基于 L2F 的 CISCO 虚拟拨号网络构建方法

姜军 任庆东 （大庆石油学院计算机系 151400）

摘要：VPDN(虚拟私有拨号网络)是 Cisco 公司提出的远程存取虚拟专网的解决方案。本文对 VPDN 的技术原理、实现方法进行了详细分析，并给出了一个具体应用配置实例。

关键词：VPN VPDN Tunnel L2F Internet

1. 前言

VPN(虚拟私有网络)为企业用户提供了一种跨越 Internet 访问企业私有网络信息的方式。VPN 是一种服务。VPN 有许多优点：企业可使用它创建分布式 LAN，节省了组建企业广域网的费用；对企业出差在外办公的工作人员可以拨号访问本地 ISP 的访问服务器，即可以访问企业网络内部私有信息，从而节省了长途电话费用；对于 ISP，VPN 为其提供增值服务，ISP 不局限于提供基本的访问 Internet 功能，使 ISP 与厂商联系更加紧密。据美国 Infonetics Research 企业的虚拟专网研究报告指出，当企业放弃租用的数据专线，而改用虚拟专网连接远程网站时，整个广域网络的成本可节约 20％到 47％。至于从远程存取虚拟专网，则是企业以电话拨号方式进行远程存取所需成本的 60％到 80％。IP Sec 或 Tunnel(隧道)技术是 VPN 实现的关键。VPDN(虚拟私有拨号网络)是 Cisco 企业提出的远程存取虚拟专网的解决方案，它基于 Tunnel 技术。本文对 VPDN 的技术原理和实现方法进行探讨并给出了应用实例。

2. VPDN 的技术原理

VPDN 的拓朴结构图见图 1，企业用户用 PPP 协议拨号到 ISP 的 NAS(访问服务器)，NAS 与企业网关协商，用 L2F 创建 Tunnel，对 PPP 进行封装成数据包在 Tunnel 内传输，在 Tunnel 的出口 企业网关拆包后进行 PPP 协商。若成功，在企业用户和企业网关建立了一个 PPP 连接。就好象企业用户直接拨入到企业网关一样，尽管实际上拨入到 ISP 的 NAS。

VPDN 的关键在于如何创建遂道(tunnel)，隧道是将一种通信协议封装成数据包的机制，此通信协议在遂道的入口和出口的网络之间进行协商。遂道的入口和出口作为 CISCO 路由器的一个遂道端口，遂道端口本身类似于一个硬件端口，但它由软件配置来实现。在遂道内传输的数据包格式见图 2。

遂道包括三种协议：乘客协议(passenger protocol)、封装协议(encapsulating protocol)和运载协议(carrier protocol)。Passenger protocol 为被封装在遂道内的协议，在 VPDN 中此协议为 PPP 或 SLIP。encapsulating protocol 用来创建维护和撤除遂道，在 VPDN 中 encapsulating protocol 使用 L2F(第二层转发)。carrier protocol 用来运载 passenger protocol。由于 IP 协议具有健壮的路由功能，因此，L2F 首先选用 IP 来对其进行运载。L2F 和 IP 没有任何依赖关系存在。F. R、X. 25 VCs(虚电路)，ATM SVC(交换虚电路)都可以用来作为 carrier protocol。

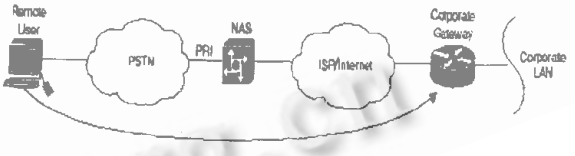

图 1 VPDN 拓扑结构图

VPDN 提供了端到端的传输，远程用户的主机和企业 LAN 主机不需要特殊的软件。PPP 认证由企业网关进行管理，与 ISP 无关，VPDN 支持 PAP、CHAP、TACACS＋、RADIUS、一次性口令认证。远程用户的 IP 地址由企业网关提供，企业网关和 ISP 可分别对拨入用户记帐。

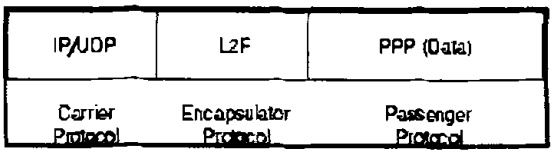

图 2 VPDN 拓扑结构图

3. VPDN 的实现方法

远程用户经电话网拨入到 NAS，初始化连接，NAS 使用 CHAP 或 PAP 对远程用户端提供的用户名进行认证以决定用户是否申请 VPDN 服务。申请 VPDN 服务用户名应具有一定的结构，如 smith@hp.com 或 NAS 维持一张用户名和服务的对照表。对照表指定企业网关的 IP 地址。若未申请虚拟拨号服务，NAS 提供传统的 Internet 访问功能。此时，用户主机的地址分配和授权均由 NAS 指定。

若此用户申请 VPDN 服务，并且遂道尚未建立，则应用 L2F 对遂道进行初始化，具体步骤如下：

·NAS 和 Corporation gateway 对对方的共享密钥进行认证，NAS 发送 L2F－CONF，它包含 NAS 的名字和随机挑战(Challenge)值 A。Corporation gateway 收到 L2F－CONF 后，向 NAS 返回 L2F－CONF，它包含 Corporation gateway 的名字，随机挑战值 B 和密钥 A'，A' 为对 NAS 口令和 A 进行 MD5 加密值。

·NAS 收到 L2F－CONF 后，将 NAS 口令同 A 一起进行 MD5 加密得到值与 A' 进行比较，若相同，NAS 向 Corporation gateway 发送 L2F－OPEN，它包含有密码 B'，B' 为 Corporation gateway 的口令和随机挑战值 B 一起进行 MD5 加密所得值。

·Corporation gateway 一旦接收到 L2F－OPEN，将本地的口令和 B 一起进行 MD5 加密，所得值同 B' 进行比较，若匹配，Corporation gateway 向 NAS 发送 L2F－OPEN，它包含值 A'。此后，NAS 发送的信息都包含 B'，Corporation gateway 发送的信息都包含 A'。至此，一个遂道便被建立了，见图 3。

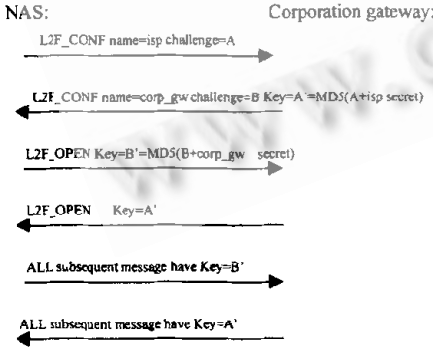

图 3 L2F 初始化 Tunnel 的过程

当 Tunnel 建立后，NAS 向 Corporation gateway 发出一个初始化连接，请求建立一个拨号会话，并且为拨号连接分配一个未被使用的 MID(复用标识号)，MID 代表了在遂道内的一个连接，此初始化连接也包含了用户认证信息，Corporation gateway 对拨号用户进行认证，以决定接收连接或拒绝连接。若使用 CHAP 认证，初始化建立信息包括挑战值、用户名、口令。若使用 PAP 认证，则仅包括用户名和明文口令。

若 Corporation gateway 接受了初始化配置连接，Corporation gateway 为 PPP 连接建立一个虚拟端口。此虚拟端口类似于直接拨入到 Corporation gateway 的 PPP 端口。对用户的授权和地址分配方法和直接拨入到 Corporation gateway 的用户是同样的。

4. 应用实例

图 4 是应用 VPDN 构建虚拟拨号 VPN 应用实例的拓扑结构图：

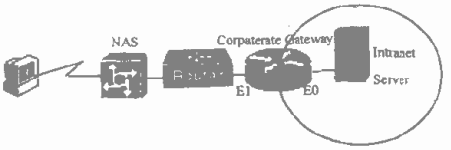

图 4 应用实例拓扑结构图

Corporation Gateway 外部接口 E1 的 IP 地址：10.1.1.1，内部 IP 地址为 10.65.0.010.65.255.255，将 Corporation Gateway 用 access－list 命令配置为防火墙，不允许外部网络请求公司内部的的 Telnet 服务。内部网络用户可以请求外部网络的任何服务。NAS 接口 E0 的 IP 地址：10.2.1.1。客户端使用 win95 拨号网络。win95 客户机分别以 NAS 用户 jj 和公司网络用户 jmith@hp.com 拨号入网，则此两用户的对公司网络的使用权完全不相同。公司网络用户在 Corporation Gateway 进行认证，得到 IP 地址为公司内部使用的 IP 地址。因此，它可以使用公司网络提供的 FTP、telnet 等服务。NAS 用户得到 IP 地址为外部网络的 IP 地址。因此根据 Corporation Gateway 的防火墙规则，它向公司内部网络提出的 telnet 请求均被拒绝。部分系统配置如下：

NAS:

```
Nas(config)# username jj pass 0 jj
```

```
/ * 激活 VPDN 服务 * /
Nas(config) # vpdn enable
/ * 配置本地 ISP 名字 corporate gateway 名字和共享密钥 * /
Nas(config) # username isp password 0 there
Nas(config) # username hp - gw password 0 hello
/ * 指定公司网络名 建立 Tunnel 使用的本地名 网关 IP 地址 * /
Nas(config) # vpdn outgoing hp.com isp ip 10.1.1.1
/ * 使用 IP pool 为客户端分配 IP 地址 * /
Nas(config) # ip address - pool local
Nas(config) # ip local pool default 10.2.1.10 10.2.1.26

Nas ( config ) # chat - script star "" " at&fs0 = 1e1q0v1&d2&c1 \ q3" OK
Nas(config) # interface Ethernet0
Nas(config - if)) # ip address 10.2.1.1 255.255.0.0
Nas(config) # exit
/ * 配置异步口参数 * /
Nas(config) # interface Group - Async1
Nas(config - if) # ip unnumbered Ethernet0
Nas(config - if) # encapsulation ppp
Nas(config - if) # async dynamic routing
Nas(config - if) # async mode interactive
Nas(config - if) # ppp authentication chap
Nas(config - if) # peer def ip add pool
Nas(config - if) # group - range 1 16
Nas(config - if) # exit

Nas(config) # line 1 16
Nas(config - line) # autoselect ppp
Nas(config - line) # login local
Nas(config - line) # modem InOut
Nas(config - line) # transport input all
Nas(config - line) # speed 115200
Nas(config - line) # flowcontrol hardware
```

Corporation Gateway:

```
/ * 激活 VPDN 服务 * /
Corp(config) # vpdn enable
/ * 配置本地 ISP 名字 、corpate gateway 名字和共享密钥 * /
Corp(config) # username hp - gw password 0 hello
Corp(config) # username isp password 0 there
/ * VPDN 用户名 口令 * /
Corp(config) # username jsmith@hp.com password 0 test
/ * 建立 Tunnel 使用的 NAS 名字、本地名 、虚拟异步口端口号/
Corp(config) # vpdn incoming isp hp - gw virtual - template 1
/ * 配置虚拟异步口端口参数 * /
Corp(config) # interface Virtual - Template1
Corp(config - if) # ip unnumbered Ethernet0
Corp(config - if) # encap ppp
Corp(config - if) # ppp authentication chap
Corp(config - if)peer def ip add 10.65.1.10
Corp(config - if) # exit
/ * 配置路由器防火墙, Corporation 内部网可访问外部服务
防火墙外部网不能 telnet 到内部网主机上 * /
Corp(config) # int eth 1
Corp(config - if) # ip add 10.1.1.1 255.255.255.0
Corp(config - if) # ip access 102 in
Corp(config - if) # exit
Corp(config) # access 102 permit tcp any any establish
Corp(config) # access 102 deny tcp any any eq 23
Corp(config) # access 102 permit tcp any any
```

参考文献

[1] Cisco systems Document CD, 1997

[2] Cisco, " Solutions for Virtual Private Dialup Networks" , http://www cisco.com, 1998

[3] Cisco, " Virtual Private Dialup Network", http://www cisco.com, 1998

(来稿时间:1999 年 3 月)