【实验名称：UDP数据包分析实验】

学生姓名：李雪菲 合作学生：无

实验地点：济事楼330 实验时间：2025-05-15

【实验目的】

1. 了解 UDP 协议的特点，学习 UDP 协议的无连接、不可靠传输和简单的错误检测机制。

2. 分析 UDP 报文结构，通过实验了解 UDP 数据报的首部格式，包括源端口号、目的端口号、长度和校验和字段的作用。

3. 掌握如何使用网络分析工具：学生将使用工具如 Wireshark 来捕获和分析 UDP 数据包，这不仅包括识别基本的 UDP 流量，还包括深入理解数据包中的信息，如端口号、数据长度和可能的传输错误。

4.通过分析 UDP 通信过程中的数据包，学生可以学习如何诊断网络中的问题，例如丢包、端口不可达错误以及由校验和错误导致的数据包丢弃。

【实验原理】

一、UDP 概述

UDP（用户数据报协议）是一种位于网络传输层的协议，它在 IP 的数据报服务之上增加了基本的服务功能，包括复用与分用服务以及差错检测。UDP 是一个简单的面向消息的传输协议，不像 TCP（传输控制协议）那样提供可靠性保证， 也不进行连接管理。

二、UDP 应用特点

UDP（用户数据报协议）的应用特点主要体现在其设计和功能的简洁性以及对于特定应用环境的适用性。以下是 UDP 的主要应用特点：

1. 无连接性：UDP 是一个无连接的协议，这意味着在数据传输前不需要建立连接，从而减少了通信的延迟。这种特性使得 UDP 非常适合需要快速数据传输 的场景，例如 DNS 查询。

2. 简单的首部结构：UDP 的首部只有 8 字节，比 TCP 的 20 字节首部要小得多。 这种简单的首部结构减少了数据传输的总开销，尤其是在传输小量数据时更为高效。

3. 尽最大努力的交付：UDP 不保证数据的可靠交付。它不会对丢失的数据包进行重传，也没有确认机制，这样可以避免在网络条件不佳时造成的延迟。

4. 无拥塞控制：UDP 没有内置的拥塞控制机制，因此它允许应用层更好地控制数据的发送时间和频率。这对于实时应用（如视频流、实时游戏）来说非常重要，因为这些应用更关注延迟而不是每个数据包的完整性。

5. 面向报文：UDP 是面向报文的，它保持应用层数据的边界。这意味着 UDP 一次发送一个完整的消息，并保持消息的完整性。应用层在接收时也必须一次性完整地接收整个消息，这简化了应用层的处理逻辑。

三、UDP 报文格式

UDP（用户数据报协议）报文的格式设计简单而高效，使其在网络中的处理 非常快速。UDP 数据报整体分为首部和数据两部分，封装在 IP 数据报中进行传输。



【实验设备】

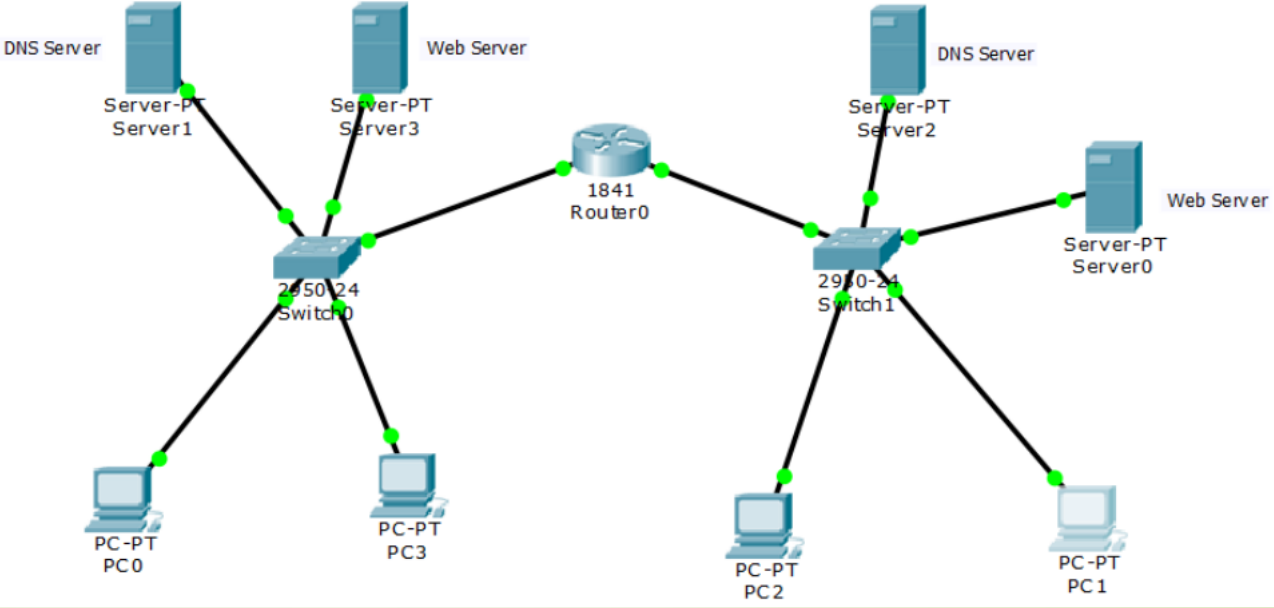
1. 一台电脑
2. Cisco packet tracer 仿真软件
3. Wireshark 仿真软件

【实验步骤】

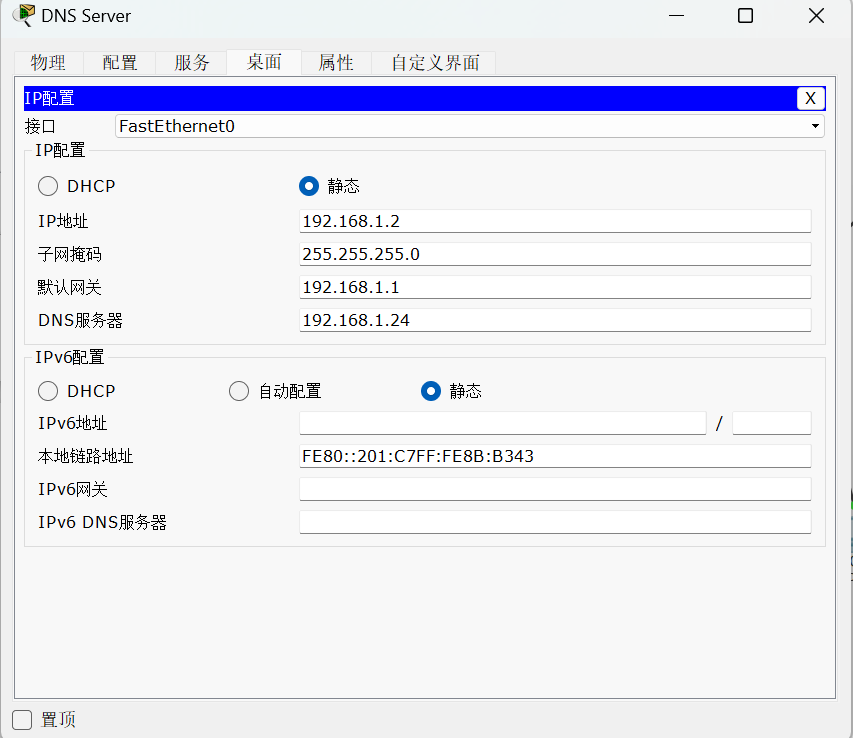
1. 搭建网络结构图
2. 设置WEB服务器和简单的DNS服务器
3. 打开PC0浏览器，输入配置Web服务器的 Web 地址，如www.tongji.edu.cn或 www.test.com，产生UDP数据报文
4. 分析在 Packet Tracer 中 UDP 报文情况。
5. 用 WireShark 抓取 UDP 数据包，查看 UDP 报文字段内容，并解读。

【实验现象】

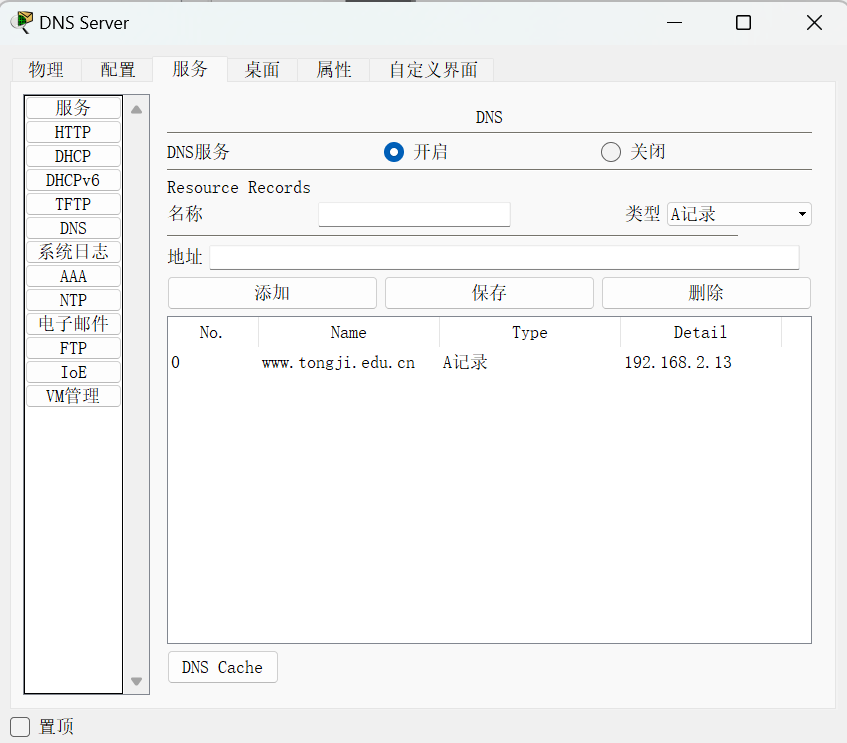
1. 搭建网络结构图



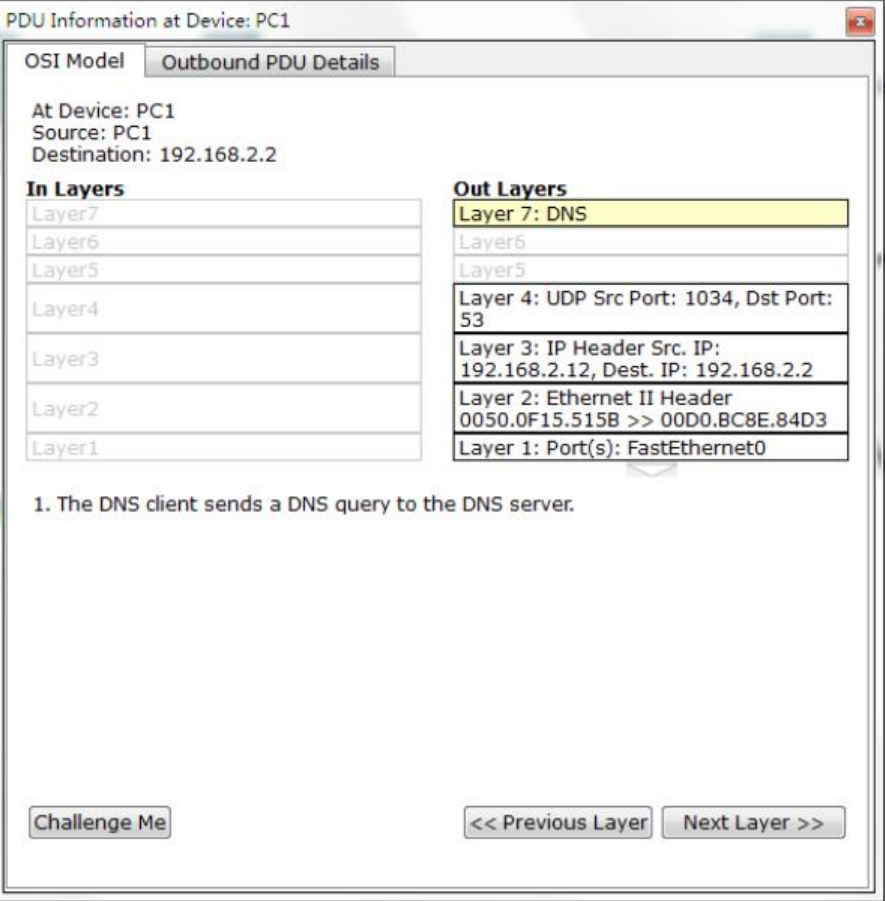
1. 设置WEB服务器和简单的DNS服务器

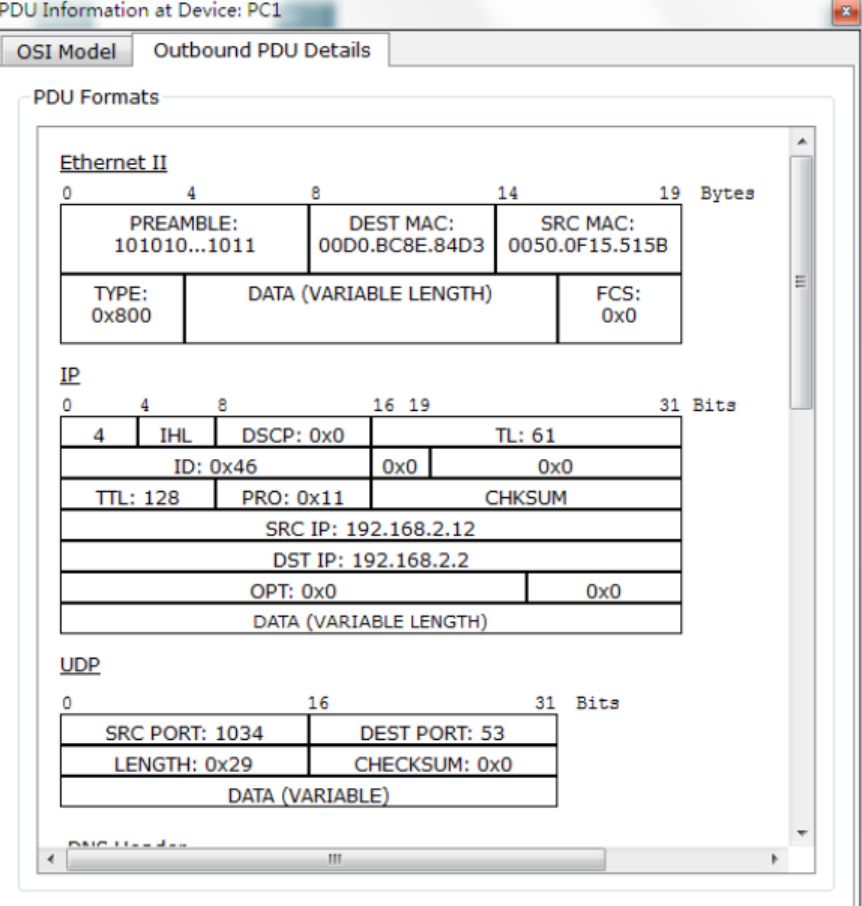


1. 打开PC0浏览器，输入配置Web服务器的 Web 地址，如www.tongji.edu.cn或 www.test.com，产生UDP数据报文



1. 分析在 Packet Tracer 中 UDP 报文情况。





在 Packet Tracer 中，UDP 报文的详细情况如下：

输入 PDU 详情（Inbound PDU Details）

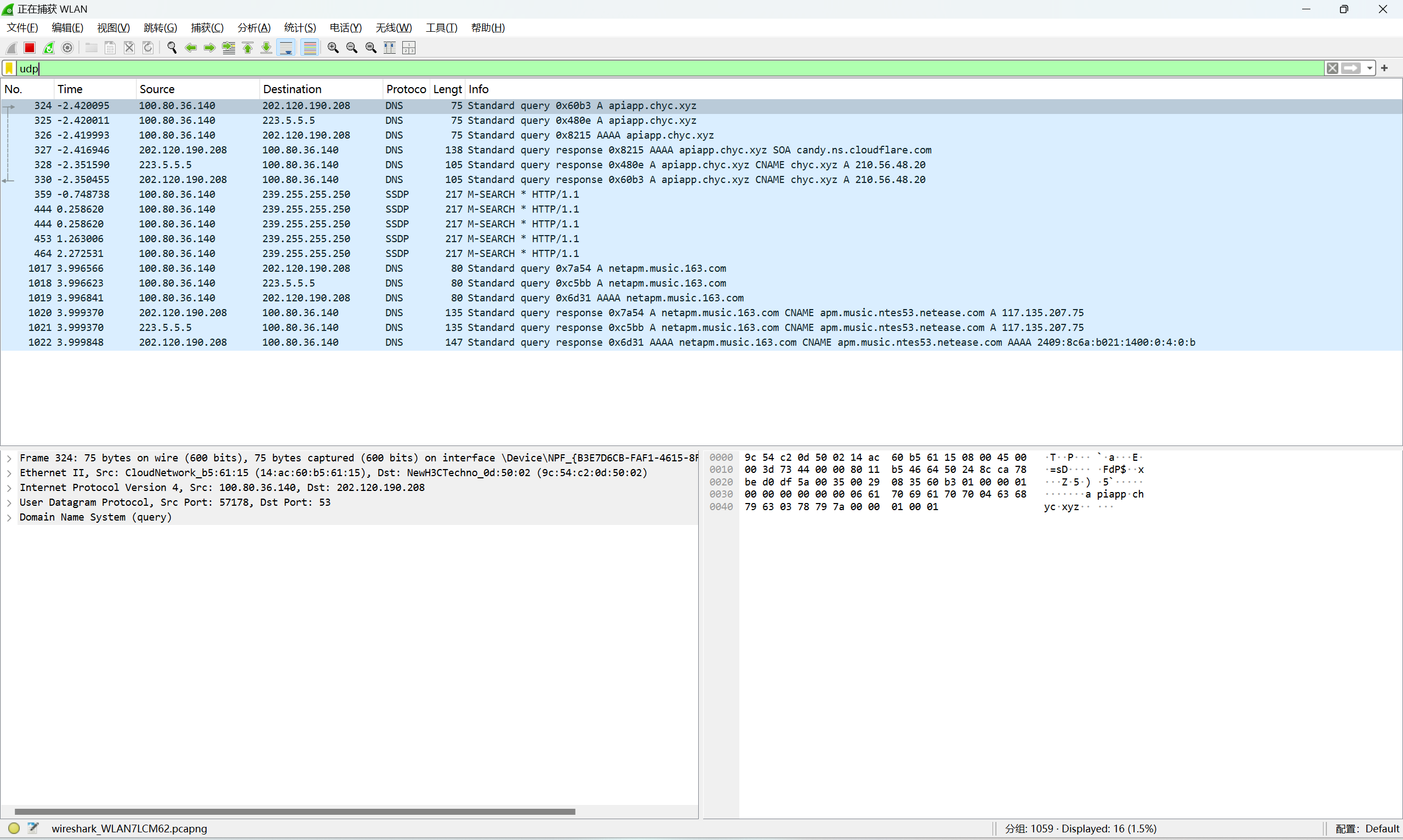
源端口（Source Port）：表示这是一个来自 DNS 服务器的响应。

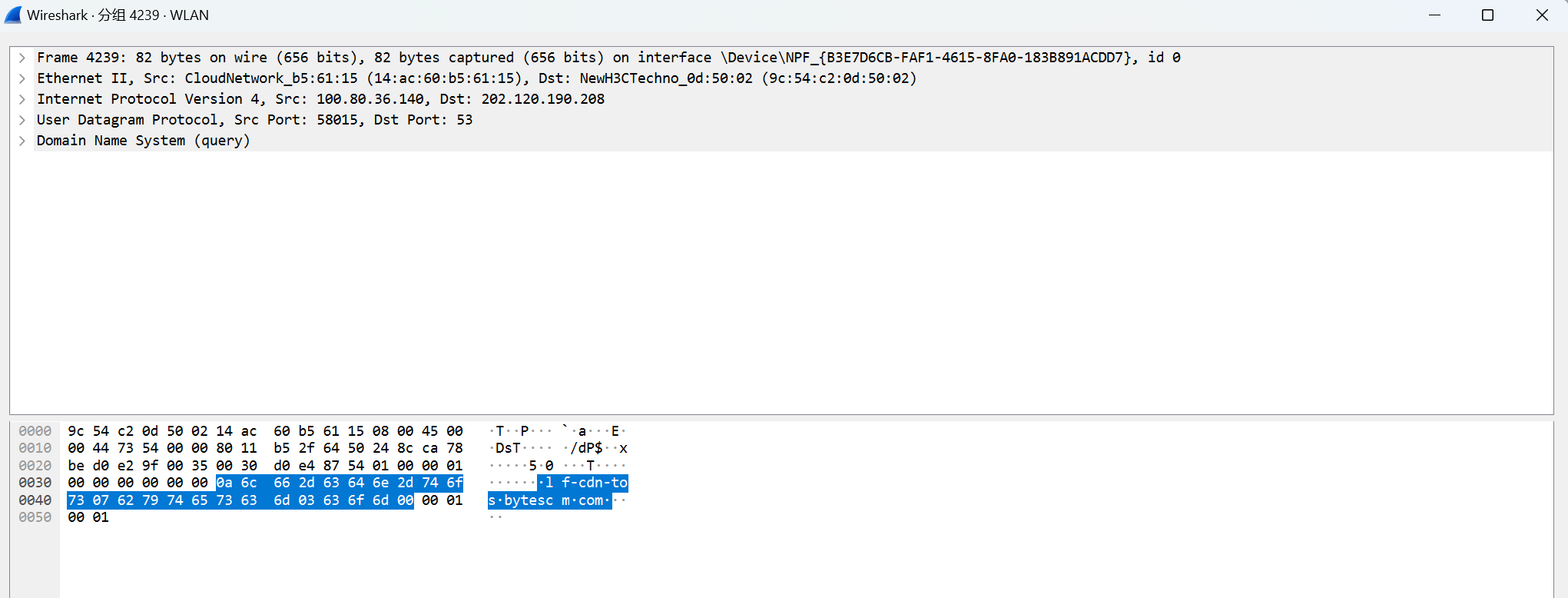
目的端口（Destination Port）：这是客户端的端口，用于接 收 DNS 响应。

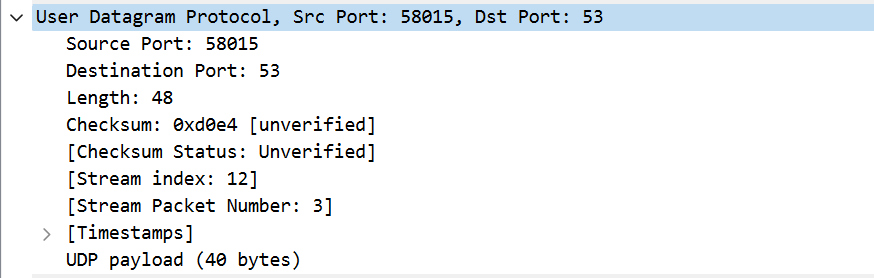
长度（Length）：这表示 UDP 报文的长度，包括首部和数据， 十进制为 41 字节。

校验和（Checksum）：校验和用于错误检测，这里显示为 0，可 能是在某些网络环境下不使用或者未被计算。

5.用 WireShark 抓取 UDP 数据包，查看 UDP 报文字段内容，并解读。







Source Port (源端口): 58015,发送方（客户端）使用的临时端口号，用于接收 DNS 响应。

Destination Port (目的端口): 53,目标服务端口（DNS 协议默认端口）。

Length (长度): 48,UDP 首部（8 字节） + 数据部分（40 字节）的总长度。

Checksum (校验和): 0xd0e4,用于检测数据完整性，此处显示 [unverified]（未验证），实际由接收方计算校验。