

# 基于策略路由和 NAT 的多出口校园网仿真实验设计

叶沿飞

贵州电子信息职业技术学院, 中国·贵州 凯里 556000

**摘要:** 随着高校广大师生教学、学习等行为对互联网的需求剧增, 原有一条 ISP 出口链路已不能满足校园网日常应用需求, 很多高校会租用多条 ISP 出口链路。一是可以提供校园网出口链路冗余备份, 二是可以增加校园网出口带宽。论文提出了利用策略路由和网络地址转换技术构建多出口校园网, 并进行仿真实验设计, 不仅给出了详细的配置过程, 而且还模拟了在出口链路发生故障情况下, 数据包的路由过程。验证了策略路由和 NAT 方案可以实现多出口校园网链路备份和负载均衡, 满足了校园网日常应用需求。

**关键词:** 策略路由; NAT; 负载均衡

## Design of Multi Exit Campus Network Simulation Experiment Based on Policy Routing and NAT

Yanfei Ye

GuiZhou Vocational Technology College of Electronics & Information, Kaili, Guizhou, 556000, China

**Abstract:** With the sharp increase in the demand for the Internet from teaching, learning and other behaviors of teachers and students in colleges and universities, the original ISP export link can no longer meet the daily application needs of campus networks, and many colleges and universities will rent multiple ISP export links. One is to provide redundant backup of campus network exit links, and the other is to increase the bandwidth of campus network exits. The paper proposes the construction of a multi exit campus network using strategy routing and network address translation technology, and conducts simulation experiment design. It not only provides a detailed configuration process, but also simulates the routing process of data packets in the event of a failure in the exit link. Verified that the strategy routing and NAT scheme can achieve multi exit campus network link backup and load balancing, meeting the daily application needs of the campus network.

**Keywords:** policy routing; NAT; load balancing

### 1 引言

目前, 校园网已成为各大院校保障广大师生教学、科研、学习、生活等的重要基础设施, 当校园网用户需要访问校外资源时, 由于受限于中国各大运营商网络互联互通的瓶颈, 通常采用的校园网方案是使用多个网络出口。论文提出了一种基于策略路由和网络地址转换技术的解决方案。其中, 应用网络地址转换技术是保证校园网用户对互联网资源的访问, 而策略路由的应用则主要是为了实现流量负载均衡和链路备份。

### 2 网络地址转换 NAT

众所周知, 公有网络数据包的转发基本是由路由器来完成的, Internet 上的路由器中只有到达公网的路由表, 没有到达私网的路由表, 因此内部网络的私有地址如果想访问互联网资源就需要应用网络地址转换 NAT (Network Address Translation), 将私有 IP 地址转换为合法的公有 IP 地址。NAT 技术的应用有效地解决了内部网络私有 IP 地址如何访问 Internet 的难题, 同时也极大的缓解了 IPv4 地址的不足, 有效的隐藏内网主机, 避免遭受来自互联网的攻击。

### 3 策略路由 PBR

策略路由 PBR (Policy Based Routing) 是一种比基于路由表更加灵活的数据包路由转发机制, 可以依靠某种人为定义的策略来进行路由, 而不是依靠路由协议。策略路由是一种入站机制, 用于入站的 IP 数据包, 使用策略路由后, 能够根据数据包的源地址、目的地址、端口号、协议类型让报文选择不同的路径。符合策略路由的 IP 数据包按照策略中定义的操作进行处理, 而不符合策略路由的 IP 数据包将按照通常的路由表进行路由转发。

### 4 搭建策略路由和 NAT 双出口实验拓扑

校园网策略路由和 NAT 双出口仿真实验拓扑如图 1 所示, 实验应用场景: 某学校校园网采用双出口接入 Internet, 拥有电信、联通两条出口链路, 内网分为宿舍区和教学区, 宿舍区属于 VLAN10, 教学区属于 VLAN20, 环回口 101.1.1.1/24 和 202.1.1.1/24 模拟互联网中的两台服务器。现规划设计通过策略路由实现冗余链路, 当任何一条链路故障时, 能够自动切换保证校园网用户正常上网, 同时为了让宿舍区和教学区私网用户能正常访问 Internet, 在出口路由器 CoreRT 上配置网络地址转换 NAT。

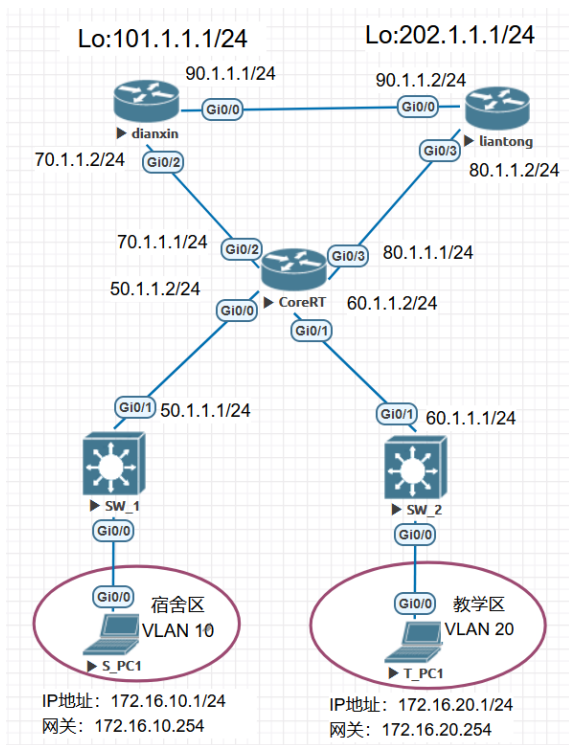


图 1 拓扑和 IP 地址规划

## 5 配置方案

步骤一：内网基础配置。

①设置宿舍区 S\_PC1 和教学区 T\_PC1 的 IP 地址与默认网关（使用路由器模拟 PC）。

```
S_PC1(config)#int g0/0
S_PC1(config-if)#ip addr 172.16.10.1 255.255.255.0
S_PC1(config-if)#no shut
S_PC1(config)#ip route 0.0.0.0 0.0.0.0 172.16.10.254
T_PC1(config)#int g0/0
T_PC1(config-if)#ip addr 172.16.20.1 255.255.255.0
T_PC1(config-if)#no shut
T_PC1(config)#ip route 0.0.0.0 0.0.0.0 172.16.20.254
```

② SW\_1 交换机 VLAN、接口 IP 与路由配置。

```
SW_1(config)#vlan 10
SW_1(config-vlan)#exit
SW_1(config)#int g0/0
SW_1(config-if)#switchport mode access
SW_1(config-if)#switchport access vlan 10
SW_1(config-if)#exit
SW_1(config)#int vlan 10
SW_1(config-if)#ip addr 172.16.10.254 255.255.255.0
SW_1(config-if)#no shut
```

```
SW_1(config-if)#int g0/1
SW_1(config-if)#no switchport
SW_1(config-if)#ip addr 50.1.1.1 255.255.255.0
SW_1(config-if)#no shut
SW_1(config-if)#exit
SW_1(config)#ip routing
SW_1(config)#router ospf 10
SW_1(config-router)#net 172.16.10.0 0.0.0.255 area 0
SW_1(config-router)#net 50.1.1.0 0.0.0.255 area 0
```

③ SW\_2 交换机 VLAN、接口 IP 地址与路由配置。

```
SW_2(config)#vlan 20
SW_2(config-vlan)#exit
SW_2(config)#interface g0/0
SW_2(config-if)#switchport mode access
SW_2(config-if)#switchport access vlan 20
SW_2(config-if)#exit
SW_2(config)#int vlan 20
SW_2(config-if)#ip addr 172.16.20.254 255.255.255.0
SW_2(config-if)#no shut
SW_2(config-if)#int g0/1
SW_2(config-if)#no switchport
SW_2(config-if)#ip addr 60.1.1.1 255.255.255.0
SW_2(config-if)#no shut
SW_2(config-if)#exit
SW_2(config)#ip routing
SW_2(config)#router ospf 10
SW_2(config-router)#net 60.1.1.0 0.0.0.255 area 0
SW_2(config-router)#net 172.16.20.0 0.0.0.255 area 0
```

④出口路由器 CoreRT 接口 IP 与路由配置。

```
CoreRT(config)#int g0/0
CoreRT(config-if)#ip addr 50.1.1.2 255.255.255.0
CoreRT(config-if)#no shut
CoreRT(config-if)#int g0/1
CoreRT(config-if)#ip addr 60.1.1.2 255.255.255.0
CoreRT(config-if)#no shut
CoreRT(config-if)#exit
CoreRT(config)#router ospf 10
CoreRT(config-router)#net 50.1.1.0 0.0.0.255 area 0
CoreRT(config-router)#net 60.1.1.0 0.0.0.255 area 0
CoreRT(config-router)#default-information originate
always
```

步骤二：外网基础配置。

①出口路由器 CoreRT 上配置接口和启用 RIP 路由协议。

```
CoreRT(config)#int g0/2
CoreRT(config-if)#ip addr 70.1.1.1 255.255.255.0
CoreRT(config-if)#no shut
CoreRT(config-if)#int g0/3
CoreRT(config-if)#ip addr 80.1.1.1 255.255.255.0
CoreRT(config-if)#no shut
CoreRT(config-if)#exit
CoreRT(config)#router rip
CoreRT(config-router)#ver 2
CoreRT(config-router)#no auto-summary
CoreRT(config-router)#net 70.0.0.0
CoreRT(config-router)#net 80.0.0.0
```

② dianxin 路由器上配置接口和启用 RIP 路由协议。

```
dianxin(config)#int loopback 0
dianxin(config-if)#ip addr 101.1.1.1 255.255.255.0
dianxin(config-if)#no shut
dianxin(config-if)#int g0/2
dianxin(config-if)#ip addr 70.1.1.2 255.255.255.0
dianxin(config-if)#no shut
dianxin(config-if)#int g0/0
dianxin(config-if)#ip addr 90.1.1.1 255.255.255.0
dianxin(config-if)#no shut
dianxin(config-if)#exit
dianxin(config)#router rip
dianxin(config-router)#ver 2
dianxin(config-router)#no auto-summary
dianxin(config-router)#net 101.0.0.0
dianxin(config-router)#net 70.0.0.0
dianxin(config-router)#net 90.0.0.0
```

③ liantong 路由器上配置接口和启用 RIP 协议。

步骤三：CoreRT 路由器上配置策略路由。

```
CoreRT(config)#int g0/0
CoreRT(config-if)#ip nat inside
CoreRT(config-if)#int g0/1
CoreRT(config-if)#ip nat inside
CoreRT(config-if)#int g0/2
CoreRT(config-if)#ip nat outside
CoreRT(config-if)#int g0/3
CoreRT(config-if)#ip nat outside
CoreRT(config-if)#exit
CoreRT(config)#ip nat inside source route-map dianxin
interface g0/2 overload
CoreRT(config)#ip nat inside source route-map liantong
interface g0/3 overload
```

步骤四：CoreRT 路由器上配置 NAT。

```
CoreRT(config)#access-list 10 permit 172.16.10.0
0.0.0.255
CoreRT(config)#access-list 20 permit 172.16.20.0
0.0.0.255
CoreRT(config)#route-map fenliu permit 10 // 定义策略路由图
CoreRT(config-route-map)#match ip address 10 // 匹配第一条访问控制列表的流量
CoreRT(config-route-map)#set ip next-hop 70.1.1.2
80.1.1.2 // 下一跳
CoreRT(config-route-map)#exit
CoreRT(config)#route-map fenliu permit 20
CoreRT(config-route-map)#match ip address 20 // 匹配第二条访问控制列表的流量
CoreRT(config-route-map)#set ip next-hop 80.1.1.2
70.1.1.2 // 下一跳
CoreRT(config-route-map)#exit
CoreRT(config)#int g0/0
CoreRT(config-if)#ip policy route-map fenliu
CoreRT(config-if)#int g0/1
CoreRT(config-if)#ip policy route-map fenliu
CoreRT(config-if)#exit
CoreRT(config)#route-map dianxin permit 10
CoreRT(config-route-map)#match interface g0/2 // 定义策略路由图，匹配 g0/2
CoreRT(config-route-map)#exit
CoreRT(config)#route-map liantong permit 20 // 定义策略路由图，匹配 g0/3
CoreRT(config-route-map)#match interface g0/3
```

## 6 效果验证

①使用 ping 命令和 traceroute 命令，验证宿舍区和教学区用户均能正常访问网络服务。如图 2 (a) 和图 2 (b) 所示。

②冗余性测试，将出口路由器 CoreRT 接口 G0/2 接口 shutdown, G0/3 口正常时, S\_PC1 和 T\_PC1 均能正常切换链路, 实现冗余, 以 S\_PC1 为例, ping 和 traceroute 命令执行结果如图 3 所示。

```
S_PC1#ping 101.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 101.1.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/9/15 ms
S_PC1#ping 202.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 202.1.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 5/8/14 ms
S_PC1#traceroute 101.1.1.1
Type escape sequence to abort.
Tracing the route to 101.1.1.1
VRF info: (vrf in name/id, vrf out name/id)
 1 172.16.10.254 9 msec 8 msec 7 msec
 2 50.1.1.2 8 msec 7 msec 7 msec
 3 70.1.1.2 11 msec 10 msec *
S_PC1#traceroute 202.1.1.1
Type escape sequence to abort.
Tracing the route to 202.1.1.1
VRF info: (vrf in name/id, vrf out name/id)
 1 172.16.10.254 12 msec 6 msec 6 msec
 2 50.1.1.2 7 msec 7 msec 10 msec
 3 70.1.1.2 16 msec 15 msec 15 msec
 4 90.1.1.2 18 msec 11 msec *
```

图 2 (a) 宿舍区用户正常访问网络服务

```
T_PC1#ping 101.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 101.1.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/11/15 ms
T_PC1#ping 202.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 202.1.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 10/12/16 ms
T_PC1#traceroute 101.1.1.1
Type escape sequence to abort.
Tracing the route to 101.1.1.1
VRF info: (vrf in name/id, vrf out name/id)
 1 172.16.20.254 6 msec 13 msec 6 msec
 2 60.1.1.2 5 msec 6 msec 8 msec
 3 80.1.1.2 12 msec 15 msec 10 msec
 4 90.1.1.1 14 msec 14 msec *
T_PC1#traceroute 202.1.1.1
Type escape sequence to abort.
Tracing the route to 202.1.1.1
VRF info: (vrf in name/id, vrf out name/id)
 1 172.16.20.254 6 msec 4 msec 4 msec
 2 60.1.1.2 11 msec 8 msec 7 msec
 3 80.1.1.2 13 msec 12 msec *
```

图 2 (b) 教学区用户正常访问网络服务

```
S_PC1#ping 101.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 101.1.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 9/10/12 ms
S_PC1#ping 202.1.1.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 202.1.1.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 6/7/9 ms
S_PC1#traceroute 101.1.1.1
Type escape sequence to abort.
Tracing the route to 101.1.1.1
VRF info: (vrf in name/id, vrf out name/id)
 1 172.16.10.254 5 msec 6 msec 5 msec
 2 50.1.1.2 7 msec 10 msec 7 msec
 3 80.1.1.2 11 msec 13 msec 17 msec
 4 90.1.1.1 18 msec 14 msec *
S_PC1#traceroute 202.1.1.1
Type escape sequence to abort.
Tracing the route to 202.1.1.1
VRF info: (vrf in name/id, vrf out name/id)
 1 172.16.10.254 5 msec 8 msec 5 msec
 2 50.1.1.2 8 msec 8 msec 9 msec
 3 80.1.1.2 16 msec 10 msec *
```

图 3 S\_PC1 冗余性测试

## 7 结语

通过在校园网出口路由器上应用策略路由 PBR 与网络地址转换 NAT，完美的实现了校园网多出口方案，提高了校园网用户访问公网资源的速度，增强了校园网出口链路的可靠性和冗余性。

### 参考文献:

- [1] 李刚.策略路由在高校网络多应用场景中的应用——以朝阳师范高等专科学校校园网为例[J].辽宁师专学报:自然科学版,2023,25(1):58-63.
- [2] 李雨江.NAT仿真实验在Packet Tracer中的设计与实现[J].电脑知识与技术:学术版,2020,16(28):4.