

1. Настроить nic teaming между двумя интерфейсами — server1 и server2.
Подсеть 192.168.12.0/24 будет находиться теперь на team0-интерфейсе.

Добавляем интерфейс team0 на оба сервера

```
ifcfg-team0 [----] 41 L:[ 1+14 15/ 19] *(267 / 322b) 0010 0x00A
DEVICE=team0
DEVICETYPE=Team
BOOTPROTO=static
DEFROUTE=no
PEERDNS=yes
PEERROUTES=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_PEERDNS=yes
IPV6_PEERROUTES=yes
IPV6_FAILURE_FATAL=no
NAME=team0
UUID=29453c3a-7fac-47d6-bcd0-c70e0fe5d0d2
ONBOOT=yes
IPADDR=192.168.12.11
NETMASK=255.255.255.0
```

Меняем настройки ens37 и ens38 добавляем в team0

```
ifcfg-ens37 [----] 12 L:[ 1+ 4 5/ 8] *(104 / 153b) 0050 0x032
DEVICETYPE=TeamPort
NAME=ens37-team0
UUID=e8a5d620-a054-4961-8020-99cbccfdb50c
DEVICE=ens37
TEAM_MASTER=29453c3a-7fac-47d6-bcd0-c70e0fe5d0d2
ONBOOT=yes

ifcfg-ens38 [----] 5 L:[ 1+ 4 5/ 7] *(97 / 152b) 0077 0x04D
DEVICETYPE=TeamPort
NAME=ens38-team0
UUID=c9f6fdf8-5759-4690-984b-88d1e991b75e
DEVICE=ens38
TEAM_MASTER=29453c3a-7fac-47d6-bcd0-c70e0fe5d0d2
ONBOOT=yes
```

Проверяем что получилось

```
[root@localhost network-scripts]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: ens33: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:68:56:9c brd ff:ff:ff:ff:ff:ff
    inet 192.168.2.128/24 brd 192.168.2.255 scope global ens33
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe68:569c/64 scope link
        valid_lft forever preferred_lft forever
3: ens37: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast master team0 state UP group default qlen 1000
    link/ether 00:0c:29:68:56:a6 brd ff:ff:ff:ff:ff:ff
4: ens38: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast master team0 state UP group default qlen 1000
    link/ether 00:0c:29:68:56:a6 brd ff:ff:ff:ff:ff:ff
5: dummy0: <BROADCAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group default qlen 1000
    link/ether 4a:9f:e8:a3:c4:9d brd ff:ff:ff:ff:ff:ff
    inet 1.1.1.1/32 brd 1.1.1.1 scope global dummy0
        valid_lft forever preferred_lft forever
    inet6 fe80::489f:e8ff:fea3:c49d/64 scope link
        valid_lft forever preferred_lft forever
8: team0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 00:0c:29:68:56:a6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.12.11/24 brd 192.168.12.255 scope global noprefixroute team0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fe68:56a6/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[root@localhost network-scripts]#
```

Проверяем на пинг

```
[root@localhost network-scripts]# ping 192.168.12.12
PING 192.168.12.12 (192.168.12.12) 56(84) bytes of data.
64 bytes from 192.168.12.12: icmp_seq=1 ttl=64 time=0.386 ms
64 bytes from 192.168.12.12: icmp_seq=2 ttl=64 time=0.502 ms
64 bytes from 192.168.12.12: icmp_seq=3 ttl=64 time=0.628 ms
64 bytes from 192.168.12.12: icmp_seq=4 ttl=64 time=0.591 ms
64 bytes from 192.168.12.12: icmp_seq=5 ttl=64 time=0.554 ms
^C
--- 192.168.12.12 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4038ms
rtt min/avg/max/mdev = 0.386/0.532/0.628/0.085 ms
[root@localhost network-scripts]#
```

```
[root@localhost network-scripts]# ping 192.168.12.11
PING 192.168.12.11 (192.168.12.11) 56(84) bytes of data.
64 bytes from 192.168.12.11: icmp_seq=1 ttl=64 time=0.453 ms
64 bytes from 192.168.12.11: icmp_seq=2 ttl=64 time=0.508 ms
64 bytes from 192.168.12.11: icmp_seq=3 ttl=64 time=0.492 ms
64 bytes from 192.168.12.11: icmp_seq=4 ttl=64 time=0.566 ms
^C
--- 192.168.12.11 ping statistics ---
4 packets transmitted, 4 received, 0% packet loss, time 3021ms
rtt min/avg/max/mdev = 0.453/0.504/0.566/0.049 ms
[root@localhost network-scripts]#
```

2. На интерфейсе team0 сервера server2 назначить статический IP из подсети 192.168.12.0/24.

Задали IP из целевой подсети

```
10: team0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 00:0c:29:c2:e3:41 brd ff:ff:ff:ff:ff:ff
    inet 192.168.12.12/24 brd 192.168.12.255 scope global noprefixroute team0
        valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:ec2:e341/64 scope link noprefixroute
        valid_lft forever preferred_lft forever
[root@localhost network-scripts]#
```

3. На сервере server2 настроить DHCP-сервер для выдачи динамического IP-адреса интерфейсу team0 сервера server1, а также IP-адрес DNS-сервера 3.3.3.3.

Устанавливаем yum install dhcp -y

Настраиваем файл /etc/dhcp/dhcpd.conf

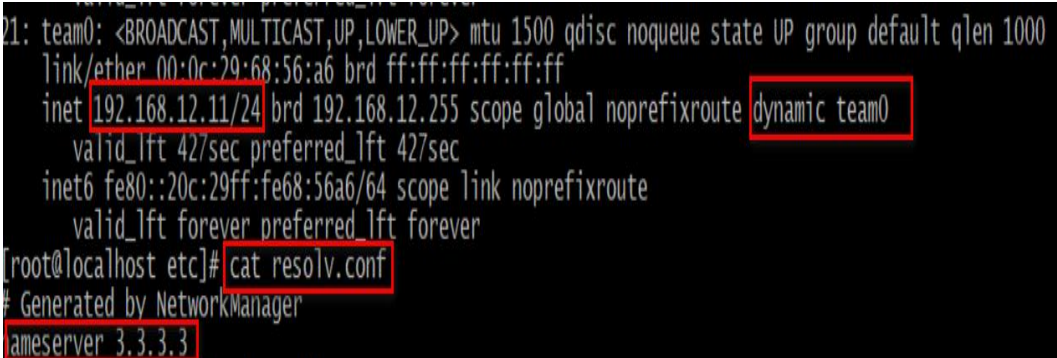
```
subnet 192.168.12.0 netmask 255.255.255.0 {  
  
    range 192.168.12.10 192.168.12.12;  
  
    option domain-name-servers 3.3.3.3;  
  
    # option domain-name "dmosk.local";  
  
    # option routers 192.168.0.1;  
  
    # option broadcast-address 192.168.0.255;  
  
    default-lease-time 600;  
  
    max-lease-time 7200;  
  
}
```

Добавляем правила firewall

firewall-cmd --permanent --add-service=dhcp

Меняем настройки для интерфейса team0 bootproto = 'dhcp'

Перезагружаем интерфейс и проверяем



```
21: team0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000  
    link/ether 00:0c:29:68:56:a6 brd ff:ff:ff:ff:ff:ff  
    inet 192.168.12.11/24 brd 192.168.12.255 scope global noprefixroute dynamic team0  
        valid_lft 427sec preferred_lft 427sec  
    inet6 fe80::20c:29ff:fe68:56a6/64 scope link noprefixroute  
        valid_lft forever preferred_lft forever  
[root@localhost etc]# cat resolv.conf  
# Generated by NetworkManager  
nameserver 3.3.3.3
```

Работает.

4. При помощи DHCP выдать серверу Server1 2 статических маршрута 4.4.4.4/32 и 5.5.5.0/24 с next hop интерфейса team0 на сервере server2

Для того что бы выдать маршруты клиент добавляем в DHCP строки /etc/dhcp/dhcpd.conf

```
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.example
#   see dhcpd.conf(5) man page
option classless-static-route code 121 = array of unsigned integer 8;

subnet 192.168.12.0 netmask 255.255.255.0 {
    range 192.168.12.11 192.168.12.12;
    option domain-name-servers 3.3.3.3;
    option classless-static-route 32, 4,4,4,4, 192,168,12,11,
                                   24, 5,5,5, 192,168,12,11;

    # option domain-name "dmosk.local";
    # option routers 192.168.0.1;
    # option broadcast-address 192.168.0.255;
    default-lease-time 600;
    max-lease-time 7200;
}
```

Перезагрузим интерфейс и проверяем, что маршруты были выданы клиенту

```
[root@localhost etc]# ip route
default via 192.168.2.2 dev ens33
2.2.2.2 via 192.168.12.12 dev team0 proto 188 metric 20
4.4.4.4 via 192.168.12.11 dev team0 proto dhcp metric 350
5.5.5.0/24 via 192.168.12.11 dev team0 proto dhcp metric 350
169.254.0.0/16 dev ens33 scope link metric 1002
169.254.0.0/16 dev dummy0 scope link metric 1005
192.168.2.0/24 dev ens33 proto kernel scope link src 192.168.2.128
192.168.12.0/24 dev team0 proto kernel scope link src 192.168.12.11 metric 350
[root@localhost etc]#
```

5. Настроить DNS-сервер для зоны example.com на сервере server3. Создать прямую и обратную зоны, а также несколько записей с разными RR. Убедиться, что только запросы на IP-адрес 3.3.3.3 будут обслуживаться этим DNS-сервером.

Настраиваем vi /etc/named.conf

На каком адресе будет слушать DNS

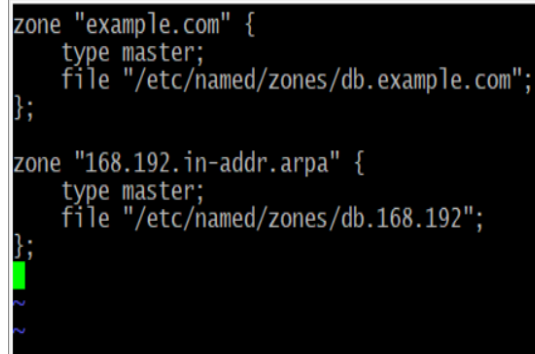
```
options {
```

```
    listen-on port 53 { 127.0.0.1;3.3.3.3};
```

добавляем файл зон

```
include "/etc/named/named.conf.local"
```

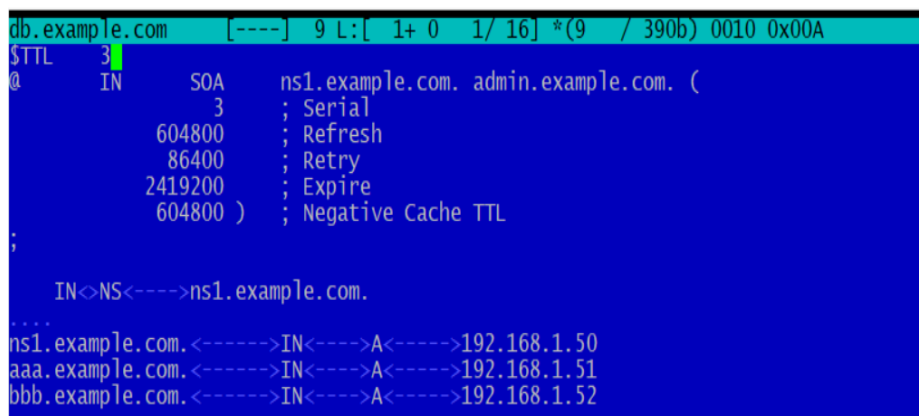
Создаём и добавляем файлы конфига зон "/etc/named/named.conf.local\



```
zone "example.com" {
    type master;
    file "/etc/named/zones/db.example.com";
};

zone "168.192.in-addr.arpa" {
    type master;
    file "/etc/named/zones/db.168.192";
};
```

Настраиваем файлы конфига зон прямой и обратный



```
db.example.com [----] 9 L: [ 1+ 0 1/ 16] *(9 / 390b) 0010 0x00A
$TTL 3
@ IN SOA ns1.example.com. admin.example.com. (
    3 ; Serial
    604800 ; Refresh
    86400 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;

IN NS ns1.example.com.
....
ns1.example.com. <-----> IN <-----> A <-----> 192.168.1.50
aaa.example.com. <-----> IN <-----> A <-----> 192.168.1.51
bbb.example.com. <-----> IN <-----> A <-----> 192.168.1.52
```

```
db.168.192 [----] 1 L:[ 1+ 7 8/ 16] *(330 / 450b) 0010 0x00A
STTL 3
@ IN SOA ns1.example.com. admin.example.com. (
        3 ; Serial
        604800 ; Refresh
        86400 ; Retry
        2419200 ; Expire
        604800 ) ; Negative Cache TTL
;
IN NS ns1.example.com.
.
.
.
50<---->IN<---->PTR<---->ns1.example.com.
51<---->IN<---->PTR<---->aaa.example.com.
52<---->IN<---->PTR<---->bbb.example.com.
```

Перезапускаем проверяем что работает с помощью dig

```
srv1 srv2 srv3 srv2
[root@server3 etc]# dig aaa.example.com @3.3.3.3 +short
192.168.1.51
[root@server3 etc]# dig bbb.example.com @3.3.3.3 +short
192.168.1.52
[root@server3 etc]# dig ns1.example.com @3.3.3.3 +short
192.168.1.50
[root@server3 etc]#
```

Обратную зону

```
srv1 srv2 srv3 srv2
[root@server3 etc]# dig -x 192.168.1.50 @3.3.3.3 +short
ns1.example.com.
[root@server3 etc]# dig -x 192.168.1.51 @3.3.3.3 +short
aaa.example.com.
[root@server3 etc]# dig -x 192.168.1.52 @3.3.3.3 +short
bbb.example.com.
[root@server3 etc]#
```

Пробуем с srv 2 (добавил пару маршрутов так как менялись настройки сети)

```
srv1 srv2 srv3 srv2
[root@server2 dhcp]# dig aaa.example.com @3.3.3.3 +short
192.168.1.51
[root@server2 dhcp]# dig bbb.example.com @3.3.3.3 +short
192.168.1.52
[root@server2 dhcp]# dig ns1.example.com @3.3.3.3 +short
192.168.1.50
[root@server2 dhcp]# dig -x 192.168.1.50 @3.3.3.3 +short
ns1.example.com.
[root@server2 dhcp]# dig -x 192.168.1.51 @3.3.3.3 +short
aaa.example.com.
[root@server2 dhcp]# dig -x 192.168.1.52 @3.3.3.3 +short
bbb.example.com.
[root@server2 dhcp]#
```


Что бы сервер принимал DNS запросы только на 3.3.3.3 делаем соответствующие настройки в /etc/named.conf, в listen-on port записываем нужные адрес.

```
options {
<----->listen-on port 53 { 3.3.3.3; };
<----->listen-on-v6 port 53 { ::1; };
<----->directory <----->"/var/named";
}
```

Проверяем через dig

Запрос на 3.3.3.3

```
[root@server3 ~]# dig -x192.168.1.50 @3.3.3.3
; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.5 <<>> -x192.168.1.50 @3.3.3.3
; global options: +cmd
; Got answer:
; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 41872
; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 4096
; QUESTION SECTION:
; 50.1.168.192.in-addr.arpa.      IN      PTR
; ANSWER SECTION:
; 50.1.168.192.in-addr.arpa. 3      IN      PTR      ns1.example.com.
; AUTHORITY SECTION:
; 1.168.192.in-addr.arpa. 3      IN      NS      ns1.example.com.
; ADDITIONAL SECTION:
; ns1.example.com.          3      IN      A      192.168.1.50
; Query time: 0 msec
```

Запрос на 127.0.0.1 соответственно не отрабатывает

```
[root@server3 ~]# dig -x192.168.1.50 @127.0.0.1
; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.5 <<>> -x192.168.1.50 @127.0.0.1
; global options: +cmd
; connection timed out; no servers could be reached
[root@server3 ~]# mcedit /etc/named.conf
```

6. Настроить фаерволл на серверах server2 и server3, чтобы разрешить только соответствующие запросы (DHCP/DNS).

Для корректной работы DNS с Firewalld добавляем правила

```
firewall-cmd --zone=public --add-service=dns --permanent
```

```
firewall-cmd --zone=public --add-service=dns
```

Для корректной работы DHCP с Firewalld добавляем правило

```
firewall-cmd --permanent --add-service=dhcp
```


7. * Настроить slave для DNS-сервера server3. Убедиться, что репликация записей происходит

Настройка slave:

Настраиваем etc/named.conf

```
options {
    listen-on port 53 { 127.0.0.1; 192.168.12.12; };
    //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; };
    allow-notify { 192.168.23.13; 3.3.3.3; };
}
```

Настраиваем зоны etc/named/named.conf.local указываем что зоны slave

```
named.conf.local [----] 42 L: [ 1+ 3 4/ 13] *(117 / 337b) 0010 0x00A
zone "example.com" {
    type slave;
    masters { 3.3.3.3; 192.168.23.13; };
    allow-notify { 3.3.3.3; 192.168.23.13; };
    file "/etc/named/zones/db.example.com";
};
zone "1.168.192.in-addr.arpa" {
    type slave;
    masters { 3.3.3.3; 192.168.23.13; };
    allow-notify { 3.3.3.3; 192.168.23.13; };
    file "/etc/named/zones/db.168.192";
};
```

Указываем type slave – означает что зона slave, masters – перечисляются мастер сервера,

Notify – сервера от которых можно принимать оповещение.

Дополнительно нужно создать целевые директории и назначить владельцем пользователя named.

Так же отключить SELinux, так как будут возникать ошибки доступа к файлам.

Дополнительные настройки со стороны мастер

```
options {
    listen-on port 53 { 3.3.3.3; 192.168.23.13; };
    //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; };
    allow-transfer { 192.168.12.12; };
}
```

Allow-query – не обязательно any разрешает запросы со всех хостов, можно указать отдельные хосты

Allow-transfer – указывает slave куда будет отправляется информация об изменении зоны.

Для файла зон

```
named.conf.local [----] 36 L:[ 1+ 8 9/ 13] *(20
zone "example.com" {
    type master;
    allow-transfer {192.168.12.12;};
    file "/etc/named/zones/db.example.com";
};

zone "1.168.192.in-addr.arpa" {
    type master;
    allow-transfer {192.168.12.12;};
    file "/etc/named/zones/db.168.192";
};
```

Аналогично Allow-transfer – указывает slave куда будет отправляется информация об изменении зоны.

В целом всё проверяем:

В файле RR на мастер добавляем A запись hhh.example.com и меняем serial

```
$TTL 120
@ IN SOA ns1.example.com. admin.example.com. (
    14 ; Serial
    10 ; Refresh
    100 ; Retry
    2419200 ; Expire
    604800 ) ; Negative Cache TTL
;

IN<NS<---->ns1.example.com.
ns1.example.com.<----->IN<----->A<----->192.168.1.50
aaa.example.com.<----->IN<----->A<----->192.168.1.51
bbb.example.com.<----->IN<----->A<----->192.168.1.52
ccc.example.com.<----->IN<----->A<----->192.168.1.53
ddd.example.com.<----->IN<----->A<----->192.168.1.54
eee.example.com.<----->IN<----->A<----->192.168.1.55
fff.example.com.<----->IN<----->A<----->192.168.1.56
ggg.example.com.<----->IN<----->A<----->192.168.1.57
rrr.example.com.<----->IN<----->A<----->192.168.1.58
hhh.example.com.<----->IN<----->A<----->192.168.1.59
```

Идём на slave и проверяет, что он резолвит добавленную запись.

Для наглядности на slave можно сравнить предыдущий размер и время файла с размером после обновления

```
total 8
-rw-r--r-- 1 named named 387 Jun 30 16:55 db.168.192
-rw-r--r-- 1 named named 554 Jun 30 16:53 db.example.com
-rwxrwxrwx. 1 named named 0 Jun 30 07:24 db-hrNmj9Ka
-rw-r--r-- 1 named named 0 Jun 30 15:22 db-JeIfRyKD
-rw-r--r-- 1 named named 0 Jun 30 15:25 db-xCRyHuOy
-rwxrwxrwx. 1 named named 0 Jun 30 07:24 db-XxMrzSn1
[root@server2 zones]# ll
total 8
-rw-r--r-- 1 named named 387 Jun 30 16:55 db.168.192
-rw-r--r-- 1 named named 597 Jun 30 16:58 db.example.com
-rwxrwxrwx. 1 named named 0 Jun 30 07:24 db-hrNmj9Ka
-rw-r--r-- 1 named named 0 Jun 30 15:22 db-JeIfRyKD
-rw-r--r-- 1 named named 0 Jun 30 15:25 db-xCRyHuOy
-rwxrwxrwx. 1 named named 0 Jun 30 07:24 db-XxMrzSn1
[root@server2 zones]#
```

Как видно размер файла на slave изменился после добавления записи

Можно резолвить со slave

```
-rw-r--r-- 1 named named 387 Jun 30 16:55 db.168.192
-rw-r--r-- 1 named named 597 Jun 30 16:58 db.example.com
-rwxrwxrwx. 1 named named 0 Jun 30 07:24 db-hrNmj9ka
-rw-r--r-- 1 named named 0 Jun 30 15:22 db-JelfRyKD
-rw-r--r-- 1 named named 0 Jun 30 15:25 db-xCRyHuQy
-rwxrwxrwx. 1 named named 0 Jun 30 07:24 db-XxMrzSn1
root@server2 zones]# dig hhh.example.com @192.168.12.12

<<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.5 <<>> hhh.example.com @192.168.12.12
; global options: +cmd
Got answer:
->>HEADER<<- opcode: QUERY, status: NOERROR, id: 958
; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2
; WARNING: recursion requested but not available

; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:: udp: 4096
; QUESTION SECTION:
hhh.example.com.                IN      A
; ANSWER SECTION:
hhh.example.com.                120     IN      A      192.168.1.59
; AUTHORITY SECTION:
example.com.                    120     IN      NS      ns1.example.com.
; ADDITIONAL SECTION:
ns1.example.com.                120     IN      A      192.168.1.50
; Query time: 0 msec
; SERVER: 192.168.12.12#53(192.168.12.12)
; WHEN: Wed Jun 30 17:04:22 EDT 2021
; MSG SIZE rcvd: 94
root@server2 zones]# dig hhh.example.com @192.168.12.12 +short
192.168.1.59
root@server2 zones]#
```

Работает.

