

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 ДНCR

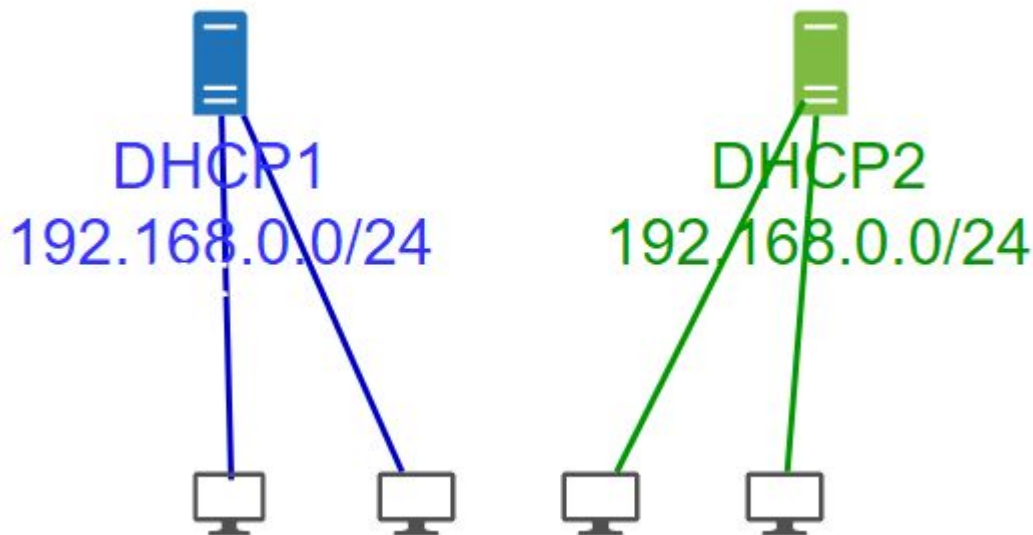


Как это отражается на работе



Выход: два сервера DHCP

- Оно действительно работает
- Но только при правильной настройке



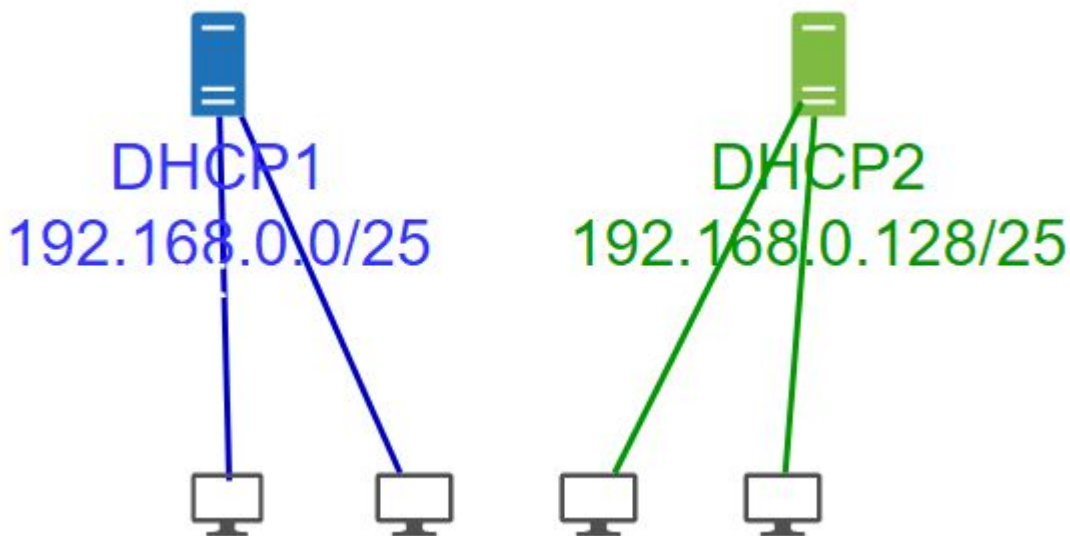
Выход: два сервера DHCP

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



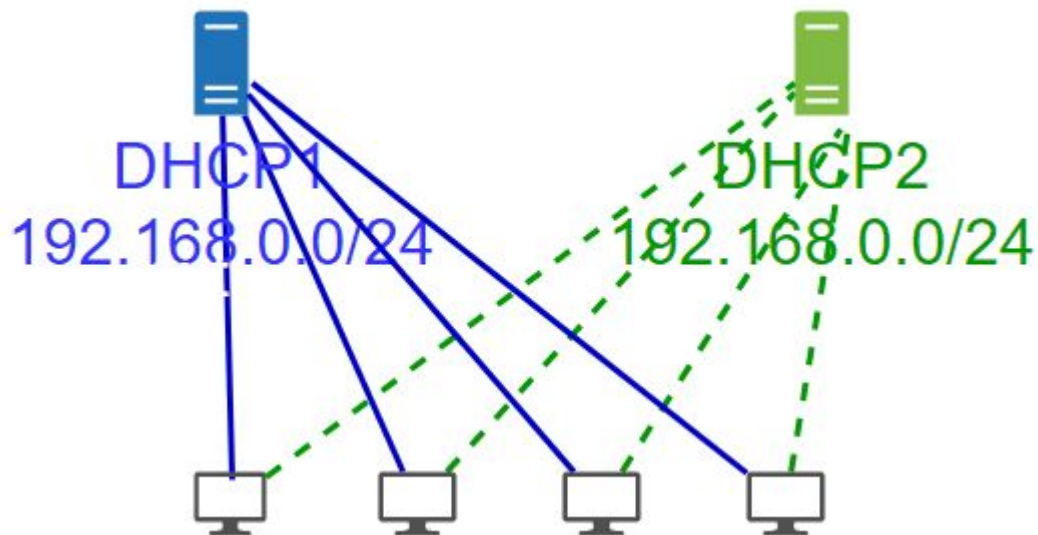
НЕ Выход: два сервера DHCP

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

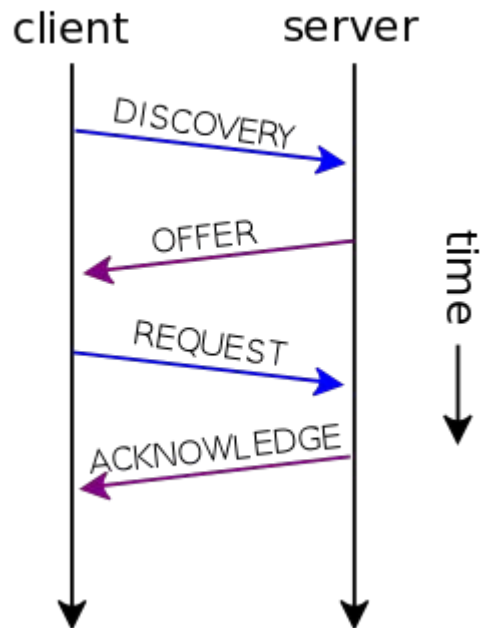


Выход: два сервера DHCP

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



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
```



Заставляем один сервер отвечать только на “протухшие” запросы

DHCP Server <client-side>

Name: OK

Interface: Cancel

Relay: Apply

Lease Time: Enable

Bootp Lease Time: Copy

Address Pool: Remove

Src. Address:

Delay Threshold:

Authoritative:

Bootp Support:

Lease Script:

☐ Add ARP For Leases

☐ Always Broadcast

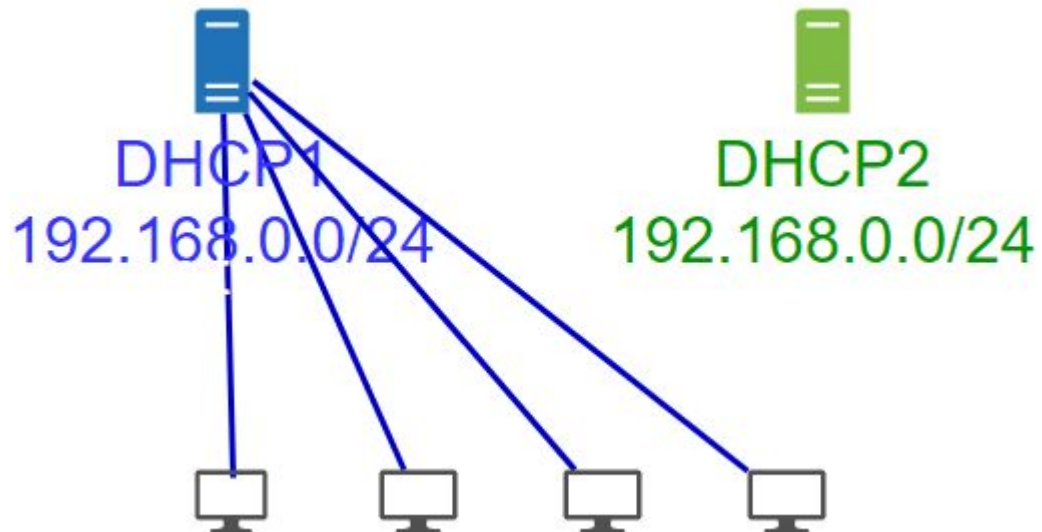
☐ Use RADIUS

disabled

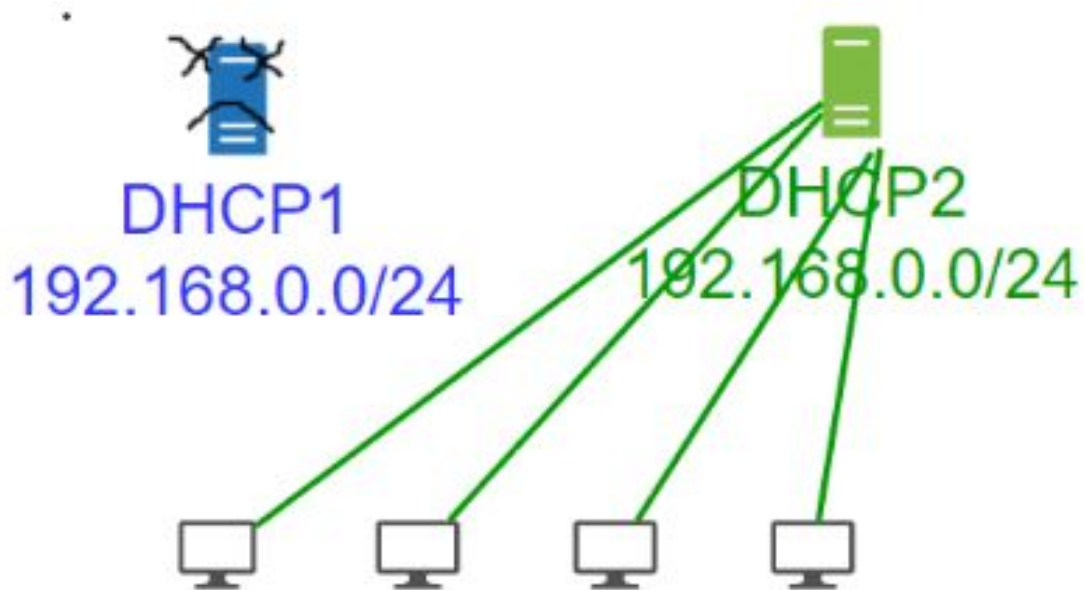
```
> Frame 32395: 342 bytes on wire (2736 bits), 342 bytes captured (2736 bits) on interface 0
> Ethernet II, Src: Microsof_44:93:02 (00:15:5d:44:93:02), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
> Internet Protocol Version 4, Src: 0.0.0.0, Dst: 255.255.255.255
> User Datagram Protocol, Src Port: 68, Dst Port: 67
▼ 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
```



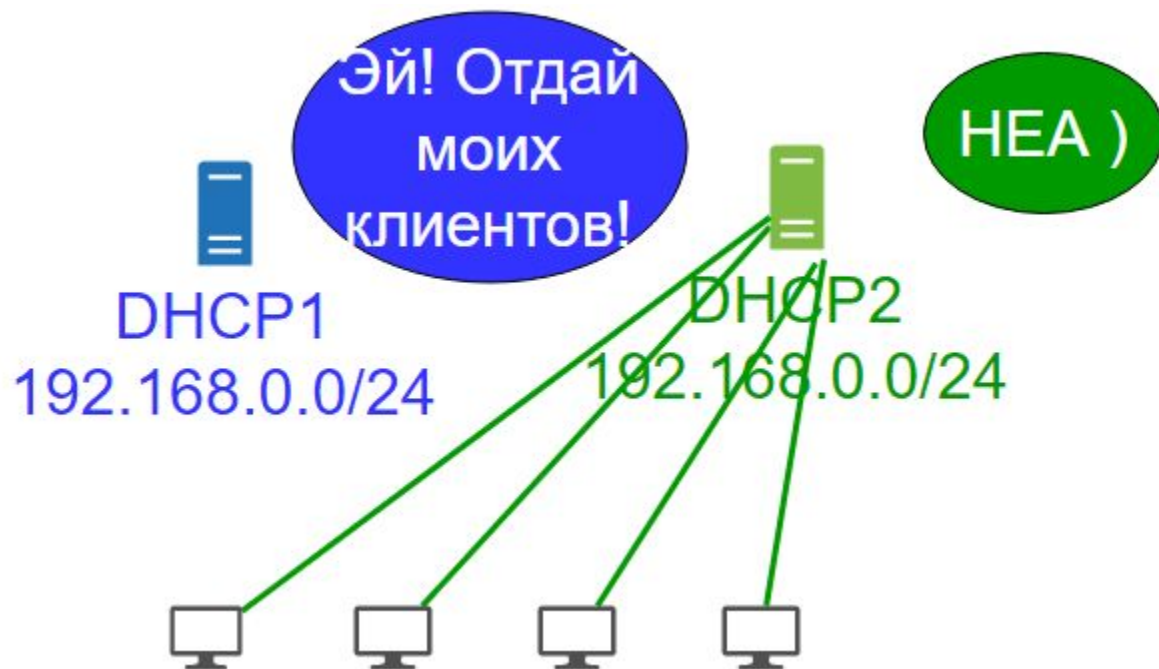
Все работает



DHCP1 отказал



DHCP1 вернулся



И всё бы ничего...

Если бы не static leases

DHCP Server

DHCP

Networks

Leases

Options

Option Sets

Alerts

Check Status

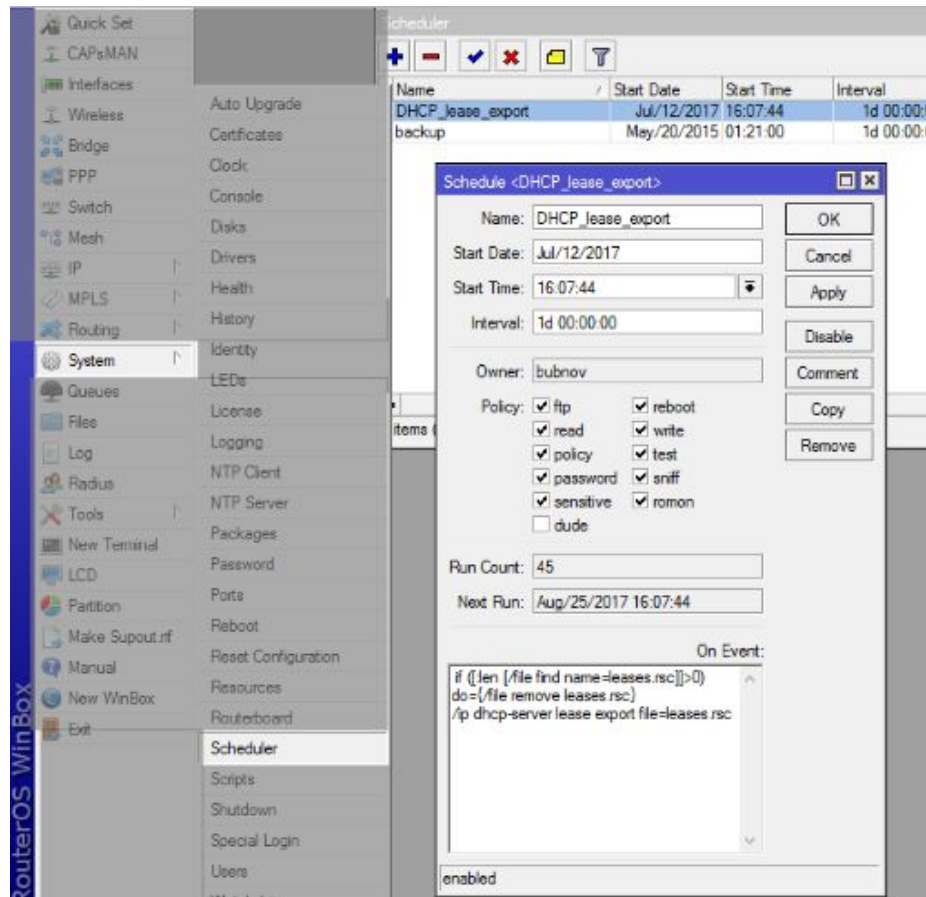
Address	MAC Address	Client ID	Server	A
192.168.11.57	00:50:56:8C:4C:4A	1:0:50:56:8c:4c:4a	client-side	
192.168.11.58	00:50:56:8C:26:4C	1:0:50:56:8c:26:4c	client-side	
192.168.11.59	00:50:56:8C:4E:72	1:0:50:56:8c:4e:72	client-side	
192.168.11.61	00:12:5D:0A:6E:02	1:0:12:5d:a:6e:2	client-side	
192.168.11.62	00:50:56:8C:2C:63	1:0:50:56:8c:2c:63	client-side	
192.168.11.63	00:50:56:8C:3B:68	1:0:50:56:8c:3b:68	client-side	
192.168.11.64	00:50:56:8C:0F:B6	1:0:50:56:8c:f:b6	client-side	
192.168.11.72	00:50:56:8C:46:68	1:0:50:56:8c:46:68	client-side	
192.168.11.80	00:50:56:8C:12:A2	1:0:50:56:8c:12:a2	client-side	
192.168.11.82	00:10:5D:F7:79:07	1:0:10:5d:f7:79:7	client-side	
192.168.11.85	00:50:56:8C:4E:3C	1:0:50:56:8c:4e:3c	client-side	
192.168.11.86	00:50:56:8C:6A:CE	1:0:50:56:8c:6a:ce	client-side	



Синхронизируем записи!

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

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



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;

}
```



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

- Поэтому схитрим и заставим резервный сервер притворяться основным

DHCP Server <server3100>

Name: server3100

Interface: vlan3100

Relay:

Lease Time: 00:05:00

Bootp Lease Time: forever

Address Pool: pool3100

Src. Address: 192.168.1.1

Delay Threshold: 00:00:10

Authoritative: yes

Bootp Support: static

Lease Script

☐ Add ARP For Leases

☐ Always Broadcast

☐ Use RADIUS

enabled



Подробнее

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





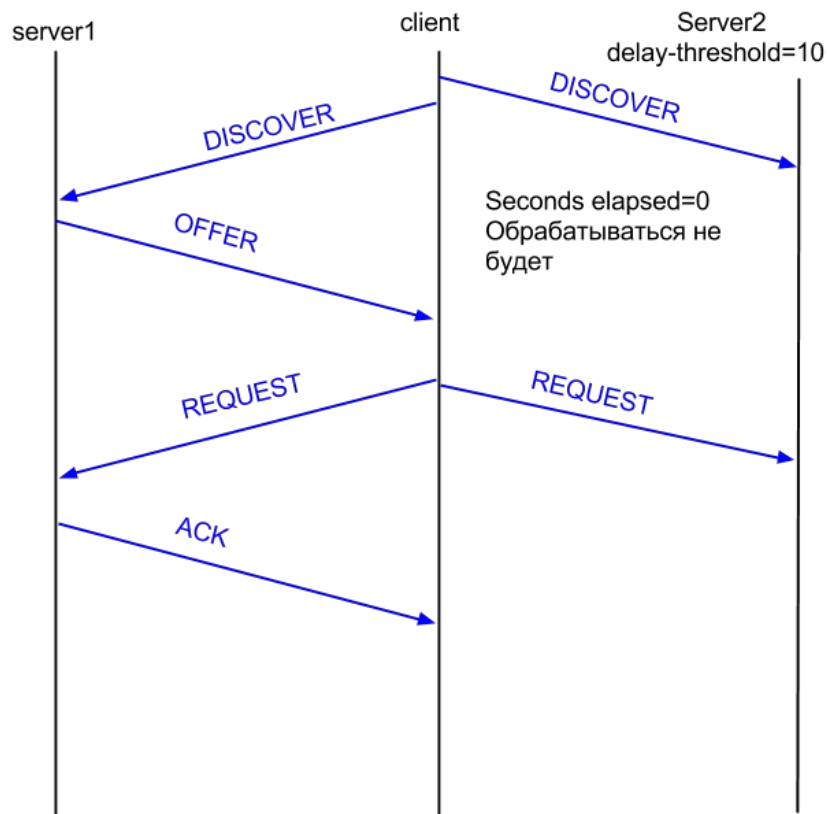
MIKROTIK NINJA

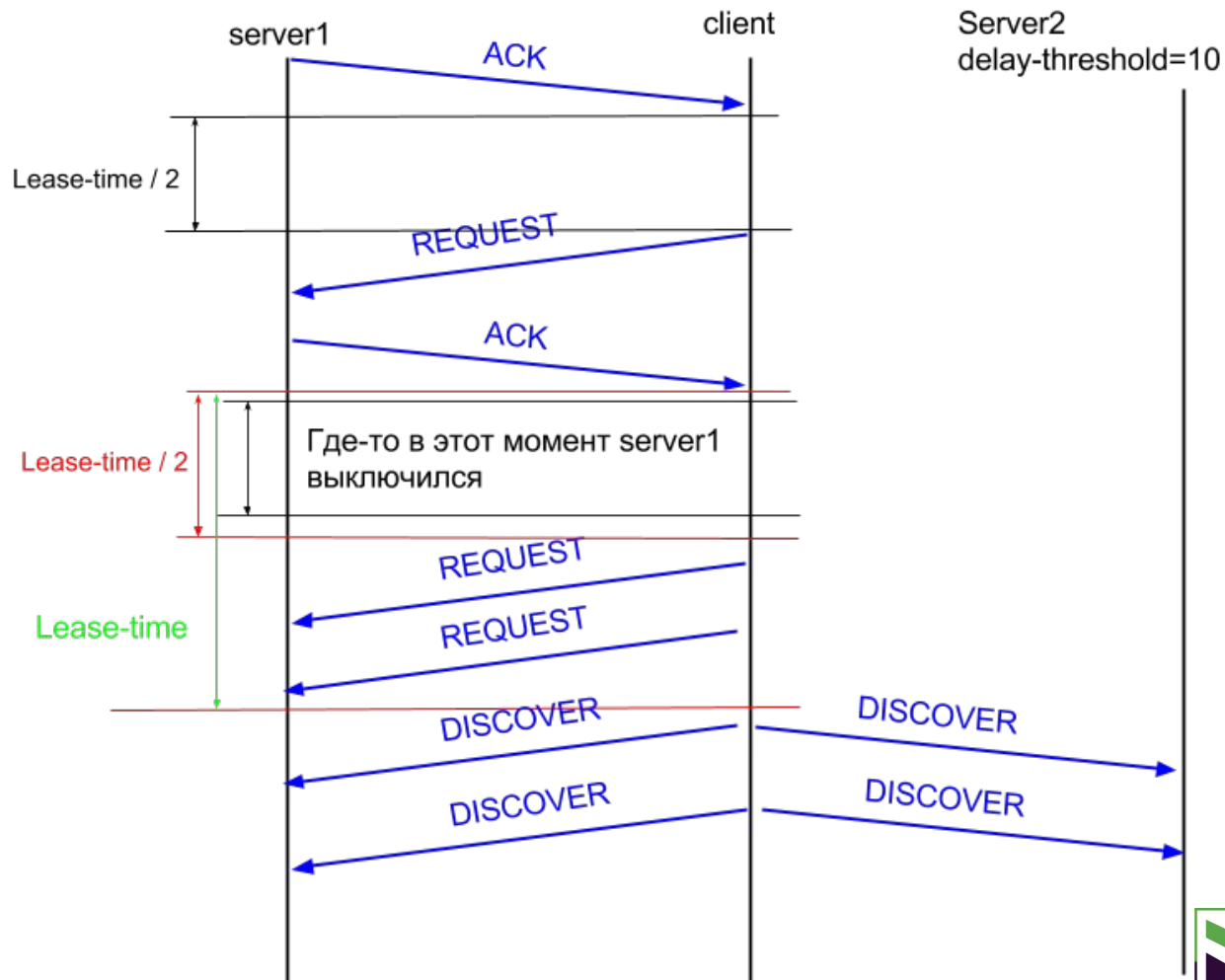
ИНТЕГРАЦИЯ • НАСТРОЙКА • ОБУЧЕНИЕ

MIKROTIK-NINJA.RU

Курсы Mikrotik в Челябинске

Заставляем один сервер отвечать только на “протухшие” запросы





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

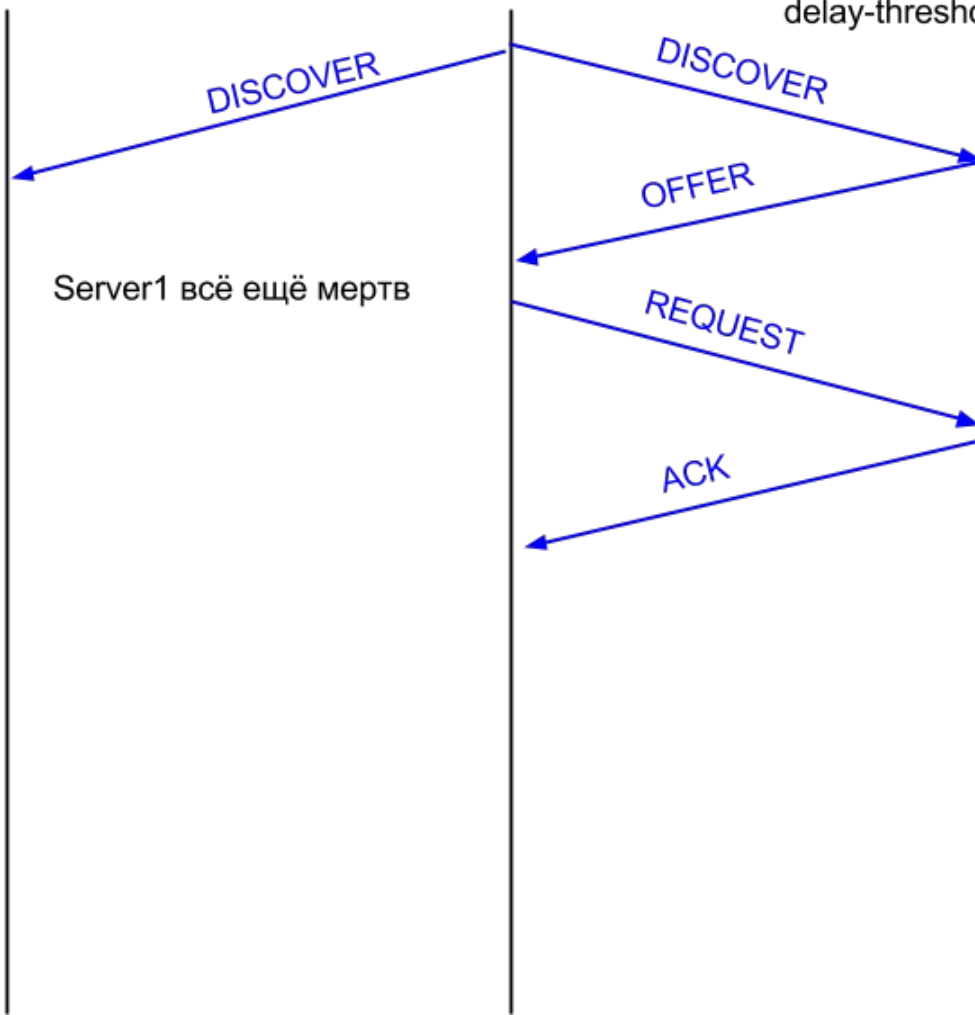


Но как только seconds elapsed в пакете превысит значение delay-threshold, server2 начнет работать с такими пакетами

server1

client

Server2
delay-threshold=10



Server1 всё ещё мертв

