版本	2019

《计算机网络》实验指导书

学年学期: 2019 - 2020 学年第 一 学期

适用专业: 信息管理与信息系统 本科

适用年级: 2018 级

任课教师: 阮晓龙

所属科室: 信息管理与信息系统教研室

河南中医药大学信息技术学院

2019 年 8 月

目 录

实验一：使用交换机组网

一、实验目的

1、掌握局域网的特点和功能，了解局域网的基本分类；

2、了解局域网内的主要设备及组网过程；

3、掌握 GNS3 的基础操作；

4、掌握使用 GNS3 建设局域网的基本方法。

二、实验学时

2 学时

三、实验类型

验证型

四、实验需求

1、硬件

每人配备计算机 1 台。

2、软件

Windows 7 以上操作系统，安装 GNS3 网络仿真与 VirtualBox 虚拟化软件，安装 Putty 软件。

3、网络

实验室局域网支持，能够访问校园网。

4、工具

无。

五、实验理论

1、局域网的基本原理；

2、局域网的基本分类；

3、交换机的工作原理；

4、局域网组网的基本方法和基本流程。

六、实验任务

1、完成 GNS3 的安装、配置，并掌握其基本操作方法；

2、在 GNS3 环境下，完成使用二层交换机构建基本局域网；

3、在 GNS3 环境下，完成跨交换机之间通信。

七、实验内容及步骤

1、GNS3 安装

①双击打开 GNS3 安装程序。

②用户可使用默认的 GNS3 安装目录，也可自行修改默认路径，如图 1-1 所示。点击【Install】按钮进行安装，如图 1-2 所示。

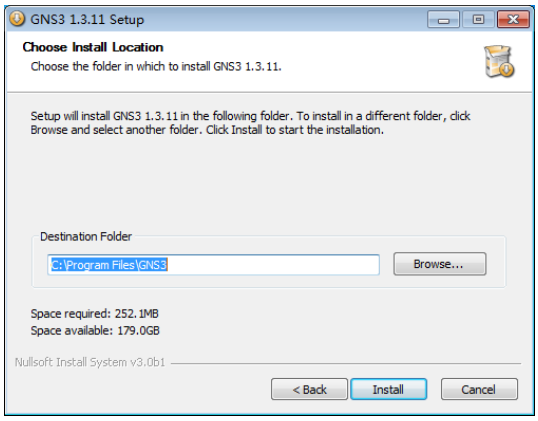

图 1-1 安装目录

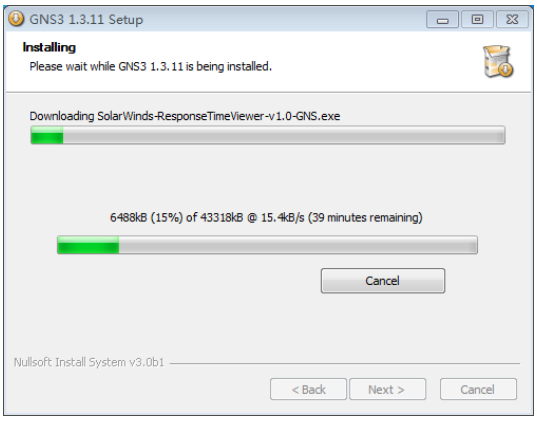

图 1-2 安装进程

③安装完成后，系统会给出如图 1-3 所示的界面。点击【Finish】完成软件安装。

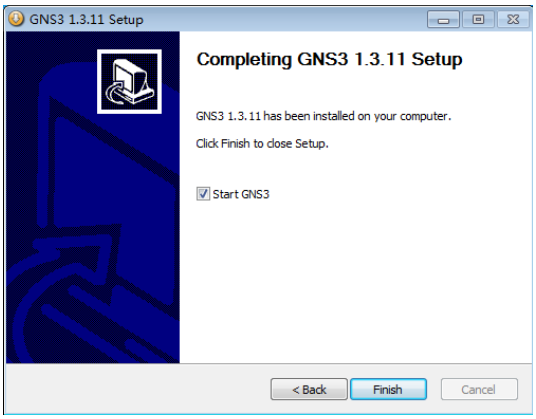

图 1-3 安装完成

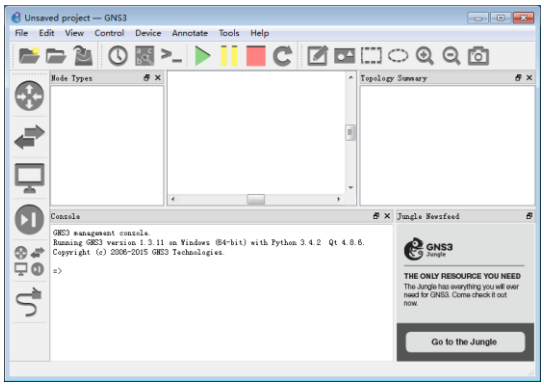

图 1-4 操作界面

④GNS3 的界面介绍

GNS3 窗口默认分为四个面板，如图 1-4 所示。左侧的面板列出了可用的节点类型（Node Types），可以看到各种路由器、防火墙、以太网交换机等图标，在需要搭建拓扑时，可从左侧面板拖拽出设备。右侧 Topogoy Summary 面板提供了拓扑汇总概要信息。中间区域包括上下两个面板，上面板是主要工作区，用于图形化显示拓扑结构。下部的Console面板，显示 Dynagen 的工作状态。

Dynagen 是用于连接到 Dynamips 程序的调试界面，由于其界面与 DOS 界面类似，所以在 GNS3 中并不常用。在使用中通常会关闭 Console、Topology Summary 窗口，从而使得整个工作区界面更加整洁。

2、使用交换机构建简单局域网

（1）安装镜像

①首先应先在 GNS3 中载入设备镜像。设备镜像文件可通过本课程网站

（http://network.ke.51xueweb.cn）下载获得，本实验所需的镜像为 c3640-ik9o3s-mz[1].124-25c。

②选择 GNS3 的【Edit】→【Preferences…】添加其镜像，如图 1-5 所示。

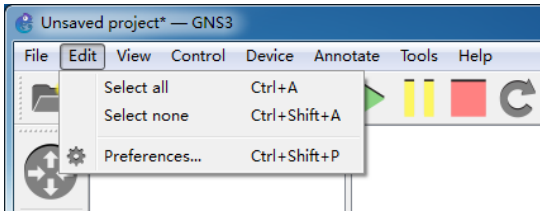

图 1-5 镜像设置

③在打开的【Preferences…】对话框中，点击【IOS routers】，然后点击【New】按钮添加镜像，如图 1-6 所示。选择下载获得的设备镜像文件，如图 1-7 所示，点击【Next >】按钮。

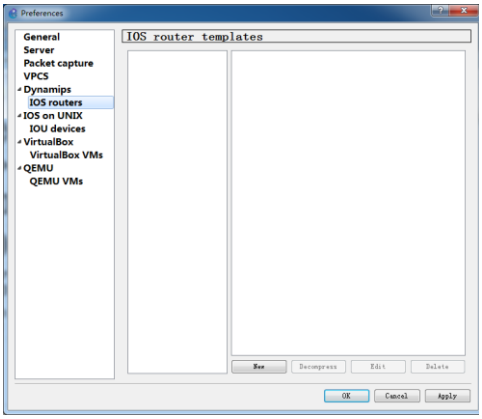

图 1-6 添加镜像

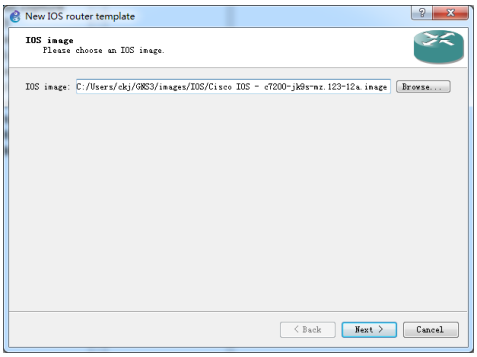

图 1-7 添加镜像位置

④将设备名称填写为 EtherSwitch 并将下方复选框勾选上，如图 1-8 所示。点击【Next >】按钮后，配置设备的内存容量，如图 1-9 所示。

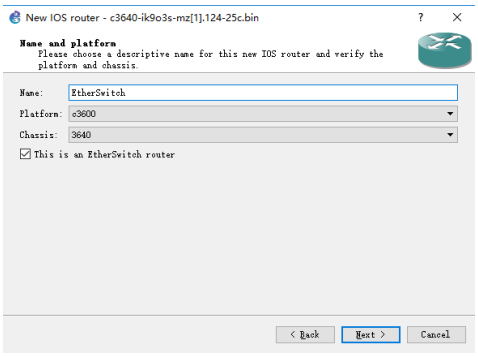

图 1-8 选择型号

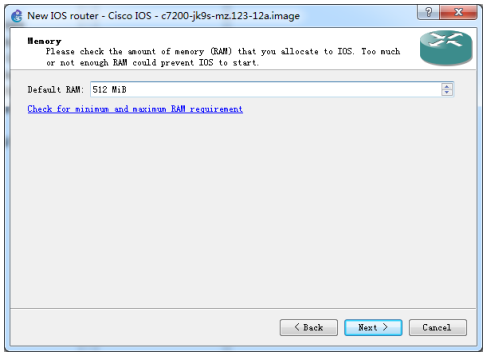

图 1-9 默认内存

⑤根据实际需要配置设备的交换机主控板的类型，如图 1-10 所示。

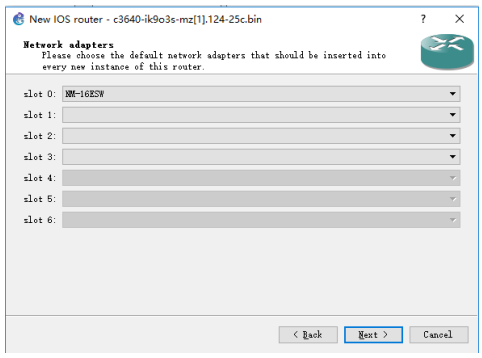

图 1-10 网络接口配置

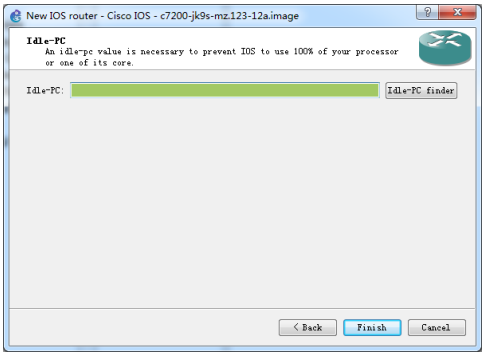

图 1-11 Idle-PC 值

⑥配置 Idle-PC 值，使用默认值即可。点击【Finish】按钮即可，如图 1-11 所示。

⑦对设备信息进行核查，如图 1-12 所示，信息确认无误后点击【Apply】→【OK】，就完成设备镜像的添加，添加完成后可在设备列表中看到添加的设备，如图 1-13 所示。

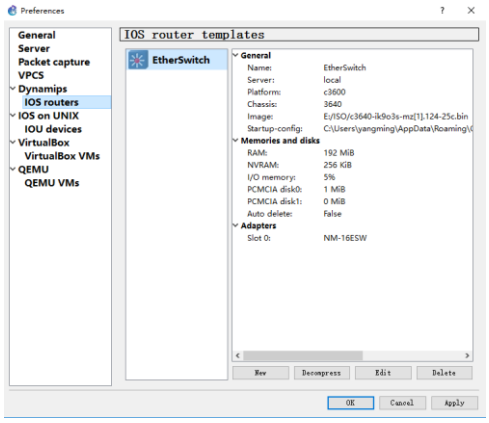

图 1-12 信息查看

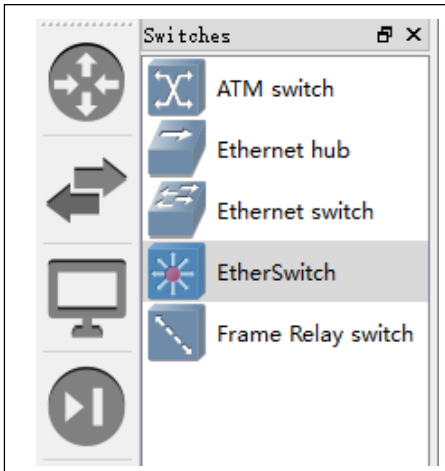

图 1-13 交换机

（2）拓扑设计

本实验局域网采用 1 台交换机(SW-1)与 2 台主机(Host-1、Host-2)组成，主机通过 GNS3 中自带的 VPCS 虚拟主机实现，网络拓扑结构如图 1-14 所示。

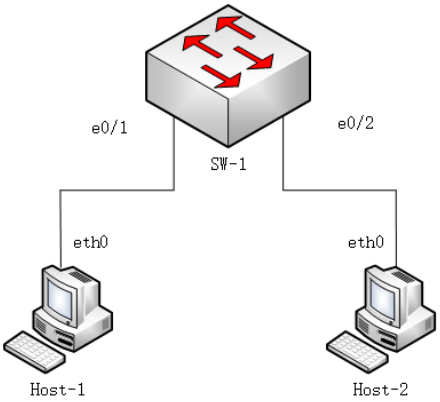

图 1-14 简单网络结构

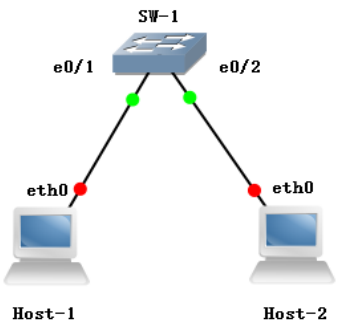

图 1-15 GNS3 网络结构

（3）按照拓扑结构的设计，在 GNS3 环境下完成局域网建设，如图 1-15 所示。

（4）按照配置表 1-1 网络地址规划表的具体要求，完成 2 台主机的网络配置。

表 1-1 网络地址规划表

序号	主机名称	网络配置	接入位置
1	Host-1	192.168.1.1/24	SW-1 e0/1
2	Host-2	192.168.1.2/24	SW-1 e0/2

（5）对主机进行网络配置

①右击 Host-1 图标，点击【Start】开启该设备。

②右击 Host-1 图标，点击【Console】打开 Host-1 的命令控制台，进行网络配置。网络配置命令如下所示。

```
>show ip
#查看 Host-1 的网络配置
>ip 192.168.1.1/24
#配置 Host-1 的 IP 地址
>show ip
#查看 Host-1 的网络配置
>save
#可以看到 Host-1 的网络配置完成，将配置进行保存
```

③结合表 1-1 的具体内容，参考 Host-1 的配置方法，完成 Host-2 的配置。并将 Host-2 的配置命令填写到表 1-2 中。

表 1-2 Host-2 配置命令

（6）网络通信测试

通过 Ping 命令进行网络通信测试，并将结果填写到表 1-3。

表 1-3 网络通信测试结果

序号	请求主机	接入位置	响应主机	接入位置	Ping 测试结果
1	Host-1	SW-1 e0/1	Host-2	SW-1 e0/2	
2	Host-2	SW-1 e0/2	Host-1	SW-1 e0/1	

3、跨交换机之间通信

（1）拓扑设计

本实验采用 2 台交换机（SW-1，SW-2）、6 台主机(Host-1、Host-2、Host-3、Host-4、Host-5、Host-6)，主机通过 GNS3 中自带的 VPCS 虚拟主机实现，网络拓扑结构如图 1-16 所示。

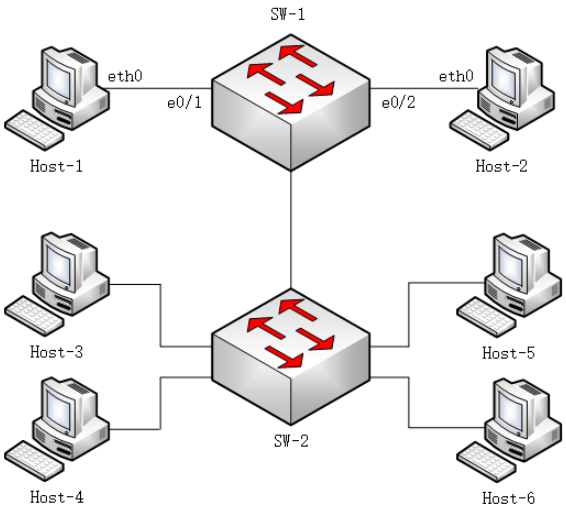

图 1-16 简单网络结构

（2）按照拓扑结构的设计，在 GNS3 环境下完成局域网建设，如图 1-17 所示。

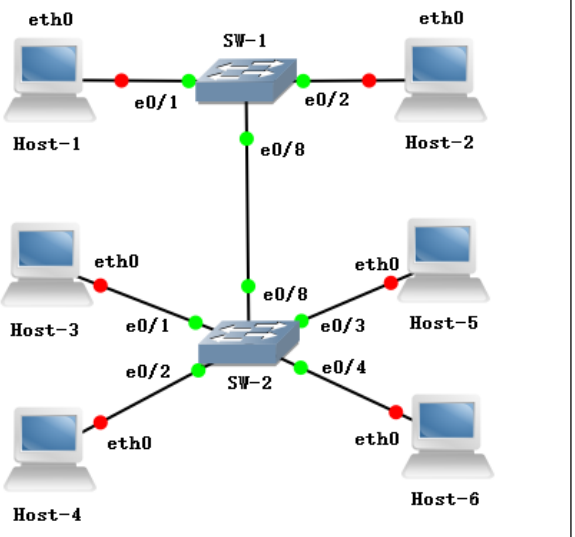

图 1-17 简单网络结构

（3）网络地址规划见表 1-4 所示。

表 1-4 网络地址规划表

序号	设备名称	网络配置	接入位置
1	Host-1	192.168.1.1/24	SW-1 e0/1
2	Host-2	192.168.1.2/24	SW-1 e0/2
3	Host-3	192.168.1.3/24	SW-2 e0/1
4	Host-4	192.168.1.4/24	SW-2 e0/2
5	Host-5	192.168.1.5/24	SW-2 e0/3

6	Host-6	192.168.1.6/24	SW-2 e0/4

（4）对主机进行网络配置

结合表 1-4 的具体内容，完成 Host-1，Host-2、Host-3、Host-4、Host-5、Host-6 的网络配置。

（5）通过 Ping 命令对 Host-1、Host-2、Host-3、Host-4、Host-5、Host-6 进行连通性测试，并填写表 1-5。

表 1-5 连通性测试

序号	请求主机	接入位置	响应主机	接入位置	Ping 测试结果
1	Host-1	SW-1 e0/1	Host-2	SW-1 e0/2	
2	Host-1	SW-1 e0/1	Host-3	SW-2 e0/1	
3	Host-1	SW-1 e0/1	Host-4	SW-2 e0/2	
4	Host-1	SW-1 e0/1	Host-5	SW-2 e0/3	
5	Host-1	SW-1 e0/1	Host-6	SW-2 e0/4	
6	Host-2	SW-1 e0/2	Host-1	SW-1 e0/1	
7	Host-2	SW-1 e0/2	Host-3	SW-2 e0/1	
8	Host-2	SW-1 e0/2	Host-4	SW-2 e0/2	
9	Host-2	SW-1 e0/2	Host-5	SW-2 e0/3	
10	Host-2	SW-1 e0/2	Host-6	SW-2 e0/4	
11	Host-3	SW-2 e0/1	Host-1	SW-1 e0/1	
12	Host-3	SW-2 e0/1	Host-2	SW-1 e0/2	
13	Host-3	SW-2 e0/1	Host-4	SW-2 e0/2	
14	Host-3	SW-2 e0/1	Host-5	SW-2 e0/3	
15	Host-3	SW-2 e0/1	Host-6	SW-2 e0/4	
16	Host-4	SW-2 e0/2	Host-1	SW-1 e0/1	
17	Host-4	SW-2 e0/2	Host-2	SW-1 e0/2	
18	Host-4	SW-2 e0/2	Host-3	SW-2 e0/1	
19	Host-4	SW-2 e0/2	Host-5	SW-2 e0/3	
20	Host-4	SW-2 e0/2	Host-6	SW-2 e0/4	
21	Host-5	SW-2 e0/3	Host-1	SW-1 e0/1	
22	Host-5	SW-2 e0/3	Host-2	SW-1 e0/2	
23	Host-5	SW-2 e0/3	Host-3	SW-2 e0/1	
24	Host-5	SW-2 e0/3	Host-4	SW-2 e0/2	
25	Host-5	SW-2 e0/3	Host-6	SW-2 e0/4	
26	Host-6	SW-2 e0/4	Host-1	SW-1 e0/1	
27	Host-6	SW-2 e0/4	Host-2	SW-1 e0/2	

28	Host-6	SW-2 e0/4	Host-3	SW-2 e0/1	
29	Host-6	SW-2 e0/4	Host-4	SW-2 e0/2	
30	Host-6	SW-2 e0/4	Host-5	SW-2 e0/3	

八、实验分析

1、GNS3

（1）使用 GNS3 仿真的网络和真实网络是否有区别？区别主要有哪些？

（2）GNS3 在网络构建中有什么用途？主要应用场景有哪些？

（3）除 GNS3 外还有哪些网络仿真软件？与 GNS3 对比有哪些优势？

2、企业网规划

（1）什么是企业网？企业网和互联网有哪些不同？

（2）进行企业网规划的时候，应该遵循哪些原则？哪些流程？

实验二：虚拟局域网与 VLAN 间通信

一、实验目的

1、理解交换机的工作原理；

2、掌握交换机的带外管理和带内管理的基本方法；

3、理解虚拟局域网（VLAN）的基本概念和原理；

4、掌握在多台二层交换机间划分虚拟局域网的详细内容和操作命令；

5、掌握 VLAN 间通信的基本原理与配置方法。

二、实验学时

2 学时

三、实验类型

综合型

四、实验需求

1、硬件

每人配备计算机 1 台。

2、软件

Windows 7 以上操作系统，安装 GNS3 网络仿真与 VirtualBox 虚拟化软件，安装 Putty 软件。

3、网络

实验室局域网支持，能够访问校园网。

4、工具

无。

五、实验理论

1、局域网的基本原理；

2、二层交换机的工作原理；

3、虚拟局域网的基本原理；

4、局域网组网的基本方法和基本流程；

5、VLAN 间路由的基本知识。

六、实验任务

1、完成基于二层交换机的局域网的建设；

2、完成交换机端口配置的具体操作，并能够完整读取交换机端口信息；

3、完成在 2 台二层交换机间划分虚拟局域网和网络功能测试。

七、实验内容及步骤

1、交换机管理

（1）打开 GNS3 软件，将 EtherSwitch 拖拽到 GNS3 工作台中，右击交换机，点击【start】按钮，开启交换机。右击交换机，点击【console】按钮，进入交换机配置界面，如图 2-1 所示。

图 2-1 交换机配置界面

对交换机端口配置进行管理，是进行交换机管理的基本操作，也是网管人员进行网络管理的基本素养。

（2）查看交换机的全部端口信息

```
查看交换机所有端口的状态
SW-1#show interface status
查看交换机所有端口详细信息
SW-1#show interface
```

（3）查看指定端口的信息

```
查看交换机端口 0/1 的状态
SW-1#show interfaces FastEthernet 0/1
FastEthernet0/1 is administratively down, line protocol is down
  Hardware is Fast Ethernet, address is cc01.0884.f001 (bia cc01.0884.f001)
  Description: *** Unused for Layer2 EtherSwitch ***
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
```

```
5 minute input rate 0 bits/sec, 0 packets/sec
5 minute output rate 0 bits/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 no buffer
    Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
    0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
    0 input packets with dribble condition detected
    0 packets output, 0 bytes, 0 underruns
    0 output errors, 0 collisions, 2 interface resets
    0 unknown protocol drops
    0 babbles, 0 late collision, 0 deferred
    0 lost carrier, 0 no carrier
    0 output buffer failures, 0 output buffers swapped out
```

阅读 FastEthernet0/1 的端口信息，并将端口信息所表达的含义填写到表 2-1 中。

表 2-1 FastEthernet0/1 端口信息含义

（4）配置端口的描述信息

```
进入交换机配置模式
SW-1#configure terminal
进入业务端口配置模式
SW-1 (config)#interface FastEthernet 0/1
配置交换机 0/1 端口的描述信息为：This is a fast ethernet interface
SW-1 (config-if)#description This is a fast ethernet interface
查看端口信息，可以看到已经发生了变化。
SW-1#show interfaces FastEthernet 0/1
Hardware is Fast Ethernet, address is cc01.0884.f001 (bia cc01.0884.f001)
```

```
  Description: This is a fast ethernet interface
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
      reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Auto-duplex, Auto-speed
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts, 0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 input packets with dribble condition detected
     0 packets output, 0 bytes, 0 underruns
     0 output errors, 0 collisions, 2 interface resets
     0 unknown protocol drops
     0 babbles, 0 late collision, 0 deferred
     0 lost carrier, 0 no carrier
     0 output buffer failures, 0 output buffers swapped out
```

（5）配置端口的速率和双工模式

```
SW-1 (config)#interface FastEthernet 0/1
SW-1(config-if)#speed ?
  10       Force 10 Mbps operation
  100      Force 100 Mbps operation
  auto     Enable AUTO speed configuration
配置端口速率为自适应。
SW-1(config-if)#speed auto
SW-1(config-if)#duplex ?
  auto     Enable AUTO duplex configuration
  full     Force full duplex operation
  half     Force half-duplex operation
配置端口为全双工模式。
SW-1(config-if)#duplex full
```

（6）配置端口的带宽控制

```
SW-1(config-if)#bandwidth ?
  <1-10000000>   Bandwidth in kilobits
  inherit        Specify that bandwidth is inherited
  receive        Specify receive-side bandwidth
配置端口的接收数据的带宽为 10Mbps。
SW-1(config-if)#bandwidth receive 10
取消端口带宽限制。
SW-1(config-if)#no bandwidth receive
```

（7）禁用和启用端口

禁用端口。
SW-1(config-if)#shutdown
启用端口
SW-1(config-if)#no shutdown

2、虚拟局域网

（1）拓扑设计

本实验采用 2 台交换机（SW-1，SW-2），6 台主机(Host-1、Host-2、Host-3、Host-4、Host-5、Host-6)，主机通过 GNS3 中自带的 VPCS 虚拟主机实现，网络拓扑结构如图 2-2 所示。

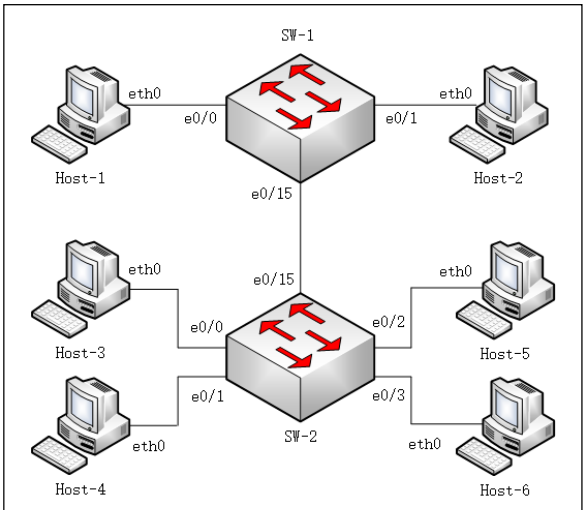

图 2-2 简单网络结构

（2）按照拓扑结构设计，在 GNS3 环境下完成局域网建设，如图 2-3 所示。

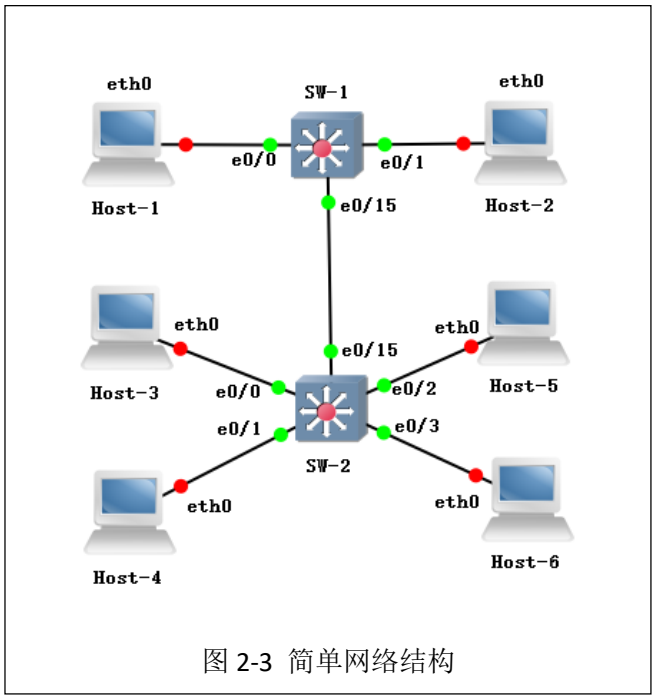

图 2-3 简单网络结构

（3）网络地址规划与 VLAN 规划设计方案见表 2-2 所示。

表 2-2 VLAN 规划表

序号	VLAN ID	VLAN name	交换机	接入端口	端口性质
1	vlan 10	VLAN0010	SW-1	F0/0	access Port
2	vlan 20	VLAN0020	SW-1	F0/1	access Port
3	vlan 10	VLAN0010	SW-2	F0/0	access Port
4	vlan 10	VLAN0010	SW-2	F0/1	access Port
5	vlan 20	VLAN0020	SW-2	F0/2	access Port
6	vlan 20	VLAN0020	SW-2	F0/3	access Port
7	-	-	SW-1	F0/15	Trunk Port
8	-	-	SW-2	F0/15	Trunk Port

（4）网络地址规划见表 2-3 所示。

表 2-3 网络地址规划表

序号	设备名称	网络配置	网关	接入位置
1	Host-1	192.168.1.1/24	192.168.1.254	SW-1 e0/1
2	Host-2	192.168.2.1/24	192.168.2.254	SW-1 e0/2
3	Host-3	192.168.1.2/24	192.168.1.254	SW-2 e0/1
4	Host-4	192.168.1.3/24	192.168.1.254	SW-2 e0/2
5	Host-5	192.168.2.2/24	192.168.2.254	SW-2 e0/3
6	Host-6	192.168.2.3/24	192.168.2.254	SW-2 e0/4

（5）对主机进行网络配置。

①右击 Host-1 图标，点击【Start】开启该设备。

②右击 Host-1 图标，点击【Console】打开 Host-1 的命令控制台，进行网络配置。网络配置命令如下所示。

```
>show ip
  //查看 Host-1 的网络配置
>ip 192.168.1.1/24 192.168.1.254
  //配置 Host-1 的 IP 地址与网关
>show ip
  //查看 Host-1 的网络配置
>save
  //可以看到 Host-1 的网络配置完成，将配置进行保存
```

③结合表 2-3 的具体内容，参考 Host-1 的配置方法，完成 Host-2、Host-3、Host-4、Host-5、Host-6 的网络配置。

（5）对交换机进行网络配置

①右击 SW-1 图标，点击【Start】开启该设备。

②右击 SW-1 图标，点击【Console】打开交换机的命令控制台进行配置。配置命令如下所示。

```
SW-1#vlan database
```

```
  //一般 3640 或者 3725 等系列路由器的交换模块需要进入 VLAN 数据库模式进行操作
SW-1(vlan)#vlan 10
SW-1(vlan)#vlan 20
SW-1(vlan)#exit
SW-1#conf t
SW-1(config)#int f0/0
//从特权模式切换到配置模式
SW-1(config-if)#switchport mode access
  //将接口模式修改为接入模式，此模式一般用于接入终端主机
SW-1(config-if)#switchport access vlan 10
SW-1(config-if)#no shutdown
SW-1(config-if)#exit
SW-1(config)#int f0/1
SW-1(config-if)#switchport mode access
SW-1(config-if)#switchport access vlan 20
SW-1(config-if)#no shutdown
SW-1(config-if)#exit
SW-1#show vlan-switch brief
  //查看该交换机 vlan 的主要情况
VLAN Name                                Status    Ports
---- ----------------------------------- --------- -------------------------------
1    default                             active    Fa0/2, Fa0/3, Fa0/4,
Fa0/5
                                                   Fa0/6,  Fa0/7,  Fa0/8,
Fa0/9
                                                   Fa0/10,         Fa0/11,
Fa0/12, Fa0/13
                                                   Fa0/14. Fa0/15
10   VLAN0010                            active    Fa0/0
20   VLAN0020                            active    Fa0/1
SW-1#conf t
SW-1(config)#int f0/15
SW-1(config-if)#switchport trunk encapsulation dot1q
  //Trunk 有两种封装标准，一种是 Cisco 私有的 ISL，一种是行业标准 802.1Q，一般采用 802.1Q 实现封装，本书统一采用 802.1Q 标准。
SW-1(config-if)#switchport mode trunk
  //将接口模式定义位 trunk 模式，交换机相连的接口一般采用 trunk 模式，用于承载不同 VLAN 的流量
SW-1(config-if)#exit
SW-1(config)#exit
SW-1#write
```

③参考 SW-1 的配置命令，完成 SW-2 的网络配置。

（6）通过 Ping 命令对 Host-1、Host-2、Host-3、Host-4、Host-5、Host-6 进行连通性测试，并填写表 2-4。

表 2-4 连通性测试

序号	请求主机	接入位置	响应主机	接入位置	Ping 测试结果

1	Host-1	SW-1 e0/0	Host-2	SW-1 e0/1	
2	Host-1	SW-1 e0/0	Host-3	SW-2 e0/0	
3	Host-1	SW-1 e0/0	Host-4	SW-2 e0/1	
4	Host-1	SW-1 e0/0	Host-5	SW-2 e0/2	
5	Host-1	SW-1 e0/0	Host-6	SW-2 e0/3	
6	Host-2	SW-1 e0/1	Host-1	SW-1 e0/0	
7	Host-2	SW-1 e0/1	Host-3	SW-2 e0/0	
8	Host-2	SW-1 e0/1	Host-4	SW-2 e0/1	
9	Host-2	SW-1 e0/1	Host-5	SW-2 e0/2	
10	Host-2	SW-1 e0/1	Host-6	SW-2 e0/3	
11	Host-3	SW-2 e0/0	Host-1	SW-1 e0/0	
12	Host-3	SW-2 e0/0	Host-2	SW-1 e0/1	
13	Host-3	SW-2 e0/0	Host-4	SW-2 e0/1	
14	Host-3	SW-2 e0/0	Host-5	SW-2 e0/2	
15	Host-3	SW-2 e0/0	Host-6	SW-2 e0/3	
16	Host-4	SW-2 e0/1	Host-1	SW-1 e0/0	
17	Host-4	SW-2 e0/1	Host-2	SW-1 e0/1	
18	Host-4	SW-2 e0/1	Host-3	SW-2 e0/0	
19	Host-4	SW-2 e0/1	Host-5	SW-2 e0/2	
20	Host-4	SW-2 e0/1	Host-6	SW-2 e0/3	
21	Host-5	SW-2 e0/2	Host-1	SW-1 e0/0	
22	Host-5	SW-2 e0/2	Host-2	SW-1 e0/1	
23	Host-5	SW-2 e0/2	Host-3	SW-2 e0/0	
24	Host-5	SW-2 e0/2	Host-4	SW-2 e0/1	
25	Host-5	SW-2 e0/2	Host-6	SW-2 e0/3	
26	Host-6	SW-2 e0/3	Host-1	SW-1 e0/0	
27	Host-6	SW-2 e0/3	Host-2	SW-1 e0/1	
28	Host-6	SW-2 e0/3	Host-3	SW-2 e0/0	
29	Host-6	SW-2 e0/3	Host-4	SW-2 e0/1	
30	Host-6	SW-2 e0/3	Host-5	SW-2 e0/2	

3、VLAN 间通信

（1）开启交换机 SW-1 的路由功能。

```
SW-1#configure terminal
SW-1(config)#ip routing
```

（2）分别在 VlAN 10 和 VLAN 20 上配置 IP 地址为 192.168.1.254、192.168.2.254。

```
SW-1(config)#interface vlan 10
SW-1(config)#ip address 192.168.1.254 255.255.255.0
SW-1(config)#exit
SW-1(config)#interface vlan 20
SW-1(config)#ip address 192.168.2.254 255.255.255.0
SW-1(config)#exit
```

（3）参考 SW-1 的配置命令，完成 SW-2 的 VlAN 配置。并将 SW-2 的配置命令填写到表 2-5 中。

表 2-5 SW-2 配置命令

（4）通过 Ping 命令对 Host-1、Host-2、Host-3、Host-4、Host-5、Host-6 进行连通性测试，并填写表 2-6。

表 2-6 连通性测试

序号	请求主机	接入位置	响应主机	接入位置	Ping 测试结果
1	Host-1	SW-1 e0/0	Host-2	SW-1 e0/1	
2	Host-1	SW-1 e0/0	Host-3	SW-2 e0/0	
3	Host-1	SW-1 e0/0	Host-4	SW-2 e0/1	
4	Host-1	SW-1 e0/0	Host-5	SW-2 e0/2	
5	Host-1	SW-1 e0/0	Host-6	SW-2 e0/3	
6	Host-2	SW-1 e0/1	Host-1	SW-1 e0/0	
7	Host-2	SW-1 e0/1	Host-3	SW-2 e0/0	
8	Host-2	SW-1 e0/1	Host-4	SW-2 e0/1	
9	Host-2	SW-1 e0/1	Host-5	SW-2 e0/2	
10	Host-2	SW-1 e0/1	Host-6	SW-2 e0/3	
11	Host-3	SW-2 e0/0	Host-1	SW-1 e0/0	
12	Host-3	SW-2 e0/0	Host-2	SW-1 e0/1	
13	Host-3	SW-2 e0/0	Host-4	SW-2 e0/1	
14	Host-3	SW-2 e0/0	Host-5	SW-2 e0/2	
15	Host-3	SW-2 e0/0	Host-6	SW-2 e0/3	
16	Host-4	SW-2 e0/1	Host-1	SW-1 e0/0	
17	Host-4	SW-2 e0/1	Host-2	SW-1 e0/1	

18	Host-4	SW-2 e0/1	Host-3	SW-2 e0/0	
19	Host-4	SW-2 e0/1	Host-5	SW-2 e0/2	
20	Host-4	SW-2 e0/1	Host-6	SW-2 e0/3	
21	Host-5	SW-2 e0/2	Host-1	SW-1 e0/0	
22	Host-5	SW-2 e0/2	Host-2	SW-1 e0/1	
23	Host-5	SW-2 e0/2	Host-3	SW-2 e0/0	
24	Host-5	SW-2 e0/2	Host-4	SW-2 e0/1	
25	Host-5	SW-2 e0/2	Host-6	SW-2 e0/3	
26	Host-6	SW-2 e0/3	Host-1	SW-1 e0/0	
27	Host-6	SW-2 e0/3	Host-2	SW-1 e0/1	
28	Host-6	SW-2 e0/3	Host-3	SW-2 e0/0	
29	Host-6	SW-2 e0/3	Host-4	SW-2 e0/1	
30	Host-6	SW-2 e0/3	Host-5	SW-2 e0/2	

八、实验分析

1、交换机端口的带宽控制和流量控制

（1）带宽控制是如何实现的？流量控制是如何实现的？请分别介绍其工作原理。

（2）请设计实验验证带宽控制和流量控制对网络性能的影响。

2、虚拟局域网与广播风暴

（1）1 台交换机最多可以划分多少个 VLAN？VLAN 对于交换机的通信效率是否有影响？请说明原因。

（2）虚拟局域网可以将 1 台交换机逻辑上划分为多个广播域，那么虚拟局域网是否能够降低广播风暴的发生？请说明原因。

（3）虚拟局域网是否能够从根本上避免广播风暴的产生？请说明原因。

实验三：使用路由器组网

一、实验目的

1、理解路由器的基本工作原理；

2、掌握路由器的基本管理和配置方法；

3、理解路由组网的方法和静态路由的具体使用；

4、理解基于路由器的园区网的结构，并进一步体会园区网的设计思路。

二、实验学时

2 学时

三、实验类型

综合型

四、实验需求

1、硬件

每人配备计算机 1 台。

2、软件

Windows 7 以上操作系统，安装 GNS3 网络仿真与 VirtualBox 虚拟化软件，安装 Putty 软件。

3、网络

实验室局域网支持，能够访问校园网。

4、工具

无。

五、实验理论

1、虚拟局域网的基本原理；

2、交换机、路由交换机、路由器的工作原理；

3、网络测试的基本原理；

4、园区网的规划设计方法和基本流程。

六、实验任务

1、基于网络规划，完成局域网建设；

2、完成 VLAN 的配置；

3、完成路由器、路由交换机的配置；

4、完成网络连通性测试。

七、实验内容及步骤

1、网络规划

（1）本实验采用 1 台路由器（RT-1）、2 台路由交换机（RS-1、RS-2）、4 台交换机（SW-1、SW-2、SW-3、SW-4)、12 台主机(Host-1 至 Host-12)。主机通过 GNS3 中自带的 VPCS 虚拟主机实现，网络拓扑结构如图 3-1 所示。

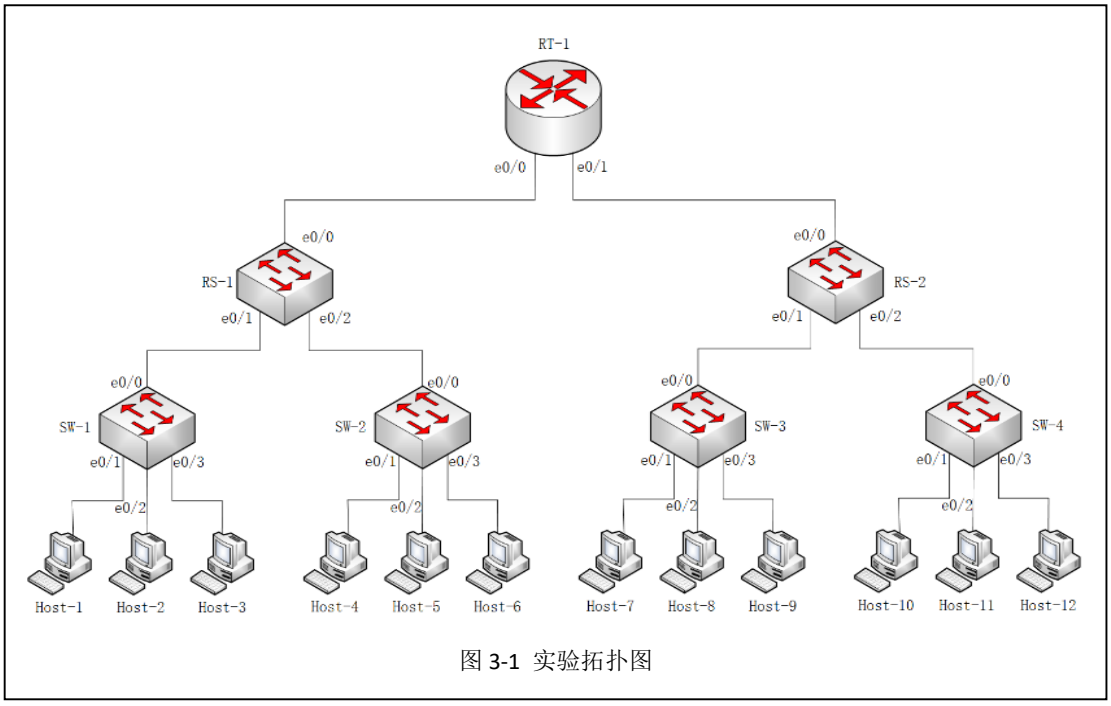

图 3-1 实验拓扑图

（2）按照拓扑结构的设计，在 GNS3 环境下完成局域网建设，如图 3-2 所示。

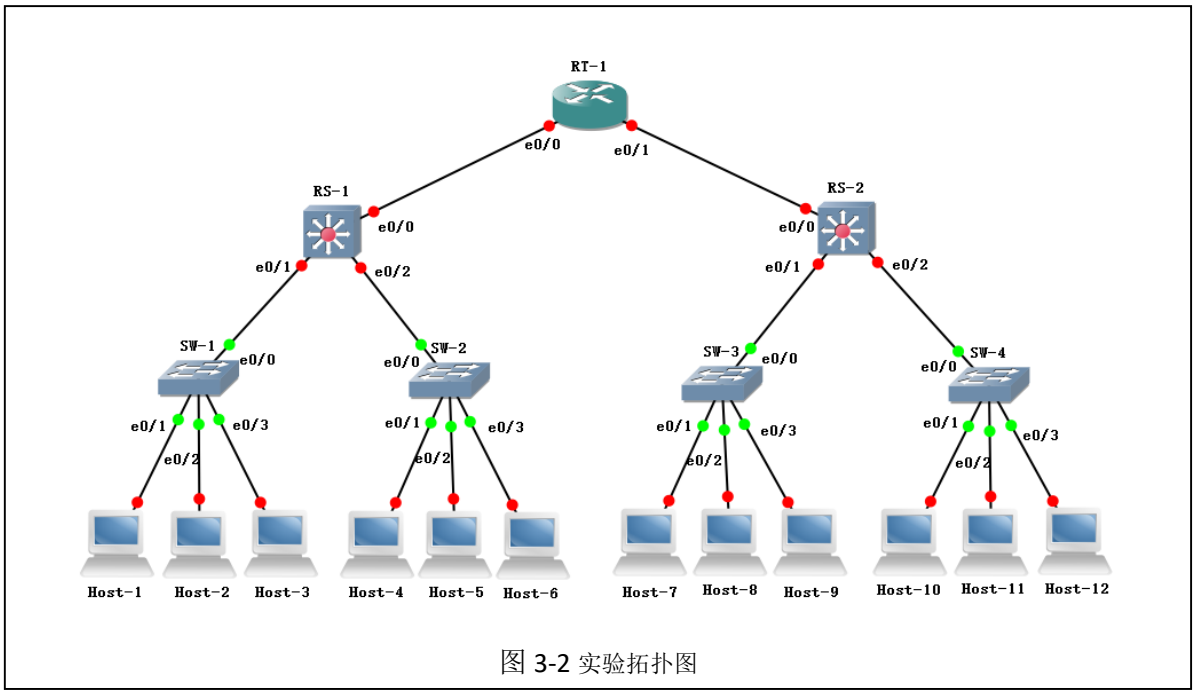

图 3-2 实验拓扑图

（3）网络地址规划与 VLAN 规划设计方案及路由规划，具体见表 3-1、表 3-2、表 3-3、表 3-4 所示。

表 3-1 VLAN 规划表

序号	交换机	VLAN ID	VLAN name	接入端口	端口性质
1	SW-1	-	-	F0/0	Trunk Port
2	SW-1	valn 10	0010	F0/1	access Port
3	SW-1	valn 20	0020	F0/2	access Port
4	SW-1	valn 30	0030	F0/3	access Port
5	SW-2	-	-	F0/0	Trunk Port
6	SW-2	valn 10	0010	F0/1	access Port
7	SW-2	valn 20	0020	F0/2	access Port
8	SW-2	valn 30	0030	F0/3	access Port
9	SW-3	-	-	F0/0	Trunk Port
10	SW-3	valn 40	0040	F0/1	access Port
11	SW-3	valn 50	0050	F0/2	access Port
12	SW-3	valn 60	0060	F0/3	access Port
13	SW-4	-	-	F0/0	Trunk Port
14	SW-4	valn 40	0040	F0/1	access Port
15	SW-4	valn 50	0050	F0/2	access Port
16	SW-4	valn 60	0060	F0/3	access Port
17	RS-1	-	-	F2/1	Trunk Port
18	RS-1	-	-	F2/2	Trunk Port
19	RS-1	vlan 10	0010	-	-
20	RS-1	vlan 20	0020	-	-
21	RS-1	vlan 30	0030	-	-
22	RS-2	-	-	F2/1	Trunk Port
23	RS-2	-	-	F2/2	Trunk Port
24	RS-2	vlan 40	0040	-	-
25	RS-2	vlan 50	0050	-	-
26	RS-2	vlan 60	0060	-	-

表 3-2 网络地址规划表

序号	主机名称	网络配置	网关	接入位置
1	Host-1	10.0.101.1/24	10.0.101.254	SW-1 F0/1
2	Host-2	10.0.102.1/24	10.0.102.254	SW-1 F0/2
3	Host-3	10.0.103.1/24	10.0.103.254	SW-1 F0/3
4	Host-4	10.0.101.2/24	10.0.101.254	SW-2 F0/1

5	Host-5	10.0.102.2/24	10.0.102.254	SW-2 F0/2
6	Host-6	10.0.103.2/24	10.0.103.254	SW-2 F0/3
7	Host-7	10.0.104.1/24	10.0.104.254	SW-3 F0/1
8	Host-8	10.0.105.1/24	10.0.105.254	SW-3 F0/2
9	Host-9	10.0.106.1/24	10.0.106.254	SW-3 F0/3
10	Host-10	10.0.104.2/24	10.0.104.254	SW-4 F0/1
11	Host-11	10.0.105.2/24	10.0.105.254	SW-4 F0/2
12	Host-12	10.0.106.2/24	10.0.106.254	SW-4 F0/3

表 3-3 设备地址规划表

序号	设备	端口	端口类型	IP 地址
1	RS-1	F2/0	no switchport	10.0.107.1/30
2	RS-2	F2/0	no switchport	10.0.108.1/30
3	RT-1	E1/1	-	10.0.107.2/30
4	RT-1	E1/2	-	10.0.108.2/30

表 3-4 路由规划表

序号	设备	路由协议	路由
1	RT-1	Static-router	10.0.101.0 255.255.255.0 10.0.107.1
2	RT-1	Static-router	10.0.102.0 255.255.255.0 10.0.107.1
3	RT-1	Static-router	10.0.103.0 255.255.255.0 10.0.107.1
4	RT-1	Static-router	10.0.104.0 255.255.255.0 10.0.108.1
5	RT-1	Static-router	10.0.105.0 255.255.255.0 10.0.108.1
6	RT-1	Static-router	10.0.106.0 255.255.255.0 10.0.108.1
7	RS-1	Static-router	10.0.104.0 255.255.255.0 10.0.107.2
8	RS-1	Static-router	10.0.105.0 255.255.255.0 10.0.107.2
9	RS-1	Static-router	10.0.106.0 255.255.255.0 10.0.107.2
10	RS-1	Static-router	10.0.108.0 255.255.255.252 10.0.107.2
11	RS-2	Static-router	10.0.101.0 255.255.255.0 10.0.108.2
12	RS-2	Static-router	10.0.102.0 255.255.255.0 10.0.108.2
13	RS-2	Static-router	10.0.103.0 255.255.255.0 10.0.108.2
14	RS-2	Static-router	10.0.107.0 255.255.255.252 10.0.108.2

2、主机配置

①右击 Host-1 图标，点击【Start】开启该设备。

②右击 Host-1 图标，点击【Console】打开 Host-1 的命令控制台，进行网络配置。配置命令如下所示。

```
>show ip
```

```
#查看 Host-1 的网络配置
>ip 10.0.100.1/24 10.30.101.254
#配置 Host-1 的 IP 地址与网关
>show ip
#查看 Host-m 的网络配置
>save
#可以看到 Host-m 的网络配置完成，将配置进行保存
```

③参照表 3-2 完成 Host-2、Host-3、Host-4、Host-5、Host-6 的网络配置。

3、接入交换机配置

①右击 SW-1 图标，点击【Start】开启该设备。

②右击 SW-1 图标，点击【Console】打开 SW-1 的命令控制台，进行网络配置。配置命令如下所示。

```
SW-1#vlan database
SW-1(vlan)#vlan 10
SW-1(vlan)#vlan 20
SW-1(vlan)#vlan 30
SW-1(vlan)#exit
SW-1#conf t
SW-1(config)#int f0/1
SW-1(config-if)#switchport mode access
SW-1(config-if)#switchport access vlan 10
SW-1(config-if)#int f0/2
SW-1(config-if)#switchport mode access
SW-1(config-if)#switchport access vlan 20
SW-1(config-if)#int f0/3
SW-1(config-if)#switchport mode access
SW-1(config-if)#switchport access vlan 30
SW-1(config-if)#exit
SW-1(config)#int f0/0
SW-1(config-if)#switchport trunk encapsulation dot1q
SW-1(config-if)#switchport mode trunk
SW-1(config-if)#exit
SW-1(config)#end
SW-1#write
```

③结合表 3-1 的具体内容，参考 SW-1 的配置方法，完成 SW-2 的网络配置。并将 SW-2 的配置命令填写到表 3-5 中。

表 3-5 SW-2 配置命令

4、路由交换机配置

①右击 RS-1 图标，点击【Start】开启该设备。

②右击 RS-1 图标，点击【Console】打开 RS-1 的命令控制台，进行网络配置。配置命令如下所示。

```
RS-1#vlan database
RS-1(vlan)#vlan 10
RS-1(vlan)#vlan 20
RS-1(vlan)#vlan 30
RS-1(vlan)#exit
RS-1#conf t
RS-1(config)#int f2/1
RS-1(config-if)#switchport trunk encapsulation dot1q
RS-1(config-if)#switchport mode trunk
RS-1(config-if)#exit
RS-1(config)#int f2/2
RS-1(config-if)#switchport trunk encapsulation dot1q
RS-1(config-if)#switchport mode trunk
RS-1(config-if)#exit
RS-1(config)#int f2/0
RS-1(config-if)#no switchport
RS-1(config-if)ip add 10.0.107.1 255.255.255.0
RS-1(config-if)exit
RS-1(config)#ip routing
RS-1 (config)#ip route 10.0.104.0 255.255.255.0 10.0.107.2
RS-1 (config)#ip route 10.0.105.0 255.255.255.0 10.0.107.2
RS-1 (config)#ip route 10.0.106.0 255.255.255.0 10.0.107.2
RS-1 (config)#ip route 10.0.108.0 255.255.255.252 10.0.107.2
RS-1 (config)#exit
RS-1#write
```

5、局部网络连通性测试

通过 Ping 命令对 Host-1、Host-2、Host-3、Host-4、Host-5、Host-6 进行连通性测试，并填写表 3-6。

表 3-6 连通性测试

序号	请求主机	接入位置	响应主机	接入位置	Ping 测试结果
1	Host-1	SW-1 e0/1	Host-2	SW-1 e0/2	
2	Host-1	SW-1 e0/1	Host-3	SW-1 e0/3	
3	Host-1	SW-1 e0/1	Host-4	SW-2 e0/1	
4	Host-1	SW-1 e0/1	Host-5	SW-2 e0/2	
5	Host-1	SW-1 e0/1	Host-6	SW-2 e0/3	
6	Host-2	SW-1 e0/2	Host-1	SW-1 e0/1	
7	Host-2	SW-1 e0/2	Host-3	SW-1 e0/3	
8	Host-2	SW-1 e0/2	Host-4	SW-2 e0/1	

9	Host-2	SW-1 e0/2	Host-5	SW-2 e0/2	
10	Host-2	SW-1 e0/2	Host-6	SW-2 e0/3	
11	Host-3	SW-1 e0/1	Host-1	SW-1 e0/1	
12	Host-3	SW-1 e0/3	Host-2	SW-1 e0/2	
13	Host-3	SW-1 e0/3	Host-4	SW-2 e0/1	
14	Host-3	SW-1 e0/3	Host-5	SW-2 e0/2	
15	Host-3	SW-1 e0/3	Host-6	SW-2 e0/3	
16	Host-4	SW-2 e0/1	Host-1	SW-1 e0/1	
17	Host-4	SW-2 e0/1	Host-2	SW-1 e0/2	
18	Host-4	SW-2 e0/1	Host-3	SW-1 e0/3	
19	Host-4	SW-2 e0/1	Host-5	SW-2 e0/2	
20	Host-4	SW-2 e0/2	Host-6	SW-2 e0/3	
21	Host-5	SW-2 e0/2	Host-1	SW-1 e0/1	
22	Host-5	SW-2 e0/2	Host-2	SW-1 e0/2	
23	Host-5	SW-2 e0/2	Host-3	SW-1 e0/3	
24	Host-5	SW-2 e0/2	Host-4	SW-2 e0/1	
25	Host-5	SW-2 e0/2	Host-6	SW-2 e0/3	
26	Host-6	SW-2 e0/3	Host-1	SW-1 e0/1	
27	Host-6	SW-2 e0/3	Host-2	SW-1 e0/2	
28	Host-6	SW-2 e0/3	Host-3	SW-1 e0/3	
29	Host-6	SW-2 e0/3	Host-4	SW-2 e0/1	
30	Host-6	SW-2 e0/3	Host-5	SW-2 e0/2	

6、右侧局域网建设

结合表 3-1 至表 3-4 的具体内容，结合左侧局域网的配置，完成 Host-7、Host-8、Host-9、Host-10、Host-11、Host-12、SW-3、SW-4、RS-2 的配置，并进行连通性测试，填写表 3-8。并将 RS-2 的配置命令填写到表 3-7 中。

表 3-7 RS-2 配置命令

表 3-8 连通性测试

序号	请求主机	接入位置	响应主机	接入位置	Ping 测试结果
1	Host-7	SW-3 e0/1	Host-8	SW-3 e0/2	
2	Host-7	SW-3 e0/1	Host-9	SW-3 e0/3	
3	Host-7	SW-3 e0/1	Host-10	SW-4 e0/1	
4	Host-7	SW-3 e0/1	Host-11	SW-4 e0/2	
5	Host-7	SW-3 e0/1	Host-12	SW-4 e0/3	
6	Host-8	SW-3 e0/2	Host-7	SW-3 e0/1	
7	Host-8	SW-3 e0/2	Host-9	SW-3 e0/3	
8	Host-8	SW-3 e0/2	Host-10	SW-4 e0/1	
9	Host-8	SW-3 e0/2	Host-11	SW-4 e0/2	
10	Host-8	SW-3 e0/2	Host-12	SW-4 e0/3	
11	Host-9	SW-3 e0/1	Host-7	SW-3 e0/1	
12	Host-9	SW-3 e0/3	Host-8	SW-3 e0/2	
13	Host-9	SW-3 e0/3	Host-10	SW-4 e0/1	
14	Host-9	SW-3 e0/3	Host-11	SW-4 e0/2	
15	Host-9	SW-3 e0/3	Host-12	SW-4 e0/3	
16	Host-10	SW-4 e0/1	Host-7	SW-3 e0/1	
17	Host-10	SW-4 e0/1	Host-8	SW-3 e0/2	
18	Host-10	SW-4 e0/1	Host-9	SW-3 e0/3	
19	Host-10	SW-4 e0/1	Host-11	SW-4 e0/2	
20	Host-10	SW-4 e0/2	Host-12	SW-4 e0/3	
21	Host-11	SW-4 e0/2	Host-7	SW-3 e0/1	
22	Host-11	SW-4 e0/2	Host-8	SW-3 e0/2	
23	Host-11	SW-4 e0/2	Host-9	SW-3 e0/3	
24	Host-11	SW-4 e0/2	Host-10	SW-4 e0/1	
25	Host-11	SW-4 e0/2	Host-12	SW-4 e0/3	
26	Host-12	SW-4 e0/3	Host-7	SW-3 e0/1	
27	Host-12	SW-4 e0/3	Host-8	SW-3 e0/2	
28	Host-12	SW-4 e0/3	Host-9	SW-3 e0/3	
29	Host-12	SW-4 e0/3	Host-10	SW-4 e0/1	
30	Host-12	SW-4 e0/3	Host-11	SW-4 e0/2	

7、路由器配置

①右击 RT-1 图标，点击【Start】开启该设备。

②右击 RT-1 图标，点击【Console】打开 RT-1 的命令控制台，进行网络配置。配置命令如下所示。

```
RT-1#conf t
RT-1(config)#int e1/1
RT-1(config-if)#no shutdown
RT-1(config-if)#ip add 10.0.107.2 255.255.255.0
RT-1(config-if)#exit
RT-1(config)#int e1/2
RT-1(config-if)#no shutdown
RT-1(config-if)#ip add 10.0.108.2 255.255.255.0
RT-1(config-if)#exit
RT-1(config)#ip route 10.0.104.0 255.255.255.0 10.0.108.1
RT-1(config)#ip route 10.0.105.0 255.255.255.0 10.0.108.1
RT-1(config)#ip route 10.0.106.0 255.255.255.0 10.0.108.1
RT-1(config)#ip route 10.0.101.0 255.255.255.0 10.0.107.1
RT-1(config)#ip route 10.0.102.0 255.255.255.0 10.0.107.1
RT-1(config)#ip route 10.0.103.0 255.255.255.0 10.0.107.1
RT-1(config)#exit
RT-1#write
```

8、整体网络连通性测试

Host-1、Host-2、Host-3、Host-4、Host-5、Host-6、Host-7、Host-8、Host-9、Host-10、Host-11、Host-12、RT-1、RS-1、RS-2、SW-1、SW-2、SW-3、SW-4 的配置完成后，通过 Ping 命令进行主机的连通性测试，并填写表 3-9。

表 3-9 整体连通性测试

序号	请求主机	接入位置	响应主机	接入位置	Ping 测试结果
1	Host-1	SW-1 e0/1	Host-2	SW-1 e0/2	
2	Host-1	SW-1 e0/1	Host-3	SW-1 e0/3	
3	Host-1	SW-1 e0/1	Host-4	SW-2 e0/1	
4	Host-1	SW-1 e0/1	Host-5	SW-2 e0/2	
5	Host-1	SW-1 e0/1	Host-6	SW-2 e0/3	
6	Host-1	SW-1 e0/1	Host-7	SW-3 e0/1	
7	Host-1	SW-1 e0/1	Host-8	SW-3 e0/2	
8	Host-1	SW-1 e0/1	Host-9	SW-3 e0/3	
9	Host-1	SW-1 e0/1	Host-10	SW-4 e0/1	
10	Host-1	SW-1 e0/1	Host-11	SW-4 e0/2	
11	Host-1	SW-1 e0/1	Host-12	SW-4 e0/3	
12	Host-2	SW-1 e0/2	Host-1	SW-1 e0/1	
13	Host-2	SW-1 e0/2	Host-3	SW-1 e0/3	
...	...	...	...	...	...

128	Host-12	SW-4 e0/3	Host-7	SW-3 e0/1	
129	Host-12	SW-4 e0/3	Host-8	SW-3 e0/2	
130	Host-12	SW-4 e0/3	Host-9	SW-3 e0/3	
131	Host-12	SW-4 e0/3	Host-10	SW-4 e0/1	
132	Host-12	SW-4 e0/3	Host-11	SW-4 e0/2	

八、实验分析

1、路由器的工作原理

（1）路由器的工作原理是什么？

（2）如何查看路由器的路由表？

（3）路由器、交换机、路由交换机在功能上有什么区别？主要应用场景是什么？

2、网络测试

（1）常见的网络测试工具有 PING 和 TraceRoute，其工作原理和应用有哪些区别？

（2）网络测试工具还有哪些？

实验四：动态路由协议

一、实验目的

1、进一步理解路由器的工作原理；

2、掌握 RIP 的基本原理和实现；

3、掌握 OSPF 的基本原理和实现。

二、实验学时

2 学时

三、实验类型

综合型

四、实验需求

1、硬件

每人配备计算机 1 台。

2、软件

Windows 7 以上操作系统，安装 GNS3 网络仿真与 VirtualBox 虚拟化软件，安装 Putty 软件。

3、网络

实验室局域网支持，能够访问校园网。

4、工具

无。

五、实验理论

1、计算机网络的基本理论；

2、交换机和路由器的工作原理；

3、动态路由算法；

4、内部网关协议（RIP、OSPF）。

六、实验任务

1、基于网络规划，完成局域网建设；

2、完成路由器的配置，实现 RIP；

3、完成路由器的配置，实现 OSPF；

4、完成网络通信测试。

七、实验内容及步骤

1、RIP 的实现

（1）拓扑设计

本实验采用 2 台交换机（SW-1，SW-2），2 台路由器（RT-1、RT-2），4 台主机(Host-1、Host-2、Host-3、Host-4)，主机通过GNS3中自带的VPCS虚拟主机实现，网络拓扑结构如图 4-1 所示。

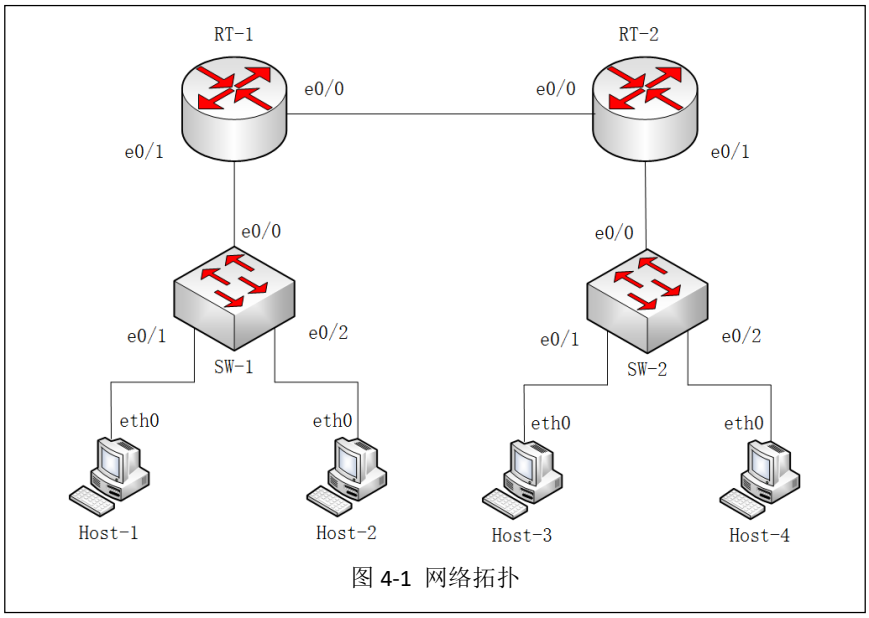

图 4-1 网络拓扑

（2）按照拓扑结构设计，在 GNS3 环境下完成局域网建设，如图 4-2 所示。

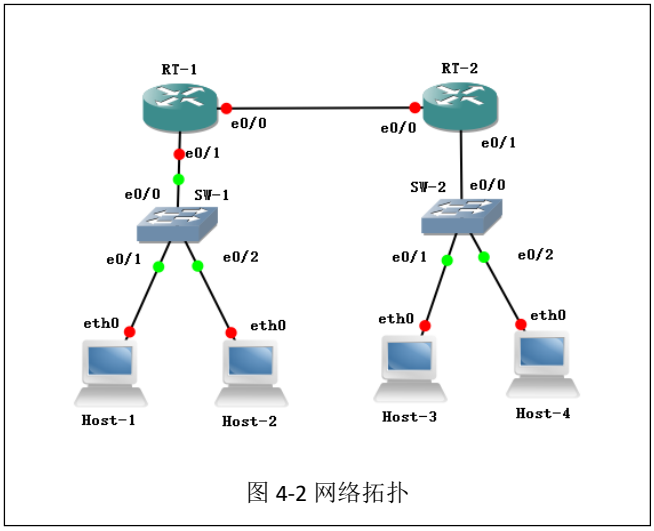

图 4-2 网络拓扑

（3）网络地址规划见表 4-1 所示。

表 4-1 网络地址规划表

序号	设备名称	网络配置	网关	接入位置
1	Host-1	192.168.1.1/24	192.168.1.254	SW-1 e0/1
2	Host-2	192.168.1.2/24	192.168.1.254	SW-1 e0/2
3	Host-3	172.16.1.1/24	172.16.1.254	SW-2 e0/1
4	Host-4	172.16.1.2/24	172.16.1.254	SW-2 e0/2

（4）对主机进行网络配置。

①右击 Host-1 图标，点击【Start】开启该设备。

②右击 Host-1 图标，点击【Console】打开 Host-1 的命令控制台，进行网络配置。配置命令如下所示。

```
>show ip
#查看 Host-1 的网络配置
>ip 192.168.1.1/24 192.168.1.254
#配置 Host-1 的 IP 地址与网关
>show ip
#查看 Host-1 的网络配置
>save
#可以看到 Host-1 的网络配置完成，将配置进行保存
```

③结合表 4-1 的具体内容，参考 Host-1 的配置方法，完成 Host-2、Host-3、Host-4 的网络配置。

（5）配置路由器 RT-1 与 RT-2

配置 RT-1 的 e0/0 端口 IP 地址为 10.0.0.1/30，e0/1 端口 IP 地址为 192.168.1.254/24，并支持 RIP，具体配置命令如下所示。

```
RT-1#configure terminal
#进入配置模式
RT-1(config)#interface e0/0
RT-1(config-if)#no switchport（若安装镜像时网络接口配有 NM-4E 则为 no shutdown）
RT-1(config-if)#ip address 10.0.0.1 255.255.255.252
#配置 e0/0 的 IP 地址
RT-1(config-if)#exit
RT-1(config)#interface e0/1
RT-1(config-if)# no switchport（若安装镜像时网络接口配有 NM-4E 则为 no shutdown）
RT-1(config-if)#ip address 192.168.1.254 255.255.255.0
#配置 e0/1 的 IP 地址
RT-1(config-if)#exit
RT-1(config)#router rip
#配置 rip
RT-1(config-router)#version 2
#rip 版本为 v2
RT-1(config-router)#network 192.168.1.0
RT-1(config-router)#network 10.0.0.0
#配置 rip 网络
```

配置 RT-2 的 e0/0 端口 IP 地址为 10.0.0.2/30，e0/1 端口 IP 地址为 172.16.1.254/24，并支持 RIP，具体配置命令如下所示。

```
RT-2#configure terminal
#进入配置模式 in
RT-2(config)#interface e0/0
RT-2(config-if)# no switchport（若安装镜像时网络接口配有 NM-4E 则为 no shutdown）
RT-2(config-if)#ip address 10.0.0.2 255.255.255.252
```

```
#配置 e0/0 的 IP 地址
RT-2(config-if)#exit
RT-2config)#interface e0/1
RT-2(config-if)# no switchport（若安装镜像时网络接口配有 NM-4E 则为 no shutdown）
RT-2(config-if)#ip address 172.16.1.254 255.255.255.0
#配置 e0/1 的 IP 地址
RT-2(config-if)#exit
RT-2(config)#router rip
#配置 rip
RT-2(config-router)#version 2
#rip 版本为 v2
RT-2(config-router)#network 172.16.1.0
RT-2(config-router)#network 10.0.0.0
#配置 rip 网络
```

查看 RT-1 路由表信息如下所示。

```
RT-1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

R     172.16.0.0/16 [120/1] via 10.0.0.2, 00:00:26, Ethernet0/0
      10.0.0.0/30 is subnetted, 1 subnets
C        10.0.0.0 is directly connected, Ethernet0/0
C     192.168.1.0/24 is directly connected, Ethernet0/1
```

查看 RT-2 路由表信息如下所示。

```
RT-2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

      172.16.0.0/24 is subnetted, 1 subnets
C        172.16.1.0 is directly connected, Ethernet0/1
      10.0.0.0/30 is subnetted, 1 subnets
C        10.0.0.0 is directly connected, Ethernet0/0
R     192.168.1.0/24 [120/1] via 10.0.0.1, 00:00:14, Ethernet0/0
```

（6）连通性测试

通过 Ping 命令进行网络通信测试，并将结果填写到表 4-2。

表 4-2 网络通信测试结果

序号	请求主机	接入位置	响应主机	接入位置	Ping 测试结果
1	Host-1	SW-1 e0/1	Host-2	SW-1 e0/2	
2	Host-1	SW-1 e0/1	Host-3	SW-2 e0/1	
3	Host-1	SW-1 e0/1	Host-4	SW-2 e0/2	
4	Host-2	SW-1 e0/2	Host-1	SW-1 e0/1	
5	Host-2	SW-1 e0/2	Host-3	SW-2 e0/1	
6	Host-2	SW-1 e0/2	Host-4	SW-2 e0/2	
7	Host-3	SW-2 e0/1	Host-1	SW-1 e0/1	
8	Host-3	SW-2 e0/1	Host-2	SW-1 e0/2	
9	Host-3	SW-2 e0/1	Host-4	SW-2 e0/2	
10	Host-4	SW-2 e0/2	Host-1	SW-1 e0/1	
11	Host-4	SW-2 e0/2	Host-2	SW-1 e0/2	
12	Host-4	SW-2 e0/2	Host-3	SW-2 e0/1	

2、OSPF 的实现

（1）拓扑设计

本实验采用 2 台交换机（SW-1，SW-2），3 台路由器（RT-1、RT-2、RT-3），4 台主机(Host-1、Host-2、Host-3、Host-4)，主机通过 GNS3 中自带的 VPCS 虚拟主机实现，网络拓扑结构如图 4-3 所示。

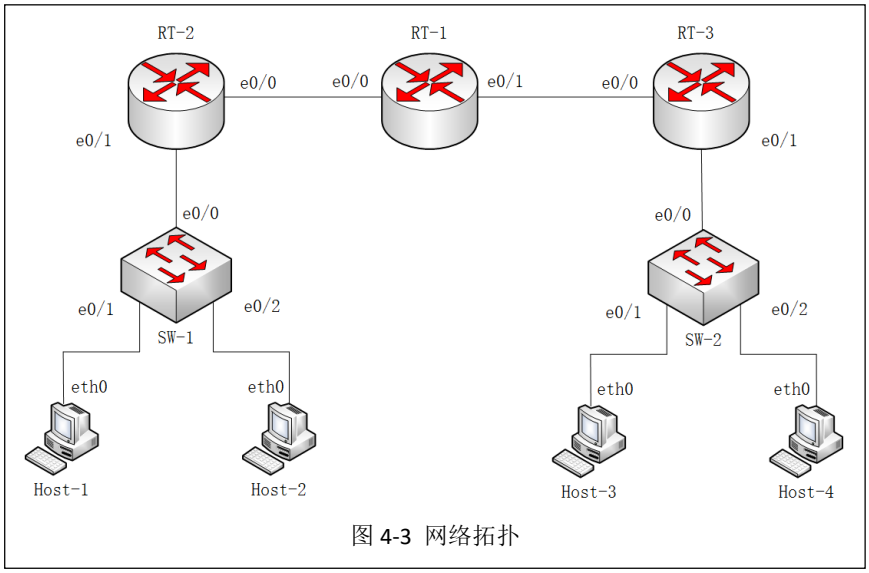

图 4-3 网络拓扑

（2）按照拓扑结构的设计，在 GNS3 环境下完成局域网建设，如图 4-4 所示。

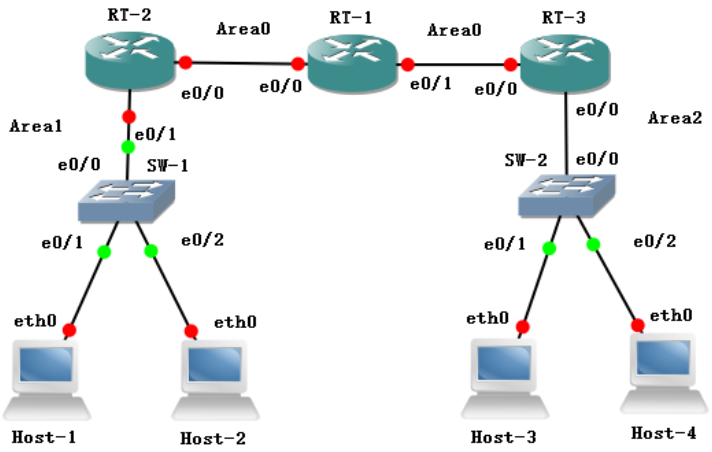

图 4-4 网络拓扑

（3）网络地址规划见表 4-3 所示。

表 4-3 网络地址规划表

序号	设备名称	网络配置	网关	接入位置
1	Host-1	192.168.1.1/24	192.168.1.254	SW-1 e0/1
2	Host-2	192.168.1.2/24	192.168.1.254	SW-1 e0/2
3	Host-3	172.16.1.1/24	172.16.1.254	SW-2 e0/1
4	Host-4	172.16.1.2/24	172.16.1.254	SW-2 e0/2

（4）结合表 4-3 的具体内容，完成 Host-1、Host-2、Host-3、Host-4 的网络配置。

（5）配置路由器 RT-1、RT-2、RT-3

配置 RT-1 的 e0/0 端口 IP 地址为 10.0.0.1/30，e0/1 端口 IP 地址为 10.0.1.1/30，并支持 OSPF，具体配置命令如下所示。

```
RT-1#configure terminal
#进入配置模式
RT-1(config)#interface e0/0
RT-1(config-if)#no shutdown
RT-1(config-if)#ip address 10.0.0.1 255.255.255.252
#配置 e0/0 的 IP 地址
RT-1(config-if)#exit
RT-1(config)#interface e0/1
RT-1(config-if)#no shutdown
RT-1(config-if)#ip address 10.0.1.1 255.255.255.252
#配置 e0/1 的 IP 地址
RT-1(config-if)#exit
RT-1(config)#router ospf 100
#配置 ospf
RT-1(config-router)#network 10.0.0.0 255.255.255.252 area 0
RT-1(config-router)#network 10.0.1.0 255.255.255.252 area 0
```

配置 RT-2 的 e0/0 端口 IP 地址为 10.0.0.2/30，e0/1 端口 IP 地址为 192.168.1.254/24，并

支持 OSPF，具体配置命令如下所示。

```
RT-2#configure terminal
#进入配置模式
RT-2(config)#interface e0/0
RT-2(config-if)#no shutdown
RT-2(config-if)#ip address 10.0.0.2 255.255.255.252
#配置 e0/0 的 IP 地址
RT-2(config-if)#exit
RT-2(config)#interface e0/1
RT-2(config-if)#no shutdown
RT-2(config-if)#ip address 192.168.1.254 255.255.255.0
#配置 e010 的 IP 地址
RT-2(config-if)#exit
RT-2(config)#router ospf 200
RT-2(config-router)#network 192.168.1.0 255.255.255.0 area 1
RT-2(config-router)#network 10.0.0.0 255.255.255.252 area 0
```

配置 RT-3 的 e0/0 端口 IP 地址为 10.0.1.2/30，e0/1 端口 IP 地址为 172.16.1.254/24，并支持 OSPF，具体配置命令如下所示。

```
RT-3#configure terminal
#进入配置模式
RT-3(config)#interface e0/0
RT-3(config-if)#no shutdown
RT-3(config-if)#ip address 10.0.1.2 255.255.255.252
#配置 e0/0 的 IP 地址
RT-3(config-if)#exit
RT-3config)#interface e0/1
RT-3(config-if)#no shutdown
RT-3(config-if)#ip address 172.16.1.254 255.255.255.0
#配置 e0/0 的 IP 地址
RT-3(config-if)#exit
RT-3(config)#router ospf 300
#配置 ospf
RT-3(config-router)#network 172.16.1.0 255.255.255.0 area 2
RT-3(config-router)#network 10.0.1.0 255.255.255.252 area 0
```

查看 RT-1 路由表信息如下所示。

```
RT-1#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

     172.16.0.0/24 is subnetted, 1 subnets
O IA     172.16.1.0 [110/20] via 10.0.1.2, 00:01:30, Ethernet0/1
```

```
        10.0.0.0/30 is subnetted, 2 subnets
C           10.0.0.0 is directly connected, Ethernet0/0
C           10.0.1.0 is directly connected, Ethernet0/1
O IA 192.168.1.0/24 [110/20] via 10.0.0.2, 00:01:30, Ethernet0/0
```

查看 RT-2 路由表信息如下所示。

```
RT-2#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
           D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
           N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
           E1 - OSPF external type 1, E2 - OSPF external type 2
           i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
           ia - IS-IS inter area, * - candidate default, U - per-user static route
           o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

        172.16.0.0/24 is subnetted, 1 subnets
O IA       172.16.1.0 [110/30] via 10.0.0.1, 00:02:03, Ethernet0/0
        10.0.0.0/30 is subnetted, 2 subnets
C           10.0.0.0 is directly connected, Ethernet0/0
O           10.0.1.0 [110/20] via 10.0.0.1, 00:02:03, Ethernet0/0
C       192.168.1.0/24 is directly connected, Ethernet0/1
```

查看 RT-3 路由表信息如下所示。

```
RT-3#show ip route
Codes: C - connected, S - static, R - RIP, M - mobile, B - BGP
           D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
           N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
           E1 - OSPF external type 1, E2 - OSPF external type 2
           i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
           ia - IS-IS inter area, * - candidate default, U - per-user static route
           o - ODR, P - periodic downloaded static route

Gateway of last resort is not set

        172.16.0.0/24 is subnetted, 1 subnets
C           172.16.1.0 is directly connected, Ethernet0/1
        10.0.0.0/30 is subnetted, 2 subnets
O           10.0.0.0 [110/20] via 10.0.1.1, 00:02:30, Ethernet0/0
C           10.0.1.0 is directly connected, Ethernet0/0
O IA 192.168.1.0/24 [110/30] via 10.0.1.1, 00:02:30, Ethernet0/0
```

（6）连通性测试

通过 Ping 命令进行网络通信测试，并将结果填写到表 4-4。

表 4-4 网络通信测试结果

序号	请求主机	接入位置	响应主机	接入位置	Ping 测试结果
1	Host-1	SW-1 e0/1	Host-2	SW-1 e0/2	
2	Host-1	SW-1 e0/1	Host-3	SW-2 e0/1	

3	Host-1	SW-1 e0/1	Host-4	SW-2 e0/2	
4	Host-2	SW-1 e0/2	Host-1	SW-1 e0/1	
5	Host-2	SW-1 e0/2	Host-3	SW-2 e0/1	
6	Host-2	SW-1 e0/2	Host-4	SW-2 e0/2	
7	Host-3	SW-2 e0/1	Host-1	SW-1 e0/1	
8	Host-3	SW-2 e0/1	Host-2	SW-1 e0/2	
9	Host-3	SW-2 e0/1	Host-4	SW-2 e0/2	
10	Host-4	SW-2 e0/2	Host-1	SW-1 e0/1	
11	Host-4	SW-2 e0/2	Host-2	SW-1 e0/2	
12	Host-4	SW-2 e0/2	Host-3	SW-2 e0/1	

八、实验分析

1、动态路由协议

（1）动态路由的工作原理是什么？

（2）静态路由与动态路由有什么区别？

2、RIP 与 OSPF

（1）以高校校园网为例，其应选用 RIP 还是 OSPF 作为学校的路由交换协议？为什么？

（2）RIP 是否会被 OSPF 替代？为什么？

3、自动汇聚

（1）路由器是如何进行路由自动汇聚的？其工作过程是什么？

（2）请介绍常用的路由自动汇聚算法及其工作原理。

实验五：ARP 协议分析

一、实验目的

1、掌握报文分析的基本方法；

2、掌握 Wireshark 软件的基本使用方法；

3、掌握使用 Wireshark 进行数据包抓取和分析的基本操作；

4、理解 ARP 报文格式和各字段含义；

5、理解 ARP 协议的通信过程。

二、实验学时

2 学时

三、实验类型

验证型

四、实验需求

1、硬件

每人配备计算机 1 台。

2、软件

Windows 7 以上操作系统，安装 Wireshark 网络嗅探软件。

3、网络

实验室局域网支持，能够访问校园网。

4、工具

无。

五、实验理论

1、网络嗅探的工作原理；

2、Wireshark 软件的基本使用方法；

3、ARP 协议原理与报文结构；

4、请查阅资料，列举几种常见的网络分析工具，并填写表 5-1。

表 5-1 网络分析工具对比分析一览表

序号	软件名称	版本号	软件开发商	安装环境
1				
…				

六、实验任务

1、完成 Wireshark 软件的安装和基本操作的学习；

2、完成 ARP 报文结构的分析；

3、完成 ARP 通信过程的分析。

七、实验内容及步骤

1、Wireshark 的基本操作

（1）下载软件包

可通过官方网站（http://www.wireshark.org）获得 Wireshark 软件安装程序；

可通过本课程网站（http://network.ke.51xueweb.cn）下载本教程所使用的 Wireshark 软件版本。

（2）安装软件

①双击 Wireshark 安装程序，进入如图 5-1 所示的 Wireshark 安装界面，点击【Next >】开始进行安装。在安装过程中，会提示用户选择安装相关组件程序，选择默认安装组件，具体如图 5-2 所示。

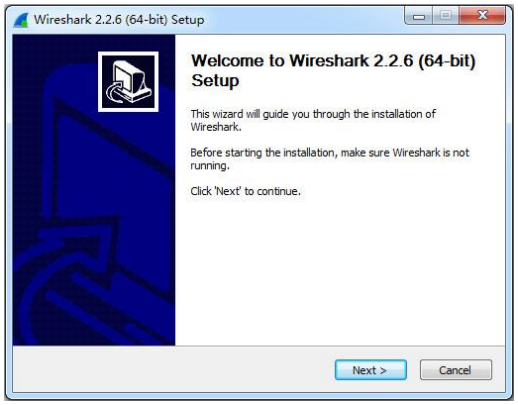

图 5-1 安装提示

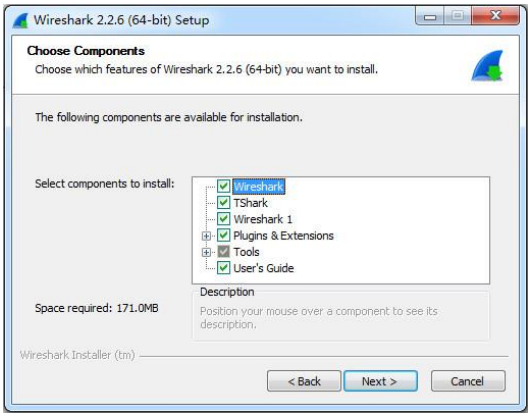

图 5-2 组件选择

②选择自定义配置，如创建快捷方式和文件扩展等，如图 5-3 所示。

③用户可使用默认的 Wireshark 安装目录，也可自行修改安装路径，如图 5-4 所示。

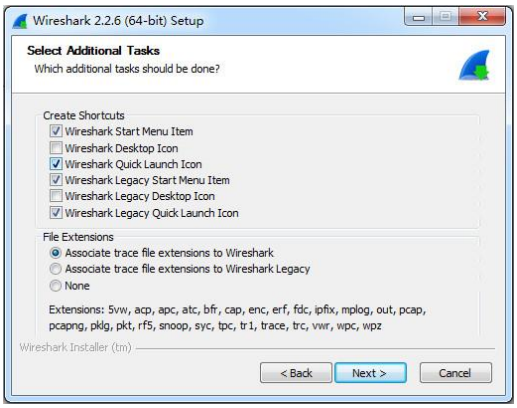

图 5-3 选择自定义配置

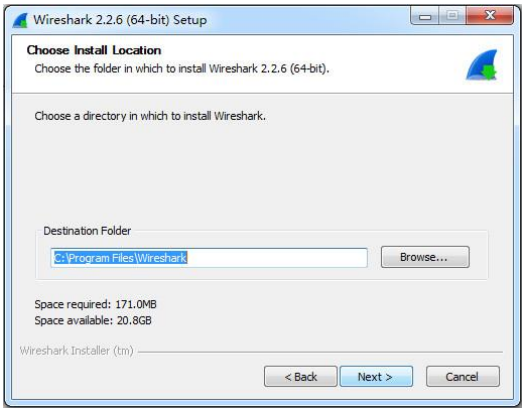

图 5-4 安装路径

④选择安装 WinPcap 软件。WinPcap 是针对 Windows 32 平台上的抓包和网络分析的一个框架软件，是 Windows 平台下免费、公共的网络访问系统。选择安装该框架软件，如图 5-5 所示，点击【Next >】继续进行 Wireshark 软件安装。

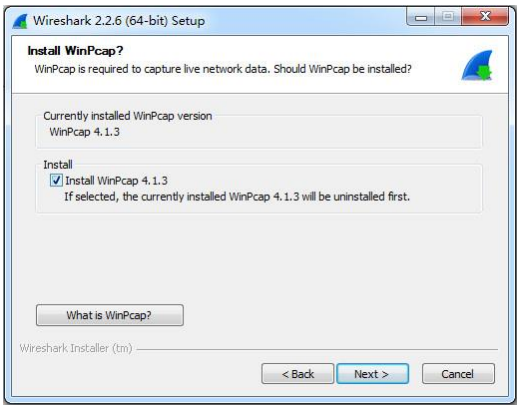

图 5-5 选择安装 Winpcap

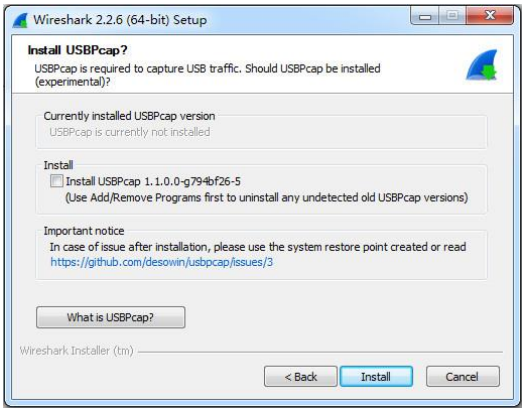

图 5-6 不安装 USBinpcap

⑤不安装 USBPcap 软件。USBPcap 是针对 USB 设备进行分析的一个框架软件，本实验不针对 USB 设备进行网络分析，所以不安装该框架，如图 5-6 所示。点击【Install】，开始进行 Wireshark 软件安装。

⑥Wireshark 软件在安装过程中将安装 WinPcap 框架，根据默认安装提示，完成该框架的安装，如图 5-7 所示。

⑦点击【Finish】完成 Wireshark 软件的安装，如图 5-8 所示。

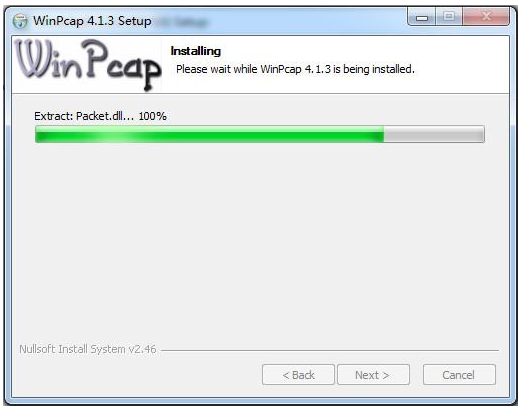

图 5-7 安装 Winpcap

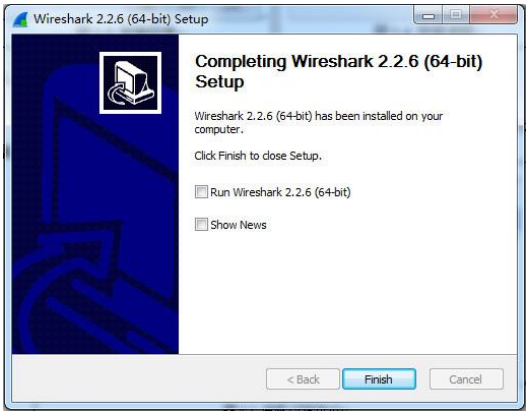

图 5-8 安装完成

⑧打开 Wireshark 软件，界面展示如图 5-9 所示，选择某一网卡适配器，选择【Start】，可查看该网卡上所传输的数据报文信息，如图 5-10 所示。

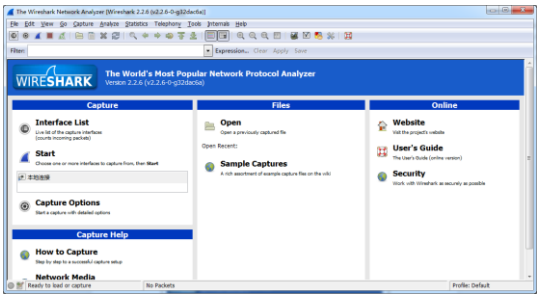

图 5-9 选择分析网卡

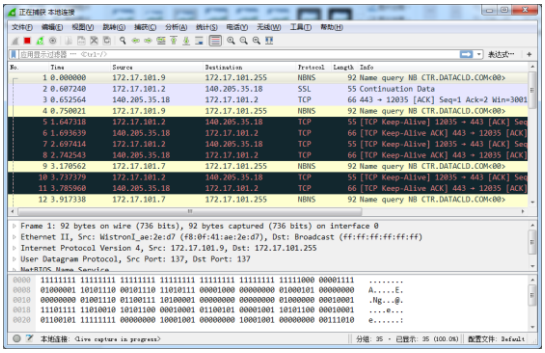

图 5-10 数据报文内容

2、ARP 数据包分析

（1）创建 ARP 协议抓包任务

打开 Wireshark，在【Filter】选项中输入报文过滤条件“arp”，选择【Start】，开始进行报文采集，如图 5-11 所示。

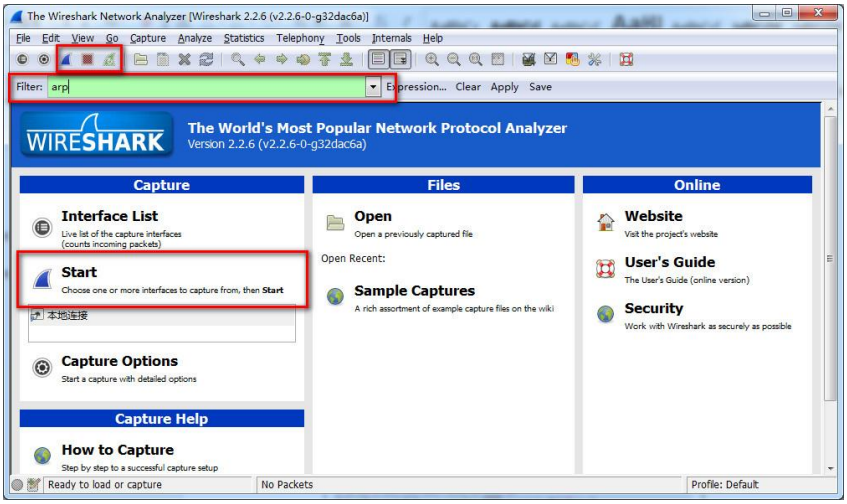

图 5-11 创建 ARP 协议抓包任务

（2）对数据包进行分析

在 Wireshark 的抓包窗体中，可以发现整个软件分为三个区域，如图 5-12 所示。上部分

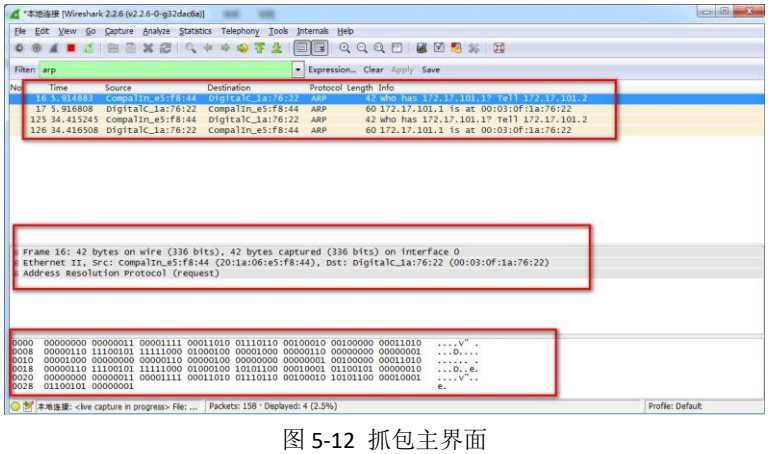

图 5-12 抓包主界面

为抓取的数据包，中间部分为数据详细分析，下部分为数据包的内容。

（3）从多条 ARP 协议数据报文中任意选择其中一条数据报文，对该数据报文进行详细分析，并填写表 5-2。

表 5-2 ARP 报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Hardware type		第　位		
2	Protocol type		第　位		
3	Hardware size		第　位		
4	Protocol size		第　位		
5	Opcode		第　位		
6	Sender MAC address		第　位		
7	Sender IP address		第　位		
8	Target MAC address		第　位		
9	Target IP address		第　位		
10	抓取数据包的详细内容：				

3、ARP 通信过程数据包分析

（1）创建 ARP 协议抓包任务

根据过程 2 中的方法获取 ARP 协议通信过程的数据包。

（2）ARP 请求报文分析

在 Wireshark 的抓包窗体中，选择一条请求数据报文进行详细分析，如图 5-13 所示，并填写表 5-3。

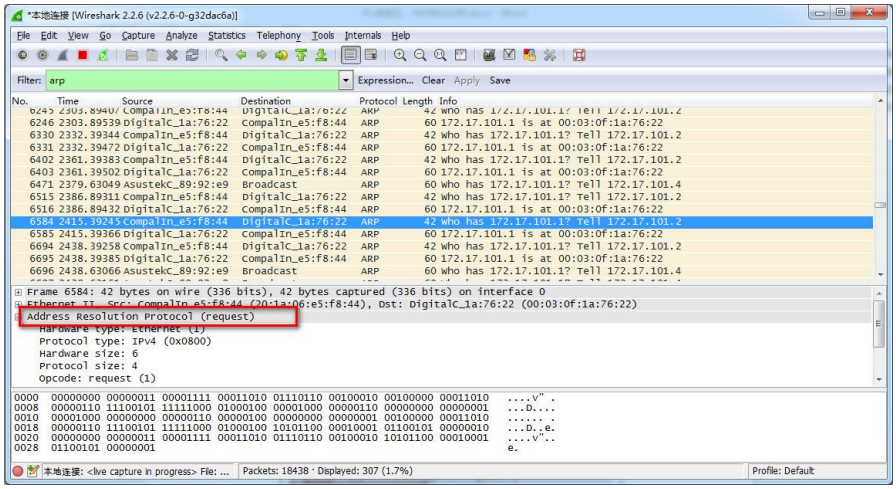

图 5-13 ARP 请求报文

表 5-3 ARP 请求报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Hardware type		第　位		
2	Protocol type		第　位		
3	Hardware size		第　位		
4	Protocol size		第　位		
5	Opcode		第　位		
6	Sender MAC address		第　位		
7	Sender IP address		第　位		
8	Target MAC address		第　位		
9	Target IP address		第　位		
10	抓取数据包的详细内容：				

（3）ARP 应答报文分析

在 Wireshark 的抓包窗体中，选择上述请求报文所对应的应答报文进行详细分析，如图 5-14 所示，并填写表 5-4。

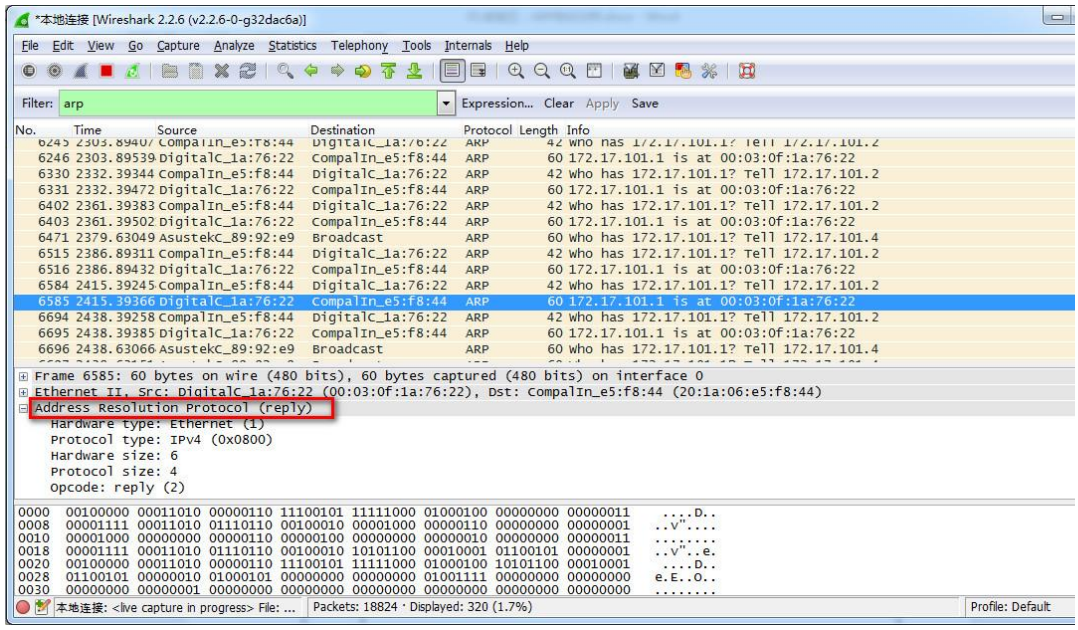

图 5-14 ARP 应答报文

表 5-4 ARP 应答报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Hardware type		第　位		
2	Protocol type		第　位		
3	Hardware size		第　位		
4	Protocol size		第　位		
5	Opcode		第　位		
6	Sender MAC address		第　位		
7	Sender IP address		第　位		
8	Target MAC address		第　位		
9	Target IP address		第　位		
10	抓取数据包的详细内容：				

（4）对比分析

根据 ARP 请求和应答的报文内容，比较两个数据报文内容的 5 个关键差别，并填

写表 5-5。

表 5-5 ARP 通信过程报文对比分析

序号	字段名称	请求报文		应答报文	
		字段值	字段表示信息	字段值	字段表示的信息
1					
2					
3					
4					
5					
6	对比描述详细内容：				

八、实验分析

1、ARP 原理

（1）ARP 的基本原理是什么？

（2）ARP 的主要作用是什么？

2、ARP 通信报文分析

（1）观察实验过程中捕获的多个 ARP 请求报文，观察这些报文的以太网目的地址是否相同，分析其原因？

（2）观察实验过程中捕获的多个 ARP 应答报文，观察这些报文的以太网目的地址是否相同，分析其原因？

实验六：UDP 与 TCP 协议分析

一、实验目的

1、理解 UDP 和 TCP 协议的基本原理；

2、理解 UDP 和 TCP 报文格式和各字段含义；

3、理解 TCP 协议的通信过程和状态变迁机制。

二、实验学时

2 学时

三、实验类型

验证型

四、实验需求

1、硬件

每人配备计算机 1 台。

2、软件

Windows 7 以上操作系统，安装 Wireshark 网络嗅探软件。

3、网络

实验室局域网支持，能够访问校园网。

4、工具

无。

五、实验理论

1、UDP 协议基本原理及其报文结构；

2、TCP 协议基本原理及其报文结构。

六、实验任务

1、完成 UDP 和 TCP 数据报文的采集；

2、完成 UDP 和 TCP 数据报文结构的分析；

3、完成 TCP 通信过程的报文分析。

七、实验内容及步骤

1、UDP 数据包分析

（1）获取数据报文

①打开 Wireshark，在【Filter】选项中输入报文过滤条件“udp”，选择【Start】，开始进行报文采集，如图 6-1 所示。

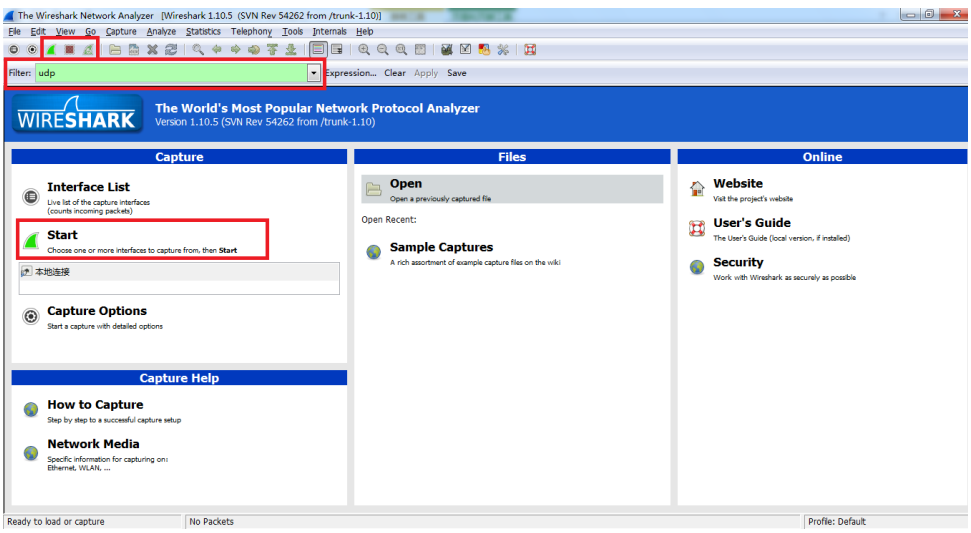

图 6-1 选择 UDP 协议

②在 Wireshark 的抓包窗体中，查看已获取的 UDP 数据报文，如图 6-2 所示。

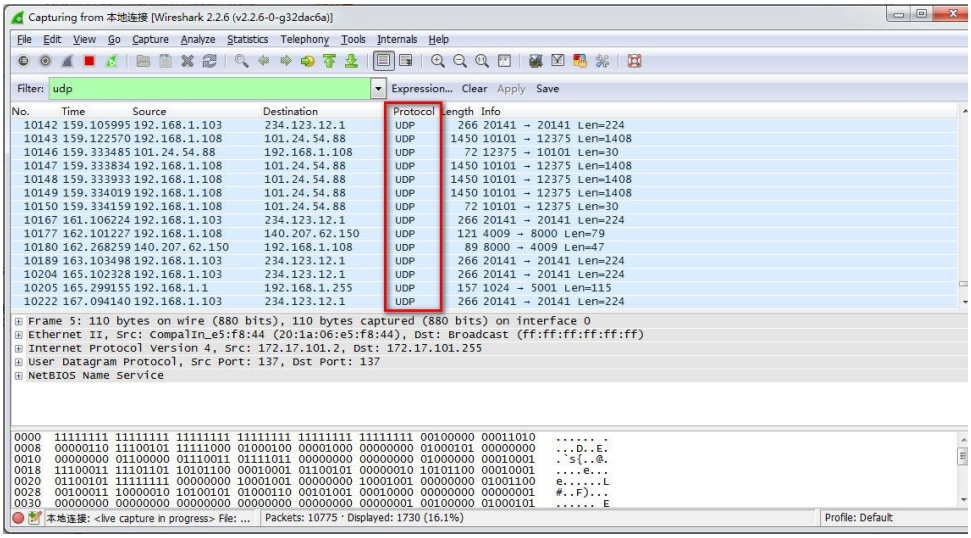

图 6-2 UDP 数据报文

（2）数据报文分析

从获取的UDP数据报文中任意选择其中一条数据报文，对该数据报文进行详细分析，并填写表 6-1。

表 6-1 UDP 协议报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Source Port		第 位		
2	Destination Port		第 位		
3	Length		第 位		
4	Checksum		第 位		

5	抓取数据包的详细内容：

2、TCP 数据包分析

（1）获取数据报文

①打开 Wireshark，在【Filter】选项中输入报文过滤条件“tcp”，选择【Start】，开始进行报文采集，如图 6-3 所示。

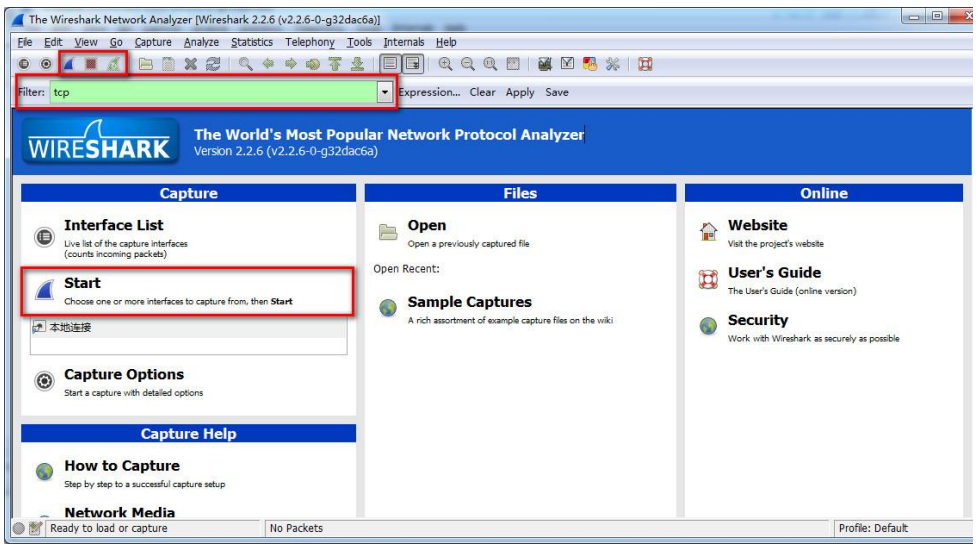

图 6-3 选择 TCP 协议

②在 Wireshark 的抓包窗体中，查看已获取的 TCP 数据报文，如图 6-4 所示。

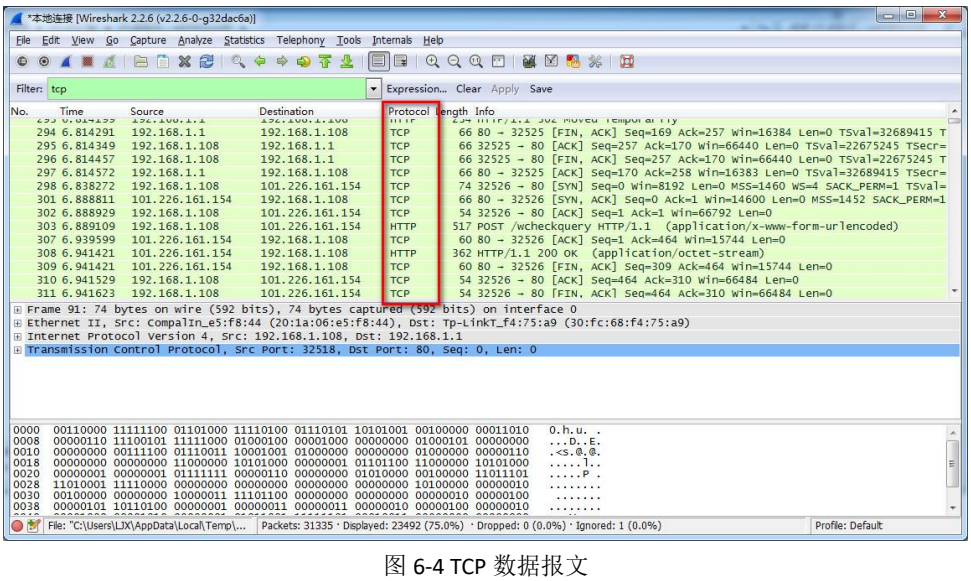

图 6-4 TCP 数据报文

（2）数据报文分析

从获取的 TCP 数据报文中任意选择其中一条数据报文，对该数据报文进行详细分析，并填写表 6-2。

表 6-2 TCP 协议报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Source Port		第　位		
2	Destination Port		第　位		
3	Sequence Number		第　位		
4	Acknowledgement Number		第　位		
5	Header Length		第　位		
6	Reserved		第　位		
7	Flags		第　位		
8	Window Size		第　位		
9	Checksum		第　位		
10	Urgent Pointer		第　位		
11	抓取数据包的详细内容：				

3、TCP 通信过程数据包分析

（1）TCP 建立连接报文分析

①获取建立连接报文。

a、打开 Wireshark，在【Filter】选项中输入报文过滤条件“tcp and ip.addr==192.168.1.103(本地主机 IP 地址)，选择【Start】，开始进行报文采集；

b、通过浏览器访问学校官网（http://www.hactcm.edu.cn），网站访问后，点击左上角红色按钮停止报文采集，如图 6-5 所示。

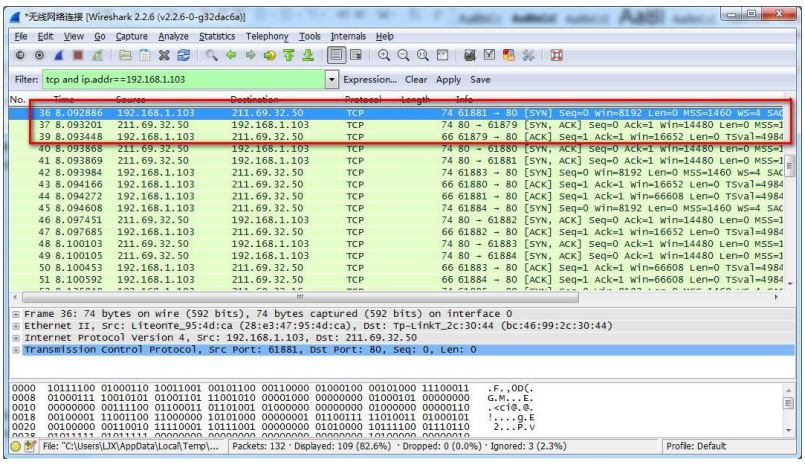

图 6-5 TCP 建立连接报文

②建立连接报文分析。

对抓取到的 TCP 报文进行分析，找到建立连接的三次握手机制所对应的报文，进行详细内容分析，并根据数据报文内容填写表 6-3。

表 6-3 TCP 建立连接报文分析

序号	字段名称	第一次	第二次	第三次	字段表示的信息
		字段值	字段值	字段值	
1	Source Port				
2	Destination Port				
3	Sequence Number				
4	Acknowledgement Number				
5	Header Length				
6	Reserved				
7	Flags				
8	Window Size				
9	Checksum				
10	Urgent Pointer				
11	抓取数据包的详细内容：				

（2）TCP 释放连接报文分析

①获取释放连接报文。关闭浏览器后，由于长时间未进行连接，将进行释放该TCP连接操作，可通过 Wireshark 网络分析工具，获取释放 TCP 连接的数据报文如图 6-6 所示。

②释放连接报文分析。

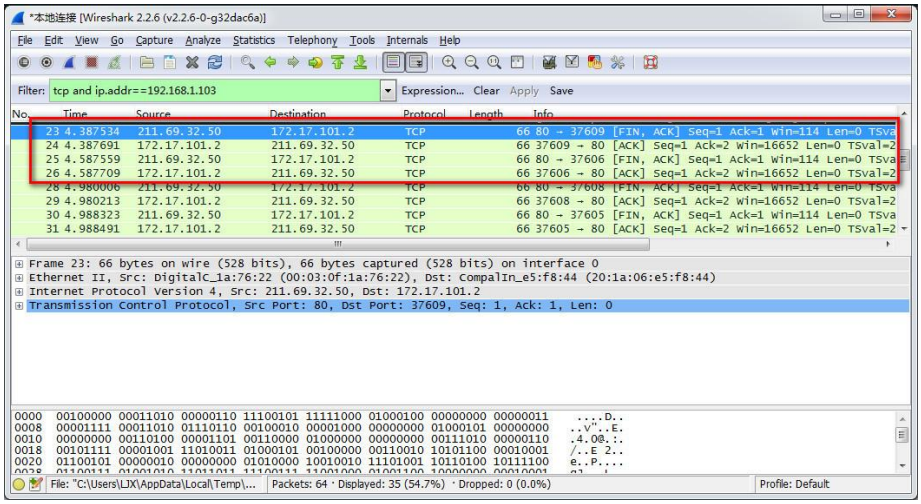

图 6-7 TCP 释放连接报文

对抓取到的TCP报文进行分析，找到释放连接所对应的数据报文，进行详细内容分析，并根据数据报文内容填写表 6-4。

表 6-4 释放连接报文分析

序号	字段名称	第一次	第二次	第三次	第四次	字段表示的信息
		字段值	字段值	字段值	字段值	
1	Source Port					
2	Destination Port					
3	Sequence Number					
4	Acknowledgement Number					
5	Header Length					
6	Reserved					
7	Flags					
8	Window Size					
9	Checksum					
10	Urgent Pointer					
11	抓取数据包的详细内容：					

（3）对比分析

根据 TCP 建立连接和释放连接的报文结构，比较两个过程数据报结构的 6 个关键差别，并填写表 6-5。

表 6-5 TCP 通信过程报文对比分析

序号	字段名称	请求连接报文		释放连接报文	
		字段值	字段表示信息	字段值	字段表示的信息
1					
2					
3					
4					
5					
6					
7	对比描述详细内容：				

八、实验分析

1、UDP 报文和 TCP 报文结构有何区别？

（1）UDP 报文和 TCP 报文结构上有什么不同？

（2）UDP 协议和 TCP 协议的不同之处是什么？

2、如何找到欲分析的数据报文？

（1）网络抓包时如何找到指定协议的数据报文？

（2）网络抓包时如何找到指定来源和目的地址的数据报文？

（3）网络抓包时如何找到指定套接字的数据报文？

（4）如何从众多的 TCP 数据报文中找到建立连接和释放连接的数据报文？

3、聊天工具使用的传输协议

（1）使用 TCP 传输协议的聊天工具有哪些，使用 UDP 传输协议的聊天工具有哪些？

（2）QQ 软件发送消息和发送文件使用的传输协议是否一样？分别是什么？

（3）软件开发者在开发软件时如何选取软件使用的传输协议？

实验七：DNS 报文分析

一、实验目的

1、理解 DNS 的基本原理；

2、理解 DNS 报文格式和各字段含义；

3、理解 DNS 解析的通信过程。

二、实验学时

2 学时

三、实验类型

验证型

四、实验需求

1、硬件

每人配备计算机 1 台。

2、软件

Windows 7 以上操作系统，安装 Wireshark 网络嗅探软件。

3、网络

实验室局域网支持，能够访问校园网，能够访问互联网。

4、工具

无。

五、实验理论

1、DNS 基本原理；

2、DNS 解析过程。

六、实验任务

1、完成 DNS 报文的采集；

2、完成 DNS 报文结构的分析；

3、完成 DNS 通信过程分析。

七、实验内容及步骤

1、DNS 数据包分析

（1）获取数据报文

①打开 Wireshark，在【Filter】选项中输入报文过滤条件“dns and ip.addr==8.8.8.8”，选择【Start】，开始进行报文采集，如图 7-1 所示。

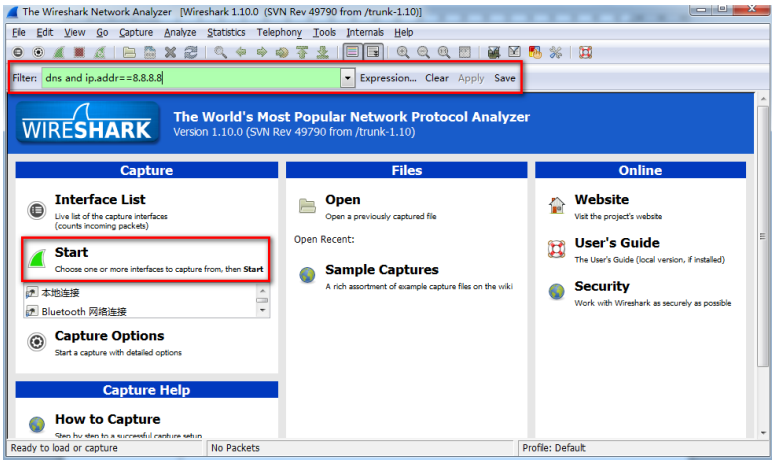

图 7-1 使用 Wireshark 工具进行 DNS 报文采集

②打开 Windows 的命令窗体，输入“nslookup –qt network.ke.51xueweb.cn 8.8.8.8”，使用 DNS 服务器“8.8.8.8”对域名记录“network.ke.51xueweb.cn”进行解析，如图 7-2 所示。

图 7-2 对域名记录 network.ke.51xueweb.cn 进行 DNS 解析请求

③在 Wireshark 的抓包窗体中，查看已获取的 DNS 数据报文，如图 7-3 所示。

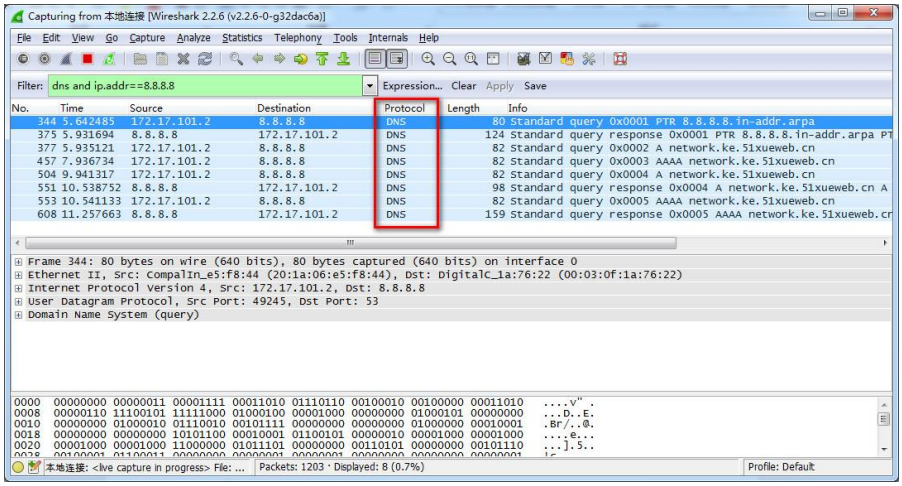

图 7-3 DNS 数据报文

（2）数据报文分析

对采集的数据报文进行分析，并完成表 7-1、表 7-2 的填写。

表 7-1 一次 DNS 解析请求过程

序号	发送时间	来源 IP	目的 IP	报文具体作用和描述
1				

2				
3				
4				
5				
6				
...				

表 7-2 域名记录 network.ke.51xueweb.cn 的 A 记录的 DNS 解析内容

序号	字段名	字段值	字段解释和说明
1	Name		
2	Type		
3	Class		
4	Time to live		
5	Data length		
6	Primary name Server		
7	Responsible authority's mailbox		
8	Serial Number		
9	Refresh Interval		
10	Retry Interval		
11	Expire Limit		
12	Minimum TTL		

2、通信过程中常见请求类型的 DNS 报文分析

（1）NS 记录

①获取 NS 记录请求应答报文。打开 Windows 的命令窗体，输入“nslookup –qt=ns network.ke.51xueweb.cn 8.8.8.8”，使用 DNS 服务器“8.8.8.8”获取 NS 记录记录结果，如图 7-4 所示。

图 7-4 进行 DNS 的 NS 记录解析请求

在 Wireshark 的抓包窗体中，查看已获取的 DNS 的 NS 记录解析数据报文，如图 7-5 所示。

②NS 记录请求应答报文分析。对 NS 记录请求应答数据报文进行分析，并根据数据报文内容填写表 7-3 和表 7-4。

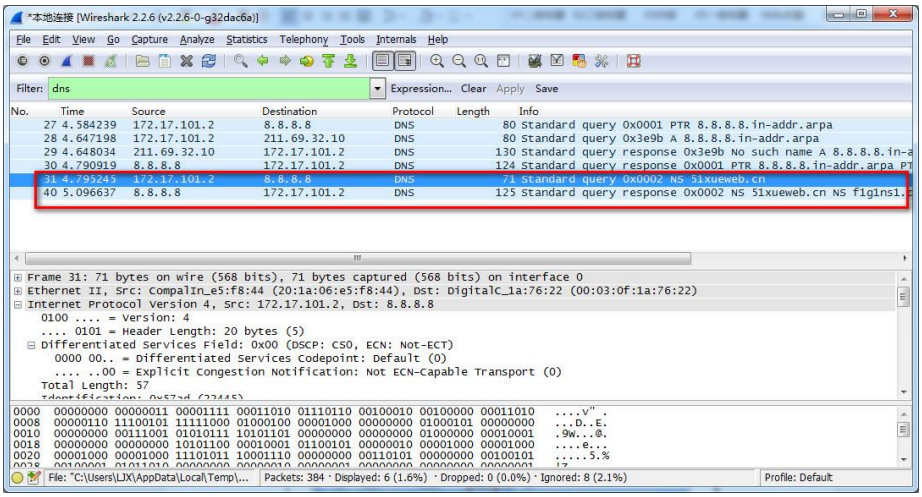

图 7-5 NS 记录请求应答报文

表 7-3 NS 记录请求报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Transaction ID		第　　位		
2	Flags		第　　位		
3	Questions		第　　位		
4	Answer RRs		第　　位		
5	Authority RRs		第　　位		
6	Additional RRs		第　　位		
7	Queries		第　　位		
8	抓取数据包的详细内容：				

表 7-4 NS 记录应答报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Transaction ID		第　　位		
2	Flags		第　　位		

3	Questions		第　位		
4	Answer RRs		第　位		
5	Authority RRs		第　位		
6	Additional RRs		第　位		
7	Queries		第　位		
8	Answers		第　位		
9	抓取数据包的详细内容：				

（2）CNAME 记录

①获取 CNAME 记录请求应答报文。打开 Windows 的命令窗体，输入“nslookup –qt=cname network.xg.hactcm.edu.cn 8.8.8.8”，使用 DNS 服务器“8.8.8.8”获取 CNAME 记录记录结果，如图 7-6 所示。

```
C:\Users\RuanXiaolong>nslookup -qt=cname network.xg.hactcm.edu.cn 8.8.8.8
服务器:  google-public-dns-a.google.com
Address:  8.8.8.8

非权威应答:
network.xg.hactcm.edu.cn        canonical name = network.ke.51xueweb.cn
```

图 7-6 CNAME 记录解析请求

在 Wireshark 的抓包窗体中，查看已获取的 CNAME 记录解析数据报文，如图 7-7 所示。

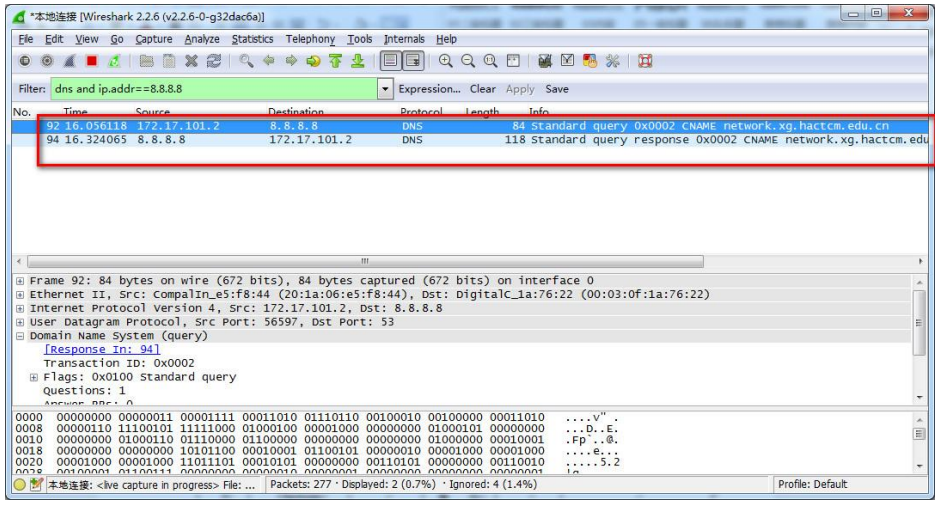

图 7-7 DNS 协议 NS 请求应答报文

②CNAME 记录请求应答报文分析。对 CNAME 记录请求应答数据报文进行分析，并根据数据报文内容填写表 7-5 和表 7-6。

表 7-5 CNAME 记录请求报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Transaction ID		第　位		
2	Flags		第　位		
3	Questions		第　位		
4	Answer RRs		第　位		
5	Authority RRs		第　位		
6	Additional RRs		第　位		
7	Queries		第　位		
8	抓取数据包的详细内容：				

表 7-6 CNAME 记录应答报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Transaction ID		第　位		
2	Flags		第　位		
3	Questions		第　位		
4	Answer RRs		第　位		
5	Authority RRs		第　位		
6	Additional RRs		第　位		
7	Queries		第　位		
8	Answers		第　位		
9	抓取数据包的详细内容：				

（3）MX 记录

①获取 MX 记录请求应答报文。打开 Windows 的命令窗体，输入“nslookup –qt=mx hactcm.edu.cn 8.8.8.8”，使用 DNS 服务器“8.8.8.8”获取 CNAME 记录记录结果，如图 7-8 所示。

```
C:\Users\RuanXiaolong>nslookup -qt=mx hactcm.edu.cn 8.8.8.8
服务器:  google-public-dns-a.google.com
Address:  8.8.8.8

非权威应答:
hactcm.edu.cn    MX preference = 10, mail exchanger = mailgate.hactcm.edu.cn
```

图 7-8 进行 DNS 的 MX 记录解析请求

在 Wireshark 的抓包窗体中，查看已获取的 MX 记录解析数据报文，如图 7-9 所示。

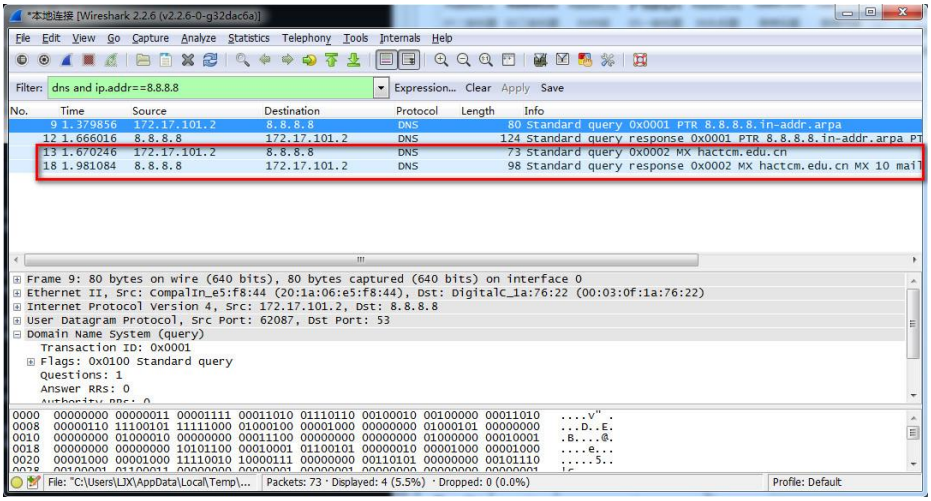

图 7-9 MX 记录请求应答报文

②MX 记录请求应答报文分析。对 MX 记录请求应答数据报文进行分析，并根据数据报文内容填写表 7-7 和表 7-8。

表 7-7 MX 记录请求报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Transaction ID		第 位		
2	Flags		第 位		
3	Questions		第 位		
4	Answer RRs		第 位		
5	Authority RRs		第 位		
6	Additional RRs		第 位		
7	Queries		第 位		
8	抓取数据包的详细内容：				

表 7-8 MX 记录应答报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Transaction ID		第　　位		
2	Flags		第　　位		
3	Questions		第　　位		
4	Answer RRs		第　　位		
5	Authority RRs		第　　位		
6	Additional RRs		第　　位		
7	Queries		第　　位		
8	Answers		第　　位		
9	抓取数据包的详细内容：				

八、实验分析

1、每访问一个网站都需要进行域名解析，域名解析的效率直接决定了网站访问的效率，如何为本地主机配置一个高效率的 DNS 服务器对于网站访问至关重要，那么如何查找和评估对自己来讲效率最高的 DNS 服务器呢？

2、域名记录和域名的关系

（1）什么是域名，什么是域名记录？二者之间的关系是什么？

（2）域名记录有几种类型？

（3）如何申请一个自己的域名？

实验八：HTTP 协议分析

一、实验目的

1、理解 HTTP 协议的基本内容；

2、理解 HTTP 协议的通信过程。

二、实验学时

2 学时

三、实验类型

综合型

四、实验需求

1、硬件

每人配备计算机 1 台。

2、软件

Windows 7 以上操作系统，安装 Wireshark 网络嗅探软件，安装 HTTP 协议调试代理工具 Fiddler。

3、网络

实验室局域网支持，能够访问校园网，能够访问互联网。

4、工具

无。

五、实验理论

1、HTTP 协议的基本原理；

2、HTTP 协议的通信过程。

六、实验任务

1、完成 HTTP 协议报文的采集；

2、完成 HTTP 协议报文结构的分析；

3、完成 HTTP 协议不同请求类型的数据报文分析。

七、实验内容及步骤

1、HTTP 数据包分析

（1）获取数据报文

①打开 Wireshark，在【Filter】选项中输入报文过滤条件“http contains “http://network.ke.51xueweb.cn””，选择【Start】，开始进行报文采集，如图 8-1 所示。

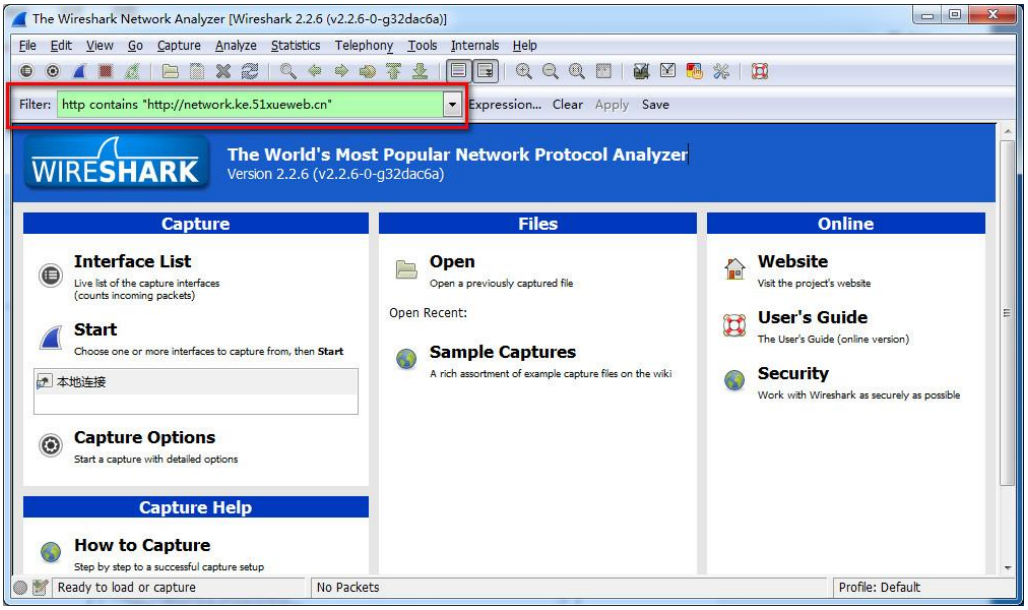

图 8-1 使用 Wireshark 工具进行 HTTP 报文采集

②打开浏览器，在地址栏中输入“http://network.ke.51xueweb.cn”，进行网页访问。

③在 Wireshark 的抓包窗体中，查看已获取的 HTTP 协议的数据报文，如图 8-2 所示。

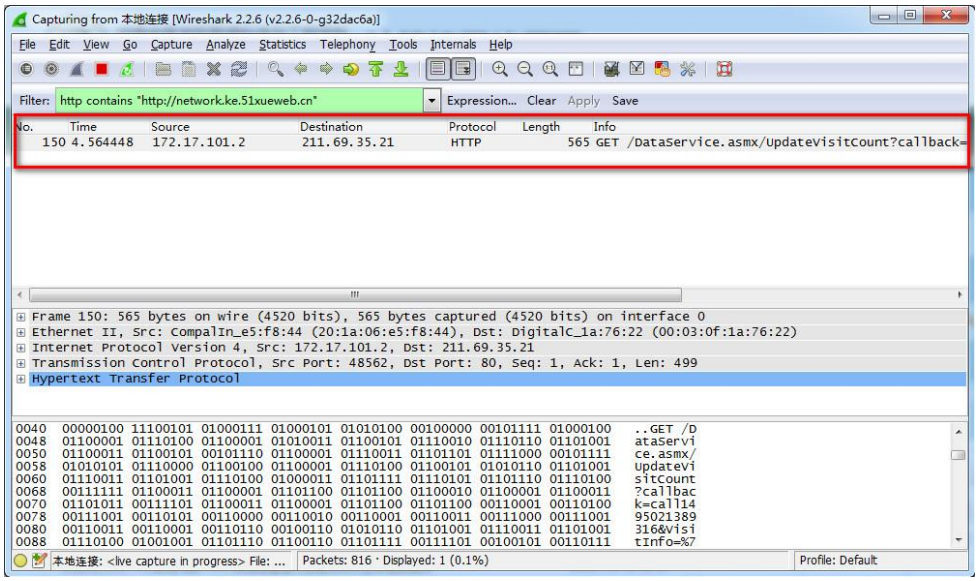

图 8-2 HTTP 数据报文

（2）数据报文分析

对获取到的 HTTP 协议报文内容进行详细分析，并填写表 8-1。

表 8-1 HTTP 协议报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Request Version		第 位		

2	Status code		第　位		
3	Response Phrase		第　位		
4	Content-Length		第　位		
5	Content-Type		第　位		
6	Content-Location		第　位		
7	Last-Modified		第　位		
8	Accept-Ranges		第　位		
9	ETag		第　位		
10	Server		第　位		
11	X-Powered-By		第　位		
12	Date		第　位		
13	Time Since Request		第　位		
14	抓取数据包的详细内容：				

2、不同类型的 HTTP 数据包分析

由于本地浏览器无法发送 HTTP 协议的 HEAD 和 POST 请求，因此本实验采用 HTTP 协议调试代理工具 Fiddler，实现不同请求类型的 HTTP 协议数据包的发送。

（1）Fiddler 安装与使用

①下载安装包

可通过官方网站（http://www.telerik.com/fiddler）获得 Fiddler 软件安装程序；

可通过本课程网站（http://network.ke.51xueweb.cn）下载本教程所使用的软件版本。

②安装软件

a、双击 Fiddler 安装程序，进入如图 8-3 所示的 Fiddler 安装界面，点击【I Agree】进行安装。

b、用户可使用默认的 Fiddler 安装目录，也可自行修改默认路径，如图 8-4 所示。

c、Fiddler 软件安装过程，如图 8-5 所示，安装完成后如图 8-6 所示。

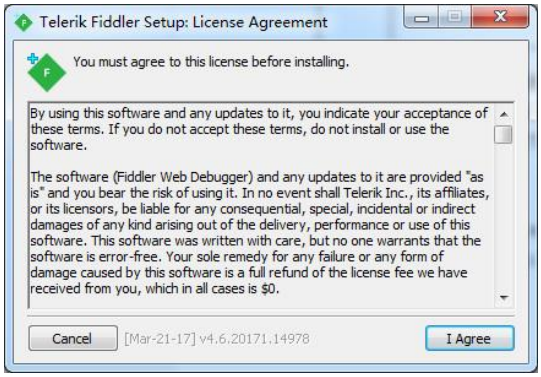

图 8-3 同意安装

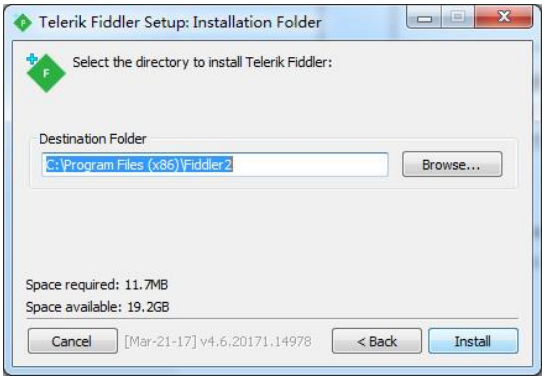

图 8-4 安装路径

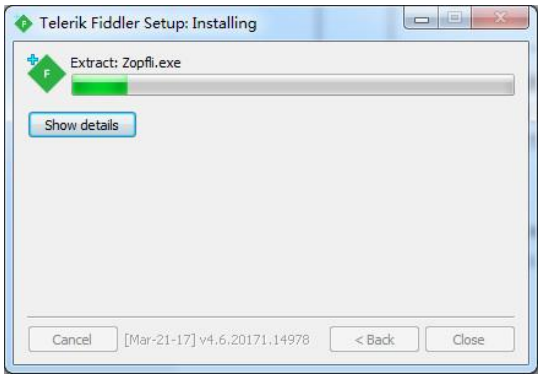

图 8-5 安装过程

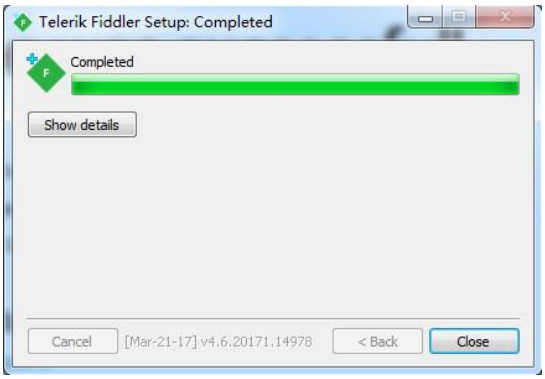

图 8-6 安装完成

③软件使用

打开软件，在右侧的操作栏目中选择【Composer】，选择 HTTP 请求类型和访问地址，实现本地发送不同类型的 HTTP 协议包操作，如图 8-7 所示。

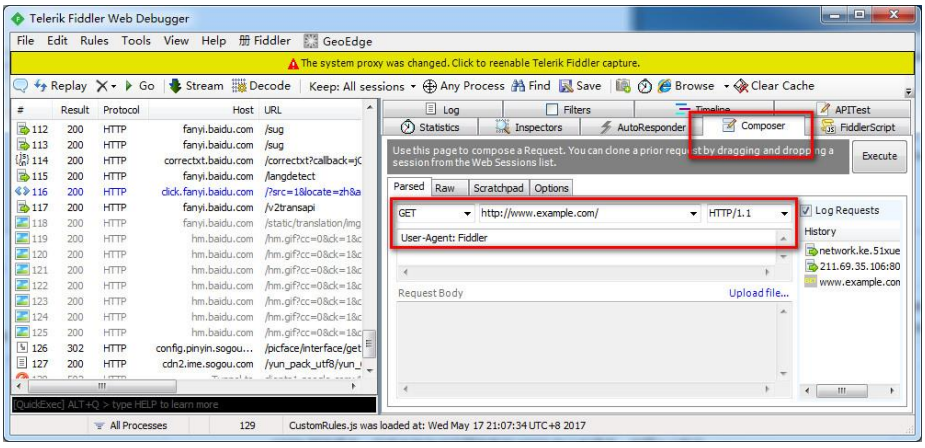

图 8-7 Fiddler 的使用

（2）HEAD 数据报文分析

①获取 HTTP Head 数据报文。

a、打开 Wireshark，在【Filter】选项中输入报文过滤条件“http”，选择【Start】，开始进行报文采集，如图 8-8 所示。

b、打开 Fiddler，在类型处选择【HEAD】类型，并输入“http://network.ke.51xueweb.cn”，

点击【Execute】开始执行，如图 8-9 所示。

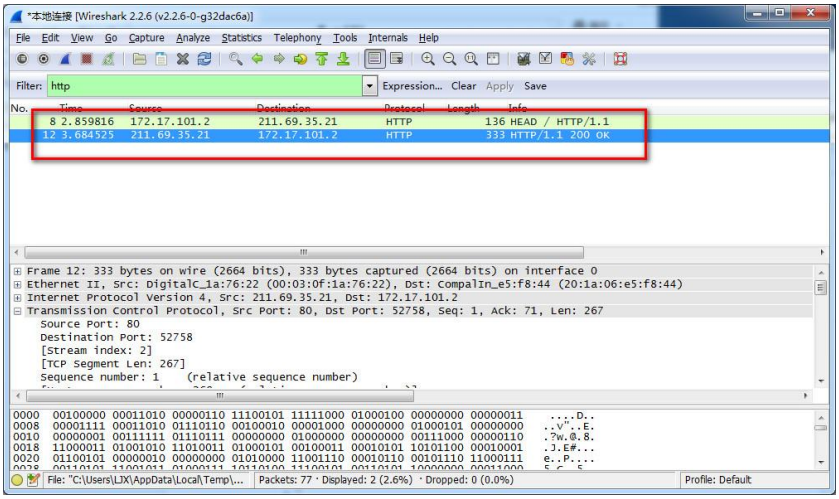

图 8-8 获得 HTTP HEAD 数据报文

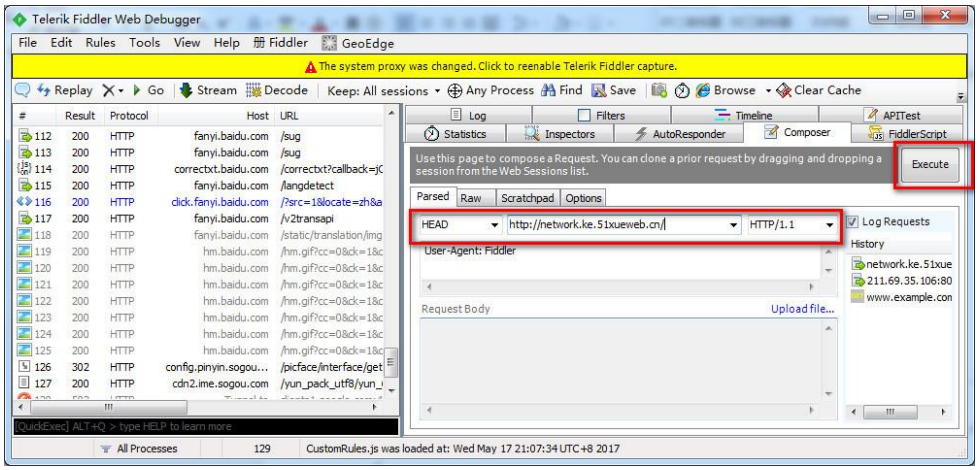

图 8-9 Fiddler 的配置

②数据报文分析。

对采集的 HTTP HEAD 协议报文进行详细分析，并填写表 8-2 和表 8-3。

表 8-2 HEAD 请求报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Request Method		第 位		
2	Request URI		第 位		
3	Request Version		第 位		
4	User-Agent		第 位		
5	Connection		第 位		
6	Host		第 位		
7	抓取数据包的详细内容：				

表 8-3 HEAD 响应报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Request Version		第　位		
2	Status code		第　位		
3	Response Phrase		第　位		
4	Content-Length		第　位		
5	Content-Type		第　位		
6	Content-Location		第　位		
7	Last-Modified		第　位		
8	Accept-Ranges		第　位		
9	ETag		第　位		
10	Server		第　位		
11	X-Powered-By				
12	Date				
13	Time Since Request				
14	抓取数据包的详细内容：				

（3）GET 数据报文分析

①获取 HTTP GET 数据报文。

a、打开 Wireshark，在【Filter】选项中输入报文过滤条件“http”，选择【Start】，开始进行报文采集。如图 8-10 所示。

b、打开 Fiddler 软件，在类型处选择【GET】类型，并输入“http://network.ke.51xueweb.cn”，点击【Execute】开始执行，如图 8-11 所示。

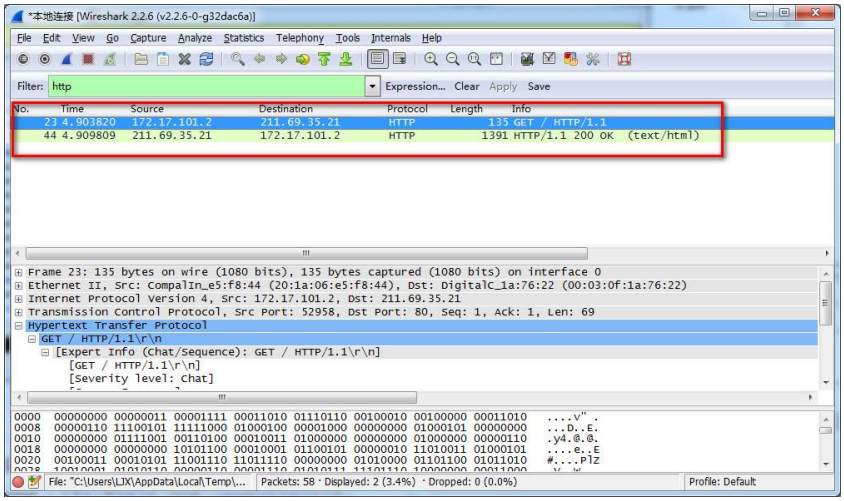

图 8-10 获得 HTTP GET 数据报文

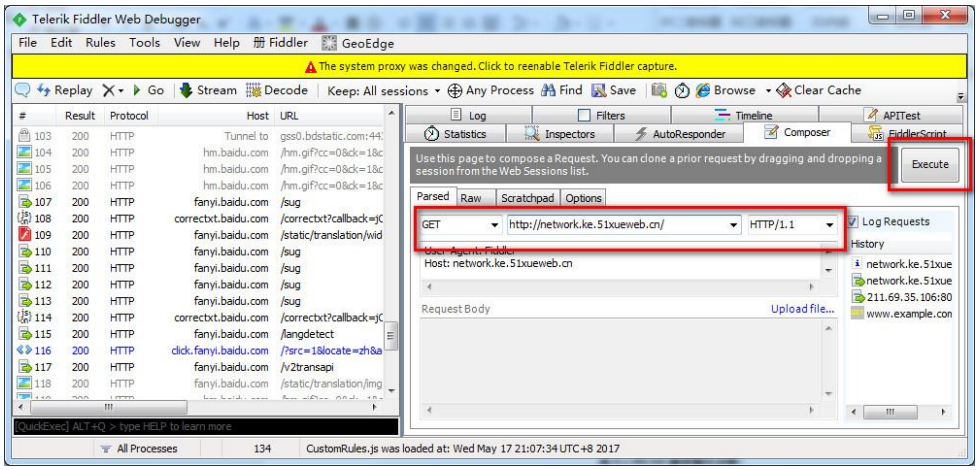

图 8-11 Fiddler 的配置

②数据报文分析。

对采集的 HTTP GET 协议报文进行详细分析，并填写表 8-4 和表 8-5。

表 8-4 GET 请求报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Request Method		第 位		
2	Request URI		第 位		
3	Request Version		第 位		
4	User-Agent		第 位		
5	Connection		第 位		
6	Host		第 位		
7	抓取数据包的详细内容：				

表 8-5 GET 响应报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Request Version		第　位		
2	Status code		第　位		
3	Response Phrase		第　位		
4	Content-Length		第　位		
5	Content-Type		第　位		
6	Content-Location		第　位		
7	Last-Modified		第　位		
8	Accept-Ranges		第　位		
9	ETag		第　位		
10	Server		第　位		
11	X-Powered-By				
12	Date				
13	Time Since Request				
14	抓取数据包的详细内容：				

（4）POST 数据报文分析

①获取 HTTP POST 数据报文。

a、打开 Wireshark，在【Filter】选项中输入报文过滤条件“http”，选择【Start】，开始进行报文采集，如图 8-12 所示。

b、打开 Fiddler，在类型处选择【POST】类型，并输入“http://network.ke.51xueweb.cn”，点击【Execute】开始执行，如图 8-13 所示。

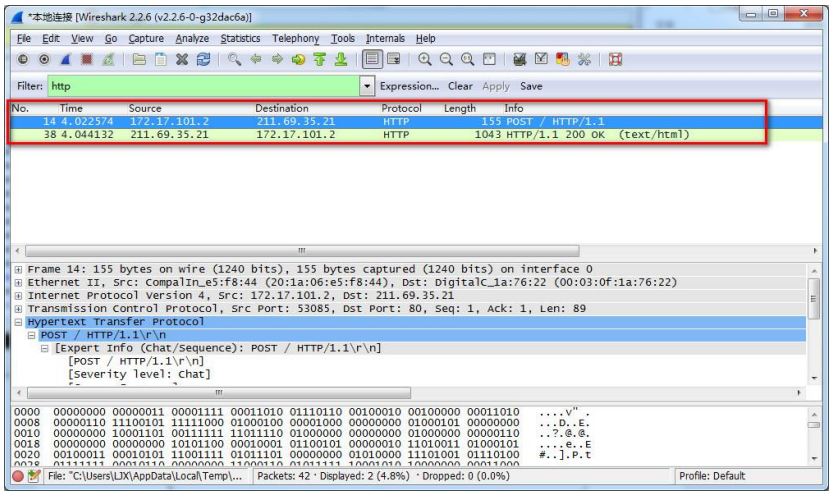

图 8-12 获得 HTTP POST 数据报文

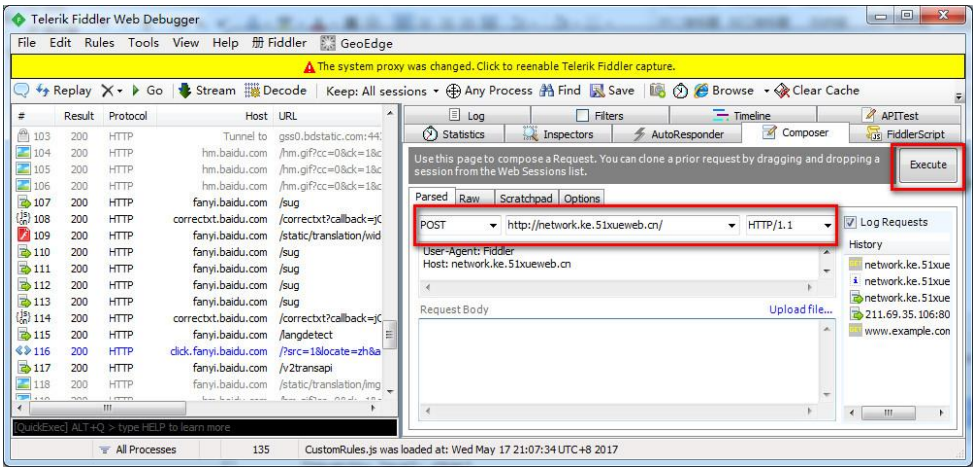

图 8-13 Fiddler 的配置

②数据报文分析。

对采集的 HTTP POST 协议报文进行详细分析，并填写表 8-6 和表 8-7。

表 8-6 POST 请求报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Request Method		第 位		
2	Request URI		第 位		
3	Request Version		第 位		
4	User-Agent		第 位		
5	Connection		第 位		
6	Host		第 位		
7	抓取数据包的详细内容：				

表 8-7 POST 响应报文分析

序号	字段名称	字段长度	起始位置	字段值	字段表示的信息
1	Request Version		第　位		
2	Status code		第　位		
3	Response Phrase		第　位		
4	Content-Length		第　位		
5	Content-Type		第　位		
6	Content-Location		第　位		
7	Last-Modified		第　位		
8	Accept-Ranges		第　位		
9	ETag		第　位		
10	Server		第　位		
11	X-Powered-By				
12	Date				
13	Time Since Request				
14	抓取数据包的详细内容：				

八、实验分析

1、HTTP 报文分析

（1）HTTP 请求报文有哪些字段，主要作用是什么？

（2）HTTP 响应报文有哪些字段，主要作用是什么？

2、HTTP 请求

（1）通过 HTTP 使用浏览器访问网站时，浏览器是否只向目的主机发送一次 HTTP 请求？如何查看这些请求？

（2）Fiddler 软件的工作原理是什么？主要应用场景有哪些？

实验九：SNMP 协议分析

一、实验目的

1、理解 SNMP 协议基本内容和通信过程；

2、掌握 MIB 的工作原理，并熟悉 Windows 操作系统的基本 MIB 信息；

3、理解网络监测的基本原理。

二、实验学时

2 学时

三、实验类型

综合型

四、实验需求

1、硬件

每人配备计算机 1 台。

2、软件

Windows 7 以上操作系统，安装 Wireshark 网络嗅探软件，安装 Net-SNMP 软件。

3、网络

实验室局域网支持，能够访问校园网，能够访问互联网。

4、工具

无。

五、实验理论

1、应用层的基本理论；

2、UDP 通信的基本理论；

3、SNMP 协议和 MIB 的基本理论；

4、对象标识 OID 的基本知识。

六、实验任务

1、完成 Windows 操作系统下 SNMP 客户端的安装与配置；

2、掌握 SNMP 请求发送的方法，并完成对 SNMP 协议的分析；

3、通过数据报文分析 SNMP 协议的通信过程。

七、实验内容及步骤

1、Windows 操作系统下 SNMP 客户端的安装与配置

（1）本实验以 Windows 7 操作系统为例，进行 SNMP 的安装与配置。

（2）打开【控制面板】【程序】【打开或关闭 Windows 功能】，如图 9-1 所示。

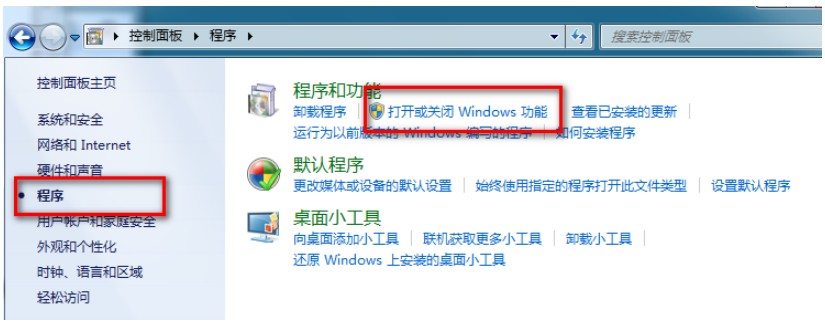

图 9-1 安装 SNMP 的准备

（3）选择【简单网络管理协议（SNMP）】后，点击【确定】按钮，进行安装，如图 9-2 所示。

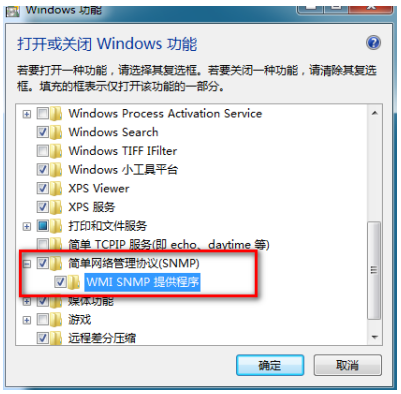

图 9-2 安装 SNMP 客户端

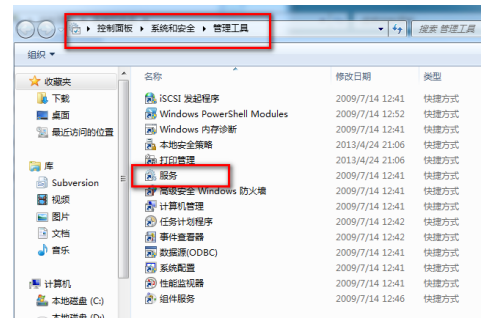

图 9-3 打开服务管理器

（4）打开【控制面板】【系统和安全】【管理工具】，双击打开【服务】，如图 9-3 所示。

（5）在【服务】窗口中，双击【SNMP Service】服务，开始对 SNMP 进行配置。

（6）在【陷阱】选项卡中，填写社区名称为“**NetworkMonitor**”，点击按钮【添加到列表】，如图 9-4 所示。

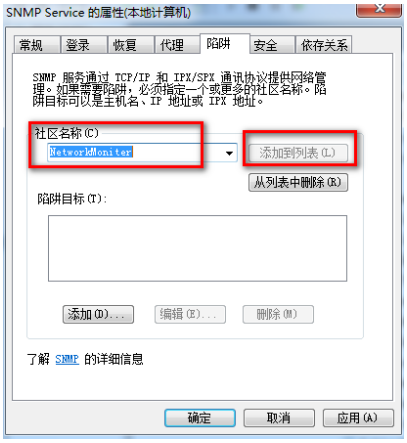

图 9-4 配置 SNMP 的陷阱

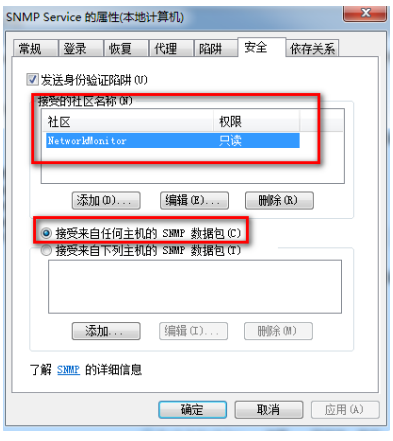

图 9-5 配置 SNMP 的安全

（7）在【安全】选项卡中，选择【添加】按钮，添加一个新的共同体“**NetworkMonitor**”，并选择【接受来自任何主机的 SNMP 数据包】，如图 9-5 所示。

（8）选择【应用】和【确定】按钮，完成配置。

（9）在【服务】窗体中，选择“SNMP Service”服务，点击【重启动此服务】，对 SNMP 服务进行重新启动，使得配置生效。如图 9-6 所示。

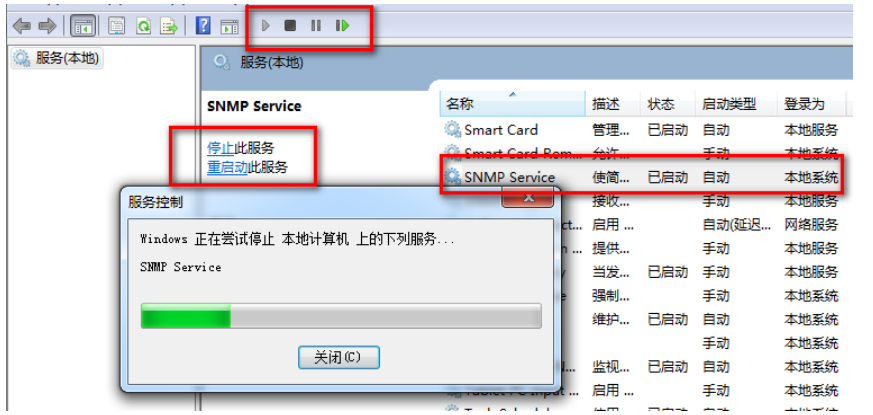

图 9-6 重启动 SNMP Service 服务

（10）至此，该 Windows 操作系统可以响应来自其他主机的 SNMP 请求。

2、安装 Net-SNMP

（1）下载安装包

可通过官方网站（http://www.net-snmp.org）获得 Net-SNMP 软件安装程序；

可通过本课程网站（http://network.ke.51xueweb.cn）下载本教程所使用的软件版本。

（2）安装 Net-SNMP。

a、双击 Net-SNMP 安装程序，进入如图 9-7 所示的 Net-SNMP 安装界面，点击【Next >】开始进行安装。点击【I accept …】，同意安装，如图 9-8 所示。点击【Next >】，选择默认安装组件，如图 9-9 所示。

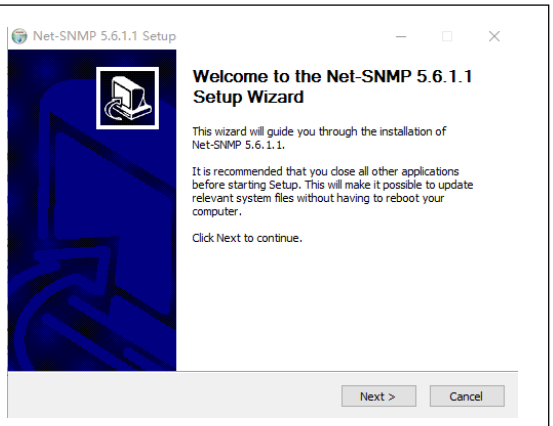

图 9-7 安装提示

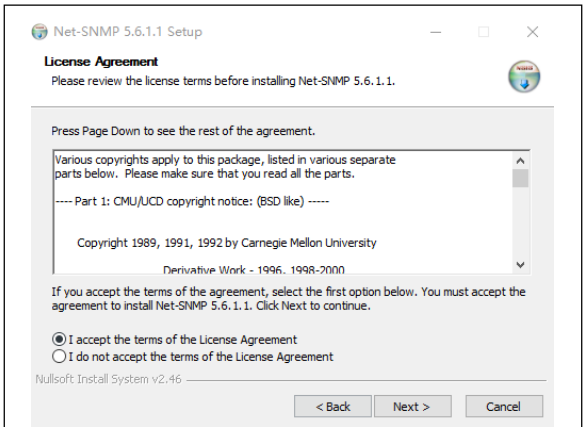

图 9-8 同意安装

b、用户可使用默认的 Net-SNMP 安装目录，也可自行修改默认路径，如图 9-10 所示。

c、Net-SNMP 软件安装过程，如图 9-11 所示，安装完成后如图 9-12 所示。

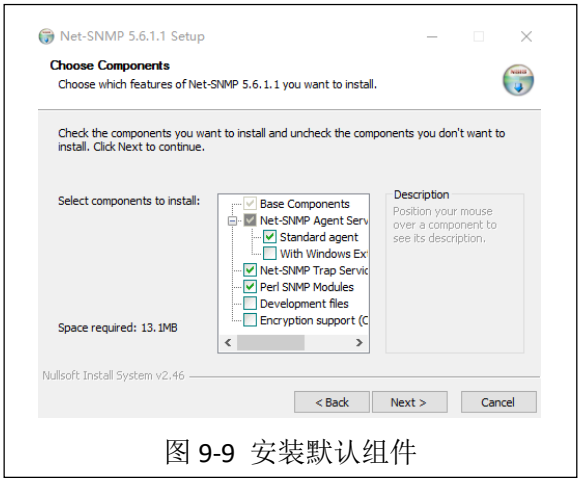

图 9-9 安装默认组件

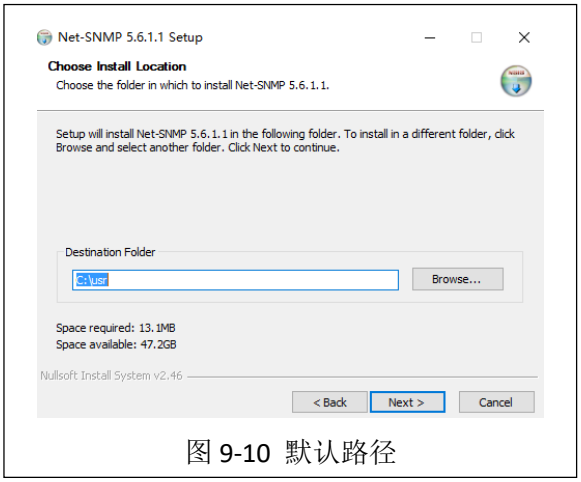

图 9-10 默认路径

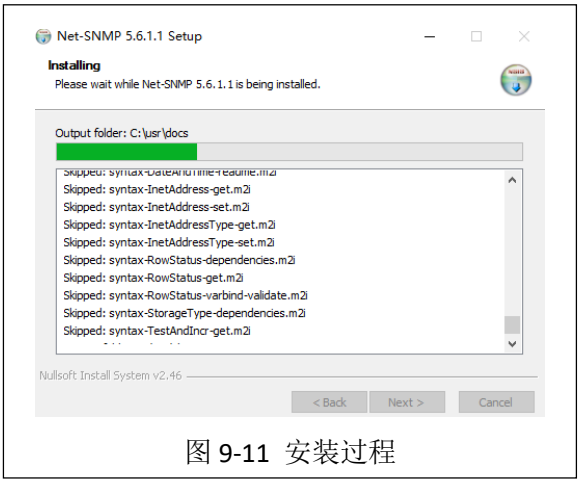

图 9-11 安装过程

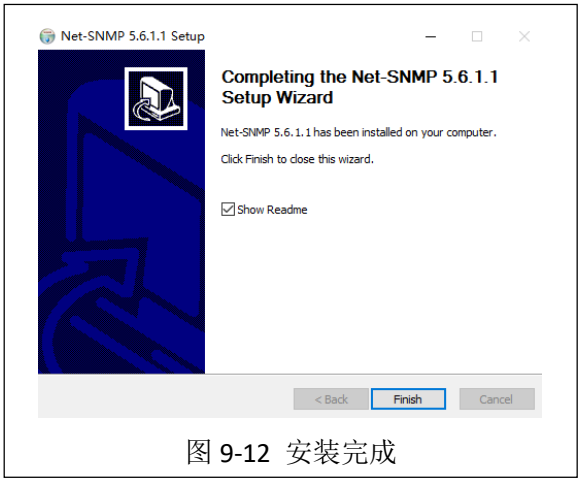

图 9-12 安装完成

3、使用 Net-SNMP 工具进行数据采集

（1）启动 Windows 命令行工具。

（2）在命令行中输入“**snmpwalk -v 2c -c NetworkMonitor localhost .1.3.6.1.2.1.1**”后回车确认。此命令是通过 Net-SNMP 工具向本地主机发送了一个 SNMP 请求，MIB 的信息为.1.3.6.1.2.1.1。

（3）查看获得的信息，并填写表 9-1 通过 SNMP 请求获得 Windows 系统的基本信息。

表 9-1 通过 SNMP 请求获得 Windows 系统的基本信息

序号	字段名	字段值	字段解释和说明
1			
2			
3			
4			
5			

6			
7			
8			

（4）通过指定 OID 的方式进行 Windows 系统基本信息的采集。

例如，“snmpget -v 2c -c NetworkMonitor localhost {系统名的 OID}”可以采集 Windows 系统的系统名信息；查看采集的信息，并将 SNMP 请求获得的 Windows 操作系统的信息填写到表 9-2 中。

表 9-2 本机设备运行状态一览表

序号	字段名	字段值	字段解释和说明
1	系统描述		
2	系统的私有 OID		
3	系统运行时间		
4	系统联系人		
5	系统名称		
6	系统位置		
7	系统服务数		
8	系统时间		
9	系统用户数		
10	系统进程		
11	系统最大进行数		
12	硬盘总大小		
13	硬盘使用情况		
14	物理内存大小		
15	物理内存使用情况		

4、SNMP 报文分析

（1）启动 Wireshark，在【Filter】中输入

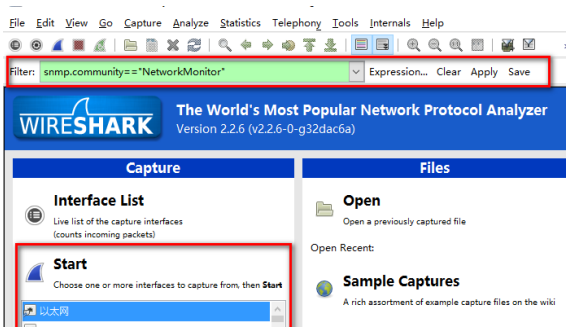

图 9-13 通过 Wireshark 工具进行 SNMP 协议的报文采集

“snmp.community=="NetworkMonitor"”，选择【Start】按钮，开始数据报文采集。如图 9-13 所示。

（2）启动 Windows 命令行工具。

（3）在命令行中输入“snmpwalk -v 2c -c NetworkMonitor localhost .1.3.6.1.2.1.1”后回车确认。

此时通过 SNMP 请求获得了本机信息，但是 Wireshark 却没有采集到任何数据，如图 9-14，9-15 所示。

```
C:\Users\helulu>snmpwalk -v 2c -c NetworkMonitor localhost .1.3.6.1.2.1.1
SNMPv2-MIB::sysDescr.0 = STRING: Hardware: Intel64 Family 6 Model 78 Stepping 3 AT/A
T COMPATIBLE - Software: Windows Version 6.3 (Build 10586 Multiprocessor Free)
SNMPv2-MIB::sysObjectID.0 = OID: SNMPv2-SMI::enterprises.311.1.1.3.1.1
DISMAN-EVENT-MIB::sysUpTimeInstance = Timeticks: (1955927) 5:25:59.27
SNMPv2-MIB::sysContact.0 = STRING:
SNMPv2-MIB::sysName.0 = STRING: helulu
SNMPv2-MIB::sysLocation.0 = STRING:
SNMPv2-MIB::sysServices.0 = INTEGER: 76
```

图 9-14 SNMP 请求查看本地主机的基本信息

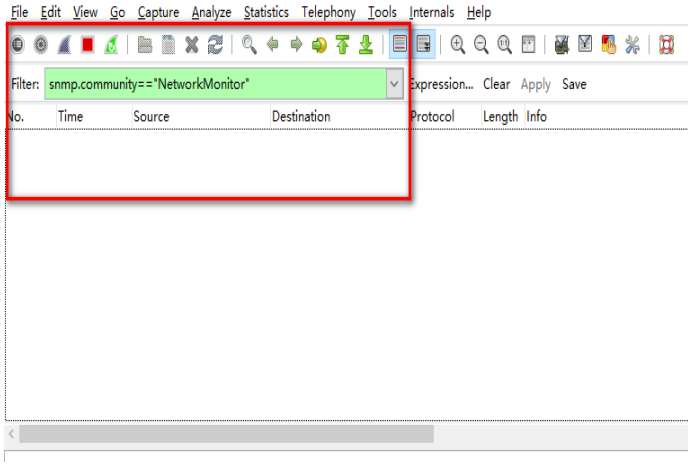

图 9-15 SNMP 数据报文

（4）在命令行中输入“**snmpwalk -v 2c -c NetworkMonitor 192.168.157.194 .1.3.6.1.2.1.1**”后回车确认。此命令是通过 Net-SNMP 工具向本小组其他计算机发送了一个 SNMP 请求，MIB 的信息为.1.3.6.1.2.1.1。此时通过 SNMP 请求获得了对方计算机的信息， Wireshark 采集到 SNMP 通信数据报文，如图 9-16 所示。

（5）从获取的 UDP 数据报文中任意选择其中一条数据报文，对该数据报文进行详细分析，填写表 9-3，9-4。

表 9-3 一次 SNMP 解析请求过程

序号	发送时间	来源 IP	目的 IP	报文具体作用和描述
1				
2				
3				
4				
5				
6				
7				
8				
…				

表 9-4 一次 SNMP 解析响应过程

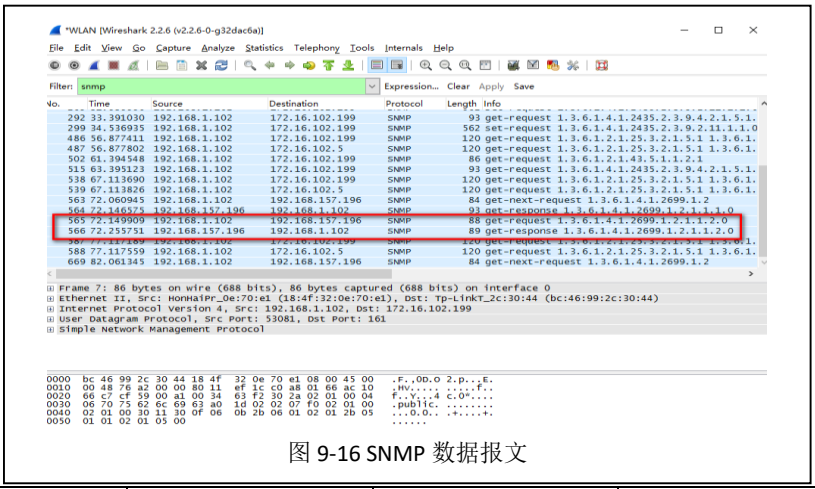

图 9-16 SNMP 数据报文

序号	发送时间	来源 IP	目的 IP	报文具体作用和描述
1				
2				
3				
4				

5				
6				
7				
8				
…				

八、实验分析

1、为什么使用 Net-SNMP 能够采集到本机信息，但无法通过 Wireshark 获取到数据报文？

2、SNMP v1、v2 和 v3

（1）SNMP 都有哪些版本？这些版本分别有那些差异？

（2）不同版本的 SNMP 协议，其报文结构和通信过程是否一致？

（3）本实验是使用 SNMP 的什么版本进行的？

3、SNMP 的安全性

（1）SNMP 在通信过程中是否安全？有哪些安全风险？

（2）SNMP 协议是如何提高自身安全性的？

（3）SNMP 在局域网和广域网的环境中，通信过程是否有差异？

4、公有 MIB 库与私有 MIB 库

（1）常见公有 MIB 库有哪些？遵循什么标准？

（2）私有 MIB 库与公有 MIB 库的区别是什么？

教学云平台：http://it.hactcm.edu.cn

课程网站：http://network.xg.hactcm.edu.cn

河南中医药大学信息管理与信息系统教研室

信息技术学院网络与信息系统科研工作室