doi:10.3969/j.issn.1000-1247.2016.01.015

基于旁路抢答机制的异网DNS管控实践

巫俊峰[1] 沈 瀚[2]
1.中国移动通信集团江苏有限公司
2.中国移动通信集团江苏有限公司无锡分公司

摘要 ISP网络存在着一定比例的异网DNS流量，不仅会降低用户上网体验，带来安全风险，而且对中小ISP而言提高了流量结算成本。对异网DNS的产生来源、DNS管控技术进行分析后，最终选择基于旁路抢答机制的异网DNS重定向系统进行部署，该实践为ISP合理管控宽带用户终端发出的DNS请求流量提供参考。

关键词 重定向 DNS管控 DNS劫持 外网DNS

1 异网DNS现状分析

DNS是互联网的入口，DNS请求发生在用户访问互联网的第一环节，ICP内容资源、CDN等都依赖于DNS的正确调度才能将用户流量引导到最合适的资源节点。正常情况下用户终端应该使用ISP分配的官方DNS，然而用户终端设置的DNS由用户自身决定，不处于ISP可控范围。现网流量监测系统发现ISP网络存在着一定比例的异网DNS流量，配置不合适的异网DNS不仅会降低用户上网体验，带来安全风险，对中小ISP而言还提高了流量结算成本。如何选择一种最优的技术方案，对异网DNS流量进行有效管控，实现资源调度的优化，是文中重点论述的问题。

1.1 异网DNS来源和影响分析

异网DNS流量的主要来源如下。

- 策反转网的用户未修改DNS配置：专线用户情况尤为突出，用户由于缺乏专业网管技术人员，转网时只调通网络，而不重视配置调优，转网后仍使用原运营商的DNS，常常在报障网速慢后才发现DNS配置错误。
- 用户自主修改DNS：第三方公众DNS借助网络广泛宣传，部分用户盲目迷信网上教程，手工修改路由器或本机的DNS配置为谷歌DNS 8.8.8.8、114 DNS等公众DNS，造成内容资源访问时“舍近求远”，难以实现本网已引入资源的精准调度。
- 用户被动修改DNS：部分互联网公司借助终端软件积极推行自己的DNS，用户在不知情的情况下，DNS被一些声称能优化网络和修复网络的软件所修改，如360 DNS优选、腾讯DNS优选等。
- 用户DNS被黑客劫持：黑客利用路由器存在弱口令、安全漏洞、恶意代码等将用户路由器或终端电脑上的DNS篡改为黑客所控制的非法DNS。当不知情的用户使用非法DNS访问网上银行或购物网站等敏感网站时，可能被指向假冒的欺诈网页，造成信息泄露和重大损失。
- 某些互联网产品在出厂时内置了DNS：如各类电视盒子、免费Wi-Fi等设备可能内置了公共DNS。

以上原因导致了异网DNS的存在，而使用不合理的异网DNS进行域名解析，会造成解析时间长、解析成功率降低、调度准确性降低等诸多问题，甚至带来安全风险。

1.2 异网DNS的流量占比

现网监测数据表明城域网中有10%～15%的DNS递归请求去往异网DNS，而异网DNS流量中谷歌DNS又占据着较大份额。

1.3 异网DNS管控目标

逐个通知客户变更DNS是一项棘手而低效的工作，迫切需要有一种技术手段，能将流向异网DNS的请求重新引导回ISP官方DNS，实现异网DNS请求的网内解析，达到如下的管控目标：

- 对异网DNS（不可信DNS）的解析请求返回ISP官方DNS的最佳解析结果，实现DNS请求100%可管控；
- 所有操作和处理过程均在用户无感知和不影响使用的情况下完成；
- 可实现调度策略的灵活配置，能针对具体用户IP和DNS进行定向调度；

• 优化用户体验，降低安全风险的同时，缩减网间流量结算成本。

2 异网DNS管控技术探讨

2.1 路由牵引方式

路由牵引方式首先需要获知异网DNS的IP地址，再通过路由发布的方式将这些IP指定ISP官方DNS，用户访问这些特定IP的DNS请求将被牵引至运营商DNS，从而实现对异网DNS流量的拦截。

优势：部署快，现网无需新增设备投资和调整网络。

劣势：仅能覆盖已知的异网DNS，未知DNS不能覆盖，存在路由广播合法性风险。

2.2 旁路抢答方式（分光镜像+抢先应答）

通过分光镜像方式采集53端口的DNS请求给重定向系统，针对流向异网DNS的递归请求，由DNS重定向系统伪装异网DNS，以抢先应答方式返回本地DNS的网内解析结果。

如图1所示，在ISP出口通过镜像或分光方式采集DNS请求，送给“DNS重定向安全装置”，由“DNS重定向安全装置”从DNS报文中提取DNS服务器地址，针对用户终端发出的DNS请求报文，根据事先定义的DNS服务器白名单进行逻辑决策，如果DNS服务器地址不是白名单之内的异网DNS，去往该异网DNS的所有域名请求通过Forward机制重新引导回ISP 官方DNS，“DNS重定向安全装置”获得解析结果后，立刻构造一个新的DNS响应报文，改用用户请求的异网DNS服务器地址作为源IP，以抢先应答方式回复用户；而去往白名单的本网及可信DNS请求不做任何处理，直接放行。“DNS重定向安全装置”有类似缓存的功能，可以存储本网DNS的解析结果。所以在系统稳定运行后可以进行微秒级响应，在用户配置的异网DNS之前优先返回给用户解析结果，用户会自动抛弃后收到的DNS响应。

优势：可以覆盖所有异网DNS流量，无单点故障隐患。

缺点：需要新增设备投资，隐蔽性稍差，用户收到两份DNS应答。

2.3 PBR策略路由方式

在ISP出口设备配置策略路由，将53端口流量策略路由至网内，指向专门部署的DNS重定向系统，DNS重定向系统向ISP官方DNS发起解析请求并获取到解析结果，最后由DNS重定向系统把结果返回给用户。DNS重定向系统在返回给用户的应答报文中，使用用户请求报文的目的地址作为源地址，实现异网DNS无感知优化，处理流程如图2所示。

优势：可以覆盖所有异网DNS流量，隐蔽性强，DNS调度优化成功率高。

缺点：省网网络设备要配置策略路由，策略复杂，需要新增设备投资，DNS重定向系统串接在网络中，存在单点故障。

2.4 三种异网DNS管控技术比较

三种异网DNS管控技术比较见表1。

综合以上方案，推荐采用旁路抢答方式作为首选部署方案。

3 旁路抢答DNS重定向系统的部署实施

2014年4月起联合南京信风公司在江苏无锡城域网进行了试点测试，借助无锡城域网两台核心设备上行链路中已经

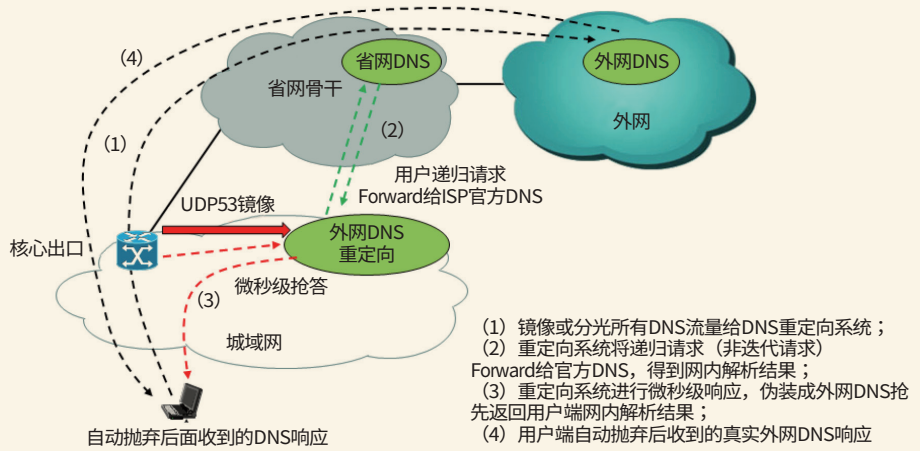

图1 DNS流量复制+抢先应答方式

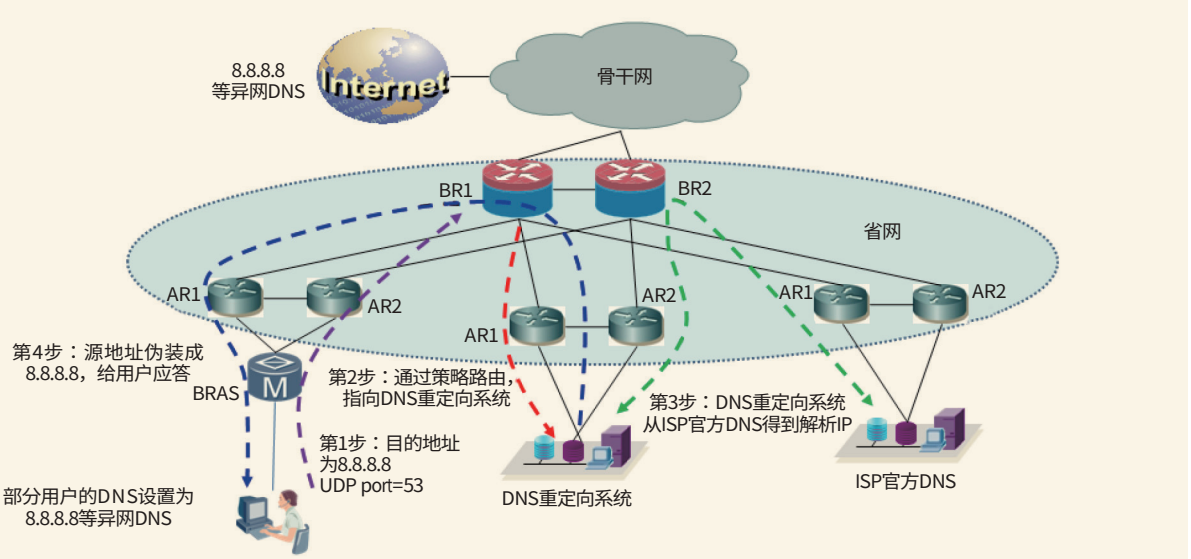

图2　PBR策略路由方式

表1　三种异网DNS管控技术比较

异网DNS管控技术	优点	缺点	是否推荐
路由牵引	部署灵活方便，无需设备投资	仅能覆盖已知的DNS，需要收集TOP异网DNS地址，存在路由广播合法性风险	—
旁路抢答	旁挂方式，无单点故障隐患	需要新增设备投资，隐蔽性稍差	推荐
策略路由	串接方式，劫持成功率最高，且隐蔽性强	需要新增设备投资，策略路由造成策略复杂，DNS重定向系统存在单点故障隐患	—

表2　DNS重定向系统配置

序号	项目	描 述	数量
一	系统硬件平台		
1	DNS重定向前置采集机	ProLiant DL380 G6 服务器 核心配置； 2个4核心Intel Xeon CPU E5504 2.00GHz； 32GB EEC内存； 5个千兆Intel网卡	1
2	DNS重定向网管服务器	普通PC 服务器，安装Linux	1
二	系统软件平台		
1	应用软件	信风DNS重定向系统软件v1.0	1

部署过的DPI系统，提取出53端口的DNS流量，复制给DNS重定向系统。

3.1 DNS重定向系统配置

DNS重定向系统配置见表2。

以上信风公司服务器配置可支持50万QPS处理能力。

3.2 DNS重定向安全装置功能模块及处理流程

经过不断测试改良，完善的“DNS重定向安全装置”应包括如下功能模块。

(1)接收解析模块

接收通过镜像或分光方式复制过来的DNS流量，从DNS报文中解析出DNS 服务器地址、用户请求源IP、用户请求域名、是用户终端发出的递归请求还是DNS服务器发出的迭代请求。

(2)判断模块

仅处理用户终端发出的递归请求，不处理DNS服务器发出的迭代请求。

再根据内置的规则先判断DNS 服务器地址是否是可信地址，再判读用户请求源IP是否属于直接放行地址。

系统将DNS服务器分为可信DNS（或称合法DNS）和非可信DNS两类。DNS服务器白名单中的都是可信DNS，包括ISP自建的本地DNS、ISP认可组织内部DNS等，白名单的描述形式可以是多个IP地址段的集合。发往DNS白名单的解析请求直接放行。

非可信DNS是不在DNS白名单中的所有其他DNS，默认为异网所有的DNS。发往非可信DNS的解析请求原则上都将被转发处理模块处理，除非源IP属于请求源IP白名单。

为满足用户实际需要，还应设定DNS请求源IP白名单，这些源IP发起的请求不管DNS 服务器地址可信或非可信，都将采取直接放行策略。

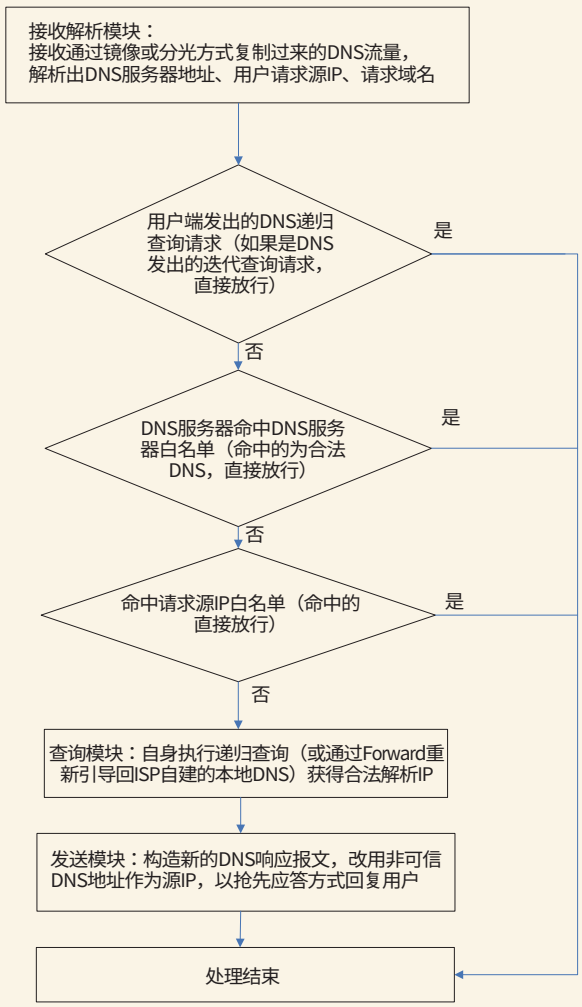

图3　DNS重定向安全装置业务流程

(3)查询模块

针对没有命中DNS白名单或没有命中DNS请求源IP白名单的解析请求，将通过自身迭代查询以获取域名数据对应的IP地址（也可以通过Forward机制转发给ISP自建的可信本地DNS以加快查询速度）。

(4)DNS缓存模块

可以存储热点域名的解析结果，进行微秒级响应。

(5)发送模块

从ISP自建的本地DNS获得解析结果后，立刻构造一个新的DNS响应报文，改用非可信DNS服务器地址作为源IP，以抢先应答方式回复用户。

相应的业务流程如图3所示。

4 DNS重定向系统的应用效果

无锡移动部署异网DNS重定向系统后，成功地将流向异网DNS的请求重定向回本省官方DNS。监控数据显示，城域网中原有13%到异网DNS的请求，全部被DNS重定向系统Forward给省内官方DNS，DNS流量得到百分之百管控。

```
[root@CZ-DNS ~]# dig @8.8.8.8 www.youku.com

; <<>> DiG 9.9.4 <<>> @8.8.8.8 www.youku.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 53154
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 512
;; QUESTION SECTION:
;www.youku.com.                 IN      A

;; ANSWER SECTION:
www.youku.com.          186     IN      CNAME   qd-w.youku.com.
qd-w.youku.com.         3486    IN      A       119.167.145.19

;; Query time: 40 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Mon Jun 16 19:08:32 CST 2014
;; MSG SIZE  rcvd: 77
```

青岛联通

图4　未使用DNS重定向前

```
[root@CZ-DNS ~]# dig @8.8.8.8 www.youku.com

; <<>> DiG 9.9.4 <<>> @8.8.8.8 www.youku.com
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59660
;; flags: qr rd ra; QUERY: 1, ANSWER: 2, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.youku.com.                 IN      A

;; ANSWER SECTION:
www.youku.com.          2064    IN      CNAME   mob-w.youku.com.
mob-w.youku.com.        44      IN      A       221.181.195.121

;; Query time: 0 msec
;; SERVER: 8.8.8.8#53(8.8.8.8)
;; WHEN: Mon Jun 16 19:08:35 CST 2014
;; MSG SIZE  rcvd: 78
```

常州移动

图5　使用DNS重定向后

4.1 质量角度评估

基于DNS旁路抢答的DNS重定向系统提升了现有流量调度系统的有效性，不管用户使用什么DNS，都能将解析结果自动修正指向到网内资源，并且DNS解析响应时间大大降低，试点地市再未接到集团用户因配置异网DNS而引发的网络慢类投诉。

www.youku.com资源已经引入移动网内，没有使用DNS重定向系统前，如图4所示，谷歌DNS 8.8.8.8将www.youku.com错误调度至网外的青岛联通IP 119.167.145.19，DNS解析时延高达40ms。

使用DNS重定向系统后，如图5所示，谷歌DNS 8.8.8.8的解析结果被纠正为无锡移动网内地址221.181.195.121，DNS解析时延由40ms下降到1ms。

据拨测系统统计，DNS重定向优化后，热点网页打开时间比优化前缩短了39%。

4.2 成本角度评估

异网流量下降明显，监控数据显示，对原来那些设

（下转74页）

4 平台性能指标

为了保证平台能够安全稳定地满足当前使用，同时又可支持未来业务灵活拓展，因此，平台基于如下性能指标进行严格设计。

平台无关性：系统采用纯Java技术构建，由于Java本身与平台无关，系统也与平台无关。

系统易用性：系统采用BS、CS相结合的方式设计，针对不同用户群的使用要求提供不同的登录方式。以用例驱动人机界面设计，界面设计遵守三次点击的原则，支持多用户、多客户端并发操作，同时支持Web和Application两种方式的客户端。

可靠性：系统保证7×24h不间断工作；系统无单点故障；具有对硬件、软件运行状态的远程监控和管理能力；应用软件具备容错能力，软件故障不会引起各类严重的系统再启动。

系统可控性：系统提供对自身运行状态的监控与管理，包括对系统中的基础设备（包括主机、网络设备、存储设备）、基础软件（如数据库、中间件）和系统内部进程的监控，系统对内部各监控对象提供实时查看、故障告警、控制操作功能。

系统开放性、可扩展性：系统可以通过WebService、Java RMI/JNDI、HTTP、Corba等技术向上提供满足规范的北向接口；系统提供不同的接口，实现与其他系统的互联互通。

5 结束语

在技术方面，整合全网数据，并进行跨地域、跨行业的综合挖掘分析；在分布式计算、存储等方面，针对超大规模数据管理与应用，解决了大量的技术问题。此外，构建科学有效的系统架构，支撑采集数据分区域预处理、传输汇聚、存储、挖掘以及输出有效分析结果等。

在应用方面，主要面向互联网数据中心提供互联网行为分析，基于超大规模IDC流量数据，实现全网级的行为检测与应用分析。目前行业内的互联网行为分析主要是针对具体应用，在较小的具体局域网范围内，针对具体应用进行分析。相比之下，以上提及的产品在服务对象的广度、深度等方面是一个大胆的尝试和创新。

此外，根据数据本身的特点，结合经典物理和量子物理，提出经典数据（Classic Data）和量子数据（Quantum Data）的概念，具有一定的借鉴意义。

参考文献

[1] 李强，王宏，王乐春.基于P2P的分布式网络管理模型研究[J].计算机工程，2006，32(13)

[2] Stefan C，Andreas B，Matthias S，*et al*.A self—organizing concept for distributed end—to—end quality monitoring[D].University of Wurzburg Institute，Wurzburg，Germany，2006

[3] 张立明.网络用户行为分析系统研究与设计[D].北京：北京邮电大学，2011

[4] 简清明.基于Winpcap库的通用程序设计模型[J].计算机系统应用，2007(2)

如对本文内容有任何观点或评论，请发E-mail至ttm@bjxintong.com.cn。

作者简介

刘化召

硕士，现就职于中通服软件科技有限公司，高级工程师，主要研究方向为计算机通信、BOSS 研发与应用。

（上接74页）

置为异网DNS的用户而言，其流量本网率从92.81%上升到98.83%，其异网流量下降约6个百分点，达到了正确引导用户访问本网资源的预期效果。

4.3 安全角度评估

重定向系统屏蔽了黑客DNS，用户信息安全风险降低。

5 结束语

基于DNS旁路抢答的异网DNS重定向系统，可让ISP合理管控域域网宽带用户终端发出的DNS请求流量，使用合法DNS以抢先应答的方式代替非可信DNS来回复用户解析请求，规避黑客DNS给用户带来的安全风险，有效提升了流量调度系统的准确性，降低了运营商的流量结算成本。

本技术方案能覆盖所有终端用户，不局限操作系统和设备类型，也不需要用户手工干涉，在用户无感知的情况下保护了域名数据安全，已经被申请为专利，对宽带电信运营商具有普遍适用性和推广价值。

参考文献

[1] 孔政，姜秀柱.DNS欺骗原理及其防御方案[J].计算机工程，2010(2)

如对本文内容有任何观点或评论，请发E-mail至ttm@bjxintong.com.cn。

作者简介

巫俊峰

硕士，现就职于江苏移动，高级工程师。

沈瀚

硕士，现就职于无锡移动，工程师。