



基于 SDN 的网络运维系统设计与开发

吴舜¹, 张辉¹, 邢宁哲¹, 宋伟¹, 黄天琳², 唐亚哲²

(1. 国网冀北电力有限公司信息通信分公司, 北京 100053; 2. 西安交通大学, 陕西 西安 710049)

摘要: 电力系统计算机网络运维管理存在功能弱、粒度粗及业务支撑能力不够等问题。试图以 SDN 技术解决上述问题, 提出了 SDN 网络运维管理框架, 构建了跨域的 SDN, 研发了运维管理系统, 部署了拓扑发现、故障检测与切换等典型运维功能。测试表明, 该系统克服了传统网络运维管理系统的缺点, 达到了设计目标。

关键词: SDN; 网络运维管理系统; 拓扑发现; 故障检测与切换

中图分类号: TN92

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2016077

Design and development of the network OA&M system based on SDN

WU Shun¹, ZHANG Hui¹, XING Ningzhe¹, SONG Wei¹, HUANG Tianlin², TANG Yazhe²

1. State Grid Jibei Information & Telecommunication Company, Beijing 100053, China

2. Xi'an Jiaotong University, Xi'an 710049, China

Abstract: The OA&M systems of network infrastructure in electric power companies have drawbacks such as weak functions, coarse-grained monitor and control on the underlying networks and bad support on service deployment. SDN technology was used to solve these problems. An SDN-based OA&M framework was presented, a cross-domain SDN network was built and the corresponding OA&M system was developed, which could perform functions like topology discovery and fault detecting along with backup components switching. The experiments results prove that the OA&M system can overcome the above drawbacks and achieve the design goal.

Key words: SDN, network OA&M system, topology discovery, fault detecting and switching

1 引言

电力系统计算机网络的运维管理系统属于电力 IT 系统的重要组成部分, 在保障电力系统的正常高效运行中起着重要的支撑作用。当前, 电力系统计算机网络大部分还是基于 TCP/IP^[1]网络技术, 其运维和管理也主要是基于传统网络管理, 存在管理功能偏弱、管理粒度粗和业务支撑能力有限等问题。

新型 SDN^[4-6]网络技术提出了控制层面和数据层面相分离的思想, 将网络的控制集中到控制器上, 可以实现全网路由、配置的集中优化。同时, 交换机端也可以针对全部网络协议层次进行细粒度流表配置和转发计数, 使得 SDN 下控制器对网络业务的配置部署和监控大大增强。这些特点都为解决传统网络管理运维系统的缺点提供了新的思路。

本文提出了 SDN 网络管理运维的框架, 并结合国网



SDN 试点项目,研发部署了跨域的 SDN,在此基础上开发了新型 SDN 网络运维管理系统,实现了简单高效的网络拓扑发现、网络链路故障检测和快速切换、服务器故障检测和切换以及特定业务网络带宽保证的 QoS。并结合视频点播业务,对所开发系统进行了测试。测试表明,SDN 网络运维管理系统具有细粒度、管理功能强大和能够有效支撑业务部署的优点。

2 电力网络运维系统现状

当前电力网络基于传统 TCP/IP^[1]网络技术,其运维和管理的主要方法是通过传统网络管理机制(例如简单网络管理协议(simple network management protocol,SNMP)^[2]),由管理者从被管设备(例如交换机、路由器、服务器等)中获取设备运行数据,进行相关的数据分析后呈现给网络管理员,再由网络管理员实施网管操作。从网络管理的角度看,当前电力网络系统运维存在两个不足:网络管理功能偏弱,存在对网管数据的分析处理能力不足以及不能区分不同的流和应用并进行细粒度的问题;网管系统对网络的配置能力不足,因为 MIB II 中大量的变量是只读变量,只有少数变量是可写变量,通过 SNMP 对网络设备的配置能力有限。因此,网管系统更多地表现为一个网络的监视系统,而不是“控制”系统。这样,网络业务部署等需要对网络设备进行大量繁琐的配置工作,加大了实施难度。

近年来快速发展的 SDN 技术为网络管理提供了新的解决方案,也为电力网络运维提出了新思路。SDN 采用集中式管理机制,通过配置流表实施业务部署,并且在全部协议层次上进行流的区分和计数的能力,有助于解决传统网络管理运维系统的各种缺陷。

3 SDN 网络运维系统框架

传统网络管理系统存在的主要问题是监控粒度太粗和对交换机和路由器的配置能力太弱,不能实施各种网络业务的部署。从监控粒度来说,SDN 交换机可以在全部协议层次上进行流的区分和计数,理论上说,就有进行每流计数和监控的能力。网管系统也就具备每流区分管理的能力。而传统网管对交换设备配置能力偏弱的问题,在 SDN 下得到了彻底的解决。因为 SDN 控制器实际上拥有全网所有交换设备的流表项配置能力,不仅能完成传统网管系统做不到的路由表的配置,还可以通过路由表(流表)中流表项的配置来实施各种网络业务的配置和部署。

本文提出了基于 SDN 的网络运维管理系统的框架,该框架主要由 3 部分组成:图形用户接口(graphic user interface,GUI)部分、控制器部分以及控制器和被管 SDN 的交互部分。其中,GUI 部分是用户和运维系统的人机界面部分,用户通过操控 GUI 来启动对网络的配置、管理和运维;控制器部分是系统的核心部分,真正的控制逻辑是在控制器端实现的。从系统动态执行流程来看,用户通过 GUI 启动运维功能,该操作通过 RESTful^[7]接口传递到控制器,控制器根据用户配置的参数,运行真正的控制逻辑,形成 SDN 中各个相关交换机的流表项,并通过 OpenFlow 协议下发。同时,运维系统通过 OpenFlow 协议从交换机中获取交换机的运行状态信息,并通过 RESTful 接口传递到前台 GUI 显示给网络管理员。

研发了一个 SDN 网络运维管理系统,具体的功能和交互方式如图 1 所示。图 1 中,左边部分是控制器部分,主要的控制逻辑在控制器内建应用中实现,内建应用通过

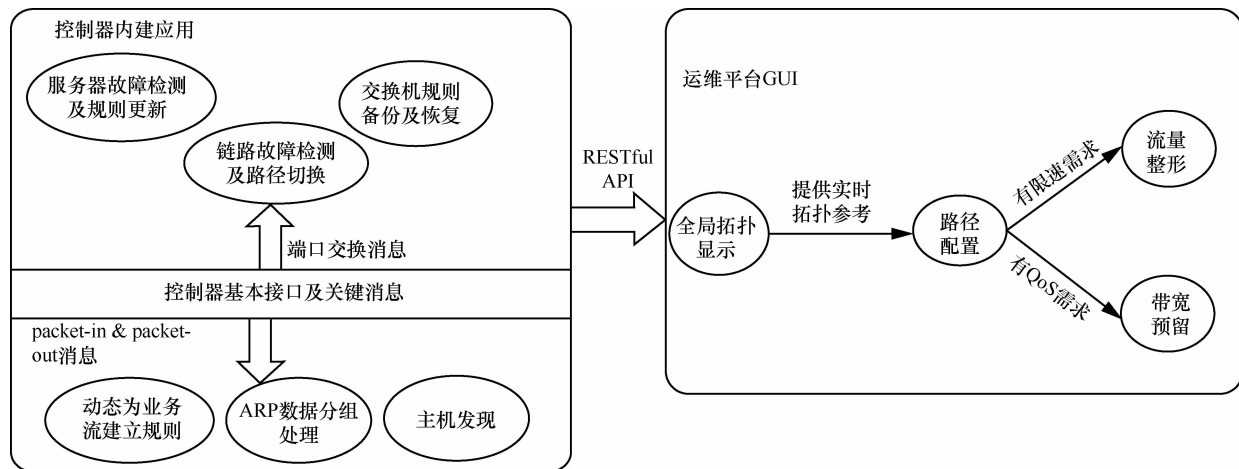


图 1 SDN 网络运维管理系统框架、功能和交互方式

OpenFlow 协议和相关的交换设备通信配置这些设备的流表,通过 RESTful 接口与前台 GUI 通信,获取前台的用户操作信息,并且把从内建应用获取到的交换设备的状态信息显示在前台 GUI 上。

4 SDN 网络运维系统功能

试点项目的 SDN 运维管理平台中,确定了几个经典的网络运维管理功能,包括网络拓扑显示功能、服务器故障检测及切换功能、链路故障检测及路径切换功能以及 QoS 保证等功能,每个功能的具体内容如下所示。

网络拓扑发现及显示功能:对于网络运维管理系统来说,网络拓扑发现及显示是一个非常重要和基本的功能。传统网络中,由于各个交换机的标准不一,不少企业还在使用不同的网络管理系统管理来自于不同厂商的交换机,因为只有这样,拓扑发现功能才能正常工作。而在 SDN 中,由于交换机的标准化,网络拓扑发现却有非常简单的实现方式,即通过 LLDP^[9] (link layer discovery protocol)消息、packet-out 和 packet-in 消息的协作使控制器得到所有交换机的邻居关系,进而构造出整个网络的拓扑。本文中 will 使用这种方式进行网络拓扑发现。

服务器故障动态处理功能:控制器能够自动监听各个服务器与交换机的连接状态,一旦正在工作的服务器出现故障,便将业务流导到健康的服务器,保障客户的服务不受影响。如图 2 所示,一旦服务器因为关机或网线松落等原因离开网络,那么控制器后台应用会接收到 OpenFlow 协议中的端口状态变化消息(port status message)。通过对该消息解析可以定位到故障服务器。即可更新该服务器的健康状态,并且对旧规则进行删除,重新构造包含新服务器 MAC 地址的 ARP 回复给客户端,为客户端和新的服务器之间建立一条最短路径的连接。

链路状态监测和切换功能:控制器能够监听网络中各个链路的连接状态,一旦某条链路断开连接,则将此路径上的数据流切换到另外一条冗余路径,保障客户的请求不受干扰。如图 3 所示,控制器根据维护的全局拓扑,可计算出点对之间的所有路径。并且根据实时拓扑更新路径健康状态。当收到端口改变消息,定位到故障路径,控制器扫描点对之间的所有路径,将所有包含该故障路径的路径健康状态设为 false。并且为受到影响的当前工作路径,重新选择一条健康的最短路径,动态更新规则。

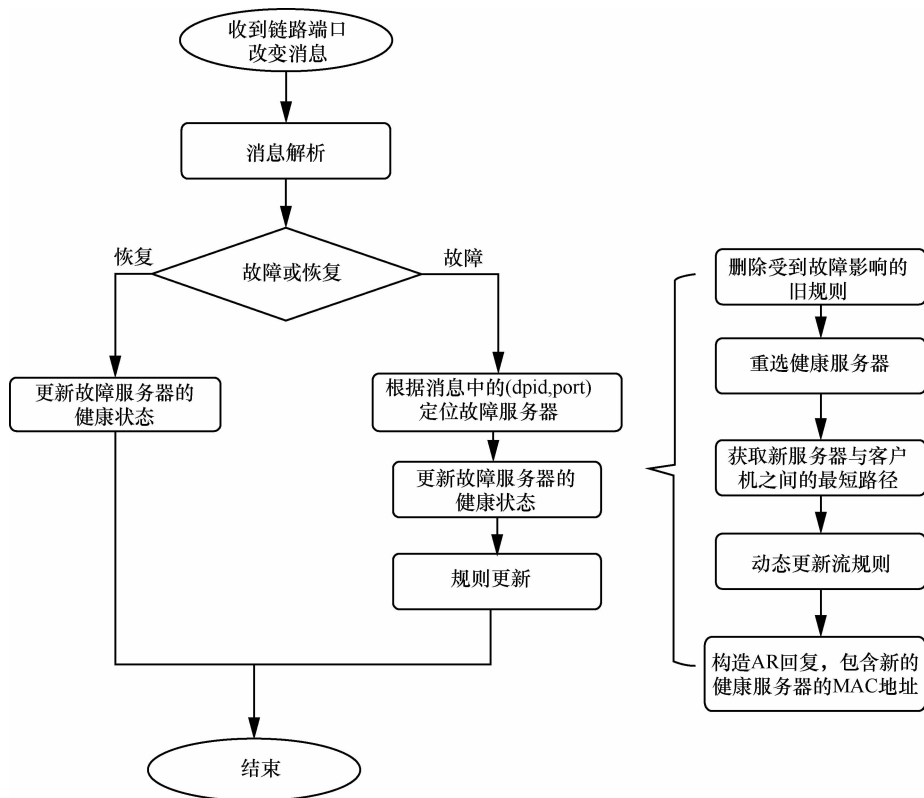


图 2 服务器故障处理流程

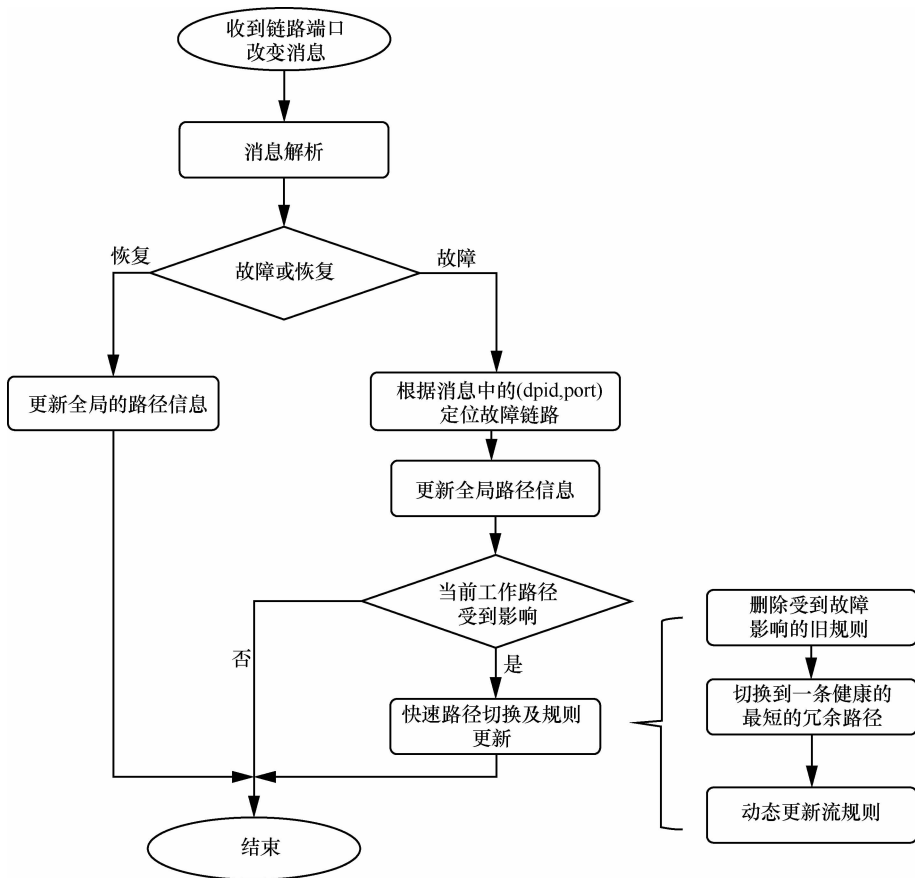


图3 链路故障处理流程

QoS 保证功能：由于 OpenFlow 协议提供队列管理的信息接口，因此可对交换机的队列进行配置（如 open vSwitch 的队列），设置其最大速率及最小速率，最小速率即可实现带宽保障。并且可设置流表将一条流与对应的队列关联，如 HTTP 流保障其带宽为 10 kbit/s，那么可以先配置某个队列，将其最小速率设为 10 kbit/s，再配置流表的匹配域为 tcp_dst_port=80，action 为将该流转发至相应队列，即可完成流表到队列的映射。具体流程如图 4 所示。

5 系统研发和测试

本文研发实现了上述的所有功能，并在国网某 2 个分公司进行了跨域的 SDN 部署。部署拓扑如图 5 所示。数据中心-1 部署在其中一个分公司，数据中心-2 部署在另外一个分公司。整个系统中部署一个 SDN 控制器（Ryu 控制器）在数据中心-1。网络中存在多条冗余路径，可用作链路故障快速切换。并且有两个视频服务器，数据中心-1 的视频服务器 1 是主服务器，只有在其出现故障时，才会自动切换到数据中心-2 的备用的视频服务器 2 用作测试服务

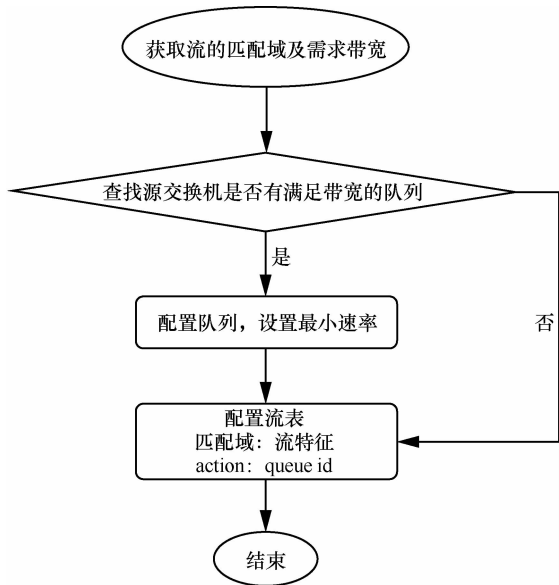


图4 QoS 保证功能

器故障处理。背景流量发生器能够产生流量造成网络拥塞，则可以测试在拥塞时，用户对视频流进行 QoS 配置，能否成功保障带宽。

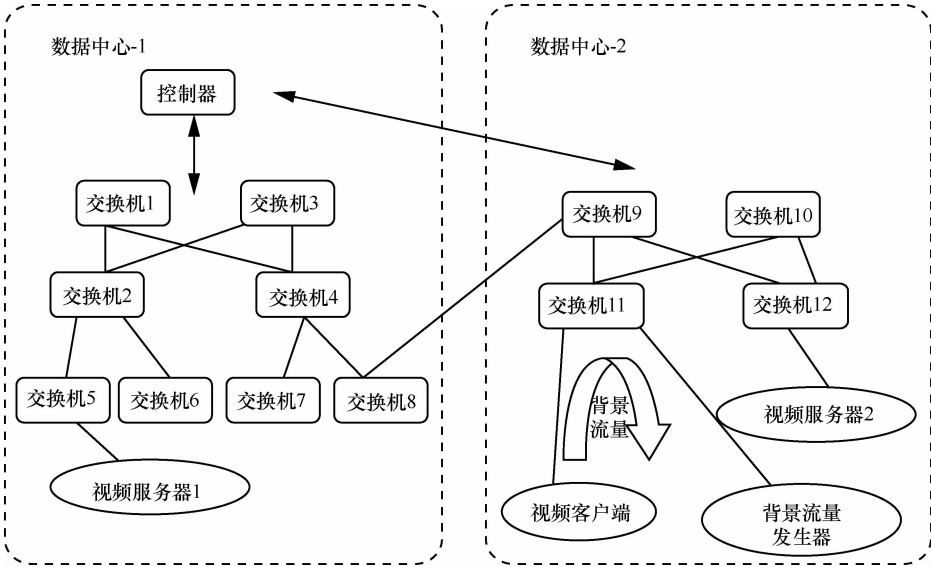


图 5 SDN 物理拓扑

当全局拓扑搭建好之后,控制器通过循环发送、接受交换机的 LLDP 分组,通过 LLDP 构建全局拓扑,并且学习从各个终端发来的数据分组,进行主机发现的过程。在较短的收敛时间内,运维平台 GUI 便能够显示到全网的全局拓扑,如图 6 所示。

从图 6 可以看到,网络中存在备用的服务器二(位于最右边,编号为 6),当服务器发生故障离开网络时,控制器会监听到端口状态改变事件,解析事件发来的消息便能够定位到故障的服务器,将其从终端集合中移除、

将流切换到另一个健康的服务器,并且进行流表规则的更新。

在服务器一上运行:ifconfig eth0 down 或者拔掉网线、关机等操作,此时可以看到,控制器对流表规则进行了更新,建立了新的双向流用于客户端与备用服务器的交互。

从图 7 可以看到:编号为 8 的主服务器一从页面消失,表示终端的维护也是实时更新的;当前的工作路径已从原来视频客户端—视频服务器 1 切换为了视频客户

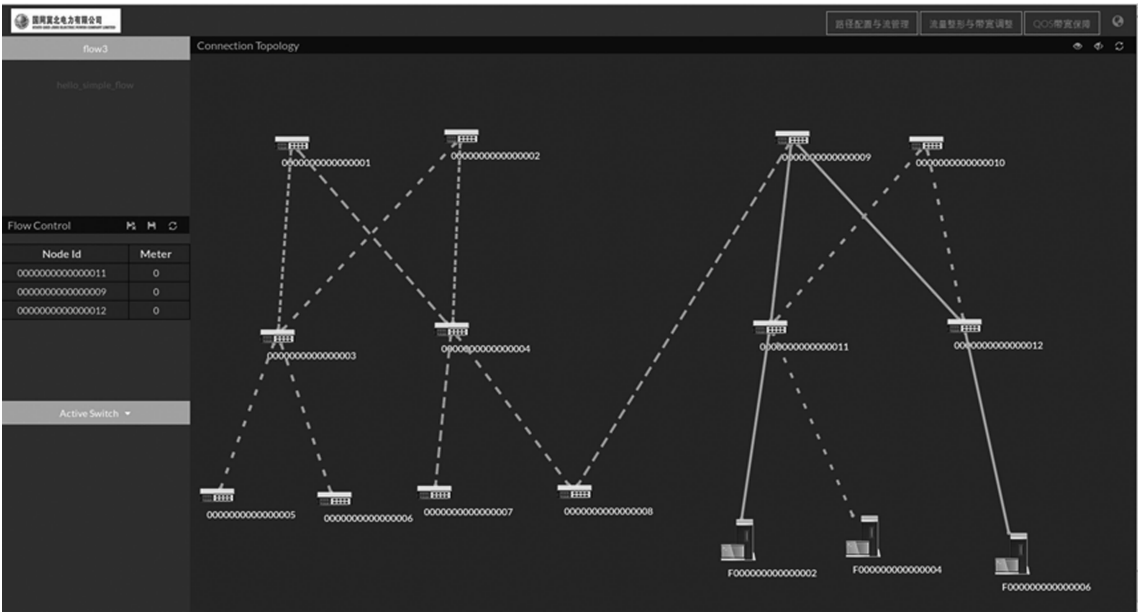


图 6 全局拓扑 GUI 显示

端一视频服务器 2; 程序动态对规则进行了更新, 重新挑选了健康服务器提供服务, 并且在该服务器与客户端之间建立了一条最短路径: 11-9-12, 客户端视频正常播放, 切换过程对其是透明的。

从图 6 可以看到,本拓扑连接在终端之间都存在冗余链路可以进行切换。

如图 8 所示, 在视频服务器 2 提供服务的情况下, 路由设置为两个终端之间的最短路径之一: 11-9-12, 此时将

9 号交换机与 11 号交换机之间的网线拔掉, 后台程序监听到 9、11 两个交换机发出的端口改变消息, 定位到两者之间的链路断开。更新全路径表, 选择另外一条健康的、最短路径提供服务, 对比图 8、图 9 可以看到: “绿色路径”已经发生改变, 改由 11-10-12 号交换机提供服务。并且 9-11 号交换机之间的连接已经消失, 表明 GUI 全局拓扑的显示是实时进行的。

QoS 保证功能目前主要是通过配置优先级队列的最

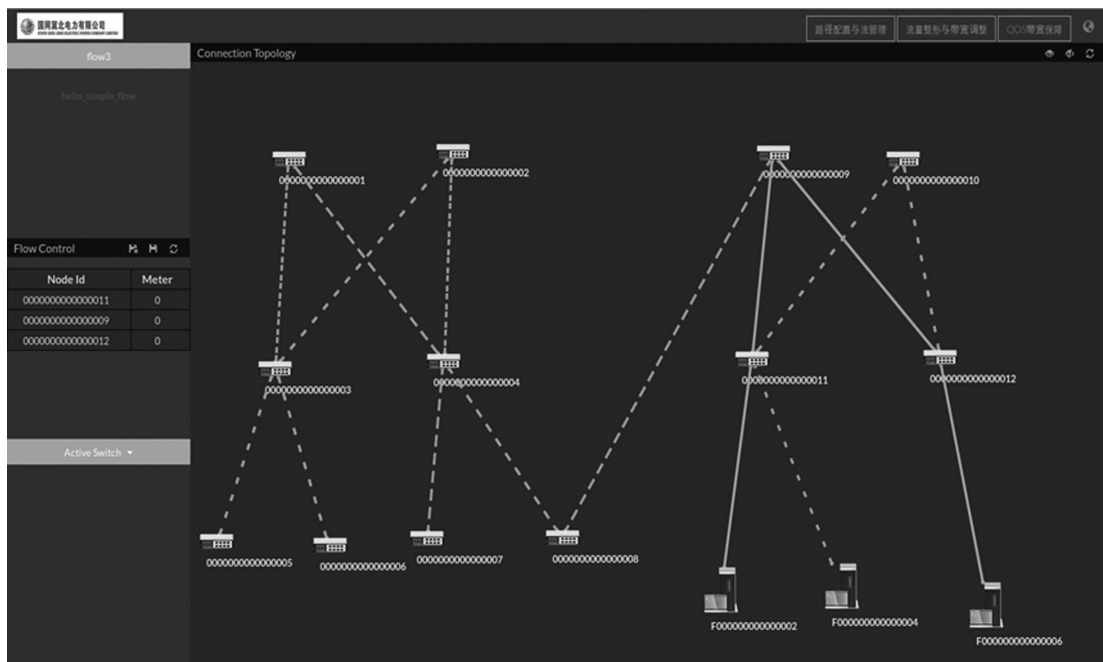


图 7 服务器故障处理—视频服务器 1 出现故障

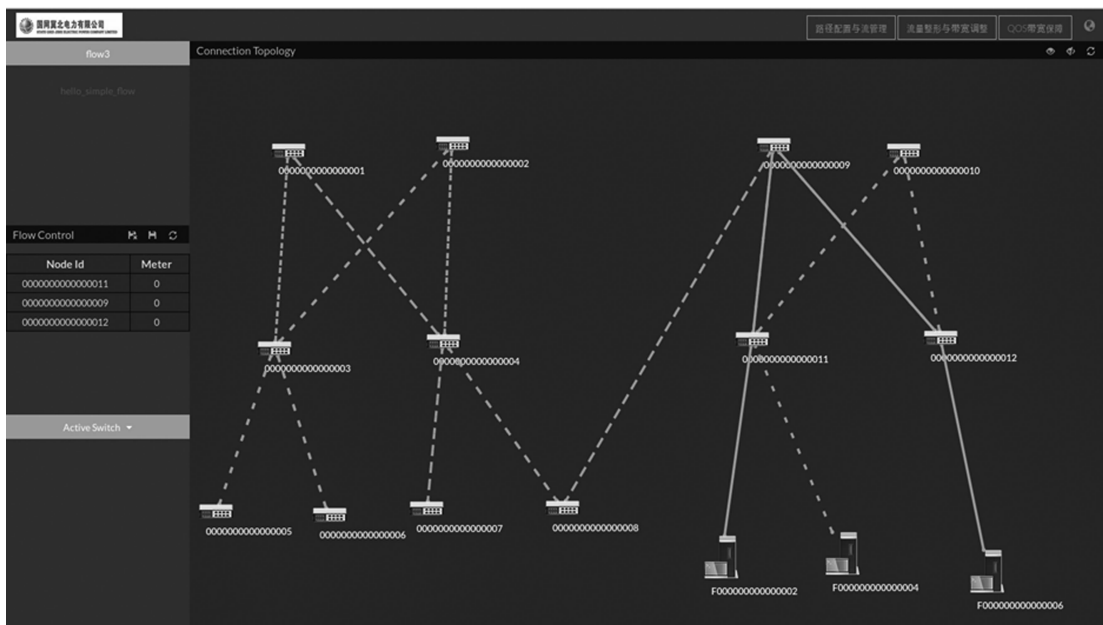


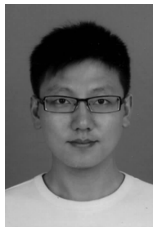
图 8 服务器 2 提供服务



[作者简介]



吴舜(1983-),男,国网冀北电力有限公司信息通信分公司工程师、高级技师,主要研究方向为电力企业信息系统运检技术、用户体验监测技术、软件定义网络技术。



宋伟(1983-),男,国网冀北电力有限公司信息通信分公司工程师、中级技师,主要研究方向为电力企业信息通信系统工程建设、计算机网络安全技术及项目高级管理。



张辉(1979-),男,国网冀北电力有限公司信息通信分公司主任,主要从事电力企业通信专业技术管理工作。



黄天琳(1991-),女,西安交通大学硕士生,主要从事网络测量、软件定义网络、计算机网络相关研发工作。



邢宁哲(1978-),男,博士,国网冀北电力有限公司信息通信分公司副总工程师,主要从事电力企业通信专业技术管理工作。



唐亚哲(1970-),男,博士,西安交通大学副教授、博士生导师,主要研究方向为计算机网络、网络管理和网络安全。