**南京航空航天大学**

计算机科学与技术学院/软件学院

**实验设计报告**

|  |  |
| --- | --- |
| 课程名称： | 计算机网络 |
| 学 号： | 162230217 |
| 姓 名： | 陈梓鹏 |
| 专 业： | 软件工程 |

二〇二四年十月

目录

[一、 实验内容 3](#_Toc181042485)

[二、 实验分析和实验设计 3](#_Toc181042486)

[1. 可能应用的场景 3](#_Toc181042487)

[2. 采用的方案、技术、连接方式 4](#_Toc181042488)

[3. 拓扑 4](#_Toc181042489)

[4. 操作步骤 5](#_Toc181042490)

[5. 状态图 6](#_Toc181042491)

[三、 实验实现 6](#_Toc181042492)

[四、 实验运行结果 9](#_Toc181042493)

[五、 实验总结和心得 12](#_Toc181042494)

# 实验内容

PacketTracer实验，根据如图1拓扑选择设备并连接，要求：

* 在 SW1 和 SW2 上 均 配 置 VLAN10 和 VLAN20 • vlan10的IP地址：192.168.10.254 • vlan20的IP地址：192.168.20.254
* 在SW1和SW2上为VLAN分配端口； • PC1和PC3属于VLAN10； • PC2和PC4属于VLAN20；
* 为PC1-PC4分配合适的IP地址和网关；
* 分别查看SW1和SW2的配置文件。

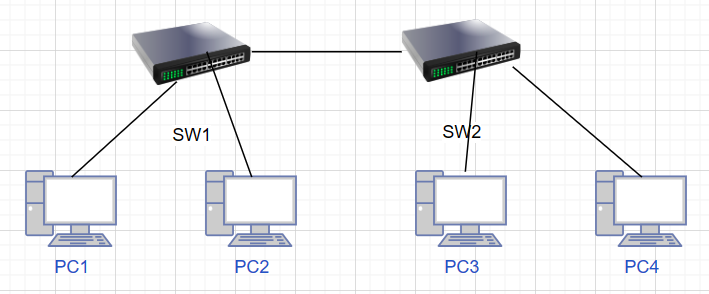


图1.网络拓扑示意图

# 实验分析和实验设计

### 可能应用的场景

**1.部门隔离**：

VLAN 配置可以用于将不同部门的设备分离，即使它们位于同一物理网络中。例如，PC1 和 PC3 可能代表财务部门的设备，属于 VLAN10，而 PC2 和 PC4 代表人力资源部门，属于 VLAN20。通过 VLAN 隔离，能够确保不同部门的网络流量互不干扰，提升安全性和效率。

**2.网络安全与管理**：

VLAN 隔离的一个关键应用是提高网络安全性。通过将不同部门、设备分配到不同的 VLAN，可以减少不同网络之间的广播域，降低广播风暴和网络攻击的可能性。并且，只有管理员或特定授权人员可以在交换机中配置和管理 VLAN。

### 采用的方案、技术、连接方式

**1. VLAN技术：**

* **方案**：实验中的核心技术是 VLAN。VLAN 技术可以将同一个物理网络划分为多个逻辑网络，每个 VLAN 可以有自己的广播域。通过 VLAN，网络管理员可以在一台交换机上配置不同的 VLAN 来隔离不同组的设备。
* **VLAN 配置**：在图中的交换机 SW1 和 SW2 上，分别配置了 VLAN10 和 VLAN20，并且给每个 VLAN 分配了相应的 IP 地址（例如 VLAN10 的IP为 192.168.10.254，VLAN20 的IP为 192.168.20.254）。

**2. Trunk 链路技术：**

* **方案**：两个交换机（SW1 和 SW2）之间的连接采用了 Trunk 链路。Trunk 是 VLAN 之间传输多 VLAN 数据的链路，允许多个 VLAN 的数据通过同一根物理链路进行传输。
* **作用**：Trunk 链路允许不同 VLAN 的流量在两个交换机之间传输，确保 SW1 和 SW2 上的 VLAN10 和 VLAN20 能够跨交换机通信。这样，PC1 和 PC3 可以位于不同的交换机上，但通过 Trunk 仍可以保持在同一 VLAN 中。

**3. IP 地址规划与网关配置：**

* **方案**：每个 VLAN 都有独立的 IP 地址规划，PC1 和 PC3（VLAN10）属于 192.168.10.0/24 网络，PC2 和 PC4（VLAN20）属于 192.168.20.0/24 网络。交换机分别为每个 VLAN 提供网关：
  + VLAN10 的IP是 192.168.10.254。
  + VLAN20 的IP是 192.168.20.254。

**4. 静态 VLAN 配置：**

* **方案**：通过静态方式手动将交换机端口分配给特定 VLAN。具体来说：
  + PC1 和 PC3 的端口被分配给 VLAN10。
  + PC2 和 PC4 的端口被分配给 VLAN20。

**5. 网络设备的物理连接：**

* **连接方式**：物理连接图中展示了典型的交换机与终端设备的连接方式：
  + PC1 和 PC2 分别通过直连网线连接到交换机 SW1 上。
  + PC3 和 PC4 通过直连网线连接到交换机 SW2 上。
  + SW1 和 SW2 之间通过一条链路连接，该链路作为 Trunk 链路，允许多 VLAN 数据通过。

### 拓扑

根据上述分析，我们可以得到如图2的拓扑图：

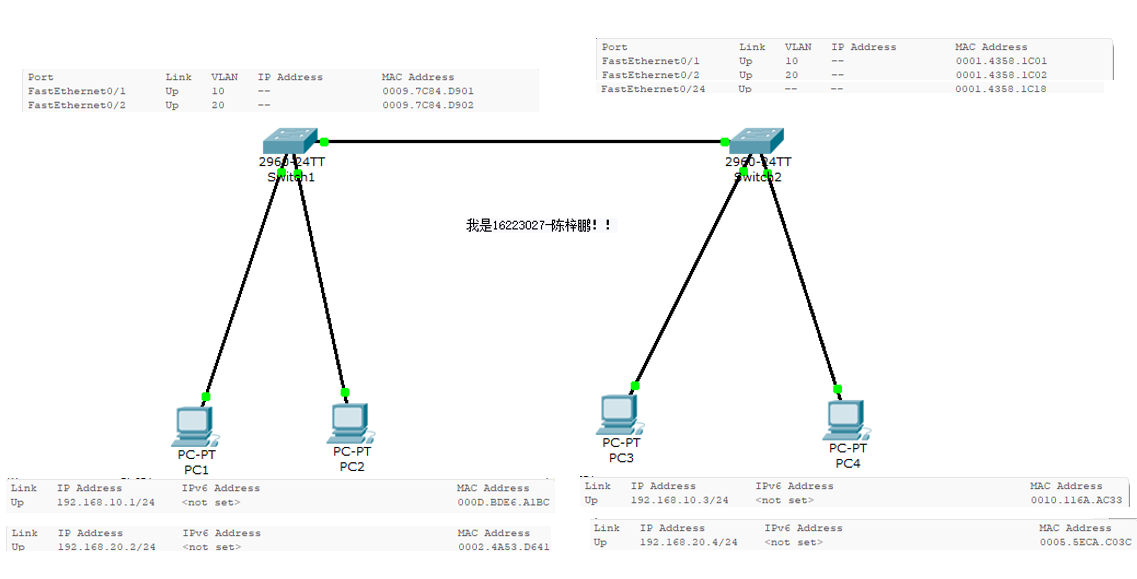
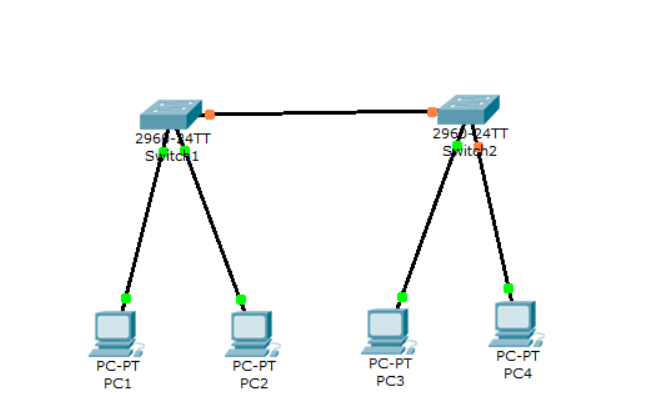
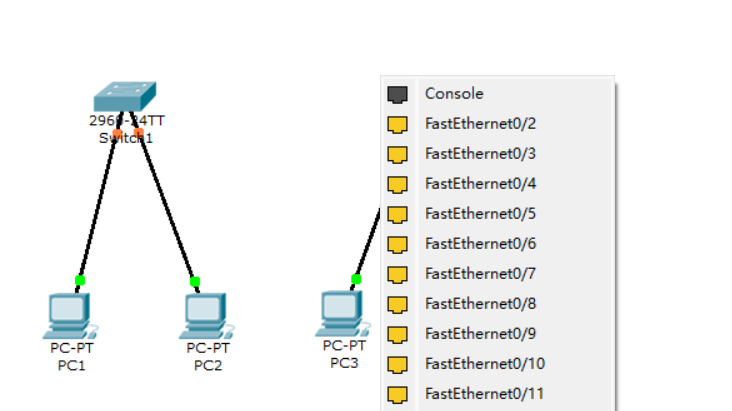
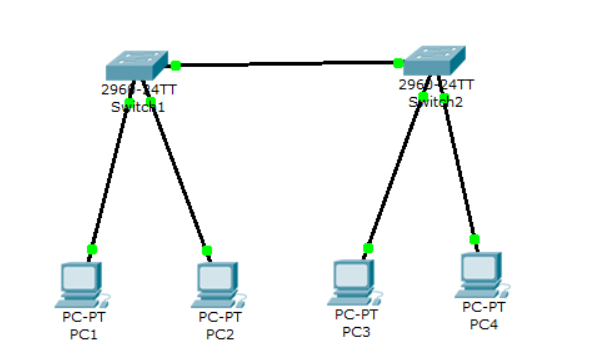


图2.实验拓扑图

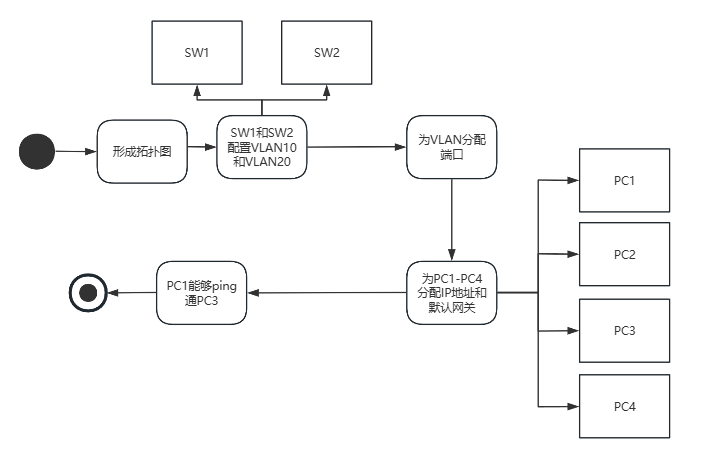
### 操作步骤

按如下步骤连接。（这里连接不复杂，不作赘述，具体接口信息可见第三节）





### 状态图



# 实验实现

首先对SW1进行配置

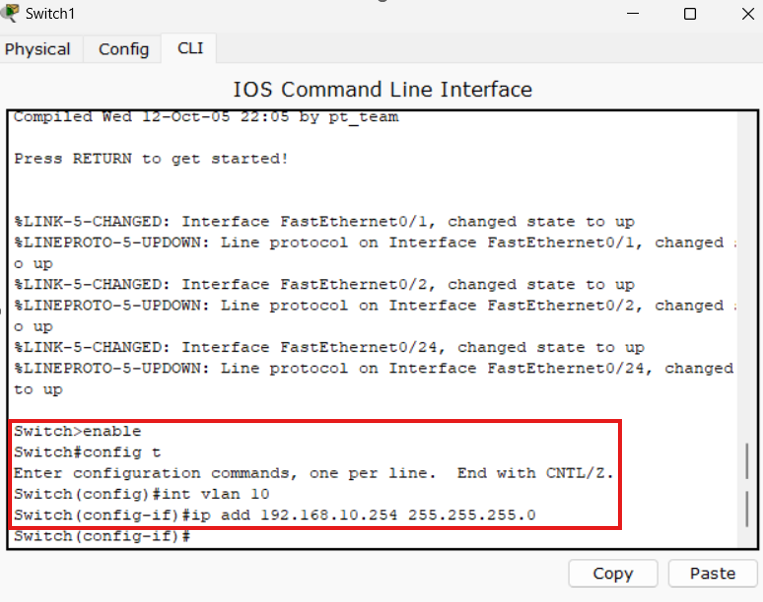
1.进入特权用户状态

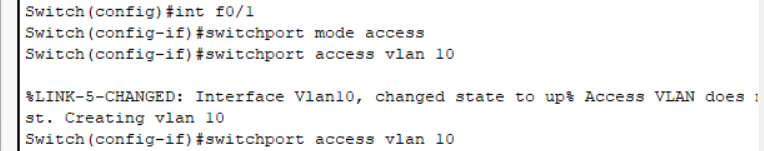
2.配置

3.创建（进入）vlan10

4.配置vlan10的ip和子网掩码并分配

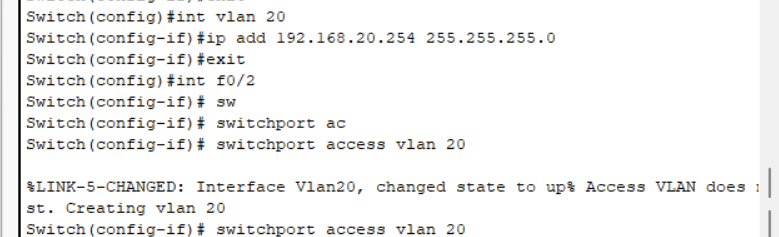
具体命令如图（红框）所示：



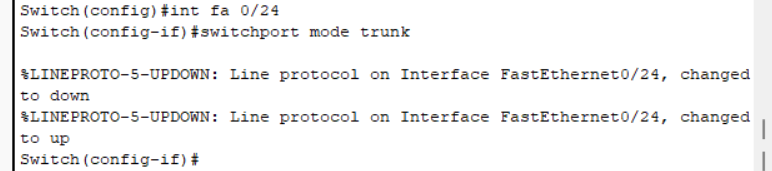


同时可以注意到配置成功后的提示。

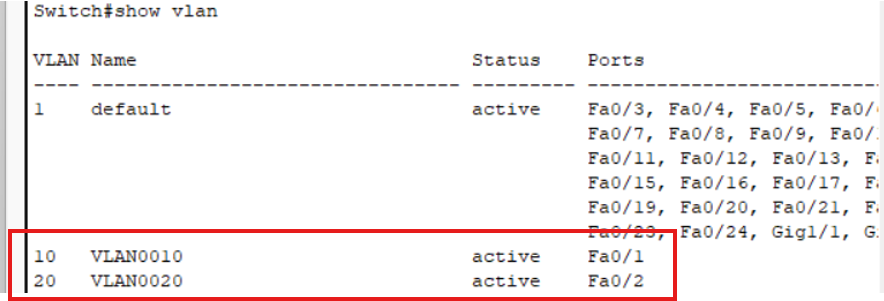
1. 对vlan20进行同样的操作



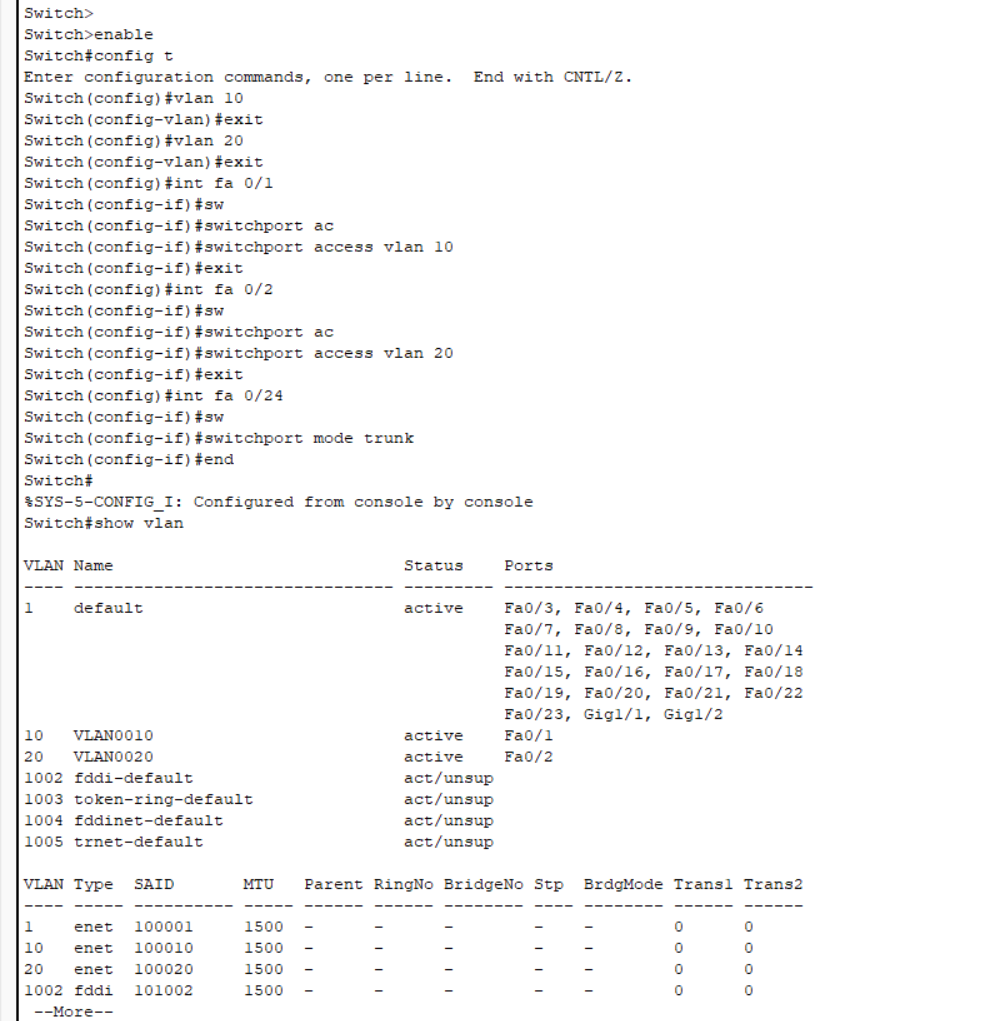
6.对端口0/24设置为trunk模式



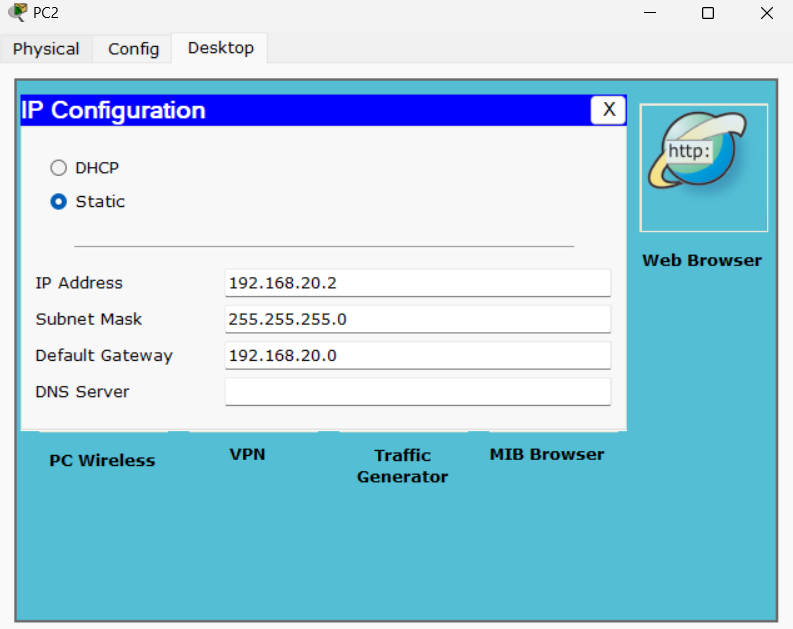
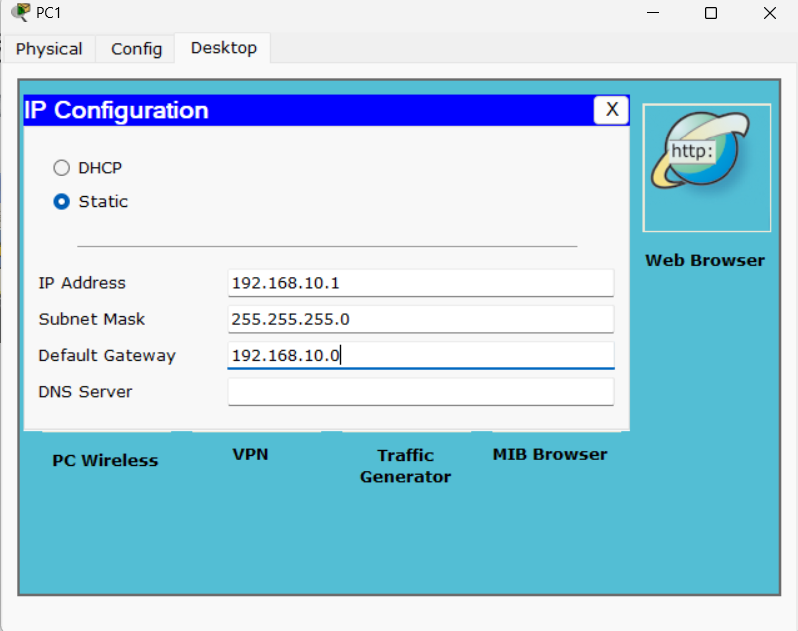
（Show vlan）

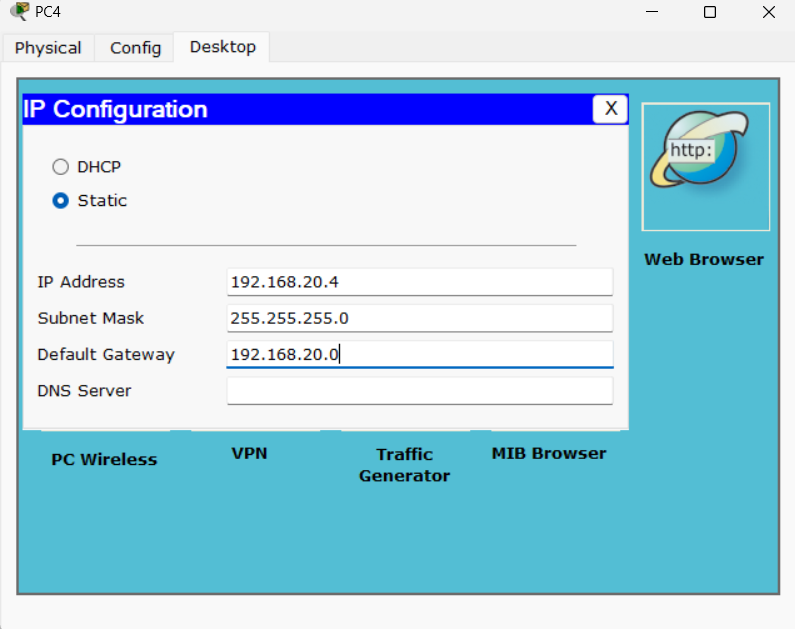
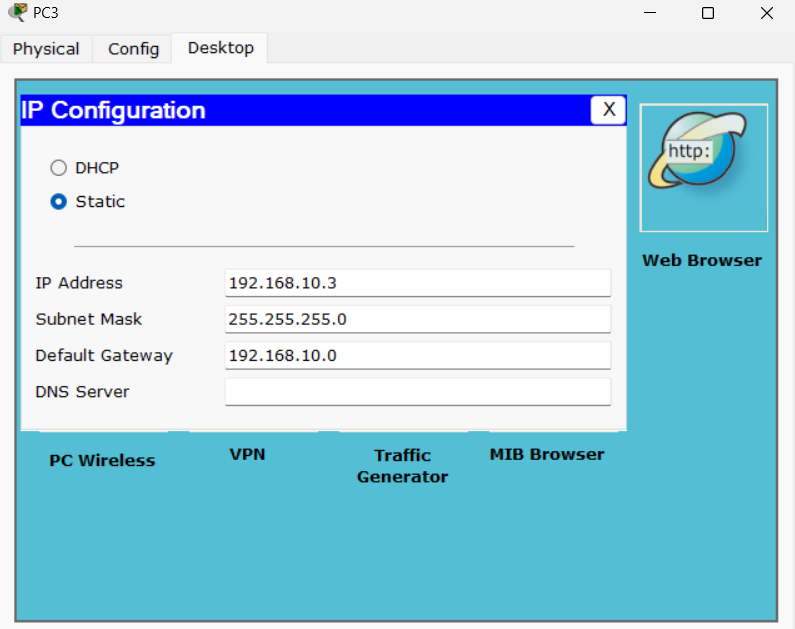


7.对S2进行相同操作 只是不用再进行ip地址划分



8.为主机设置ip地址：

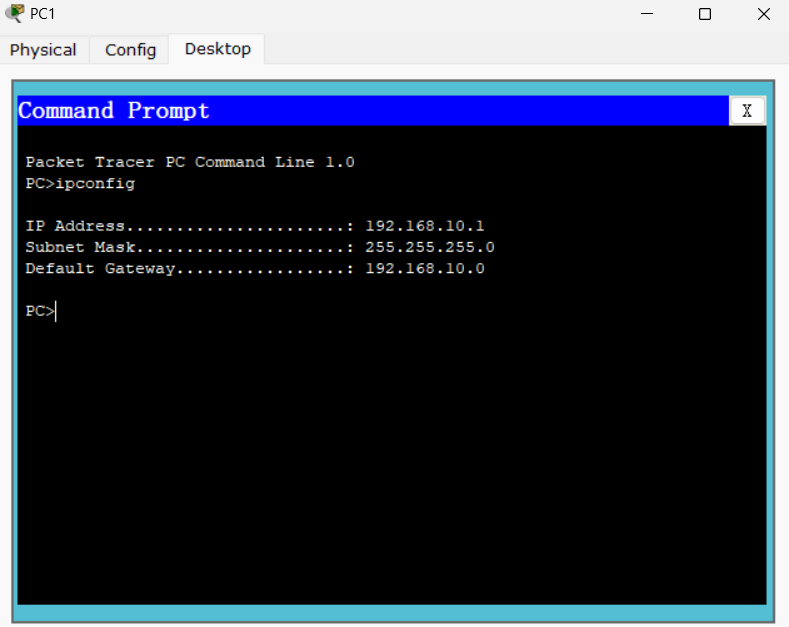




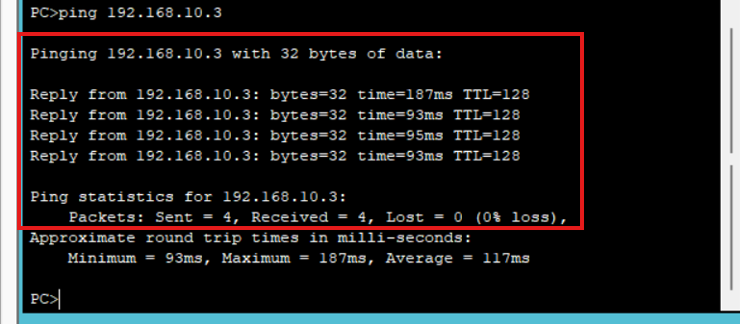
# 实验运行结果

我们这里对PC1进行测试：

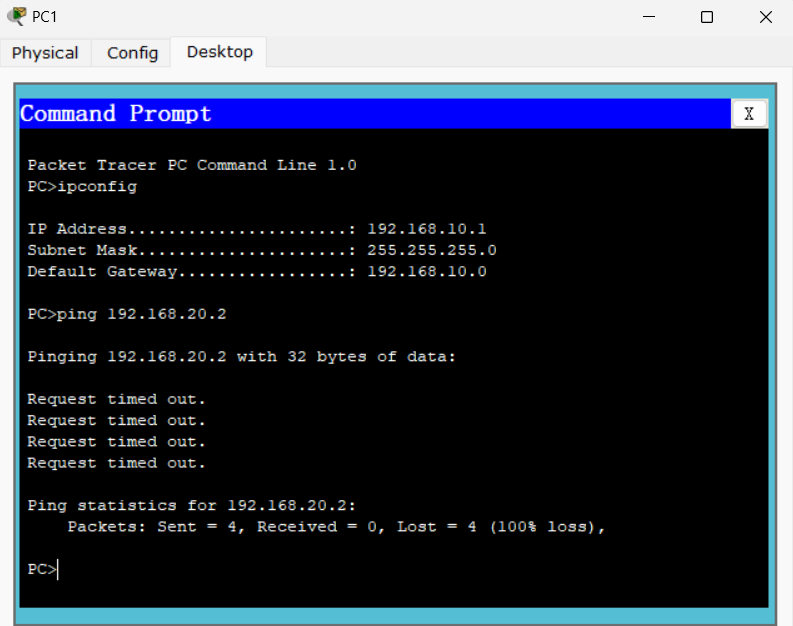
1. 首先查看PC1的IP



2. 测试192.168.10.3（即主机3）成功！

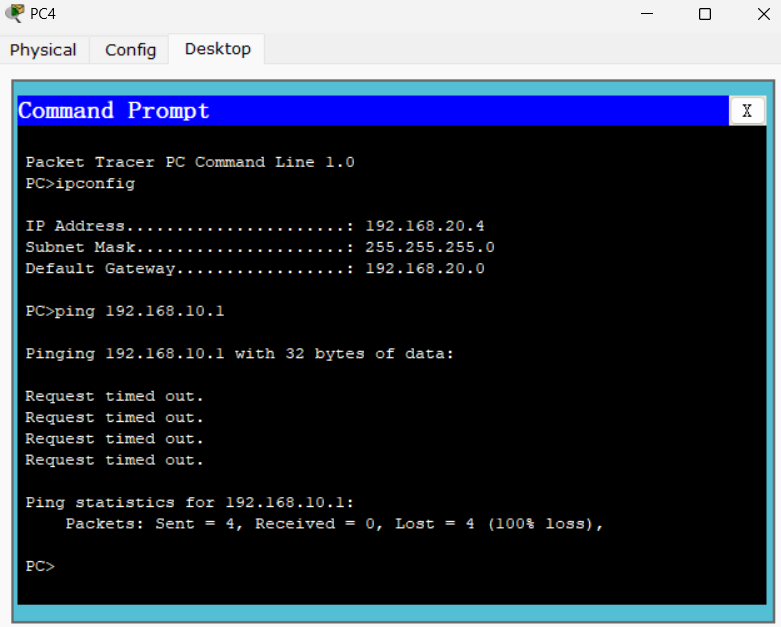


3.测试192.168.20.2 失败（符合预期，正确！）

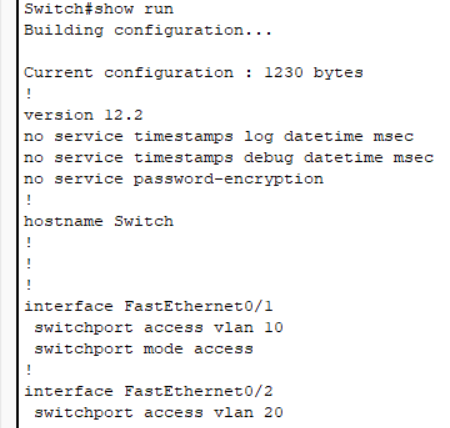


测试PC4：

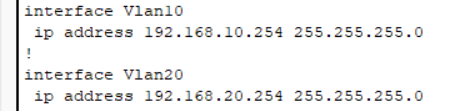
测试192.168.10.1（主机1）超时（符合预期，正确！）



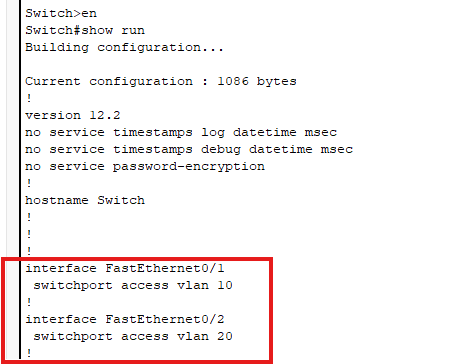
Show run查看SW1配置



键入空格触发mode可查看到vlan 10、20的ip



Show run查看SW2配置



# 实验总结和心得

VLAN 技术来实现不同设备之间的网络隔离和管理。实验虽然简单，但让我对 VLAN 和交换机之间的连接方式有了更清晰的认识。

首先，我们在 SW1 和 SW2 两台交换机上配置了两个 VLAN：VLAN10 和 VLAN20，分别分配了 192.168.10.254 和 192.168.20.254 的 IP 段。这一步其实就是划分了不同的“子网络”，让不同的 PC 属于各自的 VLAN 中。比如 PC1 和 PC3 被分到 VLAN10，而 PC2 和 PC4 属于 VLAN20。每个 VLAN 有自己的网关，就好比两个“独立的小社会”。

其次，交换机之间通过 Trunk 链路连接，这个“Trunk”有点像一个“大桥”，能够让不同 VLAN 的数据跨交换机传输，这样 PC1 虽然在 SW1 上，PC3 在 SW2 上，但它们还是可以互相通信的，因为它们在同一个 VLAN10 里面。

最后一步是给 PC 分配 IP 地址和网关，这个操作相对简单，就是确保每台电脑在自己的 VLAN 里有合适的网络地址，能通过网关访问其他 VLAN。

整个实验操作下来，其实 VLAN 的好处很明显：

1. **网络隔离**：不同的 PC 被分到了不同的 VLAN，互不干扰，特别适合企业或校园环境。
2. **提高效率**：通过 VLAN 减少了广播流量，提高了网络性能。
3. **更灵活**：即便设备在不同的交换机上，只要在同一个 VLAN 里，它们就像是在一个网络中一样，非常灵活。

总的来说，这次实验虽然涉及的技术不多，但对理解 VLAN 的作用非常有帮助。VLAN 和 Trunk 技术不仅能提高网络的管理效率，还能确保安全和性能，是现代网络中必不可少的一部分！