实验(二十三)：DNS实验

一.实验目的

- 实验的目的是通过分析Packet Tracer和WireShark中DNS数据报文，深入理解DNS解析过程，具体内容如下：
  - 在Packet Tracer中分析DNS报文情况；
  - 使用WireShark抓取DNS数据包；
  - 查看和解读DNS报文字段内容，包括DNS消息头、查询报文和应答报文中的各个字段信息。
- 通过这些步骤，实验旨在帮助我们掌握DNS的工作原理，了解DNS在网络通信中的重要性，以及熟悉使用网络分析工具进行数据包抓取和分析的基本方法

二.实验原理

- DNS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，主要功能是将主机名和域名转换为IP地址。DNS服务基于应用层协议工作，为多种应用层协议（如HTTP、SMTP和FTP）提供主机名到IP地址的解析。
- DNS概述
  - 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：
    - 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
    - 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
    - DNS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）。
    - 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。
    - 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。
- 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的延时后，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。
- 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)
….	….

- 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

- DNS报文结构
  - DNS报文主要包括以下部分：

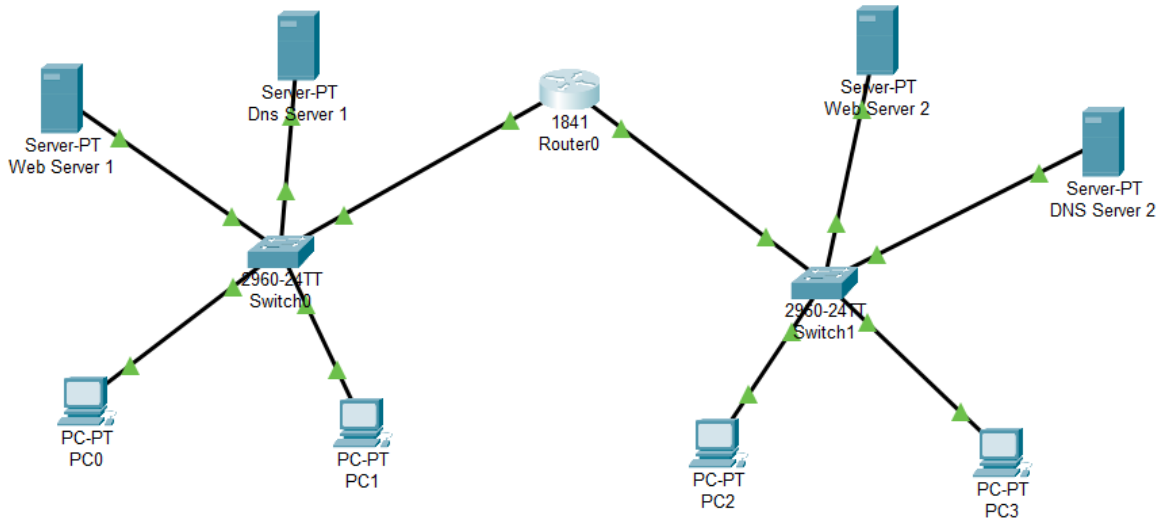
    - **报文头部**：包含标识符、标志、问题数、回答数、授权数和附加信息数等。
    - **查询部分**：包含查询的域名、查询类型和查询类等信息。
    - **回答部分**：包含域名、类型、类、生存时间、资源数据长度和实际的IP地址等。
- 分布式DNS系统
    - 为了应对互联网中海量的域名解析请求，DNS采用分布式层次结构，包括根DNS服务器、顶级域名服务器和权威DNS服务器等。分布式系统通过缓存和层次结构，有效地提高了DNS查询的效率和可靠性。

三.实验环境

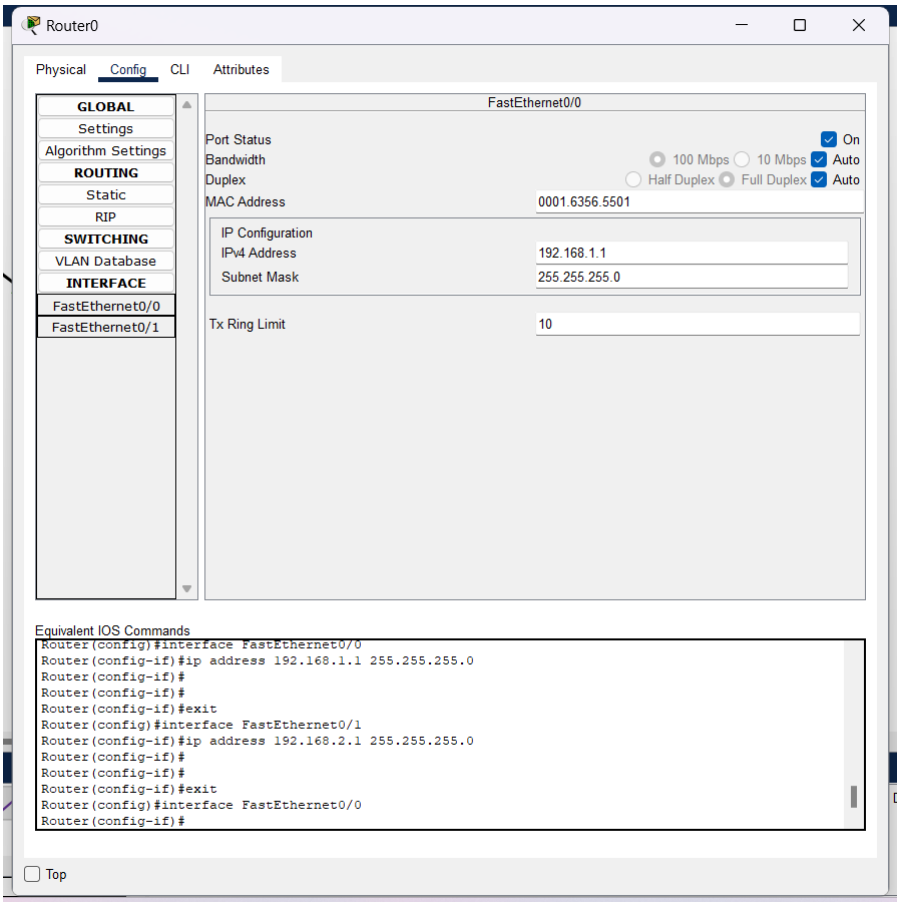
- 操作系统：Windows 11
- 网络环境：局域网
- 软件：`Cisco Packet Tracer`虚拟实验环境

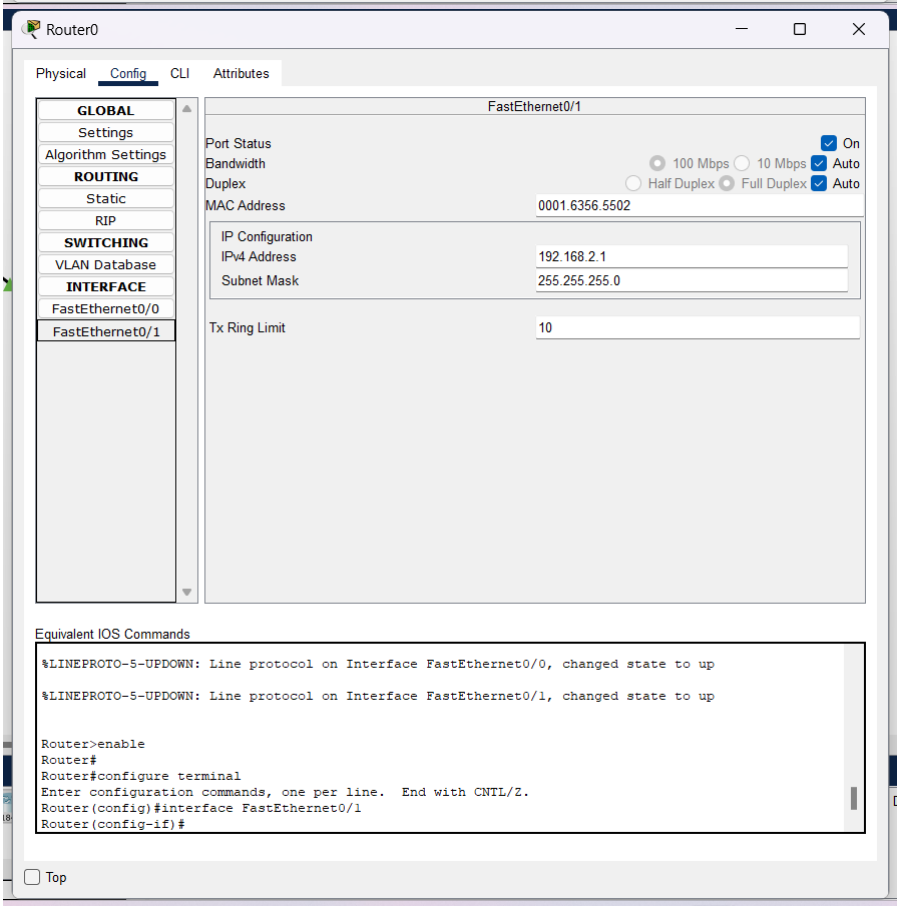
四.实验步骤

- 规划网络地址及拓扑图如下图所示

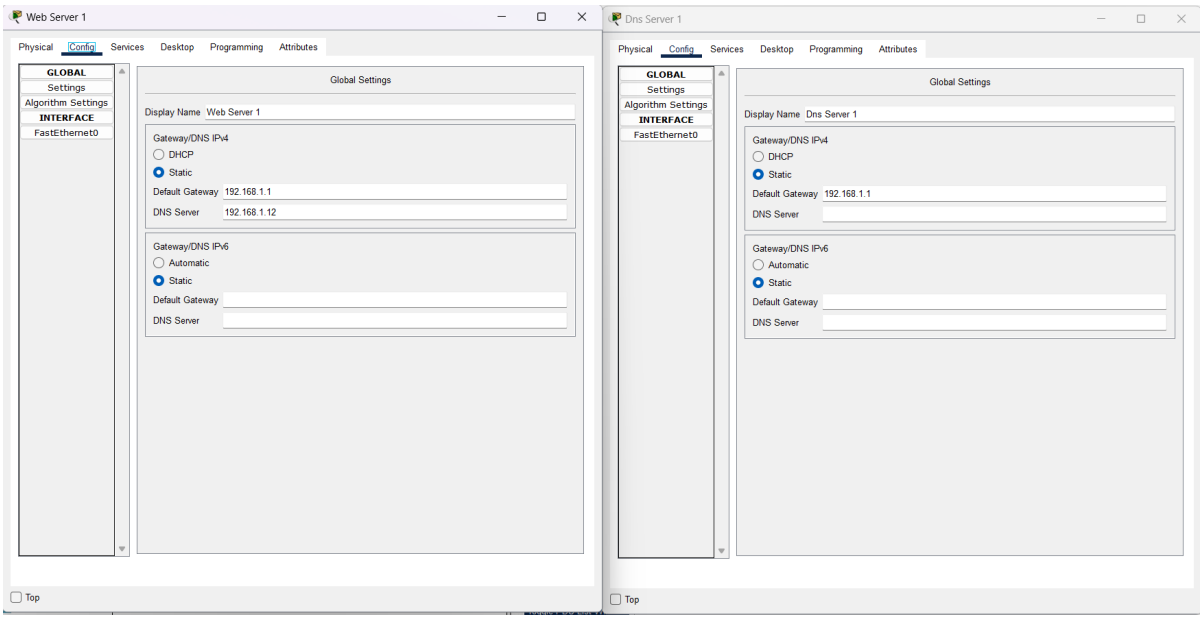


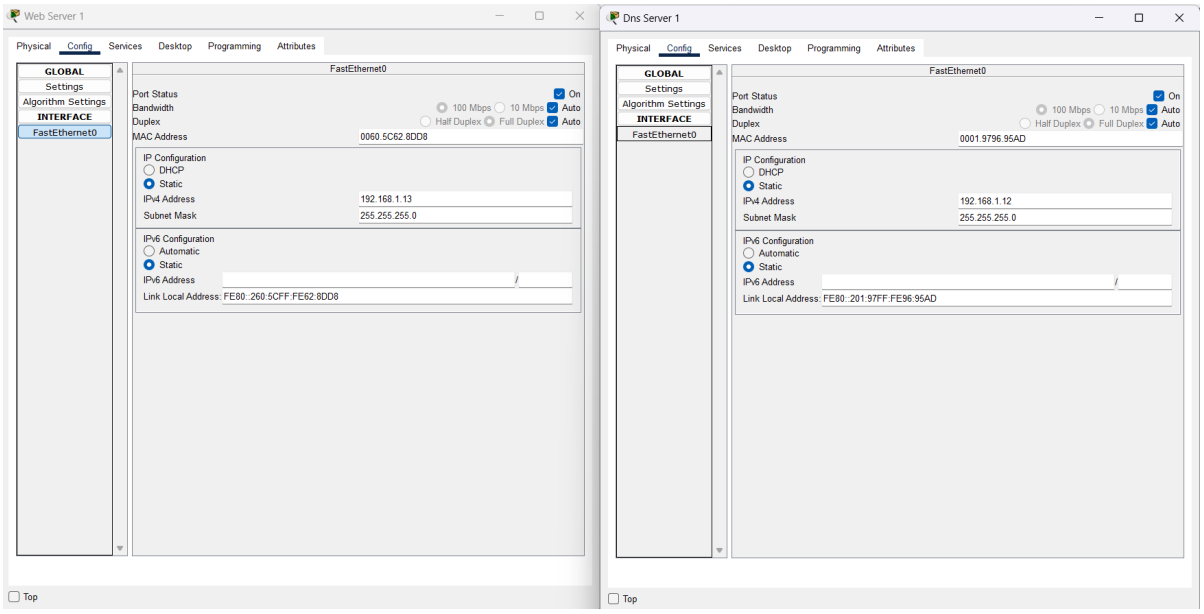
- 配置Router0（以左侧一组为例，右侧同理）



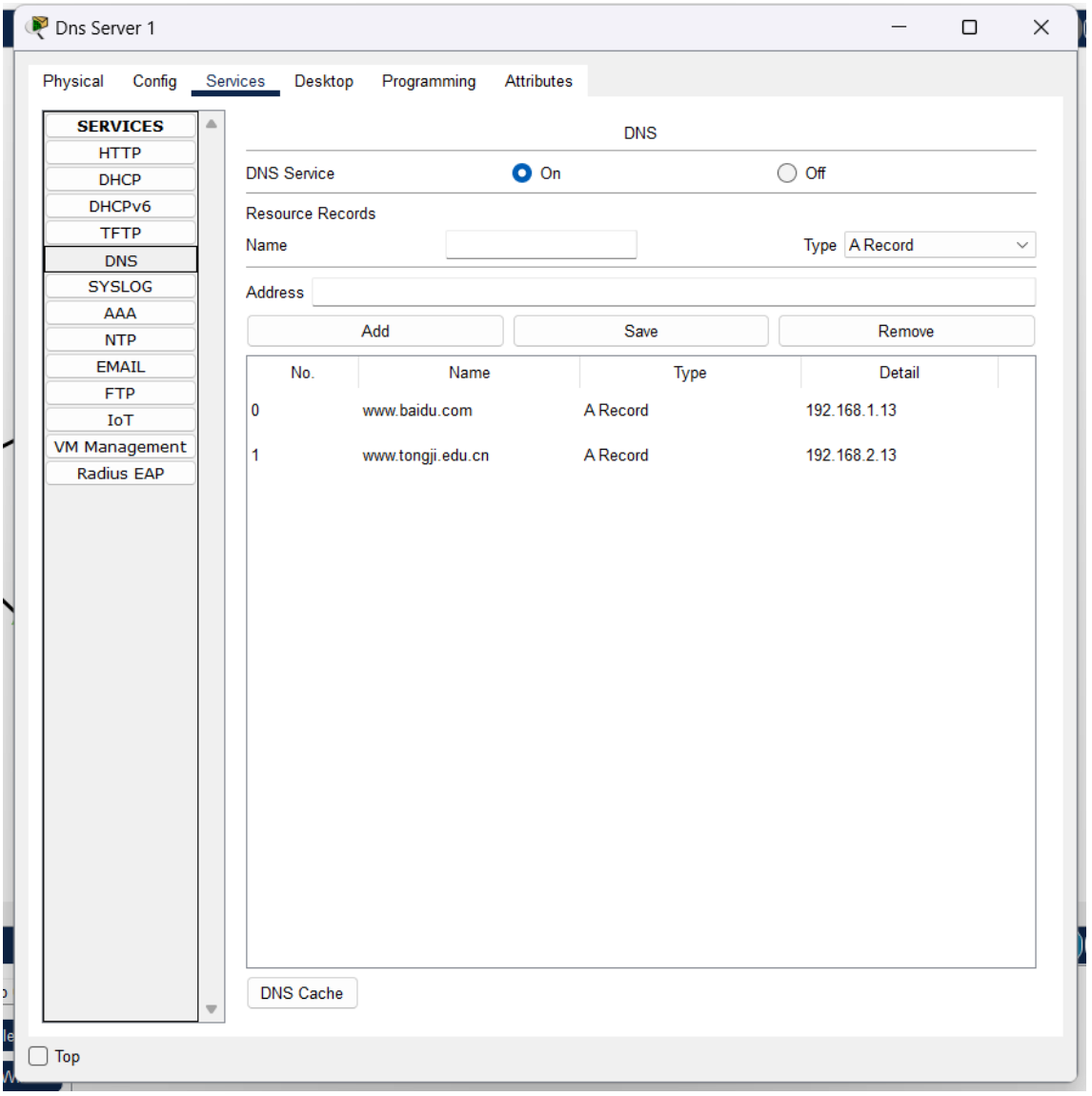


- 配置Web Server和DNS Server（以左侧一组为例，右侧同理）

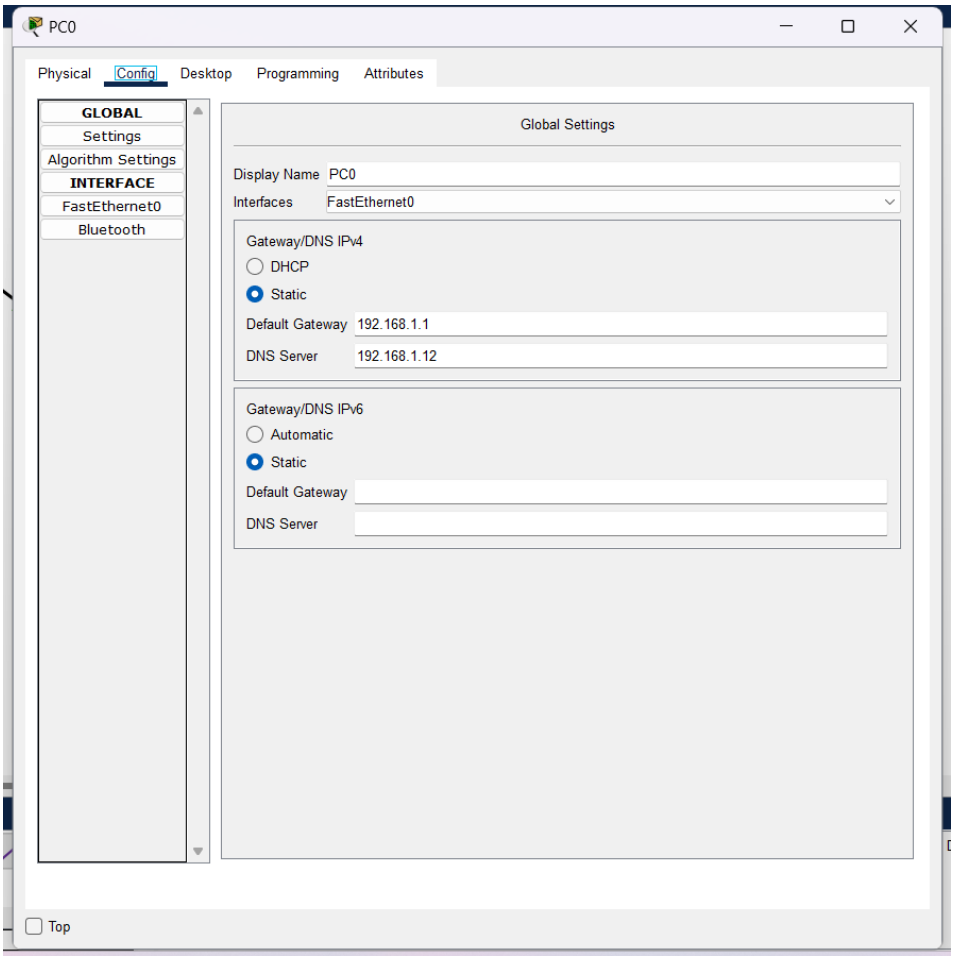


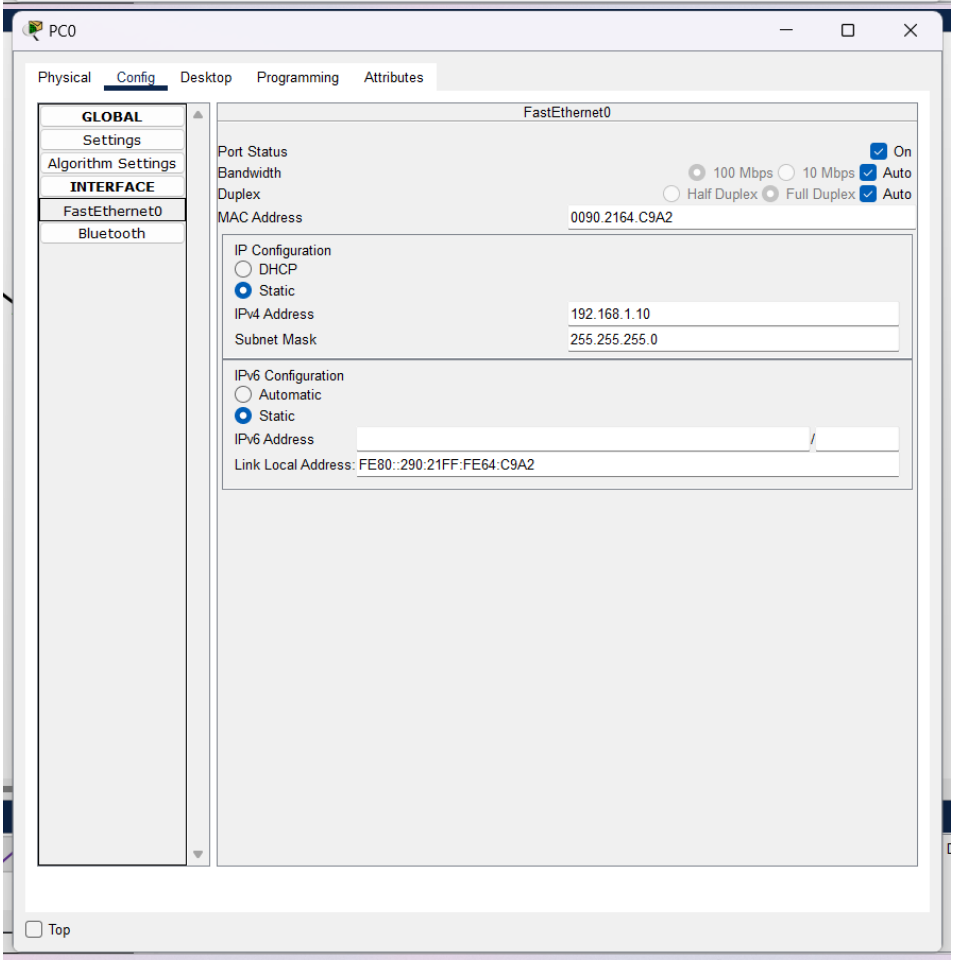


- 在DNS SERVER1添加name和ip的映射（以左侧一组为例，右侧同理）
  - name：`www.baidu.com` ip：`192.168.1.13`
  - name：`www.tongji.edu.cn` ip：`192.168.2.13`

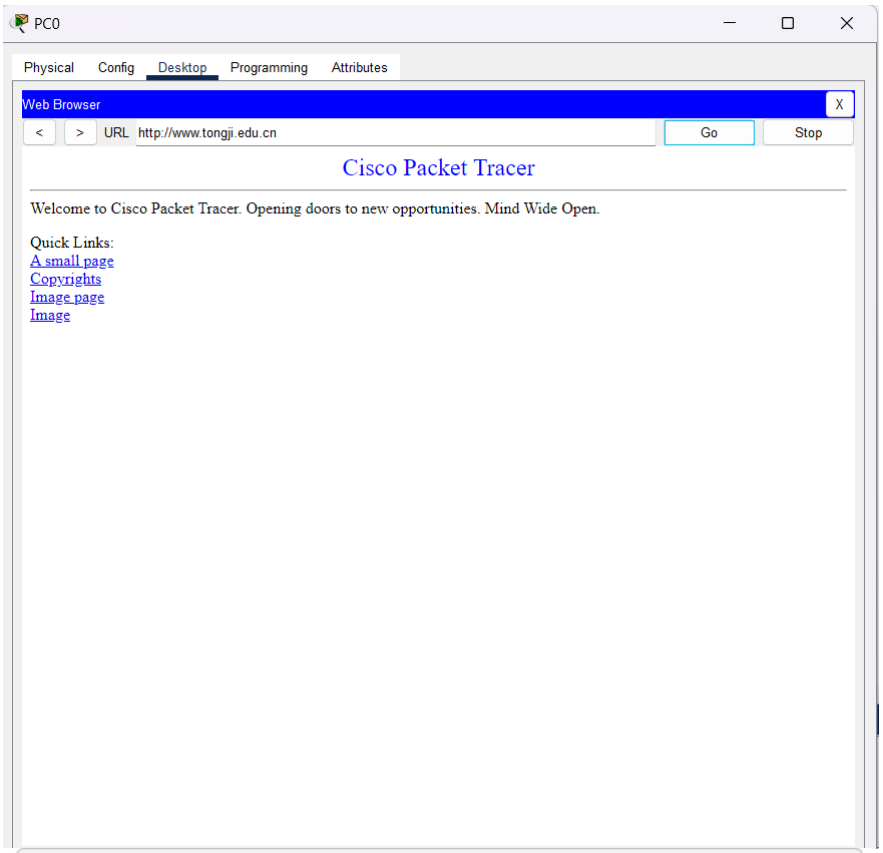


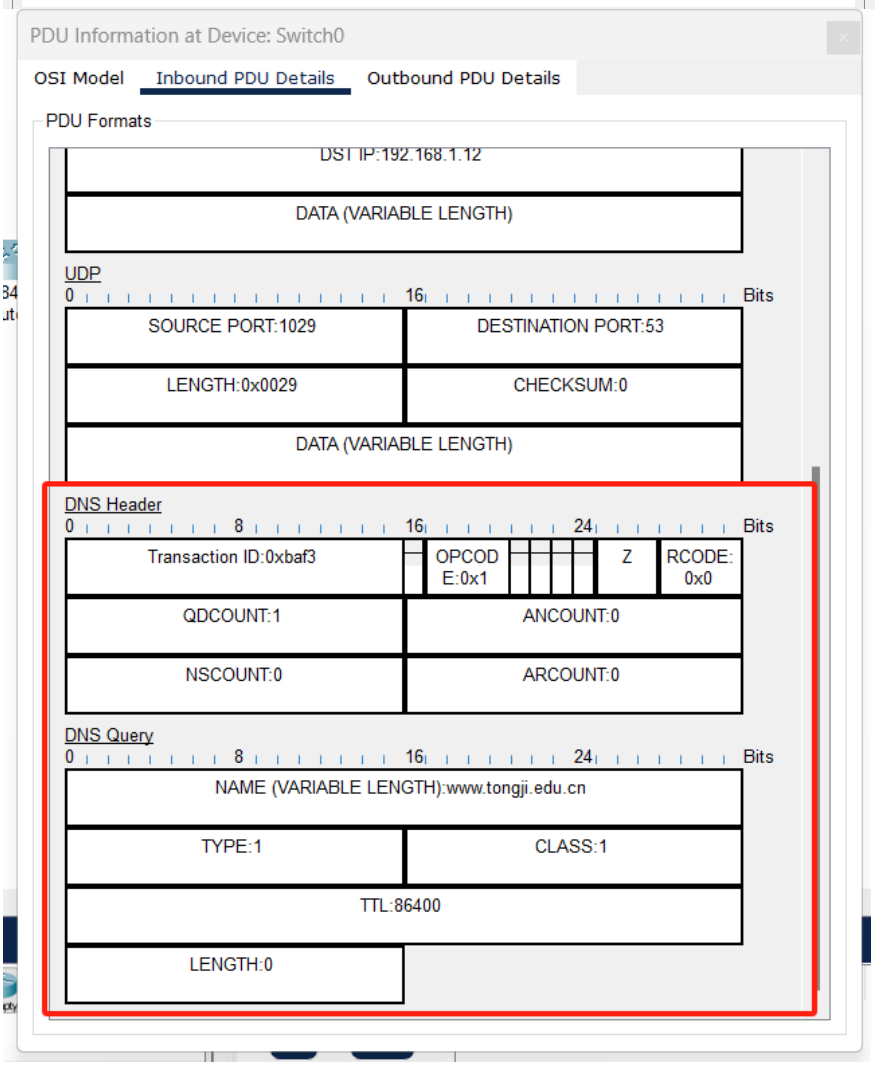
- 配置各个PC（以PC0为例）



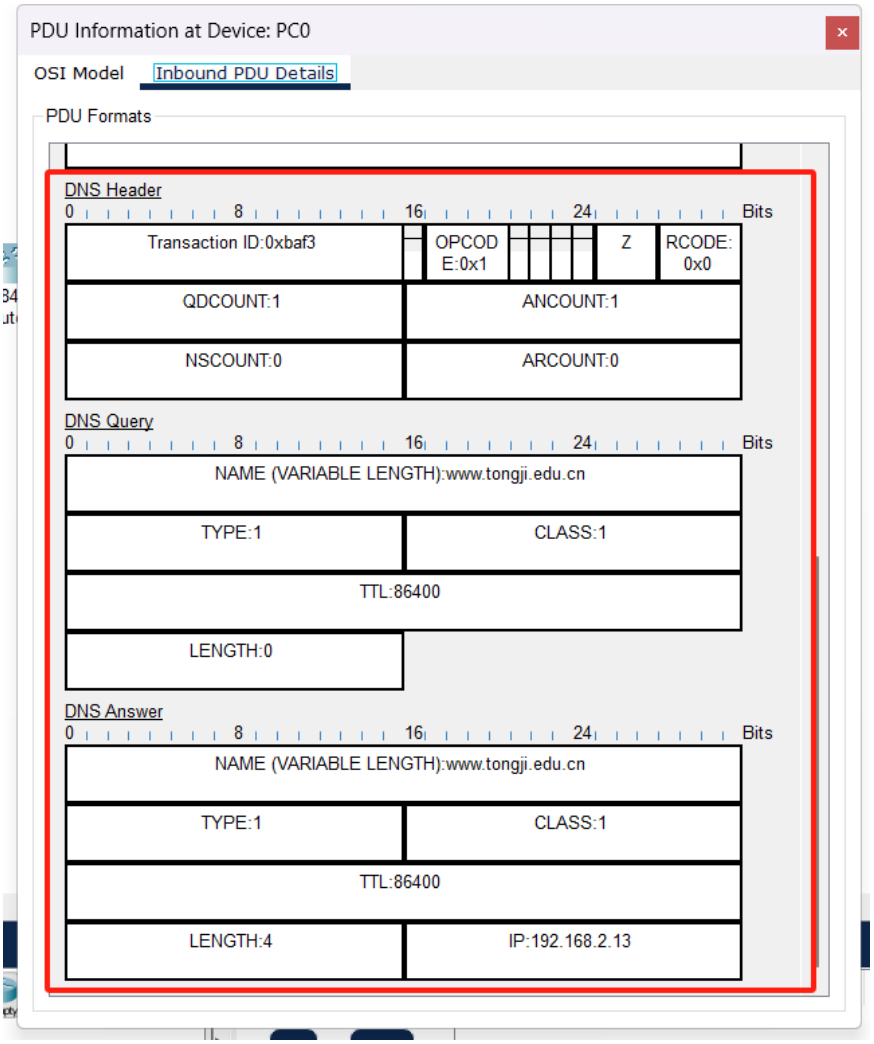


- 打开PC0浏览器，输入配置Web服务器的Web地址，产生DNS数据报文

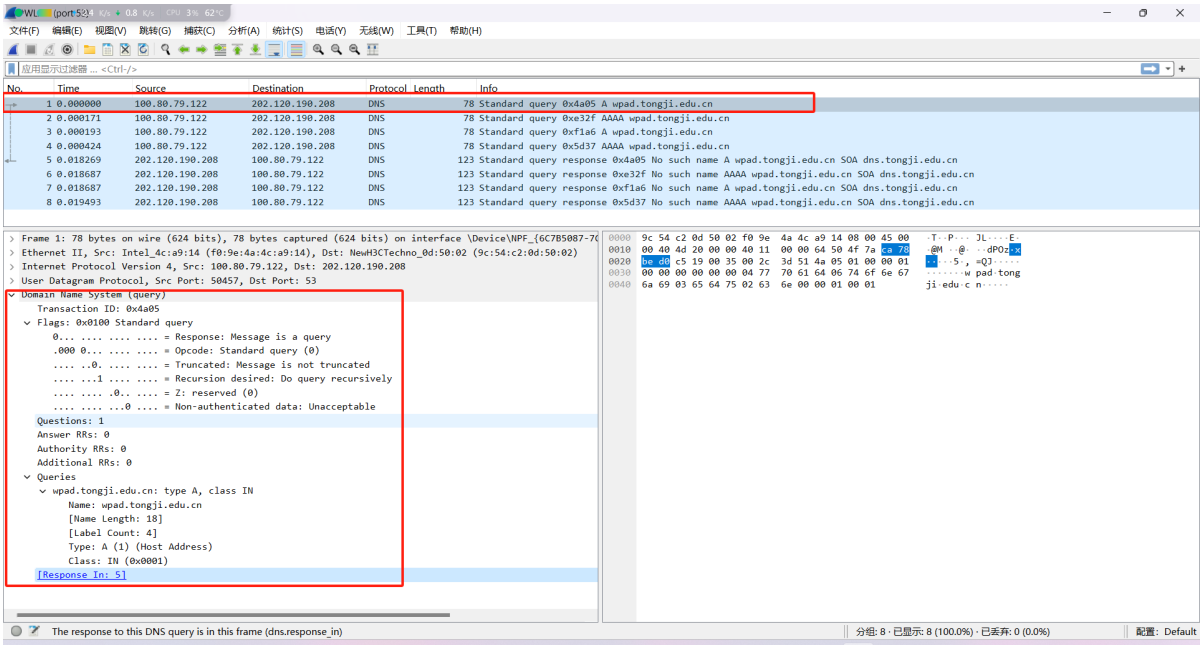




- 观察并分析DNS数据报文



- WireShark抓取DNS报文并分析



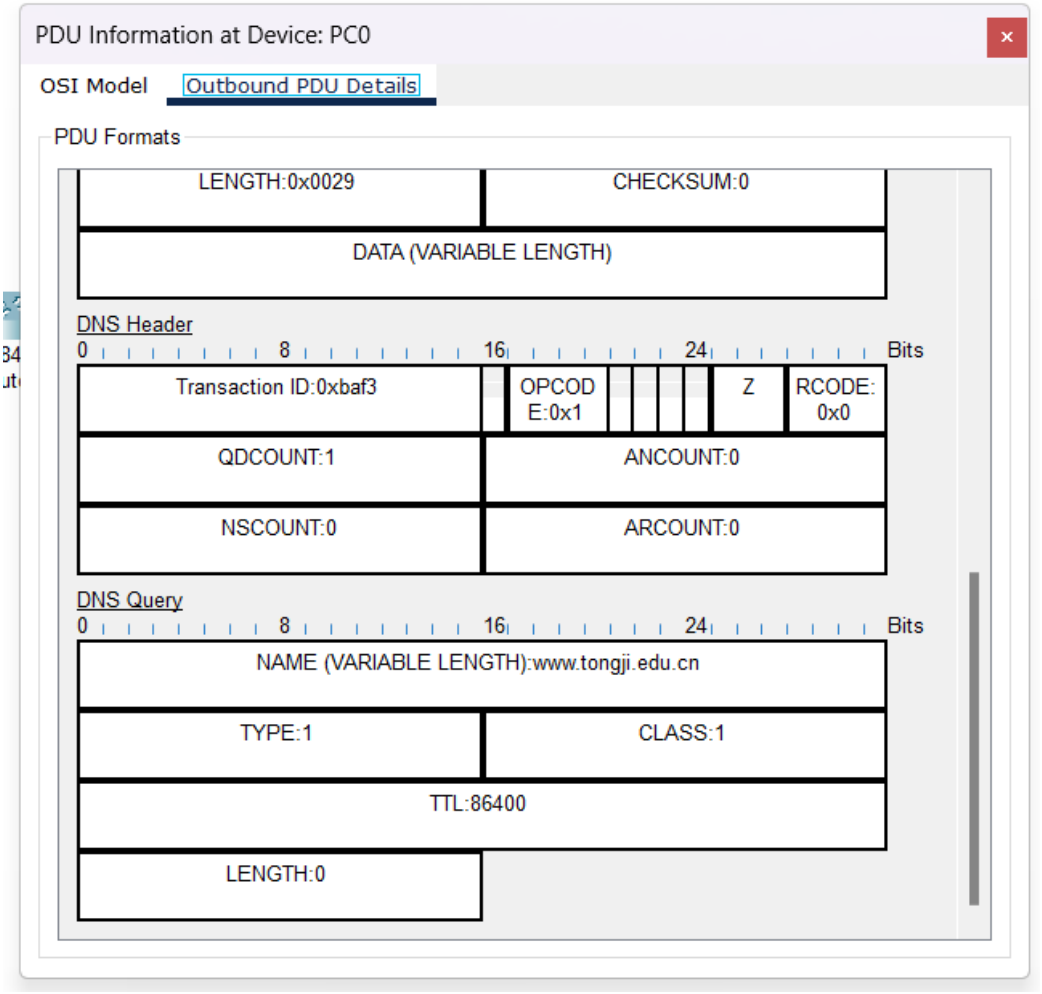
五、实验现象

- 分析在Packet tracer中DNS报文情况
  - DNS查询报文
    - Transaction ID为事务ID，DNS 报文的 ID 标识。对于请求报文和其对应的应答报文，该字段的值是相同的。通过它可以区分 DNS 应答报文是对哪个请求进行响应的。

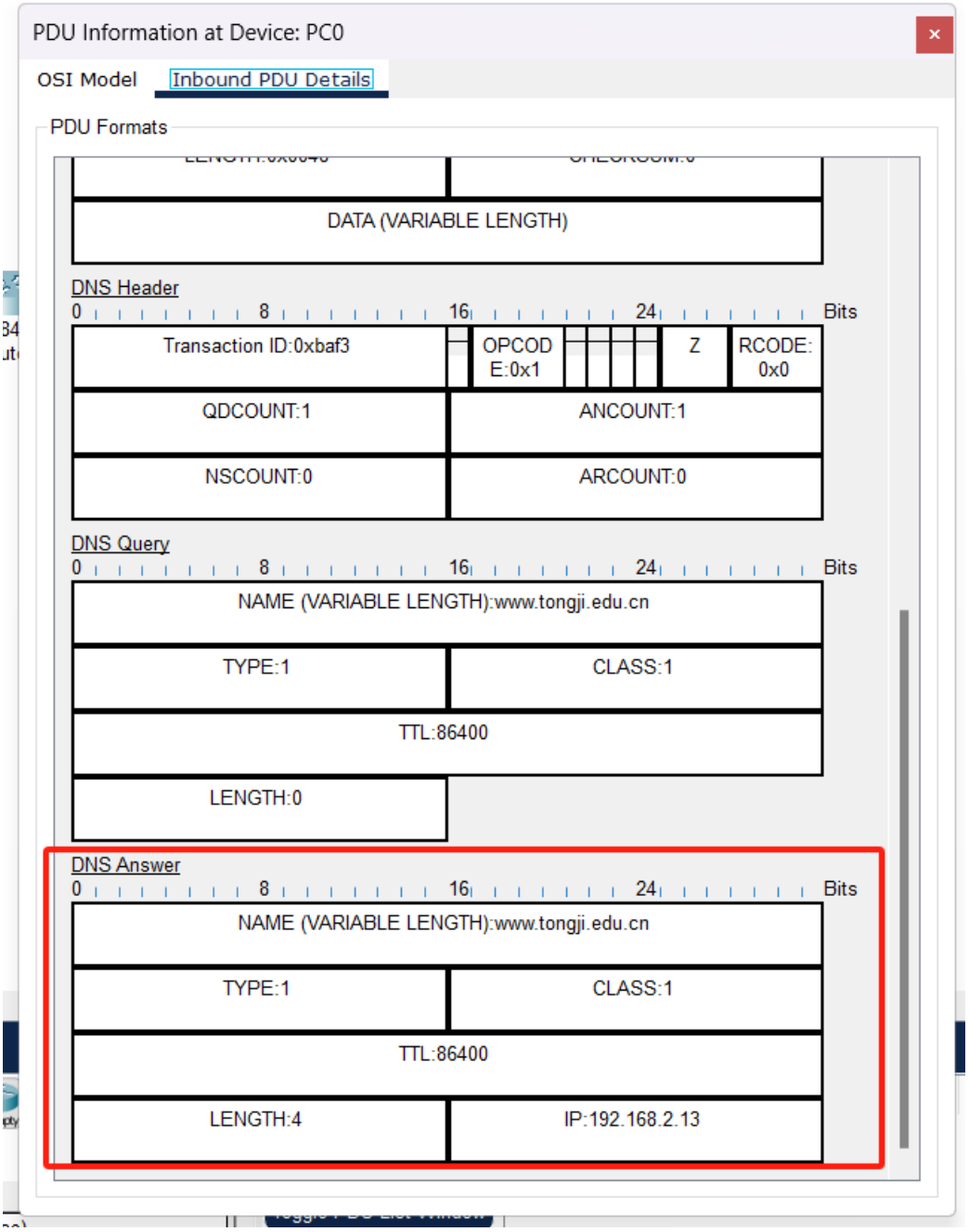
- 标志：DNS 报文中的标志字段。

QR	Opcode	AA	TC	RD	RA	Z	rcode

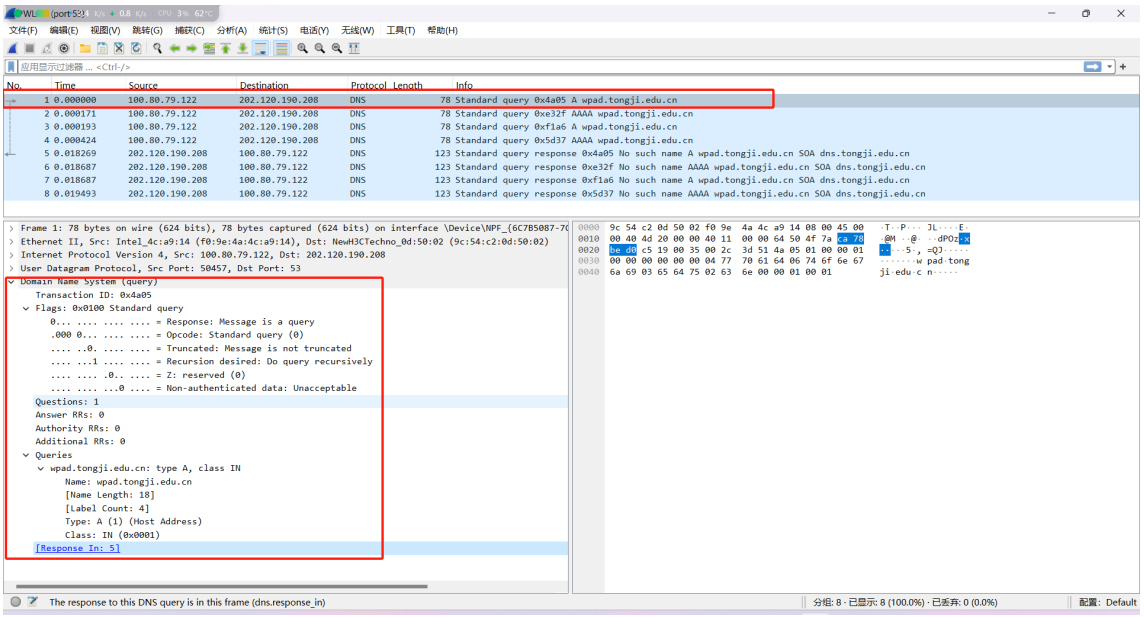
  - 标志字段中每个字段的含义如下：
    - QR（Response）：查询请求/响应的标志信息。查询请求时，值为 0；响应时，值为 1。
    - Opcode：操作码。其中，0 表示标准查询；1 表示反向查询；2 表示服务器状态请求。
    - AA（Authoritative）：授权应答，该字段在响应报文中有效。值为 1 时，表示名称服务器是权威服务器；值为 0 时，表示不是权威服务器。
    - TC（Truncated）：表示是否被截断。值为 1 时，表示响应已超过 512 字节并已被截断，只返回前 512 个字节。
    - RD（Recursion Desired）：期望递归。该字段能在一个查询中设置，并在响应中返回。该标志告诉名称服务器必须处理这个查询，这种方式被称为一个递归查询。如果该位为 0，且被请求的名称服务器没有一个授权回答，它将返回一个能解答该查询的其他名称服务器列表。这种方式被称为迭代查询。
    - RA（Recursion Available）：可用递归。该字段只出现在响应报文中。当值为 1 时，表示服务器支持递归查询。
    - Z：保留字段，在所有的请求和应答报文中，它的值必须为 0。
  - rcode（Reply code）：返回码字段，表示响应的差错状态。当值为 0 时，表示没有错误；当值为 1 时，表示报文格式错误（Format error），服务器不能理解请求的报文；当值为 2 时，表示域名服务器失败（Server failure），因为服务器的原因导致没办法处理这个请求；当值为 3 时，表示名字错误（Name Error），只有对授权域名解析服务器有意义，指出解析的域名不存在；当值为 4 时，表示查询类型不支持（Not Implemented），即域名服务器不支持查询类型；当值为 5 时，表示拒绝（Refused），一般是服务器由于设置的策略拒绝给出应答，如服务器不希望对某些请求者给出应答。
- QDCOUNT为报文请求段中的问题记录数，这里为1；
- ANCOUNT为报文回答段中的回答记录，因为这是查询报文，因此该字段为0
- NSCOUNT为报文授权段中的授权记录数，这里为0
- ARCOUNT为报文附加段中的附加记录数，这里为0
- NAME为查询名，即需要查询ip的域名，这里为`www.tongji.edu.cn`
- TYPEDNS 查询请求的资源类型。通常查询类型为 A 类型，表示由域名获取对应的 IP 地址。
- CLASS地址类型，这里为互联网地址，值为 1。
- TTL以秒为单位，表示资源记录的生命周期，一般用于当地址解析程序取出资源记录后决定保存及使用缓存数据的时间。它同时也可以表明该资源记录的稳定程度，稳定的信息会被分配一个很大的值。这里为86400秒.
- LENGTH资源数据长度，这里为0，因为还没有返回的资源数据



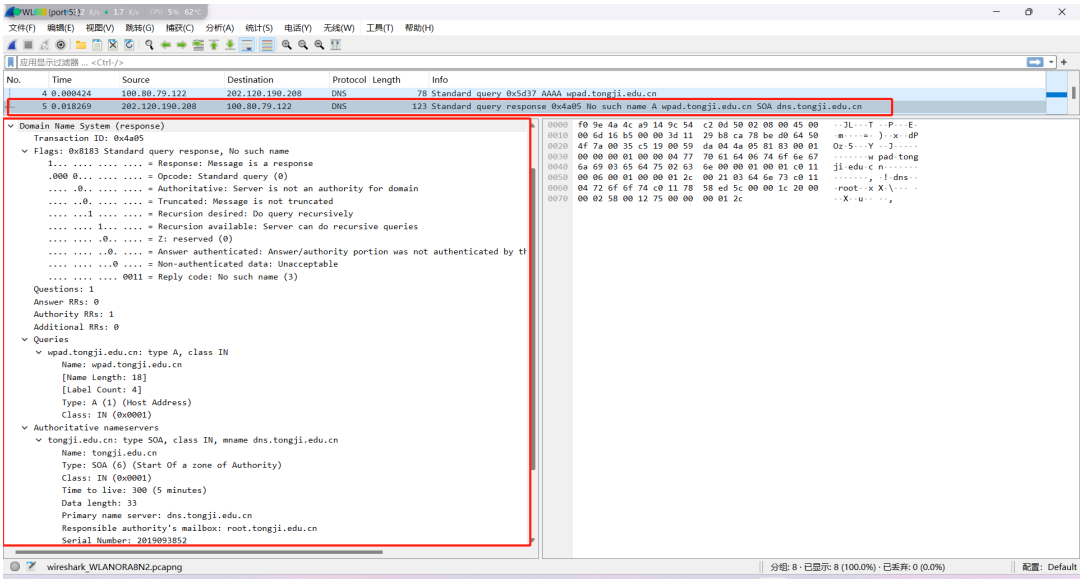
- DNS响应报文
  - 在DNS Answer中多了资源数据字段，资源数据长度为4
  - 资源数据，也就是域名对应的ip为192.168.2.13
  - 其余字段值和DNS Query的相同。



- 用WireShark抓取DNS数据包，查看并分析
  - 查询报文
    - 在查询报文中事务ID为0x4a05
    - 标识字段Recursion Desired为1
    - 问题计数为1
    - 回答资源记录数、权威名称服务器计数、附加资源记录数为0
    - 要查询的域名为`wpad.tongji.edu.cn`
    - 查询类型为A类型，表示由域名获取对应的 IP 地址
    - 查询类为1标识互联网地址。



- 响应报文
  - 在应答报文中，事务ID、回答资源记录数、权威名称服务器计数、附加资源记录数、查询类型、查询类和查询报文相同
  - 标识中Recursion Desired期望递归和Recursion Available可用递归为1
  - 生存时间为300秒
  - 资源数据长度为33



六、实验结论

- 实验结论如下：

1. **DNS解析的必要性和原理**：
   - DNS解析是网络通信中不可或缺的一部分，它将用户输入的域名转换为计算机可以识别的IP地址，从而实现网络资源的访问。
   - DNS采用分布式层次结构，通过递归查询和迭代查询等机制，提高了解析效率和系统的可靠性。
2. **Packet Tracer中的DNS报文分析**：
   - 通过Packet Tracer实验，成功模拟了DNS查询和响应的全过程。分析了DNS客户端与DNS服务器之间的通信，了解了DNS报文的构造和传输过程。

    - 实验展示了从客户端输入域名到最终获得IP地址的详细步骤，包括查询本地缓存、递归查询和迭代查询等。
3. **WireShark抓包分析**：
    - 使用WireShark抓取实际的DNS数据包，深入分析了DNS报文的各个字段，包括DNS消息头、查询报文和应答报文中的详细信息。
    - 通过抓包分析，验证了DNS解析过程中的各个步骤，观察到了实际网络中DNS查询和响应的具体数据和行为。
4. **对DNS系统的理解**：
    - 实验加深了我们对DNS系统的理解，尤其是DNS服务器之间的分工和协作机制。
    - 了解了DNS缓存的作用，以及不同层次的DNS服务器在域名解析中的具体功能。

- 通过本次实验，我不仅掌握了DNS解析的基本原理和过程，还学会了使用网络分析工具进行数据包的抓取和分析。这些知识和技能为我们在网络通信领域的进一步学习和研究打下了坚实的基础