目 录

第1章 VPN 概述

1.1 VPN 简介

虚拟私有网（Virtual Private Network）简称 VPN，是近年来随着 Internet 的广泛应用而迅速发展起来的一种新技术，用以实现在公用网络上构建私人专用网络。“ 虚拟 ”主要指这种网络是一种逻辑上的网络。

伴随企业和公司的不断扩张，员工出差日趋频繁，驻外机构及客户群分布日益分散，合作伙伴日益增多，越来越多的现代企业迫切需要利用公共 Internet 资源来进行促销、销售、售后服务、培训、合作及其它咨询活动，这为 VPN 的应用奠定了广阔市场。

1.1.1 VPN 的特点

- VPN 有别于传统网络，它并不实际存在，而是利用现有公共网络，通过资源配置而成的虚拟网络，是一种逻辑上的网络。
- VPN 只为特定的企业或用户群体所专用。从 VPN 用户角度看来，使用 VPN 与传统专网没有区别。VPN 作为私有专网，一方面与底层承载网络之间保持资源独立性，即在一般情况下，VPN 资源不会被承载网络中的其它 VPN 或非该 VPN 用户的网络成员所使用；另一方面，VPN 提供足够安全性，确保 VPN 内部信息不受外部的侵扰。
- VPN 不是一种简单的高层业务。该业务建立专网用户之间的网络互联，包括建立 VPN 内部的网络拓扑、路由计算、成员的加入与退出等，因此 VPN 技术就比各种普通的点对点的应用机制要复杂得多。

1.1.2 VPN 的优势

- 在远端用户、驻外机构、合作伙伴、供应商与公司总部之间建立可靠的安全连接，保证数据传输的安全性。这一优势对于实现电子商务或金融网络与通讯网络的融合将有特别重要的意义。
- 利用公共网络进行信息通讯，一方面使企业以明显更低的成本连接远地办事机构、出差人员和业务伙伴，另一方面极大的提高了网络的资源利用率，有助于增加 ISP（Internet Service Provider，Internet 服务提供商）的收益。
- 只需要通过软件配置就可以增加、删除 VPN 用户，无需改动硬件设施。这使得 VPN 的应用具有很大灵活性。

- 支持驻外 VPN 用户在任何时间、任何地点的移动接入，这将满足不断增长的移动业务需求。
- 构建具有服务质量保证的 VPN（如 MPLS VPN），可为 VPN 用户提供不同等级的服务质量保证，通过收取不同的业务使用费用可获得更多的利润。有关 MPLS VPN 的原理及相关介绍请参见 MPLS 配置章节。

1.1.3 VPN 网络结构

VPN 是由若干 Site 组成的集合。Site 可以同时属于不同的 VPN，但是必须遵循如下规则：两个 Site 只有同时属于一个 VPN 定义的 Site 集合，才具有 IP 连通性。按照 VPN 的定义，一个 VPN 中的所有 Site 都属于一个企业，称为 Intranet ;如果 VPN 中的 Site 分属不同的企业，则称为 Extranet。

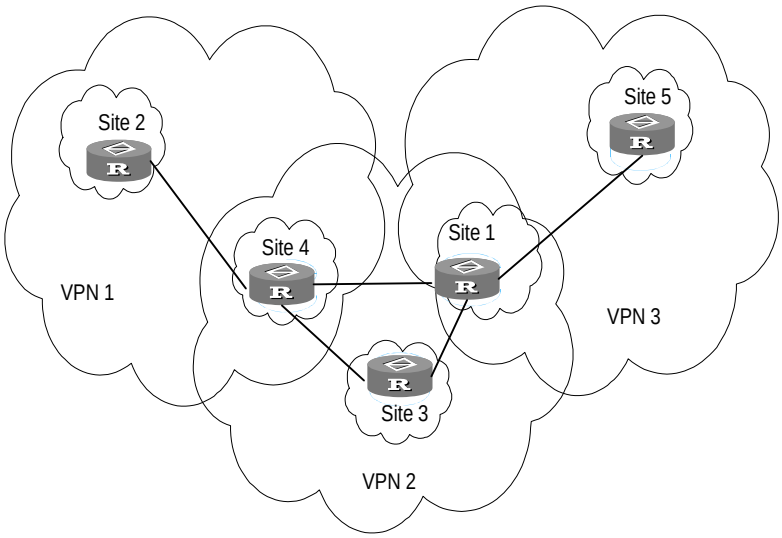

图1-1 VPN 组成示意图

上图显示了有 5 个 Site 分别构成了 3 个 VPN：

- VPN1---Site2、Site4
- VPN2---Site1、Site3、Site4
- VPN3---Site1、Site5

1.2 VPN 的基本技术

1.2.1 VPN 基本组网应用

以某企业为例，通过 VPN 建立的企业内部网如图 1-2所示：

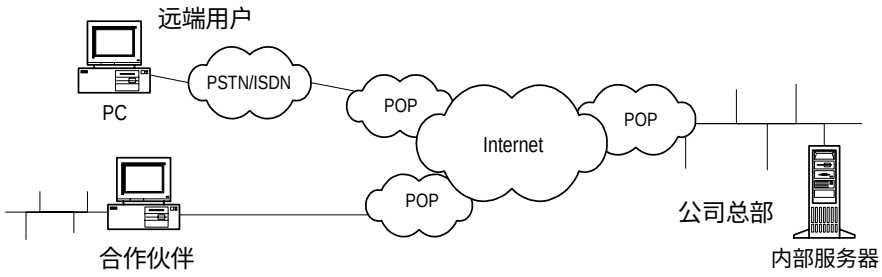

图1-2 VPN 组网示意图

从上图可以看出，企业内部资源享用者通过 PSTN/ISDN 网或局域网就可以连入本地 ISP 的 POP（Point of Presence）服务器，从而访问公司内部资源。而利用传统的 WAN 组建技术，相互之间要有专线相连才可以达到同样的目的。虚拟网组成后，远端用户和外地客户甚至不必拥有本地 ISP 的上网权限就可以访问企业内部资源，这对于流动性很大的出差员工和分布广泛的客户来说是很有意义的。

企业开设 VPN 业务所需的设备很少，只需在资源共享处放置一台支持 VPN 的服务器（如一台 Windows NT 服务器或支持 VPN 的路由器）就可以了。资源享用者通过 PSTN/ISDN 网或局域网连入本地 POP 服务器后，直接呼叫企业的远程服务器（VPN 服务器），呼叫接续过程由 ISP 的接入服务器（Access Server）与 VPN 服务器共同完成。

1.2.2 VPN 的原理

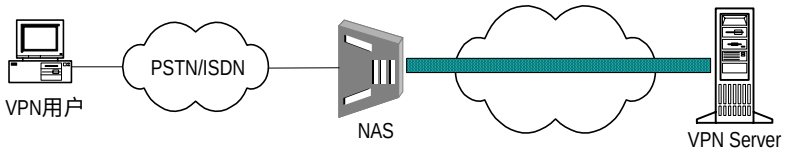

图1-3 VPN 接入示意图

如上图所示，VPN 用户通过 PSTN/ISDN 网拨入 ISP 的 NAS（Network Access Server）服务器，NAS 服务器通过用户名或接入号码识别出该用户为 VPN 用户后，就和用户的目的 VPN 服务器建立一条连接，称为隧道（Tunnel），然后将用户数据包封装成 IP 报文后通过该隧道传送给 VPN 服务器，VPN 服务器收到数据包并拆封后就可以读到真正有意义的报文了。反向的处理也一样。隧道两侧可以对报文进行加密处理，使 Internet 上的其它用户无法读取，因而是安全可靠的。对用户来说，隧道是其 PSTN/ISDN 链路的逻辑延伸，操作起来和实际物理链路相同。

隧道可以通过隧道协议来实现。根据是在 OSI 模型的第二层还是第三层实现隧道，隧道协议分为第二层隧道协议和第三层隧道协议。

1. 第二层隧道协议

第二层隧道协议是将整个 PPP 帧封装在内部隧道中。现有的第二层隧道协议有：

- PPTP（Point-to-Point Tunneling Protocol）：点到点隧道协议，由微软、Ascend 和 3COM 等公司支持，在 Windows NT 4.0 以上版本中支持。该协议支持点到点 PPP 协议在 IP 网络上的隧道封装，PPTP 作为一个呼叫控制和管理协议，使用一种增强的 GRE（Generic Routing Encapsulation，通用路由封装）技术为传输的 PPP 报文提供流控和拥塞控制的封装服务。
- L2F（Layer 2 Forwarding）协议：二层转发协议，由北方电信等公司支持。L2F 协议支持对更高级协议链路层的隧道封装，实现了拨号服务器和拨号协议连接在物理位置上的分离。
- L2TP（Layer 2 Tunneling Protocol）：二层隧道协议，由 IETF 起草，微软等公司参与，结合了上述两个协议的优点，为众多公司所接受，并且已经成为标准 RFC。L2TP 既可用于实现拨号 VPN 业务，也可用于实现专线 VPN 业务。

2. 第三层隧道协议

第三层隧道协议的起点与终点均在 ISP 内，PPP 会话终止在 NAS 处，隧道内只携带第三层报文。现有的第三层隧道协议主要有：

- GRE（Generic Routing Encapsulation）协议：这是通用路由封装协议，用于实现任意一种网络层协议在另一种网络层协议上的封装。
- IPSec（IP Security）协议：IPSec 协议不是一个单独的协议，它给出了 IP 网络上数据安全的一整套体系结构，包括 AH（Authentication Header）、ESP（Encapsulating Security Payload）、IKE（Internet Key Exchange）等协议。

GRE 和 IPSec 主要用于实现专线 VPN 业务。

3. 第二、三层隧道协议之间的异同

第三层隧道与第二层隧道相比，优势在于它的安全性、可扩展性与可靠性。从安全性的角度看，由于第二层隧道一般终止在用户侧设备上，对用户网的安全及防火墙技术提出十分严峻的挑战；而第三层隧道一般终止在 ISP 网关上，因此一般情况下不会对用户网的安全技术提出较高要求。

从扩展性的角度看，第二层隧道内封装了整个 PPP 帧，这可能产生传输效率问题。其次，PPP 会话贯穿整个隧道并终止在用户侧设备上，导致用户侧网关必须要保存大量 PPP 会话状态与信息，这将对系统负荷产生较大的影响，也会影响到系统的扩展性。此外，由于 PPP 的 LCP 及 NCP 协商都对时间非常敏感，这样隧道的效率降低会造成 PPP 对话超时等等一系列问题。相反，第三层隧道终止在 ISP 的网关内，PPP 会话终止在 NAS 处，用户侧网关无需管理和维护每个 PPP 对话的状态，从而减轻了系统负荷。

一般地，第二层隧道协议和第三层隧道协议都是独立使用的，如果合理地将这两层协议结合起来使用，将可能为用户提供更好的安全性（如将 L2TP 和 IPSec 协议配合使用）和更佳的性能。

1.3 VPN 的分类

IP VPN 是指利用 IP 设施（包括公用的 Internet 或专用的 IP 骨干网）实现 WAN 设备专线业务（如远程拨号、DDN 等）的仿真。IP VPN 可有以下几种分类方法：

1. 按运营模式划分

(1) CPE-based VPN（Customer Premises Equipment based VPN）

用户不但要安装价格昂贵的设备及专门认证工具，还要负责繁杂的 VPN 维护（如通道维护、带宽管理等）。这种方式组网复杂度高、业务扩展能力弱。

(2) Network-based VPN（NBIP-VPN）

将 VPN 的维护等外包给 ISP 实施（也允许用户在一定程度上进行业务管理和控制），并且将其功能特性集中在网络侧设备处实现，这样可以降低用户投资、增加业务灵活性和扩展性，同时也可为运营商带来新的收入。

2. 按业务用途划分

(1) Intranet VPN（企业内部虚拟专网）

Intranet VPN 通过公用网络进行企业内部各个分布点互联，是传统的专线网或其它企业网的扩展或替代形式。

(2) Access VPN（远程访问虚拟专网）

Access VPN 向出差流动员工、远程办公人员和远程小办公室提供了通过公用网络与企业的 Intranet 和 Extranet 建立私有的网络连接。Access VPN 的结构有两种类型，一种是用户发起（Client-initiated）的 VPN 连接，另一种是接入服务器发起（NAS-initiated）的 VPN 连接。

(3) Extranet VPN（扩展的企业内部虚拟专网）

Extranet VPN 是指利用 VPN 将企业网延伸至供应商、合作伙伴与客户处，使不同企业间通过公网来构筑 VPN。

3. 按组网模型划分

(1) 虚拟租用线（VLL）

VLL（Virtual Leased Line）是对传统租用线业务的仿真，通过使用 IP 网络对租用线进行模拟，提供非对称、低成本的“ DDN ”业务。从虚拟租用线两端的用户来看，该虚拟租用线近似于过去的租用线。

(2) 虚拟专用拨号网络（VPDN）

VPDN（Virtual Private Dial Network）是指利用公共网络（如 ISDN 和 PSTN）的拨号功能及接入网来实现虚拟专用网，从而为企业、小型 ISP、移动办公人员提供接入服务。

(3) 虚拟专用 LAN 网段（VPLS）业务

VPLS（Virtual Private LAN Segment）借助 IP 公共网络实现 LAN 之间通过虚拟专用网段互连，是局域网在 IP 公共网络上的延伸。

(4) 虚拟专用路由网（VPRN）业务

VPRN（Virtual Private Routing Network）借助 IP 公共网络实现总部、分支机构和远端办公室之间通过网络管理虚拟路由器进行互连，业务实现包括两类：一种是使用传统 VPN 协议（如 IPSec、GRE 等）实现的 VPRN，另外一种是 MPLS 方式的 VPRN。

4. 按实现层次划分

(1) L3VPN：包括 BGP/MPLS VPN、IPSec VPN、GRE VPN、DVPN 等。

(2) L2VPN：包括 Martini 方式的 MPLS L2VPN、Kompalla 方式的 MPLS L2VPN、SVC 方式 MPLS L2VPN、VPLS 以及静态 CCC 配置。

(3) VPDN：L2TP、PPTP 等。

第2章 L2TP 协议配置

2.1 L2TP 协议简介

2.1.1 VPDN 概述

VPDN（Virtual Private Dial Network，虚拟私有拨号网）是指利用公共网络（如 ISDN 和 PSTN）的拨号功能及接入网来实现虚拟专用网，从而为企业、小型 ISP、移动办公人员提供接入服务。

VPDN 采用专用的网络加密通信协议，在公共网络上为企业建立安全的虚拟专网。企业驻外机构和出差人员可从远程经由公共网络，通过虚拟加密隧道实现和企业总部之间的网络连接，而公共网络上其它用户则无法穿过虚拟隧道访问企业网内部的资源。

VPDN 有下列两种实现方式：

(1) NAS 通过隧道协议，与 VPDN 网关建立通道的方式。这种方式将客户的 PPP 连接直接连到企业的网关上，目前可使用的协议有 L2F 与 L2TP。其好处在于：对用户是透明的，用户只需要登录一次就可以接入企业网络，由企业网进行用户认证和地址分配，而不占用公共地址，用户可使用各种平台上网。这种方式需要 NAS 支持 VPDN 协议，需要认证系统支持 VPDN 属性，网关一般使用路由器或 VPN 专用服务器。

(2) 客户机与 VPDN 网关建立隧道的方式。这种方式由客户机先建立与 Internet 的连接，再通过专用的客户软件（如 Win2000 支持的 L2TP 客户端）与网关建立通道连接。其好处在于：用户上网的方式和地点没有限制，不需 ISP 介入。缺点是：用户需要安装专用的软件（一般都是 Win2000 平台），限制了用户使用的平台。

VPDN 隧道协议可分为 PPTP、L2F 和 L2TP 三种，目前使用最广泛的是 L2TP。

2.1.2 L2TP 协议介绍

1. 协议背景

PPP 协议定义了一种封装技术，可以在二层的点到点链路上传输多种协议数据包，这时，用户与 NAS 之间运行 PPP 协议，二层链路端点与 PPP 会话点驻留在相同硬件设备上。

L2TP 协议提供了对 PPP 链路层数据包的通道（Tunnel）传输支持，允许二层链路端点和 PPP 会话点驻留在不同设备上，并且采用包交换网络技术进行信息交互，从而扩展了 PPP 模型。L2TP 协议结合了 L2F 协议和 PPTP 协议的各自优点，成为 IETF 有关二层隧道协议的工业标准。

2. 典型 L2TP 组网应用

使用 L2TP 协议构建的 VPDN 应用的典型组网如图 2-1所示：

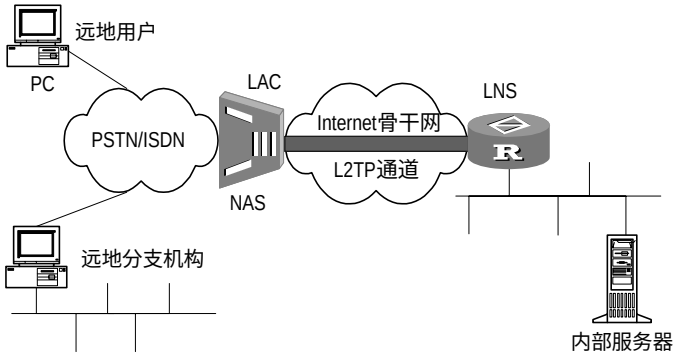

图2-1 应用 L2TP 构建的 VPDN 服务

其中，LAC 表示 L2TP 访问集中器（L2TP Access Concentrator），是附属在交换网络上的具有 PPP 端系统和 L2TP 协议处理能力的设备。LAC 一般是一个网络接入服务器 NAS，主要用于通过 PSTN/ISDN 网络为用户提供接入服务。LNS 表示 L2TP 网络服务器（L2TP Network Server），是 PPP 端系统上用于处理 L2TP 协议服务器端部分的设备。

LAC 位于 LNS 和远端系统（远地用户和远地分支机构）之间，用于在 LNS 和远端系统之间传递信息包，把从远端系统收到的信息包按照 L2TP 协议进行封装并送往 LNS，将从 LNS 收到的信息包进行解封装并送往远端系统。LAC 与远端系统之间可以采用本地连接或 PPP 链路，VPDN 应用中通常为 PPP 链路。LNS 作为 L2TP 隧道的另一侧端点，是 LAC 的对端设备，是被 LAC 进行隧道传输的 PPP 会话的逻辑终止端点。

3. L2TP 协议的技术细节

(1) L2TP 协议结构

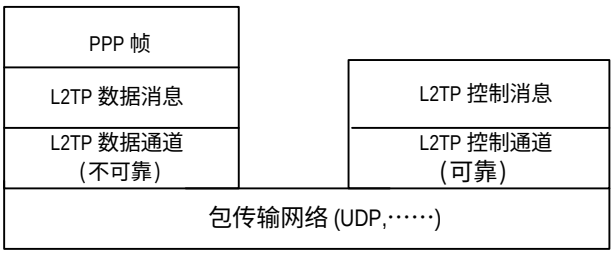

图2-2 L2TP 协议结构

上图所示 L2TP 协议结构描述了 PPP 帧和控制通道以及数据通道之间的关系。PPP 帧在不可靠的 L2TP 数据通道上进行传输，控制消息在可靠的 L2TP 控制通道内传输。

通常 L2TP 数据以 UDP 报文的形式发送。L2TP 注册了 UDP 1701 端口，但是这个端口仅用于初始的隧道建立过程中。L2TP 隧道发起方任选一个空闲的端口（未必是 1701）向接收方的 1701 端口发送报文；接收方收到报文后，也任选一个空闲的端口（未必是 1701），给发送方的指定端口回送报文。至此，双方的端口选定，并在隧道保持连通的时间段内不再改变。

(2) 隧道和会话的概念

在一个 LNS 和 LAC 对之间存在着两种类型的连接，一种是隧道（Tunnel）连接，它定义了一个 LNS 和 LAC 对；另一种是会话（Session）连接，它复用在隧道连接之上，用于表示承载在隧道连接中的每个 PPP 会话过程。在同一对 LAC 和 LNS 之间可以建立多个 L2TP 隧道，隧道由一个控制连接和一个或多个会话（Session）组成。会话连接必须在隧道建立（包括身份保护、L2TP 版本、帧类型、硬件传输类型等信息的交换）成功之后进行，每个会话连接对应于 LAC 和 LNS 之间的一个 PPP 数据流。控制消息和 PPP 数据报文都在隧道上传输。

L2TP 使用 Hello 报文来检测隧道的连通性。LAC 和 LNS 定时向对端发送 Hello 报文，若在一段时间内未收到 Hello 报文的应答，该会话将被清除。

(3) 控制消息和数据消息的概念

L2TP 中存在两种消息 :控制消息和数据消息。控制消息用于隧道和会话连接的建立、维护以及传输控制；数据消息则用于封装 PPP 帧并在隧道上传输。控制消息的传输是可靠传输，并且支持对控制消息的流量控制和拥塞控制；而数据消息的传输是不可靠传输，若数据报文丢失，不予重传，不支持对数据消息的流量控制和拥塞控制。

控制消息和数据消息共享相同的报文头。L2TP 报文头中包含隧道标识符（Tunnel ID）和会话标识符（Session ID）信息，用来标识不同的隧道和会话。隧道标识相同、会话标识不同的报文将被复用在一个隧道上，报文头中的隧道标识符与会话标识符由对端分配。

4. 两种典型的 L2TP 隧道模式

远端系统或 LAC 客户端（运行 L2TP 协议的主机）与 LNS 之间的隧道模式如图 2-3 所示：

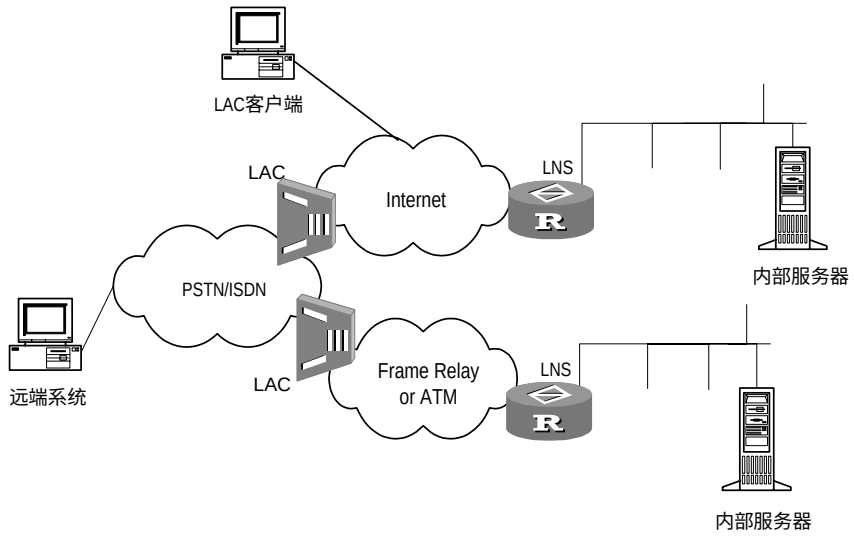

图2-3 两种典型的 L2TP 隧道模式

(1) 由远程拨号用户发起。远程系统通过 PSTN/ISDN 拨入 LAC，由 LAC 通过 Internet 向 LNS 发起建立通道连接请求。拨号用户地址由 LNS 分配；对远程拨号用户的验证与计费既可由 LAC 侧的代理完成，也可在 LNS 侧完成。

(2) 直接由 LAC 客户（指可在本地支持 L2TP 协议的用户）发起。此时 LAC 客户可直接向 LNS 发起通道连接请求，无需再经过一个单独的 LAC 设备。此时，LAC 客户地址的分配由 LNS 来完成。

5. L2TP 隧道会话的建立过程

L2TP 应用的典型组网如下图所示：

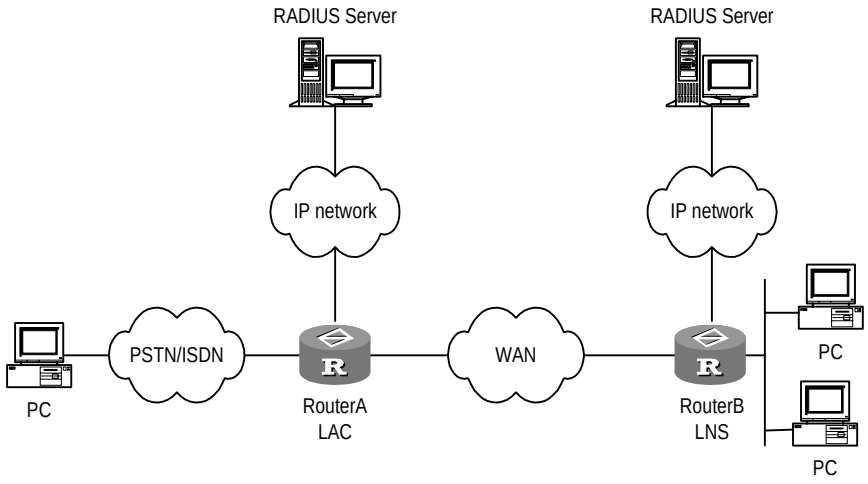

图2-4 L2TP 应用的典型组网

L2TP 隧道的呼叫建立流程可如下图所示：

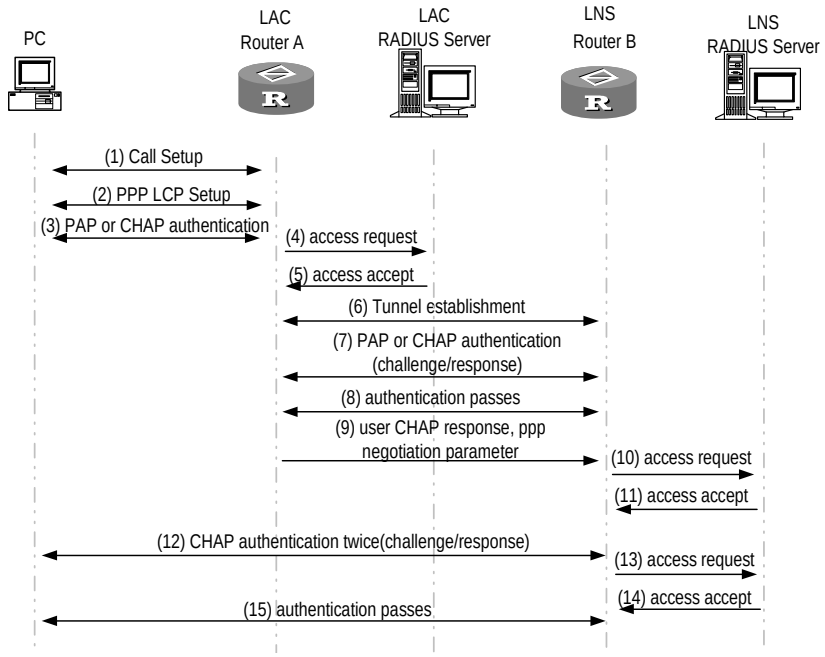

图2-5 L2TP 隧道的呼叫建立流程

L2TP 隧道的呼叫建立流程过程为：

(1) 用户端 PC 机发起呼叫连接请求；

(2) PC 机和 LAC 端（RouterA）进行 PPP LCP 协商；

(3) LAC 对 PC 机提供的用户信息进行 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，如果认证通过则返回该用户对应的 LNS 地址等相关信息，并且 LAC 准备发起 Tunnel 连接请求；

(6) LAC 端向指定 LNS 发起 Tunnel 连接请求；

(7) LAC 端向指定 LNS 发送 CHAP challenge 信息，LNS 回送该 challenge 响应消息 CHAP response，并发送 LNS 侧的 CHAP challenge，LAC 返回该 challenge 的响应消息 CHAP response；

(8) 隧道验证通过；

(9) LAC 端将用户 CHAP response、response identifier 和 PPP 协商参数传送给 LNS；

(10) LNS 将接入请求信息发送给 RADIUS 服务器进行认证；

(11) RADIUS 服务器认证该请求信息，如果认证通过则返回响应信息；

(12) 若用户在 LNS 侧配置强制本端 CHAP 认证，则 LNS 对用户进行认证，发送 CHAP challenge，用户侧回应 CHAP response；

(13) LNS 再次将接入请求信息发送给 RADIUS 服务器进行认证；

(14) RADIUS 服务器认证该请求信息，如果认证通过则返回响应信息；

验证通过，用户访问企业内部资源。

6. L2TP 协议的特点

- 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 可与 IPSec 结合起来实现数据安全，这使得通过 L2TP 所传输的数据更难被攻击。L2TP 还可根据特定的网络安全要求在 L2TP 之上采用通道加密技术、端对端数据加密或应用层数据加密等方案来提高数据的安全性。

- 多协议传输

L2TP 传输 PPP 数据包，这样就可以在 PPP 数据包内封装多种协议。

- 支持 RADIUS 服务器的验证

LAC 端将用户名和密码发往 RADIUS 服务器进行验证申请，RADIUS 服务器负责接收用户的验证请求，完成验证。

- 支持内部地址分配

LNS 可放置于企业网的防火墙之后，它可以对远端用户的地址进行动态的分配和管理，可支持私有地址应用（RFC1918）。为远端用户所分配的地址不是 Internet 地址而是企业内部的私有地址，这样方便了地址的管理并可以增加安全性。

- 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，可根据这些数据方便地进行网络计费。

- 可靠性

L2TP 协议支持备份 LNS，当一个主 LNS 不可达之后，LAC 可以重新与备份 LNS 建立连接，这样，增加了 VPN 服务的可靠性和容错性。

下面从 LAC、LNS 两侧分别介绍 L2TP 的配置。

2.2 LAC 配置

在 L2TP 的配置中，LAC 端和 LNS 端的配置有所不同，下面先介绍一下 LAC 端的配置。在各项配置任务中，必须先启动 L2TP、创建 L2TP 组，然后再进行其它功能特性的配置。PPP 配置相关命令的详细介绍请参看相关章节。

LAC 侧要进行的配置包括：

- 启用 L2TP（必选）
- 创建 L2TP 组（必选）
- 设置发起 L2TP 连接请求及 LNS 地址（必选）
- 设置本端名称（可选）
- 启用通道验证及设置密码（可选）
- 配置将 AVP 数据隐含（可选）
- 设置通道 Hello 报文发送时间间隔（可选）
- 设置用户名及域名的查找顺序（可选）
- 设置用户名、密码及配置用户验证（必选）
- 强制挂断通道（可选）
- 开启或关闭流控功能（可选）
- 配置 L2TP 会话超时时间（可选）
- 配置 L2TP Tunnel 连接保持功能（可选）
- 配置 LAC 作为客户端（可选）

2.2.1 启用 L2TP

只有启用 L2TP 后，路由器上 L2TP 功能才能正常发挥作用；如果禁止 L2TP，则即便配置了 L2TP 的参数，路由器也不会提供相关功能。

这些配置在 LAC 侧必须配置。

请在系统视图下进行下列配置。

表2-1 启用/禁止 L2TP

操作	命令
启用 L2TP	**l2tp enable**
禁止 L2TP	**undo l2tp enable**

缺省情况下，L2TP 功能是被禁止的。

2.2.2 创建 L2TP 组

为了进行 L2TP 的相关参数配置，还需要增加 L2TP 组，这不仅可以在路由器上灵活的配置 L2TP 各项功能，而且方便地实现了 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（如接收的通道对端名称、发起 L2TP 连接请求及 LNS 地址等）保持对应关系即可。

这些配置在 LAC 侧必须配置。

请在系统视图下进行下列配置。

表2-2 创建/删除 L2TP 组

操作	命令
创建 L2TP 组	**l2tp-group** *group-number*
删除 L2TP 组	**undo l2tp-group** *group-number*

在创建 L2TP 组后，就可以在 L2TP 组视图下进行和该 L2TP 组相关的其它配置了，如本端名称、发起 L2TP 连接请求及 LNS 地址等。

缺省情况下，未创建任何 L2TP 组。

2.2.3 设置发起 L2TP 连接请求及 LNS 地址

路由器不会随便去与其它路由器或 LNS 服务器建立 L2TP 通道，需要满足一定的条件才会向其它路由器或 LNS 服务器发出建立 L2TP 连接的请求。通过配置对接入用户信息的判别条件，并指定相应的 LNS 端的 IP 地址，路由器可以鉴定用户是否为 VPN 用户，并决定是否向 LNS 发起连接。最多可以设置五个 LNS，即允许存在备用 LNS。正常运行时，本路由器（LAC）按照 LNS 配置的先后顺序，依次向对端（LNS）进行 L2TP 连接请求，直到某个 LNS 接受连接请求，该 LNS 就成为 L2TP 隧道的对端。发起 L2TP 连接请求的触发条件共支持三种：完整的用户名（fullusername）、带特定域名的用户（domain）、被叫号码（dnis）。

这些配置在 LAC 侧必须配置。

请在 L2TP 组视图下进行下列配置。

表2-3 设置发起 L2TP 连接请求及 LNS 地址

操作	命令
配置鉴别用户是否是 VPN 用户的方式，并设置对应的 LNS 的 IP 地址。	**start l2tp** { **ip** *ip-addr* [**ip** *ip-addr*] [**ip** *ip-addr*] **...** } { **domain** *domain-name* | **fullusername** *user-name* }
取消连接请求配置	**undo start**

上述参数无缺省值，可根据实际情况进行配置，但必须配置一种触发条件，方可发出 L2TP 连接的请求。

2.2.4 设置本端名称

用户可在 LAC 侧配置本端通道名称。LAC 侧通道名称要与 LNS 侧配置的接收通道对端名称保持一致。

这些配置在 LAC 侧为可选配置。

请在 L2TP 组视图下进行下列配置。

表2-4 设置本端名称

操作	命令
设置本端名称	**tunnel name** *name*
恢复本端名称为默认值	**undo tunnel name**

缺省情况下，本端名称为路由器的主机名。

2.2.5 启用隧道验证及设置密码

用户可根据实际需要，决定是否在创建隧道连接之前启用隧道验证。隧道验证请求可由 LAC 或 LNS 任何一侧发起。只要有一方启用了隧道验证，则只有在对端也启用了隧道验证，两端密码完全一致并且不为空的情况下，隧道才能建立；否则本端将自动将隧道连接断开。若隧道两端都配置了禁止隧道验证，隧道验证的密码一致与否将不起作用。

这些配置在 LAC 侧为可选配置。

请在 L2TP 组视图下进行下列配置。

表2-5 设置通道验证及密码

操作	命令
启用隧道验证	**tunnel authentication**
禁止隧道验证	**undo tunnel authentication**
设置隧道验证的密码	**tunnel password** { **simple** | **cipher** } *password*
恢复隧道验证的密码为缺省值	**undo tunnel password**

缺省情况下，启用隧道验证，隧道验证的密码为空。为了保证通道安全，建议用户最好不要禁用隧道验证的功能。

2.2.6 配置将 AVP 数据隐含

L2TP 协议使用 AVP（Attribute Value Pair，属性值对）来传递和协商 L2TP 的一些参数属性等。在缺省情况下，AVP 是采用明文形式传输的。为了保证安全，用户可以通过下面的配置，将这些 AVP 隐藏起来传输。隐含 AVP 功能必须是两端都使用隧道验证的情况下才起作用。

这些配置在 LAC 侧为可选配置。

请在 L2TP 组视图下进行下列配置。

表2-6 配置将 AVP 数据隐含

操作	命令
配置将 AVP 数据隐含的方式传输	**tunnel avp-hidden**
恢复 AVP 的缺省传输方式	**undo tunnel avp-hidden**

缺省情况下，AVP 是采用明文形式传输的。

2.2.7 设置通道 Hello 报文发送时间间隔

为了检测 LAC 和 LNS 之间通道的连通性，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，如果重复发送超过 3 次都没有收到对端的响应信息则认为 L2TP 隧道已经断开，需要在 LAC 和 LNS 之间重新建立隧道连接。

这项配置在 LAC 侧为可选配置。

请在 L2TP 组视图下进行下列配置。

表2-7 设置通道 Hello 报文发送时间间隔

操作	命令
设置通道 Hello 报文发送时间间隔	**tunnel timer hello** *hello-interval*
恢复通道 Hello 报文发送时间间隔	**undo tunnel timer hello**

缺省情况下，通道 Hello 报文的发送时间间隔为 60 秒。如果 LAC 侧不进行此项配置，LAC 将采用此缺省值为周期向对端发送 Hello 报文。

2.2.8 设置被叫号码与域名的查找顺序

在域名方式下，有四种查找规则可供选择：

- dnis-domain（先按被叫号码查找，再按域名查找）
- dnis（仅按照被叫号码查找）
- domain-dnis（先按域名查找，再被叫号码查找）
- domain（仅按照域名查找）

这些配置在 LAC 侧为可选配置。

请在系统视图下进行下列配置。

表2-8 设置域名分隔符及查找顺序

操作	命令
设置查找规则	**l2tp match-order** { **dnis-domain** | **dnis** | **domain-dnis** | **domain** }
恢复缺省的查找规则	**undo l2tp match-order**

命令 **l2tp match-order** 仅仅配置了被叫号码和域名之间的查找顺序，而在实际查找过程中，一定是先按照全用户名进行查找，然后再按照该命令的配置顺序依次进行查找。

缺省情况下，先根据被叫号码，再根据域名进行查找。

2.2.9 设置用户名、密码及配置本地验证

在 LAC 侧配置 AAA 认证时，如果选择了 local（本地认证）方式，则需要在 LAC 侧配置本地用户名和口令。

LAC 通过检查远程拨入用户名与口令是否与本地注册用户名/口令相符合来进行用户身份验证，以检查用户是否为合法 VPN 用户。验证通过后才能发起建立通道连接的请求，否则将该用户转入其它类型的服务。

在 LAC 端进行用户身份验证，用户名采用 VPN 用户全名，口令为 VPN 用户注册口令。

这些配置在 LAC 侧必须配置。

1. 配置用户名、密码

表2-9 配置用户名、密码

操作	命令
设置用户名（系统视图）	**local-user** *username*
取消当前设置（系统视图）	**undo local-user** *username*
配置本地用户口令（本地用户视图）	**password** { **simple** | **cipher** } *password*

缺省情况下，LAC 侧未配置本地用户名和口令。

2. 配置 PPP 用户验证类型

请在接口视图下进行下列配置。

表2-10 配置/取消用户验证类型

操作	命令
配置对 PPP 用户进行验证	**ppp authentication-mode** { **chap** | **pap** } [**call-in** | **domain** *isp-name*]
取消对 PPP 用户进行验证	**undo ppp authentication-mode**

配置本地验证的接口应该是接入用户的接口。

3. 配置 PPP 域用户及认证方案

表2-11 配置 PPP 域用户及认证方案

操作	命令
创建 ISP 域并进入域视图（系统视图）	**domain** { *isp-name* | **default** { **disable** | **enable** *isp-name* } }
删除指定的 ISP 域（系统视图）	**undo domain** *isp-name*
配置 PPP 域用户的认证方法（ISP 域视图）	**scheme local**

2.2.10 强制断开 L2TP 连接

当用户数为零、网络发生故障或当管理员主动要求时，都会产生断开连接的过程。LAC 和 LNS 任何一端都可主动发起断开连接的请求，连接断开后，该通道上的所有控制连接与会话连接也将被清除；当有新用户拨入时，还可重新建立连接。

这些配置在 LAC 端为可选配置。

请在用户视图下进行下列配置。

表2-12 强制断开连接

操作	命令
强制断开一个隧道连接	**reset l2tp tunnel** { *remote-name* | *tunnel-id* }
强制断开一个会话连接	**reset l2tp session session-id** *session-id*
强制断开该用户的连接	**reset l2tp user user-name** *user-name*

2.2.11 开启或关闭流控功能

该配置任务可以开启或关闭 L2TP 简单的通道流控功能，达到流控目的。

这些配置在 LAC 侧为可选配置。

请在 L2TP 组视图下进行下列配置。

表2-13 开启或关闭流控功能

操作	命令
开启流控功能	**tunnel flow-control**
关闭流控功能	**undo tunnel flow-control**

缺省情况下，关闭通道流控功能。

2.2.12 配置 L2TP 会话超时时间

通常情况下，当 L2TP 的一个会话在一段时间内没有数据收发时，系统就会自动挂断这个会话。

用户可以根据需要设置会话的超时时间，甚至可以设置永不超时（即不自动挂断）。

请在 L2TP 组视图下进行下列配置。

表2-14 配置 L2TP 会话超时时间

操作	命令
配置 L2TP 会话超时时间	**session idle-time** *seconds*
配置 L2TP 会话不超时	**undo session idle-time**

缺省情况下，L2TP 会话不超时。

2.2.13 配置 L2TP Tunnel 连接保持功能

通常情况下，只有当 PPP 用户发起 L2TP 会话请求之后，LAC 才会与 LNS 建立 tunnel，并且当所有 PPP 会话（session）都断开之后，此 tunnel 也会自动拆除。

对于要求快速建立连接的应用，需要事先建立好 tunnel，一旦有 PPP 会话请求，系统可以立即建立一个会话。这就要求 LAC 与 LNS 之间总是保持一个 tunnel 连接，即使该 tunnel 上没有会话也不会被拆除。

请在 L2TP 组视图下进行下列配置。

表2-15 配置 Tunnel 连接保持功能

操作	命令
配置 Tunnel 连接保持功能	**tunnel keepstanding**
取消 Tunnel 连接保持功能	**undo tunnel keepstanding**

缺省情况下， 取消 Tunnel 连接保持功能。

📖 说明：

Tunnel 连接保持功能必须在 LAC 和 LNS 上同时配置。

配置好以上条件之后，运行 **start l2tp tunnel** 命令，以发送 tunnel 连接请求。每执行一次该命令，则发送一次连接请求。

请在 L2TP 组视图下执行下列命令。

表2-16 启动 tunnel 连接

操作	命令
启动 tunnel 连接	**start l2tp tunnel**

2.2.14 配置 LAC 作为客户端

通常情况下，L2TP 的客户端是拨号连接到 LAC 的用户主机。此时用户与 LAC 的连接总是 PPP 连接。

如果使用 LAC 同时作为客户端,那么用户与 LAC 之间的连接就不受限于 PPP 连接，而只要是一个 IP 连接就可以了，这样 LAC 能够将用户的 IP 报文转发到 LNS。

使用 LAC 同时作为客户端，是在 LAC 上建立一个虚拟的 PPP 用户，该用户与 LNS 保持一个常连接。其它所有实际用户的 IP 报文都是通过此虚拟用户转发给 LNS 的。

使用 LAC 同时作为客户端的配置是在配置 LAC 的基础上增加如下配置：

- 创建一个虚模板接口
- 配置虚模板接口参数，包括 IP 地址、PPP 验证方法及 PPP 验证的用户名、密码。
- 配置虚用户建立 L2TP 隧道

📖 说明：

配置 LAC 作为客户端应同时配置 L2TP Session 不超时，否则当没有实际用户数据流时，虚拟用户的会话会因超时而挂断。

---

1. 创建虚拟模板接口

请在系统视图下进行下列配置。

表2-17 创建/删除虚拟模板接口

操作	命令
创建虚拟模板接口	**interface virtual-template** *virtual-template-number*
删除虚拟模板接口	**undo interface virtual-template** *virtual-template-number*

2. 配置虚拟模板接口参数

请在虚拟模板接口视图下进行下列配置。

表2-18 配置虚拟模板接口参数

操作	命令
配置虚拟模板接口 IP 地址	**ip address** *address mask*
配置 PPP 验证方式	**ppp authentication-mode { pap | chap }**
配置 CHAP 验证用户名	**ppp chap user** *user-name*
配置 CHAP 验证密码	**ppp chap password { simple | cipher }** *password*
配置 PAP 验证用户名、密码	**ppp pap local-user** *user-name* **password { simple | cipher }** *password*

3. 配置虚用户建立 L2TP 隧道

请在虚拟模板接口视图下进行下列配置。

表2-19 配置虚用户建立 L2TP 隧道

操作	命令
配置虚用户建立 L2TP 隧道	**l2tp-auto-client enable**
取消虚用户建立 L2TP 隧道	**undo l2tp-auto-client enable**

缺省情况下，未配置虚用户建立 L2TP 隧道。

2.3 LNS 配置

在 LNS 的各项配置任务中，必须先启动 L2TP、创建 L2TP 组，然后再进行其它功能特性的配置。在 L2TP 支持多实例配置中，只有启用 L2TP 多实例功能，其他配置才能生效。PPP 和虚拟接口模板（Virtual-Template）的相关命令的详细介绍，请参看相关章节。

LNS 主要配置包括：

- 启用 L2TP（必选）
- 创建 L2TP 组（必选）
- 创建虚接口模板（必选）
- 设置接收呼叫的虚拟接口模板、通道对端名称和域名（必选）
- 设置本端名称(可选)
- 配置隧道验证及设置密码(可选)
- 配置将 AVP 数据隐含(可选)
- 设置通道 Hello 报文发送时间间隔(可选)
- 强制本端 CHAP 验证(可选)

- 强制 LCP 重新协商(可选)
- 设置本端地址及分配的地址池(必选)
- 设置用户名及域名的查找顺序（可选）
- 设置用户名、密码及配置用户验证(可选)
- 强制挂断通道(可选)
- 开启或关闭流控功能(可选)

2.3.1 启用 L2TP

只有启用 L2TP 后，路由器上 L2TP 功能才能正常发挥作用；如果禁止 L2TP，则即便配置了 L2TP 的参数路由器也不会提供相关功能。

这些配置在 LNS 侧必须配置。

请在系统视图下进行下列配置。

表2-20 启用/禁止 L2TP

操作	命令
启用 L2TP	**l2tp enable**
禁止 L2TP	**undo l2tp enable**

缺省情况下，L2TP 功能是被禁止的。

2.3.2 启用/禁止 L2TP 多实例功能

只有启用 L2TP 多实例功能，路由器才能为多个企业做 LNS。L2TP 多实例功能的实现丰富了 VPN 组网方式，主要应用在 MPLS-VPN 组网中。在实际组网应用中，企业的私网路由需要通过配置 vpn-instance 来实现，关于 vpn-instance 的配置可以参考 MPLS 配置相关章节。在“ 2.5.4 L2TP 多实例组网应用 ”中有简单配置步骤描述。

在 L2TP 多实例应用中，这些配置在 LNS 侧必须配置。

请在系统视图下进行下列配置。

表2-21 启用/禁止 L2TP 多实例功能

操作	命令
启用 L2TP 多实例功能	**l2tpmoreexam enable**
禁止 L2TP 多实例功能	**undo l2tpmoreexam enable**

缺省情况下，L2TP 多实例功能是被禁止的。

2.3.3 创建 L2TP 组

为了进行 L2TP 的相关参数配置，还需要增加 L2TP 组，这不仅可以在路由器上灵活的配置 L2TP 各项功能，而且方便地实现了 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（如接收的通道对端名称、发起 L2TP 连接请求及 LNS 地址等）保持对应关系即可。

这些配置在 LNS 侧必须配置。

请在系统视图下进行下列配置。

表2-22 创建/删除 L2TP 组

操作	命令
创建 L2TP 组	**l2tp-group** *group-number*
删除 L2TP 组	**undo l2tp-group** *group-number*

在创建的 L2TP 组后，就可以在 L2TP 组视图下进行和该 L2TP 组相关的其它配置了，如本端名称、接收的通道对端名称等。

缺省情况下，未创建任何 L2TP 组。

2.3.4 创建虚拟接口模板

虚拟接口模板主要用于配置路由器在运行过程中动态创建的虚接口的工作参数，如 MP 捆绑逻辑接口和 L2TP 逻辑接口等。

这些配置在 LNS 侧必须配置。

请在系统视图下进行下列配置。

表2-23 创建/删除虚接口模板

操作	命令
创建虚接口模板	**interface virtual-template** *virtual-template-number*
删除虚接口模板	**undo interface virtual-template** *virtual-template-number*

缺省情况下，未创建虚拟接口模板。

2.3.5 设置接收呼叫的虚拟接口模板、通道对端名称和域名

LNS 可以使用不同的虚拟接口模板接收不同的 LAC 创建隧道的请求。在接收到 LAC 发来的创建隧道请求后，LNS 需要检查 LAC 的名称是否与合法通道对端名称相符合，从而决定是否允许通道对方进行隧道的创建。

这些配置在 LNS 侧必须配置。

请在 L2TP 组视图下进行下列配置。

表2-24 设置/取消接收的通道对端名称

操作	命令
设置通道对端的名称（L2TP 组不为 1）	**allow l2tp virtual-template** *virtual-template-number* **remote** *remote-name* [**domain** *domain-name*]
设置通道对端的名称（L2TP 组为 1）	**allow l2tp virtual-template** *virtual-template-number* [**remote** *remote-name*] [**domain** *domain-name*]
取消通道对端的名称	**undo allow**

当 L2TP 组号为 1 时（缺省的 L2TP 组号），可以不指定通道对端名 *remote-name*。如果在 L2TP 组 1 的视图下，仍指定对端名称，则 L2TP 组 1 不作为缺省的 L2TP 组。

🕮 说明：

- 只有组号为 1 的 L2TP 组才可以设置成缺省的组。
- 当 L2TP 组号为 1 时（缺省的 L2TP 组号），任何名字的计算机都能发起隧道请求。
- “ **start** ”命令和“ **allow** ”命令是互斥的，配了一条命令之后另一条就自动失效；

2.3.6 设置本端名称

用户可在 LNS 侧配置本端通道名称。

这些配置在 LNS 侧为可选配置。

请在 L2TP 组视图下进行下列配置。

表2-25 设置本端名称

操作	命令
设置本端名称	**tunnel name** *name*
恢复本端名称为默认值	**undo tunnel name**

缺省情况下，本端名称为路由器的主机名。

2.3.7 启用隧道验证及设置密码

用户可根据实际需要决定是否在创建隧道连接之前启用隧道验证。隧道验证请求可由 LAC 或 LNS 任何一侧发起。只要有一方启用了隧道验证，则只有在对端也启用了隧道验证，两端密码完全一致并且不为空的情况下，隧道才能建立；否则本端将

自动将隧道连接断开。若隧道两端都配置了禁止隧道验证，隧道验证的密码一致与否将不起作用。

这些配置在 LNS 侧为可选配置。

请在 L2TP 组视图下进行下列配置。

表2-26 设置通道验证及密码

操作	命令
启用通道验证	**tunnel authentication**
禁止通道验证	**undo tunnel authentication**
设置通道验证的密码	**tunnel password** { **simple** | **cipher** } *password*
取消通道验证的密码	**undo tunnel password**

缺省情况下，启用隧道验证，隧道验证的密码为空。为了保证通道安全，建议用户最好不要禁用隧道验证的功能。

2.3.8 配置将 AVP 数据隐含

L2TP 协议使用 AVP（Attribute Value Pair，属性值对）来传递和协商 L2TP 的一些参数属性等。在缺省情况下，AVP 是采用明文形式传输的。为了保证安全，用户可以通过下面的配置，将这些 AVP 隐藏起来传输。隐含 AVP 功能必须是两端都使用隧道验证的情况下才起作用。

这些配置在 LNS 侧为可选配置。

请在 L2TP 组视图下进行下列配置。

表2-27 配置将 AVP 数据隐含

操作	命令
配置将 AVP 数据隐含的方式传输	**tunnel avp-hidden**
恢复 AVP 的缺省传输方式	**undo tunnel avp-hidden**

缺省情况下，AVP 是采用明文形式传输的。

2.3.9 设置通道 Hello 报文发送时间间隔

为了检测 LAC 和 LNS 之间通道的连通性，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，如果重复发送超过 3 次都没有收到对端的响应信息则认为 L2TP 隧道已经断开，需要在 LAC 和 LNS 之间重新建立隧道连接。

这些配置在 LNS 侧为可选配置。

请在 L2TP 组视图下进行下列配置。

表2-28 设置通道 Hello 报文发送时间间隔

操作	命令
设置通道 Hello 报文发送时间间隔	**tunnel timer hello** *hello-interval*
恢复通道 Hello 报文发送时间间隔	**undo tunnel timer hello**

缺省情况下，通道 Hello 报文的发送时间间隔为 60 秒。如果用户不进行此项配置，LNS 将采用此缺省值为周期向对端发送 Hello 报文。

2.3.10 强制本端 CHAP 验证

当 LAC 对用户进行代理验证后，LNS 可再次对用户进行验证。此时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 通道才能建立。

在 L2TP 组网中，LNS 侧对用户的验证方式有三种：代理验证、强制 CHAP 验证和 LCP 重协商。

这三种验证方式中，LCP 重协商的优先级最高，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，采用相应的虚拟接口模板上配置的验证方式。

如果只配置强制 CHAP 验证，则 LNS 对用户进行 CHAP 验证。强制 CHAP 验证配置在 LNS 侧为可选配置。

请在 L2TP 组视图下进行下列配置。

表2-29 强制本端 CHAP 验证

操作	命令
强制本端 CHAP 验证	**mandatory-chap**
取消本端 CHAP 验证	**undo mandatory-chap**

如果既不配置 LCP 重协商，也不配置强制 CHAP 验证，则 LNS 对用户进行的是代理验证。在这种情况下，LAC 将它从用户得到的所有验证信息及 LAC 端本身配置的验证方式发送给 LNS，LNS 侧会默认通过 LAC 侧对用户的验证结果。

在 LNS 使用代理验证时，如果虚拟接口模板配置的验证方式为 CHAP，而 LAC 端配置的验证方式为 PAP，则由于 LNS 要求的 CHAP 验证级别高于 LAC 能够提供的 PAP 验证，验证将无法通过，会话也就不能正确建立。

缺省情况下，不进行本端 CHAP 验证。

2.3.11 强制 LCP 重新协商

对由 NAS 发起的 VPN 服务请求（NAS-Initialized VPN），在 PPP 会话开始时，用户先和 NAS（网络接入服务器）进行 PPP 协商。若协商通过，则由 NAS 初始化 L2TP 通道连接，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（如需在 LNS 侧也要进行验证与计费），需要强制 LNS 与用户间重新进行 LCP 协商，此时将忽略 NAS 侧的代理验证信息。

强制 LCP 重新协商配置在 LNS 侧为可选配置。

请在 L2TP 组视图下进行下列配置。

表2-30 强制/取消 LCP 重新协商

操作	命令
强制 LCP 重新协商	**mandatory-lcp**
取消 LCP 重新协商	**undo mandatory-lcp**

缺省情况下，不进行 LCP 重新协商。

启用 LCP 重协商后，如果相应的虚拟接口模板上不配置验证，则 LNS 将不对接入用户进行二次验证（这时用户只在 LAC 侧接受一次验证），直接将全局地址池的地址给 client 端。

2.3.12 设置本端地址及分配的地址池

当 LAC 与 LNS 之间的 L2TP 隧道连接建立之后，LNS 需要从地址池中为 VPN 用户分配 IP 地址。在指定地址池之前，需要在系统视图或域视图下用 **ip pool** 命令先定义一个地址池（关于 **ip pool** 命令的详细描述请参见“安全部分”）。若 LNS 采用代理验证或强制 CHAP 验证，系统将使用域视图下的地址池给用户分配 IP 地址；若 LNS 采用 LCP 重新协商方式进行验证，系统将使用全局地址池给用户分配 IP 地址。

这些配置在 LNS 侧为可选配置。

请在虚拟接口模板视图下进行下列配置。

表2-31 设置本端地址及分配的地址池

操作	命令
设置本端 IP 地址	**ip address** *X.X.X.X netmask*
取消本端 IP 地址	**undo ip address** *X.X.X.X netmask*
指定给对方分配地址所用的地址池	**remote address** { **pool** *pool-number* | *X.X.X.X* }
删除给对方分配地址所用的地址池	**undo remote address**

当为对方指定分配地址所用的地址池时，如果关键字 **pool** 后面没有输入具体的 *pool-number* 值，则表示从缺省地址池来分配地址。

缺省情况下，从地址池 0（缺省地址池）中给对方分配地址。

2.3.13 设置被叫号码与域名的查找顺序

请在系统视图下进行下列配置。

表2-32 设置域名分隔符及查找顺序

操作	命令
设置查找规则	**l2tp match-order** { **dnis-domain | dnis | domain-dnis | domain** }
恢复缺省的查找规则	**undo l2tp match-order**

在 L2TP 多实例应用中，在 LNS 端，只能采用 **domain** 方式查找。

2.3.14 设置用户名、密码及配置用户验证

在 LNS 侧，如果配置了强制 CHAP 认证，则需要在 LNS 侧配置本地注册用户名和口令。

LNS 通过检查远程拨入用户名与口令是否与本地注册用户名/口令相符合来进行用户身份验证，以检查用户是否为合法 VPN 用户。验证通过后就可以进行 VPN 用户和 LNS 的通信，否则将通知 L2TP 清除这个 L2TP 链接。

在 LNS 端进行用户身份验证，用户名可以采用两种形式：

- 用户名为 VPN 用户全名，口令为 VPN 用户注册口令。
- 用户名为用户名+域名，口令为 VPN 用户注册口令。

这些配置在 LNS 侧为可选配置。具体配置方法请参考2.2.9 设置用户名、密码及配置本地验证。

2.3.15 强制断开 L2TP 连接

当用户数为零、网络发生故障或当管理员主动要求时，都会产生断开连接的过程。LAC 和 LNS 任何一端都可主动发起断开连接的请求，连接断开后，该通道上的所有控制连接与会话连接也将被清除；当有新用户拨入时，还可重新建立连接。

这些配置在 LNS 端为可选配置。

请在用户视图下进行下列配置。

表2-33 强制断开连接

操作	命令
强制断开一个隧道连接	**reset l2tp tunnel** { *remote-name* | *tunnel-id* }
强制断开一个会话连接	**reset l2tp session session-id** *session-id*
强制断开该用户的连接	**reset l2tp user user-name** *user-name*

2.3.16 开启或关闭流控功能

该配置任务可以开启或关闭 L2TP 简单的通道流控功能，达到流控目的。

这些配置在 LNS 侧为可选配置。

请在 L2TP 组视图下进行下列配置。

表2-34 开启或关闭流控功能

操作	命令
开启流控功能	**tunnel flow-control**
关闭流控功能	**undo tunnel flow-control**

缺省情况下，关闭通道流控功能。

2.4 L2TP 显示和调试

在完成上述配置后，在所有视图下执行 **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 **debugging** 命令可对 L2TP 进行调试。

表2-35 L2TP 的显示和调试

操作	命令
显示当前的 L2TP 用户的信息	**display l2tp user**
显示当前的 L2TP 通道的信息	**display l2tp tunnel**
显示当前的 L2TP 会话的信息	**display l2tp session**
打开所有的 L2TP 调试信息开关	**debugging l2tp all**
打开控制报文调试开关	**debugging l2tp control**
打开 PPP 报文内容的调试开关	**debugging l2tp dump**
打开 L2TP 差错信息的调试开关	**debugging l2tp error**
打开 L2TP 的事件调试信息开关	**debugging l2tp event**

操作	命令
打开隐藏 AVP 的调试信息开关	**debugging l2tp hidden**
打开 L2TP 数据报文调试开关	**debugging l2tp payload**
打开 L2TP 时间戳信息调试开关	**debugging l2tp time-stamp**

2.5 L2TP 典型配置举例

L2TP 的呼叫可以由 NAS（网络接入服务器）主动发起，也可以由客户端发起。下面将分别针对这两种情况举例说明。

2.5.1 NAS-Initialized VPN

1. 组网需求

VPN 用户访问公司总部过程如下：

- 用户以普通的上网方式进行拨号上网。
- 在接入服务器（NAS）处对此用户进行验证，发现是 VPN 用户，则由接入服务器向 LNS 发起隧道连接的请求。
- 在接入服务器与 LNS 隧道建立后，接入服务器把与 VPN 用户已经协商的内容作为报文内容传给 LNS。
- LNS 再根据预协商的内容决定是否接受此连接。
- 用户与公司总部间的通信都通过接入服务器与 LNS 之间的隧道进行传输。

2. 组网图

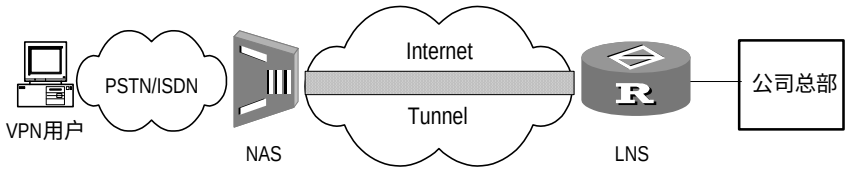

图2-6 NAS-Initialized VPN 组网图

3. 配置步骤

(1) 用户侧的配置

在用户侧，在拨号网络窗口中输入 VPN 用户名 vpdnuser，口令 Hello，拨入号码为 170。在拨号后弹出的拨号终端窗口中输入 RADIUS 验证的用户名 username 和口令 userpass。

(2) NAS 侧的配置

（本例中以 Quidway A8010 接入服务器作为 LAC 侧设备）

在 A8010 上配置拨入号码为 170。

在 RADIUS 服务器上设置一个用户名为 username、口令为 userpass 的 VPN 用户，并设置相应的 LNS 侧设备的 IP 地址（本例中 LNS 侧与通道相连接的串口的 IP 地址为 202.38.160.2）。

将本端的设备名称定义为 A8010，需要进行通道验证，通道验证密码为 quidway。

(3) 路由器（LNS 侧）的配置

设置用户名及口令（应与用户侧的设置一致）。

```
[Quidway] local-user vpdnuser
[Quidway-luser-vpdnuser] password simple Hello
```

对 VPN 用户采用本地验证。

```
[Quidway] domain system
[Quidway-isp-system ] scheme local
[Quidway-isp-system ] ip pool 1 192.168.0.2 192.168.0.100
```

启用 L2TP 服务，并设置一个 L2TP 组。

```
[Quidway] l2tp enable
[Quidway] l2tp-group 1
```

配置虚模板 Virtual-Template 的相关信息。

```
[Quidway] interface virtual-template 1
[Quidway-virtual-template1] ip address 192.168.0.1 255.255.255.0
[Quidway-virtual-template1] ppp authentication-mode chap system
[Quidway-virtual-template1] remote address pool 1
```

配置 LNS 侧本端名称及接收的通道对端名称。

```
[Quidway] l2tp-group 1
[Quidway-l2tp1] tunnel name LNS
[Quidway-l2tp1] allow l2tp virtual-template 1 remote A8010
```

启用通道验证并设置通道验证密码。

```
[Quidway-l2tp1] tunnel authentication
[Quidway-l2tp1] tunnel password simple quidway
```

2.5.2 Client-Initialized VPN

1. 组网需求

VPN 用户访问公司总部过程如下：

用户首先连接 Internet，之后，直接由用户向 LNS 发起 Tunnel 连接的请求。

在 LNS 接受此连接请求之后，VPN 用户与 LNS 之间就建立了一条虚拟的 Tunnel。

用户与公司总部间的通信都通过 VPN 用户与 LNS 之间的 Tunnel 进行传输。

2. 组网图

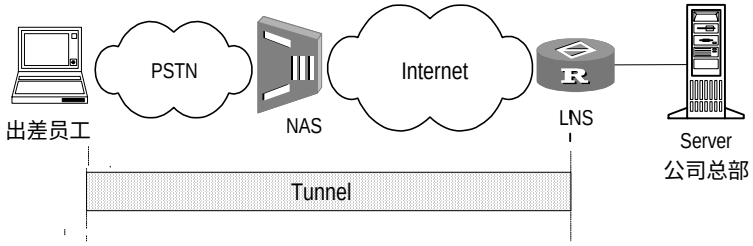

图2-7 Client-Initialized VPN 组网图

3. 配置步骤

(1) 用户侧的配置

在用户侧主机上必须装有 L2TP 的客户端软件，如 WinVPN Client，并且用户通过拨号方式连接到 Internet。然后再进行如下配置（设置的过程与相应的客户端软件有关，以下为设置的内容）：

在用户侧设置 VPN 用户名为 vpdnuser，口令为 Hello。

将 LNS 的 IP 地址设为路由器的 Internet 接口地址（本例中 LNS 侧与通道相连接的串口的 IP 地址为 202.38.160.2）。

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，进行通道验证，通道的密码为：quidway。

(2) 路由器（LNS 侧）的配置

设置用户名及口令（应与用户侧的设置一致）。

```
[Quidway] local-user vpdnuser
[Quidway-luser- vpdnuser] password simple Hello
```

对 VPN 用户采用本地验证。

```
[Quidway] domain system
[Quidway-isp-system ] scheme local
[Quidway-isp-system ] ip pool 1 192.168.0.2 192.168.0.100
```

启用 L2TP 服务，并设置一个 L2TP 组。

```
[Quidway] l2tp enable
[Quidway] l2tp-group 1
```

配置虚模板 Virtual-Template 的相关信息。

```
[Quidway] interface virtual-template 1
[Quidway-virtual-template1] ip address 192.168.0.1 255.255.255.0
[Quidway-virtual-template1] ppp authentication-mode chap system
[Quidway-virtual-template1] remote address pool 1
```

配置 LNS 侧本端名称及接收的通道对端名称。

```
[Quidway] l2tp-group 1
[Quidway-l2tp1] tunnel name LNS
[Quidway-l2tp1] allow l2tp virtual-template 1 remote vpdnuser
```

启用通道验证并设置通道验证密码。

```
[Quidway-l2tp1] tunnel authentication
[Quidway-l2tp1] tunnel password simple quidway
```

2.5.3 单用户通过路由器与总部互联

1. 组网需求

用户需要与总部进行通讯，而总部网络的地址采用的是私有地址，如 10.8.0.0 网络，则该用户将无法通过 Internet 直接访问内部的服务器。通过建立 VPN，用户就可以访问内部网络的数据。

2. 组网图

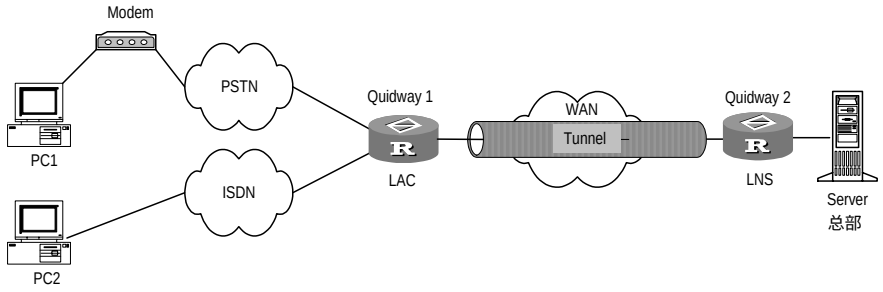

图2-8 单用户与总部互联示意图

3. 配置步骤

(1) 用户侧的配置

建一拨号网络，号码为 Quidway1 路由器的接入号码；接收由 LNS 服务器端分配的地址。

在弹出的拨号终端窗口中输入用户名 vpdnuser@huawei.com，口令为 Hello（此用户名与口令已在公司 LNS 中注册）。

(2) 路由器 Quidway1（LAC 侧）的配置

（本例中 LAC 侧的 Serial1/0/0 串口是用户接入接口，Serial1/0/0 串口的 IP 地址为 202.38.160.1，LNS 侧与通道相连接的串口 IP 地址为 202.38.160.2）。

设置用户名及口令。

```
[Quidway1] local-user vpdnuser@huawei.com
[Quidway1-luser- vpdnuser@huawei.com]password simple Hello
```

在 Serial1/0/0 接口上配置 IP 地址。

```
[Quidway1] interface serial 1/0/0
[Quidway1-Serial1/0/0] ip address 202.38.160.1 255.255.255.0
[Quidway1-Serial1/0/0] ppp authentication-mode chap domain huawei.com
```

配置 huawei.com 域用户采用本地验证。

```
[Quidway1] domain huawei.com
[Quidway1-isp- huawei.com] scheme local
```

设置一个 L2TP 组并配置相关属性。

```
[Quidway1] l2tp enable
[Quidway1] l2tp-group 1
[Quidway1-l2tp1] tunnel name LAC
[Quidway1-l2tp1] start l2tp ip 202.38.160.2 domain huawei.com
```

启用通道验证并设置通道验证密码。

```
[Quidway1-l2tp1] tunnel authentication
[Quidway1-l2tp1] tunnel password simple quidway
```

搜索的顺序为先根据域名查找，再根据被叫号码查找。

```
[Quidway1] l2tp match-order domain-dnis
```

(3) 路由器 Quidway2（LNS 侧）的配置

设置用户名及口令（与 LAC 侧的用户名与口令一致）。

```
[Quidway2] local-user vpdnuser@huawei.com
[Quidway2-luser] password simple Hello
```

配置虚模板 Virtual-Template 1。

```
[Quidway2] interface virtual-template 1
[Quidway2-virtual-template1] ip address 192.168.0.1 255.255.255.0
[Quidway2-virtual-template1] ppp authentication-mode chap domain huawei.com
```

配置域用户及本地认证方案。

```
[Quidway2] domain huawei.com
[Quidway2-isp-huawei.com] scheme local
[Quidway2-isp-huawei.com] ip pool 1 192.168.0.2 192.168.0.100
```

设置一个 L2TP 组并配置相关属性。

```
[Quidway2] l2tp enable
[Quidway2] l2tp-group 1
[Quidway2-l2tp1] tunnel name LNS
[Quidway2-l2tp1] allow l2tp virtual-template 1 remote LAC
```

启用通道验证，并设置通道验证密码为 quidway。

```
[Quidway2-l2tp1] tunnel authentication
[Quidway2-l2tp1] tunnel password simple quidway
```

强制进行本端 CHAP 验证。

```
[Quidway2-l2tp1] mandatory-chap
```

2.5.4 L2TP 多实例组网应用

1. 组网需求

多个企业共用一个 LNS，不同的企业用户需要与自己的总部进行通讯，网络的地址采用的是私有地址，如 10.8.0.0 网络，一般情况下，用户无法通过 Internet 直接访问企业内部的服务器。通过建立 VPN 并支持多实例，用户就可以访问自己企业内部网络的数据。

2. 组网图

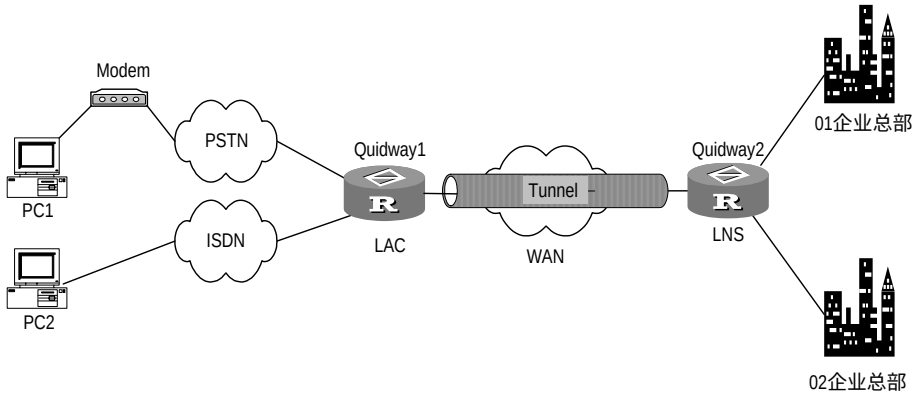

图2-9 L2TP 支持多实例组网图

3. 配置步骤

01 企业总部域名假定为 263.net，PC1 为 01 企业用户；

02 企业总部域名假定为 163.net，PC2 为 02 企业用户。

(1) 用户侧的配置

建一拨号网络，号码为 Quidway1 路由器的接入号码；接收由 LNS 服务器端分配的地址。

对于 PC1 而言，在弹出的拨号终端窗口中输入用户名 vpdn@263.net，口令为 11111（此用户名与口令已在 LNS 中注册）。

对于 PC2 而言，在弹出的拨号终端窗口中输入用户名 vpdn@163.net，口令为 22222（此用户名与口令已在 LNS 中注册）。

(2) 路由器 Quidway1（LAC 侧）的配置

（本例中 LAC 侧的 Serial1/0/0 串口是用户接入接口，Serial1/0/0 串口的 IP 地址为 202.38.160.1，LNS 侧与通道相连接的串口 IP 地址为 202.38.160.2）。

设置用户名及口令。

```
<Quidway1> system-view
```

```
[Quidway1] local-user vpdn@263.net
[Quidway1-luser-vpdn@263.net]password simple 11111
[Quidway1] local-user vpdn@163.net
[Quidway1-luser-vpdn@163.net]password simple 22222
```

配置域用户采用本地认证。

```
[Quidway1] domain vpdn@263.net
[Quidway1-isp-vpdn@263.net] scheme local
[Quidway1] domain vpdn@163.net
[Quidway1-isp-vpdn@163.net] scheme local
```

在拨号用户的接入接口上启动 CHAP 认证。

在 Serial1/0/0 接口上配置 IP 地址。

```
[Quidway1] interface serial 1/0/0
[Quidway1-Serial1/0/0] ip address 202.38.160.1 255.255.255.0
[Quidway1-Serial1/0/0] ppp authentication-mode chap domain vpdn@263.net
[Quidway1-Serial1/0/0] ppp authentication-mode chap domain vpdn@163.net
```

设置两个 L2TP 组并配置相关属性。

```
[Quidway1-Serial1/0/0] quit
[Quidway1] l2tp enable
[Quidway1] l2tp-group 1
[Quidway1-l2tp1] tunnel name LAC
[Quidway1-l2tp1] start l2tp ip 202.38.160.2 domain 263.net
[Quidway1-l2tp1] l2tp-group 2
[Quidway1-l2tp2] tunnel name LAC
[Quidway1-l2tp2] start l2tp ip 202.38.160.2 domain 163.net
```

启用通道验证并设置通道验证密码。

```
[Quidway1-l2tp2] tunnel authentication
[Quidway1-l2tp2] tunnel password simple 12345
[Quidway1-l2tp2] l2tp-group 1
[Quidway1-l2tp1] tunnel authentication
[Quidway1-l2tp1] tunnel password simple 12345
```

搜索的顺序为先根据域名查找，再根据被叫号码查找。

```
[Quidway1] l2tp match-order domain-dnis
```

(3) 路由器 Quidway2（LNS 侧）的配置

```
<Quidway2> system-view
[Quidway2] l2tp enable
[Quidway2] l2tpmoreexam enable
[Quidway2] l2tp match-order domain
[Quidway2] aaa enable
```

创建两个用户名及口令。

```
[Quidway2] local-user vpdn@263.net
[Quidway2-iuser-vpdn@263.net]password simple 12345
[Quidway2-iuser-vpdn@263.net] ip pool 1 202.38.160.10 202.38.160.100
[Quidway2] local-user vpdn@163.net
[Quidway2-iuser-vpdn@163.net]password simple 12345
[Quidway2-iuser-vpdn@163.net]ip pool 2 202.38.160.10 202.38.160.100
```

创建两个 vpn-instance。

```
[Quidway2] ip vpn-instance vpn-instance1
[Quidway2–vpn-instance] route-distinguisher 100:1
[Quidway2–vpn-instance] ip vpn-instance vpn-instance2
[Quidway2–vpn-instance] route-distinguisher 100:2
```

配置与 01 企业相连的 Ethernet 接口，绑定 vpn-instance1。

```
[Quidway2-vpn-instance] quit
[Quidway2] interface Ethernet2/0/0
[Quidway2-Ethernet2/0/0] ip binding vpn-instance vpn-instance1
[Quidway2-Ethernet2/0/0] ip address 202.38.160.3 255.255.255.0
```

配置与 02 企业相连的 Ethernet 接口，绑定 vpn-instance2。

```
[Quidway2-Ethernet2/0/0] interface Ethernet3/0/0
[Quidway2-Ethernet3/0/0] ip binding vpn-instance vpn-instance2
[Quidway2-Ethernet3/0/0] ip address 202.38.160.4 255.255.255.0
```

创建两个相应的 virtual template，分别与 vpn-instance1、vpn-instance2 绑定。

```
[Quidway2-Ethernet3/0/0] quit
[Quidway2] interface virtual-template 1
[Quidway2-Virtual-Template1] ip binding vpn-instance vpn-instance1
[Quidway2-Virtual-Template1] ip address 202.38.160.5 255.255.255.0
[Quidway2-Virtual-Template1] ppp authentication-mode pap
[Quidway2-Virtual-Template1] interface virtual-template 2
[Quidway2-Virtual-Template2] ip binding vpn-instance vpn-instance2
[Quidway2-Virtual-Template2] ip address 202.38.160.6 255.255.255.0
[Quidway2-Virtual-Template2] ppp authentication pap
```

创建两个相应的 L2TP-group 组

```
[Quidway2-Virtual-Template2] quit
[Quidway2] l2tp-group 3
[Quidway2-l2tp3] tunnel name LNS
[Quidway2-l2tp3] tunnel authentication
[Quidway2-l2tp3] allow l2tp virtual-template 1 remote LAC domain 263.net
[Quidway2-l2tp3] tunnel password simple 12345
[Quidway2-l2tp3] l2tp-group 4
[Quidway2-l2tp4] tunnel name LNS
[Quidway2-l2tp4] tunnel authentication
```

```
[Quidway2-l2tp4] allow l2tp virtual-template 2 remote LAC domain 163.net
[Quidway2-l2tp4] tunnel password simple 12345
```

上述配置中，如果 LNS 端需要采用 Redius 验证，请修改 AAA 配置即可。

2.5.5 LAC 作为客户端典型应用

1. 组网需求

使用 LAC 路由器同时作为 L2TP 客户端，与 LNS 建立常连接。并将所有私有网络的数据转发给 LNS。

2. 组网图

图2-10 LAC 作为客户端应用组网图

3. 配置步骤

📖 说明：

本例假设公网地址和路由都已正确配置。此处只说明了 VPN 相关配置。

---

(1) LAC 路由器的典型配置

设置用户名及口令。

```
[RouterA] local-user vpdnuser
[RouterA-luser-vpdnuser] password simple Hello
[RouterA-luser-vpdnuser] service-type ppp
[RouterA-luser-vpdnuser] quit
```

启用 L2TP 服务，并设置一个 L2TP 组。

```
[RouterA] l2tp enable
[RouterA] l2tp-group 1
```

配置 LAC 侧本端名称，配置对端 LNS 的 IP 地址。

```
[RouterA-l2tp1] tunnel name LAC
[RouterA-l2tp1] start l2tp ip 3.3.3.2 fullusername vpdnuser
```

启用通道验证并设置通道验证密码。

```
[RouterA-l2tp1] tunnel authentication
[RouterA-l2tp1] tunnel password simple quidway
[RouterA-l2tp1] quit
```

配置虚模板 Virtual-Template 的相关信息。

```
[RouterA] interface virtual-template 1
[RouterA-virtual-template1] ip address ppp-negotiate
[RouterA-virtual-template1] ppp pap local-user vpdnuser password simple Hello
[RouterA-virtual-template1] ppp authentication-mode pap
[RouterA-virtual-template1] quit
```

配置私网路由。

```
[RouterA] ip route-static 10.1.0.0 16 virtual-template 1
```

(2) LNS 路由器的典型配置

设置用户名及口令。

```
[RouterB] local-user vpdnuser
[RouterB-luser-vpdnuser] password simple Hello
[RouterB-luser-vpdnuser] service-type ppp
```

启用 L2TP 服务，并设置一个 L2TP 组。

```
[RouterB] l2tp enable
[RouterB] l2tp-group 1
```

配置虚模板 Virtual-Template 的相关信息。

```
[RouterB] interface virtual-template 1
[RouterB-virtual-template1] ip address 192.168.0.2 255.255.255.0
[RouterB-virtual-template1] ppp authentication-mode pap
[RouterB-virtual-template1] quit
```

配置 LNS 侧本端名称及接收的通道对端名称。

```
[RouterB] l2tp-group 1
[RouterB-l2tp1] tunnel name LNS
[RouterB-l2tp1] allow l2tp virtual-template 1 remote LAC
```

启用通道验证并设置通道验证密码。

```
[RouterB-l2tp1] tunnel authentication
[RouterB-l2tp1] tunnel password simple quidway
[RouterB-l2tp1] quit
```

配置私网路由。

```
[RouterB] ip route-static 10.2.0.0 16 virtual-template1
```

(3) 启动 L2TP 连接

在 RouteA 的虚模板接口视图下执行启动 L2TP 连接命令

```
[RouterA] interface virtual-template 1
[RouterA-virtual-template1] l2tp-auto-client enable
```

📖 说明：

LAC 和 LNS 连接的私网主机应分别以 LAC 和 LNS 为网关。

2.5.6 复杂的组网情况

Quidway 路由器支持同时作为 LAC 及 LNS，并支持同时有多路用户呼入；只要内存及线路不受限制，L2TP 可以同时接收和发起多个呼叫。这些复杂组网的需求及配置可以综合参考以上的几种组网情况，综合应用。

特别需要注意的是静态路由的配置，许多应用是依靠路由来发起的。

2.6 L2TP 故障诊断与排错

VPN 创建连接的过程比较复杂，这里就几种常见的情况进行分析。在进行 VPN 排错之前，请先确认 LAC 与 LNS 都已在公共网上，并实现正确连通。

故障之一：用户登录失败

故障排除：用户登录失败主要有以下几种原因。

- Tunnel 建立失败，Tunnel 不能建立的原因有：

(1) 在 LAC 端，LNS 的地址设置不正确。

(2) LNS（通常为路由器）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。

(3) Tunnel 验证不通过，如果配置了验证，应该保证双方的隧道密码一致。

(4) 如果是本端强制挂断了连接，而由于网络传输等原因，对端还没有收到相应的 Disconnect 报文，此时立即发起了一个隧道连接，会连不上，因为对方必须相隔一定的时间才能侦测到链路被挂断。

- PPP 协商不通过，可能原因有：

(1) 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。

(2) LNS 端不能分配地址，比如地址池设置的较小，或没有进行设置。

(3) 密码验证类型不一致。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。

故障之二：数据传输失败，在建立连接后数据不能传输，如 Ping 不通对端。

故障排除：可能有如下原因。

- 用户设置的地址有误：一般情况下，由 LNS 分配地址，而用户也可以指定自己的地址。如果指定的地址和 LNS 所要分配的地址不属于同一个网段，就会发生这种情况，建议由 LNS 统一分配地址。

- 网络拥挤：Internet 主干网产生拥挤，丢包现象严重。L2TP 是基于 UDP（用户数据报文）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。

第3章 GRE 协议配置

3.1 GRE 协议简介

1. 协议简介

GRE（Generic Routing Encapsulation，通用路由封装）协议是对某些网络层协议（如 IP 和 IPX）的数据报进行封装，使这些被封装的数据报能够在另一个网络层协议（如 IP）中传输。GRE 是 VPN（Virtual Private Network）的第三层隧道协议，在协议层之间采用了一种被称之为 Tunnel（隧道）的技术。Tunnel 是一个虚拟的点对点的连接，在实际中可以看成仅支持点对点连接的虚拟接口，这个接口提供了一条通路使封装的数据报能够在这个通路上传输，并且在一个 Tunnel 的两端分别对数据报进行封装及解封装。

一个报文要想在 Tunnel 中传输，必须要经过加封装与解封装两个过程，下面以图 3-1的网络为例说明这两个过程：

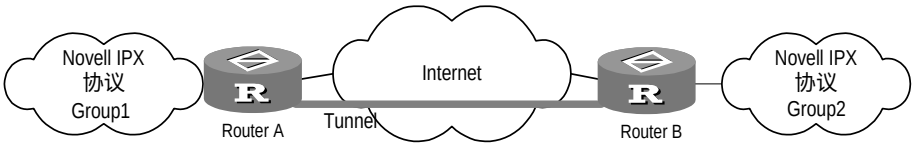

图3-1 IPX 网络通过 GRE 隧道互连

(1) 加封装过程

连接 Novell group1 的接口收到 IPX 数据报后首先交由 IPX 协议处理，IPX 协议检查 IPX 报头中的目的地址域来确定如何路由此包。若报文的目的地址被发现要路由经过网号为 1f 的网络（Tunnel 的虚拟网号），则将此报文发给网号为 1f 的 tunnel 端口。Tunnel 口收到此包后进行 GRE 封装，封装完成后交给 IP 模块处理，在封装 IP 报文头后，根据此包的目的地址及路由表交由相应的网络接口处理。

(2) 解封装的过程

解封装过程和加封装的过程相反。从 Tunnel 接口收到的 IP 报文，通过检查目的地址，当发现目的地就是此路由器时，系统剥掉此报文的 IP 报头，交给 GRE 协议模块处理（进行检验密钥、检查校验和及报文的序列号等）；GRE 协议模块完成相应的处理后，剥掉 GRE 报头，再交由 IPX 协议模块处理，IPX 协议模块象对待一般数据报一样对此数据报进行处理。

系统收到一个需要封装和路由的数据报，称之为净荷（Payload），这个净荷首先被加上 GRE 封装，成为 GRE 报文；再被封装在 IP 报文中，这样就可完全由 IP 层负

责此报文的向前传输（Forwarded）。人们常把这个负责向前传输 IP 协议称为传输协议（Delivery Protocol 或者 Transport Protocol）。

封装好的报文的形式如下图所示：

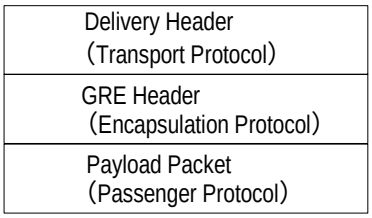

图3-2 封装好的 Tunnel 报文格式

举例来说，一个封装在 IP Tunnel 中的 IPX 传输报文的格式如下：

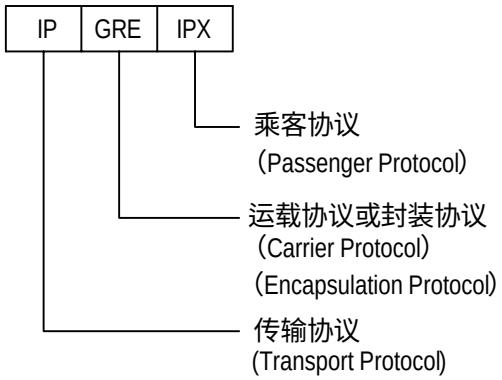

图3-3 Tunnel 中传输报文的格式

2. 应用范围

GRE 主要能实现以下几种服务类型：

(1) 多协议的本地网通过单一协议的骨干网传输

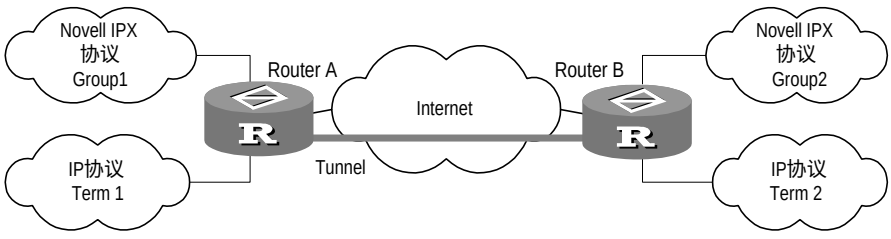

图3-4 多协议本地网通过单一协议骨干网传输

上图中，Group1 和 Group2 是运行 Novell IPX 协议的本地网，Term1 和 Term2 是运行 IP 协议的本地网。通过在 Router A 和 Router B 之间采用 GRE 协议封装的隧道（Tunnel），Group1 和 Group2、Team1 和 Team2 可以互不影响地进行通信。

(2) 扩大了步跳数受限协议（如 IPX）的网络的工作范围

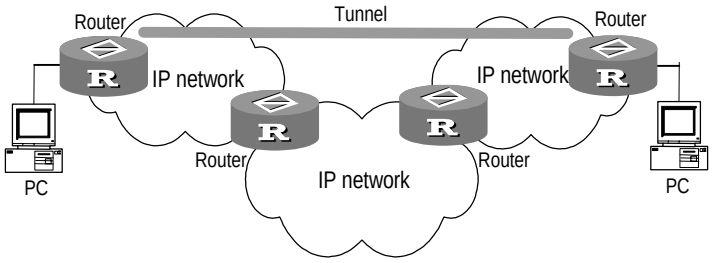

图3-5 扩大网络工作范围

若上图中的两台终端之间的步跳数超过 15，它们将无法通信。而通过在网络中使用隧道（Tunnel）可以隐藏一部分步跳，从而扩大网络的工作范围。

(3) 将一些不能连续的子网连接起来，用于组建 VPN

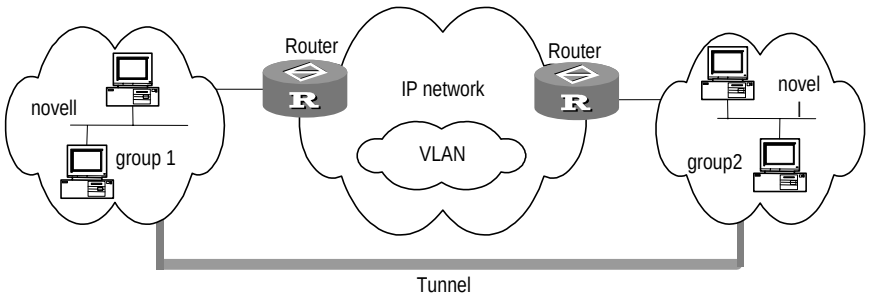

图3-6 Tunnel 连接不连续子网

运行 Novell IPX 协议的两个子网 group1 和 group2 分别在不同的城市，通过使用隧道可以实现跨越广域网的 VPN。

(4) 与 IPSec 结合使用

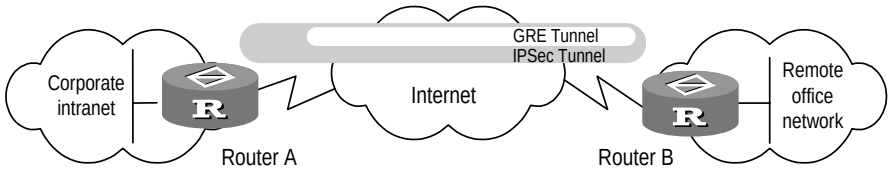

图3-7 GRE-IPSec 隧道应用

对于诸如路由协议、语音、视频等数据先进行 GRE 封装，然后再对封装后的报文进行 IPSec 的加密处理。

另外，GRE 还支持由用户选择记录 Tunnel 接口的识别关键字，和对封装的报文进行端到端校验。

由于 GRE 收发双方加封装、解封装处理以及由于封装造成的数据量增加等因素的影响，这就导致使用 GRE 会造成路由器数据转发效率有一定程度的下降。

3.2 GRE 配置

在各项配置中，必须先创建虚拟 Tunnel 接口，才能在虚拟 Tunnel 接口上进行其它功能特性的配置。当删除虚拟 Tunnel 接口后，该接口上的所有配置也将被删除。

GRE 主要配置包括：

- 创建虚拟 Tunnel 接口（必选）
- 设置 Tunnel 接口报文的封装模式（可选）
- 指定 Tunnel 的源端（必选）
- 指定 Tunnel 的目的端（必选）
- 设置 Tunnel 接口的网络地址（必选）
- 设置 Tunnel 两端进行端到端校验（可选）
- 设置 Tunnel 接口的识别关键字（可选）
- 配置通过 Tunnel 的路由（可选）

3.2.1 创建虚拟 Tunnel 接口

创建虚拟 Tunnel 接口，从而在该接口上进行 GRE 其它参数的配置。这些配置在 Tunnel 两端必须配置。

请在系统视图下进行下列配置。

表3-1 创建虚拟 Tunnel 接口

操作	命令
创建虚拟 Tunnel 接口	**interface tunnel** *number*
删除虚拟 Tunnel 接口	**undo interface tunnel** *number*

缺省情况下，不创建虚拟 Tunnel 接口。

number 为设定的接口号，范围 0～1023，但实际可建的 Tunnel 数目将受到接口总数及内存状况的限制。

3.2.2 设置 Tunnel 接口报文的封装模式

设置 Tunnel 接口的封装协议和传输协议。这些配置在 Tunnel 两端为可选配置，如果配置则必须确保 Tunnel 两端的封装模式相同。

请在 Tunnel 视图下进行下列配置。

表3-2 设置 Tunnel 接口报文的封装模式

操作	命令
设置 Tunnel 接口报文的封装模式	**tunnel-protocol gre**
删除 Tunnel 接口报文的封装模式	**undo tunnel-protocol**

缺省情况下，Tunnel 接口报文的封装模式为 GRE。

3.2.3 指定 Tunnel 的源端

在创建 Tunnel 接口后，还要指明 Tunnel 通道的源端地址，即发出 GRE 报文的实际物理接口地址。Tunnel 的源端地址与目的端地址唯一标识了一个通道。这些配置在 Tunnel 两端必须配置，且两端地址互为源地址和目的地址。

请在 Tunnel 接口视图下进行下列配置。

表3-3 设置 Tunnel 接口的源端地址

操作	命令
设置 Tunnel 接口的源端地址	**source** { *ip-addr* | *interface-type interface-num* }
删除 Tunnel 接口的源端地址	**undo source**

📖 说明：

- 不能对两个或两个以上使用同种封装协议的 Tunnel 接口配置完全相同的源地址和目的地址。
- 使用命令 **source** 设置的是实际的物理接口地址或实际物理接口，为支持动态路由协议，还需要设置 Tunnel 接口的网络地址。在 Tunnel 接口视图下通过命令 **ip address** 可完成这一设置。

3.2.4 指定 Tunnel 的目的端

在创建 Tunnel 接口后，还要指明 Tunnel 通道的目的端地址，即接收 GRE 报文的实际物理接口的 IP 地址。Tunnel 的源端地址与目的端地址唯一标识了一个通道。这些配置在 Tunnel 两端必须配置，且两端地址互为源地址和目的地址。

请在 Tunnel 接口视图下进行下列配置。

表3-4 设置 Tunnel 接口的目的端地址

操作	命令
设置 Tunnel 接口的目的端地址	**destination** *ip-addr*
删除 Tunnel 接口的目的端地址	**undo destination**

说明：

使用命令 **destination** 设置的是实际的物理接口的 IP 地址，为支持动态路由协议，还需要设置 tunnel 接口的网络地址。

3.2.5 设置 Tunnel 接口的网络地址

Tunnel 接口的网络地址可以不是申请得到的网络地址。用户设置通道两端的网络地址应该位于同一网段上。这些配置在 Tunnel 两端都必须配置，并且确保地址在同一网段。

请在 Tunnel 接口视图下进行下列设置。

表3-5 设置 Tunnel 接口的网络地址

操作	命令
设置 Tunnel 接口的 IP 地址	**ip address** *ip-addr mask*
删除 Tunnel 接口的 IP 地址	**undo ip address**

缺省情况下，未设置 Tunnel 接口的网络地址。

3.2.6 设置 Tunnel 两端进行端到端校验

在 RFC1701 中规定：若 GRE 报文头中的 Checksum 位置位，则校验和有效。发送方将根据 GRE 头及 payload 信息计算校验和，并将包含校验和的报文发送给对端。接收方对接收到的报文计算校验和，并与报文中的校验和比较，如果一致则对报文进一步处理，否则丢弃。

隧道两端可以根据实际应用需要，配置校验和或禁止校验和。如果本端配置了校验和而对端没有配置，则本端将不会对接收到的报文进行校验和检查，但对发送的报文计算校验和；相反，如果本端没有配置校验和而对端已配置，则本端将对从对端发来的报文进行校验和检查，但对发送的报文不计算校验和。

请在 Tunnel 接口视图下进行下列配置。

表3-6 设置 Tunnel 两端进行端到端校验

操作	命令
设置 Tunnel 两端进行端到端校验	**gre checksum**
禁止 Tunnel 两端进行端到端校验	**undo gre checksum**

缺省情况下，禁止 Tunnel 两端进行端到端校验。

3.2.7 设置 Tunnel 接口的识别关键字

在 RFC1701 中规定：若 GRE 报文头中的 KEY 字段置位，则收发双方将进行通道识别关键字的验证，只有 Tunnel 两端设置的识别关键字完全一致时才能通过验证，否则将报文丢弃。

请在 Tunnel 接口视图下进行配置。

表3-7 设置 Tunnel 接口的识别关键字

操作	命令
设置 Tunnel 接口的识别关键字	**gre key** *key-number*
删除 Tunnel 接口的识别关键字	**undo gre key**

key-number 可取值 0～4294967295 之间的整数。

缺省情况下，Tunnel 不使用 KEY。

3.2.8 配置通过 Tunnel 的路由

在源端路由器和目的端路由器上都必须存在经过 Tunnel 转发的路由，这样需要进行 GRE 封装的报文才能正确转发。可以配置静态路由，也可以配置动态路由。

1. 静态路由配置

可以手工配置一条到达目的地址（不是 Tunnel 的目的端地址，而是未进行 GRE 封装的报文的目的地址）的路由，下一跳是对端 Tunnel 接口的地址。在 Tunnel 的两端都要进行此项配置。配置的详细情况请参见本手册的“ 静态路由配置 ”章节，配置命令的详细解释请参见相应的命令手册。

2. 动态路由配置

如果路由器上运行了动态路由协议，只需在 Tunnel 接口上和与私网相连的路由器接口上使能该动态路由协议即可，在 Tunnel 的两端都必须进行此项配置。配置的详细情况请参见本手册的各个动态路由协议配置章节，配置命令的详细解释请参见相应的命令手册。

3.2.9 配置 keepalive 功能

请在 Tunnel 接口视图下进行配置。

表3-8 配置 keepalive 功能

操作	命令
使能 GRE 的 keepalive 功能	**keepalive** *interval times*
关闭 GRE 的 keepalive 功能	**undo keepalive** [*seconds*] [*times*]

缺省情况下，不启用 GRE 的 keepalive 功能。

seconds 缺省为 10 秒。*times* 缺省为 3 次。

3.3 GRE 显示和调试

在完成上述配置后，在所有视图下执行 **display** 命令可以显示配置后 GRE 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 **debugging** 命令可对 GRE 进行调试。GRE 除了提供针对 Tunnel 的查询和调试命令，还提供了查询 GRE 隧道的命令。

表3-9 GRE 的显示和调试

操作	命令
显示 Tunnel 接口的工作状态	**display interface tunnel** *number*
打开 Tunnel 调试信息	**debugging tunnel**

3.4 GRE 典型配置举例

1. 组网需求

运行 IP 协议的两个子网 Group1 和 Group2，通过在路由器 Quidway1 和路由器 Quidway2 之间使用三层隧道协议 GRE 实现互联。

2. 组网图

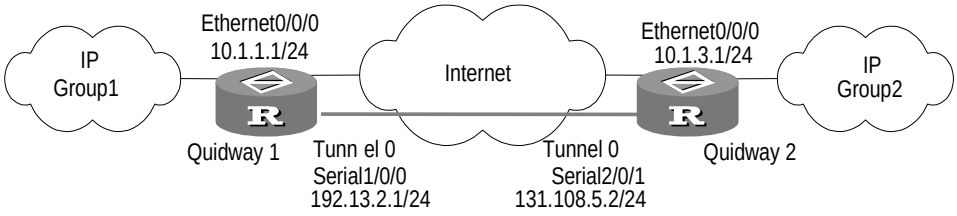

图3-8 GRE 应用组网图

3. 配置步骤

(1) 配置路由器 Quidway1

配置接口 Ethernet0/0/0。

```
[Quidway1] interface ethernet 0/0/0
[Quidway1-Ethernet0/0/0] ip address 10.1.1.1 255.255.255.0
[Quidway1-Ethernet0/0/0] quit
```

配置接口 Serial1/0/0（隧道的实际物理接口）。

```
[Quidway1] interface serial 1/0/0
[Quidway1-Serial1/0/0] ip address 192.13.2.1 255.255.255.0
[Quidway1-Serial1/0/0] quit
```

创建 Tunnel0 接口。

```
[Quidway1] interface tunnel 0
```

配置 Tunnel0 接口的 IP 地址。

```
[Quidway1-Tunnel0] ip address 10.1.2.1 255.255.255.0
```

配置 Tunnel 封装模式。

```
[Quidway1-Tunnel0] tunnel-protocol gre
```

配置 Tunnel0 接口的源地址（Serial1/0/0 的 IP 地址）。

```
[Quidway1-Tunnel0] source 192.13.2.1
```

配置 Tunnel0 接口的目的地址（Quidway2 的 Serial2/0/1 的 IP 地址）。

```
[Quidway1-Tunnel0] destination 131.108.5.2
[Quidway1-Tunnel0] quit
```

配置从 Quidway1 经过 Tunnel0 接口到 Group2 的静态路由。

```
[Quidway1] ip route-static 10.1.3.0 255.255.255.0 tunnel 0
```

(2) 配置路由器 Quidway2

配置接口 Ethernet0/0/0。

```
[Quidway2] interface ethernet 0/0/0
[Quidway2-Ethernet0/0/0] ip address 10.1.3.1 255.255.255.0
[Quidway2-Ethernet0/0/0] quit
```

配置接口 Serial2/0/1（隧道的实际物理接口）。

```
[Quidway2] interface serial 1/0/1
[Quidway2-Serial2/0/1] ip address 131.108.5.2 255.255.255.0
[Quidway2-Serial2/0/1] quit
```

创建 Tunnel0 接口。

```
[Quidway2] interface tunnel 0
```

配置 Tunnel0 接口的 IP 地址。

```
[Quidway2-Tunnel0] ip address 10.1.2.2 255.255.255.0
```

配置 Tunnel 封装模式。

```
[Quidway2-Tunnel0] tunnel-protocol gre
```

配置 Tunnel0 接口的源地址（Serial2/0/1 的 IP 地址）。

```
[Quidway2-Tunnel0] source 131.108.5.2
```

配置 Tunnel0 接口的目的地址（Quidway1 的 Serial1/0/0 的 IP 地址）。

```
[Quidway2-Tunnel0] destination 192.13.2.1
```

```
[Quidway2-Tunnel0] quit
```

配置从 Quidway2 经过 Tunnel0 接口到 Group1 的静态路由。

```
[Quidway2] ip route-static 10.1.1.0 255.255.255.0 tunnel 0
```

3.5 GRE 故障诊断与排除

GRE 的配置相对比较简单，但要注意配置的一致性，大部分的错误都可以通过使用调试命令 **debugging tunnel** 定位。这里仅就一种错误进行分析。如图 3-9所示：

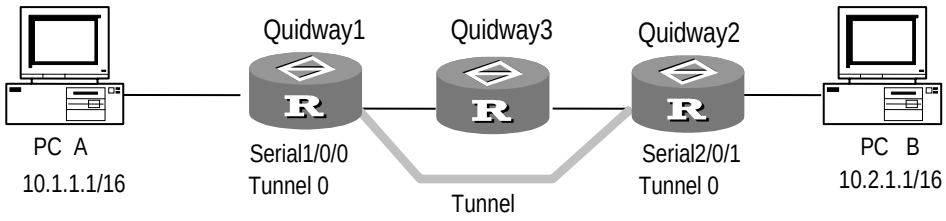

图3-9 GRE 排错示例

故障之一：Tunnel 两端接口配置正确且 Tunnel 两端可以 ping 通，但 PC A 和 PC B 之间却无法 ping 通。

故障排除：可以按照如下步骤进行。

- 在任一视图下，在 Quidway1 和 Quidway2 分别执行 **display ip routing-table** 命令，观察在 Quidway1 是否有经过 Tunnel0 接口到 10.2.0.0/16 的路由；在 Quidway2 是否有经过 Tunnel0 接口到 10.1.0.0/16 的路由。
- 如果在上一步的输出中发现缺少相应的静态路由，在系统视图下使用 **ip route-static** 命令添加。以 Quidway1 为例，配置如下：

```
[Quidway1] ip route-static 10.2.0.0 255.255.0.0 tunnel 0
```

第4章 动态 VPN

4.1 动态 VPN 简介

4.1.1 概述

在现有的 VPN 组网方案中，三层 VPN 一般采用 GRE 隧道以及 MPLS/BGP VPN 两种方式。其中 MPLS/BGP VPN 主要应用在主干转发层，GRE 隧道方式在接入层被普遍采用，但是目前的 GRE 隧道方案存在以下弊端：

- 组网及配置复杂。传统的 GRE 隧道技术采用的是点到点的隧道方案，当接入点数量为 N，且需要建立一个全联通的 VPN 时，整个网络需要手工配置 N×(N－1) / 2 个点到点的连接。
- 可维护性及可扩展性差。对于一个已经组建好的 VPN 网络，若需要增加节点或修改某个节点的配置，那么其他所有节点都必须针对这个节点修改本地配置，维护成本较高。
- 无法穿透 NAT 网关。采用传统的 GRE 方式建立隧道，如果出口有 NAPT 网关，那么就必须要一个公网地址对应一个私网地址来解决，需要大量的公网 IP 地址，这导致了 GRE 不能够应用于 NAT 网关内部。
- 无法适用于动态 IP 的情况。传统的 GRE 方式建立隧道依赖于固定的 IP 地址，根本无法为拨号用户建立 VPN。

动态 VPN（DVPN）技术提出了 NBMA 类型的隧道机制，采用了 Client 和 Server 的方式解决了传统 VPN 的以上缺陷。当多个接入设备通过骨干网将多个私网连成一个 VPN 时，同一个 VPN 的 Tunnel 之间构成 NBMA 连接，且每个接入设备针对不同 VPN 有不同的 Tunnel，一个设备可以支持多个 VPN。其特点如下：

- 不仅支持 GRE 方式建立隧道，还支持 UDP 方式的隧道，故能够穿越 NAPT 网关，解决了私网 IP 地址通过 NAPT 网关和其他路由器建立 VPN 网络的问题。
- 支持依赖动态 IP 地址构建 VPN。动态 VPN 在同一个 VPN 内部构建隧道时，只需要指定相应的 Server 的 IP 地址，并不关心自己当前使用的 IP 地址是多少，更加适应如普通拨号、xDSL 拨号等使用动态 IP 地址的组网应用。
- 支持自动建立隧道技术。动态 VPN 中的每一个节点维护着一个公网-私网地址映射表，两个节点之间的隧道完全是自动建立的。每台作为 Client 的路由器只需配置自己的相关信息，比如本地的 IP 地址、UDP 方式下使用的端口号、所

属的 VPN 和 Server 等，不需要知道其他 Client 的任何信息就可以互相通讯。不仅减少了维护管理的工作量，同时也减少了发生错误的可能性。

- 认证加密技术。动态 VPN 使用了认证、加密等技术，最大程度地保证用户数据的安全及用户网络的安全。首先，动态 VPN 提供了注册认证机制，Client 设备必须经过 Server 的认证才能加入到某个特定的动态 VPN 内，而且在 Client 之间建立隧道时也提供了相互的身份认证功能。
- 支持多个 VPN 域。动态 VPN 允许用户在一台路由器上支持多个 VPN 域。即一台路由器不仅可以属于 VPN A，也可以属于 VPN B；同一设备可以在 VPN A 中作为 Client 设备，同时还在 VPN B 中作为 Server 设备使用。大大提高了组网的灵活性，也可以更加充分的使用网络设备资源，减少了用户的投资。

4.1.2 基本网络结构

动态 VPN 采用 Client/Server 模式，对于同一个 VPN 的 N 个接入设备中，一个设置为 Server 工作方式（使用固定的公网 IP 地址），其他设置为 Client 方式，并在每一个 Client 端手工配置 Server 的公网地址。当每个 Client 到 Server 注册成功之后，各 Client 之间就自动地建立了会话通路，相当于自动实现了全连接的 VPN 隧道。

建立隧道的方式有 GRE DVPN 封装格式和 UDP DVPN 封装格式两种，当采用 UDP DVPN 封装格式时动态 VPN 可以穿过 NAT 网关建立 VPN 隧道，满足 Client 为私有 IP 地址时的需求。

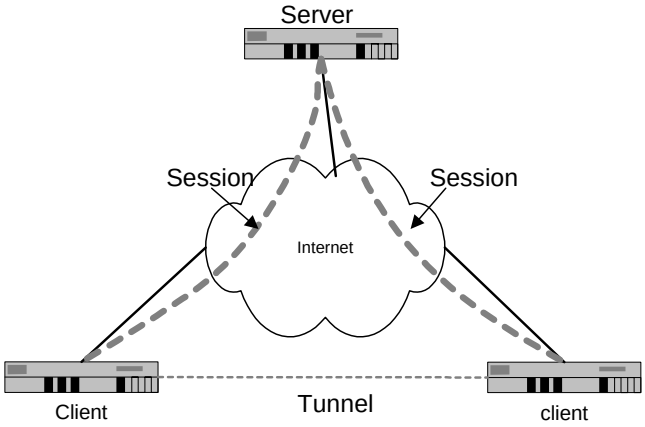

图4-1 动态 VPN 基本网络结构

4.1.3 基本原理

动态 VPN 在各个节点之间运行 DVPN 私有协议，在 Client 和 Server 端都有一张映射表，这张表是整个动态 VPN 网络的核心，表项内容包括：目的私网地址（Tunnel 接口地址），目的公网地址（WAN 接口的公网 IP 地址），目的 UDP 端口号（采用 UDP 协议时），还有会话通路状态标识等。下面对 Server 与 Client 之间的交互过程作以简单说明：

1. 注册阶段

当 Client 端配置好接口属性，指定了 Server 地址，并且接口状态 UP 之后，将向 Server 端发送注册请求报文。Server 收到注册请求报文后，根据需要在注册成功报文中反馈其他 Client 的信息，同时更新本地公网-私网地址映射表。

若此时 Server 端接收到目的地并非发往本地私网地址的数据报文，而是发往 VPN 网络中的另一个节点的报文，则需要转发该数据报文；同时向该数据报文的源节点发送下一跳重定向通告（Next Hop Redirect Notify），通知源 Client 所要到达目的地址的下一跳的相关信息。

📖 说明：

Server 端允许注册的最大节点数量缺省为 1024，该值不可配。

---

2. 会话建立阶段

Client 根据 Next Hop Redirect Notify 报文中的目的地址信息发起连接建立请求（Setup Request），这样 Client 和目的节点之间就会建立会话链接。此时数据报文将全部由源 Client 直接发送到目的 Client，不再需要通过 Server 进行转发了。

4.2 动态 VPN 的配置

动态 VPN 的配置包括两方面，一是配置 Client，二是配置 Server。

(1) Client 端的配置

Client 端的配置包括 Tunnel 接口属性配置和 dvpn-class 配置。

配置 Tunnel 接口属性包括如下步骤：

- 配置 Tunnel 接口的报文封装格式（UDP DVPN 或 GRE DVPN）
- 配置 Tunnel 接口的接口类型（配为 Client）
- 配置 Tunnel 接口所属的 VPN
- 配置 Tunnel 接口的源端
- 配置 Tunnel 接口使用的 dvpn-class 名称
- 配置 Tunnel 接口使用的 UDP 端口（若封装 UDP DVPN 格式）
- 配置各种定时器参数（可选）
- 配置 Tunnel 接口认证（可选）
- 配置 Client 向 Server 注册时的类型（可选）
- 配置一个静态 map（可选）
- 配置重定向通告、会话建链请求及会话保持的最大尝试次数（可选）

dvpn-class 视图下的命令用来配置对应 Server 的一些参数，这些参数值应与 Server 端的配置保持一致。配置的内容包括：

- 进入 dvpn-class 视图
- 配置指定 Server 的私网地址
- 配置指定 Server 的公网地址
- 配置指定 Server 使用的 UDP 端口号

(2) Server 端的配置

Server 端仅配置 Tunnel 接口属性即可，具体配置步骤如下：

- 配置 Tunnel 接口的报文封装格式（UDP DVPN 或 GRE DVPN）
- 配置 Tunnel 接口的接口类型（配为 Server）
- 配置 Tunnel 接口所属的 VPN
- 配置 Tunnel 接口的源端
- 配置 Tunnel 接口使用的 UDP 端口（若封装 UDP DVPN 格式）
- 配置各种定时器参数（可选）
- 配置 Tunnel 接口的认证（可选）
- 配置一个静态 map（可选）
- 配置重定向通告、会话建链请求及会话保持的最大尝试次数（可选）

下面从 Tunnel 接口属性配置和 dvpn-class 配置两方面进行详细说明。

4.2.1 配置 Tunnel 接口属性

1. 配置 Tunnel 接口的封装格式

在配置 DVPN 其他参数前，请务必在 Tunnel 接口上封装 DVPN，可以选择 gre dvpn 和 udp dvpn 两种封装格式。

请在 Tunnel 接口视图下进行下面配置。

表4-1 设置 Tunnel 接口报文的封装模式

操作	命令
设置 Tunnel 接口报文的封装格式	**tunnel-protocol** { **gre** | **udp** } **dvpn**

缺省情况下封装为 gre 方式。

2. 配置 Tunnel 接口的类型

Server 端应选择 **Server**，Client 端应选择 **Client**。

请在 Tunnel 接口视图下进行下面配置。

表4-2 设置 Tunnel 接口的类型

操作	命令
配置 Tunnel 接口的类型	**dvpn interface-type** { **client** | **server** }

缺省情况下为 **client** 类型。

3. 配置 Tunnel 接口所属的 VPN

本命令用来配置 Tunnel 接口所属的 VPN，属于同一 VPN 的 Tunnel 接口应配置相同的 vpn-id。

表4-3 配置 Tunnel 接口所属的 VPN

操作	命令
配置 Tunnel 接口所属的 VPN	**dvpn vpn-id** *vpn-id*
删除 Tunnel 接口所属的 VPN	**undo dvpn vpn-id**

4. 配置 Tunnel 接口的源端

Tunnel 接口的源端地址即发出报文的实际物理接口地址。Tunnel 的源端地址与目的端地址唯一标识了一个通道。这些配置在 Server 及 Client 两端必须配置，且两端地址互为源地址和目的地址。

请在 Tunnel 接口视图下进行下列配置。

表4-4 设置 Tunnel 接口的源端地址

操作	命令
设置 Tunnel 接口的源端地址	**source** { *X.X.X.X* | *interfacename* }
删除 Tunnel 接口的源端地址	**undo source**

5. 配置 Tunnel 接口使用的 dvpn-class 名称

本命令仅在 Client 端配置。在 Client 端的 dvpn-class 视图下配置好 Server 的 dvpn-class 属性，然后配置此命令引用相应的 Dvpn-class-name。

请在 Tunnel 接口视图下进行下列配置。

表4-5 配置 Tunnel 接口使用的 dvpn-class 名称

操作	命令
配置 Tunnel 接口使用的 dvpn-class 名称	**dvpn server** *dvpn-class-name*
删除 Tunnel 接口使用的 dvpn-class 名称	**undo dvpn server** *dvpn-class-name*

6. 配置 Tunnel 接口使用的 UDP 端口

本命令用来配置 Tunnel 接口所使用的 UDP 端口号，仅在 Tunnel 接口封装为 udp dvpn 时有效。

请在 Tunnel 接口视图下进行下列配置。

表4-6 配置 Tunnel 接口使用的 UDP 端口

操作	命令
配置 Tunnel 接口使用的 UDP 端口	**dvpn udp-port** *udp-port*
删除 Tunnel 接口使用的 UDP 端口	**undo dvpn udp-port**

7. 配置定时器参数

下面配置均为可选配置，一般情况下使用缺省值即可。

请在 Tunnel 接口视图下进行下列配置。

表4-7 配置定时器

操作	命令
配置 Tunnel 接口下 Map 表老化定时器。	**dvpn timer aging** *time-interval*
恢复 Tunnel 接口下 Map 表老化定时器的缺省设置。	**undo dvpn timer aging**
配置 Map 状态保持连接定时器。	**dvpn timer keepalive** *time-interval*
恢复 Map 状态保持连接定时器的缺省设置。	**undo dvpn timer keepalive**
配置下一跳重定向通告定时器。	**dvpn timer redirect** *time-interval*
恢复下一跳重定向通告定时器的缺省设置。	**undo dvpn timer redirect**
配置注册请求定时器。	**dvpn timer register** *time-interval*
恢复注册请求定时器的缺省设置。	**undo dvpn timer register**
配置会话建立请求。	**dvpn timer setup** *time-interval*
恢复会话建立请求定时器的缺省设置。	**undo dvpn timer setup**

配置 Tunnel 接口的认证

若需要配置 Tunnel 接口认证，应首先在 Server 及 Client 两端同时使能认证功能，然后在 Server 上配置 Client 的注册认证信息列表（包括 Client 的 IP 地址及 Client 的私有密钥），以便 Client 向 Server 注册时进行认证信息的匹配。最后，应分别配置 Client 的私有密钥。

请在 Tunnel 视图下进行下面配置。

(1) 使能 Tunnel 接口认证功能

表4-8 使能 Tunnel 接口认证

操作	命令
使能 Tunnel 接口的认证	**dvpn authentication enable**
关闭 Tunnel 接口认证	**undo dvpn authentication enable**

缺省情况下，没有使能 Tunnel 接口认证功能。

(2) 配置 Client 的认证信息

在 Server 上配置 Client 的认证信息，应与 Client 端的实际配置保持一致。

表4-9 配置 Client 的认证信息

操作	命令
配置 Client 的认证信息	**dvpn client private-ip** *private-ip* **key** *key-value*
删除 Client 的认证信息	**undo dvpn client private-ip** *private-ip* **key** *key-value*

缺省情况下，没有配置 Client 的认证信息。

(3) 配置密钥

在 Client 端，**dvpn key** 命令用来配置本机的私有密钥。

表4-10 配置密钥

操作	命令
配置 Client 的私有密钥	**dvpn key** *key-value*
删除 Client 的密钥	**undo dvpn key** *key-value*

缺省情况下，没有配置密钥。

8. 配置 Client 的注册类型

本命令用来配置 Client 向 Server 注册时的附加信息类型，Server 可以据此了解 Client 是否配有固定 IP 地址并明确对报文应采取的处理方式。

请在 Tunnel 接口视图下进行下面配置。

表4-11 配置 Client 的注册类型

操作	命令
配置 Client 向 Server 注册时的附加信息类型	**dvpn register-type** { **forward** | **stable** | **undistributed** | **want** | }
恢复附加信息类型的缺省设置	**undo dvpn register-type** { **forward** | **stable** | **undistributed** | **want** | }

在缺省情况下，注册的附加信息类型为不固定的公网 IP 地址，不需要 Server 向本 Client 发布信息，允许 Server 向其他节点发布本 Client 的信息，Server 不转发 Client 节点的数据报文。

9. 创建一个静态的 map

在 Client 端预先知道其他 Client 的 private-ip、public-ip、UDP dvpn 封装时的端口号的情况下，可以使用此命令来创建一个静态的 map。

表4-12 创建一个静态的 map

操作	命令
创建一个静态的 map	**dvpn map private-ip** *ip-address* **public-ip** *ip- address* [**udp-port** *port-number*]
删除一个静态的 map	**undo dvpn map private-ip** *ip-address* **public-ip** *ip- address*

缺省情况下，没有配置静态 map。

10. 配置重定向通告、会话建链请求及会话保持的最大尝试次数

本命令用来配置 Client 端重定向通告、会话建链请求及会话保持的最大尝试次数。

表4-13 配置重定向通告、会话建链请求、会话保持的最大尝试次数

操作	命令
配置 Client 端重定向通告、会话建链请求及会话保持的最大尝试次数	**dvpn retry** *retry-times*
恢复最大尝试次数的缺省设置	**undo dvpn retry**

缺省情况下，最大尝试次数为 3。

4.2.2 配置 dvpn-class

在 dvpn-class 视图下主要用来配置指定 Server 的相关信息，主要包括私网 IP 地址、公网 IP 地址、UDP 端口号等，用以 Client 与指定 Server 建立会话连接，以下配置应与 Server 端的实际配置保持一致。

1. 创建 dvpn-class 视图

请在系统视图下进行下面配置。

表4-14 创建 dvpn-class 视图

操作	命令
创建 dvpn-class 视图	**dvpn class** *dvpn-class-name*
删除 dvpn-class 视图	**undo dvpn class** *dvpn-class-name*

2. 配置 Server 端的私网 IP 地址

这里的私网 IP 地址指 Server 的 Tunnel 接口的 IP 地址。

请在 dvpn-class 视图下进行下面配置。

表4-15 配置 Server 端的私网 IP 地址

操作	命令
配置 Server 端的私网 IP 地址	**private-ip** *ip-address*
删除 Server 端的私网 IP 地址	**undo private-ip**

3. 配置 Server 端的公网 IP 地址

这里的公网 IP 地址指 Server 的 WAN 口固定配置的公有 IP 地址。

请在 dvpn-class 视图下进行下面配置。

表4-16 配置 Server 端的公网 IP 地址

操作	命令
配置 Server 端的公网 IP 地址	**public-ip** *ip-address*
删除 Server 端的公网 IP 地址	**undo public-ip** *ip-address*

4. 配置 Server 端的 UDP 端口号

当使用 UDP dvpn 封装时，请在 dvpn-class 视图下进行下面配置。

表4-17 配置 Server 端的公网 IP 地址

操作	命令
配置 Server 端的 UDP 端口号	**udp-port** *port-number*
恢复 Server 端的 UDP 端口号的缺省设置	**undo udp-port**

4.2.3 动态 VPN 的显示和调试

请在用户视图下执行 **reset dvpn map** 和 **debugging dvpn** 命令，**display dvpn map** 命令可在所有视图下执行。

表4-18 动态 VPN 的显示和调试

操作	命令
打开 DVPN 的调试开关	**debugging dvpn** { **all** | **error** | **event** | **hexadecimal** | **packet** } **undo debugging dvpn** { **all** | **error** | **event** | **hexadecimal** | **packet** }

操作	命令
显示当前节点所拥有的全部 Map 信息。	**display dvpn map** [**vpn-id** *vpn-id*] [**private-ip** *private-ip*]
清除指定的会话连接。	**reset dvpn map vpn-id** *vpn-id* **private-ip** *ip-address*

4.3 DVPN 典型组网应用

4.3.1 动态 VPN 基本配置应用

1. 组网需求

本例中总公司及所辖分公司配置为 VPN 100。总公司路由器作为 DVPN Server，WAN 口 S0/0/0 分配固定的公有 IP 地址 202.0.0.1。分公司路由器均配置为 Client，通过串口与总公司相连。此处 Client 的串口 IP 地址为私有 IP 地址或公有 IP 地址均可。

2. 组网图

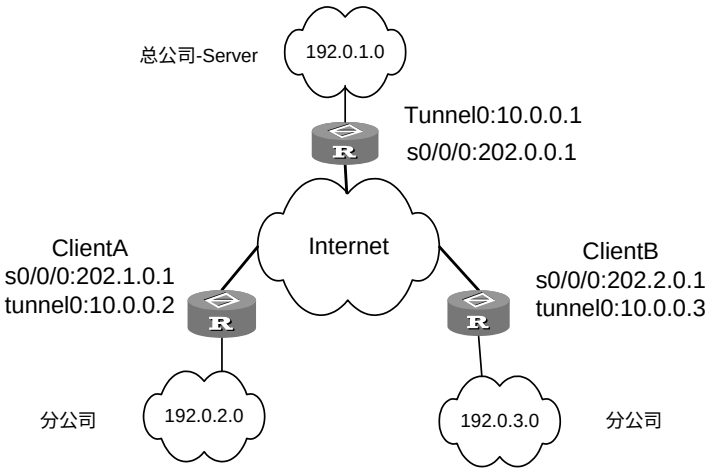

图4-2 动态 VPN 典型配置应用

3. 配置步骤

(1) 配置 Client A

配置 Serial0/0/0 接口。

```
[Client A] interface serial 0/0/0
[Client A -Serial0/0/0] ip address 202.1.0.1 255.255.255.0
```

配置 dvpn-class。

```
[ClientA] dvpn class my-server
[ClientA -dvpn-class-my-server] private-ip 10.0.0.1
```

```
[ClientA -dvpn-class-my-server] public-ip 202.0.0.1
[ClientA -dvpn-class-my-server] udp-port 8005
```

配置 tunnel 接口属性。

```
[ClientA] interface tunnel 0
[ClientA-Tunnel0] tunnel-protocol udp dvpn
[ClientA-Tunnel0] dvpn interface-type client
[ClientA-Tunnel0] dvpn vpn-id 100
[ClientA-Tunnel0] dvpn authentication enable
[ClientA-Tunnel0] dvpn key 123
[ClientA-Tunnel0] dvpn timer keepalive 10
[ClientA-Tunnel0] dvpn timer aging 30
[ClientA-Tunnel0] ip address 10.0.0.2 255.255.255.0
[ClientA-Tunnel0] dvpn udp-port 8001
[ClientA-Tunnel0] source seril0/0/0
[ClientA-Tunnel0] dvpn server my-server
[ClientA-Tunnel0] undo dvpn register-type forward
[ClientA-Tunnel0] quit
```

配置动态路由协议。

```
[ClientA] rip
[ClientA -rip] network 202.1.0.0
[ClientA -rip] network 10.0.0.0
```

ClientB 的配置与此相似。

(2) 配置 Server

配置 Serial0/0/0 接口。

```
[Server] interface serial0/0/0
[Server-serial0/0/0] ip address 202.0.0.1 255.255.255.0
```

配置 Tunnel0 接口属性。

```
[Server] interface tunnel 0
[Server-Tunnel0] tunnel-protocol udp dvpn
[Server-Tunnel0] dvpn interface-type server
[Server-Tunnel0] dvpn vpn-id 100
[Server-Tunnel0] dvpn authentication enable
[Server-Tunnel0] dvpn client private-ip 10.0.0.2 key 123
[Server-Tunnel0] dvpn key 567
[Server-Tunnel0] dvpn timer keepalive 10
[Server-Tunnel0] dvpn timer aging 30
[ClientA-Tunnel0] dvpn udp-port 8005
[Server-Tunnel0] ip address 10.0.0.1 255.255.255.0
[Server-Tunnel0] source serial 0/0/0
```

配置动态路由协议。

```
[Server] rip
[Server-rip] network 202.0.0.0
[Server-rip] network 10.0.0.0
```

4.4 Client 通过普通拨号方式连接 DVPN Server 配置举例

1. 组网需求

本例中总公司及所辖分公司配置为 VPN 100。总公司路由器作为 DVPN Server，WAN 口 S0/0/0 分配固定 IP 地址 202.0.0.1。分公司路由器均配置为 Client，通过异步串口拨号方式与总公司相连，ClientA 连接总公司路由器的 S0/0/0 口（Tel：8810148），ClientB 连接连接总公司路由器的 S1/0/0 口（Tel：8810149）。

2. 组网图

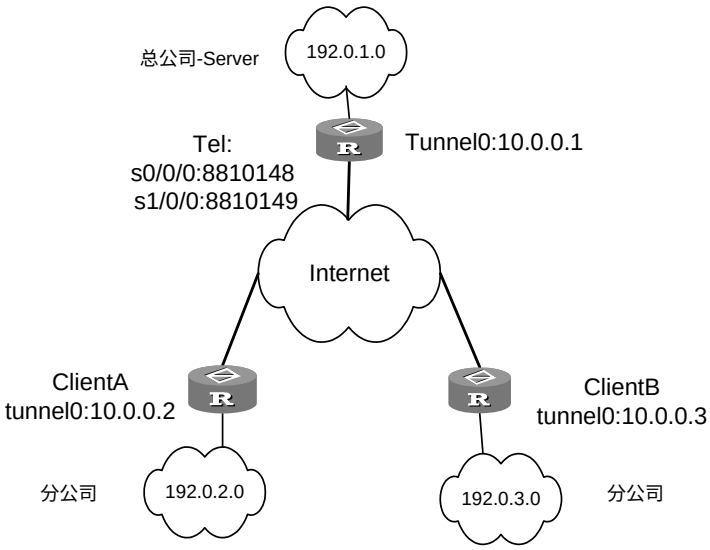

图4-3 Client 通过拨号方式连接 DVPN Server 配置举例

3. 配置步骤

(1) 配置 Client A

配置拨号访问控制列表。

```
[Client A] dialer-rule 1 ip permit
```

配置 Serial0/0/0 接口异步拨号方式。

```
[Client A] interface serial 0/0/0
[Client A-Serial0/0/0] physical-mode async
[Client A-Serial0/0/0] async mode protocol
```

配置 Serial0/0/0 接口地址、启动轮询 DCC、到达对端的拨号控制中心。

```
[Client A -Serial0/0/0] dialer enable-circular
[Client A -Serial0/0/0] dialer-group 1
[Client A -Serial0/0/0] dialer number 8810048
[Client A-Serial0/0/0] ip address ppp-negotiate
```

配置 user-interface 使能拨号方式。

```
[Client A-Serial0/0/0] user-interface tty1
[Client A -ui-tty1] modem
```

配置 dvpn-class。

```
[ClientA] dvpn class my-server
[ClientA -dvpn-class-my-server] private-ip 10.0.0.1
[ClientA -dvpn-class-my-server] public-ip 202.0.0.1
[ClientA -dvpn-class-my-server] udp-port 8005
```

配置 tunnel 接口属性。

```
[ClientA] interface tunnel 0
[ClientA-Tunnel0] tunnel-protocol udp dvpn
[ClientA-Tunnel0] dvpn interface-type client
[ClientA-Tunnel0] dvpn vpn-id 100
[ClientA-Tunnel0] dvpn authentication enable
[ClientA-Tunnel0] dvpn key 123
[ClientA-Tunnel0] dvpn timer keepalive 10
[ClientA-Tunnel0] dvpn timer aging 30
[ClientA-Tunnel0] ip address 10.0.0.2 255.255.255.0
[ClientA-Tunnel0] dvpn udp-port 8001
[ClientA-Tunnel0] source seril0/0/0
[ClientA-Tunnel0] dvpn server my-server
[ClientA-Tunnel0] undo dvpn register-type forward
[ClientA-Tunnel0] quit
```

配置动态路由协议。

```
[ClientA] rip
[ClientA -rip] network 10.0.0.0
```

ClientB 的配置与此相似。

(2) 配置 Server

配置 IP 地址池。

```
[Server] ip pool 1 202.0.0.2 202.0.0.5
```

配置 Serial0/0/0 接口异步协议方式，并为对端分配 IP 地址。

```
[Server-Dialer0] interface serial 0/0/0
[Server-Serial0/0/0] physical-mode async
[Server-Serial0/0/0] async mode protocol
```

```
[Server-Serial0/0/0] remote address 1
```

配置 Serial1/0/0 接口异步协议方式，并为对端分配 IP 地址。

```
[Server-Serial0/0/0] interface serial 1/0/0
[Server-Serial1/0/0] physical-mode async
[Server-Serial1/0/0] async mode protocol
[Server-Serial1/0/0] remote address 1
```

配置 Tunnel0 接口属性。

```
[Server] interface tunnel 0
[Server-Tunnel0] tunnel-protocol udp dvpn
[Server-Tunnel0] dvpn interface-type server
[Server-Tunnel0] dvpn vpn-id 100
[Server-Tunnel0] dvpn authentication enable
[Server-Tunnel0] dvpn client private-ip 10.0.0.2 key 123
[Server-Tunnel0] dvpn key 567
[Server-Tunnel0] dvpn timer keepalive 10
[Server-Tunnel0] dvpn timer aging 30
[Server-Tunnel0] ip address 10.0.0.1 255.255.255.0
[Server-Tunnel0] dvpn udp-port 8005
[Server-Tunnel0] source serial 0/0/0
```

配置动态路由协议。

```
[Server] rip
[Server -rip] network 10.0.0.0
```