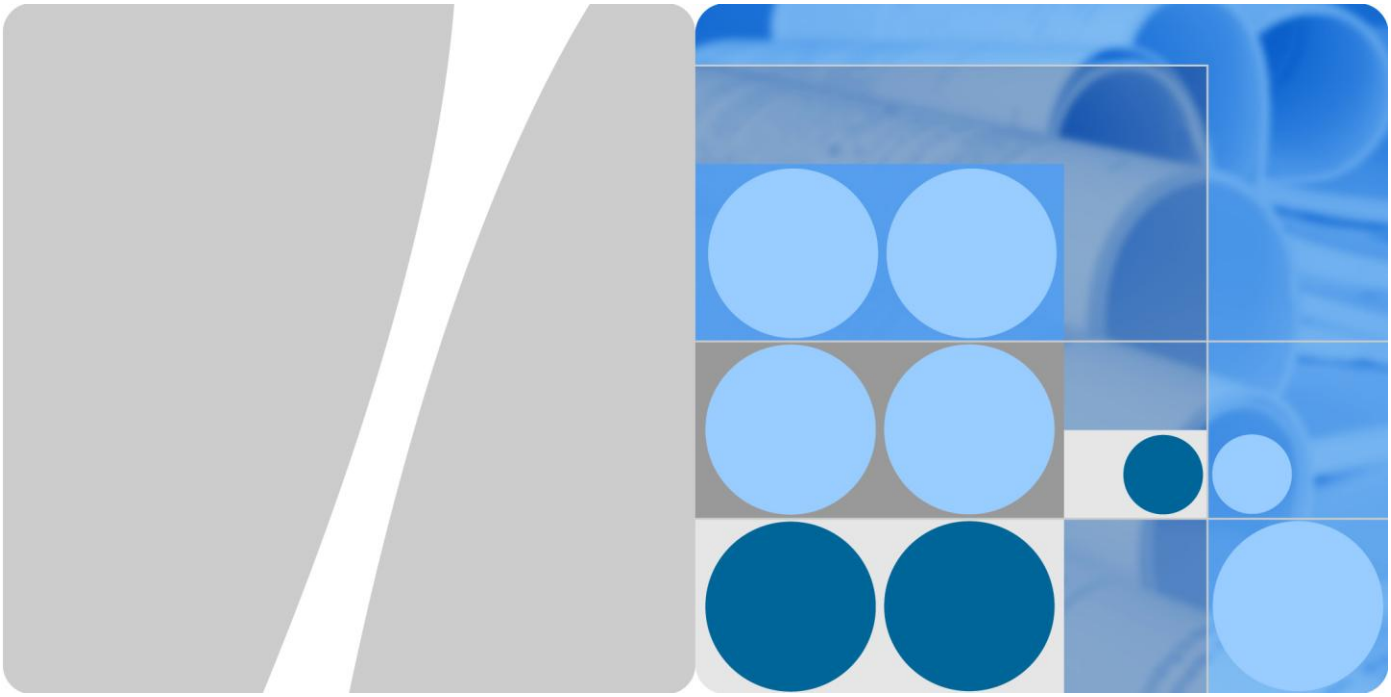


华为 AR G3 企业路由器
L2TP 技术白皮书

文档版本 01

发布日期 2012-05-10

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://enterprise.huawei.com/cn/

目 录

1 介绍

定义

二层隧道协议 L2TP（Layer 2 Tunneling Protocol）是虚拟私有拨号网 VPDN（Virtual Private Dial-up Network）隧道协议的一种。

VPDN 是指利用公共网络（如 ISDN 或 PSTN）的拨号功能接入公共网络，实现虚拟专用网，从而为企业、小型 ISP、移动办公人员等提供接入服务，是一种经济而有效的点到点连接方式。

VPDN 采用隧道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 隧道协议主要包括以下三种：

- 点到点隧道协议 PPTP（Point-to-Point Tunneling Protocol）
- 二层转发 L2F（Layer 2 Forwarding）
- 二层隧道协议 L2TP（Layer 2 Tunneling Protocol）

L2TP 结合了 L2F 和 PPTP 的各自优点，成为 IETF 有关二层隧道协议的工业标准。目前使用最广泛的是 L2TP。

目的

PPP 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，当用户与 NAS 之间运行 PPP 协议时，二层链路端点与 PPP 会话点驻留在相同硬件设备（NAS）上。

L2TP（RFC 2661）是一种对 PPP 链路层数据包进行隧道传输的技术，允许二层链路端点和 PPP 会话点驻留在通过分组交换网络连接的不同设备上，从而扩展了 PPP 模型，使得 PPP 会话可以跨越 IP 网络。

受益

L2TP 给企业带来了明显的收益：

- 企业分支可以通过 L2TP 接入到企业总部。

- 移动办公人员可以通过 L2TP 接入到企业总部。

2 参考标准和协议

本特性的参考资料清单如下：

文档编号	描述
RFC2661	Layer Two Tunneling Protocol "L2TP"

3 原理描述

关于本章

3.1 L2TP 基本原理

LAC

L2TP 访问集中器（LAC，L2TP Access Concentrator）是交换网络上具有 PPP 和 L2TP 处理能力的设备。LAC 根据 PPP 报文中所携带的用户名或者域名信息，和 LNS 建立 L2TP 隧道连接，将 PPP 协商延展 LNS。

LAC 可以建立不同的 L2TP 遂道使数据流之间相互隔离，即 LAC 可以建立多个 VPDN 连接。

LAC 在 LNS 和 PPP 终端之间传递数据。即 LAC 收到 PPP 终端的报文后进行 L2TP 封装发送至 LNS，LAC 收到 LNS 的报文后进行解封装并发送至 PPP 终端。

LNS

L2TP 网络服务器（LNS，L2TP Network Server）是接收 PPP 会话的一端，通过 LNS 的认证，PPP 会话协商成功，远程用户可以访问企业总部的资源。对 L2TP 连接，LNS 是 LAC 的对端设备，即 LAC 和 LNS 建立了 L2TP 隧道；对 PPP，LNS 是 PPP 终端发起 PPP 会话的逻辑终止端点，即 PPP 终端和 LNS 建立了一条点到点的虚拟链路。

LNS 位于企业总部私网与公网边界，通常是企业总部的网关设备。必要时，LNS 还兼有网络地址转换（NAT）功能，对企业总部网络内的私有 IP 地址与公共 IP 地址进行转换。

控制消息和数据消息

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。它的传输是可靠传输，并且支持对控制消息的流量控制和拥塞控制。
- 数据消息用于封装 PPP 帧，并在隧道上传输。它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 LNS 端分配。

L2TP 协议结构

图 3-1 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 数据通道内传输，控制消息在可靠的 L2TP 控制通道内传输。

图3-1 L2TP 协议结构

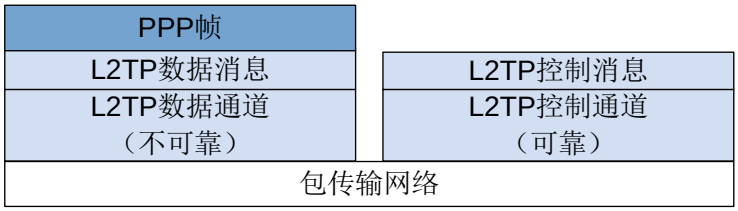
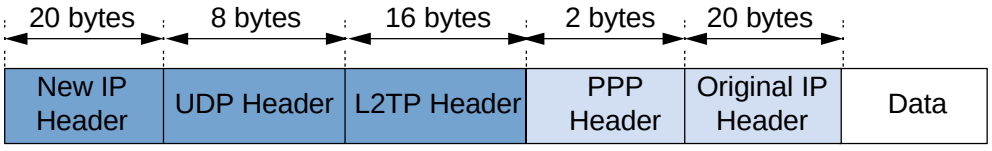


图 3-2 描述了 LAC 与 LNS 之间的 L2TP 数据报文的封装结构。通常 L2TP 数据以 UDP 报文的形式发送。L2TP 注册了 UDP 1701 端口，但是这个端口仅用于初始的隧道建立过程中。L2TP 隧道发起方任选一个空闲的端口（未必是 1701）向接收方的 1701 端口发送报文；接收方收到报文后，也任选一个空闲的端口（未必是 1701），给发送方的指定端口回送报文。至此，双方的端口选定，并在隧道保持连通的时间段内不再改变。

图3-2 L2TP 报文封装结构



隧道和会话

在一个 LNS 和 LAC 对之间存在着两种类型的连接：

- 隧道（Tunnel）连接：它对应了一个 LNS 和 LAC 对。
- 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。

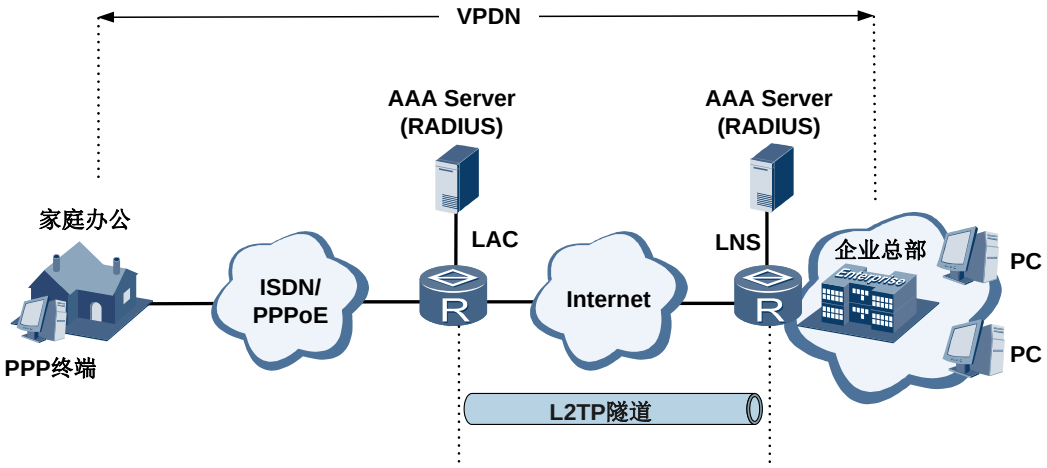
在同一对 LAC 和 LNS 之间可以建立多个 L2TP 隧道，隧道由一个控制连接和一个或多个会话连接组成。会话连接必须在隧道建立（包括身份保护、L2TP 版本、帧类型、硬件传输类型等信息的交换）成功之后进行，每个会话连接对应于 LAC 和 LNS 之间的一个 PPP 数据流。

控制消息和数据消息都在隧道上传输。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，隧道断开。

3.2 L2TP 隧道会话的建立过程

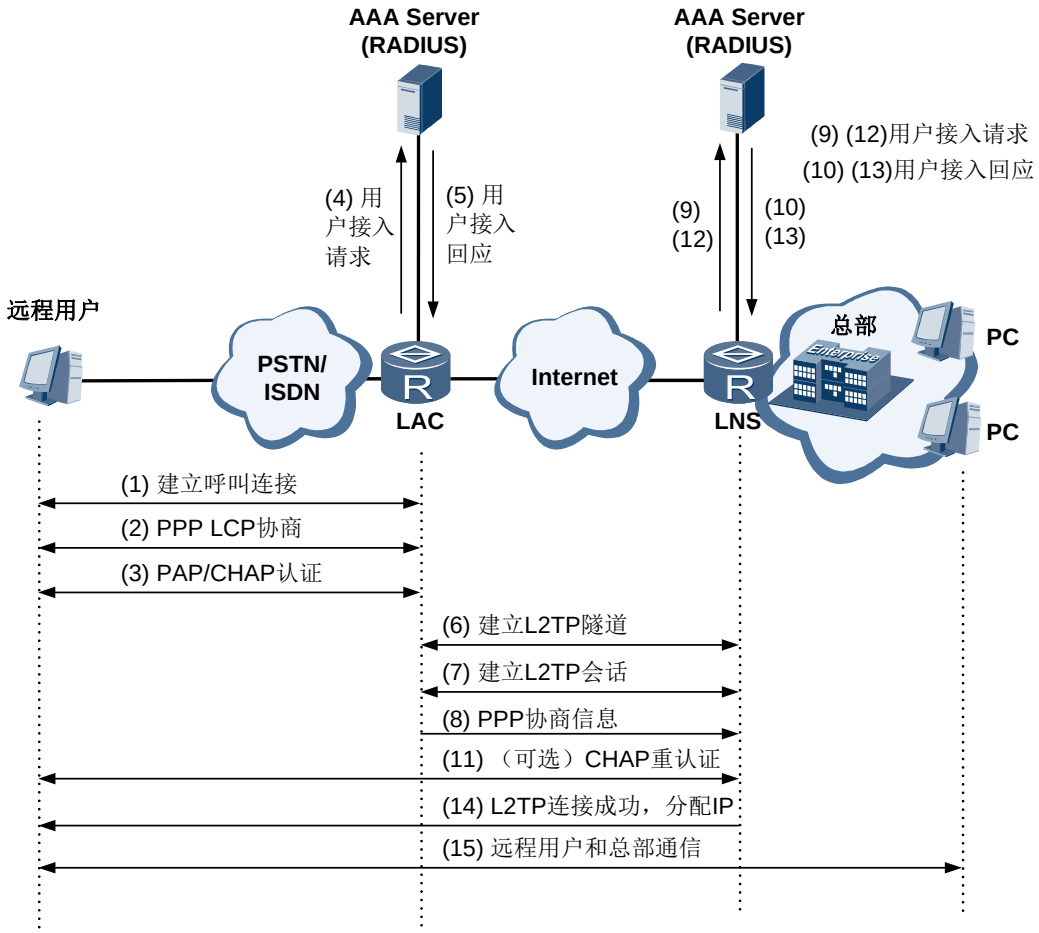
L2TP 的典型组网如图 3-3 所示：

图3-3 L2TP 隧道的典型组网示意图



进行隧道验证的 L2TP 隧道呼叫建立流程如图 3-4。

图3-4 L2TP 隧道的呼叫建立流程



1. 用户端 PC 机发起呼叫连接请求；
2. PC 机和 LAC 端进行 PPP LCP 协商；
3. LAC 对 PC 机提供的用户信息进行 PAP 或 CHAP 认证；

   # 在 LAC 的用户侧接口上对接入用户进行 CHAP 认证。

```
<Huawei> system-view
[Huawei] interface serial 1/0/0
[Huawei-Serial1/0/0] link-protocol ppp
[Huawei-Serial1/0/0] ppp authentication-mode chap
```

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，LAC 准备发起 Tunnel 连接请求；

   # LAC 创建 L2TP 组，配置 L2TP 隧道参数，根据用户名验证用户身份，向 LNS（10.1.1.1）发起隧道连接。

```
<Huawei> system-view
[Huawei] l2tp-group 1
[Huawei-l2tp1] tunnel name lac
[Huawei-l2tp1] start l2tp ip 10.1.1.1 fullusername user1
```

6. LAC 端向指定 LNS 发起 Tunnel 连接请求；

7. 在需要对隧道进行认证的情况下，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；

   # 在 LAC 和 LNS 的 L2TP 组内配置相同的认证参数，用于互相认证。以 LAC 为例，认证码为 **huawei**，密文显示：

   ```
   <Huawei> system-view
   [Huawei] l2tp-group 1
   [Huawei-l2tp1] tunnel authentication
   [Huawei-l2tp1] tunnel password cipher huawei
   ```

8. 隧道验证通过；

   # 在 LNS 接入 LAC 发起的隧道连接请求，根据虚拟模板接口 VT1 的参数和对端配置的隧道名 **lac** 建立隧道。

   ```
   <Huawei> system-view
   [Huawei] l2tp-group 1
   [Huawei-l2tp1] allow l2tp virtual-template 1 remote lac
   ```

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；

    # 在 LNS 上配置二次认证，例如对远程用户强制 CHAP 认证。

    ```
    <Huawei> system-view
    [Huawei] l2tp-group 1
    [Huawei-l2tp1] mandatory-chap
    ```

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；
15. 验证通过，LNS 端会给远端用户分配一个企业网内部 IP 地址，用户即可以访问企业内部资源。

    # 在 LNS 的虚拟接口模板配置 IP 地址作为 L2TP 接入网关地址，引入配置好的地址池资源 **pool 1**，为远程用户分配 IP 地址。

    ```
    <Huawei> system-view
    [Huawei] interface virtual-template 1
    [Huawei-Virtual-Template1] ip address 172.1.1.1 255.255.255.0
    [Huawei-Virtual-Template1] remote address pool 1
    ```

3.3 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。如果有特定的安全要求，还可以在 L2TP 之上采用隧道加密技术、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，在 PPP 数据包内可以封装多种协议。

- 支持 RADIUS 服务器的验证

  LAC 和 LNS 可以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（RFC 1918）。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（ISP 处，用于产生账单）和 LNS（企业网关，用于付费及审计）同时计费。L2TP 能够统计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，企业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，当主 LNS 不可达之后，LAC 可以与备份 LNS 建立连接，增加了 VPN 服务的可靠性和容错性。

4 应用

关于本章

4.1 典型的 L2TP 场景

4.1 典型的 L2TP 场景

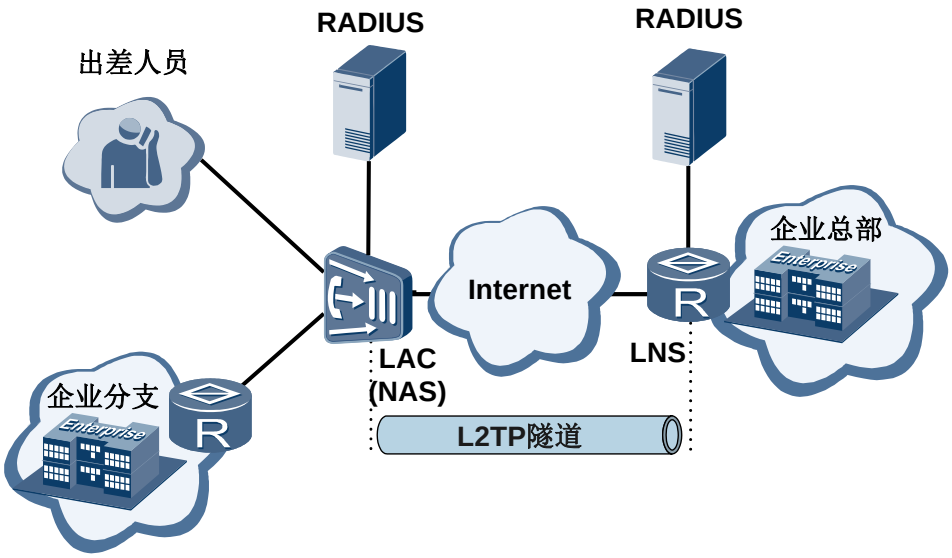
L2TP 四种典型的应用场景：

- NAS-Initialized
- Client-Initialized
- LAC-Auto-Initiated
- L2TP 多域接入场景

NAS-Initialized

如图 4-1 所示，由 LAC 端（指 NAS）发起 L2TP 隧道连接。远程拨号用户通过 PPP 拨入 LAC，由 LAC 通过 Internet 向 LNS 发起建立隧道连接请求。拨号用户的私网地址由 LNS 分配，对远程拨号用户的验证与计费既可由 LAC 侧完成，也可在 LNS 侧完成。在这种应用中，AR 可作为企业分支和企业总部的网关设备，分别提供 PPP Client 和 LNS 服务。

图4-1 NAS-Initiated 场景



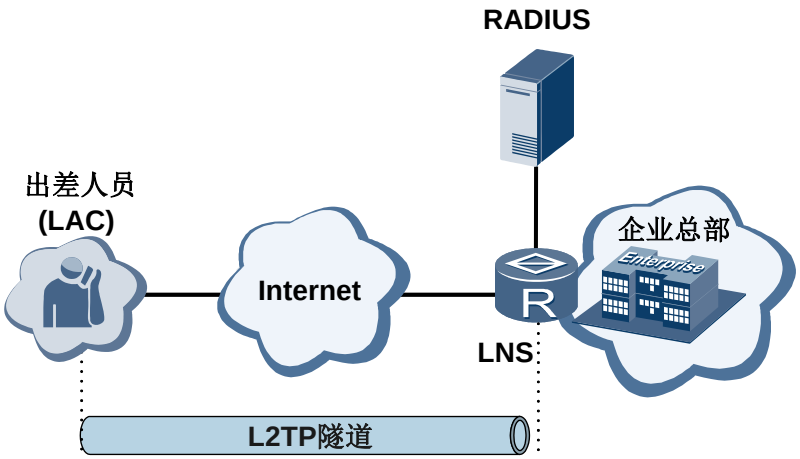
AR 作为 LNS 时，需要响应 LAC 发起的 L2TP 连接请求，如下配置表示 AR 为 LNS：

```
<Huawei> system-view
[Huawei] l2tp-group 1
[Huawei-l2tp1] allow l2tp virtual-template 1 remote lac
```

Client-Initialized

如图 4-2 所示，直接由远程用户终端（本地支持 L2TP 协议）发起 L2TP 隧道连接。用户获得 Internet 访问权限后，可直接向 LNS 发起隧道连接请求，无需经过单独的 LAC 设备建立隧道，用户的私网地址由 LNS 分配。在 Client-Initiated 模式下，AR 作为 LNS 部署在企业总部网关。

图4-2 Client-Initialized 场景



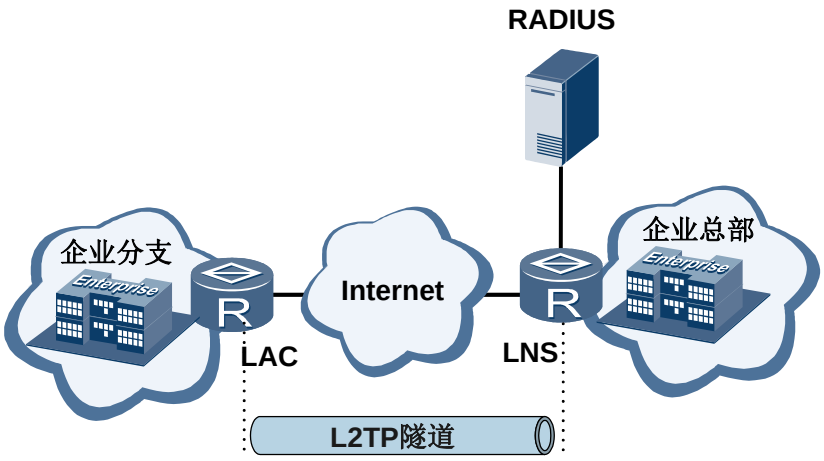
这种方式的特点是：

- 用户需要安装 L2TP 的拨号软件。使用 Windows 操作系统的用户也可以使其自带的 VPN 拨号软件。
- 用户上网的方式和地点没有限制，可以访问 Internet 即可。
- L2TP 隧道两端分别驻留在用户侧和 LNS 侧，一个 L2TP 隧道承载一个 L2TP 会话。
- 用户对信息安全有较高要求时，可使用 IPSec 进行加密和认证。

LAC-Auto-Initiated

采用 NAS-Intiated 方式建立 L2TP 隧道时，要求远程用户必须通过 PPPoE/ISDN 等拨号方式拨入 LAC，且只有远程用户拨入 LAC 后，才能触发 LAC 向 LNS 发起建立隧道连接的请求。 如图 4-3 所示，在 LAC-Auto-Initiated 模式下，LAC 上创建一个虚拟的 PPP 用户，进行虚拟拨号，LAC 将自动向 LNS 发起建立隧道连接的请求，为该虚拟 PPP 用户建立 L2TP 隧道。远程用户访问 LNS 连接的内部网络时，LAC 将通过 L2TP 隧道转发这些访问数据。在该模式下，远端系统和 LAC 之间可以是任何基于 IP 的连接，不局限于拨号连接。AR 作为自拨号 LAC，部署在企业分支的网关。

图4-3 用户直接与 LAC 相连



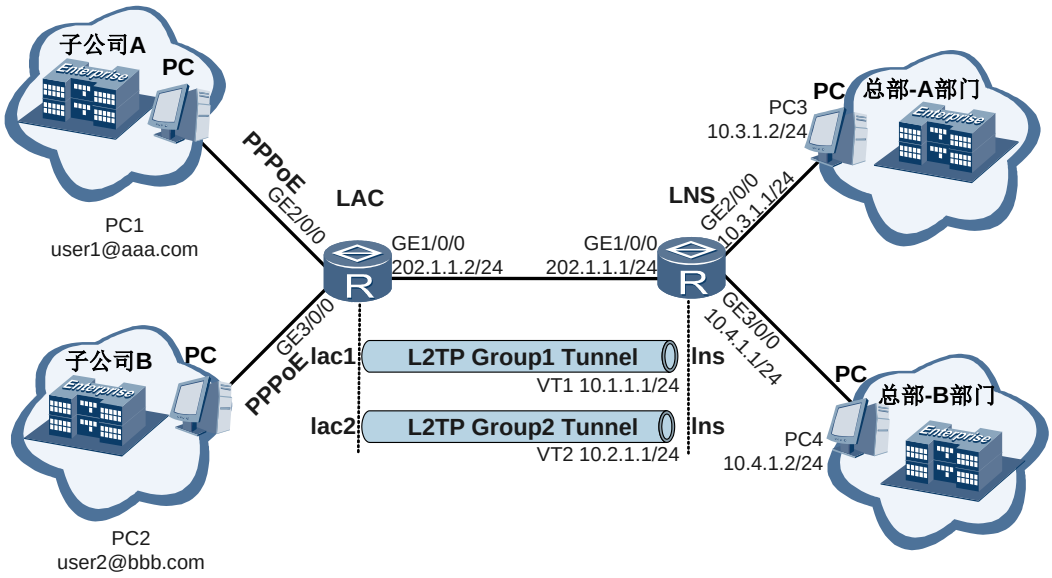
AR 作为 LAC 时，通过自拨号方式向 LNS（10.1.1.1）发起 L2TP 连接请求，自拨号的用户名 **user1**，其中自拨号的关键配置如下：

```
<Huawei> system-view
[Huawei] interface virtual-template 1
[Huawei-Virtual-Template1] ip address ppp-negotiate
[Huawei-Virtual-Template1] ppp pap local-user user1 password simple huawei
[Huawei-Virtual-Template1] l2tp-auto-client enable
[Huawei-Virtual-Template1] quit
[Huawei] l2tp-group 1
[Huawei-l2tp1] start l2tp ip 10.1.1.1 fullusername user1
```

L2TP 多域接入场景

如图 4-4 所示，企业总部和旗下子公司有业务往来，不同的子公司需要访问的总部资源有所不同，总部为不同子公司的员工提供接入服务，使用 L2TP 功能和子公司建立 VPDN 连接。在 LAC 配置基于域名判断接入用户是否为 VPDN 用户，简化 VPDN 用户的管理。每个子公司使用独立的 L2TP 隧道，获取不同网段的私网地址。子公司用户发起到总部的连接时，因为源地址和目的地址都由总部分配，所以总部可以配置 ACL 实现对子公司访问权限的管理。

图4-4 NAS-Initiated 场景



AR 作为 LAC 的配置如下：

```
#
 sysname LAC
#
 l2tp enable
#
aaa
 authentication-scheme huawei
 domain aaa.com
  authentication-scheme huawei
 domain bbb.com
  authentication-scheme huawei
 local-user user1@aaa.com password +Q4Z3D_*-N[Q=^Q`MAF4<1!!
 local-user user1@aaa.com service-type ppp
 local-user user2@bbb.com password +Q4Z3D_*-N[Q=^Q`AWTQ<1!!
 local-user user2@bbb.com service-type ppp
#
interface Virtual-Template1
 ip address ppp-negotiate
 ppp authentication-mode pap
#
interface Virtual-Template2
```

```
 ip address ppp-negotiate
 ppp authentication-mode pap
#
interface GigabitEthernet1/0/0
 ip address 202.1.1.2 255.255.255.0
#
interface GigabitEthernet2/0/0
 pppoe-server bind Virtual-Template 1
#
interface GigabitEthernet3/0/0
 pppoe-server bind Virtual-Template 2
#
l2tp-group 1
 tunnel password simple huawei
 tunnel name lac1
 start l2tp ip 202.1.1.1 domain aaa.com
#
l2tp-group 2
 tunnel password simple huawei
 tunnel name lac2
 start l2tp ip 202.1.1.1 domain bbb.com
#
return
```

AR 作为 LNS 的配置如下：

```
#
 sysname LNS
#
 l2tp enable
#
ip pool 1
 gateway-list 10.1.1.1
 network 10.1.1.0 mask 255.255.255.0
#
ip pool 2
 gateway-list 10.2.1.1
 network 10.2.1.0 mask 255.255.255.0
#
aaa
 authentication-scheme huawei
 domain aaa.com
  authentication-scheme huawei
 domain bbb.com
  authentication-scheme huawei
 local-user user1@aaa.com password +Q4Z3D_*-N[Q=^Q`MAF4<1!!
 local-user user1@aaa.com service-type ppp
 local-user user2@bbb.com password +Q4Z3D_*-N[Q=^Q`AWTQ<1!!
 local-user user2@bbb.com service-type ppp
#
interface Virtual-Template1
 ppp authentication-mode pap
 remote address pool 1
 ip address 10.1.1.1 255.255.255.0
#
interface Virtual-Template2
```

```
 ppp authentication-mode pap
 remote address pool 2
 ip address 10.2.1.1 255.255.255.0
#
interface GigabitEthernet1/0/0
 ip address 202.1.1.1 255.255.255.0
#
interface GigabitEthernet2/0/0
 ip address 10.3.1.1 255.255.255.0
#
interface GigabitEthernet3/0/0
 ip address 10.4.1.1 255.255.255.0
#
l2tp-group 1
 allow l2tp virtual-template 1 remote lac1
 tunnel password simple  huawei
 tunnel name lns
#
l2tp-group 2
 allow l2tp virtual-template 2 remote lac2
 tunnel password simple  huawei
 tunnel name lns
#
return
```