doi: 10.7690/bgzdh.2023.10.004

MPLS-VPN 在跨场区航天数据网中的应用

白　宁，范利波
（中国人民解放军 63819 部队，四川 宜宾 644000）

摘要：对分布在不同城市的跨场区航天数据网而言，依托航天骨干网构建各分站内部私有专用网络是迫切所需。将 MPLS-VPN（多协议标签交换虚拟专用网），多层标签技术应用到航天数据网中，达到高速转发业务数据和增强其稳定性及安全性。介绍 MPLS-VPN 的原理及关键技术，结合跨场区航天数据网建设的现状提出一组 MPLS-VPN 航天数据网结构，分析使用 MPLS-VPN 实现组网的部署情况，并且实验仿真跨场区航天数据网的组网环境。用 2 种常用的用户业务数据为场景，通过测试网络的性能指标，验证了采用 MPLS-VPN 架构方案的优点。

关键词：MPLS-VPN；航天数据网；隔离加密；网络仿真
中图分类号：V417^{+}.9　　**文献标志码：**A

Application of MPLS-VPN in Space Data Network of Cross-field

Bai Ning, Fan Libo
(*No*. 63819 *Unit of PLA*, *Yibin* 644000, *China*)

Abstract: For the space data network distributed in different cities, it is an urgent need to build a private network within each substation relying on the space backbone network. MPLS-VPN multilayer label technology is applied to the aerospace data network to achieve high-speed forwarding of business data and enhance its stability and security. This paper mainly introduces the principles and key technologies of MPLS-VPN, proposes a set of MPLS-VPN aerospace data network structure combined with the current situation of cross-field aerospace data network construction, analyzes the deployment of using MPLS-VPN to achieve networking, and simulates the networking environment of cross-field aerospace data network through experiments. Using two kinds of common user service data as the scene, through the test of network performance indicators, the advantages of MPLS-VPN architecture are verified.

Keywords: MPLS-VPN; aerospace data network; isolation and encryption; network simulation

0　引言

随着 5G 网络建设和算力网络的加快部署，物联网和人工智能应用层出不穷。在航天数据网中，由于测控站分布广，使得 MPLS-VPN 技术可以充分应用在航天数据网中，跨地区的局域网内部互联是发展的趋势，这就需要高效传递内部数据的同时保证内部信息安全可靠。随着多协议标签交换（multi-protocol label switching，MPLS）的不断发展，MPLS-VPN 相对于传统的 VPN 隧道，具有路由传递简单、数据组装效率高、配置组网方便等特点。笔者在讨论 MPLS 和 VPN 原理及关键技术的基础上，结合两者应用场景上的优点，论证了 MPLS-VPN 在公共网络上安全传递私有数据的可行性。在充分研究 MPLS-VPN 可靠技术基础之上，对建设跨场区的航天业务局域网提供一种灵活性强、可扩展性好的方案，包括网络的拓扑结构设计、技术特性优势分析等。满足不同业务数据的安全性与隐私性，同时实现路由交换的灵活性，以此适用未来高速发展的航天数据网应用扩展及信息化发展[1-2]。

1　MPLSVPN 原理及发展趋势

1.1　MPLS 产生原因

MPLS 是在共享通信网上使用标签建立路由路径传递数据，相比较 IP 路由方式传递更加高速、高效的新技术。其中多协议是指 MPLS 可以配合多种网络层协议和链路层协议共同建立标签路径。随着 Internet 的丰富发展，骨干网需要传递大容量、低时延的数据，而采用 IP 路由协议逐跳查找和转发效率低，无法满足高速的转发需求。当 5G 技术和云边端技术的不断发展，用户使用实时视频、智能设备终端的交互场景越来越多，需要大带宽实时性强的传输网络迫在眉睫。通常将 MPLS 协议看成 TCP/IP 协议中的 2.5 层，位于 2 层数据链路层协议和 3 层路由协议的中间层，它包含了 3 层路由寻址和 2 层

收稿日期：2023-06-08；**修回日期：**2023-07-05
作者简介：白　宁（1984—），男，重庆人，硕士。

数据帧转发的特点，通过标签建立路径，使得业务数据在此路径上固定的多次转发。传统的网络层 IP 路由是逐跳的选路转发，而 MPLS 标签转发通过标签建立一条标签转发路径，不依赖于 IP 路由表达到了面向连接的特性，降低了网络运维管理的复杂难度。虽然最初 MPLS 的产生是为了提高路由转发效率，但它还可以与其他的多做协议配合应用，如在异构网络中的流量策略设计和 QOS 服务保证中，是实现 IP 网络流量分配和避免拥塞控制的有效解决方案。MPLS-VPN 技术相结合，在解决跨地区内部互联、多业务扩展保证数据安全可靠等方面也是主要的解决方案。

1.2 MPLS-VPN 的原理

MPLS-VPN 采用 MPLS 技术在公共网络上构建专用网络，就如同 VPN 技术一样可以形成 1 条在公共网络中的专用网络隧道，它采用标签交换，1 个标签对应 1 个业务数据流，因此能较好地将不同 VPN 用户间的数据隔离，提高了安全性。同时，MPLS 自身有丰富的流量控制属性设置，可以利用区分服务做到流量工程，优化网络资源，自动快速修复网络故障，提供高可靠性和可用性。此外 MPLS 中所建立的标签转发路径 LSP 转发方式是面向连接的，一旦路径建立完成，数据就不需要通过 IP 路由逐条转发，而直接在网络层以下按照标签路径转发，减少了设备的 CPU 开销值[3-5]。从网络层次上看，MPLS-VPN 有 2 种模式：基于 MPLS 第 2 层 VPN 和基于 MPLS 第 3 层 VPN[4]。2 层 VPN 采用 MAC 帧头封装数据，3 层 VPN 使用 IP 报头封装数据。目前现网中采用 3 层 MPLS-VPN 较多，它支持多种 2 层协议与 IP 网络兼容性好。3 层 MPLS-VPN 与 BGP 协议配合使用，产生了多协议扩展(MP-BGP)，是 L3MPLS-VPN 的一种实施模式。在基础网络互连的前提下，使用 MP-BGP 协议，通过 MPLS 协议的路由器来创建 LSP 隧道，LSP 隧道不需要通过路由表转发，以此实现异构网络之间的互联。采用这种模式对跨场区航天数据网进行组网构建，网络拓扑结构如图 1 所示。

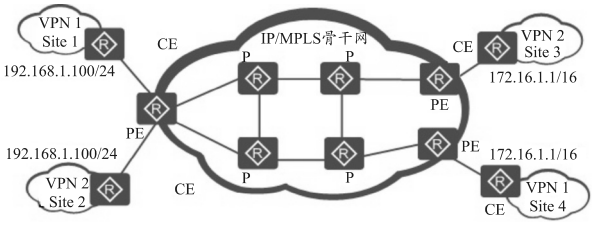

图 1 典型 MPLS-VPN 组网拓扑

1.3 MPLS 研究现状及发展趋势

MPLS-VPN 技术以及从理论研究进入到与实践共同发展阶段，随着国内运营商、科研院校以及大型企业多类业务访问需求增加，对现网中使用的 MPLS-VPN 技术的灵活扩展性、数据安全性、高宽带传输性及可靠性有了更高的要求。目前的研究主要集中在以下几点：

1) 虚拟路由算法：对 MPLS 网络的流量算法研究主要是为了提高网络传输速率和链路质量，MPLS 路由算法的改进可以融合全网资源，增强网络性能；其中国外学者在文献[6]中提出了使用改进的服务分级算法来优化 MPLS 网络中发生流量拥塞和丢包故障；国内学者在文献[7]中提出了快速重路由的 MPLS 网络优化算法。

2) 优化提升 QoS 服务质量：对 MPLS-VPN 的服务策略配置进行优化，目的就是提升网络的传输效率、降低流量拥塞等故障。目前国内外学者针对 MPLS 不同的组网模式下服务策略配置优化方案提出了多种方案。

3) 优化组网架构：由于我国的 MPLS 网络是从原来的 3 级经典网络结构中演变而来，与 MPLS 的扁平网络结构存在差异，国内外学者在优化组网架构给出了多种方案，有效地提升了网络的拓展性。

MPLS-VPN 作为目前大型企业组网改建设计方案广泛使用的 VPN 组网技术，在未来融合 IPV6 互联网过渡方案中，充分利用 IPV6 的安全特性和 QOS 特性改善和加强 MPLS-VPN，提升其可靠性[8]。同时，不断完善标准化程度，使得多家厂商设备互联互通，也是未来 MPLS-VPN 技术发展方向。

2 基于 MPLS-VPN 的航天数据网模型仿真

2.1 航天数据网拓扑结构简图

航天数据网按全国分布情况可以划分很多区域网络。以 A 区域网络为例，包括 a1 场区、a2 场区、a3 场区和 a4 场区以及 a0 核心骨干区这 5 个区域，基于 MPLS-VPN 的网络拓扑可设计如图 2 所示。充分考虑各种业务终端系统对承载网络不同的性能要求，根据每种业务类型特点，网络性能参数分类建立虚拟专用网络，保证各场区同骨干区域 a0 的 VPN 互联，不同场区不同业务数据流之间无法访问，达到各个业务数据之间的独立可靠。根据核心骨干网的覆盖范围，骨干网内不设置 P 路由器，核心骨干网内部通过 PE 路由器进行相互联接，各个场区的边缘 CE 路由器作为接入核心骨干网的

VPN 服务器，保证安全性。

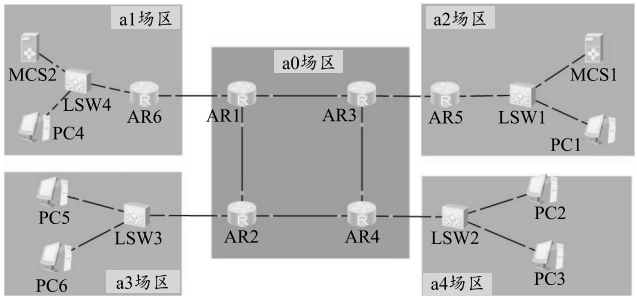

图 2　MPLS VPN 实现航天数据网拓扑

2.2　仿真实验

1) 实验参数说明。

根据对航天数据网结构的理论分析，MPLS-VPN 架构决定采用 Option A 方案，仿真实验使用华为网络仿真工具 ENSP 和 wireshark 抓包工具来搭建网络拓扑，配置主要的路由协议实现相互连通，以达到实验的仿真环境。使用的 ENSP 版本为 1.2.00.330，实验过程中使用华为 AR220 路由器和 S5700 交换机，wireshark 版本为 1.4.3，这款工具可以针对 ENSP 中的路由器线路上的流量进行抓包分析。

此实验中模拟航天数据网共使用了 8 台路由器，通过配置不同的数据流属性来模拟 2 个常规业务流：IPTV 组播数据和 FTP 文件传输。其中核心网的 R1-R4 路由器作为 MPLS-VPN 网络的 PE 路由器，创建不同的业务应用 VPN 实例；而各个场区的边缘交换机作为 CE 设备，汇聚各个场区内部用户业务数据。划分 IP 地址做了如下规划：MPLS 域内采用 10.0.0.0/8 的 A 类私有网段地址，方便区别不同的设备种类，如需要路由聚合配置时方便进一步简化路由表条目数量，提高网络地址的使用率，降低了设备运维管理难度。实验过程中操作接口对接不易出错，拓扑结构简单清晰。

网络业务的划分分别由 4 个 CE 交换机引入，a1 场区的 CE1 负责场区所有业务流量管理，CE2 负责 IPTV 流量，CE3 负责 FTP 文件传输流量，CE4 负责 IPTV 组播流量。IPTV 和 FTP 文件传输流量通过 MPLS-VPN 网络中的 PE 路由器进入骨干区域网络互连，跨场区的相同业务之间就可以通过 MPLS-VPN 创建的 LSP 路径直接互连，而不同场区的不同业务之间由于没有可达的路径，无法互连，这就做到了业务之间的隔离。A0 骨干网的 PE 路由器之间运行 OSPF 底层协议达到互连互通，OSPF 协议适合大范围的网络，没有跳数限制，能够快速感知路由状态变化，并且根据算法可以避免环路产生；PE 路由器之间采用 MP-BGP 协议；PE 与 CE 之间采用 BGP 协议与 OSPF 协议相互引入路由，同时 PE 路由器创建业务数据实例。

2) 实验操作。

根据网络模型搭建拓扑结构如图 3 所示。

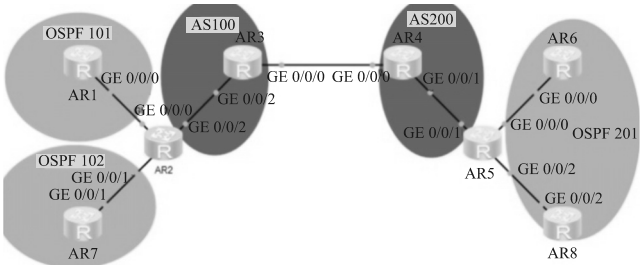

图 3　搭建实验拓扑

各路由器接口信息如表 1 所示。

表 1　设备组网 IP 地址

设备	接口	IP 地址掩码 24 位	所属 AS 区域
AR1	GE0/0/0	192.168.11.10	OSPF101
AR2	GE0/0/0	192.168.11.20	OSPF101
AR2	GE0/0/1	192.168.21.20	OSPF102
AR2	GE0/0/2	10.1.23.2	BGP100
AR3	GE0/0/0	10.1.34.3	BGP100
AR3	GE0/0/2	10.1.23.3	BGP100
AR4	GE0/0/0	10.1.34.4	BGP200
AR4	GE0/0/1	10.1.45.4	BGP200
AR5	GE0/0/0	192.168.12.50	OSPF201
AR5	GE0/0/1	10.1.45.5	BGP200
AR5	GE0/0/2	192.168.22.50	OSPF201
AR6	GE0/0/0	192.168.12.60	OSPF201
AR7	GE0/0/1	192.168.21.70	OSPF102
AR8	GE0/0/2	192.168.22.80	OSPF201

当整个航天数据网没有运行 MPLS 协议时，场区之间互连仅用 OSPF 内部 IGP 互联和 BGP 协议场区间互连，R1 的全局路由表中不仅有 R6 的路由条目，还包含达到其他场区路由器的路由条目，可以看出，采用这样的互相连接方式没有对不相干的路由进行路由隔离。如图 4 所示，同理观察 R7 也有这样的问题。

```
<AR1>dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 18        Routes : 18

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        1.1.1.1/32  Direct  0    0           D   127.0.0.1       LoopBack0
        2.2.2.2/32  O_ASE   150  1           D   192.168.11.20   GigabitEthernet
0/0/0
        3.3.3.3/32  O_ASE   150  1           D   192.168.11.20   GigabitEthernet
0/0/0
        4.4.4.4/32  O_ASE   150  1           D   192.168.11.20   GigabitEthernet
0/0/0
        5.5.5.5/32  O_ASE   150  1           D   192.168.11.20   GigabitEthernet
0/0/0
        6.6.6.6/32  O_ASE   150  1           D   192.168.11.20   GigabitEthernet
0/0/0
        7.7.7.7/32  O_ASE   150  1           D   192.168.11.20   GigabitEthernet
0/0/0
        8.8.8.8/32  O_ASE   150  1           D   192.168.11.20   GigabitEthernet
0/0/0
     10.1.23.0/30   O_ASE   150  1           D   192.168.11.20   GigabitEthernet
0/0/0
     10.1.45.4/30   O_ASE   150  1           D   192.168.11.20   GigabitEthernet
0/0/0
```

图 4　R1 全局路由表

在 R1 路由器上使用 ping 命令来查看到达业务对端网络的连通性，如图 5 所示。

```
<AR1>ping 6.6.6.6
  PING 6.6.6.6: 56  data bytes, press CTRL_C to break
    Reply from 6.6.6.6: bytes=56 Sequence=1 ttl=251 time=140 ms
    Reply from 6.6.6.6: bytes=56 Sequence=2 ttl=251 time=100 ms
    Reply from 6.6.6.6: bytes=56 Sequence=3 ttl=251 time=120 ms
    Reply from 6.6.6.6: bytes=56 Sequence=4 ttl=251 time=110 ms
    Reply from 6.6.6.6: bytes=56 Sequence=5 ttl=251 time=120 ms

  --- 6.6.6.6 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 100/118/140 ms
```

图 5　R1-R6 的时延情况

从图中看出，从 R1 对 R6 进行 Ping 测试连通性，从源地址 R1 的 1.1.1.1 发包到目的地址 6.6.6.6 的 R6 最低延时为 100 ms，最高延时为 140 ms，平均延时为 118 ms。时延抖动达到了 22 ms。

接下来采用 MPLS-VPN 方案实现互联，首先在 MPLS 骨干网中配置底层 OSPF 协议使之相互连通，开启各个路由器互连接口的 MPLS 功能和 MPLS LDP 标签自动分配功能，查看路由和标签分配信息，保证 IGP 协议和 MPLS 工作正常。在核心网中 R2，R3，R4，R5 与分场区互连的接口上开启 MPLS 功能，并且创建 VPN 实例，通过查看 MPLS 标签分发状态，确认是否创建了 LSP 路径，如图 6 所示。

```
[AR2]dis mpls lsp
------------------------------------------------------------------------------
                LSP Information: BGP LSP
------------------------------------------------------------------------------
FEC                 In/Out Label  In/Out IF                      Vrf Name
1.1.1.1/32          1025/NULL     -/-                           1
192.168.11.0/24     1026/NULL     -/-                           1
------------------------------------------------------------------------------
                LSP Information: LDP LSP
------------------------------------------------------------------------------
FEC                 In/Out Label  In/Out IF                      Vrf Name
2.2.2.2/32          3/NULL        -/-
3.3.3.3/32          NULL/3        -/GE0/0/2
3.3.3.3/32          1024/3        -/GE0/0/2
```

图 6　MPLS 的 LSP 标签分配

同时再次在 R1 上查看路由表，确认不相干的路由条目已经被隔离掉，如图 7 所示。从图中可以看到，在 a1 场区与 a6 场区只进行组播业务情况下，没有其他场区的路由条目，做到了路由隔离，增加了信息的安全性，减少了维护难度。

```
<AR1>dis ip routing-table
Route Flags: R - relay, D - download to fib
------------------------------------------------------------------------------
Routing Tables: Public
         Destinations : 11        Routes : 11

Destination/Mask    Proto   Pre  Cost      Flags NextHop         Interface

        1.1.1.1/32  Direct  0    0           D   127.0.0.1       LoopBack0
        6.6.6.6/32  O_ASE   150  1           D   192.168.11.20   Ethernet0/0/0
       10.1.23.0/24 OSPF    10   2           D   192.168.11.20   Ethernet0/0/0
       10.1.34.0/24 O_ASE   150  1           D   192.168.11.20   Ethernet0/0/0
       10.1.45.0/24 O_ASE   150  1           D   192.168.11.20   Ethernet0/0/0
        127.0.0.0/8 Direct  0    0           D   127.0.0.1       InLoopBack0
        127.0.0.1/32 Direct  0    0           D   127.0.0.1       InLoopBack0
   192.168.11.0/24  Direct  0    0           D   192.168.11.10   Ethernet0/0/0
  192.168.11.10/32  Direct  0    0           D   127.0.0.1       Ethernet0/0/0
   192.168.12.0/24  O_ASE   150  1           D   192.168.11.20   Ethernet0/0/0
```

图 7　R1 的路由表

使用 ping 的来测试网络的延时情况如图 8 所示。从图中可以看出：测试时延时间变小了，如果在现实环境中，两地距离上百公里情况下，时延的减少会更加明显，传输性能得到较大提升。

```
<AR1>ping 6.6.6.6
  PING 6.6.6.6: 56  data bytes, press CTRL_C to break
    Reply from 6.6.6.6: bytes=56 Sequence=1 ttl=255 time=40 ms
    Reply from 6.6.6.6: bytes=56 Sequence=2 ttl=255 time=30 ms
    Reply from 6.6.6.6: bytes=56 Sequence=3 ttl=255 time=50 ms
    Reply from 6.6.6.6: bytes=56 Sequence=4 ttl=255 time=30 ms
    Reply from 6.6.6.6: bytes=56 Sequence=5 ttl=255 time=50 ms

  --- 6.6.6.6 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 30/40/50 ms
```

图 8　改进后的 R1-R6 时延情况

3　实验结果分析

通过实验仿真的对比结果可以看出，MPLS-VPN 技术可以实现路由信息隔离，与传统的 VPN 技术相比，不需要增加不同站点间的隧道和额外的报文加密，减少了运维管理难度，网络配置简单高效；使用了 MP-BGP 协议同多种 IGP 路由协议联合引入，同时通过 CIDR 能够支撑广域网海量的路由条目数量，采用路由聚合可简化路由器中的路由表，节省存储空间；由于 MPLS 是搭建在已有底层互连路由协议之上的协议，不改变当前现有的网络拓扑结构，配置更加简单高效，节省网络升级成本；此外，通过实验也验证了采用 MPLS-VPN 的数据传输速率得到了提升，相对于传统 IP 路由网络，能够降低异地场区间网络延迟和丢包率，减少时延抖动；如新增业务终端时，只需在 CE 路由器上增加业务终端节点的路由，同时配置与之连接的 PE 的业务实例，就可以实现场区间业务互连，扩展性强，而骨干网络中其他 PE 路由器等无需任何修改，降低了运维管理难度，出现故障易排查，减少了硬件的关联。由此可见，在远距离的跨场区航天数据网中采用 MPLS-VPN 技术能够实现低成本高性能的网络服务。

4　结束语

笔者首先讨论了 MPLS 和 VPN 的工作原理，论述了 MPLS-VPN 融合运用的关键技术，分析了 MPLS-VPN 的技术特点和使用场景。将 MPLS-VPN 技术应用于跨场区航天数据网建设的需求相结合，提出了用 MPLS-VPN 技术实现跨场区航天数据网的组网方案，通过实验仿真的方法，搭建了具备核心功能的网络架构，对比使用传统 IP 路由技术与使用 MPLS-VPN 技术的网络性能指标差异，论证 MPLS-VPN 技术在跨场区航天数据网中应用，具有安全性好、扩展性强等优点。

（下转第 20 页）