

基于DNS技术实现网络的扩展和高可靠性

吴翔毅

(华侨大学 网络中心,福建 泉州 362021)

【摘要】本文阐述了接入双ISP的校园网络,在无法使用动态路由的情况,利用DNS技术实现网络的扩展和高可靠性的解决方案。它综合了BIND的Forwarder、MX记录、Round Robin、View等关键技术,合理利用双ISP的带宽资源,从而达到提高网络速度、提高网络稳定性的目的。

【关键词】DNS;Forwarder;MX;VIEW;负载均衡

【中图分类号】TP393.03 **【文献标识码】**A **【文章编号】**1673-1891(2009)02-0040-03

1 引言

由于CERNET(中国教育和科研计算机网)对大部分国外站点的访问是按照流量收费的。如果完全通过CERNET来对外访问,则会因为流量巨大造成网络费用过高。且CERNET与CHINANET(中国公用计算机互联网)等网络互联带宽有限及网络资源的分布不均,很多高校校园网用户与CHINANET互相访问的速度非常慢。

基于费用、速度和资源利用情况的考虑,CERNET的用户纷纷开通第二出口,很多用户的第二出口选择接入CHINANET。我校也通过当地电信接入了CHINANET。但是,基于CERNET与CHINANET双方彼此不为对方的IP地址提供路由的原因,我校无法使用动态路由来实现双出口线路的冗余备份及负载均衡。如何充分利用双线路实现网络的扩展和高可靠性,是我们主要考虑的问题。

2 校园网现状及问题分析

2.1 校园网现状

(1)我校从CERNET申请到的IP地址有32 C,从CHINANET申请到了64个IP地址。

(2)CERNET与CHINANET双方彼此不为对方的IP地址提供路由,即我校CERNET的IP地址不能直接通过CHINANET的线路访问Internet,我校CHINANET的IP地址也不能通过CERNET的线路直接访问Internet。

(3)校园网所有计算机均使用部署了CERNET IP的DNS服务器进行域名解析。

(4)大部分应用服务器部署了CERNET的IP地址,包括邮件服务器(mail.hqu.edu.cn),少部分应用服务器部署了CHINANET的IP地址。

(5)校内用户使用CERNET的IP地址及私有IP地址。采用策略路由及NAT转换技术使校园网用户访问教育科研网的资源时走CERNET线路出口;

访问其它站点包括国外站点时走CHINANET提供的线路出口;校外CERNET用户要访问校园网部署了CERNET的IP的服务器时走CERNET线路出口,访问校园网部署了CHINANET的IP的服务器时走CHINANET线路出口。

2.2 问题分析

这样分配IP及路由既合理利用了网络资源,又降低了网络费用,但是没能解决网络应用上的链路单点故障及网络应用的负载均衡的问题。由于DNS的工作原理及我校的实际情况,一旦CERNET的线路中断,我校的DNS服务与外界的通信将中断,并导致:

(1)校内用户无法使用域名通过CHINANET的线路访问Internet。

(2)校园网外的用户无法通过域名访问hqu.edu.cn域下的所有服务器,即使相关服务器使用CHINANET的IP地址。

(3)邮件服务服务器不能及时收发电子邮件,可能导致电子邮件被退回甚至丢失。

3 部署CHINANET IP地址的DNS服务器,实现DNS服务器的扩展和高可靠性

从体系结构上来说,域名系统DNS是一种分布式的、层次型的、客户机/服务器式的数据库管理系统。根域名服务器对解析来说是非常重要的。在缺乏其他信息的情况下,解析总是不得不从根域名服务器开始。假设校园网外的用户想访问我校http://www.hqu.edu.cn网站,在对方本地DNS服务器的缓存中没有我校域名www.hqu.edu.cn对应的IP地址信息的情况下,对方的本地DNS服务器最终将会从edu.cn的DNS服务器中获得我校DNS服务器的IP地址,再从我校DNS服务器中获得www.hqu.edu.cn对应的IP地址:210.34.240.107,然后,用户才能与www.hqu.edu.cn网站进行通信。

在CERNET线路中断的情况下,校园网外的用

收稿日期:2009-04-02

作者简介:吴翔毅(1974-),男,福建龙海人,工程师,主要从事网络管理、负载均衡的研究。

户将无法访问我校 CERNET IP 的服务器,包括 DNS 服务器,也无法通过域名访问我校部署了 CHINNET IP 的服务器,虽然在 CERNET 线路中断的情况下,仍然能通过 CHINANET 线路访问我校部署了 CHINNET IP 的服务器,但是,因为无法与我校 DNS 服务器进行通信,也就没办法解析到相应的 IP 地址。

部署第三台 DNS 服务器,使用 CHINANET IP 地址:202.109.210.10,并申请将此 DNS 服务器的 IP 地址在 EDU.CN 的 DNS 服务器上进行注册,这样,就在 CHINANET 线路上部署了一台备份 DNS 服务器,一旦 CERNET 线路中断,校园网外的用户最终可以从 EDU.CN 的 DNS 上获得我校第三台 DNS 服务器的 IP 地址,从而从 CHINANET 线路与我校的 DNS 服务器进行通信,解析到我校的域名。

4 利用 Forwarder 实现 DNS 服务器的高可用性

部署 CHINANET IP 的 DNS 服务器,达到了校外用户解析我校域名在双出口线路上实现备份的目的,不至于产生解析上的单点故障。但对于校内用户解析校外域名,仍然存在单点故障,一旦 CERNET 出口线路中断,将导致校园网用户无法使用域名通过 CHINANET 线路访问非 CERNET 上的资源。解决方法有两种:其一,让校园网用户手动设置自己计算机的首选 DNS 服务器为:210.34.240.100,备用 DNS 服务器为:202.109.210.10 或让用户自动获得 DNS 服务器信息。其二,使用 DNS 转发功能,从而不需用户进行额外的操作,做到对用户透明,且节省 DNS 解析的国际流量费用。

BIND 提供了很多非常好的特性,转发(Forwarder),就是其中的一个。可以将 CHINANET 上的 DNS 服务器当成转发器,在 CERNET IP 的 DNS 的配置文件上做以下设置,将 DNS 解析转发到 CHINANET IP 的 DNS 服务器上。转发机制是这样的:当设置了转发器后,所有非本域的和在缓存中无法找到的域名查询都将转发到设置的 DNS 转发器上,由 CHINANET 上的 DNS 来完成解析工作并做缓存。因而将 CERNET 上的 DNS 流量转移到了 CHINANET 上,节省了国际流量费。

转发器的配置格式是:

```
options {
    forwarders { CHINANET 上的 IP 地址; };
};
```

5 利用 MX 记录实现邮件服务器的扩展和高可靠性

DNS 提供一种机制,能为邮件发送指定备份邮件服务器。这种机制还允许一台邮件服务器为别的邮件服务器承担邮件处理任务。DNS 用了一种资源记录类型来实现增强的邮件路由,那就是 MX 记录。MX 记录为一个域名指定了一个 mail exchanger(邮件交换器):它是一台邮件服务器,负责处理或转发该域名的邮件。邮件收发器总是最先试着向优先级值最小的邮件交换器发送邮件。部署两台邮件服务器,一台使用 CERNET 的 IP 地址,另一台使用 CHINANET 的 IP 地址。在 DNS 服务器上设置以下两条 MX 记录:

```
hqu.edu.cn. IN MX 10 mail.hqu.edu.cn.
hqu.edu.cn. IN MX 20 ct.hqu.edu.cn.
```

上面 MX 记录中的数字,表示优先级,邮件优先投递到数值最小的邮件服务器上。以上两条记录说明了,发往 @hqu.edu.cn 的邮件将被优先发送到 mail.hqu.edu.cn 上,如果 mail.hqu.edu.cn 不可达,邮件将被发送到 ct.hqu.edu.cn 上,再从 ct.hqu.edu.cn 上择机发往 mail.hqu.edu.cn。

在这种部署方法上,既实现了邮件服务器的冗余备份,又实现了邮件服务器在 CERNET 和 CHINANET 线路上的备份,默认下邮件通过 CERNET 线路到我校的邮件服务器上,CERNET 线路中断的情况下,邮件仍然能通过 CHINANET 线路发送到 ct.hqu.edu.cn,再从 ct.hqu.edu.cn 转发到 mail.hqu.edu.cn。即使 mail.hqu.edu.cn 停机,邮件也能暂时保存在 ct.hqu.edu.cn 上,当 mail.hqu.edu.cn 恢复正常时再发往 mail.hqu.edu.cn。如果把 mail.hqu.edu.cn 换成 CHINANET 上的 IP 地址,ct.hqu.edu.cn 换成 CERNET 上的 IP 地址,还能节省下大部分的国际邮件流量费。

6 利用 DNS Round Robin 实现应用服务器的负载均衡

DNS Round Robin 技术就是采用域名服务器作为分配负载的关键设备来完成服务器之间的负载平衡,即把对同一个域名的客户请求,轮流解析成不同的 IP 地址,分配到不同的后端服务器上。利用 DNS Round Robin 技术可以实现由多台对称结构的服务器来提供某种应用服务,解决在大量并发访问时单台服务器的处理能力和 I/O 能力成为瓶颈问题。在对称结构中,建立内容完全一致的 Web 服务器并不困难,因此,负载均衡技术就成为建立一个高负载 Web 站点的关键性技术。DNS Round Robin 就是这种技术实现的一种方式,只需在 DNS 数据库中建立多条 A 记录即可,以下是一个配置实例:

```
www      IN      A      210.34.240.107
www      IN      A      202.109.210.8
```

DNS Round Robin 技术在接入单 ISP 的情况下能很好地进行工作,但在接入双 ISP 的情况下,没能考虑到用户与所访问服务器的网络距离,DNS 仅仅是随机地解析一个 IP 地址给用户,这样就存在着如 CERNET 用户解析到 CHINANET 的 IP,需从 CHINANET 线路访问服务器的情况。而利用 Bind 的 View 功能能很好地解决这个问题。

7 利用 Bind VIEW 合理利用 CERNET 和 CHINANET 的带宽资源

DNS View 策略解析最基本的功能是可以智能地判断访问网站的用户,然后根据不同的访问者把你的域名分别解析成不同的 IP 地址。如访问者是 CERNET 用户,DNS 策略解析服务器会把你的域名对应的 CERNET IP 地址解析给这个访问者。如果用户是电信用户,DNS 策略解析服务器会把你的域名对应的电信 IP 地址解析给这个访问者。

DNS 智能策略解析还可以给你的多个主机实现负载均衡,这时来自各地的访问流量会比较平均的分布到你的每一个主机上。一个配置实例如下:

在 /etc/named.conf 中配置以下内容:

```
acl "CERNET" {CERNET IP 地址段;;
```

```
view "CERNET" {
  match-clients {CERNET;};
  zone "hqu.edu.cn" {
    type master;
    file "zone.hqu.edu.cn.CERNET";
  };
};
view "any" {
  match-clients {any;};
  zone "hqu.edu.cn" {
    type master;
    file "zone.hqu.edu.cn.ChinaNET";
  };
};
```

在 zone.hqu.edu.cn.CERNET 中增加 A 记录:

```
www IN A 210.34.240.107 ;教育网 IP
```

在 zone.hqu.edu.cn.ChinaNET 中增加 A 记录:

```
www IN A 202.109.210.8 ;电信网 IP
```

由于网络可能存在不同情况的不稳定,假如学校的教育网出口出现故障,教育网用户就无法通过 210.34.240.107 访问 www.hqu.edu.cn。这时如果让教育网的用户解析 www.hqu.edu.cn 获得地址 202.109.210.8 的话,他们就可以通过 CHINANET 访问。

注释及参考文献:

- [1]Paul Albitz , Cricket Liu. DNS and BIND(第4版)(影印版)[M].北京:清华大学出版社,2003.
- [2]Internet Systems Consortium. BIND 9 Administrator Reference Manual[EB/OL]. <http://www.isc.org>
- [3]SUN Microsystem. Administering Domain Name Service System & Network Administration.

Implementation of Expanding and Achieving High-reliability Network Based on DNS

WU Xiang-yi

(Network Center of Huaqiao University, Quanzhou, Fujian 362021)

Abstract: This paper mainly introduces the solution for implementation of expanding and achieving high-reliability network based on DNS, in the case that dynamic routing can not work on the campus network that access internet through dual ISP. It combines the Forwarder, MX Record, Round Robin, View and other key technologies of BIND, it rationally using dual-ISP bandwidth and increasing network access speed to improve the stability of the campus network.

Key words: DNS; Forwarder; MX; VIEW; Load balancing