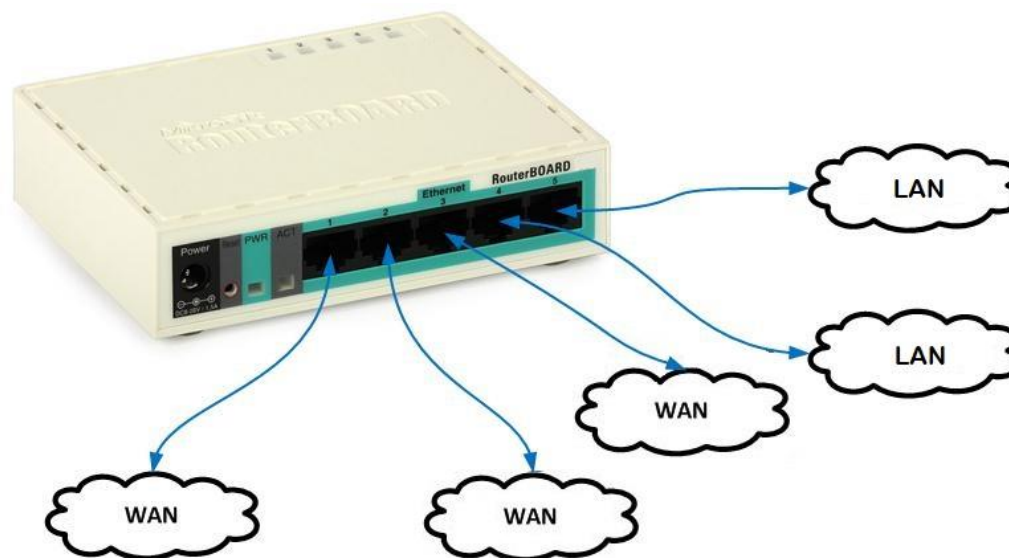


Несколько каналов WAN с резервированием и распределением на основе Mikrotik



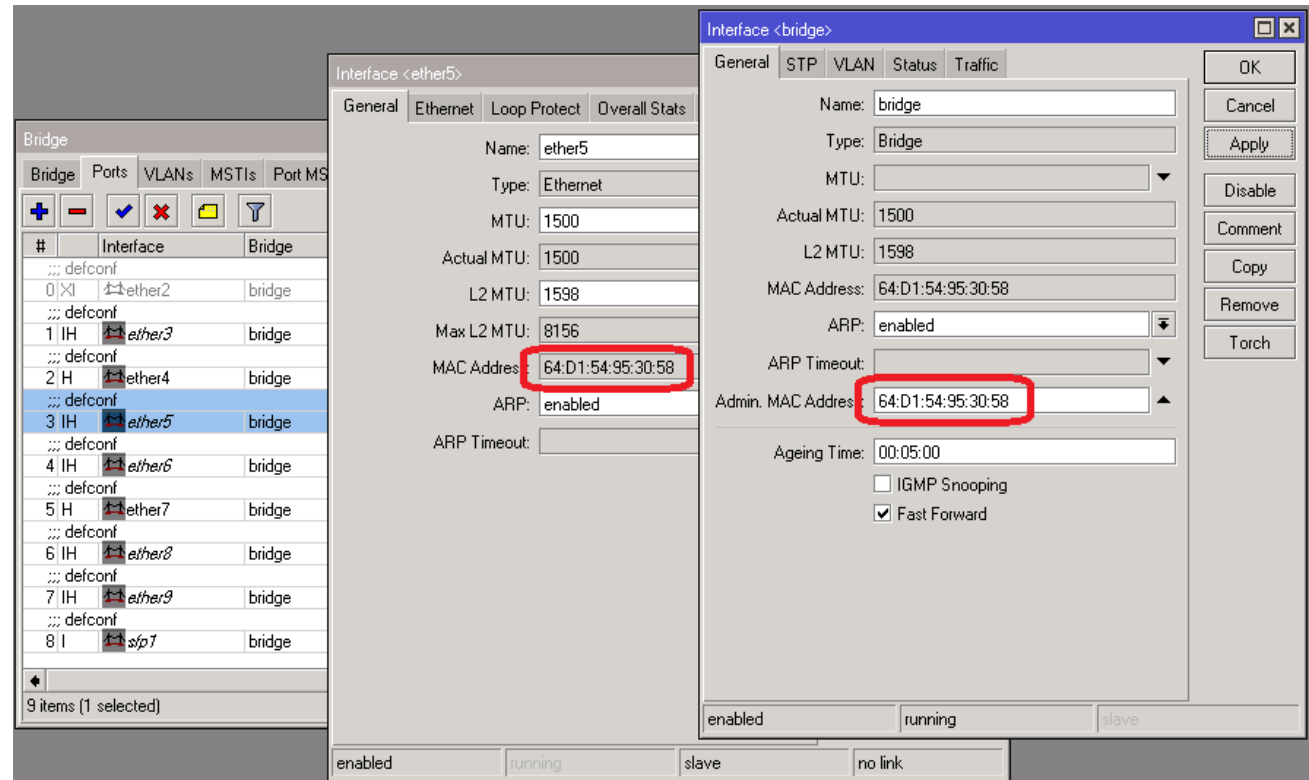
Постановка задачи

- Настроить доступ к сети интернет через несколько физически разделенных по интерфейсам каналов
- Реализовать маркировку пакетов для распределения трафика
- Обеспечить корректную работу dst-nat для всех ISP
- Настроить механизм контроля доступности и работоспособности канала с автоматическим резервированием
- Обеспечить гибкость работы системы для динамических IP адресов на WAN интерфейсах

Простейшая схема работы нескольких WAN

- ether1 – основной канал (статический IP)
- ether2 – резервный канал (динамический IP)

Не забываем
исключить
ether2 из
bridge



Устанавливаем настройки ISP1, ISP2 через GUI

The screenshot displays three windows from the Mikrotik WinBox GUI:

- Address List:** Shows a table of IP addresses and their associated interfaces.
- DHCP Client:** Shows the configuration for the DHCP client on the ether2-wan2 interface, with the default gateway set to 4.
- Route List:** Shows the routing table with a default route for MainChannel.

| Address | Network | Interface |
|--------------------|----------------|-------------|
| 37.57.71.0/24 | 37.57.71.0 | ether1-wan1 |
| 82.117.249.0/25 | 82.117.249.128 | ether2-wan2 |
| ::: defconf | | |
| 192.168.249.254/24 | 192.168.249.0 | bridge |

| Interface | Use P... | Add D... | Default | IP Address | Expires After | Status |
|-------------|----------|----------|---------|----------------|---------------|--------|
| ether2-wan2 | yes | yes | 4 | 2.117.249.1... | 05:50:18 | bound |

| Dest. Address | Gateway | Distance | Routing Mark | Pref. Source |
|----------------------|------------------------------------|----------|--------------|----------------|
| ::: MainChannel | | | | |
| AS 0.0.0.0/0 | 37.57.71.254 reachable ether1-wan1 | 3 | | |
| DS 0.0.0.0/0 | 82.117.249.129 unreachable | 4 | | |
| DAC 37.57.71.0/24 | ether1-wan1 reachable | 0 | | 37.57.71.0 |
| DAC 82.117.249.12... | ether2-wan2 reachable | 0 | | 82.117.249.128 |
| DAC 192.168.249.0... | bridge reachable | 0 | | 192.168.249.0 |

Или прописываем настройки ISP1, ISP2 из консоли

```
/ip address add address=37.57.71.XXX/24 interface=ether1-wan1  
/ip route add dst-address=0.0.0.0/0 gateway=37.57.71.254  
distance=3 comment="MainChannel"  
/ip dhcp-client add interface=ether2-wan2 default-route-  
distance=4 disabled=no
```

Настраиваем блокирующие правила для **ether2** по аналогии заводских у **ether1**

```
/ip list member add interface=ether2-wan2 list=WAN
```

Выключаем правило fasttrack connection

| # | Action | Chain | Src. Address | Protocol | Dst. Port | In. Interface | Out. Int... | Connection State | Connection NAT... | Packets |
|--|----------|---------|--------------|----------|-----------|---------------|-------------|-----------------------|-------------------|---------|
| ::: special dummy rule to show fasttrack counters | | | | | | | | | | |
| 0 | D | pas... | forward | | | | | | | 0 |
| ::: defconf: accept established,related,untracked | | | | | | | | | | |
| 1 | ✓ acc... | input | | | | | | established relate... | | 1 080 |
| ::: defconf: drop invalid | | | | | | | | | | |
| 2 | ✗ drop | input | | | | | | invalid | | 300 |
| ::: defconf: accept ICMP | | | | | | | | | | |
| 3 | ✓ acc... | input | | 1 (icmp) | | | | | | 1 |
| ::: defconf: accept ICMP | | | | | | | | | | |
| 4 | ✓ acc... | input | | 6 (tcp) | 8291 | | | | | 4 |
| ::: defconf: drop all not coming from LAN | | | | | | | | | | |
| 5 | ✗ drop | input | | | | | | | | 3 380 |
| ::: defconf: accept in ipsec policy | | | | | | | | | | |
| 6 | ✓ acc... | forward | | | | | | | | 0 |
| ::: defconf: accept out ipsec policy | | | | | | | | | | |
| 7 | ✓ acc... | forward | | | | | | | | 0 |
| ::: defconf: fasttrack | | | | | | | | | | |
| 8 | X | fast... | forward | | | | | established related | | 0 |
| ::: defconf: accept established,related, untracked | | | | | | | | | | |
| 9 | ✓ acc... | forward | | | | | | established relate... | | 0 |
| ::: defconf: drop invalid | | | | | | | | | | |
| 10 | ✗ drop | forward | | | | | | invalid | | 0 |
| ::: defconf: drop all from WAN not DSTNATed | | | | | | | | | | |
| 11 | ✗ drop | forward | | | | | | new | dstnat | 0 |

12 items (1 selected)

Задействуем несколько каналов WAN

Выделяем трафик, который должен ходить через WAN2, в примере используется отбор по src-address, на практике же может быть любой другой критерий:

```
/ip firewall mangle add chain=prerouting src-address=192.168.249.10 connection-nat-state=!dstnat action=mark-routing new-routing-mark=by_wan2 comment="SecondChannel"
```

Далее необходимо создать route для пакетов помеченных «by_wan2», но так как на интерфейсе ether2 IP и Gateway динамические, значит и правило должно быть динамически обновляющимся. Реализуем это при помощи dhcp-client Script

https://wiki.mikrotik.com/wiki/Manual:IP/DHCP_Client#Lease_script_example

Скрипт DHCP client интерфейса ether2

DHCP Client <ether2-wan2>

DHCP Options: hostname
clientid

Default Route Distance: 4

Script:

```
{
:local mark "by_wan2"
:local count [/ip route print count-only where comment="WAN2"]
if ($bound=1) do={
  if ($count = 0) do={
    /ip route add gateway="$gateway-address" comment="WAN2" routing-mark=$mark
  } else={
    if ($count = 1) do={
      :local test [/ip route find where comment="WAN2"]
      if ([/ip route get $test gateway] != "$gateway-address") do={
        /ip route set $test gateway="$gateway-address"
      }
    } else={
      :error "Multiple routes found"
    }
  }
} else={
  /ip route remove [find comment="WAN2"]
}
}
```

enabled Status: bound

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Release
Renew

Настроим DST-NAT для всех интерфейсов

- Для локальных интерфейсов:

```
/ip firewall nat add chain=srcnat src-address=192.168.249.0/24 dst-address=192.168.249.0/24 action=masquerade
```

- Для ether1 интерфейса:

```
/ip firewall nat add chain=dstnat dst-address=37.57.71.XXX protocol=tcp dst-port=22777 comment="SSH to Server WAN1" action=dst-nat to-addresses=192.168.249.10 to-ports=22
```

- Для ether2 интерфейса:

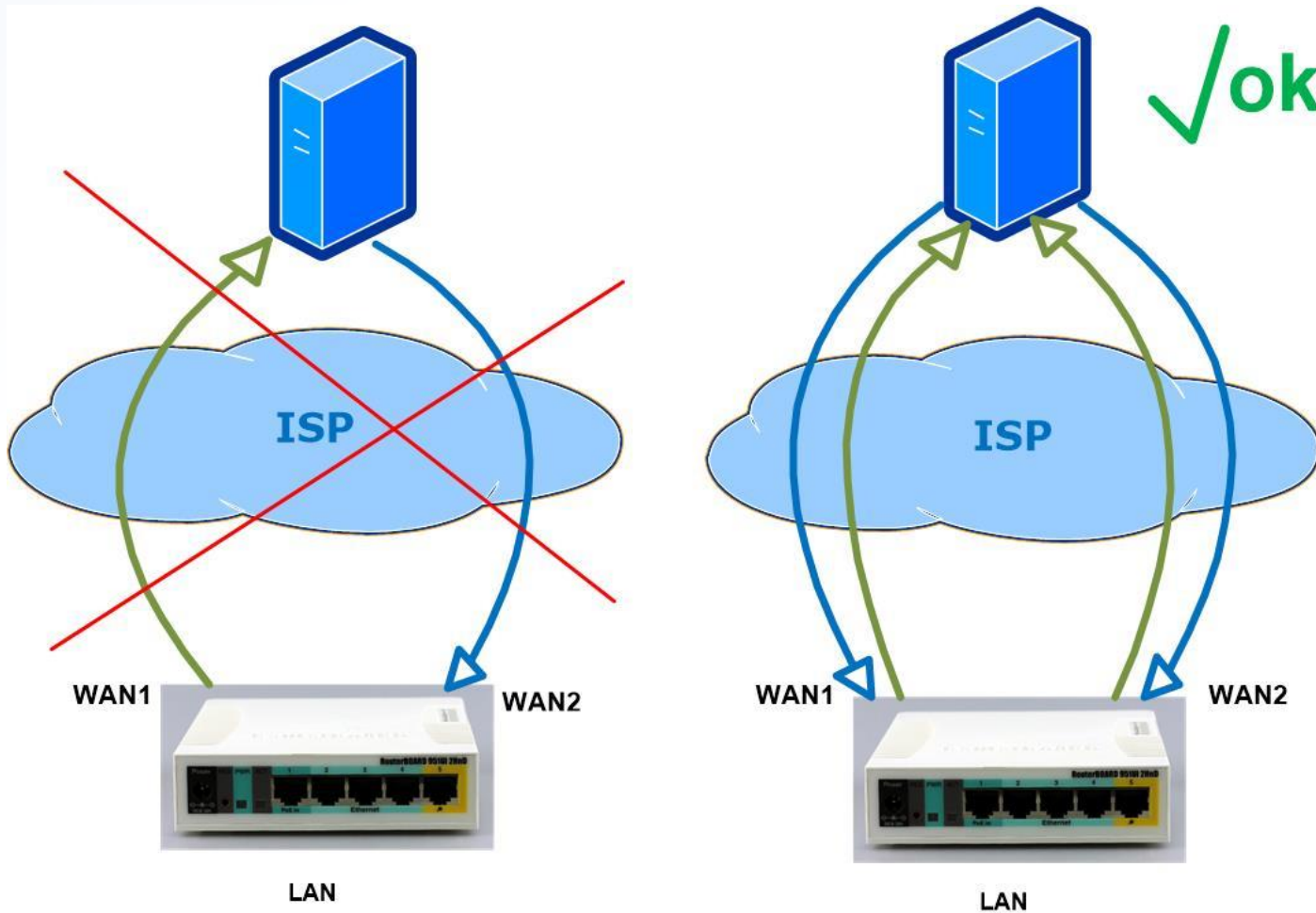
```
/ip firewall nat add chain=dstnat dst-address=1.1.1.1 protocol=tcp dst-port=22777 comment="SSH to Server WAN2" action=dst-nat to-addresses=192.168.249.10 to-ports=22
```

Ip 1.1.1.1 вставлен не ошибочно и не CopyPast'ом. Он будет автоматически заменен на правильный, модифицированным dhcp-client скриптом

Модифицированный скрипт DHCP-client для ether2

```
{ :local rmark "by_wan2"
:local count [/ip route print count-only where comment~"WAN2"]
:if ($bound=1) do={
  :if ($count = 0) do={
    /ip route add gateway="$gateway-address" comment="WAN2" routing-mark=$rmark
    /ip route add dst-address=8.8.4.4 gateway="$gateway-address" comment="test_WAN2"
    :local dstnatcheck [/ip firewall nat find where comment~"WAN2"]
    /ip firewall nat set $dstnatcheck dst-address="$lease-address"
    :log warning ("New WAN2 IP= ".$lease-address")
  } else={
    :if ($count = 2) do={
      :local test [/ip route find where comment~"WAN2"]
      :if ([/ip route get $test gateway] != "$gateway-address") do={
        /ip route set $test gateway="$gateway-address"
        :local dstnatcheck [/ip firewall nat find where comment~"WAN2"]
        /ip firewall nat set $dstnatcheck dst-address="$lease-address"
        :log warning ("New WAN2 IP= ".$lease-address")
      }
    } else={
      :log error ("Multiple routes found") }
    }
  } else={
    /ip route remove [find comment~"WAN2"] } }
```

Зачем нужна маркировка пакетов



Маркировка пакетов для dst-nat

```
/ip firewall mangle add chain=forward in-interface=ether1-wan1 action=mark-connection new-connection-mark=by_wan1
```

```
/ip firewall mangle add chain=forward in-interface=ether2-wan2 action=mark-connection new-connection-mark=by_wan2
```

```
/ip firewall mangle add chain=prerouting src-address=192.168.249.0/24 connection-mark=by_wan1 action=mark-routing new-routing-mark=by_wan1
```

```
/ip firewall mangle add chain=prerouting src-address=192.168.249.0/24 connection-mark=by_wan2 action=mark-routing new-routing-mark=by_wan2
```

ip route для пакетов с маркированным маршрутом **by_wan2** создается автоматически dhcpc-client скриптом, а вот для пакетов **by_wan1** не забываем создать маршрут самостоятельно:

```
/ip route add dst-address=0.0.0.0/0 gateway=37.57.71.254 routing-mark=by_wan1 comment=WAN1
```

Маркировка пакетов для input connections

```
/ip firewall mangle add chain=input in-interface=ether1-wan1  
action=mark-connection new-connection-mark=mkt_wan1
```

```
/ip firewall mangle add chain=input in-interface=ether2-wan2  
action=mark-connection new-connection-mark=mkt_wan2
```

```
/ip firewall mangle add chain=output connection-mark=mkt_wan1  
action=mark-routing new-routing-mark=by_wan1
```

```
/ip firewall mangle add chain=output connection-mark=mkt_wan2  
action=mark-routing new-routing-mark=by_wan2
```

Пропишем статический route на 8.8.8.8 для контроля WAN1

```
/ip route add dst-address=8.8.8.8 gateway=37.57.71.254  
comment=test_WAN1
```

Контроль работоспособности WAN1 и WAN2

```
/tool netwatch add host=8.8.8.8 up-script="/ip route set distance=3  
[find comment=\"MainChannel\"]" down-script="/ip route set  
distance=7 [find comment=\"MainChannel\"]"
```

```
/tool netwatch add host=8.8.4.4 up-script="/ip firewall mangle set  
disable=no [find comment=\"SecondChannel\"]" down-script="/ip  
firewall mangle set disable=yes [find comment=\"SecondCha  
nnel\"]"
```

```
/ip firewall filter add chain=output out-interface=ether1-wan1  
dst-address=8.8.4.4 action=drop
```