Отключаю пока что анонсирование подсетей

R1
R1(config)# router ospf
R1(config-router)# no network 1.1.1.1/32 area 0
R1(config-router)# no network 192.168.12.0/24 area 0

R2
R2(config-router)# no network 2.2.2.2/32 area 0
R2(config-router)# no network 192.168.12.0/24 area 0
R2(config-router)# no network 192.168.23.0/24 area 0

R3
R3(config-router)# no network 3.3.3.3/32 area 0
R3(config-router)# no network 192.168.23.0/24 area 0

Используем nmcli для создания и настройки nic teaming

Создаём bond интерфейс team0 в режиме active backup

```
[root@R1 ~]# nmcli con add type bond con-name team0 ifname team0 mode active-backup ip4 192.168.12.100/24
Connection 'team0' (d77baf09-3e6d-44fc-bfff-c730e0e6e2c7) successfully added.
[root@R1 ~]#
```

Добавляем интерфейсы ens34 и ens38 в качестве bond-slave для интерфейса team0

```
[root@R1 ~]# nmcli con add type bond-slave ifname ens34 master team0
Connection 'bond-slave-ens34' (ebe71629-84bf-4e4f-9ec2-8f4465de2b70) successfully added.
[root@R1 ~]# nmcli con add type bond-slave ifname ens38 master team0
Connection 'bond-slave-ens38' (7f2d1a7d-8c65-4390-9c19-f9d81380be89) successfully added.
[root@R1 ~]#
[root@R1 ~]# 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:fb:63:98 brd ff:ff:ff:ff:ff:ff
    inet 192.168.0.201/24 brd 192.168.0.255 scope global noprefixroute ens33
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fefb:6398/64 scope link
       valid_lft forever preferred_lft forever
3: ens34: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:fb:63:a2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.12.1/24 brd 192.168.12.255 scope global noprefixroute ens34
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fefb:63a2/64 scope link
       valid_lft forever preferred_lft forever
4: ens38: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 00:0c:29:fb:63:ac brd ff:ff:ff:ff:ff:ff
    inet 192.168.12.3/24 brd 192.168.12.255 scope global noprefixroute ens38
       valid_lft forever preferred_lft forever
    inet6 fe80::20c:29ff:fefb:63ac/64 scope link
       valid_lft forever preferred_lft forever
5: dummy0: <BROADCAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group default qlen 1000
    link/ether 2e:7e:95:d1:59:60 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::2c7e:95ff:fed1:5960/64 scope link
       valid_lft forever preferred_lft forever
6: team0: <NO-CARRIER,BROADCAST,MULTICAST,MASTER,UP> mtu 1500 qdisc noqueue state DOWN group default qlen 1000
    link/ether ce:5f:fb:7a:c6:f6 brd ff:ff:ff:ff:ff:ff
    inet 192.168.12.100/24 brd 192.168.12.255 scope global noprefixroute team0
       valid_lft forever preferred_lft forever
[root@R1 ~]#
```

Включаем bond-slave’ы

```
[root@R1 ~]# nmcli con up bond-slave-ens34
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/23)
[root@R1 ~]# nmcli con up bond-slave-ens38
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/24)
```

Включаем team0

```
[root@R1 ~]# nmcli connection up team0
Connection successfully activated (master waiting for slaves) (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/25)
```

Проверим статус bond интерфейса

```
[root@R1 ~]# cat /proc/net/bonding/team0
Ethernet Channel Bonding Driver: v3.7.1 (April 27, 2011)

Bonding Mode: fault-tolerance (active-backup)
Primary Slave: None
Currently Active Slave: ens34
MII Status: up
MII Polling Interval (ms): 100
Up Delay (ms): 0
Down Delay (ms): 0

Slave Interface: ens34
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 00:0c:29:fb:63:a2
Slave queue ID: 0

Slave Interface: ens38
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 00:0c:29:fb:63:ac
Slave queue ID: 0
```

Проведем аналогичные действия на R2

```
[root@R2 ~]# nmcli con add type bond con-name team0 ifname team0 mode active-backup ip4 192.168.12.10/24
Connection 'team0' (c5756cda-6816-48ad-8edf-c8f3bc87ce11) successfully added.
[root@R2 ~]# nmcli con add type bond-slave ifname ens34 master team0
Connection 'bond-slave-ens34' (959536ef-37c2-43a9-a5f5-11443c751045) successfully added.
[root@R2 ~]# nmcli con add type bond-slave ifname ens39 master team0
Connection 'bond-slave-ens39' (3d2e3822-e2f8-43b0-b6e3-317b2dc166b3) successfully added.
[root@R2 ~]# nmcli con up bond-slave-ens34
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/24)
[root@R2 ~]# nmcli con up bond-slave-ens39
Connection successfully activated (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/25)
[root@R2 ~]# nmcli connection up team0
Connection successfully activated (master waiting for slaves) (D-Bus active path: /org/freedesktop/NetworkManager/ActiveConnection/26)
[root@R2 ~]# cat /proc/net/bonding/team0
Ethernet Channel Bonding Driver: v3.7.1 (April 27, 2011)

Bonding Mode: fault-tolerance (active-backup)
Primary Slave: None
Currently Active Slave: ens34
MII Status: up
MII Polling Interval (ms): 100
Up Delay (ms): 0
Down Delay (ms): 0

Slave Interface: ens34
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 00:0c:29:5c:58:54
Slave queue ID: 0

Slave Interface: ens39
MII Status: up
Speed: 1000 Mbps
Duplex: full
Link Failure Count: 0
Permanent HW addr: 00:0c:29:5c:58:68
Slave queue ID: 0
```

На данный момент мы имеем на R1 интерфейс team0 с ip 192.168.12.100
и на R2 интерфейс team0 с ip 192.168.12.10

Проверим связность

```
[root@R1 ~]# ping 192.168.12.10\
>
PING 192.168.12.10 (192.168.12.10) 56(84) bytes of data.
64 bytes from 192.168.12.10: icmp_seq=1 ttl=64 time=0.231 ms
64 bytes from 192.168.12.10: icmp_seq=2 ttl=64 time=0.273 ms
64 bytes from 192.168.12.10: icmp_seq=3 ttl=64 time=0.247 ms
64 bytes from 192.168.12.10: icmp_seq=4 ttl=64 time=0.495 ms
^C
```

```
[root@R2 ~]# ping 192.168.12.100
PING 192.168.12.100 (192.168.12.100) 56(84) bytes of data.
64 bytes from 192.168.12.100: icmp_seq=1 ttl=64 time=0.301 ms
64 bytes from 192.168.12.100: icmp_seq=2 ttl=64 time=0.430 ms
64 bytes from 192.168.12.100: icmp_seq=3 ttl=64 time=0.271 ms
^C
```

Изменим интерфейс team0 на R1, что бы тот получал настройки по dhcp

```
nmcli con mod team0 ipv4.method auto
```

Проверим конфиг

```
[root@R1 network-scripts]# cat ifcfg-team0
BONDING_OPTS=mode=active-backup
TYPE=Bond
BONDING_MASTER=yes
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=dhcp
IPADDR=192.168.12.100
PREFIX=24
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=team0
UUID=d77baf09-3e6d-44fc-bfff-c730e0e6e2c7
DEVICE=team0
ONBOOT=yes
[root@R1 network-scripts]#
```

Установим на R2 dhcp сервер

yum install dhcp -y

Отредактируем конфиг файл
vim /etc/dhcp/dhcpd.conf

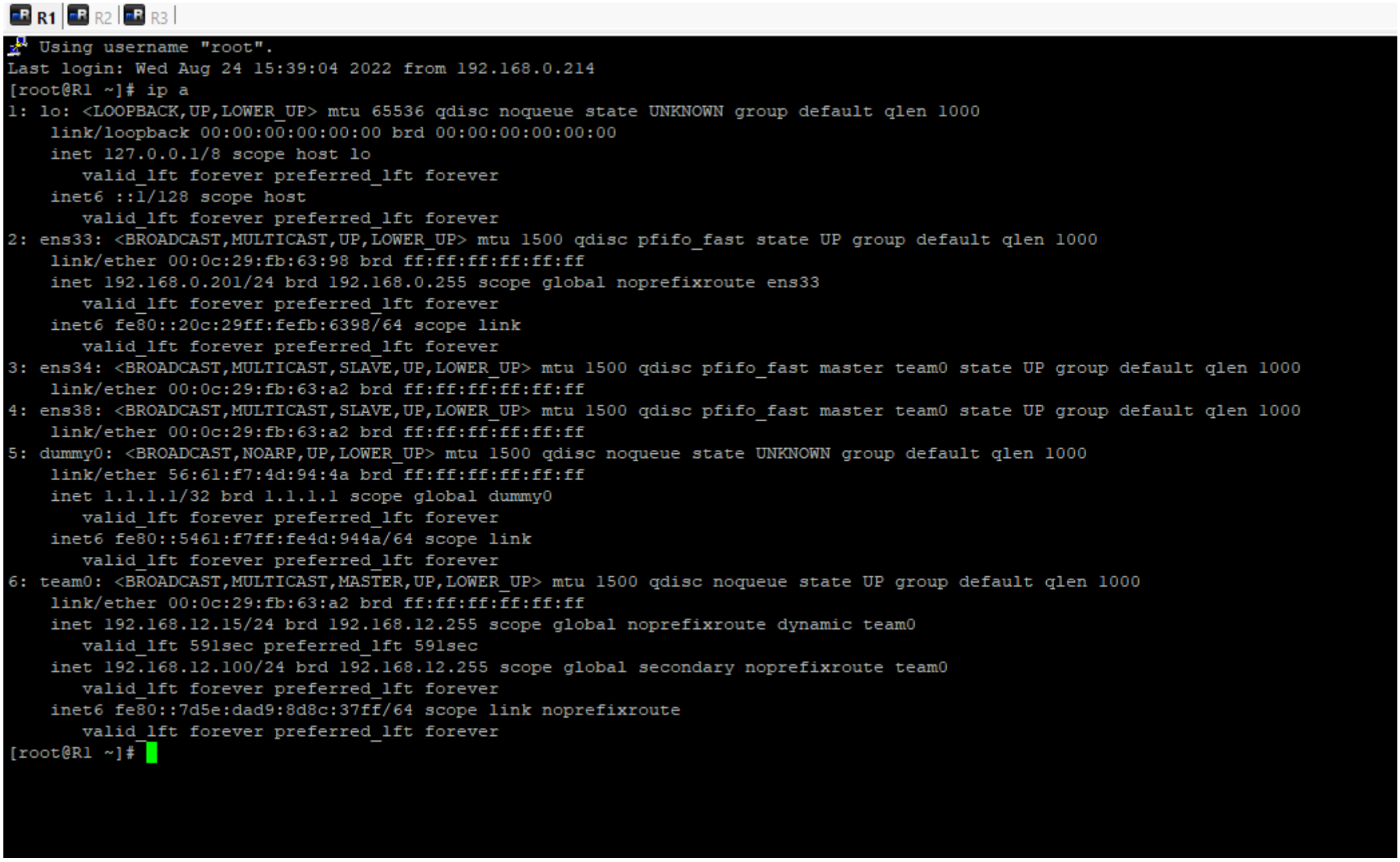
R1 R2 R3

```
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.example
#   see dhcpd.conf(5) man page
#
subnet 192.168.12.0 netmask 255.255.255.0 {
  authoritative;
  range 192.168.12.15 192.168.12.50;
  option domain-name-servers 3.3.3.3;
  option broadcast-address 192.168.12.255;
  default-lease-time 600;
  max-lease-time 7200;
}
~
~
~
```

Запустим службу, включим автозапуск

systemctl start dhcpd
systemctl enable dhcpd

Ребутаем R1, проверяем что ip адрес получен по dhcp



Адресс DNS 3.3.3.3 также получен успешно

```
[root@R1 ~]# cat /etc/resolv.conf
# Generated by NetworkManager
nameserver 192.168.0.1
nameserver 3.3.3.3
[root@R1 ~]#
```

Вернем ospf и проанонсируем маршруты

```
R1# conf t
R1(config)# router ospf
R1(config-router)# network 1.1.1.1/32 area 0
R1(config-router)# network 192.168.12.0/24 area 0
```

```
R2# conf t
R2(config)# router ospf
R2(config-router)# network 2.2.2.2/32 area 0
R2(config-router)# network 192.168.12.0/24 area 0
R2(config-router)# network 192.168.23.0/24 area 0
```

```
R3# conf t
R3(config)# router ospf
R3(config-router)# network 3.3.3.3/32 area 0
R3(config-router)# network 192.168.23.0/24 area 0
R3(config-router)# exit
```

Проверим связность

```
[root@R1 ~]# ping 3.3.3.3
PING 3.3.3.3 (3.3.3.3) 56(84) bytes of data.
64 bytes from 3.3.3.3: icmp_seq=1 ttl=63 time=1.25 ms
64 bytes from 3.3.3.3: icmp_seq=2 ttl=63 time=0.677 ms
64 bytes from 3.3.3.3: icmp_seq=3 ttl=63 time=0.568 ms
```

Отредактируем конфиг файл dhcp.
Включим опцию передачи бесклассовых маршрутов (rfc3442)
Прочитав rfc3442, попробуем передать маршрут 4.4.4.4/32, добавив строку

R1 R2 R3

```
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.example
#   see dhcpd.conf(5) man page
#
option rfc3442-classless-static-routes code 121 = array of integer 8;
subnet 192.168.12.0 netmask 255.255.255.0 {
  authoritative;
  range 192.168.12.15 192.168.12.50;
  option domain-name-servers 3.3.3.3;
  option broadcast-address 192.168.12.255;
  default-lease-time 600;
  max-lease-time 7200;
  option rfc3442-classless-static-routes 32, 4, 4, 4, 4, 192, 168, 12, 10;
}
```

делаем рестарт dhcp

```
systemctl restart dhcpd
```

Посмотрим маршруты на R1

```
[root@R1 ~]# ip route
default via 192.168.0.1 dev ens33 proto static metric 100
2.2.2.2 via 192.168.12.10 dev team0 proto 188 metric 20
3.3.3.3 via 192.168.12.10 dev team0 proto 188 metric 20
4.4.4.4 via 192.168.12.10 dev team0 proto dhcp metric 300
169.254.0.0/16 dev dummy0 scope link metric 1005
192.168.0.0/24 dev ens33 proto kernel scope link src 192.168.0.201 metric 100
192.168.12.0/24 dev team0 proto kernel scope link src 192.168.12.100 metric 300
192.168.12.0/24 dev team0 proto kernel scope link src 192.168.12.15 metric 300
192.168.23.0/24 via 192.168.12.10 dev team0 proto 188 metric 20
[root@R1 ~]#
```

Появился маршрут 4.4.4.4 полученный по dhcp

Отредактируем конфиг dhcp, добавив маршрут 5.5.5.5

```
vim /etc/dhcp/dhcpd.conf
```

```
#
# DHCP Server Configuration file.
#   see /usr/share/doc/dhcp*/dhcpd.conf.example
#   see dhcpd.conf(5) man page
#
option rfc3442-classless-static-routes code 121 = array of integer 8;
subnet 192.168.12.0 netmask 255.255.255.0 {
  authoritative;
  range 192.168.12.15 192.168.12.50;
  option domain-name-servers 3.3.3.3;
  option broadcast-address 192.168.12.255;
  default-lease-time 600;
  max-lease-time 7200;
  option rfc3442-classless-static-routes 32, 4, 4, 4, 4, 192, 168, 12, 10, 32, 5, 5, 5, 5, 192, 168, 12, 10;
}
~
~
```

Перезагрузим демон dhcp

systemctl restart dhcpd

Проверим маршруты на R1

R1 | R2 | R3

```
Using username "root".
Last login: Thu Aug 25 12:57:32 2022 from 192.168.0.214
[root@R1 ~]# ip route
default via 192.168.0.1 dev ens33 proto static metric 100
4.4.4.4 via 192.168.12.10 dev team0 proto dhcp metric 300
5.5.5.5 via 192.168.12.10 dev team0 proto dhcp metric 300
169.254.0.0/16 dev dummy0 scope link metric 1005
192.168.0.0/24 dev ens33 proto kernel scope link src 192.168.0.201 metric 100
192.168.12.0/24 dev team0 proto kernel scope link src 192.168.12.100 metric 300
192.168.12.0/24 dev team0 proto kernel scope link src 192.168.12.15 metric 300
[root@R1 ~]#
```

На R3 устанавливает bind

yum install bind -y

Редактируем конфиг dns сервера, прописываем адрес нашего днс сервера - 3.3.3.3

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

        /*
```

И добавляем путь к файлу, в котором опишем наши зоны.

```
zone "." IN {
        type hint;
        file "named.ca";
};

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

Открывает и заполняем файл, в котором будут наши зоны.

vim /etc/named/named.conf.local

Описываем зоны example.com и обратную зону

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

zone "23.168.192.in-addr.arpa" {
        type master;
        file "/etc/named/zones/db.23.168.192";
};
~
```

vim /etc/named/zones/db.example.com
Вписываем ресурсные записи для зоны example

```
$TTL 604800
@ IN SOA ns1.example.com. admin.example.com. (
        20210806
        604800
        86400
        2419200
        604800 )


        IN NS ns1.example.com.

ns1.example.com. IN A 192.168.23.2
test.example.com. IN A 192.168.23.50
abc.example.com. IN A 192.168.23.60
~
~
```

vim /etc/named/zones/db.23.168.192
Пишем ресурсные записи для обратной зоны

```
$TTL 604800
@ IN SOA example.com. admin.example.com. (
        20210806
        604800
        86400
        2419200
        604800 )
; name servers
        IN NS ns1.example.com.

; PTR Records
2 IN PTR ns1.example.com. ; 192.168.23.2
50 IN PTR test.example.com. ; 192.168.23.50
51 IN PTR abc.example.com. ; 192.168.23.51
~
~
~
~
```

Проверим правильность заполненных файлов

```
[root@R3 named]#
[root@R3 named]# named-checkconf /etc/named/named.conf.local
[root@R3 named]#
```

```
[root@R3 named]# named-checkzone example.com /etc/named/zones/db.example.com
zone example.com/IN: loaded serial 20210806
OK
[root@R3 named]#
```

```
[root@R3 named]# named-checkzone 23.168.192.in-addr.arpa /etc/named/zones/db.23.168.192
zone 23.168.192.in-addr.arpa/IN: loaded serial 20210806
OK
[root@R3 named]#
```

systemctl start named
systemctl enable named

Пробуем разрешить адрес abc.example.com на R1

```
[root@R1 ~]# dig abc.example.com @3.3.3.3

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9 <<>> abc.example.com @3.3.3.3
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: REFUSED, id: 14478
;; flags: qr rd; QUERY: 1, ANSWER: 0, AUTHORITY: 0, ADDITIONAL: 1
;; WARNING: recursion requested but not available

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;abc.example.com.               IN      A

;; Query time: 0 msec
;; SERVER: 3.3.3.3#53(3.3.3.3)
;; WHEN: Thu Aug 25 15:10:42 MSK 2022
;; MSG SIZE  rcvd: 44
```

Получаем status: REFUSED

Мы забыли вписать в конфиг dns сервера, кому разрешено присылать запросы. Это поле allow_query

vim /etc/named.conf

Впишем сразу одну большую подсеть 192.168.0.0/16

```
options {
        listen-on port 53 { 127.0.0.1; 3.3.3.3; };
        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     { localhost; 192.168/16; };

        /*
```

systemctl restart named

Проверяем, идём на R1

```
[root@R1 ~]# dig abc.example.com @3.3.3.3

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9 <<>> abc.example.com @3.3.3.3
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 46471
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;abc.example.com.               IN      A

;; ANSWER SECTION:
abc.example.com.        604800  IN      A       192.168.23.60

;; AUTHORITY SECTION:
example.com.            604800  IN      NS      ns1.example.com.

;; ADDITIONAL SECTION:
ns1.example.com.        604800  IN      A       192.168.23.2

;; Query time: 0 msec
;; SERVER: 3.3.3.3#53(3.3.3.3)
;; WHEN: Thu Aug 25 15:17:35 MSK 2022
;; MSG SIZE  rcvd: 94
```

Разрешение доменного имени abc.example.com проходит успешно.

Проверим что наш днс сервер не доступен по ip адресу физического сетевого интерфейса 192.168.23.2

```
[root@R1 ~]# dig abc.example.com @192.168.23.2

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9 <<>> abc.example.com @192.168.23.2
;; global options: +cmd
;; connection timed out; no servers could be reached
```

Получаем тайм аут.

Настроим firewall.

Включим для начала файрвол на R1

```
Using username "root".
Last login: Thu Aug 25 13:02:32 2022 from 192.168.0.214
[root@R1 ~]# firewall-cmd --list-services
FirewallD is not running
[root@R1 ~]# systemctl start firewalld
[root@R1 ~]# firewall-cmd --list-services
dhcpv6-client ssh
[root@R1 ~]#
```

На данный момент у нас разрешён только ssh и dhcpv6

Проверим получил ли наш интерфейс team0 настройки по dhcp. Обнаруживаем что настройки получены, но у нас 2 ip адреса на интерфейсе.

```
6: team0: <BROADCAST,MULTICAST,MASTER,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 00:0c:29:fb:63:a2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.12.15/24 brd 192.168.12.255 scope global noprefixroute dynamic team0
       valid_lft 340sec preferred_lft 340sec
    inet 192.168.12.100/24 brd 192.168.12.255 scope global secondary noprefixroute team0
       valid_lft forever preferred_lft forever
    inet6 fe80::7d5e:dad9:8d8c:37ff/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

vim /etc/sysconfig/network-scripts/ifcfg-team0

Удаляем строчки

IPADDR=192.168.12.100

PREFIX=24

```
BONDING_OPTS=mode=active-backup
TYPE=Bond
BONDING_MASTER=yes
PROXY_METHOD=none
BROWSER_ONLY=no
BOOTPROTO=dhcp
DEFROUTE=yes
IPV4_FAILURE_FATAL=no
IPV6INIT=yes
IPV6_AUTOCONF=yes
IPV6_DEFROUTE=yes
IPV6_FAILURE_FATAL=no
IPV6_ADDR_GEN_MODE=stable-privacy
NAME=team0
UUID=d77baf09-3e6d-44fc-bfff-c730e0e6e2c7
DEVICE=team0
ONBOOT=yes
~
~
~
```

Ребутаемся. Проверяем

```
6: team0: <BROADCAST,MULTICAST,MASTER,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 00:0c:29:fb:63:a2 brd ff:ff:ff:ff:ff:ff
    inet 192.168.12.15/24 brd 192.168.12.255 scope global noprefixroute dynamic team0
       valid_lft 592sec preferred_lft 592sec
    inet6 fe80::7d5e:dad9:8d8c:37ff/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Итак, dhcp работает по умолчанию с включенным файрволом.

Теперь нам надо разрешить ospf, чтобы установить соседство с R2, анонсировать и получить маршруты

```
[root@R1 services]# firewall-cmd --add-protocol=89
success
[root@R1 services]#
[root@R1 services]# vtysh

Hello, this is FRRouting (version 8.3).
Copyright 1996-2005 Kunihiro Ishiguro, et al.

R1# show ip ospf neighbor

Neighbor ID     Pri State           Up Time         Dead Time Address         Interface                        RXmtL RqstL DBsmL
192.168.0.202     1 Full/DR         14.173s           35.828s 192.168.12.10   team0:192.168.12.15                  0     0     0
```

После ребута у нас отключился файрволл. Включаем, добавляем в автозапуск, добавляем правила в файрвол.

```
[root@R1 ~]# systemctl start firewalld
[root@R1 ~]# systemctl enable firewalld
Created symlink from /etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service to /usr/lib/systemd/system/firewalld.service.
Created symlink from /etc/systemd/system/multi-user.target.wants/firewalld.service to /usr/lib/systemd/system/firewalld.service.
[root@R1 ~]# firewall-cmd --add-protocol=89 --permanent
success
[root@R1 ~]# firewall-cmd --add-service=dns --permanent
success
[root@R1 ~]#
```

Проделаем тоже самое на R2 и R3.

```
[root@R2 ~]# systemctl start firewalld
[root@R2 ~]# systemctl enable firewalld
Created symlink from /etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service to /usr/lib/systemd/system/firewalld.service.
Created symlink from /etc/systemd/system/multi-user.target.wants/firewalld.service to /usr/lib/systemd/system/firewalld.service.
[root@R2 ~]# firewall-cmd --add-protocol=89 --permanent
success
[root@R2 ~]# firewall-cmd --add-service=dns --permanent
success
[root@R2 ~]# firewall-cmd --add-service=dhcp --permanent
success
[root@R2 ~]#
```

```
Using username "root".
Last login: Thu Aug 25 12:57:36 2022 from 192.168.0.214
[root@R3 ~]# systemctl start firewalld
[root@R3 ~]# systemctl enable firewalld
Created symlink from /etc/systemd/system/dbus-org.fedoraproject.FirewallD1.service to /usr/lib/systemd/system/firewalld.service.
Created symlink from /etc/systemd/system/multi-user.target.wants/firewalld.service to /usr/lib/systemd/system/firewalld.service.
[root@R3 ~]# firewall-cmd --add-protocol=89 --permanent
success
[root@R3 ~]# firewall-cmd --add-service=dns --permanent
success
[root@R3 ~]# firewall-cmd --add-service=dhcp --permanent
success
[root@R3 ~]#
```

После настройки соседство не установилось, пробуем reboot всех машин.

```
R1# sh ip ospf neighbor

Neighbor ID     Pri State           Up Time         Dead Time Address         Interface                       RXmtL RqstL DBsmL
192.168.0.202     1 Full/DR         3m34s             30.506s 192.168.12.10   team0:192.168.12.15                 0     0     0
```

```
R2# sh ip ospf neighbor

Neighbor ID     Pri State           Up Time         Dead Time Address         Interface                       RXmtL RqstL DBsmL
192.168.0.203     1 Full/DR         4m18s             31.241s 192.168.23.2    ens35:192.168.23.1                  0     0     0
192.168.0.201     1 Full/Backup     4m17s             30.804s 192.168.12.15   team0:192.168.12.10                 0     0     0
```

```
R3# sh ip ospf neighbor

Neighbor ID     Pri State           Up Time         Dead Time Address         Interface                       RXmtL RqstL DBsmL
192.168.0.202     1 Full/Backup     6m26s             39.819s 192.168.23.1    ens34:192.168.23.2                  0     0     0
```

Соседство есть, маршруты получены, dhcp работает. Осталось проверить DNS

R2

```
[root@R2 ~]# dig abc.example.com @3.3.3.3

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9 <<>> abc.example.com @3.3.3.3
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 49311
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;abc.example.com.               IN      A

;; ANSWER SECTION:
abc.example.com.        604800  IN      A       192.168.23.60

;; AUTHORITY SECTION:
example.com.            604800  IN      NS      ns1.example.com.

;; ADDITIONAL SECTION:
ns1.example.com.        604800  IN      A       192.168.23.2

;; Query time: 0 msec
;; SERVER: 3.3.3.3#53(3.3.3.3)
;; WHEN: Fri Aug 26 13:40:00 MSK 2022
;; MSG SIZE  rcvd: 94
```

R1

```
[root@R1 ~]# firewall-cmd --list-services
dhcpv6-client dns ssh
[root@R1 ~]# dig abc.example.com @3.3.3.3




; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9 <<>> abc.example.com @3.3.3.3
;; global options: +cmd
;; connection timed out; no servers could be reached
```

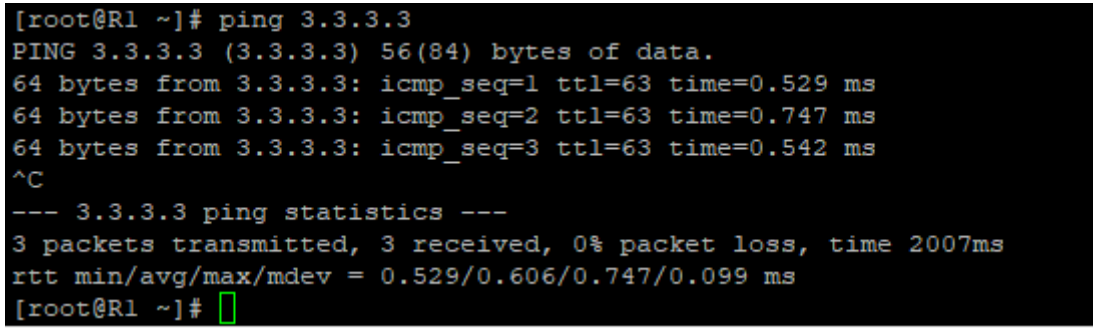
На R2 получается разрешить имя, а на R1 ошибка тайм аут.
Скорее всего файрволл настроен правильно. Смотрим tcpdump на R2 и ещё раз запускаем
dig abc.example.com @3.3.3.3

```
[root@R2 ~]# tcpdump -nni team0 udp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on team0, link-type EN10MB (Ethernet), capture size 262144 bytes
13:43:51.068738 IP 192.168.12.15.38689 > 3.3.3.3.53: 43851+ [1au] A? abc.example.com. (44)
13:43:56.069516 IP 192.168.12.15.38689 > 3.3.3.3.53: 43851+ [1au] A? abc.example.com. (44)
13:44:01.072138 IP 192.168.12.15.38689 > 3.3.3.3.53: 43851+ [1au] A? abc.example.com. (44)
```

```
[root@R2 ~]# tcpdump -nni ens35 udp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens35, link-type EN10MB (Ethernet), capture size 262144 bytes
^C
0 packets captured
0 packets received by filter
0 packets dropped by kernel
[root@R2 ~]#
```

Из интерфейса ens35 трафик не уходит. Значит на R2 где то отбрасываются пакеты

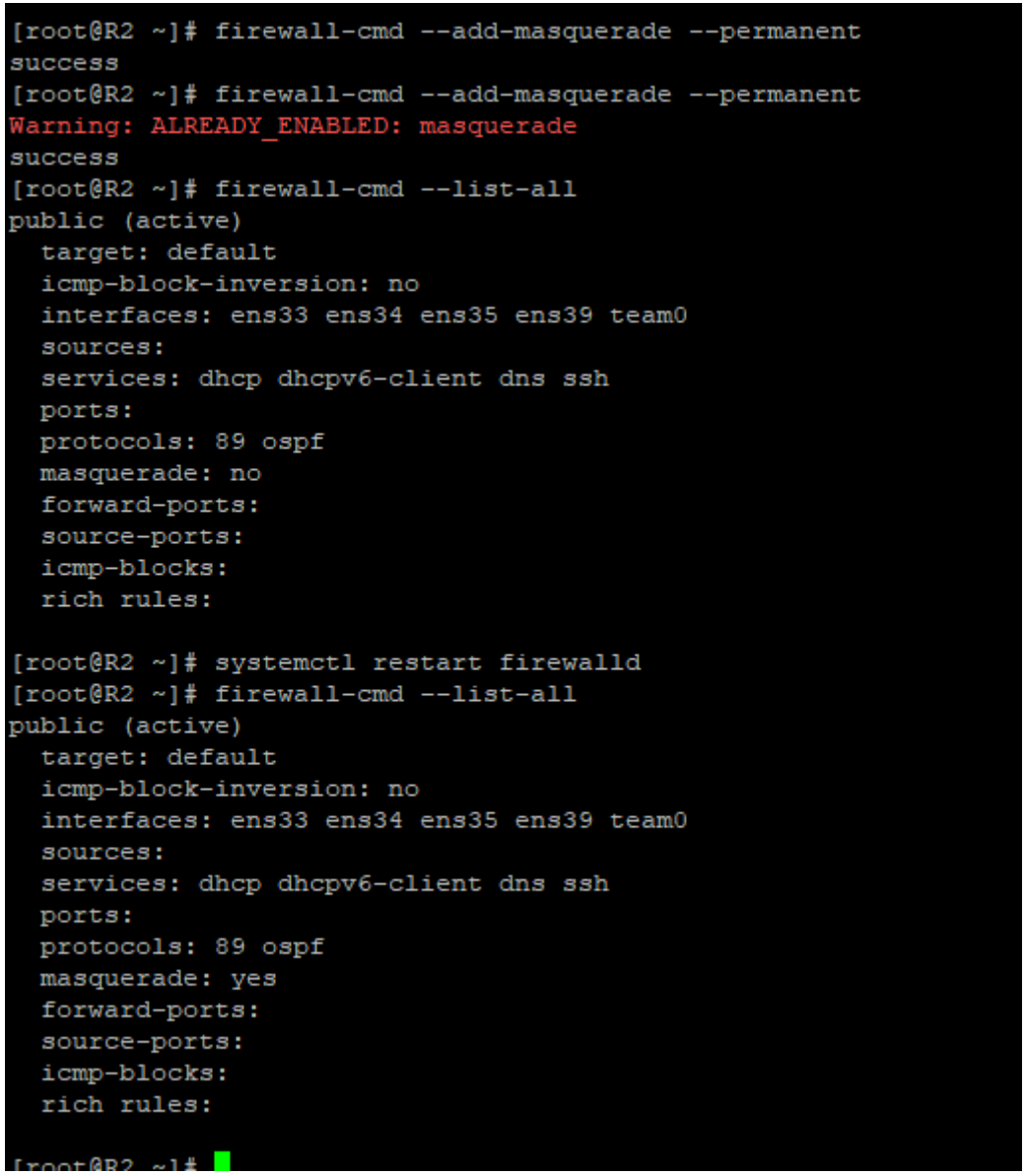
Причем пинг с R1 на R3 идёт



Попробуем опцию masquarade на R2.
Маскарад подменяет src ip на адрес этой машины. И пропускает пакет дальше.

```
firewall-cmd --add-masquerade --permanent
```

Делаем рестарт службы, чтобы перечитать правила.
Проверяем список действующих правил



Пробуем разрешить abc.example.com на R1

```
[root@R1 ~]# dig abc.example.com @3.3.3.3

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9 <<>> abc.example.com @3.3.3.3
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 19110
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;abc.example.com.               IN      A

;; ANSWER SECTION:
abc.example.com.        604800  IN      A       192.168.23.60

;; AUTHORITY SECTION:
example.com.            604800  IN      NS      ns1.example.com.

;; ADDITIONAL SECTION:
ns1.example.com.        604800  IN      A       192.168.23.2

;; Query time: 0 msec
;; SERVER: 3.3.3.3#53(3.3.3.3)
;; WHEN: Fri Aug 26 14:12:04 MSK 2022
;; MSG SIZE  rcvd: 94

[root@R1 ~]#
```

Успешно!

На R2 tcpdump выглядит таким образом. Видим что в пакете src ip подменяется на ip R2 и проходит дальше.

```
[root@R2 ~]# tcpdump -nni ens35 udp
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on ens35, link-type EN10MB (Ethernet), capture size 262144 bytes
14:12:53.313712 IP 192.168.23.1.60608 > 3.3.3.3.53: 20334+ [1au] A? abc.example.com. (44)
14:12:53.314113 IP 3.3.3.3.53 > 192.168.23.1.60608: 20334* 1/1/2 A 192.168.23.60 (94)
```