Отказоустойчивый DHCP сервер на Mikrotik RouterOS

MIKROTIK NINJA

ИНТЕГРАЦИЯ · НАСТРОЙКА · ОБУЧЕНИЕ

Бубнов Дмитрий

Mikrotik-ninja.ru

/mikrotikninja

/mikrotikninja

/groups/mikrotikninja/

/bubnovdnet

bubnovd.net


#SYSADMINKA
Make sysadmins great again
/sysadminka
/event137391313
/groups/sysadminka/
/sysadminka
sysadminka.org

Dynamic Host Configuration Protocol

- Помощник админа
- Не только адрес и шлюз. Ещё DNS, WINS, NTP, маршруты и много другого
- Relay, Options

Как новичок представляет себе отказ DHCP

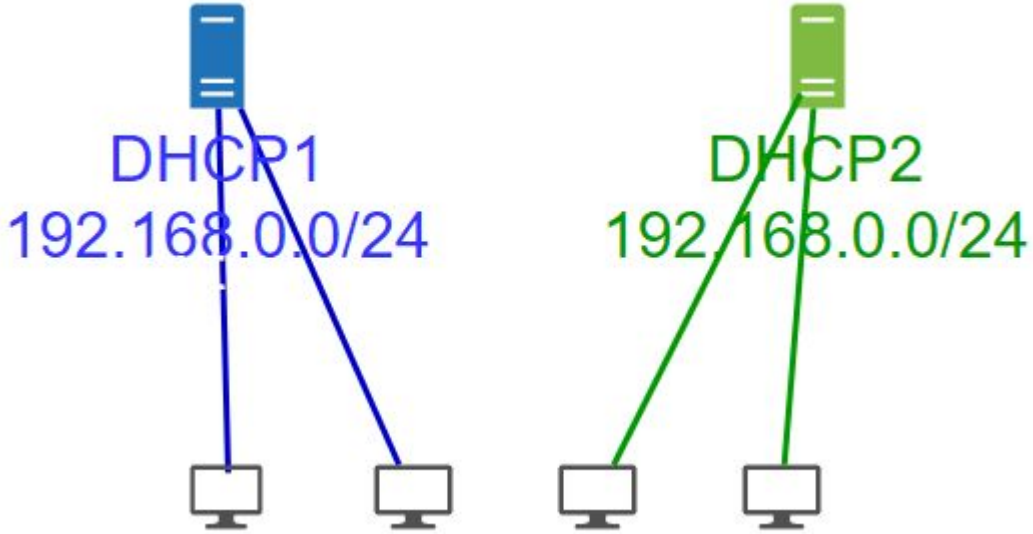
MIKROTIK NINJA

Как это отражается на работе

MIKROTIK NINJA

Выход: два сервера DHCP

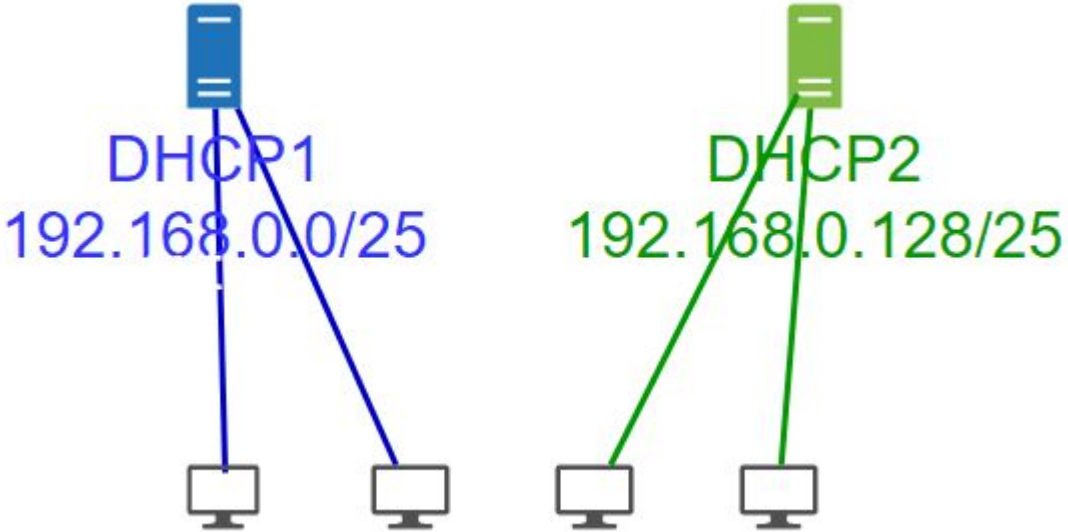
- Оно действительно работает
- Но только при правильной настройке



MIKROTIK NINJA

Выход: два сервера DHCP

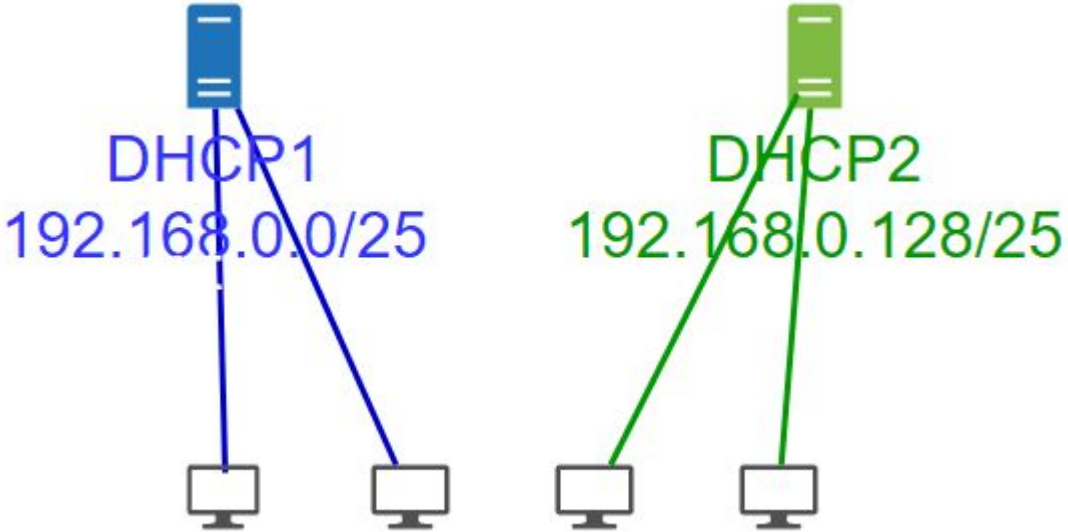
- Делим сеть на зоны
- При отказе одного из серверов теряем лишь половину сети



MIKROTIK NINJA

НЕ Выход: два сервера DHCP

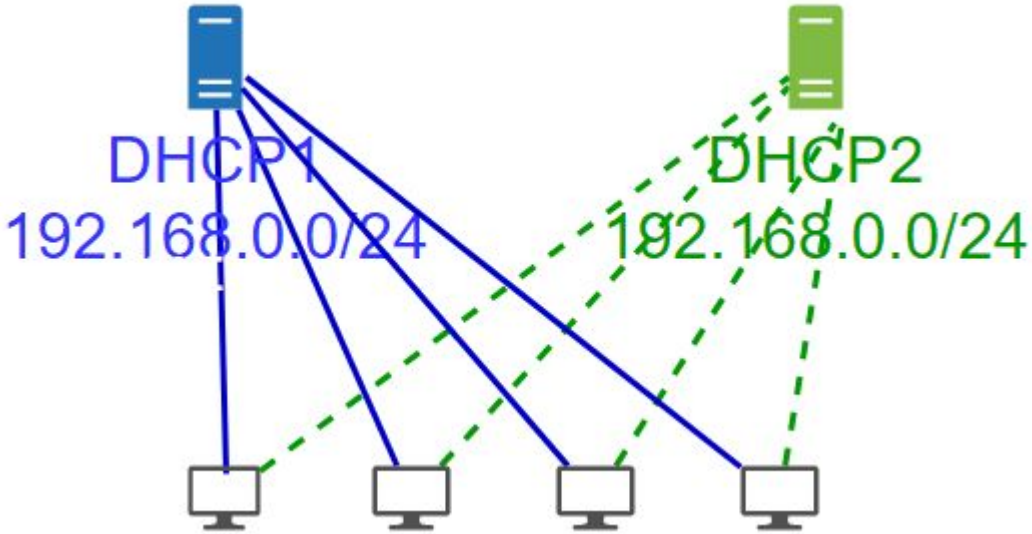
- Камеры, телефоны, принтеры и другие устройства часто имеют Static Lease
- Доступ к сети у них останется, но доступ к ним?



MIKROTIK NINJA

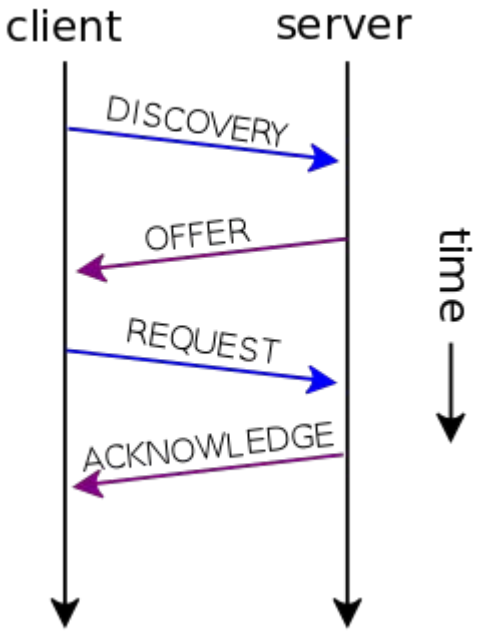
Выход: два сервера DHCP

- Всё равно нужно два **одинаковых** сервера
- В режиме Active/Passive



MIKROTIK NINJA

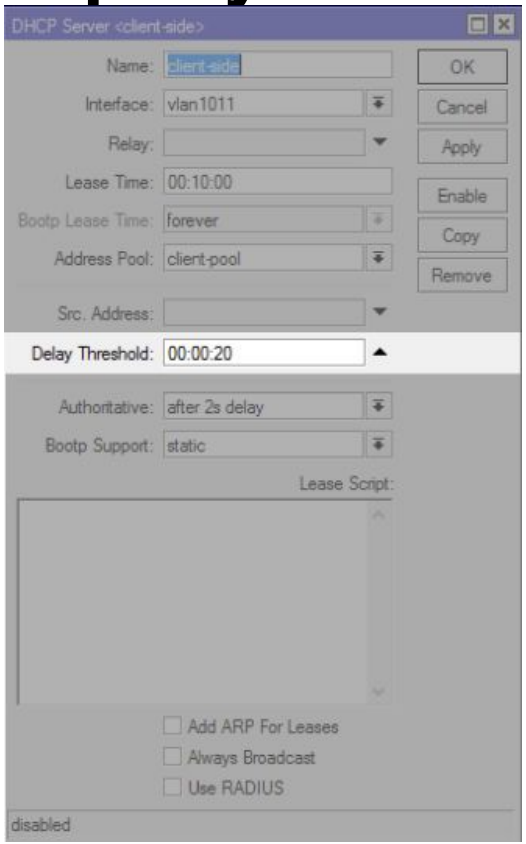
Принцип работы протокола




```
> Frame 32395: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
> Ethernet II, Src: Microsof_44:93:02 (00:15:5d:44:93:02), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Bootstrap Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x6e9bcd51
    Seconds elapsed: 53
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
```

MIKROTIK NINJA

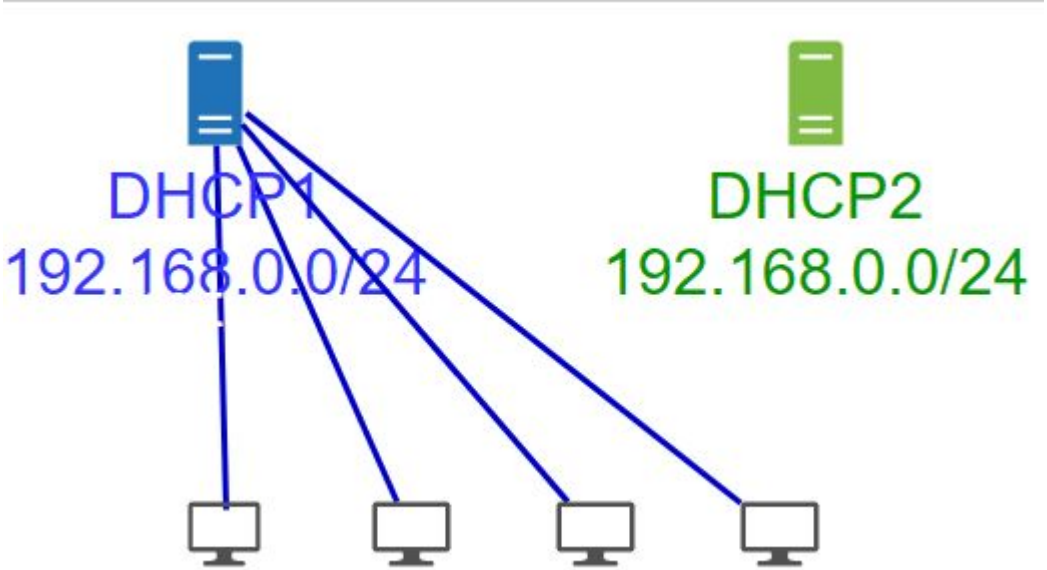
Заставляем один сервер отвечать только на “протухшие” запросы




```
> Frame 32395: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
> Ethernet II, Src: Microsof_44:93:02 (00:15:5d:44:93:02), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
v Bootstrap Protocol (Discover)
    Message type: Boot Request (1)
    Hardware type: Ethernet (0x01)
    Hardware address length: 6
    Hops: 0
    Transaction ID: 0x6e9bcd51
    Seconds elapsed: 53
  > Bootp flags: 0x0000 (Unicast)
    Client IP address: 0.0.0.0
    Your (client) IP address: 0.0.0.0
    Next server IP address: 0.0.0.0
    Relay agent IP address: 0.0.0.0
```

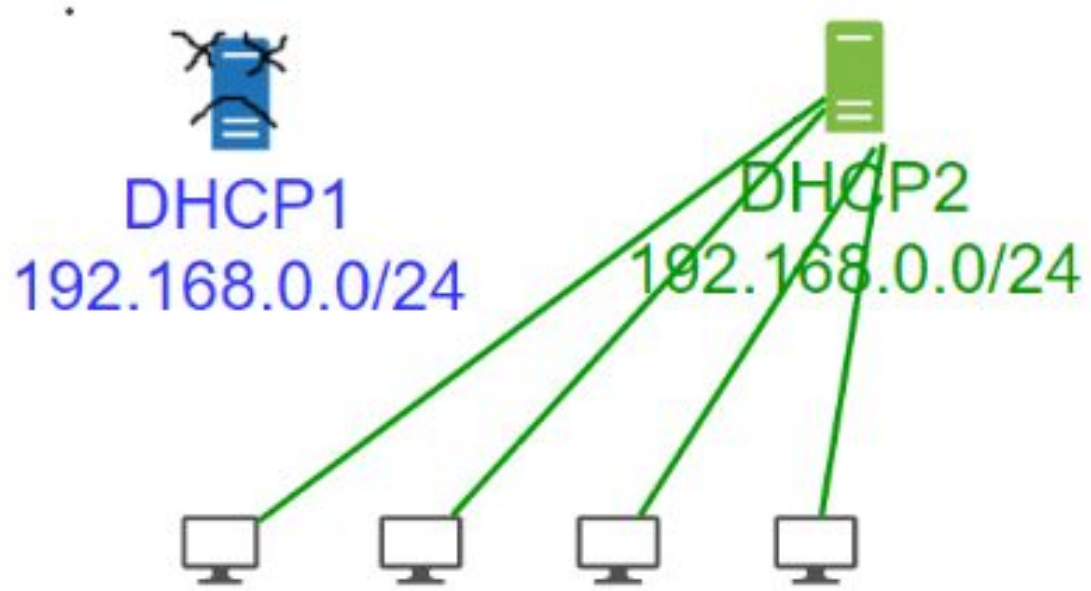
MIKROTIK NINJA

Все работает



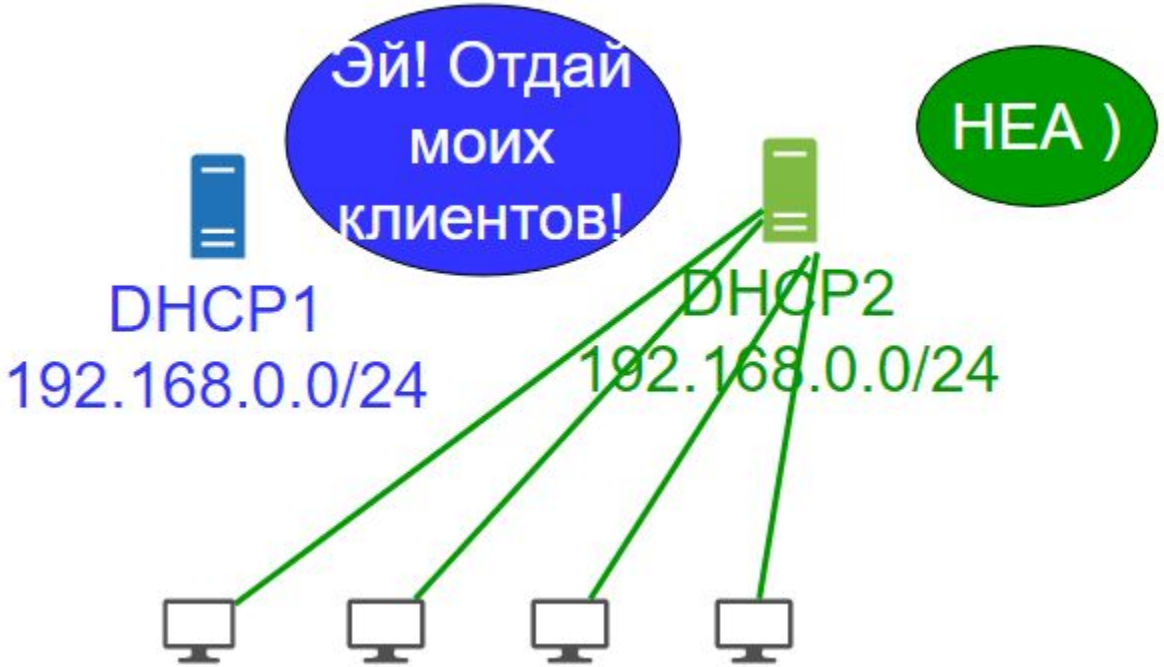
MIKROTIK NINJA

DHCP1 отказал



MIKROTIK NINJA

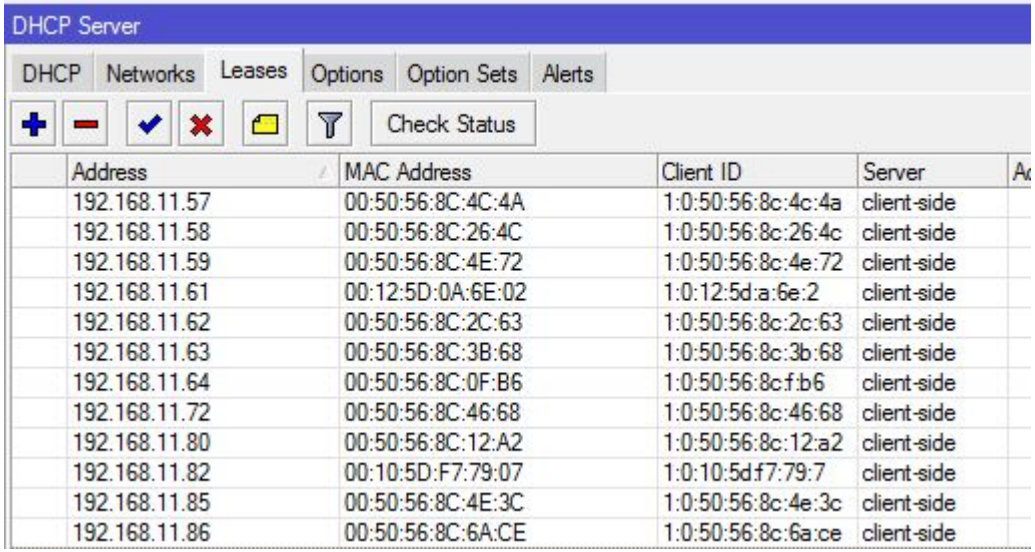
DHCP1 вернулся



MIKROTIK NINJA

И всё бы ничего...

Если бы не static leases

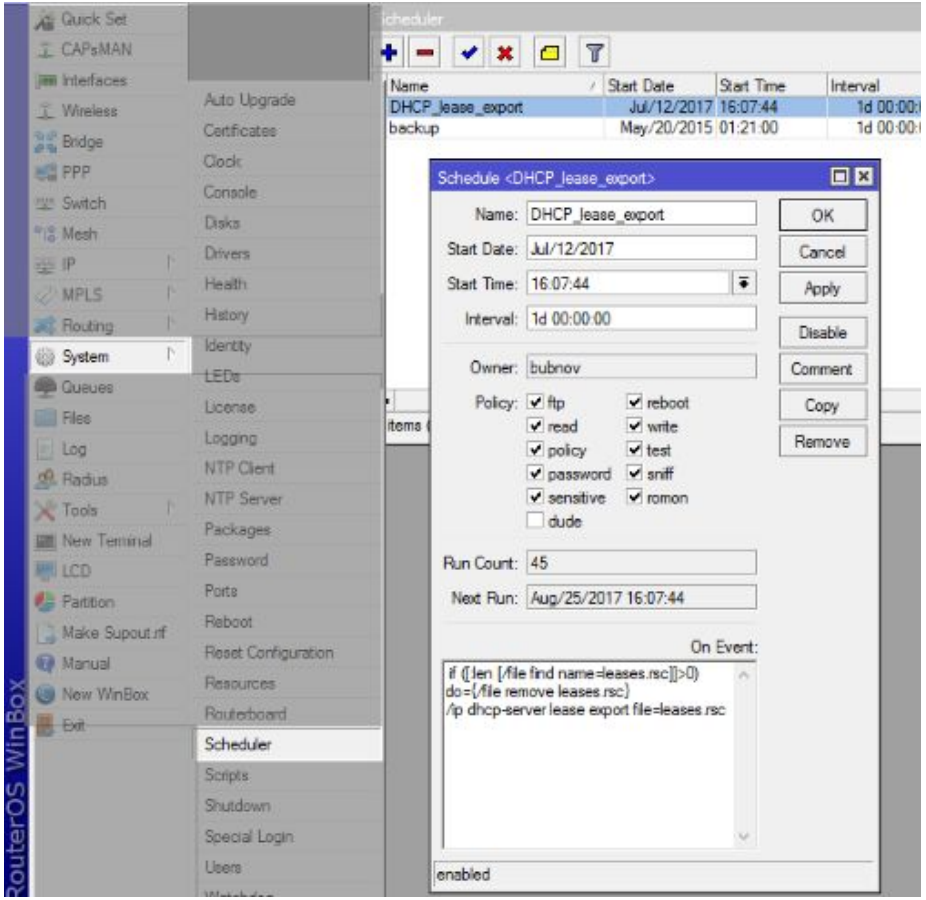


MIKROTIK NINJA

Синхронизируем записи!

```
if ([:len [/file find
name=leases.rsc]]>0) do={/file
remove leases.rsc}

/ip dhcp-server lease export
file=leases.rsc
```



MIKROTIK NINJA

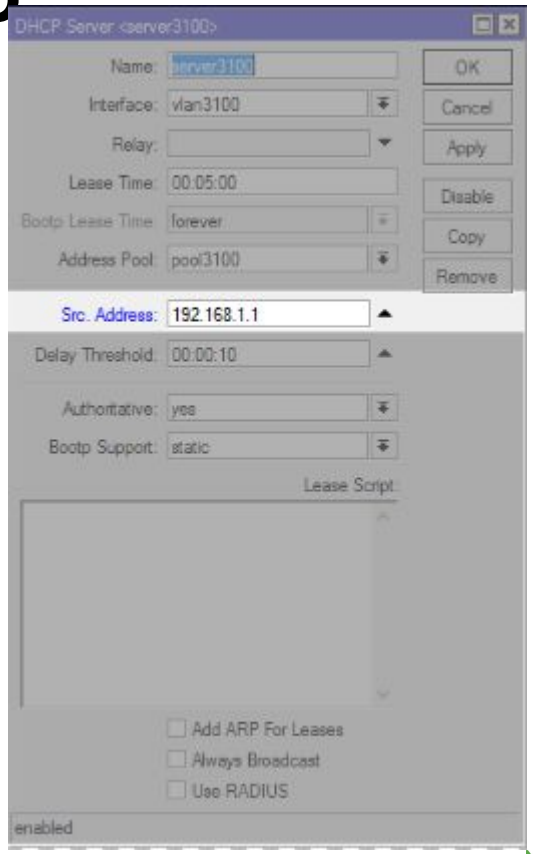
Синхронизируем записи!

```
 if ([:len [/file find name=leases.rsc]]>0) do={/file remove leases.rsc}
/tool fetch mode=ftp address=192.168.1.1 src-path=leases.rsc user=RB password=RB
 if ([:len [/file find name=leases.rsc]]>0) do={
        foreach i in=[/ip dhcp-server lease find ] do={
                /ip dhcp-server lease remove $i
        };
        import leases.rsc;
}
```

MIKROTIK NINJA

Поддерживать актуальные записи на двух железках тяжело... И скучно

- Поэтому схитрим и заставим резервный сервер притворяться основным



MIKROTIK NINJA

Подробнее

http://www.bubnovd.net/2017/07/dhcp-failover-with-routeros.html

MIKROTIK NINJA

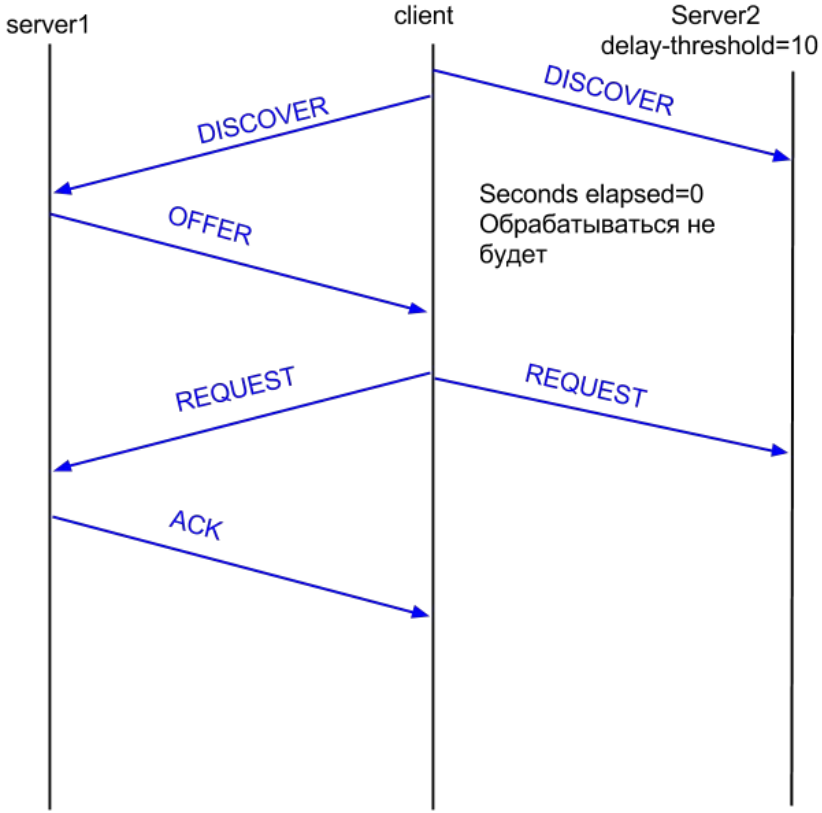
MIKROTIK NINJA

ИНТЕГРАЦИЯ · НАСТРОЙКА · ОБУЧЕНИЕ

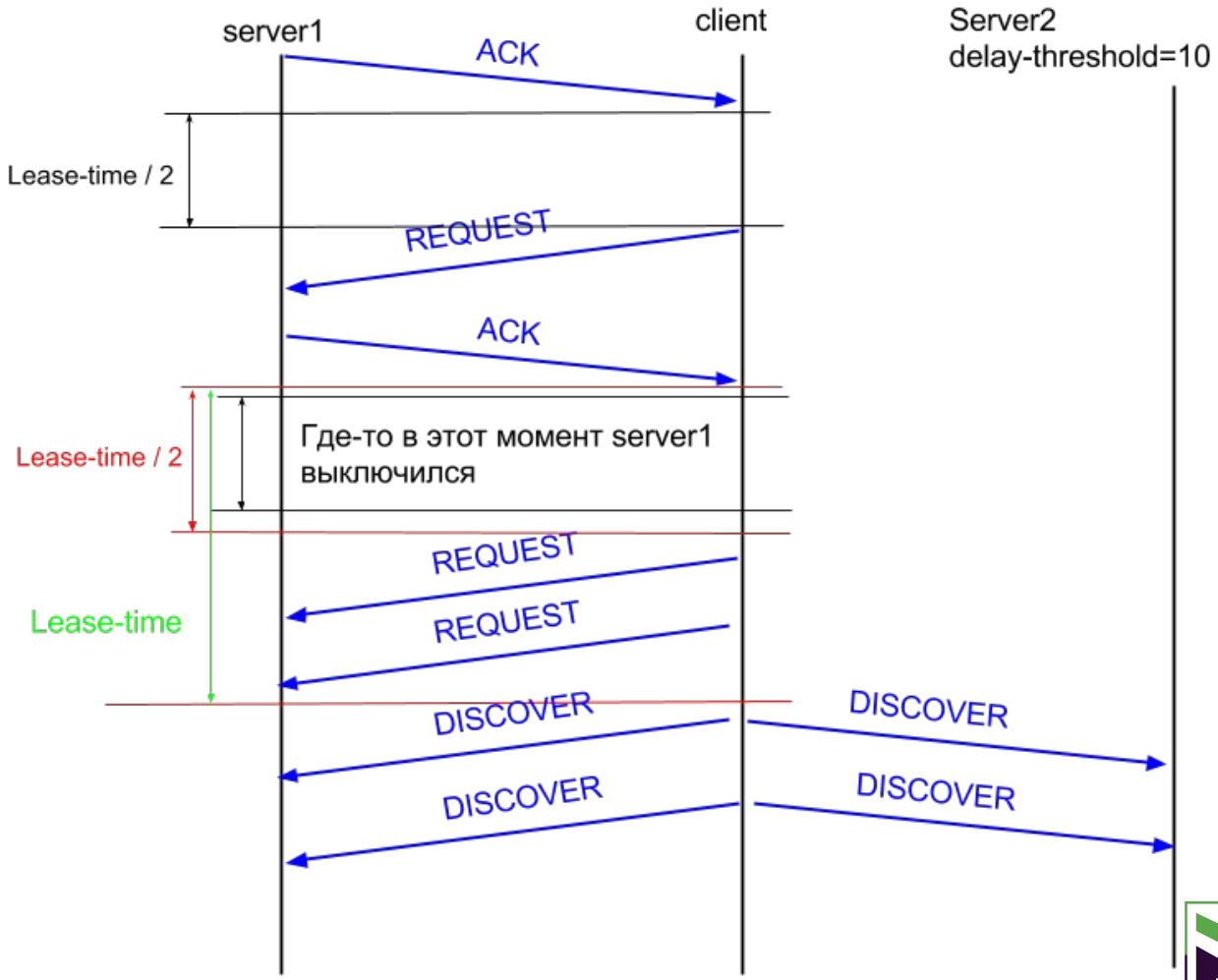
MIKROTIK-NINJA.RU

Курсы Mikrotik в Челябинске

Заставляем один сервер отвечать только на “протухшие” запросы



MIKROTIK NINJA



Эти REQUEST'ы никогда не попадут к server1, так как он уже выключен

Начался новый поиск DHCP сервера. Первые несколько DISCOVER server2 не обработает, так как seconds elapsed в них меньше 10

Но как только seconds elapsed в пакете превысит значение delay-threshold, server2 начнет работать с такими пакетами