Documentação rede inventário

Davi Bezerra

November 2025

1 Inicío

Este laboratório é uma prática simplificada de um ambiente de redes com virtual box. O intuito é implementar a configuração de Failover de links WAN utilizando Netwatch.

Links de referência:

1. https://mkcontroller.com/mikrotik-failover-complete-guide-for-high-availability-and-business-continuity/
2. https://ravel.com.br/blog/mikrotik-configuracao-de-failover-via-netwatch/

Equipamentos iniciais:

1. RouterOS versão Cloud Hosted Router VDI Image
2. Duas interfaces NAT
3. Duas interfaces Host-Only

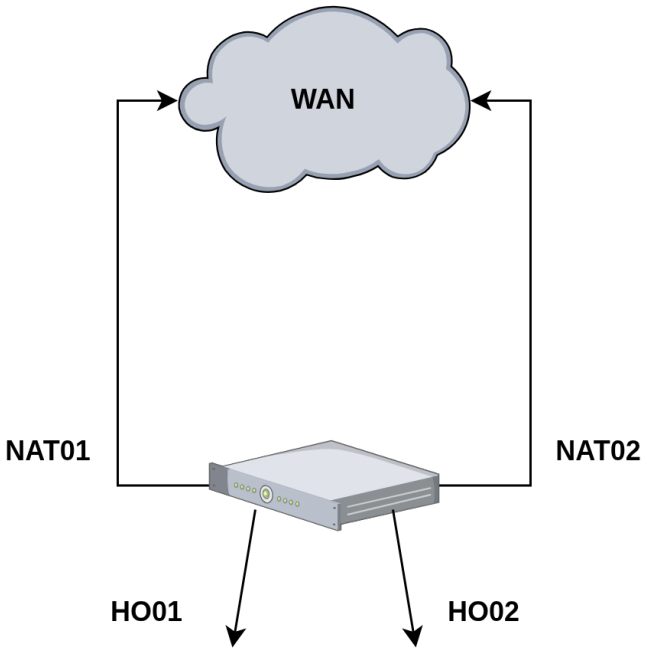

Figure 1: Cenário simplificado

1.1 Configuração inicial

Resumidamente, temos que ativar primeiro as interfaces no virtual box. Em ferramentas, criamos duas interfaces Host-only (não serão utilizadas no projeto, apenas para manter no MikroTik para uso posterior) e inserimos 4 interfaces na VM.

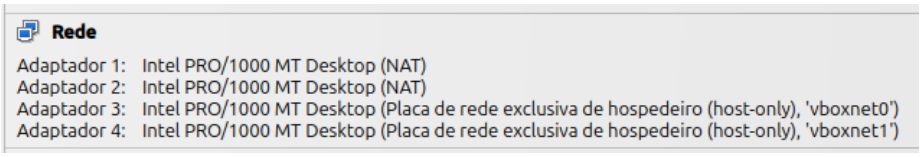

Figure 2: Interfaces virtualbox

No MikroTik, podemos ver a lista de interfaces com o comando `interface print`, que vai gerar a lista

```
[admin@MikroTik] > interface print
Flags: R - RUNNING
Columns: NAME, TYPE, ACTUAL-MTU, MAC-ADDRESS
#   NAME    TYPE      ACTUAL-MTU  MAC-ADDRESS
0 R ether4  ether           1500  08:00:27:EA:82:B1
```

```
1 R ether5  ether           1500  08:00:27:74:9A:C5
2 R ether6  ether           1500  08:00:27:E6:22:04
3 R ether7  ether           1500  08:00:27:C6:C9:21
4 R lo      loopback       65536  00:00:00:00:00:00
```

As duas primeiras interfaces são as interfaces NAT. Em seguida, ativamos o DHCP das interfaces NAT com os comandos:

```
ip dhcp-client add interface=ether4 disabled=no
ip dhcp-client add interface=ether5 disabled=no
```

(OPCIONAL)
Ativamos agora endereços estáticos para as interfaces Host-only:

```
ip address add address=192.168.56.5/24 interface=ether6
ip address add address=192.168.57.5/24 interface=ether7
```

Para ver as interfaces e IPs registrados, usamos o comando `ip address print`:

```
[admin@MikroTik] > ip address print
Flags: I - INVALID; D - DYNAMIC
Columns: ADDRESS, NETWORK, INTERFACE
#    ADDRESS            NETWORK       INTERFACE
0 I  192.168.56.10/24   192.168.56.0  *3
1    192.168.56.5/24    192.168.56.0  ether6
2    192.168.57.5/24    192.168.57.0  ether7
3  D 10.0.3.15/24       10.0.3.0      ether5
4  D 10.0.2.15/24       10.0.2.0      ether4
```

1.2 Criação de rotas WAN

Na interface web do MikroTik, acessamos a aba IP - DHCP Client e desativamos as opções ativas. O MikroTik não tem mais acesso a internet nesse momento. Em rotas, temos que definir agora a principal e a secundária. Em IP - Rotas, clicamos em Novo e inserimos essas informações:

Definimos e comentamos a rota principal, que estará ativa na maior parte do tempo, e a rota secundária, que assume quando a principal cai.

1.3 Monitoramento e Failover

Para criar o failover, temos que habilitar o monitoramento com Netwatch. Primeiro, criamos uma rota de monitoramento WAN que usa o mesmo gateway da rota principal. Usamos o endereço IP de um servidor raiz da internet (192.5.5.241).

Essa rota será usada pelo netwatch para verificar a integridade do gateway. Em Tools - Netwatch, criamos essa configuração:

Basicamente, o netwatch realiza a ação de verificar a cada 30 segundos se há alcance para esse IP de destino através da rota definida. Se não houver, ele

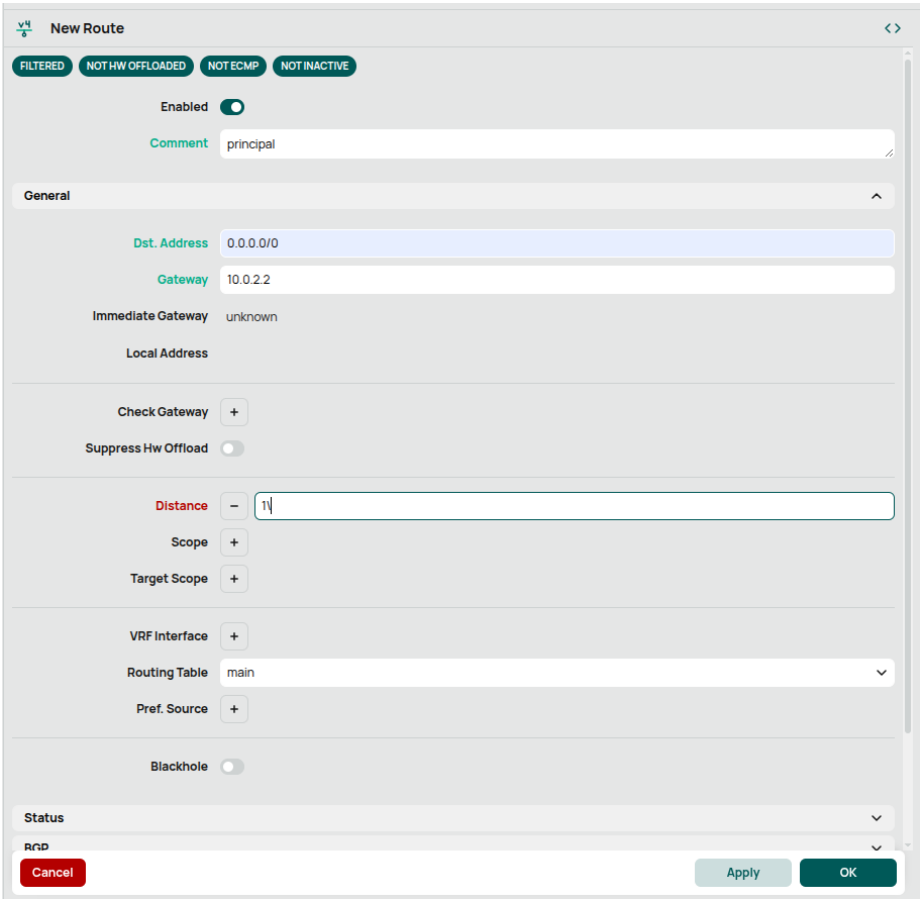

Figure 3: Rota principal

desativa o gateway principal. O ato de desativar o gateway automaticamente repassa o tráfego para o secundário, pois a distancia está definida como 1 para o principal e 2 para o secundário.

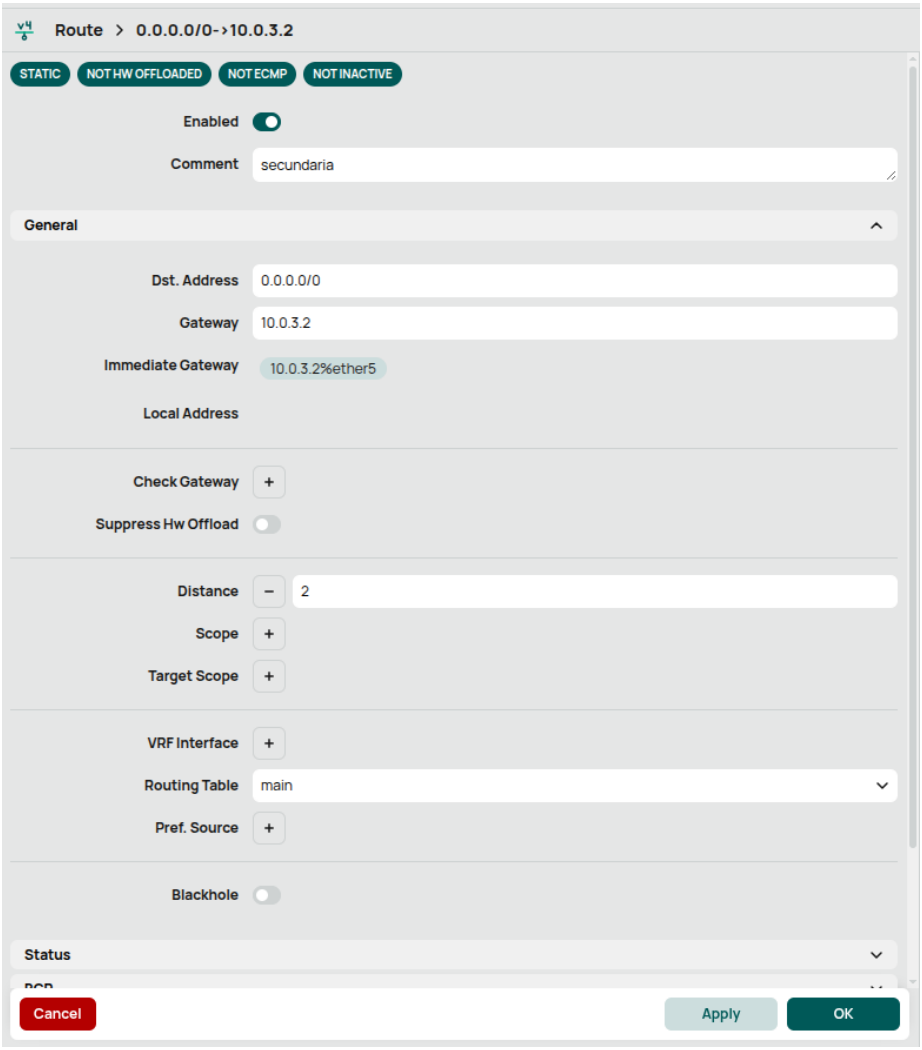

Figure 4: Rota secundária

1.4 Teste de conectividade

Por terminal, podemos dar um ping para a internet pública com o comando ping 8.8.8.8:

Para fazer o teste de failover, deixamos o ping sem parar e no virtual box, na configuração de interface do gateway, habilitamos a opção cabo desconectado:

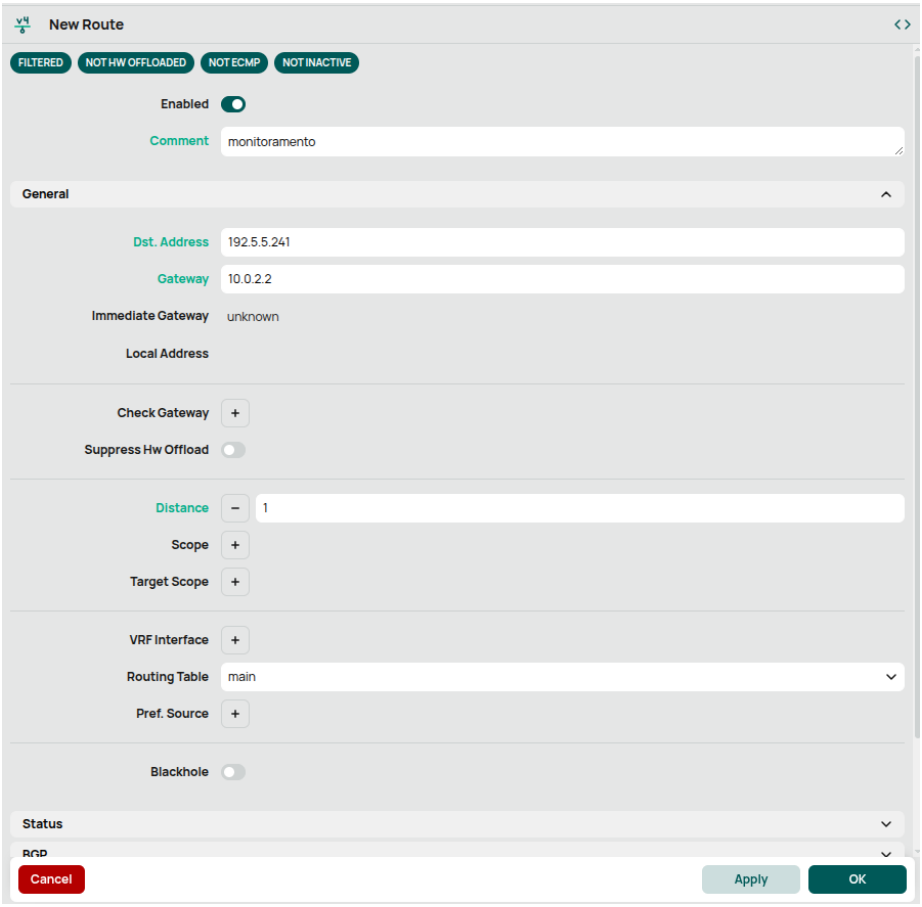

Figure 5: Rota de monitoramento

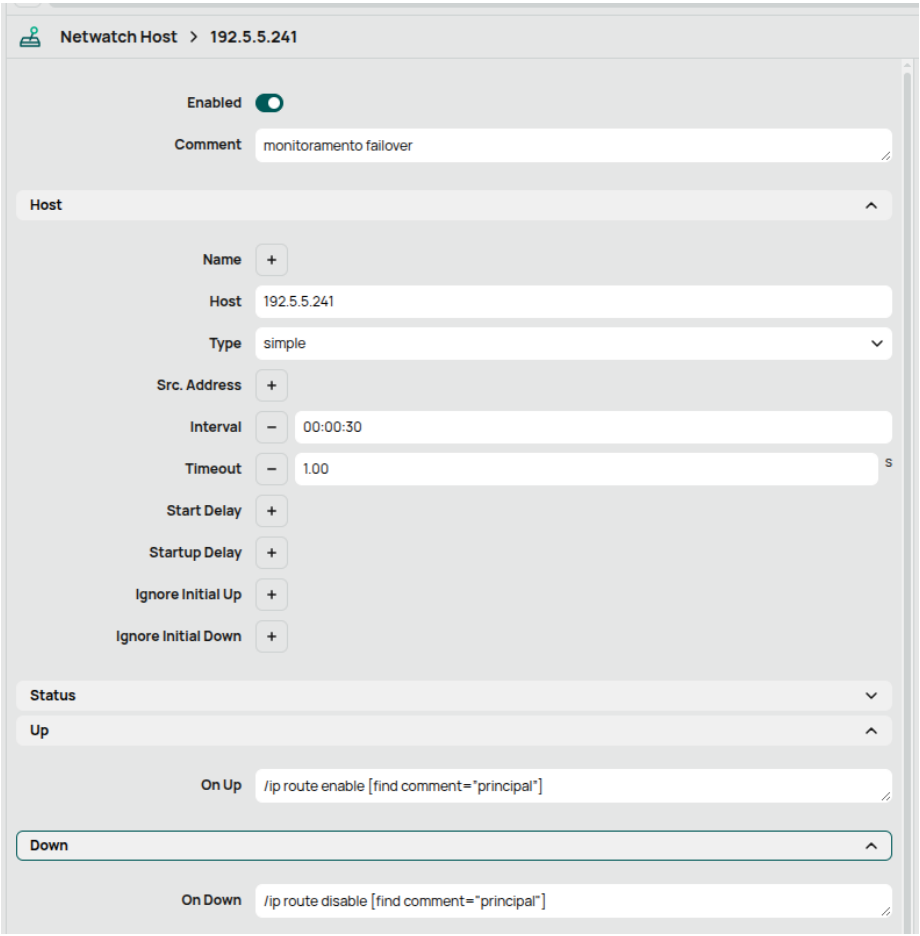

Figure 6: Monitoramento com Netwatch

```
[admin@MikroTik] > ping 8.8.8.8
  SEQ HOST                                     SIZE TTL TIME       STATUS
    0 8.8.8.8                                    56 254 42ms175us
    1 8.8.8.8                                    56 254 40ms521us
    2 8.8.8.8                                    56 254 41ms878us
    3 8.8.8.8                                    56 254 42ms71us
    4 8.8.8.8                                    56 254 40ms300us
    5 8.8.8.8                                    56 254 42ms435us
    6 8.8.8.8                                    56 254 44ms289us
    7 8.8.8.8                                    56 254 42ms771us
    8 8.8.8.8                                    56 254 40ms800us
    9 8.8.8.8                                    56 254 41ms723us
   10 8.8.8.8                                    56 254 46ms204us
```

Figure 7: Ping inicial

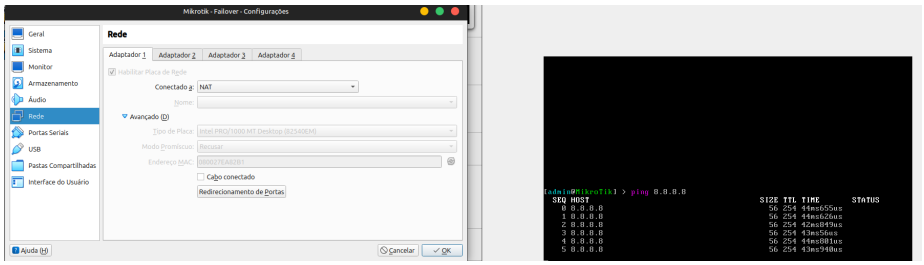

Figure 8: Cabo desconectado

Ao desconectar o cabo, vemos que em um dos pings recebemos timeout, mas logo em seguida o acesso ao ip é reestabelecido, mostrando que o monitoramento e ativação da rota secundária funciona:

```
48 8.8.8.8                                56 254 42ms451us
49 8.8.8.8                                56 254 42ms813us
50 8.8.8.8                                56 254 42ms46us
51 8.8.8.8                                                timeout
52 8.8.8.8                                56 254 42ms630us
53 8.8.8.8                                56 254 42ms783us
54 8.8.8.8                                56 254 43ms758us
55 8.8.8.8                                56 254 42ms407us
56 8.8.8.8                                56 254 43ms966us
 sent=57 received=56 packet-loss=1% min-rtt=40ms589us avg-rtt=43ms247us
max-rtt=69ms709us
```

Figure 9: Reconexão