文章编号：2096-1472(2021)-12-24-05
DOI:10.19644/j.cnki.issn2096-1472.2021.012.006

基于软件定义网络校园网络运维设计研究

刘 敏

(湄洲湾职业技术学院，福建 莆田 351119)
✉fengtilm@qq.com

摘 要：随着校园网网络应用的不断增长，网络中的流量监控、故障排查、风险预警等问题面临巨大挑战。在运用SDN技术对南向基础网络进行自动化部署，对北向构建校园网网络管理节点的基础上，利用gPRC(Google远程过程调用)、ERSPAN(封装远程端口镜像)技术设计了校园网络运维平台，对网络中的物理链路、TCP质量、业务进行分析，提高了校园网络的运维效率，对后继智能化的网络运维研究具有借鉴意义。

关键词：网络运维；软件定义网络；gRPC；ERSPAN
中图分类号：TP393 **文献标识码**：A

Research on Campus Network Operation and Maintenance Design based on Software Defined Network

LIU Min

(*Meizhouwan Vocational Technology College*, *Putian* 351119, *China*)
✉fengtilm@qq.com

Abstract: With the increasing campus network applications, network traffic monitoring, troubleshooting, risk warning and other issues are facing huge challenges. In this research, SDN (Software Defined Network) technology is used to deploy the basic network automation in the south, and network management node is constructed in the north. On this basis, this paper proposes to design a campus network operation and maintenance platform by using gPRC (Google Remote Procedure Call) and ERSPAN (Encapsulated Remote Port Mirroring) technology. Physical links, TCP (Transmission Control Protocol) quality, and business of the network are analyzed. This platform improves the efficiency of campus network operation and maintenance, and it has provided a reference for subsequent intelligent network operation and maintenance research.

Keywords: network operation and maintenance; software defined network; gRPC; ERSPAN

1 引言(Introduction)

随着云计算、人工智能、虚拟现实等各种技术在校园网中的应用，网络规模、数据流量快速增长。传统的网络运维方式越来越难以满足校园网络的应用需求[1]。

(1)网络越来越复杂化，采用传统运维模式带来的运维成本越来越高。由于校园网信息化程度不断深入，以及信息化业务不断上线，不同网络需求使得网络传统运维方式面临前所未有的挑战，难度越来越高。

(2)传统的运维系统大部分是故障驱动，缺少有效的干预手段及事前预测。在传统运维系统中，只能在网络出现故障后，采用人工登记报修、电话或口头等方式告知运维人员，运维人员在接到通知后，通过电话沟通、远程操作等方法查找故障原因，提出可能的解决方案，故障排除时间长、效率低。

(3)传统的运维系统是分钟级数据采集，无法实现实时、精准的数据采集。传统TCP/IP技术运维采用SNMP协议，从路由器、服务器、交换机等被管设备获取设备运行的数据，SNMP轮询的方式必须要在一定的间隔时间内不断地进行轮询，间隔时间太短增大了网络通信拥塞的风险，一般在分钟

基金项目：2019年度福建省中青年教师科研项目“基于SDN的网络运维管理研究与应用”(高校教育信息化专项)(JAT191930).

级的时间内采集和统计数据，同时MIB II中大量的变量是只读变量，可写变量太少。

(4)传统的运维系统重点在于网络监控，缺乏网络关联分析。网络监控工具将校园网整张网的布局和设备在网络监平台中呈现出来，图形化显示当前网络的连通性和整张网的网络设备可达情况，无法得到网络设备网络质量的详细信息。

针对校园网中所面临的运维现状，基于SDN网络架构，采用ERSPAN对流量进行实时采集，并进行流量分析，通过推模式主动把设备数据信息上送采集器，从而实现比传统SNMP查询方式更实时、更高效的数据采集性能。

2　相关工作(Related work)

2.1　SDN(软件定义网络)

SDN技术得到了很多开源组织、创业厂商、设备制造商和运营商的认可和推崇，SDN让网络运作简化的思想是当今众多的网络平台所共同认可的。其核心思想是通过标准化技术实现控制平面与转发平面分离从而简化网络管理，采用高性能API Gateway提供符合RESTful标准的北向API，向应用层开放使网络的转发功能具有可编程性，南向API支持NetConf、OpenFlow、BGP-LS、PCEP、SNMP等接口标准，实现对网络流量灵活化、集中化、细粒度的控制，从而为网络的集中管理和应用创新提供了良好的平台[2-4]。

2.2　gRPC、ERSPAN

gRPC(Google Remote Procedure Call，Google远程过程调用)[5]是由Google发布的基于HTTP 2.0传输层协议承载的高性能开源软件框架，目标是让远程服务调用更加简单、透明。RPC框架负责屏蔽底层的传输方式(TCP或者UDP)、序列化方式(XML/JSON/二进制)和通信细节，遵从server/client模型，客户端可以像调用本地函数一样调用server端提供的接口；提供了支持多种编程语言的、对网络设备进行配置和管理的方法，通信双方可以基于该软件框架进行二次开发。

ERSPAN(Encapsulated Remote Switch Port Analyzer，封装远程端口镜像)[6]是一种三层远程端口镜像技术，通过复制指定端口、VLAN或CPU的报文，并通过GRE隧道将复制的报文发送到远程数据监测设备，使用户可以利用数据监测设备分析这些报文(称为镜像报文)，以进行网络监控和故障排除。

3　校园网络运维平台研究与设计(Research and design of campus network operation and maintenance platform)

3.1　运维平台系统架构

如图1所示，整个系统分为：(1)向北开放的API，为运维应用以及其他上层应用提供分析能力；(2)数据分析平台，采用Spark、Flink等分布式计算引擎以及AI人工智能模型库完成数据在线/离线分析任务；(3)基于大数据的数据采集器、分布式部署架构实现数据采集能力的横向扩展，以满足不同网络规模的数据采集需求；(4)通过SDN控制器内的NETCONF等方式向设备下发配置，实现对网络设备的管理，同时控制器可以根据分析器提供的分析数据，为网络设备下发配置，对网络设备的转发行为进行调整，也可以控制网络设备有选择地对数据进行采样和上报。

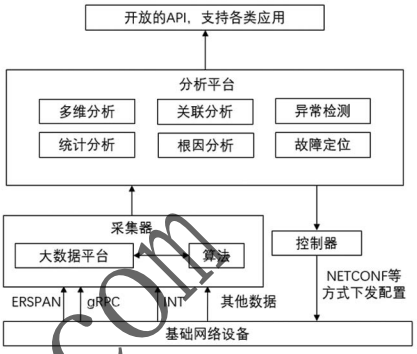

图1 校园网络的运维系统架构

Fig.1 Campus network operation and maintenance system architecture

3.2　基于EVPN(以太网虚拟专用网络)的SDN校园网络运行机制

利用EVPN技术实现SDN在校园网络中的数据控制平面和数据转发平面分离[7]。数据控制与转发分离机制新增五种BGP EVPN消息类型EVPN NLRI(Network Layer Reachability Information，网络层可达性信息)：Ethernet Auto-discovery Route(RT-1)、MAC/IP Advertisement Route(RT-2)、Inclusive Multicast Ethernet Tag Route(RT-3)、Ethernet Segment Route(RT-4)、IP Prefix Advertisement Route(RT-5)。在数据控制面引入RR(路由反射器)，核心设备与分支设备协商ibgp evpn邻居，所有的分支设备都只和RR建立BGP对等体关系，RR发现并接收分支设备发起的RT-2或者RT-3的路由通告，连接后形成Client列表，分支设备将收到的路由信息反射给其他所有的分支设备，实现控制面的路由转发。在数据转发面，依靠RT-3建立BUM广播表，每个分支设备都通告自己的VNI(虚拟网络实例)信息，这样，每个分支设备都有全网的VXLAN信息以及VXLAN和下一跳的关系。分支设备会和那些跟自己有相同VXLAN的下一跳自动建立VXLAN隧道，并将此VXLAN隧道跟这些相同的VXLAN关联，对每个VXLAN而言，所有这些建立并关联的VXLAN隧道就构成了BUM广播，形成了二层广播域隧道，实现数据转发[8]。

3.3　校园运维系统数据采集机制

基础网络数据采集机制如图2所示。

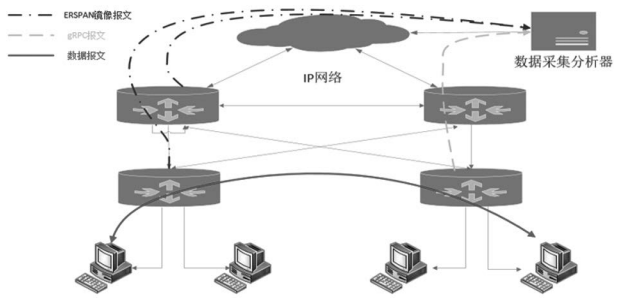

图2 基础网络数据采集机制

Fig.2 Basic network data collection mechanism

gRPC是一次订阅，多次推送，采集设备管理、接口管理、IP转发、LLDP、系统日志等业务数据，采集器与设备之间的数据链路采用TCP协议，使用TLS协议对通道加密和进行双向证书认证，进行安全通信。采集器与设备进行安全通信后，应用HTTP 2.0协议使设备指定服务端口等待采集器发起的连接请求，采集器执行相关程序登录设备并调用proto文件提供的gRPC方法向设备下发配置和发送订阅需要采集的接口流量统计、CPU、告警等数据信息的请求消息，设备以Protocol Buffer编码等形式回复应答消息。

ERSPAN是对原始基于字节流的传输层流量报文进行镜像，可以对TCP报文转发路径上的下发流匹配规则，将TCP报文镜像到采集器，实现对应用流的流量统计、路径还原、延时计算、应用识别等分析处理。

4 基于SDN校园网络运维的实现(Implementation of campus network operation and maintenance based on SDN)

4.1 gRPC远程监控

gRPC采用客户端/服务器模型，使用HTTP 2.0协议传输报文，实现设备自动读取各种统计信息(CPU、内存、接口等)，根据采集器的订阅要求将采集的信息通过gRPC协议上报给采集器，实现更加实时、高效的数据采集功能。gRPC数据采集如图3所示。

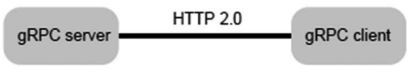

图3 gRPC数据采集

Fig.3 gRPC data collection

gRPC的工作机制：(1)服务器通过监听指定服务端口来等待客户端的连接请求。(2)用户通过执行客户端程序登录服务器。(3)客户端调用proto文件提供的gRPC方法发送请求消息。(4)服务器回复应答消息。

设备数据采集模式：设备作为gRPC服务器，采集器作为gRPC客户端模式。

(1)公共proto文件。公共RPC方法，其内容和含义如下：

```
syntax = " proto2 " ;
package grpc_service;
message GetJsonReply { //Get方法应答结果
required string result = 1;
}
message SubscribeReply { //订阅结果
required string result = 1;
}
message ConfigReply { //配置结果
required string result = 1;
}
message ReportEvent { //订阅事件结果定义
required string token_id = 1; // token_id
required string stream_name = 2; //订阅的事件流名称
required string event_name = 3; //订阅的事件名
required string json_text = 4; //订阅结果json字符串
}
message GetReportRequest{ //获取事件订阅结果请求
required string token_id = 1; //成功后的token_id
}
message SubscribeRequest { //定义事件流名称
required string stream_name = 1;
}
service GrpcService { //定义gRPC方法
rpc SubscribeByStreamName (SubscribeRequest) returns (SubscribeReply) {} //订阅事件流
rpc GetEventReport (GetReportRequest) returns (stream ReportEvent) {} //获取事件结果
}
```

(2)业务模块proto文件。支持Device、Ifmgr、IPFW、LLDP、Syslog等多个业务模块的proto文件，描述具体的业务数据格式。Device模块数据的RPC方法，其内容和含义如下：

```
syntax = " proto2 " ;
import " grpc_service.proto " ;
package device;
message DeviceBase { //获取设备基本信息结构定义
optional string HostName = 1; //设备的名称
```

```
optional string HostOid = 2；//sysoid
optional uint32 MaxChassisNum = 3；//最大框数
optional uint32 MaxSlotNum = 4；//最大slot数
optional string HostDescription = 5；//设备描述信息
}
message DevicePhysicalEntities { //设备物理实体信息
message Entity {
optional uint32 PhysicalIndex = 1；//实体索引
optional string VendorType = 2；//vendor类型
optional uint32 EntityClass = 3；//实体类型
optional string SoftwareRev = 4；//软件版本
optional string SerialNumber = 5；//序列号
optional string Model = 6；//模式
}
repeated Entity entity = 1；
}
service DeviceService { //定义的RPC方法
rpc GetJsonDeviceBase(DeviceBase) returns (grpc_service.GetJsonReply) {} //获取设备基本信息
rpc GetJsonDevicePhysicalEntities(DevicePhysicalEntities) returns
(grpc_service.GetJsonReply) {}
} //获取设备实体信息
```

4.2 ERSPAN流分析

(1)将镜像报文封装为ERSPAN Type II的GRE报文。GRE报文如图4所示。

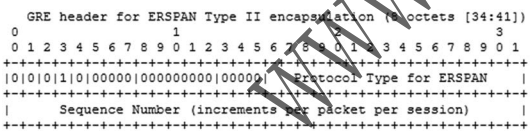

图4 ERSPAN的GRE报文

Fig.4 GRE message of ERSPAN

(2)TCP会话传输的数据流大小：

①请求方向流量：请求方向的FIN-ACK序列号和SYN序列号。

②应答方向流量：应答方向的FIN-ACK序列号和SYN-ACK序列号。

(3)TCP报文在网络设备中进行三层转发时，按照IP首部的TTL字段会逐跳递减原理，先内层匹配内容，然后排序内外层报文的TTL，再匹配识别完成路径还原；由采集器对每份数据流打时间戳，并根据时间戳信息计算TCP在设备间的逐跳传输延时；对TCP内层报文的五元组信息，以及应用层的主机号和端口信息进行应用识别。

5 实验结果与分析(Experimental results and analysis)

5.1 gRPC配置

(1)配置Device(gRPC服务器)

开启gRPC功能。

<Device>system-view

[Device]grpc enable

创建本地用户test，配置该用户的密码，授权用户角色为network-admin，可以使用的服务类型为HTTPS服务。

[Device]local-user test

[Device-luser-manage-test]password simple 123456TESTplat&!

[Device-luser-manage-test]authorization-attribute user-role network-admin

[Device-luser-manage-test]service-type https

[Device-luser-manage-test]quit

(2)配置gRPC客户端

①在gRPC客户端安装gRPC环境。

②获取.proto文件(该文件中已写入订阅LLDP事件的配置)，并通过protocol buffers编译器生成特定语言(例如Java、Python、C/C++、Go)的执行代码。

③编写客户端程序，调用上一步生成的代码。

④执行客户端程序，登录gRPC服务器。

5.2 ERSPAN配置

(1)配置 Device A

配置OSPF协议。

[DeviceA] ospf 1

[DeviceA-ospf-1] area 0

[DeviceA-ospf-1-area-0.0.0.0] network 10.1.1.0 0.0.0.255

[DeviceA-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255

创建本地镜像组1。

[DeviceA] mirroring-group 1 local

配置本地镜像组1的源端口为GigabitEthernet1/0/1，目的端口为GigabitEthernet1/0/2，镜像报文的目的IP地址为40.1.1.2，源IP地址为20.1.1.1。

[DeviceA] mirroring-group 1 mirroring-port gigabitethernet 1/0/1 both

[DeviceA] mirroring-group 1 monitor-port gigabitethernet 1/0/2 destination-ip 40.1.1.2 source-ip 20.1.1.1

(2)配置Device B

配置OSPF协议。

[DeviceB] ospf 1

[DeviceB-ospf-1] area 0

[DeviceB-ospf-1-area-0.0.0.0] network 20.1.1.0 0.0.0.255

(3)验证配置

显示Device A上所有镜像组的配置信息。

[DeviceA] display mirroring-group all

Mirroring group 1:

Type: Local

Status: Active

Mirroring port:

GigabitEthernet1/0/1 Both

Monitor port: GigabitEthernet1/0/2

Encapsulation: Destination IP address 40.1.1.2

Source IP address 20.1.1.1

Destination MAC address 000f-e241-5e5b

5.3 分析

gRPC采集数据包括网络设备的实时资源信息、RDMA统计信息、RDMA告警信息等，如表1所示。

表1 gRPC采集的相关数据信息

Tab.1 Relevant data information collected by gRPC

数据大类	数据维度	数据项	备注
实时资源信息	整机	CPU占用率、内存占用率	采集频率1 分钟级
	接口	收/发包数、收/发广播包数、收/发组播包数、收/发单播包数、收/发字节数 收/发丢包数、收/发错包数	采集频率1 分钟级
RDMA统计信息	状态信息	ingress/egress丢包总量 ingress/egress buffer统计 headroom buffer统计	(1)每个端口、每个队列 (2)采集频率1 秒级
RDMA告警信息	故障事件	ingress丢包 egress丢包 headroom buffer超限 egress buffer超限	采集频率1 秒级

ERSPAN技术采集网络TCP特征报文，上传数据采集分析器。分析器通过TCP流分析技术，实现如下功能分析：(1)分析沿途交换机上报的TCP镜像报文可获得应用流量转发路径；分析采集TCP报文时间戳可获得应用建立TCP连接时延及沿途交换机转发时延，定位应用体验差是因为网络慢还是应用本身的问题；分析TCP报文头可获取应用TCP连接持续时间及流量大小。(2)根据TCP流生命周期的交互协议报文，结合大数据分析算法，实现TCP连接异常检测，如TCP连接异常、TTL会话异常。ERSPAN采集到的部分数据分析如图5所示。

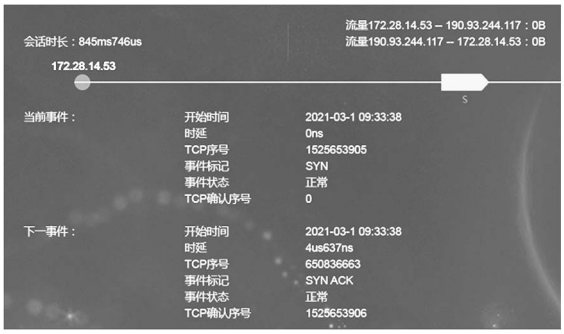

图5 ERSPAN采集到的部分数据分析

Fig.5 Part of the data collected by ERSPAN are analyzed

6 结论(Conclusion)

SDN可以通过控制器下发配置使得网络运维更为方便。本文致力于通过gRPC、ERSPAN技术持续采集设备数据、日志数据、流量数据、拓扑数据等，通过对数据的统计分析，实时洞察整网状态，结合SDN控制器的网络运行策略，得出网络运行过程中产生的问题，快速定位网络故障位置，方便网络运维。本文的设计研究也存在一些不足之处：并未结合人工智能、大数据技术进行研究，通过模型，利用历史数据训练，预防网络故障的发生；也未对通过网络发现的问题自动修改SDN控制器的网络配置策略，自动解决网络问题进行研究。

参考文献(References)

[1] 王关祥.高校网络运行管理与安全维护研究[J].网络安全技术与应用,2019(10):92-93.

[2] MCKEOWN N, ANDERSON T, BALARISHNAN H, et al. Openflow: Enabling innovation in campus networks[J]. ACMSIGCOMM Computer Communication Review, 2008, 38(2):69-74.

[3] 张少军,兰巨龙,胡宇翔,等.软件定义网络控制平面可扩展性研究进展[J].软件学报,2018,29(01):160-175.

[4] 左青云,陈鸣,赵广松,等.基于OpenFlow的SDN技术研究[J].软件学报,2013,24(5):1078-1097.

[5] 张凤军,罗广军,邱帆,等.基于SDN的分组传送网架构设计及实现[J].中国电子科学研究院学报,2020,15(07):665-671.

[6] 潘竹虹,许卓斌.信息采集网络支撑系统的设计与实现[J].厦门大学学报(自然科学版),2016,55(03):426-433.

[7] 赵俊,包丛笑,李星.基于OpenFlow协议的覆盖网络路由器设计[J].清华大学学报(自然科学版),2018,58(02):164-169.

[8] ZHAO Z F, HONG F, LI R P. SDN based VxLAN optimization in cloud computing networks[J]. IEEE Access, 2017(5):23312-23319.

作者简介：

刘 敏(1977-)，男，硕士，讲师.研究领域：网络技术，大数据技术.