维普资讯 http://www.cqvip.com

基于 VPN 技术的组网方案探讨

杨彦彬[1,2]　冯久超[1]

(华南理工大学电信学院　广州 510640)[1]　(广东邮电职业技术学院通信系　广州 510630)[2]

摘　要　基于 VPN 技术，提出了一种为大公司分布在不同区域的分支机构提供一种非常廉价、安全、灵活自如的网络信息传输解决方案，并通过组建试验网络的测试，证明了方案的可行性。

关键词　虚拟专用网，隧道技术，访问控制列表

Exploring for a Networking Scheme Based on VPN Technology

YANG Yan-bin[1,2]　FENG Jiu-chao[1]

(School of Electronic and Information, South China University of Technology, Guangzhou 510640, China)[1]

(Department of Communication, Guangdong Vocational College of Post & Telecommunication, Guangzhou 510630, China)[2]

Abstract　Based on VPN technique, a cheap, security and flexible network solution for big companies with many branches is proposed. It is also proven that this solution is available by testing a constructed network.

Keywords　Virtual private network, Tunneling technique, Access control list

1　引言

近年来，随着中国企业自身的发展壮大与国际化，很多大公司的业务已遍及了中国大陆主要省市及海外市场，公司在工作上信息和话务来往越来越多。各分支机构的互访一般是租用专线，这样的连接方式要支付昂贵的通信费用，缺乏灵活性，同时对于企业地理位置的改变也不能很好地适应[1]。

客观上，利用 VPN(Virtual Private Network)技术组建的网络，它能屏蔽公共网络的结构，也能对网络中传输的数据进行加密处理，使得整个企业网络逻辑上成为一个内部网络，这能为大公司分布在不同区域的分支机构提供一种非常廉价、安全、灵活自如的网络信息传输解决方案。

在这种背景下，各大公司纷纷希望利用 VPN 技术组建自己的网络。文献[2]介绍了 VPN 的种类和提供模型，并按运营商对扩展性的观点和用户对灵活性的观点对模型进行了比较。以北美骨干承载网络为例说明了即使提供的总站点数相同，提供少数大型网络比多数小型网络困难，这对我们组建 VPN 有一定的参考作用。在利用 VPN 技术组建新网络时，如何保留原网络的应用，文献[3]也给出了几点建议，值得我们参考。不过很多文献都只是从理论角度给出 VPN 组网时采用何种模型，从路由可控、QoS 颗粒度等方面进行比较，如需组网并没有一个行之有效的组网方案可以借鉴，正是由于这种原因，本文给出了一个具体的组网方案，并通过组建试验网络的测试，证明了方案的可行性。

2　VPN 技术简介

2.1　VPN 的概念

文献[1]对 VPN 做了以下定义：首先，VPN 是一个网络；这意味着它在属于该 VPN 的不同网络实体间交换信息。第二，它是私有的，意味着它具有私有网络的全部特征。基于以上的特征，我们认为 VPN 是在公众网络上所建立的虚拟私有专用网络，该网络拥有与企业内部专用网络相同的安全、可靠和可管理的功能特点，它替代了传统的拨号访问，利用 INTERNET 公网资源作为企业专网的延续，节省昂贵的接入费用。对于 VPN 的详细内容还可以参考文献[4]。

2.2　VPN 的优点

VPN 具有如下的优点：

良好的安全性：资料安全保密性与可靠的传输性。VPN 架构中采用了多种安全机制，如隧道(Tunneling)、加密(Encryption)、认证(Authentication)、防火墙(Firewall)等技术，通过上述的各项网络安全技术，确保资料在公众网络中传输的安全可靠。

低成本：企业不必租用专线建设专网，不必大量的网络维护人员和设备投资。VPN 在设备的使用量及广域网络的频宽使用上，均比专线式的架构节省，故能使企业网络的总成本降低。根据分析，在 LAN-to-LAN 连接时，用 VPN 较使用专线的成本节省 30%～50% 左右；而就远程访问而言，用 VPN 更能比直接拨接至企业内部网络节省 60%～80% 的成本[5]。

容易扩展：VPN 的架构有弹性，当有必要将网络扩充或是变更网络架构时，VPN 可以轻易地达到目的，VPN 的平台具备完整的扩展性，大至企业总部的设备，小至各分公司，甚至个人拨号用户，均可被包含于整体的 VPN 架构中，同时，VPN 的平台亦具有对未来广域网络频宽扩充及连接架构更新的弹性。

管理方便：VPN 网络路由设备配置简单，无需增加太多的网络设备及物理线路使网络的管理较为轻松；不论分公司或是远程访问用户再多，均只需通过互联网的路径进入企业网络。

2.3　VPN 的安全技术

目前 VPN 主要采用四项技术来保证安全，这四项技术分别是隧道技术(Tunneling)、加解密技术(Encryption & De-

杨彦彬　在职博士生，讲师，主要从事数据通信方面的教学与研究工作；冯久超　博士，教授，博导。

维普资讯 http://www.cqvip.com

cryption)、密钥管理技术(Key Management)、使用者与设备身份认证技术(Authentication)。

(1) 加解密技术是数据通信中一项较成熟的技术,VPN可直接利用现有技术。

(2) 密钥管理技术的主要任务是如何在公用数据网上安全地传递密钥而不被窃取。现行密钥管理技术又分为SKIP与ISAKMP/OAKLEY两种。SKIP主要是利用Diffie-Hellman的演算法则,在网络上传输密钥;在ISAKMP中,双方都有两把密钥,分别用于公用、私用。

(3) 身份认证技术最常用的是使用者名称与密码或卡片式认证等方式。

(4) 隧道是指在公用网建立一条数据通道(隧道),让数据包通过这条隧道传输。现有两种类型的网络隧道协议,一种是二层隧道协议,用于传输二层网络协议,它主要应用于构建远程访问虚拟专网(Access VPN);另一种是三层隧道协议,用于传输三层网络协议,它主要应用于构建企业内部虚拟专网(Intranet VPN)和扩展的企业内部虚拟专网(Extranet VPN)。

网络隧道技术涉及了三种网络协议,即网络隧道协议、隧道协议下面的承载协议和隧道协议所承载的被承载协议。本文采用采用的是虚拟路由器+IP隧道VPN的方式组网[6],该网络具有以下特点:

(1) 可直接采用现有路由协议(如OSPF,IS-IS等)完成VPN内各分支路由的传递和转发,不需要对路由协议进行扩展。

(2) 众多不同的VPN用户共用一个VPN骨干网络拓扑,只须调整本地VPN接入,而无须全程调整VPN网络拓扑即可实现VPN用户的增加或删减,具有快捷的VPN业务生成特点。

3 理论组网方案

本文采用虚拟路由器+IP隧道VPN的方式组网,给出了图1的理论组网方案。预期实现穿越INTERNET的整个企业网络在逻辑上成为一个内部网络,可以自由访问的目标。其中的OSPF区域为电信运营商的网络,本文只关注如何利用公网实现互联,并不涉及公网的组网方式。有兴趣的读者可以参考文献[2,7],它们为建设VPN核心网络提供了相应的理论参考。

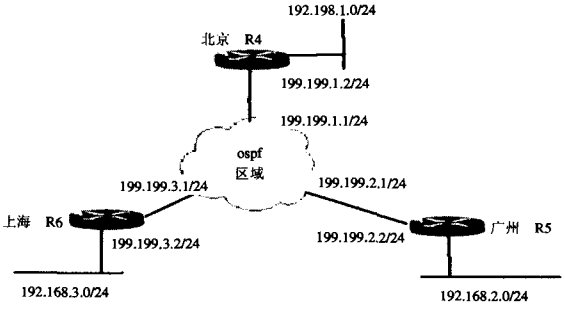

图1 虚拟路由器+IP隧道VPN理论组网方案

公司总部是信息存放、处理的中心,网络内部主机数量多,数据流量大,安全性和实时性要求高。采用电信光纤接入因特网,高性能地接入服务器。各分部内部建有中等规模的局域网,同时通过当地电信提供的宽带接入方式接入因特网。

4 组建试验网

为了验证方案的可行性,我们搭建了图2的虚拟路由器+IP隧道VPN试验网。其中:路由器ospf1,ospf2,ospf3有用于模拟INTERNET网,运行OSPF协议。路由器4,5,6则为VPN网关。计算机192.168.1.2,192.168.1.3,192.168.2.2,192.168.3.2则模拟局域网内的计算机。企业与核心网直接有固定IP的专线相连。

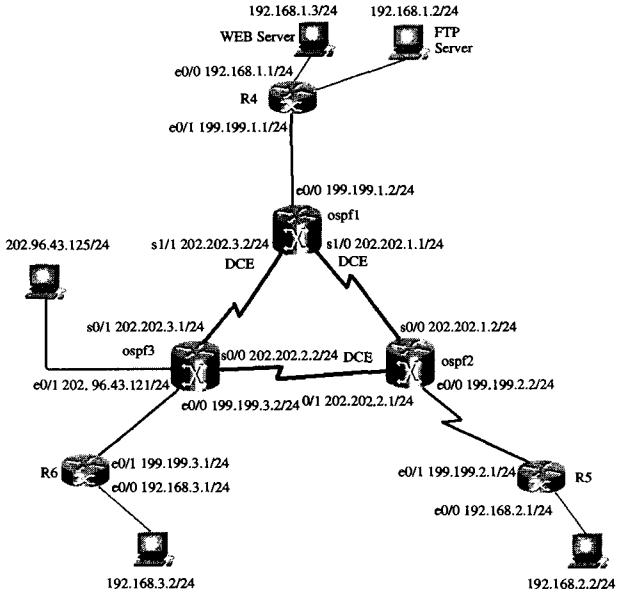

图2 虚拟路由器+IP隧道VPN试验网方案

(1) 路由器R4上的配置如下:

```
r4# sh run
! Current configuration:
!
hostname r4
!
access-list 100 permit ip 192.168.1.0/24 192.168.2.0/24
access-list 100 deny ip any any
access-list 101 permit ip 192.168.1.0/24 192.168.3.0/24
access-list 101 deny ip any any
access-list 150 permit tcp 192.168.3.2/32 192.168.1.2/32 eq 21
access-list 150 permit tcp 192.168.3.2/32 192.168.1.2/32 eq 20
access-list 150 deny tcp 192.168.3.0/24 192.168.1.2/32 eq 21
access-list 150 deny tcp 192.168.3.0/24 192.168.1.2/32 eq 20
access-list 150 permit ip any any
ip filter on
ipsec on
crypto isakmp enable
crypto isakmp key 123456 address 199.199.2.1
crypto isakmp key 123456 address 199.199.3.1
!
interface serial1/0
!
interface serial1/1
!
interface serial1/2
!
interface serial1/3
!
interface eth0/0
ip address 199.199.1.1/24
crypto map r4
!
interface eth0/1
  ip address 192.168.1.1/24
!
interface async0/0
!
interface tunnel0
  ip address 192.168.254.1/24
  tunnel source 199.199.1.1
  tunnel destination 199.199.3.1
tunnel key 123456
tunnel checksum
```

维普资讯 http://www.cqvip.com

```
   tunnel sequence-datagrams
ip access-group 150 in
!
interface tunnel1
   ip address 192. 168. 253. 1/24
   tunnel source 199. 199. 1. 1
   tunnel destination 199. 199. 2. 1
   tunnel key 123456
   tunnel checksum
tunnel sequence-datagrams
!
crypto ipsec transform-set r4r5 ah-md5-hmac esp-3des
!
crypto ipsec transform-set r4r6 ah-md5-hmac esp-3des
!
crypto map r4 1 ipsec-isakmp
match address 101
set peer 199. 199. 3. 1
set transform-set r4r6
!
crypto isakmp policy 1
authentication pre-share
!
ip route 0. 0. 0. 0/0 199. 199. 1. 2
ip route 192. 168. 2. 0/24 192. 168. 253. 2
ip route 192. 168. 3. 0/24 192. 168. 254. 2
!
line console 0
line aux 0
line vty 0 9
!
! end
```

(2) 路由器 R5 上的配置如下：

```
r5# sh run
! Current configuration:
!
hostname r5
!
interface eth0/0
ip address 199. 199. 2. 1/24
!
interface eth0/1
ip address 192. 168. 2. 1/24
!
interface eth4/0
!
interface async0/0
!
interface tunnel1
ip address 192. 168. 253. 2/24
tunnel source eth0/0
tunnel destination 199. 199. 1. 1
!
no logging on
!
ip route 0. 0. 0. 0/0 199. 199. 2. 2
ip route 192. 168. 1. 0/24 192. 168. 253. 1
!
line console 0
line aux 0
line vty 0 9
!
! end
```

(3) 路由器 R6 上的配置如下：

```
r6# sh run
! Current configuration:
!
hostname r6
!
access-list 1 permit 192. 168. 3. 0/24
access-list 101 permit ip 192. 168. 3. 0/24 192. 168. 1. 0/24
access-list 101 deny ip any any
ipsec on
crypto isakmp enable
crypto isakmp key 123456 address 199. 199. 1. 1
!
interface eth0/0
ip address 199. 199. 3. 1/24
ip nat outside
crypto map r6
!
interface eth0/1
ip address 192. 168. 3. 1/24
ip nat inside
!
interface eth4/0
!
interface async0/0
!
interface tunnel0
   ip address 192. 168. 254. 2/24
   tunnel source 199. 199. 3. 1
   tunnel destination 199. 199. 1. 1
   tunnel key 123456
   tunnel checksum
   tunnel sequence-datagrams
!
crypto ipsec transform-set r6r4 ah-md5-hmac esp-3des
!
crypto map r6 1 ipsec-isakmp
   match address 101
   set peer 199. 199. 1. 1
   set transform-set r6r4
!
crypto isakmp policy 1
   authentication pre-share
!
crypto map r6 1 ipsec-isakmp
   match address 101
   set peer 199. 199. 1. 1
   et transform-set r6r4
!
crypto isakmp policy 1
   authentication pre-share
!
no logging on
!
ip route 0. 0. 0. 0/0 199. 199. 3. 2
ip route 192. 168. 1. 0/24 192. 168. 254. 1
ip nat on
ip nat inside source list 1 interface eth0/0
!
line console 0
line aux 0
line vty 0 9
!
! end
```

通过组建图 2 的试验网，可以实现上海、广州分部所有计算机访问北京总部的 Web 服务器，查看公司内部公告。北京总部通过访问控制列表 ACL，只允许各分部的特定计算机 192. 168. 2. 2，192. 168. 3. 2 访问北京总部 FTP 服务器上的机密资料，其它计算机被拒绝访问。上海分布通过采用网络地址转换 NAT，还可以访问公网的资源 202. 96. 43. 125。

建立 VPN 后，可为内部网络用户提供专业的防火墙保护。可实现各应用系统等网络版应用系统的远程互联，减少投资成本，最大限度地发挥公司应用系统的效率，实现无纸化办公。各分公司可以像在同一间办公室里一样共享并同步应用 OA 系统，使公司管理更加统一规范，保证各种信息流的实时更新，确保公司管理高效、透明、安全、快捷，信息的及时传递，通知任务的及时执行，提高工作效率。通过“网上邻居”共享数据文件，访问远程的企业资源数据库，中心的网络管理员可以对整个 VPN 网络进行集中的状态监控和远程管理配置，可以在各个 VPN 节点设置动态的流量管理策略，为企业实时业务和多媒体数据流提供良好的带宽保证。构建了这个网络之后，还可以实现其他如视频会议、VoIP、视频监控等扩展应用，节省大量长途话费。对于提供 VOIP 等扩展应用，文献[8]对 VoIP 网关的分配提供了理论参考。文献[8]介绍了在分配 VoIP 网关时，考虑安全性和流量可用性的同时，又要考虑到网络的存活性。通过对比基于遗传算法、模拟退火算法、贪婪算法，根据仿真结果得出了文献[8]提出的五大算法的优越性。

结束语 本文根据当前许多大公司需要跨地域组网的需求，提出了采用虚拟路由器＋IP 隧道 VPN 技术进行组网，可以满足大公司廉价、安全、灵活组网的要求。通过组建的试验网络测试，证明了方案的可行性和科学性，对于解决该类问题具有很好的参考价值。

维普资讯 http://www.cqvip.com

参 考 文 献

[1] Venkateswaran R. Virtual private networks. Potentials, 2001, 20(1): 11-15

[2] Rosenbaun G, Lau W, Jha S. An analysis of virtual private network solutions. Local Computer Networks, 2003, 10: 395-404

[3] Yurcik W, Doss D. A planning framework for implementing virtual private networks. IT Professional, 2001, 3(3): 41-44

[4] Gleeson B. A Framework for IP Based Virtual Private Networks. IETF RFC2764, 2000, 2. http://www.ietf.org/rfc/rfc2764.txt

[5] 杨波. IP VPN 技术应用的研究. 长沙通信职业技术学院学报, 2006, 5(1): 40-44

[6] 杨彦彬. 可运营的 IP-VPN 业务. 广东邮电职业技术学院学报, 2005, 1(1): 21-23

[7] Rosenbaum G, Lau W, Jha S. Recent directions in virtual private network solutions. Networks, 2003(9/10): 217-223

[8] Tamasi L, Orincsay D, Gabor B, et al. Design of survivable VPN based VoIP networks. Design of Reliable Communication Networks, 2005, 10: 8

(上接第 102 页)

盘上开辟一个存储区，按 Snapshot 的指针将内存中的数据复制到磁盘上，然后更改指针指向磁盘上的块。读取时按照数据区域指针对应的块读进相应的内存块。Snapshot 的原理图如图 3 所示。

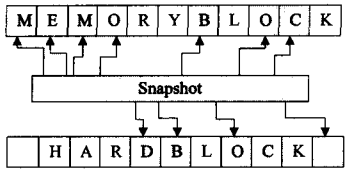

图 3 Snapshot 的原理

内存状态的复制过程如下：

(1)内存配置服务通过 SOAP 消息与原网格服务进行通信，消息中包含进行 Snapshot 标准操作的指令。

(2)对 Snapshot 生成的多个文件进行复制。

(3)在新环境中对 Snapshot 在内存中进行恢复。

5 实验

SGSR 复制方法能够很好地完成网格服务的复制任务，复制后的网格服务能够顺利地运行。我们对同一个网格服务在未使用和使用 SGSR 的情况下的用户访问响应时间和吞吐量分别进行了测量，实验结果如图 4、图 5 所示。

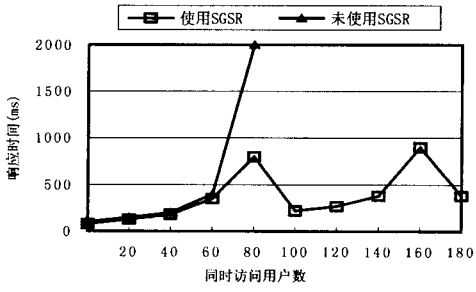

图 4 用户访问的响应时间

在图 4 中，未使用 SGSR 的情况下，在同时访问网格服务的用户数小于 60 的情况下响应时间较少。当用户数达到 80 后，服务处于超负荷状态，响应时间迅速增加。而使用 SGSR 后，当访问用户数接近 80 时就开始对网格服务进行复制，复制成功后一部分用户转向访问网格服务的副本。由于网格服务的用户访问数减少，响应时间迅速降低，因此 SGSR 可以很好地解决访问瓶颈的问题。

图 5 是使用 SGSR 和未使用 SGSR 时吞吐量的比较。未使用 SGSR 时，网格服务副本只有一个。随着任务不断增加，吞吐量增大(未过载)，最终达到饱和。使用 SGSR 后，当吞吐量趋近饱和的时候，可以通过复制出新的网格服务副本来提高系统整体的吞吐量。

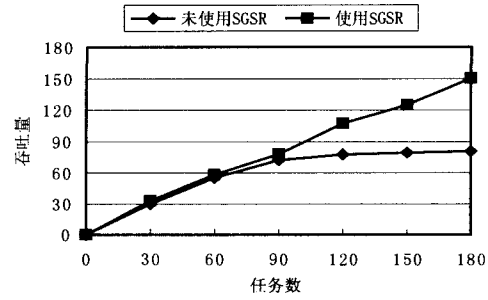

图 5 吞吐量比较

结束语 本文提出的 SGSR 网格服务复制机制，实现了有状态的网格服务的复制。网格副本服务技术只能进行无状态的副本复制，这是二者最大的区别。SGSR 完成了对网格服务所需硬件环境的搭建，软件环境的复制，网格服务程序代码、有状态资源的状态和内存状态的复制。SGSR 的注册和网格副本服务技术的注册机制大致一样，可以使用网格副本服务技术的注册机制进行注册。SGSR 在所需资源是安装态的情况下，能够在很短的时间内完成复制任务，为网格服务的复制提供了一种参考的方法。SGSR 能够很好地解决网格服务的过载和访问瓶颈问题，在达到某些特定条件时能够主动对网格服务进行复制。在以后的工作中，我们会继续完善安全的功能，并考虑当原网格服务进行更新时复制的新服务如何进行更新。

参 考 文 献

[1] Keahey K, Foster I, Freeman T, et al. Virtual Workspaces in the Grid // Europar. Lisbon, Portugal, 2005

[2] Keahey K, Foster I, Freeman T, et al. Virtual Workspaces: Achieving Quality of Service and Quality of Life in the Grid. Scientific Programming Journal, 2006

[3] Krsul I, Ganguly A, Zhang J, et al. VMPlants: Providing and Managing Virtual Machine Execution Environments for Grid Computing // SC04. Pittsburgh, PA, 2004

[4] Foster I, Frey J, Graham S, et al. Modeling Stateful Resources with Web Services. http://www-128.ibm.com/developerworks/webservices/library/specification/ws-resource/ws-modelingresources.html

[5] http://www.globus.org