综合VPDN实现方案技术探讨

**摘要：对固网移动网融合后为更好的向企业客户提供多种接入方式的端到端的解决方案进行了研究，解决在统一平台上引进移动分组网的APN技术及IP城域网中的VPDN技术后，实现对企业用户的统一认证、计费、管理、维护、统计等相关内容。**

　　本系统中涵盖综合VPDN平台、[路由器](http://product.dzsc.com/product/searchfile/7239.html" \t "_blank)、GGSN、BARS等多厂商设备组网实现了专线、in[te](http://product.dzsc.com/product/searchfile/10366.html)rnet、MPLS VPN等企业接入方式，动态L2TP、静态L2TP方式、GRE连接方式等多种用户接入方式，满足各种用户接入需求，有效利用网络资源，并提供认证和加密等安全策略。

　　1.引言

　　中国联通移动通信网络迅速发展，特别是移动互联网业务的迅猛发展，许多企业有强烈的随时随地直接接入企业内部网络的需求，实现移动办公、远程抄表、气象监控、移动视频监控、远程电站监控、地质监测等业务。

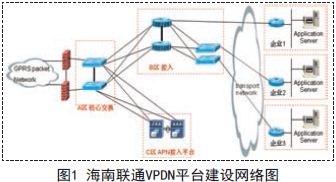
　　随着接入企业及用户的增加，如何对终端接入企业网络进行控制，实现更加安全地访问企业网络，如何管理企业终端用户成为目前行业应用系统建设中重点要解决的问题。为更好发展企业用户，为企业用户提供集中认证和授权业务，为企业专网接入提供用户信息集中管理服务，保障企业专网接入的安全性，保障核心网安全，减少对现有GGSN性能的影响，使网络结构更清晰、设备功能更明确、降低投资成本，需建设一套APN接入管理平台，满足企业通过移动网、固网方式接入企业专网的安全和管理需求。

　　2.技术实现方案

　　2.1 VPDN拓扑设计

　　根据可靠性先进性等网络设计原则，我们针对移动网分组网络、IP城域网的IP数据包的传输特点，设计以下拓扑网络。

　　该网络结构通过分层设计，能够满足企业用户小数据量，突发性的特点。



　　在整个平台的网络建设中，划分A、B、C3个区。A区为综合VPDN管理接入平台的核心交换转发区，主要用来提供在移动网分组域核心网/IP城域网和综合VPDN管理平台之间的数据路由转发。B区是企业接入区，用来提供企业用户的专线接入。

　　C区是综合VPDN管理平台，用来提供企业托管认证服务和管理服务。整个平台通过主从互备的两台防火墙将移动网分组域核心网/IP城域网和综合VPDN管理平台隔离开，以保证综合VPDN管理平台不会受到来自移动网分组域核心网/IP城域网方向的攻击。对于来自企业侧方向的恶意攻击，在L[NS](http://ns.dzsc.com/)接入路由中配置相应的ACL规则来保证平台的安全性。采用此种分层网络，可以加速数据转发，快速汇聚VPDN数据。依附该网络，提供基于L2TP和GRE两种隧道方式的系统接入方案。一种是基于L2TP的接入方案，一种是基于GRE的接入方案。

　　和这两种方案对应着三种不同的系统接入认证流程。

　　2.2 系统本地接入流程

　　综合VPDN管理接入平台由于和GGSN设备密切相关，因此APN的接入流程也包含了多样性。根据GGSN和LNS路由设备之间隧道建立的方式，主要划分为基于L2TP和基于GRE两种方式的接入流程。其中在基于L2TP接入的方式当中，根据GGSN设备LNS参数的配置方式，又可以划分为基于静态配置LNS参数和基于动态配置LNS参数两种接入流程。这两种接入流程对于企业侧客户使用透明，但流程对GGSN设备的要求会有所不同。

　　2.2.1 基于L2TP方式的移动网分组域接入流程

　　（1）基于LNS参数静态配置的方式

　　在整个接入流程中，AAA认证只发生一次，就是LNS向AAA发起的认证，以验证MS合法性。认证通过后，会返回给GGSN相应的终端IP地址或者IP地址池（取决业务和AAA配置）。采用静态配置，需要在GGSN设备上设置好APN对应的LNS IP、TunnelID、Tunnel password等属性值。

　　具体的认证流程如下：1）在MS侧，MS发送激活请求消息的时候，携带APN以及用户名，建议格式为username@domain,其中domain为APN标识。2）SGSN收到消息后，解析APN,得到GGSN地址，向该GGSN发送PDP激活请求消息，并透传PCO信息。

　　3）GGSN根据预先配置的LNS参数信息，向LNS[服务器](http://product.dzsc.com/product/searchfile/5368.html)发起L2TP隧道请求，建立L2TP隧道。GGSN在收到的激活请求消息里，解析得到用户名和密码并透传。4）LNS将获得的用户名密码封装在R[ADI](http://adi1.dzsc.com/)US报文中，发起认证请求。5）AAA认证通过后，向LNS返回终端用户的IP地址属性并在L2TP会话中将IP地址或IP地址池返回给GGSN.6）GGSN在PDP报文中将终端用户的IP地址携带给SGSN.7）MS从PDP报文中获得所需的IP地址。8）MS根据IP地址和企业网[服务器](http://wiki.dzsc.com/info/1807.html" \t "_blank)建立VPN连接。

　　（2）基于LNS参数动态配置的方式

　　在动态配置LNS参数的L2TP的接入流程中，仍旧发生二次认证。一次认证是GGSN和AAA服务器之间，GGSN会将NAI域名发送到AAA服务器，AAA根据NAI域名返回所需MS对应的LNS参数值。二次认证发生在LNS和AAA服务器之间，LNS会将用户名和密码发送到AAA服务器，AAA认证通过后，将IP地址或IP地址池返回给LNS设备。这种方式需要GGSN能够接受AAA返回的动态LNS隧道参数以及需要确认GGSN向AAA发送的认证包的参数信息，也需要运营商确认GGSN设备支持此种功能。

　　2.2.2 基于GRE方式的移动网分组域接入流程

　　基于GRE隧道方式的接入流程是移动网分组域网络中常用的方式，在该方式下的认证流程只需要GGSN和AAA之间的一次认证通过后，MS即可获得所需要的IP地址。

　　具体的认证流程如下：1）MS向SGSN发起激活PDP报文请求。2）SGSN收到请求报文后，解析APN得到GGSN的IP,进行PDP报文的创建。3）GGSN根据用户名得到AAA服务器的IP地址，然后将用户名和密码封装在AAA报文中发起认证请求。4）AAA验证后向GGSN返回MS属性值。5）GGSN向AAA发送计费开始报文。6）GGSN向SGSN发送创建PDP报文响应。7）GGSN收到AAA发送的计费报文响应。8）MS从SGSN返回的PDP报文中获得IP.9）MS进行VPN连接，开始和企业应用服务器进行通信。

　　2.2.3 基于l2TP方式的固网接入方式

　　基于L2TP方式的固网接入方式具体的认证流程如下：

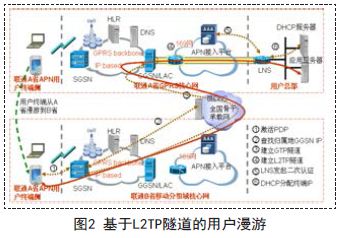
　　1）终端通过ADSL的形式拨号到BRAS设备。2）BRAS设备向固网AAA发送APN的认证请求，请求携带APN标示，以及用户名，格式为username@domain.3）固网AAA会根据用户名中domain字段认证是否是合法用户，并向BRAS返回LNS地址以及隧道密钥。（或者固网AAA把请求转发给APNAAA.APN-AAA做此操作。）4）BRAS根据LNS参数，和LNS建立l2TP会话。5）LNS向APNAAA发送二次认证请求。认证请求中携带用户的用户名和密码。6）APN-AAA认证用户名和密码是否正确。认证通过，返回LNS用户的地址池。7）LNS向GGSN推送终端拨号所需IP地址。8）终端获得AAA授权的IP地址。9）终端使用此IP地址和企业网建立PPP连接。

　　2.3 系统漫游接入流程

　　当使用移动网分组域的VPDN用户在本地注册，但是漫游到外地时，如何来接入到VPDN网络中去呢？在移动网分组域网络中，VPDN用户的漫游情况依靠SGSN,HLR和DNS设备的配合来确定归属地GGSN的IP地址，由拜访地的SGSN向归属地的GGSN创建PDP报文，建立GTP隧道。PDP会话创建之后，由归属地的GGSN向企业LNS或接入设备建立L2TP隧道或者GRE隧道，最后完成终端用户的IP地址分配，直至建立PDP.漫游用户建立L2TP隧道或GRE隧道的流程类似，只是在建立隧道时有所区别，下面将详细讨论漫游时用户采用L2TP隧道方式接入平台的情况。

　　基于L2TP方式的分组接入流程：

　　这里的LNS参数信息可以预先配置在GGSN设备里，或者由VPDN AAA来分配。我们不做详细区分。下面举个例子，图2是在A省注册的用户漫游到B省的网络拓扑。



　　当终端用户从A省漫游到B省时，用户的漫游流程如下：

　　1）终端用户向拜访地B省SGSN发起激活PDP报文请求；

　　2）SGSN根据终端所在区域，附加网络运营商标识形成完整的APN,发送到DNS进行解析，获得归属地GGSN的IP地址；

　　3）B省SGSN向归属地A省GGSN发起创建PDP报文请求，建立GTP隧道；

　　4）A省GGSN向LNS发起L2TP呼叫，建立L2TP隧道和会话；

　　5）LNS向AAA发起二次认证，使终端用户获得认证；

　　6）DHCP分配给终端IP地址。

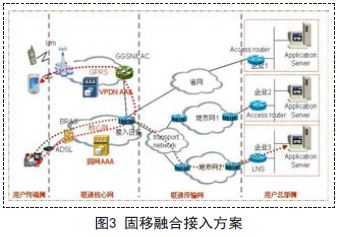
　　2.4 固移融合方案

　　综合V P D N管理平台不仅能够支持无线接入，还要支持固网接入包含ADSL的接入。因为大多数企业往往不会局限于一种接入方式，而是无线接入，宽带接入同时使用，如图3所示。

　　综合VPDN管理接入平台支持固网VPDN用户的接入，当采用L2TP隧道接入方式时，需要两次认证过程：第一次为BRAS设备向固网AAA发起的认证请求，用于获取LNS的相关参数；第二次为LNS设备向综合VPDN管理平台的AAA发起的认证请求，用于用户身份的认证。第一次认证主要用于根据APN域名获取LNS的相关参数，因此它可以用三种方式实现：1）直接在BRAS设备上静态配置APN域名和LNS参数的对应关系，由BRAS设备在本地完成第一次认证。

　　BRAS必须支持静态配置APN和LNS相关参数，对固网AAA基本没有配合上的要求。

　　2）在固网AAA上配置APN域名和LNS参数的对应关系，由固网AAA在第一次认证的应答消息中将LNS参数返给BRAS设备，这种方式需要在固网AAA上对企业开户。3）第一次认证和第二次认证都在综合VPDN管理平台的AAA上完成，固网AAA只做转发，即当固网AAA收到企业用户（域名）的接入请求时，将接入请求转发给综合VPDN管理平台的AAA进行处理。



　　3.结束语

　　综合V P D N方案主要解决移动网、固网客户随时随地安全统一接入到企业的内部网络，实现对企业用户的统一认证、计费、管理、维护、统计等相关内容，实现移动办公、远程抄表、气象监控、移动视频监控、远程电站监控、地质监测等业务，为运营企业拓展行业用户带来一体化的解决方案。（作者：孙照斌，钟颋，佟晶）

技术资料出处:电子技术网  
该文章仅供学习参考使用，版权归作者所有。  
因本网站内容较多，未能及时联系上的作者，请按本网站显示的方式与我们联系。[现在联系我们](tencent://message/?uin=1335406878&Site=www.dzsc.com&Menu=yes)

http://www.dzsc.com/img/images/data/about02.gif

[4G智能手机天线设计解决方案](http://www.dzsc.com/data/html/2013-9-3/103920.html)

2010年全球移动数据消费量增长了2.6倍。这是移动数据使用量连续三年接近3倍的增幅。到2015年，全球移动数据业务量有望增长到2010年的26倍。导致这种戏剧性增长的关键因素之...

[针对移动通信多模市场的数字多模分布式无线覆盖系统](http://www.dzsc.com/data/html/2013-1-18/102585.html)

随着移动通信网络的多年高速发展，目前国内运营商均具备多个运营网络。任何一个运营网络均处于技术发展和网络演进的过程中，该过程将长期存在。另外，用户量的增大，数据业...

[基站天线与移动通信干扰抑制](http://www.dzsc.com/data/html/2012-12-15/102300.html)

覆盖、容量、吞吐率是移动通信运营商最为关注的三大指标。随着移动通信的不断发展普及，网络覆盖的广度与深度都已经达到相当高的水平。可是在实际运营中，运营商经常会接到...

[LTE架构下的多媒体资源分发方案](http://www.dzsc.com/data/html/2012-10-22/101791.html)

随着移动通信和互联网技术的飞速发展，人们对数据业务的需求，尤其是对多媒体数据业务的需求变得越来越强烈。在传统互联网领域，多媒体业务可以通过内容分发网络（CDN）来开...

|  |
| --- |
| **VPDN组网技术** |
| 一、VPDN简介 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。  二、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1所示：  http://source.xze.cn/files/upload/003047003/5910/20062793726562.jpg  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  A)L2TP协议结构   http://source.xze.cn/files/upload/003047003/5910/200627101122890.jpg  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。  B) 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。  C) 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之间对PPP帧的隧道模式如图3所示：  http://source.xze.cn/files/upload/003047003/5910/200627101620781.jpg  两种典型的L2TP隧道模式  a. 由远程拨号用户发起。  远程系统拨入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，在这里MA5200充当LAC  b. 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通道的呼叫建立流程可如图4所示：  http://source.xze.cn/files/upload/003047003/5910/20062710194671.jpg  L2TP通道的呼叫建立流程  6)L2TP优势  a. 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。  b. 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。  c. 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。  d. 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。  e. 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。  f. 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。 |