7-PR-DNS-3

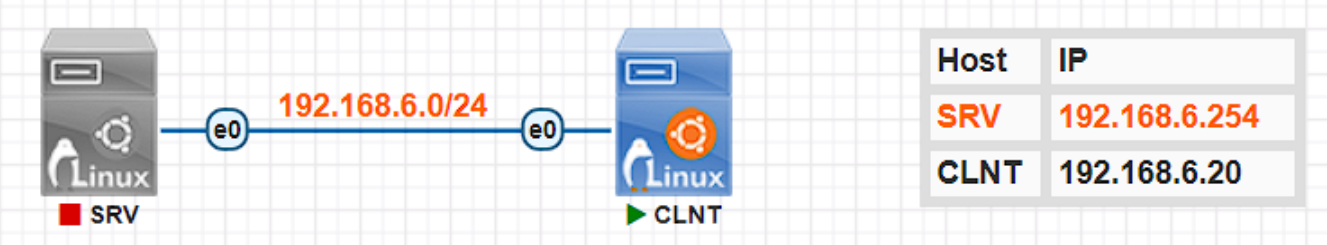

Таблица адресов

Hosts	Address
Client	DHCP
DNS1	192.168.1.11/26
DNS2	192.168.1.12/26
RTR	192.168.1.1/26
	DHCP

Задание

Базовая настройка

1. Настройте имена устройств в соответствии с топологией ``hostnamectl set-hostname ...
2. Настройте адреса устройств в соответствии с таблицей адресов

```
#DNS1
auto ens4
iface ens4 inet static
        address 192.168.1.11/26
        gateway 192.168.1.1
#DNS2

auto ens4
iface ens4 inet static
        address 192.168.1.12/26
        gateway 192.168.1.1

#RTR
```

```
auto ens4
iface ens4 inet static
        address 192.168.1.11/26


#Client
    auto ens4
iface ens4 inet dhcp
    #ставим DHCP протокол на роутер
    apt install isc-dhcp-server
    vi /etc/dhcp/dhcpd.conf/
    option domain-name "vm.local";
    option domain-name-server 192.168.1.11, 192.168.1.12;

    subnet 192.168.1.0 netmask 255.255.255.192{
        range 192.168.1.16 192.168.1.62;
        option domain-name-server 192.168.1.11, 192.168.1.12;
        option domain-name "vm.local";
        option routers 192.168.1.1;
        }
    vi /etc/default/isc-dhcp-server/
    INTERFACESv4 = "ens5"

#Применение коонфигурраций
systemctl restart networking
systemctl restart isc-dhcp-server
```

1. Настройте на серверах DNS сервера - адреса DNS1, DNS2

Сетевые службы

1. Настройте DHCP сервер на RTR
    1. DNS сервера - адреса DNS1 и DNS2
    2. Имя домена - vm.local

```
apt install bind9
#DNS1
cp /etc/bind/named.conf.local /var/lib/bind/vm.zone
cp /etc/bind/named.conf.options /var/lib/bind/
cp /etc/bind/db.local /var/lib/bind/vm.local
cp /var/lib/bind/vm.local /var/lib/bind/db.vm.local
```

```
zone "vm.local" {
        type.master;
        file '/var/lib/bind/vm.local";
        allow-transfer { 192.168.1.12; };

};

zone "1.168.192.in-addr.arpa" {
        type master;
        file "/var/lib/bind/db.vm.local";
        allow-update { 192.168.1.11; };
};
```

```
acl clients {
        localhost;
        192.168.1.0/26;
};
options {
        directory "/var/cache/bind";

        // If there is a firewall betwe
        // to talk to, you may need to
        // ports to talk.  See http://u

        // If your ISP provided one or
        // nameservers, you probably wa
        // Uncomment the following bloc
        // the all-0's placeholder.

        // forwarders {
        //      0.0.0.0;
        // };

        //==============================
        // If BIND logs error messages
        // you will need to update your
        //==============================
        dnssec-validation auto;

        listen-on-v6 { any; };

        allow-query{ clients; };
        recursion yes;
};
```

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     vm.local. root.vm.local. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      vm.local.
@       IN      A       127.0.0.1
@       IN      AAAA    ::1
```

1. Настройте на RTR кэширующий DNS
    1. Должен принимать запрос только на внутренний адрес
    2. Разрешите обработку запрос только адресов из локальной сети
        1. Создайте список доступа
    3. Разрешите рекурсивные запросы

```
option domain-name "vm.local";
option domain-name-servers 192.168.1.11, 192.168.1.12;

default-lease-time 600;
max-lease-time 7200;

# The ddns-updates-style parameter controls whether or n
# attempt to do a DNS update when a lease is confirmed.
# behavior of the version 2 packages ('none', since DHCP
# have support for DDNS.)
ddns-update-style interim;

update-static-leases on;

zone vm.local {
        primary 192.168.1.11;
        secondary 192.168.1.12;
}
zone 1.168.192.in-addr.arpa {
        primary 192.168.1.11;
        secondary 192.168.1.12;
}
```

```
# A slightly different configuration for an internal subnet.
subnet 192.168.1.0 netmask 255.255.255.192 {
  range 192.168.1.16 192.168.1.62;
  option domain-name-servers 192.168.1.11, 192.168.1.12;
  option domain-name "vm.local";
  option routers 192.168.1.1;

}
```

2. Настройте DNS1 как уполномоченный DNS сервер

```
acl clients {
        localhost;
        192.168.1.0/26;
};
options {
        directory "/var/cache/bind";

        // If there is a firewall between you and
        // to talk to, you may need to fix the fir
        // ports to talk.  See http://www.kb.cert.

        // If your ISP provided one or more IP add
        // nameservers, you probably want to use t
        // Uncomment the following block, and inse
        // the all-0's placeholder.

         forwarders {
                192.168.1.1;
         };

        //========================================
        // If BIND logs error messages about the r
        // you will need to update your keys.  See
        //========================================
        dnssec-validation auto;

        listen-on-v6 { any; };

        allow-query_{ clients; };
        recursion yes;
};
```

```
zone "vm.local" {
        type master;
        file "/var/lib/bind/vm.local";
        allow-transfer { 192.168.1.12; };
        allow-update { 192.168.1.1; };
};

zone "1.168.192.in-addr.arpa" {
        type master;
        file "/var/lib/bind/arpa.vm.local";
        allow-transfer { 192.168.1.12; };
        allow-update { 192.168.1.1; };
};
```

1. Неразрешимые запросы должны пересылаться на адрес RTR
2. Создайте зоны:

1. **vm.local**

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     vm.local. root.vm.local. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      vm.local.
@               NS      dns2.vm.local.
@               NS      dns2.vm.local.
@       IN      A       127.0.0.1
@       IN      AAAA    ::1
dns1            A       192.168.1.11
dns2            A       192.168.1.12
rtr             A       192.168.1.1
ntp             CNAME   rtr.vm.local.
www             CNAME   dns1.vm.local.
Client          A       192.168.1.52
~
```

2. **обратного просмотра**

```
$ORIGIN .
$TTL 604800     ; 1 week
1.168.192.in-addr.arpa  IN SOA  vm.local. root.vm.local. (
                                3          ; serial
                                604800     ; refresh (1 week)
                                86400      ; retry (1 day)
                                2419200    ; expire (4 weeks)
                                604800     ; minimum (1 week)
                                )
                        NS      vm.local.
                        A       127.0.0.1
                        AAAA    ::1
$ORIGIN 1.168.192.in-addr.arpa.
1                       PTR     rtr.vm.local.
11                      PTR     dns1.vm.local.
12                      PTR     dn2.vm.local.
$TTL 300        ; 5 minutes
52                      PTR     Client.vm.local.
~
```

3. Создайте записи для служб:
    1. A записи для DNS серверов и RTR
    2. NS записи для DNS серверов
    3. CNAME записи www для DNS1 и ntp для RTR
    4. PTR записи для серверов и роутера
4. Настройте динамическую регистрацию новых клиентов

3. Настройте DNS2 как подчиненный DNS сервер:

```
zone "vm.local" {
        type slave;
        masters { 192.168.1.11; };
        file "/var/lib/bind/vm.local";

};

zone "1.168.192.in-addr.arpa" {
        type slave;
        masters { 192.168.1.11; };
        file "/var/lib/bind/db.vm.local";

};
acl clients {
        localhost;
        192.168.1.0/26;
};
options {
        directory "/var/cache/bind

        // If there is a firewall
        // to talk to, you may nee
        // ports to talk.  See htt

        // If your ISP provided on
        // nameservers, you probab
        // Uncomment the following
        // the all-0's placeholder

         forwarders {
                192.168.1.1;
         };

        //========================
        // If BIND logs error mess
        // you will need to update
        //========================
        dnssec-validation auto;

        listen-on-v6 { any; };

        allow-query { clients; };
        recursion yes;
};
```

    1. Настройте получение зон с DNS1:
        1. vm.local
        2. обратного просмотра
    2. Настройте динамическую регистрацию новых клиентов

3. Неразрешимые запросы должны пересылаться на адрес RTR

```
;
; BIND data file for local loopback interface
;
$TTL    604800
@       IN      SOA     vm.local. root.vm.local. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      vm.local.
@               NS      dns1.vm.local.
@               NS      dns2.vm.local.
@       IN      A       127.0.0.1
@       IN      AAAA    ::1
dns1            A       192.168.1.11
dns2            A       192.168.1.12
ntp             CNAME   rtr.vm.local.
rtr             A       192.168.1.1
www             CNAME   dns1.vm.local.
Client          A       192.168.1.52
~
```

```
;
$TTL    604800
1.168.192.in-addr.arpa  IN      SOA     vm.local. root.vm.local. (
                              2         ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;
@       IN      NS      vm.local.
@       IN      A       127.0.0.1
@       IN      AAAA    ::1
1               PTR     rtr.vm.local.
11              PTR     dns1.vm.local.
12              PTR     dns2.vm.local.
52              PTR     Client.vm.local.
```

Минимальная самопроверка

1. Клиент получает адрес по DHCP
   `ip -c add`
2. Клиент успешно запрашивает адреса для имен серверов и служб
   `nslookup vm.local`
3. Адрес клиента так же резолвится как по имени так и по адресу
   `vi /etc/resolv.conf`