**西安电子科技大学网信院**

**《组网与运维》**

**线 上 实 验 报 告**

**班级：xxxxxxx**

**姓名：xxxxxx**

**学号：xxxxxxxxxxx**

**日期：2021/12/12**

# 1.集线器与交换机的对比实验

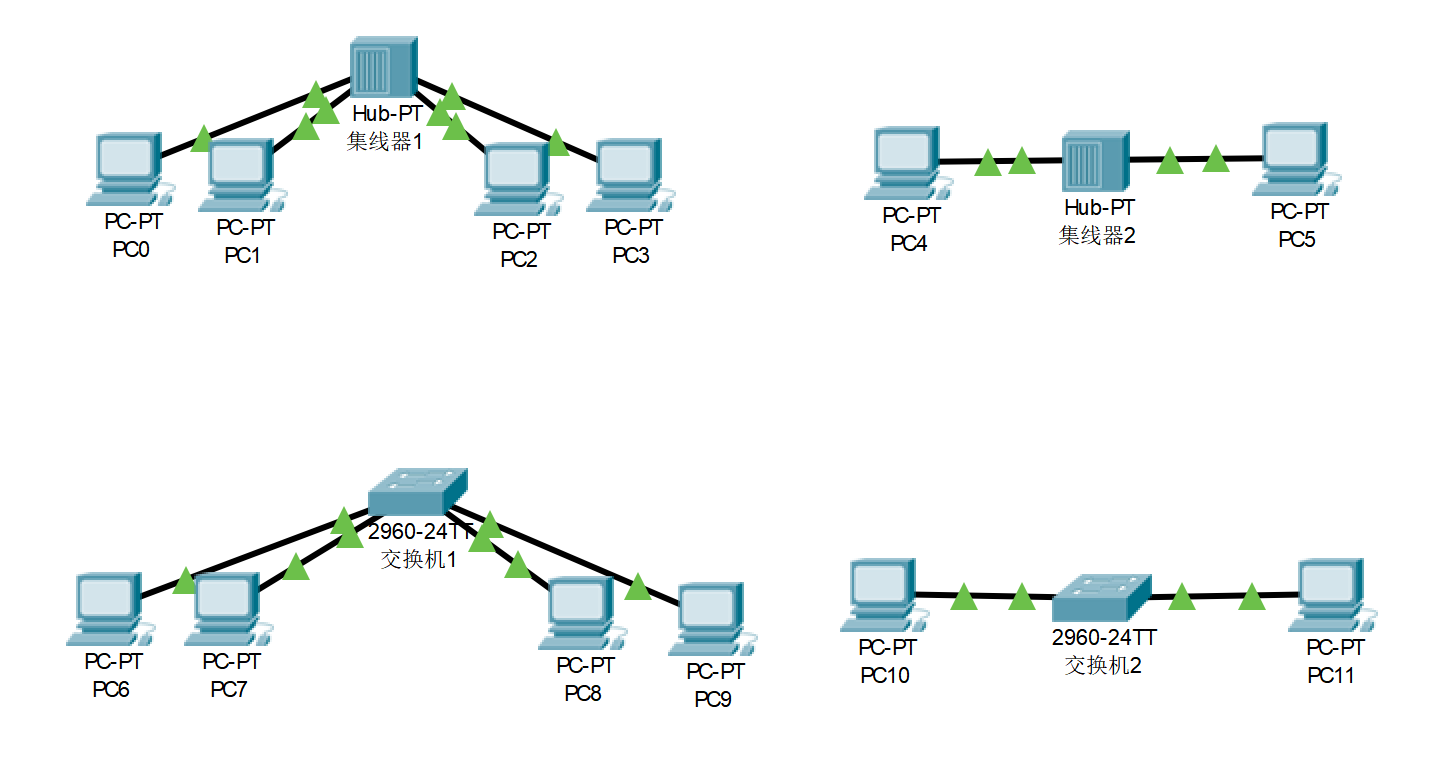
## 一、实验目的

1. 了解集线器和交换机如何转发数据。
2. 理解冲突域和广播域的概念。
3. 理解集线器和交换机在扩大网络规模中的作用和局限性。

## 二、实验步骤

1. 给出实验中用到的4个拓扑图

（不能从老师的资料中截图，从自己的界面里截图）



1. 给出实验中使用的IP配置表

（不能从老师的资料中截图，自己制表）

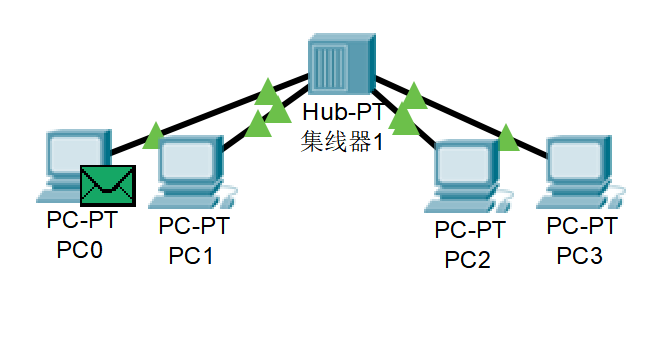
|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 主机名 | IP地址 | 子网掩码 | 主机名 | IP地址 | 子网掩码 |
| PC0 | 192.168.1.1 | 255.255.255.0 | PC6 | 192.168.1.1 | 255.255.255.0 |
| PC1 | 192.168.1.2 | 255.255.255.0 | PC7 | 192.168.1.2 | 255.255.255.0 |
| PC2 | 192.168.1.3 | 255.255.255.0 | PC8 | 192.168.1.3 | 255.255.255.0 |
| PC3 | 192.168.1.4 | 255.255.255.0 | PC9 | 192.168.1.4 | 255.255.255.0 |
| PC4 | 192.168.1.5 | 255.255.255.0 | PC10 | 192.168.1.5 | 255.255.255.0 |
| PC5 | 192.168.1.6 | 255.255.255.0 | PC11 | 192.168.1.6 | 255.255.255.0 |

1. 任务一：观察集线器和交换机的运行

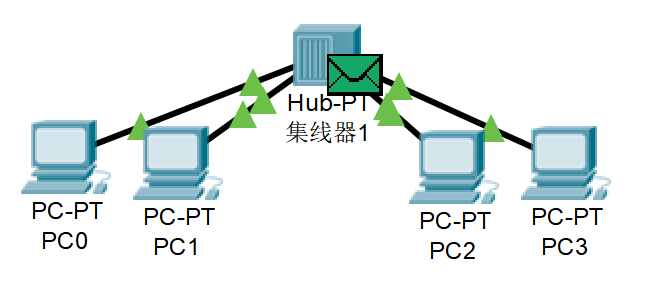
（根据教材或老师给的详细资料，使用自己的语言描述实验步骤，在文字描述的同时，尽量多截图说明）

（1）集线器对单播包的处理

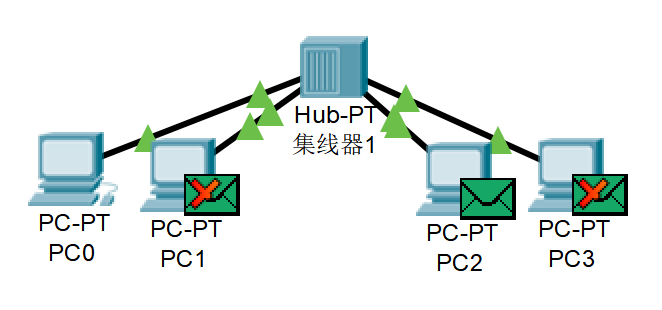
从PC0向PC2发送数据包



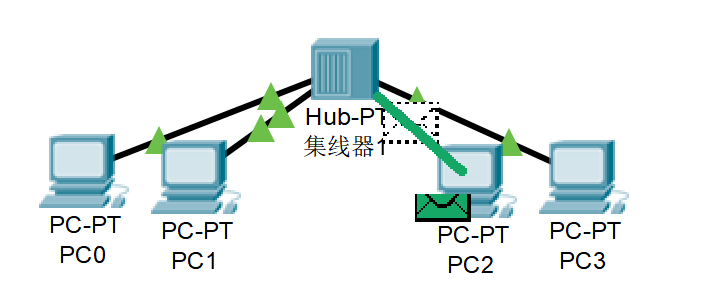
首先数据包被发送到集线器



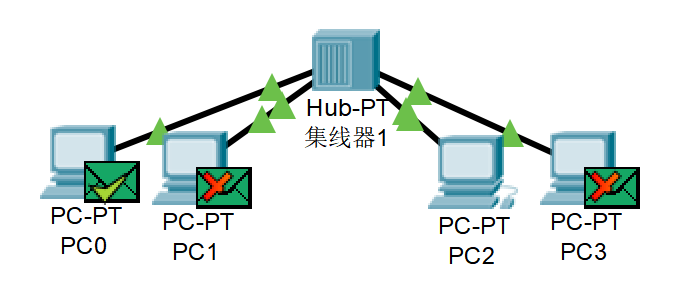
集线器向PC1,PC2,PC3转发改数据包，PC1和PC3收到数据包后，发现不是传给自己的所有丢弃到，只有PC2接受该数据包。



PC2接收该数据包后对PC0进行应答，首先向集线器发送数据包。

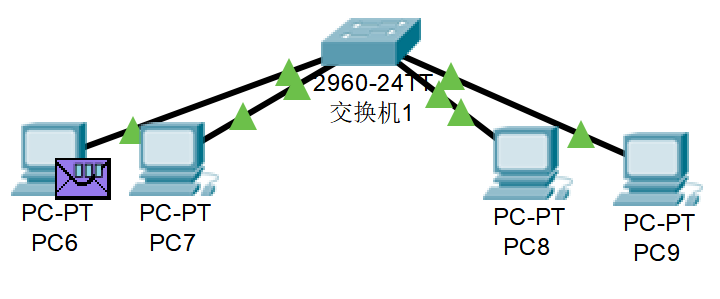


集线器收到该数据包后向PC0,PC1和PC3进行转发，PC1和PC3收到数据包后，发现不是传给自己的所有丢弃到，只有PC0接受该数据包。

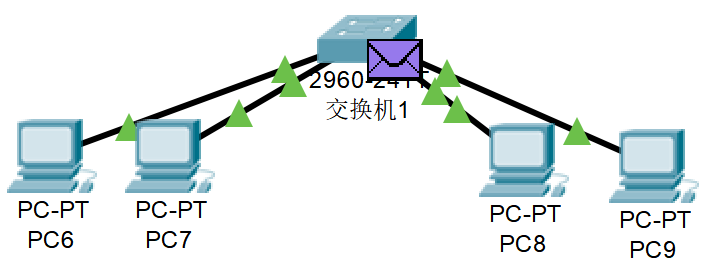


（2）交换机对单播包的处理

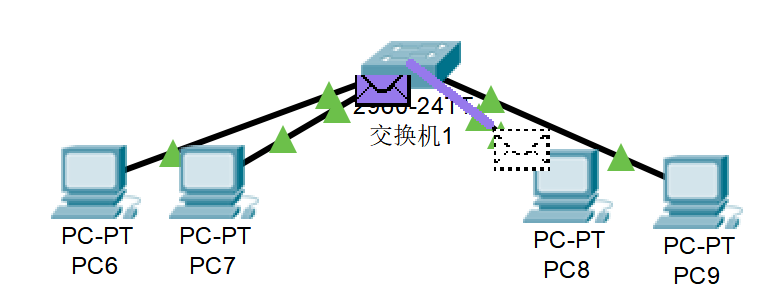
从PC6向PC8发送数据包

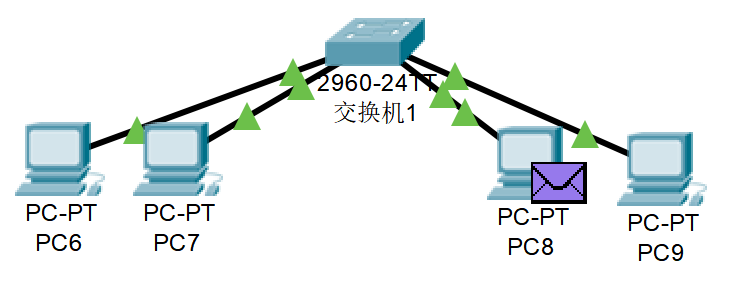


首先数据包被发送到交换机

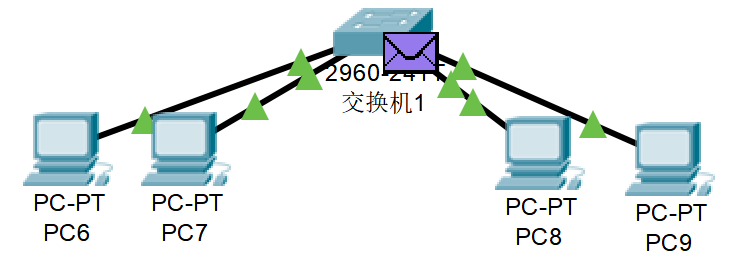


交换机直接向PC8转发该数据包





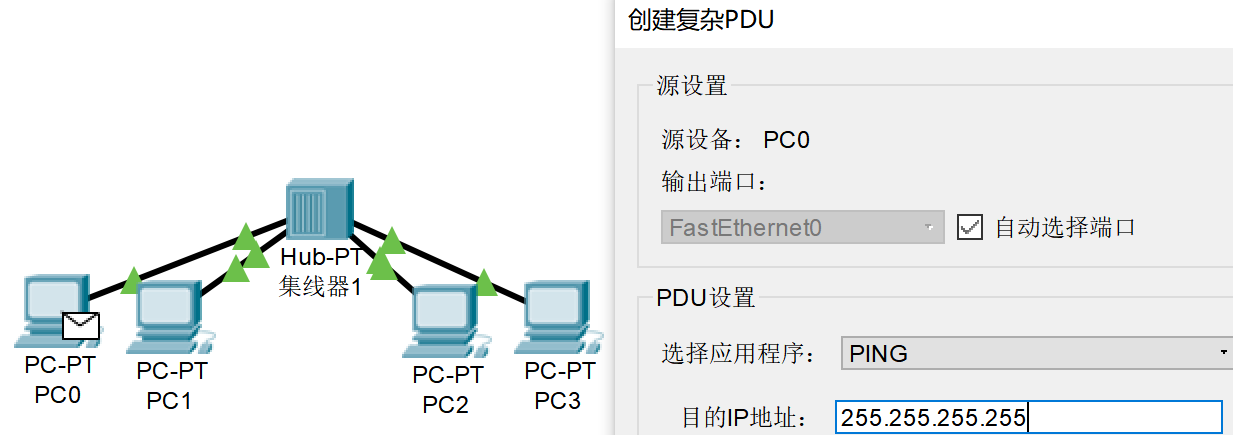
PC8接收该数据包后对PC6进行应答，首先向交换机发送数据包。

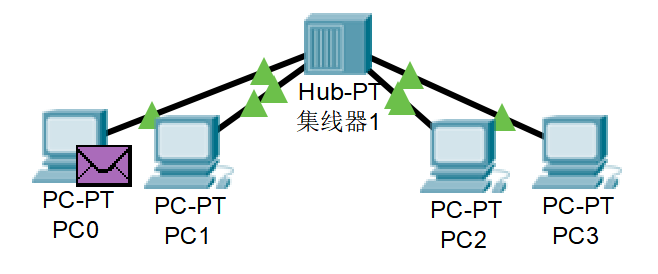


交换机收到该数据包后直接向PC6进行转发，PC6收到该数据包后,确认了PC8收到了它所发出的数据包。

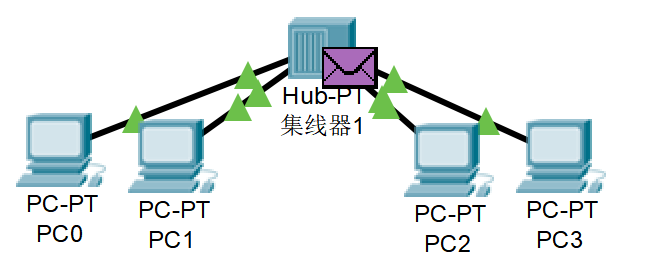
（3）集线器对广播包的处理

从PC0发送了一个广播包，目的IP地址设置为广播地址255.255.255.255

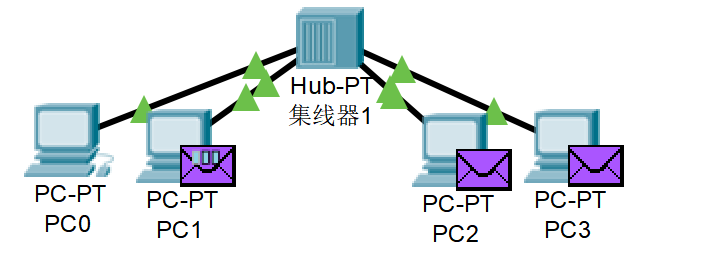




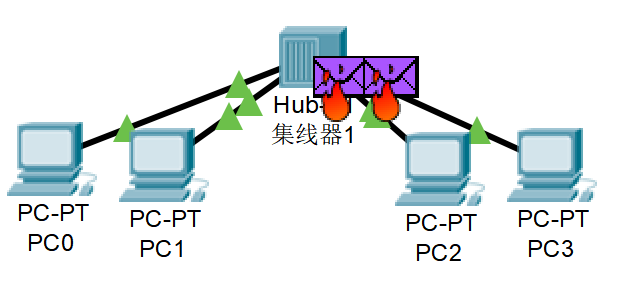
首先数据包被发送到集线器



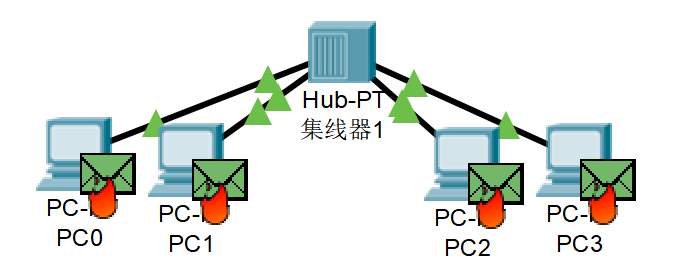
集线器向PC1,PC2,PC3转发数据包



PC1,PC2,PC3收到数据包后对PC1进行应答，向集线器发送数据包，这时造成了冲突。

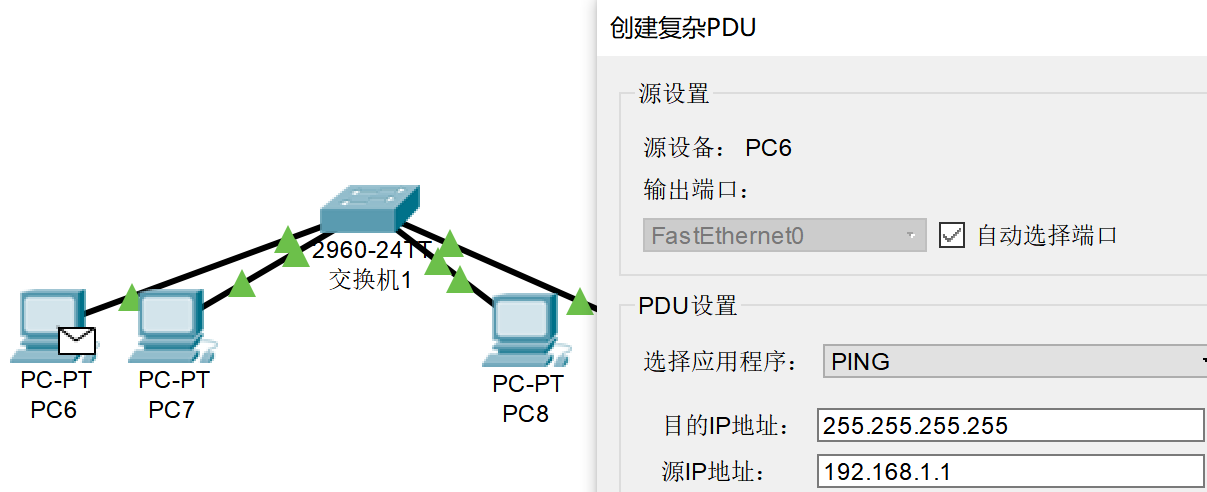


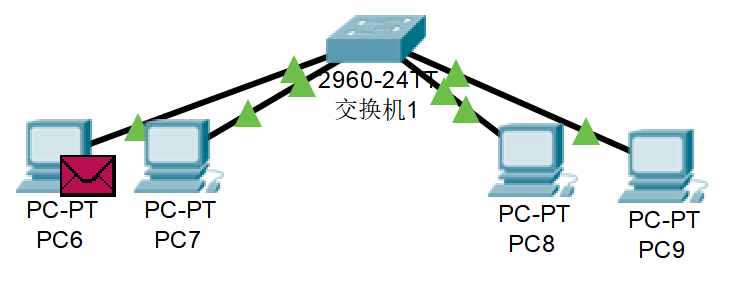
集线器发现冲突后，向PC0,PC1,PC2,PC3发送数据包，告知它们发生了冲突。



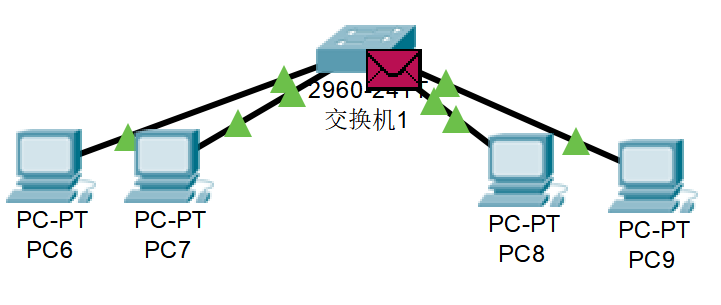
（4）交换机对广播包的处理

从PC6发送了一个广播包，目的IP地址设置为广播地址255.255.255.255

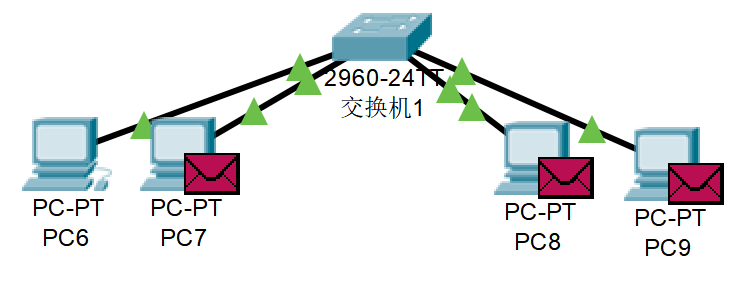




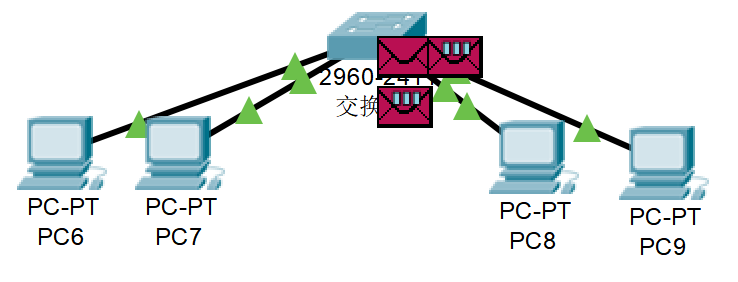
首先数据包被发送到交换机



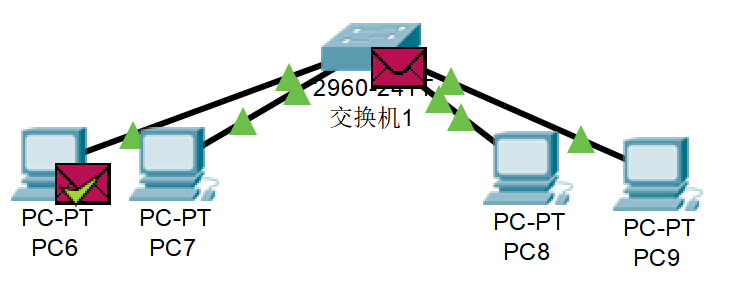
交换机向PC7,PC8,PC9转发数据包

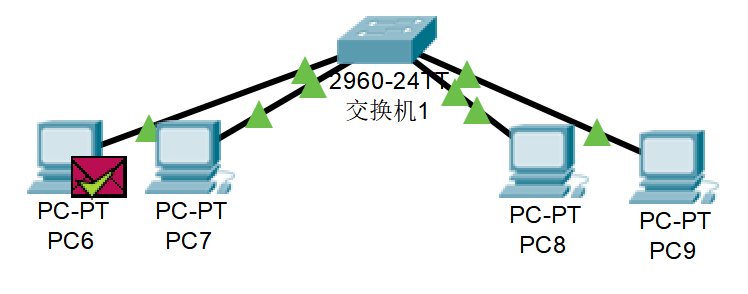


PC7,PC8,PC9收到数据包后对PC6进行应答，向交换机发送数据包。



交换机依次将数据包转发给PC6直到最后一个数据包转发完毕，从而避免了冲突的产生。

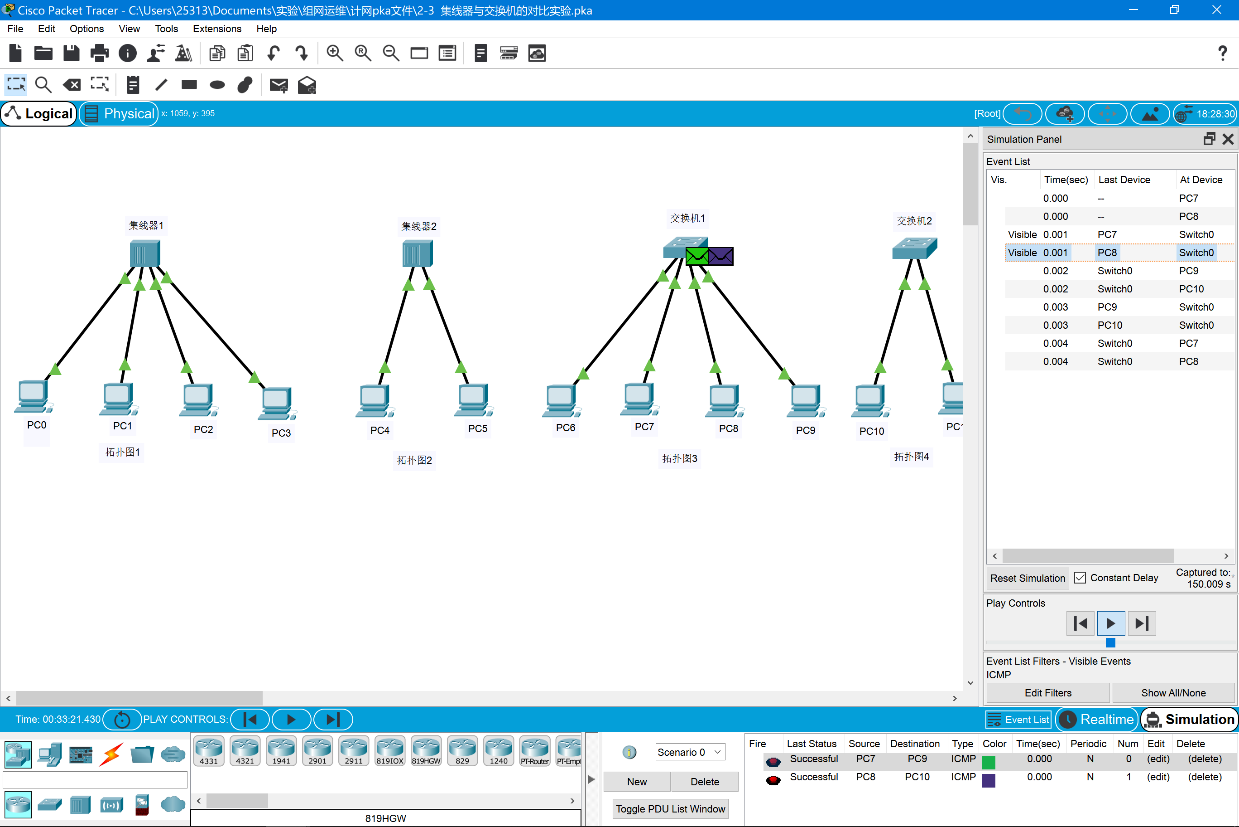
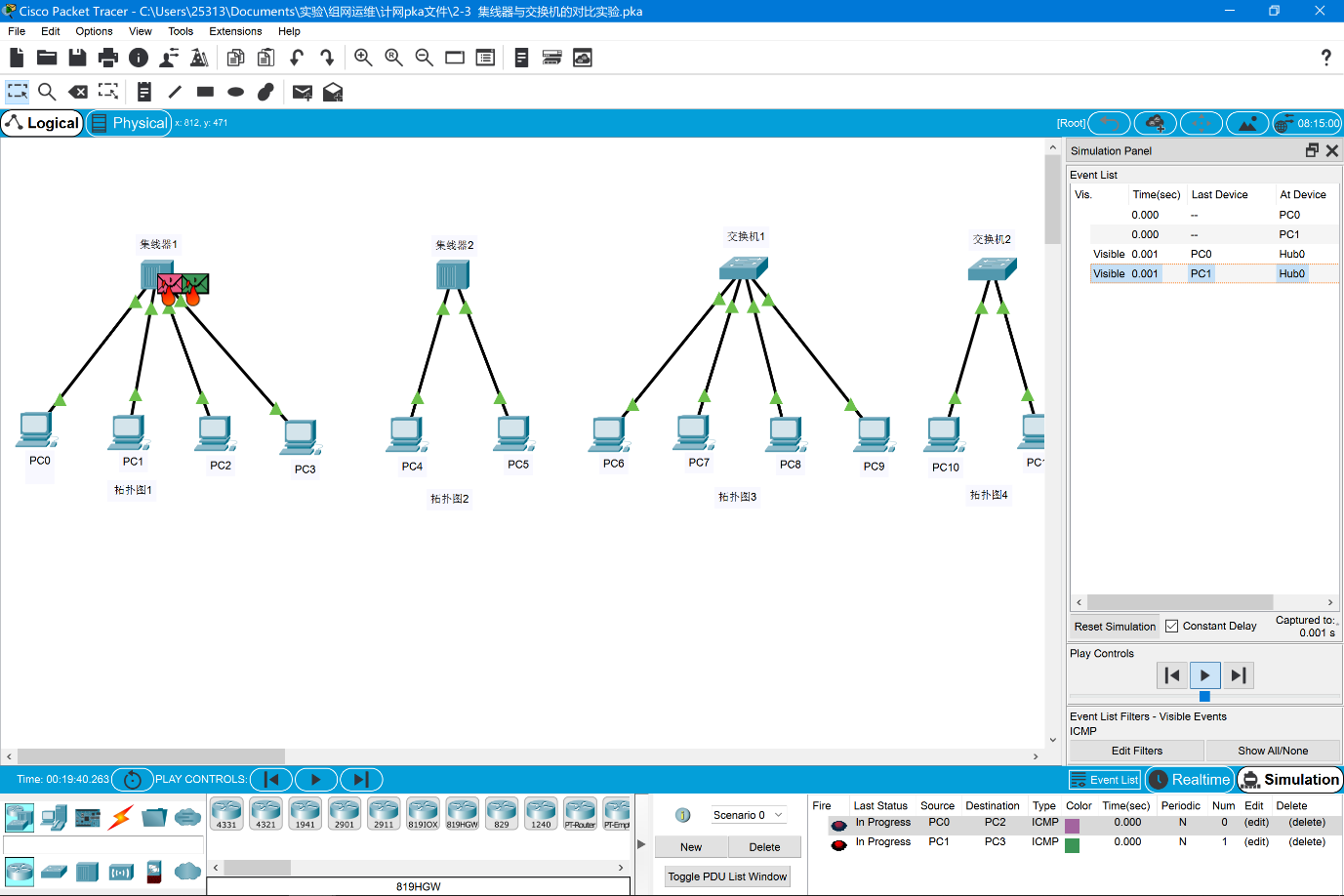




1. 任务二：分别观察以集线器和以交换机为中心的以太网中，多个站点同时发送数据的情况，理解冲突域的概念。

（根据教材或老师给的详细资料，使用自己的语言描述实验步骤，在文字描述的同时，尽量多截图说明）

当多个站点发送数据时，集线器会发生冲突，而交换机不会。

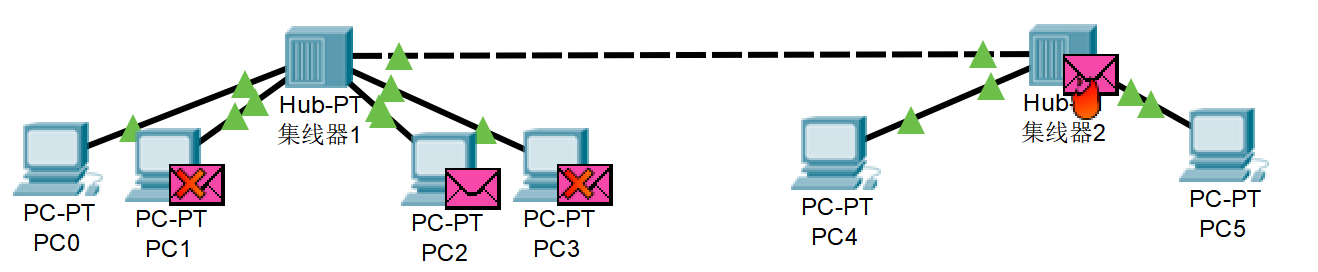
****

1. 任务三：观察集线器和交换机在扩展以太网覆盖范围的同时，对冲突域和广播域范围的影响。

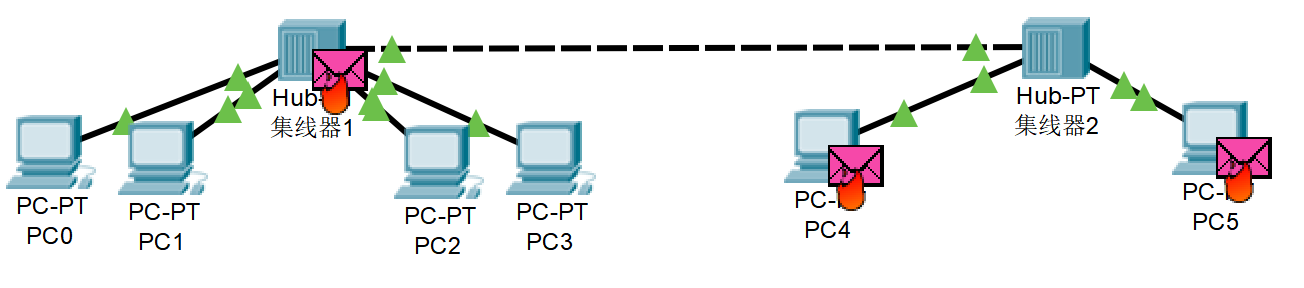
（根据教材或老师给的详细资料，使用自己的语言描述实验步骤，在文字描述的同时，尽量多截图说明）

集线器扩展以太网范围后，在集线器处发生了冲突。在广播时，PC2的应答包会在集线器1发生冲突，应答包也会发生冲突。交换机扩展以太网范围后，交换机会根据转发表进行转发，不会扩大冲突域，因此依旧没有发生冲突。

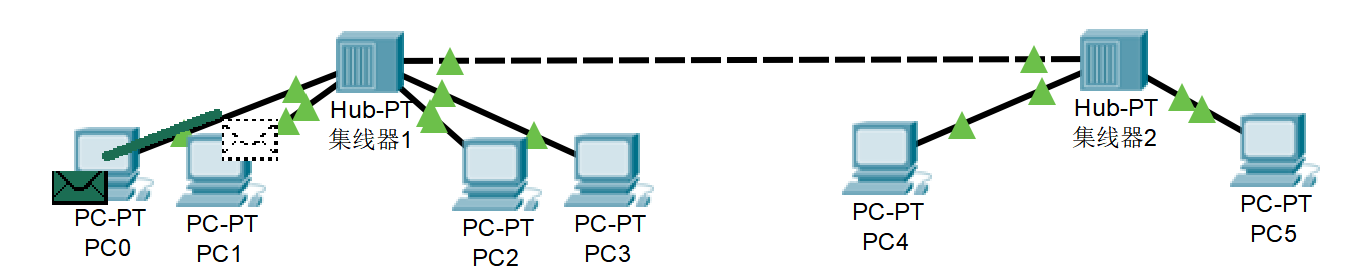
（1）集线器对冲突域的影响：PC0向PC2发送数据包，PC4向PC5发送数据包。PC0先将数据包发送给了集线器1，集线器1收到该数据包后进行广播，PC1和PC3发现不是发送给自己的所以将数据包丢弃，PC2接收到该数据包后准备应答。因为PC4也在向PC5发送，所以集线器2检测到了数据冲突。



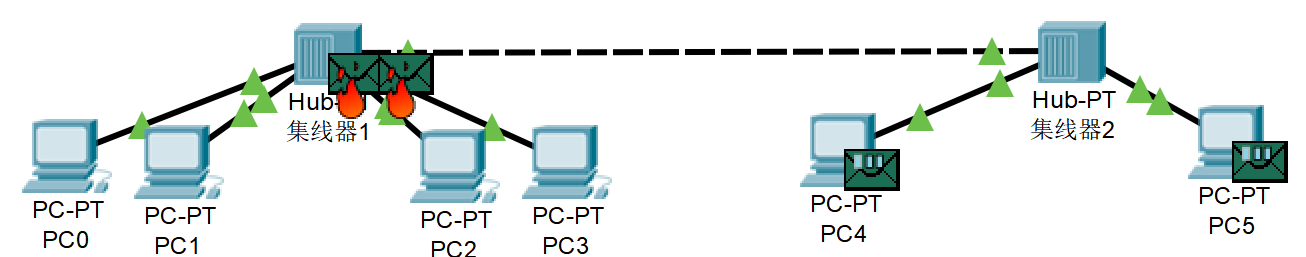
集线器2与PC2分别将发生冲突的消息告知给集线器1和PC4、PC5，集线器1知道发生冲突后，将发生冲突的消息也告知给PC0、PC1、和PC3和集线器2，集线器2收到来自集线器1的冲突消息后有再次向PC4和PC5告知发生了冲突。



（2）集线器对广播域的影响：从PC0发出广播包

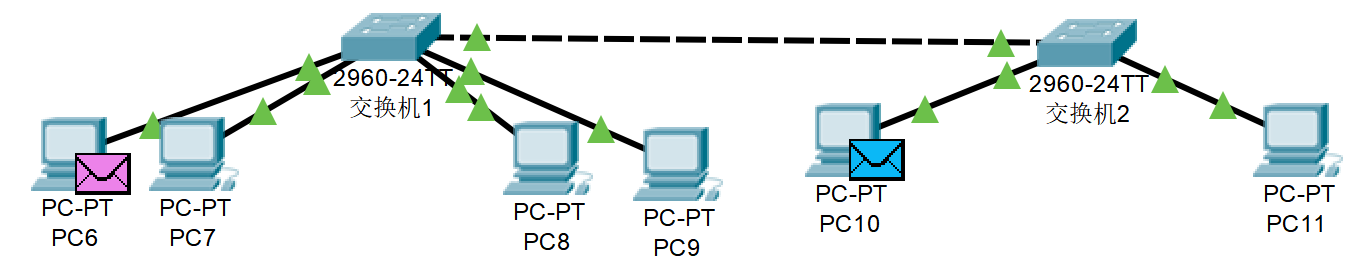


PC1、PC2和PC3收到数据包后进行应答，集线器1检测到了数据冲突，并告知其下的PC和集线器2发生了数据冲突。

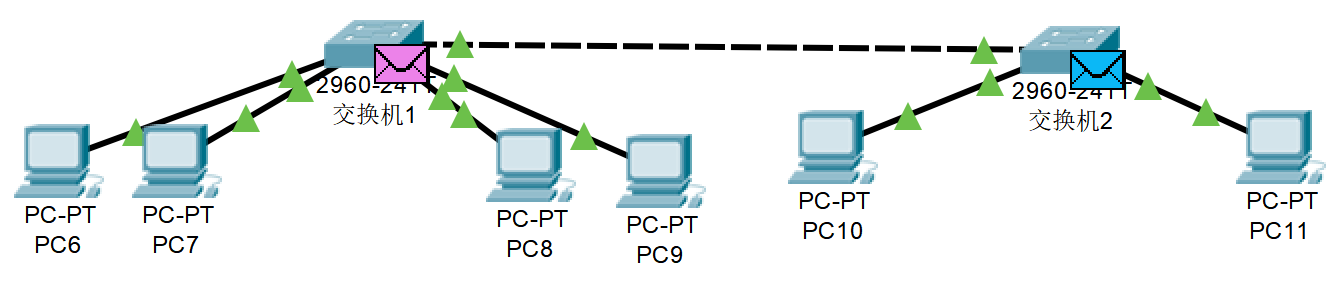


（3）交换机扩展以太网时对冲突域范围的影响

PC6向PC8发送数据包，PC10向PC11发送数据包



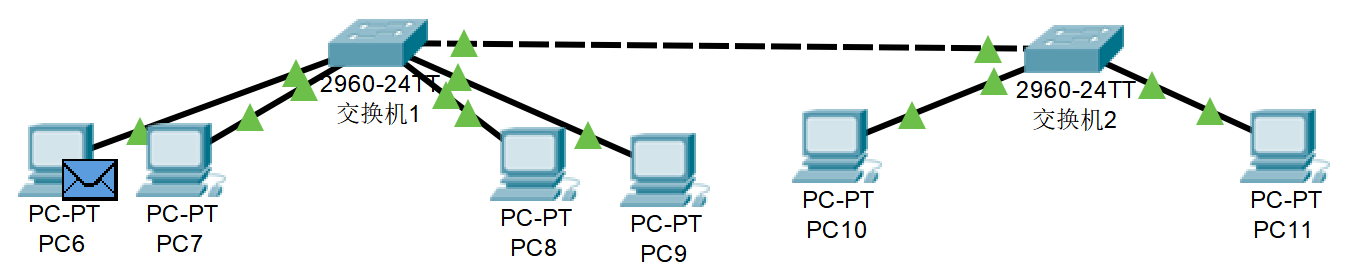
PC6和PC10分别先将数据包发送给了交换机1和交换机2，然后再由交换机1和交换机2将数据包分别转发给PC8和PC11



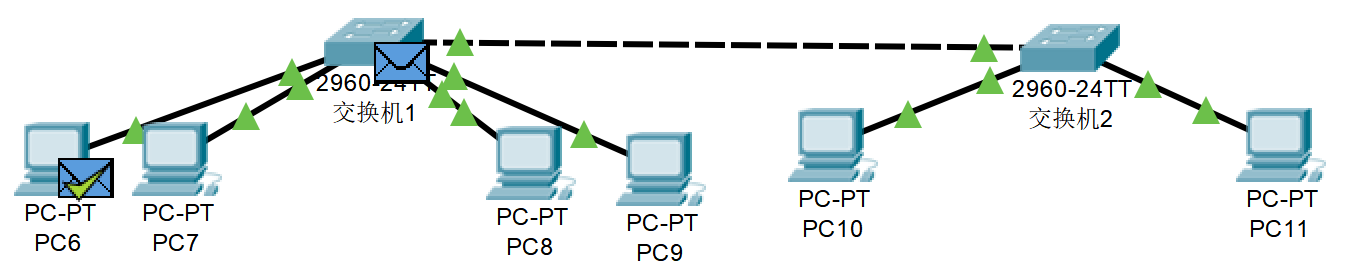


（4）交换机扩展以太网时对广播域范围的影响

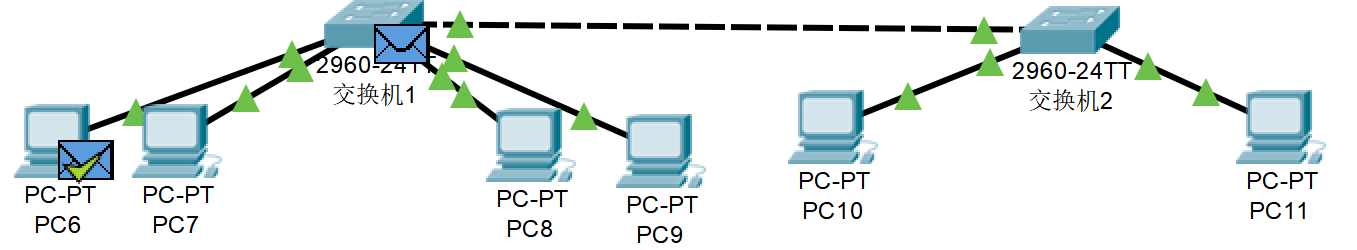
PC6发送广播数据包，发送给交换机1后，交换机1将数据包转发给PC7、PC8、PC9和交换机2，交换机2收到后，又转发给PC10和PC11。



交换机1将收到PC7、PC8和PC9的应答数据包依次转发给PC6，PC6收到后确认了PC7、PC8和PC9收到了它所发出的数据包。



PC10和PC11收到后进行应答，依次将应答数据包发送给交换机2，并由交换机2转发给交换机1， 再由交换机1转发给PC6，PC6收到应答数据包后，确认PC10与PC11收到了它所发出的数据包。



## 三、思考与总结

1. 集线器在接收到发送给某节点的单播包时是如何转发数据的？交换机又是如何处理单播包的？

答：集线器将单播数据包发送给其他所有端口，而交换机先根据数据包学习 物理地址，建立每个端口对应的物理地址表，然后根据单播数据包的目的物理地址直接把数据包发往相应的端口。因此，集线器会把包发给所有PC，而交换机只把数据发向目的PC。

1. 在以集线器/交换机为中心的以太网中，当多个站点同时发送数据时，是否会发生冲突？为什么？

答：以集线器为中心的以太网中多个站点同时发送数据时会发生冲突，而交换机不会发生冲突。因为以集线器为中心的以太网本质上仍然是总线结构，而在以交换机为中心的以太网中，交换机会根据转发表进行转发，不会扩大冲突域。

1. 使用集线器扩大以太网规模时，有没有可能会使以太网的性能下降？为什么？

答：有可能。用集线器扩大以太网规模时，也会扩大冲突域。

1. 使用交换机扩大以太网规模时，有没有可能会使以太网的性能下降？为什么？

答：有可能。使用交换机解决了冲突域的问题，但是交换机并不隔离广播域，使用交换机扩大网络规模的同时也扩大了广播域。这将使以太网中广播包的数量增加，当广播包的数据量达到一定数量时，网络性能下降。

1. 实验过程中还遇到什么问题，如何解决的？通过该实验有何收获？

答：通过这次实验，我了解了集线器和交换机如何转发数据，理解了冲突域和广播域的概念，同时也理解了集线器和交换机在扩大网络规模中的作用和局限性。

# 2.交换机工作原理

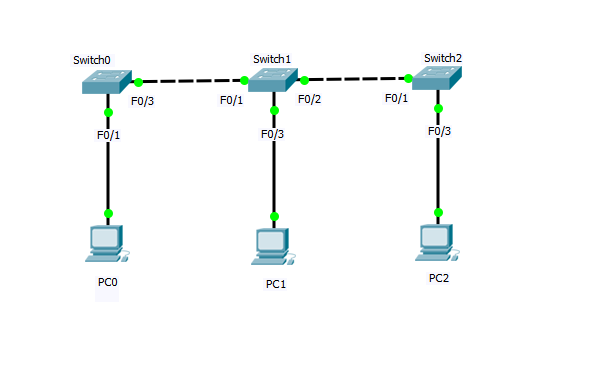
## 一、实验目的

1. 理解交换机通过逆向自学习算法建立地址转发表的过程。
2. 理解交换机转发数据帧的规则。
3. 理解交换机的工作原理。

## 二、实验步骤

1. 给出实验中用到的拓扑图

（不能从老师的资料中截图，从自己的界面里截图）



1. 给出实验中使用的IP配置表

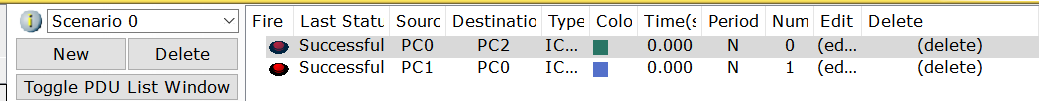
（不能从老师的资料中截图，自己制表）

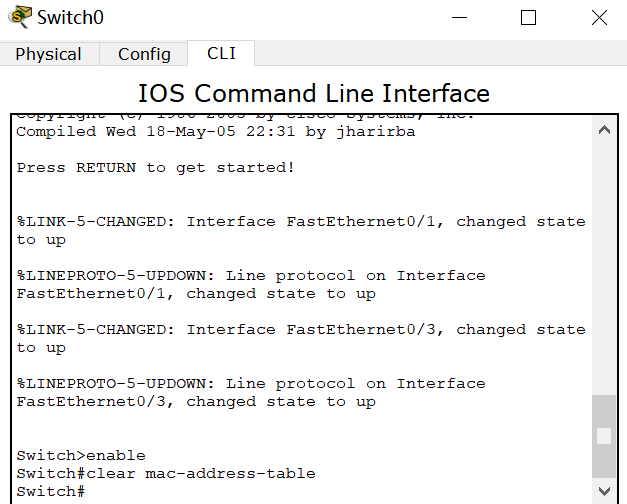
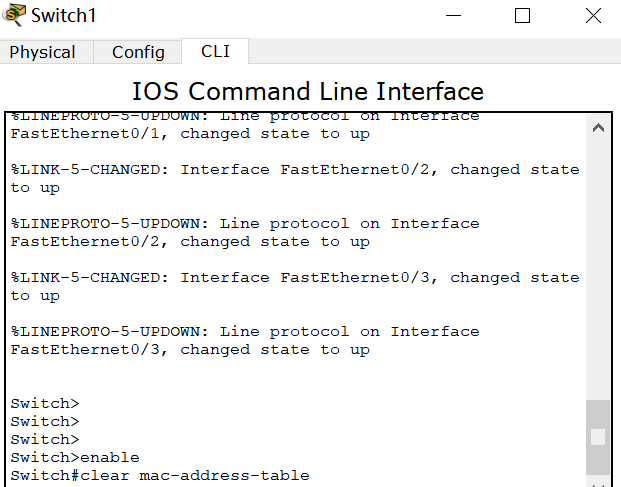
|  |  |  |
| --- | --- | --- |
| 主机名 | IP地址 | 子网掩码 |
| PC0 | 192.168.1.1 | 255.255.255.0 |
| PC1 | 192.168.1.2 | 255.255.255.0 |
| PC2 | 192.168.1.3 | 255.255.255.0 |

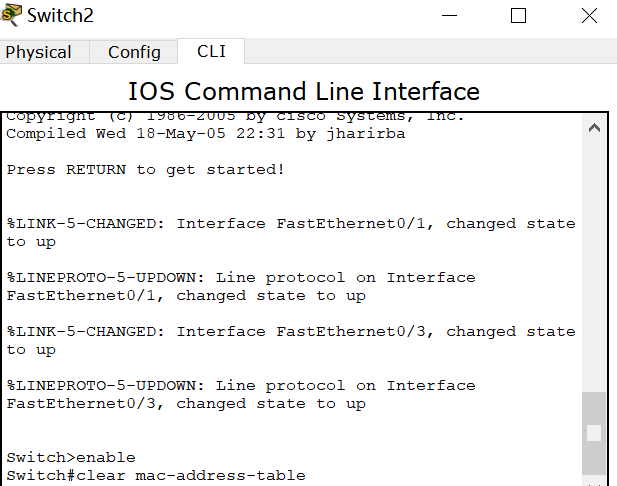
1. 任务一：准备工作。

（按教材完成，配图并使用自己的语言简单描述）

A、来回切换三次实时模式和模拟模式，在实时模式下运行事件列表中预设场景，再删除所有场景。

B、删除交换机地址转化表（CLI选项卡输入命令）

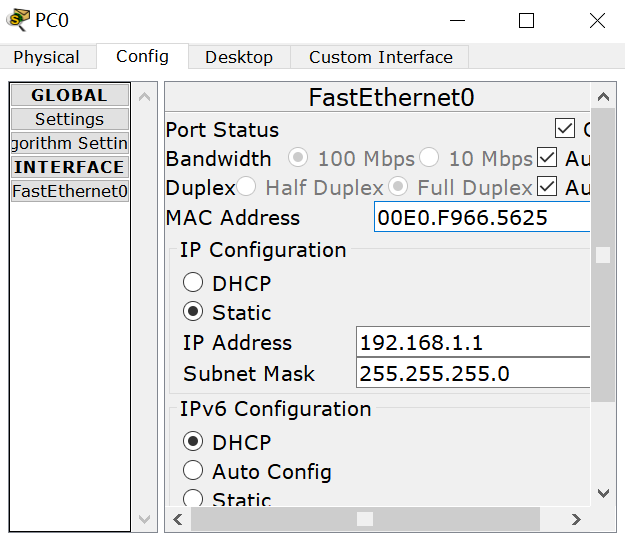
 



1. 任务二：观察交换机的工作原理。

（根据教材的详细资料，使用自己的语言描述实验步骤，在文字描述的同时，尽量多截图说明）

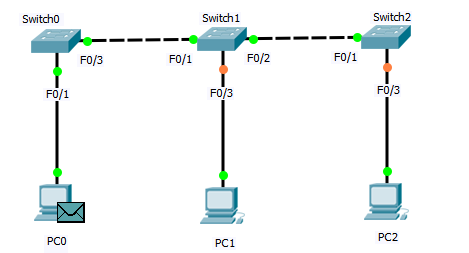
1. 查看并记录PC0和PC2的MAC地址

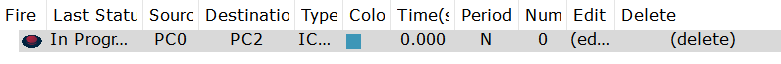


PC0——00E0.F966.5625

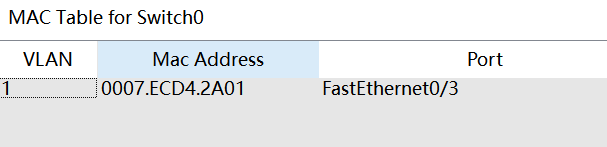
PC2——00D0.BCE9.C0B8

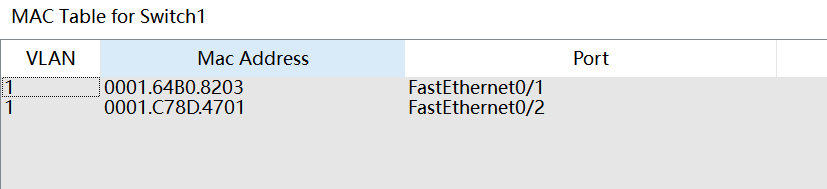
1. 添加从PC0到PC2的数据包

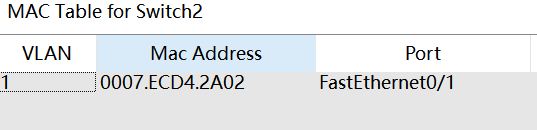




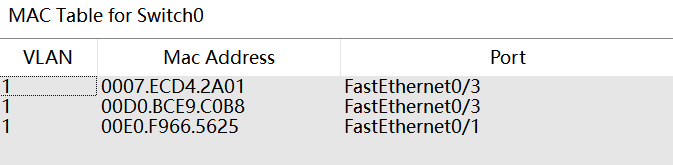
1. 分别查看三台交换机在发送数据前的地址转化表

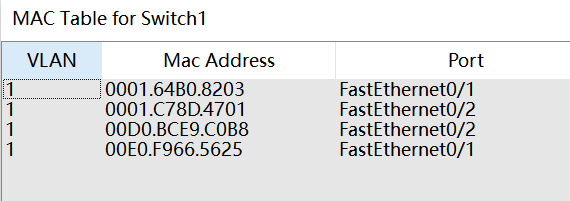






1. 查看switch0的学习和转发过程

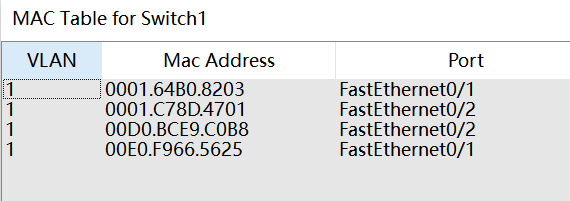


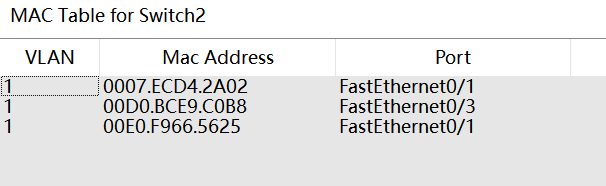


ICMP包到达交换机的时候，交换机根据报文里的源、目的MAC地址，查看自己的MAC地址表，如果有目的MAC记录，就将ICMP报文从相应端口转发出去；如果交换机里没有目的MAC记录，就泛洪从除了接收报文的其它所有端口转发出去，得到目的MAC的端口号并记录进MAC 地址表，并将数据转发

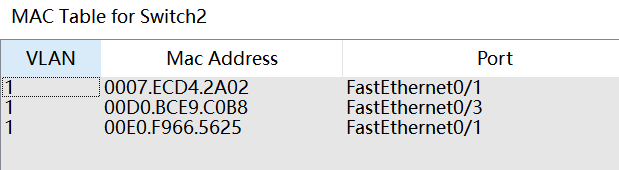
1. 观察switch1和switch2的学习和转发过程

Switch1转switch2





Switch转pc2



## 三、思考与总结

1. 在实验过程中，将观察结果填入下表。转发表栏内填写交换机接收到数据后MAC地址转发表中增加的项，如无增加或该交换机未收到该数据帧，则用横线表示。对数据的处理填写转发、洪泛或丢弃，如交换机未收到该数据帧，则用横线表示。

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 发送的帧 | Switch0的转发表 | | Switch1的转发表 | | Switch2的转发表 | | Switch0的处理 | Switch1的处理 | Switch2的处理 |
| 地址 | 接口 | 地址 | 接口 | 地址 | 接口 |
| PC0→PC2 | 00E0.F966.5625 | F0/1 | 00E0.F966.5625 | F0/1 | 00E0.F966.5625 | F0/1 | 洪泛 | 洪泛 | 洪泛 |
| PC1→PC0 | 00D0.BA0E.6137 | F0/3 | 00D0.BA0E.6137 | F0/3 | —— | — | 转发 | 转发 | 转发 |

1. Switch0收到PC0向PC2发送的数据帧后，其地址转发表是否有变化？如有，给出增加的条目并解释原因。

答:有，增加条目为: 00E0.F966.5625 F0/1。 交换机使用逆向自学习算法建立转发表，所以当通过某个端口接收到某站点发送的数据帧时，将记录站点MAC地址与端口之间的映射关系。

1. Switch1收到PC0向PC2发送的数据帧后，是如何处理的？说明其如此处理的原因。

答:向除接收端口之外的所有其他端口转发，即洪泛转发。因为在PC0向PC2发送数据帧时，Swtich1 的转发表中没有PC2对应的转发表项，为了保证数据的传输，当转发表中没有目标主机对应的转发表项时，采用洪泛转发。

1. 在删除Switch1上的地址转发表前后，PC1向PC0发送数据时Switch2是如何处理的？说明其如此处理的原因。

丢弃数据帧。因为在之前的两个实验步骤中，Swtch2 已经建立了PC1和PC0两台主机的转发表项，且两台主机都与F0/1相连，即此传输过程中的源主机与目标主机与同一端口相连，此时交换机丢弃数据帧。

1. 实验过程中还遇到什么问题，如何解决的？通过该实验有何收获？

答：通过这次实验，我理解了交换机通过逆向自学习算法建立地址转发表的过程，理解了交换机转发数据帧的规则和交换机的工作原理。

# 3.虚拟局域网（VLAN）工作原理

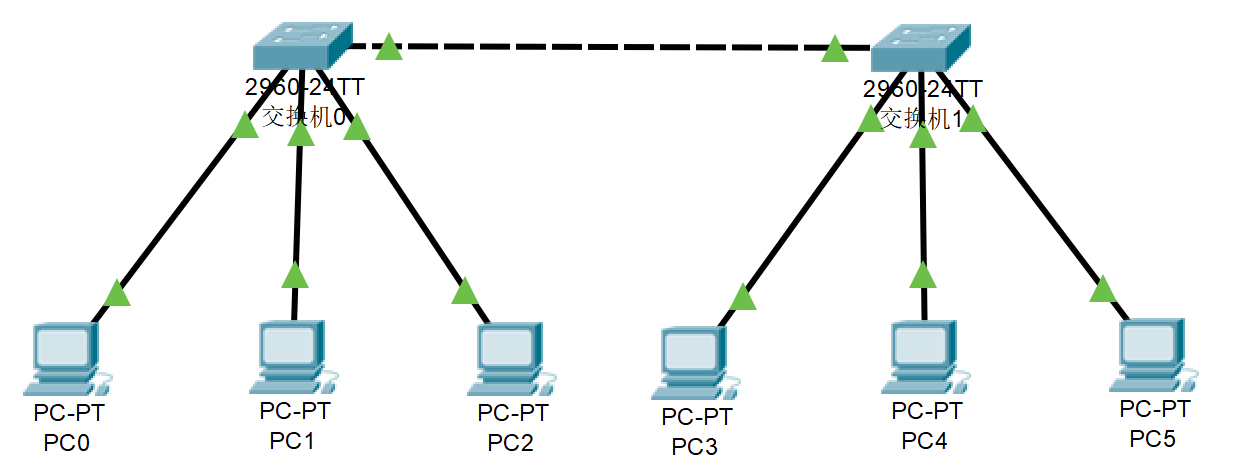
## 一、实验目的

1. 理解虚拟局域网VLAN的概念。
2. 了解VLAN技术在交换式以太网中的使用。
3. 理解VLAN技术在数据链路层隔离广播域的作用。

## 二、实验步骤

1. 给出实验中用到的拓扑图

（不能从老师的资料中截图，从自己的界面里截图）



1. 给出实验中使用的IP配置表

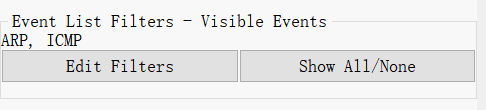
（不能从老师的资料中截图，自己制表）

|  |  |  |  |
| --- | --- | --- | --- |
| 主机名 | IP地址 | 子网掩码 | 所属VLAN |
| PC0 | 192.168.1.1 | 255.255.255.0 | VLAN1 |
| PC1 | 192.168.1.2 | 255.255.255.0 | VLAN1 |
| PC2 | 192.168.1.3 | 255.255.255.0 | VLAN1 |
| PC3 | 192.168.1.4 | 255.255.255.0 | VLAN1 |
| PC4 | 192.168.1.5 | 255.255.255.0 | VLAN1 |
| PC5 | 192.168.1.6 | 255.255.255.0 | VLAN1 |

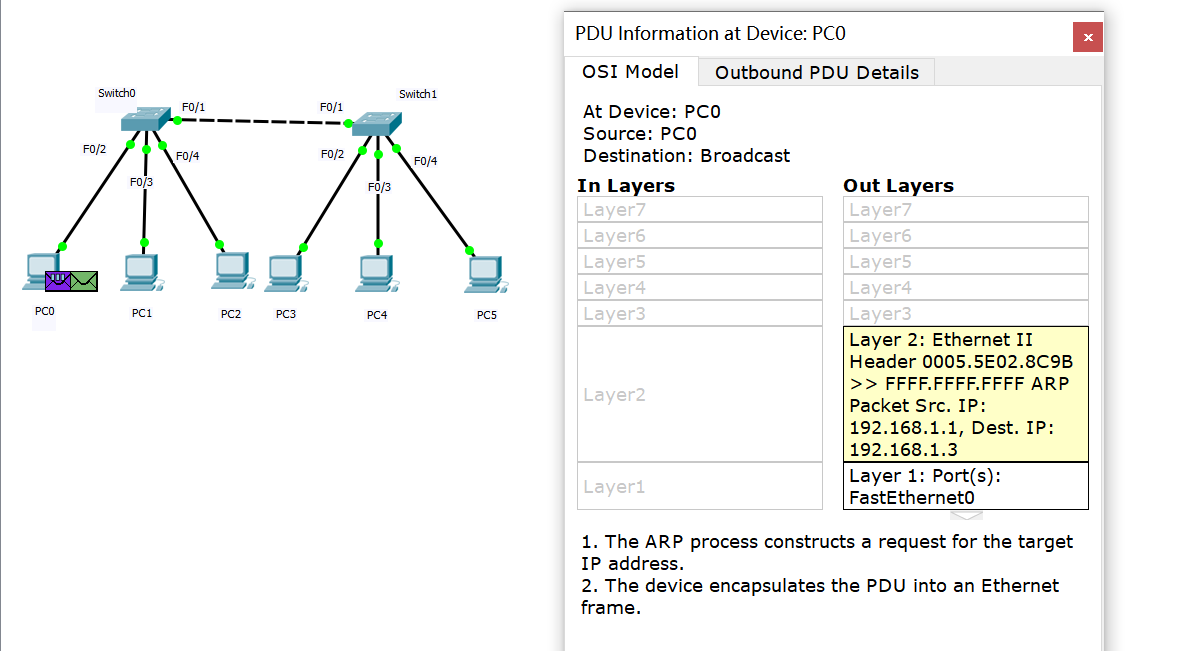
1. 任务一：观察未划分VLAN前，交换机对广播包的处理。

（根据教材的详细资料，使用自己的语言描述实验步骤，在文字描述的同时，尽量多截图说明）

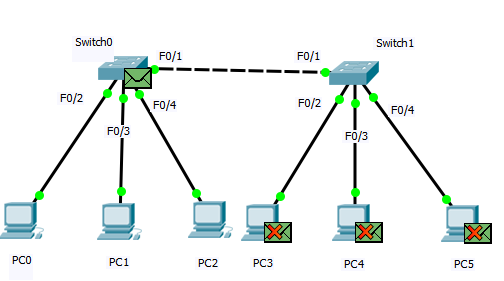
1. 进入模拟模式，设置Event List Filters只显示ARP和ICMP事件



1. 添加pc0到pc2的PDU
2. 查看ARP包的封装信息



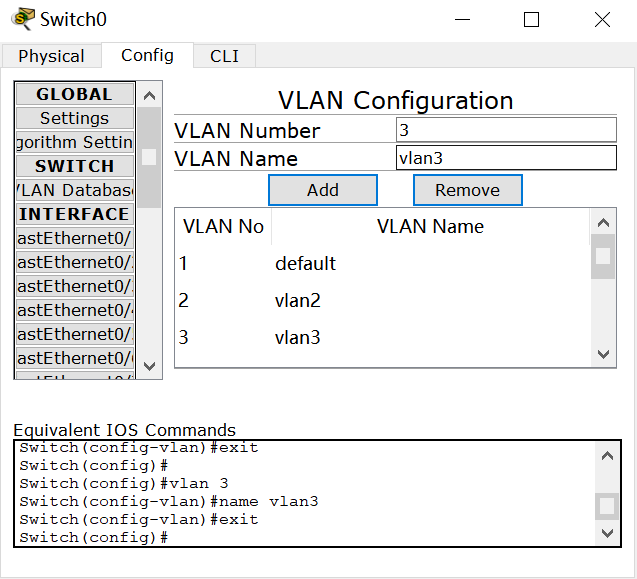
1. 点击自动播放按钮，观察数据传输过程

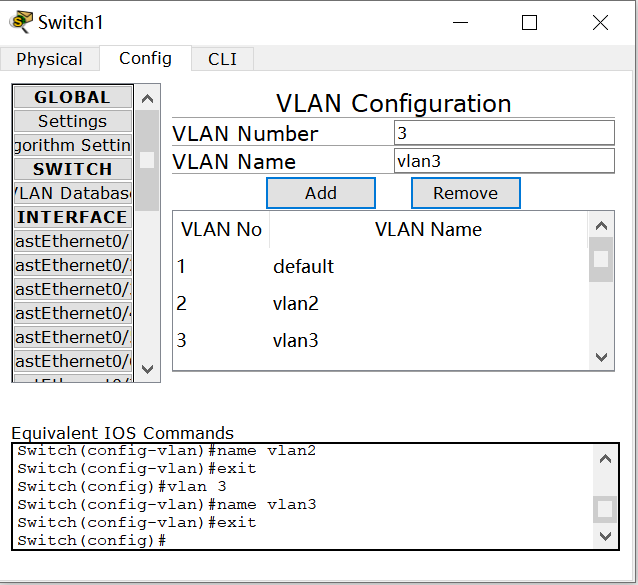


1. 删除所有场景
2. 任务二：创建两个VLAN，并将端口划分到不同VLAN内。

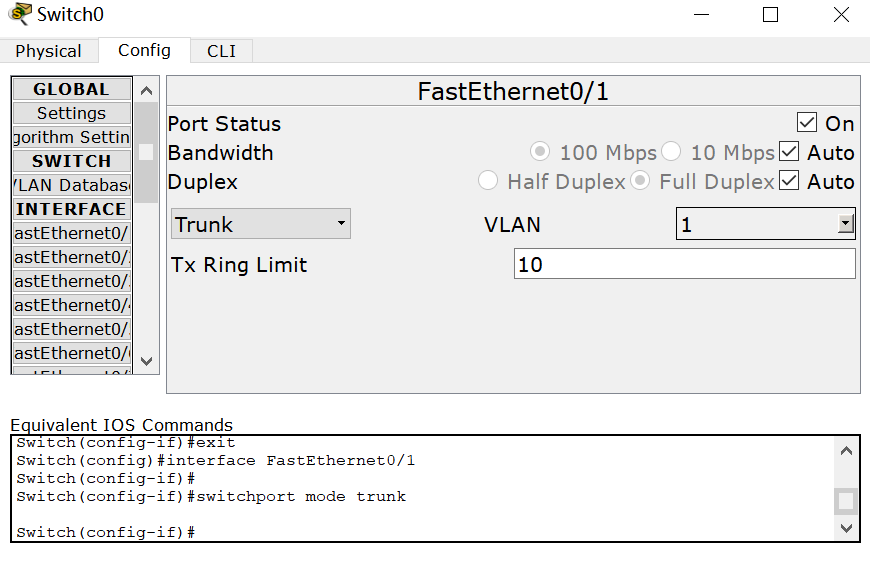
（根据教材的详细资料，使用自己的语言描述实验步骤，在文字描述的同时，尽量多截图说明）

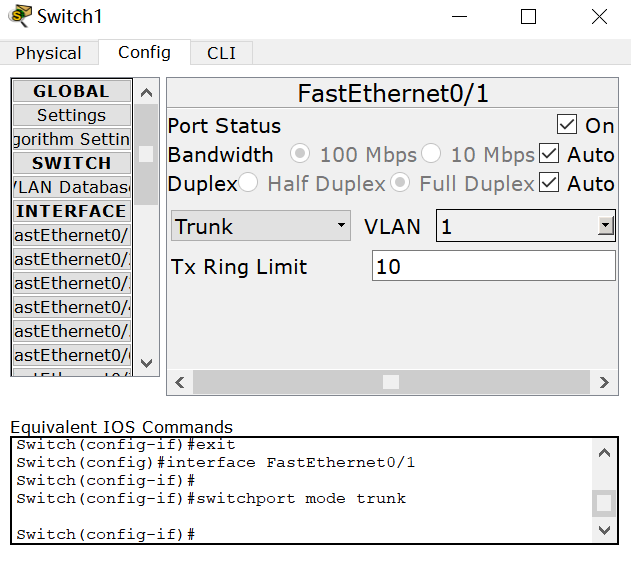
1. 创建VLAN



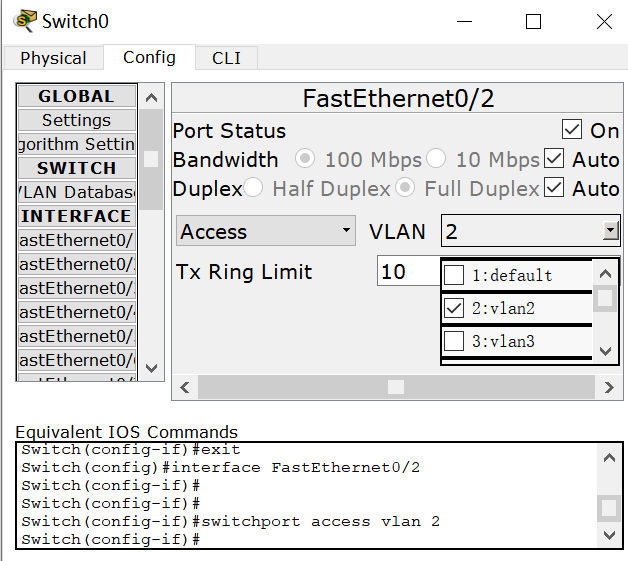


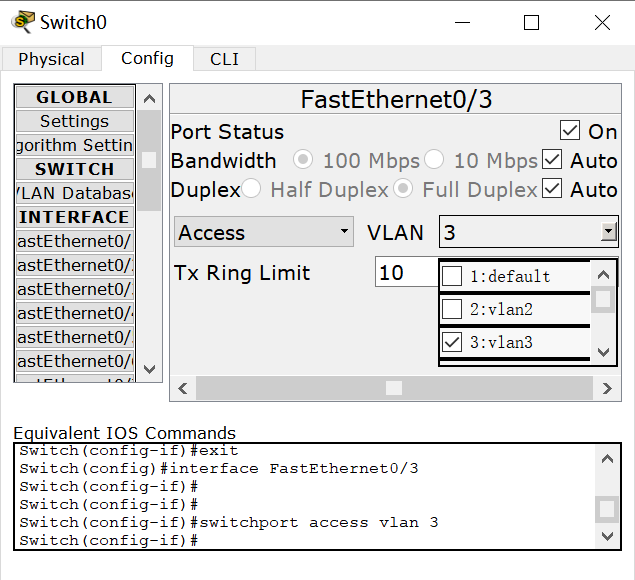
1. 设置switch0和switch1之间的中继连接

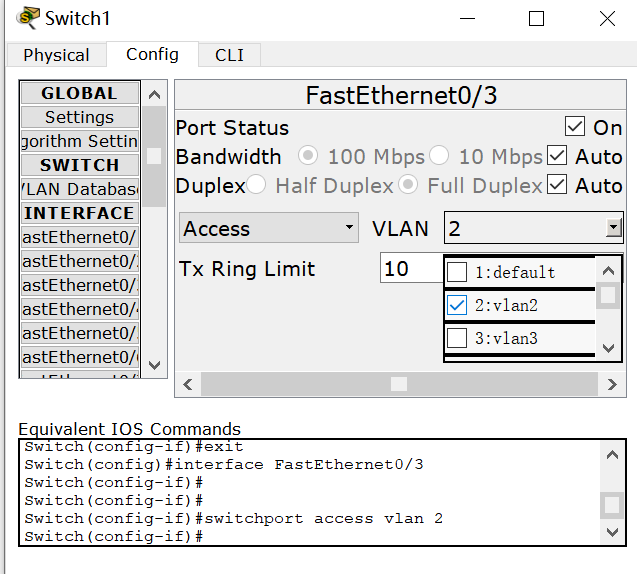


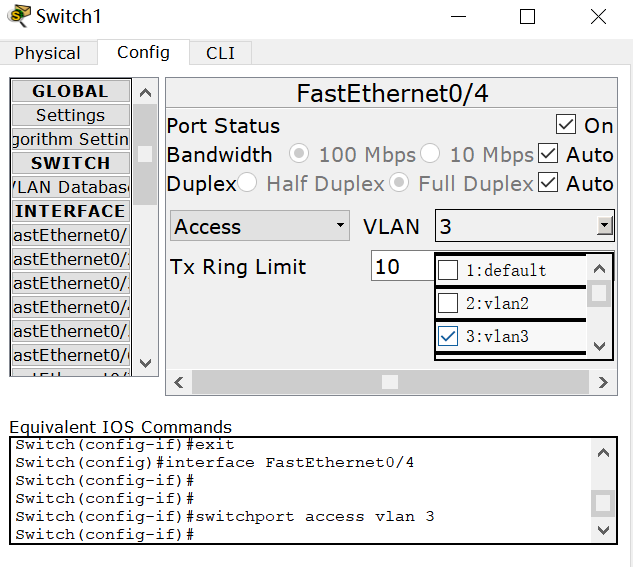


1. 将端口划分在不同的VLAN下



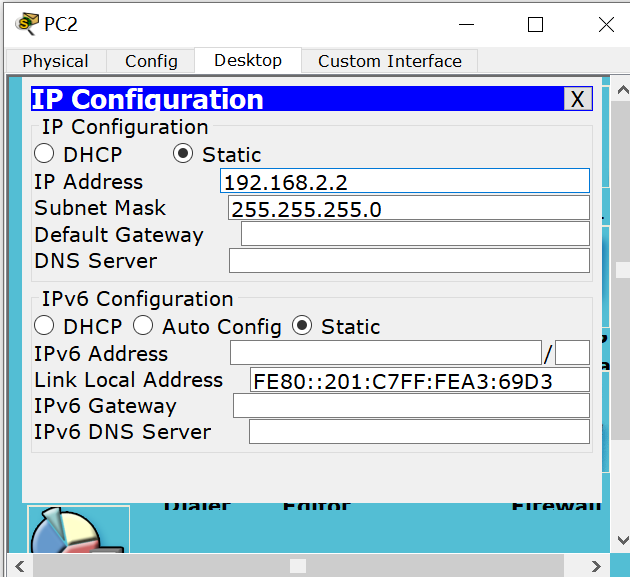


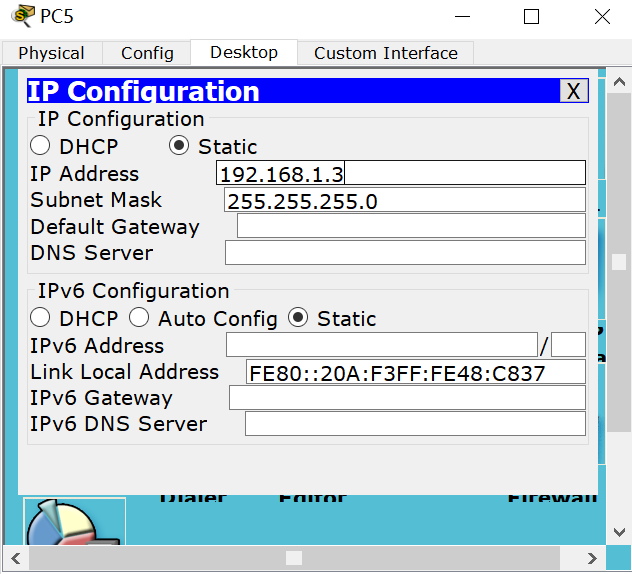




1. 修改pc的IP地址





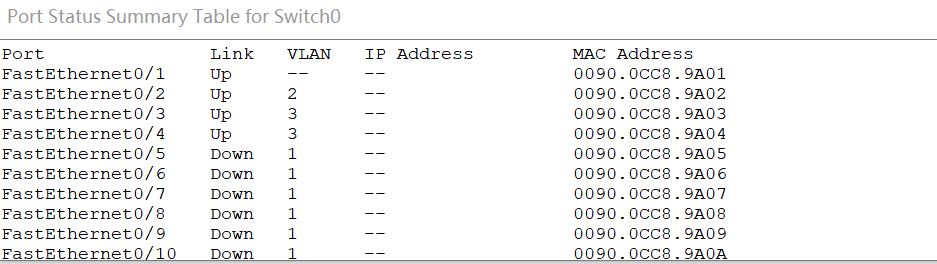


修改完毕后来回切换实时模式和模拟模式直至交换机灯呈绿色

1. 任务三：观察划分VLAN后，交换机对广播包的处理。

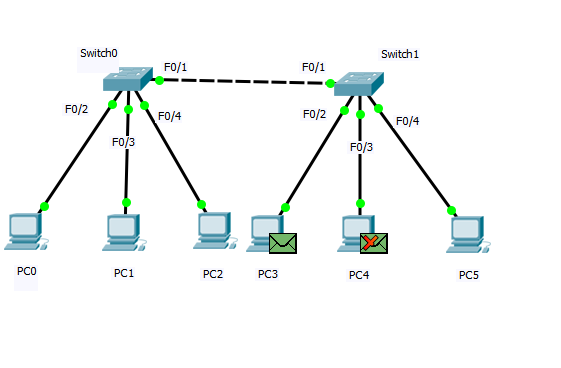
（根据教材的详细资料，使用自己的语言描述实验步骤，在文字描述的同时，尽量多截图说明）

A、查看交换机上的VLAN信息



1. 观察交换机对广播包的处理





## 三、思考与总结

1. 在任务一中，两台交换机分别如何处理广播包？其广播包的传播范围有多大？

答:交换机向所有端口转发广播包，广播包的传播范围是交换机连接的所有站点。

1. 在任务三中，当一台PC发送广播包时，与之连接在同一台交换机上的其它PC是否一定能接收到该广播包？根据实验结果举例说明。

答:不一定。只有与发送广播包的PC划分到同一VLAN内的PC才能接收到该广播包。

1. 通过分析任务一和任务三的实验结果，说明划分VLAN的作用。

答:划分VLAN可以在数据链路层隔离广播域。

1. 实验过程中还遇到什么问题，如何解决的？通过该实验有何收获？

答：通过这次实验，我更加深入地理解了虚拟局域网VLAN的概念，了解了VLAN技术在交换式以太网中的使用，同时也理解了VLAN技术在数据链路层隔离广播域的作用。

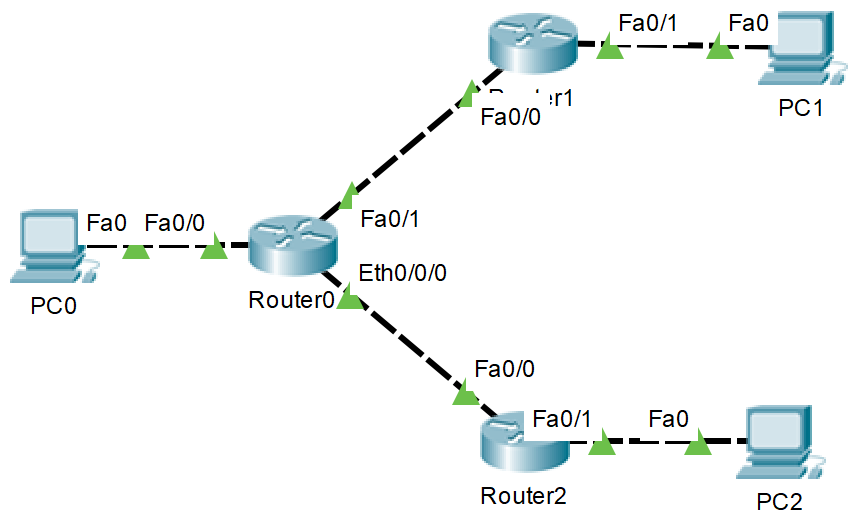
# 4.IP分析

## 一、实验目的

1. 熟悉IP的报文格式及关键字段的含义。
2. 掌握IP地址的分配方法。
3. 理解路由器转发IP数据报的流程。

## 二、实验步骤

1. 给出实验中用到的拓扑图



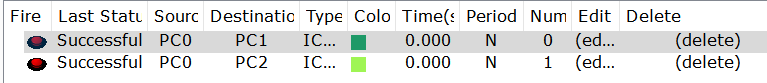
1. 给出实验中使用的IP配置表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 设备 | 接口 | IP地址 | 掩码 | 默认网关 |
| PC0 | 以太接口 | 10.1.1 | 255.255.255.0 | 10.1.254 |
| PC1 | 以太接口 | 10.2.1 | 255.255.255.0 | 10.2.254 |
| PC2 | 以太接口 | 10.3.1 | 255.255.255.0 | 10.3.254 |
| Router0 | Fa0/0 | 10.1.1.254 | 255.255.255.0 |  |
| Router0 | Fa0/1 | 192.168.1.1 | 255.255.255.0 |  |
| Router0 | Eth0/0 | 192.168.2.1 | 255.255.255.0 |  |
| Router1 | Fa0/0 | 192.168.1.2 | 255.255.255.0 |  |
| Router1 | Fa0/1 | 10.1.2.254 | 255.255.255.0 |  |
| Router2 | Fa0/0 | 192.168.2.2 | 255.255.255.0 |  |
| Router2 | Fa0/1 | 10.1.3.254 | 255.255.255.0 |  |

1. 任务一：观察路由表。

（根据教材的详细资料，使用自己的语言描述实验步骤，在文字描述的同时，尽量多截图说明）

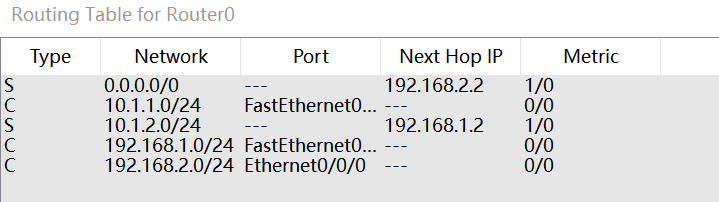
A、初始化ARP表信息

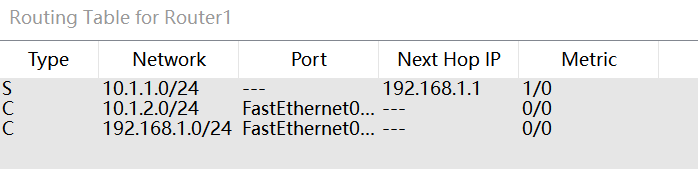


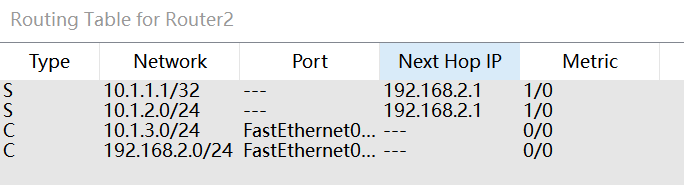
1. 观察IP数据报的转发



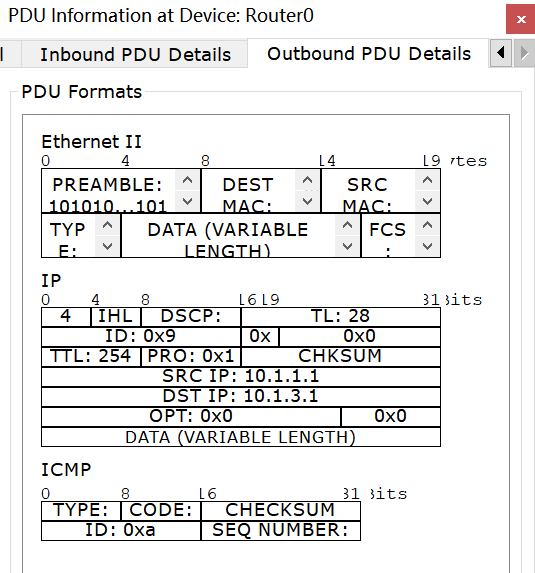
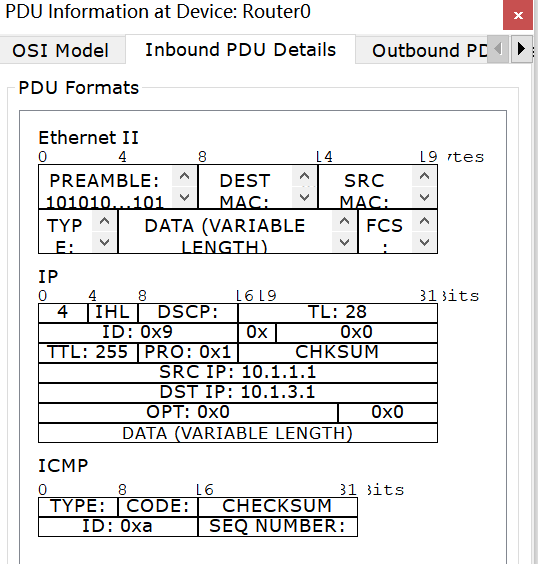
1. 任务二：观察数据包的封装及字段变化。
2. 初始化路由器的路由表并查看

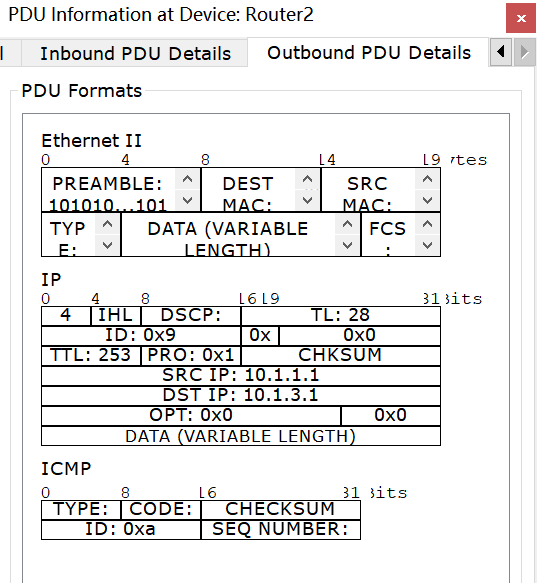
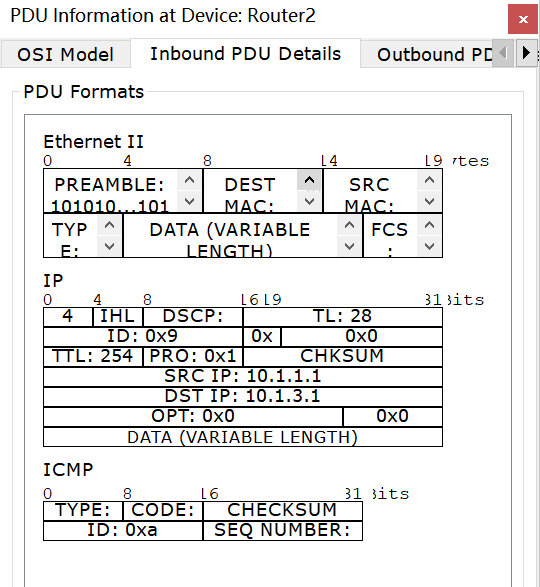




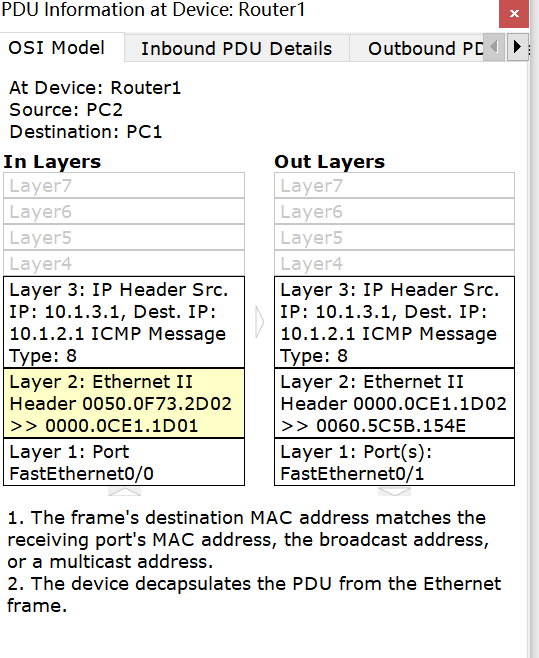


1. 观察PC0-PC2的往返过





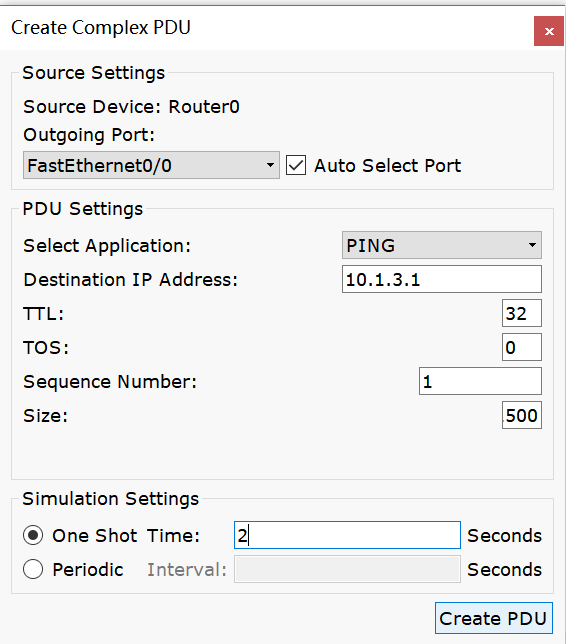
1. 观察PC2-PC1的往返过程



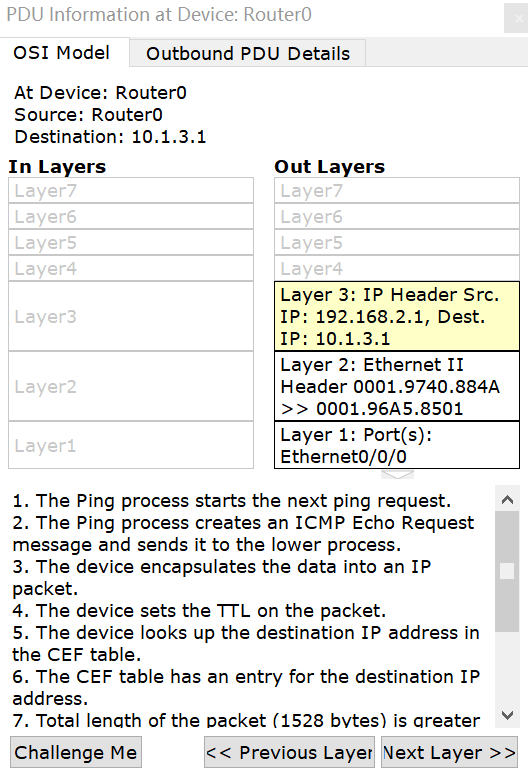
1. 任务三：观察路由器转发IP数据报的方式。

（根据教材的详细资料，使用自己的语言描述实验步骤，在文字描述的同时，尽量多截图说明）

1. 产生需要分片的数据报



1. 任务四：观察IP分片过程。



## 三、思考与总结

1. 一个IP分组经路由器转发后，有哪些字段会发生变化？

答:TTL字段需要减一，而IP头部的校验和需要重新计算，因此这两个字段会发生变化。

1. 任务二的步骤2中，为什么数据单元的源MAC地址和目的MAC地址在转发时会发生变化？。

答：因为Router0有一个朝向Router2的默认路由

1. 路由器如何处理无法继续转发数据包？

答：TTL字段为0时，路由次数达到上线，此时路由器直接将数据包丢弃，不再进行转发。

1. 任务四为什么将Size值改为1500就可以产生分片？

答：原数据长度超过以太网帧的最大传输能力。

1. 为什么任务四的两个分片的长度分别为1500和48？

答:原数据长度为1500+8 (ICMP报文头长度) =1508字节，超过以太网帧的最大传输能力，因此需要分成两片。长度分别为1480 字节和28字节，封装成IP后，每片的长度分别为1480+20=1500字节, 28+20=48字节。

# 5.直连路由与静态路由

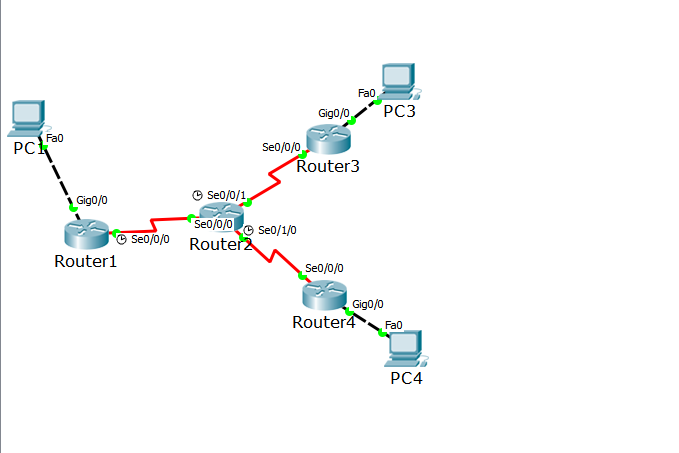
## 一、实验目的

1. 理解直连路由。
2. 理解静态路由，并掌握静态路由配置。

## 二、实验步骤

1. 给出实验中用到的拓扑图

（不能从老师的资料中截图，从自己的界面里截图）

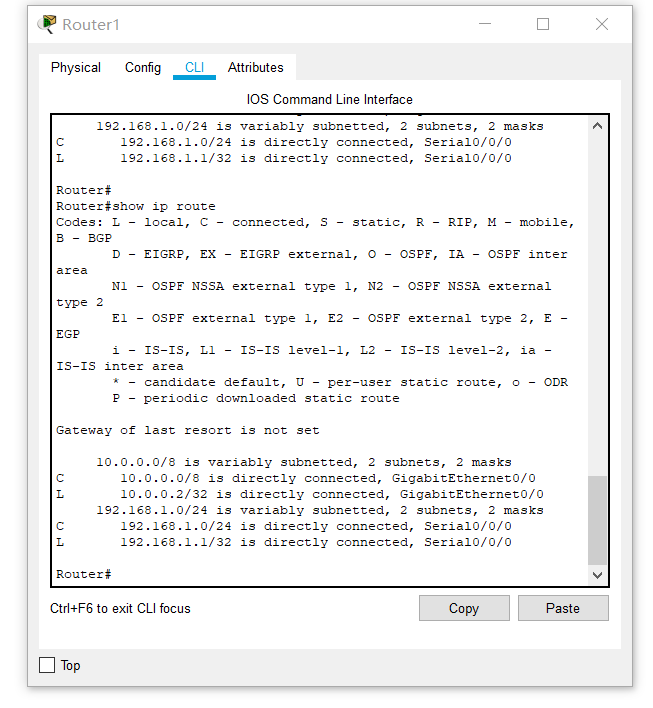


1. 给出实验中使用的IP配置表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 设备 | 接口 | IP地址 | 掩码 | 默认网关 |
| PC1 | Fa0 | 10.0.0.1 | 255.0.0.0 | 10.0.0.2 |
| PC2 | Fa0 | 13.0.0.1 | 255.0.0.0 | 13.0.0.2 |
| PC3 | Fa0 | 14.0.0.1 | 255.0.0.0 | 14.0.0.2 |
| Router1 | Gig0/0 | 10.0.0.2 | 255.0.0.0 | —— |
| Router1 | Se0/0/0 | 192.168.1.1 | 255.255.255.0 | —— |
| Router2 | Se0/0/0 | 192.168.1.2 | 255.255.255.0 | —— |
| Router2 | Se0/0/1 | 192.168.2.1 | 255.255.255.0 | —— |
| Router2 | Se0/10 | 192.168.3.1 | 255.255.255.0 | —— |
| Router3 | Gig0/0 | 13.0.0.2 | 255.0.0.0 | —— |
| Router3 | Se0/10 | 192.168.2.2 | 255.255.255.0 | —— |
| Router4 | Gig0/0 | 14.0.0.2 | 255.0.0.0 | —— |
| Router4 | Se0/10 | 192.168.3.2 | 255.255.255.0 | —— |

1. 任务一：观察直连路由。

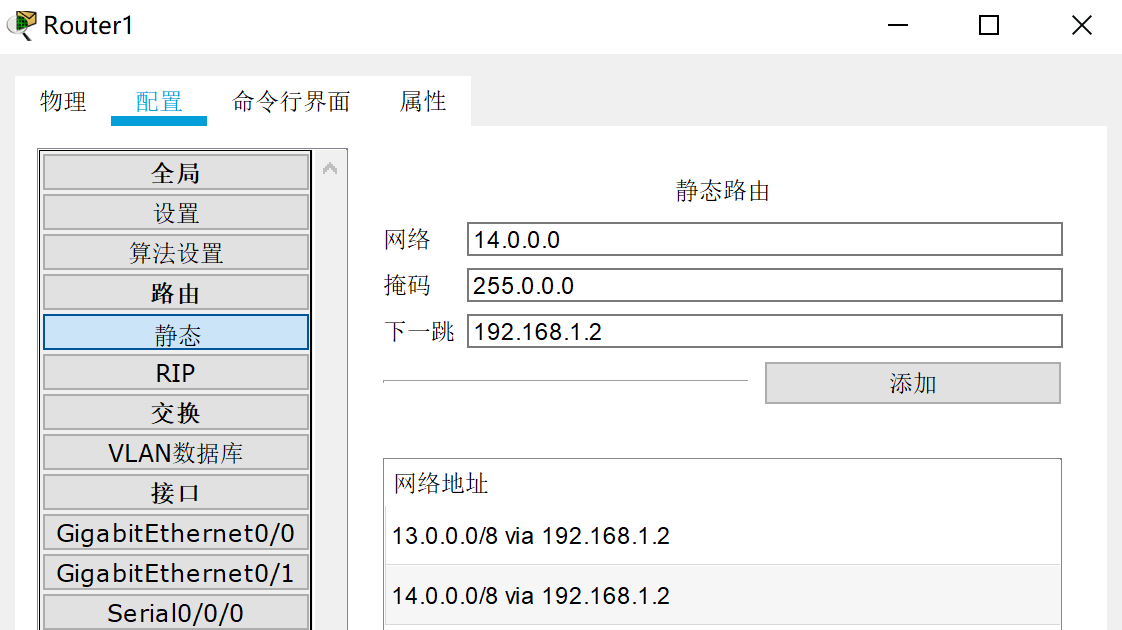
（根据教材的详细资料，使用自己的语言描述实验步骤，在文字描述的同时，尽量多截图说明）



1. 任务二：静态配置路由。

（根据教材的详细资料，使用自己的语言描述实验步骤，在文字描述的同时，尽量多截图说明）

步骤1：为路由器配置正确的静态路由



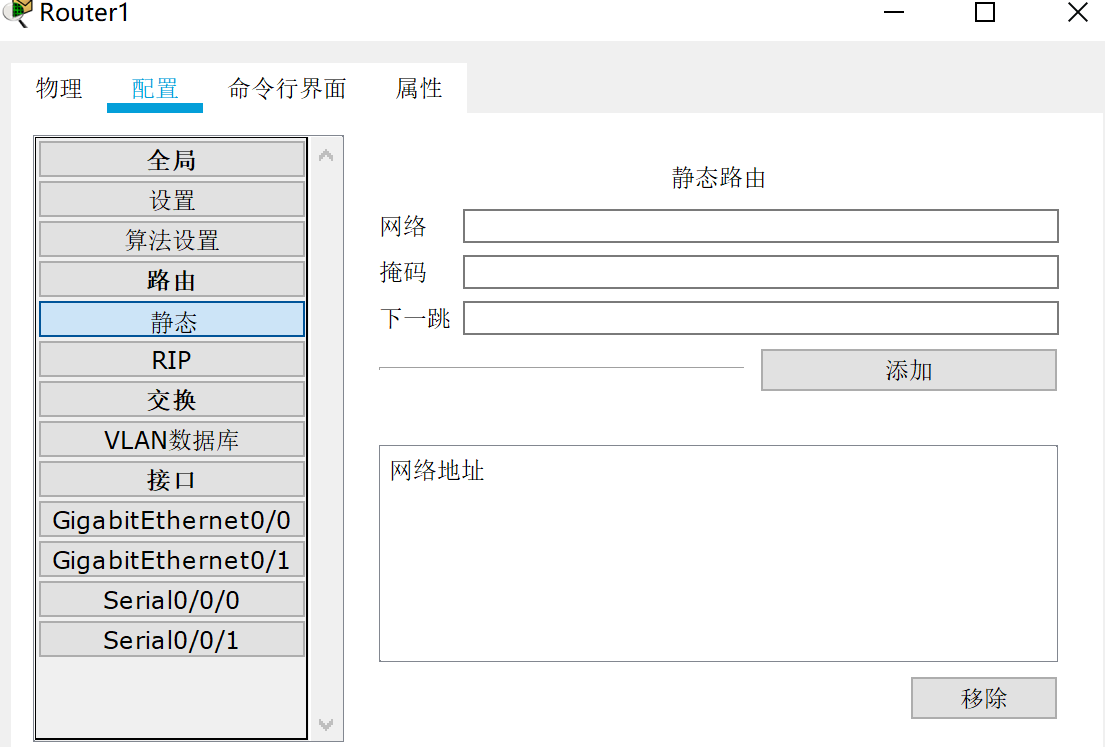
步骤2：为每个路由器配置路由表

|  |  |  |  |
| --- | --- | --- | --- |
| 路由器 | Network | Mask | Next Hoop |
| Router1 | 13.0.0.0 | 255.0.0.0 | 192．168.1.2 |
| 14.0.0.0 | 255.0.0.0 | 192．168.1.2 |
| Router2 | 10.0.0.0 | 255.0.0.0 | 192．168.1.1 |
| 13.0.0.0 | 255.0.0.0 | 192．168.2.2 |
| 14.0.0.0 | 255.0.0.0 | 192．168.3.2 |
| Router3 | 10.0.0.0 | 255.0.0.0 | 192．168.2.1 |
| 14.0.0.0 | 255.0.0.0 | 192．168.2.1 |
| Router4 | 10.0.0.0 | 255.0.0.0 | 192．168.3.1 |
| 13.0.0.0 | 255.0.0.0 | 192．168.3.1 |

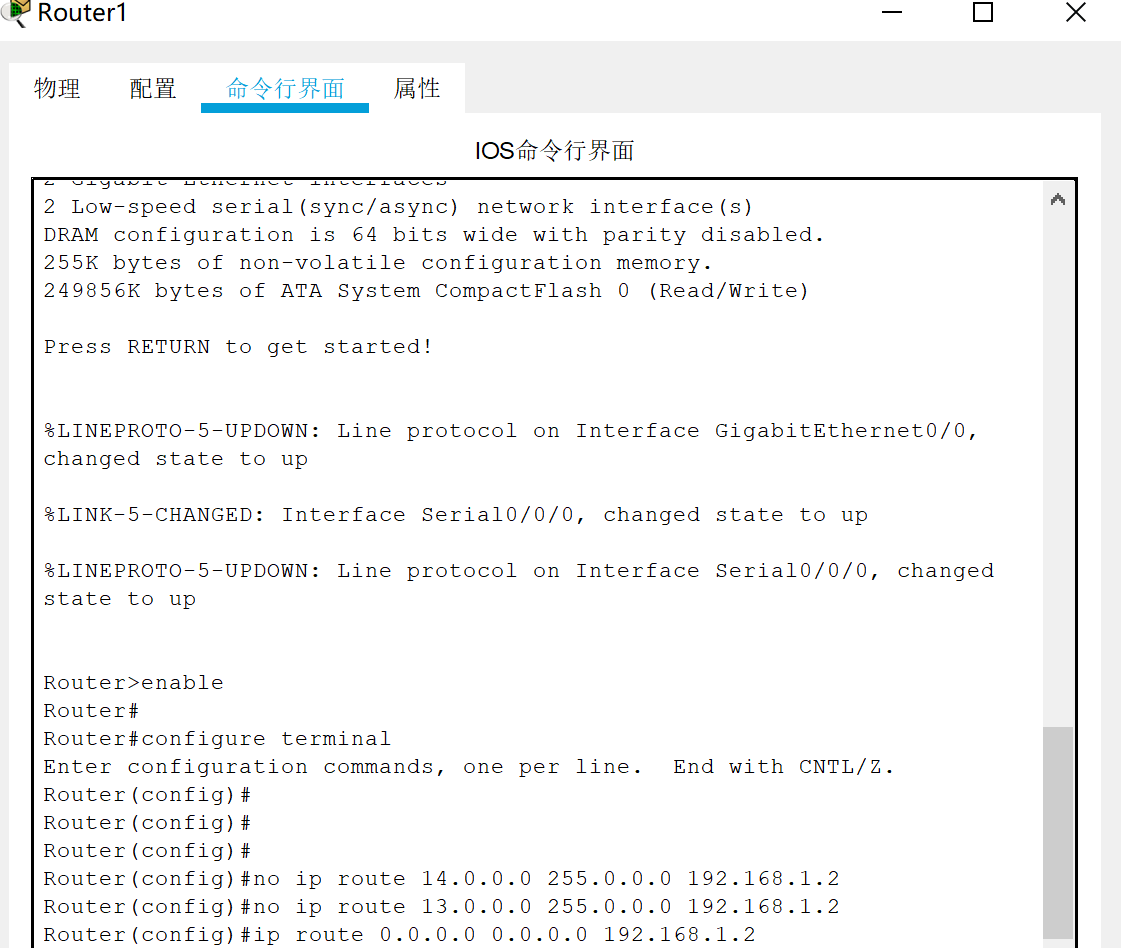
步骤3：检查路由配置是否正确

1. 任务三：配置默认路由。

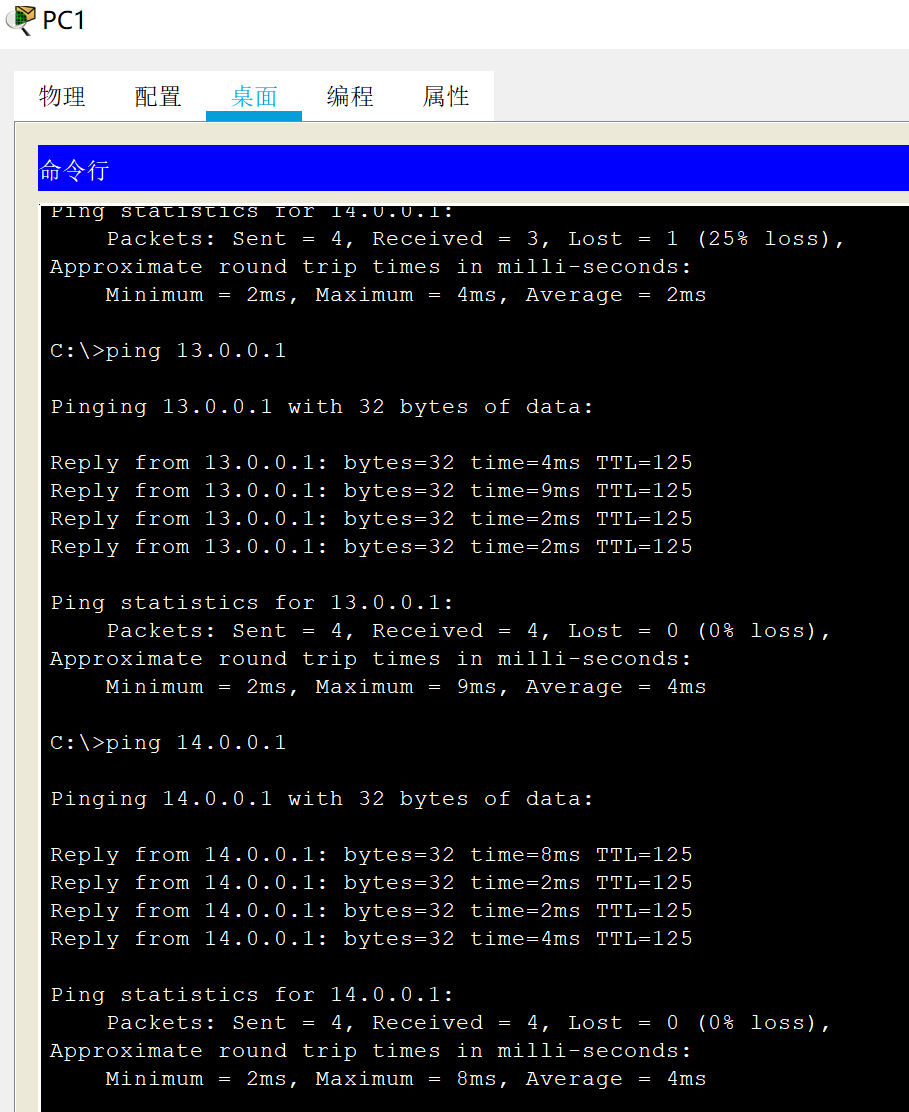
（根据教材的详细资料，使用自己的语言描述实验步骤，在文字描述的同时，尽量多截图说明）



在命令行界面使用ip route 0.0.0.0 0.0.0.0 192.168.1.2配置默认路由，使用show ip route查看router1的路由表，可以看到默认路由已经配置成功。



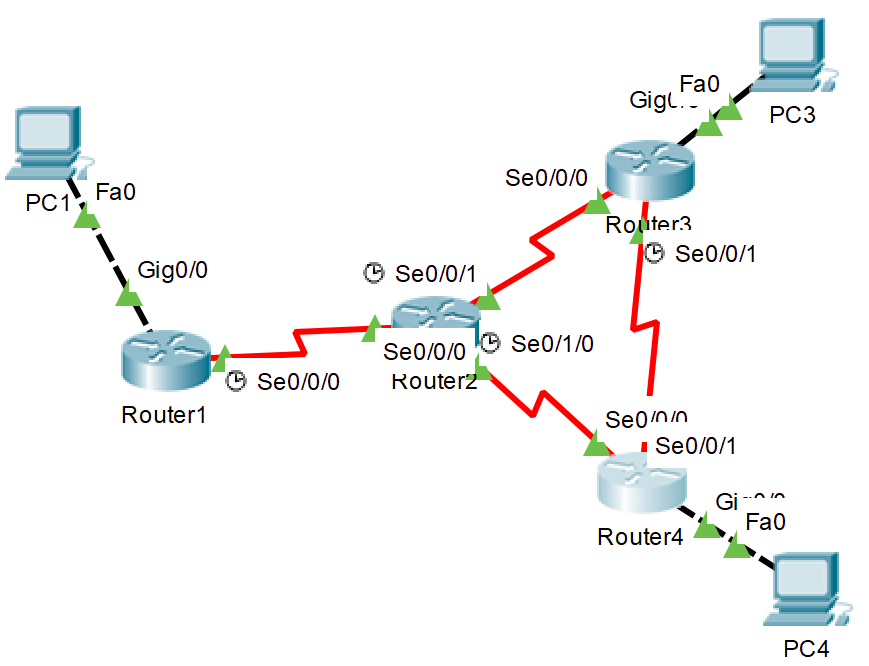
在PC1上使用ping命令去测试到PC2(13.0.0.1)和PC3(14.0.0.1)的连通性，可以ping通，连通性没有异常，使用默认路由可以取代两个静态路由。



1. 任务四：观察路由环路问题

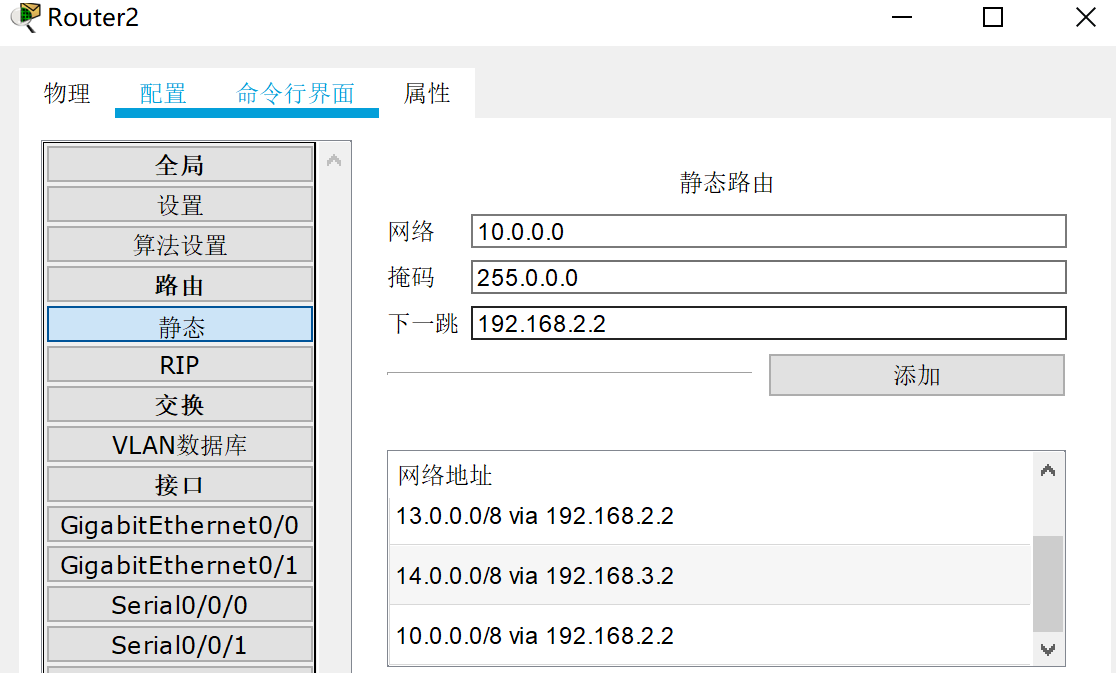
（根据教材的详细资料，使用自己的语言描述实验步骤，在文字描述的同时，尽量多截图说明）

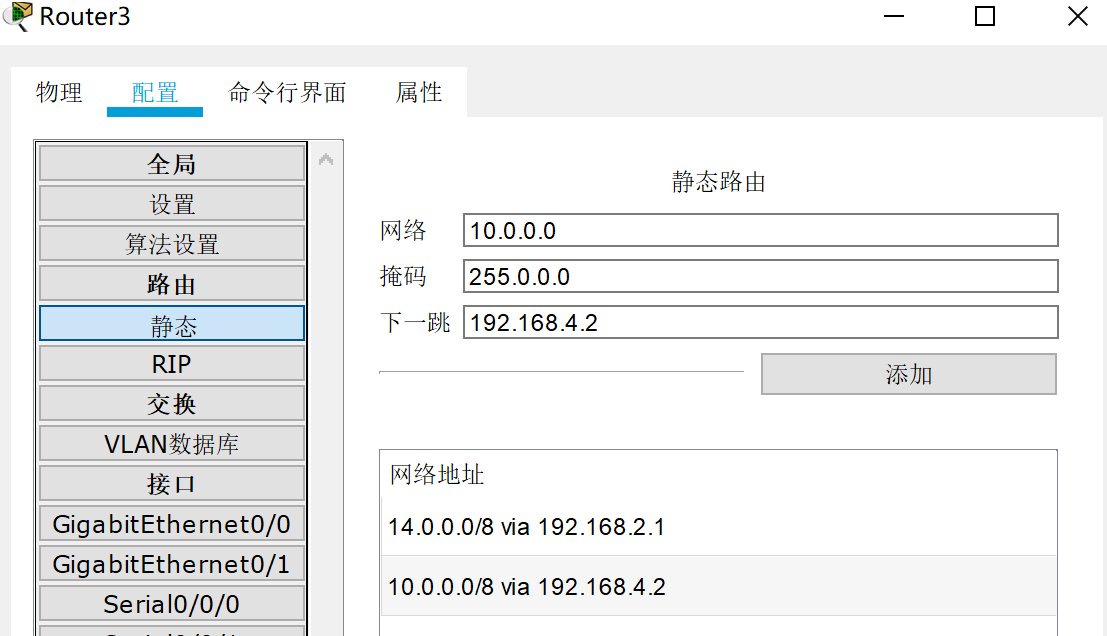
步骤1：在网络中配置出一条路由环路



首先在router3和router4之间增加一条串行线，并修改router2的静态路由，将下一跳接口改为192.168.2.2（即router3的Se0/0/0接口）；修改router3的静态路由，将通往10.0.0.0的下一跳接口改为192.168.4.2（即router4的Se0/0/1接口），形成环路。

步骤2：观察数据包在环路中的转发情况





从PC4向PC1发送数据包，可以发现产生了环路，数据包一直在router4—router2—router3—router4之间循环。

## 三、思考与总结

1. 如果路由器转发的数据包的目的网络不在路由表中，会如何处理？

答：如果有默认路由，按默认端口转发，否则丢弃。

1. 在任务四中的步骤2中，环路造成的循环转发过程会不会停止？原因是什么？

答：当被转发的IP包的TTL字段降到0时，循环转发将停止。

1. 默认路由有何作用？

答：默认路由在某些时候非常有效,当存在末梢网络时,默认路由会大大简化路由器的配置,减轻管理员的工作负担,提高网络性能. 默认路由（Default route），是对IP数据包中的目的地址找不到存在的其他路由时，路由器所选择的路由。

1. 实验过程中还遇到什么问题，如何解决的？通过该实验有何收获？

答：通过这次实验，我理解了直连路由和静态路由，并掌握了静态路由的配置方法。

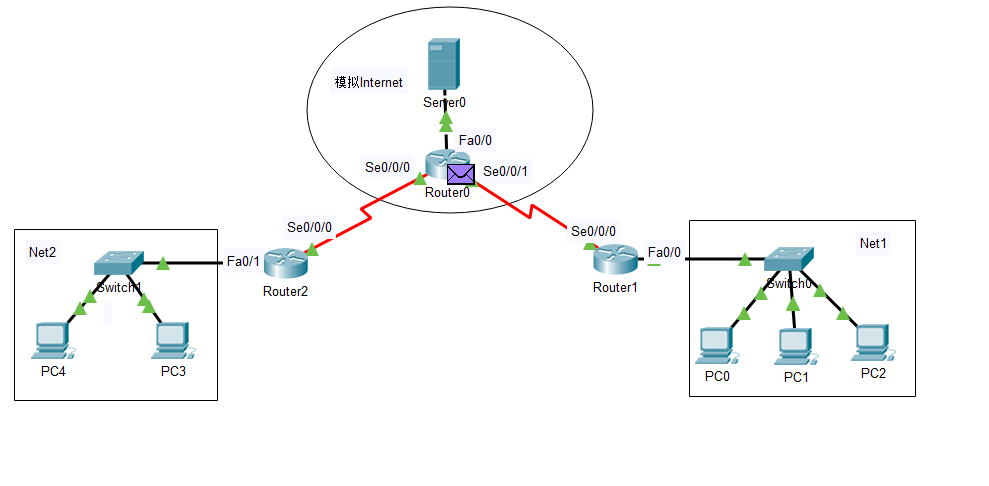
# 6.VPN与NAT协议分析

## 一、实验目的

1. 理解VPN使用的IP隧道技术的工作原理。
2. 理解NAT技术的工作原理。

## 二、实验步骤

1. 给出实验中用到的拓扑图

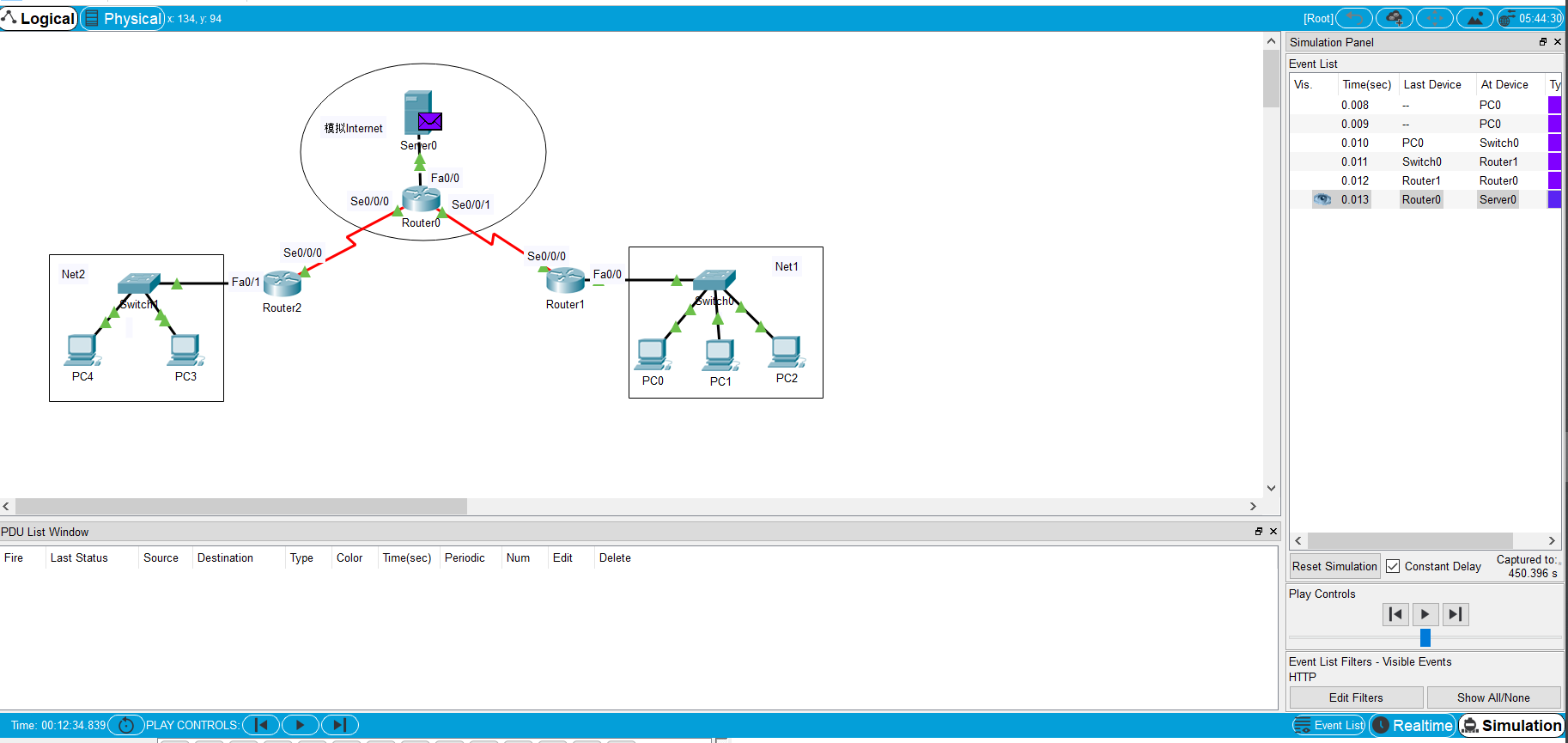


1. 给出实验中使用的IP配置表

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 设备 | 接口 | IP地址 | 掩码 | 默认网关 |
| PC0 | Fa0 | 192.168.1.1 | 255.255.255.0 | 192.168.1.254 |
| PC1 | Fa0 | 192.168.1.2 | 255.255.255.0 | 192.168.1.254 |
| PC2 | Fa0 | 192.168.1.3 | 255.255.255.0 | 192.168.1.254 |
| PC3 | Fa0 | 192.168.2.1 | 255.255.255.0 | 192.168.2.254 |
| PC4 | Fa0 | 192.168.2.2 | 255.255.255.0 | 192.168.2.254 |
| Router1 | Fa0/0 | 192.168.1.254 | 255.255.255.0 | —— |
| Router1 | Se0/0/0 | 158.22.120.34 | 255.255.0.0 | —— |
| Router2 | Se0/0/0 | 158.22.120.168 | 255.255.0.0 | —— |
| Router2 | Fa0/1 | 61.159.62.12 | 255.0.0.0 | —— |
| Server0 | Fa0 | 61.159.62.134 | 255.0.0.0 | 61.159.62.12 |

1. 任务一：观察学习NAT的工作原理。







1. 任务二：观察学习VPN工作原理。

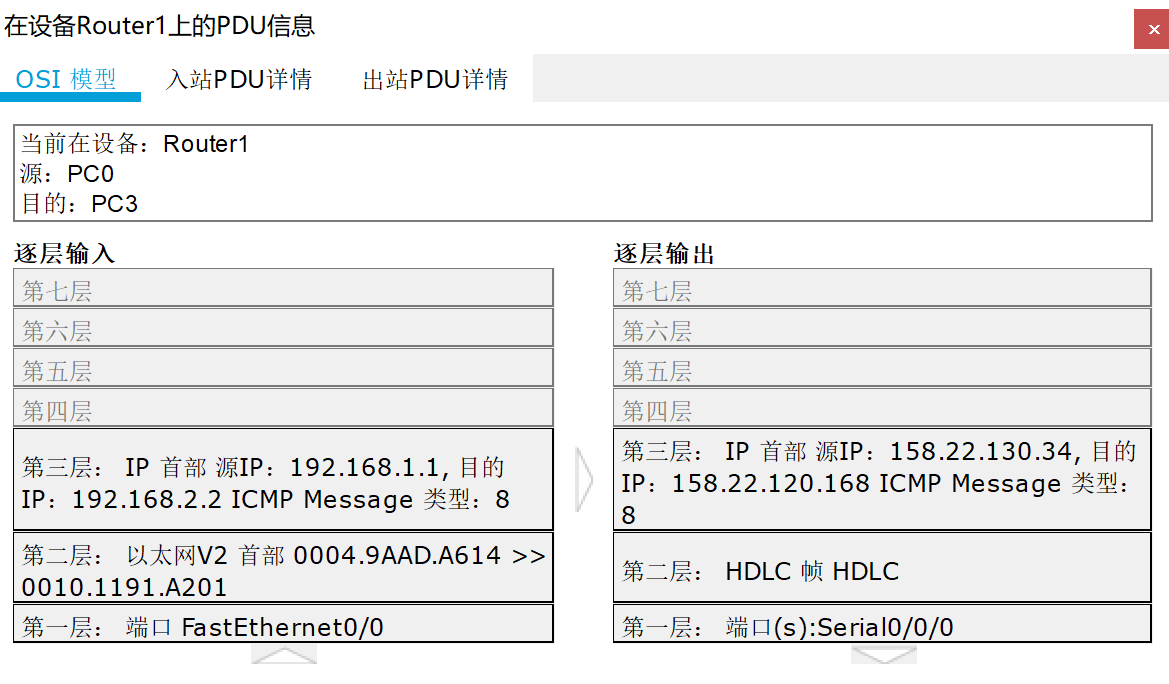
步骤1：初始化模拟

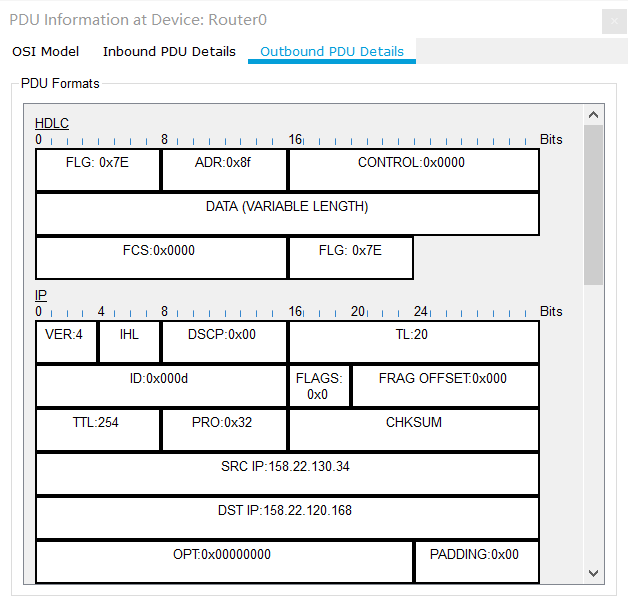
PC0向PC3发送一个包含ICMP报文的IP数据包，来初始化VPN连接。



步骤2：观察VPN的隧道技术

PDU的源IP和目的IP地址分别为 192.168.1.1（PC0的IP 地址）和 192.168.2.2（PC3的IP 地址）。而在 Outbound PDU 中，PDU 的源IP和目的IP地址已经更改158.22.130.34（Router1 的 Se0/0/0的IP地址）和158.22.120.168（Router2的Se0/0/0的IP地址），并且原IP包已经被重新封装在新的IP包中，这就是隧道技术的工作原理。





## 三、思考与总结

1. 在任务一中，Router1如何区分Server0返回给不同主机的HTTP报文？

答：NAT服务器（Router1）通过不同的端口号来识别不同的主机的报文。

1. 在任务二中，VPN中采用隧道技术的原因是什么？。

答：由于Net1和Net2都是使用私有地址，因此无法直接通过Internet进行通信；采用隧道技术可以方便地将源目地址转换为全局地址，而且到达目标路由器后，也很容易获得真正目标主机的IP地址。

1. Net1网络和Net2网络的IP地址能否编在同一段？

答：不能，这样会使两个网段间的主机的IP地址冲突

1. 实验过程中还遇到什么问题，如何解决的？通过该实验有何收获？

答：通过这次实验，我理解了VPN使用IP隧道技术的工作原理，同时也理解了NAT技术的工作过程。

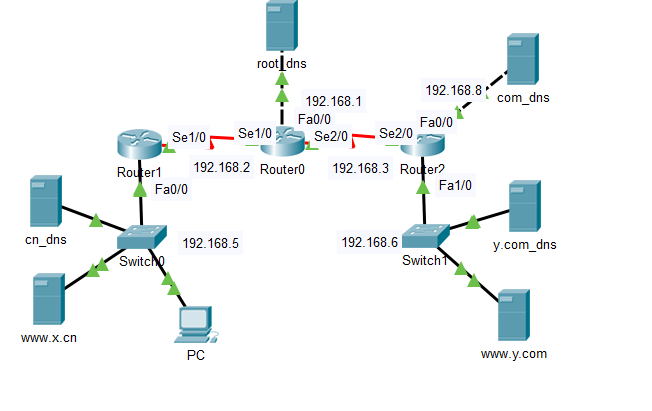
# 7.DNS解析实验

## 一、实验目的

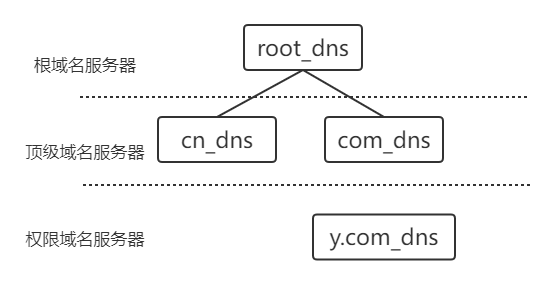
1. 理解DNS系统的工作原理。
2. 熟悉DNS服务器的工作过程。
3. 熟悉DNS报文格式。
4. 理解DNS缓存的作用。

## 二、实验步骤

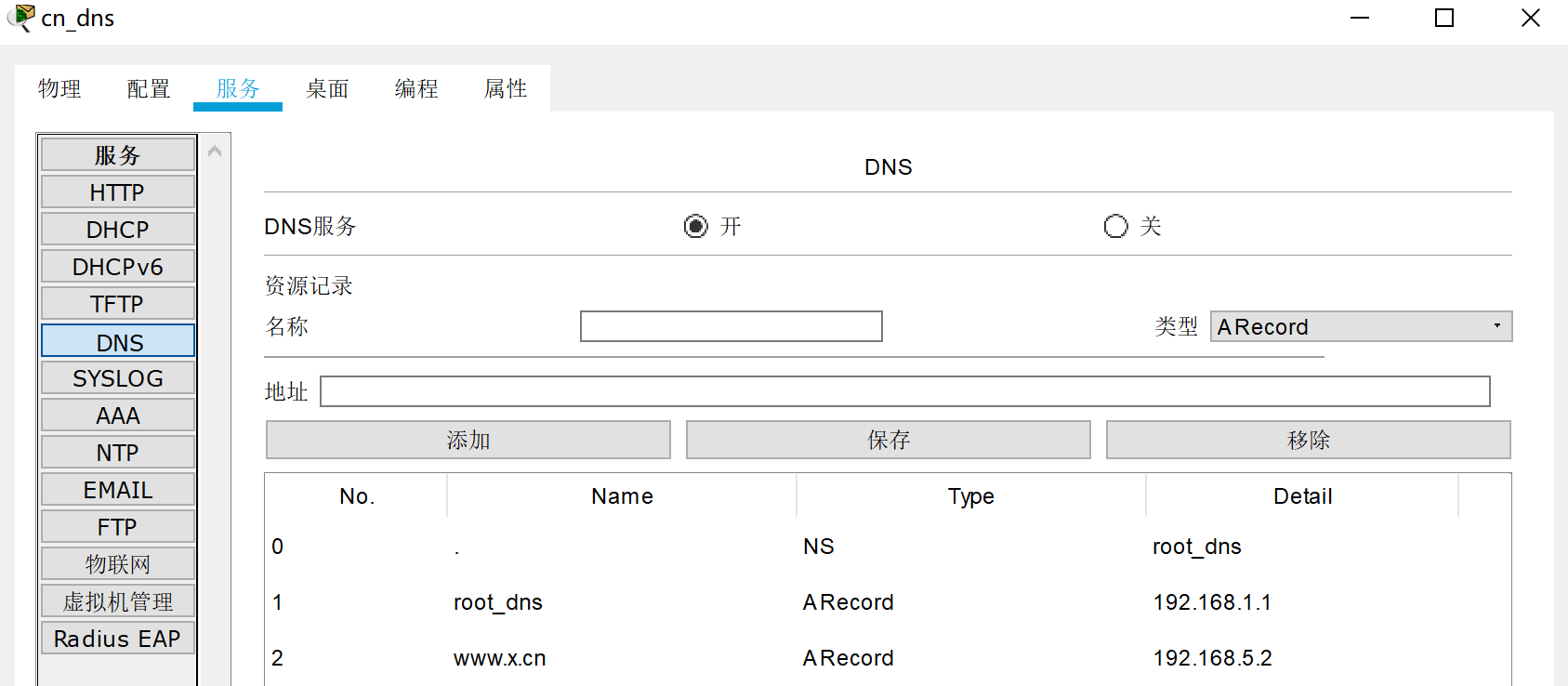
1. 给出实验中用到的拓扑图。

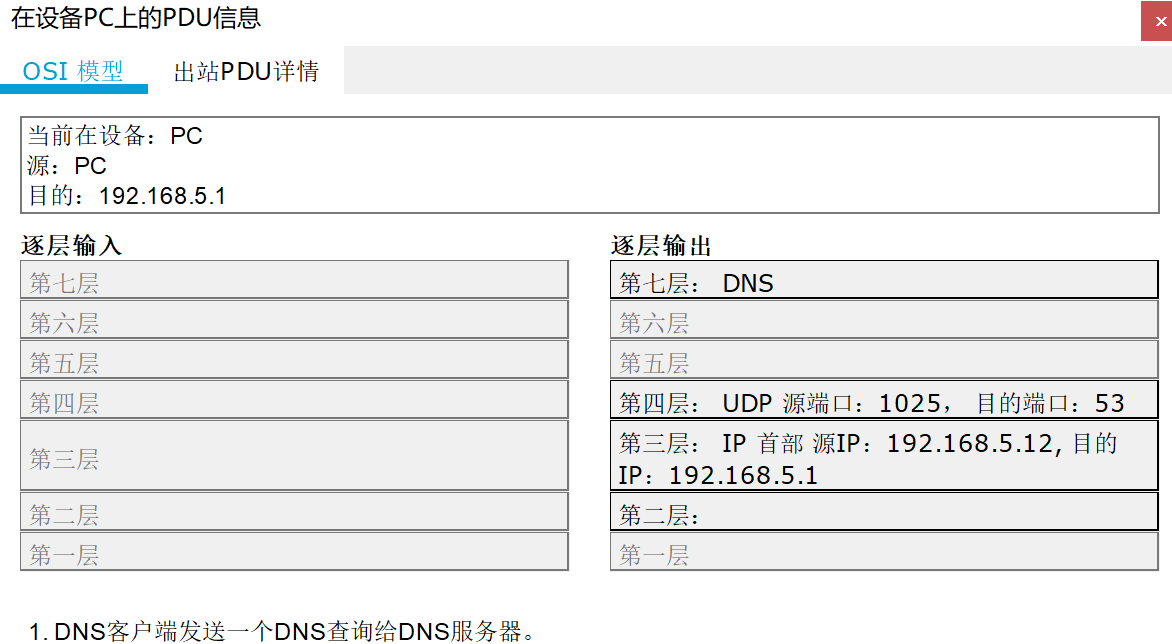


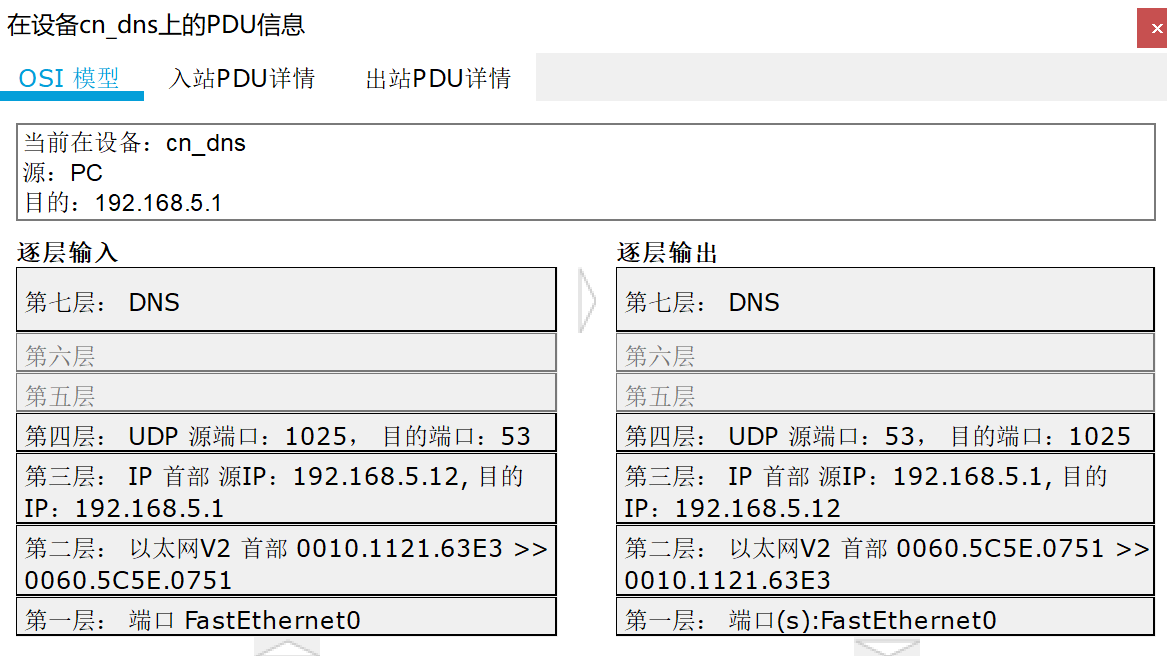
1. 绘制DNS域名服务器层次结构。



1. 任务一：观察本地域名解析过程。







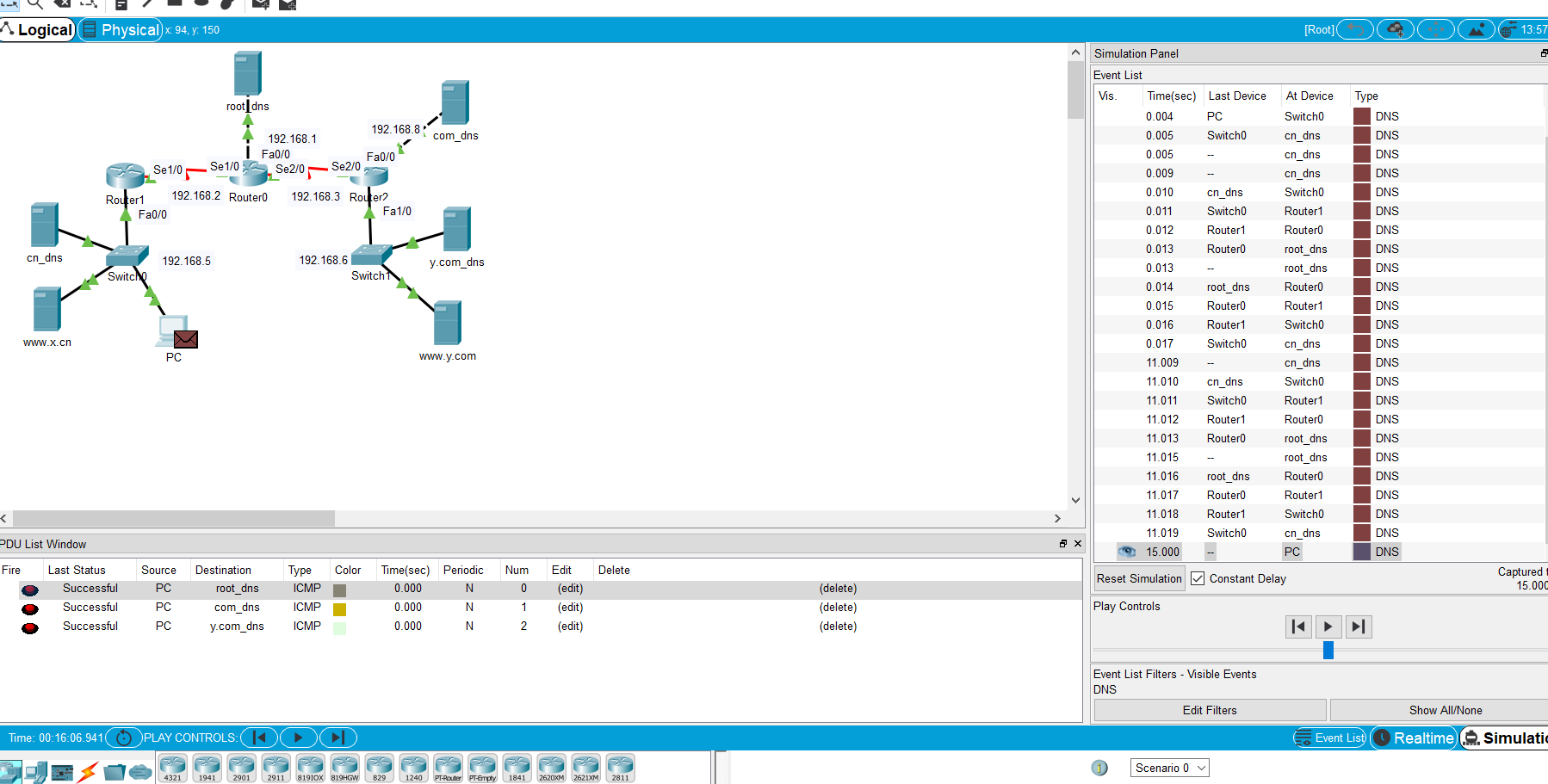
在PC上访问www.x.cn

① 由于PC中设置了DNS服务器的地址为192.168.5.1，因此当PC输入域名www.x.cn请求网页时，它将作为 DNS 客户端向本地域名服务器cn\_dns发送一个DNS查询请求，请求域名www.x.cn的 IP 地址。

② 本地域名服务器 cn\_dns 收到 PC 的 DNS 查询请求后，首先尝试在本地区域文件查找，发现确实存在相应的资源记录，于是将域名www.x.cn对应的 IP 地址 192.168.5.2 放入 DNS 的应答报文发送给 PC。

③ PC 收到本地域名服务器 cn\_dns的应答报文后，取出报文中解析出的IP 地址 192.168.5.2，并对其进行访问，此时在 Web Browser（Web浏览器）中显示相应的 Web 页面。

1. 任务二：观察外网域名解析过程。



步骤1：在PC的浏览器窗口请求外部Web服务器的网页

步骤2：捕获DNS事件并分析外网域名解析过程

QDCOUNT从PC发出到最后一直是1；ANCOUNT在www.y.com返回Switch1的时候变为1，在第二次com\_dns返回Router2时变为2。

1. 任务三：观察缓存的作用。

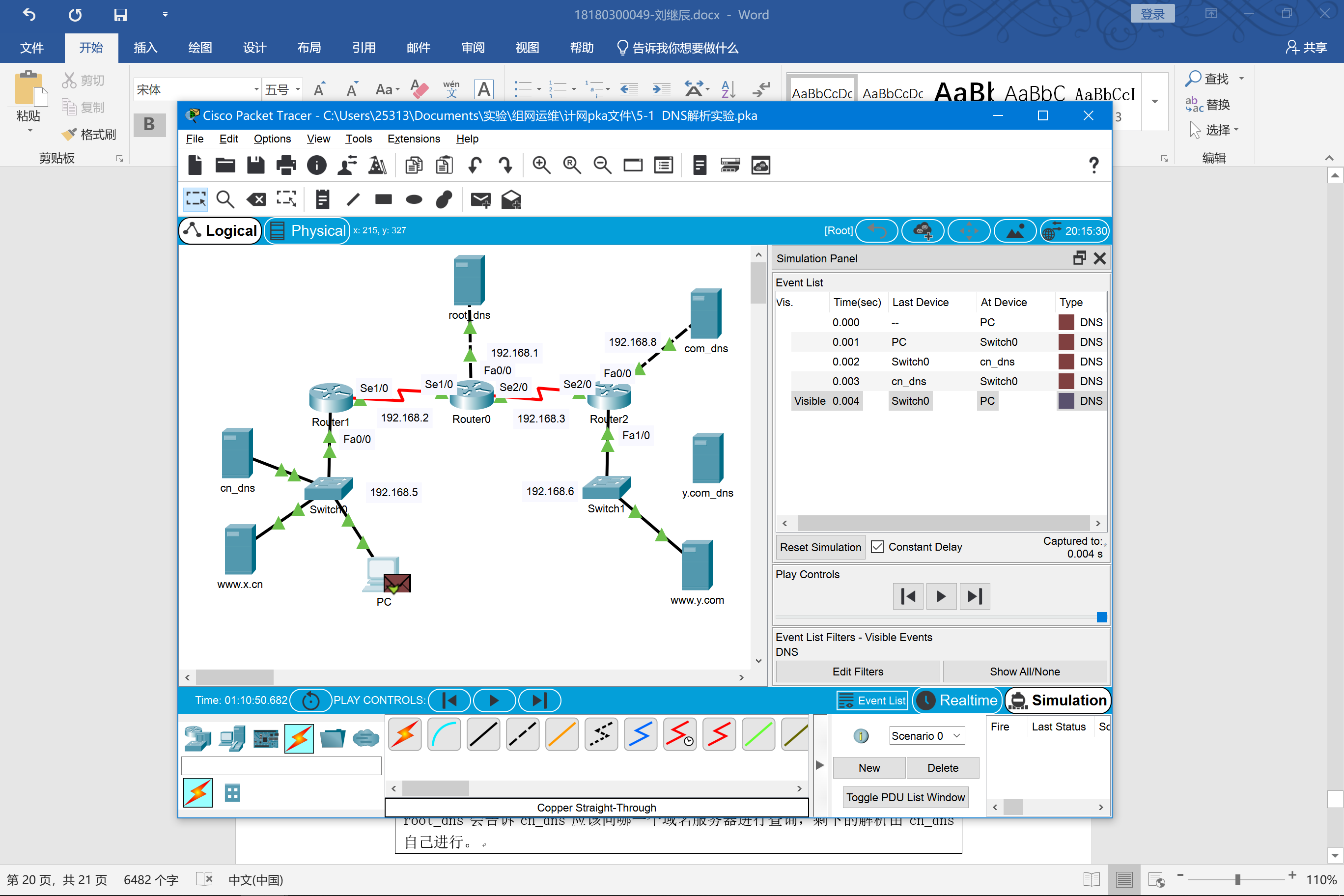
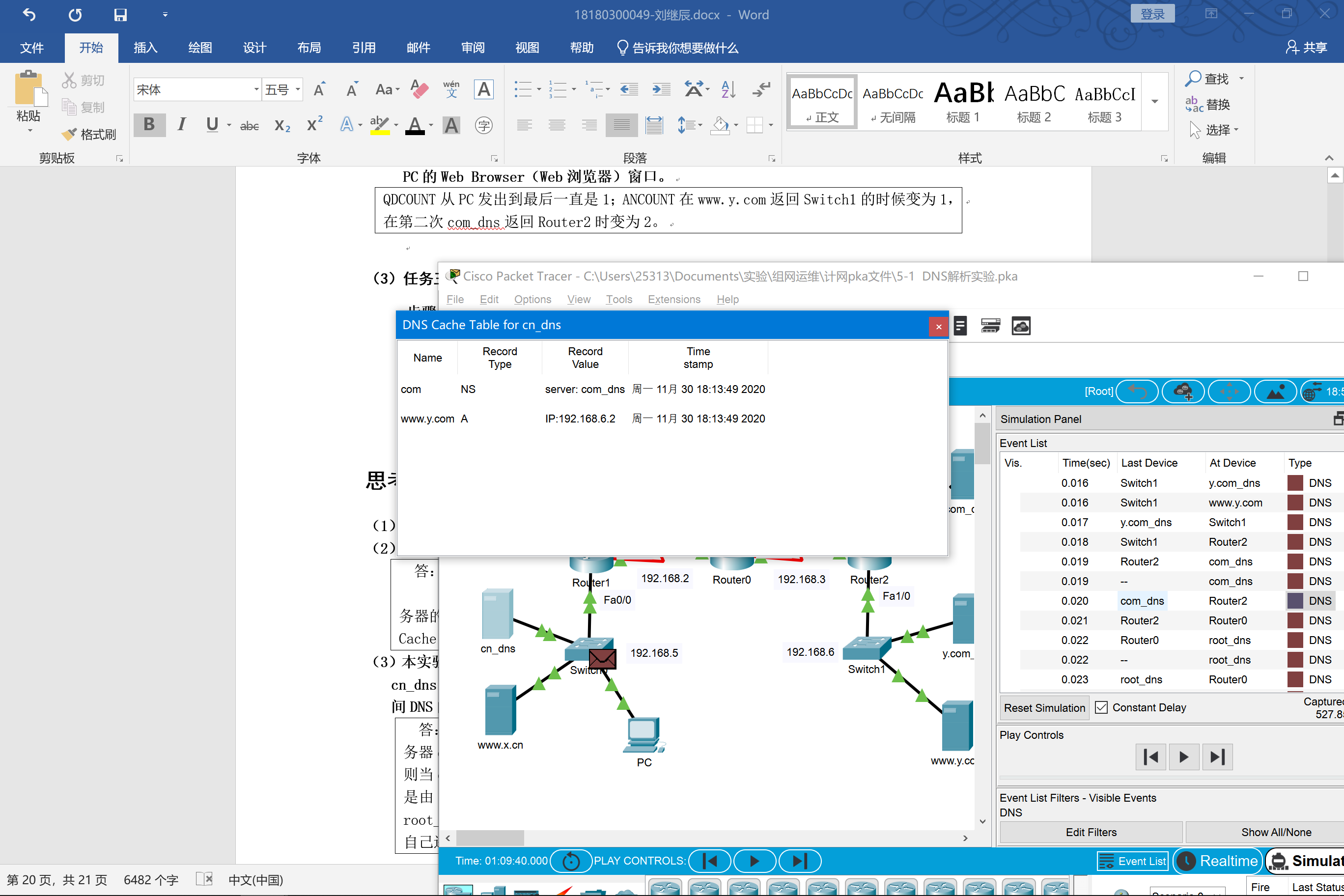
步骤1：查看本地域名服务器cn\_dns的缓存

步骤2：在PC的浏览器窗口请求外部Web服务器的网页

重复任务二，再次观察此次解析外网域名的过程。

完成后单击Reset Simulation（重置模拟）按钮，将原有的事件全部清空；同时关闭PC机的Web Browser（Web浏览器）窗口。

cn\_dns缓存内存在了www.y.com的IP地址，再次访问不在需要再向其他DNS服务器请求。



## 三、思考与总结

1. DNS协议使用运输层的什么协议？

答：TCP和UDP协议，DNS在进行区域传输的时候使用TCP协议，其它时候则使用UDP协议。

1. DNS缓存有什么作用？在Packet Tracer中如何清空DNS缓存。

答：DNS缓存用来存放最近解析过的域名等信息，因此可以提高解析效率。若需要在Packet Tracer中清空某个DNS服务器的缓存，可以进入该 DNS服务器的配置窗口，单击窗口下方的DNS Cache按钮，在弹出的窗口中单击下方的Clear Cache按钮即可把DNS缓存清空。

1. 本实验中PC与本地域名服务器cn\_dns之间的解析是递归还是迭代？本地域名服务器cn\_dns与根域名服务器root\_dns之间呢？若后者用另一种解析方法，则域名服务器之间DNS的请求和应答的交互过程应如何运行？

答：本实验中PC与本地域名服务器cn\_dns之间的解析是递归查询，本地域名服务器cn\_dns与根域名服务器root\_dns之间也是递归查询。若后者用的是迭代查询，则当cn\_dns向根域名服务器root\_dns请求解析而 root\_dns无法解析出结果时，不是由root\_dns全权帮助cn\_dns直接解析出结果并将解析结果告知cn\_dns而是root\_dns会告诉cn\_dns应该向哪一个域名服务器进行查询，剩下的解析由cn\_dns自己进行。

1. 实验过程中还遇到什么问题，如何解决的？通过该实验有何收获？

答：通过这次实验，我理解了DNS系统的工作原理，熟悉了DNS服务器的工作过程，同时也熟悉了DNS报文格式和DNS缓存的作用。

# 8.DHCP分析

## 一、实验目的

1. 了解DHCP的作用。
2. 熟悉DHCP的工作过程。
3. 熟悉DHCP的报文格式。

## 二、实验步骤

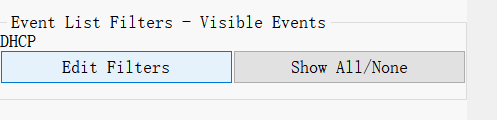
1. 给出实验中用到的拓扑图

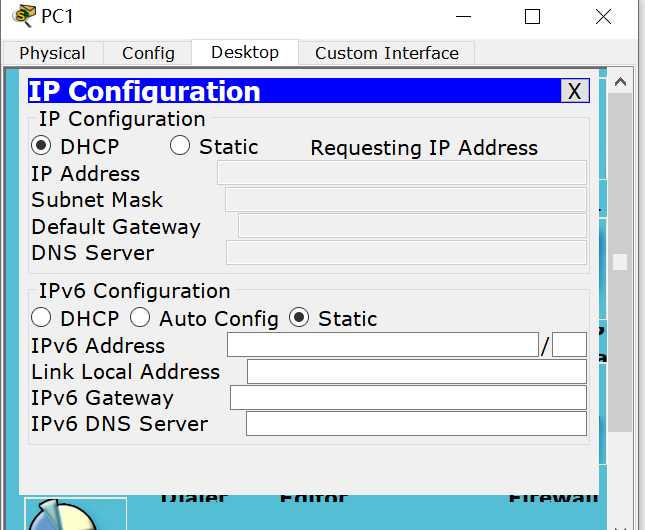


1. 任务一：DHCP服务器为内网主机PC1动态分配IP地址。

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 设备 | 接口 | IP地址 | 子网掩码 | 网关 |
| Router1 | Fa1/0 | 192.168.2.254 | 255.255.255.0 |  |
| Se2/0 | 192.168.4.1 | 255.255.255.0 |  |
| Router2 | Fa0/0 | 192.168.3.254 | 255.255.255.0 |  |
| Se2/0 | 192.168.4.2 | 255.255.255.0 |  |
| DHCP | Fa0 | 192.168.2.1 | 255.255.255.0 | 192.168.2.254 |

1. 捕获DHCP事件





1. 分析DHCP的工作过程及报文格式

DHCP的工作过程大致如下。

①PC1首先以广播方式发送一一个 DHCP Discover Packet (DHCP发现报文)，由于此时PC1还未设置IP地址信息，该报文的源IP为0.0.0.0。②DHCP服务器收到DHCP发现报文后，发现未与DHCP客户端(即PC1)进行绑定，于是从地址池中找出第一一个可用的IP地址封装成DHCPOffer Packet (DHCP 提供报文)并以广播方式发送出去。

③PC1收到DHCP提供报文后，以广播方式发送一一个DHCP RequestPacket (DHCP请求报文)，请求使用预分配的IP地址。

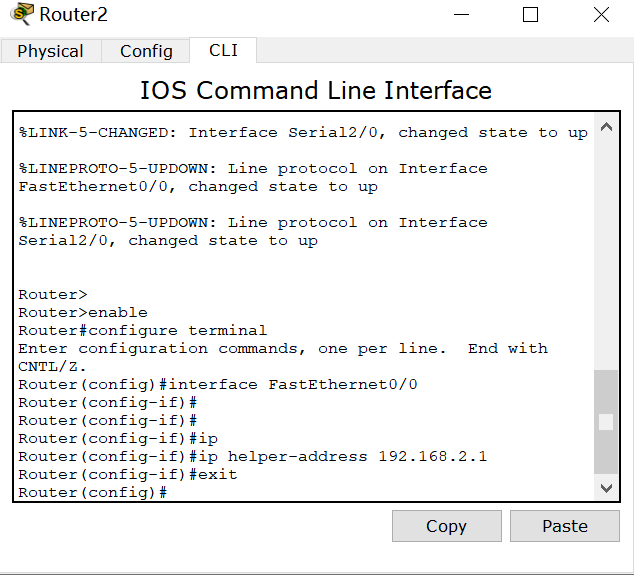
④DHCP服务器收到DHCP请求报文后，将被请求的IP地址从其地址池中与DHCP客户端(PC1)的MAC地址绑定，并以广播方式发送一- 个DHCP Ack Packet (DHCP确认报文)。

⑤PC1 收到该报文后，在本机进行IP配置。

由于路由器的端口默认隔离广播，因此在上述过程中路由器Routerl每次收到广播包后，均将其丢弃。

1. 任务二：DHCP服务器为外网主机PC2动态分配IP地址。

A、配置DHCP中继命令



1. 分析DHCP的工作过程

DHCP的工作过程大致如下。

①PC2首先以广播方式发送一个DHCP Discover Packet (DHCP发现报文)，由于此时PC2还未设置IP地址信息，该报文的源IP为0.0.0.0。

②Router2从Fa0/0端口收到该报文后，由于该端口配置了DHCP中继，且该报文是广播包，符合Helper criteria (助手标准)，可以转发。重新封装的数据包转发给Helper Address (助手地址) 192.168.2.1, 且将源IP设置为Router2的Fa0/O端口的IP地址，之后查找路由表并转发。

③DHCP服务器收到DHCP发现报文后，发现未与DHCP客户端(即PC2)进行绑定，从地址池中找出第一个可用的IP地址封装成DHCP OfferPacket (DHCP提供报文)发送出去。

④Router2从Helper address (助手地址)收到报文后，从Fa0/0端口转发出去。

⑤PC2收到DHCP提供报文后，再次以广播方式发送一个DHCPRequest Packet (DHCP请求报文)，请求使用预分配的IP地址。

⑥Router2再次转发该报文。

⑦DHCP服务器收到DHCP请求报文后，将被请求的IP地址从其地址池中与DHCP客户端(PC2) 的MAC地址绑定，并发送-一个DHCP AckPacket (DHCP确认报文)。

⑧Router2 从Fa0/0端口将该报文转发给PC2。

⑨PC2 收到该报文后，在本机进行IP配置。

完成后单击Reset Simulation (重置模拟)按钮，将原有的事件全部清空:同时关闭PC2的配置窗口。

## 三、思考与总结

1. 如何判断报文的发送方式是单播还是广播？

答:由发送报文首部中的目标IP地址来判断。若是某个具体的IP，则说明该报文是单播发送方式:若是255.255.255.255， 则说明该报文是广播。

1. 任务二中为何需要在路由器Router2中配置DHCP中继？DHCP中继有何作用？

答:因为任务二中DHCP服务器需要为外网主机动态分配IP地址，而DHCP报文以广播方式发出，路由器的端口默认又是隔离广播的，此时若需要路由器转发广播包，则必须在路由器收到广播包的端口配置iphelper-address，才能转发ip forward-protocol中定义的广播包，并以单播方式送出。DHCP中继的作用: DHCP中继代理可以用来转发跨网的DHCP请求及响应，因此可以避免在每个物理网络都建立一台DHCP服务器。

1. 分析DHCP服务器在分派IP地址时的规律。

答:从DHCP配置的地址池中的第- -个地址开始往后分配。

1. 若有多个DHCP服务器，DHCP的工作过程会有变化吗？

答：同一网络有两个DHCP会冲突，大家都在分配相同的IP出去，IP会冲突的。

1. 实验过程中还遇到什么问题，如何解决的？通过该实验有何收获？

答：通过这次实验，我了解了DHCP的作用，熟悉了DHCP的工作过程以及其报文格式。