广域网整合中 Stateful NAT、OSPF 双进程相结合的设计与应用①

李健俊[1] 俞先永[2] 刘 鹏[1] 姜学峰[1] (1.浙江中烟工业有限责任公司 浙江 杭州 310009;
2.杭州新世纪信息技术股份有限公司 浙江 杭州 310053)

摘 要: 大型企业重组和兼并，需要将多个独立的私网整合为一个统一管理的网络。提出利用 Stateful Nat 和 OSPF 双进程技术相结合，解决双路由模式下两个私网间的 NAT 同步和私网地址发布的问题，从而实现设备的冗余热备和负载均衡，提高网络的可靠性和安全性。

关键词: 广域网；Stateful NAT；OSPF

Design and Application of Stateful NAT and Multiple OSPF Processes in the Merge of WAN

LI Jian-Jun[1], YU Xian-Yong[2], LIU Peng[1], JIANG Xue-Feng[1] (1.China Tobacco Zhejiang Industrial Co.Ltd., Hangzhou 310009, China;2.Hangzhou New Century Information Technology Co.Ltd., Hangzhou 310053, China)

Abstract: The reorganization and annexation of large enterprises need to merge private networks into a unified network. This paper explains how to use the Stateful Nat and multiple OSPF processes to solve the problems of the NAT synchronization and the distribution of the private IP address between private networks, in order to make border routers working in hot standby and load balancing state to promote the reliability and security of the network.

Keywords: WAN; Stateful NAT; OSPF

当前企业兼并逐渐成为经济运行中的正常现象，企业兼并从数量,规模到种类都日益扩大。兼并企业的资源整合是指兼并双方相互使用、复制对方的优势资源并形成良好的资源关系，资源的整合重组促进业务成长，改变企业业务的品种和服务，改善企业业务的技术和组织系统。重组使企业可以通过改变业务运行方法提高企业的效率和效益，而不仅仅是简单地从规模的扩大等获得效益。

信息资源整合的前提是网络资源的整合，网络资源的整合不仅节约了企业资金投入，实现了多个部门间信息设备、光纤专线、人员和服务等资源的共享共用。整合信息网络资源，可强化网络互连互通和信息资源共享；改变网络及安全管理层次不清晰和无法集中监控信息系统状态，为今后信息系统的统一管理打下基础；理顺网络和应用系统的架构，使得企业信息系统的逻辑结构更加清晰，互连线路采取集中维护，分级管理，使建成后的网络在维护管理和实际应用更加科学、规范及高效性。

将若干个独立的网络整合为一个统一平台的大网络，在广域链路中的冗余热备、负载均衡、解决地址冲突成为网络资源整合中最需要实现的功能。为了解决 IP 地址不规范和网络平滑过渡,网络地址转换 NAT 技术提供了一种完全将私有网和公共网隔离的方法；开放最短路经优先(OSPF)以协议标准化强，功能强大，成为目前 Internet 广域网和 Intranet 企业网采用最多、应用最广泛的路由选择协议之一。

① 收稿时间:2009-07-06

1　广域网络需求

大型企业随着战略发展和市场开拓，企业重组和兼并需要将逐个独立的网络体整合为一个统一的网络平台。总部设计通过两台核心路由器与各分支机构连接，作为企业网广域核心网络。分支机构采用两台路由器双链路上行与总部两台核心路由器连接，分支机构内部用两台核心交换机，采用 HSRP 协议互为冗余备份，核心交换机与路由器交叉相连。

由于分支机构内部有不规范的 IP 地址，所以在分支机构两台路由器上只能通过 NAT 地址转换来实现与总部的互访，但这样会与链路负载均衡冲突。NAT 的应用是发起的数据包经过路由器时，路由器才会建立 NAT 转换表，没有发起数据包经过，只有返回数据经过则路由器不会建立 NAT 转换表，而是直接选择丢弃。言而简之，如果通过 OSPF 动态路由协议调整 COST 值实现的话，分支机构两台路由器平时只有一台路由器工作，另一台路由器处于热备份状态，达不到负载均衡的效果。

OSPF 动态路由协议接口宣告的原则为只要将接口宣告，则不管这个接口的 IP 地址是否规范，由于分支机构内部服务器和部分客户端 IP 地址不规范，当分支机构内部互连出现故障自动切换时，与 OSPF 动态路由协议发生冲突，使得整个企业网路由变得混乱，导致网络瘫痪。

针对网络整合的需求，有三个问题需要解决：

(1) 总部与分支机构互连链路需要流量负载均衡方式，而不是只作主备关系；

(2) 分支机构内部路由器与交换机互连线路任何一条出现故障，均能快速自动切换；

(3) 分支机构中将规范的 IP 地址发布至总部网络，不规范的 IP 地址不发布，以免造成路由混乱。

2　设计和工作原理

针对以上网络需求，可用 Stateful NAT 和 OSPF 双进程相结合来实现。Stateful NAT 用于实现双路由器 NAT 同步，OSPF 双进程用于实现路由条目发布的控制。网络拓扑如图 1 所示。

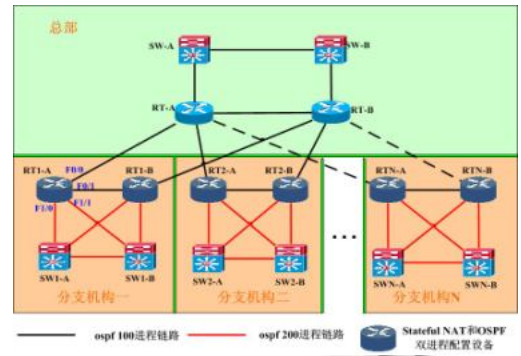

图 1　网络拓扑设计图

2.1 Stateful NAT 设计

在拥有双路由器多出口的情况下，可以在两台路由器间运行 stateful NAT[1]，其好处在于 NAT primary 路由器的 NAT 信息可以被 NAT backup 路由器接收到，NAT primary 路由器和 NAT backup 路由器之间通过 TCP 协议进行通讯。当 NAT primary 路由器失效后，NAT backup 路由器保存有 NAT 信息并接替上来，从而保证业务流量不中断。在分支机构两台路由器上启用 Stateful NAT 来实现 NAT 同步，这样不管那台路由器发起数据包，则为自动同步到另一台路由器上，解决了数据包发起和返回必须为同一台路由器的情况，即实现了链路流量负载均衡功能，又实现了双机冗余备份的功能。

2.2 Stateful Nat 配置

Stateful NAT 有两种配置方式：SNAT Primary/Backup、SNAT 和 HSRP 联动。SNAT Primary/Backup 配置方式是手动指定哪台路由器为 primary，哪台为 backup；和 HSRP 联动则由 HSRP 的状态来决定 SNAT 的 Primary/Backup 状态。选择 Stateful NAT 配置方式为手动指定的方式。以下以 RT1-A 为例进行配置：

2.2.1 配置 NAT 同步主备路由器[2]

```
ip nat Stateful id 1      //配置 Stateful id,RT1-B 上应配为 2
primary 172.16.1.61       //配置主路由器
 peer 172.16.1.62         //配置对等路由器
mapping-id 10             //配置 mapping-id，主要被下面 NAT 转换语句来引用定义
```

2.2.2 配置 NAT 转换地址池

```
ip nat pool wan 172.16.2.20 172.16.2.30
```

netmask 255.255.255.0 //配置地址池，wan 为地址池名称

ip nat inside source list 100 pool wan mapping-id 10 overload //配置 NAT，对控制列表 100 中符合要求的地址段则进行地址转换

2.2.3 配置 NAT 转换用访问控制列表

access-list 100 permit ip 192.168.0.0 0.0.255.255 any //配置控制列表，名称为 100

2.3 OSPF 双进程设计

OSPF 动态路由协议为基于链路状态的动态路由协议，当任何一条链路出现故障时，均可以通过 OSPF 路由动态进行切换，OSPF 进程与进程之间路由表是独立的。为了即要实现企业网内路由器、交换机动态路由切换和网络链路流量分担，同时又要保证分支机构不规范地址不发布，可通过采用 OSPF 双进程来实现。

OSPF 双进程就是在一台路由器上启用两个 OSPF 处理进程，每个 OSPF 进程有自己的接口和自己的 LSDB 数据库，在 UPDATE 数据库时也只描述自己进程所属的数据库。通过对双进程路由表策略性互导并打上标签来实现路由过滤和防止路由环路。

图 2 中路由器 RT1－A 有四个接口：F0/0、F2/1、F1/0、F1/1，其中端口 F0/1、F2/1 属于 OSPF 进程 100，F1/0、F1/1 属于 OSPF 进程 200，当 OSPF 100 发送 UPDATE 时，Router LSA 中仅描述 F0/0 和 F2/1，传给自己的邻居。同理 OSPF200 的 Router LSA 也只描述 F1/0 和 F1/1。那么结果就是 OSPF 100 的邻居 RT－A、RT－B 只能学到 OSPF 100 的数据库里的路由，OSPF200 的邻居 SW1－A、SW1－B 只能学到 OSPF200 数据库里的路由，不同进程内的设备没有到达对端的路由信息，起到了很好地路由隔离作用[3]。

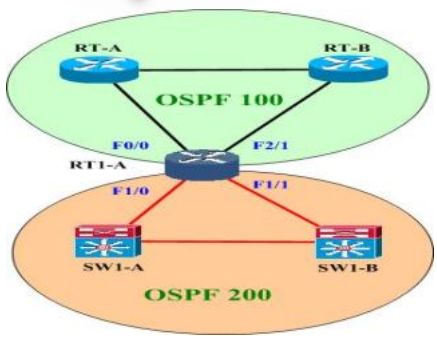

图 2 OSPF 多进程示意图

2.4 OSPF 双进程设备配置

设备配置只在分支机构设备上进行，总部路由器和交换机配置不作变动。Stateful NAT 和 OSPF 双进程配置只需对分支机构路由器 RT1－A、RT1－B、RT2－A 和 RT2－B 上配置即可。在 SW1－A、SW1－B、SW2－A 和 SW2－B 三层交换机上启用 OSPF 路由。企业网中规范 IP 地址段为 172.0.0.0/8，分支机构一规范 IP 地址段为 172.46.0.0/16，不规范 IP 地址段为 192.168.0.0/16。

路由器 RT1-A 有四个接口，其中与总部相连的接口(F0/0、F0/1)属于 OSPF 进程 100，与三层交换机相连的接口(F1/0、F1/1)属于 OSPF 进程 200。

2.4.1 接口 COST 值设置

Interface f0/0 //配置 F0/0 接口

Ip ospf cost 1 //设置 OSPF COST 值为 1

Interface f0/1 //配置 F0/0 接口

Ip ospf cost 1 //设置 OSPF COST 值为 1

2.4.2 创建 OSPF 进程 100

router ospf 100 //启动 OSPF 进程，进程号为 100，注意：进程号在本地路由器有效

redistribute ospf 200 subnets tag 3 route-map fenzi1 //将 OSPF 进程 200 的路由经过过滤后再发布至 OSPF 100，并打上标签 3(在 RT1－B 路由器上打的标签为 4)，路由过滤规则名称为 fenzi1

network 172.16.67.6 0.0.0.0 area 1 //设置 OSPF 通告的网络范围，将对 F0/0 接口通告

network 172.16.67.61 0.0.0.0 area 1 //设置 OSPF 通告的网络范围，将对 F0/1 接口通告

distribute-list route-map disloop in //对路由表进行过滤，根据 route-map disloop 里的条件进行过滤

2.4.3 创建 OSPF 进程 200[4]

router ospf 200 //启动 OSPF 进程，进程号为 200

redistribute ospf 100 subnets tag 3 route-map zhongbu //将 OSPF 进程 100 的路由经过过滤后再发布至 OSPF 100，并打上标签 3(在 RT1－B 路由器上打的标签为 4)，路由过滤规则名

称为 zhongbu

network 192.168.158.69 0.0.0.0 area 0 //设置 OSPF 通告的网络范围，将对 F1/0 接口通告

network 192.168.158.73 0.0.0.0 area 0 //设置 OSPF 通告的网络范围，将对 F1/1 接口通告

distribute-list route-map disloop in //对路由表进行过滤，根据 route-map disloop 里的条件进行过滤

2.4.4 创建路由过滤规则[5]

access-list 12 permit 172.0.0.0 0.255.255.255 //总部及其它分支机构规范的 IP 地址网段

route-map zhongbu permit 10 //创建路由过滤规则，名称为 zhongbu

match ip address 12 //符合 access-list 12 规则的地址段被接受，其它地址段被拒绝!

access-list 11 permit 172.46.0.0 0.0.255.255 //分支机构一规范的 IP 地址网段

route-map fenzi1 permit 10 //创建路由过滤规则，名称为 fenzi1

match ip address 11 //符合 access-list 11 规则的地址段被接受，其它地址段被拒绝

route-map disloop deny 10 //创建路由过滤规则，名称为 disloop

match tag 4 //路由表打了标签 4 的路由被拒绝

route-map disloop permit 20 //路由过过滤规则 disloop 其它路由全部接受

在RT1-A路由器OSPF 100的路由表导入OSPF 200，并打上 Tag 3，拒绝 Tag 4。OSPF 200 通过过滤的方法将需要的路由导入 OSPF 100，防止私有地址发布至 OSPF 100，导入的路由打上 Tag 3，拒绝 Tag 4。在 RT1-B 路由器 OSPF 100 导入 OSPF 200 打上 Tag 4，拒绝 Tag 3，来防止路由环路。

3 结语

本文叙述了采用 Stateful NAT 和标准 OSPF 路由协议进行网络整合中广域链路的设计和实现的过程，并按照路由进行分发、过滤和控制，虽然配置相对比较复杂，需要占用大量的处理器资源，但达到了路由设计要求，在浙江中烟工业有限责任公司的网络整合项目中得到顺利实施和验证，为大型企业在兼并过程中的网络整合工作提供了一个较为成功的案例。为了提高广域网链路的可靠性和安全性，建议分支机构链路采用两个不同运营商线路与总部核心路由器相连。

参考文献

1 CCF 精品技术论坛. Internet 多出口实例分析(二) [2009-3-23].http://bbs.et8.net/bbs/showthread.php?t=512788

2 思科公司. Stateful Failover of Network Address Translation (SNAT) Phase 1 [2009-3-22]. http://www.cisco.com/en/US/docs/ios/12_2t/12_2t13/feature/guide/ftsnat.html

3 王建明.OSPF 路由协议双进程规划及其实现.中国科技信息, 2008,(7):119－120.

4 Parkhurst WR. Cisco OSPF 命令与配置手册.北京:人民邮电出版社, 2003,3:281－292.

5 Jeff Doyle.TCP/IP 路由技术(第一卷).北京:人民邮电出版社, 2003. 525－537.