Лабораторная работа № 14

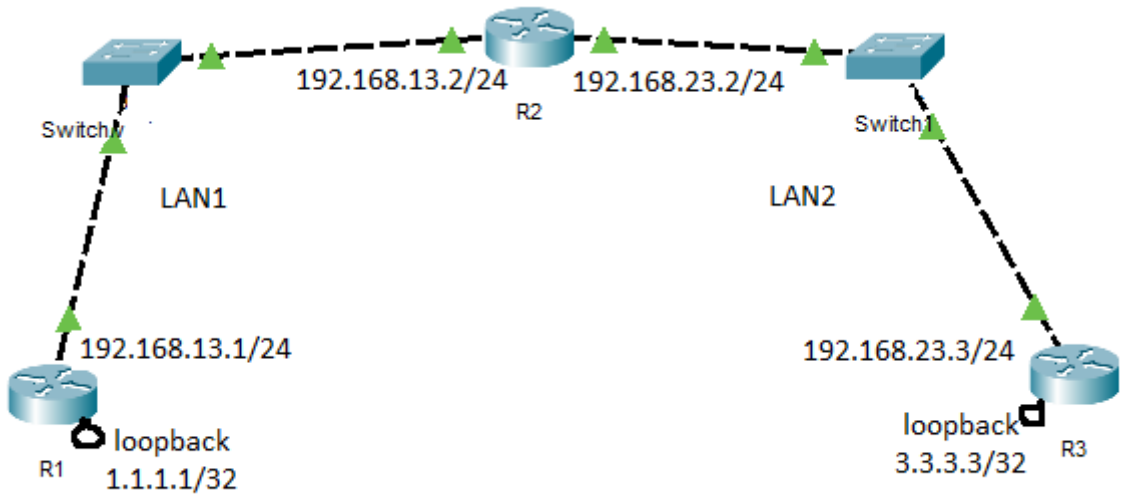
Тема: Сетевые сервисы на Linux. DNS-сервер на linux.
Цель работы: Создать и настроить DNS-сервер на базе операционной системы Linux.
Необходимое оборудование и программное обеспечение: Виртуальные машины под управлением Linux (CentOS, Ubuntu или др.).

Пример настройки серверов.

Тестовый стенд состоит и трех виртуальных машин на Centos 7.
R1:
Nic1 – NAT (что бы был доступ в Интернет)
Nic2 – внутренняя сеть (lan1) 192.168.13.0/24
dummy0 – 1.1.1.1/32

R2:
Nic1 – NAT (что бы был доступ в Интернет)
Nic2 – внутренняя сеть (lan1) 192.168.13.2/24
Nic3 – внутренняя сеть (lan2) 192.168.23.2/24
dummy0 – 2.2.2.2/32

R3:
Nic1 – NAT (что бы был доступ в Интернет)
Nic2 – внутренняя сеть (lan2) 192.168.23.0/24
dummy0 –3.3.3.3/32



Установка BIND (Berkeley Internet Name Domain):
sudo yum install bind bind-utils -y

```
[root@r2 ~]# yum install bind bind-utils -y
Загружены модули: fastestmirror
Loading mirror speeds from cached hostfile
 * base: mirror.ps.kz
 * epel: epel.sg.ssimn.org
```

Конфигурация BIND: Основной конфигурационный файл BIND располагается в **/etc/named.conf**

Указываем, на каком адресе слушать сокет и кому можно отправлять запросы

```
options {
        listen-on port 53 { 127.0.0.1;192.168.13.2;2.2.2.2; };
        listen-on-v6 port 53 { ::1; };
        directory       "/var/named";
        dump-file       "/var/named/data/cache_dump.db";
        statistics-file "/var/named/data/named_stats.txt";
        memstatistics-file "/var/named/data/named_mem_stats.txt";
        recursing-file  "/var/named/data/named.recursing";
        secroots-file   "/var/named/data/named.secroots";
        allow-query     { any; };
```

В конце файла добавляем:
include "/etc/named/named.conf.local";

```
include "/etc/named.rfc1912.zones";
include "/etc/named.root.key";
include "/etc/named/named.conf.local";
```

Теперь настраиваем /etc/named/named.conf.local
В этом файле мы указываем, какие будут зоны. Так как мы создаем файл с нуля, он будет пустым.
Рассмотрим на примере домена catec2024.net:

```
  GNU nano 2.3.1          Файл: /etc/named/named.conf.local

zone "catec2024.net" {
    type master;
    file "/etc/named/zones/db.catec2024.net";
    allow-query { any; };
};

zone "3.3.3.in-addr.arpa" {
    type master;
    file "/etc/named/zones/db.3.3.3";
};
```

Создаём файлы зон внутри /etc/named/zones/ директории:
mkdir /etc/named/zones
nano /etc/named/zones/db.catec2024.net

```
  GNU nano 2.3.1        Файл: /etc/named/zones/db.catec2024.net

$TTL    86400
@       IN      SOA     www.catec2024.net. admin.catec2024.net. (
         2024032001      ; Serial (дата + двузначный номер)
             604800      ; Refresh
              86400      ; Retry
            2419200      ; Expire
             604800 )    ; Negative Cache TTL
;
; Name servers - NS records
       IN      NS      www.catec2024.net.

; Name servers - A records
www.catec2024.net.          IN    A     3.3.3.3

; 3.3.3.3/32 - A records
www.catec2024.net.          IN    A     3.3.3.3
```

файл обратной зоны
nano /etc/named/zones/db.3.3.3

```
  GNU nano 2.3.1          Файл: /etc/named/zones/db.3.3.3

$TTL 604800
@     IN      SOA     catec2024.net. admin.catec2024.net. (
       2024032002      ; Serial (дата + двузначный номер)
           604800      ; Refresh
            86400      ; Retry
          2419200      ; Expire
           604800 )    ; Negative Cache TTL

; name servers
    IN NS www.catec2024.net.

; PTR Records
3 IN PTR www.catec2024.net. ; 3.3.3.3
```

Для проверки валидности синтаксиса конфига демона можно пользоваться утилитой named-checkconf.

```
[root@r2 ~]# named-checkconf
[root@r2 ~]#
```

Синтаксис зон проверяется другой утилитой — named-checkzone. Она требует ввода имени зоны и файла зоны. Например:
named-checkzone catec2024.net /etc/named/zones/db.catec2024.net

```
[root@r2 ~]# named-checkzone catec2024.net /etc/named/zones/db.catec2024.net
zone catec2024.net/IN: loaded serial 2024032001
OK
[root@r2 ~]#
```

После того, как проверили, что синтаксис валиден, не забываем включить сервис:

```
[root@r2 ~]# systemctl enable named
[root@r2 ~]# systemctl start named
[root@r2 ~]# systemctl status named
● named.service - Berkeley Internet Name Domain (DNS)
   Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; vendor preset: d
isabled)
   Active: active (running) since Ср 2024-03-20 17:56:44 +05; 13min ago
 Main PID: 1602 (named)
   CGroup: /system.slice/named.service
           └─1602 /usr/sbin/named -u named -c /etc/named.conf

мар 20 17:56:44 r2 named[1602]: zone 3.3.3.in-addr.arpa/IN: loaded serial 2...02
мар 20 17:56:44 r2 named[1602]: zone catec2024.net/IN: loaded serial 2024032001
мар 20 17:56:44 r2 named[1602]: zone 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.... 0
мар 20 17:56:44 r2 named[1602]: zone localhost/IN: loaded serial 0
мар 20 17:56:44 r2 named[1602]: zone localhost.localdomain/IN: loaded serial 0
мар 20 17:56:44 r2 named[1602]: all zones loaded
мар 20 17:56:44 r2 named[1602]: running
мар 20 17:56:44 r2 named[1602]: zone 3.3.3.in-addr.arpa/IN: sending notifie...2)
мар 20 17:56:54 r2 named[1602]: managed-keys-zone: Unable to fetch DNSKEY s...ut
мар 20 17:56:54 r2 named[1602]: resolver priming query complete
Hint: Some lines were ellipsized, use -l to show in full.
[root@r2 ~]#
```

Добавим правило в файоволл:

```
[root@r2 ~]# firewall-cmd --zone=public --add-service=dns --permanent
success
[root@r2 ~]# firewall-cmd --reload
success
[root@r2 ~]# firewall-cmd --list-all
public (active)
  target: default
  icmp-block-inversion: no
  interfaces: enp0s3 enp0s8 enp0s9
  sources:
  services: dhcpv6-client dns ssh
  ports: 3260/tcp
  protocols: ospf
  masquerade: no
  forward-ports:
  source-ports:
  icmp-blocks:
  rich rules:

[root@r2 ~]#
```

Прописываем DNS – сервер в настройках DHCP:

```
  GNU nano 2.3.1            Файл: /etc/dhcp/dhcpd.conf

#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.example
#   see dhcpd.conf(5) man page
#
# Сеть 1
subnet 192.168.13.0 netmask 255.255.255.0 {
    range 192.168.13.100 192.168.13.200;
    option routers 192.168.13.2;
    option domain-name-servers 2.2.2.2, 8.8.8.8;
}

# Сеть 2
subnet 192.168.23.0 netmask 255.255.255.0 {
    range 192.168.23.100 192.168.23.200;
    option routers 192.168.23.2;
    option domain-name-servers 8.8.8.8;
}
```

Перезапускаем DHCP-сервер

```
[root@r2 ~]# systemctl restart dhcpd
[root@r2 ~]#
```

Перезапустим процесс получения настроек на хосте r1, и попробуем узнать IP-адрес по имени домена:

```
[root@r1 ~]# dhclient enp0s8
[root@r1 ~]# dig www.catec2024.net @2.2.2.2

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.15 <<>> www.catec2024.net @2.2.2.2
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 59785
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;www.catec2024.net.             IN      A

;; ANSWER SECTION:
www.catec2024.net.      86400   IN      A       3.3.3.3

;; AUTHORITY SECTION:
catec2024.net.          86400   IN      NS      www.catec2024.net.

;; Query time: 5 msec
;; SERVER: 2.2.2.2#53(2.2.2.2)
;; WHEN: Ср мар 20 18:15:23 +05 2024
;; MSG SIZE  rcvd: 76

[root@r1 ~]# _
```

DNS работает.

Задание:

1. Собрать стенд из 3-х виртуальных машин, согласно схеме и вашего варианта задания. Имена хостов должны содержать ваше имя на латинице, например: stepan-r1 или ravhat-r2.

2. Настроить DHCP – сервер.

3. Настроить интерфейсы DHCP-клиентов на получение настроек от сервера.

4. Проверить связность командой ping или mtr.

№ варианта	LAN 1	LAN 2
1	192.168.10.0/24	192.168.20.0/24
2	192.168.30.0/24	192.168.40.0/24
3	192.168.50.0/24	192.168.60.0/24
4	192.168.70.0/24	192.168.80.0/24
5	192.168.90.0/24	192.168.100.0/24
6	192.168.110.0/24	192.168.120.0/24
7	192.168.130.0/24	192.168.140.0/24
8	192.168.150.0/24	192.168.160.0/24
9	192.168.170.0/24	192.168.180.0/24
10	192.168.190.0/24	192.168.200.0/24
11	192.168.210.0/24	192.168.220.0/24
12	192.168.230.0/24	192.168.240.0/24
13	192.168.10.0/24	192.168.20.0/24
14	192.168.30.0/24	192.168.40.0/24
15	192.168.50.0/24	192.168.60.0/24
16	192.168.70.0/24	192.168.80.0/24
17	192.168.90.0/24	192.168.100.0/24
18	192.168.110.0/24	192.168.120.0/24
19	192.168.130.0/24	192.168.140.0/24
20	192.168.150.0/24	192.168.160.0/24