Лабораторная работа № 2. Настройка DNS-сервера.

Данила Стариков
НПИбд-02-22

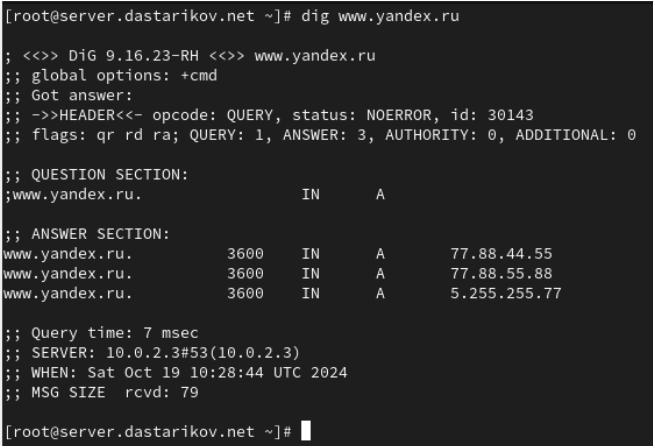
Российский университет дружбы народов имени Патриса Лумумбы

2024

Цель работы

- Приобретение практических навыков по установке и конфигурированию DNS-сервера, усвоение принципов работы системы доменных имён.

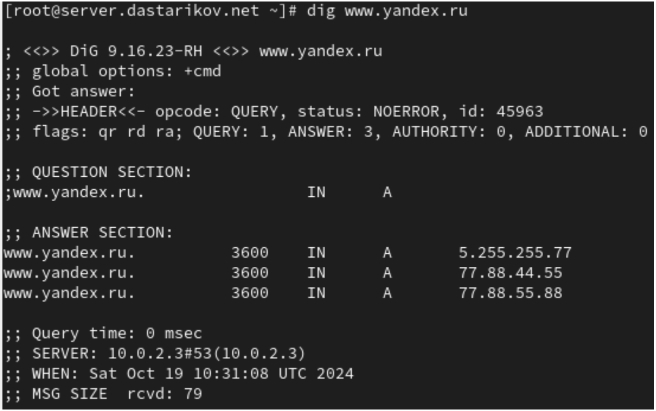
Установка DNS-сервера



```
[root@server.dastarikov.net ~]# dig www.yandex.ru

; <<>> DiG 9.16.23-RH <<>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 30143
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.yandex.ru.                 IN      A

;; ANSWER SECTION:
www.yandex.ru.          3600    IN      A       77.88.44.55
www.yandex.ru.          3600    IN      A       77.88.55.88
www.yandex.ru.          3600    IN      A       5.255.255.77

;; Query time: 7 msec
;; SERVER: 10.0.2.3#53(10.0.2.3)
;; WHEN: Sat Oct 19 10:28:44 UTC 2024
;; MSG SIZE  rcvd: 79

[root@server.dastarikov.net ~]#
```

Рис.: Запрос к DNS-адресу www.yandex.ru

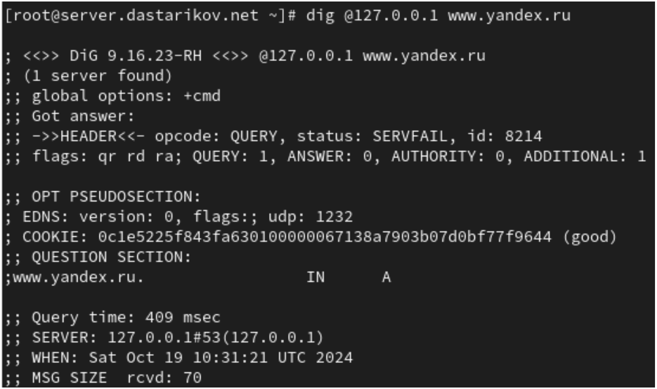
Конфигурирование кэширующего DNS-сервера при отсутствии фильтрации DNS-запросов маршрутизаторами



```
[root@server.dastarikov.net ~]# dig www.yandex.ru

; <<>> DiG 9.16.23-RH <<>> www.yandex.ru
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 45963
;; flags: qr rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;www.yandex.ru.                 IN      A

;; ANSWER SECTION:
www.yandex.ru.          3600    IN      A       5.255.255.77
www.yandex.ru.          3600    IN      A       77.88.44.55
www.yandex.ru.          3600    IN      A       77.88.55.88

;; Query time: 0 msec
;; SERVER: 10.0.2.3#53(10.0.2.3)
;; WHEN: Sat Oct 19 10:31:08 UTC 2024
;; MSG SIZE  rcvd: 79
```

Рис.: Запрос к DNS-адресу www.yandex.ru

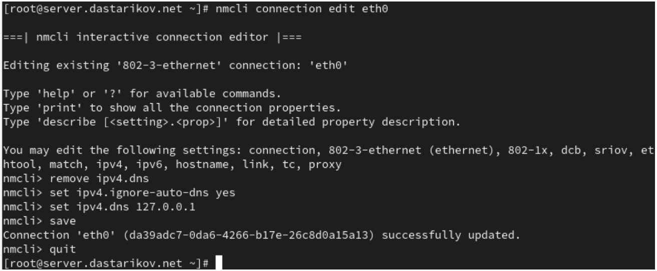
Конфигурирование кэширующего DNS-сервера при отсутствии фильтрации DNS-запросов маршрутизаторами



```
[root@server.dastarikov.net ~]# dig @127.0.0.1 www.yandex.ru

; <<>> DiG 9.16.23-RH <<>> @127.0.0.1 www.yandex.ru
; (1 server found)
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: SERVFAIL, id: 8214
;; flags: qr rd ra; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 0c1e5225f843fa630100000067138a7903b07d0bf77f9644 (good)
;; QUESTION SECTION:
;www.yandex.ru.                 IN      A

;; Query time: 409 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sat Oct 19 10:31:21 UTC 2024
;; MSG SIZE  rcvd: 70
```

Рис.: Запрос к DNS-адресу www.yandex.ru с заданным адресом сервера.

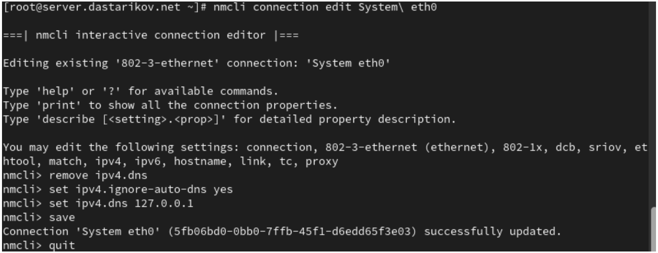
Конфигурирование кэширующего DNS-сервера при отсутствии фильтрации DNS-запросов маршрутизаторами



```
[root@server.dastarikov.net ~]# nmcli connection edit eth0

===| nmcli interactive connection editor |===

Editing existing '802-3-ethernet' connection: 'eth0'

Type 'help' or '?' for available commands.
Type 'print' to show all the connection properties.
Type 'describe [<setting>.<prop>]' for detailed property description.

You may edit the following settings: connection, 802-3-ethernet (ethernet), 802-1x, dcb, sriov, et
htool, match, ipv4, ipv6, hostname, link, tc, proxy
nmcli> remove ipv4.dns
nmcli> set ipv4.ignore-auto-dns yes
nmcli> set ipv4.dns 127.0.0.1
nmcli> save
Connection 'eth0' (da39adc7-0da6-4266-b17e-26c8d0a15a13) successfully updated.
nmcli> quit
[root@server.dastarikov.net ~]# 
```

Рис.: Настройка сетевого соединения eth0.

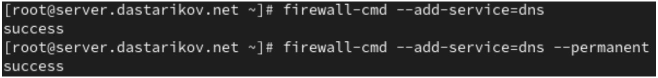
Конфигурирование кэширующего DNS-сервера при отсутствии фильтрации DNS-запросов маршрутизаторами



```
[root@server.dastarikov.net ~]# nmcli connection edit System\ eth0

===| nmcli interactive connection editor |===

Editing existing '802-3-ethernet' connection: 'System eth0'

Type 'help' or '?' for available commands.
Type 'print' to show all the connection properties.
Type 'describe [<setting>.<prop>]' for detailed property description.

You may edit the following settings: connection, 802-3-ethernet (ethernet), 802-1x, dcb, sriov, et
htool, match, ipv4, ipv6, hostname, link, tc, proxy
nmcli> remove ipv4.dns
nmcli> set ipv4.ignore-auto-dns yes
nmcli> set ipv4.dns 127.0.0.1
nmcli> save
Connection 'System eth0' (5fb06bd0-0bb0-7ffb-45f1-d6edd65f3e03) successfully updated.
nmcli> quit
```

Рис.: Настройка сетевого соединения System eth0.

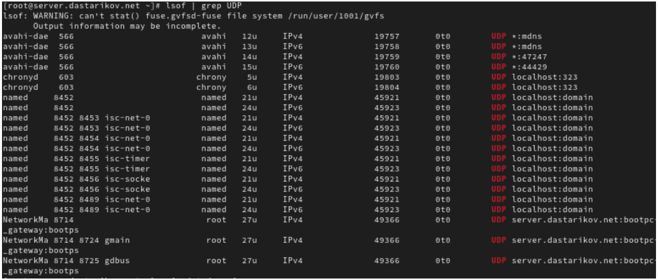
Конфигурирование кэширующего DNS-сервера при отсутствии фильтрации DNS-запросов маршрутизаторами



```
[root@server.dastarikov.net ~]# firewall-cmd --add-service=dns
success
[root@server.dastarikov.net ~]# firewall-cmd --add-service=dns --permanent
success
```

Рис.: Настройка межсетевого экрана.

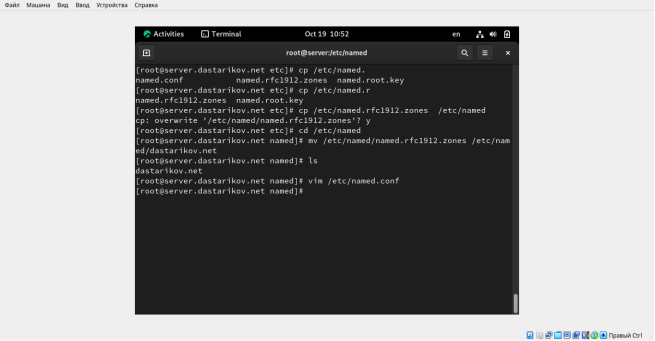
Конфигурирование кэширующего DNS-сервера при отсутствии фильтрации DNS-запросов маршрутизаторами



```
[root@server.dastarikov.net ~]# lsof | grep UDP
lsof: WARNING: can't stat() fuse.gvfsd-fuse file system /run/user/1001/gvfs
      Output information may be incomplete.
avahi-dae  566                         avahi   12u     IPv4              19757       0t0        UDP *:mdns
avahi-dae  566                         avahi   13u     IPv6              19758       0t0        UDP *:mdns
avahi-dae  566                         avahi   14u     IPv4              19759       0t0        UDP *:47247
avahi-dae  566                         avahi   15u     IPv6              19760       0t0        UDP *:44429
chronyd    603                        chrony    5u     IPv4              19803       0t0        UDP localhost:323
chronyd    603                        chrony    6u     IPv6              19804       0t0        UDP localhost:323
named     8452                         named   21u     IPv4              45921       0t0        UDP localhost:domain
named     8452                         named   24u     IPv6              45923       0t0        UDP localhost:domain
named     8452 8453 isc-net-0          named   21u     IPv4              45921       0t0        UDP localhost:domain
named     8452 8453 isc-net-0          named   24u     IPv6              45923       0t0        UDP localhost:domain
named     8452 8454 isc-net-0          named   21u     IPv4              45921       0t0        UDP localhost:domain
named     8452 8454 isc-net-0          named   24u     IPv6              45923       0t0        UDP localhost:domain
named     8452 8455 isc-timer          named   21u     IPv4              45921       0t0        UDP localhost:domain
named     8452 8455 isc-timer          named   24u     IPv6              45923       0t0        UDP localhost:domain
named     8452 8456 isc-socke          named   21u     IPv4              45921       0t0        UDP localhost:domain
named     8452 8456 isc-socke          named   24u     IPv6              45923       0t0        UDP localhost:domain
named     8452 8489 isc-net-0          named   21u     IPv4              45921       0t0        UDP localhost:domain
named     8452 8489 isc-net-0          named   24u     IPv6              45923       0t0        UDP localhost:domain
NetworkMa 8714                          root   27u     IPv4              49366       0t0        UDP server.dastarikov.net:bootpc-
_gateway:bootps
NetworkMa 8714 8724 gmain               root   27u     IPv4              49366       0t0        UDP server.dastarikov.net:bootpc-
_gateway:bootps
NetworkMa 8714 8725 gdbus               root   27u     IPv4              49366       0t0        UDP server.dastarikov.net:bootpc-
_gateway:bootps
```

Рис.: Просмотр прослушиваемых портов.

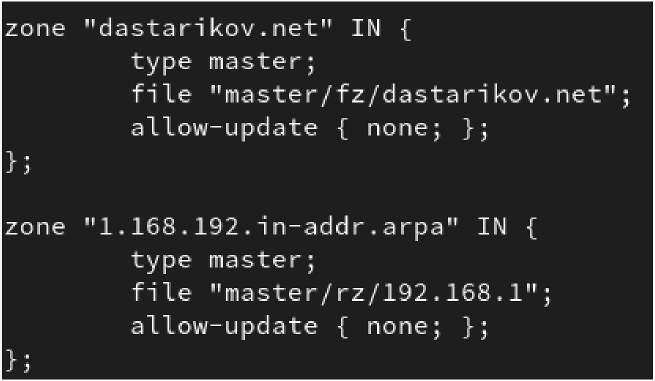
Конфигурирование кэширующего DNS-сервера при наличии фильтрации DNS-запросов маршрутизаторами



```
[root@server.dastarikov.net etc]# cp /etc/named.
named.conf           named.rfc1912.zones  named.root.key
[root@server.dastarikov.net etc]# cp /etc/named.r
named.rfc1912.zones  named.root.key
[root@server.dastarikov.net etc]# cp /etc/named.rfc1912.zones  /etc/named
cp: overwrite '/etc/named/named.rfc1912.zones'? y
[root@server.dastarikov.net etc]# cd /etc/named
[root@server.dastarikov.net named]# mv /etc/named/named.rfc1912.zones /etc/nam
ed/dastarikov.net
[root@server.dastarikov.net named]# ls
dastarikov.net
[root@server.dastarikov.net named]# vim /etc/named.conf
[root@server.dastarikov.net named]#
```

Рис.: Настройка файлов для описания DNS-зон.

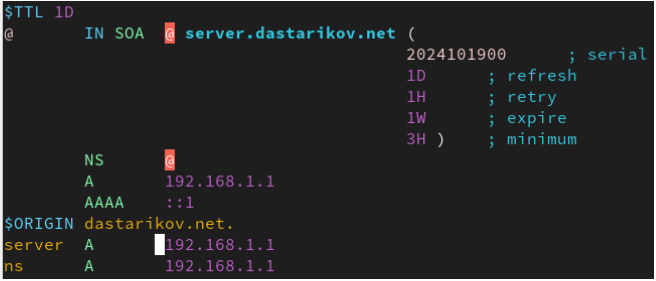
Конфигурирование кэширующего DNS-сервера при наличии фильтрации DNS-запросов маршрутизаторами



```
zone "dastarikov.net" IN {
        type master;
        file "master/fz/dastarikov.net";
        allow-update { none; };
};

zone "1.168.192.in-addr.arpa" IN {
        type master;
        file "master/rz/192.168.1";
        allow-update { none; };
};
```

Рис.: Описание DNS-зон.

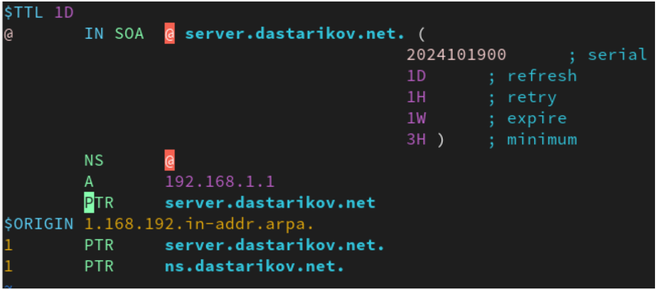
Конфигурирование кэширующего DNS-сервера при наличии фильтрации DNS-запросов маршрутизаторами



```
$TTL 1D
@       IN SOA  @ server.dastarikov.net (
                                        2024101900      ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      @
        A       192.168.1.1
        AAAA    ::1
$ORIGIN dastarikov.net.
server  A       192.168.1.1
ns      A       192.168.1.1
```

Рис.: Настройка прямой DNS-зоны.

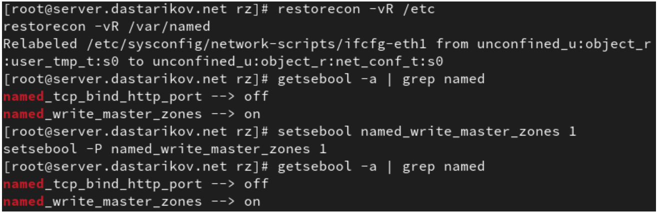
Конфигурирование кэширующего DNS-сервера при наличии фильтрации DNS-запросов маршрутизаторами



```
$TTL 1D
@       IN SOA  @ server.dastarikov.net. (
                                        2024101900      ; serial
                                        1D      ; refresh
                                        1H      ; retry
                                        1W      ; expire
                                        3H )    ; minimum
        NS      @
        A       192.168.1.1
        PTR     server.dastarikov.net
$ORIGIN 1.168.192.in-addr.arpa.
1       PTR     server.dastarikov.net.
1       PTR     ns.dastarikov.net.
```

Рис.: Настройка обратной DNS-зоны.

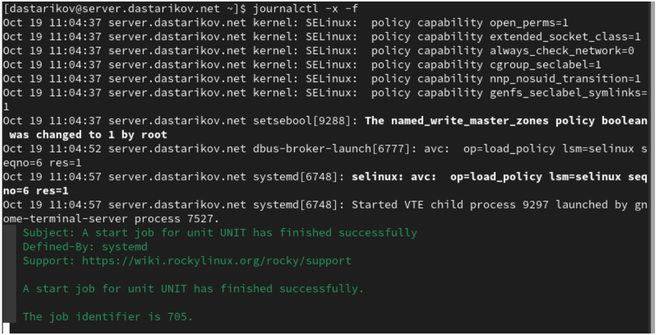
Конфигурирование кэширующего DNS-сервера при наличии фильтрации DNS-запросов маршрутизаторами



```
[root@server.dastarikov.net rz]# restorecon -vR /etc
restorecon -vR /var/named
Relabeled /etc/sysconfig/network-scripts/ifcfg-eth1 from unconfined_u:object_r
:user_tmp_t:s0 to unconfined_u:object_r:net_conf_t:s0
[root@server.dastarikov.net rz]# getsebool -a | grep named
named_tcp_bind_http_port --> off
named_write_master_zones --> on
[root@server.dastarikov.net rz]# setsebool named_write_master_zones 1
setsebool -P named_write_master_zones 1
[root@server.dastarikov.net rz]# getsebool -a | grep named
named_tcp_bind_http_port --> off
named_write_master_zones --> on
```

Рис.: Настройка меток SELinux.

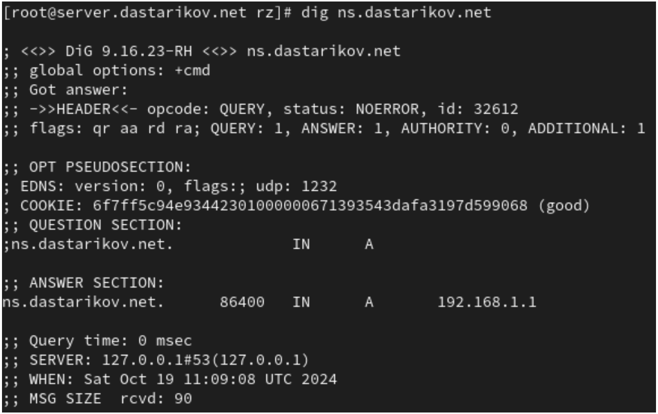
Конфигурирование кэширующего DNS-сервера при наличии фильтрации DNS-запросов маршрутизаторами



```
[dastarikov@server.dastarikov.net ~]$ journalctl -x -f
Oct 19 11:04:37 server.dastarikov.net kernel: SELinux:  policy capability open_perms=1
Oct 19 11:04:37 server.dastarikov.net kernel: SELinux:  policy capability extended_socket_class=1
Oct 19 11:04:37 server.dastarikov.net kernel: SELinux:  policy capability always_check_network=0
Oct 19 11:04:37 server.dastarikov.net kernel: SELinux:  policy capability cgroup_seclabel=1
Oct 19 11:04:37 server.dastarikov.net kernel: SELinux:  policy capability nnp_nosuid_transition=1
Oct 19 11:04:37 server.dastarikov.net kernel: SELinux:  policy capability genfs_seclabel_symlinks=
1
Oct 19 11:04:37 server.dastarikov.net setsebool[9288]: The named_write_master_zones policy boolean
 was changed to 1 by root
Oct 19 11:04:52 server.dastarikov.net dbus-broker-launch[6777]: avc:  op=load_policy lsm=selinux s
eqno=6 res=1
Oct 19 11:04:57 server.dastarikov.net systemd[6748]: selinux: avc:  op=load_policy lsm=selinux seq
no=6 res=1
Oct 19 11:04:57 server.dastarikov.net systemd[6748]: Started VTE child process 9297 launched by gn
ome-terminal-server process 7527.
   Subject: A start job for unit UNIT has finished successfully
   Defined-By: systemd
   Support: https://wiki.rockylinux.org/rocky/support

   A start job for unit UNIT has finished successfully.

   The job identifier is 705.
```

Рис.: Просмотр записей журнала системных сообщений.

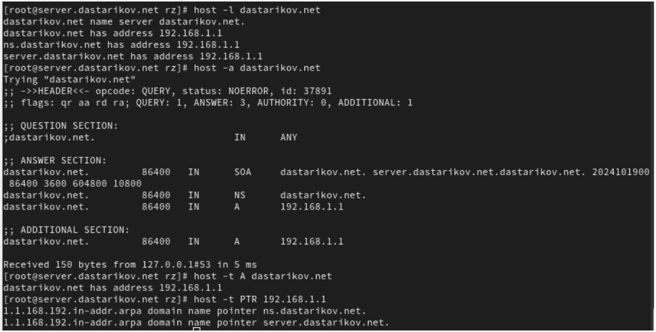
Анализ работы DNS-сервера



```
[root@server.dastarikov.net rz]# dig ns.dastarikov.net

; <<>> DiG 9.16.23-RH <<>> ns.dastarikov.net
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 32612
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 1232
; COOKIE: 6f7ff5c94e93442301000000671393543dafa3197d599068 (good)
;; QUESTION SECTION:
;ns.dastarikov.net.             IN      A

;; ANSWER SECTION:
ns.dastarikov.net.      86400   IN      A       192.168.1.1

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Sat Oct 19 11:09:08 UTC 2024
;; MSG SIZE  rcvd: 90
```

Рис.: Получение описания DNS-зоны с сервера.

Анализ работы DNS-сервера



```
[root@server.dastarikov.net rz]# host -l dastarikov.net
dastarikov.net name server dastarikov.net.
dastarikov.net has address 192.168.1.1
ns.dastarikov.net has address 192.168.1.1
server.dastarikov.net has address 192.168.1.1
[root@server.dastarikov.net rz]# host -a dastarikov.net
Trying "dastarikov.net"
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 37891
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 3, AUTHORITY: 0, ADDITIONAL: 1

;; QUESTION SECTION:
;dastarikov.net.                IN      ANY

;; ANSWER SECTION:
dastarikov.net.         86400   IN      SOA     dastarikov.net. server.dastarikov.net.dastarikov.net. 2024101900
 86400 3600 604800 10800
dastarikov.net.         86400   IN      NS      dastarikov.net.
dastarikov.net.         86400   IN      A       192.168.1.1

;; ADDITIONAL SECTION:
dastarikov.net.         86400   IN      A       192.168.1.1

Received 150 bytes from 127.0.0.1#53 in 5 ms
[root@server.dastarikov.net rz]# host -t A dastarikov.net
dastarikov.net has address 192.168.1.1
[root@server.dastarikov.net rz]# host -t PTR 192.168.1.1
1.1.168.192.in-addr.arpa domain name pointer ns.dastarikov.net.
1.1.168.192.in-addr.arpa domain name pointer server.dastarikov.net.
```

Рис.: Проверка корректиности работы DNS-сервера.

Выводы

- В результате лабораторной работы приобрели практические навыки по установке и конфигурированию DNS-сервера.