yes**
禁用 L2TP/PPTP 客户端连接实例	**set connection**/*conn-name* **enabled no**

备注：缺省情况下，“ **enabled** ”的值为“ **yes** ”，即启用 L2TP/PPTP 客户端连接实例。

表 3-24 启用/禁用一个 L2TP/PPTP 客户端连接实例

3.3.19 删除一个 L2TP/PPTP 客户端连接实例

如果不再需要某 L2TP/PPTP 客户端连接实例，则可删除改连接实例。在 HiPER 中，一次只能删除一个 L2TP/PPTP 客户端连接实例。

配置命令如表 3-25 所示。

操作	命令
删除一个 L2TP/PPTP 客户端连接实例	**delete connection/***conn-name*
备注：删除某个 L2TP/PPTP 客户端连接实例时，输入的连接实例名“ *conn-name* ”必须与新建该连接实例时输入的连接实例名完全匹配。	

表 3-25 删除一个 L2TP/PPTP 客户端连接实例

3.4 L2TP/PPTP 服务器配置

L2TP/PPTP 服务器配置主要包括以下内容：

- 新建一个 L2TP/PPTP 服务器连接实例
- 配置描述信息
- 启用 PPP 封装
- 配置 PPP 验证方式及密码
- 配置 PPP 压缩
- 配置远端内网地址
- 允许/禁止分配 IP 地址
- 配置虚端口地址
- 配置 MRU 和 MTU
- 配置空闲时间和会话时间
- 配置 lqm 检测
- 配置路由优先级和断开优先级
- 启用/禁用一个 L2TP/PPTP 服务器连接实例
- 删除一个 L2TP/PPTP 服务器连接实例

3.4.1 新建一个 L2TP/PPTP 服务器连接实例

首先，需要创建一个 L2TP/PPTP 服务器连接实例，并为该连接实例自定义一个名字。需要注意的是，这个名字同时也作为验证 L2TP/PPTP 客户端时的用户名。

配置命令如表 3-26 所示。

操作	命令

新建一个 L2TP/PPTP 服务器连接实例	**new connection/***conn-name*
备注：“ *conn-name* ”为自定义的 L2TP/PPTP 服务器连接实例的名称。	

表 3-26 新建一个 L2TP/PPTP 服务器连接实例

3.4.2 配置描述信息

当系统有多条连接实例存在时，为区别这些连接实例，方便辨别，可以为连接实例增加描述信息。一般情况下，无需设置。

配置命令如表 3-27 所示：

操作	命令
对 L2TP/PPTP 服务器连接实例进行描述	**set connection/***conn-name* **description** *description*
备注：“ **description** ”缺省值为空。	

表 3-27 对 L2TP/PPTP 服务器连接实例进行描述

3.4.3 启用 PPP 封装

由于 L2TP/PPTP 隧道是建立在 PPP 基础上的，因此，首先需要通过 PPP 协议封装数据包，即在 L2TP/PPTP 服务器连接实例上启用 PPP 封装。

缺省情况下，L2TP/PPTP 服务器连接实例是启用 PPP 封装的，因此，无需修改相关配置。

配置命令如表 3-28 所示。

操作	命令
在 L2TP/PPTP 服务器连接实例上启用 PPP 封装	**set connection/***conn-name* **encaps type ppp**
备注：“ **encaps type** ”缺省值为“ **ppp** ”。	

表 3-28 在 L2TP/PPTP 服务器连接实例上启用 PPP 封装

3.4.4 配置 PPP 验证方式及密码

当远端 L2TP/PPTP 客户端与本地 L2TP/PPTP 服务器进行拨号连接时，在 PPP 协商过程中 HiPER 支持以下几种身份验证方式：

- **None**：不进行 PPP 验证；
- **PAP**：口令验证协议；
- **CHAP**：质询握手验证协议；
- **MS-CHAP**：微软质询握手验证协议。

如果选择了 PAP、CHAP 以及 MS-CHAP 中的任一种作为 PPP 验证方式，那么，还需设置相关的验证用户名及密码。注意，对于一个 L2TP/PPTP 服务器连接实例来说，新建该实

例时输入的名字即为 PPP 验证时使用的用户名。在 PPP 协商的过程中，验证方（服务器）和被验证方（客户端）的身份验证方式、用户名及密码必须一致。

配置命令如表 3-29 所示。

操作	命令
配置 PPP 验证方式	**set connection/***conn-name* **encaps send authtype** {**None | PAP | CHAP | MS-CHAP** }
配置 PPP 验证密码	**set connection/***conn-name* **encaps recv pw** *ppp-password*
备注：缺省情况下，“ **send authtype** ”值为 PAP，“ **send name** ”和“ **send pw** ”的值都为空。	

表 3-29 配置 PPP 验证方式及密码——L2TP/PPTP 服务器

3.4.5 配置 PPP 压缩

缺省情况下，PPP 层上是禁止使用数据压缩的，但是，HiPER 可支持以下几种数据压缩方法：

- **Stac**：stac 压缩方法；
- **Stac-9**：stac-9 压缩算法；
- **MS-Stac**：微软 stac 压缩算法。

一般情况下，无需配置 PPP 压缩的。但是，如果 L2TP/PPTP 隧道对端设备启用了某种 PPP 压缩方法，那么，在这里必须配置与之相同的压缩方法。

配置命令如表 3-30 所示。

操作	命令
配置 PPP 压缩	**set connection/***conn-name* **encaps comp** {**None | Stac | Stac-9 | MS-Stac** }
备注：缺省情况下，“ **encaps comp** ”值为“ **None** ”，即禁止使用数据压缩。	

表 3-30 配置 PPP 压缩——L2TP/PPTP 服务器

3.4.6 配置远端内网地址

远端内网地址即 L2TP/PPTP 隧道对端局域网的地址，它由参数“ 远端内网 IP 地址 ”和“ 远端内网子网掩码 ”来设置。其中，“ 远端内网 IP 地址 ”为远端内网中任意一个合法的 IP 地址，一般可以设置为 L2TP/PPTP 隧道对端设备的 LAN 口 IP 地址，也可以设置为远端内网的子网号。

配置命令如表 3-31 所示。

操作	命令
配置远端内网 IP 地址	**set connection/***conn-name* **ip address remoteip** *ip-address*
配置远端内网子网掩码	**set connection/***conn-name* **ip address remotemask** *ip-netmask*

备注：缺省情况下，“ **remoteip”**的值和 “ **remotemask** ” 的值都为 0.0.0.0。

表 3-31 配置远端内网地址——L2TP/PPTP 服务器

提示：

1. 配置完 “ 远端内网 IP 地址 ” 和 “ 远端内网子网掩码 ” 之后，系统会自动生成一条目的地址为预设的 “ *ip-address* ” 的主机路由，其网络掩码为 255.255.255.255；以及一条目的地址也为 “ *ip-address* ” 的子网路由，其网络掩码为预设的 “ *ip-netmask* ”。

2. 如果客户端为移动用户，一般情况下，无需设置 “ 远端内网 IP 地址 ” 和 “ 远端内网子网掩码 ”；但是，如果不是手工指定虚端口地址（章节 3.4.8），L2TP/PPTP VPN 地址池（章节 3.2.3）中也无空闲地址分配，那么可设置 “ 远端内网 IP 地址 ”，这时，系统将使用 “ 远端内网 IP 地址 ” 作为隧道两端设备的虚端口的路由地址。

3.4.7 允许/禁止分配 IP 地址

缺省情况下，是允许 L2TP/PPTP 服务器为拨入的用户（客户端）分配 IP 地址的；此时，L2TP/PPTP 服务器会从 L2TP/PPTP 地址池中将一个空闲的 IP 地址分配客户端，作为连接 L2TP/PPTP 隧道两端的路由地址。注意，所有拨入用户共享一个 L2TP/PPTP 地址池，地址池的配置请参见章节 3.2.3。

配置命令如表 3-32 所示。

操作	命令
允许为拨入的用户分配 IP 地址	**set connection/***conn-name* **ip assignip yes**
禁止为拨入的用户分配 IP 地址	**set connection/***conn-name* **ip assignip no**
备注：缺省情况下，为允许为拨入的用户分配 IP 地址。	

表 3-32 允许/禁止分配 IP 地址——L2TP/PPTP 服务器

3.4.8 配置虚端口地址

当 L2TP/PPTP 隧道两端设备建立连接时，会各用一个虚端口来连接对方。如果远程客户端没有设置在 VPN 内使用的虚端口的 IP 地址，就需要为其分配 IP 地址。这时，一般是 L2TP/PPTP 服务器从地址池中分配一个空闲的 IP 地址作为两个虚端口的路由地址，具体可参见章节 3.4.7、章节 3.2.3。

但是，某些情况下，L2TP/PPTP 客户端要求手工设置虚端口地址，这时就需要在 HiPER 中手工指定隧道两端设备的虚端口的 IP 地址。

在 HiPER 中，无论是作为 L2TP/PPTP 客户端，还是作为 L2TP/PPTP 服务器，都要求本地虚端口和对端虚端口处于同一个子网中；因此，本地虚端口和远端虚端口将使用同一个子网掩码。

配置命令如表 3-33 所示。

操作	命令

配置本地虚端口 IP 地址	**set connection**/*conn-name* **ip address wanif** *ip-address*
配置远端虚端口 IP 地址	**set connection**/*conn-name* **ip address localif** *ip-address*
配置虚端口子网掩码	**set connection**/*conn-name* **ip address localmask** *ip-netmask*
备注：缺省情况下，“ **wanif**”、“ **localif** ”的值和“ **localmask** ”的值都为 0.0.0.0。	

表 3-33 配置虚端口地址——L2TP/PPTP 服务器

3.4.9 配置 MRU 和 MTU

一般情况下，数据包接收者的最大接收单元（MRU）必须大于等于数据包发送者的最大发送单元（MTU）。HiPER 中，L2TP/PPTP 服务器连接实例的 MRU 和 MTU 的缺省值均为 1524 字节，L2TP/PPTP 拨号时 HiPER 将自动与对方设备协商，除非特别应用，不要修改。

配置命令如表 3-34 所示。

操作	命令
配置 L2TP/PPTP 服务器的最大接收单元	**set connection**/*conn-name* **encaps mru** *mru-size*
配置 L2TP/PPTP 服务器的的最大发送单元	**set connection**/*conn-name* **encaps mtu** *mtu-size*
备注：缺省情况下，“ **encaps mru** ”和“ **encaps mtu** ”的值都为 1524，单位为字节。	

表 3-34 配置 MRU 和 MTU——L2TP/PPTP 服务器

3.4.10 配置空闲时间和会话时间

如前所述（参见章节 1.4.4），HiPER 作为 L2TP/PPTP 服务器时，可以设置空闲时间和会话时间。

- 空闲时间（**dial idleTimeout**）：在没有访问流量后自动断线前等待的时长，当 L2TP/PPTP 隧道连接成功后，如果隧道空闲（没有数据传输）的时间超过了预设的“ 空闲时间 ”，HiPER 将主动断开连接。缺省值为 0，代表不自动断线，即连接空闲不自动挂断。单位：秒。
- 会话时间（**dial sessionTimeout**）：即连接生存时间（一般无需设置），一旦 L2TP/PPTP 隧道连接的时间（从拨号成功开始）超出了预设的“ 会话时间 ”，HiPER 将主动断开隧道连接。缺省值为 0，代表不限制会话时间。单位：秒。

配置命令如表 3-35 所示。

操作	命令
配置 L2TP/PPTP 客户端的空闲时间	**set connection**/*conn-name* **dial idleTimeout** *idle-time*
配置 L2TP/PPTP 客户端的会话时间	**set connection**/*conn-name* **dial sessionTimeout** *session-time*
备注：缺省情况下，“ **dial idleTimeout** ”的值为 120，“ **dial sessionTimeout** ”的值为 0。	

表 3-35 配置空闲时间和会话时间——L2TP/PPTP 服务器

3.4.11 配置 lqm 检测

如前所述（参见章节 1.4.6），在 L2TP/PPTP 客户端连接实例上可启用 lqm 检测，并设置“ lqm 检测间隔 ”和“ lqm 生命周期 ”。

- lqm 检测间隔（**encaps lqm min**）：发送 lqm 检测包的时间间隔。单位：毫秒。
- lqm 生命周期（**encaps lqm max**）：lqm 检测包的统计周期。单位：毫秒。

如果启用了 lqm 检测，在 L2TP/PPTP 隧道连接成功后，HiPER 将每隔“ lqm 检测间隔 ”向 L2TP/PPTP 隧道对端设备发送 lqm 检测包，如果在某个“ lqm 生命周期 ”范围内一直没有收到对方回应，则断开此连接。

配置命令如表 3-36 所示。

操作	命令
启用/禁用 lqm 检测	**set connection/***conn-name* **encaps lqm active** { **yes** | **no**}
配置 lqm 检测间隔	**set connection/***conn-name* **encaps lqm min** *lqm-interval*
配置 lqm 生命周期	**set connection/***conn-name* **encaps lqm max** *lqm-period*
备注：缺省情况下，“ **encaps lqm active** ”的值为“ **yes** ”，即启用 lqm 检测； “ **encaps lqm min** ”和“ **encaps lqm max** ”的值分别为 1000、15000，单位为毫秒。	

表 3-36 配置 lqm 检测——L2TP/PPTP 服务器

提示：对于 L2TP/PPTP 客户端来说，一般情况下无需启用 lqm 检测，系统会发送默认的 HELLO 数据包到 L2TP/PPTP 隧道对端设备来探测隧道连接是否正常。

3.4.12 配置路由优先级和断开优先级

如前所属（参见章节 3.3.9），当配置完“ 远端内网 IP 地址 ”和“ 远端内网子网掩码 ”之后，系统会自动生成对应的主机路由和子网路由。此处设置的路由优先级和断开优先级就是这两条路由的优先级和断开优先级。

优先级必须比断开优先级高，值越低优先级越高。关于优先级及断开优先级的应用，请参考《HiPER 命令行配置手册——网络层协议》的第 5 章。

配置命令如表 3-37 所示。

操作	命令
配置路由优先级	**set connection/***conn-name* **ip preference up** *uppref*
配置路由断开优先级	**set connection/***conn-name* **ip preference down** *downpref*
备注：缺省情况下，“ **ip preference up** ”和“ **ip preference down** ”的值分别为 60 和 120。	

表 3-37 配置优先级和断开优先级——L2TP/PPTP 服务器

3.4.13 启用/禁用一个 L2TP/PPTP 服务器连接实例

允许设置各个 L2TP/PPTP 客户端连接实例的使能状态：启用或禁用。启用时，相应的 L2TP/PPTP 客户端可以根据拨号规则向外发起连接。当禁用时，当前连接实例不能用，仅在 CLI 的配置文件中可见。

如果你暂时不需要使用某个 L2TP/PPTP 客户端连接实例，只需禁用该连接实例即可；当需要恢复使用该连接实例时，只需启用该连接实例即可。

配置命令如表 3-38 所示。

操作	命令
启用 L2TP/PPTP 客户端连接实例	**set connection/***conn-name* **enabled yes**
禁用 L2TP/PPTP 客户端连接实例	**set connection/***conn-name* **enabled no**
备注：缺省情况下，“ **enabled** ”的值为“ **yes** ”，即启用 L2TP/PPTP 客户端连接实例。	

表 3-38 启用/禁用一个 L2TP/PPTP 客户端连接实例

3.4.14 删除一个 L2TP/PPTP 服务器连接实例

如果不再需要某 L2TP/PPTP 客户端连接实例，则可删除改连接实例。在 HiPER 中，一次只能删除一个 L2TP/PPTP 客户端连接实例。

配置命令如表 3-39 所示。

操作	命令
删除一个 L2TP/PPTP 客户端连接实例	**delete connection/***conn-name*
备注：删除某个 L2TP/PPTP 客户端连接实例时，输入的连接实例名“ *conn-name* ”必须与新建该连接实例时输入的连接实例名完全匹配。	

表 3-39 删除一个 L2TP/PPTP 客户端连接实例

3.5 L2TP 隧道验证配置

PPTP 中，PPTP 客户端和 PPTP 服务器建立隧道的过程是不需要验证的。也就是说，PPTP 协议只有用户验证这一个验证过程。

但是，L2TP 中 LAC（L2TP 客户端）和 LNS（L2TP 服务器）之间建立隧道的过程中可以选择进行隧道验证，这时只有隧道验证通过后才会对拨号用户进行验证。隧道验证通过在 LAC 和 LNS 之间配置“ 设备 ID/共享密钥 ”来实现。在“ 隧道验证 ”过程中，通过 MD5 消息摘要算法来保证数据传输和验证过程本身的安全。

HiPER 中 L2TP 的实现缺省是不进行 L2TP 隧道验证，这也是绝大部分设备的出厂设置。采用这种配置，可以提高系统的 VPN 处理能力，加快系统建立 L2TP/PPTP 隧道的速度。

3.5.1 L2TP 服务器相关配置

3.5.1.1 启用/禁用 L2TP 隧道验证

HiPER 作为 L2TP 服务器使用时，如果要求进行 L2TP 隧道验证，那么，首先需要启用系统的隧道验证功能。此时，所有以 HiPER 作为 L2TP 服务器的 L2TP 隧道连接都必须进行隧道验证。

配置命令如表 3-40 所示。

操作	命令
启用 L2TP 隧道验证	**set ip vpn L2tpAuth yes**
禁用 L2TP 隧道验证	**set ip vpn L2tpAuth no**
备注：此命令为全局命令。如果在 HiPER（L2TP 服务器）中启用了 L2TP 隧道验证，那么，所有以 HiPE 作为 L2TP 服务器的 L2TP 隧道连接都必须进行隧道验证。	

表 3-40 启用/禁用 L2TP 隧道验证——L2TP 服务器

3.5.1.2 配置对端主机名及隧道密码

在启用了 L2TP 隧道验证之后，还需将 L2TP 隧道对端设备（L2TP 客户端）的主机名及隧道密码加入到本地用户列表中，以实现隧道验证。注意，如果要求进行隧道验证，那么 L2TP 客户端的主机名及隧道密码必须与本地相关配置匹配。

配置命令如表 3-41 所示。

操作	命令
配置 L2TP 隧道对端设备（L2TP 客户端）的主机名	**new user**/*tunnel-name*
配置 L2TP 隧道对端设备（L2TP 客户端）的隧道密码	**set user**/*tunnel-name* **passwd** *tunnel-passwd*
备注：“ **passwd** ”的缺省值为空。	

表 3-41 配置对端主机名及隧道密码——L2TP 服务器

3.5.2 L2TP 客户端相关配置

HiPER 作为 L2TP 客户端使用时，缺省情况下，是不进行隧道验证的。如果要求进行隧道验证，则必须在相关的 L2TP 客户端连接实例上设置隧道密码，以供隧道验证使用。

本地主机名可通过命令 **set system unitname** *unitname* 设置。也可以不设置主机名，这时，系统将使用设备的 MBID 号码（可通过命令 **revision** 获得）作为隧道验证时的主机名。

配置命令如表 3-42 所示。

操作	命令

配置本地主机名	**set system unitname** *unitname*
配置 L2TP 隧道密码	**set connection/***conn-name* **tunnel secret** *tunnel-passwd*
备注：缺省情况下，“ **system unitname** ”和“ **tunnel secret** ”值都为空。	

表 3-42 配置本地主机名及隧道密码——L2TP 客户端

3.6 L2TP/PPTP 隧道的拨号与挂断

3.6.1 手工连接和挂断 L2TP/PPTP 隧道

在 HiPER 中，作为 L2TP/PPTP 客户端时，无论选择哪一种“ 拨号类型 ”，均可由用户主动拨号或挂断隧道连接，即允许使用手动拨号或挂断隧道连接命令；作为 L2TP/PPTP 服务器时，无法主动拨号，但允许使用手工挂断隧道连接命令。

配置命令如表 3-43 所示。

操作	命令
手工拨号（发起建立 L2TP/PPTP 隧道请求）	**dial connection/***conn-name*
手工挂断 L2TP/PPTP 隧道	**hangup connection/***conn-name*
手工挂断当前所有拨号连接	**hangup**
备注：只允许 L2TP/PPTP 客户端使用手工拨号命令；但是，L2TP/PPTP 客户端和服务器均可使用手工挂断 L2TP/PPTP 隧道连接命令。	

表 3-43 手工连接和挂断 L2TP/PPTP 隧道

3.6.2 小结——L2TP/PPTP 隧道的拨号与挂断机制

在 L2TP/PPTP 隧道建立连接的过程中，只能由“ 拨出 ”方（L2TP/PPTP 客户端）发起建立隧道请求；但是，“ 拨出 ”方（L2TP/PPTP 客户端）和“ 拨入 ”方（L2TP/PPTP 服务器）均可中断隧道连接。

L2TP/PPTP 隧道的拨号方式由 L2TP/PPTP 客户端配置的“ 拨号类型 ”来确定，相关配置参见章节 3.3.13。

1. 如果“ 拨号类型 ”选择为“ 自动拨号 ”（推荐使用），配置完成后 L2TP/PPTP 客户端会自动向 L2TP/PPTP 服务器发起建立隧道请求，直至 L2TP/PPTP 隧道连接成功为止。一旦隧道连接中断，L2TP/PPTP 客户端就会自动拨号，发起建立隧道请求。
2. 如果“ 拨号类型 ”选择为“ 按需拨号 ”，配置完成后，一旦 L2TP/PPTP 客户端监听到有用户数据需要传输时，就拨号，发起建立隧道请求。同样，当隧道连接中断时，只有等到有用户数据需要传输时，L2TP/PPTP 客户端才会拨号。
3. 如果“ 拨号类型 ”选择为“ 手动拨号 ”，配置完成后，必须通过手动建立连接，才能使 L2TP/PPTP 客户端发起建立 L2TP/PPTP 隧道请求。同样，当隧道连接中断时，只有通过手动促使 L2TP/PPTP 客户端拨号。

当 L2TP/PPTP 隧道连接成功后，如果隧道连接中断，正常情况下存在以下几种可能性。

1. L2TP/PPTP 隧道连接成功后，HiPER 会发送 L2TP/PPTP 隧道默认的 HELLO 数据包来探测连接是否正常，如果没有收到隧道对端回应的 HELLO 数据包，HiPER 将会自动挂断隧道连接。
2. 如果启用了 lqm 检测功能，系统将每隔“ lqm 检测间隔 ”发送检测包来判断连接是否正常，如果在“ lqm 生命周期 ”内一直没有收到对方回应的数据包，HiPER 也会自动挂断隧道连接。相关配置参见章节 3.3.16、3.4.11。
3. 当 L2TP/PPTP 隧道连接成功后，如果隧道空闲（没有数据传输）的时间超过了预设的“ 空闲时间 ”，HiPER 关将主动断开连接。相关配置参见章节 3.3.15、3.4.10。
4. 如果配置了“ 会话时间 ”，一旦隧道连接的时间（从拨号成功开始）超出了“ 会话时间 ”，HiPER 安全网关会自动挂断隧道连接。相关配置参见章节 3.3.15、3.4.10。
5. 如果用户主动拆除隧道（手动挂断），L2TP/PPTP 隧道将断开。相关配置参见章节 3.5.1。

提示：

1. 当 HiPER 作为 L2TP/PPTP 客户端使用时，如果设置了“ 拨号时段 ”，那么只有在设置的“ 拨号时段 ”时间范围内才允许 HiPER 拨号，发起建立隧道请求。相关配置参见章节 3.3.14。
2. 当 HiPER 作为 L2TP/PPTP 客户端使用时，如果设置了“ 上线时段 ”，那么在超出这个时间段的时间后 HiPER 会自动挂断隧道连接。相关配置参见章节 3.3.14。

3.7 L2TP/PPTP 的显示和调试

3.7.1 L2TP/PPTP 的显示

3.7.1.1 显示 L2TP/PPTP 隧道连接的历史记录

1. 配置命令

在 HiPER 中，可以查看建立及挂断 L2TP/PPTP 隧道连接时，隧道两端的历史记录。在命令行的系统历史记录中，信息按照从旧到新的顺序从上往下排列，最下端的信息最新。

配置命令如表 3-44 所示。

操作	命令
显示 L2TP/PPTP 历史记录	**show session history**

表 3-44 显示 L2TP/PPTP 隧道连接的历史记录

2. L2TP/PPTP 隧道连接的历史记录涵义

如表 3-45 所示，列出了使用命令 **show session history** 查看时，L2TP/PPTP 隧道连接过程中，隧道两端常见的历史记录及涵义。这里以 L2TP 为例进行说明，PPTP 隧道的历史记录类似。

	历史纪录	记录含义
L2TP 客户端（拨出端）	Outgoing Call @0:1-1 Call Connected, on Line 1, on Channel 0 L2tp Up 200.200.200.173 Session Up [X]	连接开始呼出 物理层/链路层连接完成，但 IP 仍不可用 L2TP 成功和 IP 地址为 200.200.200.173 的设备建立连接 某连接成功建立，[x]为 L2TP 隧道名
	Outgoing Call @0:1-1 Call Connected, on Line 1, on Channel 0 L2tp Up 200.200.200.173 Call Terminated @clearSession:1	连接开始呼出 物理层/链路层连接完成，但 IP 仍不可用 L2TP 成功和 IP 地址为 200.200.200.173 的设备建立连接 呼叫失败（用户名、密码、验证方式等 PPP 层错误）
	Outgoing Call @0:1-1 Call Terminated @clearSession:1	连接开始呼出 呼叫失败（找不到对端或者是对端无响应）
	Session down [x]	某连接挂断，[x]为 L2TP 隧道名
L2TP 服务器（拨入端）	Incoming Call, on Line 1, on Channel 0 Call Connected, on Line 1, on Channel 0 Assigned to port L2tp Up 200.200.200.176 Session Up [X]	有远端呼叫拨入 物理层/链路层连接完成，但 IP 仍不可用 协商成功，为拨入的连接分配虚端口 L2TP 成功和 IP 地址为 200.200.200.176 的设备建立连接 某连接成功建立，[x]为 L2TP 隧道名
	Incoming Call, on Line 1, on Channel 0 Call Connected, on Line 1, on Channel 0 Assigned to port L2tp Up 200.200.200.176 Security error VPN_remote Call Terminated @clearSession:1	有远端呼叫拨入 物理层/链路层连接完成，但 IP 仍不可用 为拨入的连接分配虚端口 L2TP 成功和 IP 地址为 200.200.200.176 的设备建立连接 安全层错误（用户名、密码、验证方式等 PPP 层错误） 呼叫失败
	Session down [x]	某连接挂断，[x]为 L2TP 隧道名
备注：此命令用于查看系统历史记录，L2TP/PPTP 拨号历史记录只是其中的一部分。		

表 3-45 L2TP 隧道连接的历史记录描述

3. 查看实例

1. 如图 3-1 所示实例中，显示了 L2TP 隧道连接成功时，L2TP 客户端的历史记录。PPTP 客户端显示信息类似。

```
hiper% show session history

11:57:50      Outgoing Call @001:163-8341
11:57:50      Call Connected U, on Line  1, on Channel  0
11:57:50      L2tp Up 100.100.100.2
11:57:51      Session Up client
```

图 3-1 显示 L2TP 客户端历史记录——隧道连接成功实例

2. 如图 3-2 所示实例中，显示了 L2TP 隧道连接成功时，L2TP 服务器的历史记录。PPTP 服务器显示信息类似。

```
hiper% show session history

00:43:54      Incoming Call @U:27608-3, on Line  1, on Channel  0
00:43:54      Call Connected U, on Line  1, on Channel  0
00:43:54      Assigned to port U
00:43:54      L2tp Up 100.100.100.1
00:43:55      Session Up xjh
```

图 3-2 显示 L2TP 服务器历史记录——隧道连接成功实例

3.7.1.2 显示 L2TP/PPTP 隧道的拨出/拨入用户信息

1. 配置命令

在 HiPER 中，可以查看 L2TP/PPTP 隧道连接成功时，拨出方（L2TP 客户端）和拨入方（L2TP 服务器）的用户信息。

配置命令如表 3-46 所示。

操作	命令
显示 L2TP/PPTP 隧道的用户信息	**show session userinfo**
备注：此命令用于查看系统的 PPPoE、L2TP、PPTP 拨号用户信息。L2TP、PPTP 用户信息只是其中的一部分。	

表 3-46 显示 L2TP/PPTP 隧道的拨出/拨入用户信息

2. 查看实例

如图 3-3 所示实例中，显示了 L2TP 隧道连接成功时，拨出（L2TP 客户端）的用户信息。PPTP 客户端的用户信息类似。

```
hiper% show session userinfo

dir  prof/user    callid   port   chan   tx   rx    srv     address
0    client/xjh   22       0:-    2:1    n/a  n/a   L2TP    10.10.10.14

Total Active users:   1, high  1
```

图 3-3 显示 L2TP 客户端用户信息——实例

如图 3-4 所示实例中，显示了 L2TP 隧道连接成功时，拨入（L2TP 服务器）的用户信息。PPTP 服务器的用户信息类似。

```
hiper% show session userinfo

dir  prof/user    callid    port  chan   tx    rx    srv     address
I    xjh/xjh      5         0:-   2:1    n/a   n/a   L2TP    10.10.10.14

Total Active users:   1, high  1
```

图 3-4 显示 L2TP 服务器用户信息——实例

3. 部分参数涵义

3. 如图 3-3、3-4 所示，L2TP/PPTP 隧道连接成功时，拨出方（L2TP 客户端）和拨入方（L2TP 服务器）的用户信息中部分参数涵义如下：

- dir：呼叫的方向。其中，O 表示拨出，即 L2TP 客户端；I 表示拨入，即 L2TP 服务器。
- prof/user：prof 为拨号连接名；user 为用户名。
- callid：内部索引号；与 **show session callinfo** 中的 callid 相同。
- srv：使用协议。如果是 L2TP 隧道，显示为 L2TP，表示用户正在使用 L2TP 协议连接；如果是 PPTP 隧道，则显示为 PPTP，表示用户正在使用 PPTP 协议连接。
- address：当 L2TP/PPTP 隧道两端设备连接对方时，会各用一个虚端口连接对方，该地址即为虚端口的路由地址。如果是 L2TP/PPTP 服务器自动分配地址，L2TP/PPTP 客户端中显示的是 L2TP/PPTP 服务器分配的 IP 地址，L2TP/PPTP 服务器中显示的是分配给 L2TP/PPTP 客户端的 IP 地址。
- Total Active users：系统中当前激活的拨号用户（包括 PPPoE 拨号用户、L2TP 拨号用户、PPTP 用户）的个数。
- high：系统中曾经激活的拨号用户（包括 PPPoE 拨号用户、L2TP 拨号用户、PPTP 用户）的最大个数。

3.7.1.3 显示 L2TP/PPTP 隧道的拨出/拨入呼叫信息

1. 配置命令

在 HiPER 中，可以查看 L2TP/PPTP 隧道连接成功时，拨出（L2TP 客户端）呼叫和拨入（L2TP 服务器）呼叫的信息。

配置命令如表 3-47 所示。

操作	命令
显示 PPPoE 拨号呼叫信息	**show session callinfo**

表 3-47 显示 L2TP/PPTP 隧道的拨出/拨入呼叫信息

2. 查看实例

如图 3-5 所示实例中，显示了 L2TP/PPTP 隧道连接成功后，拨出（L2TP 客户端）呼叫或拨入（L2TP 服务器）呼叫的信息。

```
hiper% show session callinfo

callid    dnis        clid        inbytes      outbytes     duration
22        unknown     unknown     213          229          0:01:04:52

Total active calls:   1, high  1
```

图 3-5 显示 L2TP/PPTP 隧道的拨出/拨入呼叫信息——实例

3. 部分参数涵义

如图 3-5 所示，PPPoE 拨号呼叫信息中部分参数涵义如下：

- callid：内部索引号；与 **show session userinfo** 中的 callid 相同。
- inbytes：通过该 L2TP/PPTP 隧道（虚端口）接收的数据包的统计数量。单位：字节。
- outbytes：通过该 L2TP/PPTP 隧道（虚端口）发送的数据包的统计数量。单位：字节。
- duration：该 L2TP/PPTP 隧道连接成功至查看时刻的时间。单位：天:小时:分钟:秒。
- Total Active calls：系统中当前激活的拨号呼叫（包括 PPPoE 呼叫、L2TP 呼叫、PPTP 呼叫）的数量。
- high：系统中曾经激活的拨号呼叫（包括 PPPoE 拨号用户、L2TP 拨号用户、PPTP 用户）的最大数量。

3.7.1.4 查看相关的静态路由

1. 查看 L2TP/PPTP 客户端的相关静态路由

如图 3-6 所示实例中，提供了 L2TP/PPTP 隧道连接成功前后，L2TP/PPTP 客户端的相关静态路由对比。

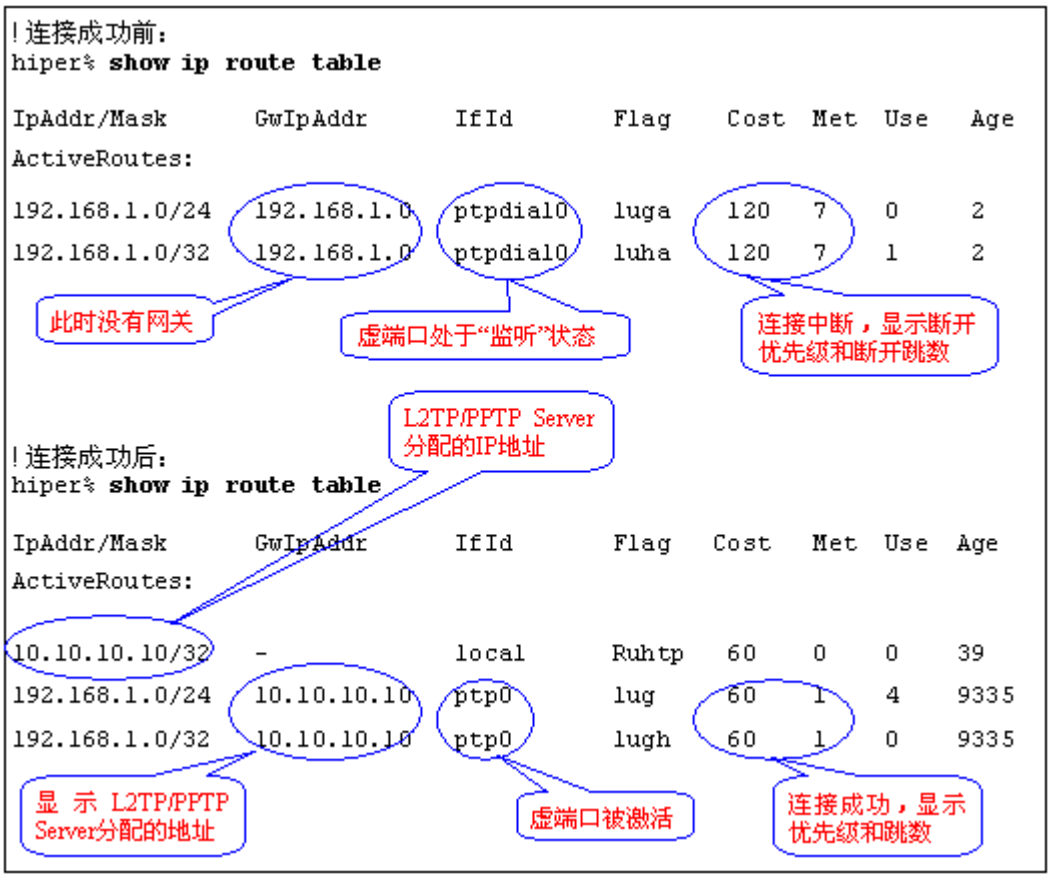

图 3-6 L2TP/PPTP 客户端静态路由对比——实例

2. 查看 L2TP/PPTP 服务器的相关静态路由

如图 3-7 所示实例中，提供了 L2TP/PPTP 隧道连接成功前后，L2TP/PPTP 服务器的相关静态路由对比。

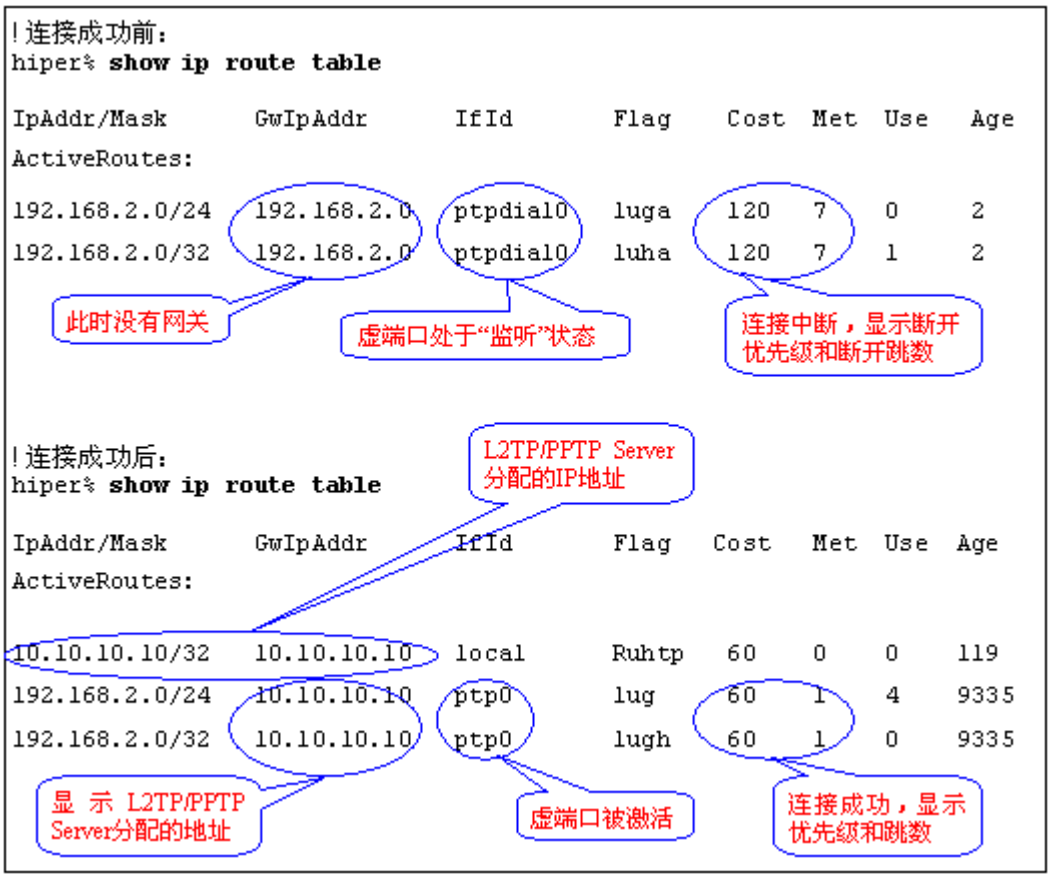

图 3-7 L2TP/PPTP 服务器静态路由对比——实例

3.7.2 L2TP/PPTP 的诊断

3.7.2.1 L2TP/PPTP 客户端诊断

1. L2TP/PPTP 客户端诊断 1

对于 L2TP/PPTP 客户端来说，执行命令 **show session history** 命令后，如果出现如图 3-8 所示信息，则表示 L2TP/PPTP 隧道连接失败。

```
hiper% show session history

00:17:42        Outgoing Call @001:2-2
00:18:08        Call Terminated @clearSession:2
```

图 3-8 L2TP/PPTP 客户端诊断 1

如果出现了如图 3-8 所示的现象，请按下面列出的原因依次检查相关配置。

1) 本地 L2TP/PPTP 数据包不可到达 L2TP/PPTP 服务器：
   - 本地 L2TP/PPTP/PPTPGRE 静态映射没有作或者不生效；
   - 本地线路不支持 L2TP/PPTP 的通过（NAT 接入环境发生可能性比较大）；
   - 如果 L2TP/PPTP 服务器使用域名，本地没有配置 DNS 或者配置的 DNS 不能解析正确的地址；

- 如果 L2TP/PPTP 服务器使用域名，配置的动态域名没有生效；
- L2TP 和对方隧道验证不匹配。

2) L2TP/PPTP 服务器不响应（此时 L2TP/PPTP 服务器的 **show session history** 无任何输出）：
   - 本地 L2TP/PPTP/PPTPGRE 静态映射没有作或者不生效；
   - L2TP/PPTP 两端的隧道协议不匹配；
   - L2TP 和对方隧道验证不匹配。

2. L2TP/PPTP 客户端诊断 2

对于 L2TP/PPTP 客户端来说，执行命令 **show session history** 命令后，如果出现如图 3-9 所示信息，则表示 L2TP/PPTP 隧道连接失败。

```
hiper% show session history

00:08:33        Outgoing Call @001:11-11
00:08:33        Call Connected U, on Line  1, on Channel  0
00:08:33        {L2tp|PPTP} Up 100.100.100.1
00:08:38        Call Disconnected @networkStateChan+, on Line  1
00:08:38        Call Terminated @clearSession:11
```

图 3-9 L2TP/PPTP 客户端诊断 2

如果出现了如图 3-9 所示的现象，请按下面列出的原因依次检查相关配置。

1) 本地用户名/密码被对方验证失败；
2) 本地验证方式和对方不匹配；
3) L2TP/PPTP 和对方加密协商不匹配。

3.7.2.2 L2TP/PPTP 服务器诊断

对于 L2TP/PPTP 服务器来说，执行命令 **show session history** 命令后，如果出现如图 3-10 所示信息，则表示 L2TP/PPTP 隧道连接失败。

```
hiper% show session history

00:00:09        Incoming Call , on Line  1, on Channel  0
00:00:09        Call Connected , on Line  1, on Channel  0
00:00:09        Assigned to port
00:00:09        {L2tp|PPTP} Up 100.100.100.2
01:54:14        Security error vpn_lan
01:54:18        Call Terminated @clearSession:5
```

图 3-10 L2TP/PPTP 服务器诊断

如果出现了如图 3-10 所示的现象，请按下面列出的原因依次检查相关配置。

1) 验证对方用户名/密码失败；
2) 对方验证方式和本地不匹配；
3) L2TP/PPTP 和对方加密协商不匹配。

3.8 L2TP/PPTP 典型配置实例

本节仅提供 HiPER 之间、HiPER 与 windows 2000/XP 之间建立 L2TP 隧道和 PPTP 隧道的配置实例，更多的 L2TP 配置实例、PPTP 配置实例以及综合应用实例，请参考《HiPER ReoS 5.0 VPN 配置手册》。

3.8.1 L2TP 配置实例

一. 需求

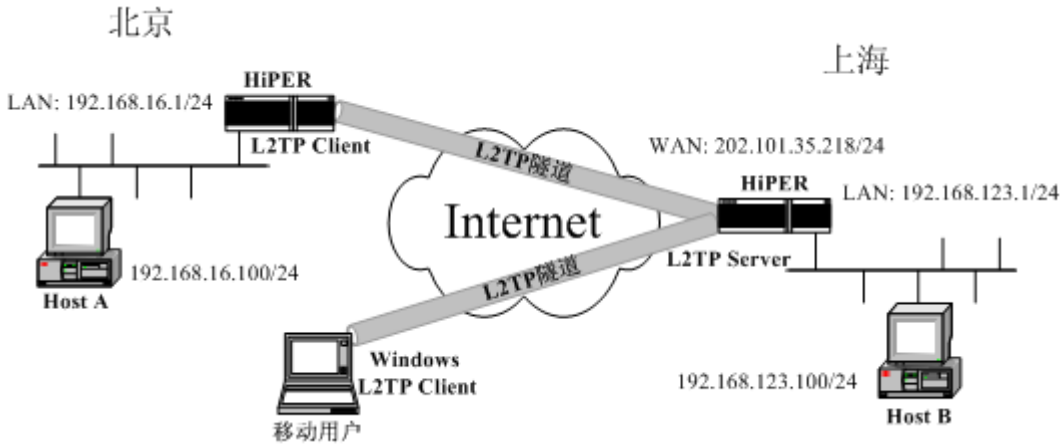

图 3-11 L2TP 配置实例

在本方案中，某公司总部在上海。在北京有一个分公司希望可以实现两地局域网内部资源的相互访问。该公司还有一些出差和远程办公的移动用户希望在远程访问总公司局域网内部资源。

本方案使用 L2TP 协议建立 VPN 隧道，如图 3-11 所示，在上海公司总部使用 HiPER VPN 安全网关作为 L2TP 服务器；在北京使用 HiPER VPN 安全网关作为 L2TP 客户端，拨号类型为按需拨号，空闲时间为 3600 秒；移动用户使用 Windows 2000 内置的 L2TP 客户端软件。地址如下：

上海的 HiPER：

局域网 IP 地址：192.168.123.0/255.255.255.0

HiPER 的 LAN 口 IP 地址：192.168.123.1/255.255.255.0

HiPER 的 WAN 口 IP 地址：202.101.35.218/255.255.255.0

北京的 HiPER

局域网 IP 地址：192.168.16.0/255.255.255.0

HiPER 的 LAN 口 IP 地址：192.168.16.1/255.255.255.0

移动用户：

使用 Windows 2000 通过 L2TP 拨号完成隧道连接。

二. 分析

上海和北京的 HiPER，都需要进行相关的全局配置：配置系统启用 L2TP 协议，配置工作模式分别为 LNS 和 LAC，配置相关的 NAT 静态映射。此外，对于上海的 HiPER 来说，还需配置 L2TP VPN 地址池。

三. 配置步骤

1. 配置上海的 HiPER 作为 L2TP 服务器

a. 全局配置

！配置系统启用 L2TP 协议
```
set ip vpn tunnelmode l2tp
```

！配置系统工作在 LNS 模式下
```
set ip vpn l2tpmode LNS
```

！配置 L2TP VPN 地址池，起始 IP 地址为 10.10.10.10，数目为 50
```
set ip pool pooL1start 10.10.10.10
set ip pool pooL1count 50
```

！保存配置
```
write
```

b. 配置 UDP 1701 端口的 NAT 静态映射

！新建一条 NAT 映射，名字为 l2tp-map
```
new ip nat static/l2tp-map
```

！ 协议为 UDP
```
set ip nat static/l2tp-map protocol udp
```

！ 内部端口和外部端口均为 1701
```
set ip nat static/l2tp-map dstport 1701
set ip nat static/l2tp-map localport 1701
```

！内部地址为 HiPER 的 LAN 口地址
```
set ip nat static/l2tp-map localaddress 192.168.123.1
```

！ 绑定到主线路上，本例中主线路 NAT 规则名为 ETHbind
```
set ip nat static/l2tp-map binding ETHbind
```

！ 设置端口 1701 在 NAT 前后保持不变
```
set ip nat static/l2tp-map autolocalIP yes
```

！保存配置
```
write
```

c. 为北京的 HiPER 创建 L2TP 拨入帐号

！新建一个 L2TP 服务器连接实例，实例名为 vpn_bj，此名称同时也将作为北京的 HiPER 的 PPP 验证用户名使用
```
new connection/vpn_bj
```

！ 配置 PPP 验证方式为 PAP
```
set connection/vpn_bj encaps send authtype PAP
```

！配置 PPP 验证密码为 vpntest
```
set connection/vpn_bj encaps recv pw vpntest
```

！配置远端内网 IP 地址和子网掩码
```
set connection/vpn_bj ip address remoteip 192.168.16.1
set connection/vpn_bj ip address remotemask 255.255.255.0
```

！保存配置
write

d. 为移动用户创建 L2TP 拨入帐号

！新建一个 L2TP 服务器连接实例，实例名为 vpn_mobile，此名称同时也将作为移动用户的 PPP 验证用户名使用
new connection/vpn_mobile

！配置 PPP 验证方式为 PAP、密码为 vpntest
set connection/vpn_mobile encaps send authtype PAP
set connection/vpn_mobile encaps recv pw vpntest

！配置远端内网 IP 地址和子网掩码
set connection/vpn_mobile ip address remoteip 192.168.210.1
set connection/vpn_mobile ip address remotemask 255.255.255.255

！保存配置
write

2. 配置北京的 HiPER 作为 L2TP 客户端

a. 全局配置

！配置系统启用 L2TP 协议
set ip vpn tunnelmode l2tp

！配置系统工作在 LAC 模式下
set ip vpn l2tpmode LAC

！保存配置
write

b. 配置 UDP 1701 端口的 NAT 静态映射

！新建一条 NAT 映射，名字为 l2tp-map
new ip nat static/l2tp-map

！协议为 UDP
set ip nat static/l2tp-map protocol udp

！内部端口和外部端口均为 1701
set ip nat static/l2tp-map dstport 1701
set ip nat static/l2tp-map localport 1701

！内部地址为 HiPER 的 LAN 口地址
set ip nat static/l2tp-map localaddress 192.168.16.1

！绑定到主线路上，本例中主线路 NAT 规则名为 ETHbind
set ip nat static/l2tp-map binding ETHbind

！设置端口 1701 在 NAT 前后保持不变
set ip nat static/l2tp-map autolocalIP yes

！保存配置
write

c. 配置 L2TP 客户端连接实例

！新建一个 L2TP 客户端连接，实例名为 vpn_sh
```
new connection/vpn_sh
```
！配置首拨号码（为任意值）
```
set connection/vpn_sh dial first 001
```
！配置 PPP 验证方式为 PAP、用户名为 vpn_bj、密码为 vpntest
```
set connection/vpn_sh encaps send authtype PAP
set connection/vpn_sh encaps send name vpn_bj
set connection/vpn_sh encaps send pw vpntest
```
！启用 L2TP 客户端功能
```
set connection/vpn_sh tunnel type client
```
！配置第二层隧道协商的协议类型为 L2TP
```
set connection/vpn_sh tunnel protocol l2tp
```
！配置隧道服务器地址为 202.101.35.218
```
set connection/vpn_sh tunnel serveraddress 202.101.35.218
```
！配置远端内网 IP 地址和子网掩码
```
set connection/vpn_bj ip address remoteip 192.168.123.1
set connection/vpn_bj ip address remotemask 255.255.255.0
```
！设置拨号类型为按需拨号
```
set connection/vpn_bj line calltype Switched
set connection/vpn_bj line dialoutspoof yes
```
！设置空闲时间为 3600 秒
```
set connection/vpn_bj dial idletimeout 3600
```
！保存配置
```
write
```

3. 配置 Windows 2000 作为 L2TP 客户端

按照以下步骤配置 Windows 2000 计算机，使其成为 L2TP 客户端。

a. 配置 L2TP 拨号连接

1） 进入 Windows 2000 的“ 开始 ”→“ 设置 ”→“ 网络与拨号连接 ”→“ 新建连接 ”。
2） 启动“ 网络连接向导 ”，单击“ 下一步 ”。
3） 在“ 网络连接类型 ”中，选择“ 通过 Internet 连接到专用网络 ”，单击“ 下一步 ”。
4） 选择“ 不拨初始连接 ”，单击“ 下一步 ”。
5） 在“ 目的地址 ”一栏，输入准备连接的 L2TP 服务器的 IP 地址“ 202.101.35.218 ”，单击“ 下一步 ”。
6） 选择“ 只有我自己可以使用此连接 ”，单击“ 下一步 ”。
7） 输入“ 您为这个连接使用的名称 ”为“ l2tp ”。
8） 单击“ 完成 ”。
9） 双击“ l2tp ”连接，在 l2tp 连接窗口，单击“ 属性 ”。
10） 进入“ 安全措施 ”属性页面，选择“ 高级（自定义设置）”，单击“ 设置 ”。

11） 在“数据加密”中选择“可选加密（没有加密也可以连接）”。
12） 在“允许这些协议”选中“不加密的密码（PAP）”、“质询握手身份验证协议（CHAP）”、“Microsoft CHAP（MS-CHAP）”，单击“确定”。
13） 进入“网络”属性页面，在“我正在呼叫的 VPN 服务器的类型”选择“第 2 层隧道协议（L2TP）”。
14） 单击“确定”，保存所做的修改。

b. 禁用 IPSec

1） 双击“l2tp”连接，在 l2tp 连接窗口，单击“属性”。
2） 选择“网络”属性页面。
3） 确认“NWLink IPX/SPX/NetBIOS Compatible Transport Prococol”协议没有被选中。
4） 选择“Internet 协议（TCP/IP）”，单击“属性”。
5） 单击“高级属性”属性页面。
6） 进入“选项”属性页面，选择“IP 安全机制”，单击“属性”。
7） 确认“不使用 IPSec”被选中。
8） 单击“确定”，关闭连接属性窗口。

c. 修改注册表

缺省的 Windows 2000 L2TP 传输策略不允许 L2TP 传输不使用 IPSec 加密，可以通过修改 Windows 2000 注册表来禁用缺省的行为。

方法一：运行光盘\registry\目录下的 l2tp.reg 文件。

方法二：手工修改：

1） 进入 Windows 2000 的“开始”→“运行”里面输入“Regedt32”，打开“注册表编辑器”，定位“HKEY_Local_Machine \ System \ CurrentControl Set \ Services \ RasMan \ Parameters ”主键。
2） 选择“编辑”→“添加数值”，为该主键添加以下键值：
数值名称：ProhibitIpSec
数据类型：reg_dword
值：1
3） 保存所做的修改，重新启动电脑以使改动生效。

提示：必须添加“ProhibitIpSec”注册表键值到每个要使用 L2TP 的运行 Windows 2000 操作系统的电脑。

d. 使用 L2TP 隧道连接到 HiPER L2TP 服务器

1） 确认计算机已经连接到 Internet（可能是拨号连接或者是固定 IP 接入）。
2） 启动前面步骤中创建的“l2tp”拨号连接。
3） 输入的 l2tp 连接的用户名：vpn_mobile 和密码：vpntest。
4） 单击“连接”。
5） 连接成功后，在 MS-DOS 方式下输入“ipconfig”，可以看到一个在 L2TP 服务器地址池中的地址，就是 L2TP 服务器分配给本机的 IP 地址。

3.8.2 PPTP 配置实例

一.需求

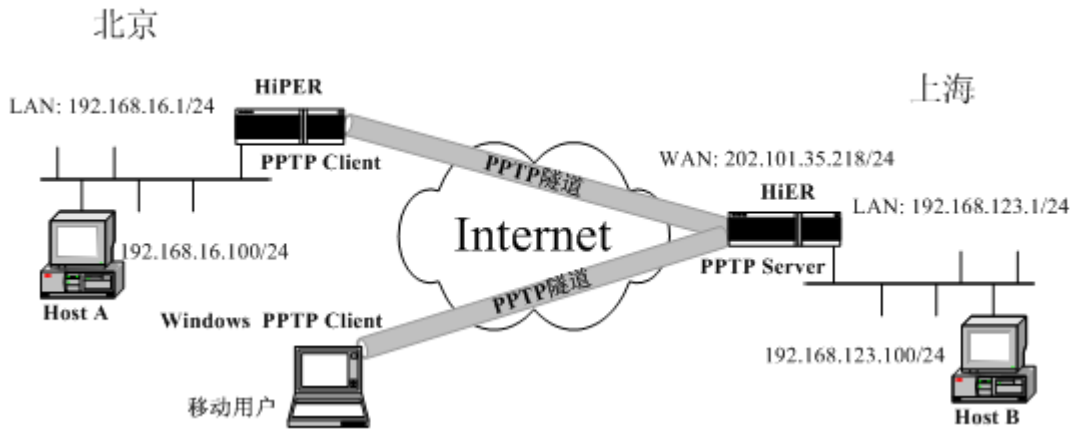

图 3-12 PPTP 配置实例

在本方案中，某公司总部在上海。在北京有一个分公司希望可以实现两地局域网内部资源的相互访问。该公司还有一些出差和远程办公的移动用户希望在远程访问总公司局域网内部资源。

本方案使用 PPTP 协议建立 VPN 隧道，如图 3-11 所示，在上海公司总部使用 HiPER VPN 安全网关作为 PPTP 服务器；在北京使用 HiPER VPN 安全网关作为 PPTP 客户端，拨号类型为按需拨号，空闲时间为 3600 秒；移动用户使用 Windows 2000 内置的 PPTP 客户端软件。地址如下：

上海的 HiPER：

局域网 IP 地址：192.168.123.0/255.255.255.0

HiPER 的 LAN 口 IP 地址：192.168.123.1/255.255.255.0

HiPER 的 WAN 口 IP 地址：202.101.35.218/255.255.255.0

北京的 HiPER

局域网 IP 地址：192.168.16.0/255.255.255.0

HiPER 的 LAN 口 IP 地址：192.168.16.1/255.255.255.0

移动用户：

使用 Windows 2000 通过 PPTP 拨号完成隧道连接。

二.分析

上海和北京的 HiPER，都需要进行相关的全局配置：配置系统启用 PPTP 协议，配置工作模式分别为 PAC 和 PNS，配置相关的 NAT 静态映射。此外，对于上海的 HiPER 来说，还需配置 PPTP VPN 地址池。

三.配置步骤

1. 配置上海的 HiPER 作为 PPTP 服务器

a. 全局配置

！配置系统启用 PPTP 协议

```
set ip vpn tunnelmode pptp
```

！配置系统工作在 PAC 模式下

```
set ip vpn pptpmode PAC
```

！配置 PPTP VPN 地址池，起始 IP 地址为 10.10.10.10，数目为 50
```
set ip pool pooL1start 10.10.10.10
set ip pool pooL1count 50
```
！保存配置
```
write
```

b. 配置 TCP 1723 端口的 NAT 静态映射

！新建一条 NAT 映射，名字为 pptp-map
```
new ip nat static/pptp-map
```
！ 协议为 TCP
```
set ip nat static/pptp-map protocol tcp
```
！ 内部端口和外部端口均为 1723
```
set ip nat static/pptp-map dstport 1723
set ip nat static/pptp-map localport 1723
```
！内部地址为 HiPER 的 LAN 口地址
```
set ip nat static/pptp-map localaddress 192.168.123.1
```
！ 绑定到主线路上，本例中主线路 NAT 规则名为 ETHbind
```
set ip nat static/pptp-map binding ETHbind
```
！ 设置端口 1723 在 NAT 前后保持不变
```
set ip nat static/pptp-map autolocalIP yes
```

c. 配置 GRE 协议的 NAT 静态映射

！新建一条 NAT 映射，名字为 gre-map
```
new ip nat static/gre-map
```
！ 协议为 GRE
```
set ip nat static/gre-map protocol gre
```
！内部地址为 HiPER 的 LAN 口地址
```
set ip nat static/gre-map localaddress 192.168.123.1
```
！ 绑定到主线路上，本例中主线路 NAT 规则名为 ETHbind
```
set ip nat static/gre-map binding ETHbind
```

d. 为北京的 HiPER 创建 PPTP 拨入帐号

！新建一个 PPTP 服务器连接实例，实例名为 vpn_bj，此名称同时也将作为北京的 HiPER 的 PPP 验证用户名使用
```
new connection/vpn_bj
```
！ 配置 PPP 验证方式为 PAP
```
set connection/vpn_bj encaps send authtype PAP
```
！配置 PPP 验证密码为 vpntest
```
set connection/vpn_bj encaps recv pw vpntest
```
！配置远端内网 IP 地址和子网掩码
```
set connection/vpn_bj ip address remoteip 192.168.16.1
```

```
set connection/vpn_bj ip address remotemask 255.255.255.0
```

！保存配置

```
write
```

e. 为移动用户创建 PPTP 拨入帐号

！新建一个 PPTP 服务器连接实例，实例名为 vpn_mobile，此名称同时也将作为移动用户的 PPP 验证用户名使用

```
new connection/vpn_mobile
```

！ 配置 PPP 验证方式为 PAP、密码为 vpntest

```
set connection/vpn_mobile encaps send authtype PAP
set connection/vpn_mobile encaps recv pw vpntest
```

！配置远端内网 IP 地址和子网掩码

```
set connection/vpn_mobile ip address remoteip 192.168.210.1
set connection/vpn_mobile ip address remotemask 255.255.255.255
```

！保存配置

```
write
```

2. 配置北京的 HiPER 作为 PPTP 客户端

a. 全局配置

！配置系统启用 PPTP 协议

```
set ip vpn tunnelmode pptp
```

！配置系统工作在 PNS 模式下

```
set ip vpn pptpmode pns
```

！保存配置

```
write
```

b. 配置 TCP 1723 端口的 NAT 静态映射

！新建一条 NAT 映射，名字为 pptp-map

```
new ip nat static/pptp-map
```

！ 协议为 TCP

```
set ip nat static/pptp-map protocol tcp
```

！ 内部端口和外部端口均为 1723

```
set ip nat static/pptp-map dstport 1723
set ip nat static/pptp-map localport 1723
```

！内部地址为 HiPER 的 LAN 口地址

```
set ip nat static/pptp-map localaddress 192.168.16.1
```

！ 绑定到主线路上，本例中主线路 NAT 规则名为 ETHbind

```
set ip nat static/pptp-map binding ETHbind
```

！ 设置端口 1723 在 NAT 前后保持不变

```
set ip nat static/pptp-map autolocalIP yes
```

！保存配置
write

c. 配置 GRE 协议的 NAT 静态映射

！新建一条 NAT 映射，名字为 gre-map
new ip nat static/gre-map

！ 协议为 GRE
set ip nat static/gre-map protocol gre

！内部地址为 HiPER 的 LAN 口地址
set ip nat static/gre-map localaddress 192.168.16.1

！ 绑定到主线路上，本例中假设主线路 NAT 规则名为 ETHbind
set ip nat static/gre-map binding ETHbind

d. 配置 PPTP 客户端连接实例

！新建一个 PPTP 客户端连接，实例名为 vpn_sh
new connection/vpn_sh

！配置首拨号码（为任意值）
set connection/vpn_sh dial first 002

！ 配置 PPP 验证方式为 PAP、用户名为 vpn_bj、密码为 vpntest
set connection/vpn_sh encaps send authtype PAP
set connection/vpn_sh encaps send name vpn_bj
set connection/vpn_sh encaps send pw vpntest

！ 启用 PPTP 客户端功能
set connection/vpn_sh tunnel type client

！ 配置第二层隧道协商的协议类型为 PPTP
set connection/vpn_sh tunnel protocol pptp

！配置隧道服务器地址为 202.101.35.218
set connection/vpn_sh tunnel serveraddress 202.101.35.218

！配置远端内网 IP 地址和子网掩码
set connection/vpn_sh ip address remoteip 192.168.123.1
set connection/vpn_sh ip address remotemask 255.255.255.0

！设置拨号类型为按需拨号
set connection/vpn_sh line calltype Switched
set connection/vpn_sh line dialoutspoof yes

！设置空闲时间为 3600 秒
set connection/vpn_sh dial idletimeout 3600

！保存配置
write

3. 配置 Windows XP 作为 PPTP 客户端

按照以下步骤配置 Windows XP 计算机，使得它能够连接到 HiPER PPTP 服务器。

a. 配置 PPTP 拨号连接：

1） 进入 Windows XP 的“ 开始 ”→“ 设置 ”→“ 控制面板 ”，选择“ 切换到分类视图 ”。
2） 选择“ 网络和 Internet 连接 ”。
3） 选择“ 建立一个您的工作位置的网络连接 ”。
4） 选择“ 虚拟专用网络连接 ”，单击“ 下一步 ”。
5） 为连接输入一个名字为“ pptp ”，单击“ 下一步 ”。
6） 选择“ 不拨此初始连接 ”，单击“ 下一步 ”。
7） 输入准备连接的 PPTP 服务器的 IP 地址“ 202.101.35.218 ”，单击“ 下一步 ”。
8） 单击“ 完成 ”。
9） 双击“ pptp ”连接，在 pptp 连接窗口，单击“ 属性 ”。
10） 选择“ 安全 ”属性页面，选择“ 高级（自定义设置）”，单击“ 设置 ”。
11） 在“ 数据加密 ”中选择“ 可选加密（没有加密也可以连接）”。
12） 在“ 允许这些协议 ”选中“ 不加密的密码（PAP）”、“ 质询握手身份验证协议（CHAP）”、“ Microsoft CHAP（MS-CHAP）”，单击“ 确定 ”。
13） 选择“ 网络 ”属性页面，在“ VPN 类型 ”选择“ PPTP VPN ”。
14） 确认“ Internet 协议（TCP/IP）”被选中。
15） 确认“ NWLink IPX/SPX/NetBIOS Compatible Transport Prococol ”、“ 微软网络文件和打印共享 ”、“ 微软网络客户 ”协议没有被选中。
16） 单击“ 确定 ”，保存所做的修改。

b. 使用 PPTP 隧道连接到 HiPER PPTP 服务器：

1） 确认计算机已经连接到 Internet（可能是拨号连接或者是固定 IP 接入）。
2） 启动前面步骤中创建的“ pptp ”拨号连接。
3） 输入的 pptp 用户名“ vpn_mobile ”和密码“ vpntest ”。
4） 单击“ 连接 ”。
5） 连接成功后，在 MS-DOS 方式下输入“ ipconfig ”，可以看到一个在 PPTP 服务器地址池中的地址，就是 PPTP 服务器分配给本机的 IP 地址。

附录一 图目录

附录二 表目录