DOI：10. 16516/j. gedi. issn2095-8676. 2018. S1. 033

基于路由侦听监测的数据网监视及仿真系统设计

衷宇清[1]，陈昌娜[1]，王雅娟[2]，晏平[3]
（1. 南方电网公司广州供电局通信中心，广州 510200；
2. 中国能源建设集团广东省电力设计研究院有限公司，广州 510663；3. 云南诺寻科科技有限公司，昆明 650000）

摘要：[**目的**]为了直观实时的掌握数据网运行情况，提高数据网运维的效率。[**方法**]探讨了一种路由侦听监测方式，通过采集 OSPF、BGP 等协议信息，呈现与路由器“看”到的完全一样的实时全网地图，从而可及时发现三层路由的运行情况和异常信息。[**结果**]基于该路由侦听监测方式，设计了一种数据网监视及仿真系统，包括系统总体架构和应用场景等。[**结论**]该系统可辅助网管人员发现和处理故障，回放历史路由事件，并可在不影响现网的前提下用于网络割接等工作的测试和论证。

关键词：数据网仿真；网络侦听监测；OSPF
中图分类号：TN919. 5　　**文献标志码**：A　　**文章编号**：2095-8676(2018)S1-0183-06

A Model of Data Network Monitoring and Simulation System Based on Route Interception Monitoring

ZHONG Yuqing[1], CHEN Changna[1], WANG Yajuan[2], YAN Ping[3]
(1. Communication Center of Guangzhou Power Grid Co. Ltd., Guangzhou 510200, China;
2. China Energy Engineering Group Guangdong Electric Power Design Institute Co., Ltd., Guangzhou 510663, China;
3. Nuoxunke Science & Technology Co., Ltd., Kunming 650000, China)

Abstract: [**Introduction**] In order to grasp the condition of data network intuitively and real-time, and improve the efficiency of data network operation and maintenance. [**Method**] This paper proposed a method of routing detection. By collecting the protocol information such as OSPF and BGP, it could present the exactly the same real time whole network map as the router "see", so that the link fault and the third layer routing abnormality could be detected in time. [**Result**] Based on the routing detection method, this paper proposed a model of data network monitoring and simulation system, including system architecture and data flow, etc. [**Conclusion**] The system can assist network management personnel to detect and deal with fault, record historical routing events for analysis, and test network cutting program without affecting the in-use network.

Key words: data network simulation; network interception monitoring; OSPF

在数据网综合监视方面，当前数据网网管主要基于 SNMP 网管协议和 XFLOW 统计信息进行网络监视，而该方式的不足是对路由协议一无所知，不能发现路由环路、路由震荡、数据包来去路径不一致等三层路由的问题。

在数据网仿真方面，随着数据网的结构和规模越来越复杂以及网络应用的多样化，单纯地依靠纯理论和经验来进行网络运行状态的预判、引导网络割接工作已经不能适应高水平的网络运维的发展，迫切需要一套数据网仿真系统在故障、割接等各类场景下为运维工作提供依据和参考。

为解决以上问题，本文提出了一种基于路由侦听监测的数据网监视及仿真系统。该系统可辅助网管人员发现和处理故障，回放历史路由事件，并在不影响现网的前提下用于网络割接等工作的测试和论证。

1　现有数据网状态采集方式

当前数据网中采用的网络状态采集方式主要有指令采集方式、探针监测方式两种。

收稿日期：2018-08-29　　**修回日期**：2018-12-05
基金项目：广州供电局科技项目“电力系统数据网的路由综合监测、仿真操作平台研究”(GZHKJXM20160008)

指令采集方式(SNMP、Xflow 等)中，SNMP 收集的网络流量信息包括：输入/输出字节数、包丢弃数、包错误数等[1]。Xflow 则由路由器对经过自身的流量进行统计，统计的信息包括 IP 包的源地址、目的地址、源端口号、目的端口号等[2]。指令采集方式不需额外部署设备，因此应用广泛，但存在实时性差、采集的信息有限等缺点，只能实现流量统计分析，不能实现实时路由分析。

探针监测方式是在某段链路上部署探针，收集经过此链路的所有报文，并传送到协议分析服务器上进行存储，并进行解码分析。其优点是能够提供丰富的从物理层到应用层的详细信息，缺点是需要在监测链路节点上部署硬件探针，成本较高，且无法做到全网各条链路的整体监测[3]。

2 路由侦听监测采集方式的实现

电力专网数据网普遍采用的 IGP 协议是 OSPF。OSPF 协议的基础是 D 算法，该算法采用递归思想，以某个节点为起点，计算到其他节点的最短路径，基于 LSA(Link State Advertisement)消息，每台路由器能清楚知道整个网络拓扑(全网有向图)，进而可以独立的计算出自己至全网各个节点的最短路径树，即生成路由表，是一种白盒算法。

本文提出的路由侦听监测方式是基于 OSPF 协议白盒算法的特点，将一台路由管理设备挂接在 IP 网络上，通过采集 OSPF、BGP 等协议信息，持续绘制全网实时的三层拓扑图，并实时监测全网路由的变化，记录路由变动的历史数据，从而实现三层路由的监测和分析。它可及时发现链路故障和三层路由的异常，如路由环路、数据包来去路径不一致、路由抖动、路由器配置错误等问题，弥补当前 SNMP、XFLOW 协议对路由状态一无所知的空白。

路由侦听监测方式与指令采集方式、探针方式的对比如表 1 所示[4]。

在电力数据网的应用实际中，指令采集方式应用最为广泛，探针方式由于成本高，一般只部署在 IDC 和核心网络设备之间。路由侦听方式与这两种方式相比，具有明显的互补性：与探针方式相比，它具有全网监测特性，与指令采集方式相比，它具有实时监测三层路由的特性。路由侦听方式与指令采集方式、探针方式联合使用，可大大提高数据网的可视化能力和管理水平。

表 1 路由侦听监测方式与指令采集方式、探针方式对比

Tab. 1 Comparison of route interception mode, instruction acquisition mode and probe mode

对比	指令采集方式	探针方式	路由侦听方式
部署方式	通过定期向 IP 网络中各节点发送指令(SNMP，XFLOW 等)，提取路由信息，实现较为灵活。	所有链路上部署探针，采集相关协议报文，并上传到协议分析仪，实施复杂。	只需将路由管理仪与路由域中任一台网元建立邻居关系即可实现对该路由协议的监控，实施简单。
监测程度	实时性差，可能会“错过”瞬断类故障，高频率指令查询对节点设备带来较高负荷。	实现物理层～应用层全级监测，监测精度高，也更深入。可实现故障点的确定和原因深度分析。	可以监测三层路由的变化，对协议报文进行解码分析，能发现故障可能点而且可以分析故障原因。
硬件需求	仅需一台网管服务器需要通过一台服务器完成采集。	每条链路都需要探针接口，硬件需求多。	作为一台网元接入网内进行侦听，仅需一台服务器，作为网元接入网内进行侦听设备。
投资比较	硬件投资较少，但是软件开发难度大。	IP 网络规划越大，需要探针越多，投资就越大。	相比探针方式，硬件投资较少，基本与网络规模无关。

3 基于路由侦听监测的数据网监视及仿真系统设计

基于路由侦听监测采集方式设计的数据网监视及仿真系统，应能对使用 OSPF、BGP 路由协议的一个或多个 AS 域进行三层路由数据采集，并形成全网的三层拓扑图，在仿真软件中建立网络模型，反映网络的实时状态(现在)、实时记录网络的演变过程，进行故障重现和推演(过去)，还可设置工程割接时的链路中断、系统设置修改、节点关机维护等检修和故障场景，模拟网络将出现的各种状态，从而为割接、检修、规划工作提供重要参考(未来)。

本平台所需硬件为 1 台服务器和 1 台客户端，服务器建议放置在中心机房，连接到所监测网络的网管交换机上，与所监测网络 IP 可达即可。

仿真系统软件框架如图 1 所示[5-6]。

3.1 GUI 应用层

1)图形输出：提供网络拓扑输出到图形文件的功能。

2)文件输出：提供网络数据、报表数据输出到

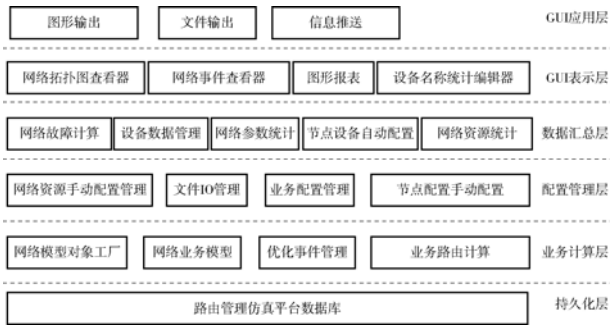

图 1　基于侦听监测采集方式的数据网仿真系统架构

Fig. 1　Data network simulation system architecture based on interception monitoring

xml 文件、excel 文件的功能。

3) 信息推送：该模块通过持续访问信息推送表，进行相关人员的信息推送，能够第一时间将网络故障、重要报警发送给指定的人员。

3.2　GUI 表示层

1) 网络拓扑图查看器：图形化显示现网网络拓扑，提供各种网络资源的图形可视化查询功能。

2) 网络事件查看器：图形化显示现网事件详细信息。

3) 图形报表：处理统计分析中，图形表格和图表的形式显示统计报表结果，并提供导出接口。

4) 设备名称统计编辑器：处理设备名称定义的请求，通过对设备进行命令，更好地查询设备的详细信息。

3.3　数据汇总层

1) 网络故障计算：根据收集到的 LSA 等相关信息，实时分析现网是否发生故障，发生什么样的故障。模块内提供单点和多点故障分析的接口，提供多种网络故障情况的进行分析接口。同时提供用户自定义故障等级的接口，将达到用户告警等级的相关故障提交到消息推送表中，从而进行实时反馈。

2) 采集数据管理：该模块负责现网实时数据采集和管理，通过使用侦听监测方式，与现网设备进行交互，实时获取现网设备的链路状态和设备状态。通过对采集到的数据进行格式化，使用统一的格式将数据进行提交进行持久化。通过侦听采集方式，提高了数据采集实时性，有效避免了数据遗漏。

3) 网络参数统计：定义网络的全局参数，提供各种网络资源统计接口。

4) 节点设备自动备份：实现对现网节点设备的自动配置备份，生成符合工程要求的配置备份文件，并提供针对设备故障分析的接口。

5) 网络资源统计：对网络各种资源、性能指标、设备报价统计分析，提供相关接口用于生成报表。

3.4　配置管理层

1) 网络资源手动配置管理：处理网络中域、链路、开销等资源属性的创建、删除和配置操作。

2) 文件 IO 管理：对系统的数据 IO 流程进行统一管理，协调数据 IO、模型数据、GUI 视图之间的流程处理，是文件 IO 流程符合正常软件使用习惯，并提供数据 IO 错误和异常的处理。

3) 业务配置管理：实现模拟网络中各种类型业务的配置管理，包括业务类型、速率类型、业务端口的配置，并手动对业务进行设计和配置。

4) 节点设备手动配置：实现手动对节点设备资源进行管理，通过图形化界面显示对节点设备 ID、类型、路由协议使用等进行配置。

3.5　业务计算层

1) 网络模型对象工厂：处理所有网络中仿真模型对象的初始化创建，提供统一的模型工厂创建接口。

2) 网络业务模型：描述系统处理的仿真业务模型并提供模型接口，包括了网络的节点、链路、网络域、链路开销、接口前缀掩码等。

3) 优化事件管理：处理优化计算的各种约束条件、优化目标的设置，并管理优化计算接口的调用，处理优化计算结果的输出。同时可以将仿真对象纳入计算范畴，使仿真对象与实时数据进行汇总并进行统一的计算。提供了基于实时数据的仿真功能，提供仿真效率。

4) 业务路由计算：基于 TOP-K 的算法模块，根据收集到的 LSA 进行自动分析计算。通过所收集到的链路状态信息，将链路分布到有向图中，通过在有向图中进行 TOP-K 算法运算，得到各节点间的最优路由。

3.6　持久化层

路由管理仿真平台数据库：对现网数据、计算数据进行数据库保存持久化。软件数据处理流程如图 2 所示。

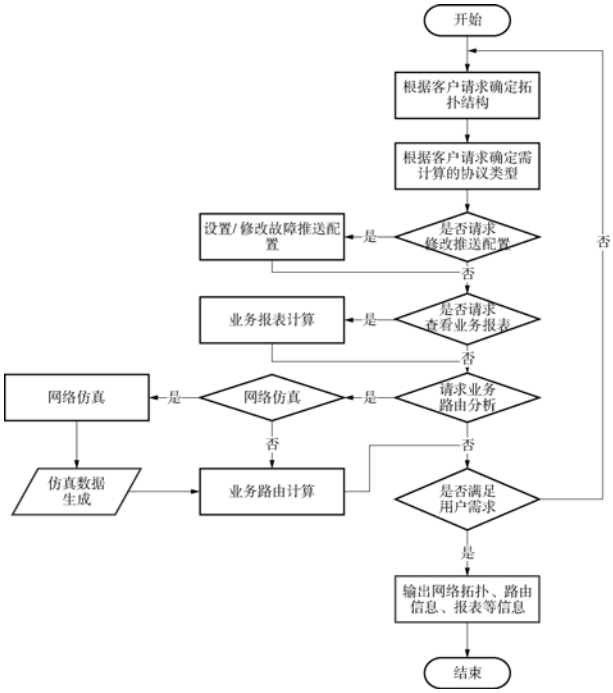

图2 基于侦听监测采集方式的数据网仿真系统数据处理流程图

Fig. 2 Data flow of data network simulation system based on interception monitoring

4 数据网综合监视及仿真系统应用

平台需要有3个主要的应用场景：分析场景、实时场景和模拟场景。

4.1 分析场景(过去)

平台可记录下历史路由事件，可以回到过去的某一个时间点，查看在这个时间点路由器的状态、信息、事件等，分析故障的原因，以供后续加固网络。

4.2 实时场景(现在)

实时的显示当前的网络状况，在网络发生故障时将故障的链路变成红色，并在界面下方提供实时的报警记录，还可以将报警信息以短信等形式发送。

4.3 模拟场景(未来)

仿真平台可在不影响现网的情况下，设置工程割接时的链路中断、参数修改、节点关机维护等检修场景，预测可能发生的情景，以便运维人员提前做好业务规划，避免业务中断。还可以对网络规划进行研究，优化组网策略。

5 数据网综合监视及仿真系统应用案例

5.1 故障定位——路由抖动

某天相关网络管理人员频繁收到链路UP/DOWN实时告警，使用平台的事件分析功能，查看平台的事件数量柱状图时，发现有部分柱体远高于其他柱体(如图3所示)，通过详细事件分析功能，选取柱体较高的部分，查看柱状图对应的详细事件信息，发现链路UP/DOWN事件确实较多，怀疑存在链路不稳定导致路由抖动。

图3 柱状图中有部分柱体远高于其他柱体

Fig. 3 Some of the pillars in the histogram are much higher than others

通过路由抖动汇总表功能对现网的路由抖动汇总情况进行查看，发现88.148.253.88/30这个网段在一天的时间范围内发生多次路由UP/DOWN抖动。通过对通告这个网段的信息进行分析，发现ID为10.142.251.89的路由器的IP为88.148.253.89的端口在不停的抖动，从而导致路由抖动。通过排查该路由器物理接口，发现88.148.253.89对应的物理接口存在连线网线老化松动的情况，更换网线后，路由正常不再出现抖动。

通过平台的告警、事件分析功能发现了现网存在路由抖动的问题，通过详细事件分析功能对路由抖动事件进行详细分析，找到了引起路由抖动的设备和端口，为快速发现定位故障提供了有效的保障。

5.2 仿真割接——割接前仿真设备下线

收到某供电局综合数据网割接需求，需要关闭一台在线运行的汇聚层设备添加板卡。没有仿真平台时该类割接会对现网造成的影响只能人工估计，存在考虑不周全的隐患。仿真系统上线后，在平台的网络拓扑上查询到了需要下线的设备，通过在平台上使用仿真功能将该路由器Down，然后进行业

务测试，发现下线该汇聚层设备后原有正常对称路径(如图 4 所示)变成非对称路径(如图 5 所示)，由于原有业务对路径的对称性要求很高，下线设备后业务将受到很大影响。

使用平台进行业务调整并反复使用仿真功能进行测试，修改相关链路的 Metric 值，将非对称路径调整为对称路径(如图 6 所示)，不影响该业务的正常使用。同时测试其他业务情况，发现其他业务均正常。

进行正式割接时，将设备下线并对受影响的业务进行调整，确保没有非对称路径，有效保证了割接的正确实施。

通过使用平台，提前发现了潜在的割接风险，同时通过使用平台进行割接演练仿真，保证了业务迁移的正确性，为割接演练、引导割接提供了有效的保障。

6　结论

网络路由侦听监测方式是一种新型的网络状态采集方式，它基于 OSPF 协议白盒算法的特点，可

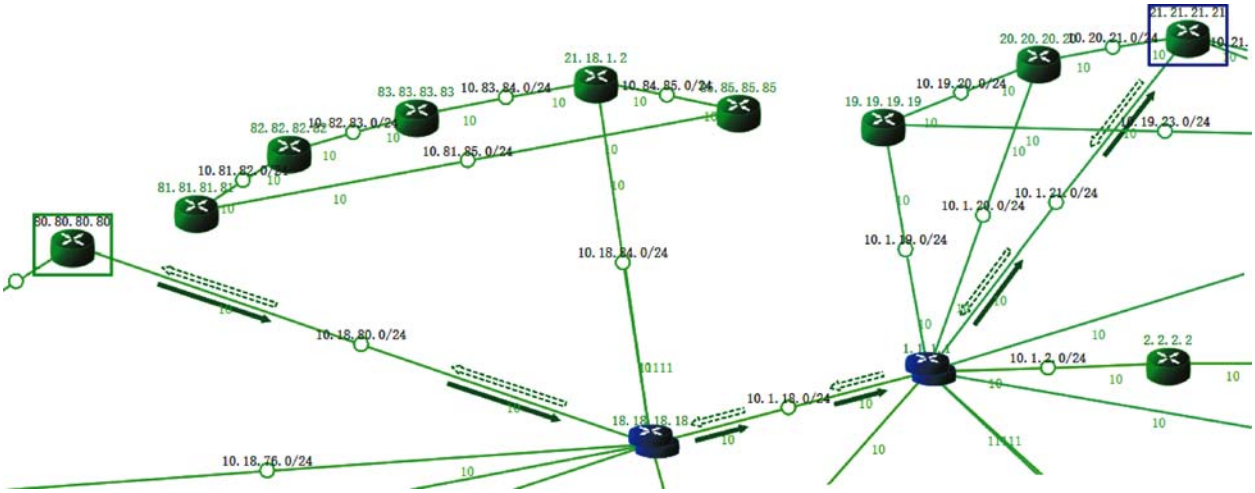

图 4　综合数据网汇聚层设备下线前为对称路径

Fig. 4　Before down the convergence layer device

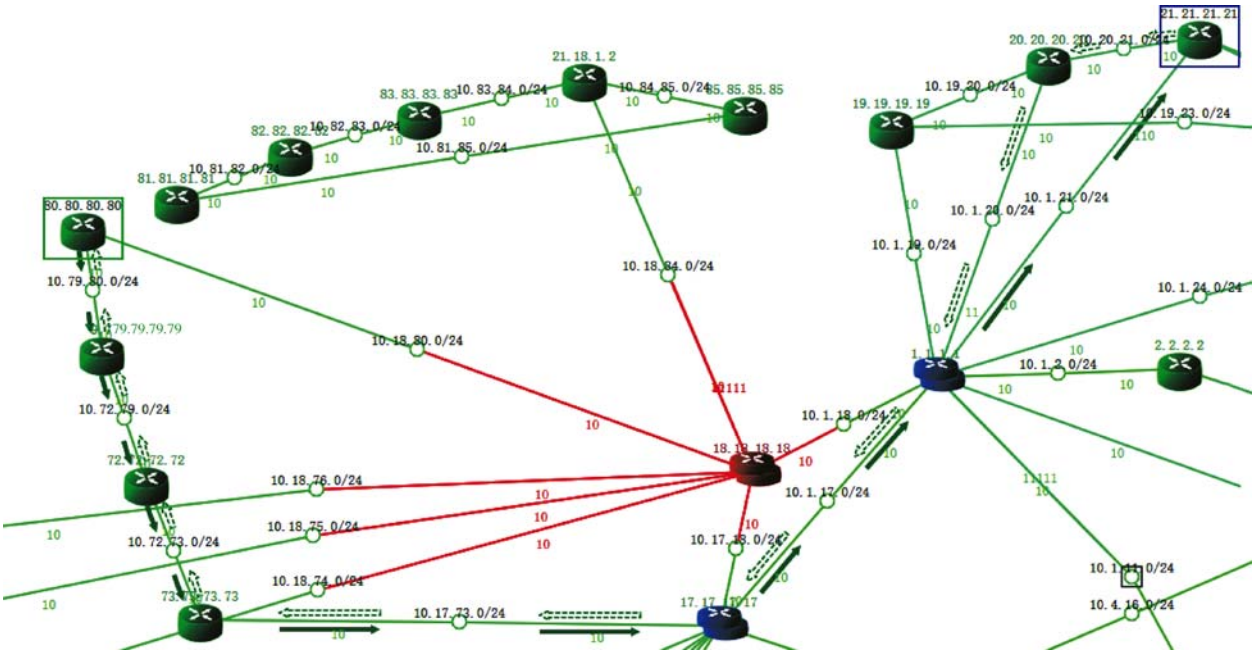

图 5　通过仿真模拟汇聚层设备下线后发现非对称路径

Fig. 5　An asymmetric path appears after the convergence layer device is offline by simulation

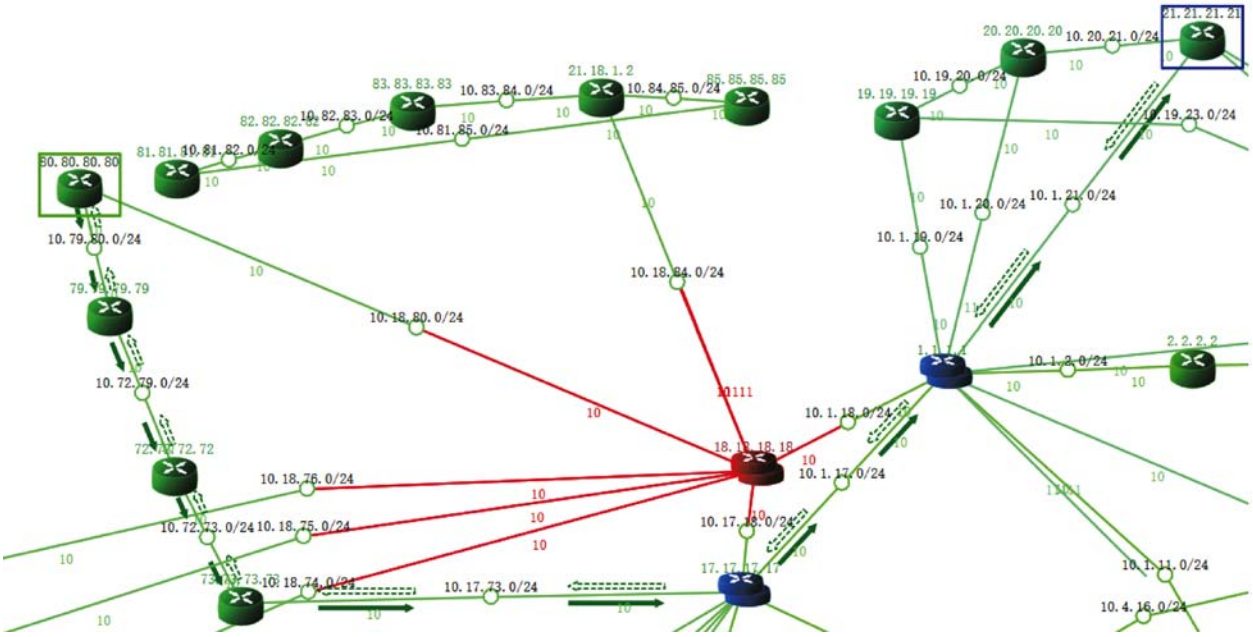

图6 通过仿真修改将非对称路径变为对称路径

Fig. 6 Change the asymmetric path to symmetric path by simulation

呈现与路由器“看”到的完全一样的实时全网地图，从而可及时发现链路故障和三层路由的异常，实现全网路由的实时监视。基于网络侦听监测的数据网监视和仿真系统可辅助网管人员进行故障发现和处理，记录各类历史路由时间用于分析，并在不影响现网的情况用于网络割接等工作的测试和论证。该系统在广州局综合数据网进行了试运行，帮助发现了路由抖动问题，并提前发现了潜在的割接风险，验证了该系统的实用性。

参考文献：

[1] WRIGHT G R，陆雪莹，蒋慧．TCP/IP 详解卷 1：协议[M]．北京：机械工业出版社，2000.

[2] WRIGHT G R，陆雪莹，蒋慧．TCP/IP 详解卷 2：实现[M]．北京：机械工业出版社，2000.

[3] CHOI H K，LIMB J O. A behavioral model of web traffic[C]//IEEE Computer Society. Proceedings. Seventh International Conference on Network Protocols，Toronto，Canada，Oct. 31 to Nov. 3，1999. USA：IEEE Computer Society，1999：327.

[4] 刘倩，齐晓莉，高峰，等．采用侦听方式实现 IP 路由分析方案研究[J]．电信工程技术与标准化，2012，25(3)：66-69.

[5] 马涛．电力综合数据网模拟仿真系统设计与实现[D]．成都：电子科技大学，2016.

[6] 卜佑军．IP 网多路径数据传输关键技术研究[D]．郑州：解放军信息工程大学，2012：18-21.

作者简介：

ZHONG Y Q

衷宇清(通信作者)

1968-，男，江西南昌人，广州供电局通信中心高级工程师，工学硕士，主要从事电力系统通信规划、运行、技术管理(e-mail)zhongyq@guangzhou.csg.cn。

陈昌娜

1982-，女，广东汕头人，工程师，工学学士，主要从事电力通信设备的运行维护、电力通信项目的协调实施管理、电力通信网管系统的建设和推广等工作(e-mail)eleanor_ccn@163.com。

王雅娟

1983-，女，山东济南人，高级工程师，工学硕士，主要从事电力通信的研究、设计工作，承担过多项电网建设、改造、科技、规划项目(e-mail)13570364329@163.com。

晏平

1977-，男，云南昆明人，工程师，通信工程专业，主要从事 IP 网络路由理论研究和成果转化、IP 网络管理的精细化研究等工作(e-mail)13908860026@139.com。

(责任编辑 郑文棠)