**Mikrotik с**ъбитие
за професионалисти ентусиасти и
всички който имат желание да
се **забавляват!**

# NetCamp

## 2021

# Mikrotik VRRP. Реализация при ROS v6 и ROS v7

Несебър 08.2021

# Да се запознаем

## инж. Георги Анастасов

*За мен!* *Сертифициран мрежов специалист и консултант за продукти на* ***Mikrotik*** *с опит в проектиране и изграждане на малки и средни компютърни мрежи, сървъри и системи за архивиране.*

**WEB: www.steadypc.com**
**E-mail: office@steadypc.com**
**GSM: +359 878806291**

# Mikrotik Scripting работа с файлове.

## Съдържание



# VRRP

Описание на протокола

01

# Mikrotik VRRP.
# RoS v6

## 1. VRRP протокол RFC 5987, RFC 3768.

- Протокол, поддържащ резервираност на рутери чрез виртуален рутер с процес на избор на Master рутер на основата приоритет на рутера;

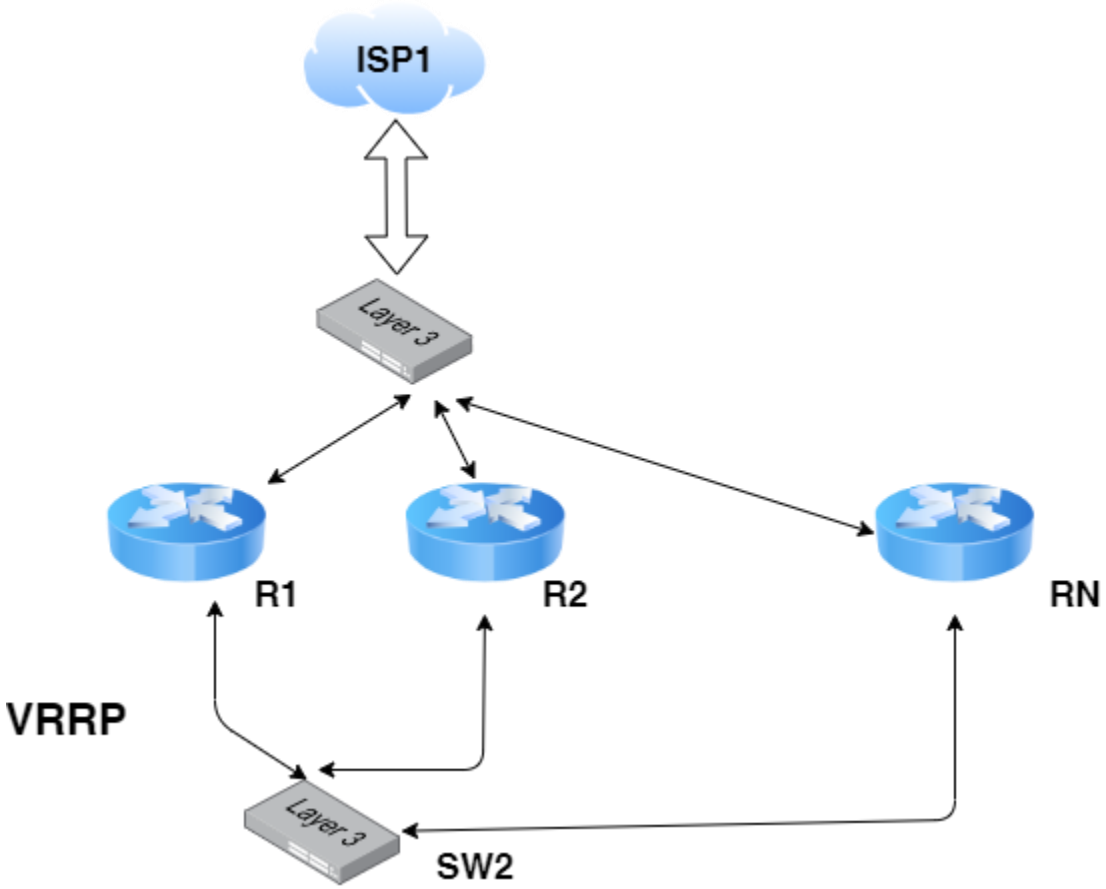
- **Протокол 112 (VRRP)**
  Използва Multicast пакети към destination address Pv4 *224.0.0.18* и IPv6 *FF02:0:0:0:0:0:0:12*. TTL 255 ;

- Сорс адреса за IPv4 е primary IP address на интерфейса, от който се изпраща
- Сорс адреса за IPv6 е link-local адреса на интерфейса

# Mikrotik VRRP.
## RoS v6

- Само Master рутера изпраща периодични Advertisement съобщения;
  - Всички рутери трябва да се конфигурират с еднакъв advertisement interval
- Приоритет на рутера 1 – 254;
  - Най висок приоритет е 254
- TTL=255 – съобщенията се разпространяват само до следващия рутер;
- MAC адрес 00:00:5E:00:XX  XX е VID в hex формат. Пр: VRID=10 -> hex(0A)

# Mikrotik VRRP.
## RoS v6



# Mikrotik VRRP.
## RoS v6

**2. Виртуален рутер.**

- Интерфейс, върху който се настройва;
- Име – еднакво за всички рутери;
- VRID – еднакво за всички рутери;
- IP  адрес – еднакъв за всички рутери. Маска на VRRP интерфейса /32 ;
- Интервал – еднакъв за всички;
- **Приоритет** – различен. Определя Master и Backup;

# Mikrotik VRRP.
## RoS v6

- Security – еднаква фраза за всички. Препоръчва се за WAN интерфейси;

- Preemption mode;

* Ако preemption-mode=yes, Master рутера винаги има приоритет – дори ако backup рутера има по-висок приоритет, няма да бъде избран за master, докато текущия master стане недостъпен.

- VRRP маже да се конфигурира на всякакви интерфейси  Bridge, VLAN, Ethernet интерфейс

**Съвместим с други производители. Поддържа повече от 2 рутера**

# Mikrotik VRRP ROS v7

Нови функции и съвместимост с други устройства

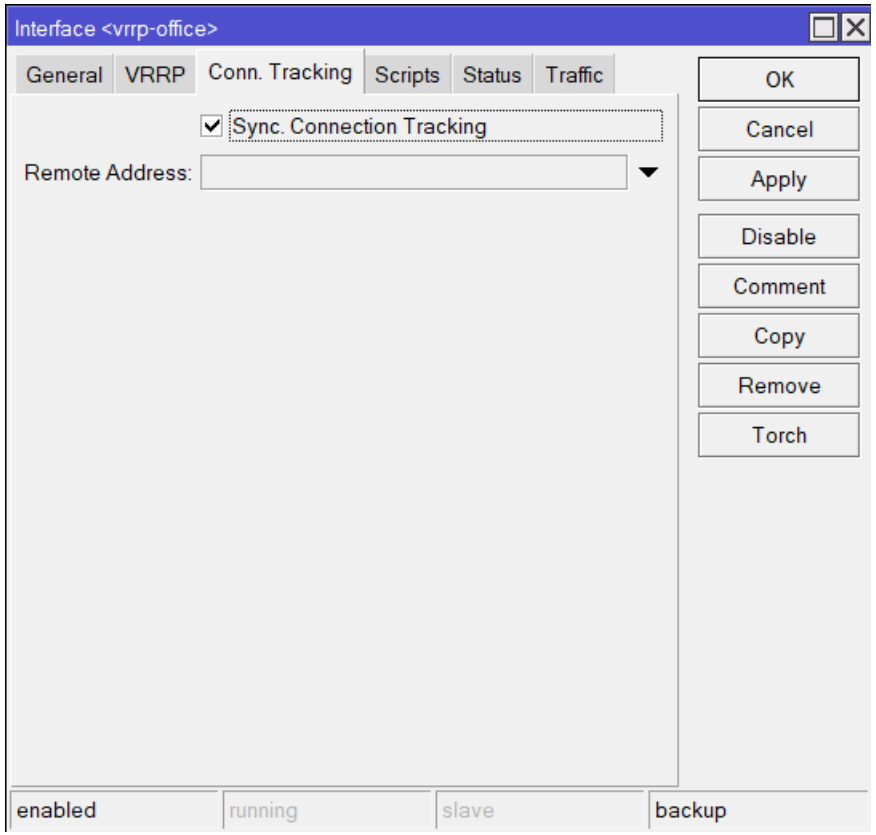
02

# Mikrotik VRRP ROS v7
## Нови функции

- Sync Connection Tracking
- Активира се и на двата рутера

```
sync-connection-tracking=yes
```

- **Не е съвместим с други производители**



# Mikrotik VRRP ROS v7
## Нови функции

**VRRP с connection syncing protocol поддържа само два рутера master и backup.**

- Собствен протокол на MikroTik. Работи само с  MikroTik рутери;
- Двата рутера трябва да поддържат една и съща версия на RoutersOS v7;
- VRRP Preemption Mode трябва да е забранен (preemption-mode=no);
- Синхронизирането с connection syncing protocol използва IPv4 за вътрешна синхронизация. При IPv6 (v3-protocol=ipv6), *remote-address* е задължителен;
- При IPv4, *remote-address* не е задължителен, но е препоръчително да се използва за намаляване на латентността при синхронизиране на VRRP

# 03

## Mikrotik Резервираност HA

Дефиниране на задачата
Изисквания
Особености на задачата
Проблеми

# Резервираност HA
## Дефиниране на задачата

Тип на резервираността

1. **Active – Active** вариант с баланс на натоварването;

2. **Active – Standby** вариант с резервен VRRP рутер в готовност;

3. **Active – Passive** вариант с рутер в чекмеджето

# Резервираност НА
# Изисквания и план

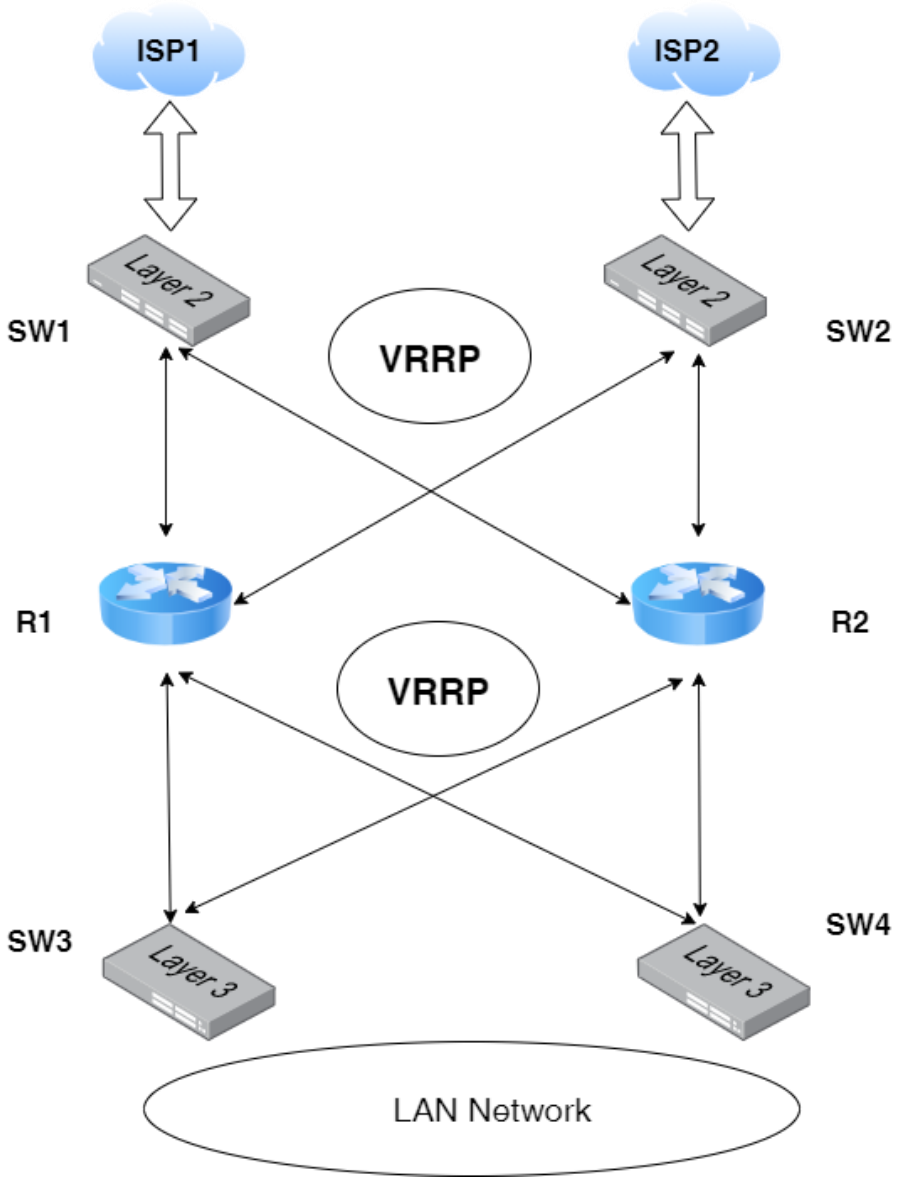
**Идея и изисквания**

- **Не е задължително рутерите да са еднакви;**
- Допълнителни суичове за реализиране на VRRP;
- Предварителен подробен план на резервираността и функционалността на устройствата;
- Промените в конфигурациите могат да се осъществят автоматично със скрипт или на ръка

# Резервираност HA
## Пълна схема

Active - Active
Active – Standby

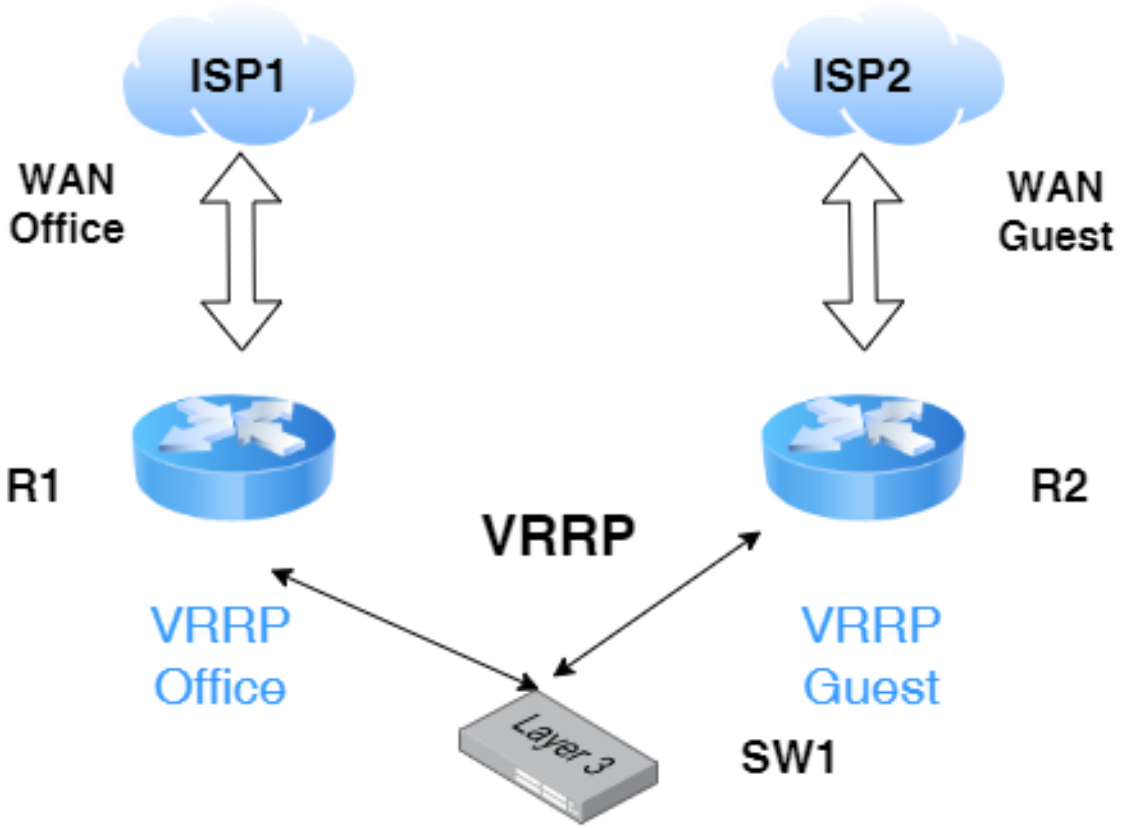
Цялостен вариант



# Резервираност HA
## Съкратен вариант

Active - Active

Съкратен вариант



# Резервираност НА
# Особенности в реализацията

1. **Прехвърляне на конфигурация на backup рутера R2.**

1.1. Прави се backup на конфигурацията на R1 и се прехвърля на R2;

1.2. Прави се Reset MAC address на LAN физическите интерфейси и bridges;

1.3. Прави се скрипт за настройка на разликите или разликите се правят на ръка;

1.4. High Availability скрипт реализиращ периодично т. 2.1,2.2, 2.3.

**Огледайте конфигурацията и използвайте само необходимото за робота в авариен режим на резервният рутер!**

# Резервираност HA
# Особености в реализацията

## 2. Определяне на разликите в конфигурациите.

### 2.1. Определяне на броя VRRP интерфейси и настройка на VRRP.

- Определете броя на рутерите;
- Задайте IP адрес на интерфейсите;
- Създайте VRRP на интерфейсите;
- Задайте vrid на vrrp интерфейса;
- Задайте IP адрес на VRRP интерфейса – един и същ за съответният vrrid ;
- Определете дали ще ползвате preemption mode;
- Определете дали ще ползвате connection tracking sync

**Създайте част от скрипт за промяна на различните стойности за  R2.**

# Резервираност HA
# Особенности в реализацията

## 2.2. DHCP client на WAN VRRP интерфейсите.

- Проверете дали доставчиците приемат MAC адресите на WAN VRRP интерфейсите и определете дали ще ползвате суич пред WAN интерфейсите за VRRP резервиране;
- MAC адресите на физическите интерфейси трябва да са различни;
- **При съкратената схема променете MAC адресите на WAN интерфейсите** на R1 и R2, така че ръчно да можете да  прехвърлите на кабела на интернет доставчиците.

**Създайте част от скрипт за промяна на различните стойности за  R2.**

# Резервираност HA
# Особенности в реализацията

**2.3 DHCP във вътрешната мрежа**

- DHCP на VRRP интерфейс (/24);
- DHCP от друго устройство в мрежата;
- Определете статичните DHCP за R2 ;
- **При съкратения вариант с баланс на трафика двата рутера имат различни DHCP сървъри на VRRP интерфейсите.**

**Създайте част от скрипт за промяна на различните стойности за R2.**

# Резервираност HA
# Особености в реализацията

### 2.4 Скриптове и scheduler

- Прехвърлете всички скриптове и schedulers, но преценете кои schedulers ще са разрешени и кои ще се разрешават и забраняват динамично, в зависимост от това дали рутера преминава от master или backup.

**Създайте част от скрипт за промяна на различните стойности за  R2.**

# Резервираност HA
# Особености в реализацията

### 2.5 Сертификати

- Уеднаквете сертификатите и в двата рутера чрез експорт и импорт на публичните и собствените самоподписани сертификати;
- При прехвърляне с backup се пренасят и всички сертификати;
- При съкратеният вариант трябва да се генерират сертификати за IP на двата доставчика съответно за R1 и R2

**Ако е необходимо създайте част от скрипт за промяна на различните стойности за  R2.**

# Резервираност HA
# Особенности в реализацията

### 2.6 CAPSMAN

- Обръщението към Capsman трябва да е по IP адрес на VRRP интерфейса. По този начин Capsman ще е активен на рутера, който е master;

При съкратеният вариант с динамично разпределение на трафика, R1 обслужва Capsman. Office трафика минава през R1, а Guest трафика минава през R2.

- При рутери с ROS v7 и  Точки за достъп  с ROS v6, Разликата във версиите води до проблеми с работата на VRRP с избор на master и backup.

**Ако е необходимо, създайте част от скрипт за промяна на различните стойности за  R2.**

# Резервираност HA
# Особености в реализацията

## 2.7 DDNS на VPN  при WAN VRRP интерфейсите

- При статични IP адреси VPN връзките се обработват от master рутера;
- При DHCP client на WAN VRRP интерфейс при клиента трябва да се конфигурират два VPN тунела – към DDNS на R1 и към R2, тъй като не може да се определи автоматично кой от двата рутера е master;
- **IP Sec в тунелен режим** – можете само със статични IP и при прехвърлени сертификати;
- **Виж презентация на Петър Димитров  NetCamp 2020** „Резервиранена IPsec в тунеленрежим с 2 peer-а “

**Създайте част от скрипт за промяна на различните стойности за  R2.**

# Резервираност HA
# Особености в реализацията

### 2.8 DUDE

- **Dude** не може да се прехвърля лесно в такава конфигурация.

# Резервираност HA
# Особености в реализацията

### 2.8 Firewall Filter правила

- Използвайте интерфейс листи. По този начин, ако използвате друг модел Mikrotik рутер, трябва да конфигурирате само интерфейсите влизащи в интерфейс листите.

**Създайте част от скрипт за промяна на различните стойности за  R2.**

# Резервираност HA
# Особенности в реализацията

### 2.8 Firewall Filter правила

- Използвайте интерфейс листи. По този начин ако използвате друг модел Mikrotik рутер, трябва да конфигурирате само интерфейсите влизащи в интерфейс листите;

- Използвайте коментари на правилата, за да можете променяте нужното правило като търсите с

find comment=“My comment”

**Създайте част от скрипт за промяна на различните стойности за  R2.**

04

## Резервираност НА скриптове

SSH ключове, трансфер на конфигурацията. Отдалечени команди. Скриптове за реализация.

# Резервираност HA скриптове
## Идея


1. Export r1.rsc

1.1 Save r1.rsc to R2

1.2 Start transfer.rsc to HA R2

2. Reset R2

3. Start ha.rsc

3.1 Import r1.rsc

3.2 Import r2-ha.rsc

# Резервираност НА скриптове
# SSH ключове

Използване на скрипт за синхронизиране на R2 с трансфер по SSH

1. Създават се двойка SSH ключове **id_dsa** и **id_dsa.pub** на Linux машина.

* Потребителя в публичния ключ трябва да е еднакъв с потребителя в рутера!

1.1. Създават се потребителски имена и пароли за R1 и R2 за конфигуриране на трансфера и се разрешава SSH.

- ROS v7.1beta6 не поддържа импорт на частен SSH ключ в GUI.

# Резервираност НА скриптове SSH ключове

1.2. Добавяне на SSH ключовете в CLI

- За R1 – частен и публичен
- За R2  – публичен

# Резервираност НА скриптове
# SSH ключове

- SSH ключове в R1.

/user ssh-keys import user=ftpupload public-key-file=id_dsa.pub
/user ssh-keys private import user=ftpupload private-key-file=id_dsa

- SSH ключове в R2.

/user ssh-keys import user=ftpupload public-key-file=id_dsa.pub

# Резервираност HA скриптове
# Трансфер на конфигурацията

2. Запазване на скриптовете след reset на R2
- Поставете скриптовете и файловете, които искате да запазите в папка **/flash**

**ha.rsc**
**r2-ha.rsc**

- Добавяне на настройка **:add** Промяна на настройка **:set [find ..] …**

# Резервираност НА скриптове
# Трансфер на конфигурацията

3. Трансфер на файл от R1 към R2 с команда /tool fetch

**FTP transfer**

/tool fetch address=192.168.123.3 src-path=r1.rsc user=ftpupload mode=ftp password=test dst-path=/flash/r1.rsc upload=yes;

**SFTP transfer**

/tool fetch upload=yes url="sftp://192.168.123.3/flash/r1.rsc" user=ftpupload password=test src-path=r1.rsc;

# Резервираност НА скриптове
# Отдалечени команди

4. Стартиране на скрипт от R1 в R2 чрез **ssh-exec**

#Execute command on R2

/system ssh-exec address=192.168.123.3 user=ftpupload command="system reset-configuration keep-users=yes no-defaults=yes run-after-reset=/flash/ha.rsc"

# Резервираност HA скриптове
# Настройка на R2

5. Промяна на настройки в R2 чрез скрипт r2-ha.rsc

5.1 Промяна на IP адрес

/ip address set [/ip address find interface=bridge1] address=192.168.123.3/24

Или

/ip address set [/ip address find address=192.168.123.2] address=192.168.123.3/24

# Резервираност HA скриптове
# Настройка на R2

5.1 Забраняване на инструкции **чрез сравняване на коментари**.

```
/tool netwatch enable [find comment="R2 ISP link check"];
/tool netwatch disable [find comment="R1 ISP link check"];
```

Или **чрез определяне на поредността** на командата /tool netwatch print

```
/tool netwatch
disable 1
enable 0
```

6. Общото време за синхронизация на конфигурацията е **под 2 минути**.

# Резервираност HA

## Скрипт

**R1 transfer.rsc script**

```
#Export R1 configuration
/export file-name=r1.rsc show-sensitive;
:delay 15s;
:log info "Backup of R1 is done";

#Save r1.rsc to router R2
/tool fetch upload=yes url="sftp://192.168.123.3/flash/r1.rsc" user=ftpupload
password=test src-path=r1.rsc keep-result=no;
:delay 15s;
:log info "Backup of R1  is transfered to R2";

#R1 Reset R2 and start ha.rsc after reset
/system ssh 192.168.123.3 command="system reset-configuration keep-users=yes
no-defaults=yes run-after-reset=/flash/ha.rsc„
```

- keep-users=yes запазва потребителите и SSH ключовете.
- Скрипта се стартира периодично в system scheduler.

# Резервираност HA

## Скрипт

**HA script**

```
:local r1file "flash/r1.rsc";
:local r2file "flash/r2-ha.rsc";
:delay 15s;

# import of R1 configuration
:log info "BEGIN IMPORT file=$r1file";
:import $r1file;
:log info "END IMPORT file=$r1file";
:delay 15s;

#set R2 configuration for HA
:log info "BEGIN IMPORT file=$r1file";
:import $r2file;
:log info "END IMPORT file=$r1file";
```

# Резервираност HA

## Скрипт

**R2 r2-ha.rsc script**

```
#Setting R2 HA
#Set bridge1 R2 IP address

/ip address set [/ip address find interface=bridge1] address=192.168.123.3/24;
#/ip address set [/ip address find address=192.168.123.2] address=192.168.123.3/24

#Set R2 system identity
/system identity set name="MikroTik R2";

#Set R2 VRRP priority

/tool netwatch enable [find comment="R2-ISP-link-check"];
/tool netwatch disable [find comment="R1-ISP-link-check"];

#Disable Scheduling of transfer.rsc script from R1
/system scheduler disable schedule-ha;
```

# Проверка за ISP свързаност

Скрипт за проверка на свързаност
Други варианти

05

# Проблеми при отпадане на ISP свързаност

**Проблеми с отпадането на свързността на IPS доставчик.**

- При настройване на VRRP **само на LAN интерфейсите**, при отпадане на ISP1 доставчика на R1, VRRP  няма да пренасочи трафика автоматично през R2 като направи неговият LAN интерфейс master.

- Използване на рекурсивна маршрутизация – само при цялостният вариант;

- Netwatch скрипт

# Проблеми при отпадане на ISP свързаност

Решение:

- Netwatch скрипт за промяна на VRRP Priority от master в slave и обратно чрез наблюдение на

отдалечен IP адрес (1.1.1.1 или 8.8.8.8).

# Netwatch
# Скрипт

3а R1 vrrp-office master

```
/tool netwatch
add down-script="/interface vrrp set [find name=vrrp-office]
priority=80" host=\
    1.1.1.1 interval=3s timeout=800ms up-script=\
    "/interface vrrp set [find name=vrrp-office] priority=160"
```

# Netwatch
# Скрипт

3a R2 vrrp-office backup

```
/tool netwatch
add down-script="/interface vrrp set [find name=vrrp-office]
priority=90" host=\
    1.1.1.1 interval=3s timeout=800ms up-script=\
    "/interface vrrp set [find name=vrrp-office] priority=150"
```

# Проверка за ISP свързаност

## Рекурсивна маршрутизация

/ip route

add check-gateway=ping comment="Reqursive Gateway" distance=1 gateway=8.8.4.4 scope=10

add comment="Recursive routing" distance=1 dst-address=8.8.4.4/32  gateway=1.1.1.1 scope=30

# Проблеми на конфигурацията

06

**Security проблеми**

Проблеми с ARP

# Проблеми на конфигурацията
## Проблеми с ARP

В ROS, ако VRRP интерфейса и интерфейса, върху който е VRRP е настроен са в една мрежа /24, то VRRP интерфейса и интерфейса, на който VRRP е master, имат един и същ MAC адрес в ARP таблицата.

Това води до проблеми с Reverse Path Filtering при NVR, Linux NAS, TrueNAS, APC UPS карти за управление и други устройства, които следят за конфликт на IP адреси в мрежовия сегмент, в който работят, тъй като за тях това наподобява Man in the middle атака.

# Проблеми на конфигурацията
## Проблеми с ARP

При използването на VRRP с Reverse Path Filtering, се препоръчва  rp-filter да се избере loose или no. В противен случай, VRRP интерфейса може да е недостъпен.

/ip settings set rp-filter=loose

или

/ip settings set rp-filter=no

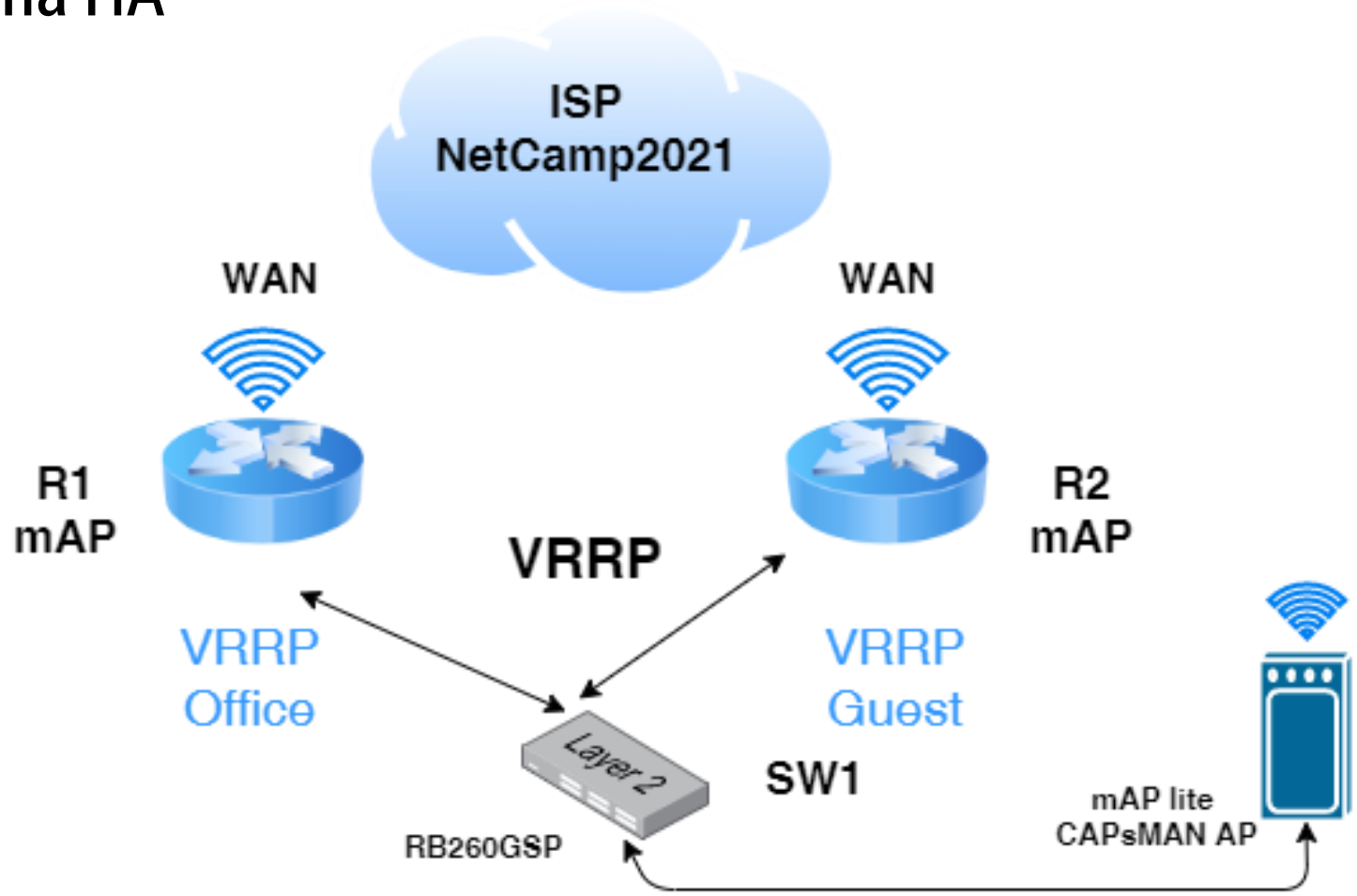
## Демонстрация на HA

# ДЕМОНСТРАЦИЯ

https://www.youtube.com/watch?v=T96XVXwHzYA&list=RDMMT96XVXwHzYA&start_radio=1

# MIKROTIK VRRP

## Демонстрация на HA



# MIKROTIK VRRP

## Демонстрация на HA

- За да стартирате ръчно процеса на синхронизация на R2 с R1, влезте в R1 с потребителя собственик на скрипта и на който сте добавили SSH ключов ете и стартирайте ръчно скрипта transfer в R1.

- Ако нещо се обърка в процеса на синхронизация на R1 с R2, поставете следните файлове в R2 в папка /flash r1.rsc(ескпорт на конфигурацията на R1), ha.rsc, r2-ha.rc и стартирайте в R2 в command line следната команда:

/system reset-configuration keep-users=yes no-defaults=yes run-after-reset=flash/ha.rsc

- ROS v7.1.rc2 при експорта на конфигурацията на R1, за да се експортват паролите на профилите в CAPsMAN Security Cfg и Wireless Security profiles, трябва да използваме командата:

/export file-name=r1.rsc show-sensitive

# ВЪПРОСИ

# Благодаря за вниманието!