实验 28：组网技术实验

姓名	学号	合作学生	指导教师	实验地点	实验时间
林继申	2250758	无	陈伟超	济事楼 330	2024/05/23

【实验目的】

本次组网技术实验的主要目的是学习和实现单臂路由，以促进不同虚拟局域网（VLAN）之间的互联互通。通过配置一个路由器接口上的子接口（逻辑接口），实验旨在实现原本相互隔离的 VLAN 之间的网络互通。这种设置特别适用于需要跨 VLAN 访问的场景，例如公司内不同部门之间的网络访问需求。具体包括：

1. 掌握单臂路由的概念和应用场景。
2. 学习如何配置路由器的子接口来处理不同 VLAN 的交流。
3. 理解并实现 VLAN 的配置和管理。
4. 通过实验设置，检验和分析网络的连通性，以及在特定场景下（如部门间需要通讯时）的网络表现。

【实验原理】

一、单臂路由概述

单臂路由，又称为 router-on-a-stick，是一种网络配置策略，通过在单一的物理路由器接口上配置多个虚拟的子接口来实现不同虚拟局域网（VLAN）之间的数据交换和互联互通。这种方法允许一台物理路由器利用单个接口来管理多个 VLAN 的流量，通过在物理接口上实现逻辑分割，使每个子接口都可以代表一个单独的 VLAN，并对应配置独立的 IP 路由策略。单臂路由的核心在于使用 802.1Q VLAN 标签技术，这项技术使得来自不同 VLAN 的数据包能够在同一物理接口上传输，而每个数据包的 VLAN 身份通过标签来识别和区分。这种配置方式非常适合那些硬件资源有限但需要处理多个网络分段的场合，例如小型企业或者分布式网络环境，因为它可以显著降低硬件成本，简化网络结构，同时提高网络的可扩展性和灵活性。

二、单臂路由主要特点

1. 逻辑子接口配置：在物理接口上创建多个子接口，每个子接口都有自己的 VLAN 标识（通过 802.1Q 标签）和 IP 地址。这样可以使得路由器理解来自不同 VLAN 的数据包，并根据配置进行正确的路由。

2. Trunk 链路：路由器与交换机之间的连接必须配置为 Trunk 模式，以便能够携带多个VLAN的数据包。Trunk链路可以携带属于不同VLAN的所有数据包，每个数据包都带有 VLAN 标识。
3. 跨 VLAN 路由：通过配置单臂路由，可以使不同的 VLAN 间能够互相通信。例如，在一个企业环境中，不同部门可能位于不同的 VLAN，通常这些 VLAN 是相互隔离的以提高安全性。通过单臂路由，可以有选择性地允许特定 VLAN 之间的数据流动，如管理层需要访问多个部门的数据。

三、单臂路由应用场景

1. 企业网络：适用于需要成本效益的解决方案来实现 VLAN 间的路由，尤其是在小型或中型企业中。
2. 多租户环境：在提供 IT 服务的环境中，可以用单臂路由来隔离不同客户的网络，同时允许必要的通信。
3. 教育机构：学校可以使用单臂路由将教师、学生、行政等网络分开，同时允许行政访问需要的资源。

四、单臂路由优缺点

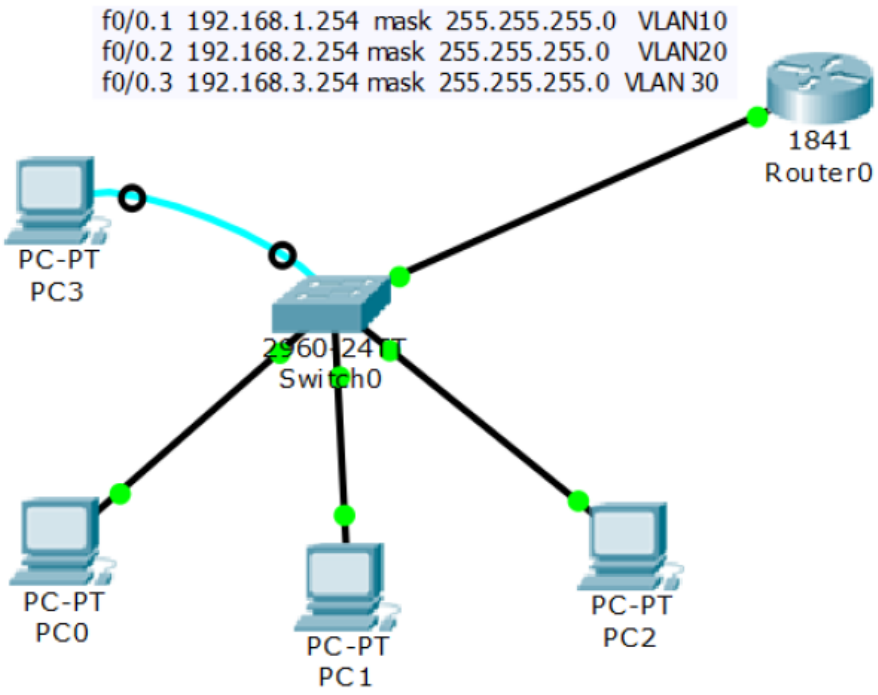
1. 优点
   - 成本效率：相比于为每个 VLAN 配置一个物理接口，单臂路由只需一个物理接口，减少了硬件成本。
   - 简化网络设计：简化了网络的物理布局，降低了管理复杂性。
2. 缺点
   - 带宽限制：所有 VLAN 的数据都通过同一个物理接口传输，可能会在高流量时段造成瓶颈。
   - 安全考虑：虽然有助于 VLAN 间的通信，但配置不当可能导致安全漏洞。

【实验设备】

1. 操作系统：Windows 10
2. 网络环境：局域网
3. 应用程序：Cisco Packet Tracer 6.0

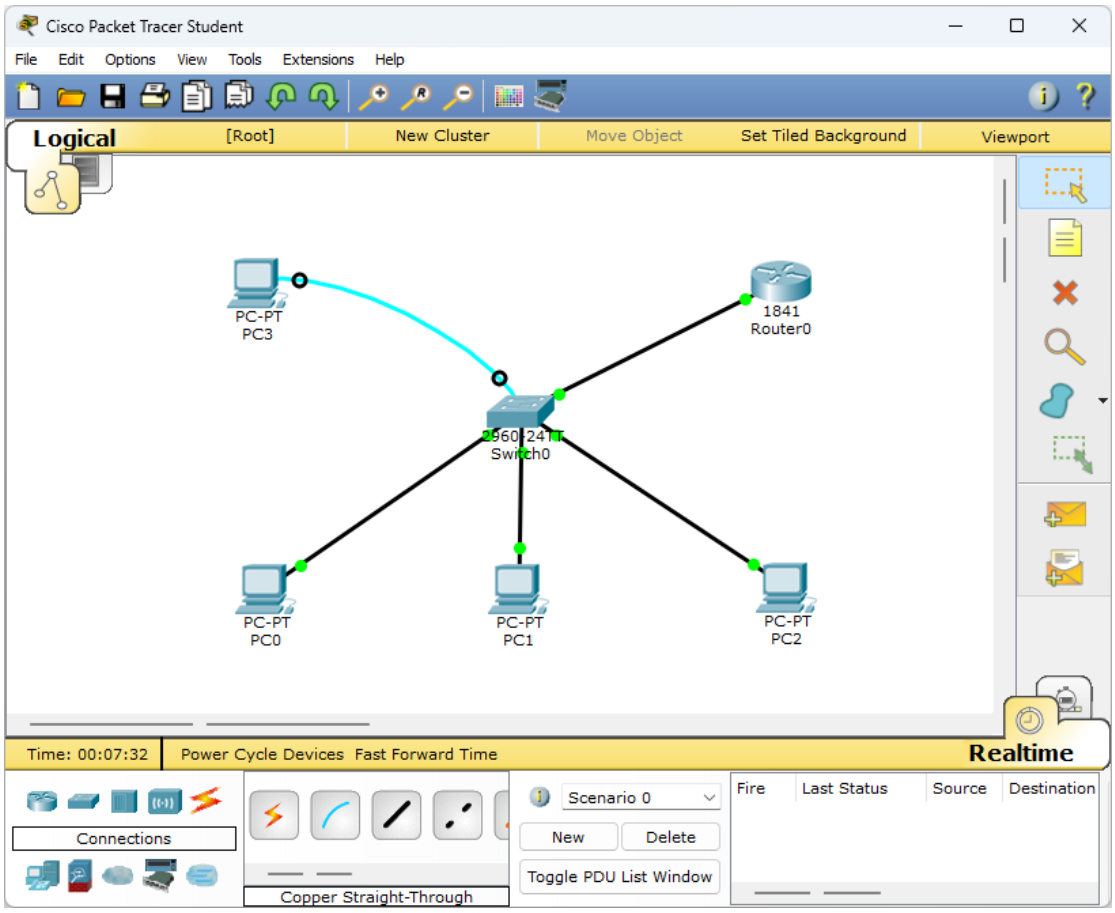
【实验步骤】

1. 规划网络地址及拓补图。

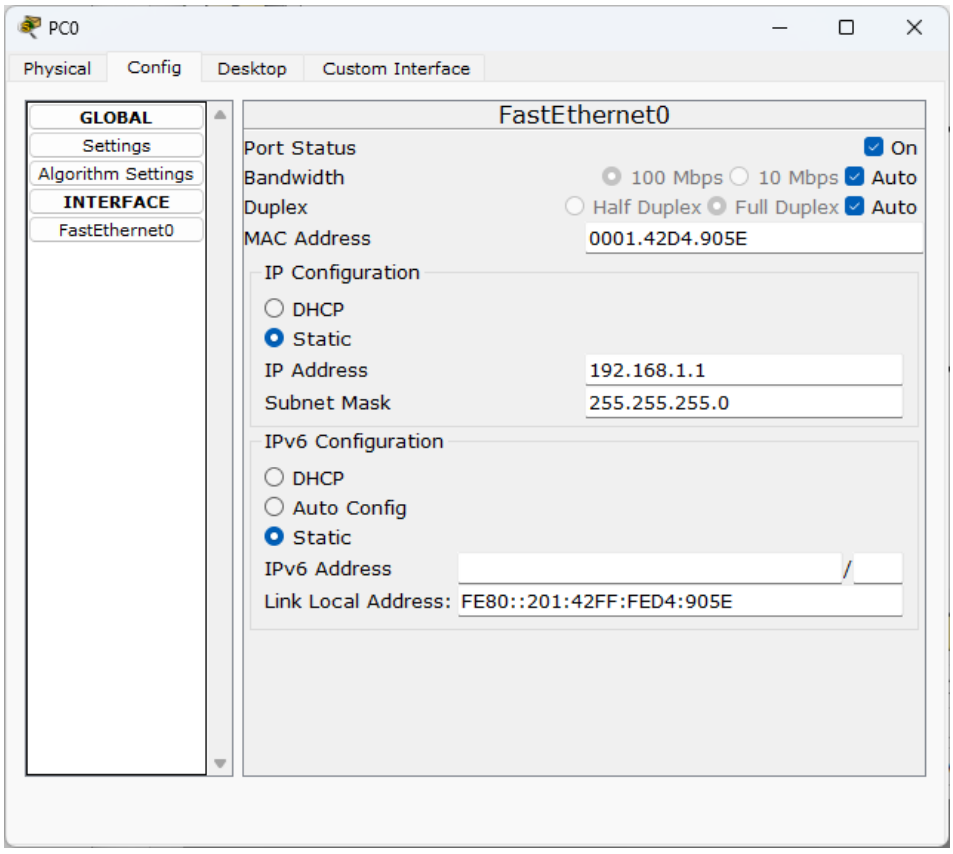


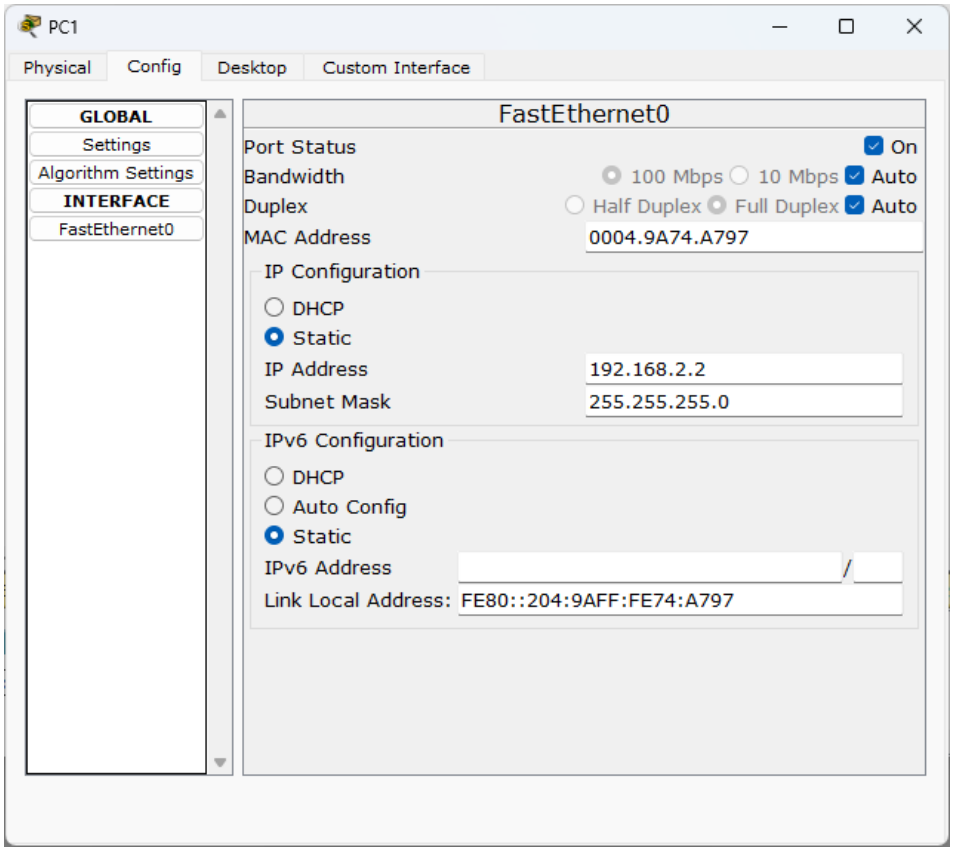
PC0 192.168.1.1 mask 255.255.255.0 F0/1 VLAN10
PC1 192.168.2.2 mask 255.255.255.0 F0/2 VLAN20
PC2 192.168.3.3 mask 255.255.255.0 F0/3 VLAN 30

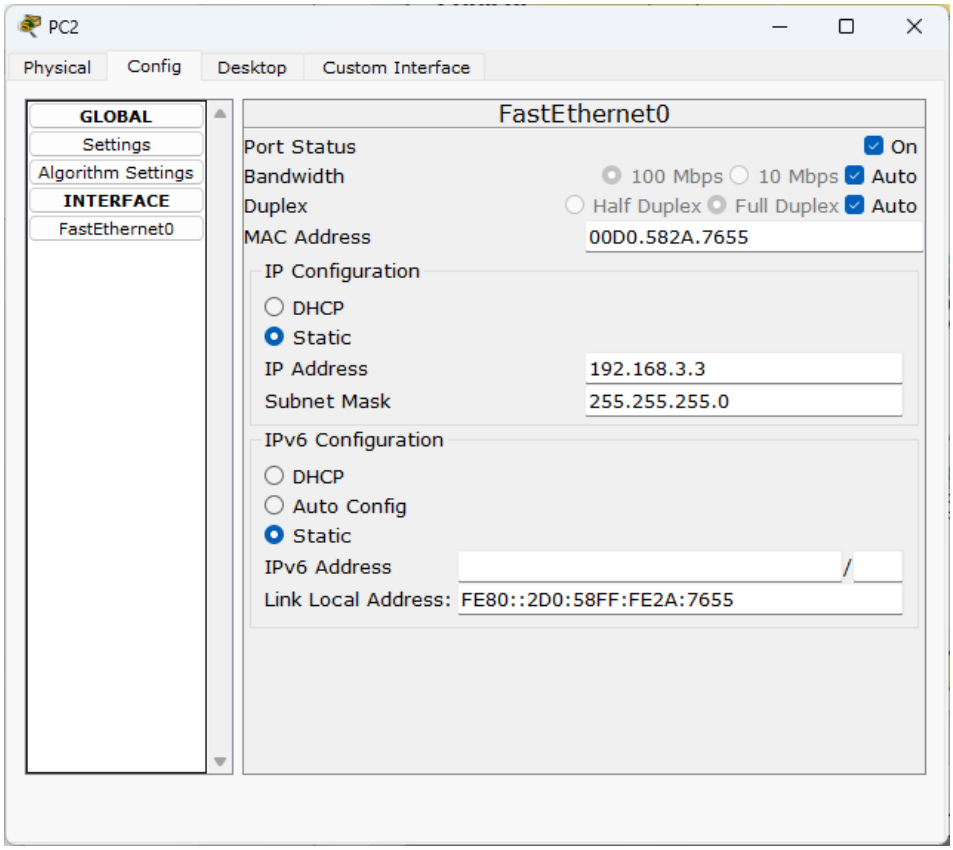
2. 启动 Cisco Packet Tracer 来模拟网络环境，并连接设备。



3. 通过 Config 图形化界面为三台 PC 机配置 IP 及掩码。

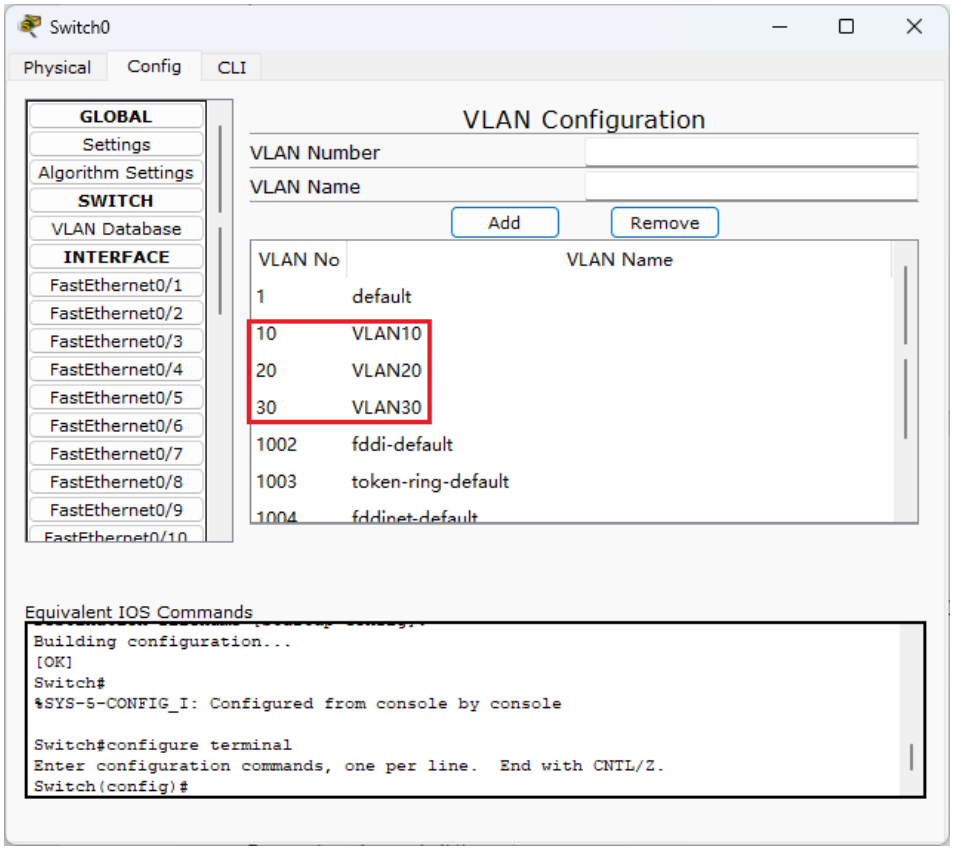




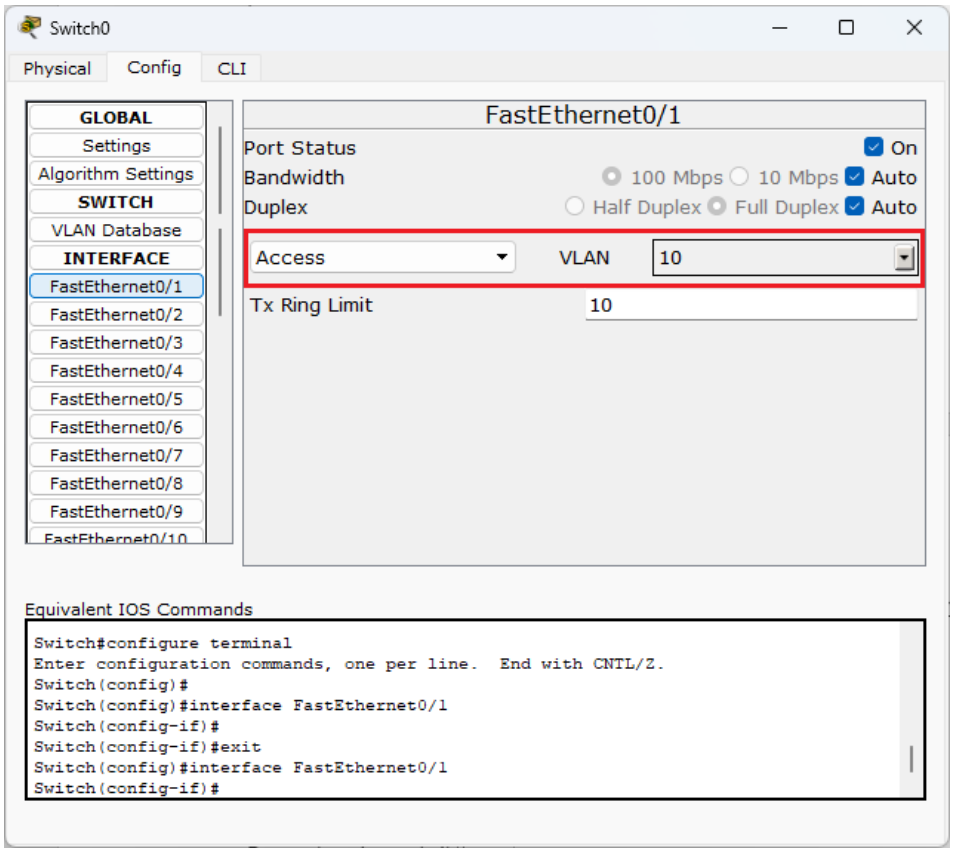


4. 在配置 VLAN 前测试 PC0，PC1，PC2 之间相互 ping，查看并记录实验结果。

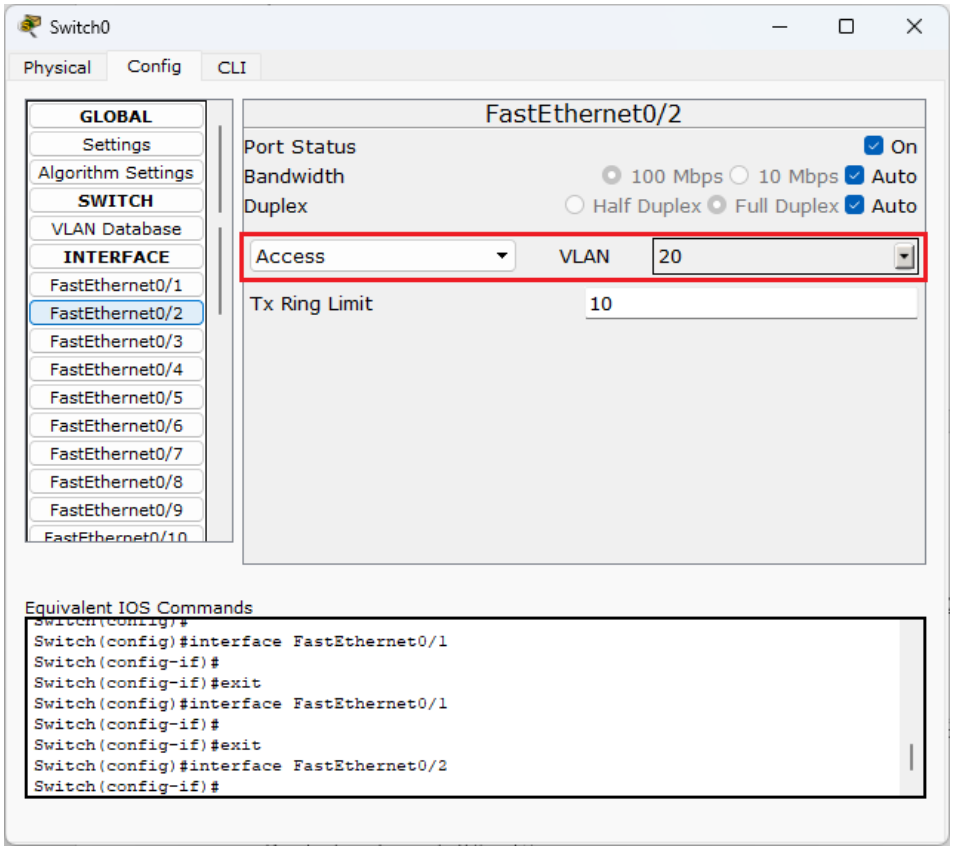
5. 通过图形化界面，为 PC0/PC1/PC2 分别配置 VLAN10，VLAN20，VLAN30。



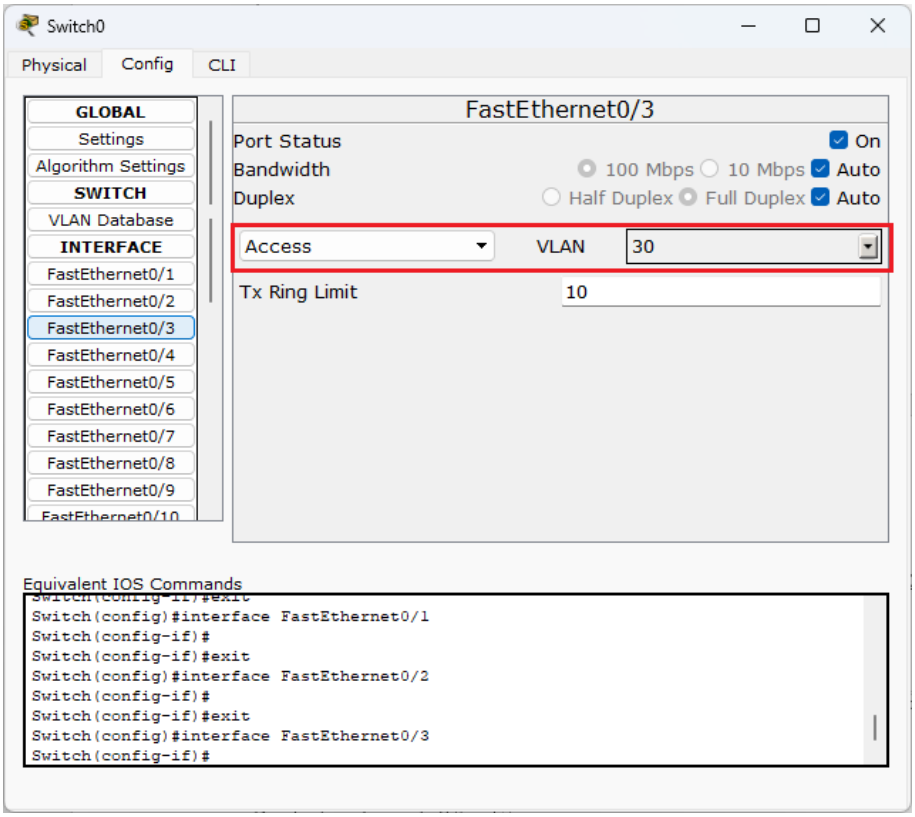
- PC0 配置：192.168.1.1 mask 255.255.255.0 F0/1 VLAN 10



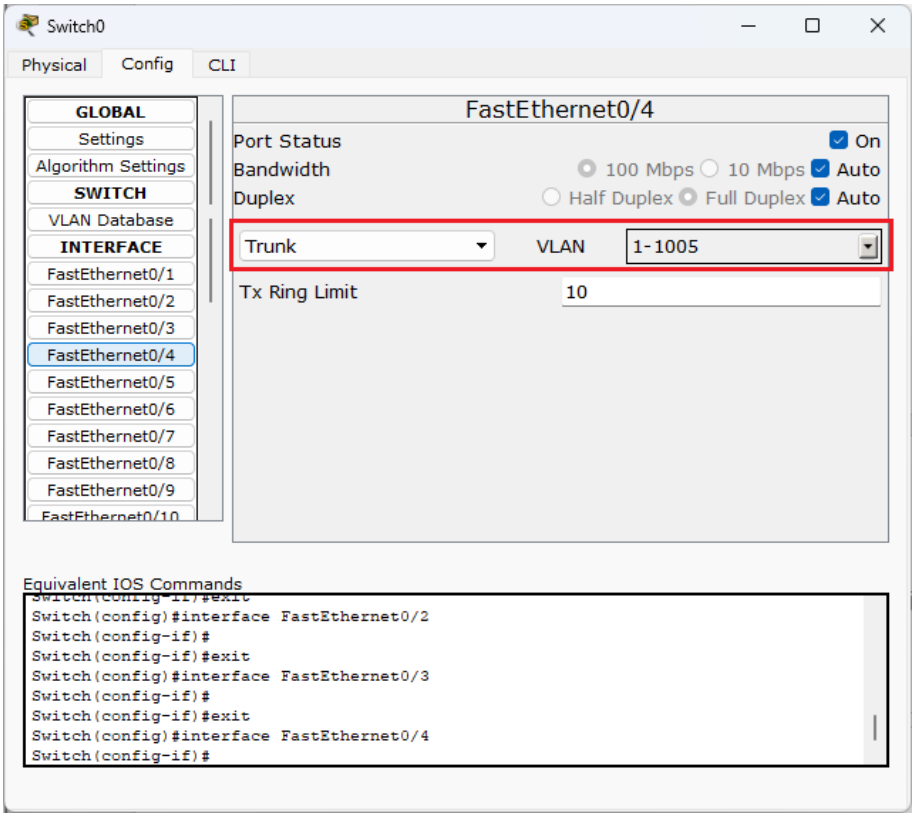
- PC1 配置：192.168.2.2 mask 255.255.255.0 F0/2 VLAN 20



- PC2 配置：192.168.3.3 mask 255.255.255.0 F0/3 VLAN 30



6. 在配置单臂路由前测试 PC0，PC1，PC2 之间相互 ping，查看并记录实验结果。
7. 配置交换机，将连接路由器的端口设置为 Trunk 模式，允许所有 VLAN 通过。



8. 在 Router0 的 CLI 中输入以下命令，配置单臂路由。

- 配置 VLAN10 的网关。

```
interface fa0/0.1
encapsulation dot1q 10
ip address 192.168.1.254 255.255.255.0
exit
```

- 配置 VLAN20 的网关。

```
interface fa0/0.2
encapsulation dot1q 20
ip address 192.168.2.254 255.255.255.0
exit
```

- 配置 VLAN30 的网关。

```
interface fa0/0.3
encapsulation dot1q 30
ip address 192.168.3.254 255.255.255.0
exit
```

9. 在配置单臂路由后测试 PC0,PC1,PC2 之间相互 ping,查看并记录实验结果。

【实验现象】

1. 在配置 VLAN 前，PC0，PC1，PC2 之间相互 ping，实验现象为：PC0、PC1、PC2 之间相互 ping 通，通信成功。
2. 在配置单臂路由前，PC0，PC1，PC2 之间相互 ping，实验现象为：用 PC0 分别 ping PC1、PC2，用 PC1 分别 ping PC0、PC2，用 PC2 分别 ping PC1、PC0. 均请求失败。
3. 在配置单臂路由后，PC0，PC1，PC2 之间相互 ping，实验现象为：PC0、PC1、PC2 之间相互 ping 通，通信成功。

【分析讨论】

一、配置 VLAN 前的 Ping 测试

在配置 VLAN 之前，PC0、PC1 和 PC2 位于同一个广播域内，没有进行 VLAN 划分。这意味着所有设备都在同一个网络中，可以自由地互相通信。因此，在实验现象中观察到 PC0、PC1、PC2 之间可以相互 ping 通且通信成功，这是因为在同一个 VLAN（或未划分 VLAN 时的默认 VLAN）中，所有设备都可以直接通过 MAC 地

址学习和 ARP 解析来发现对方的位置并进行通信。

二、配置单臂路由前的 Ping 测试

在对 PC0、PC1 和 PC2 配置不同的 VLAN 后（VLAN10, VLAN20, VLAN30），这三台 PC 机分别位于三个不同的广播域中。VLAN 的主要功能是进行网络隔离，使得不同 VLAN 的设备不能直接通信，除非通过路由器进行路由。由于在这一步中还没有配置单臂路由，路由器尚未对跨 VLAN 的数据包进行处理，因此 PC0、PC1 和 PC2 无法跨 VLAN 通信，导致实验现象中的 ping 请求失败。

三、配置单臂路由后的 Ping 测试

配置单臂路由后，路由器的每个子接口被配置为不同 VLAN 的网关。通过 802.1Q 标签技术，这些子接口可以正确地识别和处理来自不同 VLAN 的数据包。路由器为每个 VLAN 间提供了必要的路由功能，使得属于不同 VLAN 的 PC 机能够通过路由器相互通信。因此，在单臂路由配置完成后，PC0、PC1 和 PC2 能够成功进行跨 VLAN 的 ping 通信。这表明路由器正确地处理了 VLAN 间的路由需求，使得不同 VLAN 的设备可以根据需要安全地互联互通。

四、简单组网设计

（一）组网设计需求

某公司三个部门，每部门 20 人，每人一台 PC 机，每个部门在同一网段，部门内机器彼此可以互访，不同部门之间平时网络相互隔离，但三个部门的工作人员混在一起办公。假如年末，公司这三个部门之间网络需保持互通，以便网络互通“联欢”，请给出网络解决方案。

（二）组网设计方案

为满足三个部门内部互访及部门间隔离的需求，可以为每个部门设置独立的虚拟局域网（VLAN）。选择合适的私有地址空间和子网掩码，确保每个部门内足够的 IP 地址供分配，同时易于管理和扩展。

1. 给出网络规划、地址及掩码（内网地址）

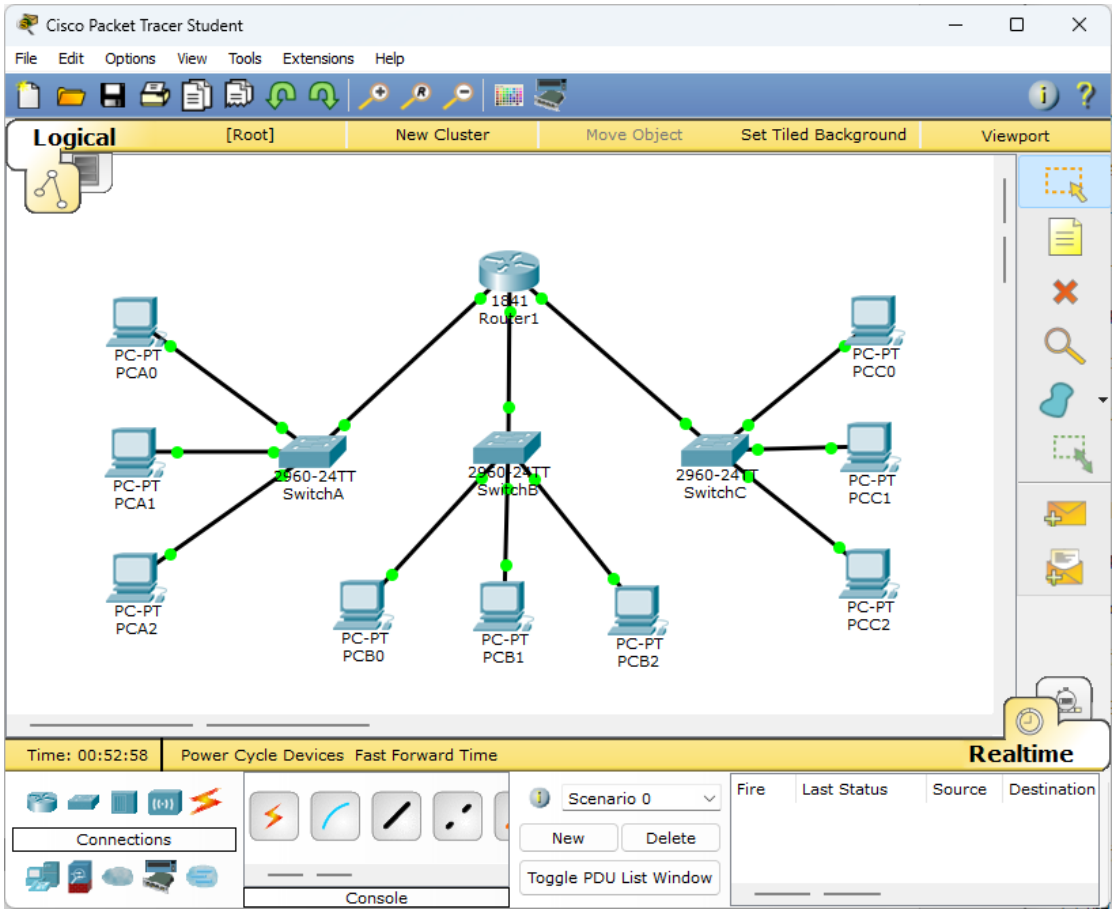
部门	部门 A	部门 B	部门 C
网络地址	192.168.10.0/24	192.168.20.0/24	192.168.30.0/24
广播地址	192.168.10.255	192.168.20.255	192.168.30.255
可用地址	192.168.10.1 至	192.168.20.1 至	192.168.30.1 至

	192.168.10.254	192.168.20.254	192.168.30.254
子网掩码	255.255.255.0	255.255.255.0	255.255.255.0

2. 规划硬件端口分配
   - 路由器：路由器配置三个子接口处理来自三个 VLAN 的数据。
     - fa0/0.10：VLAN10 的网关（192.168.10.254）
     - fa0/0.20：VLAN20 的网关（192.168.20.254）
     - fa0/0.30：VLAN30 的网关（192.168.30.254）
   - 交换机：配置为支持 Trunk 模式，连接路由器的 fa0/0 端口，确保所有 VLAN 数据能够通过一个物理接口传输。
   - PC 分配：每个部门分配 20 个端口，分别配置到对应的 VLAN。
3. 每个部门至少三个终端且配置（每部门三个为例）
   - 部门 A
     - PCA0：IP 192.168.10.1，掩码 255.255.255.0
     - PCA1：IP 192.168.10.2，掩码 255.255.255.0
     - PCA2：IP 192.168.10.3，掩码 255.255.255.0
   - 部门 B
     - PCB0：IP 192.168.20.1，掩码 255.255.255.0
     - PCB1：IP 192.168.20.2，掩码 255.255.255.0
     - PCB2：IP 192.168.20.3，掩码 255.255.255.0
   - 部门 C
     - PCC0：IP 192.168.30.1，掩码 255.255.255.0
     - PCC1：IP 192.168.30.2，掩码 255.255.255.0
     - PCC2：IP 192.168.30.3，掩码 255.255.255.0
4. 在模拟器配置

   使用 Cisco Packet Tracer 模拟器配置上述网络。包括路由器的子接口配置、交换机的 Trunk 配置、以及 PC 的静态 IP 配置。
5. 测试设备的连通性
   - VLAN 内连通性测试：在每个 VLAN 内部使用 ping 命令测试 PC 之间的连通性。

- VLAN 间连通性测试：初始配置下，VLAN 间不应通信，测试确认隔离性。



（三）年末联欢网络互通解决方案

为了在年末联欢时实现三个部门之间的网络互通，我们可以通过配置访问控制列表（ACL）来控制和管理 VLAN 间的流量。

1. 定义 ACL 规则

创建扩展 ACL 以允许每个 VLAN 内的主机访问其他两个 VLAN 的网络。需要为从每个 VLAN 到其他两个 VLAN 的通信分别创建一组规则。

- 部门 A 访问部门 B 和 C：

```
access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.20.0 0.0.0.255
access-list 101 permit ip 192.168.10.0 0.0.0.255 192.168.30.0 0.0.0.255
```

- 部门 B 访问部门 A 和 C：

```
access-list 102 permit ip 192.168.20.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 102 permit ip 192.168.20.0 0.0.0.255 192.168.30.0
```

```
0.0.0.255
```

- 部门 C 访问部门 A 和 B：

```
access-list 103 permit ip 192.168.30.0 0.0.0.255 192.168.10.0 0.0.0.255
access-list 103 permit ip 192.168.30.0 0.0.0.255 192.168.20.0 0.0.0.255
```

2. 应用 ACL 到路由器接口

将创建的 ACL 应用到路由器的相应子接口上，控制进出的数据包。对于每个子接口配置入站 ACL。

- 部门 A 访问部门 B 和 C：

```
interface fa0/0.10
ip access-group 101 in
```

- 部门 B 访问部门 A 和 C：

```
interface fa0/0.20
ip access-group 102 in
```

- 部门 C 访问部门 A 和 B：

```
interface fa0/0.30
ip access-group 103 in
```

3. 测试和验证

使用 ping 命令检查 ACL 规则是否正确实施，确保各部门能够相互访问，确保不影响部门内部的网络通信。

4. 临时性配置

记得在联欢活动结束后，移除对应的 ACL 设置，为联欢活动添加的特定规则，以保持原有的网络隔离策略。