面向集成的 VPN 构建策略①

陶志勇[1,2], 王如龙[2], 张 锦[2]

[1](长沙民政学院 软件学院, 长沙 410004)
[2](湖南大学 软件学院, 长沙 410082)

摘 要: 针对传统 VPN(Virtual Private Network)技术构建的企业网络存在扩展、地址冲突、互访控制难于实现等问题. 本文提出一种面向集成的VPN构建思路. 在分析这些问题产生原因的基础上, 集成思路的基本思想是将有效的解决方案进行集成, 以解决 VPN 构建中出现的不同问题. 该思路采用 MPLS 解决隧道扩展性问题, 采用 BGP 解决站点间地址冲突及访问控制的问题. 为了评估该设计方法的性能, 本文在企业网络中应用该思想构建了实际的企业 VPN. 实际运行结果表明, 采用该方法构建的 VPN 在扩展性、站点间地址冲突、访问控制等方面要优于传统技术.

关键词: 多协议标签交换; 边界网关路由协议; 虚拟私有网

Construction Strategies Aimed at Integrated VPN

TAO Zhi-Yong[1,2] , WANG Ru-Long[2], ZHANG Jin[2]

[1](Software school of Changsha social work college, Changsha 410004, China)
[2](Software school of Hunan University, Changsha, 410082, China)

Abstract: Enterprise network constructed through VPN technology has many problems including scalability, device address confliction, difficulty in realizing mutual access control. As to the problems, the paper proposes the idea of constructing an integrated VPN which integrate the effective solutions in order to solve different problems on the basis of making analysis on the reasons for these problems. The idea also solves the problem of tunnel scalability by MPLS and gets the solution to address confliction and access control by BGP. In addition, In order to evaluate the performance of this design method, it applies the idea to construct actual VPN in enterprise network. Practice result has proved this method is superior to VPN technology in scalability, device address conflict, access control, and VPN technology.

Key words: MPLS; BGP; VPN

1 引言

现代企业在发展过程中, 对企业网络对网络提出了越来越高的要求. 综合来看, 传统企业网与各分支机构通信, 一般通过这两种途径实现. 一种是通过 Internet 或运营商骨干 IP 网络, 一种是通过专线方式连接各分支机构. 但随着技术的不断进步, 以及网络环境的日益复杂等因素, 采用这两种组网方式由于运营成本高、安全、灵活性差, 受到严峻的挑战[1,2].

虚拟私有网[3](Virtual Private Network, VPN)是近年来随着网络的发展而迅速发展起来的一种隧道技术. 该技术通过利用公共网络进行通信, 一方面使企业以更低的成本实现连接远程分支机构, 另一方面提高了公共网络的资源利用率. 因此各种各样的 VPN 技术纷纷出炉, 如 GRE、L2TP、IPSEC[4]. 但是这些 VPN 技术的隧道都是静态建立, 扩展性不强; 本地地址冲突和站点间的访问控制问题在这些 VPN 技术上实现困难, 满足不了企业网络发展的需要[5,6].

多协议标签交换[7](Multiprotocol Label Switching, MPLS)是一种新兴的 IP 骨干网技术. MPLS 这种技术不但可以加快报文的转发速率, 而且它还是一种天然的动态隧道技术; 边界网关协议[8](Border Gateway Protocol, BGP)提供的丰富路由属性可以给不同站点的

① 基金项目:国家 863 计划项目(2009AA010314);国家科技支撑计划项目(2012BAF12B20);湖南省教育厅资助项目(13C1051)
收稿时间:2013-08-19;收到修改稿时间:2013-09-25

路由信息打上标记, 解决了数据在传输过程中的访问控制以及地址冲突的问题.

我国发展该技术的策略与其它通信技术在我国的研究与发展往往滞后于国际发展速度不同, 该技术一经提出, 就立即得到通信界的跟踪研究, 可以说对于该项技术理论方面的研究工作几乎与世界同步. 应用方面, MPLS VPN 业务近几年引起了全球运营业的普遍关注. 国外大的运营商如 AT&T,Sprint, Verizon, BeIISouth 都已经开始应用 MPLS 与 BGP 构建的 VPN 网络. 我国运营商中最早推出 MPLS 与 BGP 构建 VPN 业务的是中国网通, 推出时间为 2002 年 6 月. 随着市场前景的日益看好, 中国电信、中国铁通也开始提供这项服务. 此外, 一些跨国运营商也开始关注中国市场, 围绕该项 VPN 业务的竞争正在中国市场上逐渐升温.

本文针对某案例中采用传统 VPN 技术构建的企业网络, 存在扩展难、维护困难、站点间地址冲突及站点的间互访控制等问题, 提出了采用 MPLS 与 BGP 技术构建的 VPN 解决方案, 并在实验室进行了具体的实现. 实践证明, 采用该技术在扩展性、可靠性方面要优于传统的 VPN 技术[9,10].

2 设计思想及操作步骤

针对传统 VPN 技术构建的企业网络所产生的诸多问题, 一种改进设计思想是, 采用 MPLS 技术来建立动态隧道, 给私网数据穿越公网架设了一座“桥梁”, 解决网络维护难、扩展困难的问题; 采用虚拟路由(Virtual Routing and Forwarding, VRF)在一台设备上虚拟多台路由器, 给不同的 VPN 用户构建自己的路由表, 不同 VPN 用户的路由表相互隔离, 互不干扰. 分别让不同虚报路由器与不同用户站点通信, 解决了本地 PE(Provider Edge)设备地址冲突问题; 针对传播过程中私网路由的问题, 采用 BGP 技术来解决, BGP 技术可以跨设备建立邻居关系, 交互路由信息, 使公网里的中间设备不需要处理这些私网路由信息; 对于路由传播过程中私网路由的接收和撤销问题, 通过在传递的时候打“标记”来解决, 接收端通过“标记”来识别和撤销不同 VPN 用户的路由信息. 该设计方案具体的实现如下:

(1) 在公网中的设备上启动 MPLS, 运行标签分发协议 LDP(Label Distribution Protocol), 通过 LDP 协议标签分配的原理, 在所有的用户公网出口设备之间建立起抵达对方的标签转发路径, 给私网数据穿越公网提供通道.

(2) 在连接用户的 PE 设备上采用 VRF 技术, 不同 VPN 用户的地址信息分别学习不同的虚拟路由器中, 各虚拟路由器中的路由表相互独立, 互不影响, 解决了本地 PE 设备地址冲突的问题.

(3) 在连接用户的 PE 设备上运行 BGP 路由协议, 通过 BGP 路由协议来传递私网路由信息, 使两设备之间的其它设备不需要处理这些相同私网路由信息.

(4) 在 PE 设备运行 BGP 路由协议的同时, 给不同站点用户分配 BGP 的 RT (Route Target)属性值来实现站点间的互访问控制.

(5) 在 PE 设备上配置给每个用户站点分配 RD(Route Distinguisher)属性值和私网标签值. 给路由信息分别打上“标记”, 让设备根据这些“标记”来识别不同站点的路由信息. 解决地址冲突及路由撤销的问题.

MPLS 给私网数据穿越公网提供了一条逻辑通道; VRF 技术解决了本地 PE 设备收到相同地址信息, 引起的地址冲突的问题; BGP 路由协议解决了私网路由在传播时的学习、撤销、转发、访问控制等问题. 因此, MPLS 和 BGP 构建的 VPN 技术在隧道建立、站点间互访控制、地址冲突方面都优于传统的 VPN 技术, 其应用的领域也越来越广泛.

3 方案评估

3.1 评估方案分析

为了评估该设计思想的可行性, 通过在某运营的网络中应用该方案, 对该方案的可行性进行验证. 某运营商网络遍布全省, 网络结构采用层次化网络模型, 把网络分为三层, 核心层、汇聚层和接入层. 核心、汇聚、接入层设备分别采用华三 CR16000K、SR8800、SR6600 设备. 同时, 该运营商采用 GRE 的 VPN 技术为企业的分支机构接入企业内网提供 VPN 服务. 如图 1 所示.

图 1 中的 VPN1 和 VPN2 分别表示不同的企业网络, 用户设备 CE1 和 CE2 连接运营商网络设备 PE1, CE3 与 CE4 连接运营商的 PE4. 该网络运行一定时间后, 网络工程人员发现该网络存在有以下问题.

(1) 维护困难: 这种采用 GRE 技术建立的静态隧

道, 若想修改一个站点隧道参数, 会影响到所有站点.

(2) 扩展性差: 新增一个站点, 隧道的布署是呈平方级增加的.

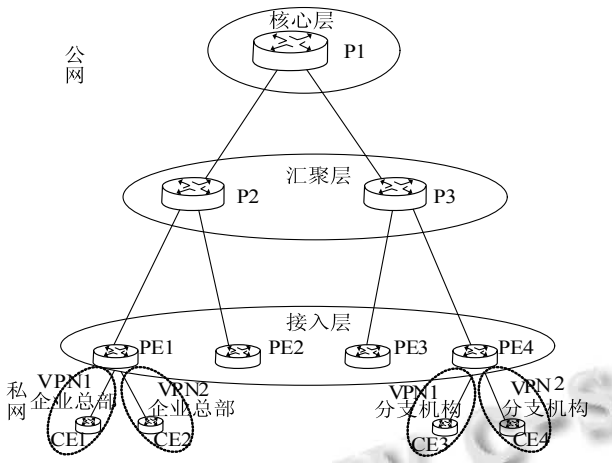

图 1 运营商连接用户的网络拓扑图

(3) 对于不同用户站点使用相同的地址信息, 引起的地址冲突问题采用策略路由的解决方案实现复杂.

(4) 站点间的互访控制通过访问控制列表实现繁琐.

随着企业业务发展的需要, 越来越多的企业希望把构建企业内部网络的工作交给运营商网络来完成. 而负责运营商的工程技术人员意识到已现有的条件满足不了企业网络发展的需要, 期待有更好的解决方案, 解决现在网络存在的诸多问题.

该网络系统主要是实现各个用户站点间的通信, 每个站点间的实现通信的方法相同. 通过利用学院网络环境, 可以模拟出两站点间的通信. 实现过程如图 2 所示.

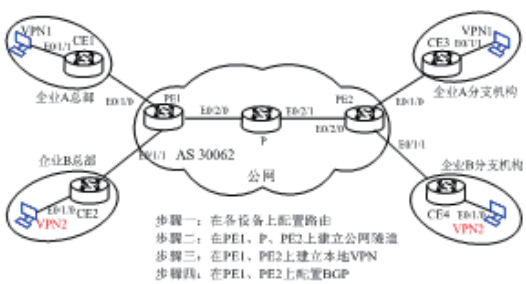

图 2 实验拓扑图

实验各设备接口的IP地址和子网掩码如表 1 所示.

表 1 各设备接口地址分配表

设备名称	接口	接口地址	掩码
VPN1 总部 CE1	Loopback0	1.1.1.1	255.255.255.255
	E0/1/0	192.168.1.254	255.255.255.0
	E0/1/1	192.168.5.254	255.255.255.0
VPN2 总部 CE2	Loopback0	1.1.1.1	255.255.255.255
	E0/1/0	192.168.6.254	255.255.255.0
	E0/1/1	192.168.2.254	255.255.255.0
总部 PE1	Loopback0	10.10.10.1	255.255.255.255
	E0/1/0	192.168.1.253	255.255.255.0
	E0/1/1	192.168.2.253	255.255.255.0
	E0/2/0	200.0.0.1	255.255.255.0
P	Loopback0	10.10.10.2	255.255.255.255
	E0/2/0	200.0.0.2	255.255.255.0
	E0/2/1	200.0.1.1	255.255.255.0
分支 PE2	Loopback0	10.10.10.3	255.255.255.255
	E0/1/0	192.168.3.253	255.255.255.0
	E0/1/1	192.168.4.253	255.255.255.0
	E0/2/0	200.0.1.2	255.255.255.0
VPN1 分支 CE3	Loopback0	2.2.2.2	255.255.255.255
	E0/1/0	192.168.3.254	255.255.255.0
	E0/1/1	192.168.7.254	255.255.255.0
VPN2 分支 CE4	Loopback0	2.2.2.2	255.255.255.255
	E0/1/0	192.168.8.254	255.255.255.0
	E0/1/1	192.168.4.254	255.255.255.0

要实现总部与分支机构的通信, 通过以下三个步骤完成.

(一) 公网隧道的配置

在公网设备通过运行 OSPF 动态路由协议来交互路由信息, 各设备交互完路由信息后就可以实现互访. 具体的配置如表 2 所示.

表 2 设备的 MPLS 配置

设备的配置	配置命令的作用
PE1 设备的配置:	
[PE1]mpls lsr-id 10.10.10.1	配置设备的 lsr id
[PE1]mpls	启用设备的 mpls 功能
[PE1]mpls ldp	启用 mpls ldp 协议
在 PE1 设备的 e0/2/0 接口上启动 mpls 和 mpls ldp 协议	

在表 1 中, 给 PE1 设备上配置了 lsr id, 并在设备上运行了 MPLS 和 MPLS LDP 协议, 在 P、PE2 设备

作相同的配置后. 各设备就能处理 MPLS 报文, 且 MPLS LDP 协议会给这三个 lsr id 分配标签, 并自动形成对应的标签转发表项, 从而形成对应的隧道, 完成隧道的建立.

(二) PE 的本地 VPN 配置

在公网设备上运行 MPLS 后, 架设了一座“桥梁”, 给私网数据穿越公网提供了通道. 而对于不同用户站点采用相同的地址, 使PE设备上产生地址冲突的问题, 传统的解决方法是采用策略路由与访问控制列表相结合的办法来解决, 这种方法实现复杂, 而且影响设备的性能. 在该实验中给不同 VPN 用户分配不同的 RT、RD 值, 并使用 VRF 技术与 OSPF 多进程加接口绑定来解决. 通过这几种技术的结合可以把不同 VPN 用户的路由信息分别学习不同的虚拟路由器上, 各个虚拟路由器相互隔离, 互不干扰. 该方案的实现需要在本地的 PE 设备上需做如表 3 的配置.

表 3　PE 的本地 VPN 配置

设备的配置	配置命令的作用
PE1 的配置:	
[PE1]ip vpn-instance vpn1	创建 vpn1
[PE1-vpn-instance-vpn1]route-distinguisher 30053:1	配置 vpn1 的 RD 值
[PE1-vpn-instance-vpn1]vpn-target 110:1 export-extcommunity	配置 vpn1 中 RT 的输出数值
[PE1-vpn-instance-vpn1]vpn-target 110:1 import-extcommunity	配置 vpn1 中 RT 的输入数值
[PE1]int e0/1/0	配置接口 e0/1/0
[PE1-Ethernet0/1/0]ip binding vpn-instance vpn1	把接口与 vpn1 进行绑定
[PE1-Ethernet0/1/0]ip add 192.168.1.253 24	给接口分配 IP
在 PE1 设备上 vpn2 的配置与 vpn1 相同, 在此不再赘述	

在表 3 中, 在 PE1 设备上创建了不同的 VPN, 给不同的 VPN 分配了不同的 RT、RD 值, 不同的 VPN 分别与不同的接口作了绑定, 并在 PE2 设备作相同的配置. 使不同的 VPN 用户有自己的 RT、RD 值, 实现了相同 VPN 用户的互访, 不同 VPN 用户不能通信.

(三) BGP 配置

公网隧道的配置给私网数据穿透公网提供了通道; 本地 PE 上的 VPN 配置, 实现了不同 VPN 用户的路由表相互独立, 互不干涉. 网络设备它如何区分不同 VPN 用户的路由信息的呢? 纵观路由协议, 只有 BGP 动态路由协议可以完成该项工作, 通过在设备上运行 BGP 动态路由协议后, 它可以给不同的路由信息打上标志来传送. 对端设备收到这些路由信息时通过这些标记来区分不用 VPN 用户的路由. BGP 的配置如表 4 所示.

表 4　PE 设备的 BGP 配置

设备的配置	配置命令的作用
PE1 的配置:	
[PE1]bgp 30052	配置 bgp 并指定进程号是 30052
[PE1-bgp]peer 10.10.10.3 as-number 30052	配置 PE1 的对等体
[PE1-bgp]peer 10.10.10.3 connect-int LoopBack 0	采用 Loopback 接口来建立邻居
[PE1-bgp]ipv4-family vpnv4	使能设备的 vpnv4 功能
[PE1-bgp-af-vpnv4]peer 10.10.10.3 enable	使能要交互 vpnv4 路由的邻居
[PE1-bgp]ipv4-family vpn-instance vpn1	配置 vpnv4 的 vpn1
[PE1-bgp-vpn1]import-route direct	在 vpn1 中引入直连路由信息
[PE1-bgp-vpn1]import-route ospf 100	在 vpn1 中引入 ospf 进程 100 的路由信息
[PE1]ospf 100 vpn-instance vpn1	配置进程 100 与 vpn1 绑定
[PE1-ospf-100]import-route bgp	在进程 100 中引入 bgp 路由信息
在 PE1 设备上 vpn2 的配置与 vpn1 相同, 在此不再赘述	

PE2 设备的 BGP 配置与 PE1 设备相同, 在上述 BGP 的配置中, 通过在 BGP 动态路由协议中分别引入了 VPN1 和 VPN2 的私网路由信息发送给对方. 对方收到后, 根据 RT、RD 标记来区分路由信息, 分别学习到不同的 VPN 用户的路由表中. 至此, 不同 VPN 用户的私网路由信息通过几次信息交互后, 相互学习到了对方的路由信息, 实现了互访. 不同 VPN 能实现互访, 得益于在该实验中使用 MPLS 和 BGP 构建的 VPN, 在 PE1、P、PE2 设备上架设了一座“桥梁”, 为私网数据的传送提供了通道.

3.2 性能评估

根据上述规划与配置, 已完成了该网络的构建. 构建的网络是否连通, 并与传统 VPN 技术相比该技术存在哪些方面的优势. 下面对该网络进行性能测试与性能分析.

(一) 性能测试

该项目中急需要解决 PE 设备对于不同的用户站点采用相同的地址冲突问题, 在该实验中是否得以解

决. 通过在 PE1 设备上分别查取各自 VPN 用户对应的路由表, 如图 3 所示结果.

```
<PE1>dis ip routing-table vpn-instance vpn1
Routing Tables: vpn1
         Destinations : 9        Routes : 9

Destination/Mask    Proto   Pre  Cost      NextHop         Interface

1.1.1.1/32          OSPF    10   1         192.168.1.254   Eth0/1/0
2.2.2.2/32          BGP     255  2         10.10.10.3      NULL0
127.0.0.0/8         Direct  0    0         127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0         127.0.0.1       InLoop0
192.168.1.0/24      Direct  0    0         192.168.1.253   Eth0/1/0
192.168.1.253/32    Direct  0    0         127.0.0.1       InLoop0
192.168.3.0/24      BGP     255  0         10.10.10.3      NULL0
192.168.5.0/24      OSPF    10   2         192.168.1.254   Eth0/1/0
192.168.7.0/24      BGP     255  3         10.10.10.3      NULL0
```

```
<PE1>dis ip routing-table vpn-instance vpn2
Routing Tables: vpn2
         Destinations : 9        Routes : 9

Destination/Mask    Proto   Pre  Cost      NextHop         Interface

1.1.1.1/32          OSPF    10   1         192.168.2.254   Eth0/1/1
2.2.2.2/32          BGP     255  2         10.10.10.3      NULL0
127.0.0.0/8         Direct  0    0         127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0         127.0.0.1       InLoop0
192.168.2.0/24      Direct  0    0         192.168.2.253   Eth0/1/1
192.168.2.253/32    Direct  0    0         127.0.0.1       InLoop0
192.168.4.0/24      BGP     255  0         10.10.10.3      NULL0
192.168.6.0/24      OSPF    10   2         192.168.2.254   Eth0/1/1
192.168.8.0/24      BGP     255  3         10.10.10.3      NULL0
```

图 3 PE1 设备 VPN1 与 VPN2 路由表

通过图 3 查看各 VPN 用户的路由表,结果表明对于 1.1.1.1 这条 CE1、CE2 都使用的地址信息, 在 PE1 设备上都学习到了, 并分别接收到不同的 VPN 路由表中. 实践证明了该实验成功的解决了不同用户站点采用相同地址, 导致的地址冲突问题.

对于用户站点间的互访控制问题, 通过查看 CE1、CE2 的路由表, 并在 CE1 设备上访问 CE2 与 CE3 得到的结果如图 4 所示.

```
<CE1>dis ip routing-table
Routing Tables: Public
         Destinations : 10       Routes : 10

Destination/Mask    Proto   Pre  Cost      NextHop         Interface

1.1.1.1/32          Direct  0    0         127.0.0.1       InLoop0
2.2.2.2/32          OSPF    10   3         192.168.1.253   Eth0/1/0
127.0.0.0/8         Direct  0    0         127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0         127.0.0.1       InLoop0
192.168.1.0/24      Direct  0    0         192.168.1.254   Eth0/1/0
192.168.1.254/32    Direct  0    0         127.0.0.1       InLoop0
192.168.3.0/24      O_ASE   150  1         192.168.1.253   Eth0/1/0
192.168.5.0/24      Direct  0    0         192.168.5.254   Eth0/1/1
192.168.5.254/32    Direct  0    0         127.0.0.1       InLoop0
192.168.7.0/24      OSPF    10   4         192.168.1.253   Eth0/1/0
```

```
<CE2>dis ip r
<CE2>dis ip routing-table
Routing Tables: Public
         Destinations : 10       Routes : 10

Destination/Mask    Proto   Pre  Cost      NextHop         Interface

1.1.1.1/32          Direct  0    0         127.0.0.1       InLoop0
2.2.2.2/32          OSPF    10   3         192.168.2.253   Eth0/1/1
127.0.0.0/8         Direct  0    0         127.0.0.1       InLoop0
127.0.0.1/32        Direct  0    0         127.0.0.1       InLoop0
192.168.2.0/24      Direct  0    0         192.168.2.254   Eth0/1/1
192.168.2.254/32    Direct  0    0         127.0.0.1       InLoop0
192.168.4.0/24      O_ASE   150  1         192.168.2.253   Eth0/1/1
192.168.6.0/24      Direct  0    0         192.168.6.254   Eth0/1/0
192.168.6.254/32    Direct  0    0         127.0.0.1       InLoop0
192.168.8.0/24      OSPF    10   4         192.168.2.253   Eth0/1/1
```

图 4 CE1、CE2 设备路由表

根据图 4 的显示结果, 可以看到 CE1 设备学习到了相同 VPN 用户 CE3 的路由信息, 而在 CE2 设备的路由表中没有学习到 CE1、CE3 的路由信息, 通过在 CE1 设备上分别访问 CE3 与 CE2, CE1 能访问 CE3, 访问不了 CE2. 实验结果证实了, 相同 VPN 用户之间能通信, 不同 VPN 用户不能互访问, 进而实现了站点间 VPN 用户的互访问控制.

(二) 性能分析

上述的理论研究与实践给性能分析提供了依据, 下面从扩展性、网络结构、网络管理等方面来分析传统 VPN 技术与该 VPN 技术性能差别.

(1) 扩展性

传统的 VPN 是在运营商网络之上构建的, 在实现用户站点间的全网状通信时, 假设站点数用 N 来表示, 那么就需要建立 N2 平方的隧道数 ; 而 MPLS 和 BGP 技术构建的 VPN 不会存在该问题. 下面以用户站点数构建的 VPN 网络对两者进行对比, 如图 5 所示.

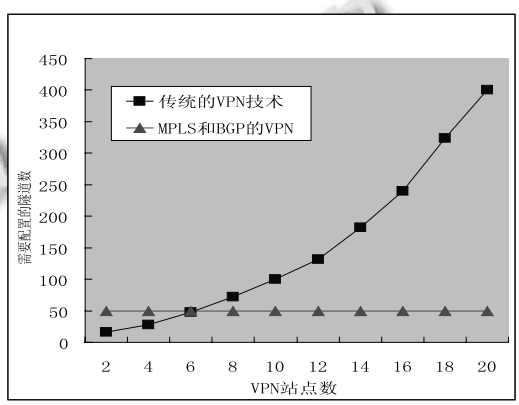

图 5 两种 VPN 技术构建隧道数对比

通过图 5 的分析, 传统 VPN 网络是随着用户站点数的增加隧道的建立是成平方的增长, 扩展性成为制约传统 VPN 技术发展的重要因素. 而 MPLS 和 BGP 技术构建的网络隧道的建立与用户站点数量无关, 解决了隧道建立 N 平方的问题.

(2) 其它方面性能对比

在网络管理、网络结构、站点间互访控制等方面对该 VPN 技术与传统 VPN 技术进行分析, 得到结果如表 5 所示.

通过上述分析, 得出该技术在网络管理、访问控制、地址冲突等问题的解决上都要优于传统的 VPN 技术. MPLS 和 BGP 技术构建的 VPN 的这些优点, 也使该技术的应用领域也越来越广泛.

表 5 两种 VPN 技术其它方面性能对比

对比项目	传统 VPN	MPLS 和 BGP 的 VPN
网络管理	容易	复杂
网络结构	简单	随站点数增加而复杂
站点地址冲突	实现容易	实现困难
结构扩充性	高	低
建设成本	成本低	成本高
站点互访问控制	实现容易	实现复杂

4 结语

网络结构扩展性差、设备地址冲突及互访问控制实现难制约了传统 VPN 技术的发展. 本文分析了产生这些问题的原因. 主要的原因是隧道的建立是静态, 以及无法实现不同 VPN 用户信息的隔离. 针对这些问题, 提出了 MPLS 和 BGP 技术构建的 VPN, 并利用实验室环境应用了该项技术. 事实证明, 采用该技术在扩展性、用户站点间互访问控制等方面要优于传统的 VPN 技术, 给企业构建自己的专用网络提供了一种解决方案.

参考文献

1 Hou JF, Ma MK. Research on PE-CE connection simulation in MPLS VPN. Computer Engineering, 2010, 36(12):123–125.

2 Zhang DL, Ionescu D. Qos Perfomance analysis in deployment of diffServaware MPLS traffic engineering. Proc. of the 8thACIS International Conference on Software Engineering. Ottawa, Canada. 2007. 963–967.

3 Rahman MA, Kabir AH, Lutfullah KAM, et al. Performance analysis and the study of the behavior of MPLS protocols. Proc. of the International Conference On Computer and Communication Engineering. Kuala Lumpur, Malaysia. 2008. 226–229.

4 Vitch PJ. Enterprise buyer's guide to Layer3 MPLS VPN service. Enterprise Network & Servers, 2005, 11: 18–20.

5 Lee YW, Kim S, Park J, el al. A lightweigllt implementation of RSVP-TE protocol for MPLS-TE signaling. Computer Communications, 2007, 30(6): 1199–1204.

6 Chu J, Lea CT. Optimal link weights for IP-based networks supporting hose-model VPN. IEEE/ACM Transactions on Networking, 2009, 17(3):778–788.

7 Ren JQ, Ma HL, Wang BQ. Implementaion of inter-AS BGP/MPLS VPN in high-performance router. Computer Engineering, 2009, 35(3):126–129.

8 Vitch PJ. Enterprise buyer's guide to Layer 3 MPLS VPN service. Enterprise Network & Servers, 2005, (11): 18–20.

9 Li P, Tang JY, Chen DW, et al. Study on classification and comparison of virtual private network. Computer Engineering, 2006, 32(22):133–135.

10 Rahman MA, Kabir AH, Lutfullah KA, et al. Performance analysis and the study of the behavior of MPLS protocols. International Conference on Computer and Communication Engineering ICCCE. 2008. 13–15.

(上接第 22 页)

3 Lv RJ. A scalable bandwidth allocation method for synchronous wireless mesh network. Journal of Computational Information Systems, 2012, 8(19): 8001– 8008.

4 Kumar P. Design, Implementation, and Evaluation of New MAC Protocols for Long Distance 802.11 Networks. Kanpur, Uttar Pradesh, India. May 2006.

5 雷昕,郭琳.宽带无线 Mesh 网络中的多扇区天线阵列设计. 中国电子科学研究院学报,2012,7(4):178–181.

6 侯蓉晖,史浩山,杨少军. 无线传感器网络链路统计特性研究与应用. 系统仿真学报,2007,(7):1507–1511.

7 黄庭培,李栋,张招亮,崔莉. 一种突发性链路感知的自适应链路质量估计方法.计算机研究与发展,2010,(S2):168–174.

8 赵海,朱思远,孙佩刚,张希元.无线传感器网络链路质量测量问题研究.东北大学学报(自然科学版),2008,(2):193–196.

9 徐卓农,王建新,黄家玮.无线网络中的多速率调整机制综述.计算机科学,2011,(4):43–47.

10 徐伟强,胡四平,汪亚明,张云华. IEEE802.11 中多速率多节点公平的数据分组长度调整策略.通信学报,2011,(2): 120–129.