实验 25_TCP 段分析实验

学生姓名:林觉凯　　合作同学:无

实验地点:济事楼 330　　实验时间:2024.5.13

【实验目的】

TCP 段是传输控制协议(Transmission Control Protocol)中的数据单元，在 TCP/IP 协议栈中，TCP 负责提供可靠的、面向连接的数据传输服务。本次实验通过使用网络仿真软件 Cisco Packet Tracer 和 Wireshark 进行 TCP 段分析，让我们更好地理解 TCP 协议的底层运作原理，同时也了解并使用 Wireshark 软件进行 TCP 包的抓取方法及分析过程。

【实验原理】

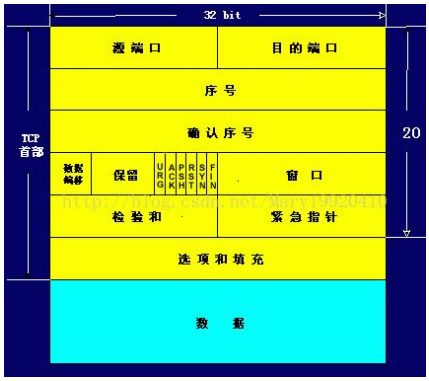
TCP 数据：

1.TCP 的概述

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。

2.TCP 数据的报文格式

TCP 报文是 TCP 层传输的数据单元，也叫报文段。



3. 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：这是 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。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。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。

4. 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。

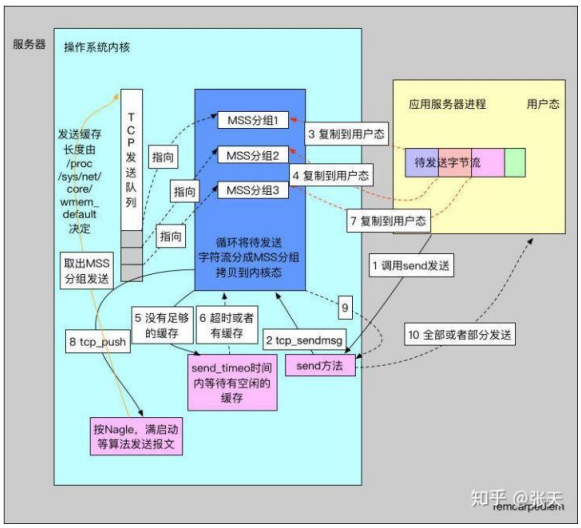
源端口									目标端口
Y									
X+1									
偏置值	保留		URG	1	PSH	RST	1	FIN	窗口
检查和									紧急指针
任选项+补丁									
用户数据									

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。

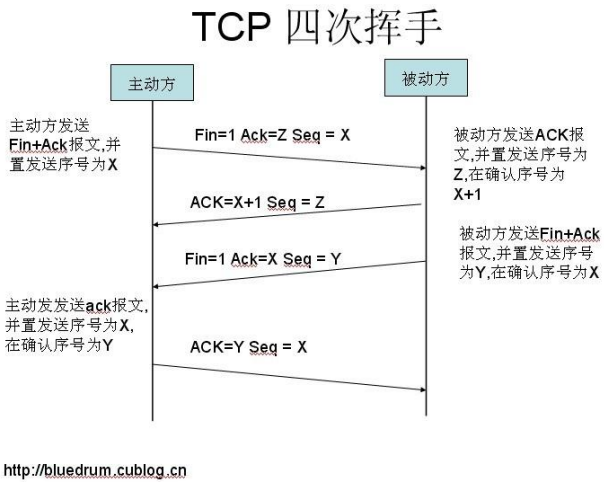
源端口									目标端口
发送顺序号									
Y+1									
偏置值	保留		URG	1	PSH	RST	SYN	FIN	窗口
检查和									紧急指针
任选项+补丁									
DATA（X+1）									

Tip:SYN 攻击在三次握手过程中，服务器发送 SYN-ACK 之后，收到客户端的 ACK 之前的 TCP 连接称为半连接(half-open connect).此时服务器处于 Syn_RECV 状态.当收到 ACK 后，服务器转入 ESTABLISHED 状态。攻击客户端在短时间内伪造大量不存在的 IP 地址，向服务器不断地发送 syn 包，服务器回复确认包，并等待客户的确认，由于源地址是不存在的，服务器需要不断的重发直至超时，这些伪造的 SYN 包将长时间占用未连接队列，正常的 SYN 请求被丢弃，目标系统运行缓慢，严重者引起网络堵塞甚至系统瘫痪。

Tip2:TCP 发送报文，操作系统内核与用户态。



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：

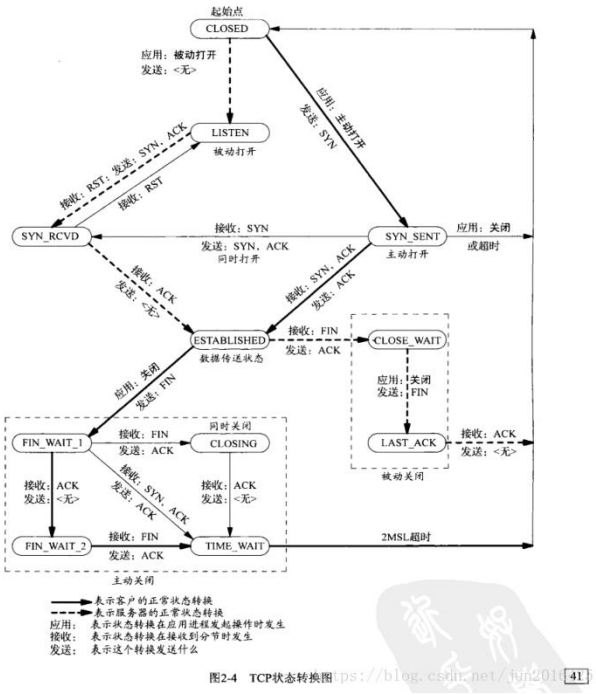


图2-4 TCP状态转换图 41

【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

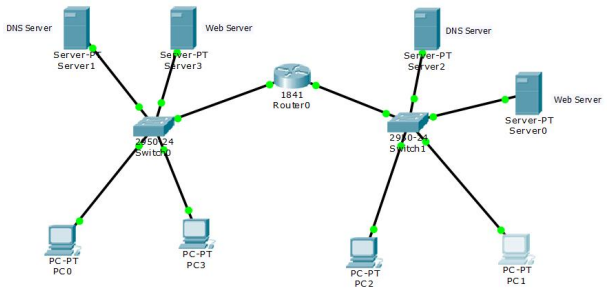
【实验步骤】

1.按照右图所示完成网络设备的连线。

2.打开网络浏览器，产生数据报文。

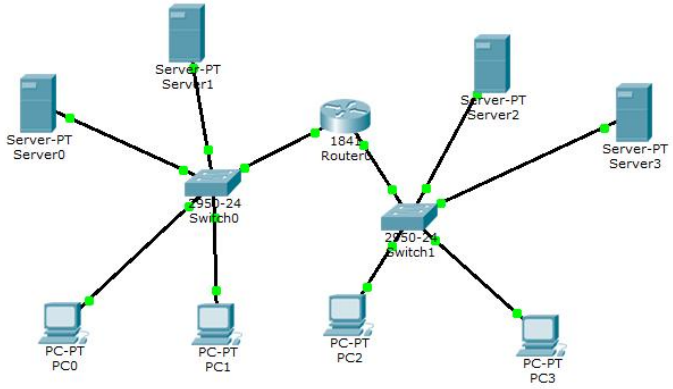
3.抓取并且查看 TCP 报文。

4.使用 Wireshark 软件抓取 TCP 报文并分析。

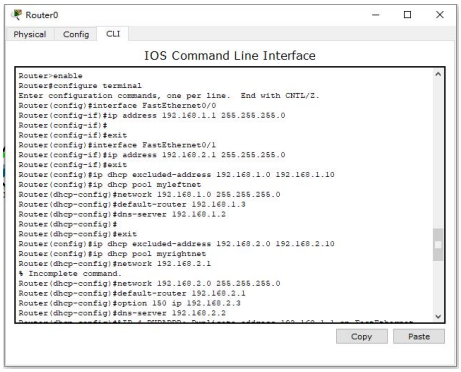


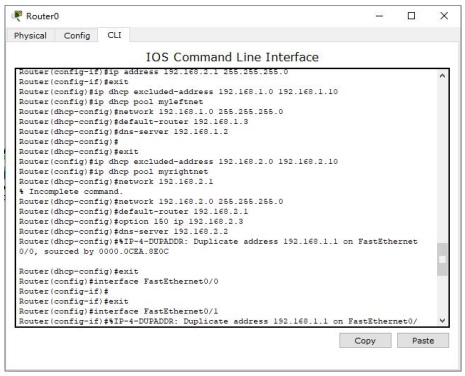
【实验现象】

首先按题目的要求完成网络设备的连线。



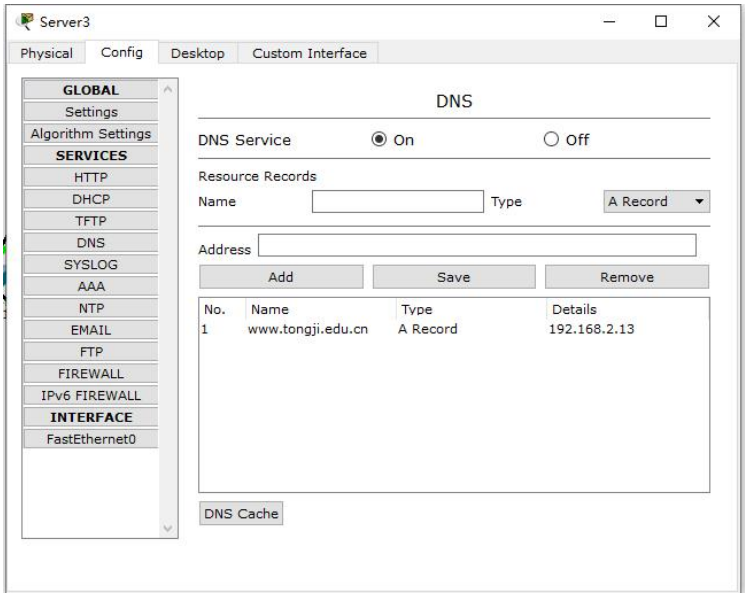
为每一台 PC 机配置相应的 IP，可以使用 DHCP 进行配置。



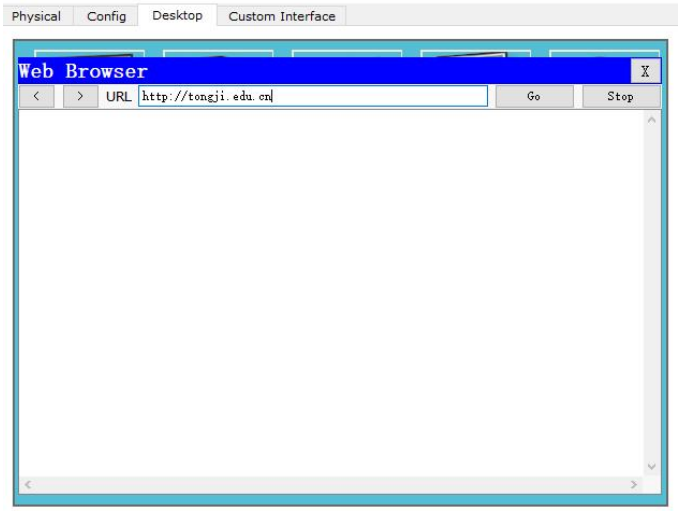


为 Server2 和 Server3 配置各自对应的 gateway、IP 和子网掩码。

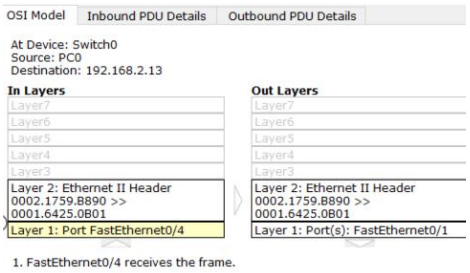
在 Server3 上配置 DNS，在这里我们将域名设置为 www.tongji.edu.cn，Address 设置为映射到 Server2 的 IP 地址 192.168.2.13。

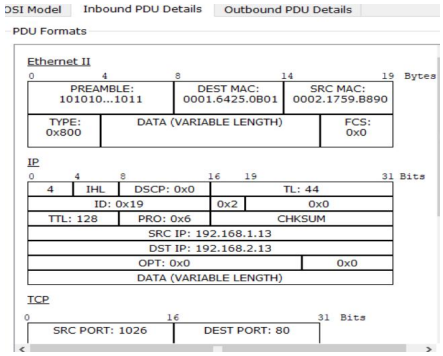


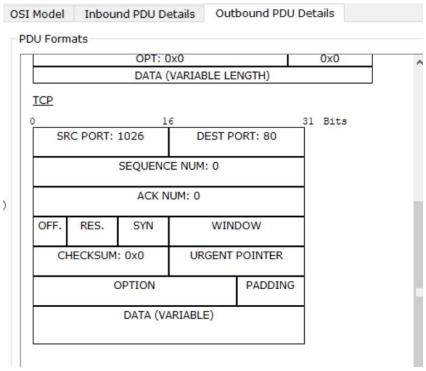
这时，我们便可以打开 PC0 的 Web Brower，访问 Web，输入所配置的域名 www.tongji.edu.cn，便可以产生相应的 TCP 数据报文。



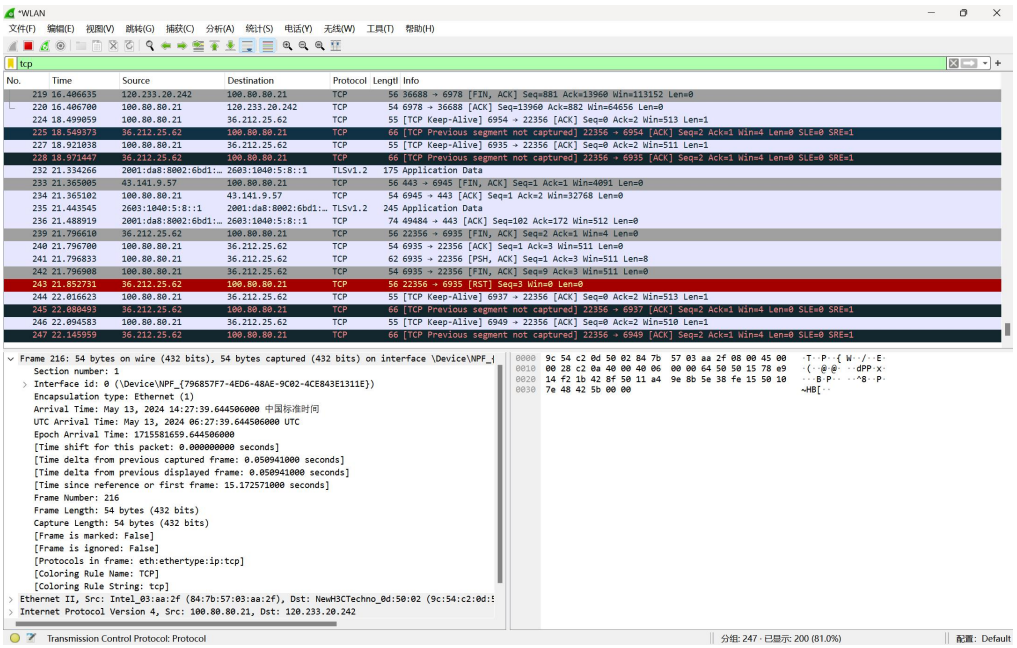
之后便可以使用 Packet Tracer 分析 TCP 报文。







用仿真软件 WireShark 抓取 TCP 数据包：



在如图所示的抓包中，进行查看 TCP 报文字段内容。

源端口：0x1b42 为 6962。

目标端口：0x8f50 为 36752。

序列号：0x11a49e8b 为 464349707。

确认号：0x5e38fe15 为 1586552085。

数据偏移和保留位：0x50 为 01010000，其中前 4 位表示数据偏移，偏移量为 5 个 32 位字，即 20 个字节。

控制位：0x10，转换为二进制为 00010000，代表 ACK(Acknowledgment)标志被设置，确认号字段有效。

窗口大小：0x7e48 为 32328。

校验和：0x425b 为 16987。

紧急指针：0x0000 为 0。

数据：在提供的数据中，剩余的部分是 TCP 数据段的实际数据。

【分析讨论】

通过本次实验，我比较深入的了解了 TCP 的概念和分析 TCP 数据包的方法。对于网络的可靠性来说，TCP 的三次握手和四次挥手是建立和终止 TCP 连接的过程在其中起到了非常重要的作用，也即 TCP 连接建立过程数据报文和 TCP 拆链过程数据报文，以下是相应的总结：

TCP 连接建立过程包括三次握手，涉及到三个数据报文，分别是 SYN，SYN-ACK，ACK。客户端发送 SYN 报文(SYN=1，seq=x)：客户端向服务器发送一个 SYN 报文，其中 SYN 标志位被设置为 1，表明客户端请求建立连接，并且选择一个序列号 seq=x，该序列号是一个随机数或者是一个起始序列号。服务器回复 SYN-ACK 报文(SYN=1，ACK=1，seq=y，ack=x+1)：服务器接收到客户端的 SYN 报文后，向客户端发送一个 SYN-ACK 报文作为响应。在这个报文中，SYN 和 ACK 标志位都被设置为 1，表示服务器同意建立连接，并且确认客户端的 SYN 报文，序列号 seq=y 是服务器随机选择的，而确认号 ack=x+1，表示服务器已经收到了客户端的 SYN 报文，并且序列号为 x 的数据已经被正确接收。客户端发送 ACK 报文(ACK=1，ack=y+1)：客户端接收到服务器的 SYN-ACK 报文后，向服务器发送一个 ACK 报文作为确认。在这个报文中，ACK 标志位被设

置为 1，表示客户端确认服务器的 SYN 报文，并且确认号 ack=y+1，表示客户端已经收到了服务器的 SYN-ACK 报文，并且序列号为 y 的数据已经被正确接收。

TCP 连接的拆链过程通常包括四次挥手，涉及到四个数据报文，分别是 FIN，ACK，FIN，ACK。客户端发送 FIN 报文(FIN=1，seq=x)：当客户端决定关闭连接时，它向服务器发送一个 FIN 报文，其中 FIN 标志位被设置为 1，表示客户端不再发送数据，但仍愿意接收数据。序列号 seq=x 是客户端选择的一个随机数或者是最后一个数据包的序列号。服务器回复 ACK 报文(ACK=1，ack=x+1)：服务器接收到客户端的 FIN 报文后，向客户端发送一个 ACK 报文作为确认。在这个报文中，ACK 标志位被设置为 1，表示服务器确认收到了客户端的 FIN 报文，确认号 ack=x+1 表示服务器已经接收了序列号为 x 的数据，并且表示服务器仍然可以发送数据。服务器发送 FIN 报文(FIN=1，seq=y)：当服务器决定关闭连接时，它向客户端发送一个 FIN 报文，其中 FIN 标志位被设置为 1，表示服务器不再发送数据，但仍愿意接收数据。序列号 seq=y 是服务器选择的一个随机数或者是最后一个数据包的序列号。客户端回复 ACK 报文（ACK=1，ack=y+1）：客户端接收到服务器的 FIN 报文后，向服务器发送一个 ACK 报文作为确认。在这个报文中，ACK 标志位被设置为 1，表示客户端确认收到了服务器的 FIN 报文，确认号 ack=y+1 表示客户端已经接收了序列号为 y 的数据，并且表示客户端仍然可以发送数据。

实验 27_DNS 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:2024.5.13

【实验目的】

DNS(Domain Name System)是互联网中的一种分布式命名系统，用于将域名转换为 IP 地址以供计算机网络之间进行通信。本次实验通过探究 DNS 的功能与工作过程，并且通过在仿真软件中模拟和分析 DNS 域名解析过程，理解 DNS 的工作原理和 DNS 服务在网络通信中作用。

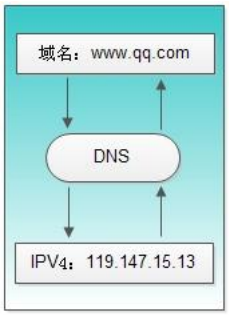
【实验原理】

DNS 原理

1. DNS 的概述

为什么需要 DNS 解析域名为 IP 地址？网络通讯大部分是基于 TCP/IP 的，而 TCP/IP 是基于 IP 地址的，所以计算机在网络上进行通讯时只能识别如“202.96.134.133”之类的 IP 地址，而不能认识域名。我们无法记住 10 个以上 IP 地址的网站，所以我们访问网站时，更多的是在浏览器地址栏中输入域名，就能看到所需要的页面，这是因为有一个叫“DNS 服务器”的计算机自动把我们的域名“翻译”成了相应的 IP 地址，然后调出 IP 地址所对应的网页。

具体什么是 DNS？DNS(Domain Name System)是“域名系统”的英文缩写，是一种组织成域层次结构的计算机和网络服务命名系统，它用于 TCP/IP 网络，它所提供的服务是用来将主机名和域名转换为 IP 地址的工作。DNS 就是这样的一位“翻译官”，它的基本工作原理可用下图来表示为什么需要 DNS 解析域名为 IP 地址？



2. DNS 的过程

DNS 是应用层协议，事实上他是为其他应用层协议工作的，包括不限于 HTTP

和 SMTP 以及 FTP，用于将用户提供的主机名解析为 ip 地址。

具体过程如下：

①用户主机上运行着 DNS 的客户端，就是我们的 PC 机或者手机客户端运行着 DNS 客户端了。

②浏览器将接收到的 url 中抽取出域名字段，就是访问的主机名，比如 http://www.baidu.com/, 并将这个主机名传送给 DNS 应用的客户端。

③DNS 客户机端向 DNS 服务器端发送一份查询报文，报文中包含着要访问的主机名字段(中间包括一些列缓存查询以及分布式 DNS 集群的工作)。

④该 DNS 客户机最终会收到一份回答报文，其中包含有该主机名对应的 IP 地址。

⑤一旦该浏览器收到来自 DNS 的 IP 地址，就可以向该 IP 地址定位的 HTTP 服务器发起 TCP 连接。

3. DNS 服务的体系架构

DNS domain name system 主要作用就是将主机域名转换为 ip 地址。假设运行在用户主机上的某些应用程序(如 Web 浏览器或者邮件阅读器)需要将主机名转换为 IP 地址。这些应用程序将调用 DNS 的客户机端，并指明需要被转换的主机名。(在很多基于 UNIX 的机器上，应用程序为了执行这种转换需要调用函数 gethostbyname())。用户主机的 DNS 客户端接收到后，向网络中发送一个 DNS 查询报文。所有 DNS 请求和回答报文使用的 UDP 数据报经过端口 53 发送。

经过若干 ms 到若干 s 延时后，用户主机上的 DNS 客户端接收到一个提供所希望映射的 DNS 回答报文。这个查询结果则被传递到调用 DNS 的应用程序。因此，从用户主机上调用应用程序的角度看，DNS 是一个提供简单、直接的转换服务的黑盒子。但事实上，实现这个服务的黑盒子非常复杂，它由分布于全球的大量DNS服务器以及定义了DNS服务器与查询主机通信方式的应用层协议组成。

3. DNS 分布式集群工作方式

DNS 的一种简单的设计模式就是在因特网上只使用一个 DNS 服务器，该服务器包含所有的映射，在这种集中式的设计中，客户机直接将所有查询请求发往单一的 DNS 服务器，同时该 DNS 服务器直接对所有查询客户机做出响应，尽管这种设计方式非常诱人，但他不适用当前的互联网，因为当今的因特网有着数量

巨大并且在持续增长的主机，这种集中式设计会有单点故障(故障一个，全球着急)。

通信容量(上亿台主机发送的查询DNS报文请求，包括但不限于所有的HTTP请求，电子邮件报文服务器，TCP长连接服务)，远距离的时间延迟(澳大利亚到纽约的举例)，维护开销大(因为所有的主机名-ip映射都要在一个服务站点更新)等问题。DNS服务器一般分三种，根DNS服务器，顶级DNS服务器，权威DNS服务器。使用分布式的层次数据库模式以及缓存方法来解决单点集中式的问题。

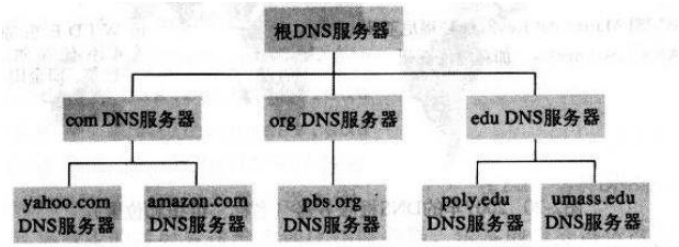
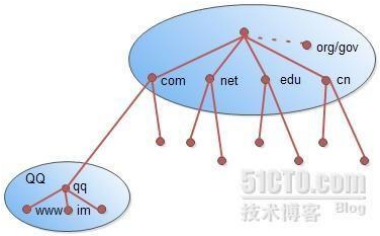


图2-19 DNS服务器的部分层次结构

4. DNS 域名称

域名系统作为一个层次结构和分布式数据库。包含各种类型的数据，包括主机名和域名。DNS数据库中的名称形成一个分层树状结构称为域命名空间。域名包含单个标签分隔点，例如：im.qq.com完全限定的域名(FQDN)唯一地标识在DNS分层树中的主机的位置，通过指定的路径中点分隔从根引用的主机的名称列表。下图显示与主机称为im内qq.com DNS树的示例。

主机的FQDN是im.qq.com DNS域的名称层次结构。



4. DNS 域名称空间的组织方式

按其功能命名空间中用来描述 DNS 域名称的五个类别的介绍详见下表中，以及与每个名称类型的示例。

名称类型	说 明	示 例
根域	DNS域名中使用时，规定由尾部句点(.)来指定名称位于根或更高级别的域层次结构	单个句点(.)或句点用于末尾的名称
顶级域	用来指示某个国家/地区或组织使用的名称的类型名称	.com
第二层域	个人或组织在Internet上使用的注册名称	qq.com
子域	已注册的二级域名派生的域名，通俗的讲就是网站名	www.qq.com
主机名	通常情况下，DNS域名的最左侧的标签标识网络上的特定计算机，如h1	h1.www.qq.com

互联网域名系统由名称注册机构负责维护分配由组织和国家/地区的顶级域在 Internet 上进行管理。这些域名有很多缩写，两个字母和三个字母的国家/地区使用的缩写使用下表所示。一些常见的 DNS 域名称如下图：

DNS域名称	组织类型
com	商业公司
edu	教育机构
net	网络公司
gov	非军事政府机构
Mil	军事政府机构
xx	国家/地区代码(cn表中国)
….	….

5. DNS 域名资源记录

DNS 数据库中包含的资源记录(RR)。每个 RR 标识数据库中的特定资源。我们在建立 DNS 服务器时，经常会用到 SOA,NS,A 之类的记录，在维护 DNS 服务器时，会用到 MX，CNAME 记录。常见的 RR 见下图：

说 明	类	时间(ttl)	类型	数 据
起始授权机构	互联网 (IN)	默认值为60分钟	SOA	所有者名称 主名称服务器 DNS 名称、 序列号 刷新间隔 重试间隔 过期时间 最小 TTL
主机	互联网 (IN)	记录特定 TTL （如果存在），否则区域 （SOA） TTL	A	所有者名称 （主机的 DNS 名称） 主机 IP 地址
名称服务器	互联网 (IN)	记录特定 TTL （如果存在），否则区域 （SOA） TTL	NS	所有者名称 名称服务器 DNS 名称
邮件交换器	互联网 (IN)	记录特定 TTL （如果存在），否则区域 （SOA） TTL	MX	所有者名称 邮件 Exchange Server DNS 名称的首选项值
别名	互联网 (IN)	记录特定 TTL （如果存在），否则区域 （SOA） TTL	CNAME	所有者名称 （别名） 主机的 DNS 名称

6. DNS 服务的工作过程

当 DNS 客户机需要查询程序中使用的名称时，它会查询本地 DNS 服务器来解析该名称。客户机发送的每条查询消息都包括 3 条信息，以指定服务器应回答的问题。

(1)指定的 DNS 域名，表示为完全合格的域名(FQDN)；

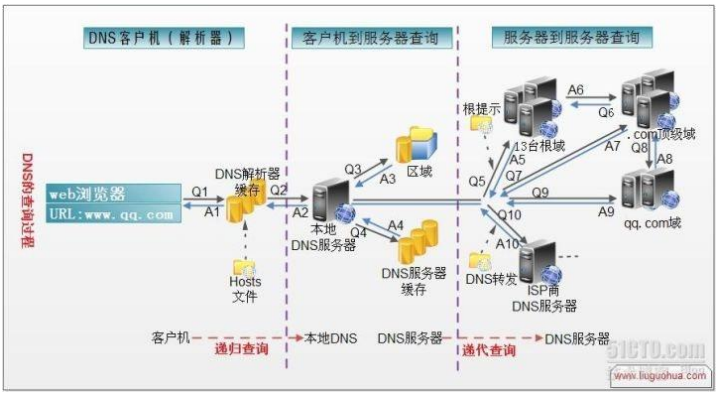
(2)指定的查询类型,它可根据类型指定资源记录,或作为查询操作的专门类型；

(3)DNS 域名的指定类别。

对于 DNS 服务器，它始终应指定为 Internet 类别。例如，指定的名称可以是计算机的完全合格的域名，如 im.qq.com，并且指定的查询类型用于通过该名称搜索地址资源记录。DNS 查询以各种不同的方式进行解析。客户机有时也可通过使用从以前查询获得的缓存信息就地应答查询。DNS 服务器可使用其自身的

资源记录信息缓存来应答查询，也可代表请求客户机来查询或联系其他 DNS 服务器，以完全解析该名称，并随后将应答返回至客户机。这个过程称为递归。

另外，客户机自己也可尝试联系其他的 DNS 服务器来解析名称。如果客户机这么做，它会使用基于服务器应答的独立和附加的查询，该过程称作迭代，即 DNS 服务器之间的交互查询就是迭代查询。DNS 查询的过程如下图所示。



(1)在浏览器中输入 www.qq.com 域名，操作系统会先检查自己本地的 hosts 文件是否有这个网址映射关系，如果有，就先调用这个 IP 地址映射，完成域名解析。

(2)如果 hosts 里没有这个域名的映射，则查找本地 DNS 解析器缓存，是否有这个网址映射关系，如果有，直接返回，完成域名解析。

(3)如果 hosts 与本地 DNS 解析器缓存都没有相应的网址映射关系，首先会找 TCP/IP 参数中设置的首选 DNS 服务器，在此我们叫它本地 DNS 服务器，此服务器收到查询时，如果要查询的域名，包含在本地配置区域资源中，则返回解析结果给客户机，完成域名解析，此解析具有权威性。

(4)如果要查询的域名，不由本地 DNS 服务器区域解析，但该服务器已缓存了此网址映射关系，则调用这个 IP 地址映射，完成域名解析，此解析不具有权威性。

(5)如果本地 DNS 服务器本地区域文件与缓存解析都失效，则根据本地 DNS 服务器的设置(是否设置转发器)进行查询，如果未用转发模式，本地 DNS 就把请求发至 13 台根 DNS，根 DNS 服务器收到请求后会判断这个域名(.com)是谁来授权管理，并会返回一个负责该顶级域名服务器的一个 IP。本地 DNS 服务器收到 IP 信息后，将会联系负责.com 域的这台服务器。这台负责.com 域的服务器收

到请求后，如果自己无法解析，它就会找一个管理.com 域的下一级 DNS 服务器地址(http://qq.com)给本地 DNS 服务器。

(5)当本地 DNS 服务器收到这个地址后，就会找 http://qq.com 域服务器，重复上面的动作，进行查询，直至找到 www.qq.com 主机。

(6)如果用的是转发模式，此 DNS 服务器就会把请求转发至上一级 DNS 服务器，由上一级服务器进行解析，上一级服务器如果不能解析，或找根 DNS 或把转请求转至上上级，以此循环。不管是本地 DNS 服务器用是是转发，还是根提示，最后都是把结果返回给本地 DNS 服务器，由此 DNS 服务器再返回给客户机。从客户端到本地 DNS 服务器是属于递归查询，而 DNS 服务器之间就是的交互查询就是迭代查询。

7. DNS 域名解析顺序

(1)浏览器缓存

当用户通过浏览器访问某域名时，浏览器首先会在自己的缓存中查找是否有该域名对应的 IP 地址(若曾经访问过该域名且没有清空缓存便存在)；

(2)系统缓存

当浏览器缓存中无域名对应 IP 则会自动检查用户计算机系统 Hosts 文件 DNS 缓存是否有该域名对应 IP；

(3)路由器缓存

当浏览器及系统缓存中均无域名对应 IP 则进入路由器缓存中检查，以上三步均为客服端的 DNS 缓存；

(4)ISP(互联网服务提供商)DNS 缓存

当在用户客服端查找不到域名对应 IP 地址，则将进入 ISP DNS 缓存中进行查询。比如你用的是电信的网络，则会进入电信的 DNS 缓存服务器中进行查找；

(5)根域名服务器

当以上均未完成，则进入根服务器进行查询。全球仅有 13 台根域名服务器，1 个主根域名服务器，其余 12 为辅根域名服务器。根域名收到请求后会查看区域文件记录，若无则将其管辖范围内顶级域名(如.com)服务器 IP 告诉本地 DNS 服务器；

(6)顶级域名服务器

顶级域名服务器收到请求后查看区域文件记录，若无则将其管辖范围内主域名服务器的 IP 地址告诉本地 DNS 服务器；

(7)主域名服务器

主域名服务器接受到请求后查询自己的缓存，如果没有则进入下一级域名服务器进行查找，并重复该步骤直至找到正确纪录；

(8)保存结果至缓存

本地域名服务器把返回的结果保存到缓存，以备下一次使用，同时将该结果反馈给客户端，客户端通过这个 IP 地址与 web 服务器建立链接。

【实验设备】

硬件设备：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

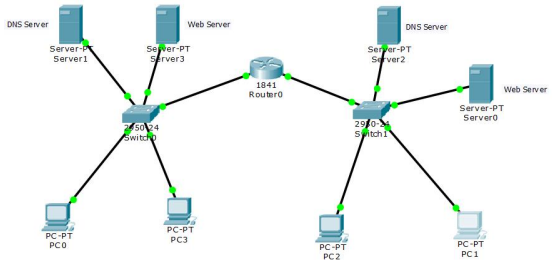
【实验步骤】

1.如右图所示完成构建网络拓扑。

2.配置相应的 DHCP 和域名。

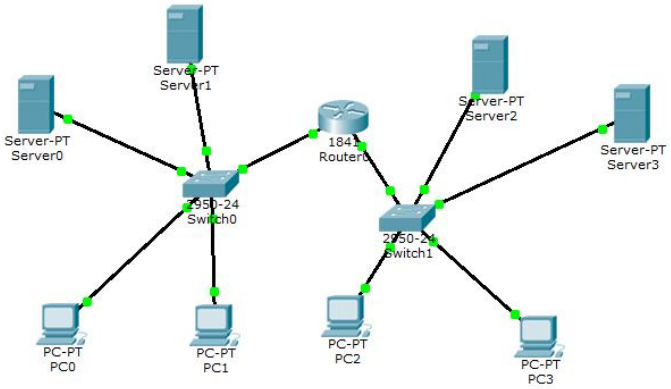
3.在仿真模式中发送通过域名发送请求并且查看。

4.使用 wireshark 进行 DNS 报文抓取并分析。



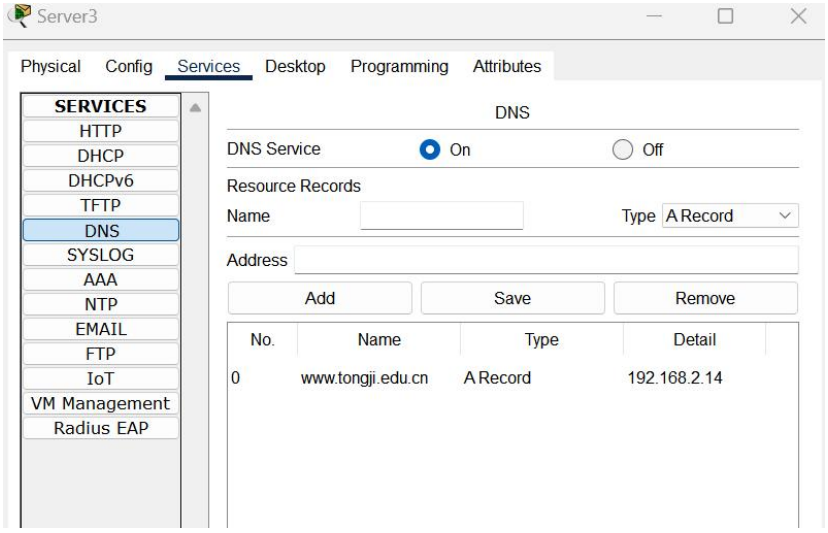
【实验现象】

首先按题目的要求完成网络设备的连线。

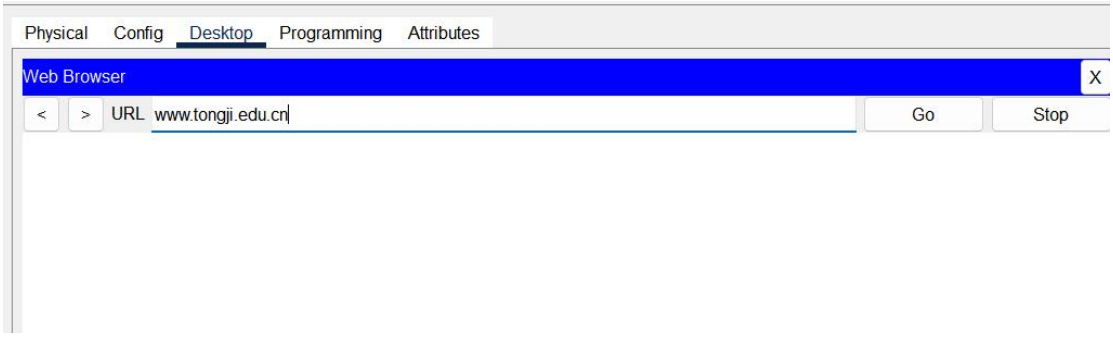


和上一个实验同样的方法配置每一台 PC 机配置相应的 IP。

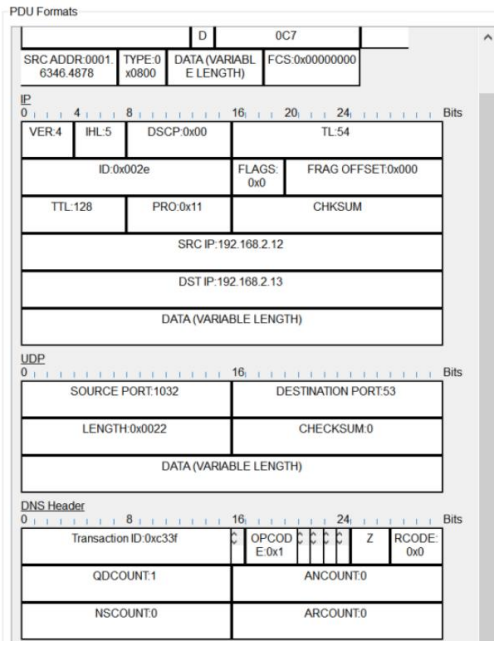
接着在 Server3 上配置 DNS，在这里我们将域名设置为 www.tongji.edu.cn，Address 设置为映射到 Server2 的 IP 地址 192.168.2.14。

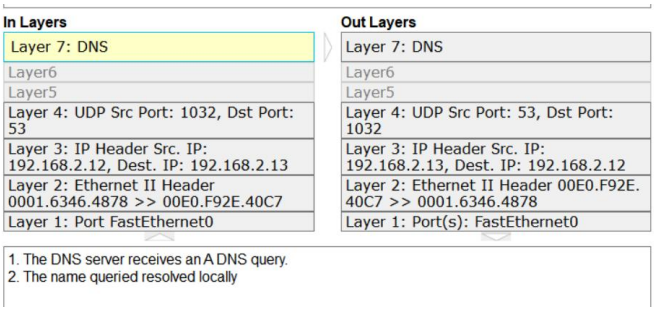


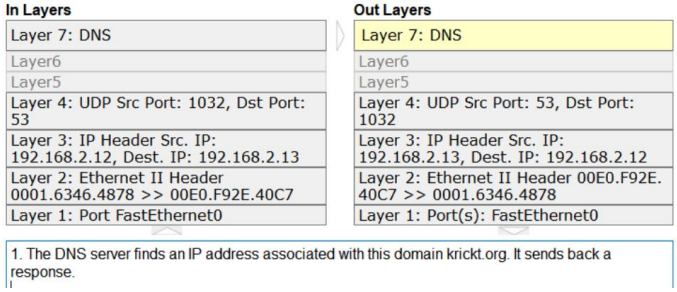
这时，我们便可以打开 PC2 的 Web Brower，访问 Web，输入所配置的域名 www.tongji.edu.cn，便可以产生相应的 TCP 数据报文。



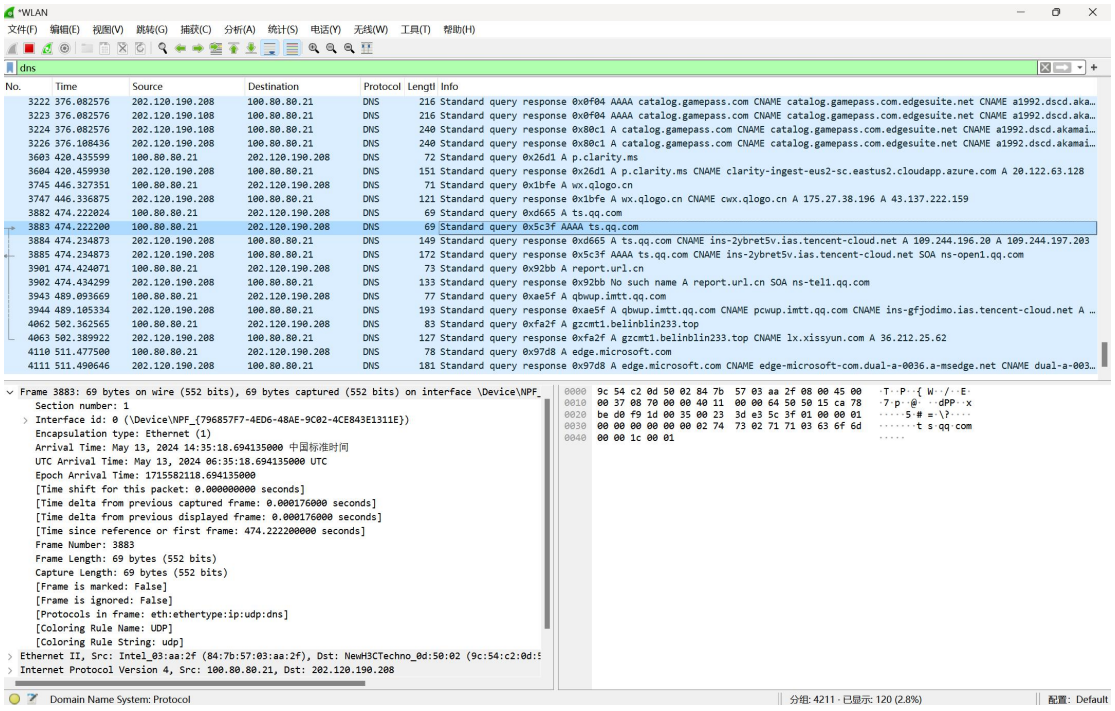
之后便可以使用 Packet Tracer 分析 DNS 报文。







用仿真软件 WireShark 抓取 DNS 数据包：



标识符：5c 3f。用于在 DNS 请求和响应之间匹配。

标志：01 00。其中最高位为 0 表示这是一个标准查询，第二位为 1 表示这是一个递归查询。

问题数：00 01。表示问题部分的条目数，本数据包中有一个问题。

回答数：00 00。表示回答部分的条目数，本数据包中没有回答。

授权部分数：00 00。表示授权部分的条目数，本数据包中没有授权部分。

附加部分数：00 00。表示附加部分的条目数，本数据包中没有附加部分。

查询名称：02 74 73 02 71 71 03 63 6f 6d 00。这是一个查询域名的编码形式。02 表示接下来有两个字节的长度，然后是字符"ts"，接着 02 表示接下来有两个字节的长度，之后 03 表示接下来有三个字节的长度，然后是字符"com"，最后以 00 结尾表示域名结束。

查询类型：00 1c。表示查询的类型，00 1c 代表 IPv6 地址。

查询类：00 01。表示查询的类别，00 01 代表 Internet 地址。

【分析讨论】

本次 DNS 实验和上次的 TCP 段分析实验比较相似。通过本次实验，我们更加深入了解了 DNS 的概念和工作过程，同时学会了应该如何用 Wireshark 软件

抓取 DNS 数据包并且进行分析。

DNS 域名转换的过程通常包括以下步骤：

查询请求：当用户在浏览器中输入一个域名(例如 example.com)时，操作系统会发出 DNS 查询请求到本地 DNS 服务器。

本地 DNS 服务器查询：本地 DNS 服务器首先检查自己的 DNS 缓存，如果已经缓存了该域名的解析结果，则直接返回对应的 IP 地址。如果没有缓存，本地 DNS 服务器则开始进行递归查询。

递归查询：本地 DNS 服务器向根域名服务器发出查询请求，根域名服务器负责返回顶级域名服务器的 IP 地址。

顶级域名服务器查询：本地 DNS 服务器接收到根域名服务器返回的 IP 地址后，向对应的顶级域名服务器发出查询请求，顶级域名服务器负责返回次级域名服务器的 IP 地址。

权限域名服务器查询：本地 DNS 服务器接收到顶级域名服务器返回的 IP 地址后，向权限域名服务器(也称为权威域名服务器)发出查询请求，权限域名服务器负责返回所查询域名的 IP 地址。

IP 地址返回：本地 DNS 服务器收到权限域名服务器返回的 IP 地址后，将结果缓存并返回给用户的操作系统。用户的操作系统将收到的 IP 地址用于建立与服务器的连接。

结果缓存：本地 DNS 服务器会将查询结果缓存一段时间，以便下次查询相同域名时能够直接返回结果，提高查询效率。