实验 21：以太网帧分析实验

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	2024/04/25

【实验目的】

1. 了解并识别 MAC 地址以及其在网络通信中的重要性。MAC 地址是网络设备的物理地址，对于网络中设备的识别和通信至关重要。
2. 使用 Wireshark 这一网络分析工具，抓取并分析 MAC 数据包。Wireshark 是一款强大的网络协议分析工具，能帮助学生理解网络通信过程中数据的传输和处理。
3. 深入理解以太网的数据帧结构，包括前导码、帧开始符、MAC 地址、以太类型字段等。
4. 观察并分析在使用 ICMP（如 ping 命令）数据包转发过程中 MAC 地址的变化情况，以加深对网络层与数据链路层交互作用的理解。

【实验原理】

一、以太网

以太网是一种广泛应用的计算机局域网技术，由 IEEE 的 IEEE 802.3 标准制定。这一标准涵盖了包括物理层连线、电子信号传输以及介质访问控制层协议的详细规定。因其高效和广泛的应用，以太网已成为当今最常见的局域网技术之一。

以太网有两种主要形式：经典以太网和交换式以太网。经典以太网是以太网的原始形式，其数据传输速率从 3 Mbps 到 10 Mbps 不等。而交换式以太网则支持更高的数据传输速率，包括 100 Mbps、1 Gbps（千兆以太网），甚至 10 Gbps（万兆以太网）。

在网络拓扑结构上，以太网从原来的总线型拓扑逐渐演变为星型拓扑。这种变化主要是通过使用交换机来实现的，目的是为了减少数据传输中的冲突，提高网络速度和效率。即使在物理结构上采用星型拓扑，以太网在逻辑上依然保留了总线型拓扑的特性，并使用了 CSMA/CD（载波侦听多路访问/碰撞检测）技术来管理数据传输。

以太网的每一个设备都有一个全球唯一的 48 位的 MAC 地址，这个地址由设备的制造商在制造时分配并烧录在网络接口卡上。MAC 地址的唯一性保证了网络

中的设备能够相互识别和通信。随着以太网技术的普及，许多设备制造商开始将以太网接口直接集成到计算机的主板中。

总体而言，以太网技术的普及和发展极大地促进了网络通信的效率和可靠性，使得网络设备的互联互通成为可能。

二、MAC 地址

MAC 地址，全称为媒体访问控制地址（Media Access Control address），是网络设备在制造过程中固化在网络接口卡（Network Interface Card, NIC）的唯一标识符。这个地址通常被存储在网卡的 EPROM（一种可编程读写的存储芯片）中，并可以通过特定程序进行修改。

MAC 地址共有 48 位，等同于 6 个字节，通常用十六进制表示，分为两部分：制造商标识符和设备标识符。例如，MAC 地址“00-16-EA-AE-3C-40”中，“00-16-EA”是由 IEEE（电气与电子工程师协会）分配给网络硬件制造商的 OUI（Organizationally Unique Identifier，组织唯一标识符），用于区分不同的制造商。“AE-3C-40”则是该制造商分配给具体网络产品的标识，代表了网卡或其他网络设备的系列号。

在 MAC 地址的编码中，最高有效字节的第二位（LSb，低第二位）称为 U/L 位（Universal/Local），用于表示地址是全球统一的还是局部使用的。如果此位为 0，表示地址是全局统一的；如果为 1，则表示地址是局部使用的。所有标准的 OUI 分配都将此位设置为 0。

此外，MAC 地址的最高有效字节的最低位（LSb，低第一位）用于指示地址是单播还是多播。如果此位为 0，表示是单播地址，用于单个设备；如果此位为 1，则表示是多播地址，用于多个设备。

MAC 地址的全球唯一性和这些结构特点使得在网络中每个设备都可以具有独一无二的身份，从而在数据传输过程中能够确保数据准确地发送至正确的目的地。

三、MAC 数据包格式

MAC 数据包格式，尤其是以太网环境下的 Ethernet II 帧结构，对于理解网络通信的基本机制至关重要。下面是对以太网帧的详细介绍，主要关注于 Ethernet II 帧格式，这是目前最常用的以太网数据包格式：

1. 帧间距：以太网帧之间需要有至少 12 字节的空闲线路状态码，也称为帧间隔，这有助于区分连续的数据帧，确保数据传输的清晰界限。
2. 以太帧类型：以太网支持多种帧类型，每种帧都有其特定的结构和最大传输单元（MTU）值。Ethernet II 帧（也称为 DIX 帧）是其中最常见的类型，直接支持 IP 协议等上层协议。
3. Ethernet II 帧格式：
   - 前导码和帧开始符：通常帧的开始有一个特定的前导码和帧开始符，用来标示帧的起始点。
   - 目标 MAC 地址和源 MAC 地址：每个 Ethernet II 帧都包含 6 字节的目标 MAC 地址和 6 字节的源 MAC 地址，分别指定帧的接收者和发送者。
   - 类型字段：紧随 MAC 地址后的是两字节的类型字段，用于指定帧中承载的数据类型。例如，0x0800 代表 IPv4 数据，0x0806 代表 ARP 请求，0x86DD 代表 IPv6 数据。
4. 长度与类型字段的区分：
   - 在早期的以太网版本中，这个字段被用来表示数据的长度，但在 Ethernet II 标准中，它被用作类型字段。
   - 如果该字段的值大于或等于 1536（0x0600），则解释为类型字段，表明帧是一个 Ethernet II 帧。
   - 如果该字段的值在 46 到 1500 字节之间（不包括 1500～1536 的未定义区域），则表示帧长度，并且帧遵循 IEEE 802.3 标准。
5. 数据和帧校验序列：类型字段后是数据负载，长度可变。每个帧的末尾包括一个 32 位的循环冗余校验码（CRC），用于检测传输过程中的错误。

这种结构的设计使得 Ethernet II 帧能够高效地支持多种网络协议，同时保持数据传输的准确性和可靠性，是网络通信中的基础设施之一。

802.3 以太网帧结构

前导码	帧开始符	MAC 目标地址	MAC 源地址	802.1Q 标签 (可选)	以太类型	负载	冗余校验	帧间距
10101010 7个octet	10101011 1个octet	6 octets	6 octets	(4 octets)	2 octets	46–1500 octets	4 octets	12 octets
		64–1522 octets						
72–1530 octets								
84–1542 octets								

【实验设备】

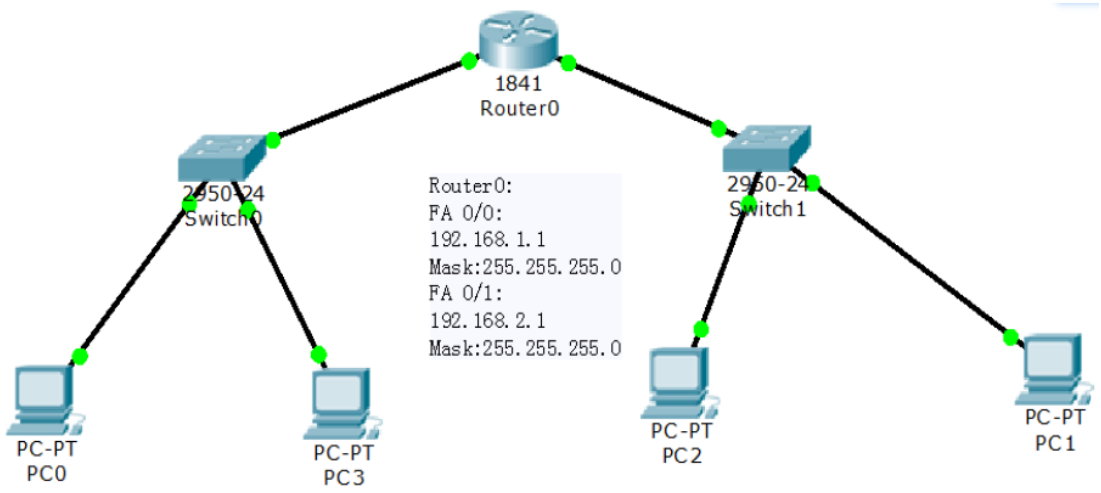
1. 操作系统：Windows 10

2. 网络环境：局域网

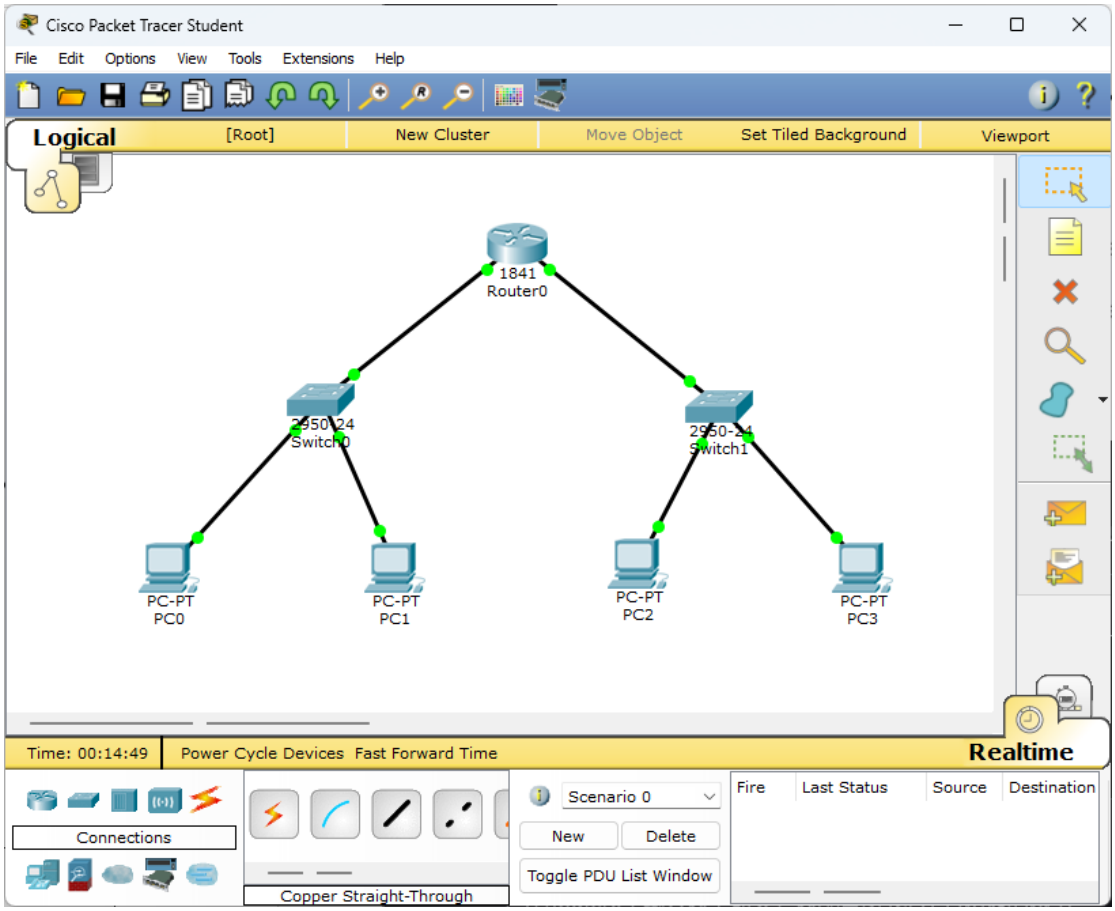
3. 应用程序：Cisco Packet Tracer 6.0

【实验步骤】

1. 规划网络地址及拓扑图。

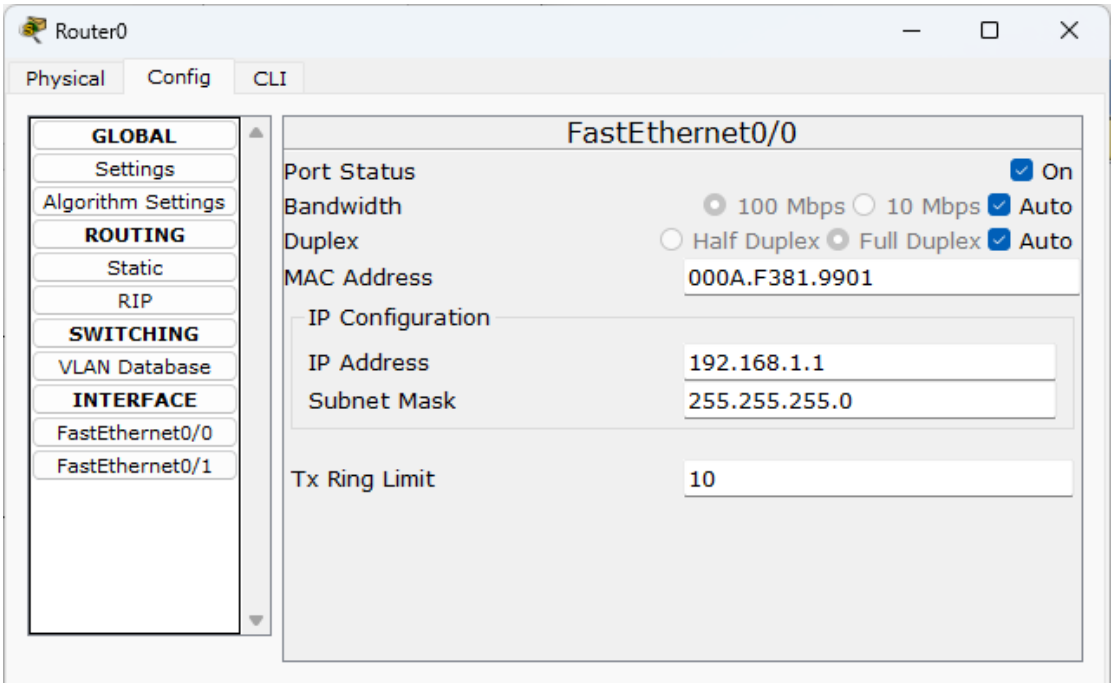


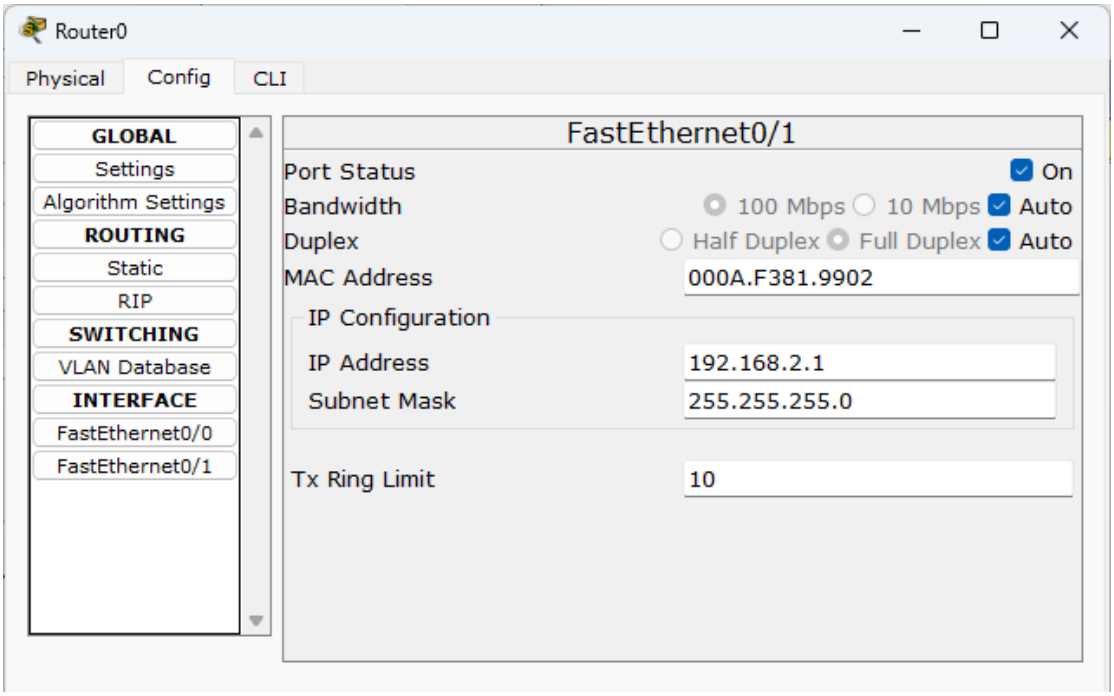
2. 启动 Cisco Packet Tracer，按照上图连接网络。



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
```





4. 配置 DHCP 前查看各 PC IP 地址情况。
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
```

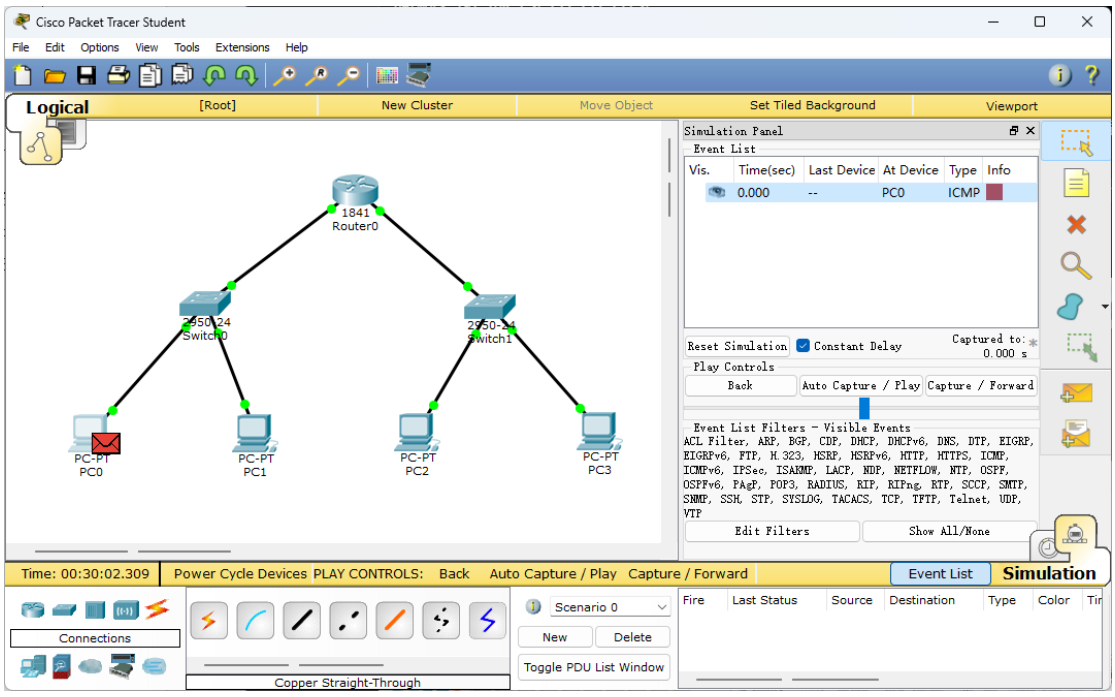
6. 配置 DHCP 后查看各 PC IP 地址情况。

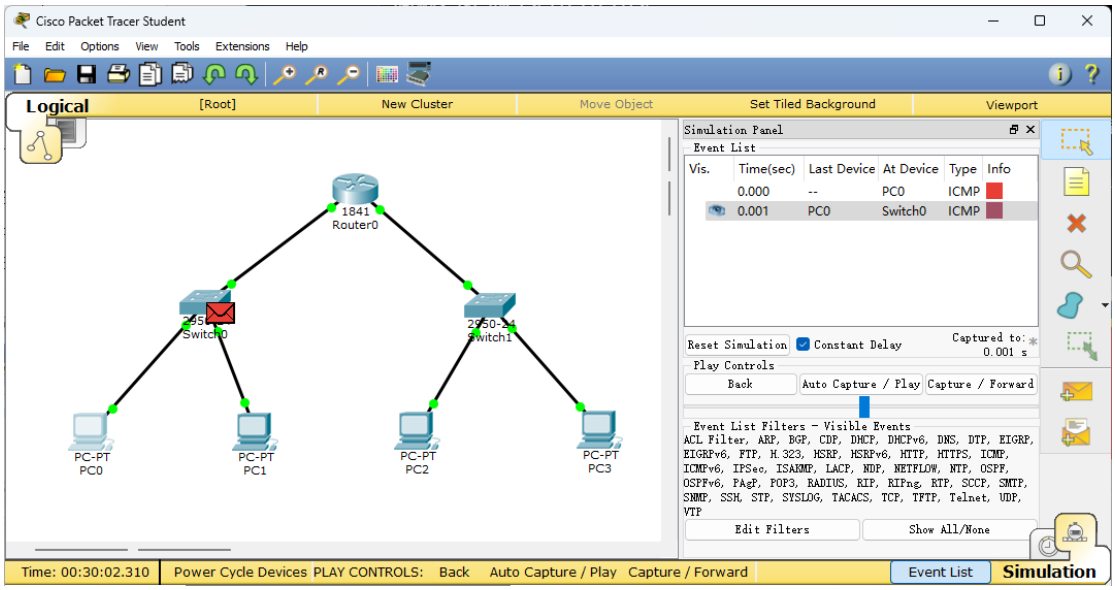
7. 从 Realtime 模式切换至 Simulation 模式，模拟 ICMP（ping 命令）。

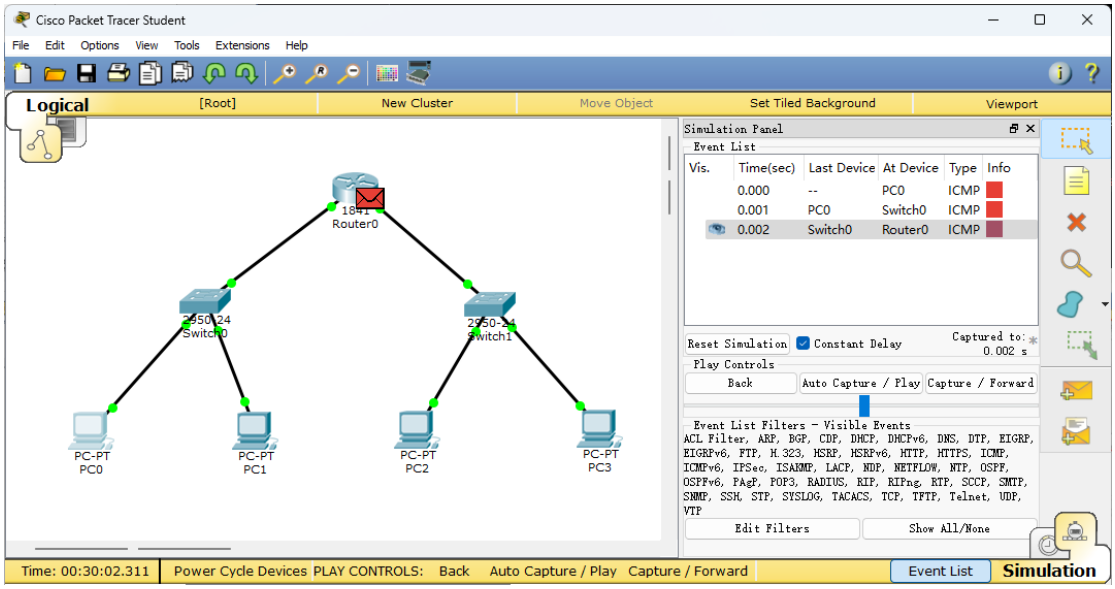
   7.1 在 PC0 的终端输入 ping 192.168.2.12 命令，即 ping PC2。

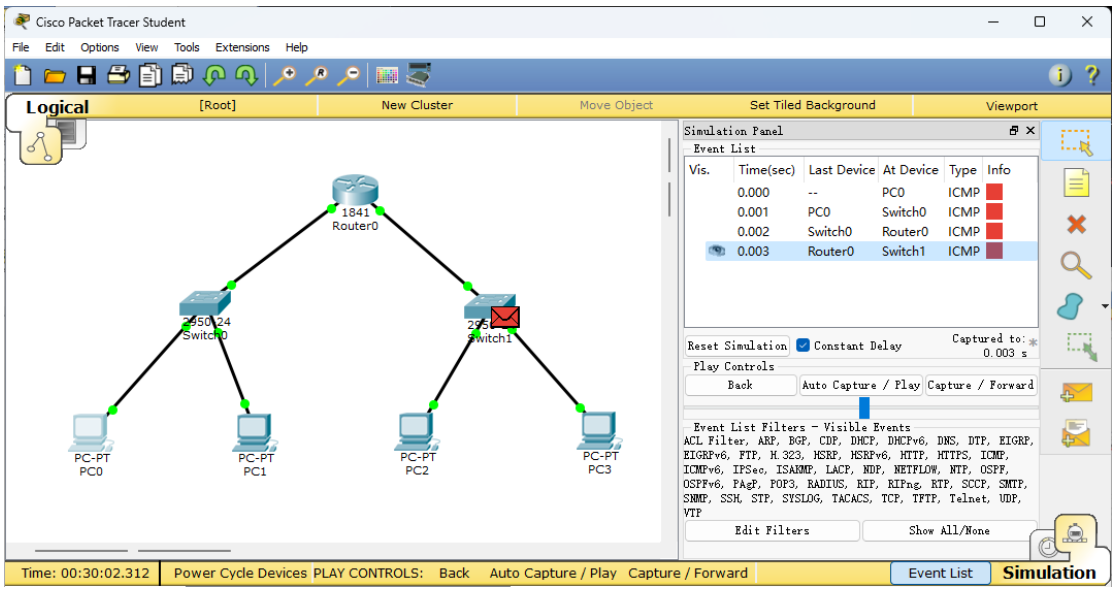
   7.2 点击 Capture/Forward 单步执行，也可以点击 Auto Capture/Play 自动执行，查看相关数据。

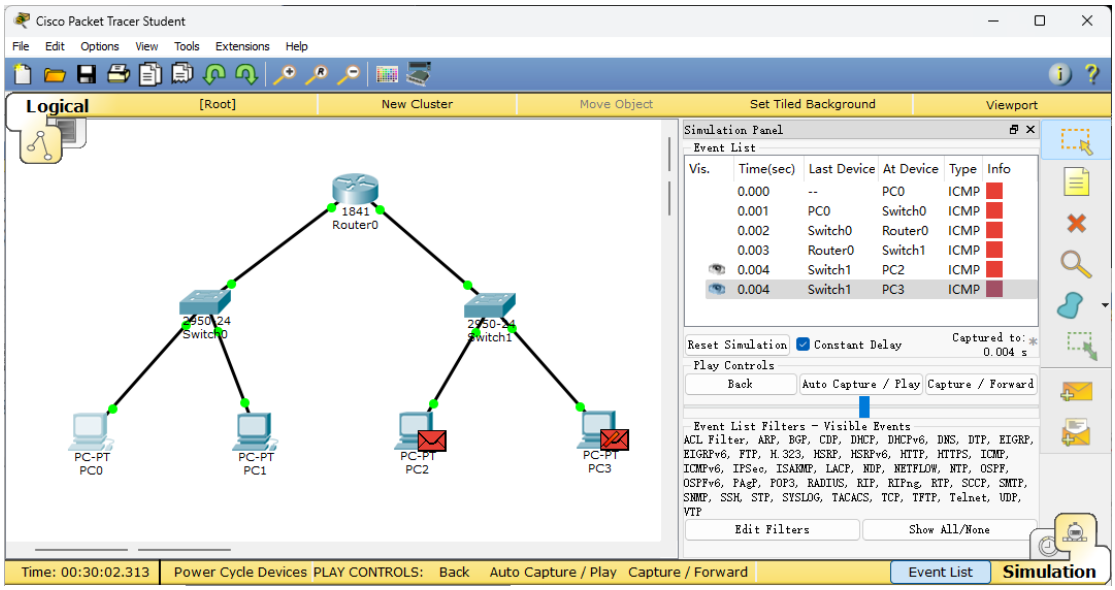
   7.3 在 Even List 中的 Info 栏可以查看相关信息。

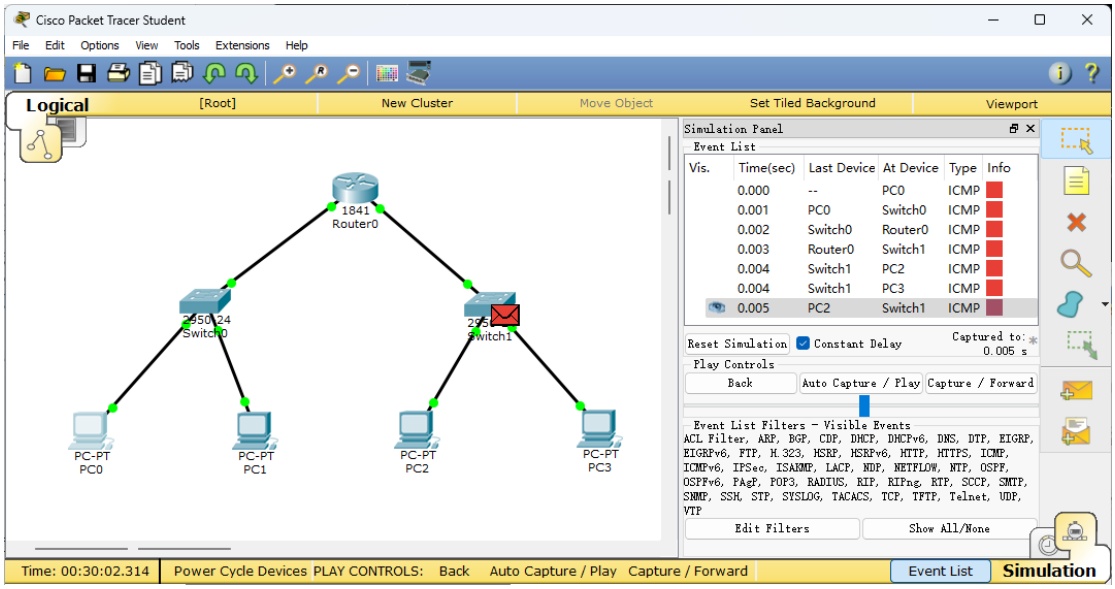


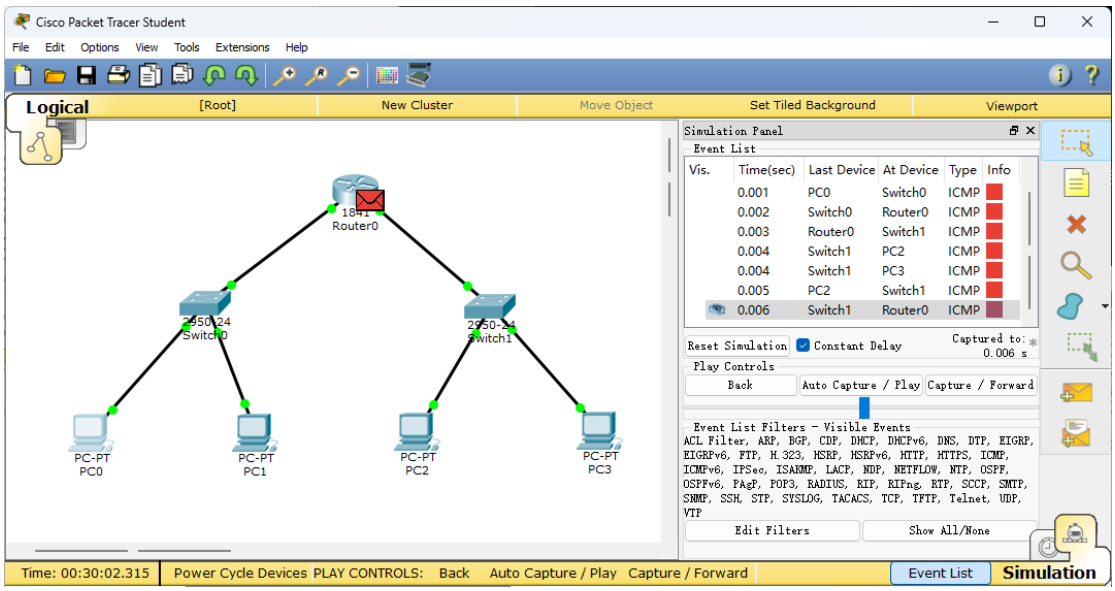

Cisco Packet Tracer Student
File Edit Options View Tools Extensions Help
Logical [Root] New Cluster Move Object Set Tiled Background Viewport
1841 Router0
2950-24 Switch0
2950-24 Switch1
PC-PT PC0
PC-PT PC1
PC-PT PC2
PC-PT PC3
Simulation Panel
Event List
Vis. Time(sec) Last Device At Device Type Info
0.000 -- PC0 ICMP
0.001 PC0 Switch0 ICMP
Reset Simulation Constant Delay Captured to: 0.001 s
Play Controls
Back Auto Capture / Play Capture / Forward
Event List Filters - Visible Events
ACL Filter, ARP, BGP, CDP, DHCP, DHCPv6, DNS, DTP, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, LACP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, RADIUS, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP
Edit Filters Show All/None
Time: 00:30:02.310 Power Cycle Devices PLAY CONTROLS: Back Auto Capture / Play Capture / Forward Event List Simulation

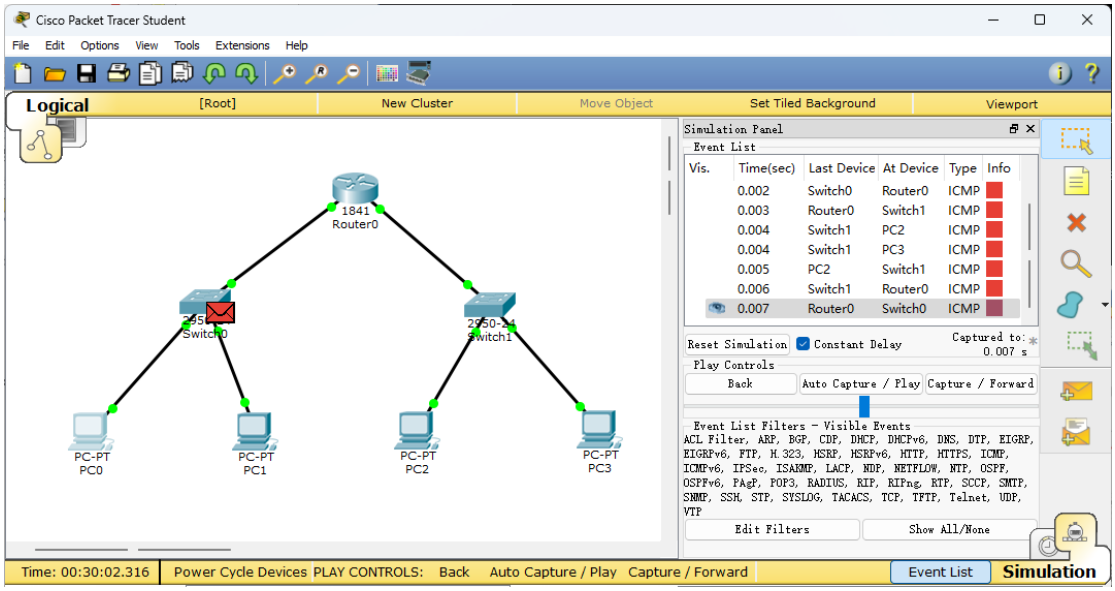

Cisco Packet Tracer Student
File Edit Options View Tools Extensions Help
Logical [Root] New Cluster Move Object Set Tiled Background Viewport
1841 Router0
2950-24 Switch0
2950-24 Switch1
PC-PT PC0
PC-PT PC1
PC-PT PC2
PC-PT PC3
Simulation Panel
Event List
Vis. Time(sec) Last Device At Device Type Info
0.000 -- PC0 ICMP
0.001 PC0 Switch0 ICMP
0.002 Switch0 Router0 ICMP
Reset Simulation Constant Delay Captured to: 0.002 s
Play Controls
Back Auto Capture / Play Capture / Forward
Event List Filters - Visible Events
ACL Filter, ARP, BGP, CDP, DHCP, DHCPv6, DNS, DTP, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, LACP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, RADIUS, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP
Edit Filters Show All/None
Time: 00:30:02.311 Power Cycle Devices PLAY CONTROLS: Back Auto Capture / Play Capture / Forward Event List Simulation

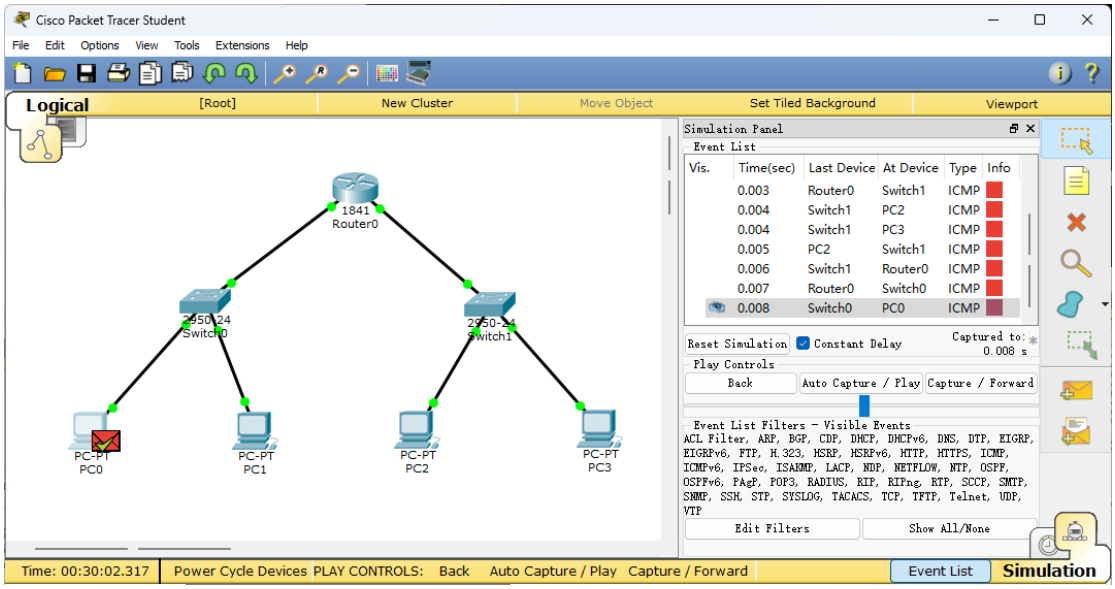

Cisco Packet Tracer Student
File Edit Options View Tools Extensions Help
Logical [Root] New Cluster Move Object Set Tiled Background Viewport
1841 Router0
2950-24 Switch0
2950-24 Switch1
PC-PT PC0
PC-PT PC1
PC-PT PC2
PC-PT PC3
Simulation Panel
Event List
Vis. Time(sec) Last Device At Device Type Info
0.000 -- PC0 ICMP
0.001 PC0 Switch0 ICMP
0.002 Switch0 Router0 ICMP
0.003 Router0 Switch1 ICMP
Reset Simulation Constant Delay Captured to: 0.003 s
Play Controls
Back Auto Capture / Play Capture / Forward
Event List Filters - Visible Events
ACL Filter, ARP, BGP, CDP, DHCP, DHCPv6, DNS, DTP, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, LACP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, RADIUS, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP
Edit Filters Show All/None
Time: 00:30:02.312 Power Cycle Devices PLAY CONTROLS: Back Auto Capture / Play Capture / Forward Event List Simulation


Cisco Packet Tracer Student
File Edit Options View Tools Extensions Help
Logical [Root] New Cluster Move Object Set Tiled Background Viewport
1841 Router0
2950-24 Switch0
2950-24 Switch1
PC-PT PC0
PC-PT PC1
PC-PT PC2
PC-PT PC3
Simulation Panel
Event List
Vis. Time(sec) Last Device At Device Type Info
0.000 -- PC0 ICMP
0.001 PC0 Switch0 ICMP
0.002 Switch0 Router0 ICMP
0.003 Router0 Switch1 ICMP
0.004 Switch1 PC2 ICMP
0.004 Switch1 PC3 ICMP
Reset Simulation Constant Delay Captured to: 0.004 s
Play Controls
Back Auto Capture / Play Capture / Forward
Event List Filters - Visible Events
ACL Filter, ARP, BGP, CDP, DHCP, DHCPv6, DNS, DTP, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, LACP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, RADIUS, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP
Edit Filters Show All/None
Time: 00:30:02.313 Power Cycle Devices PLAY CONTROLS: Back Auto Capture / Play Capture / Forward Event List Simulation


Cisco Packet Tracer Student
File Edit Options View Tools Extensions Help
Logical [Root] New Cluster Move Object Set Tiled Background Viewport
1841 Router0
2950-24 Switch0
2950-24 Switch1
PC-PT PC0
PC-PT PC1
PC-PT PC2
PC-PT PC3
Simulation Panel
Event List
Vis. Time(sec) Last Device At Device Type Info
0.000 -- PC0 ICMP
0.001 PC0 Switch0 ICMP
0.002 Switch0 Router0 ICMP
0.003 Router0 Switch1 ICMP
0.004 Switch1 PC2 ICMP
0.004 Switch1 PC3 ICMP
0.005 PC2 Switch1 ICMP
Reset Simulation Constant Delay Captured to: 0.005 s
Play Controls
Back Auto Capture / Play Capture / Forward
Event List Filters - Visible Events
ACL Filter, ARP, BGP, CDP, DHCP, DHCPv6, DNS, DTP, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, LACP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, RADIUS, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP
Edit Filters Show All/None
Time: 00:30:02.314 Power Cycle Devices PLAY CONTROLS: Back Auto Capture / Play Capture / Forward Event List Simulation


Cisco Packet Tracer Student
File Edit Options View Tools Extensions Help
Logical [Root] New Cluster Move Object Set Tiled Background Viewport
1841 Router0
2950-24 Switch0
2950-24 Switch1
PC-PT PC0
PC-PT PC1
PC-PT PC2
PC-PT PC3
Simulation Panel
Event List
Vis. Time(sec) Last Device At Device Type Info
0.001 PC0 Switch0 ICMP
0.002 Switch0 Router0 ICMP
0.003 Router0 Switch1 ICMP
0.004 Switch1 PC2 ICMP
0.004 Switch1 PC3 ICMP
0.005 PC2 Switch1 ICMP
0.006 Switch1 Router0 ICMP
Reset Simulation Constant Delay Captured to: 0.006 s
Play Controls
Back Auto Capture / Play Capture / Forward
Event List Filters - Visible Events
ACL Filter, ARP, BGP, CDP, DHCP, DHCPv6, DNS, DTP, EIGRP, EIGRPv6, FTP, H.323, HSRP, HSRPv6, HTTP, HTTPS, ICMP, ICMPv6, IPSec, ISAKMP, LACP, NDP, NETFLOW, NTP, OSPF, OSPFv6, PAgP, POP3, RADIUS, RIP, RIPng, RTP, SCCP, SMTP, SNMP, SSH, STP, SYSLOG, TACACS, TCP, TFTP, Telnet, UDP, VTP
Edit Filters Show All/None
Time: 00:30:02.315 Power Cycle Devices PLAY CONTROLS: Back Auto Capture / Play Capture / Forward Event List Simulation

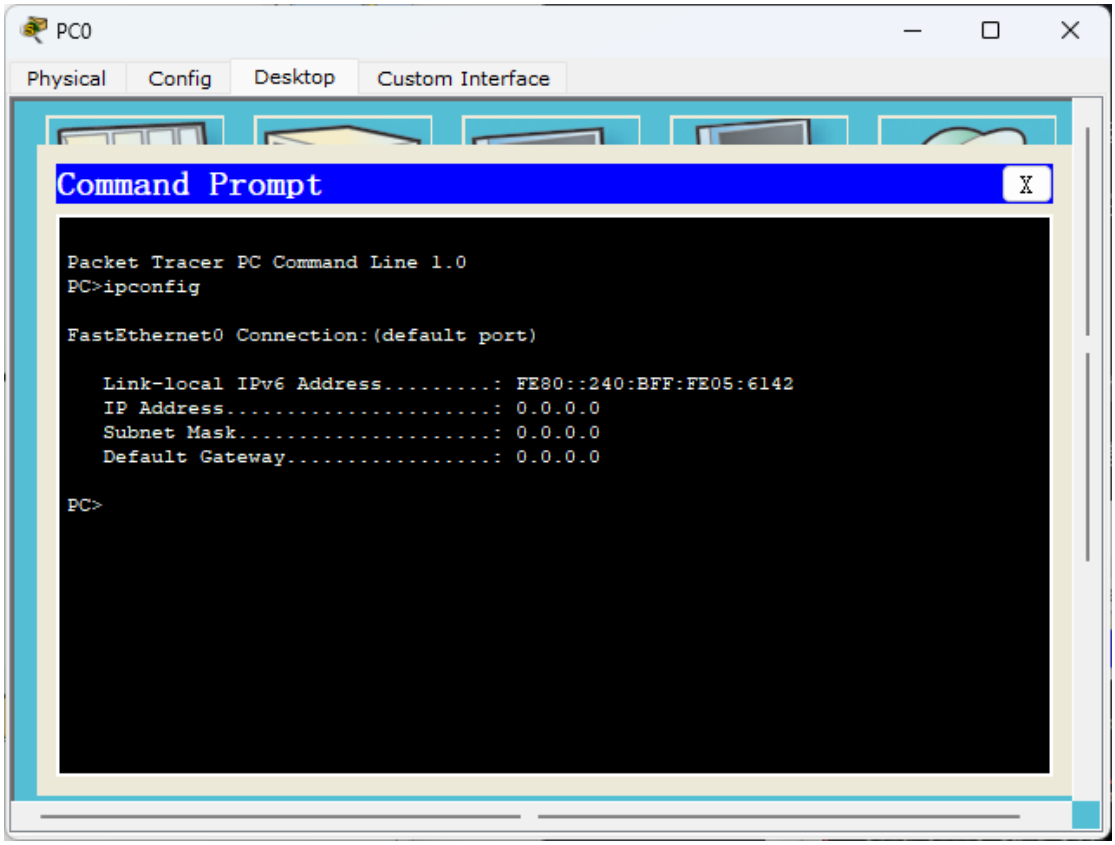


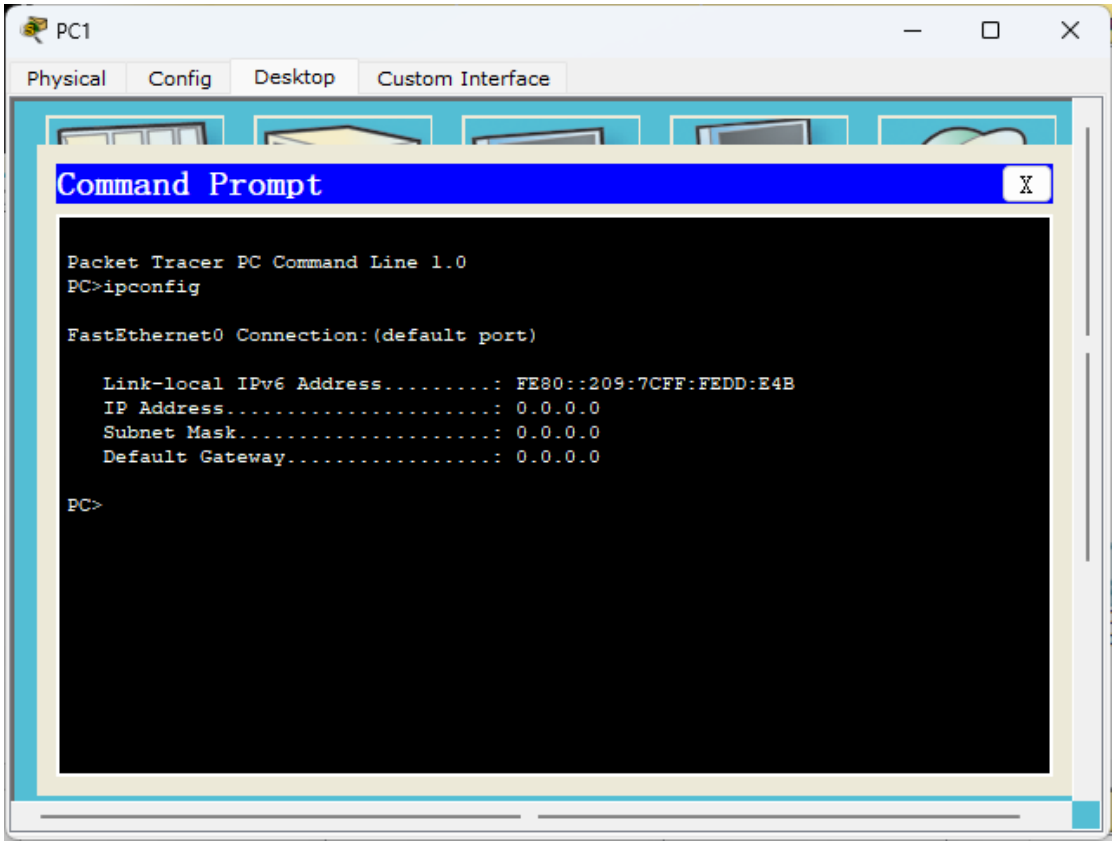


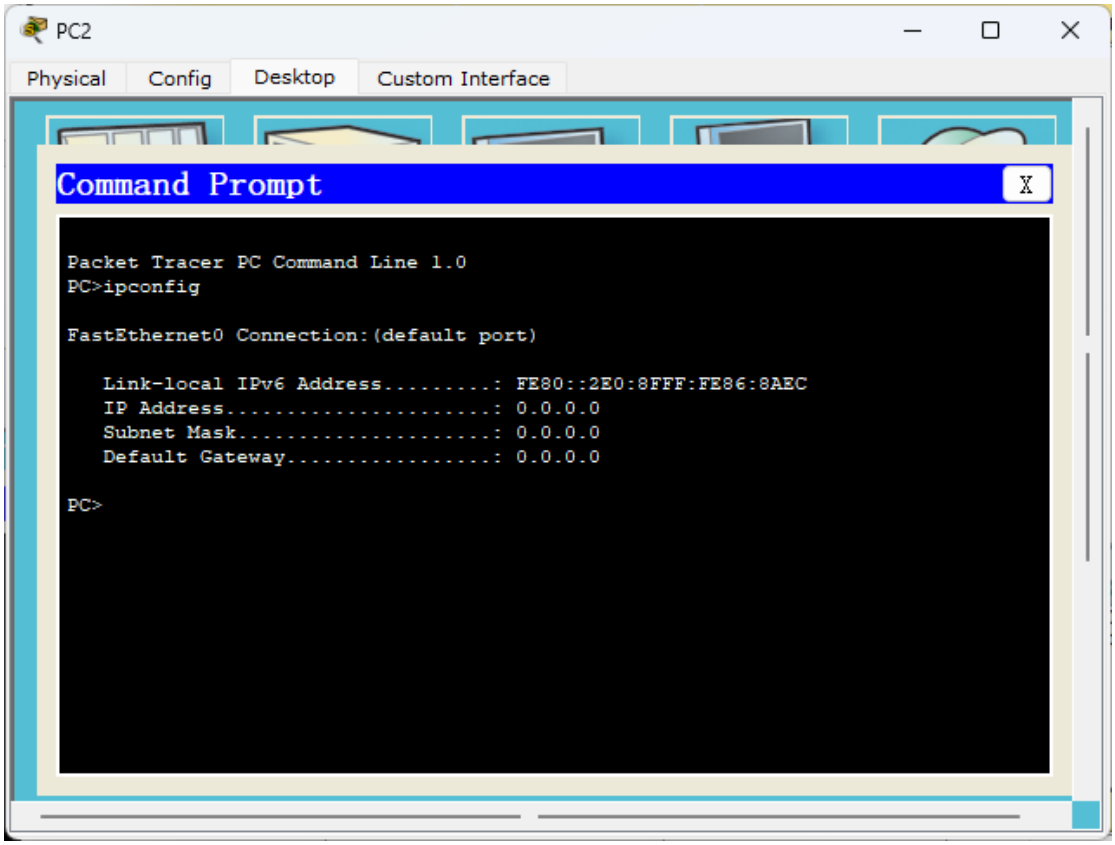
8. 本机命令提示符输入 ipconfig/all 命令，查看本机的 MAC 地址。
9. 安装 WireShark 软件并练习使用，并分析 MAC DIX V2 帧。
10. 用 WireShark 抓取 MAC 数据包，选用 WLAN 方式进行抓包。
11. 查看 MAC 数据包字段内容，并解读。
12. 分析在 Cisco Packet Tracer 中模拟 ICMP（ping 命令），ICMP 数据包转发过程中 MAC 地址变化情况。

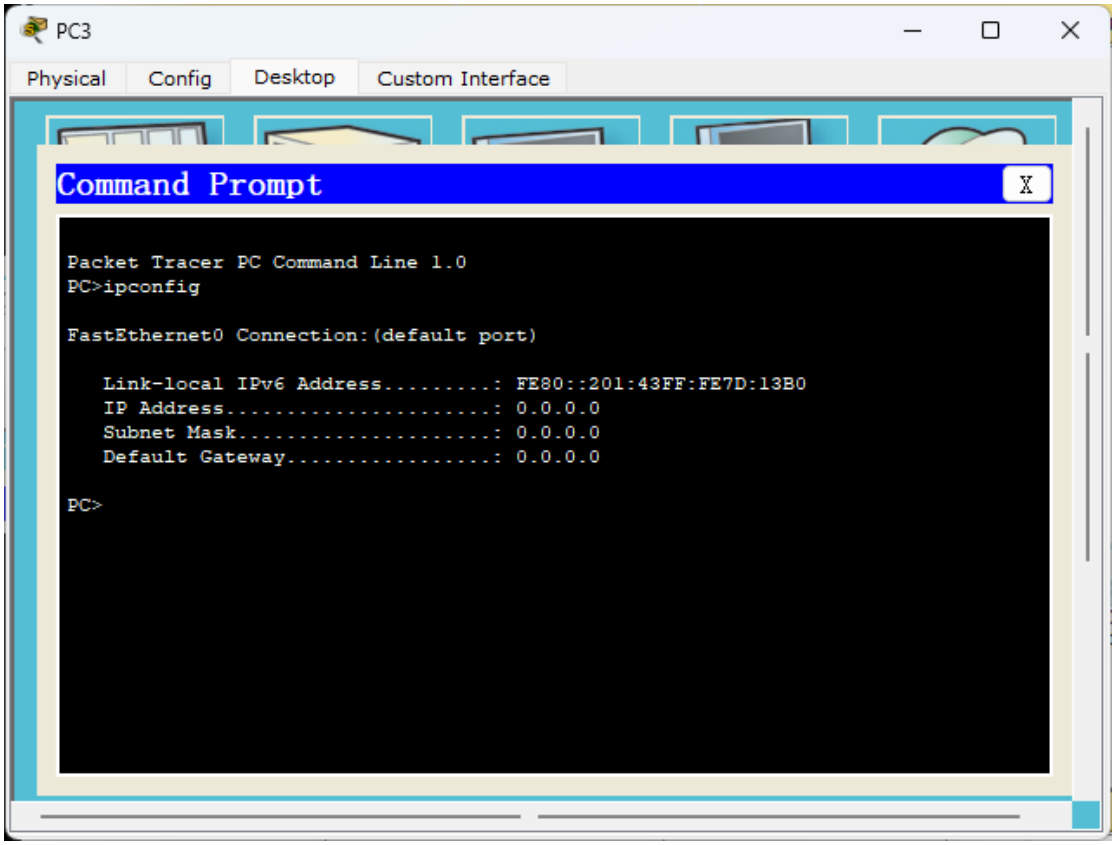
【实验现象】

1. 配置 DHCP 前查看各 PC IP 地址情况，各 PC 机的 IP 地址、子网掩码、默认网关均相同，为 0.0.0.0。


PC0
Physical
Config
Desktop
Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ipconfig
FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::240:BFF:FE05:6142
IP Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: 0.0.0.0
PC>


PC1
Physical
Config
Desktop
Custom Interface
Command Prompt
Packet Tracer PC Command Line 1.0
PC>ipconfig
FastEthernet0 Connection:(default port)
Link-local IPv6 Address.....: FE80::209:7CFF:FEDD:E4B
IP Address.....: 0.0.0.0
Subnet Mask.....: 0.0.0.0
Default Gateway.....: 0.0.0.0
PC>





2. 配置 DHCP 后查看各 PC IP 地址情况。

- PC0：

```
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::290:21FF:FEAD:CD14
   IP Address.....: 192.168.1.12
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.1.1
```

- PC1：

```
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::207:ECFF:FECE:EB7E
   IP Address.....: 192.168.1.14
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.1.1
```

- PC2：

```
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::2E0:8FFF:FE48:E19B
   IP Address.....: 192.168.2.12
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.2.1
```

- PC3：

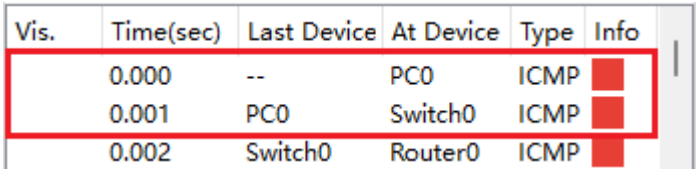
```
PC>ipconfig

FastEthernet0 Connection:(default port)

   Link-local IPv6 Address.....: FE80::20C:CFFF:FEE5:5B6D
   IP Address.....: 192.168.2.14
   Subnet Mask.....: 255.255.255.0
   Default Gateway.....: 192.168.2.1
```

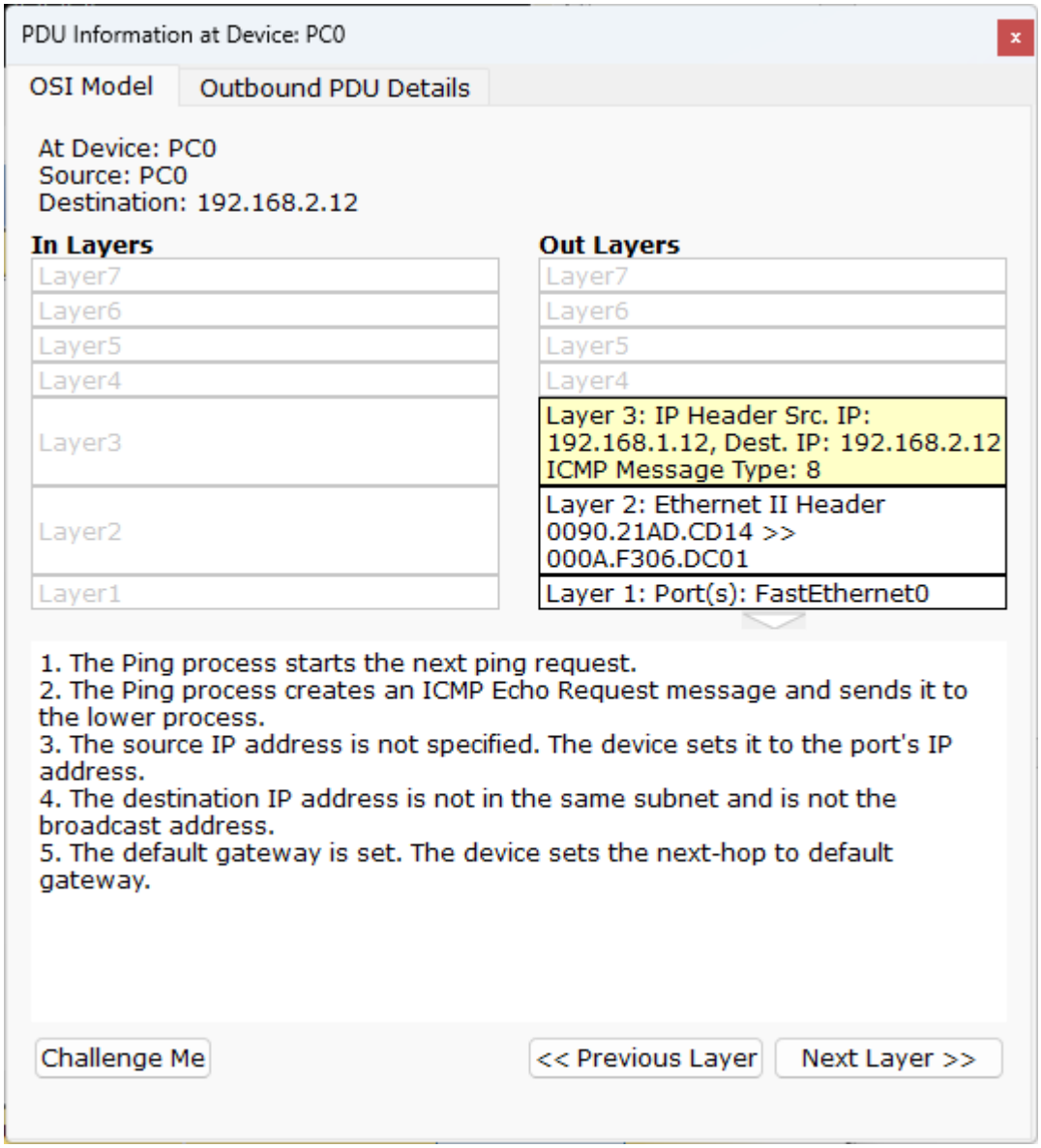
PC	IP Address	Subnet Mask	Default Gateway
PC0	192.168.1.12	255.255.255.0	192.168.1.1
PC1	192.168.1.14	255.255.255.0	192.168.1.1
PC2	192.168.2.12	255.255.255.0	192.168.2.1
PC3	192.168.2.14	255.255.255.0	192.168.2.1

3. 从 Realtime 模式切换至 Simulation 模式，模拟 ICMP（ping 命令），在 Even List 中的 Info 栏可以查看相关信息，这里分析前两个 Event 的相关数据。



Vis.	Time(sec)	Last Device	At Device	Type	Info
	0.000	--	PC0	ICMP	
	0.001	PC0	Switch0	ICMP	
	0.002	Switch0	Router0	ICMP	

3.1 PDU Information at Device: PC0（OSI Model）



这张图展示了在使用 Cisco Packet Tracer 进行网络模拟时，一个 ICMP 回显请求的数据包细节。它是根据 OSI 模型来组织的，图中包含了出站 PDU（协议数据单元）的详细信息。在 OSI 模型的不同层次上，可以看到如下信息：

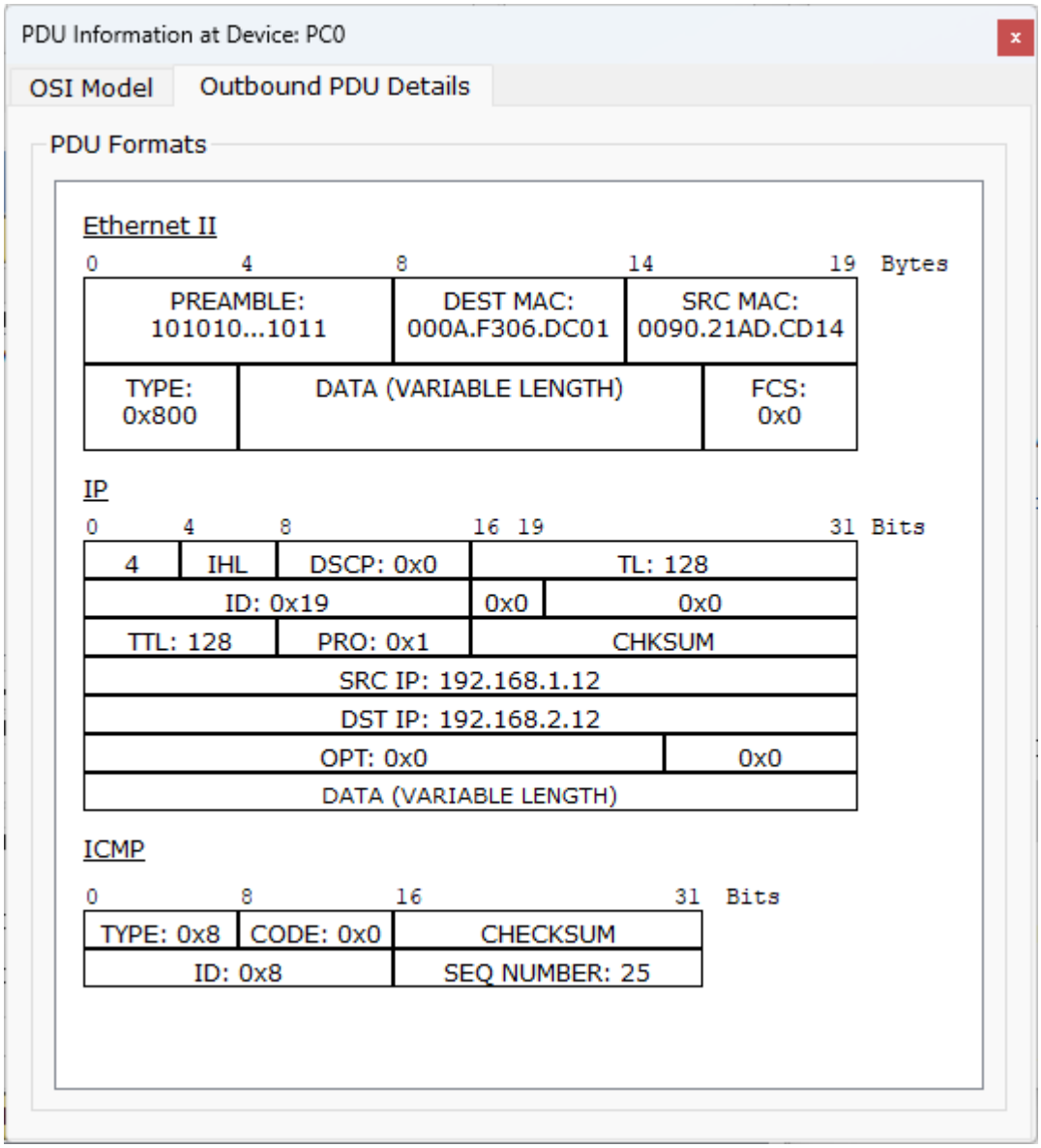
- 源地址（Source）和目的地址（Destination）被设置为 192.168.2.12。
- 出站层（Out Layers）显示数据包是如何从应用层（Layer 7）通过各个网络层逐步构建的，包括 IP 头信息（Layer 3），以及 Ethernet II 头信息（Layer 2），最后是物理层端口信息（Layer 1）。
- 在 Layer 3，我们可以看到源 IP（Src. IP）和目的 IP（Dest. IP）以及 ICMP 消息类型为 8，这是回显请求的类型。

- Layer 2 展示了以太网头信息，其中包含了 MAC 地址。
- Layer 1 指的是使用的物理端口，这里是 FastEthernet0。

屏幕底部列出的 1 至 5 点描述了 ping 过程中发生的步骤：

- Ping 过程启动下一个 ping 请求。
- Ping 过程创建了一个 ICMP 回显请求消息，并将其发送给较低层的处理过程。
- 源 IP 地址未指定，设备将其设置为端口的 IP 地址。
- 目的 IP 地址不在同一子网中，也不是广播地址。
- 已设置默认网关。设备将下一跳设置为默认网关。

3.2 PDU Information at Device: PC0（Outbound PDU Details）



这张图显示了Cisco Packet Tracer模拟中，一个ICMP数据包的出站PDU（协议数据单元)细节,涵盖了三个不同的网络层的格式:以太网II、IP和ICMP。

以太网II（Ethernet II）：

- 前导码（Preamble）：101010...1011，用于同步。
- 目的MAC地址（DEST MAC）：000A.F306.DC01。
- 源MAC地址（SRC MAC）：0090.21AD.CD14。
- 类型（Type）：0x800，表示载荷是一个IP数据包。
- 数据（Data）：可变长度，包含了封装的IP数据包。
- 帧检验序列（FCS）：0x0，用于错误检测。

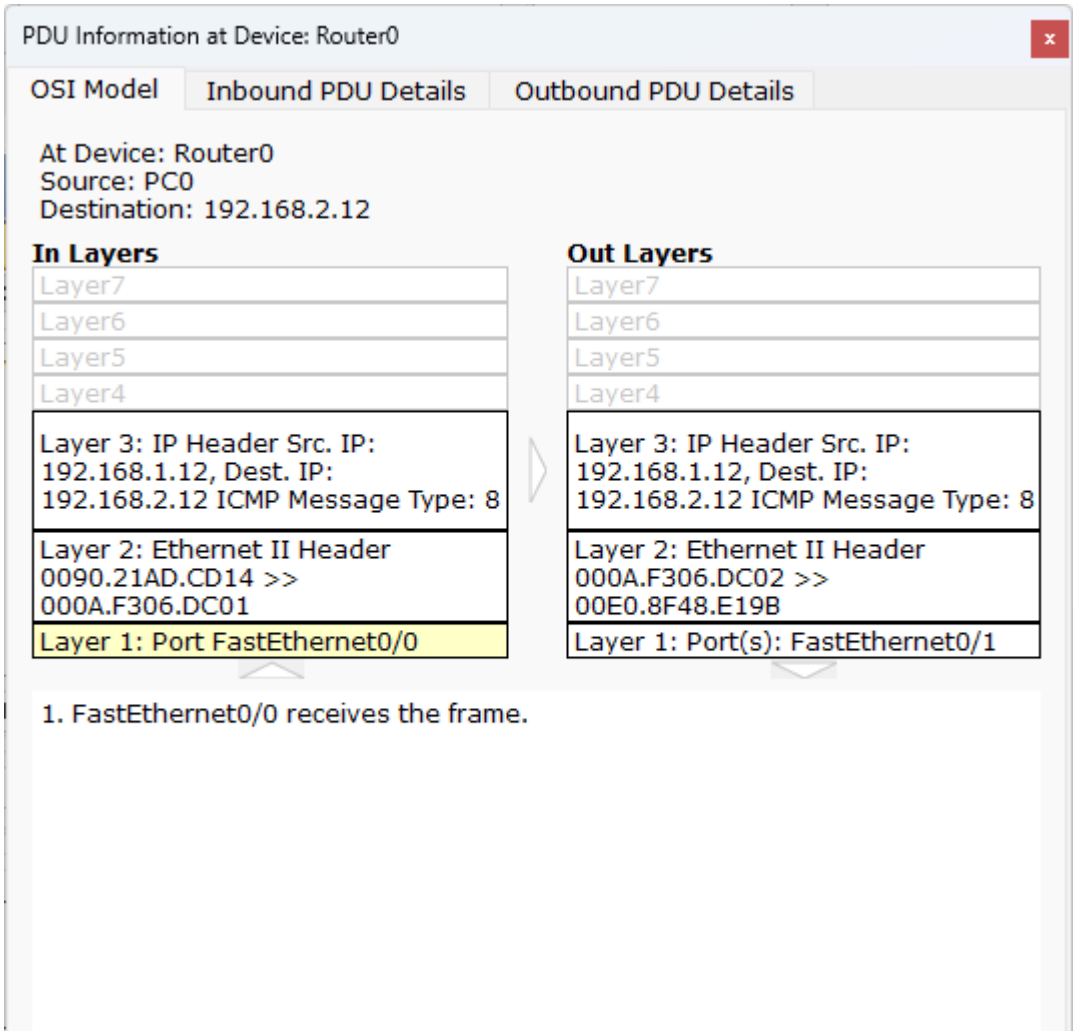
IP：

- 版本（Version）：4，表示IPv4。
- 头长度（IHL - Internet Header Length）：表示IP头部的长度。
- 差分服务代码点（DSCP）：0x0，表示数据包的服务质量。
- 总长度（TL - Total Length）：128字节。
- 标识（ID）：0x19，一个唯一标识符。
- 标志和片偏移(Flags and Fragment Offset):0x0,相关于数据包分段。
- 生存时间（TTL - Time To Live）：128，数据包在网络中的生存时间。
- 协议（PRO）：0x1，表示承载的是ICMP数据。
- 头部校验和（Checksum）：用于错误检测。
- 源IP地址（SRC IP）：192.168.1.12。
- 目的IP地址（DST IP）：192.168.2.12。
- 选项（Options, OPT）：0x0，通常用于调试和网络测试。

ICMP：

- 类型（Type）：0x8，表示这是一个回显请求（通常用于ping)。
- 代码（Code）：0x0，具体化了类型。
- 校验和（Checksum）：用于错误检测。
- 标识符（ID）：0x8，用于标识回显请求。
- 序列号（Sequence Number, SEQ NUMBER）：25，用于标记发送的回显请求序列。

3.3 PDU Information at Device: Router0（OSI Model）



这张图是 Cisco Packet Tracer 中，一个路由器设备（Router0）的 ICMP 数据包的 PDU（协议数据单元）信息。这些信息反映了数据包在网络中的移动，从它进入路由器（入站 PDU 细节），到它从路由器出去（出站 PDU 细节）。

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：

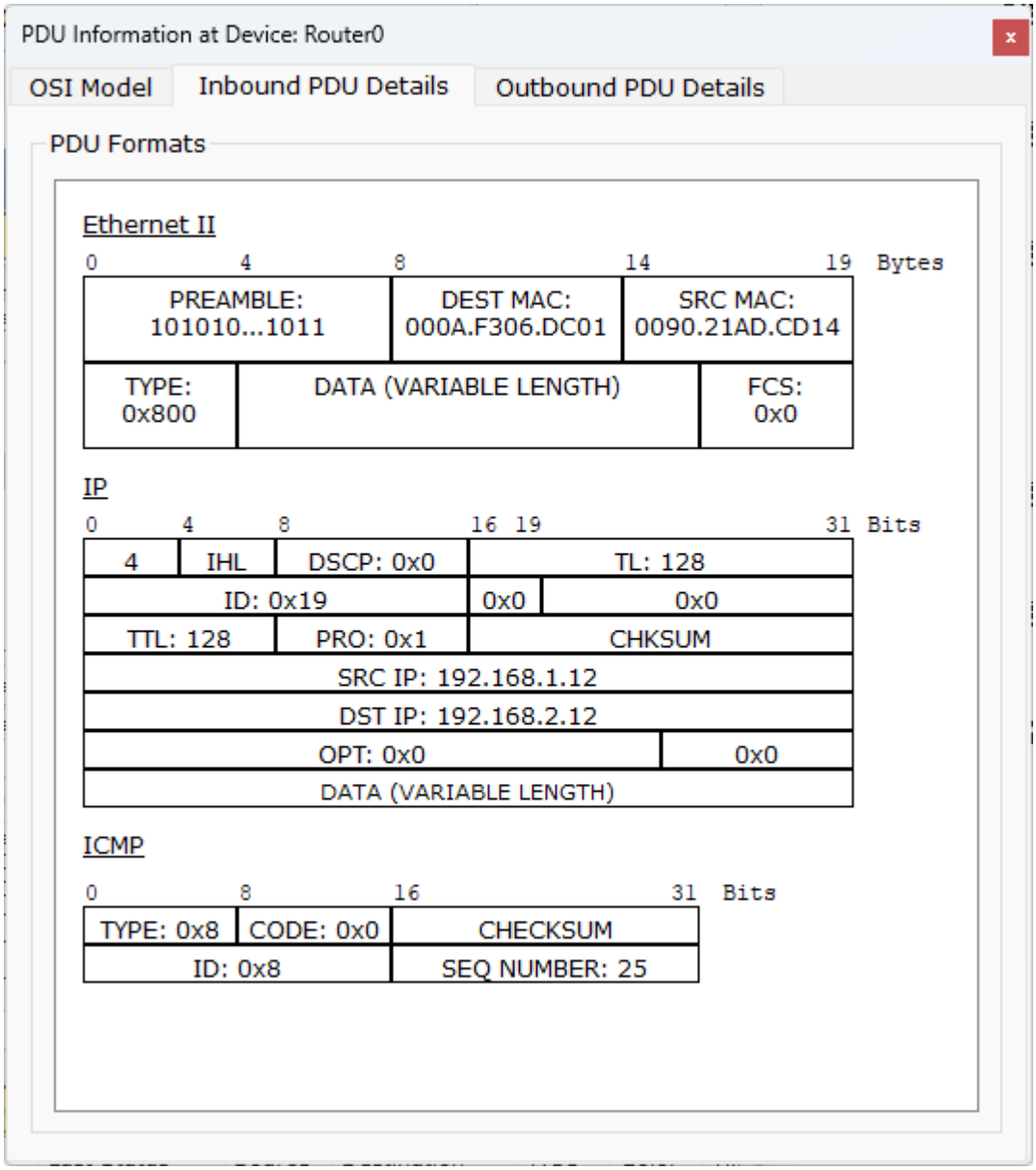
- Layer 3：IP 头信息显示源 IP 为 192.168.1.12，目的 IP 为 192.168.2.12，ICMP 消息类型为 8（回显请求）。
- Layer 2：以太网 II 头信息展示源 MAC 地址为 0090.21AD.CD14，目的 MAC 地址为 000A.F306.DC01。

- 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，ICMP 消息类型仍为 8。
- 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。

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



这张图显示了在Cisco Packet Tracer模拟环境中，路由器（Router0）上的 ICMP 数据包的入站 PDU（协议数据单元）细节。它提供了数据包的三个层次的信息：以太网 II 层，IP 层和 ICMP 层。

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，承载了 IP 和 ICMP 层的信息。
- 帧检验序列（FCS）：0x0，用于检测帧在传输过程中的错误。

IP：

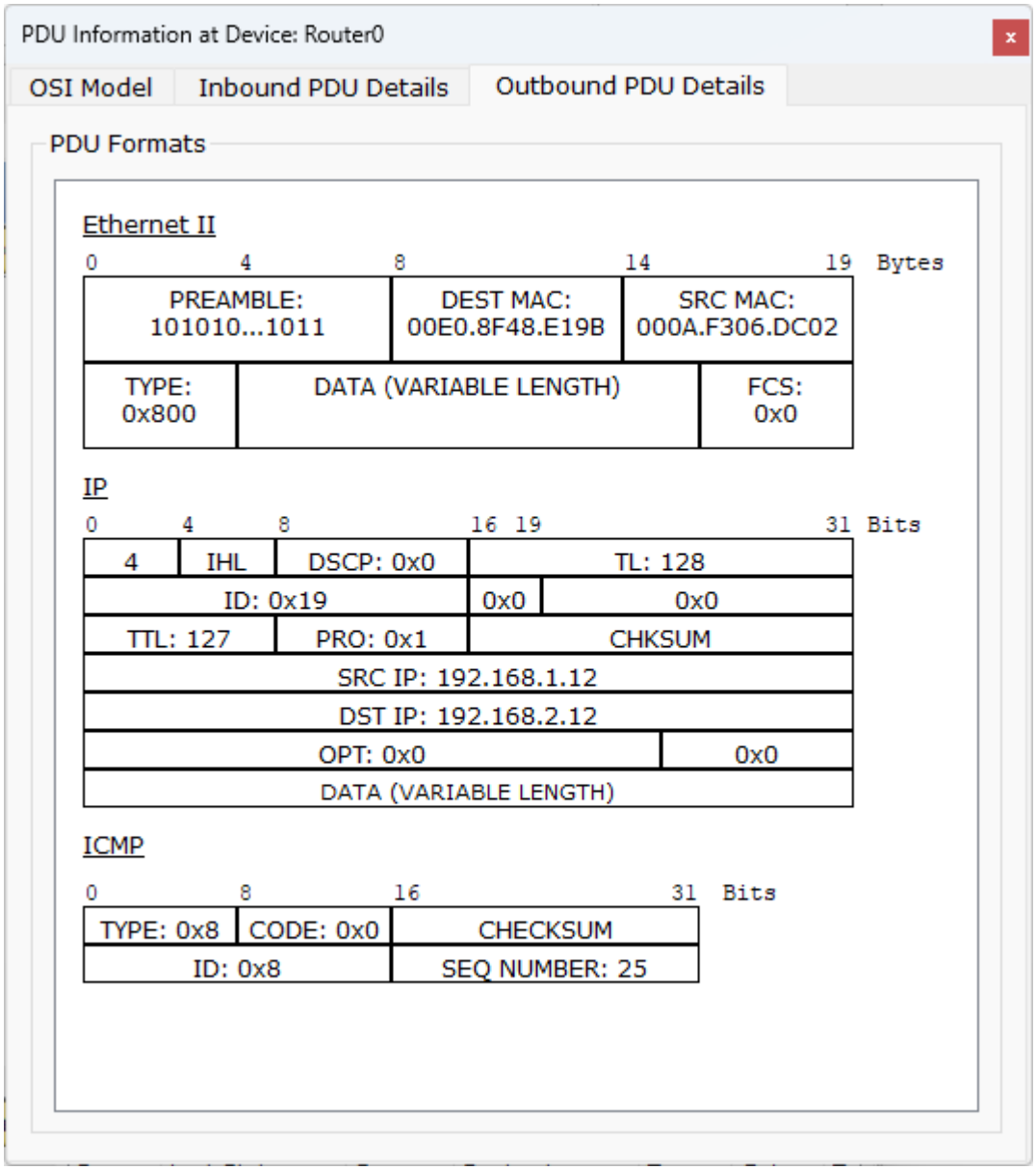
- 版本（Version）：4，指的是 IPv4。
- 头部长度（IHL - Internet Header Length）：通常表示 IP 头部的长度。
- 差分服务代码点（DSCP）：0x0，用于分类流量。
- 生存时间（TTL - Time To Live）：128，数据包可经过的最大路由器数目。
- 协议（Protocol）：0x1，表示这是 ICMP 协议。
- 总长度（Total Length, TL）：128 字节。
- 标识（Identification, ID）：0x19，用于唯一识别分组的序列号。
- 头部校验和（Checksum）：用于验证头部信息的正确性。
- 源 IP 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。

ICMP：

- 类型（Type）：0x8，代表这是一个 ICMP 回显请求（ping 请求）。
- 代码（Code）：0x0，与特定的 ICMP 类型相关的附加信息。
- 校验和（Checksum）：用于确保 ICMP 消息的完整性。
- 标识符（Identifier, ID）：0x8，可能用于匹配请求与回复。

- 序列号（Sequence Number）：25，用于标记发送的 ICMP 请求的顺序。

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



这张图展示了 Cisco Packet Tracer 中，路由器（Router0）上的一个 ICMP 数据包的出站 PDU（协议数据单元）的详细信息。我们可以看到数据包的以太网 II 层，IP 层和 ICMP 层的信息，以及它们是如何准备离开路由器的。

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，携带 IP 数据包和其包含的 ICMP 消息。
- 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，表示承载的是 ICMP 数据。
- 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，发送 ICMP 请求的设备的 IP。
- 目的 IP 地址（Destination IP, DST IP）：192.168.2.12，接收 ICMP 请求的目的设备的 IP。

ICMP：

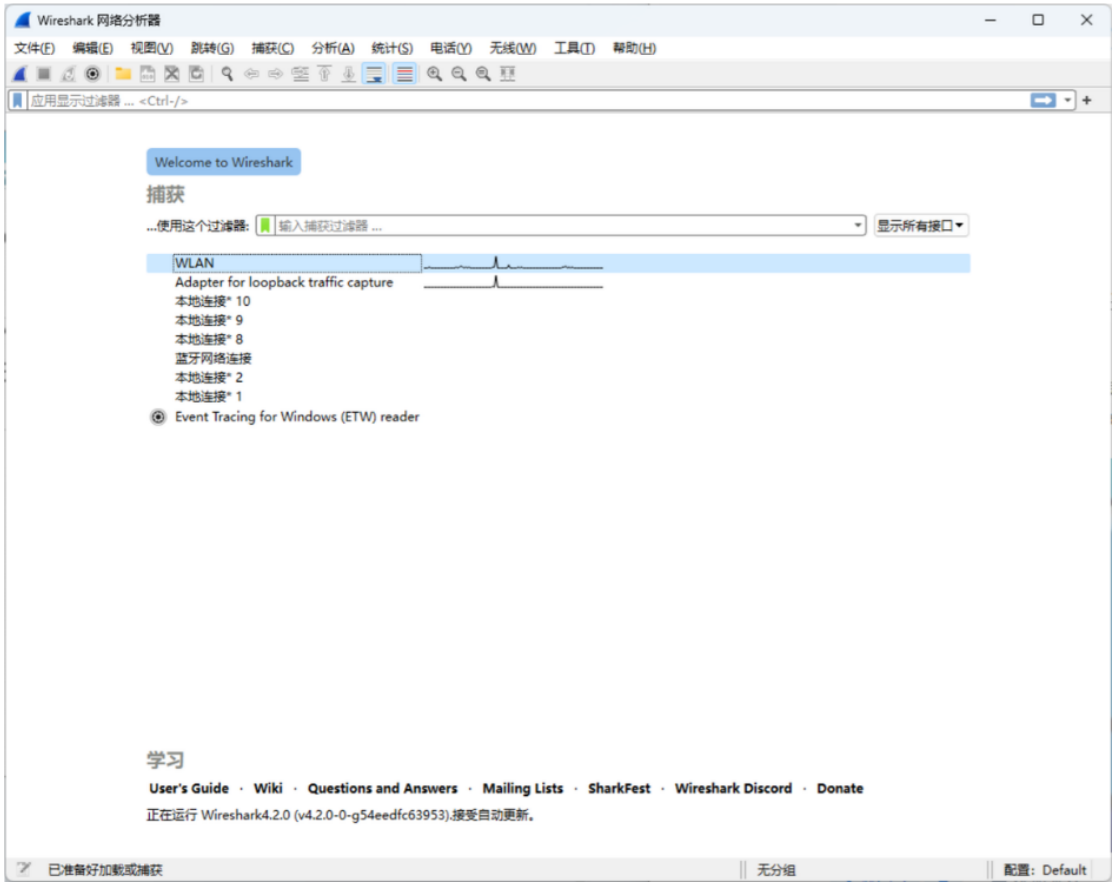
- 类型（Type）：0x8，代表 ICMP 回显请求，也就是 ping 请求。
- 代码（Code）：0x0，与 ICMP 类型相关的附加信息。
- 校验和（Checksum）：用于验证 ICMP 消息的完整性。
- 标识符（Identifier, ID）：0x8，可能用于将回显请求和回显应答匹配起来。
- 序列号（Sequence Number）：25，用于标记发送的 ICMP 请求的顺序。

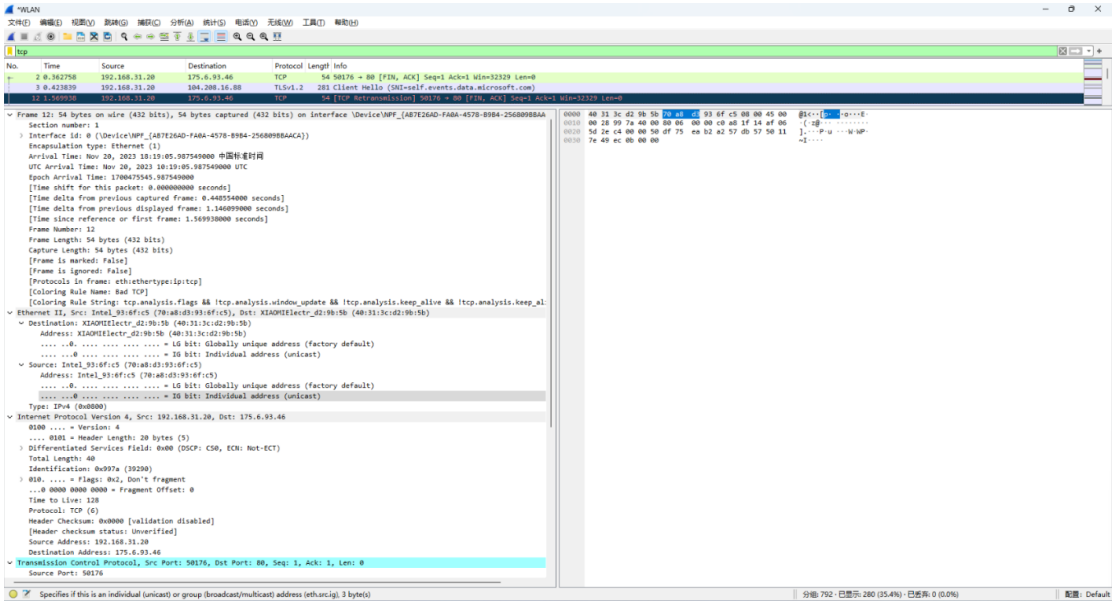
4. 本机命令提示符输入 ipconfig/all 命令，查看本机的 MAC 地址，为 D4-54-8B-33-2B-7E。

```
无线局域网适配器 WLAN:

   连接特定的 DNS 后缀 . . . . . : tongji.edu.cn
   描述. . . . . : Intel(R) Wi-Fi 6 AX201 160MHz
   物理地址. . . . . : D4-54-8B-33-2B-7E
   DHCP 已启用 . . . . . : 是
   自动配置已启用. . . . . : 是
   IPv6 地址 . . . . . : 2001:da8:8002:6bd1:3da8:a8dd:269f:38c7(首选)
   临时 IPv6 地址. . . . . : 2001:da8:8002:6bd1:2928:8444:6090:5cad(首选)
   本地链接 IPv6 地址. . . . . : fe80::b6ff:9493:f8d0:9a9e%6(首选)
   IPv4 地址 . . . . . : 100.81.138.91(首选)
   子网掩码 . . . . . : 255.254.0.0
   获得租约的时间 . . . . . : 2024年4月28日 18:43:28
   租约过期的时间 . . . . . : 2024年4月28日 20:43:27
   默认网关. . . . . : fe80::9e54:c2ff:fe0d:5002%6
                                100.81.255.254
   DHCP 服务器 . . . . . : 100.81.255.254
   DHCPv6 IAID . . . . . : 64246923
   DHCPv6 客户端 DUID . . . . . : 00-01-00-01-29-5C-8A-6A-88-A4-C2-22-79-31
   DNS 服务器 . . . . . : 202.120.190.208
                                202.120.190.108
   TCPIP 上的 NetBIOS . . . . . : 已启用
```

5. 用 WireShark 抓取 MAC 数据包，选用 WLAN 方式进行抓包，查看 MAC 数据包字段内容，并解读。





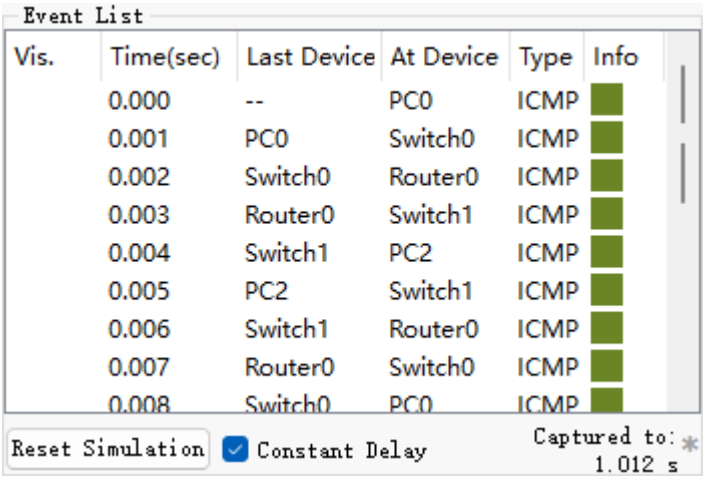
这张图来自 Wireshark，它捕获并详细展示了网络流量中的数据包信息。在这个特定的截图中，描述了一个 TCP 数据包，这个数据包包含了一个终止连接的请求（FIN 标志），并且确认了之前接收到的 TCP 段（ACK 标志）。下面是这些字段的解释以及包含的信息：

- 帧（Frame）：展示了该数据包在 Wireshark 捕获序列中的编号（第 12 个数据包），以及数据包的长度（54 字节）。它还告诉我们，数据包中包含了 Ethernet II、IP 和 TCP 这几个协议层。
- 以太网 II（Ethernet II）：
  - 目的 MAC 地址（Destination MAC Address）：一个唯一标识网络上接收设备物理地址的代码，这里是 XIAOMI 设备的地址（d2:9b:5b 结尾）。
  - 源 MAC 地址（Source MAC Address）：同样是一个唯一的代码，用于标识发送这个数据包的设备，这里是 IntelCor（93:6f:c5 结尾）。
  - 类型（Type）：表示这是一个 IPv4 协议的数据包（0x0800）。
- IPv4（Internet Protocol Version 4）：
  - 源 IP 地址（Source IP Address）：逻辑地址，标识发送数据包的设备，为 192.168.31.20。
  - 目的 IP 地址（Destination IP Address）：数据包的目的地逻辑地址，为 175.6.93.46。
  - 总长度（Total Length）：告诉我们整个 IP 数据包的长度。

- 生存时间（Time To Live，TTL）：设置为 128，这是数据包可以经过的最大路由器跳数，在到达目的地之前。

- TCP（Transmission Control Protocol）：
  - 源端口（Source Port）：本地端口号 50176，用于识别发送者的应用程序。
  - 目的端口（Destination Port）：端口号 80，通常用于 HTTP 服务。
  - 序列号（Sequence Number）：数据包的序列号为 1，用于确保数据按照发送顺序被接收。
  - 确认号（Acknowledgment Number）：确认号为 1，表示接收方已经正确接收到序列号为 1 的数据包，并期望下一个序列号。
  - 头部长度（Header Length）：TCP 头部长度为 20 字节，等于 5 个 32 位字。
  - 标志（Flags）：包含 FIN 和 ACK 标志，其中 FIN 表示发送方想要关闭连接，ACK 表示这是对先前收到数据包的确认。
  - 窗口大小（Window）：32329，表示接收方还可以接收多少字节的数据，这是 TCP 流量控制的一部分。
  - 校验和（Checksum）：0xec0b，这是一个检测数据包在传输过程中是否出错的数值。
  - 紧急指针（Urgent Pointer）：值为 0，表示没有紧急数据。

6. 分析在 Cisco Packet Tracer 中模拟 ICMP（ping 命令），ICMP 数据包转发过程中 MAC 地址变化情况。



- MAC 地址变化情况：

Time(sec)	Last Device	At Device	Type	DEST MAC	SRC MAC
0.000	--	PC0	ICMP	000A.F306.DC01	0090.21AD.CD14
0.001	PC0	Switch0	ICMP	000A.F306.DC01	0090.21AD.CD14
0.002	Switch0	Router0	ICMP	00E0.8F48.E19B	000A.F306.DC02
0.003	Router0	Switch1	ICMP	00E0.8F48.E19B	000A.F306.DC02
0.004	Switch1	PC2	ICMP	000A.F306.DC02	00E0.8F48.E19B
0.005	PC2	Switch1	ICMP	000A.F306.DC02	00E0.8F48.E19B
0.006	Switch1	Router0	ICMP	0090.21AD.CD14	000A.F306.DC01
0.007	Router0	Switch0	ICMP	0090.21AD.CD14	000A.F306.DC01
0.008	Switch0	PC0	ICMP	0090.21AD.CD14	000A.F306.DC01
…	…	…	…	…	…

- 起始 MAC 地址和目的 MAC 地址分析：

Time (sec)	Last Device	At Device	Type	DEST MAC	SRC MAC
0.000	--	PC0	ICMP	Switch0 接口 MAC 地址	PC0 MAC 地址
0.001	PC0	Switch0	ICMP	Switch0 接口 MAC 地址	PC0 MAC 地址
0.002	Switch0	Router0	ICMP	Router0 MAC 地址	Switch0 MAC 地址
0.003	Router0	Switch1	ICMP	Switch1 接口 MAC 地址	Router0 MAC 地址
0.004	Switch1	PC2	ICMP	PC2 MAC 地址	Switch1 接口 MAC 地址
0.005	PC2	Switch1	ICMP	PC2 MAC 地址	Switch1 接口 MAC 地址
0.006	Switch1	Router0	ICMP	PC0 MAC 地址	Switch0 接口 MAC 地址
0.007	Router0	Switch0	ICMP	PC0 MAC 地址	Switch0 接口 MAC 地址
0.008	Switch0	PC0	ICMP	Switch0 接口 MAC 地址	PC0 MAC 地址
…	…	…	…	…	…

【分析讨论】

一、MAC 地址的重要性

MAC 地址的不变性和唯一性保证了局域网内设备的可靠识别和数据链路层的准确通信。它是实现网络设备物理层寻址的关键，与 IP 地址相结合，实现了

从逻辑寻址到物理寻址的映射。

二、ICMP 数据包转发中 MAC 地址的变化

在实验中观察到，当 ICMP 数据包在内网中传输时，MAC 地址在通过路由器或交换机时会发生变化。这是因为：

- 在同一个子网内，交换机根据 MAC 地址表进行帧的转发。
- 而跨子网通信，路由器需要根据 IP 地址进行路由，然后将帧的目的 MAC 地址更改为下一跳的 MAC 地址或目的主机的 MAC 地址。

三、ARP 的作用

ARP 协议用于将网络层的 IP 地址解析成数据链路层的 MAC 地址。在本地子网内，如果主机需要知道另一个 IP 地址对应的 MAC 地址，它将广播一个 ARP 请求，询问哪台机器持有该 IP 地址。持有该 IP 地址的机器会以 ARP 响应的方式回复其 MAC 地址。

四、MAC 地址与 IP 地址的联系与区别

1. MAC 地址（Media Access Control Address）
   - 物理地址：MAC 地址通常被称为物理地址或硬件地址，因为它是固化在网络接口控制器硬件的。
   - 层次位置：它在 OSI 模型的数据链路层（第二层）使用。
   - 长度和格式：MAC 地址由 48 位组成，通常以六组两个十六进制数字表示（例如 00:1A:C2:7B:00:47）。
   - 分配方式：它由设备制造商分配，并通常不会改变。
   - 作用范围：在局域网内进行数据传输时使用，主要在同一个广播域内的设备之间传输帧。
   - 功能：它确保了帧能够在同一个网络段或局域网中正确地从一个物理设备传输到另一个物理设备。
2. IP 地址（Internet Protocol Address）
   - 逻辑地址：IP 地址是一个逻辑地址，与网络设备的位置有关。
   - 层次位置：它在 OSI 模型的网络层（第三层）使用。
   - 长度和格式：IPv4 地址由 32 位组成，分为 4 个 8 位的数字（例如 192.168.1.1），而 IPv6 地址由 128 位组成。

- 分配方式：IP 地址可以是静态分配的，也可以是通过动态主机配置协议（DHCP）动态分配的。
- 作用范围：它用于不同网络或广播域间的设备进行数据传输。
- 功能：IP 地址使设备能够在全球范围的互联网上找到彼此，并确保数据包能够从源头正确地路由到目的地。

3. MAC 地址与 IP 地址的联系
   - 相互转换：在局域网通信中，IP 地址需要转换为 MAC 地址以进行物理层传输，这通常通过 ARP 协议完成。
   - 配合使用：数据包从一个设备传输到另一个设备的过程中，同时使用 MAC 地址和 IP 地址，其中 IP 地址用于在网络间路由，MAC 地址用于在同一网络内的数据链路层传输。
   - 同一设备：在一台网络设备中，通常会同时配置有 MAC 地址和 IP 地址，两者共同工作确保数据包能够在网络中正确传输。