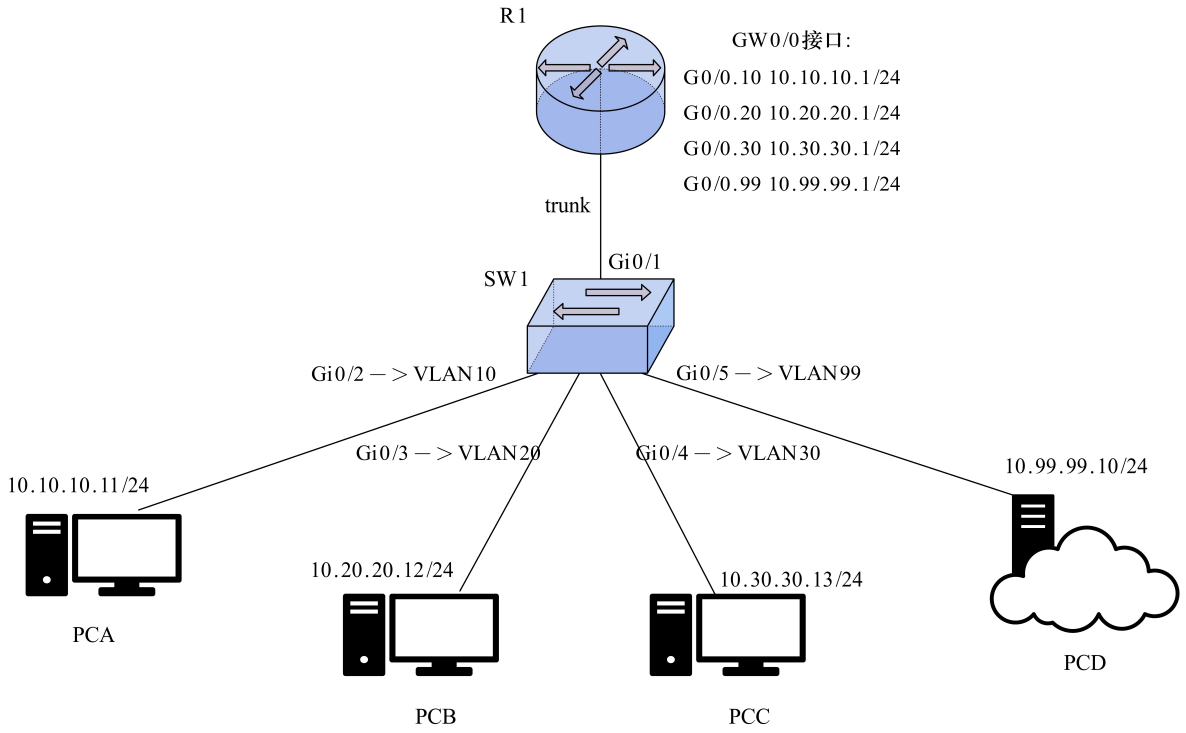
# 企业局域网分部门隔离与公共服务器访问

## 设计方案

仅使用 1 台路由器（R1）与 1 台二层交换机（SW1）。R1 上配置 4 个子接口（或物理接口绑定子网），分别作为市场部、人事部、财务部与服务器网段的网关；SW1 侧为各主机提供 Access 端口并把端口划入对应 VLAN。通过 R1 的 ACL 限制跨网段访问，只允许各部门到服务器地址，其余互访拒绝。




## 操作步骤与配置命令

1. 路由器 R1：子接口与三层转发

```
interface GigabitEthernet0/0.10
 encapsulation dot1q 10
 ip address 10.10.10.1 255.255.255.0
interface GigabitEthernet0/0.20
 encapsulation dot1q 20
 ip address 10.20.20.1 255.255.255.0
interface GigabitEthernet0/0.30
 encapsulation dot1q 30
 ip address 10.30.30.1 255.255.255.0
interface GigabitEthernet0/0.99
 encapsulation dot1q 99
 ip address 10.99.99.1 255.255.255.0
no shut
```

2. 交换机 SW1：VLAN 与端口

```
vlan 10
 name DEPT_MARKET
vlan 20
 name DEPT_HR
```

```
vlan 30
 name DEPT_FIN
vlan 99
 name SERVER_NET

interface GigabitEthernet0/1   ! 上联到 R1（Trunk）
 switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk allowed vlan 10,20,30,99

interface GigabitEthernet0/2   ! PCA
 switchport mode access
 switchport access vlan 10
interface GigabitEthernet0/3   ! PCB
 switchport mode access
 switchport access vlan 20
interface GigabitEthernet0/4   ! PCC
 switchport mode access
 switchport access vlan 30
interface GigabitEthernet0/5   ! PCD
 switchport mode access
 switchport access vlan 99
```

1. R1 上 ACL：仅允许到服务器地址，其余拒绝

```
ip access-list extended DEPT_TO_SERVER
 permit ip 10.10.10.0 0.0.0.255 host 10.99.99.10
 permit ip 10.20.20.0 0.0.0.255 host 10.99.99.10
 permit ip 10.30.30.0 0.0.0.255 host 10.99.99.10
 deny   ip any any

interface GigabitEthernet0/0.10
 ip access-group DEPT_TO_SERVER in
interface GigabitEthernet0/0.20
 ip access-group DEPT_TO_SERVER in
interface GigabitEthernet0/0.30
 ip access-group DEPT_TO_SERVER in
```

4. 终端 IP 设置：

- PCA：`10.10.10.11/24`，GW `10.10.10.1`
- PCB：`10.20.20.12/24`，GW `10.20.20.1`
- PCC：`10.30.30.13/24`，GW `10.30.30.1`
- PCD：`10.99.99.10/24`，GW `10.99.99.1`

# 实验结果与分析

- 部门间互不可达：从任一部门到另两个部门 IP 的访问被 ACL 拒绝（例如 PCA→PCB/PCC ping 超时）。
- 可访问公共服务器：从各部门到 PCD 能成功（ping/curl/http）。

# 结论

使用“1 台路由器 + 1 台交换机”即可实现部门隔离与公共服务器访问：路由器子接口作为各网关，交换机提供 VLAN 接入，R1 上 ACL 精准放行到服务器地址，达成需求且实现简洁清晰。