INTELLIGENT MANAGEMENT ROUTER FOR ENTERPRISES

Mikrotik User Meeting in MONGOLIA

Otgonkhuu.A
otgonkhuu@mobinet.mn
June 16, 2017. MobiNet LLC

Content

1. Overview
2. WAN connectivity
3. Security & Firewall
4. User management
5. Redundancy
6. L4 load-balancer
7. Advanced bandwidth management & QoS
8. SmartUPS
9. Powerful troubleshooting and network analysis
10. Monitoring and alerting
11. Extra features (API and scripting)

1. Overview

RouterOS is the powerful router operating system including necessary features like routing, firewall, bandwidth management, wireless access point, backhaul link, hotspot gateway, VPN server, MPLS node, load-balancer and many more. There are plenty of possibilities and advantages which are not mentioned in this presentation. In this presentation, tried to cover only popular and useful use cases for enterprises.

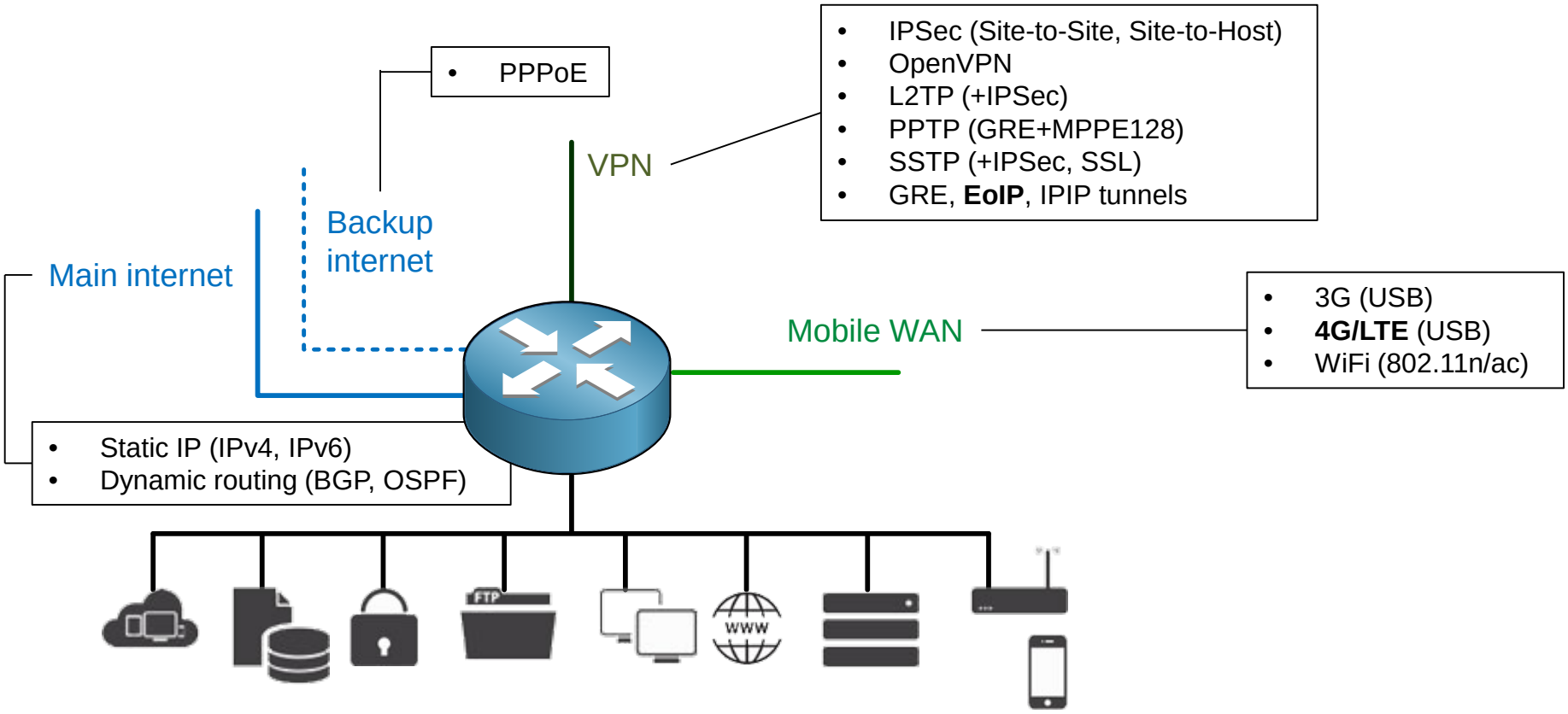
RouterOS fits in **Software-Defined** approach which supports X86 machine and virtualization including VirtualBox 5, VMWare ESXi/Workstation/Fusion, Qemu, Hyper-V on Windows Server 2012, Citrix XenServer, Microsoft Azure and Amazon Web Services (AWS) and as well as OpenFlow standard.

Following common challenges of enterprise networking can be overcome with RouterOS solution.

- Overall network load (throughput) is under 10GE but requires **flexible** networking features like advanced QoS, load-balanced redundant network, traffic filtering, security etc…
- Proof of Concept **without** additional **cost** – Use existing hardware as software router
- Do I really pay for appropriate internet usage – Data traffic **analysis**
- **QoI** (Quality of Investment) – Cost efficient but easily scalable solution based on the current requirement (**Economy of scale**)

2. WAN connectivity

- Main internet connection (MobiNet Leased Line)
- VPN (Virtual Private Network)
- Backup connection (MobiNet Leased Line Economy)
- Mobile WAN

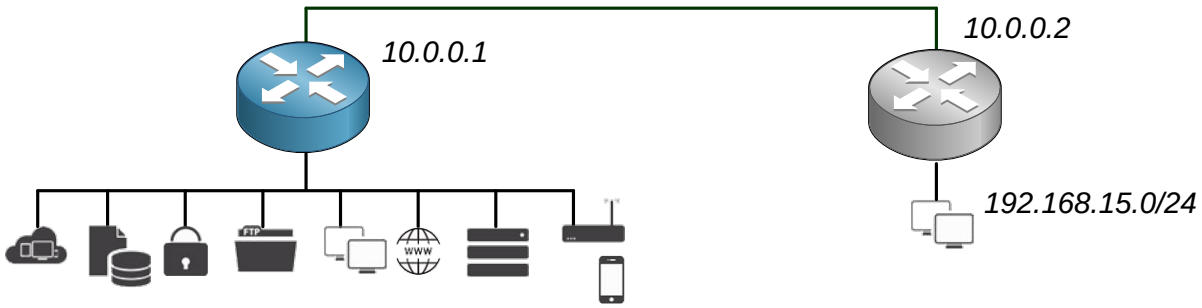


- MobiNet Leased Line as main internet connection with static IP configuration:

```
[Mobinet@lab] > /ip address add address=202.21.X.2/29 interface=ether1 disabled=no
[Mobinet@lab] > /ip route add dst-address=0.0.0.0/0 gateway=202.21.X.1 distance=1 check-gateway=arp disabled=no
[Mobinet@lab] > /ip firewall nat add chain=srcnat out-interface=ether1 action=masquerade disabled=no
```

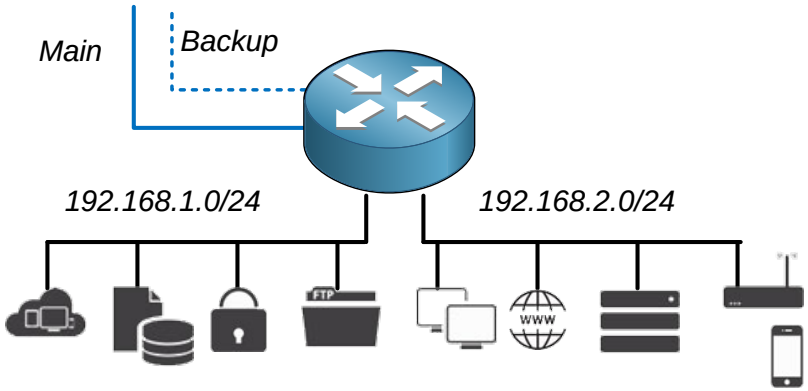
- VPN – PPTP (network-to-network) example:

```
[Mobinet@lab] > /ip address add address=10.0.0.1/29 interface=ether2 disabled=no
[Mobinet@lab] > /interface pptp-client add name=VPN_int user=test password=test \
[Mobinet@lab] > connect-to=10.0.0.2 add-default-route=no disabled=no
[Mobinet@lab] > /ip route add dst-address=192.168.15.0/24 gateway=VPN_int disabled=no
```



- MobiNet LL Economy as backup internet connection

```
[Mobinet@lab] > /interface pppoe-client add name=2nd_wan user=123 password=123 \
[Mobinet@lab] > default-route-distance=2 use-peer-dns=yes interface=ether2 disabled=no
[Mobinet@lab] > /ip firewall nat add chain=srcnat out-interface=2nd_wan action=masquerade disabled=no
# Use backup internet connection efficiently. Simplest example to separate traffic by organizational units:
[Mobinet@lab] > /ip firewall mangle add chain=prerouting src-address=192.168.2.0/24 \
[Mobinet@lab] > action=mark-routing new-routing-mark=Fin_dep disabled=no
[Mobinet@lab] > /ip route add dst-address=0.0.0.0/0 gateway=2nd_wan distance=1 routing-mark=Fin_dep check-gateway=ping
[Mobinet@lab] > /ip route add dst-address=0.0.0.0/0 gateway=202.21.X.1 distance=2 routing-mark=Fin_dep disabled=no
```



- Mobile WAN – 4G USB modem configuration example https://wiki.mikrotik.com/wiki/Supported_Hardware

```
[Mobinet@lab] > /interface lte set [find] name=mobile_wan apn=internet disabled=no
[Mobinet@lab] > /ip dhcp-client add default-route-distance=3 interface=mobile_wan disabled=no
[Mobinet@lab] > /ip firewall nat add chain=srcnat out-interface=mobile_wan action=masquerade disabled=no
```

3. Security & Firewall

- RouterOS is can not be gateway antivirus or WAF in standalone way. But basic security protections can be achieved by itself. Also possible to support your advanced firewall appliances to save it`s resource.
- Basic firewall

```
[Mobinet@lab] > /ip firewall address-list add list=local address=192.168.1.0/24 disabled=no
[Mobinet@lab] > /ip firewall address-list add list=local address=192.168.2.0/24 disabled=no
[Mobinet@lab] > /ip firewall filter add chain=forward connection-state=invalid action=drop
[Mobinet@lab] > /ip firewall filter add chain=forward connection-state=established action=accept
[Mobinet@lab] > /ip firewall filter add chain=forward connection-state=related action=accept
[Mobinet@lab] > /ip firewall filter add chain=forward src-address-list=local action=accept
[Mobinet@lab] > /ip firewall filter add chain=forward action=drop
```

- Permit VPN in firewall

```
[Mobinet@lab] > /ip firewall filter add chain=forward in-interface=VPN_int action=accept place-before=1
```

- Make sure your router is not an open DNS server

```
[Mobinet@lab] > /interface list add name=wan_list
[Mobinet@lab] > /interface list member add list=wan_list interface=ether1
[Mobinet@lab] > /interface list member add list=wan_list interface=2nd_wan
[Mobinet@lab] > /ip firewall raw add chain=prerouting protocol=udp dst-port=53 \
[Mobinet@lab] > in-interface-list=wan_list action=drop disabled=no
[Mobinet@lab] > /ip firewall raw add chain=prerouting protocol=tcp dst-port=53 \
[Mobinet@lab] > in-interface-list=wan_list action=drop disabled=no
```

- Disable unnecessary access to the router

```
[Mobinet@lab] > /ip service {disable api; disable api-ssl; disable ftp; disable www; \
[Mobinet@lab] > disable www-ssl; disable ssh; disable telnet}
```

- Content filter – Example of blocking https:// web (SSL)

```
[Mobinet@lab] > /ip firewall layer7-protocol add name=facebook regexp="^.+(facebook.com).*\$"
[Mobinet@lab] > /ip firewall address-list add list=allowed_hosts address=192.168.1.16-18 disabled=no
[Mobinet@lab] > /ip firewall mangle add chain=prerouting layer7-protocol=facebook protocol=tcp dst-port=80,443 \
[Mobinet@lab] > src-address-list=!allowed_hosts action=mark-connection new-connection-mark=fb_conn \
[Mobinet@lab] > passthrough=yes disabled=no
[Mobinet@lab] > /ip firewall mangle add chain=prerouting connection-mark=fb_conn action=mark-packet \
[Mobinet@lab] > new-packet-mark=fb_packet disabled=no
[Mobinet@lab] > /ip firewall filter add chain=forward packet-mark=fb_packet action=drop
```

- Some useful firewall rules

```
# Identify syn_flood DOS attack
[Mobinet@lab] > /ip firewall filter add chain=input in-interface-list=wan_list connection-limit=100,32 \
[Mobinet@lab] > protocol=tcp tcp-flags=syn action=add-src-to-address-list address-list=blacklist \
[Mobinet@lab] > address-list-timeout=30m

# Identify port scanners
[Mobinet@lab] > /ip firewall filter add chain=input in-interface-list=wan_list psd=21,3s,3,1 \
[Mobinet@lab] > protocol=tcp action=add-src-to-address-list address-list=blacklist address-list-timeout=1d

# Mitigate blacklisted internet sources
[Mobinet@lab] > /ip firewall raw add chain=prerouting src-address-list=blacklist action=drop disabled=no

# Identify Spammers inside the local network to prevent public IP listed in global black lists
[Mobinet@lab] > /ip firewall filter add chain=forward in-interface-list=wan_list connection-limit=30,32
[Mobinet@lab] > limit=30/1m,0:packet protocol=tcp dst-port=25,587,465 action=add-src-to-address-list \
[Mobinet@lab] > address-list=spam address-list-timeout=1d
[Mobinet@lab] > /ip firewall raw add chain=prerouting protocol=tcp dst-port=25,587,465 src-address-list=spam \
[Mobinet@lab] > action=drop disabled=no
```


For more useful rules and ideas please visit to the link https://wiki.mikrotik.com/wiki/Firewall

4. User management

- Secure your local area network that every host should have registration and known as company staff
- Simple example on DHCP to lease IP only to the known host and block manual IP configuration on hosts

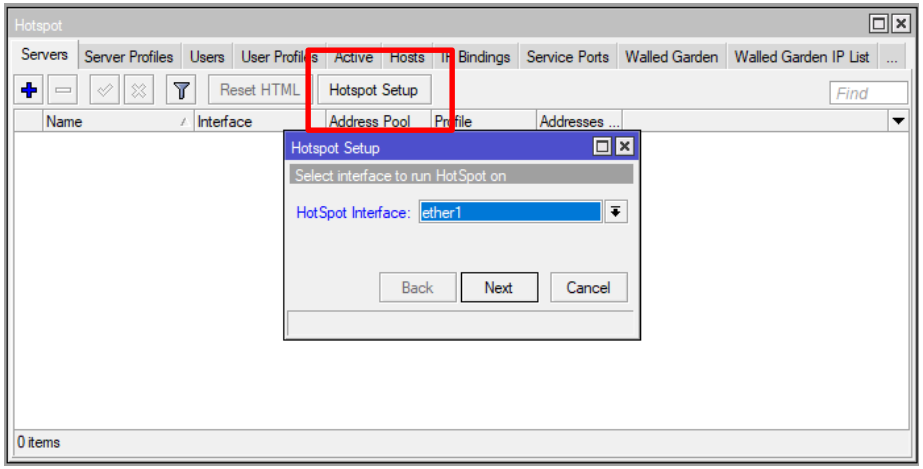
```
[Mobinet@lab] > /ip dhcp-server lease add mac-address=00:01:AB:CD:EF:23 address=192.168.1.10
[Mobinet@lab] > /ip dhcp-server set [find] address-pool=static-only add-arp=yes
[Mobinet@lab] > /interface ethernet set ether1 arp=reply-only
```

- This prevents unauthorized hosts to communicate with router/gateway, but those hosts still have layer2 access to the local network. To be more secure, Layer2 access switches can have port based authentication. Routerboard CRS switches can achieve it with less cost (Low TCO)

- Same Layer 2 protection should apply to the company`s private wireless network.

```
[Mobinet@lab] > /interface wireless access-list add mac-address=00:01:AB:CD:EF:23 interface=local_wireless \
[Mobinet@lab] > vlan-mode=no-tag comment=Otgoo
[Mobinet@lab] > /interface wireless set local_wireless default-authentication=no default-forwarding=no
```

- An other option of internal user management is Hostpot
- Enterprises like Hotels, can have single WiFi-mesh infrastructure to authenticate both staffs and guests
- Based on credentials, staffs connects to the secure private network and guests connects to the advertised hotspot. Even guest can connect to the internet without credential, just CONTINUE button
- This setup can align with wired (Ethernet) network too
- Hotspot is something easy to configure with SETUP option



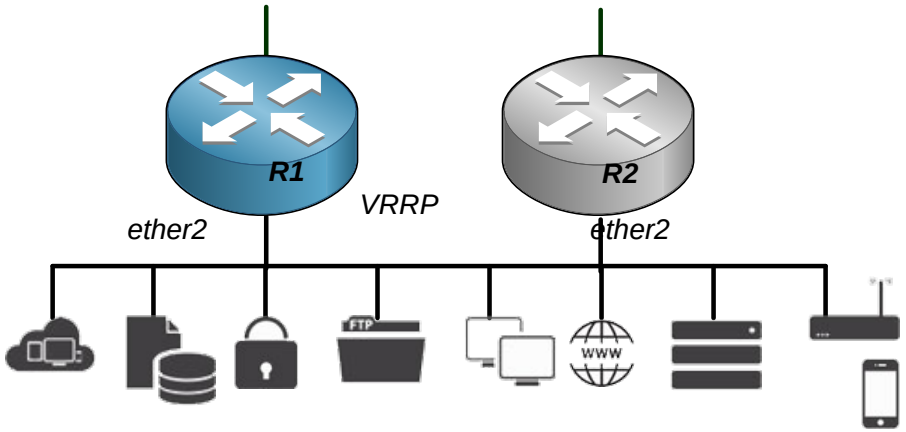
- More advanced **user management** can be covered by User manager package of RouterOS and 3rd party Radius server.

5. Redundancy

- Hardware and WAN connectivity redundancy in single office

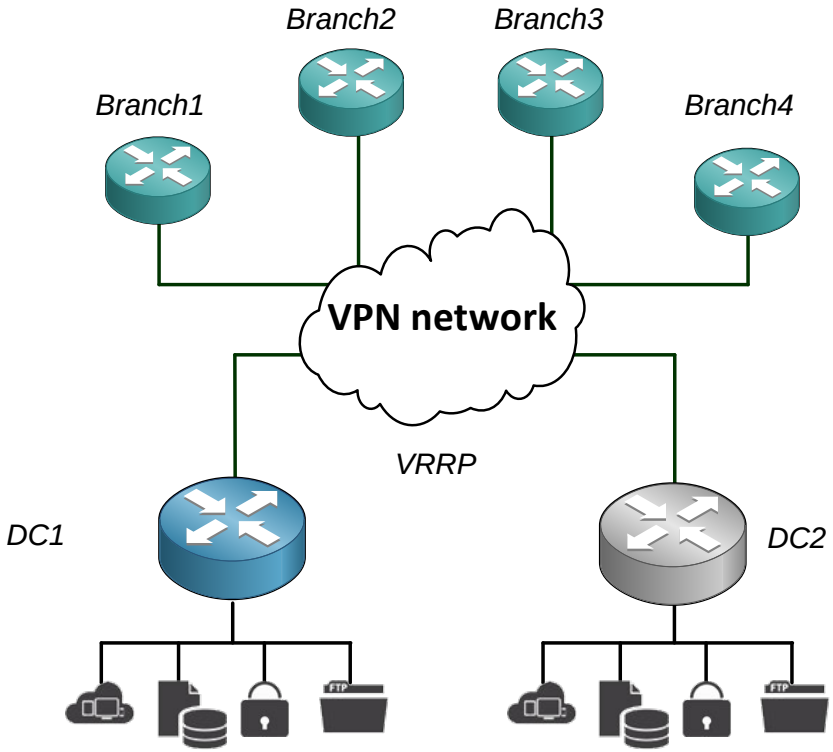
```
[Mobinet@R1] > /interface vrrp add name=vrrp_lan vrid=111 priority=253 interval=1s \
[Mobinet@R1] > preemption-mode=yes disabled=no interface=ether2
[Mobinet@R1] > /ip address add address=192.168.1.2/24 disabled=no interface=ether2
[Mobinet@R1] > /ip address add address=192.168.1.1/24 disabled=no interface=vrrp_lan

[Mobinet@R2] > /interface vrrp add name=vrrp_lan vrid=111 priority=252 interval=1s \
[Mobinet@R2] > preemption-mode=no disabled=no interface=ether2
[Mobinet@R2] > /ip address add address=192.168.1.3/24 disabled=no interface=ether2
[Mobinet@R2] > /ip address add address=192.168.1.1/24 disabled=no interface=vrrp_lan
```

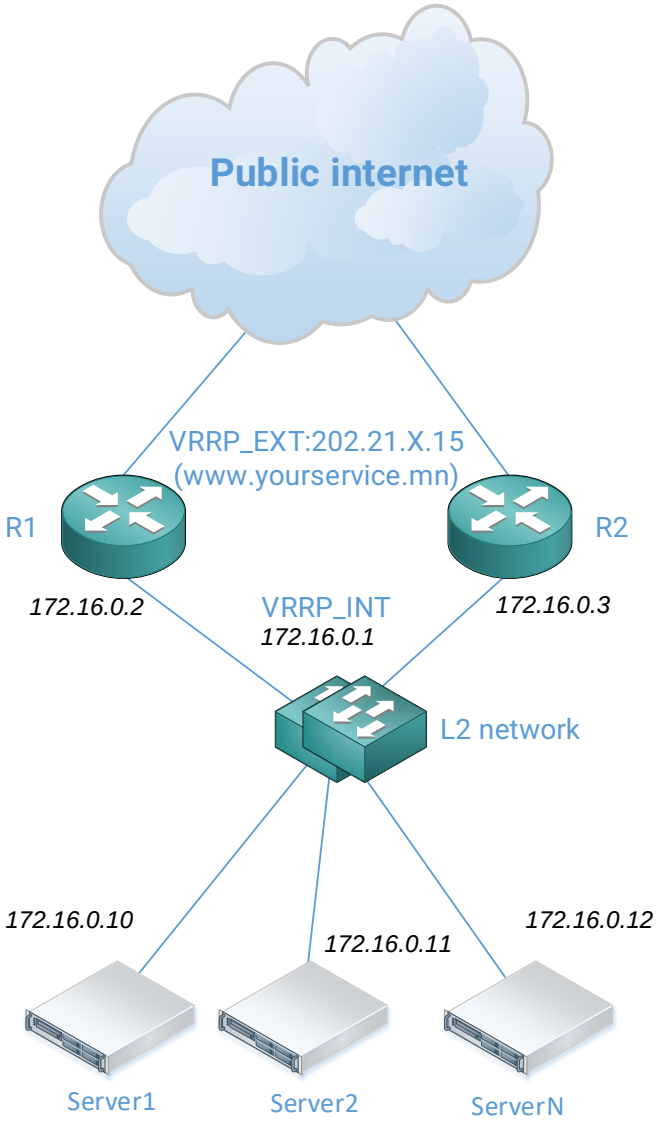


5. Redundancy

- Hardware and WAN connectivity redundancy with backup datacenter
  - Same mechanism can be applied. VRRP on the WAN interfaces
  - Branch hosts can access to the mission critical services (servers) anytime even main datacenter has issue (Application layer redundancy should be implemented on servers)
  - VPN connection type can be anything like IPSec or PPP
  - **Load-balancing** is possible in both cases



6. L4 load-balancer



- Web service load balancing with no server quantity limitation.
- Routers will handle **L4 load balancing**.
- Router detects not only Web servers network issue but also HTTP service (port 80, 443). If something happen with Server N, router will exclude this server from load balancing list automatically. Auto switching time will be depending on server quantity and frequency to check

  Switching test **[server_qty x 5 sec + 4 seconds]**
- Each router can act as other one if something happens with router itself. This is standard automatic VRRP protocol switches within 2 seconds.
- Router will manage **L4 firewall** functionality. Servers don`t need to handle IP firewall separately.
- Limitation: Can not act as WAF /Web application firewall/

- VRRP will be configured exactly same method as previous
- Load-balancing forwarding and scripting sections will be same for both R1 and R2 routers

```
/ip firewall nat add chain=dstnat dst-address=202.21.X.15 protocol=tcp dst-port=80,443 \
per-connection-classifier=src-address-and-port:3/0 action=dst-nat to-address=172.16.0.10 comment=loadbalance_s1
/ip firewall nat add chain=dstnat dst-address=202.21.X.15 protocol=tcp dst-port=80,443 \
per-connection-classifier=src-address-and-port:3/1 action=dst-nat to-address=172.16.0.11 comment=loadbalance_s2
/ip firewall nat add chain=dstnat dst-address=202.21.X.15 protocol=tcp dst-port=80,443 \
per-connection-classifier=src-address-and-port:3/2 action=dst-nat to-address=172.16.0.12 comment=loadbalance_s3
```

- Check TCP port 443 with fetch
  (In order to show friendly, script parameters are not in correct syntax format. Please copy source section in the winbox)

```
/system script add name=s1_fetch source=
      /file remove [find name=testfile.10];
      /tool fetch "https://172.16.0.10/test.txt" dst-path=testfile.10 mode=https port=443;
      /ip dns static add address=0.0.0.1 name=s1;
      /ip dns static add address=0.0.0.1 name=s2;
      /ip dns static add address=0.0.0.1 name=s3;
      /ip dns static add address=0.0.0.1 name=s0;
      /ip dns static add address=0.0.0.1 name=z;
/system script add name=s2_fetch source=
      /file remove [find name=testfile.11];
      /tool fetch "https://172.16.0.11/test.txt" dst-path=testfile.11 mode=https port=443;
      /ip dns static add address=0.0.0.1 name=s1;
      /ip dns static add address=0.0.0.1 name=s2;
      /ip dns static add address=0.0.0.1 name=s3;
      /ip dns static add address=0.0.0.1 name=s0;
      /ip dns static add address=0.0.0.1 name=z;
/system script add name=s3_fetch source=
      /file remove [find name=testfile.12];
      /tool fetch "https://172.16.0.12/test.txt" dst-path=testfile.12 mode=https port=443;
      /ip dns static add address=0.0.0.1 name=s1;
      /ip dns static add address=0.0.0.1 name=s2;
      /ip dns static add address=0.0.0.1 name=s3;
      /ip dns static add address=0.0.0.1 name=s0;
      /ip dns static add address=0.0.0.1 name=z;
```

```
/system script add name=s_status_check source=
   if ([/file print count-only where name=testfile.10]=1) do={
   /log info "172.16.0.10 is ok"; /ip dns static set [find where name=s1] comment=1;} else={/log info "172.16.0.10 is down";
   /ip dns static set [find where name=s1] comment=0;}
   if ([/file print count-only where name=testfile.11]=1) do={
   /log info "172.16.0.11 is ok"; /ip dns static set [find where name=s2] comment=1;} else={/log info "172.16.0.11 is down";
   /ip dns static set [find where name=s2] comment=0;}
   if ([/file print count-only where name=testfile.12]=1) do={
   /log info "172.16.0.12 is ok"; /ip dns static set [find where name=s3] comment=1;} else={/log info "172.16.0.12 is down";
   /ip dns static set [find where name=s2] comment=0;}

/system script add name=update_balancer source=
   :global s1 [/ip dns static get [find where name=s1] comment];
   :global s2 [/ip dns static get [find where name=s2] comment];
   :global s3 [/ip dns static get [find where name=s3] comment];
   :global s0 ($s1+$s2+$s3);
   :global z 0;

   if ($s1=1) do={
   /ip firewall nat set [find where comment=loadbalance_s1] disabled=no per-connection-classifier="src-address-and-port:$s0/$z";
   :global z ($z+1)} else={
   /ip firewall nat set [find where comment=loadbalance_s1] disabled=yes};

   :if ($s2=1) do={
   /ip firewall nat set [find where comment=loadbalance_s2] disabled=no per-connection-classifier="src-address-and-port:$s0/$z";
   :global z ($z+1)} else={
   /ip firewall nat set [find where comment=loadbalance_s2] disabled=yes};

   :if ($s3=1) do={
   /ip firewall nat set [find where comment=loadbalance_s3] disabled=no per-connection-classifier="src-address-and-port:$s0/$z";
   :global z ($z+1)} else={
   /ip firewall nat set [find where comment=loadbalance_s3] disabled=yes};
```

- Tested log in real environment

```
16:32:44 script,info STARTED
16:32:46 info fetch: file "testfile.10" downloaded
16:32:56 info fetch: file "testfile.12" downloaded
16:32:59 script,info 172.16.0.10 is ok
16:32:59 system,info static dns entry changed by load-balancer
16:32:59 script,info 172.16.0.11 is down
16:32:59 system,info static dns entry changed by load-balancer
16:32:59 script,info 172.16.0.12 is ok
16:33:00 system,info static dns entry changed by load-balancer
16:33:02 system,info nat rule changed by load-balancer
16:33:02 system,info nat rule changed by load-balancer
16:33:02 system,info nat rule changed by load-balancer
16:33:02 script,info FINISHED
```

7. Advanced bandwidth management & QoS

- Utilize available bandwidth **efficiently**
- **Real-time** equal bandwidth distribution among available hosts in the office
- Destination based different **QoS management**
- Application **classification** and it`s QoS

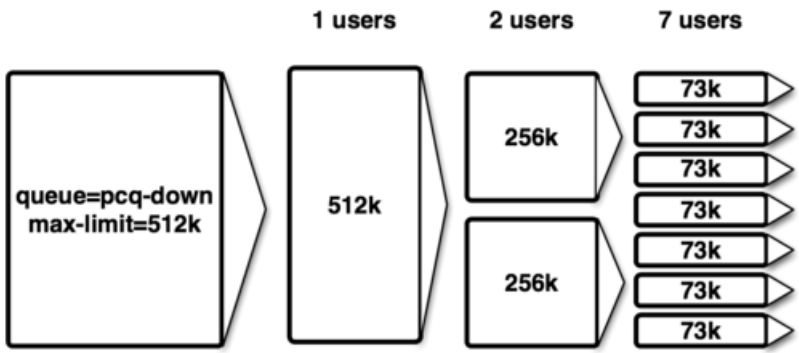
Queue List

Simple Queues | Interface Queues | Queue Tree | Queue Types

oo Reset Counters | oo Reset All Counters | Find

#	Name	Target	Upload Max Limit	Download Max Limit	Packet Marks	Upload Limit At	Download Limit At	Download Priority	Download Queue Type
1	Mongolian_Interexchange(MIX)	192.168.0.0/16	1000M	1000M	mix_up, mix_down	unlimited	unlimited	1	default-small
0	Internet	192.168.0.0/16	25M	25M		unlimited	unlimited	8	default-small
3	VoIP	202.21.1.16	4M	4M	VoIP_up, VoIP_down	unlimited	unlimited	2	default-small
2	CEO	192.168.1.100	5M	5M		unlimited	unlimited	3	default-small
4	Financial&Legal	192.168.1.0/25	8M	8M		unlimited	unlimited	4	default-small
5	CFO	192.168.1.10	3M	3M		unlimited	unlimited	1	default-small
6	Financial&Legal_Staffs	192.168.1.0/25	8M	8M		unlimited	unlimited	2	pcq-download-default
7	IT_Dep	192.168.2.0/24	15M	15M		unlimited	unlimited	5	default-small
11	Application_communication	202.21.1.15, 202.21.1.14	5M	5M		unlimited	unlimited	1	pcq-download-default
12	IT_Staffs	192.168.2.0/24	15M	15M		unlimited	unlimited	2	pcq-download-default
8	HR	192.168.3.0/27	2M	2M		1M	1M	6	pcq-download-default
9	Factory	192.168.3.64/26	2M	2M		1M	1M	7	pcq-download-default
10	Guest	172.16.255.0/24	2M	2M		unlimited	unlimited	8	pcq-download-default

13 items (1 selected) | 0 B queued | 0 packets queued



MobiNet Powered by MobiCom

#	Name	Target	Upload Max Limit	Download Max Limit
1	Mongolian_Interexchange(MIX)	192.168.0.0/16	1000M	1000M
0	Internet	192.168.0.0/16	25M	25M
3	VoIP	202.21.1.16	4M	4M
2	CEO	192.168.1.100	5M	5M
4	Financial&Legal	192.168.1.0/25	8M	8M
5	CFO	192.168.1.10	3M	3M
6	Financial&Legal_Staffs	192.168.1.0/25	8M	8M
7	IT_Dep	192.168.2.0/24	15M	15M
11	Application_communication	202.21.1.15, 202.21.1.14	5M	5M
12	IT_Staffs	192.168.2.0/24	15M	15M
8	HR	192.168.3.0/27	2M	2M
9	Factory	192.168.3.64/26	2M	2M
10	Guest	172.16.255.0/24	2M	2M

- Example of MIX (Mongolian InterExchange) traffic classification

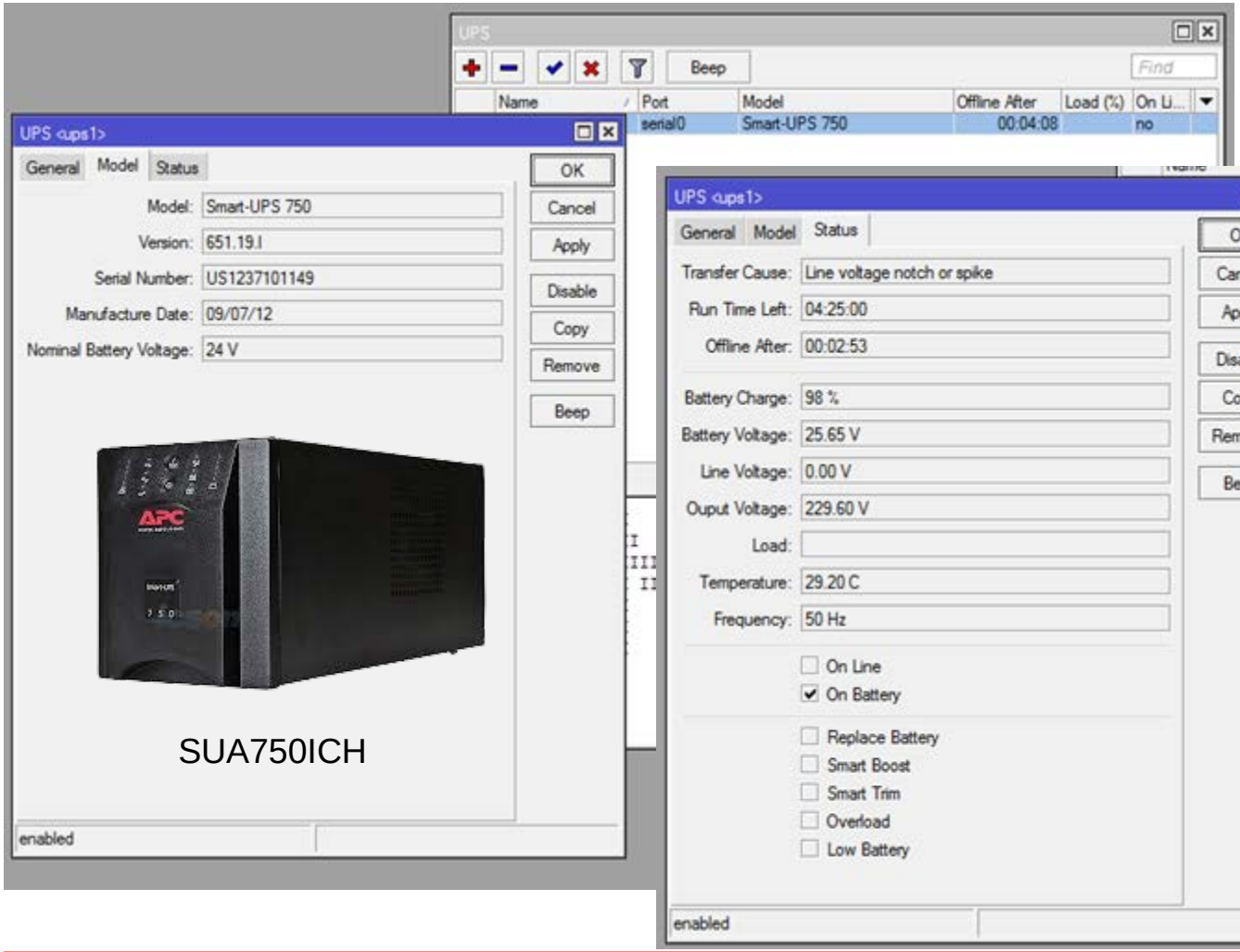
```
[Mobinet@lab] > /ip firewall address-list add list=MIX_ISP address=202.131.224.0/19 disabled=no
[Mobinet@lab] > /ip firewall mangle add chain=prerouting src-address-list=MIX_ISP action=mark-packet \
[Mobinet@lab] > new-packet-mark=mix_down
[Mobinet@lab] > /ip firewall mangle add chain=postrouting dst-address-list=MIX_ISP action=mark-packet \
[Mobinet@lab] > new-packet-mark=mix_up
[Mobinet@lab] > /queue simple add name=Mongolian_Interexchange(MIX) packet-mark=mix_up,mix_down max-limit=1G/1G \
[Mobinet@lab] > target=0.0.0.0/0
```

- If your hardware has enough RAM, increase your queue sizes. It helps to drop less packets when traffic amount reaches limits at peak hours

```
[Mobinet@lab] > /queue type set default-small pfifo-limit=1000
[Mobinet@lab] > /queue type set pcq-download-default pcq-limit=5000 pcq-total-limit=200000
```

8. SmartUPS

- RouterOS supports APC SmartUPS series smart signaling protocol over USB and Serial interfaces
- Alert power-outage, safe hibernate router when battery capacity become low



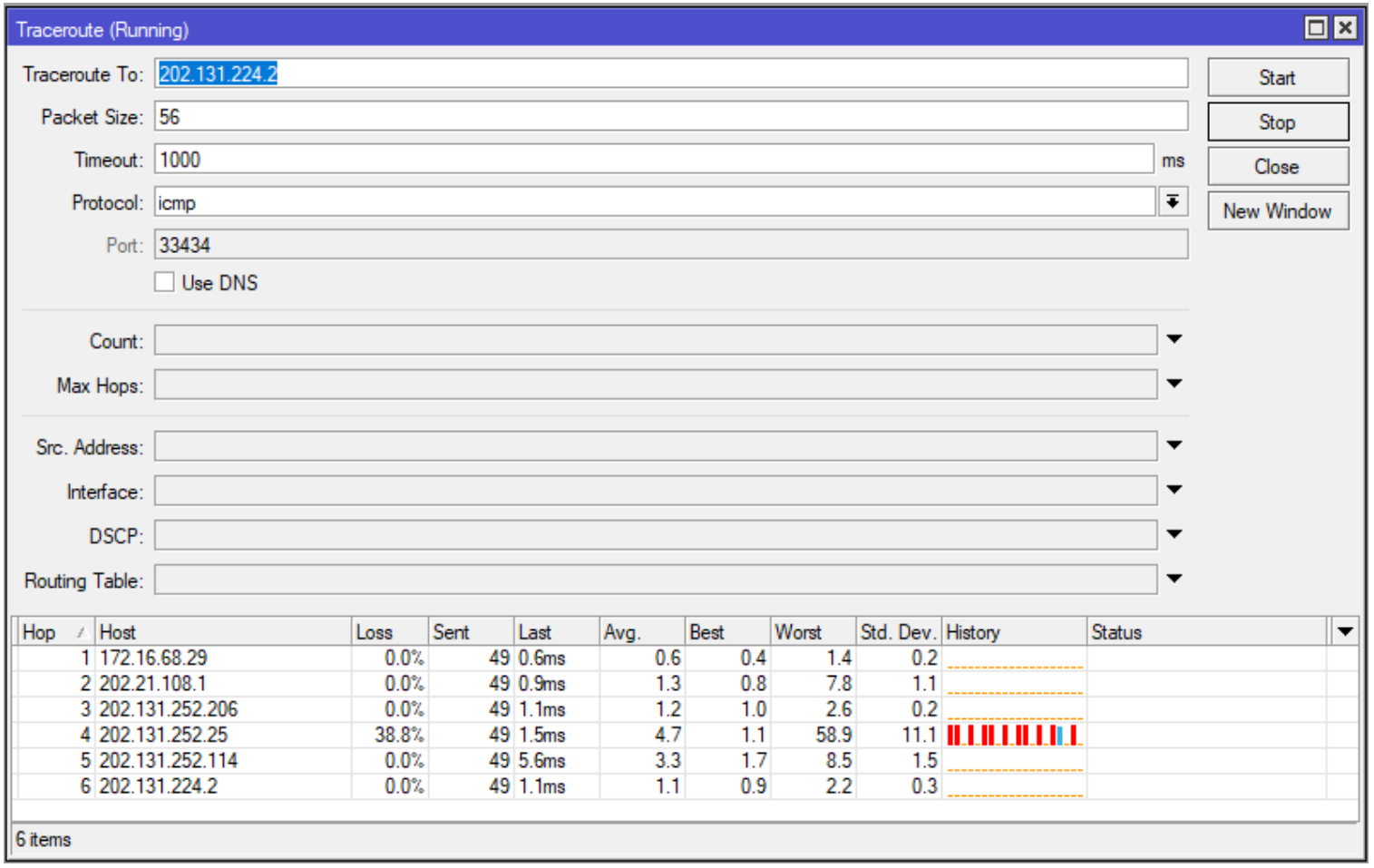
SUA750ICH

SMT1500i

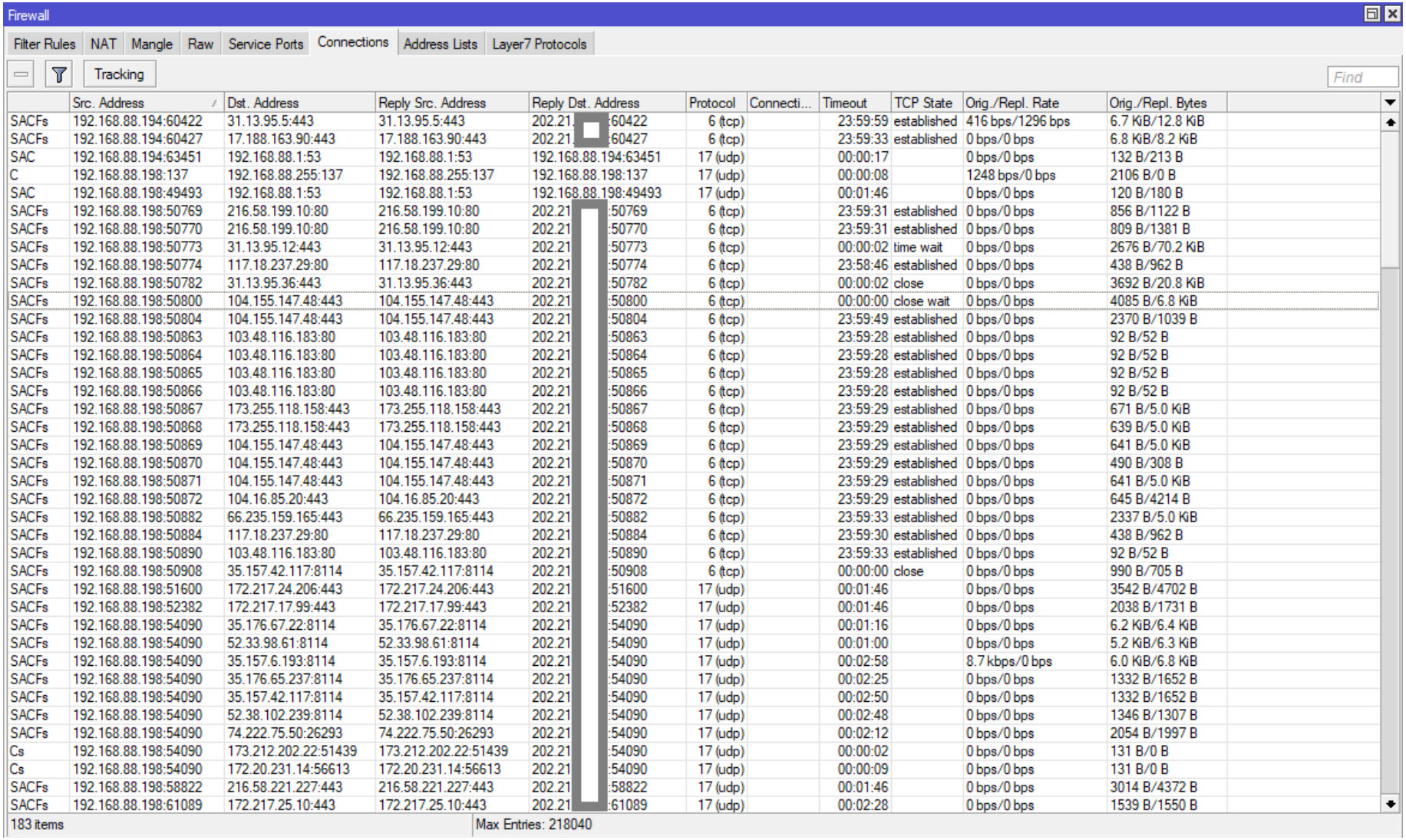
SC420i

9. Powerful troubleshooting and network analysis

- MTR including both trace route and ping
- ARP ping, IPScan “/tool traceroute 202.131.224.2”



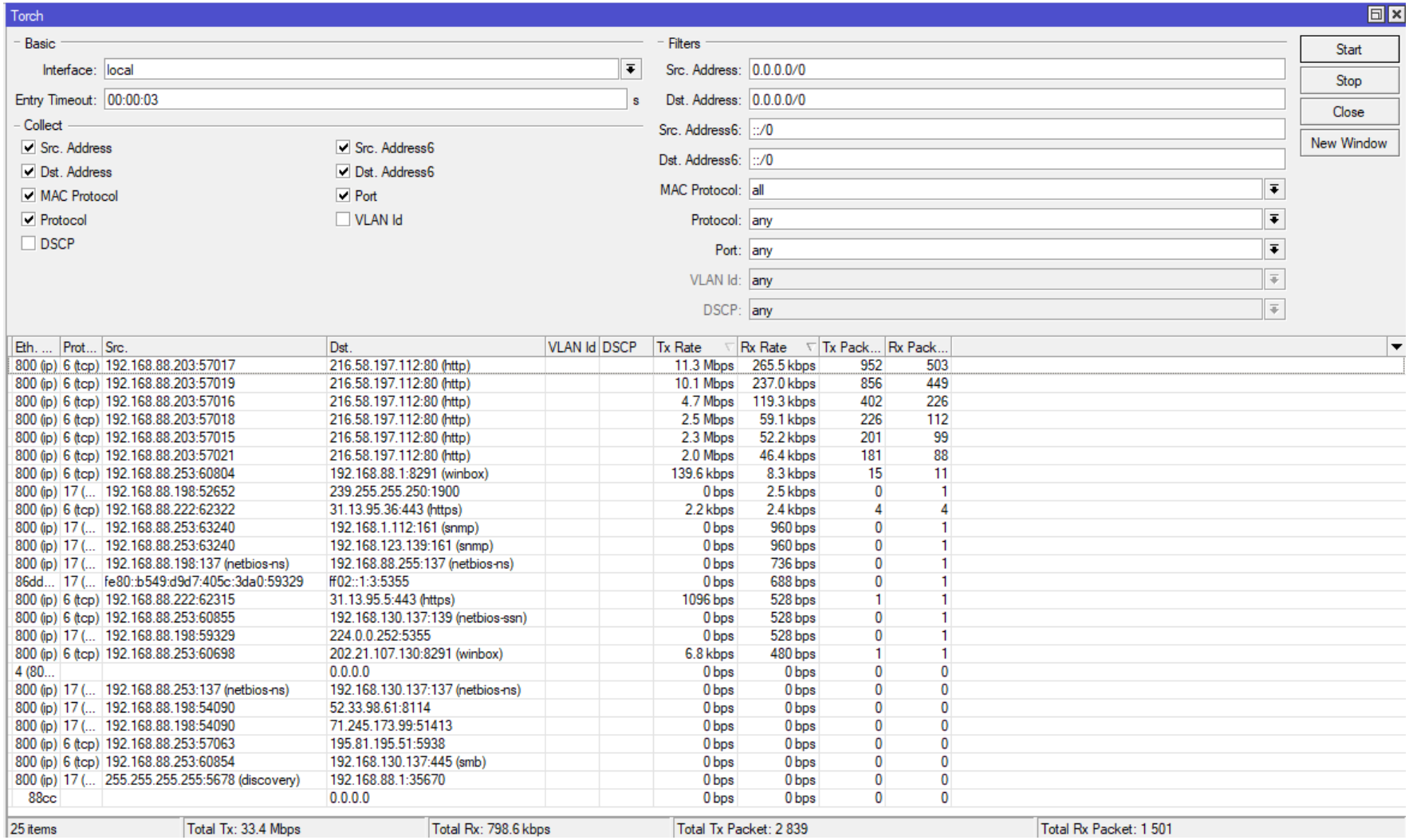
- Real-time connection tracking



	Src. Address	Dst. Address	Reply Src. Address	Reply Dst. Address	Protocol	Connecti...	Timeout	TCP State	Orig./Repl. Rate	Orig./Repl. Bytes
SACFs	192.168.88.194:60422	31.13.95.5:443	31.13.95.5:443	202.21 :60422	6 (tcp)		23:59:59	established	416 bps/1296 bps	6.7 KiB/12.8 KiB
SACFs	192.168.88.194:60427	17.188.163.90:443	17.188.163.90:443	202.21 :60427	6 (tcp)		23:59:33	established	0 bps/0 bps	6.8 KiB/8.2 KiB
SAC	192.168.88.194:63451	192.168.88.1:53	192.168.88.1:53	192.168.88.194:63451	17 (udp)		00:00:17		0 bps/0 bps	132 B/213 B
C	192.168.88.198:137	192.168.88.255:137	192.168.88.255:137	192.168.88.198:137	17 (udp)		00:00:08		1248 bps/0 bps	2106 B/0 B
SAC	192.168.88.198:49493	192.168.88.1:53	192.168.88.1:53	192.168.88.198:49493	17 (udp)		00:01:46		0 bps/0 bps	120 B/180 B
SACFs	192.168.88.198:50769	216.58.199.10:80	216.58.199.10:80	202.21 :50769	6 (tcp)		23:59:31	established	0 bps/0 bps	856 B/1122 B
SACFs	192.168.88.198:50770	216.58.199.10:80	216.58.199.10:80	202.21 :50770	6 (tcp)		23:59:31	established	0 bps/0 bps	809 B/1381 B
SACFs	192.168.88.198:50773	31.13.95.12:443	31.13.95.12:443	202.21 :50773	6 (tcp)		00:00:02	time wait	0 bps/0 bps	2676 B/70.2 KiB
SACFs	192.168.88.198:50774	117.18.237.29:80	117.18.237.29:80	202.21 :50774	6 (tcp)		23:58:46	established	0 bps/0 bps	438 B/962 B
SACFs	192.168.88.198:50782	31.13.95.36:443	31.13.95.36:443	202.21 :50782	6 (tcp)		00:00:02	close	0 bps/0 bps	3692 B/20.8 KiB
SACFs	192.168.88.198:50800	104.155.147.48:443	104.155.147.48:443	202.21 :50800	6 (tcp)		00:00:00	close wait	0 bps/0 bps	4085 B/6.8 KiB
SACFs	192.168.88.198:50804	104.155.147.48:443	104.155.147.48:443	202.21 :50804	6 (tcp)		23:59:49	established	0 bps/0 bps	2370 B/1039 B
SACFs	192.168.88.198:50863	103.48.116.183:80	103.48.116.183:80	202.21 :50863	6 (tcp)		23:59:28	established	0 bps/0 bps	92 B/52 B
SACFs	192.168.88.198:50864	103.48.116.183:80	103.48.116.183:80	202.21 :50864	6 (tcp)		23:59:28	established	0 bps/0 bps	92 B/52 B
SACFs	192.168.88.198:50865	103.48.116.183:80	103.48.116.183:80	202.21 :50865	6 (tcp)		23:59:28	established	0 bps/0 bps	92 B/52 B
SACFs	192.168.88.198:50866	103.48.116.183:80	103.48.116.183:80	202.21 :50866	6 (tcp)		23:59:28	established	0 bps/0 bps	92 B/52 B
SACFs	192.168.88.198:50867	173.255.118.158:443	173.255.118.158:443	202.21 :50867	6 (tcp)		23:59:29	established	0 bps/0 bps	671 B/5.0 KiB
SACFs	192.168.88.198:50868	173.255.118.158:443	173.255.118.158:443	202.21 :50868	6 (tcp)		23:59:29	established	0 bps/0 bps	639 B/5.0 KiB
SACFs	192.168.88.198:50869	104.155.147.48:443	104.155.147.48:443	202.21 :50869	6 (tcp)		23:59:29	established	0 bps/0 bps	641 B/5.0 KiB
SACFs	192.168.88.198:50870	104.155.147.48:443	104.155.147.48:443	202.21 :50870	6 (tcp)		23:59:29	established	0 bps/0 bps	490 B/308 B
SACFs	192.168.88.198:50871	104.155.147.48:443	104.155.147.48:443	202.21 :50871	6 (tcp)		23:59:29	established	0 bps/0 bps	641 B/5.0 KiB
SACFs	192.168.88.198:50872	104.16.85.20:443	104.16.85.20:443	202.21 :50872	6 (tcp)		23:59:29	established	0 bps/0 bps	645 B/4214 B
SACFs	192.168.88.198:50882	66.235.159.165:443	66.235.159.165:443	202.21 :50882	6 (tcp)		23:59:33	established	0 bps/0 bps	2337 B/5.0 KiB
SACFs	192.168.88.198:50884	117.18.237.29:80	117.18.237.29:80	202.21 :50884	6 (tcp)		23:59:30	established	0 bps/0 bps	438 B/962 B
SACFs	192.168.88.198:50890	103.48.116.183:80	103.48.116.183:80	202.21 :50890	6 (tcp)		23:59:33	established	0 bps/0 bps	92 B/52 B
SACFs	192.168.88.198:50908	35.157.42.117:8114	35.157.42.117:8114	202.21 :50908	6 (tcp)		00:00:00	close	0 bps/0 bps	990 B/705 B
SACFs	192.168.88.198:51600	172.217.24.206:443	172.217.24.206:443	202.21 :51600	17 (udp)		00:01:46		0 bps/0 bps	3542 B/4702 B
SACFs	192.168.88.198:52382	172.217.17.99:443	172.217.17.99:443	202.21 :52382	17 (udp)		00:01:46		0 bps/0 bps	2038 B/1731 B
SACFs	192.168.88.198:54090	35.176.67.22:8114	35.176.67.22:8114	202.21 :54090	17 (udp)		00:01:16		0 bps/0 bps	6.2 KiB/6.4 KiB
SACFs	192.168.88.198:54090	52.33.98.61:8114	52.33.98.61:8114	202.21 :54090	17 (udp)		00:01:00		0 bps/0 bps	5.2 KiB/6.3 KiB
SACFs	192.168.88.198:54090	35.157.6.193:8114	35.157.6.193:8114	202.21 :54090	17 (udp)		00:02:58		8.7 kbps/0 bps	6.0 KiB/6.8 KiB
SACFs	192.168.88.198:54090	35.176.65.237:8114	35.176.65.237:8114	202.21 :54090	17 (udp)		00:02:25		0 bps/0 bps	1332 B/1652 B
SACFs	192.168.88.198:54090	35.157.42.117:8114	35.157.42.117:8114	202.21 :54090	17 (udp)		00:02:50		0 bps/0 bps	1332 B/1652 B
SACFs	192.168.88.198:54090	52.38.102.239:8114	52.38.102.239:8114	202.21 :54090	17 (udp)		00:02:48		0 bps/0 bps	1346 B/1307 B
SACFs	192.168.88.198:54090	74.222.75.50:26293	74.222.75.50:26293	202.21 :54090	17 (udp)		00:02:12		0 bps/0 bps	2054 B/1997 B
Cs	192.168.88.198:54090	173.212.202.22:51439	173.212.202.22:51439	202.21 :54090	17 (udp)		00:00:02		0 bps/0 bps	131 B/0 B
Cs	192.168.88.198:54090	172.20.231.14:56613	172.20.231.14:56613	202.21 :54090	17 (udp)		00:00:09		0 bps/0 bps	131 B/0 B
SACFs	192.168.88.198:58822	216.58.221.227:443	216.58.221.227:443	202.21 :58822	17 (udp)		00:01:46		0 bps/0 bps	3014 B/4372 B
SACFs	192.168.88.198:61089	172.217.25.10:443	172.217.25.10:443	202.21 :61089	17 (udp)		00:02:28		0 bps/0 bps	1539 B/1550 B

183 items | Max Entries: 218040

- Real-time traffic torching



- Packet sniffer
- Supports TZSP stream to export output to the wireshark host

Packet Sniffer Packets

Time...	Interface	Direction	Src. Address	Src. Port	Dst. Address	Dst. Port	Prot...	IP Pr...	Size
3.791	local	tx	172.217.24.193	443	192.168.88.202	65310	204...	6 (tcp)	1470
3.791	wlan1	tx	172.217.24.193	443	192.168.88.202	65310	204...	6 (tcp)	1470
3.791	vlan465	rx	172.217.24.193	443	202.21.120.4	65310	204...	6 (tcp)	1470
3.791	local	tx	172.217.24.193	443	192.168.88.202	65310	204...	6 (tcp)	1470
3.791	wlan1	tx	172.217.24.193	443	192.168.88.202	65310	204...	6 (tcp)	1470
3.791	vlan465	rx	172.217.24.193	443	202.21.120.4	65310	204...	6 (tcp)	1470
3.791	local	tx	172.217.24.193	443	192.168.88.202	65310	204...	6 (tcp)	1470
3.791	wlan1	tx	172.217.24.193	443	192.168.88.202	65310	204...	6 (tcp)	1470
3.791	vlan465	rx	172.217.24.193	443	202.21.120.4	65310	204...	6 (tcp)	1470
3.791	local	tx	172.217.24.193	443	192.168.88.202	65310	204...	6 (tcp)	1470
3.791	wlan1	tx	172.217.24.193	443	192.168.88.202	65310	204...	6 (tcp)	1470
3.791	vlan465	rx	172.217.24.193	443	202.21.120.4	65310	204...	6 (tcp)	1470
3.791	local	tx	172.217.24.193	443	192.168.88.202	65310	204...	6 (tcp)	1470
3.791	wlan1	tx	172.217.24.193	443	192.168.88.202	65310	204...	6 (tcp)	1470
3.791	vlan465	rx	172.217.24.193	443	202.21.120.4	65310	204...	6 (tcp)	1470

9699 items (1 selected)

Packet Sniffer Hosts

Address	Rate	Peek Rate	Total
8.8.8.8	0 bps/0 bps	2.0 kbps/2.7 kbps	332/764
10.108.1.1	0 bps/0 bps	0 bps/1216 bps	0/152
10.109.1.0	0 bps/0 bps	0 bps/1240 bps	0/155
17.188.163.90	0 bps/0 bps	4.1 kbps/3.7 kbps	519/471
23.99.112.148	0 bps/0 bps	960 bps/0 bps	120/0
31.13.95.5	0 bps/0 bps	3.2 kbps/5.1 kbps	717/1047
35.188.15.108	0 bps/0 bps	2.8 kbps/5.4 kbps	591/684
37.53.198.145	0 bps/0 bps	3.1 kbps/0 bps	393/0
52.207.132.141	0 bps/0 bps	960 bps/0 bps	120/0
59.151.175.53	0 bps/0 bps	2.8 kbps/0 bps	360/0
62.210.109.136	0 bps/0 bps	0 bps/480 bps	0/60
66.235.159.165	0 bps/0 bps	984 bps/1008 bps	123/126
79.49.58.16	0 bps/0 bps	0 bps/1072 bps	0/134
103.48.116.183	0 bps/0 bps	984 bps/1008 bps	123/126
103.219.165.215	0 bps/0 bps	0 bps/480 bps	0/60

48 items (1 selected)

Packet Sniffer Connections

Src. Address	Dst. Address	Bytes	Resends	MSS
31.13.95.5:443	202.21.120.4:604...	110/0	0/0	0/0
31.13.95.5:443	192.168.88.194:6...	110/0	110/0	0/0
129.0.1.209:7949	202.21.120.4:243...	4294967...	0/0	0/0
129.0.1.209:7949	202.21.120.4:243...	4294967...	0/0	0/0
129.0.1.209:34037	202.21.120.4:177...	32/0	4294967...	0/0
129.0.1.209:34037	202.21.120.4:177...	214/0	0/0	0/0
129.0.1.209:40247	202.21.120.4:334...	4294967...	0/0	0/0
129.0.1.209:44249	202.21.120.4:6337	32/0	0/0	0/0
129.0.1.209:44249	202.21.120.4:6337	32/0	0/0	0/0
129.0.1.209:44249	202.21.120.4:6337	32/0	0/0	0/0
129.0.1.209:44249	202.21.120.4:6337	32/0	0/0	0/0
129.0.1.209:44249	202.21.120.4:6337	32/0	0/0	0/0
129.0.1.209:44249	202.21.120.4:6337	32/0	0/0	0/0
129.0.1.209:44249	202.21.120.4:6337	32/0	0/0	0/0
129.0.1.209:44249	202.21.120.4:6337	32/0	224/0	0/0

404 items (1 selected)

Packet Sniffer Protocols

Protocol	IP Protocol	Port	Packets	Bytes	Share (%)
2048 (ip)			9695	10238992	99.99
2048 (ip)	6 (tcp)		9662	10235738	99.96
2048 (ip)	6 (tcp)	443	8930	10155145	99.17
2048 (ip)	6 (tcp)	65310	8901	10149156	99.12
2048 (ip)	6 (tcp)	8291	68	40646	0.39
2048 (ip)	6 (tcp)	6337	641	38656	0.37
2048 (ip)	6 (tcp)	44249	641	38656	0.37
2048 (ip)	6 (tcp)	60804	62	37976	0.37
2048 (ip)	6 (tcp)	65259	5	3805	0.03
2048 (ip)	17 (udp)		33	3254	0.03
2048 (ip)	6 (tcp)	60698	6	2670	0.02
2048 (ip)	17 (udp)	53	24	2597	0.02
2048 (ip)	6 (tcp)	51102	12	1230	0.01
2048 (ip)	6 (tcp)	60422	12	954	0.00
2048 (ip)	17 (udp)	58428	4	710	0.00

38 items (1 selected)

10. Monitoring and alerting

- Small but useful tool “Graphing”. It graphs and stores queue and interfaces traffic usage.
- Basic monitoring protocols SNMP, NetFlowV9
- E-mail alerting and SMS alerting with USB 3G/4G modem
- Bandwidth test server and client functionality that generates real data. Client supports Windows machine
- Netwatch monitors defined hosts by ICMP and can take any action based on UP/DOWN event. Simple example:

```
[Mobinet@lab] > /tool netwatch add host=192.168.1.10 interval=5s timeout=100ms down-script="/tool e-mail
send server=202.131.224.27 port=25 from=lab@mobinet.mn to=otgonkhuu@mobinet.mn
subject=video_processing_gone_down"
```

11. Extra features (API and scripting)

RouterOS Script and API features enables plenty of possibilities and advantages.

- Auto provisioning like create/remove automatic rules
- Automatically register local users which connected to CRM/ERP
- In a hotel possible to integrate into hotel CRM and create hotspot client with necessary policy.
- Broad range of network automation
- Act as SMS-to-Email server
- One-time password for networking access
- On-Demand speed booster
- Network based advertisement system
- Many more…

WIKI.MIKROTIK.COM

FORUM.MIKROTIK.COM

THANK YOU

Otgonkhuu.A
otgonkhuu@mobinet.mn
June 16, 2017. MobiNet LLC