protectiONE Data Retention Overview

protectiONE DR system collect and store IPv4 and IPv6 network flows data in two ways:

realtime:

- DR system includes one or more probes connected to LAN and WAN mirrored ports of device performing NAT
- flows are assembled in realtime from mirrored data
- each probe can process one NAT device
- traffic is monitored for DoS, DDoS and port scanning attacks and detection events can be passed to external device for attack mitigation

passive:

- DR system supports NetFlow and IPFIX flow data collection and storing
- multiple NAT devices can be configured to send flow data to DR system
- because of offline nature of NetFlow or IPFIX protocols, where flow data are sent in five minute batches, no attack detection is performed
- for NetFlow protocol v9 is required because of NAT source address and port fields

system configuration

DR system has two 1GbE network interfaces which are used as service ports and two 10GbE or 40GbE or 100GbE network interfaces per each realtime probe. A basic DR system consists of:

eth0:

- service port with firewall for web interface access, API access and flow data collection
- static IP address and gateway (default 192.168.0.123/24, gw 192.168.0.1)
- default firewall setting is allow web, API and flow data access from 192.168.0.0/16, 172.16.0.0/12, 100.64.0.0/10 and 10.0.0.0/8
- 1GbE RJ45

eth1:

- service port without firewall only used for primary configuration
- DHCP
- 1GbE RJ45

lan1, wan1:

- ports with mirrored traffic from device performing NAT
- 10GbE SFP+ or 40GbE QSFP+ or 100GbE QSFP28

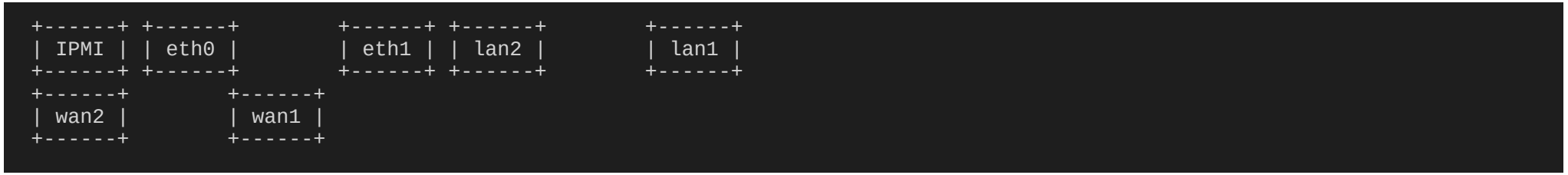
network setup

For initial configuration you can use eth1 port with DHCP or eth0 port with default IPv4 and gateway. eth1 with DHCP is recommended, because when you will change eth0 IPv4 address to desired one, device will disconnect and reconnection to new IPv4 address will be required.

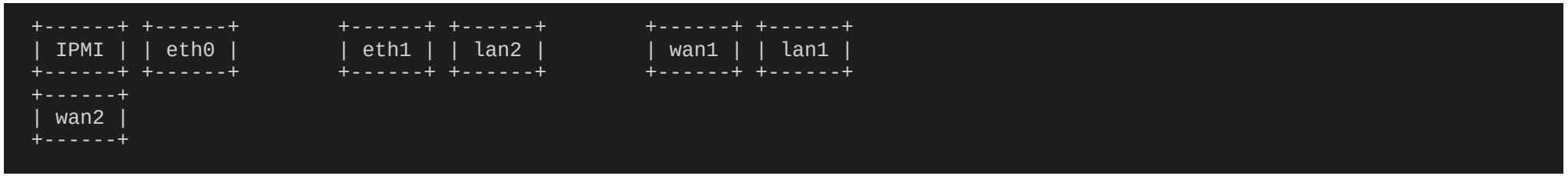
backpanel diagram

Supermicro 1U:

ASRock 2U:



ASRock 1U:



perform these steps

1. connect eth1 port to broadcast domain with DHCP server (or if you are using eth0 connect it to notebook/PC with IPv4 address set from 192.168.0.0/24)

2. find IPv4 assigned to DR system in web interface of this DHCP server (or use CLI interface or whatever way to obtain this information DHCP server supports)

3. open web interface of DR system in your preferred web browser (replace with assigned one or with 192.168.0.123 if you are using eth0):

   https://

4. on login dialog enter default user "admin" and default password "flowd"

5. go to menu Settings/Firewall and modify sets "webadmin", "apiadmin", "netflowclients" as you need

   - "webadmin" - IPv4 addresses or subnets with access to web interface
   - "apiadmin" - IPv4 addresses or subnets with access to API

- "netflowclients" - IPv4 addresses or subnets with access to UDP ports of NetFlow, sFlow and IPFIX (2055, 2056, 4432, 4739, 6343, 9995, 9996)

WARNING: don't forget to add IPv4 address or subnet from which you will access web interface to "webadmin" set WARNING: if you are using eth0, don't remove 192.168.0.0/16 subnet from webadmins in this step

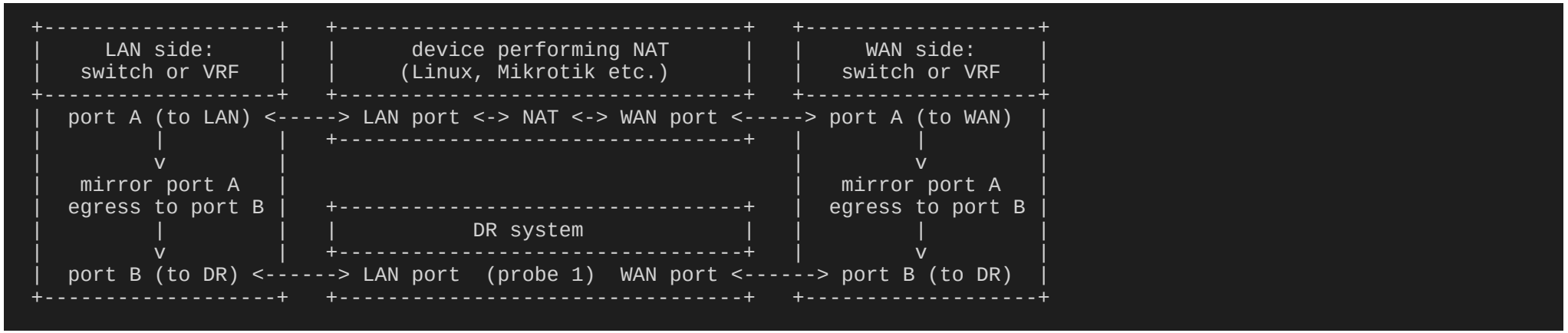
6. go to menu Settings/Interfaces and configure IPv4 address and gateway for service port eth0

7. if you were using DHCP on eth1, you can disconnect eth1, connect eth0 and access web interface on newly configured IPv4 address

mirroring probes setup

Each mirrored traffic collecting probe in DR system is connected to two 10GbE or 40GbE ports, one marked as LAN and one as WAN. These ports intercepts mirrored ingress traffic to device performing NAT. There are several topologies which can be used to configure port mirroring. Use port mirroring on switches on LAN and WAN side of NAT device (mirror only egress traffic from switch to NAT device) or use optical taps.

Port mirroring on two switches (or one switch with two VRF) on both sides of NAT device



Set port mirroring on switches on both sides (LAN and WAN) to mirror egress traffic of port connected to NAT device to port connected to DR system.

Example configuration for HP 5900 series switch:

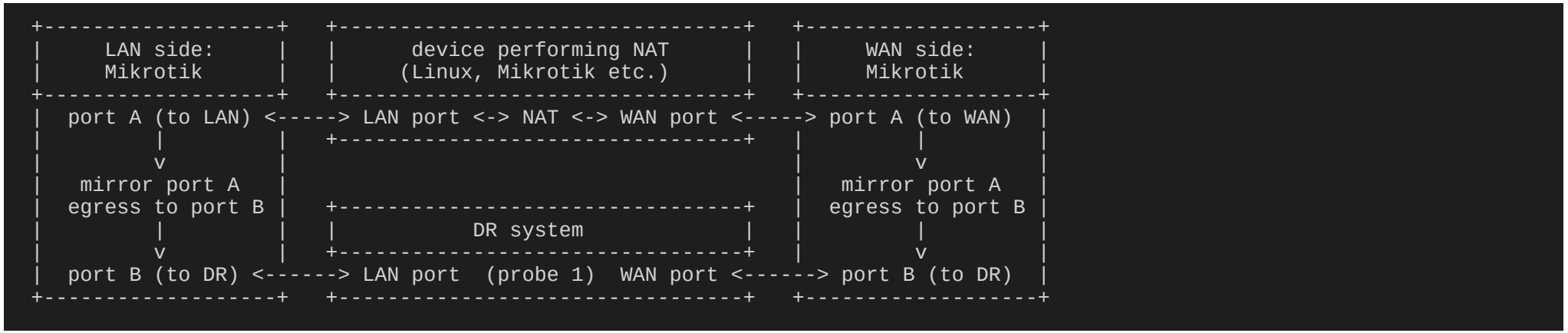
- port 1/0/1 is connected to NAT device and port 1/0/3 to DR system
- example shows only one side (either LAN or WAN), so configuration has to be done twice for both LAN and WAN

```
# Create local mirroring group 1.
<SwitchC> system-view
[SwitchC] mirroring-group 1 local
# Configure Ten-GigabitEthernet 1/0/1 as the source port of the mirroring group. Configure the mirroring group to monitor
the outgoing (egress) traffic of the port.
[SwitchC] mirroring-group 1 mirroring-port Ten-GigabitEthernet 1/0/1 outbound
# Configure Ten-GigabitEthernet 1/0/3 as the monitor port of the mirroring group.
[SwitchC] mirroring-group 1 monitor-port Ten-GigabitEthernet 1/0/3
# Disable the spanning tree feature on Ten-GigabitEthernet 1/0/3 to make sure mirroring operates correctly.
[SwitchC] interface ten-gigabitethernet 1/0/3
[SwitchC-Ten-GigabitEthernet1/0/3] undo stp enable
[SwitchC-Ten-GigabitEthernet1/0/3] quit
```

Port mirroring on two Mikrotik devices on both sides of NAT device

Egress mirroring supports following Mikrotik hardware (not full list, newer devices can support egress mirroring too):

- L009 series
- RB5009 series
- CCR2004-16G-2S+
- CRS1xx/2xx series



Most Mikrotik devices can mirror only one port (except CCR devices, which can mirror multiple ports), because mirroring is implemented in hardware switch. Please consult following:

https://help.mikrotik.com/docs/display/ROS/Switch+Chip+Features#SwitchChipFeatures-PortMirroring

https://help.mikrotik.com/docs/pages/viewpage.action?pageId=103841835

https://help.mikrotik.com/docs/display/ROS/CRS3xx%2C+CRS5xx%2C+CCR2116%2C+CCR2216+switch+chip+features#CRS3xx,CRS5xx,CCR2116,CCR2216switchchipfeatures-Mirroring

Example configuration for L009 series, RB5009 series and CCR2004-16G-2S+ Mikrotik:

- port ether1 is connected to NAT device and port ether5 to DR system
- example shows only one side (either LAN or WAN), so configuration has to be done twice for both LAN and WAN

- if there are more than one switch chip (e.g. CCR2004-16G-2S+ has two switch chips, ports ether1-ether8 and ether9-ether16), RouterOS supports one mirror per each chip, but for each mirror all source ports and target port must be on the same switch chip - mirroring between switch chips is not supported

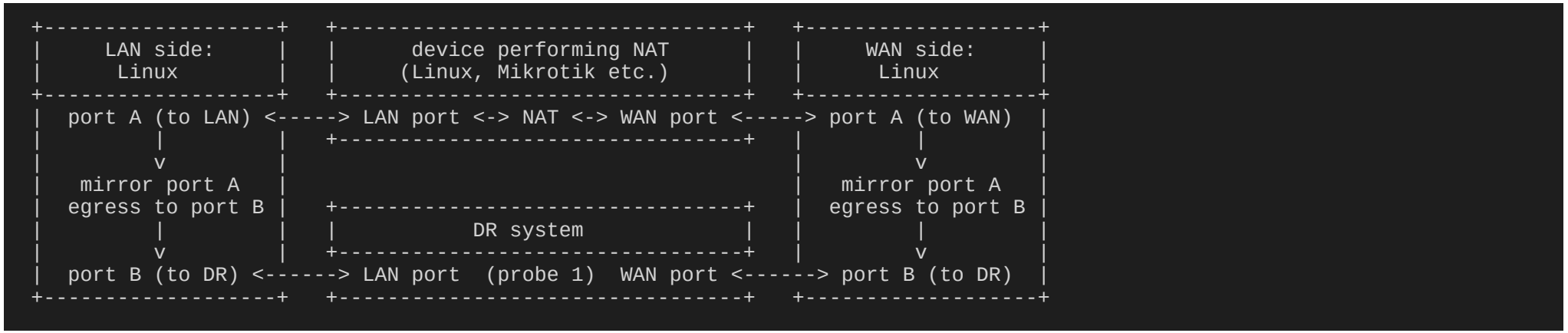
```
/interface ethernet switch
set switch1 mirror-target=ether5
/interface ethernet switch port
set ether1 mirror-egress
```

Example configuration for CRS1xx/2xx series Mikrotik:

- port ether1 is connected to NAT device and port ether5 to DR system
- example shows only one side (either LAN or WAN), so configuration has to be done twice for both LAN and WAN
- two mirroring ports are supported per switch

```
/interface ethernet switch
set switch1 egress-mirror0=ether5
/interface ethernet switch port
set ether1 egress-mirror-to=mirror0
```

Port mirroring on two Linux servers on both sides of NAT device

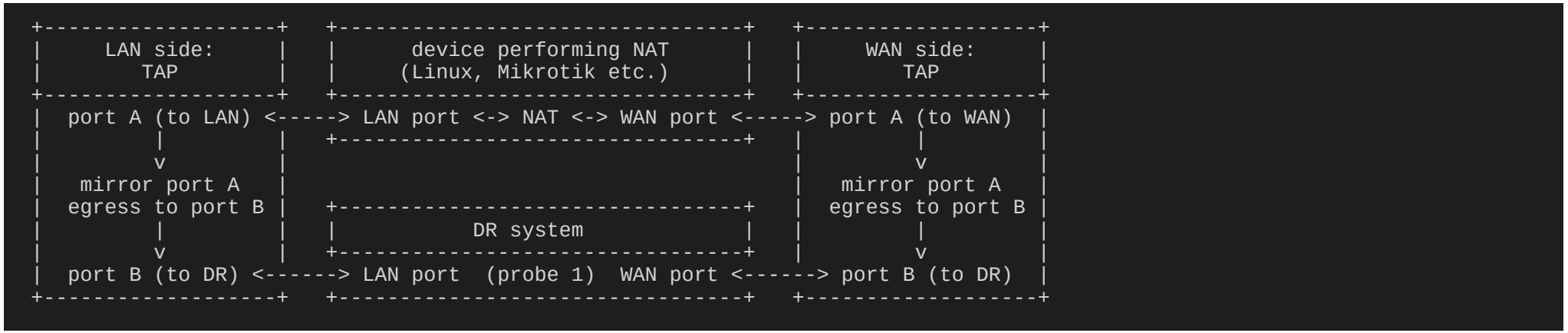


Example configuration:

- port eth1 is connected to NAT device and port eth5 to DR system
- example shows only one side (either LAN or WAN), so configuration has to be done twice for both LAN and WAN

```
tc qdisc add dev eth1 handle 1: root prio
tc filter add dev eth1 parent 1: protocol all u32 match u32 0 0 action mirred egress mirror dev eth5
```

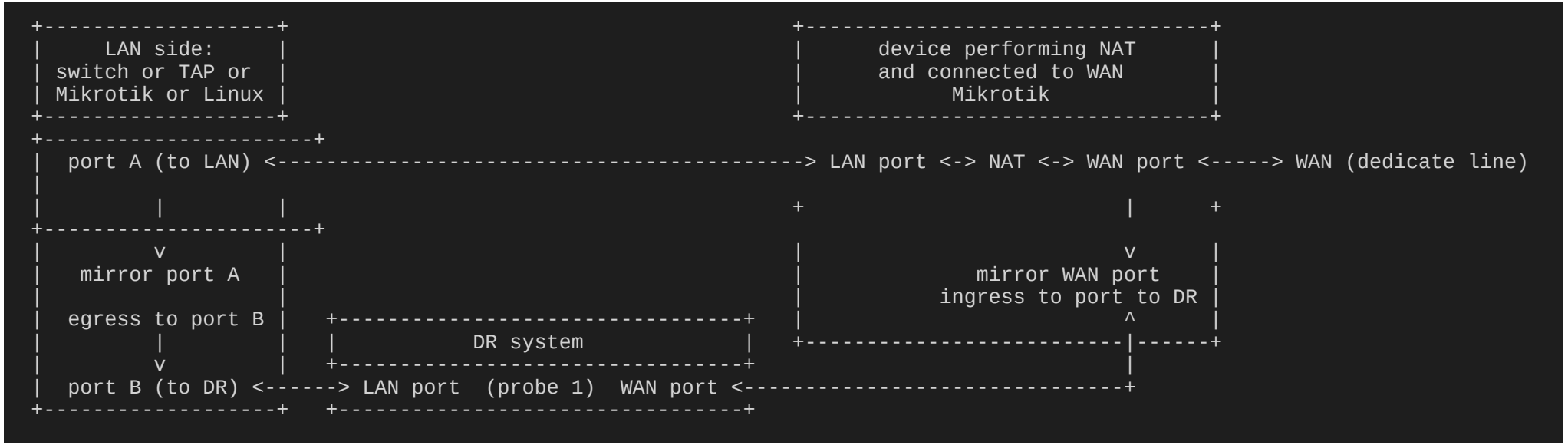
Port mirroring on two optical TAPs



Connect optical TAP so that only mirror of traffic to NAT device is connected to input SFP+ of DR system.

Port mirroring on Mikrotik device performing NAT with other device on LAN side

Only Mikrotik device mirroring WAN side is shown here. For setup with Mikrotik mirroring LAN side just switch sides.

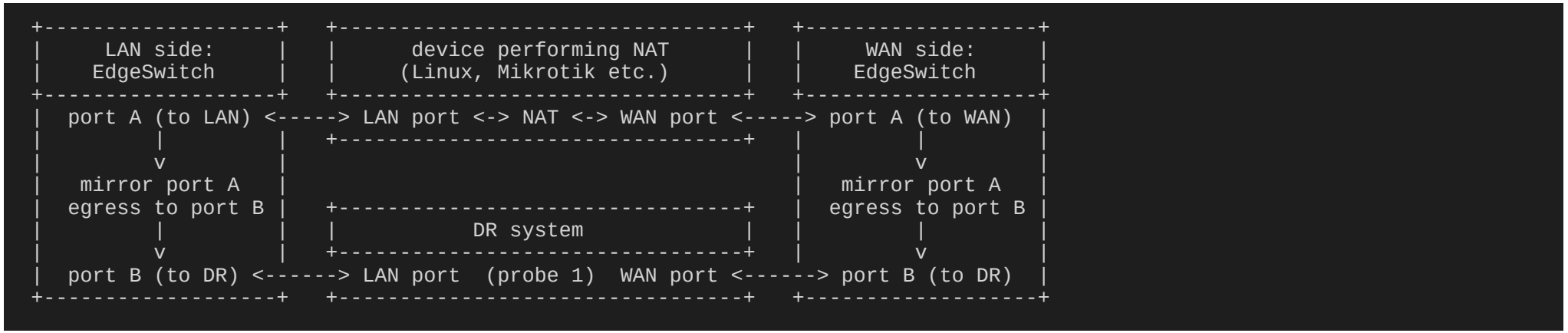


Example configuration for CCR series Mikrotik:

- port ether1 is connected to WAN dedicated line, port ether5 to DR system
- for LAN side configuration see one of previous examples for given device

```
/interface ethernet switch
set switch1 mirror-target=ether5
/interface/ethernet/switch/rule
add mirror-ports=ether1 switch=switch1
```

Port mirroring on two Ubiquiti Edge switches on both sides of NAT device



Example configuration:

- port 1 is connected to NAT device and port 5 to DR system
- example shows only one side (either LAN or WAN), so configuration has to be done twice for both LAN and WAN

In web interface:

1. go to **System > Port > Mirroring**
2. for **Destination** select port 5
3. click **Configure Source**
4. for **Type** select Interface and in **Available Source Port(s)** select port 1 with **Direction** Tx and click **Add**
5. store configuration with **System > Configuration Storage > Save**

NetFlow v9, IPFIX setup

DR system can be configured with multiple NetFlow v9 and IPFIX collectors. Each collector can listen on one of UDP ports 2055, 2056, 4432, 4739, 6343, 9995, 9996. Default settings is Netflow v9 and IPFIX collector on port **4739**.

Note: NetFlow versions older than v9 are not supported because lack of NAT fields.

Note: sFlow is not supported because it is packet sampling protocol, which means it can miss some flows and as such is inapplicable for Data Retention.

Note: Sources of NetFlow v9 or IPFIX data must be allowed in DR system firewall. Add IPv4 addresses of these sources to **netflowclients** set in menu "**Settings / Firewall**".

Mikrotik IPFIX configuration

First make sure RouterOS has correct time and NTP client set at "System/Clock" and "System/NTP Client" (for NTP servers you can use pool servers, e.g. for Czech Republic: 0.cz.pool.ntp.org, 1.cz.pool.ntp.org). Then in "IP/Traffic Flow" set following options:

General

- Enabled: [x]
- Active Flow Timeout: 5 minutes

- Inactive Flow Timeout: 15 seconds (default)

IPFIX (enable only following fields)

- Last Forwarded: [x]
- First Forwarded: [x]
- System Init Time: [x]
- Packets: [x]
- Bytes: [x]
- Src. Address: [x]
- Dst. Address: [x]
- Src. Port: [x]
- Dst. Port: [x]
- Protocol: [x]
- NAT Src. Address: [x]
- NAT Dst. Address: [x]
- NAT Src. Port: [x]
- NAT Dst. Port: [x]

Then press "Targets" button and add new target with following options:

- Enabled: [x]
- Src. Address: (IPv4 address of this Mikrotik device)
- Dst. Address: (IPv4 address of DR system)
- Port: (IPFIX port of DR system, default 4739)
- Version: IPFIX

- v9/IPFIX Template Refresh: 20 (default)
- v9/IPFIX Template Timeout: 1800 (default)

SNMP

DR system can be monitored by SNMP. Monitoring SNMP clients have to be enabled in firewall in menu "IP Services / SNMP" or by API calls for adding items in IPv4 set global/snmpclients or in IPv6 global6/snmpclients6, see WAMP API Guide.

```
SNMP connection parameters:
version: 2c
port: 161/UDP
user: flowd
community: flowd
```

Besides standard monitoring SNMP data are extended with status of database drivers, IPFIX/NetFlow collectors and flow probes. Try snmpwalk (don't forget to allow you SNMP client IPv4 address in firewall):

```
localhost ~ # snmpwalk -v 2c -c flowd <ipv4_addr_of_dr_server> NET-SNMP-EXTEND-MIB::nsExtendObjects
NET-SNMP-EXTEND-MIB::nsExtendNumEntries.0 = INTEGER: 1
NET-SNMP-EXTEND-MIB::nsExtendCommand."flowd-stats" = STRING: /etc/snmp/scripts/flowd-stats.py
NET-SNMP-EXTEND-MIB::nsExtendArgs."flowd-stats" = STRING:
NET-SNMP-EXTEND-MIB::nsExtendInput."flowd-stats" = STRING:
NET-SNMP-EXTEND-MIB::nsExtendCacheTime."flowd-stats" = INTEGER: 5
NET-SNMP-EXTEND-MIB::nsExtendExecType."flowd-stats" = INTEGER: exec(1)
NET-SNMP-EXTEND-MIB::nsExtendRunType."flowd-stats" = INTEGER: run-on-read(1)
NET-SNMP-EXTEND-MIB::nsExtendStorage."flowd-stats" = INTEGER: permanent(4)
NET-SNMP-EXTEND-MIB::nsExtendStatus."flowd-stats" = INTEGER: active(1)
NET-SNMP-EXTEND-MIB::nsExtendOutput1Line."flowd-stats" = STRING: total_database_flows:135295 total_probe_flows:107018
total_collector_flows:102589
NET-SNMP-EXTEND-MIB::nsExtendOutputFull."flowd-stats" = STRING: total_database_flows:135295 total_probe_flows:107018
total_collector_flows:102589
NET-SNMP-EXTEND-MIB::nsExtendOutNumLines."flowd-stats" = INTEGER: 1
NET-SNMP-EXTEND-MIB::nsExtendResult."flowd-stats" = INTEGER: 0
NET-SNMP-EXTEND-MIB::nsExtendOutLine."flowd-stats".1 = STRING: total_database_flows:135295 total_probe_flows:107018
total_collector_flows:102589
```