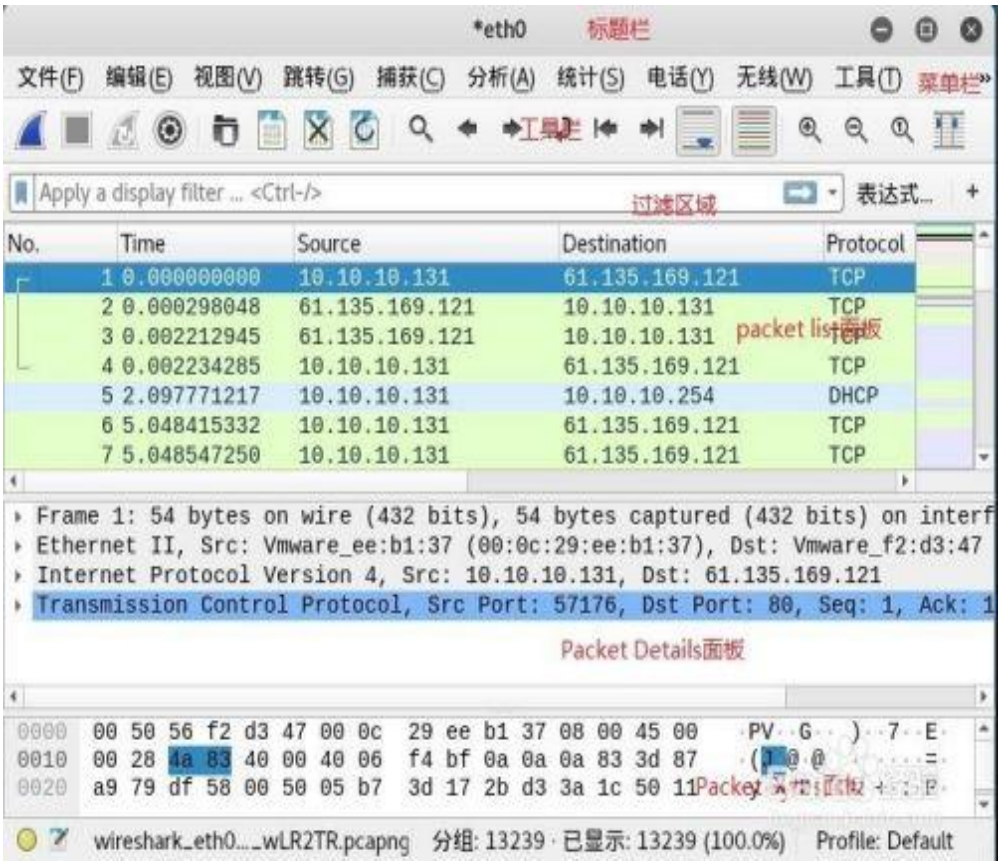
<table>
<tr><td>课题名称</td><td colspan="5">学习任务 1：初步认识和使用 Wireshark</td></tr>
<tr><td>所属项目</td><td colspan="5">项目三　网络安全协议分析</td></tr>
<tr><td>所属课程</td><td>网络安全技术</td><td>授课时数</td><td>4</td><td>授课地点</td><td>机房</td></tr>
<tr><td>学情分析</td><td colspan="5">1、学生原有知识分析
本课程面向计算机应用技术二年级学生，他们已经具备一些计算机网络基础知识，包括：IP 地址，常用的网络协议等，对 TCP/IP 七层网络体系结构有了一定的认识，掌握了数据包封装和解封的理论知识，为本节实训课的开展奠定了基础。
2、学生认知能力分析
高职学生普遍认知特点为表象性思维较强，对新奇、不断变化的事物有很强的好奇心；但是逻辑思维能力相对较差，在分析解决问题方面存在思维惰性。
3、学生学习能力及学习风格
学生学习总体表现为说过的、讲过的不知道、记不住，只有做过的才能理解，获得新知识和经验的途径倾向于观察和实际动手操作。在教学过程中采用讲授和实训相结合的方式，且通过教师演示、软件模拟增强学生对于抓包工具的直观感受。</td></tr>
<tr><td>教学目标</td><td colspan="5">知识目标：
掌握 Wireshark 抓包工具的使用方法
认识真实网络环境中的各种协议数据包
技能目标：
培养学生对抓包工具的使用
正确筛选过滤不同协议类型的数据包</td></tr>
<tr><td>教学重点</td><td colspan="5">正确使用 Wireshark 抓包工具并筛选过滤指定协议类型的数据包</td></tr>
<tr><td>教学难点</td><td colspan="5">筛选过滤指定协议类型的数据包</td></tr>
<tr><td>教学资源</td><td colspan="5">Wireshark 软件　PPT</td></tr>
<tr><td>教学方法</td><td colspan="5">任务驱动法 讲授法 多媒体辅助教学法</td></tr>
</table>

教学过程	
课前	作业一：预习常见的网络协议 作业二：发放实验任务
导入新课	数据包是真实网络环境中传输的最小数据单元，前面已经介绍了常用网络协议的数据包格式，为了更直观的认识真实网络环境中的数据包，今天我们通过 Wireshark 这款抓包软件来对局域网内的数据包进行抓取并筛选。
知识讲解	一、Wireshark 认识 1、Wireshark（前称 Ethereal）是一个网络数据包分析软件。网络数据包分析软件的功能是截取网络数据包，并尽可能显示出最为详细的网络数据包数据，为用户提供关于网络和上层协议的各种信息。Wireshark 使用 WinPCAP 作为接口，直接与网卡进行数据报文交换。 网络管理员使用 Wireshark 来检测网络问题，网络安全工程师使用 Wireshark 来检查资讯安全相关问题，开发者使用 Wireshark 来为新的通讯协定除错，普通使用者使用 Wireshark 来学习网络协定的相关知识。当然，有的人也会“居心叵测”的用它来寻找一些敏感信息……。 Wireshark 相对于 tcpdump 而言，界面更友好，功能更强大。 2、首先认识一下 wireshark 界面各个功能如下图。Packet List 面板主要显示抓取的数据包；Packet Details 面板展示数据包的详细信息，分层次显示一个数据包中的内容；Packet Bytes 面板以十六进制和 ASCII 码的形式显示数据包的内容，及数据包最原始的样子。我们在分析数据包的过程中主要关注 Packet List 以及 Packet Details。



3、常用按钮从左到右的功能依次是：

（1）开始捕获分组。

（2）停止捕获分组。

（3）重新开始当前捕获。

（4）捕获选项。

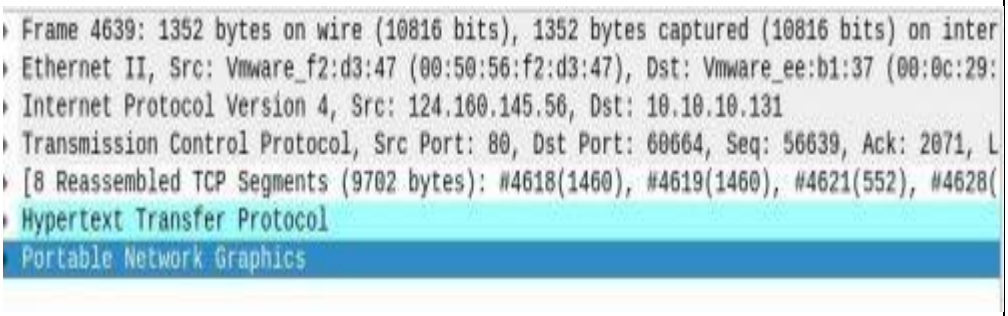
（5）打开已保存的捕获文件。

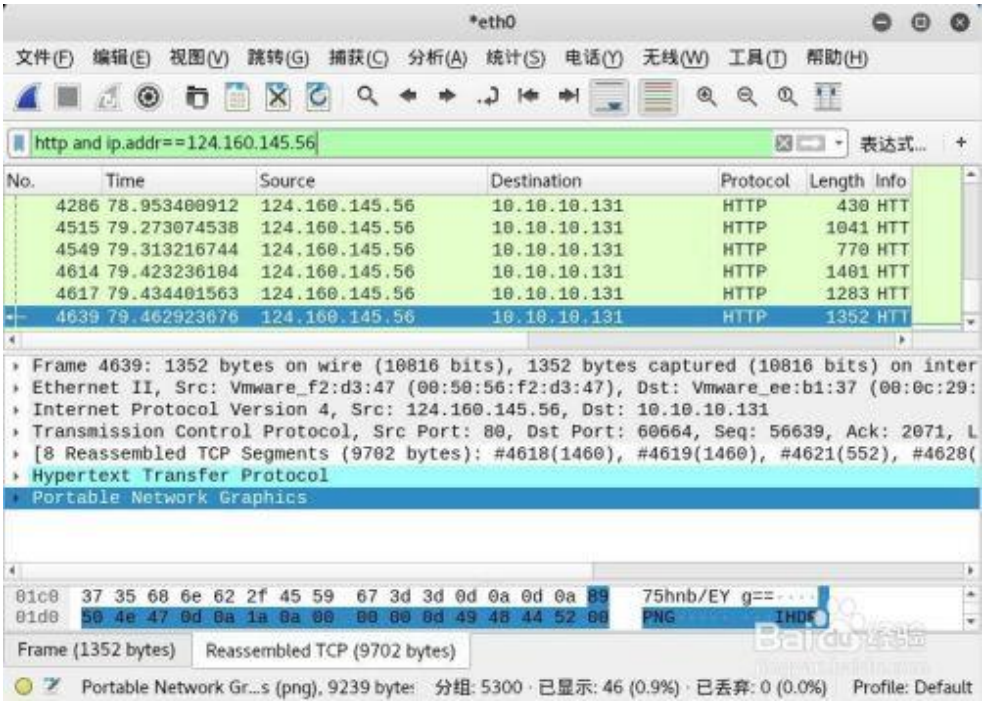
（6）保存捕获文件。

（7）关闭捕获文件。

（8）重新加载文件。

（9）查找一个分组。

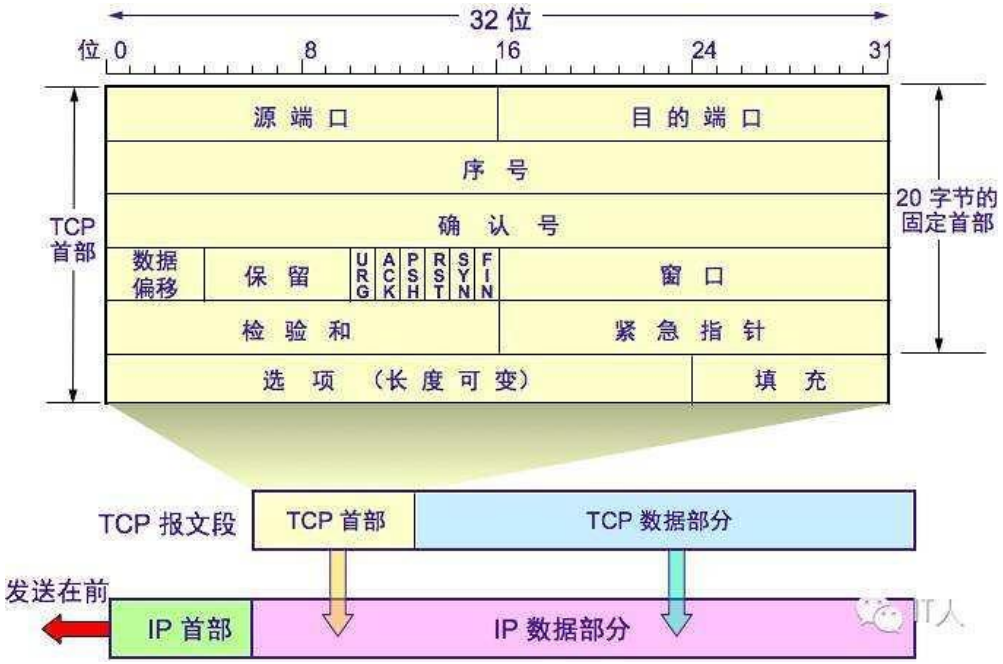
知识讲解	二、认识 HTTP 数据包 1、单击“开始捕获”按钮，然后打开浏览器，访问 www.baidu.com，停止捕获。 2、任意抓取一个 HTTP 协议的数据包，双击该分组，并查看下列信息： （1）Frame：物理层数据帧的情况。 （2）Ethernet II：数据链路层以太网帧头部的信息。 （3）Internet Protocol Version 4：网络层 IP 包的头部信息。 （4）Transmission Control Protocol：传输层的数据段头部信息，这里显示的是 TCP 协议。 （5）Hypertext Transfer Protocol：应用层信息，这里显示的是 HTTP 协议。  3、通过该数据包分组，重新复习 TCP/IP 协议的五层体系结构：从高到低分别是应用层、传输层、网络层、数据链路层和物理层。

知识讲解	三、筛选过滤器的用法 1、筛选过滤器位于菜单栏第三行，用户可以直接在过滤器中输入过滤条件，如果忘记过滤条件，过滤器的下拉列表中会有提示；如果过滤条件输入正确，过滤器的背景颜色是绿色，否则是红色。 2、在对筛选结果应用多个过滤条件的时候，需要结合与（and）、或（or）、非（not）等逻辑运算符，这样可以提高筛选效率。  例如：http and ip.addr == 124.160.145.56 （1）协议过滤：tcp、http、icmp （2）端口过滤：tcp.(srcport|dstport) == 80 tcp.port == 80 3、追踪 HTTP（TCP）流。在有些情况下，为了完整查看文件内容，需要对数据包内容进行跟踪，方法是：右击某个数据包分组，选则追踪流->http 流或者 tcp 流，就可以具体分析文件的全部内容。

知识讲解	四、数据包着色 在进行数据包筛选的过程中，为了能更好的对抓取到的数据包进行区分，那么就需要对数据包进行着色，使用不同颜色来对不同应用规则的数据包进行标注。 1、着色方法：在数据包列表中，单击选中一个需要进行标注的数据包，在菜单栏单击图标  即可应用默认着色规则对数据包进行着色。 2、着色规则： （1）Bad TCP：即 TCP 解析出错，通常重传，乱序，丢包，重复响应都在此条规则的范围内。 （2）HSRP 即热备份路由协议（Hot Standby Router Protocol）。 （3）Spanning Tree Topology Change：生成树协议的状态标记为 0x80，生成树拓扑发生变化。 （4）OSPF State Change：OSPF（Open Shortest Path First，开放式最短路径优先协议）的 msg 类型不是 hello。 （5）ICMP errors：ICMP 协议错误，协议的 type 字段值错误。 （6）ARP：arp 协议 （7）ICMP：icmp 协议 （8）HTTP：http 协议 （9）TCP：tcp 协议 （10）UDP：udp 协议 （11）Broadcast：广播数据 （12）TCP SYN/FIN：TCP 连接的起始和关闭 （13）IPX：互联网数据包交换类协议 （14）DCERPC：即 DCE/RPC，分散式运算环境/远端过程调用 （15）TTL low or unexpected：TTL 异常 （16）SMB：Server Message Block 类协议 （17）Checksum Errors：条件中的各类协议的 checksum 异常，在 PC 上抓包时网卡的一些设置经常会使 Wireshark 显示此错误
技能训练	实验任务详见实验报告。

<table>
<tr><td>课题名称</td><td colspan="5">学习任务 2：TCP 连接的“三次握手”与“四次挥手”</td></tr>
<tr><td>所属项目</td><td colspan="5">项目三　网络安全协议分析</td></tr>
<tr><td>所属课程</td><td>网络安全技术</td><td>授课时数</td><td>6</td><td>授课地点</td><td>机房</td></tr>
<tr><td>学情分析</td><td colspan="5">1、学生原有知识分析
本课程面向计算机应用技术二年级学生，他们已经具备一些计算机网络基础知识，包括：IP 地址，常用的网络协议等，对 TCP/IP 七层网络体系结构有了一定的认识，并且已掌握了 Wireshark 数据抓包软件的基本使用方法，为本节实训课的开展奠定了基础。
2、学生认知能力分析
高职学生普遍认知特点为表象性思维较强，对新奇、不断变化的事物有很强的好奇心；但是逻辑思维能力相对较差，在分析解决问题方面存在思维惰性。
3、学生学习能力及学习风格
学生学习总体表现为说过的、讲过的不知道、记不住，只有做过的才能理解，获得新知识和经验的途径倾向于观察和实际动手操作。在教学过程中采用讲授和实训相结合的方式，且通过教师演示、软件模拟增强学生对于抓包工具的直观感受。</td></tr>
<tr><td>教学目标</td><td colspan="5">知识目标：
掌握 TCP 报文的首部格式
掌握 TCP 传输控制协议的“三次握手”与“四次挥手”过程
技能目标：
培养学生正确识别 TCP 建立连接时的“三次握手”过程
培养学生正确识别 TCP 释放连接时的“四次挥手”过程</td></tr>
<tr><td>教学重点</td><td colspan="5">正确使用 Wireshark 抓包工具并筛选过滤指定协议类型的数据包</td></tr>
<tr><td>教学难点</td><td colspan="5">“三次握手”与“四次挥手”过程</td></tr>
<tr><td>教学资源</td><td colspan="5">Wireshark 软件　PPT 短视频</td></tr>
<tr><td>教学方法</td><td colspan="5">任务驱动法 讲授法 多媒体辅助教学法</td></tr>
</table>

<table>
<tr><td colspan="2">教学过程</td></tr>
<tr><td>课前</td><td>作业一：预习 TCP 报文的固定首部格式
作业二：预习 TCP 连接的“三次握手”和“四次挥手”过程
作业三：发放实验任务</td></tr>
<tr><td>导入新课</td><td>传输层由两个重要的协议：传输控制协议 TCP 和用户数据报协议 UDP。其中，UDP 协议提供面向非连接的不可靠的传输服务，而 TCP 提供面向连接的、可靠的传输服务。
TCP 连接的建立采用客户服务器方式。主动发起连接建立的应用进程叫做客户（client），而被动等待连接建立的应用进程叫做服务器（Server）。为了保证数据在传输的过程中绝对可靠，需要进行“三次握手”和“四次挥手”，今天我们借助 Wireshark 抓包软件在真实的网络环境中验证识别 TCP 建立连接的“三次握手”和释放连接的“四次挥手”。
一、背景知识
TCP 是面向连接的协议。TCP 运输连接的建立和释放是每一次面向连接的通信中必不可少的过程。因此，传输连接有三个阶段：连接建立、数据传送和连接释放。在 TCP 连接建立过程中要解决以下三个问题：
（1）要使每一方能够感知对方的存在。
（2）要允许双方协商一些参数（如窗口最大值、是否使用窗口扩大选项和时间戳选项以及服务质量等）。
（3）能够对运输实体资源（如缓存大小、连接表中的项目）进行分配。
TCP 连接的建立采用客户服务器方式。主动发起连接建立的应用进程叫做客户（client），而被动等待连接建立的应用进程叫做服务器（Server）。</td></tr>
</table>

知识讲解	二、TCP 报文首部  （1）源端口和目的端口：各占 2 个字节，分别写入源端口号和目的端口号。 （2）序列号 seq：占 4 个字节，用来标记数据段的顺序，TCP 把连接中发送的所有数据字节都编上一个序号，第一个字节的编号由本地随机产生；给字节编上序号后，就给每一个报文段指派一个序号；序列号 seq 就是这个报文段中的第一个字节的数据编号。当序号增加到 2^{32}-1 后，下一个序号就又回到 0，也就是说，需要使用 mod 2^{32} 运算。 （3）确认号 ack：占 4 个字节，期待收到对方下一个报文段的第一个数据字节的序号；序列号表示报文段携带数据的第一个字节的编号；而确认号指的是期望接收到下一个字节的编号；因此当前报文段最后一个字节的编号+1 即为确认号。记住：若确认号=N，则表明：到序号 N-1 为止的所有数据都已正确收到。 （4）数据偏移：占 4 位，它指出 TCP 报文段的数据起始处举例 TCP 报文段的起始处有多远，这个字段实际上是指出 TCP 报文段的首部长度。由于首部中还有长度不确定的选项字段，因此数据偏移字段是必要的。但应注意，“数据偏移”的单位是 4 字节。 （5）紧急 URG：当 URG=1 时，发送应用进程就告诉发送方的 TCP 有紧急数据要传送，于是发送方 TCP 就把紧急数据插入到本报文段数

据的最前面，而在紧急数据后面的数据仍是普通数据。

（6）确认 ACK：占 1 位，仅当 ACK=1 时，确认号字段才有效。ACK=0 时，确认号无效。TCP 规定，在连接建立后所有传送的报文段都必须把 ACK 置 1。

（7）同步 SYN：在连接建立时用于同步序号。当 SYN=1，ACK=0 时，表明这是一个连接请求报文段。若同意连接，则在响应报文段中使得 SYN=1，ACK=1。因此，SYN=1 表示这是一个连接请求，或连接接受报文。SYN 这个标志位只有在 TCP 建产连接时才会被置 1，握手完成后 SYN 标志位被置 0。

（8）终止 FIN：用来释放一个连接。FIN=1 表示：此报文段的发送方的数据已经发送完毕，并要求释放运输连接。

PS：ACK、SYN 和 FIN 这些大写的单词表示标志位，其值要么是 1，要么是 0；ack、seq 小写的单词表示序号。

（9）选项：长度可变，最长可达 40 字节，当没有选项时，TCP 的首部长度是 20 字节。

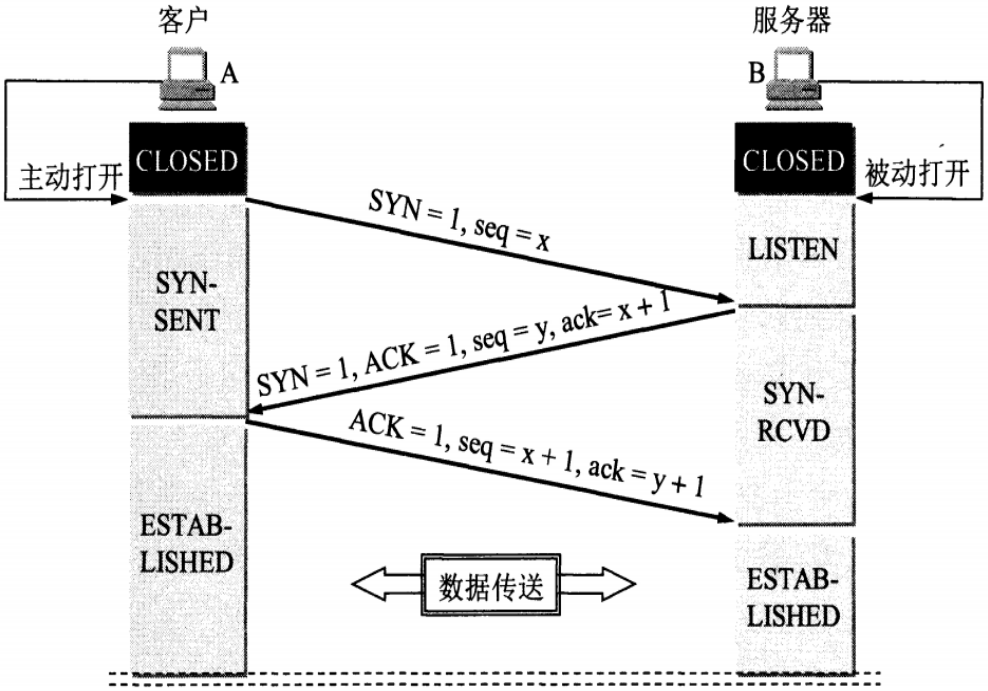
三、TCP“三次握手”

1、所谓三次握手（Three-Way Handshake），是指建立一个 TCP 连接时，需要客户端和服务端总共发送 3 个包以确认连接的建立。

Step1：客户端发送一个 SYN=1，ACK=0 标志的数据包给服务端，请求进行连接，这是第一次握手；

Step2：服务端收到请求并且允许连接的话，就会发送一个 SYN=1，ACK=1 标志的数据包给发送端，告诉它，可以通讯了，并且让客户端发送一个确认数据包，这是第二次握手；

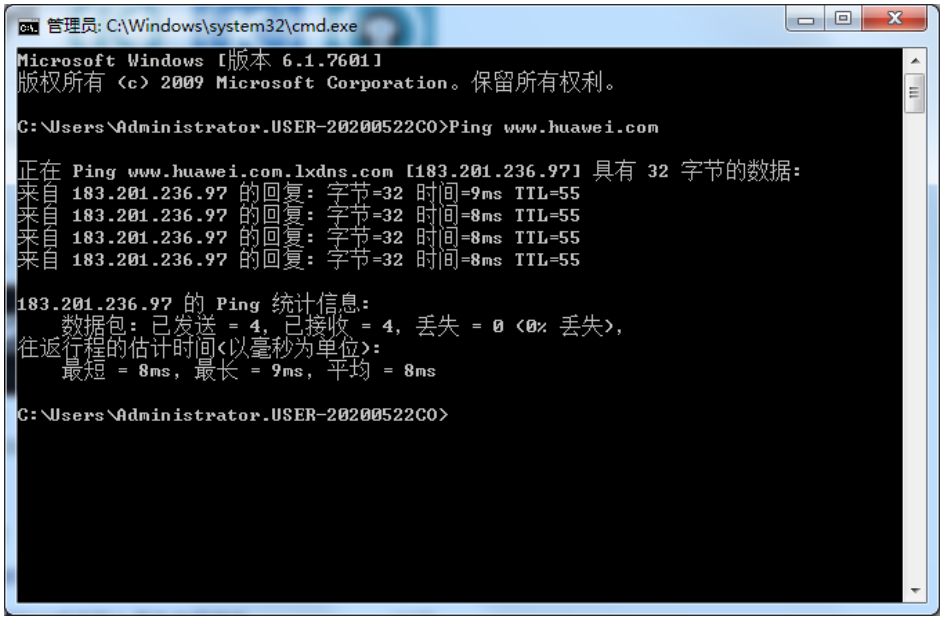
Step3：服务端发送一个 SYN=0，ACK=1 的数据包给客户端端，告诉它连接已被确认，这就是第三次握手。此包发送完毕，客户端和服务器进入 ESTABLISHED（TCP 连接成功）状态，完成三次握手。



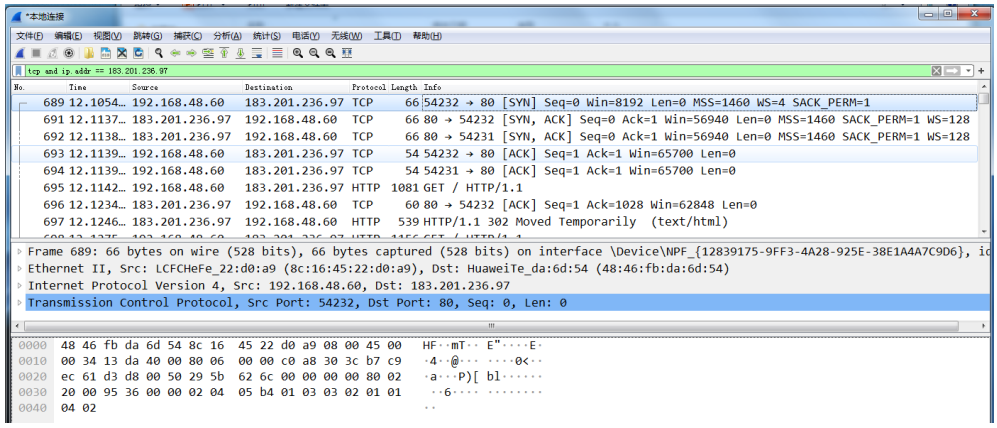
2、通过 Wireshark 抓包软件来验证 TCP 建立连接的“三次握手”

（1）启动 wireshark 抓包，打开浏览器输入 www.huawei.com；

（2）在命令行窗口中输入 ping www.huawei.com，获取 IP 地址；



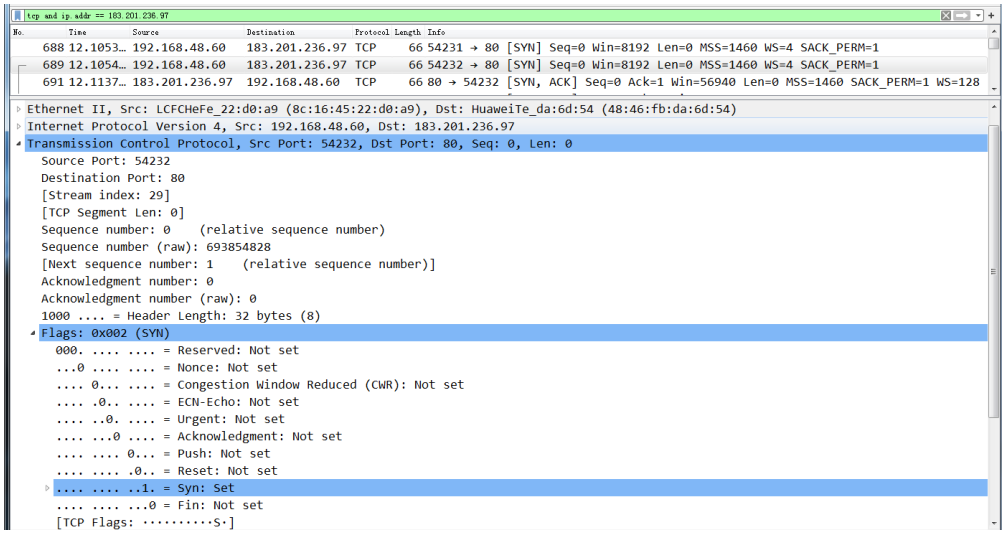
（3）在 Wireshark 的显示过滤器中输入过滤条件 tcp and ip.addr == 183.201.236.97；



图中可以看到，wireshark 截获到了三次握手的三个数据包，之后的数据包才是 HTTP 的，这说明 HTTP 的确是使用 TCP 建立连接的。

3、接下来，依次查看每次“握手”对应的数据包。

（1）第一次“握手”数据包：客户端发送一个 TCP，标志位为 SYN，序列号为 0，代表客户端请求建立连接，如下图所示。



数据包的关键属性如下：

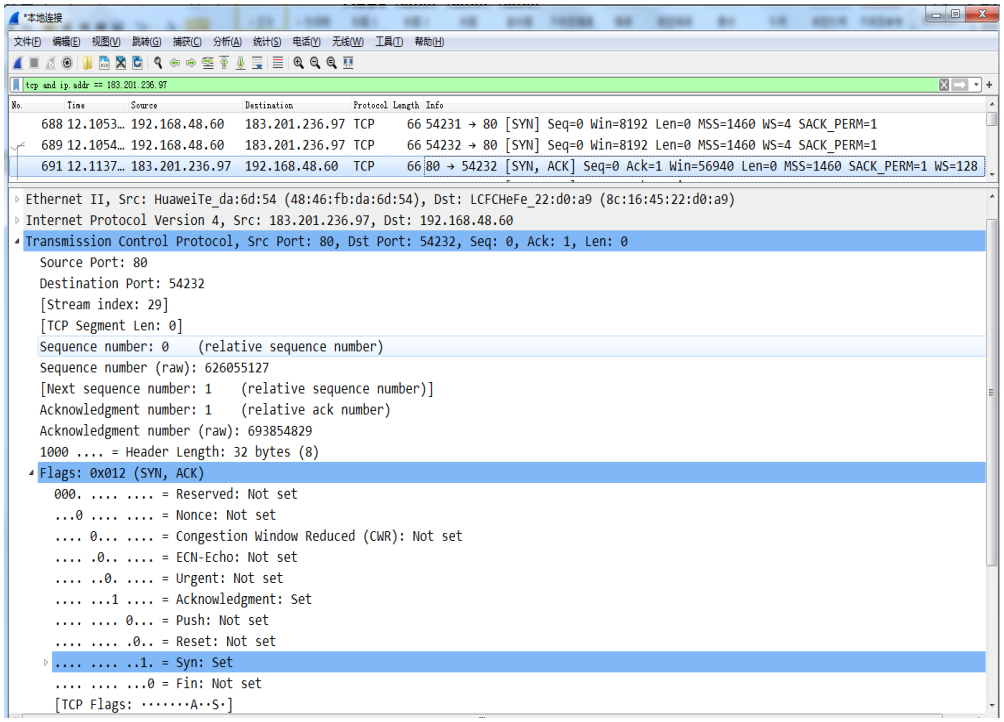
SYN ：标志位，表示请求建立连接

Seq = 0 ：初始建立连接值为 0，数据包的相对序列号从 0 开始，表示当前还没有发送数据

Ack =0：初始建立连接值为 0，已经收到包的数量，表示当前没有接收到数据

（2）第二次“握手”数据包：服务器发回确认包，标志位为 SYN，ACK。将确认序号(Acknowledgement Number)设置为客户的 ack 值加

1，即 0+1=1，如下图所示。



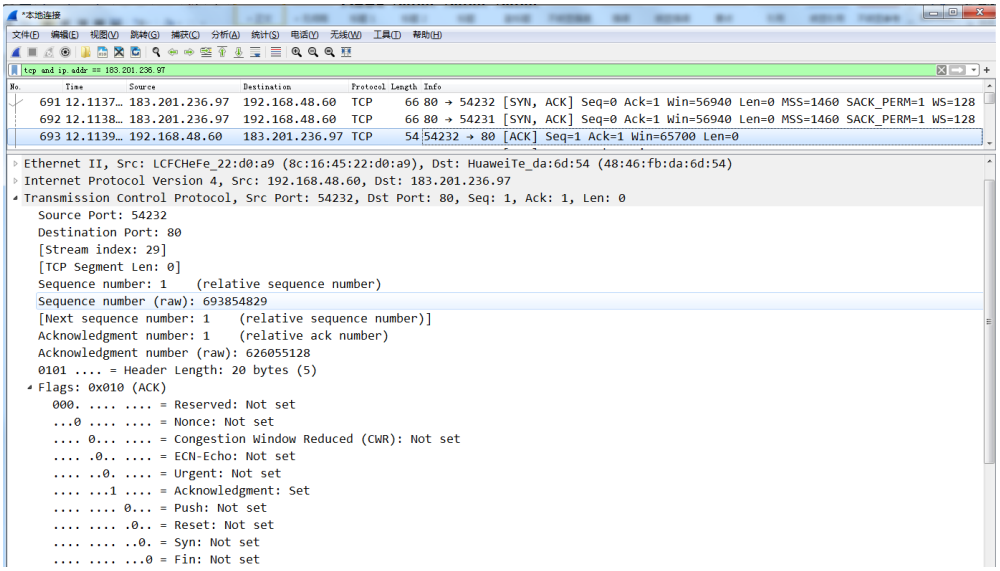
数据包的关键属性如下：

[SYN + ACK]: 标志位，同意建立连接，并回送 SYN+ACK

Seq = 0 ：初始建立值为 0，表示当前还没有发送数据

Ack = 1：表示当前端成功接收的数据位数，虽然客户端没有发送任何有效数据，确认号还是被加 1，因为包含 SYN 或 FIN 标志位。（并不会对有效数据的计数产生影响，因为含有 SYN 或 FIN 标志位的包不携带有效数据）

（3）第三次“握手”数据包：客户端再次发送确认包(ACK)，SYN 标志位为 0，ACK 标志位为 1，并且把服务器发来 ack 的序号字段+1，放在确定字段中发送给服务器，如下图所示。



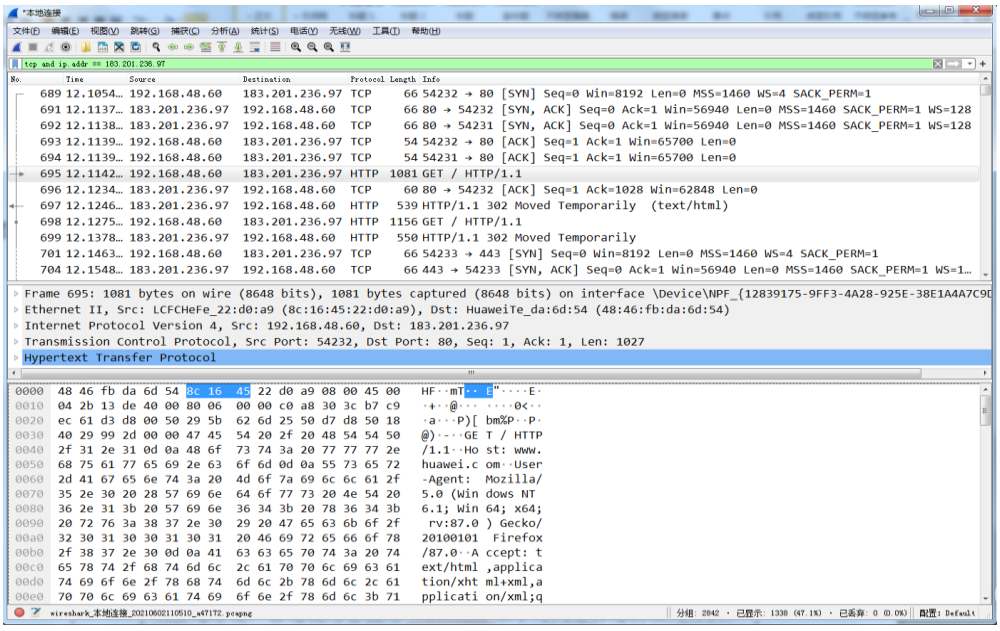
数据包的关键属性如下：

ACK ：标志位，表示已经收到记录

Seq = 1 ：表示当前已经发送 1 个数据

ack = 1：表示当前端成功接收的数据位数，虽然服务端没有发送任何有效数据，确认号还是被加 1，因为包含 SYN 或 FIN 标志位（并不会对有效数据的计数产生影响，因为含有 SYN 或 FIN 标志位的包并不携带有效数据)。

（4）就这样通过了 TCP 三次握手，建立了连接，接下来开始进行数据交互，如下图所示。



四、TCP 释放连接“四次挥手”

1、所谓四次挥手（Four-Way Wavehand），即终止 TCP 连接，就是指断开一个 TCP 连接时，需要客户端和服务端总共发送 4 个数据包以确认连接的断开。

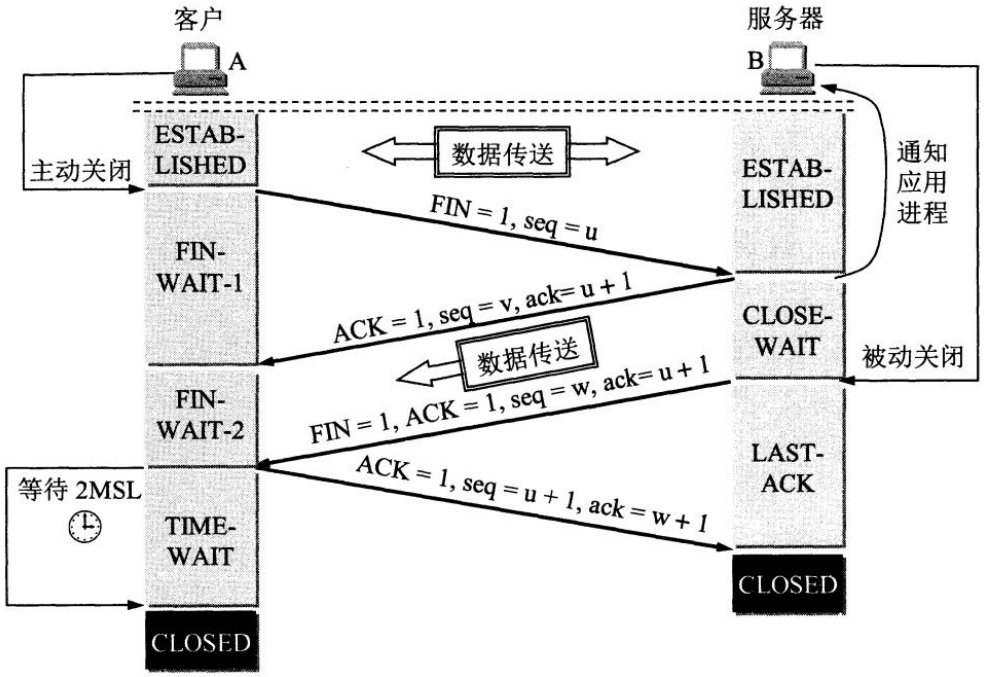
Step1：第一次挥手，Client 发送一个 FIN，用来关闭 Client 到 Server 的数据传送，Client 进入 FIN_WAIT_1 状态。

Step2：第二次挥手，Server 收到 FIN 后，发送一个 ACK 给 Client，确认序号为收到序号+1（与 SYN 相同，一个 FIN 占用一个序号），Server 进入 CLOSE_WAIT 状态。

Step3；第三次挥手，Server 发送一个 FIN，用来关闭 Server 到 Client 的数据传送，Server 进入 LAST_ACK 状态。

Step4：第四次挥手，Client 收到 FIN 后，Client 进入 TIME_WAIT 状态，接着发送一个 ACK 给 Server，确认序号为收到序号+1，Server 进入 CLOSED 状态，完成四次挥手。

由于 TCP 连接时全双工的，因此，每个方向都必须要单独进行关闭，这一原则是当一方完成数据发送任务后，发送一个 FIN 来终止这一方向的连接，收到一个 FIN 只是意味着这一方向上没有数据流动了，即不会再收到数据了，但是在这个 TCP 连接上仍然能够发送数据，直到这一方向也发送了 FIN。首先进行关闭的一方将执行主动关闭，而另一方则执行被动关闭，如下图所示。



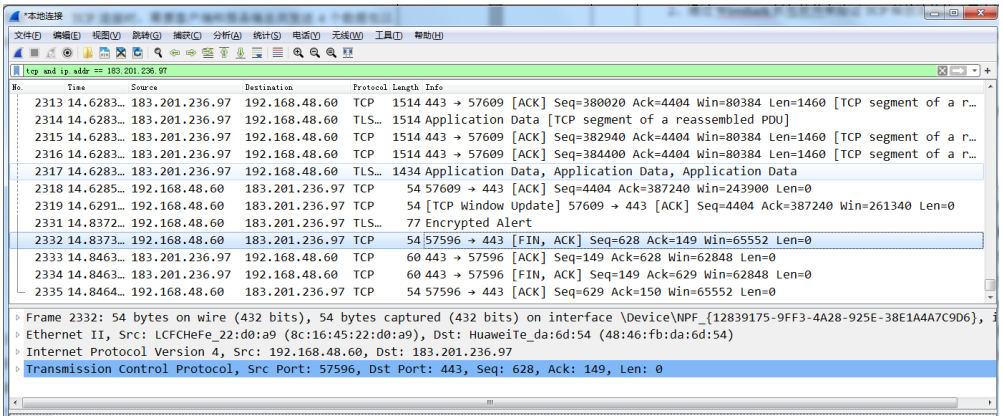
2、通过 Wireshark 抓包软件来验证 TCP 释放连接的“四次挥手”

（1）启动 wireshark 抓包，打开浏览器输入 www.huawei.com；

（2）在命令行窗口中输入 ping www.huawei.com，获取 IP 地址；

（3）在浏览器中关闭网址 www.huawei.com；

（4）在 Wireshark 的显示过滤器中输入过滤条件 tcp and ip.addr == 183.201.236.97

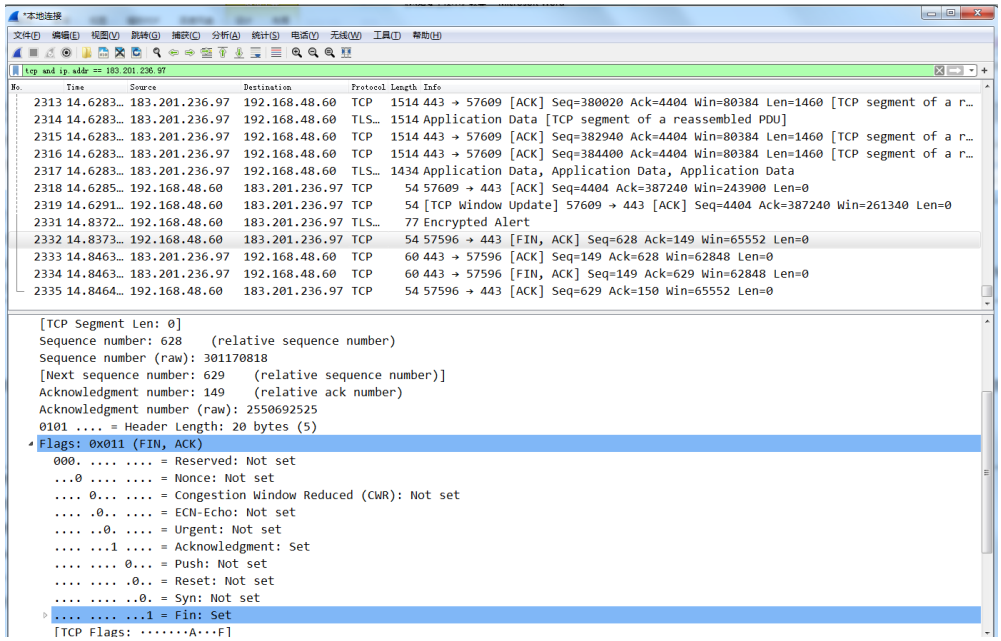


图中可以看到，wireshark 截获到了“四次挥手”的四个数据包，之后就没有数据包出现了。

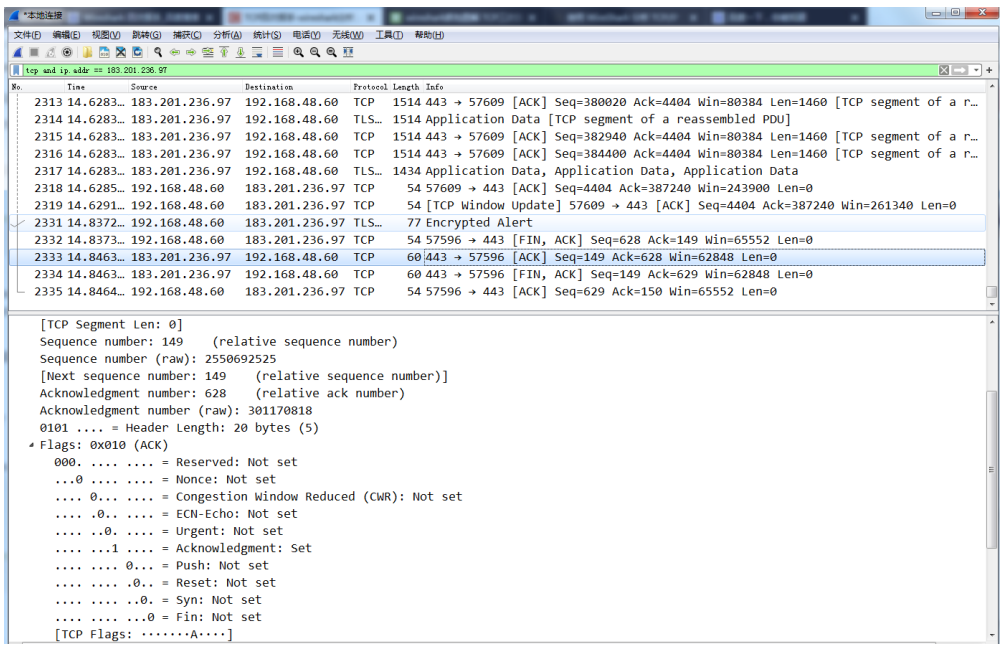
3、接下来，依次查看每次“挥手”对应的数据包。

（1）第一次“挥手”数据包：Client 首先发起了断开连接请求，Fin=1 表示 Client 已经没有数据要发送了，这个时候就会发送一个请求关闭

连接的信息给 Server 端，同样，这里包含 Seq = 451、Ack=149，Seq 表示这一次发送数据的起始序号，而 Ack =149 表示 Client 已经收到了 Server 端发送的 149 之前的所有的数据，期待下一次 Server 发送的 Seq = 149。ACK = 1 表示这是一个应答数据包，ACK 和 FIN 一起发送就表示这个数据包是一个确认和请求关闭连接，如下图所示。

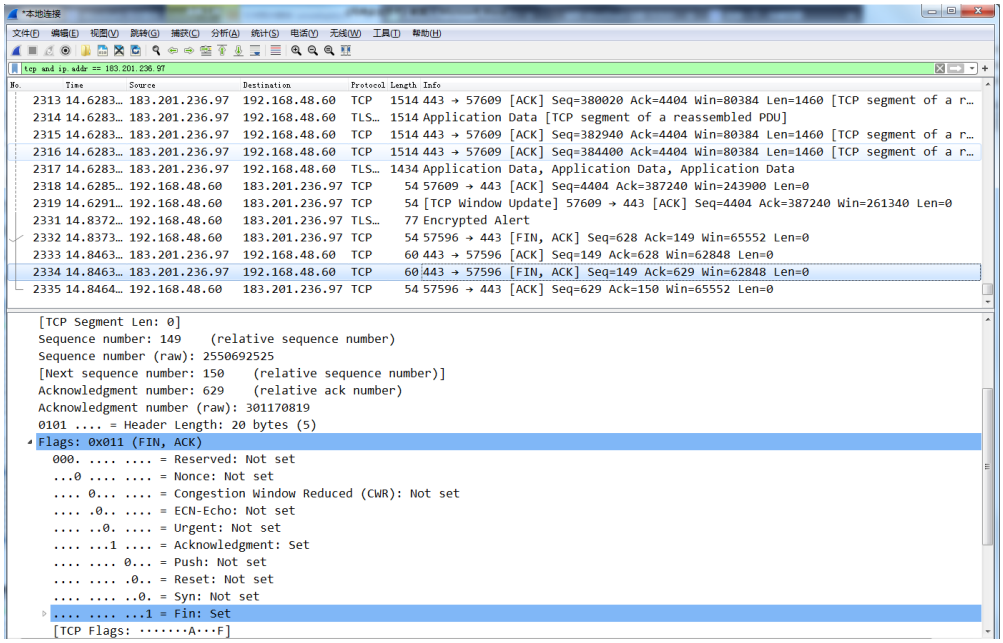


（2）第二次“挥手”数据包：Server 发送确认断开数据包，ACK=1，表示确定客户请求断开的信息成功接收了，如下图所示。

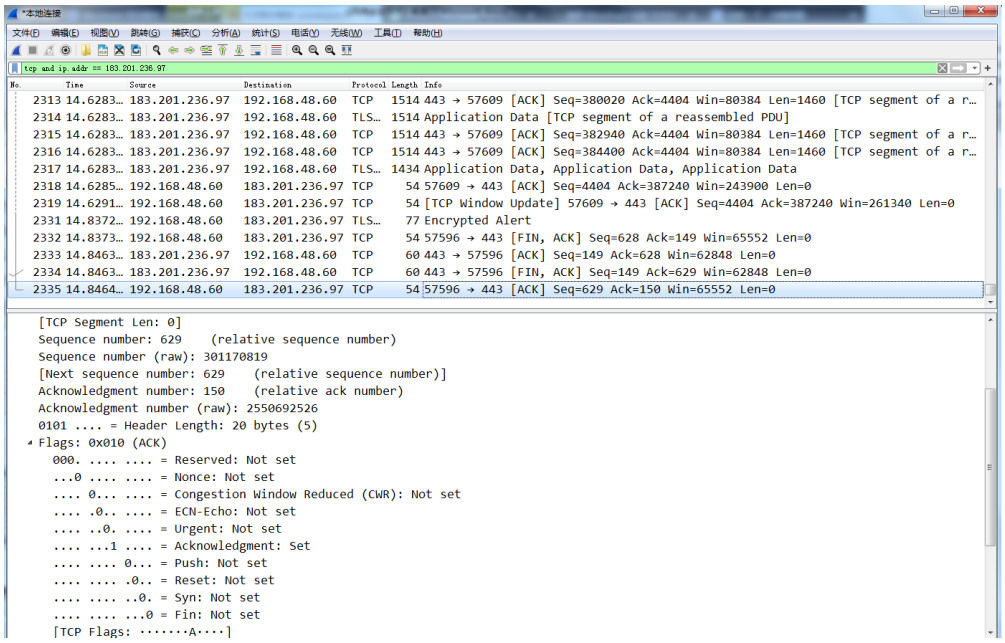


（3）第三次“挥手”数据包：Server 发送同意断开连接数据包，Fin=1，

ACK=1，期待客户端下次发送数据包序号（ack）为 629，如下图所示。



（4）第四次“挥手”数据包：这个数据包的 ACK=1，FIN=0，表示这只是一个单纯的确认数据包，表示客户端已收到服务器端同意断开连接的请求。而 Seq=629，表示客户端发给服务器端序号为 629 之前的数据包已经全部发送完毕，可以释放连接。



（5）为什么需要四次挥手？因为 TCP 是一个全双工通信机制的协议，只有通信双方都关闭的时候才表示这个连接断开了。

技能训练	实验任务详见实验报告。

<table>
<tr><td>课题名称</td><td colspan="5">学习任务 3：访问控制列表 ACL</td></tr>
<tr><td>所属项目</td><td colspan="5">项目三　网络安全协议分析</td></tr>
<tr><td>所属课程</td><td>网络安全技术</td><td>授课时数</td><td>6</td><td>授课地点</td><td>机房</td></tr>
<tr><td>学情分析</td><td colspan="5">1、学生原有知识分析
本课程面向计算机应用技术二年级学生，他们已经具备一些计算机网络基础知识，包括：IP 地址，常用的网络协议等，掌握了 Cisco Packet Tracer 的基本使用方法，能够绘制简单的网络拓扑结构图，为本节实训课的开展奠定了基础。
2、学生认知能力分析
高职学生普遍认知特点为表象性思维较强，对新奇、不断变化的事物有很强的好奇心；但是逻辑思维能力相对较差，在分析解决问题方面存在思维惰性。
3、学生学习能力及学习风格
学生学习总体表现为说过的、讲过的不知道、记不住，只有做过的才能理解，获得新知识和经验的途径倾向于观察和实际动手操作。在教学过程中采用讲授和实训相结合的方式，且通过教师演示、软件模拟增强学生对于访问控制的直观感受。</td></tr>
<tr><td>教学目标</td><td colspan="5">知识目标：
掌握访问列表顺序配置的重要性
掌握扩展访问列表的配置方法
技能目标：
使用 Cisco Packet Tracer 绘制网络拓扑结构图
掌握配置访问控制列表 ACL 的方法</td></tr>
<tr><td>教学重点</td><td colspan="5">掌握配置访问控制列表 ACL 的方法</td></tr>
<tr><td>教学难点</td><td colspan="5">掌握配置访问控制列表 ACL 的方法</td></tr>
<tr><td>教学资源</td><td colspan="5">Cisco Packet Tracer 软件　PPT</td></tr>
<tr><td>教学方法</td><td colspan="5">任务驱动法 讲授法 多媒体辅助教学法</td></tr>
</table>

教学过程	
课前	作业一：预习 Cisco Packet Tracer 的使用方法 作业二：预习 Cisco Packet Tracer 中 PC、交换机、路由器的配置 作业二：发放实验任务
导入新课	某些安全性要求比较高的主机、网络或者应用程序需要进行访问控制，这就需要使用访问控制列表提供操作条件，可以针对目标 IP 地址进行控制，也可以针对某些协议进行控制。今天我们通过 Cisco Packet Tracer 模拟器来制定安全策略，通过指定访问控制列表来检查指定接口上的数据包，并决定是否转发这些数据包。
知识讲解	一、访问控制列表 ACL 的认识 1、访问控制列表(ACL)是一种基于包过滤的访问控制技术，它可以根据设定的条件对接口上的数据包进行过滤，允许其通过或丢弃。访问控制列表被广泛地应用于路由器和三层交换机，借助于访问控制列表，可以有效地控制用户对网络的访问，从而最大程度地保障网络安全。 2、访问控制列表的功能 （1）限制网络流量、提高网络性能。例如，ACL 可以根据数据包的协议，指定这种类型的数据包具有更高的优先级，同等情况下可预先被网络设备处理。 （2）提供对通信流量的控制手段。 （3）提供网络访问的基本安全手段。 （4）在网络设备接口处，决定哪种类型的通信流量被转发、哪种类型的通信流量被阻塞。例如，用户可以允许 E- mail 通信流量被路由，拒绝所有的 Telnet 通信流量。例如，某部门要求只能使用 WWW 这个功能，就可以通过 ACL 实现；又例如，为了某部门的保密性，不允许其访问外网，也不允许外网访问它，就可以通过 ACL 实现。 3、工作原理 （1）当一个数据报进入一个端口，路由器检查这个数据报是否可

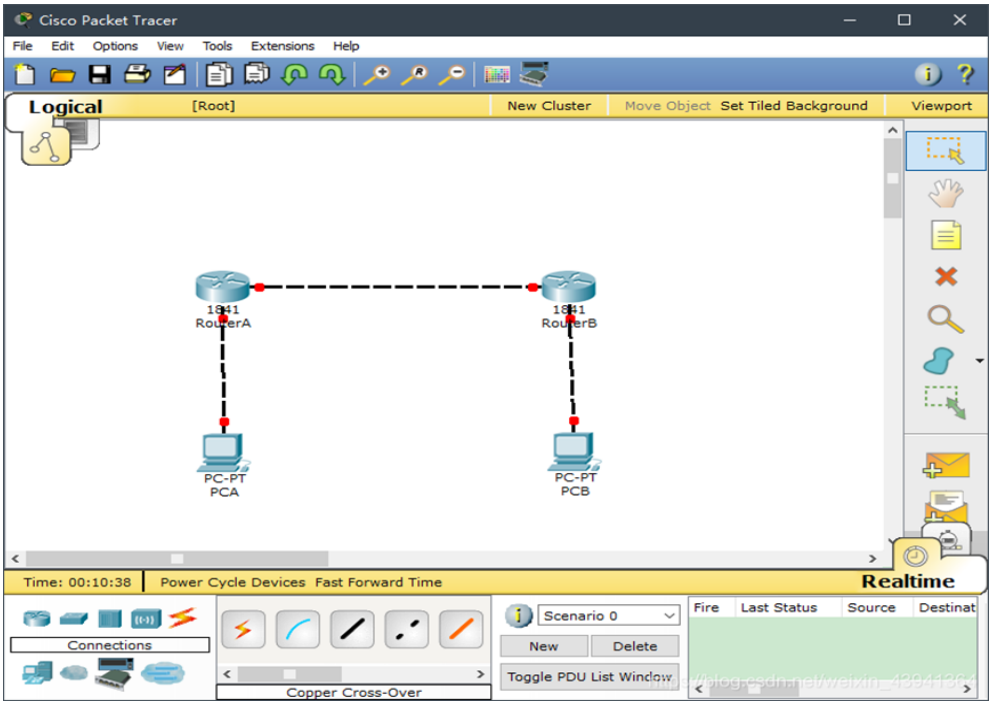
路由。如果是可以路由的，路由器检查这个端口是否有 ACL 控制进入数据报。如果有，根据 ACL 中的条件指令，检查这个数据报。如果数据报是被允许的，就查询路由表，决定数据报的目标端口。

（2）路由器检查目标端口是否存在 ACL 控制流出的数据报。若不存在，这个数据报就直接发送到目标端口。若存在，就再根据 ACL 进行取舍，然后在转发到目的端口。

当 ACL 处理数据包时，一旦数据包与某条 ACL 语句匹配，则会跳过列表中剩余的其他语句，根据该条匹配的语句内容决定允许或者拒绝该数据包。如果数据包内容与 ACL 语句不匹配，那么将依次使用 ACL 列表中的下一条语句测试数据包。该匹配过程会一直继续，直到抵达列表末尾。最后一条隐含的语句适用于不满足之前任何条件的所有数据包。这条最后的测试条件与这些数据包匹配，通常会隐含拒绝一切数据包的指令。此时路由器不会让这些数据进入或送出接口，而是直接丢弃。最后这条语句通常称为隐式的“deny any”语句。由于该语句的存在，所以在 ACL 中应该至少包含一条 permit 语句，否则，默认情况下，ACL 将阻止所有流量。

二、访问控制列表的设计与实现

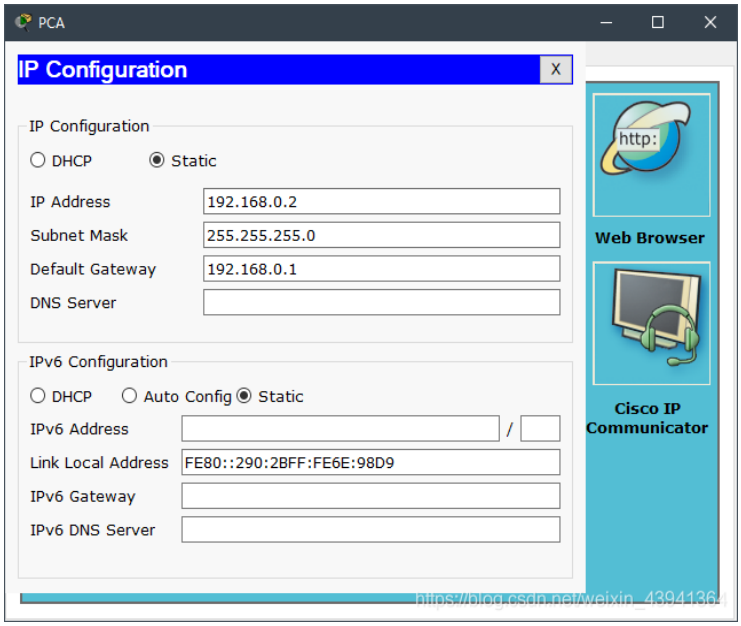
1、新建拓扑结构图，如下图所示。

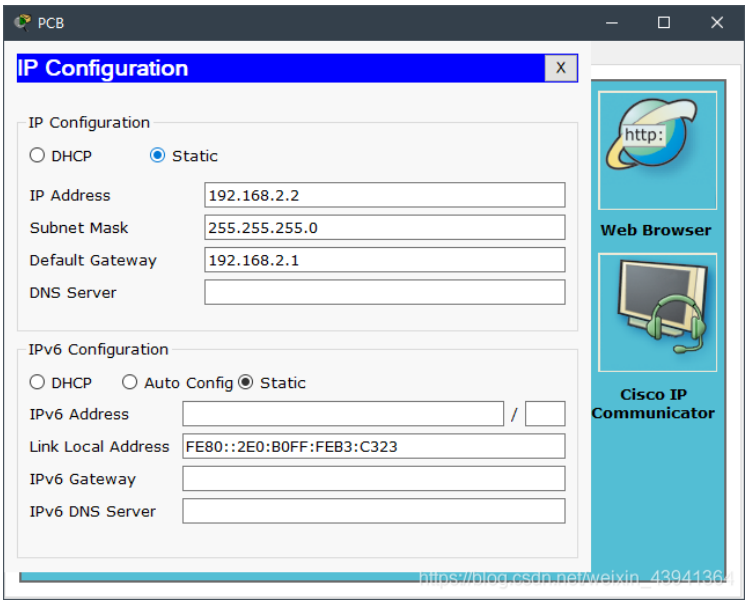


2、拓扑结构图中，各设备的接口 IP 地址配置信息，如下表所示。

设备	IP 地址	
	接口 F0/0	接口 F0/1
Router-A	192.168.0.1/24	192.168.1.1/24
Router-B	192.168.2.1/24	192.168.1.2/24
设备	IP 地址	网关
PC-A	192.168.0.2/24	192.168.0.1
PC-B	192.168.2.2/24	192.168.2.1

3、配置各个设备的名称及 IP 地址并测试连接情况。



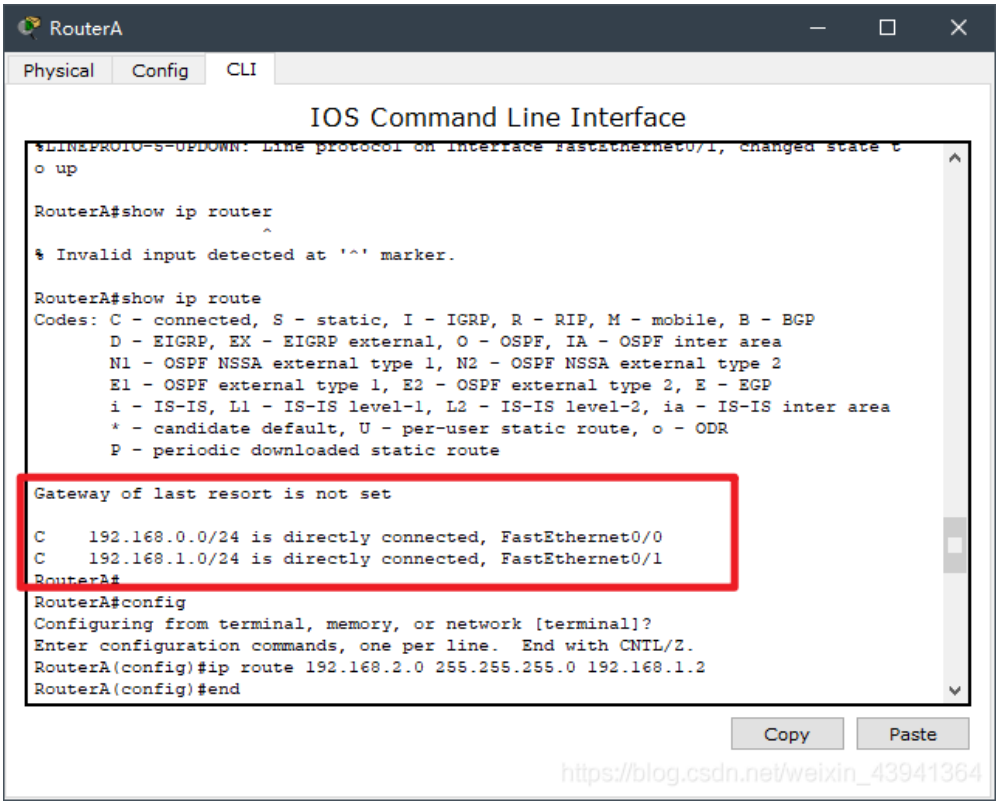


4、分别用 PC-A ping 其它各个设备并记结果。

（1）首先是 ping 路由器 A 的两个接口，结果：都可以 ping 通。

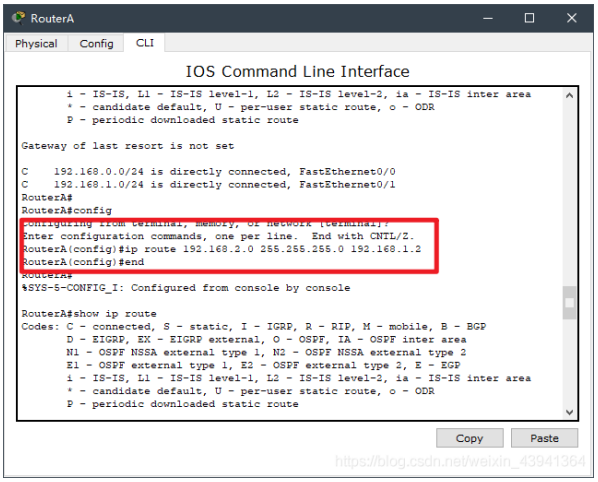
（2）其次是 ping 路由器 B 的两个接口，结果：ping 不通。

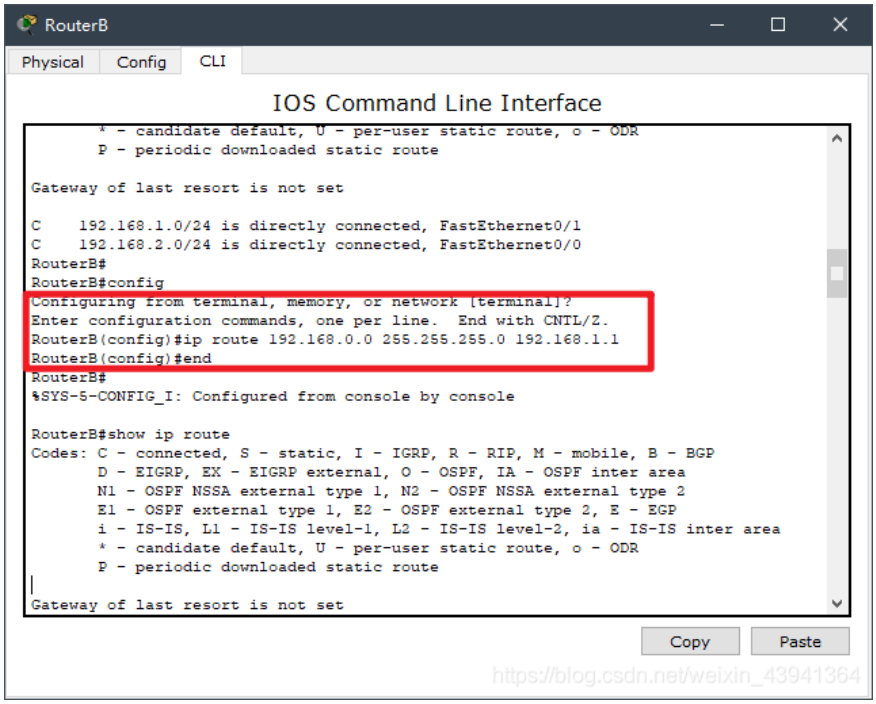
原因：因为路由器只能连接相邻的两个网络，它的路由表中只有和它相邻的两个网络的路由信息，所以一旦跨越两个网络以上就不可达了，可以先看一下现在的路由表：



5、配置静态路由

（1）配置路由器 A 和 B 的路由信息。

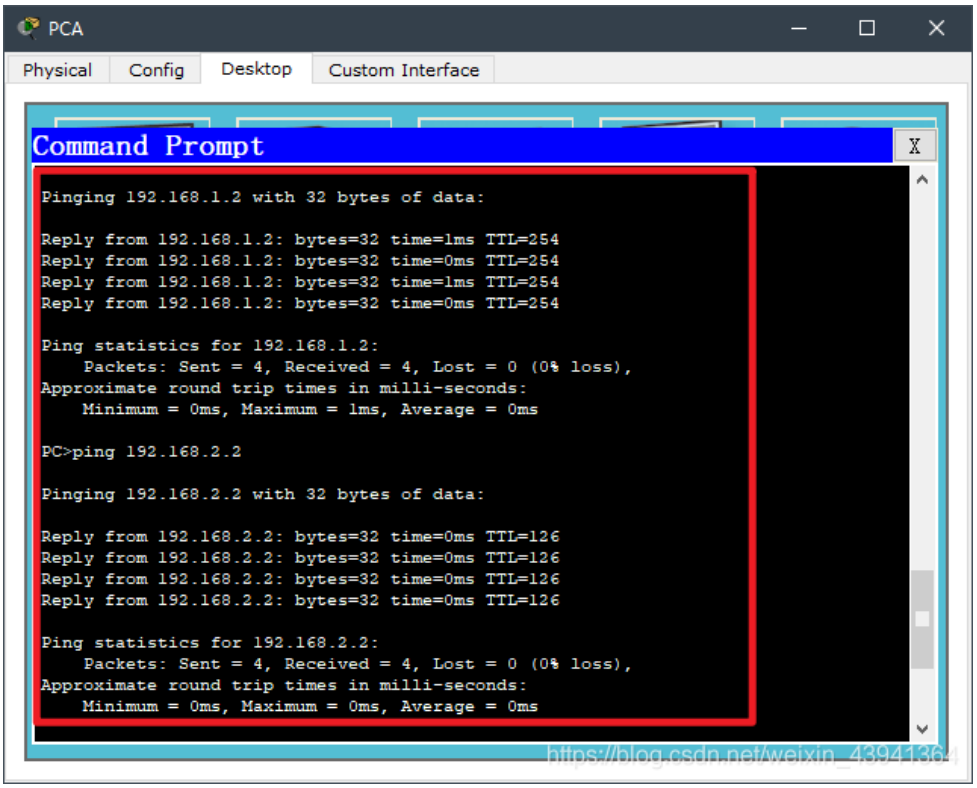




（2）查看路由表信息，命令行输入：show ip route。

（3）发现路由器 A 和 B 都多了一条静态路由记录信息。

6、检查 PC-A 能否与 PC-B 通讯？



7、配置访问控制器列表禁止 PC-A 所在的网段对 PC-B 的访问。

RouterB

Physical Config CLI

IOS Command Line Interface

```
RouterB>en
RouterB#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
RouterB(config)#ip access-list standard 1
RouterB(config-std-nacl)#deny 192.168.0.0 0.0.0.255
RouterB(config-std-nacl)#permit any
RouterB(config-std-nacl)#end
RouterB#
%SYS-5-CONFIG_I: Configured from console by console

RouterB#show run
Building configuration...

Current configuration : 630 bytes
!
version 12.4
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname RouterB
```

Copy Paste

8、验证访问控制列表是否配置成功，命令行输入：show run。

RouterB

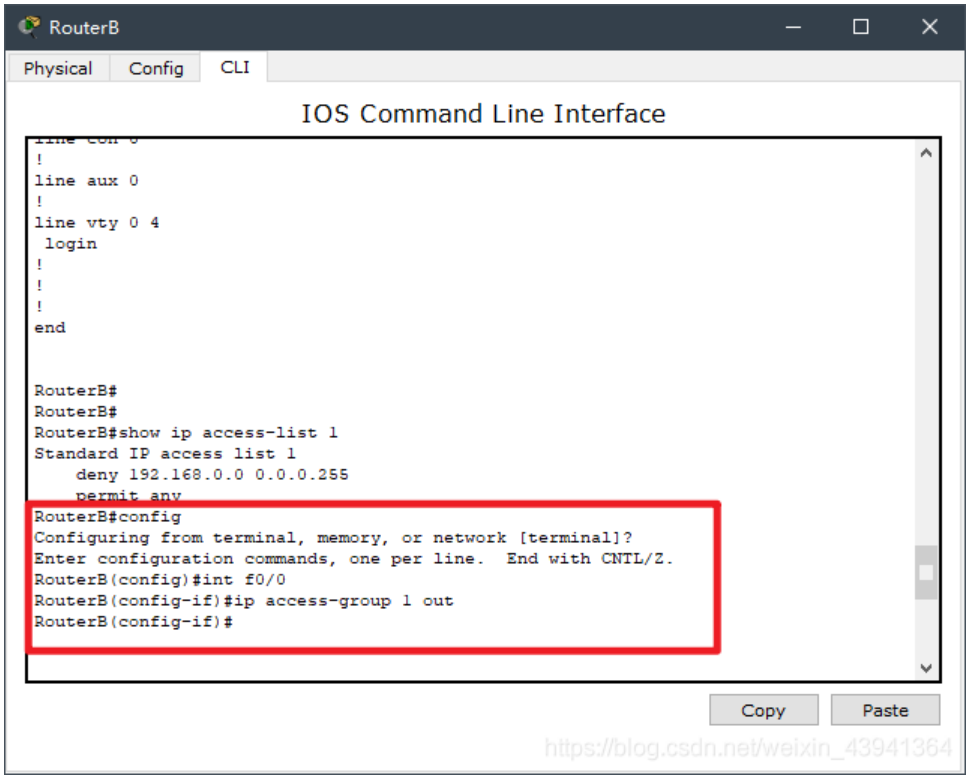
Physical Config CLI

IOS Command Line Interface

```
!
!
interface FastEthernet0/0
 ip address 192.168.2.1 255.255.255.0
 duplex auto
 speed auto
!
interface FastEthernet0/1
 ip address 192.168.1.2 255.255.255.0
 duplex auto
 speed auto
!
interface Vlan1
 no ip address
 shutdown
!
ip classless
ip route 192.168.0.0 255.255.255.0 192.168.1.1
!
!
access-list 1 deny 192.168.0.0 0.0.0.255
access-list 1 permit any
!
!
!
!
```

Copy Paste

9、此时，再用 ping 命令测试 PC-A 和 PC-B 的连通性，发现 PC-A 可以 ping 通 PC-B。因为：仅仅是配置了访问控制列表，但是并没有指定给哪一个端口。



10、ACL 应用于指定接口后，就生效了，即：PC-A　ping 不通 PC-B。

注：取消访问控制列表的命令是 no ip access-group 1 out。

技能训练	实验任务详见实验报告。