**中国矿业大学计算机科学与技术学院**

**2023-2024(2)《计算机网络实验》课程报告(本科)**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 专业班级: | | 计算机科学与技术2022-2班 | | | | 姓名: | 杨晓琦 | | | 学号: | | 08222213 | |
|  | | | 指派的网络号： | | | 172.16.82~172.16.84 | | | | |  | | |
| **序号** | **报告题目** | **基础理论掌握程度** | | **综合知**  **识应用**  **能力** | **实验**  **内容** | **报告**  **格式** | **完成**  **状况** | **工作量** | **学习、**  **工作**  **态度** | **抄袭**  **现象** | | **其它** | **综合**  **成绩** |
|  |  |  | |  |  |  |  |  |  |  | |  |  |
|  |  |  | |  |  |  |  |  |  |  | |  |  |
|  |  |  | |  |  |  |  |  |  |  | |  |  |
|  |  |  | |  |  |  |  |  |  |  | |  |  |
|  |  |  | |  |  |  |  |  |  |  | |  |  |
|  |  |  | |  |  |  |  |  |  |  | |  |  |
|  |  |  | |  |  |  |  |  |  |  | |  |  |
|  |  |  | |  |  |  |  |  |  |  | |  |  |
| 任课教师： | | 杨东平 | | |  |  |  | |  | | |  |  |
| 批阅时间： | |  | | | |  |  | |  | | | | |

**目录**

[2 网络仿真和抓包分析工具学习和使用 1](#_Toc167884802)

[2.1 实验1：Wireshark的学习与使用 1](#_Toc167884803)

[2.1.1 预备知识 1](#_Toc167884804)

[2.1.2 Wireshark的下载与安装 2](#_Toc167884805)

[2.1.3 认识Wireshark用户界面 2](#_Toc167884806)

[2.1.4 Wireshark实时捕捉数据包 3](#_Toc167884807)

[2.1.5 文件的输出与输入 5](#_Toc167884808)

[2.1.6 应用举例 6](#_Toc167884809)

[2.1.7 信息过滤和分析 7](#_Toc167884810)

[2.2 实验2：PacketTracer的学习与使用 10](#_Toc167884811)

[2.2.1 预备知识 10](#_Toc167884812)

[2.2.2 Packet Tracer软件的安装 10](#_Toc167884813)

[2.2.3 PT主界面窗口 10](#_Toc167884814)

[2.2.4 PT应用示例 18](#_Toc167884815)

[2.3 实验体会 26](#_Toc167884816)

# 2 网络仿真和抓包分析工具学习和使用

**实验内容：**

1) Wireshark的学习与使用

2) PacketTracer的学习与使用

**实验报告要求(必须认真阅读)：**

1. 不得使用实验指导书中的图片(截图)及图片(截图)的相关说明，否则所涉及实验内容视作无效， 并按0分计入成绩；
2. 实验中所使用的IP地址必须按照统一分配给个人的IP地址完成，否则所涉及实验内容视作无效，并按0分计入成绩；
3. 实验内容需要使用的网站、数据文件或其它软件必须作明确的说明，并配有相应的截图(或运行截图或文件目录截图)，否则所涉及实验内容视作抄袭，并按0分计入成绩；
4. 使用仿真软件的实验内容必须同时提交仿真软件所形成的工程文件，否则所涉及的实验内容视作未完成，并按0分计入成绩；
5. 编程的实验内容必须在报告中指出编程环境及其版本号，并同时提交编程环境所形成的工作空间文件或工程文件，以及源代码文件，否则所涉及的实验内容视作未完成，并按0分计入成绩；
6. 实验步骤及实验步骤所涉及的参数必须明确，否则酌情扣除一定的分数；
7. 必须在规定的时间内完成每一次的实验任务，并提交相关文件，否则该次实验内容按0分计入成绩。

## 2.1 实验1：Wireshark的学习与使用

### 2.1.1 预备知识

Wireshark (电鲨鱼）的前身叫Ethereal（幽灵)，是目前世界上最流行的开源网络分析工具。Ethereal似乎与 Ethernet有关，因为Ethereal抓取的原始包就是以太网（Ethernet)的帧。而帧是互联网中最底层的数据包，所有的上层协议数据都被包裹在这个数据帧内。这个强大的工具可以逐层剥离数据帧内各层协议数据，并为用户提供关于网络和上层协议的各种信息。Wireshark的作用就是拆分和分析数据帧中的各层协议数据，而它的这种能力就源于它对不断加入的各种协议规则的学习，而它的抓包能力，则是通过对操作系统提供的网络接口数据读取函数库pcap network library的调用实现的。

抓包是获取网络中的某一个网络节点的所有数据.并对这些数据按照网络协议进行解析。通过网卡或网口抓包，可以获取经过这个网卡或网口的所有报文，真实的记录下网络中发生的一切事情。当一些网络出现异常问题，从基本的信息无法进行问题定位时，就需要用到网络数据抓包。通过抓包，可以看到网络报文有否正常发送出去?发过来的网络报文是否有收到？报文格式是不是正确？从数据报文侧，查看网络节点的整个网络情况，定位问题原因，排查网络故障。

### 2.1.2 Wireshark的下载与安装

下载并安装Wireshark4.2.4.0版本。如图1-1所示。

图1-1Wireshark属性详细信息

### 2.1.3 认识Wireshark用户界面

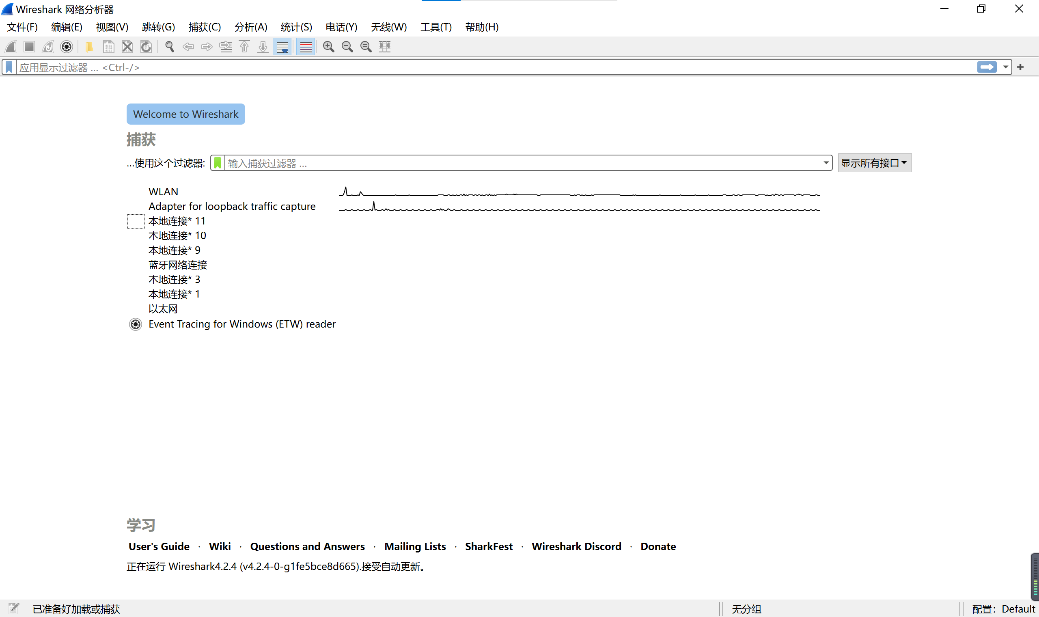
(1)进入启动页面。如图1-2所示。

图1-2 Wireshark启动界面

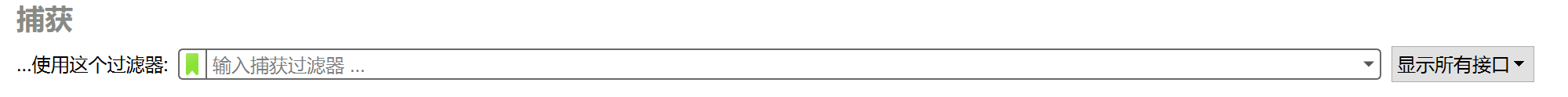
(2)设置捕获过滤器。如图1-3所示。

图1-3 过滤器窗口

(3)选择“WLAN”并进行抓包。如图1-4所示。

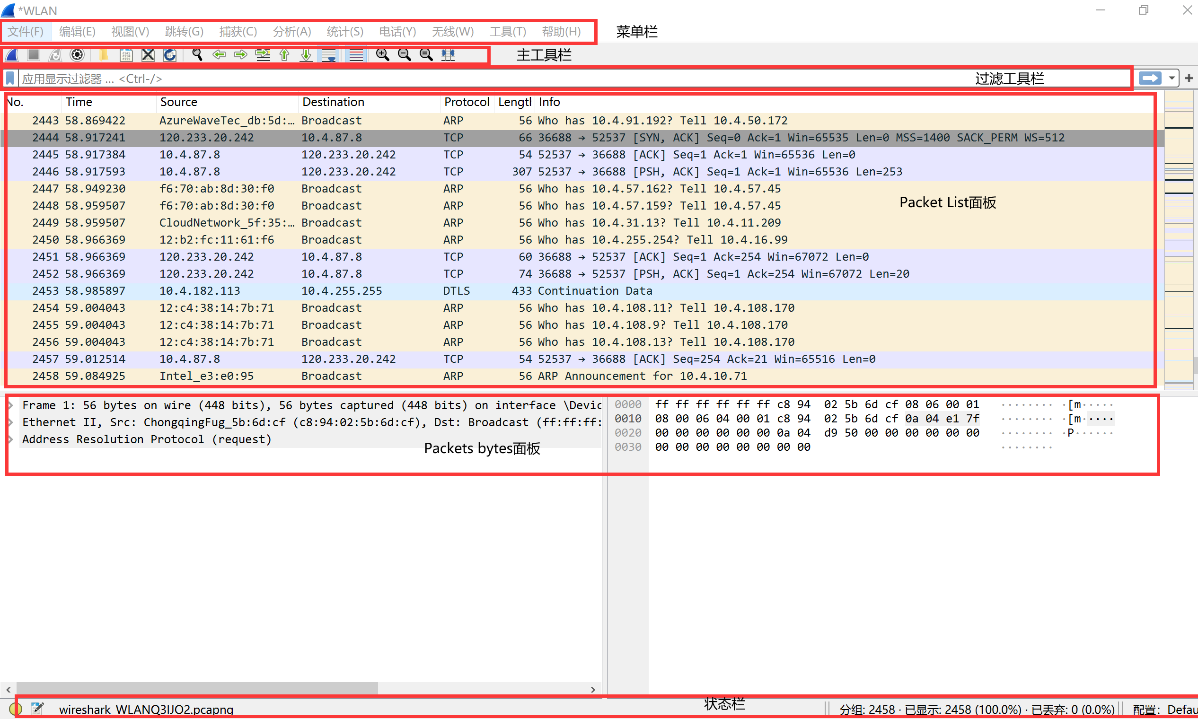
Wireshark主界面由七个部分组成：①菜单栏；②过滤工具栏；③过滤工具栏；④Packet List面板；⑤Packet detail面板；⑥Packets bytes面板；⑦状态栏。

图1-4 Wireshark主界面

### 2.1.4 Wireshark实时捕捉数据包

(1)启动捕捉数据包。

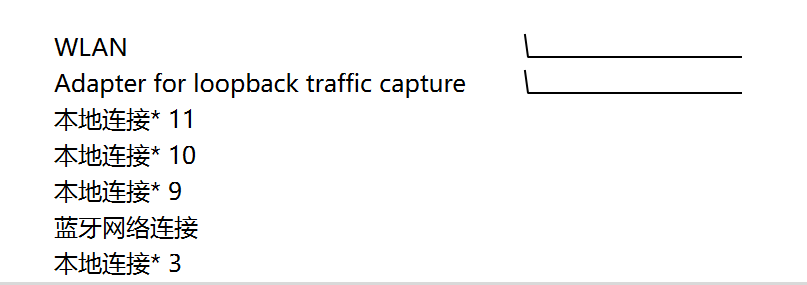
(2)进入捕捉接口对话框。如图1-5所示。

图1-5 捕捉接口对话框

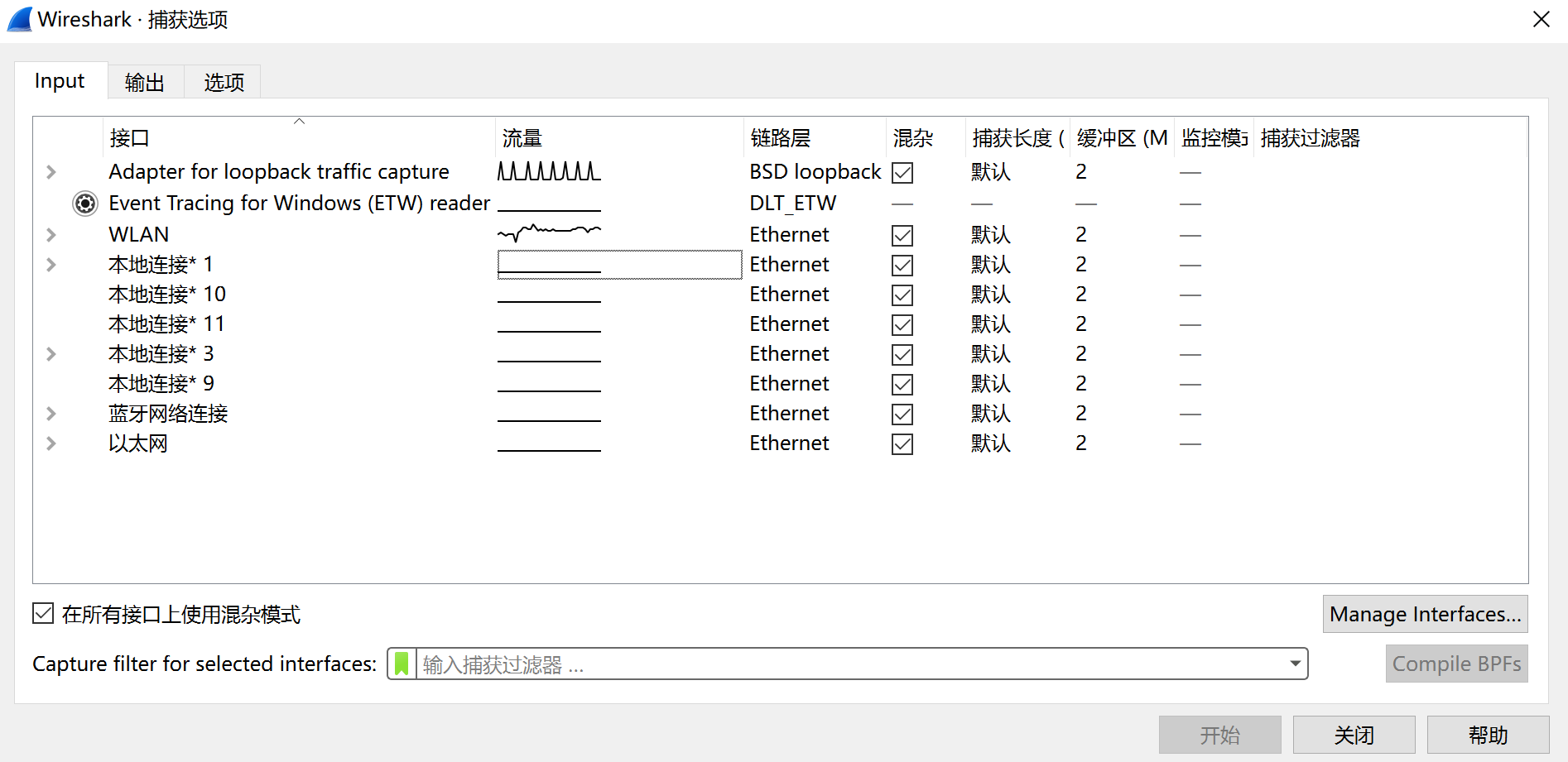
(3)进入捕捉选项对话框。如图1-6所示。

图1-6 捕捉选项对话框

(4)停止捕捉。

(5)重新启动捕捉。如图1-7所示。

图1-7 停止捕获与重新开始

### 2.1.5 文件的输出与输入

(1)抓包文件的保存。如图1-8所示。

图1-8 保存文件对话框

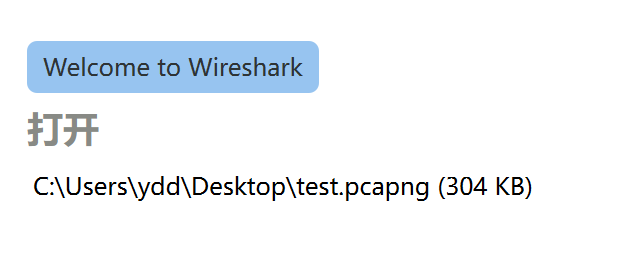
(2)Wireshark捕捉文件输入，读取之前保存的抓包文件test.pcapng。如图1-9所示。

图1-9 打开文件对话框

### 2.1.6 应用举例

(1)启动Wireshark。如图1-10所示。

图1-10 Wireshark起始界面

(2)选择抓包网络接口。

(3)开始抓包。

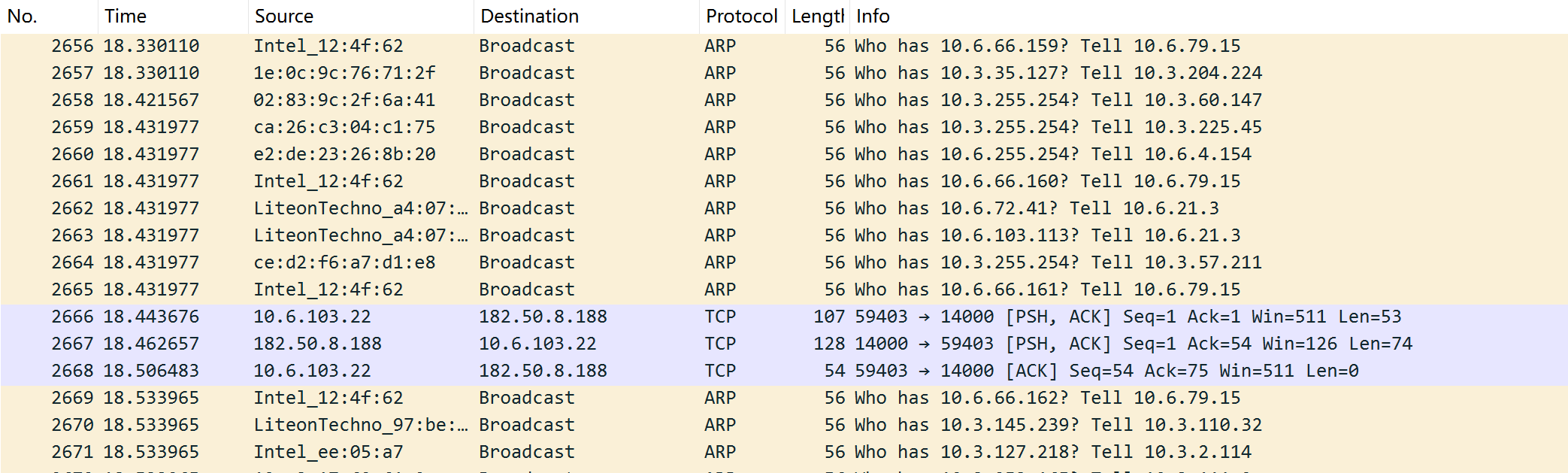
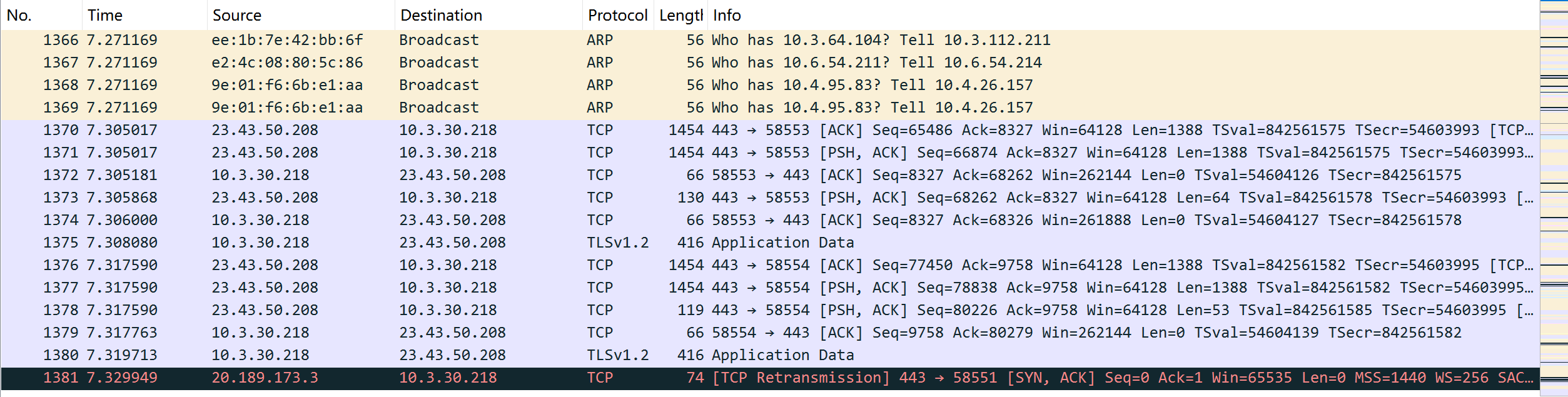
(4)打开PPLive网络电视，选择节目进行播放。如图1-11所示。

图1-11 Wireshark主界面抓包摘要信息窗口滚动列表

(5)暂停抓包。点击“停止按钮”。如图1-12所示。

图1-12 Wireshark主界面抓包摘要信息窗口停止滚动列表

(6)保存抓包文件。

### 2.1.7 信息过滤和分析

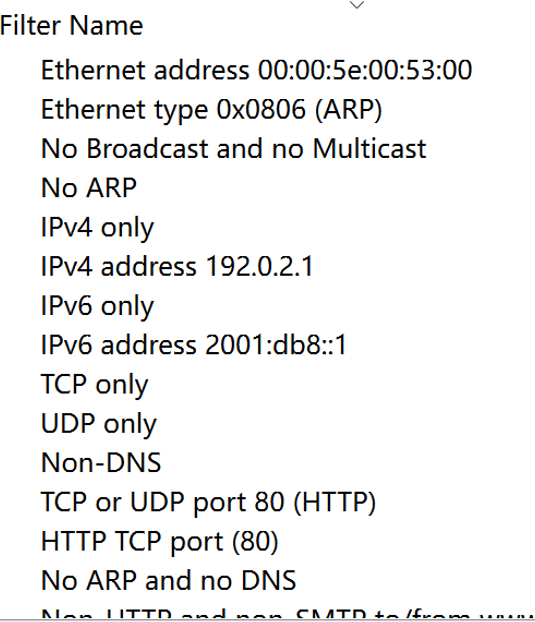
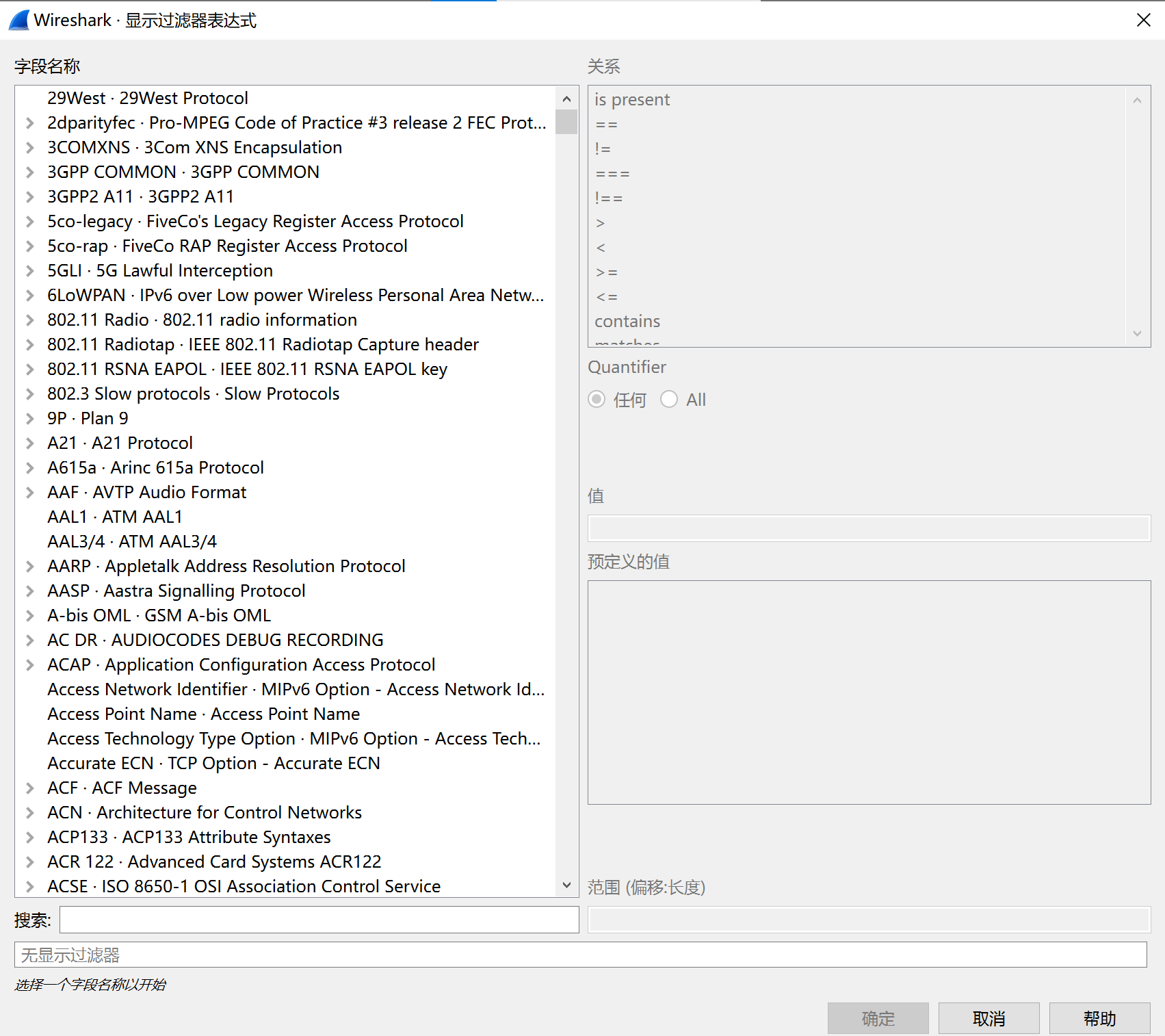
(1)设置“捕捉过滤器”。为过滤器起一个名字并保存，然后进行捕捉。如图1-13所示。

图1-13 捕捉过滤器名字

(2)设置“显示过滤器”。 如图1-14所示。

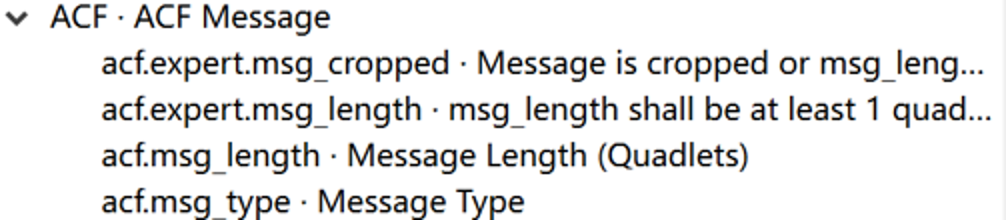
图1-14 显示过滤器过滤条件设置对话框

图1-15 域名(Field name)的子类选择

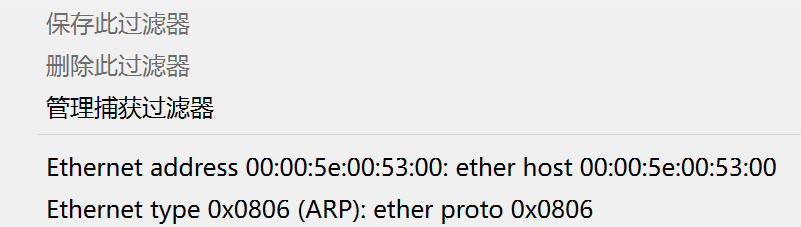
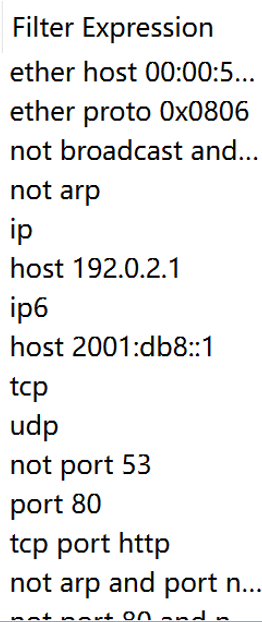
(3)捕获过滤器表达式。如图1-16和1-17所示。

图1-16 管理捕获过滤器按钮

图1-17 捕获表达式

(4)显示过滤器表达式及其书写规律

过滤表达式由过滤项、过滤关系和过滤值三项组成。

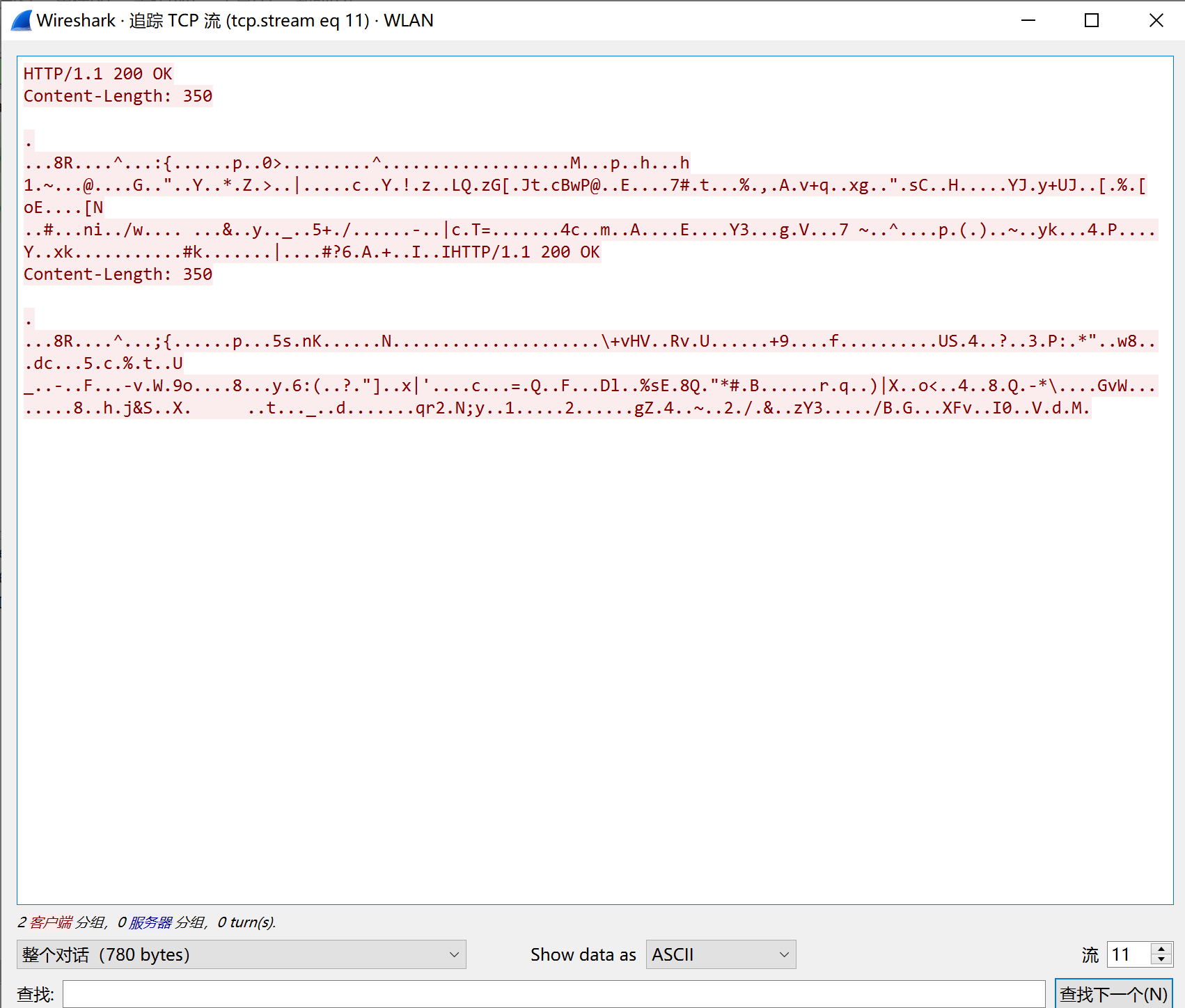
(5)跟踪TCP流。选择WLAN包，进行跟踪。如图1-18所示。

图1-18 跟踪TCP流对话框

## 2.2 实验2：PacketTracer的学习与使用

### 2.2.1 预备知识

Packet Tracer是由 Cisco公司开发的一个辅助学习工具，是一个功能强大的免费网络仿真程序。PT通过仿真技术对现实的物理设备进行仿真，PT支持 JavaScript和CSS，支持HTTP、FTP、SNMP等多种服务器。PT为学习思科网络课程的初学者设计、配置、排除网络故障提供了一个模拟的网络环境。用户可以在PT的图形用户界面上直接使用拖曳方法建立网络拓扑，并可提供数据包在网络中行进的详细处理和转发过程，观察模拟的网络实时运行情况。通过PT可以学会IOS的配置，锻炼网络故障排查能力。

PT的主工作区设计有逻辑和物理两种工作状态。工作在逻辑状态时，工作区内的设备只具逻辑节点意义；工作在物理状态时，工作区内的设备呈现物理组成与配置意义。

PT进行数据包跟踪时，为用户提供了实时和模拟两种工作模式，两种模式可相互切换。实时模式是一种连续时间模式，模拟实际的网络工作情形；模拟模式是让时间停下来，模拟人工操纵下的网络逐跳传输的工作情形。

### 2.2.2 Packet Tracer软件的安装

图2-1 Packet Tracer属性详细信息

### 2.2.3 PT主界面窗口

(1)主界面有九个分区，如图2-2所示。具体功能如下：

①菜单栏：此栏中有文件File、编辑Edit、选项Option、视图View、工具Tool、扩展Extension和帮助Help等项目。用户可以通过选择项目，给出下拉菜单列表，再进一步选择列表项，完成一些基本命令如打开、保存、打印和选项设置等操作，还可以访问帮助向导。

②主工具栏：主工具栏，此栏提供了菜单栏中主要菜单命令的快捷按钮图标。在本栏的最右侧还设置了一个信息按钮,可以点击该信息按钮，为当前网络添加说明信息。

③逻辑/物理转换按钮：电子此按钮可完成逻辑工作状态和物理工作状态之间转换。

④工作区：这是用户使用PT的主要操作区，在此区域中用户可以创建网络拓扑，监视模拟过程,查看各种信息和统计数据。

⑤常用工具栏：此栏提供了常用的工作区工具，包括选择、整体移动、备注、删除、查看、添加简单数据包和添加复杂数据包等。

⑥实时/模拟转换按钮：点击此按钮可完成实时工作模式和模拟工作模式之间转换。

⑦网络设备库：该分区为网络设备选择区，包含设备类型选择和特定设备选择两个相邻分区。

⑧设备类型库：此库包含不同类型的设备如路由器、交换机、HUB、无线设备、连线、终端设备和网云等。

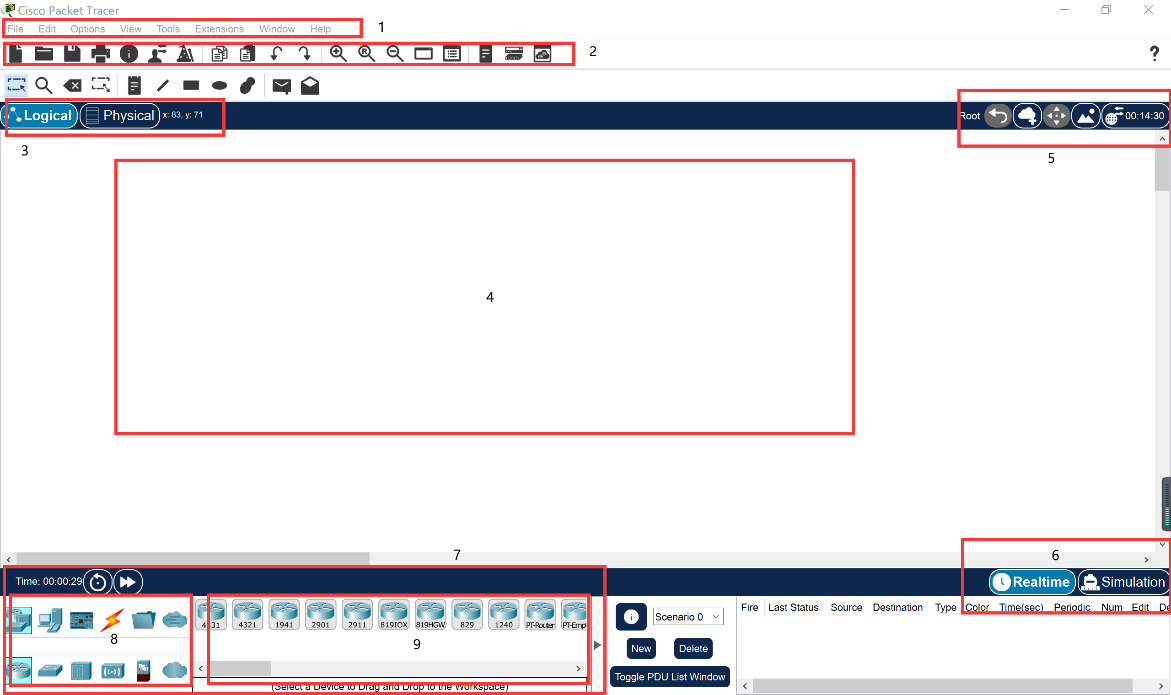
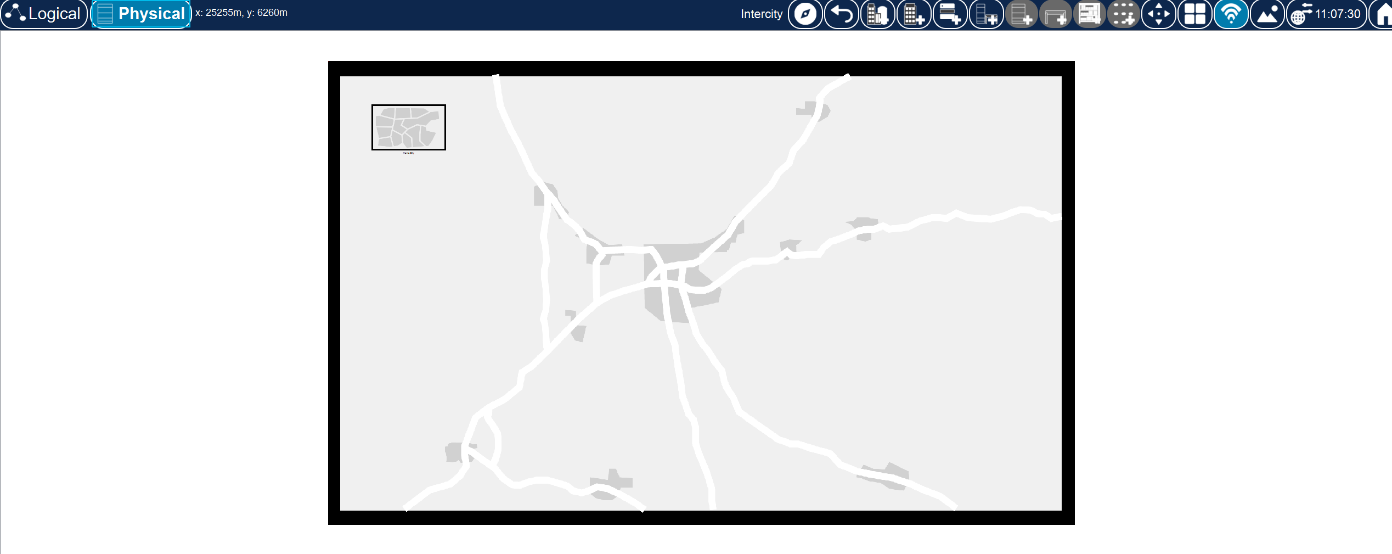
⑨特定设备库：此库包含选定设备类型中不同型号的设备，它随着设备类型库的选择级联显示。

图2-2 Packet Tracer 主界面及功能分区

(2)工作状态转换。PT设有实时(Real-time)与模拟(simulation)两种工作方式，实时模式也是默认模式，模拟模式相当于人工调试模式。如下各图所示。

图2-3 逻辑工作状态

图2-4 物理工作状态

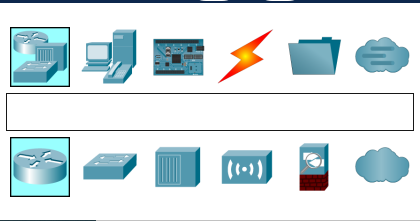
(3)图例导航使用。图例导航区也称设备导航区。

图2-5 设备导航区

PT的连接线按下图从左到右依次为：自动选线、控制线、直通线、交叉线、光纤、电话线、同轴电缆、DCE、DTE。

图2-6 PT中的连接线

(4)工作区的使用

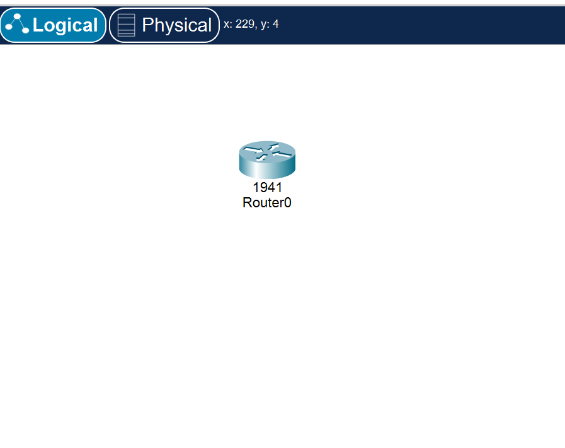
①拖动路由器图标到工作区。如图2-7所示。

图2-7 在工作区拖拽放置一个设备

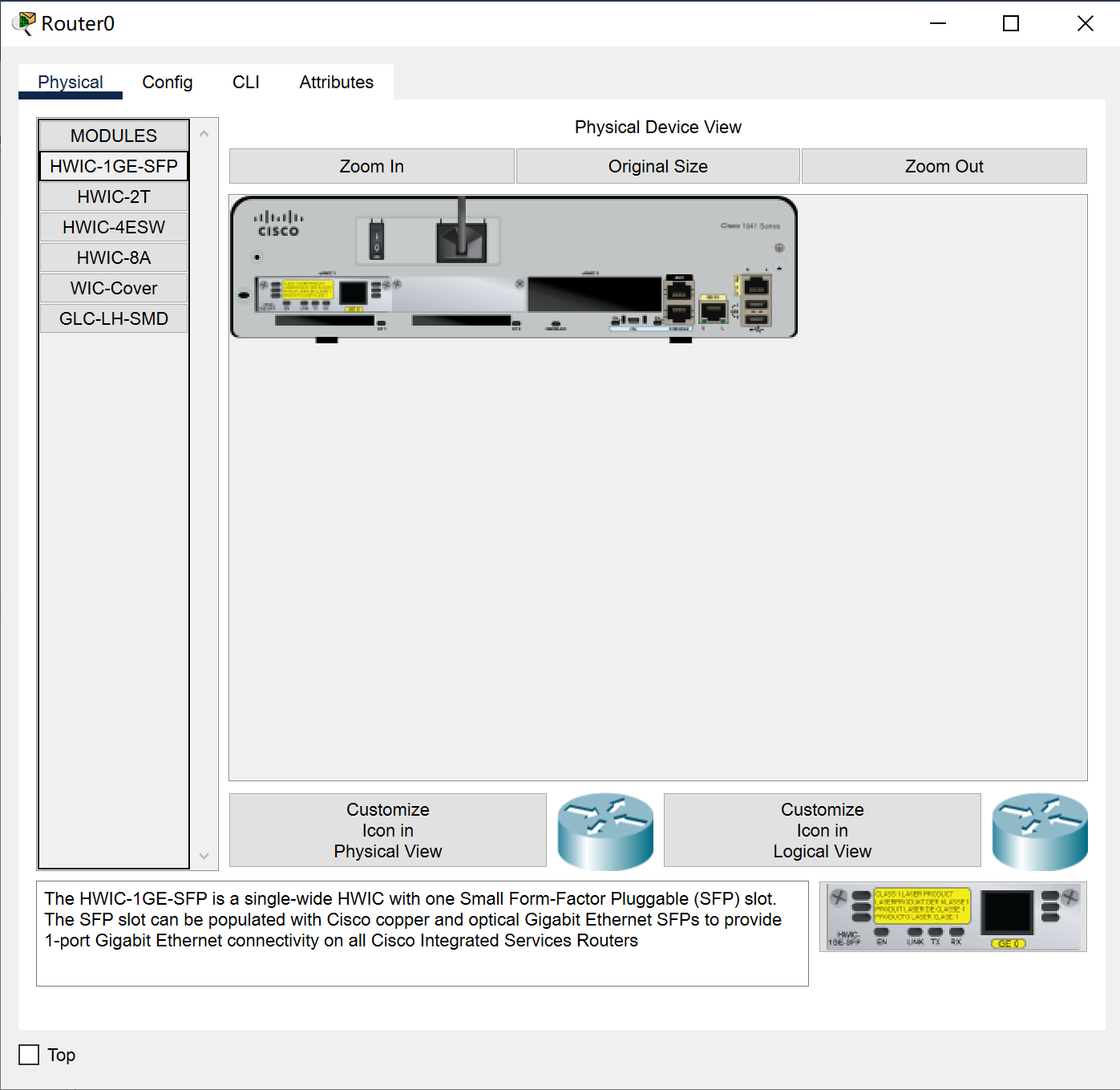
②进入路由器的设备界面，关闭电源，选择HWIC-4ESW模块至空槽中。如图2-8所示。

图2-8 设备的物理模块配置界面

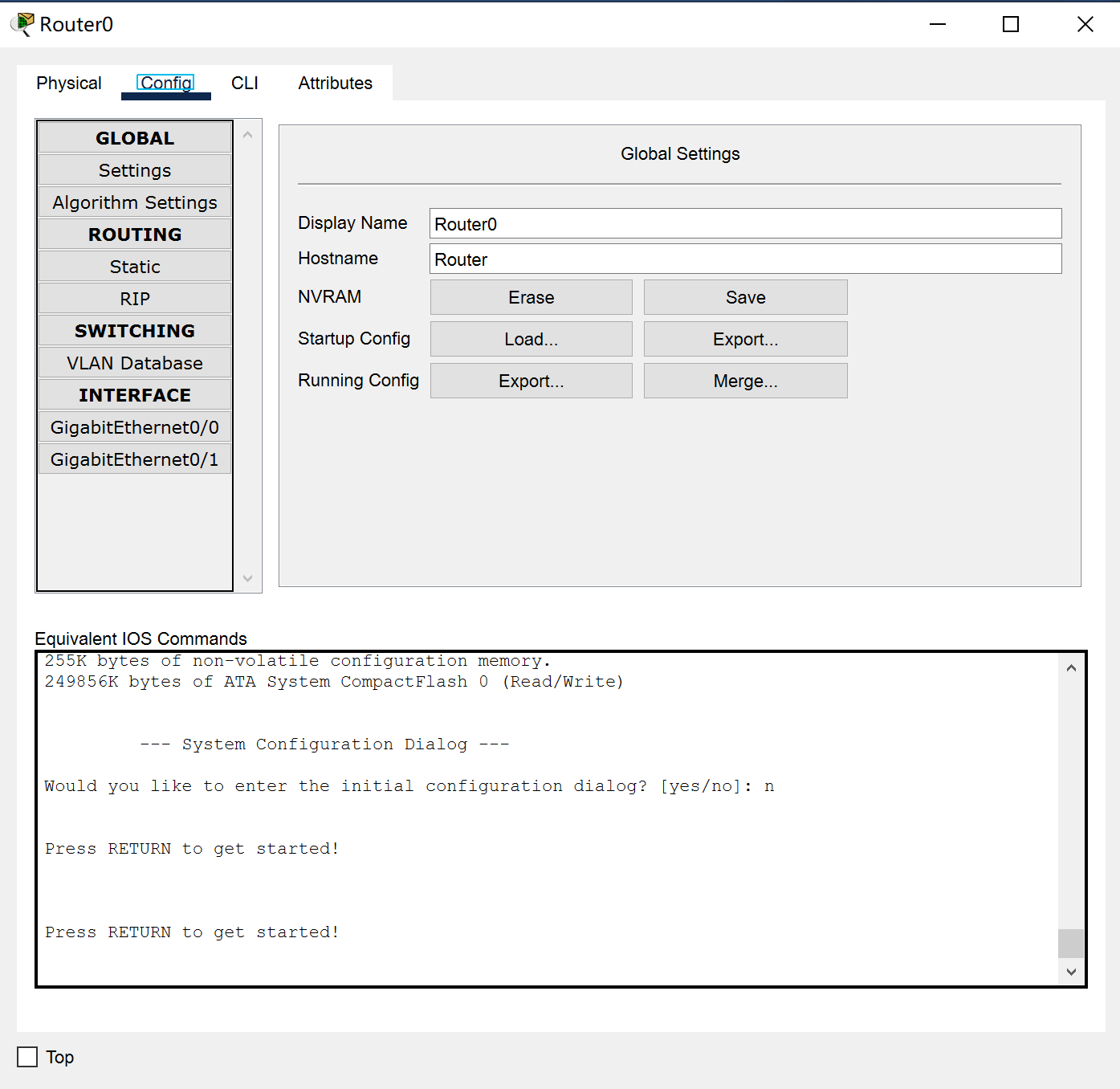
③在config标签下可以进行图形界面交互。如图2-9所示。

图2-9 设备工作参数的人机交互配置界面

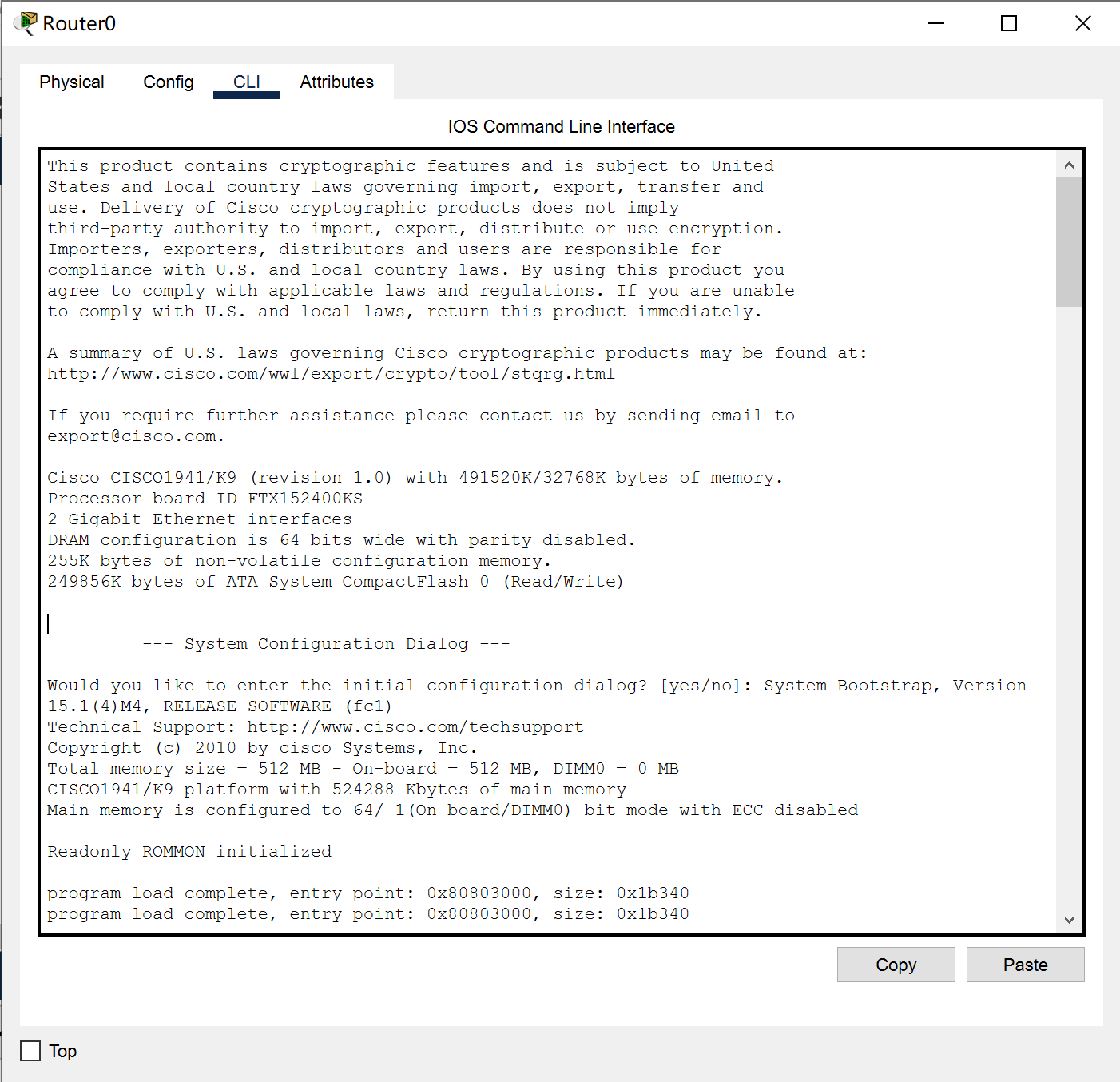
④在CLI标签下可以进行命令行配置。如图2-10所示。

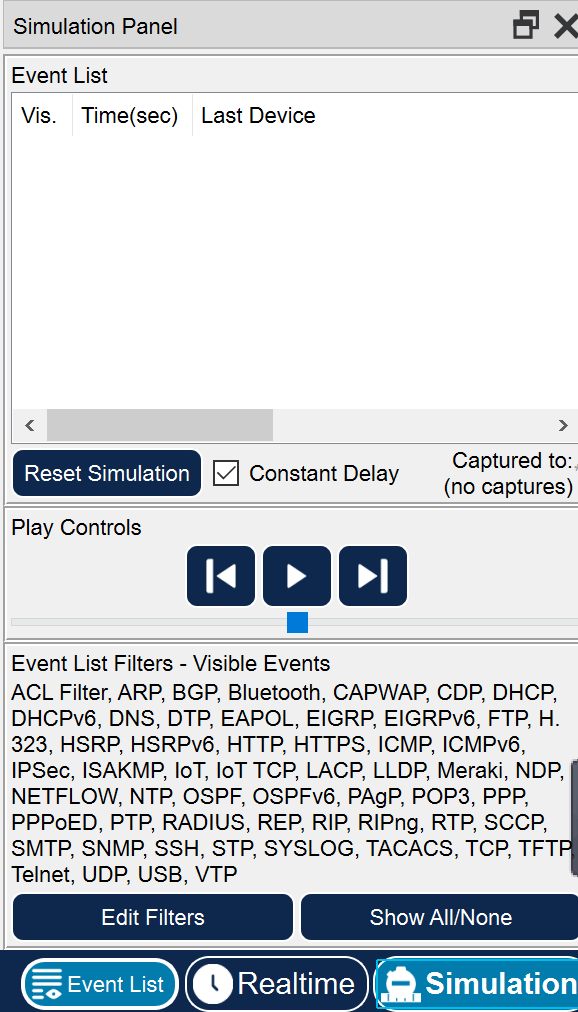
图2-10 设备工作参数的命令行配置界面

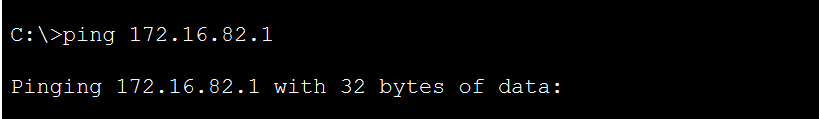
(5)模拟工作模式Simulation的使用。如图2-11所示。

①PT界面右下角为RealTime mode(实时模式)和Simulation mode(模拟模式)的切换按钮。

图2-11 PT工作模式切换工作按钮

②将工作模式切换到Simulation模式。

图2-12 PT工作模式切换到模拟方式

③打开pc的cmd命令窗口，按照给定的IP地址范围，输入ping 172.16.82.1，再点击自动捕获按钮。如图2-13、2-14所示。

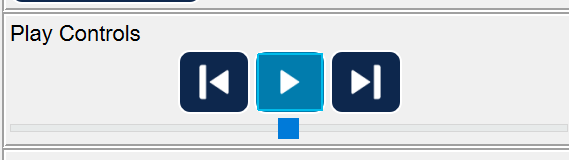
图2-13 在模拟方式下透过PC1发送数据包

图2-14 自动捕获按钮

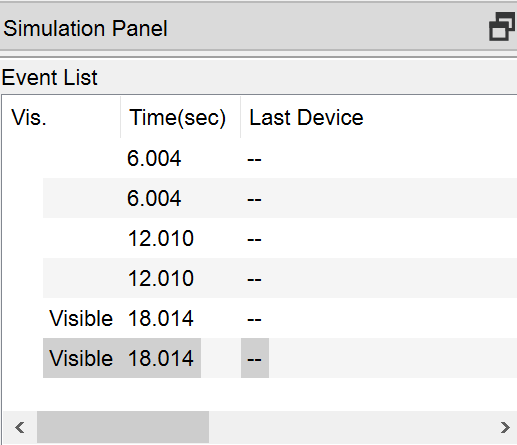
④数据包传输动画。第一列Vis.表示在图中运动的数据包；第二列Time表示所用时间；第三列Last Device表示数据包路过的上一个设备。如图2-15所示。

图2-15 模拟方式下数据包行进动画及列表显示

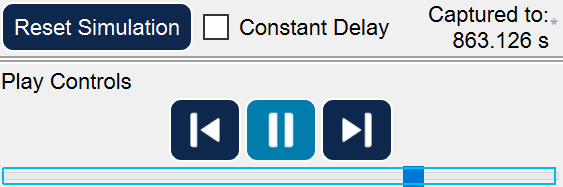
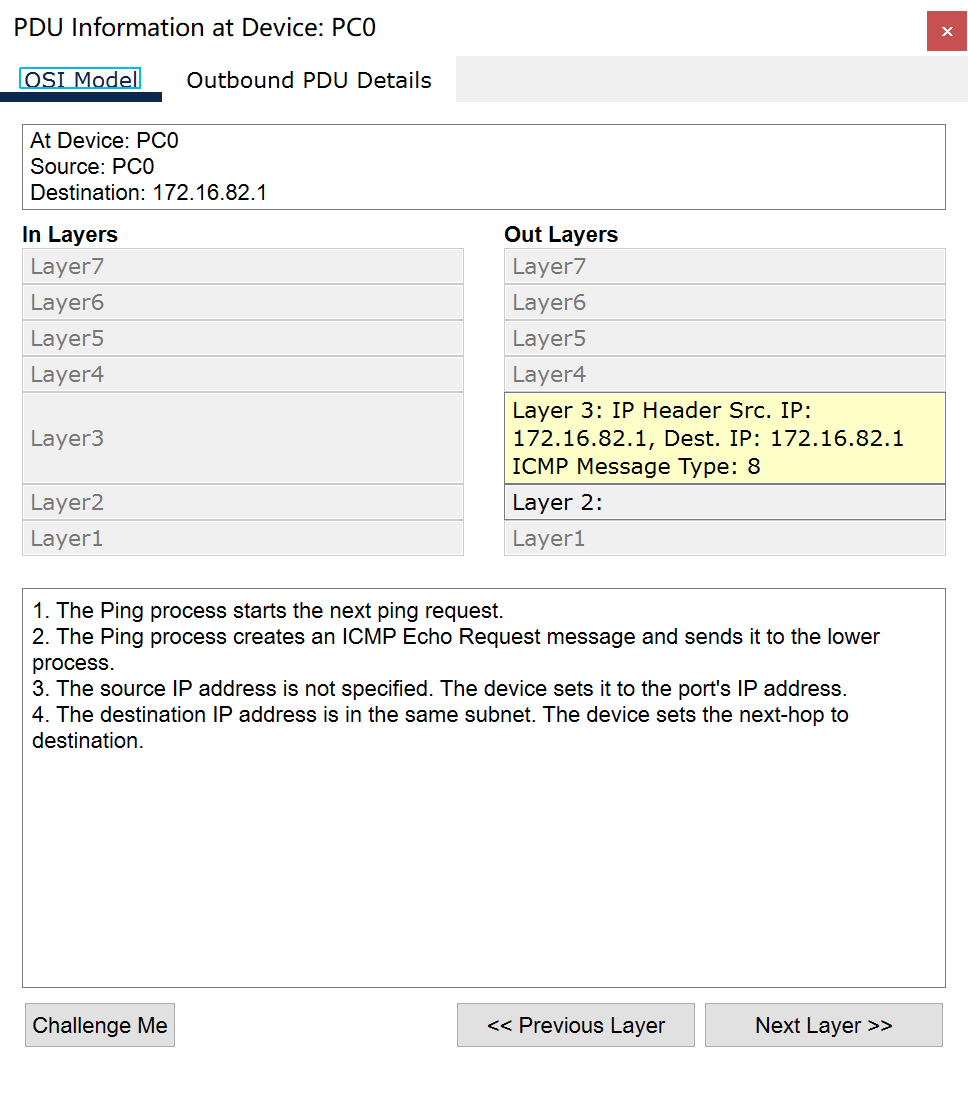
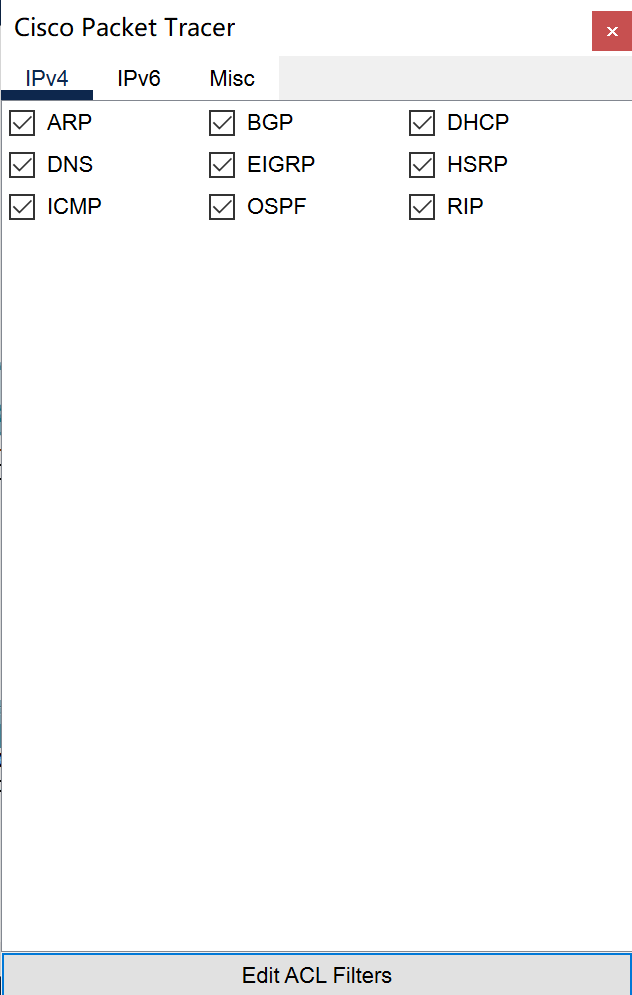
⑤数据包传输快慢调整。拖动下图蓝色滑块可以调节数据包传输的快慢。如图2-16所示。

图2-16 模拟方式下数据包进行动画速度调整

⑥查看数据包结构。点击动画中的数据包，从对话框中可以看到数据包的详细格式，包括源地址，目的地址等详细内容。如图2-17所示。

图2-17 模拟方式下查看数据包详细信息

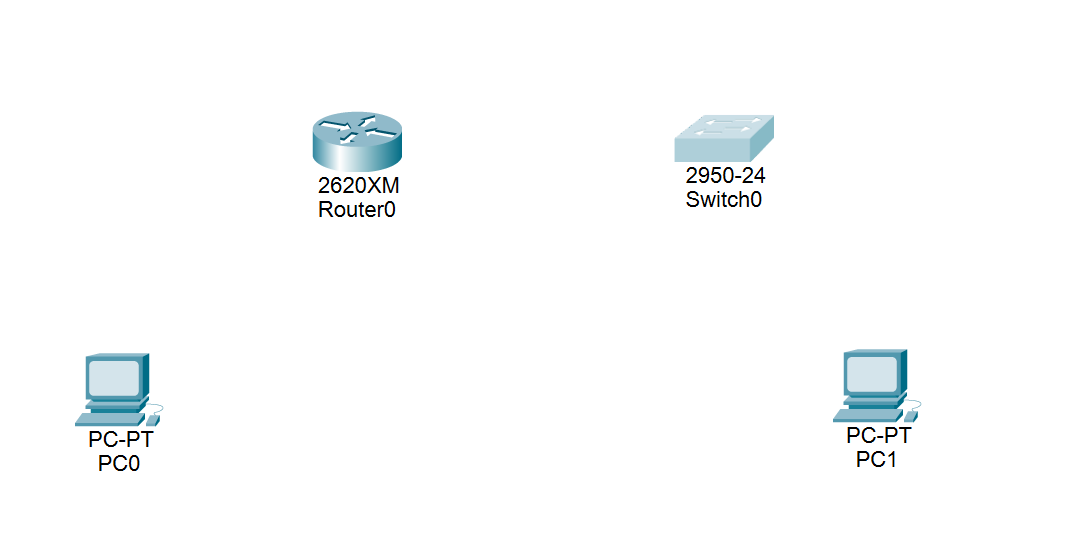
⑦过滤数据包。选择只想在动画中看到的数据包，勾上即可。如图2-18所示。

图2-18 模拟方式下过滤数据包列表

### 2.2.4 PT应用示例

(1)设备选择及连接

①选择设备。在工作区中添加一个2620XM路由器，一个2620-64交换机和两台PC机。如图2-19所示。

图2-19 设备添加

②添加物理模块。由于默认的2600XM有三个端口，连接PC0已经被占去ETHERNET0/0,Console口和AUX口，因此要添加物理模块。先关闭电源，再为Router0添加NM-4E模块，最后打开电源。

(3)配置设备参数。

①配置Router0,打开设备配置对话框。

②配置FastEthernt0/0端口。

IP地址：172.16.82.1

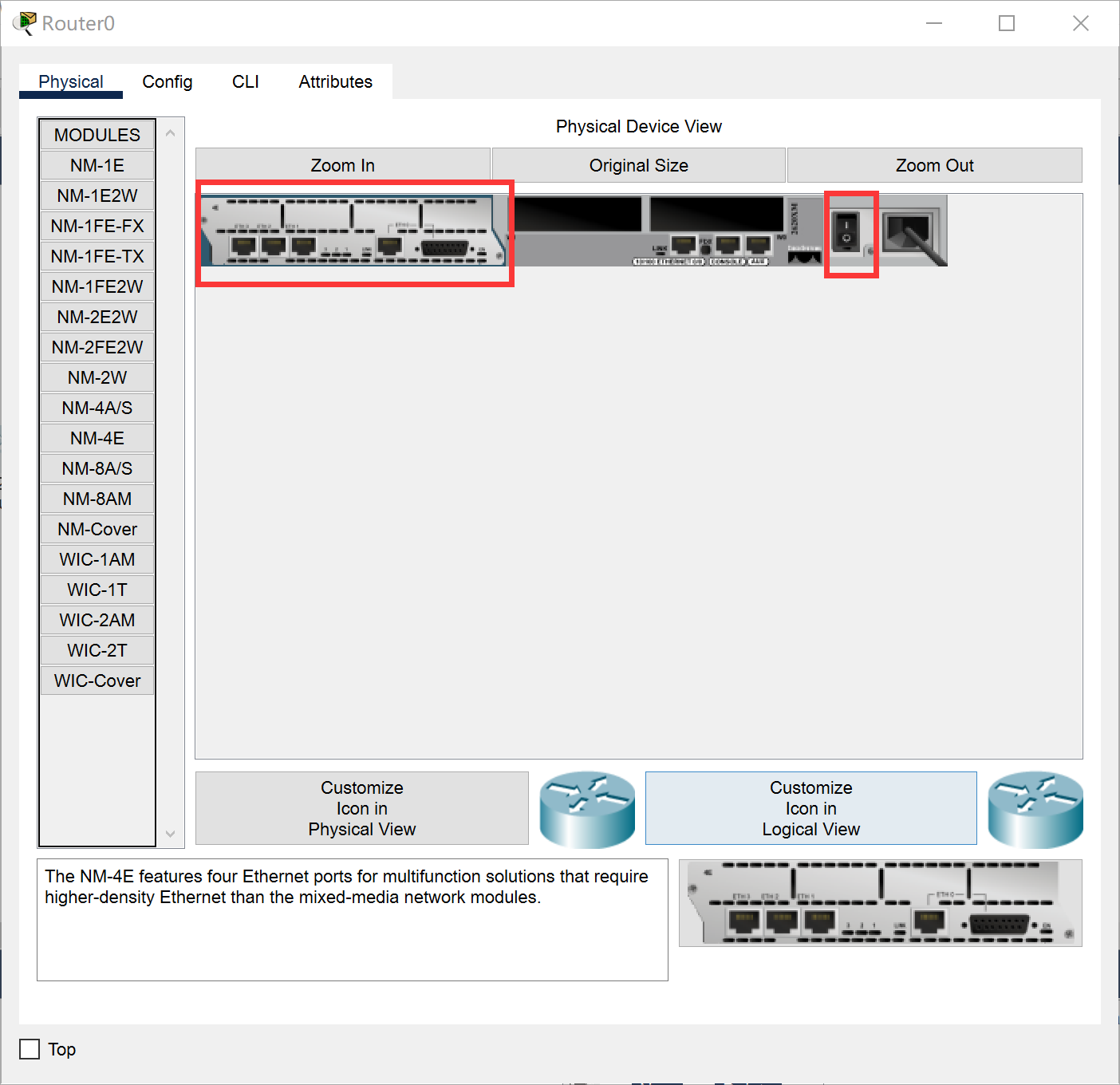
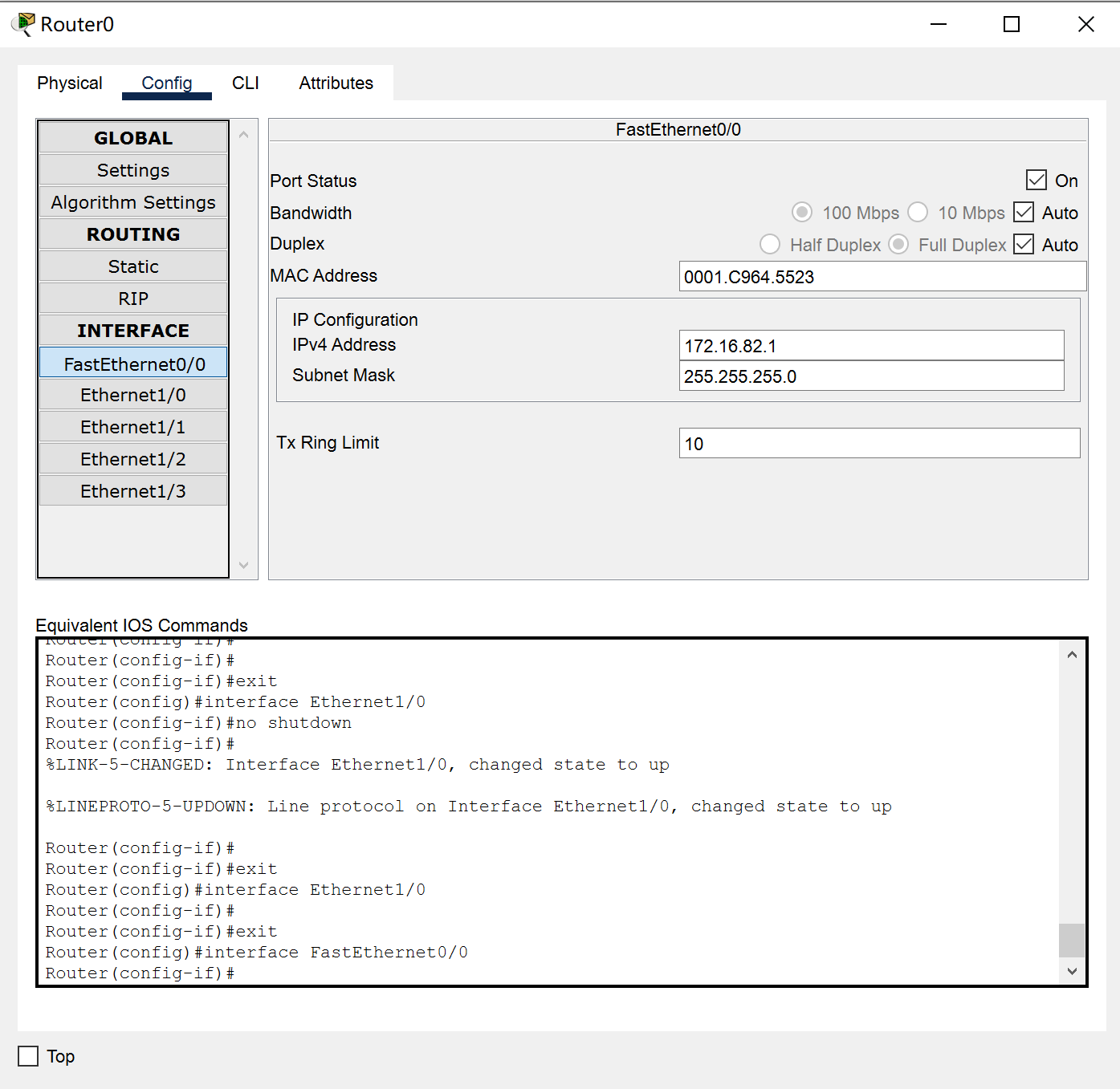
子网掩码：255.255.255.0

图2-20 Router0安装模块界面

图2-21 Router0的FastEthernet0/0配置

③终端设备的配置。

配置PC0：

默认网关：172.16.82.1

IP地址：172.16.82.2

子网掩码：255.255.255.0

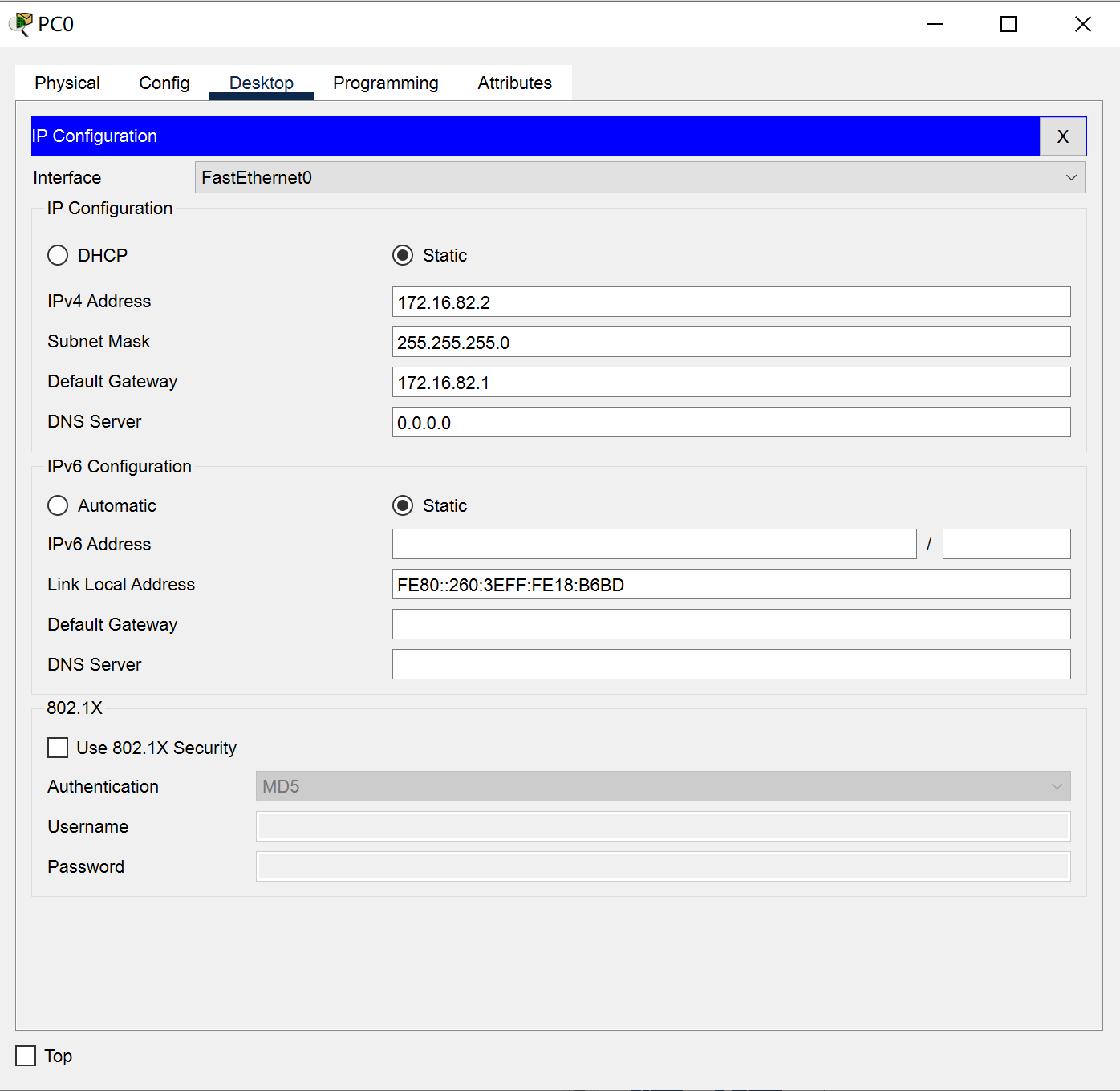


图2-22 PC0配置

配置Router0上的Ethernet1/0端口：

IP地址：172.16.83.1

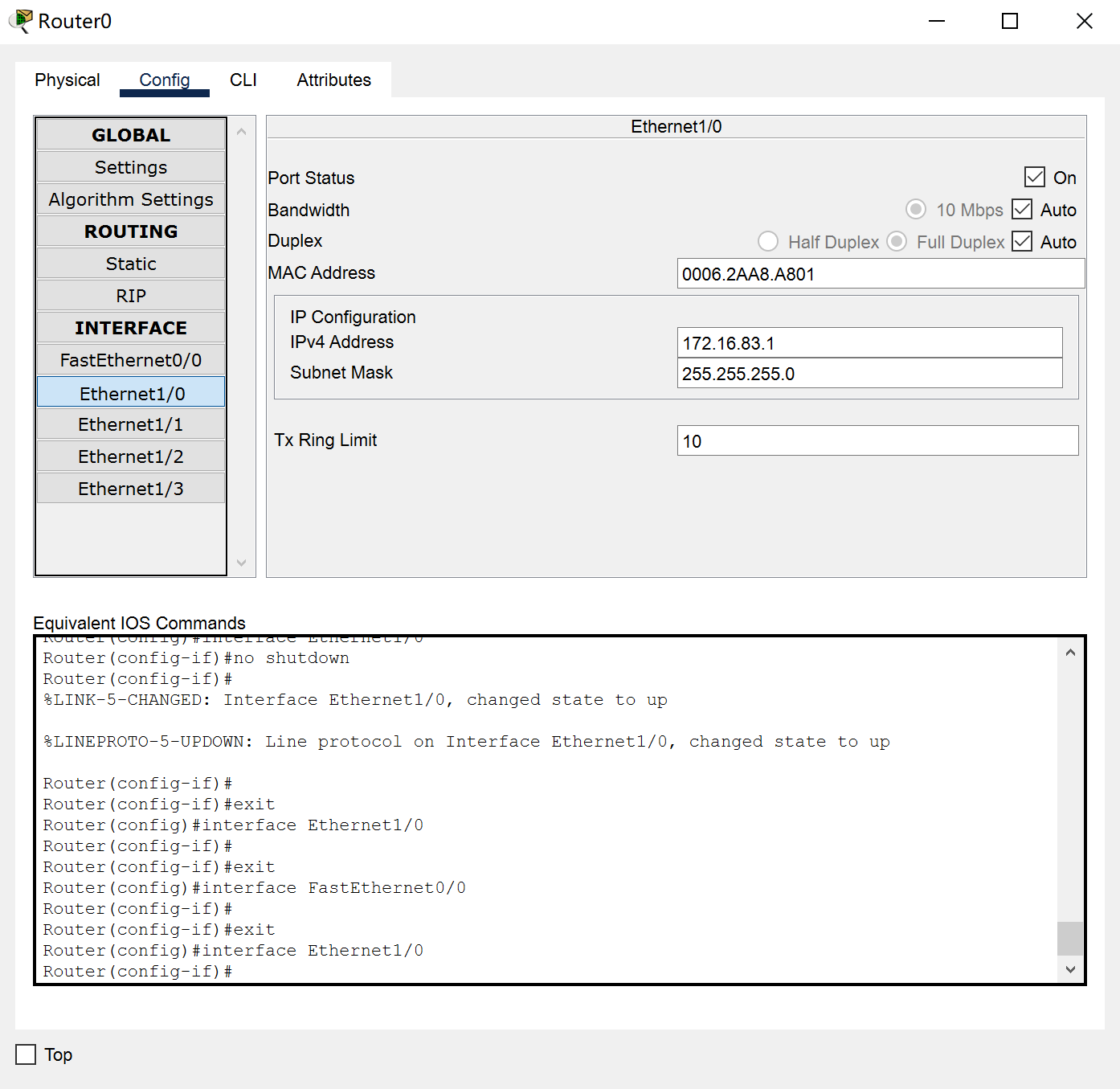
子网掩码：255.255.255.0

图2-23 Router0的Ethernet1/0配置

配置PC1：

默认网关：172.16.83.1

IP地址：172.16.83.2

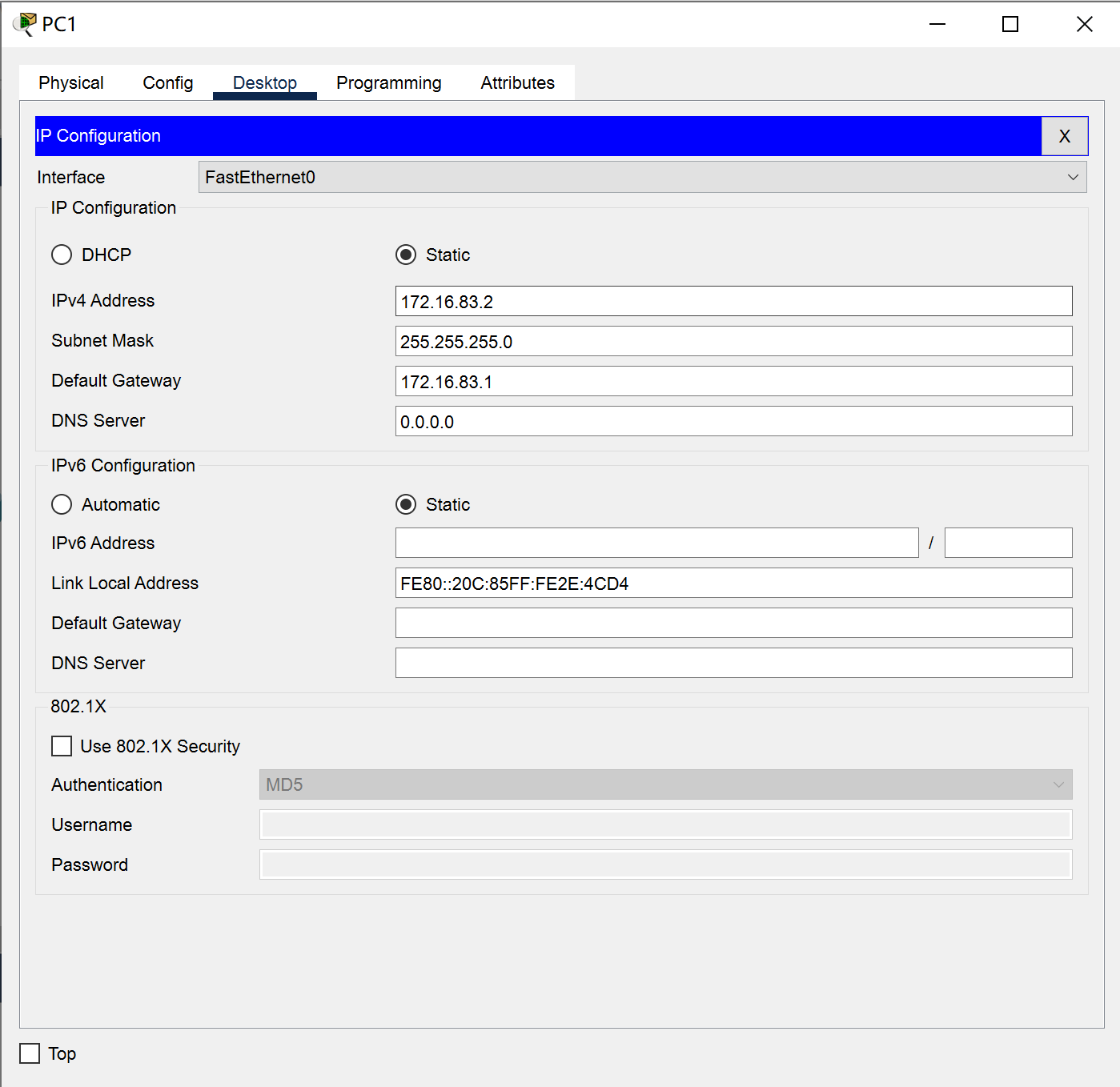
子网掩码：255.255.255.0

图2-24 PC的配置

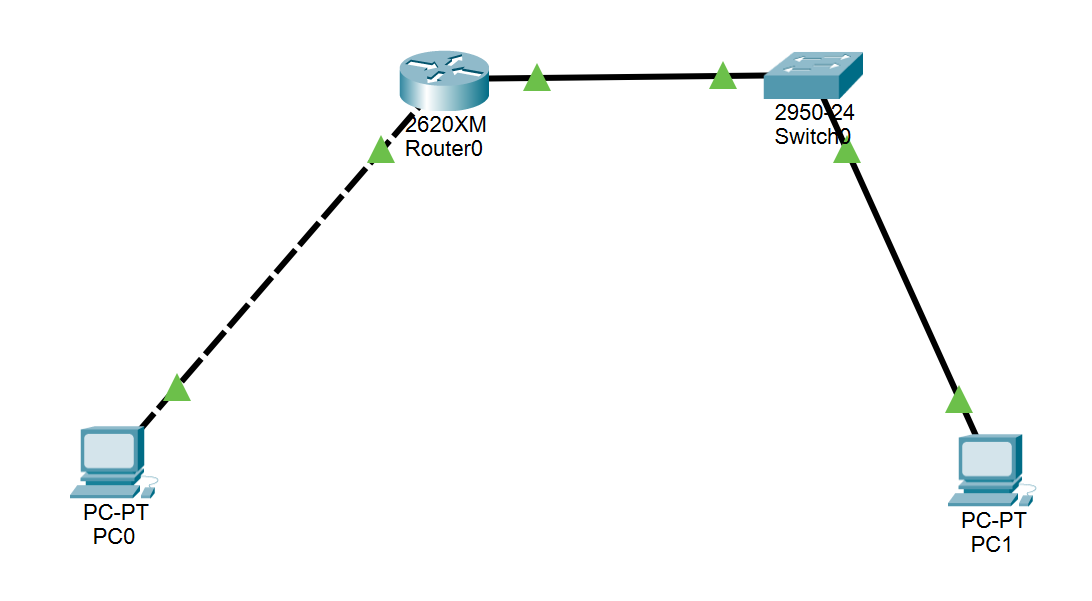
按上述配置完成后，发现所有圆点变为绿色。如图2-25所示。

图2-25 配置完成后就绪状态

(4)测试设备的连通性。如图2-26所示。

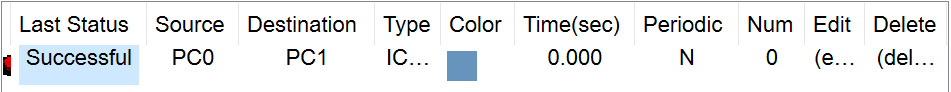
①在Realtime模式下添加一个从PC1->PC0的简单数据包。会观察到Last Status的状态为Successful,说明PC1->PC0的链路是通的。

图2-26 添加数据包

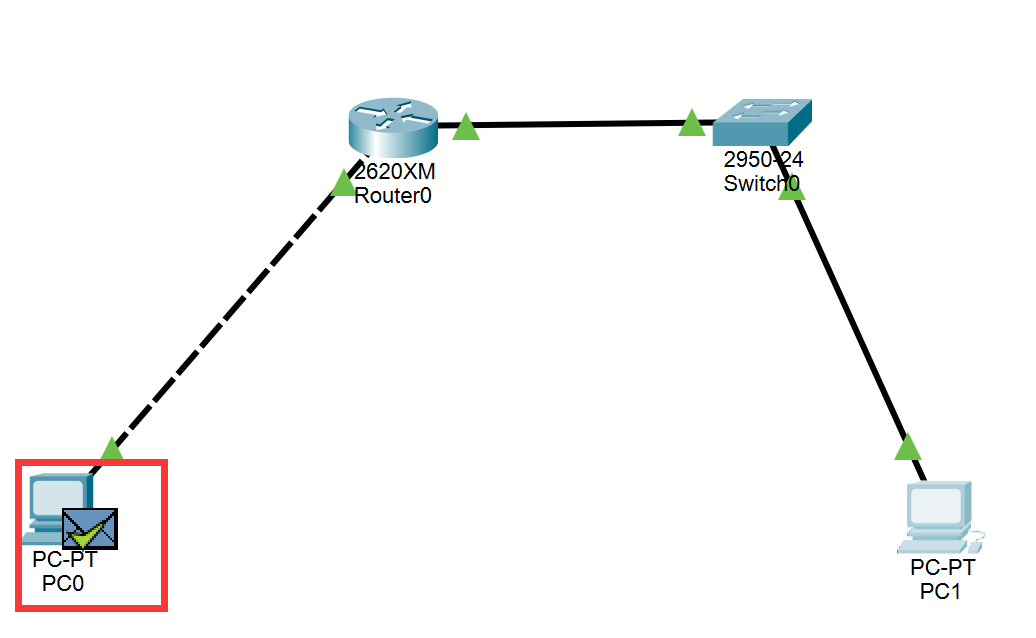
②在Simulation模式下跟踪这个数据包。点击Auto Capture，会发现数据包从PC0->PC1->PC0,顺利返回。如图2-27所示。

图2-27 数据包顺利传输

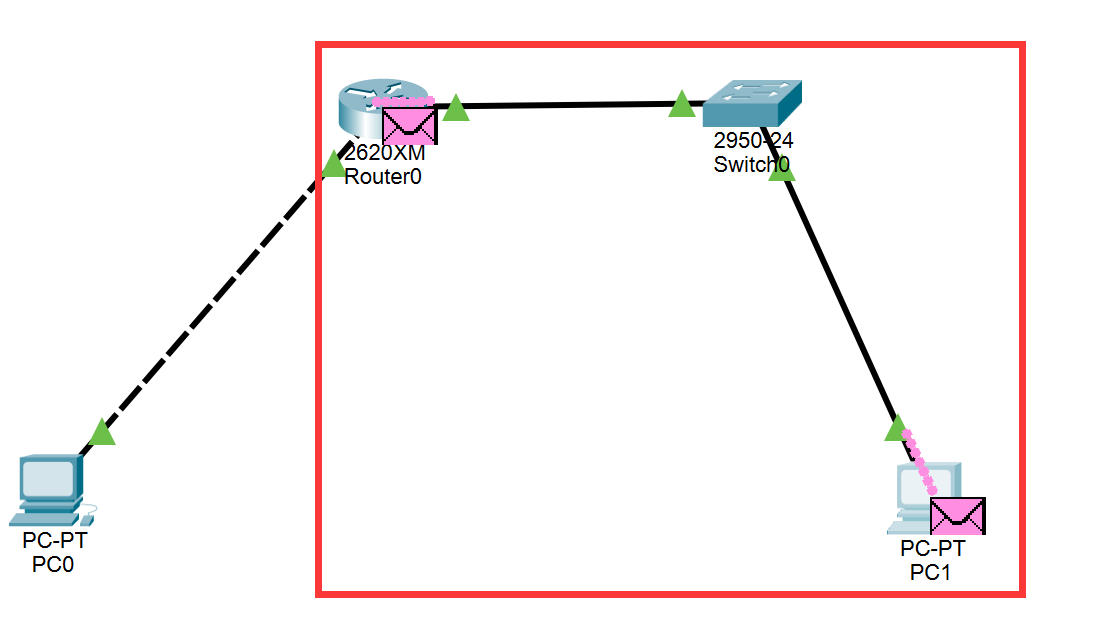
③点击capture/Forward。产生的一系列的事件说明了数据包的传输路径。如图2-28所示。

图2-28 数据包传输路径

④观察数据包在进出设备时OSI模型上的变化以及数据包或帧格式的变化。点击Router0上的数据包，打开PDU Information对话框。如图2-29所示。

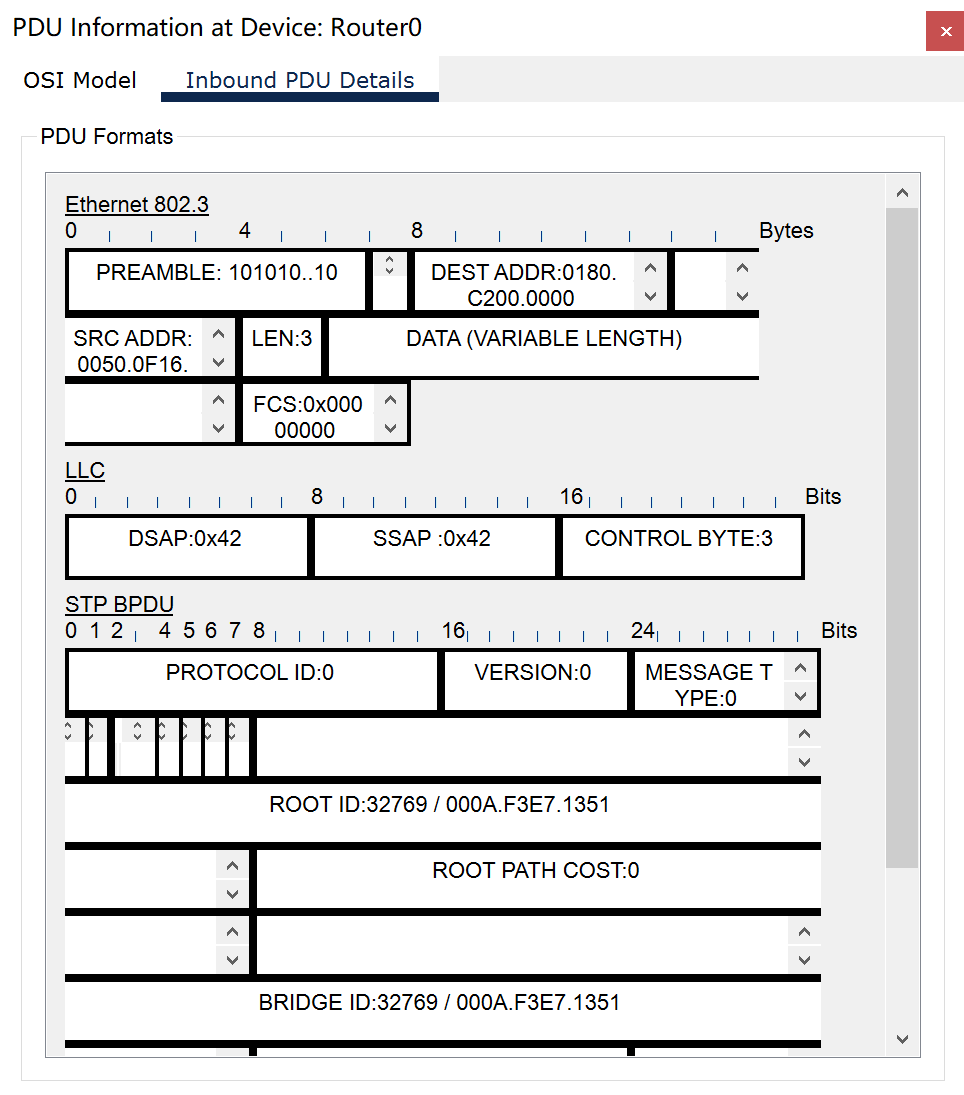
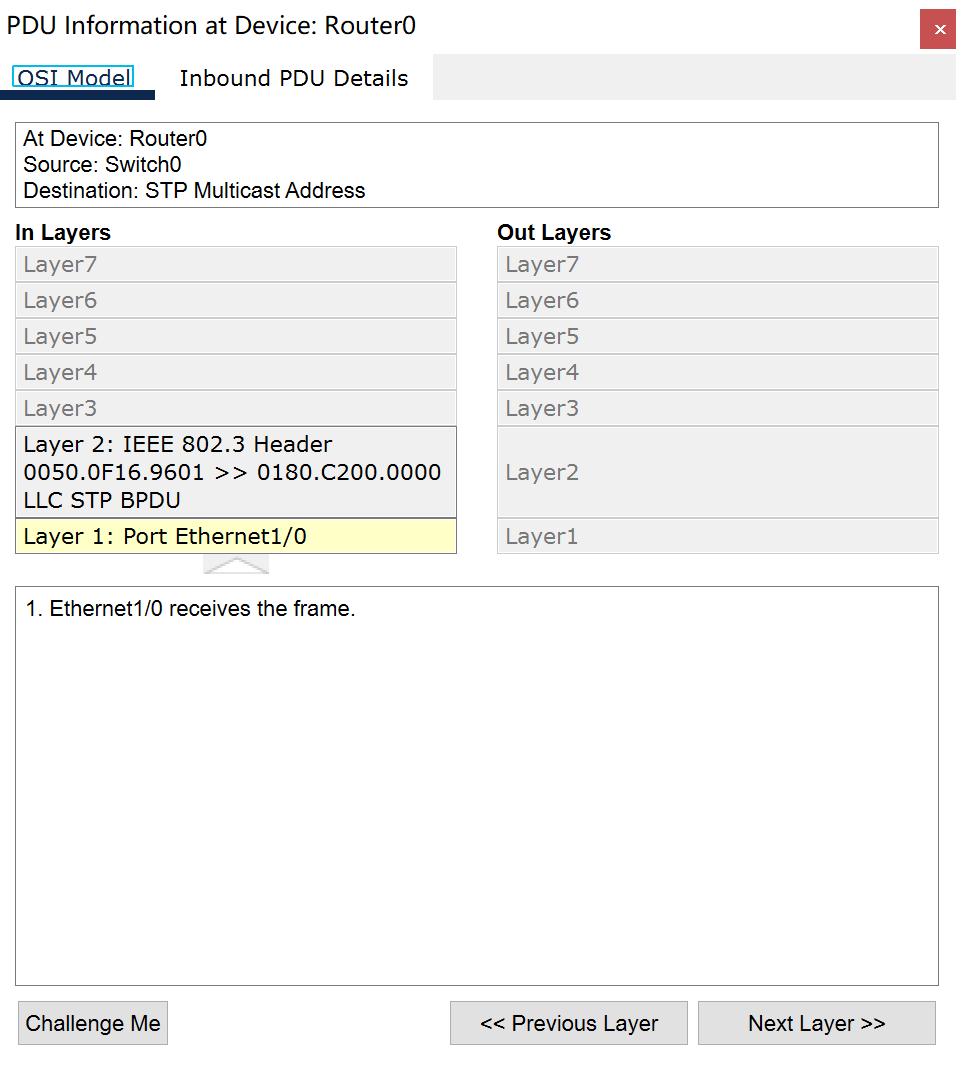
图2-29 数据包在OSI模型上的变化

图2-30 数据包在Inbound PDU Details中的变化

## 2.3 实验体会

经过计算机网络第二次实验的学习与实践，我深感自己在网络分析与设计方面的能力得到了显著提升。这次实验不仅加深了我对网络理论知识的理解，更使我在实践中锻炼了解决问题的能力，为我今后在网络领域的学习和工作打下了坚实的基础。

在实验中，我首先接触并熟练掌握了Wireshark这一强大的网络分析工具。通过设定抓包条件，我能够精确地捕获到网络中传输的各种数据包，并对其进行深入的分析。这一过程中，我逐渐理解了数据包的结构、传输过程以及在网络通信中的作用。这种直观的学习方式使我对网络协议和数据传输有了更为深刻的认识。

同时，我也学会了使用PT工具进行网络设计与分析。PT工具丰富的设备库、协议库和工具库为我提供了广阔的设计空间。在实验中，我不仅能够根据需求增删设备库和协议库，还能够利用PT工具进行网络设计、分析、测试和评估。通过亲手设计并验证各种网络场景，我逐渐掌握了网络设计的基本原理和方法，并培养了自己的设计创新能力。

在实践过程中，我遇到了一些挑战和困难。例如，在分析复杂网络数据时，我需要仔细研究数据包的每一个字段，并结合网络协议进行深入分析。这需要我具备扎实的网络理论知识和较强的逻辑思维能力。此外，在设计复杂网络场景时，我也需要充分考虑各种网络设备和协议之间的兼容性和交互性，以确保设计的合理性和有效性。这些挑战虽然增加了实验的难度，但也让我更加深入地理解了网络技术的复杂性和多样性。

我不仅掌握了Wireshark和PT等网络分析工具的使用技巧，还学会了如何运用这些工具解决实际问题。此外，我也更加深入地理解了网络技术的原理和应用场景，为我今后在网络领域的学习和工作提供了有力的支持。

----------------------------------以下表格用于评阅，不得擅自修改、删除--------------------------------------------

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **序号** | **报告内容** | **基础理论掌握程度** | **综合知**  **识应用**  **能力** | **报告**  **内容** | **报告**  **格式** | **完成**  **状况** | **工作量** | **学习、**  **工作**  **态度** | **抄袭**  **现象** | **其它** | **综合**  **成绩** |
| **8** | **应用层** | 请选择 | 请选择 | 请选择 | 请选择 | 请选择 | 请选择 | 请选择 | 学号:  姓名: | 目录、章节编目、错别字、乱码、截图、程序功能、程序源代码、源代码注释、体会、文献 |  |
| 批阅时间 | | 2024年5月22日 | | | | | | | | | |

----------------------------------以上表格用于评阅，不得擅自修改、删除--------------------------------------------