

一种基于域名错误的 DNS 重定向协议^①

王艳峰 王 正 阎保平 (中国互联网络信息中心 中国科学院计算机网络信息中心 北京 100190;
中国科学院研究生院 北京 100049)

摘要: 域名系统(DNS)重定向是为互联网服务提供商(ISP)和 DNS 应用服务提供商(ASP)的用户实现增值服务的的功能。定义以不同于错误查询域名的按相关性排序的推荐域名列表作为错误描述。提出重定向服务器的两个转交过程,以利于正确及时地找到推荐域名。此外,提出使用延长资源记录请求的处理算法。定义重定向报文结构以在 DNS 协议内容纳重定向 IP 地址信息。

关键词: 域名系统; DNS 重定向; 域名错误; 资源记录

ADNS Redirect Protocol for Domain Name Errors

WANG Yan-Feng, WANG Zheng, YAN Bao-Ping

(China Internet Network Information Center; Computer Network Information Center, Chinese Academy of Sciences, Beijing 100190, China; Graduate School, Chinese Academy of Sciences, Beijing 100049, China)

Abstract: Domain name system (DNS) redirect is expected to be the emerging functionality to perform a value added services for users by the Internet Service Providers (ISP) and the DNS Application Service Providers (ASP). This paper specifies the error description as the list of suggested domain names other than the original one, which are sorted by their relevance. Two handover processes for the redirected server is proposed, which can facilitate finding the suggested domain names both correctly and timely. Besides, the request handling algorithm is proposed using the prolonged resource records. The message structure of the redirect is defined to accommodate the redirect IP information in the DNS protocol.

Keywords: domain name system; DNS redirect; domain name error; resource record

1 背景

域名系统(DNS)是当今互联网的基础设施^[1-3],完成主机名到 IP 地址的映射,从而建立起网络使用者和互联网路由系统的关键连接。

作为一种全球服务,除了具有高度的可扩展性和保证高负载下的较好性能外,人们期望 DNS 能够面向互联网服务提供商(ISP)和 DNS 应用服务提供商(ASP)的用户需求,提供一些附加的增强服务。这些增强服务可以通过 DNS 重定向来实现,并且这些服务通常是用户可选的。DNS 重定向可以为用户提供多种增值服务,例如解释 web 地址错误,防止用户接触到一些含有恶意代码的域名所在的网址等等。

虽然 DNS 重定向的实现方式有多种,但 T. Creighton 等^[4]建议基于 DNS 递归服务器来实现,这样做的好处是实现代价较小,且容易与现有的 DNS 协议兼容,因此本文的协议也采用 DNS 递归服务器来实现。

DNS 递归服务器负责处理客户端发送的 DNS 查询报文,向权威服务器发送查询请求,获取域名对应的 IP 地址(表示为资源记录的形式)。这些资源记录同时缓存在递归服务器,直至生存时间(TTL)过期。递归服务器通常由 ISP 提供。

DNS 重定向系统对 DNS 协议增加的主要实体是 web 错误处理服务器。当 DNS 递归服务器收到 NXDOMAIN 应答时,用户将被重定向到 web 错误处理服务器,由

① 基金项目:国家发改委 CNGI 项目(CNGI-09-03-04);中科院知识创新项目(081 408 1105);中科院计算机网络信息中心青年基金(CNIC_QN_08006)
收稿时间:2009-10-05;收到修改稿时间:2009-12-01

后者返回给用户的 web 页面的内容可能包含域名错误的多种信息,不同的 ISP 和 DNS ASP 可能有所不同。域名错误信息可以是用户应该收到的域名错误的描述信息,也可以是与错误域名相似的 URL 的链接或搜索页面等等不一而足。

本文的协议定义域名错误的描述信息为不同于原始查询域名的推荐域名的列表,并且以域名的相关度排序。这种定义可以满足用户最常见的对于错误域名处理的需求,这里我们把完成这种功能的 web 错误处理服务器称为重定向服务器。

本文的 DNS 重定向协议提出重定向服务器的两种转交过程,有利于准确及时地找到推荐域名。此外,我们提出使用延长的资源记录的查询处理算法。我们还定义重定向的报文结构,可以在现有的 DNS 协议框架内容纳重定向 IP 信息。

2 DNS重定向协议

2.1 DNS 重定向协议概述

图 1 显示了 web 错误重定向的流程。首先,用户主机向递归服务器发送一个查询不可用域名 IP 地址的请求,如 `www.example.invalid`。如果递归服务器在缓存中找不到域名所对应的 NXDOMAIN 否定缓存(不存在的域名),就向域名的权威服务器发送查询请求,同时把本查询转交给重定向服务器,即 web 错误处理服务器。这一转交是必要的,因为当用户主机按后来的重定向请求重定向服务器时,请求中可能不包含最初查询的域名。例如,用户主机可能只用相对地址来请求服务器的某种资源。如果重定向服务器不知道查询域名,就不能提供一个推荐域名的列表而只是一个单纯的指示错误页面。这种请求转交的另一个目的是让重定向服务器的预处理查询成为可能,因此可以节省错误信息的响应时间。虽然在 NXDOMAIN 应答转交后,重定向服务器再进行错误处理,同样可以完成重定向,这种预处理却能够使用户感受到的域名解析延迟最小,而不至于由于重定向处理而付出过大的延迟代价。详细的查询请求算法将在第 1.2 节说明。查询请求算法的主要目的是利用延长的资源记录找到对用户最有用的候选域名。资源记录的延长机制将在第 1.3 节说明。对于错误的域名,权威服务器会向递归服务器返回一个 NXDOMAIN 的应答。递归服务器首先把这个应答转交给重定向服务器,并把不同于

NXDOMAIN 的重定向 IP 地址返回给用户主机。含有重定向 IP 地址的 DNS 报文结构将在第 1.4 节说明。在这第二次转交后,重定向服务器可能会根据权威服务器的应答对可能已经计算出来的推荐域名作出相应的修改。这种修改主要由两种原因造成:一是缓存的资源记录可能与 NXDOMAIN 的应答不一致;二是对查询的域名没有任何相关的缓存资源记录。主机通过重定向 IP 地址请求重定向服务器,重定向服务器返回处理的应答。以上就是 web 错误重定向的处理流程。

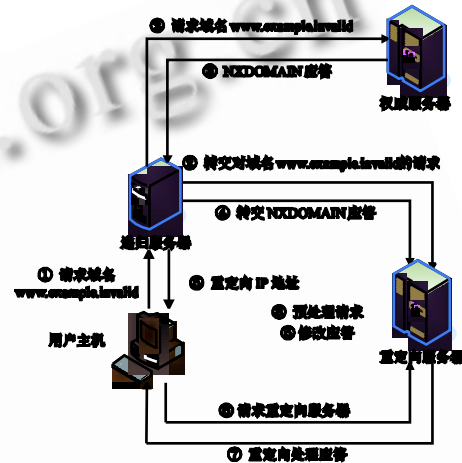


图 1 Web 错误重定向处理流程

2.2 错误处理算法

错误处理算法的主要思想是对于不存在的域名,找到用户主机真实意图查询域名所对应的资源记录集合。这里我们利用两种相关性的衡量标准。第一是域名拼写的相似度,第二是域名的流行度。我们从递归、根、CN 顶级域名服务器的 DNS 日志中发现,人为的拼写错误是域名错误的主要来源之一。例如用户本意查询的域名是“`www.example.com`”,却错误地在浏览器的地址栏中输入了“`www.example.com`”。因此查询的不存在域名和其它域名的拼写相似度是表征域名相关性的重要标准之一。我们需要考虑的另一个重要因素是域名的流行度。对递归服务器日志的统计分析表明,域名的查询频率体现出一种类 zipf 分布(如图 2 所示,在 $\log\text{-}\log$ 坐标下为近似线性关系)^[5]。这表明域名流行度的分布是极不均衡的,大量的查询集中在热点域名上。因此对于与错误查询域名同样拼写相似度的域名来说,较流行的域名相关度排名应较高,为此次用户真实查询域名的可能性更大。对于候选域名的总体评价,应该在拼写相似度和流行度之间有一

个均衡,其中一种最简单的方式是加权:

$$\text{Score} = \text{likelihood} + \alpha * \text{popularity} \quad (1)$$

这里 α 是加权因子。

为了计算式(1)右半部分的流行度,重定向服务器应该记录所有转交给它的域名,按访问频率进行排序,然后计算得到相对流行度。对于式(1)右半部分的拼写相似度,近年来有多种算法被提出[6-8]。

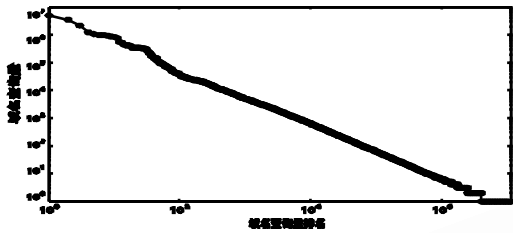


图2 双对数坐标下域名查询量分布

错误处理算法所有使用的域名均包含于重定向服务器所保存的资源记录中。这些资源记录来自于递归服务器转交的权威服务器应答,以延长的TTL缓存,可以分为两种类型:否定资源记录(表示不存在的域名)和肯定资源记录(表示正确域名)。当重定向服务器收到转交的请求后,首先查找否定资源记录。由于候选存在域名的相关度评价很耗时,我们为不同类型的请求赋予不同的优先级以提高处理效率,高优先级在低优先级之前处理。我们把查询请求分为五类,对应五种优先级。

①如果重定向服务器从收到的第二次转交的应答中发现某域名实际不存在,则如果此域名尚未处理或未完成处理,则应立即赋予最高的优先级。

②如果重定向服务器发现请求在缓存的否定资源记录中命中,这个域名很可能是错误的(由后来的转交应答验证),因此这种类型的请求具有次高的优先级。

③对于那些否定和肯定缓存均没有命中的请求,可以被看作是未决的(暂时难以确定域名是否存在),因此赋予中等优先级。

④某些请求命中了肯定缓存,这表明它们很可能就是实际存在的域名,对于实际存在的域名不需要重定向服务器处理,因此这种类型的请求具有次低的优先级。

⑤如果重定向服务器从收到的第二次转交的应答中发现某域名实际存在,则如果此域名尚未处理或未完成处理,则应立即从等待处理队列中删除。

通过这种分优先级的处理,错误概率最高的域名被优先处理,可以达到优化系统资源的目的,从而保证重定向服务器完成任务的时间效率。

这种基于优先级的处理可能中止于第二次转交。优先级2、3和4实际上都是基于对域名是否真实存在的预测进行的优先级别定级。当收到第二次转交的权威服务器应答时,这种预测将完成验证。如果此应答为肯定应答,而对于这个请求域名的优先级2、3和4的处理尚未结束,则应把它移入优先级5,即处理中止。因为肯定应答表明此域名实际上是存在的,继续处理是没有必要的。反之,如果此应答为否定应答,而对于这个请求域名的优先级2、3和4的处理尚未结束,则应把它移入优先级1,即优先处理。因为否定应答表明此域名实际上是不存在的。

2.3 延长的资源记录

为了丰富重定向服务器推荐域名所使用的域名数据库,我们利用延长的资源记录。对于转交的权威服务器的应答,重定向服务器缓存应答中的资源记录,这与递归服务器的缓存类似。但根据DNS协议,递归服务器的缓存是基于资源记录中的生存期(TTL),当TTL过期时,资源记录应该从缓存中移除。TTL的长度从几秒到几个月不等,但大都是以小时为量级。特别地,否定缓存的TTL一般都比较短(由区域SOA记录的最小生存期字段决定)。因此,即使查询域名实际上是不存在的,之前缓存的否定应答也经常会上过期,因此缓存没有命中,导致本应是优先级2的域名落入了优先级3。我们的假定是,即使是过期的资源记录也能够提供对于域名存在性的有价值信息。换言之,不存在的域名在过期后仍有很大的概率仍然存在,而反之,存在的域名在过期后仍有很大的概率仍然存在。符合这种假定的实际作法是给缓存的资源记录延长其生存期。由于资源记录的占用空间很小,因此通常对它的缓存通常不受限于存储空间。作为资源记录数据库大小和查找空间的一个折衷,我们建议使用原始TTL的3-5倍作为重定向服务器缓存的TTL。

2.4 DNS重定向报文结构

本节我们说明采用何种报文来为用户主机提供重定向IP地址。尽管我们可以选择一种特定的通知报文或者其它的带外报文,但出于与DNS报文的兼容性考虑,我们设计在普通的DNS报文中容纳重定向IP地

址。这种方案的好处是不需要对现有的 DNS 协议作大的改动,从而易于在现有的 DNS 软件(如 BIND 等等)中扩展和实现。

当递归服务器收到 NXDOMAIN 的应答并且用户选择采用重定向服务时,递归服务器就构造含有重定向服务器 IP 地址的 DNS 报文,把它作为应答返回给用户主机。这种构造的重定向报文主要包含两个主要的改动和重新定义(如图 3 所示)。在权威部分,以 NS 资源记录的形式把不存在域名的 DNS 服务器填充为 NXDOMAIN。这将告知用户主机权威服务器返回的应答是 NXDOMAIN,同时这种形式由于不同于权威服务器返回的 NXDOMAIN 应答,因此也告诉用户主机这一报文是重定向报文。另一个改动是在回答部分以 A(如为 IPv6,则为 AAAA)资源记录的形式把重定向服务器的 IP 地址作为不存在域名的 IP 地址。

```
/* Authority section */
nxdomain.example.com. IN NS NXDOMAIN
/* Answer section */
nxdomain.example.com. IN A 102.20.20
```

图 3 DNS 重定向报文结构

3 实验结果

我们的系统实验环境为一个局域网,主机数量为 237。本地 DNS 递归服务器的原始软件为 BIND 9.2.3,修改 BIND 代码,增添了两次转交过程的处理。重定向服务器部署在本地。

基于一个月的递归服务器日志进行域名流行度的计算,定义域名流行度为域名在一个月内的日志内出现的次数除以域名查询总量,即域名出现的概率。拼写相似度的检查基于 CORRECT 软件^[7],其输出为候选域名的概率值。

当用户查询错误域名时,会根据重定向返回的推荐域名列表,选择下一次查询的域名,如果推荐域名列表中包含用户的所要查询的真实域名,则用户下一次查询的域名就会是这一列表中的域名。定义重定向命中率为推荐域名列表被选中的概率。令返回的域名列表的个数为 10,取不同的加权系数,实验时间长度都为自 8:00 开始的两天时间,得到的重定向命中率如图 4 所示。由图 4 可见,加权系数为 4 时,重定向命中率最大。

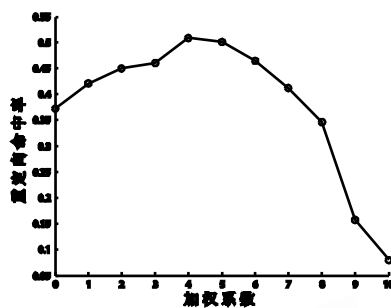


图 4 不同加权系数下的重定向命中率

为了考察推荐域名列表中域名个数对重定向命中率的影响,令加权系数为 4、域名个数为 20,同样经历两天的实验,记录各个命中域名的排名,由此可以得到小于 20 的所有域名个数对应的命中率,如图 5 所示。可见,重定向命中率随域名个数而增加,当域名个数为 20 时的最高命中率约为 0.57,此后,增加域名个数对重定向命中率的影响并不大。此外由于域名个数的增加会增大传输报文的长度,因此盲目增大域名个数并不可取,建议一个合理的数值是取为 12 左右。

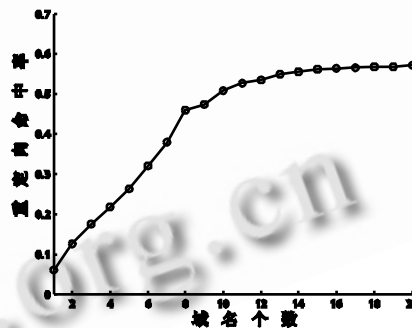


图 5 不同域名个数下的重定向命中率

4 结语

针对 DNS 服务的重定向功能,本文提出把按相关性排序的推荐域名的列表作为域名错误的描述信息。提出向重定向服务器的两种转交,可以帮助有效及时地发现用户真实意图的域名。提出利用延长资源记录的处理算法。提出重定向报文结构,可以在扩展的 DNS 协议内容纳重定向信息。

参考文献

- 1 Albitz P, Liu C. DNS and BIND. O'Reilly and Associates, 1998.

(下接第 41 页)

- 2 Mockapetris P. Domain names-implementation and specification, STD 13, RFC 1035, November 1987.
- 3 Elz R, Bush R. Clarifications to the DNS Specification, RFC 2181, July 1997.
- 4 Creighton T, Griffiths C, Livingood J, Weber R. draft-livingood-dns-redirect-00, Internet-Draft, 2009
- 5 Wang Z, Lee XD, Jin J, Yan BP. Efficient Filtering Algorithm for Repeated Queries in DNS Log. The 8th IEEE International Symposium on Network Computing and Applications (NCA09). 2009.
- 6 Berger AL, Vincent J, Pietra D, Stephen A, Pietra D. A maximum entropy approach to natural language processing. Computational Linguistics, 1996,22(1):39 – 71.
- 7 Kenneth W, Church, William A, Gale. Probability scoring for spelling correction. In Statistics and Computing, 1991,1:93 – 103
- 8 Cucerzan S, Brill E. Spelling correction as an iterative process that exploits the collective knowledge of web users. Proc. of EMNLP,04, 2004. 293 – 300.