MikroTik SA

MikroTik
CERTIFIED
Training Partner

New Features and Updates in RouterOS

About MikroTik SA

- Independent Network Specialist company
- Not owned by / affiliated to MikroTik Latvia
- Official training and support partner for MikroTik
- Specialist in all forms of wireless and wired networking technologies
- Offers high speed PTP links, carrier independent backbone services, high availability SLA's, Network Management and Configuration services

About the Presenter

David Savage

- Is a MikroTik Certified Trainer and consultant
- Installs and manages and wireless networks
- Has over 25 years experience in the IT field
- Teaches general networking and MikroTik RouterOS

In this Presentation

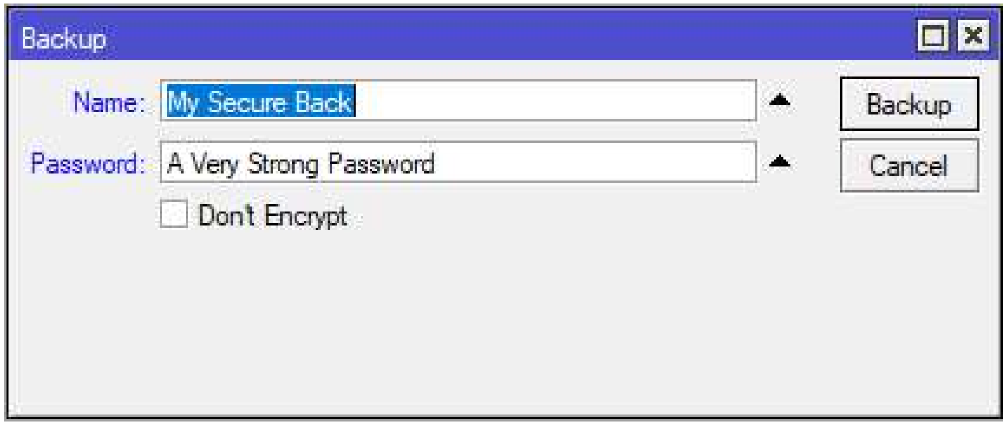
- MikroTik RouterOS is under constant development
- Difficult to keep up to date with new features and improvements to current features
- I hope to change that and bring you up to date with just some of the new features

System Backup and Restore

- **PROBLEM**: RouterOS backup was vulnerable to cracking with a possibility to reveal users and passwords
- **SOLUTION**: Since RouterOS v6.13 it is possible to encrypt the backup files with RC4
- Encryption - the backup file is encrypted by default, if the current RouterOS user has a password configured, or if the "password" parameter is used
  - If your RouterOS user doesn't have a password set then the backup file is not encrypted
  - To enable encryption in this case, use the "password" parameter.

Backup Parameters

- Encryption - the backup file is encrypted by default, if the current RouterOS user has a password configured, or if the "password" parameter is used
  - If your RouterOS user doesn't have a password set then the backup file is not encrypted
  - To enable encryption in this case, use the "password" parameter.



Name: My Secure Back

Password: A Very Strong Password

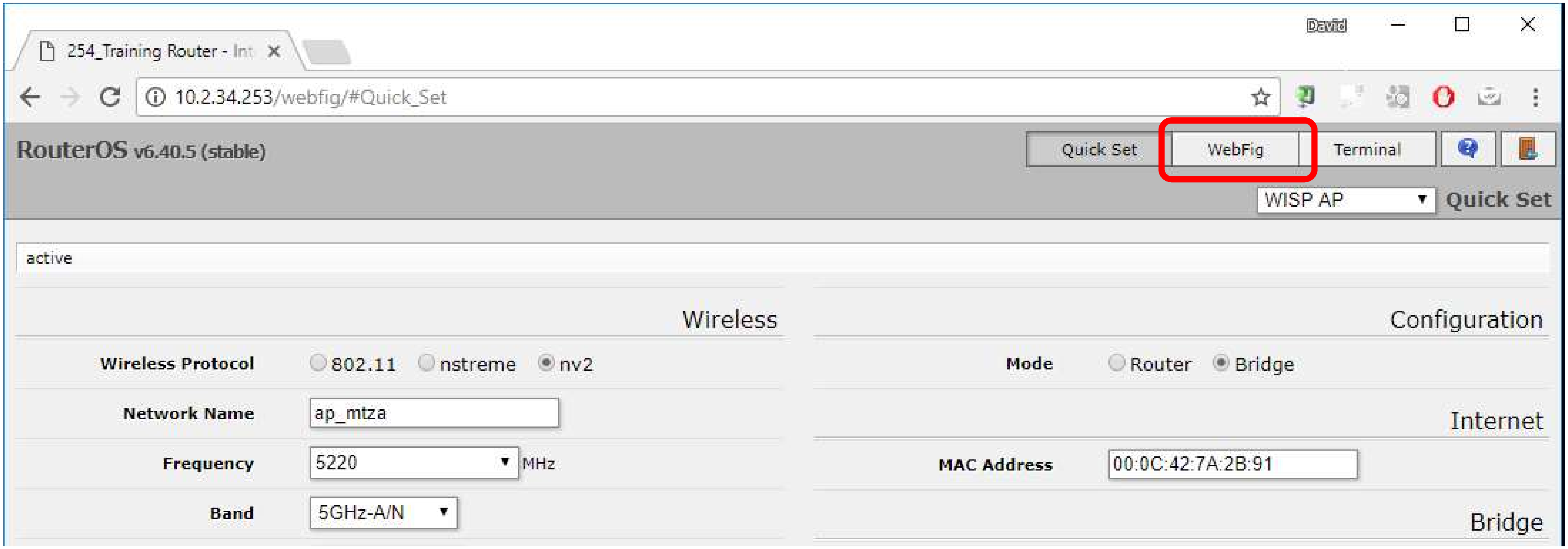
□ Don't Encrypt

Web Administration

- **PROBLEM**: You want to provide access to the router, but with limited menu options
- **SOLUTION**: Use Webfig with a custom designed skin to limit access to certain menus and options

Configuring Skins

1. Login to web interface with admin account
2. Select the Webfig” option (top right)



Wireless Protocol ○ 802.11 ○ nstreme ● nv2

Network Name ap_mtza

Frequency 5220 MHz

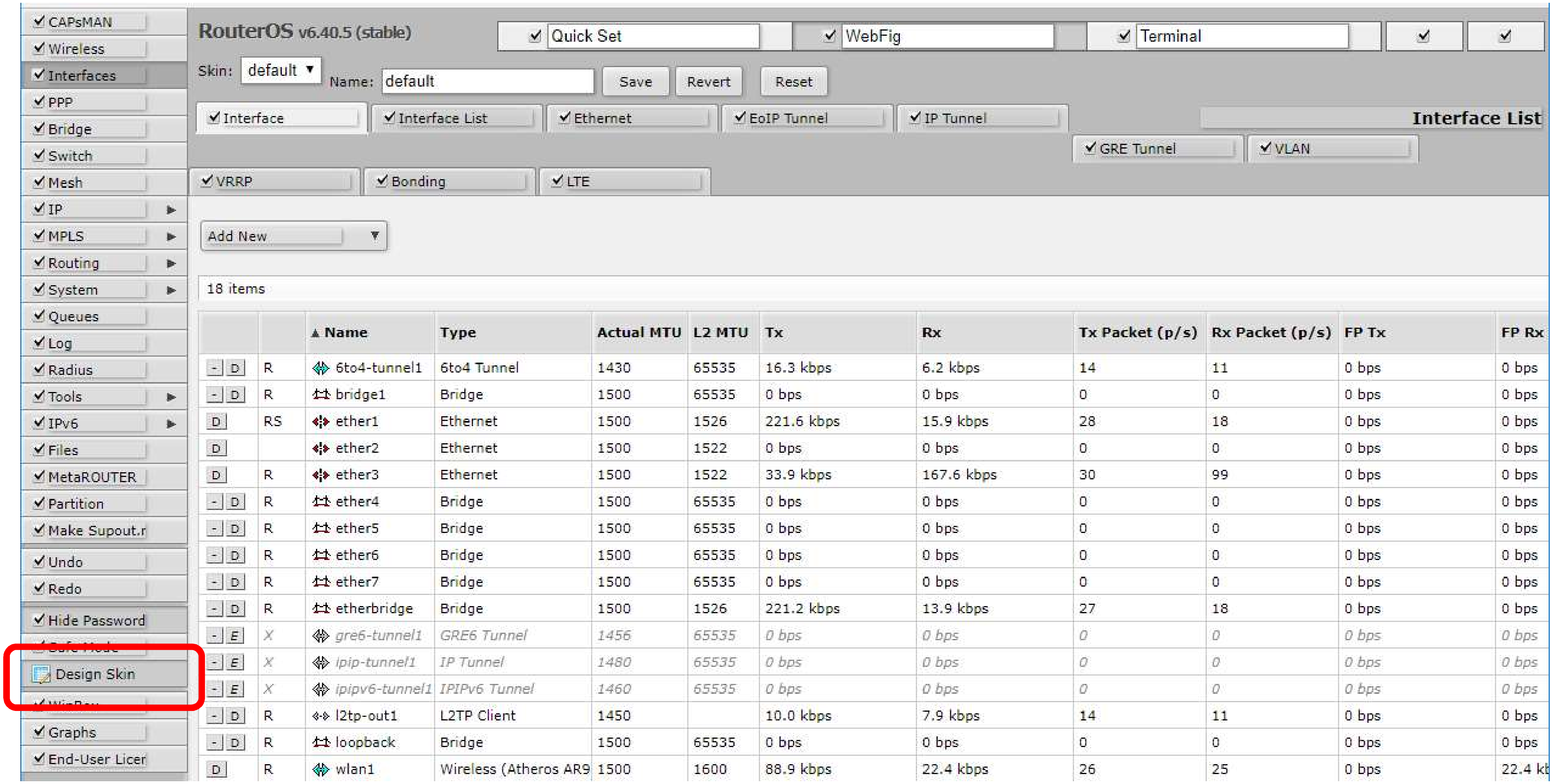
Band 5GHz-A/N

Mode ○ Router ● Bridge

MAC Address 00:0C:42:7A:2B:91

Configuring Skins

1. Choose “Design Skin” and select / deselect / rename options as required

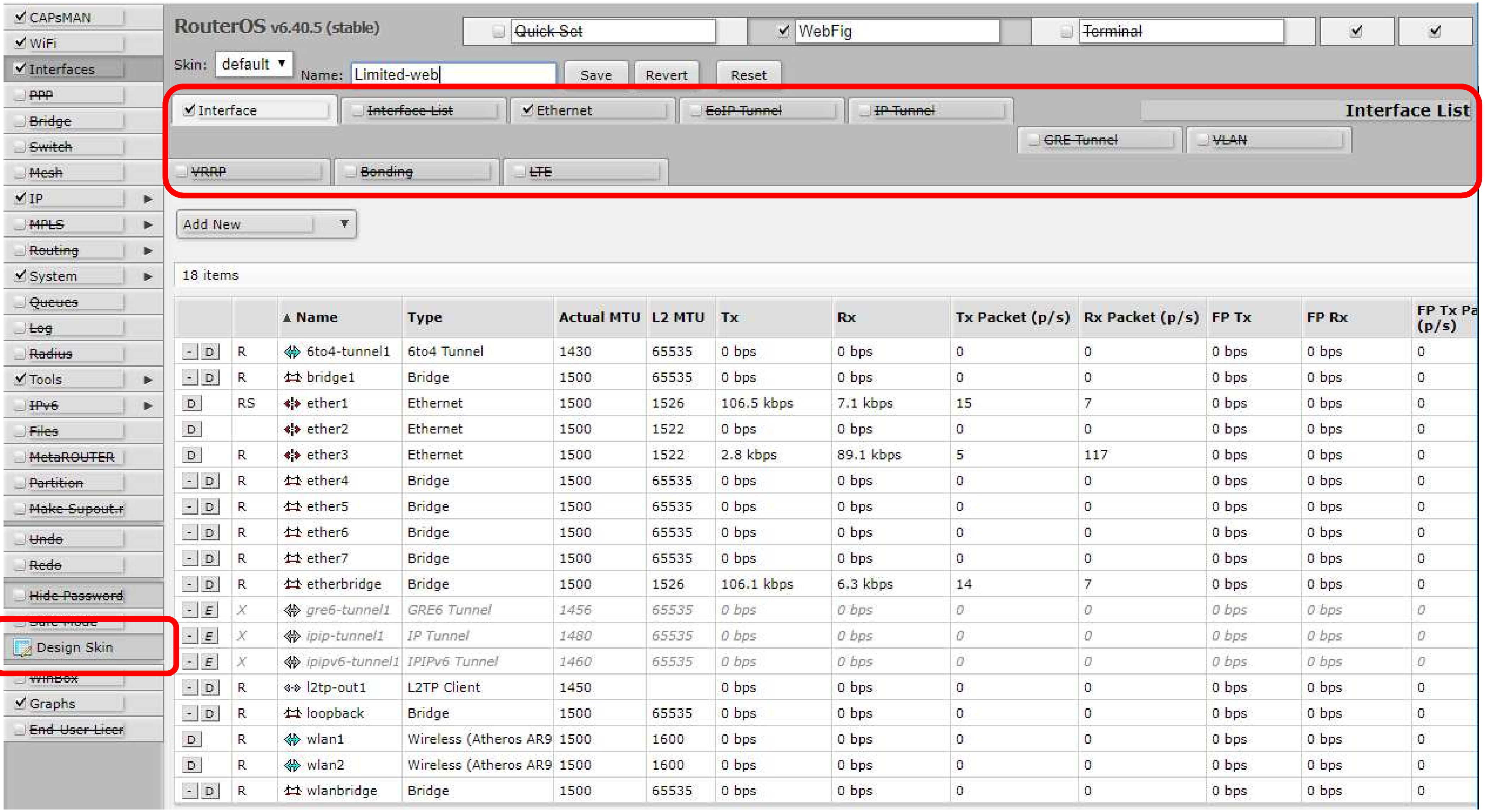


Skin: default ▼ Name: default

18 items

		▲ Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx
- D	R	6to4-tunnel1	6to4 Tunnel	1430	65535	16.3 kbps	6.2 kbps	14	11	0 bps	0 bps
- D	R	bridge1	Bridge	1500	65535	0 bps	0 bps	0	0	0 bps	0 bps
D	RS	ether1	Ethernet	1500	1526	221.6 kbps	15.9 kbps	28	18	0 bps	0 bps
D		ether2	Ethernet	1500	1522	0 bps	0 bps	0	0	0 bps	0 bps
D	R	ether3	Ethernet	1500	1522	33.9 kbps	167.6 kbps	30	99	0 bps	0 bps
- D	R	ether4	Bridge	1500	65535	0 bps	0 bps	0	0	0 bps	0 bps
- D	R	ether5	Bridge	1500	65535	0 bps	0 bps	0	0	0 bps	0 bps
- D	R	ether6	Bridge	1500	65535	0 bps	0 bps	0	0	0 bps	0 bps
- D	R	ether7	Bridge	1500	65535	0 bps	0 bps	0	0	0 bps	0 bps
- D	R	etherbridge	Bridge	1500	1526	221.2 kbps	13.9 kbps	27	18	0 bps	0 bps
- E	X	gre6-tunnel1	GRE6 Tunnel	1456	65535	0 bps	0 bps	0	0	0 bps	0 bps
- E	X	ipip-tunnel1	IP Tunnel	1480	65535	0 bps	0 bps	0	0	0 bps	0 bps
- E	X	ipipv6-tunnel1	IPIPv6 Tunnel	1460	65535	0 bps	0 bps	0	0	0 bps	0 bps
- D	R	l2tp-out1	L2TP Client	1450		10.0 kbps	7.9 kbps	14	11	0 bps	0 bps
- D	R	loopback	Bridge	1500	65535	0 bps	0 bps	0	0	0 bps	0 bps
D	R	wlan1	Wireless (Atheros AR9	1500	1600	88.9 kbps	22.4 kbps	26	25	0 bps	22.4 kb

2. Choose “Design Skin” and select / deselect / rename options as required



□ ~~Quick Set~~ ☑ WebFig □ ~~Terminal~~ ☑ ☑

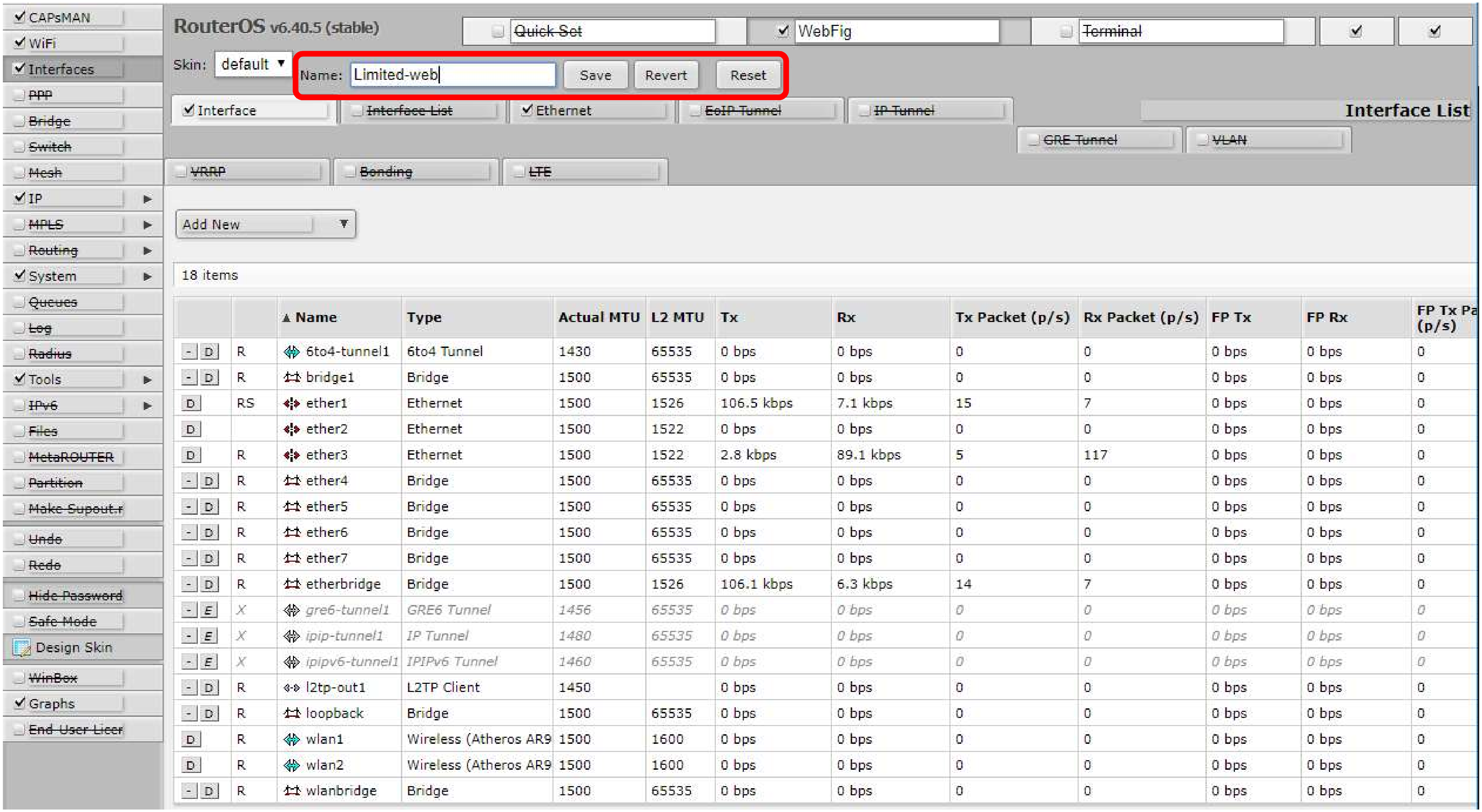
Skin: default ▼ Name: Limited-web

☑ Interface □ ~~Interface List~~ ☑ Ethernet □ ~~EoIP Tunnel~~ □ ~~IP Tunnel~~ Interface List □ ~~GRE Tunnel~~ □ ~~VLAN~~ □ ~~VRRP~~ □ ~~Bonding~~ □ ~~LTE~~

18 items

		▲ Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx	FP Tx Pa (p/s)
- D	R	6to4-tunnel1	6to4 Tunnel	1430	65535	0 bps	0 bps	0	0	0 bps	0 bps	0
- D	R	bridge1	Bridge	1500	65535	0 bps	0 bps	0	0	0 bps	0 bps	0
D	RS	ether1	Ethernet	1500	1526	106.5 kbps	7.1 kbps	15	7	0 bps	0 bps	0
D		ether2	Ethernet	1500	1522	0 bps	0 bps	0	0	0 bps	0 bps	0
D	R	ether3	Ethernet	1500	1522	2.8 kbps	89.1 kbps	5	117	0 bps	0 bps	0
- D	R	ether4	Bridge	1500	65535	0 bps	0 bps	0	0	0 bps	0 bps	0
- D	R	ether5	Bridge	1500	65535	0 bps	0 bps	0	0	0 bps	0 bps	0
- D	R	ether6	Bridge	1500	65535	0 bps	0 bps	0	0	0 bps	0 bps	0
- D	R	ether7	Bridge	1500	65535	0 bps	0 bps	0	0	0 bps	0 bps	0
- D	R	etherbridge	Bridge	1500	1526	106.1 kbps	6.3 kbps	14	7	0 bps	0 bps	0
- E	X	*gre6-tunnel1*	*GRE6 Tunnel*	*1456*	*65535*	*0 bps*	*0 bps*	*0*	*0*	*0 bps*	*0 bps*	*0*
- E	X	*ipip-tunnel1*	*IP Tunnel*	*1480*	*65535*	*0 bps*	*0 bps*	*0*	*0*	*0 bps*	*0 bps*	*0*
- E	X	*ipipv6-tunnel1*	*IPIPv6 Tunnel*	*1460*	*65535*	*0 bps*	*0 bps*	*0*	*0*	*0 bps*	*0 bps*	*0*
- D	R	l2tp-out1	L2TP Client	1450		0 bps	0 bps	0	0	0 bps	0 bps	0
- D	R	loopback	Bridge	1500	65535	0 bps	0 bps	0	0	0 bps	0 bps	0
D	R	wlan1	Wireless (Atheros AR9	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0
D	R	wlan2	Wireless (Atheros AR9	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0
- D	R	wlanbridge	Bridge	1500	65535	0 bps	0 bps	0	0	0 bps	0 bps	0

3. Save the modified skin under a new filename



Skin: default ▼

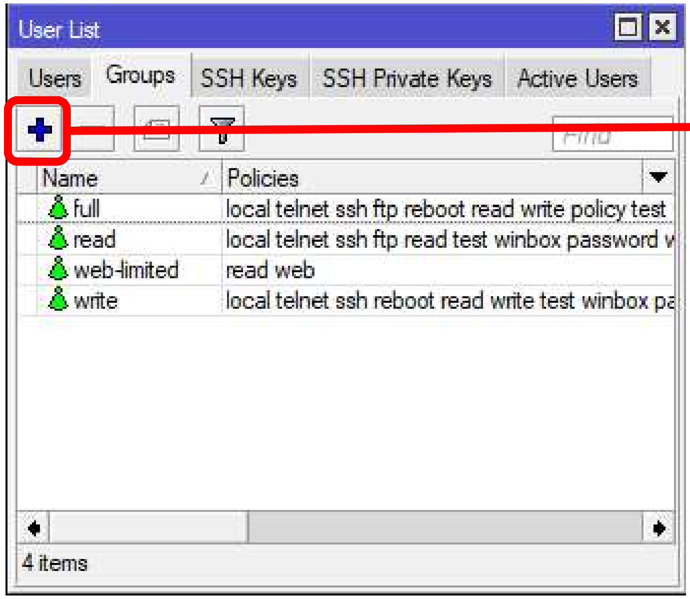
Name: Limited-web

18 items

		▲ Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx	FP Tx Pa (p/s)
- D	R	6to4-tunnel1	6to4 Tunnel	1430	65535	0 bps	0 bps	0	0	0 bps	0 bps	0
- D	R	bridge1	Bridge	1500	65535	0 bps	0 bps	0	0	0 bps	0 bps	0
D	RS	ether1	Ethernet	1500	1526	106.5 kbps	7.1 kbps	15	7	0 bps	0 bps	0
D		ether2	Ethernet	1500	1522	0 bps	0 bps	0	0	0 bps	0 bps	0
D	R	ether3	Ethernet	1500	1522	2.8 kbps	89.1 kbps	5	117	0 bps	0 bps	0
- D	R	ether4	Bridge	1500	65535	0 bps	0 bps	0	0	0 bps	0 bps	0
- D	R	ether5	Bridge	1500	65535	0 bps	0 bps	0	0	0 bps	0 bps	0
- D	R	ether6	Bridge	1500	65535	0 bps	0 bps	0	0	0 bps	0 bps	0
- D	R	ether7	Bridge	1500	65535	0 bps	0 bps	0	0	0 bps	0 bps	0
- D	R	etherbridge	Bridge	1500	1526	106.1 kbps	6.3 kbps	14	7	0 bps	0 bps	0
- E	X	*gre6-tunnel1*	*GRE6 Tunnel*	*1456*	*65535*	*0 bps*	*0 bps*	*0*	*0*	*0 bps*	*0 bps*	*0*
- E	X	*ipip-tunnel1*	*IP Tunnel*	*1480*	*65535*	*0 bps*	*0 bps*	*0*	*0*	*0 bps*	*0 bps*	*0*
- E	X	*ipipv6-tunnel1*	*IPIPv6 Tunnel*	*1460*	*65535*	*0 bps*	*0 bps*	*0*	*0*	*0 bps*	*0 bps*	*0*
- D	R	l2tp-out1	L2TP Client	1450		0 bps	0 bps	0	0	0 bps	0 bps	0
- D	R	loopback	Bridge	1500	65535	0 bps	0 bps	0	0	0 bps	0 bps	0
D	R	wlan1	Wireless (Atheros AR9	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0
D	R	wlan2	Wireless (Atheros AR9	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps	0
- D	R	wlanbridge	Bridge	1500	65535	0 bps	0 bps	0	0	0 bps	0 bps	0

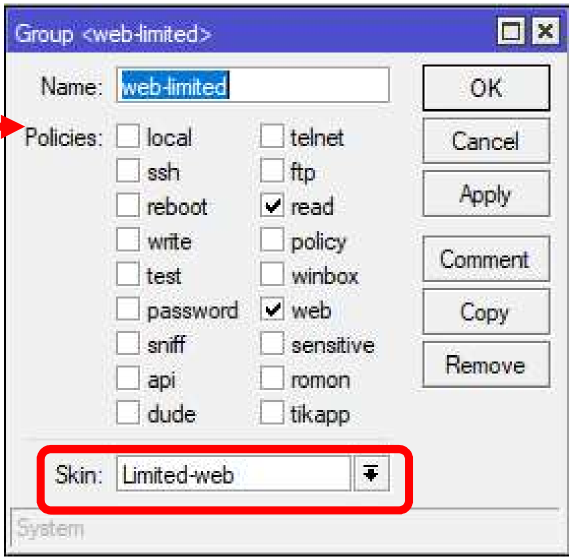
4. Under System → User → Group add a new group with limited web only permissions

5. Add a new user with membership of the limited group


User List

Name	Policies
full	local telnet ssh ftp reboot read write policy test
read	local telnet ssh ftp read test winbox password v
web-limited	read web
write	local telnet ssh reboot read write test winbox pa

4 items

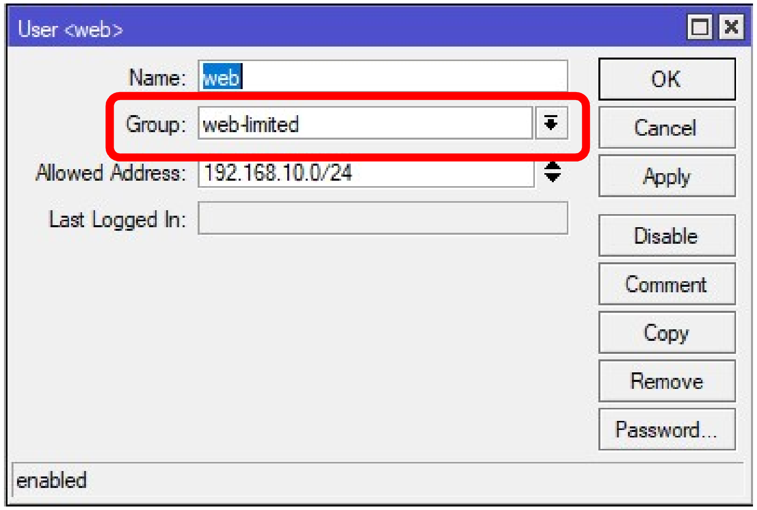

Group <web-limited>

Name: web-limited

Policies:

☐ local	☐ telnet
☐ ssh	☐ ftp
☐ reboot	☑ read
☐ write	☐ policy
☐ test	☐ winbox
☐ password	☑ web
☐ sniff	☐ sensitive
☐ api	☐ romon
☐ dude	☐ tikapp

Skin: Limited-web


User <web>

Name: web

Group: web-limited

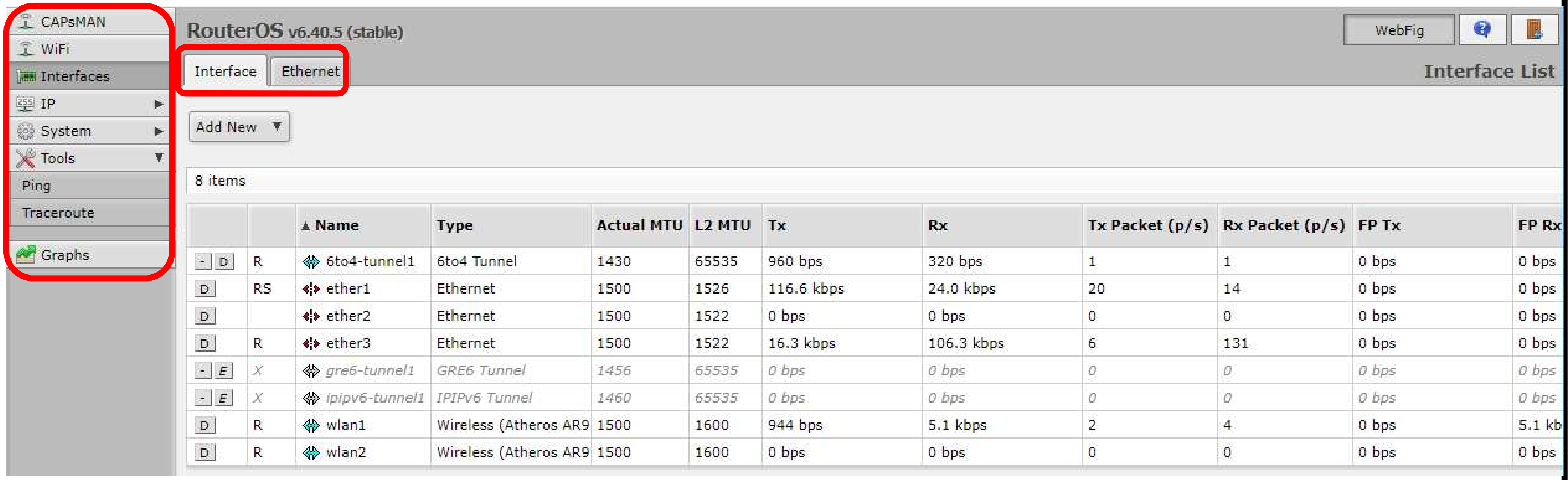
Allowed Address: 192.168.10.0/24

Last Logged In:

enabled

5. Login with the limited user

You now have a strictly limited view as per your defined skin policy



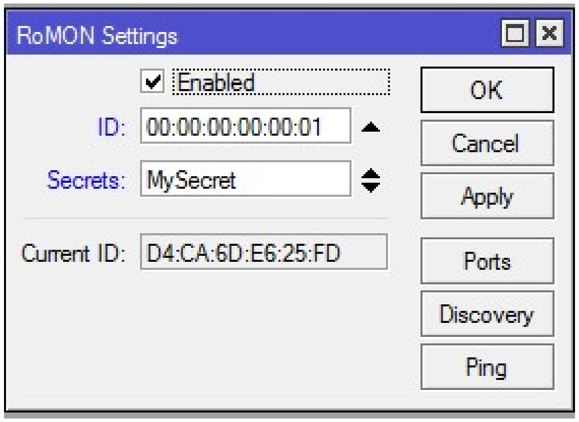
		▲ Name	Type	Actual MTU	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx
- D	R	6to4-tunnel1	6to4 Tunnel	1430	65535	960 bps	320 bps	1	1	0 bps	0 bps
D	RS	ether1	Ethernet	1500	1526	116.6 kbps	24.0 kbps	20	14	0 bps	0 bps
D		ether2	Ethernet	1500	1522	0 bps	0 bps	0	0	0 bps	0 bps
D	R	ether3	Ethernet	1500	1522	16.3 kbps	106.3 kbps	6	131	0 bps	0 bps
- E	X	*gre6-tunnel1*	*GRE6 Tunnel*	*1456*	*65535*	*0 bps*	*0 bps*	*0*	*0*	*0 bps*	*0 bps*
- E	X	*ipipv6-tunnel1*	*IPIPv6 Tunnel*	*1460*	*65535*	*0 bps*	*0 bps*	*0*	*0*	*0 bps*	*0 bps*
D	R	wlan1	Wireless (Atheros AR9	1500	1600	944 bps	5.1 kbps	2	4	0 bps	5.1 kb
D	R	wlan2	Wireless (Atheros AR9	1500	1600	0 bps	0 bps	0	0	0 bps	0 bps

RoMON

- **PROBLEM**: RouterOS Winbox can only access directly connected routers by MAC addres
- **SOLUTION**: RoMON - Router Management Overlay Network
- RoMON works by establishing an independent MAC layer peer discovery and data forwarding network
- RoMON network operates independently from L2 or L3 forwarding configuration

Configure RoMON

- Tool → RoMON allows the service to be enabled/disabled
- ID can optionally be specified otherwise default is ether1 MAC
- Secrets will encrypt RoMON comms with MD5 – secret must be the same for adjacent ports
- RoMON Ports allows setting up ports individually with costs

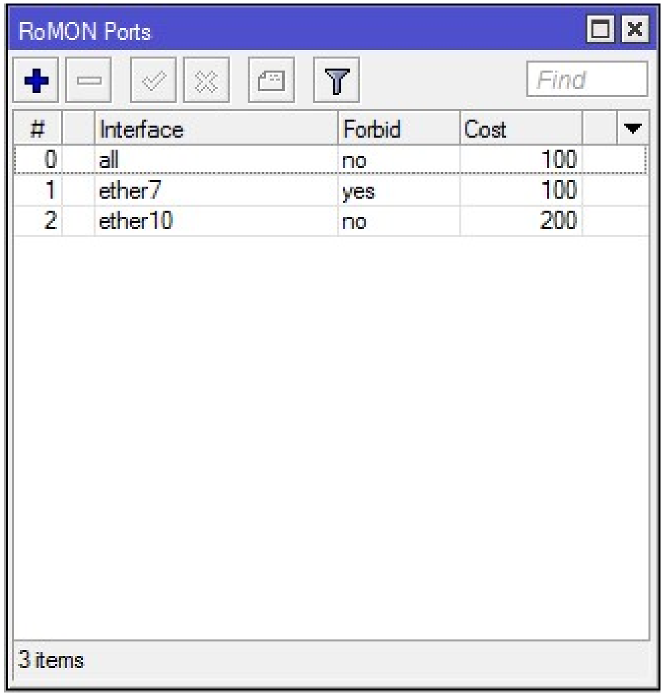


☑ Enabled

ID: 00:00:00:00:00:01

Secrets: MySecret

Current ID: D4:CA:6D:E6:25:FD

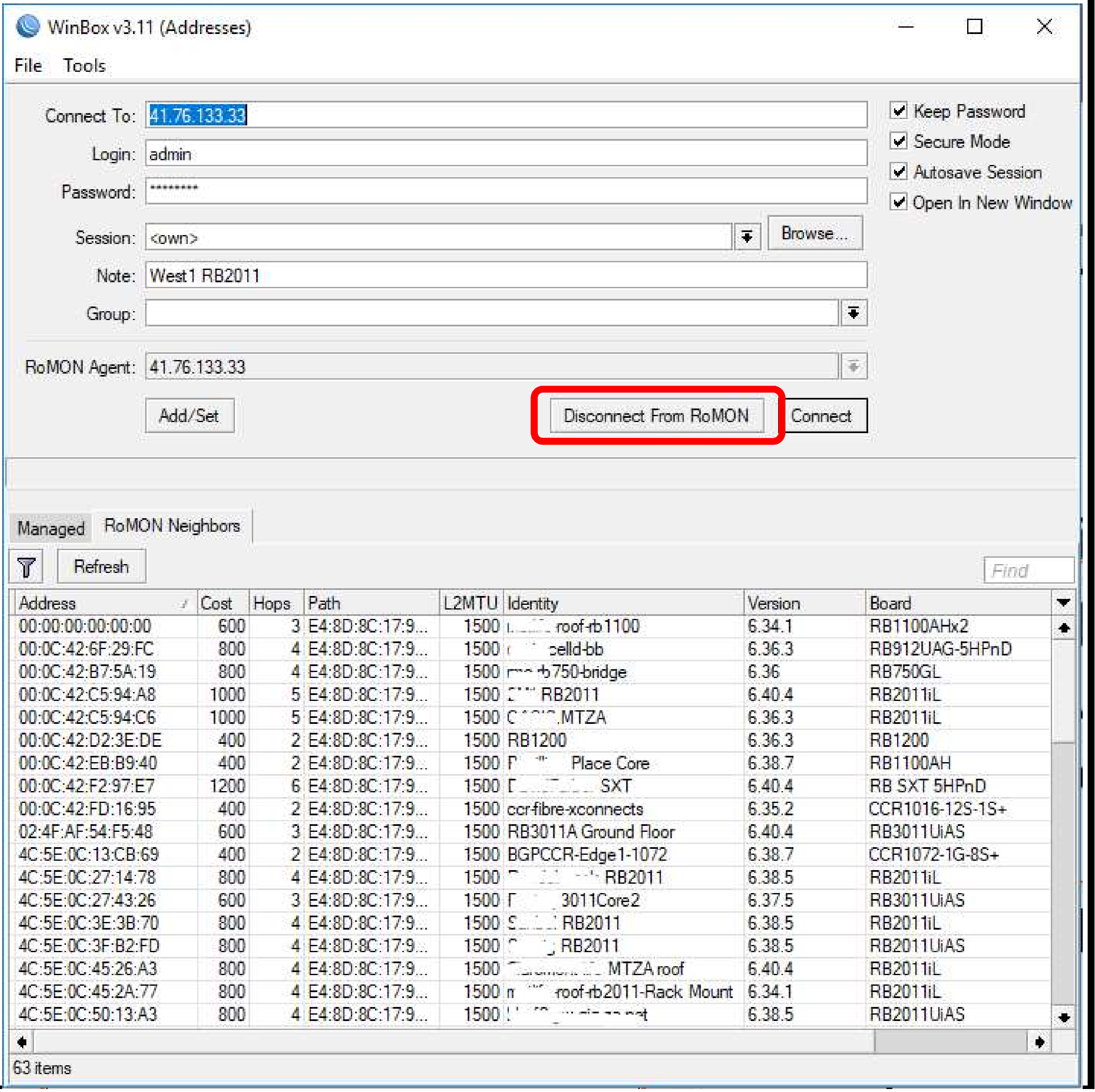


#	Interface	Forbid	Cost
0	all	no	100
1	ether7	yes	100
2	ether10	no	200

3 items

Connecting to RoMON

- Winbox V3 must be used
- Select a RoMON enabled router and choose “Connect to RoMON”
- RoMON enabled routers will now be displayed



Connect To: 41.76.133.33

Login: admin

Password: ********

Session: <own>

Note: West1 RB2011

Group:

RoMON Agent: 41.76.133.33

☑ Keep Password

☑ Secure Mode

☑ Autosave Session

☑ Open In New Window

Address	Cost	Hops	Path	L2MTU	Identity	Version	Board
00:00:00:00:00:00	600	3	E4:8D:8C:17:9...	1500	[redacted] roof-rb1100	6.34.1	RB1100AHx2
00:0C:42:6F:29:FC	800	4	E4:8D:8C:17:9...	1500	[redacted] celld-bb	6.36.3	RB912UAG-5HPnD
00:0C:42:B7:5A:19	800	4	E4:8D:8C:17:9...	1500	[redacted]b750-bridge	6.36	RB750GL
00:0C:42:C5:94:A8	1000	5	E4:8D:8C:17:9...	1500	[redacted] RB2011	6.40.4	RB2011iL
00:0C:42:C5:94:C6	1000	5	E4:8D:8C:17:9...	1500	[redacted].MTZA	6.36.3	RB2011iL
00:0C:42:D2:3E:DE	400	2	E4:8D:8C:17:9...	1500	RB1200	6.36.3	RB1200
00:0C:42:EB:B9:40	400	2	E4:8D:8C:17:9...	1500	[redacted] Place Core	6.38.7	RB1100AH
00:0C:42:F2:97:E7	1200	6	E4:8D:8C:17:9...	1500	[redacted] SXT	6.40.4	RB SXT 5HPnD
00:0C:42:FD:16:95	400	2	E4:8D:8C:17:9...	1500	ccr-fibre-xconnects	6.35.2	CCR1016-12S-1S+
02:4F:AF:54:F5:48	600	3	E4:8D:8C:17:9...	1500	RB3011A Ground Floor	6.40.4	RB3011UiAS
4C:5E:0C:13:CB:69	400	2	E4:8D:8C:17:9...	1500	BGPCCR-Edge1-1072	6.38.7	CCR1072-1G-8S+
4C:5E:0C:27:14:78	800	4	E4:8D:8C:17:9...	1500	[redacted] RB2011	6.38.5	RB2011iL
4C:5E:0C:27:43:26	600	3	E4:8D:8C:17:9...	1500	[redacted] 3011Core2	6.37.5	RB3011UiAS
4C:5E:0C:3E:3B:70	800	4	E4:8D:8C:17:9...	1500	[redacted] RB2011	6.38.5	RB2011iL
4C:5E:0C:3F:B2:FD	800	4	E4:8D:8C:17:9...	1500	[redacted] RB2011	6.38.5	RB2011UiAS
4C:5E:0C:45:26:A3	800	4	E4:8D:8C:17:9...	1500	[redacted] MTZA roof	6.40.4	RB2011iL
4C:5E:0C:45:2A:77	800	4	E4:8D:8C:17:9...	1500	[redacted] roof-rb2011-Rack Mount	6.34.1	RB2011iL
4C:5E:0C:50:13:A3	800	4	E4:8D:8C:17:9...	1500	[redacted]	6.38.5	RB2011UiAS

63 items

Wireless System

Wifi Protected Setup (WPS)

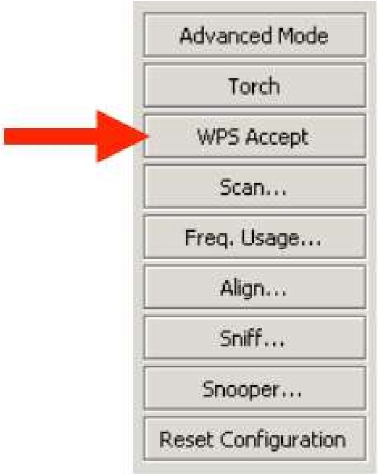
NV2 Sync

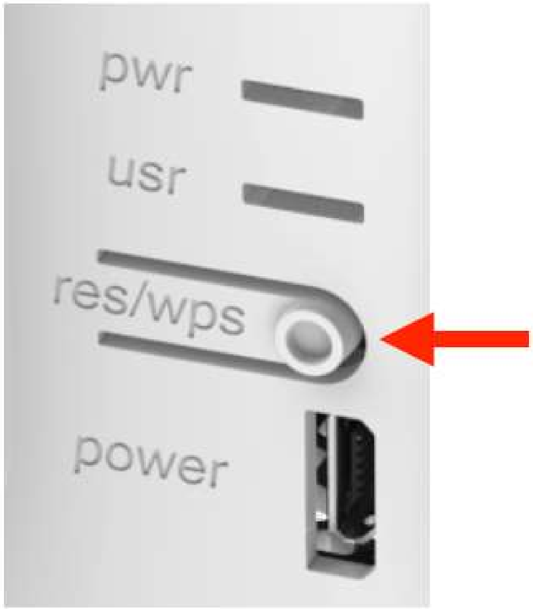
WPS

- WiFi Protected Setup (WPS) is a feature for convenient access to the WiFi without entering the passphrase
- RouterOS supports both WPS accept (for AP) and WPS client (for station) modes
- To easily allow guest access to your access point WPS accept button can be used
- When pushed, it will grant an access to connect to the AP for 2min or until a device (station) connects
- The WPS accept button has to be pushed each time a new device needs to connect

Using WPS

- A RouterOS devices with a WiFi interface has a virtual WPS push button
- Certain routers have a front panel button, check for wps button on the router
- Virtual WPS button is available in QuickSet and in wireless interface menu
- It can be disabled if needed
- WPS client is supported by most operating systems





Nstreme Version 2

- Nv2 protocol is a proprietary wireless protocol developed by MikroTik for use with Atheros 802.11 wireless chips
- Nv2 is based on TDMA (Time Division Multiple Access) media access technology instead of CSMA (Carrier Sense Multiple Access) media access technology used in regular 802.11 devices.
- TDMA media access technology solves hidden node problem and improves media usage, thus improving throughput and latency, especially in PtMP networks.

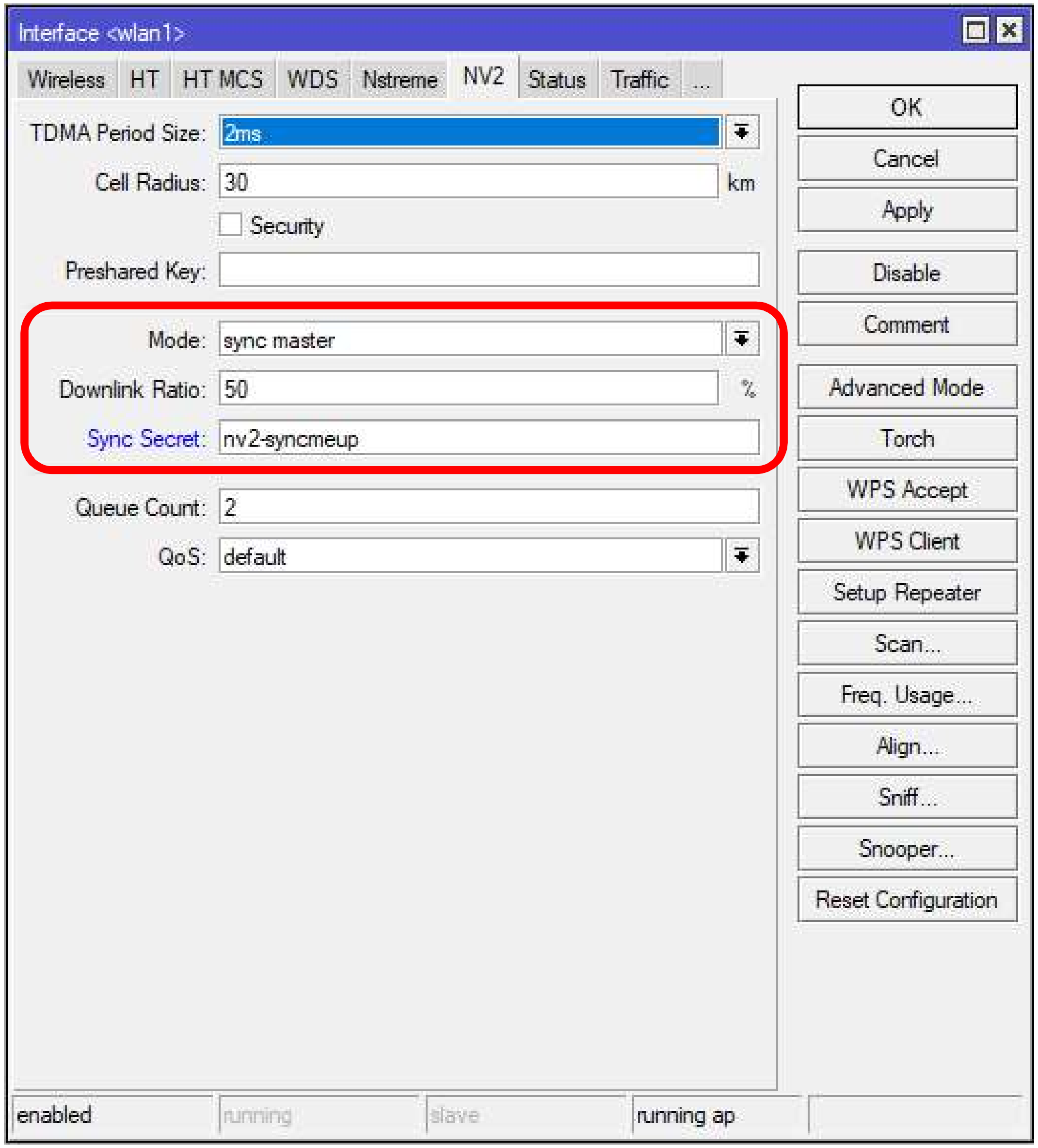
Nv2 AP Synchronization

- This (experimental) feature will let multiple MikroTik Nv2 APs on the same location to coexist in a better fashion by reducing the interference between each other.
- This feature will synchronize the transmit/receive time windows of APs in the same frequency, so that all synced MikroTik Nv2 APs transmits/receives at the same time.
- That allows to reuse the same wireless frequency on the location for multiple APs giving more flexibility in frequency planning.

Nv2 AP Synchronization

- For Nv2 Synchronization a Master Nv2 AP should be chosen and "nv2-mode=sync-master" should be specified together with "nv2-sync-secret".
- For Nv2 Slave APs the same wireless frequency as Master AP should be used and "nv2-mode=sync-slave" should be specified with the same "nv2-sync-secret" as the in Master AP configuration.
- After Master AP is found the Slave AP will start operating as AP and it adapts the period size and downlink ratio from the synced Master AP.

Nv2 AP Synchronization



TDMA Period Size: 2ms

Cell Radius: 30 km

□ Security

Preshared Key:

Mode: sync master

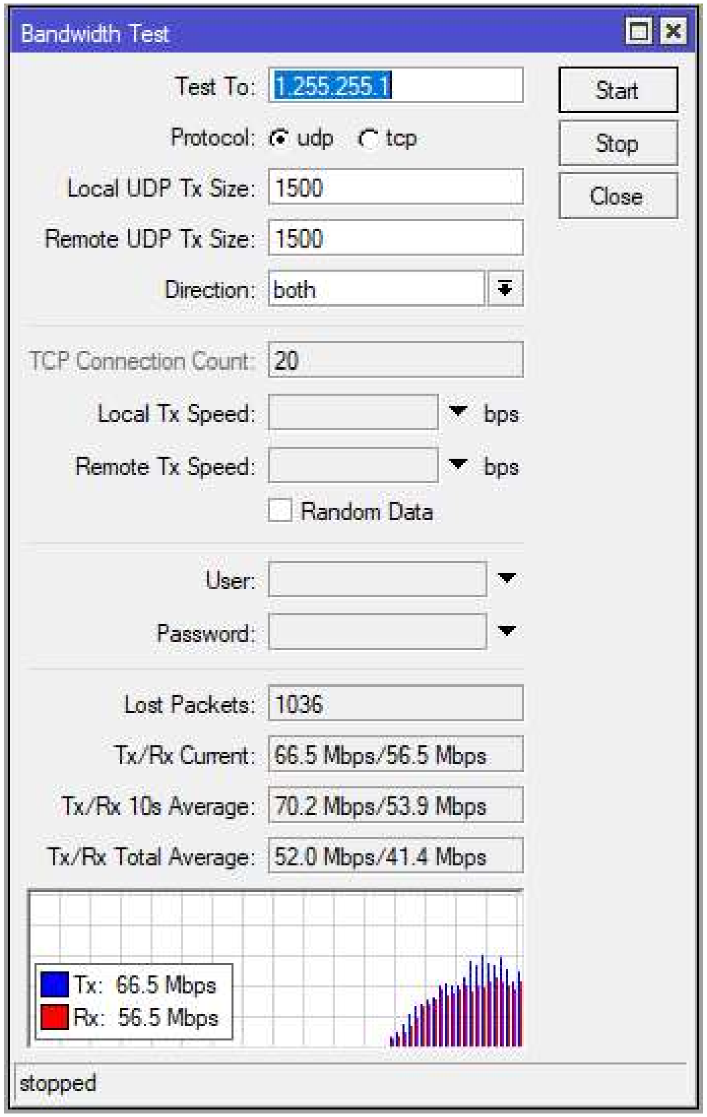
Downlink Ratio: 50 %

Sync Secret: nv2-syncmeup

Queue Count: 2

QoS: default

enabled | running | slave | running ap



Test To: 1.255.255.1

Protocol: ● udp ○ tcp

Local UDP Tx Size: 1500

Remote UDP Tx Size: 1500

Direction: both

TCP Connection Count: 20

Local Tx Speed: bps

Remote Tx Speed: bps

□ Random Data

User:

Password:

Lost Packets: 1036

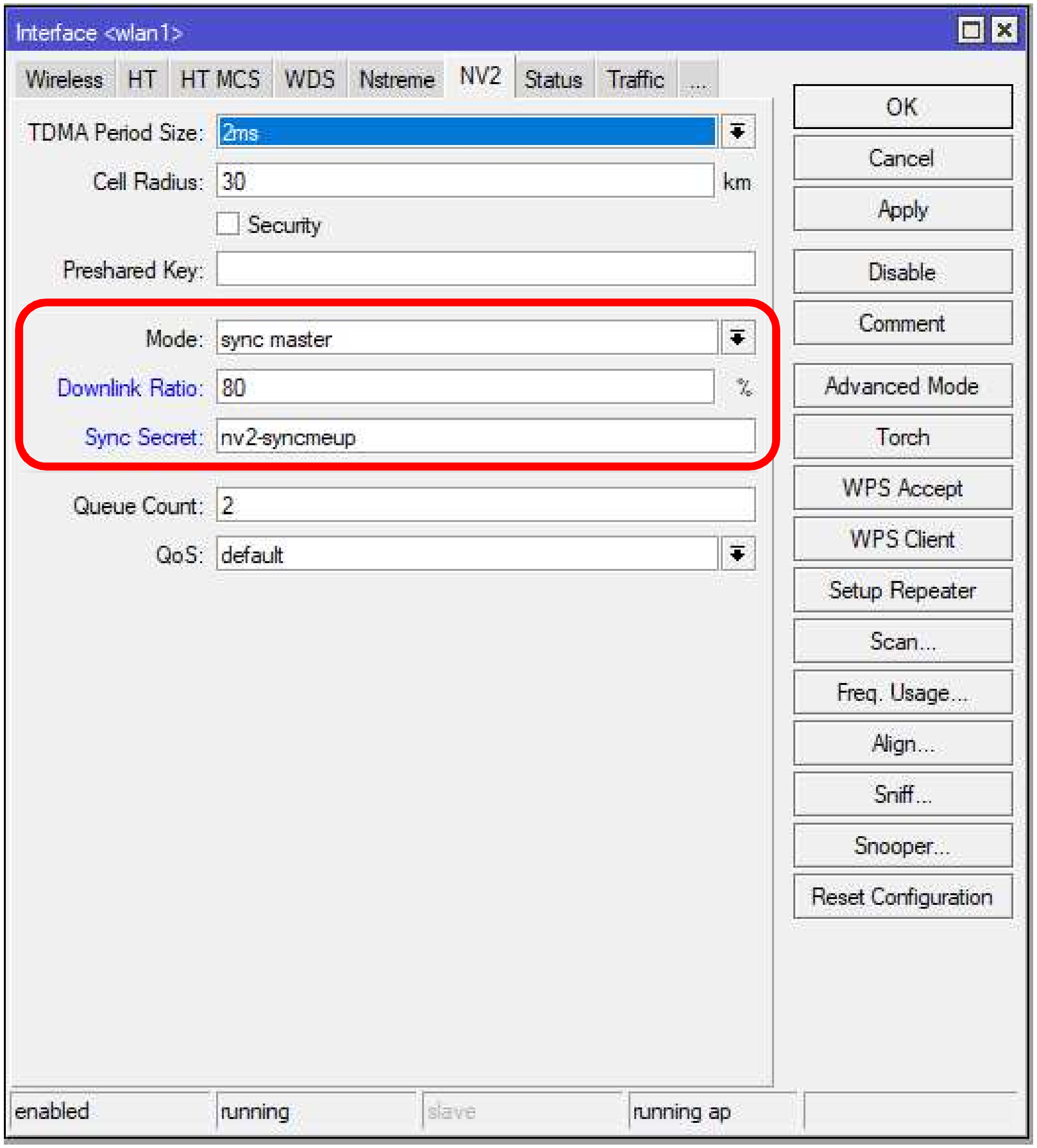
Tx/Rx Current: 66.5 Mbps/56.5 Mbps

Tx/Rx 10s Average: 70.2 Mbps/53.9 Mbps

Tx/Rx Total Average: 52.0 Mbps/41.4 Mbps

stopped

Nv2 AP Synchronization



Interface <wlan1>

TDMA Period Size: 2ms

Cell Radius: 30 km

□ Security

Preshared Key:

Mode: sync master

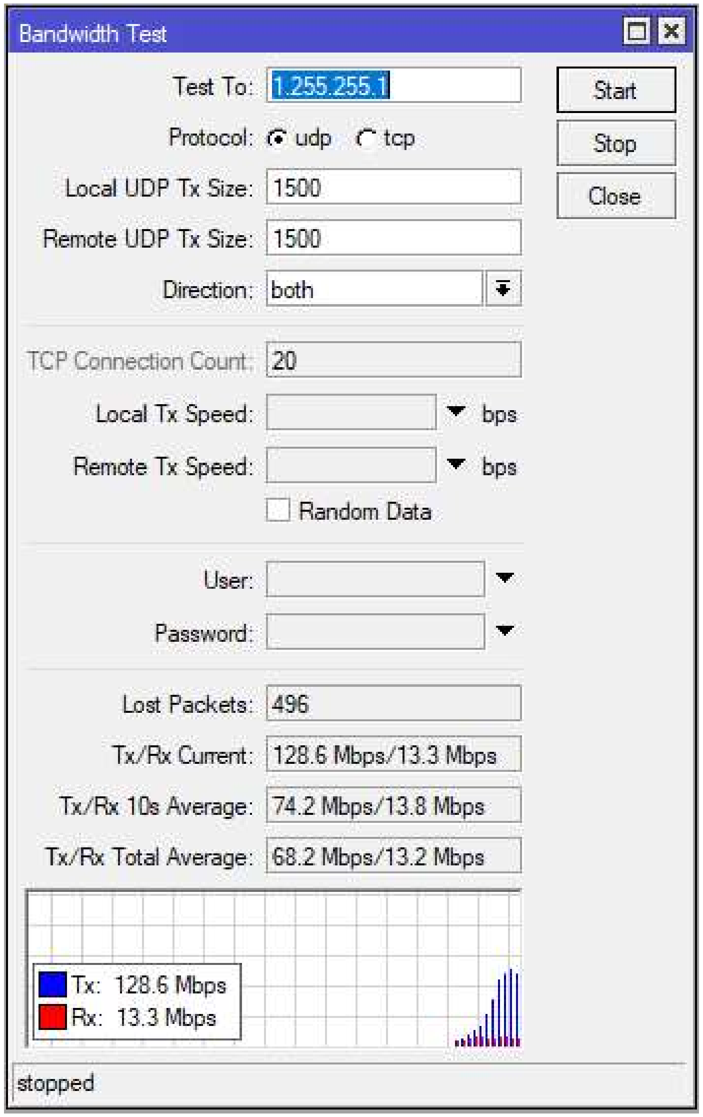
Downlink Ratio: 80 %

Sync Secret: nv2-syncmeup

Queue Count: 2

QoS: default

enabled | running | slave | running ap



Bandwidth Test

Test To: 1.255.255.1

Protocol: ● udp ○ tcp

Local UDP Tx Size: 1500

Remote UDP Tx Size: 1500

Direction: both

TCP Connection Count: 20

Local Tx Speed: bps

Remote Tx Speed: bps

□ Random Data

User:

Password:

Lost Packets: 496

Tx/Rx Current: 128.6 Mbps/13.3 Mbps

Tx/Rx 10s Average: 74.2 Mbps/13.8 Mbps

Tx/Rx Total Average: 68.2 Mbps/13.2 Mbps

🟦 Tx: 128.6 Mbps
🟥 Rx: 13.3 Mbps

stopped

VPN

Virtual Private Networks

EoIP, VLAN

PPTP,L2TP
PPPoE

PPTP and L2TP Tunnels

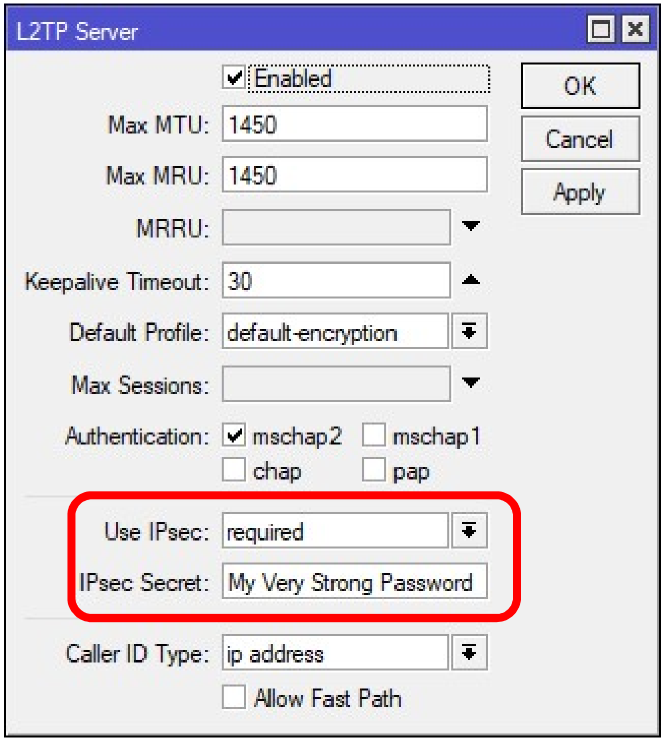
- **PROBLEM**: VPN’s build with PPTP/L2TP use legacy encryption methods
  - OpenVPN and SSTP (Secure Socket Tunneling Protocol) are far more secure, however client and server certificates are required
- **SOLUTION**: Use L2TP with easy IPSEC setup to securely establish “road warrior” connections for mobile devices

IPSEC

- Internet Protocol Security (IPsec) - a set of protocols to support secure communication at the IP layer
- Originally developed alongside IPv6, later backported to IPv4
- Provides encryption to the IP protocol for both IPv4 and IPv6
- Is an extensible protocol under constant development, update and improvement

L2TP with IPSEC

- Easy way to provide IPSEC encryption using existing L2TP services
- Set “Use Ipsec” to yes or required as per your policy
- On mobile device choose L2TP/IPsec PSK or similar option



L2TP Server

☑ Enabled

Max MTU: 1450

Max MRU: 1450

MRRU:

Keepalive Timeout: 30

Default Profile: default-encryption

Max Sessions:

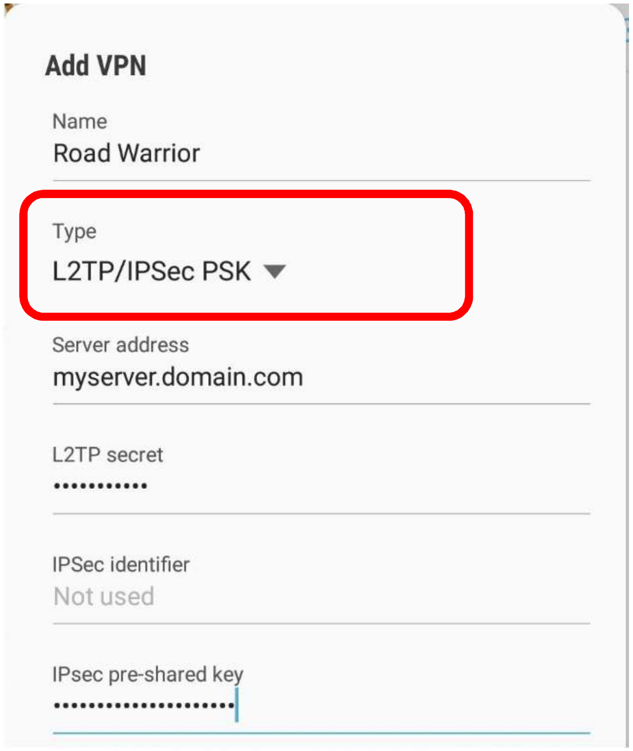
Authentication: ☑ mschap2 □ mschap1 □ chap □ pap

Use IPsec: required

IPsec Secret: My Very Strong Password

Caller ID Type: ip address

□ Allow Fast Path



Add VPN

Name
Road Warrior

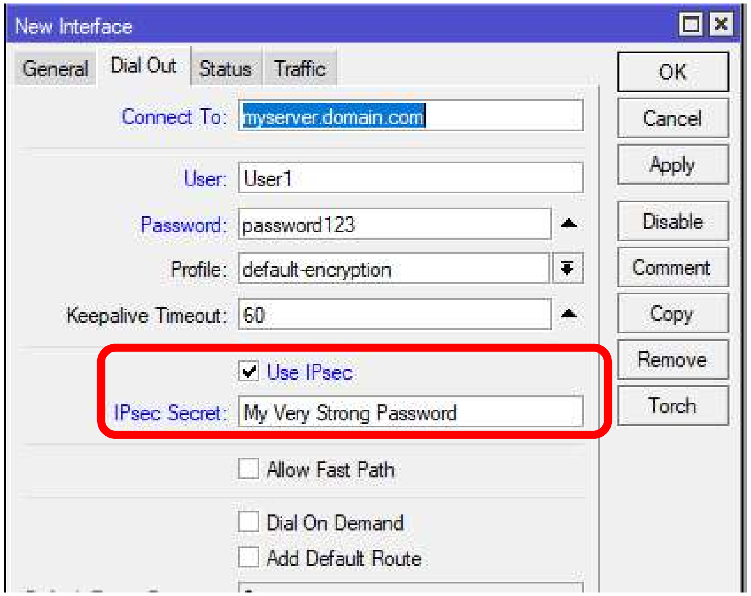
Type
L2TP/IPSec PSK

Server address
myserver.domain.com

L2TP secret
••••••••••

IPSec identifier
Not used

IPsec pre-shared key
••••••••••••••••••••



New Interface

General | Dial Out | Status | Traffic

Connect To: myserver.domain.com

User: User1

Password: password123

Profile: default-encryption

Keepalive Timeout: 60

☑ Use IPsec

IPsec Secret: My Very Strong Password

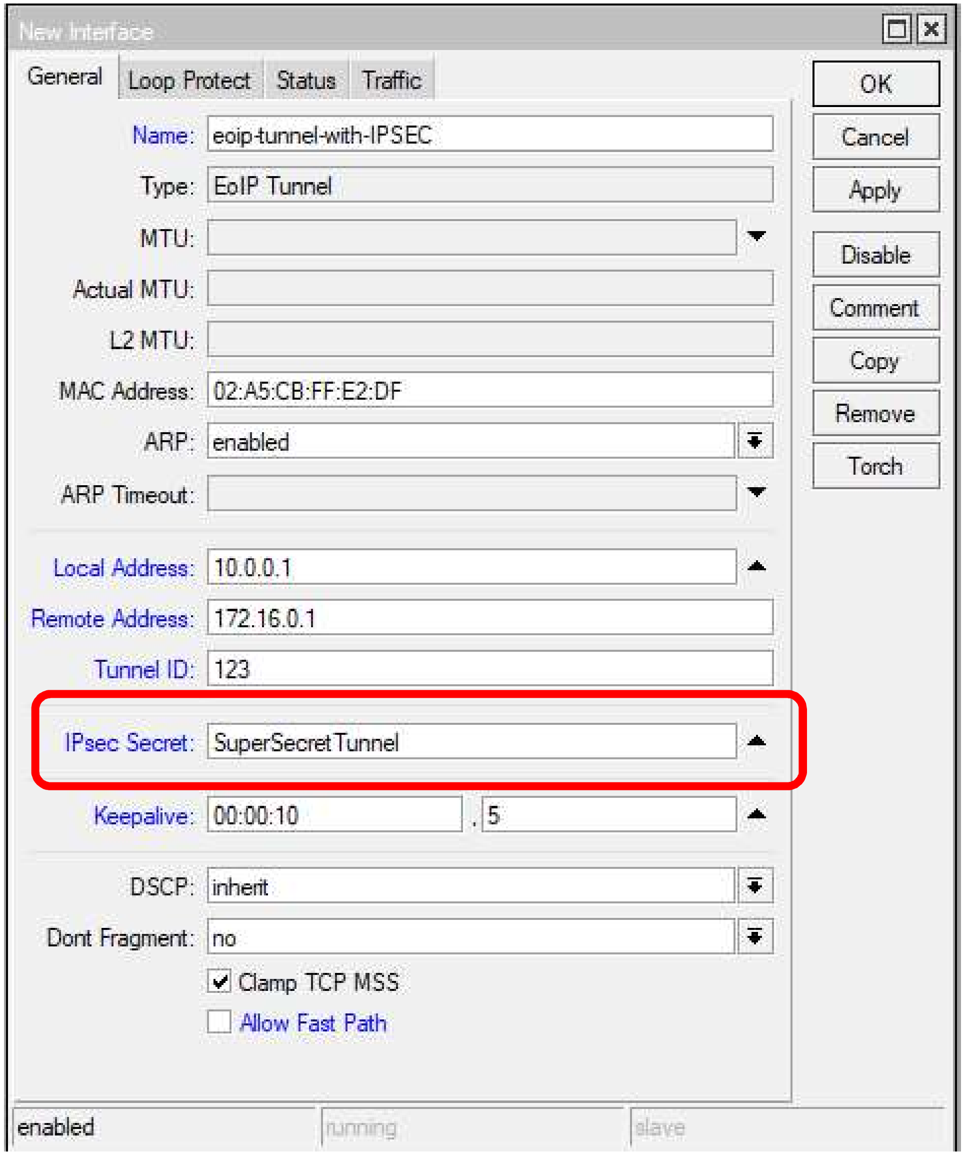
□ Allow Fast Path

□ Dial On Demand

□ Add Default Route

Simple Tunnel with IPSEC

- IPIP, GRE and EoIP tunnels now also support IPSEC encryption under RouterOS
- Simply specify IPSEC secret when setting up tunnel to enable



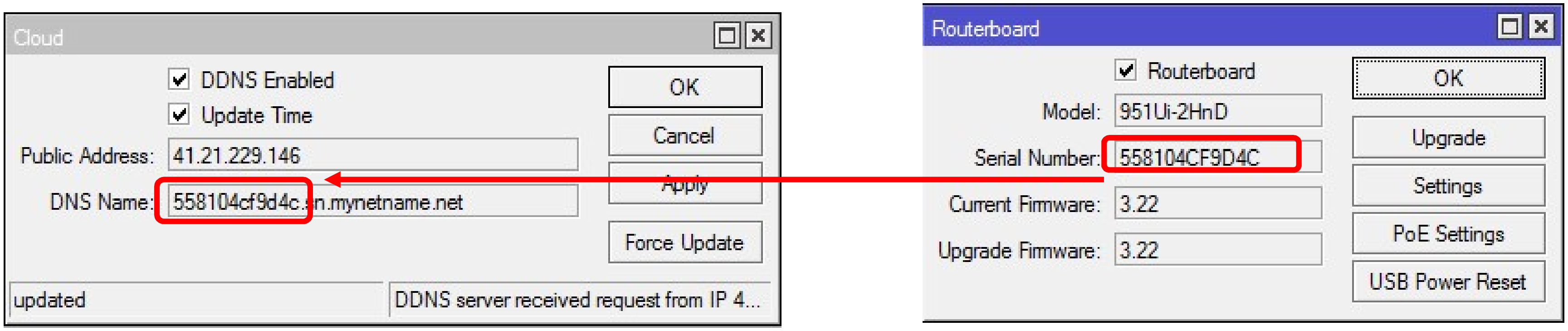
Name: eoip-tunnel-with-IPSEC
Type: EoIP Tunnel
MTU:
Actual MTU:
L2 MTU:
MAC Address: 02:A5:CB:FF:E2:DF
ARP: enabled
ARP Timeout:
Local Address: 10.0.0.1
Remote Address: 172.16.0.1
Tunnel ID: 123
IPsec Secret: SuperSecretTunnel
Keepalive: 00:00:10 . 5
DSCP: inherit
Dont Fragment: no
☑ Clamp TCP MSS
□ Allow Fast Path

enabled | running | slave

IP Cloud Service

- If you run a client providing a dynamic IP address you cannot assign a static DNS
- Past solutions include running a DynDNS client or scripting a solution
- IP → Cloud is a free service from MikroTik that will translate your public outgoing IP to a dynamic DNS server hosted on the MikroTik cloud
- Since the name is taken from the routers serial number you can predict what the name will be

```
[admin@Trainer Dave] /ip cloud> print
     ddns-enabled: yes
      update-time: yes
   public-address: 41.21.229.146
         dns-name: 558104cf9d4c.sn.mynetname.net
           status: updated
          warning: DDNS server received request from IP 41.21.229.146 but
your local IP was 192.168.5.254; DDNS service might not work.
```



☑ DDNS Enabled
☑ Update Time
Public Address: 41.21.229.146
DNS Name: 558104cf9d4c.sn.mynetname.net
updated
DDNS server received request from IP 4...

☑ Routerboard
Model: 951Ui-2HnD
Serial Number: 558104CF9D4C
Current Firmware: 3.22
Upgrade Firmware: 3.22

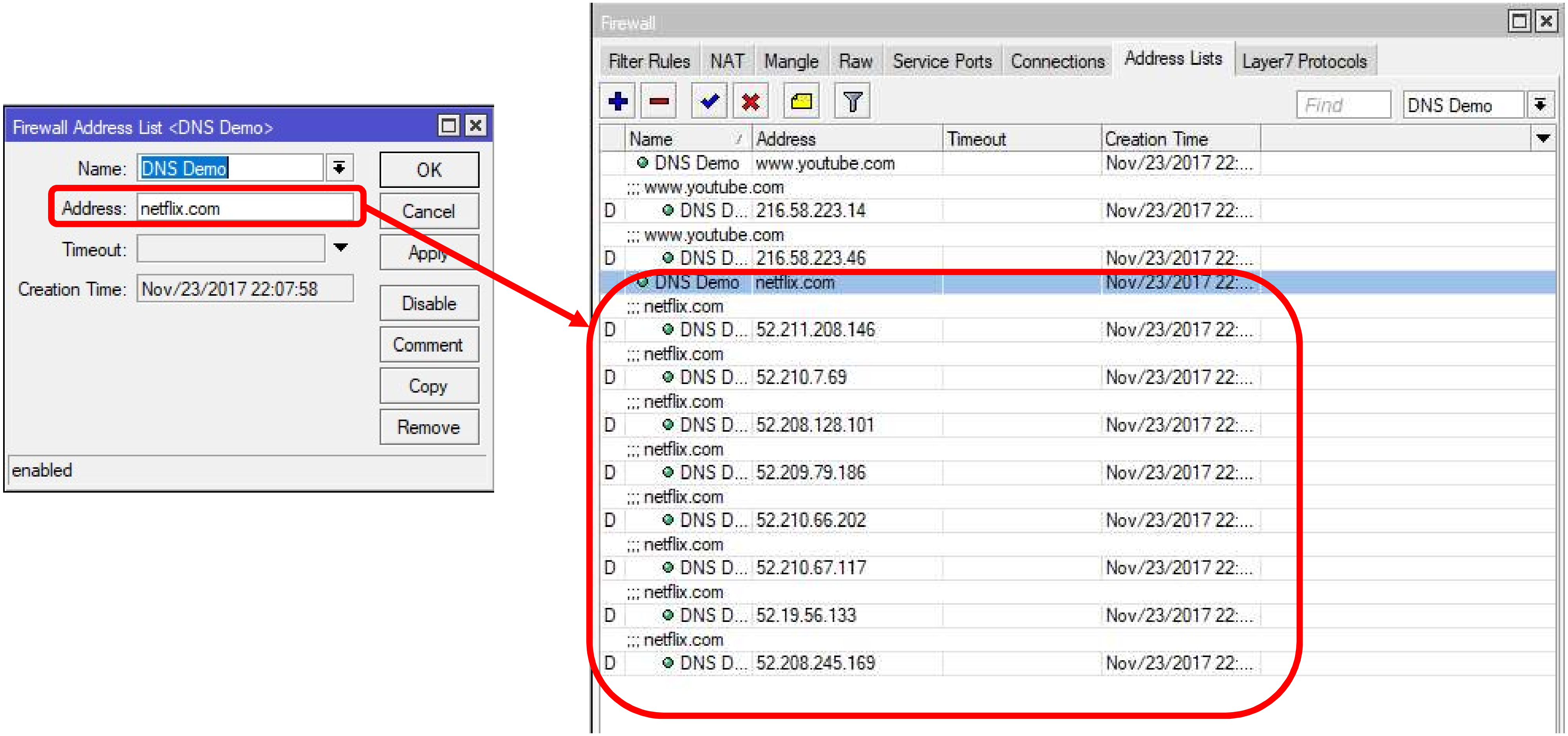
Firewall Improvements

Address list by DNS name

Improved rules for adding addresses

Firewall Address List

- **PROBLEM**: You need to apply firewall rules by DNS name instead of static address
- **SOLUTION**: Firewall address list can now track DNS names for dynamic address generation
- Lists will be refreshed according to upstream TTL record
- Domains with multiple servers will generate multiple records



Name: DNS Demo

Address: netflix.com

Timeout:

Creation Time: Nov/23/2017 22:07:58

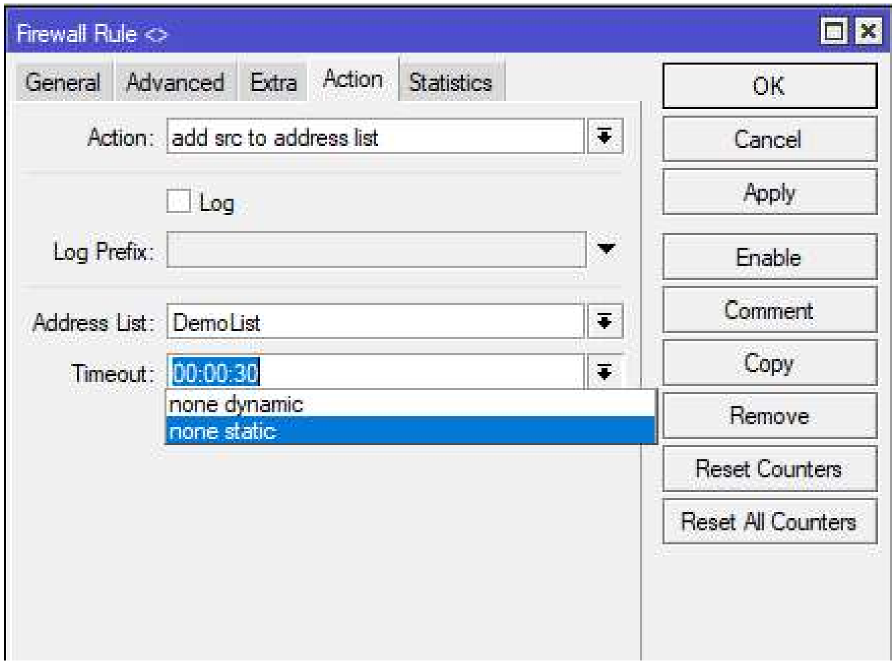
enabled

DNS Demo

	Name	Address	Timeout	Creation Time
	● DNS Demo	www.youtube.com		Nov/23/2017 22:...
	;;; www.youtube.com			
D	● DNS D...	216.58.223.14		Nov/23/2017 22:...
	;;; www.youtube.com			
D	● DNS D...	216.58.223.46		Nov/23/2017 22:...
	● DNS Demo	netflix.com		Nov/23/2017 22:...
	;;; netflix.com			
D	● DNS D...	52.211.208.146		Nov/23/2017 22:...
	;;; netflix.com			
D	● DNS D...	52.210.7.69		Nov/23/2017 22:...
	;;; netflix.com			
D	● DNS D...	52.208.128.101		Nov/23/2017 22:...
	;;; netflix.com			
D	● DNS D...	52.209.79.186		Nov/23/2017 22:...
	;;; netflix.com			
D	● DNS D...	52.210.66.202		Nov/23/2017 22:...
	;;; netflix.com			
D	● DNS D...	52.210.67.117		Nov/23/2017 22:...
	;;; netflix.com			
D	● DNS D...	52.19.56.133		Nov/23/2017 22:...
	;;; netflix.com			
D	● DNS D...	52.208.245.169		Nov/23/2017 22:...

Firewall Address List

- Firewall action “Add src/dst to address list” has improved options
- Choose between a set timeout value, none static or none dynamic



Action: add src to address list

□ Log

Log Prefix:

Address List: DemoList

Timeout: 00:00:30

none dynamic
none static

Question Time