计算机科学 COMPUTER SCIENCE
http://www.jsjkx.com
DOI:10.11896/jsjkx.210400061

基于双层虚拟思想的边缘设备性能优化研究

陶志勇[1,2]　张　锦[2,3]　阳王东[2]　陈为满[1,3]
1 长沙民政职业技术学院软件学院　长沙 410004
2 湖南大学信息科学与工程学院　长沙 410082
3 湖南师范大学信息科学与工程学院　长沙 410012
(27537406@qq.com)

摘　要　随着运营商边缘设备接入用户数的不断增加,需要处理的数据量成倍增长,使边缘设备负载过重,从而影响了多协议标签交换与边界网关协议构建的虚拟私有网数据的正常交互。目前,MCE,HOPE,SDN 方案在解决该问题方面都存在一定的局限性:1)MCE 方式边缘设备接口不支持创建逻辑通道,因此该方案无法使用;2)HOPE 方式会产生路由环路等问题;3)SDN 方式单台 SDN 控制器处理并发的会话数不能超过 6.4 万。针对上述问题,文中提出了基于双层虚拟思想的边缘设备优化方案,该方案包括边缘设备虚拟化、虚拟私有网隧道建立、虚拟私有网信息隔离 3 个基本步骤。在此基础上,从网络模型、网络资源池的构建、网络资源池分裂 3 个方面进行方案优化。基于搭建的实验环境对方案性能进行评估,与传统方式构建的虚拟私有网在包转发率、可管理性、扩展性等方面进行了对比分析。结果表明,双层虚拟的设计方案通过构建网络资源池,实现了资源的统一调度与管理,能够有效解决运营商边缘设备负载过重的问题,是构建虚拟私有网的有效方案。

关键词:虚拟化;多协议标签交换;边界网关协议;虚拟私有网;边缘设备
中图法分类号　TP393

Study on Performance Optimization of Edge Devices Based on Two-layer Virtualization

TAO Zhi-yong[1,2],ZHANG Jin[2,3],YANG Wang-dong[2] and CHEN Wei-man[1,3]
1 Software School,Changsha Social Work College,Changsha 410004,China
2 College of Computer Science and Electronic Engineering,Changsha 410082,China
3 College of Computer Science and Electronic Engineering,Hunan Normal University,Changsha 410012,China

Abstract　With the continuous increase in the number of users which access to ISP's edge devices,the amount of data needs to be processed has doubled,which causes the edge device to be overloaded,and affects the normal interaction of the virtual private network data constructed by the multi-protocol label switching and the border gateway protocol. At this stage,the MCE,HOPE and SDN solutions all have certain limitations in solving this problem:the MCE mode edge device interface does not support the creation of logical channels,the solution cannot be used;the HOPE mode causes problems such as routing loops;the number of concurrent sessions processed by a single SDN controller in the SDN mode cannot exceed 64000. In response to the above problems,an edge device optimization solution based on dual-layer virtualization is proposed. This solution includes the following three basic steps:edge device virtualization,virtual private network tunnel establishment,and virtual private network information isolation. On this basis,the solution is optimized from the network model,the construction of the network resource pool and the splitting of the network resource pool. The performance of the solution is evaluated based on the experimental environment,and compared with the virtual private network constructed in the traditional way in terms of packet forwarding rate,manageability,and scalability. The analysis results show that the dual-layer virtual solution which is designed to construct a network resource pool can realize the unified scheduling and management of resources,effectively solve the overloaded problem of ISP's edge equipment,and also be an effective solution for building a virtual private network.

Keywords　Virtualization,Multi-protocol label switching,Border gateway protocol,Virtual private network,Edge device

到稿日期:2021-04-06　返修日期:2021-07-01
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(19C0106,17C0084);长沙民政职业技术学院"各类课题校级培育项目"项目成果(21mypy86)
This work was supported by the National Natural Science Foundation of China(61872127),Research Foundation of the Education Department of Hunan Province(19C0106,17C0084) and Achievements of "Various College-level Cultivation Projects" of Changsha Social Work College(21mypy86).
通信作者:张锦(mail_zhangjin@163.com)

1 引言

多协议标签交换[1]（Multi-protocol Label Switching，MPLS）与边界网关协议[2]（Border Gateway Protocol，BGP）构建的虚拟私有网（Virtual Private Network，VPN）因能使企业的员工随时随地办公，且具有部署快、灵活性好、成本低等优点，因此越来越受青睐[3]。特别是随着新冠疫情的蔓延，这种异地协同办公的需求更是呈爆炸式增长。而对于提供 VPN 服务的运营商来说，一台边缘设备需同时给上万甚至上十万用户提供 VPN 服务，使边缘设备负载过重，从而影响其数据的正常交互。因此如何给边缘设备减负是亟待解决的问题。

然而，MPLS 与 BGP 构建的 VPN 还存在扁平化的组网特点，即使处于接入层的运营商边缘设备的性能低于运营商网络中处于汇聚层与核心层的设备，也需要承受相同的数据处理量[4-5]。因特网工程任务组（Internet Engineering Task Force，IETF）RFC-2547 阐释了导致 MPLS 与 BGP 构建的 VPN 扁平化的原因，主要是运营商边缘设备不但需要处理来自公网的数据，而且还需要处理接入用户的私网数据，进而使边缘设备负载过重[6-8]。

MPLS 与 BGP 扁平化的组网特点以及边缘设备接入用户数的不断增加，会使运营商边缘设备负载越来越重。为了给运营商边缘设备减负，目前主要的方式有 3 种。一种是 MCE（Multi-VRF CE）方式，该方式让边缘设备只处理接入用户的私网数据，公网数据则交给边缘设备的上一层设备处理，进而减轻边缘设备的负担[9]；另外一种是 HOPE（Hiberarchy of PE）方式，其公网数据的处理与 MCE 方式一样，而对于私网数据的处理只需边缘设备承载一条默认路由，从而进一步减轻边缘设备的负担[10]；还有一种是 SDN 方式，在边缘设备上旁挂 SDN（Software Defined Network）控制器，边缘设备的控制报文由 SDN 控制器来处理，以减少边缘设备处理的数据量[11]。但不管是 MCE 与 HOPE，还是 SDN 方式，都存在欠缺。MCE 方式边缘设备的接口不支持创建逻辑通道，因此该方案无法使用；HOPE 方式违背了 BGP 技术的基本原理，会产生路由环路等问题；SDN 方式中单台 SDN 控制器只支持 6.4 万的会话能力，边缘设备交给 SDN 控制器处理的会话数超过该值时，SDN 控制器无法处理。因此，上述 3 种方式都有待进一步的研究[12-14]。

IRF（Intelligent Resilient Framework）[15]是一种基于云计算的网络虚拟化技术，在知网以 IRF 智能弹性架构为关键词检索（截止检索日期为 2021 年 5 月 10 日），检索到核心期刊论文 6 篇，非核心论文 13 篇，学位论文 3 篇。以上检索数据表明，对于该技术的研究尚处于起步阶段。而本文针对 MCE，HOPE，SDN 方式给边缘设备减负都存在局限性的问题，提出了一种双层虚拟的设计方案。通过 IRF 将多台边缘设备虚拟成一台逻辑设备，让多台边缘设备共同承载公网数据与私网数据的处理，实现数据的分布式处理与负载均衡，并在逻辑设备上采用 MPLS 与 BGP 构建 VPN，以保障接入用户私网数据的正常交互。同时，将该方案与传统方式构建的网络在吞吐率、包转发率、交换容量等维度进行数据对比，验证了双层虚拟方案的可用性、稳定性和可靠性[16-18]。

2 基于双层虚拟思想的边缘设备性能优化

2.1 设计思想

双层虚拟设计的第一层虚拟针对的是设备层的虚拟，采用 IRF 技术将两台或多台边缘设备虚拟成一台逻辑设备，即 N∶1 的虚拟化；第二层虚拟针对的是网络层的虚拟，采用 MPLS 与 BGP 技术在运营商的边缘设备上虚拟多个私有网，并分别给不同的用户提供异地办公服务，即 1∶N 的虚拟。设备层 N∶1 的虚拟构建了一个网络资源池，使所有边缘设备的资源都能通过网络资源池进行统一的调度与管理，接入用户的数据由资源池中的边缘设备共同负载分担；网络层 1∶N 的虚拟，控制不同用户的数据并分别由各自的虚拟私有网来承载，进而实现不同用户数据的隔离与负载分担。

2.2 网络模型

为了更好地阐释该设计思想相比传统方式的优越性，该方案构建了一个浓缩的网络模型，该模型采用两台边缘设备连接接入用户，而传统方式是采用一台边缘设备。图 1 给出了采用双层虚拟设计思想构建的网络模型。该模型将两台边缘设备虚拟成一台逻辑设备，构建一个网络资源池，让两台设备来负载分担其用户 A 的总部与用户 A 的分部和用户 B 的总部与用户 B 的分部的私网数据的交互。同时分别为不同用户构建其独立的虚拟私有网，并在公网中构建一条逻辑通道，由公网中的逻辑通道来承载不同用户的私网数据。

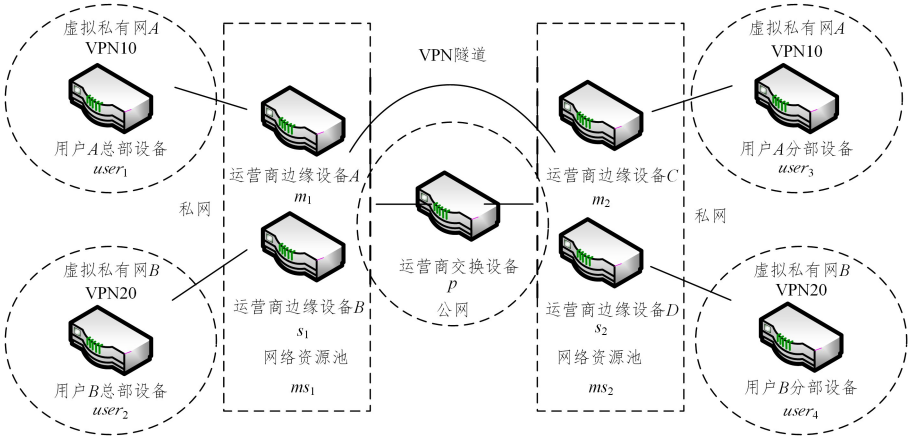


图 1 双层虚拟网络模型

Fig. 1 Two-tier virtual network model

为了便于后续描述，该方案对网络模型中的设备进行相应的定义。用户 A 总部设备与用户 B 总部设备分别表示为 $user_1$，$user_2$，用户 A 分部设备与用户 B 分部设备表示为 $user_3$，$user_4$；网络模型中连接用户 A 总部设备与用户 B 总部设备的运营商边缘设备 A、运营商边缘设备 B 分别表示为 m_1 和 s_1，两台边缘设备通过 IRF 技术虚拟化后的网络资源池称为 ms_1；网络模型中连接用户 A 分部设备与用户 B 分部设备的运营商边缘设备 C、运营商边缘设备 D 分别表示为 m_2 和 s_2，运营商边缘设备 C、运营商边缘设备 D 虚拟化后的网络资源池称为 ms_2；图 1 中公网的运营商交换设备表示为 p，运营商边缘设备给用户 A 总部设备与用户 A 分部设备构建的虚拟私有网 A 表示为 vpn_{10}；运营商边缘设备给用户 B 总部设备与用户 B 分部设备构建的虚拟私有网 B 表示为 vpn_{20}。

2.3 方案设计

图 1 所示的网络模型中实现 m_1 与 s_1、m_2 与 s_2 共同负载分担 $user_1$ 与 $user_2$、$user_3$ 与 $user_4$ 的私网数据，需完成边缘设备的虚拟化、虚拟私有网隧道的建立和虚拟私有网信息的隔离 3 个关键步骤，具体设计思路如下。

(1)边缘设备的虚拟化

图 1 中网络模型 m_1 与 s_1，m_2 与 s_2 能否成功虚拟化，直接影响接入用户的数据能否负载分担。采用 IRF 技术，通过在 m_1 与 s_1，m_2 与 s_2 上部署域、逻辑端口、优先级等配置，将运营商边缘设备 m_1 与 s_1 虚拟成 ms_1，m_2 与 s_2 虚拟成 ms_2。网络虚拟资源池形成后，资源池中的两台边缘设备共同承载 $user_1$ 与 $user_2$，$user_3$ 与 $user_4$ 的私网数据。而随着接入用户数的成倍增长，资源池中两台边缘设备如果还是存在负载过重的问题，则可以将更多的边缘设备加入网络资源池中，共同分担数据的处理。

(2)虚拟私有网隧道的建立

边缘设备虚拟化的完成为不同用户建立虚拟私有网打下了夯实的基础。若需在网络层建立虚拟私有网，则需要在 ms_1，p，ms_2 的公网设备上建立一条隧道，为不同用户的私网数据穿越公网提供路径。而 MPLS 技术构建的标签转发路径是一种天然的隧道技术，因此在 ms_1，p，ms_2 上采用 MPLS 技术来生成标签转发表，实现隧道的动态建立，在 ms_1，p，ms_2 上建立起一座“桥梁”，为 $user_1$ 与 $user_3$、$user_2$ 与 $user_4$ 私网数据的交互提供通道。

(3)虚拟私有网信息的隔离

MPLS 技术只是在公网中建立了一条逻辑通道，为不同用户的私网数据穿越公网提供了路径。而为不同用户构建其单独的虚拟私有网，实现其用户私网数据的信息隔离，则需 BGP 技术、多进程技术、虚拟路由技术相结合。图 1 中的 $user_1$ 与 $user_3$、$user_2$ 与 $user_4$ 分别处于虚拟私有网 vpn_{10}、vpn_{20} 中。实现 vpn_{10} 与 vpn_{20} 的信息隔离，需在图 1 的网络模型中采用本地隔离与交互隔离。本地隔离即采用多进程技术在 ms_1 上建立两个进程，将 ms_1 与 $user_1$ 和 $user_2$ 交互的私网数据分别导入各自的进程路由表中，并采用虚拟路由技术给 $user_1$ 与 $user_2$ 创建对应的实例，使 $user_1$ 与 $user_2$ 的进程和 $user_1$ 与 $user_2$ 的实例绑定，然后将 $user_1$ 与 $user_2$ 进程路由表中的私网信息导入各自的实例路由表中，完成其私网数据的本地隔离。ms_2 上的私网数据的本地隔离与上述方法相同，在此不再赘述。而 ms_1 与 ms_2 交互私网数据如何实现其数据的隔离，需要利用 BGP 的属性 RT 和 LABLE 来完成。在 ms_1 上给 $user_1$ 与 $user_2$ 的私网路由分配不同的 RT、LABLE 属性值，ms_2 同理。让 RT 和 LABLE 属性值分别与各自的实例绑定，交互私网数据时通过 RT 与 LABLE 值识别与区分该数据是属于哪一个用户的私网数据，进而实现不同用户数据的访问控制与隔离。

2.4 方案优化

上述设计理念采用 IRF 虚拟化技术与 MPLS 和 BGP 深度融合，将多台运营商边缘设备虚拟成一台逻辑设备，构建了网络资源池，通过网络资源池的多台物理设备共同承载不同用户的私网数据，进而实现数据的负载分担，并在运营商边缘上给每个用户构建其独立的虚拟私有网，保障了用户异地办公私网数据的正常交互。为使本设计方案更加稳定、健壮、可靠，从网络模型、网络资源池的构建和网络资源池分裂 3 个方面对方案进行优化。

(1)网络模型优化

图 1 所示的网络模型中，ms_1 与 $user_1$，$user_2$，p 设备，ms_2 与 $user_3$，$user_4$，p 设备通信时，采用的是单链路，一旦链路出现问题，则存在单点故障，从而影响到数据的正常交互。针对上述存在的问题，对设计方案进行以下优化，如图 2 所示。

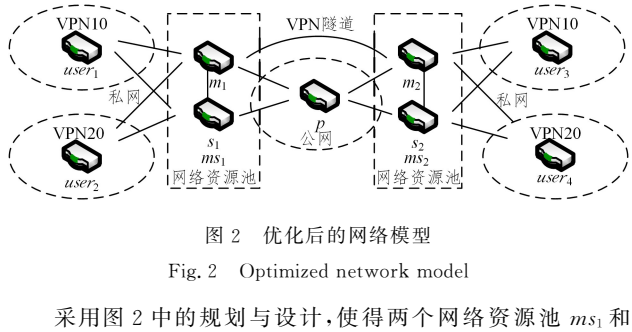


图 2 优化后的网络模型

Fig. 2 Optimized network model

采用图 2 中的规划与设计，使得两个网络资源池 ms_1 和 ms_2 分别与自己相连的 $user_1$，$user_2$，$user_3$，$user_4$，p 设备采用双链路的方式进行连接，通过将设备的两个物理端口绑定成一个逻辑端口来使用。当资源池中某台物理设备的链路或物理端口出现故障时，可以通过另外一台物理设备来完成用户数据的传输。这样不但在网络资源池实现了设备的冗余，而且还实现了链路的冗余，进而增加了网络的带宽，提高了通信时的稳定性，增强了网络的可靠性。

考虑到 m_1 与 s_1、m_2 与 s_2 设备相连采用的是单链路的方式。m_1 与 s_1、m_2 与 s_2 设备构建网络资源池后，如果两台相连的设备接口不稳定或者相连的链路存在问题，则会导致网络资源池产生分裂。由于网络资源池形成时主设备会将所有的信息同步到从设备，而一旦网络资源池分裂，两台设备地址等信息相同，会产生冲突，从而影响网络通信的正常交互。为加强网络资源池构建后的可用性与稳定性，在 m_1 与 s_1 或者 m_2 与 s_2 上采用环形连接的方式，如图 3 所示。

(2)网络资源池构建优化

图 3 为用环形连接的方式将两台物理设备虚拟成一台逻辑设备，当单条链路或接口发生故障时，可以通过另外一条链路与接口来完成协议报文与数据报文的交互，保障了网络资源池的正常运行，加强了网络资源池的稳定性与可靠性。

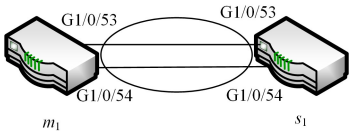


图 3 资源池构建优化拓扑

Fig. 3 Resource pool construction optimized topology

(3)网络资源池分裂优化

环形连接方式构建的网络资源池可以避免因单链路出现故障而导致网络资源池不能正常工作的问题。但是，如果两条链路都出现故障，则同样会引起网络资源池中物理设备的分裂，使得分裂的物理设备有相同的 IP 地址信息，引起地址冲突。解决问题的一种思路是在构建的网络资源池中增加一条链路，利用双向转发检测(Bidirectional Forwarding Detection，BFD)中的扩展字段携带检测 IRF 的有关信息，实时监控网络资源池的状态。图 4 给出了在 ms_1 和 ms_2 上部署 BFD 检测机制的结果。

图 4 通过 BFD 检测机制来检测资源池的状态，一旦发现资源池中的物理设备分裂，使资源池中的从设备的相应端口 down 掉，就只转发协议报文，不转发业务报文，避免产生地址等信息冲突，增强了网络资源池的健壮性与可靠性。

```
[m1]dis bfd session
 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 session working in control packet mode:

 LD/RD            SourceAddr      DestAddr        State  Holdtime    Interface
 129/129          192.168.1.1     192.168.1.2     Up     1891ms      Vlan3
[m2]dis bfd session
 Total Session Num: 1     Up Session Num: 1     Init Mode: Active

 IPv4 session working in control packet mode:

 LD/RD            SourceAddr      DestAddr        State  Holdtime    Interface
 129/129          192.168.2.1     192.168.2.2     Up     1213ms      Vlan5
```

图 4 BFD 检测机制的结果

Fig. 4 BFD detection mechanism result

3 性能分析

3.1 实验设置

为了验证其方案设计理念的可行性，利用实验室的 H3C S5800-60C 交换机，搭建方案所需实验模型，模拟出项目环境，测试其方案的可用性、可行性和稳定性。具体的实现分为以下 3 步来完成，其实验模型如图 5 所示。

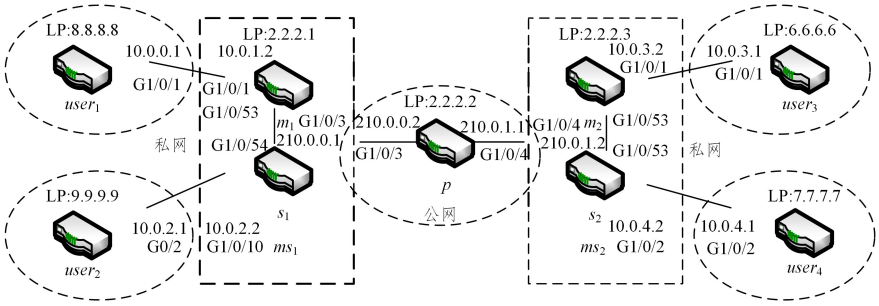


图 5 方案实验模型图

Fig. 5 Scheme experimental model diagram

(1)边缘设备虚拟化的实现

边缘设备是否成功虚拟化，关系到私网数据的负载分担能否实现。而实现实验模型中 m_1 与 s_1 设备的虚拟化，需在 m_1 与 s_1 上采用 irf member 指令分配成员编号，并将其连接的物理接口通过 irf-port 指令加入到相应的逻辑端口，同时激活配置让 m_1 与 s_1 进行竞争选举，竞选成功的一方成为网络资源池中的 master，另外一方则成为网络资源池中的 standby。而对于 m_2 与 s_2 设备的虚拟，其方法与 m_1 和 s_1 相同，在此不再赘述。通过上述方法在 m_1 与 s_1、m_2 与 s_2 上构建的网络资源池状态结果如图 6 所示，成员编号为 1 的 m_1 与 m_2 通过竞争选举为 master，成员编号为 2 的 s_1 与 s_2 被选为 standby，上述状态说明已成功完成 m_1 与 s_1、m_2 与 s_2 的虚拟化。

```
<m1>dis irf
MemberID    Role      Priority  CPU-Mac          Description
 *+1        Master    1         3618-9401-0304   ---
   2        Standby   1         3618-977e-0404   ---
--------------------------------------------------
 * indicates the device is the master.
 + indicates the device through which the user logs in.

 The bridge MAC of the IRF is: 3618-9401-0300
 Auto upgrade                : yes
 Mac persistent              : 6 min
 Domain ID                   : 0
<m2>dis irf
MemberID    Role      Priority  CPU-Mac          Description
 *+1        Master    1         3618-bbbc-0604   ---
   2        Standby   1         3618-be35-0704   ---
--------------------------------------------------
 * indicates the device is the master.
 + indicates the device through which the user logs in.

 The bridge MAC of the IRF is: 3618-bbbc-0600
 Auto upgrade                : yes
 Mac persistent              : 6 min
 Domain ID                   : 0
```

图 6 网络资源池构建图

Fig. 6 Network resource pool construction diagram

(2)虚拟私有网隧道的实现

在该实验模型中，在 ms_1，p，ms_2 公网设备上建立一条传输私网数据的逻辑通道，使私网数据能跨越公网中的 p 设备，实现其不同用户私网数据的交互，需 3 个步骤来完成。首先在 ms_1，p，ms_2 设备上启动其 MPLS 的功能，其次在 3 台设备上执行 mpls lsr-id 指令，分别给 ms_1 的 2.2.2.1、p 设备的 2.2.2.2、ms_2 的 2.2.2.3 标识设备在 MPLS 协议中的身份，再次在 ms_1，p，ms_2 设备及对应接口上执行标签分发协议(Lable Distribution Protocol，LDP)，给设备分配对应的标签并使其设备与接口能处理 MPLS 协议报文的能力。图 7 是完成上述部署后，查看 p 设备的 mpls 邻居与标签转发表的状态，operational 的状态结果表明 p 设备与 m_1、m_2 建立好邻居关系，且 2.2.2.1，2.2.2.2，2.2.2.3 分别获得了相应的 in 与 out 标签，标签转发表已形成，即隧道已建立。

```
<p>dis mpls ldp peer
Total number of peers: 2
Peer LDP ID          State        Role    GR   MD5  KA Sent/Rcvd
2.2.2.3:0            Operational  Passive Off  Off  2/2
2.2.2.1:0            Operational  Active  Off  Off  3/3
<p>dis mpls ldp lsp
Status Flags: * - stale, L - liberal, B - backup
FECs: 3          Ingress: 2          Transit: 2          Egress: 1

FEC              In/Out Label        Nexthop         OutInterface
2.2.2.1/32       -/1151(L)
                 -/3                 210.0.0.1       GE1/0/3
                 1151/3              210.0.0.1       GE1/0/3
2.2.2.2/32       3/-
                 -/1150(L)
                 -/1151(L)
2.2.2.3/32       -/1150(L)
                 -/3                 210.0.1.2       GE1/0/4
                 1150/3              210.0.1.2       GE1/0/4
```

图 7 MPLS 邻居与标签状态图

Fig. 7 MPLS neighbor and label state diagram

(3)虚拟私有网信息隔离的实现

给实验模型中的 $user_1$ 与 $user_3$、$user_2$ 与 $user_4$ 构建独立的虚拟私有网,关键是在 ms_1 与 ms_2 上实现其数据的隔离。按照方案设计中虚拟私有网信息的隔离方法来完成实验的部署后,其设备的状态结果如图 8 所示。图 8 中方框说明 $user_1$ 与 $user_3$、$user_2$ 与 $user_4$ 分别学习到对方的路由后,将学习到的路由导入自身对应的实例路由表,说明不同用户的私网数据已纳入各自的实例路由表中管理,实现了数据的隔离。

```
<m1>dis ip routing-table vpn-instance vpn10 | exclude Dir

Destinations : 15        Routes : 15

Destination/Mask    Proto   Pre Cost        NextHop         Interface
6.6.6.6/32          BGP     255 2           2.2.2.3         GE1/0/3
8.8.8.8/32          O_INTRA 10  1           10.0.1.1        GE1/0/1
10.0.3.0/24         BGP     255 0           2.2.2.3         GE1/0/3
<m1>dis ip routing-table vpn-instance vpn20 | exclude Dir

Destinations : 15        Routes : 15

Destination/Mask    Proto   Pre Cost        NextHop         Interface
7.7.7.7/32          BGP     255 2           2.2.2.3         GE1/0/3
9.9.9.9/32          O_INTRA 10  1           10.0.2.1        GE2/0/10
10.0.4.0/24         BGP     255 0           2.2.2.3         GE1/0/3
<m2>dis ip routing-table vpn-instance vpn10 | exclude Dir

Destinations : 15        Routes : 15

Destination/Mask    Proto   Pre Cost        NextHop         Interface
6.6.6.6/32          O_INTRA 10  1           10.0.3.1        GE1/0/1
8.8.8.8/32          BGP     255 2           2.2.2.1         GE1/0/4
10.0.1.0/24         BGP     255 0           2.2.2.1         GE1/0/4
<m2>dis ip routing-table vpn-instance vpn20 | exclude Dir

Destinations : 15        Routes : 15

Destination/Mask    Proto   Pre Cost        NextHop         Interface
7.7.7.7/32          O_INTRA 10  1           10.0.4.1        GE2/0/2
9.9.9.9/32          BGP     255 2           2.2.2.1         GE1/0/4
10.0.2.0/24         BGP     255 0           2.2.2.1         GE1/0/4
```

图 8 网络资源池 ms_1 和 ms_2 的 vpn_{10} 与 vpn_{20} 实例路由表

Fig. 8 Routing table of vpn_{10} and vpn_{20} instance of network resource pool ms_1 and ms_2

3.2 性能分析

为了评估方案的有效性,将双层虚拟设计理念构建的虚拟私有网与传统方式采用单台边缘设备或多台边缘设备独立工作后构建的虚拟网进行了定性与定量对比,对比情况如表 1 所列。

(1)定性对比

表 1 列出了两种方案在 7 个维度上的对比数据,对比分析表明,采用本文方案构建的虚拟私有网在可靠性、维护性、设备利用率等方面优于传统方式构建的虚拟私有网。

表 1 方案特性对比

Table 1 Scheme feature comparison

对比项目	本文方案	传统方式
可靠性	高(能实现设备与链路的冗余)	一般(只能实现链路的冗余)
交换容量	大	小
吞吐率	高	低
收敛时间	快	慢
MTTR	毫秒级	秒级
维护性	好	一般
设备利用率	高	低

(2)定量对比

定量对比包括包转发率、管理性、扩展性 3 个方面,对比情况如下。

1)包转发率

采用 IRF 技术可以将多台物理设备虚拟成一台逻辑设备,从而构建网络资源池。在资源池中,多台物理设备共同承载与分担数据接收与转发,有效解决了标签边缘设备负载过重的问题,并有效地提高了设备的数据处理能力。图 9 中本文设计方案与传统方式都采用 H3C S5800-60C 设备来构建虚拟私有网,单台设备的包转发率是 213 Mpps。本文方案随着网络资源池中交换机数量的增加,所有交换机的资源能进行统一的管理与调度,当资源池中的边缘设备数达到 9 台时,其包转发率能达到 1 917 Mpps。而采用传统方式构建的虚拟私有网,由于每台交换机都是独立运行的,即使增加交换机,也无法实现资源的融合,且设备的包转发率也没有增长。

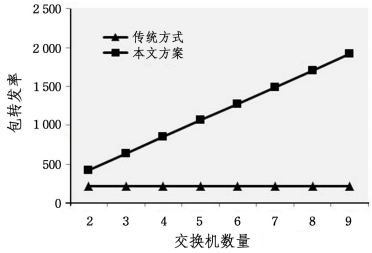


图 9 两种方案包转发率的对比

Fig. 9 Comparison of packet forwarding rate of two schemes

2)管理性

随着运营商网络接入的用户数不断增加,需要的交换机也会不断增多。本文方案采用的 H3C S5800-60C 设备最多可以支持 9 台设备进行虚拟化,虚拟化后在一台主设备中可以管理与部署资源池中的其他设备,无需单独对每一台设备进行管理与部署,大大减轻了管理人员的工作负担。图 10 给出了本文方案与传统方案随着交换机数量的增加在管理交换机数量上的对比,当交换机达到 72 台时,本文方案只需要在 9 台设备上完成所有交换机的管理与部署,而采用传统方式需要对每台设备进行单独的管理与部署。而当交换机达到几百、上千台时,该方案的可管理性优势更加明显。

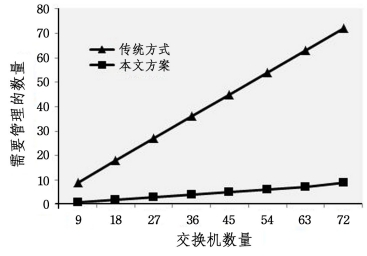


图 10 两种方案交换机管理数量的对比

Fig. 10 Comparison of the number of switches managed by two solutions

3)扩展性

因为本文方案可以将多台物理交换机通过 IRF 技术虚拟成一台逻辑交换机,在逻辑交换机上实现资源的统一调配与管理,所以能够有效解决传统方式随着用户数的增多交换机端口数不够用的问题。下式可计算该方案在网络资源池的逻辑节点上可供用户连接的交换机端口数:

$$N = X * Y \sum_{i=1}^{3} N_i * M_i$$

其中,N 表示该方案资源池中可以提供用户连接的端口总数;X 为资源池中交换机的数量;Y 表示不同类型的板卡数量;N_i 为交换机的主控板数、业务板卡数以及扩展板卡数;M_i 表示交换机不同类型板卡的端口数。上述公式表明,随着交换机数量的增加,网络资源池供用户连接的端口数不断增长。而传统方式中各交换机独立运行,不能实现设备资源的整合,因此设备的交换机端口数无法扩展。图 11 给出了以 H3C S5800-60C 设备为例,本文设计方案与传统方式交换机端口

扩展情况的对比。本文方案可以将 9 台物理设备虚拟成一台逻辑设备，而一台物理设备的主控板、业务板、扩展板可供用户连接的端口数共有 84 个，随着资源池中物理设备的增加，扩展的端口数量就越多。图 11 中的对比数据显示，本设计方案的扩展性优于传统方案。

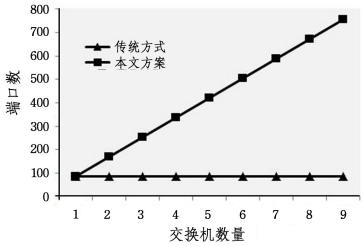


图 11 两种方案的端口数对比

Fig. 11 Comparison of the number of ports in the two schemes

结束语 运营商边缘设备随着接入用户数的增多而负载过重，从而影响其数据的正常交互。为此，本文提出了双层虚拟思想的设计方案，让 IRF 与 MPLS 和 BGP 技术深度融合，并对该设计方案在稳定性、健壮性、可靠性方面进行了优化，有效地解决了设备负载过重的问题。为了评估方案的优越性，本文从包转发率、管理性、扩展性等 10 个维度与传统方式进行了对比分析。对比数据表明，双层虚拟设计方案优于传统方式，为解决运营商边缘设备过载的问题提供了新的思路与路径，是一种有效的解决方案。因实验室设备条件有限，无法测试方案的时延、收敛性。下一步准备购买相应设备，测试本文方案与传统方式在时延、收敛性方面的情况，并对两种方案的测试结果进行对比，总结出本文方案的优势。此外，还将进一步研究 IRF、MPLS 和 BGP 技术在跨域中的应用。

参 考 文 献

[1] QIAN X D. Application of MPLS VPN technology in Jiangyin City Emergency Broadcasting System Network [J]. China Cable TV, 2021(3): 241-244.

[2] LI J, CHEN Z, SUN W. The concept of MPLS-based VPN technology applied to enterprise network outgoing line backup[J]. Communication Technology, 2019, 52(5): 1167-1173.

[3] WANG H Y. Research on the Application of MPLS in Military Informatization Construction[D]. Dalian: Dalian University of Technology, 2010: 72-84.

[4] LI Y F. Simulation design of enterprise cross-domain networking based on BGP MPLS VPN[J]. Laboratory Research and Exploration, 2021, 40(3): 121-128.

[5] SONG G J, HU C, ZHOU F. MPLS-VPN architecture optimization based on layered PE technology[J]. Computer Engineering, 2017, 43(6): 66-72.

[6] SHENG W S, ZHOU C, SUN Y W. The application of MPLS VPN in enterprise networks [J]. Computer Technology and Development, 2020, 30(11): 117-122.

[7] DONG X Y, CHANG P, WANG B L, et al. Design and research of campus network MPLS VPN system[J]. Computer Applications and Software, 2017, 34(10): 209-213.

[8] WANG G Z, WANG P, LUO Z Y, et al. An MPLS VPN-based model for building education network of decentralized campus library[J]. Journal of Harbin University of Science and Technology, 2017, 22(3): 31-35.

[9] ZHANG X Y, WEI G W. Research and Implementation of MPLS L2 Layer VPN Technology Based on GRE and IPSec[J]. Cyberspace Security, 2020, 11(5): 85-90.

[10] KANG B H, BALITANAS M O. Vulnerabilities of VPN using IPSec and defensive measures[J]. International Journal of Advanced Science and Technology, 2009, 8(7): 9-18.

[11] SHENG W S, ZHOU C, SUN Y W. Application of MPLS VPN in Enterprise Networks[J]. Computer Technology and Development, 2020, 30(11): 117-122.

[12] HONG X J. The Application of Virtual Network Technology in Computer Network Security[J]. Network Security Technology and Application, 2020(10): 41-43.

[13] HUANG S P, XIE J, KAN H Y. Research on the Application of IRF Virtualization Technology in the Network[J]. Experimental Technology and Management, 2014, 31(11): 124-126.

[14] BAO L L, TANG H S, JIANG S Y, et al. Research on the design of meteorological network based on IRF2 and LACP MAD[J]. Computer Applications and Software, 2019, 36(1): 37-141.

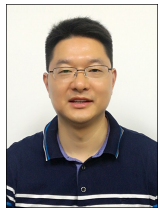
[15] CHEN M, TAO X M, HU C, et al. Design and implementation of network test platform based on network function virtualization[J]. Chinese Journal of Computers, 2018, 41(9): 2016-2028.

[16] ABENI L, KIRALY C, LI N, et al. On the performance of KVM-based virtual routers [J]. Computer Communications, 2015, 38(5): 40-53.

[17] WANG J W, ZHANG X L, LI Q, et al. Research progress of network function virtualization technology[J]. Chinese Journal of Computers, 2019, 42(2): 185-206.

[18] ZHOU W L, YANG X, XU M W. Overview of Research on Network Function Virtualization Technology [J]. Computer Research and Development, 2018, 55(4): 675-688.

TAO Zhi-yong, born in 1980, postgraduate, associate professor, is a member of China Computer Federation. His main research interests include network communication and cloud computing.



ZHANG Jin, born in 1979, postgraduate, Ph. D, professor, Ph. D supervisor, is a member of China Computer Federation. His main research interests include network communication, cloud computing and software engineering.