计算机系统应用 ISSN 1003-3254, CODEN CSAOBN
Computer Systems & Applications,2022,31(2):137–142 [doi: 10.15888/j.cnki.csa.008369]

E-mail: csa@iscas.ac.cn
http://www.c-s-a.org.cn
Tel: +86-10-62661041

面向虚拟私有网的网络设备虚拟化技术①

陶志勇[1,2], 张　锦[2,3], 阳王东[2], 唐铁斌[1]

[1](长沙民政职业技术学院 软件学院, 长沙 410004)
[2](湖南大学, 长沙 410082)
[3](湖南师范大学, 长沙 410012)
通信作者: 张　锦, E-mail: mail_zhangjin@163.com

摘　要: 针对边缘设备随着接入的分支机构增多, 需处理的公网与私网数据爆增, 导致边缘设备负载过重, 影响数据的正常交互. 为此, 分析了产生问题的根源, 提出了网络设备虚拟化技术与多协议标签交换与边界网关协议技术相融合的解决方案. 为验证方案的可行性, 借助实验室设备, 搭建了方案所需环境, 完成了方案的部署. 部署完成后对方案的可用性、数据访问控制与隔离、数据的分布式处理与负载分担进行了测试, 并与传统方式在设备冗余性、扩展性、管理性等 10 个维度进行了对比. 测试与对比结果表明, 该方案能在边缘设备上实现数据的分布式处理与负载分担, 优于传统方式, 是一种有效的 VPN 解决方案.

关键词: 虚拟私有网; 网络; 设备; 虚拟化

引用格式: 陶志勇,张锦,阳王东,唐铁斌.面向虚拟私有网的网络设备虚拟化技术.计算机系统应用,2022,31(2):137–142. http://www.c-s-a.org.cn/1003-3254/8369.html

Network Equipment Virtualization Technology for Virtual Private Network

TAO Zhi-Yong[1,2], ZHANG Jin [2,3], YANG Wang-Dong[2], TANG Tie-Bin[1]

[1](College of Software, Changsha Social Work College, Changsha 410004, China)
[2](Hunan University, Changsha 410082, China)
[3](Hunan Normal University, Changsha 410012, China)

Abstract: As the number of branches connected to edge devices increases, the public and private network data that needs to be processed explodes, causing the edge devices to be overloaded and affecting the normal interaction of data. To solve these problems, this study analyzes the root cause of the problems and proposes a solution that integrates network equipment virtualization technology with multi-protocol label switching and border gateway protocol technology. For the feasibility verification of the solution, with the help of laboratory equipment, the environment required for the solution is built, and the deployment of the solution is completed. Then, the solution's availability, data access control and isolation, distributed data processing and load sharing are tested, and it is compared with traditional methods in ten dimensions such as equipment redundancy, scalability, and management. The test and comparison results show that the solution can realize the distributed data processing and load sharing on edge devices, and it is superior to traditional methods as an effective VPN solution.

Key words: virtual private network; network; equipment; virtualization

1　引言

随着企业业务的发展, 越来越多的企业采用 VPN (virtual private network, 虚拟私有网) 的方式保障企业总部与各分支机构及业务合作伙伴数据的交互. 而随

① 基金项目: 国家自然科学基金 (61872127); 湖南省教育厅资助科研项目 (19C0106)
收稿时间: 2021-04-11; 修改时间: 2021-05-11, 2021-05-27; 采用时间: 2021-06-30; csa 在线出版时间: 2022-01-17

着企业分支机构、业务合作伙伴呈爆炸式的增长, 传统 VPN 如 GRE[1]、L2TP[2]、IPSEC[3] 方式构建的 VPN 由于隧道需静态建立, 每一个分支机构、业务合作伙伴需要分别构建其隧道, 使得隧道的建立呈平方增长, 这种静态隧道的部署方式配置繁杂、管理困难、业务数据的隔离实现复杂, 已满足不了企业发展的需要[4].

而 MPLS (multi-protocol label switching, 多协议标签交换[5]) 的 LDP (label distribution protocol, 标签分发协议) 根据公网路由信息能动态生成标签转发表, 其标签转发表的形成为私网数据穿越公网提供了通道. 对于企业各分支机构或合作伙伴业务数据的隔离, 由于 BGP (border gateway protocol, 边界网关协议)[6] 可以为不同的业务数据打"标记", 并根据其"标记"来识别与控制业务数据的访问. 因此, 越来越多的企业青睐于采用 MPLS 构建天然隧道, 采用 BGP 控制数据的访问与隔离, 目前 MPLS 与 BGP 技术构建的 VPN 应用越来越广泛[7–9].

然而, 随着企业接入的分支机构及合作伙伴爆炸式增长, 对运行 MPLS 与 BGP 技术的设备性能是一大考验. 因为该设备处于公网与私网的交界处, 不但要处理来自公网的数据, 而且需要处理来自各分支机构的私网数据. 当需处理的数据量超过设备所承载的范围, 会影响到数据的正常交互, 严重时导致设备宕机[10,11].

IRF (intelligent resilient framework)[12] 是一种基于云计算的网络设备虚拟化技术, 该技术可以将多台物理设备虚拟成一台逻辑设备, 逻辑设备融合了所有物理设备的资源, 可以多台物理设备对数据进行分布式的处理与负载均衡. 因此, 本文将该技术与 MPLS 与 BGP 技术相结合, 采用 IRF 实现数据的分布式的处理与负载均衡; 采用 MPLS 构建隧道, 为私网数据穿越公网提供通道; 采用 BGP 实现数据的访问控制与隔离, 进而为企业构建一个稳定、可靠、安全的虚拟私有网, 为企业稳步发展保驾护航[13–15].

2 方案设计

为了更好地阐释该设计方案相比传统方式的优越性, 方案构建了两个网络拓扑, 一个是采用传统方式构建的网络拓扑, 另外一台是采用网络设备虚拟化技术构建的网络拓扑. 图 1 是采用传统方式构建的网络拓扑. 在图 1 所示的网络拓扑中, 在公网的边缘设备 A、公网设备、边缘设备 B 上构建一条隧道, 并在边缘设备上分别给分支机构 A 设备与企业总部机构 A 设备、分支机构 B 设备与企业总部机构 B 设备构建其独立的虚拟私有网, 分别是 VPNA 与 VPNB. 通过隧道来传输分支机构 A 与企业总部机构 A、分支机构 B 与企业总部机构 B 的私网数据.

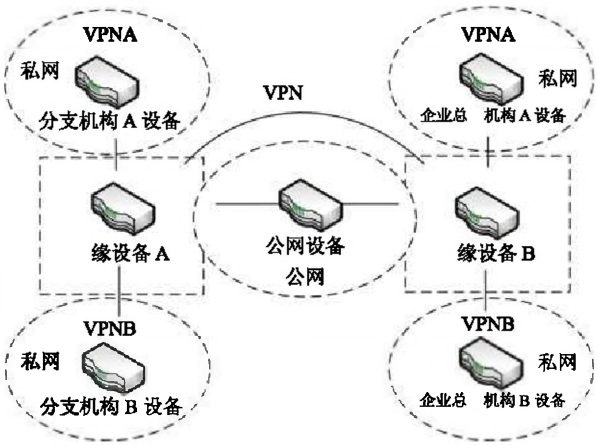

图 1 传统方式构建的网络拓扑

而采用网络设备虚拟化技术构建的网络拓扑如图 2 所示. 该网络拓扑为了后续描述的方便, 将传统方式拓扑图中的分支机构 A 与分支机构 B 分别表示 branch1、branch2; 企业总部机构 A 与企业总部机构 B 称之为 h1、h2; 连接分支机构 A 与分支机构 B 的两台边缘设备表示为 ed1、ed2, 两台边缘设备虚拟化后的设备表示为 v1; 连接企业总部机构 A 与企业总部机构 B 的边缘设备分别称之为 ed3、ed4, 两台边缘设备虚拟化后的设备表示为 v2. 在该网络拓扑中, 分支机构 A 与分支机构 B、企业总部机构 A 与企业总部机构 B 采用了相同的私网地址, 而通过方案的访问控制与隔离技术, 即使采用了相同的地址, 也不会引起地址的冲突.

实现 branch1 与 branch2、h1 与 h2 业务数据的隔离, 由 v1、v2 分别负载分担 branch1 与 branch2、h1 与 h2 业务数据, 以及 branch1 与 h1、branch2 与 h2 的私网数据穿越公网, 保障其私网数据的交互, 其方案的设计理念如图 2 所示.

(1) 首先采用网络设备虚拟化技术 IRF 将 ed1 与 ed2、ed3 与 ed4 分别虚拟成 v1 与 v2, 为分布式处理与负载分担 branch1 与 branch2、h1、h2 的私网数据奠定基础. 虚拟化部署成功后, 采用多进程与虚拟路

由技术相结合的方式实现 branch1 与 branch2、h1 与 h2 私网数据的本地隔离, 进而加强数据的安全性.

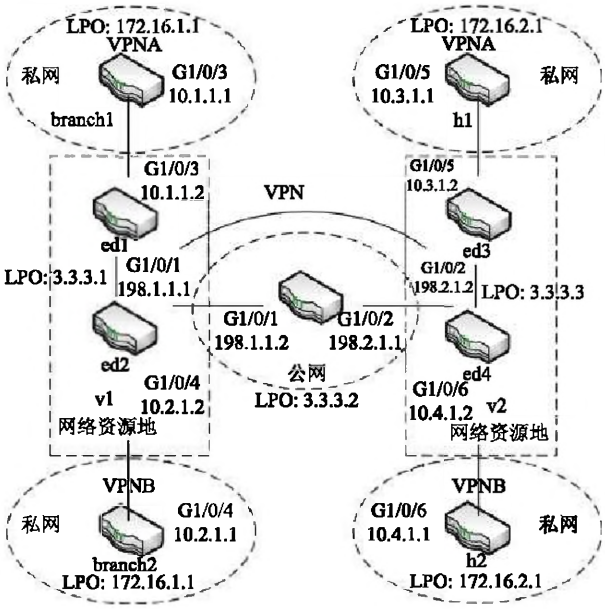

图 2 采用网络设备虚拟化技术构建的网络拓扑

(2) 其次在 v1、p、v2 设备上, 部署 MPLS 技术, 生成标签转发表, 根据标签转发表来构建动态隧道. 为 branch1 与 branch2、h1 与 h2 私网数据穿越公网提供通道.

(3) 最后在 v1 与 v2 设备上, 部署 BGP 技术, 借助其 BGP 的 LABEL 属性为 branch1 与 branch2、h1 与 h2 私网数据打上不同的“标记”, 即使 branch1 与 branch2、h1 与 h2 采用了相同的私网地址, 根据其标记也可以识别. 同时部署 BGP 的 RT (route target) 属性控制其 branch1 的私网数据穿越公网后, 只能与 h1 进行业务数据的交互, 不能与 h2 进行业务数据的交互. 同理, branch2 的私网数据只能与 h2 交互, 不能与 h1 交互. 通过上述两种 BGP 属性实现私网数据的访问控制及私网数据的隔离, 保障了数据的安全.

3 方案实现

为了验证设计理念的可行性与优越性, 借助其实验室的网络设备, 搭建设计理念图 2 所需的环境, 通过网络资源池的构建、隧道的建立、私网数据的控制与隔离完成方案的部署.

(1) 网络资源池的构建

图 2 中 ed1 与 ed2 能否虚拟成 v1, 直接影响能对 branch1 与 branch2 进行分布式处理与负载分担. 而实现图 2 拓扑中 ed1 与 ed2 的虚拟化, 需将两台设备规划于一个域中进行管理, 并保障两台设备在域内成员编号的唯一性. 同时, 分别在两台物理设备上创建其对应的逻辑端口, 将两台设备相连的物理端口与逻辑端口绑定. 上述部署完成后, 在两台设备运行 irf-port-configuration active 指令使两台物理设备 ed1 与 ed2 进行竞争选举, 竞选胜出的一方成为该资源池中的主设备, 另外一台成为从设备, 在资源池中对主设备的部署都会同步到从设备. 图 3 是采用上述方法部署后, 在 ed1 上查看网络设备虚拟化的情况, 从图 3 的结果说明已将 ed1 与 ed2 两台物理设备成功虚拟为一台逻辑设备. 而对于 ed3 与 ed4 设备的虚拟, 其方法与 ed1 与 ed2 相同, 在此不再赘述.

```
<ed1>dis irf
MemberID    Role     Priority  CPU-Mac         Description
 *+1        Master   1         1456-a37d-0304  ---
   2        Standby  1         1456-a6f4-0404  ---
--------------------------------------------------
 * indicates the device is the master.
 + indicates the device through which the user logs in.

 The bridge MAC of the IRF is: 1456-a37d-0300
 Auto upgrade                : yes
 Mac persistent              : 6 min
 Domain ID                   : 0
```

图 3 ed1 与 ed2 的资源池构建

(2) 网络资源池上隧道的建立

网络资源池的构建使 ed1 与 ed2、ed3 与 ed4 能对 branch1 与 branch2、h1 与 h2 私网数据进行分布式处理与负载分担. 而 branch1 与 h1, branch2 与 h2 私网数据的交互需在图中的网络资源池上构建一条穿越公网的隧道. MPLS 技术的标签分配协议分配的标签转发表是一种天然隧道. 因此, 在该方案中, 在 v1、p、v2 设备上采用 MPLS 技术, 为图 2 中的 v1 的 3.3.3.1、p 设备的 3.3.3.2、v2 的 3.3.3.3 分配标签. 其标签的分配分为两步完成, 第一是启动 3 台设备的 MPLS 功能, 并在 3 台设备上通过 mpls lsr-id 指令给 3 台设备标识其身份; 第二是在 3 台设备相连的接口下启动 MPLS 与 MPLS LDP 协议的功能, 让设备能交互 MPLS 协议报文, 并生成标签转发表, 形成转发私网数据的路径. 图 4 是采用上述策略后, ed1 设备生成的标签转发表情况.

图 4 生成的标签转发表, 当私网数据需要穿越公网时, 采用标签转发表中的标签来封装私网数据, 将私网数据封装在标签里面, 根据标签来完成数据的转发, 进而使得私网数据成功穿越公网.

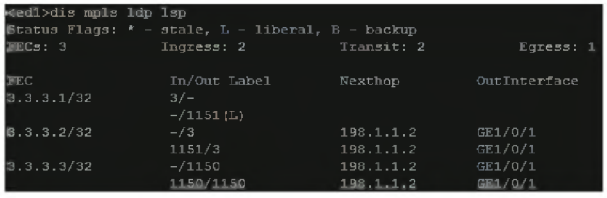

图 4　ed1 设备的标签转发表

(3) 私网数据的访问控制与隔离

为了更好地验证该设计方案能实现私网数据的访问控制与数据隔离, branch1 与 branch2、h1 与 h2 采用了相同的私网地址, 如方案不能实现对私网数据的访问控制与隔离, branch1 与 branch2、h1 与 h2 私网数据到达 v1 与 v2 时, 会产生地址冲突.

图 5 为 ed1 主设备给 branch1 与 branch2 私网路由分配的 label 与 RT 值. 如图 5 所示, ed1 主设备给 branch1 设备的172.16.1.1 分配的 label 属性值是 1 279, 而给 branch2 设备的 172.16.1.1 分配的 label 属性值是 1 276, 进而通过 label 属性值区分 172.16.1.1 属于 branch1, 还是属于 branch2 的私网数据.

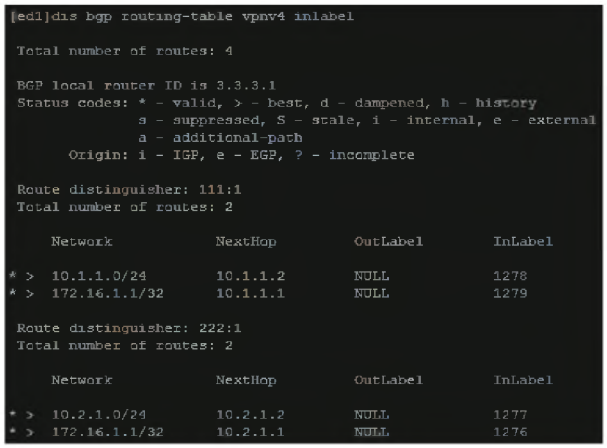

图 5　ed1 主设备给 branch1 与 branch2 私网路由分配的 label 与 RT 值

4　方案评估

(1) 方案测试

为了评估方案的有效性, 从可用性、安全性、数据分布式处理与负载均衡量方面对方案进行相应的测试.

1) 可用性测试

在 branch1 上运行 tracert 命令与 ping 命令去访问企业总部机构 A, 其测试结果如图 6 所示.

图 6 的 tracert 与 ping 命令测试结果充分表明, branch1 到达企业总部机构 A 的路径通畅, 而且能相互访问.

在 branch2 上运行 tracert 命令与 ping 命令去访问企业总部机构 B, 其测试结果如图 7 所示.

图 7 的测试结果与图 6 一样, 图 6 和图 7 的测试结果说明 branch1 与 h1, branch2 与 h2 的私网数据成功穿越公网, 并能进行私网数据的交互.

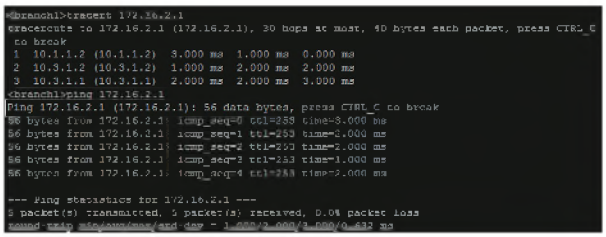

图 6　在 branch1 上运行 tracert 命令与 ping 命令去访问企业总部机构 A 的结果

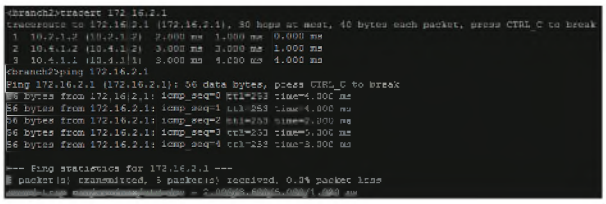

图 7　在 branch2 上运行 tracert 命令与 ping 命令去访问企业总部机构 B 的结果

2) 数据访问控制与隔离测试

考虑到数据的安全性, 企业不同分支机构的私网数据及总部不同业务部门的业务数据不能让其相互访问, 在 ed1 通过运行 dis ip routing-table vpn-instance vpna protocol ospf 与 dis ip routing-table vpn-instance vpnb protocol ospf 命令后显示的结果如图 8 所示, 不同分支机构在 ed1 上的私网数据分别导入到各自的实例路由表中, 实现了不同分支机构数据的隔离, 并避免了地址的冲突, 使地址可以重复利用. 而总部不同业务部门的数据隔离, 测试方法相同, 在此不再赘述.

3) 分布式处理与负载均衡量的测试

传统方式采用一台边缘设备承载不同分支机构的私网数据, 而随着接入的分支机构的增多, 边缘设备的负载越来越重, 当负载达到边缘设备的极限时, 会影响私网数据的正常交互. 而该设计方案, 采用多台物理设备虚拟成一台逻辑设备, 形成一个网络资源池, 资源池所有的设备资源能进行统一的调度与管理, 由多台设备共同承载不同分支机构的私网数据, 通过分布

式处理的方式减轻设备的负载. 图 9 是通过抓包软件 Wireshark, 抓取 branch1 的地址 172.16.1.1 访问 h1 的 10.3.1.1 的情况; 图 10 是 branch2 的地址 172.16.1.1 访问 10.4.1.1 的情况, 图 9 表明 ed1 承载 branch1 访问 h1 的数据, 图 10 显示 ed2 承载 branch2 访问 h2 的数据, 进而实现了数据的分布式处理与负载分担.

(2) 性能对比

该设计思想采用多台边缘设备分担不同分支机构的私网数据, 实现了私网数据的分布式处理与负载均衡. 该设计理念相比传统方式, 还存在如表 1 的优势.

表 1 从 10 个维度将本文方案与传统方式进行了对比, 对比情况表明, 本文方案从可靠性、扩展性、可管理性等方面要优于传统方式.

```
[ed1]dis ip routing-table vpn-instance vpna protocol ospf

Summary count : 2

OSPF Routing table status : <Active>
Summary count : 1

Destination/Mask    Proto   Pre Cost        NextHop         Interface
172.16.1.1/32       O_INTRA 10  1           10.1.1.1        GE1/0/3

OSPF Routing table status : <Inactive>
Summary count : 1

Destination/Mask    Proto   Pre Cost        NextHop         Interface
10.1.1.0/24         O_INTRA 10  1           0.0.0.0         GE1/0/3
[ed1]dis ip routing-table vpn-instance vpnb protocol ospf

Summary count : 2

OSPF Routing table status : <Active>
Summary count : 1

Destination/Mask    Proto   Pre Cost        NextHop         Interface
172.16.1.1/32       O_INTRA 10  1           10.2.1.1        GE2/0/4

OSPF Routing table status : <Inactive>
Summary count : 1

Destination/Mask    Proto   Pre Cost        NextHop         Interface
10.2.1.0/24         O_INTRA 10  1           0.0.0.0         GE2/0/4
```

图 8 不同分机构的实例路由表

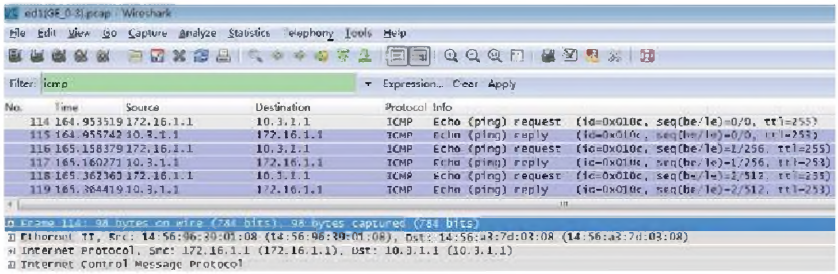

图 9 ed1 承载 branch1 访问 h1 的数据

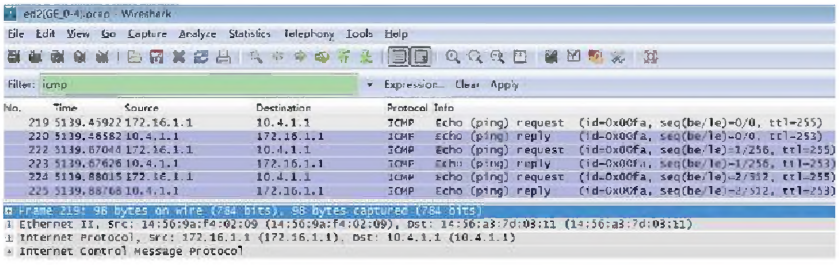

图 10 ed2 承载 branch2 访问 h2 的数据

表 1 本设计方案与传统方式的对比

对比名称	本文方案	传统方式
设备冗余	可以实现	不可以
跨设备的链路聚合	可以实现	不可以
网络部署速度	快	一般
扩展性	好	差
可管理性	好	一般
资源利用率	好	差
可靠性	高	低
可用性	高	一般
网络结构	简单	复杂
可维护性	好	一般

5 结束语

方案为了解决随着边缘设备接入的分支机构越来越多, 使得边缘设备需要处理的私网数据与公网数据暴增, 进而导致边缘设备负载过重, 影响其数据的正常交互, 进而提出了网络设备虚拟化技术 IRF 与 MPLS 和 BGP 技术深度融合的解决方案. 同时, 利用实验室设备实证了方案的可行性, 对方案进行了可用性、安全性、可靠性的测试, 并与传统方式构建的 VPN 进行了对比分析, 从测试与对比结果表明, 该方案能实现数据的分布式处理与负载分担, 相比传统方式存在有一定的优势, 是一种有效 VPN 解决方案. 因实验室条件有限, 无法

对方案的吞吐量、并发数进行测试. 下一步准备购买相关设备, 测试本文方案与传统方案的吞吐量与并发数, 并对测试结果进行对比分析, 总结出本方案的优势.

参考文献

1 段小焕. GRE over IPSec VPN 技术实现异地 WLAN 统一管理. 电子技术与软件工程, 2020, (6): 15–17.

2 彭治湘. L2TP over IPSec VPN NAT 穿越技术研究与实验仿真. 信息技术与信息化, 2020, (10): 204–206. [doi: 10.3969/j.issn.1672-9528.2020.10.065]

3 李超凡, 刘伟, 吴响, 等. 高性能 IPSec VPN 工程设计与仿真. 实验技术与管理, 2021, 38(2): 73–77.

4 张翔宇, 魏国伟. 基于 GRE 和 IPSec 的 MPLS L2 层 VPN 技术研究与实现. 网络空间安全, 2020, 11(5): 85–90. [doi: 10.3969/j.issn.1674-9456.2020.05.013]

5 李洁, 陈震, 孙蔚, 等. 基于 MPLS 的 VPN 技术应用于企业网络出局线路备份的构想. 通信技术, 2019, 52(5): 1167–1173. [doi: 10.3969/j.issn.1002-0802.2019.05.022]

6 宋高俊, 胡成, 周芳. 基于分层 PE 技术的 MPLS-VPN 架构优化. 计算机工程, 2017, 43(6): 66–72. [doi: 10.3969/j.issn.1000-3428.2017.06.011]

7 董旭源, 常鹏, 王宝亮, 等. 校园网 MPLS VPN 系统的设计研究. 计算机应用与软件, 2017, 34(10): 209–213. [doi: 10.3969/j.issn.1000-386x.2017.10.036]

8 王广泽, 汪鹏, 罗智勇, 等. 一种 MPLS VPN 的分散校区图书馆教育网组建模型. 哈尔滨理工大学学报, 2017, 22(3): 31–35.

9 李永芳. 一种跨域铁路数据网综合组网设计与仿真. 实验室研究与探索, 2021, 40(2): 102–108, 126.

10 圣文顺, 周诚, 孙艳文. MPLS VPN 在企业网络中的应用. 计算机技术与发展, 2020, 30(11): 117–122. [doi: 10.3969/j.issn.1673-629X.2020.11.022]

11 陶骏, 匡磊, 徐旺, 等. 基于 MPLS VPN 和 MSDP 的跨域组播网络设计. 计算机科学, 2017, 44(S1): 263–265, 287.

12 鲍磊磊, 唐红昇, 姜淑杨, 等. 基于 IRF2 和 LACP MAD 的气象网络设计研究. 计算机应用与软件, 2019, 36(1): 37–141.

13 王进文, 张晓丽, 李琦, 等. 网络功能虚拟化技术研究进展. 计算机学报, 2019, 42(2): 185–206.

14 周伟林, 杨芫, 徐明伟. 网络功能虚拟化技术研究综述. 计算机研究与发展, 2018, 55(4): 675–688. [doi: 10.7544/issn1000-1239.2018.20170937]

15 杨仕博, 张磊, 王华, 等. 大型企业资源池网络设备边界防护关键技术及设计. 网络安全技术与应用, 2018, (10): 106–108. [doi: 10.3969/j.issn.1009-6833.2018.10.057]