

实验五：DNS 协议分析

一、实验目的

- 1、了解 DNS；
- 2、熟悉 DNS 报文结构；
- 3、掌握 DNS 通信过程。

二、实验学时

2 学时

三、实验类型

验证性



四、实验需求

1、硬件

每人配备计算机 1 台，不低于双核 CPU、8G 内存、500GB 硬盘。

2、软件

推荐 Ubuntu Desktop 操作系统，安装 GNS 3 仿真软件，安装 Wireshark 抓包工具。
支持 Windows 操作系统，安装 GNS 3 仿真软件，安装 Wireshark 抓包工具。

3、网络

计算机使用固定 IP 地址接入局域网，并支持对互联网的访问。

4、工具

无。

五、实验任务

- 1、完成 DNS 报文结构分析；
- 2、完成 DNS 记录类型的报文分析；
- 3、完成 DNS 查询分析。

六、实验内容及步骤

任务 1：实验准备

步骤 01：实验拓扑设计

实验拓扑结构，如图 5-1 所示。

步骤 02：实验网络设计

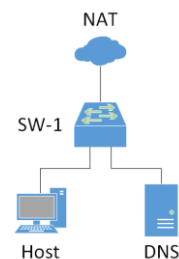


图 5-1 拓扑设计

①拓扑说明

表 5-1 主机地址规划

设备	设备类型	规格型号	备注
Host、DNS	DNS	--	--
SW-1	二层交换机	Ethernet switch	--

②交换机接口规划

表 5-2 交换机规划

交换机	接口	VLANID	连接设备	接口类型
SW-1	e0	1	NAT	默认
SW-1	e1	1	Host	默认
SW-1	e2	1	DNS	默认

③主机地址规划

表 5-3 主机地址规划

主机	IP 地址/子网掩码	网关	DNS	接入位置
Host	192.168.122.10 /24	192.168.122.1	192.168.122.200	e1
DNS	192.168.122.200/24	192.168.122.1	8.8.8.8	e2

步骤 03：实验准备的补充说明

本实验使用 DNS 终端设备需要 Docker 仿真器支持。

(1) 安装 Docker

在 Ubuntu Desktop 上，通过终端在线安装 Docker，操作命令如下：

参考命令：

```
#移除老版本
sudo apt remove docker docker-engine docker.io
#安装以下软件包
sudo apt-get install apt-transport-https ca-certificates curl software-properties-common
#引入官方 Docker GPG 钥匙
curl -fsSL https://download.docker.com/linux/ubuntu/gpg | sudo apt-key add -
/#增加相关源
sudo add-apt-repository "deb [arch=amd64] https://download.docker.com/linux/ubuntu
$(lsb_release -cs) stable"
#安装 Docker-CE，当提示需要占用磁盘空间，是否继续时，输入 Y 继续
sudo apt update
sudo apt install docker-ce
#将当前用户 net 添加到以 libvirt、kvm、wireshark、docker 组
sudo usermod -aG libvirt net
sudo usermod -aG kvm net
sudo usermod -aG wireshark net
sudo usermod -aG docker net
```

安装完成后重启系统，使用户权限生效。

注：实验教学提供的实验平台 VM 已经安装 Docker。

(2) 添加 DNS 终端模板

①在左侧终端设备列表下方点击【+New template】打开模板创建窗口，如图 5-2 所示。

②点击【Next>】，选择要安装的应用，展开“Guest”或在筛选框中输入“dns”进行筛选，并选择要安装的应用（DNS），如图 5-3 所示。

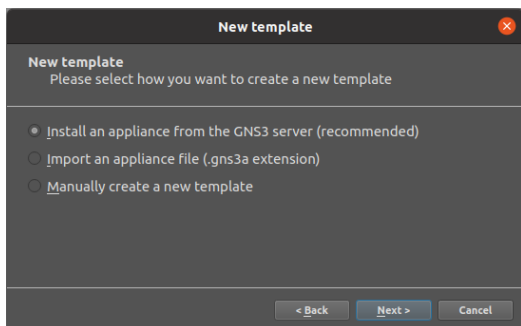


图 5-2 创建新模板

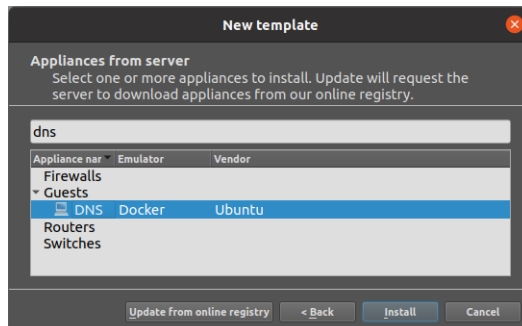


图 5-3 选择应用

③点击【Install】，选择服务器类型，如图 5-4 所示。

④点击【Next>】，显示使用说明，如图 5-5 所示。

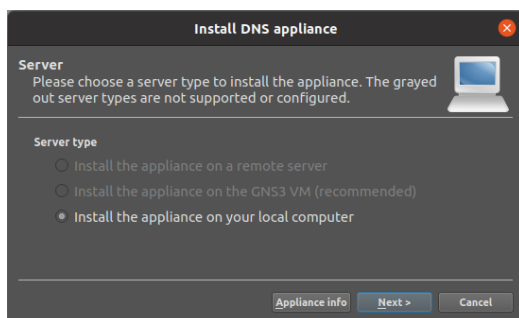


图 5-4 选择服务器类型

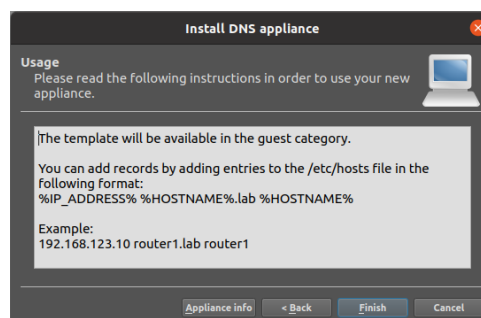


图 5-5 完成安装

⑤点击【Finish】完成添加，设备工具栏中显示 DNS 设备模板，如图 5-6 所示。

步骤 04：在 GNS3 中实现网络

（1）在 GNS3 中，按实验拓扑设计和实验网络设计实现网络，如图 5-7 所示。

（2）配置 Host 网络地址。

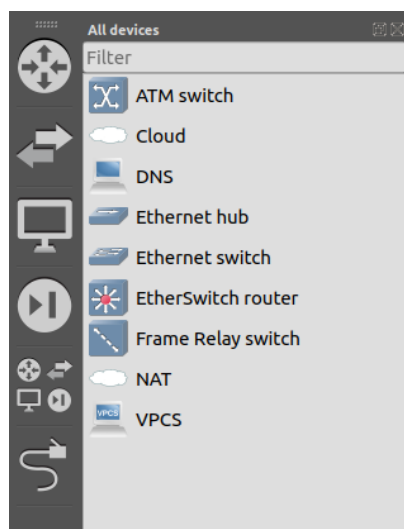


图 5-6 设备工具栏显示

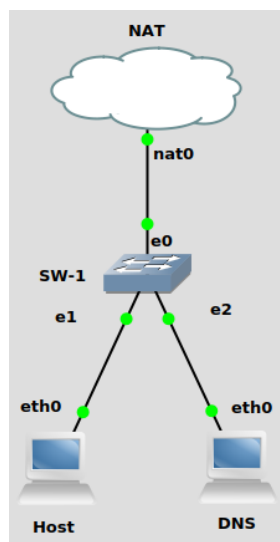


图 5-7 实现网络

①右键 Host，点击【Configure】按钮，打开节点属性配置窗口，如图 5-8 所示。

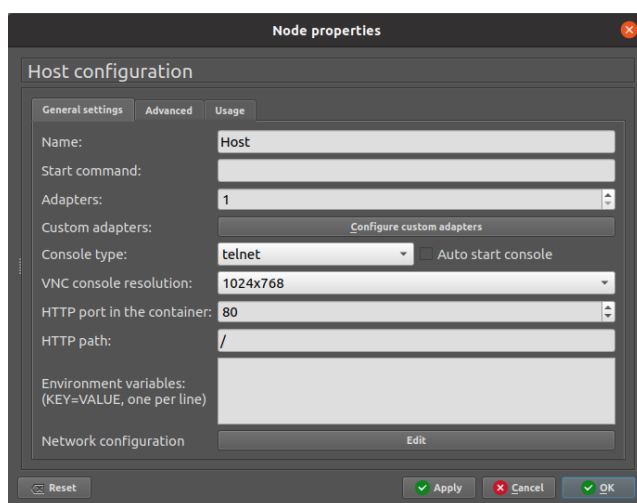


图 5-8 打开节点属性配置窗口

②在“General settings”选项卡中“Network configuration”配置项后点击【Edit】按钮打开主机接口配置弹出框。依表 5-3 进行网络地址配置，如图 5-9 所示。

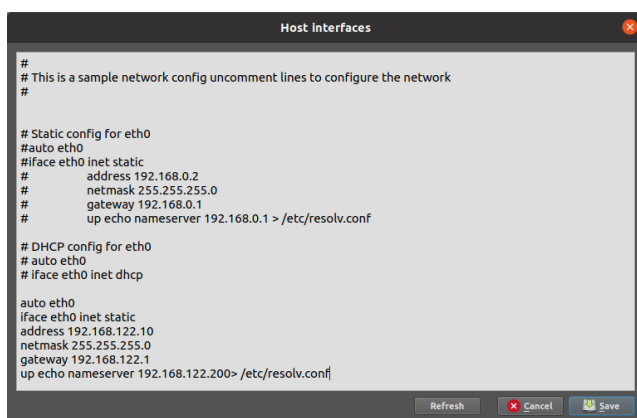


图 5-9 配置网络地址

③依次点击【Save】、【OK】完成配置。

(3) 参照(2)操作，按表 5-3 配置 DNS 主机的网络地址。

(4) 网络连通性测试。

启动网络，在 Host、DNS 终端分别执行“Ping 8.8.8.8”，测试网络通信情况。

表 5-4 网络通信测试用例

源主机	通信结果
Host	
DNS	

任务 2：DNS 报文结构分析

步骤 01：设置抓包点，启动 Wireshark 进行抓包

如图 5-10 所示，在交换机 SW-1 连接 Host 的 e1 接口启动抓包，并在 Wireshark 的过滤器中输入“dns”筛选报文。

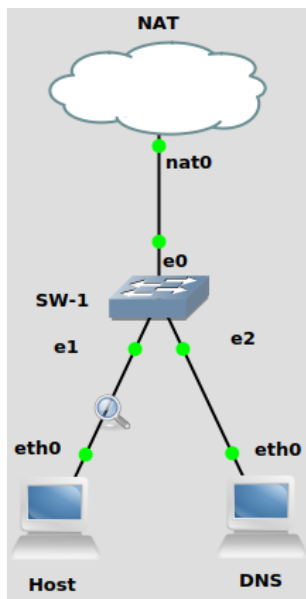


图 5-10 抓包位置设置

步骤 02：执行 DNS 查询命令

在 Host 主机控制台执行 nslookup 命令，查询域名记录 “network.xg.hactcm.edu.cn”，操作如下：

参考命令：

```
nslookup network.xg.hactcm.edu.cn
```

提醒：

- nslookup 默认使用本机设置的 DNS，进行 A 记录类型查询
- nslookup 查询时指定记录类型、DNS 的方式为：nslookup -type=类型 域名记录 DNS，如：nslookup -type=NS hactcm.edu.cn 192.168.122.200

步骤 03：分析 DNS 报文结构

在 Wireshark 窗体中查看抓到的 DNS 报文。

(1) 分析 DNS 请求报文结构，并填写表 5-5

表 5-5 DNS 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	数据包的详细内容				

--	--

(2) 分析 DNS 应答报文结构，并填写表 5-6。

表 5-6 DNS 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	数据包的详细内容				

任务 3：DNS 记录类型分析

本任务在任务 2 的基础上进行。

步骤 01：分析 A 记录报文

(1) 执行 A 记录查询

在 Host 控制台执行 nslookup 命令，对域名记录 “network.xg.hactcm.edu.cn” 执行 A 记录查询请求，操作如下：

参考命令：

```
nslookup -type=A network.xg.hactcm.edu.cn
```

(2) 分析请求报文内容，并填写表 5-7。

表 5-7 A 记录的 DNS 请求内容

序号	字段名称	字段值	字段解释和说明
1	Name		
2	Name Length		
3	Label Count		

4	Type		
5	Class		

(3) 分析应答报文内容，并填写表 5-8。

表 5-8 A 记录的 DNS 解析内容

序号	字段名称	字段值	字段解释和说明
1	Name		
2	Type		
3	Class		
4	Time to live		
5	Data Length		
6	Address		

步骤 02: 分析 AAAA 记录报文

(1) 执行 AAAA 记录查询

在 Host 控制台执行 nslookup 命令，对域名记录“www.mi.com”执行 AAAA 记录查询请求，操作如下：

参考命令：

```
nslookup -type=AAAA www.mi.com 8.8.8.8
```

(2) 分析请求报文内容，并填写表 5-9。

表 5-9 AAAA 记录的 DNS 请求内容

序号	字段名称	字段值	字段解释和说明
1	Name		
2	Name Length		
3	Label Count		
4	Type		
5	Class		

(3) 分析应答报文内容，并填写表 5-10。

表 5-10 AAAA 记录的 DNS 解析内容

序号	字段名称	字段值	字段解释和说明
1	Name		
2	Type		
3	Class		
4	Time to live		
5	Data Length		
6	AAAA Address		

步骤 03：分析 MX 记录报文**(1) 执行 MX 记录查询**

在 Host 控制台执行 nslookup 命令，对域名记录“mail.163.com”执行 MX 记录查询请求，操作如下：

参考命令：

```
nslookup -type=MX mail.163.com 8.8.8.8
```

(2) 分析请求报文内容，并填写表 5-11。**表 5-11 MX 记录的 DNS 请求内容**

序号	字段名称	字段值	字段解释和说明
1	Name		
2	Name Length		
3	Label Count		
4	Type		
5	Class		

(3) 分析应答报文内容，并填写表 5-12。**表 5-12 MX 记录的 DNS 解析内容**

序号	字段名称	字段值	字段解释和说明
1	Name		
2	Type		
3	Class		
4	Time to live		
5	Data Length		
6	CNAME		

步骤 04：分析 NS 记录报文**(1) 执行 NS 记录查询**

在 Host 控制台执行 nslookup 命令，对域名记录“hactcm.edu.cn”执行 NS 记录查询请求，操作如下：

参考命令：

```
nslookup -type=NS hactcm.edu.cn 8.8.8.8
```

(2) 分析请求报文内容，并填写表 5-13。**表 5-13 NS 记录的 DNS 请求内容**

序号	字段名称	字段值	字段解释和说明
1	Name		
2	Name Length		
3	Label Count		

4	Type		
5	Class		

(3) 分析应答报文内容，并填写表 5-14。

表 5-14 NS 记录的 DNS 解析内容

序号	字段名称	字段值	字段解释和说明
1	Name		
2	Type		
3	Class		
4	Time to live		
5	Data Length		
6	Name Servcer		

步骤 05: 分析 CNAME 记录报文

(1) 执行 CNAME 记录查询

在 Host 控制台执行 nslookup 命令，对域名记录 “www.baidu.com” 执行 CNAME 记录查询请求，操作如下：

参考命令：

```
nslookup -type=CNAME www.baidu.com 8.8.8.8
```

(2) 分析请求报文内容，并填写表 5-15。

表 5-15 CNAME 记录的 DNS 请求内容

序号	字段名称	字段值	字段解释和说明
1	Name		
2	Name Length		
3	Label Count		
4	Type		
5	Class		

(3) 分析应答报文内容，并填写表 5-16。

表 5-16 CNAME 记录的 DNS 解析内容

序号	字段名称	字段值	字段解释和说明
1	Name		
2	Type		
3	Class		
4	Time to live		
5	Data Length		
6	CNAME		

步骤 06: 分析 TXT 记录报文

(1) 执行 TXT 记录查询

在 Host 控制台执行 nslookup 命令，对域名记录 “hactcm.edu.cn” 执行 TXT 记录查询请求，操作如下：

参考命令：

```
nslookup -type=TXT hactcm.edu.cn 8.8.8.8
```

(2) 分析请求报文内容，并填写表 5-17。

表 5-17 TXT 记录的 DNS 请求内容

序号	字段名称	字段值	字段解释和说明
1	Name		
2	Name Length		
3	Label Count		
4	Type		
5	Class		

(3) 分析应答报文内容，并填写表 5-18。

表 5-18 TXT 记录的 DNS 解析内容

序号	字段名称	字段值	字段解释和说明
1	Name		
2	Type		
3	Class		
4	Time to live		
5	Data Length		
6	TXT Length		
7	TXT		

步骤 07：分析 PTR 记录报文

(1) 执行 PTR 记录查询

在 Host 控制台执行 nslookup 命令，对域名记录 “mail.163.com” 的地址 123.126.97.202 执行 PTR 记录查询请求，操作如下：

参考命令：

```
nslookup -type=PTR 123.126.97.202 8.8.8.8
```

(2) 分析请求报文内容，并填写表 5-19。

表 5-19 PTR 记录的 DNS 请求内容

序号	字段名称	字段值	字段解释和说明
1	Name		
2	Name Length		

3	Label Count		
4	Type		
5	Class		

(3) 分析请求报文内容，并填写表 5-20。

表 5-20 PTR 记录的 DNS 解析内容

序号	字段名称	字段值	字段解释和说明
1	Name		
2	Type		
3	Class		
4	Time to live		
5	Data Length		
6	Domain Name		

任务 4: DNS 查询分析

步骤 01: 设置抓包点，启动 Wireshark 进行抓包

如图 5-11 所示，交换机 SW-1 连接 DNS 的 e2 接口启动抓包，并在 Wireshark 的过滤器中输入“dns”筛选报文。

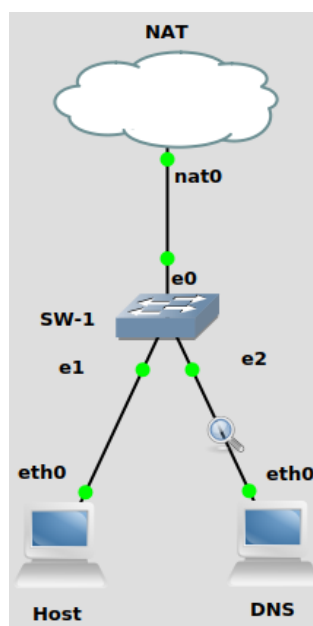


图 5-11 抓包位置设置

步骤 02: 执行 DNS 查询命令

在 Host 控制台执行 nslookup 命令，执行域名记录“network.xg.hactcm.edu.cn”查询请求，操作如下：

参考命令：

```
nslookup -type=A network.xg.hactcm.edu.cn
```

步骤 03: 抓取 DNS 查询过程报文

在 Wireshark 窗体中查看 DNS 查询通信过程报文，如图 5-12 所示。

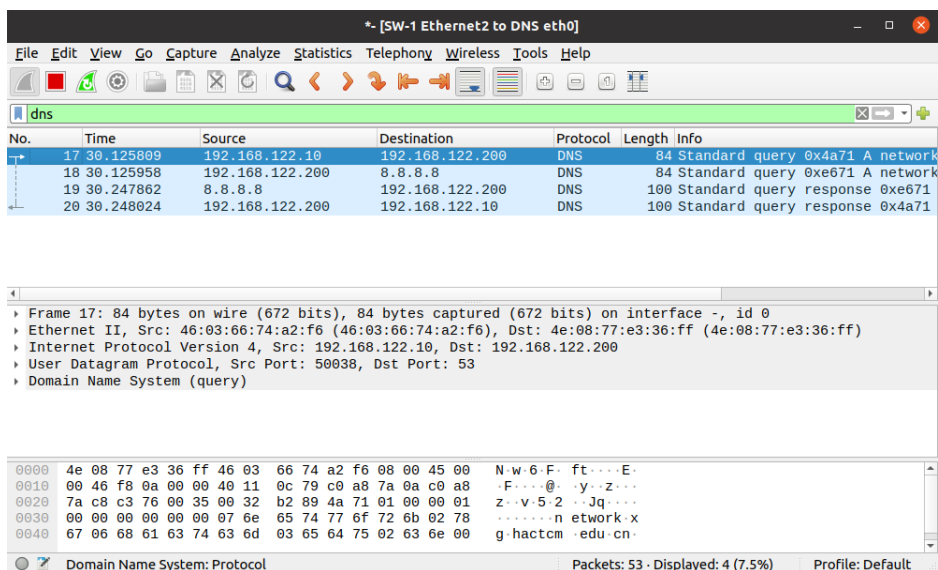


图 5-12 DNS 查询通讯过程

步骤 04：分析 DNS 查询过程，并填写表 5-21。

表 5-21 DNS 查询过程

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				
...				

七、实验考核

1、任务说明

使用 Wireshark 在 GNS3 仿真环境中完成 DNS 协议分析。

2、任务要求

要求 1：部署实验网络

要求 2：抓包分析 DNS 报文结构

要求 3：抓包分析 DNS 记录类型

要求 4：抓包分析 DNS 查询过程

3、考核要求

题目 1：使用 Wireshark 分析域名记录“www.hactcm.edu.cn”的 DNS 请求报文结构，请提交【DNS 请求报文】截图。

题目 2：分析【DNS 请求报文】，请填写以下信息：

DNS 请求报文长度：_____字节；

字段 Transaction ID 的长度：_____字节，起始位置：_____位，字段值：_____
_____，字段表示的信息：_____；

字段 Flags 的长度：_____字节，起始位置：_____位，字段值：_____
_____, 字段表示的信息：_____；

字段 Questions 的长度：_____字节，起始位置：_____位，字段值：_____
_____, 字段表示的信息：_____；

字段 Answer RRs 的长度：_____字节，起始位置：_____位，字段值：_____
_____, 字段表示的信息：_____；

字段 Authority RRs 的长度：_____字节，起始位置：_____位，字段值：_____
_____, 字段表示的信息：_____；

字段 Additional RRs 的长度：_____字节，起始位置：_____位，字段值：_____
_____, 字段表示的信息：_____；

字段 Query 的长度：_____字节，起始位置：_____位，字段值：_____
_____, 字段表示的信息：_____。

题目 3：使用 Wireshark 分析域名记录“www.hactcm.edu.cn”的 DNS 应答报文结构，请提交【DNS 应答报文】。

题目 4：分析【DNS 应答报文】，请填写以下信息：

字段 Answers 的长度：_____字节，起始位置：_____位，字段值：_____
_____, 字段表示的信息：_____。

题目 5：参照任务 4 操作，抓取域名记录“www.hactcm.edu.cn”查询过程报文，提交 DNS 查询过程报文截图。

题目 6：分析 DNS 查询过程，请按照下述格式详细填写 DNS 查询过程的报文信息：

该过程产生_____个 DNS 报文；

报文序号：_____, 发送时间：_____, 来源 IP：_____, 目的 IP：_____
_____, 报文具体作用和描述：_____；

报文序号：_____, 发送时间：_____, 来源 IP：_____, 目的 IP：_____
_____, 报文具体作用和描述：_____；

... ..