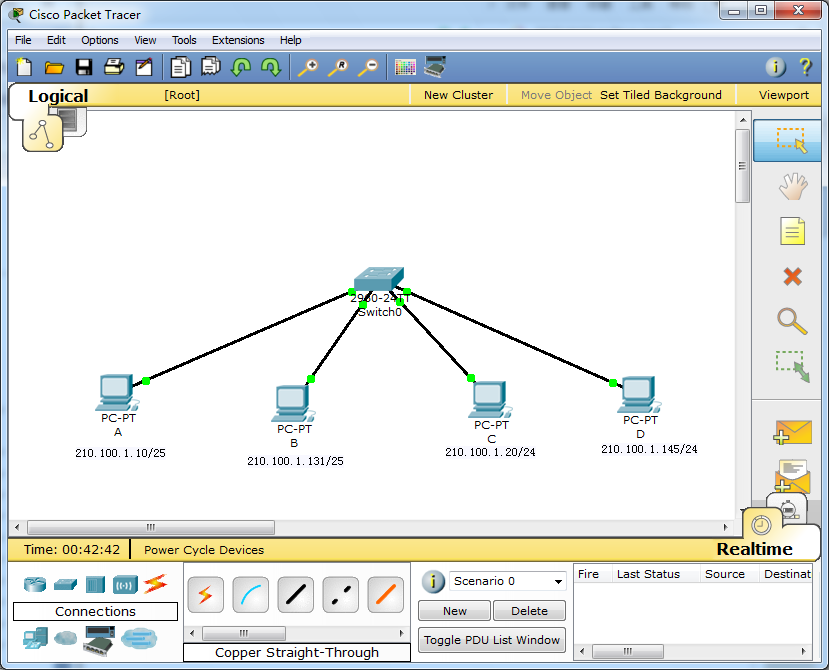
综合验证性实验：

实验一、网络命令的使用

第一部分：子网划分与连通性测试



某单位一个局域网中，使用交换机连接了4台计算机，它们的网络参数（IP地址/子网掩码）配置如图所示，请完成如下问题：

1. 对四个IP地址进行分析，哪些地址位于同一个子网，哪些地址网络地址相同，但是子网掩码不同。

分析：网络属性的表示格式为：ip/子网掩码的位数，网络号为ip地址和子网掩码逐位相与。由此可得表1。

表1 网络配置属性表

|  |  |  |  |
| --- | --- | --- | --- |
| 主机编号 | IP地址 | 子网掩码 | 网络地址 |
| PC-PTA | 210.100.1.10 | 255.255.255.128 | 210.100.1.0 |
| PC-PTB | 210.100.1.131 | 255.255.255.128 | 210.100.1.128 |
| PC-PTC | 210.100.1.20 | 255.255.255.0 | 210.100.1.0 |
| PC-PTD | 210.100.1.145 | 255.255.255.0 | 210.100.1.0 |

**如果在同一子网，那么子网掩码和网络号均相同**，由此可得：主机C和D的地址位于同一个子网。

同时，由表1得，主机A与主机C，D的网络地址相同，但是子网掩码不同。

1. 主机之间互相ping，列出结果，并认真分析原因。

主机之间的连通性测试如图1-4。

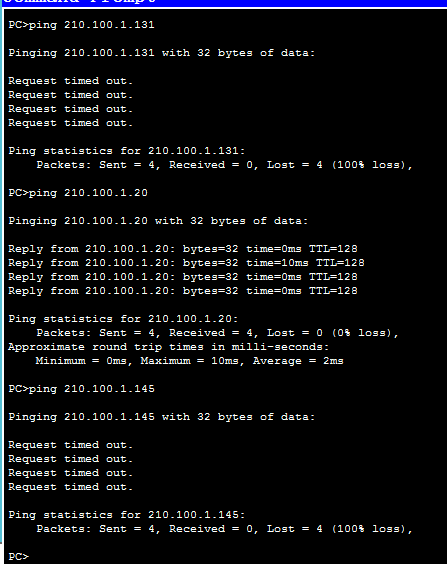


图1 A与其它主机之间的ping测试

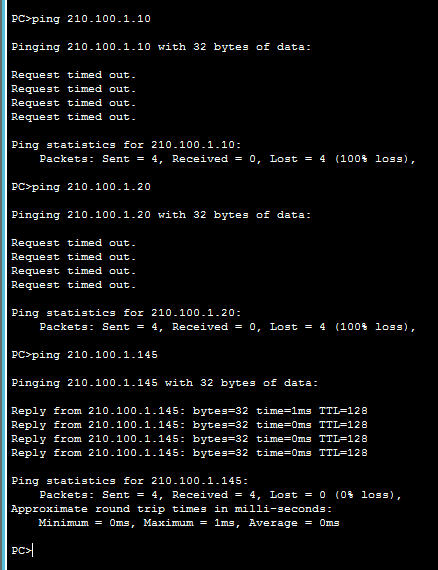


图2 B与其它主机之间的ping测试

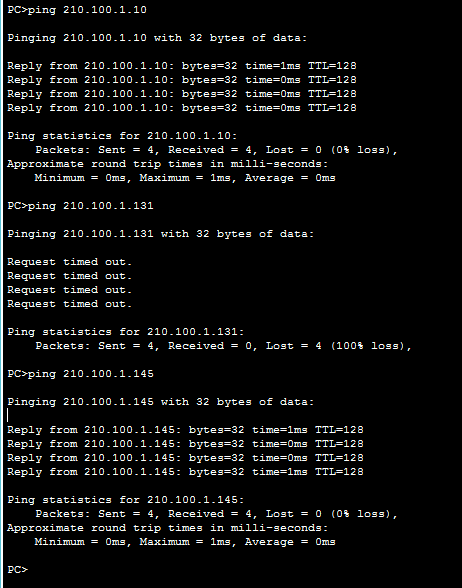


图3 C与其它主机之间的ping测试

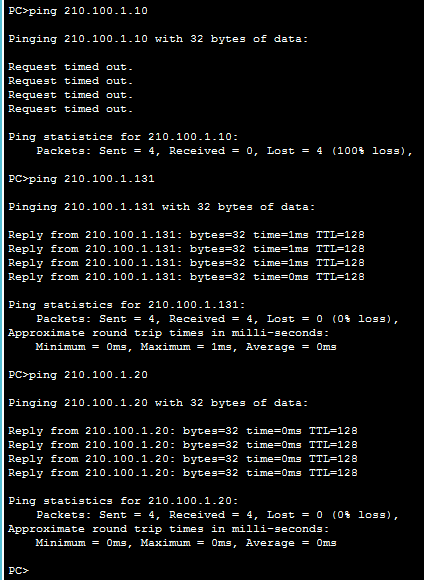


图 4 D与其它主机之间的ping测试

表2 各个主机之间的ping结果以及原因

|  |  |  |  |
| --- | --- | --- | --- |
| 源主机 | 目的主机 | 连通性 | 原因 |
| A | B | 不通 | A先将B的ip地址和自己的子网掩码逐位相与得到的网络地址为210.100.1.128,和自己的网络地址不同,而网关为空，故ping不通 |
| A | C | 通 | A先将C的ip地址和自己的子网掩码逐位相与得到的网络地址和自己的网络地址相同，同时C收到A的数据包后发送给A的回复信息时将A的ip地址和自己的子网掩码相与后得到的网络地址和自己的网络地址相同，故通 |
| A | D | 不通 | A先将D的ip地址和自己的子网掩码逐位相与得到的网络地址为210.100.1.128,和自己的网络地址不同,而网关为空，故ping不通 |
| B | A | 不通 | B先将A的ip地址和自己的子网掩码逐位相与得到的网络地址为210.100.1.0,和自己的网络地址不同,而网关为空，故ping不通 |
| B | C | 不通 | B先将C的ip地址和自己的子网掩码逐位相与得到的网络地址为210.100.1.0,和自己的网络地址不同,而网关为空，故ping不通 |
| B | D | 通 | B先将D的ip地址和自己的子网掩码逐位相与得到的网络地址和自己的网络地址相同，同时D收到B的数据包后发送给B的回复信息时将B的ip地址和自己的子网掩码相与后得到的网络地址和自己的网络地址相同，故通 |
| C | A | 通 | C先将A的ip地址和自己的子网掩码逐位相与得到的网络地址和自己的网络地址相同，同时A收到C的数据包后发送给C的回复信息时将C的ip地址和自己的子网掩码相与后得到的网络地址和自己的网络地址相同，便认为C和自己在同一个网络,故通 |
| C | B | 不通 | C先将B的ip地址和自己的子网掩码逐位相与,得到的子网掩码为210.100.1.0,和自己的子网掩码相同,便认为是在同一个网络,因此发送给B信息,B收到之后在给C回复时将C的ip地址和自己的子网掩码逐位相与得到的网络号为210.100.1.0和自己的网络号不同,因此ping不通. |
| C | D | 通 | 不论是C将D的ip地址和自己的子网掩码逐位相与还是D将C的ip地址和自己的子网掩码逐位相与得到的网络号均与各自的网络号相同,故可以ping同. |
| D | A | 不通 | 虽然D将A的ip地址和自己的子网掩码逐位相与得到的网络号和自己的网络号相同,但是A将D的ip地址和自己的子网掩码逐位相与得到的网络号为210.100.1.128和自己的网络号不同,故不同. |
| D | B | 通 | 不论是D将B的ip地址和自己的子网掩码逐位相与还是B将D的ip地址和自己的子网掩码逐位相与得到的网络号均与各自的网络号相同,故可以ping同. |
| D | C | 通 | 不论是D将C的ip地址和自己的子网掩码逐位相与还是C将D的ip地址和自己的子网掩码逐位相与得到的网络号均与各自的网络号相同,故可以ping同. |

第二部分：深刻理解运输层协议

运输层是负责数据通信的最高层，充分理解和验证运输层协议有助于对数据通信、数据传输的深刻理解，以及对其下层协议的理解。请用Wireshark软件完成如下要求：

1. TCP三次握手全过程。三次交互。首部关键字段理解：序号、确认号、同步/确认开关量、接收窗口等。（知识点：TCP报文首部、TCP连接管理）

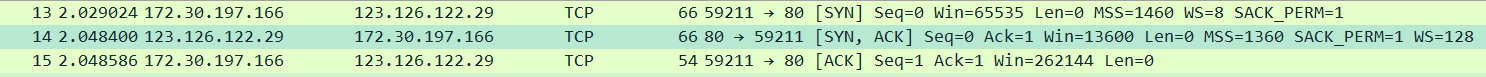


图5 TCP的三次握手

分析：如表3。第一次握手时，本地主机连接远程服务器。发送一个序号为0，确认号为0的TCP，同时SYN=1，代表次TCP为请求连接。设置自己的接受窗口为65535。第二次握手时，远程服务器收到请求后进行回复，自己的序号为0，对收到的数据进行确认，希望得到编号为1的数据，设置SYN=1，ACK=1，代表此TCP为对请求的确认。

第三次为本地对远程服务器的再次确认，序号为1，确认号为1，ACK=1，接受窗口变为了32768。第三次确认是为了避免第一次的请求报文重复发送带来的重复连接。

表3 TCP协议的三次握手

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 握手次序 | 序号 | 确认号 | 同步/确认开关量 | 接受窗口 |
| 第一次握手 | 0 | 0 | SYN=1 | 65535 |
| 第二次握手 | 0 | 1 | SYN=1，ACK=1 | 13600 |
| 第三次握手 | 1 | 1 | ACK=1 | 32768 |

1. UDP报文传输，首部内容分析，端口等字段。（知识点：UDP协议）

分析：当收到UDP报文时，读取到目的端口就把数据发送给此端口，当发送时，只需在数据中添加UDP首部。

表4 UDP首部的字段

|  |  |  |  |
| --- | --- | --- | --- |
| 源端口 | 目的端口 | 数据长度 | 检验和 |
| 57522 | 8000 | 130 | 0xf4b5 |

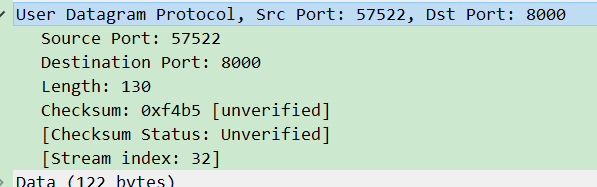


图6 截获的udp报文

1. TCP停等协议，发送-确认交互，尤其观测是累计确认还是单一确认。（知识点：TCP可靠传输-停等协议）

累积确认就是接收方不需要对收到的分组逐个发送确认，而是在收到几个分组后，对按序到达的最后一个分组发送确认，这就表示：到这个分组为止的所有分组都已经正确收到了。

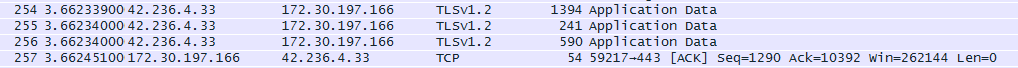


图7 累积确认。

1. TCP超时重传，能否设计出发送后超时重传，观察计时时间，重传报文段与第一次发送的报文段时间差。（知识点：TCP可靠传输-停等协议）

分析： TCP协议要求在发送端每发送一个报文段，就启动一个定时器并等待确认信息；接收端成功接收新数据后返回确认信息。若在定时器超时前数据未能被确认，TCP就认为报文段中的数据已丢失或损坏，需要对报文段中的数据重新组织和重传。



图8 超时重传

1. TCP连接释放，能否捕获完成双向释放请求和确认，注意观察主机中协议端口状态。（知识点：TCP连接管理）

分析：不失一般性，假设通信的双方为A和B，并且设A首先发起释放请求。

TCP连接的A发送释放请求，标记字段FIN=1，ACK=1；序号为1，确认字段ACK=102967，长度Len=0。

B收到释放请求之后，发送一个标记字段ACK=1，序号为102967，长度为0的TCP报文。并且发送一个释放连接请求，标记字段FIN=1，ACK=1，序号为102967，确认号为2，Len=0的请求报文。

A收到释放请求后发送一个确认报文，标记字段ACK=1，序号=2，确认号为102968。

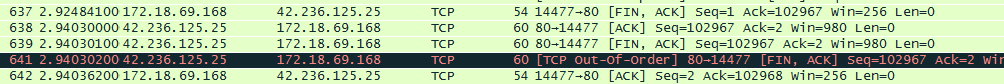


图9 TCP连接的释放

1. 不同高层协议在运输层的反映，如http、QQ、FTP等应用。（知识点：TCP、UDP协议及应用层协议）

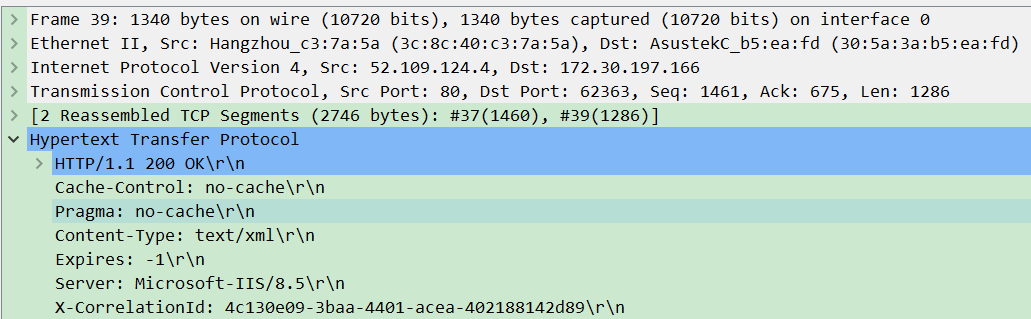


图10 http协议

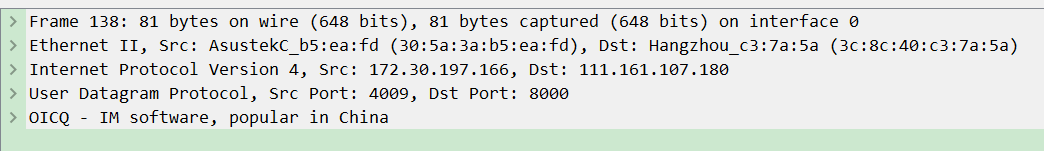


图11 OICQ（QQ）协议

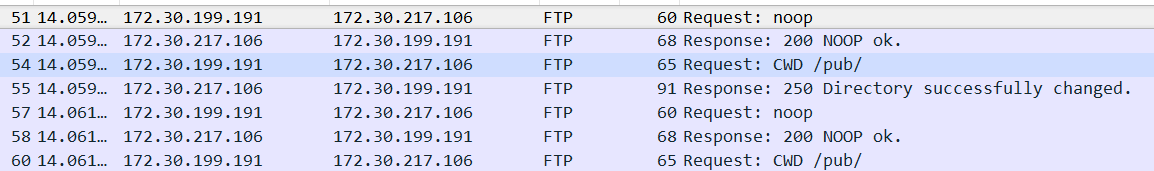


图12 捕获的ftp包

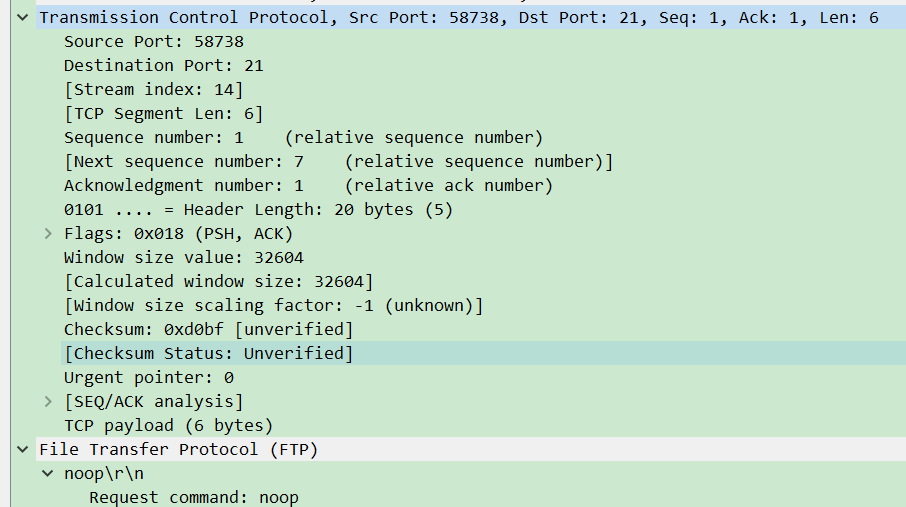


图13 捕获的第一个ftp包

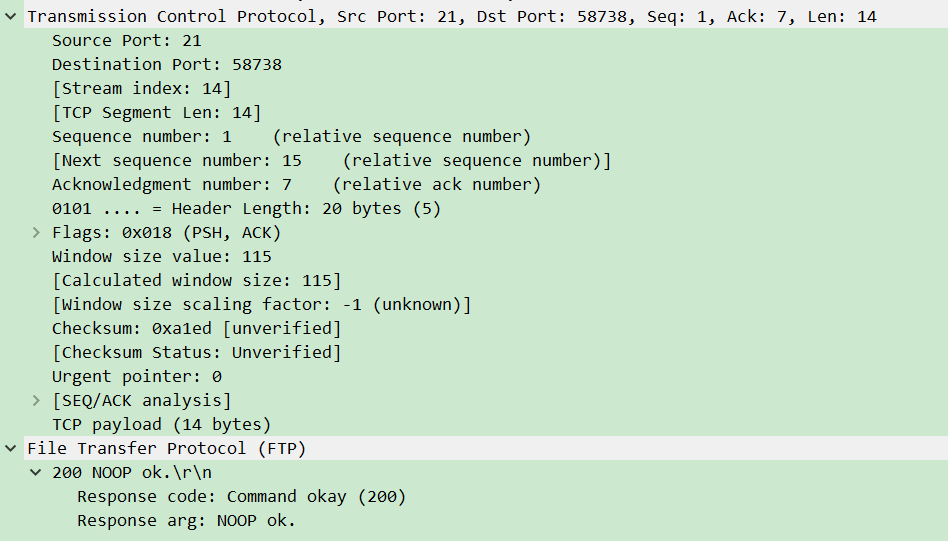


图14 捕获的第二个ftp包

表5 对ftp协议的分析（第一个包）

|  |  |  |  |
| --- | --- | --- | --- |
| 源端口号 | 58738 | 目的端口号 | 21 |
| 源IP地址 | 172.30.199.191 | 目的IP地址 | 172.30.217.106 |
| 源MAC地址 | 30:5a:3a:b5:ea:fd | 目的MAC地址 | 00:0c:29:14:fb:f9 |
| 序号 | 1 | 确认号 | 1 |
| 长度 | 6 | 应用层协议 | File Transfer Protocol |

表6 对ftp协议的分析（第二个包）

|  |  |  |  |
| --- | --- | --- | --- |
| 源端口号 | 21 | 目的端口号 | 58738 |
| 源IP地址 | 172.30.217.106 | 目的IP地址 | 172.30.199.191 |
| 源MAC地址 | 00:0c:29:14:fb:f9 | 目的MAC地址 | 30:5a:3a:b5:ea:fd |
| 序号 | 1 | 确认号 | 7 |
| 长度 | 14 | 应用层协议 | File Transfer Protocol |