

MikroTik RouterOS

MTCNA

MikroTik Certified Network Engineer

MikroTik SA

Presented by

MikroTikSA

Certified MikroTik Training Partner

Schedule

08:30 – 10:00	Morning Session I
10:30 – 11:00	Morning Session II
12:00 – 13:00	Lunch / Breakaway
13:00 – 14:30	Afternoon Session I
15:00 – 16:30	Afternoon Session II
16:30 – 17:00	Q&A

Course materials – version 16.6.1

Routers, cables

Restrooms and smoking area locations

Course Objective

Provide the necessary knowledge and hands-on training for installing, configuring and troubleshooting network setups built using RouterOS software.

Upon completion of the course you will be familiar with most RouterOS functions

About MikroTik SA

Independent Wireless 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

Instructor and Class

David Savage

- Is a MikroTik Certified Trainer and consultant
- Installs and manages and wireless networks
- Has over 18 years experience in the IT field
- Teaches general networking and MikroTik RouterOS

The Class

- Introduce yourself to the class
- Who you are, company, experience and what you hope to gain from this course

In This Manual

The LAB pages are practical exercises that can be practised in class. Try them out now and learn from your mistakes!

A blue rectangular box with a gradient from light blue at the top to a darker blue at the bottom. The word "LAB" is written in blue, sans-serif capital letters at the top right corner of the box, with a slight reflection effect below it.

LAB

TIPs indicate particularly important points (with a good possibility of an exam question). Note these well.

A red asterisk symbol followed by the word "TIP" in a bold, red, sans-serif font. The text has a slight drop shadow and a white outline.

*TIP

Exams and Certificate

The exam will be written on the afternoon of the last course day

You must have an account on [mikrotik.com](http://www.mikrotik.com) and be enrolled in the training course

- If you do not please register during the course on <http://www.mikrotik.com> and ensure that the trainer enrolls you on the course

You must pass the exam to obtain your certificate

- The passmark is 60%
- If you achieve between 50%-59% you may request to attempt the exam immediately again (1 rewrite per delegate)

Certificates are issued online automatically and will be viewable in your account

All delegates receive a Level4 MikroTik license which will be available in your account after the course

First Access

Ensure that your Ethernet cable is plugged in and lit

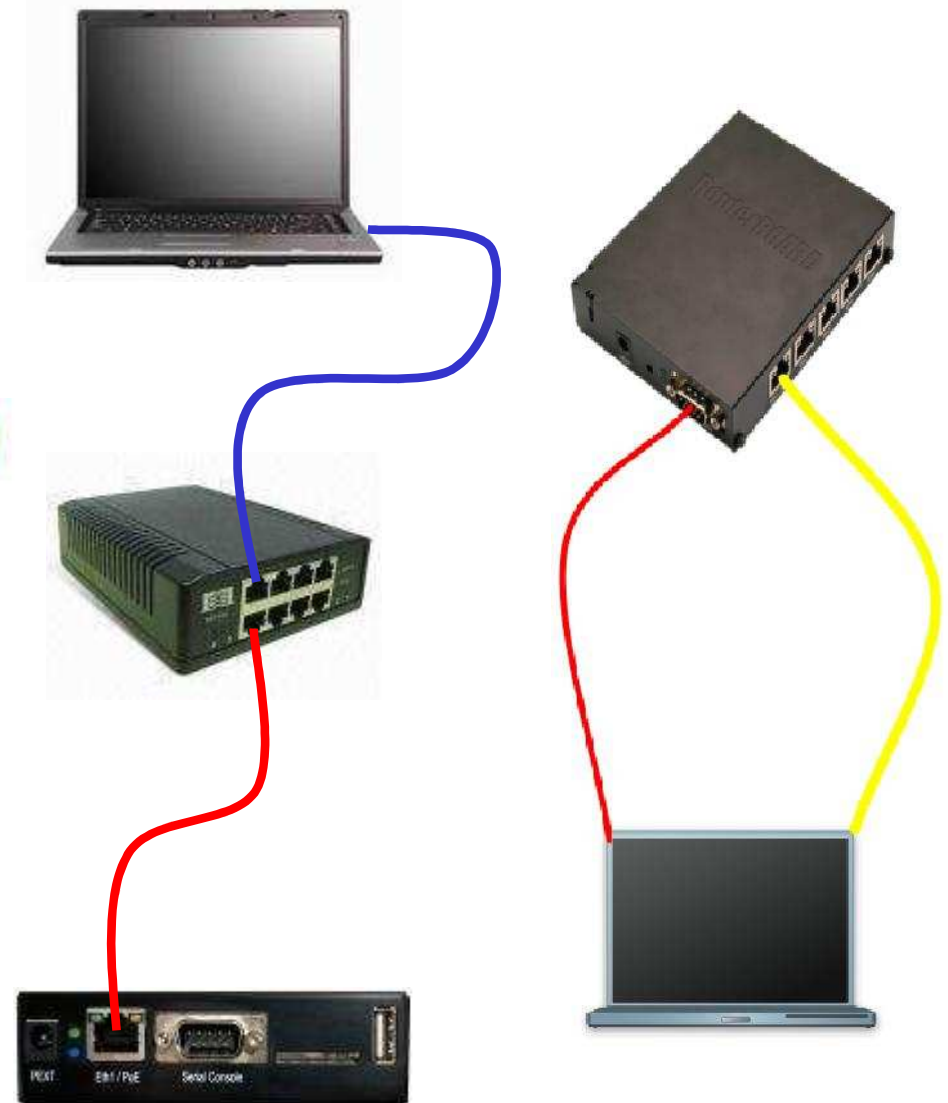
An optional Serial cable can be connected to the serial port

- The default baud rate for current Routerboards is 115200

***TIP**

Disable your windows firewall to allow MAC winbox access

- It is also suggested to disable UAC in Windows7
- Also check for other firewalls e.g Norton Internet Security
- VPN interfaces e.g. VMWare, Hamachi can cause issues



Downloading Winbox Loader

From <http://mikrotik.com/download>

From the trainer router \\10.1.1.254

From any reachable MikroTik Router http://router_IP



**Download Winbox
Here**

**Access Web
Configuration Here**

Accessing the Router

GUI – graphical user interface

Winbox GUI (enabled interface required)

CLI – command line interface

Monitor and keyboard (video adapter required)

Serial terminal (**COM port**)

MAC Telnet (enabled interface required)

Telnet (ip address required)

SSH (ip address required)

Other

http server / webfig (ip address required)

ftp server (ip address required)

Custom API

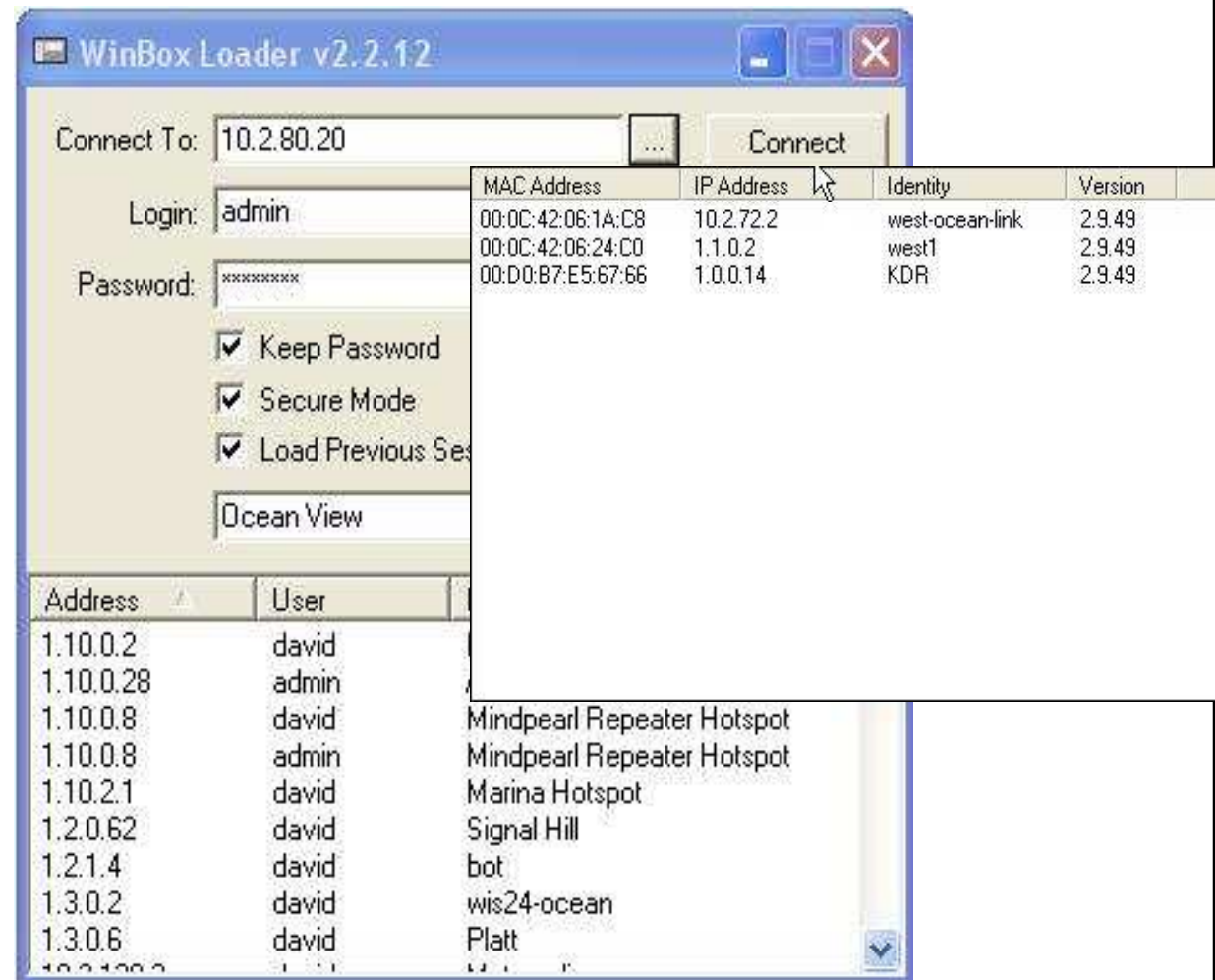
Winbox Loader Options

Winbox loader can connect to the router using

- IP address of the router
- MAC address of the router

Winbox loader can discover and show a list of routers on the LAN segment, if you press the button with three dots [...] next to the address field

Select the router you want to connect to from the list



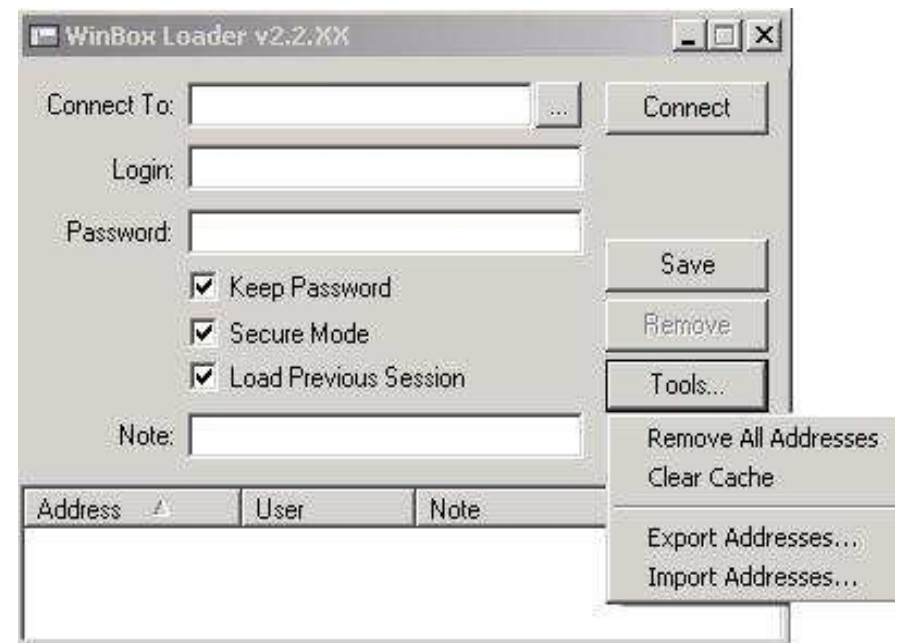
Winbox Loader Maintenance

You can save addresses and passwords for easy access

Use secure mode across unencrypted wireless links

You can Export addresses and Import them on another computer

You can clear the cache and remove all addresses



Connecting to the Router

Connect to the router using it's MAC address

- 'admin' as user name
- no password (hit [Enter])

Winbox Loader should load plugins from the router and open up the router's configuration window

If there is no license for the router, it is going to run for 24h and require you to enter a valid license key

- This only applies to X86 platforms
- All Routerboards come with a full license installed, Level 3-6 depending on model

RouterOS License Levels

Level number	0 FREE	1 DEMO	3 WISP CPE	4 (WISP)	5 WISP	6 Controller
Upgradable To	-	no upgrades	ROS v6.x	ROS v6.x	ROS v7.x	ROS v7.x
Wireless AP	24h limit	-	-	yes	yes	Yes
Wireless Client and Bridge	24h limit	-	yes	yes	yes	yes
RIP, OSPF, BGP protocols	24h limit	-	yes(*)	yes	yes	yes
EoIP tunnels	24h limit	1	unlimited	unlimited	unlimited	unlimited
PPPoE tunnels	24h limit	1	200	200	500	unlimited
PPTP tunnels	24h limit	1	200	200	500	unlimited
L2TP tunnels	24h limit	1	200	200	500	unlimited
OVPN tunnels	24h limit	1	200	200	unlimited	unlimited
VLAN interfaces	24h limit	1	unlimited	unlimited	unlimited	unlimited
HotSpot active users	24h limit	1	1	200	500	unlimited
Queues	24h limit	1	unlimited	unlimited	unlimited	unlimited
User manager active sessions	24h limit	1	10	20	50	Unlimited

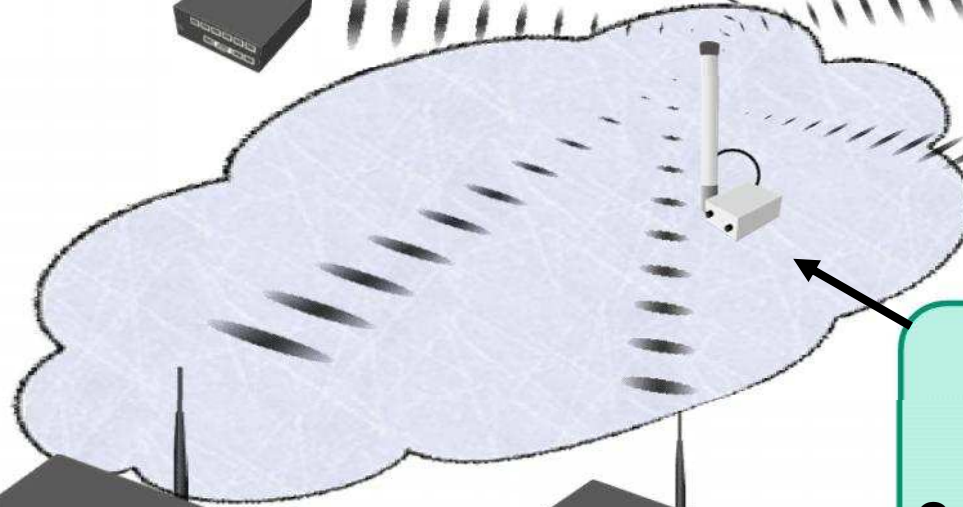
Class Network

X – a unique number given by the teacher. Use it to avoid IP address conflicts

192.168.X.1/24



ether1 IP:192.168.X.254/24
wlan1 IP:10.1.1.X/24



Band: 5GHz
SSID: ap_mtza
DNS:10.1.1.254
Gateway:10.1.1.254



DHCP Hotspot



Band: 2.4GHz
SSID: Internet

Free internet access is provided on a “responsible use” basis. Please don’t abuse it i.e. no massive movie downloads, torrents etc.

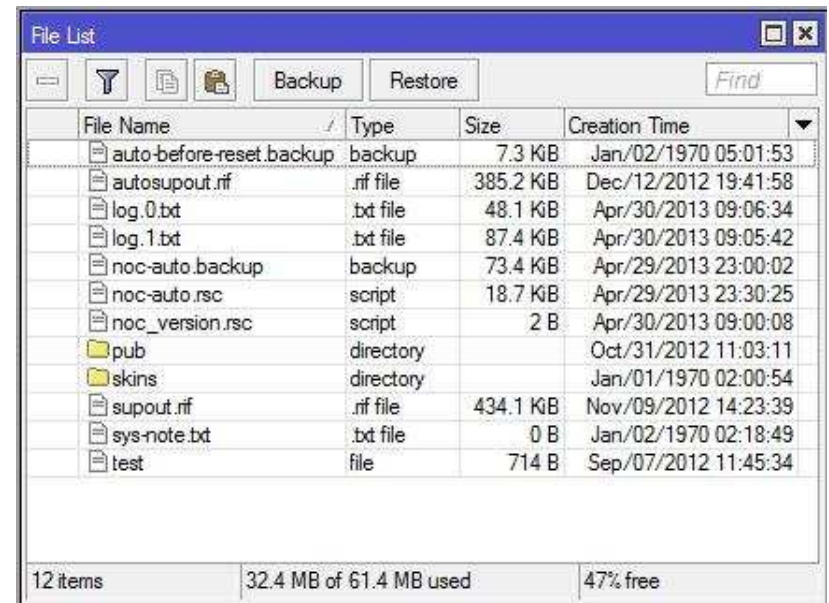
Router File Management

Files such as backups are stored on the router in the Files window. Click on Files in Winbox to access this window now.

To ensure that you do not accidentally restore another users' backup, **please highlight and delete all files in the files menu.**

- None of these files are required for router operation.

You may also backup and restore the router from here (more on this later on)



File Name	Type	Size	Creation Time
auto-before-reset.backup	backup	7.3 KB	Jan/02/1970 05:01:53
autosupout.rif	.rif file	385.2 KB	Dec/12/2012 19:41:58
log.0.txt	.txt file	48.1 KB	Apr/30/2013 09:06:34
log.1.txt	.txt file	87.4 KB	Apr/30/2013 09:05:42
noc-auto.backup	backup	73.4 KB	Apr/29/2013 23:00:02
noc-auto.rsc	script	18.7 KB	Apr/29/2013 23:30:25
noc_version.rsc	script	2 B	Apr/30/2013 09:00:08
pub	directory		Oct/31/2012 11:03:11
skins	directory		Jan/01/1970 02:00:54
supout.rif	.rif file	434.1 KB	Nov/09/2012 14:23:39
sys-note.txt	.txt file	0 B	Jan/02/1970 02:18:49
test	file	714 B	Sep/07/2012 11:45:34

12 items 32.4 MB of 61.4 MB used 47% free

admin@41.76.133.33 (West RB750-UP) - WinBox v5.22 on RB750UP (mipsbe)

Login name and IP/MAC of router
Name of Router
RouterOS Version and Hardware Platform

Uptime: 6d 18:05:27 Date: Apr/30/2013 Time: 13:44:26

Hide Passwords

Interfaces
Wireless

Access Ethernet and Wireless Interfaces here, as well as VLAN, EoIP and other common interfaces

Right Click anywhere up here to add Time, Date, Uptime and other realtime information

IP

Common setting pertaining to IP such as Addresses, Routes, Firewall settings

Files

Router File management

Log

Router Log

Tools

Common Network Management tools such as Ping, Traceroute and Bandwidth Test

New Terminal

Router Command Prompt (CLI)

RouterOS WinBox

MetaROUTER
Make Supout.rif
Manual
Exit

Basic Router Setup I

User Management
Assigning IP Addresses
Basic Wireless Theory
Station Wireless Configuration
DHCP Client
Setting up DNS
Masquerading
Accessing the Internet

Default User

'admin' is the default user of the router after installing the RouterOS

- there is no password for 'admin'
- 'admin' belongs to the group 'full'
- group 'full' has the maximum permissions

To secure the router

- passwords can be set for users
- new users can be added
- if necessary, new user groups can be added
- User groups give finer grained control over access permissions

Adding a User

The screenshot displays a network management interface with three overlapping windows:

- User List:** A table showing a list of users with columns for Name, Group, and Allowed Address. The table contains 7 items.
- New User:** A dialog box for adding a new user. The Name field is set to 'user1', the Group is set to 'write', and the Allowed Address field is empty.
- Change Password:** A dialog box for changing a password. The New Password field is filled with four asterisks, and the Confirm Password field is filled with three asterisks.

Name	Group	Allowed Address
Byron Ismay		
byron	write	
David Savage		
david	full	
dtech	write	
Local Emergency user		
local	full	127.0.0.1
Grant Delaney		
mufasa	write	
theunis	full	
Rehan Weekend IT		
wis24-7	full	

Router Password



If you lose your password THERE IS NO WAY TO RECOVER IT

The only thing you can do is a hard reset using the reset button on the router, or re-install the software with Netinstall

- All settings on the router will be lost in both cases
- See http://wiki.mikrotik.com/wiki/Manual:Password_reset for other router types



To reset RouterOS config
Hold metal object in here
while the board boots.



User Groups

User groups are used to customise permissions for various levels of access

Default groups are Read, Change and Full

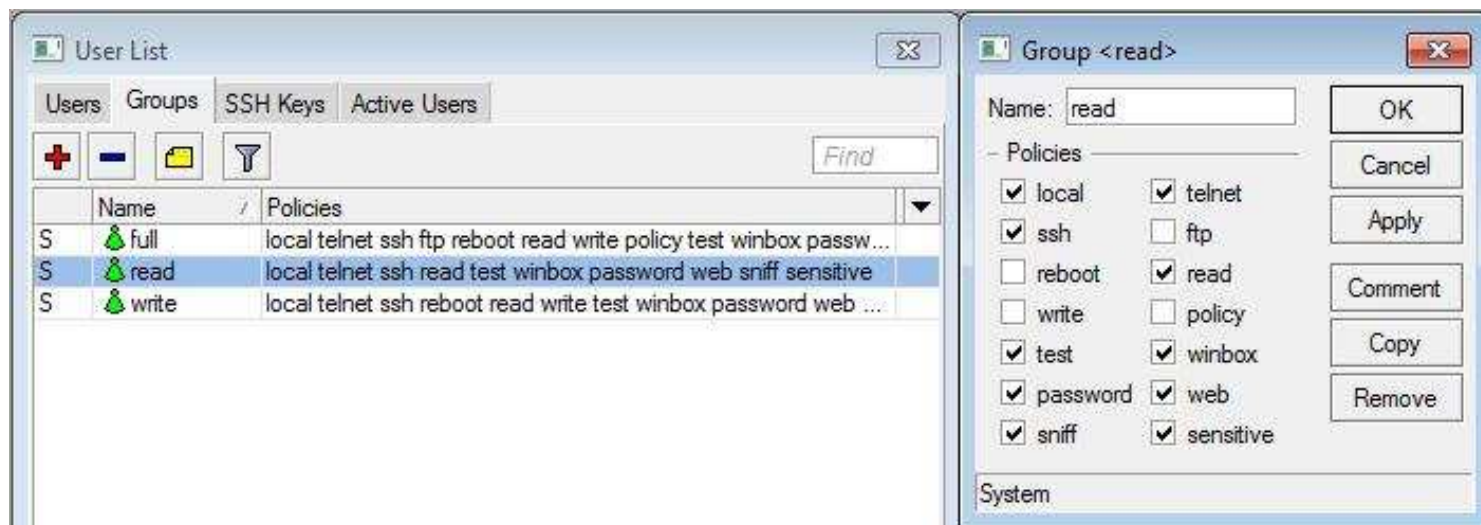
The default groups can be modified, you can also add additional custom groups

- Note that by default the Read group has reboot rights



You can create custom groups for WebBox with custom skins

- Create the skin in WebBox then assign to a custom group



Permission	Policy
local	policy that grants rights to log in locally via console
ssh, telnet, winbox, web, API	policy that grants rights to log in remotely via ssh, telnet, winbox, web or API
ftp	policy that grants full rights to log in remotely via FTP and to transfer files from and to the router. Users with this policy can both read, write and erase files, regardless of "read/write" permission, as that deals only with RouterOS configuration.
read	policy that grants read access to the router's configuration. All console commands that do not alter router's configuration are allowed. Doesn't affect FTP
write	policy that grants write access to the router's configuration, except for user management. This policy does not allow to read the configuration, so make sure to enable read policy as well
policy	policy that grants user management rights. Should be used together with write policy. Allows also to see global variables created by other users (requires also 'test' policy).
test	policy that grants rights to run ping, traceroute, bandwidth-test, wireless scan, sniffer, snoop and other test commands
reboot	policy that allows rebooting the router
reboot	policy that allows rebooting the router
password	policy that grants rights to change the password
sniff	policy that grants rights to use packet sniffer tool.
sensitive	grants rights to see sensitive information in the router, see http://wiki.mikrotik.com/wiki/Manual:Router_AAA#User_Groups as to what is sensitive.

User Management

LAB

Add a user for yourself with full access permissions

Login with your new user and change the default admin account to Read Only

Make sure the Read Only account cannot reboot the router

Add a custom user group to use for Bandwidth Testing only

Add a user called btest with no password to be used for bandwidth tests

- Needs Read, Test and Winbox rights

Configuration Steps

Connect your laptop to the router (assign IP Address)

Connect the router to the wireless network (wireless configuration)

Do the necessary setup for network access (DHCP Client)

Do the necessary setup for Internet access (DNS, NAT)



Checking IP Devices with PING

Ping is a basic network troubleshooting tool

- It is based around ICMP – Internet Control Message Protocol which along with Traceroute and Path MTU Discovery form a basis for network troubleshooting

It shows whether or not a host IP address is contactable

- Just because a host cannot be pinged does not mean it is not there, a firewall might be preventing ICMP traffic

It is available from most IP devices

- From Winbox: Tools → Ping
- From New Terminal: ping [host_ip or DNS_name]
- From Windows Command Prompt: Start → Run → cmd.exe

Assigning an IP Address

Go to IP → Address in winbox

Click “+” to open up new address dialogue box

- Specify the IP address AND netmask, e.g. 192.168.44.254/24
- Select the interface, e.g. ether1
- Click “OK”

There is no need to specify a Network address, since it is calculated automatically from the address and netmask



Changing an IP Address

When you need to change an IP address, it is best to remove the old address and add a new one as described before

In case of editing the IP address, do not forget that the Network address may change and need to be recalculated (v1-4.x only)

- Remove the previous network address so that RouterOS calculates new values





IP Addressing

LAB

Add an IP address to your routers Ether1 interface

- It should be 192.168.xy.254/24
- Don't forget the subnet mask in CIDR notation!

Change your laptop's IP address to 192.168.xy.1

- Your router will be your Default Gateway and DNS Server

Make sure you can ping your router from your laptop
Command Prompt

Connect to your router using its IP address instead of MAC address

Where can you confirm that you have connected by IP?

What is Wireless?

Broadly speaking, wireless refers to technology which allows the transmission of data by the transmission of electromagnetic waves

MikroTik supports wireless through the use of either integrated electronics or the addition of a mini-pci wireless card

The card may support multiple frequencies (dual-band) and multiple band widths (5MHz, 10MHz, 20MHz, 40MHz, 80MHz and any subset in between in 500KHz increments)

The card may support multiple technologies (CSMA/CA, MIMO, Turbo Mode, AC Mode)

Common Terms

A **service set** is all the devices associated with a local or enterprise IEEE 802.11 wireless local area network (LAN)

A **service set identifier (SSID)** is a name that identifies a particular 802.11 wireless LAN

- A client device receives broadcast messages from all Access Points within range advertising their SSIDs

IEEE 802.11 is a set of standards for implementing wireless local area network (WLAN) computer communication in the 2.4, 3.6 and 5 GHz frequency bands

Supported Frequencies

Wireless cards usually support the following frequencies:

- For all 2.4GHz bands: 2312-2499MHz in 5Mhz increments
- 2.4 Ghz “standard” channels 1 to 11 spans the frequencies from 2412Mhz – 2462Mhz
- For all 5GHz bands: 4920-6100MHz in 20Mhz increments
- 5Ghz “standard” channels from 5180-5320 and from 5745-5825 in 20Mhz increments

Your country regulations allow only particular frequency ranges

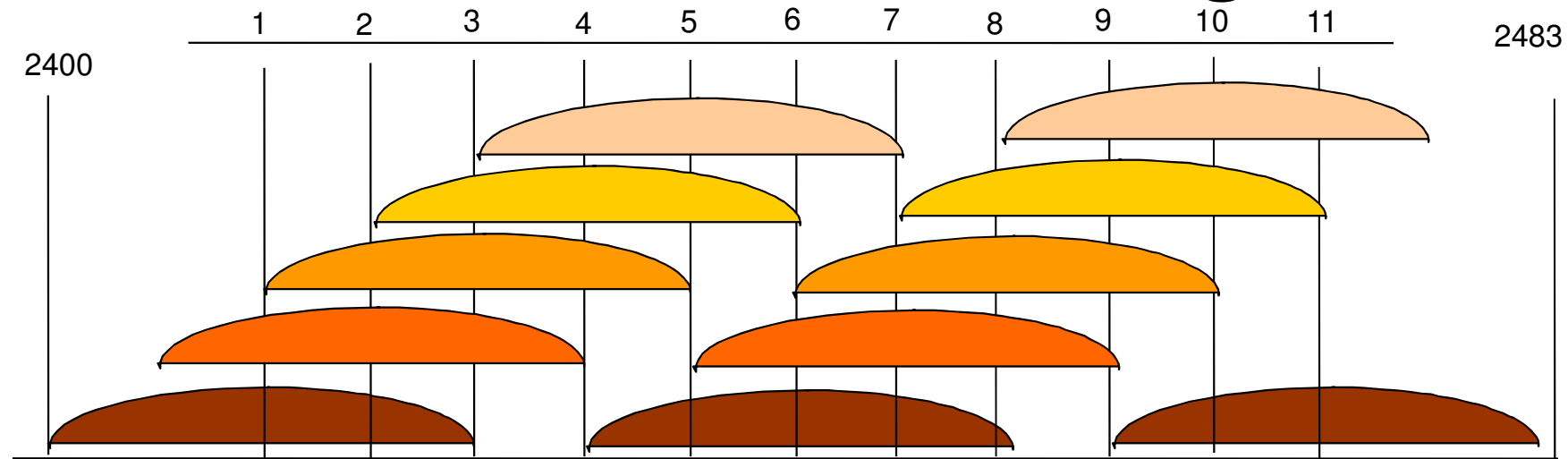
Superchannel “test mode” unlocks all frequencies supported by the wireless hardware

Wireless Standards

IEEE Standard	Frequency	Speed
802.11a	5GHz	54Mbps
802.11b	2.4GHz	11Mbps
802.11g	2.4GHz	54Mbps
802.11n	2.4 and 5GHz	Up to 450 Mbps*
802.11ac	5GHz	Up to 1300 Mbps*

* Depending on RouterBOARD model

Channels- 802.11b/g



11 channels (US), 22 MHz wide

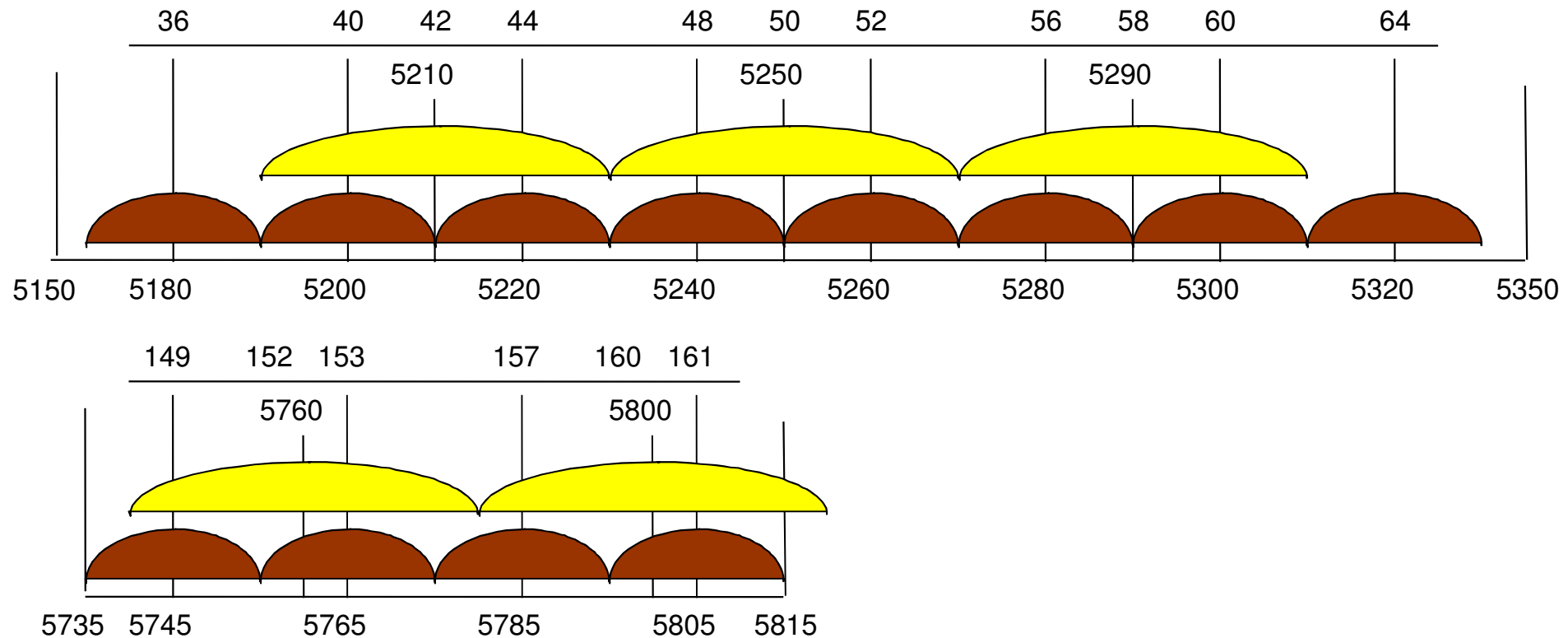
- South Africa can also access channel 12 and 13
- Not all devices support these channels

3 non-overlapping channels

3 Access Points can occupy same area without interfering

- If channels 1,6,11 are occupied then there is no interference free channel

Channels- 802.11a/n



12 channels, 20 MHz wide

5 turbo channels, 40MHz wide

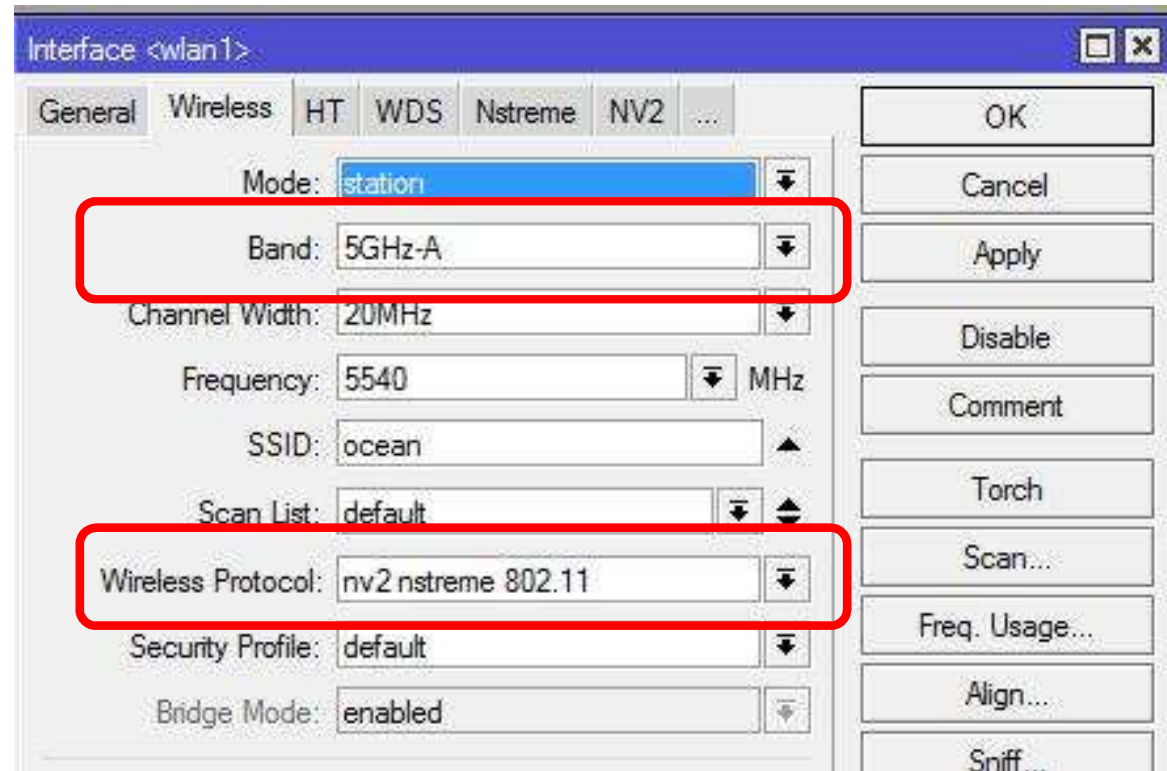
In theory we have multiple non-overlapping channels

In reality we need to leave at least 20 Mhz between channels
(40Mhz recommended)

Wireless Modulation Settings

Use BAND to select a/b/g/n/ac mode of operation (backward compatible modes are possible)

Use Wireless Protocol to select 802.11 / Nstreme / NV2 operation



Protocol Settings

Value	AP	Client
unspecified	establish nstreme or 802.11 network based on old nstreme setting	connect to nstreme or 802.11 network based on old nstreme setting
any	same as unspecified	scan for all matching networks, no matter what protocol, connect using protocol of chosen network
802.11	establish 802.11 network	connect to 802.11 networks only
nstreme	establish Nstreme network	connect to Nstreme networks only
Nv2	establish Nv2 network	connect to Nv2 networks only
Nv2-nstreme-802.11	establish Nv2 network	scan and connect to Nv2 networks, otherwise scan and connect to Nstreme networks, otherwise scan and connect to 802.11 network.
Nv2-nstreme	establish Nv2 network	scan and connect to Nv2 networks, otherwise scan and connect to Nstreme networks

Wireless Interface Mode Settings

bridge/ap-bridge – AP mode; bridge mode supports only one client

station – client which can not be bridged

station-pseudobridge/station-pseudobridge-clone – client which can be bridged (with limitations)

alignment-only – for positioning antennas

nstreme-dual-slave – card will be used in nstreme-dual interface

wds-slave – works as ap-bridge mode but adapts to the WDS peers frequency

station-wds – client which can be bridged (AP should support WDS feature)

station-bridge – NV2-only mode for client bridging without WDS

Wireless Station

Joins a Service Set as defined by SSID

Follows the Access Point within the Scan List

- Frequency setting has no effect
- Scan list also depends on Country setting

Restrictions based on Connect List rules

Use the Scan tool to find Access Points

When you highlight an entry in the Scan List and select Connect the router:

- Enables the wireless card if it is disabled
- Sets the mode to
 - Station for non-RouterOS access points
 - Station-bridge for RouterOS access points
- This will overwrite other modes you may have set e.g. ap-bridge, station-wds, station-pseudobridge etc.

Scanning for Networks

Letter	Meaning
A	Active
B	Base Service Set
P	Privacy (Security)
R	RouterOS AP
N	Nstreme Network
T	TDMA (NV2)
W	WDS (Wireless Distribution System)

Interface <wlan1 >

General | **Wireless** | Data Rates | Advanced | WDS | ...

Mode: station

Band: 2.4GHz-B/G

Frequency: 2432 MHz

SSID: AP2G

Radio Name: 000C420CB283

Scan List:

Security Profile: default

Frequency Mode: manual txpower

Country: no_country_set

Antenna Gain: 0 dBi

DFS Mode: none

proprietary Extensions: pre-2.9.25

Default AP Tx Rate: bps

Default Client Tx Rate: bps

Default Authenticate

Default Forward

Hide SSID

OK
Cancel
Apply
Disable
Comment
Scan...
Freq. Usage...
Align...
Sniff...
Snooper...

Scan <wlan1 > (running)

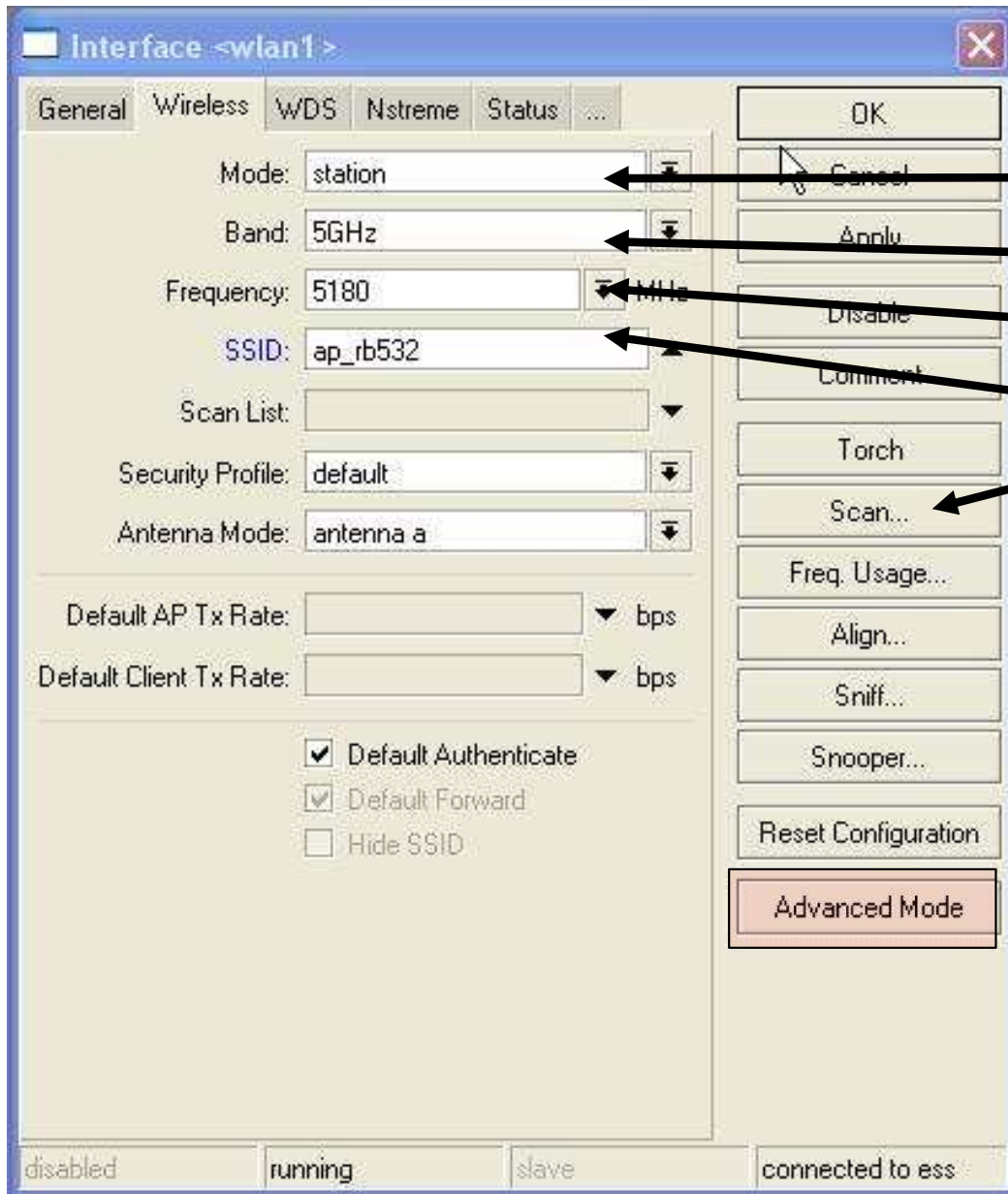
Find

Start
Stop
Close
Connect

	Address	SSID	Band	Frequ...	Signa...	Radio Name	RouterO...
AB	00:02:6F:08:53:18		2.4GHz-G	2432	-41		
AB	00:02:6F:33:C7:B1	MikroTik	2.4GHz-G	2412	-89		
ABR	00:02:6F:45:15:43	AP2G	2.4GHz-G	2432	-65	00026F451543	3.0beta7
ABR	00:0B:68:31:52:69	tests	2.4GHz-G	2452	-93	000B68315269	2.9.27
ABP	00:0B:68:37:56:94	hotspot	2.4GHz-G	2412	-54	HotSpot2	3.0beta6
ABR	00:0B:68:37:5B:B4	dzintars	2.4GHz-G	2442	-79	testa_ruters	2.8.28
BR	00:0B:68:37:62:70	MikroTik	2.4GHz-G	2412	-95	000B68376270	2.9.17
ABP	00:0B:68:37:67:0D	hotspot	2.4GHz-G	2412	-47	HotSpotMain	3.0beta5
ABR	00:0B:68:4D:02:29	ap_laptop	2.4GHz-G	2412	-91	000B684D0229	2.9.39
ABP	00:0B:68:4D:03:6B	hotspot	2.4GHz-G	2412	-71	HotSpot4	3.0beta6
ABP	00:0B:68:4D:03:99	hotspot	2.4GHz-G	2412	-78	HotSpot5	3.0beta6
ABP	00:0B:68:4D:04:2A	hotspot	2.4GHz-G	2412	-75	HotSpot1	3.0beta6
ABR	00:0C:42:05:01:39	test_ap	2.4GHz-G	2412	-90	000C42050139	2.9.19
ABR	00:0C:42:05:05:8A	Uldim2	2.4GHz-G	2457	-67	000C4205058A	3.0beta6
ABR	00:0C:42:05:06:F3	Demo	2.4GHz-G	2452	-94	000C420506F3	2.9.39

22 items [1 selected]

Wireless Basic Configuration



Wireless operating mode

Frequency Band

Channel

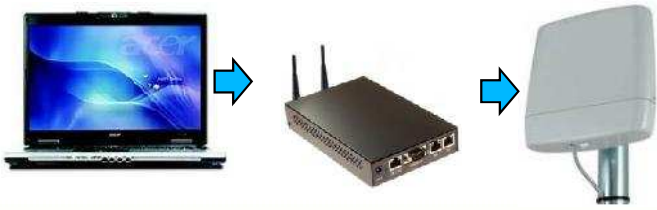
Service Set Identifier

Scan tool used for finding Access Points

The wireless configuration is accessed from the Wireless>Interfaces tab

Not all the configuration options are shown – use Advanced Mode button to display all options

The 4 fields above are all you will need for basic wireless configurations



Wireless Setup

LAB

Enable your wireless interface on the router (Wlan1)

Set “band” to 5Ghz and press “Apply”

Make sure that the mode is on “Station”

Scan your area for wireless networks in this band by pressing the “Scan” button

Connect to the network with SSID: ap_mtza

Monitor the status of wireless connection

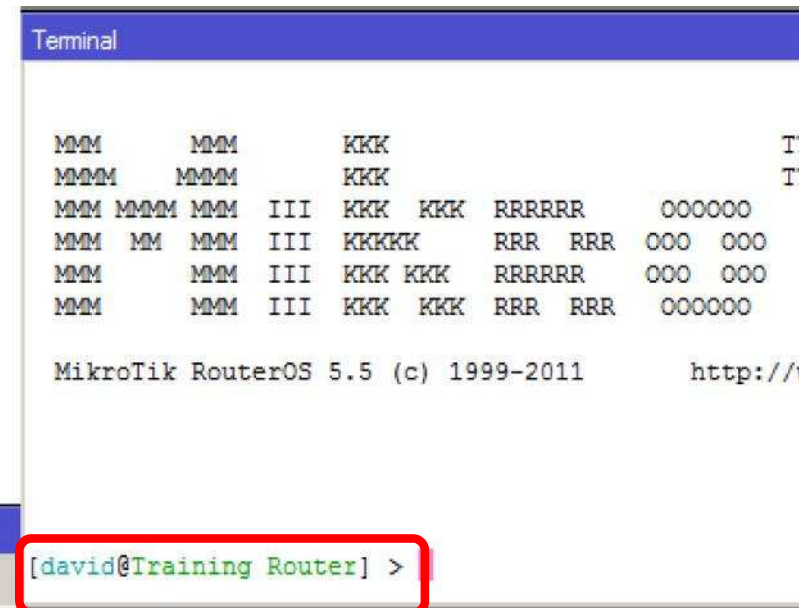
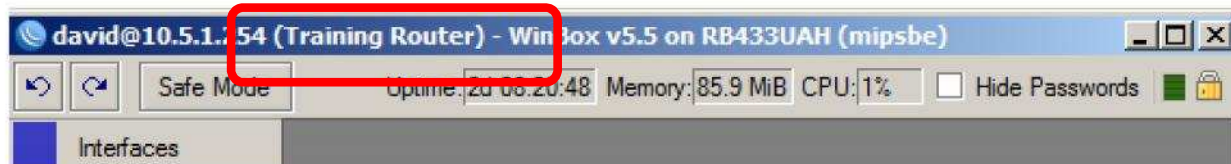
- Is it connected and running?
- Is there an entry in **Wireless>Registration**?

System Identity

You can use **System** → **Identity** to set the identity of your router.

This will identify your router in various places

- At the top of the main winbox window
- In **IP > Neighbours**
- In a Terminal window



The screenshot shows the 'Neighbor List' window in WinBox. It has two tabs: 'Neighbors' and 'Discovery Interfaces'. The 'Neighbors' tab is active, showing a table of discovered neighbors. A red box highlights the 'Identity' column in the table.

Interface	IP Address	MAC Address	Identity	Platform	Version	Board Na...	IPv6
ether2	10.0.28.105	00:0C:42:4...0F:E3	Study AP	MikroTik	3.31	RB411AH	no
ether2	10.0.28.107	00:0C:42:8...5A:59	Brag Room	MikroTik	4.10	RB750	no
ether2	10.0.28.254	00:0C:42:7...1E:A5	Slink Office Core Ro...	MikroTik	5.2	RB493AH	no
wlan1	10.1.1.11	00:0C:42:6...13:CA	11_Tiaan	MikroTik	5.5	RB433	no
wlan1	10.1.1.12	00:0C:42:0...AA:E2	12_tobie	MikroTik	5.5	RB433	no
wlan1	10.1.1.13	00:0C:42:6...32:8C	13_Deon	MikroTik	5.6	RB433AH	no
wlan1	10.1.1.24	00:0C:42:6...13:CD	24_Jaco	MikroTik	5.5	RB433	no
wlan1	10.1.1.25	00:0C:42:6...9C:22	25_Hennie	MikroTik	5.5	RB333	yes

Neighbour Viewer

By default discovery is turned on for all Ethernet and wireless interfaces

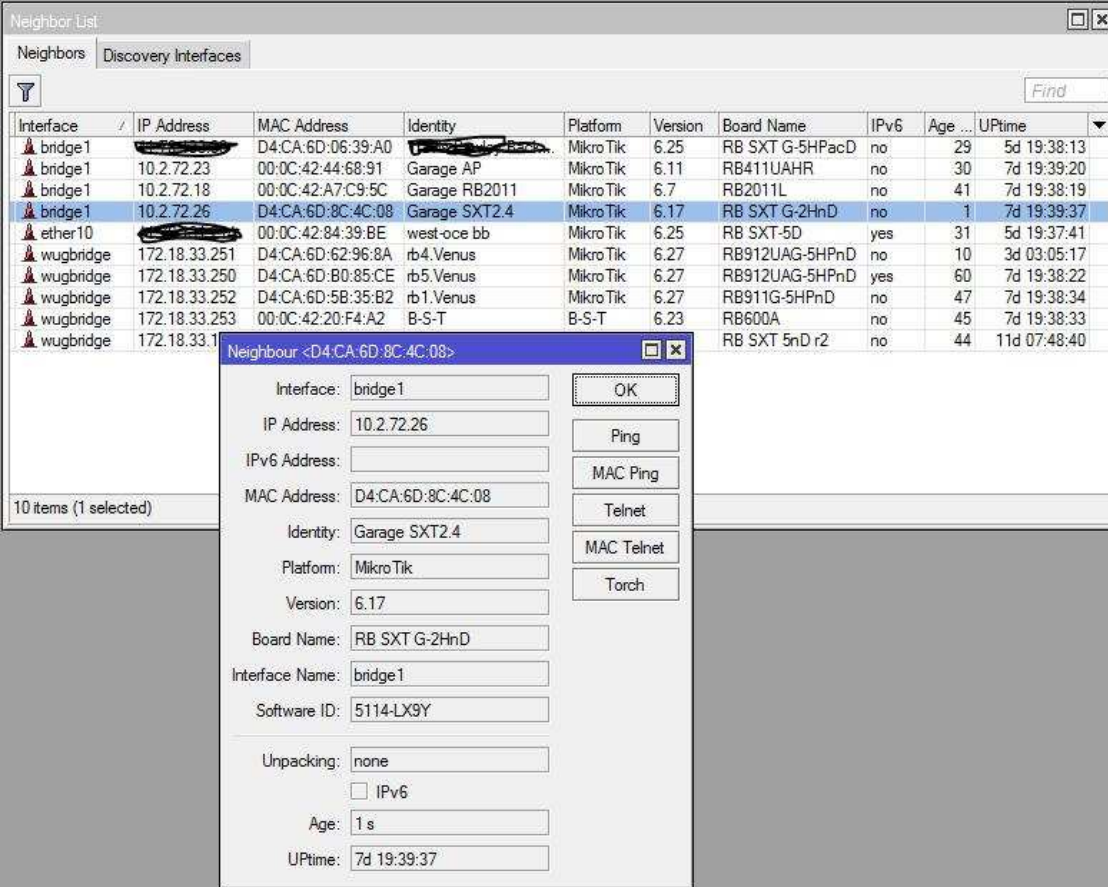
When enabled the router will send out basic information on its system and process received discovery packets broadcasted in Layer-2 network

Enable discovery to see your neighbours and the trainer router

MNDP operates on layer2 (local) networks

Neighbour Discovery uses UDP port 5678

***TIP**



The screenshot displays the 'Neighbor List' window with the 'Discovery Interfaces' tab selected. A table lists discovered neighbors with columns for Interface, IP Address, MAC Address, Identity, Platform, Version, Board Name, IPv6, Age, and Uptime. One neighbor is selected, and a detailed view window is open for it.

Interface	IP Address	MAC Address	Identity	Platform	Version	Board Name	IPv6	Age	Uptime
bridge1	[REDACTED]	D4:CA:6D:06:39:A0	[REDACTED]	MikroTik	6.25	RB SXT G-5HPacD	no	29	5d 19:38:13
bridge1	10.2.72.23	00:0C:42:44:68:91	Garage AP	MikroTik	6.11	RB411UAHR	no	30	7d 19:39:20
bridge1	10.2.72.18	00:0C:42:A7:C9:5C	Garage RB2011	MikroTik	6.7	RB2011L	no	41	7d 19:38:19
bridge1	10.2.72.26	D4:CA:6D:8C:4C:08	Garage SXT2.4	MikroTik	6.17	RB SXT G-2HnD	no	1	7d 19:39:37
ether10	[REDACTED]	00:0C:42:84:39:BE	west-oce bb	MikroTik	6.25	RB SXT-5D	yes	31	5d 19:37:41
wugbridge	172.18.33.251	D4:CA:6D:62:96:8A	rb4.Venus	MikroTik	6.27	RB912UAG-5HPnD	no	10	3d 03:05:17
wugbridge	172.18.33.250	D4:CA:6D:80:85:CE	rb5.Venus	MikroTik	6.27	RB912UAG-5HPnD	yes	60	7d 19:38:22
wugbridge	172.18.33.252	D4:CA:6D:58:35:B2	rb1.Venus	MikroTik	6.27	RB911G-5HPnD	no	47	7d 19:38:34
wugbridge	172.18.33.253	00:0C:42:20:F4:A2	B-S-T	B-S-T	6.23	RB600A	no	45	7d 19:38:33
wugbridge	172.18.33.1					RB SXT 5nD r2	no	44	11d 07:48:40

Neighbour <D4:CA:6D:8C:4C:08>

Interface: bridge1
IP Address: 10.2.72.26
IPv6 Address:
MAC Address: D4:CA:6D:8C:4C:08
Identity: Garage SXT2.4
Platform: MikroTik
Version: 6.17
Board Name: RB SXT G-2HnD
Interface Name: bridge1
Software ID: 5114-LX9Y
Unpacking: none
Age: 1 s
Uptime: 7d 19:39:37

Setting up the router



Click on **System** → **Identity**

Set the system identity of the board to XY_your-name

Example: ***55_BigDave***

Set the wireless cards' radio name to

XY_your-name_interface_name. Example:

55_BigDave_wlan1” (TIP: use the *Advanced* button)

Enable Discovery on your Wlan interface (or ensure it was enabled by default

- Do your neighbours show up in IP Neighbours?

DHCP

In TCP/IP based networks, an IP address must be assigned to each computer

An IP address is a unique numeric identifier that identifies computers on the network.

The Dynamic Host Configuration Protocol (DHCP) is a service that can be implemented to automatically assign unique IP addresses to (DHCP-enabled) clients.

It does not have much built in security - thus it is constrained to trusted networks

DHCP server always listens on UDP port 67 DHCP client - on UDP port 68

DHCP Lease Process

DHCPDISCOVER: This message is used to request an IP address lease from a DHCP server; sent as a broadcast packet over the network, requesting for a DHCP server to respond to it

DHCPOFFER: This message is a response to a DHCPDISCOVER message, and is sent by one or numerous DHCP servers.

DHCPREQUEST: The client sends the initial DHCP server which responded to its request a DHCP Request message.

DHCPACK message: The DHCP Acknowledge message is sent by the DHCP server to the DHCP client and is the process whereby which the DHCP server assigns the IP address lease to the DHCP client.



DHCP client

The client can accept:

- IP address with respective netmask
- Default gateway
- Two DNS server addresses
- Two NTP server addresses
- Domain name
- WINS-server information

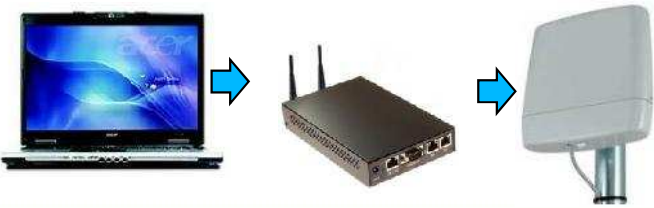
These settings will not override those you had on your router before.

The client can provide certain ID information to the server (see Hostname and Client ID in DHCP Server)

DHCP Client

The screenshot shows the RouterOS WinBox interface. On the left sidebar, the 'IP' menu is highlighted with a red circle. Below it, the 'DHCP Client' option is also highlighted with a red circle. In the main window, the 'DHCP Client' configuration window is open for the 'ether1' interface. The window has a header with a '+' button circled in red. The configuration fields include: Interface: ether1, Hostname: (empty), Client ID: (empty), Use Peer DNS (checked), Use Peer NTP (checked), Add Default Route (checked), and Default Route Distance: 0. The status at the bottom is 'disabled' and 'stopped'.

The screenshot shows the 'DHCP Client <bridge1>' configuration window. The 'Status' tab is active. The configuration fields are: IP Address: 10.2.72.27/27, Gateway: 10.2.72.2, DHCP Server: 41.223.35.59, Expires After: 2d 23:59:42, Primary DNS: 168.210.2.2, and Secondary DNS: 41.223.35.6. The status at the bottom is 'disabled' and 'bound'.



DHCP Client

LAB

Add a DHCP client to the wireless interface

Specify all the checkbox options

Check DHCP Client Status – what address is assigned?

Check your settings in the following:

- IP Addresses
- IP DNS
- System NTP Client
- IP Routes

Check the following

- Ping to an IP address 168.210.2.2
- Ping to a DNS address www.google.com

Advanced: What is Default Route Distance?

DNS Client and Cache

DNS cache minimizes DNS requests to an external DNS server as well as DNS resolution time

MikroTik router's can act as a DNS server for any DNS-compliant clients

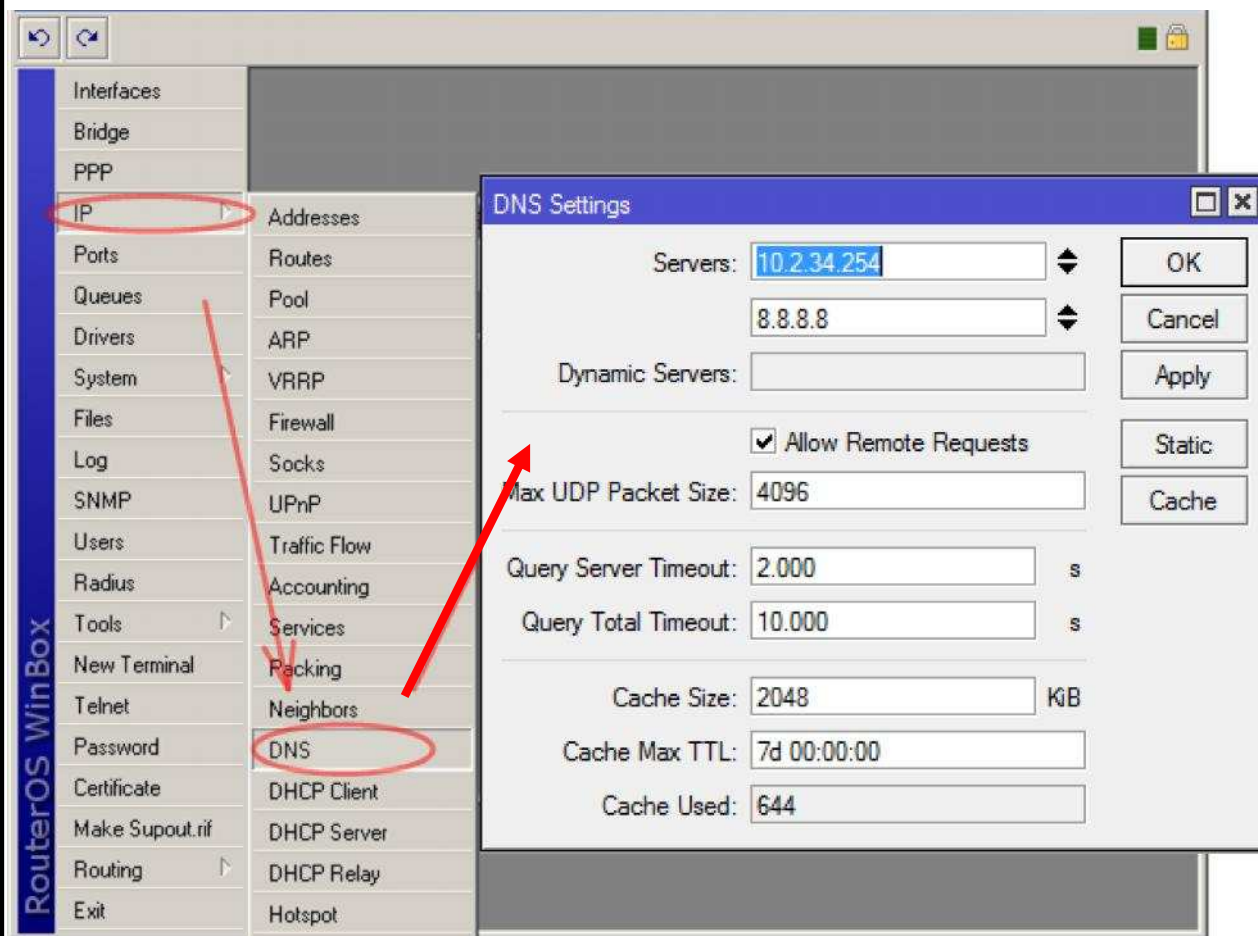
Adding DNS Server address/es provides domain name resolution for the router itself

To use as a caching-only server, check the "Allow Remote Requests" box

- This allows the router to be used as a DNS server
- Be very careful about opening your router to amplification attacks, especially if it has a public IP

The DNS configuration can be provided for DHCP, all PPP and Hotspot connected users

Adding DNS

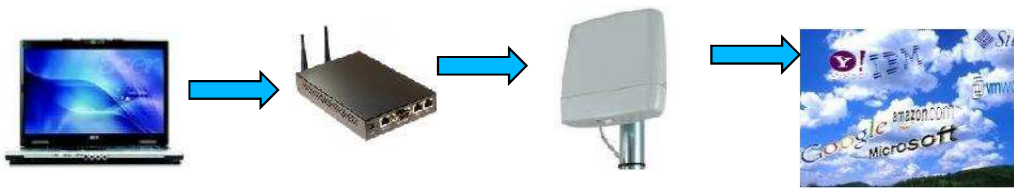


Dynamic Servers indicates server settings obtained via DHCP / PPPoE

Check "Allow Remote Requests" for caching server use (to allow the router to be used as a DNS Server)

Cache Size indicates how much memory to reserve for DNS caching

Max UDP Packet Size allows UDP datagrams over 512K



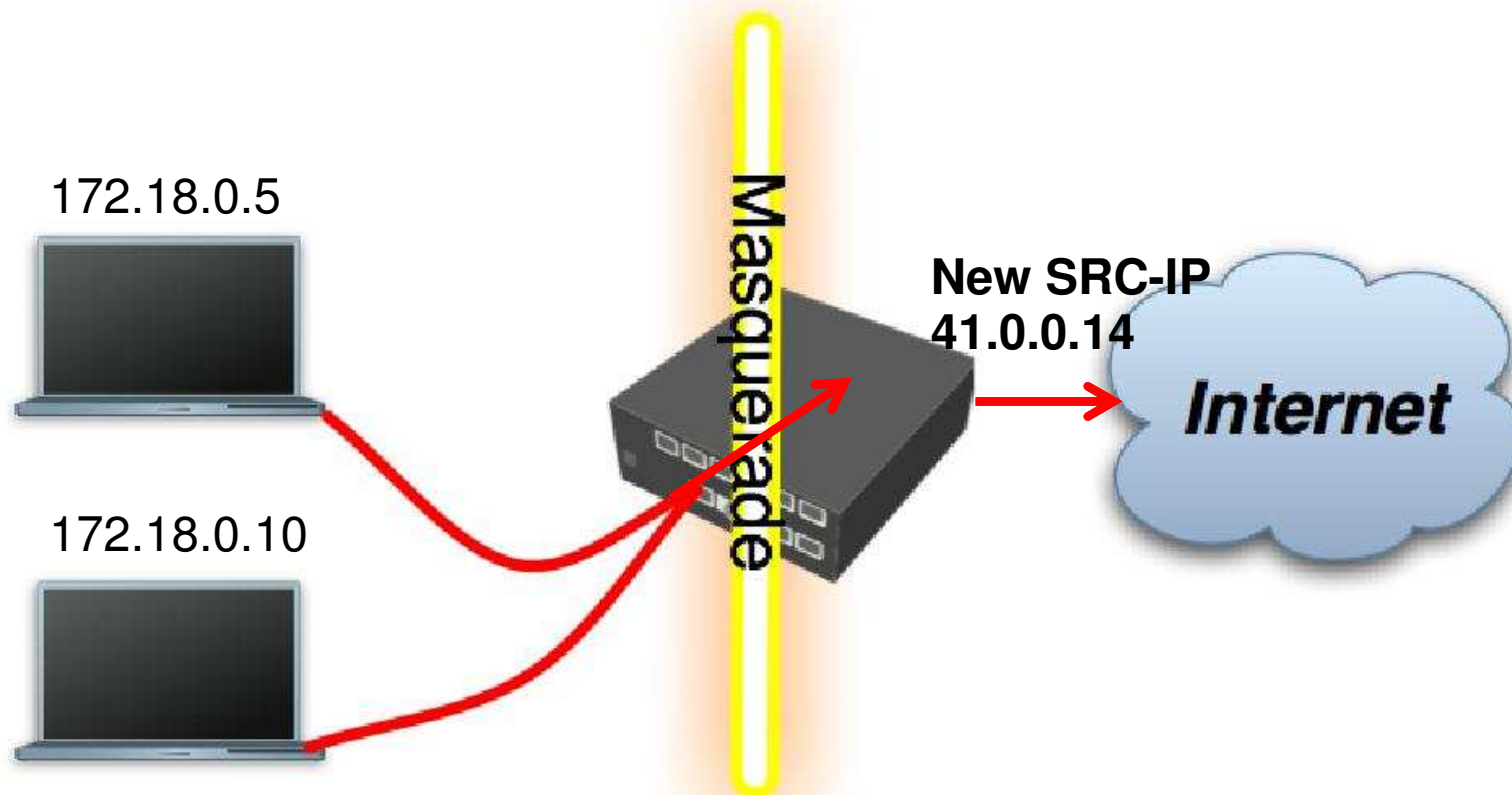
DNS

LAB

- Check IP → DNS – Do you have a dynamic entry from DHCP?
 - This is only available while the DHCP client is Active and Running
- Add a manual DNS Server now using the trainer router (you will need this later in the course)
 - This can be the same as the dynamic entry
 - The dynamic entry overrides the manual entry
- Can you ping DNS names from your router? Check from Terminal
- Make sure “Allow remote requests” checkbox is ticked in IP > DNS > Settings
- Change your laptop IP settings to use your router as a DNS server
- Can you laptop resolve DNS names (try pinging www.google.com from your laptop)
- Can you ping Google? Why not?

Masquerading

Hosts on private network ranges cannot access the Internet directly as there is no way for servers on the Internet to route packets back to a private IP address



Firewall Masquerade

Masquerading is a specific application of Network Address Translation (NAT). It is most commonly used to hide hosts of a private LAN behind router's external IP addresses

Masquerading is performed on packets that are originated from your private network

Masquerading replaces the private source address and port of IP packets with the router's external IP address when passing through the router

Masquerade is used for Public network access, where private addresses are present


Private networks include:

- 10.0.0.0-10.255.255.255 (10.0.0.0/8)
- 172.16.0.0-172.31.255.255 (172.16.0.0/12)
- 192.168.0.0-192.168.255.255 (192.168.0.0/16)



Adding Masquerading

LAB

Go to **IP** → **Firewall** in winbox
Select the **NAT** tab and click 
to add a new rule

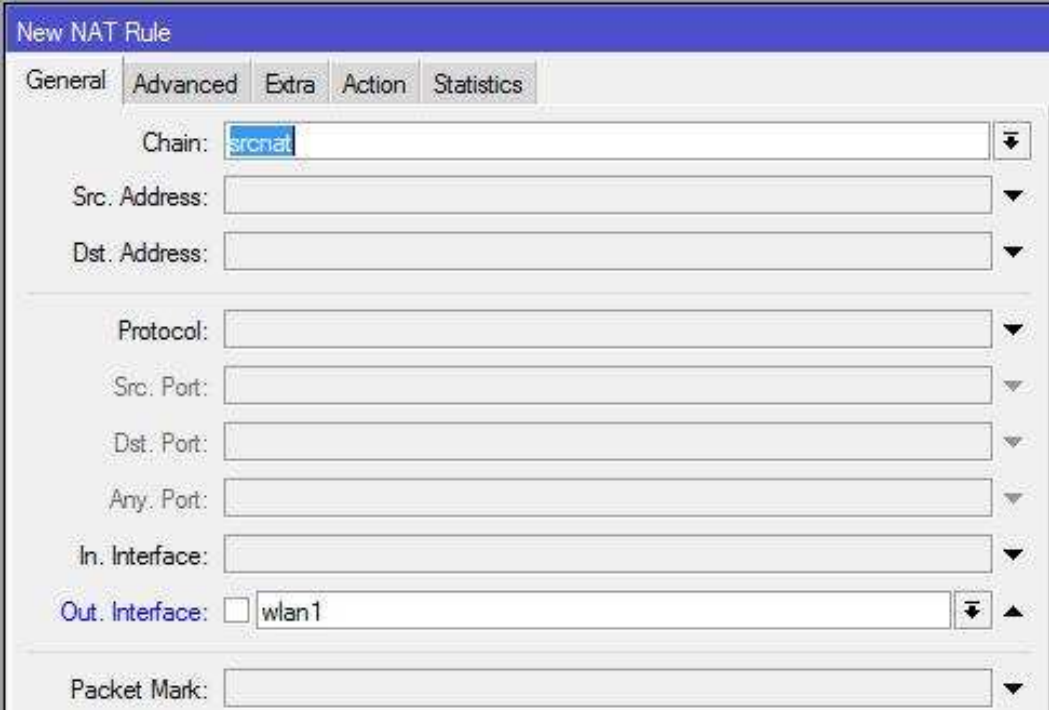
In **General**

- Select chain **srcnat**
- Select out-interface as your wlan


In **Action**

- Set action **masquerade**
- Click **OK**

Check for Internet access



The screenshot shows the 'New NAT Rule' dialog box with the 'General' tab selected. The 'Chain' dropdown is set to 'srcnat'. The 'Out. Interface' dropdown is set to 'wlan1'. Other fields like 'Src. Address', 'Dst. Address', 'Protocol', 'Src. Port', 'Dst. Port', 'Any. Port', 'In. Interface', and 'Packet Mark' are empty.



The screenshot shows the 'New NAT Rule' dialog box with the 'Action' tab selected. The 'Action' dropdown is set to 'masquerade'. The 'OK', 'Cancel', and 'Apply' buttons are visible on the right side of the dialog.

Why Don't I have Internet?

1. Can I ping/traceroute an internet IP from my router? Try 8.8.8.8
 - Check WAN IP - ping 10.1.1.254
 - Check default route - IP Routes
2. Can I ping/traceroute a DNS name from Terminal?
 - Check IP DNS
3. Can I ping/traceroute an internet IP from my laptop? Try 8.8.8.8
 - Check Laptop IP/Subnet/Default Gateway
 - Check Masquerade rule
4. Can I ping/traceroute a DNS name from my laptop?
 - Check router IP DNS - Allow Remote Requests

Still nothing? Now you can call the trainer!

System Backup and Restore

Selecting Files and clicking Backup will create a current backup identified with the routers Identity and current date and time

You can optionally specify a custom name and a password required to restore

To restore a router simply copy the backup file onto the target router, select and click Restore

The restoration procedure assumes the configuration is restored on the same router, where the backup file was originally created, so it will create partially broken configuration if the hardware has been changed.

- The backup file is non-editable
- Entire router config is saved including usernames and passwords
- The contents of /files are not included in the backup

• The Usermanager DB has its own backup utility

***TIP**

Backup Parameters

Since RouterOS v6.13 it is possible to encrypt the backup files with RC4

Command Description

- **save name=[filename]** - Save configuration backup to a file (when no name is provided, default name will be used, and previous file will be overwritten)
- **dont-encrypt** - tells the system to not use any encryption and make the file readable in text editors (DANGEROUS)
- **password** - when not specified, current user password will be required when restoring the file, when specified - this password will be required

Encryption - Since RouterOS v6.13 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.
- Notice that it is pointless to set a password if you use "dont-encrypt=yes"

System Backup

LAB

Create a configuration backup called “*your_name*-Backup-DHCP” and copy it to your laptop

DHCP Server

You may have a separate DHCP server for each Ethernet-like interface



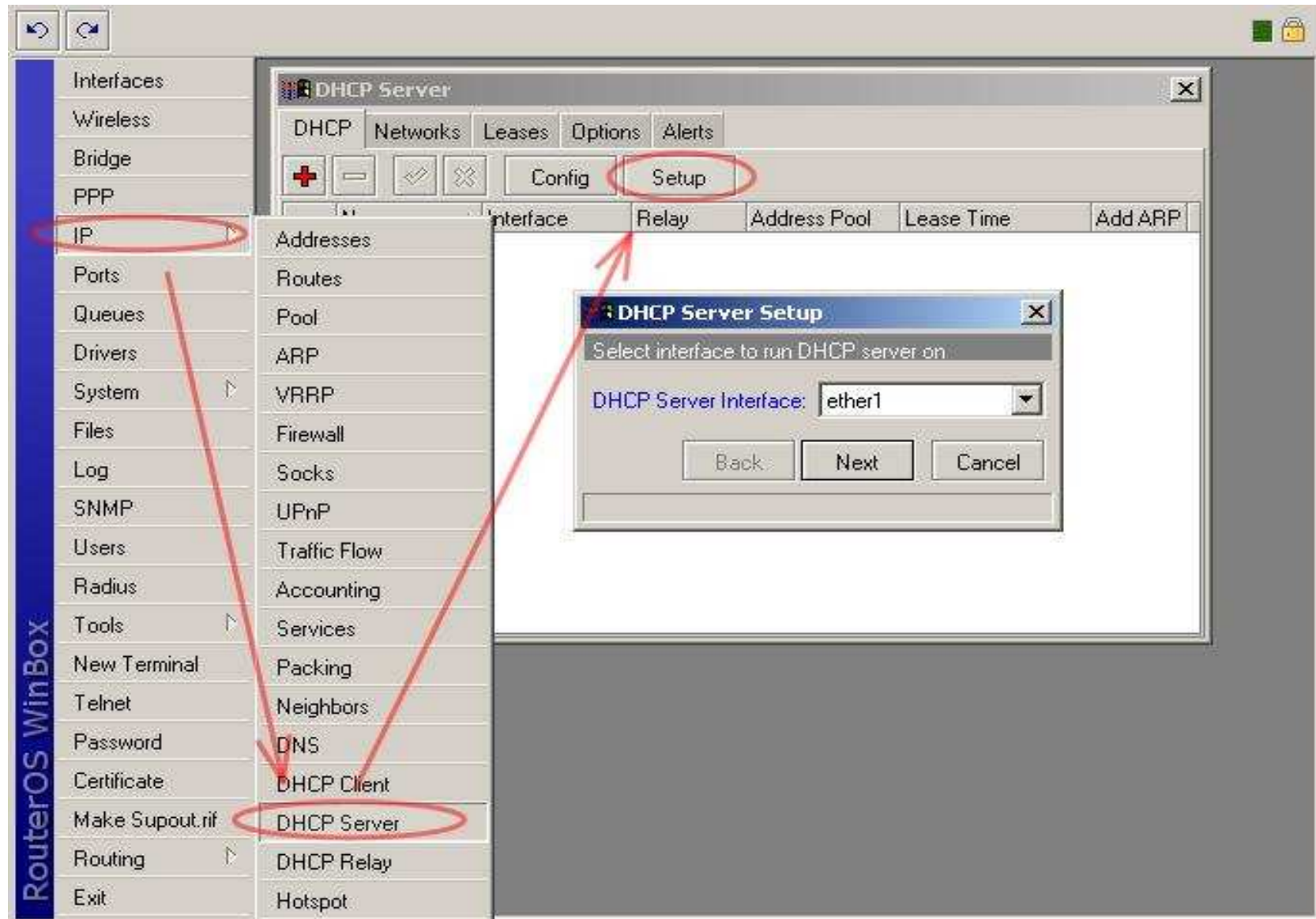
- Ether, Wlan, Vlan, VAP, Bridge
- If any interface is in a bridge then the DHCP-server **must** run on the bridge, not on any of the interfaces

There can be more than one DHCP server on the one interface, but only if using the **relay** option (advanced configurations only)

The easiest method is to use the step-by-step DHCP server configuration by using **DHCP-server setup**

To setup the DHCP Server easily you should have valid settings on your router for IP Address (on the interface you want to run setup on) as well as valid DNS Server settings

DHCP Server Setup (Step 1)



DHCP Server setup wizard

First, you must specify the interface to put the DHCP server on

Next specify the address space for the DHCP server to distribute addresses from

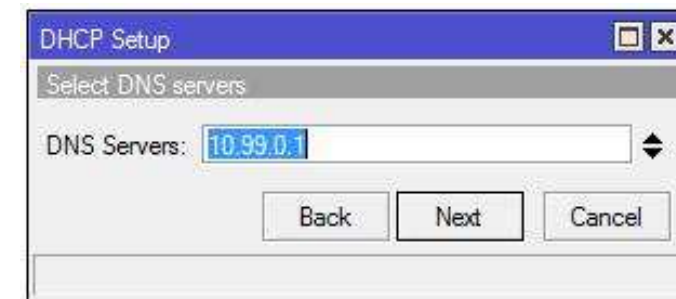
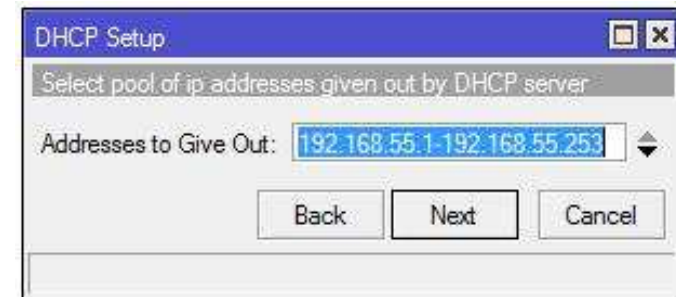
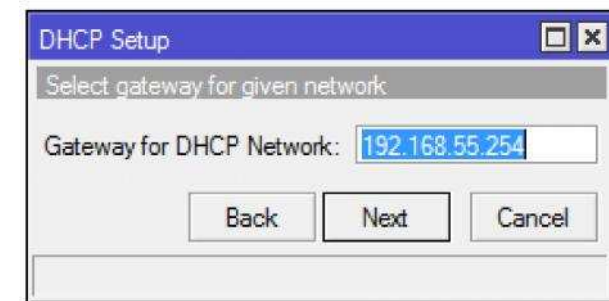
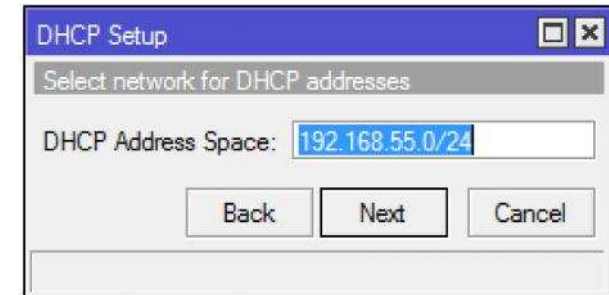
Chose a DHCP-server IP address from the previously selected address space

If there is no matching network on the selected interface then it is likely a remote network, therefore additionally you must specify the relay option

Next select an address range that will be given to clients

Next select your default DNS server

Finally you need to specify the lease time - the time that a client may reserve and use an address



DHCP Static Lease

Once a lease has been assigned it appears in DHCP →
Leases

The lease is valid for *lease_time* days

- 10 minutes default for standard setups
- 1 hour for hotspot setups

A lease can be converted to static

- This reserves that IP for the specific MAC reservation
- Useful for devices like network printers and servers

Once the lease has been made static it can be modified
further

DHCP Setup

LAB

Create a DHCP server on your Ether 1 interface

Change your laptop IP settings to obtain an IP address automatically

Check that you receive an IP address and can still browse the internet

Check **IP > DHCP-Server > leases** – is there an entry there?

Convert your lease to Static and force an IP assignment of 192.168.xy.123

- Renew your IP and check functionality

Restore from backup and reset your laptop IP

Configuration reset

Command name: `/system reset-configuration`

This command clears all configuration of the router and sets it to the default including

- login name and password ('admin' and no password),
- IP addresses and other configuration
- interfaces will be disabled
- After the reset command router will reboot.

Command modifiers

- **keep-users:** *keeps router users and passwords*
- **no-defaults:** *doesn't load any default configurations*
- **skip-backup:** *automatic backup is not created before reset, when yes is specified*
- **run-after-reset:** *specify export file name to run after reset*

Router Factory Setup

Full list at

http://wiki.mikrotik.com/wiki/Manual:Default_Configurations

For indoor consumer units:

- Generally Ether 1 is WAN port with DHCP client and discovery turned off, masquerade is set out this port
- Ether 2 – x is bridged together with an IP of 192.168.88.1 on the master port or bridge and a DHCP server setup
- If there is a wireless interface it will run as AP with SSID mikrotik-xx:xx:xx, bridged into the LAN ports

Outdoor wireless units run the wlan interface as the WAN port

All other units only have a default IP of 192.168.88.1 on Ether 1

Quickset

Used for quick router configuration for basic setups

All options can be set from one place

Info

WLAN MAC Address: 00:0C:42:84:39:BF
LAN MAC Address: 00:0C:42:84:39:BE

Wireless

Country: south africa
Channel Width: 20MHz

Address	Network Name	Channel	Protocol	Signal Strength
RB 00:02:6F:3E:20:62		5805/20/a	nstreme	-82
RB 00:0B:6B:09:9B:DE	www.comtel.co.za[kb-gard]	5200/20/a	802.11	-85
R 00:0B:6B:37:A1:F3	www.comtel.co.za[vi-centc]	5320/20/a	802.11	-86
PR 00:0B:6B:4E:92:58	VALINK	5520/20/a	nstreme	-80
PR 00:0C:42:05:C2:A9	mk	5180/20/a	802.11	-81
RB 00:0C:42:60:01:9A	oce-blockc	5320/20/a	nv2	-72
RB 00:0C:42:63:B3:50	http://ctwug.za.net/Airw...	5180/20/a	nv2	-87
RB 00:0C:42:65:32:72		5805/20/a	nstreme	-83
RB 00:0C:42:67:9C:22	CTwug-seapoint-test	5300/20/an	nv2	-41

Configuration

Mode: Router Bridge

Wireless Network

Address Acquisition: Automatic PPPoE Static

IP Address: 10.1.1.55
Netmask: 255.255.255.0 (/24)
Gateway: 10.1.1.254
DNS Servers: 10.1.1.254

Upload: unlimited bits/s
Download: unlimited bits/s

Local Network

IP Address: 192.168.55.254
Netmask: 255.255.255.0 (/24)
 DHCP Server
DHCP Server Range: 192.168.55.1-192.168.55.253
 NAT
 Bridge All LAN Ports

System

Router Identity: Huevos Grandes

Buttons: OK, Cancel, Apply, Connect, Check For Updates, Reset Configuration, Password...

Quickset

LAB

Use System → Reset Configuration to reset the router to factory defaults

- No default - true
- Keep users – false
- Skip Backup – true

Use the Quickset utility to quickly setup the router as per previous settings

- Router Mode
- Wireless – ap_mtza
- Ether – 192.168.x.254/24, WLAN – DHCP client (automatic)
- Add NAT rule
- Add a DHCP Server with manual range
- Set System Identity

Test configuration then restore from backup-DHCP

Web Administration

The router can also be configured with a web based interface (Webfig)

Accessible via the routers web page http://router_IP

Type in username and password to access

Operation is identical to Winbox

Custom skins can be created to limit access

The trainer will demonstrate using Webfig with custom skins and administrative access

Webfig

LAB

Log in to your router using a web browser on
<http://192.168.xy.254>

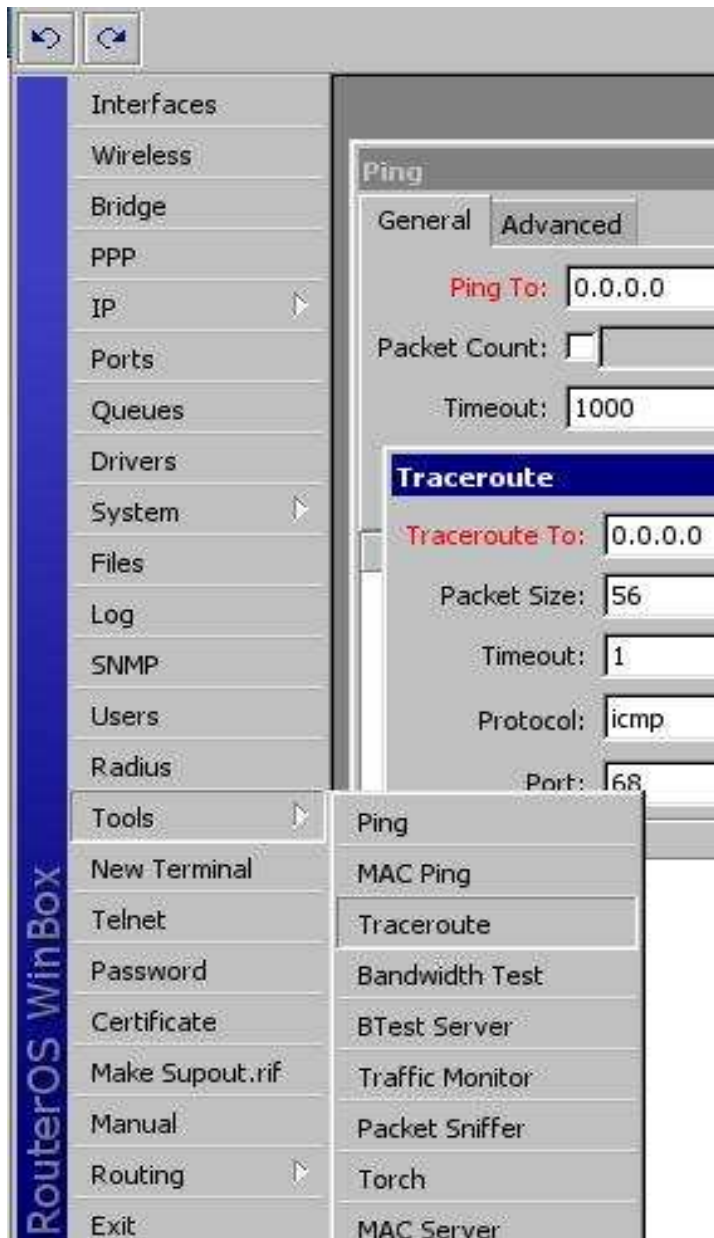
Create a custom webfig skin to limit access to only interfaces,
wireless and tools

Create a custom group for the limited skin

Create and assign a user to the custom group

Test the functionality

Network Management Tools



Use ping to check the presence of systems on the network by IP address

Traceroute can be used to track down routing problems on the network

Bandwidth test can be used to check the performance of routers and connections

IP scan can be used to check for multiple network hosts

All utilities can be found in the Tools menu

Traceroute

Use DNS – reverse lookup of IP's

Count – iterations of MTR

Max Hops – TTL

Source Address – useful to troubleshoot routing/NAT

Interface – outgoing interface

DSCP – QOS pointer

Routing table – use custom route marks

The screenshot shows the Traceroute (Running) window with the following configuration:

- Traceroute To: www.mweb.co.za
- Packet Size: 56
- Timeout: 1000 ms
- Protocol: icmp
- Port: 33434
- Use DNS
- Count: [dropdown]
- Max Hops: [dropdown]
- Src. Address: [dropdown]
- Interface: [dropdown]
- DSCP: [dropdown]
- Routing Table: [dropdown]

The table below shows the results of the traceroute:

Hop	Host	Loss	Sent	Last	Avg.	Best	Worst	Std. Dev.	History
1	41.76.131.214	0.0%	34	0.4ms	0.5	0.3	1.5	0.3	
2	41.76.133.114	0.0%	34	5.5ms	5.4	1.9	25.1	4.9	
3	oc-hh-gw.gig.za.net	0.0%	34	9.0ms	6.3	2.0	18.0	4.0	
4	hh-oc.gig.za.net	0.0%	34	12.8ms	13.7	4.5	74.1	12.5	
5	hhcore.gig.za.net	0.0%	34	9.1ms	10.3	3.9	25.7	5.3	
6	roe-hh-gw.gig.za.net	0.0%	34	12.1ms	14.0	6.1	32.4	5.1	
7	41.76.128.245	0.0%	34	18.6ms	22.1	8.0	39.7	8.3	
8	196.6.121.73	0.0%	34	11.8ms	19.5	11.0	44.0	7.6	
9	196.6.121.49	0.0%	34	24.7ms	23.7	10.6	49.3	8.4	
10	mweb-2.cinx.net.za	0.0%	34	20.6ms	23.0	10.1	57.4	7.7	
11	197-84-7-33.cpt.mweb.co.za	0.0%	34	20.7ms	29.0	16.5	72.1	11.5	
12	197-84-5-238.cpt.mweb.co.za	0.0%	34	25.8ms	22.7	10.1	35.3	6.3	
13	196.28.178.66	0.0%	34	23.8ms	23.1	12.4	43.5	7.6	
14	cte-core-sw2.vwol.net	0.0%	34	42.1ms	22.5	11.8	42.1	6.4	
15	www.mweb.co.za	0.0%	34	31.1ms	34.3	14.6	375.1	59.7	

15 items

Bandwidth Test

Specify User/Password for remote device or turn off Authenticate under Tools → Btest Server

Useful for checking link performance

Large CPU overhead for running test

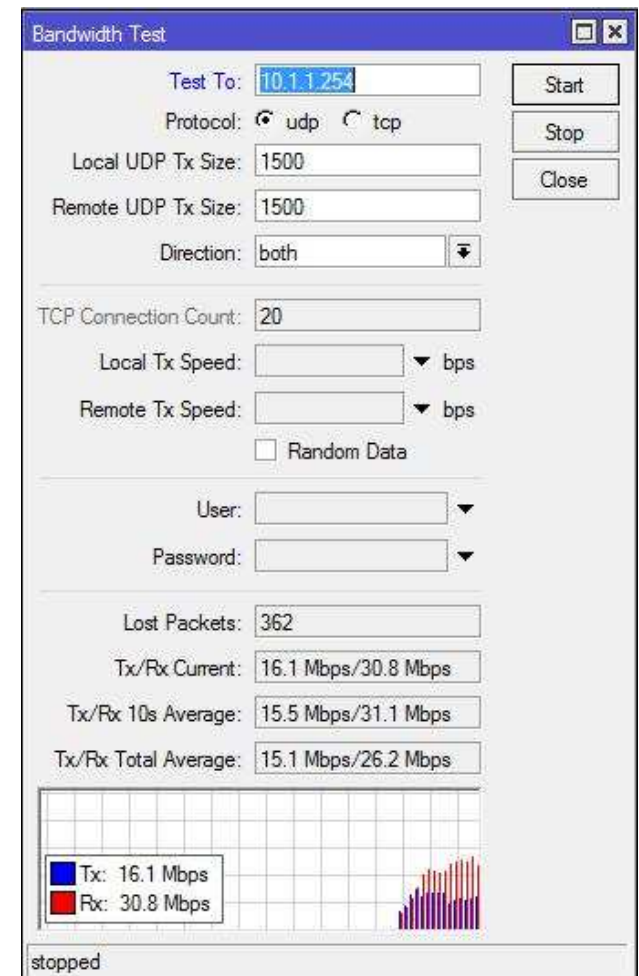
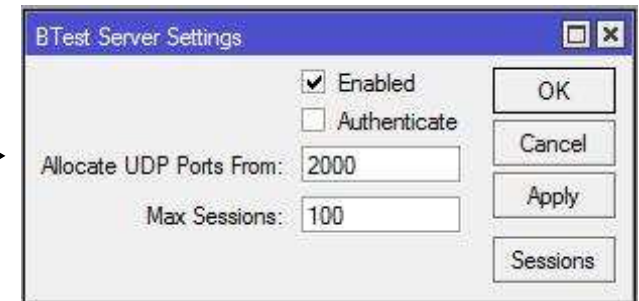
- Especially TCP

UDP tests asynchronous speeds

- Useful for checking wireless sync rate vs actual performance

TCP checks “real world” performance

- Use multiple connections to simulate normal network activity



Monitoring the Network Traffic

MikroTik RouterOS tools for monitoring the network traffic:

- Interface tx/rx bits/s and packets/s, numbers and graphs
- Torch tool for more detailed traffic report through an interface
- Sniffer for capturing data about Ethernet packets transmitted on a LAN segment connected to an interface
- Firewall logs and connection tracking tables
- Interface traffic graphs
- IP Scanner tool

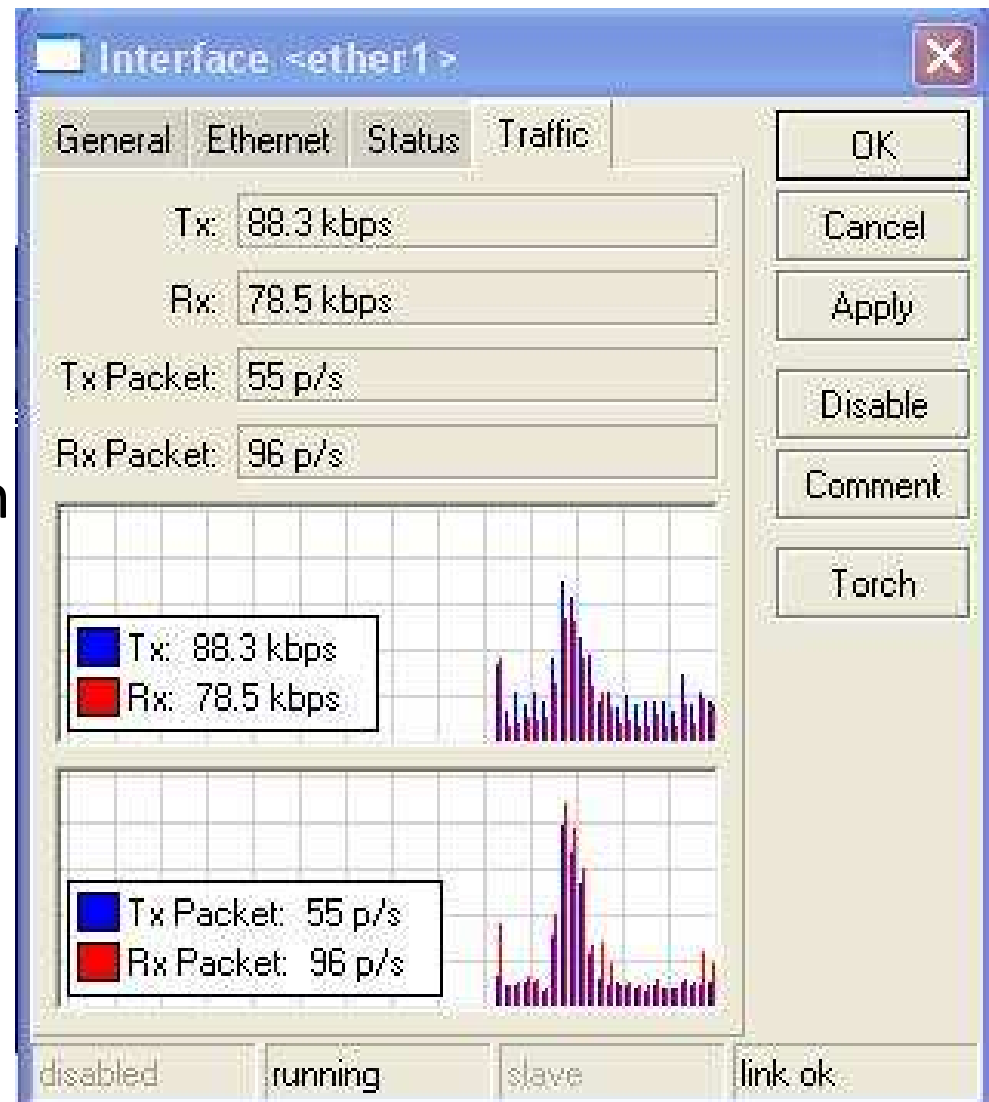
Interface Traffic Monitor

You can open Interfaces in winbox to see tx/rx rates

Open any interface and select the “Traffic” tab to see the graphs and real time speed

Use the “monitor-traffic” command in terminal to get the traffic data per one or more interfaces, for example:

- `/interface monitor-traffic ether1`
- `/interface monitor-traffic ether1,ether2,ether3`



Torch Tool

Torch tool offers a detailed actual traffic report for an interface

It's easiest to use torch in winbox:

- Go to “Tools” > “Torch”
- Select an interface to monitor and click “Start”
- Use “Stop” and “Start” to freeze/continue
- Refine the display by selecting protocol and port
- Double-click on specific IP address to fill in the Src. Or Dst. Address field (0.0.0.0/0 is for any address)

Torch

Basic

Interface: wlan1

Entry Timeout: 00:00:03 s

Collect

Src. Address Src. Address6

Dst. Address Dst. Address6

MAC Protocol Port

Protocol VLAN Id

DSCP

Filters

Src. Address: 0.0.0.0/0

Dst. Address: 0.0.0.0/0

Src. Address6: ::/0

Dst. Address6: ::/0

MAC Protocol: all

Protocol: any

Port: any

VLAN Id: any

DSCP: any

Start

Stop

Close

New Window

Et...	Protocol	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
800 (ip)	17 (udp)	10.2.34.30:161 (snmp)	10.2.72.20:49156			240 bps	240 bps	0	0
800 (ip)	47	10.2.76.5	41.76.131.213			5.3 kbps	0 bps	4	0
800 (ip)	47	10.2.90.17	41.76.131.213			5.3 kbps	0 bps	4	0
800 (ip)	47	10.2.65.10	41.76.133.33			5.3 kbps	0 bps	4	0
800 (ip)	1 (icmp)	10.2.76.5	41.76.131.213			0 bps	1354 bps	0	1
800 (ip)	47	10.2.96.162	41.76.133.33			565 bps	160 bps	0	0
800 (ip)	6 (tcp)	104.138.210.233:48588	41.76.132.31:23 (telnet)			0 bps	197 bps	0	0
800 (ip)	17 (udp)	10.2.34.28:58439	10.2.72.7:8611			0 bps	160 bps	0	0
800 (ip)	17 (udp)	41.76.134.155:63582	10.2.72.20:34313			0 bps	354 bps	0	0
800 (ip)	1 (icmp)	41.76.128.117	172.18.197.170			0 bps	240 bps	0	0
800 (ip)	17 (udp)	84.7.93.60:25353	41.76.131.213:1025			0 bps	386 bps	0	0
800 (ip)	1 (icmp)	84.7.93.60	41.76.131.213			461 bps	0 bps	0	0
800 (ip)	6 (tcp)	216.58.223.37:443 (https)	41.76.131.213:63093			144 bps	301 bps	0	0
800 (ip)	1 (icmp)	10.2.34.28	41.76.131.213			458 bps	0 bps	0	0
800 (ip)	89 (ospf)	224.0.0.5	41.76.133.113			218 bps	0 bps	0	0
800 (ip)	1 (icmp)	41.76.128.36	41.76.133.105			122 bps	160 bps	0	0
800 (ip)	1 (icmp)	41.76.128.36	41.76.133.33			122 bps	160 bps	0	0
800 (ip)	1 (icmp)	41.76.128.36	41.76.133.38			122 bps	160 bps	0	0
800 (ip)	1 (icmp)	10.2.90.1	41.76.131.213			0 bps	11.6 kbps	0	6
800 (ip)	17 (udp)	197.155.6.100:53 (dns)	41.76.133.105:41799			352 bps	704 bps	0	0
800 (ip)	6 (tcp)	89.138.75.237:2571	41.76.133.32:445 (smb)			0 bps	248 bps	0	0
24 items		Total Tx: 18.7 kbps	Total Rx: 16.4 kbps	Total Tx Packet: 12		Total Rx Packet: 7			

Graphing

You can add rules to give you basic graphing for router interfaces

Use Tools → Graphing to add support for interface graphing

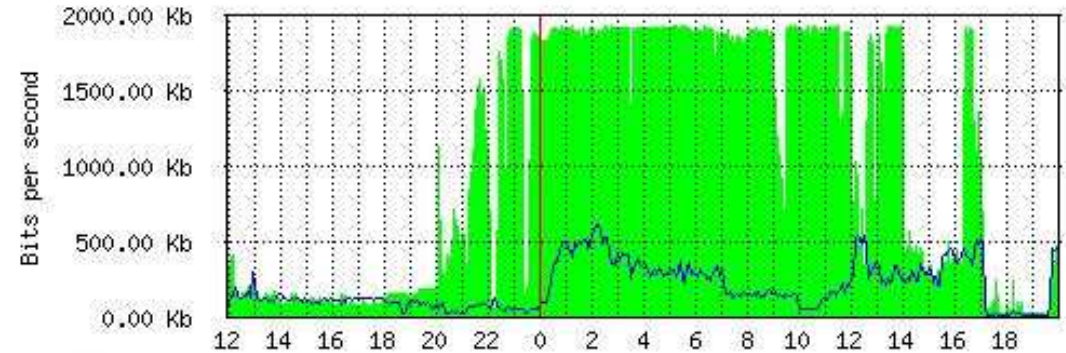
Use the web interface to view graphs

Interface Statistics

ether2

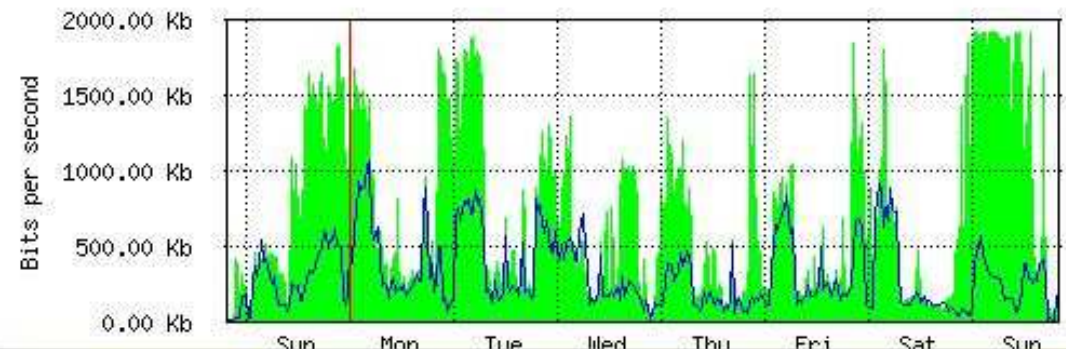
Last update: Sun Jul 12 19:53:09 2009

"Daily" Graph (5 Minute Average)



Max In: 1.93 Mb Average In: 1.03 Mb Current In: 469.79 Kb
Max Out: 610.34 Kb Average Out: 187.51 Kb Current Out: 452.14 Kb

"Weekly" Graph (30 Minute Average)



Logging

System → Logging allows you to configure logging options for the router

You can log to memory, disk, email and remote syslog

You can log all functions of RouterOS

All messages stored in the routers local memory can be printed from /log menu.

- Each entry contains the time and date when event occurred, topics that the message belongs to and the message itself.

If you have enough memory/diskspace you should increase the number of log entries stored

Logging

Rules Actions

Topics	Prefix	Action
critical		echo
critical	west 1	remote
error		memory
error	west 1	remote
info		memory
info	west 1	remote
warning		memory
warning	west 1	remote
web-proxy		memory

Log Action <disk>

Name:

Type:

File Name:

Lines Per File:

File Count:

Stop on Full

default

Increase line and file count

Add multiple rules and locations

New Log Action

Name:

Type:

Email:

default:

New Log Rule

Topics:

Prefix:

Action:

disabled

Add new rules

SNMP

Simple Network Management Protocol (SNMP) is an Internet-standard protocol for managing devices on IP networks

SNMP can be used to graph various data with tools such as CACTI, MRTG or The Dude

Enabled in IP → SNMP



The screenshot shows a dialog box titled "SNMP Settings". The "Enabled" checkbox is checked. The "Contact Info" field contains "someone@mikrotiksa.com", and the "Location" field contains "South Wing". The "Engine ID" field is empty. The "Trap Target" field is empty. The "Trap Community" field contains "public", and the "Trap Version" field contains "1". The "Trap Generators" and "Trap Interfaces" fields are empty. On the right side of the dialog, there are buttons for "OK", "Cancel", "Apply", and "Communities".

Management Tools

LAB

Enable Graphing for all interfaces, queues and resources

Add a log rule to monitor DHCP

- Enable/disable DHCP client and check results with and without logging

Try a Bandwidth Test across the wireless network to your neighbour

- Check the traffic using the Interface traffic monitor
- Use Torch to monitor the interface during bandwidth test
- Try using single and multiple connections

Use **Tool** → **Btest server** to remove authentication for Bandwidth Test – test functionality again

RoMON

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

Each router on the RoMON network is assigned a RoMON ID

The RoMON ID can be selected from port MAC address or specified by user

The RoMON protocol does not provide encryption services

- Encryption is provided at "application" level, by e.g. using ssh or by using secure winbox

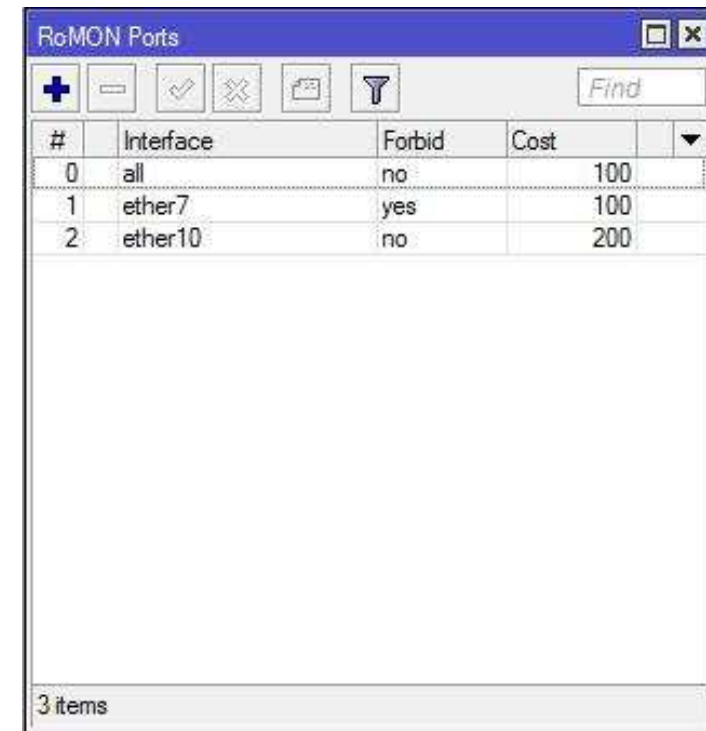
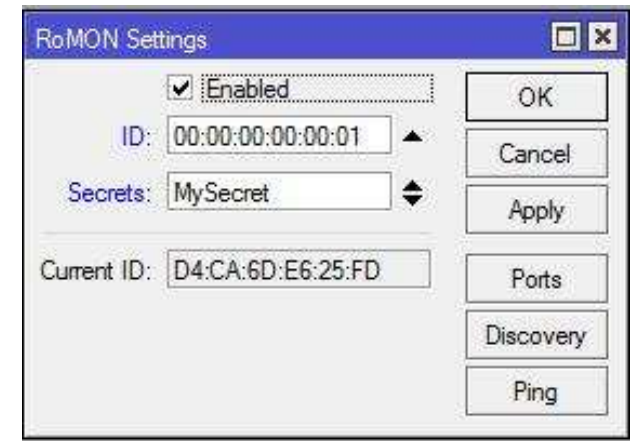
Configure RoMON

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



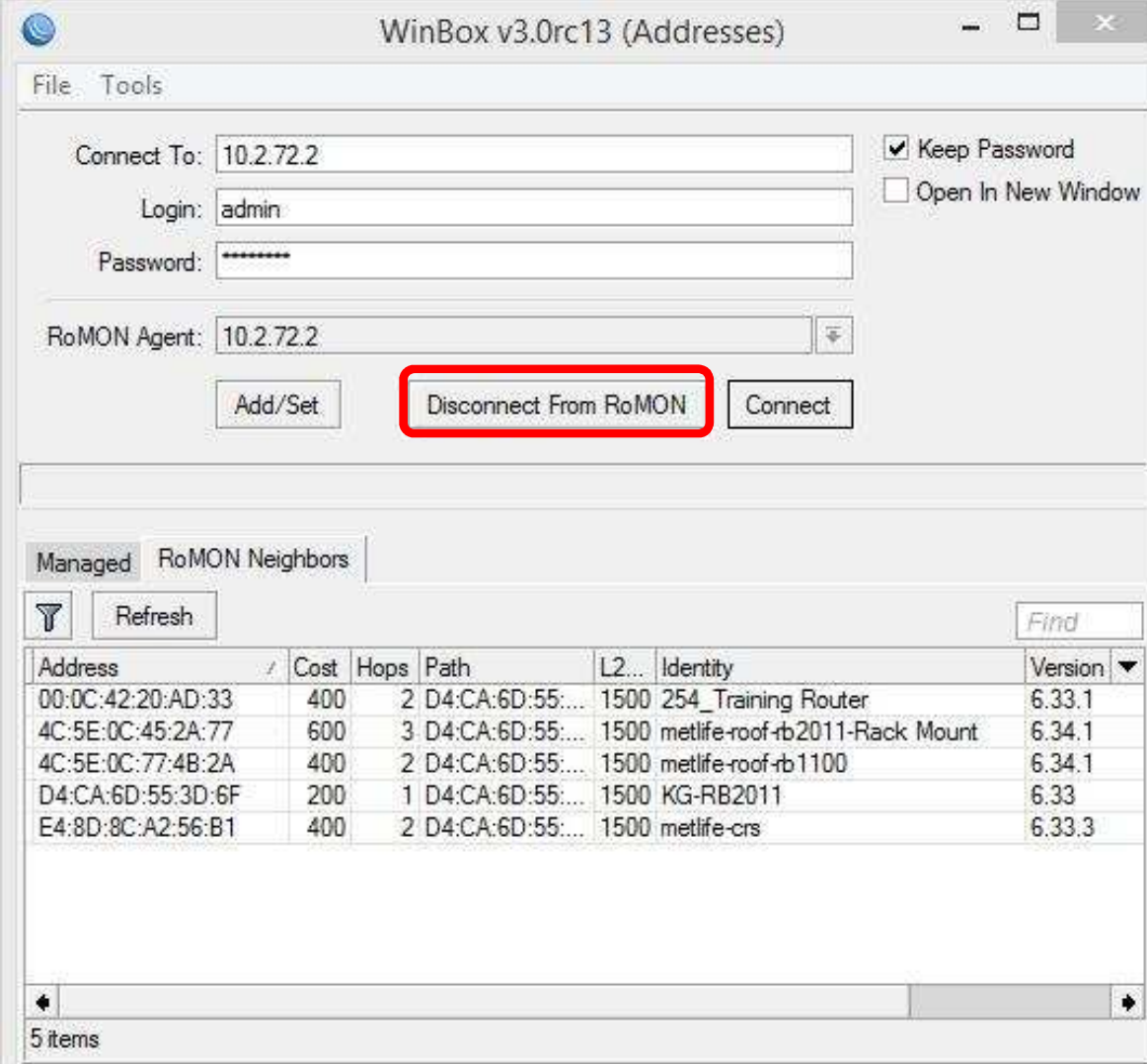
The RoMON Ports dialog box displays a table with the following data:

#	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



The screenshot shows the WinBox v3.0rc13 (Addresses) interface. The window title is "WinBox v3.0rc13 (Addresses)". The interface includes a menu bar with "File" and "Tools". Below the menu bar, there are several input fields and buttons:

- Connect To:** 10.2.72.2
- Login:** admin
- Password:** *****
- RoMON Agent:** 10.2.72.2
- Buttons:** Add/Set, Disconnect From RoMON (highlighted with a red box), Connect
- Checkboxes:** Keep Password, Open In New Window

Below the input fields, there are two tabs: "Managed" and "RoMON Neighbors". The "RoMON Neighbors" tab is selected. Below the tabs, there is a "Refresh" button and a "Find" input field. A table displays the following data:

Address	Cost	Hops	Path	L2...	Identity	Version
00:0C:42:20:AD:33	400	2	D4:CA:6D:55:...	1500	254_Training Router	6.33.1
4C:5E:0C:45:2A:77	600	3	D4:CA:6D:55:...	1500	metlife-roof-rb2011-Rack Mount	6.34.1
4C:5E:0C:77:4B:2A	400	2	D4:CA:6D:55:...	1500	metlife-roof-rb1100	6.34.1
D4:CA:6D:55:3D:6F	200	1	D4:CA:6D:55:...	1500	KG-RB2011	6.33
E4:8D:8C:A2:56:B1	400	2	D4:CA:6D:55:...	1500	metlife-crs	6.33.3

At the bottom of the window, there is a scroll bar and the text "5 items".

Romon

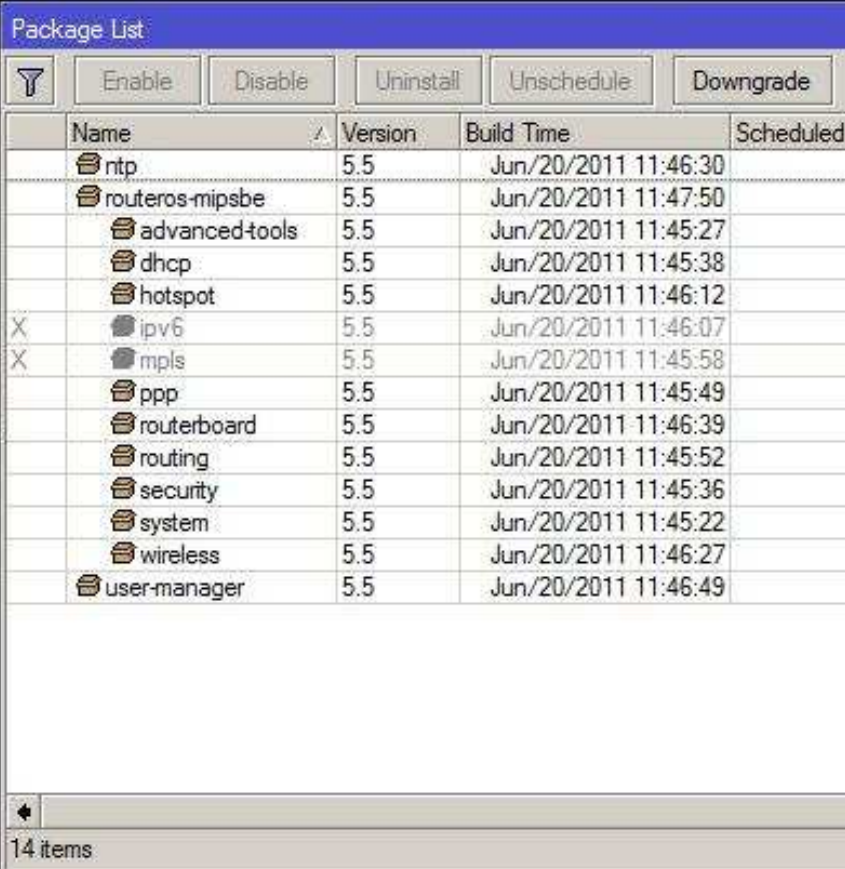


Enable the RoMON service

Configure a secret of “ClassRoMON”

Test the configuration – only works with Winbox V3

RouterOS Packages



The screenshot shows the 'Package List' window in RouterOS WinBox. At the top, there are buttons for 'Enable', 'Disable', 'Uninstall', 'Unschedule', and 'Downgrade'. Below these is a table with columns for Name, Version, Build Time, and Scheduled. The table lists 14 packages, all at version 5.5. The 'ip6' and 'mpls' packages have an 'X' in the first column, indicating they are disabled. The status bar at the bottom shows '14 items'.

Name	Version	Build Time	Scheduled
ntp	5.5	Jun/20/2011 11:46:30	
routeros-mipsbe	5.5	Jun/20/2011 11:47:50	
advanced-tools	5.5	Jun/20/2011 11:45:27	
dhcp	5.5	Jun/20/2011 11:45:38	
hotspot	5.5	Jun/20/2011 11:46:12	
X ip6	5.5	Jun/20/2011 11:46:07	
X mpls	5.5	Jun/20/2011 11:45:58	
ppp	5.5	Jun/20/2011 11:45:49	
routerboard	5.5	Jun/20/2011 11:46:39	
routing	5.5	Jun/20/2011 11:45:52	
security	5.5	Jun/20/2011 11:45:36	
system	5.5	Jun/20/2011 11:45:22	
wireless	5.5	Jun/20/2011 11:46:27	
user-manager	5.5	Jun/20/2011 11:46:49	

RouterOS software packages can be

- enabled or disabled to achieve necessary set of RouterOS functions
- installed and uninstalled to free up disk space
- upgraded to the latest version or downgraded

Go to **System** → **Packages** in winbox for package management

To effect the changes, router has to be rebooted using the **System** → **Reboot** command

RouterOS Packages

Package	Features
Package	Features
advanced-tools (<i>mipsle, mipsbe, ppc, x86</i>)	advanced ping tools. netwatch, ip-scan, sms tool, wake-on-LAN
calea (<i>mipsle, mipsbe, ppc, x86</i>)	data gathering tool for specific use due to "Communications Assistance for Law Enforcement Act" in USA
dhcp (<i>mipsle, mipsbe, ppc, x86</i>)	Dynamic Host Control Protocol client and server
hotspot (<i>mipsle, mipsbe, ppc, x86</i>)	HotSpot user management
ipv6 (<i>mipsle, mipsbe, ppc, x86</i>)	IPv6 addressing support
mpls (<i>mipsle, mipsbe, ppc, x86</i>)	Multi Protocol Labels Switching support
multicast (<i>mipsle, mipsbe, ppc, x86</i>)	Protocol Independent Multicast - Sparse Mode; Internet Group Managing Protocol - Proxy
ntp (<i>mipsle, mipsbe, ppc, x86</i>)	Network protocol client and service
ppp (<i>mipsle, mipsbe, ppc, x86</i>)	MIPPP client, PPP, PPTP, L2TP, PPPoE, ISDN PPP clients and servers
routerboard (<i>mipsle, mipsbe, ppc, x86</i>)	accessing and managing RouterBOOT. RouterBOARD specific information.

RouterOS Packages

Package	Features
routing (<i>mipsle, mipsbe, ppc, x86</i>)	dynamic routing protocols like RIP , BGP , OSPF and routing utilities like BFD , filters for routes .
security (<i>mipsle, mipsbe, ppc, x86</i>)	IPSEC, SSH, Secure WinBox
system (<i>mipsle, mipsbe, ppc, x86</i>)	basic router features like <i>static routing, ip addresses, sNTP, telnet, API, queues, firewall, web proxy, DNS cache, TFTP, IP pool, SNMP, packet sniffer, e-mail send tool, graphing, bandwidth-test, torch, EoIP, IPIP, bridging, VLAN, VRRP etc.). Also, for RouterBOARD platform - MetaROUTER Virtualization</i>
user-manager (<i>mipsle, mipsbe, ppc, x86</i>)	MikroTik User Manager
wireless (<i>mipsle, mipsbe, ppc, x86</i>)	wireless interface support
routeros-mipsle (<i>mipsle</i>)	combined package for mipsle (RB100, RB500) (includes <i>system, hotspot, wireless, ppp, security, mpls, advanced-tools, dhcp, routerboard, ipv6, routing</i>)
routeros-mipsbe (<i>mipsbe</i>)	combined package for mipsbe (RB400) (includes <i>system, hotspot, wireless, ppp, security, mpls, advanced-tools, dhcp, routerboard, ipv6, routing</i>)
routeros-powerpc (<i>ppc</i>)	combined package for powerpc (RB300, RB600, RB1000) (includes <i>system, hotspot, wireless, ppp, security, mpls, advanced-tools, dhcp, routerboard, ipv6, routing</i>)
routeros-x86 (<i>x86</i>)	combined package for x86 (Intel/AMD PC, RB230) (includes <i>system, hotspot, wireless, ppp, security, mpls, advanced-tools, dhcp, routerboard, ipv6, routing</i>)

Router hardware and platform

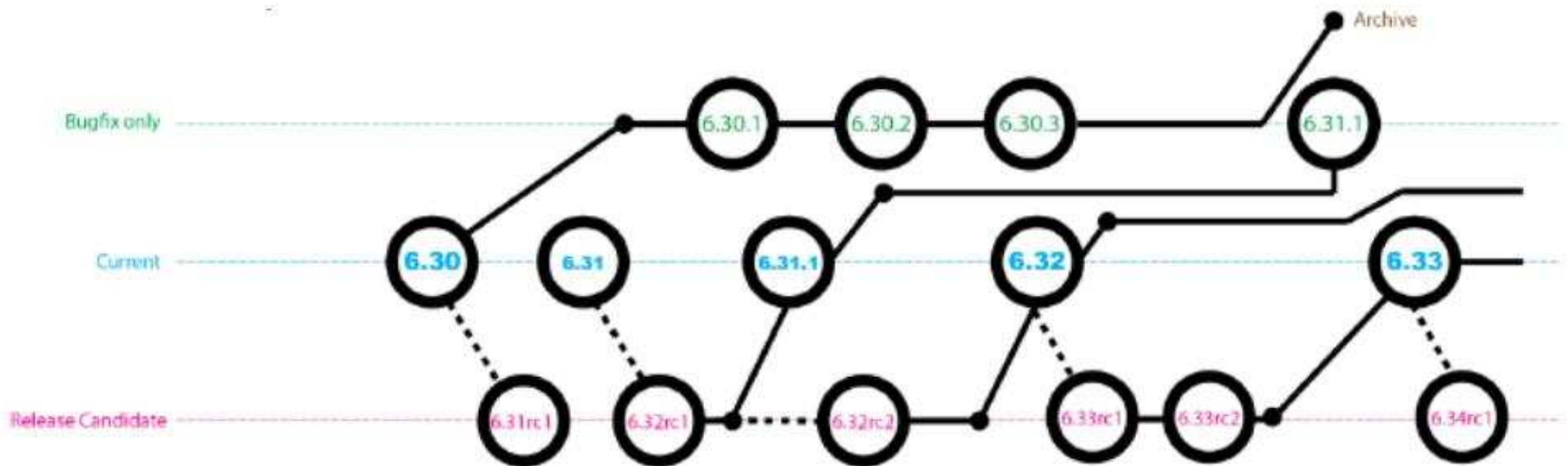
Platform	Models	Package
X86	All PC based routers RB230	routeros-x86-xx.npk
Power PC	RB333 RB600 RB800 RB1000,1100,1200	routeros-ppc-xx.npk
MipsBE	RB411,433,435,450,493 RB711, 750, 751 RB-SXT, Sextant, Groove, Metal, OmniTik RB9xx, RB2011 Series	routeros-mipsbe-xx.npk
MipsLE (Legacy)	RB111,112, RB532	routeros-mipsle-xx.npk
Tile	All Tiler based routers (Cloud Core Series) CCR-xxxx	routeros-tile-xx.npk
ARM	RB3011	routeros-arm-xx.npk
Smips	RB HexLite	routeros-smips-xx.npk

RouterOS Releases

Bugfix Only – fixes, no new releases

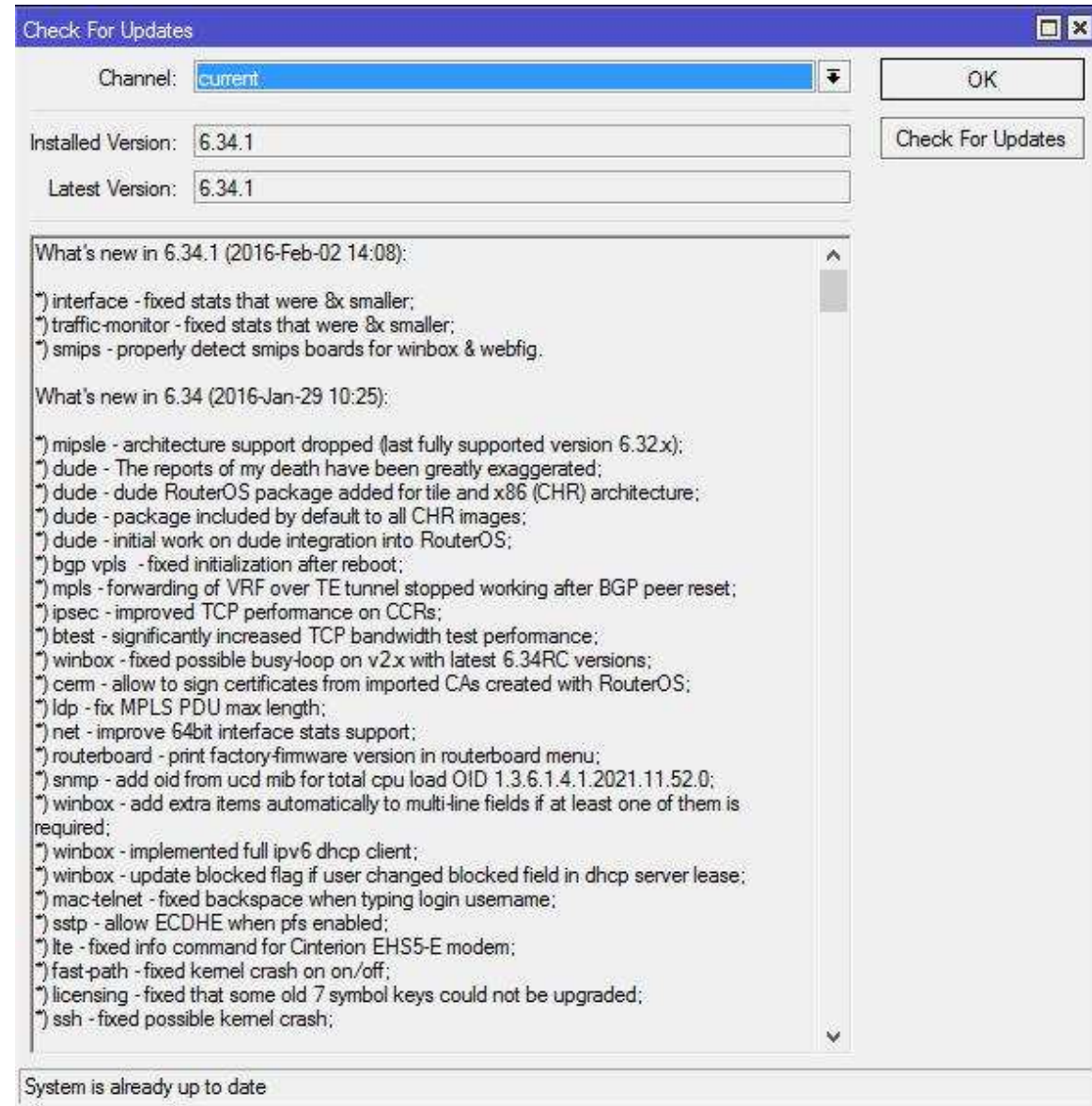
Current – fixes and new features

Release Candidate – “nightly build” beta and test features



Upgrade from System Packages

From System →
Packages click Check for Updates
Review the changelog if necessary
Choose upgrade channel if required
Select Download or Download and Upgrade



Manual Upgrading

Check if the license allows the upgrade

- **System** → **License** in winbox
- `/system license print` in command line

Upload new version of RouterOS software package(s) to the router using

- ftp binary mode to the built in FTP server
- Winbox drag-n-drop feature to the Files window

Reboot the router



Auto Upgrade

You can use System → Auto Upgrade to upgrade the router from a common router

- The common router must have the packages stored in its filesystem in the /pub directory
- Any FTP server can be used as long as files are stored in the user root directory

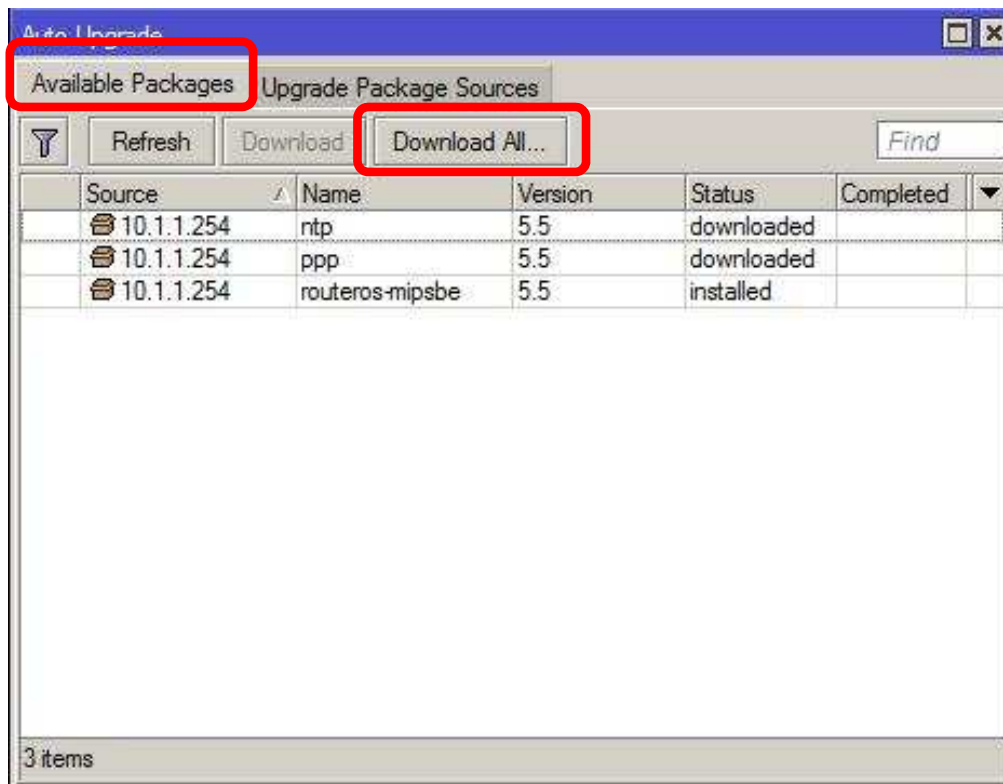
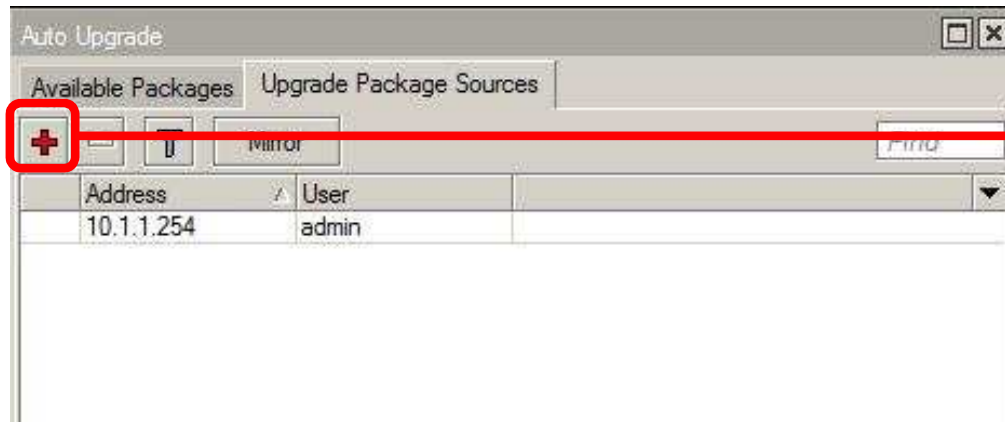
Add the common router in Upgrade Package Sources

- You need a user account with at least read and ftp access

You can then select the package/s from Available Packages and select Download

The router will then be upgraded with the selected package or ROS version

Adding a package source



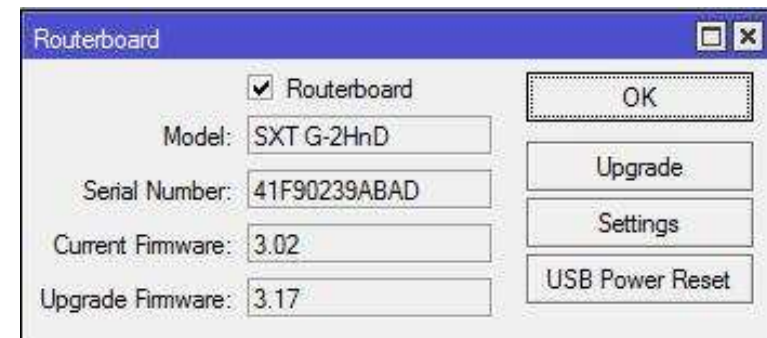
Firmware Upgrade and RouterBOOT

RouterBOOT reset button has three functions:

- Hold this button during boot time until LED light starts flashing, release the button to reset RouterOS configuration (total 5 seconds)
- Keep holding for 5 more seconds, LED turns solid, release now to turn on CAPs mode (total 10 seconds)
- Or Keep holding the button for 5 more seconds until LED turns off, then release it to make the RouterBOARD look for Netinstall servers (total 15 seconds)

RouterBOOT can be upgraded from RouterOS by:

- Upgrade to the latest version of RouterOS (newest firmware is included)
- Run command
/system routerboard upgrade
- Reboot your router to apply the upgrade



Packages and Upgrade

LAB

Note system resource usage (esp. memory)

Use System Packages to disable unnecessary packages

Reboot the router

Check system resource usage – has anything changed?

Use Auto Update to update your router to the latest version

- Server: 10.1.1.254 User/Pass: admin/admin
- Do not unplug the router during this process!
- How do you confirm a successful upgrade?

Check System → Routerboard for updated BIOS and upgrade if necessary

Downgrading the Router

Upload an older version software packages to the router

Go to **System > Packages** and click “Downgrade” to reboot the router and install the older packages

- Note, that **System > Reboot** won't install older packages, you need to go to “Packages” and click the “Downgrade” button

 **TIP**

Import and Export

You can export all the configuration from a specific menu to an editable script file:

- [admin@MikroTik] > /export file=all
- [admin@MikroTik] > /ip address *export file=address*
- files will be stored on the router

You can import script files

- [admin@MikroTik] > /import file=all
- [admin@MikroTik] > /import file=address
- Files must be on the router

Only changes to the default router config will be exported

- You can use *export verbose* for a full export

Script file is a plain text file which contains CLI commands, but no user passwords

Netinstall

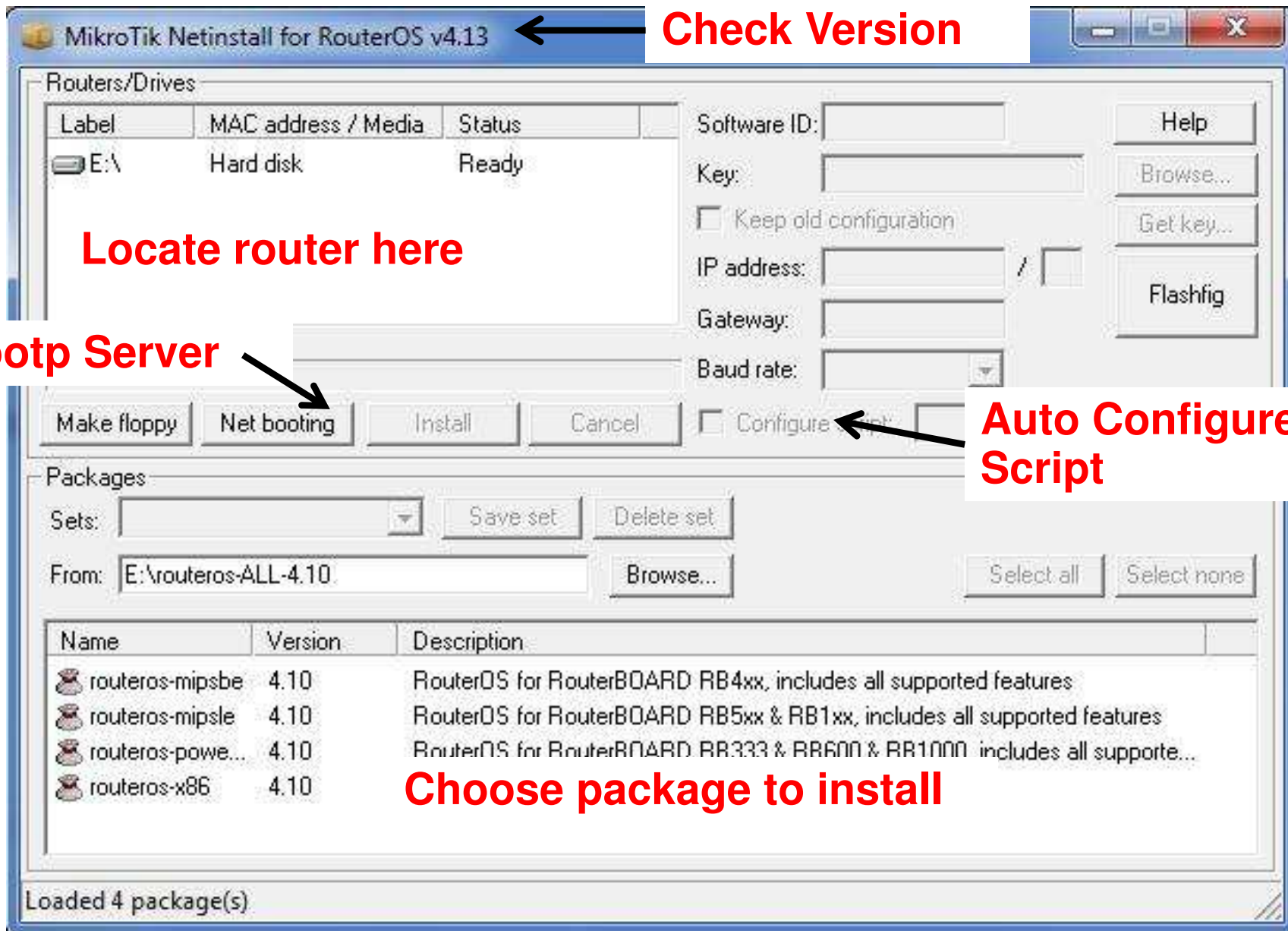
Used for installing and reinstalling RouterOS

- Can be used to re-install router to default in the case of lost password
- Used when the OS becomes corrupted for some reason
- If no OS is available the Routerboard device will automatically try to find a Netinstall server (bios must be latest version)

Runs on Windows computers

Direct network connection to router is required or over switched LAN

Available at www.mikrotik.com



Check Version

Locate router here

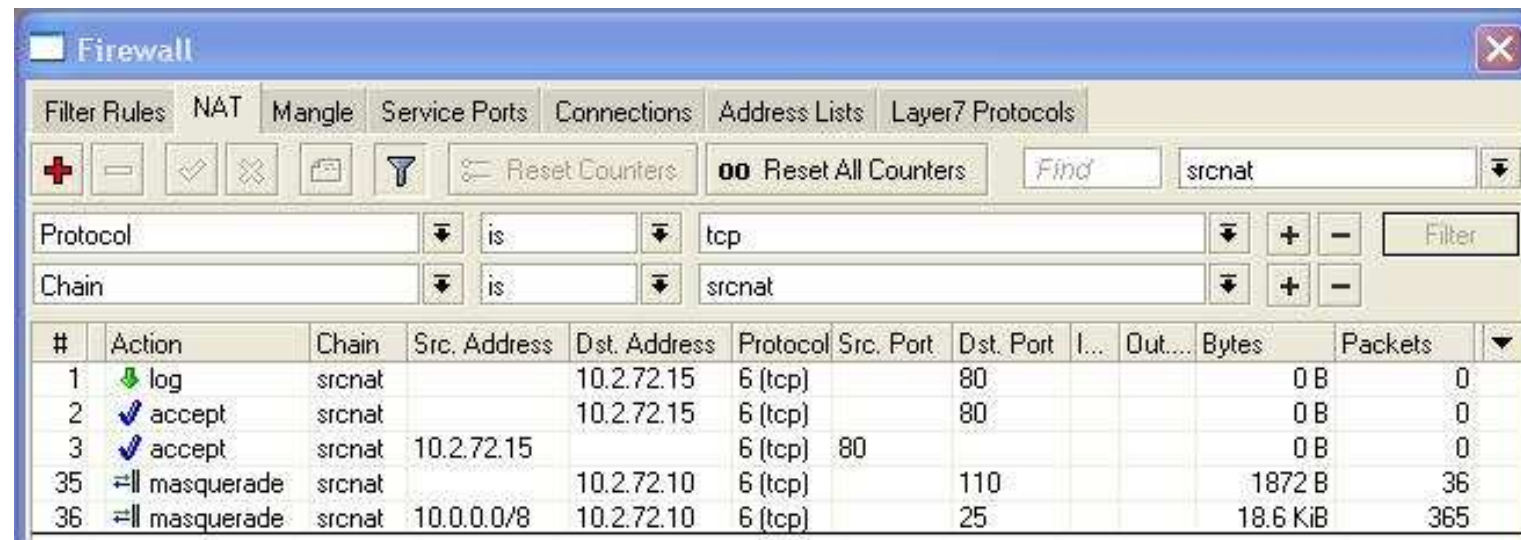
Enable Bootp Server

Auto Configure Script

Choose package to install

Filter and Find

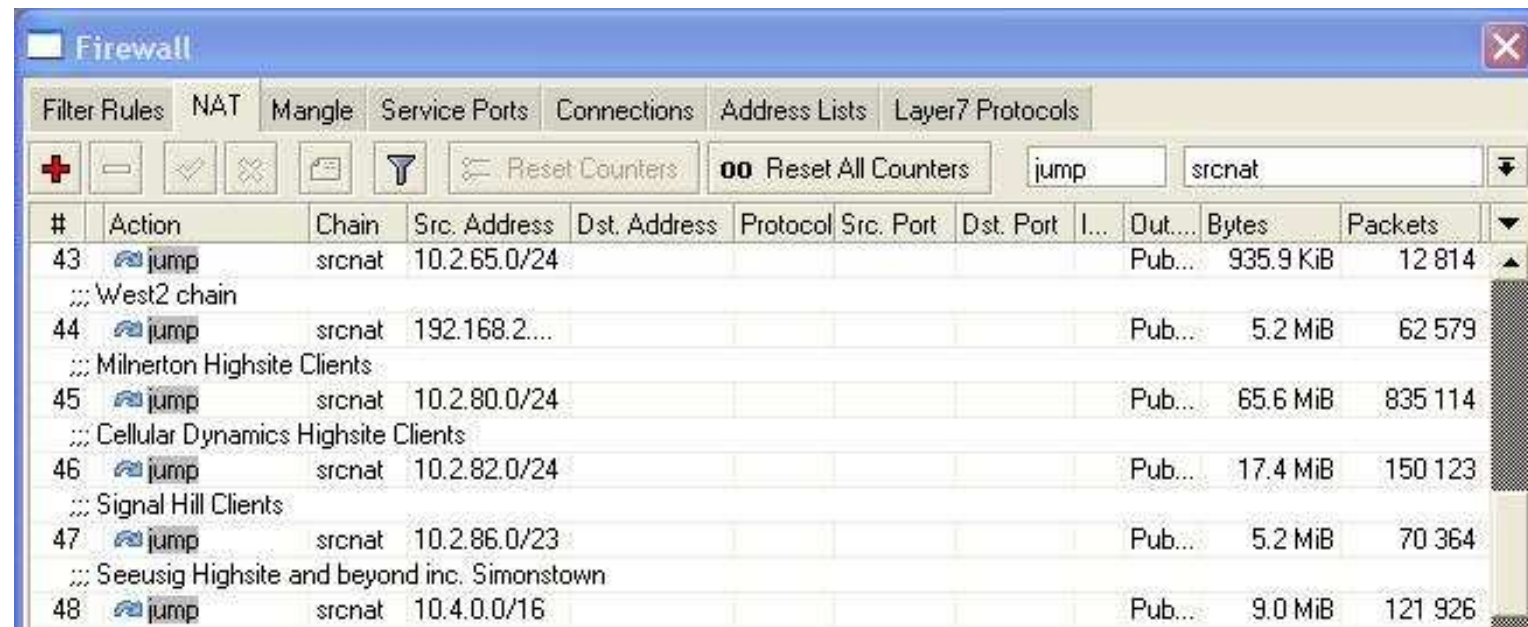
Use the filter function to display only parameters found by the filter



Firewall Filter Rules window showing the 'Find' function applied to the 'srcnat' chain. The table displays the following rules:

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	...	Out...	Bytes	Packets
1	log	srcnat		10.2.72.15	6 (tcp)		80			0 B	0
2	accept	srcnat		10.2.72.15	6 (tcp)		80			0 B	0
3	accept	srcnat	10.2.72.15		6 (tcp)	80				0 B	0
35	masquerade	srcnat		10.2.72.10	6 (tcp)		110			1872 B	36
36	masquerade	srcnat	10.0.0.0/8	10.2.72.10	6 (tcp)		25			18.6 KiB	365

Use find to highlight particular entries



Firewall Filter Rules window showing the 'Find' function applied to the 'srcnat' chain. The table displays the following rules:

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	...	Out...	Bytes	Packets
43	jump	srcnat	10.2.65.0/24						Pub...	935.9 KiB	12 814
::: West2 chain											
44	jump	srcnat	192.168.2...						Pub...	5.2 MiB	62 579
::: Milnerton Highsite Clients											
45	jump	srcnat	10.2.80.0/24						Pub...	65.6 MiB	835 114
::: Cellular Dynamics Highsite Clients											
46	jump	srcnat	10.2.82.0/24						Pub...	17.4 MiB	150 123
::: Signal Hill Clients											
47	jump	srcnat	10.2.86.0/23						Pub...	5.2 MiB	70 364
::: Seeusig Highsite and beyond inc. Simonstown											
48	jump	srcnat	10.4.0.0/16						Pub...	9.0 MiB	121 926

Using SAFE mode



Safe mode prevents you from accidentally locking yourself out of your router

Any changes made during Safe mode will not be committed to the router until you exit Safe mode properly

- Safe mode changes the running config in memory but does not commit the changes to disk until safe mode is properly exited

To enter and exit Safe mode use Ctrl-X key combination in a Terminal window or click the Safe Mode button at the top of Winbox

- Note the 2 safe modes are independent of each other (depends on ROS version – please test functionality first)

Using SAFE mode

Winbox Safe Mode

The screenshot shows the WinBox v5.2 interface on a MikroTik RB SXT-5D. The title bar reads "david@41.223.35.59 (west1) - WinBox v5.2 on RB SXT-5D (mipsbe)". A "Safe Mode" button is visible in the top toolbar. The left sidebar contains a menu with categories: Interfaces, Wireless, Bridge, PPP, Switch, Mesh, IP, MPLS, Routing, System, Queues, Files, and Log. The main terminal window displays the RouterOS boot sequence and configuration menu. The terminal output includes a ASCII art logo, the version "MikroTik RouterOS 5.2 (c) 1999-2011", and the URL "http://www.mikrotik.com/". The prompt is "[david@west1] >". Below the prompt, the text "[Safe Mode taken]" is displayed. The prompt has changed to "[david@west1] <SAFE>". A red dashed box highlights the text "CTRL + X" next to the prompt.

```
david@41.223.35.59 (west1) - WinBox v5.2 on RB SXT-5D (mipsbe)
Safe Mode

Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log

Terminal

MMM      MMM      KKK      TTTTTTTTTT      KKK
MMMM     MMMM     KKK      TTTTTTTTTT      KKK
MMM MMMM MMM III  KKK  KKK  RRRRRR      OOOOOO      TTT      III  KKK  KKK
MMM MM  MMM III  KKKKK  RRR  RRR  OOO  OOO      TTT      III  KKKKK
MMM      MMM III  KKK  KKK  RRRRRR      OOO  OOO      TTT      III  KKK  KKK
MMM      MMM III  KKK  KKK  RRR  RRR      OOOOOO      TTT      III  KKK  KKK

MikroTik RouterOS 5.2 (c) 1999-2011      http://www.mikrotik.com/

[david@west1] >
[Safe Mode taken]
[david@west1] <SAFE>
```

CTRL + X

Network Time Protocol

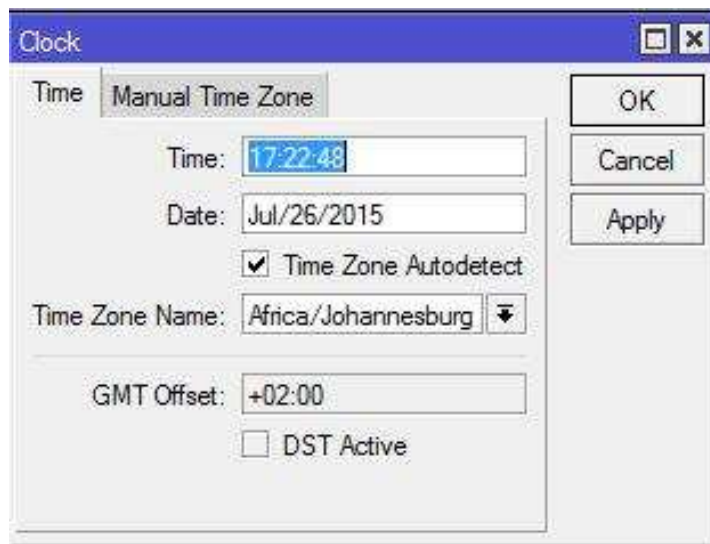
NTP is used to maintain the correct time for routers that do not have a battery backup

To get correct logging or graphing data you must set the correct time on the router

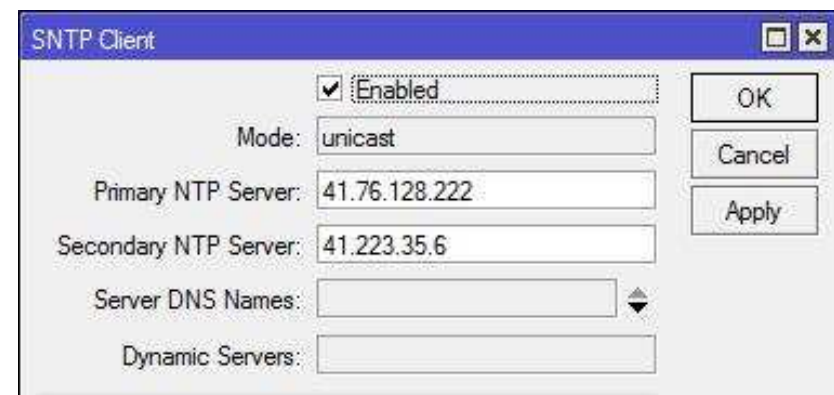
RouterOS has both an (S)NTP Client and Server

- The NTP Server requires the NTP package be installed

To use NTP set the time zone in **System > Clock**, enable the NTP client in System → NTP Client and specify a time server



The screenshot shows the 'Clock' configuration window in RouterOS. It has two tabs: 'Time' and 'Manual Time Zone'. The 'Manual Time Zone' tab is active. The 'Time' field is set to '17:22:48', the 'Date' is 'Jul/26/2015', and 'Time Zone Autodetect' is checked. The 'Time Zone Name' is set to 'Africa/Johannesburg' with a dropdown arrow. The 'GMT Offset' is '+02:00' and 'DST Active' is unchecked. There are 'OK', 'Cancel', and 'Apply' buttons on the right side.



The screenshot shows the 'SNTP Client' configuration window in RouterOS. The 'Enabled' checkbox is checked. The 'Mode' is set to 'unicast'. The 'Primary NTP Server' is '41.76.128.222' and the 'Secondary NTP Server' is '41.223.35.6'. The 'Server DNS Names' and 'Dynamic Servers' fields are empty. There are 'OK', 'Cancel', and 'Apply' buttons on the right side.

NTP Client

LAB

Set your Time Zone correctly in the System Clock

Enable (S)NTP Client – you can use the trainer router 10.1.1.254 as the NTP Server or 41.76.128.222

You can also use the SAIX igubu server – 196.25.1.1

* Advanced *

Install NTP package and setup an NTP Server

On your neighbour set to sync time with your NTP Server
– reboot the client and check that it sets time correctly

- You will need to uncheck the Use Peer NTP option in DHCP client

More Configuration?

System → Scheduler allows you to run scripts at specified times

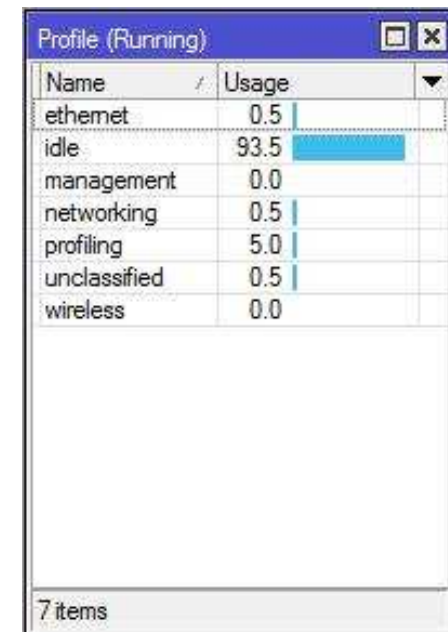
System → Watchdog can reboot the router if the kernel fails or if an IP address is no longer pingable

- Automatic Supout creates a **Support Output** file that can be sent to MikroTik for evaluation

Tools → Email defines mail server parameters for systems that use it (e.g. logging, scripts)

Tools → Netwatch can execute arbitrary commands whenever an IP Address goes up or down

Tools → Profile shows CPU usage for various subsystems in RouterOS



The screenshot shows a window titled "Profile (Running)" with a table of CPU usage for various subsystems. The table has two columns: "Name" and "Usage". The "idle" row is highlighted in blue.

Name	Usage
ethernet	0.5
idle	93.5
management	0.0
networking	0.5
profiling	5.0
unclassified	0.5
wireless	0.0

7 items

Support Channels

Use “Make supout.rif” (Routing Information File) to capture live information on problem routers – this is required for any MikroTik support requests

- Supout can also be created automatically by System Watchdog

Email support@mikrotik.com along with the supout.rif file and a clear description of the issue

Supout.rif uploader and viewer is also available in your account on mikrotik.com

Full manual and many examples and scenarios are available on wiki.mikrotik.com

Open forum discussions are available on forum.mikrotik.com

Network Communication

OSI Model

Layer2 vs Layer3 networking

IPv4 Subnetting

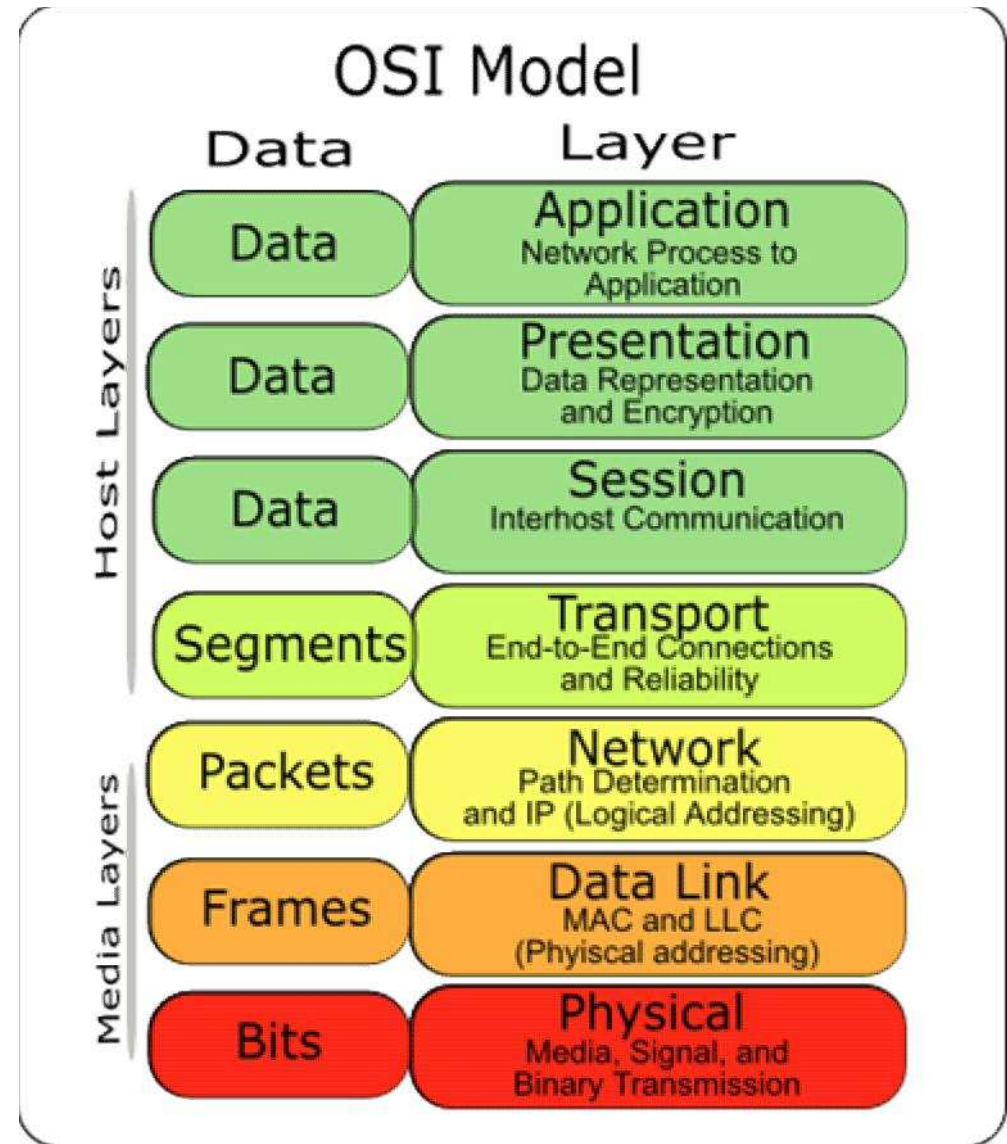
Address Resolution Protocol

OSI layer Communication

Process of communication is divided into seven layers

Lowest is physical layer, highest is application layer

For our purposes we can consider everything above layer 3 to be Application level communication



Application

Presentation

Session

Transport

These layers are more concerned with client level communication. Software generates data to be communicated and passes it onto the lower levels for transport to another host

Network

Sometimes also called the TCP/IP Layer, this is where routing decisions are made for sending data between networks

Data Link

This is where network cards communicate using MAC addresses.

Physical

This is the physical transmission layer

Physical Layer

The physical layer is the physical connections including the cables, Network Cards, wireless interfaces and other devices that make up the network

This is the layer that you can see and feel

It uses various ways of signalling depending on the medium it is transmitting through

Usual associations are electromagnetic waves (wireless), electrical pulses (wired, Ethernet), light waves (Fibre)

DataLink Layer

This layer is where the network packets are translated into raw bits (00110101) to be transmitted on the physical layer.

This layer uses the most basic addressing scheme, MAC Addresses.

The main purpose of a MAC address is to provide a unique (hardware) identifier for each host.

This does not provide any means for routing or organizing the hosts that participate on a network.

All switches and routers will have a separate MAC address per Ethernet like port

Hubs do not have MAC addresses

Data Link Layer (MAC Addresses)

MAC Addresses (Media Access Control) are unique addresses given to network hosts.

- First part of the MAC address is assigned to the manufacturer of the hardware;
- The rest of the address is determined by the manufacturer;
- Devices, that are not manageable (e.g., HUBs and some switches) do not have MAC addresses.

Manufacturer:Unique ID

Example: **00:0C:42:04:9F:AE**

It can be any combination of numbers 0-9 and letters A-F

MAC addresses are used for addressing in the Data Link Layer (Layer 2) of the OSI network model.

MAC addresses are not used to group hosts on the network together.

Analogy: MAC address is like a your ID number.

Network Layer

The network layer is responsible for logical (TCP/IP) addressing.

It allows for grouping computers together unlike the MAC address where there may be no similarity from one MAC address to another.

The network layer provides the functional and procedural means of transferring variable length data sequences (called datagrams) from one node to another connected to the same network

Datagram delivery at the network layer is not guaranteed to be reliable.

IPv4 Addresses

IP addresses are used for logical addressing in the Network Layer (Layer 3) of the OSI network model.

IP addresses

- are unique, 32-bit addresses
- are referenced by humans via dotted decimal notation, one number per 8 bits (1 octet or byte), e.g., 159.148.147.1
- consist of three primary classes A, B, and C (class D is for multicast) of the form [netid:hostid]

Analogy: Think of a MAC address like a person's ID (Social Security) number, it is just a number that is unique from anyone else's. Now think of an IP address like a person's mailing address. The mailing address group people into zones by using the postcode, city, province, and street identifiers.

Classful Addressing

IP Subnets were originally divided into class A,B and C Subnets

Class	Network Octets	Host Octets	Range 1 st Octet	Subnet Mask	Private Range
A	1	3	0-126	255.0.0.0	10.0.0.0- 10.255.255.255
B	2	2	128-191	255.255.0.0	172.16.0.0-172.31.255.255
C	3	1	192-223	255.255.255.0	192.168.0.0- 192.168.255.255

IP Addressing

Each octet has a range from 0-255 which translates to binary of 00000000-11111111 (8 bits)

So an address link 192.168.0.23 with a subnet mask of 255.255.255.0 can be represented as

**11000000.10101000.00000000.00010111
11111111.11111111.11111111.00000000**

Another way of representing the subnet mask is to specify the number of bits in the mask portion dedicated to the subnet

So we can represent the address above with 192.168.0.23/24 (“slash 24”)

Private IP ranges

0.0.0.0/8 and 127.0.0.0/8 (localhost) are reserved addresses and cannot be used in networking

There are other addresses not used on the public Internet

These *private subnets* consist of private IP addresses and are usually behind a firewall or router that performs NAT (network address translation).

- Private IPs are never publicly routed because no one owns them.

Private IP addresses are used in most LAN and WAN environments where a public address space is not available or is not large enough

Private Ranges

The following blocks of IP addresses are allocated for private networks:

10.0.0.0/8 (10.0.0.0 to 10.255.255.255)

172.16.0.0/12 (172.16.0.0 to 172.31.255.255)

192.168.0.0/16 (192.168.0.0 to 192.168.255.255)

169.254.0.0/16 (169.254.0.0 to 169.254.255.255)*

*Note that 169.254.0.0/16 is a block of private IP addresses used for random self IP assignment where DHCP servers are not available

Subnets

There are many situations where class A,B and C networks do not provide fine grained enough apportioning of network numbers.

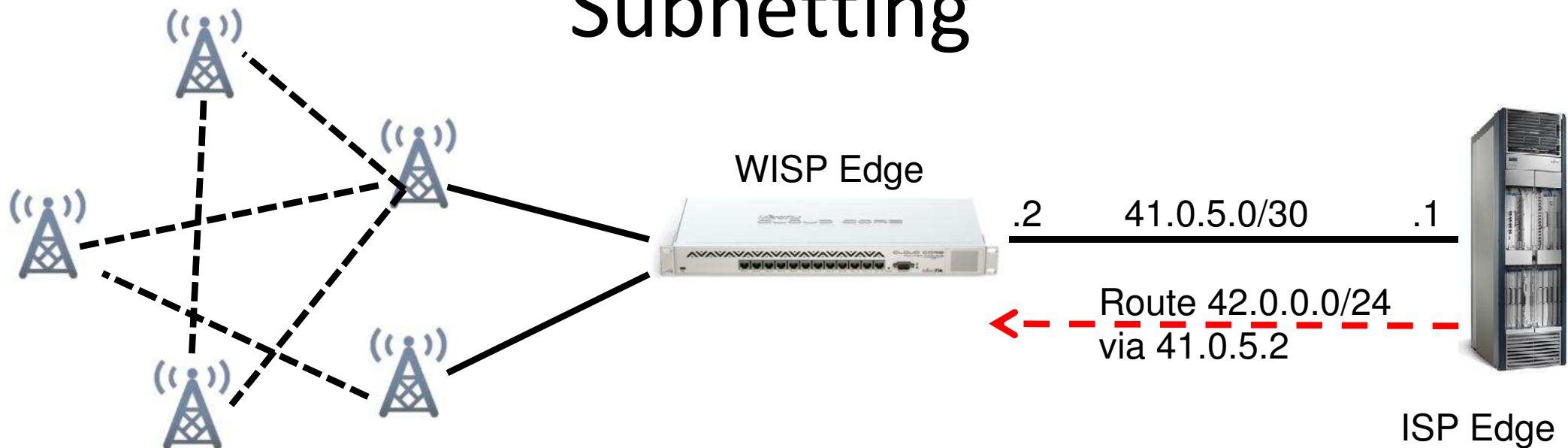
Given IP class networks can be subdivided into smaller subnetworks

Size of the subnetwork is determined by the network mask (subnet mask, netmask)

There are three types of network mask notations:
Binary, Decimal and number of bits in netid

CIDR notation ignores the traditional classes of network and instead focuses on the number of bits in the net-id to determine the number of hosts and available networks

Subnetting



Class C Network: 42.0.0.0/24

- 1 network with 256 hosts (254 useable)
- IP's can range from 1-254

/27 networks:

42.0.0.0/27	42.0.0.32/27	42.0.0.64/27	42.0.0.96/27
42.0.0.128/27	42.0.0.160/27	42.0.0.192/27	42.0.0.224/27

- The class C network is split into 8 networks
- Each network has 32 IP's - 30 useable

Subnetting Reference Chart

Subnet Mask (Netmask)	Binary	CIDR	Hosts	Nets	Notes
255.255.255.255	11111111.11111111.11111111.11111111	/32	1	255	single host mask
255.255.255.254	11111111.11111111.11111111.11111110	/31	0		unusable mask, no host bits
255.255.255.252	11111111.11111111.11111111.11111100	/30	2	64	Point to Point
255.255.255.248	11111111.11111111.11111111.11111000	/29	6	32	
255.255.255.240	11111111.11111111.11111111.11110000	/28	14	16	
255.255.255.224	11111111.11111111.11111111.11100000	/27	30	8	
255.255.255.192	11111111.11111111.11111111.11000000	/26	62	4	
255.255.255.128	11111111.11111111.11111111.10000000	/25	126	2	
255.255.255.0	11111111.11111111.11111111.00000000	/24	254	1	1 Class C network
255.255.254.0	11111111.11111111.11111110.00000000	/23	510		2 Class C networks
255.255.252.0	11111111.11111111.11111100.00000000	/22	1022		4 Class C
255.255.248.0	11111111.11111111.11111000.00000000	/21	2046		8 Class C
255.255.240.0	11111111.11111111.11110000.00000000	/20	4094		16 Class C
255.255.224.0	11111111.11111111.11100000.00000000	/19	8190		32 Class C
255.255.192.0	11111111.11111111.11000000.00000000	/18	16382		64 Class C
255.255.128.0	11111111.11111111.10000000.00000000	/17	32766		128 Class C
255.255.0.0	11111111.11111111.00000000.00000000	/16	65534		1 Class B Network (255 Class C)

Network Address

The first address in an IP range is called the Network Address

It is used to label the network

Routers route to network ranges not specific IP addresses

Network addresses are used to tell routers where to send packets

Example:

```
/route add 192.168.10.0/24 gateway=10.1.1.254
```

```
/route add 196.32.0.32/27 gateway 196.25.66.7
```

Broadcast Address

The last IP in the range is called the Broadcast address
The broadcast address is used to talk to all hosts on the network.

The broadcast is an address with the host portion set to all 1's, for example:

- 128.192.10.255 for network 128.192.10.0/24
- 128.192.10.191 for network 128.192.10.128/26

Broadcast Domain

A broadcast domain is part of the network that can hear broadcast traffic from hosts of this network

Broadcasts are needed for:

- establishing initial communications with another host, i.e., address resolution
- for dhcp and the like assignments of ip addresses

Remote networks can be bridged over a tunnel to create single broadcast domain

Many services operate in a broadcast domain



- HotSpot, DHCP Server, PPPoE Server

Computers on the same broadcast domain can communicate directly without needing a router

ARP

Address Resolution Protocol (ARP) is used to associate MAC addresses with IP addresses.

ARP process works as follows:

- ARP requestor sends a broadcast frame with the destination IP address, its source IP address and MAC address, asking for the destination MAC address.
- Host with destination IP address sends a directed frame back to ARP requestor filling in its MAC address and storing the MAC address of the sender in an ARP table (or cache).

You can see the ARP cache by looking in **IP** → **Arp**

Static entries can be added if ARP is disabled

ARP is only used in IPv4, IPv6 uses Neighbour Discovery and SLAAC for initial communication

ARP Table

The ARP table shows the IP Address, MAC Address, interface and state (Dynamic or static)

You can create entries manually or from an existing entry

Clients will need the exact IP/ARP combination to get network access when arp=disabled on a particular interface

The screenshot shows a network management interface with two windows. The top window, titled 'ARP List', displays a table of ARP entries. The bottom window, titled 'ARP <10.2.72.33>', is a dialog for editing a specific entry.

	IP Address	MAC Address	Interface
D	10.2.72.10	00:30:4F:4C:90:03	ether1
D	10.2.72.20	00:09:34:20:6A:F6	ether1
D	10.2.72.21	00:23:08:B7:95:8A	ether1
D	10.2.72.24	00:06:DC:80:45:2A	ether1
D	10.2.72.27	3C:8B:FE:41:8A:53	ether1
D	10.2.72.33	00:0C:42:5A:AE:61	ether1
D	10.2.72.35	00:0C:42:0E:59:9C	ether1
D	41.215.232.65	00:0B:6B:56:34:56	wlan1
D	41.223.35.57	00:21:04:FA:8A:72	ether1
D	41.223.35.58	00:0C:42:5A:AE:61	ether1
D	41.223.35.61	E0:91:53:11:3D:D5	ether1
	172.18.8.241	00:30:4F:4C:90:03	ether1
	172.18.33.254	00:0C:42:1D:36:DE	ether1

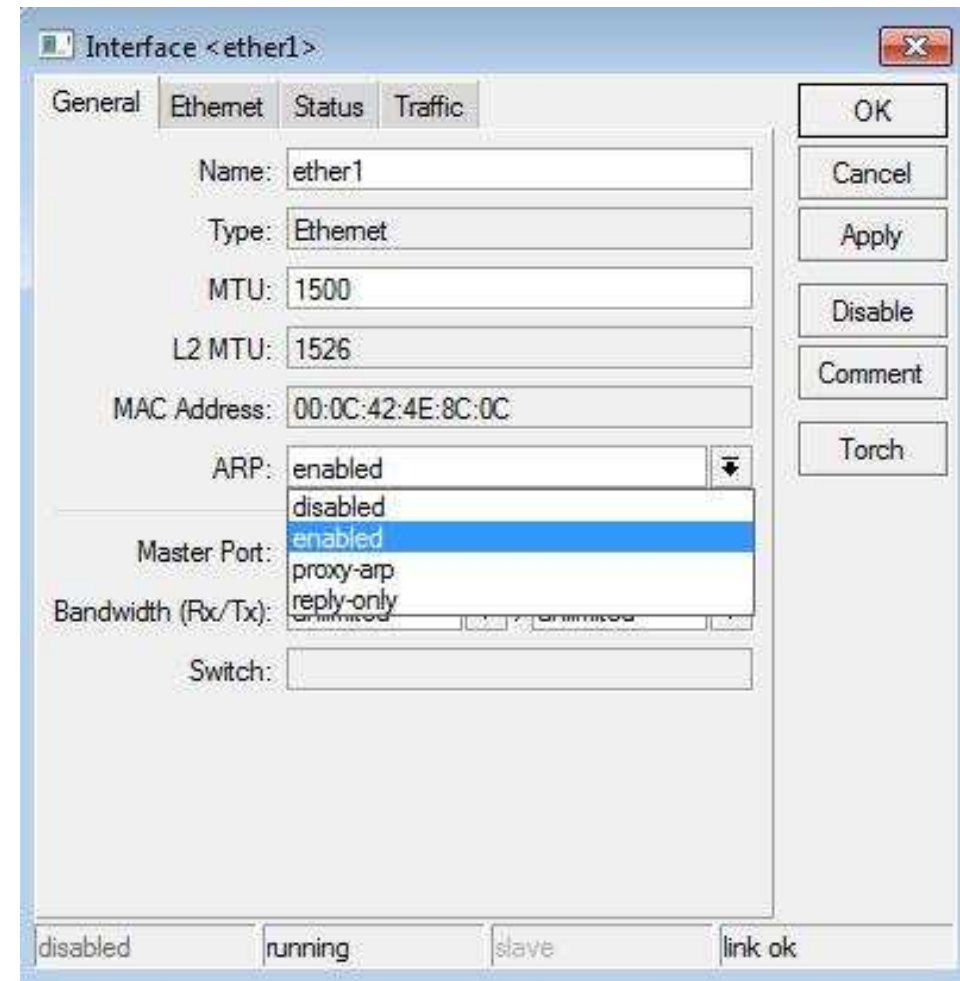
The 'ARP <10.2.72.33>' dialog box contains the following fields and buttons:

- IP Address: 10.2.72.33
- MAC Address: 00:0C:42:5A:AE:61
- Interface: ether1
- Buttons: OK, Copy, Remove, Make Static (highlighted in red), Ping

Static ARP Configuration

Use the Interface General tab to set ARP behaviour

- Enabled – normal operation
- Disabled – manual setting on client and server
- Reply-only – Manual setting on server
- Proxy-arp – Proxy requests between 2 directly connected networks e.g across a PTP tunnel



Static ARP

LAB

Create a static ARP entry for your laptop

Set arp=reply-only on your router's Local Network interface

Test network connectivity

Change your computer IP address

Test Internet connectivity

Set ARP back to Enabled and restore your laptop's IP address

Network Bridging

Theory of bridging

Transparent network management

Joining networks together

Ethernet Bridge

Ethernet-like networks can be connected together using OSI Layer 2 bridges

The bridge feature allows interconnection of hosts of separate LANs as if they were attached to a single LAN segment

Bridges extend the broadcast domain and increase the network traffic on bridged LAN

Bridges can be created directly from the Bridge menu.

Remote networks can be bridged using VLAN technologies such as EOIP or Bridged PPP (BCP)

An Ethernet switch is a kind of “multiport bridge”

Note that collisions are not possible in a full duplex switched network



Advantages of a Bridge

Simplified network structure

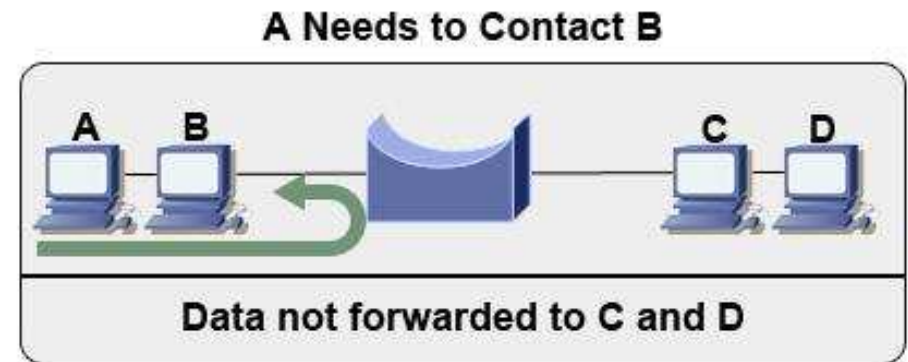
Isolate collision domains with micro-segmentation

Easy expansion of broadcast domain

Access control and network management capabilities (esp. when using transparent bridging)

Certain IP services rely on bridged networks to operate correctly

- PPPoE Concentrators, HotSpot servers, DHCP Services, VLANs

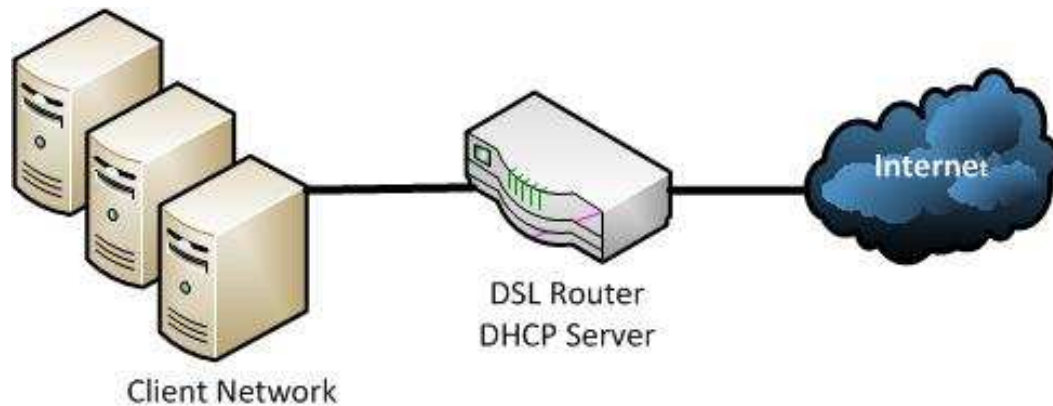


Transparent Bridge Filtering

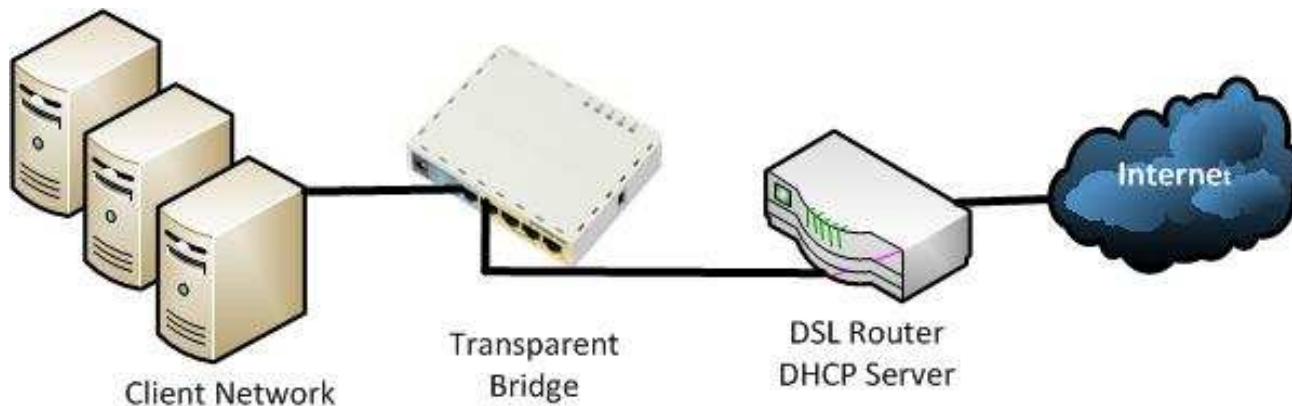
You can use the bridge function to transparently insert a MikroTik device into an existing network

- No modification of IP's, gateways etc. is required

This allows bandwidth management, firewalling, transparent proxying and other services



Standard client network, DHCP runs on DSL router



Transparently bridged network
DHCP still on ADSL router
Now possible to proxy, bandwidth limit etc. transparently to clients

Disadvantages of a Bridge

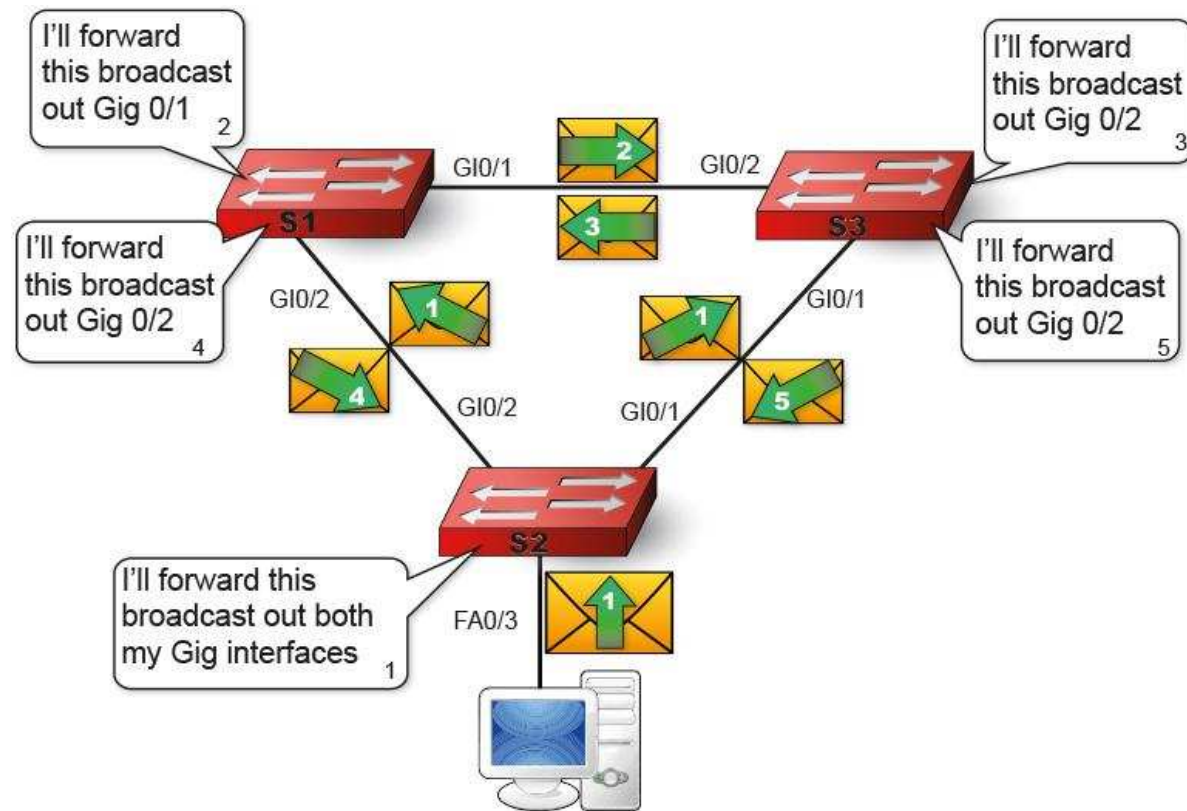
Does not limit the scope of broadcasts

Does not scale to large networks

Buffering and processing introduces delays

A complex network topology can pose a problem for transparent bridges.

- multiple paths between transparent bridges and LANs can result in bridge loops
- The (rapid) spanning tree protocol helps to reduce problems with complex topologies.



Adding a Bridge Interface

To add a bridge interface to the router

- Click **Bridge** in winbox to open up the bridge window
- Click **+** to add a new bridge interface, give the bridge a name (if desired) and click **OK**

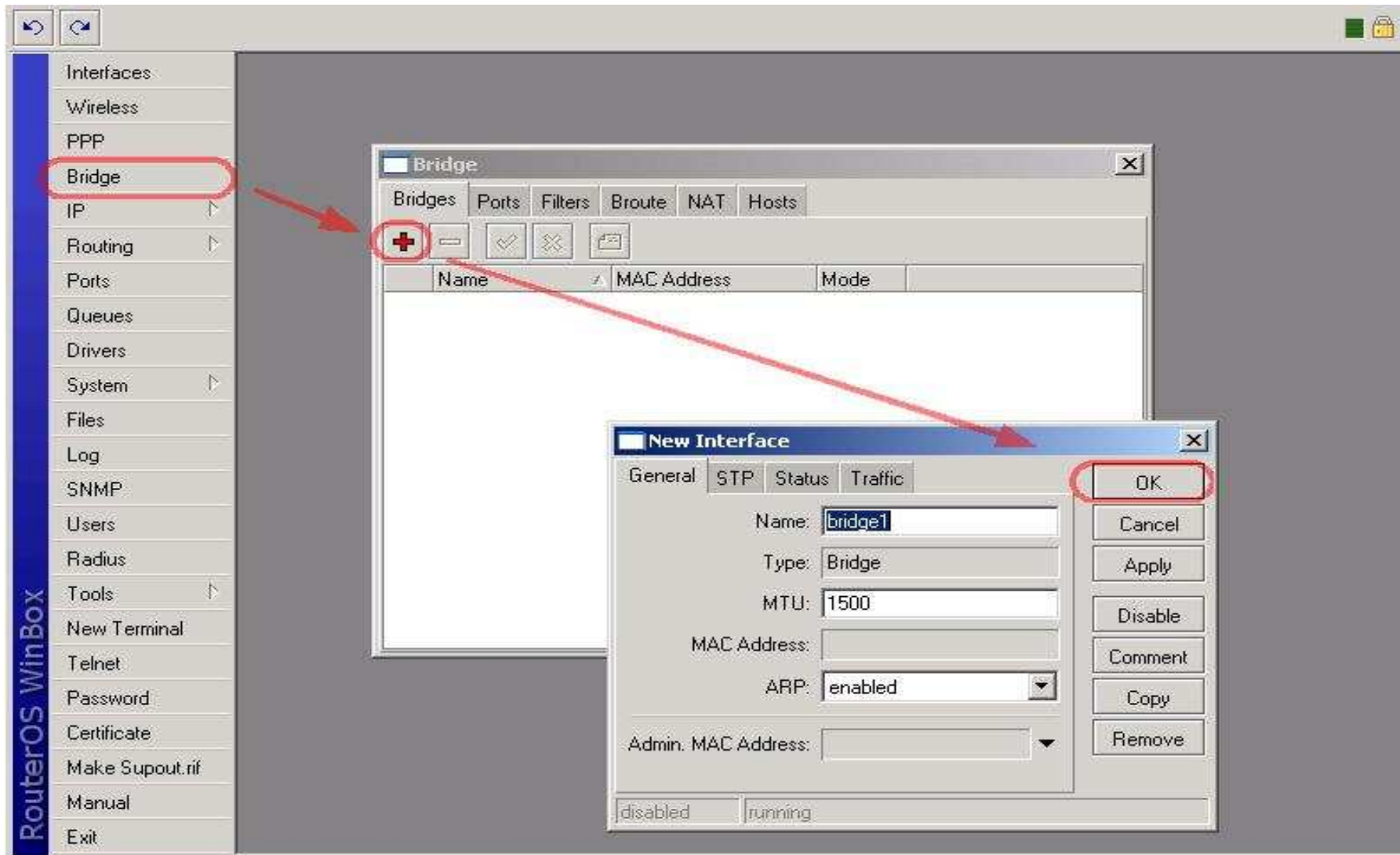
This creates the bridge “container”

- By itself the bridge interface does nothing (unless it is used as a loopback interface)
- You still need to add “ports” (interfaces) to the bridge container to achieve the desired functionality

In command line, use command

- **/interface bridge add** to add a bridge
- **/interface bridge print** to see the bridge interface

Creating a Bridge



Adding Ports to the Bridge

To add ports to the bridge

- Select the **Ports** tab in Bridge window
- Click **+** to add a new bridge port
- Select the interface to be added to the specified bridge
- Click **OK**

Any Ethernet type interface can be bridged except the wireless interface in station mode

- Ether ports
- VLAN's
- Wireless AP
- Virtual AP
- EoIP Tunnels
- PPTP/L2TP/SSTP with BCP (Bridge Control Protocol)

***TIP**

Assigning Ports to the Bridge

The screenshot displays the RouterOS WinBox interface. On the left sidebar, the 'Bridge' menu item is highlighted with a red oval. The main window shows the 'Bridge' configuration page with the 'Ports' tab selected. A table lists the assigned ports:

Interface	Bridge
ether1	bridge1

The 'Bridge Port <ether1>' dialog box is open, showing the following configuration options:

- Interface: ether2
- Bridge: bridge1
- Priority: 80 hex
- Path Cost: 10
- Edge: auto
- Point To Point: auto
- External FDB: auto

Red arrows indicate the flow of the process: from the 'Bridge' menu, to the 'Ports' tab, to the '+' button, and finally to the 'Bridge Port' dialog box.

Bridging

LAB

Connect to your neighbour using an Ethernet cable on port 2

Bridge your ether1 and ether2 together

Check in Winbox loader – when you press the 3 dots do you see your neighbours router along with your own?

Add an additional IP to your laptop from the same /24 range – use 172.16.x.1/24 and 172.16.x.2/24

- X must be the same on both computers – use the lowest of your assigned numbers
- Additional IP's can be added in Interface properties → TCP/IPv4 → Advanced

Test ping to each other (check firewall settings)

Restore your router from backup

Wireless and VPN Bridging



Due to limitations of 802.11 you cannot bridge a wireless device running in station mode

To bridge wireless clients a number of options are available

- Station-pseudobridge and Station-pseudobridge-clone for non-RouterOS AP's
- Station-wds and Station-bridge (easiest) for RouterOS AP's

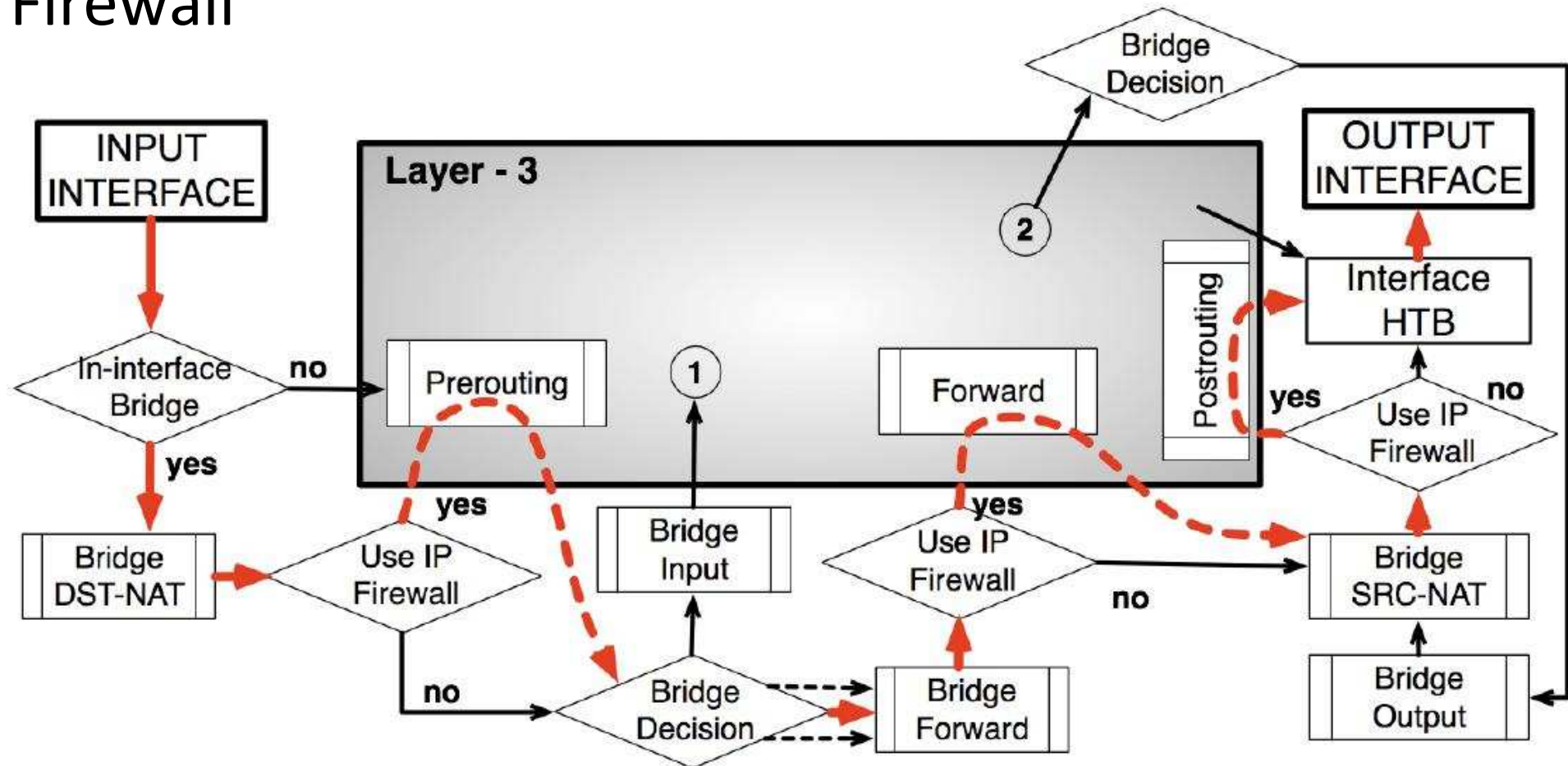
You can bridge IP routed networks using any VPN technology that supports carrying MAC addresses

- EoIP (Ethernet over IP) – MikroTik proprietry protocol
- PPTP/L2TP with BCP (Point to Point / Layer 2 Tunneling Protocol with Bridge Control Protocol) – also PPPoE with BCP could work

Using IP Firewall in Bridge

Enable in Bridge → Settings → Use IP Firewall

Traffic flowing through the bridge can be processed by IP Firewall



IP Routing

Transferring Datagrams through Networks

Basic Routing Theory

At it's simplest, routing involves the forwarding of datagrams (packets, frames) between different physical networks

The objective is the delivery of packets between two systems connected to different networks

When a host needs to send a packet to another host it will examine the IP / Mask combination to determine if the destination is on the local network or on a remote network

If the destination is local the packet is delivered directly

If the destination is not local the host examines its routing table for a matching destination entry

If it finds a matching route it will send the packet to the relevant gateway

If it does not have a matching route it will look for a default (catchall) route and send the packet there

IP Routes

Static Routing is the most basic routing you can do

It is very fast, but has no redundancy capabilities

To access go to “IP” > “Routes” in winbox

***TIP**

If you have added an IP address to router's interface, and the interface is enabled, there should be a dynamic (D) active (A) route for the directly connected (C) network

These are “known” routes that the router builds automatically based on your IP settings – the router will add one for each IP address that is assigned to it

Note if you have a default route from DHCP/PPPoE it can appear as both Dynamic and Static at the same time!

***TIP**

Static IP Routes

You need to add more routes to “tell” the router where to send IP packets for hosts, that do not belong to any of the directly connected networks.

You can add routes to specific networks over specific gateways

- Please note, that the gateway should always be directly reachable over one of the router's interfaces!

Use Gateway Interface only for “tunnelling” type interfaces where the IP might change

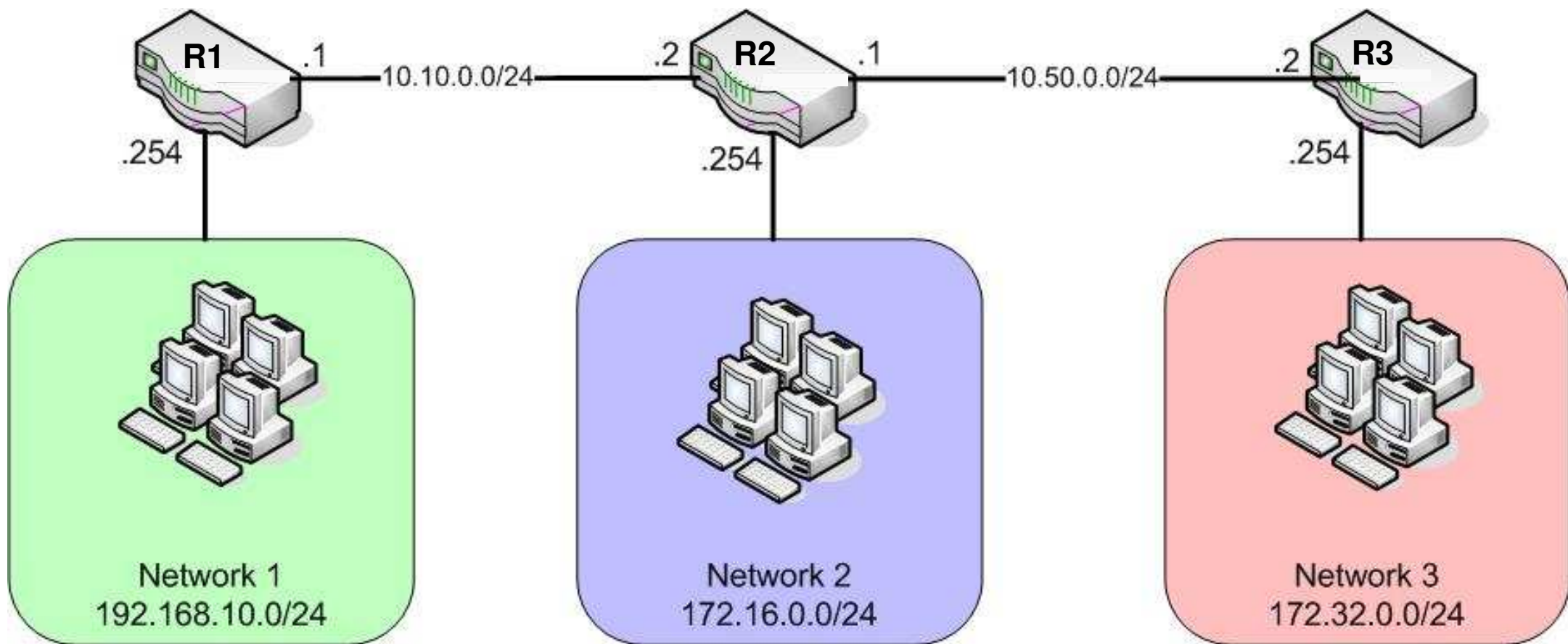
***TIP**

The screenshot shows the 'New Route' dialog box with the following configuration:

- Destination: 192.168.56.0/24
- Gateway: 10.1.1.56
- Gateway Interface: (empty)
- Interface: (empty)
- Check Gateway: (empty)
- Type: unicast
- Distance: (empty)
- Scope: 255
- Target Scope: 10
- Routing Mark: (empty)
- Pref. Source: (empty)

Buttons on the right: OK, Cancel, Apply, Disable, Comment, Copy, Remove.

Bottom status: disabled (selected), active.



DST NET	GATEWAY
172.16.0.0/24	10.10.0.2
172.32.0.0/24	10.10.0.2

DST NET	GATEWAY
192.168.10.0/24	10.10.0.1
172.32.0.0/24	10.50.0.2

DST NET	GATEWAY
192.168.10.0/24	10.50.0.1
172.16.0.0/24	10.50.0.1

Static Routing

LAB

Test the wireless connection between you and your neighbour's router using the ping command

- How can you get your neighbour's IP address?

Add a static route to your router so you can reach your neighbour's network 192.168.Y.0/24 over the wireless interface

Test if the routing is correct using ping and traceroute to

- 192.168.Y.254 (router's address)
- 192.168.Y.1 (workstation's address)

Make sure your laptop Firewall allows ping requests

- Can you ping your laptop from your own router?

Default Route

If there is a “smart” host on the network which knows how to send packets to other networks, you can use it as the default gateway for your router and add a static default route with

- destination 0.0.0.0/0 (any address)
- the IP address of the “smart” host as the gateway

If the router cannot find a valid route in its static or dynamic route tables it will send the packet to the default gateway.

The default route can be added in a number of ways

- Via DHCP client
- Via PPPoE client
- Static route
- Dynamic routing protocol
(OSPF, RIP, BGP)

***TIP**

Adding the Default Route

The screenshot shows the RouterOS WinBox interface. The left sidebar contains a menu with 'IP' and 'Routes' highlighted with red circles. The main window displays the 'Route List' dialog, which contains a table of existing routes. Below this, the 'New Route' dialog is open, showing the 'General' tab with the following fields:

- Dst. Address: 0.0.0.0/0
- Gateway: 10.1.1.55
- Type: unicast
- Distance: (empty)
- Scope: 30
- Target Scope: 10
- Routing Mark: (empty)
- Pref. Source: (empty)

The 'New Route' dialog also features buttons for OK, Cancel, Apply, Disable, Comment, Copy, and Remove. At the bottom of the dialog, there are status indicators for 'enabled' and 'active'.

	Destination	Gateway	Pref. Source	Distance	Interface	Routing Mark
DAC	10.1.100.0/24		10.1.1.1	0	wlan1	
DAC	172.16.12.0/24		172.16.12.1	0	ether3	
DAC	192.168.1.0/24		192.168.1.254	0	ether1	

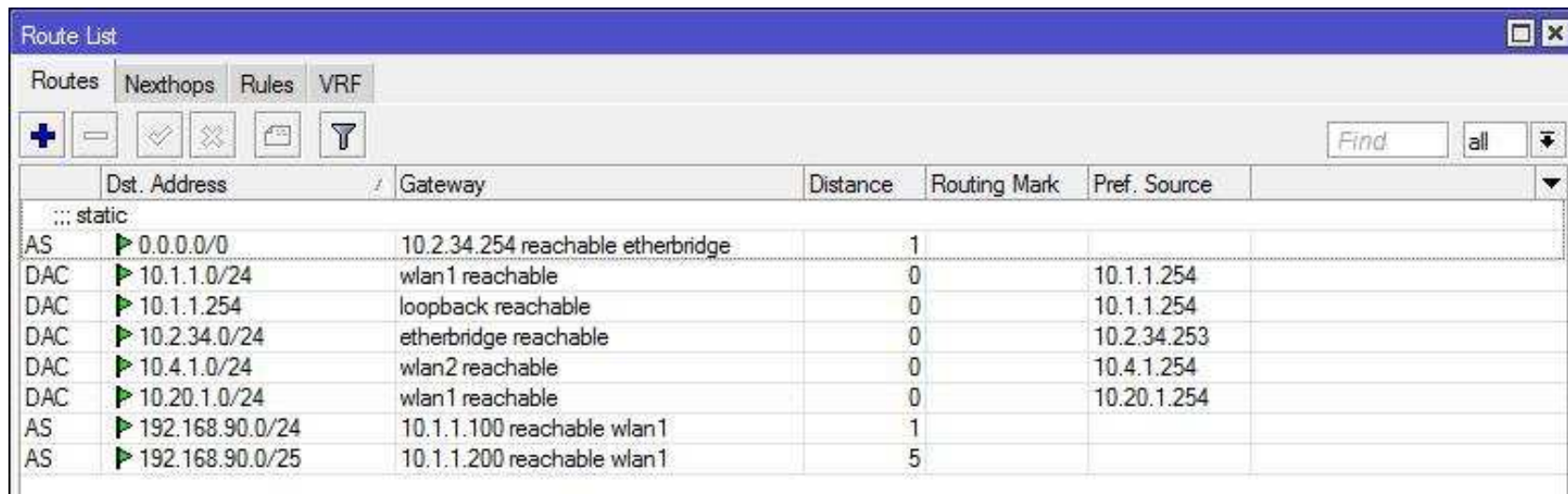
Specific Routing

If there are two or more routes pointing to the same address, the more specific one will be used

Dst: 192.168.90.0/24, gateway: 1.2.3.4

Dst: 192.168.90.128/25, gateway: 5.6.7.8

If a packet needs to be sent to 192.168.90.135, gateway 5.6.7.8 will be used, irrespective of route distance



The screenshot shows a 'Route List' window with a table of routes. The table has columns for 'Dst. Address', 'Gateway', 'Distance', 'Routing Mark', and 'Pref. Source'. The routes are listed as follows:

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
AS	0.0.0.0/0	10.2.34.254 reachable etherbridge	1		
DAC	10.1.1.0/24	wlan1 reachable	0		10.1.1.254
DAC	10.1.1.254	loopback reachable	0		10.1.1.254
DAC	10.2.34.0/24	etherbridge reachable	0		10.2.34.253
DAC	10.4.1.0/24	wlan2 reachable	0		10.4.1.254
DAC	10.20.1.0/24	wlan1 reachable	0		10.20.1.254
AS	192.168.90.0/24	10.1.1.100 reachable wlan1	1		
AS	192.168.90.0/25	10.1.1.200 reachable wlan1	5		

Route Distance

***TIP**

If you have multiple routes to the same destination (e.g. 2 default routes) then the one with the lower distance will be chosen

Static routes and PPPoE routes have a default distance of 1

- This can be altered if required

DHCP Client default route distance is 0

- This will therefore override a static or PPPoE route

	Dst. Address	Gateway	Distance	Routing Mark
AS	0.0.0.0/0	10.0.0.1 reachable ether4	5	
S	0.0.0.0/0	10.0.0.2 reachable ether4	10	

10.0.0.1 is the chosen gateway as it has a lower distance

Advanced Routing?

The MTCRE Certified Routing Engineer covers advanced routing subjects such as

- Multipath routing
- Static and dynamic failover
- Policy Routing
- Open Shortest Path First (OSPF) routing

The MTCINE Certified Internetworking Engineer is the most advanced MikroTik course covering mainly

- iBGP and eBGP Border Gateway Protocol
- MPLS MultiProtocol Label Switching
- VPLS Pseudowires
- VRF Virtual Routing and Forwarding

Command Line Interface

Text-based RouterOS Configuration

Command Line Interface (CLI)

You can access the CLI by clicking “New Terminal”

For the first time log in as ‘admin’, no password.

Once logged in, press `[?]` to see all commands at the current menu level

- `[admin@MikroTik] > [?]`

Press `[Tab]` twice to see a short list of all available commands

- `[admin@MikroTik] > ip [Tab][Tab]`

Use up and down arrow to cycle through previous commands

- Up to 200 are stored

You can use these commands at any level

- `[admin@MikroTik] > ip address [?]`

- `[admin@MikroTik] > ip address print [Enter]`

Using CLI : Console Completion

Commands and arguments don't have to be completely typed, hit *[Tab]* to complete the typing:

- [admin@MikroTik] > ip add[Tab]
- [admin@MikroTik] > ip address

If single *[Tab]* doesn't work, hit it twice to see available options

- [admin@MikroTik] > i[Tab][Tab]
import interface ip
- [admin@MikroTik] > in[Tab]
- [admin@MikroTik] > interface

The CLI will change colour to show you validity

```
[david@Milnerton] > ip address add address=10.5.72.1/24 interface=ether2
```

Using CLI : Navigation

You can go step-by-step down into menus:

- [admin@MikroTik] > ip [Enter]
- [admin@MikroTik] ip > address [Enter]
- [admin@MikroTik] ip address> print [**Enter**]

Use “..” to go one level up in the menu tree

- [admin@MikroTik] ip address> .. [Enter]
- [admin@MikroTik] ip > .. [Enter]
- [admin@MikroTik] >

Use [/] to go up to the root level

- [admin@MikroTik] ip address> /
- [admin@MikroTik] >

'Print' and 'Monitor'

'print' is one of the most often used commands in the CLI. It prints a list of items, and can be issued with a number of arguments, e.g.,

- `print status,`
- `print interval=2s,`
- `print without-paging, etc.`

Use 'print ?' to see the available arguments

The items can be identified by their number for further modification

Note this number is dynamically assigned at the time of issuing the print command

'monitor' continuously shows status of items

- `/in et monitor ether2`

'Add', 'Set' and 'Remove'

Use the *'add'* command to create additional items, you can specify a set of options for this new item in a particular menu.

You can change or add some options for already existing items by using the *'set'* command

Or you can delete items by using the *'remove'* command

Use the line number returned by “print” for remove and set commands

'Undo' and 'Redo'

To revert to a previous configuration state, use the '/undo' command

```
- [admin@MikroTik] > /undo
```

To repeat the last undone action, enter the '/redo' command

```
- [admin@MikroTik] > /redo
```

'Undo' and 'Redo' are available in winbox GUI as two buttons with arrows on top left corner of the winbox window.

More Common Commands

Use **/interface wireless** to perform common wireless functions

- `/interface wireless print`
- `/interface wireless scan 0`
- `/interface wireless set band=2.4GHz-B/G ssid=Internet`

Use **/ip route** to check and set or add routes

- `/ip route print`
- `/ip route add dst-address=0.0.0.0/0 gateway=41.23.31.1`

Use **/ping** and **/tool traceroute** for troubleshooting

- `/ping www.google.com`
- `/tool traceroute www.google.com`

Command Line



Remove your

- DHCP Client

Use the Terminal to add an IP address 10.1.1.XY/24

- Check ping to Trainer Wlan IP 10.1.1.254

Add a Default Route via Terminal

- Check traceroute to Internet

Monitor the status of your interfaces via Terminal while you browse the net.

Create a backup called “*backup-your_name-ROUTED*” (from Winbox) Save the backup to your laptop

Wireless Theory

AP mode

Access control

Interface Settings

Wireless tools

Station-WDS and Bridging

Nstreme and NV2

Access Point

Uses “AP-Bridge” mode

- “bridge” mode is for allowing 1 client to connect with Level 3 license, useful for PTP

Creates wireless infrastructure by defining Service Sets (SSID)

Participates in Wireless Area

Expects stations to follow its frequency (DFS by Scan List)

Uses authentication based on Access Lists

Interface <wlan-pavilion-place>

General Wireless Data Rates Advanced WDS ...

Mode: ap bridge

Band: 5GHz

Frequency: 5765 MHz

SSID: pp-oc-bb

Radio Name: Ocean - Seapoint

Scan List:

Security Profile: default

Frequency Mode: manual txpower

Country: ireland

Antenna Mode: antenna a

Antenna Gain: 0 dBi

DFS Mode: none

Proprietary Extensions: post-2.9.25

WMM Support: disabled

Default AP Tx Rate: bps

Default Client Tx Rate: bps

Default Authenticate

Default Forward

Hide SSID

OK

Cancel

Apply

Disable

Comment

Torch

Scan...

Freq. Usage...

Align...

Sniff...

Snooper...

Reset Configuration

Simple Mode

disabled running slave running ap

Wireless AP/Station II

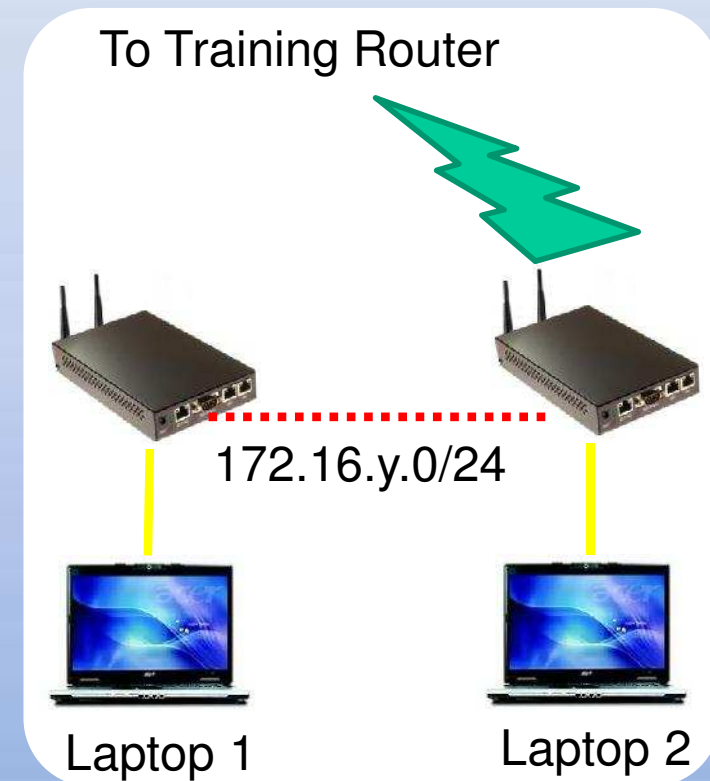
LAB

On the AP unit:

- Add a static route to your neighbours 192.168.x.0/24 range via the Wlan2 connection (172... IP)

On the station unit:

- disable your connection to Trainer router (Wlan1)
- disable your NAT (masquerade) rule
- Configure routing to get internet through your neighbours wireless (modify your default route)
- Test internet access via your neighbours router



Bridging a Station

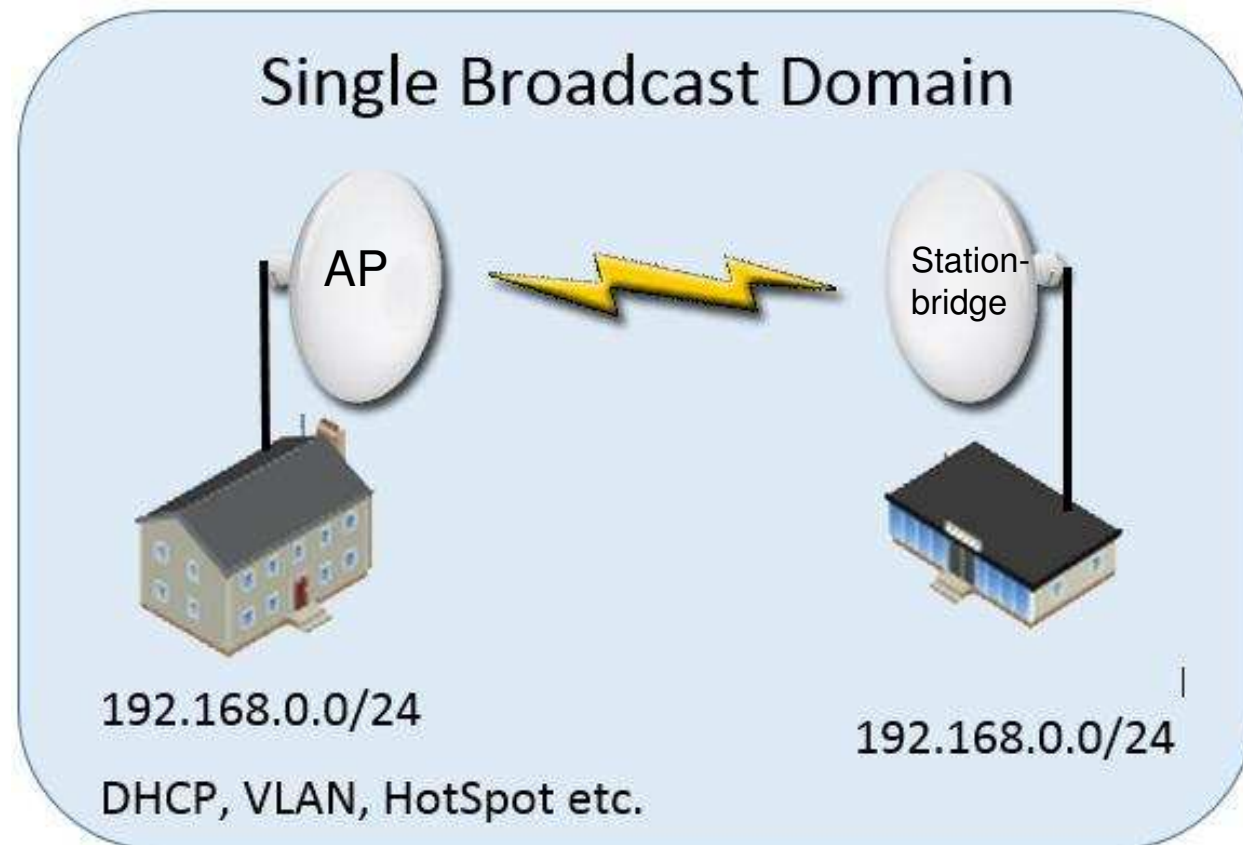
Normally a station cannot be bridged because of 802.11 limitations

Station-bridge mode can be used to overcome this limitation

A station-bridge client can be bridged to another interface on the router and pass through layer2 information

To create a client<>client transparent bridge:

1. Create a bridge interface on both sides
2. On the AP Wireless enable bridge mode (usually enabled by default)
3. Add any required Ether and Wlan interfaces into the bridge
4. On the station enable station-bridge mode and bridge the wireless and ether interfaces



Station Bridge mode

LAB

Create a transparent bridge using standard ap-bridge on the AP and station-bridge on the client

- All you need to do is change the mode to station-bridge on the station side – all other settings remain the same

On the AP and Client:

- Create a bridge
- add the ether and wireless interfaces

In the Wireless interface:

- Check that Bridge Mode is enabled (default)

Move the 172.16.y. IP to the bridge on the AP side

- DHCP must run on the bridge if any interface is in a bridge

Setup a DHCP server on the bridge on the AP

On both laptops set to DHCP, test ping to each other, check internet connectivity

- The station unit is essentially transparent to the network

Registration Table

Contains information about who is connected to the AP or which AP the station connects to

The image displays a Mikrotik WinBox interface. At the top, the 'Wireless Tables' window is open, showing the 'Registration' tab. A table lists connected clients, with one entry highlighted in blue. Below this, three 'AP Client' configuration windows are shown, each corresponding to the highlighted client in the table. Red circles and arrows highlight the 'Registration' tab, the client entry, and the 'General', 'Signal', and 'Statistics' tabs in the AP Client windows.

Wireless Tables - Registration

Interface	Radio Name	MAC Address	AP	Tx/Rx Rate	Last Activity	Signal Strength	WDS	Uptime
wlan1	X_unknown	00:0C:42:05:00:1C	no	54Mbps	0.000	-68	no	00:01:37

AP Client <00:0C:42:05:00:1C> - General

Radio Name: X_unknown
MAC Address: 00:0C:42:05:00:1C
Interface: wlan1
Uptime: 00:01:37
Ack. Timeout: 25 us
RouterOS Version: 2.9.XX
AP Tx Limit:
Client Tx Limit:
Last IP:
 AP
 WDS

AP Client <00:0C:42:05:00:1C> - Signal

Last Activity: 0.000 s
Signal Strength: -58 dBm
Tx Signal Strength: -53 dBm
Signal To Noise: 37 dB
Tx/Rx CCQ: 93/95 %

- Signal Strengths

Rate	Strength
6Mbps	-54
9Mbps	-54
12Mbps	-56
18Mbps	-58
24Mbps	-60
36Mbps	-62
48Mbps	-64
54Mbps	-68

AP Client <00:0C:42:05:00:1C> - Statistics

Tx/Rx Rate: 54Mbps
Tx/Rx Packets: 550/794745
Tx/Rx Bytes: 41576/1202538377
Tx/Rx Frames: 550/794804
Tx/Rx Frame Bytes: 38630/1197770772
Tx/Rx Hw Frames: 550/794813
Tx/Rx Hw. Frame Bytes: 51830/1216846302

Access Management

default-forwarding (Access Point mode only)

- Gives the ability to disable communication between wireless clients on the Layer 2 level
- Stops clients from establishing PTP connections directly to each other (and bypassing your bandwidth management system)

default-authentication (AP and Station mode)

- Allows the AP to register a client even if it is not in the access list
- For a station mode client it allows it to associate with an AP not listed in the client's connect list

Wireless Access List

Individual settings for each client in access list will override the interface default settings

Access list entries can be made from the registration table entries by using action 'Copy to Access List'

Access list entries are ordered, just like in firewall

Matching by individual or all interfaces "interface=all"

Signal Strength specifies a minimum RX signal level

AP and Client TX Limits can be used for rate limiting per client

- Only works with RouterOS Clients
- Non-ROS clients will ignore the rate limit

***TIP**

"Time" – specifies when this rule is active

Global rules can be specified by leaving MAC field blank

- Default Authenticate must be turned off on interface

Access List Operation

Access list rules are checked sequentially from the top
Disabled rules are always ignored.

Only the first matching rule is applied

If there are no matching rules for the remote connection,
then the default values from the wireless interface
configuration are used

If remote device is matched by rule that has
authentication=no value, the connection from that
remote device is rejected

Wireless Access list

The image shows a network configuration interface with two windows. The main window, titled "Wireless Tables", has tabs for "Interfaces", "Nstreme Dual", "Access List", "Registration", "Connect List", and "Security Profiles". The "Access List" tab is active, displaying a table with columns: MAC Address, Interface, Signal Str..., Authentication, and Forwarding. Two entries are listed, both for MAC address 00:0C:42:0C:0A:ED on interface wlan1 with a signal strength range of -120..120. The first entry has Authentication set to "no" and Forwarding set to "no". The second entry has Authentication set to "yes" and Forwarding set to "yes". A status bar at the bottom indicates "2 items [1 selected]".

The second window, titled "AP Access Rule <00:0C:42:0C:0A:ED>", provides a detailed configuration for the selected rule. It includes the following fields and options:

- MAC Address: 00:0C:42:0C:0A:ED
- Interface: wlan1
- Signal Strength Range: -120..120
- AP Tx Limit: (empty)
- Client Tx Limit: (empty)
- Authentication:
- Forwarding:
- Private Key: none
- Private Pre Shared Key: (empty)
- Time: 08:00:00 - 18:00:00
- Days: sun, mon, tue, wed, thu, fri, sat

Control buttons on the right side of the dialog include: OK, Cancel, Apply, Disable, Comment, Copy, and Remove. The status "disabled" is shown at the bottom of the dialog.

Wireless Access List



Restore backup *your_name*-WIRELESS

Disable the default interface settings on wlan2:
default-forwarding, default-authentication

Make sure that nobody is connected to your AP

Add access list entry with your neighbour's MAC address and make sure it connects

Switch roles and test again

Add a client and AP TX limit, test the functionality using bandwidth test

- Be sure to specify kbps in limit!

Wireless Connect List

You can allow or deny a station from connecting to a specific AP by using Connect list rules

Connect list entries can be made from registration table entries by using the action 'Copy to Connect List'

Connect list entries are ordered, just like in firewall

Used also for WDS links

Can be used to limit by MAC, SSID, Signal Strength, Area Prefix

Allows for 1 client to be able to connect to multiple security profiles

***TIP**

Connect List Operation

connect-list rules are always checked sequentially, starting from the first.

disabled rules are always ignored.

Only the first matching rule is applied.

If connect-list does not have any rule that matches remote access point, then the default values from the wireless interface configuration are used.

Connect List Operation

If access point is matched by rule that has connect=yes value, connection with this access point will be attempted.

- In station mode, if several remote access points are matched by connect list rules with connect=yes value, connection will be attempted with access point that is matched by rule higher in the connect-list.
- If no remote access points are matched by connect-list rules with connect=yes value, then value of default-authentication interface property determines whether station will attempt to connect to any access point. If default-authentication=yes, station will choose access point with best signal and compatible security.

In access point mode, connect-list is checked before establishing WDS link with remote device.

- If access point is not matched by any rule in the connect list, then the value of default-authentication determines whether WDS link will be established.

Wireless Connect List

New Station Connect Rule

Interface: wlan1

MAC Address: 00:02:6F:45:15:43

Connect

SSID: AP2G

Area Prefix:

Signal Strength Range: -120..120

Security Profile: default

disabled

1

New Station Connect Rule

Interface: wlan1

MAC Address:

Connect

SSID: AP2G

Area Prefix:

Signal Strength Range: -75..120

Security Profile: default

disabled

2

New Station Connect Rule

Interface: wlan1

MAC Address:

Connect

SSID:

Area Prefix:

Signal Strength Range: -120..120

Security Profile: default

disabled

3

Wireless Tables

Interfaces | Nstreame Dual | Access List | Registration | **Connect List** | Security Profiles

Find

#	Interface	MAC Address	Connect	Area Prefix	Signal Str...	Security ...
0	wlan1	00:02:6F:45:15:43	yes		-120..120	default
1	wlan1		yes		-75..120	default
2	wlan1		no		-120..120	default

3 items [1 selected]

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

RouterOS does not support the insecure PIN mode



Other Settings

Max-station-count (Wireless Advanced tab) – controls how many devices may be connected to the AP at any given time

Scan List – used with Superchannel mode to scan for frequencies outside of the defined Country setting

- Acceptable formats: default,5545,5100-5200

Data Rates – used to limit max available data rate for non 802.11N modes

TX Power – used to limit TX power on card when using card-rates mode

Adaptive Noise Immunity (ANI) adjusts various receiver parameters dynamically to minimize interference

Wireless Security

Security profiles are configured under the `/interface wireless security-profiles` path in the console, or in the **Security Profiles** tab of the **Wireless** window

MikroTik supports all common forms of wireless security, including WEP, WPA and WPA2

WEP support is provided for backward compatibility but as it is a weak security method it should be avoided

To configure security you first need to define a security profile

- You can then assign the profile to an interface
- You can also assign the profile to a connect list rule

Wireless Encryption

New Security Profile

General | RADIUS | EAP | Static Keys

Name: profile1

Mode: dynamic keys

Authentication Types

WPA PSK WPA2 PSK

WPA EAP WPA2 EAP

Unicast Ciphers

tkip aes ccm

Group Ciphers

tkip aes ccm

WPA Pre-Shared Key: WPA_keys

WPA2 Pre-Shared Key: WPA_keys

Supplicant Identity:

Group Key Update: 00:05:00

OK Cancel Apply Copy Remove

Interface <wlan1>

General | Wireless | Data Rates | Advanced | WDS | ...

Mode: ap bridge

Band: 2.4GHz-B/G

Frequency: 2412 MHz

SSID: AP2G

Radio Name: 000C420CB283

Scan List:

Security Profile: profile1

Frequency Mode: manual txpower

Country: no_country_set

Antenna Gain: 0 dBi

DFS Mode: none

Proprietary Extensions: post-2.9.25

Default AP Tx Rate: bps

Default Client Tx Rate: bps

Default Authenticate

Default Forward

Hide SSID

disabled | running | running ap

OK Cancel Apply Disable Comment Scan... Freq. Usage... Align... Sniff... Snooper...

Wireless Encryption



Restore backup-*your_name*-WIRELESS

Create a new security profile with options:

mode=dynamic-keys

authentication-type=wpa2-psk

group/unicast ciphers=aes-ccm

wpa2-key=test_password

Assign the profile to your wlan2 interface on the AP

- Verify that the client can no longer connect

Assign the profile on the client and verify connectivity

Try to replicate the same behaviour on the client using a Connect List rule

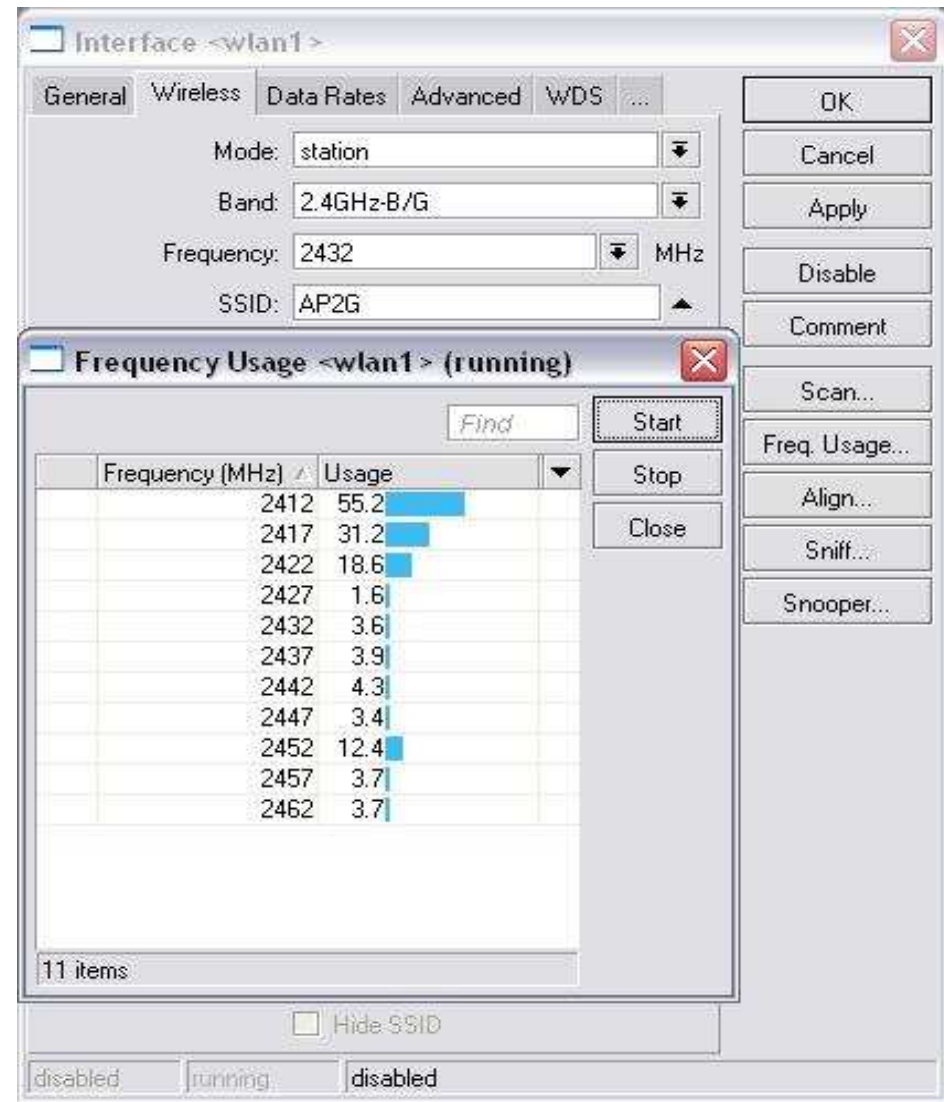
Frequency Usage Tool

Frequency Usage Monitor looks only for IEEE 802.11 frames

Interface is disabled during the Frequency usage monitor

Use it to get a quick idea of which frequencies are busy

Will only scan within the Country / Scan List setting



Wireless Snooper Tool

Shows all wireless usage for a given band including AP's, clients and unknown data sources

The screenshot displays the 'Snooper <wlan1> (running)' application window. It features a 'Networks' tab and a 'Stations' tab. A table lists various wireless networks with columns for Frequency, Band, Address, SSID, Of Freq. (%), Of Traf. (%), Bandwidth, and Networks. The network 'AP2G' with address '00:02:6F:45:15:43' is selected. A 'Wireless Network <00:02:6F:45:15:43>' dialog box is open, showing details for this network, including its frequency (2432 MHz), band (2.4GHz-B/G), address, SSID (AP2G), and other statistics.

Frequency	Band	Address	SSID	Of Freq. (%)	Of Traf. (%)	Bandwidth	Networks	Stations
2412	2.4GHz...	00:0B:6B:4D:03:6B	hotspot	0.0	0.0	0 bps		
2412	2.4GHz...	00:0B:6B:4D:03:99	hotspot	0.0	0.0	0 bps		
2412	2.4GHz...	00:0B:6B:4D:04:2A	hotspot	1.7	18.5	15.5 kbps		
2412	2.4GHz...	00:0C:42:05:01:39	test_ap	0.4	5.1	3.8 kbps		
2412	2.4GHz...	00:0C:42:05:28:30	hotspot	0.0	0.0	0 bps		
2412	2.4GHz...	02:0B:6B:37:67:0D	hot	0.5	5.7	4.4 kbps		
2417	2.4GHz...			4.5		24.6 kbps	0	
2422	2.4GHz...			1.8		15.2 kbps	1	
2422	2.4GHz...	00:0C:42:0C:83:47	m-pak	0.0	0.0	0 bps		
2427	2.4GHz...			2.1		17.4 kbps	0	
2432	2.4GHz...			15.3		3.7 Mbps	3	
2432	2.4GHz...	00:02:6F:08:53:18		0.6	4.1	4.3 kbps		
2432	2.4GHz...	00:02:6F:45:15:43	AP2G	12.8	83.4	3.7 Mbps		
2432	2.4GHz...	00:0E:2E:40:89:A7	MY AP	0.3	2.5	2.8 kbps		
2437	2.4GHz...			1.7		14.1 kbps	1	
2437	2.4GHz...	00:16:B6:D9:53:D6	linksys	0.5	31.8	4.4 kbps		
2442	2.4GHz...			2.3		18.1 kbps	2	
2442	2.4GHz...	00:0B:6B:37:5B:B4	dzintars	0.9	41.8	7.7 kbps		
2442	2.4GHz...	00:17:9A:FD:F7:81	racer	0.4	20.9	3.8 kbps		
2447	2.4GHz...			1.9		15.7 kbps	0	
2452	2.4GHz...			1.7		10.5 kbps	3	
2452	2.4GHz...	00:0B:6B:31:52:69	tests	0.0	0.0	0 bps		
2452	2.4GHz...	00:0C:42:05:06:F3	Demo	0.0	0.0	0 bps		

35 items (1 selected)

Wireless Network <00:02:6F:45:15:43> dialog box details:

- General tab selected
- Frequency: 2432 MHz
- Band: 2.4GHz-B/G
- Address: 00:02:6F:45:15:43
- SSID: AP2G
- Of Freq.: 12.8 %
- Of Traf.: 83.4 %
- Bandwidth: 3.7 Mbps
- Stations: 2
- SSID source: beacon
- Supported Rates: 1Mbps 2Mbps 5.5Mbps...
- Basic Rates: 1Mbps 2Mbps 5.5Mbps...
- Capabilities: ess short-preamble

Packet Sniffer and Spectral Scan

Packet Sniffer is used to sniff packets on the interface
Spectral scan is available via CLI or The Dude – gives a more accurate representation of wireless activity

Please note if any of the following is running then the wireless interface is disabled and cannot connect or allow connections:

- Scan tool
- Frequency Usage
- Snooper
- Sniffer
- Spectral Scan

***TIP**

802.11N

802.11n is a wireless mode designed to increase throughput with the same amount of wireless spectrum (bandwidth)

It is only supported on Atheros 802.11N wireless cards

- Can run on 2.4 or 5 Ghz depending on card

You need to be running ROS 4 or later to support N cards

- License needs to be upgraded if moving from ROS3

Enabled by setting Wireless Band to an N-enabled mode (N-only or A/N for compatibility)

HT chains

- Are antennas for one radio
- Used for 802.11n and is a factor in throughput

802.11n

LAB

Set your country setting to South Africa on Wlan2

The trainer will assign frequencies for each AP

With the AP on 802.11 run a bandwidth test between your 172.16.y IP addresses (i.e. test Wlan2 performance)

Change the AP to 5Ghz-N-only

Set your protocol to 802.11

- You may need to use wlan1 if you do not have 2 N cards on your router

Run a bandwidth test

Note the results

802.11AC

IEEE 802.11ac is a wireless networking standard in the 802.11 family providing high-throughput wireless local area networks (WLANs) on the 5 GHz band

This specification has expected multi-station WLAN throughput of at least 1 gigabit per second and a single link throughput of at least 500 megabits per second

This is accomplished by extending the air interface concepts embraced by 802.11n:

- wider RF bandwidth (up to 160 MHz)
- more MIMO spatial streams (up to eight)
- downlink multi-user MIMO (up to four clients)
- high-density modulation (up to 256-QAM)

MikroTik 802.11AC

Only supported on 802.11AC chipsets

Current configurations support up to 3 spatial streams at up to 80MHz bandwidth

Bandwidth	20 MHz	40 MHz	80 MHz	160 MHz
# of Spatial Streams				
1	86.7 Mbps	200 Mbps	433.3 Mbps	866.7 Mbps
2	173.3 Mbps	400 Mbps	866.7 Mbps	1733 Mbps
3	288.9 Mbps	600 Mbps	1300 Mbps	2340 Mbps
4	346.7 Mbps	800 Mbps	1733 Mbps	3466 Mbps
5	433.3 Mbps	1000 Mbps	2166 Mbps	4333 Mbps
6	577.8 Mbps	1200 Mbps	2340 Mbps	5200 Mbps
7	606.7 Mbps	1400 Mbps	3033 Mbps	6066.7 Mbps
8	693.3 Mbps	1600 Mbps	3466 Mbps	6933 Mbps

Nstreme Version 2

Nv2 protocol is a proprietary wireless protocol developed by MikroTik for use with Atheros 802.11 wireless chips

- Cannot be used with other TDMA systems such as Ubiquiti Airmax or Motorola Canopy
- only devices supporting Nv2 can participate in a Nv2 network

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.

Enabling Nv2

Nv2 is supported on ROS4.13 onward via the dedicated NV2 package

- Use **System > Packages** to enable / disable

ROS5.x supports NV2 natively

Once enabled you control it under the Wireless tab in **Interface > Wireless**

On the AP set the Wireless Protocol to: nv2

On the client set Wireless Protocol to: nv2 nstreme 802.11

- This allows the client to be backward compatible with previous versions of wireless

Nv2

The word "LAB" is written in large, blue, 3D block letters with a reflection effect below it.

Change your AP mode to Nv2 without N-mode

Do a bandwidth test

Note the results

Try NV2 with N-mode

Do a bandwidth test

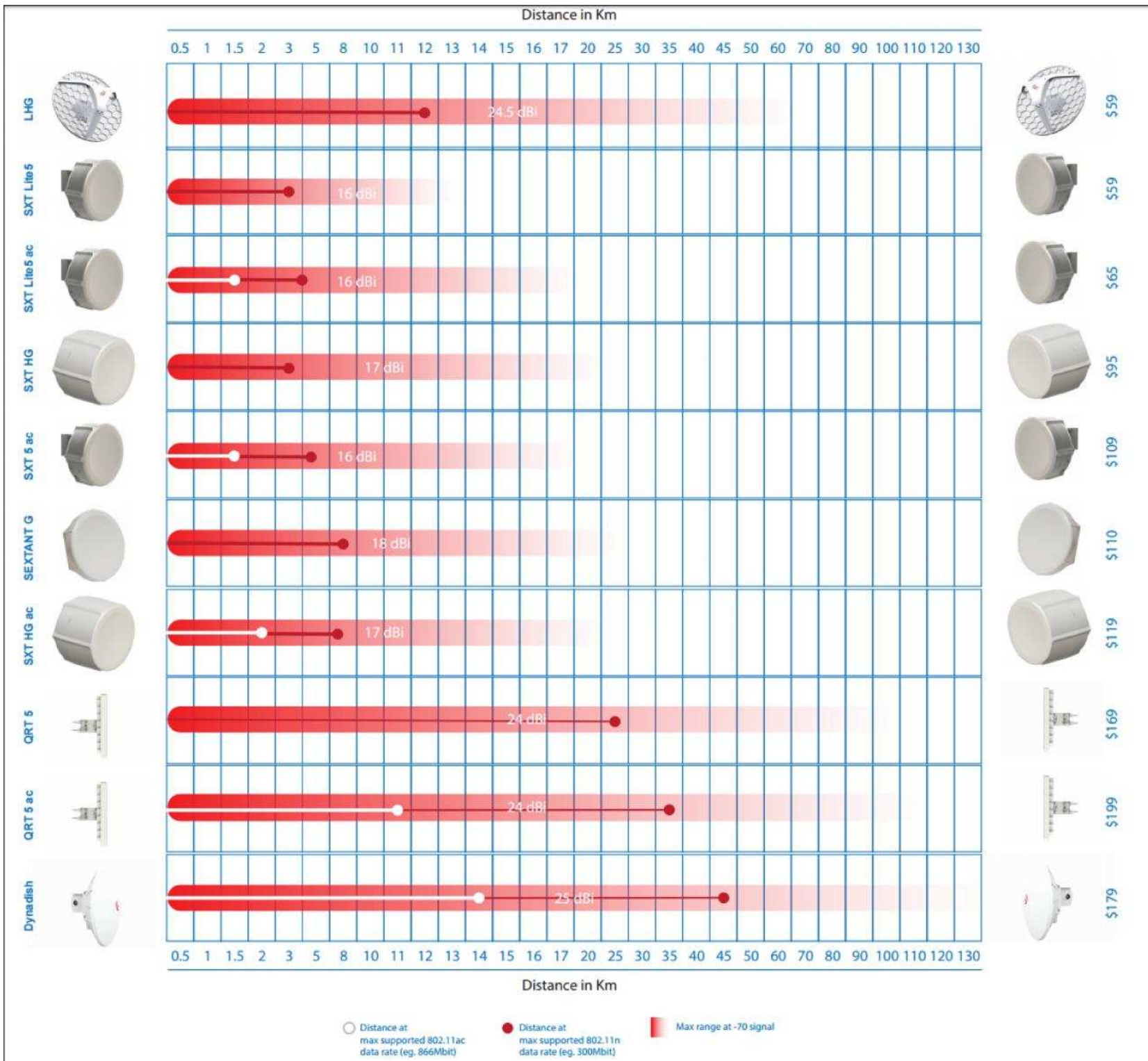
Note the results

MikroTik Product Selection

To help you choose the best product for your needs, we have created a selection guide, based on the theoretical distance each product can achieve at its maximum speed, and at its minimum data rate.

This table shows you how far can you reach depending on whether your priority is absolute distance, or maximum data rate.

The white dot shows distance when at the maximum 802.11ac data rate, the red dot shows the distance when at the maximum 802.11n data rate, and the red bar shows approximate maximum distance while at a signal of -70, which is still acceptable, but the data rate nears the lowest.



Distance at max supported 802.11ac data rate (eg. 866Mbit)
 Distance at max supported 802.11n data rate (eg. 300Mbit)
 Max range at -70 signal

Bandwidth Management

Simple Queues

Bursting

Speed Limiting

- Direct control over the data rate of inbound traffic is impossible
- The router controls the data rate indirectly by dropping incoming packets
 - TCP protocol adapts itself to the effective connection speed
- Simple Queues are the easiest way to limit data rate
- Simple queues make data rate limitation easy. One can limit:
 - Client's rx rate (client's download)
 - Client's tx rate (client's upload)
 - Client's tx + rx rate (client's aggregate)
- While being easy to configure, Simple Queues give control over all QoS features

Basic Limitation

To create a basic limitation, specify at least a target address and upload/download limitation

Target address can be the following:

- 0.0.0.0/0 – default target all
- Single IP Address
- IP Subnet
- Interface name (selected from dropdown)

Several IP's / Subnets / Interfaces can be selected in the same rule

Simple Limitation

The image shows the Mikrotik WinBox interface. On the left is a sidebar menu with 'Queues' highlighted. The main window displays the 'Queue List' with a table containing one entry: 'limit wlan' with a target of '10.2.34.0/24' and upload/download limits of '100M'. A dialog box titled 'Simple Queue <limit wlan>' is open, showing configuration details. Red circles and arrows highlight specific fields in the dialog: the 'Name' field, the 'Target' field, the 'Max Limit' fields, and the 'Burst' section.

#	Name	Target	Upload Max Limit	Download Max Limit	Packet Marks	Total Max Limit (bi...
1	limit wlan	10.2.34.0/24	100M	100M		

Who is going to be limited
Target Destination

Limitation to apply

Burst Settings

Simple Queue

LAB

Restore backup-*your_name*-ROUTED

Create a queue to limit your laptop's upload and download data rate to 64Kbps/128Kbps

Verify the limits are working

Make a second queue underneath the first one to limit to 32Kbps/32Kbps

- Which queue has precedence?
- Re-order the queues and test again

Add a queue to provide unlimited speed to your router from your laptop

- How do you specify a destination address?

More Queue Settings

Dst address allows you to specify an ip to limit data to e.g. to limit access to a certain web server to a certain amount)

Time allows you to specify which times the queue is valid for

Priority is a number from 1-8 with 1 having highest priority

Packet mark allows protocol limits by using the firewall mangle facility

Interface applies the limit to a specified interface

Queue type controls how HTB manages data rate limitations

Queue colors in Winbox:

- 0% - 50% available traffic used - green
- 51% - 75% available traffic used - yellow
- 76% - 100% available traffic used - red

Burst

Burst is one of the means to ensure enhanced (better) QoS

Bursts are used to allow higher data rates (exceeding the max-rate) for a short period of time

Bursts can give clients the impression of a higher speed service and a better browsing experience while still limiting data rates on bigger downloads

To calculate burst you need to know the average data rate (calculated over a burst-time period) and how it relates to the burst threshold

Average Data Rate

Average data rate is calculated as follows:

- **burst-time** is being divided into 16 periods
- router calculates the **average data rate** of each class over these small periods

Note, that the **actual burst period** is not equal to the burst-time. It can be several times shorter than the burst-time depending on the max-limit, burst-limit, burst-threshold, and actual data rate history (see the graph example on the next slide)

To work out actual time from zero rate use the formula
$$\text{actual_time} = \text{burst_time} / (\text{burst_limit} / \text{burst_threshold})$$

Limitation with Burst

The image shows the RouterOS WinBox interface. On the left is a vertical menu with the following items: Interfaces, Wireless, Bridge, PPP, IP, Routing, Ports, Queues, Drivers, System, Files, Log, SNMP, Users, Radius, Tools, New Terminal, Telnet, Password, Certificate, Make Supout.nif, Manual, and Exit. The 'Queues' menu item is circled in red. A red arrow points from this menu item to the 'Queue List' window. In the 'Queue List' window, the 'Simple Queues' tab is active. A red circle highlights a '+' button in the toolbar. Another red arrow points from this button to the 'New Simple Queue' dialog box. The 'New Simple Queue' dialog has several tabs: General, Advanced, Statistics, Traffic, Total, and Total Statistics. The 'General' tab is selected. It contains the following fields:

- Name: laptop_queue
- Target Address: 192.168.XY.1
- Target Upload: (64k bits/s)
- Target Download: (128k bits/s)
- Burst Limit: 128k (bits/s)
- Burst Threshold: 32k (bits/s)
- Burst Time: 20 (s)

The 'Burst' section is circled in red. At the bottom of the dialog, there is a 'disabled' status indicator.

Burst Exercise



Limit your laptop's upload/download

- max-limit to 1024k/1024k (1M/1M)
- burst-limit up to 2048k/2048k (2M/2M)
- burst-threshold 512Kbps/512Kbps
- burst-time 60 seconds

Calculate the expected burst time and check the result

Change the burst limit to 10M/10M and compare the results

Change burst-threshold to 5M/5M - compare the results

Change burst-threshold to 128Kbps/128Kbps and burst time to 120 seconds - compare the results

Queue Types

Bandwidth Management (Queues)

- FIFO (PFIFO and BFIFO) is a basic First-in First-out queue type
- PCQ (Per Connection Queuing) provides equal sharing of bandwidth with the ability to specify limitations on a per client basis
- SFQ (Stochastic Fairness Queuing) uses a round robin algorithm to balance the flows of traffic through the queue
- RED (Random Early Drop) is a queuing mechanism which tries to avoid network congestion by controlling the average queue size

Queue Tree is an advanced queue method that needs mangle rules to work, otherwise it works like a simple queue

Per Connection Queuing

PCQ is used to optimize massive QoS systems where most of the queues are exactly the same only for different sub-streams.

The PCQ algorithm is simple

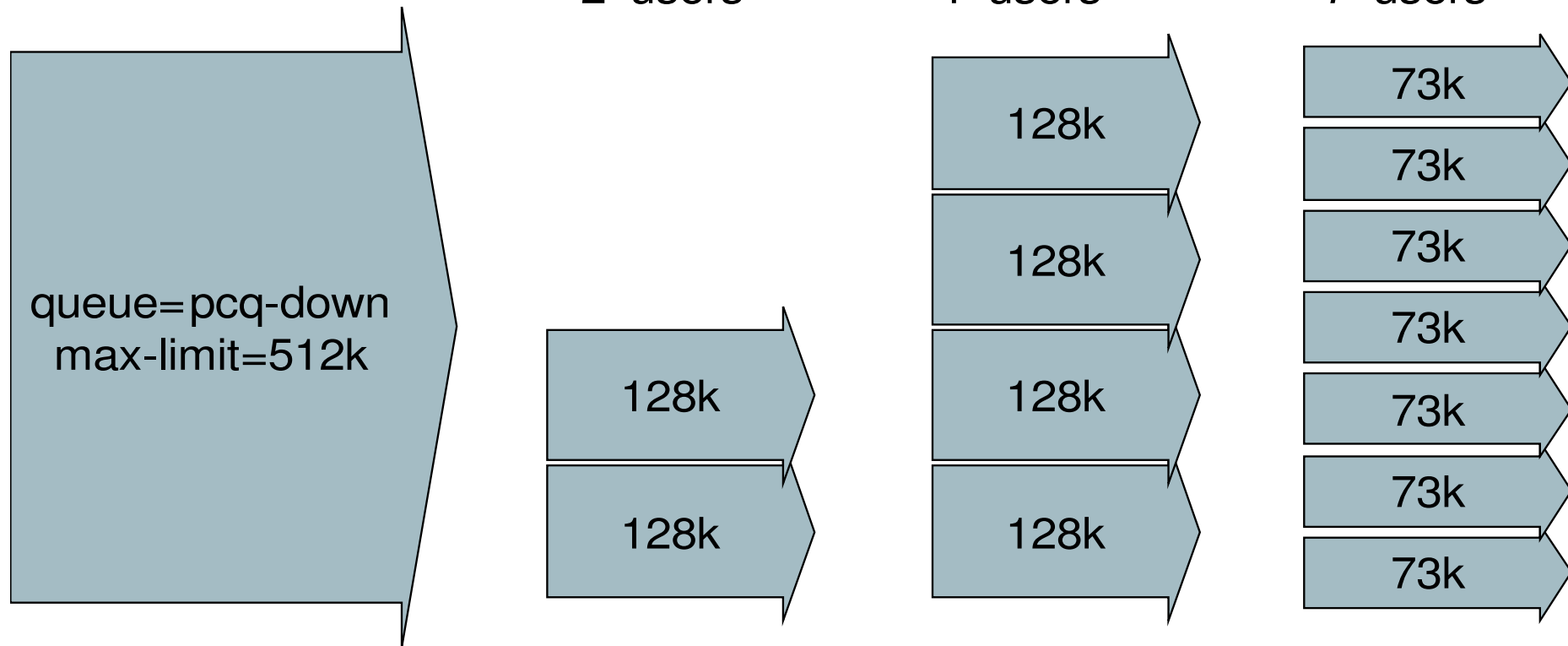
- first it uses selected classifiers to distinguish one sub-stream from another
- then it applies an identical individual FIFO queue size and limitation on every sub-stream
- then it groups all sub-streams together and applies a global FIFO queue size and limitation.

PCQ parameters:

- **pcq-classifier** (dst-address | dst-port | src-address | src-port; : selection of sub-stream identifiers
- **pcq-rate** (number) : maximal available data rate of each sub-stream
- **pcq-limit** (number) : queue size of one sub-stream in packets
- **pcq-total-limit** (number) : queue size of global FIFO queue

PCQ in Action – hard rate limit

- `pcq-rate=128000`



Set pcq-rate to a number to balance all flows in the queue and limit each flow to a set rate

- Each flow can get up to set rate if there is enough total bandwidth

Set classifier – dst-address for download queue, src-address for upload queue

The image shows two screenshots from Mikrotik WinBox. The top screenshot is the 'Queue List' window, with the 'Queue Types' tab selected. A red box highlights the '+' button in the top-left corner of the list. A red arrow points from this button to the 'New Queue Type' dialog box below. The bottom screenshot shows two 'New Queue Type' dialog boxes side-by-side. The left dialog is for 'pcq-download' and the right is for 'pcq-upload'. In both, the 'Rate' field is set to '128k' and is highlighted with a red box. In the 'pcq-download' dialog, the 'Classifier' section has 'Dst. Address' checked and highlighted with a red box. In the 'pcq-upload' dialog, 'Src. Address' is checked and highlighted with a red box. Both dialogs also show 'Kind' set to 'pcq', 'Limit' set to '50', and 'Total Limit' set to '2000'.

Type Name	Kind
default	pfifo
ethernet-default	pfifo
wireless-default	sfq
synchronous-default	red
hotspot-default	sfq
default-small	pfifo

New Queue Type: pcq-download

Type Name: pcq-download
Kind: pcq
Rate: 128k
Limit: 50
Total Limit: 2000

Burst Rate: []
Burst Threshold: []
Burst Time: 00:00:10

Classifier:
 Src. Address Dst. Address
 Src. Port Dst. Port

Src. Address Mask: 32
Dst. Address Mask: 32
Src. Address6 Mask: 64
Dst. Address6 Mask: 64

New Queue Type: pcq-upload

Type Name: pcq-upload
Kind: pcq
Rate: 128k
Limit: 50
Total Limit: 2000

Burst Rate: []
Burst Threshold: []
Burst Time: 00:00:10

Classifier:
 Src. Address Dst. Address
 Src. Port Dst. Port

Src. Address Mask: 32
Dst. Address Mask: 32
Src. Address6 Mask: 64
Dst. Address6 Mask: 64

PCQ example

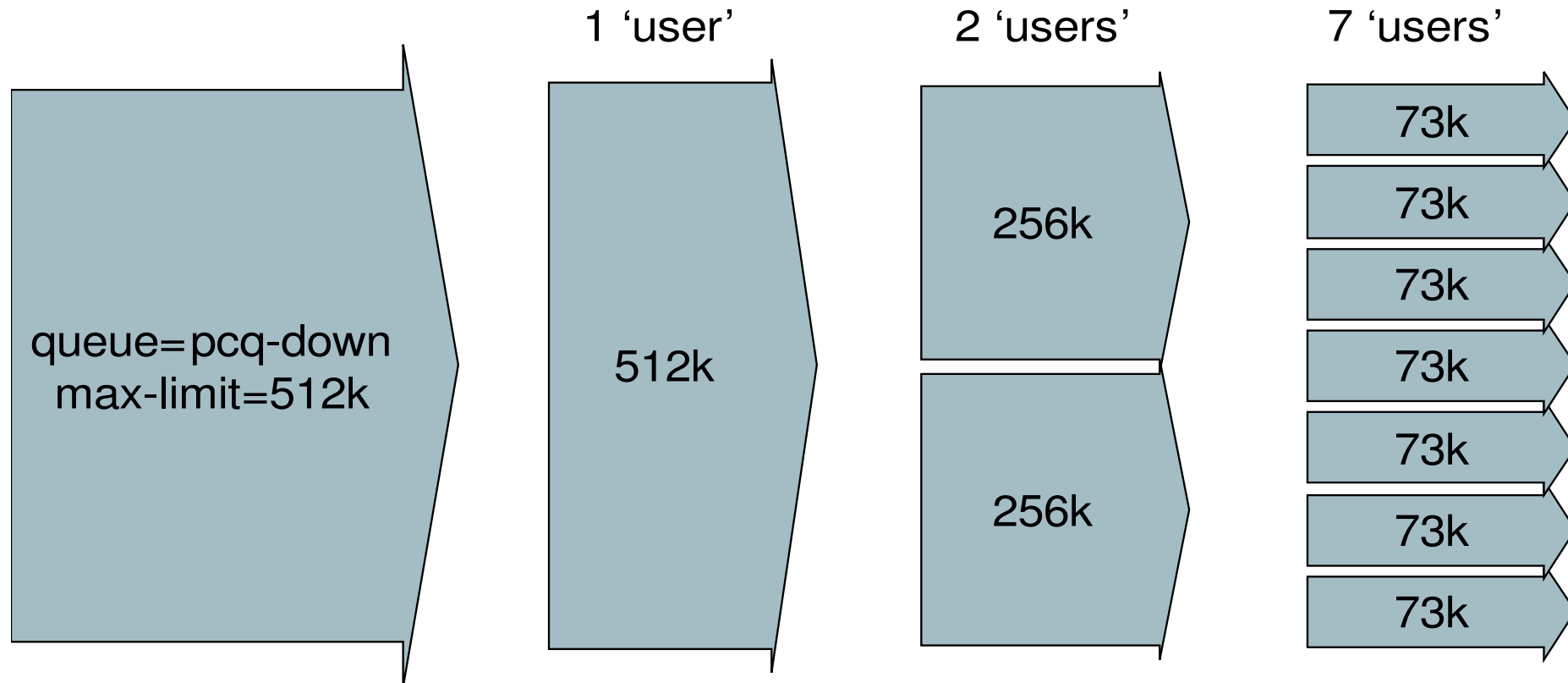
If 'limit-at' and 'max-limit' are set to '0', then the subqueues can take up all bandwidth available for the parent

Set the PCQ Rate to '0', if you do not want to limit subqueues, i.e, they can use the bandwidth up to 'max-limit', if available

Set the PCQ Rate to <number> to hard limit each subqueue to a specified amount

PCQ in Action – soft rate limit

pcq-rate=0



Set pcq-rate to zero to balance all flows in the queue without limiting individual flows

- Each flow can get up to total limit of queue

Set classifier – dst-address for download queue, src-address for upload queue

The image shows a screenshot of the Mikrotik WinBox interface. At the top, the 'Queue List' window is open, showing a table of queue types. A red box highlights the '+' icon in the top-left corner of the table, and a red arrow points from it to the 'New Queue Type' dialog box below. The 'Queue List' window has tabs for 'Simple Queues', 'Interface Queues', 'Queue Tree', and 'Queue Types', with 'Queue Types' selected. The table lists several queue types with their respective kinds: default (pfifo), ethernet-default (pfifo), wireless-default (sfq), synchronous-default (red), hotspot-default (sfq), and default-small (pfifo). Below the 'Queue List' are two 'New Queue Type' dialog boxes. The left dialog is for 'pcq-download' and the right is for 'pcq-upload'. Both dialogs have 'Rate' fields set to '0', which are highlighted with red boxes. In the 'pcq-download' dialog, the 'Classifier' section has 'Dst. Address' checked, also highlighted with a red box. In the 'pcq-upload' dialog, 'Src. Address' is checked, also highlighted with a red box. Both dialogs have 'Limit' set to 50 and 'Total Limit' set to 2000. The 'Burst Rate', 'Burst Threshold', and 'Burst Time' fields are also visible in both dialogs.

Type Name	Kind
default	pfifo
ethernet-default	pfifo
wireless-default	sfq
synchronous-default	red
hotspot-default	sfq
default-small	pfifo

New Queue Type: pcq-download

Type Name: pcq-download
Kind: pcq
Rate: 0
Limit: 50
Total Limit: 2000
Burst Rate:
Burst Threshold:
Burst Time: 00:00:10
Classifier:
 Src. Address Dst. Address
 Src. Port Dst. Port
Src. Address Mask: 32
Dst. Address Mask: 32
Src. Address6 Mask: 64
Dst. Address6 Mask: 64

New Queue Type: pcq-upload

Type Name: pcq-upload
Kind: pcq
Rate: 0
Limit: 50
Total Limit: 2000
Burst Rate:
Burst Threshold:
Burst Time: 00:00:10
Classifier:
 Src. Address Dst. Address
 Src. Port Dst. Port
Src. Address Mask: 32
Dst. Address Mask: 32
Src. Address6 Mask: 64
Dst. Address6 Mask: 64

Applying the Queue Type

The image shows a screenshot of the Mikrotik WinBox interface, specifically the Queue List and configuration windows. The Queue List window is at the top, showing a table with columns: Name, Parent, Packet ..., Limit At (b..., Max Limit ..., Avg. R..., Queued Bytes, Bytes, and Packets. Below the table are tabs for Simple Queues, Interface Queues, Queue Tree, and Queue Types. A red arrow points from the Queue Types tab to the 'New Queue' dialog box. Another red arrow points from the Queue List table area to the 'Advanced' tab of the 'New Simple Queue' dialog box.

The 'New Simple Queue' dialog box (bottom left) has tabs for General, Advanced, Statistics, Traffic, Total, and Total Statistics. The 'Advanced' tab is selected. The 'Queue Type' dropdown is set to 'pcq-upload' and is highlighted with a red box. Other fields include P2P, Packet Marks, Dst. Address, Interface (all), Target Upload/Download (unlimited), Parent (none), and Priority (8).

The 'New Queue' dialog box (bottom right) has tabs for General and Statistics. The 'General' tab is selected. The 'Name' field is 'master_in' and the 'Parent' dropdown is 'global-in', both highlighted with red boxes. The 'Queue Type' dropdown is set to 'pcq-upload' and is also highlighted with a red box. Other fields include Packet Marks, Priority (8), Limit At, Max Limit, Burst Limit, Burst Threshold, and Burst Time.

VPN

Virtual Private Networks

EoIP, VLAN

PPTP, L2TP

PPPoE

VPN Benefits

A **virtual private network (VPN)** is a computer network in which some of the links between nodes are carried by open connections or virtual circuits in some larger network (e.g. the Internet) as opposed to running across a single private network.

The link-layer protocols of the virtual network are said to be tunneled through the larger network.

One common application sets up secure communications through the public Internet, but a VPN needs not have explicit security features, such as authentication or content encryption.

Corporate resources (e-mail, servers, printers) can be accessed securely by users having granted access rights from outside (home, while travelling, etc.)

Point-to-Point protocol tunnels

Capable of authentication and data encryption

- Authentication allows accurate mapping of data usage to a user account
- Encryption secures the link against network sniffing

Such tunnels are:

- PPPoE (Point-to-Point Protocol over Ethernet)
- PPTP (Point-to-Point Tunnelling Protocol)
- L2TP (Layer 2 Tunnelling Protocol)
- SSTP (Secure Socket Tunnelling Protocol)

PPTP and L2TP Tunnels

PPTP uses TCP port 1723 and IP protocol 47/GRE

MikroTik includes support for a PPTP Client and Server

Level 4 License supports up to 200 ppp type sessions

PPTP clients are available for and included in almost every OS

PPTP and L2TP have mostly the same functionality

L2TP traffic uses UDP port 1701 only for link establishment,
further traffic is using any available UDP port

Configuration of both tunnels are identical in RouterOS

PPTP Client



Restore from backup `backup-your_name-WIRELESS`

- Disable your default route

Create a PPTP client

- Server Address:10.1.1.254
- User: class
- Password: class
- Add default route = yes

Add a masquerade rule to masquerade out **all ppp** interfaces

Do you still have internet access? Check the log for troubleshooting problem connections

Check your IP address and Default Gateway setting

Disable the PPTP interface, enable your default route and attempt to create a PPTP connection from your laptop

- Does it operate as expected?

SSTP

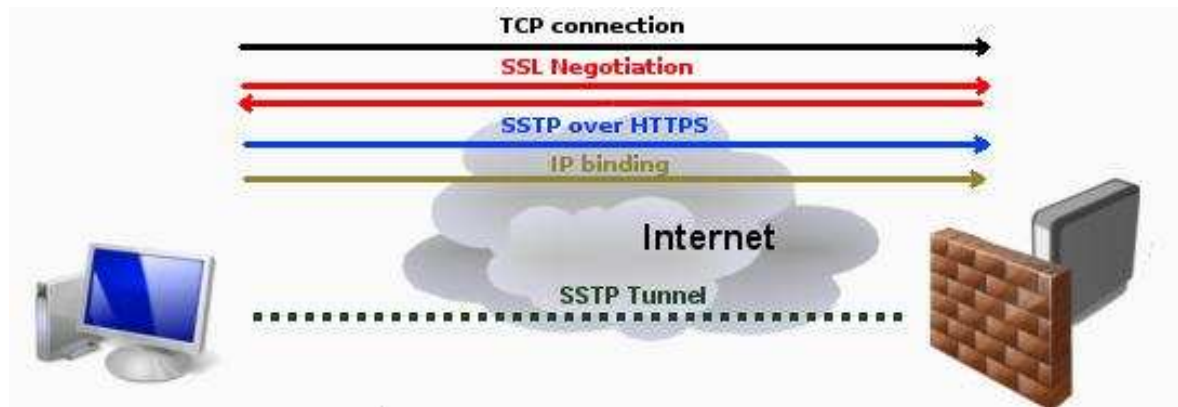
Secure Socket Tunneling Protocol (SSTP) is a way to transport PPP tunnels over a SSL 3.0 channel.

The use of SSL over TCP port 443 allows SSTP to pass through virtually all firewalls and proxy servers.

- Useful if your ISP is blocking standard tunnelling type protocols

If both client and server are MikroTik routers, then it is possible to establish SSTP tunnel without certificates and with any available authentication type.

Otherwise to establish secure tunnels **mschap** authentication and client/server certificates from the same chain should be used.



PPPoE tunnels

PPPoE works in OSI 2nd (data link) layer

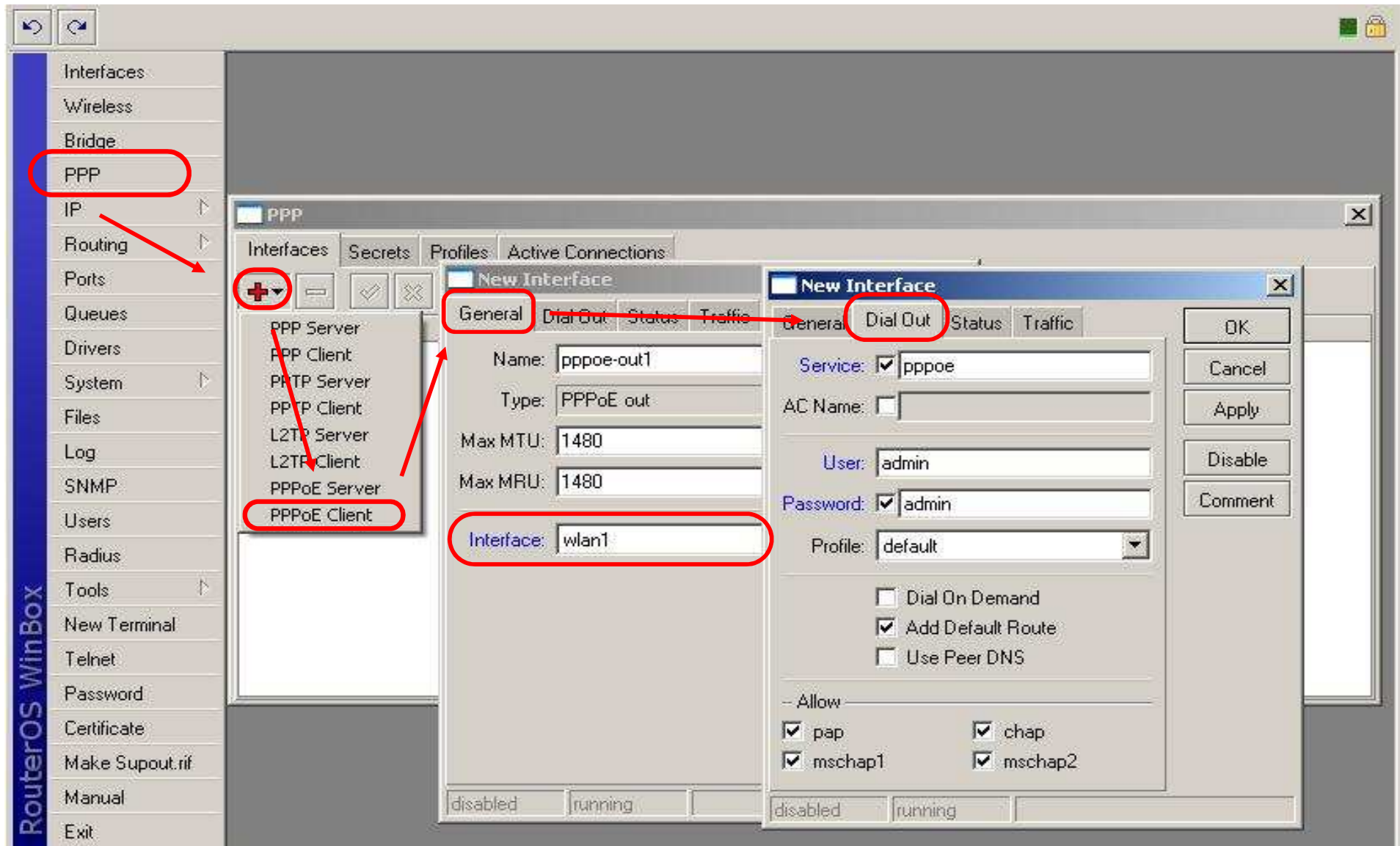
- it is not a routed protocol
- Clients must be directly connected to the server
- PPPoE is used to hand out IP addresses to clients based on the user authentication
- It's like a secure version of DHCP that includes accounting
- It is a tool for ISP's to manage and account clients

PPPoE requires a dedicated access concentrator (server), which PPPoE clients connect to.

Most operating systems have PPPoE client software

PPPoE is the most commonly used method for client IP assignement and bandwidth management

PPPoE client



PPPoE Client

The logo consists of the letters 'LAB' in a bold, blue, 3D-style font. The letters are slightly shadowed and have a reflection effect below them, giving them a metallic or glossy appearance.

Remove your Wlan IP address and the default route (disable DHCP Client)

Create a PPPoE client

- Interface: wlan1
- User: class
- Password: class
- Add default route = yes

Check the log to troubleshoot your connection

Check your PPPoE connection

- Is the interface enabled?
- Is it “connected” and running (R)?
- Is there a dynamic (D) IP address assigned to the pppoe client interface in the IP Address list?
- What are the netmask and the network address?
- What routes do you have on the pppoe client interface?

PPPoE with Encryption

LAB

The PPPoE access concentrator is changed to use encryption

You should use encryption, either:

- change the ppp profile used for the pppoe client to default-encryption
- modify the ppp profile used for the pppoe client to use encryption

See if you get the pppoe connection running

- Check the connections on the trainer router
- Is it showing an encryption method?

Point-to-point Addressing

Point-to-point addressing utilizes only two IPs per link while /30 utilizes four IPs

There is no broadcast address, but the network address must be set manually to the opposite IP address.

Example:

Router1: address=1.1.1.1/32, network=2.2.2.2

Router2: address=2.2.2.2/32, network=1.1.1.1

There can be identical /32 addresses on the router – each address will have different connected route (network value will be different)

This is the same as an “unnumbered” address on other systems

PPPoE/PPTP/L2TP Server Setup

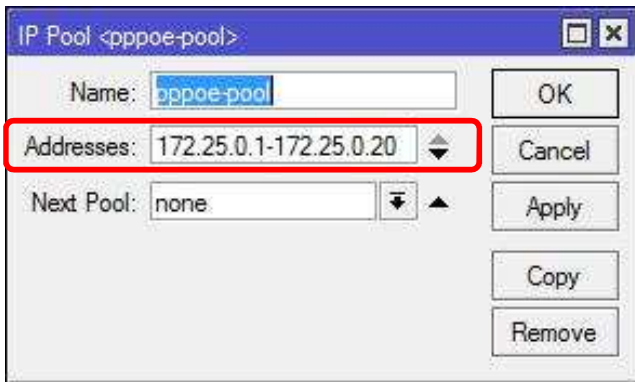
To setup a PPPoE/PPTP/L2TP server you require an IP pool to assign addresses, a modified PPP profile and a PPP Secret

The trainer will take you through setting up the server components step by step – restore from backup-wireless

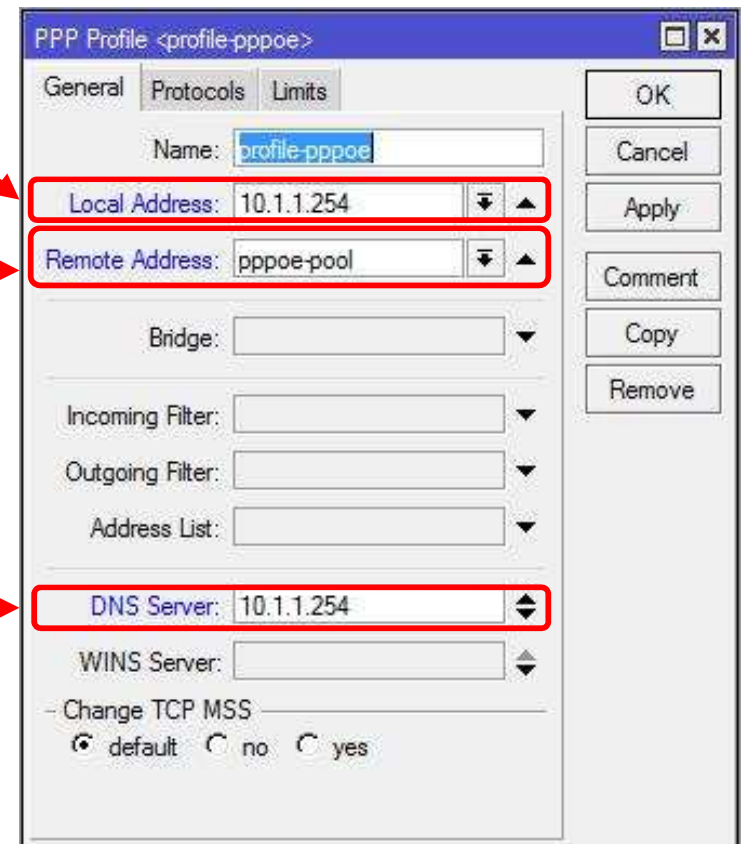
Local Address defines the routers end of the PPP tunnel

Remote Address defines the addresses give to clients

DNS Server indicates which DNS to hand to clients



Use IP→Pool to create a range of IP addresses to assign to clients



DNS Server: 10.1.1.254

PPP Secrets



PPP Secrets store usernames and passwords that can be used by any VPN service

You can assign a secret to a specific protocol or to all protocols

- It's 1 or everything, you cannot be selective

PPP Secrets are local to the router – they cannot be shared across routers

RADIUS can be used to create a centralized authentication system (e.g. MikroTik User Manager)

Adding a PPPoE Server

Under PPP→PPPoE Server you can add a new server

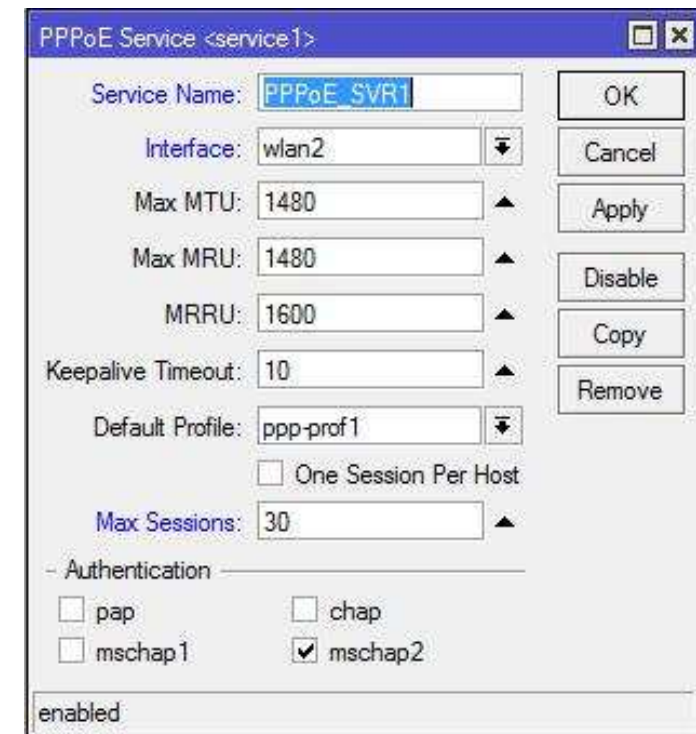
Define an interface and profile

Authentication methods:

- PAP, CHAP, MSCHAPv1, MSCHAPv2
- Only MSCHAPv2 needs to be supported

Specify One Session Per Host to limit
to only 1 dialup per secret

Max Sessions limits the total number
sessions the AC will support



PPPoE Service <service1>

Service Name: PPPoE SVR1

Interface: wlan2

Max MTU: 1480

Max MRU: 1480

MRRU: 1600

Keepalive Timeout: 10

Default Profile: ppp-prof1

One Session Per Host

Max Sessions: 30

Authentication

pap chap

mschap1 mschap2

enabled

PPPoE Server

LAB

Work in teams of 2 or 3

Add a PPPoE Pool, Profile and Secret according to the trainer walkthrough

Add a PPPoE Server to Wlan2 Interface on one side

On the other side disable Wlan1 and setup a PPPoE client on Wlan2

Modify masquerade settings to allow internet access



PPP Secret <ppp2>

Name:

Password:

Service:

Caller ID:

Profile:

Local Address:

Remote Address:

Routes:

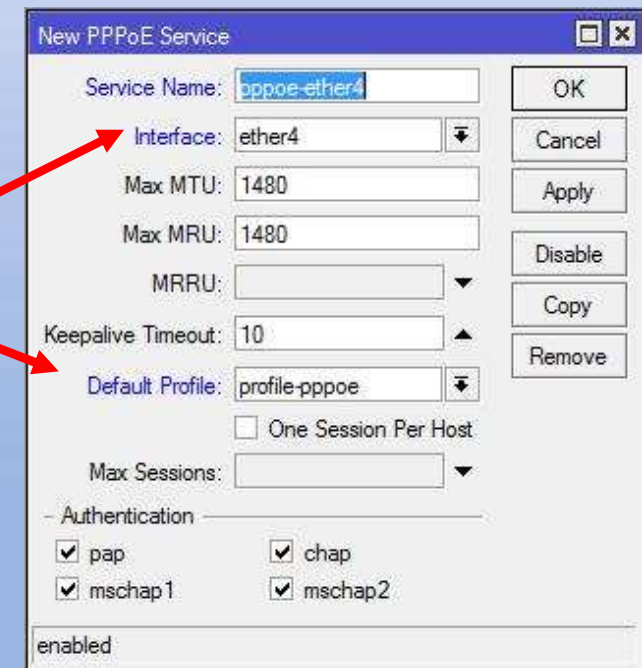
Limit Bytes In:

Limit Bytes Out:

enabled

Buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove

On the New PPPoE Service tab define at least the Interface and the correct Profile Name



New PPPoE Service

Service Name:

Interface:

Max MTU:

Max MRU:

MRRU:

Keepalive Timeout:

Default Profile:

One Session Per Host

Max Sessions:

Authentication

pap chap

mschap1 mschap2

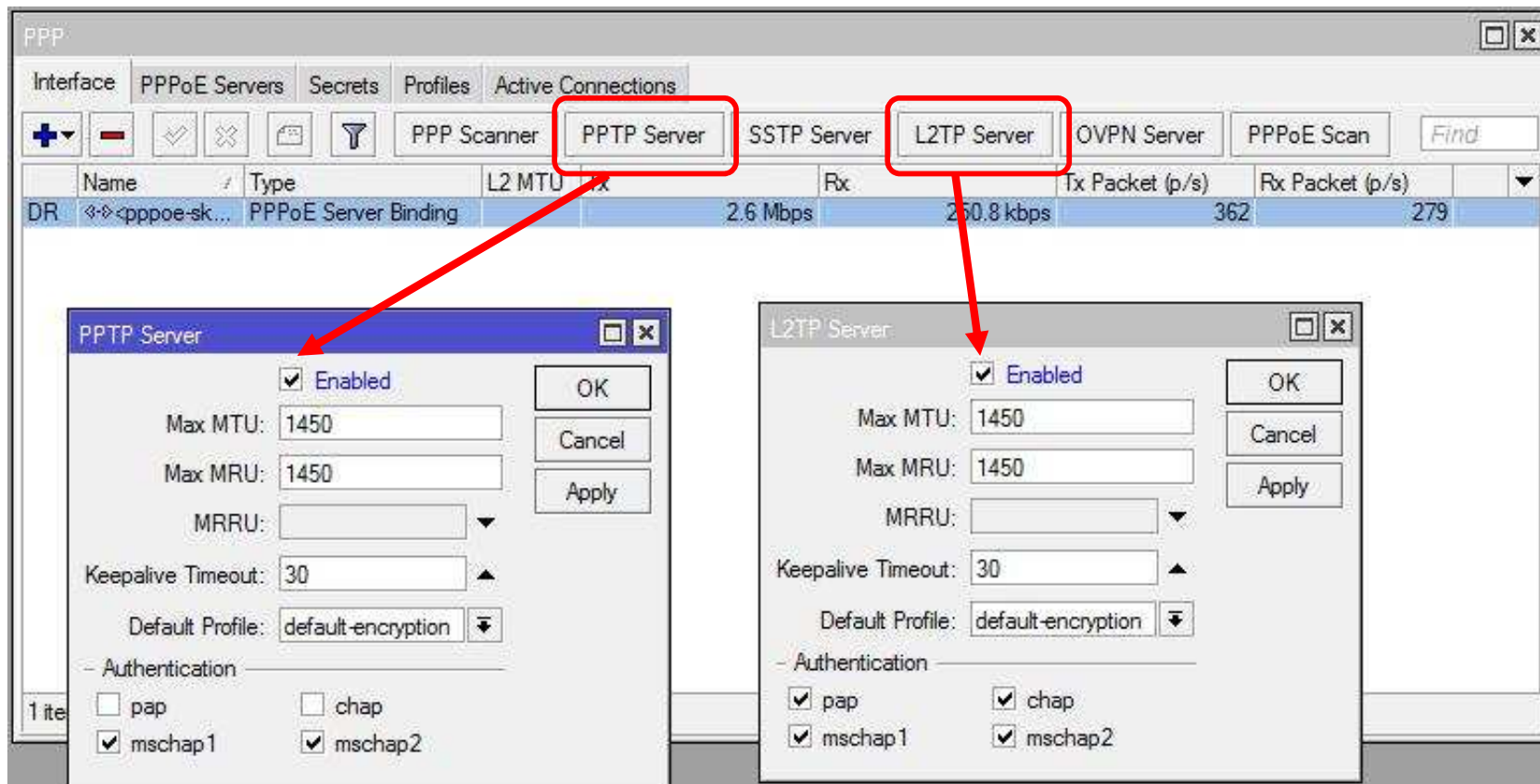
enabled

Buttons: OK, Cancel, Apply, Disable, Copy, Remove

Enabling a PPTP/L2TP/SSTP Server

To enable the PPTP, SSTP or L2TP servers you need to check the relevant box under PPP Interface

Make sure to select the correct profile

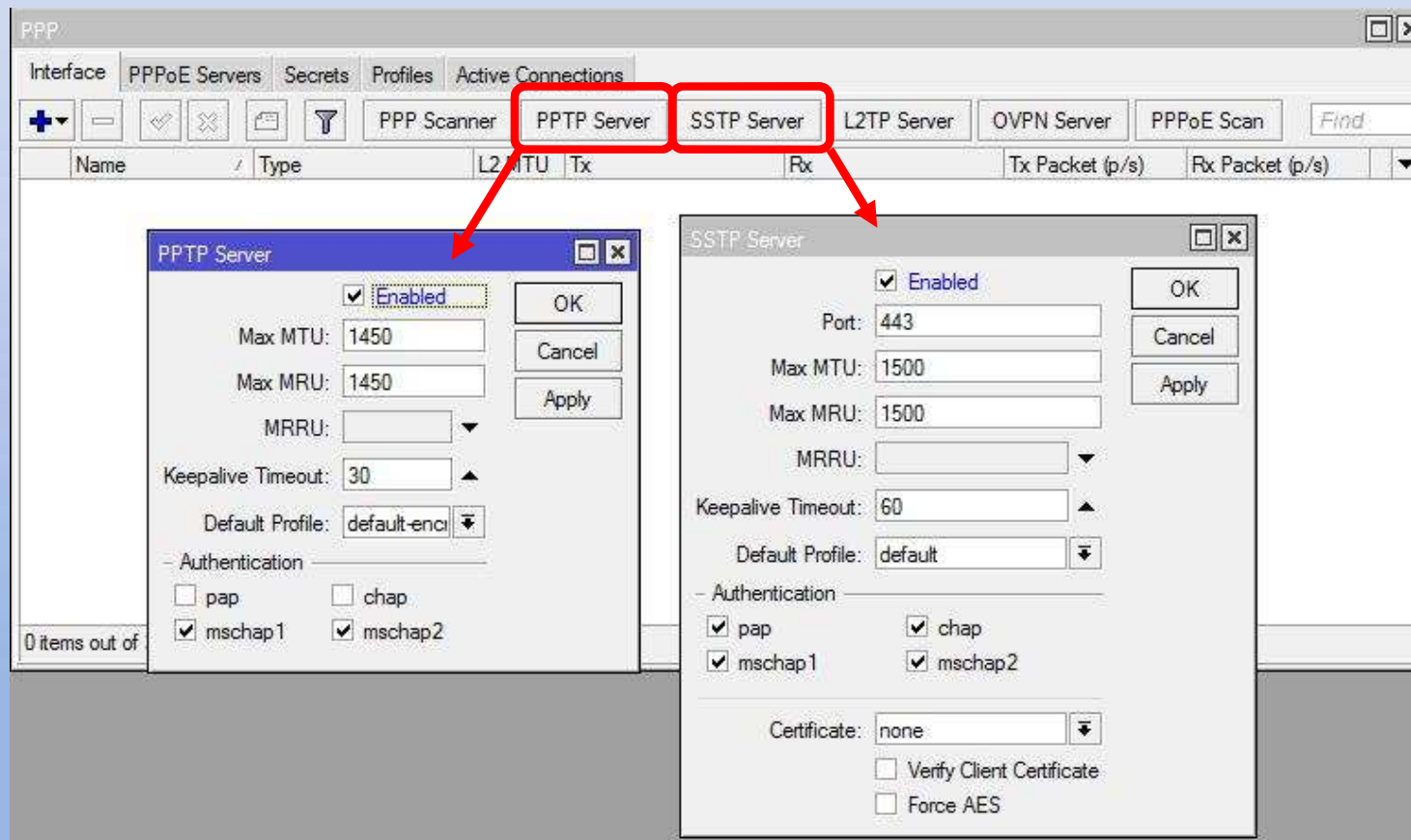


PPTP/SSTP Server

LAB

Under PPP → Interface enable the PPTP and SSTP servers using the profile created earlier

Create a PPTP/SSTP clients as appropriate and check the correct operation



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
```

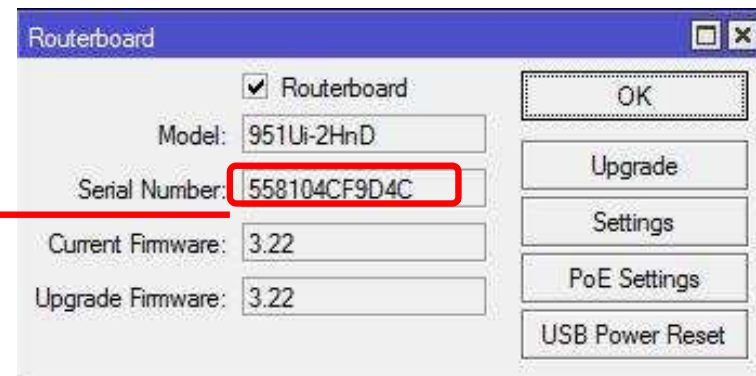
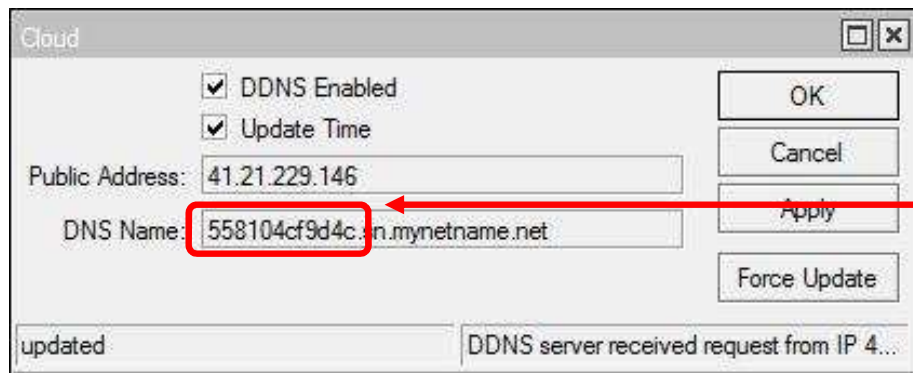
```
update-time: yes
```

```
public-address: 41.21.229.146
```

```
dns-name: 558104cf9d4c.sn.mynetname.net
```

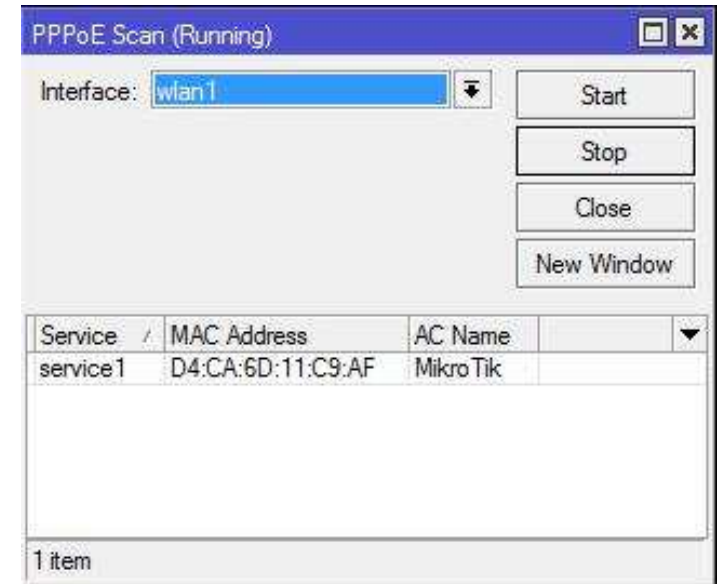
```
status: updated
```

```
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.
```



PPPoE Scanner

PPP → PPPoE Scan can be used to detect the presence of PPPoE Servers on a particular interface
Useful for troubleshooting connectivity issues for clients and determining if the layer2 setup is correct between client and server



Firewall

Packet filtering through the router

IP Firewalls

Network firewalls keep outside threats away from sensitive data available inside the network.

- When different networks are joined together, there is always a threat that someone from outside of your network will break into your LAN
- Such break-ins may result in private data being stolen and distributed, valuable data being altered or destroyed, or entire hard drives being erased.

Firewalls are used as a means of preventing or minimizing the security risks inherent in connecting to other networks.

- Properly configured firewalls play a key role in efficient and secure network infrastructure deployment.

Firewall Filters

The firewall implements packet filtering and thereby provides security functions that are used to manage data flow to, from and through the router.

Along with the Network Address Translation it serves as a tool for preventing unauthorized access to directly attached networks and the router itself as well as a filter for outgoing traffic.

Most firewall functions depend on the Connection Tracking table especially NAT rules



- Note that Connection-State \neq TCP state

You can use Firewall Address Lists to apply rules to sets of IP addresses

Firewall Filter Structure

The firewall operates by means of firewall rules

Each rule consists of two parts:

- the matcher which matches traffic flow against given conditions
- the action which defines what to do with the matched packet.

A Firewall Filter rule is an IF-THEN statement

IF <condition(s)> THEN <action>

Packets traverse rules in a definite order, from top to bottom

If a packet matches the condition(s) of a rule fully, then the specified action is performed on it. Otherwise, the next rule is evaluated

Firewall Filter Structure (cont.)

Firewall filter rules are organized in chains

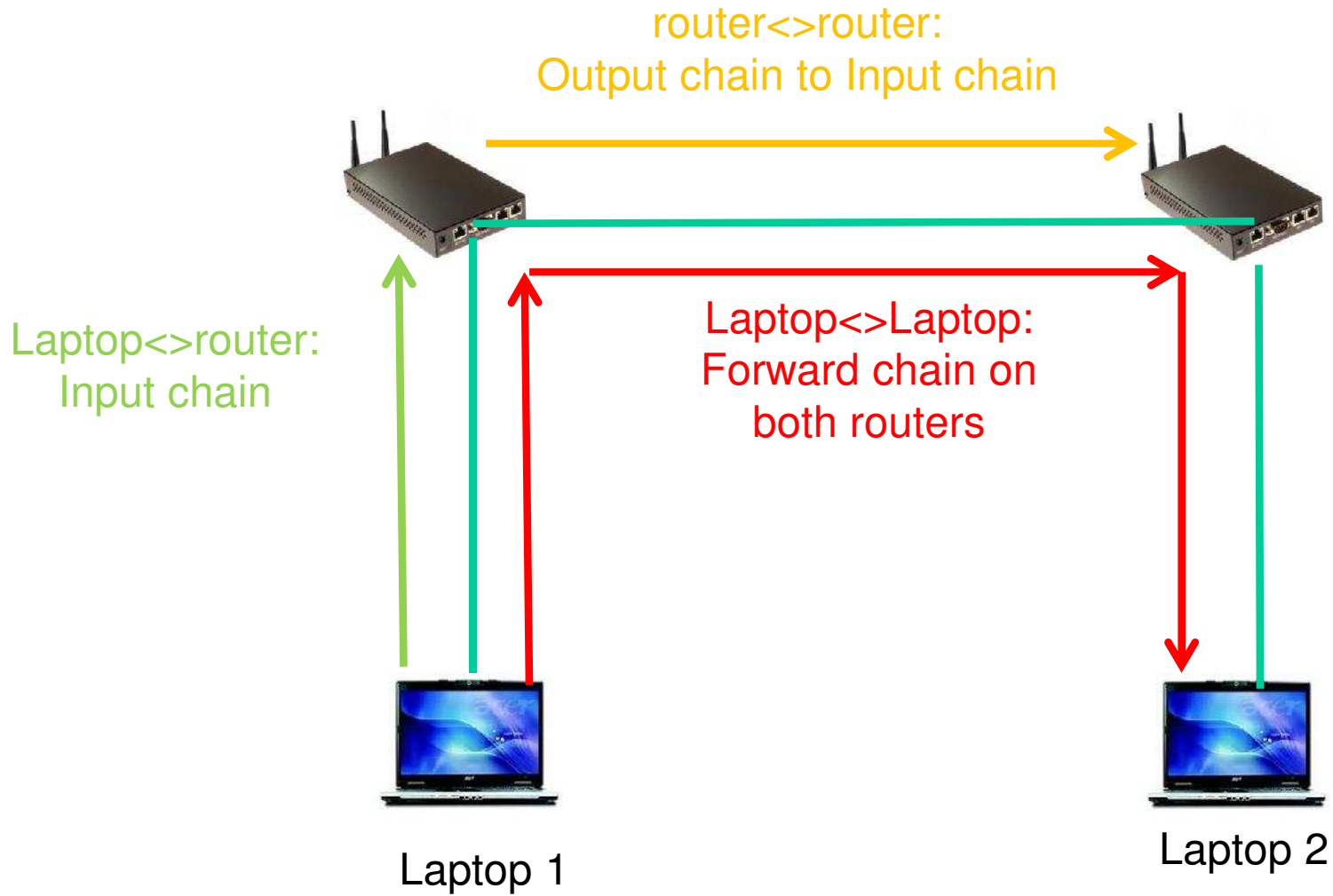
Chains are used to organize the firewall structure and to make processing more efficient

There are three built-in chains:

- input – processes packets addressed to the router (the **dst-address** is one of the routers addresses)
- output – processes packets originated by the router (the **src-address** is one of the routers addresses)
- forward – processes traffic flowing through the router (neither the src nor dst addresses belong to the router)

Generally the bulk of traffic will be passing through the forward chain

Filter Chains



Connection Tracking



Connection Tracking (or Conntrack) is the heart of the firewall

Connection tracking allows the kernel to keep track of all logical network connections or sessions and thereby relate all of the packets which may make up that connection

NAT relies on this information to translate all related packets in the same way

Iptables can use this information to act as a stateful firewall

The screenshot shows a window titled "Connection Tracking" with the following settings:

Enabled:	auto	OK
TCP Syn Sent Timeout:	00:00:05	Cancel
TCP Syn Received Timeout:	00:00:05	Apply
TCP Established Timeout:	1d 00:00:00	
TCP Fin Wait Timeout:	00:00:10	
TCP Close Wait Timeout:	00:00:10	
TCP Last Ack Timeout:	00:00:10	
TCP Time Wait:	00:00:10	
TCP Close:	00:00:10	
UDP Timeout:	00:00:10	
UDP Stream Timeout:	00:03:00	
ICMP Timeout:	00:00:10	
Generic Timeout:	00:10:00	
<input type="checkbox"/> TCP SynCookie		

Connection Tracking TIP

By disabling the conntrack system you will lose total functionality of the NAT system and some of the filter and mangle system

- Some filter and mangle rules can still operate if the matcher is not dependant on conntrack
- Any statefull type of rule will not work

Each conntrack table entry represents bidirectional data exchange

Conntrack takes a lot of CPU resources

- disable it, if you don't use any firewall functions on that router or
- Leave on auto to let the router decide when to enable (it will be enabled when a firewall filter, nat or mangle rule is added)

Firewall Basics

The General tab contains the standard operators for who the firewall rule is going to apply to

- It defines how the packet will be matched

Chain defines which chain is being processed

- The defaults are Input, Output and Forward

Src and Dst address defines whether the rule is coming from certain addresses or going to certain addresses

You can define the protocol and port for either src or dst port.

- Most of the time you would specify Dst. Port

P2P can be used to match Peer-to-Peer applications like Kazaa and Bit-torrent

- This uses Layer7 technology
- You should update the router frequently to get the latest matches

New Firewall Rule

General | Advanced | Extra | Action | Statistics

Chain: forward **Firewall Chain to traverse**

Src. Address: 41.210.2.4 **Where the packet comes from**

Dst. Address: 96.128.5.100 **Where the packet is going**

Protocol: 6 (tcp) **Protocol to match**

Src. Port:

Dst. Port: 80 **Port to match**

Any. Port:

P2P:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

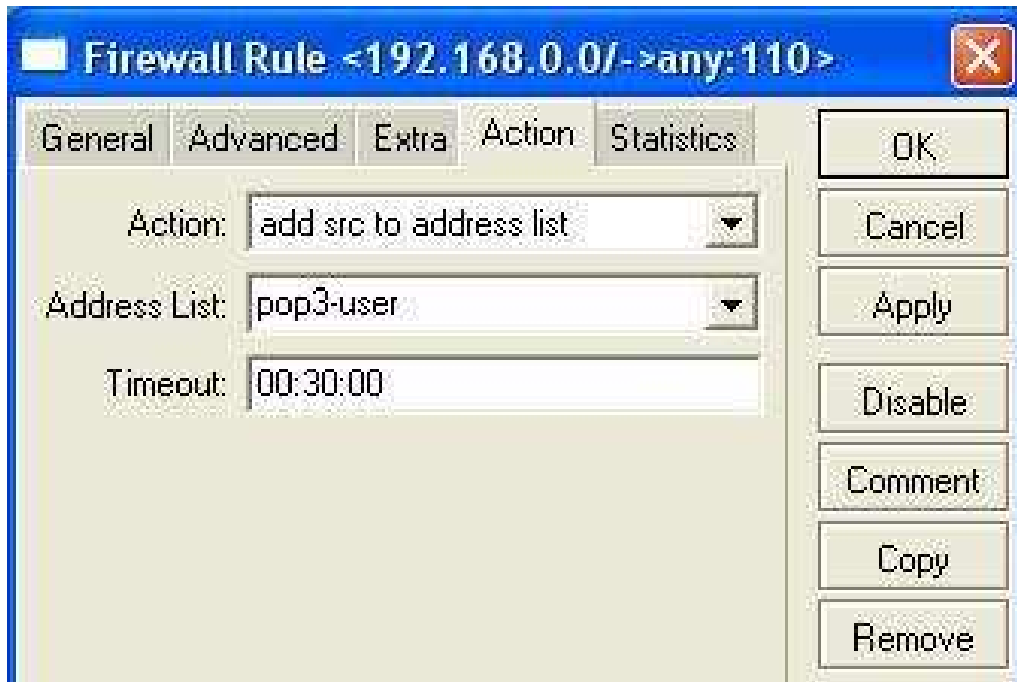
Connection State:

disabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

This rule will match all HTTP (tcp:80) packets coming from the IP: 41.210.2.4 and going to the IP: 96.128.5.100

Firewall Actions



Use the Action tab to specify what action to carry out on packets that are matched by the operators on the other tabs

Once the action is carried out no further Firewall processing occurs unless the action is Log or Passthrough

Firewall Filter Rule Actions

The most basic firewall filter rule actions are

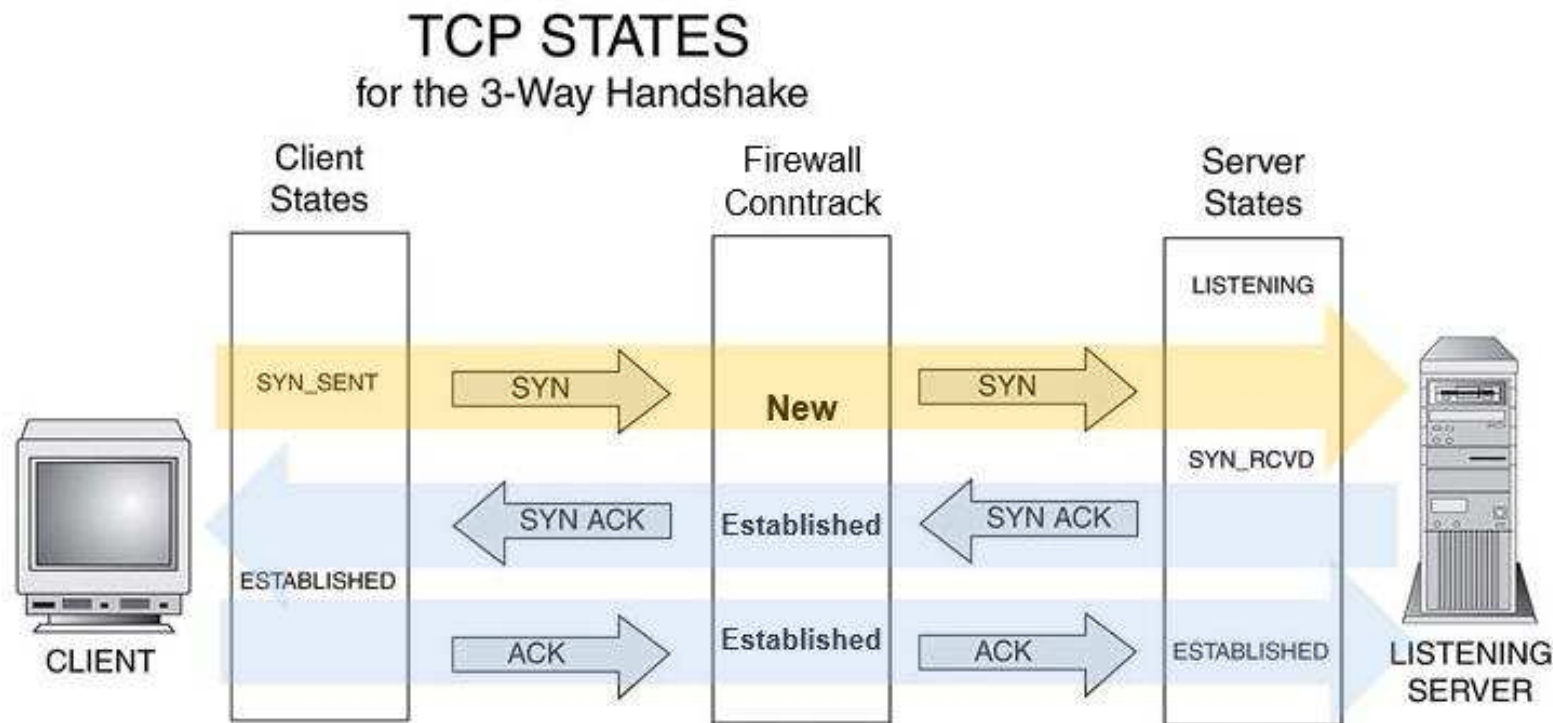
- **accept** – accept the packet by the firewall (usually used to bypass certain rules from certain IP's)
- **drop** – silently discard the packet
- **log** – log the packet and pass on to the next rule
- **passthrough** – Takes no action at all (used for byte counting)
- **reject** - drop the packet and send ICMP reject message

Other actions are

- **add src/dst to address list** – Create a dynamic address list for either source or destination IP
- **jump/return** – used to jump to and return from custom chains
- **tarpit** – used for DOS protection – send a reply to the requestor but drop the packet

TCP 3-way Handshake

Connection State – A state assigned to each packet as it gets evaluated by the Conntrack system



Condition: Connection State

A status assigned to each packet:

- New – packet is opening a new connection
- Established – packet belongs to already known connection
- Related – packet creates a new connection that is in some kind **related** to already known connection
- Invalid – packet does not belong to any of the known connections

Firewalls will generally consist of a number of rules to accept traffic and a rule to drop everything else

Connection state rules ensure that we can evaluate connections to and from the router, but not evaluate already established and related connection

First Rule Example

Firewall Rule

General | Advanced | Extra | Action | Statistics

Chain: input

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

P2P:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark:

Routing Mark:

Connection State: invalid

Connection Type:

disabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove

Firewall Rule

General | Advanced | Extra | Action | Statistics

Action: drop

Comment

OK
Cancel
Apply
Disable
Comment
Copy
Remove

disabled

Firewall SPI



Restore from backup-ROUTED

Add following rules to the “input” chain of firewall filter:

- Accept all packets with “Connection State” “established”
- Accept all packets with “Connection State” “related”
- Drop all packets with “Connection State” “invalid”

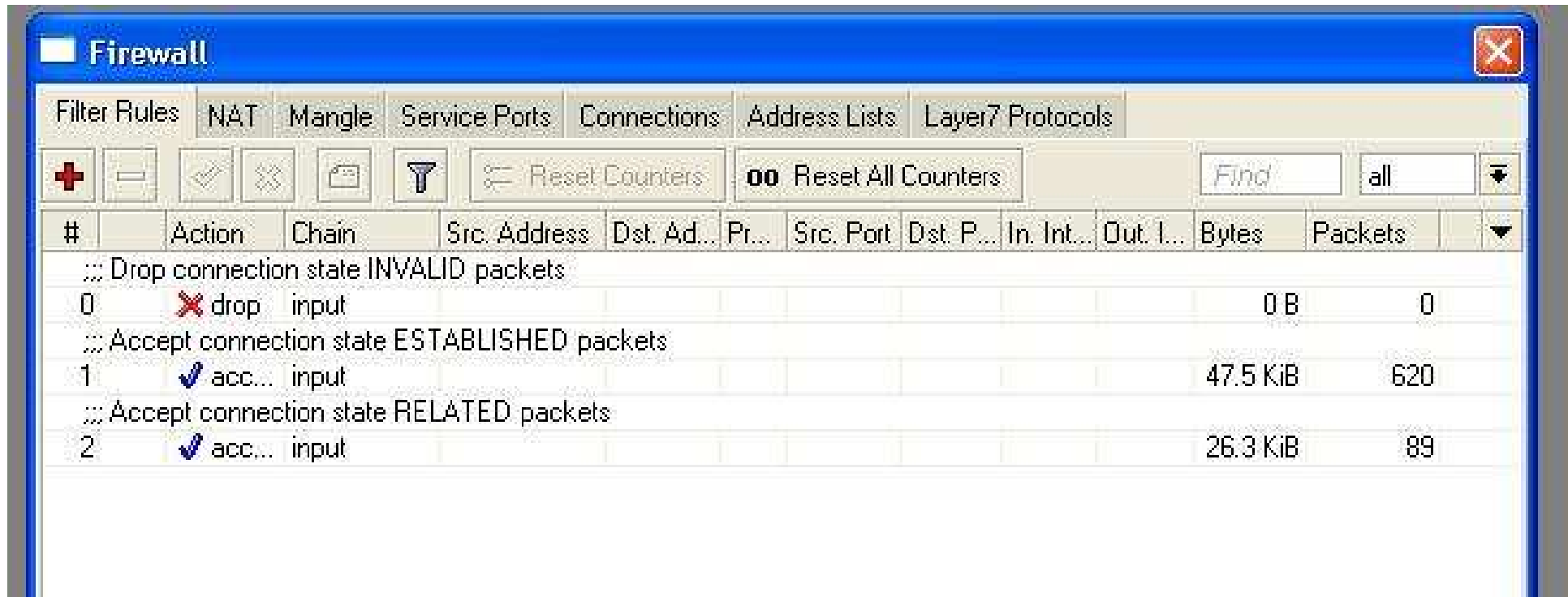
Label all your rules with comments

These rules ensure that we only process Connection State “new” packets through the firewall

- Once the connection is established or related we know it’s a valid packet and we would just waste processor power by evaluating it

Monitor the firewall filter rule counters

Lab result



The screenshot shows the Mikrotik WinBox Firewall Filter Rules configuration window. The 'Filter Rules' tab is active. The table below shows the configuration and statistics for three filter rules. Rule 0 is 'drop' and has 0 bytes and 0 packets. Rule 1 is 'accept' and has 47.5 KiB and 620 packets. Rule 2 is 'accept' and has 26.3 KiB and 89 packets.

#	Action	Chain	Src. Address	Dst. Ad...	Pr...	Src. Port	Dst. P...	In. Int...	Out. I...	Bytes	Packets
::: Drop connection state INVALID packets											
0	✘ drop	input								0 B	0
::: Accept connection state ESTABLISHED packets											
1	✔ acc...	input								47.5 KiB	620
::: Accept connection state RELATED packets											
2	✔ acc...	input								26.3 KiB	89

Are the counters increasing for established and related connections?

Check your results against the trainer router

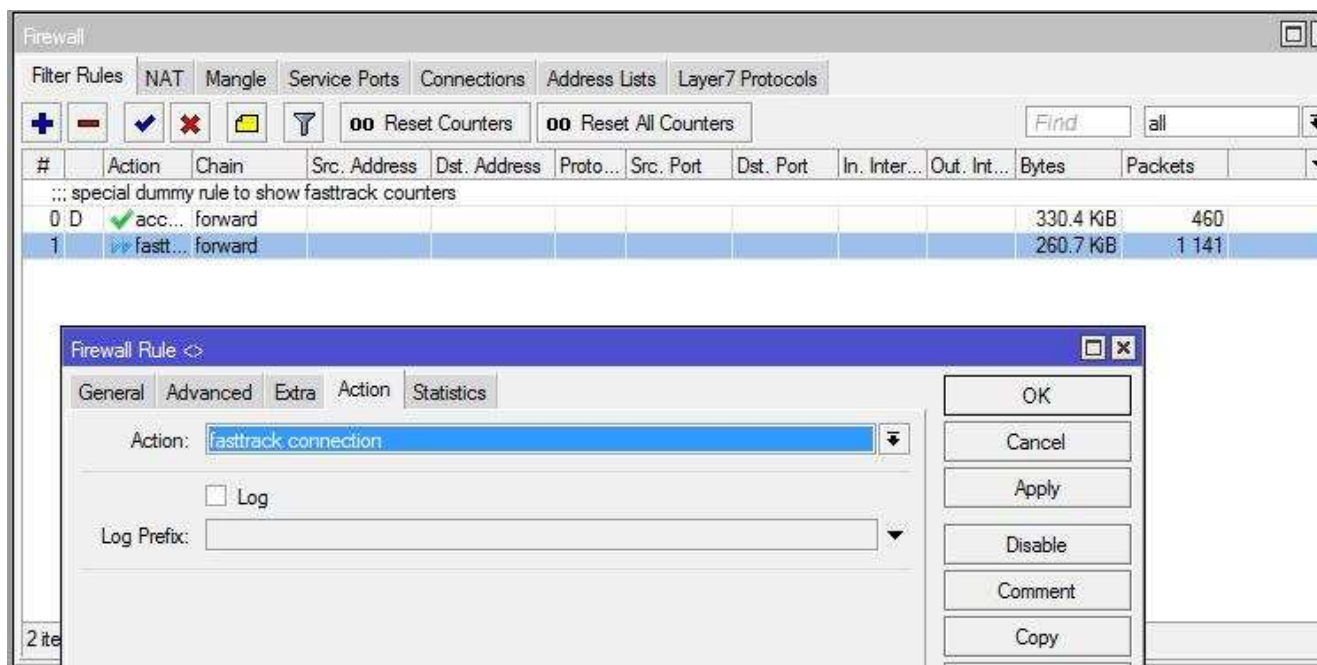
Fastrack

A method to accelerate packet flow through the router

An established or related connection can be marked for fasttrack connection

Bypasses firewall, connection tracking, simple queue and other features

Currently supports only TCP and UDP protocols



More Firewall Rules

LAB

Add a rule to accept all connections to your router from your internal IP range

Add a rule to accept Winbox from the outside network

Log and Drop all other packets going to the router

- From ROS 6.17 this can be done in the same rule

A list of common ports is available on the following slides

Test it out – you should be able to winbox to your neighbours router, but you should not be able to ping it.

Common Ports

Nr.	Port	Protocol	Comments
1	20	tcp	FTP
2	21	tcp	FTP
3	22	tcp	SSH,SFTP
4	23	Tcp	Telnet
5	53	tcp	DNS
6	80	tcp	HTTP
7	179	tcp	BGP
8	443	tcp	SHTTP (Hotspot)
9	1080	tcp	SoCKS (Hotspot)
10	1719	tcp	h323 (Telephony)
11	1720	tcp	h323 (Telephony)
12	1723	tcp	PPTP
13	1731	tcp	h323 (Telephony)
14	2000	tcp	Bandwidth server
15	2828	tcp	uPnP
16	3128	tcp	WEB Proxy
17	3986	tcp	Winbox (proxy)
18	3987	tcp	Winbox (ssl proxy)
19	8080	tcp	WEB Proxy test
20	8291	tcp	Winbox

Nr.	Port	Protocol	Comments
21	53	udp	DNS
22	67	udp	DHCP server
23	68	udp	DHCP client
24	123	udp	NTP
25	161	udp	SNMP
26	500	udp	IPSec
27	520	udp	RIP
28	521	udp	RIP
29	1701	udp	L2TP
30	1718	udp	h323 (Telephony)
31	1900	udp	uPnP
32	5000+	udp	h323 (Telephony)
33	5678	udp	Neighbour Discovery
34	20561	udp	(MAC)Winbox
35	-----	/4	IPIP
36	-----	/47	PPTP, EoIP
37	-----	/50	IPSec
38	-----	/51	IPSec
39	-----	/89	OSPF
40	-----	/112	VRRP

More Practice

LAB

Create a forward chain rule to drop all TCP port 80 traffic from your laptop

- Can you browse the Internet?

Create a rule to drop all Netbios traffic and all Microsoft DS traffic going through your router

- Netbios = TCP port 137-139
- Microsoft DS = TCP port 445

Accept the following traffic to your router

- Neighbour Discovery
- SSH, MAC Winbox, Bandwidth Test

Test the results

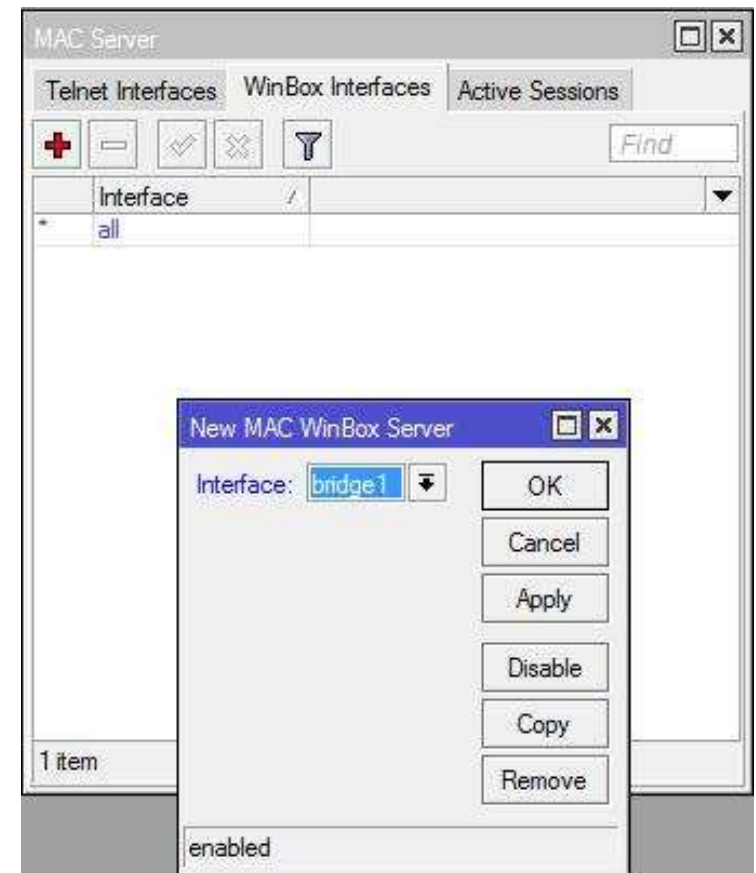
Important Issue

Firewall filters do not filter
MAC level communications

You should turn off MAC-telnet
and MAC-Winbox features at
least on the public facing
interface (**Tools → MAC**
Server)

***TIP**

You can disable the network
discovery feature so that the
router does not reveal itself (**IP**
→ Neighbour → Discovery)



Network Address Translation

Masquerade

Source NAT

Redirect

Destination NAT

Network Address Translation

Network Address Translation (NAT) is a method of remapping one IP address space into another by modifying network address information in IP packet headers while they are in transit across a router

The technique was originally used for ease of rerouting traffic in IP networks without renumbering every host

It has become a popular and essential tool in conserving global address space allocations in face of IPv4 address exhaustion by sharing one Internet-routable IP address of a NAT gateway for an entire private network

NAT Types

As there are two IP addresses and ports in an IP packet header, there are two types of NAT

- The one, which rewrites source IP address and/or port is called source NAT (src-nat)

Sometimes also known as “overload natting”, “one-to-many nat”

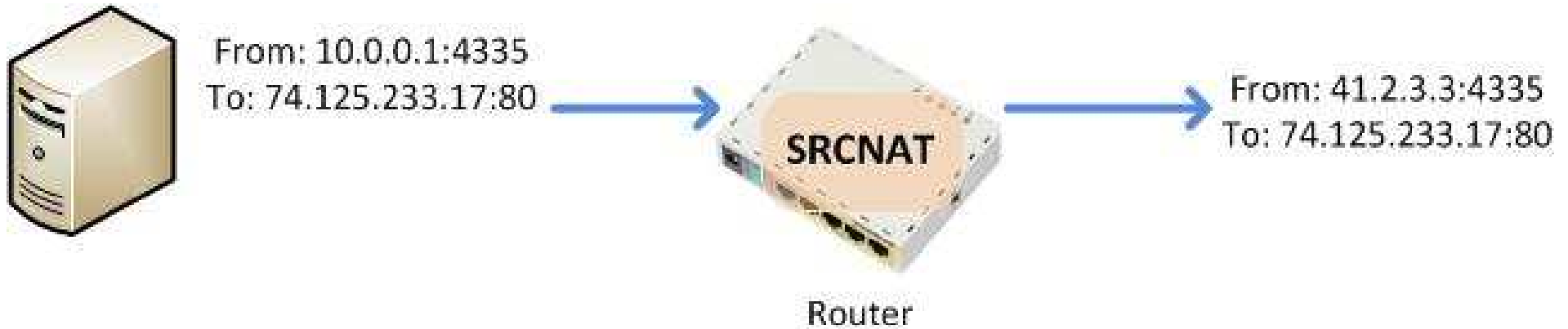
If the NAT type is unspecified it usually refers to source nat

- The other, which rewrites destination IP address and/or port is called destination NAT (dst-nat)

Sometimes also known as “port forwarding”, “opening ports”, “port mapping”

Firewall NAT rules process only the first packet of each connection (connection state “new” packets)

NAT Type Diagrams



Firewall NAT

The firewall NAT facility is a tool for rewriting a packet's header information.

Similar to Firewall Filter, the Firewall NAT consists of a sequence of IF-THEN rules

0) IF <condition(s)> THEN <action>

If a packet doesn't meet all the conditions of the rule, it will be sent on to the next rule.

If a packet meet all the conditions of the rule, the specified action will be performed on it.

NAT Actions

There are 6 specific actions in NAT

- dst-nat
- redirect
- src-nat
- masquerade
- netmap
- same

There are 7 more actions in the NAT, but they are exactly the same as in firewall filters

Masquerade

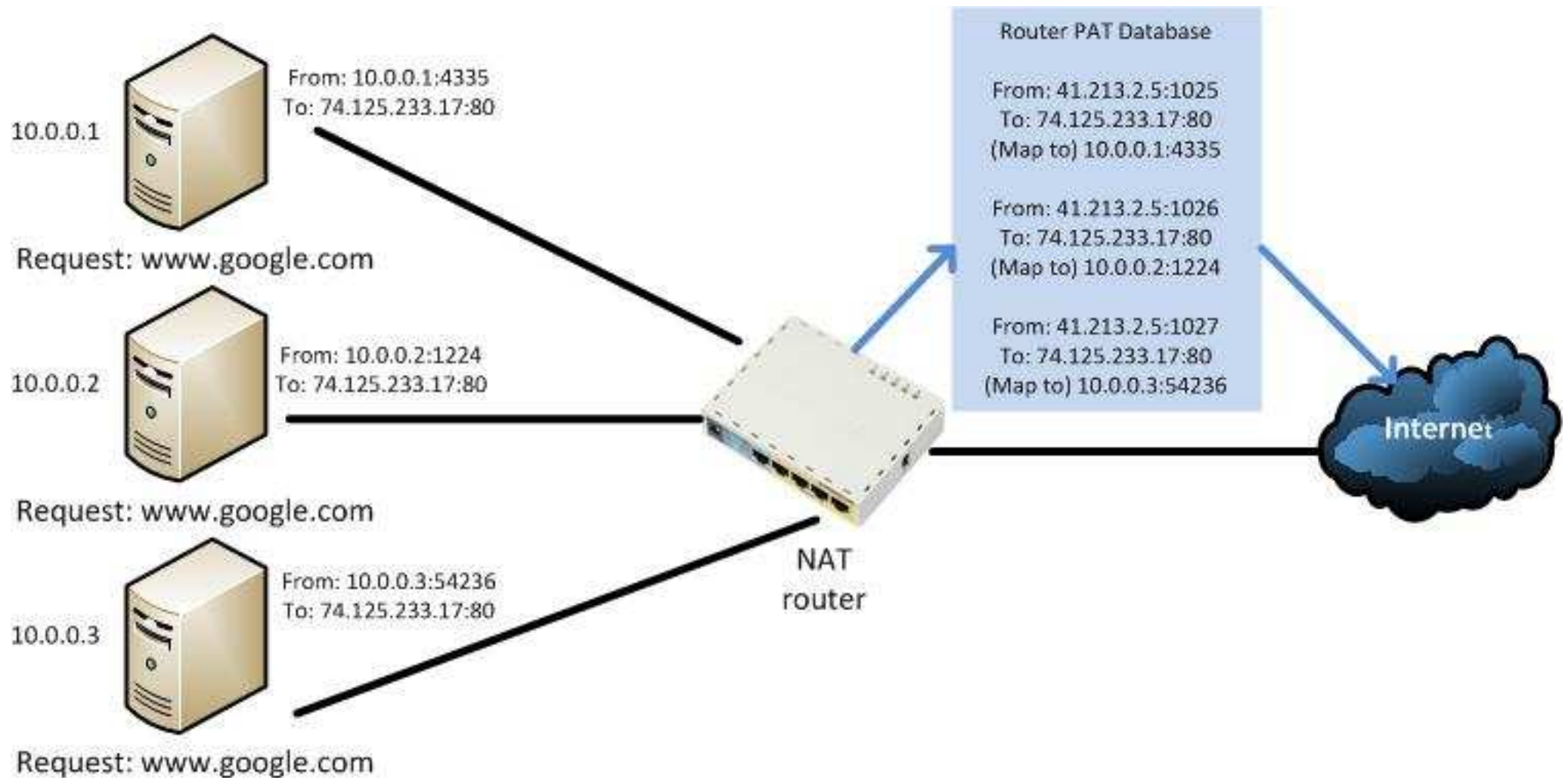
Action “masquerade” changes packet's source address to the router's address and specified port

This action can take place only in chain srcnat

Typical application: hide specific LAN resources behind one dynamic public IP address

The router uses a form of Port Address Translation to track requests from inside the network to external servers

Port Address Translation



Masquerade Rule Example

The screenshot shows the 'New NAT Rule' dialog box with the 'General' tab selected. The 'Chain' dropdown is set to 'srcnat'. The 'Src. Address' field is checked and contains '192.168.XY.0/24'. Other fields like 'Dst. Address', 'Protocol', 'Src. Port', 'Dst. Port', 'In. Interface', 'Out. Interface', 'Packet Mark', 'Connection Mark', 'Routing Mark', and 'Connection Type' are empty. A 'disabled' status indicator is visible at the bottom left.

New NAT Rule

General | Advanced | Extra | Action | Statistics

Chain: srcnat

Src. Address: 192.168.XY.0/24

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark:

Routing Mark:

Connection Type:

disabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove

The screenshot shows the 'New NAT Rule' dialog box with the 'Action' tab selected. The 'Action' dropdown is set to 'masquerade'. The 'disabled' status indicator is visible at the bottom left.

New NAT Rule

General | Advanced | Extra | Action | Statistics

Action: masquerade

disabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove

Src-nat

Action “src-nat” changes packet's source address and/or port to specified address and/or port

This action can take place only in chain srcnat

Typical application: hide specific LAN resources behind specific public IP address

Specify either a Source Address range or an Out Interface under General (or both)

- Source address ensures only valid ranges from your network are NATted
- Out Interface ensures only outgoing packets are NATted, and not incoming packets (also important for Masquerade)

Under Action = src-nat specify to-address as the public IP to map to (port is not usually required)

Src-nat Rule Example

NAT Rule <10.2.72.0/27>

General Advanced Extra Action Statistics

Chain:

Src. Address: 192.168.100.0/24

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface: ether3

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

enabled

NAT Rule <10.2.72.0/27>

General Advanced Extra Action Statistics

Action:

Log

Log Prefix:

To Addresses: 41.100.2.5

To Ports:

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

enabled

Source NAT Drawbacks

Hosts behind a NAT-enabled router do not have true end-to-end connectivity:

- connection initiation from outside is not possible
- some TCP services will work in “passive” mode
- src-nat behind several IP addresses is unpredictable
- some protocols will require so-called NAT helpers to work correctly (NAT traversal)

Src-nat



Restore backup-ROUTED

Modify your setup to use SRC-NAT instead of Masquerade to maintain internet access

Test the result

Redirect

Action “redirect” changes packet's destination address to router's address and specified port

This action can take place only in chain dstnat

Typical application: transparent proxying of network services (DNS,HTTP)



Redirect Rule Example

NAT Rule <80>

General Advanced Extra Action Statistics

Chain:

Src. Address: 192.168.55.0/24

Dst. Address:

Protocol: 6 (tcp)

Src. Port:

Dst. Port: 80

Any. Port:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

enabled

NAT Rule <80>

General Advanced Extra **Action** Statistics

Action:

To Ports:

enabled

Redirect



Capture all UDP port 53 packets originated from your private network 192.168.XY.0/24 and redirect them to the router itself.

Set your laptops DNS server to a random IP address (try 1.2.3.4)

Clear your router's and your laptop's DNS cache

- Command Prompt “ipconfig /flushdns”

Try browsing the Internet

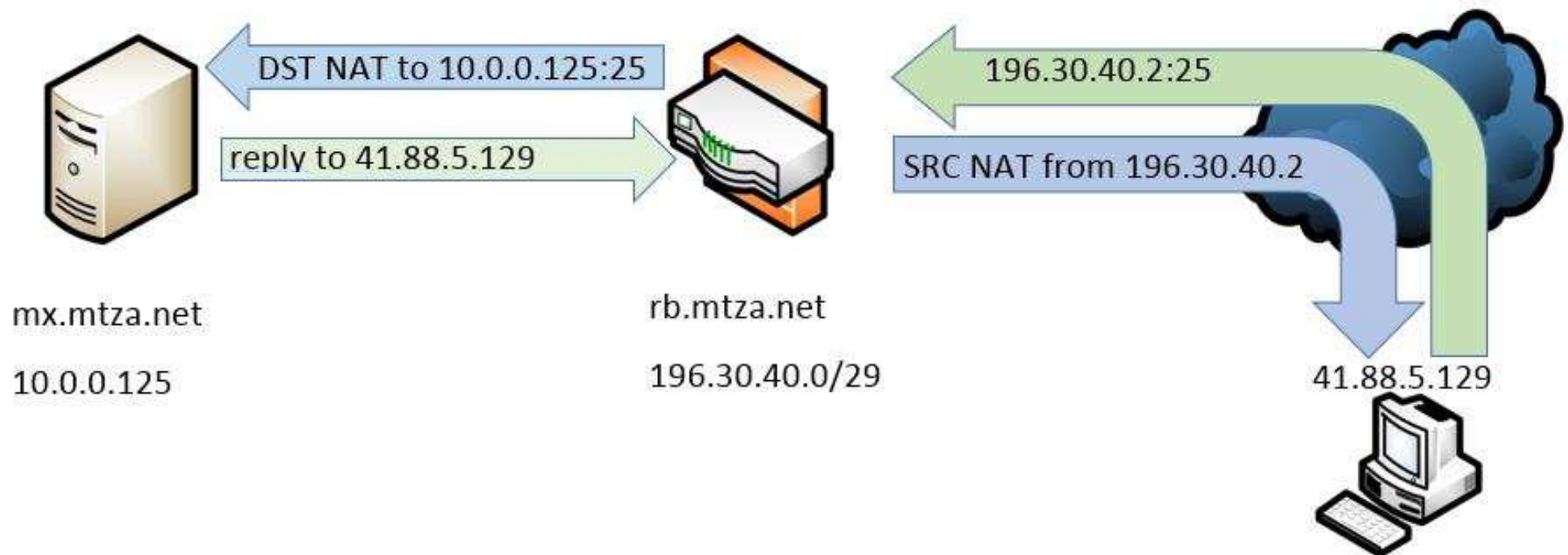
Take a look at the DNS cache of the router

Dst-nat

Action “dst-nat” changes packet's destination address and port to specified address and port

This action can take place only in chain dstnat

Typical application: ensure access to local network services from public network



Dst-nat Rule Example

New NAT Rule

General | Advanced | Extra | Action | Statistics

Chain:

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark:

Routing Mark:

Routing Table:

Connection Type:

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

enabled

New NAT Rule

General | Advanced | Extra | Action | Statistics

Action:

Log

Log Prefix:

To Addresses:

To Ports:

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters

enabled

Dst-nat



Capture all TCP port 80 (HTTP) packets originated from your private network 192.168.XY.0/24 and change destination address to 10.2.34.252 port 808 using a dst-nat rule

Clear your browser's cache on the laptop

Try browsing the Internet

IP Firewall Mangle

Firewall Mangle is used to apply special “marks” to packets that can be used elsewhere in the firewall and router

Common uses of mangle

- Mark traffic by address or protocol for custom routing (Route Mark)
- Mark traffic by address or protocol for bandwidth management (Connection and Packet Mark)
- Mark traffic by address or protocol for Wireless Multimedia management (Set Priority or Type of Service)

Matching is the same for other firewall rules, use Action based on what the mark is used for

Creating a Mangle example

For bandwidth management you need to use both Connection and Packet marks

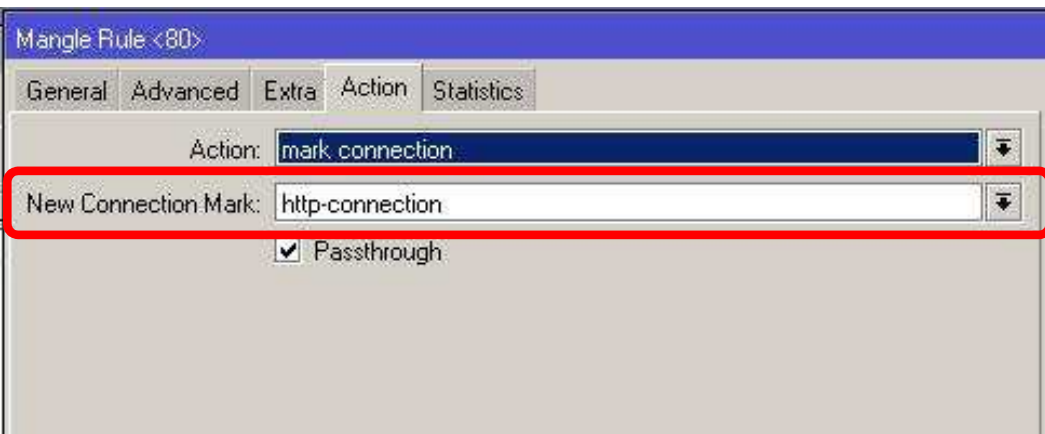
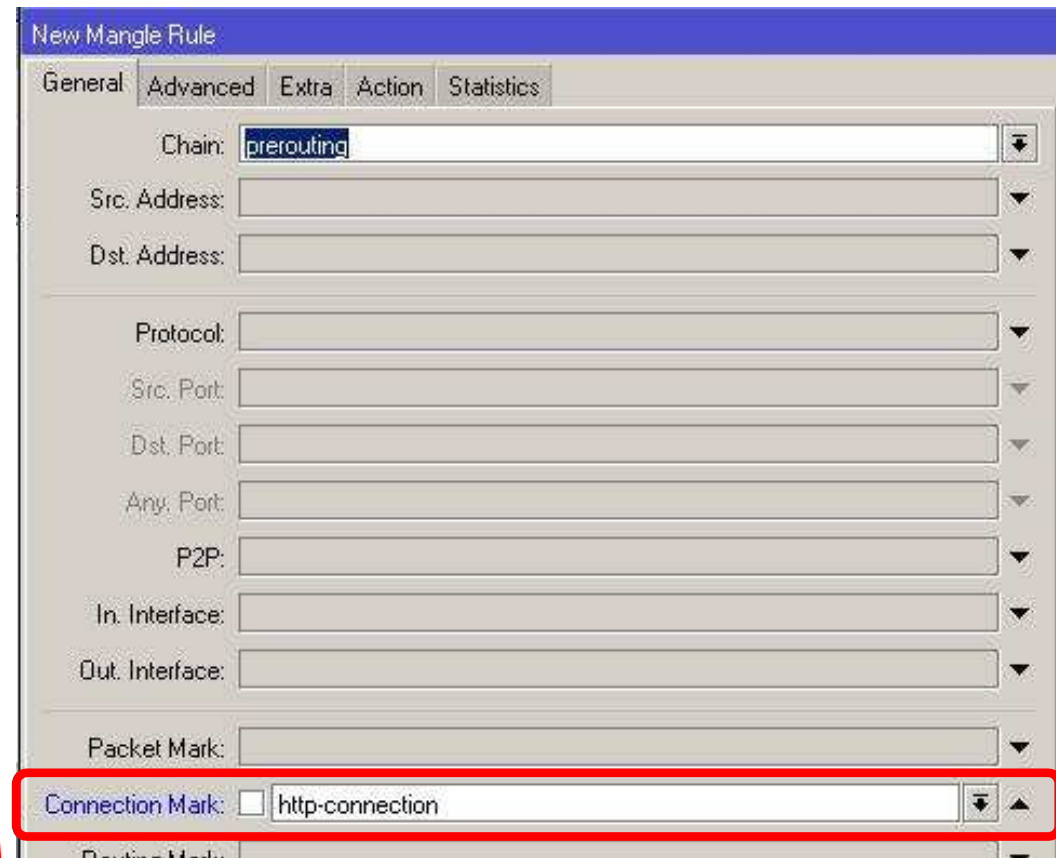
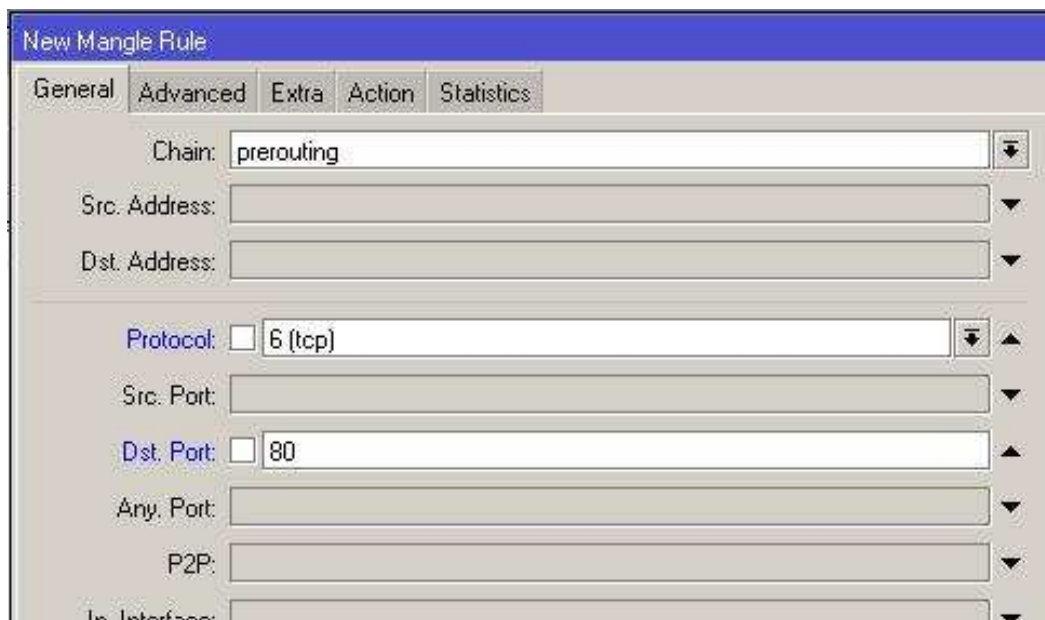
First identify the traffic and apply a Connection Mark

Then create a Packet Mark (flow mark) to track the flow of packets

- This is more efficient as it uses the ConnTrack table for packet matching

Once the Packet Mark is established you can use the advanced tab in your simple queue to limit by packet mark

Passthrough specifies if the processing should stop or proceed to further rules



Connection Mark

Packet mark from
Connection Mark

Using the Packet Mark

Use the Advanced tab to specify the flow mark

The screenshot shows the 'New Simple Queue' dialog box with the 'General' tab selected. The 'Name' field is set to 'limit-http'. The 'Target Address' field is empty. The 'Target Upload' and 'Target Download' checkboxes are checked. The 'Max Limit' is set to 256k for upload and 1M for download. The 'Burst' section is expanded, showing 'Burst Limit' at 512k for upload and 2M for download, 'Burst Threshold' at 128k for upload and 512k for download, and 'Burst Time' at 30 seconds for both. The 'Time' section is collapsed. The 'enabled' checkbox at the bottom is checked.

The screenshot shows the 'New Simple Queue' dialog box with the 'Advanced' tab selected. The 'P2P' dropdown is set to 'none'. The 'Packet Marks' field is set to 'http-flow' and is highlighted with a red rectangle. The 'Dst. Address' field is empty. The 'Interface' is set to 'all'. The 'Target Upload' and 'Target Download' checkboxes are checked. The 'Limit At' is set to 'unlimited' for both. The 'Queue Type' is set to 'default-small' for both. The 'Parent' is set to 'none' and the 'Priority' is set to 8. The 'enabled' checkbox at the bottom is checked.

Mangle



Create a Mangle to mark all web traffic (TCP:80,443)

- Create a Connection Mark
- Create a Packet Mark based on the Connection Mark

Create a simple queue to limit all HTTP traffic to 128kbps

Test the limitation

Address List Options

Instead of creating one filter rule for each IP network address, you can create a single rule by using an IP address list.

Use “Src./Dst. Address List” options in the Filter rule Advanced tab

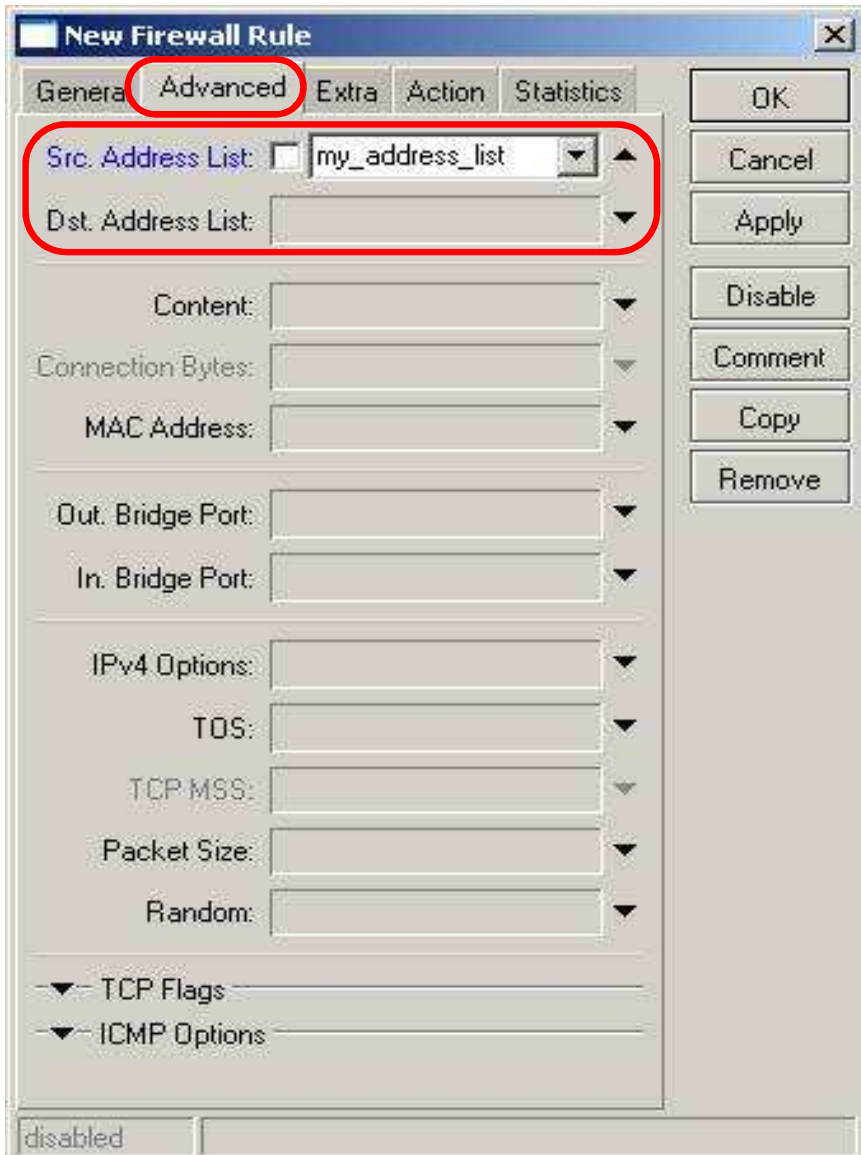
Create an address list in the “/ip firewall address-list” menu

- Use single address, range or subnet or any combination

You can create a list by single IP, range of IP’s or CIDR network

You can use 1 address list per firewall rule

Rules can also be created dynamically by using the Add <> to Address List action in Firewall Filter, NAT or Mangle



Firewall Summary

Firewall Filter

- Used to control traffic flow to, from and through the router
- Most often used to drop unwanted traffic based on user defined rules
- Uses three pre-defined chains, input (to the router), output (from the router), forward (through the router)
- Can have unlimited custom defined chains

Firewall NAT (Network Address Translation)

- Use to selectively alter the source IP of the packet (srcnat) or destination IP (dstnat)
- Masquerade is used to allow multiple system connectivity behind a single public facing IP
- Redirect sends traffic to the router

Firewall Mangle

- Used to add special marks (labels) to the packet for processing elsewhere in the router
- Often used for Queue Trees which require a Packet Mark to work
- Can also change the packet header (TOS, MSS, DSCP) often used for Quality of Service

Address List is used to group together single or groups of IP's for use in firewall rules (Filter, NAT or Mangle)

Connection Tracking must be enabled for NAT, Mangle and most Filter rules to work

Is There Still Time?

Hotspot

Open Shortest Path First

HotSpot

HTTP based user authentication and
authorization

HotSpot

All the standard access types we have looked at need some user input or setup to work

- DHCP, PPPoE, PPTP, L2TP all require some level of setup on the client

A system is needed whereby a user can obtain network or internet access with almost no user effort

The HotSpot is used for authentication in local network

- Meaning it is used in Layer2
- All AP's must be bridged to the HotSpot interface

***TIP**

Authentication is based on HTTP/HTTPS protocol which means it can work with any Internet browser

HotSpot is a system combining various independent features of RouterOS together to provide 'Plug-and-Play' access

HotSpot Operation

A user who is connected to the hotspot tries to open a web page

The router checks whether the user is already authenticated in the HotSpot system.

- If he is then access is given

If not, the user is redirected to the HotSpot login page.

The user then specifies the login information

If the login information has been correct, then the router

- authenticates the client in the Hotspot system
- opens the requested web page
- opens a status popup window

This user can access the network through the HotSpot gateway

Please log on to use the internet hotspot service

login

password

HOTSPOT GATEWAY
powered by *MikroTik*

Powered by MikroTik RouterOS

Welcome anyuser!

IP address:	10.1.100.1
bytes up/down:	23.1 KiB / 43.5 KiB
connected:	40s
status refresh:	1m

HotSpot features

User authentication

- By voucher
- By MAC Address
- By Trial account

User accounting by time, data transferred/received

Data limitation

- by data rate
- by amount

User limitation by time

- Both uptime limits and airtime window are possible (when using RADIUS)

RADIUS support

Walled garden

Customizable HTML pages

Auto one-to-one NAT (Universal Client Support)

HotSpot Setup Wizard

For best results start on a clean router with basic internet access

- The hotspot won't function correctly without proper DNS lookup

The best way to setup the HotSpot is by using the automated setup function

Start HotSpot setup and select interface to run HotSpot on

Set address of HotSpot interface

- The default is the first IP on the interface

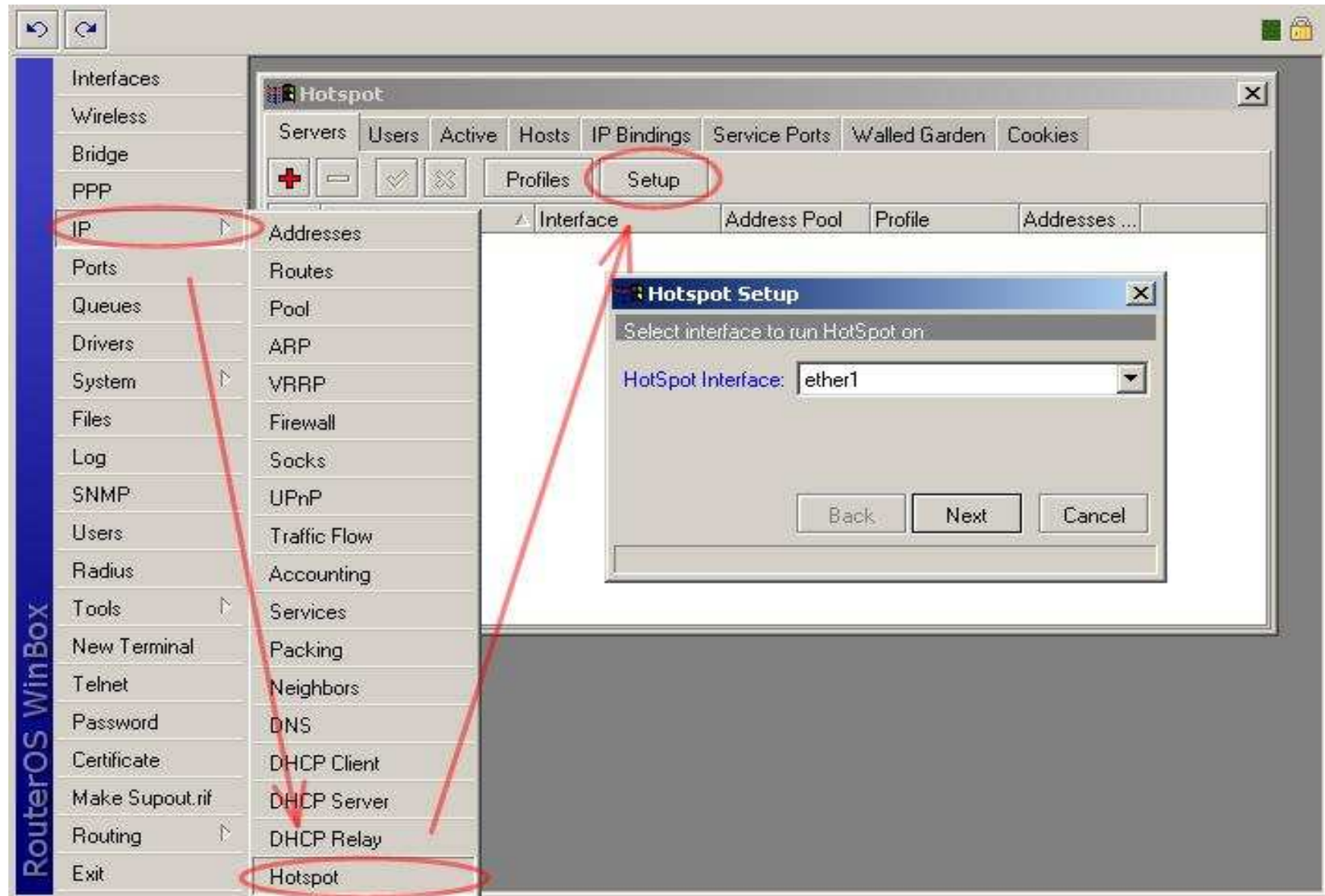
Choose whether to masquerade hotspot network

- An IP > Firewall > NAT rule will be created for you

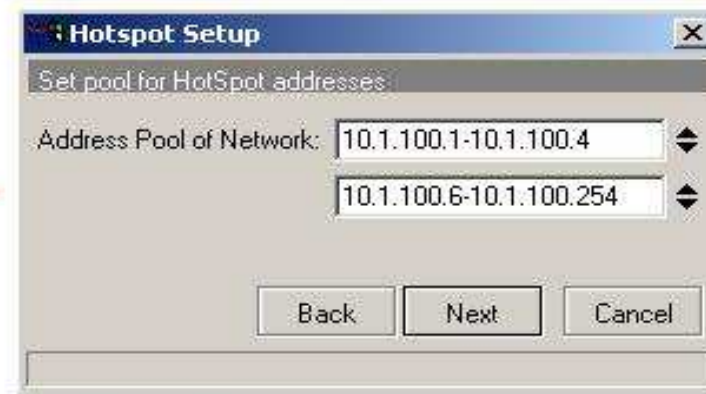
Select pool for HotSpot addresses

Select HotSpot SSL certificate (if using HTTPS)

HotSpot Setup Wizard (Step 1)



HotSpot Setup Wizard (Step 2-5)



HotSpot Setup Wizard

Select SMTP server to automatically redirect outgoing mails to local SMTP server

- Clients do not need to alter their outgoing mail settings
- Authenticated SMTP servers may cause issues – an IP Firewall Address list can fix this

Only an issue if running on TCP/25 with Auth

Set up DNS servers to be used by the router and HotSpot users

- You can use the routers current DNS if available

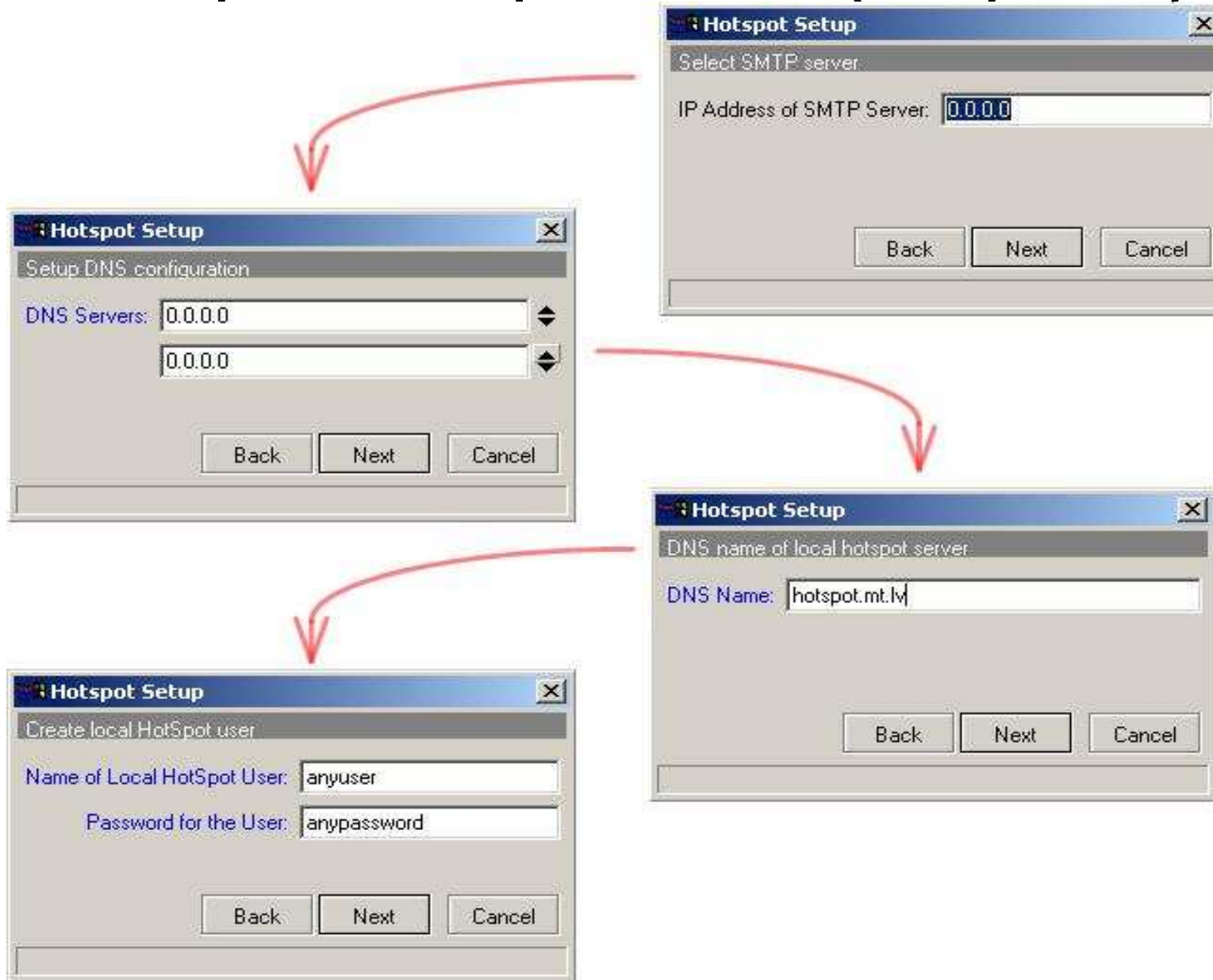
Set DNS name of local hotspot server

- This must look like a FQDN, a single name will not work
- Do not use anything.**local**

And then finally you can create one Hotspot user.

- This will usually be the hotspot admin user

HotSpot Setup Wizard (Step 5-8)



Hotspot Setup

LAB

Restore your router from backup-*your_name*-ROUTED

Confirm internet access

Setup your HotSpot on ether1

Once complete you will be disconnected from the router (if you were logged on with IP address)

Open a web browser – you should get the hotspot login screen

Enter details for the first user you created

- You should now have full network access

ADVANCED: Setup a hotspot on 2.4Ghz on your 2nd wlan card.

- Unplug from Ether and connect wirelessly to your hotspot
- Test functionality

Open Shortest Path First Protocol

Fault-tolerant network with
optimized traffic flow

What is OSPF?

Open Shortest Path First (OSPF) is a dynamic routing protocol for use in (IP) networks.

Specifically, it is a link-state routing protocol and falls into the group of interior gateway protocols operating within an autonomous system (AS).

OSPF is perhaps the most widely-used interior gateway protocol (IGP) in large enterprise networks

OSPF is used to dynamically build routes in a network that has rapidly changing content or multiple routes to destinations

Using OSPF

OSPF can be used for:

- switching to a redundant or standby link upon the failure or abnormal termination of the currently active link
- Load balancing in networks with multiple physical links
- routing topology updates in highly dynamic network
- ensuring internal AS consistency when using BGP

OSPF support in RouterOS is provided via a separate 'routing' package – check that it is enabled (normally enabled by default)

Make sure the firewall does not filter out OSPF communications

- OSPF neighbours use IP protocol 89 for communication with each other

Ensure your network IP plan is correct

- No default ranges left on routers!
- Troubleshooting IP conflicts on OSPF networks is extremely complicated and time consuming

Before you begin

LAB

Restore from backup Backup-ROUTED

Remove your default route in `/ip routes`

Remove any masquerade rules in `/ip firewall nat`

The trainer will now guide you through OSPF setup

- Configure distribution of routes under **OSPF > Instance**
- Add the required networks under **OSPF > Network**

Check the routing table – are you building up the routes via OSPF?

Do you have internet access? Why not?

OSPF Route Redistribution

Set redistribute connected routes [and static routes]:

```
/routing ospf
```

```
set redistribute-connected=as-type-1
```

```
set redistribute-static=as-type-1
```

If you use RIP or BGP as well, you may want to redistribute routes learned by these protocols

Leave 'Distribute default' route to 'never', unless it is an ASBR (edge router)

OSPF Routes

Route List								
Routes Rules								
Find all								
	Destination	Gateway	Gateway ...	Interface	Distance	Routing Mark	Pref. Source	
DAo	▶ 2.1.32.28/30	41.223.35.36		ether1	110			
DAo	▶ 2.1.254.0/28	41.223.35.36		ether1	110			
DAo	▶ 2.1.254.16/30	41.223.35.36		ether1	110			
DAo	▶ 10.0.0.0/8	41.223.35.36		ether1	110			
DAo	▶ 10.0.0.0/24	41.223.35.34		ether1	110			
DAo	▶ 10.0.30.0/23	41.223.35.34		ether1	110			
DAo	▶ 10.0.32.0/21	41.223.35.34		ether1	110			
DAo	▶ 10.0.36.0/24	41.223.35.34		ether1	110			
DAo	▶ 10.0.66.0/24	41.223.35.34		ether1	110			
DAo	▶ 10.1.0.0/16	41.223.35.34		ether1	110			
DAo	▶ 10.1.0.0/24	41.223.35.34		ether1	110			
DAo	▶ 10.2.1.252/30	41.223.35.101		at-bb-bb	110			
DAC	▶ 10.2.16.0/28			ether1	0		10.2.16.1	
DAC	▶ 10.2.16.244/30			at-bb-bb	0		10.2.16.245	
DAo	▶ 10.2.16.248/29	41.223.35.34		ether1	110			
DAo	▶ 10.2.17.0/24	41.223.35.34		ether1	110			
DAo	▶ 10.2.17.0/28	41.223.35.34		ether1	110			
DAo	▶ 10.2.18.248/29	41.223.35.35		ether1	110			
DAo	▶ 10.2.24.0/21	41.223.35.34		ether1	110			
DAo	▶ 10.2.32.0/27	41.223.35.22, 41.223.35.34		at-mi-bb, ether1	110			
DAo	▶ 10.2.60.0/24	41.223.35.22, 41.223.35.34, 41.223.35.97		at-mi-bb, ethe...	110			
DAo	▶ 10.2.63.252/30	41.223.35.97		at-bb-bb	110			
DAo	▶ 10.2.64.1	41.223.35.22, 41.223.35.34		at-mi-bb, ether1	110			
DAo	▶ 10.2.64.15	41.223.35.22, 41.223.35.34		at-mi-bb, ether1	110			
DAo	▶ 10.2.64.19	41.223.35.22, 41.223.35.34		at-mi-bb, ether1	110			
DAo	▶ 10.2.64.27	41.223.35.22, 41.223.35.34		at-mi-bb, ether1	110			
DAo	▶ 10.2.64.228/30	41.223.35.22, 41.223.35.34		at-mi-bb, ether1	110			
DAo	▶ 10.2.64.232/29	41.223.35.22, 41.223.35.34, 41.223.35.97		at-mi-bb, ethe...	110			

OSPF Settings

LAB

The trainer router will now be set as an edge router

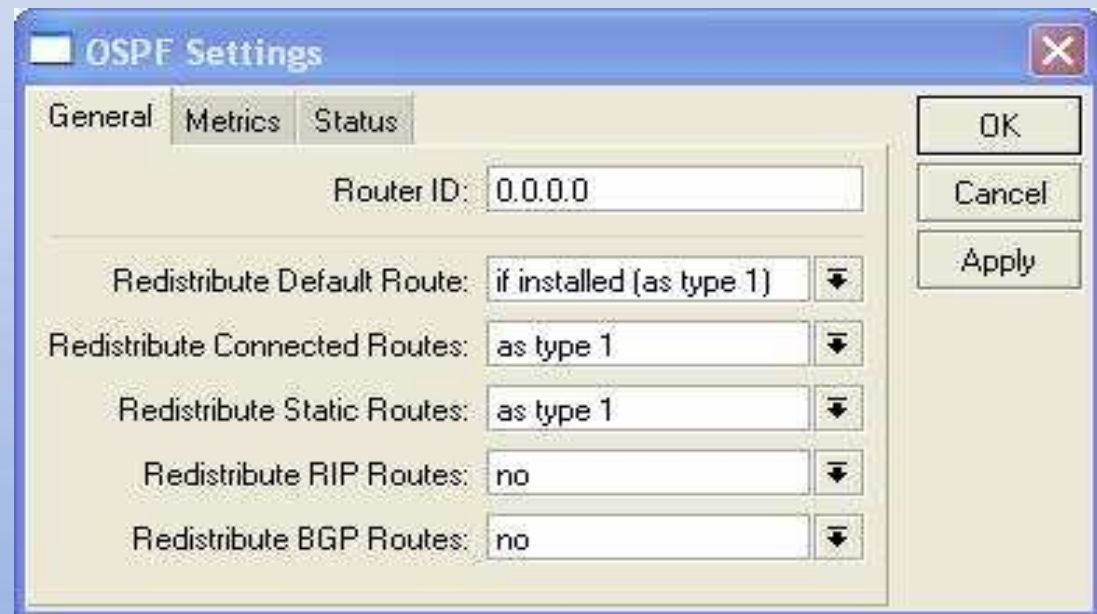
Do you have internet and network access now?



The image shows a screenshot of the 'OSPF Settings' dialog box for a standard router. The 'General' tab is selected. The 'Router ID' is set to '0.0.0.0'. The 'Redistribute Default Route' is set to 'never'. The 'Redistribute Connected Routes' is set to 'as type 1'. The 'Redistribute Static Routes' is set to 'as type 1'. The 'Redistribute RIP Routes' is set to 'no'. The 'Redistribute BGP Routes' is set to 'no'. The 'OK', 'Cancel', and 'Apply' buttons are visible on the right side.

Setting	Value
Router ID	0.0.0.0
Redistribute Default Route	never
Redistribute Connected Routes	as type 1
Redistribute Static Routes	as type 1
Redistribute RIP Routes	no
Redistribute BGP Routes	no

Standard OSPF router settings



The image shows a screenshot of the 'OSPF Settings' dialog box for an ASBR (edge) router. The 'General' tab is selected. The 'Router ID' is set to '0.0.0.0'. The 'Redistribute Default Route' is set to 'if installed (as type 1)'. The 'Redistribute Connected Routes' is set to 'as type 1'. The 'Redistribute Static Routes' is set to 'as type 1'. The 'Redistribute RIP Routes' is set to 'no'. The 'Redistribute BGP Routes' is set to 'no'. The 'OK', 'Cancel', and 'Apply' buttons are visible on the right side.

Setting	Value
Router ID	0.0.0.0
Redistribute Default Route	if installed (as type 1)
Redistribute Connected Routes	as type 1
Redistribute Static Routes	as type 1
Redistribute RIP Routes	no
Redistribute BGP Routes	no

OSPF ASBR (edge) router settings

Certification Test

Check your Emails for Exam Invitation

Open Book exam

- Google.com
- Mikrotik.com/documentation
- Wiki.mikrotik.com
- Forum.mikrotik.com
- Routerboard.com

Exam is 1 Hour Long.

- 60% Pass Grade
- Everyone's Questions are different
- 25 questions from a large pool of possible questions

Please reset your router after you are done