实验二　Wireshark 的使用与 PackerTracer 的使用

实验目的：掌握网络协议分析软件 Wireshark 的常用操作和网络模拟器 PackerTracer 的常用操作。

实验环境：计算机若干、直通双绞线若干、小型非管理交换机 10 台。

实验步骤：

1、**配置对等局域网**

2、**Wireshark 的使用**

（1）启动系统。点击 “Wireshark”图标，将会出现如图 1 所示的系统界面。

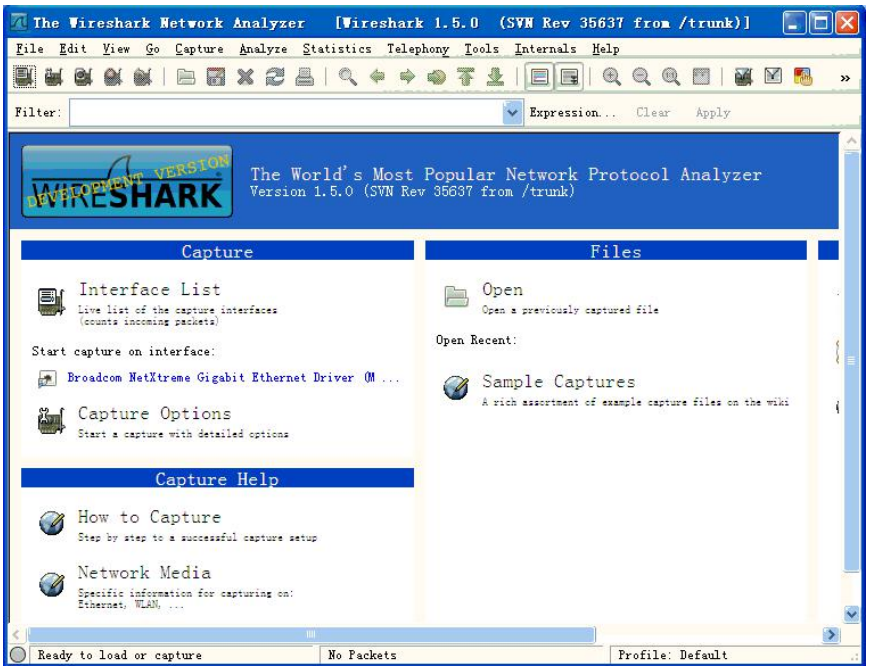

图 1 Wireshark 系统界面

其中“俘获(Capture)”和“分析(Analyze)”是 Wireshark 中最重要的功能。

(2) 分组俘获。点击“Capture/Interface”菜单，出现如图 2 所示界面。

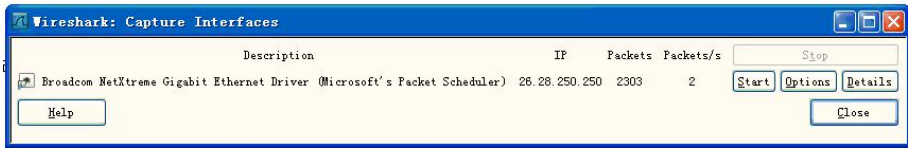

图 2 俘获/接口界面

如果该机具有多个接口卡，则需要指定希望在哪块接口卡俘获分组。点击“Options”，则出现图3 所示的界面。

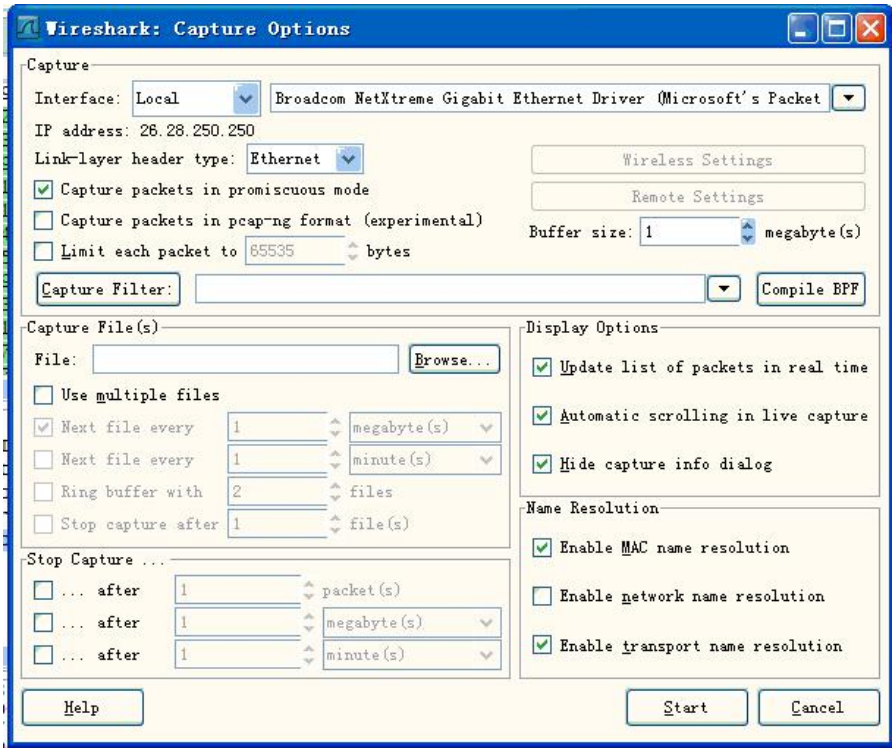

图3 俘获/接口/选项界面

在该界面上方的下拉框中将列出本机发现的所有接口；选择一个所需要的接口；也能够在此改变俘获或显示分组的选项。

此后，在图2 或者图3 界面中，点击“Start(开始)”，Wireshark 开始在指定接口上俘获分组，并显示类似于图4 的界面。

当需要时，可以点击“Capture/Stop” 停止俘获分组，随后可以点击“File/Save”将俘获的分组信息存入踪迹(trace)文件中。当需要再次俘获分组时，可以点击“Captuer/Start”重新开始俘获分组。

(3) 协议分析。系统能够对Wireshark 俘获的或打开的踪迹文件中的分组信息(用File/Open 功能)进行分析。如图4 所示，在上部“俘获分组的列表”窗口中，有编号(No)、时间(Time)、源地址(Source)、目的地址(Destination)、协议(Protocol)、长度(Length)和信息(Info)等列(栏目)，各列下方依次排列着俘获的分组。中部“所选分组首部的细节信息”窗口给出选中协议数据单元的首部详细内容。下部“分组内容”窗口中是对应所选分组以十六进制数和ASCII 形式的内容。

若选择其中某个分组如第255 号帧进行分析。从图4 中的信息可见，该帧传输时间为俘获后的15.129546 秒；从源IP 地址119.147.41.101 传输到目的IP 地址222.95.175.235；帧的源MAC 地址和目的MAC 地址分别是00.e0.fc.65.73.59 和00.16.35.aa.f3.75 (从中部分组首部信息窗口中可以看到)；分组长度74 字节；是TCP 携带的HTTP 报文。

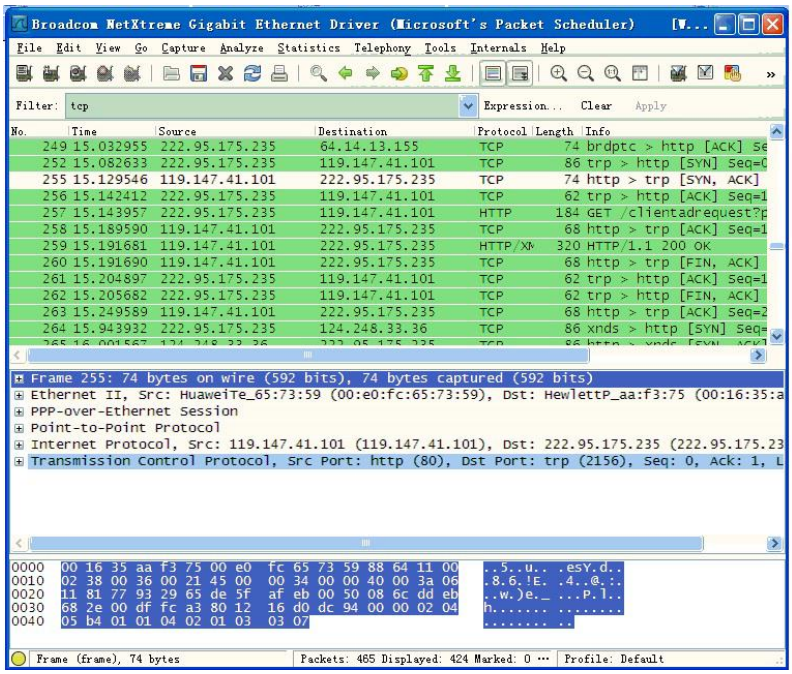

图4 Wireshark 的俘获分组界面

从分组首部信息窗口，可以看到各个层次协议及其对应的内容。例如，对应图5 的例子，包括了Ethernet II 帧及其对应数据链路层信息(参见图5)，可以对应Ethernet II 帧协议来解释对应下方协议字段的内容。接下来，可以发现Ethernet II 协议上面还有PPP-over-Ethernet 协议、Point-to-Point 协议、IP 和TCP 等，同样可以对照网络教材中对应各种协议标准，分析解释相应字段的含义。

注意：当我们分析自行俘获分组时，即使无法得到与如图4 所示完全一样的界面，但也能够得到非常相似的分析结果。在后面的实验中，读者应当有意地改变相应的报文内容或IP地址等，培养这种举一反三能力的能力。

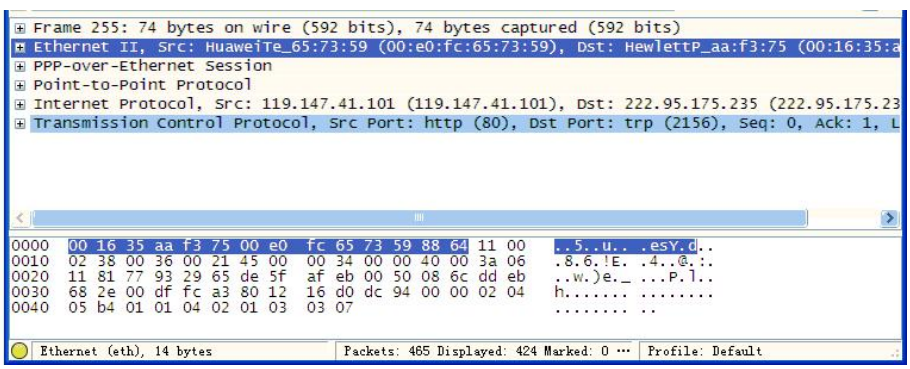

图5 Ethernet 帧及其对应数据链路层信息

当俘获的分组太多、类型太杂时，可以使用Analyze 中的“使能协议(Enabled Protocols)”和过滤器(Filters)等功能，对所分析的分组进行筛选，排除掉无关的分组，提高分析效率。

思考：

(1)通过使用Wireshark 协议分析仪，应当理解Wireshark 的工作原理，对于与之相关的

网络接口(指出网络接口卡类型)、网络地址(指出IP 地址、MAC 地址)、网络协议(指出发现的集中协议)等重要概念有基本的理解。

(2)在图4上部“俘获分组的列表”窗口中，有编号(No)、时间(Time)等字段信息。对于一段时间范围内往返于相同源和目的地之间的相同类型的分组，这些编号、时间等能否构成分析网络协议运行、交互轨迹的信息？

相关概念：

1) Wireshark 简介。Wireshark 是一种具有图形用户界面的网络协议分析仪，可以用于从实际运行的网络俘获分组或从以前保存的踪迹文件中交互地浏览、分析处理分组数据。Wireshark 是一个免费软件，因商标原因从Ethereal 改名而得，是能够在Windows、Linux/Unix和Mac 计算机上运行的免费分组嗅探器(packet sniffer)。Wireshark 能够读取libpcap 俘获文件，也能够读取包括用Tcpdump 俘获的文件，以及snoop，atmsnoop, LanAlyzer, Sniffer (压缩和非压缩的), Microsoft Network Monitor, AIX 的iptrace, NetXray, Sniffer Pro, Etherpeek, RADCOM的 WAN/LAN analyzer, Lucent/Ascend router debug output, HP-UX 的nettl, Cisco的安全入侵检测系统以IPLog 格式输出的pppd 日志文件。它能够自行分析文件类型，即使用gzip 进行压缩也是如此。

Wireshark 对于在实践中分析和调试网络协议，特别是对初学者理解网络协议都是十分有用的工具。当在家中或在实验室中使用桌面计算机运行网络应用程序时，可以用Wireshark观察本机基于网络协议与在因特网别处执行的协议实体交互和交换报文情况。因此，Wireshark能够使用户计算机成为真实动态实验的有机组成部分，通过动手实验来观察网络的奥秘，进而深入理解和学习它们。能够得到极大地深化读者的网络概念和提升实验技能：观察网络协议的动作和动手操作它们，即观察两个协议实体之间交换的报文序列，钻研协议运行的细节，使协议执行某些动作，观察这些动作及其后果。

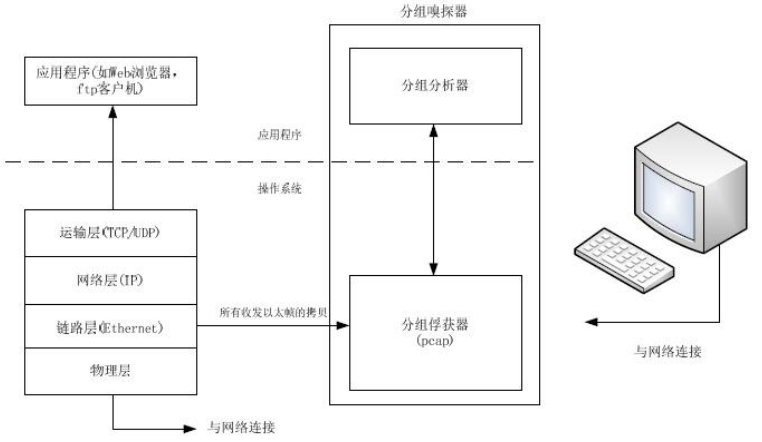

图6 分组嗅探器结构

2) Wireshark 的结构。作为分组嗅探器，Wireshark 俘获从计算机发送接收的报文，通常也能够存储和显示这些俘获的报文中各个协议字段的内容。分组嗅探器自身是被动的，观测运行在计算机中的应用程序和协议所发送及接收的报文，但自身并不发送分组。类似地，接收到的分组决不会显式地以分组嗅探器为目的地址，它们仅是在机器上运行的应用程序和协

议收发分组的副本。图6 显示了分组嗅探器的结构。图中的计算机通常运行着应用程序及其协议，显示在图中方框内的分组嗅探器是计算机中附加的一个普通软件，它由两部分组成。分组俘获器接收计算机收发的每个链路层帧的副本。大家知道较高层协议如HTTP、FTP、TCP、UDP、DNS 或IP 之间交换的报文全都逐个封装在链路层帧中，并在物理介质如以太电缆上传输。如果图中的物理介质是以太双绞线等，则所有高层协议则将封装在以太帧中。俘获所有链路层帧从而使读者能够观察到在计算机中执行的所有应用程序和协议收发的报文。

嗅探器的第二部分是分组分析器，它显示协议报文的所有字段的内容。为了实现该功能，分组分析器必须要能理解协议交换的所有报文结构。例如，如果想要显示图中由FTP 交换报文的各个字段，则该分组分析器需要理解以太帧格式，这样才能识别以太帧中的IP 数据报，进而通过分析IP 数据报才能从中提取TCP 报文段。只有理解了TCP 段结构，才能提取包含在TCP 段中的FTP 报文。最终，只有理解了FTP 协议，才能正确显示“USER”、“PASS”或“LIST”等命令。

注意事项：

1) 安装Wireshark 网络协议分析仪前应安装WinPcap 网络监测驱动程序。

2) 俘获分组前应注意选择正确的网络接口。

3) 协议分组的俘获结果可以保存在指定的文件中，并可以在以后再行使用。

4) Wireshark 网络协议分析仪还具有其他丰富的功能，读者可以参阅随软件的“Wireshark帮助”文档自行学习。

3、PackerTracer 的使用

1) 使用 **PacketTracer** 模拟器

(1) 启动系统。点击 “CISCO Packet Tracer”图标，将会出现如图1 所示的系统界面。

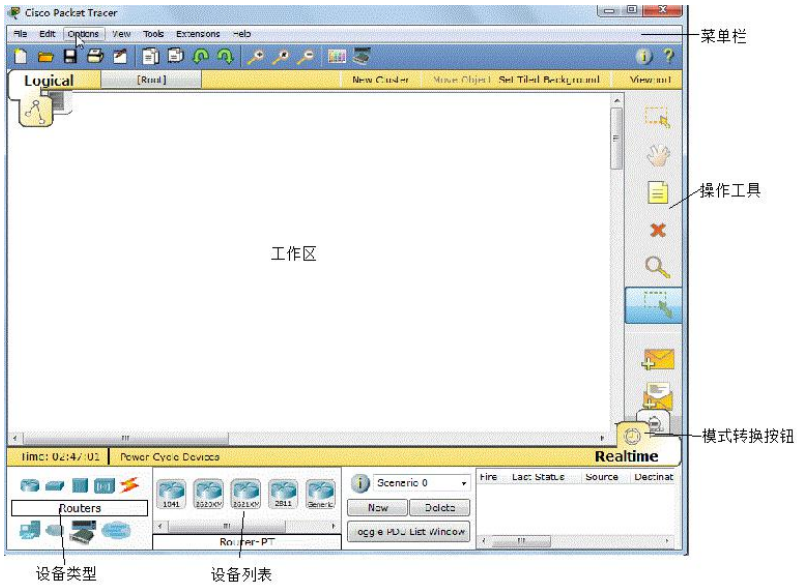

图1 PacketTracer 的主界面

菜单栏中包含新建、打开、保存等基本文件操作，其下方是一些常用的快捷操作图标。

工作区则是绘制、配置和调试网络拓扑图的地方。操作工具位于工作区右边，自上而下有7个按钮。这些操作工具的作用分别是：选择(Selected)，用于选中配置的设备；移动(Move Layout)，用于改变拓扑布局；放置标签(Place Note)，用于给网络设备添加说明；删除(Delete)，用于去除拓扑图中的元素，如设备、标签等；检查(Inspect)，用于查询网络设备的选路表、MAC 表、ARP 表等；增加简单的PDU(Add Simple PDU)，用于增加IP 报文等简单操作；增加复杂的PDU(Add Complex PDU)，可以在设置IP 报文后再设置TTL 值等操作。使用检查工具可以查看网络设备(交换机、路由器)的3 张表，该功能等同于在IOS 命令行中采用相应的show 命令，如show arp。增加简单的PDU 和增加复杂的PDU 两个工具用于构造测试网络的报文时使用，前者仅能测试链路或主机之间是否路由可达，后者则具有更多的功能。例如，要测试PC0 到Router0 之间的连通性，可以先用增加简单的PDU 工具点击PC0，再用该工具点击Router0 就可以看出两设备之间是否连通。如图2 所示。

图2 用增加简单的PDU 工具测试设备之间的连通性

增加复杂的PDU 工具的使用方法稍复杂些，也是先用工具依次点击所要测试链路的两端，再设置所要发送的报文格式。设置报文格式如图3 所示。

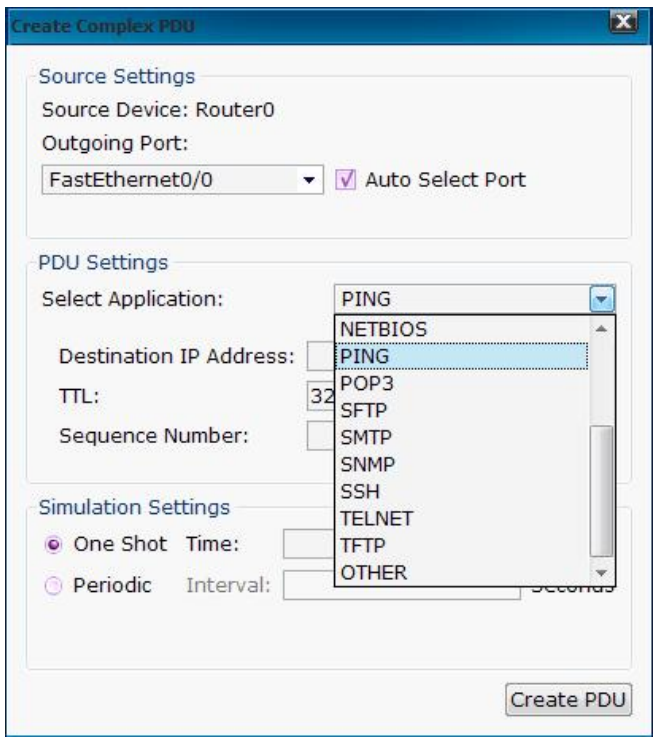

图3 定制增加复杂的PDU 中的报文

在主界面右下角，是转换实时模式与模拟模式的按钮。在实时模式下，所有操作中报文的传送是在瞬间完成。在模拟状态下，报文的传送是按操作一步一步地向前走，有助于

我们仔细地观察报文的具体传输过程。

(2) 绘制网络拓扑图

绘制网络拓扑图主要有以下几个步骤：增加网络设备，增加设备硬件模块，连接设备和配置设备等。

增加网络设备：在主界面下方有增加网络设备的功能区，该区域有两个部分：设备类别选择区域以及显示某个类别设备的详细型号区域。先点击设备类别，再选择具体型号的设备。例如，先从左下角区域选择了路由器类别，此时右侧区域将显示可用的各种CISCO路由器型号列表，点选后可以将其拖入工作区。这样，可以从中选用所要的(大量的!)网络设备。

增加设备硬件模块(选项)：如果选用的网络设备恰好适用，则可以进行下一步。但有时有些设备基本合用，但还缺少某些功能，如某种硬件接口数量不够等，这就需要通过增加设备硬件模块来解决。例如，如果选择了路由器2620XM，发现它仅有一个10/100Mbps 的以太端口，一个控制端口和一个辅助设备端口。若需要扩展一个光纤介质的100 Mbps 的以太端口和一些RJ45 端口的以太端口。这时双击工作区路由器2620XM 图标，可以看到如图4所示的界面。从图中左侧物理模块列表中找出模块NM-1FE-FX，从左下方窗口中的描述发现它符合要求，就可以将其拖入上部的物理设备视图中。由此，可以完成所有相关操作。

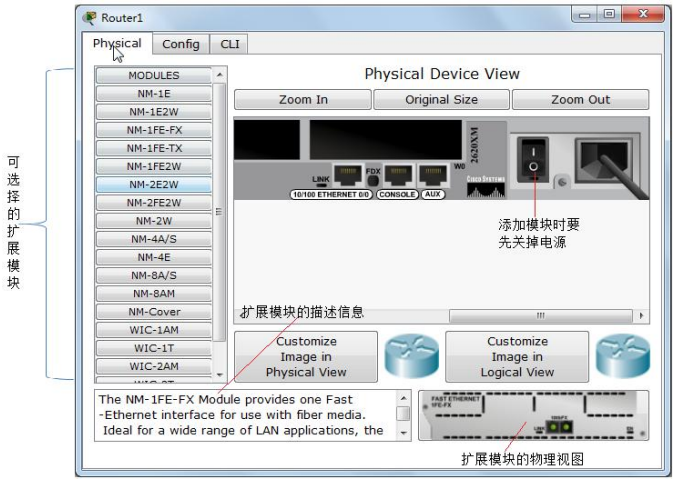

图4 路由器2620XM 的物理接口

连接设备：在设备类型区域选取“连接(Connections)”，再在右侧选取具体连接线缆类型。注意到连接线缆有如下不同类型： 线缆有控制口(Console) 、直连铜线(Copper Straight-Through)、交叉铜线(Copper Cross-Over)和光纤(Fiber)等，你需要选取适当的线缆类型才能保证设备能够正确连通。

配置设备：配置网络设备是一件细致的工作，将在其他实验中讲解配置网络设备详细过程。

下面以图5 为例，讲解绘制一幅简单的网络拓扑图的过程(参见图5) 。

先用上述方法从设备区拖入两台PC 和一台交换机，再用直通铜线与某个RJ45 以太端口连接。稍侯片刻，线缆端的点就会变绿，表示所有的物理连接都是正确的，否则要检查并排除所存在的物理连接方面的问题。

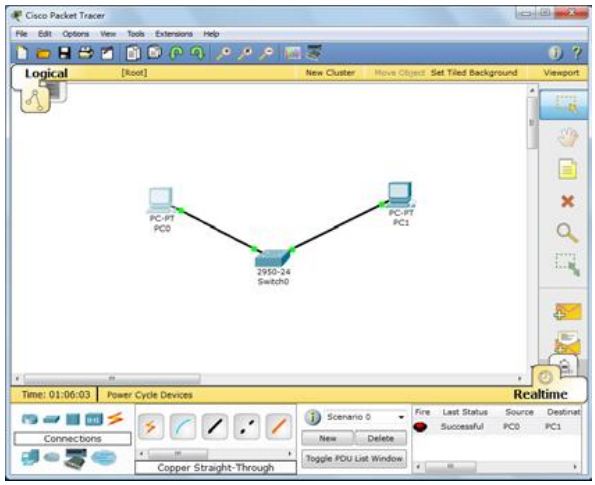

图5 经交换机连接两台PC

为了使两台PC 之间IP 能够连通，需要进一步配置该网络的网络层协议。双击PC0 的图标，进入“Config/FastEthernet”界面，开始配置“IP Configuration”。选静态(Static)方式，IP 地址可以输入：192.168.1.1，子网掩码可以选：255.255.255.0。对PC1 图标，也进行类似的配置，只是IP 地址可以为：192.168.1.2。为了检验配置是否正确，双击PC0，进入“Desktop/Command Ptompt”界面，键入：ping 192.2.162.2，这时就应当出现PC1 对该Ping 响应的信息。由于交换机是一种自配置的设备，无需配置就能使用其基本功能工作。

2)观察与**IP** 网络接口的各种网络硬件

为了能够利用IP 进行通信，网络设备硬件接口之间至少要用一种物理介质连接好，并且要求这些硬件接口与物理介质相匹配。下面，通过实验来研究相关内容。

从PacketTracer 中打开路由器2620XM 的物理设备视图，仔细做下列工作：观察有关NM-1FE-FX 模块描述；将其拖入设备，观察模块面板上的硬件接口情况(可以用Zoom In 放大)；做笔记，并自行分析该模块的适用场合。

对路由器2620XM 的NM-1FE-TX、NM-2FE2W、NM-8AM、NM cover plate 模块分别做出上述工作。

3)ping 和**traceroute** 实验

(1) 启动系统。在网络设备库中选择型号为“1841”的路由器一台，PC 机两台，如图6所示。

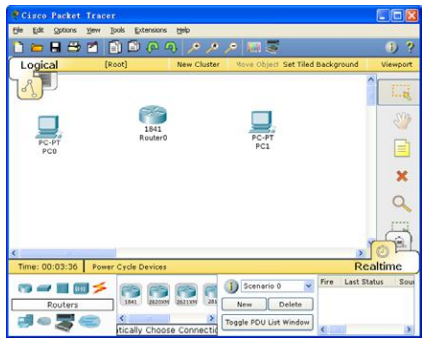

图6 构建网络拓扑

(2) 创建链路。在设备库中选择链路，选择自动添加链路类型，然后分别点击需要添加链路的设备，结果如图7 所示，此时链路两端红色表示链路不通。

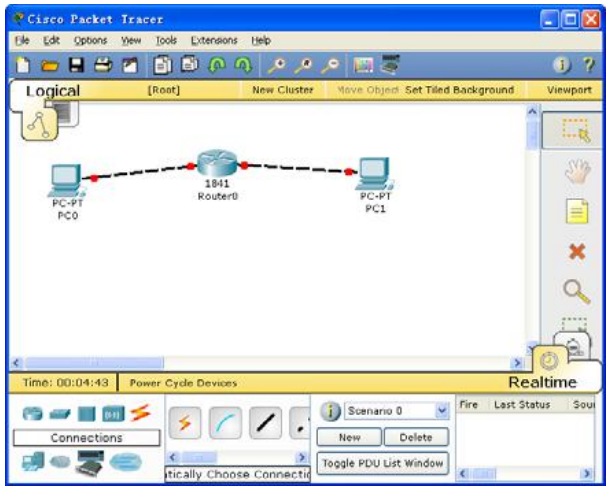

图7 添加链路

(3) 配置网络设备。双击设备，得到设备的配置界面。在PC 机的配置界面中，选择“Desktop”标签，选择“IP Configuration”，配置PC 机的地址信息，如图8 所示。按上述方法，将PC0 的IP 设置为192.168.1.2，子网掩码255.255.255.0，默认网关192.168.1.1。用同样的方法设置PC1 的IP 为192.168.2.2，子网掩码255.255.255.0，默认网关192.168.2.1。

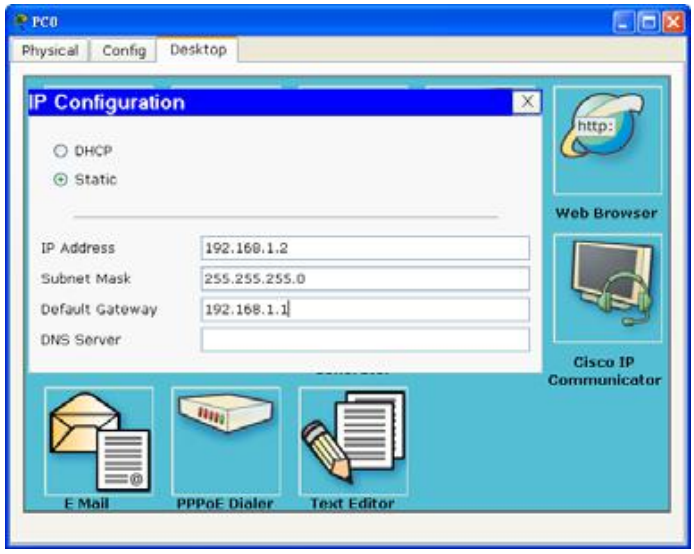

图8 PC 配置

配置路由器端口。设置Router0，在路由器配置界面中选择“config”标签，选择“FastEthernet0/0” ， 将IP 设置成192.168.1.1 ， 子网掩码255.255.255.0 ， 同样设置“FastEthernet0/1”，将IP 设置成192.168.2.1，子网掩码255.255.255.0，如图9 所示，注意将路由器端口打开。

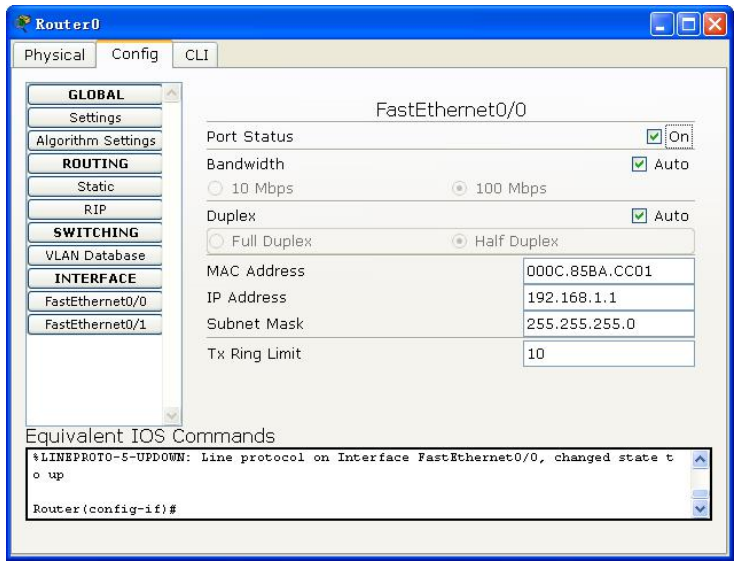

图9 路由器配置

(4) 使用Ping 命令，并在模拟模式下观察。如图10 所示，进入模拟模式。双击PC0 的图标，选择“Desktop”标签，选择“Command Prompt”，输入“ping 192.168.2.2”，如图11 所示。同时，点击“Auto capture/play”按钮，运行模拟过程，观察事件列表“Event List”中的报文。

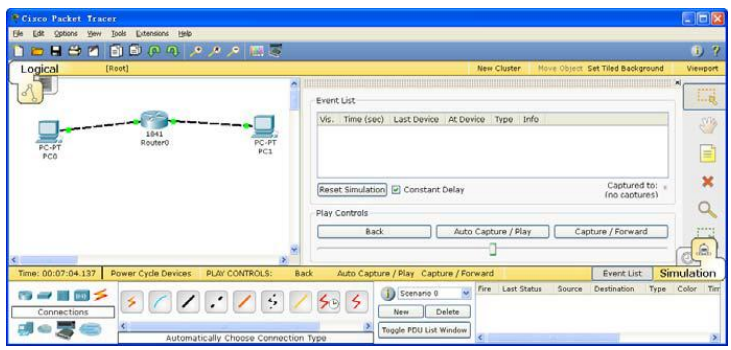

图10 进入模拟模式

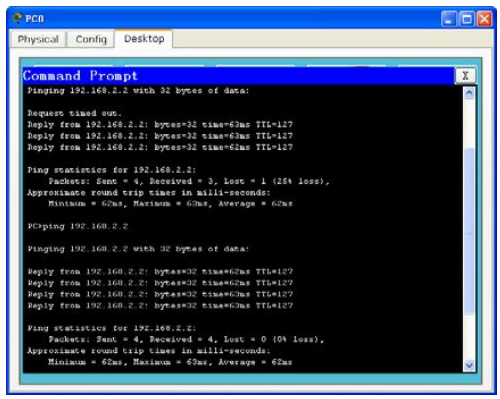

图11 运行ping 命令

(5) 使用tracert 命令，并在模拟模式下观察。

相关概念：

Packet Tracer 网络模拟器。PacketTracer 是著名网络设备厂商CISCO 公司开发的一种集成模拟、可视化、交互式学习和评价环境，供网络初学者学习计算机网络的设计、配置和排除故障之用。Packet Tracer 根据网络设备和协议的简化模型，以模拟、可视化、连续播放网络现象，使用者能够获得理解网络行为的感受，获得操作、配置网络设备的经验。

注意事项：

当物理连接正确时，与设备端口连接的线缆上的点应当变为绿色。否则，应当检查线缆的类型是否正确以及接口卡是否处于“开(on)”的状态。