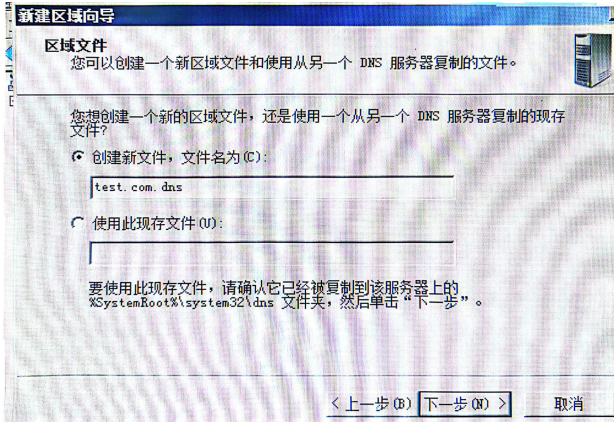


四川大学计算机学院、软件学院

实验报告

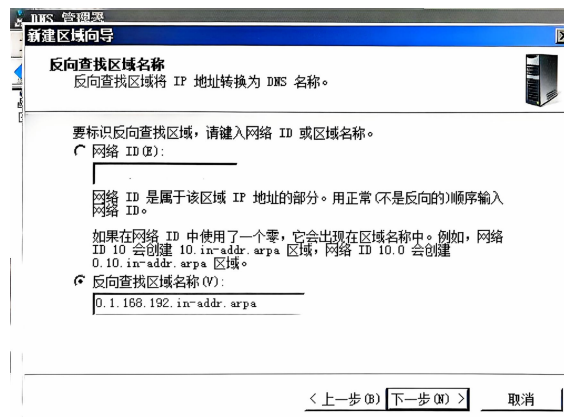
学号：2022141460176 姓名：杨一舟 专业：计算机科学与技术 第 7 周

课程名称	计算机网络课程设计	实验课时	2 课时
实验项目	DNS 服务器配置与 DNS 协议分析	实验时间	2024 年 10 月 17 日
实验目的	在 Windows Server 环境下, 搭建并配置局域网内部的 DNS 服务器, 并通过对 DNS 报文的捕获和分析, 掌握 DNS 协议的原理和工作过程。		
实验环境	Windows Server 、 Wire Shark		
实验内容（算法、程序、步骤和方法）	一、在 Windows Server 系统下搭建 DNS 服务器		
	<div>1.1. 配置 DNS 正向查找区域</div> <div>在“开始”中通过管理工具打开 DNS 管理器。</div> <div>创建正向查找区域的步骤如下：</div> <div><div>1. 新建区域。</div><div>2. 选择主要区域。</div><div>3. 输入新建区域域名 test.com</div><div>5. 创建区域文件。</div><div>6. 选择不允许动态更新。</div></div> <div></div>		

1.2 创建反向查找区域

反向区域是用于将 IP 地址映射到对应的域名
创建反向查找区域的步骤如下：

1. 新建区域。
2. 选择主要区域。
3. 点击反向查找区域。
4. 选择 IPv4 反向查找区域。
5. 网络 ID 填写为 192.168.1.0
6. 创建区域文件。
7. 点击不允许动态更新。

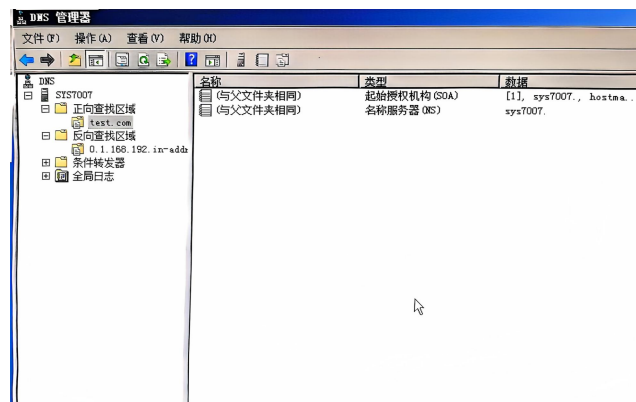


1.3 新建主机

新建并配置主机的步骤如下：

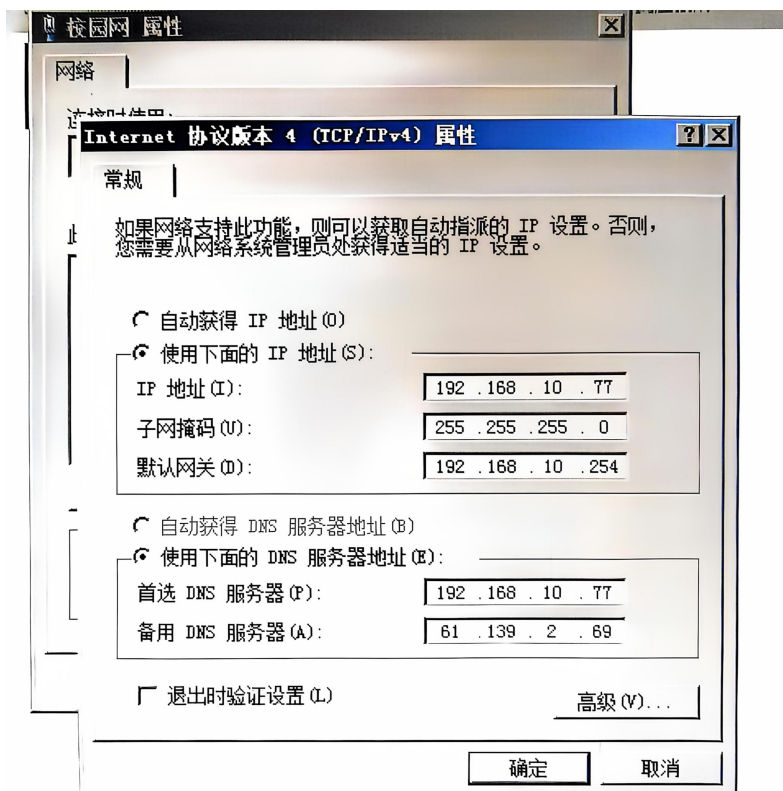
1. 选择正向查找区域的 test.com 区域。
2. 选择“新建主机”选项，进入主机域名的配置界面。
3. 输入主机名“www”和该主机的 IP 地址。
4. 在别名配置界面，输入“www1”作为别名

完成 1.1 至 1.3 后应如下图所示：



1.4 DNS 客户端配置，配置本机 IP 地址为 DNS 服务器

在开始中打开网络和共享中心，选择属性中的 Internet 协议版本 4，在首选 DNS 服务器中填写本机的 IP 地址 192.168.10.77



1.5 DNS 解析测试

正向域名解析：在 Windows 的 cmd 中先使用 ipconfig/flushdns 来清空主机的 DNS 缓存。然后输入主机域名 ping www.test.com 与主机别名 ping www1.test.com，观察能否成功解析域名。

```
C:\Users\Administrator>ping www.test.com

正在 Ping www.test.com [192.168.10.77] 具有 32 字节的数据:
来自 192.168.10.77 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.10.77 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.10.77 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.10.77 的回复: 字节=32 时间<1ms TTL=64

192.168.10.77 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间<以毫秒为单位>:
        最短 = 0ms, 最长 = 0ms, 平均 = 0ms
```

```
C:\Users\Administrator>ping www1.test.com

正在 Ping www.test.com [192.168.10.77] 具有 32 字节的数据:
来自 192.168.10.77 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.10.77 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.10.77 的回复: 字节=32 时间<1ms TTL=64
来自 192.168.10.77 的回复: 字节=32 时间<1ms TTL=64

192.168.10.77 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间<以毫秒为单位>:
        最短 = 0ms, 最长 = 0ms, 平均 = 0ms
```

反向域名解析: 通过 nslookup 命令进行测试, 能够通过 IP 获取到对应的域名则解析成功。

```
C:\Users\Administrator>nslookup 192.168.10.77
服务器:  www.test.com
Address:  192.168.10.77

名称:     www.test.com
Address:  192.168.10.77
```

二、利用 Wire shark 抓取 DNS 数据包

1) 在捕获 ping 命令的 ICMP 报文之前, 从客户端主机发送了什么类型的应用层报文?

发送了 DNS 报文

253	1.727355	192.168.10.77	1.192.137.42	DNS	676 Standard query 0x0a04[Malformed Packet]
254	1.751835	1.192.137.42	192.168.10.77	DNS	261 Standard query 0x0a04[Malformed Packet]
255	1.752056	1.192.137.42	192.168.10.77	DNS	261 Standard query 0x0a04[Malformed Packet]
256	1.752084	192.168.10.77	1.192.137.42	ICMP	289 Destination unreachable (Port unreachable)
390	2.564282	192.168.10.77	1.192.137.42	DNS	676 Standard query 0x0a04[Malformed Packet]
392	2.596457	1.192.137.42	192.168.10.77	DNS	261 Standard query 0x0a04[Malformed Packet]
393	2.596678	1.192.137.42	192.168.10.77	DNS	261 Standard query 0x0a04[Malformed Packet]
521	3.401162	192.168.10.77	1.192.137.42	DNS	676 Standard query 0x0a04[Malformed Packet]
523	3.428269	1.192.137.42	192.168.10.77	DNS	261 Standard query 0x0a04[Malformed Packet]
524	3.428488	1.192.137.42	192.168.10.77	DNS	261 Standard query 0x0a04[Malformed Packet]
525	3.428515	192.168.10.77	1.192.137.42	ICMP	289 Destination unreachable (Port unreachable)

(接上)
实验内容
(算法、程序、步骤和方法)

2) DNS 报文是封装在 UDP 报文, 还是封装在 TCP 的报文中?

封装在 UDP 报文中

```
√ Internet Protocol Version 4, Src: 193.0.14.129, Dst: 192.168.10.77
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
  > Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
    Total Length: 758
    Identification: 0x8bba (35770)
  > 000. .... = Flags: 0x0
    ...0 0000 0000 0000 = Fragment Offset: 0
    Time to Live: 54
    Protocol: UDP (17)
    Header Checksum: 0x5bc9 [validation disabled]
    [Header checksum status: Unverified]
    Source Address: 193.0.14.129
    Destination Address: 192.168.10.77
    [Stream index: 30]
  > User Datagram Protocol, Src Port: 53, Dst Port: 64904
  > Domain Name System (response)
```

3) 在解析 www.test.com 域名时, 服务器用什么类型的资源记录作为应答报文返回给客户端?

返回了 A 类型的记录

```
√ Domain Name System (response)
  Transaction ID: 0x58a5
  > Flags: 0x8010 Standard query response, No error
  Questions: 1
  Answer RRs: 0
  Authority RRs: 7
  Additional RRs: 11
  > Queries
    > i.pki.goog: type A, class IN
  > Authoritative nameservers
  > Additional records
```

4) 在进行别名 www1.test.com 域名解析时, 服务器返回什么类型的资源记录?

返回了 CNAME 类型的记录

```
Questions: 1
Answer RRs: 2
Authority RRs: 0
Additional RRs: 0
> Queries
√ Answers
  > www1.test.com: type CNAME, class IN, cname www.test.com
    Name: www1.test.com
    Type: CNAME (Canonical NAME for an alias) (5)
    Class: IN (0x0001)
    Time to live: 3600 (1 hour)
    Data length: 10
    CNAME: www.test.com
  > www.test.com: type A, class IN, addr 192.168.10.77
```

5) 通过 nslookup 命令反向解析 IP 地址对应的域名是, 服务器返回什么类型的资源记录?

返回了 PTR 类型的记录

```
Questions: 1
Answer RRs: 0
Authority RRs: 0
Additional RRs: 0
v Queries
  v 15.10.168.192.in-addr.arpa: type PTR, class IN
    Name: 15.10.168.192.in-addr.arpa
    [Name Length: 26]
    [Label Count: 6]
    Type: PTR (domain name PoinTeR) (12)
    Class: IN (0x0001)
```

数据
记录
和计
算

本实验的主要步骤已经在实验内容部分进行了展示，并附带了实验过程中的照片记录，确保了实验的准确性和可靠性。

结论 (结果)	<p>在本实验中，我们成功配置了一台 DNS 服务器，使其能够正确响应来自客户端的域名解析请求，并且通过抓包工具观察到了标准的 DNS 查询与响应过程。实验中配置的正向查找区域功能正常，能够将指定的域名映射到对应的 IP 地址；同时，反向查找区域也正确地将 IP 地址映射回主机名。</p>
小结	<p>在本实验中，我们深入探讨了 DNS 系统的内部工作原理及其在网络通信中的重要性。通过对 DNS 服务器的配置，我们了解了如何设置区域文件、转发器以及如何处理 DNS 请求的整个流程。同时，我们也使用如 Wireshark 的抓包工具对 DNS 协议进行了分析，观察到了 DNS 请求与响应的数据包格式，理解了域名解析至 IP 地址的过程。</p>
指导老师 评议	<div>成绩评定：<div>指导教师签名：</div></div>

实验报告说明

专业实验中心

实验名称 要用最简练的语言反映实验的内容。如验证某程序、定律、算法，可写成“验证×××”；分析×××。

实验目的 目的要明确，要抓住重点，可以从理论和实践两个方面考虑。在理论上，验证定理、公式、算法，并使实验者获得深刻和系统的理解，在实践上，掌握使用实验设备的技能技巧和程序的调试方法。一般需说明是验证型实验还是设计型实验，是创新型实验还是综合型实验。

实验环境 实验用的软硬件环境（配置）。

实验内容（算法、程序、步骤和方法） 这是实验报告极其重要的内容。这部分要写明依据何种原理、定律算法、或操作方法进行实验，要写明经过哪几个步骤。还应该画出流程图（实验装置的结构示意图），再配以相应的文字说明，这样既可以节省许多文字说明，又能使实验报告简明扼要，清楚明白。

数据记录和计算 指从实验中测出的数据以及计算结果。

结论（结果） 即根据实验过程中所见到的现象和测得的数据，作出结论。

小结 对本次实验的体会、思考和建议。

备注或说明 可写上实验成功或失败的原因，实验后的心得体会、建议等。

注意：

- 实验报告将记入实验成绩；
- 每次实验开始时，交上一次的实验报告，否则将扣除此次实验成绩。