# L2TP VPN基本原理

发表于 2019-08-21 | 更新于 2019-08-23 | 分类于 网络安全 | 阅读次数： 8542 | 字数： 5,331 | 阅读时长： 19

## L2TP VPN简介

### L2TP基本概念：

L2TP（Layer 2 Tunneling Protocol） VPN是一种用于承载PPP报文的隧道技术，该技术主要应用在远程办公场景中为出差员工远程访问企业内网资源提供接入服务。

### 目的：

L2TP VPN技术出现以后，使用L2TP VPN隧道“承载”PPP报文在Internet上传输成为了解决上述问题的一种途径。无论出差员工是通过传统拨号方式接入Internet，还是通过以太网方式接入Internet，L2TP VPN都可以向其提供远程接入服务。

### L2TP VPN的优点：

- 身份验证机制

  支持本地认证。

  支持Radius服务器等认证方式

- 多协议传输

  L2TP传输PPP数据包，PPP本身可以传输多协议，而不仅仅是IP可以在PPP数据包内封装多种协议

- 计费认证地址分配

  可在LAC和LNS两处同时计费，即ISP处（用于产生账单）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

  LNS可放置于企业网的USG之后，对远端用户地址进行动态分配和管理，可支持私有地址应用

- 不受NAT限制穿越

- 支持远程接入

- 灵活的身份验证及时以及高度的安全性

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

- L2TP隧道可以与IPSec结合，使通过L2TP所传输的数据更难被攻击。

  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。

- 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，增加了VPN服务的可靠性和容错性

# L2TP VPN的原理

## L2TP VPN的主要应用场景：

LAC和LNS介绍：

LAC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，主要用于为PPP类型的用户提供接入服务
LAC位于LNS和用户之间，用于在LNS和用户之间传递信息包，它把用户收到的信息包按照L2TP协议进行封装并送往LNS，同时也将从LNS收到的信息包进行解封装并送往用户。LAC与用户之间采用本地连接或PPP链路，VPDN应用中通常为PPP链路。

LNS既是PPP端系统，又是L2TP协议的服务器端，通常作为一个企业内部网的边缘设备。
LNS作为L2TP隧道的另一侧端点，是LAC的对端设备 ，是LAC进行隧道传输的PPP会话的逻辑终止端点。通过在公网中建立LAC隧道，将用户的PPP连接的另一端由原来的LAC在逻辑上延伸了企业网内部的LNS。

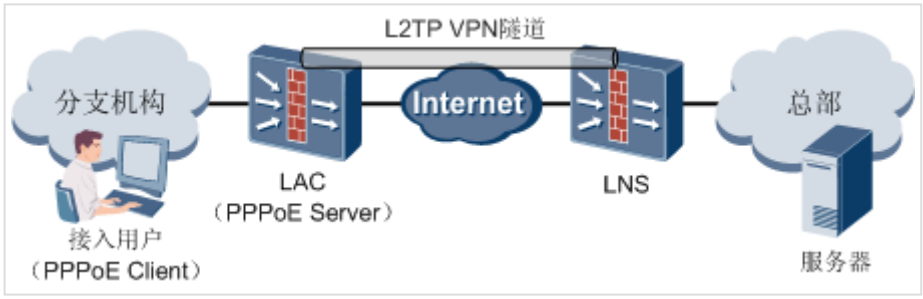
**L2TP VPN主要有三种应用场景。**分别是：

1. **NAS-Initiated场景（拨号用户访问企业内网）**

   > NAS（Network Access Server）:是运营商用来向拨号用户提供PPP/PPPoE接入服务的服务器，拨号用户通过NAS访问外部网络。
   >
   > LNS（L2TP Network Server）是企业总部的出口网关。

   用户通过PPPoE拨入LAC（L2TP Access Concentrator），触发LAC和LNS之间建立隧道。接入用户地址由LNS分配，对接入用户的认证可由LAC侧的代理完成，也可两侧都对接入用户做认证。当所有L2TP用户都下线时，隧道自动拆除以节省资源，直至再有用户接入时，重新建立隧道。

   此组网适用于分支机构用户向总部发起连接，且一般用于分支机构的用户不经常访问企业总部的情况。




图：NAS-Initiated VPN隧道组网图

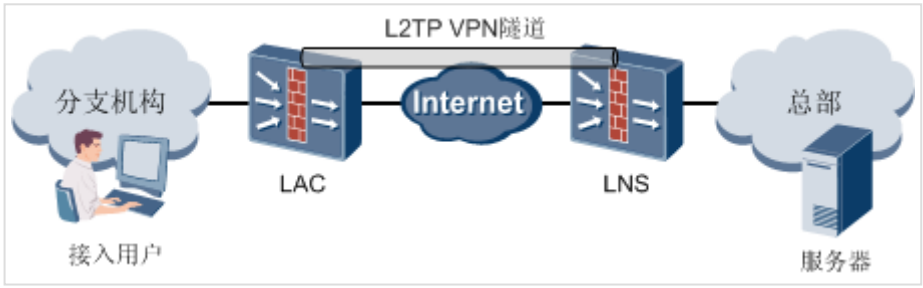
2. **LAC自动拨号**

LAC与LNS之间建立一条**永久性**L2TP会话。客户端不用PPP拨号，而通过IP连接即可在隧道中传输数据。

用户通过配置触发建立LAC与LNS之间的永久性L2TP会话。LAC使用存储在本地的用户名和LNS建立一个永久存在的L2TP隧道，此时的L2TP隧道就相当于一个物理连接。用户与LAC之间的连接就不受限于PPP连接，而只需IP连接，LAC即可将用户的IP报文转发到LNS。

这种组网也适用于分支机构接入总部，用于分支机构员工访问总部频率较高的情况。与NAS-Initiated VPN场景相比：

- 分支机构员工感知不到隧道存在，不需要使用用户名接入。LAC为分支机构的多个用户提供L2TP服务，免去了每个用户使用L2TP都需要先拨号的麻烦。
- 这种组网下，LNS只对LAC进行认证。其缺点为：分支机构用户只要能够连接LAC即可使用L2TP隧道接入总部，而不需被认证。存在一定的安全隐患。此时用户接入总部以通过设备的用户认证功能对接入总部的用户进行认证，从而提高安全性。



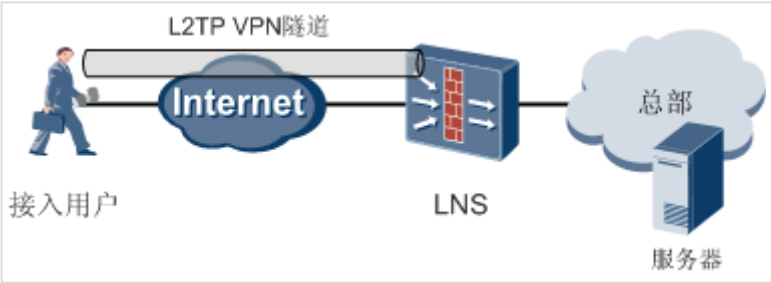

图：LAC自动拨号组网示例

3. **Client-Initiated场景（移动办公用户访问企业内网）**

直接由接入用户（可为支持L2TP协议的PC）发起连接。此时接入用户可直接向LNS发起隧道连接请求，无需再经过一个单独的LAC设备。接入用户地址的分配由LNS来完成。

由于LNS端需要为每个远程用户建立一条隧道，与NAS-Initiated VPN场景相比，LNS端配置更复杂一些。与其他两种场景相比，其优点在于接入用户不受地域限制。

此场景适用于出差员工使用PC、手机等移动设备接入总部服务器，实现移动办公。




图：Client-Initiated组网示意图

## 隧道和会话建立原理：

### 隧道和会话的概念：

在LNS和LAC对之间存在着两种类型的连接。

**隧道（Tunnel）连接**：它定义了互相通信的两个实体LNS和LAC。

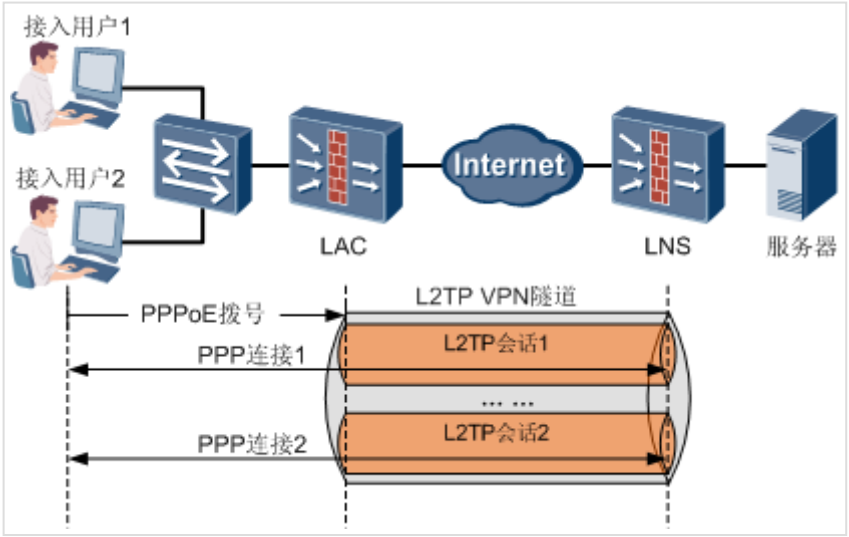
- 在一对LAC和LNS之间可以建立多条隧道。隧道由一个控制连接和至少一个会话组成。
- L2TP首先需要建立L2TP隧道，然后在L2TP隧道上建立会话连接，最后建立PPP连接。所有的L2TP需要承载的数据信息都是在PPP连接中进行传递的。

**会话（Session）连接**：它复用在隧道连接之上，用于表示承载隧道连接中的每个PPP连接过程。

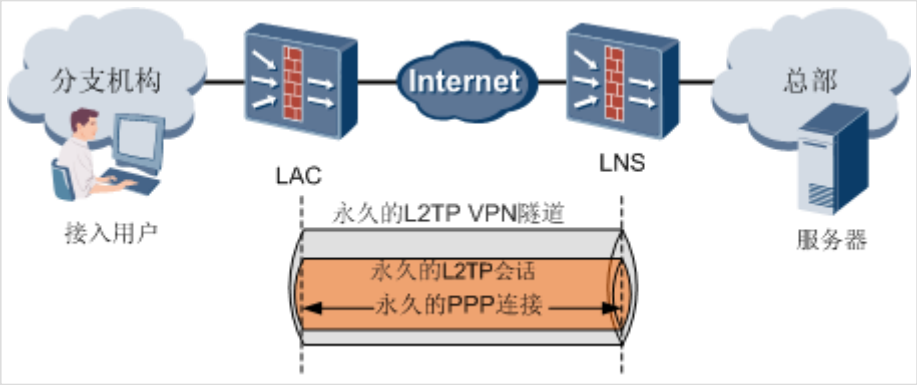
- 会话是有方向的，从LAC向LNS发起的会话叫做Incoming会话，从LNS向LAC发起的会话叫做Outgoing会话。

**隧道和会话的关系：**

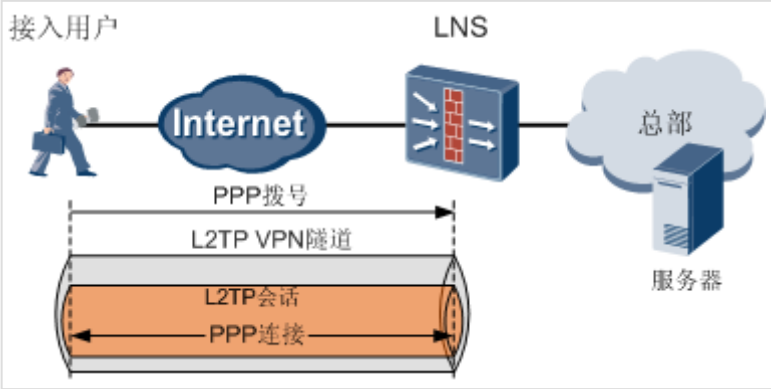
- NAS-Initiated VPN场景中，一对LAC和LNS的链接可以存在多条隧道；一条隧道中可承载多条会话。即：多个用户可以共用一条隧道。




- LAC自动拨号场景中，**LAC和LNS建立永久的隧道。且仅承载一条永久的L2TP会话和PPP连接。**




- Client-Initiated VPN场景中，每个接入用户和LNS之间均建立一条隧道；每条隧道中仅承载一台L2TP会话和PPP连接。




**控制消息和数据消息：**

**控制消息：**控制消息用于隧道和会话连接的建立、维护以及传输控制；位于隧道和会话建立过程中。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；主要的控制消息包括控制报文、会话报文等。

**控制报文用于建立和拆除、维持隧道**，主要包括：

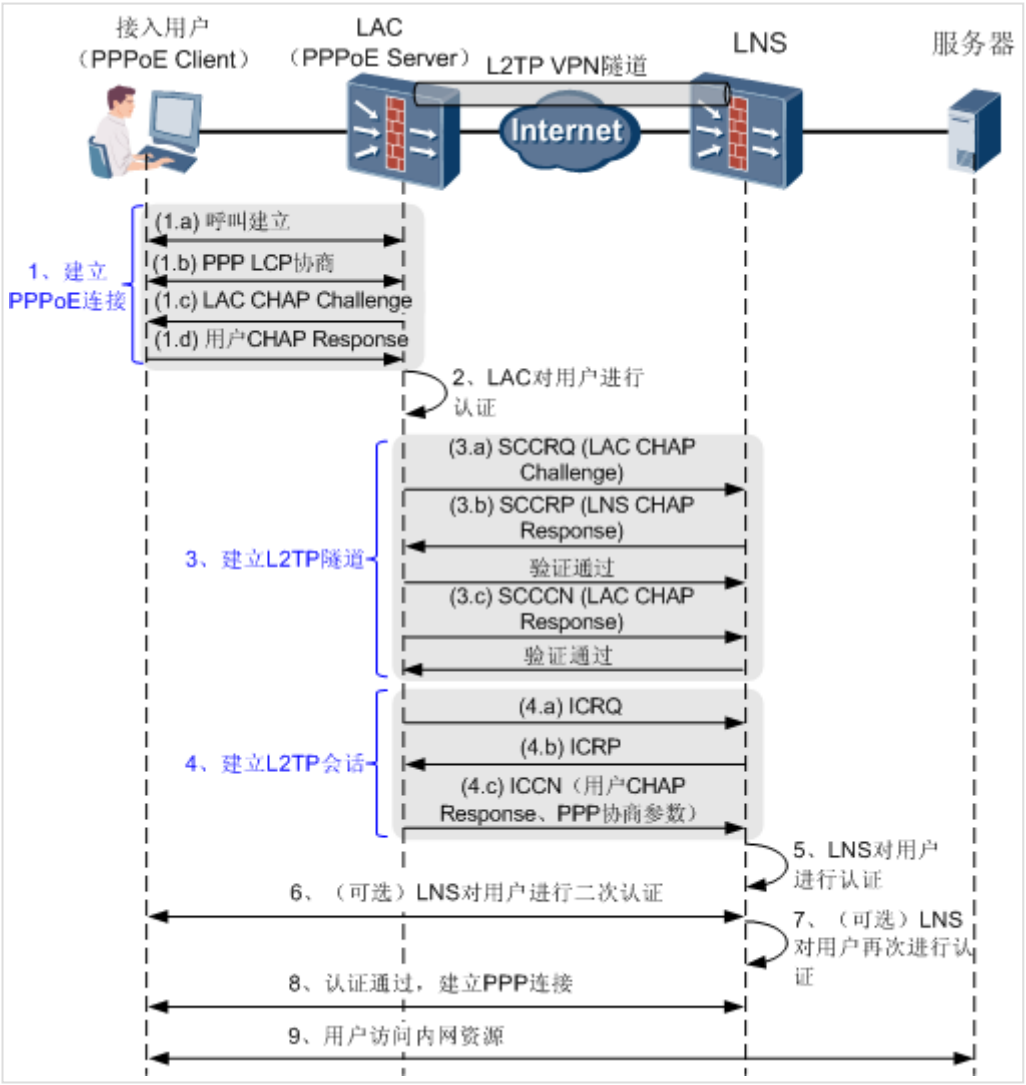
- SCCRQ（Start-Control-Connection-Request）：控制连接发启请求。由LAC或者LNS向对端发送，用来初始化LAC和LNS之间的隧道，开始隧道的建立过程。NGFW的应用场景中，一般都是由LAC向LNS发起请求。
- SCCRP（Start-Control-Connection-Reply）：表示接受了对端的连接请求，隧道的建立过程可以继续。
- SCCCN（Start-Control-Connection-Connected）：对SCCRP的回应，完成隧道的建立。
- StopCCN（Stop-Control-Connection-Notification）：由LAC或者LNS发出，通知对端隧道将要停止，控制连接将要关闭。另外，所有活动的会话都会被清除。
- HELLO：隧道保活控制消息。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，如果在一段时间内未收到Hello报文的应答，隧道将被清除。

**会话报文用于建立和拆除会话**，主要包括：

- ICRQ（Incoming-Call-Request）：当LAC检测到有用户拨入电话的时候，向LNS发送ICRQ，请求在已经建立的隧道中建立会话。
- ICRP（Incoming-Call-Reply）：用来回应ICRQ，表示ICRQ成功，LNS也会在ICRP中标识L2TP会话必要的参数。
- ICCN（Incoming-Call-Connected）：用来回应ICRP，L2TP会话建立完成。
- CDN（Call-Disconnect-Notify）：由LAC或者LNS发出，通知对端会话将要停止。

**数据消息**：用于承载用户的PPP连接数据报文，并在隧道上进行传输。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。

## NAS-Initiated VPN隧道和会话建立过程：




图：NAS-Initiated VPN隧道和会话建立过程

1. 建立PPPoE连接

2. LAC对用户进行认证。

3. 建立L2TP隧道

   L2TP数据以UDP报文形式发送。L2TP注册了UDP端口1701，但是这个端口仅用于初始的隧道建立过程。L2TP隧道发起方（LAC）任选一个空闲端口（未必是1701）向接收方（LNS）的1701端口发送报文；LNS收到报文后，使用1701端口给LAC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。

   1. LAC检查用户的LCP协商中的认证信息（Domain、Username等），查找能够匹配的L2TP组，根据L2TP组的配置对某个LNS进行L2TP呼叫建立L2TP隧道。如果此时LAC发现L2TP隧道已经建立，则LAC发起会话连接，否则首先建立L2TP隧道。

2. LAC端向指定的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。

   LAC和LNS之间通过SCCRQ、SCCRP和SCCCN消息完成L2TP隧道的建立，并且双方都知道对方的Tunnel ID等信息，后续的数据报文都会添加Peer的Tunnel ID信息，这样接收者就可以知道收到的L2TP报文属于本地的哪个隧道。

4. 建立L2TP会话

   LAC和LNS使用ICRQ、ICRP和ICCN消息建立L2TP会话，这些消息都在前面建立的L2TP隧道中传递，并且都会添加隧道对端的Tunnel ID信息。

   在ICCN消息中，LAC端将用户CHAP response、response identifier和PPP协商参数传送给LNS，以便后续LNS与用户建立PPP连接。

5. LNS根据用户名、密码等信息对用户进行认证。

6. LNS对用户进行二次认证（可选）

7. LNS对用户在此认证（可选）

8. 用户与LNS之间建立PPP连接。

   完成了L2TP会话以后，LAC会将Client的相关PPP参数通过L2TP会话转发给LNS，LNS和用户进行PPP的认证。

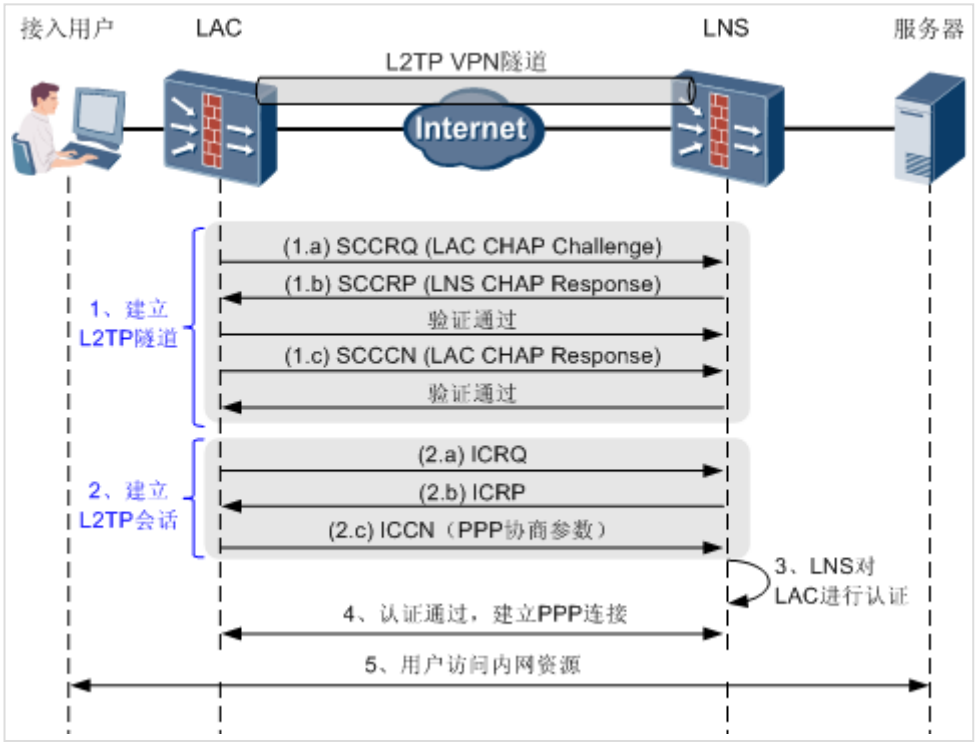
   LNS向用户分配地址然后建立PPP连接，注意此时的PPP连接在用户和LNS之间建立，并不是在LAC和LNS之间。

   此时的LAC也保持着和用户的PPP连接，用于将来自LNS的L2TP数据报文解封装以后通过PPP连接传递给Client。

9. 用户访问内网资源。

### LAC自动拨号隧道和会话的建立：

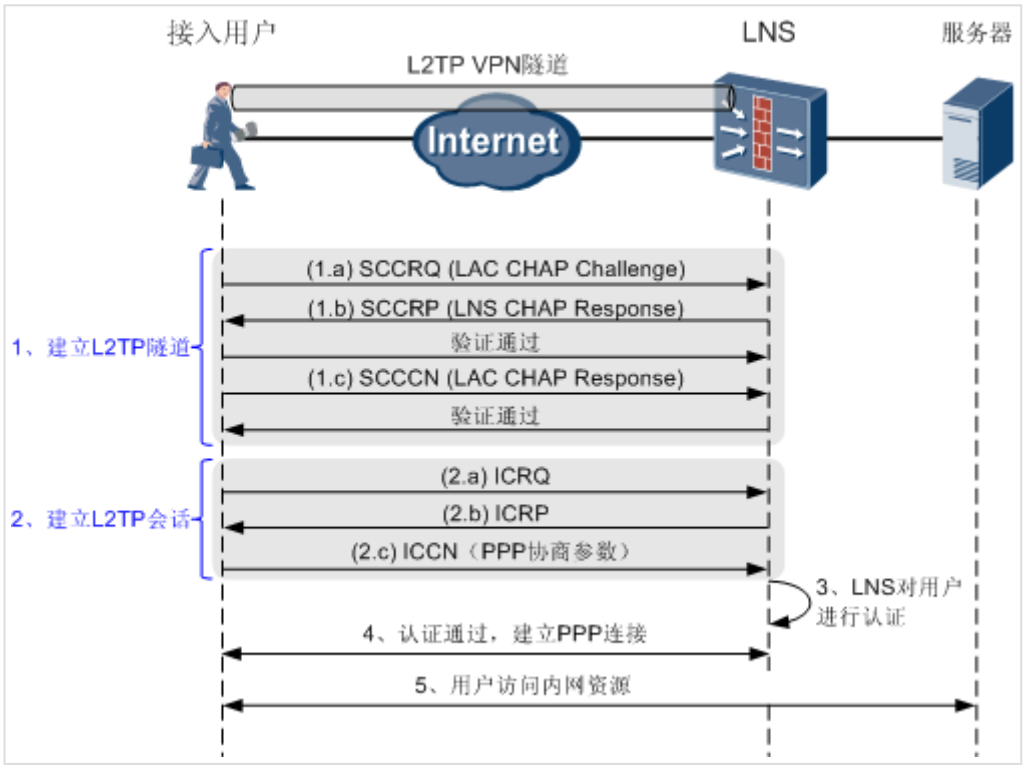
与触发建立隧道的方式不同，LAC自动拨号场景是无需触发的永久隧道。一旦配置完毕，即可建立永久隧道，并承载唯一的一条永久会话。LAC为LNS的唯一的客户端。




图：LAC自动拨号的隧道和会话建立过程

## Client-Initiated VPN隧道和会话的建立：

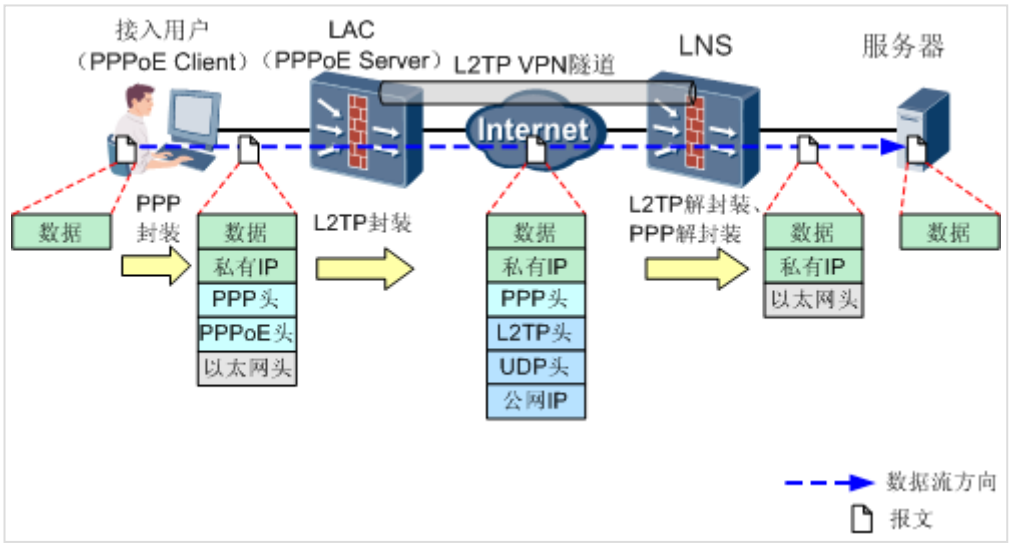
Client-Initiated VPN场景下，隧道建立过程与NAS-Initiated VPN相似。与NAS-Initiated VPN场景相比，Client-Initiated VPN场景相当于将Client和LAC合为了一个整体。




图：Client-Initiated VPN隧道和会话建立过程

## L2TP VPN的报文封装：

**NAS-Initiated VPN组网数据封装过程：**

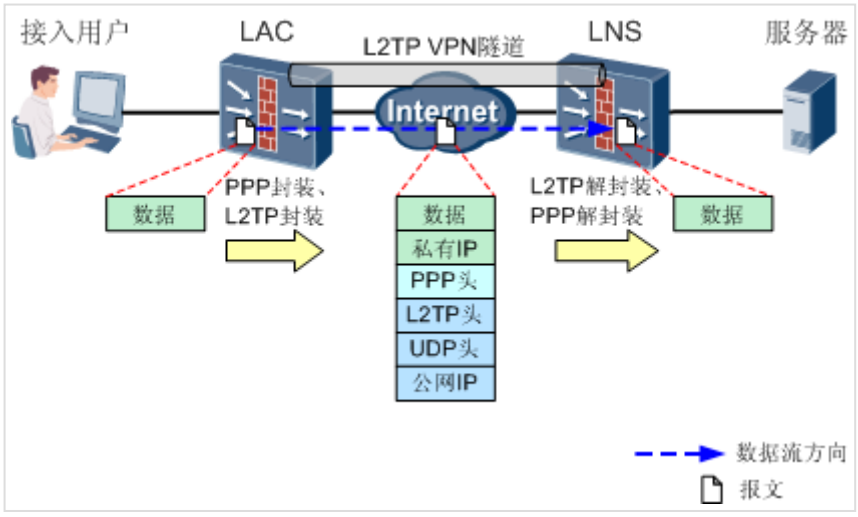



图：NAS-Initiated VPN场景组网报文封装过程

NAS-Initiated VPN组网中，接入用户访问内网服务器时：

1. 当隧道和会话均建立完成后，接入用户已获取LNS分配的地址，并用此地址来访问内网服务器。
2. 接入用户向LAC发起PPPoE拨号，为数据添加私有IP、PPP报文头和PPPoE报文头，并添加太网头后，发送给LAC。
3. LAC收到报文后，依次剥离以太网头、PPPoE报文头，并对报文依次封装L2TP报文头、UDP报文头，并添加公网IP，发送给LNS。
4. LNS收到报文后，首先对报文进行L2TP解封装，依次剥离公网IP、UDP报文头、L2TP报文头。之后进行PPP解封装，剥离PPP报文头。最后添加以太网头，并根据私有IP的目的地址将报文发送给内网服务器。
5. 服务器接收报文后，获取报文数据，并将响应报文发送给LNS。

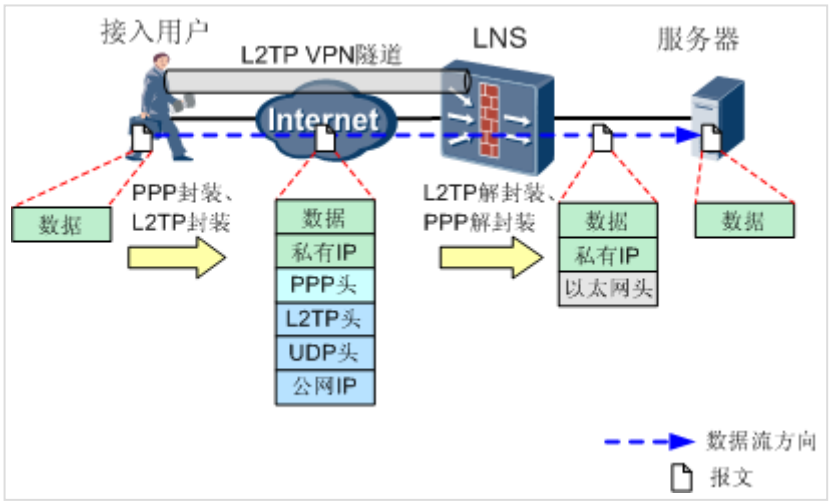
**LAC自动拨号组网数据封装过程：**




图：LAC自动拨号场景组网报文封装过程

LAC自动拨号组网中，PPP封装和L2TP封装仅限于LAC和LNS之间的报文交互。

### Client-Initiated VPN组网数据封装过程：




图：Client-Initiated VPN场景组网报文封装过程

## L2TP VPN的认证：

L2TP支持使用PAP和CHAP两种方式进行PPP认证。

### VT（Virtual-Template）接口：

PPP、Ethernet都是二层协议，它们之间不能直接互相承载。当用户配置PPPoE等二层协议时，这些**二层协议之间需要通过虚拟访问接口VA（Virtual-Access）进行通信**。前面已经提到，L2TP中会使用PPPoE协议。VT接口是用于配置虚拟访问接口的模板。在L2TP会话连接建立之后，LAC、LNS均需要创建虚拟访问接口用于和对端（即用户）交换数据。此时，系统将按照用户的配置，选择VT接口，根据该模板的配置参数（包括接口IP地址、PPP认证方式等）动态地创建虚拟访问接口。

命令行配置中，VT接口下可选择CHAP或PAP认证方式来对用户进行PPP认证。Web配置中不支持手工配置认证方式，系统优先选择CHAP方式，其次选择PAP方式。

### LAC自主拨号场景：

LAC自主拨号场景中，LAC侧不对用户进行认证，只在LNS侧对LAC配置的用户进行PPP认证（PAP或CHAP）。在命令行配置中，体现在VT接口下配置的PPP认证方式。

### Client-Initiated VPN场景：

Client-Initiated VPN场景中，在LNS侧对用户进行PPP认证（PAP或CHAP）。在命令行配置中，体现在VT接口下配置的PPP认证方式。

### NAS-Initiated VPN场景：

NAS-Initiated VPN场景中，L2TP可对用户进行两次PPP认证：第一次发生在LAC侧，第二次发生在LNS侧。只有一种情况LNS侧不对接入用户进行二次认证：启用LCP重协商后，不在相应的VT接

口上配置认证。这时，用户只在LAC侧接受一次认证。

另外，不论对于LAC或LNS，如果其配置的用户认证方式为“不认证”，则不论VT接口中使用何种认证方式，都不对用户进行认证。

以下对于认证方式的描述都是基于配置的用户认证方式不为“不认证”的情况。

- LAC端认证方式

  LAC端可对用户进行PAP或CHAP认证。在命令行配置中，使用VT接口下配置的PPP认证方式。

- LNS端认证方式

  LNS对用户的认证方式除由PPP认证方式决定外，还取决于配置的L2TP认证方式。L2TP认证方式有三种：代理认证、强制CHAP认证和LCP重协商。其中，LCP重协商的优先级最高，代理认证优先级最低。

  - LCP重协商

    如果需要在LNS侧进行比LAC侧更严格的认证，或者LNS侧需要直接从用户获取某些信息（当LNS与LAC是不同厂商的设备时可能发生这种情况），则可以配置LNS与用户间进行LCP重协商。LCP重协商使用相应VT接口配置的认证方式。此时将忽略LAC侧的代理认证信息。

  - 强制CHAP认证

    如果只配置强制CHAP认证，则LNS对用户进行CHAP认证，如果认证不通过，会话就不能建立成功。

  - 代理认证

    代理认证就是LAC将它从用户得到的所有认证信息及LAC配置的认证方式传给LNS，LNS会利用这些信息和LAC端传来的认证方式对用户进行认证。

    NAS-Initiated VPN中，在PPP会话开始时，用户先和LAC进行PPP协商。若协商通过，则由LAC初始化L2TP隧道连接，并将用户信息、认证信息等传递给LNS，由LNS根据收到的代理认证信息判断用户是否合法。

    代理认证与VT接口的PPP认证方式的关系：

    - LNS的PPP认证方式不能比LAC复杂。例如，如果LAC端配置的认证方式为PAP，而LNS配置的PPP认证方式为CHAP，则由于LNS要求的CHAP认证级别高于LAC能够提供的PAP认证，认证将无法通过，会话也就不能正确建立。
    - 其他情况下，如果LNS与LAC的认证方式不一致，LNS将采用LAC发送过来的认证方式进行协商，忽略VT接口配置的认证方式。

# 三种组网模式的对比

## 三种组网对比：

| 项目 | Client-Initiated VPN | NAS-Initiated VPN | LAC-Auto-Initiated VPN |
| --- | --- | --- | --- |
| 协商方式 | L2TP Client 和 LNS 协商建立L2TP隧道和L2TP会话、建立 PPP 连接 | 接入用户使用 PPPoE 拨号触发 LAC 和 LNS 之间协商建立 L2TP 隧道和 L2TP 会话，接入用户和 LNS 协商建立 PPP 连接 | LAC 主动拨号，和 LNS 协商建立 L2TP 隧道和 L2TP 会话、建立 PPP 连接 |
| 隧道和会话关系 | 每个 L2TP Client 和 LNS 之间均建立一条 L2TP 隧道，每条隧道中仅承载一条 L2TP 会话和 PPP 连接 | LAC 和 LNS 的连接可存在多条 L2TP 隧道，一条 L2TP 隧道中可承载多条 L2TP 会话 | LAC 和 LNS 之间建立一条永久的 L2TP 隧道，且仅承载一条永久的 L2TP 会话和 PPP 连接 |
| 安全性 | LNS 对 L2TP Client 进行 PPP 认证（PAP 或 CHAP），安全性较高 | LAC 对接入用户进行认证，LNS 对接入用户进行二次认证（可选），安全性最高 | LAC 不对用户进行认证，LNS 对 LAC 配置的用户进行 PPP 认证（PAP 或 CHAP），安全性低 |
| 回程路由配置 | LNS 上会自动下发 UNR 路由，指导回程报文进入 L2TP 隧道，无需手动配置 | LNS 上会自动下发 UNR 路由，指导回程报文进入 L2TP 隧道，无需手动配置 | LNS 上需要手动配置目的地址为网段的静态路由，或者在 LAC 上配置 easy-IP 方式的源 NAT |

- Client-Initiated VPN：其优点在于接入用户不受地域限制。此场景适用于员工使用PC、手机等移动设备接入总部服务器，实现移动办公。
- NAS-Initiated VPN：接入用户（PC）通过PPPoE拨入LAC，由LAC通过Internet向LNS发起建立隧道连接请求。接入用户地址由LNS分配，对接入用户的认证可由LAC侧代理完成，也可两侧都对接入用户做认证。当所有L2TP用户都下线时，隧道自动拆除以节省资源，直至再有用户接入时，重新建立隧道。此组网适用于分支机构用户向总部发起连接，且一般用于分支机构的用户不经常访问企业总部的情况。
- LAC-Auto：分支机构员工感知不到隧道存在，不需要使用用户接入。LAC为分支机构的多个用户提供L2TP服务，免去了每个用户使用L2TP都需要先拨号的麻烦
  这种组网下，LNS只对LAC进行认证。其缺点为：分支机构用户只要能够连接LAC即可使用L2TP隧道接入总部，而不需被认证。存在一定的安全隐患。此时用户接入总部以通过设备的用户认证功能对接入总部的用户进行认证，从而提高安全性

## L2TP和PPTP区别：

- L2TP：公有协议、UDP1701、支持隧道验证，支持多个协议，多个隧道，压缩字节，支持三种模式
- PPTP：私有协议、TCP1723、不支持隧道验证，只支持IP、只支持点到点

**PPTP：**

点对点隧道协议（PPTP）是由包括Microsoft和3com等公司组成的PPTP论坛开发的，一种点对点隧道协议，基于拨号使用的PPP协议使用PAP或CHAP之类的加密算法，或者使用Microsoft的点对

点加密算法MPPE。

**L2TP：**

第二层隧道协议（L2TP）是IETF基于L2F（Cisco的2层转发协议）开发的PPTP后续版本，是一种工业标准Internet隧道协议。

两者的主要区别主要有以下几点：

1. PPTP只能在两端间建立单一隧道，L2TP支持在两端点间使用多隧道，这样可以针对不同的用户创建不同的服务质量
2. L2TP可以提供隧道验证机制，而PPTP不能提供这样的机制，但当L2TP或PPTP与IPSec共同使用时，可以由IPSec提供隧道验证，不需要在第二层协议上提供隧道验证机制
3. PPTP要求互联网络为IP网络，而L2TP只要求隧道媒介提供面向数据包的点对点连接，L2TP可以在IP（使用UDP），FR，ATM，x.25网络上使用
4. L2TP可以提供包头压缩。当压缩包头时，系统开销（voerhead）占用4个字节，而PPTP协议下要占用6个字节

**L2TP什么情况下需要强制认证?**

> 在NAS模式下。且LNS不信任LAC，配置了强制认证的情况下

> 参考文档：华为HedEx文档。