VPN 混合组网的研究

刘占洋　徐蕾　方滨华

（中国铁通哈尔滨分公司）

摘要：在铁通公司 VPN 现网运行中全部采用的是基于 VPSL VPN，随着业务的发展，且由于铁通公司网络覆盖存在部分盲点，已不能完全满足部分用户的需求，制约了 VPN 业务的快速发展。采用基于 IPSec VPN 作为 VPSL VPN 的补充实现混合组网是现阶段迫切解决的问题。

关键字：VPN　混合组网　双网卡　双网关

1、引言：

基于 IPSec VPN 与基于 VPSL VPN 是在共用网络上建立专用网络的两种不同 VPN 技术。其中，基于 VPSL VPN 是在铁通公用互联网设备上提供的一种点到多点的 VPN 业务,特点是在铁通公用互联网设备上通过数据配置实现与 Internet 的隔离。目前，铁通哈尔滨分公司利用 VPSL VPN 已实现如“哈尔滨市医疗保险中心、哈尔滨铁路局医疗保险中心、哈尔滨城市通智能卡有限公司”等多家大型机构的组网。随着业务的不断发展，当用户部分接入点有移设或新增需求时，存在因铁通不具备接入能力而被迫离网的现象，导致用户对铁通的服务不满。因此已迫在眉睫研究其它 VPN 实现方式来解决上述问题。基于 IPSec VPN 是通过相应的隧道、加密和认证技术来保证用户内部网络数据在公网上安全传输，从而真正实现网络数据的专有性,特点是只要各联网接入点能够连接到 Internet 即可实现 IPSec VPN 组网，这是与 VPSL VPN 相比最大的优势。

2、IPSec VPN独立组网实现方式：

上面说到，IPSec VPN对数据进行了加密和认证。那么，这是如何实现的呢？答案就是隧道协议。VPN通过隧道协议对数据进行加密和认证。目前铁通IPSec VPN使用非常安全的IPSec隧道协议。实现原理如下：

❶ A 通过主识别号找到 VDN，提交许可证到 VDN 请求认证通过，并要求和 B 建立通信隧道

❷ VDN 通知 A 已经通过认证

❸ B 上网后也通过主识别号找到 VDN 提交许可证到 VDN，请求 VDN 认证通过，寻求是否可以和别的点建立通信隧道

❹ VDN 通知 B 已经通过认证

❺ VDN 将 B 的在线信息告诉 A

❻ VDN 将 A 的在线信息告诉 B

❼ A 通过获得的 B 的 IP 找到 B 并请求和 B 建立通信隧道

❽ B 响应 A 请求，并和 A 交流数据

上图中的 VDN 服务平台位于铁通北京分公司，平台管理帐号由铁通各省分公司负责业务的开通和维护。

由于 VDN 平台的强大功能，使得 APN 终端设备建立 VPN 隧道变得非常安全和快速，也使得安装变得相当简单。在已经配置上网线路的情况下，只需要配置由

VDN 平台分配的虚拟域名、主机名和许可证号三个参数就可以让 APN 设备之间快速建立 VPN 隧道。把复杂的参数配置过程就这样简单化了。所以 APN 的安装过程就是配置上网线路和这三个参数的过程，其中配置上网线路跟普通路由器几乎没有区别。目前铁通公司 IPSec VPN 终端设备采用奥联公司（型号：GW100）。

3、VPLS VPN独立组网实现方式：

VPLS VPN 是一项利用绑定在 IP 包中的标签通过网络进行数据包转发的技术。采用标签交换，一个标签对应一个用户数据流，非常易于用户间数据的隔离，保证客户信令和数据流的私密性。从用户的角度看来，**VPLS VPN** 就是一个虚拟的广域网交换机，在用户的 VPN 内把数据帧转发到正确的目的地。铁通 **VPLS VPN** 的基本模型：用 MPLS PE（Provider Edge Router）设备创建合理的私有的用户 VPN。把用户站点以 PPPOE 的连接方式通过 BAS 设备（CE）与 PE 设备连接起来提供 VPLS 服务。一旦用户数据包到达 PE 设备之后，PE 设备决定以太网的帧转发，通过 PE 在 MPLS 网络上交换数据。PE 设备使用 MPLS 的标签分发协议（LDP）在铁通的网络云图内创建合理的、全网格的以太网虚拟电路。一个通过以太网连接到铁通 VPLS 网络的用户站点可以互通多个其他用户终端站点，这样就实现了多点以太网服务。MPLS 网络的 PE 设备通过给每个用户 MPLS VPN 创建独立的虚拟路由转发表或者 VRF 表来实现多重 VPN。以太网 VPLS 服务环境中，PE 设备维护虚拟交换实例 VSI（Virtual Switch Instance）。虚拟交换实例实质是每个用户 VPLS 独有的两层转发表。PE 设备根据特定 VPLS VPN 内以太网帧交换所需要的转发信息创建独立的 VSI 表。通过 PE 的 VSI 就可以实现 MAC 地址学习。当有新的转发信息时，MAC 地址就会进行更新。

4、基于 IPSec VPN 与 VPSL VPN 混合组网的测试过程

测试环境：

1、 中心点：

应用服务器：采用 WINDOWS XP 操作系统，双网卡（一个连接铁通 VPLS VPN，另一个连接本地局域网。）

网络：一条铁通 VPLS VPN 接入线路（ADSL 私网静态 IP）

一条中国电信“我的 e 家”宽带（PPPOE 上网方式）

测试软件：腾讯通、局域网文件及打印机共享

2、 分支点：

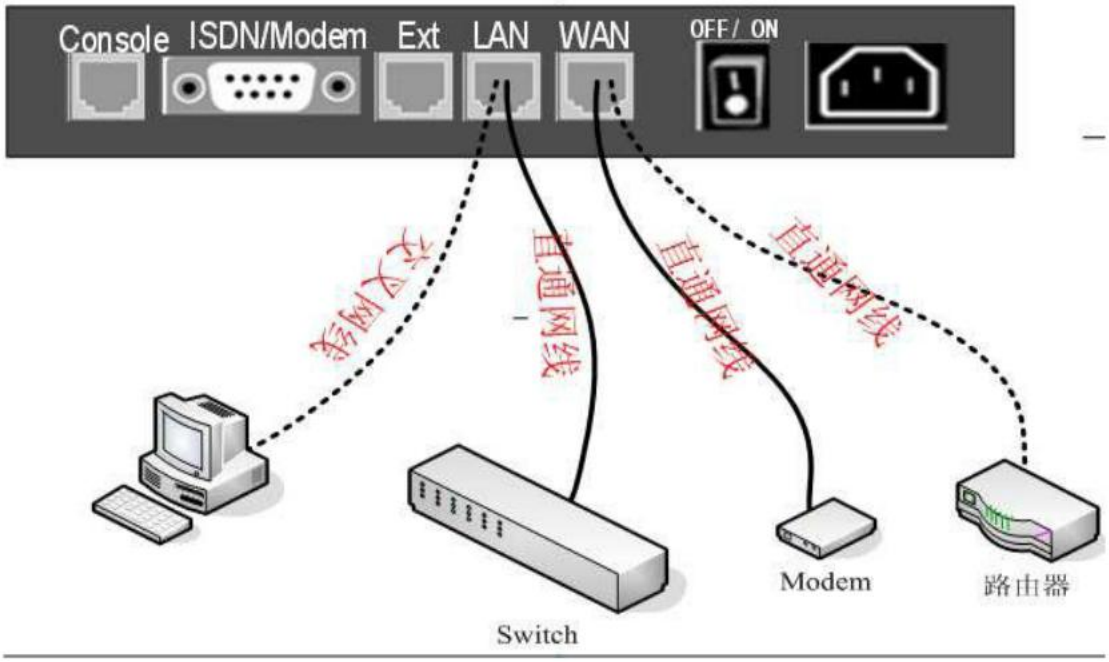
电脑：一台普通 PC 机

网络：铁通 ADSL（静态 IP）+路由器组建的局域网内

测试软件：腾讯通、局域网共享

测试过程：

1、 在中心点和分支点分别安装一台奥联 IPSec VPN 终端（型号：GW100），并将互联网线路连接至外网接口，同时将内网接口分别连接应用服务器的内网网卡和分支点测试电脑的网卡。



2、 正确将奥联 IPSec VPN 终端联入网络后，正常使用需要进行以下信息配置，具体配置过程如下：

第一步：奥联 IPSec VPN 终端 LAN 口 IP 配置

① 修改本地配置电脑 IP 及网关配置

② 使用缺省 IP 登陆奥联 IPSec VPN 终端 web 管理界面

③ 为奥联 IPSec VPN 终端配置新的 LAN IP 地址

第二步：奥联 IPSec VPN 终端 WAN 口上网方式配置

第三步：奥联 IPSec VPN 终端许可证信息配置

3、 为实现在一台应用服务器上通过双网卡实现基于 IPSec VPN 与 VPSL VPN 混合组网，需要在应用服务器上设置双网卡双网关，将铁通 VPSL VPN 网关设置为默认网关，通过在应用服务器上增加静态路由将到 IPSec VPN 网段的路由指向中心点奥联 IPSec VPN 终端。具体 DOS 命令为：route -p add 。

5、混合组网分析：

混合组网有两种主要的实现方式：一种是通过在中心点增加一台电信级路由器，将路由器的两个外网口分别连接 IPSec VPN 接入线路和 VPSL VPN 接入线路，内网口连接应用服务器；另一种实现方式是通过在中心点服务器上安装双网卡，

代替路由器的两个外网口，分别连接 IPSec VPN 接入线路和 VPSL VPN 接入线路，同时将铁通 VPSL VPN 网关设置为默认网关，并在应用服务器上通过 DOS 命令 route 增加静态路由，将到 IPSec VPN 网段的路由指向另一块网卡连接的奥联 IPSec VPN 终端。双网卡实现方式，投资成本低廉，适用于小型 VPN 网络，而路由器实现方式，虽然投资成本较高，但性能高且稳定，因而适用于中、大型 VPN 网络。

6、结束语：

随着用户 VPN 应用需求的不断变化以及电信运营商之间互联互通的不断改善，IPSec VPN 以其灵活的实现方式，必将在 VPN 领域得到更广泛的应用，同时 IPSec VPN 与 VPLS VPN 的混合组网应用也将长期存在。一些研究表明在下世纪将会有 70%～80%的商务使用 VPN 设备。公司希望花费不高的代价来传输商务信息。VPN 在这方面起了很重要的作用，它提供了减少开支、提高服务、维护客户基础的方法。虽然 VPN 在理解和应用方面都是高度复杂的技术，甚至确定其是否适用于本公司也一件复杂的事件，但在大多数情况下 VPN 的各种实现方法都可以应用于每个公司。即使不需要使用加密数据，也可节省开支。此外，在未来几年里，客户和厂商很可能会使用 VPN，从而使电子商务重又获得生机，毕竟全球化、信息化、电子化是大势所趋。

参考文献：

[1] 《VPLS 虚拟专用以太网业务技术入门》上海贝尔
[2] 《APN OLYM2008 使用说明书》深圳奥联科技有限公司