



运营商 DNS 海量数据分析技术优化和应用

彭巍¹, 贺晓东¹, 陆小铭¹, 汲传鑫²

(1. 中国电信股份有限公司广州研究院, 广东 广州 510630;

2. 上海牙木通讯技术有限公司, 上海 200030)

摘要: 主要分析了域名数据分析的原理和传统域名数据分析方法的局限性, 结合网络发展的趋势提出了一种基于 Hadoop 的运营商 DNS 海量数据分析技术, 对该技术的架构、实现方案、优势进行了分析, 并且在大数据网上对该方案进行了应用, 最后对 DNS 数据分析的效果进行了阐述, 该技术可为网络的发展优化、建设提供科学的参考。

关键词: DNS; Hadoop; 数据分析

中图分类号: TN929.5

文献标识码: A

doi: 10.11959/j.issn.1000-0801.2018092

Optimization and application of the carrier DNS data analysis technology

PENG Wei¹, HE Xiaodong¹, LU Xiaoming¹, JI Chuanxin²

1. Guangzhou Research Institute of China Telecom Co., Ltd., Guangzhou 510630, China

2. Shanghai Yamu Communication Technology Co., Ltd., Shanghai 200030, China

Abstract: The principles of DNS data analysis and the limitations of traditional DNS data analysis method were analyzed. According to the trend of the development of the IP network, an analysis technology based on the Hadoop towards huge amounts of DNS data was proposed. Also the architecture, implementation scheme and advantages of the technology scheme were described, then the effect of Hadoop DNS data analysis which applied in the telecom network was expounded. The research results can provide scientific reference for the development and optimization of the telecom network.

Key words: domain name system, Hadoop, data analysis

1 引言

DNS (域名系统) 作为承载全球亿万域名正常使用的系统, 是互联网的基础设施, 是广大用户访问互联网的入口。用户通过 DNS 获取访问

网站、网址的 IP 地址解析结果, 网络运营者可通过 DNS 记录、获取广大用户诸多互联网访问的相关数据, 因此通过相关的用户域名访问流量多维分析, 可获取重要的用户互联网访问信息, 有助于运营商大幅提升互联网精细化运营和管

控能力。通过数据多维分析,根据域名、用户等多个维度进行挖掘,可以确定用户的互联网使用行为,为更好地提供差异化域名服务提供信息数据,同时为网络发展布局、工程建设、网络安全建设提供科学依据。本文探讨了大型运营商在DNS海量数据多维分析方面的关键技术以及优化提升方案,以获取高效、科学、准确的DNS访问多维分析数据。

2 域名数据分析的必要性

随着互联网的飞速发展,相关的业务量和业务种类产生了质的飞跃。在互联网业务量增长的同时也出现了各种各样的新问题,包括在用户群和网络流量爆炸性增长的情况下如何提升网络的服务质量、如何提升用户的网络使用体验、如何更合理地利用资源等。DNS数据反映了互联网域名访问的整体情况,包括广大互联网用户经常访问的网站/网址、在某一个网站内用户访问的主要内容是新闻或视频或电子商务等,因此基于域名访问的海量数据可对互联网用户群的访问特征、兴趣进行分析,获取互联网整体的访问行为;另一方面,通过对海量访问域名数据的分析,还可以将互联网上的重要域名与IP地址之间的映射管理数据进行存储,假如域名系统出现故障或问题,可提供实时和必要的容灾、备份功能,保证互联网的正常、稳定、高效运行;此外,对于互联网用户的访问信息,对于网络运营商而言可以根据相关科学数据进行网络建设的优化、IDC建设布局的实施,保证提升网络流量的传送效率、减少无谓的流量长途穿越,对于互联网整体层面的质量提升以及网络资源利用率的提高具有重要的意义。

而面对海量的DNS查询数据,如何进行高效、实时的数据分析是一个难题。大型网络运营商在组建自身的DNS节点为用户提供直接服务的同时,也需要构建海量DNS数据分析系统。通过应

用海量数据存储与高性能数据挖掘系统,实现域名流量数据的存储、深度分析,并通过多维分析功能模块实现域名、用户、网络等不同维度和各维度组合的分析能力,最终获取科学、准确、多维度的域名分析参数。

3 传统域名数据分析技术及局限性

3.1 域名访问信息的内容及特征

某个用户在某段时间向DNS查询某个域名,例如www.abc.com,DNS会向用户返回域名对应的IP地址抵制,假设为202.?.0.1,此数据信息可以在DNS数据分析系统中记录下来。每天这样的数据信息量是巨大的,据统计,仅某省运营商网内的查询量峰值就可以达到800万QPS(每秒查询次数)。因此DNS查询数据反映了互联网域名访问的全网整体情况,目前DNS数据存储的主要维度包括源IP地址、域名、时间戳、解析IP地址、状态码和用户所访问的DNS服务IP地址。通过这些数据维度的组合分析能够获取大量具有实际指导意义的科学数据。例如全网的域名访问Top N排名,即每个网站访问量的排名;还有各区域网络用户的访问排名;各业务分类(视频、即时通信、网页等)的访问数据等。不仅如此,目前各网络运营者以及ICP(内容提供商)均提供了域名智能解析功能,即对于不同的用户群提供同一域名的不同解析结果,域名多维分析结果对提升智能解析的效率具有重要的反馈意义。

3.2 传统域名数据分析技术

传统的海量DNS数据分析方法,一般分为4个部分:第一是将远程的DNS存储数据通过网络传输到本地文件系统中,该过程非常耗费网络资源,并且因为数据量非常大,耗费的时间也相当长;第二是将传输过来的海量数据进行结构化解析,通常为了加快该进度,一般通过多进程的解析日志模式,假如数据日志量超过一定的规模量,那么解析时间就会非常长;第三是将结构化



数据存储到结构化的数据库中，常见的数据库集群有 RAC 集群、GreenPlum 集群等；第四是通过数据库进行分析数据，最终给出数据分析结果，在数据量极大的情况下，结构化数据库计算非常缓慢甚至无法进行。图 1 就是常见的处理流程。

3.3 传统域名数据分析技术的局限性

通过上述流程和图 1，可见传统的域名数据处理分析方法有以下四大缺点。

- 海量网络传输：对于用户群非常庞大的网络运营商，例如广东省某运营商网内就有几千万的互联网用户，每个 DNS 节点上的数据采集前置机上都有数据量非常大的 DNS 存储数据，如果采用这种方法，每天多达几百 Gbit/s 规模的日志数据传输的网络成本和时间成本会非常大。
- 海量冗余存储：传统的方法会冗余存储 3 份数据，即传输到本地的一份、结构化解析的一份和存放在数据库的一份，运营商每天的日志数据非常大，无法支撑如此大的存储压力。
- 频繁代码解析：假如日志格式发生变化都需要人工修改结构化解析脚本，那么运营

者就可能不断持续地进行调优测试，网络运营维护的时间成本和人力成本都会非常高，效率也低下。

- 高成本数据库：结构化数据库有一个明显的缺点就是一旦数据量大运行就会很慢，这同样增加了数据库运营维护的工作量和人力成本。

因此，在“互联网+”发展的趋势下，随着网络用户和流量的增长，传统的域名数据分析方法已经难以适应目前网络的增长趋势，迫切需要进行相关域名数据分析技术的优化和应用研究、部署。

4 基于 Hadoop 的海量 DNS 数据解析系统的技术优化和应用

4.1 Hadoop 数据分析的关键技术

Hadoop 是一个通用且易于实施应用的 MapReduce 软件框架，基于 Hadoop 架构的应用程序能够运行在由上千个单独机器组成的大型集群上，并可以采用一种可靠容错的方式并行处理达到 TB 级别的数据量。一个 MapReduce 作业(job)通常会把输入的数据集切分为若干独立的数据

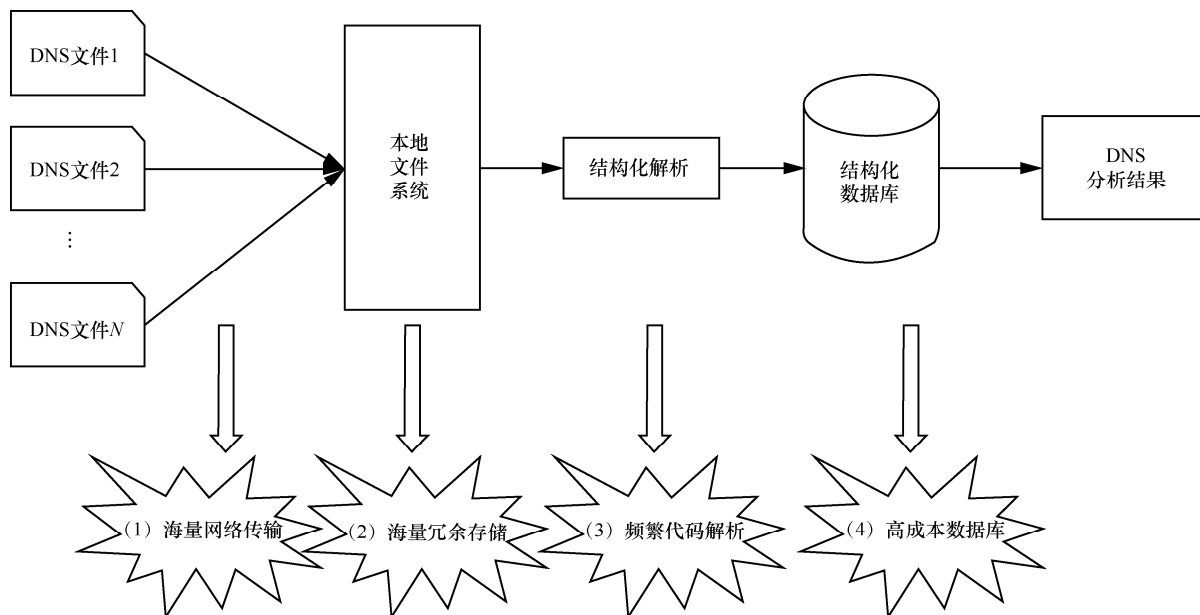


图 1 传统域名数据分析方法处理流程

块, 由 map 任务(task)以完全并行的方式处理它们。首先整体框架会对 map 的输出进行排序, 然后把结果输入 reduce 任务; 通常作业的输入和输出都会被存储在文件系统中。整个框架负责任务的调度和监控以及重新执行已经失败的任务。Hadoop 的优势是利用大量的普通机器, 将海量的数据碎片化、分布式地计算, 并利用其独有的 HDFS (分布式文件系统) 进行存储管理, 实现海量高效稳定计算。

4.2 基于 Hadoop 的海量域名数据分析的技术优化应用

某省运营商每日仅某一地市的 DNS 日志数据就可能达到几百个 Gbit/s, 超过几十亿条域名记录, 传统方式非常依赖高性能的机器进行解析和分析, 成本上和效率上难以为继。

因此, 为了优化传统域名数据分析模式, 本文提出了一种基于 Hadoop 的海量 DNS 数据分析

系统的技术优化方案, 该方案在广东省某大型运营商的网络中得到了实施应用。整体体系采用 Hadoop 框架, 主要分为以下 3 个步骤。

步骤 1 在远程日志服务器上直接搭建 HDFS, 采用 ORC 的文件格式, 极大地减少了文件存储, 并无需传输到本地。

步骤 2 基于 MapReduce 技术, 将日志按照 MapReduce 框架解析, 程序会自动分布式处理和计算, 无需增加服务器, 直接使用 DNS 服务器即可。

步骤 3 基于 Hive 将结果汇总计算生成报表, 整个过程没有多余的存储、多余的网络传输、多余的数据成本, 具体如图 2 所示。

采用基于 Hadoop 框架的域名数据分析优化方案, 相比传统方法具有以下几大优势和技术创新。

- 实现了 Hadoop 海量数据的本地计算, 极大

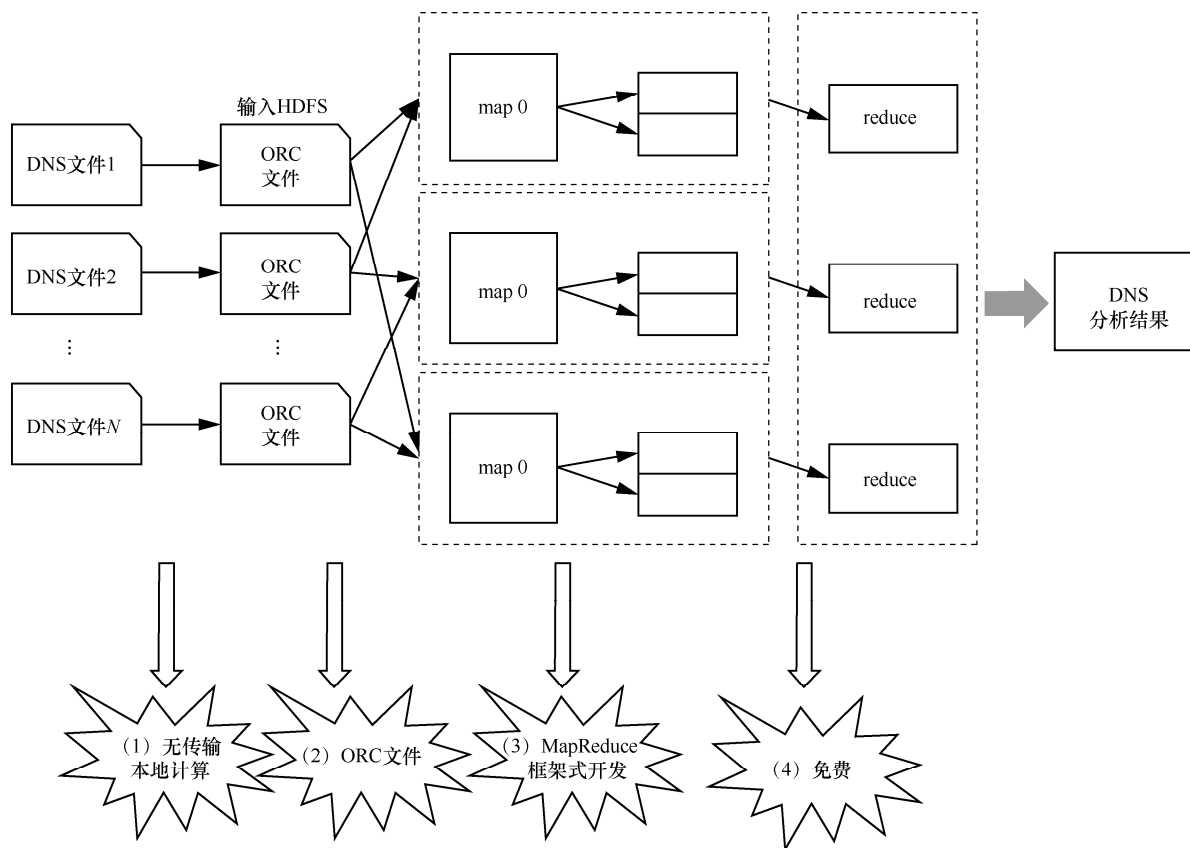


图2 基于 Hadoop 框架的域名数据分析优化方案



地提升了数据处理效率。整个系统无大量的网络数据传输过程,计算过程置于域名数据服务器本地,只需配置好 Zookeeper 功能即可实现远程计算。传统的数据分析计算需要将数据传输到服务器集群去进行,这种模式极大地增加了网络传输成本和时间成本,例如某地市每天 DNS 日志数据量为 500 Gbit/s,假设网管传送带宽为 10 Mbit/s,那传输该日志数据就需要近 14.2 h。而采用了 Hadoop 本地计算优化,也即把 DNS 节点的数据前置服务器当成 Hadoop 的节点,实现了本地服务器的数据计算,大大提高了数据分析能力,减少了时间成本和运营维护成本,提高了数据分析的实时性和高效性。

- 基于 ORC 文件极限存储模式,对比传统方法极大地减少数据存储量,并且只需存储 1 次。普通的 HDFS 采用的文件格式占用存储非常大,直接严重影响了数据存储效率,间接延长了数据处理时间。本优化方案采用了 ORC 文件存储,有效降低了数据存储成本并提升了时间效率,经测试采用 ORC 格式存储压力是原有模式的 3.33%。
- 基于 MapReduce 框架进行开发,发生任何的格式变化或数据异常,只要按照标准 MapReduce 框架即可实现格式通用,和传统方法相比减少了开发维护的工作量。运营维护工作简易,无需专门的数据库维护人员,减少了购置数据库机器和软件许可的采购成本。

5 现网海量 DNS 数据分析技术优化的效果

基于上述域名数据分析的技术优化应用,可以对域名查询存储的海量流量数据信息进行高效的计算、分析划分。存储的域名数据由查询的源

地址、域名、解析地址等信息构成,因此可以通过对上述类型数据进行按源地址、域名、解析地址等维度进行归类。同时再结合网络地址段划分,又可以进行网络维度例如宽带网、移动网,或者省网中的各地市网络地址段进行划分,实现多个维度的信息区分,包括以下几点:

- 用户维度,以地址进行划分;
- 域名维度,以查询的域名划分;
- 网络维度范围,例如宽带网、移动网以源地址划分,或者不同地市的城域网以网络地址段进行划分;
- 业务维度,以各域名所属的业务类型进行划分;
- 其他各维度的组合分类。

并且可以用报表、图形等多种方式进行呈现。实现 DNS 数据多维度分析的效果概述如图 3 所示。

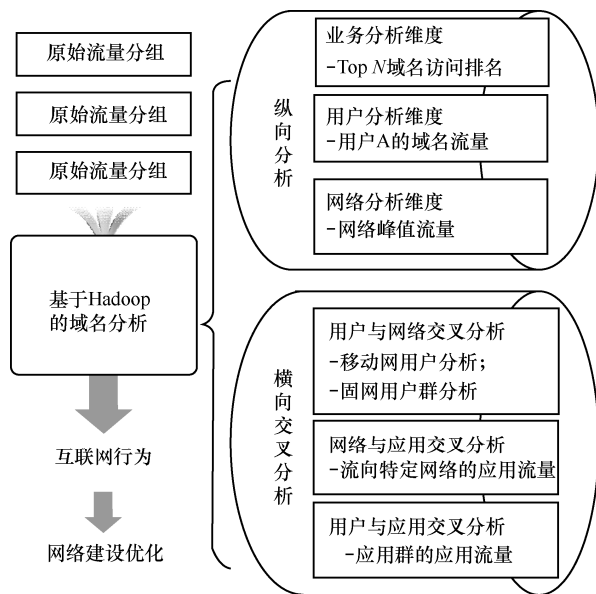


图 3 DNS 数据分析的效果

(1) 互联网业务维度占比分析

互联网业务类型是网络运营者和广大互联网企业、用户都非常关心的重要数据,通过相关的数据信息的组合分析可以获取具有实际指导意义的分析场景,以互联网业务为例可获取域名业务类型占比参考数据。将占总访问量 80%以上的域

名和产品业务类型进行分类整合并归纳出电商类、通信类、视频类、地图类、下载类、社交类、音乐类、视频类等 20 个域名类型。通过域名类型的占比来分析全网资源的业务情况。图 4 显示主要的访问集中在购物类和视频类，二者分别占总访问量的 21.28% 和 15.74%。

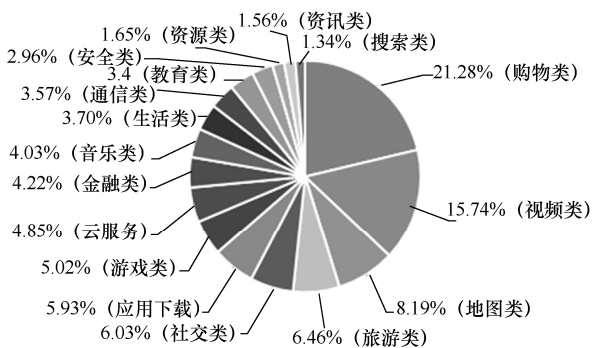


图4 域名业务维度占比分析

(2) 某一业务类型维度的排名分析

通过 DNS 海量数据分析，不仅能实现域名类型和域名所属业务相互组合分析不同域名类型中域名所属的业务量、相关排名和占比，还可以通过环比不同周期的域名业务量发现互联网中业务种类变化趋势以及相同业务中的竞争关系变化。对于业务量持续发展快速的域名可以进行相关的资源调整，如图 5 所示。

(3) 域名流量维度的监控分析

对重点关注的域名进行实时流量的监控，及时发现流量的异常变化，如图 6 所示。

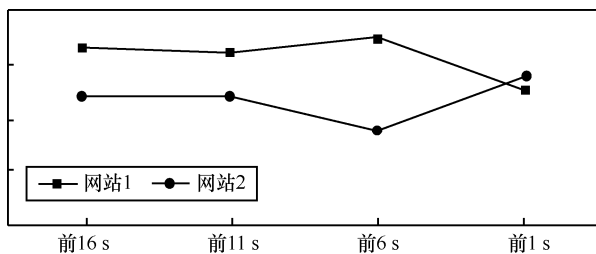


图6 域名流量监控分析

此外，还可以分析用户群结合域名维度、网络结合域名访问维度等各种组合的分析模式，在此不作详细叙述。总之，DNS 海量数据的分析结果具有重要的参考价值，对于网络运营商而言，可以依据相关数据进行网络的优化改造建设、IDC 数据中心的布局 and 规划、DNS 智能解析优化、用户发展规划等工作，对于 ICP（内容提供商）而言，可以进行 CDN（内容分发网络）的规划建设、解析优化等工作，对于互联网用户则可以获取互联网热门的舆情信息等。

6 结束语

本文对域名数据分析的技术进行了阐述和分析，总结和指出了传统域名数据分析方法的局限性，并提出了一种基于 Hadoop 的 DNS 海量数据分析方案，并且在运营商现网中得到了实施和应用。该方案有效地体现了运营商网络的智能化、精细化发展方向，DNS 数据分析的结果可以为网络发展建设提供科学、准确、详尽的数据参数，为持续提升互联网访问的质量

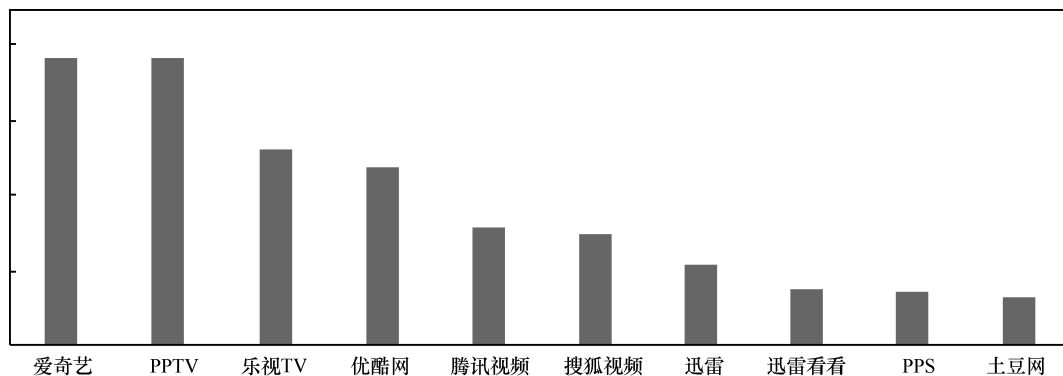


图5 视频类业务不同网站的访问分析



奠定了坚实的基础, 有利于国家“互联网+”战略的发展和实施。

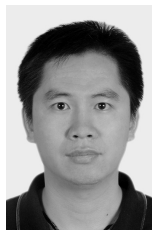
参考文献:

- [1] 彭巍, 曹维华, 贺晓东. 大型运营商 DNS 智能解析关键技术及方案[J]. 电信科学, 2016, 32(1): 159-163.
PENG W, CAO W H, HE X D. Key technology and solution of intelligent resolution for the huge carrier DNS[J]. Telecommunications Science, 2016, 32(1): 159-163.
- [2] 彭巍, 曹维华, 李文云, 等. 基于全局 Anycast 的智能域名系统架构演进研究[J]. 广东通信技术, 2014(5): 14-17.
PENG W, CAO W H, LI W Y, et al. The solution of global Anycast architecture of the DNS network[J]. Guangdong Communication Technology, 2014(5): 14-17.
- [3] 曹维华, 贺晓东, 彭巍, 等. 基于转发和控制分离的 DNS 新型架构研究[J]. 广东通信技术, 2015(10): 41-44.
CAO W H, HE X D, PENG W, et al. Research on DNS architecture based on forwarding and control separation[J]. Guangdong Communication Technology, 2015(10): 41-44.
- [4] 申志伟, 房秉毅. 一种智能动态域名系统在大型电子商务中的应用方法[J]. 电信科学, 2014, 30(1): 128-135.
SHEN Z W, FANG B Y. Application method of smart dynamic DNS in huge e-commerce[J]. Telecommunications Science, 2014, 30(1): 128-135.
- [5] 漆晨曦. 电信企业大数据分析、应用及管理发展策略[J]. 电信科学, 2013, 29(3): 12-16.
QI C X. Big data analysis and management in telecommunications[J]. Telecommunications Science, 2013, 29(3): 12-16.
- [6] 黎宏剑, 刘恒, 黄广文, 等. 基于 Hadoop 的海量电信数据云计算平台研究[J]. 电信科学, 2012, 28(8): 80-85.
LI H J, LIU H, HUANG G W, et al. Study on massive telecom data cloud computing platform based on Hadoop[J]. Telecommunications Science, 2012, 28(8): 80-85.
- [7] 陈娜, 徐歆壹, 宋红兵, 等. 基于 Hadoop 的电信 BSS 大数据

平台建设研究[J]. 电信科学, 2013, 29(3): 36-40, 47.

CHEN N, XU X Y, SONG H B, et al. Research on big data system of telecom based on the Hadoop[J]. Telecommunications Science, 2013, 29(3): 36-40, 47.

[作者简介]



彭巍 (1975-), 男, 中国电信股份有限公司广州研究院工程师, 主要研究方向为 IP 网络相关领域。



贺晓东 (1975-), 男, 中国电信股份有限公司广州研究院高级工程师, 主要研究方向为 IP 网络、宽带接入网等。



陆小铭 (1978-), 男, 中国电信股份有限公司广州研究院高级工程师, 主要研究方向为 IP 骨干网络管理、SDN 等。



汲传鑫 (1985-), 男, 上海牙木通讯技术有限公司高级工程师, 主要研究方向为 DNS 设备与系统的研发等。