



TONGJI UNIVERSITY

《计算机网络》 实验报告

小组成员：（第四批第六组）

2050259 何征昊

2052697 刘 毅

2151713 汪心成

日 期：2023年 5月 23日

实验一、虚拟局域网 VLAN

实验时间：2023-4-14

1、实验名称

- 跨交换机实现 VLAN

2、实验目的

- 理解跨交换机之间 VLAN 的特点

3、背景描述

- 公司有以下两个部门
 - 销售部
 - 技术部
- 要求
 - 销售部的个人计算机系统能够分散连接，相互通信
 - 技术部和销售部相互隔离

4、技术原理

- Tag Vlan
 - 相同 VLAN 内的主机之间可以直接访问
 - 不同 VLAN 内的主机相互隔离

遵守 IEEE802.1q 协议标准

- 在利用配置了Tag Vlan 的接口进行数据传输时，需要在数据帧内添加 4 个字节的 802.1q 标签信息，用于标识该数据帧属于哪个VLAN，以便于对端交换机接收到数据帧后进行准确的过滤。
- VLAN的特点：
 - 基于逻辑的分组
 - 在同一VLAN内和真实局域网相同
 - 不受物理位置限制
 - 减少节点在网络中移动带来的管理代价
 - 不同VLAN内用户要通信需要借助三层设备
- VLAN的用途
 - 控制不必要的广播的扩散，从而提高网络带宽利用率，减少资源浪费
 - 划分不同的用户组，对组之间的访问进行限制，从而增加安全性
- 交换机端口模式
 - ACCESS端口

Access端口只能属于一个VLAN，它发送的帧不带有VLAN标签，一般用于连接计算机的端口
 - Trunk端口

可以允许多个VLAN通过，它发出的帧一般是带有VLAN标签的，一般用于交换机之间连接的端口

5、实现功能

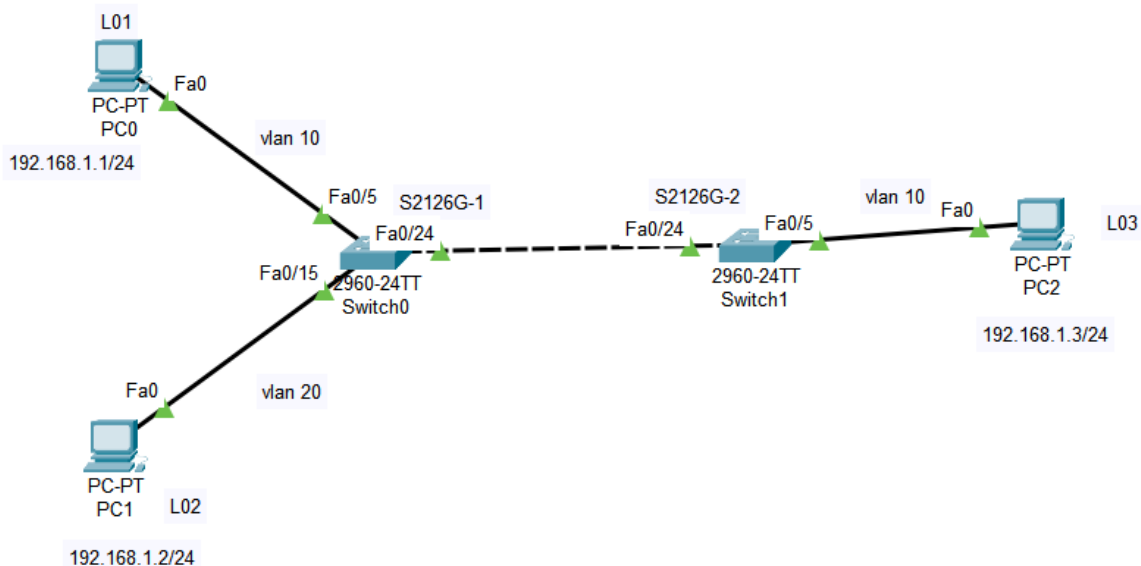
- 使得
 - 在同一 VLAN 内的计算机系统能够跨交换机进行相互通信
 - 在不同 VLAN 内的计算机系统不能进行相互通信

6、实验设备

- S2126G (2台)
- 主机 (3台)
- 直连线 (4条)

7、实验拓扑

- 使用 Cisco Packet Tracer 画出如下的实验拓扑：



- ip地址规划

部门	ip地址
销售部	192.168.1.1/24、192.168.1.3/24
技术部	192.168.1.2/24

8、实验过程

8.1 实体交换机连线

- 交换机 S2126G-1
 - 计算机 L01 连接到 交换机 S2126G-1 的 Fa0/5 端口
 - 计算机 L02 连接到 交换机 S2126G-1 的 Fa0/15 端口
- 交换机 S2126G-2

- 计算机 L03 连接到 交换机S2126G-2 的 Fa0/5 端口
- 交换机 S2126G-1 的 Fa0/24 端口 与 交换机 S2126G-2 的 Fa0/24 端口相连

8.2 手动配置 IP 地址

- 打开计算机配置
 - 在“网络和Internet设置”中，打开更改适配器选项
 - 选中需要更改的网络，打开属性
 - 打开Internet 协议版本，配置 IP 地址

Internet 协议版本 4 (TCP/IPv4) 属性

常规

如果网络支持此功能，则可以获取自动指派的 IP 设置。否则，你需要从网络系统管理员处获得适当的 IP 设置。

☐ 自动获得 IP 地址(O)

☒ 使用下面的 IP 地址(S):

IP 地址(I): 1 . . .

子网掩码(U): . . .

默认网关(D): . . .

☐ 自动获得 DNS 服务器地址(B)

☒ 使用下面的 DNS 服务器地址(E):

首选 DNS 服务器(P): . . .

备用 DNS 服务器(A): . . .

☐ 退出时验证设置(L)

高级(V)...

确定 取消

- 具体配置如下：
 - 计算机 L01
 - IPv4地址：192.168.1.1
 - 子网掩码：255.255.255.0
 - 计算机 L02
 - IPv4地址：192.168.1.2
 - 子网掩码：255.255.255.0
 - 计算机 L03
 - IPv4地址：192.168.1.3
 - 子网掩码：255.255.255.0

8.3 划分 VLAN

SwitchA

- 创建Vlan 10, Fa0/5 端口划分到 Vlan 10 中

```
1 RG-S2126G-1>
2 RG-S2126G-1>enable 14
3 Password:
4 RG-S2126G-1# config terminal
5 RG-S2126G-1(config)# vlan 10
6 RG-S2126G-1(config-vlan)# name sales
7 RG-S2126G-1(config-vlan)#exit
8 RG-S2126G-1(config)#interface fastethernet0/5
9 RG-S2126G-1(config-if)#switchport access vlan 10
```

- 验证：可以通过以下命令查看是否正确划分好了

```
1 RG-S2126G-1# show vlan id 10
```

- 同理，继续在 SwitchA 上创建Vlan 20, Fa0/15 端口划分到 Vlan 20 中

```
1 方法与前面相同
```

SwitchB

- 创建Vlan 10, Fa0/5 端口划分到 Vlan 10 中

```
1 方法与前面相同
```

连接 SwitchA 和 SwitchB

- 把 SwitchA 和 SwitchB 相连的 Fa0/24 端口定义为 Tag Vlan 模式

```
1 RG-S2126G-1#interface fastethernet0/24
2 RG-S2126G-1#switchport mode trunk
```

- 验证：可以通过以下命令查看

```
1 RG-S2126G-1#show interfaces fastethernet0/24 switchport
```

- 注意，在SwitchA 和SwitchB 上都要设置一遍！

9、测试结果

现场记录：

```
Telnet 172.16.0.4

RG-S2126G-2>
RG-S2126G-2>en 14
Password:
Password:
RG-S2126G-2#con te
Enter configuration commands, one per line. End with CNTL/Z.
RG-S2126G-2(config)#vlan 10
2023-04-14 21:36:44 @5-CONFIG:Configured from outband
RG-S2126G-2(config-vlan)#name sales
2023-04-14 21:36:52 @5-CONFIG:Configured from outband
RG-S2126G-2(config-vlan)#exit
2023-04-14 21:36:54 @5-CONFIG:Configured from outband
RG-S2126G-2(config)#int fast0/5
2023-04-14 21:37:08 @5-CONFIG:Configured from outband
RG-S2126G-2(config-if)#sw acc vlan 10
2023-04-14 21:37:18 @5-CONFIG:Configured from outband
RG-S2126G-2(config-if)#Z
RG-S2126G-2#sh vlan id 10

VLAN Name                Status    Ports
-----
10    sales                  active    Fa0/5

RG-S2126G-2#int fast0/24
% Invalid input detected at '' marker.
RG-S2126G-2#con ter
```

验证方法

- 在命令行方式下通过ping命令验证

```
1 | ping 192.168.1.x
```

结果

- 计算机L01 和计算机L03 能够进行相互通信，ping 正常。
- 计算机L02 无法进行通信，ping 请求超时。

```
管理员: C:\WINDOWS\system32\CMD.exe
Microsoft Windows [版本 10.0.19045.2604]
(c) Microsoft Corporation。保留所有权利。

C:\Users\Net317>ping 192.168.1.3

正在 Ping 192.168.1.3 具有 32 字节的数据:
来自 192.168.1.3 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.3 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.3 的回复: 字节=32 时间<1ms TTL=128
来自 192.168.1.3 的回复: 字节=32 时间<1ms TTL=128

192.168.1.3 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 0ms, 最长 = 0ms, 平均 = 0ms

C:\Users\Net317>ping 192.168.1.2

正在 Ping 192.168.1.2 具有 32 字节的数据:
来自 192.168.1.3 的回复: 无法访问目标主机。
请求超时。
请求超时。
请求超时。

192.168.1.2 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 1, 丢失 = 3 (75% 丢失),

C:\Users\Net317>
C:\Users\Net317>ping 192.168.1.1
```

```
管理员: C:\WINDOWS\system32\CMD.exe

C:\Users\Net317>ping 192.168.1.2

正在 Ping 192.168.1.2 具有 32 字节的数据:
来自 192.168.1.3 的回复: 无法访问目标主机。
请求超时。
请求超时。
请求超时。

192.168.1.2 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 1, 丢失 = 3 (75% 丢失),

C:\Users\Net317>
C:\Users\Net317>ping 192.168.1.1

正在 Ping 192.168.1.1 具有 32 字节的数据:
来自 192.168.1.1 的回复: 字节=32 时间=3ms TTL=128
来自 192.168.1.1 的回复: 字节=32 时间=2ms TTL=128
来自 192.168.1.1 的回复: 字节=32 时间=2ms TTL=128
来自 192.168.1.1 的回复: 字节=32 时间=2ms TTL=128

192.168.1.1 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 2ms, 最长 = 3ms, 平均 = 2ms

C:\Users\Net317>
```

10、参考配置

- 示例：创建vlan10并命名sale，把0/5端口划入vlan 10，查看vlan10信息

```
1  ! 创建、命名
2  vlan 10
3  name sale
4  exit
5
6  ! 划入
7  int fa0/5
8  sw acc vlan 10
9
10 ! 查看
11 show vlan id 10
```

- 交换机与交换机之间相连的端口（示例是0/24）设置tag vlan

```
1  ! 设置
2  int fa0/24
3  sw mode trunk
4
5  ! 查看
6  show int fa0/24 switchport
```

truck模式支持tag vlan

11、实验心得

- 本次实验心得
 - 第一次接触计算机网络实验，初步认识了计算机网络的架构。
 - 其中，切身学习并实现了“跨交换机实现Vlan”的实验，能够完成在同一 VLAN 内的计算机系统能够跨交换机进行相互通信、在不同 VLAN 内的计算机系统不能进行相互通信的功能，达到对交换机配置 Tag Vlan 设置不同的 Vlan id，从而实现数据帧的准确过滤！

- 总的来说，通过跨交换机实现VLAN可以实现网络资源的有效管理和隔离，提高网络性能和安全性。在实验中，我学到了如何划分VLAN、配置交换机和设备的VLAN成员关系、实现跨交换机的VLAN通信以及进行故障排除等技能。这对于构建复杂的企业网络和提供安全的网络环境非常有帮助。

实验二、生成树和端口聚合

实验时间：2023-4-21

1、实验名称

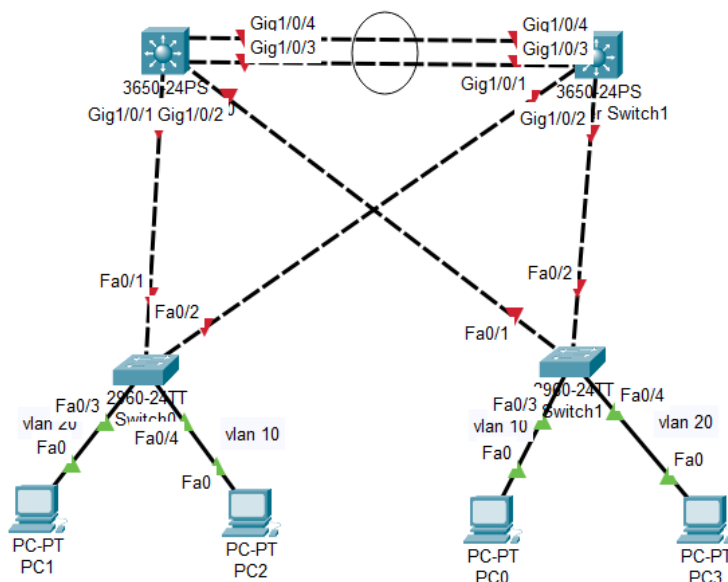
- 端口聚合提供冗余备份链路，快速生成树协议RSTP的配置

2、实验目的

- 理解端口聚合的配置及原理
- 理解快速生成树协议RSTP的配置及原理

3、背景描述

- 1、pc0\pc1\pc2\pc3的ip地址在192.168.x.0/24网段，其中x为学号最后二位
- 2、使用rapid-pvst协议且使得muti sw 0为vlan 10的根交换机,vlan 20的根交换机为muti sw 1
- 3、测试，pc0 ping pc2 连续ping，当sw1 根端口down掉，然后再次no shutdown，看丢包情况



4、技术原理

- 端口聚合
 - 概念：端口聚合（Port Aggregation），也称为链路聚合、端口绑定或以太网绑定，是一种将多个物理网络端口捆绑成一个逻辑端口的技术。
 - 作用：可以提供更高的带宽、冗余和负载均衡
- 生成树

- 概念：生成树（Spanning Tree）是图论中的概念，指的是在一个连通图中，通过选择部分边构成一棵树，使得该树包含图中的所有顶点，并且没有形成回路。生成树在计算机网络中有广泛的应用，其中最常见的是生成树协议用于构建冗余路径和防止环路的形成。
- 作用：确保网络的可靠性和冗余性，避免数据包的循环和冲突，从而提供稳定的通信环境

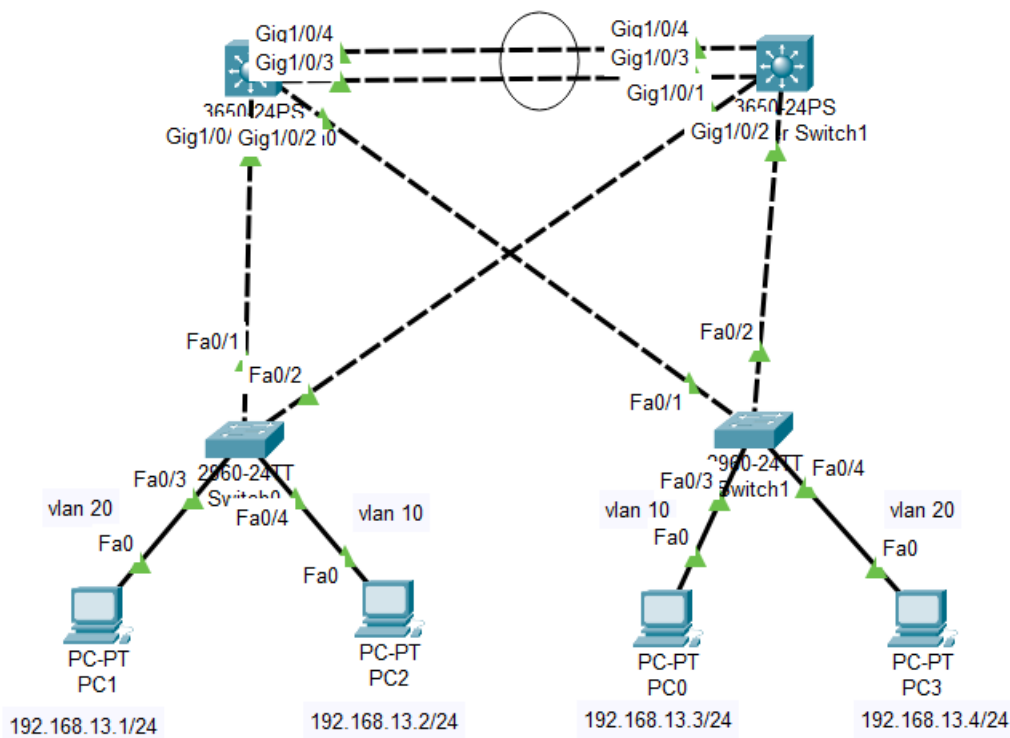
5、实现功能

- 增加交换机之间的传输带宽，实现冗余链路备份
- 实现网络在有冗余链路的情况下，避免环路的产生，避免广播风暴

6、实验设备

- 三层交换机（两台）
- 二层交换机（两台）
- PC（四台）
- 直连线或交换线

7、实验拓扑



- ip地址规划

注意：图中的PC0-3顺序中，PC0在中间，不是第一个！

设备	ip地址
PC0	192.168.13.3/24 (vlan 10)
PC1	192.168.13.2/24 (vlan 20)

设备	ip地址
PC2	192.168.13.1/24 (vlan 10)
PC3	192.168.13.4/24 (vlan 20)

8、实验过程

- 连接线路
- 配置IP地址
- 交换机上设置vlan
- 配置三层交换机的端口聚合
- 设置快速生成树协议，避免环路产生、避免广播风暴产生
- 测试ping
- sw1 根端口down掉，然后再no shutdown，查看丢包情况

9、测试结果

- 在配置好后，第一次测试ping
 - 在同一个vlan下的主机能够正常相互通信，不同vlan不能相互通信
- sw1根端口down掉；再次no shutdown。
 - 测试结果一样，仍然能正常实现对应vlan下的通信
 - down掉sw1根端口，快速生成树协议会自动选择新的线路，保证正常通信

10、参考配置

- vlan的配置

与实验一基本相同，请见前文。

- 端口聚合的配置

某switch上配置端口聚合的示例：

```

1  ! 进入config后:
2  ! 创建聚合接口
3  int aggregateport 1      ! 创建聚合接口AG1
4  sw mode trunk           ! 配置AG模式为trunk
5  exit
6
7  ! 把接口划为AG1上
8  int range fa 0/1-2      ! 把接口 fa0/1、fa0/2作为AG1
9  port-group 1
10
11 ! 查看
12 show aggregatePort 1 summary

```

思科虚拟实验：

```

1 Switch(config)#int rang g 1/0/2-3
2 Switch(config-if-range)#sw tr en d
3 Switch(config-if-range)#sw mode tr
4 设置端口聚合并加入到聚合端口中:
5 Switch(config-if-range)#channel-group 1 mode on
6 显示以太通道
7 Switch#sh etherchannel summary

```

- 生成树的配置

```

1 sw 0 和 muti sw 1:
2 Switch(config)#spanning-tree mode rapid-pvst
3 muti sw 0:
4 Switch(config)#spanning-tree mode rapid-pvst
5 设置优先级, 使得此交换机在vlan 10为根交换机
6 Switch(config)#spanning-tree vlan 10 priority 4096
7 查看生成树
8 muti sw 0:
9 Switch#sh spanning-tree
10 sw 0:
11 Switch#sh spanning-tree

```

思科虚拟实验:

```

1 设置生成树
2 Switch(config)#spanning-tree mode rapid-pvst
3
4 设置优先级, 使得此交换机在vlan 10为根交换机
5 Switch(config)#spanning-tree vlan 10 priority 4096
6
7 查看生成树
8 Switch#sh spanning-tree

```

- 查看聚合端口

```

1 muti sw 0:
2 Switch#sh etherchannel summary

```

- 测试

思科虚拟实验:

```

1 关闭某个端口, 查看丢包情况, 如: sw0
2 int fa 0/1
3 shutdown
4 no shutdown
5
6 连续ping:
7 pc0 : ping -t 192.168.10.2

```

11、实验心得

- 端口聚合有一个注意事项，最好先配置好端口聚合，再连线，否则可能引起广播风暴。
 - 在实验过程中，注意到生成树和端口聚合之间的关系。生成树算法可以帮助避免网络中的环路，而端口聚合则可以将多个链路绑定在一起，形成更高带宽和冗余备份。
- 这两种技术可以结合使用，以实现更强大和可靠的网络架构。我体会到了它们对于提高网络可靠性、性能和带宽的重要性，并学到了如何配置和管理这些技术。

实验三、路由实验

实验时间：2023-4-28

1、实验名称

- 静态路由

2、实验目的

- 掌握设置静态路由，实现网络通信的方式

3、背景描述

- 校园网通过一台路由器连接到校园网外部，通过设置静态路由，实现校园内部的主机和校园外部的主机的相互通信。

4、技术原理

- 路由器是网络层的设备。它能够根据 IP 包头信息，选择一条最佳路由，转发分组，实现不同网段的相互访问。
- 路由表的产生方式有三种：
 - 直连路由
 - 静态路由
 - 动态协议学习产生的路由

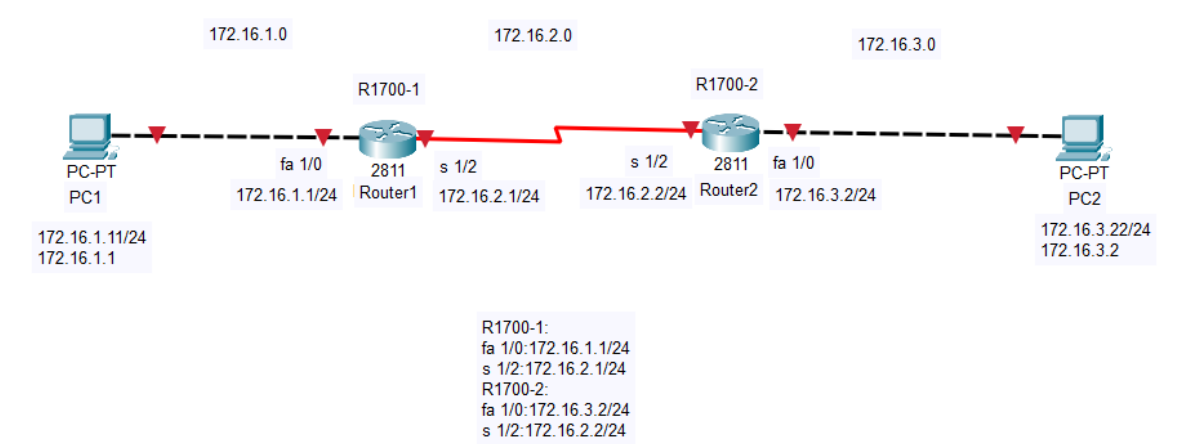
5、实现功能

- 实现不同网络间的互联互通，从而实现信息的共享和传递。

6、实验设备

- R1700（两台）
- V35缆线（1条）
- PC（两台）
- 直连线或交叉线（2条）

7、实验拓扑



- ip地址规划

设备	ip地址
PC1	172.16.1.11/24 (网关: 172.16.1.1)
PC2	172.16.3.22/24 (网关: 172.16.3.2)
R1	fa 1/0: 172.16.1.1/24 s 1/2: 172.16.2.1/24
R2	fa 1/0: 172.16.3.2/24 s 1/2: 172.16.2.2/24

8、实验过程

- 配置 R1 的接口 IP 和串口的时钟频率
在R1上配置静态路由
- 配置 R2 的接口 IP 和串口的时钟频率
在R1上配置静态路由

配置命令行，具体见后面 10.参考配置






- 具体实验时，R1的配置结果记录如下：

```
Telnet 172.16.0.4
interface FastEthernet 1/1
 duplex auto
 speed auto
!
interface Null 0
!
ip route 172.16.3.0 255.255.255.0 172.16.2.2
!
voice-port 2/0
!
voice-port 2/1
!
voice-port 2/2
!
voice-port 2/3
line con 0
line aux 0
line vty 0 4
 login
!
end
RG-R1700-1#
RG-R1700-1#
RG-R1700-1#
RG-R1700-1#
```

9、测试结果

- 测试网络的互通性
 - 从PC1 (172.16.1.11) ping PC2 (172.16.3.22)
通信成功
 - 从PC2 (172.16.3.22) ping PC1 (172.16.1.11)
通信成功

下图为实验记录从PC1 ping PC2的结果记录：

1,  表示二层交换机、 表示三层交换机、 表示核心交换机、 表示路由器、 表示防火墙

```
已打开 管理: C:\WINDOWS\system32\cmd.exe
Microsoft Windows [版本 10.0.19045.2604]
(c) Microsoft Corporation. 保留所有权利。

C:\Users\Net317>ping 172.16.3.22

正在 Ping 172.16.3.22 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

G-R172.16.3.22 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),

C:\Users\Net317>ping 172.16.3.22

正在 Ping 172.16.3.22 具有 32 字节的数据:
来自 172.16.3.22 的回复: 字节=32 时间=22ms TTL=126
来自 172.16.3.22 的回复: 字节=32 时间=21ms TTL=126
来自 172.16.3.22 的回复: 字节=32 时间=20ms TTL=126
来自 172.16.3.22 的回复: 字节=32 时间=21ms TTL=126

172.16.3.22 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 20ms, 最长 = 22ms, 平均 = 21ms

C:\Users\Net317>
```

10、参考配置

- 配置路由器的接口 IP 和串口的时钟频率

```
1  ! 配置接口IP
2  int fa 1/0
3  ip addr 172.16.1.1 255.255.255.0
4  no shutdown
5  int ser 1/2
6  ip addr 172.16.2.1 255.255.255.0
7
8  ! 配置串口时钟频率
9  clock rate 64000
10 no shutdown
```

- 配置路由器静态路由（下为R1的，去往3.0网段，从172.16.2.2/24出去，即ser1/2口）

```
1 ip route 172.16.3.0 255.255.255.0 172.16.2.2
2 ! 或写下面这种也可以
3 ip route 172.16.3.0 255.255.255.0 ser 1/2
```

- 查看路由器接口配置

```
show ip interface brief
```

- 查看路由器某接口状态

```
show interface serial 1/2
```

- 查看路由表

```
show ip route
```

- 查看交换机当前生效的配置信息

```
show running-config
```

11、实验心得

- 本次实验，利用了网络层设备路由器，实现了不同网段的互联互通。

注意一些事项，两台路由器通过串口连接时，必须在其中一端设置时钟频率（DCE）

- 静态路由是计算机网络中一种简单而有效的路由选择方法。
 - 静态路由的配置相对简单，只需手动配置路由表，指定目的网络和下一跳路由器即可，而且可以精确控制数据包的路由路径。

在小型网络或特定场景下非常实用，同时适用于网络拓扑稳定、变化较少的情况。
 - 但是，静态路由不具备自适应能力，无法根据网络状态的变化进行动态调整。

在大型网络中，静态路由可能不适用于扩展性要求高的情况。

实验四、三层交换技术实验

实验时间：2023-5-5

1、实验名称

- 三层交换技术的网络通信

2、实验目的

- 理解并掌握三层交换的原理和配置方法

3、背景描述

- 不同VLAN之间需要通讯，需要第三层路由技术实现通讯。
- PC1和PC2处在不同网段，通过路由器和三层交换机，实现两者的通信

4、技术原理

- 三层交换

三层交换（也称多层交换技术，或IP交换技术）是相对于传统交换概念而提出。

所周知，传统交换技术是在OSI网络标准模型中第二层：数据链路层，而三层交换技术在网络模型中的第三层实现高速转发。

简单地说，三层交换技术就是“二层交换技术+三层转发”。

三层交换技术通过一台具有三层交换功能设备实现。

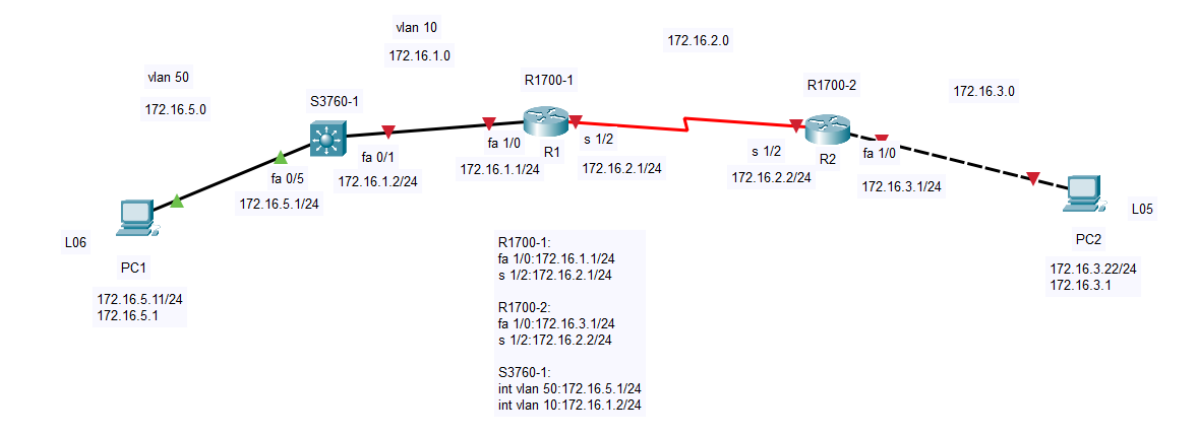
5、实现功能

- 通过三层设备路由功能，将数据报文从一个 VLAN，转发三层路由设备上；
- 利用三层路由设备作为桥接，再转发到另外一个VLAN三层路由上，再通过广播方式传输到另外一个VLAN中。

6、实验设备

- S3760（一台）
- 路由器（两台）
- PC（2台）
- 直连线

7、实验拓扑



- ip地址规划

设备	ip地址
PC1	172.16.5.11/24 (网关: 172.16.5.1)
PC2	172.16.3.22/24 (网关: 172.16.3.1)
S3760	fa 0/5: 172.16.5.1/24 fa 0/1: 172.16.1.2/24
R1	fa 1/0: 172.16.1.1/24 s 1/2: 172.16.2.1/24
R2	fa 1/0: 172.16.3.1/24 s 1/2: 172.16.2.2/24

8、实验过程

- 规划 IP 地址和子网掩码
- 按照拓扑图连接线路
- 配置三层交换机、路由器的SVI 接口ip地址
- 开启三层交换功能，接口处ip作为子网内的主机网关
- 配置路由表
- 测试

9、测试结果

- 从PC1 172.16.5.11/24 ping PC2 172.16.3.22/24

10、参考配置

```
1 Switch(config)# interface vlan vlan-id           ! 进入SVI 接口配置模式。
2 Switch(config-if)# ip address ip-address mask
3 ! 给SVI接口配置IP地址，开启三层交换功能，这些地址作为各VLAN内主机网关。
4
5 Switch(config)# interface interface-id           ! 进入三层交换机的接口配置模式。
6 Switch(config-if)#no switch                     ! 开启该接口的三层交换功能
7 Switch(config-if)# ip address ip-address mask
8 ! 给指定的接口配置IP地址，这些IP地址作为各个子网内主机网关。
9
10 Switch#show running-config                     ! 检查一下刚才的配置是否正确。
11 Switch#show ip route
12
```

11、实验心得

- 通过此次实验，我学习了关于路由器和三层交换机的知识，并明白了它们如何利用IP地址和路由表来实现数据转发。

在配置完三层交换器后，进行了一系列的实验和测试，发送了不同目的地的数据包，并观察了数据包是如何在交换器之间进行路由转发的。通过抓包和观察路由表的变化，能够验证交换器的路由功能是否按预期工作。

实验五、访问控制列表和NAT配置

实验时间：2023-5-12

1、实验名称

- 编号的标准 IP 访问列表、网络地址转换(NAT)配置实验

2、实验目的

- 掌握路由器上编号的标准 IP 访问列表规则及配置方法
- 掌握网络地址转换(NAT)的原理及配置方法

3、背景描述

- 假设现有某企业网，有S3650三层交换机一台，S2960二层交换机两台，配置web服务和FTP服务的服务器一台。

企业经理部PC机4台，财务部PC机5台，业务部PC机30台，企业网申请了三个合法IP地址(100.10.10.1/24, 100.10.10.2/24, 100.10.10.3/24)。

注：拓扑图中企业内部ip都在192.x.0.0/16（就当这个网段为私有地址）网段中，其中x为学号最后二位

- 需求：
 - 企业内部除业务部和财务部PC不能互相通信外，其他都能互相通信。
 - 企业内部主机都能访问服务器（包括web和ftp）
 - 企业内部主机都能访问互联网

4、技术原理

- 访问控制列表

访问控制列表（Access Control List, ACL）是一种网络安全机制，用于过滤和控制网络流量。

条件可以基于源 IP 地址、目标 IP 地址、传输层端口、协议类型等来过滤。

- NAT

- 网络地址转换(NAT,Network Address Translation)属接入广域网(WAN)技术，是一种将私有(保留)地址转化为合法IP地址的转换技术，它被广泛应用于各种类型Internet接入方式和各种类型的网络中。
- 有静态地址转换、动态地址转换、端口复用动态地址转换 3种方法。
- 这里我们使用的是 动态地址转换，把其中部分合法ip用作地址池的网络。（有一个用在路由器的接口ip上了）

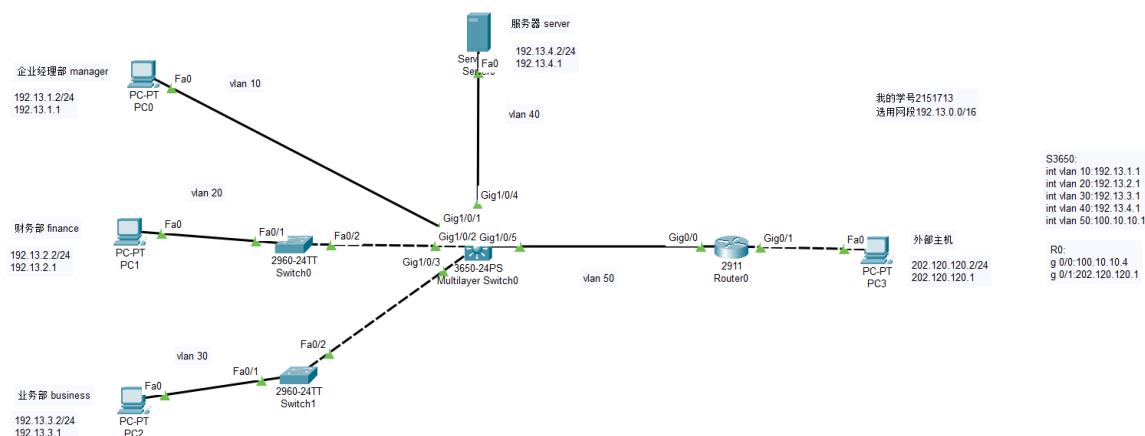
5、实现功能

- 业务部和财务部PC隔离
- 内部主机访问服务器、互联网
- 外部主机也能访问企业内部服务

6、实验设备

- 二层交换机（两台）
- 三层交换机（一台）
- 服务器（一台）
- 内网主机（三台）
- 外网主机（一台）
- 路由器（外网的）

7、实验拓扑



- ip地址规划

设备	ip地址
PC0	192.13.1.2/24 (网关: 192.13.1.1)
PC1	172.16.2.2/24 (网关: 192.13.2.1)
PC2	172.16.3.2/24 (网关: 192.13.3.1)
server	172.16.4.2/24 (网关: 192.13.4.1)
外部主机	202.120.120.2/24 (网关: 202.120.120.1)
R0	g 0/0: 100.10.10.4 g 0/1: 202.120.120.1
vlan 10	192.13.1.1
vlan 20	192.13.2.1
vlan 30	192.13.3.1
vlan 40	192.13.4.1
vlan 50	100.10.10.1

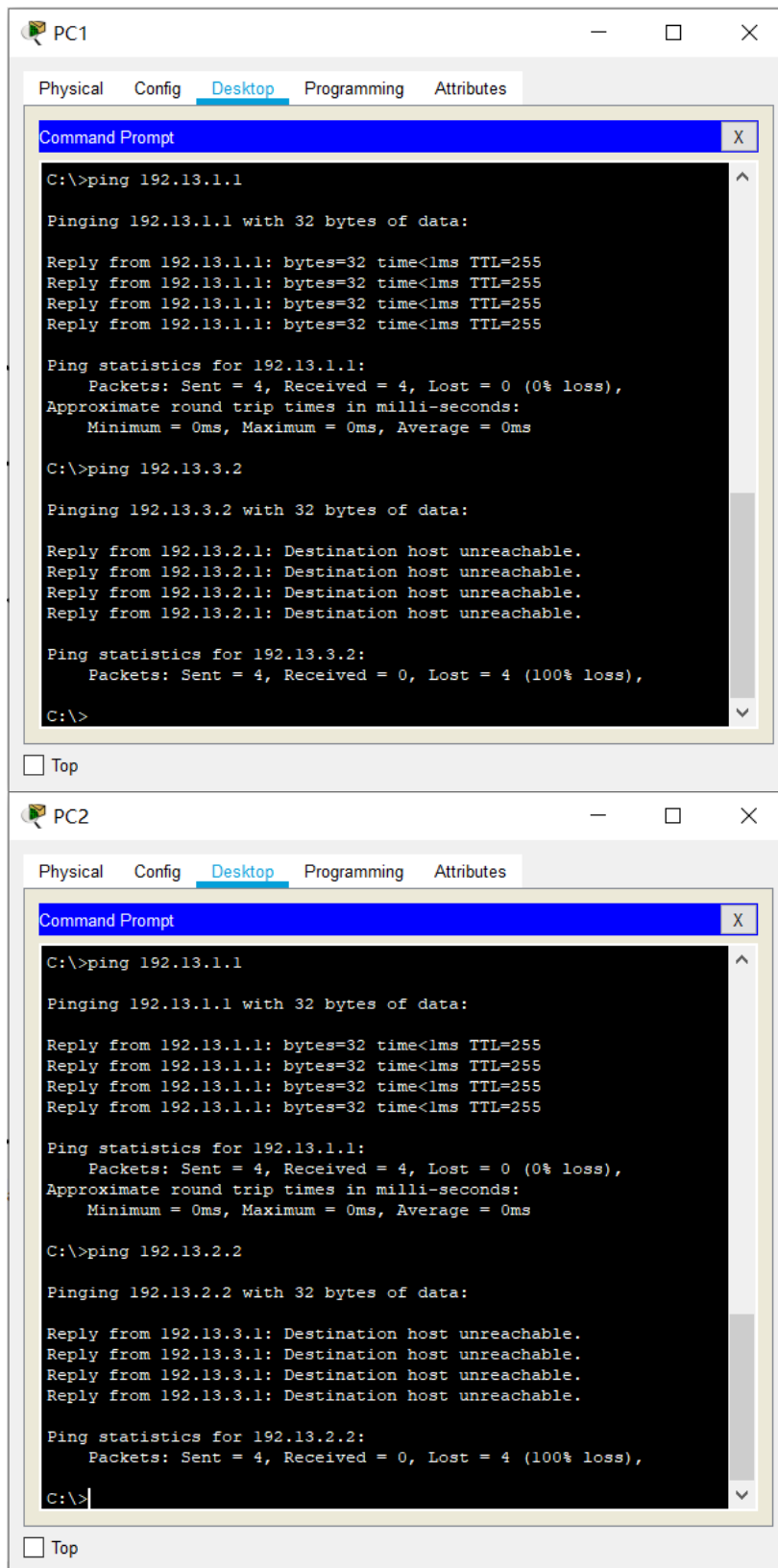
8、实验过程

- 放置主机、连接线路，设置ip和网关
- 配置vlan与接口的ip
- 配置三层交换技术，实现不同vlan下的通信
- 连接外网的三层交换机设置一个合法的公网 ip 100.10.10.1
- 配置外网路由器，接入内网的接口连接企业的合法ip 100.10.10.1 的交换机接口
- 配置访问控制列表，
 - 在g 1/0/2处deny业务部的数据包，
 - 在g 1/0/3处deny技术部的数据包。

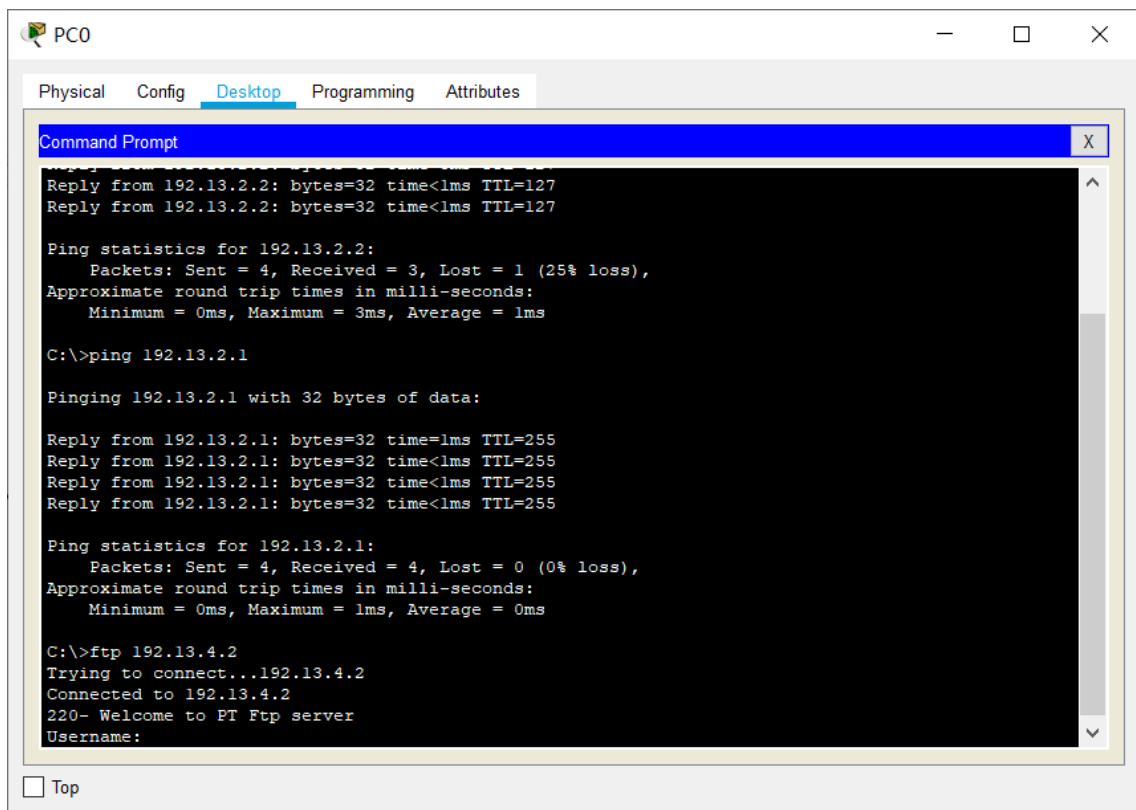
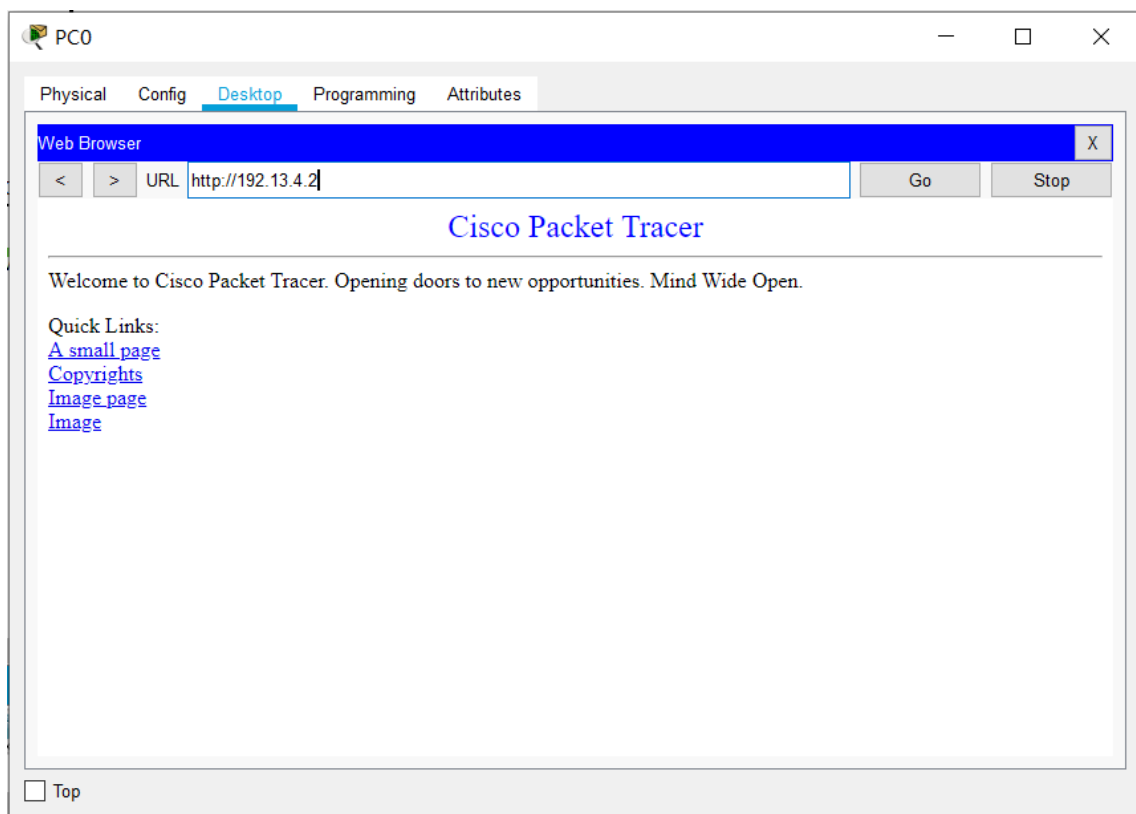
使得业务部和技术部无法通信。

9、测试结果

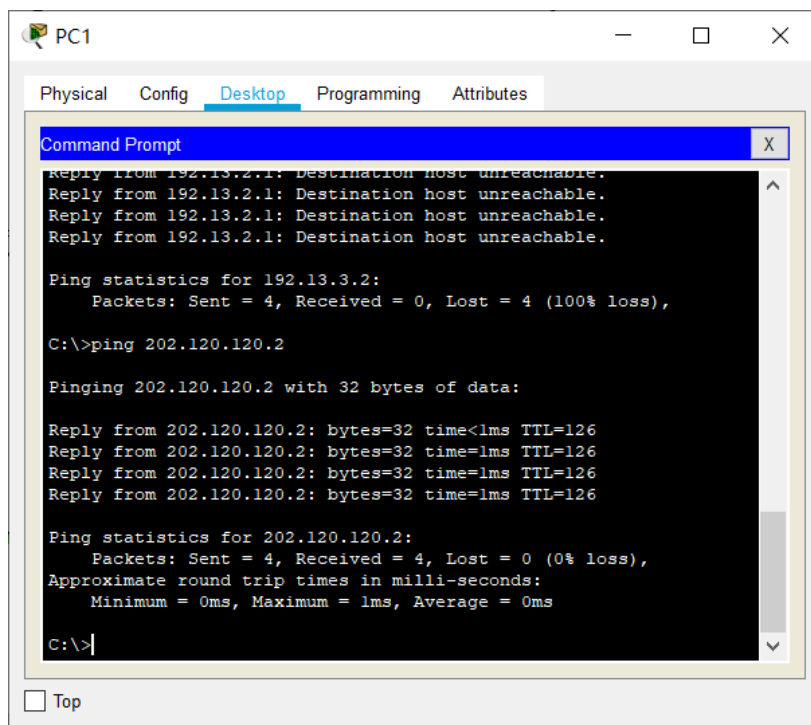
- 1、内部主机，除了业务部和财务部PC不能互相通信外，其他都能互相通信（下图显示，财务部和业务部不能相互通信）



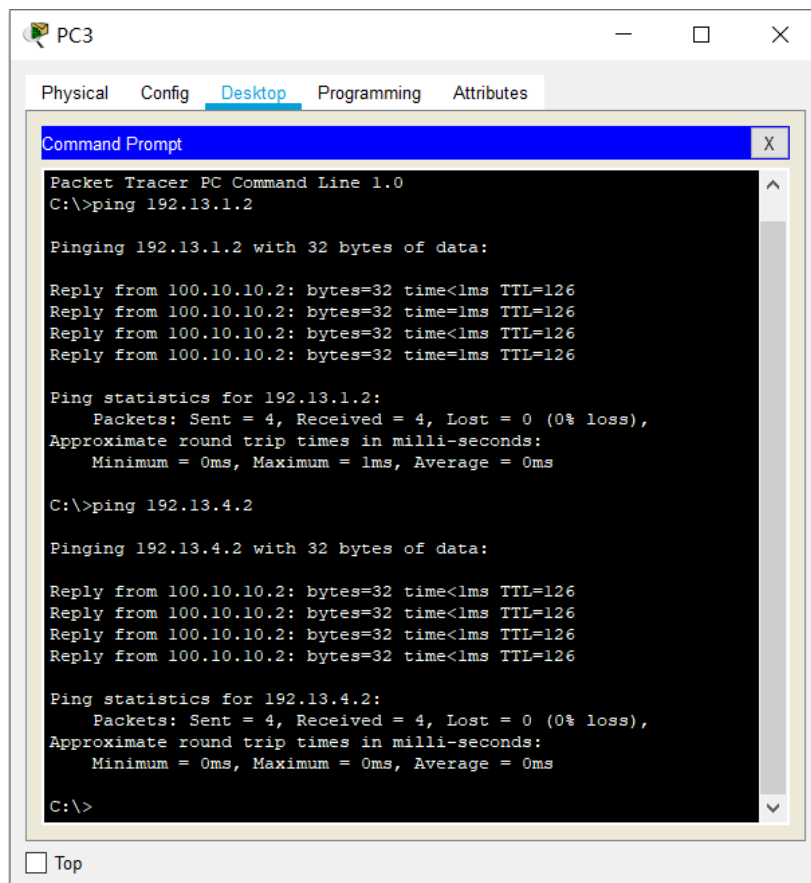
- 2、内部主机都能访问服务器 (http和ftp)



- 3、内部主机都能访问互联网（下图只用PC1展示，其他效果一样）



- 4、外部主机也能访问企业web服务和ftp服务



10、参考配置

- 1、不允许1.0网段访问server

```
1 R2:
2 access-list 1 deny 192.168.1.0 0.0.0.255
3 access-list 1 permit any
4 int g 0/1
5 ip access-group 1 out
6 一般而言：越接近目标越好
7 no ip access-group 1 out
8 no access-list 1
```

- 2、不允许1.0网段访问server的ftp服务，其他都可以

```
1 R0:
2 access-list 101 deny tcp 192.168.1.0 0.0.0.255 host 192.168.5.2 eq ftp
3 access-list 101 permit ip any any
4 int g 0/0
5 ip access-group 101 in
6 一般而言：越接近源越好
```

- 3、只允许192.168.1.3访问server的ftp服务

```
1 R0:
2 access-list 102 permit tcp host 192.168.1.3 host 192.168.5.2 eq ftp
3 access-list 102 deny tcp any host 192.168.5.2 eq ftp
4 access-list 102 permit ip any any
5 int g 0/2
6 ip access-group 102 out
```

11、实验心得

- 进行访问控制列表（ACL）和网络地址转换（NAT）的配置实验是学习网络安全和网络管理的重要一步。

ACL 实验主要注意在哪个位置进行过滤，是进还是出？

NAT 实验主要注意如何分配给的几个合法公网ip地址。

- 通过实验，可以深入理解 ACL 和 NAT 的原理和配置步骤，并掌握如何应用它们来加强网络安全和提供灵活的网络连接。在实验过程中，及时的验证、调试和修正是非常重要的，以确保配置的正确性和有效性。

实验六、综合实验

实验时间：2023-5-19

1、实验名称

- 中型企业网络设计与实施

2、实验目的

- 综合所学过的所有网络技术，熟悉并掌握各种技术的综合使用时的原理和配置方法

3、背景描述

- 假设现有某企业网，有三层交换机一台，二层交换机一台，路由器一台。

企业网采用三层架构，二层和三层交换机连接采用聚合方式。企业技术部(15台)、财务部门(4台)分属不同的VLAN，企业申请了中国电信两个合法ip地址：100.10.10.1/24、100.10.10.2/24。

- 注：

拓扑图中企业内部所有地址都来源于192.168.x.0（其中x=批号*20+组号如第一批第五小组x就等于25）网段且以最节约地址的方式做连续ip地址规划。

- 需求：

在企业内部所有计算机都能互相访问，除财务部门以外且都能访问互联网（假定中国电信的一台主机ip地址为200.20.20.20/24，财务部不能访问外网必须使用访问控制列表方式，私有地址不允许出外网）

4、技术原理

- vlan间的通信
 - 相同 VLAN 内的主机之间可以直接访问
 - 不同 VLAN 内的主机相互隔离
- 子网规划
 - 子网规划是在网络设计中划分IP地址空间的过程，以创建逻辑上独立的子网。
 - 它的目的是合理利用IP地址，提供有效的地址分配和路由管理。
- ospf
 - OSPF（Open Shortest Path First）是一种内部网关协议（IGP），用于在自治系统（AS）内部进行动态路由选择。
 - OSPF 原理基于链路状态算法，通过邻居发现、链路状态更新、最短路径计算和路由表生成，实现了自治系统内部的动态路由选择。
- 数据包过滤
 - 数据包过滤是一种网络安全机制，用于根据特定规则过滤和控制网络中的数据包流动。它的原理基于对数据包的检查和匹配，以决定是否允许或阻止数据包通过网络设备。
 - 这里我们是通过 访问控制列表 直接deny财务部的 ip 网段实现的。
- NAT
 - 网络地址转换(NAT,Network Address Translation)属接入广域网(WAN)技术，是一种将私有(保留)地址转化为合法IP地址的转换技术，它被广泛应用于各种类型Internet接入方式和各种类型的网络中。
 - 有静态地址转换、动态地址转换、端口复用动态地址转换 3种方法。
 - 这里我们使用的是 动态地址转换，把其中一个合法ip用作地址池的网络。（另一个用在路由器的接口ip上了）
- 端口聚合
 - 端口聚合（Port Aggregation），是一种将多个物理网络端口捆绑成一个逻辑端口的技术。
 - 可以提供更高的带宽、冗余和负载均衡。

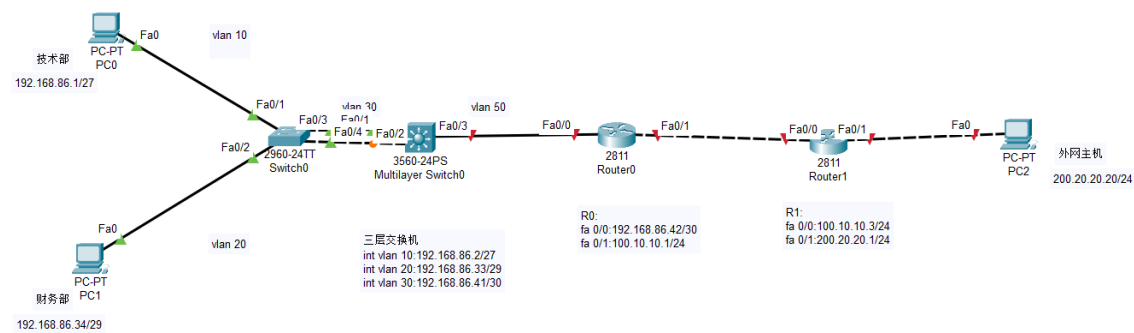
5、实现功能

- 实现在企业内部所有计算机都能互相访问，除财务部门以外且都能访问互联网

6、实验设备

- 三层交换机（一台）
- 二层交换机（一台）
- 路由器（一台）
- 企业技术部PC（15台）
- 财务部门PC（4台）

7、实验拓扑



- vlan 地址划分

设备	可用ip地址	网关	广播地址
vlan 10 192.168.86.0/27 网段	192.168.86.1/27 ~ 192.16.86.30/27	192.168.86.1/27	192.168.86.31/27
vlan 20 192.168.86.32/29 网段	192.168.86.33/29 ~ 192.16.86.38/29	192.168.86.33/29	192.16.86.39/29
vlan 50 192.168.86.40/30 网段	192.168.86.41/30 ~ 192.16.86.42/30	仅两个可用 ip	192.168.86.43/30

- ip地址规划

设备	ip地址
PC0（技术部）	192.168.86.2/27 ~ 192.16.86.30/27（网关：192.168.86.1/27）
PC1（财务部）	192.168.86.34/29 ~ 192.16.86.38/29（网关：192.168.86.33/29）
外部主机 200.20.20.0/24 网段	200.20.20.20/24（网关：200.20.20.1/24）

设备	ip地址
Switch0	fa 0/1: 192.168.86.1/27 fa 0/2: 192.168.86.33/29
Multilayer Switch0	fa 0/1-2: 192.168.86.43/30 fa 0/3: 172.16.2.2/24
R0	fa 0/0: 192.168.86.42/30 fa 0/1: 100.10.10.1/24
R1	fa 0/0: 100.10.10.3/24 fa 0/1: 200.20.20.1/24

备注：

技术部原本规划的是 192.168.86.2 ~ 192.168.86.30

192.168.86.1 用作网关

但由于实验过程中，出现一点问题，

临时将 192.168.86.1 和 192.168.86.2 互换（即网关和一个主机的地址换了一下）

8、实验过程

- 配置三台PC机和接线
 - PC1作为技术部，接二层交换机1口，设置IP地址192.168.88.1/27，网关192.168.88.2
 - 见前方备注
 - PC2作为财务部，接二层交换机2口，设置IP地址192.168.88.34/29，网关192.168.88.33
 - PC3作为互联网，接外网路由器fa1/0口，设置IP地址200.20.20.20/24，网关200.20.20.1
- 配置双层交换机 vlan，配置聚合端口
- 配置三层交换机 vlan，配置聚合端口
- 三层交换机配置ospf路由、dhcp
- 配置内网路由器 (ospf、dhcp server、访问控制列表、NAT)
 - 配置静态路由到 100.10.10.3
- 配置外网路由器 (ip和ospf)
- 在内网路由器上，配置访问控制列表
- 测试互联网连通性

9、测试结果

- 技术部PC测试
 - 从PC0（技术部）ping 192.168.88.34（连通） ping 200.20.20.20（连通）
- 财务部PC测试
 - 从PC1（财务部）ping 192.168.88.2（连通） ping 200.20.20.20（阻塞）
- 外部主机
 - 从外部主机 ping 192.168.88.2（阻塞） ping 192.168.88.34（阻塞）

10、参考配置

- 二层交换机

```
1 switch#conf t
2 switch(config)#vlan 10
3 switch(config-vlan)#exit
4 switch(config)#vlan 20
5 switch(config-vlan)#exit
6 switch(config)#int fa 0/3
7 switch(config-if)#sw acc vlan 10
8 switch(config-if)#int fa 0/4
9 switch(config-if)#sw acc vlan 20
10 switch(config-if)#exit
11
12 switch(config)#int aggr 1 //配置聚合端口
13 switch(config-if)#sw mode tr
14 switch(config-if)#exit
15 switch(config)#int rang fa 0/1-2
16 switch(config-if-range)#port-group 1
```

- 三层交换机

```
1 switch#conf t
2 switch(config)#vlan 10
3 switch(config-vlan)#exit
4 switch(config)#vlan 20
5 switch(config-vlan)#exit
6 switch(config)#vlan 30
7 switch(config-vlan)#exit
8 switch(config)#int fa 0/3
9 switch(config-if)#sw acc vlan 50
10 switch(config-if)#exit
```

配置聚合端口

```
1 switch(config)#int aggr 1
2 switch(config-if)#sw mode tr
3 switch(config-if)#exit
4 switch(config)#int rang fa 0/1-2
5 switch(config-if-range)#port-group 1
6 switch(config-if-range)#exit
```

配置网段接口ip

```

1 switch(config)#int vlan 10
2 switch(config-if)#ip add 192.168.88.2 255.255.255.224
3 switch(config-if)#no sh
4 switch(config-if)#exit
5 switch(config)#int vlan20
6 switch(config-if)#ip add 192.168.88.33 255.255.255.248
7 switch(config-if)#no sh
8 switch(config-if)#exit
9 switch(config)#int vlan 50
10 switch(config-if)#ip add 192.168.88.41 255.255.255.252
11 switch(config-if)#no sh
12 switch(config-if)#exit

```

配置ospf路由、配置dhcp、配置静态路由

```

1 switch(config)#router ospf
2 switch(config-router)#network 192.168.88.0 255.255.255.224 area 0
3 switch(config-router)#network 192.168.88.32 255.255.255.248 area 0
4 switch(config-router)#network 192.168.88.40 255.255.255.252 area 0
5 switch(config-router)#end
6 switch(config)#service dhcp
7 switch(config)#ip helper-add 192.168.88.42
8 switch(config)#ip route 0.0.0.0 0.0.0.0 192.168.88.42

```

- 配置内网路由器

```

1 Router1#conf t
2 Router1(config)#int fa 1/0
3 Router1(config-if)#ip add 192.168.88.42 255.255.255.252
4 Router1(config)#no sh
5 Router1(config)#int se 1/2
6 Router1(config-if)#ip add 100.10.10.1 255.255.255.0
7 Router1(config)#no sh
8
9 Router1(config)#router ospf //配置ospf
10 Router1(config-router)#network 192.168.88.42 0.0.0.0 area 0
11 Router1(config-router)#network 100.10.10.0 0.0.0.0 area 0
12 Router1(config-router)#end
13
14 Router1(config)#service dhcp //配置dhcp vlan10
15 Router1(config)#ip dhcp pool vlan10
16 Router1(dhcp-config)#network 192.168.88.0 255.255.255.224
17 Router1(dhcp-config)#default-router 192.168.88.2
18 Router1(dhcp-config)#dns-server 8.8.8.8 8.8.2.2
19 Router1(dhcp-config)#lease 0 1
20 Router1(dhcp-config)#exit
21
22 Router1(config)#service dhcp //配置dhcp vlan 20
23 Router1(config)#ip dhcp pool vlan20
24 Router1(dhcp-config)#network 192.168.88.32 255.255.255.248
25 Router1(dhcp-config)#default-router 192.168.88.33
26 Router1(dhcp-config)#dns-server 8.8.8.8 8.8.2.2
27 Router1(dhcp-config)#lease 0 1
28 Router1(dhcp-config)#exit
29

```

```

30 Router1(config)#int se 1/2 //配置NAT
31 Router1(config-if)#ip nat outside
32 Router1(config)#int fa 1/0 //配置NAT
33 Router1(config-if)#ip nat inside
34 Router1(config-if)#exit
35
36 Router1(config)#ip nat pool one 100.10.10.2 100.10.10.2 netmask
255.255.255.0 //配置NAT
37 Router1(config)#access-list 1 permit 192.168.88.0 0.0.0.255
38 Router1(config)#ip nat inside source list 1 pool one overload

```

- 配置静态路由

```

1 switch(config)#ip route 0.0.0.0 0.0.0.0 100.10.10.3

```

- 配置外网路由器

```

1 Router2#conf t
2 Router2(config)#int se 1/2
3 Router2(config-if)#ip add 100.10.10.3 255.255.255.0
4 Router2(config)#no sh
5 Router2(config)#int fa 1/0
6 Router2(config-if)#ip add 200.20.20.1 255.255.255.0
7 Router2(config)#no sh

```

- 在内网路由器上，配置访问控制列表

```

1 Router1(config)#access-list 2 deny 192.168.88.32 0.0.0.7
2 Router1(config)#access-list 2 permit any
3 Router1(config)#int fa 1/0
4 Router1(config-if)#ip access-group 2 in
5 Router1(config-if)#end

```

11、实验心得

- 在进行中型企业网络设计的实验过程中，我积累了以下的心得体会：

根据中型企业的需求，我设计了适合的网络拓扑。这包括选择合适的网络设备、划分子网、确定网络层次结构等。我考虑了网络的可扩展性、冗余性和安全性，以满足中型企业的日常运营需求。

其中子网规划情况如下：

由于我们要尽可能地节省ip地址，要做连续的ip地址规划，需要结合各个子网下的主机数目需求对ip地址进行计算划分。

- 技术部（15台PC）

15个主机地址+1个网关地址+1个广播地址+1网段地址

总共 18 个

$$2^4 = 16 \quad 2^5 = 32$$

所以需要主机位 5 位，则网络前缀 $32 - 5 = 27$ 位

最终在 192.168.86.0 网段，可用 192.168.86.1/27 ~ 192.16.86.30/27，

其中 192.168.86.1/27 作为网关，192.168.86.31/27 是广播地址。

- 财务部（4台PC）

4个主机地址+1个网关地址+1个广播地址+1网段地址

总共 7 个

$$2^2 = 4 \quad 2^3 = 8$$

所以需要主机位 3 位，则网络前缀 $32-3 = 29$ 位

最终在 192.168.86.32/29 网段，可用 192.168.86.33/29 ~ 192.168.86.38/29，

其中 192.168.86.33/29 作为网关，192.168.86.39/29 是广播地址。

- 三层交换机与路由器间

只需要2个可用ip即可

网段为 192.168.86.40/30，

可用 192.168.86.41/30 和 192.168.86.42/30

广播地址 192.168.86.43/30

因此，最终所有的规划用到最少ip地址数为 0 - 43

- 通过设计子网规划，我学习并掌握了 ip地址规划的原理和方法，理解网段、可用主机地址、网关地址、广播地址的概念。

- 其次，对中小型企业网络的规划，还有各类配置需要注意

尤其对接口ip的配置不要出错（接口不对、ip打错数字等），

配置过程中，要注意部分步骤有先后顺序，

在操作过程中，最好能够在几个主要功能操作完毕后，进行一定的测试，及时发现错误：

- 比如，在配置完毕前面的操作，但还未进行配置访问控制列表的配置（即还未deny财务部的通信）

此时可以测试一下所有的主机的通信情况，

应该是包括财务部在内的所有内部主机都能相互通信，且能访问互联网（和外部主机通信）。

- 操作了deny财务部整合，

财务部无法访问互联网，其他主机情况和上述保持一致。