使用基本 ACL 限制公司网络访问

1. 项目背景

Jan16 公司有开发部、市场部和财务部，各有计算机若干台、财务系统服务器 1 台，使用三层交换机进行局域网组建，并通过路由器连接至外部网络。出于数据安全的考虑，需要在交换机上进行访问控制。项目拓扑如图 1 所示。具体要求如下：

（1） SW1 上为开发部、市场部、财务部及财务系统分别创建了 VLAN10、20、30、40；

（2） 要求财务系统服务器仅允许财务部进行访问；

（3） 财务系统服务器仅在内网使用，不允许访问外部网络；

（4） 测试计算机、交换机和路由器的 IP 和接口信息如拓扑所示。

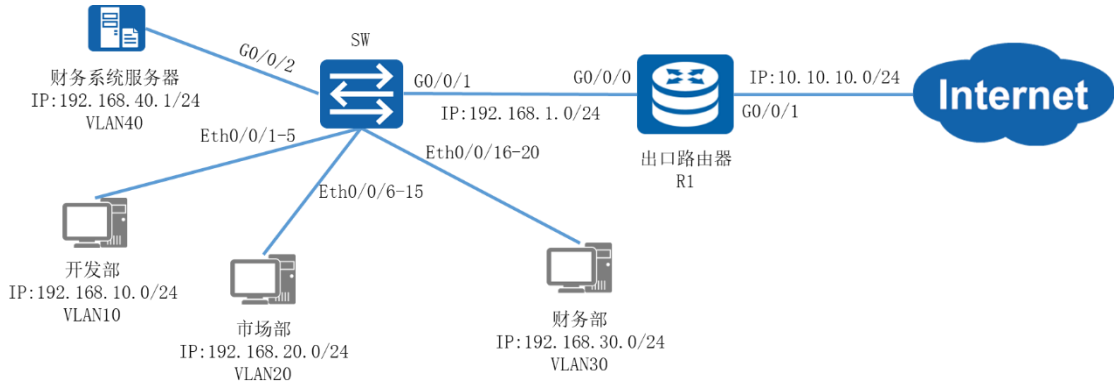

图 1 网络拓扑图

2. 项目规划设计

三层交换机的访问控制策略主要是通过 ACL 访问控制列表对不同 VLAN 的 IP 地址段进行流量匹配控制。标准 ACL 可以对 IP 包进行源地址匹配，即检查通过 IP 包中的源地址信息，如果源地址与 ACL 中的规则相匹配，就执行放行或拦截的操作。为了让其它部门无法访问财务系统服务器，可以在三层交换机中配置匹配财务部 IP 地址段、拒绝其他所有 IP 的 ACL，并在 G0/0/2 接口的 OUT 方向上应用；同时在添加拒绝财务部系统服务器 IP 地址段的 ACL，在 G0/0/1 接口的 OUT 方向上应用，组织财务部系统服务器访问外部网络。外部网络连接方面，三层交换机配置默认路由指向出口路由器。出口路由器可根据 ISP 接入方式采用对应的路由协议，这里不作描述。

配置步骤如下：

（1） 配置交换机基础环境

（2） 配置路由器基础环境

（3） 配置基本 ACL 访问控制

（4） 配置各部门计算机的 IP 地址

具体规划如下表：

表 1 VLAN 规划表

VLAN ID	IP 地址段	用途
VLAN10	192.168.10.0/24	开发部
VLAN20	192.168.20.0/24	市场部
VLAN30	192.168.30.0/24	财务部
VLAN40	192.168.40.0/24	财务系统

VLAN50	192.168.1.0/24	连接外部网络

表 2 IP 地址规划表

设备	接口	IP 地址
R1	G0/0/0	192.168.1.1/24
R1	G0/0/1	10.10.10.1/24
SW1	VLANIF10	192.168.10.254/24
SW1	VLANIF20	192.168.20.254/24
SW1	VLANIF30	192.168.30.254/24
SW1	VLANIF40	192.168.40.254/24
SW1	VLANIF50	192.168.1.254/24
财务系统服务器	Eth0/0/1	192.168.40.1/24
开发部	Eth0/0/1	192.168.10.1/24
市场部	Eth0/0/1	192.168.20.1/24
财务部	Eth0/0/1	192.168.30.1/24

表 3 端口规划表

本端设备	本端接口	对端设备	对端接口
SW	E0/0/1-5	开发部 PC	Eth0/0/1
SW	E0/0/6-15	市场部 PC	Eth0/0/1
SW	E0/0/16-20	财务部 PC	Eth0/0/1
SW	G0/0/2	财务系统	Eth0/0/1
SW	G0/0/1	R1	G0/0/0
R1	G0/0/0	SW	G0/0/1
R1	G0/0/1	Internet	Null
财务系统服务器	Eth0/0/1	SW	G0/0/2
开发部	Eth0/0/1	SW	Eth0/0/1-5
市场部	Eth0/0/1	SW	Eth0/0/6-15
财务部	Eth0/0/1	SW	Eth0/0/16-20

3.项目实施

（1）配置交换机基础环境

①为各部门创建相应的 VLAN

```
<Huawei>system-view
[Huawei]sysname SW1
[SW1]vlan batch 10 20 30 40 50
```

②将各部门计算机所使用的端口类型转换为 ACCESS 模式，并设置接口 PVID，将端口划分到相应的 VLAN

```
[SW1]port-group group-member Ethernet 0/0/1 to Ethernet 0/0/5
[SW1-port-group]port link-type access
[SW1-port-group]port default vlan 10
[SW1-port-group]quit
[SW1]port-group group-member Ethernet 0/0/6 to Ethernet 0/0/15
[SW1-port-group]port link-type access
```

```
[SW1-port-group]port default vlan 20
[SW1-port-group] quit
[SW1]port-group group-member Ethernet 0/0/16 to Ethernet 0/0/20
[SW1-port-group]port link-type access
[SW1-port-group]port default vlan 30
[SW1-port-group] quit
[SW1]interface G0/0/2
[SW1-GigabitEthernet0/0/2]port link-type access
[SW1-GigabitEthernet0/0/2]port default vlan 40
[SW1-port-group] quit
[SW1]interface G0/0/1
[SW1-GigabitEthernet0/0/1]port link-type access
[SW1-GigabitEthernet0/0/1]port default vlan 50
[SW1-port-group] quit
```

③配置 vlanif 接口的 IP 地址，作为各部门的网关

```
[SW1]interface Vlanif 10
[SW1-Vlanif10]ip add 192.168.10.254 24
[SW1]interface Vlanif 20
[SW1-Vlanif20]ip add 192.168.20.254 24
[SW1]interface Vlanif 30
[SW1-Vlanif30]ip add 192.168.30.254 24
[SW1]interface Vlanif 40
[SW1-Vlanif40]ip add 192.168.40.254 24
[SW1]interface Vlanif 50
[SW1-Vlanif50]ip add 192.168.1.254 24
```

④配置交换机默认路由

```
[SW1]ip route-static 0.0.0.0 0.0.0.0 192.168.1.1
```

（2）配置路由器基础环境

①配置路由器接口 IP 地址

```
[Huawei]system-view
[Huawei]sysname R1
[R1]int G0/0/0
[R1-GigabitEthernet0/0/0]ip add 192.168.1.1 24
[R1]int G0/0/1
[R1-GigabitEthernet0/0/1]ip add 10.10.10.1 24
```

②配置路由器静态路由

```
[R1]ip route-static 192.168.10.0 255.255.255.0 192.168.1.254
[R1]ip route-static 192.168.20.0 255.255.255.0 192.168.1.254
[R1]ip route-static 192.168.30.0 255.255.255.0 192.168.1.254
[R1]ip route-static 192.168.40.0 255.255.255.0 192.168.1.254
```

（3）配置基本 ACL 控制访问

①在交换机上配置 ACL 规则，允许数据包源网段为 192.168.30.0 的报文通过。将规则

应用到 G0/0/2 的端口上。

```
[SW1]acl 2000
[SW1-acl-basic-2000]rule permit source 192.168.30.0 0.0.0.255
[SW1-acl-basic-2000]rule deny
[SW1]int G0/0/2
[SW1-GigabitEthernet0/0/2]traffic-filter outbound acl 2000
```

②在交换机上配置 ACL 规则，拒绝数据包源网段为 192.168.40.0 的报文通过。将规则应用到 G0/0/1 的端口上。

```
[SW1]acl 2001
[SW1-acl-basic-2001]rule deny source 192.168.40.0 0.0.0.255
[SW1]int G0/0/1
[SW1-GigabitEthernet0/0/1]traffic-filter outbound acl 2001
```

（4）配置各部门计算机的 IP 地址

图 2 财务系统服务器 IP 配置图

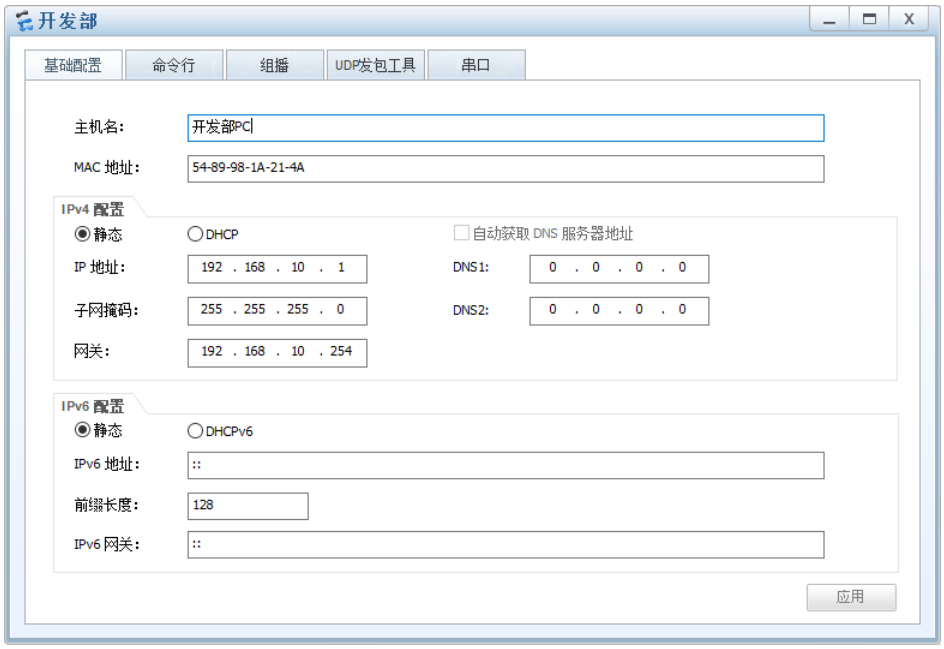

图 3 开发部 PC IP 配置图

图 4 市场部 PC IP 配置图

图 5 财务部 PC IP 配置图

4. 项目验证

（1）查看访问控制列表

① SW1 的配置

```
[SW1]display acl all
 Total nonempty ACL number is 2

Basic ACL 2000, 2 rules
Acl's step is 5
 rule 5 permit source 192.168.30.0 0.0.0.255
 rule 10 deny

Basic ACL 2001, 1 rule
Acl's step is 5
 rule 5 deny source 192.168.40.0 0.0.0.255
```

（2）测试各部门计算机的互通性

通过 Ping 命令，测试各部门内部通信息的情况。

使用开发部计算机 Ping 市场部及财务部的计算机:

```
PC>ping 192.168.20.1

Ping 192.168.20.1: 32 data bytes, Press Ctrl_C to break
From 192.168.20.1: bytes=32 seq=1 ttl=127 time=47 ms
From 192.168.20.1: bytes=32 seq=2 ttl=127 time=47 ms
From 192.168.20.1: bytes=32 seq=3 ttl=127 time=31 ms
From 192.168.20.1: bytes=32 seq=4 ttl=127 time=31 ms
```

```
From 192.168.20.1: bytes=32 seq=5 ttl=127 time=31 ms

--- 192.168.20.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 31/37/47 ms

PC>ping 192.168.30.1

Ping 192.168.30.1: 32 data bytes, Press Ctrl_C to break
From 192.168.30.1: bytes=32 seq=1 ttl=127 time=32 ms
From 192.168.30.1: bytes=32 seq=2 ttl=127 time=31 ms
From 192.168.30.1: bytes=32 seq=3 ttl=127 time=47 ms
From 192.168.30.1: bytes=32 seq=4 ttl=127 time=31 ms
From 192.168.30.1: bytes=32 seq=5 ttl=127 time=31 ms

--- 192.168.30.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 31/34/47 ms
```

(3) 测试各部门与财务系统的连接性

使用开发部的计算机 Ping 财务系统：

```
PC>ping 192.168.40.1

Ping 192.168.40.1: 32 data bytes, Press Ctrl_C to break
Request timeout!
Request timeout!
Request timeout!
Request timeout!
Request timeout!

--- 192.168.40.1 ping statistics ---
  5 packet(s) transmitted
  0 packet(s) received
  100.00% packet loss
```

使用财务部的计算机 Ping 财务系统：

```
PC>ping 192.168.40.1

Ping 192.168.40.1: 32 data bytes, Press Ctrl_C to break
From 192.168.40.1: bytes=32 seq=1 ttl=127 time=47 ms
From 192.168.40.1: bytes=32 seq=2 ttl=127 time=31 ms
```

```
From 192.168.40.1: bytes=32 seq=3 ttl=127 time=32 ms
From 192.168.40.1: bytes=32 seq=4 ttl=127 time=31 ms
From 192.168.40.1: bytes=32 seq=5 ttl=127 time=47 ms

--- 192.168.40.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 31/37/47 ms
```

可以观察到其他部门无法连接到财务系统服务器上,唯有财务部可以连接到财务系统上。

(4) 测试外部网络的连通性

通过 Ping 命令，测试各部门 PC 及财务系统服务器是否能够访问外网。

使用开发部的计算机 Ping 外部网络：

```
PC>ping 10.10.10.1

Ping 10.10.10.1: 32 data bytes, Press Ctrl_C to break
From 10.10.10.1: bytes=32 seq=1 ttl=254 time=31 ms
From 10.10.10.1: bytes=32 seq=2 ttl=254 time=47 ms
From 10.10.10.1: bytes=32 seq=3 ttl=254 time=31 ms
From 10.10.10.1: bytes=32 seq=4 ttl=254 time=47 ms
From 10.10.10.1: bytes=32 seq=5 ttl=254 time=31 ms

--- 10.10.10.1 ping statistics ---
  5 packet(s) transmitted
  5 packet(s) received
  0.00% packet loss
  round-trip min/avg/max = 31/37/47 ms
```

使用财务系统服务器 Ping 外部网络：

```
PC>ping 10.10.10.1

Ping 10.10.10.1: 32 data bytes, Press Ctrl_C to break
Request timeout!
Request timeout!
Request timeout!
Request timeout!
Request timeout!

--- 10.10.10.1 ping statistics ---
  5 packet(s) transmitted
  0 packet(s) received
  100.00% packet loss
```

可以观察到到其他部门均能访问外部网络，唯有财务系统服务器无法访问外部网络。