**实验24\_ARP消息分析实验**

**学生姓名:林觉凯 合作同学:无**

**实验地点:济事楼330 实验时间:2024.5.20**

【**实验目的**】

ARP(地址解析协议)是一种用于将IP地址映射到MAC地址的协议。通过本次ARP消息分析实验，我们可以具体地了解到ARP协议的作用，同时理解ARP协议解决逻辑地址到物理地址的映射问题，以及ARP协议在局域网中的作用。

【**实验原理**】

ARP协议

1. ARP出现原因

ARP协议是“Address Resolution Protocol”(地址解析协议)的缩写。其作用是在以太网环境中，数据的传输所依懒的是MAC地址而非IP地址，而将已知IP地址转换为MAC地址的工作是由ARP协议来完成的。在局域网中，网络中实际传输的是“帧”，帧里面是有目标主机的MAC地址的。在以太网中，一个主机和另一个主机进行直接通信，必须要知道目标主机的MAC地址。但这个目标MAC地址是如何获得的呢？它就是通过地址解析协议获得的。

所谓“地址解析”就是主机在发送帧前将目标IP地址转换成目标MAC地址的过程。ARP协议的基本功能就是通过目标设备的IP地址，查询目标设备的MAC地址，以保证通信的顺利进行。

2. ARP映射方式

2.1. 静态映射

静态映射的意思是要手动创建一张ARP表，把逻辑(IP)地址和物理地址关联起来。这个ARP表储存在网络中的每一台机器上。

例如，知道其机器的IP地址但不知道其物理地址的机器就可以通过查ARP表找出对应的物理地址。这样做有一定的局限性，因为物理地址可能发生变化：

(1)机器可能更换NIC(网络适配器)，结果变成一个新的物理地址。

(2)在某些局域网中，每当计算机加电时，他的物理地址都要改变一次。

(3)移动电脑可以从一个物理网络转移到另一个物理网络，这样会时物理地址改变。要避免这些问题出现，必须定期维护更新ARP表，此类比较麻烦而且会影响网络性能。

2.2. 动态映射

动态映射时，每次只要机器知道另一台机器的逻辑(IP)地址，就可以使用协议找出相对应的物理地址。已经设计出的实现了动态映射协议的有ARP和RARP两种。ARP把逻辑(IP)地址映射为物理地址。RARP把物理地址映射为逻辑(IP)地址。

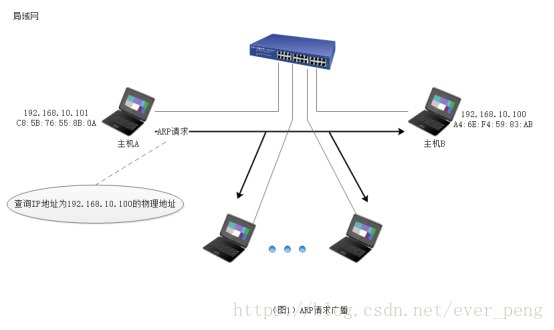
3. ARP原理及流程

在任何时候，一台主机有IP数据报文发送给另一台主机，它都要知道接收方的逻辑(IP)地址。但是IP地址必须封装成帧才能通过物理网络。

这就意味着发送方必须有接收方的物理(MAC)地址，因此需要完成逻辑地址到物理地址的映射。而ARP协议可以接收来自IP协议的逻辑地址，将其映射为相应的物理地址，然后把物理地址递交给数据链路层。

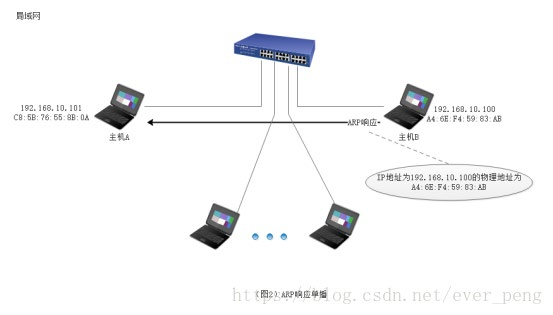
3.1.ARP请求

任何时候，当主机需要找出这个网络中的另一个主机的物理地址时，它就可以发送一个ARP请求报文，这个报文包好了发送方的MAC地址和IP地址以及接收方的IP地址。因为发送方不知道接收方的物理地址，所以这个查询分组会在网络层中进行广播。(见图1)



3.2.ARP响应

局域网中的每一台主机都会接受并处理这个ARP请求报文，然后进行验证，查看接收方的IP地址是不是自己的地址，只有验证成功的主机才会返回一个ARP响应报文，这个响应报文包含接收方的IP地址和物理地址。这个报文利用收到的ARP请求报文中的请求方物理地址以单播的方式直接发送给ARP请求报文的请求方。(见图2)



4.1.报文格式

硬件类型：16位字段，用来定义运行ARP的网络类型。每个局域网基于其类型被指派一个整数。例如：以太网的类型为1。ARP可用在任何物理网络上。

协议类型：16位字段，用来定义使用的协议。

例如：对IPv4协议这个字段是0800。ARP可用于任何高层协议

硬件长度：8位字段，用来定义物理地址的长度，以字节为单位。例如：对于以太网的值为6。

协议长度：8位字段，用来定义逻辑地址的长度，以字节为单位。例如：对于IPv4协议的值为4。

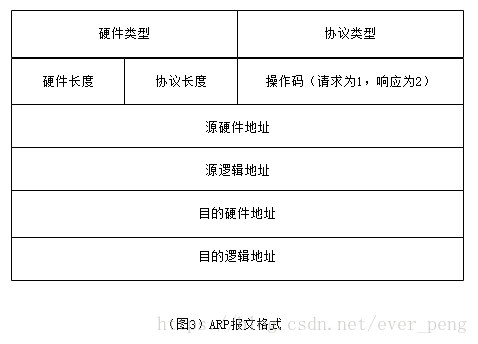
操作码：16位字段，用来定义报文的类型。已定义的分组类型有两种：ARP请求(1)，ARP响应(2)。

源硬件地址：这是一个可变长度字段，用来定义发送方的物理地址。例如：对于以太网这个字段的长度是6字节。

源逻辑地址：这是一个可变长度字段，用来定义发送方的逻辑(IP)地址。例如：对于IP协议这个字段的长度是4字节。目的硬件地址：这是一个可变长度字段，用来定义目标的物理地址，例如，对以太网来说这个字段位6字节。对于ARP请求报文，这个字段为全0，因为发送方并不知道目标的硬件地址。目的逻辑地址：这是一个可变长度字段，用来定义目标的逻辑(IP)地址，对于IPv4协议这个字段的长度为4个字节。

4. ARP协议报文字段抓包解析

4.1. 报文格式(见图3)



4.2. ARP报文总长度

ARP报文的总长度为64字节。首先要知道帧的概念 帧是在数据链路层传输

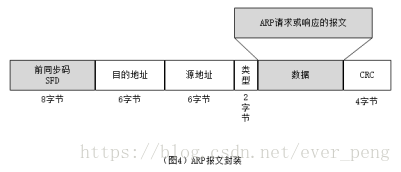
的数据格式，比如以太网v2，以太网IEEE802.3和PPP等。所以Wireshark抓到的帧是包含帧头的，即包含以太网v2的帧头，长14 bytes；而ARP数据包的长度固定为28 bytes；帧总长度=帧头+网络层包头+传输层报文头+应用数据；而ARP请求中ARP包已经是最高层，之上没有传输层和应用层，所以总长度为：

帧总长度=帧头+ARP包头=14+28=42 bytes；而真正发包的时为了保证以太网帧的最小帧长为64 bytes，会在报文里添加一个padding字段，用来填充数据包大小。使用wireshark抓包时，抓到的包为60 bytes。比以太网帧的最小帧长扫了4 bytes，原因是因为wireshark抓包时不能抓到数据包最后的CRC字段。

CRC字段是为了校验以太网帧的正确性。在数据包填充完成后，回去通过算法计算一个值放到数据包的CRC字段中。当接受端收到数据包后，会同样使用算法计算一个值，然后和CRC字段的值进行对比，查看是否相同。如果不同则证明数据包被更改，如果相同则证明数据包并未被更改。

4.3.报文封装

ARP报文直接封装在数据链路帧中，例如，图4中，ARP分组被封装在以太网的帧中。注意，帧中的类型字段指出此帧所携带的数据是ARP报文。



【**实验设备**】

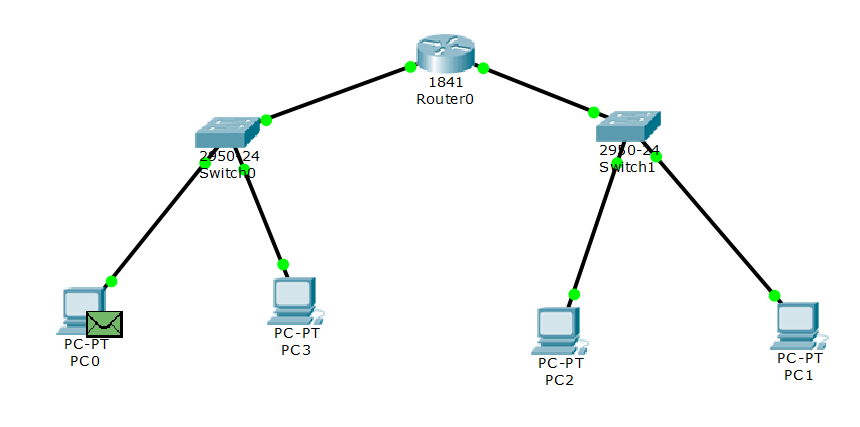
硬件设备：济事楼330机房电脑和本人的笔记本电脑

软件设备：Windows操作系统和Cisco Packet Tracer网络仿真软件

【**实验步骤**】

1.按照实验的要求放置网络设备并完成连线(如下图);

2.在仿真模式下发送请求，并抓取ARP报文并且分析报文;

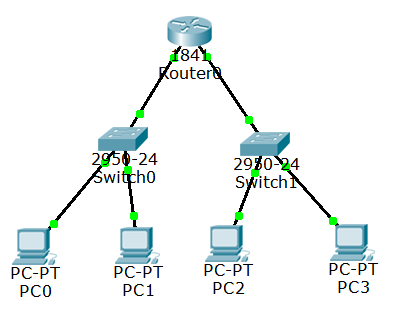
3.通过抓包软件Wireshark抓取ARP报文并分析。

【**实验现象**】

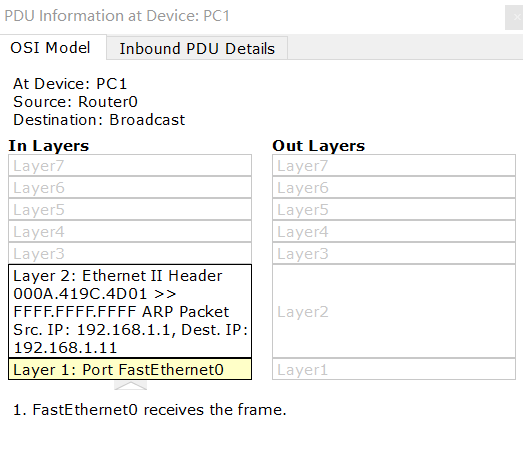
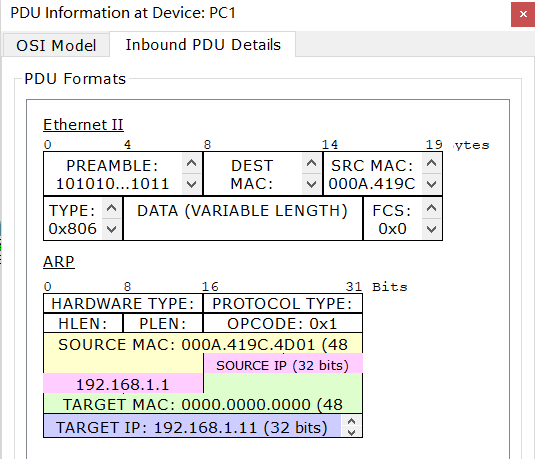
查看本人笔记本电脑的ARP

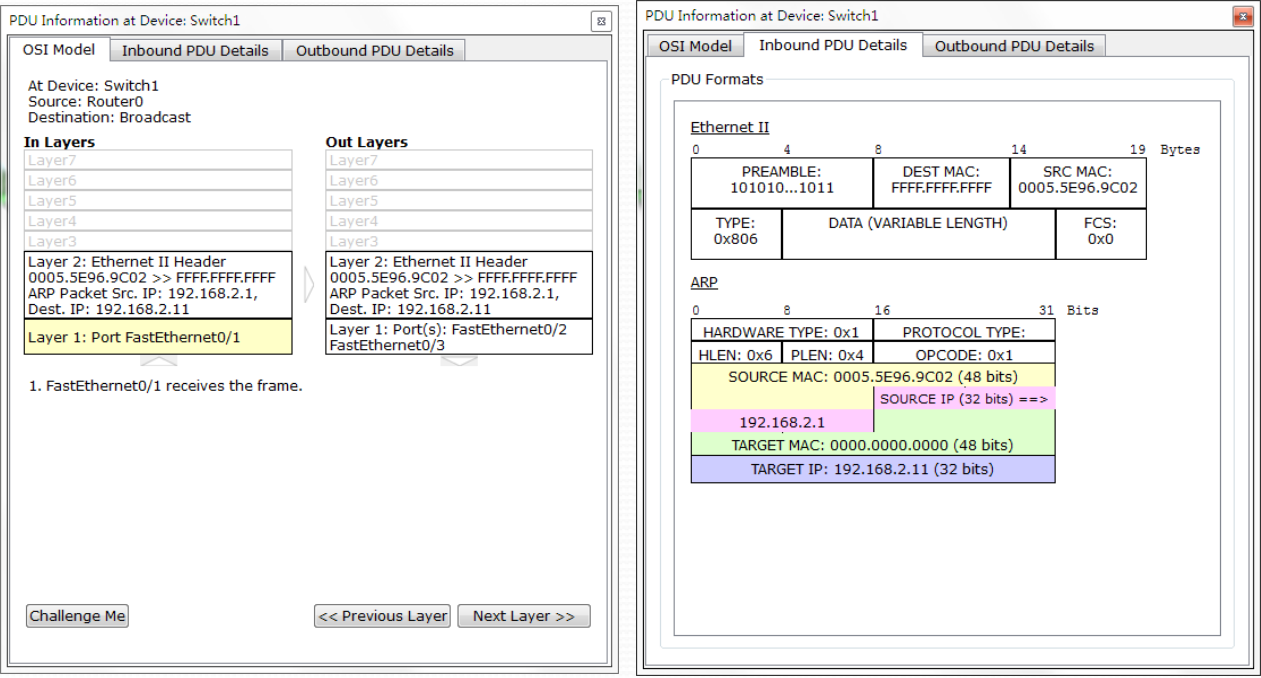


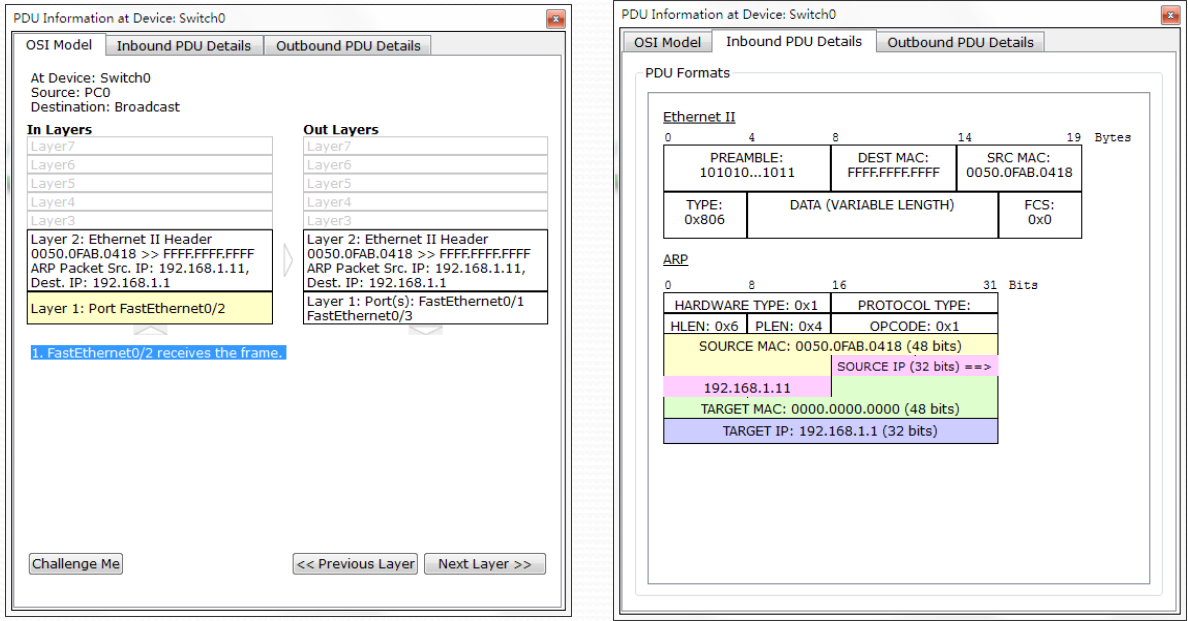
首先按照实验的要求完成拓扑图的连接与完善。

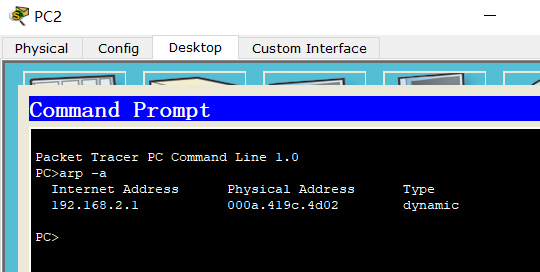


发送请求，并使用Packet Tracer抓取ARP报文并且分析报文;



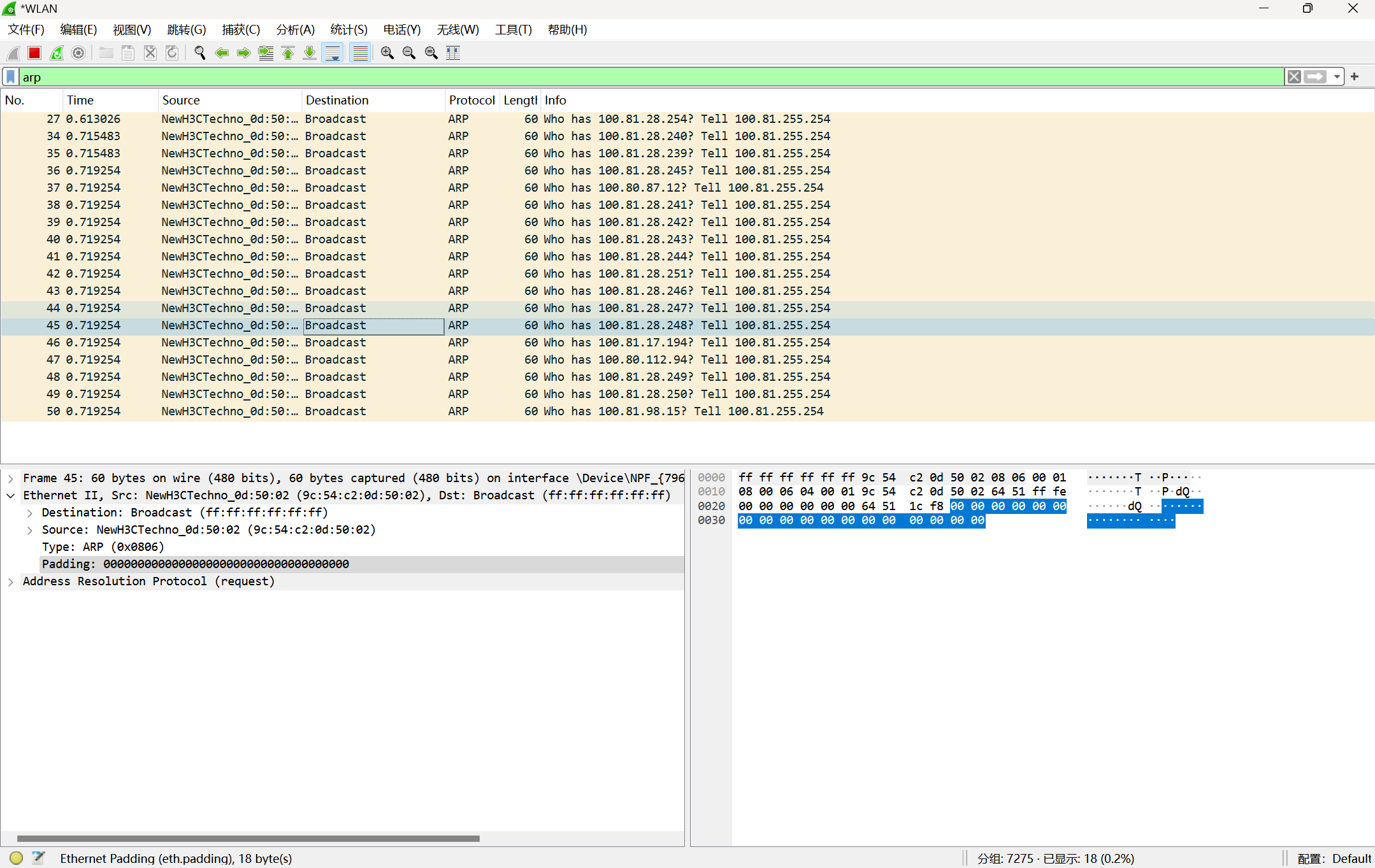




Packet Tracer 分析报文

查看终端的ARP命令

ARP -d

通过抓包软件Wireshark抓取ARP报文并分析。

00 01：目标硬件类型，这里是以太网。

08 00：目标协议类型，这里是IPv4。

06：硬件地址长度，通常为以太网地址的长度，即6字节。

04：协议地址长度，IPv4地址通常是4字节。

00 01：操作码，这里是请求(Request)。

9c 54 c2 0d 50 02：发送方以太网地址，即发送ARP请求的设备的MAC地址。

64 51 ff fe：发送方的IPv4地址，即发送ARP请求的设备的IP地址。

【**分析讨论**】

本次实验通过分析ARP请求和应答消息的数据包，我们深入理解地址解析协议的工作原理。实验中，我们学习了ARP消息的格式和含义，了解了如何通过ARP消息解析目标设备的MAC地址。这有助于我们更好地理解局域网中设备之间的通信过程，并学会利用ARP消息来诊断和解决网络通信中的问题。

ARP的工作原理可以简要概括为以下步骤：

ARP请求： 当主机A需要与目标主机B通信时，但不知道目标主机B的MAC地址时，主机A会在本地网络广播一个ARP请求，询问网络中是否有与目标IP地址相对应的MAC地址。

ARP应答： 目标主机B收到ARP请求后，如果知道自己的IP地址，就会直接发送一个ARP应答给主机A，包含自己的MAC地址。这个ARP应答是单播发送的，只有主机A会收到。

MAC地址映射： 主机A收到ARP应答后，会将目标IP地址和MAC地址的映射关系存储在本地的ARP缓存中，以便将来通信时直接使用。

ARP缓存： 主机A在ARP缓存中保存了目标IP地址和MAC地址的映射关系，这样在以后与目标主机B通信时，就不需要再次发送ARP请求，直接从ARP缓存中获取目标主机B的MAC地址即可。

ARP的工作原理简单而直接，它解决了IP地址到MAC地址的映射问题，使得设备能够在局域网上相互通信。

**实验28\_组网技术**

**学生姓名:林觉凯 合作同学:无**

**实验地点:济事楼330 实验时间:2024.5.20**

【**实验目的**】

单臂路由(Single Arm Routing)是一种网络设计模式，它只有一个物理接口用于连接到局域网或广域网，而该接口同时扮演着路由器和网络设备的角色。通过本次组网技术实验，我们可以初步了解单臂路由的工作原理和优缺点，以及它在网络设计和部署中的实际应用场景。

【**实验原理**】

单臂路由

1.单臂路由的概述

“单臂路由(router-on-a-stick)是指在路由器的一个接口上通过配置子接口(或“逻辑接口”，并不存在真正物理接口)的方式，实现原来相互隔离的不同VLAN(虚拟局域网)之间的互联互通。”交换机连接主机的端口为access链路交换机连接路由器的端口为Trunk链路。

2.单臂路由应用

VLAN能有效分割局域网，实现各网络区域之间的访问控制。但现实中，往往需要配置某些VLAN之间的互联互通。比如，某个公司划分为管理层、销售部、财务部、人力部、研发部、审计部，并为不同部门配置了不同的VLAN，部门之间不能相互访问，有效保证了各部门的信息安全。但经常出现管理部门需要跨越VLAN访问其他各个部门，这个功能就由单臂路由来实现。另外，单臂路由也具有较高的性价比！

3.单臂路由主要配置过程

(1)配置VLAN10 的网关

Router(config)#interface fa0/0.1 //进入第1个子接口，进行配置

Router(config-subif)#encapsulation dot1q 10 // 为这个接口配置802.1Q协议封装，最后面的10是vlan号;

Router(config-subif)#ip address 192.168.1.254 255.255.255.0 //为该接口划分网关地址和掩码。

Router(config-subif)#exit

(2)配置VLAN20 的网关

Router(config)#interface fa0/0.2 //进入第1个子接口，进行配置

Router(config-subif)#encapsulation dot1q 20 //为这个接口配置802.1Q协议封装，最后面的20是vlan号;

Router(config-subif)#ip address 192.168.2.254 255.255.255.0 //为该接口划分网关地址和掩码。

Router(config-subif)#exit

(3)配置VLAN30 的网关

Router(config)#interface fa0/0.3 //进入第1个子接口，进行配置

Router(config-subif)#encapsulation dot1q 30 //为这个接口配置802.1Q协议封装，最后面的30是vlan号;

Router(config-subif)#ip address 192.168.3.254 255.255.255.0 //为该接口划分网关地址和掩码。

Router(config-subif)#exit

【**实验设备**】

硬件设备：济事楼330机房电脑和本人的笔记本电脑

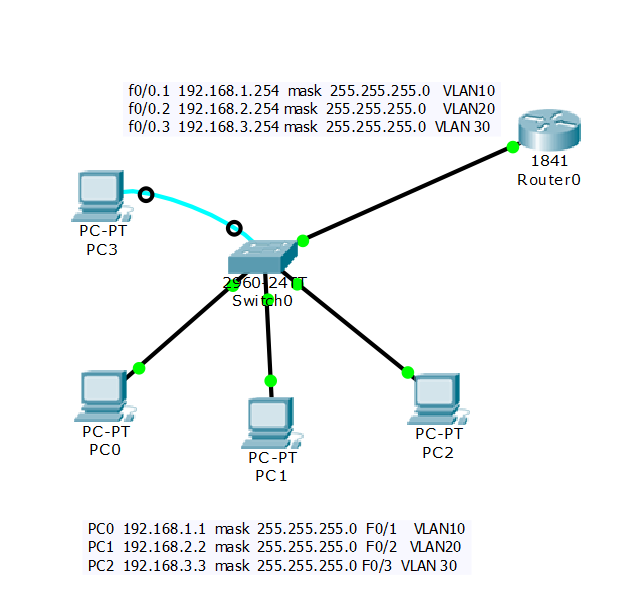
软件设备：Windows操作系统和Cisco Packet Tracer网络仿真软件

【**实验步骤**】

1.按照下图所示完成网络拓扑关系图的连接。

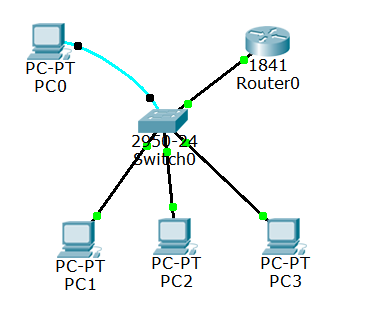
2.输入相应的命令(串)新建 VLAN10、VLAN20、VLAN30，并且分配相应的端口，完成相应的VLAN配置，并且观察是否可以ping连通。(即模拟每个部门在同一网段，部门内机器彼此可以互访，不同部门之间平时网络相互隔离)

3.配置单臂路由，完成相应的任务，最后再观察是否可以ping连通。(即模拟年末，公司这三个部门之间网络需保持互通，以便网络互通“联欢”)

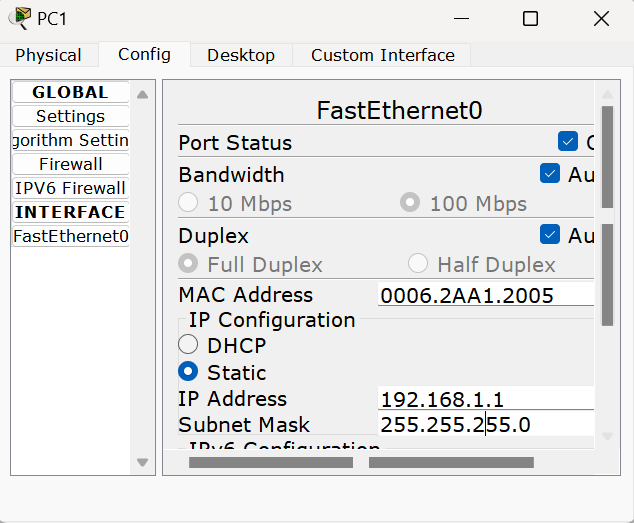
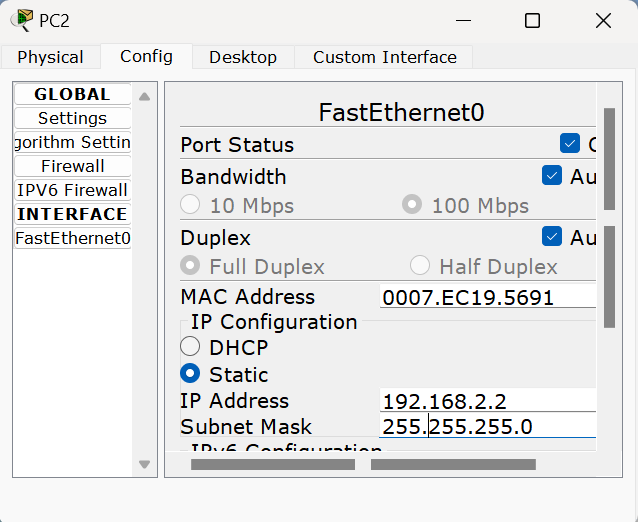
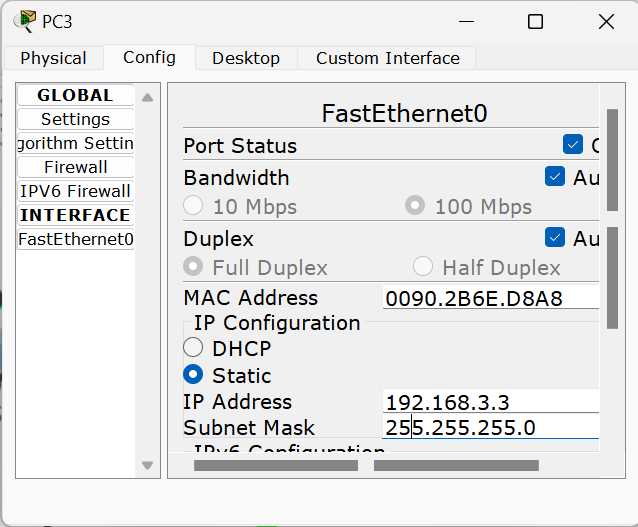


【**实验现象**】

首先打开模拟仿真软件，完成网络拓扑关系图的连接。



完成各个PC机的IP地址、子网掩码和网关。

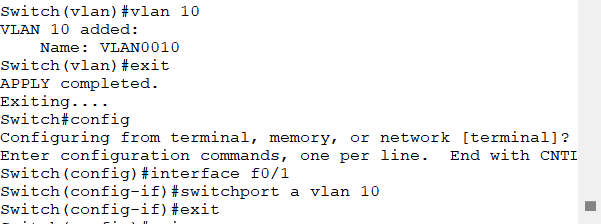


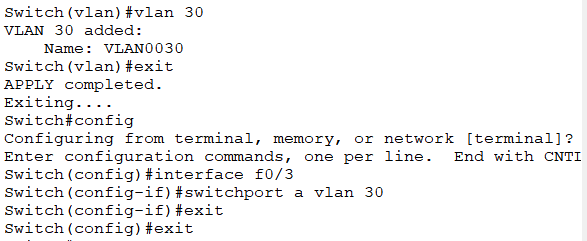
PC1:IP地址：192.168.1.1；子网掩码：255.255.255.0；网关：192.168.1.254

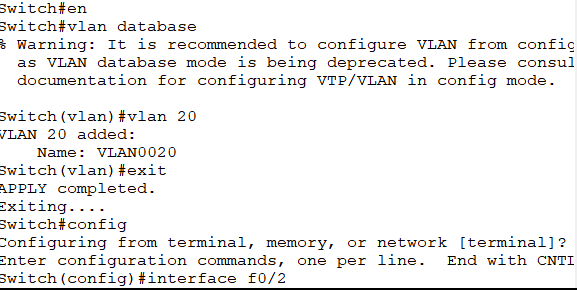
PC2:IP地址：192.168.2.2；子网掩码：255.255.255.0；网关：192.168.2.254

PC3:IP地址：192.168.3.3；子网掩码：255.255.255.0；网关：192.168.3.254

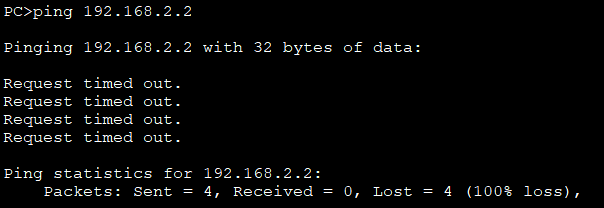
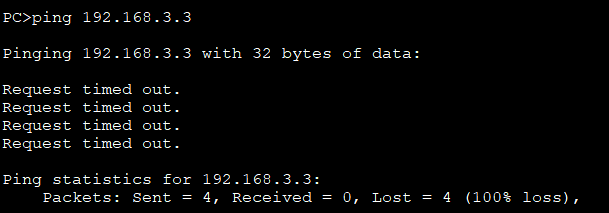
接下来按照先前的实验内容配置vlan10、vlan20、vlan30。





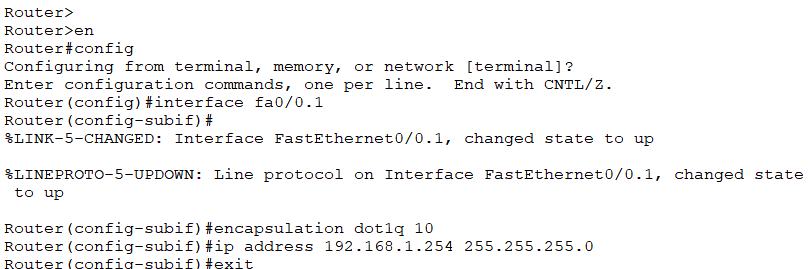
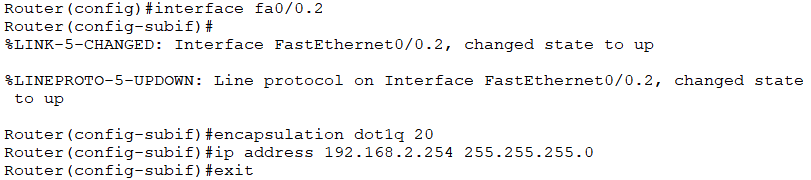


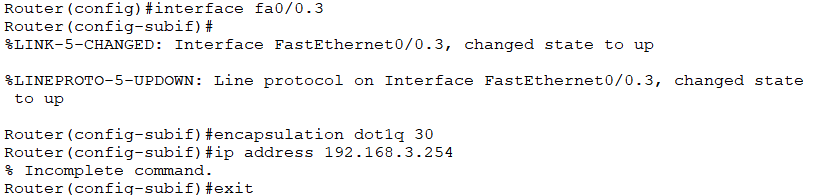
以PC1为例，ping其余两台PC机。



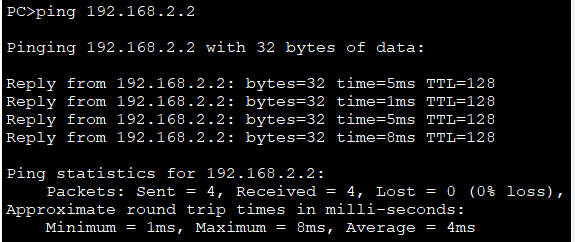
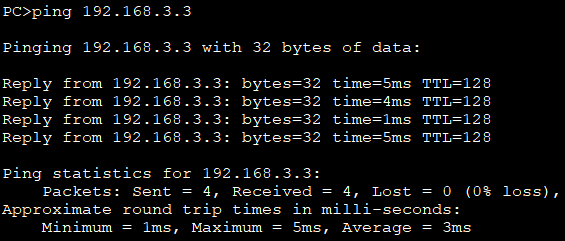
我们发现，此时是ping不通的，这是因为，当配置了不同的VLAN后，同一个交换机下的PC处于不同的VLAN中，而VLAN之间默认是隔离的。这样就实现了模拟每个部门在同一网段，部门内机器彼此可以互访，不同部门之间平时网络相互隔离这种情况。

接着我们利用路由器配置对应的单臂路由。





我们这时候再次以PC1为例，ping其余两台PC机。



我们发现，配置好单臂路由后，可以互相ping通。这样就实现了模拟在年末，公司这三个部门之间网络需保持互通，以便网络互通“联欢”。这是因为当设备位于不同部门时，单臂路由器会根据其路由表进行路由处理，并将流量转发到正确的部门。单臂路由器具有路由不同部门之间的流量的能力，因此可以实现不同部门之间的连通。

如果有更多的终端，也可以依照上文的方法配置相应的单臂路由，实现更多部门终端之间的互通。

【**分析讨论**】

本次实验的内容与学期初的一个实验相联系，这也让我复习了先前了解到的知识。通过本次实验，我学会了如何配置和管理单臂路由器，以及如何处理本地流量和路由外部流量。我不仅提升了对单臂路由技术的理解，也提高了网络配置和管理的能力。同时，知识的互相交互，前后应用，也让我受益匪浅。

单臂路由是一种网络设计模式，通常用于实现特定的网络功能或优化网络架构。在单臂路由中，只有一个物理接口用于连接到网络，同时该接口充当了路由器和网络设备的角色。它的工作原理如下：

接收流量： 单臂路由器接收来自网络的所有流量，包括本地流量和路由外部流量。处理本地流量： 如果接收到的流量是本地网络之间的通信，则单臂路由器直接转发流量，无需进行路由处理。路由外部流量： 如果接收到的流量需要通过路由器转发到另一个网络，则单臂路由器会根据其路由表进行路由处理，并将流量转发到正确的网络。NAT转换： 在某些情况下，单臂路由器可能会执行网络地址转换（NAT），以确保流量离开局域网时具有正确的源地址。

单臂路由具有以下优点：

节省成本： 单臂路由器通常只需要一个物理接口，因此在硬件和部署成本上相对较低。简化配置： 单臂路由器只需要管理一个物理接口的配置，而不必担心多个接口的配置和管理。灵活性： 单臂路由器可以灵活地部署于各种网络环境中，并且可以根据需求进行快速调整和扩展。

单臂路由的应用场景：

虚拟专用网(VPN)：单臂路由可用于建立VPN连接，实现远程访问和安全通信。访问控制列表(ACL)：单臂路由可用于配置和管理网络访问控制列表，控制流量的访问权限。网络监控和流量分析：单臂路由可用于监控网络流量，并进行分析和管理。

在实际应用中，单臂路由可以作为组网技术的一部分，用于实现特定的网络架构和功能。例如，在建立虚拟专用网(VPN)或设置访问控制列表(ACL)时，可以使用单臂路由来简化网络设计，并且通过组网技术将其与其他设备整合在一起，以实现完整的网络解决方案。