第 28 卷 第 3 期
2013 年 6 月

天津科技大学学报
Journal of Tianjin University of Science & Technology

Vol. 28 No. 3
Jun. 2013

多互联网服务提供商网络接入的研究与实施

郭建忠[1]，侯仁平[2]，徐全富[3]，韩红哲[1]
（1. 天津科技大学信息化建设与管理办公室，天津 300457；
2. 天津科技大学计算机科学与信息工程学院，天津 300222；3.天津科技大学理学院，天津 300457）

摘 要：给出基于核心交换机、出口路由器等设备，并采用静态路由、策略路由、地址转换、自动侦测、负载分担等技术的多互联网服务提供商网络出口接入方案，研究了如何避免网络瓶颈，优化网络服务质量. 测试数据表明，服务器在做多出口发布后，数据包丢包率减小，平均延时减小，路由跳数减少，网络服务质量明显改善. 园区网网络服务质量和健壮性也明显改善.

关键词：策略路由；网络地址转换；自动侦测；链路备份；负载分担
中图分类号：TP393 **文献标志码**：A **文章编号**：1672-6510(2013)03-0075-04

Research and Implementation of Multi-interface Connection with Internet Service Providers

GUO Jianzhong[1], HOU Renping[2], XU Quanfu[3], HAN Hongzhe[1]
(1. Construction and Management Office of Information, Tianjin University of Science & Technology, Tianjin 300457, China; 2. College of Computer Sciences and Information Engineering, Tianjin University of Science & Technology, Tianjin 300222, China; 3. College of Sciences, Tianjin University of Science & Technology, Tianjin 300457, China)

Abstract: Based on a core switch and WAN router, a multi-interface connection with internet service providers was proposed, which used the technologies such as static routing, policy-based routing, network address translation, auto detect, and load balancing. How to avoid the network bottleneck and optimize the quality of network services was also research on. The results show that using the proposed method, packet drop ratio, average link delay, and route hop were reduced, and the servers' service quality was obviously improved. Meanwhile, the service quality and robustness of the internal network on campus were also significantly improved.

Key words: policy-based routing; network address translation (NAT); auto detect; link backup; load balancing

我国的网络接入单位在使用过程中存在联通、电信、教育科研网等各大互联网服务提供商(internet service provider, ISP)网络互联互通瓶颈问题. 部分研究方案[1–2]解决了互联互通，但其或为参考模型或局限于 Linux 系统；文献[3]利用网络设备进行部署，但是其策略路由没有考虑链路备份. 而且，上述文献都没把单位内部服务器通过智能 DNS 进行多出口发布. 文献[4]虽然实现了多出口网络，并且做了服务器多出口发布，但是也没有考虑链路备份和负载分担.

针对以上问题，本文对多 ISP 接入进行研究，将出口设备与智能DNS相结合，以期较好地解决各大 ISP 网络互联互通瓶颈，提高内外网用户访问网络资源的速度，避免没有线路冗余路由备份发生的单点故障.

1 多 ISP 网络接入的问题及解决方法

在多 ISP 网络出口接入的研究中，需要解决 4 个问题：(1)接入单位如何实现接入多 ISP 网络；(2)接入单位接入多 ISP 网络后如何提高内网用户外网网

收稿日期：2012–11–14；**修回日期**：2013–01–21
基金项目：天津市高等学校科技发展基金资助项目(20121101)；天津科技大学科学研究基金资助项目(20070222)
作者简介：郭建忠（1979—），男，内蒙古人，工程师，guo@tust.edu.cn.

络资源访问速度和使用效率；(3) 接入单位接入多 ISP 网络后如何避免单点故障；(4) 如何利用各 ISP 所分 IP 地址做内网服务器智能 DNS 多出口发布. 网络拓扑示意图见图 1.

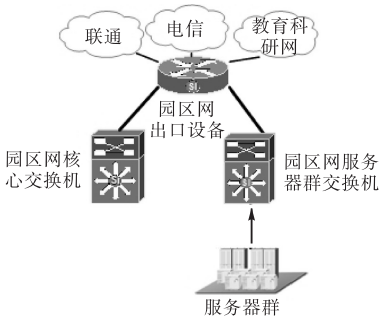

图 1　网络拓扑示意图

Fig. 1　Figure of network topology

解决问题 1 可以采用在相应网络出口设备配置地址转换(NAT)[5]的方法. 地址转换的机制就是将园区网内网主机的 IP 地址和端口转换为 ISP 分配的公有 IP 地址和端口，即＜内网 IP 地址 + 端口＞与＜公有地址 + 端口＞之间的转换.

解决问题 2 首选是申请自治域(AS)号码后使用边界网关动态路由协议，但是目前大部分接入单位无法申请到自治域(AS)号码，所以路由协议不得不选择静态路由协议. 利用各 ISP IP 地址聚合结果，设置静态路由指定到哪个 ISP 的数据就走对应的链路，其余未知 IP 地址利用等值的缺省路由指向各运营商出口. 这样就避免了 ISP 互联互通瓶颈，实现了园区网出口流量的负载分担，提高了园区网用户访问外网和外网用户访问园区网内网服务器的访问速度.

解决问题 3 的方法是将每条静态路由、缺省路由与对应运营商自动侦测组进行绑定. 自动侦测[6](auto detect)是一种利用 ICMP[7] Request/Reply 报文，定期检测网络连通状况的功能；自动侦测的对象是侦测组中目的 IP 地址集合，侦测结果反映了当前网络的连通状态，即目的主机是否可达，从而保证设备能够及时发现网络中存在的问题，并产生相应动作. 用户可以将某条静态路由和某个侦测组进行绑定，利用自动侦测的返回结果来控制静态路由的有效性：当侦测组可达时，静态路由生效；当侦测组不可达时，静态路由无效. 如果某一个 ISP 的链路出现故障，绑定了自动侦测组的静态路由和缺省路由自动切换到另一个 ISP 的链路，实现了链路备份. 这样可以降低园区网接入互联网单点故障的风险，从而提高了园区网运行的健壮性.

解决问题 4 时采用的方法是将园区网中 DNS[8]服务器配置成智能 DNS，针对不同 ISP 的外网用户返回园区网内网各服务器不同 ISP 的 IP 地址，园区网出口设备作服务器内网 IP 地址、端口与对应的 ISP IP 地址、端口的 NAT 静态转换. 外网用户在访问园区网服务器时数据包通过对应 ISP 的线路，这样就避免了外网用户在访问园区网内网服务器时 ISP 之间互联互通瓶颈，并且实现了多出口负载分担. DNS 服务软件 BIND 9[9]以上版本的视图[10](View)功能可以实现对不同 ISP 用户返回相应 ISP 所分服务器的 IP 地址，视图功能允许域名服务器根据查询者 DNS 服务器源地址而有区别地应答 DNS 查询，每个视图定义了一个在用户子集中可见的 DNS 名称空间，通过在多个视图中定义同一个域，不同的域数据按照视图语句的顺序可以传递给不同的用户.

2　多 ISP 网络接入的相关配置

2.1　园区网出口设备 NAT 配置

2.1.1　内网用户 IP 地址 NAT 配置

利用各 ISP 所分 IP 地址作为地址池，为园区网内网用户 IP 地址做 NAT 转换，配置过程如下：

(1) 配置 NAT 地址池[6]：

```
nat address-group 2 2.2.2.5 2.2.2.30
```

(2) 配置园区网内网允许 NAT 转换 IP 地址范围的访问控制列表：

```
acl number 3 000
  rule 0 permit ip source 1.1.0.0 0.0.15.255
  rule 1 deny ip
```

(3) 在园区网出口设备连接相应 ISP 接口下配置 NAT 转换：

```
nat outbound 3 000 address-group 2
```

2.1.2　服务器 IP 地址 NAT 配置

利用各 ISP 所分 IP 地址作为转换地址，为园区网内网服务器 IP 地址作 NAT 转换，配置过程如下：

```
nat server protocol tcp global 2.2.2.4 inside 1.1.2.2 www
```

其他 ISP NAT 配置与上述配置过程一样，只需将ISP所分IP地址、服务器 IP 地址做对应替换即可.

2.2　园区网出口设备的路由配置

2.2.1　静态路由配置

(1) 配置对 ISP 链路进行自动侦测的自动侦测组[6]1：

detect-group 1

detect-list 1 ip address 1.1.1.1

以上地址 1.1.1.1 为 ISP 的网关地址，根据实际组网情况可以修改成 ISP 网络中某个 ICMP 报文可达的 IP 地址，以侦测网络路径更远的 ISP 网络设备，从而避免 ISP 内部网络故障. 同样可以配置其他 ISP 自动侦测组 detect-group 2 和 detect-group 3.

(2)配置静态路由[6]与自动侦测组关联，使访问 ISP1 的流量优先通过 ISP1 的出口链路，其他 ISP 出口链路作为备份. 在具体配置过程中可以用各 ISP 实际网关地址替换地址 1.1.1.1、2.2.2.1 和 3.3.3.1，配置示例：

ip route-static 58.192.0.0 255.240.0.0 1.1.1.1 preference 60 detect-group 1

ip route-static 58.192.0.0 255.240.0.0 2.2.2.1 preference 90 detect-group 2

ip route-static 58.192.0.0 255.240.0.0 3.3.3.1 preference 120 detect-group 3

2.2.2　缺省路由配置

配置三条等值缺省路由，在互为备份的基础上实现负载分担：

ip route-static 0.0.0.0 0.0.0.0 1.1.1.1 preference 200 detect-group 1

ip route-static 0.0.0.0 0.0.0.0 2.2.2.1 preference 200 detect-group 2

ip route-static 0.0.0.0 0.0.0.0 3.3.3.1 preference 200 detect-group 3

2.2.3　策略路由配置

如果园区网内网服务器或者用户 IP 地址需要通过指定 ISP 出口进行数据传输，可以利用园区网网络出口设备设置相应策略路由[6]实现.

(1)配置园区网内网允许通过某 ISP 出口进行数据传输的内网 IP 地址范围访问控制列表[6]：

```
acl number 3002
  rule 0 permit ip source 1.1.2.1 0
  ……
  rule 12 permit ip source 1.1.12.12 0.0.0.7
```

(2)配置策略路由 FaBu，实现园区网内网允许通过某 ISP 出口进行数据传输：

```
route-policy FaBu permit node 0
  if-match acl 3002
  apply ip-address next-hop 1.1.1.1
```

(3)在网络出口设备中与核心交换机对应的接口上起用策略路由 FaBu：

```
ip policy route-policy FaBu
```

2.3　智能 DNS 服务器配置

2.3.1　智能 DNS 服务器视图配置

通过在 DNS 服务软件 BIND 9 配置多个视图，实现智能 DNS 功能，可以实现对不同 ISP 用户返回相应 ISP 所分服务器的 IP 地址. BIND 配置文件 named.conf[11]中关于视图功能的配置如下：

```
view "internal" {
  match-clients { 1.1.0.0/20; 11.11.0.0/19; }; //此处为内网 IP 地址范围
  zone "test.com" {
    type master;
    file "zone.test.internal"; };
  zone "2.1.1.in-addr.arpa" {
    type master;
    file "zone.test.internal.rev"; };
};
```

其他 ISP 对应的视图也按照上述格式配置，在 match-clients 中将 ISP 对应的所有 IP 地址聚合结果写入即可. 在最后一个视图中，设置 match-clients 中的 IP 地址范围为 any，匹配所有未知 IP 地址，配置域名对应的正向、反向解析.

2.3.2　智能 DNS 服务器域名正向解析配置

域名正向解析配置文件 zone.test.internal 中的 www 服务器配置：

```
www IN A 1.1.2.2
```

2.3.3　智能 DNS 服务器域名反向解析配置

反向解析配置文件 zone.test.internal.rev 中的 www 服务器配置：

```
2 IN PTR www.test.com.
```

域名对应的其他 ISP 正向和反向解析配置与文件 zone.test.internal 和 zone.test.internal.rev 类似.

2.4　多出口部署后数据测试结果

外网用户测试服务器结果分为两种情况：服务器只从一个 ISP 发布；服务器做多 ISP 发布. 联通用户 ping 命令测试结果见表 1.

表 1　测试结果

Tab. 1　Test results

序号	丢包率/%		平均延时/ms		路由跳数	
	单 ISP	多 ISP	单 ISP	多 ISP	单 ISP	多 ISP
1	21	2	169	71	20	6
2	23	3	170	17	20	6
3	23	3	157	21	20	6
4	15	1	156	16	20	6
5	24	0	157	15	20	6

由表 1 数据分析可知，服务器做多出口发布后，数据包丢包率减小，平均延时减小，路由跳数减少，服务器提供网络服务质量明显改善. 园区网内网用户访问服务器过程和外网用户访问服务器的过程一样，网络服务质量和健壮性同样明显改善，方案实施后得到了内网外网用户良好评价.

3 结　语

在多 ISP 网络接入的研究中，利用地址转换（NAT）、自动侦测、静态路由、缺省路由、智能 DNS 等技术实现了单位用户接入多 ISP 网络，提高了内网用户外网资源的访问速度和使用效率，避免了单一 ISP 出口容易出现单点故障，利用各 ISP 所分 IP 地址做内网服务器发布，有效地提高了外网用户访问内网服务器的速度和效率.

在实践过程中，各出口 NAT 设置应在物理或者逻辑上的同一个设备上部署，以免外网用户访问内网服务器时数据包路由走向不一致，无法建立 TCP 连接而不能访问服务器. 应将电子邮件服务器所使用的各 ISP IP 地址在上级 IP 地址管理机构做域名反向解析，避免由于反垃圾邮件策略限制而造成用户电子邮件收发不正常. 适当将 NAT 地址池加大，可以提高 NAT 转换性能，为园区网用户提供高效的网络接入服务. 为了优化网络接入，应将 DNS 服务器利用各 ISP 分配的 IP 地址在上级域名注册机构进行注册，这样互联网 DNS 服务器在解析内网服务器域名时可以通过各 ISP 的网络和 DNS 服务器进行通信，可以解决某 ISP 网络接入出现故障而无法解析接入单位域名的问题.

参考文献：

[1] 王彬，何文娟. 多出口多寻址模式的网络设计[J]. 计算机工程，2007，33(21)：259–261.

[2] 梁可结，魏文红，王高才. 一种有效的网络多出口流量调度方案[J]. 计算机工程，2010，36(5)：117–121.

[3] 王春丽，杨金艳. 运用策略路由解决网络多出口问题[J]. 铁道通信信号，2010，46(5)：70–72.

[4] 蔡昭权. 策略路由和动态 DNS 在校园网中的应用[J]. 计算机工程与设计，2005，26(5)：1396–1398.

[5] wikipedia. Network address translation[EB/OL]. 2012–03–02. http://en. wikipedia. org/wiki/Network_ address_ translation.

[6] 杭州华三通信技术有限公司. Comware V3 操作手册[EB/OL]. 2007–12–18. http://www.h3c.com.cn/Service/Document_Center/Routers/Catalog/AR_46/AR_46/Confiure/Operation_Manual/AR_46_OM%28V3.11%29/.

[7] wikipedia. Internet Control Message Protocol[EB/OL]. 2012–03–18. http://en.wikipedia.org/wiki/Internet_Control_Message_Protocol.

[8] wikipedia. Domain Name System[EB/OL]. 2012–03–20. http://en.wikipedia.org/wiki/Domain_Name_System.

[9] Internet Systems Consortium. BIND[EB/OL]. 2012–02–29. http://www.isc.org/software/bind.

[10] ChinaUnix. Bind9 View 底下的 master/slave 设定方案[EB/OL]. 2008–09–27. http://www.chinaunix.net/jh/16/308556. html.

[11] Internet Systems Consortium. BIND 9. 8. 1 Administrator Reference Manual[EB/OL]. 2011–10–19. https://deepthought.isc.org/article/AA-00499/116/BIND-9.8.1-Administrator-Reference-Manual. html.

责任编辑：常涛