

Выполнил: студент группы 2345 Романенко Кирилл

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

<https://skrinhitam.wordpress.com/2019/10/30/how-to-configure-network-teaming-in-centos-rhel-7/>

SERVER1

Установил team
yum install teamd

Для настройки интерфейса использую enp0s8 и enp0s9, которые настраивал в ДЗ №2.

```
[root@server1 kdromanenko]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc
    link/loopback 00:00:00:00:00:00 brd 00:
    inet 127.0.0.1/8 scope host lo
        valid_lft forever preferred_lft fore
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft fore
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP>
    link/ether 08:00:27:17:88:c8 brd ff:ff:
    inet 192.168.1.81/24 brd 192.168.1.255
        valid_lft 24577sec preferred_lft 245
    inet6 fe80::c5f3:cc03:8705:d0ca/64 scop
        valid_lft forever preferred_lft fore
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP>
    link/ether 08:00:27:a5:22:b1 brd ff:ff:
    inet 192.168.12.1/24 brd 192.168.12.255
        valid_lft forever preferred_lft fore
    inet6 fe80::a00:27ff:fea5:22b1/64 scop
        valid_lft forever preferred_lft fore
4: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP>
    link/ether 08:00:27:8f:90:b7 brd ff:ff:
    inet6 fe80::a97d:dba7:6360:82d9/64 scop
        valid_lft forever preferred_lft fore
[root@server1 kdromanenko]#
```

Изменил настройки enp0s8 и enp0s9. Чтобы интерфейсы были up, но без ip

vim /etc/sysconfig/network-scripts/ifcfg-enp0s8

```
DEVICE=enp0s8
DEVICETYPE=Teamport
ONBOOT=yes
TEAM_MASTER=team0
NM_CONTROLLED=no
TEAM_PORT_CONFIG='{ "prio": 100 }
```

vim /etc/sysconfig/network-scripts/ifcfg-enp0s9

```
DEVICE=enp0s9
DEVICETYPE=Teamport
```

```
ONBOOT=yes
TEAM_MASTER=team0
NM_CONTROLLED=no
TEAM_PORT_CONFIG='{"prio": 100}'
```

Создал и настроил новый интерфейс: team0
vim /etc/sysconfig/network-scripts/ifcfg-team0

```
DEVICE=team0
DEVICETYPE=Team
ONBOOT=yes
BOOTPROTO=None
NM_CONTROLLED=no
IPADDR=192.168.12.1
PREFIX=24
TEAM_CONFIG='{"runner": {"name": "activebackup"}, "link_watch": {"name": "ethtool"}}'
```

Отключил интерфейсы enp0s8 и enp0s9
ip link set enp0s8 down
ip link set enp0s9 down

Поднял team0
ifup team0

Проверил
ip a

```
5: team0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 08:00:27:a5:22:b1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.12.1/24 brd 192.168.12.255 scope global team0
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fea5:22b1/64 scope link
        valid_lft forever preferred_lft forever
```

teamdctl team0 state

```
[root@server1 kdromanenko]# teamdctl team0 state
setup:
  runner: activebackup
ports:
  enp0s8
    link watches:
      link summary: up
      instance[link_watch_0]:
        name: ethtool
        link: up
        down count: 0
  enp0s9
    link watches:
      link summary: up
      instance[link_watch_0]:
        name: ethtool
        link: up
        down count: 0
runner:
  active port: enp0s8
```

SERVER2

Установил team
yum install teamd

Для настройки интерфейса использую enp0s8 и enp0s9, которые настраивал в ДЗ №2.

```
[root@server2 ~]# ip a
1: lo: <LOOPBACK,UP,LOWER_UP>
    link/loopback 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host
        valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
        valid_lft forever preferred_lft forever
2: enp0s3: <BROADCAST,MULTICAST,UP,LOWER_UP>
    link/ether 08:00:27:2f:cb:00
    inet 192.168.1.34/24 brd 192.168.1.255 scope global
        valid_lft 22579sec preferred_lft forever
    inet6 fe80::a00:27ff:fe2f:cb00/64 scope link
        valid_lft forever preferred_lft forever
3: enp0s8: <BROADCAST,MULTICAST,UP,LOWER_UP>
    link/ether 08:00:27:50:ef:00
    inet 192.168.12.2/24 brd 192.168.12.255 scope global
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe50:ef00/64 scope link
        valid_lft forever preferred_lft forever
4: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP>
    link/ether 08:00:27:04:93:00
    inet 192.168.23.2/24 brd 192.168.23.255 scope global
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe04:9300/64 scope link
        valid_lft forever preferred_lft forever
```

Создал и настроил новый интерфейс: team0
vim /etc/sysconfig/network-scripts/ifcfg-team0

```
DEVICE=team0
DEVICETYPE=Team
ONBOOT=yes
BOOTPROTO=none
NM_CONTROLLED=no
IPADDR=192.168.12.2
PREFIX=24
TEAM_CONFIG='{"runner": {"name": "activebackup"}, "link_watch": {"name": "ethtool"}}'
```

Изменил настройки enp0s8 и enp0s9. Чтобы интерфейсы были up, но без ip

vim /etc/sysconfig/network-scripts/ifcfg-enp0s8

```
DEVICE=enp0s8
DEVICETYPE=Teamport
ONBOOT=yes
TEAM_MASTER=team0
NM_CONTROLLED=no
TEAM_PORT_CONFIG='{"prio": 100}'
```

```
vim /etc/sysconfig/network-scripts/ifcfg-enp0s9
```

```
DEVICE=enp0s9
DEVICETYPE=Teamport
ONBOOT=yes
TEAM_MASTER=team0
NM_CONTROLLED=no
TEAM_PORT_CONFIG={'prio': 100}'
```

Отключил интерфейсы enp0s8 и enp0s9

```
ip link set enp0s8 down
```

```
ip link set enp0s9 down
```

Поднял team0

```
ifup team0
```

Проверил

```
ip a
```

```
5: team0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 08:00:27:50:ef:fa brd ff:ff:ff:ff:ff:ff
    inet 192.168.12.2/24 brd 192.168.12.255 scope global team0
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe50:effa/64 scope link
        valid_lft forever preferred_lft forever
```

```
teamdctl team0 state
```

```
setup:
  runner: activebackup
ports:
  enp0s8
    link watches:
      link summary: up
      instance[link_watch_0]:
        name: ethtool
        link: up
        down count: 0
  enp0s9
    link watches:
      link summary: up
      instance[link_watch_0]:
        name: ethtool
        link: up
        down count: 0
runner:
  active port: enp0s8
```

SERVER 1 и SERVER 2

Проверил связность

```
[root@server1 kdromanenko]# ping 192.168.12.2
PING 192.168.12.2 (192.168.12.2) 56(84) bytes of data.
64 bytes from 192.168.12.2: icmp_seq=1 ttl=64 time=0.759 ms
64 bytes from 192.168.12.2: icmp_seq=2 ttl=64 time=0.997 ms
^C
--- 192.168.12.2 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1000ms
rtt min/avg/max/mdev = 0.759/0.878/0.997/0.119 ms
```

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

Поменял настройку интерфейса

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

ДО	ПОСЛЕ
DEVICE=team0 DEVICETYPE=Team ONBOOT=yes BOOTPROTO=none NM_CONTROLLED=no IPADDR=192.168.12.2 PREFIX=24 TEAM_CONFIG='{"runner": {"name": "activebackup"}, "link_watch": {"name": "ethtool"}}'	DEVICE=team0 DEVICETYPE=Team ONBOOT=yes BOOTPROTO=static NM_CONTROLLED=no IPADDR=192.168.12.2 PREFIX=24 TEAM_CONFIG='{"runner": {"name": "activebackup"}, "link_watch": {"name": "ethtool"}}'

Перезагрузил интерфейс team0

`ifdown team0`

`ifup team0`

Проверил понятие интерфейса и связность с SERVER 1

`ip a`

```
6: team0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 08:00:27:50:ef:fa brd ff:ff:ff:ff:ff:ff
    inet 192.168.12.2/24 brd 192.168.12.255 scope global team0
        valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe50:effa/64 scope link
        valid_lft forever preferred_lft forever
```

`ping 192.168.12.1`

```
PING 192.168.12.1 (192.168.12.1) 56(84) bytes of data.
64 bytes from 192.168.12.1: icmp_seq=1 ttl=64 time=0.833 ms
64 bytes from 192.168.12.1: icmp_seq=2 ttl=64 time=1.09 ms
^C
--- 192.168.12.1 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 100lms
rtt min/avg/max/mdev = 0.833/0.962/1.091/0.129 ms
```

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.

SERVER 2

Установил dhcp

`yum install dhcp`

Скопировал пример настройки файла в /etc/dhcp/dhcpd.conf

`cp /usr/share/doc/dhcp-4.2.5/dhcpd.conf.example /etc/dhcp/dhcpd.conf`

Закомментировал все строчки конфига, чтобы потом включить только нужные опции

`sed s/^#/ /etc/dhcp/dhcpd.conf | tee /etc/dhcp/dhcpd.conf`

Раскомментировал файл dhcpd.conf

vim /etc/dhcp/dhcpd.conf

```
## A slightly different configuration for an internal subnet.
subnet 192.168.12.0 netmask 255.255.255.0 {
    range 192.168.12.100 192.168.12.199;
    option domain-name-servers 3.3.3.3;
    # option domain-name "internal.example.org";
    option routers 192.168.12.1;
    option broadcast-address 192.168.12.255;
    default-lease-time 600;
    max-lease-time 7200;
}
```

Включил dhcpd при загрузке системы, а также запустил службу
systemctl enable dhcpd
systemctl start dhcpd
systemctl status dhcpd

```
● dhcpd.service - DHCPv4 Server Daemon
   Loaded: loaded (/usr/lib/systemd/system/dhcpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Вт 2022-08-25 15:59:14 MSK; 10s ago
     Docs: man:dhcpd(8)
           man:dhcpd.conf(5)
  Main PID: 2438 (dhcpd)
   Status: "Dispatching packets..."
    CGroup: /system.slice/dhcpd.service
            └─2438 /usr/sbin/dhcpd -f -cf /etc/dhcp/dhcpd.conf -user dhcpd -group dhcpd --no-pid
```

SERVER 1

Поменял настройку интерфейса

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

ДО	ПОСЛЕ
DEVICE=team0 DEVICETYPE=Team ONBOOT=yes <u>BOOTPROTO=none</u> NM_CONTROLLED=no IPADDR=192.168.12.2 PREFIX=24 TEAM_CONFIG='{"runner": {"name": "activebackup"}, "link_watch": {"name": "ethtool"}}'	DEVICE=team0 DEVICETYPE=Team ONBOOT=yes BOOTPROTO=dhcp NM_CONTROLLED=no TEAM_CONFIG='{"runner": {"name": "activebackup"}, "link_watch": {"name": "ethtool"}}'

Перезагрузил интерфейс team0

ifdown team0

ifup team0

Проверил поднятие интерфейса и выдачу ip по dhcp

ip a

```
8: team0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 08:00:27:a5:22:b1 brd ff:ff:ff:ff:ff:ff
    inet 192.168.12.100/24 brd 192.168.12.255 scope global dynamic team0
        valid_lft 585sec preferred_lft 585sec
    inet6 fe80::a00:27ff:fea5:22b1/64 scope link
        valid_lft forever preferred_lft forever
```

Вывод: Выдан ipv4 на 585 sec

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

<https://lyalyuev.info/2016/12/06/how-to-push-routes-from-isc-dhcp-server/>

SERVER 2

Настроил DHCP

vim /etc/dhcp/dhcpd.conf

Ввёл конфигурацию в основной файл таким образом

```
option classless-routes code 121 = array of unsigned integer 8;
option classless-routes 32, 4,4,4,4, 192,168,12,2,
                        32, 5,5,5,5, 192,168,12,2;
option classless-routes-win code 249 = array of unsigned integer 8;
option classless-routes-win 32, 4,4,4,4, 192,168,12,2,
                        32, 5,5,5,5, 192,168,12,2;
```

```
#
subnet 192.168.12.0 netmask 255.255.255.0 {
    range 192.168.12.100 192.168.12.199;
    option domain-name-servers 3.3.3.3;
#   option domain-name "internal.example.org";
    option routers 192.168.12.1;
    option broadcast-address 192.168.12.255;
    default-lease-time 600;
    max-lease-time 7200;
}
#
option classless-routes code 121 = array of unsigned integer 8;
option classless-routes 32, 4,4,4,4, 192,168,12,2,
                        32, 5,5,5,5, 192,168,12,2;
option classless-routes-win code 249 = array of unsigned integer 8;
option classless-routes-win 32, 4,4,4,4, 192,168,12,2,
                        32, 5,5,5,5, 192,168,12,2;
#
## Hosts which require special configuration options can be listed in
```

Перезагрузил сервис dhcpd и проверил статус

systemctl restart dhcpd

systemctl status dhcpd


```
[root@server2 ~]# systemctl status dhcpd
● dhcpd.service - DHCPv4 Server Daemon
   Loaded: loaded (/usr/lib/systemd/system/dhcpd.service; enabled; vendor preset: disabled)
   Active: active (running) since Ут 2022-08-25 18:58:34 MSK; 2s ago
     Docs: man:dhcpd(8)
           man:dhcpd.conf(5)
   Main PID: 2768 (dhcpd)
   Status: "Dispatching packets..."
   CGroup: /system.slice/dhcpd.service
           └─2768 /usr/sbin/dhcpd -f -cf /etc/dhcp/dhcpd.conf -user dhcpd -group dhcpd --no-pid

авг 25 18:58:34 server2 dhcpd[2768]:
авг 25 18:58:34 server2 dhcpd[2768]:
авг 25 18:58:34 server2 dhcpd[2768]: No subnet declaration for enp0s3 (192.168.1.34).
авг 25 18:58:34 server2 dhcpd[2768]: ** Ignoring requests on enp0s3. If this is not what
авг 25 18:58:34 server2 dhcpd[2768]: you want, please write a subnet declaration
авг 25 18:58:34 server2 dhcpd[2768]: in your dhcpd.conf file for the network segment
авг 25 18:58:34 server2 dhcpd[2768]: to which interface enp0s3 is attached. **
авг 25 18:58:34 server2 dhcpd[2768]:
авг 25 18:58:34 server2 dhcpd[2768]: Sending on Socket/fallback/fallback-net
авг 25 18:58:34 server2 systemd[1]: Started DHCPv4 Server Daemon.
```

DHCP настроен и активирован

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.

SERVER 3

Установил необходимые пакеты
yum install bind bind-utils

Открыл файл и внес правки

vim /etc/named.conf

Закомментировал строку

include "/etc/named.rfc1912.zones";

Добавил строку

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

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

Создал зоны для домена example.com

vim /etc/named/named.conf.local

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

Далее в этом файле создал PTR-зону

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



```

zone "example.com" {
type master;
file "/etc/named/zones/db.example.com"; #файл конфига зоны
};

zone "168.192.in-addr.arpa" {
type master;
file "/etc/named/zones/db.168.192"; #файл конфига обратной зоны для 192.168.1.0/24
};

```

Расширил зону до 192.168.0.0, т.к. сервер локальный

Создал файл зон внутри /etc/named/zones

```

chmod 777 /etc/named
mkdir /etc/named/zones

```

Дополнил файл зон

vim /etc/named/zones/db.example.com

```

$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 192.168.1.220
ns1.example.com. IN A 192.168.1.220
text.example.com. IN A 192.168.1.221
img.example.com. IN A 192.168.1.222
static.example.com. IN A 192.168.1.223

```

```

$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      192.168.1.220
ns1.example.com.      IN      A      192.168.1.220
text.example.com.      IN      A      192.168.1.221
img.example.com.      IN      A      192.168.1.222
static.example.com.      IN      A      192.168.1.223

```

Дополнил файл обратной зоны

vim /etc/named/zones/db.168.192

```

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

```

```
604800 )
IN NS ns1.example.com.
220.1 IN PTR ns1.example.com.
221.1 IN PTR text.example.com.
222.1 IN PTR img.example.com.
223.1 IN PTR static.example.com.
```

```
$TTL 604800
@      IN      SOA      example.com.  admin.example.com. (
        20210806
        604800
        86400
        2419200
        604800 )
      IN      NS       ns1.example.com.
220.1  IN      PTR      ns1.example.com.
221.1  IN      PTR      text.example.com.
222.1  IN      PTR      img.example.com.
223.1  IN      PTR      static.example.com.
```

Проверил созданные файлы named-checkconf и named-checkzone
named-checkconf /etc/named/named.conf.local

named-checkzone example.com /etc/named/zones/db.example.com

ВЫВОД:

zone example.com/IN: loaded serial 20210806

OK

named-checkzone 168.192.in-addr.arpa /etc/named/zones/db.168.192

zone 168.192.in-addr.arpa/IN: loaded serial 20210806

OK

Включаю автозапуск

systemctl enable named

systemctl start named

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

На обоих серверах работаю через iptables

ss -tunap

Открытые порты DHCP – udp 68, DNS – tcp/udp 53

iptables -A INPUT -p udp --dport 53 -j ACCEPT

iptables -A INPUT -p tcp --dport 53 -j ACCEPT

iptables -A OUTPUT -p udp --sport 53 -j ACCEPT

iptables -A OUTPUT -p tcp --sport 53 -j ACCEPT

iptables -A INPUT -p udp --dport 68 -j ACCEPT

iptables -A OUTPUT -p udp --dport 68 -j ACCEPT