Выполнил Мешечкин Д. Инфобез-2345

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

1) Устанавливаются на оба сервера R1 и R2 #yum install teamd. На обоих серверах будут использоваться интерфейсы enp0s9 и enp0s10. Интерфейсы enp0s9 использовались в ДЗ к вебинару №2 как интерфейсы сети 192.168.12.0/24 для создания сети между серверами R1 и R2, интерфейсы enp0s10 - пустые и созданы из VB.
2) Создаю логические интерфейсы на R1 и R2.
   #touch ifcfg-team0
   далее заполнения файла конфигурации интерфейса
   DEVICE=nm-team
   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=c794ce57-2879-4426-9632-50cf05f8d5b5
   ONBOOT=yes
   IPADDR=192.168.12.1
   NETMASK=255.255.255.0
   Для UUID использовал какой-то рандомный генератор из сети.
   Далее прописываю интерфейсы enp0s9 enp0s10 в team0
   #touch ifcfg-team-slave-enp0s9
   далее заполняется файл конфигурации
   NAME=team-slave-enp0s9
   UUID=9b5d1511-43ee-4184-b20d-540c2820bb6a
   DEVICE=ens37
   ONBOOT=yes
   TEAM_MASTER=c794ce57-2879-4426-9632-50cf05f8d5b5
   DEVICETYPE=TeamPort
   UUID использовались из генератора UUID и соответственно отнесены все к R1 и R2, и enp0s9 и enp0s10. Так же из файлов конфигурации интерфейсов были удалены строчки IPADDR. Перезагрузку переживают. IPадреса переназначены согласно методичке 192.168.12.0/24. Продолжают переживать все ребуты dummy0 интерфейсы.

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

Статический IP адрес прописан в прошлом задании, выдается.

```
4: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast master nm-team state UP group default qlen 1000
    link/ether 08:00:27:23:a0:0e brd ff:ff:ff:ff:ff:ff
5: enp0s10: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast master nm-team state UP group default qlen 1000
    link/ether 08:00:27:23:a0:0e brd ff:ff:ff:ff:ff:ff
6: dummy0: <BROADCAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group default qlen 1000
    link/ether 96:06:45:0e:6d:44 brd ff:ff:ff:ff:ff:ff
    inet 2.2.2.2/32 brd 2.2.2.2 scope global dummy0
       valid_lft forever preferred_lft forever
    inet6 fe80::9406:45ff:fe0e:6d44/64 scope link
       valid_lft forever preferred_lft forever
7: nm-team: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 08:00:27:23:a0:0e brd ff:ff:ff:ff:ff:ff
    inet 192.168.12.2/24 brd 192.168.12.255 scope global noprefixroute nm-team
       valid_lft forever preferred_lft forever
    inet6 fe80::a00:27ff:fe23:a00e/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

Задание 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.

На сервере R2 устанавливается пакет **#yum install dhcp**

Копирую настройки с перезаписью **# cp /usr/share/doc/dhcp-4.2.5/dhcpd.conf.example /etc/dhcp/dhcpd.conf**

Закомментирую все строки конфига sed **s/^/#/ /etc/dhcp/dhcpd.conf | tee /etc/dhcp/dhcpd.conf**

Далее настройка dhcp сервера **/etc/dhcp/dhcpd.conf**

subnet 192.168.12.0 netmask 255.255.12.0 {
range 192.168.12.100 192.168.12.199;
option domain-name-servers 3.3.3.3;
option routers 192.168.12.1;
option broadcast-address 192.168.12.255;
default-lease-time 600;
max-lease-time 7200;
}

Необходимо включить службу DHCP и включить её запуск при старте сервера.

systemctl enable dhcpd
systemctl start dhcpd
systemctl status dhcpd

```
4: enp0s9: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast master nm-team state UP group default qlen 1000
    link/ether 08:00:27:95:8b:cb brd ff:ff:ff:ff:ff:ff
5: enp0s10: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast master nm-team state UP group default qlen 1000
    link/ether 08:00:27:95:8b:cb brd ff:ff:ff:ff:ff:ff
6: dummy0: <BROADCAST,NOARP,UP,LOWER_UP> mtu 1500 qdisc noqueue state UNKNOWN group default qlen 1000
    link/ether ae:b9:36:2b:db:c2 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::acb9:36ff:fe2b:dbc2/64 scope link
       valid_lft forever preferred_lft forever
7: nm-team: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc noqueue state UP group default qlen 1000
    link/ether 08:00:27:95:8b:cb brd ff:ff:ff:ff:ff:ff
    inet 192.168.12.101/24 brd 192.168.12.255 scope global noprefixroute dynamic nm-team
       valid_lft 529sec preferred_lft 529sec
    inet6 fe80::a00:27ff:fe95:8bcb/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
```

В итоге team0 интерфейс получает IP адресс с помощью DHCP в интервале 100-199.

Так же можно проверить распределение трафика по интерфейсам enp0s9 enp0s10, стоит roundrobin, где пакеты по очереди отсылаются по интерфейсам.

```
[root@server1 ~]# teamdctl nm-team state
setup:
  runner: roundrobin
ports:
  enp0s10
    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
```

Задание 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 выполнения задания необходимо:

На сервере R2:

touch /etc/sysconfig/network-scripts/route-team0
4.4.4.4/32 via 192.168.12.2
5.5.5.5/32 via 192.168.12.2
cd /etc/dhcp/dhcpd.conf
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;

В итоге прописывается маршрут до сетей 4.4.4.4/32 через интерфейс 192.168.12.2 и 5.5.5.5/32 через интерфейс 192.168.12.2. Проверяю на R1

```
[root@server1 ~]# traceroute 4.4.4.4
traceroute to 4.4.4.4 (4.4.4.4), 30 hops max, 60 byte packets
 1  192.168.12.2 (192.168.12.2)  0.181 ms  0.127 ms  0.081 ms
 2  192.168.12.2 (192.168.12.2)  3006.863 ms !H  3006.671 ms !H  3006.615 ms !H
[root@server1 ~]# traceroute 5.5.5.5
traceroute to 5.5.5.5 (5.5.5.5), 30 hops max, 60 byte packets
 1  192.168.12.2 (192.168.12.2)  0.307 ms  0.278 ms  0.266 ms
 2  192.168.12.2 (192.168.12.2)  3005.978 ms !H  3005.911 ms !H  3005.886 ms !H
[root@server1 ~]#
```

Пакеты идут через 192.168.12.2 но не доходят. А куда им идти, если нет этих IP в сети. Пакеты не уходят за пределы "серверной сети".

Задание 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.

Настройка BIND:

yum install bind

далее в файле **/etc/named.conf** комментируется строка и и добавляется новая строка с локальными зонами

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

Далее в файле **/etc/named/named.conf.local** создаем зоны для домена example.com

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

Далее в этом же файле создается PTR-зона.

```
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
};
```

Сервер локальный и зона расширена до 192.168.0.0

Далее создается файл зон внутри **/etc/named/zones**

chmod 777 /etc/named

mkdir /etc/named/zones

и дополняю файл зон **/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
```

Далее настройка файла обратной зоны **/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.
```

Далее проверка созданных файлов **named-checkconf** и **named-checkzone**

named-checkconf /etc/named/named.conf.local

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

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

```
[root@server3 etc]# named-checkconf /etc/named/named.conf.local
[root@server3 etc]# named-checkzone example.com /etc/named/zones/db.example.com
zone example.com/IN: loaded serial 20210806
OK
[root@server3 etc]# named-checkzone 168.192.in-addr.arpa /etc/named/zones/db.168.192
zone 168.192.in-addr.arpa/IN: loaded serial 20210806
OK
```

Проверка успешна, включаем автозапуск при старте и запускаем рантайм сервис
systemctl enable named
systemctl start named

```
[root@server3 etc]# systemctl start named
[root@server3 etc]# systemctl enable named
Created symlink from /etc/systemd/system/multi-user.target.wants/named.service to /usr/lib/systemd/system/named.service.
[root@server3 etc]# systemctl status named
● named.service - Berkeley Internet Name Domain (DNS)
   Loaded: loaded (/usr/lib/systemd/system/named.service; enabled; vendor preset: disabled)
   Active: active (running) since Mon 2022-08-22 14:54:11 EDT; 14s ago
 Main PID: 11599 (named)
   CGroup: /system.slice/named.service
           └─11599 /usr/sbin/named -u named -c /etc/named.conf

Aug 22 14:54:11 server3 named[11599]: network unreachable resolving './DNSKEY/IN': 2001:500:200::b#53
Aug 22 14:54:11 server3 named[11599]: network unreachable resolving './NS/IN': 2001:500:200::b#53
Aug 22 14:54:11 server3 named[11599]: network unreachable resolving './DNSKEY/IN': 2001:500:2f::f#53
Aug 22 14:54:11 server3 named[11599]: network unreachable resolving './NS/IN': 2001:500:2f::f#53
Aug 22 14:54:11 server3 named[11599]: network unreachable resolving './DNSKEY/IN': 2001:500:a8::e#53
Aug 22 14:54:11 server3 named[11599]: network unreachable resolving './NS/IN': 2001:500:a8::e#53
Aug 22 14:54:11 server3 named[11599]: network unreachable resolving './DNSKEY/IN': 2001:500:1::53#53
Aug 22 14:54:11 server3 named[11599]: network unreachable resolving './NS/IN': 2001:500:1::53#53
Aug 22 14:54:11 server3 named[11599]: managed-keys-zone: Key 20326 for zone . acceptance timer complete: key now trusted
Aug 22 14:54:11 server3 named[11599]: resolver priming query complete
```

```
[root@server3 etc]# dig text.example.com @127.0.0.1

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9 <<>> text.example.com @127.0.0.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 10091
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

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

;; ANSWER SECTION:
text.example.com.       604800  IN      A       192.168.1.221

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

;; ADDITIONAL SECTION:
ns1.example.com.        604800  IN      A       192.168.1.220

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Aug 22 15:09:57 EDT 2022
;; MSG SIZE  rcvd: 95
```

```
[root@server3 etc]# dig -x 192.168.1.223 @127.0.0.1

; <<>> DiG 9.11.4-P2-RedHat-9.11.4-26.P2.el7_9.9 <<>> -x 192.168.1.223 @127.0.0.1
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 9198
;; flags: qr aa rd ra; QUERY: 1, ANSWER: 1, AUTHORITY: 1, ADDITIONAL: 2

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags:; udp: 4096
;; QUESTION SECTION:
;223.1.168.192.in-addr.arpa.    IN      PTR

;; ANSWER SECTION:
223.1.168.192.in-addr.arpa. 604800 IN   PTR     static.example.com.

;; AUTHORITY SECTION:
168.192.in-addr.arpa.   604800  IN      NS      ns1.example.com.

;; ADDITIONAL SECTION:
ns1.example.com.        604800  IN      A       192.168.1.220

;; Query time: 0 msec
;; SERVER: 127.0.0.1#53(127.0.0.1)
;; WHEN: Mon Aug 22 15:27:47 EDT 2022
;; MSG SIZE  rcvd: 121
```

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

Добавление записей в firewalld так же откладываю дальше в ящик, докидываю строки для DHCP и DNS в iptables:
ss -tunap указывает на udp 68 открытый порт для DHCP, tcp/udp 53 порт на DNS.
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
Опять же можно ограничить всё адресами локальной сети для более закрытого микроклимата серверов.