# 实验一 应用层（2课时）

## — 、 实验目的

**学习 Wireshark 的基本操作，抓取和分析有线局域网的数据包**，熟悉一些应用层命令和协议。

## 二 、实验内容

1. 学会使用Wireshark抓包软件，会使用过滤器
2. **学习 Wireshark 基本操作：重点掌握捕获过滤器和显示过滤器。**分析HTTP和DNS协议
3. 测试curl命令，访问一个web页面。（选做）
4. 利用telnet命令测试get命令，访问www.baidu.com。（选做）
5. 利用telnet命令测试SMTP服务，解析其过程。（选做）
6. 测试tracert命令，并解析其过程。
7. 使用nslookup查询域名信息，简要分析。

## 三、实验原理

### 1. Wireshark 简介

Wireshark 软件是目前全球使用最广泛的开源网络数据包分析工具（前身为 Ethe- real），由 Gerald Combs 编写并于 1988 年获开源许可发布。网络数据包分析是指进入网络通信系统、捕获和解码网络上实时传输数据以及搜集统计信息的过程。通过 Wireshark 对网络数据进行分析，我们能够了解网络是如何运行的、数据包是如何被转发的、应用是如何被访问的；能够分析各层网络协议的性能、掌握通信主体的运行情况，确认带宽分配和时延大小、查看应用的快慢并改进优化，识别网络中存在的攻击或恶意行为、解决网络异常和故障。Wireshark 可以在 Windows、Linux 和 macOS 操作系统中运行，具备友好的图形界面、丰富的统计及图表分析功能。

### 2. 显示过滤器的使用

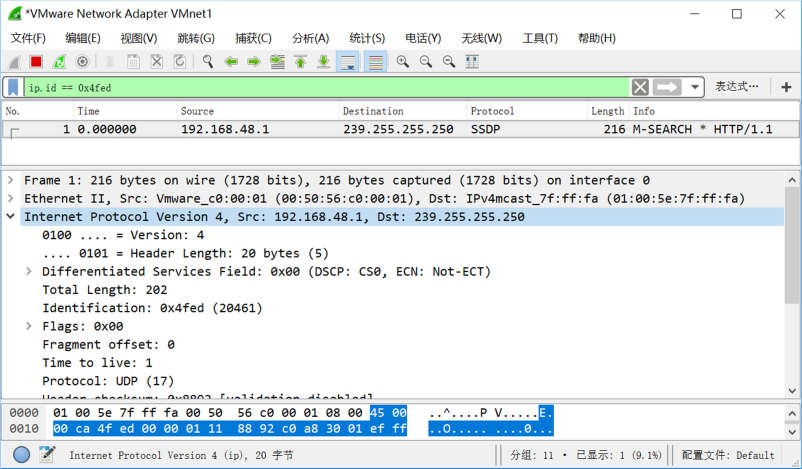
显示过滤器作用于捕获的数据包集合，用来指示 Wireshark 显示符合过滤条件的数据包。大家可以在 Packet List 面板上方的 Filter 文本框中编辑输入一个显示过滤器。

例如要过滤掉 Packet List 中所有的 ARP 数据包(ARP 数据实在太多了！)，把光标移动到

Filter 文本框中，然后输入!arp，就可以在 Packet List 面板中隐藏所有的 ARP 数据包了。



又例如要定位 ID 为 0X4fed 的 IP 数据包，可以使用如图 C-8 所示的 ip.id == 0X4fed 的过滤器



可以在 Filter 文本框中编辑显示过滤器。

显示过滤器的构造语法中有比较操作符、逻辑操作符和搜索操作符等。比较操作符可以让大家进行值的比较。而逻辑操作符可以使用多个过滤条件。Wireshark 也提供了搜索和匹配操作符。

过滤器表达式的比较操作符：

|  |  |  |
| --- | --- | --- |
| 操作符 | 说明 | 例子 |
| == | 等于 | tcp.flags.syn==1 |

|  |  |  |
| --- | --- | --- |
| != | 不等于 | tcp.port!= 80 |
| > | 大于 | ip.addr>192.168.1.5 |
| < | 小于 | ip.id<2454 |
| >= | 大于或等于 | frame.len>=1500 |
| <= | 小于或等于 | frame.number<=2333 |

过滤器表达式的逻辑操作符：

|  |  |  |
| --- | --- | --- |
| 操作符 | 说明 | 例子 |
| And, && | 两个条件同时满足 | ip.addr==192.168.1.5 and tcp.port==80 |
| or, || | 其中一个条件被满足 | ip.addr==192.168.1.5 or ip.addr==192.168.1.4 |
| not, ! | 没有条件被满足 | not arp |

过滤器表达式的搜索和匹配操作符：

操作符 说明 例子

contains 包含某个值 http contains "https[://ww](http://www.wireshark.org/)w.[wireshark.or](http://www.wireshark.org/)g"

matches, ~ 匹配某个值 http.request.uri matches ["www](http://www.mit.edu/).[mit.edu"](http://www.mit.edu/)

了解显示过滤器的操作符以后，大家就可以开始构造自己的过滤器了。TCP/IP 协议中能够用来构造显示过滤器的最重要两种元素是协议名称和协议头部字段的名称。协议名称例如http、ip、tcp 等。协议头部的字段，例如 ip.addr、tcp.flags.ack 等。总结了常用的几种显示过滤器。

常用的显示过滤器：

例子 说明

tcp.flags.syn==1 具有 syn 标志位的数据段

tcp.flags.rst==1 具有 rst 标志位的数据段

not arp 排除 arp 流量

ftp ftp 流量

tcp.port==21 or tcp.port==23 telnet 或 ftp 流量

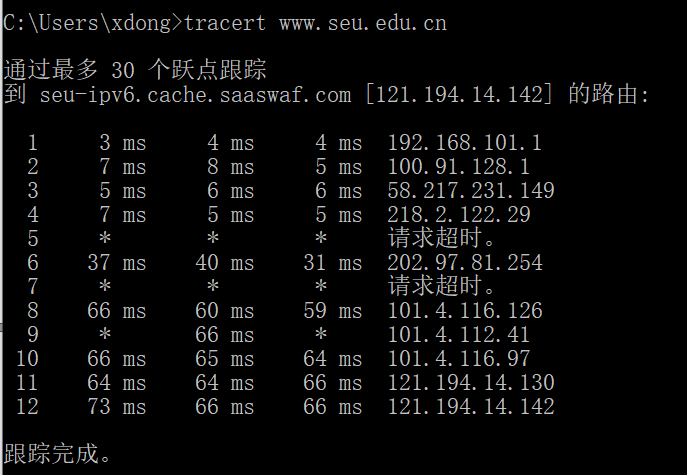
smtp or pop or smtp Email 流量

在显示过滤器构造过程中，在编辑过滤器表达式字符串的时候一定要注意 Wireshark 的用户提示。**如果用户输入的显示过滤器语法正确，输入框背景会变为绿色。对于错误的显示过滤器表达式，输入框背景将会显示红色。**

### 

### 3. Traceroute/Traceroute

Internet， 即国际互联网，是目前世界上最大的计算机网络，更确切地说是网络的网络。它由遍布全球的几万局域网和数百万台计算机组成，并通过用于异构网络的 TCP/IP协议进行网间通信。互联网中，信息的传送是通过网中许多段的传输介质和设备（路由器，交换机，服务器，网关等等）从一端到达另一端。每一个连 接在Internet上的设备，如主机、路由器、接入服务器等一般情况下都会有一个独立的IP地址。通过Traceroute我们可以知道信息从你的计算 机到互联网另一端的主机是走的什么路径。当然每次数据包由某一同样的出发点（source）到达某一同样的目的地(destination)走的路径可能 会不一样，但基本上来说大部分时候所走的路由是相同的。UNIX系统中，我们称之为Traceroute,MS Windows中为Tracert。 Traceroute通过发送小的数据包到目的设备直到其返回，来测量其需要多长时间。一条路径上的每个设备Traceroute要测3次。输出结果中包括每次测试的时间(ms)和设备的名称（如有的话）及其IP地址。  
在大多数情况下，作为网络工程技术人员或者系统管理员会在UNIX主机系统下，直接执行命令行：  
Traceroute hostname  
而在Windows系统下是执行Tracert的命令：  
Tracerert hostname  
比如在北京地区使用windows 主机（已经与北京163建立了点对点的连接后）  
使用windows系统中的Tracert命令：(用户可用：开始->运行,输入"command" 调出command窗口使用此命令）  
C:\\>tracert www.yahoo.com  
Tracing route to www.yahoo.com [204.71.200.75]  
over a maximum of 30 hops:  
  
1 161 ms 150 ms 160 ms 202.99.38.67  
2 151 ms 160 ms 160 ms 202.99.38.65  
3 151 ms 160 ms 150 ms 202.97.16.170  
4 151 ms 150 ms 150 ms 202.97.17.90  
5 151 ms 150 ms 150 ms 202.97.10.5  
6 151 ms 150 ms 150 ms 202.97.9.9  
7 761 ms 761 ms 752 ms border7-serial3-0-0.Sacramento.cw.net [204.70.122.69]  
8 751 ms 751 ms \* core2-fddi-0.Sacramento.cw.net [204.70.164.49]  
9 762 ms 771 ms 751 ms border8-fddi-0.Sacramento.cw.net [204.70.164.67]  
10 721 ms \* 741 ms globalcenter.Sacramento.cw.net [204.70.123.6]  
11 \* 761 ms 751 ms pos4-2-155M.cr2.SNV.globalcenter.net [206.132.150.237]  
12 771 ms \* 771 ms pos1-0-2488M.hr8.SNV.globalcenter.net [206.132.254.41]  
13 731 ms 741 ms 751 ms bas1r-ge3-0-hr8.snv.yahoo.com [208.178.103.62]  
14 781 ms 771 ms 781 ms www10.yahoo.com [204.71.200.75]  
  
Trace complete.



### 4. nslookup

nslookup用于查询DNS的记录，查询域名解析是否正常，在网络故障时用来诊断网络问题。

直接查询：

nslookup domain [dns-server]

//如果没有指定dns服务器，就采用系统默认的dns服务器。

查询其它记录

nslookup -qt = type domain [dns-server]

type:

A -->地址记录

AAAA -->地址记录

AFSDB Andrew -->文件系统数据库服务器记录

ATMA -->ATM地址记录

CNAME -->别名记录

HINHO -->硬件配置记录，包括CPU、操作系统信息

ISDN -->域名对应的ISDN号码

MB -->存放指定邮箱的服务器

MG -->邮件组记录

MINFO -->邮件组和邮箱的信息记录

MR -->改名的邮箱记录

MX -->邮件服务器记录

NS --> 名字服务器记录

PTR ->反向记录

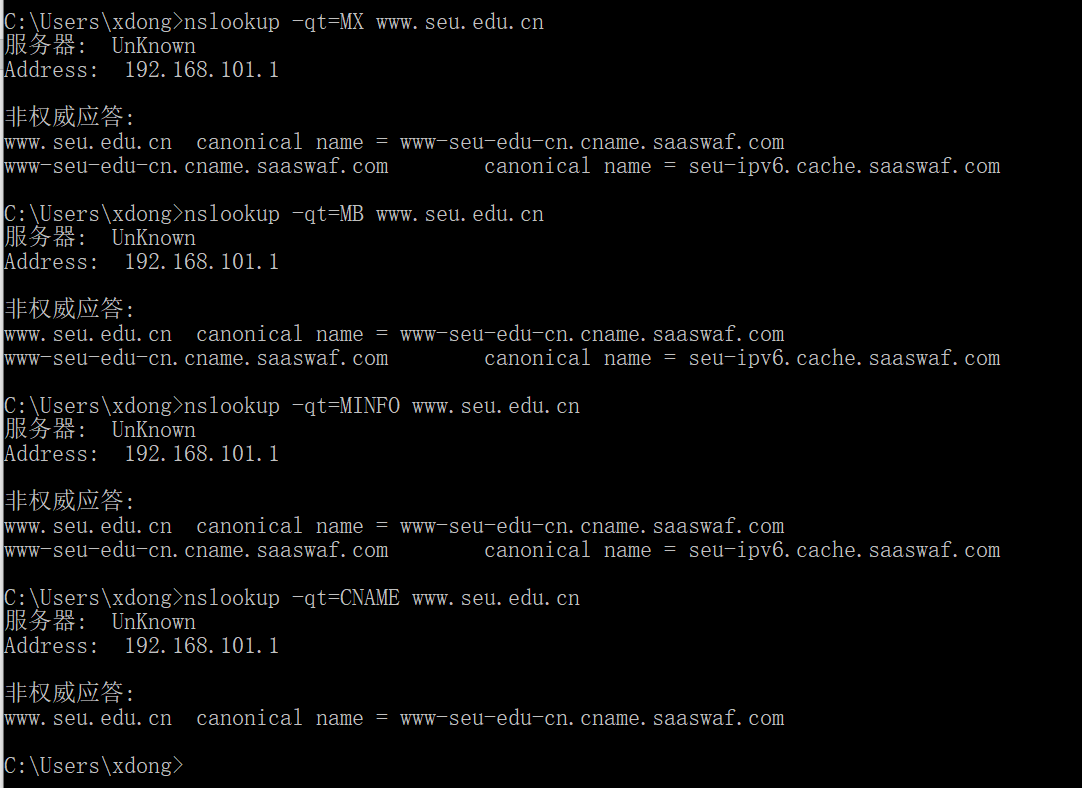
RP -->负责人记录

RT -->路由穿透记录

SRV -->TCP服务器信息记录

TXT -->域名对应的文本信息

X25 -->域名对应的X.25地址记录



## 四、实验报告

要求：每人一份实验报告，写出实验的主要步骤、解析与体会。