实验 22：IP 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	2024/05/09

【实验目的】

1. 理解 IP 协议和数据包结构：学生将学习 IP 数据包的组成，包括首部和数据两部分的详细结构，了解各个字段的功能，例如版本、首部长度、总长度、标识、标志、片偏移、生存时间（TTL）、协议、首部校验和以及源地址和目的地址等。
2. 掌握 IP 数据包的封装和拆封过程：通过实验，学生将了解 IP 层是如何封装和拆封数据报来提供不可靠无连接的数据报传输服务的。
3. 学习 IP 数据包的传输和分片机制：实验中将介绍 IP 数据包在不同网络环境下的传输方式，以及如何处理数据报的分片和重组，特别是在跨越具有不同最大传输单元（MTU）值的网络时。
4. 使用网络分析工具进行数据包捕获和分析：学生将使用如 Wireshark 等网络分析工具，实际捕获和分析 IP 数据包。这不仅包括数据包的捕获，还包括如何读取和解释数据包中的信息。
5. 诊断网络问题和验证网络设计：通过对捕获的数据包进行分析，学生可以学习如何诊断网络中的问题，并验证网络设计和配置是否正确。
6. 实践网络安全和性能评估：学生将通过分析数据包来评估网络的安全性和性能，了解如何通过配置和优化来提高网络的效率和安全性。

【实验原理】

一、IP 协议

IP 协议（Internet Protocol）提供不可靠、无连接的数据报传输服务。IP 层提供的服务是通过对数据报进行封装和拆封实现的。IP 数据报的格式分为两个主要部分：报头和数据部分。报头部分包含确保数据正确传输所需的各种控制信息，而数据部分包括上层协议需要传输的数据。

1. IP 数据报文格式概览

IP 数据报由报头和数据两部分组成，报头用于携带传输控制信息，数据部分包含实际的传输数据。

2. 报头

报头的固定部分长度为 20 字节，是每个 IP 数据报文都包含的基础信息。可选字段的长度可变，可以根据需要包含更多的控制信息。

3. 报头的固定部分字段

- 版本：4 位，表示 IP 协议的版本号。常见的版本是 IPv4。
- 首部长度：4 位，指示报头的长度，单位为 4 字节。
- 区分服务：8 位，用于不同服务类型的需求。
- 总长度：16 位，表示整个数据报的长度，单位为字节。
- 标识：16 位，唯一标识一个数据报。
- 标志：3 位，控制数据报的分片行为。
- 片偏移：13 位，指示数据报在分片后的位置。
- 生存时间（TTL）：8 位，指示数据报在网络中的最大跳数。
- 协议：8 位，指示承载的数据使用的协议。
- 首部校验和：16 位，仅校验报头部分。
- 源地址和目的地址：各 4 字节，指示数据的源和目标。

4. 报头的可选部分

报头的可选字段长度可变，提供额外的传输控制、排错和安全选项，最大长度为 40 字节。

5. 报头校验

使用 16 位二进制反码求和算法，对报头部分进行校验。

6. 数据报分片

如果数据报的总长度超过网络的 MTU（最大传输单元），需要进行分片。每个分片都复制原数据报的报头，并修改相关字段以表示其位置和顺序。

7. 数据报的传输顺序

在传输时，数据按位序从高位到低位传输。

8. TOS（服务类型）

服务类型字段占用 8 位，设定了数据报的优先级、延迟、吞吐量和可靠性等特性。

9. 最大传输单元（MTU）

每个网络都有固定的 MTU，表示网络帧的最大长度。分片通常由路由器负责，以适应不同网络的 MTU。

10. 分片和重组

数据报被分片后，接收端主机会根据标识、标志和偏移量字段进行重组，恢复成原始数据报。

11. IP 选项

IP 选项字段用于控制数据报的传输过程，可设置传输路由、记录路径、时间戳等。常用的选项有：

- 源路由选择：严格或宽松地指定数据报的路径。
- 记录路由：记录数据报经过的路由器。
- 时间戳：记录数据报通过每个路由器的时间和地址。

二、ARP 协议

ARP（地址解析协议）是一种网络协议，用于在 IP 网络中将设备的 IP 地址转换为物理层的 MAC 地址，从而实现同一局域网中设备之间的通信。它通过广播 ARP 请求，目标设备回复其 MAC 地址，然后发送设备将此对应关系缓存，以便后续快速访问。ARP 对于以太网环境中的正常通信至关重要，但同时也易受 ARP 欺骗和缓存中毒等网络攻击的威胁。

ARP 消息的结构通常包括：

- 硬件类型：指定所用链路层协议，如以太网为 1。
- 协议类型：标识需要解析的上层协议，如 IPv4 为 0x0800。
- 硬件地址长度：表示 MAC 地址的长度。
- 协议地址长度：表示 IP 地址的长度。
- 操作码：指定 ARP 请求或回复（1 为请求，2 为回复）。
- 发送方 MAC 地址：发送设备的 MAC 地址。
- 发送方 IP 地址：发送设备的 IP 地址。
- 目标 MAC 地址：目标设备的 MAC 地址（请求时为空）。
- 目标 IP 地址：目标设备的 IP 地址。

【实验设备】

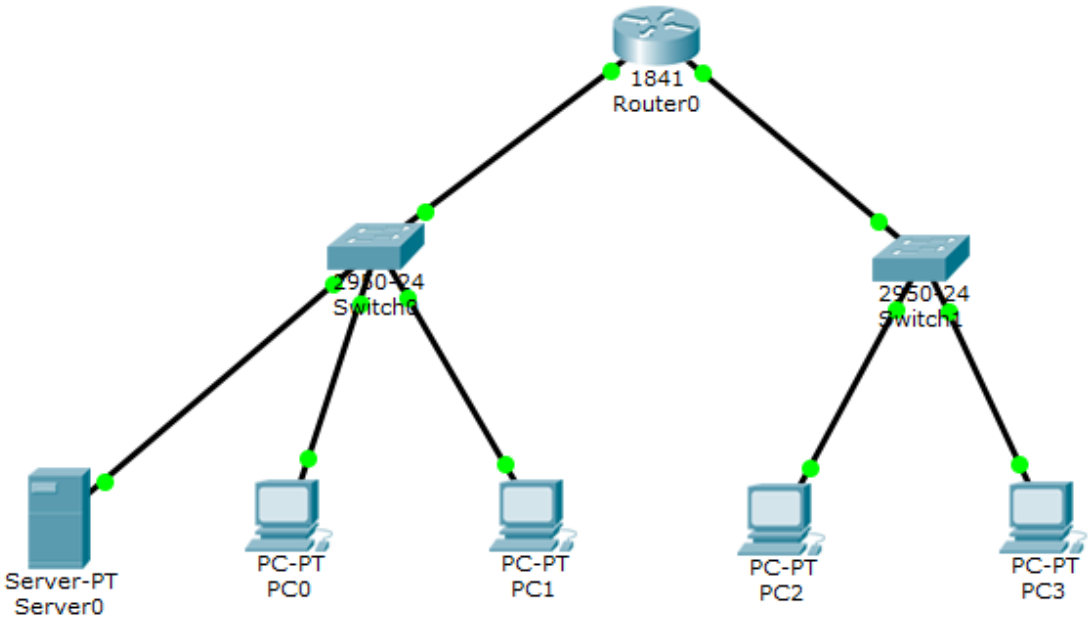
1. 操作系统：Windows 10

2. 网络环境：局域网

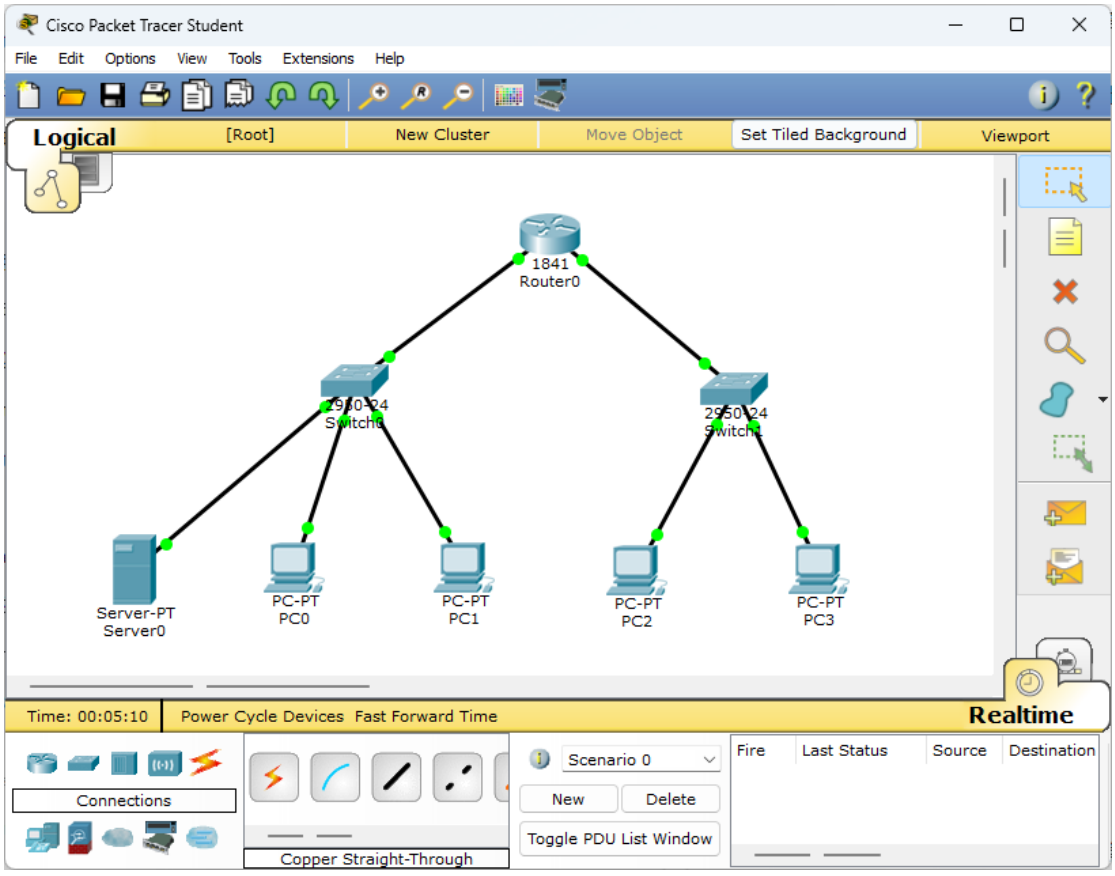
3. 应用程序：Cisco Packet Tracer 6.0

【实验步骤】

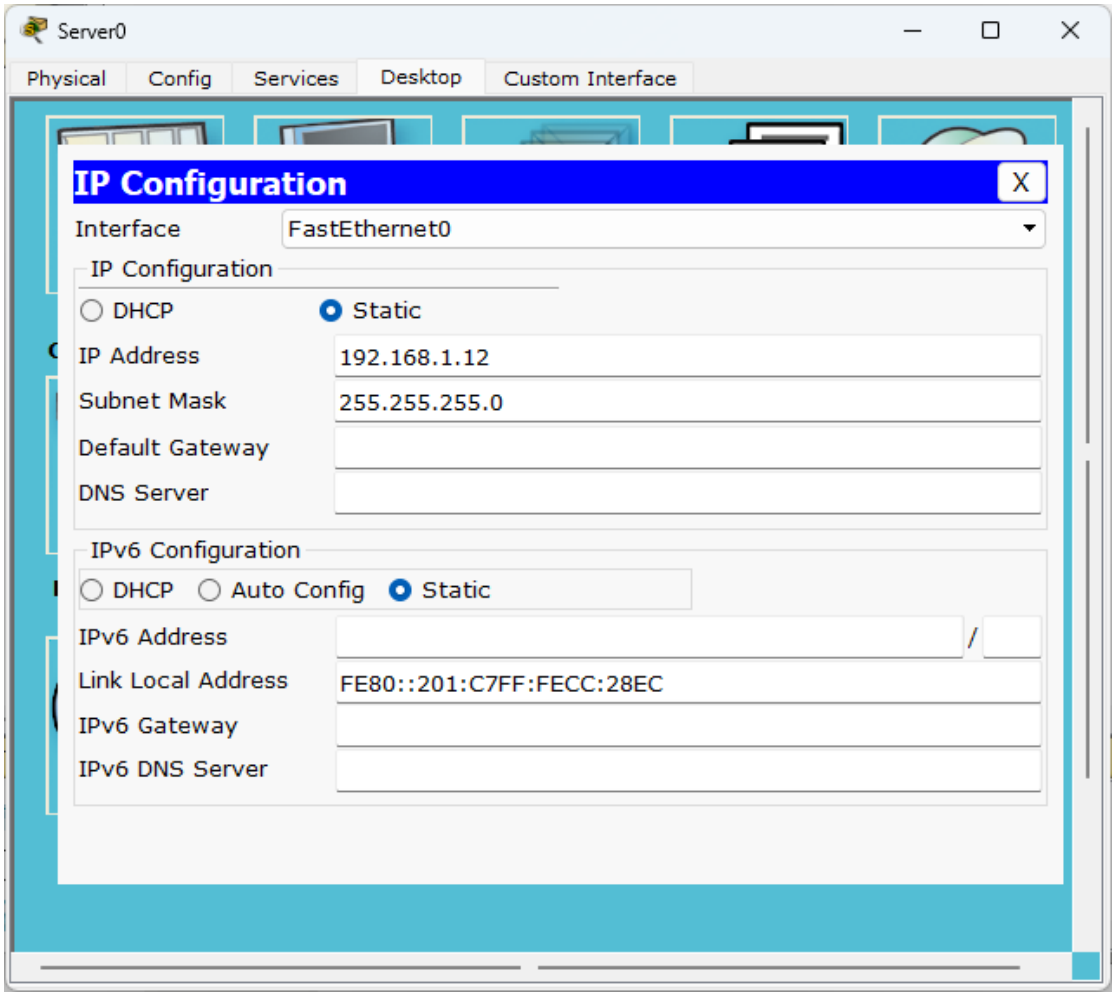
1. 规划网络地址及拓扑图。



2. 启动 Cisco Packet Tracer，按照上图连接网络。



3. 配置服务器，设置静态 IP 为 192.168.1.12，子网掩码为 255.255.255.0。

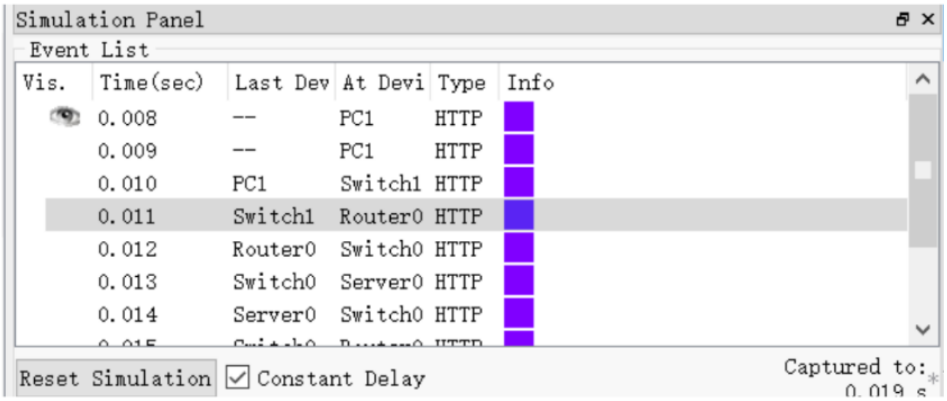


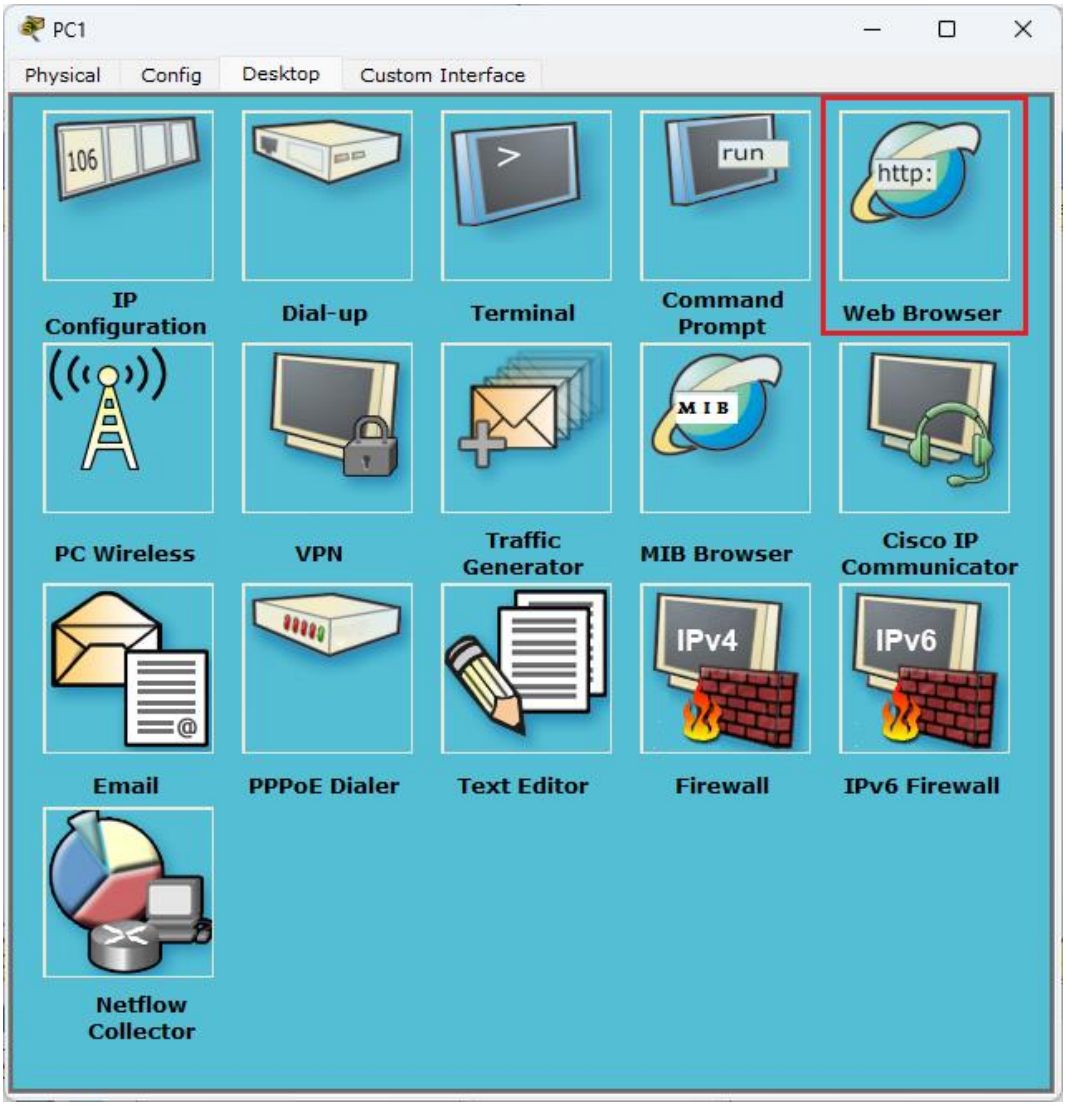
4. 从 Realtime 模式切换至 Simulation 模式。

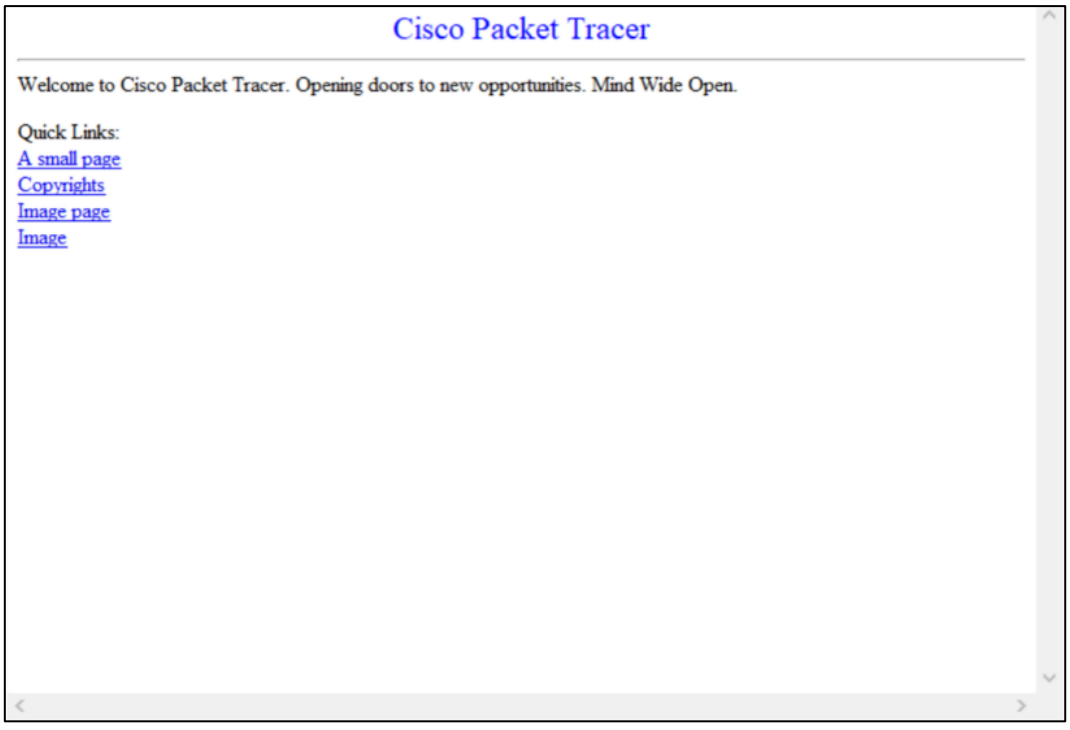
4.1 在 PC1 的 Web Browser 中输入服务器网址 http://192.163.1.12，产生 IP 数据报文。

4.2 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。

4.3 在 Even List 中的 Info 栏可以查看相关信息。




PC1
Physical
Config
Desktop
Custom Interface
IP Configuration
Dial-up
Terminal
Command Prompt
Web Browser
PC Wireless
VPN
Traffic Generator
MIB Browser
Cisco IP Communicator
Email
PPPoE Dialer
Text Editor
Firewall
IPv6 Firewall
Netflow Collector


Cisco Packet Tracer
Welcome to Cisco Packet Tracer. Opening doors to new opportunities. Mind Wide Open.
Quick Links:
A small page
Copyrights
Image page
Image

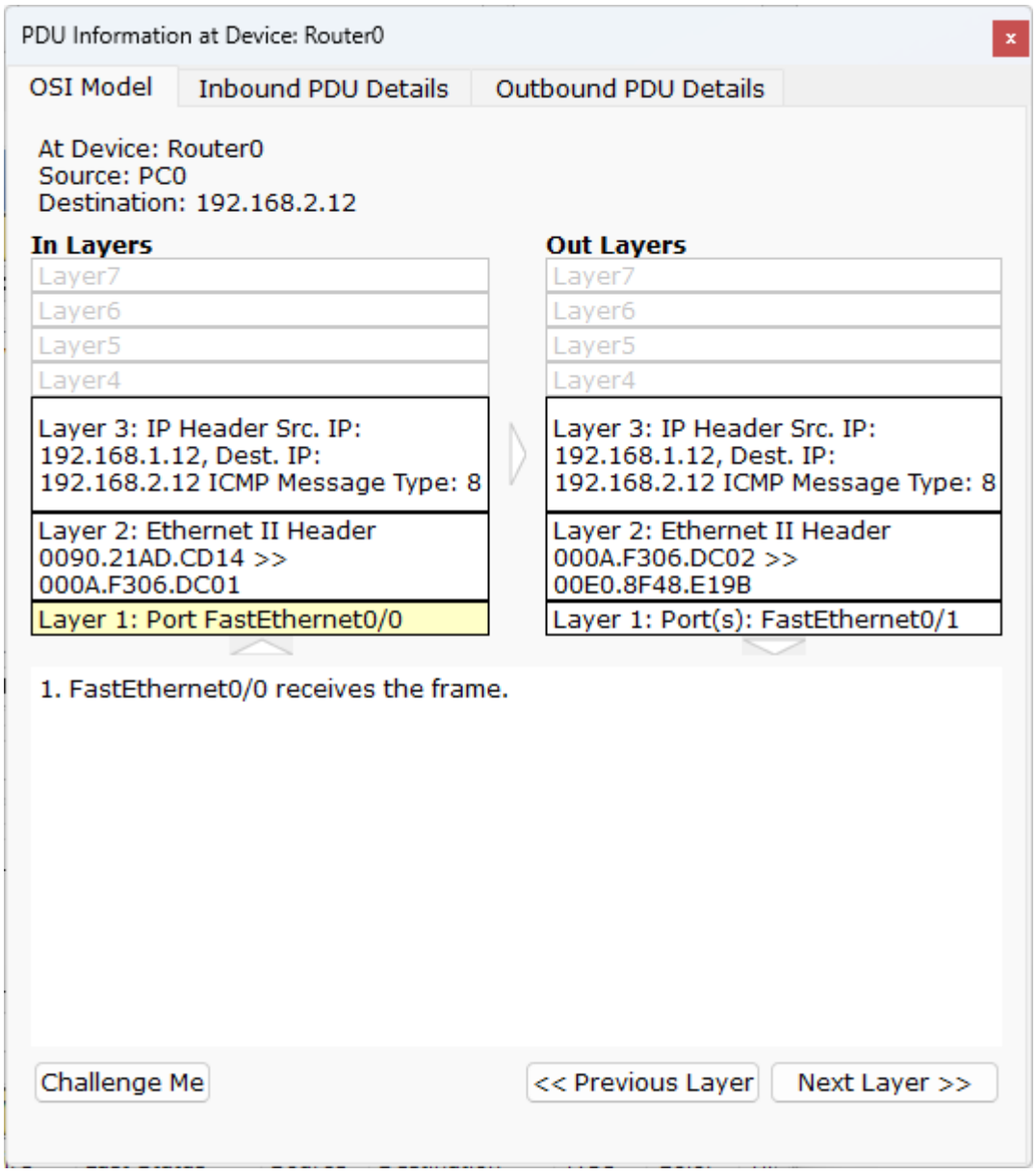
5. 分析 IP 数据报文。

6. 用 WireShark 抓取 IP 数据包，并解读。

【实验现象】

1. 从 Realtime 模式切换至 Simulation 模式，在 Even List 中的 Info 栏可以查看相关信息，这里对 Router0 的相关 Event 进行如下分析。

1.1 PDU Information at Device: Router0（OSI Model）



入站 PDU 细节（Inbound PDU Details）：

- 在设备：Router0
- 源地址（Source）：PC0
- 目的地址（Destination）：192.168.2.12

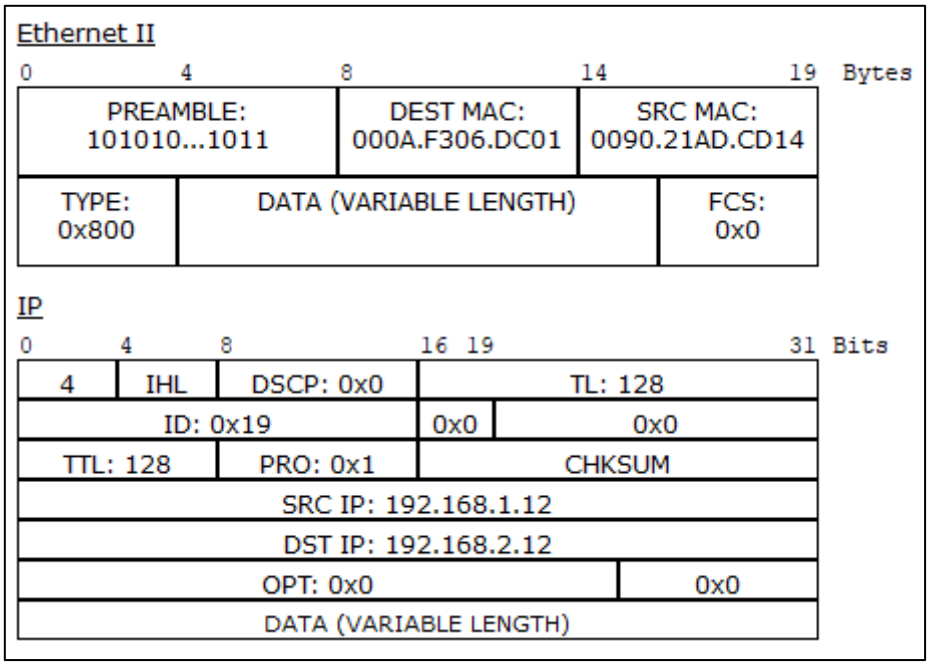
入站层（In Layers）信息显示数据包是如何被路由器接收的：

- Layer 3:IP 头信息显示源 IP 为 192.168.1.12,目的 IP 为 192.168.2.12。
- Layer 2:以太网 II 头信息展示源 MAC 地址为 0090.21AD.CD14,目的 MAC 地址为 000A.F306.DC01。
- Layer 1：表明该数据包是通过端口 FastEthernet0/0 进入路由器的。
- 出站 PDU 细节（Outbound PDU Details）

出站层（Out Layers）信息显示数据包在经过路由器处理后如何出站：

- Layer 3：IP 头部信息不变，仍然显示源 IP 为 192.168.1.12 和目的 IP 为 192.168.2.12。
- Layer 2：以太网 II 头信息此时展示的源 MAC 地址变为路由器的源 MAC 地址 000A.F306.DC02，而目的 MAC 地址变为另一个 MAC 地址（可能是下一个跳转目标的 MAC 地址）00E0.8F48.E19B。
- Layer 1：数据包现在是通过端口 FastEthernet0/1 离开路由器的。

1.2 PDU Information at Device: Router0（Inbound PDU Details）



以太网 II（Ethernet II）：

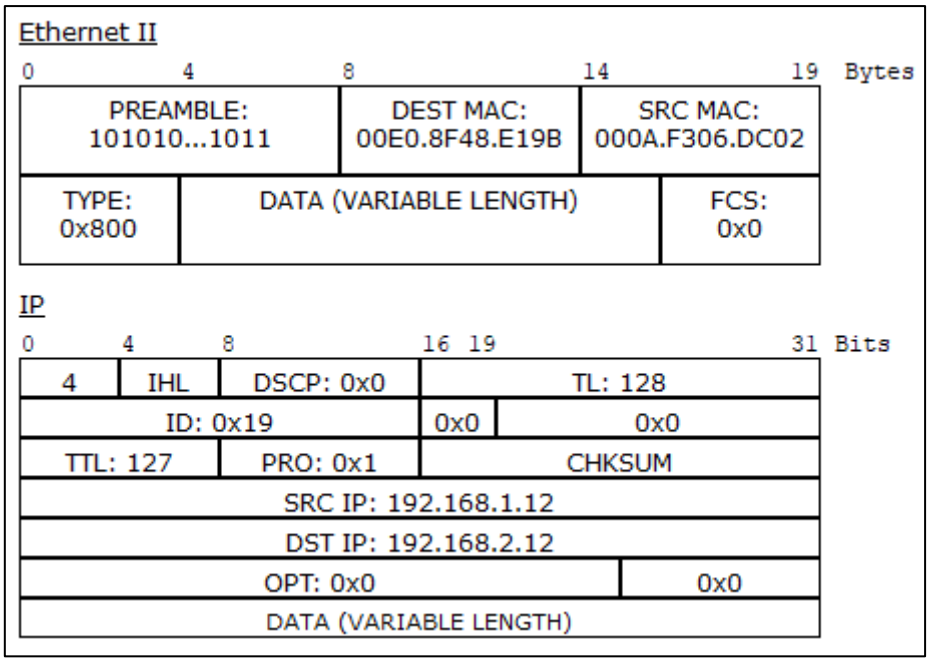
- 前导码（Preamble）：101010...1011，用于帧的同步。
- 目的 MAC 地址（DEST MAC）：000A.F306.DC01，是路由器接口或下一个跳转的 MAC 地址。
- 源 MAC 地址（SRC MAC）：0090.21AD.CD14，是发送者的 MAC 地址。

- 类型（Type）：0x800，说明后面跟随的是一个 IP 协议的数据包。
- 数据（Data）：可变长度。
- 帧检验序列（FCS）：0x0，用于检测帧在传输过程中的错误。

IP：

- 版本（Version）：4，指的是 IPv4。
- 头部长度（IHL - Internet Header Length）：通常表示 IP 头部的长度。
- 差分服务代码点（DSCP）：0x0，用于分类流量。
- 生存时间（TTL - Time To Live）：128，数据包可经过的最大路由器数目。
- 协议（Protocol）：0x1。
- 总长度（Total Length, TL）：128 字节。
- 标识（Identification, ID）：0x19，用于唯一识别分组的序列号。
- 头部校验和（Checksum）：用于验证头部信息的正确性。
- 源 IP 地址（SRC IP）：192.168.1.12，发送者的 IP 地址。
- 目的 IP 地址（DST IP）：192.168.2.12，接收者的 IP 地址。
- 选项（Options, OPT）：0x0，可能用于各种 IP 功能，但在此为空。

1.3 PDU Information at Device: Router0（Outbound PDU Details）



以太网 II（Ethernet II）：

- 前导码（Preamble）：用于帧同步的二进制模式，这里以 101010...1011

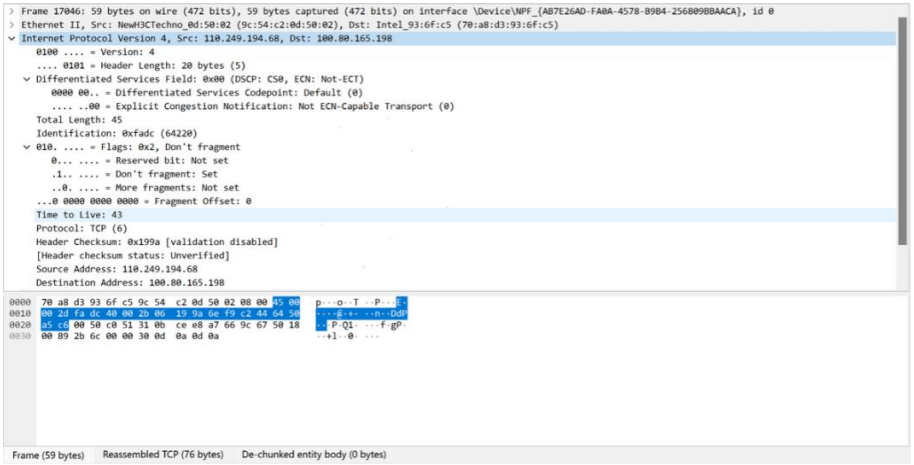
展示。

- 目的 MAC 地址（DEST MAC）：00E0.8F48.E19B，指向的是下一跳或最终目的地址的硬件地址。
- 源 MAC 地址（SRC MAC）：000A.F306.DC02，代表路由器的发送接口的硬件地址。
- 类型（Type）：0x800，表明该帧是一个 IP 数据包。
- 数据（Data）：可变长度。
- 帧检验序列（Frame Check Sequence, FCS）：0x0，用于错误检测（在实际网络中使用，但在模拟中可能不展示真实值）。

IP：

- 版本（Version）：4，指代 IPv4。
- 头部长度（Internet Header Length, IHL）：头部的字节长度。
- 差分服务代码点（Differentiated Services Code Point, DSCP）：0x0，用于指定数据包的服务类型。
- 总长度（Total Length, TL）：128 字节，表示整个 IP 数据包的长度。
- 标识（Identification, ID）：0x19，用于分片和重组的标识符。
- 生存时间（Time To Live, TTL）：127，每过一个路由器节点减 1。
- 协议（Protocol, PRO）：0x1。
- 头部校验和（Checksum）：用于检测头部信息是否被更改。
- 源 IP 地址（Source IP, SRC IP）：192.168.1.12。
- 目的 IP 地址（Destination IP, DST IP）：192.168.2.12。

2. 用 WireShark 抓取 IP 数据包，并解读如下：



- 版本 (Version): 4 - 这表明数据报使用的是 IPv4 协议。
- 首部长度 (Header Length): 20 字节（5 个 32 位字）- 这指示首部长度为 20 字节，不包含任何选项。
- 区分服务字段 (Differentiated Services Field, DSCP): 0x00 - 这表明没有设置特殊的区分服务或流量优先级。
- 总长度 (Total Length): 45 字节 - 这个字段指示整个 IP 数据报的长度（包括首部和数据）。但这似乎是截图中显示不全或误解的数值，因为 45 字节过小，不太可能仅包括首部和有效载荷。
- 标识 (Identification): 0xf4ac - 用于标识主机发送的每个数据报，关键用于数据报的分片和重组。
- 标志 (Flags): Don't Fragment (DF) - 这表示数据报不应被分片。
- 片偏移 (Fragment Offset): 0 - 表示该数据包是更大数据包的第一个片段或完整包。
- 生存时间 (Time to Live, TTL): 43 - 表示数据报可以在网络中的最大跳数。
- 协议 (Protocol): TCP (6) - 表明此数据报的上层协议是 TCP。
- 头部校验和 (Header Checksum): 用于检测在传输过程中首部信息是否出现错误。
- 源 IP 地址 (Source Address): 110.249.194.68 - 数据包的发送方地址。
- 目的 IP 地址 (Destination Address): 100.80.165.198 - 数据包的接收方地址。

【分析讨论】

一、配置 Web 服务器并从客户端查看

在配置了 Web 服务器并设置了静态 IP 地址之后，从客户端通过浏览器访问服务器网址能成功加载页面。这显示了 IP 地址和网络配置的正确性，以及 HTTP 协议在客户端和服务器之间如何工作。成功的页面加载证实了网络层到应用层的各个组件都被正确设置和协调工作。

二、用 WireShark 抓取 IP 数据包

使用 WireShark 捕获了在网络上传输的数据包。通过分析这些数据包，可以观察到 IP 头部的详细信息，包括但不限于源地址、目的地址、总长度、协议等。这有助于理解网络数据流动和协议的实际应用。WireShark 作为一个强大的网络分析工具，使我们能够实时捕获和分析网络交通，是网络管理和故障排除的关键工具。

三、查看 IP 报文字段内容并解读

实验详细解读了 IP 报文的各个字段，包括版本、首部长度、服务类型等。每个字段的解读不仅加深了对 IP 协议的理解，也揭示了数据包是如何根据不同的需求被处理和优先级分配的。特别是分片和重组机制的理解，对于处理跨网络数据传输至关重要。

四、分析在 Packet Tracer 中 IP 报文情况

通过使用 Packet Tracer，模拟了网络环境并观察了 IP 数据包在各网络设备间的传输过程。Packet Tracer 提供了一个动态的可视化界面，允许观察和跟踪数据包的每一步行为。通过详细的数据包信息，我们可以看到如何通过路由器和交换机处理和转发 IP 数据包，并且能够验证各种网络配置和协议的影响，比如 IP 路由、子网划分以及网络层的错误处理。