MPLS VPN 在企业网络中的应用

圣文顺,周　诚,孙艳文
(南京工业大学浦江学院,江苏 南京 211200)

摘　要:对分布在不同城市的跨城域大型公司而言,依托 Internet 构建公司内部私有专用网络是迫切所需。VPN 技术就是在公用网络上建立专用网络并进行加密通讯,这种网络技术具有数据共享和数据传输的功能,其优势是具有安全性、稳定性、便捷性和扩展性,同时还可以提高企业或公司的网络管理水平,在企业网络中已经得到了广泛应用。但依托 Internet 构建的 VPN 网络在流量、稳定性和安全性方面依旧面临着许多威胁,MPLS 是将 IP 技术与 ATM 技术融合的产物,更好地实现了路由选择和数据交换功能。它包含了第二层标记交换特点和第三层路由的特性,通过结合二层的数据链路协议和三层的路由转发技术,有效解决了当前网络状况下的数据分组转发问题。该文主要讨论在企业核心网络中使用 MPLS VPN 来实现不同业务部门之间的隔离与加密,以确保业务数据的信息传输安全。

关键词:MPLS VPN;企业专网;多协议标签交换;隔离加密;网络安全;虚拟专用网
中图分类号:TP391　　**文献标识码**:A　　**文章编号**:1673-629X(2020)11-0117-06
doi:10.3969/j.issn.1673-629X.2020.11.022

Application of MPLS VPN in Enterprise Network

SHENG Wen-shun, ZHOU Cheng, SUN Yan-wen
(Nanjing Tech University Pujiang Institute, Nanjing 211200, China)

Abstract: For large cross-metropolitan companies distributed in different cities, it is urgent to build private networks within the company based on the Internet. VPN technology is to establish a private network on the public network and carry out encrypted communication. This network technology has the functions of data sharing and data transmission. Its advantages are security, stability, convenience and expansibility, and it also can improve the network management level of enterprises or companies, which has been widely used in enterprise networks. However, the VPN network built on the Internet still faces many threats in terms of traffic, stability and security. MPLS, as the product of the integration of IP technology and ATM technology, better realizes routing and data exchange functions. It includes the characteristics of Layer 2 Layer Label Switching and Layer 3 Routing. By combining Layer 2 Data Link Protocol and Layer 3 Routing and Forwarding Technology, it effectively solves the problem of data packet forwarding under current network conditions. We mainly discuss the use of MPLS VPN in enterprise core network to achieve the isolation and encryption between different business departments to ensure the security of business data transmission.

Key words: MPLS VPN; enterprise private network; multiprotocol label switching; isolated encryption; network security; virtual private network

0　引　言

90 年代初,随着社会与经济的不断发展,互联网流量快速增长,众多企业进入了互联网云时代。由于许多公司不在同一个地点办公,因此一所跨城域大型公司可能包括多个子公司和办事处。NAT 虽然可以满足基本需求,但由于过去硬件技术的限制,路由器采用最长匹配算法[1]逐跳转发数据包,成为网络数据转发的瓶颈,因此快速路由技术[2]成为当时研究的一个热点。

MPLS(multi-protocol label switching)即多协议标签交换技术,VPN 则是指虚拟专用网络。MPLS VPN 技术是运用多协议标签交换技术在主干网络上构建关于企业的 IP 虚拟局域网,从而实现了网络在不同地区的应用,具备快速、高效、安全的特性。MPLS VPN 能

收稿日期:2019-05-13　　**修回日期**:2019-09-16
基金项目:国家重点研发计划重点专项(2017YFC0803700);江苏省 2019 年度高校自然科学研究项目(19KJD520005);江苏省 2019 年度江苏省大学生创新创业训练计划项目(201913905009Y);南京工业大学浦江学院 2018 年度大学生创新创业训练计划项目(PJ201813905020)
作者简介:圣文顺(1979-),男,讲师,研究方向为机器学习、智能推荐。

为不同的网络用户提供差别性的服务,它将公共网络的多样性、拓展性、可靠性并结合流量工程等相关网络技术体现出来,从而让网络的使用更为快速、高效。在各种方案中,IETF 确定 MPLS 协议作为标准的协议。MPLS 采用短而定长的标签进行数据转发[3],大大提高了硬件限制下的转发能力;而且 MPLS 可以扩展到多种网络协议(如 IPv6,IPX 等)。随着设备硬件性能不断提升,MPLS 在提高数据转发速度上的优势逐渐弱化,但其支持多层标签嵌套[4]和设备内转控分离[5]的特点,使其在 VPN、TE 等新兴应用中得到了广泛应用。

1 MPLS VPN 的产生原因

众所周知,目前 IPv4 地址的可用资源已经趋于枯竭,并且已经成为了制约网络发展的瓶颈,因此 NAT(network address translation)技术[6-7]应运而生。NAT 方式通过满足通信的基本要求,进行网络通信,但是也必然存在一定的缺陷。

首先,NAT 方式要对应路由器来开启 NAT 进程,因此会加大路由器的负荷;其次,NAT 方式容易造成局域网的 IP 地址对外不可见,使得分公司和办事处无法直接访问总部内部的应用程序。随着互联网在软件应用中地位的逐渐提升,带宽大和时延低也成为一种需求。

为了满足更快的数据传输率,每个路由器生产商进行了大批量的改进和研究工作,例如思科公司为路由器优化了路由表搜索算法并添加了 CEF 等功能。但仍旧不能彻底解决当前互联网市场所存在的问题。

MPLS 技术的诞生是两个曾经相互对立的 ATM 和 IP 技术融合的产物。MPLS 技术兼顾了 IP 技术信令简单和 ATM 交换引擎高效的优点。IP 设备厂商和 ATM 设备厂商,都是在各自原来的基础上实现 MPLS 技术。相对于 IP 设备厂商而言,它并不是修改了原有的 IP 包封装于二层链路帧中的规范,而是在二、三层包头之间增加了一个标签。ATM 设备厂商则使用标签来代替 VPI/CVI 概念,并且需要在 ATM 交换机上修改信令控制代码,确保路由协议可实现不同路由之间三层信息的传递。

在图 1 中,AR1 与 AR2 的 loopback1 接口的地址都是属于私网地址,由于它们不在同一块网络中,若它们的 IP 地址同为 172.16.1.1,是不会产生冲突的;然而,若是将这种情况放入 VPN 网络中,传统的 VPN 网络结构中的设备是无法识别用户重叠的路由信息的。因此 MPLS VPN 的出现解决了传统 VPN 技术的固有缺陷之一,即地址空间的重叠问题。

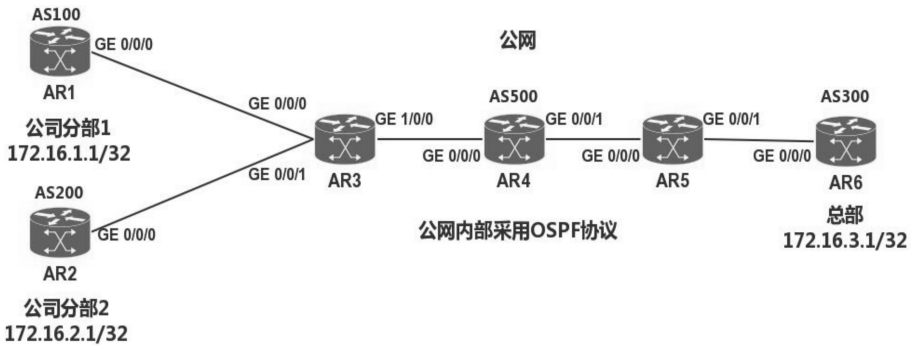

图 1 网络体系结构

2 选择路由协议来承载 MPLS VPN

MPLS 技术的核心优势是利用标签列表的查找代替传统路由表的递归查询,从而实现标签的快速交换,提高数据传输速率。MPLS 在解决大数据量网络传输速度的同时,还需要考虑客户数据的保密性问题,于是催生了 MPLS VPN。MPLS VPN 是 MPLS 技术与 VPN 的结合,通常应用在大型企业与运营商内部。MPLS VPN 提供了路由反射、环路避免、流量工程和负载均衡等多种优化服务,但是如何选择路由协议去承载 MPLS VPN,无疑是当下一大难点。

一般的 IGP 协议只能用来承载 IPV4 报文,然而这是远远不够的,MP BG 报文的出现解决了无法承载 VPN 报文和 IPV6 报文的问题。它在承载 VPN 报文的同时还携带一些必要的扩展属性。因此该文给出如下选择方法来选择路由协议:

(1)公共网络上的 VPN 路由数量庞大,BGP 是唯一支持大量路由的协议[8];

(2)BGP 的报文基于 TLV 的结构[9-10],便于扩展;

(3)BGP 可以承载附加在路由后面的任何信息,并作为可选属性传递给其他邻居;

(4)本地路由冲突的问题:可以通过在同一台 PE 设备上为不同的 VPN 建立单独的路由,这样冲突的路由就被隔离开来;

(5)在路由传递过程中,为不同的 VPN 路由添加

不同的标识以示区别,这些标识可作为 BGP 属性[11-12]进行传递;

(6)由于 IP 报文不可更改,可以在 IP 报文头前加一些信息。由始发路由器打上标记,接收路由器在收到带标记的数据包时,根据标记转发给正确的 VPN。

3　在网络传递过程中区分冲突路由

将 VPN 路由发布到全局路由表之前,使用一个全局唯一的标识和路由绑定,用以区分冲突的私网路由[13]。这个标识被称为 RD(route distinguisher)。

RD 即 VPN 路由标识符[14],由 8 字节组成,用于区分相同地址空间的 IPv4 前缀,配置时同一 PE 设备上分配给每个 VPN 的 RD 必须唯一。增加了 RD 的 IPv4 地址称为 VPN-IPv4 地址(即 VPNv4 地址)[15]。运营商设备采用 BGP 协议作为承载 VPN 路由的协议,并将 BGP 协议进行了扩展,称为 MP-BGP(multiprotocol extensions for BGP-4)[16]。PE 从 CE 接收到客户的 IPv4 私网路由后,将客户的私网路由添加各种标识信息后变为 VPNv4 路由放入 MP-BGP 的 VPNv4 路由表中,并通过 MP-BGP 协议在公网上传递。

由于 CE 与 PE 间路由协议的规划,其设备之间需要交互路由信息。由于 MPLS VPN 是三层 VPN 网络,因此 CE 节点设备必须选择三层设备。三层设备指接入层、汇聚层、核心层,即是指 MPLS VPN 技术在网络中通过三个层次来进行设计与应用。核心层的作用是调节并疏散网络中的信息;接入层的作用是做到全面化、系统化来满足网络交互与隔离的需求;汇聚层的作用则是做好处理和分析工作,提升网络服务。CE 与 PE 设备间采用静态路由协议,方便了维护人员进行管理并减少了维护的复杂度。

4　MPLS VPN 企业网的安全策略

MPLS VPN 为了实现网络的安全性,通过采取隔离用户路由信息和隔离用户地址等方法来提高标记欺骗和抵抗外部入侵的目的。MPLS 是一种隧道技术,使用它来建立 VPN 十分高效。但是 MPLS 技术本身非常新颖,所以对 MPLS VPN 的安全性从多方面做了一个详细的、适用于 BGP 的分析和介绍。

在用户网络边缘设备 CE(customer edge)上,有接口直接与服务提供商 SP(service provider)网络相连,CE 可以是 SVN、交换机或一台主机。通常情况下,CE "感知"不到 VPN 的存在,也不需要支持 MPLS。服务提供商边缘设备 PE((provider edge)则与 CE 直接相连,在 MPLS 网络中,对 VPN 的所有处理都发生在 PE 上。

若在 CE 节点和 PE 节点之间运行动态路由协议,则 CE 路由器的 IP 地址是 PE 路由器唯一了解的 VPN 网络内部信息。要将 MPLS 网络核心隐藏,则需要将 CE 和 PE 路由器设置为静态路由。MPLS VPN 网络对数据信息和传输安全保障的具体方法如下:

(1)MPLS 核心层。

RD(路由标志:route distinguisher)的唯一性保证了用户在无需进行 NAT,甚至不用任何变动的情况下,依旧可以保留原有的 IP 地址和应用,并穿过基于 MPLS 的 VPN。使得 IP VPN 与用户 IP 网络的集成更加容易、便捷。

在 MPLS VPN 网络中,为了保证每个端点的唯一性,供应商将定义的唯一的一个 RD 和 VPN 的 IP 地址一一结合。用户保留自己的私有地址而无需通过 NAT 或者供应商所给的地址,原因是 VPN 相关节点的 FIB 中存入了 VPN 的 IP 地址入口信息,且这些信息都将通过流量路由找到它对应的节点。

一般连接 EXTRANET VPN,需要通过 RD 定义的两个 VPN 之间的信任关系。因为两个相连之间可以实现 VPN 互连根本意识不到其余 VPN 的存在。

(2)MPLS-VPN 加密保证安全性。

BGP(border gateway protocol)规定哪些路由信息可以通过哪些属性和协议进行通信。每个 VPN 的唯一 RD 和逻辑端口号决定了 VPN 成员的属性。然而用户并不知道 RD 的值,只能通过定义的端口才能通信。为了让每个边缘 LSR 只保存和自己相关的 FIB(forwarding information base)表和 VPN 信息,BGP 在 LSR 之间交换 FIB 表进行更新,并且这种更新只能发生在 LSR 上,加强了其安全性和保密性。

因为每个用户的 RD 都是由其逻辑端口号所决定,而 RD 在一开始定义时只与某个 VPN 相关联,所以用户只能访问相关联的 VPN。由于用户只能意识到这个 VPN,因此通过加密来保证其安全性。

(3)数据的完整性保障。

数据的完整性通过 MPLS VPN 对普通数据包进行选择封装来实现。每个路由节点收到的数据包都由 MPLS 协议进行封装,然后按标签分类进行交换。因而不需要对整个数据包进行识别,保证了数据的完整性。

(4)路由隔离。

VPN 之间的路由隔离是由 MPLS VPN 来实现的。路由隔离是指每个虚拟路由转发实例(VFI)都是由连接每个的 VPN 的 PE 路由器来维护的,其驻留都来自同一 VPN。每个 VPN 都会产生一个相对独立的 VFI,所以不会被该 PE 路由器上其他 VPN 影响。

然而在穿越 MPLS 核心到其他路由器时,往往会

将 BGP 的信息重新分发给核心网络,因此在多协议 BGP 里增加了唯一的 VPN 标志符来实现隔离。这种隔离只将路由信息重新分发,并将保存到特定的 VFI 中。所以穿过 MPLS 的每个 VPN 路由之间都是独立、隔离的。

5 MPLS VPN 的配置说明

模拟 MPLS VPN 仿真网络,进行虚拟局域网络逻辑结构统一、基于公网进行内网数据传输的可靠性测试实验,目的是验证 MPLS VPN 技术满足跨区域企业专用网络的相关技术要求。

5.1 配置需求

分部与总部之间采用 MPLS VPN 进行通信,用户与运营商之间使用 BGP 协议传递路由。如图 1 所示,配置 MPLS VPN 需要从以下两个方面考虑:用户侧设备的配置和运营商骨干网络的配置。

用户侧设备的配置主要考虑 CE 与 PE 之间使用何种协议将私网路由传递到运营商网络;而运营商骨干网络的配置需要从以下三个方面考虑:运营商骨干网络 IGP 协议的配置,保证运营商网络路由可达;VPN 的配置,将私网路由通过运营商设备封装并传递;MP-BGP 与 MPLS 协议的配置,实现私网路由的传递与标签隧道[17]的建立。专用 PE 设备分工明确,每个 PE 设备只保存自己的 VPN 路由,P 设备只保存公网路由。因此解决共享 PE 设备上地址空间重叠的思路是:

将专用 PE 设备与 P 设备的功能在同一台 PE 设备上完成,并实现 VPN 路由的隔离。其实传统 VPN 解决地址冲突的问题也存在一些方法:使用 ACL,NAT 等,但这些办法都没能从本质上解决问题。要想彻底解决问题,必须在理论上有所突破。可以从专用 PE 上得到启示,专用 PE 设备分工明确,每个 PE 只保存自己的 VPN 路由,P 设备只保存公网路由。而现在的思路是:将专用 PE 设备与 P 设备的功能在一台 PE 设备上完成。在共享 PE 设备上使用 VRF 技术将重叠的路由隔离:每个 VPN 的路由放入自己对应的 VPN Routing Table 中。

PE 设备在维护多个 VPN Routing Table 时,同时还维护一个公网的路由表。

5.2 配置思路

前提 1:直连 IP 地址可达,地址不冲突,线路无故障。

前提 2:IGP 可达,IP 路由表中存在 MPLS VPN 建立邻居使用 loopback 地址。检测的时候使用 ping -a 挂源去 ping。

前提 3:BGP 邻居关系建立。MPLS VPN 使用的是 MP-BGP,所以想要实现 VPN,就要先建立 BGP 的邻居关系[18],否则向上层前提检查。如果上层前提没问题,检查 peer 是否指定,IPv4 地址簇[19]是否指定 peer ip 地址 enable。

5.3 配置 MPLS VPN

(1)首先全局使用 MPLS 和 mpls ldp。

建议配置 mpls lsr-id(建议一台设备的所有 ID,都最好统一)。

```
mpls lsr-id 3.3.3.3
mpls
#
mpls ldp
```

(2)创建 VPN 实例。

创建 VPN 实例的时候需要配置 RD 值和 RT 值,其中 RD 值负责形成 VPNv4 地址(格式为 RD+IPV4 地址)。

RT 值负责不同 VRF 表的加入,本端出方向值与对端入方向值[20]相同,对端才能加入本端发过去的表,数据是有去有回。因此,对端的出方向要和本端的入再一致。有时候配置起来 RT 的出和入使用的都是一个值,RD 值和 RT 值工程师人为规划就可以。骨干网创建实例与设置 RT(route target)属性配置代码如下:

```
ip vpn-instance zhouchneg1
ipv4-family
  route-distinguisher 1:1
  vpn-target 12:3 export-extcommunity
  vpn-target 3:12 import-extcommunity
#
ip vpn-instance zhoucheng2
ipv4-family
  route-distinguisher 2:2
  vpn-target 12:3 export-extcommunity
  vpn-target 3:12 import-extcommunity
```

(3)接口处理。

下行接口因为要将网络添加到不同的 VRF 表中,因此,下行接口或者连接 CE、连接终端的接口要绑定到 VPN 实例中,在配置的时候,先绑定实例,再配置 IP 地址等信息,不然一旦绑定就会将接口的信息全部清空。上行接口以及 P 设备沿途的接口需要在接口下使能 MPLS、使能 mpls ldp,用于标签的传递。总结起来就是下行接口绑实例,上行接口转发标签。在接口上绑定 VPN 的配置代码如下:

```
interface GigabitEthernet0/0/0
ip binding vpn-instance zhouchenhg1
ip address 10.1.13.3 255.255.255.0
interface GigabitEthernet0/0/1
ip binding vpn-instance zhoucheng2
```

```
ip address 10.1.23.3 255.255.255.0
```

(4)配置 MP-BGP。

在 BGP 的 VPNV4 地址中,peer 对等体,然后将不同协议学来的路由分别引入进内网即可。使用 BGP 传递路由的代码如下:

```
bgp 500
peer 5.5.5.5 as-number 500
peer 5.5.5.5 connect-interface LoopBack0
#
ipv4-family unicast
  undo synchronization
  peer 5.5.5.5 enable
#
ipv4-family vpnv4
  policy vpn-target
  peer 5.5.5.5 enable
#
ipv4-family vpn-instance zhoucheng1
  peer 10.1.13.1 as-number 100
#
ipv4-family vpn-instance zhoucheng2
  peer 10.1.23.2 as-number 200
```

5.4　用户设备核心配置

用户设备的配置主要是为了使得总部与分公司之间互相通达,但各分公司之间则实现网络隔离(见图 2 ~ 图 4)。

```
The device is running!

<rl>ping -a 172.16.1.1 172.16.3.1
  PING 172.16.3.1: 56 data bytes, press CTRL_C to break
    Reply from 172.16.3.1: bytes=56 Sequence=1 ttl=252 time=50
    Reply from 172.16.3.1: bytes=56 Sequence=2 ttl=252 time=40
    Reply from 172.16.3.1: bytes=56 Sequence=3 ttl=252 time=40
    Reply from 172.16.3.1: bytes=56 Sequence=4 ttl=252 time=40
    Reply from 172.16.3.1: bytes=56 Sequence=5 ttl=252 time=40

---172.16.3.1 ping statistics---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 40/42/50 ms
```

图 2　总部与分部互 ping 可通

```
<rl>ping 172.16.2.1
  PING 172.16.2.1: 56 data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

---172.16.2.1 ping statistics---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
```

图 3　分公司之间网络隔离

```
<rl>ping 10.0.13.1
  PING 10.0.13.1: 56 data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

---10.0.13.1 ping statistics---
    5 packet(s) transmitted
    0 packet(s) received
    100.00% packet loss
```

图 4　分公司与公网成功隔离

具体的配置代码如下:

```
bgp 100
peer 10.1.13.3 as-number 500
#
ipv4-family unicast
  undo synchronization
  network 172.16.1.1 255.255.255.255
  peer 10.1.13.3 enable


bgp 200
peer 10.1.23.3 as-number 500
#
ipv4-family unicast
  undo synchronization
  network 172.16.2.1 255.255.255.255
  peer 10.1.23.3 enable
```

6　结束语

通过该文的解析可以很清楚地发现,在企业网络中部署 MPLS VPN,可以非常有效地增强企业网络通信的安全性,只有总部才会知道所有分部门的具体信息,而分部门之间是无法通信的,运营商也无法学习到各个分部门的路由信息。

MPLS VPN 技术在广域网以及其他网络的相关应用,应结合用户与市场的实际需求,才能使国内企业不断发展并稳步向前。广域网在 MPLS VPN 技术应用的支持下,日益提升网络的安全,以此达到满足国内企业网络通信安全发展的目的。未来的网络安全情况很是严峻,MPLS VPN 在一定程度上解决了企业通信安全的问题,但是配置很复杂,对于运维人员来说也是一个不小的挑战。

参考文献:

[1] BENSALAH F, KAMOUN N E, BAHNASSE A. Analytical performance and evaluation of the scalability of layer 3 tunneling protocols: case of voice traffic over IP[J]. International Journal of Computer Science and Network Security, 2017,

17(4):361-369.
[2] 颜云生,陶 骏,夏傅仪,等. 基于 AHP 算法的电子书包评估系统[J]. 计算机系统与应用,2017,26(8):49-54.
[3] 陶 骏,沈 阳,王 丽,等. 基于 SDN 的 QoS 多播网络仿真[J]. 大庆师范学院学报,2017,37(6):42-47.
[4] BAHNASSE A,KAMOUN N E. Policy-based smart adaptive quality of service for network convergence[J]. International Journal of Computer Science and Information Security,2015,13(3):21-27.
[5] 潘德伟. 关于 MPLS VPN 技术的网络安全性探讨[J]. 数字技术与应用,2017(7):202-203.
[6] BAHNASSE A, KAMOUN N E. A policy based management of a smart adaptive QoS for the dynamic and multipoint virtual private network[J]. International Journal of Control and Automation,2016,9(5):185-198.
[7] 陶 骏,赵 林,王 淼,等. 基于 NAT 和 FIT AP 的实验室无线网络构建[J]. 计算机与网络,2017,43(20):68-70.
[8] 林岚君. 电信运营商 IP 承载网发展策略研究[J]. 电信快报,2014(8):17-20.
[9] WILLIAMSON B. IP 多播网络的设计与部署[M]. 北京:人民邮电出版社,2011:476-482.
[10] BENSALAH F,KAMOUN N E,BAHNASSE A. Evaluation of tunnel layer impact on VOIP performances (IP-MPL S-MPLS VPN-MPLS VPN IPsec)[J]. International Journal of Computer Science and Network Security,2017,17(3):87-92.
[11] 李 皓. IP 承载网系统设计与实现[D]. 北京:北京工业大学,2013.
[12] KUMAR C R,DHANUMJAYULU C,BAGUBALI A,et al. Architecture for MPLS L3 VPN deployment in service provider network[J]. Journal of Telecommunications System & Management,2017,6(1):152-155.
[13] 高 羽,王 当. IPSec 技术在 MPLS VPN 安全保障中的运用[J]. 信息与电脑,2016(18):186-187.
[14] 宋高俊,胡 成,周 芳. 基于分层 PE 技术的 MPLS-VPN 架构优化[J]. 计算机工程,2017,43(6):66-72.
[15] 王晓贺,赵 伟. 基于 MPLS VPN 的电信级多业务 IP 承载网设计研究[J]. 无线互联科技,2016(5):4-5.
[16] 侯剑锋,马明凯. MPLS VPN 中 PE-CE 互连仿真研究[J]. 计算机工程,2010,36(12):123-125.
[17] BAHNASSE A,TALEA M,LOUHAB F E,et al. SAS-IMS for smart mobile security in IP multimedia subsystem[C]// Proceedings of the 2017 international conference on smart digital environment (ICSDE ′17). Rabat, Morocco: ACM, 2017:35-41.
[18] 闫长江,吴东君. SDN 原理解析[M]. 北京:人民邮电出版社,2016:100-105.
[19] SHAHZAD A, HUSSAIN M. IP backbone security: MPLS VPN technology[J]. International Journal of Future Generation Communication and Networking,2013,6(5):61-62.
[20] DOUGLAS E C. 用 TCP/IP 进行网络互连:第 2 卷[M]. 北京:电子工业出版社,2009:130-157.

(上接第 116 页)

[11] 教育部. 教育部关于一流本科课程建设的实施意见[EB/OL]. 2019-10-30. http://www. moe. gov. cn/srcsite/A08/s7056/201910/t20191031_406269. html.
[12] 林 健. 面向未来的中国新工科建设[J]. 清华大学教育研究,2017,38(2):26-35.
[13] DECUIR J. Introducing bluetooth smart: part 1: a look at both classic and new technologies[J]. IEEE Consumer Electronics Magazine,2014,3(1):12-18.
[14] DECUIR J. Introducing bluetooth smart: part II: applications and updates[J]. IEEE Consumer Electronics Magazine, 2014,3(2):25-29.
[15] 封亚辉,王亚春,戴东情,等. 基于测试的可穿戴设备风险评估和安全认证[J]. 网信军民融合,2019(6):60-63.
[16] 李雪妍,陈 伟,杜俊雄. 物联网僵尸网络的恶意域名检测技术研究[J]. 计算机技术与发展,2019,29(8):113-118.
[17] ARIAS O,WURM J,HOANG K,et al. Privacy and security in internet of things and wearable devices[J]. IEEE Transactions on Multi-Scale Computing Systems,2015,1(2):99-109.
[18] 秦玉海,陈 杰,康小彤. 蓝牙嗅探方案的探讨[J]. 科技传播,2017,9(17):72-73.