**华中科技大学计算机学院**

**《计算机通信与网络》实验报告**

实验名称 计算机通信与网络

|  |  |  |  |
| --- | --- | --- | --- |
| 姓 名 | 班 级 | 学 号 | 得 分 |
| 潘翔 | IOT1601 | U201614898 |  |

教师评语：

[Lab1 使用网络协议分析仪Wireshark 2](#_Toc112613722)

[1.1 环境 2](#_Toc1854403009)

[1.2 实验目的 2](#_Toc390191883)

[1.3 实验内容及步骤 2](#_Toc1304948641)

[1.4 实验结果 2](#_Toc1749979394)

[1.4.1 分析ping的报文 2](#_Toc1682212851)

[1.4.2 分析VPN 4](#_Toc1546759834)

[1.4.3 TraceRoute路径分析 5](#_Toc937182977)

[1.5 实验中的问题及心得 6](#_Toc475746566)

[参考文献 6](#_Toc430510863)

[Lab2 网络模拟器Packet Tracer的使用 9](#_Toc880905639)

[2.1 环境 9](#_Toc1342999981)

[2.2 实验目的 9](#_Toc2061467252)

[2.3 实验内容及步骤 9](#_Toc213804989)

[2.4 实验结果 9](#_Toc2016646008)

[2.5 实验中的问题及心得 9](#_Toc420857483)

[参考文献 9](#_Toc42179454)

**华中科技大学计算机学院**

**《计算机通信与网络》实验报告**

实验名称 使用网络协议分析仪Wireshark

|  |  |  |  |
| --- | --- | --- | --- |
| 姓 名 | 班 级 | 学 号 | 得 分 |
| 潘翔 | IOT1601 | U201614898 |  |

教师评语：

# Lab1 使用网络协议分析仪Wireshark

## 1.1 环境

操作系统： ArchLinux x64

网络平台： Wireshark 2.6.3

网络环境：

Link encap:Ethernet  HWaddr a0:8c:fd:24:5d:4c     
inet addr:222.20.100.153  Bcast:222.20.101.255  Mask:255.255.254.0   
inet6 addr: fe80::2476:27:cd9d:d75b/64 Scope:Link   
inet6 addr: 2001:250:4000:803c:e3c1:b69:d9f2:67b0/64 Scope:Global

## 1.2 实验目的

1. 能够正确安装配置网络协议分析软件Wireshark。
2. 熟悉使用Wireshark分析网络协议的基本方法。
3. 加深对协议格式、 协议层次和协议交换过程的理解。

## 1.3 实验内容及步骤

1. 启动WireShark
2. 因为WireShark需要网卡权限，输入命令 sudo wireshark
3. 选择当前网卡elo1
4. 尝试不同的协议和报文进行抓包分析

## 1.4 实验结果

### 1.4.1 分析ping的报文

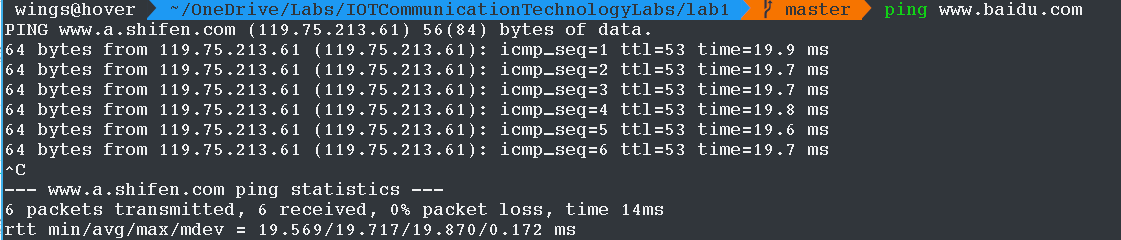


图1-1 ping [www.baidu.com](http://www.baidu.com)结果

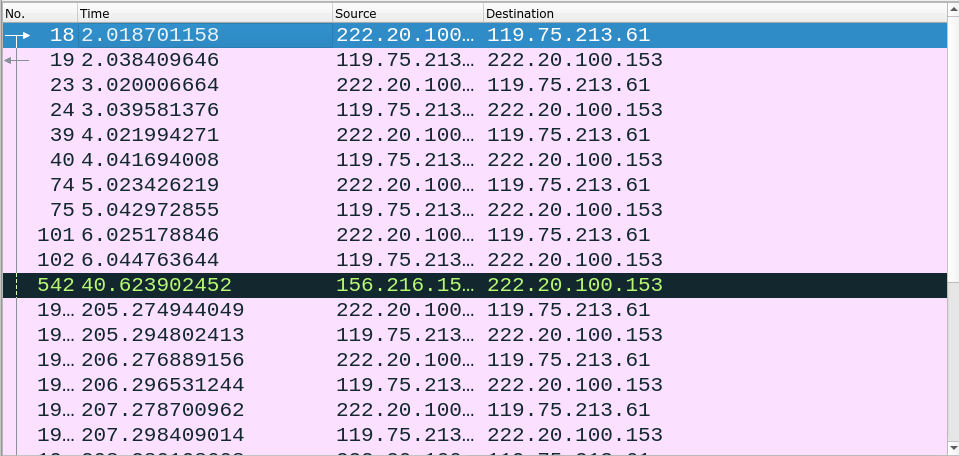


图1-2 wireshark结果



图1-3 ICMP报文结构

协议类型：V4

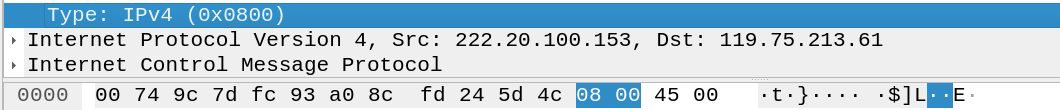


图1-4 协议类型

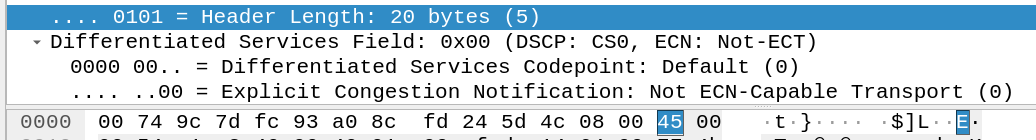


图1-5 首部长度

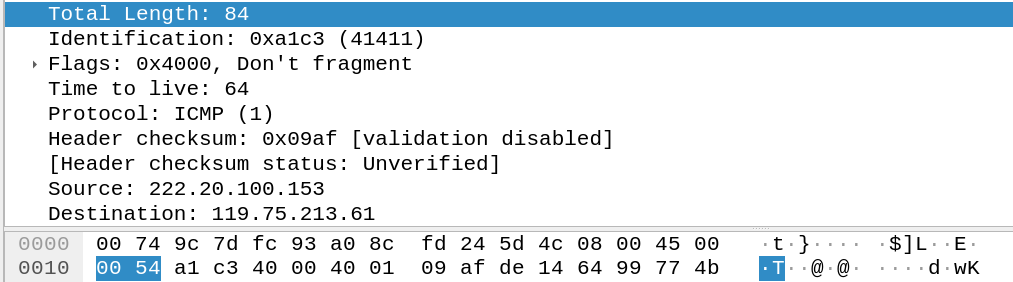


图1-6 总长度

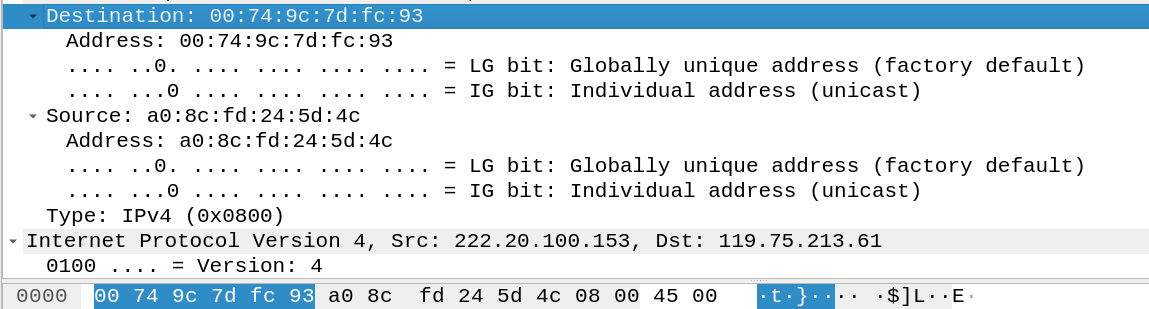


图1-7 源地址与目标地址

### 1.4.2 分析VPN

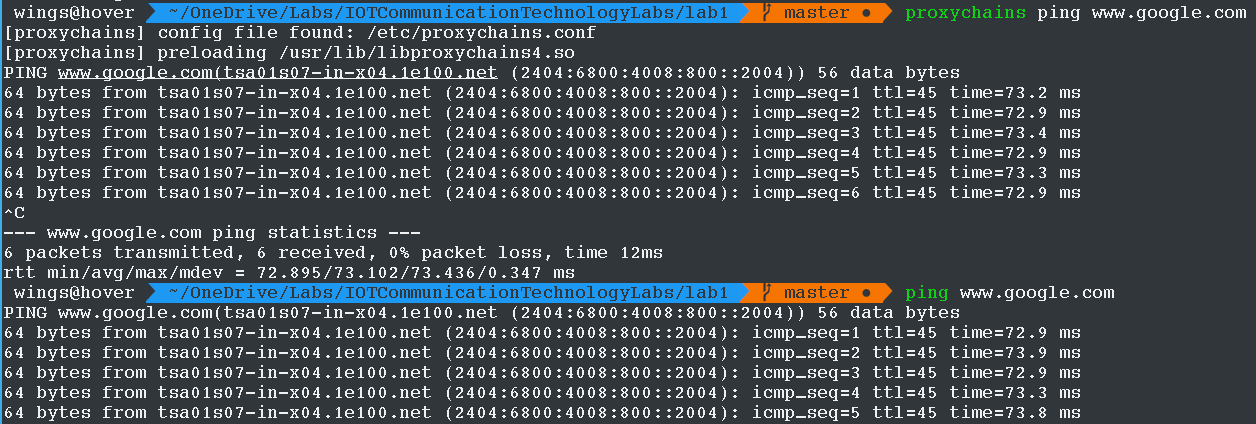


图1-8 proxychains ping

在proxychains中，对于能够直接连接且速度较快的访问请求采用直接访问形式，故实际上仍为直接访问。

对于www.google.com采用IPV6连接方式。

### 1.4.3 TraceRoute路径分析

TraceRoute的默认程序基于ICMP报文实现，而ICMP报文可能被防火墙拦截（路由器不响应）等原因无法收到反馈报文，tcpTraceRoute采用TCP “SYN”包，而如果目标地址是允许访问的，SYN标志位的数据段是TCP建立连接时进行“三次握手”的第一次握手，通常不会故增加采用了tcpTraceRoute进行测试。

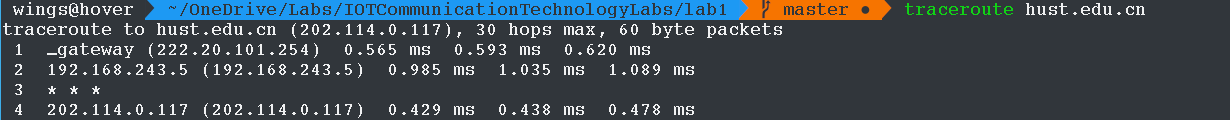


图1-9 traceroute hust.edu.cn

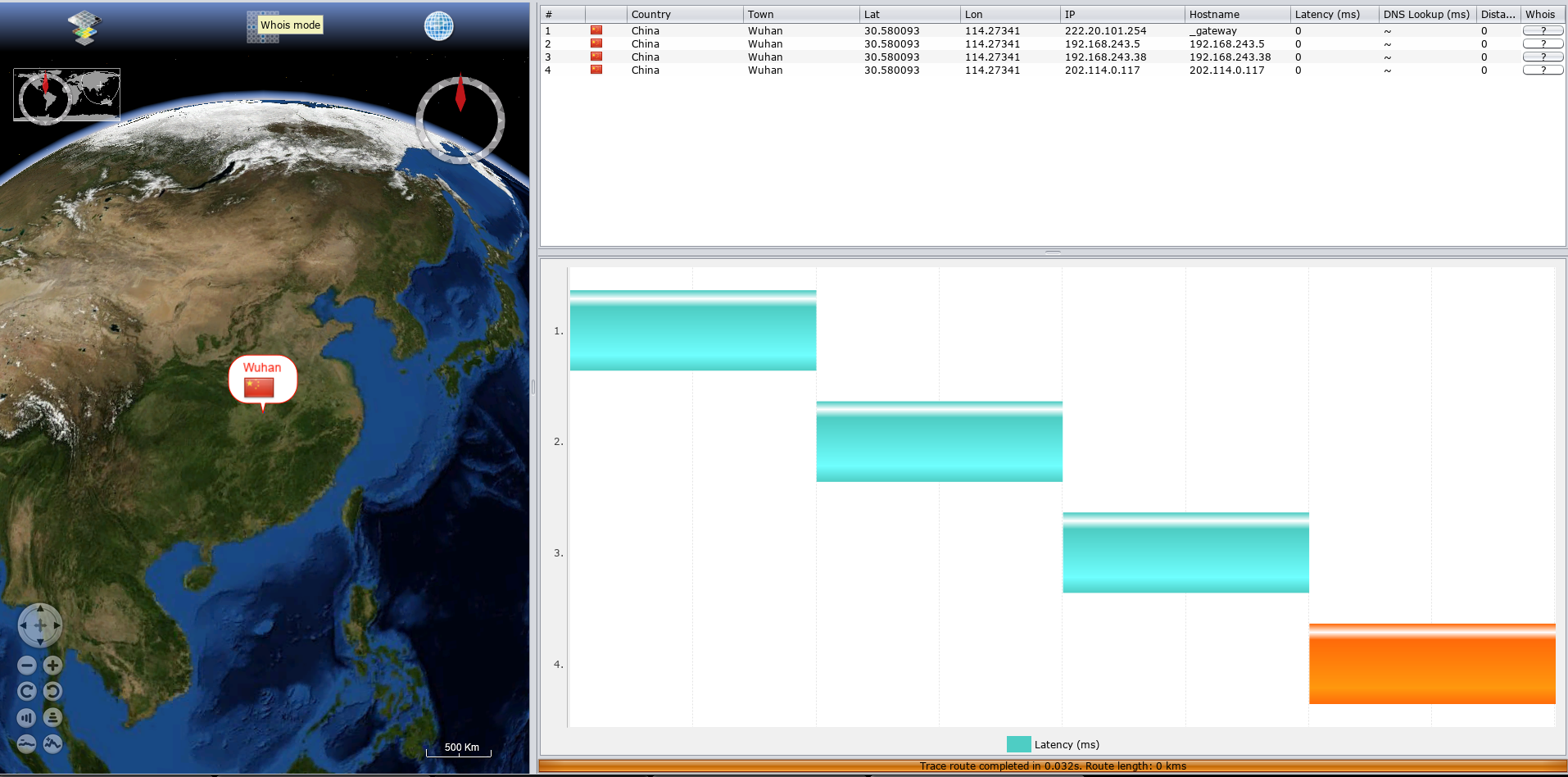


图1-10 visual-traceroute hust.edu.cn

从图中可以看出，在进行hust.edu.cn ICMP报文中，对于局域网段的返回报文不同的程序有不同的处理方式。

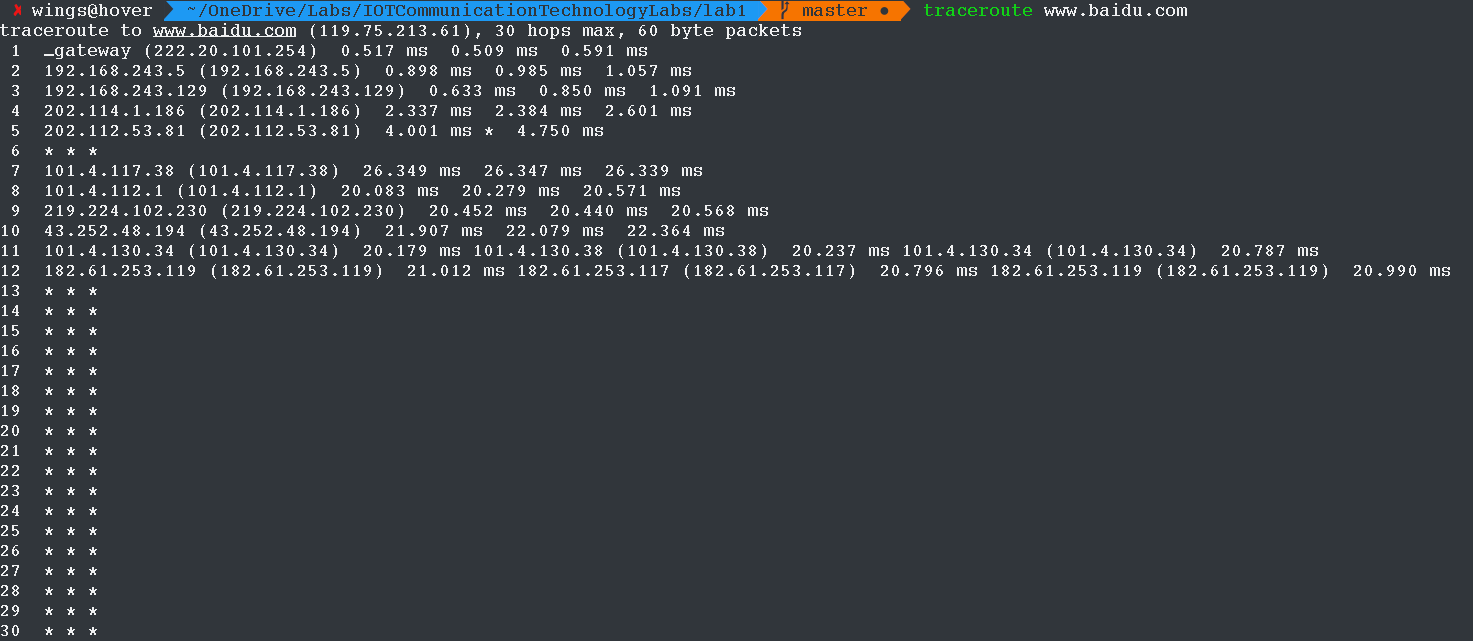


图1-11 traceroute www.baidu.com

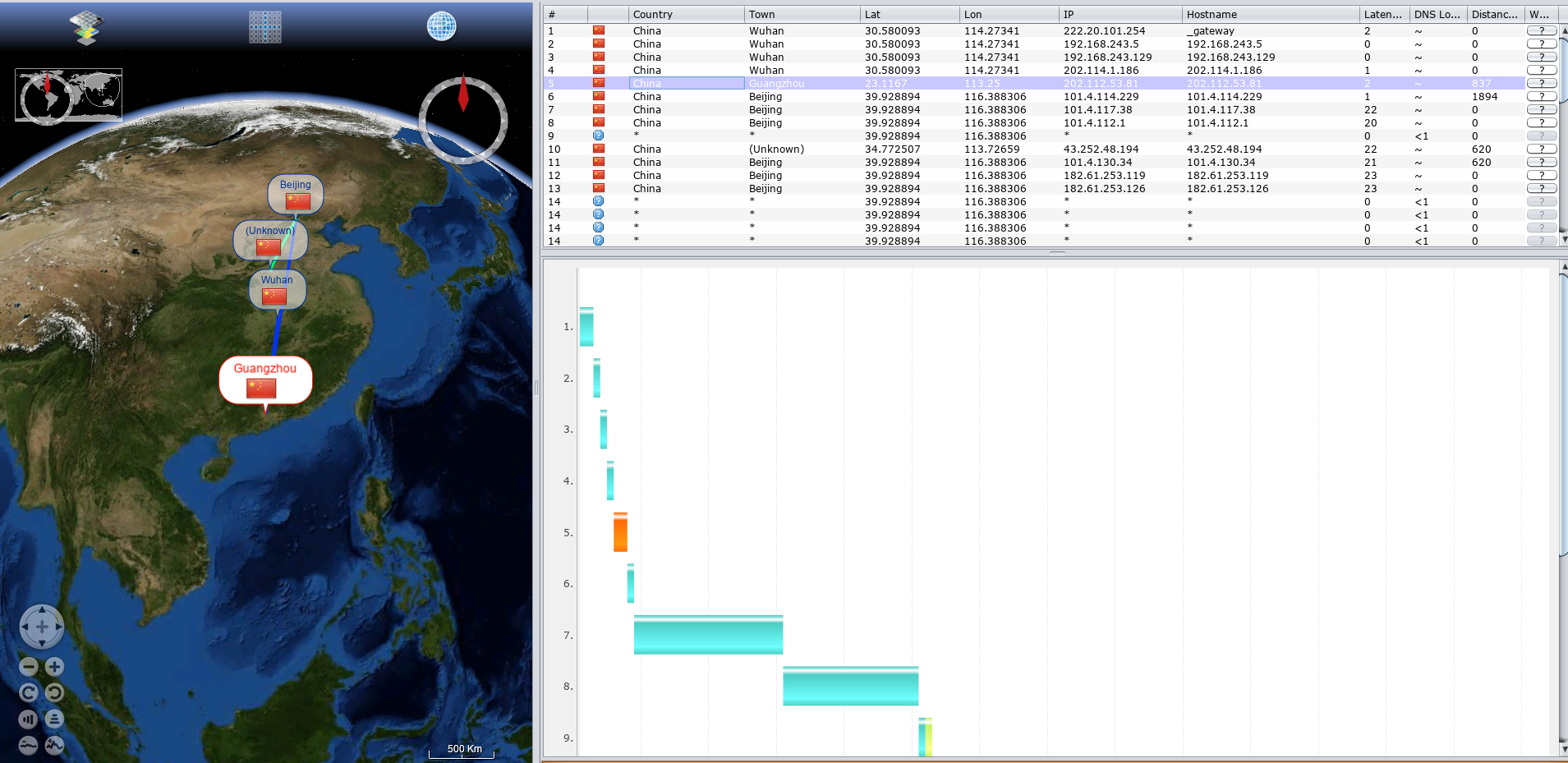


图1-12 visual-traceroute [www.baidu.com](http://www.baidu.com)

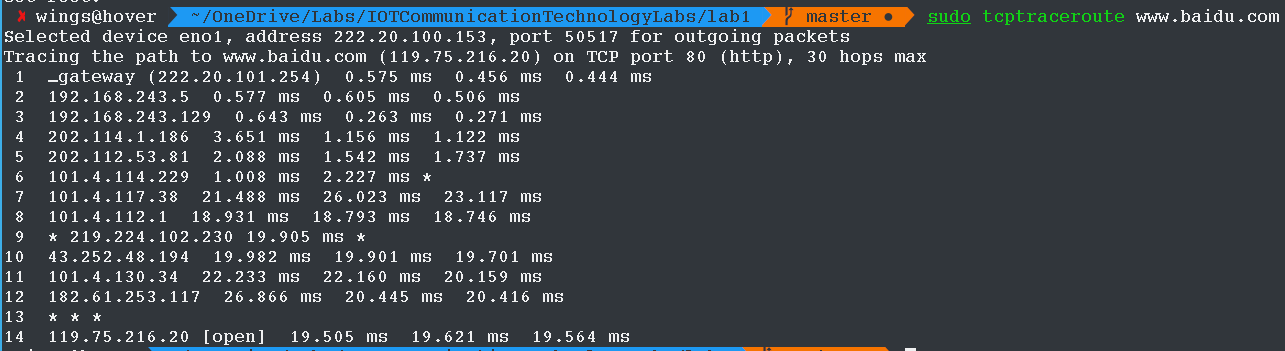


图1-13 tcptraceroute [www.baidu.com](http://www.baidu.com)

1. 与上文hust.edu.cn结果进行比较，从IP地址可以看出，均有从局域网段到广域网段的跳转。
2. 而在182.61.253.117/119处对ICMP包进行了拦截处理，故无法收到反馈报文，使用tcptraceroute可以得到反馈。
3. 可以看到使用可视化时，传播过程先到广州，再到北京，报文传输的路径选择与实际的物理距离有差异

## 1.5 实验中的问题及心得

实验过程中，因为较为熟悉网络的配置过程，故没有产生太多的困难，开始采用traceroute和ping时，想到使用proxychains进行一下测试，在过程中发现并无返回报文，应该是防火墙或者路由对与此类报文进行了阻塞处理，而进行了一次正常追踪之后，使用proxychains与正常结果相同，故猜测可能存在机制选择能够连接的方式。

分析过程使用了可视化工具帮助分析。

正常的ICMP报文对于商用服务器来说是一定的负担，故基于ICMP报文的traceroute可能被阻拦，故尝试采用基于‘SYN’包的tcptracroute，最终成功。

实验过程中，熟练了网络的debug方法，和了解了不同报文的字段结构。

## 参考文献

1. <https://wiki.archlinux.org/index.php/Network_Debugging>

**华中科技大学计算机学院**

**《计算机通信与网络》实验报告**

实验名称 使用网络协议分析仪Wireshark

|  |  |  |  |
| --- | --- | --- | --- |
| 姓 名 | 班 级 | 学 号 | 得 分 |
| 潘翔 | IOT1601 | U201614898 |  |

教师评语：

# Lab2 网络模拟器Packet Tracer的使用

## 2.1 环境

操作系统： ArchLinux x64

网络平台： Wireshark 2.6.3

网络环境：

Link encap:Ethernet  HWaddr a0:8c:fd:24:5d:4c     
inet addr:222.20.100.153  Bcast:222.20.101.255  Mask:255.255.254.0   
inet6 addr: fe80::2476:27:cd9d:d75b/64 Scope:Link   
inet6 addr: 2001:250:4000:803c:e3c1:b69:d9f2:67b0/64 Scope:Global

## 2.2 实验目的

1. 掌握使用Packet Tracer模拟网络场景的基本方法，加深对网络环境、 网络设备和网络协议交互过程等方面的理解。
2. 安装和配置网络模拟器软件Packet Tracer， 观察与IP网络接口的各种网络硬件及其适用场合。

## 2.3 实验内容及步骤

## 2.4 实验结果

## 2.5 实验中的问题及心得

## 参考文献

[1] CiscoPacketTracer网络实验手册