Mikrotik

Blocking .zip domains with DNS proxy

Background

https://www.youtube.com/watch?v=V82lHNsSPww

Use Mikrotik DNS proxy for blocking

The code snippet below will cause a Mikrotik DNS proxy to return 127.255.255.127 for all .zip domains, including all subdomains.

```
/ip dns static
add address=127.255.255.127 comment="block access to all .zip domains" regexp=".+\\.zip\$"
ttl=10s
```

The requirement for this to work of course is that all of the hosts on the network only source their DNS through the Mikrotik DNS proxy.

#end

Creating a CHR instance in AWS EC2

RouterOS CHR instances in AWS EC2

I have experience with T2, T3, and T3a, primarily nano and micro, CHR instances. I prefer to use T3 instances as they provide two CPU cores for practically the same low price.

TL;DR

If you want to use T3 or T3a instance, you need to create fresh Router OS 7 CHR instances or else you will experience a corrupted disk on subsequent upgrades.

I have not experienced any upgrade failures with T2 instances.

The whole story

Mikrotik provides a RouterOS CHR v6.44.3 AMI in the AWS Marketplace. I have a number of production EC2 instances built from that AMI. When I started testing ROS 7 instances, I spun up new instances using this AMI, upgrading to the latest v6, and then whatever the current v7 was at the time. These upgrades all succeeded and ran with no issues, until Mikrotik released to the next version and I attempted to upgrade. The result each time, regardless of the target version (7.2, 7.3, 7.4, 7.5, and 7.6), was a corrupted disk. If you view the screenshot of the instance, you will find the last message "Loa01" on the console.

I opened ticket SUP-77812 with Mikrotik on March 24th after experiencing my third router failure. This failure occurred while upgrading from ROS 7.1.3 to 7.1.5.

During some testing in May, I was able to determine that this disk corruption was consistent with T3 instances, but never occurred with T2 instances.

I attempted to create my own AMI with the CHR VHD, VHDX, and OVA disks, but I never was successful. Recently I learned where I went wrong. I was using the "aws ec2 import-image" command., which always resulted in a failure related to missing OS files. I later learned that it appears this command can only be used to import certain approved operating systems. I should have been using the "aws ec2 import-snapshot" command which will import disk images.

I now have my own AMIs to test with.

Instance Testing

Here are the tests that I performed with t3.nano and t3a.nano instances.

Mikrotik 6.44.3 AMI -> 6.49.7 -> 7.1 -> 7.2 FAILED with disk corruption.
Mikrotik 6.44.3 AMI -> 6.49.7 -> 7.2 -> 7.3 FAILED with disk corruption.
Mikrotik 6.44.3 AMI -> 6.49.7 -> 7.3 -> 7.4 FAILED with disk corruption.
Mikrotik 6.44.3 AMI -> 6.49.7 -> 7.4 -> 7.5 FAILED with disk corruption.
Mikrotik 6.44.3 AMI -> 6.49.7 -> 7.5 -> 7.6 FAILED with disk corruption.

My 6.49.7 AMI -> 7.1 -> 7.2 FAILED with disk corruption.
My 6.49.7 AMI -> 7.1 -> 7.3 FAILED with disk corruption.
My 6.49.7 AMI -> 7.1 -> 7.4 FAILED with disk corruption.
My 6.49.7 AMI -> 7.1 -> 7.5 FAILED with disk corruption.
My 6.49.7 AMI -> 7.1 -> 7.6 FAILED with disk corruption.

My 7.1 AMI -> 7.2 -> 7.3 -> 7.4 -> 7.5 -> 7.6 SUCCESS!!! (At least that means no failures...)

I was even able to take this last instance to the current development pre-release (7.7beta9 currently) and back again a few times with no issues.

It appears that any Mikrotik EC2 T3 or T3a instance that started life as a RouterOS 6 device will succeed on the immediate upgrade to any RouterOS 7 version, but any subsequent upgrade to any other RouterOS 7 minor release will result in failure with a corrupted disk.

Proving the theory

I have tested the following with my 7.6 AMI on T3.nano and T3a.nano instances, downgrading and then upgrading the entire ROS 7.X

My 7.6 AMI -> 7.5 downgrade -> 7.4 downgrade -> 7.3 downgrade -> 7.2 downgrade -> 7.1 downgrade -> 7.2 -> 7.3 -> 7.4 -> 7.5 -> 7.6 SUCCESS the whole way!!!

It would appear that something in ROS 6 is resulting in the eventual death of ROS 7 VMs running as AWS EC2 t3 and t3a instances. On the forums, there have been reports of this occurring with other instance types, but I have not taken the time to catalog data outside of my own experiences.

Steps to create an RouterOS CHR 7.6 Amazon Machine Image

Credit for the AMI creation process goes to the clearlinux team. I found their process documented in a gihub issue linked here.

Prior to using this procedure, you will need to have a properly setup aws cli environment that has permissions (IAM Roles) allowing for vm importing and access to your S3 bucket. Here's Amazon's

documentation for adding the permissions and roles.

1. Make sure you have a properly configured AWS CLI environment.
2. Download the CHR 7.6 Raw disk image from the Mikrotik Downloads page.
3. Upload the chr-7.6.img file to an S3 bucket.
4. Create the two files shown below.
5. Update your S3Bucket and S3Key in the json file.
6. Run the following command: "bash aws-import-snapshot-mikrotik-chr-76.sh import-snapshot"
7. Grab the value of **ImportTaskId** from the output of the last command.
8. Run the following command: "bash aws-import-snapshot-mikrotik-chr-76.sh monitor-import [**ImportTaskId**]" with the **ImportTaskId** as the last argument.
9. Wait until the Status shows complete, at which time you can press CTRL-C to break the script.
10. Grab the value of **SnapshotId** from the output.
11. Run the following command: "bash aws-import-snapshot-mikrotik-chr-76.sh register-image [**SnapshotId**]" with the **SnapshotId** as the last argument.
12. Grab the value of **ImageId** from the output of the last command. If everything was successful, this is the ID of your AMI.
13. Go to the AWS control panel for EC2 -> Images -> AMIs to find your new Amazon Machine Image. You can now use it to **Launch instance from AMI**.

mikrotik-routeros-chr-76-raw-containers.json

```
{
  "Description": "Mikrotik RouterOS CHR v7.6 RAW",
  "Format": "raw",
  "UserBucket": {
    "S3Bucket": "my-s3-bucket",
    "S3Key": "mikrotik/chr-7.6.img"
  }
}
```

aws-import-snapshot-mikrotik-chr-76.sh

```
#!/bin/bash

description="Mikrotik RouterOS CHR v7.6"
json_file="mikrotik-routeros-chr-76-raw-containers.json"

arch_type="x86_64"
```

```
#arch_type="amd64"

JOB="$1"

case $JOB in
  "import-snapshot")
    aws ec2 import-snapshot --description "${description} image" --disk-container
file://${json_file}
    ;;

  "monitor-import")
    import_task_id="$2"

    while true; do
      clear
      date
      echo ""
      aws ec2 describe-import-snapshot-tasks --import-task-ids ${import_task_id}
      sleep 10
    done

    #
    #snapshot_id=$(aws ec2 describe-import-snapshot-tasks --import-task-ids ${import_task_id} |
grep SnapshotId | awk -F '"'  '{print $4}')
    #
    ;;

  "register-image")
    snapshot_id="$2"

    aws ec2 register-image \
      --name "$description" \
      --description "$description" \
      --architecture "$arch_type" \
      --virtualization-type hvm \
      --ena-support \
      --root-device-name "/dev/sda1" \
      --block-device-mappings "[{\"DeviceName\": \"/dev/sda1\", \"Ebs\": { \"SnapshotId\":
\"$snapshot_id\"}}]"
  ;;
```

```
□*)
□□echo "Unknown job type: ${JOB}"
□;;
esac
```

END

Failover for type=FWD entries in the RouterOS DNS proxy

The Mikrotik DNS resolver supports static entries with type=FWD (forward). Combining this with the regex (and now the match-subdomain option since v7.6) allows you to forward queries for specific domains to a server. Unfortunately, *the type=FWD resolver does not support any sort of failover*.

No native failover for type=FWD

The first example below shows two FWD entries for the myad.loc domain. Each entry is configured to forward-to a different DNS server, as you would expect in a normal Active-Directory environment.

```
# RouterOS 7.6 and newer example
# the second FWD entry will never actually be used
/ip dns static
add name=myad.loc ttl=1m type=FWD forward-to=10.0.0.11 match-subdomain=yes
add name=myad.loc ttl=1m type=FWD forward-to=10.0.0.12 match-subdomain=yes



# older RouterOS example
# the second and fourth FWD entries will never actually be used
/ip dns static
add regexp="myad\\.loc" ttl=1m type=FWD forward-to=10.0.0.11
add regexp="myad\\.loc" ttl=1m type=FWD forward-to=10.0.0.12
add regexp=".*\\.myad\\.loc" ttl=1m type=FWD forward-to=10.0.0.11
add regexp=".*\\.myad\\.loc" ttl=1m type=FWD forward-to=10.0.0.12
```

Because there is no failover mechanism for type=FWD entries, the second entry will never actually get used, even if the forward-to target of the first entry is offline.

There is a workaround - sort of

Since the forward-to target can be a hostname, a workaround that has been discussed on the forums is to create multiple type=A records for a fake hostname, one for each DNS server you wish to forward to, and then set the forward-to target of the type=FWD record to this overloaded fake hostname.

Here's a configuration using our myad.loc example domain:

```
# RouterOS 7.6 and newer example
/ip dns static
add name=myad.loc.rslv ttl=1m address=10.0.0.11
add name=myad.loc.rslv ttl=1m address=10.0.0.12
add name=myad.loc ttl=1m type=FWD forward-to=myad.loc.rslv match-subdomain=yes



# older RouterOS example
/ip dns static
add name=myad.loc.rslv ttl=1m address=10.0.0.11
add name=myad.loc.rslv ttl=1m address=10.0.0.12
add regexp="myad\\.loc" ttl=1m type=FWD forward-to=myad.loc.rslv
add regexp=".*\\.myad\\.loc" ttl=1m type=FWD forward-to=myad.loc.rslv
```

There is no real failover using this method, but rather "dumb round robin". If one of your servers is offline, queries will still be sent to it. Verified using Wireshark, the RouterOS DNS proxy will make five FWD attempts to one DNS server, and then pass a failure back to the client.....

... more details to come ...

:end

Notes

Stream packet sniffer to Wireshark

- Start a promiscuous capture with filter "udp port 37008"
- Setup Mikrotik Packet Sniffer to stream to your IP address

Setup system emailer

I have noticed that in RouterOS v2, the emailer uses the system identity as the HELO/EHLO host name. Some mail servers won't accept a host name with spaces or other characters. RouterOS v3 doesn't seem to be effected by this.

The following is for version 3 and 4:

```
/tool e-mail
set server=69.18.98.42:587 from="mikrotik@change.me"
/system watchdog
set auto-send-supout=yes send-email-to=notify@change.me send-smtp-server=69.18.98.42
```

The following is required for version 5:

```
/tool e-mail
set address=69.18.98.42 port=587 from="mikrotik@change.me"
/system watchdog
set auto-send-supout=yes send-email-to=notify@change.me send-smtp-server=69.18.98.42
```

NTP Client and Time Zone

```
/system clock
set time-zone-name=America/Chicago
/system ntp client
```

```
set enabled=yes mode=unicast primary-ntp=129.6.15.28 secondary-ntp=129.6.15.29
```

Google Public DNS Settings

For newer routers:

```
/ip dns
set allow-remote-requests=yes cache-max-ttl=1w cache-size=2048KiB max-udp-packet-size=512
servers=8.8.8.8,8.8.4.4
```

For older routers:

```
/ip dns
set allow-remote-requests=yes cache-max-ttl=1w primary-dns=8.8.8.8 secondary-dns=8.8.4.4
```

OpenDNS DNS Settings

For newer routers:

```
/ip dns
set allow-remote-requests=yes cache-max-ttl=1w cache-size=2048KiB max-udp-packet-size=512
servers=208.67.222.222,208.67.220.220
```

For older routers:

```
/ip dns
set allow-remote-requests=yes cache-max-ttl=1w primary-dns=208.67.222.222 secondary-
dns=208.67.220.220
```

Protecting your WAN Interface

```
# Pick your WAN input interface
# DO NOT COPY AND PASTE ALL THESE RULES!!!

/ ip firewall filter

add chain=input in-interface=ether1 action=jump jump-target=protect-wan-input src-address-
list=!allowed-management comment="Filter WAN input" disabled=no
add chain=input in-interface=ether2 action=jump jump-target=protect-wan-input src-address-
list=!allowed-management comment="Filter WAN input" disabled=no
add chain=input in-interface=ether3 action=jump jump-target=protect-wan-input src-address-
list=!allowed-management comment="Filter WAN input" disabled=no
add chain=input in-interface=ether4 action=jump jump-target=protect-wan-input src-address-
list=!allowed-management comment="Filter WAN input" disabled=no
add chain=input in-interface=ether5 action=jump jump-target=protect-wan-input src-address-
list=!allowed-management comment="Filter WAN input" disabled=no
add chain=input in-interface=ether6 action=jump jump-target=protect-wan-input src-address-
list=!allowed-management comment="Filter WAN input" disabled=no
add chain=input in-interface=ether7 action=jump jump-target=protect-wan-input src-address-
list=!allowed-management comment="Filter WAN input" disabled=no
add chain=input in-interface=ether8 action=jump jump-target=protect-wan-input src-address-
list=!allowed-management comment="Filter WAN input" disabled=no
add chain=input in-interface=ether9 action=jump jump-target=protect-wan-input src-address-
list=!allowed-management comment="Filter WAN input" disabled=no
add chain=input in-interface=ether10 action=jump jump-target=protect-wan-input src-address-
list=!allowed-management comment="Filter WAN input" disabled=no
add chain=input in-interface=ether11 action=jump jump-target=protect-wan-input src-address-
list=!allowed-management comment="Filter WAN input" disabled=no

add chain=input in-interface=pppoe action=jump jump-target=protect-wan-input src-address-
list=!allowed-management comment="Filter WAN input" disabled=no

add chain=input action=jump jump-target=protect-wan-input in-interface=vlan src-address-
list=!allowed-management comment="" disabled=no

# The protect-wan-input chain

/ ip firewall filter
add action=drop chain=protect-wan-input comment="Protect services running on the WAN
interface" disabled=no dst-port=21 protocol=tcp
```

```
add action=drop chain=protect-wan-input comment="" disabled=no dst-port=22 protocol=tcp
add action=drop chain=protect-wan-input comment="" disabled=no dst-port=23 protocol=tcp
add action=drop chain=protect-wan-input comment="" disabled=no dst-port=53 protocol=tcp
add action=drop chain=protect-wan-input comment="" disabled=no dst-port=53 protocol=udp
add action=drop chain=protect-wan-input comment="" disabled=no dst-port=80 protocol=tcp
add action=drop chain=protect-wan-input comment="" disabled=no dst-port=443 protocol=tcp
add action=drop chain=protect-wan-input comment="" disabled=no dst-port=3128 protocol=tcp
add action=drop chain=protect-wan-input comment="" disabled=no dst-port=8080 protocol=tcp
add action=drop chain=protect-wan-input comment="" disabled=no dst-port=64872-64875
protocol=tcp
add action=jump chain=protect-wan-input comment="" disabled=no jump-target=manage-icmp
protocol=icmp
add chain=protect-wan-input action=accept comment="Log traffic WAN traffic" disabled=no

# manage-icmp chain

/ ip firewall filter
add chain=manage-icmp protocol=icmp icmp-options=8:0 action=accept comment="Allow pings"
disabled=no
add chain=manage-icmp protocol=icmp icmp-options=0:0 action=accept comment="Accept responses
to our pings" disabled=no
add chain=manage-icmp protocol=icmp icmp-options=3:0 action=accept comment="# Accept
notifications of unreachable hosts" disabled=no
add chain=manage-icmp protocol=icmp icmp-options=4:0 action=accept comment="# Accept
notifications to reduce sending speed" disabled=no
add chain=manage-icmp protocol=icmp icmp-options=11:0 action=accept comment="# Accept
notifications of lost packets" disabled=no
add chain=manage-icmp protocol=icmp icmp-options=12:0 action=accept comment="# Accept
notifications of protocol problems" disabled=no
add chain=manage-icmp protocol=icmp action=drop comment="Drop all other ICMP traffic"
disabled=no
```

Traffic Marking and outbound queueing

```
/ip firewall mangle
add action=jump chain=prerouting comment="Jump to mark-traffic: MUST RETURN FROM THIS JUMP"
disabled=no jump-target=mark-traffic
```

```
add action=jump chain=output comment="Jump to mark-traffic: MUST RETURN FROM THIS JUMP"
disabled=no jump-target=mark-traffic packet-mark=no-mark
add action=mark-packet chain=mark-traffic comment="mark-traffic: default mark bulk"
disabled=no new-packet-mark=bulk passthrough=yes
add action=mark-packet chain=mark-traffic comment="mark-traffic: voice" disabled=no dst-
address-list=voice-servers new-packet-mark=voice passthrough=yes
add action=return chain=mark-traffic comment="" disabled=no packet-mark=voice
add action=return chain=mark-traffic comment="mark-traffic: end of chain return" disabled=no
```

```
/queue type
add kind=sfq name=qos sfq-allot=1514 sfq-perturb=5

/queue tree
add burst-limit=0 burst-threshold=0 burst-time=0s disabled=no limit-at=0 max-limit=0
name=queue-wan1-root packet-mark="" parent=ether1 priority=8 queue=qos
add burst-limit=0 burst-threshold=0 burst-time=0s disabled=no limit-at=0 max-limit=0
name=queue-wan1-bulk packet-mark=bulk,no-mark parent=queue-wan1-root priority=8 queue=qos
add burst-limit=0 burst-threshold=0 burst-time=0s disabled=no limit-at=0 max-limit=0
name=queue-wan1-voice packet-mark=voice parent=queue-wan1-root priority=1 queue=qos
add burst-limit=0 burst-threshold=0 burst-time=0s disabled=no limit-at=0 max-limit=0
name=queue-wan1-priority-data packet-mark=priority-data parent=queue-wan1-root priority=7
queue=qos

/queue tree
add burst-limit=0 burst-threshold=0 burst-time=0s disabled=no limit-at=0 max-limit=0
name=queue-wan2-root packet-mark="" parent=ether2 priority=8 queue=qos
add burst-limit=0 burst-threshold=0 burst-time=0s disabled=no limit-at=0 max-limit=0
name=queue-wan2-bulk packet-mark=bulk,no-mark parent=queue-wan2-root priority=8 queue=qos
add burst-limit=0 burst-threshold=0 burst-time=0s disabled=no limit-at=0 max-limit=0
name=queue-wan2-voice packet-mark=voice parent=queue-wan2-root priority=1 queue=qos
add burst-limit=0 burst-threshold=0 burst-time=0s disabled=no limit-at=0 max-limit=0
name=queue-wan2-priority-data packet-mark=priority-data parent=queue-wan2-root priority=7
queue=qos
```

Best Effort Queuing with Global-In and Guaranteed Queuing on outbound with two ISPs and connection tracking

This sets up three root queues: queue-root-global-in (best effort), queue-root-isp1 (guaranteed), queue-root-isp2 (guaranteed).

queue-root-global-in deals with traffic coming from the internet to the router and catches traffic that is bound for the router itself as well as traffic that will be forwarded through to NAT clients. There is a subqueue for each isp.

queue-root-isp1 deals with the outbound traffic to isp1 from the router as well as NAT clients behind the router.

queue-root-isp2 deals with the outbound traffic to isp2 from the router as well as NAT clients behind the router.

The traffic that is handled in these last two queues is marked by the mark-traffic mangle chain. The packet marks are generic to the type of traffic (bulk, priority, voice) because the root queues are connected to specific interfaces.

The traffic that is handled in the global-in queue is marked by rules in the prerouting chain. The packets marks are specific to the interface that the traffic came in on (isp1-bulk, isp2-bulk, etc) because the root queue is not connected to a specific interface but to global-in, which is an aggregate of ALL incoming packets on ALL interfaces.

```
/queue type
add kind=sfq name=qos sfq-allot=1514 sfq-perturb=5


/queue tree
add burst-limit=0 burst-threshold=0 burst-time=0s comment="isp1 outbound queue" disabled=no
limit-at=128k max-limit=100M name=queue-root-isp1 parent=ether1 priority=8 queue=qos
add burst-limit=0 burst-threshold=0 burst-time=0s disabled=no limit-at=128k max-limit=100M
name=isp1-bulk packet-mark=bulk,no-mark parent=queue-root-isp1 priority=8 queue=qos
add burst-limit=0 burst-threshold=0 burst-time=0s disabled=no limit-at=128k max-limit=100M
name=isp1-priority packet-mark=priority parent=queue-root-isp1 priority=7 queue=qos
add burst-limit=0 burst-threshold=0 burst-time=0s disabled=no limit-at=128k max-limit=100M
name=isp1-voice packet-mark=voice parent=queue-root-isp1 priority=1 queue=qos

add burst-limit=0 burst-threshold=0 burst-time=0s comment="isp2 outbound queue" disabled=no
```

```
limit-at=128k max-limit=100M name=queue-root-isp2 parent=ether2 priority=8 queue=qos
add burst-limit=0 burst-threshold=0 burst-time=0s disabled=no limit-at=128k max-limit=100M
name=isp2-bulk packet-mark=bulk,no-mark parent=queue-root-isp2 priority=8 queue=qos
add burst-limit=0 burst-threshold=0 burst-time=0s disabled=no limit-at=128k max-limit=100M
name=isp2-priority packet-mark=priority parent=queue-root-isp2 priority=7 queue=qos
add burst-limit=0 burst-threshold=0 burst-time=0s disabled=no limit-at=128k max-limit=100M
name=isp2-voice packet-mark=voice parent=queue-root-isp2 priority=1 queue=qos

add burst-limit=0 burst-threshold=0 burst-time=0s disabled=no limit-at=0 max-limit=0
name=global-in-root parent=global-in priority=8 comment="inbound queue root" queue=qos

add burst-limit=0 burst-threshold=0 burst-time=0s disabled=no limit-at=128k max-limit=100M
name=isp1-from-internet-root parent=global-in-root priority=8 comment="isp1 inbound queue"
queue=qos
add burst-limit=0 burst-threshold=0 burst-time=0s disabled=no limit-at=128k max-limit=100M
name=isp1-fi-bulk packet-mark=isp1-fi-bulk parent=isp1-from-internet-root priority=8 queue=qos
add burst-limit=0 burst-threshold=0 burst-time=0s disabled=no limit-at=128k max-limit=100M
name=isp1-fi-priority packet-mark=isp1-fi-priority parent=isp1-from-internet-root priority=7
queue=qos
add burst-limit=0 burst-threshold=0 burst-time=0s disabled=no limit-at=128k max-limit=100M
name=isp1-fi-voice packet-mark=isp1-fi-voice parent=isp1-from-internet-root priority=1
queue=qos

add burst-limit=0 burst-threshold=0 burst-time=0s disabled=no limit-at=128k max-limit=100M
name=isp2-from-internet-root parent=global-in-root priority=8 comment="isp2 inbound queue"
queue=qos
add burst-limit=0 burst-threshold=0 burst-time=0s disabled=no limit-at=128k max-limit=100M
name=isp2-fi-bulk packet-mark=isp2-fi-bulk parent=isp2-from-internet-root priority=8 queue=qos
add burst-limit=0 burst-threshold=0 burst-time=0s disabled=no limit-at=128k max-limit=100M
name=isp2-fi-priority packet-mark=isp2-fi-priority parent=isp2-from-internet-root priority=7
queue=qos
add burst-limit=0 burst-threshold=0 burst-time=0s disabled=no limit-at=128k max-limit=100M
name=isp2-fi-voice packet-mark=isp2-fi-voice parent=isp2-from-internet-root priority=1
queue=qos
```

These are the associated firewall rules:

```
/ip firewall mangle
add action=jump chain=prerouting comment="Jump to mark-traffic: MUST RETURN FROM THIS JUMP"
```

```
disabled=no jump-target=mark-traffic

add action=mark-packet chain=prerouting comment="isp1 global-in packet marking - bulk"
disabled=no in-interface=ether1 new-packet-mark=isp1-fi-bulk passthrough=yes
add action=mark-packet chain=prerouting comment="isp1 global-in voice" disabled=no in-
interface=ether1 new-packet-mark=isp1-fi-voice passthrough=no src-address-list=voice-servers
add action=mark-packet chain=prerouting comment="isp1 global-in priority placeholder"
disabled=yes in-interface=ether1 new-packet-mark=isp1-fi-priority passthrough=no src-
address=1.1.1.1

add action=mark-packet chain=prerouting comment="isp2 global-in packet marking - bulk"
disabled=no in-interface=ether2 new-packet-mark=isp2-fi-bulk passthrough=yes
add action=mark-packet chain=prerouting comment="isp2 global-in voice" disabled=no in-
interface=ether2 new-packet-mark=isp2-fi-voice passthrough=no src-address-list=voice-servers
add action=mark-packet chain=prerouting comment="isp2 global-in priority placeholder"
disabled=yes in-interface=ether2 new-packet-mark=isp2-fi-priority passthrough=no src-
address=2.2.2.2

add action=jump chain=output comment="Jump to mark-traffic: MUST RETURN FROM THIS JUMP"
disabled=no jump-target=mark-traffic packet-mark=no-mark

add action=mark-connection chain=prerouting comment="isp1 connection tracking" connection-
state=new disabled=no in-interface=ether1 new-connection-mark=isp1 passthrough=no
add action=mark-routing chain=prerouting connection-mark=isp1 disabled=no in-interface=!ether1
new-routing-mark=isp1 passthrough=no
add action=mark-routing chain=output connection-mark=isp1 disabled=no new-routing-mark=isp1
passthrough=no src-address=1.1.1.0/30

add action=mark-connection chain=prerouting comment="isp2 connection tracking" connection-
state=new disabled=no in-interface=ether2 new-connection-mark=isp2 passthrough=no
add action=mark-routing chain=prerouting connection-mark=isp2 disabled=no in-interface=!ether2
new-routing-mark=isp2 passthrough=no
add action=mark-routing chain=output connection-mark=isp2 disabled=no new-routing-mark=isp2
passthrough=no src-address=2.2.2.0/30

add action=mark-packet chain=mark-traffic comment="mark-traffic: default mark bulk"
disabled=no new-packet-mark=bulk passthrough=yes
add action=mark-packet chain=mark-traffic comment="mark-traffic: voice" disabled=no dst-
address-list=voice-servers new-packet-mark=voice passthrough=yes
add action=return chain=mark-traffic disabled=no packet-mark=voice
```

```
add action=mark-packet chain=mark-traffic comment="mark-traffic: priority (placeholder)"
disabled=yes dst-address=1.1.1.1 new-packet-mark=priority passthrough=yes
add action=return chain=mark-traffic disabled=yes packet-mark=priority

add action=return chain=mark-traffic comment="mark-traffic: end of chain return" disabled=no
```

These are the needed routing table entries:

```
/ip route
add check-gateway=ping comment="default route via isp1" disabled=no distance=1 dst-
address=0.0.0.0/0 gateway=1.1.1.1
add check-gateway=ping comment="default route via isp2" disabled=no distance=20 dst-
address=0.0.0.0/0 gateway=2.2.2.1

add check-gateway=ping comment="isp1 default route" disabled=no dst-address=0.0.0.0/0
gateway=1.1.1.1 routing-mark=isp1
add check-gateway=ping comment="isp2 default route" disabled=no dst-address=0.0.0.0/0
gateway=2.2.2.1 routing-mark=isp2
```

Enable/Disable Services

```
/ ip service
set telnet port=23 address=0.0.0.0/0 disabled=no
set ftp port=21 address=0.0.0.0/0 disabled=yes
set www port=80 address=0.0.0.0/0 disabled=yes
set ssh port=22 address=0.0.0.0/0 disabled=no
set www-ssl port=443 address=0.0.0.0/0 certificate=none disabled=yes
```

Enable/Disable Service Ports

```
/ ip firewall service-port
set ftp ports=21 disabled=no
```

```
set tftp ports=69 disabled=no
set irc ports=6667 disabled=no
set h323 disabled=yes
set quake3 disabled=no
set gre disabled=no
set pptp disabled=no
```

Initial SNMP configuration

This simply turns on SNMP and sets the public community to only be access from localhost, which renders it useless.

Add your own community entry to make use of SNMP, but I recommend not deleting the public entry. This is due to an issue in the Mikrotik export function for SNMP.

```
/snmp
set contact="" enabled=yes engine-boots=0 engine-id="" location="" \
    time-window=15 trap-sink=0.0.0.0 trap-version=1
/snmp community
set public address=127.0.0.1/32 authentication-password="" \
    authentication-protocol=MD5 encryption-password="" encryption-protocol=\
    DES name=public read-access=yes security=none write-access=no
```

For v5:

```
/snmp
set contact="" enabled=yes engine-id="" location="" trap-community=public \
    trap-target=0.0.0.0 trap-version=1
/snmp community
set public address=127.0.0.1/32 authentication-password="" \
    authentication-protocol=MD5 encryption-password="" encryption-protocol=DES \
    name=public read-access=yes security=none write-access=no
add address=0.0.0.0/0 authentication-password="" authentication-protocol=MD5 \
    encryption-password="" encryption-protocol=DES name=localmon read-access=\
    yes security=none write-access=no
/snmp
set contact="" enabled=yes engine-id="" location="" trap-community=public \
```

```
    trap-target=0.0.0.0 trap-version=1
```

Protecting your LAN

```
/ip firewall filter
add chain=protect-lan connection-state=invalid action=drop comment="Drop invalid packets"
disabled=no
add chain=protect-lan connection-state=established action=accept comment="Allow established
traffic to pass" disabled=no
add chain=protect-lan connection-state=related action=accept comment="Allow related traffic to
pass" disabled=no
add chain=protect-lan action=drop comment="Drop everything else" disabled=no
```

Private IP Subnet address lists

```
/ip firewall address-list
add address=10.0.0.0/8 comment="private 10.0.0.0/255.0.0.0" disabled=no list=private-ip-
subnets
add address=172.16.0.0/12 comment="private 172.16.0.0/255.240.0.0" disabled=no list=private-
ip-subnets
add address=192.168.0.0/16 comment="private 192.168.0.0/255.255.0.0" disabled=no list=private-
ip-subnets
```

Dealing with SPAM from inside

These rules will allow outbound smtp from valid internal addresses, block it from ip's that we think are compromised, and track connections to determine if we think an ip is compromised.

```
/ip firewall filter
add action=jump chain=forward comment="Push outbound SMTP traffic to the filter-smtp chain -
check address lists for banned IPs" disabled=no dst-port=25 \
    in-interface=bridge-lan jump-target=filter-smtp protocol=tcp
```

```
/ip firewall filter
add action=drop chain=filter-smtp comment="SPAM: Block SMTP from blacklist static list"
disabled=no \
    src-address-list=smtp-possible-spammers-static
add action=add-src-to-address-list address-list=smtp-possible-spammers address-list-timeout=9m
\
    chain=filter-smtp comment=\
    "SPAM: Test outbound connections for connection limit for whitelisted limit" connection-
limit=\
    10,32 disabled=no dst-port=25 protocol=tcp src-address-list=smtp-allowed-outbound
add action=add-src-to-address-list address-list=smtp-possible-spammers address-list-timeout=9m
\
    chain=filter-smtp comment="SPAM: Test outbound connections for connection limit" \
    connection-limit=2,32 disabled=no dst-port=25 protocol=tcp src-address-list=\
    !smtp-allowed-outbound
add action=log chain=filter-smtp comment="SPAM: Log SMTP from blacklist" disabled=no log-
prefix=\
    possible-spammer src-address-list=smtp-possible-spammers
add action=drop chain=filter-smtp comment="SPAM: Block SMTP from blacklist" disabled=no \
    src-address-list=smtp-possible-spammers
add action=return chain=filter-smtp comment="SPAM: Good packet... return" disabled=no
```

Once this is done, we need to be notified somehow. This is done with a script that runs every X minutes. The script sends a single email for each address listed. Add addresses to the smtp-possible-spammers list for 10 minutes (or more) and run this scripts every 5 minutes.

```
:local spamadmin notify@change.me

:local count 0
:local message ""
:local tmp

:foreach i in=[/ip firewall address-list find list=smtp-possible-spammers] \
do={ \
:set count ($count + 1)
:set tmp ([/ip firewall address-list get $i address])
:set message ($message . $tmp . "\r\n")
:log warning ("possible spammfer found at " . $tmp)
}
```

```
:if ($count > 0) \
do={ \
:log info "watch-for-spammers sending notification"
/tool e-mail send \
     to=$spamadmin \
     subject=([/system identity get name] . ": $count possible spammers found") \
     body=$message
}

Paste the following in a terminal to create the above script:

/system script
add name=watch-for-spammers source=":local spamadmin notify@change.me\r\
    \n\r\
    \n:local count 0\r\
    \n:local message \"\"\r\
    \n:local tmp\r\
    \n\r\
    \n:foreach i in=[/ip firewall address-list find list=smtp-possible-spammer\
    s] \\\r\
    \ndo={ \\\r\
    \n:set count (\$count + 1)\r\
    \n:set tmp ([/ip firewall address-list get \$i address])\r\
    \n:set message (\$message . \$tmp . \"\\r\\n\")\r\
    \n:log warning (\"possible spammfer found at \" . \$tmp)\r\
    \n}\r\
    \n\r\
    \n:if (\$count > 0) \\\r\
    \ndo={ \\\r\
    \n:log info \"watch-for-spammers sending notification\"\r\
    \n/tool e-mail send \\\r\
    \n     to=\$spamadmin \\\r\
    \n     subject=([/system identity get name] . \": \$count possible spammer\
    s found\") \\\r\
    \n     body=\$message\r\
    \n}\r\
    \n"
```

This is the line to add the scheduled task.

```
/system scheduler
add comment="" disabled=no interval=5m name="check-spammer-list" on-event="/system script run
watch-for-spammers" \
    start-date=jan/01/1970 start-time=00:00:00
```

An alternate method is to allow outbound SMTP only from a specified list of IP's. The rules below allow outbound SMTP from addresses on the list smtp-allowed-outbound, and logs all other tries to smtp-possible-spammers followed by the drop.

```
/ ip firewall filter
add chain=lan-forward-out action=accept dst-port=25 protocol=tcp \
    src-address-list=smtp-allowed-outbound comment="SPAM: Allow traffic from \
    whitelist" disabled=no
add chain=lan-forward-out action=add-src-to-address-list dst-port=25 \
    protocol=tcp address-list=smtp-possible-spammers address-list-timeout=0s \
    comment="Log all other outbound SMTP" disabled=no
add chain=lan-forward-out action=drop dst-port=25 protocol=tcp comment="Drop \
    all other outbound SMTP" disabled=no
```

Scripting

```
# list addresses in visisted-mailserver address-list
/ip firewall address-list
:foreach i in [find list=visited-mailservers ] do={:put [get $i address]}
```

Automated Backups

Make sure you change the smtpserver value to a valid SMTP server for your Internet connection.

```
:log info "backup Beginning now"
:local toaddress systembackup@change.me

:global subject ([/system identity get name] . " Backup " . [/system clock get time])
```

```
:global backupfile ([/system identity get name] . "_backup")

:log info "backup Backing up config"
/export file="$backupfile"

:log info "backup pausing for 3s"
:delay 3s

:log info "backup being emailed"
/tool e-mail send to=$toaddress subject=$subject file="$backupfile.rsc"

:log info "backup finished"
```

Paste the following in a terminal to create the above script:

```
/system script
add name=backup-router
policy=ftp,reboot,read,write,policy,test,winbox,password,sniff,sensitive source=":log info
\"backup\
    \_Beginning now\"\r\
    \n:local toaddress systembackup@change.me\r\
    \n\r\
    \n:global subject ([/system identity get name] . \" Backup \" . [/system clock get
time])\r\
    \n:global backupfile ([/system identity get name] . \"_backup\")\r\
    \n\r\
    \n:log info \"backup Backing up config\"\r\
    \n/export file=\"\$backupfile\"\r\
    \n\r\
    \n:log info \"backup pausing for 3s\"\r\
    \n:delay 3s\r\
    \n\r\
    \n:log info \"backup being emailed\"\r\
    \n/tool e-mail send to=\$toaddress subject=\$subject file=\"\$backupfile.rsc\"\r\
    \n\r\
    \n:log info \"backup finished\"\r\
    \n"
```

If you want the router to automatically email you the backup on an interval use the following script:

```
/system scheduler
add disabled=no interval=1w name=backup-router-weekly on-event="/system script run backup-
router \r\n"\
    start-date=jan/01/2012 start-time=01:00:00
```

Netwatching

This will send an email on up and down:

```
/tool netwatch
add comment="some-device" disabled=no \
down-script="/tool e-mail send to=email@domain.com subject=\"some-device down\"" \
up-script="/tool e-mail send to=email@domain.com subject=\"some-device up\"" \
host=1.1.1.1
```

This will add an entry to the log on up and down:

```
/tool netwatch
add comment="some-device" disabled=no \
    down-script="/log warning message=\"some-device down\"" \
    up-script="/log warning message=\"some-device up\"" \
    host=1.1.1.1 interval=10s timeout=1s
```

Clearing the arp cache

The following script will clear the arp cache every $delaytime a total of $numloops times.

```
:log info "clearing arp table of dynamic entries"
:local counter 0
:local delaytime 5
:local numloops 12
```

```
:while ($counter < $numloops) do={ \

:log info "clearing arp loop"

:foreach i in=[/ip arp find dynamic=yes] do={ \
/ip arp remove $i
}

:log info "delaying..."

:delay $delaytime

}
```

Clear connections

This script clears the connection tracking table:

```
add name=clear-connections
policy=ftp,reboot,read,write,policy,test,winbox,password,sniff,sensitive,api source=":log info
message=\"clearing connections begin\
    \"\r\
    \n:foreach i in=[/ip firewall connection find] do={/ip firewall connection remove \$i}\r\
    \n:log info message=\"clearing connections end\"\r\
    \n"
```

Upgrade timing

```
RouterBoard 150

RouterOS 2.9.46, BIOS 2.9 -> RouterOS 2.9.51: 2m45s
RouterOS 2.9.51, BIOS 2.9 -> BIOS 2.12: 30s

RouterOS 2.9.51, BIOS 2.12 -> RouterOS 3.9: 2m5s
RouterOS 2.9.51, BIOS 2.12 -> RouterOS 3.9: 2m0s
```

```
RouterOS 3.9, BIOS 2.12 -> BIOS 2.14: 28s
RouterOS 3.9, BIOS 2.12 -> BIOS 2.14: 28s
```

OSPF Route Filtering

```
/routing filter
add action=accept chain=ospf-private-only-out comment="" disabled=no invert-match=no
prefix=10.0.0.0/8 prefix-length=8-32
add action=accept chain=ospf-private-only-out comment="" disabled=no invert-match=no
prefix=172.16.0.0/12 prefix-length=12-32
add action=accept chain=ospf-private-only-out comment="" disabled=no invert-match=no
prefix=192.168.0.0/16 prefix-length=16-32
add action=discard chain=ospf-private-only-out comment="" disabled=no invert-match=no
add action=accept chain=ospf-private-only-in comment="" disabled=no invert-match=no
prefix=10.0.0.0/8 prefix-length=8-32
add action=accept chain=ospf-private-only-in comment="" disabled=no invert-match=no
prefix=172.16.0.0/12 prefix-length=12-32
add action=accept chain=ospf-private-only-in comment="" disabled=no invert-match=no
prefix=192.168.0.0/16 prefix-length=16-32
add action=discard chain=ospf-private-only-in comment="" disabled=no invert-match=no

/routing ospf instance
set [ find default=yes ] disabled=no distribute-default=never in-filter=ospf-private-only-in
metric-bgp=auto metric-connected=20 metric-default=1 \
    metric-other-ospf=auto metric-rip=20 metric-static=20 name=default out-filter=ospf-
private-only-out redistribute-bgp=no redistribute-connected=as-type-1 \
    redistribute-other-ospf=no redistribute-rip=no redistribute-static=no router-id=0.0.0.0
```

Hotspot and Apple IOS

http://forum.mikrotik.com/viewtopic.php?f=2&t=42942 http://www.cadincweb.com/why-your-apple-ios-7-device-wont-connect-to-the-wifi-network

```
/ip hotspot profile set hsprof1 dns-name=""
/ip hotspot walled-garden
add action=allow disabled=no dst-host=www.appleiphonecell.com dst-port=""
add action=allow disabled=no dst-host=captive.apple.com dst-port=""
add action=allow disabled=no dst-host=www.apple.com dst-port=""
path=/library/test/success.html
```

Send email with attached log on startup

```
/system scheduler
add comment="" disabled=no interval=0s name=startup-notify on-event="/log print
file=mikrotik.log.txt\r\
    \n/tool e-mail send to=notify@change.me subject=\"\$[/system identity get name] startup at
\$[/system c\
    lock get time] \$[/system clock get date]\" body=\"See attached log file\"
file=mikrotik.log.txt\r\
    \n" policy=ftp,reboot,read,write,policy,test,winbox,password,sniff,sensitive start-
time=startup
```

Private use MAC addresses

The following range of MAC Addresses are reserved for private use:

```
AC:DE:48:00:00:00 to AC:DE:48:FF:FF:FF
```

When creating bridge interfaces on the Mikrotik router, create an admin MAC address using this range. I pull the last three octets from an actual device on the router.

Pantech UML290

What makes it work is the phone number: ***99***3#**

```
/interface ppp-client
add add-default-route=yes allow=pap,chap,mschap1,mschap2 data-channel=0 \
    dial-command=ATDT dial-on-demand=no disabled=no info-channel=0 \
```

```
    keepalive-timeout=30 max-mru=1500 max-mtu=1500 modem-init="" mrru=disabled \
    name=ppp-out1 null-modem=no password="" phone=*99***3# pin="" port=usb2 \
    profile=default use-peer-dns=yes user=""
```

```
/interface ppp-client
set 0 add-default-route=yes allow=pap,chap,mschap1,mschap2 data-channel=0 \
    dial-command=ATDT dial-on-demand=no disabled=no info-channel=0 \
    keepalive-timeout=30 max-mru=1500 max-mtu=1500 modem-init="" mrru=disabled \
    name=ppp-out-cellular null-modem=no password="" phone=*99***3# pin="" port=usb2 \
    profile=default use-peer-dns=yes user=""
```

Sprint - Sierra Wireless 598

```
/interface ppp-client
add add-default-route=yes allow=pap,chap,mschap1,mschap2 data-channel=0 \
    dial-command=ATDT dial-on-demand=no disabled=no info-channel=0 \
    keepalive-timeout=30 max-mru=1500 max-mtu=1500 modem-init="" mrru=disabled \
    name=ppp-out-cellular null-modem=no password="" phone=#777 pin="" port=usb1 \
    profile=default use-peer-dns=no user=""
```

IPSEC/IPIP/MSS Mangling

```
MSS should be set to 40 bytes less than the MTU of the circuit.
All caluclations below assume a circuit the supports a maximum MTU of 1500 bytes.
If these tunnels traverse a PPPoE circuit, an additional 20 bytes would need to be subtracted
for PPPoE overhead.

IPSEC Max Overhead: 58 bytes (depends on tunnel/transport/ESP/AH)
IPIP Tunnel Overhead: 50 bytes
GRE Tunnel Overhead: 24 bytes
EOIP Tunnel Overhead: None due to fragmentation support

MSS without IPSEC:
```

```
GRE Tunnel  : MTU 1476 - 40 = MSS 1436 (If MSS >= 1437-65535, change mss to 1436)
IPIP Tunnel : MTU 1450 - 40 = MSS 1410 (If MSS >= 1411-65535, change mss to 1410)

MSS with IPSEC:
EOIP Tunnel :
GRE Tunnel  : MTU 1476 - 58 - 40 = MSS 1378 (If MSS >= 1379-65535, change mss to 1378)
IPIP Tunnel : MTU 1450 - 58 - 40 = MSS 1352 (If MSS >= 1353-65535, change mss to 1352)

To be on the safe side, you could just create a generic rule to change the MSS down to 1350.
Doing this sacrifices anywhere from 2 to 86 bytes, but covers your bases for all tunnel types.
```

Rule sets for MSS 1350

```
/ip firewall mangle
add action=jump chain=forward in-interface=ipip- jump-target=change-mss
add action=jump chain=forward out-interface=ipip- jump-target=change-mss

add action=change-mss chain=change-mss comment="change-mss - change TCP MSS - currently set to
1350" new-mss=1350 passthrough=no protocol=tcp tcp-flags=syn tcp-mss=1351-65535
add action=return chain=change-mss comment="change-mss - return - enable if needed - delete if
not" disabled=yes
```

Rule sets for MSS 1330

```
/ip firewall mangle
add action=jump chain=forward in-interface=ipip- jump-target=change-mss
add action=jump chain=forward out-interface=ipip- jump-target=change-mss

add action=change-mss chain=change-mss comment="change-mss - change TCP MSS - currently set to
1330" new-mss=1330 passthrough=no protocol=tcp tcp-flags=syn tcp-mss=1331-65535
add action=return chain=change-mss comment="change-mss - return - enable if needed - delete if
not" disabled=yes
```

Rule sets for MSS 1300

```
/ip firewall mangle
add action=jump chain=forward in-interface=ipip- jump-target=change-mss
add action=jump chain=forward out-interface=ipip- jump-target=change-mss

add action=change-mss chain=change-mss comment="change-mss - change TCP MSS - currently set to
1300" new-mss=1300 passthrough=no protocol=tcp tcp-flags=syn tcp-mss=1301-65535
add action=return chain=change-mss comment="change-mss - return - enable if needed - delete if
not" disabled=yes
```

DNS Changer IP Subnets

```
/ip firewall address-list
add address=85.255.112.0/20 disabled=no list=DNSchanger
add address=67.210.0.0/20 disabled=no list=DNSchanger
add address=93.188.160.0/21 disabled=no list=DNSchanger
add address=77.67.83.0/24 disabled=no list=DNSchanger
add address=213.109.64.0/20 disabled=no list=DNSchanger
add address=64.28.176.0/20 disabled=no list=DNSchanger
```

Web proxy blocking IP based URLs

I had a customer today tell me that their Barracuda web filter is the only device they've found to date that can do IP based URL blocking. He said he knows Fortinet and Sonicwall can't do it, and Palo Alto said they might be able to. The proxy access rule below for the Mikrotik does just that:

```
/ip proxy access
add action=deny dst-host=":([0-9]{1,3})\\.([0-9]{1,3})\\.([0-9]{1,3})\\.([0-9]{1,3})"
```

Writing files in RouterOS

Source

Notes:

- While you can fetch and read the contents of any file, you are limited to working with 4096 character files as this is a limitation on the amount of information that can be contained in a string variable in RouterOS at this time.
- When creating new files in RouterOS via terminal the extension .txt will be appended to anything that doesn't already have .txt at the end.
- You can work with newlines \n\r as delimeters (which is super helpful when downloading something list of IP addresses from somewhere)

```
The basic commands for working with a file, using variables in place of static content or file
names:
1. To create a new file
/file print file=$filename

2. To read an existing file
:set $filedata [/file get $filename contents]

3. To write to an existing file
/file set $filename contents=$newdata

4. To append to an existing file
/file set $filename contents=([get $filename contents] . $newdata)
```

PoE Budgets and Specs

hEX PoE (RB960PGS) and PowerBox Pro (RB906PGS-PB)

- 5 Gigabit Ethernet ports, 1 Gigabit SFP cage
  - SFP cage is not connected to the switch chip. Wire-speed switching on the SFP port is not supported
- Single core 400 Mhz, 128 MB RAM, 16 MB flash
- Port 1 supports passive (24V) or active (802.3 af/at) PoE input to power the device
- Ports 2-5 support passive or active PoE output, depending on the input voltage
  - if 48-57 V input voltage is used, output supports 802.3 af/at mode B (4,5+)(7,8-) compatible devices
- The power consumption of this device under maximum load with attachments is 59 W. Without attachments is 6 W.
- **Output power budgets**
  - Total output max: 2 A (should probably be stated as 48 W instead)
    - 24 V * 2 A = **48 W**
    - 48 V * 1 A = **48 W**
  - Per port output maximums
    - Input voltage: 12-30 V
      - Per port output max: 1 A
        - 24 V * 1 A = 24 W
    - Input voltage: 31-57 V
      - Per port output max: 450 ma
        - 48 V * 450 ma = **21.6 W**

CRS112-8P-4S-IN

- 8 Gigabit Ethernet ports, 4 Gigabit SFP cages
- Single core 400 Mhz, 128 MB RAM, 16 MB flash
- Dual power inputs on the back. Allows support for simultaneous passive and active PoE
  - 18-28 V
  - 48-57 V
- Ports 1-8 support passive or active PoE output, depending on the input voltage
  - if 48-57 V input voltage is used, output supports 802.3 af/at mode B (4,5+)(7,8-) compatible devices
- **Output power budgets**
  - Total output maximums
    - 24 V * 2.8 A = 67.2 W
    - 48 V * 1.4 A = **67.2 W**
  - Per port output maximums

        - Input voltage: 12-30 V
            - Per port output max: 1 A
                - 24 V * 1 A = 24 W
        - Input voltage: 31-57 V
            - Per port output max: 450 ma
                - 48 V * 450 ma = **21.6 W**

CSS610-8P-2S+IN

- 8 Gigabit Ethernet ports, 2 10 Gigabit SFP+ cages
- **SwitchOS** lite only (no RouterOS)
- Power input on the front of the switch:
    - 12-57 V via 5.5 mm power jack
- Ports 1-8 support passive or active PoE output, depending on the input voltage
    - if 48-57 V input voltage is used, output supports 802.3 af/at mode B (4,5+)(7,8-) compatible devices
- Max power consumption with attachments is 162 W. Without attachments is 12 W.
- **Output power budgets**
    - Total output maximums: **140 W**
    - Per port output maximums
        - Input voltage: 12-30 V
            - Per port output max: 1 A
                - 24 V * 1 A = 24 W
        - Input voltage: 31-57 V
            - Per port output max: 625 ma
                - 48 V * 625 ma = **30 W**

netPower 16P

- 16 Gigabit Ethernet ports, 2 10 Gigabit SFP+ cages
- RouterOS or SwitchOS
- ARM 32-bit Single core 800 Mhz, 256 MB RAM, 16 MB flash
    - Dual power inputs on the back. Allows support for simultaneous passive and active PoE
        - 18-30 V
        - 48-57 V
- Ports 1-16 support passive or active PoE output, depending on the input voltage
    - if 48-57 V input voltage is used, output supports 802.3 af/at mode B (4,5+)(7,8-) compatible devices
- Max power consumption with attachments is 325 W. Without attachments is 21 W.
- **Output power budgets**
    - Total output maximums: **140 W**
    - Max PoE-out on low (<30 V) voltage: 5.6 A: 2.8 A per 8 port group, max 1.1 A per port

    - Max PoE-out on high (>30 V) voltage: 2.8 A (**134.4 W)**: 1.4 A per 8 port group (**67.2 W**), max 0.6 A per port (**28.8 W**)
    - Per port output maximums
        - Input voltage: 12-30 V
            - Per port output max: 1 A
                - 24 V * 1 A = 24 W
        - Input voltage: 31-57 V
            - Per port output max: 625 ma
                - 48 V * 625 ma = **30 W**

CRS328-24P-4S+RM

- 500 W power supply built-in
- The device consumes up to 44 W leaving guaranteed 450 W (3 x 150 W per every 8 Ethernet port group)
- Each port can provide up to 30 W of power with any power output option you choose.
- Power output options: Passive PoE, low voltage PoE, 802.3af/at (Type 1 “PoE” / Type 2 “PoE+”) with auto-sensing. PoE-Out is passed over mode B pins (4,5+)(7,8-).

CRS354-48P-4S+2Q+RM

- 750 W power supply built-in
- Each port can provide up to 30 W of power with any power output option you choose.
- Power output options: Passive PoE, low voltage PoE, 802.3af/at (Type 1 “PoE” / Type 2 “PoE+”) with auto-sensing. PoE-Out is passed over mode B pins (4,5+)(7,8-).
- Output per port (53V out) 570 mA (30 W)
- Output per port (26V out) 1000 mA (26 W)
- Total output power 700 W
- Total output 27 A at 26 V (702 W), or 13.2 A at 53 V (699.6 W).

#end

Recursive routing in RouterOS 6 vs 7

Recursive routing allows you to create a route with a defined next hop that is not actually directly adjacent to the router.

The working example configurations below assume three distinct Internet connections from three different providers. Each connection is serviced by a provider supplied modem/router combo CPE device running NAT with 192.168.1/2/3.1 IP addresses on the respective LAN interfaces, meaning if the Internet connection in front of any one modem fails, the Mikrotik router connected behind the provider CPE device will still be able to ping its immediate default gateway of 192.168.1/2/3.1. This is where recursive lookups come in.

RouterOS 6 working example configuration

ROSv6 does not enforce the rules related to scope and target-scope for rules that use recursive lookups. This is important to note when upgrading from ROSv6 to v7 as those rules will no longer work after the upgrade, until you fix the target-scopes.

RouterOS 7 principles

ROSv7 adds a slight bit of complexity as it actually enforces some rules related to scope and target-scope that ROSv6 did not. The relevant documentation is located on the Router OS IP Routing page under the Nexthop Lookup section.

The static entries that define your recursive routes need to have scope=10 target-scope=10.

The static entries that use a recursive routes as the gateway need to have scope=30 target-scope=11.

The key here is the target-scope of the route must be larger than the scope of the defined recursive route being used at the gateway in order to affect the change in the next-hop attribute.

RouterOS 7 working example configuration

```
/routing table
add fib name=isp1
add fib name=isp2
add fib name=isp3

/ip/route

#
# recursive lookup entries
#
add disabled=no distance=1 dst-address=1.1.1.1/32         gateway=192.168.1.1 routing-
table=main scope=10 target-scope=10 comment="STATIC ROUTE FOR RECURSIVE ROUTING - via isp1 -
Cloudflare primary   DNS server"
add disabled=no distance=1 dst-address=1.0.0.1/32         gateway=192.168.2.1 routing-
table=main scope=10 target-scope=10 comment="STATIC ROUTE FOR RECURSIVE ROUTING - via isp2 -
Cloudflare secondary DNS server"

add disabled=no distance=1 dst-address=8.8.8.8/32         gateway=192.168.1.1 routing-
table=main scope=10 target-scope=10 comment="STATIC ROUTE FOR RECURSIVE ROUTING - via isp1 -
Google primary   DNS server"
add disabled=no distance=1 dst-address=8.8.4.4/32         gateway=192.168.2.1 routing-
table=main scope=10 target-scope=10 comment="STATIC ROUTE FOR RECURSIVE ROUTING - via isp2 -
Google secondary DNS server"
add disabled=no distance=1 dst-address=4.2.2.2/32         gateway=192.168.3.1 routing-
table=main scope=10 target-scope=10 comment="STATIC ROUTE FOR RECURSIVE ROUTING - via isp3 -
Google tertiary  DNS server"

add disabled=no distance=1 dst-address=9.9.9.9/32         gateway=192.168.1.1 routing-
table=main scope=10 target-scope=10 comment="STATIC ROUTE FOR RECURSIVE ROUTING - via isp1 -
Quad9 primary   DNS server"
add disabled=no distance=1 dst-address=149.112.112.112/32 gateway=192.168.2.1 routing-
table=main scope=10 target-scope=10 comment="STATIC ROUTE FOR RECURSIVE ROUTING - via isp2 -
Quad9 secondary DNS server"
add disabled=no distance=1 dst-address=9.9.9.11/32        gateway=192.168.3.1 routing-
table=main scope=10 target-scope=10 comment="STATIC ROUTE FOR RECURSIVE ROUTING - via isp3 -
Quad9 primary   EDNS server"
add disabled=no distance=1 dst-address=149.112.112.11/32  gateway=192.168.3.1 routing-
table=main scope=10 target-scope=10 comment="STATIC ROUTE FOR RECURSIVE ROUTING - via isp3 -
Quad9 secondary EDNS server"
```

```
add disabled=no distance=1 dst-address=68.94.156.1/32     gateway=192.168.3.1 routing-
table=main scope=10 target-scope=10 comment="STATIC ROUTE FOR RECURSIVE ROUTING - via isp3 -
AT&T primary DNS server"
add disabled=no distance=1 dst-address=68.94.157.1/32     gateway=192.168.3.1 routing-
table=main scope=10 target-scope=10 comment="STATIC ROUTE FOR RECURSIVE ROUTING - via isp3 -
AT&T primary DNS server"



#
# default routes using various recursive lookup entries as the gateway
#
add check-gateway=ping dst-address=0.0.0.0/0 gateway=1.1.1.1 routing-table=main distance=1
scope=30 target-scope=11 comment="default gateway via isp1 using recursive lookup"
add check-gateway=ping dst-address=0.0.0.0/0 gateway=8.8.8.8 routing-table=main distance=2
scope=30 target-scope=11 comment="default gateway via isp1 using recursive lookup"
add check-gateway=ping dst-address=0.0.0.0/0 gateway=9.9.9.9 routing-table=main distance=3
scope=30 target-scope=11 comment="default gateway via isp1 using recursive lookup"

add check-gateway=ping dst-address=0.0.0.0/0 gateway=1.0.0.1         routing-table=main
distance=4 scope=30 target-scope=11 comment="default gateway via isp2 using recursive lookup"
add check-gateway=ping dst-address=0.0.0.0/0 gateway=8.8.4.4         routing-table=main
distance=5 scope=30 target-scope=11 comment="default gateway via isp2 using recursive lookup"
add check-gateway=ping dst-address=0.0.0.0/0 gateway=149.112.112.112 routing-table=main
distance=6 scope=30 target-scope=11 comment="default gateway via isp2 using recursive lookup"

add check-gateway=ping dst-address=0.0.0.0/0 gateway=68.94.156.1 routing-table=main distance=7
scope=30 target-scope=11 comment="default gateway via isp3 using recursive lookup"
add check-gateway=ping dst-address=0.0.0.0/0 gateway=68.94.157.1 routing-table=main distance=8
scope=30 target-scope=11 comment="default gateway via isp3 using recursive lookup"
add check-gateway=ping dst-address=0.0.0.0/0 gateway=4.2.2.2.2   routing-table=main distance=9
scope=30 target-scope=11 comment="default gateway via isp3 using recursive lookup"

#
# default routes using actual next hops - no outage detection will occur unless the physical
Ethernet interface is disconnect
# having distances above 200 allows learned routes via OSPF (110) and BGP (200) to be used
before these are
#
add check-gateway=none dst-address=0.0.0.0/0 gateway=192.168.1.1 routing-table=main
distance=201 scope=30 target-scope=10 comment="default gateway via isp using actual next hop -
```

```
no failover unless Ethernet is disconnected"
add check-gateway=none dst-address=0.0.0.0/0 gateway=192.168.2.1 routing-table=main
distance=202 scope=30 target-scope=10 comment="default gateway via isp using actual next hop -
no failover unless Ethernet is disconnected"
add check-gateway=none dst-address=0.0.0.0/0 gateway=192.168.3.1 routing-table=main
distance=203 scope=30 target-scope=10 comment="default gateway via isp using actual next hop -
no failover unless Ethernet is disconnected"
```

The Dude

For being mostly free (at most $45), Mikrotik's The Dude monitoring system is on of the most useful network monitoring tools any IT group could possibly deploy.

Here's some customizations I regularly use.

Notifications

Templates

The are notification template customizations I use.

Email

Subject

```
[Service.Status] [Probe.Name] on [Device.Name] (Map: [Device.NetMaps])
```

Body

```
Service [Probe.Name] on [Device.Name] is now [Service.Status] ([Service.ProblemDescription])
Map: [Device.NetMaps]
Address: [Device.AddressesCommaList] ([Device.FirstDnsName])
Custom Field 1: [Device.CustomField1]
Custom Field 2: [Device.CustomField2]
Custom Field 3: [Device.CustomField3]
Notes:
[Device.NotesCommaList]
```

log to events

```
[Service.Status] [Probe.Name] on [Device.Name] - [Device.FirstAddress] ([Device.FirstDnsName])
- ([Service.ProblemDescription]) - (Map: [Device.NetMaps])
```

log to events - csv

```
"[Device.NetMaps]","[Device.Name]","[Device.FirstAddress]","[Device.FirstDnsName]","[Probe.Name]","[Service.Status]","[Service.ProblemDescription]"
```

log to events - json

```
{"map":"[Device.NetMaps]", "device":"[Device.Name]", "firstAddress":"[Device.FirstAddress]", "firstDNSName":"[Device.FirstDnsName]", "probe":"[Probe.Name]", "status":"[Service.Status]", "problemDescription":"[Service.ProblemDescription]"}
```

Functions

snmp_link_info()

```
if (
string_size(oid(concatenate("iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifAdminStatus.", link_index() ), 300, 600)),
concatenate(
concatenate("if:", link_index(), " - "),
oid(concatenate("iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifDescr.",link_index()), 60),
"
Admin ",
oid(concatenate("iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifAdminStatus.",link_index()), 60),
", Oper ",
oid(concatenate("iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOperStatus.",link_index()), 60),
"
Last change: ",
oid(concatenate("iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifLastChange.",link_index()), 60),
"",
"
"
)
,
""
)
```

apc_ats_output_current

```
oid("1.3.6.1.4.1.318.1.1.8.5.4.3.1.4.1.1.1") * 0.1
```

apc_ats_output_voltage

```
oid_raw("1.3.6.1.4.1.318.1.1.8.5.4.3.1.3")
```

apc_ats_redundancy_status

```
Description: 1 = Not Redundant, 2 = Redundant
Code:
oid("1.3.6.1.4.1.318.1.1.8.5.1.3")
```

apc_ats_redundancy_status_text

```
Description: 1 = Not Redundant, 2 = Redundant
Code:
if(apc_ats_redundancy_status() = 2,"Not Redundant","Redundant")
```

apc_ats_selected_source

```
Description: 1 = Source A, 2 = Source B
Code:
oid("1.3.6.1.4.1.318.1.1.8.5.1.2")
```

apc_ats_selected_source_text

```
Description: 1 = Source A, 2 = Source B
Code:
if(apc_ats_selected_source() = 2,"Source B","Source A")
```

displayCustomField1

```
if(string_size(device_property("CustomField1")) >
0,concatenate(device_property("CustomField1"),"
"),"")
```

displayCustomField2

```
if(string_size(device_property("CustomField1")) >
0,concatenate(device_property("CustomField1"),"
```

```
"),"")
```

displayCustomField3

```
if(string_size(device_property("CustomField3")) >
0,concatenate(device_property("CustomField3"),"
"),"")
```

displayCustomFields12

```
concatenate(
if(string_size(device_property("CustomField1")) >
0,concatenate(device_property("CustomField1"),"
"),""),
if(string_size(device_property("CustomField2")) >
0,concatenate(device_property("CustomField2"),"
"),"")
)
```

displayCustomFields123

```
concatenate(
if(string_size(device_property("CustomField1")) >
0,concatenate(device_property("CustomField1"),"
"),""),
if(string_size(device_property("CustomField2")) >
0,concatenate(device_property("CustomField2"),"
"),""),
if(string_size(device_property("CustomField3")) >
0,concatenate(device_property("CustomField3"),"
"),"")
)
```

procurve_uptime

```
oid_column("1.0.8802.1.1.2.1.2.1.0")
```

ups_alarm_status

```
oid_raw("iso.org.dod.internet.mgmt.mib-2.upsMIB.upsObjects.upsAlarm.upsAlarmPresent")
```

ups_battery_estimatedChargeRemaining_raw

```
if(ups_status_available(), oid_raw("1.3.6.1.2.1.33.1.2.4.0"), 0)
```

ups_battery_estimatedMinutesRemaining_raw

```
if(ups_status_available(), oid_raw("1.3.6.1.2.1.33.1.2.3.0"), 0)
```

ups_battery_status

```
if(ups_status_available(), oid("1.3.6.1.2.1.33.1.2.1.0"), "None")
```

ups_battery_status_raw

```
if(ups_status_available(), oid_raw("1.3.6.1.2.1.33.1.2.1.0"), 0)
```

ups_output_load_percentage_raw

```
if(ups_status_available(), oid_raw("1.3.6.1.2.1.33.1.4.4.1.5.1"), 0)
```

ups_status

```
oid("iso.org.dod.internet.mgmt.mib-2.upsMIB.upsObjects.upsAlarm.upsAlarmPresent")
```

ups_status_available

```
array_size(oid_column("iso.org.dod.internet.mgmt.mib-2.upsMIB.upsObjects.upsAlarm"))
```

ups_status_show

```
concatenate(
if(ups_status_available(), concatenate("UPS: ",
  oid("1.3.6.1.2.1.33.1.2.1.0"),
  " (",
  oid("1.3.6.1.2.1.33.1.2.4.0"),
  "% / ",
  oid("1.3.6.1.2.1.33.1.2.3.0"),
  " minutes)
"), ""),
"")
```

Probes

ups_output_load

```
Name: ups_output_load
Type: Function
Agent: default
Available: ups_status_available()
Error: if(ups_battery_status_raw() <> 2, ups_battery_status(), "")
Value: ups_output_load_percentage_raw()
Unit: status
```

ups_status

```
Name: ups_status
Type: Function
Agent: default
Available: ups_status_available()
Error: if(ups_battery_status_raw() <> 2, ups_battery_status(), "")
Value: ups_battery_status_raw()
Unit: status
```

#end

DHCP Server Option Matcher

MAC OUI

The following MAC OUI matching requires at least RouterOS 7.18.2. It leverages matching the MAC OUI via DHCP Option 61 (Client-ID) which is 0x01 followed by the client MAC address.

Testing environment

```
# configuration validation environment on test router

/ip pool
add name=dhcp_pool-lan-diag1 ranges=192.168.231.100-192.168.231.199
add name=dhcp_pool-lan-diag1-matcher-testing1 ranges=192.168.231.200-192.168.231.209

/ip dhcp-server network
add address=192.168.231.0/24 dns-server=192.168.231.1 domain=diag1.loc gateway=192.168.231.1

/ip dhcp-server
add address-pool=dhcp_pool-lan-diag1 interface=bridge-lan-diag1 lease-time=10m name=dhcp-lan-
diag1
```

```
# matcher for OUI:F8:E4:3B (Anker USB-C adapter)
/ip dhcp-server matcher
add name=oui-match_Anker-F8E43B  \
    server=dhcp-lan-diag1 \
    address-pool=dhcp_pool-lan-diag1_matcher-testing1 \
    option-set=test-set-1 \
    code=61 \
    value=0x01f8e43b \
    matching-type=substring
```

Actual product matchers

The matchers below exclude the dhcp server, pool and other settings. You will need to tweak them as needed, but the code snippets below will at least load the OUI matchers into RouterOS for you.

```
# Polycom
/ip dhcp-server matcher
add name=oui-match_Poly-0004F2 matching-type=substring code=61 value=0x010004f2
add name=oui-match_Poly-64167F matching-type=substring code=61 value=0x0164167f
```

Vendor Class Ids

Below is a list of known vendor Class Ids that have been observed from DHCP requests.

Vendor Class Ids

Option 60 Content	Vendor	Notes
Algo 8301 Paging Adapter ALGO_VENDORamp; Scheduler		
android-dhcp-9		
CISCO SPA112	Cisco (Linksys)	Analog adapter
Fanvil X6U-V2	Fanvil	Vendor Class Id is not enable by default. Hostname matching is needed for out of the box use. The default hostname for this specific model would be "X6U-V2"
HT7XX dslforum.org	Grandstream	Analog adapter
MSFT 5.0		
Polycom-VVX250	Polycom	Just change the model number for other devices
TOSHIBA IPedge		
ubnt		
udhcp 0.9.8		
udhcp 1.15.3		

Mikrotik DHCP Server Option Matchers Configurations

Voice related matchers

```
# Polycom Vendor-Id / Class-Id matchers
:do { /ip dhcp-server option sets add name=voice-polycom } on-error={}
/ip dhcp-server matcher
add address-pool=dhcp_pool-lan-voice code=60 name="Vendor Class Id (60):Polycom-VVX101"
option-set=voice-polycom server=dhcp-lan value=Polycom-VVX101
add address-pool=dhcp_pool-lan-voice code=60 name="Vendor Class Id (60):Polycom-VVX250"
option-set=voice-polycom server=dhcp-lan value=Polycom-VVX250
add address-pool=dhcp_pool-lan-voice code=60 name="Vendor Class Id (60):Polycom-VVX300"
option-set=voice-polycom server=dhcp-lan value=Polycom-VVX300
add address-pool=dhcp_pool-lan-voice code=60 name="Vendor Class Id (60):Polycom-VVX310"
option-set=voice-polycom server=dhcp-lan value=Polycom-VVX310
add address-pool=dhcp_pool-lan-voice code=60 name="Vendor Class Id (60):Polycom-VVX311"
option-set=voice-polycom server=dhcp-lan value=Polycom-VVX311
add address-pool=dhcp_pool-lan-voice code=60 name="Vendor Class Id (60):Polycom-VVX410"
option-set=voice-polycom server=dhcp-lan value=Polycom-VVX410
add address-pool=dhcp_pool-lan-voice code=60 name="Vendor Class Id (60):Polycom-VVX411"
option-set=voice-polycom server=dhcp-lan value=Polycom-VVX411
add address-pool=dhcp_pool-lan-voice code=60 name="Vendor Class Id (60):Polycom-VVX500"
option-set=voice-polycom server=dhcp-lan value=Polycom-VVX500
add address-pool=dhcp_pool-lan-voice code=60 name="Vendor Class Id (60):Polycom-VVX501"
option-set=voice-polycom server=dhcp-lan value=Polycom-VVX501
add address-pool=dhcp_pool-lan-voice code=60 name="Vendor Class Id (60):Polycom-VVX600"
option-set=voice-polycom server=dhcp-lan value=Polycom-VVX600

# Fanvil Vendor-Id / Class-Id matchers
:do { /ip dhcp-server option sets add name=voice-fanvil } on-error={}
/ip dhcp-server matcher
add address-pool=dhcp_pool-lan-voice code=12 name="Hostname(12):X5U" option-set=voice-fanvil
server=dhcp-lan value="X5U"
add address-pool=dhcp_pool-lan-voice code=12 name="Hostname(12):X5U-V2" option-set=voice-
fanvil server=dhcp-lan value="X5U-V2"
add address-pool=dhcp_pool-lan-voice code=12 name="Hostname(12):X6U" option-set=voice-fanvil
server=dhcp-lan value="X6U"
add address-pool=dhcp_pool-lan-voice code=12 name="Hostname(12):X6U-V2" option-set=voice-
fanvil server=dhcp-lan value="X6U-V2"
add address-pool=dhcp_pool-lan-voice code=12 name="Hostname(12):X210" option-set=voice-fanvil
server=dhcp-lan value="X210"
add address-pool=dhcp_pool-lan-voice code=12 name="Hostname(12):X210-V2" option-set=voice-
fanvil server=dhcp-lan value="X210-V2"
```

```
add address-pool=dhcp_pool-lan-voice code=60 name="Vendor Class Id (60):Fanvil X5U" option-set=voice-fanvil server=dhcp-lan value="Fanvil X5U"
add address-pool=dhcp_pool-lan-voice code=60 name="Vendor Class Id (60):Fanvil X5U-V2" option-set=voice-fanvil server=dhcp-lan value="Fanvil X5U-V2"
add address-pool=dhcp_pool-lan-voice code=60 name="Vendor Class Id (60):Fanvil X6U" option-set=voice-fanvil server=dhcp-lan value="Fanvil X6U"
add address-pool=dhcp_pool-lan-voice code=60 name="Vendor Class Id (60):Fanvil X6U-V2" option-set=voice-fanvil server=dhcp-lan value="Fanvil X6U-V2"
add address-pool=dhcp_pool-lan-voice code=60 name="Vendor Class Id (60):Fanvil X210" option-set=voice-fanvil server=dhcp-lan value="Fanvil X210"
add address-pool=dhcp_pool-lan-voice code=60 name="Vendor Class Id (60):Fanvil X210-V2" option-set=voice-fanvil server=dhcp-lan value="Fanvil X210-V2"



# Need to add
# 2N IP Vario
# 2N IP Verso
# Axis A8105-E Network Video Door Station
# Axis A8207-VE Network Video Door Station
# Axis A8207-VE Mk II Network Video Door Station
# Axis C1310-E Network Horn Speaker
# Barix
# Cisco SPA112
# Cisco SPA303
# Cisco SPA525G2
```

-end

Scripting

Arrays

Basics

Arrays in RouterOS can be normal indexed arrays or associative (key/value pair arrays).

Array element separator is the semi-colon.

```
# normal indexed example
{
  :local myArray { "ContainerLog"; "ContainerDebug" }
  :foreach e in=$myArray do={ :put $e }
}
```

```
# key-value example
{
  :local myArray { a="ContainerLog"; b="ContainerDebug" }
  :foreach k,v in=$myArray do={ :put "$k -> $v" }
}
```

Create empty array and adding entries

Two ways to create an empty array:

```
{
:put "Creating and adding to global emptyArray1";
:global emptyArray1 [{}];
:set emptyArray1 ($emptyArray1, 1);
:set emptyArray1 ($emptyArray1, 2);

:put "Creating and adding to global emptyArray2";
:global emptyArray2 [:toarray ""];
:set emptyArray2 ($emptyArray2, 1);
:set emptyArray2 ($emptyArray2, 2);
```

```
:put "Printing environment:";
:env print;

:put "Putting arrays:";
:put $emptyArray1;
:put $emptyArray2;
}
```

The output of the above code is:

```
Creating and adding to global emptyArray1
Creating and adding to global emptyArray2
Printing environment:
emptyArray1={1; 2}
emptyArray2={1; 2}
tmp1=[]
tmp2={}

Putting arrays:
1;2
1;2
```

Using a regular array:

```
{
:local array1 [:toarray ""];
:set array1 ($array1, "entry1");
:set array1 ($array1, "entry2");
:put ("array1: " . [:tostr $array1]);
}
```

Using an associative array (key / value pairs):

```
# without quotes around variable in set statement
{
:local array2 [:toarray ""];
:set ($array2->"entry1") 1;
:set ($array2->"entry2") 2;
:put ("array2: " . [:tostr $array2]);
}
```

```
# with quotes around variable in set statement
{
:local array2 [:toarray ""];
:set ("$array2"->"entry1") 1;
:set ("$array2"->"entry2") 2;
:put ("array2: " . [:tostr $array2]);
}
```

Indexed array

```
# define a variable to play with
:global array1

# a normal array with no keys
:set array1 {1;2}

# referencing an array by index
:put ($array1->0)
:put ($array1->1)

# iterate over each element with for
:for x from=0 to=[:len $array1] step=1 do={
  :put ($array1->$x)
}

# iterate over each element with foreach
:foreach a in=$array1 do={
  :put $a
}
```

Associative (key/value pair) arrays

```
# define a variable to play with
:global array1

# an associative array, or key/value pairs
:set array1 {a=1;b=2}

# referencing an array value by key
:put ($array1->"a")
```

```
:put ($array1->"b")

# iterate over each pair
:foreach k,v in=$array1 do={
  :put ($k . " -> " . $v)
}
```

:tostr

Sometimes RouterOS returns a value in a format that you're not expecting, and strange things will happen because you don't understand how RouterOS is handing you data. This primarily happens when you think RouterOS is going to give you a string, but its actually giving you an array.

If you run values through ***:tostr*** before using them, fewer unexpected things will happen to your script.

The example below shows us getting the neighbor interface for a specific device. If the interface is a member of a bridge, the result we get looks like "[bridge_port_name];[bridge_interface_name]" when using ***:put***. If the interface is not part of a bridge, the result we get looks like "[interface_name]" when using ***:put***. If you were to save that result to a global variable, and then do ***:env print*** you'll see that what we received both times is actually being stored as an array {"ether5";"bridge-lan"} and {"ether5"} respectively.

When you use :put with a variable that is storing an array, interesting things can happen, as you can see in the example OUTPUT.

```
# find the neighbor we want some information about
:global neighbor [/ip neighbor get [find where address=192.168.91.173]]

# get the local interface we're connected via
:global neighborLocalInterface [/ip neighbor get $neighbor interface]

# check the result... using put, it looks like its a normal string
:put $neighborLocalInterface
# OUTPUT: ether5;bridge-lane

# check the type - it's actually an array
:put [:typeof $neighborLocalInterface]
# OUTPUT: array

# verify that through environment print
:environment print
```

```
# OUTPUT: str={"ether5"; "bridge-lan"}

# here's something strange that happens if you print without tostr
:put ("interface: $neighborLocalInterface")
# OUTPUT: interface: ether5;interface: bridge-lan

# here's what we were expecting to see, thanks to the use of :tostr
:put ("interface: $[:tosr $neighborLocalInterface]")
# OUTPUT: interface: ether5;bridge-lan
```

Notice the output of the :put on line 20 has some unexpected content.

Playing with arrays

```
# MSHARP 20180827
# Playing with arrays
# Lesson learned: You cannot mix using keys and not using keys in the same array, even a
multi-dimensional one.

{
:local a1 {0}
:local count 0

:put "============================================================="
:put "Testing the handling of a single dimmension array with no keys"
:set a1 {1;2}
:put "Putting the full array:"
:put $a1
:put "Putting array elements in a foreach loop:"
:set count 0
:foreach i in=$a1 do={
  :put $i
  :set count ($count + 1)
}
:put "count:$count"
:put "===================="
:put "Putting array elements in a foreach loop using keys:"
:set count 0
:foreach k,v in=$a1 do={
  :put ($k . " - " . $v)
```

```
  :set count ($count + 1)
}
:put "count:$count"
:put "============================================================="

:put "Testing the handling of a single dimmension array with keys"
:set a1 {a=1;b=2}
:put "Putting the full array:"
:put $a1
:put "Putting array elements in a foreach loop without using keys:"
:set count 0
:foreach i in=$a1 do={
  :put $i
  :set count ($count + 1)
}
:put "count:$count"
:put "===================="
:put "Putting array elements in a foreach loop using keys:"
:set count 0
:foreach k,v in=$a1 do={
  :put ($k . " - " . $v)
  :set count ($count + 1)
}
:put "count:$count"
:put "============================================================="

:put "Testing the handling of a multi-dimensional array using no keys"
:set a1 {{1;2};{3;4}}
:put "Putting the full multi-dimensional array:"
:put $a1
:foreach i in=$a1 do={
  :put "Putting one of the sub-arrays:"
  :put $i
  :put "Putting the items in the array individually:"
  :set count 0
  :foreach k in=$i do={
    :put $k
    :set count ($count + 1)
  }
  :put "count:$count"
```

```
  :put "Putting the key - value pairs of the array"
  :set count 0
  :foreach k,v in=$i do={
    :put ($k . " - " . $v)
    :set count ($count + 1)
  }
  :put "count:$count"
  :put "====================="
}
:put "============================================================="

:put "Testing the handling of a multi-dimensional array using keys"
:set a1 {{a=1;b=2};{c=3;d=4}}
:put "Putting the full multi-dimensional array:"
:put $a1
:foreach i in=$a1 do={
  :put "Putting one of the sub-arrays:"
  :put $i
  :put "Putting the items in the array individually:"
  :set count 0
  :foreach k in=$i do={
    :put $k
    :set count ($count + 1)
  }
  :put "count:$count"
  :put "Putting the key - value pairs of the array"
  :set count 0
  :foreach k,v in=$i do={
    :put ($k . " - " . $v)
    :set count ($count + 1)
  }
  :put "count:$count"
  :put "====================="
}
:put "============================================================="



:put "Testing the handling of a multi-dimensional array, one subarray not using keys and the
using keys."
:put "Notice that mixing keys and no keys does not work properly."
```

```
:set a1 {{1;2};{c=3;d=4}}
:put "Putting the full multi-dimensional array:"
:put $a1
:foreach i in=$a1 do={
  :put "Putting one of the sub-arrays:"
  :put $i
  :put "Putting the items in the array individually:"
  :set count 0
  :foreach k in=$i do={
    :put $k
    :set count ($count + 1)
  }
  :put "count:$count"
  :put "Putting the key - value pairs of the array"
  :set count 0
  :foreach k,v in=$i do={
    :put ($k . " - " . $v)
    :set count ($count + 1)
  }
  :put "count:$count"
  :put "====================="
}
:put "============================================================="

#END
}
```

#end

Scripting

Scripting with traceroute

POC

Running /tool traceroute with the as-value option will return the hops as an array.

```
{
  :local trDestination 1.1.1.1;
  :local trDuration 3s;
  :local tr [/tool traceroute $trDestination as-value duration=3s];
  :put ("number of hops in $trDuration:" . [:len $tr]);
  :foreach hop in=$tr do={
    :put ([$hop]->"address");
  }
}
```

#end

Logging

Interesting log messages

These are log messages that have been observed that would be ideal to receive administrative notifications regarding.

```
system,error,critical could not save configuration changes, not enough storage space available.
```

Snippets

Snippets

DHCP Leases to CSV

CSV output of DHPC related items in RouterOS

Static DHCP leases to CSV output

```
{
    # process only static leases
    :local staticLeases [/ip dhcp-server lease find where dynamic=no]
    :foreach l in=$staticLeases do={
        :local lma [/ip dhcp-server lease get $l mac-address]
        :local la [/ip dhcp-server lease get $l address]
        :local lc [/ip dhcp-server lease get $l comment]
        :put "$lma,$la,\"$lc\""
    }
}
```

All DHCP leases to CSV output

```
{
    # process all leases
    :local staticLeases [/ip dhcp-server lease find]
    :foreach l in=$staticLeases do={
        :local lma [/ip dhcp-server lease get $l mac-address]
        :local la [/ip dhcp-server lease get $l address]
        :local lc [/ip dhcp-server lease get $l comment]
        :local ld [/ip dhcp-server lease get $l dynamic]
        :put "$lma,$la,$ld,\"$lc\""
    }
}
```

-end

Snippets

DHCP Server Lease last-seen comparison

```
/ip dhcp-server lease print where last-seen > "30d"
```

```
/ip dhcp-server lease print where last-seen > "30d" && last-seen !="never"
```

```
/ip dhcp-server lease print where last-seen > "30d" && last-seen !="never" && server=dhcp-lan
&& comment~"^auto-static"
```

Container

Howto

Prepping the base configuration

```
{
  /system logging action
  :foreach actionName in={ "ContainerLog"; "ContainerDebug" } do={
    :if ([:len [find where name="$actionName"]] = 0) do={
      add name=$actionName target=memory
      :put "[ADDED] $actionName action added"
    } else={ :put "[INFO] $actionName action already exists" }
  }

  /system logging
  :if ([:len [find where topics~"container"]] > 0) do={
    :put "[WARNING] Some logs dealing with the container topic already exist:"
    print where topics~"container"
  }

  /system logging
  :if ([:len [find where action="ContainerLog" and (topics~"container" and topics~"!debug")]]
= 0) do={
    add action=ContainerLog topics=container,!debug
    :put "[ADDED] ContainerLog logging added"
  } else={ :put "[INFO] ContainerLog=container,!debug logging already exists" }

  /system logging
  :if ([:len [find where action="ContainerDebug" and (topics~"container" and topics~"debug")]]
= 0) do={
    add action=ContainerDebug topics=container,debug
```

```
    :put "[ADDED] ContainerDebug logging added"
  } else={ :put "[INFO] ContainerDebug=container,debug logging already exists" }

}
```

```
/container config set registry-url=https://registry-1.docker.io
/container config set tmpdir=/z-pod/tmp

/container config set ram-high=500.0MiB
/container config set memory-high=500.0MiB
```

```
/interface veth
add address=100.122.31.11/24 gateway=100.122.31.1 gateway6="" name=veth1
add address=100.122.31.12/24 gateway=100.122.31.1 gateway6="" name=veth2
add address=100.122.31.13/24 gateway=100.122.31.1 gateway6="" name=veth3
add address=100.122.31.14/24 gateway=100.122.31.1 gateway6="" name=veth4
add address=100.122.31.15/24 gateway=100.122.31.1 gateway6="" name=veth5
add address=100.122.31.16/24 gateway=100.122.31.1 gateway6="" name=veth6
add address=100.122.31.17/24 gateway=100.122.31.1 gateway6="" name=veth7
add address=100.122.31.18/24 gateway=100.122.31.1 gateway6="" name=veth8
add address=100.122.31.19/24 gateway=100.122.31.1 gateway6="" name=veth9

/interface bridge
add comment="container lan - docker1" name=bridge-docker1

/ip address
add address=100.122.31.1/24 interface=bridge-docker1 network=100.122.31.0

/interface bridge port
add bridge=bridge-docker1 interface=veth1
add bridge=bridge-docker1 interface=veth2
add bridge=bridge-docker1 interface=veth3
add bridge=bridge-docker1 interface=veth4
add bridge=bridge-docker1 interface=veth5
add bridge=bridge-docker1 interface=veth6
add bridge=bridge-docker1 interface=veth7
add bridge=bridge-docker1 interface=veth8
add bridge=bridge-docker1 interface=veth9

/ip firewall nat
```

```
add action=masquerade chain=srcnat comment="wan - srcnat traffic from container network to the Internet" dst-address-list=!private-ip-subnets ipsec-policy=out,none out-interface=ether1 src-address=100.122.31.0/24
```

Alpine

To install a plain alpine:latest container on a Mikrotik RouterOS device, use the following:

```
remote-image=library/alpine:latest
```

```
/container
add name=alpine-1 \
  remote-image=library/alpine \
  interface=veth-alpine-1 \
  logging=yes \
  root-dir=sata1/c/alpine-diag-1 \
  cmd="tail -f /dev/null"
```

bluecrow76/alpine-netdiag

It's just the above but with updates and nmap installed.

```
/container
add name=alpine-1 \
  remote-image=bluecrow76/alpine-netdiag \
  interface=veth-alpine-netdiag-1 \
  logging=yes \
  root-dir=sata1/c/alpine-netdiag-1 \
  cmd="tail -f /dev/null"
```

Uptime Kuma

```
# mounts - pick the one you need, or edit to fit
```

```
# /
/container mounts add dst=/app/data name=uptime-kuma_app-data src=/c-mnt/uptime-kuma/app-data
/container mounts add dst=/app/data name=uptime-kuma_app-data-certs src=/c-mnt/uptime-kuma/app-data-certs

# /nvme1
/container mounts add dst=/app/data name=uptime-kuma_app-data src=/nvme1/c-mnt/uptime-kuma/app-data
/container mounts add dst=/app/data name=uptime-kuma_app-data-certs src=/nvme1/c-mnt/uptime-kuma/app-data-certs

# /pcie1
/container mounts add dst=/app/data name=uptime-kuma_app-data src=/pcie1/c-mnt/uptime-kuma/app-data
/container mounts add dst=/app/data name=uptime-kuma_app-data-certs src=/pcie1/c-mnt/uptime-kuma/app-data-certs

# /sata1
/container mounts add dst=/app/data name=uptime-kuma_app-data src=/sata1/c-mnt/upme-kuma/app-datat
/container mounts add dst=/app/data name=uptime-kuma_app-data-certs src=/sata1/c-mnt/upme-kuma/app-data-certs
```

```
# environment lists
/container envs
add key=NODE_EXTRA_CA_CERTS name=uptime-kuma-1 value=/app/data/certs/ca_bundle.pem
```

```
# build the actual container - use the one that suites or edit to fit

# onboard flash
{
:local image louislam/uptime-kuma:1
:local iface veth1
:local rootdir "/c/uptime-kuma-1"
/container/add name=uptime-kuma-1 remote-image=$image interface=$iface root-dir=$rootdir envlist=uptime-kuma-1 mounts=uptime-kuma_app-data,uptime-kuma_app-data-certs
}

# nvme1
{
```

```
:local image louislam/uptime-kuma:1
:local iface veth1
:local rootdir "/nvme1/c/uptime-kuma-1"
/container/add name=uptime-kuma-1 remote-image=$image interface=$iface root-dir=$rootdir
envlist=uptime-kuma-1 mounts=uptime-kuma_app-data,uptime-kuma_app-data-certs
}

# pcie1
{
:local image louislam/uptime-kuma:1
:local iface veth1
:local rootdir "/pcie1/c/uptime-kuma-1"
/container/add name=uptime-kuma-1 remote-image=$image interface=$iface root-dir=$rootdir
envlist=uptime-kuma-1 mounts=uptime-kuma_app-data,uptime-kuma_app-data-certs
}

# sata1
{
:local image louislam/uptime-kuma:1
:local iface veth1
:local rootdir "/sata1/c/uptime-kuma-1"
/container/add name=uptime-kuma-1 remote-image=$image interface=$iface root-dir=$rootdir
envlist=uptime-kuma-1 mounts=uptime-kuma_app-data,uptime-kuma_app-data-certs
}
```

-end

Flashfig and Netinstall

Microsoft Hyper-V

Flashfig will not work properly on a Windows computer running Microsoft Hyper-V. You will get the error message "no TFTP request" in the Flashfig console when routers attempt to connect.