基于主动测量的CN权威镜像选址效果评估

陈闻宇[1],肖中南[1],徐彦之[2]

1. 中国互联网络信息中心,北京 100190
2. 中关村互联网金融行业协会,北京 100080

摘要 域名服务器(DNS)镜像技术是提升DNS系统安全性、稳定性和解析性能的重要方法。以CN镜像服务器的实测数据为例,采用主动测量法,主动向被探测的网络或者对象发送特定的数据包,根据响应时间和应答数据包分析研究对象的网络特征,以此评估CN权威服务器的选址效果。结果显示,镜像技术使全球各地都能提供较好的CN解析服务,虽然服务效果存在地理上的差异性,但与CN节点的部署实际情况相符。该效果评估方法能够为节点部署提供可靠的决策依据,有助于DNS节点高效有序的规划建设。

关键词 域名服务器;主动测量;DNS镜像;开放递归

中图分类号 TP311 **文献标志码** A **doi** 10.3981/j.issn.1000-7857.2015.12.015

Evaluation of CN authority DNS mirror server distribution based on active measurement

CHEN Wenyu[1], XIAO Zhongnan[1], XU Yanzhi[2]

1. China Internet Network Information Center, Beijing 100190, China
2. Z-Park Association of Internet Finance, Beijing 100080, China

Abstract DNS(domain name server)is one of the most important basic facilities of Internet. The technique of DNS mirror is a key solution to improvinge DNS system's security, stability and analyticity. In this article, we develop a new solution to evaluation and optimization of the global CN DNS mirror distribution. We send a certain data package to the target server and calculate the response time for analysis of the scanned server's behavior. User's experiences that CN DNS servers' performances vary due to geographic differences are considered in our study. The solution can provide reliable suggestion to DNS distribution for a more efficient and orderly plan.

Keywords domain name server (DNS);active measurement;DNS mirror;open resolver

域名系统在诞生后的几十年中,一直为全球互联网的正确运行提供关键性的基础服务,其重要性也与日俱增。作为Internet的重要基础设施,DNS的核心功能是完成域名到IP地址的相互映射,能够使人们更方便地访问互联网,而不用去记住能够被机器直接读取的IP地址数串[1]。因此,各种基于域名的Web网站访问、电子邮件系统、文件共享系统等都依靠DNS的支持而得以正常开展,DNS解析是当今互联网绝大多数应用的实际寻址方式。域名技术的再发展及基于域名技术的多种应用,进一步丰富了互联网的应用和协议。域名也是互联网上的身份标识,是不可重复的唯一标识资源。

随着互联网规模的不断扩大,由于DNS系统本身的复杂性和全球化分布的特点及与DNS相关的各种新技术的研究和逐步部署,DNS系统正面临着越来越大的挑战。DNS现有的管理、配置和规划机制及保护自己免受各种攻击的安全机

收稿日期:2015-01-16;修回日期:2015-03-23
基金项目:中国科学院计算机网络信息中心青年基金项目(CNIC_QN_1309)
作者简介:陈闻宇,工程师,研究方向为软件工程、项目管理,电子信箱:chenwenyu@cnnic.cn
引用格式:陈闻宇, 肖中南, 徐彦之. 基于主动测量的CN权威镜像选址效果评估[J]. 科技导报, 2015, 33(12): 88-92.

制都非常有限。目前,全球DNS系统主要依赖多点镜像(Anycast)、负载均衡等方法应对流量突发访问及遭受DDoS攻击时保持正常运行。

Anycast是一项将单个服务器复制并分布部署到多点的技术(镜像),所有复制的服务器对外都是同一个IP地址,并包含同样的DNS记录数据[2]。DNS镜像技术是提升DNS系统安全性、稳定性和解析性能的重要方法[3]。有研究表明,38%~80%的DNS查询流量被路由到最近解析节点。通过测量表明,解析到最近节点的比例与区文件数据的稳定性之间是相互影响的,两者需要取一个均衡[4]。

Anycast技术涉及到节点的选址,DNS服务提供组织在选址时会综合考虑各种因素,如用户来源分布、选址所在地网络状况及成本等[5],以最优化服务质量。本研究从CN权威服务解析的实际效果评估其服务质量,进而评估其镜像节点的选址合理性。

为了达到上述目的,主要采用主动测量方法,即利用一定的工具或手段,主动向被探测的网络或者对象发送特定的数据包,根据响应时间及结果研究、分析网络行为。主动测量需要向网络中注入流量,这会增加网络负载,影响网络性能,因此在实际操作中需要控制测量频率。

主动测量需要依赖于监测点的部署,一般在主要网络部署多个监测点,综合分析处理各个监测点的监测结果,以提高监测结果的完备性和准确性[6]。

在该领域,文献[7]研究了基于多点主动测量权威名字服务器的分布、地理位置及其对性能和安全性的影响。文献[8]定义了DNS服务质量,并综合分析了影响因素及服务质量提高办法,给出了基于网络性能指标的服务质量评价模型。文献[9]以路由路径平均长度、路由往返时延RTT、时延抖动、路径瓶颈带宽和丢包率作为DNS解析网络性能测量参数,建立测试方法,并对全国各省市60个DNS递归服务器进行了主动测量。

本研究需要获取从全球各个国家访问CN的时延,以研究其实际效果,最大的难点在于获取覆盖全球各国的监测点,根据DNS的内部原理,采用开放递归采集相关数据。

1　数据采集

1.1　开放递归

开放递归是指为其管辖区域外的客户端提供DNS解析服务的DNS递归服务器。由于其开放性,可以在任意地方、由任何人向其发起查询。本研究利用向分布在全球各地的开放递归发起特定查询,分析响应结果,以获取所需数据(开放递归常常被用来作为DNS放大攻击的源[10])。如果能获取开放递归列表,相当于拥有了分布在全球的大量探测点。

传统上对网络进行扫描使用最多的工具是nmap,但nmap扫描速度并不理想,如电子前哨基金会(EFF)曾在2010年对整个互联网进行了扫描,使用nmap,耗时2~3个月[11]。因此许多研究机构采用抽样的方式来评估当前互联网各种维度的规模。zmap的出现使得以较短时间扫描整个互联网成为现实。TCP是可靠的面向连接的协议,zmap通过将连接信息编码至发送的数据包中实现无状态扫描,无状态扫描不需维护TCP状态,不占用系统相关资源,它能够在1 Gbps带宽环境下在45 min内扫描完毕整个互联网,因而扫描速度非常快。

本研究中扫描开放53端口的服务器时使用的工具是zmap;进行了3次扫描,耗时3周左右,表1分别统计了开放53端口(DNS服务器的默认端口即为53)的服务器数量和属于开放递归的服务器数量,后者属于前者的子集。首先向全网IP发起探测,记录53端口能连通的IP列表,在此基础上,向53端口发起DNS查询,记录能正确响应的IP列表。由于网络主机处于动态变化中,而本研究中只关注相对稳定的开放递归。为了过滤数据中的噪声,取3次所得开放递归(IP)的交集。图1为开放递归服务器全球分布,开放递归数量大于1万的明细见表2。

表1　53端口及递归服务器扫描数据

Table 1　Scanned 53port & open resolvers

扫描次数	服务器数/台	
	开放53端口	开放递归
第1次	13876889	1593534
第2次	14722382	1681151
第3次	13133968	1425668

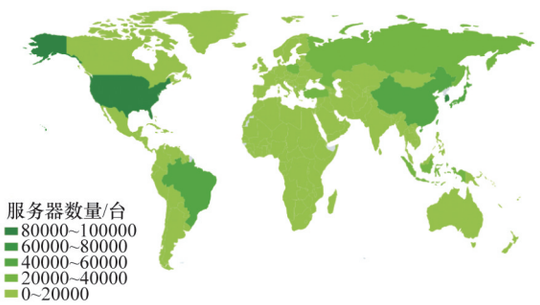

图1　开放递归服务器全球分布(2014)

Fig. 1　Open resolver server global distribution (2014)

表2　各国递归服务器数量

Table 2　Open resolever server quantity

国家	开放递归服务器/台	国家	开放递归服务器/台
韩国	112426	英国	15498
美国	103836	西班牙	14874
香港	61022	乌克兰	14261
中国	59255	德国	13972
巴西	58148	意大利	12649
日本	53190	捷克	12066
俄罗斯	37076	澳大利亚	11838
土耳其	32486	法国	11159
印度尼西亚	27313	阿根廷	10718
台湾	24721	印度	10638
波兰	23660	加拿大	10453

1.2 数据采集

数据采集目的是获得开放递归访问CN权威服务器的解析时延,该时延即反映了从开放递归所在国家(地区)到CN权威解析时延。测量多次,并将同一地区的时延数据合并可得CN权威服务选址效果,总体的时延越小,说明选址效果越佳。为了实现该目的,构造查询逻辑:1)确保CN的权威IP都在递归缓存中,让后续查询不经过根服务器,直接到达CN权威服务器;2)通过开放递归,询问一个随机的CN域名,该域名需要足够随机,确保不存在(生成3个随机域名,每个查2次):第1次查询递归无缓存数据,递归直接查CN权威,第2次查询递归有缓存数据,直接返回(忽略递归本身的数据处理时间)。第1次查询响应时间记为t_1,第2次查询响应时间记为t_2,两次查询响应时间之差即可近似为开放递归到CN权威的解析时延。

1.3 原理分析

图2是正常的DNS解析。

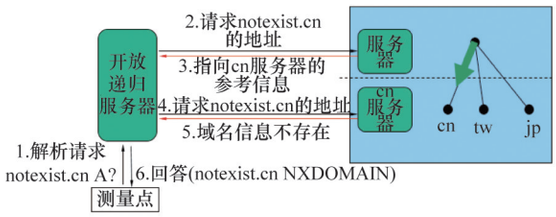

图2 正常的DNS解析

Fig. 2 Normal DNS work process

域名解析的工作原理:

1)客户机(即本文中的测量点)提出域名解析请求,并将该请求发送给本地的域名服务器(即本文中的开放递归服务器);

2)当本地的域名服务器收到请求后,先查询本地的缓存,如果有该记录项,则本地的域名服务器直接将查询的结果返回;

3)如果本地的缓存中没有该记录,则本地域名服务器将请求发给根域名服务器,根域名服务器再返回给本地域名服务器一个查询域(根的子域,如CN)的顶级域名服务器的地址;

4)本地服务器再向查询返回的域名服务器(权威服务器)发送请求,收到该请求的服务器查询其数据库,并返回与此请求所对应的资源记录(下级域名服务器的地址或者域名所对应的IP地址等,返回不存在信息),本地域名服务器将返回的结果(该结果也包括不存在信息)保存到缓存;

5)重复4),直到找到正确的纪录;

6)本地域名服务器把返回的结果保存到缓存,以备下一次使用,同时将结果返回给客户机。

图3是经过设计之后的DNS解析。为了达到测量目的,需要绕开正常的DNS解析流程。根据DNS数据缓存原理,设计了如下查询逻辑步骤。

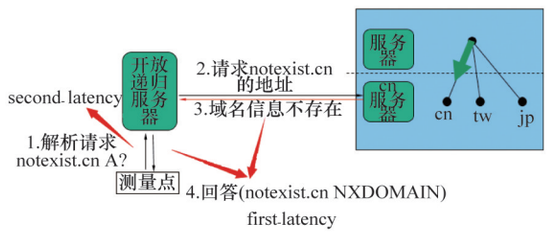

图3 设计之后的DNS解析

Fig. 3 DNS work process after redesigning

1)测量点询问CN的NS信息,并将该请求发送给开放递归服务器,该过程按正常的解析流程(详细过程略),目的是将CN的NS信息放入开放递归缓存。

2)测量点询问一个不存在的CN域名的A记录,并将该请求发送给开放递归服务器,经过步骤1)之后,开放递归中有CN的缓存,直接向CN服务器发起查询,CN服务器返回域名不存在信息,递归将该信息缓存,此时所得到的查询时间即为first_latency,记为t_1。

3)测量点再次询问步骤2)中构造的不存在的CN域名的A记录,并将该请求发送给开放递归服务器;经步骤1)后,递归已经知道该域名不存在,不再向CN服务器发起查询,直接返回不存在信息,此时所得到的查询时间即为second_latency,记为t_2。实现上述查询逻辑的操作步骤为:

(1)构造查询,使CN的权威信息都在递归缓存里。

(2)执行查询(该查询循环3次)。① 构造一个不存在的域名[notexist].cn。② 向递归查询该域名A记录。③ 记录响应时间t_1。④ 向递归查询该域名A记录。⑤ 记录响应时间t_2。⑥ 如果两次查询都成功,记录递归IP、域名、t_1、t_2。

在第1次查询之前,先通过开放递归查询CN的服务器信息,使递归缓存该信息,该缓存信息会保留1天(CN的TTL时间),确保开放递归直接查询CN服务器;第2次查询,由于CN的否定缓存时间为6 h,所以在第1次查询该域名后,域名不存在的信息将会保留在缓存,确保该信息直接从递归返回,第2次查询时,递归直接将该信息返回给用户。

2 数据分析

2.1 数据预处理

经过数据采集得到每个递归的3条数据,共1190802条记录,413646个开放递归,依次做如下处理:

1)过滤掉无效数据(主要是指$t_1<t_2$的数据,共110904条记录),由于网络的瞬时抖动或者丢包,会产生此类数据,经过此步骤后,有效数据共1079898,对应着405774个开放递归;

2)数据聚合,从递归的3条数据中选择时延的中值,每个递归只保留一条结果数据;

3)关联IP地理库信息,获得开放递归的洲、国家、省份(国内递归)3个层次的信息。

2.2　不同维度的数据分析

在预处理基础上,计算洲、国家、省份(国内递归)3个层次的时延数据,同上分析,每次数据聚合时,选择数据的中值作为最终结果。

1) 图4为各大洲CN解析时延分布,通过数据可知欧洲的整体时延(57.5 ms)最好,非洲、南美洲和大洋洲的整体时延都超过200 ms,分别为241、226和258 ms,这是因为CN在上述3大洲目前没有部署节点,来自这些地区的用户查询会路由到离其最近的其他洲节点。

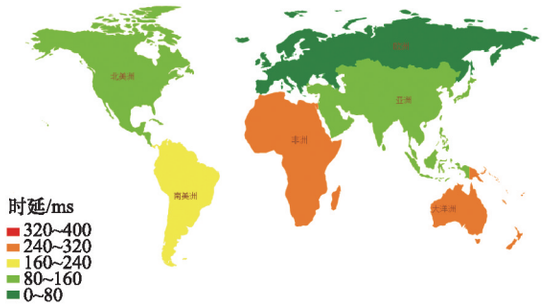

图4　各大洲CN解析时延分布

Fig. 4　Continents CN domain name resolution latency

2) 图5是世界各国(地区)CN解析时延分布,整体时延最好的国家(地区)为中国香港(8 ms)和韩国(11 ms),中国大陆地区的总体时延为44 ms。

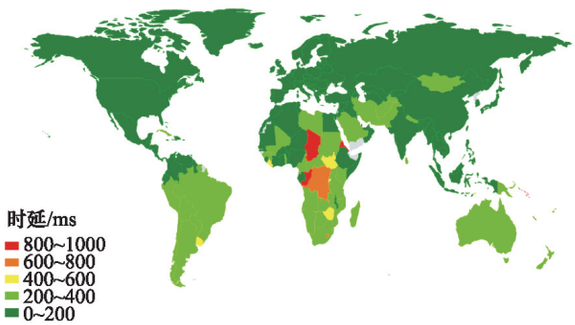

图5　各国家(地区)CN解析时延分布

Fig. 5　Counties(regions)CN domain name resolution latency

总体来看,CN权威服务在各国的访问时延,有32%的国家(地区)小于100 ms,69%在200 ms以内,低于500 ms的国家(地区)为96%。

3) 图6为中国CN解析时延分布,整体时延最好的为香港和澳门,分别为8和19 ms。统计显示,97%的省、自治区、直辖市时延都在100 ms以内。

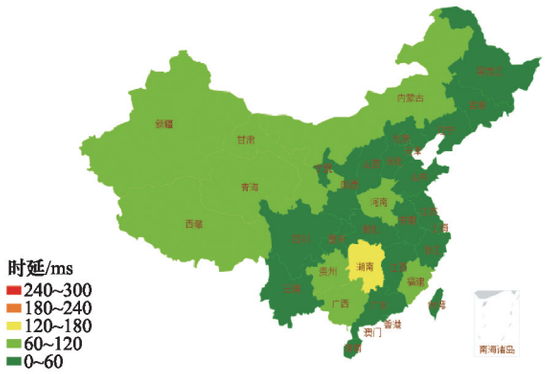

图6　中国CN解析时延分布

Fig. 6　Domestic CN domain name resolution latency

3　网民分布

根据Internet World Stats上的数据显示,截至2013年底,全球各大洲的网民分布及各个洲的网民比见表3,表3中第4列为CN节点在各大洲部署比例。

表3　各大洲网民信息统计

Table 3　Netizen information of different continents

洲名	网民数	网民比/%	CN节点比/%
北美洲	379959365	14.1	14.3
南美洲	222334228	8.2	—
非洲	240146482	8.9	—
亚洲	1265143702	46.9	71.4
欧洲	566261317	20.1	14.3
大洋洲	24804226	0.9	—

从整体上看,CN节点部署在网民比较多的北美、亚洲和欧洲,策略是正确的。特别是使中国网民享受到了更加优质的CN解析服务。同时,从上述分析中也可以看到,虽然在南美、非洲和大洋洲没有部署节点,但这些地区的用户也能享受到相对较好的CN解析服务(200~300 ms时延)。如果想要进一步提升CN在全球整体服务质量,建议在这3个大洲部署CN节点。

4　结论

研究了一种基于主动测量评估CN权威服务选址效果的方法,通过该方法可以看到CN权威服务目前能为全球各地都提供较好的解析服务,但服务效果还存在地理上的差异性。在欧洲、亚洲、北美洲的使用体验要强于非洲、南美洲和大洋洲,这与CN节点的部署实际情况相符。CN作为国家顶级域,也特别考虑了中国用户的使用体验,中国各省、直辖市、自治区都能享受到非常流畅的解析服务。

通过实测法从最终的解析效果分析节点部署,该方法可以用来辅助节点部署的决策判断,循序渐进,逐步调整节点的数量和地点。

参考文献(References)

[1] Mopetckaris P. Request for coments 1034: Domain names-concepts and facilities[S]. Washington DC: The Internet Engineering Task Force, 1987.

[2] Hardie T. Request for coments 3258: Distributing authoritative name servers via shared uni-cast addresses[S]. Washington DC: The Internet Engineering Task Force, 2002.

[3] 王伟, 李晓东, 孙国念. 域名镜像服务器部署分析[J]. 计算机工程与应用, 2008, 44(7): 161-163.
Wang Wei, Li Xiaodong, Sun Guonian. Analysis of DNS mirror server [J]. Computer Engineering and Application, 2008, 44(7): 161-163.

[4] Sarat S, Pappas V, Terzis A. On the use of anycast in DNS[C]// Proceedings of 15th International Conference on Computer Communications and Networks. Arlington Virginia: IEEE Xplore, 2006: 71-78.

[5] 邓光青, 孔宁, 王胜开, 等. 一种基于网络测量的DNS节点选址方法: 中国, 103491202A[P]. 2015-03-23.
Deng Guangqing, Kong Ning, Wang Shengkai, et al. A solution of DNS node selection based on network detection: CN, 103491202A[P]. 2015-03-23.

[6] Liang J J, Jiang J, Duan H X, et al. Measuring query latency of top level DNS servers [C]//Proceedings of 14th Passive and Active Measurement Conference. Hong Kong: Lecture Notes in Computer Science, 2013, 7799: 145-154.

[7] 王垚, 胡铭曾, 云晓春, 等. DNS权威名字服务器性能与安全性的研究[J]. 通信学报, 2006, 27(2): 147-152.
Wang Yao, Hu Mingzeng, Yun Xiaochun, et al. Research on DNS authoritative server's performance and security[J]. Journal on Commuication, 2006, 27(2): 147-152.

[8] 胡鹏. DNS服务质量评价模型研究[D]. 哈尔滨: 哈尔滨工业大学, 2012.
Hu Peng. Research on the evaluation model of the service quality of DNS[D]. Harbin: Harbin Institute of Technology, 2012.

[9] 杜跃进, 张兆心, 王克, 等. 基于用户感知的DNS解析网络性能测量技术[J]. 南京航空航天大学学报, 2013, 45(1): 110-115.
Du Yuejin, Zhang Zhaoxin, Wang Ke, et al. Performance measurement technology of DNS resolution network based on user perception[J]. Journal of Nanjing University of Aeronautics & Astronautics, 2013, 45 (1): 110-115.

[10] Georgios Kambourakis, Tassos Moschos, Dimitris Geneiatakis, et al. Etecting DNS amplification attacks[C]// Proceedings of Critical Information Infrastructures Security, CRITIS 2007. Málaga, Spain: Lecture Notes in Computer Science, 2008, 5141: 185-196.

[11] Peter Eckersley, Jesse Burns. An observatory for the SSLiverse[R/OL]. [2010-07-10]. https://www.eff.org/files/defconssliverse.pdf

(责任编辑 赵业玲)

·学术动态·

中国科学技术协会

第17届中国科协年会举办女科学家高层论坛

2015年5月22日,第17届中国科协年会举办主题为"科技女性与创新驱动发展"的女科学家高层论坛,中国科协副主席、中国科协常委会女科技工作者专门委员会主任、协会常务副会长程东红主持开幕式并致辞,十一届全国政协副主席、中国女科技工作者协会会长、中国科学院院士王志珍出席论坛并作总结发言,300位来自科研院所、高等院校、企业的女科技工作者和女大学生代表参加论坛。

论坛特邀报告由专委会委员、协会副会长、国家自然科学基金委副主任高瑞平主持。全国人大常委、专委会副主任、协会常务副会长、中国科学院党组副书记方新作"适应新常态,强化新动力"的主旨报告,中国工程院副院长陈左宁、中国科学院宁波材料技术与工程研究所所长崔平、联想集团高级副总裁乔健、广东大华农动物保健品股份有限公司总裁兼科研首席陈瑞爱4位优秀女科学家、女企业家代表,分别作题为"大数据时代下的智慧计算"、"科研成果转化的挑战与应战"、"国际化——联想一小步,中国一大步"、"发挥产学研力量,为驱动创新助力"的专题报告。

详见中国科协网http://www.cast.org.cn/n35081/n35096/n10225918/16405221.html。