

《网络运维管理》—— 实验指导书

实验四：实现本地 DNS 服务

一、实验简介

在实验二的基础上，基于 CentOS8 操作系统通过 BIND 创建 DNS 服务器，将其部署在园区网内，为园区网内的主机提供 DNS 查询、域名解析服务，并通过抓包分析 DNS 报文结构和 DNS 服务器进行 DNS 查询的通信过程。

二、实验目的

- 1、熟悉使用 BIND 实现 DNS 服务器的方法；
- 2、掌握主、从 DNS 查询服务的配置方法；
- 3、掌握主、从域名解析服务的配置方法；
- 4、掌握 DNS 查询通信过程。

三、实验理论

- 1、DNS

四、实验规划

1、网络拓扑规划

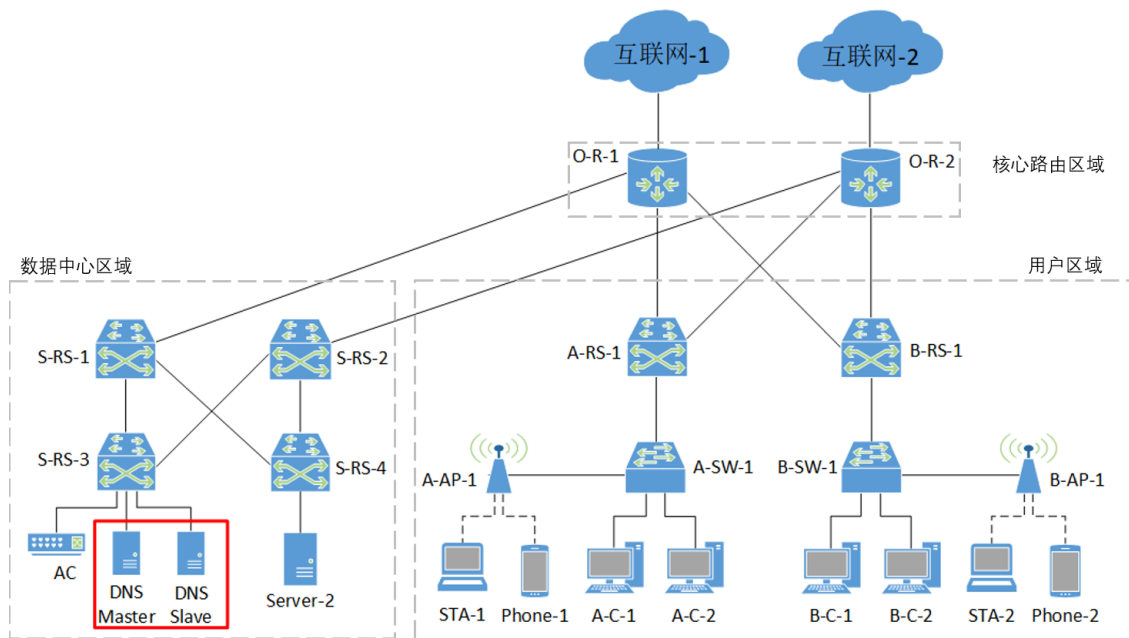


图 1 实验四的网络拓扑规划

表 1 网络设备说明

序号	设备线路	设备类型	规格型号	备注
1	A-C-1、A-C-2	用户主机	PC	A 区用户



2	B-C-1、B-C-2	用户主机	PC	B 区用户
3	STA-1、STA-2	移动终端	STA	移动用户
4	Phone-1、Phone-2	移动终端	Cellphone	移动用户
5	A-SW-1、B-SW-1	二层交换机	S3700	用户区域接入交换机
6	A-RS-1、B-RS-1	三层交换机	S5700	用户区域汇聚交换机
7	O-R-1、O-R-2	核心路由器	AR2220	核心区域路由器
8	S-RS-1、S-RS-2	三层交换机	S5700	数据中心汇聚交换机
9	S-RS-3、S-RS-4	三层交换机	S5700	数据中心接入交换机
10	A-AP-1、B-AP-1	无线接入点（AP）	AP3030	接入移动终端
11	AC-1	无线控制器	AC6605	用于 AP 的管理和配置
12	DNS Master	DNS 服务器	虚拟机接入	主 DNS 服务器
13	DNS Slave	DNS 服务器	虚拟机接入	辅 DNS 服务器

【说明】在 VirtualBox 中创建两台虚拟机，并配置成主 DNS 服务器和辅 DNS 服务器，接入到园区网的数据中心区域

2、交换机 VLAN 设计

设计要求：

- (1) 本实验采用基于端口划分 VLAN。
- (2) 用户主机（有线）VLAN 设计：第一个 VLAN ID 用自己的学号后两位+1 来定义。例如 2021181001，其第 1 个 VLAN 的 ID 是 2，后面的 VLAN 依次加 1，即 VLAN3、VLAN 4……
- (3) 移动终端（无线）VLAN 设计：第一个 VLAN ID 用自己的学号后两位+200 来定义。例如 2021181001，其第 1 个 VLAN 的 ID 是 201，后面的 VLAN 依次加 1，即 VLAN 202、VLAN203……
- (4) 无线用户终端采用 2.4GHz 和 5GHz 两个频段接入网络，分别属于不同 VLAN；
- (5) 其他 VLAN 设计：三层虚拟接口的 VLAN，AP 所属的 VLAN 等，由学生自行设计。

3、IP 地址设计

设计要求：

(1) 用户主机（含无线终端）IP 地址设计：格式是 192.A.B.*，其中，A 等于学号的最后两位，B 必须大于等于学号的后两位且小于等于学号后两位+5，*表示该位数值由考生自定。例如张三（2021181002）可以使用的 IP 地址范围是：192.2.2.0~192.2.7.255。设计用户主机 IP 地址时要考虑路由聚合。

注意：各网段的默认网关地址，使用本网段最后一个单播地址。

(2) 服务器 IP 地址设计：格式是 172.16.A.*，其中，A 等于学号的最后两位，*表示该位数值由考生自定。

(3) 路由接口 IP 地址设计：路由接口 IP 地址格式是 10.0.A.*。其中，A 等于学号的最后两位，*表示该位数值由考生自定。

(4) 其他 IP 地址设计由学生自定。

4、路由表规划

本实验采用 OSPF 协议。

5、DNS 记录规划

- (1) DNS 服务器中，至少应包括 A 记录、CNAME 记录、NS 记录；
- (2) A 记录中，**必须**至少有一条以**学生名字全拼**命名的域名记录，例如“张三”，要设置一条名为 www.zhangsan.cn 的 A 记录，其对应的 IP 地址为 200.1.1.A，A 为学号后 2 位。

五、实验内容及打分

本实验共包含 3 个任务，由学生独立完成。教师在实验课上检查实验完成情况并提出相应问题，将根据各任务的完成情况及回答问题情况进行打分。

【提示】各任务的具体操作，可参考教材或课程网站

1、任务一：在 eNSP 中部署园区网并实现全网通信（10 分）

- (1) 根据网络拓扑规划，在 eNSP 中部署硬件设备（此时不包含 DNS 服务器）；
- (2) 实现全网互通；

【提示】本实验是在实验二的基础上完成的。

2、任务二：创建 DNS 服务器（30 分）

根据前面规划设计的有关要求，创建主 DNS 服务器和辅 DNS 服务器，主要步骤包括：

- (1) 在 VirtualBox 中创建主 DNS 服务器虚拟机，并安装 CentOS 8 操作系统；
- (2) 在虚拟机上安装 BIND 并启动 named 服务；
- (3) 通过“复制”的方式，创建辅 DNS 服务器的虚拟机。

3、任务三：配置 DNS 服务（30 分）

在主 DNS 服务器上，进行 DNS 服务相关配置，主要包括

- (1) 配置 CentOS 系统自带的防火墙，开放 53 端口的 UDP 协议和 TCP 协议；
- (2) 修改主配置文件/etc/named.conf，包括修改 53 端口监听信息等；
- (3) 修改区域声明文件/etc/named.rfc1912.zones
- (4) 创建域名的正向解析区域配置文件，在文件中添加各种记录信息；
- (5) 重启 named 服务

4、任务四：为园区网用户提供本地域名服务（30 分）

将 DNS 服务器部署进园区网，并且为园区网内的用户主机提供 DNS 服务，主要包括：

- (1) 将 DNS-Master 和 DNS-Slave 服务器部署到园区网；
- (2) 配置 DNS-Master 和 DNS-Slave 的 IP 地址，使得园区网内用户能够访问到 DNS 服务器；
- (3) 测试验证主、从 DNS 服务器之间的数据同步；
- (4) 将 DNS-Master 和 DNS-Slave 分别设置为园区网用户主机的本地域名服务器（一个为主、一个为辅）；
- (5) 测试 DNS 服务的效果。



4、回答问题 (30 分)

教师在实验课上检查实验完成情况并提出相应问题, 将根据各任务的完成情况及回答问题情况进行打分。

六、实验拓展及分析

1、本实验中, 假设有两位同学在配置 DNS 服务器 (虚拟机) 的网卡时, 一个将网卡设置成“桥接”模式, 另一个将 DNS 服务器 (即虚拟机) 的网卡设置为“网络地址转换 (NAT)”, 最后都可以连接互联网并完成 DNS 的在线安装, 请分析一下他们分别是如何具体配置的?

2、分别将 211.69.32.8、114.114.114.114、8.8.8.8 作为本地 DNS, 然后用 nslookup 命令测试 www.baidu.com 的 DNS 查询结果, 例如

```
C:\Users\XCg>nslookup www.baidu.com 8.8.8.8
```

分别写出每次 DNS 查询的结果, 即 www.baidu.com 对应的 IP 地址, 对比这些地址是否一样, 若不一样, 试着分析原因。

3、在上面第 2 题中, 执行 nslookup www.baidu.com 8.8.8.8 后, 显示结果如下图, 其中显示出“非权威应答”, 试分析其原因。

```
C:\Users\XuChenggang>nslookup www.baidu.com 8.8.8.8
服务器: dns.google
Address: 8.8.8.8

非权威应答:
名称: www.a.shifen.com
Addresses: 240e:83:205:58:0:ff:b09f:36bf
           240e:83:205:5a:0:ff:b05f:346b
           220.181.38.150
           220.181.38.149
Aliases: www.baidu.com
```

4、假设 A-C-1 访问 www.baidu.com, 但其不知道 www.baidu.com 对应的 IP 地址, 并且其本地 DNS 服务器 (172.16.64.10) 也不知道如何解析该域名。因此本地 DNS 要通过迭代查询的方式, 向互联网上的 DNS 服务器 (包括根 DNS、顶级 DNS 等) 进行查询。并将查询的结果 (即 www.baidu.com 对应的 IP 地址) 反馈给 A-C-1。

请通过抓包, 验证上述的 DNS 查询过程。

