一台华为路由器作为出口核心路由器，IP地址为192.168.0.1，与核心交机的g0/0/1接口连接；有一台核心交换机，规划接NAS设备与文件服务器等，规划端口为g0/0/2-7号端口，规划IP地址为192.168.1.X段IP地址；核心交换机的g0/0/8-16口规划用作接财务用的电脑，规划192.168.2.X段IP地址；核心交换机的g0/0/17-24口规划用作接财务用的电脑，规划192.168.2.X段IP地址。要求所有设备均能通过192.168.0.1路由器上网，同时财务电脑与技术部电脑都能正常访问192.168.1.X段设备，但财务电脑与技术部电脑相互之间不能互相通讯。



华为网络隔离配置方案

基于您的网络架构（路由器出口IP 192.168.0.1，核心交换机直连服务器、财务和技术部终端），通过‌VLAN划分+ACL策略‌实现需求：

‌VLAN规划‌：

VLAN 10：服务器段（192.168.1.0/24），网关192.168.1.1

VLAN 20：财务电脑段（192.168.2.0/24），网关192.168.2.1

VLAN 30：技术部电脑段（192.168.3.0/24），网关192.168.3.1

‌隔离逻辑‌：

财务（VLAN 20）与技术部（VLAN 30）二层隔离（不同广播域）

通过路由器ACL阻断三层互访，但允许两者访问服务器段和上网512

‌配置步骤‌

‌1. 核心交换机配置‌

system-view

vlan batch 10 20 30 # 创建所有VLAN

# 服务器端口（g0/0/2-7）

interface range GigabitEthernet 0/0/2 to 0/0/7

 port link-type access

 port default vlan 10 # 加入服务器VLAN

quit

# 财务端口（g0/0/8-16）

interface range GigabitEthernet 0/0/8 to 0/0/16

 port link-type access

 port default vlan 20 # 加入财务VLAN

quit

# 技术部端口（g0/0/17-24）

interface range GigabitEthernet 0/0/17 to 0/0/24

 port link-type access

 port default vlan 30 # 加入技术部VLAN

quit

# 连接路由器的上行口（g0/0/1）

interface GigabitEthernet 0/0/1

 port link-type trunk

 port trunk allow-pass vlan 10 20 30 # 透传所有业务VLAN:ml-citation{ref="1,8" data="citationList"}

quit

‌2. 路由器配置（网关与隔离策略）‌

system-view

# 接口配置（连接核心交换机的物理口）

interface GigabitEthernet 0/0/0 # 假设连接核心g0/0/1的接口

 port link-type trunk

 port trunk allow-pass vlan 10 20 30 # 透传VLAN流量:ml-citation{ref="5,6" data="citationList"}

quit

# 创建子接口作为各VLAN网关

interface GigabitEthernet 0/0/0.10 # 服务器网关

 dot1q termination vid 10

 ip address 192.168.1.1 255.255.255.0

 arp broadcast enable

quit

interface GigabitEthernet 0/0/0.20 # 财务网关

 dot1q termination vid 20

 ip address 192.168.2.1 255.255.255.0

 arp broadcast enable

quit

interface GigabitEthernet 0/0/0.30 # 技术部网关

 dot1q termination vid 30

 ip address 192.168.3.1 255.255.255.0

 arp broadcast enable

quit

# 配置ACL阻断财务与技术部互访

acl 3000

 rule 5 deny ip source 192.168.2.0 0.0.0.255 destination 192.168.3.0 0.0.0.255 # 阻断财务→技术部

 rule 10 deny ip source 192.168.3.0 0.0.0.255 destination 192.168.2.0 0.0.0.255 # 阻断技术部→财务

 rule 15 permit ip # 允许其他流量（访问服务器+上网）:ml-citation{ref="12,13" data="citationList"}

quit

# 应用ACL到网关子接口

interface GigabitEthernet 0/0/0.20

 traffic-filter inbound acl 3000 # 财务网关入方向过滤

quit

interface GigabitEthernet 0/0/0.30

 traffic-filter inbound acl 3000 # 技术部网关入方向过滤

quit

# 配置出口上网（运营商公网IP地址为20.20.20.100公网地址 255.255.255.0子网掩码 20.20.20.1网关）

ip route-static 20.20.20.100 255.255.255.0 20.20.20.1

quit

save # 保存配置:ml-citation{ref="6,8" data="citationList"}

‌关键验证点‌

‌连通性测试‌：

财务/技术部PC均可访问服务器（如 ping 192.168.1.100）

所有设备可上网（ping 114.114.114.114）

‌隔离性测试‌：

财务PC（192.168.2.X）无法访问技术部PC（192.168.3.X），反之亦然

‌配置检查命令‌：

交换机：display vlan（确认端口VLAN绑定）

路由器：display acl 3000（查看ACL命中计数）

‌注意事项‌

‌端口隔离‌：接入层端口已通过access vlan实现部门内互通、部门间隔离，无需额外端口隔离命令。

‌路由器子接口‌：必须配置dot1q termination vid和arp broadcast enable以终结VLAN标签58。

‌ACL顺序‌：拒绝规则需置于允许规则之前（华为ACL默认自上而下匹配）。

‌保存配置‌：执行save避免重启丢失。