**Lab25\_DNS实验项目**

学生姓名：苏家铭 合作学生：无

实验地点：宿舍 实验时间：2023年12月20日

**【实验目的】**

本实验旨在探究DNS（Domain Name System）的功能与运作机制，通过模拟和分析DNS域名解析过程，深入理解域名转换为IP地址的工作原理，并探讨DNS服务在网络通信中的重要性与作用。

**【实验原理】**

DNS的作用是将人类可读的域名转换为计算机可识别的IP地址。这个过程类似于电话簿中查找人名并找到对应的电话号码。当你在浏览器中输入一个域名（比如www.example.com），你的计算机首先会向DNS服务器发出请求，询问这个域名对应的IP地址是什么。

DNS服务器就像是互联网的电话簿，它存储了大量域名和对应的IP地址。当DNS服务器接收到你的请求时，它会查找域名对应的IP地址并将这个信息返回给你的计算机。一旦你的计算机得到了这个IP地址，它就能够与相应的服务器建立连接，下载网页内容或者执行其他网络通信的操作。

这种域名到IP地址的转换过程使得我们可以更方便地访问互联网，因为我们更容易记住有意义的域名，而不是一串数字。DNS的作用是至关重要的，它让互联网更加易用和友好，同时也帮助网络通信更高效地进行。

DNS过程

DNS客户端提取域名：当用户在浏览器中输入一个URL时，浏览器会提取其中的域名部分，如“www.baidu.com”。DNS查询报文发送: 用户的计算机会向配置的DNS服务器发送查询报文，这个报文中包含了需要解析的域名信息。DNS服务器处理请求: DNS服务器收到查询报文后，会尝试在自身的缓存中查找相应的IP地址。如果找到了，就直接返回IP地址；如果没有找到，DNS服务器会向其他DNS服务器发送查询，直到找到对应的IP地址为止。返回IP地址: 一旦找到了对应的IP地址，DNS服务器将其作为回答打包成报文发送回用户的计算机。建立TCP连接: 用户的浏览器收到DNS返回的IP地址后，便可以使用这个IP地址向相应的服务器发起TCP连接，以请求网页内容或执行其他网络通信操作。

DNS服务的体系架构

DNS（Domain Name System）的主要作用是将人类可读的域名转换为计算机能够理解的IP地址。这种转换过程是由分布在全球的DNS服务器共同完成的。

DNS的体系架构和工作方式是一个分布式的体系，它避免了单一DNS服务器成为单点故障，同时能够应对因特网上数量巨大并且不断增长的主机。DNS的架构包含了不同类型的DNS服务器：

1. 根DNS服务器（Root DNS Servers）: 这些服务器位于DNS层次结构的最顶层，它们存储着整个DNS系统的基础信息，并负责指向顶级域名服务器。根DNS服务器并不直接提供域名解析服务，而是指导查询流向顶级域名服务器。
2. 顶级DNS服务器（Top-Level Domain Servers）: 这些服务器负责管理顶级域名（如.com、.org、.net等），并记录着下一级DNS服务器的信息，比如权威DNS服务器。
3. 权威DNS服务器（Authoritative DNS Servers）: 这些服务器存储着特定域名下的具体IP地址记录。当DNS客户端发送查询请求时，最终会到达权威DNS服务器，它提供所需域名对应的IP地址信息。

DNS（Domain Name System）是一个以层次结构和分布式数据库为基础的系统，用于将人类可读的域名转换为计算机可识别的IP地址。这种层级结构形成了域命名空间，使每个域名都能在DNS树中唯一标识位置。全限定域名（FQDN）如"im.qq.com"在这个结构中扮演着重要角色，完整地指明了主机在DNS分层树中的位置。这种层级结构使用点来分隔，描述了域名之间的层次关系。

在DNS域名空间的组织方式中，各种类型的域名被定义和使用。顶级域名（TLD）和次级域名（Subdomain）在这个层级结构中扮演不同的角色。同时，DNS数据库中包含多种资源记录（RR），例如SOA、NS、A、MX、CNAME等。这些记录指定了管理域的权威服务器、域名服务器、IP地址映射、邮件交换服务器等重要信息。

管理和分配是DNS系统运作的关键。互联网域名系统由注册机构负责管理，他们负责分配和管理各种顶级域，包括组织和国家/地区的顶级域。这些域名使用缩写或特定标识符，例如国家/地区的域名缩写或两个字母标识。这种组织结构使得DNS系统能够高效、准确地管理和解析域名，确保了全球范围内域名的唯一性和可用性。

DNS服务的工作过程是一个分层的查询系统。当DNS客户机需要解析特定名称时，它会发送查询消息到本地DNS服务器，其中包括完全限定的域名（FQDN）、查询类型和DNS域的指定类别。这个过程的查询可以是递归或迭代的。

递归查询是指本地DNS服务器代表客户机向其他DNS服务器查询并获得最终答案，而迭代查询是指客户机自己向其他DNS服务器发送查询，并根据返回的信息向下一个服务器查询，直到获得最终答案。

整个DNS查询过程包括多种方式的解析。客户机有时会利用缓存信息直接回答查询，本地DNS服务器也会使用自身的缓存或代表请求客户机查询其他DNS服务器，完成整个名称解析过程。

DNS解析顺序涉及多个阶段：

1. 浏览器、系统和路由器缓存的查找。
2. ISP（互联网服务提供商）DNS缓存的查询。
3. 根域名服务器的查询，若无则返回管辖范围内的顶级域名服务器IP。
4. 顶级域名服务器的查询，若无则返回管辖范围内的主域名服务器IP。
5. 主域名服务器的查询，直至找到正确记录并将结果保存至本地DNS缓存。

**【实验设备】**

PC机一台，并安装有Cisco Packet Tracer软件

**【实验步骤】**

构建网络拓扑。

配置DHCP，注意这里需要指定DNS服务器的IP地址。

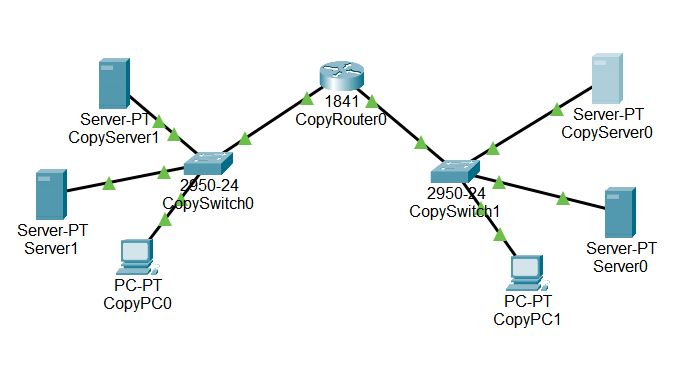
配置域名。

在仿真模式中发送通过域名发送请求。

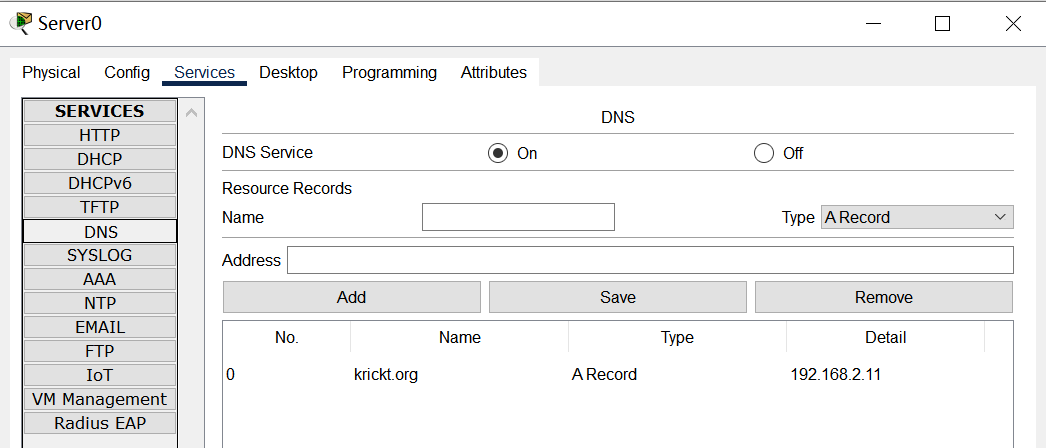
查看DNS。

在wireshark中DNS报文抓取并分析。

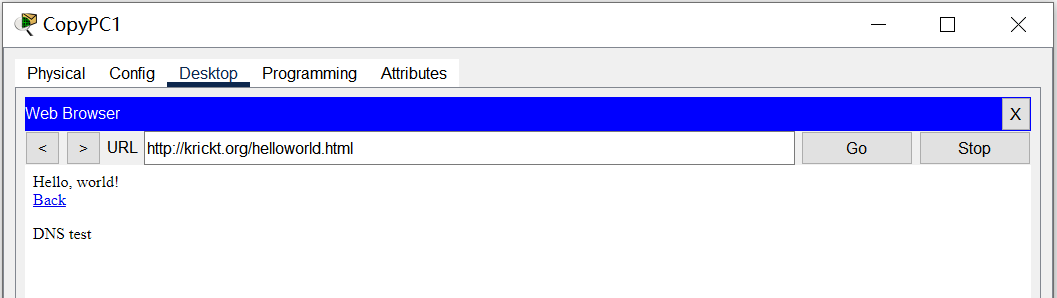
**【实验现象】**



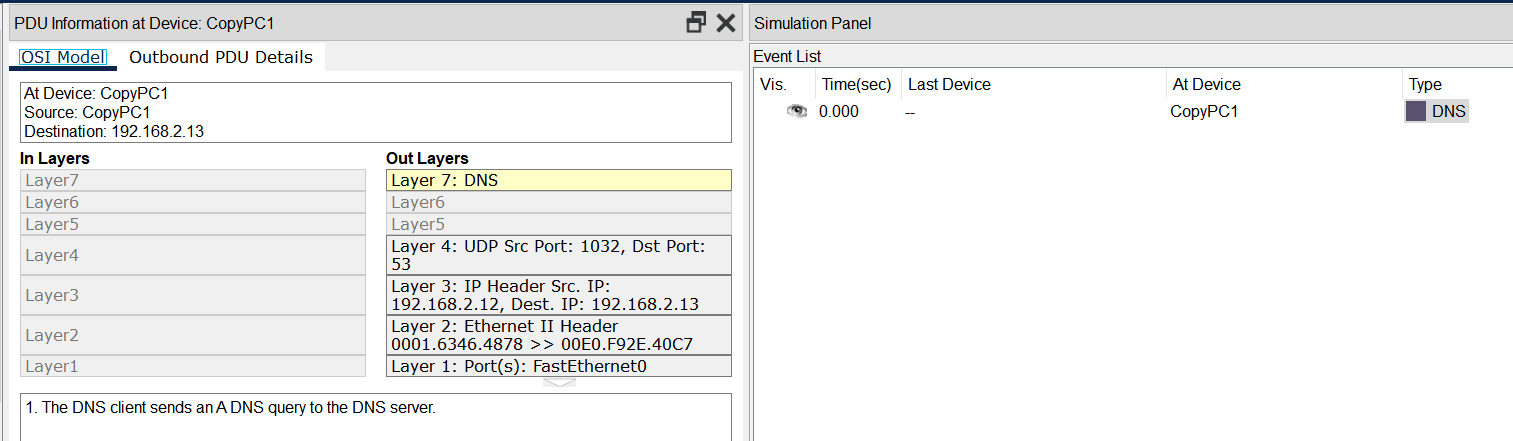
网络拓扑结构



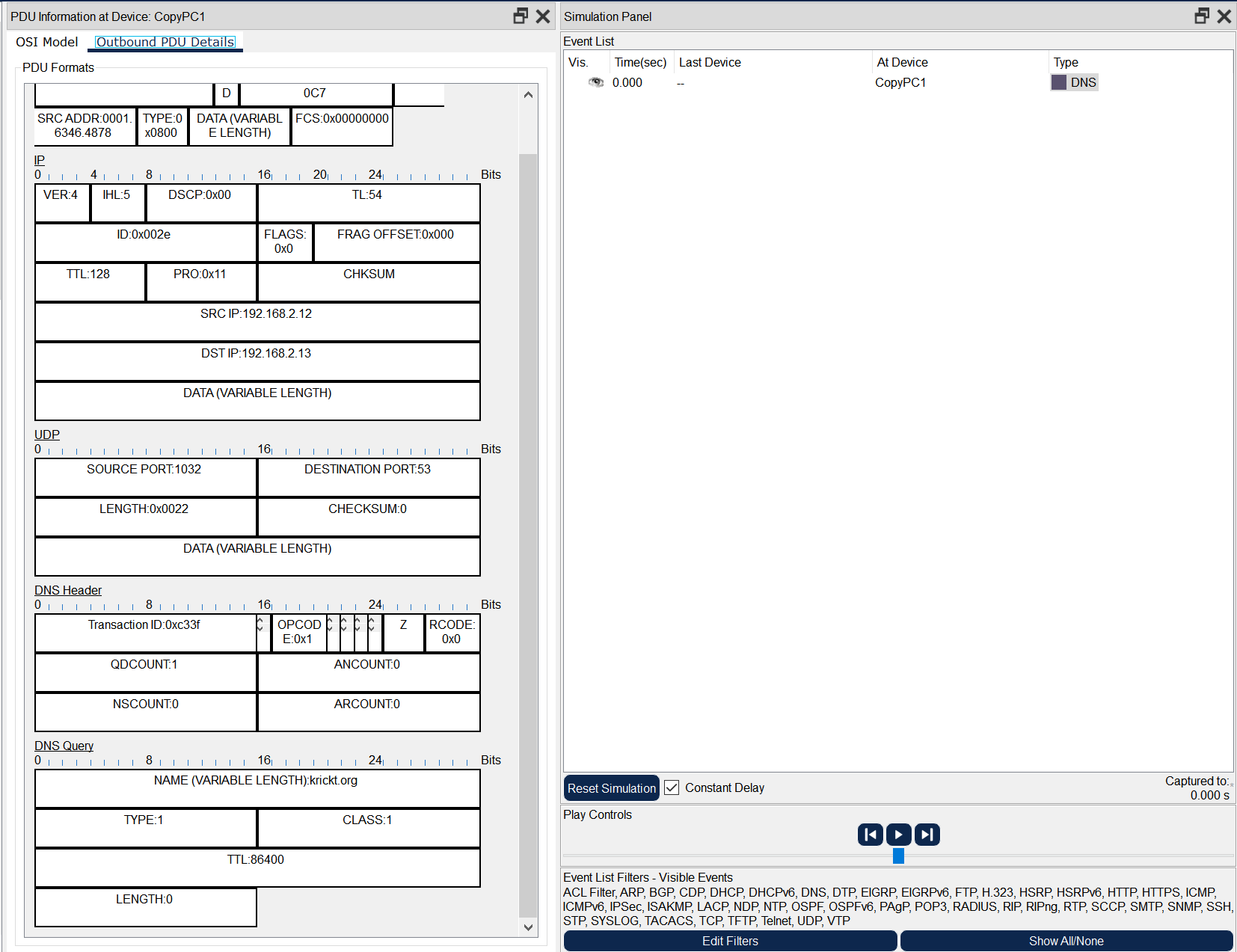
设置域名



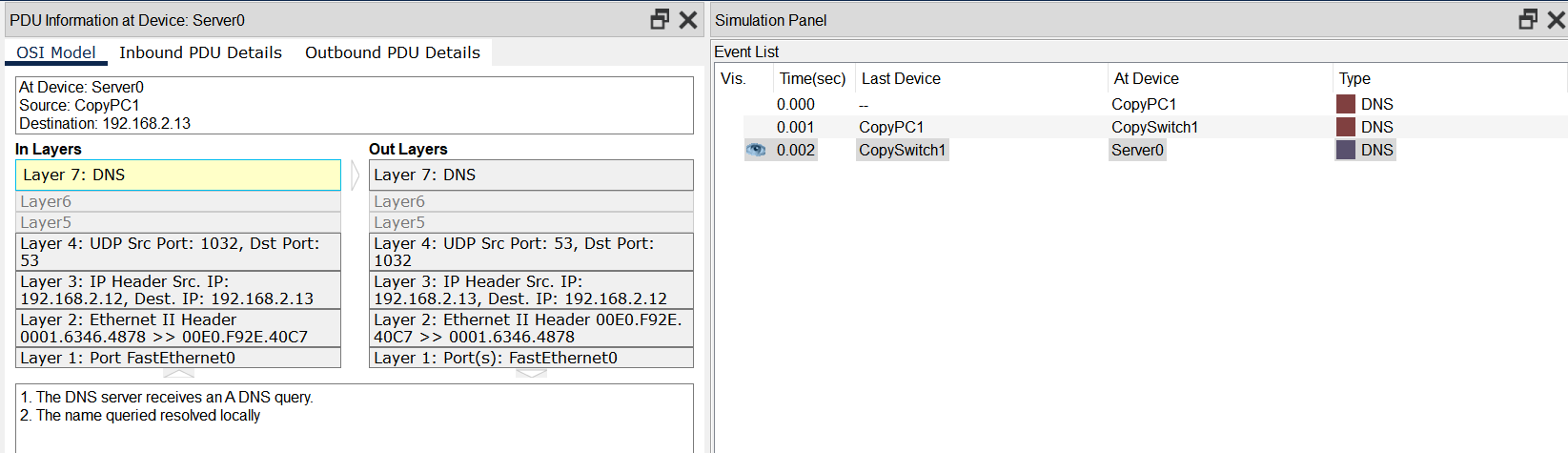
访问网页



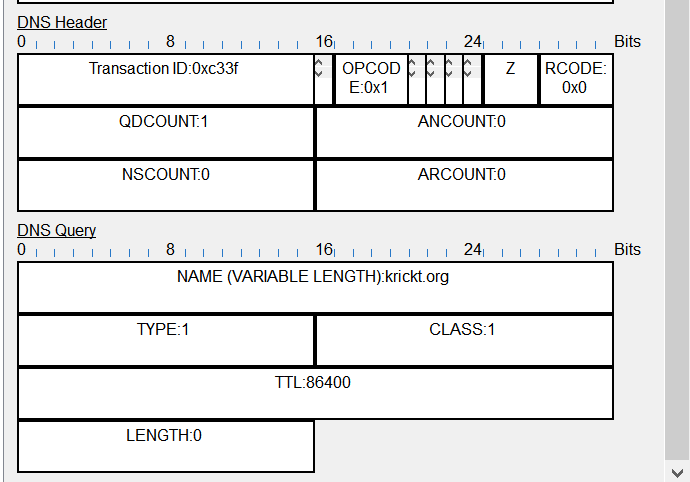
客户端发出请求



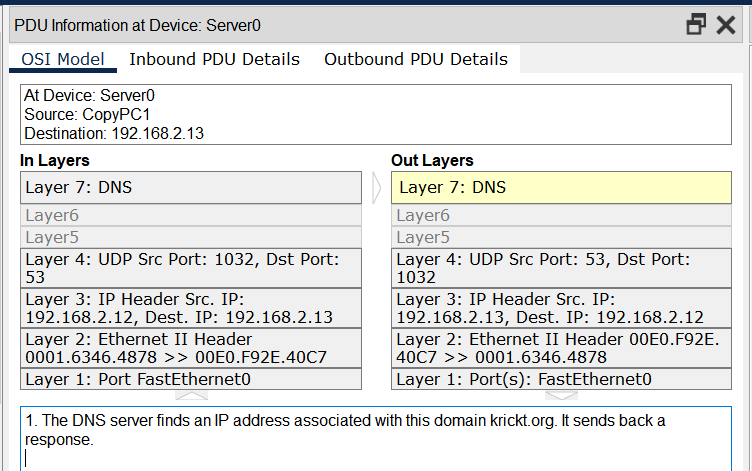
发出DNS查询格式



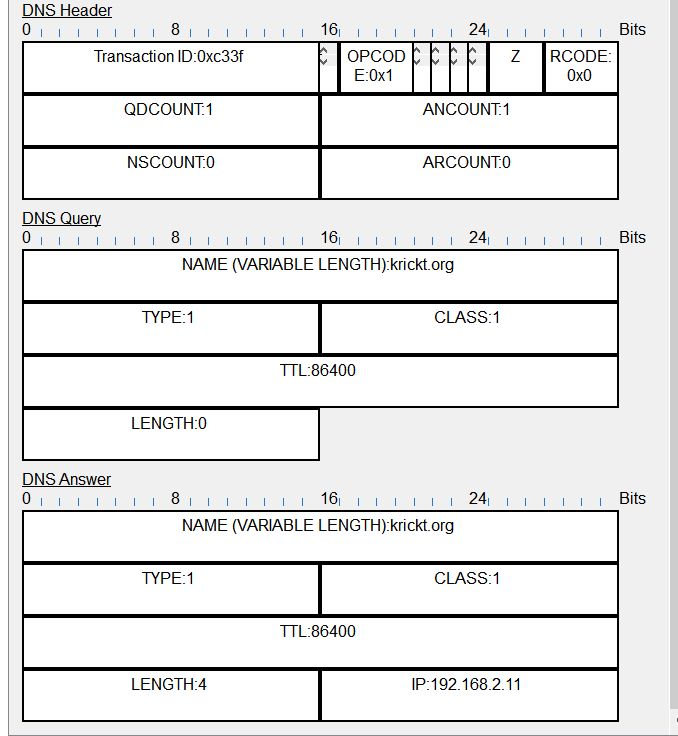
DNS服务器收到请求



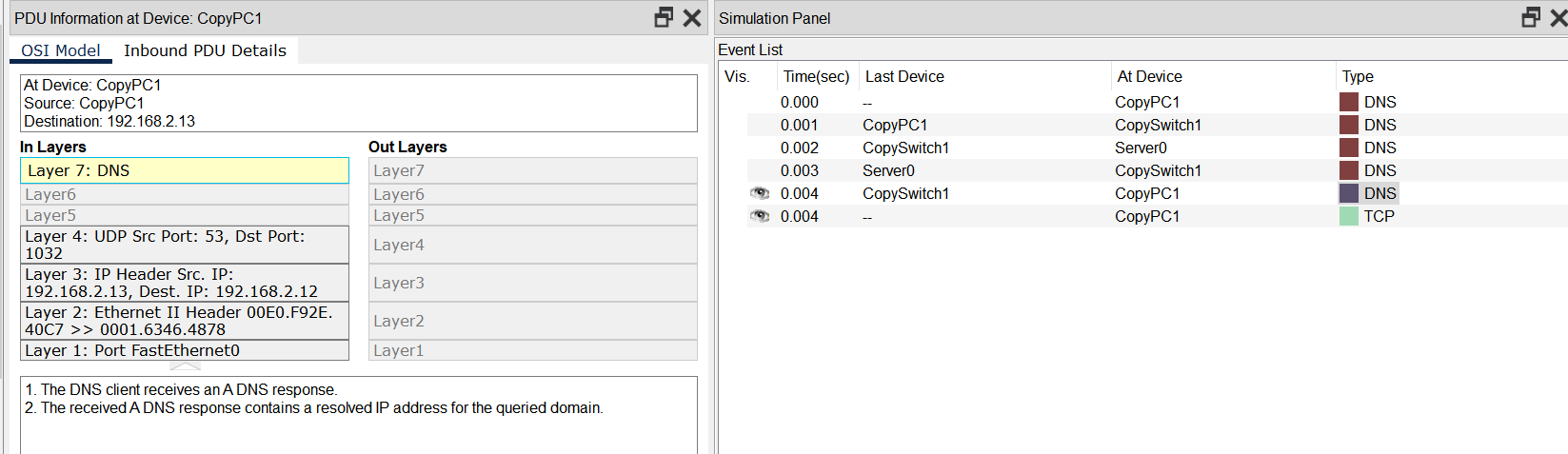
收到的请求格式



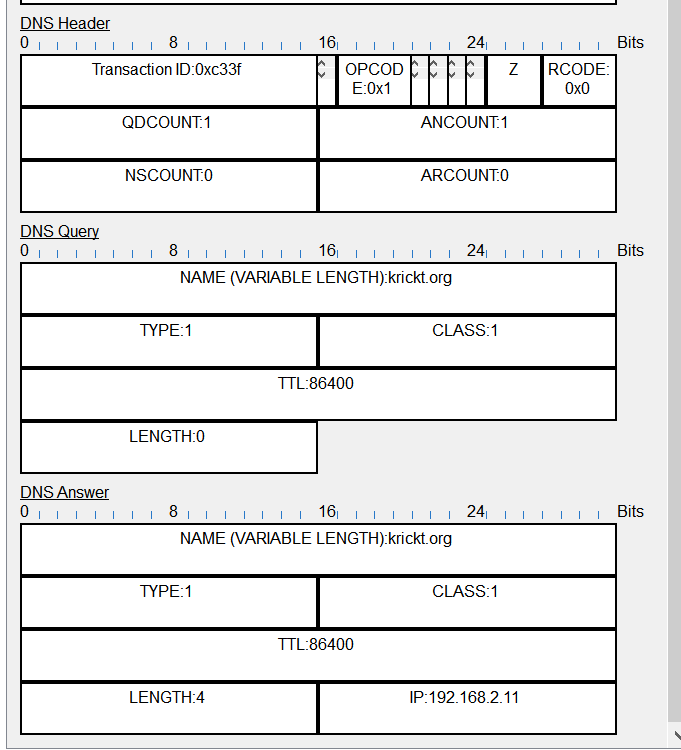
DNS服务器响应请求



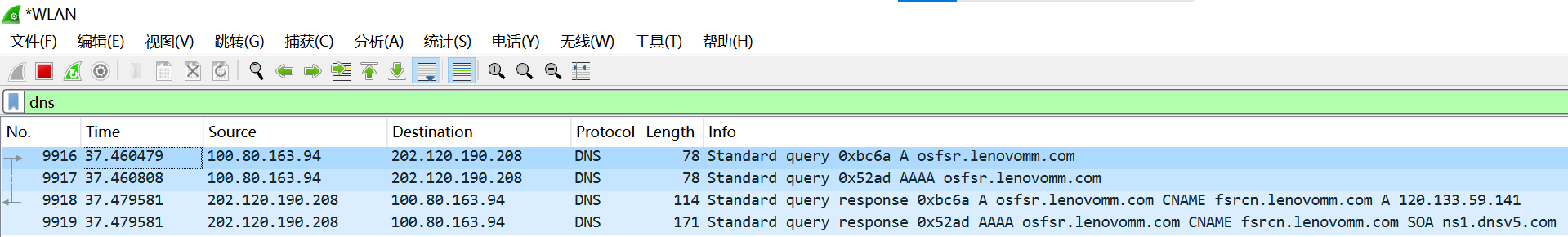
响应格式



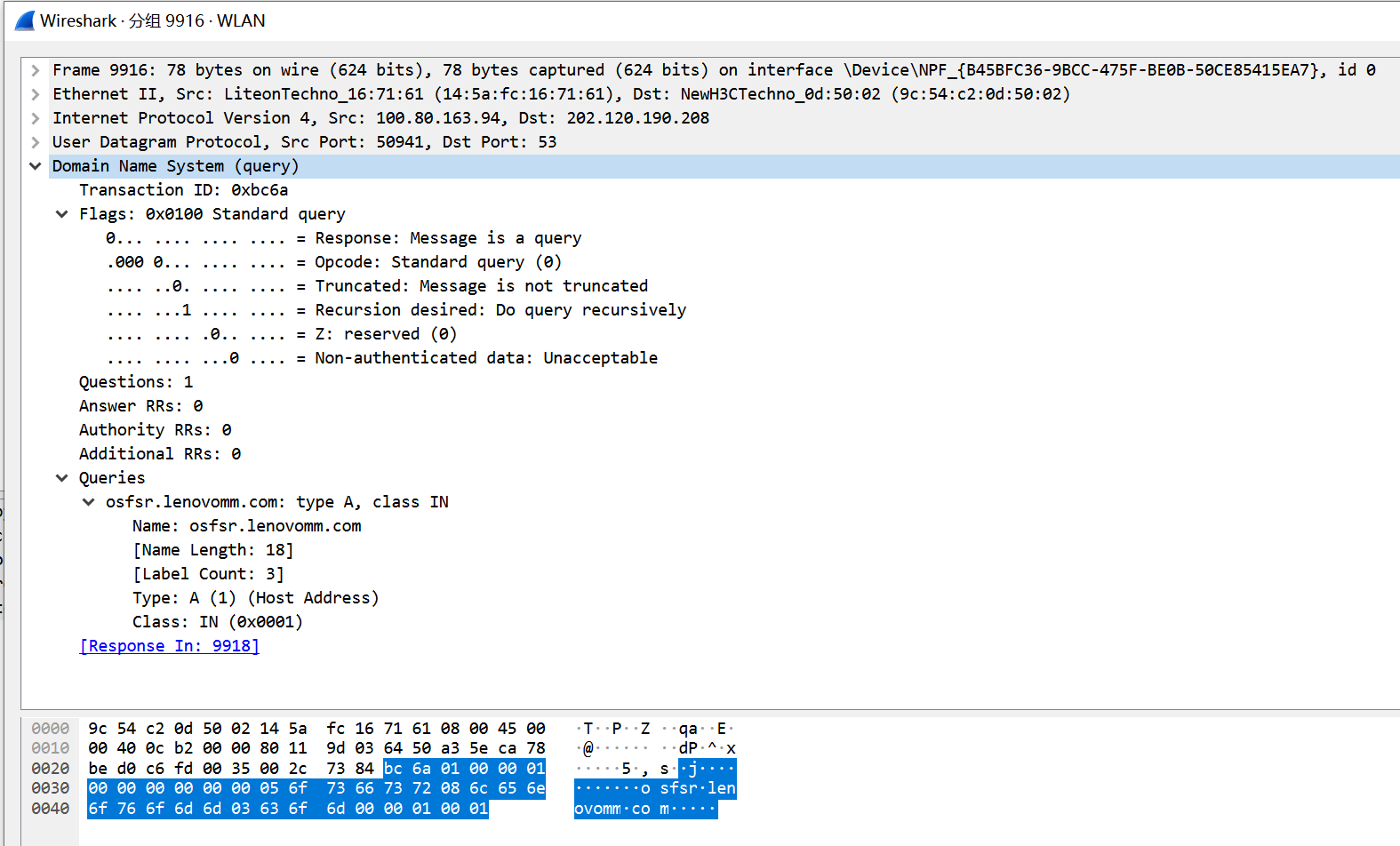
客户端收到响应



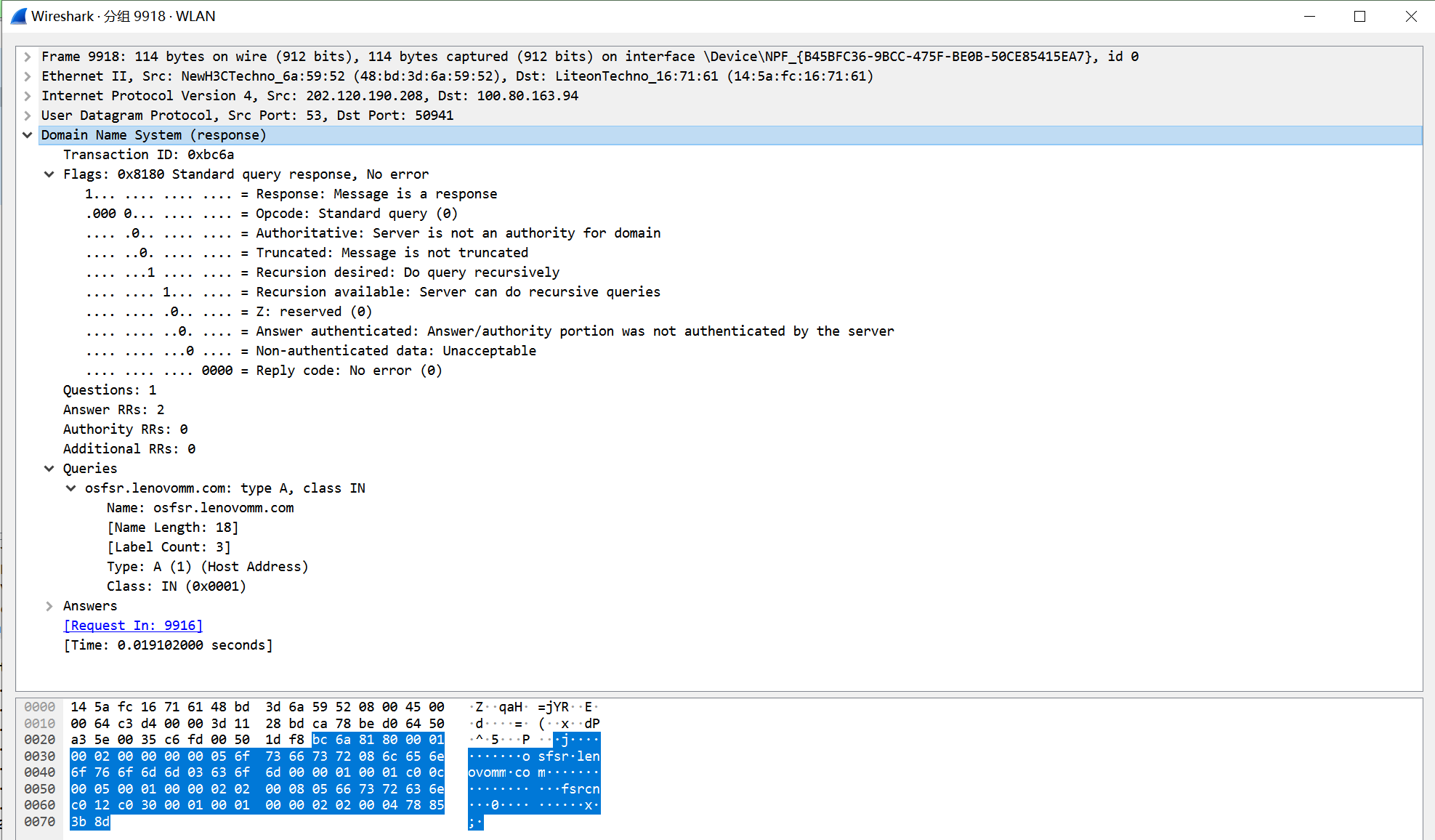
响应格式



wireshark查询结果

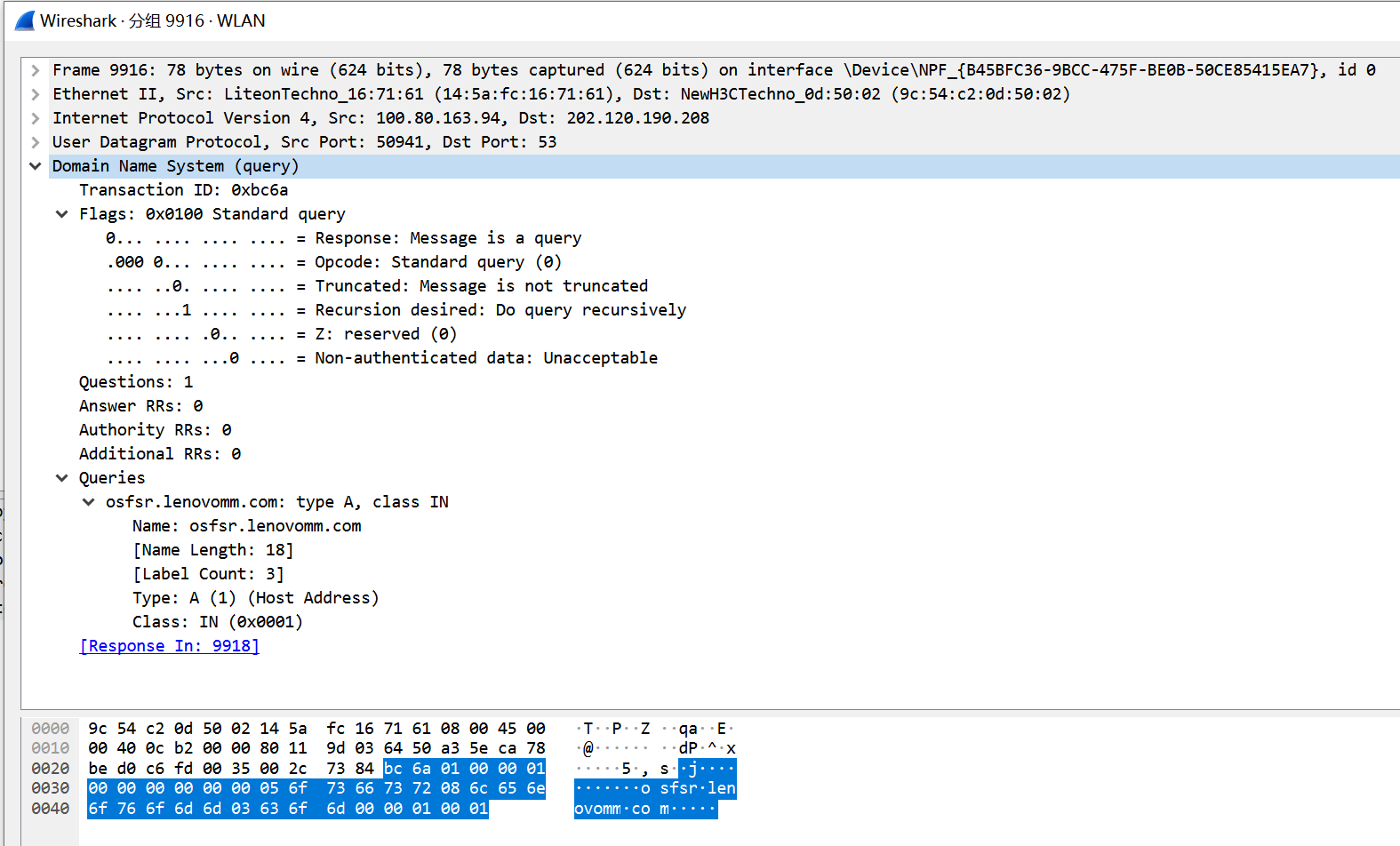


查询请求



查询响应

【分析讨论】



我们以Wireshark抓取的DNS报文进行分析。

这里是发起一个查询请求，为bc 6a 01 00 00 01 00 00 00 00 00 05 6f 73 66 73 72 08 6c 65 6e 6f 76 6f 6d 6d 03 63 6f 6d 00 00 01 00 01。

报文头部：

bc 6a: 标识一个DNS报文的标识号。

01 00: 标识这是一个标准查询请求。

00 01: 表示查询报文中的问题数（即，包含一个查询）。

00 00: 表示回答数、授权数和附加数都为0。

查询部分：

00 00: 请求部分的标识。

00 05: 表示查询部分中有5个字节。

6f 73 66 73 72: 这部分解析为"osfsr"（十六进制转ASCII）。

08: 之后是8个字节。

6c 65 6e 6f 76 6f 6d 6d: 解析为"lenovomm"（十六进制转ASCII）。

03: 之后是3个字节。

63 6f 6d: 解析为"com"（十六进制转ASCII）。

00: 表示域名部分的结尾。

00 01: 表示查询类型为A记录。

00 01: 表示查询类别为IN类。

请求的域名为"osfsr.lenovomm.com"，查询类型为A记录（IPv4地址）。

当选择DNS使用UDP（User Datagram Protocol）而不是TCP（Transmission Control Protocol）时，涉及到一些关键方面。DNS选择UDP主要基于以下考虑：连接建立开销：TCP需要建立连接、维护状态和进行断开，这导致了额外的时间开销。相比之下，UDP是无连接的传输协议，不需要在发送数据之前建立连接，因此节省了连接建立所需的时间和资源。快速响应：DNS的查询通常需要快速响应，特别是在互联网中有大量的DNS查询。UDP是一种轻量级协议，没有TCP的确认机制和重传保证，但它更快速地发送和接收数据包，适合快速的查询和响应。简单性和效率：UDP相对于TCP更加简单，不需要像TCP那样维护连接状态，这使得DNS服务器的实现更加轻便、高效，并降低了系统负担。重试机制：DNS在UDP上操作时，如果未收到响应或收到错误响应，客户端可以选择重新发送查询，而不必等待TCP连接的超时重传，从而提高了容错性。