**【实验名称】：TCP段分析实验**

**学生姓名：陈嘉瑞 合作学生： 无**

**实验地点：济事楼330网络实验室 实验时间：2023年12月4日**

**【实验目的】**

1. 了解TCP协议
2. 掌握使用WireShark抓取TCP报文的方法
3. 掌握分析TCP报文的方法

**【实验原理】**

1. TCP概述

TCP是传输层的协议，功能即为在IP的数据报服务之上增加了最基本的服务：复用和分用以及差错检测。TCP 是一个基于连接的四层协议，提供全双工地，可靠地传输系统。它能够保证数据被远程主机接收。并且能够为高层协议提供flow-controlled 服务。空间上，TCP需要在端系统中维护连接状态，需要一定的开销。此连接装入包括接收和发送缓存，拥塞控制参数和序号与确认号的参数。UDP不维护连接状态，也不跟踪这些参数，开销小。空间和时间上都具有优势。

1. TCP报文格式

TCP报文是TCP层传输的数据单元，也叫报文段。



1. TCP报文字段

A、端口号：用来标识同一台计算机的不同的应用进程。

1）源端口：源端口和IP地址的作用是标识报文的返回地址。

2）目的端口：端口指明接收方计算机上的应用程序接口。

TCP报头中的源端口号和目的端口号同IP数据报中的源IP与目的IP唯一确定一条TCP连接。

B、序号和确认号：是TCP可靠传输的关键部分。序号是本报文段发送的数据组的第一个字节的序号。在TCP传送的流中，每一个字节一个序号。例如：一个报文段的序号为300，此报文段数据部分共有100字节，则下一个报文段的序号为400。所以序号确保了TCP传输的有序性。确认号，即ACK，指明下一个期待收到的字节序号，表明该序号之前的所有数据已经正确无误的收到。确认号只有当ACK标志为1时才有效。比如建立连接时，SYN报文的ACK标志位为0。

C、数据偏移／首部长度：4bits。由于首部可能含有可选项内容，因此TCP报头的长度是不确定的，报头不包含任何任选字段则长度为20字节，4位首部长度字段所能表示的最大值为1111，转化为10进制为15，15\*32/8 = 60，故报头最大长度为60字节。首部长度也叫数据偏移，是因为首部长度实际上指示了数据区在报文段中的起始偏移值。

D、保留：为将来定义新的用途保留，现在一般置0。

E、控制位：URG ACK PSH RST SYN FIN，共6个，每一个标志位表示一个控制功能。

1）URG：紧急指针标志，为1时表示紧急指针有效，为0则忽略紧急指针。

2）ACK：确认序号标志，为1时表示确认号有效，为0表示报文中不含确认信息，忽略确认号字段。

3）PSH：push标志，为1表示是带有push标志的数据，指示接收方在接收到该报文段以后，应尽快将这个报文段交给应用程序，而不是在缓冲区排队。

4）RST：重置连接标志，用于重置由于主机崩溃或其他原因而出现错误的连接。或者用于拒绝非法的报文段和拒绝连接请求。

5）SYN：同步序号，用于建立连接过程，在连接请求中，SYN=1和ACK=0表示该数据段没有使用捎带的确认域，而连接应答捎带一个确认，即SYN=1和ACK=1。

6）FIN：finish标志，用于释放连接，为1时表示发送方已经没有数据发送了，即关闭本方数据流。

F、窗口：滑动窗口大小，用来告知发送端接受端的缓存大小，以此控制发送端发送数据的速率，从而达到流量控制。窗口大小时一个16bit字段，因而窗口大小最大为65535。

G、校验和：奇偶校验，此校验和是对整个的 TCP 报文段，包括 TCP 头部和 TCP 数据，以 16 位字进行计算所得。由发送端计算和存储，并由接收端进行验证。

H、紧急指针：只有当URG 标志置 1 时紧急指针才有效。紧急指针是一个正的偏移量，和顺序号字段中的值相加表示紧急数据最后一个字节的序号。 TCP 的紧急方式是发送端向另一端发送紧急数据的一种方式。

I、选项和填充：最常见的可选字段是最长报文大小，又称为MSS（Maximum Segment Size），每个连接方通常都在通信的第一个报文段（为建立连接而设置SYN标志为1的那个段）中指明这个选项，它表示本端所能接受的最大报文段的长度。

I、选项和填充：选项长度不一定是32位的整数倍，所以要加填充位，即在这个字段中加入额外的零，以保证TCP头是32的整数倍。

J、数据部分： TCP 报文段中的数据部分是可选的。在一个连接建立和一个连接终止时，双方交换的报文段仅有 TCP 首部。如果一方没有数据要发送，也使用没有任何数据的首部来确认收到的数据。在处理超时的许多情况中，也会发送不带任何数据的报文段。

1. TCP连接过程

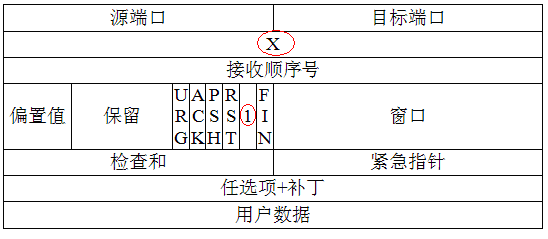
相对于SOCKET开发者,TCP创建过程和链接折除过程是由TCP/IP协议栈自动创建的。因此开发者并不需要控制这个过程。但是对于理解TCP底层运作机制，相当有帮助。TCP连接过程简单一句话概括：“三次握手四次挥手”。

A. TCP三次握手

所谓三次握手(Three-way Handshake)，是指建立一个TCP连接时，需要客户端和服务器总共发送3个包。三次握手的目的是连接服务器指定端口，建立TCP连接,并同步连接双方的序列号和确认号并交换 TCP 窗口大小信息.在socket编程中，客户端执行connect()时。将触发三次握手。

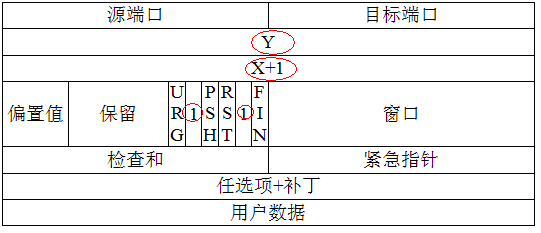
第一次握手:

客户端发送一个TCP的SYN标志位置1的包指明客户打算连接的服务器的端口，以及初始序号X,保存在包头的序列号(Sequence Number)字段里。



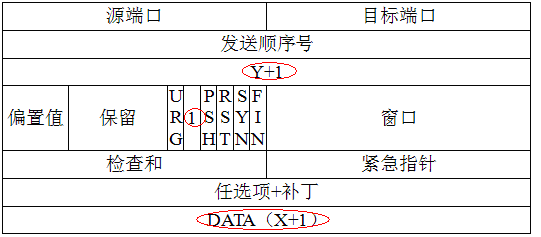
第二次握手:

服务器发回确认包(ACK)应答。即SYN标志位和ACK标志位均为1同时，将确认序号(Acknowledgement Number)设置为客户的I S N加以1.即X+1。



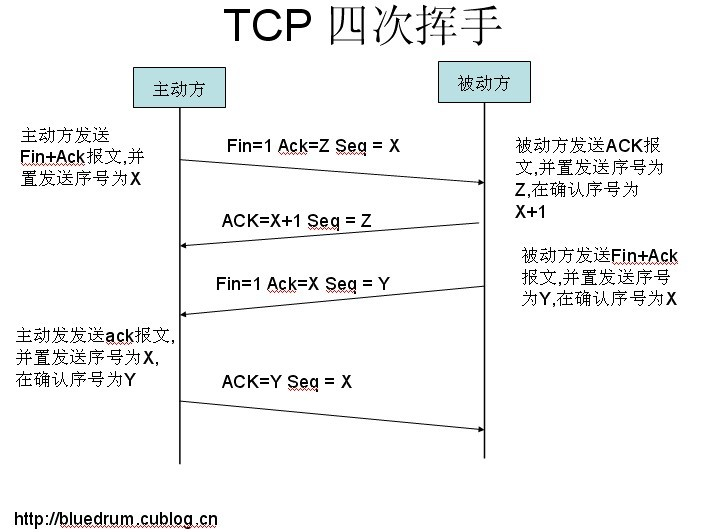
第三次握手.

客户端再次发送确认包(ACK) SYN标志位为0,ACK标志位为1.并且把服务器发来ACK的序号字段+1,放在确定字段中发送给对方.并且在数据段放写ISN的+1.

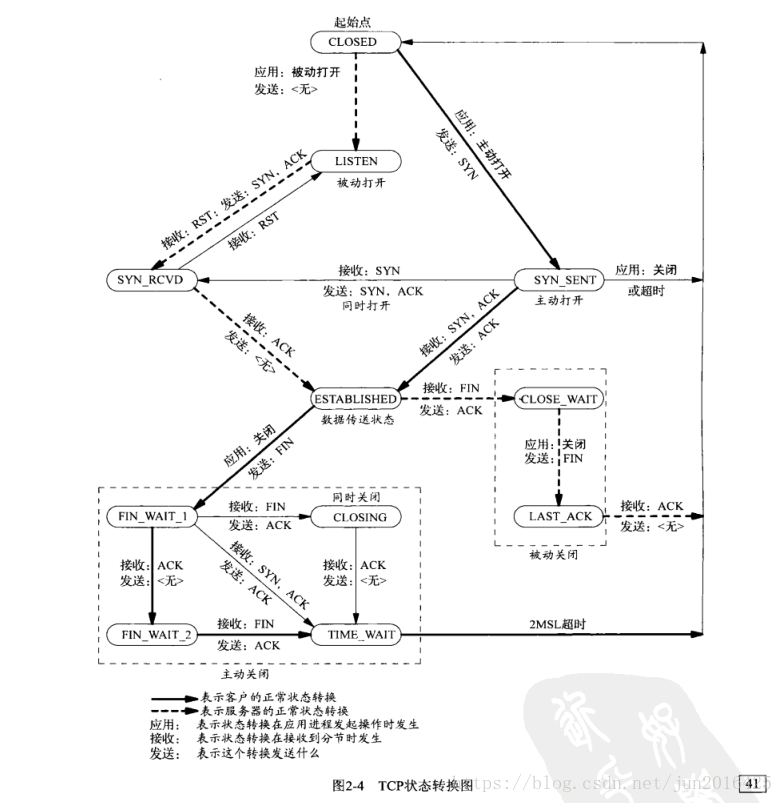


B.TCP 四次挥手

TCP的连接的拆除需要发送四个包，因此称为四次挥手(four-way handshake)。客户端或服务器均可主动发起挥手动作，在socket编程中，任何一方执行close()操作即可产生挥手操作。



C. TCP三次握手会涉及TCP的状态转换图如下



**【实验设备】**

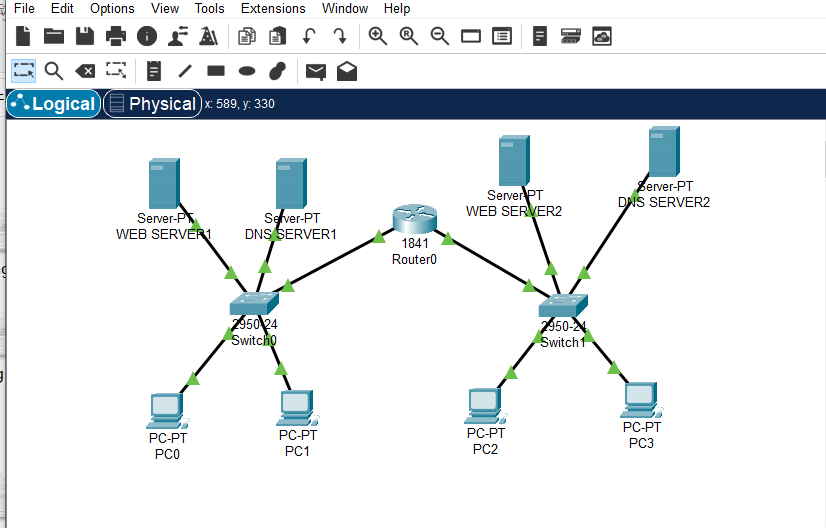
个人笔记本电脑、Cisco Packet Tracer实验软件。

**【实验步骤】**

1. 规划网络地址及拓扑图；
2. 配置Web Server和DNS Server
3. 配置各个PC
4. 打开PC0浏览器，输入配置Web服务器的Web地址，产生TCP数据报文
5. 观察TCP数据报文
6. 分析PT软件中的TCP报文
7. WireShark抓取TCP报文
8. 分析WireShark抓取的报文信息

**【实验现象】**

1. 规划网络地址及拓扑图；

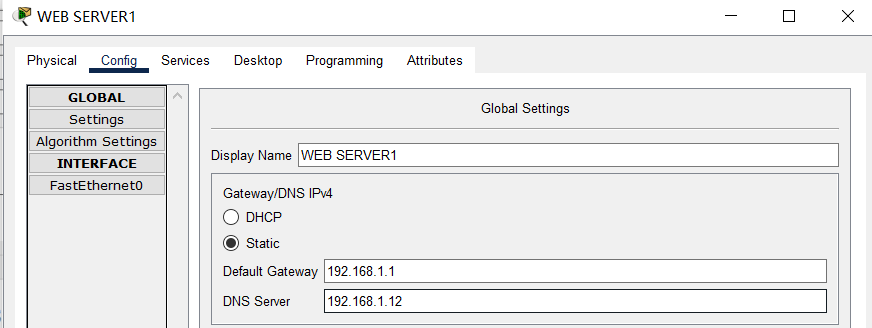


1. 配置Web Server和DNS Server

配置WEB SERVER1的网关及DNS服务器地址：

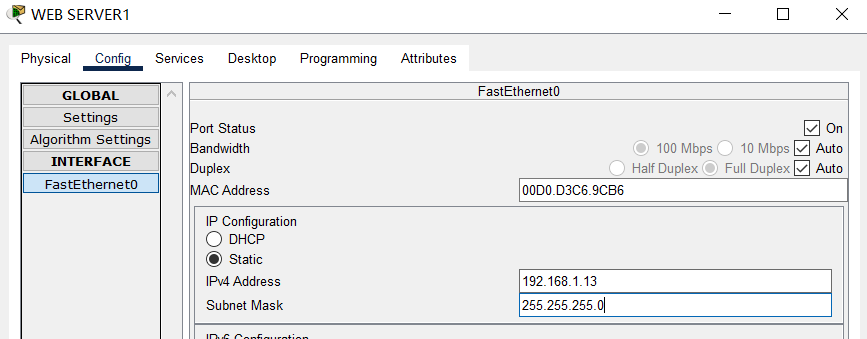
网关：192.168.1.1

DNS：192.168.1.12



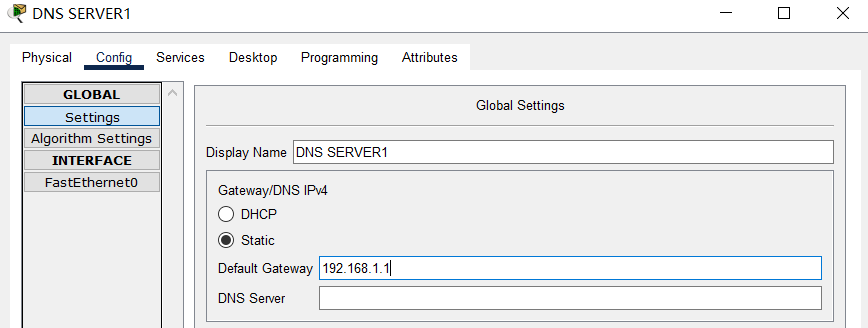
配置WEB SERVER1的地址：

IP：192.168.1.13



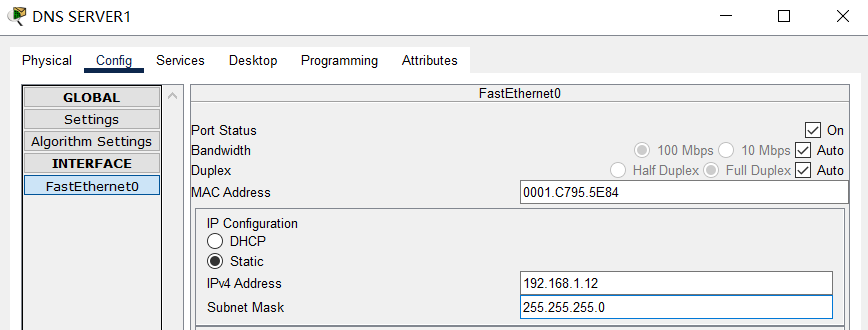
配置DNS SERVER1的网关：

网关：192.168.1.1



配置DNS SERVER1的地址：

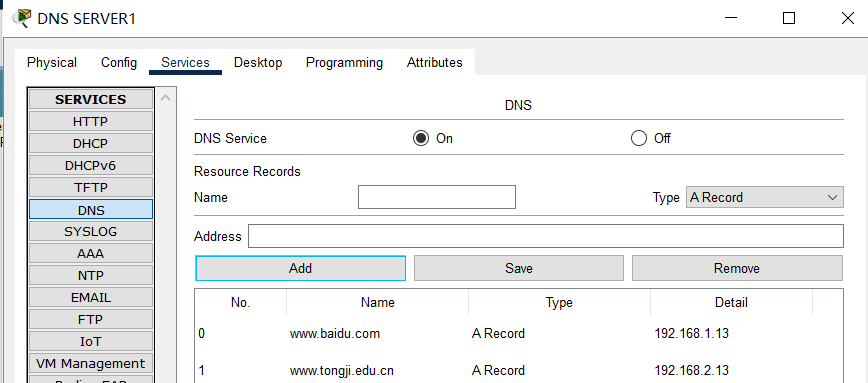
IP：192.168.1.12



在DNS SERVER1添加name和ip的映射：

name：[www.baidu.com](http://www.baidu.com) ip：192.168.1.13

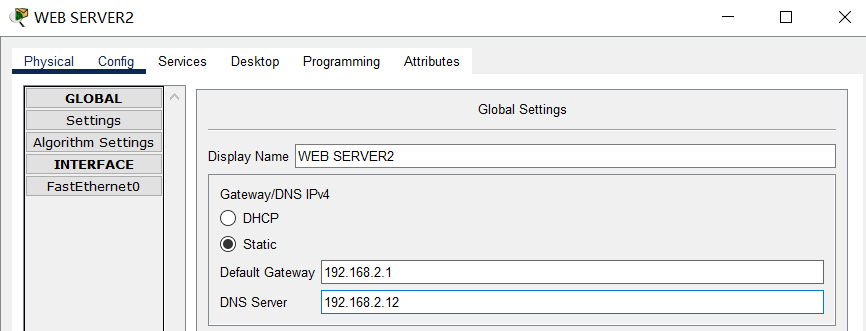
name：[www.](http://www.baidu.com)tongji.edu.cn ip：192.168.2.13



配置WEB SERVER2的网关及DNS服务器地址：

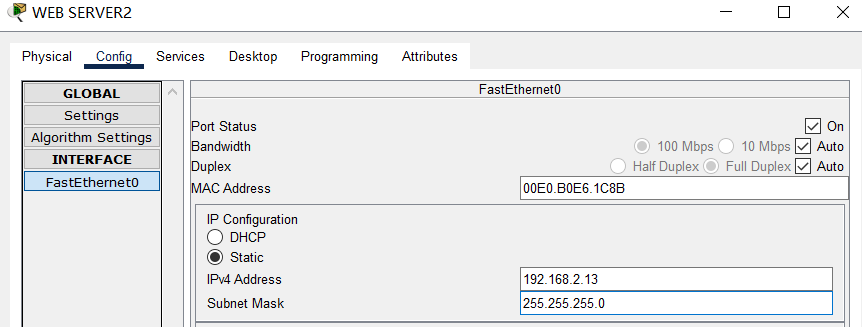
网关：192.168.2.1

DNS：192.168.2.12



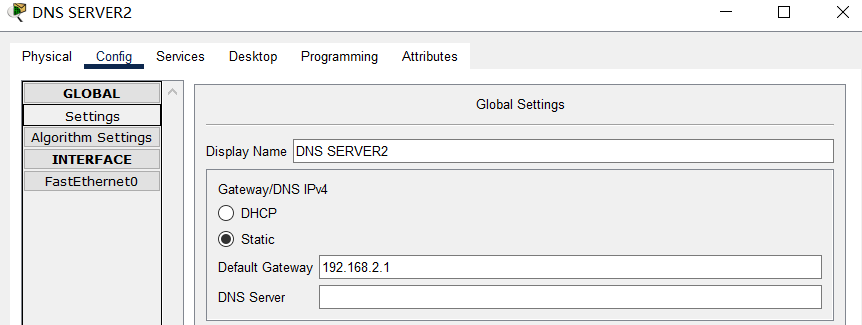
配置WEB SERVER2的地址：

IP：192.168.2.13



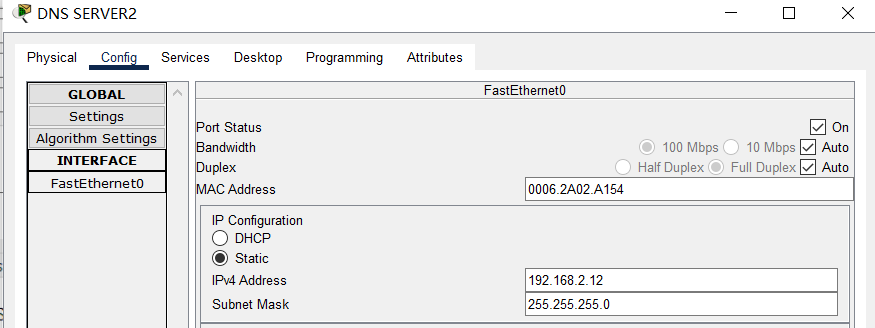
配置DNS SERVER2的网关：

网关：192.168.2.1



配置DNS SERVER2的地址：

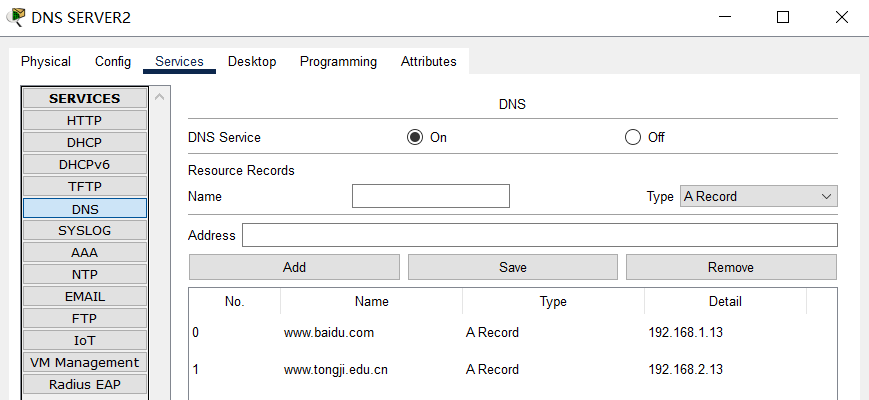
IP：192.168.2.12



在DNS SERVER2添加name和ip的映射：

name：[www.baidu.com](http://www.baidu.com) ip：192.168.1.13

name：[www.](http://www.baidu.com)tongji.edu.cn ip：192.168.2.13



1. 配置各个PC

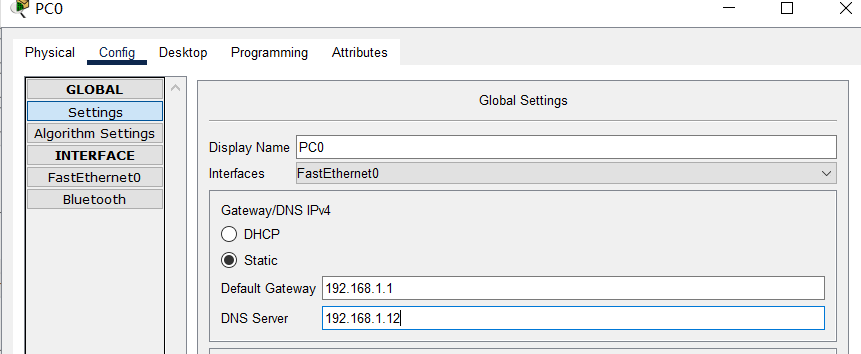
配置PC0-PC3的DNS服务器地址、网关、IP：

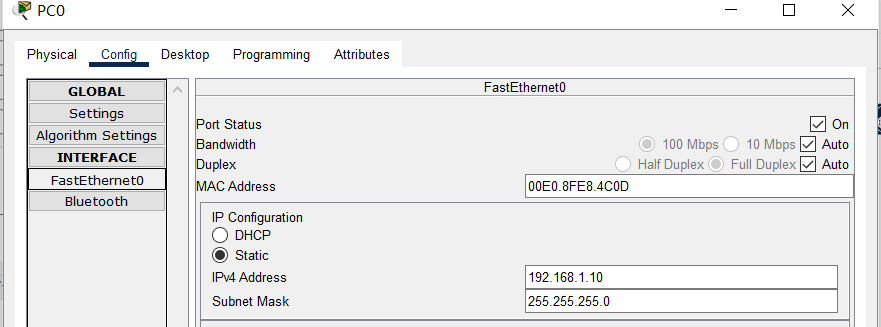
PC0:

网关：192.168.1.1

DNS服务器：192.168.1.12

IP：192.168.1.10



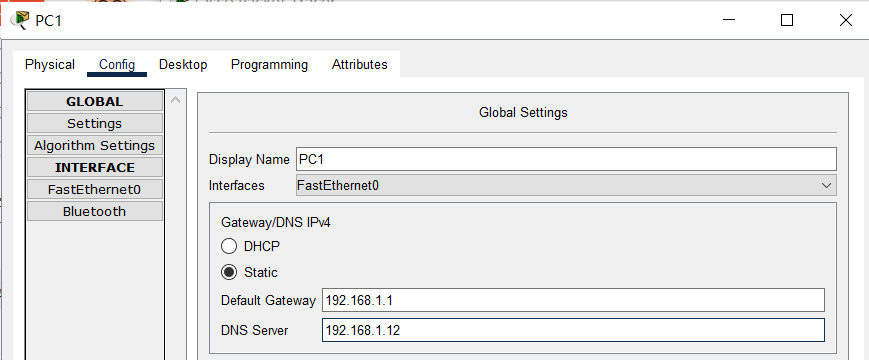


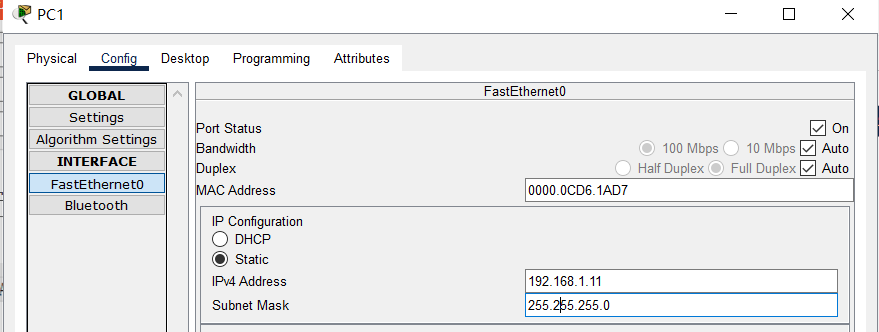
PC1:

网关：192.168.1.1

DNS服务器：192.168.1.12

IP：192.168.1.11



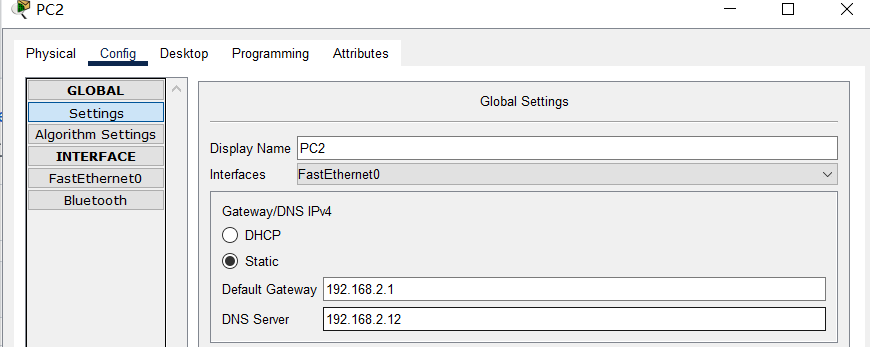


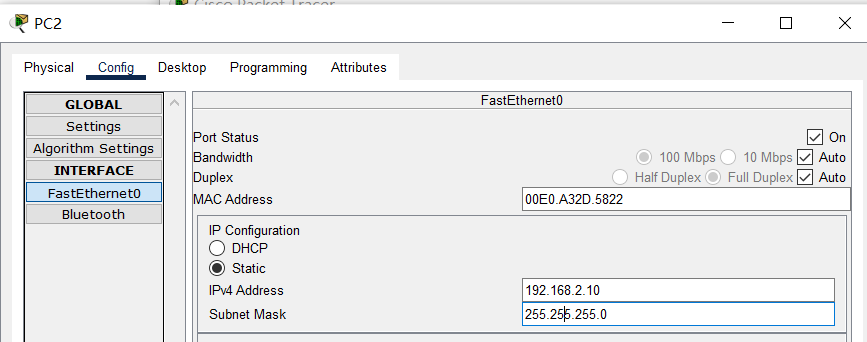
PC2:

网关：192.168.2.1

DNS服务器：192.168.2.12

IP：192.168.2.10



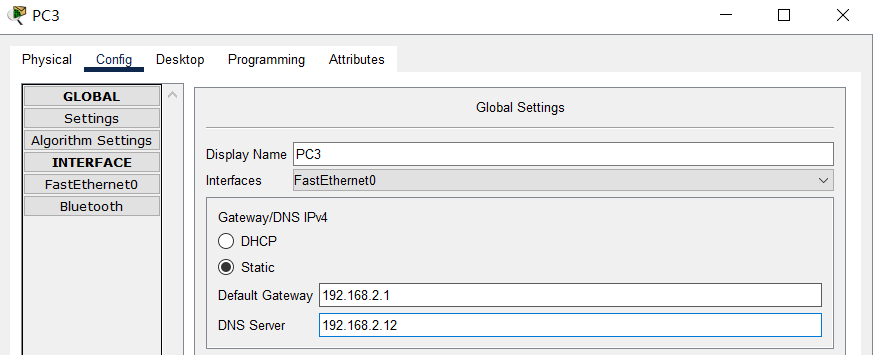


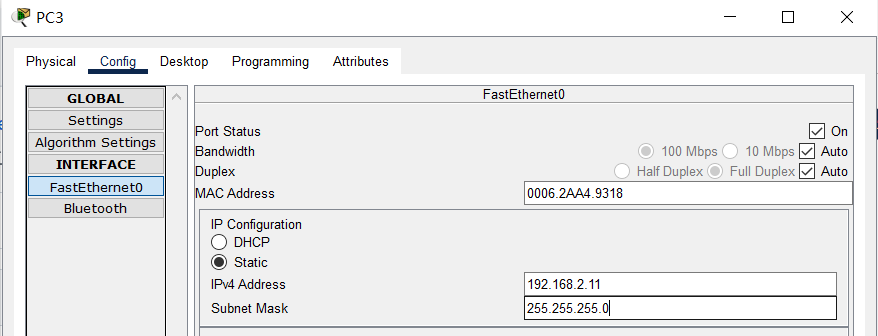
PC3:

网关：192.168.2.1

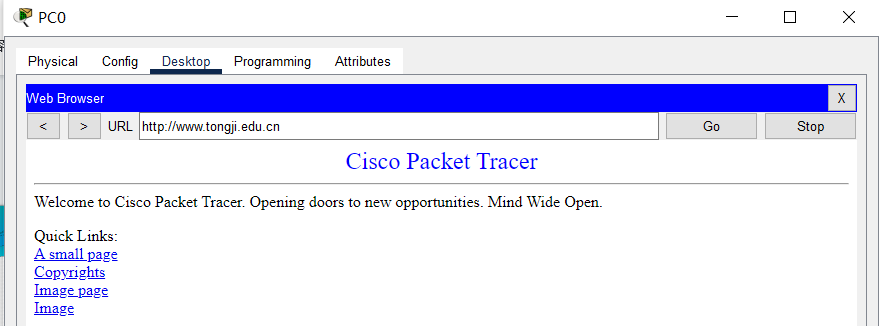
DNS服务器：192.168.2.12

IP：192.168.2.11

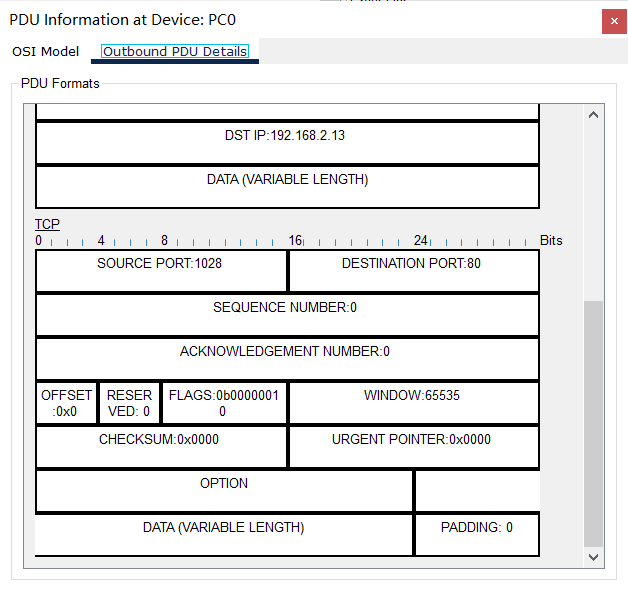




1. 打开PC0浏览器，输入配置Web服务器的Web地址，产生TCP数据报文

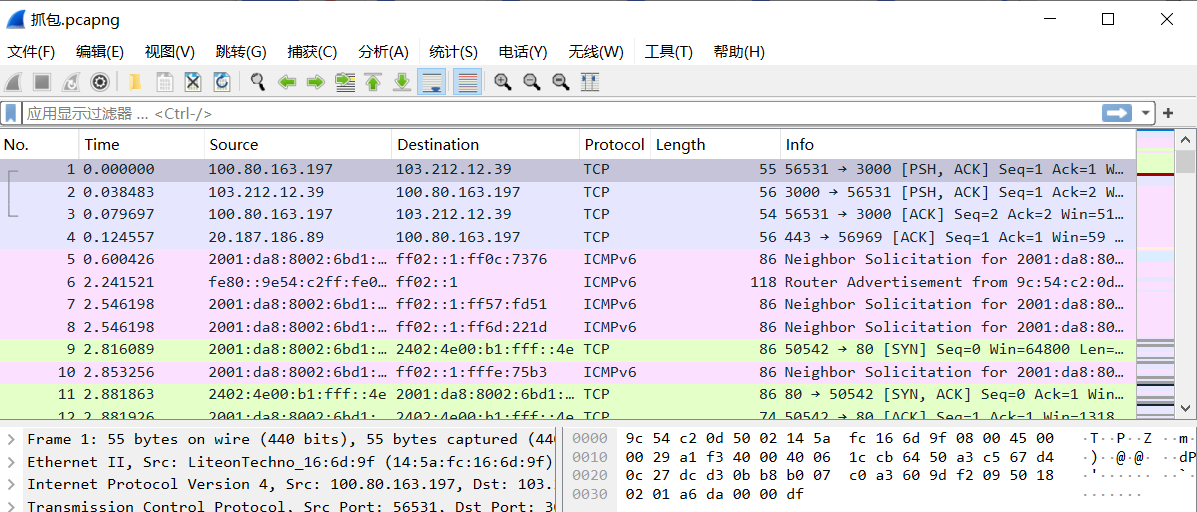


1. 观察TCP数据报文



（在分析与讨论中进行详细分析）

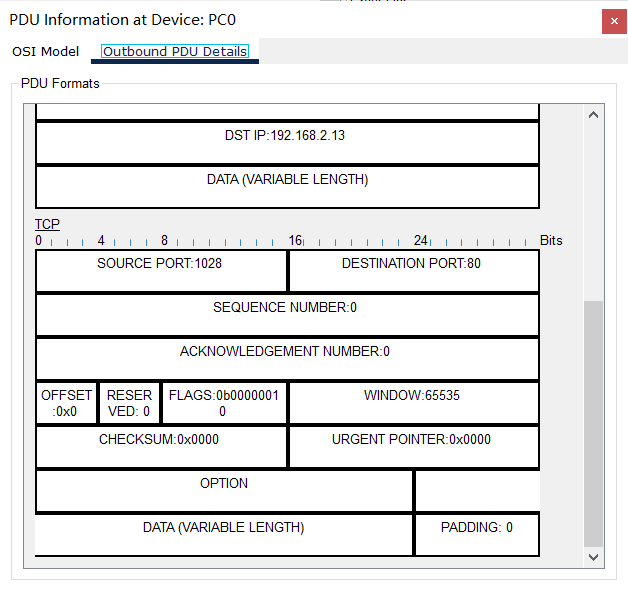
1. WireShark抓取TCP报文



**【分析讨论】**

1. **分析在Packet tracer中TCP报文情况；**

我们以PT软件中捕获的一个报文为例



在该报文中：

源端口号为1028

目标端口为80

初始序号为0

接收顺序号为0

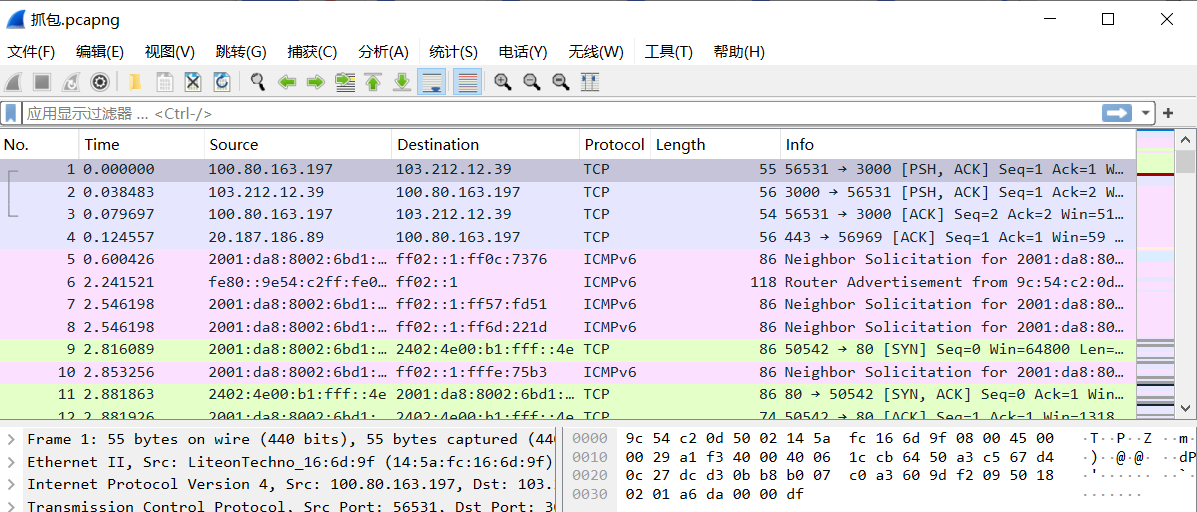
偏置为0

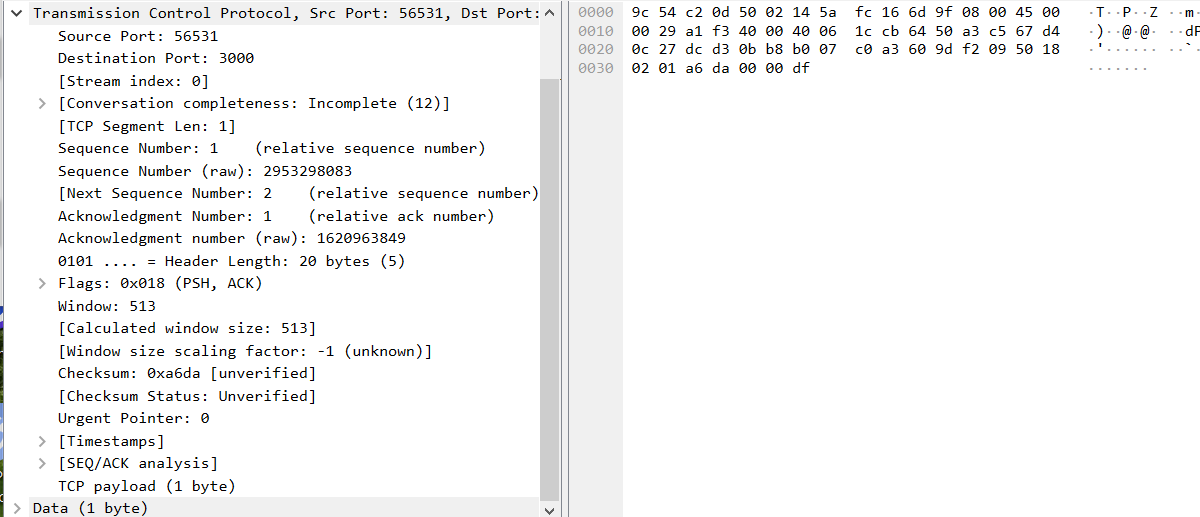
SYN标志为1，表明客户端希望连接服务器端口(第一次握手)

窗口为65535

其余字段均为0

1. **查看WireShark抓取的TCP报文字段内容，并解读；**





在这个TCP报文例子中：

源端口为56531

目标端口为3000

发送顺序号为1

接收顺序号为1

在标志位中，Acknowledgement为1表示接收确认序号有效，Push标志位为1表示指示接收方在接收到该报文段以后，应尽快将这个报文段交给应用程序，而不是在缓冲区排队。

窗口大小为513，用来告知发送端，接收端的缓存窗口大小为513

检查和为0xa6da

1. **仔细研读TCP连接建立过程数据报文；**

这里使用PT软件中的TCP报文进行分析。

在分析之前再次回顾TCP报文段重要字段的内容

**序号**：表示发送的数据字节流，确保TCP传输有序，对每个字节编号

**确认序号**：发送方期待接收的下一序列号，接收成功后的数据字节序列号加 1。只有ACK=1时才有效。

**ACK**：确认序号的标志，ACK=1表示确认号有效，ACK=0表示报文不含确认序号信息

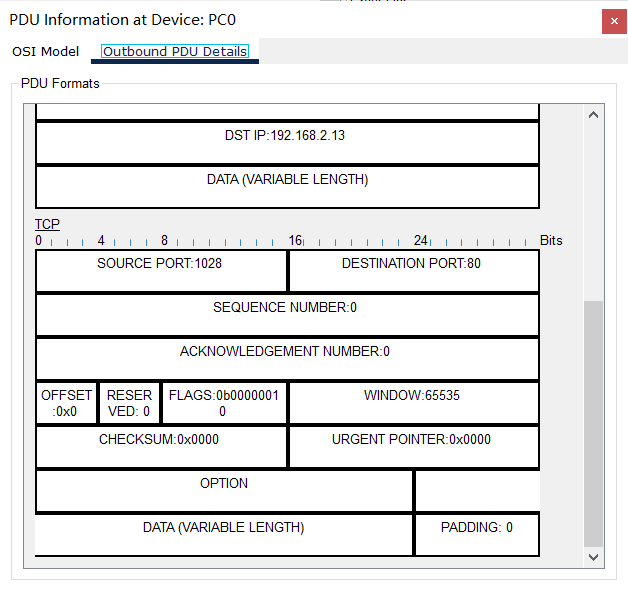
**SYN**：连接请求序号标志，用于建立连接，SYN=1表示请求连接

**FIN**：结束标志，用于释放连接，为1表示关闭本方数据流

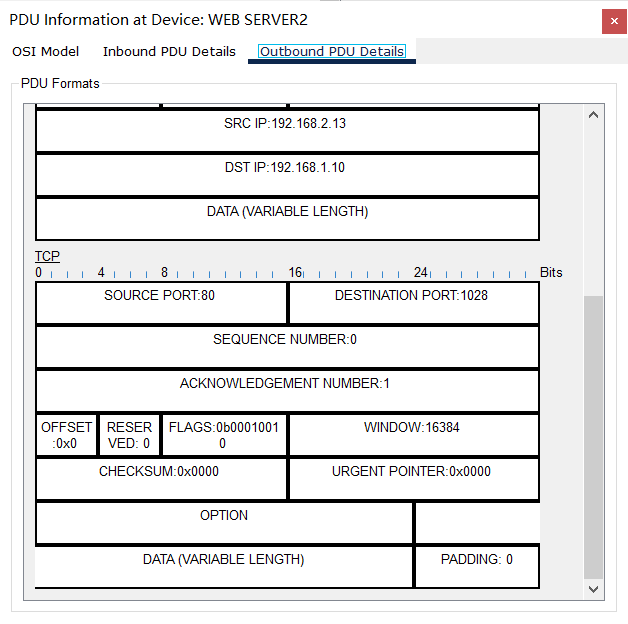
打开PC0的Web Browser

使用PT的仿真（simulation）模式

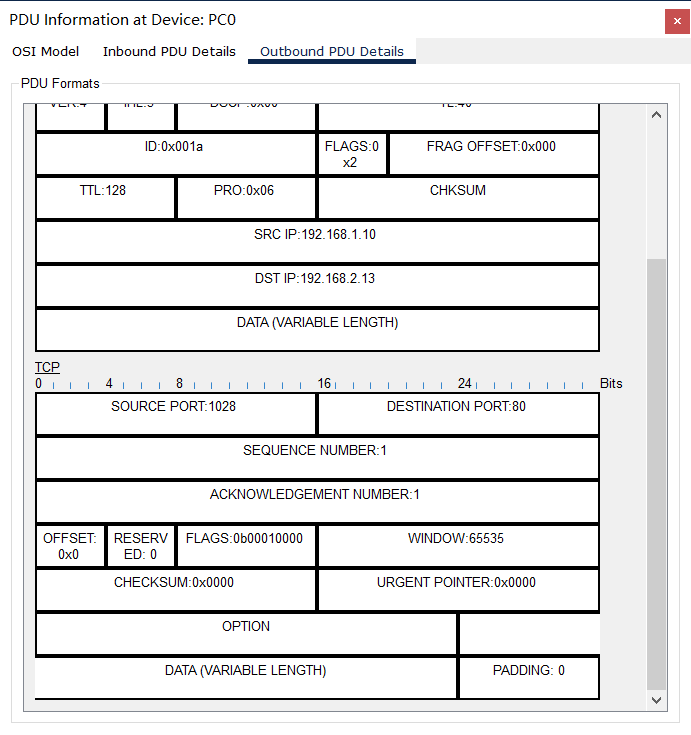
输入网址http://www.tongji.edu.cn点击go，此时产生一个TCP数据包



第一次握手，PC0发送了一个SYN位为1的包，表明PC0打算与服务器建立连接，发送序列号X为0

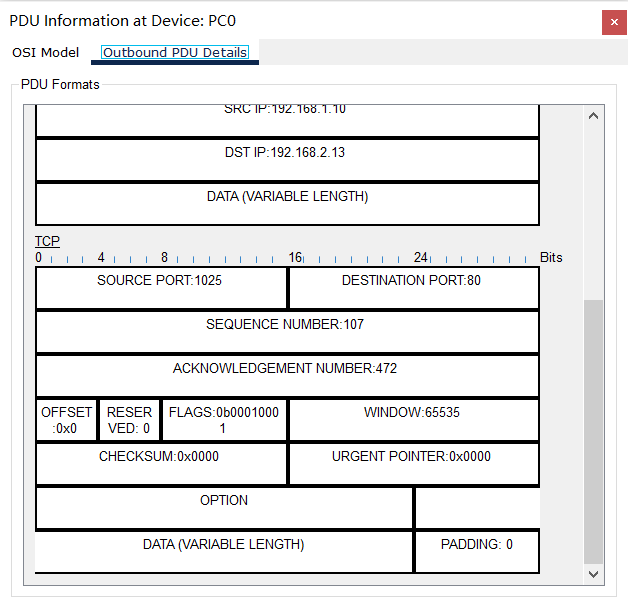


这是服务器收到P0的包后向PC0发送的TCP报文。在这个报文中，接受序列号为X+1，即为1，接受序列号Y为0.标识位中，SYN和ACK为都被置为1。

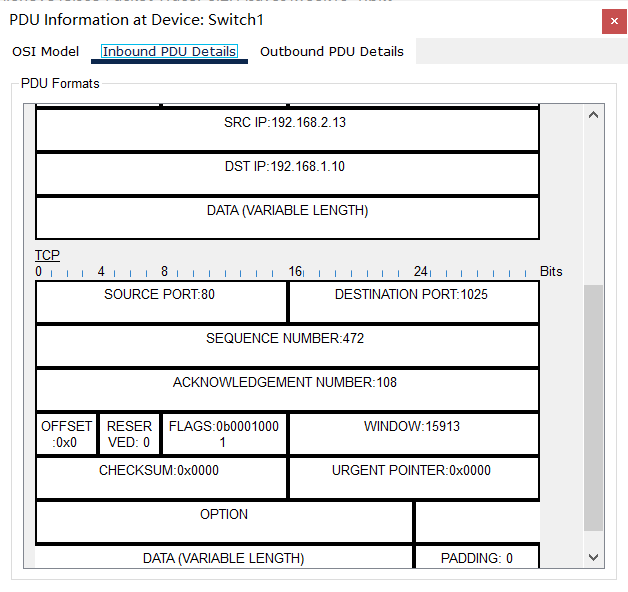


该包为第三次握手，由PC0向服务器发送的数据包，接收顺序号为Y+1即为1，标识位中只有ACK被置为1

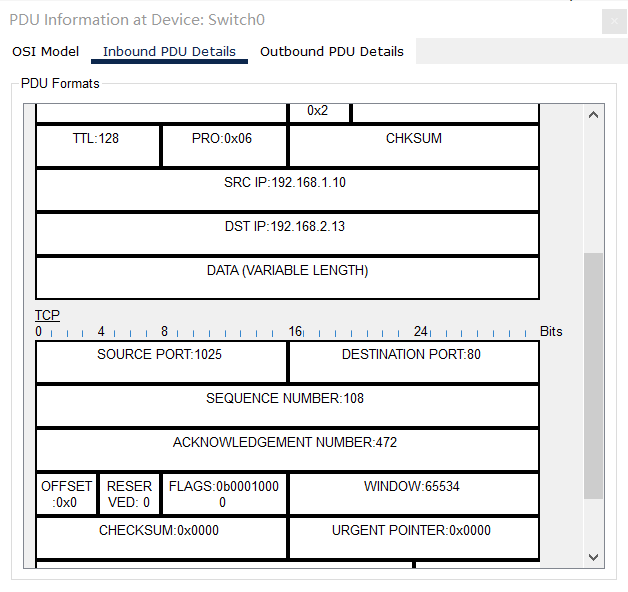
1. **仔细研读TCP拆链过程数据报文；**



第一次挥手，PC0为主动方，发送Fin+Ack报文，将标识位中这两位置为1，发送序号X为107，接受序号Z为472.



第二次和第三次挥手，这个地方十分重要。这里我一开始很奇怪，不是四次挥手吗，怎么服务器只发了一个包。后来上网查询得知，这里把四次挥手简化为了三次挥手，第二次和第三次挥手合成了一个包，接受序列号为X+1即108，发送序列号为Y即472，并且Fin和Ack位都置为了1。



第四次挥手，主动方即PC0发送ACK报文，置发送序列号为X=108，接收序列号为Y=472.

完成拆链过程。

**【实验名称】：UDP用户数据报分析实验**

**学生姓名：陈嘉瑞 合作学生： 无**

**实验地点：济事楼330网络实验室 实验时间：2023年12月4日**

**【实验目的】**

1. 了解UDP协议
2. 掌握使用WireShark抓取UDP报文的方法
3. 掌握分析UDP报文的方法

**【实验原理】**

1. UDP概述

UDP是传输层的协议，功能即为在IP的数据报服务之上增加了最基本的服务：复用和分用以及差错检测。

UDP提供不可靠服务，具有TCP所没有的优势：

UDP无连接，时间上不存在建立连接需要的时延。空间上，TCP需要在端系统中维护连接状态，需要一定的开销。此连接装入包括接收和发送缓存，拥塞控制参数和序号与确认号的参数。UCP不维护连接状态，也不跟踪这些参数，开销小。空间和时间上都具有优势。

1. UDP应用特点

DNS如果运行在TCP之上而不是UDP，那么DNS的速度将会慢很多。HTTP使用TCP而不是UDP，是因为对于基于文本数据的Web网页来说，可靠性很重要。同一种专用应用服务器在支持UDP时，一定能支持更多的活动客户机。分组首部开销小，TCP首部20字节，UDP首部8字节。

UDP没有拥塞控制，应用层能够更好的控制要发送的数据和发送时间，网络中的拥塞控制也不会影响主机的发送速率。某些实时应用要求以稳定的速度发送，能容 忍一些数据的丢失，但是不能允许有较大的时延（比如实时视频，直播等）

UDP提供尽最大努力的交付，不保证可靠交付。所有维护传输可靠性的工作需要用户在应用层来完成。没有TCP的确认机制、重传机制。如果因为网络原因没有传送到对端，UDP也不会给应用层返回错误信息。

UDP是面向报文的，对应用层交下来的报文，添加首部后直接乡下交付为IP层，既不合并，也不拆分，保留这些报文的边界。对IP层交上来UDP用户数据报，在去除首部后就原封不动地交付给上层应用进程，报文不可分割，是UDP数据报处理的最小单位。正是如此UDP显得不够灵活，不能控制读写数据的次数和数量。比如我们要发送100个字节的报文，调用一次sendto函数就会发送100字节，对端也需要用recvfrom函数一次性接收100字节，不能使用循环每次获取10个字节，获取十次这样的做法。

UDP常用一次性传输比较少量数据的网络应用，如DNS,SNMP等，因为对于这些应用，若是采用TCP，为连接的创建，维护和拆除带来不小的开销。UDP也常用于多媒体应用（如IP电话，实时视频会议，流媒体等）数据的可靠传输对他们而言并不重要，TCP的拥塞控制会使它们有较大的延迟，也是不可容忍的。总之，UDP协议提供不可靠无连接的数据报传输服务。

1. UDP报文格式

UDP的首部格式

UDP数据报分为首部和用户数据部分，整个UDP数据报作为IP数据报的数据部分封装在IP数据报中，UDP数据报文结构如图所示：



UDP首部有8个字节，由4个字段构成，每个字段都是两个字节，1).源端口： 源端口号，需要对方回信时选用，不需要时全部置0.

2).目的端口：目的端口号，在终点交付报文的时候需要用到。

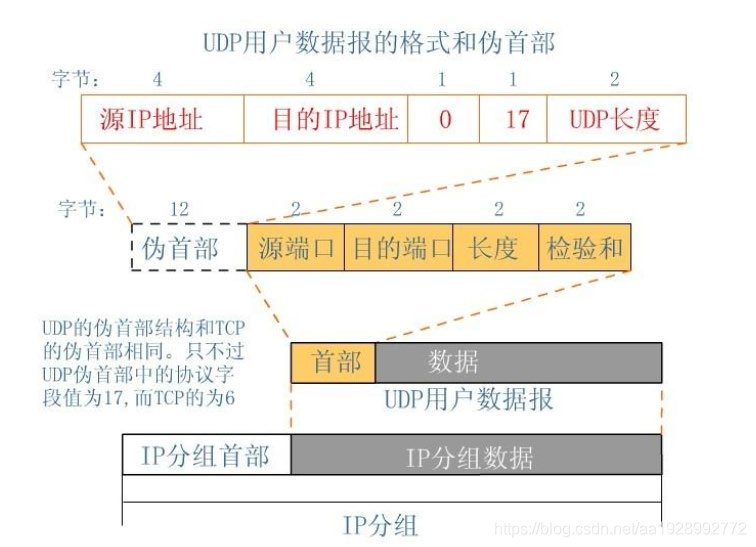
3).长度：UDP的数据报的长度（包括首部和数据）其最小值为8（只有首部）

4).校验和：检测UDP数据报在传输中是否有错，有错则丢弃。该字段是可选的，当源主机不想计算校验和，则直接令该字段全为0。当传输层从IP层收到UDP数据报时，就根据首部中的目的端口，把UDP数据报通过相应的端口，上交给应用进程。如果接收方UDP发现收到的报文中的目的端口号不正确（不存在对应端口号的应用进程0,），就丢弃该报文，并由ICMP发送“端口不可达”差错报文给对方。

UDP校验

在计算校验和的时候，需要在UDP数据报之前增加12字节的伪首部，伪首部并不是UDP真正的首部。只是在计算校验和，临时添加在UDP数据报的前面，得到一个临时的UDP数据报。校验和就是按照这个临时的UDP数据报计算的。伪首部既不向下传送也不向上递交，而仅仅是为了计算校验和。这样的校验和，既检查了UDP数据报，又对IP数据报的源IP地址和目的IP地址进行了检验。

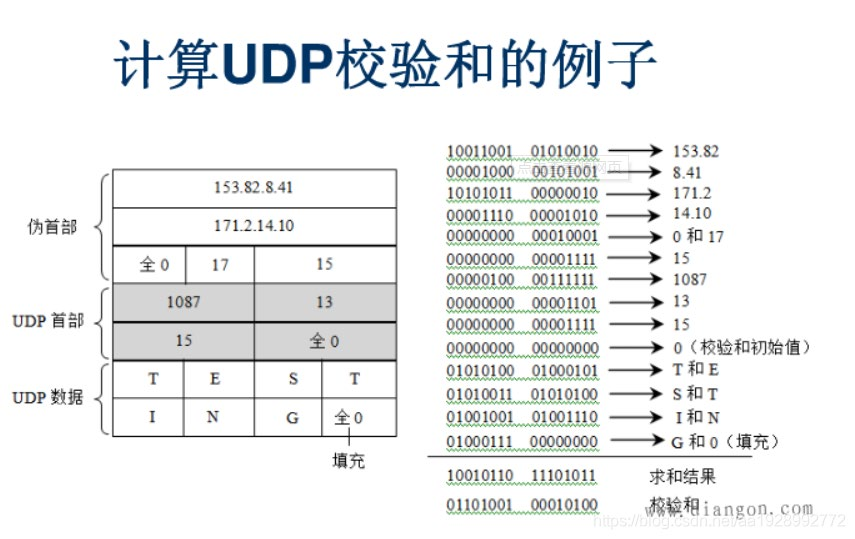
UDP校验和的计算方法和IP数据报首部校验和的计算方法相似，都使用二进制反码运算求和再取反，但不同的是：IP数据报的校验和只检验IP数据报的首部，但UDP的校验和是把首部和数据部分一起校验。



发送方，首先是把全零放入校验和字段并且添加伪首部，然后把UDP数据报看成是由许多16位的子串连接起来，若UDP数据报的数据部分不是偶数个字节，则要在数据部分末尾增加一个全零字节（此字节不发送），接下来就按照二进制反码计算出这些16位字的和。将此和的二进制反码写入校验和字段。在接收方，把收到得UDP数据报加上伪首部（如果不为偶数个字节，还需要补上全零字节）后，按二进制反码计算出这些16位字的和。

当无差错时其结果全为1,。否则就表明有差错出现，接收方应该丢弃这个UDP数据报。注意：

1. .校验时，若UDP数据报部分的长度不是偶数个字节，则需要填入一个全0字节，但是此字节和伪首部一样，是不发送的。
2. 2).如果UDP校验和校验出UDP数据报是错误的，可以丢弃，也可以交付上层，但是要附上错误报告，告诉上层这是错误的数据报。3).通过伪首部，不仅可以检查源端口号，目的端口号和UDP用户数据报的数据部分，还可以检查IP数据报的源IP地址和目的地址。这种差错检验的检错能力不强，但是简单，速度快。



**【实验设备】**

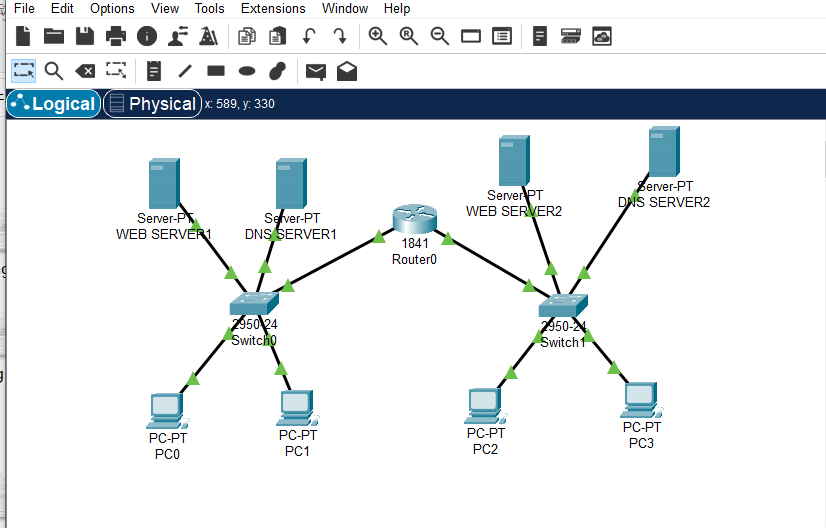
个人笔记本电脑、Cisco Packet Tracer实验软件。

**【实验步骤】**

1. 规划网络地址及拓扑图；
2. 配置Web Server和DNS Server
3. 配置各个PC
4. 打开PC0浏览器，输入配置Web服务器的Web地址，产生UDP数据报文
5. 观察UDP数据报文
6. 分析PT软件中的UDP报文
7. WireShark抓取UDP报文
8. 分析WireShark抓取的报文信息

**【实验现象】**

1. 规划网络地址及拓扑图；

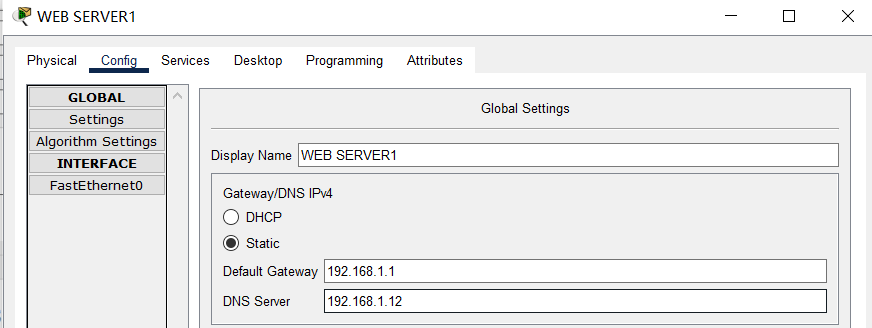


1. 配置Web Server和DNS Server

配置WEB SERVER1的网关及DNS服务器地址：

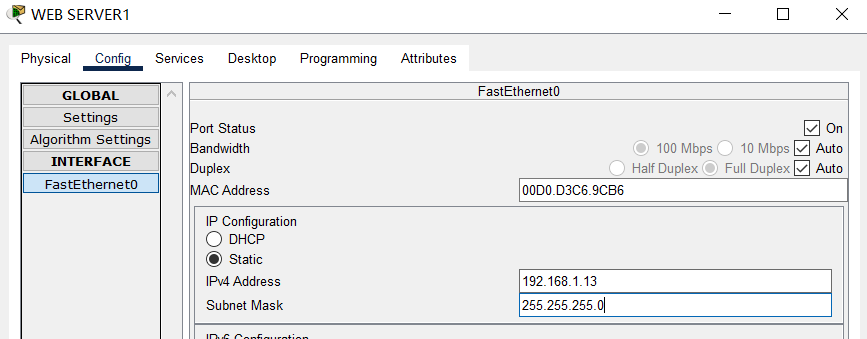
网关：192.168.1.1

DNS：192.168.1.12



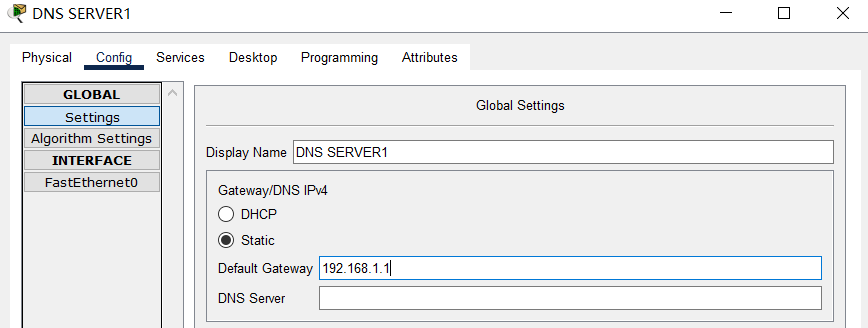
配置WEB SERVER1的地址：

IP：192.168.1.13



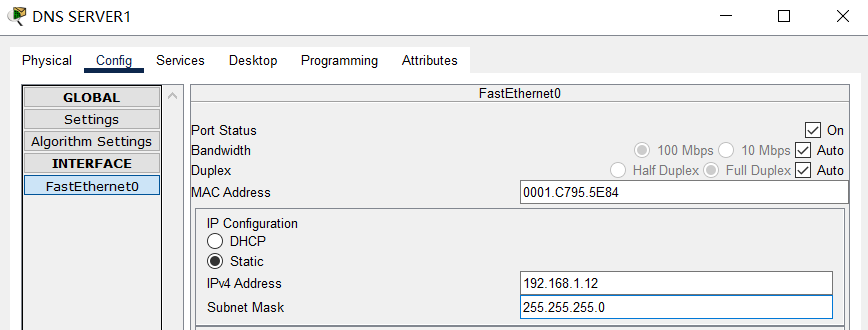
配置DNS SERVER1的网关：

网关：192.168.1.1



配置DNS SERVER1的地址：

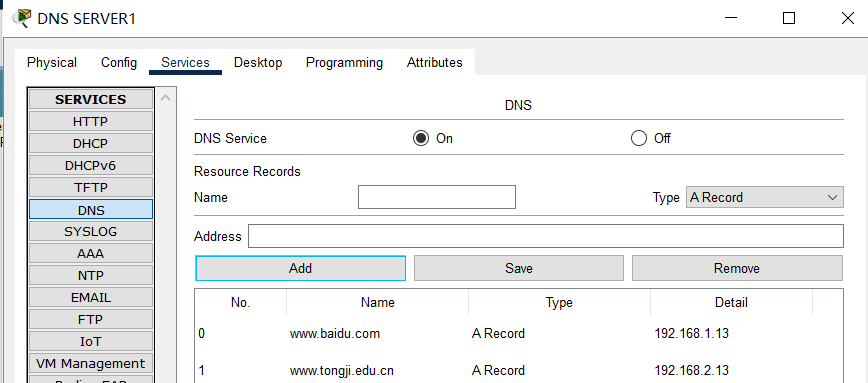
IP：192.168.1.12



在DNS SERVER1添加name和ip的映射：

name：[www.baidu.com](http://www.baidu.com) ip：192.168.1.13

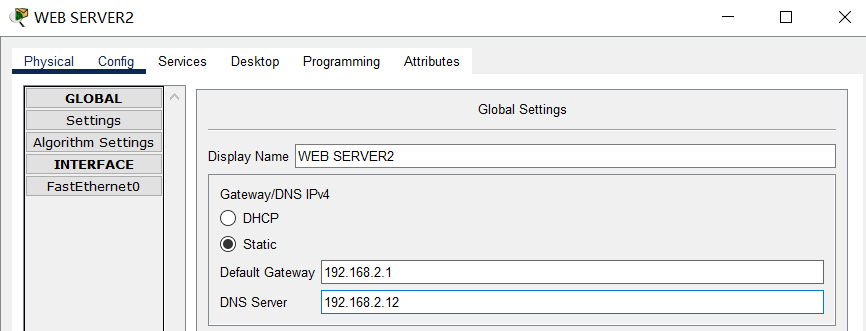
name：[www.](http://www.baidu.com)tongji.edu.cn ip：192.168.2.13



配置WEB SERVER2的网关及DNS服务器地址：

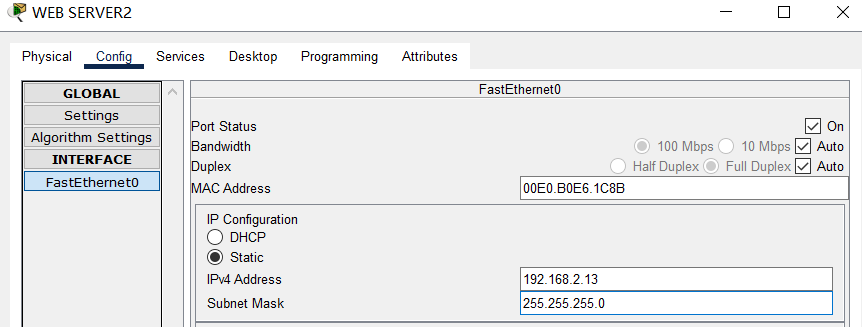
网关：192.168.2.1

DNS：192.168.2.12



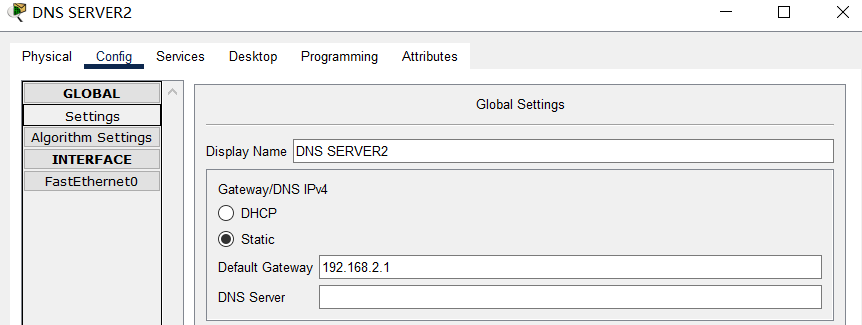
配置WEB SERVER2的地址：

IP：192.168.2.13



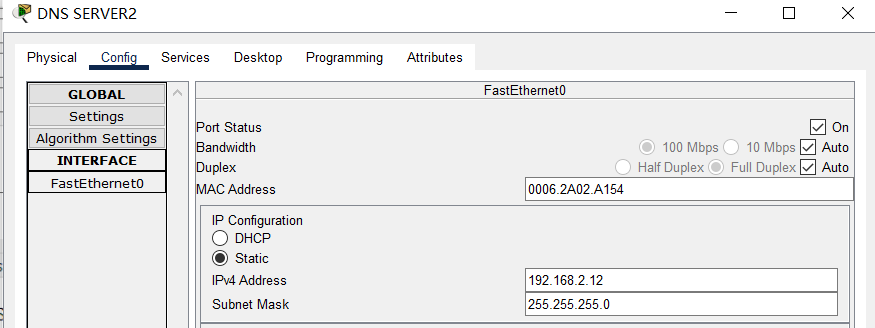
配置DNS SERVER2的网关：

网关：192.168.2.1



配置DNS SERVER2的地址：

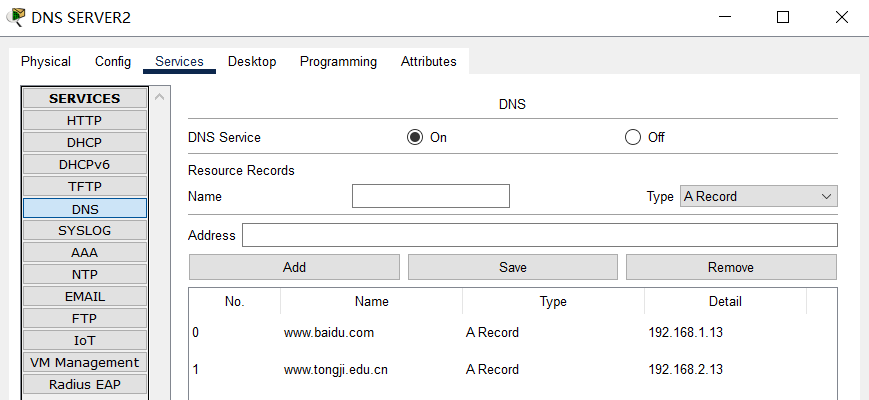
IP：192.168.2.12



在DNS SERVER2添加name和ip的映射：

name：[www.baidu.com](http://www.baidu.com) ip：192.168.1.13

name：[www.](http://www.baidu.com)tongji.edu.cn ip：192.168.2.13



1. 配置各个PC

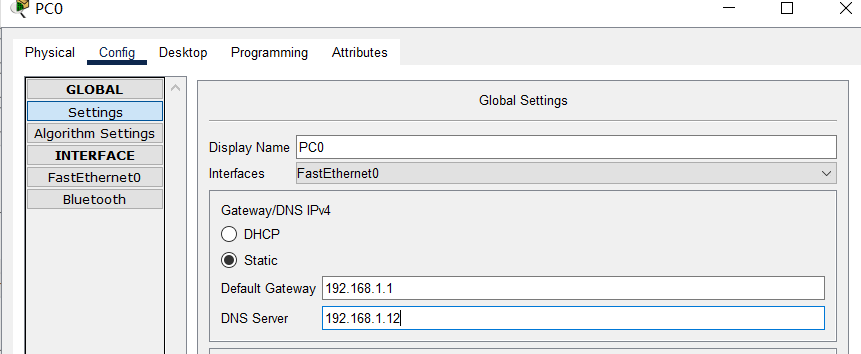
配置PC0-PC3的DNS服务器地址、网关、IP：

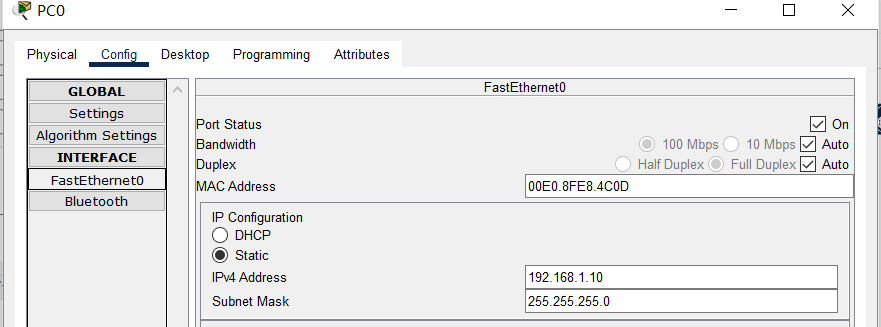
PC0:

网关：192.168.1.1

DNS服务器：192.168.1.12

IP：192.168.1.10



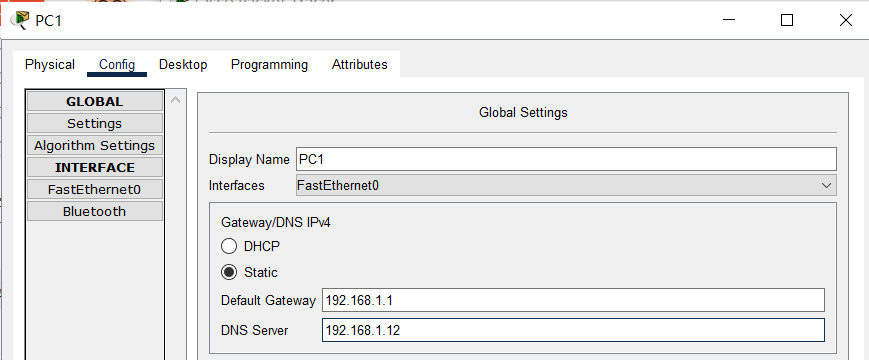


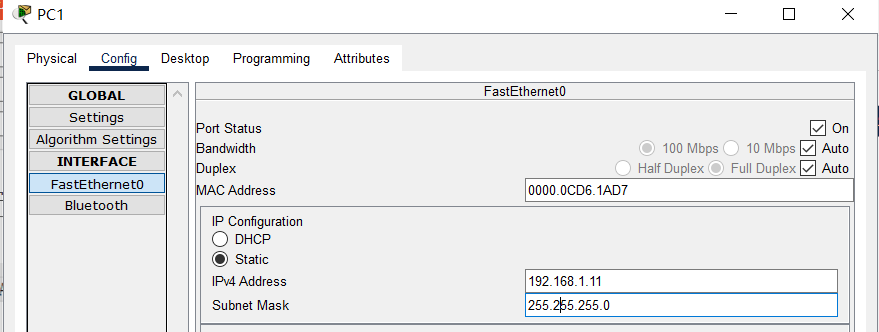
PC1:

网关：192.168.1.1

DNS服务器：192.168.1.12

IP：192.168.1.11



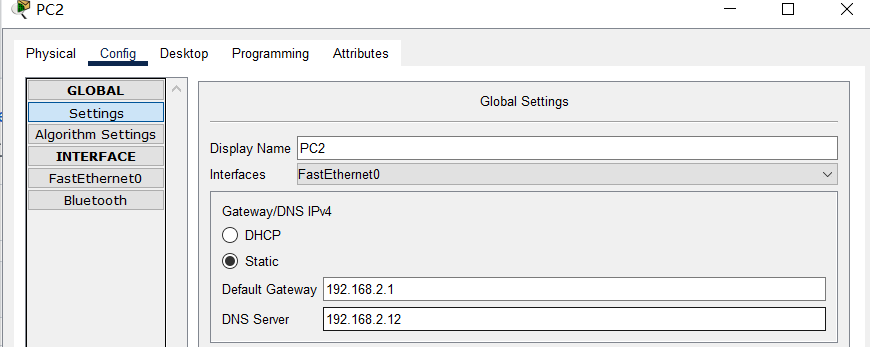


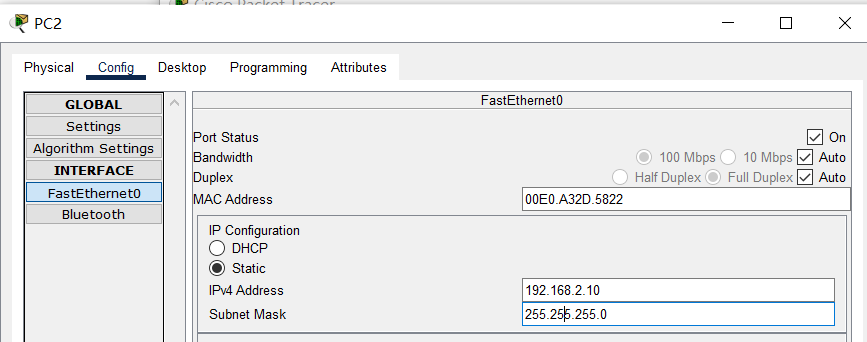
PC2:

网关：192.168.2.1

DNS服务器：192.168.2.12

IP：192.168.2.10



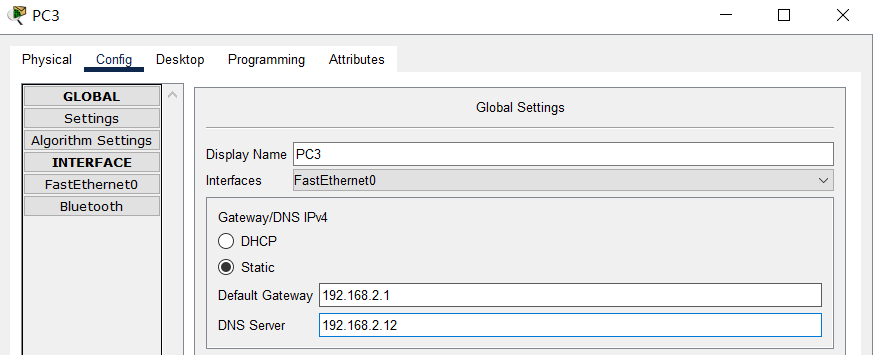


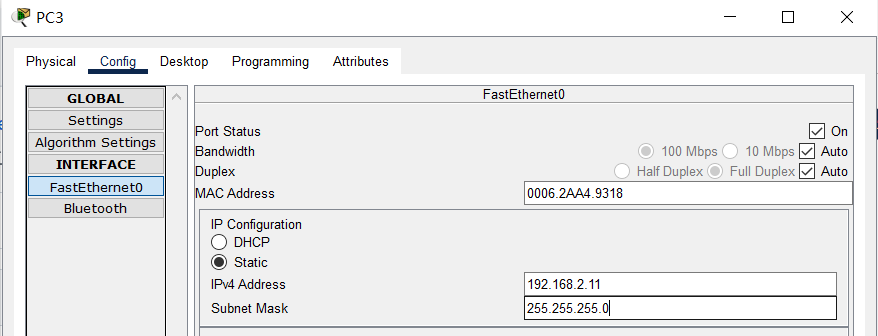
PC3:

网关：192.168.2.1

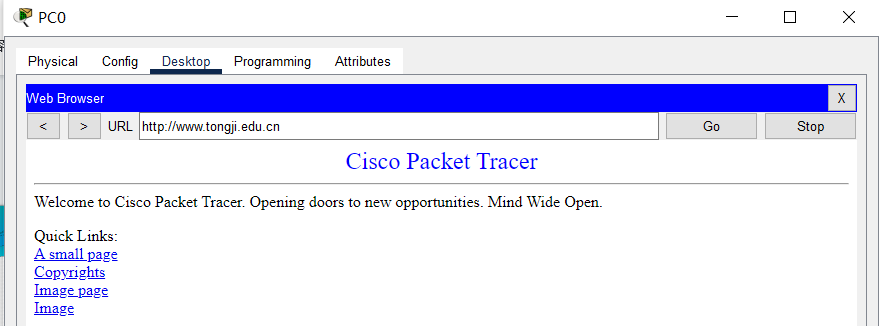
DNS服务器：192.168.2.12

IP：192.168.2.11

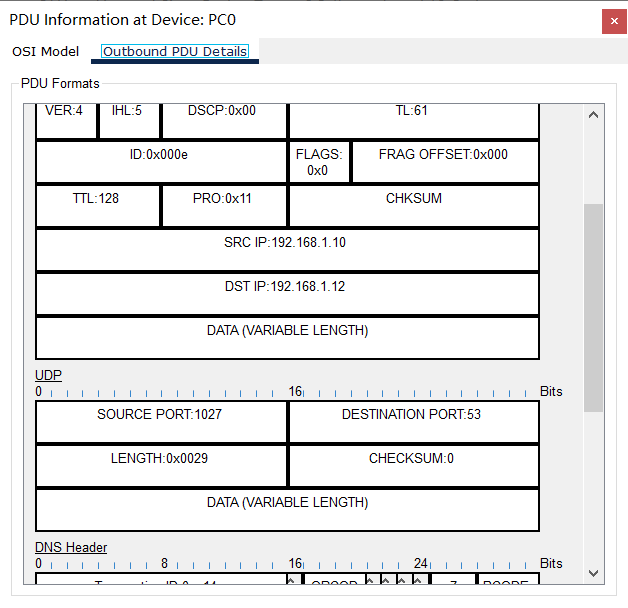




1. 打开PC0浏览器，输入配置Web服务器的Web地址，产生UDP数据报文

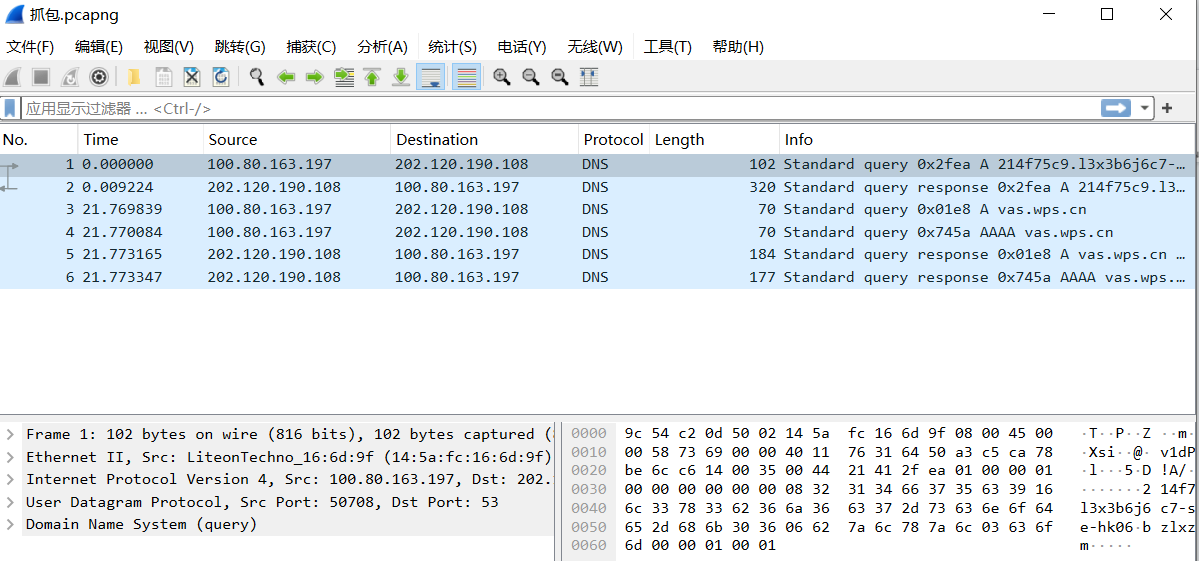


1. 观察UDP数据报文



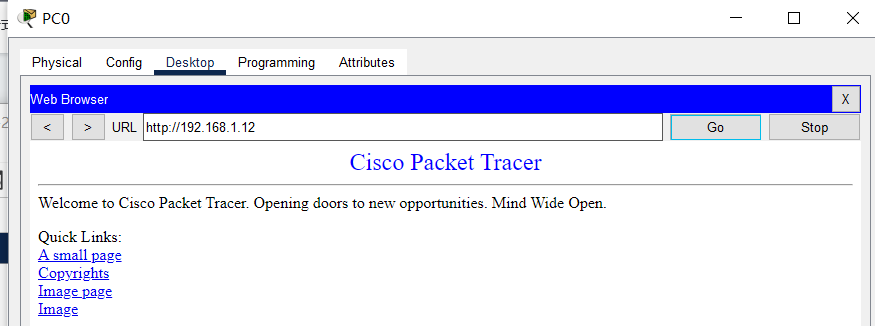
（在分析与讨论中进行详细分析）

1. WireShark抓取TCP报文



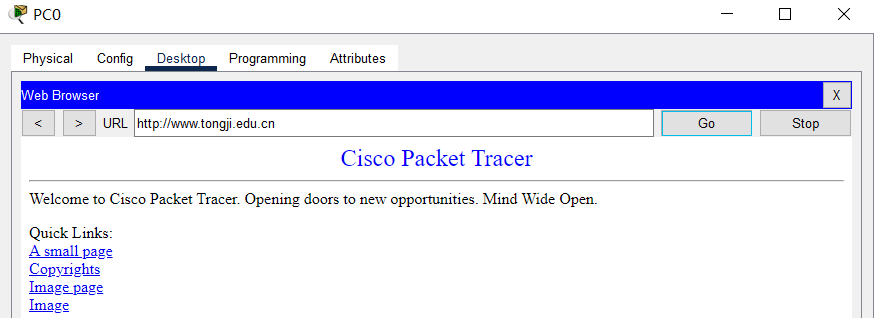
**【分析讨论】**

1. 配置Web服务器，并从客户端查看；



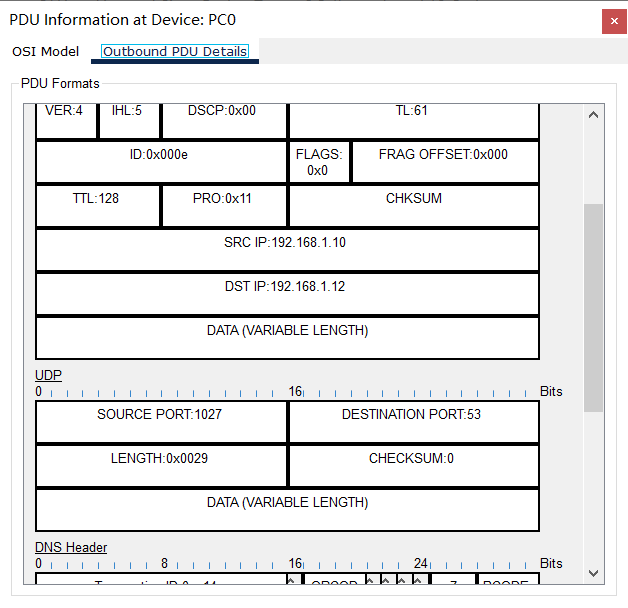
服务器配置已在前面介绍。打开PC0输入网址访问配置的服务器可以看到服务器访问正常

1. 配置DNS服务器；



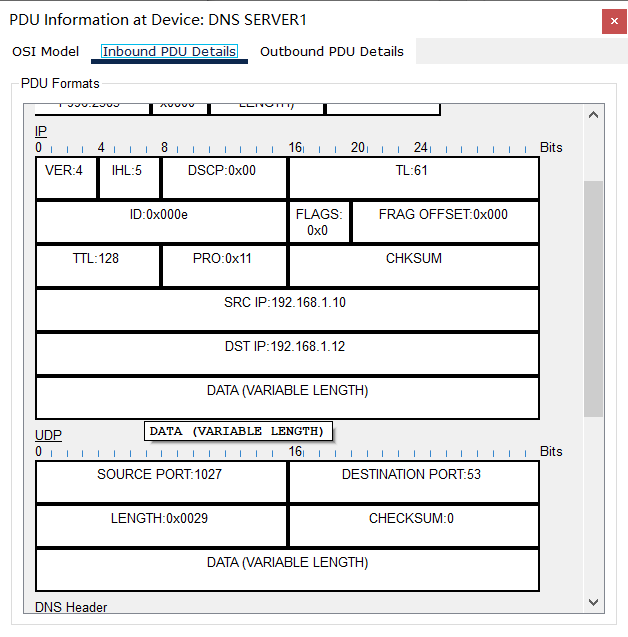
DNS服务器配置过程已在前面介绍，尝试从PC0以域名形式访问服务器，可以看到成功访问，说明DNS服务器配置正常

1. 分析在Packet tracer中UDP报文情况；

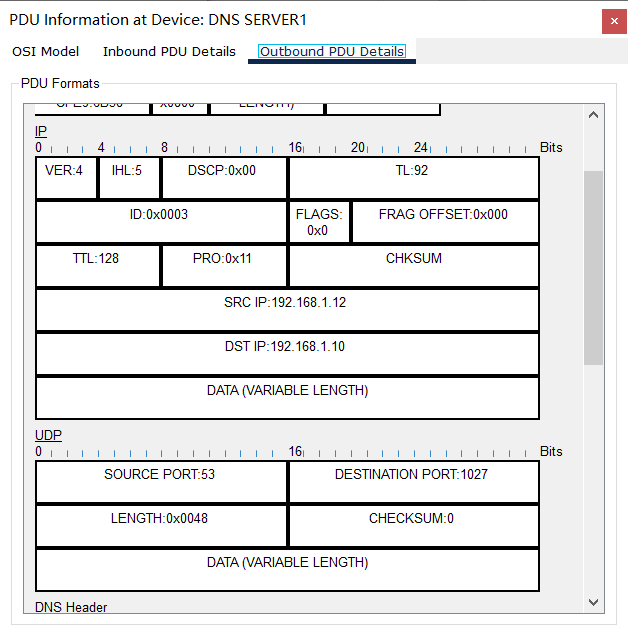


UDP数据报分为首部和用户数据部分。在这个例子中我们可以看到：

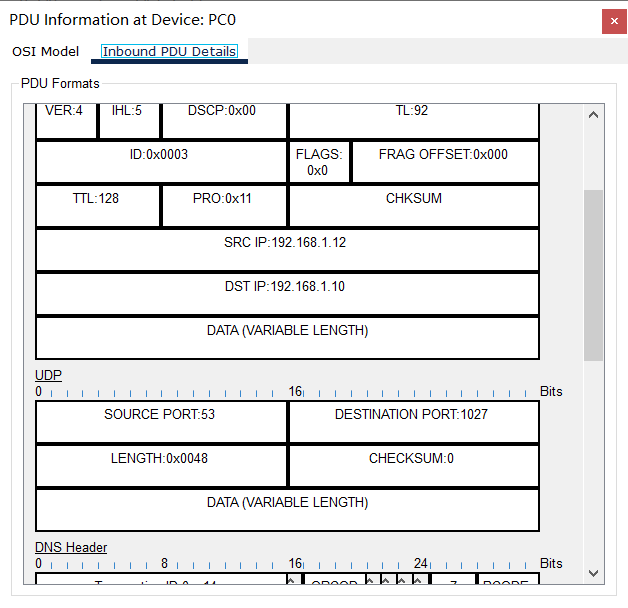
源端口号为1027，目的端口号为53，UDP数据报长度为0x0029即41（包括了首部和数据），校验和为0标识源主机不想计算校验和



这是DNS服务器接收的PC0发来的UDP报文，可以看到其内容和PC0发送时完全一致

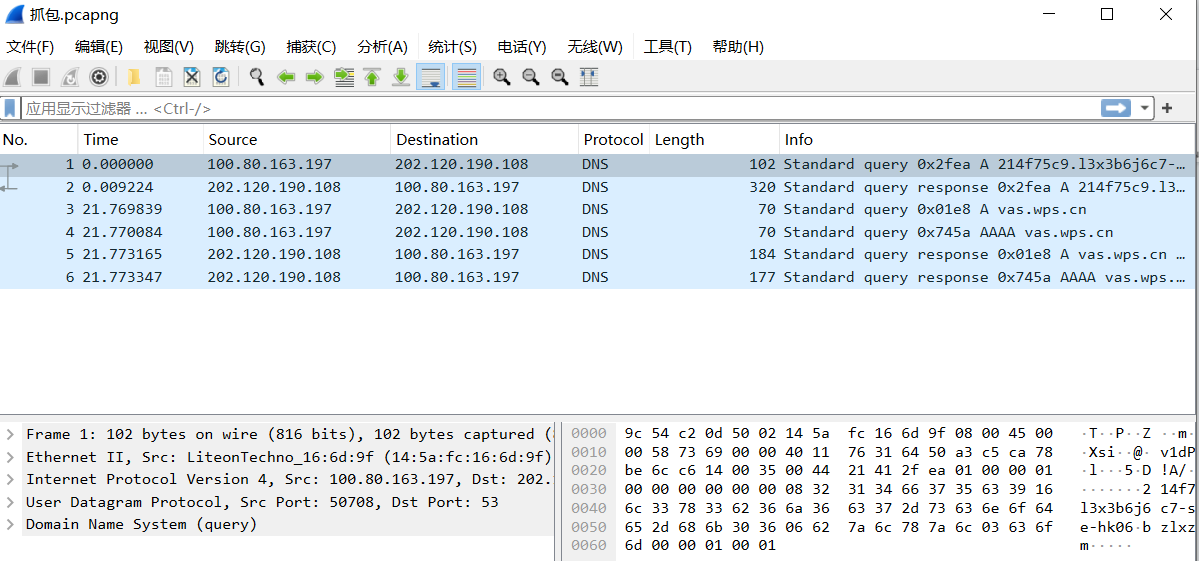


这是DNS服务器向PC0发送的UDP报文，可以看出其源端口号为DNS服务器的53端口，目的端口号为PC0的1027端口，数据报长度为0x48即72，校验和为0.

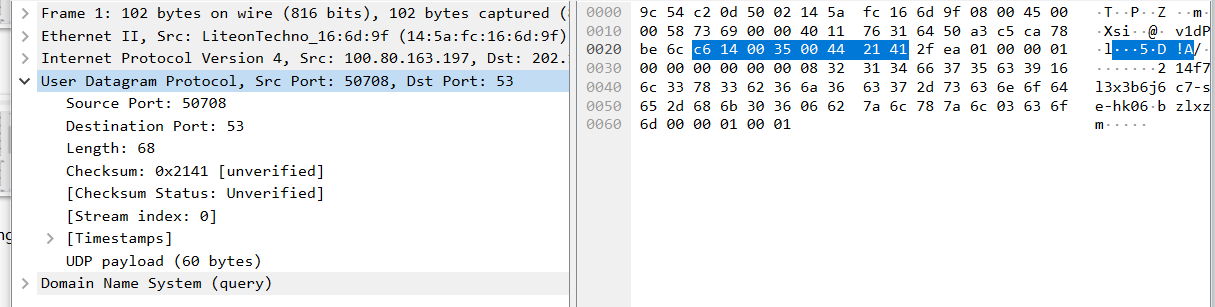


这是PC0接受的DNS服务器发来的UDP报文，其内容和服务器发送时所封装的内容一致。

1. 用WireShark抓取UDP数据包；



1. 查看UDP报文字段内容，并解读；



可以看到，在这个UDP数据报中，源端口号为50708，目的端口号为53，数据报长度为0x44即68，校验和为0x214。