TOP10 RouterOS configuration mistakes
Presenter – Andis Arins

- MikroTik Consultant at WISP TRACON / router.lv
- MikroTik / Microsoft certified trainer
- Member of the board in Latvian Internet Association
- Review expert for EU in future networking research

andis[at]router.lv
www.linkedin.com/in/in/andisarins
The same IP on multiple interfaces
The same IP on multiple interfaces

<table>
<thead>
<tr>
<th>Address</th>
<th>Network</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.0.0.1/24</td>
<td>10.0.0.0</td>
<td>ether1</td>
</tr>
<tr>
<td>10.0.0.1/24</td>
<td>10.0.0.0</td>
<td>ether2</td>
</tr>
</tbody>
</table>
The same IP on multiple interfaces

```
[admin@MUM16TX-AA] > /ip address print
Flags: X - disabled, I - invalid, D - dynamic
  #   ADDRESS     NETWORK     INTERFACE
  0  10.0.0.1/24  10.0.0.0    ether1
  1  10.0.0.1/24  10.0.0.0    ether2
```

```
[admin@MUM16TX-AA] >
[admin@MUM16TX-AA] >
[admin@MUM16TX-AA] > /ip route print
Flags: X - disabled, A - active, D - dynamic,
C - connect, S - static, r - rip, b - bgp, o - ospf, m - mme,
B - blackhole, U - unreachable, P - prohibit
  #   DST-ADDRESS     PREF-SRC     GATEWAY     DISTANCE
  0  ADC  10.0.0.0/24  10.0.0.1     ether1     0
     10.0.0.0/24  10.0.0.1     ether2     0
```

survival strategy: MAC telnet or connection from different network
Lack of monitoring
Lack of monitoring

- What is the health of my router?
- Is it reachable from everywhere it should?
- Isn’t it overloaded?
Lack of monitoring

```
[admin@ccr1072] > /system health print

   cpu-overtemp-check: yes
   cpu-overtemp-threshold: 100C
   cpu-overtemp-startup-delay: 1m
   cpu-temperature: 39C
   power-consumption: 55.2W
   board-temperature1: 28C
   board-temperature2: 27C
   board-temperature3: 32C
   psu1-voltage: 12V
   psu1-current: 4.6A
   psu2-voltage: 0V
   psu2-current: 0A
   fan1-speed: 4724RPM
   fan2-speed: 4518RPM
   fan3-speed: 4724RPM
   fan4-speed: 4627RPM

[admin@ccr1072] > /system health print oid

active-fan: 1.3.6.1.4.1.14988.1.1.3.9.0
voltage: 1.3.6.1.4.1.14988.1.1.3.8.0
temperature: 1.3.6.1.4.1.14988.1.1.3.10.0
processor-temperature: 1.3.6.1.4.1.14988.1.1.3.11.0
current: 1.3.6.1.4.1.14988.1.1.3.13.0
power-consumption: 1.3.6.1.4.1.14988.1.1.3.12.0
psu1-state: 1.3.6.1.4.1.14988.1.1.3.15.0
psu2-state: 1.3.6.1.4.1.14988.1.1.3.16.0
```
Lack of monitoring

IP - SNMP

```
/snmp> send-trap
```

for proactive action
Lack of monitoring

The Dude

you can monitor and manage your devices

new features since RouterOS 6.34
Lack of monitoring

![Netwatch configuration window](image)

- **Host**: 8.8.8.8
- **Interval**: 00:00:03
- **Timeout**: 1000 ms
- **Status**: down
- **Since**: Apr/28/2016 10:00:06

**tools-netwatch**
Lack of monitoring

tools-
Traffic monitor
Lack of monitoring

IP- Traffic Flow
Lack of monitoring

Also HA solutions without monitoring may fail one day

VRRP for 99.9%+ availability

0.365 days or 8.76 hours down in year
DNS issues

8
DNS issues

Many requests from spoofed IPs

```
# ip firewall filter
add action=drop chain=input connection-state=new dst-port=53 in-interface=\ether1-INTERNET protocol=udp
add action=drop chain=input connection-state=new dst-port=53 in-interface=\ether1-INTERNET protocol=tcp
```
DNS issues

10.0.0.0/24

Active Directory

10.0.0.0/24
Firewall inefficiency
Firewall inefficiency

internet

123.123.123.123

webserver
NAT issues
NAT issues

10.0.0.0/24  123.123.123.123
src-ip: 10.0.0.10  dst-ip: 159.148.147.196
NAT masquerade

src-ip: 10.0.0.10
src-ip: 123.123.123.123
dst-ip: 159.148.147.196
NAT issues

bad
/ip firewall nat
add action=masquerade chain=srcnat

ok
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether1-INTERNET

/ip firewall filter
add action=drop chain=forward connection-state=new dst-address=\10.0.0.0/24 in-interface=ether1-INTERNET
NAT issues

IPSec

/ip firewall nat
add action=masquerade chain=srcnat out-interface=
  ether1-INTERNET src-address=10.0.0.0/24

/ip firewall nat
add chain=srcnat dst-address=192.168.0.0/24 src-address=
  10.0.0.0/24
add action=masquerade chain=srcnat out-interface=
  ether1-INTERNET src-address=10.0.0.0/24
Allowed IP Spoofing
Allowed IP Spoofing

10.0.0.0/24

dst-ip: 159.148.147.196

123.123.123.123

? 1. routing decision 2. firewall decision
Allowed IP Spoofing

Tools- Traffic Generator
Allowed IP Spoofing

Test your network  https://spoofer.caida.org/

- Firewall as a service in SDN OpenFlow network
  Andis Arins
  Information, Electronic and Electrical Engineering (AIEEE), 2015 IEEE 3rd Workshop on Advances in
  Year: 2015
  Pages: 1 - 5, DOI: 10.1109/AIEEE.2015.7367309

IEEE Conference Publications

- Abstract  (html)  (pdf)  (307 Kb)  

http://ieeexplore.ieee.org/
Allowed IP Spoofing

10.0.0.0/24

dst-ip: 159.148.147.196

routing decision
Bridge issues
Bridge issues

```
/interface bridge
add name=bridget1-switch-without
/interface bridge port
add bridge=bridget1-switch-without interface=ether2
add bridge=bridget1-switch-without interface=ether1-INTERNET
```
Bridge issues

 wan | master | slave | slave | slave |

 lan

bridge

```
/interface ethernet
set [ find default-name=ether2 ] name=ether2-master
set [ find default-name=ether3 ] master-port=ether2-master
set [ find default-name=ether4 ] master-port=ether2-master
set [ find default-name=ether5 ] master-port=ether2-master
```
Bridge issues

DHCP-Server on individual port, not on bridge itself
PoE issues
PoE issues

Mikrotik PoE standard (4,5pin +) (7,8pin -)

Hello from DC !!!
PoE issues

DC power 1

eth1
PoE in

data,power 2

DC adapter
Waiting for hackers
Waiting for hackers

Dude (if installed) port 2211
### Firewall

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>drop Invalid connections</td>
<td>input</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>184 B</td>
<td>3</td>
</tr>
<tr>
<td>1</td>
<td>allow Established connections</td>
<td>input</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>342.3 K</td>
<td>5 010</td>
</tr>
<tr>
<td>2</td>
<td>allow remote administration from mikrotik office, here could come also other whitelists</td>
<td>input</td>
<td>159.148.147.0/24</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0 B</td>
<td>0</td>
</tr>
<tr>
<td>3</td>
<td>allow pings ICMP</td>
<td>input</td>
<td></td>
<td></td>
<td>1 (icmp)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0 B</td>
<td>0</td>
</tr>
<tr>
<td>4</td>
<td>allow DNS requests from LAN. Here could be any other services like VPN from internet, Proxy, OSPF etc</td>
<td>input</td>
<td>192.168.200.0/24</td>
<td>17 (udp)</td>
<td>53</td>
<td>ether3-wan</td>
<td>ether3-wan</td>
<td></td>
<td></td>
<td>2652 B</td>
<td>36</td>
</tr>
<tr>
<td>5</td>
<td>allow DNS requests from LAN. Here could be any other services like VPN from internet, Proxy, OSPF etc</td>
<td>input</td>
<td>192.168.200.0/24</td>
<td>17 (udp)</td>
<td>53</td>
<td>ether3-wan</td>
<td>ether3-wan</td>
<td></td>
<td></td>
<td>7.9 K</td>
<td>88</td>
</tr>
<tr>
<td>6</td>
<td>drop everything else</td>
<td>input</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>6.3 K</td>
<td>48</td>
</tr>
</tbody>
</table>

```bash
/ip firewall filter
add action=drop chain=input comment="drop Invalid connections" connection-state=invalid
add chain=input comment="allow Established connections" connection-state=established
add chain=input comment="allow remote administration from mikrotik office. here could come also other whitelists" "src-address=159.148.147.0/24
add chain=input comment="allow pings ICMP" protocol=icmp
add chain=input comment="allow DNS requests from LAN. Here could be any other services like VPN from internet, Proxy, OSPF etc" dst-port=53 "in-interface=ether3-wan protocol=udp
add chain=input in-interface=ether3-wan src-address=192.168.200.0/24
add action=drop chain=input comment="drop everything else"
```
Waiting for hackers

MAC telnet/winbox server on all interfaces

default configuration allows MAC access only from initial bridge
Try to Guess ...
admin / no password

```
[admin@MikroTik] > /system routerboard print
    routerboard: yes
        model: RouterBOARD 941-2nD
        serial-number: 5F5E0563B341
        firmware-type: qca9531L
        factory-firmware: 3.24
        current-firmware: 3.33
        upgrade-firmware: 3.33
    
[admin@MikroTik] > /user export
# apr/28/2016 09:31:07 by RouterOS 6.35.1
# software id = DIPN-Z4TN
#
/user
add comment="system default user" group=full name=admin
```
admin / no password
That’s it!