第二节　运营商的 VPDN 服务

在 Network-based VPN 模式下，VPN 的构建、管理和维护由运营商控制，允许用户在一定程度上进行业务管理和控制。功能特性集中在网络侧设备处实现，用户网络设备只需要支持网络互联，无需特殊的 VPN 功能，因此客户使用运营商的 VPN 业务，可以沿用原来的不支持 VPN 功能的路由器等设备，保护原有的投资。

Network-based VPN 包括 MPLS VPN 等业务；MLPS VPN 在组网业务里面已经有介绍。在介绍一下目前广泛应用的运营商 VPDN 服务。

大家指导，目前的宽带接入大多数使用 PPPOE 拨号接入互联网。类似的，使用 VPDN 拨号可以接入运营商的内网。

VPDN（Virtual Private Dialup Network）即虚拟专用拨号网络，是 VPN 技术的一种，主要应用于拨号（电话、ADSL）接入的用户组建虚拟专网的场合。VPDN 具有投资小见效快、实现简单等优点，因此各运营商都在大力发掘客户的 VPDN 组网需求。目前运营商提供的 VPDN 业务一般采用 L2TP 技术。

VPDN 组网业务是运营商在互联网基础上开放的，基于窄带或宽带拨号方式，以二层隧道技术为主而组建企业虚拟专用网络的一种业务。以 L2TP/L2F 技术在两端建立安全隧道（Tunnel），通过虚拟专用的通道来传输信息，防止来自 Internet 的恶意攻击，确保用户通信数据的安全。

L2TP（Layer 2 Tunnel Protocol）第二层隧道协议，是为在用户和企业的服务器之间透明传输 PPP 报文而设置的隧道协议。支持内部地址分配.。主要组成有 LAC、LNS 等。

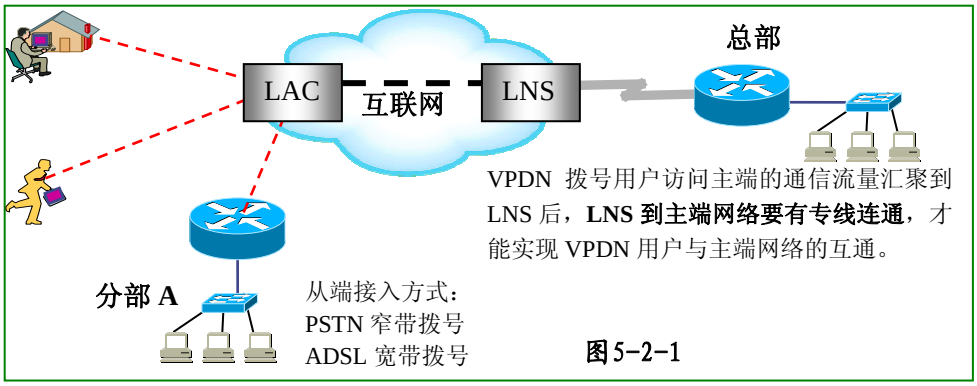
LAC（L2TP Access Concentrator）L2TP 访问集中器，附属在交换网络上的具有 PPP 端系统和 L2TP 协议处理能力的设备，LAC 一般就是一个网络接入服务器（NAS，Network Access Server），它通过 PSTN/Internet 为用户提供网络接入服务。

LNS（L2TP Network Server），用于处理 L2TP 协议的服务器。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，表示承载在隧道连接中的每个 PPP 会话过程。

企业用户可以采取窄带（PSTN 网络）和宽带（ADSL 接入、PON 接入等）的方式来使用 VPDN 组网业务。

VPDN 组网在接入方面涉及到主端与从端两种角色：

主端是企业网络的核心，企业的主要网络与信息资源放在主端。从端是企业网络的分支，从端通过 VPN 网络访问与使用主端的资源。主端通过固定专线连接到运营商的网络的 LNS，从端通过 VPDN 拨号进入 VPN 网络，对主端的访问数据通过 LAC 送到 LNS，再到达主端网络。



象其它“点对多点”的 VPN 业务一样，在申请业务时，运营商先给你分配一个 VPN 群组，并用一个编号代表你的网络。当 VPDN 用户的拨号登录网络是，运营商的接入服务器通过拨号帐号的后缀域名来区分这个用户属于哪个客户的 VPN 群组，并按照所属群组进行通信的安全隔离，帐号形式如：market@abc.gd。帐号的后缀域名一般在业务开通前由客户与运营商协商而定，一般情况下企业采用企业自身的中文拼音或英文名称作为其 VPDN 域名。VPDN 组网业务只提供企业内部虚拟网络的访问，不支持访问公网信息资源。VPDN 组网用户若需访问公网信息资源，则需另外采用合适的上网业务方式实现。

VPDN 拨号进入 VPN 网络的过程与一般普通用户拨号上 internet 的过程是很相似的。

一般普通宽带拨号用户经过的网络环节如下：

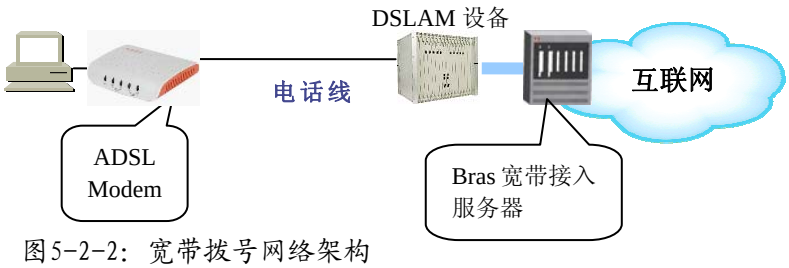


图 5-2-2：宽带拨号网络架构

而宽带 VPDN 拨号用户经过的网络环节如下：

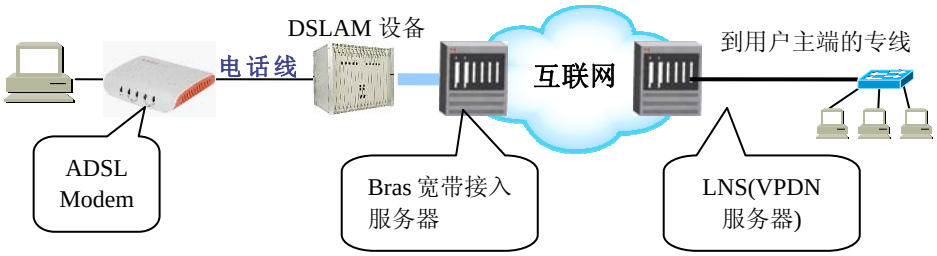


图 5-2-3：VPDN拨号网络架构

从上面两个图来看，VPDN 拨号与拨号上 Internet 的网络连接情况是很相似的，主要的不同是对于 VPDN 客户，客户的主端需申请一条专线连接到 LNS 服务器。VPDN 拨号建立的隧道从 LAC 处开始，到 LNS 处终结。VPDN 拨号用户对主端网络的通信流量汇聚到 LNS 后，LNS 到主端网络要有专线连通，才能实现 VPDN 用户与主端网络的互通。

主端到 LNS 的接入方式可以选择第三章里介绍的组网专线。所需带宽可根据 VPDN 的用户并发数和每个用户平均带宽来测算。

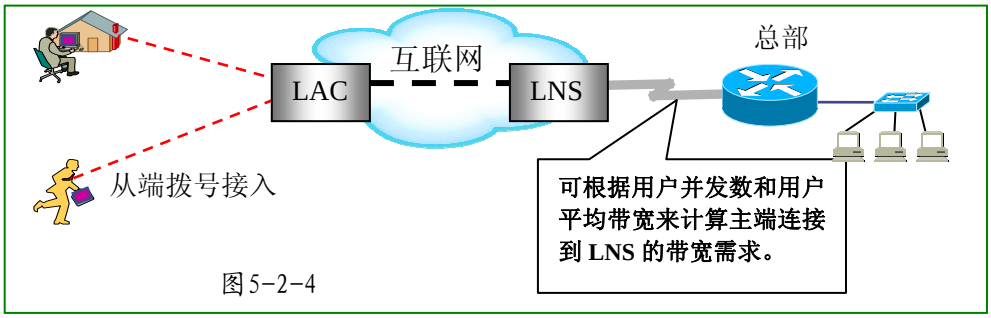


图 5-2-4

●VPDN 案例：

某省某石油公司拟实现全省加油站的组网，希望采用低成本、低维护量、使用放心、服务可靠、可扩展的的网络方案。经过考虑联网需求与电信业务价格，该公司选用了 VPDN 业务，将企业的 Intranet 构建在 Internet 之上，同时保障一定的数据安全性。

各个加油站采用 ADSL 接入，提供 RJ45 接口，无需额外购置路由器、交换机，一次性投资少，使用和维护的门槛低；采取包月形式，可实时在线。各个加油站 512K 接入，足以满足其应用需求，实现远端加油站用户快速、高效、安全地访问企业内部信息资源。扩展性强，拓展新的加油站或有其他站点加盟，开通 ADSL 线路，开放帐号密码即可使用，总部互联带宽也可根据业务发展平滑升速，无需对物理线路及路由器等设备进行改造。

作为 VPDN 主端的总部采用 10M 专线连接到 LNS。

该组网特点

（1）拨号终端用户使用的地址仍然是私有 IP 地址，但是终端用户能够“借用”公网的通路（L2TP 隧道）访问公司的私网，LNS 是连接 Internet 公网和公司私网的桥梁。

（2）数据的安全性有保障：公网上的其他非 VPDN 用户不能访问私有网络资源；该公司的 VPN 帐号格式为“加油站的拼音@公司名称”，只有用公司的 VPN 帐号拨入的连接才能访问该公司内网；同时将 IP 地址与网卡 MAC 地址绑加强安全性。

（3）由于 IP 网络缺乏 QoS 保障，带宽 QoS 保障没有无法达到 TDM 类专线的效果。一般来说运营商的 IP 骨干网的带宽是比较充裕的，因此该问题不是很明显。

●基于移动网络的 VPDN：

3G 高速上网席卷而来，随时随地高速无线访问互联网成为现实。移动办公迎来美好的前景。使用运营商的 3G 无线网络来实现 VPN，是上一节所介绍的使用有线宽带实现 VPN 的一种应用拓展，将应用拓展到无线的领域，实现真正意义上的移动办公。移动 3G 技术提供了大带宽的无线接入技术，成为移动办公应用的基础设施之一。

基于 3G 移动网络的 VPN 组网也一样有 2 种方式，即：客户可以自建 VPN 服务器，然后用户通过二次拨号进入 VPN 网络；客户不建设 VPN 服务器，直接使用 3G 的 VPDN 业务，直接拨号进入 VPN 网络。

智能化终端一般都使用运营商 VPDN 拨号，如物流公司的手持式扫描仪可以嵌入 3G 模块，在智能化终端里设置好 VPDN 拨号的帐号与密码，在使用终端时会自动拨入企业内网，上传与下载相关数据，非常便捷。

当 VPDN 用户拨号 NSP（网络服务提供商）的网络访问服务器 NAS（Network Access Server），发出 PPP 连接请求，NAS 收到呼叫后，在用户和 NAS 之间建立 PPP 链路，然后，NAS 对用户进行身份验证，确定是合法用户，就启动 VPDN 功能，与公司总部内部连接，访问其内部资源。拨号服务器与公司的企业网关之间直接建立 tunnel，在此过程中用户的数据如 IPX、IP 等协议，经过系列封装，通过 tunnel 传递到企业网关，再进行解包，传递到企业内部。

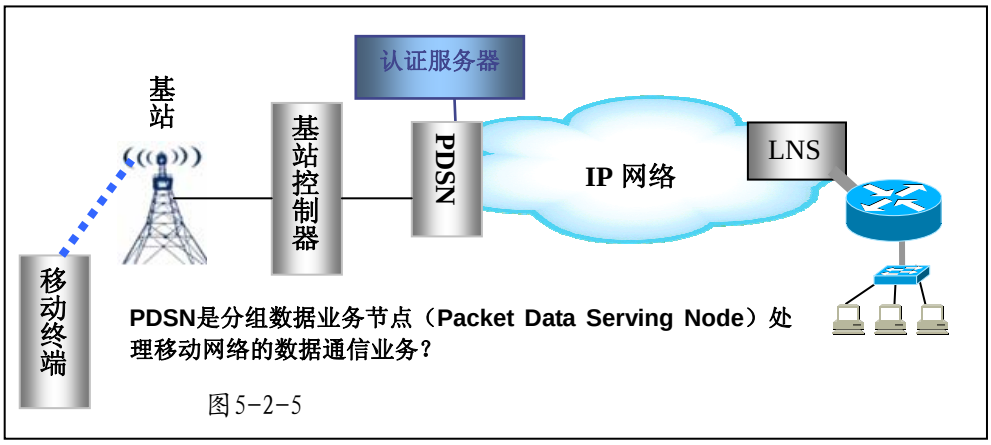


图 5-2-5

PDSN 作为 VPDN 业务的 LAC 设备，主要负责 L2TP 隧道的发起和建立。接入 AAA 主要完成业务终端的 VPDN 业务接入认证、授权、计费，并实现各种业务控制及用户终端的漫游等功能。LNS AAA 服务器主要完成业务终端访问客户网络的认证、授权。

LNS 设备是负责无线 VPDN 客户接入的网络设备（如路由器），和 PDSN 一起完成 L2TP 隧道的建立。LNS 设备可部署在中国电信机房中，也可部署在客户网络中。

●基于移动网络的 VPDN 应用案例：

广东某物流公司为物流人员配备 CDMA 终端，使物流人员可以通过终端实时将送件和收件的信息发送到公司的服务器，使客户可以通过互联网查询物件的送抵情况。

物流人员的数量为 250 人，CDMA 终端的信息传送约占用 100k 左右的的带宽。

方案如下图：

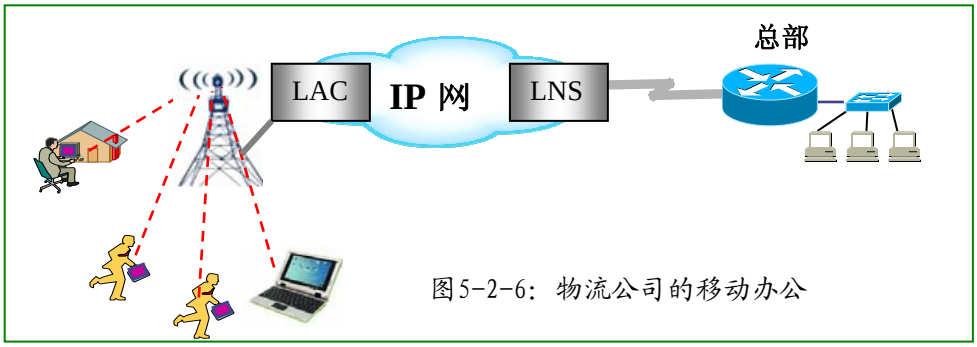


图 5-2-6：物流公司的移动办公

物流人员使用智能 CDMA 终端，运行客户端软件时可以自动拨号连接到 VPN 网络。客户总部申请一条电路连接到运营商的 LNS 服务器，将物流人员 VPDN 拨入后的通信数据汇集传输到公司总部；带宽需求根据用户并发数和用户平均带宽来测算。

因此该物流公司需要申请的业务为：

①总部到 LNS 的 IP 专线；

② 250 个 CDMA 的 VPDN 帐号，供物流人员的终端拨入 VPN 网络用。