实验 25：UDP 数据包分析实验

姓名	学号	合作学生	指导教师	实验地点	实验时间
林继申	2250758	无	陈伟超	济事楼 330	2024/05/23

【实验目的】

1. 了解 UDP 协议的特点：学生将学习 UDP 协议的无连接、不可靠传输和简单的错误检测机制。这包括理解 UDP 为什么比 TCP 有更少的时延，以及为什么在某些应用中（如实时视频、VoIP、DNS 查询等）更适合使用 UDP 而不是 TCP。
2. 分析 UDP 报文结构：通过实验，学生将了解 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. 学习 UDP 的实际应用:实验中,学生将配置和观察使用 UDP 协议的网络服务，例如 DNS 服务器。这有助于学生理解在实际网络环境中 UDP 的运用场景和行为。
5. 诊断网络问题：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。
6. 评估 UDP 的性能和可靠性：学生将评估 UDP 协议在不同网络条件下的性能，理解 UDP 协议在高速网络传输中如何受到网络延迟和丢包的影响，并探索如何在应用层增加额外的机制来提高通信的可靠性。

【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。
6. 适用于多种应用：
   - DNS：UDP 用于 DNS 查询，因为 DNS 请求通常很小，并且要求快速响应。
   - 实时应用：UDP 常用于实时应用，如 VOIP（语音通信）、实时视频会议和在线游戏，因为这些应用可以容忍一定的数据丢失，但对延迟非常敏感。
   - 多媒体流：流媒体传输等应用使用 UDP 来减少播放时的延迟。

总体来说，UDP 的设计哲学是提供快速、简单且灵活的传输服务，尽管这样的服务是不可靠的。这使得 UDP 在那些不需要或少需要可靠性但需求低延迟或高效率的场景中非常有用。

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。以下是 UDP 报文格式的详细介绍：

1. UDP 首部格式

UDP 首部固定长度为 8 字节，由以下四个字段各占两字节组成：

- 源端口号：这是发送方的端口号，用于接收方回复消息时指定返回的端口。如果发送方不需要回复，则可以将此字段设置为 0。
- 目的端口号：这是接收方的端口号，用于在目的地将数据报文正确地交付给相应的应用程序。
- 长度：这个字段指定了 UDP 首部和数据的总长度，最小值为 8 字节（即只有首部，没有数据）。
- 校验和：用于检测 UDP 数据报在传输过程中是否发生错误。如果设置为 0，则表示发送方没有计算校验和，接收方也不应进行校验。

2. 校验和计算

校验和的计算包括首部和数据两部分，以确保数据的完整性。为了进行校验和的计算，还需要在 UDP 数据报前临时添加一个 12 字节的伪首部。伪首部包括：

- 源 IP 地址（4 字节）
- 目的 IP 地址（4 字节）
- 保留字节（全 0，1 字节）
- 协议类型（1 字节，表示 UDP）
- UDP 长度（2 字节，与 UDP 首部中的长度字段相同）

伪首部不是 UDP 数据报的实际一部分，不会传送，只是在计算校验和时使用。校验和的计算方法是将整个 UDP 数据报（包括伪首部、首部和数据）视为 16 位的字序列，进行二进制反码求和。如果最后的求和结果为全 1，则表示数据在传输过程中没有错误；如果不是，则表明数据报在传输过程中出现了错误。

3. 错误处理

如果接收到的 UDP 数据报校验和不正确，表明数据报可能已损坏。接收方可以选择丢弃此数据报，或者可以选择接收但向应用层报告数据可能已损坏。此外，如果接收方发现目的端口号不存在，则会丢弃该数据报，并可能通过 ICMP 协议向发送方发送“端口不可达”错误消息。

通过这种设计，UDP 提供了一种快速但不保证可靠性的传输方式，适合对传输效率和低延迟有高要求的网络应用。

【实验设备】

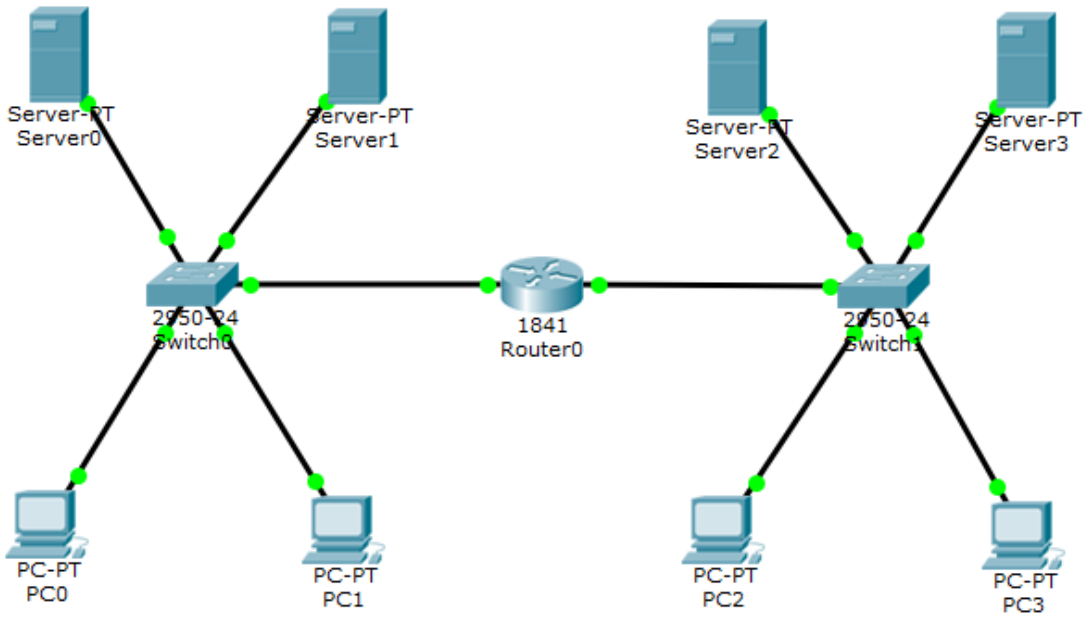
1. 操作系统：Windows 10

2. 网络环境：局域网

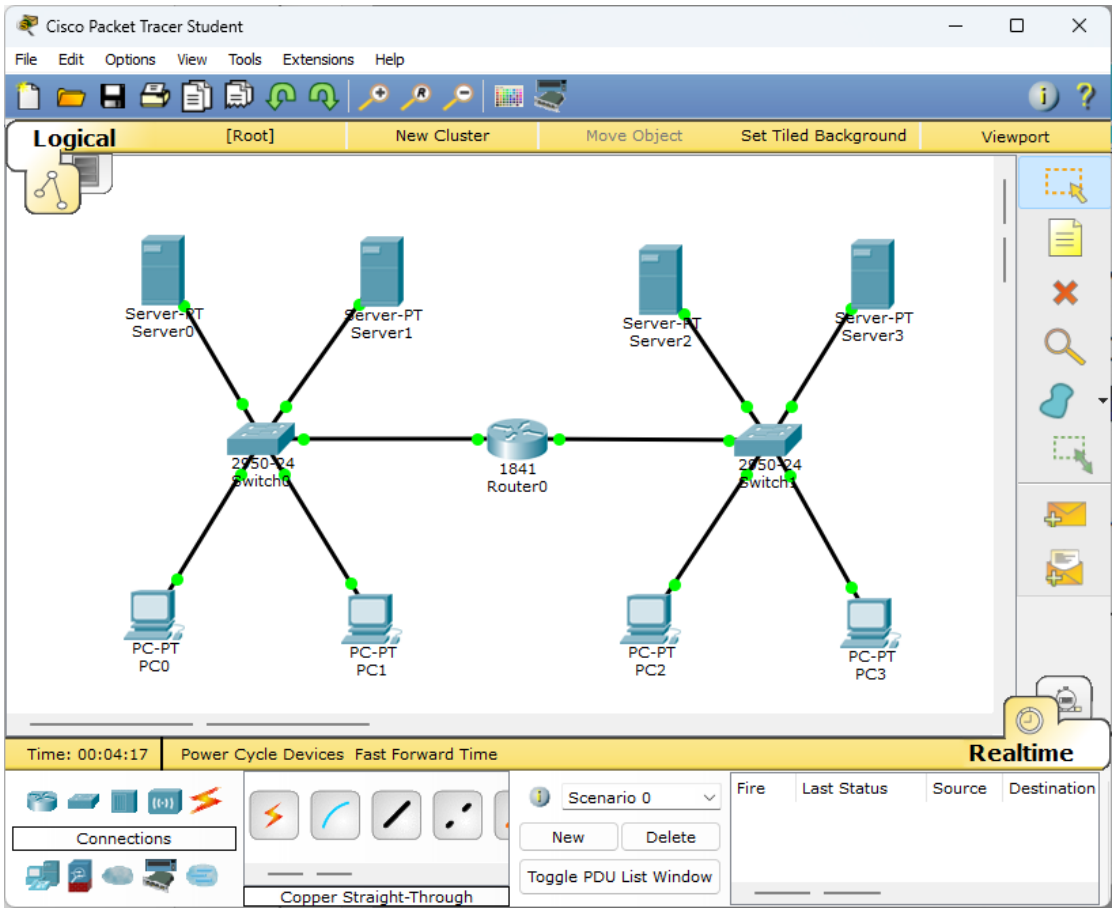
3. 应用程序：Cisco Packet Tracer 6.0

【实验步骤】

1. 规划网络地址及拓扑图。

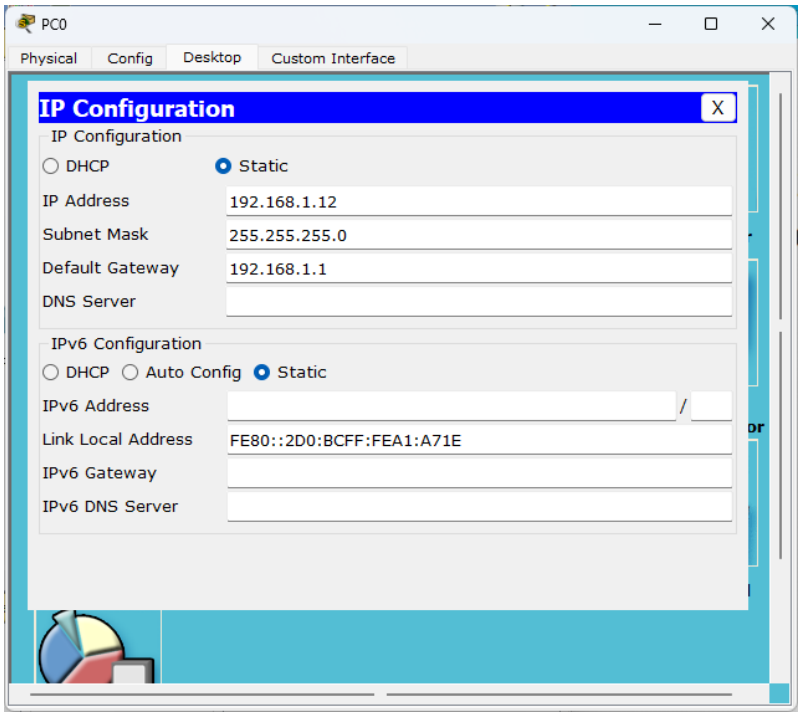


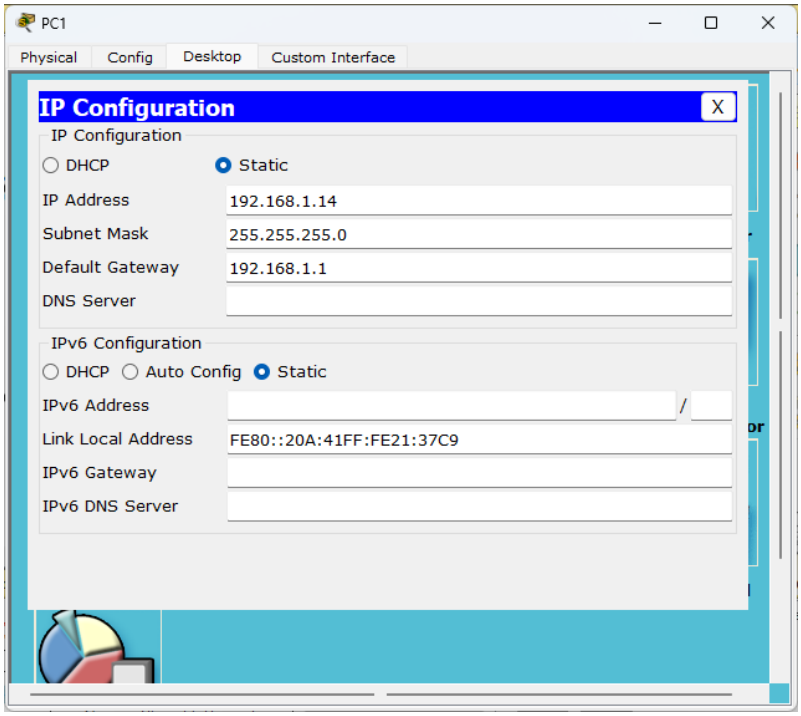
2. 启动 Cisco Packet Tracer，按照上图连接网络。

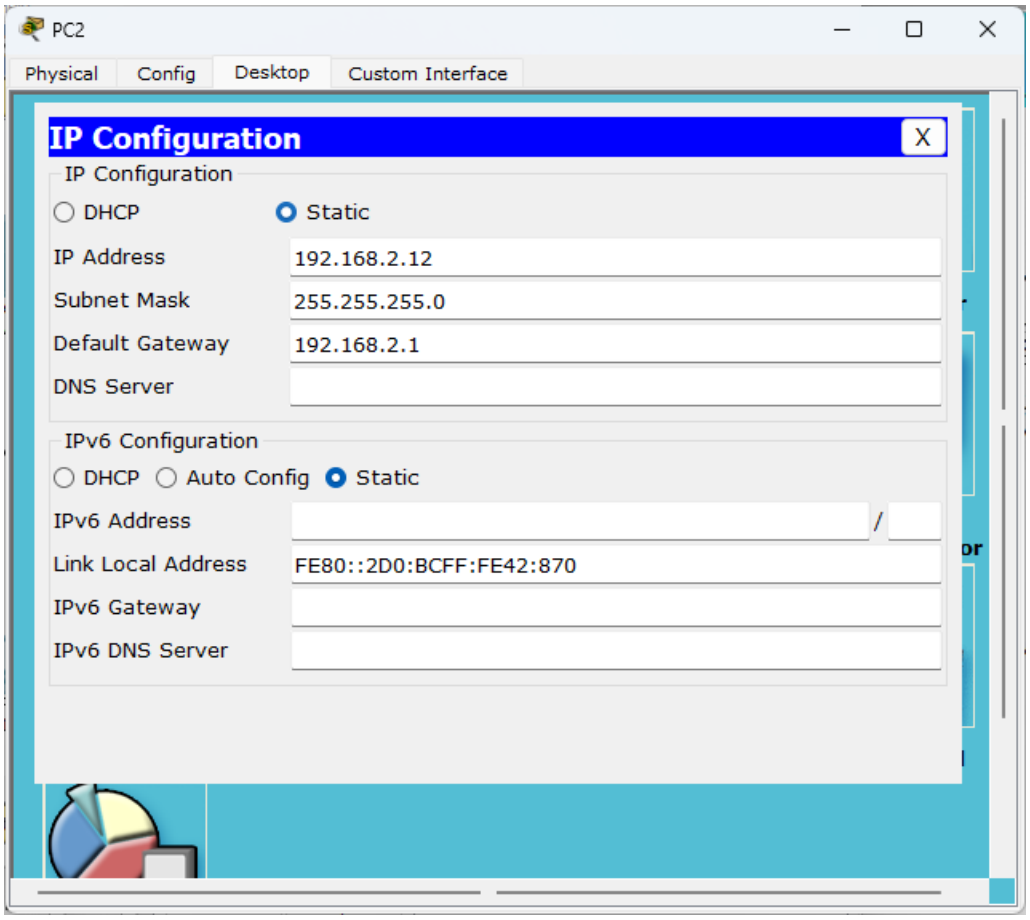


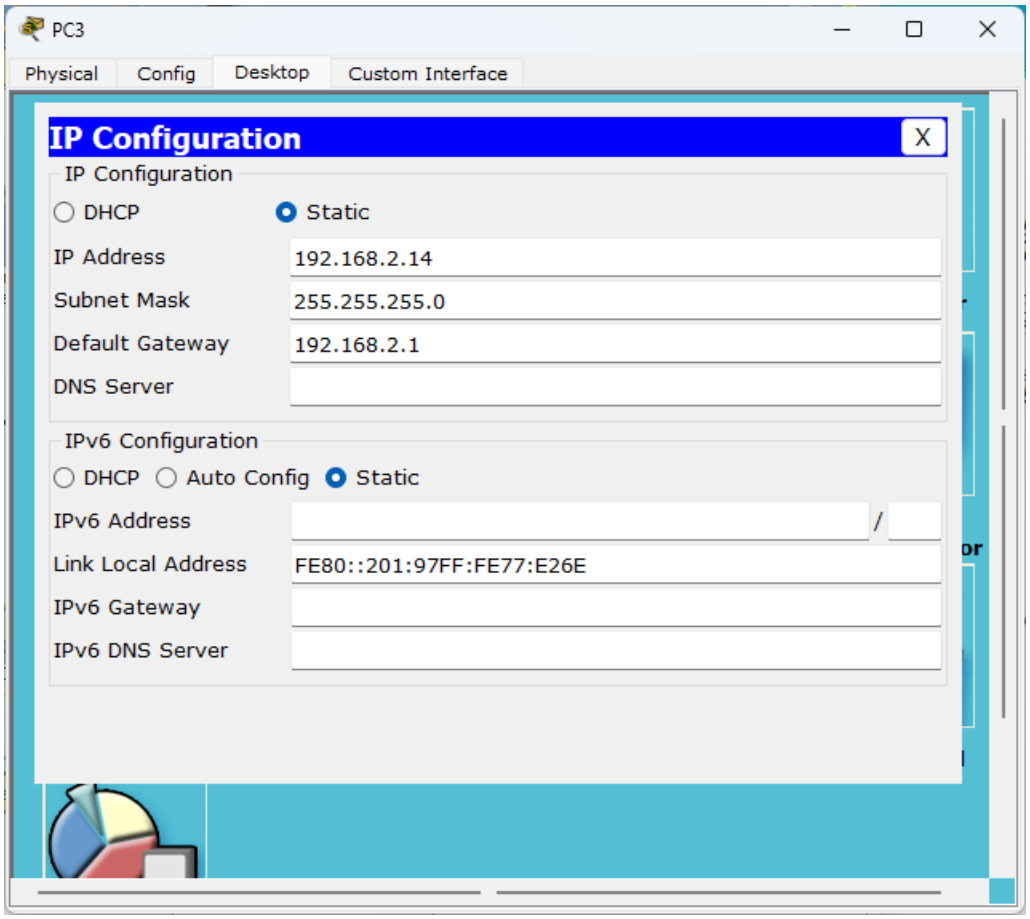
3. 为每台 PC 机配置如下静态 IP 地址、子网掩码和默认网关。

PC	IP Address	Subnet Mask	Default Gateway
PC0	192.168.1.12	255.255.255.0	192.168.1.1
PC1	192.168.1.14	255.255.255.0	192.168.1.1
PC2	192.168.2.12	255.255.255.0	192.168.2.1
PC3	192.168.2.14	255.255.255.0	192.168.2.1



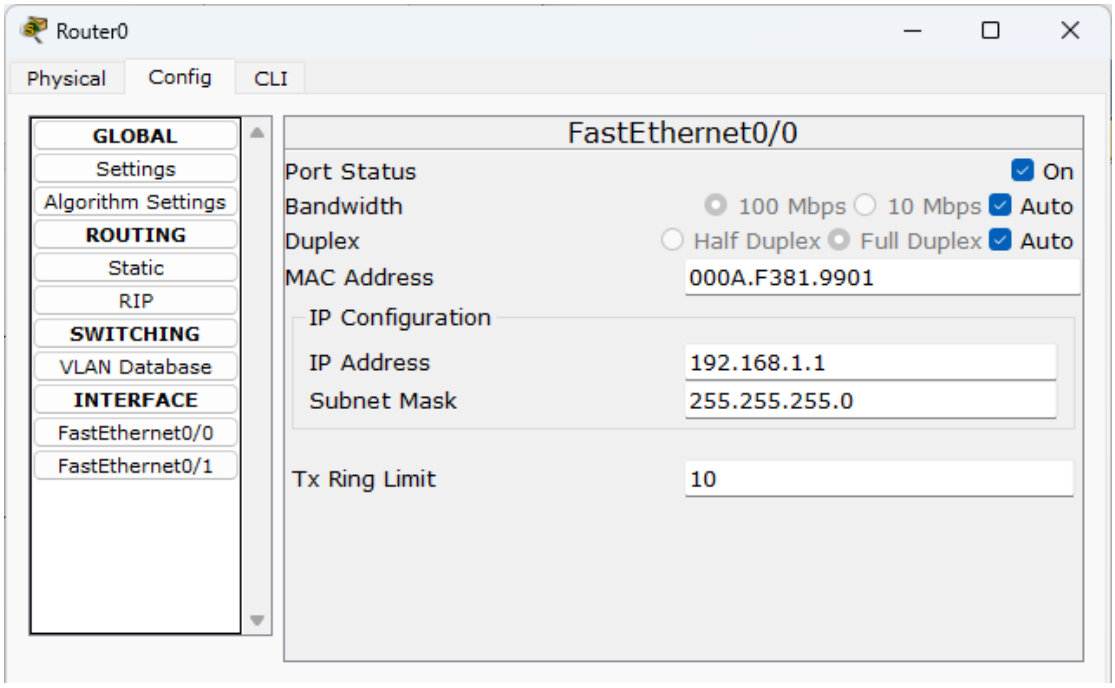


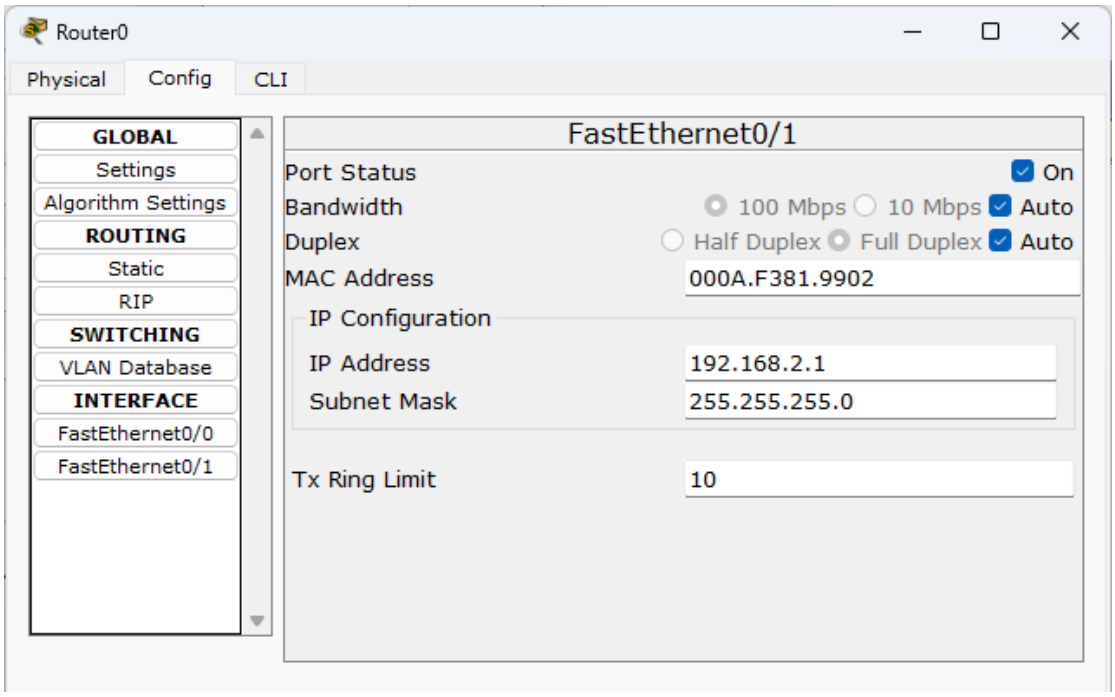

PC2
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.2.12
Subnet Mask
255.255.255.0
Default Gateway
192.168.2.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::2D0:BCFF:FE42:870
IPv6 Gateway
IPv6 DNS Server


PC3
Physical
Config
Desktop
Custom Interface
IP Configuration
X
IP Configuration
DHCP
Static
IP Address
192.168.2.14
Subnet Mask
255.255.255.0
Default Gateway
192.168.2.1
DNS Server
IPv6 Configuration
DHCP
Auto Config
Static
IPv6 Address
/
Link Local Address
FE80::201:97FF:FE77:E26E
IPv6 Gateway
IPv6 DNS Server

4. 参照先前实验（实验 18：动态 IP 地址分配 DHCP 实验）配置路由器 Router0 的接口，可以通过在 CLI 中输入以下命令进行配置，也可以通过图形化界面进行配置。

```
interface FastEthernet0/0
ip address 192.168.1.1 255.255.255.0
interface FastEthernet0/1
ip address 192.168.2.1 255.255.255.0
```





5. 在路由器 Router0 配置 DHCP。

- 在 CLI 输入以下命令配置路由器 DHCP 左边网络。

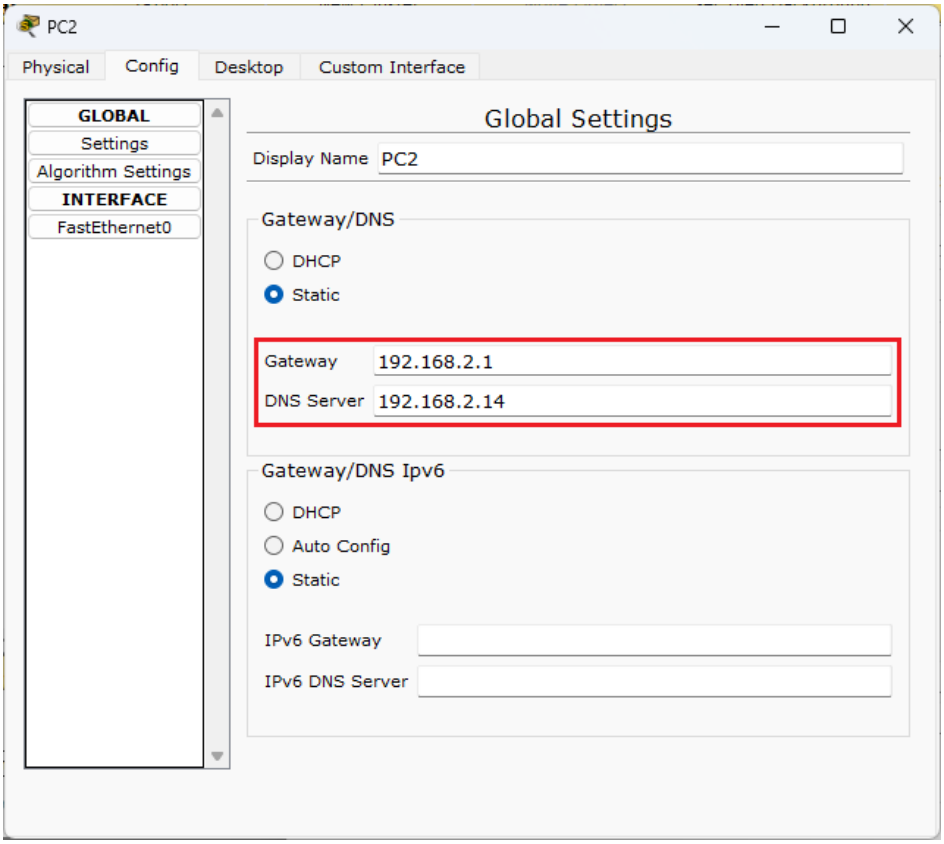
```
ip dhcp excluded-address 192.168.1.0 192.168.1.10
ip dhcp pool myleftnet
network 192.168.1.0 255.255.255.0
default-router 192.168.1.1
option 150 ip 192.168.1.3
dns-server 192.168.1.2
```

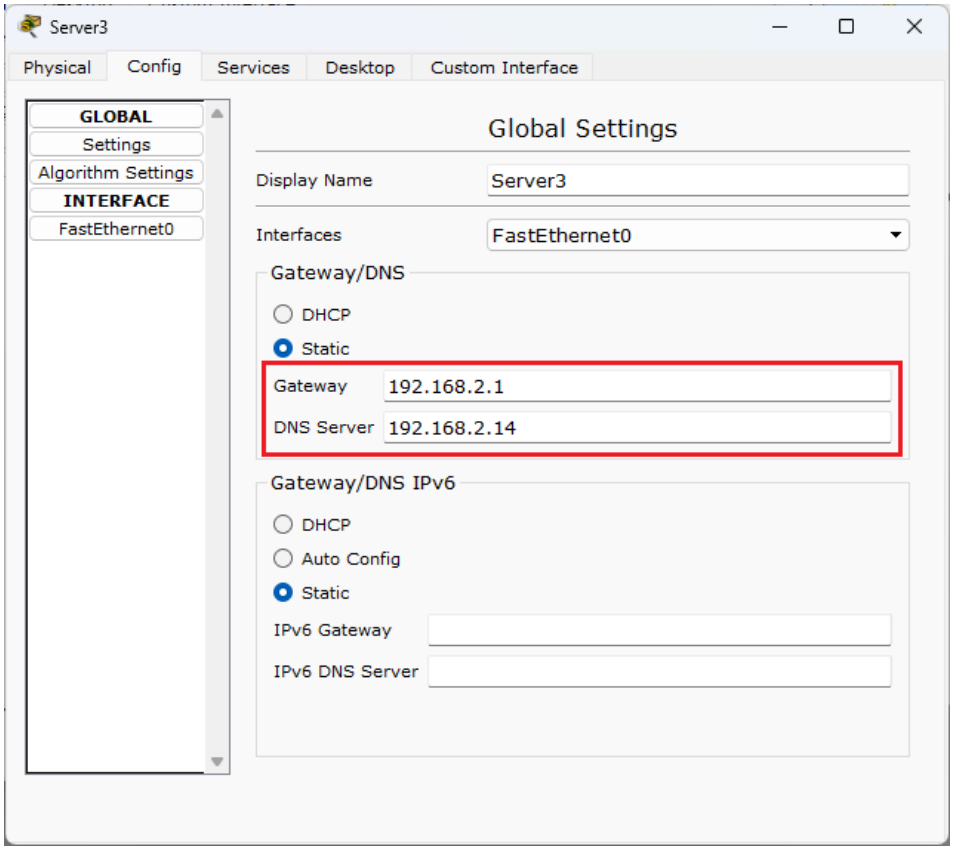
- 在 CLI 输入以下命令配置路由器 DHCP 右边网络。

```
ip dhcp excluded-address 192.168.2.0 192.168.2.10
ip dhcp pool myrightnet
network 192.168.2.0 255.255.255.0
default-router 192.168.2.1
option 150 ip 192.168.2.3
dns-server 192.168.2.2
```

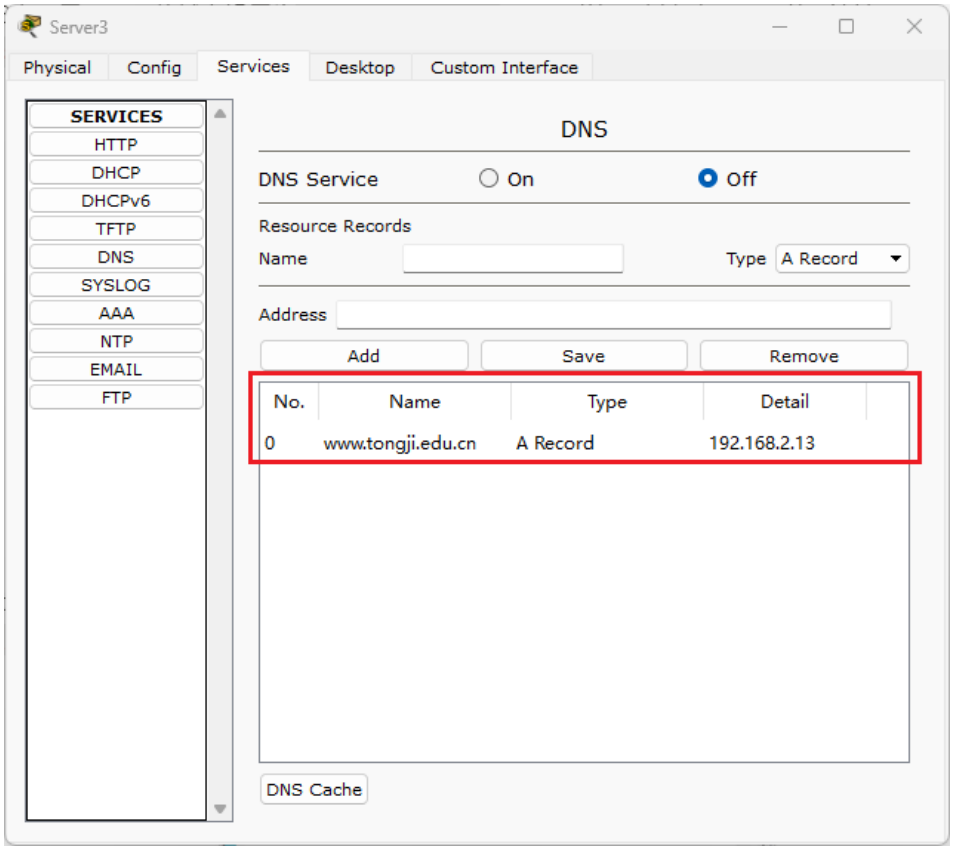
6. 配置 Server 的 Gateway 和 DNS Server。

7. 配置 PC2 的 DNS Server 为 192.168.2.14。设置 PC2 的 DNS Server 与 Server3 的 DNS Server 相同是为了能够通过 Server3 构建映射访问到 Server2。





8. 配置 Server3 的 Services，Name 设置为 www.tongji.edu.cn，Detail 设置为 Server2 的 IP 地址（192.168.2.13）。



9. 从 Realtime 模式切换至 Simulation 模式。

9.1 在 PC2 的 Web Browser 中输入 http://www.tongji.edu.cn，产生 UDP 数据流量，分析 UDP 数据报文。

9.2 点击 Capture/Forward 单步执行，也可以点击 Auto Capture/Play 自动执行，查看相关数据。

9.3 在 Even List 中的 Info 栏可以查看相关信息。

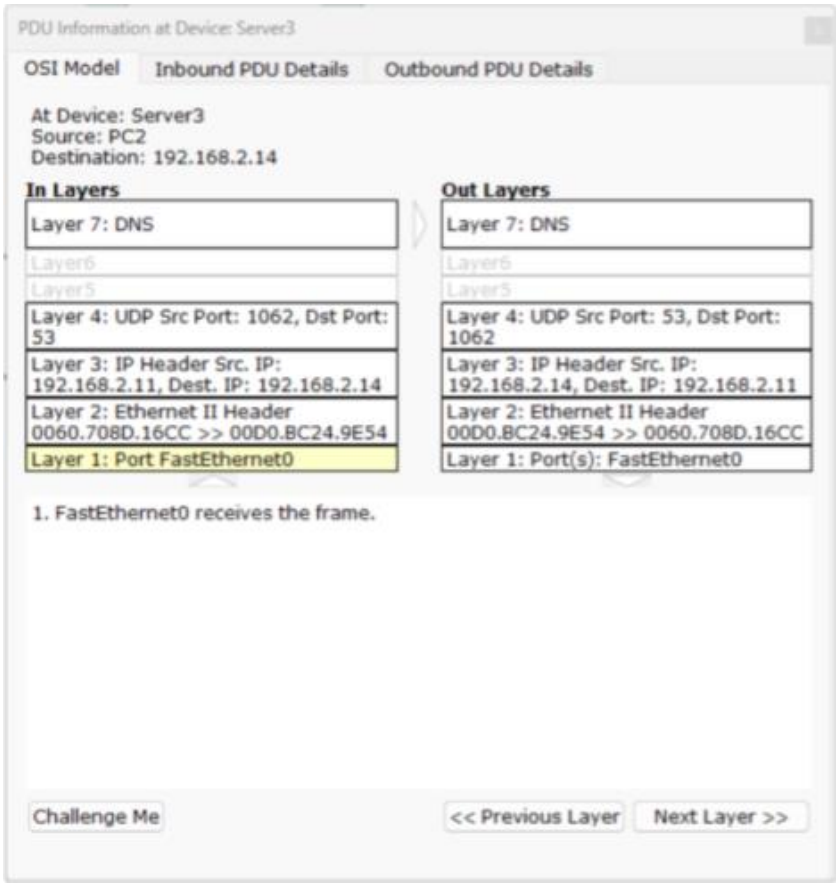
10. 分析在 Packet Tracer 中 UDP 报文情况。

11. 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. 分析在 Packet Tracer 中 UDP 报文情况。

1.1 PDU Information at Device: Server3（OSI Model）



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）：53，表示这是一个来自 DNS 服务器的响应。
  - 目的端口（Destination Port）：1062，这是客户端的端口，用于接

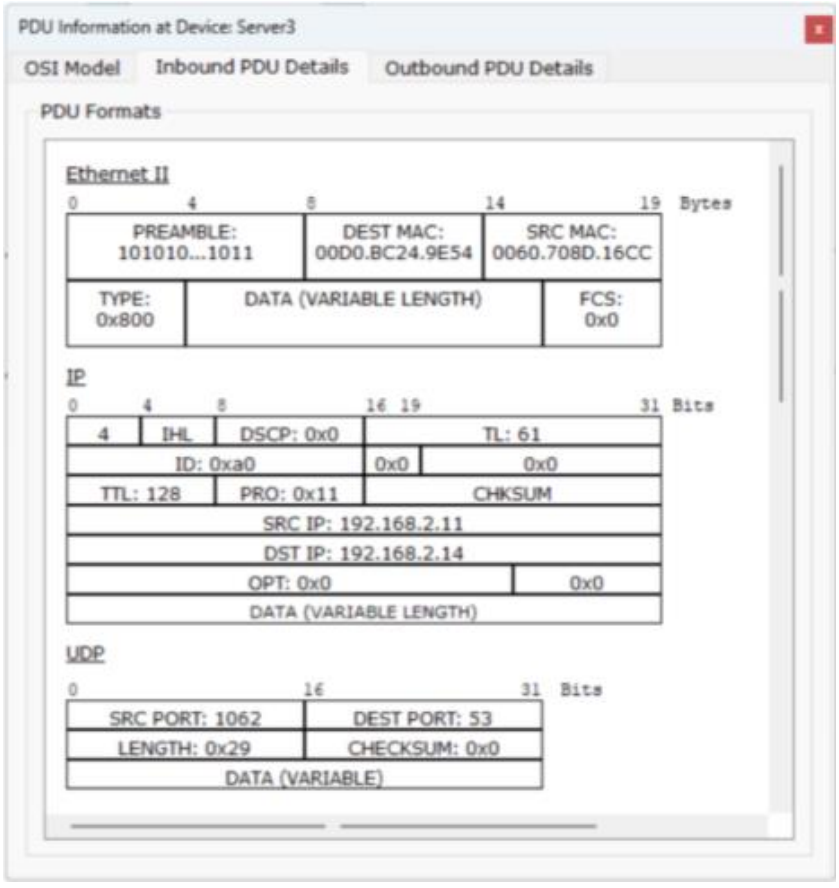
收 DNS 响应。

- 长度（Length）：0x29，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）：0x0，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。

- 输出 PDU 详情（Outbound PDU Details）
  - 源端口（Source Port）：1062，客户端用于发送 DNS 查询的端口。
  - 目的端口（Destination Port）：53，目标是 DNS 服务器的标准端口。
  - 长度（Length）：0x48，报文长度，包括首部和数据，十进制为 72 字节。
  - 校验和（Checksum）：0x0，同上，校验和显示为 0。

这些信息展示了 UDP 数据包在发送和接收时的基本特征，输入和输出的 PDU（协议数据单元）提供了关于数据包移动和处理的详细信息。

1.2 PDU Information at Device: Server3（Inbound PDU Details）

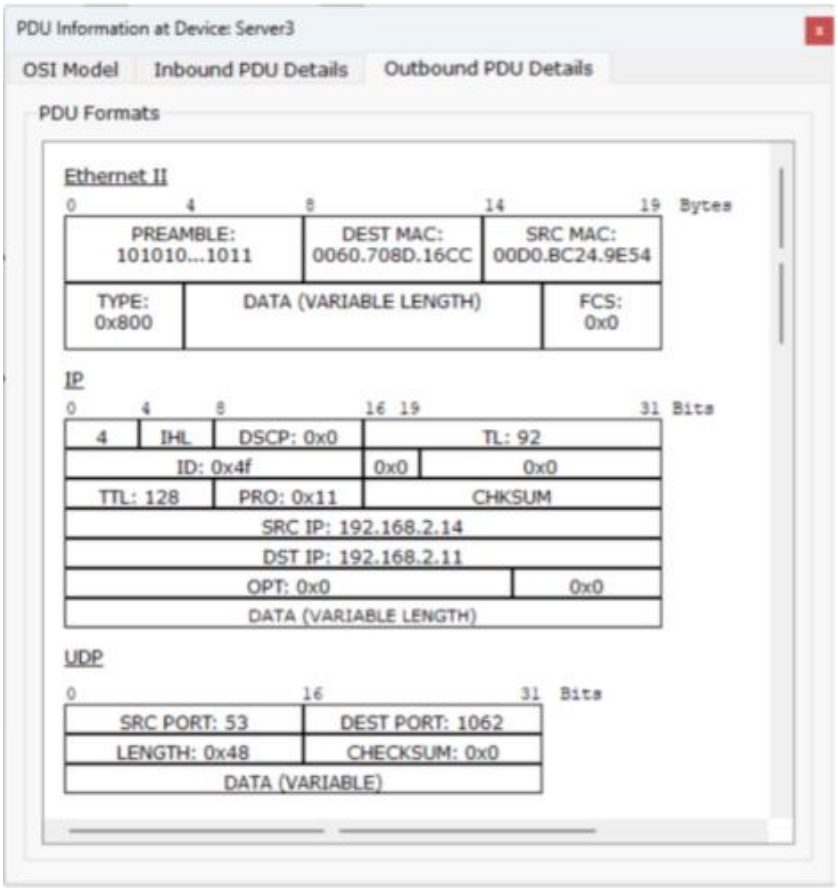


UDP 层：

- 源端口（SRC PORT）：1062，源端口号。
- 目的端口（DEST PORT）：53，DNS 服务的标准端口，表明这是一个 DNS 查询。
- 长度（LENGTH）：0x29，包括 UDP 首部和数据的总长度，十进制为 41 字节。
- 校验和（CHECKSUM）：0x0，可能未计算或不使用。

此图的信息可以帮助理解网络数据包是如何封装和在网络中传输的，以及如何通过不同的网络层来处理数据。每一层都对数据进行相应的封装，增加特定的首部信息，确保数据能正确地从源头传输到目的地。

1.3 PDU Information at Device: Server3（Outbound PDU Details）



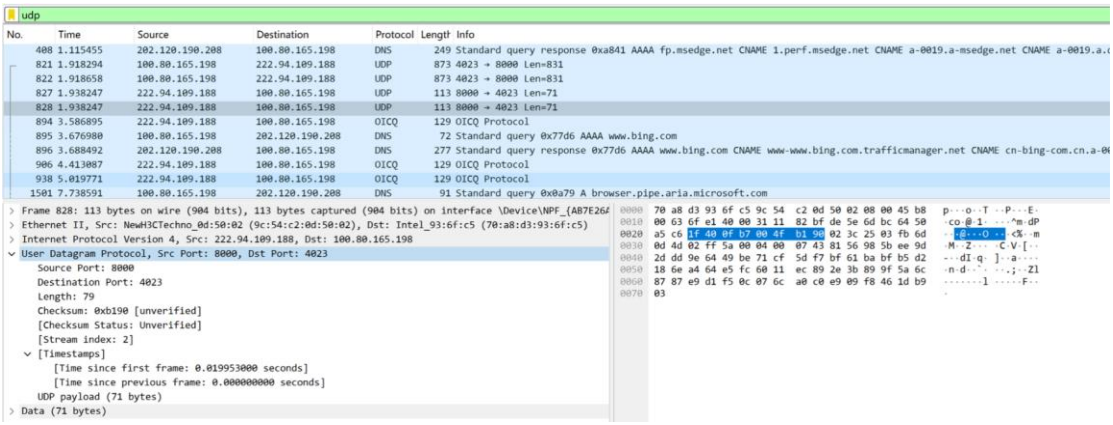
UDP 层：

- 源端口（SRC PORT）：53，表明这是从 DNS 服务器发出的响应。
- 目的端口（DEST PORT）：1062，客户端使用此端口接收 DNS 响应。
- 长度（LENGTH）：0x48，表示 UDP 数据报的总长度为 72 字节（包括首部和数据）。

- 校验和（CHECKSUM）：0x0，表示没有计算校验和，或者不进行校验。

这里的 UDP 数据报明确显示了一个从 DNS 服务器（端口 53）到客户端（端口 1062）的响应。长度字段表明整个 UDP 数据报，包括首部和数据的长度，而校验和字段的值为 0，可能是因为在特定的配置或环境中，校验和未被计算或者故意设置为 0 以避免校验过程。

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



用 WireShark 抓取 UDP 数据包，查看 UDP 报文字段内容，并解读如下：

- 通用信息
  - 数据包编号：828。
  - 长度：113 bytes on wire（即物理层面的总字节数），904 bits。
- IP 协议信息
  - 源 IP 地址（Src IP）：222.94.109.188，发送此数据包的设备的 IP 地址。
  - 目的 IP 地址（Dst IP）：100.80.165.198，接收此 UDP 数据报的设备的 IP 地址。
  - 协议（Protocol）：UDP，表明这是一个 UDP 数据包。
  - 总长度（Total Length）：92 bytes，包括 IP 首部和数据。
- UDP 协议信息
  - 源端口（Source Port）：8000，发送数据报的应用程序端口号。
  - 目的端口（Destination Port）：4023，数据报应当被送达的应用程序端口号。
  - 长度（Length）：79，表示 UDP 数据报的总长度，包括 UDP 首部和数

据。

- 校验和（Checksum）：0xb190，校验和值用于错误检测，状态为“unverified”。

- 时间戳信息
  - 从首个数据包开始的时间：0.01995300 seconds，从会话开始到此数据包抓取的时间。
  - 从前一个数据包开始的时间：0.00000000 seconds，从上一个数据包到此数据包的间隔时间。
- 数据负载
  - UDP 负载长度：71 bytes，这是除 UDP 首部外的实际数据负载。

这些信息对于网络分析非常关键，可以帮助理解网络通信的动态过程、数据流的方向、通信双方的身份，以及数据包的结构。此外，MAC 地址、IP 地址、端口号等元素对于网络故障诊断、安全分析和网络性能优化都有重要作用。

【分析讨论】

一、分析在 Packet Tracer 中 UDP 报文情况

在本实验中，通过 Packet Tracer 模拟了 UDP 数据报的发送与接收过程，重点观察了 UDP 协议的无连接和简单首部特性。通过直观的网络仿真,理解 UDP 如何在不建立连接的情况下进行数据传输，以及这种传输方式如何减少通信延迟。在 DNS 查询这一特定应用案例中，观察到 UDP 首部的源端口和目的端口的设置，以及数据报文长度和校验和的具体应用。此部分的实验不仅加深了对 UDP 基础结构的认识，还提供了实际操作网络分析工具的机会，能够直观地看到协议在实际网络环境中的工作方式。

二、用 WireShark 抓取 UDP 数据包并查看 UDP 报文字段内容

使用 Wireshark 进行的数据捕获实验进一步加强对网络协议分析的实践技能。通过捕获实时网络流量，深入了解 UDP 数据包的传输细节，包括但不限于端口号的功能、数据长度的意义以及校验和的重要性。通过分析特定的 UDP 流量，如 DNS 响应和 VoIP 通信，得以观察和理解 UDP 在减少传输延迟和处理轻量级数据方面的有效性。此外，通过识别传输中可能的错误（如校验和错误）也能够掌握基本的网络问题诊断方法。