实验 22_以太网帧分析实验

学生姓名:林觉凯　　合作同学:无

实验地点:济事楼 330　　实验时间:2024.5.6

【实验目的】

以太网帧(Ethernet frame)是在以太网网络中传输数据的基本单位。它是一个数据包，包含了网络通信所需的各种信息。本实验在学习了以太网协议相关知识的基础上，在 Cisco Packet Tracer 网络仿真软件中观察在帧传输中 MAC 地址的变化情况，同时学习使用了一个新的网络仿真软件 WireShark，在这个软件中我们需要进行抓包并且分析 MAC 帧。

【实验原理】

以太网介绍：

以太网是一种计算机局域网技术。IEEE 组织的 IEEE 802.3 标准制定了以太网的技术标准，它规定了包括物理层的连线、电子信号和介质访问层协议的内容。以太网是目前应用最普遍的局域网技术。

以太网是目前现实世界社会中最普遍的一种计算机网络。以太网有两类：第一类是经典以太网，而第二类是交换式以太网，它们使用了一种称之为交换机的设备连接不同的计算机。

经典以太网是以太网的原始形式，运行速度从 3~10 Mbps 不等；而交换式以太网正是广泛应用的以太网，可运行在 100、1000 和 10000Mbps 那样的高速率，分别以快速以太网、千兆以太网和万兆以太网的形式呈现。

以太网的标准拓扑结构为总线型拓扑，但目前的快速以太网(100BASE-T、1000BASE-T 标准)为了减少冲突，将能提高的网络速度和使用效率最大化，使用交换机来进行网络连接和组织。

如此一来，以太网的拓扑结构就成了星型；但在逻辑上，以太网仍然使用总线型拓扑和 CSMA/CD(Carrier Sense Multiple Access/Collision Detection，即载波多重访问/碰撞侦测)的总线技术。

每一个节点有全球唯一的 48 位地址也就是制造商分配给网卡的 MAC 地址，以保证以太网上所有节点能互相鉴别。由于以太网十分普遍，许多制造商把以太网卡直接集成进计算机主板。

MAC 地址介绍：

MAC 地址也叫物理地址、硬件地址，由网络设备制造商生产时烧录在网卡(Network lnterface Card)的 EPROM(一种闪存芯片，通常可以通过程序擦写)。MAC 地址的长度为 48 位(6 个字节)，通常表示为 12 个 16 进制数，如：00-16-EA-AE-3C-40 就是一个 MAC 地址，其中前 3 个字节，16 进制数 00-16-EA 代表网络硬件制造商的编号，它由 IEEE(电气与电子工程师协会)分配，而后 3 个字节，16 进制数 AE-3C-40 代表该制造商所制造的某个网络产品(如网卡)的系列号。MAC 地址在世界是唯一的。

MAC 地址由网络其前 3 字节表示 OUI(Organizationally Unique Identifier)，是 IEEE 的注册管理机构给不同厂家分配的代码，区分不同的厂家。后 3 字节由厂家自行分配 MAC 地址最高字节(MSB)的低第二位(LSb)表示这个 MAC 地址是全局的还是本地的，即 U/L(Universal/Local)位，如果为 0，表示是全局地址。所有的 OUI 这一位都是 0。MAC 地址最高字节(MSB)的低第一位(LSb)，表示这个 MAC 地址是单播还是多播。0 表示单播。

MAC 数据包格式：

前导码和帧开始符一个帧以 7 个字节的前导码和 1 个字节的帧开始符作为帧的开始。其相应的 16 进制表示为 0x55 0x55 0x55 0x55 0x55 0x55 0x55 0xD5。报头报头包含源地址和目标地址的 MAC 地址，以太类型字段和可选的用于说明 VLAN 成员关系和传输优先级的 IEEE 802.1Q VLAN 标签。

帧校验码：

帧校验码是一个 32 位循环冗余校验码，以便验证帧数据是否被损坏。

MAC 数据包格式：

帧间距：当一个帧发送出去之后，发送方在下次发送帧之前，需要再发送至少 12 个 octet 的空闲线路状态码。

以太帧类型：以太帧有很多种类型。不同类型的帧具有不同的格式和 MTU 值。但在同种物理媒体上都可同时存在。以太网第二版称之为 Ethernet II 帧，DIX 帧，是最常见的帧类型。并通常直接被 IP 协议使用。

Ethernet II：以太 II 帧(也称作 DIX 以太网，是以这个设计的主要成员，DEC,Intel 和 Xerox 的名字命名的。把紧接在目标和源 MAC 地址后面的这个两字

节定义为以太网帧数据类型字段。例如，一个 0x0800 的以太类型说明这个帧包含的是 IPv4 数据报。同样的，一个 0x0806 的以太类型说明这个帧是一个 ARP 帧，0x8100 说明这是一个 IEEE 802.1Q 帧，而 0x86DD 说明这是一个 IPv6 帧。

当这个工业界的标准通过正式的 IEEE 标准化过程后，在 802.3 标准中以太类型字段变成了一个(数据)长度字段。(最初的以太包通过包括他们的帧来确定它们的长度，而不是以一个明确的数值。)但是包的接收层仍需知道如何解析包，因此标准要求将 IEEE802.2 头跟在长度字段后面，定义包的类型。多年之后，802.3x-1997 标准，一个 802.3 标准的后继版本，正式允许两种类型的数据包同时存在。

实际上，两种数据包都被广泛使用，而最初的以太数据包在以太局域网中被广泛应用，因为他的简便和低开销。为了允许一些使用以太 II 版本的数据报和一些使用 802.3 封装的最初版本的数据包能够在同一个以太网段使用，以太类型值必须大于等于 1536(0x0600)。这个值比 802.3 数据包的最大长度 1500byte (0x05DC)要更大。

因此如果这个字段的值大于等于 1536，则这个帧是以太 II 帧，而那个字段是类型字段。否则(小于 1500 而大于 46 字节)，他是一个 IEEE 802.3 帧，而那个字段是长度字段。1500～1536(不包含)的数值未定义。

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】

硬件设备：本人的笔记本电脑

软件设备：Windows 操作系统和 Cisco Packet Tracer 网络仿真软件

【实验步骤】

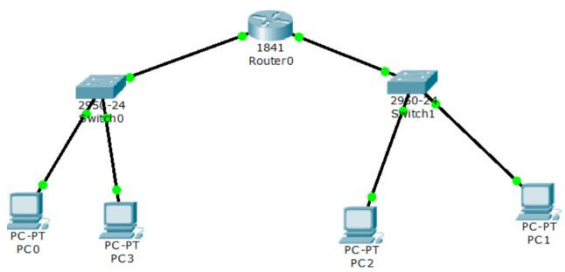
1.首先规划网络地址及拓扑图(如右图所示)；

2.路由器接口 IP 地址配置；

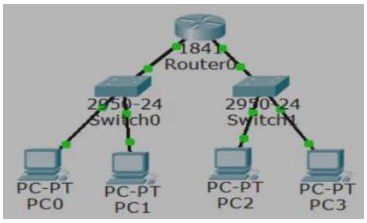
3.配置 DHCP 之前检查 PC 是否存在 IP 地址；

4.在 R0，配置 DHCP；

5.验证各个 PC 的 IP 地址。

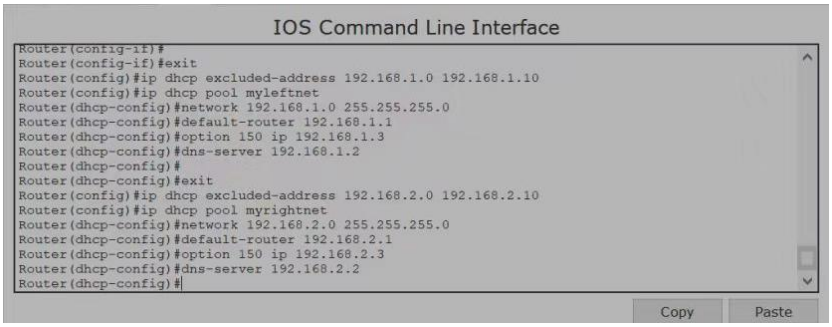


【实验现象】

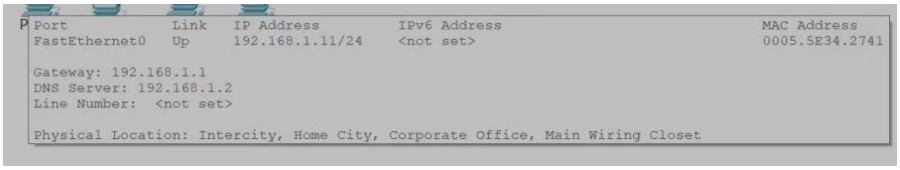


首先规划网络地址及拓扑图,连接线路同时配置好路由器端口。此步骤前几次实验做过多次，这里不再赘述。

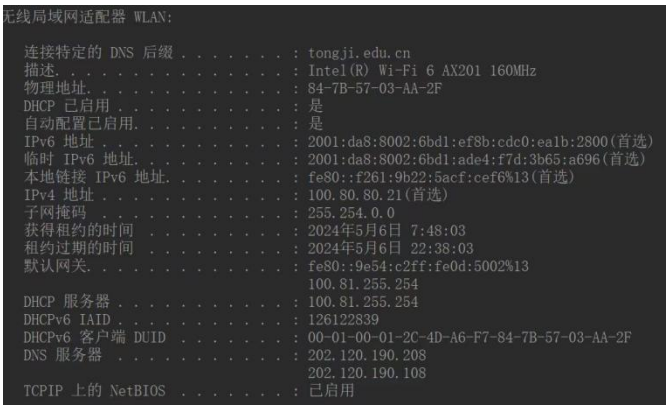
接着完成 R0 的 DHCP 配置。



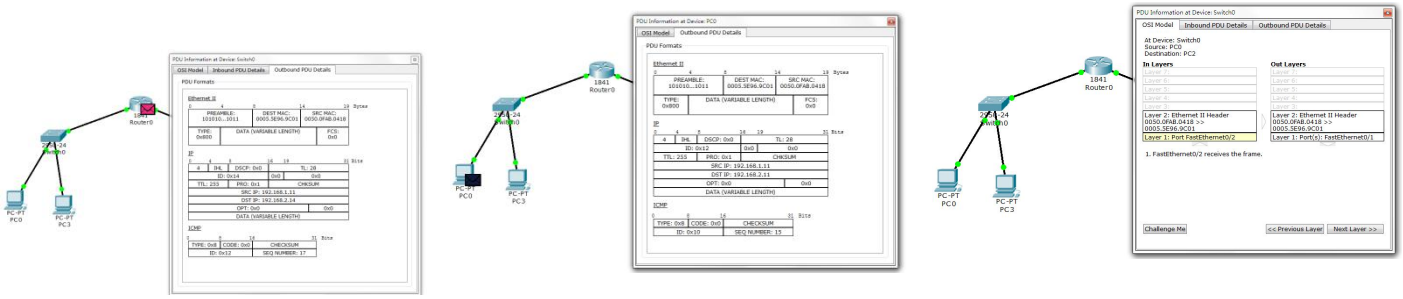
在配置 DHCP 前，我们会发现 PC 的 IP 显示为 not set，在配置好 DHCP 后，PC 的 IP 有被相应的分配。

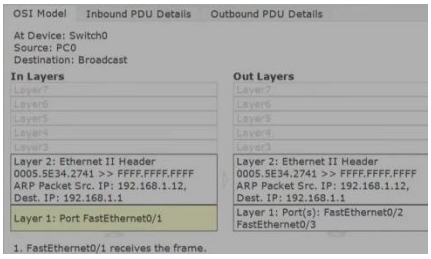


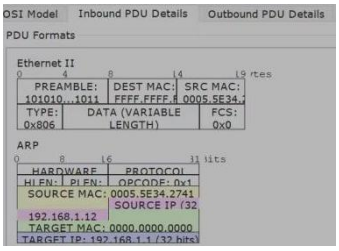
查看本机的 MAC 地址(物理地址)：

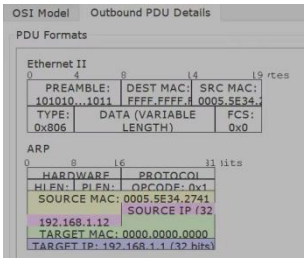


接下来点击模拟 ICMP 包，查看相关数据。例如：



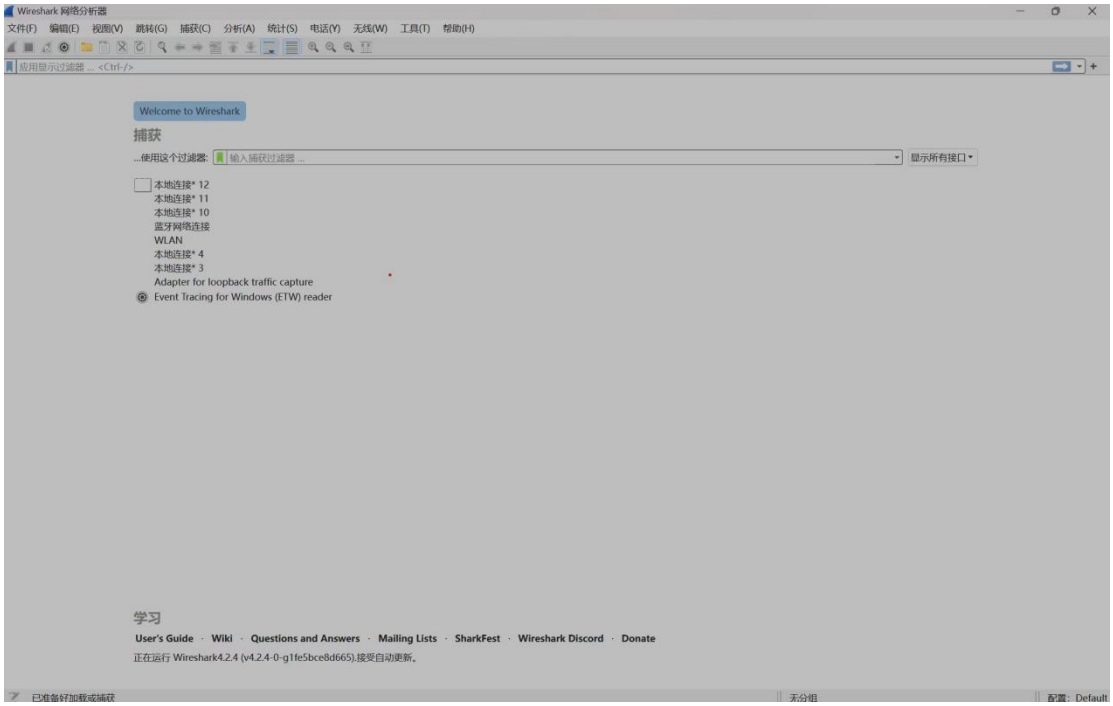




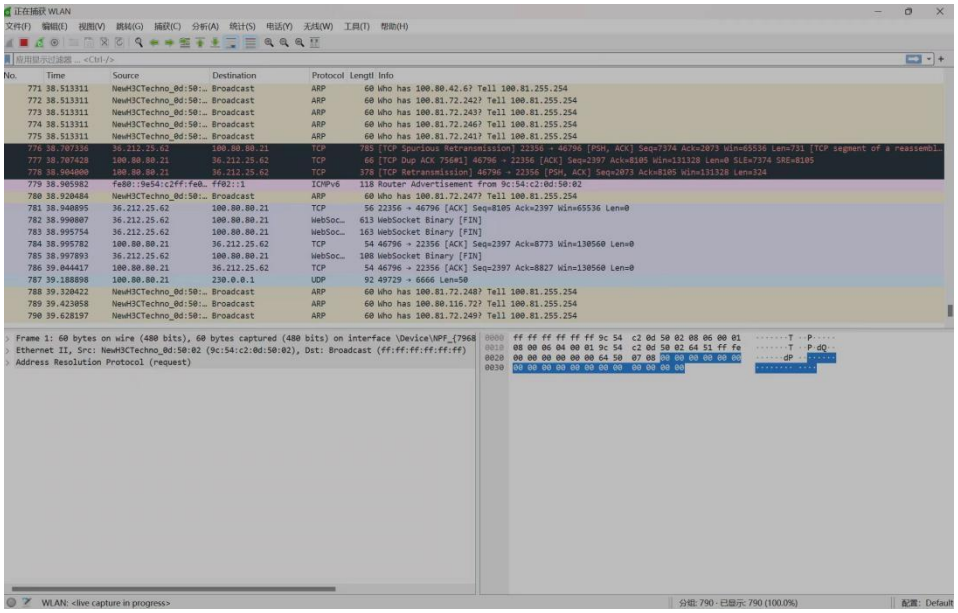


在 PC0 发出 ICMP 帧，发送到交换机。

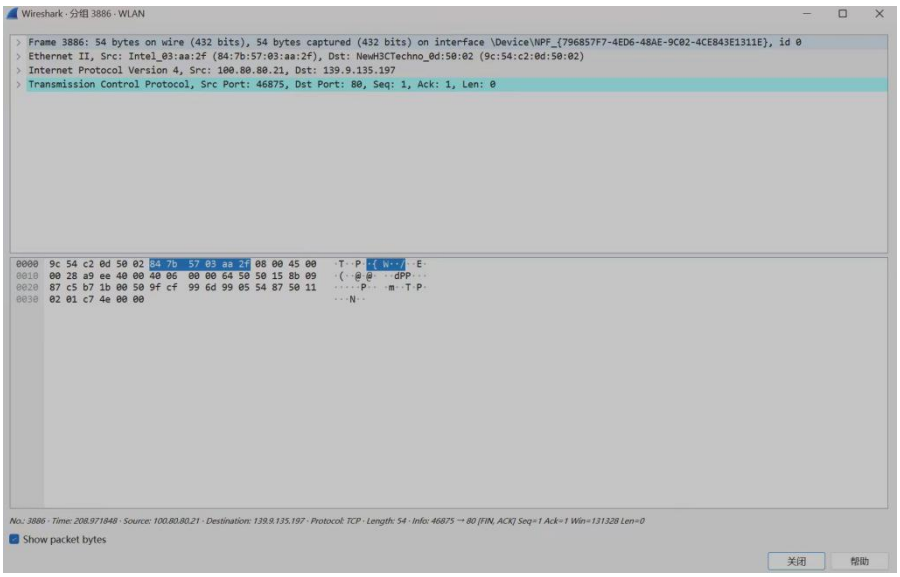
打开 WireShark 软件，准备用 WireShark 抓取 MAC 数据包。



在这个软件里我们可以使用 WireShark 抓包。



在 WireShark 界面中，我们可以选择一条数据包记录，然后点击，便可以显示其详细信息，可以观察到源 MAC 地址和目的 MAC 地址。



在图片中，源 MAC 地址便是 Src:Intel_03:aa:2f(84:7b:57:03:aa:2f),目的 MAC 地址便是 Dst:NewH3CTechno_0d:50:02(9c:54:c2:0d:50:02)。

分析在 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。在 ICMP 数据包的转发过程中，源 MAC 地址通常保持不变，而目标 MAC 地址会根据网络设备的转发规则在每个网络节点进行修改。初始发送时，目标 MAC 地址指向下一个网络节点，如路由器或交换机。每个中间路由器/交换机接收数据包后，根据其路由表中的下一跳信息更新目标 MAC 地址，以指示下一个网络节点的地址。这个过程一直持续到数据包到达最终目标主机。

【分析讨论】

本次实验的过程较为复杂，我详细了解了以太网这个局域网技术及其分类，并且对于帧的格式有了进一步深入的理解。与此同时，实验让我对 ping 命令有了更加深入的理解和思考，这个命令对交换器和路由器有着复杂的帧的转发。本次实验还让我初步接触了 WireShark 又一个网络仿真软件，它生动形象地展示了以太网帧的格式，让我的学习更加方便快速。

MAC 是这次实验的重点之一，我在课后查找学习了关于 MAC 的其他知识。MAC(Media Access Control)数据包字段通常指的是以太网数据包中的 MAC 地址字段。以太网是一种常见的局域网技术，它使用 MAC 地址来唯一标识网络中的

设备。以下是以太网数据包中常见的字段及其含义：

目标 MAC 地址(Destination MAC Address)：这是数据包要发送到的设备的 MAC 地址。接收设备会检查这个字段，如果它与自己的 MAC 地址匹配，则接收数据包。

源 MAC 地址(Source MAC Address)：这是发送数据包的设备的 MAC 地址。这个字段用于告诉接收设备数据包的来源。

类型/长度字段(Type/Length)：在以太网 II 格式中，这个字段指示了数据包中的数据类型(例如 IPv4、IPv6 等)。在 IEEE 802.3 格式中，这个字段表示数据帧的长度。

数据字段(Data)：这是实际的数据部分，可能是从网络层(如 IP 层)传递下来的数据。

帧校验序列(FCS，Frame Check Sequence)：这是一个用于检测数据传输过程中是否发生了错误的字段。接收设备会使用这个字段来验证数据包的完整性。

以上参数数据我们均可以在实验中通过 WireShark 抓包显示分析。

解读 MAC 数据包字段通常涉及了解每个字段的含义以及它们在数据传输过程中的作用。通过分析这些字段，网络设备可以正确地路由和传递数据包，确保数据的可靠性和完整性。

实验 23_IP 数据包分析实验

学生姓名:林觉凯　　合作同学:无

实验地点:济事楼 330　　实验时间:2024.5.6

【实验目的】

IP 数据包(Internet Protocol packet)是在网络层(第三层)使用的基本数据单位，用于在网络中传输数据。本实验通过进行 IP 数据包的分析，我们需要了解 IP 协议的工作原理，并且在网络软件中分析 IP 报文。通过本次实验，有助于我们更好地了解 IP 数据包的内容和传输过程。

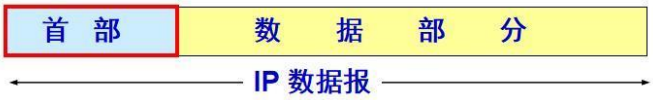
【实验原理】

IP 协议：

1. IP 数据报文格式总览

IP 协议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 IP 层对数据报的封装与拆封来实现的。IP 数据报的格式分为报头区和数据区两大部分，其中报头区是为了正确传输高层数据而加的各种控制信息，数据区包括高层协议需要传输的数据。

一个 IP 数据报由首部和数据两部分组成。



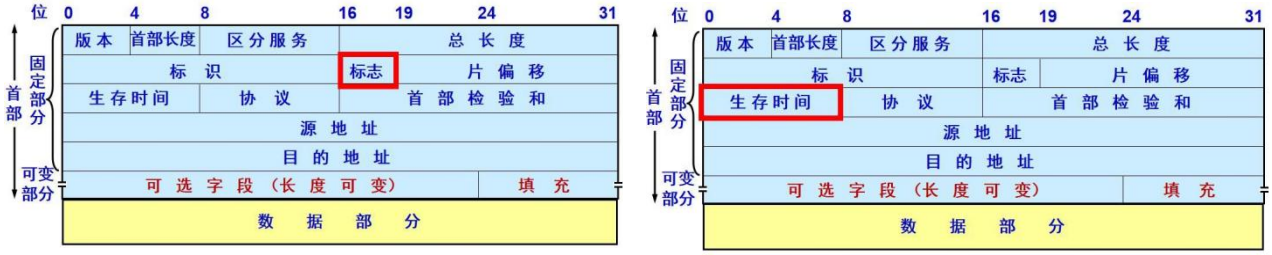
2.头部：头部的前一部分是固定长度，共 20 字节，是所有 IP 数据报必须具有的。在首部的固定部分的后面是一些可选字段，其长度是可变的。

3. IP 数据报首部的固定部分中的各字段版本——占 4 位，指 IP 协议的版本。目前的 IP 协议版本号为 4 (即 IPv4)。IP 数据报首部的固定部分中的各字段首部长度——占 4 位，可表示的最大数值是 15 个单位(一个单位为 4 字节)，因此 IP 的首部长度的最大值是 60。

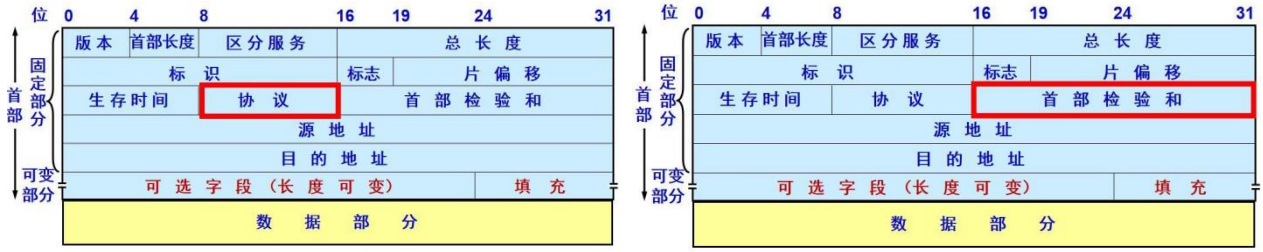
IP 数据报首部的固定部分中的各字段区分服务——占 8 位，用来获得更好的服务。在旧标准中叫做服务类型，但实际上一直未被使用过。 IP 数据报首部的固定部分中的各字段总长度——占 16 位，指首部和数据之和的长度，单位为字节，因此数据报的最大长度为 65535 字节。总长度必须不超过最大传送单元 MTU。

IP 数据报首部的固定部分中的各字段标识(identification) ——占 16 位，它是一个计数器，用来产生 IP 数据报的标识。IP 数据报首部的固定部分中的各字段标志(flag) ——占 3 位，目前只有前两位有意义。标志字段的最低位是 MF (More ragment)。MF = 1 表示后面“还有分片”。MF = 0 表示最后一个分片。 标志字段中间的一位是 DF (Don’t Fragment) 。只有当 DF = 0 时才允许分片。

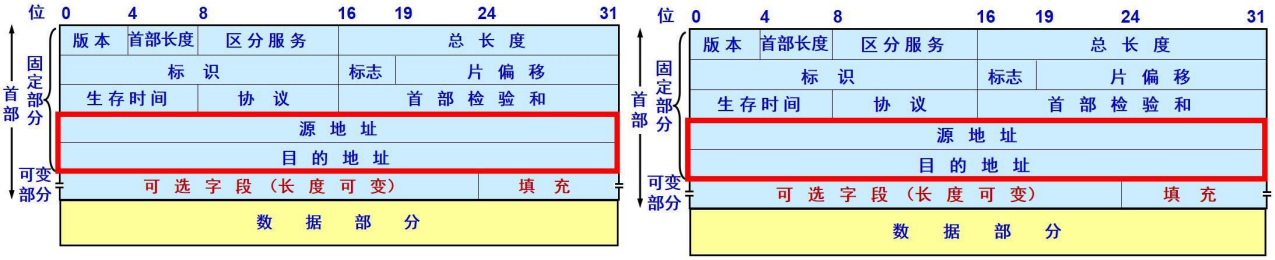
IP 数据报首部的固定部分中的各字段片偏移—— 占 13 位，指出：较长的分组在分片后某片在原分组中的相对位置。片偏移以 8 个字节为偏移单位。IP 数据报首部的固定部分中的各字段生存时间——占 8 位，记为 TTL (Time To Live)，指示数据报在网络中可通过的路由器数的最大值。



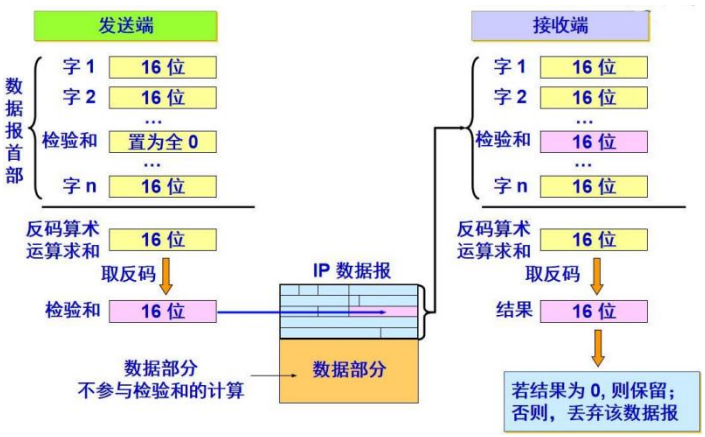
IP 数据报首部的固定部分中的各字段协议——占 8 位，指出此数据报携带的数据使用何种协议，以便目的主机的 IP 层将数据部分上交给那个处理过程。 IP 数据报首部的固定部分中的各字段首部检验和——占 16 位，只检验数据报的首部，不检验数据部分。这里不采 CRC 检验码而采用简单的计算方法。IP 数据报首部检验和的计算采用 16 位二进制反码求和算法。



IP 数据报首部的固定部分中的各字段源地址和目的地址都各占 4 字节。IP 数据报首部的固定部分中的各字段 IP 数据报首部的可变部分 IP 首部的可变部分就是一个选项字段，用来支持排错、测量以及安全等措施，内容很丰富。选项字段的长度可变，从 1 个字节到 40 个字节不等，取决于所选择的项目。

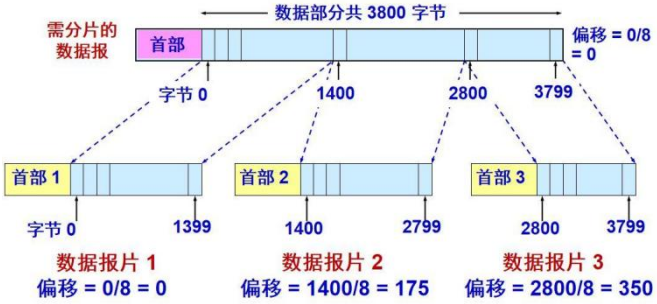


4. IP 数据报首部校验：IP 数据报首部检验和的计算采用 16 位二进制反码求和算法。



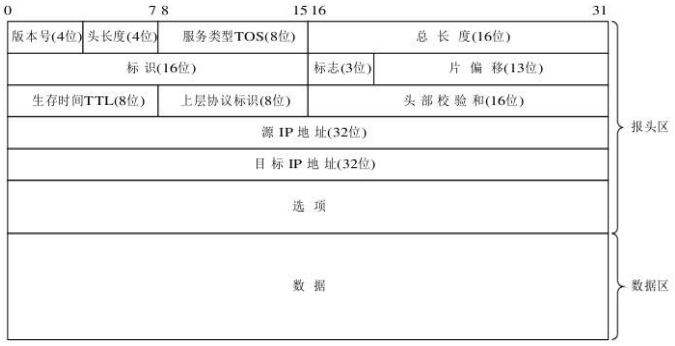
5. IP 数据报分段：给出一数据报的总长度为 3820 字节，其数据部分的长度为 3800 字节(使用固定首部)，需要分片为长度不超过 1420 字节的数据报片。

(1)因固定首部长度为 20 字节，因此每个数据报片的数据部分长度不能超过 1400 字节。(2)于是分为 3 个数据报片，其数据部分的长度分别为 1400、1400 和 1000 字节。(3)原始数据报首部被复制为各数据报片的首部，但必须修改有关字段的值(如标志字段)。



	总长度	标识	MF	DF	片偏移
原始数据报	3820	12345	0	0	0
数据报片1	1420	12345	1	0	0
数据报片2	1420	12345	1	0	175
数据报片3	1020	12345	0	0	350

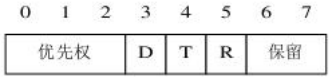
6. IP 数据报文格式传输：注意，下图表示的数据，最高位在左边，记为 0 位；最低位在右边，记为 31 位。在网络中传输数据时，先传输 0~7 位，其次是 8~15 位，然后传输 16~23 位，最后传输 24~31 位。



7. IP 数据报文上层协议：

十进制编号	协 议	说 明
0	无	保留
1	ICMP	网际控制报文协议
2	IGMP	网际组管理协议
3	GGP	网关—网关协议
4	无	未分配
5	ST	流
6	TCP	传输控制协议
8	EGP	外部网关协议
9	IGP	内部网关协议
11	NVP	网络声音协议
17	UDP	用户数据报协议

8. IP 数据报文的 TOS：服务类型(TOS、type of service)：占用 8 位二进制位，用于规定本数据报的处理方式。服务类型字段的 8 位分成了 5 个子域：



(1)—优先权(0-7)数越大，表示该数据报优先权越高。网络中路由器可以使用优先权进行拥塞控制，如当网络发生拥塞时可以根据数据报的优先权来决定数据报的取舍。(2)—短延迟位 D(Delay)：该位置 1 时，数据报请求以短延迟信道传输，0 表示正常延时。(3)—高吞吐量位 T(Throughput)：该位置 1 时，数据报请求以高吞吐量信道传输，0 表示普通。(4)—高可靠位 R(Reliability)：该位置 1 时，数据报请求以高可靠性信道传输，0 表示普通。(5)—保留位。

目前在 Internet 中使用的 TCP/IP 协议大多数情况下网络并未对 TOS 进行处理，但在实际编程时，有专门的函数来设置该字段的各域。一些重要的网际应用协议中都设置了建议使用的 TOS 值：

应用程序	短延迟位D	高吞吐量位T	高可靠性位	低成本位	十六进制值	特性
Telnet	1	0	0	0	0x10	短延迟
FTP控制	1	0	0	0	0x10	短延迟
FTP数据	0	1	0	0	0x08	高吞吐量
TFTP	1	0	0	0	0x10	短延迟
SMTP命令	1	0	0	0	0x10	短延迟
SMTP数据	0	1	0	0	0x08	高吞吐量
DNS UDP查询	1	0	0	0	0x10	短延迟
DNS TCP查询	0	0	0	0	0x00	普通
DNS 区域传输	0	1	0	0	0x08	高吞吐量
ICMP差错	0	0	0	0	0x00	普通
ICMP查询	0	0	0	0	0x00	普通
SNMP	0	0	1	0	0x04	高可靠性
IGP	0	0	1	0	0x04	高可靠性
NNTP	0	0	0	1	0x02	低成本

9.最大传输单元：

IP 数据报在互联网上传输时，可能要经过多个物理网络才能从源端传输到目的端。不同的网络由于链路层和介质的物理特性不同，因此在进行数据传输时，对数据帧的最大长度都有一个限制，这个限制值即最大传输单元 MTU(Maximum Transmission Unit).同一个网络上的两台主机之间通信时，该网络的 MTU 值是确定的，不存在分片问题。分片问题一般只存在于具有不同 MTU 值的互联网中。

由于现在互联网主要使用路由器进行网络连接，因此分片工作通常由路

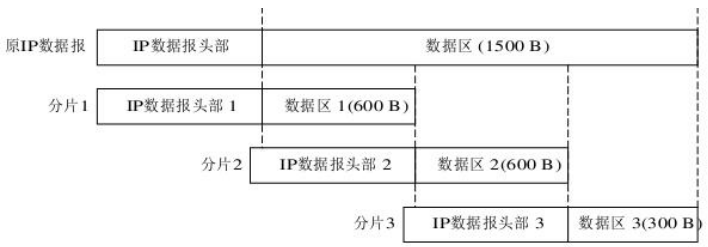
由器负责。当两台主机之间的通信要通过多个具有不同 MTU 值的网络时，MTU 的瓶颈是通信路径上最小的 MTU 值，它被称为路径 MTU。由于路由选择不一定是对称的(从 A 到 B 的路由可能与从 B 到 A 的路由不同)，因此，路径 MTU 在两个方向上不一定是一致的，下表是几种常用网络的 MTU 值：

网 络 名 称	MTU(单位：字节)
以太网	1500
IEEE802.3/802.2	1492
FDDI	4352
ATM(信元)	48
X.25	576
点到点(低延时)	296
令牌环网(IBM 16 MB/s)	17 914
令牌环网(IEEE802.5 IBM 16 MB/s)	4464

10.分片：

把一个数据报为了适合网络传输而分成多个数据报的过程称为分片，被分片后的各个 IP 数据报可能经过不同的路径到达目标主机。一个 IP 数据报在传输过程中可能被分片，也可能不被分片。如果被分片，分片后的 IP 数据报和原来没有分片的 IP 数据报结构是相同的，即也是由 IP 头部和 IP 数据区两个部分组成：分片后的 IP 数据报，数据区是原 IP 数据报数据区的一个连续部分，头部是原 IP 数据报头部的复制，但与原来未分片的 IP 数据报头部有两点主要不同：标志和片偏移：

片偏移：IP 数据报被分片后，各片数据区在原来 IP 数据区中的位置用 13 位片偏移来表示。上图中分片 1 的偏移为 0；分片 2 的偏移为 600；分片 3 的偏移为 1200 实际在 IP 地址中,由于偏移是以 8 个字节为单位进行计算的,因而在 IP 数据报中分片 1 的偏移是 0；分片 2 的偏移是 75；分片 3 的偏移是 150。



11.接收组包：

重组：

当分了片的 IP 数据报到达最终目标主机时，目标主机对各分片进行组装，恢复成源主机发送时的 IP 数据报，这个过程叫做 IP 数据报的重组。在 IP 数据报头部中，标识用 16 位二进制数表示，它唯一地标识主机发送的每一份数据报。在一个数据报被分片时，每个分片仅把数据报“标识”字段的值原样复制一份，所以一个数据报的所有分片具有相同的标识。目标端主机重组数据报的原理是：(1)—根据“标识”字段可以确定收到的分片属于原来哪个 IP 数据报；(2)—根据“标志”字段的“片未完 MF”子字段可以确定分片是不是最后一个分片；(3)—根据“偏移量”字段可以确定分片在原数据报中的位置。

12. IP 数据报选项：

IP 数据报“选项”主要有两大功能：

(1)用来实现对数据报传输过程中的控制，如规定数据报要经过的路由。

(2)进行网络测试，如一个数据报传输过程中经过了哪些路由器。IP“选项“域共分为四大类，每类分为若干个选项，每个选项有确定的编号：

选项类	用　途	选项号	长度	功　　能
0 类	数据报或网络控制	0	—	IP 数据报头中的任选项域结束
		1	—	无操作
		2	11 字节	安全和处理限制(用于军事领域，详细内容参见 RFC 1108[Kent 1991])
		3	可变	设置宽松源路由选择
		7	可变	记录数据报经过的路由
		9	可变	设置严格源路由选择
1 类	未使用			
2 类	调试与测量		可变	记录 Internet 时戳
3 类	未使用			

IP 数据报“选项”由三个部分组成：选项码、选项长度和选项数据。选项码和选项长度各占一个字节，中，选项长度用于确定整个选项部分的长度；选项码又分为复制、选项类和选项号：复制：占一位，用来控制一个带有选项的 IP 数据报被分片后对选项的处理方式。该位置 1 时将选项复制到所有分片中；置 0 时将选项仅复制到第一个分片中。选项类和选项号用于确定该选项是哪类选项中的哪个选项，其实就是确定该选项的功能。

源路由选择：是指 IP 数据报在互联网中传输时，所经过的路由是由发出 IP 数据报的源主机指定的，以区别于数据报在互联网中传输时由路由器的 IP 层自动寻径所得到的路由。通过设置源路由选择选项，可以测试网络中指定路由的连通性，以使数据报绕开出错的网络，也可用于测试特定网络的吞吐量。源路由选择可分为两类：严格源路由选择和宽松源路由选择。

(1)—严格源路由选择有发送端规定 IP 数据报必须经过的路径上的每一个路由器，相邻路由器之间不得有中间路由器，并且所经过的路由器的顺序不可更改。如果一个路由器发送源路由所指定的下一个路由器不在其直接连接的网络上，那么它就返回一个“源路由失败”的ICMP差错报文。严格源路由选择选项格式如下：

1字节	1字节	1字节	4字节	4字节	4字节		4字节
选项码	选项长度	指针	第1站IP地址	第2站IP地址	第3站IP地址	…	第9站IP地址

(2)—宽松源路由选择：由发送方指明一个数据报经过的 IP 地址清单，但是在数据报传输的路径上，在选项中指定的两个 IP 地址之间可以有其他 IP 地址的路由器。格式与严格的相同，只是选项码字段值为 0x83。

记录路由：通过设置记录路由选项，IP 数据报就可以记录数据报从源主机传输到目标主机时，所经过路径上的各个路由器的 IP 地址。记录路由选项的数据格式和严格源路由选择格式相同，但选项码字段值为 0x87，指针初值为 4，指向存放第一个 IP 地址的位置。每个路由器的 IP 地址存入选项的数据区中，指针字段的值也随着增加(从 4 开始到 8，12，16，最大到 36)，它始终指向下一个存放 IP 地址的位置。当记录了 9 个 IP 地址后，指针字段的值为 40，表示数据区已满。

记录时间戳：就是 IP 数据报每经过一个路由器都记下它的 IP 地址和时间。时间戳中的时间以 ms 为单位，时间戳取值一般为格林威治时间(UT，Universal Time)自午夜开始计时的毫秒数时间戳选项格式如下：

1字节	1字节	1字节	4位	4位	4字节	4字节	4字节	4字节	
选项码	选项长度	指针	溢出	标志	第1站IP地址	第1时间戳	第2站IP地址	第2时间戳	…

时间戳选项的选项码是 0x44。选项长度表示选项的总长度(一般为 36 或 40)，指针指向下一个可用空间的指针(值为 5、9、13 等)。

记录时间戳“溢出 OF”字段表示因时间戳选项数据区空间

不够而未能记录下来的时间戳个数；“标志 FL”字段用于控制时间戳选项的格

式，取值如下：

标志字段值	含　义
0	只记录时间戳，不记录 IP 地址，即在图 2-15 所示的格式中去掉 IP 地址项，只记录每台路由器的时间戳。由于没有 IP 地址做参考，所以用途有限
1	记录数据报通过路径时每台路由器的 IP 地址和时间戳。在选项列表中只有存放 4 对 IP 地址和时间戳的空间。其格式与图 2-15 所示的格式一致
3	发送端对选项列表进行初始化，存放了 4 个 IP 地址和 4 个取值为 0 的时间戳值。只有当列表中的下一个 IP 地址与当前路由器地址相匹配时，才记录它的时间戳。这种方式用途较广

【实验设备】

硬件设备：济事楼 330 机房电脑和本人的笔记本电脑

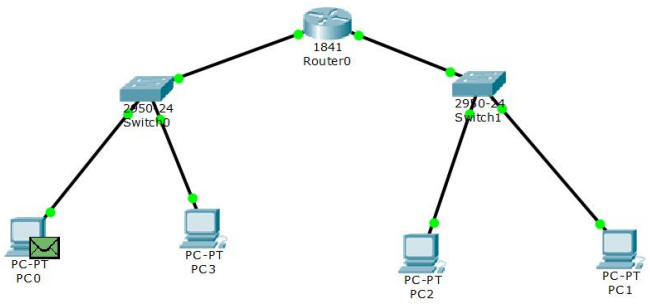
软件设备：Windows 操作系统和 Cisco Packet Tracer 网络仿真软件

【实验步骤】

1.首先规划网络地址及拓扑图(如下图所示)

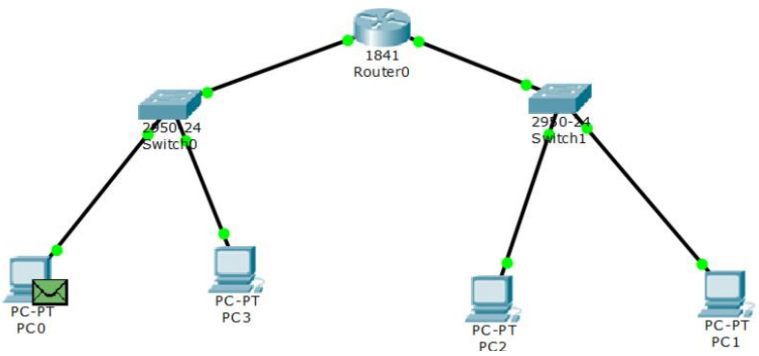
2.设置 WEB 服务器；

3.打开 PC0 浏览器，输入配置 Web 服务器的 IP 地址，产生 IP 数据报文。

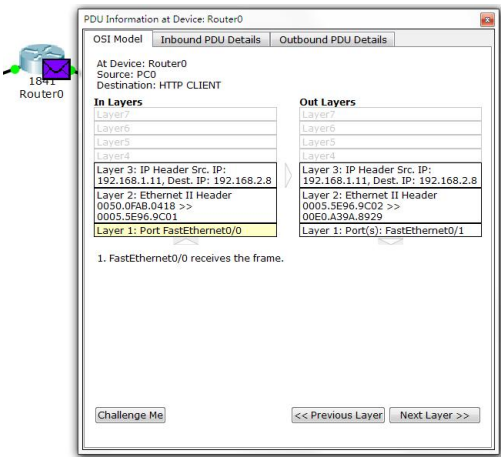


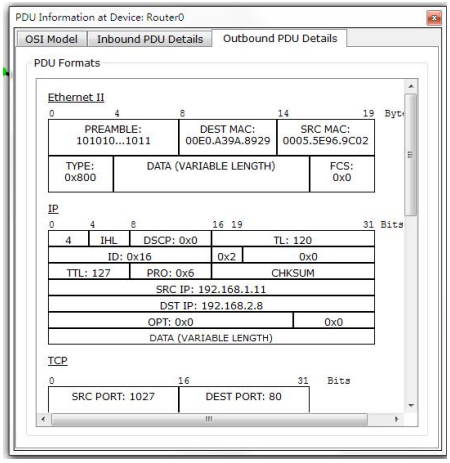
【实验现象】

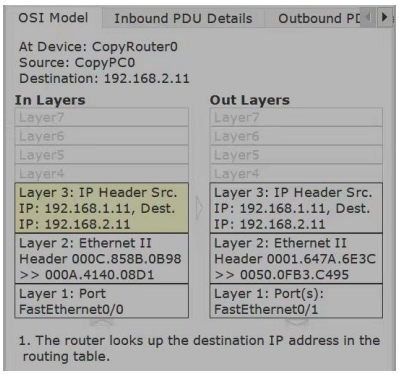
首先，完成网络结构图的连接。并且设置 WEB 服务器；打开 PC0 浏览器，输入配置 Web 服务器的 IP 地址，产生 IP 数据报文。

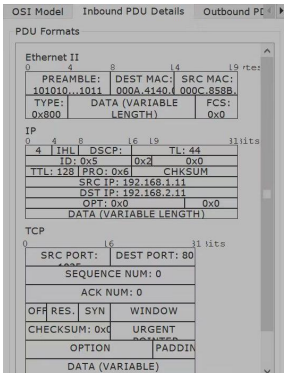


接下来使用 Packet Tracer 分析报文，分析路由器报文：

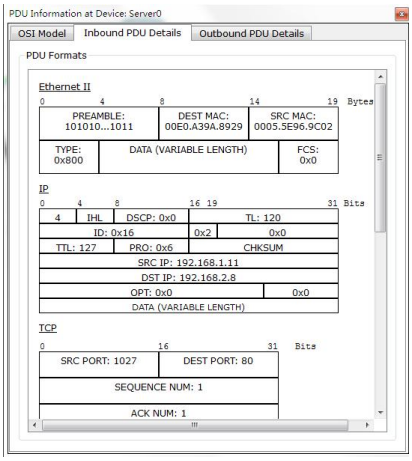


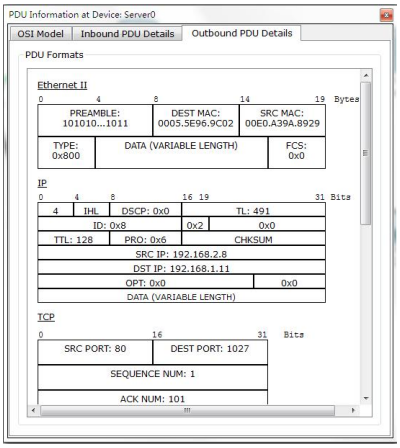


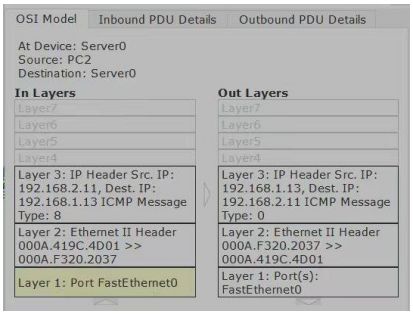


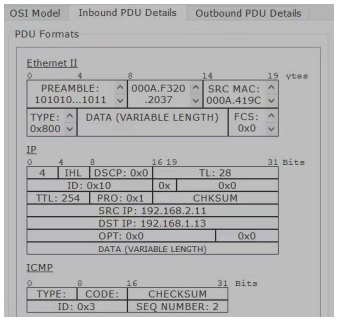


查看服务器报文：

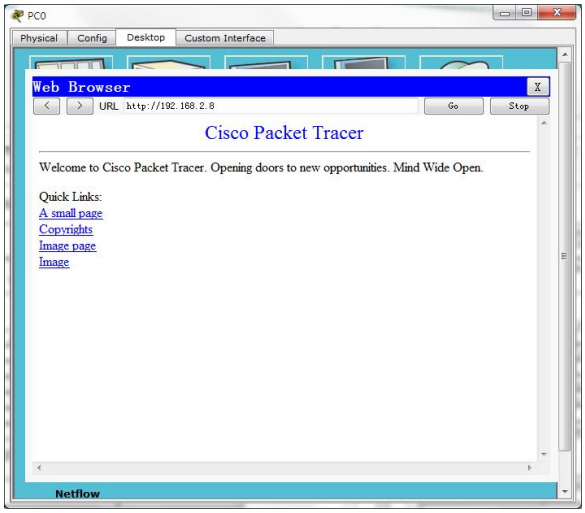




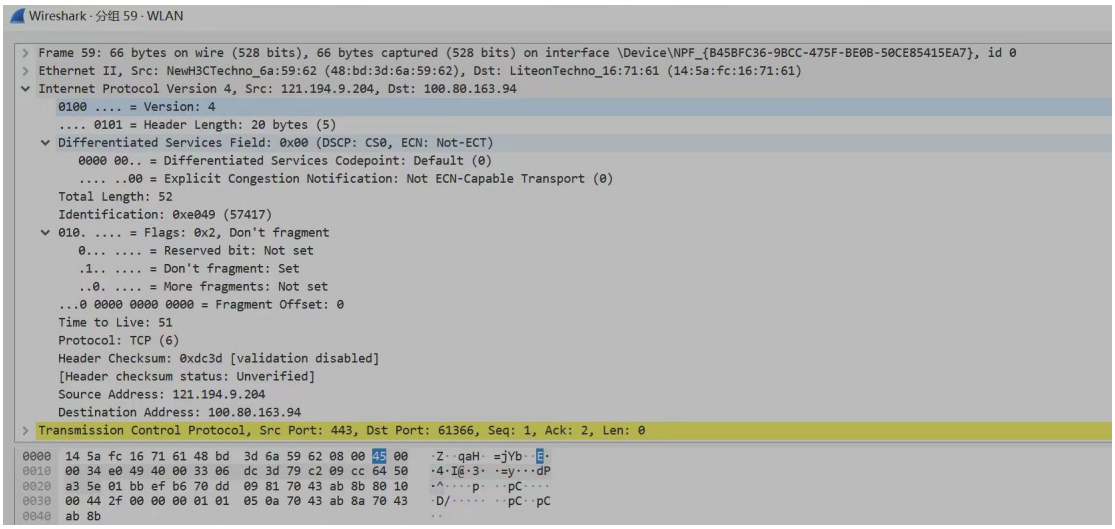




PC0 WEB Browser:



使用 WireShark IP 报文抓取 IP 数据包分析。



1.版本号(Version)**:4(IPv4)

2.头部长度(Header Length):5 即 20 字节(因为 5 乘以 4 字节是 20 字节)

3.区分服务(Differentiated Services):00 00 (通常用于 QoS，但这里为默认值)

4.总长度(Total Length):00 34 e0 (大端序表示的十进制值是 13,120 字节)

5.标识(Identification):49 40 (以十进制表示是 18,048)

6.标记(Flags):00 (前三位，标志位)

7.片偏移(Fragment Offset): 33 06 (13 位，以 8 字节为单位)

8.生存时间(Time to Live): dc (以十进制表示是 220)

9.协议(Protocol):3d (IPv4 协议号，这里可能是 ICMPv6)

10.头部校验和(Header Checksum):79 c2 (以十进制表示是 31,266)

11.源地址(Source Address):09 cc 64 50 (IPv4 地址)

12.目标地址(Destination Address): a3 5e (IPv4 地址)

【分析讨论】

通过本次 IP 数据包分析实验，使我我充分地了解到 IP 数据包为网络层的单元；通过 Wireshark 抓包分析实验，我更好地理解了在网络中数据包传输的行为和传输路径。同时，让我更加熟练地使用了 Wireshark 虚拟网络。

要分析 IP 数据包，我们需要查看其各个字段以及它们的含义：

版本(Version): 4 位，指示 IP 协议的版本号。IPv4 的版本号为 4。

头部长度(Header Length): 4 位，表示 IP 头部的长度，以 32 位字(4 字节)为单位。最小长度为 5 个字，最大长度为 15 个字(即 60 个字节)。

区分服务(Differentiated Services): 8 位，用于指示数据包的服务类型、优先级或 QoS。

总长度(Total Length): 16 位，指示整个 IP 数据包的长度，包括头部和数据部分。最大长度为 65535 字节。

标识(Identification): 16 位，用于标识数据包的唯一性，通常在数据包需要分片时使用。

标志(Flags): 3 位，用于控制 IP 分片。

片偏移(Fragment Offset): 13 位，指示分片相对于原始数据包的位置。

生存时间(Time to Live): 8 位，表示数据包在网络中可以传输的最大跳数。每经过一个路由器，该值减 1，直到为 0，数据包会被丢弃。

协议(Protocol): 8 位,指示数据部分所使用的协议,例 TCP、UDP 或 ICMP 等。

头部校验和(Header Checksum): 16 位，用于检查 IP 头部在传输过程中是否发生了错误。

源地址(Source Address): 32 位，指示发送数据包的源 P 地址。

目标地址(Destination Address): 32 位，指示接收数据包的目标 IP 地址。

选项(Options):可选，用于指定一些特殊的功能或参数，如记录路由、时间戳等。

数据(Data): 携带了传输层协议的数据，例如 TCP 或 UDP。