

吴叔坤, 黄文辉. 广东台网网络服务架设实例[J]. 华南地震, 2015, 35(3): 15-24. [WU Shukun, HUANG WenHui. Network Services Building for Guangdong Digital Seismic Network[J]. South china journal of seismology, 2015, 35(3): 15-24.]

## 广东台网网络服务架设实例

吴叔坤, 黄文辉

(广东省地震局, 广州 510070)

**摘要:** 概述了广东台网网络概况和应用背景, 通过网络架设实例, 详细描述了网络设计的多方面应用及其基于开源系统的部署方法, 总结了有了架设基本网络服务后可继续丰富更多网络服务的展望。

**关键词:** 架设; 域名服务; DMZ; 防火墙; 负载均衡

**中图分类号:** P315.78      **文献标志码:** A      **文章编号:** 1001-8662 (2015) 03-0015-10

**DOI:** 10.13512/j.hndz.2015.03.003

## Network Services Building for Guangdong Digital Seismic Network

WU Shukun, HUANG WenHui

(Earthquake Administration of Guangdong Province, Guangzhou 510070, China)

**Abstract:** The paper provides an overview of the basic situation and application background of Guangdong Digital Seismic Network. Through the network service building example, the paper describes in detail many applications of network design and its configuration methods based on open source systems by some maintenance examples, and summarizes the future more services available after basic network services building.

**Keywords:** Building; Domain service; DMZ; Firewall; Load balance

### 0 引言

广东省数字地震台网(以下简称广东台网)是广东省人民政府和中国地震局共同投资建设的区域地震台网。从建成到现在, 广东台网不但承担了地震速报任务, 而且还是国家地震速报的备份中心以及可能是将来的中国地震台网中心的速报灾备中心, 因此对广东台网的网络进行科学经济

的设计和应用对广东台网的日常工作尤为重要。

由于各种历史原因, 广东台网的网络设计和应用比其他地震台网的网络相对复杂。目前我国大多数地震台网中心的网络都是由信息部门提供线路接入和管理, 然后给各部门提供服务。广东台网由于前期网络设计比较规范合理, 至今多数网络都是专线直接到广东台网, 然后由广东台网管理, 并为广东省地震局提供互联网出口服务。

**收稿日期:** 2014-08-19

**基金项目:** 地震行业科研专项 (201308008)

**作者简介:** 吴叔坤 (1977- ), 男, 工程师, 现主要从事监测预报工作。

**E-mail:** wsk@gddsn.org.cn.

目前,广东台网的专线接入有分别有 VPDN、帧中继、SDH、卫星以外,还有电信和联通的外网光纤接入。图 1 是台网的网络基本拓扑结构,从图中可出,广东台网主要由 DMZ(非军事区)、生产系统业务区、办公区、开发区 4 个子网和一个行业专线子节点构成,而广东台网根据应用和需求,分别架设了基于 FreeBSD 操作系统的路由器、防火墙、DNS 服务器、WWW 服务器、邮件服务器、VPN 服务器等,使广东台网的网络服务完全具备了轻量级的企业应用能力。提供外网服务的负载均衡服务器(防火墙)、邮件服务器、DNS 服务器

和 Web 服务器一般都部署在 DMZ 区内以提供服务,也因为广东台网网络应用是基于 FreeBSD 开源系统的部署应用,因此在图例里的任一服务器均可完全配置成既包含了路由器的功能,也包含了防火墙、网络冗余、负载均衡等功能,这样一机多用的好处是既简化了网络结构的冗余,也大大减少了相关硬件设备的成本,有利于管理员简化管理以及为机房节省空间;由于开发区域网络和办公区域网络等几个子网功能相对简单,因此在本文中不做详细赘述。本文将详细阐述讨论提供外网服务的设置方法和应用。

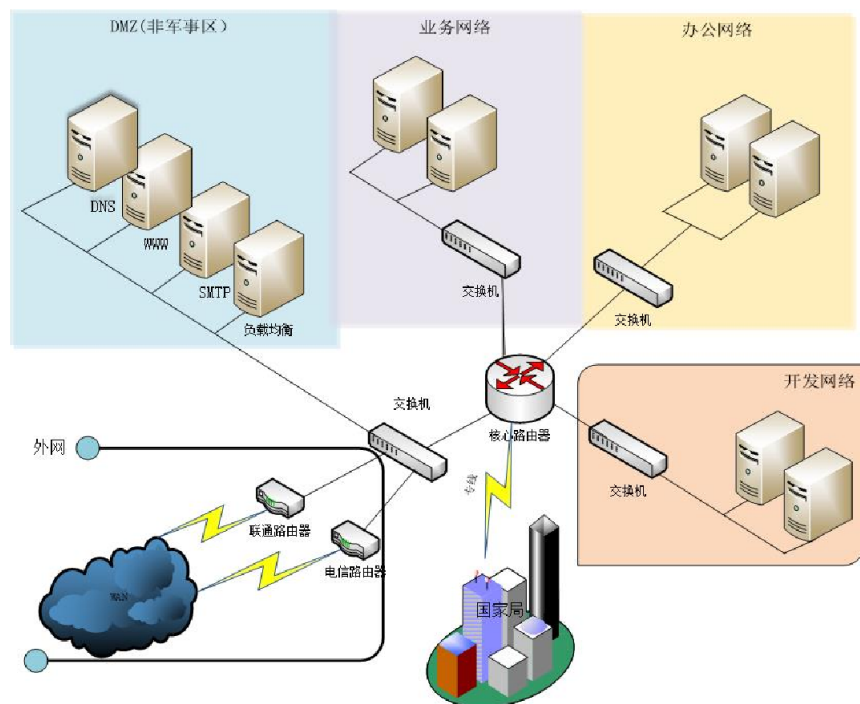


图 1 广东台网网络拓扑图

Fig.1 Network topology map of GDASN

## 1 智能域名服务器的实现

### 1.1 BIND9 简介

BIND (Berkeley Internet Name Domain) 就是大家日常所接触的 DNS 服务器的软件实现,如图 2 所示,是现今互联网上最常用的 DNS 服务器软件<sup>[1]</sup>,因此现在有接近 90% 的服务器都使用 BIND 做为其 DNS 服务器<sup>[2]</sup>。BIND 体系架构采用树形目录的层层继承方式,是一种分布式网络信息查找服务,其主要功能是用来解决主机名和其相对应 Internet 地址的映射软件,类似于身份证号码和名字的关系,系统可以通过姓名自动找到身份证号,

反之亦然。

正如图 2 所示, DNS 是一个分布式的名称对应系统,类似于电脑的树目录结构:在最顶端是一个“根”,然后其下层分为好几个基本类别名称,如: com、net、org、gov 等;再下层是组织或机构名称,如 apple、sina、gddsn 等;继而是主机名称,如: www、mail、ftp 等。因当初 Internet 是美国发起的,所以当时并没有国家域名这一项,但随着互联网的快速发展, DNS 也加入了 cn、fr、au 等国家域名名称。所以一个完整的 DNS 名称表示就好像是这样的: www.gddsn.org.cn, 而整个名称对应的就是一个 IP 地址的映射了。

DNS 域名查询采用由下而上的查询方式。当

DNS 被查询到有关本域名内的主机名称时, DNS 服务器会立刻返回结果给用户, 查询结束; 当所查询的主机名在本级 DNS 服务器以外时, DNS 服务器会首先检查本身缓存有没有此主机名的纪录, 如果有, 则返回结果, 如没有, 则转向上一级服务器查询, 以此类推, 直至查到结果或者抵达到 DNS 根部为止。因此, 从这个查询过程可以看出, 没有任何一台 DNS 服务器会包含所有域名的 DNS 资料, 资料都是分布在全球各个地方的 DNS 服务器中, 而管理 DNS 根的组织只需知道各 DNS 服务器的地址就可以了<sup>[3]</sup>。

广东台网域名服务软件主要使用了 BIND9 做为驱动, 主要原因是因为它提供了更安全强大、快速稳定的域名服务, 并且已集成到类 UNIX 系统里面, 省去了下载安装的烦恼, 所以部署起来也比较方便简单一些。

截至目前, 广东台网已具备固定公网 IP 地址条件, 申请了自己的完整域名, 并且自己完成本地域名的解析, 因此需要为广东台网的内外子网搭建一个域名服务系统。对广东台网目前的网络状况来说, 其工作主要是使用 BIND9 的试图功能配置一个具有内外网服务器的主域服务器。

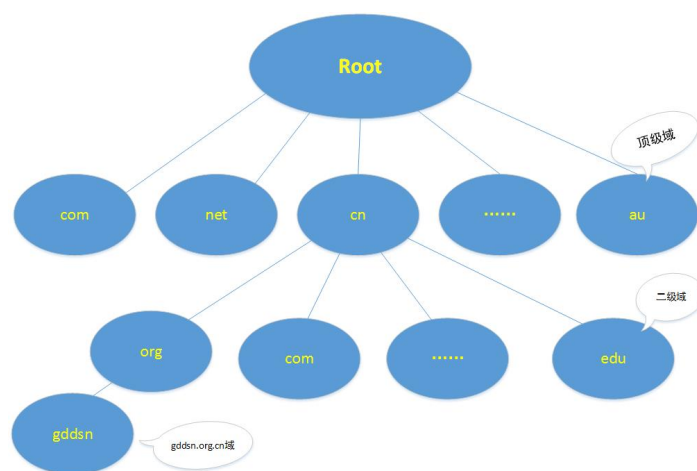


图2 DNS体系架构图

Fig.2 DNS architecture diagram

## 1.2 智能 DNS 的实现过程

### 1.2.1 BIND9 文件体系结构

BIND9 主要文件结构如下所示:

/etc/namedb/named.conf 全局配置文件

/etc/namedb/master 表示主域服务器配置目录

/etc/namedb/slave 表示定义的是辅助域名服务器配置目录

### 1.2.2 详细配置

(1) 配置 named.conf 全局配置文件。这里的任意配置修改都会对整个 BIND 系统起作用, 配置文件的前两项主要是为了安全而设置的只能让内网和本地外网连接过来做 DNS 查询; 由图 1 的网络拓扑图看出, 因为 DNS 在 DMZ (Demilitarized Zone) 非军事网络区内, 因此它也包含有内网和外网两个区域, 所以我们要用到 BIND9 的 View (视图) 功能, 让内外网的子网区域 (zone) 分别在其中的视图里。文件配置内容如下:

① 建立访问控制区, 内容如下:

```

acl "trusted" {
    192.168.168.0/24;
    12.34.56.78/30;
    localhost;
};

```

② 全局选项的一些常规参数, 内容如下:

```

options {
    directory "/etc/namedb";
    pid-file "/var/run/named/pid";
    allow-query {
        trusted;
    };
};

```

③ 建立广东台网 gddsn-ext 外网视图, 内容如下所示:

```

view "gddsn-ext" {
    match-clients {trusted;};
    recursion no;
};

```

```

zone "gddsn.org.cn" {
type master;
file "zones/ext.gddsn.org.cn.hosts";
};
zone "56.34.12.in-addr.arpa" {
type master;
file zones/"56.34.12.in-addr.arpa";
};

```

④ 建立广东台网 gddsn-lan 内网视图, 内容如下:

```

view "gddsn-lan" {
match-clients { trusted; };
//recursion yes;
zone "." {
type hint;
file "zones/lan.gddsn.org.cn.hosts";
};
};
// 其他一些回路网口等保留设置可以忽略跳过
zone "localhost" {
type master;
file "master/localhost-forward.db";
};
zone "127.in-addr.arpa" {
type master;
file "master/localhost-reverse.db";
};
zone "255.in-addr.arpa" {
type master;
file "master/empty.db";
};
}

```

至此, 广东台网的 gddsn 视图创建完毕。

(2) 设置外网 gddsn-ext 域名正反向解析。这里的设置主要就是创建外网 gddsn-ext 视图里的两个区(zone)里定义的 file 正反向解析资源文件。方法是在/etc/namedb 目录下创建 zones 目录, 然后在新建目录下分别创建 ext.gddsn.org.cn.hosts 和 56.34.12.in-addr.arpa 文件。此处唯一需要注意的就是每修改完配置文件, 记得给序列号更新下以让 BIND 及时更新修改过的记录。

① 创建正向解析文件 zones/ext.gddsn.org.cn.hosts, 内容如下:

```

$ORIGIN gddsn.org.cn.
$TTL 3600

```

```

@IN SOA gddsn.org.cn. root.gddsn.org.cn. (
20060401; Serial
3600; Refresh
900; Retry
3600000; Expire
3600); Minimum
IN NS ns.gddsn.org.cn.
IN MX mail.gddsn.org.cn.
ns IN A 12.34.56.80
mail IN A 12.34.56.81

```

② 创建反向解析 zones/56.34.12.in-addr.arpa, 内容如下:

```

$ORIGIN gddsn.org.cn.
$TTL 3600
@ IN SOA ns.gddsn.org.cn. root.gddsn.org.cn. (
20060401; Serial
3600; Refresh
900; Retry
3600000; Expire
3600); Minimum
IN NS ns.gddsn.org.cn.
80 IN PTR ns.gddsn.org.cn.
81 IN PTR mail.gddsn.org.cn.

```

③ 设置内网 gddsn-lan 域名正向解析。对于内部局域网, 因为各主机都在一个子网内, 用户只需知道网内主机名称就已满足日常需要, 所以无特殊需求的情况下, 只需设置正向解析即可。方法同外网正向解析设置一样, 在/etc/namedb/zones 下建立正向解析数据库文件 zones/lan.gddsn.org.cn.hosts。其主要内容如下:

```

$ORIGIN gddsn.org.cn.
$TTL 3600
@ IN SOA gddsn.org.cn. root.gddsn.org.cn. (
20060401; Serial
3600; Refresh
900; Retry
3600000; Expire
3600); Minimum
IN NS ns.gddsn.org.cn.
IN MX mail.gddsn.org.cn.
ns IN A 12.34.56.70
mail IN A 12.34.56.71
gw-ext IN A 12.34.56.74;
Lan data

```

```
gw-lan IN A 192.168.168.1
bacula IN A 192.168.168.2
balance IN A 192.168.168.3
```

1.3 智能 DNS 的测试

最简单的方法是使用一般操作系统自带的 ping 指令来 ping 不同的主机名称, 测试是否和 BIND 映射的 IP 地址相同, 从下面结果可以看出内外网的域名都已正确解析出 BIND 设置里的 IP 地址。

```
ping gw-ext.gddsn.org.cn
PING gw-ext.gddsn.org.cn ( 12.34.56.74 ) : 56
data bytes
64 bytes from 12.34.56.74: icmp_seq=0 ttl=64
time=0.076 ms
64 bytes from 12.34.56.74: icmp_seq=1 ttl=64
time=0.108 ms
64 bytes from 12.34.56.74: icmp_seq=2 ttl=64
time=0.197 ms
ping gw-lan.gddsn.org.cn
PING gw-lan.gddsn.org.cn (192.168.168.1) : 56
data bytes
64 bytes from 192.168.168.1: icmp_seq=0 ttl=64
time=0.195 ms
64 bytes from 192.168.168.1: icmp_seq=1 ttl=64
time=0.201 ms
64 bytes from 192.168.168.1: icmp_seq=2 ttl=64
time=0.188 ms
```

2 邮件服务器的实现过程

2.1 背景简介

Email(Electronic Mail)是 Internet 最基本, 也最重要的服务之一。成功架设了域名服务器以后, 就可以架设广东台网专属域名的邮件服务器了。在一般官方正式邮件交流中, 特别是和国外相关机构人员邮件交流中, 如果你所在机构的有专属的域名邮件系统, 无形增加了机构部门的专业技术地位和权威, 让人觉得是比较正式的官方交流。因此, 对比 gml、163 或 QQ 等公共邮件服务, 专属邮件具有不可比拟的优势。广东台网采用的邮件服务是基于 postfix 的邮件系统服务。

2.2 Postfix 邮件服务的实现过程

选择postfix 软件, 主要原因是其在快速、易于管理和提供尽可能高的安全性等方面都有较好的表现, 同时与类 UNIX 上的 Sendmail 邮件保持较好的兼容, 因此是架设 FreeBSD 平台下的邮件服务器的较好选择。

2.2.1 postfix 简介

Postfix 是由 IBM 资助开发的免费邮件服务器, 它是一个全球范围被广泛采用的邮件服务系统, Apple Server、AOL、NASA、斯坦福大学等都使用它做为自己的邮件服务系统<sup>[4]</sup>, 如图 3 所示。在图 3 中, 蓝色矩形也就是所谓的查询表, 查询表一般包含用户访问控制列表或者垃圾邮件列表等相关

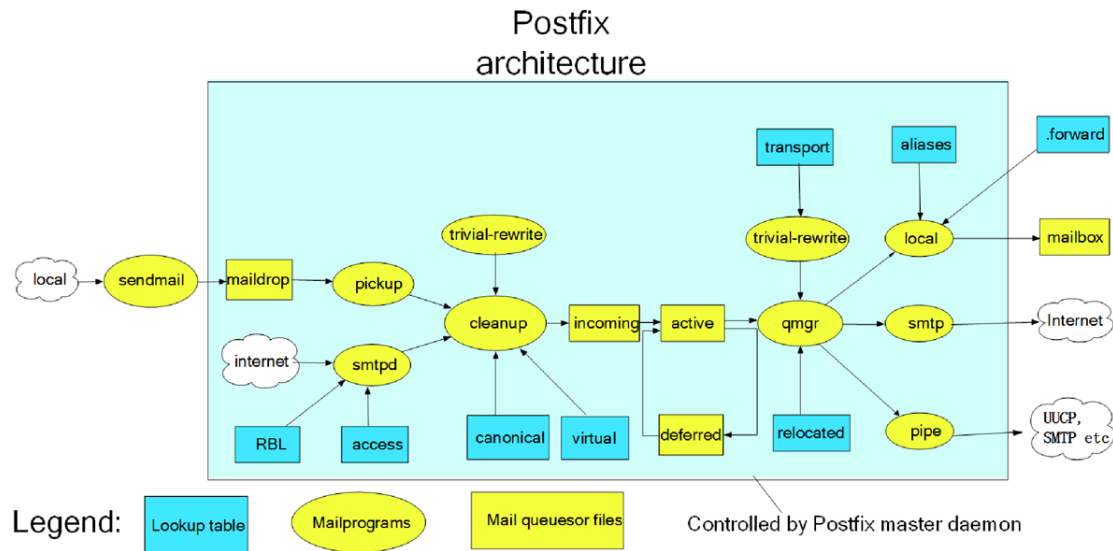


图 3 Postfix 体系架构图

Fig.3 Postfix architecture diagram

信息；黄色椭圆代表的是只完成单一目的的后台邮件服务守护进程，这相当于把整个 Postfix 系统分片成多个小服务后台程序；黄色矩形表示邮件队列或者是文件，不管哪种，文件都是存在硬盘里；白云代表每一个进出的邮件，例如 smtpd 从别的邮件服务器收到邮件，用户用 smtp 把邮件转发出去到别的邮箱。

从图 3 的软件架构图中可以明显看出，Postfix 核心是由多个后台运行服务程序组成，每一个服务程序都只负责电子邮件传递的单一指定部分，例如 SMTP 服务，任务调度，地址重写以及本地转发服务器等。为了节省系统资源，当服务程序完成任务而空闲时，他们都会自动终止。

客户端程序运行在外部，他们通过与 Postfix 服务器中在用户 ~/.forward 查询文件进行交互，通过邮件传递的指令，最后再通过一个小程序完成邮件的提交或者邮件队列状态信息的查询。从概念上讲，Postfix 管理该传递消息传递和错误通知的一个从上到下的任务管道式过程。所有的消息和通知“状态”信息保留在文件系统中。在管道的进程大多不用集中控制；这种相对的自主权，简化了错误恢复。当一个进程在完成一个事务之前出现故障，它会退回到上一管道晚一点重试并且丢弃其输出到下一管道的输出结果。很多 Postfix 的守护进程在他们遇到问题的时候可以简单地进入“假死”状态；当一个服务请求到达时，他们又会自动重新启动。这种方法使得 Postfix 具有高度的自适应性，只要在操作系统或硬件不突然损坏情况下<sup>[9]</sup>。

Postfix 邮件服务器的特点有：

(1) 开源免费。软件公开源代码，全球免费使用。用户可以定制修改源程序或及时给发现漏洞的代码发布更新补丁。

(2) 架构先进，配置灵活。从 postfix 的架构图的黄色椭圆图示部分可以看出，它的核心主程序被分割成是由多个小程序组成，每个小程序都完成其特定的功能，从而提高了系统的安全和稳定。它的架构设计类似于多 CPU 的任务“分片”原理操作，使其速度更快，配置也更灵活。

(3) 兼容性强。Postfix 本来与 sendmail 兼容，从而使 sendmail 用户很容易迁移到 postfix 或两者共存。

(4) 速度快，稳定可靠。Postfix 运行在并行会话状态，每秒能处理约 300 封邮件<sup>[4]</sup>。

(5) 反垃圾能力强。Postfix 支持反向域名解析

及各种正则表达式等流行方式进行垃圾邮件过滤。

## 2.2.2 Postfix 邮件配置过程

postfix 安装部分笔者在此就不再赘述。当 postfix 安装完成后，所有的配置文件

/usr/local/etc/postfix 目录下，其中的 main.cf 是主配置文件，初始的主配置文件已可以让 postfix 正常运行，但要让其正常收发邮件并提高安全级别，还需要对主配置文件进行一些修改，x 修改项内容如下所示：

# 配置邮件主机名称和域名，他们是主配置文件中最基本的配置，很多其他的配置选项要使用到这两项。

```
myhostname = mail.gddsn.org.cn
```

```
mydomain = gddsn.org.cn
```

# 设置信任 IP 地址范围，只允许给出的网络连接系统发送邮件。

```
mynetworks = 127.0.0.0/8, 12.34.56.78/30,
              192.168.168.0/24
```

# 配置邮件服务器反垃圾邮件过滤处理，主要内容如下面所示。其主要设置目标就是：

(1) 对接收的邮件进行 DNS 反向解析检查，无法解析域名的邮件至今丢弃。

(2) 发送邮件前必须先通过验证。

(3) 添加实时黑名单功能，把每次收到的邮件都自动到反垃圾邮件机构的服务器上去查对，如果邮件来源于黑名单，则拒收邮件。

```
smtpd_delay_reject = yes
```

```
smtpd_helo_required = yes
```

```
smtpd_helo_restrictions =
```

```
    permit_mynetworks
```

```
    check_helo_access
```

```
hash:/usr/local/etc/postfix/helo_access
```

```
    reject_non_fqdn_hostname
```

```
    reject_invalid_hostname
```

```
    permit
```

```
smtpd_sender_restrictions =
```

```
    permit_sasl_authenticated
```

```
    permit_mynetworks
```

```
    reject_non_fqdn_sender
```

```
    reject_unknown_sender_domain
```

```
    reject_rhsbl_sender dsn.rfc-ignorant.org
```

```
    permit
```

```
smtpd_recipient_restrictions =
```

```
    permit_sasl_authenticated
```

```
    permit_mynetworks
```

```

reject_invalid_hostname
reject_non_fqdn_recipient
reject_unknown_recipient_domain
reject_unauth_destination
check_policy_service inet:127.0.0.1:12525
check_sender_access
hash: /usr/local/etc/postfix/sender_access
check_recipient_access
hash: /usr/local/etc/postfix/recipient_access
reject_rbl_client sbl-xbl.spamhaus.org, permit

```

### 2.3 Postfix 邮件服务的测试

对 Postfix 的测试最简单的办法就是使用通用的邮件客户端进行邮件收发的测试。首先配置好邮件客户端的连接信息,接着用公共邮箱给自己私有邮箱发一封测试信,再用邮件客户端给通用公共邮箱发一封邮件,最后稍等片刻再检查下是否成功发送或收到邮件。这些操作都是基于图形界面操作,简单明了,在次不再赘述。在此主要实际测试下基于命令行而省却配置邮件客户端繁琐配置的测试方法:

```

(1) 用 telnet 命令登陆邮件服务器的 smtp 端口
telnet localhost 25
Trying 127.0.0.1...
Connected to mail.gddsn.org.cn.
Escape character is '^]'.
220 gddsn.org.cn ESMTP Postfix

```

(2) 输入 helo 命令表明用户身份,成功返回 250 代码

```

helo localhost
250 gddsn.org.cn
(3) 输入 mail from:命令初始化一个邮件会话
mail from: wsk@gddsn.org.cn
250 2.1.0 Ok

```

```

(4) 输入 rcpt to: 命令标示收件人地址
rcpt to: sukenwoo@163.com
250 2.1.5 Ok

```

```

(5) 输入 data 指令表明邮件开始信息写作
data

```

```

354 End data with <CR><LF>.<CR><LF>

```

(6) 输入任意短信内容,结束用“.”表示内容结束

```

hello, test
.
250 2.0.0 Ok: queued as 10D6C2E08A

```

(7) 结束邮件会话,退出。

```
quit
```

```
221 2.0.0 Bye
```

```
Connection closed by foreign host.
```

进行完上述操作如没有出现错误的话,表明邮件服务器已经在正常运行。相信过不了片刻,你所发的收件人邮箱会有一封来自你私有邮箱发出的一封测试邮件。

## 3 网络负载均衡服务器的实现过程

广东台网外网出口的一个典型特点就是联通、电信双光纤接入,因此为了更好地利用网络带宽资源,提高网络出口访问的带宽和稳定,笔者为此搭建了外网出口的负载均衡服务器,如图 4 所示。

### 3.1 负载均衡服务器简介

顾名思义,负载均衡服务器就是就是将工作任务中的负载(网络流量)进行平衡,分摊到各个子节点上分流,从而提升网络的吞吐能力。从另一方面来说,它也可以叫做网络冗余服务器,从图 4 的网络拓扑图可以发现,负载均衡路由连接了联通、电信两个以上物理连接出口,假设其中任意一个物理连接出现故障时,服务器可通过另外一条物理链路出去,最终在用户甚至不知道网络出现故障的情况下,其日常业务仍可照常运行。

### 3.2 负载服务器实现方法

#### 3.2.1 设计思路

利用多线路接入的优势,设计做到任意某一线路中断,系统自动切换至线路正常的一端;如双线路都正常,则:① 设置策略路由,访问电信的优先走电信网关出口,访问联通的优先走联通网关出口;② 采用轮询方式的负载均衡。第一个数据包走第一条线路,第二个数据包走第二条线路以达到负载均衡;在同一会话交互里,让后续通信链路继续使用初始建立会话时的链路。

#### 3.2.2 实现方法

FreeBSD 操作系统自带了 Packet Filter 功能(简称 PF),其主要配置文件是/etc/pf.conf。笔者此处主要就是利用 PF 里的一个 route-to 功能,让输出连接可以平均分配到多个输出路径上以达到负载均衡目的。以下是修改配置文件选项的详细设置方法。



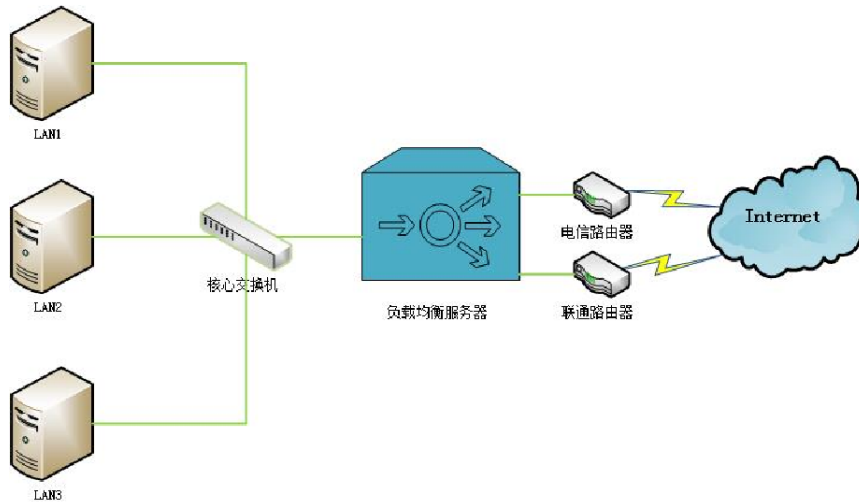


图4 负载均衡服务拓扑图

Fig.4 Topology map of loading balance

在/boot/loader.conf 下增加多路由表支持

net.fibs=2

在/etc/rc.local 下增加多个缺省网关

setfib 1 route delete default

setfib 1 route add default 5.6.7.9

以下是广东台网负载均衡的 pf.conf 配置文件内容:

(1) 设置内网卡, 定义内部子网; 绑定外网卡及设置外网的缺省网关

lan\_net = "192.168.0.0/16"

int\_if = "dc0"

ext\_if1= "bge0"

ext\_if2= "bge1"

ext\_gw1= "1.2.3.4"

ext\_gw2= "5.6.7.8"

(2) 设置对应的网络转换规则和默认规则

nat on \$ext\_if1 from \$lan\_net to any -> (\$ext\_if1) static-port

nat on \$ext\_if2 from \$lan\_net to any -> (\$ext\_if2) static-port

block in

block out

(3) 设置内网卡出去的数据包允许通过

pass out on \$int\_if to \$lan\_net

(4) 在内网卡上本局域网访问本机的数据包允许通过并不再往下匹配其他规则

pass in quick on \$int\_if from \$lan\_net to \$int\_if

(5) 为局域网访问负载均衡

pass in on \$int\_if route-to { (\$ext\_if1 \$ext\_gw1), \ (\$ext\_if2 \$ext\_gw2) } round-robin proto tcp from \

\$lan\_net to any flags S/SA modulate state

pass in on \$int\_if route-to { (\$ext\_if1 \$ext\_gw1), \ (\$ext\_if2 \$ext\_gw2)} round-robin proto {udp,icmp} \ from \$lan\_net to any flags keep state

(6) 因为安全连接不允许会话中间有任何改变, 特别设定 https 访问走单一链路

pass in on \$int\_if proto tcp from \$lan\_net to port https route-to (\$ext\_if1 \$ext\_gw1)

(7) route packets from any IPs on \$ext\_if1 to \$ext\_gw1 and the same for \$ext\_if2 and \$ext\_gw2

(8) 在接联通的网卡上允许通过来自电信的数据包路由到接电信的网卡上, 同理亦然

pass out on \$ext\_if1 route-to (\$ext\_if2 \$ext\_gw2) from \$ext\_if2 to any rtable 0

pass out on \$ext\_if2 route-to (\$ext\_if1 \$ext\_gw1) from \$ext\_if1 to any rtable 1

(9) 特别设置以便让 traceroute 命令的 UDP 数据包通过

pass out on \$ext\_if1 inet proto udp from any to any port 33433 > 33626 keep state

### 3.3 负载均衡服务器测试

测试的主要目的是检验使用多链路负载均衡系统在多条链路上分担出口流量的功能。测试步骤如下:

#### 3.3.1 线路正常时的测试

在双线路正常情况下用浏览器访问在线 IP 地址查询网站 [www.ip138.com](http://www.ip138.com), 得到的查询结果分别如图 5 和图 6 所示:

可以看出, 当链路正常时, 访问同一网站的



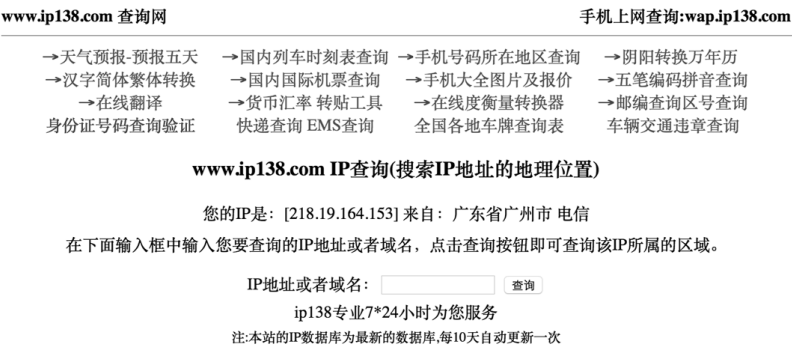


图 5 访问 IP 显示为电信

Fig.5 Access IP address showed as China telecom



图 6 访问 IP 显示为联通

Fig.6 Access IP address showed as China unicom

客户端 IP 地址可能会是两个出口的其中一个，由此可见，负载均衡是可用的。

3.3.2 在任一线路失效时测试

此测试的目的是验证当一条链路失效时，负载均衡系统能否依旧使用另一条正常线路工作。测试如下：

人为中断任一外网 xianl，看内网机器能否访问 www.ip138.com，并查看 IP 地址是否为正常线路的外网地址。本实验中中断联通的外网线路时得到图 5 所示的结果；中断电信链路时得到的如图 6 显示的结果。

综合以上测试，可以看出负载均衡服务器在多链路正常时能合理分配利用从而使总访问出口带宽扩大，且实现了当一个链路发生故障时，访问出口依然能切换到正常的一条链路上，这不但增加了台网的网络访问速度，还为台网网络访问提供了更高的可靠性和性能。因此，负载均衡服务器的架设是解决合理利用多出口资源问题的不错选择。

4 结语

按照本文所描述的方法搭建完成最基本的域名服务器以后，广东台网的基本网络框架就已搭建成型，笔者也可以在此框架的基础上继续架设更多的增值服务，例如本文描述的邮件服务。到目前为止，广东台网也基于此框架建成了软件开发论坛、国家备份地震自动速报网页服务、SVN 服务器等，未来也可以为部门机构搭建更多的私有云服务、FTP、VPN 等网络服务器，从而让广东台网的网络服务更丰富多彩<sup>[6-9]</sup>。

搭建网络服务，首要考虑的就是安全，其次是稳定。基于开源系统的网络服务先天性的优势就是它安全、开源免费。全世界用户都可以是开发者或是测试者，比如某人发现软件有漏洞公布出来、开发者收到就可以在零天内发布安全补丁把安全漏洞补上。开源系统还提供丰富的日志追踪和系统调试功能使管理员很快就能定位出系统问题出现在哪，从而快速修复问题；基于开源系统搭建的服务器，既可以配置成单一的路由器、

防火墙、负载均衡等，也可以配置成它们的组合甚至是“多合一”的全网络功能服务器，这不但减少了机房网络设备的数量，而且降低设备花费成本，使用起来更简便。

综上所述，基于开源的网络服务可以满足广东台网网络需求并可持续发展。

#### 参考文献：

- [1] 吴永权, 黄文辉, 苏柱金. 国家测震台网的实时数据传输与服务[J]. 华南地震, 2013, 33 (3): 77-84.
- [2] 洪旭瑜, 余丹, 刘坚刚, 等. 地震前兆台网 oracle 数据库与管理系统的维护与管理[J]. 华南地震, 2013, 33 (4): 117-124.
- [3] 刘琼山, 段洪杰, 杨黎薇, 等. 云南强震动台网中心应用系统的设计与实现[J]. 华北地震科学, 2014, 32 (3): 50-54.
- [4] 林洋, 张 颖. 服务器虚拟化在数据中心的应用实践[J]. 华南地震, 2014, 35 (1): 62-66.