

*Mikro***Tik**

Certified Network Associate (MTCNA)

Riga, Latvia

January 1 - January 3, 2016

About the Trainer

- Name
- Experience
- ...



Your photo

Course Objectives

- Provide an overview of RouterOS software and RouterBOARD products
- Hands-on training for MikroTik router configuration, maintenance and basic troubleshooting

Learning Outcomes

The student will:

- Be able to configure, manage and do basic troubleshooting of a MikroTik RouterOS device
- Be able to provide basic services to clients
- Have a solid foundation and valuable tools to manage a network

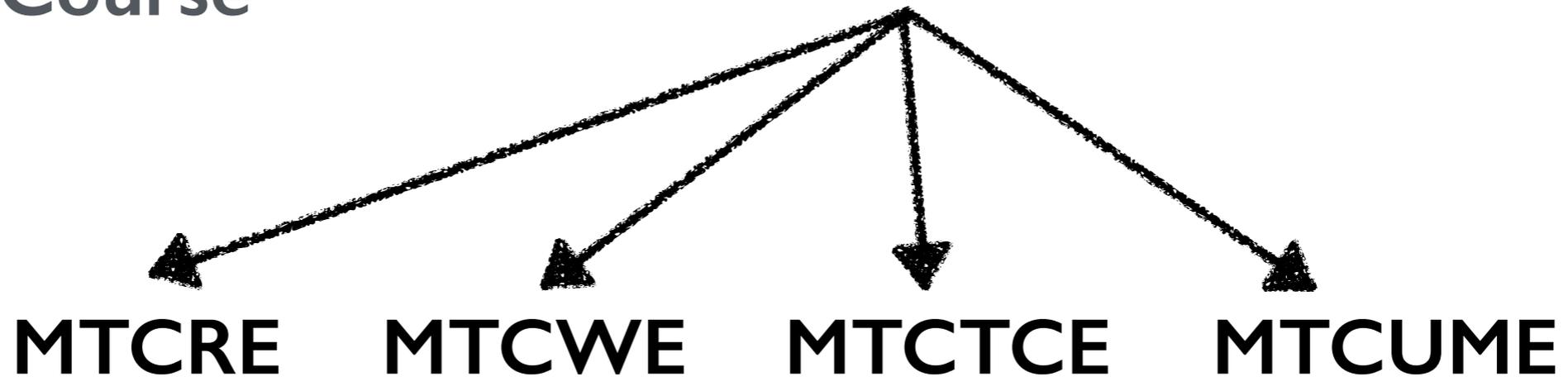
MikroTik Certified

Courses

Introduction
Course



MTCNA



MTCINE

For more info see: <http://training.mikrotik.com>

MTCNA Outline

- Module 1: Introduction
- Module 2: DHCP
- Module 3: Bridging
- Module 4: Routing
- Module 5: Wireless
- Module 6: Firewall

MTCNA Outline

- Module 7: QoS
- Module 8: Tunnels
- Module 9: Misc
- Hands on LABs during each module (more than 40 in total)
- Detailed outline available on mikrotik.com

Schedule

- Training day: 9AM - 5PM
- 30 minute breaks: 10:30AM and 3PM
- 1 hour lunch: 12:30PM
- Certification test: last day, 1 hour

Housekeeping

- Emergency exits
- Bathroom location
- Food and drinks while in class
- Please set phone to 'silence' and take calls outside the classroom

Introduce Yourself

- Your name and company
- Your prior knowledge about networking
- Your prior knowledge about RouterOS
- What do you expect from this course?
- Please, note your number (XY): ____



Certified Network Associate (MTCNA)

Module I

Introduction

About MikroTik

- Router software and hardware manufacturer
- Products used by ISPs, companies and individuals
- Mission: to make Internet technologies faster, more powerful and affordable to a wider range of users

About MikroTik

- 1996: Established
- 1997: RouterOS software for x86 (PC)
- 2002: First RouterBOARD device
- 2006: First MikroTik User Meeting (MUM)
 - Prague, Czech Republic
- 2015: Biggest MUM: Indonesia, 2500+

About MikroTik

- Located in Latvia
- 160+ employees
- mikrotik.com
- routerboard.com



MikroTik RouterOS

- Is the operating system of MikroTik RouterBOARD hardware
- Can also be installed on a PC or as a virtual machine (VM)
- Stand-alone operating system based on the Linux kernel

RouterOS Features

- Full 802.11 a/b/g/n/ac support
- Firewall/bandwidth shaping
- Point-to-Point tunnelling (PPTP, PPPoE, SSTP, OpenVPN)
- DHCP/Proxy/HotSpot
- And many more... see: wiki.mikrotik.com

MikroTik RouterBOARD

- A family of hardware solutions created by MikroTik that run RouterOS
- Ranging from small home routers to carrier-class access concentrators
- Millions of RouterBOARDS are currently routing the world



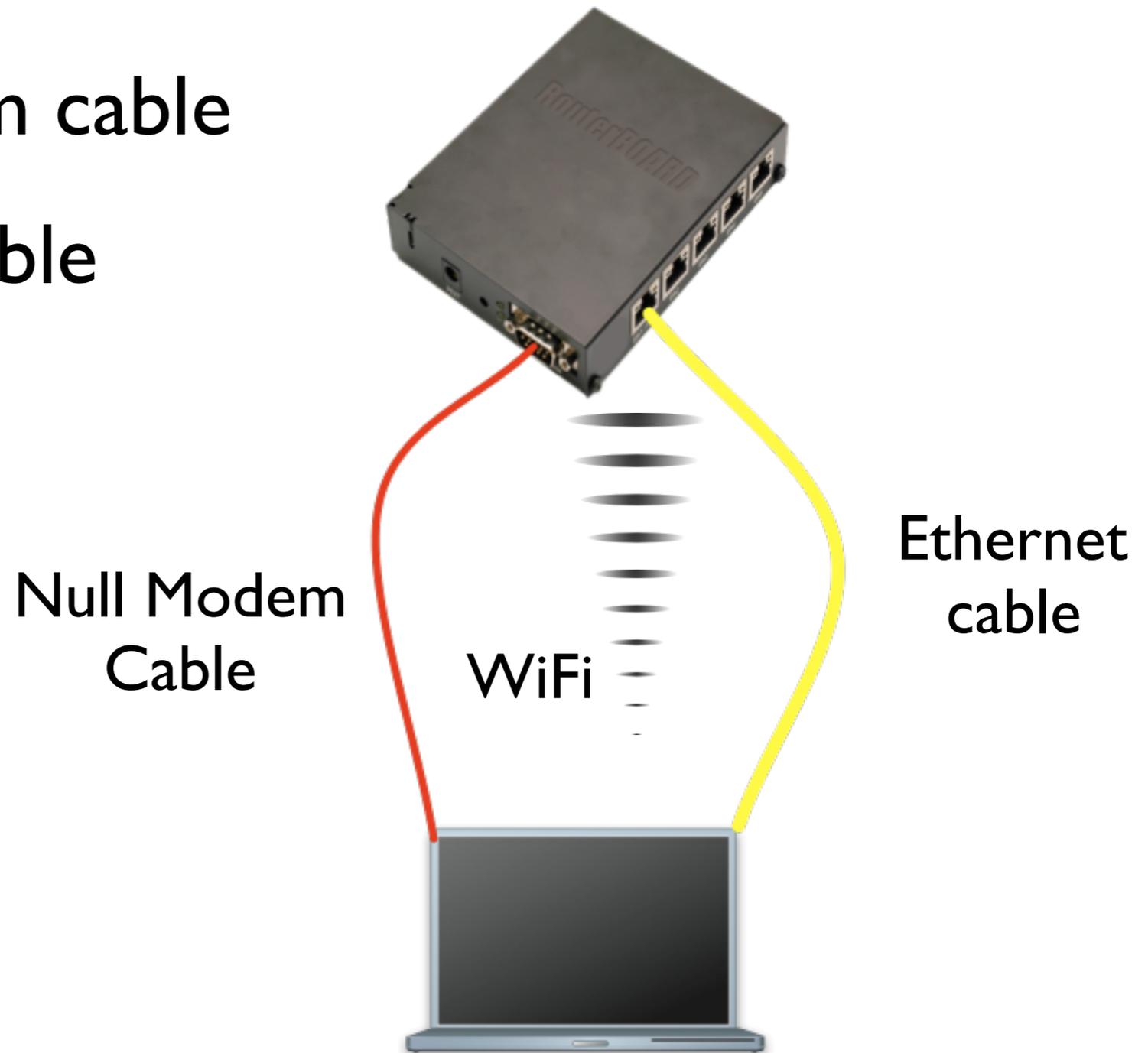
MikroTik RouterBOARD

- Integrated solutions - ready to use
- Boards only - for assembling own system
- Enclosures - for custom RouterBOARD builds
- Interfaces - for expanding functionality
- Accessories



First Time Access

- Null modem cable
- Ethernet cable
- WiFi

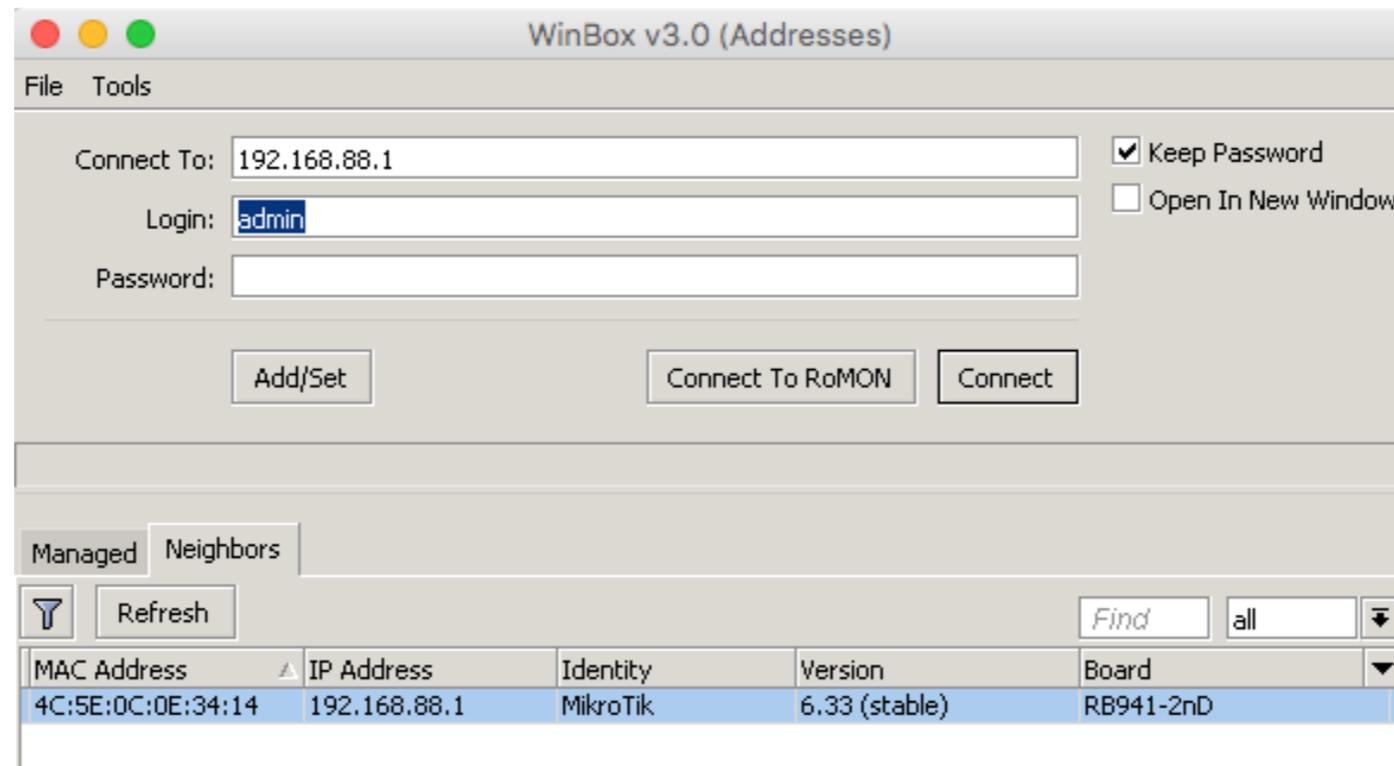


First Time Access

- WinBox - <http://www.mikrotik.com/download/winbox.exe>
- WebFig
- SSH
- Telnet
- Terminal emulator in case of serial port connection

WinBox

- Default IP address (LAN side): 192.168.88.1
- User: admin
- Password: (blank)

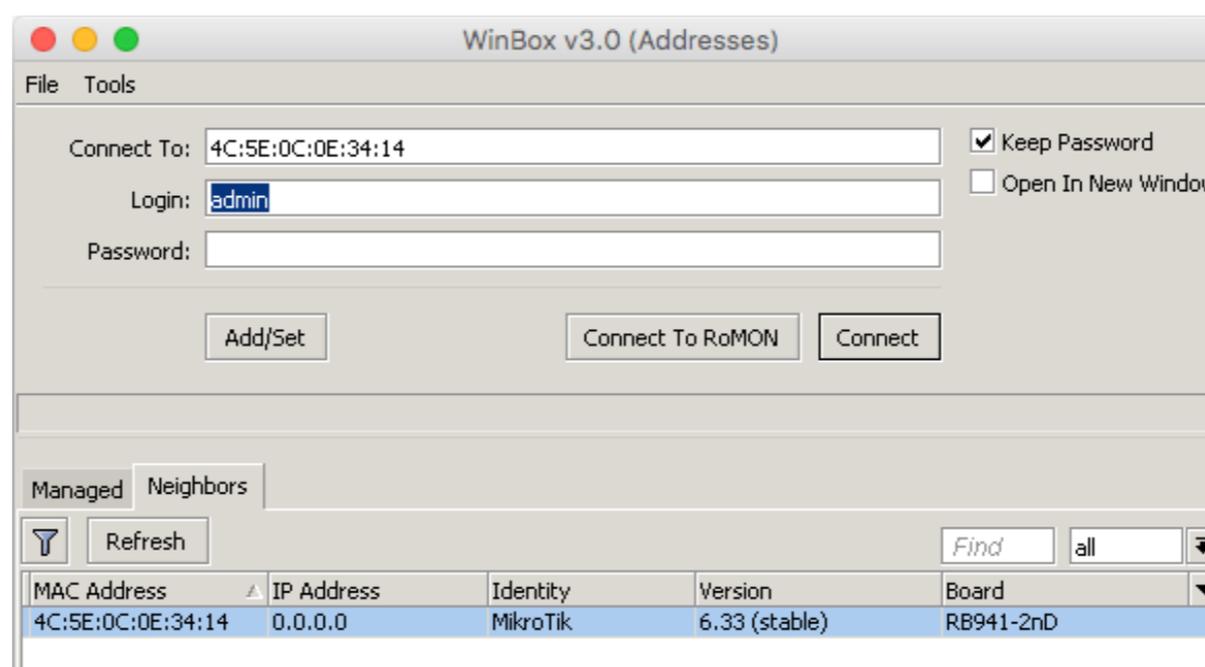


MAC WinBox

- Observe WinBox title when connected using IP address
- Connect to the router using MAC address
- Observe WinBox title

MAC WinBox

- Disable IP address on the bridge interface
- Try to log in the router using IP address (not possible)
- Try to log in the router using MAC WinBox (works)

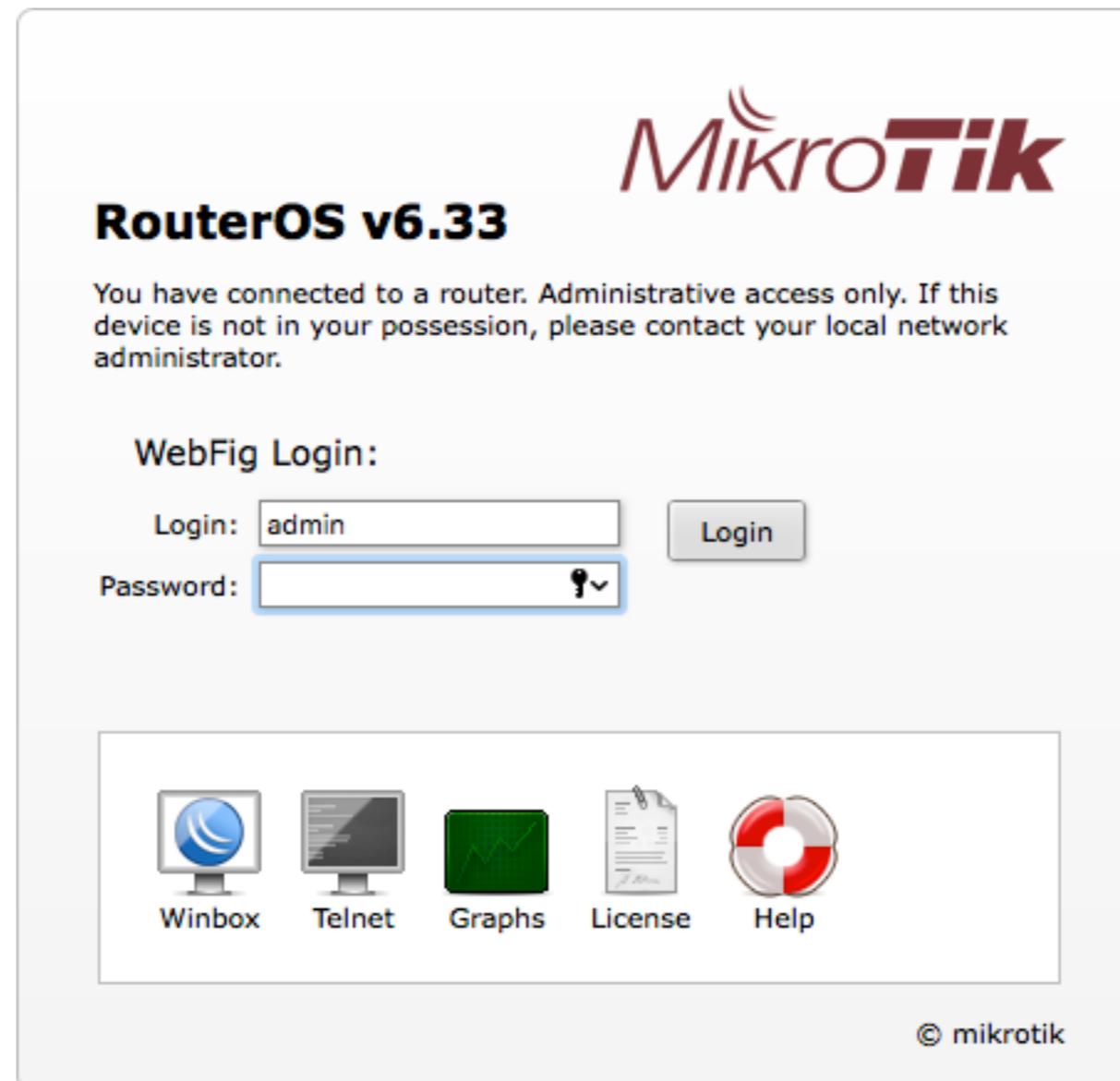


MAC WinBox

- Enable IP address on the bridge interface
- Log in the router using IP address

WebFig

- Browser - <http://192.168.88.1>



The screenshot shows the Mikrotik RouterOS v6.33 WebFig login interface. At the top right is the Mikrotik logo. Below it, the text "RouterOS v6.33" is displayed. A warning message states: "You have connected to a router. Administrative access only. If this device is not in your possession, please contact your local network administrator." The "WebFig Login:" section contains a "Login:" label, a text input field with "admin" entered, a "Login" button, a "Password:" label, and a password input field with a key icon and a dropdown arrow. Below the login fields is a row of five icons: Winbox (a blue globe), Telnet (a terminal window), Graphs (a green square with a white checkmark), License (a document icon), and Help (a red and white lifebuoy). The copyright notice "© mikrotik" is located at the bottom right of the page.

Quick Set

- Basic router configuration in one window
- Accessible from both WinBox and WebFig
- In more detail described in “Introduction to MikroTik RouterOS and RouterBOARDS” course

Quick Set

Quick Set

Configuration

Mode: Router Bridge

Wireless Network

Address Acquisition: Static Automatic PPPoE

IP Address: 10.5.120.244

Netmask: 255.255.255.0 (/24)

Gateway: 10.5.120.1

Upload: unlimited bits/s

Download: unlimited bits/s

Local Network

IP Address: 192.168.88.1

Netmask: 255.255.255.0 (/24)

DHCP Server

DHCP Server Range: 192.168.88.10-192.168.88.254

NAT

System

Router Identity: MikroTik

Password:

Confirm Password:

Wireless

Status: connected to ess

AP MAC: 4C:5E:0C:0A:0F:A3

Network Name: 3rd_fl

Tx/Rx Signal Strength: -42/-43 dBm

Tx/Rx CCQ: 47/46 %

Signal To Noise: 66 dB

Wireless Protocol: 802.11

LAN MAC Address: 4C:5E:0C:0E:34:13

LAN MAC Address: 4C:5E:0C:0E:34:13

Default Configuration

- Different default configuration applied
- For more info see [default configuration wiki page](#)
- Example: SOHO routers - DHCP client on Ether1, DHCP server on rest of ports + WiFi
- Can be discarded and 'blank' used instead

Command Line Interface

- Available via SSH, Telnet or 'New Terminal' in WinBox and WebFig

```
MMM   MMM   KKK           TTTTTTTTTT   KKK
MMM MMM MMM III KKK KKK RRRRRR   000000   TTT   III KKK KKK
MMM MM  MMM III KKKKK   RRR  RRR  000  000   TTT   III KKKKK
MMM     MMM III KKK KKK RRRRRR   000  000   TTT   III KKK KKK
MMM     MMM III KKK KKK RRR  RRR  000000   TTT   III KKK KKK

MikroTik RouterOS 6.33 (c) 1999-2015      http://www.mikrotik.com/

[?]          Gives the list of available commands
command [?]  Gives help on the command and list of arguments

[Tab]       Completes the command/word. If the input is ambiguous,
            a second [Tab] gives possible options

/           Move up to base level
..         Move up one level
/command    Use command at the base level

[admin@MikroTik] > █
```

Command Line Interface

- `<tab>` completes command
- **double** `<tab>` shows available commands
- `'?'` shows help
- Navigate previous commands with `<↑>`,
`<↓>` buttons

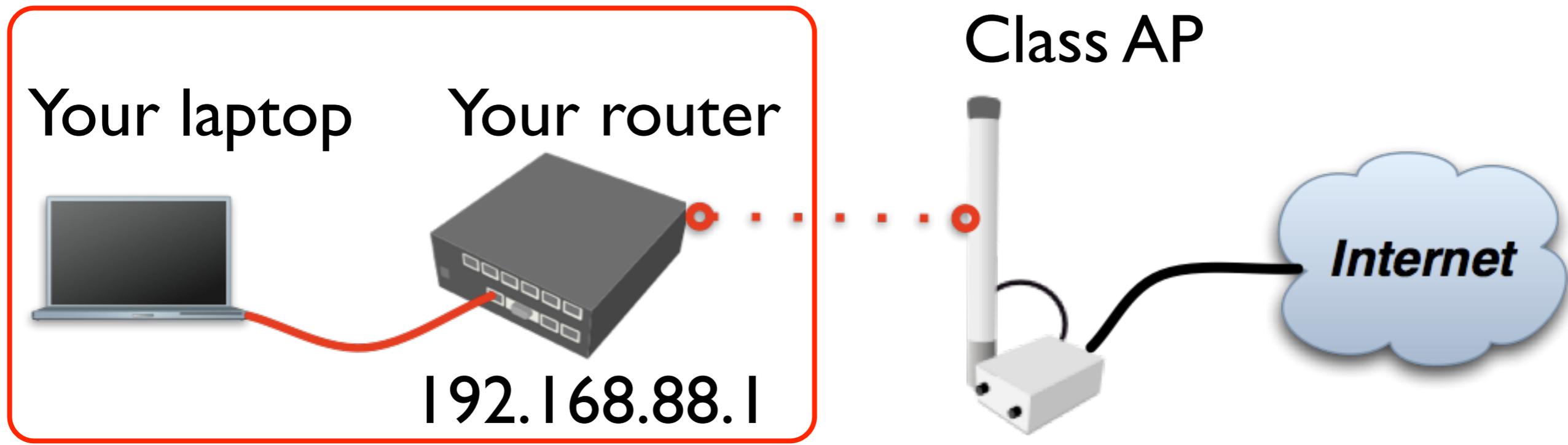
Command Line Interface

- Hierarchical structure (similar to WinBox menu)
- For more info see [console wiki page](#)

```
[admin@MikroTik] > /interface print
Flags: D - dynamic, X - disabled, R - running, S - slave
#   NAME                TYPE      ACTUAL-MTU L2MTU
0   S ether1-gateway      ether     1500      1598
1   RS ether2-master-local ether     1500      1598
2   S ether3-slave-local  ether     1500      1598
3   RS ether4-slave-local ether     1500      1598
4   R wlan1                wlan      1500      1600
5   R bridge-local        bridge    1500      1598
[admin@MikroTik] > █
```

In WinBox: Interfaces menu

Internet Access

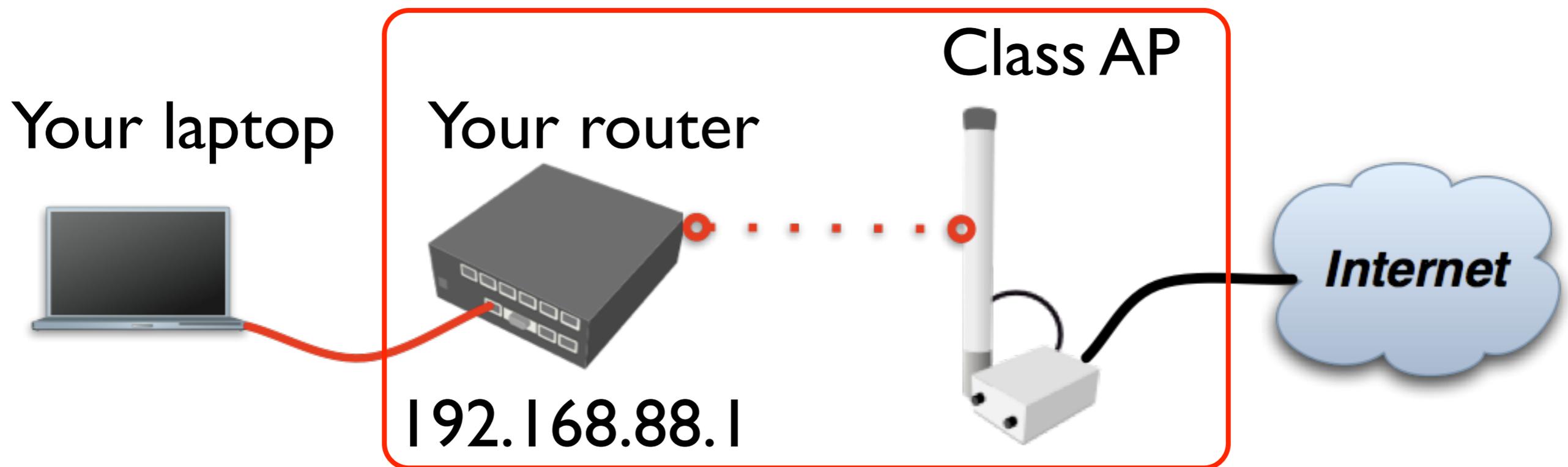


Laptop - Router

- Connect laptop to the router with a cable, plug it in any of LAN ports (2-5)
- Disable other interfaces (wireless) on your laptop
- Make sure that Ethernet interface is set to obtain IP configuration automatically (via DHCP)

Router - Internet

- The Internet gateway of your class is accessible over wireless - it is an access point (AP)



Router - Internet

- To connect to the AP you have to:
 - Remove the wireless interface from the bridge interface (used in default configuration)
 - Configure **DHCP** client to the wireless interface

Router - Internet

- To connect to the AP you have to:
 - Create and configure a wireless security profile
 - Set the wireless interface to station mode
 - And configure NAT masquerade

Router - Internet

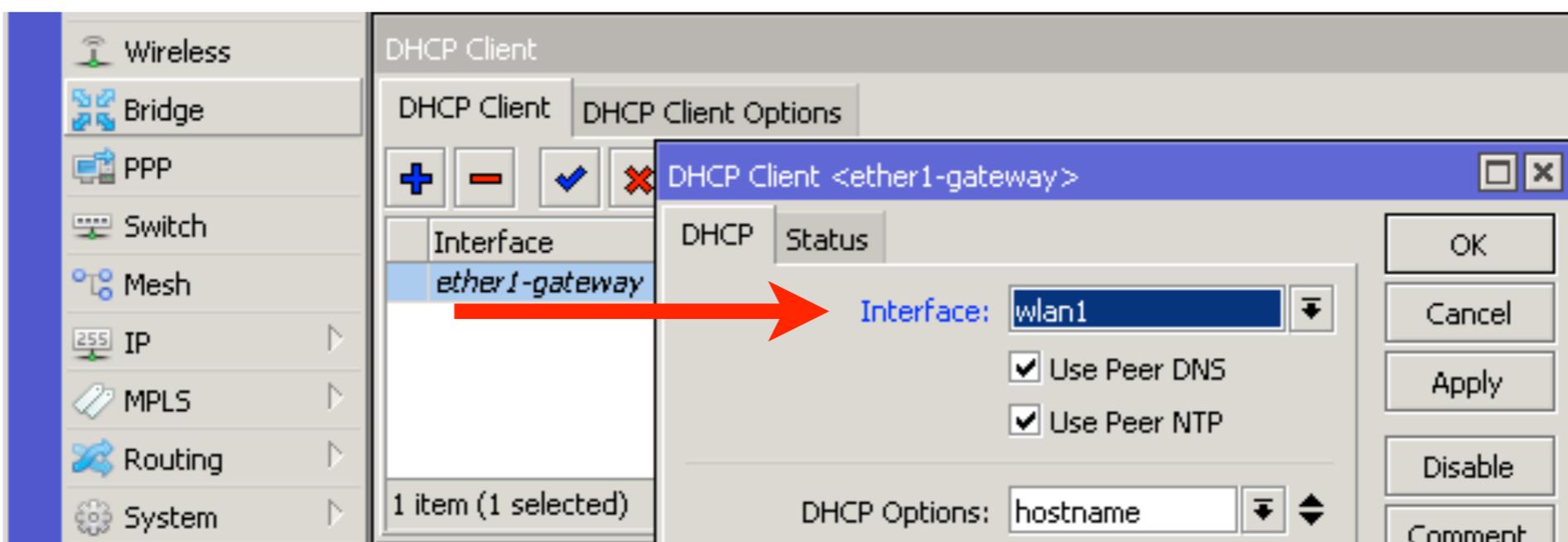
Remove the WiFi interface from the bridge

Interface	Bridge	Priority (...)	Path Cost	Horizon	Role
ether2-master-local	bridge-local	80	10		designated port
wlan1	bridge-local	80	10		disabled port

Bridge → Ports

Router - Internet

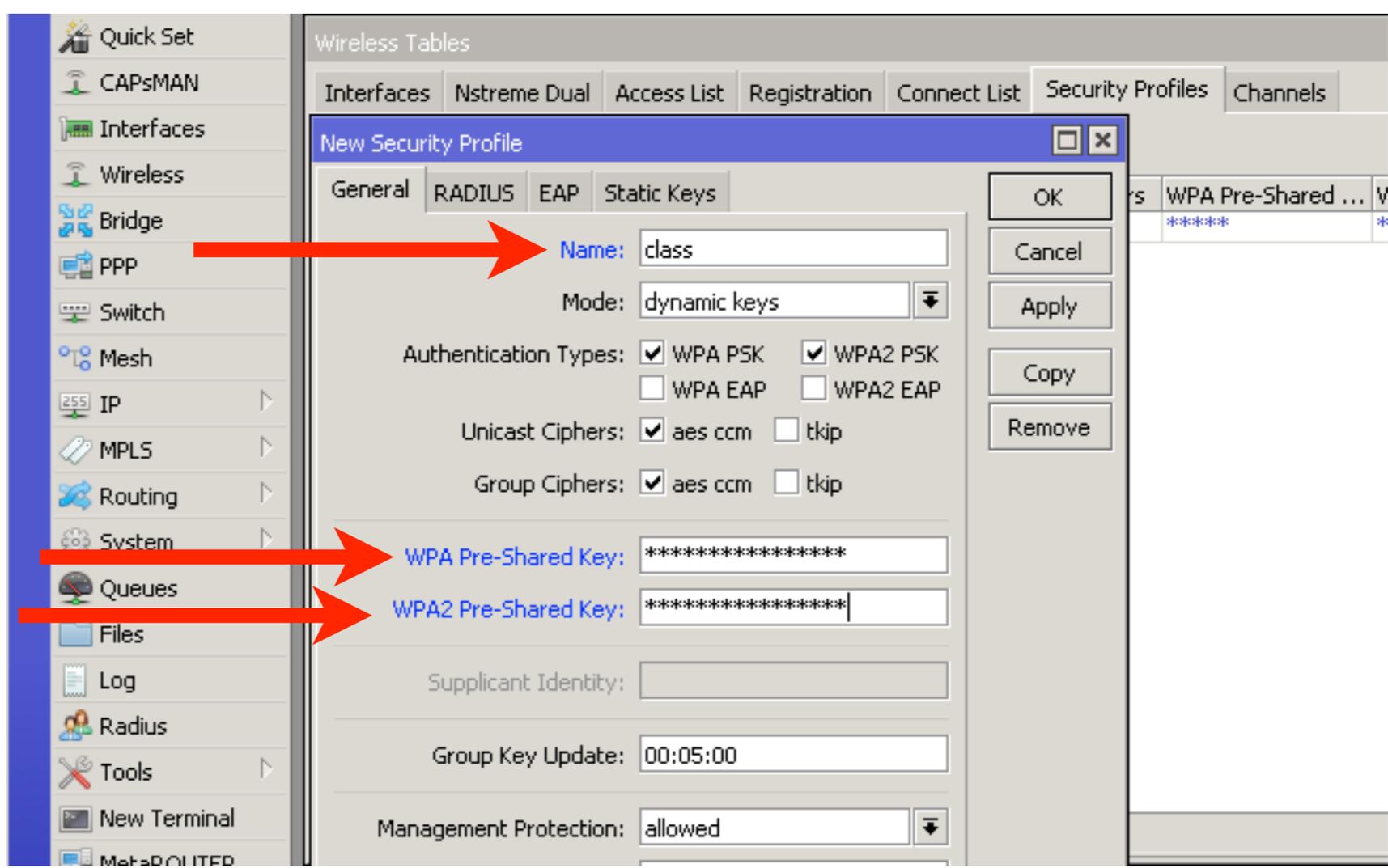
Set DHCP client to the WiFi interface



IP → DHCP Client

Router - Internet

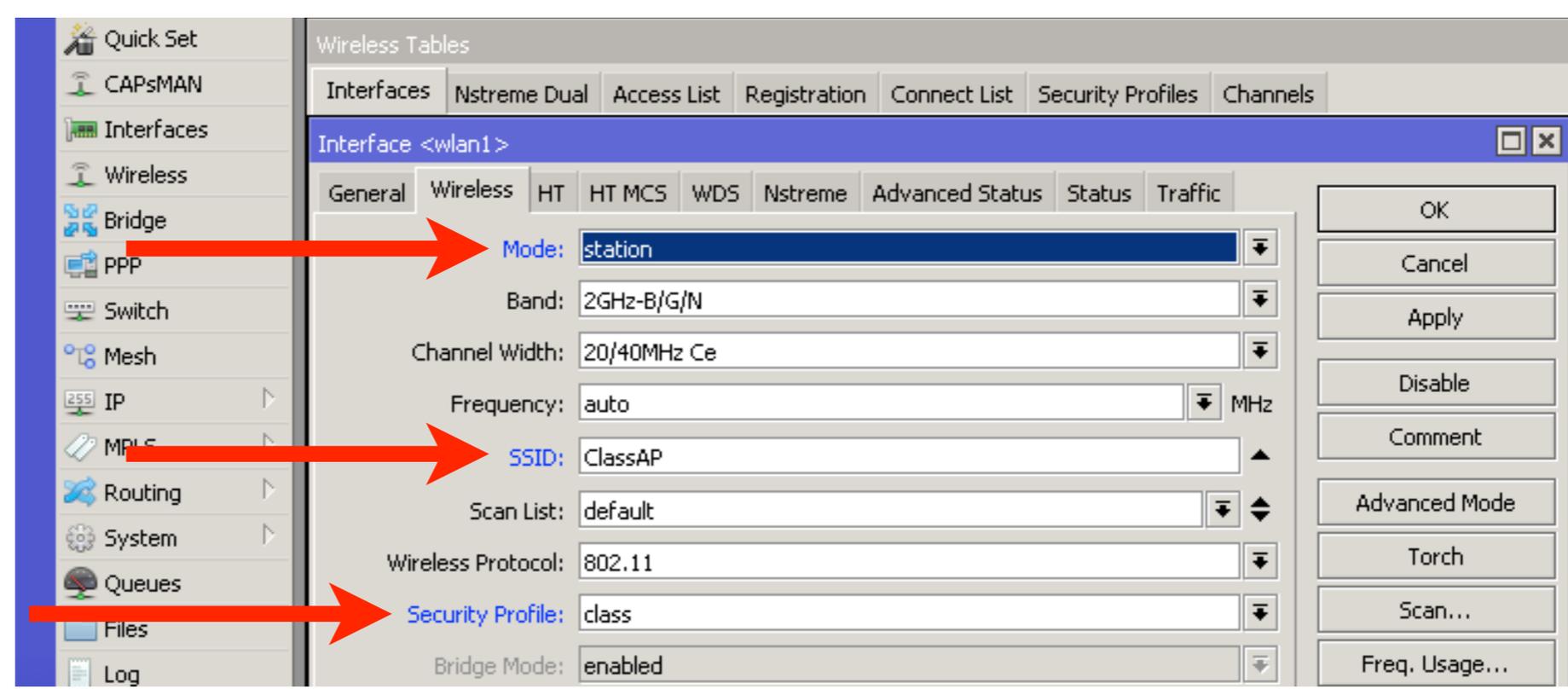
**Set Name
and
Pre-Shared
Keys**



Wireless → Security Profiles

Router - Internet

Set Mode to 'station', SSID to 'ClassAP' and Security Profile to 'class'

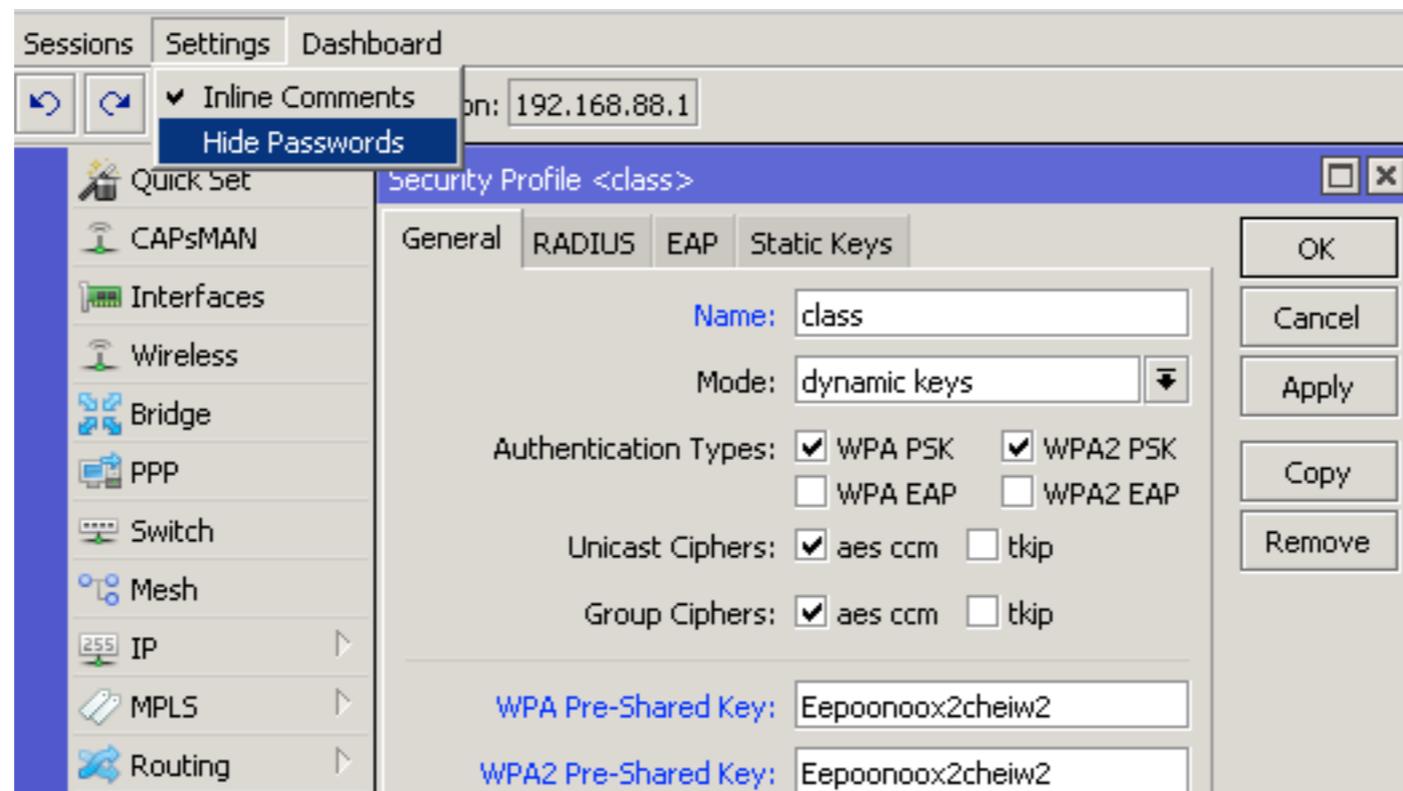


Wireless → Interfaces

- “Scan...” tool can be used to see and connect to available APs

WinBox Tip

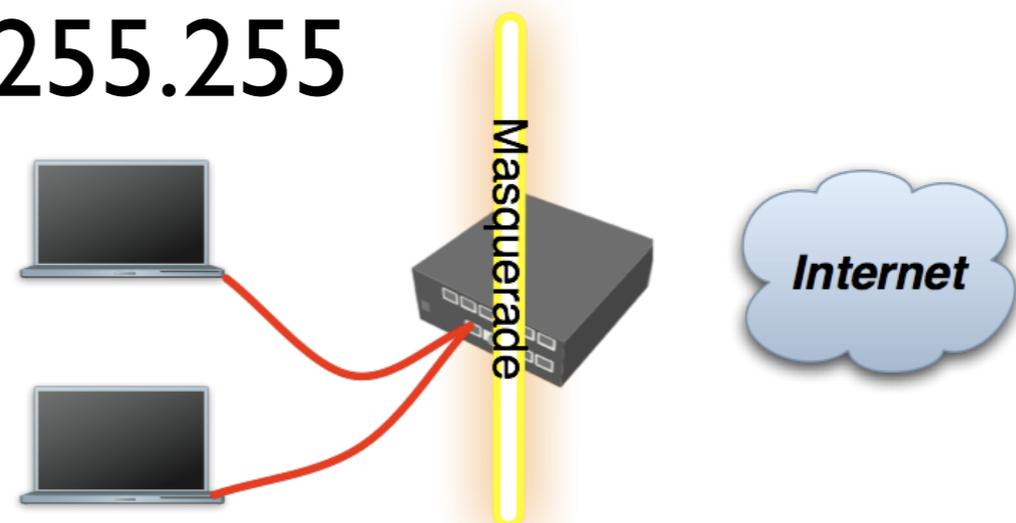
- To view hidden information (except user password), select Settings → Hide Passwords



Wireless → Security Profiles

Private and Public Space

- **Masquerade** is used for Public network access, where private addresses are present
- Private networks include
10.0.0.0-10.255.255.255,
172.16.0.0-172.31.255.255,
192.168.0.0-192.168.255.255



Router - Internet

Configure masquerade on the WiFi interface

Firewall

Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Interface	Out. Interface
0	masquerade	srcnat							ether1-gateway

NAT Rule <>

General Advanced Extra Action Statistics

Chain: srcnat

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

In. Interface:

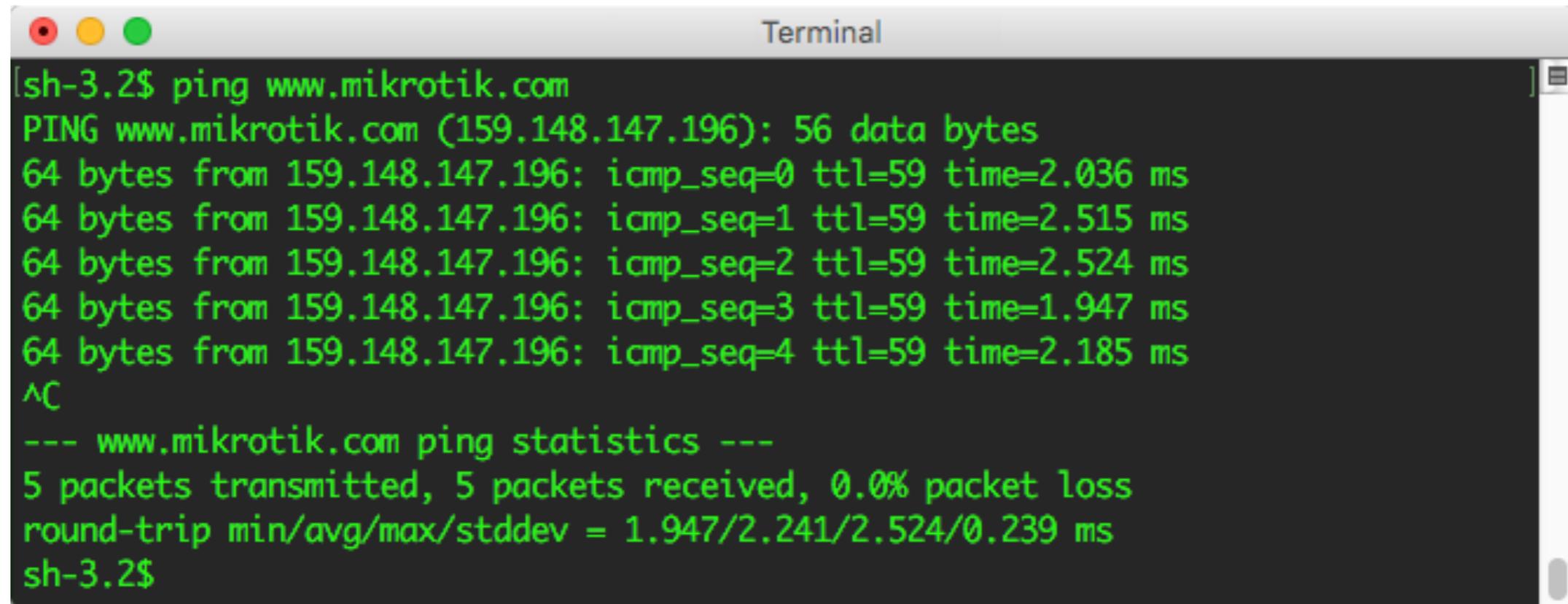
Out. Interface: wlan1

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

IP → Firewall → NAT

Check Connectivity

- Ping www.mikrotik.com from your laptop



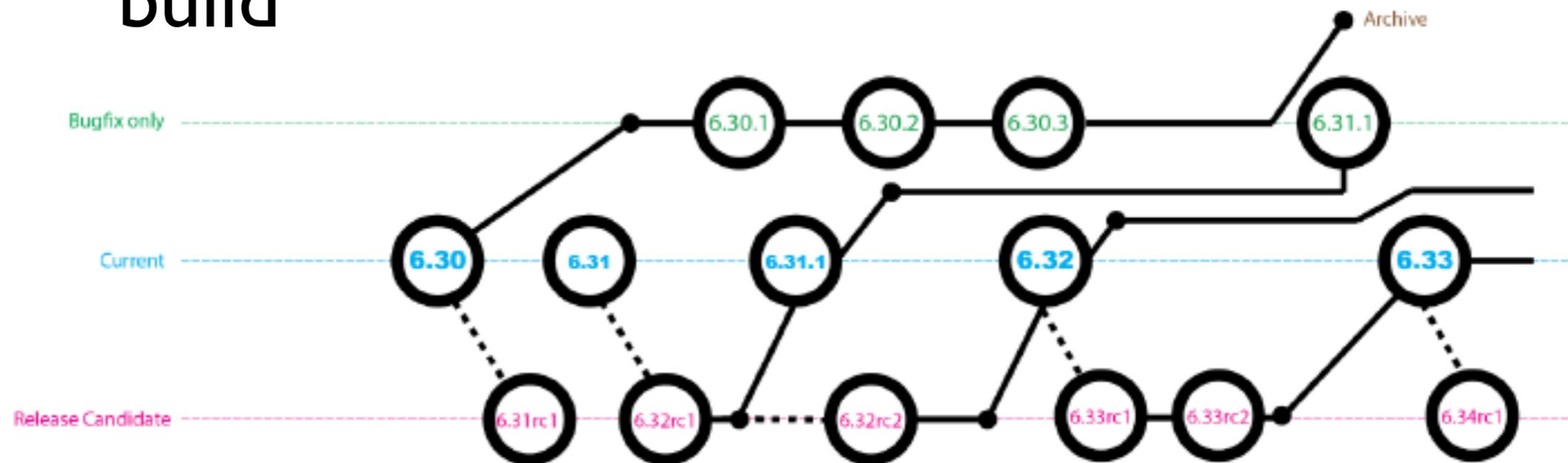
```
Terminal
[sh-3.2$ ping www.mikrotik.com
PING www.mikrotik.com (159.148.147.196): 56 data bytes
64 bytes from 159.148.147.196: icmp_seq=0 ttl=59 time=2.036 ms
64 bytes from 159.148.147.196: icmp_seq=1 ttl=59 time=2.515 ms
64 bytes from 159.148.147.196: icmp_seq=2 ttl=59 time=2.524 ms
64 bytes from 159.148.147.196: icmp_seq=3 ttl=59 time=1.947 ms
64 bytes from 159.148.147.196: icmp_seq=4 ttl=59 time=2.185 ms
^C
--- www.mikrotik.com ping statistics ---
5 packets transmitted, 5 packets received, 0.0% packet loss
round-trip min/avg/max/stddev = 1.947/2.241/2.524/0.239 ms
sh-3.2$
```

Troubleshooting

- The router cannot ping further than AP
- The router cannot resolve names
- The laptop cannot ping further than the router
- The laptop cannot resolve domain names
- Masquerade rule is not working

RouterOS Releases

- **Bugfix only** - fixes, no new features
- **Current** - same fixes + new features
- **Release Candidate** - consider as a 'nightly build'



Upgrading the RouterOS

- The easiest way to upgrade

The screenshot shows the Mikrotik WinBox interface. On the left is a sidebar with navigation options: Quick Set, CAPsMAN, Interfaces, Wireless, Bridge, PPP, Switch, Mesh, IP, MPLS, Routing, System, Queues, Files, and Log. The main window displays the 'Package List' section with a table of installed packages and a 'Check For Updates' dialog box.

Name	Version	Build Time	Scheduled
routeros-mipsbe	6.32.3	Oct/19/2015 11:13:47	
advanced-tools	6.32.3	Oct/19/2015 11:13:47	

The 'Check For Updates' dialog box shows the following information:

- Channel: current
- Installed Version: 6.32.3
- Latest Version: 6.33

Buttons in the dialog include OK, Download, and Download&Install. A text area below shows the release notes for version 6.33:

What's new in 6.33 (2015-Nov-02 14:51):

- *) certificate - added option to disable crl download in '/certificate settings';
- *) userman - fix report generation problem which could result in some users being skipped from it;
- *) hotspot - add login-timeout setting to force mac login for unauth hosts;
- *) hotspot - add mac-auth-mode setting for mac-as-passwd option;
- *) ipsec - fix set on multiple policies which could result in adding non existent

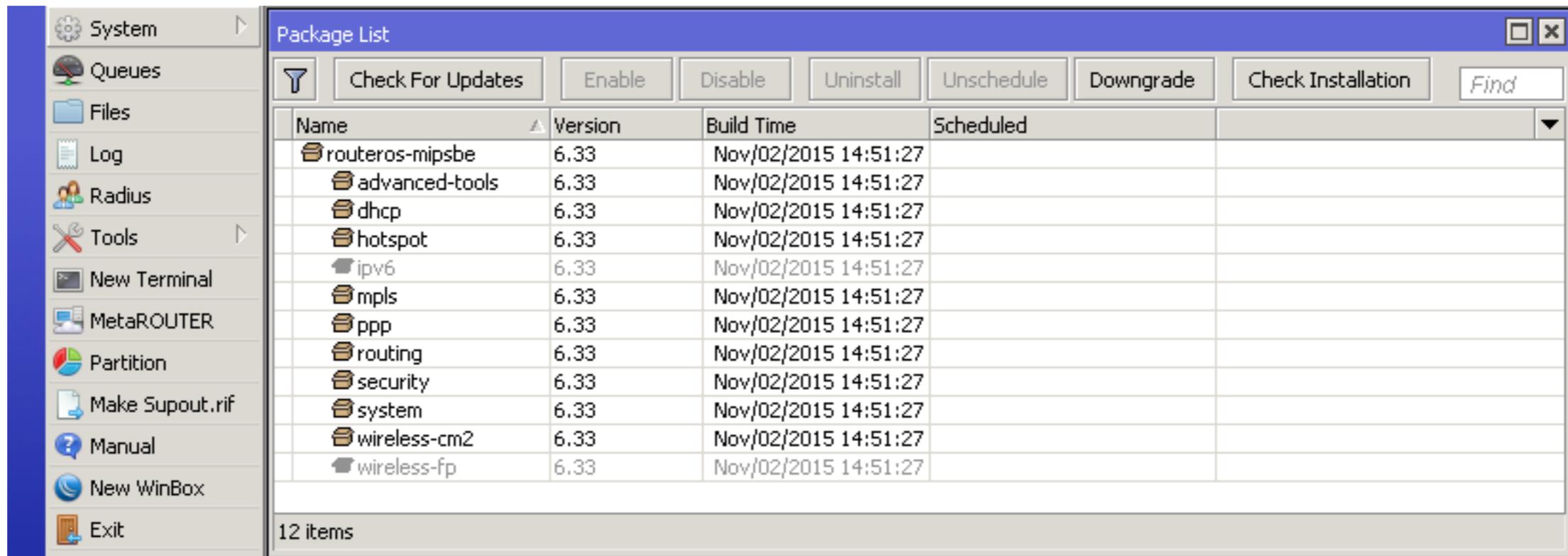
System → Packages → Check For Updates

Upgrading the RouterOS

- Download the update from www.mikrotik.com/download page
 - Check the architecture of your router's CPU
- Drag&drop into the WinBox window
 - Other ways: WebFig Files menu, FTP, sFTP
- Reboot the router

Package Management

- RouterOS functions are enabled/disabled by packages



The screenshot shows the Mikrotik WinBox interface. The left sidebar contains a menu with the following items: System, Queues, Files, Log, Radius, Tools, New Terminal, MetaROUTER, Partition, Make Supout.rif, Manual, New WinBox, and Exit. The 'System' menu item is selected. The main window is titled 'Package List' and contains a table of installed packages. The table has the following columns: Name, Version, Build Time, and Scheduled. The table contains 12 items, all with version 6.33 and build time Nov/02/2015 14:51:27. The 'System' package is highlighted in blue.

Name	Version	Build Time	Scheduled
routeros-mipsbe	6.33	Nov/02/2015 14:51:27	
advanced-tools	6.33	Nov/02/2015 14:51:27	
dhcp	6.33	Nov/02/2015 14:51:27	
hotspot	6.33	Nov/02/2015 14:51:27	
ipv6	6.33	Nov/02/2015 14:51:27	
mpls	6.33	Nov/02/2015 14:51:27	
ppp	6.33	Nov/02/2015 14:51:27	
routing	6.33	Nov/02/2015 14:51:27	
security	6.33	Nov/02/2015 14:51:27	
system	6.33	Nov/02/2015 14:51:27	
wireless-cm2	6.33	Nov/02/2015 14:51:27	
wireless-fp	6.33	Nov/02/2015 14:51:27	

System → Packages

RouterOS Packages

Package	Functionality
advanced-tools	Netwatch, wake-on-LAN
dhcp	DHCP client and server
hotspot	HotSpot captive portal server
ipv6	IPv6 support
ppp	PPP, PPTP, L2TP, PPPoE clients and servers
routing	Dynamic routing: RIP, BGP, OSPF
security	Secure WinBox, SSH, IPsec
system	Basic features: static routing, firewall, bridging, etc.
wireless-cm2	802.11 a/b/g/n/ac support, CAPsMAN v2

- For more info see [packages wiki page](#)

RouterOS Packages

- Each CPU architecture has a combined package, e.g. 'routeros-mipsbe', 'routeros-tile'
- Contains all the standard RouterOS features (wireless, dhcp, ppp, routing, etc.)
- Extra packages can be downloaded from www.mikrotik.com/download page

RouterOS Extra Packages

- Provides additional functionality
- Upload package file to the router and reboot

Package	Functionality
gps	GPS device support
ntp	Network Time Protocol server
ups	APC UPS management support
user-manager	MikroTik User Manager for managing HotSpot users

Package Management

- Disable the wireless package
- Reboot the router
- Observe the interface list
- Enable the wireless package
- Reboot the router

Package Management

- Observe WinBox System menu (no NTP client/server)
- Download extra packages file for your router's CPU architecture
- Install ntp package and reboot the router
- Observe WinBox System menu

Downgrading Packages

- From System → Packages menu
- ‘Check For Updates’ and choose different Channel (e.g. **bugfix-only**)
- Click ‘Download’
- Click ‘Downgrade’ in ‘Package List’ window

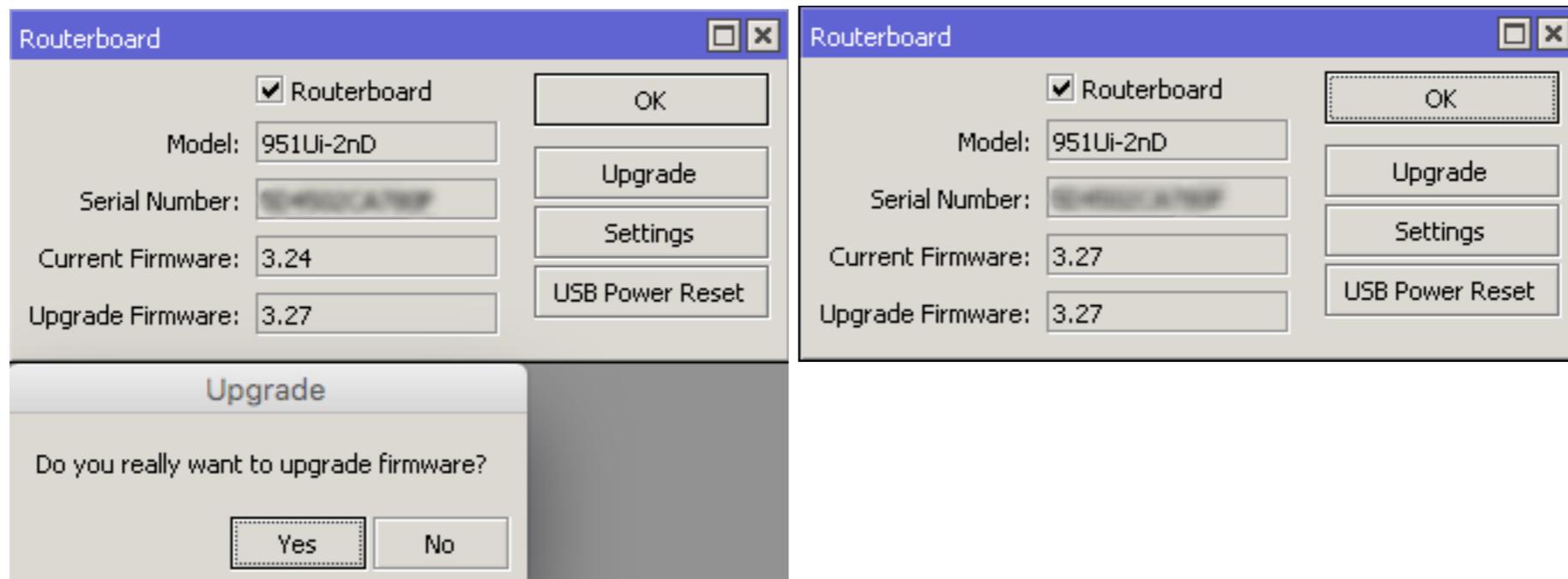
Downgrading Packages

- Downgrade RouterOS from **current** to **bugfix-only** version
- Upgrade it back to the **current** version

RouterBOOT

- Firmware responsible for starting RouterOS on RouterBOARD devices
- Two boot loaders on RouterBOARD - main and backup
- Main can be updated
- Backup loader can be loaded if needed

RouterBOOT



System → Routerboard

- For more info see [RouterBOOT wiki page](#)

Router Identity

- Option to set a name for each router
- Identity information available in different places



System → Identity

```
/          Move up to base level
..         Move up one level
/command   Use command at the base level
[admin@XY_YourName] >
```

admin@192.168.88.1 (XY_YourName) - WinBox v6.33 on hAP (mipsbe)

MAC Address	IP Address	Identity	Version	Board
D4:CA:6D:E2:65:90	192.168.88.1	XY_YourName	6.33 (stable)	RB951Ui-2nD

Router Identity

- Set the identity of your router as follows:
YourNumber(XY)_YourName
- For example: **13_JohnDoe**
- Observe the WinBox title menu

RouterOS Users

- Default user **admin**, group **full**
- Additional groups - **read** and **write**
- Can create your own group and fine tune access

RouterOS Users

The image displays two screenshots of the RouterOS web interface, illustrating the process of creating a user and a group.

Left Screenshot: User List and New User Dialog

The "User List" window shows a table with columns: Name, Group, Allowed Address, Last Logged In, and Comment. The "admin" user is listed with group "full" and last logged in on Nov/05/2015 13:39:59. Below the table is the "New User" dialog box with the following fields:

- Name: myuser
- Group: read
- Allowed Address: (empty)
- Last Logged In: (empty)
- Password: (empty)
- Confirm Password: (empty)

Buttons include OK, Cancel, Apply, Disable, Comment, Copy, and Remove. The "enabled" checkbox is checked.

Right Screenshot: User List and New Group Dialog

The "User List" window shows a table with columns: Name, Policies, and Skin. The "full", "read", and "write" groups are listed. Below the table is the "New Group" dialog box with the following fields:

- Name: mygroup
- Policies: (checkboxes for local, telnet, ssh, ftp, reboot, read, write, policy, test, winbox, password, web, sniff, sensitive, api)
- Skin: default

Buttons include OK, Cancel, Apply, Comment, Copy, and Remove.

System → Users

RouterOS Users

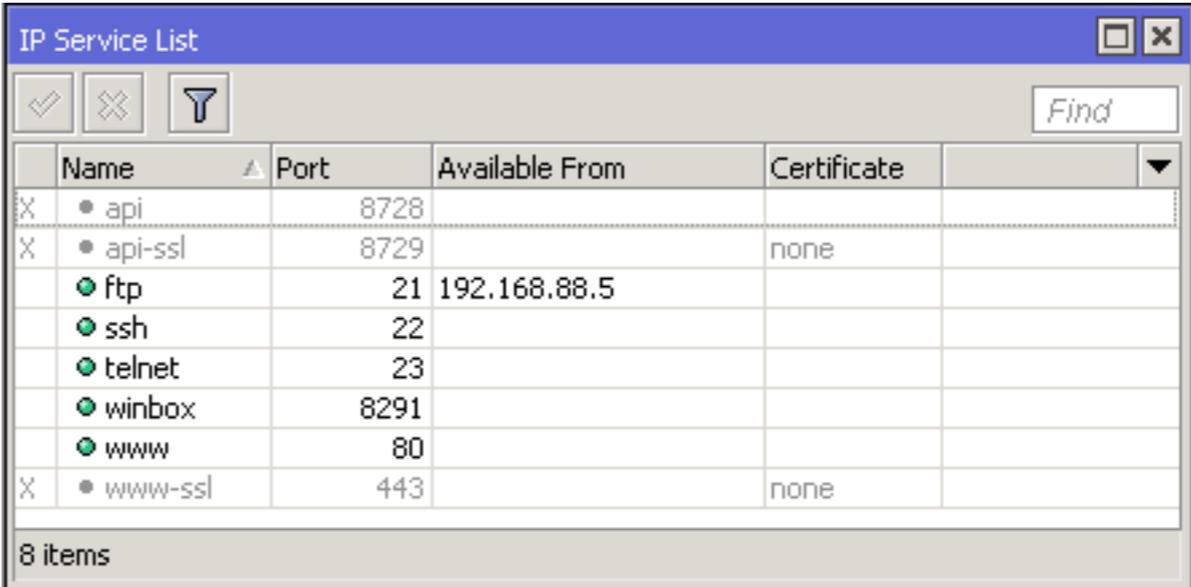
- Add a new user to the RouterOS with **full access** (*note name and password*)
- Change admin user group to read
- Login with the new user
- Login with the admin user and try to change router's settings (not possible)

RouterOS Users

- Generate SSH private/public key pair using 'ssh-keygen' (OS X and Linux) or 'puttygen' (Windows)
- Upload the public part of the key to the router
- Import and attach it to the user
- Login to the router using the private key

RouterOS Services

- Different ways to connect to the RouterOS
- API - Application Programming Interface
- FTP - for uploading/downloading files to/from the RouterOS



The screenshot shows the 'IP Service List' window in RouterOS. It contains a table with the following data:

	Name	Port	Available From	Certificate	
X	• api	8728			
X	• api-ssl	8729		none	
	• ftp	21	192.168.88.5		
	• ssh	22			
	• telnet	23			
	• winbox	8291			
	• www	80			
X	• www-ssl	443		none	

8 items

IP → Services

RouterOS Services

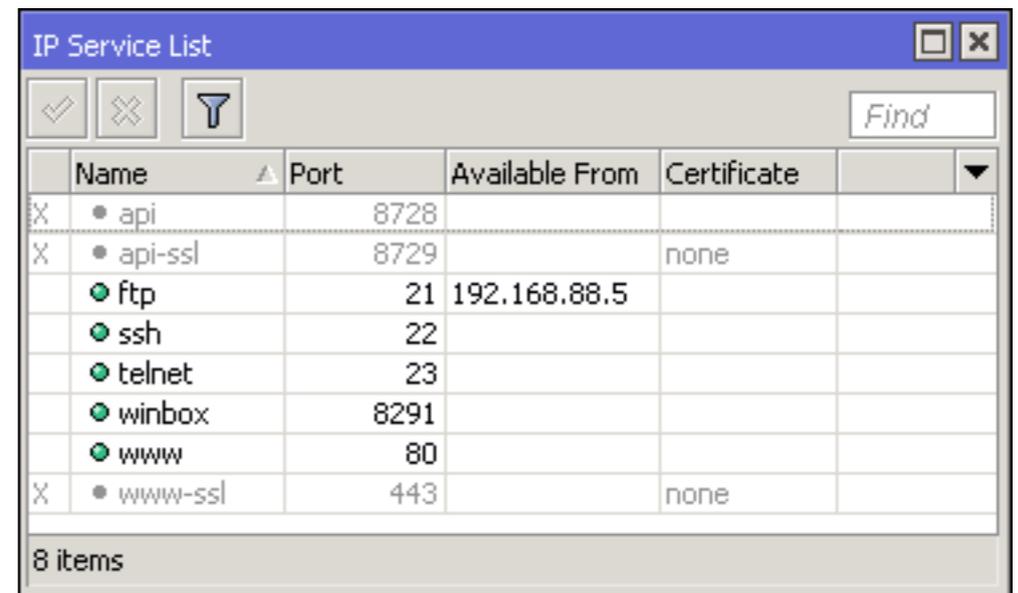
- SSH - secure command line interface
- Telnet - insecure command line interface
- WinBox - GUI access
- WWW - access from the web browser

	Name	Port	Available From	Certificate
X	• api	8728		
X	• api-ssl	8729		none
	• ftp	21	192.168.88.5	
	• ssh	22		
	• telnet	23		
	• winbox	8291		
	• www	80		
X	• www-ssl	443		none

IP → Services

RouterOS Services

- Disable services which are not used
- Restrict access with 'available from' field
- Default ports can be changed



	Name	Port	Available From	Certificate	
X	• api	8728			
X	• api-ssl	8729		none	
	• ftp	21	192.168.88.5		
	• ssh	22			
	• telnet	23			
	• winbox	8291			
	• www	80			
X	• www-ssl	443		none	

8 items

IP → Services

RouterOS Services

- Open RouterOS web interface - <http://192.168.88.1>
- In WinBox disable www service
- Refresh browser page

Configuration Backup

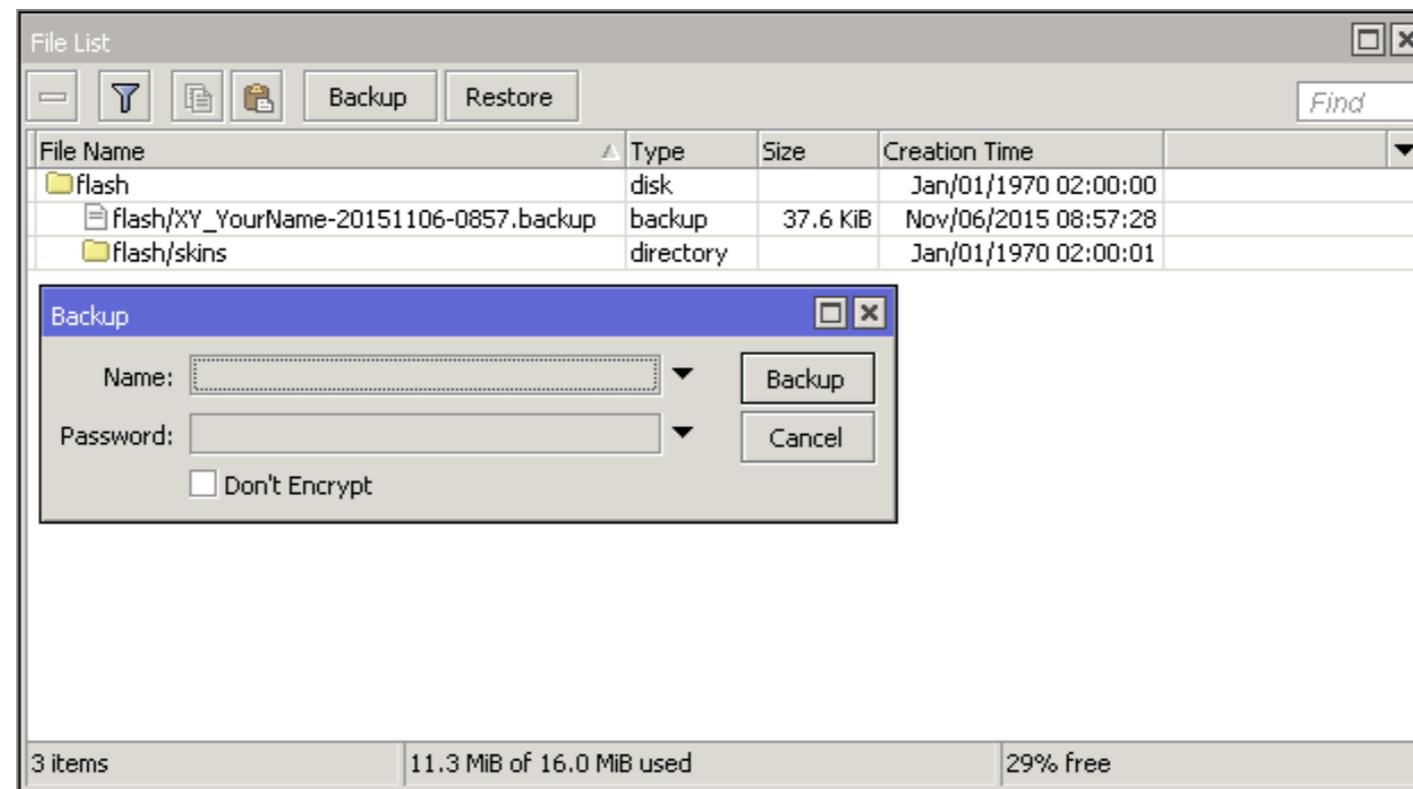
- Two types of backups
- Backup (.backup) file - used for restoring configuration **on the same router**
- Export (.rsc) file - used for moving configuration to **another router**

Configuration Backup

- Backup file can be created and restored under Files menu in WinBox
- Backup file is binary, by default encrypted with user password. Contains a full router configuration (passwords, keys, etc.)

Configuration Backup

- Custom name and password can be entered
- Router identity and current date is used as a backup file name



Configuration Backup

- Export (.rsc) file is a script with which router configuration can be backed up and restored
- Plain-text file (editable)
- Contains only configuration that is different than the factory default configuration

Configuration Backup

- Export file is created using 'export' command in CLI
- Whole or partial router configuration can be saved to an export file
- RouterOS user passwords are not saved when using export

Configuration Backup

```
[admin@XY_YourName] > /export file=flash/router_conf_20151106
[admin@XY_YourName] > /file print
# NAME                                TYPE                                SIZE  CREATION-TIME
0 flash                               disk                                jan/01/1970 02:00:00
1 flash/skins                         directory                           jan/01/1970 02:00:01
2 flash/XY_YourName-20151106-0939.backup 37.6KiB nov/06/2015 09:39:10
3 flash/router_conf_20151106.rsc       script                               3595  nov/06/2015 09:40:35
[admin@XY_YourName] >
```

- Store files in 'flash' folder
- Contains ready to use RouterOS commands

```
[admin@XY_YourName] > /export
# nov/06/2015 09:46:57 by RouterOS 6.33
# software id = 85WZ-DDQS
#
/interface bridge
add admin-mac=D4:CA:6D:E2:65:90 auto-mac=no name=bridge-local
/interface ethernet
set [ find default-name=ether1 ] name=ether1-gateway
set [ find default-name=ether2 ] name=ether2-master-local
set [ find default-name=ether3 ] master-port=ether2-master-local name=ether3-slave-local
set [ find default-name=ether4 ] master-port=ether2-master-local name=ether4-slave-local
set [ find default-name=ether5 ] master-port=ether2-master-local name=ether5-slave-local
/ip neighbor discovery
set ether1-gateway discover=no
/interface wireless security-profiles
set [ find default=yes ] supplicant-identity=MikroTik
add authentication-types=wpa-psk,wpa2-psk eap-methods="" management-protection=allowed mode=dynamic-keys name=\
class supplicant-identity="" wpa-pre-shared-key=baelezaice3leiM wpa2-pre-shared-key=baelezaice3leiM
```

Configuration Backup

- Export file can be edited by hand
- Can be used to move configuration to a different RouterBOARD
- Restore using '/import' command

```
[admin@XY_YourName] > /import flash/router_conf_20151106.rsc
```

```
Script file loaded and executed successfully
```

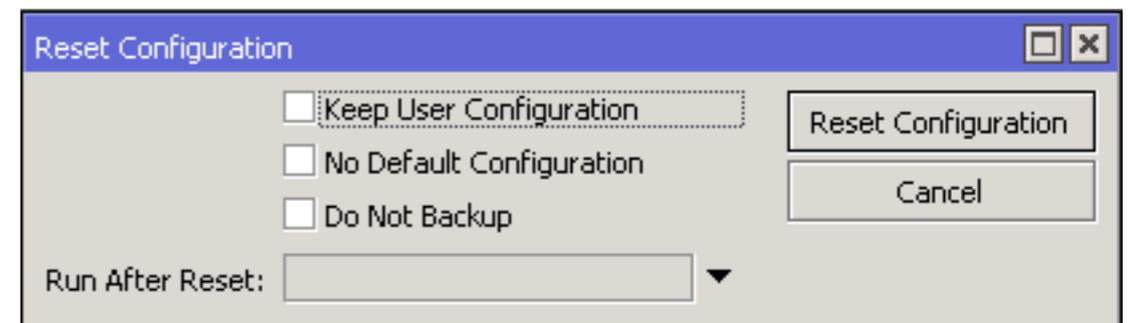
```
[admin@XY_YourName] > █
```

Configuration Backup

- Download to a computer using WinBox (drag&drop), FTP or WebFig
- Don't store the copy of the backup only on the router! It is not a good backup strategy!

Reset Configuration

- Reset to default configuration
- Retain RouterOS users after reset
- Reset to a router without any configuration ('blank')
- Run a script after reset



System → Reset Configuration

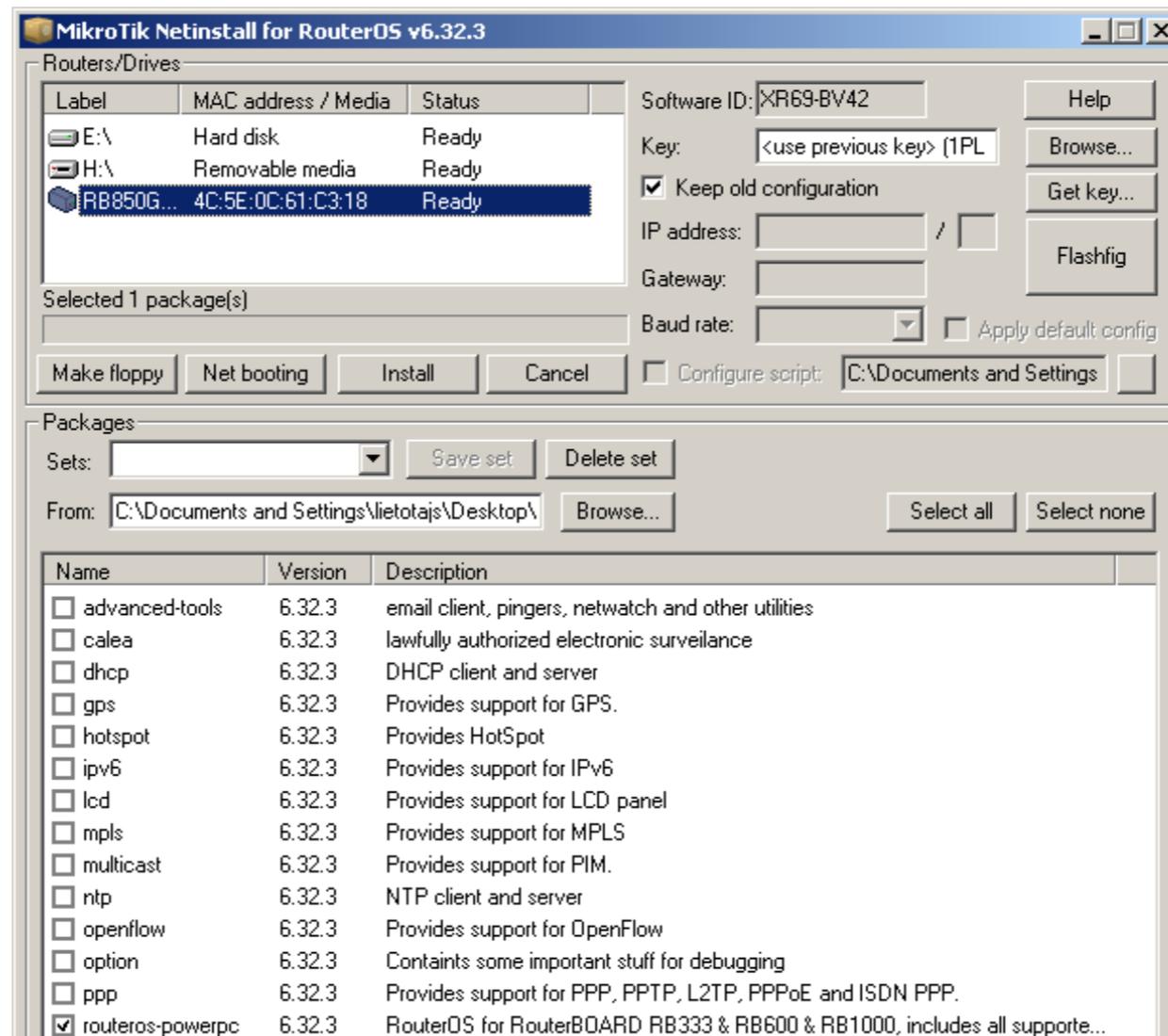
Reset Configuration

- Using physical 'reset' button on the router
 - Load backup RouterBOOT loader
 - Reset router configuration
 - Enable CAPs mode (Controlled AP)
 - Start in Netinstall mode
- For more info see [reset button wiki page](#)

Netinstall

- Used for installing and reinstalling RouterOS
- Direct network connection to the router is required (can be used over switched LAN)
- Cable must be connected to Ether1 port (except CCR and RB1xxx - last port)
- Runs on Windows
- For more info see [Netinstall wiki page](#)

Netinstall



- Available at www.mikrotik.com/download

Configuration Backup

- Create a .backup file
- Copy it to your laptop
- Delete the .backup file from the router
- Reset router configuration
- Copy .backup file back to the router
- Restore router configuration

Configuration Backup

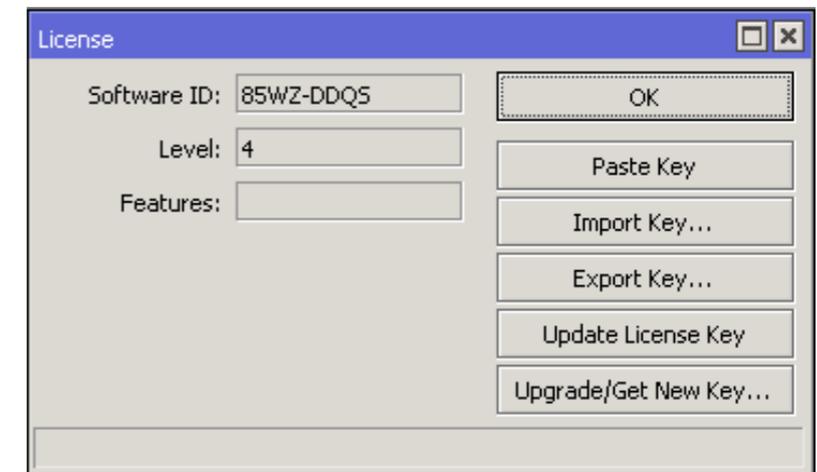
- Create a backup using 'export' command
- Copy it to your laptop
- Delete the export file from the router
- Reset router configuration
- Copy export file back to the router
- Restore router configuration

Netinstall

- Download Netinstall
- Boot your router in Netinstall mode
- Install RouterOS on your router using Netinstall
- Restore configuration from previously saved backup file

RouterOS License

- All RouterBOARDs are shipped with a license
- Different license levels (features)
- RouterOS updates for life
- x86 license can be purchased from www.mikrotik.com or distributors



System → License

RouterOS License

Level	Type	Typical Use
0	Trial Mode	24h trial
1	Free Demo	
3	CPE	Wireless client (station), volume only
4	AP	Wireless AP: WISP, HOME, Office
5	ISP	Supports more tunnels than L4
6	Controller	Unlimited RouterOS features

Additional Information

- wiki.mikrotik.com - RouterOS documentation and examples
- forum.mikrotik.com - communicate with other RouterOS users
- mum.mikrotik.com - MikroTik User Meeting page
- Distributor and consultant support
- support@mikrotik.com

Module 1 Summary



Certified Network Associate (MTCNA)

Module 2

DHCP

DHCP

- Dynamic Host Configuration Protocol
- Used for automatic IP address distribution over a local network
- Use DHCP only in trusted networks
- Works within a broadcast domain
- RouterOS supports both DHCP client and server

DHCP Client

- Used for automatic acquiring of IP address, subnet mask, default gateway, DNS server address and additional settings if provided
- MikroTik SOHO routers by default have DHCP client configured on ether1 (WAN) interface

DHCP Client

The screenshot displays the Mikrotik WinBox DHCP Client configuration interface. At the top, there are tabs for 'DHCP Client' and 'DHCP Client Options'. Below the tabs is a toolbar with icons for adding, deleting, and refreshing entries, along with 'Release' and 'Renew' buttons. A table lists the DHCP clients:

Interface	Use Peer DNS	Add Default Route	IP Address	Expires After	Status
wlan1	yes	yes	10.5.120.243/24	00:20:57	bound

Below the table, two sub-windows are open, both titled 'DHCP Client <wlan1>'. The left sub-window shows the configuration for the DHCP client on the wlan1 interface. It includes fields for 'Interface' (wlan1), 'Use Peer DNS' (checked), 'Use Peer NTP' (checked), 'DHCP Options' (hostname, clientid), 'Add Default Route' (yes), and 'Default Route Distance' (1). The right sub-window shows the status of the DHCP client, including 'IP Address' (10.5.120.243/24), 'Gateway' (10.5.120.1), 'DHCP Server' (10.5.120.2), 'Expires After' (00:21:25), 'Primary DNS' (10.5.120.1), 'Secondary DNS', 'Primary NTP' (10.5.8.1), 'Secondary NTP', and 'CAPS Managers'. Both sub-windows have 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', 'Release', and 'Renew' buttons. The status bar at the bottom of each sub-window shows 'enabled' and 'Status: bound'.

IP → DHCP Client

DNS

- By default DHCP client asks for a DNS server IP address
- It can also be entered manually if other DNS server is needed or DHCP is not used

DNS Settings

Servers: 8.8.8.8

Dynamic Servers: 10.5.8.1

Allow Remote Requests

Max UDP Packet Size: 4096

Query Server Timeout: 2.000 s

Query Total Timeout: 10.000 s

Cache Size: 2048 KIB

Cache Max TTL: 7d 00:00:00

Cache Used: 202

OK

Cancel

Apply

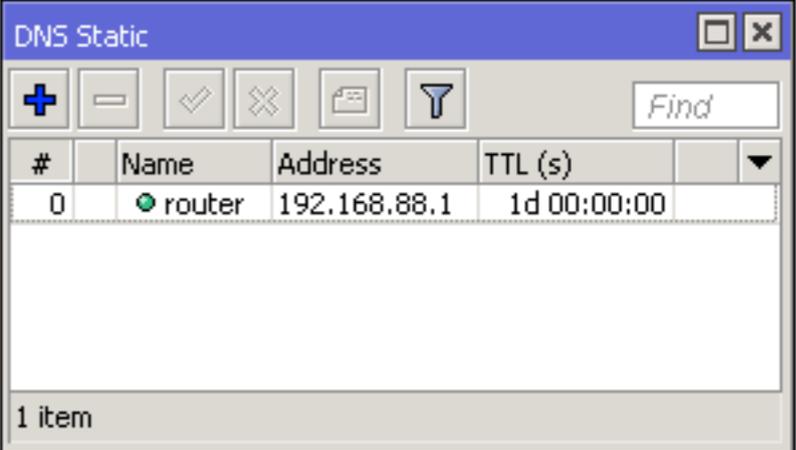
Static

Cache

IP → DNS

DNS

- RouterOS supports static DNS entries
- By default there's a static DNS A record named **router** which points to **192.168.88.1**
- That means you can access the router by using DNS name instead of IP
- <http://router>



#	Name	Address	TTL (s)
0	router	192.168.88.1	1d 00:00:00

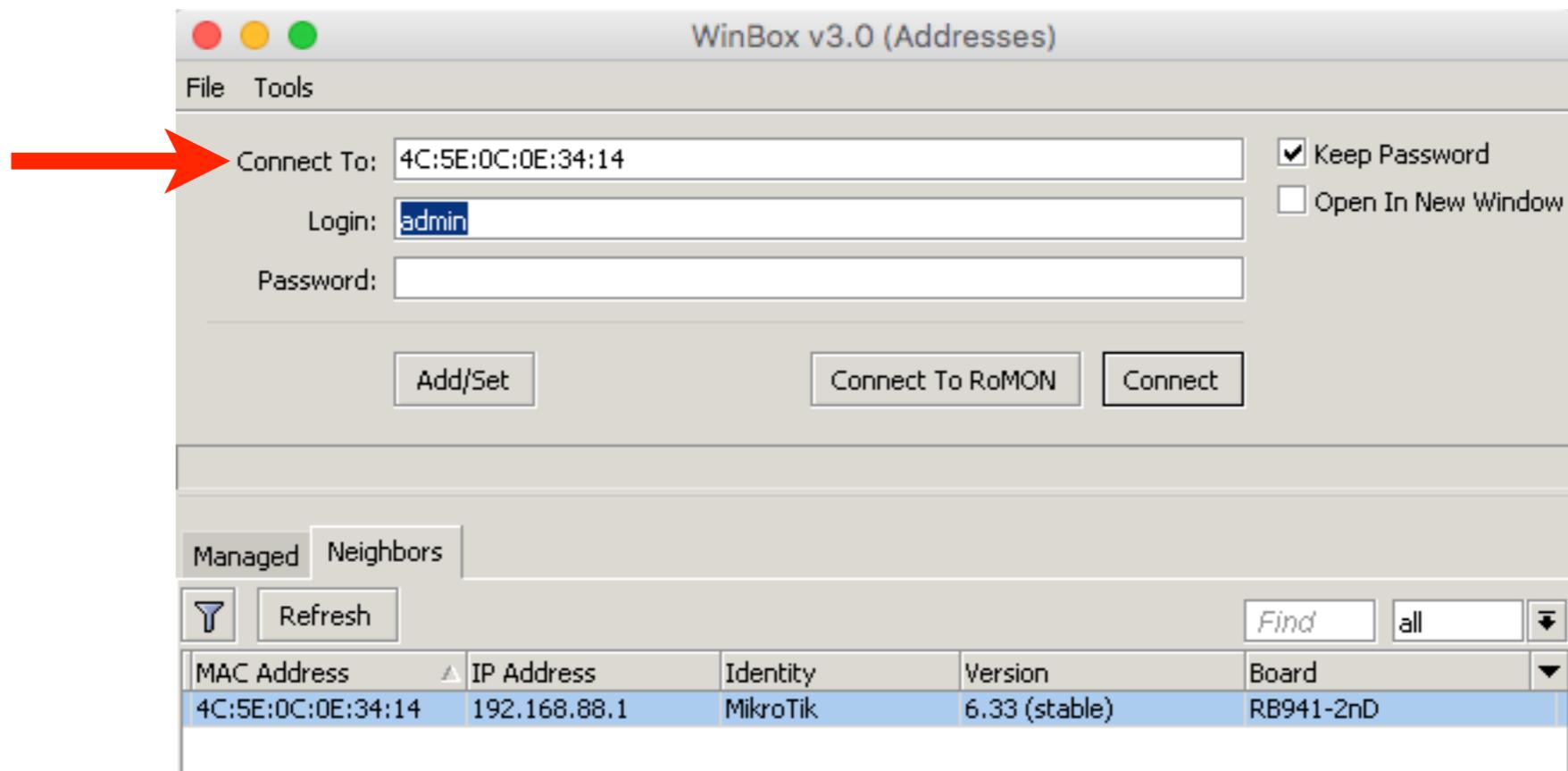
IP → DNS → Static

DHCP Server

- Automatically assigns IP addresses to requesting hosts
- IP address should be configured on the interface which DHCP Server will use
- To enable use 'DHCP Setup' command

DHCP Server

- Disconnect from the router
- Reconnect using the router's MAC address



DHCP Server

- We're going to remove existing DHCP Server and setup a new one
- Will use your number (XY) for the subnet, e.g. 192.168.XY.0/24
- To enable DHCP Server on the bridge, it must be configured on the **bridge interface** (not on the bridge port)

DHCP Server

**Remove
DHCP Server**



Name	Interface	Relay	Lease Time	Address Pool	Add ARP For Leases
default	bridge-local		00:10:00	unknown	no

1 item (1 selected)

**Remove
DHCP Network**



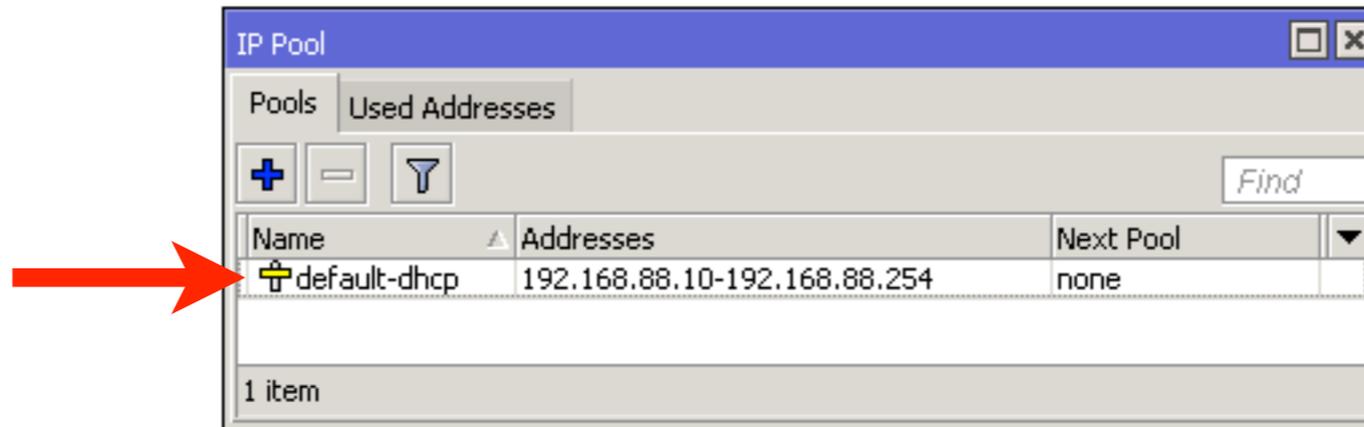
Address	Gateway	DNS Servers	Domain	WINS Servers	Next Ser...
;;; default configuration					
192.168.88.0/24	192.168.88.1				

1 item (1 selected)

IP → DHCP Server

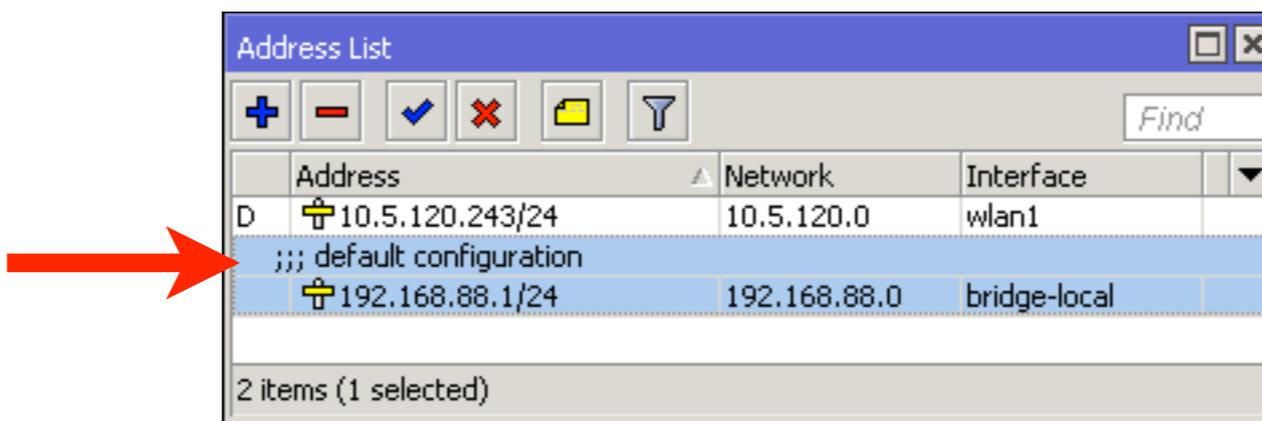
DHCP Server

**Remove
IP Pool**



IP → Pool

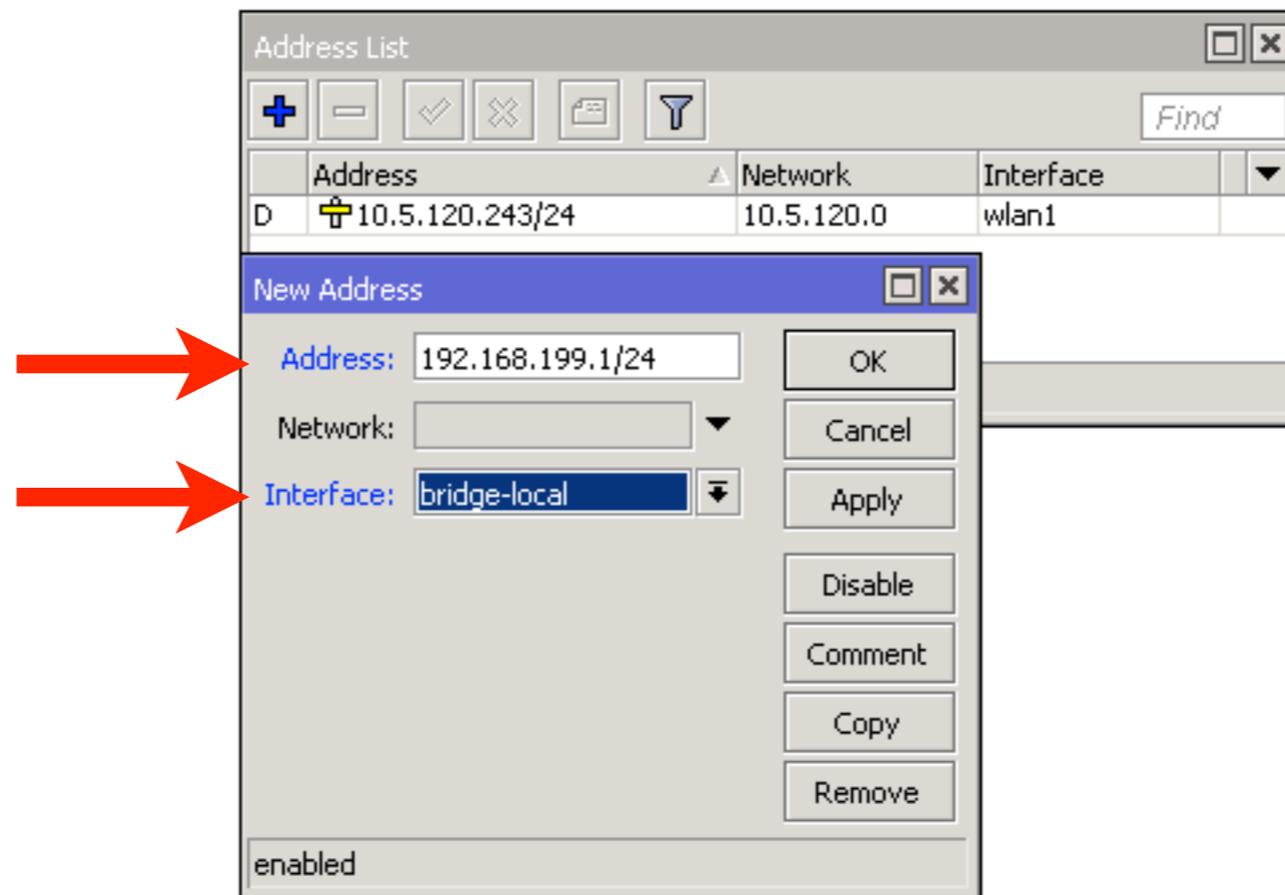
**Remove
IP Address**



IP → Address

DHCP Server

**Add IP Address
192.168.XY.1/24
on the bridge
interface**



- For example, XY=199

DHCP Server

<p>DHCP Setup</p> <p>Select interface to run DHCP server on</p> <p>DHCP Server Interface: <input type="text" value="bridge-local"/></p> <p>1</p> <p>Back Next Cancel</p>	<p>DHCP Setup</p> <p>Select network for DHCP addresses</p> <p>DHCP Address Space: <input type="text" value="192.168.199.0/24"/></p> <p>2</p> <p>Back Next Cancel</p>
<p>DHCP Setup</p> <p>Select gateway for given network</p> <p>Gateway for DHCP Network: <input type="text" value="192.168.199.1"/></p> <p>3</p> <p>Back Next Cancel</p>	<p>DHCP Setup</p> <p>Select pool of ip addresses given out by DHCP server</p> <p>Addresses to Give Out: <input type="text" value="192.168.199.2-192.168.199.254"/></p> <p>4</p> <p>Back Next Cancel</p>
<p>DHCP Setup</p> <p>Select DNS servers</p> <p>DNS Servers: <input type="text" value="10.5.120.1"/></p> <p>5</p> <p>Back Next Cancel</p>	<p>DHCP Setup</p> <p>Select lease time</p> <p>Lease Time: <input type="text" value="00:10:00"/></p> <p>6</p> <p>Back Next Cancel</p>

IP → DHCP Server → DHCP Setup

DHCP Server

- Disconnect from the router
- Renew the IP address of your laptop
- Connect to the router's new IP address
192.168.XY.1
- Check that the connection to the Internet is available

DHCP Server

- DHCP Server Setup wizard has created a new IP pool and DHCP Server

	Address	Network	Interface
D	10.5.120.243/24	10.5.120.0	wlan1
	192.168.199.1/24	192.168.199.0	bridge-local

2 items

Name	Addresses	Next Pool
dhcp_pool1	192.168.199.2-192.168.199.254	none

1 item

Name	Interface	Relay	Lease Time	Address Pool	Add ARP For Leases
dhcp1	bridge-local		00:10:00	dhcp_pool1	no

1 item

DHCP Static Leases

- It is possible to always assign the same IP address to the same device (identified by MAC address)
- DHCP Server could even be used without dynamic IP pool and assign only preconfigured addresses

DHCP Static Leases

The screenshot shows the Mikrotik WinBox DHCP Server interface. The 'Leases' tab is active, displaying a table with one lease entry. A dialog box titled 'DHCP Lease <192.168.199.254,192.168.199.254>' is open, showing the details of the selected lease. The 'Make Static' button is highlighted with a red arrow, and a red text box below it says 'Convert dynamic lease to static'.

Address	MAC Address	Client ID	Server	Active Address	Active MAC Address	Active Host Name	Expires After	Status
D				192.168.199.254	00:1E:C2:FB:F8:36	Kk	00:06:47	bound

DHCP Lease <192.168.199.254,192.168.199.254>

Active

Active Address: 192.168.199.254

Active MAC Address: 00:1E:C2:FB:F8:36

Active Client ID: 1:0:1e:c2:fb:f8:36

Active Host Name: Kk

Active Server: dhcp1

Expires After: 00:06:47

Last Seen: 00:03:13

Agent Circuit Id:

Agent Remote Id:

dynamic enabled radius blocked bound

OK

Copy

Remove

Make Static

Check Status

Convert dynamic lease to static

IP → DHCP Server → Leases

DHCP Static Leases

- Set DHCP Address Pool to static-only
- Create a static lease for your laptop
- Change the IP address assigned to your laptop by DHCP server to 192.168.XY.123
- Renew the IP address of your laptop
- Ask your neighbor to connect his/her laptop to your router (will not get an IP address)

ARP

- Address Resolution Protocol
- ARP joins together client's IP address (Layer3) with MAC address (Layer2)
- ARP operates dynamically
- Can also be configured manually

ARP Table

- Provides information about IP address, MAC address and the interface to which the device is connected

	IP Address	MAC Address	Interface
D	10.5.120.2	4C:5E:0C:0A:0F:9A	wlan1
D	192.168.199.254	00:1E:C2:FB:F8:36	bridge-local

IP → ARP

Static ARP

- For increased security ARP entries can be added manually
- Network interface can be configured to **reply-only** to known ARP entries
- Router's client will not be able to access the Internet using a different IP address

Static ARP

The image shows two overlapping windows from the Mikrotik WinBox interface. The left window, titled 'ARP List', displays a table of ARP entries. The right window, titled 'ARP <192.168.199.199>', shows the configuration for a specific entry.

	IP Address	MAC Address	Interface
D	10.5.120.1	4C:5E:0C:0A:0F:9A	wlan1
D	10.5.120.2	4C:5E:0C:0A:0F:9A	wlan1
D	192.168.199.199	00:1E:C2:FB:F8:36	bridge-local

3 items (1 selected)

Static ARP entry →

ARP <192.168.199.199> configuration:

- IP Address: 192.168.199.199
- MAC Address: 00:1E:C2:FB:F8:36
- Interface: bridge-local
- Published

Buttons: OK, Copy, Remove, Make Static, Ping, MAC Ping, Telnet, MAC Telnet, Torch

dynamic | enabled | published

IP → ARP

Static ARP

**Interface will
reply only to
known ARP
entries**

The screenshot shows the Mikrotik WinBox configuration window for an interface named 'bridge-local'. The 'General' tab is active, and the 'ARP' dropdown menu is set to 'reply-only'. A red arrow points from the text on the left to this dropdown menu. Other fields include Name (bridge-local), Type (Bridge), MTU (1500), Actual MTU (1500), L2 MTU (1598), MAC Address (D4:CA:6D:E2:65:90), and Admin. MAC Address (D4:CA:6D:E2:65:90). The interface status is shown as 'enabled', 'running', and 'slave'.

Interfaces → bridge-local

DHCP and ARP

- DHCP Server can add ARP entries automatically
- Combined with **static leases** and **reply-only ARP** can increase network security while retaining the ease of use for users

DHCP and ARP

The screenshot shows the Mikrotik WinBox DHCP Server configuration window for a server named 'dhcp1'. The configuration includes the following fields:

- Name: dhcp1
- Interface: bridge-local
- Relay: (empty)
- Lease Time: 00:10:00
- Bootp Lease Time: forever
- Address Pool: dhcp_pool1
- Src. Address: (empty)
- Delay Threshold: (empty)
- Authoritative: after 2s delay
- Bootp Support: static
- Lease Script: (empty text area)
- Buttons: Add ARP For Leases, Always Broadcast, Use RADIUS

At the bottom of the window, the status is 'enabled'. To the right of the window, a table shows the configuration for the address pool:

Address Pool	Add ARP For Leases
dhcp_pool1	no

IP → DHCP Server

Add ARP entries for DHCP leases

Static ARP

- Make your laptop's ARP entry static
- Set the bridge interface ARP to reply-only to disable adding dynamic ARP entries
- You should still have the DHCP server to static-only and a static lease for the laptop. If not, repeat the previous LAB
- Enable 'Add ARP For Leases' on DHCP server

Static ARP

- Remove your laptop's static entry from the ARP table
- Check the Internet connection (not working)
- Renew the IP address of your laptop
- Check the Internet connection (should work)
- Connect to the router and observe the ARP table

Module 2

Summary



Certified Network Associate (MTCNA)

Module 3

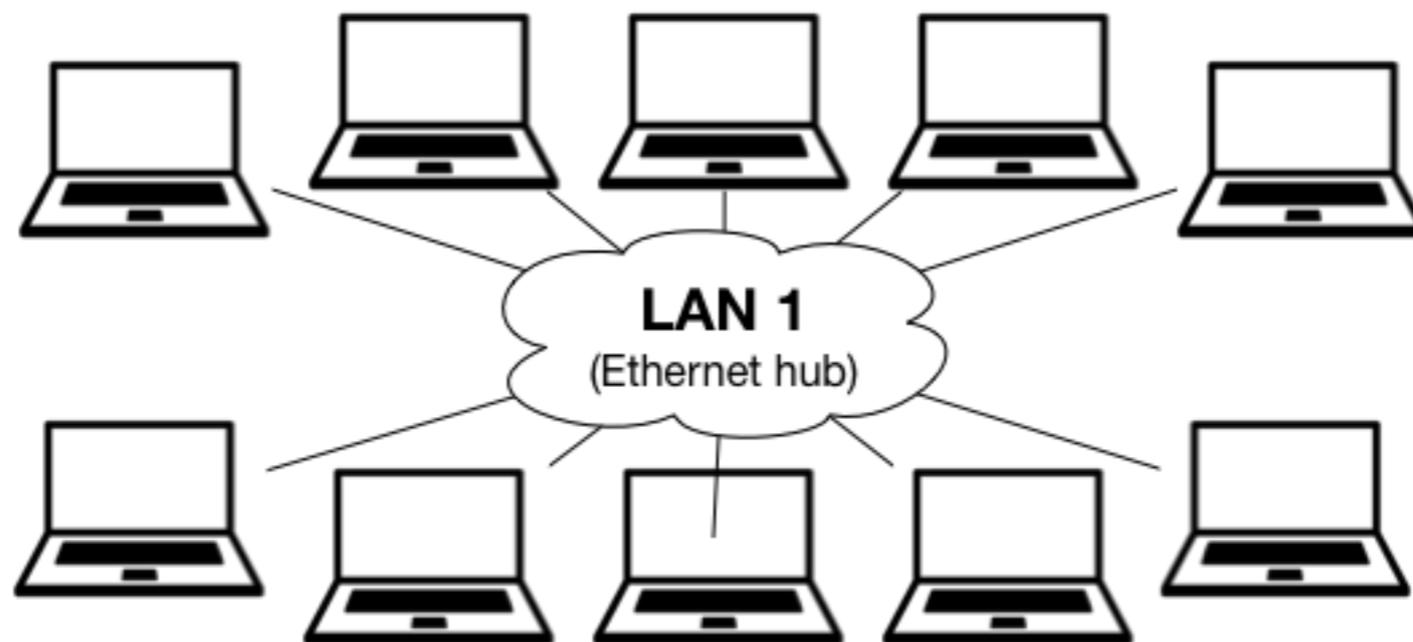
Bridging

Bridge

- Bridges are OSI layer 2 devices
- Bridge is a transparent device
- Traditionally used to join two network segments
- Bridge splits collision domain in two parts
- Network switch is multi-port bridge - each port is a collision domain of one device

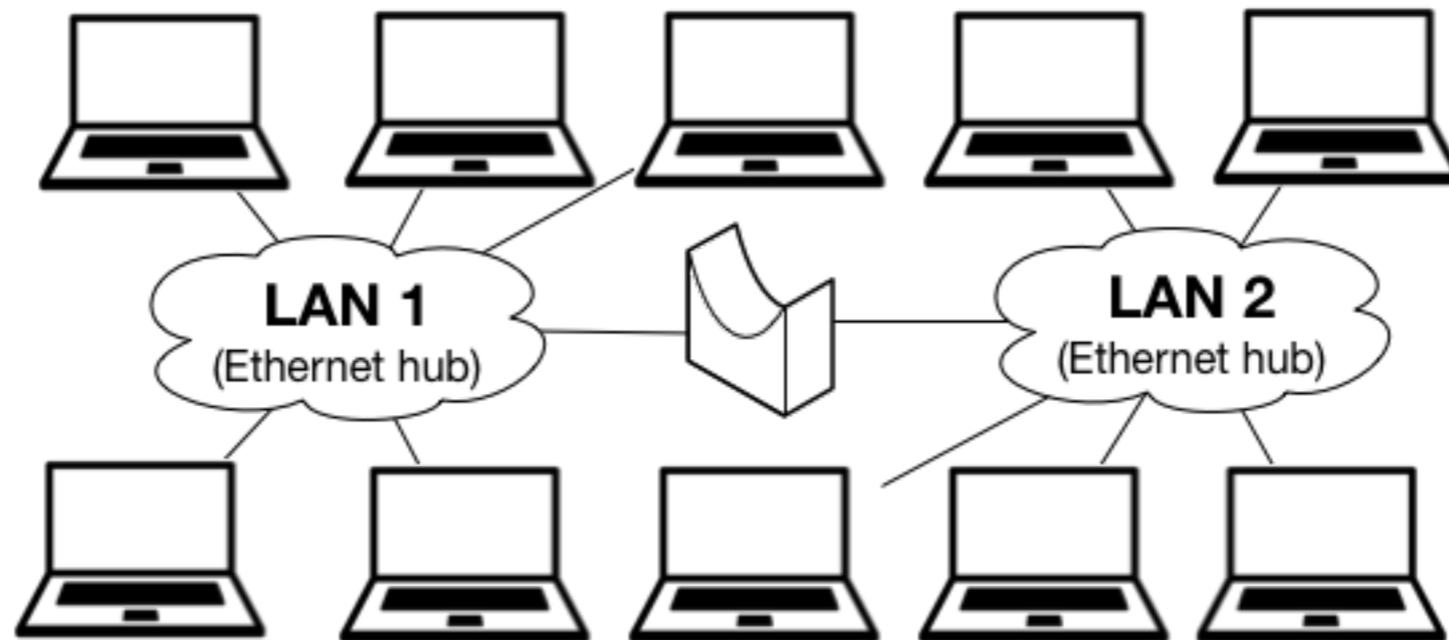
Bridge

- All hosts can communicate with each other
- All share the same collision domain



Bridge

- All hosts still can communicate with each other
- Now there are 2 collision domains



Bridge

- RouterOS implements software bridge
- Ethernet, wireless, SFP and tunnel interfaces can be added to a bridge
- Default configuration on SOHO routers bridge wireless with ether2 port
- Ether2-5 are combined together in a switch. Ether2 is master, 3-5 slave. Wire speed switching using switch chip

Bridge

- It is possible to remove master/slave configuration and use bridge instead
- Switch chip will not be used, higher CPU usage
- More control - can use IP firewall for bridge ports

Bridge

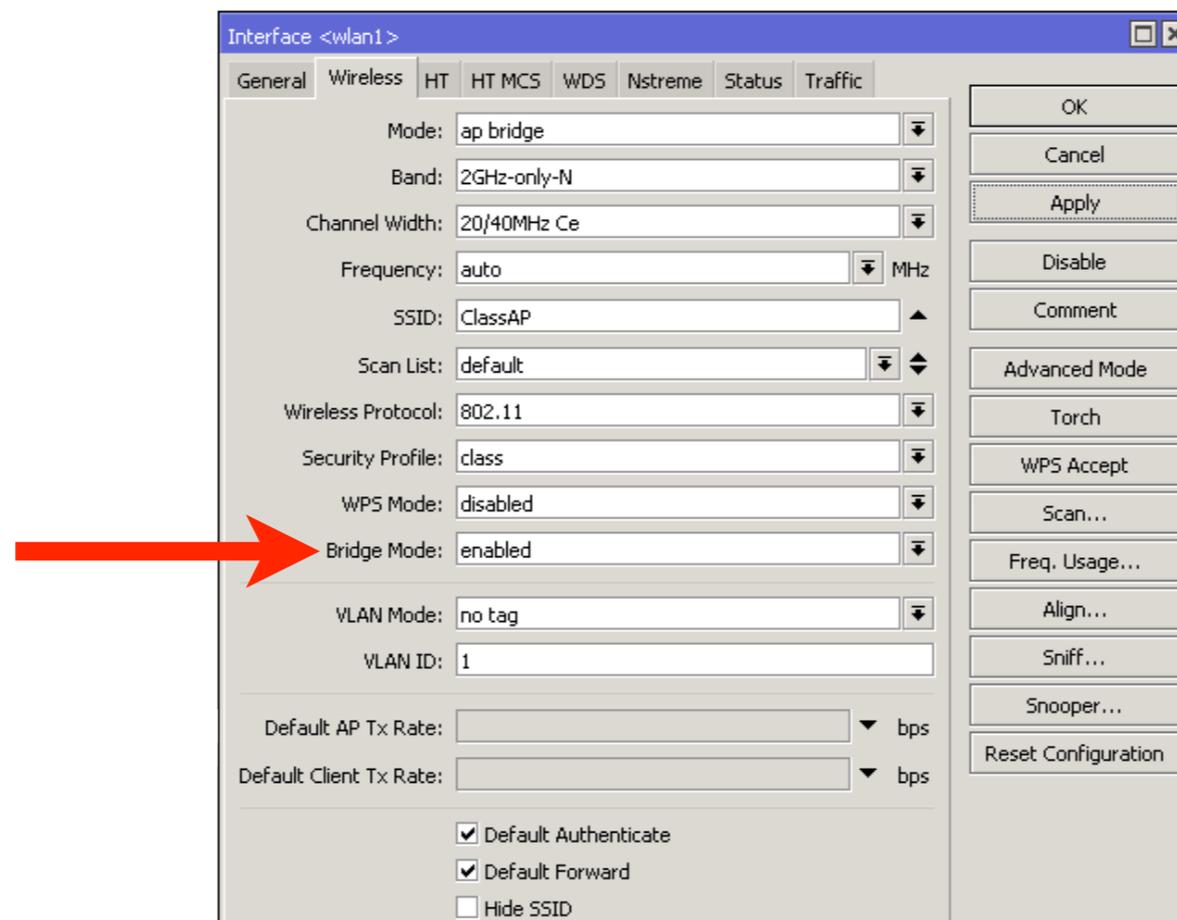
- Due to limitations of 802.11 standard, wireless clients (mode: station) do not support bridging
- RouterOS implements several modes to overcome this limitation

Wireless Bridge

- **station bridge - RouterOS to RouterOS**
- **station pseudobridge - RouterOS to other**
- **station wds (Wireless Distribution System) - RouterOS to RouterOS**

Wireless Bridge

- To use station bridge, 'Bridge Mode' has to be enabled on the AP



Bridge

- We are going to create **one big network** by bridging local Ethernet with wireless (Internet) interface
- All the laptops will be in the same network
- Note: be careful when bridging networks!
- **Create a backup before starting this LAB!**

Bridge

- Change wireless to **station bridge** mode
- Disable DHCP server
- Add wireless interface to existing bridge-local interface as a port

Bridge

Set mode to station bridge

Interface <wlan1>

General Wireless HT HT MCS WDS Nstreme Advanced Status Status Traffic

Mode: station bridge

Band: 2GHz-only-N

Channel Width: 20MHz

Frequency: auto MHz

SSID: ClassAP

Scan List: default

Wireless Protocol: 802.11

Security Profile: class

OK
Cancel
Apply
Disable
Comment
Advanced Mode
Torch
WPS Accept

Wireless → wlan1

Disable DHCP Server

DHCP Server

DHCP Networks Leases Options Option Sets Alerts

+ - ✓ ✗ ⏏ DHCP Config DHCP Setup Find

Name	Interface	Relay	Lease Time	Address Pool	Add ARP For Leases
default	bridge-local		00:10:00	unknown	no

1 item (1 selected)

IP → DHCP Server

Bridge

Bridge

Bridge Ports Filters NAT Hosts

Interface	Bridge	Priority (...)	Path Cost	Horizon	Role	Root Path Cost	Comment
ether2-master-local	bridge-local	80	10		designated port		

New Bridge Port

General Status

Interface: wlan1

Bridge: bridge-local

Priority: 80 hex

Path Cost: 10

Horizon:

Edge: auto

Point To Point: auto

External FDB: auto

Auto Isolate

OK Cancel Apply Disable Comment Copy Remove

enabled inactive

Add wireless interface to the bridge

Bridge → Ports

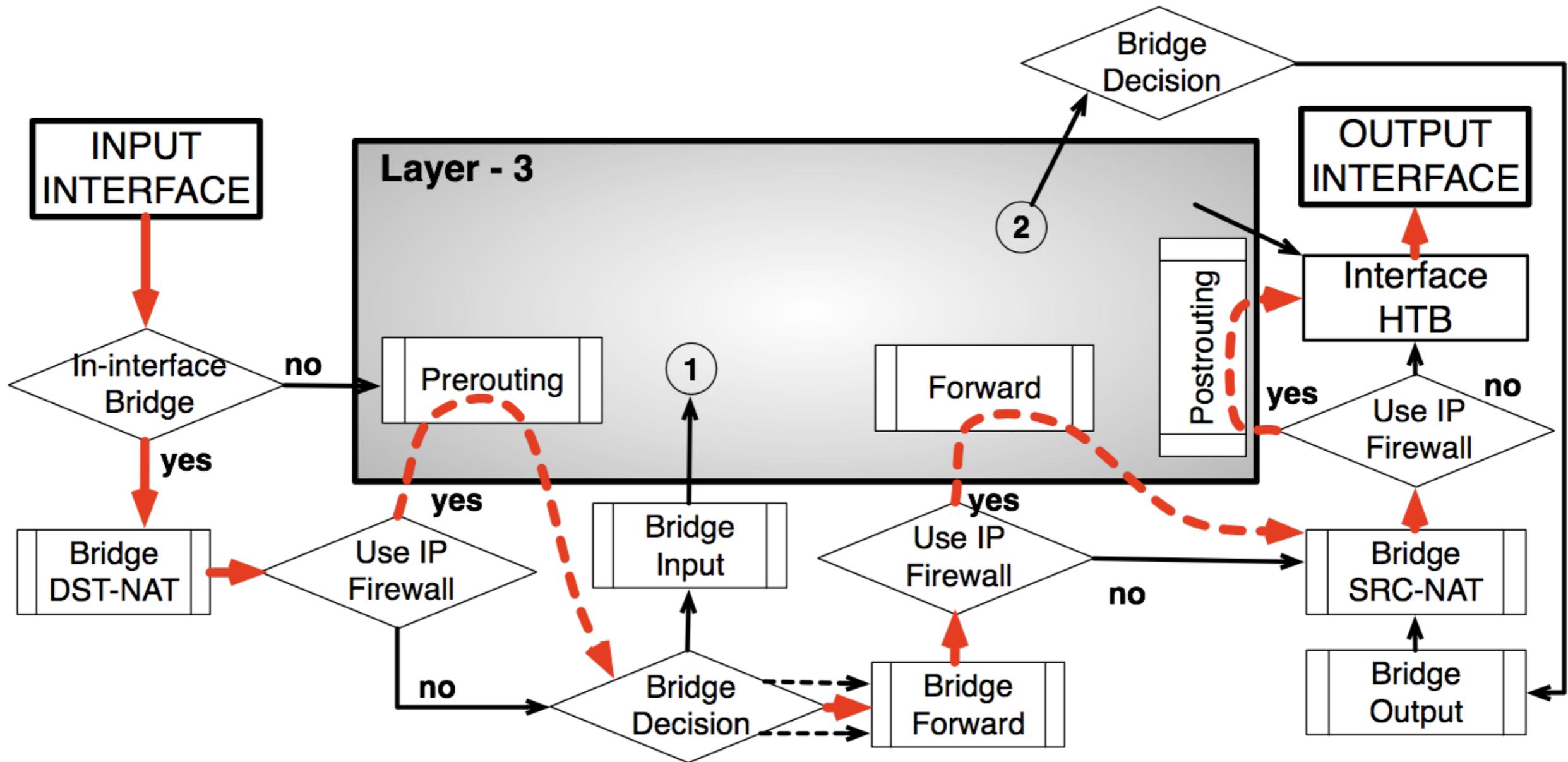
Bridge

- Renew the IP address of your laptop
- You should acquire IP from the trainer's router
- Ask your neighbor his/her laptop IP address and try to ping it
- Your router now is a **transparent bridge**

Bridge Firewall

- RouterOS bridge interface supports firewall
- Traffic which flows through the bridge can be processed by the firewall
- To enable: Bridge → Settings → Use IP Firewall

Bridge Firewall



Bridge

- Restore your router's configuration from the backup you created before bridging LAB
- Or restore previous configuration by hand

Module 3

Summary



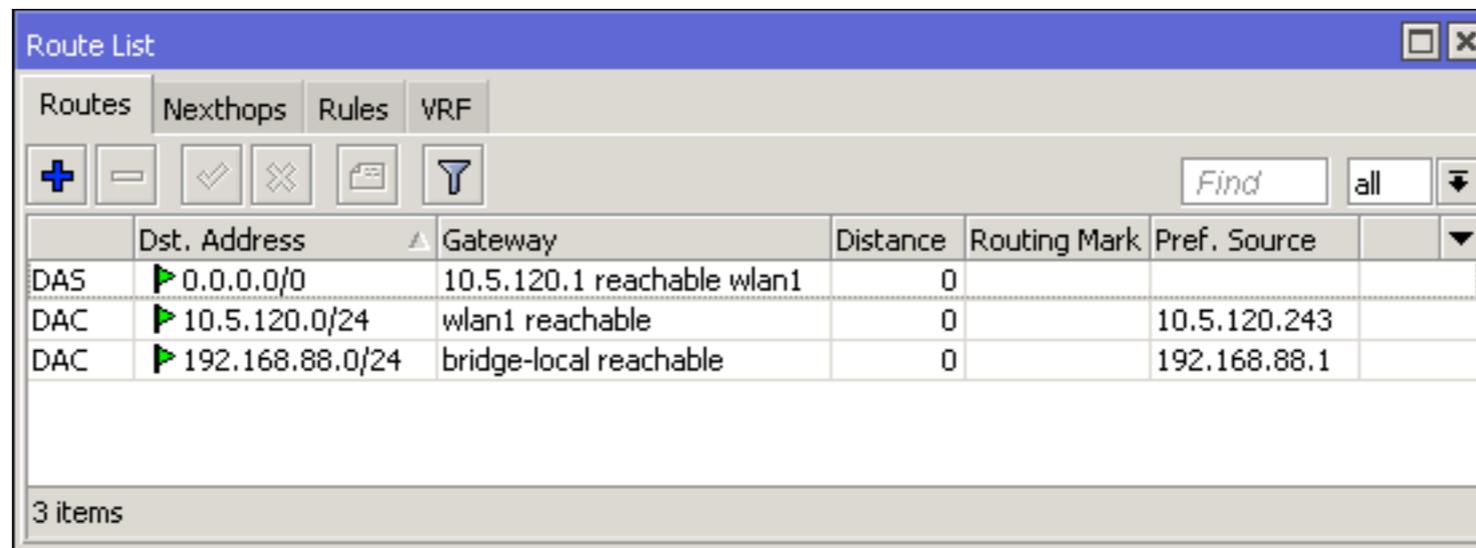
Certified Network Associate (MTCNA)

Module 4

Routing

Routing

- Works in OSI network layer (L3)
- RouterOS routing rules define where the packets should be sent



The screenshot shows the 'Route List' window in RouterOS. It features a toolbar with icons for adding, deleting, and filtering routes, along with a search field. The main area contains a table with the following data:

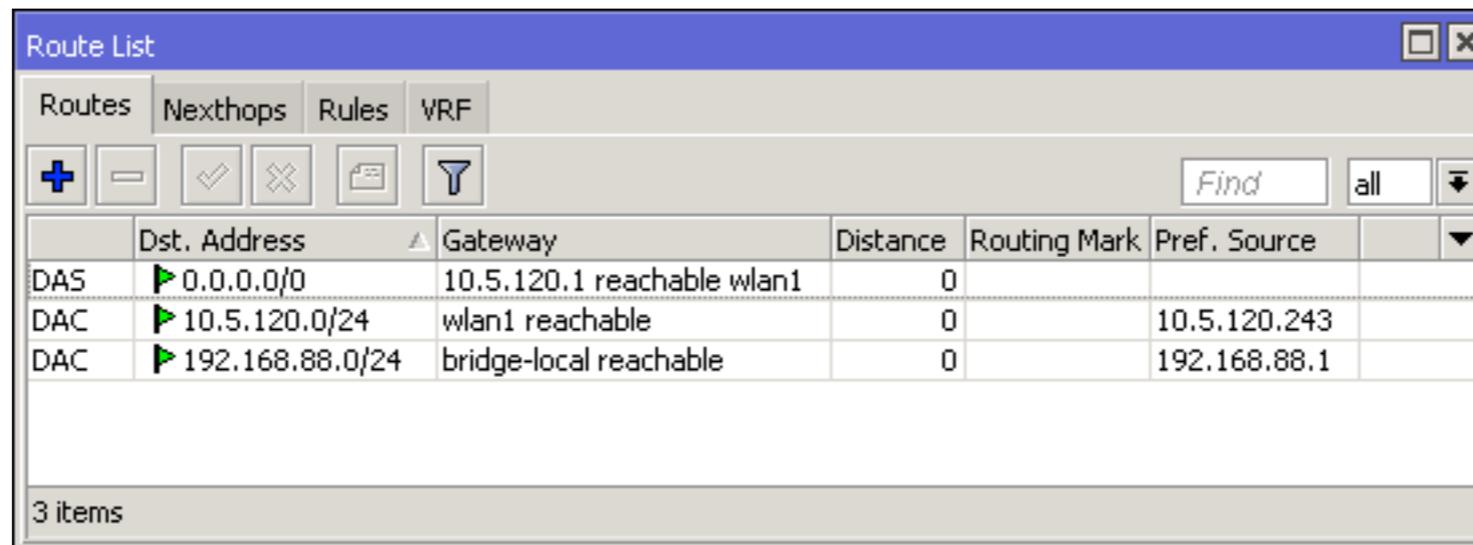
	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source	
DAS	0.0.0.0/0	10.5.120.1 reachable wlan1	0			
DAC	10.5.120.0/24	wlan1 reachable	0		10.5.120.243	
DAC	192.168.88.0/24	bridge-local reachable	0		192.168.88.1	

3 items

IP → Routes

Routing

- **Dst. Address:** networks which can be reached
- **Gateway:** IP address of the next router to reach the destination



The screenshot shows the 'Route List' window in Mikrotik WinBox. It features a table with columns for 'Dst. Address', 'Gateway', 'Distance', 'Routing Mark', and 'Pref. Source'. There are three rows of data, each with a green arrow icon in the 'Dst. Address' column. The table is titled 'Route List' and has tabs for 'Routes', 'Nexthops', 'Rules', and 'VRF'. Below the table, it indicates '3 items'.

	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
DAS	0.0.0.0/0	10.5.120.1 reachable wlan1	0		
DAC	10.5.120.0/24	wlan1 reachable	0		10.5.120.243
DAC	192.168.88.0/24	bridge-local reachable	0		192.168.88.1

IP → Routes

New Static Route

New Route

General Attributes

Dst. Address: 192.168.90.0/24

Gateway: 192.168.89.5

Check Gateway:

Type: unicast

Distance:

Scope: 30

Target Scope: 10

Routing Mark:

Pref. Source:

OK

Cancel

Apply

Disable

Comment

Copy

Remove

enabled active

IP → Routes

Routing

- Check gateway - every 10 seconds send either ICMP echo request (ping) or ARP request.
- If several routes use the same gateway and there is one that has **check-gateway** option enabled, all routes will be subjected to the behaviour of check-gateway

Routing

- If there are two or more routes pointing to the same address, the more precise 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

Default Gateway

- Default gateway: a router (next hop) where all the traffic for which there is no specific destination defined will be sent
- It is distinguished by 0.0.0.0/0 destination network

Default Gateway

- Currently the default gateway for your router is configured automatically using DHCP-Client
- Disable 'Add Default Route' in DHCP-Client settings
- Check the Internet connection (not working)

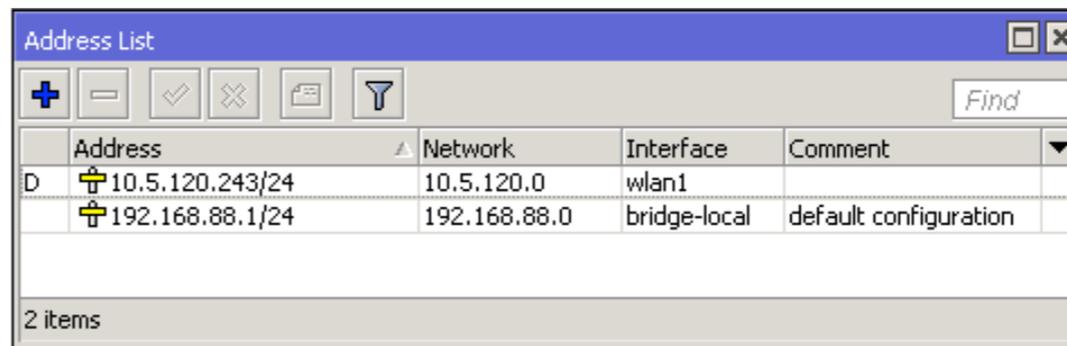
Default Gateway

- Add default gateway manually (trainer's router)
- Check that the connection to the Internet is available

Dynamic Routes

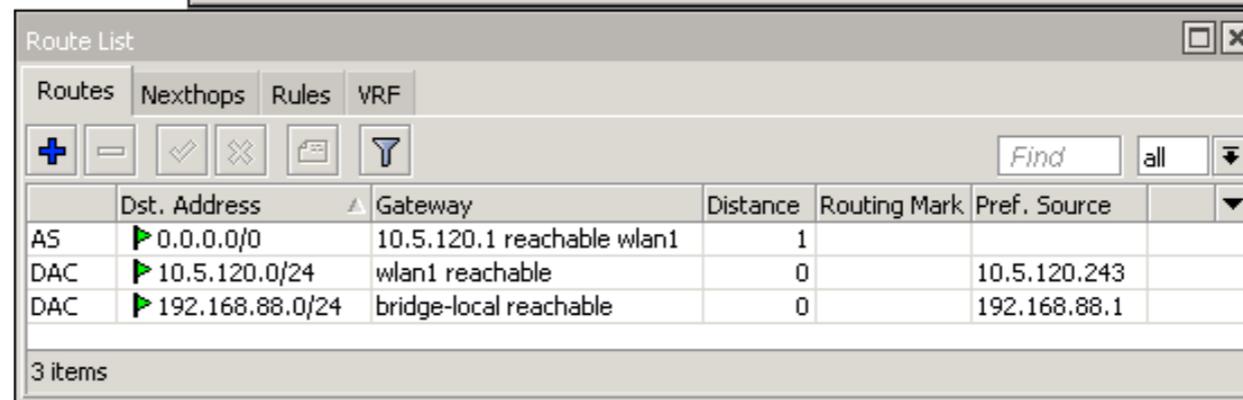
- Routes with flags **DAC** are added automatically
- **DAC** route originates from IP address configuration

IP → Addresses



	Address	Network	Interface	Comment
D	10.5.120.243/24	10.5.120.0	wlan1	
	192.168.88.1/24	192.168.88.0	bridge-local	default configuration

2 items



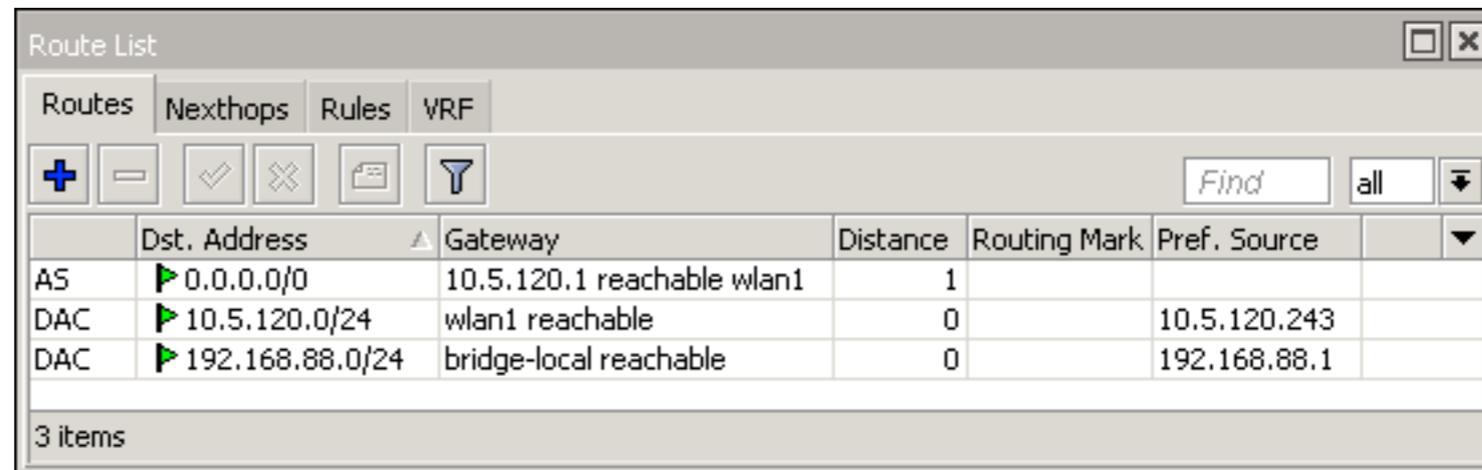
	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source
AS	0.0.0.0/0	10.5.120.1 reachable wlan1	1		
DAC	10.5.120.0/24	wlan1 reachable	0		10.5.120.243
DAC	192.168.88.0/24	bridge-local reachable	0		192.168.88.1

3 items

IP → Routes

Route Flags

- A - active
- C - connected
- D - dynamic
- S - static



	Dst. Address	Gateway	Distance	Routing Mark	Pref. Source	
AS	▶ 0.0.0.0/0	10.5.120.1 reachable wlan1	1			
DAC	▶ 10.5.120.0/24	wlan1 reachable	0		10.5.120.243	
DAC	▶ 192.168.88.0/24	bridge-local reachable	0		192.168.88.1	

3 items

IP → Routes

Static Routing

- Static route defines how to reach a specific destination network
- **Default gateway** is also a static route. It directs all traffic to the gateway

Static Routing

- The goal is to ping your neighbor's laptop
- Static route will be used to achieve this
- Ask your neighbor the IP address of his/her wireless interface
- And the subnet address of his/her internal network (192.168.XY.0/24)

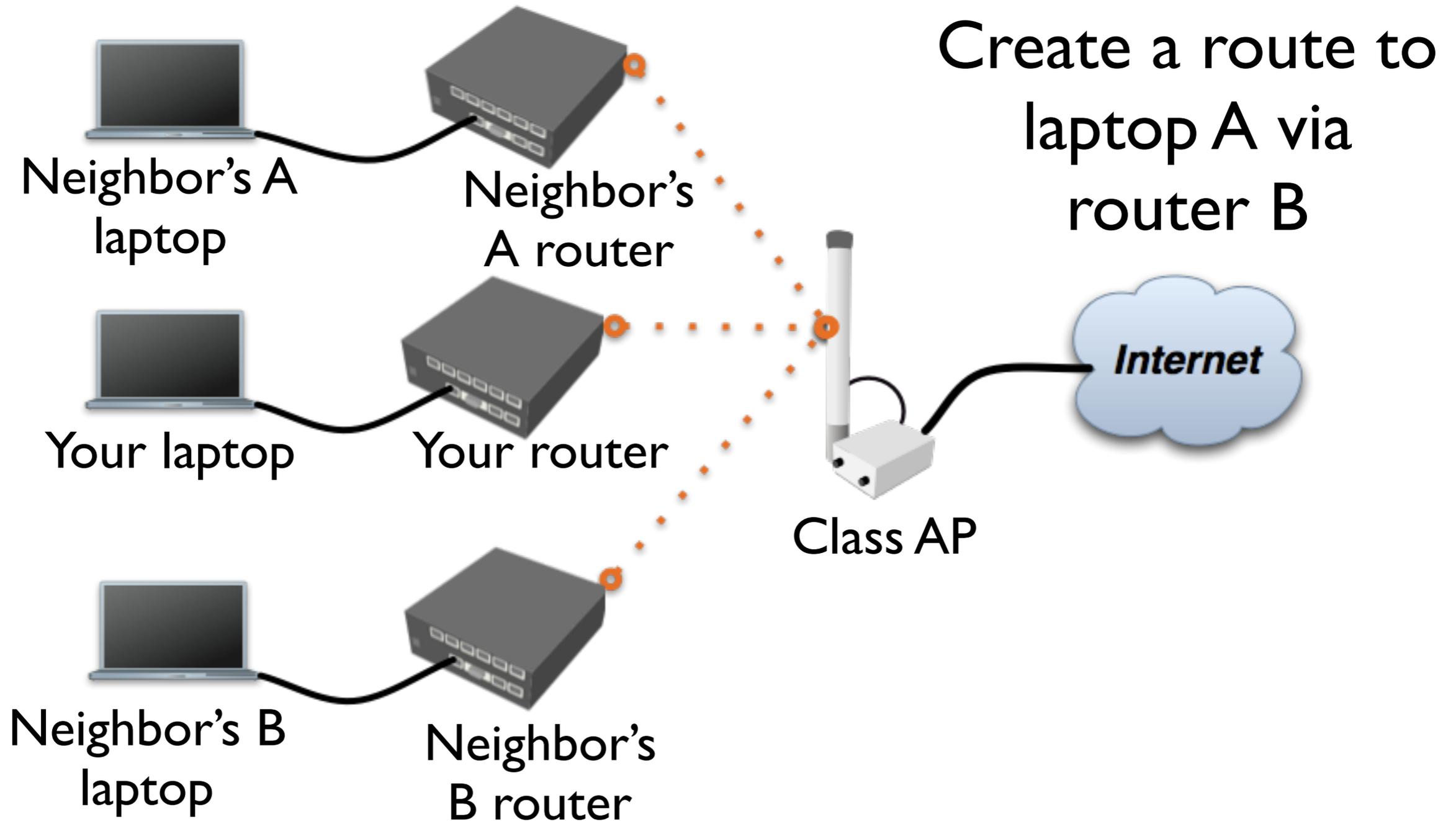
Static Routing

- Add a new route rule
- Set **Dst. Address** - your neighbor's local network address (eg. 192.168.37.0/24)
- Set **Gateway** - the address of your neighbor's wireless interface (eg. 192.168.250.37)
- Now you should be able to ping your neighbor's laptop

Static Routing

- Team up with 2 of your neighbors
- Create a static route to one of your neighbor's (A) laptop via the other neighbor's router (B)
- Ask your neighbor B to make a static route to neighbor's A laptop
- Ping your neighbor's A laptop

Static Routing



Static Routing

- Easy to configure on a small network
- Limits the use of router's resources
- Does not scale well
- Manual configuration is required every time a new subnet needs to be reached

Module 4

Summary



Certified Network Associate (MTCNA)

Module 5

Wireless

Wireless

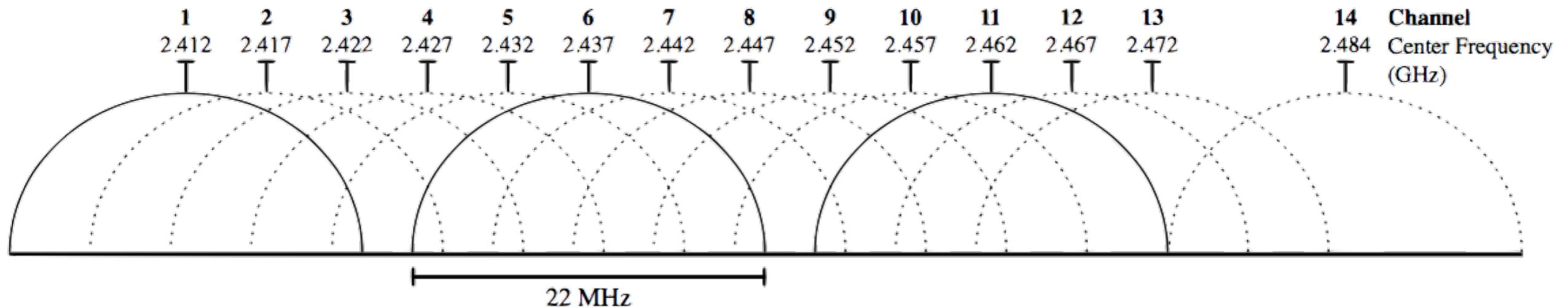
- MikroTik RouterOS provides a complete support for IEEE 802.11a/n/ac (5GHz) and 802.11b/g/n (2.4GHz) wireless networking standards

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*

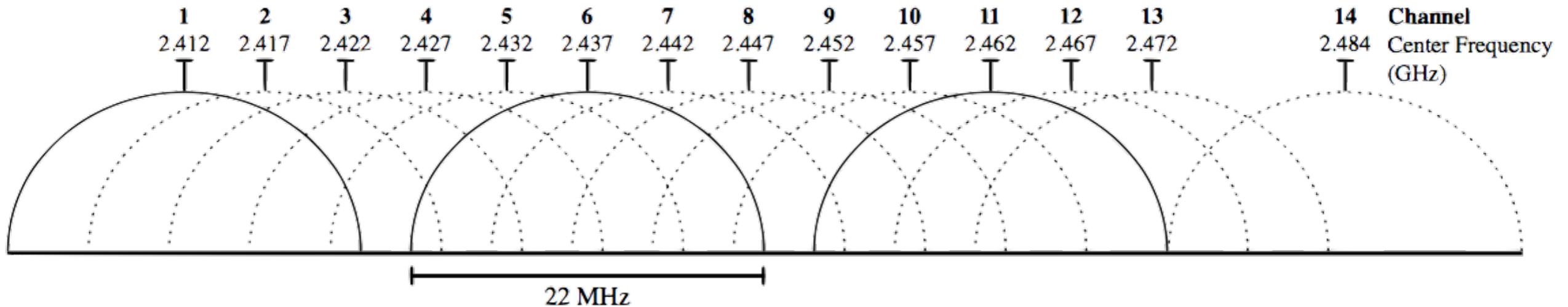
* Depending on RouterBOARD model

2.4GHz Channels



- 13x 22MHz channels (most of the world)
- 3 non-overlapping channels (1, 6, 11)
- 3 APs can occupy the same area without interfering

2.4GHz Channels



- US: 11 channels, 14th Japan-only
- Channel width:
 - 802.11b 22MHz, 802.11g 20MHz, 802.11n 20/40MHz

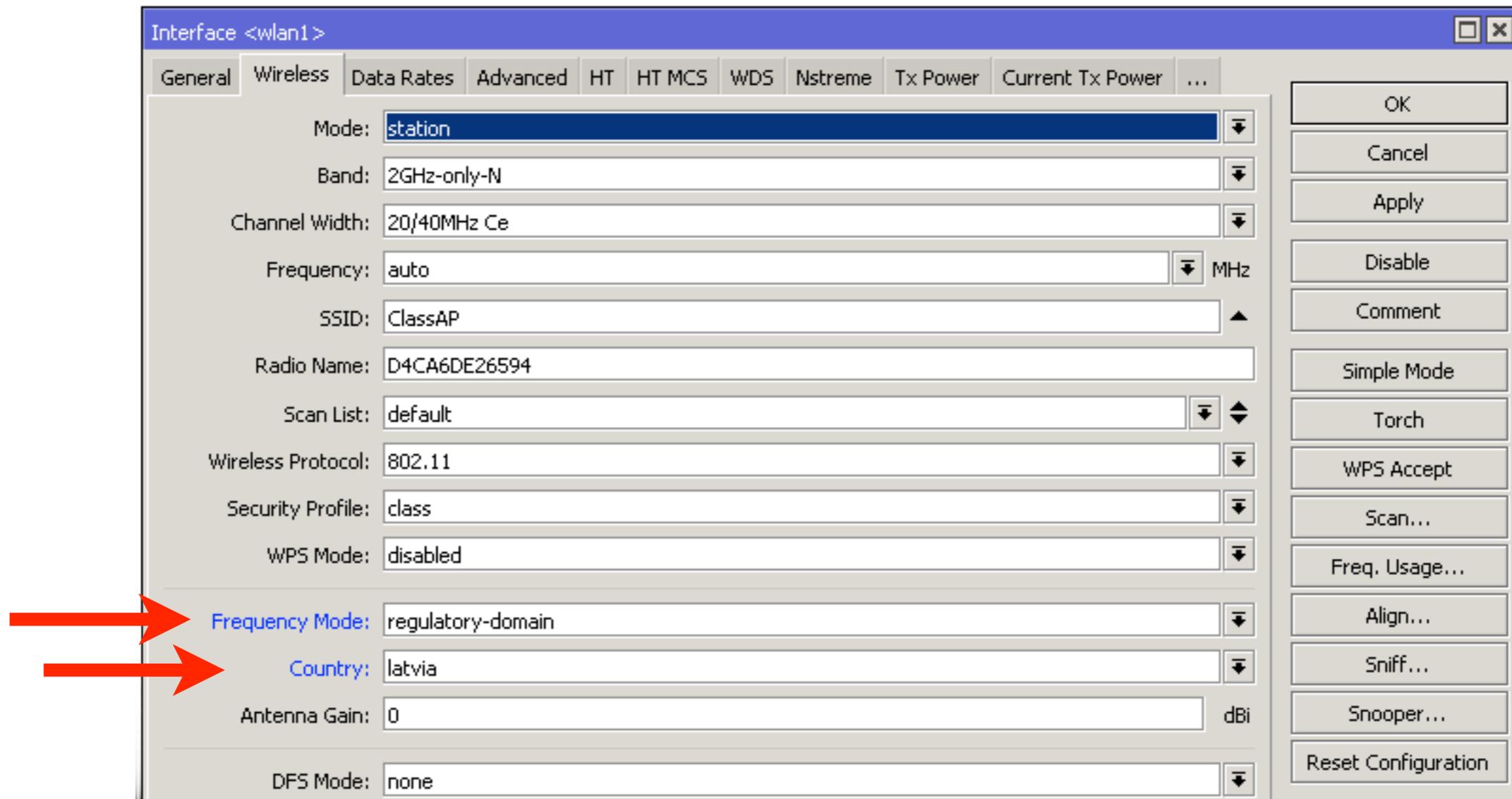
5GHz Channels

- RouterOS supports full range of 5GHz frequencies
- 5180-5320MHz (channels 36-64)
- 5500-5720MHz (channels 100-144)
- 5745-5825MHz (channels 149-165)
- Varies depending on country regulations

5GHz Channels

IEEE Standard	Channel Width
802.11a	20MHz
802.11n	20MHz
	40MHz
802.11ac	20MHz
	40MHz
	80MHz
	160MHz

Country Regulations



- Switch to 'Advanced Mode' and select your country to apply regulations

Country Regulations

- Dynamic Frequency Selection (DFS) is a feature which is meant to identify radars when using 5GHz band and choose a different channel if a radar is found
- Some channels can only be used when DFS is enabled (in EU: 52-140, US: 50-144)

Country Regulations

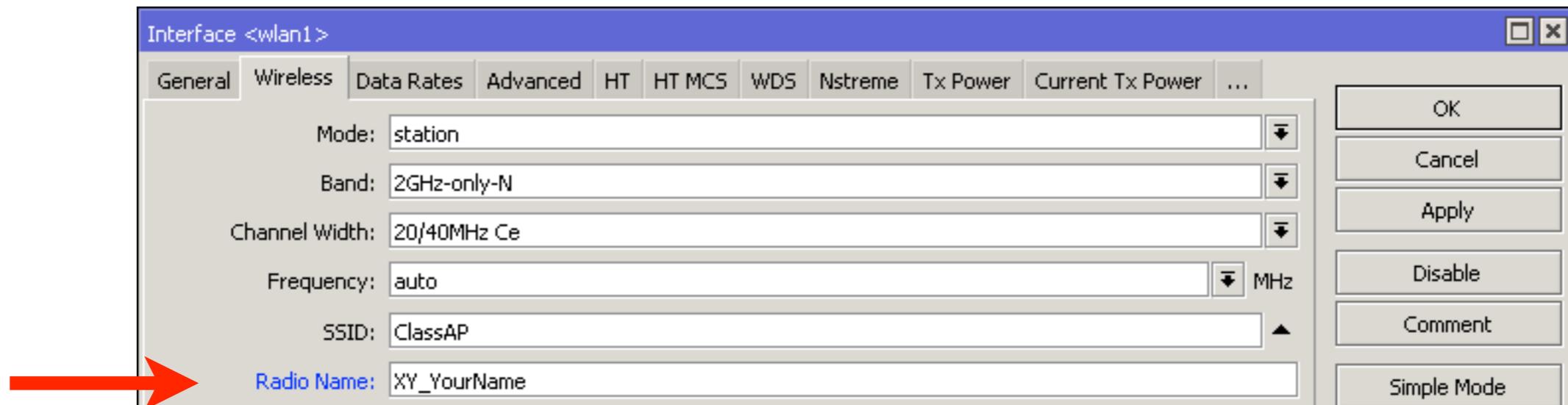
- DFS Mode radar detect will select a channel with the lowest number of detected networks and use it if no radar is detected on it for 60s
- Switch to 'Advanced Mode' to enable DFS

Frequency Mode:	regulatory-domain	▼
Country:	latvia	▼
Antenna Gain:	0	dBi
DFS Mode:	none	▼
WMM Support:	no radar detect none radar detect	
Bridge Mode:	enabled	▼

Wireless

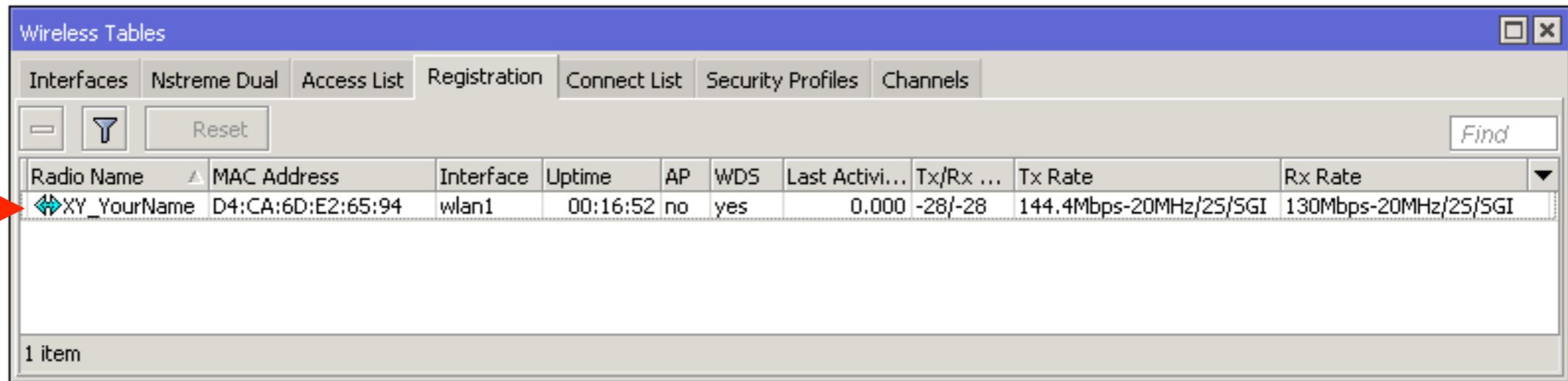
Radio Name

- Wireless interface “name”
- RouterOS-RouterOS only
- Can be seen in Wireless tables



Radio Name

- Wireless interface “name”
- RouterOS-RouterOS only
- Can be seen in Wireless tables



Radio Name	MAC Address	Interface	Uptime	AP	WDS	Last Activi...	Tx/Rx ...	Tx Rate	Rx Rate
XY_YourName	D4:CA:6D:E2:65:94	wlan1	00:16:52	no	yes	0.000	-28/-28	144.4Mbps-20MHz/25/SGI	130Mbps-20MHz/25/SGI

Wireless → Registration

Radio Name

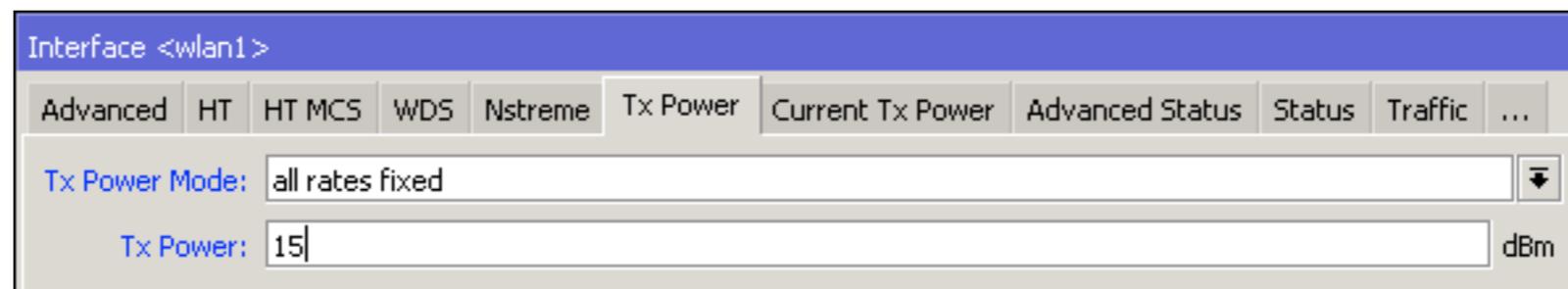
- Set the radio name of your wireless interface as follows:
YourNumber(XY)_YourName
- For example: **13_JohnDoe**

Wireless Chains

- 802.11n introduced the concept of MIMO (Multiple In and Multiple Out)
- Send and receive data using multiple radios in parallel
- 802.11n with one chain (SISO) can only achieve 72.2Mbps (on legacy cards 65Mbps)

Tx Power

- Use to adjust transmit power of the wireless card
- Change to **all rates fixed** and adjust the power



Wireless → Tx Power

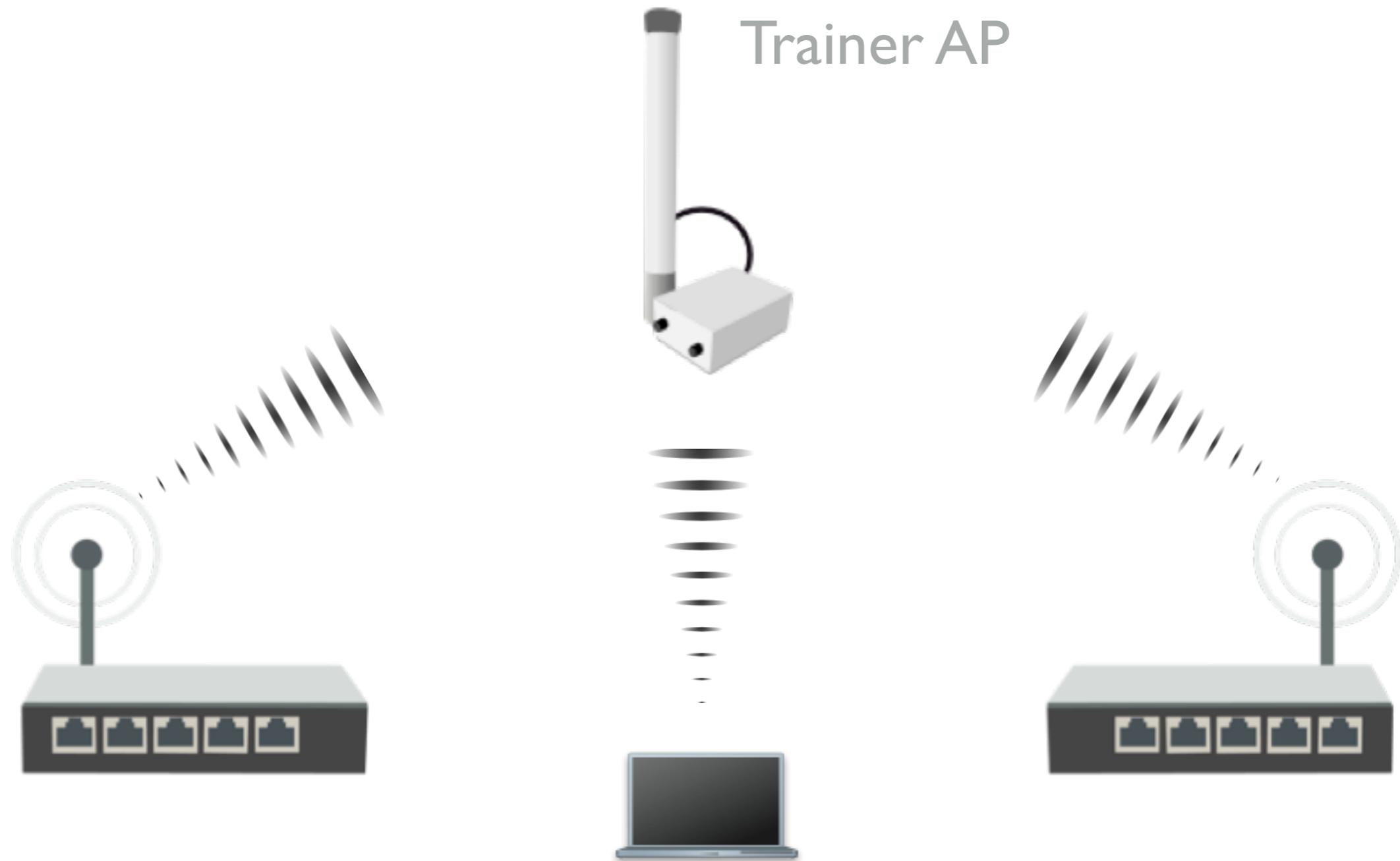
Tx Power

Wireless card	Enabled Chains	Power per Chain	Total Power
802.11n	1	Equal to the selected Tx Power	Equal to the selected Tx Power
	2		+3dBm
	3		+5dBm
802.11ac	1	Equal to the selected Tx Power	Equal to the selected Tx Power
	2	-3dBm	
	3	-5dBm	

Rx Sensitivity

- Receiver sensitivity is the lowest power level at which the interface can detect a signal
- When comparing RouterBOARDS this value should be taken into account depending on planned usage
- Smaller Rx sensitivity threshold means better signal detection

Wireless Network



Wireless stations

Wireless Station

- Wireless station is client (laptop, phone, router)
- On RouterOS wireless mode **station**

Wireless Station

- Set interface mode=station
- Select band
- Set SSID (wireless network ID)
- Frequency is not important for client, use scan-list

The screenshot shows the Mikrotik WinBox configuration window for the 'wlan1' interface, specifically the 'Wireless' tab. The configuration is as follows:

Field	Value
Mode	station
Band	2GHz-only-N
Channel Width	20/40MHz Ce
Frequency	auto MHz
SSID	ClassAP
Scan List	default
Wireless Protocol	802.11
Security Profile	class
WPS Mode	disabled
Bridge Mode	enabled
VLAN Mode	no tag
VLAN ID	1
Default AP Tx Rate	bps
Default Client Tx Rate	bps
Default Authenticate	<input checked="" type="checkbox"/>
Default Forward	<input checked="" type="checkbox"/>

Red arrows in the image point to the 'Mode', 'Band', 'SSID', and 'Security Profile' fields, indicating the configuration steps mentioned in the text.

Security

- Only WPA (WiFi Protected Access) or WPA2 should be used
- WPA-PSK or WPA2-PSK with AES-CCM encryption
- Trainer AP already is using WPA-PSK/WPA2-PSK

Security

- Both WPA and WPA2 keys can be specified to allow connection from devices which do not support WPA2
- Choose strong key!

Security Profile <class>

General | RADIUS | EAP | Static Keys

Name: class

Mode: dynamic keys

Authentication Types: WPA PSK WPA2 PSK
 WPA EAP WPA2 EAP

Unicast Ciphers: aes ccm tkip

Group Ciphers: aes ccm tkip

WPA Pre-Shared Key: *****

WPA2 Pre-Shared Key: *****

Supplicant Identity:

Group Key Update: 00:05:00

Management Protection: allowed

Management Protection Key:

OK
Cancel
Apply
Copy
Remove

Wireless → Security Profiles

Connect List

- Rules used by **station** to select (or not to select) an AP

Station Connect Rule <4C:5E:0C:0A:0F:A3>

Interface: wlan1

MAC Address: 4C:5E:0C:0A:0F:A3

Connect

SSID: ClassAP

Area Prefix:

Signal Strength Range: -120..120

Wireless Protocol: 802.11

Security Profile: class

enabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove

Wireless → Connect List

Connect List

- Currently your router is connected to the class AP
- Create a rule to disallow connection to the class AP

Access Point

- Set interface mode=ap bridge
- Select band
- Set frequency
- Set SSID (wireless network ID)
- Set Security Profile

The screenshot shows the 'Interface <wlan1>' configuration window in WinBox. The 'Wireless' tab is active. The configuration fields are as follows:

- Mode: ap bridge
- Band: 2GHz-only-N
- Channel Width: 20/40MHz Ce
- Frequency: auto MHz
- SSID: ClassAP
- Scan List: default
- Wireless Protocol: 802.11
- Security Profile: class
- WPS Mode: disabled
- Bridge Mode: enabled
- VLAN Mode: no tag
- VLAN ID: 1
- Default AP Tx Rate: [] bps
- Default Client Tx Rate: [] bps
- Default Authenticate
- Default Forward
- Hide SSID

Buttons on the right side include: OK, Cancel, Apply, Disable, Comment, Advanced Mode, Torch, WPS Accept, Scan..., Freq. Usage..., Align..., Sniff..., Snooper..., and Reset Configuration.

WPS

- WiFi Protected Setup (WPS) is a feature for convenient access to the WiFi without the need of entering the passphrase
- RouterOS supports both WPS accept (for AP) and WPS client (for station) modes

WPS Accept

- 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 when a new device needs to be connected

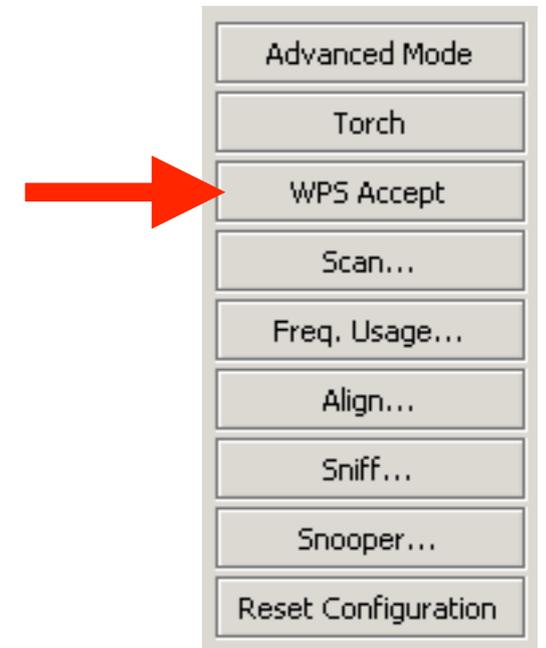
WPS Accept

- For each device it has to be done only once
- All RouterOS devices with WiFi interface have virtual WPS push button
- Some have physical, check for wps button on the router



WPS Accept

- 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 including RouterOS
- RouterOS does not support the insecure PIN mode



Access Point

- Create a new security profile for your access point
- Set wireless interface mode to **ap bridge**, set **SSID** to your class number and name, select the security profile
- Disable DHCP client on the wireless interface (will lose Internet connection)

Access Point

- Add wireless interface to the bridge
- Disconnect the cable from the laptop
- Connect to your wireless AP with your laptop
- Connect to the router using WinBox and observe wireless registration table
- When done, restore previous configuration

WPS

- If you have a device that supports WPS client mode connect it to your AP using WPS accept button on your router (either physical or virtual)
- Check router logs during the process
- When done, restore previous configuration

Snooper

- Get full overview of the wireless networks on selected band
- **Wireless interface is disconnected during scanning!**
- Use to decide which channel to choose

Snooper

Wireless Snooper (Running)

Interface: Start Stop Close Settings New Window

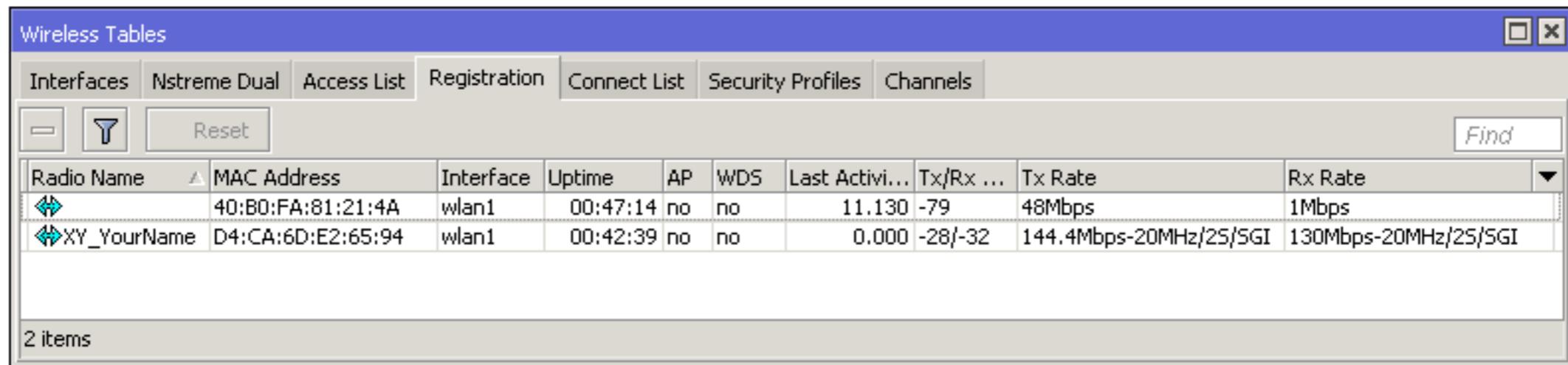
all

Channel	Address	SSID	Signal	Of Freq. (%)	Of Traf. (%)	Bandwidth	Net...	Sta...
2412/20/gn(20dBm)	64:66:B3:40:E6:5E	Maximums	-71	0.0	0.0	0 bps		
2412/20/gn(20dBm)	50:56:A8:01:69:71		-81	0.0	0.0	0 bps		
2412/20/gn(20dBm)	4C:5E:0C:61:B4:36	Hotspot		1.3	8.4	12.4 kbps		1
2412/20/gn(20dBm)	4C:5E:0C:61:B4:36	Hotspot	-91	1.3	8.4	12.4 kbps		
2412/20/gn(20dBm)	00:0C:42:18:5C:49		-86	0.0	0.0	0 bps		
2412/20/gn(20dBm)	00:0C:42:0C:1B:4E			0.1	1.2	9.1 kbps		1
2412/20/gn(20dBm)	00:0C:42:0C:1B:4E		-86	0.1	1.2	9.1 kbps		
2412/20/gn(20dBm)	00:0B:6B:30:7F:A6	raivis		0.0	0.0	0 bps		0
2412/20/gn(20dBm)	00:0B:6B:30:7F:A6		-73	0.0	0.0	0 bps		
2412/20/gn(20dBm)				16.0		108.8 kbps	7	12
2417/20/gn(20dBm)	84:A6:C8:06:F3:83		-83	0.0	0.0	0 bps		
2417/20/gn(20dBm)				11.4		81.4 kbps	0	1
2422/20/gn(20dBm)	58:48:22:3F:56:B5	Mob	-80	0.0	0.0	0 bps		
2422/20/gn(20dBm)	4C:5E:0C:D6:CB:81	Mob		1.2	14.7	11.0 kbps		2
2422/20/gn(20dBm)	4C:5E:0C:D6:CB:81	Mob	-51	1.2	14.7	11.0 kbps		
2422/20/gn(20dBm)	4C:5E:0C:6C:5C:F2	anrijs-map		1.3	16.2	12.3 kbps		1
2422/20/gn(20dBm)	4C:5E:0C:6C:5C:F2	anrijs-map	-61	1.3	16.2	12.3 kbps		
2422/20/gn(20dBm)	4C:5E:0C:13:E6:65	MikroTik-mAPLite		0.0	0.0	0 bps		1
2422/20/gn(20dBm)	4C:5E:0C:13:E6:65	MikroTik-mAPLite	-88	0.0	0.0	0 bps		

Wireless → Snooper

Registration Table

- View all connected wireless interfaces
- Or connected access point if the router is a station



Radio Name	MAC Address	Interface	Uptime	AP	WDS	Last Activi...	Tx/Rx ...	Tx Rate	Rx Rate
	40:B0:FA:81:21:4A	wlan1	00:47:14	no	no	11.130	-79	48Mbps	1Mbps
XY_YourName	D4:CA:6D:E2:65:94	wlan1	00:42:39	no	no	0.000	-28/-32	144.4Mbps-20MHz/25/SGI	130Mbps-20MHz/25/SGI

2 items

Wireless → Registration

Access List

- Used by access point to control allowed connections from stations
- Identify device MAC address
- Configure whether the station can authenticate to the AP
- Limit time of the day when it can connect

Access List

Wireless Tables

Interfaces | Nstreme Dual | Access List | Registration | Connect List | Security Profiles | Channels

#	MAC Address	Interface	Signal St...	Authentication	Forwarding
0	AA:6C:B4:8A:C0:C9	wlan1	-120..120	yes	yes

AP Access Rule <AA:6C:B4:8A:C0:C9>

MAC Address: AA:6C:B4:8A:C0:C9

Interface: wlan1

Signal Strength Range: -120..120

AP Tx Limit: []

Client Tx Limit: []

Authentication

Forwarding

VLAN Mode: no tag

VLAN ID: 1

Private Key: none 0x []

Private Pre Shared Key: []

Management Protection Key: []

Time: 00:00:00 - 1d 00:00:00

Days: sun mon tue wed thu fri sat

enabled

Wireless → Access List

Access List

- If there are no matching rules in the access list, default values from the wireless interface will be used

Registration Table

- Can be used to create connect or access list entries from currently connected devices

The screenshot shows the Mikrotik WinBox interface. At the top, the 'Wireless Tables' menu is open, with 'Registration' selected. Below it, a table lists registered devices. The second row is highlighted, showing a device named 'XY_YourName' with MAC address 'D4:CA:6D:E2:...' and interface 'wlan1'. An 'AP Client <D4:CA:6D:E2:65:94>' window is open, displaying statistics for the selected device. The statistics include Tx Rate (144.4Mbps-20MHz/25/SGI), Rx Rate (130Mbps-20MHz/25/SGI), Tx/Rx Packets (665 966/674 414), Tx/Rx Bytes (430.8 MiB/251.7 MiB), Tx/Rx Frames (537 992/538 270), Tx/Rx Frame Bytes (434.5 MiB/250.7 MiB), Tx/Rx Hw. Frames (583 935/559 042), and Tx/Rx Hw. Frame Bytes (504.1 MiB/273.2 MiB). The window also contains buttons for OK, Remove, Reset, Copy to Access List, Copy to Connect List, Ping, MAC Ping, Telnet, MAC Telnet, and Torch.

Radio Name	MAC Address	Interface	Uptime	AP	WDS	Last Activi...	Tx/Rx ...	Tx F
	BC:6C:21:8A:...	wlan1	00:14:51	no	no	0.000	-36	72.2
XY_YourName	D4:CA:6D:E2:...	wlan1	07:06:45	no	no	0.000	-36/-28	144

General	802.1x	Signal	Nstreme	NV2	Statistics
Tx Rate:	144.4Mbps-20MHz/25/SGI				
Rx Rate:	130Mbps-20MHz/25/SGI				
Tx/Rx Packets:	665 966/674 414				
Tx/Rx Bytes:	430.8 MiB/251.7 MiB				
Tx/Rx Frames:	537 992/538 270				
Tx/Rx Frame Bytes:	434.5 MiB/250.7 MiB				
Tx/Rx Hw. Frames:	583 935/559 042				
Tx/Rx Hw. Frame Bytes:	504.1 MiB/273.2 MiB				

Wireless → Registration

Default Authenticate

The screenshot shows the 'Interface <wlan1>' configuration window in WinBox, with the 'Wireless' tab selected. The configuration is as follows:

- Mode: ap bridge
- Band: 2GHz-only-N
- Channel Width: 20/40MHz Ce
- Frequency: auto MHz
- SSID: ClassAP
- Scan List: default
- Wireless Protocol: 802.11
- Security Profile: class
- WPS Mode: disabled
- Bridge Mode: enabled
- VLAN Mode: no tag
- VLAN ID: 1
- Default AP Tx Rate: [empty] bps
- Default Client Tx Rate: [empty] bps
- Default Authenticate (highlighted with a red arrow)
- Default Forward
- Hide SSID

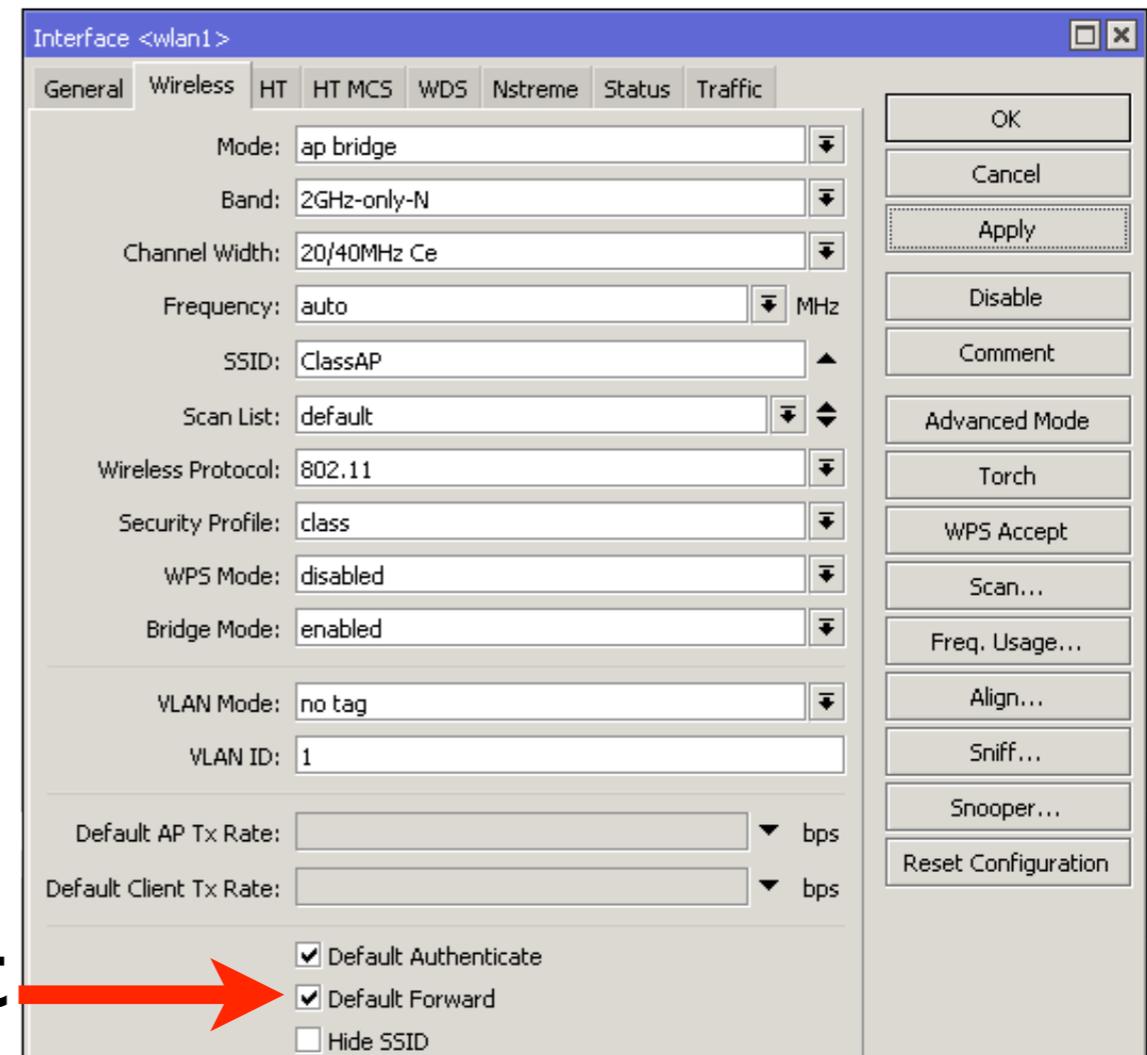
Buttons on the right side of the window include: OK, Cancel, Apply, Disable, Comment, Advanced Mode, Torch, WPS Accept, Scan..., Freq. Usage..., Align..., Sniff..., Snooper..., and Reset Configuration.

Default Authenticate

Default Authentication	Access/Connect List Entry	Behavior
✓	+	Based on access/connect list settings
	-	Authenticate
✗	+	Based on access/connect list settings
	-	Don't authenticate

Default Forward

- Use to allow or forbid communication between stations
- Enabled by default
- Forwarding can be overridden for specific clients in the access list



Interface <wlan1>

General Wireless HT HT MCS WDS Nstreme Status Traffic

Mode: ap bridge

Band: 2GHz-only-N

Channel Width: 20/40MHz Ce

Frequency: auto MHz

SSID: ClassAP

Scan List: default

Wireless Protocol: 802.11

Security Profile: class

WPS Mode: disabled

Bridge Mode: enabled

VLAN Mode: no tag

VLAN ID: 1

Default AP Tx Rate: bps

Default Client Tx Rate: bps

Default Authenticate

Default Forward

Hide SSID

OK

Cancel

Apply

Disable

Comment

Advanced Mode

Torch

WPS Accept

Scan...

Freq. Usage...

Align...

Sniff...

Snooper...

Reset Configuration

Module 5

Summary



Certified Network Associate (MTCNA)

Module 6

Firewall

Firewall

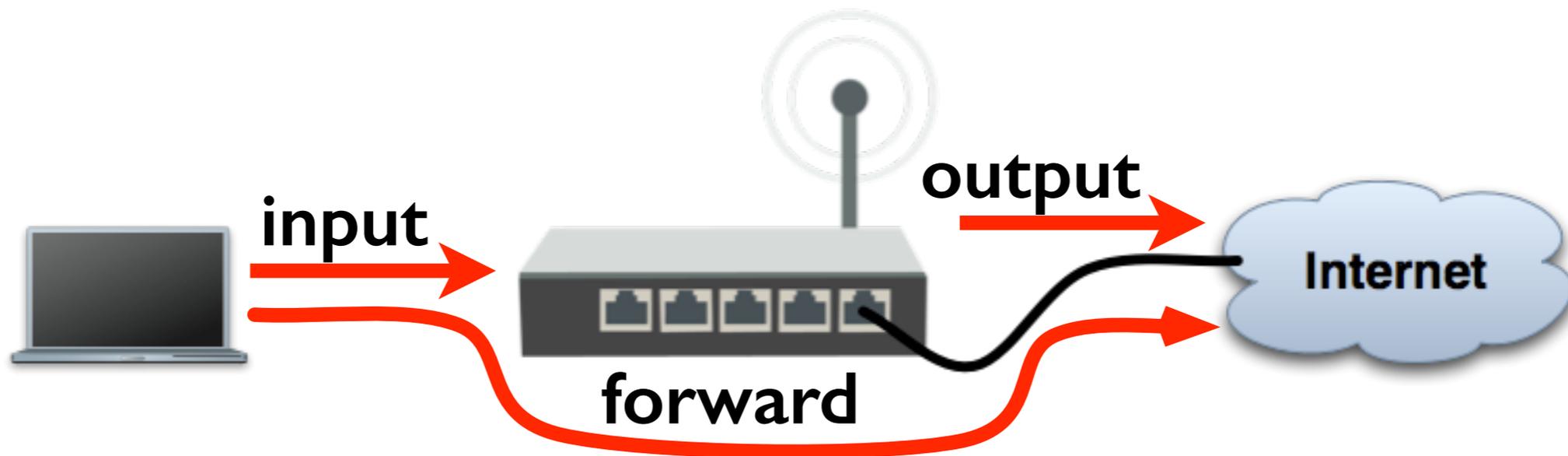
- A network security system that protects internal network from outside (e.g. the Internet)
- Based on rules which are analysed sequentially until first match is found
- RouterOS firewall rules are managed in Filter and NAT sections

Firewall Rules

- Work on **If-Then** principle
- Ordered in chains
- There are predefined chains
- Users can create new chains

Firewall Filter

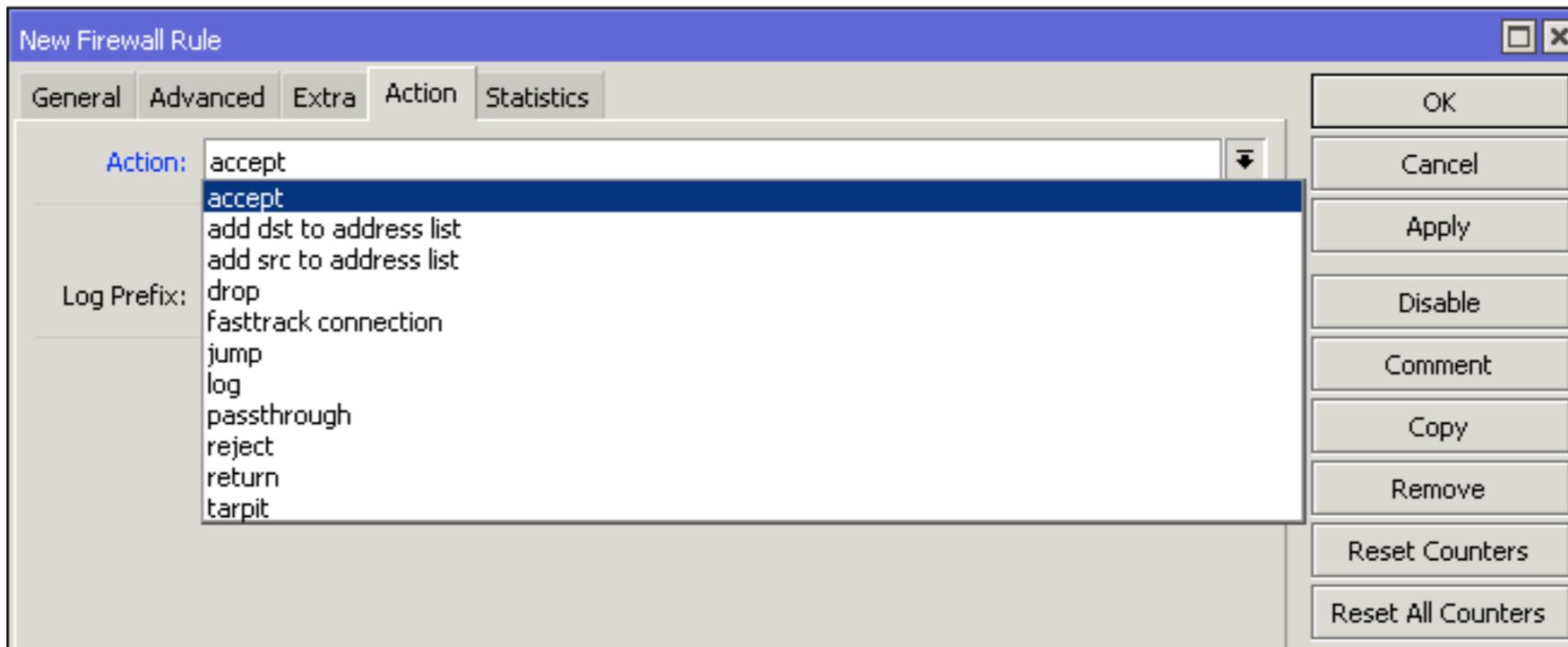
- There are three default chains
 - **input** (to the router)
 - **output** (from the router)
 - **forward** (through the router)



Filter Actions

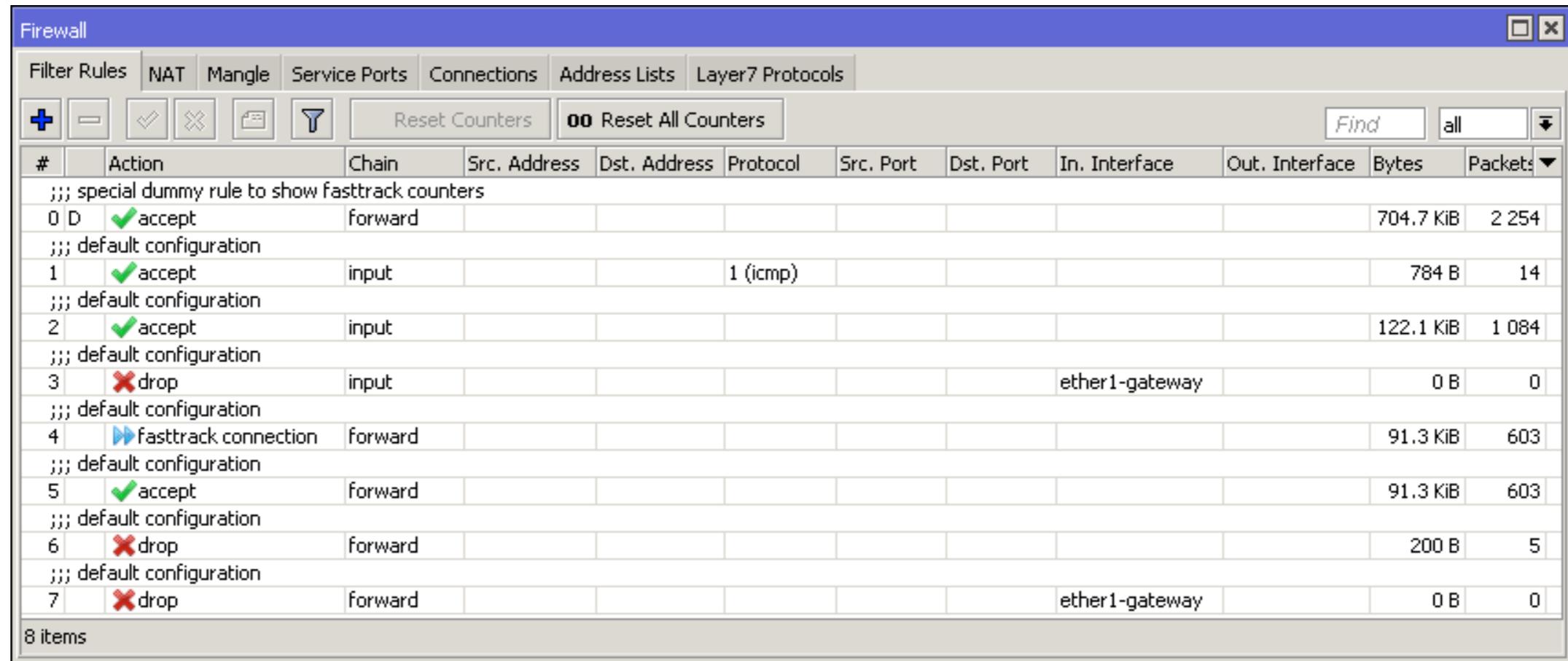
- Each rule has an action - what to do when a packet is matched
- **accept**
- **drop silently or reject** - drop and send ICMP reject message
- **jump/return to/from** a user defined chain
- And other - see [firewall wiki page](#)

Filter Actions



IP → Firewall → New Firewall Rule (+) → Action

Filter Chains



The screenshot shows the Mikrotik WinBox Firewall Filter Rules configuration window. The table displays 8 items, including comments and active rules. The rules are organized sequentially by chain (input, forward) and include actions like 'accept' and 'drop'. Comments are used to group rules and provide context.

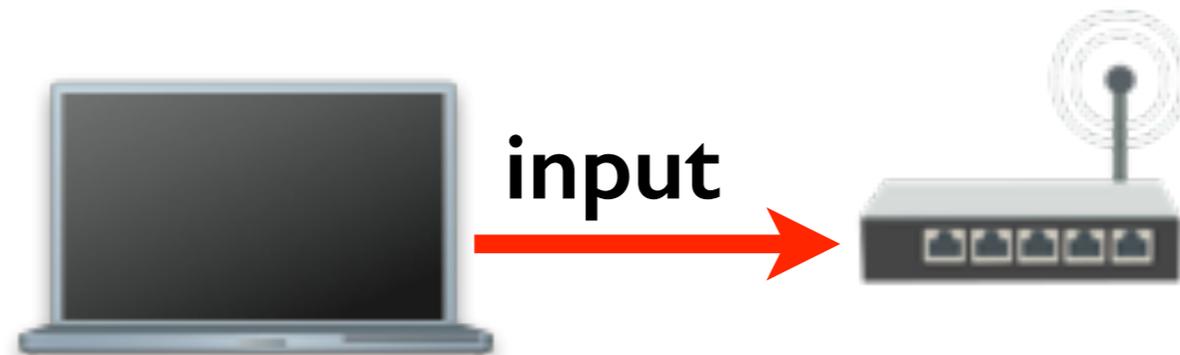
#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Interface	Out. Interface	Bytes	Packets
;;; special dummy rule to show fasttrack counters											
0	D ✓ accept	forward								704.7 KiB	2 254
;;; default configuration											
1	✓ accept	input			1 (icmp)					784 B	14
;;; default configuration											
2	✓ accept	input								122.1 KiB	1 084
;;; default configuration											
3	✗ drop	input						ether1-gateway		0 B	0
;;; default configuration											
4	▶▶ fasttrack connection	forward								91.3 KiB	603
;;; default configuration											
5	✓ accept	forward								91.3 KiB	603
;;; default configuration											
6	✗ drop	forward								200 B	5
;;; default configuration											
7	✗ drop	forward						ether1-gateway		0 B	0

IP → Firewall

- TIP: to improve readability of firewall rules, order them sequentially by chains and add comments

Chain: input

- Protects the router itself
- Either from the Internet or the internal network



Chain: input

- Add an **accept input** filter rule on the **bridge** interface for your laptop IP address (Src.Address = 192.168.XY.200)
- Add a **drop input** filter rule on the **bridge** interface for everyone else

Chain: input

New Firewall Rule

General | Advanced | Extra | Action | Statistics

Chain:

Src. Address: 192.168.199.200

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

P2P:

In. Interface: bridge-local

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

IP → Firewall → New Firewall Rule (+)

Chain: input

- Change the IP address of your laptop to static, assign 192.168.XY.199, DNS and gateway: 192.168.XY.1
- Disconnect from the router
- Try to connect to the router (not possible)
- Try to connect to the internet (not possible)

Chain: input

- Although traffic to the Internet is controlled with firewall **forward** chain, web pages cannot be opened
- **WHY?** (answer on the next slide)

Chain: input

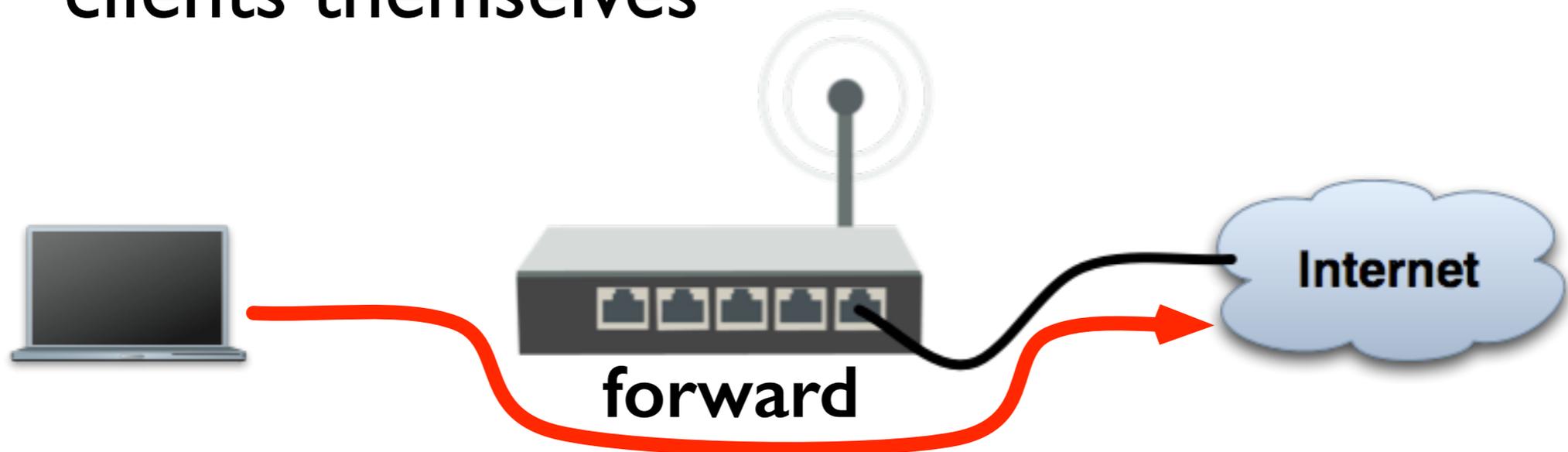
- Your laptop is using the router for domain name resolving (DNS)
- Connect to the router using MAC WinBox
- Add an **accept input** filter rule on the **bridge** interface to allow DNS requests, port: **53/udp** and place it above the drop rule
- Try to connect to the Internet (works)

Chain: input

- Change back your laptop IP to dynamic (DHCP)
- Connect to the router
- Disable (or remove) the rules you just added

Chain: forward

- Contains rules that control packets going through the router
- Forward controls traffic between the clients and the Internet and between the clients themselves



Chain: forward

- By default internal traffic between the clients connected to the router is allowed
- Traffic between the clients and the Internet is not restricted

Chain: forward

- Add a **drop forward** filter rule for http port (80/tcp)
- When specifying ports, IP protocol must be selected

New Firewall Rule

General Advanced Extra Action Statistics

Chain:

Src. Address:

Dst. Address:

Protocol: 6 (tcp)

Src. Port:

Dst. Port: 80

OK
Cancel
Apply
Disable
Comment
Copy
Remove

IP → Firewall → New Firewall Rule (+)

Chain: forward

- Try to open www.mikrotik.com (not possible)
- Try to open router WebFig <http://192.168.XY.1> (works)
- Router web page works because it is traffic going to the router (**input**), not through (**forward**)

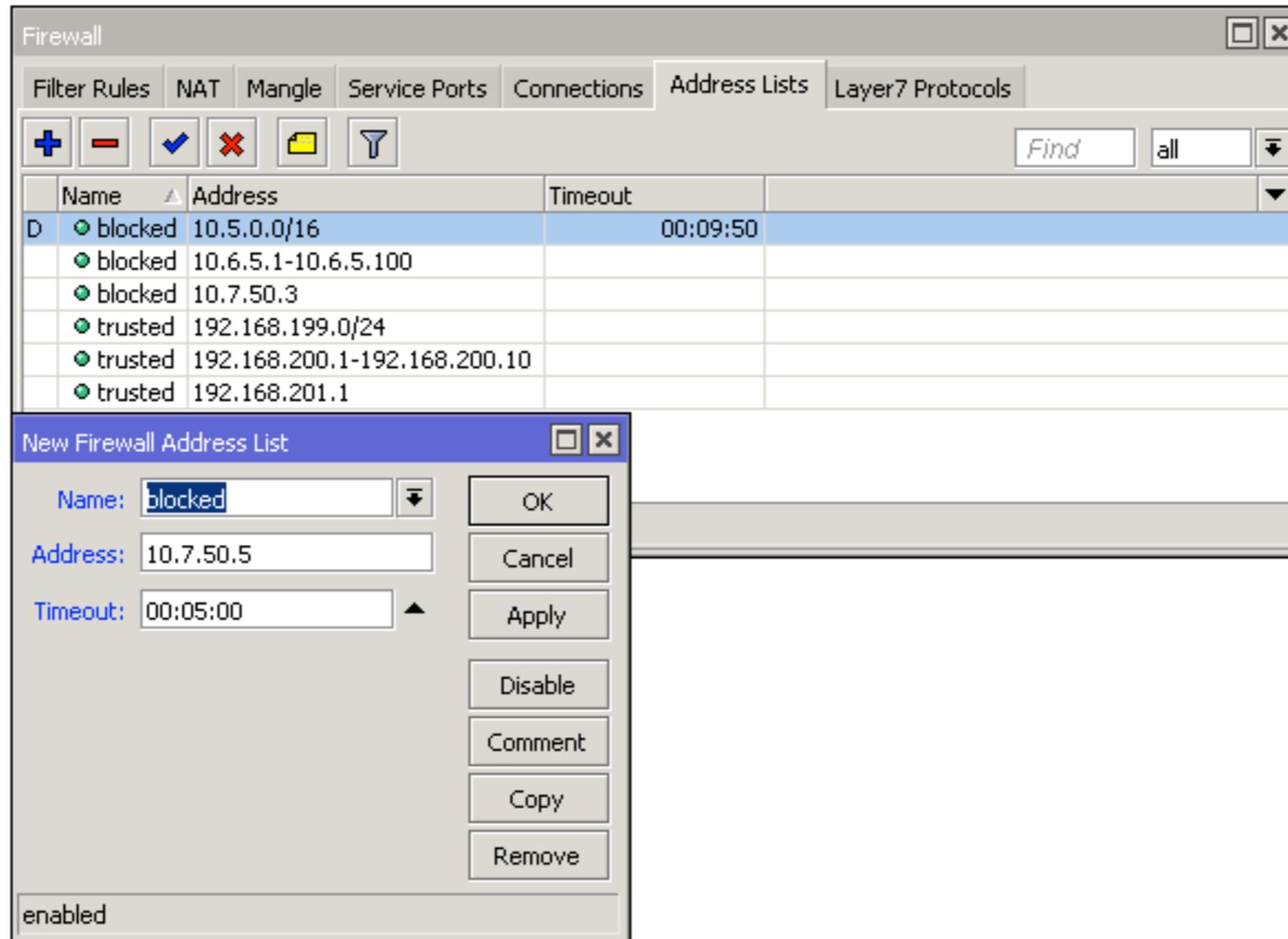
Frequently Used Ports

Port	Service
80/tcp	HTTP
443/tcp	HTTPS
22/tcp	SSH
23/tcp	Telnet
20,21/tcp	FTP
8291/tcp	WinBox
5678/udp	MikroTik Neighbor Discovery
20561/udp	MAC WinBox

Address List

- Address list allows to create an action for multiple IPs at once
- It is possible to automatically add an IP address to the address list
- IP can be added to the list permanently or for a predefined amount of time
- Address list can contain one IP address, IP range or whole subnet

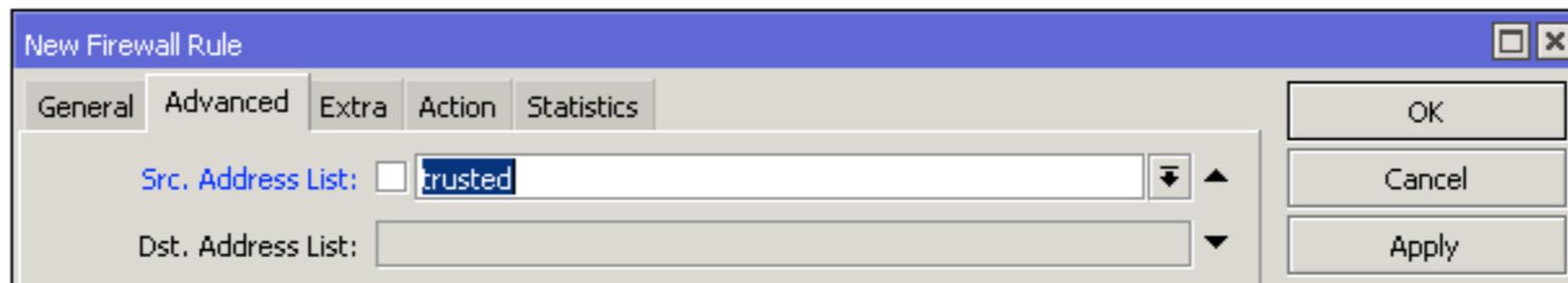
Address List



IP → Firewall → Address Lists → New Firewall Address List (+)

Address List

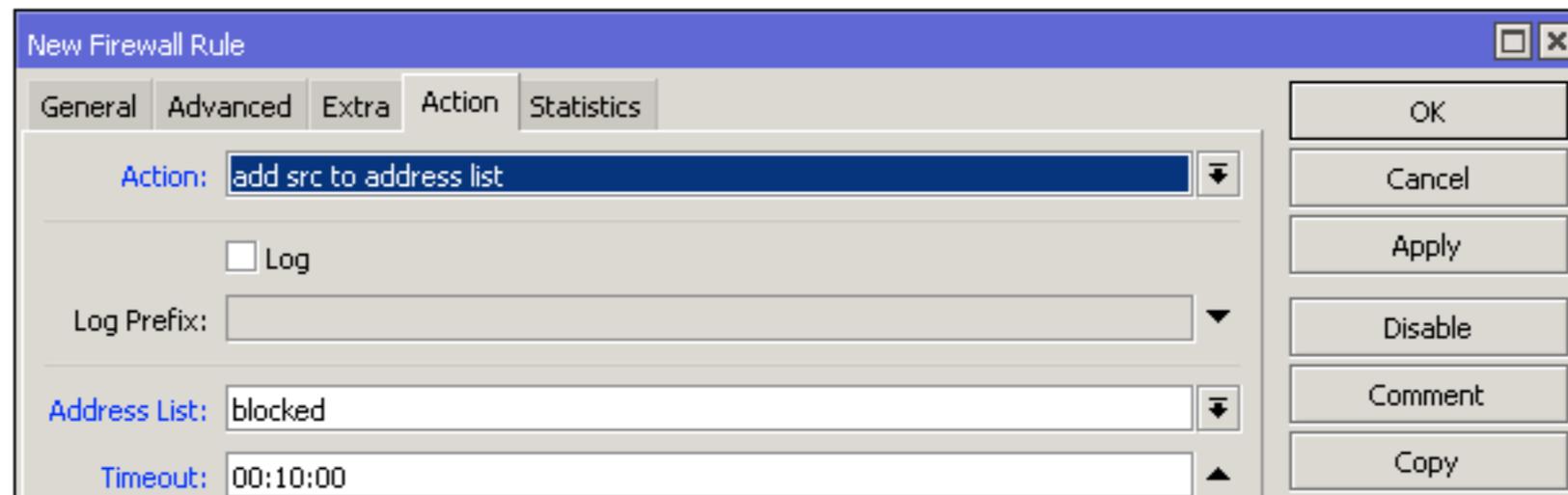
- Instead of specifying address in General tab, switch to Advanced and choose Address List (Src. or Dst. depending on the rule)



IP → Firewall → New Firewall Rule (+) → Advanced

Address List

- Firewall action can be used to automatically add an address to the address list
- Permanently or for a while



IP → Firewall → New Firewall Rule (+) → Action

Address List

- Create an address list with allowed IPs, be sure to include your laptop IP
- Add an **accept input** filter rule on the **bridge** interface for WinBox port when connecting from the address which is included in the address list
- Create a **drop input** filter for everyone else connecting to the WinBox

Firewall Log

- Each firewall rule can be logged when matched
- Can add specific prefix to ease finding the records later

Firewall Log

The screenshot shows the Mikrotik WinBox interface. The main window is titled 'Firewall' and displays a table of firewall rules. The 'Action' column shows 'accept' for several rules. A 'Firewall Rule' dialog box is open, showing the 'Action' tab with 'accept' selected and 'Log' checked. The 'Log Prefix' is set to 'FWPING'. Below the dialog, a 'Log' window displays a list of log entries for ICMP traffic.

#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Interface	Out. Interface	Bytes	Packets
0	accept	forward								998.6 MiB	1 354 681
1	accept	input			1 (icmp)					336 B	4

Time	Memory	Source	Destination	Protocol	Length
Nov/26/2015 14:25:12	memory	firewall, info	FWPING input: in:bridge-local out:(none), src-mac 00:1e:c2:fb:f8:36, proto ICMP (type 8, code 0), 192.168.199.200->192.168.199.254, len 84	ICMP	84
Nov/26/2015 14:25:13	memory	firewall, info	FWPING input: in:bridge-local out:(none), src-mac 00:1e:c2:fb:f8:36, proto ICMP (type 8, code 0), 192.168.199.200->192.168.199.254, len 84	ICMP	84
Nov/26/2015 14:25:14	memory	firewall, info	FWPING input: in:bridge-local out:(none), src-mac 00:1e:c2:fb:f8:36, proto ICMP (type 8, code 0), 192.168.199.200->192.168.199.254, len 84	ICMP	84

IP → Firewall → Edit Firewall Rule → Action

Firewall Log

- Enable logging for both firewall rules that were created during Address List LAB
- Connect to WinBox using allowed IP address
- Disconnect and change the IP of your laptop to one which is not in the allowed list
- Try to connect to WinBox
- Change back the IP and observe log entries

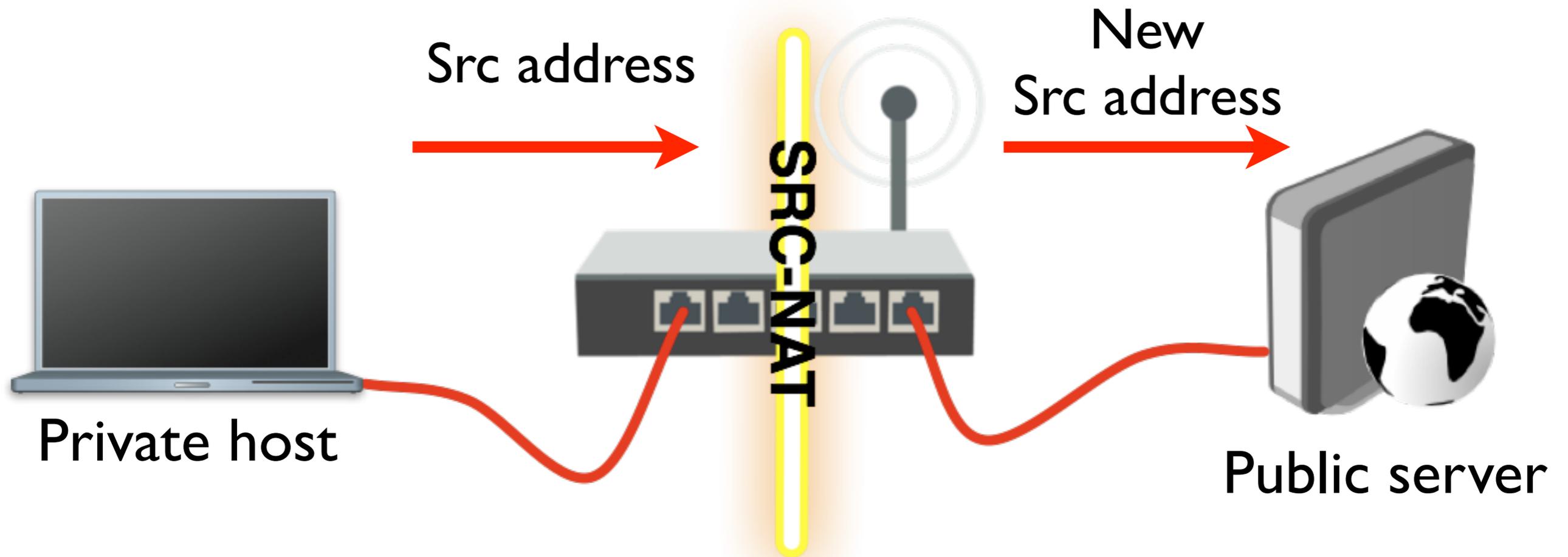
NAT

- Network Address Translation (NAT) is a method of modifying source or destination IP address of a packet
- There are two NAT types - 'source NAT' and 'destination NAT'

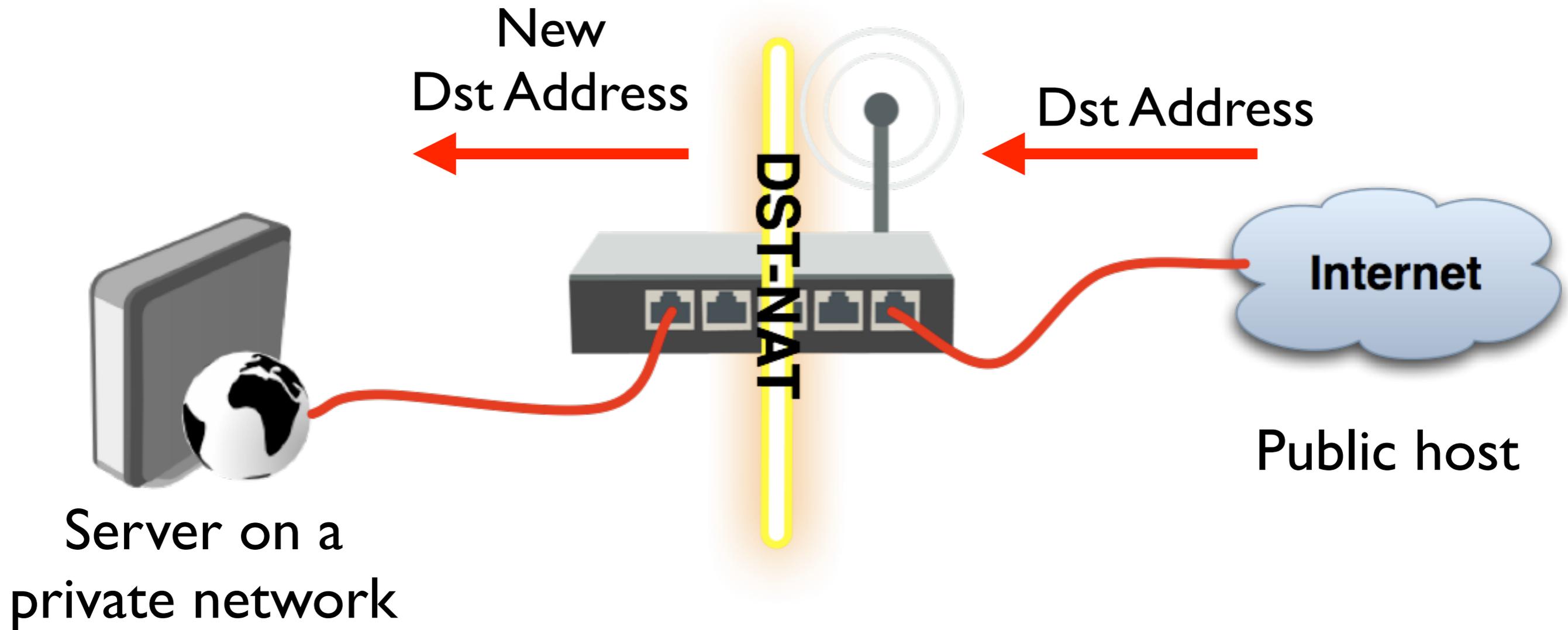
NAT

- NAT is usually used to provide access to an external network from a one which uses private IPs (**src-nat**)
- Or to allow access from an external network to a resource (e.g. web server) on an internal network (**dst-nat**)

NAT



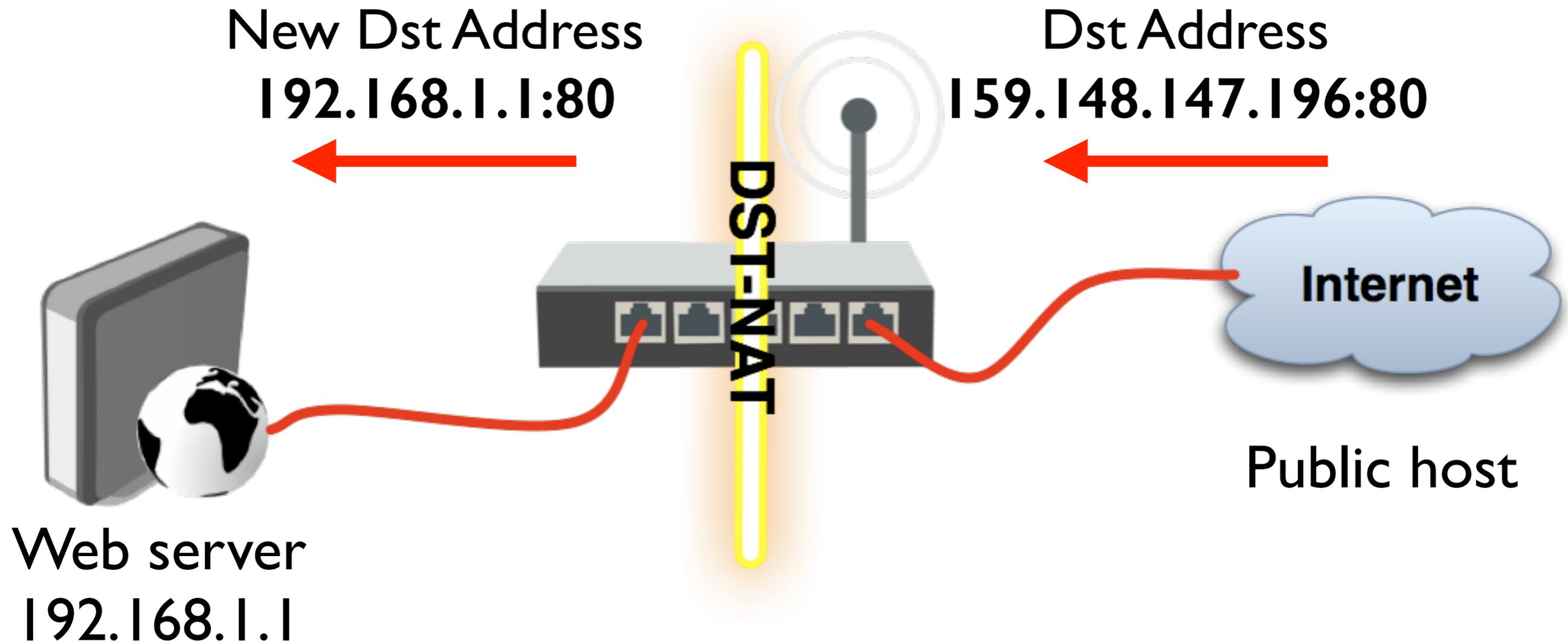
NAT



NAT

- Firewall **srcnat** and **dstnat** chains are used to implement NAT functionality
- Same as Filter rules, work on **If-Then** principle
- Analysed sequentially until first match is found

Dst NAT



Dst NAT

The image shows two screenshots of the Mikrotik WinBox Firewall configuration interface. The top screenshot is the 'NAT Rule <80>' configuration window, with the 'General' tab selected. The 'Chain' is set to 'dstnat'. The 'Protocol' is set to '6 (tcp)'. The 'Dst. Port' is set to '80'. The 'In. Interface' is set to 'ether1-gateway'. The bottom screenshot is the 'New NAT Rule' configuration window, with the 'Action' tab selected. The 'Action' is set to 'dst-nat'. The 'Log' checkbox is unchecked. The 'To Addresses' field is set to '192.168.199.200'. The 'To Ports' field is set to '80'. Both windows have a vertical stack of buttons on the right side: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, and Reset All Counters.

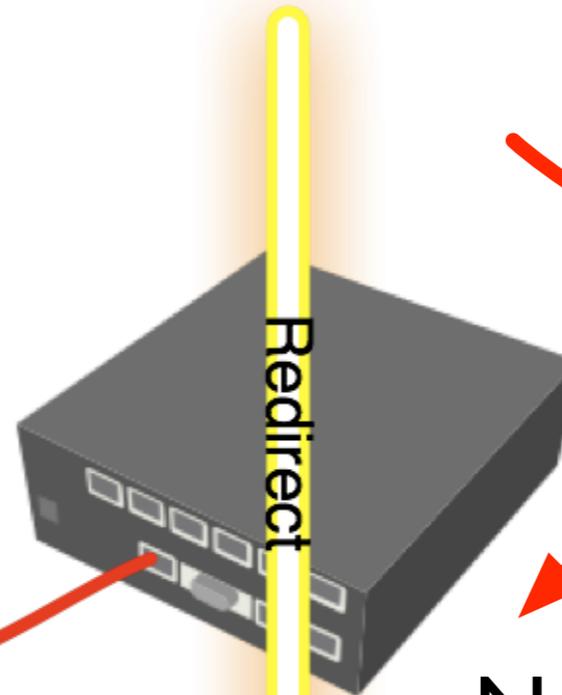
IP → Firewall → NAT → New NAT Rule (+)

Redirect

- Special type of `dstnat`
- This action redirects packets to the router itself
- Can be used to create transparent proxy services (e.g. DNS, HTTP)

Redirect

Dst Address
Configured DNS server:53



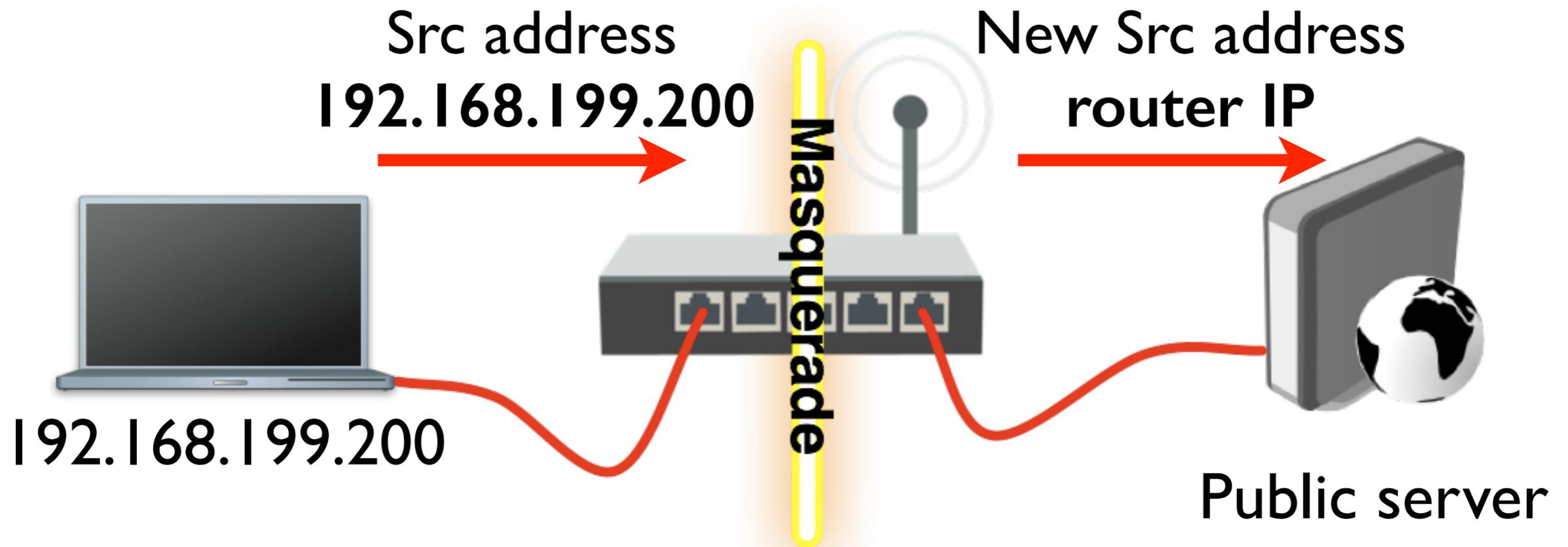
New Dst Address
Router:53

DNS
Cache

Redirect

- Create dstnat redirect rule to send all requests with a destination port HTTP (tcp/80) to the router port 80
- Try to open www.mikrotik.com or any other website that uses HTTP protocol
- When done disable or remove the rule

Src NAT



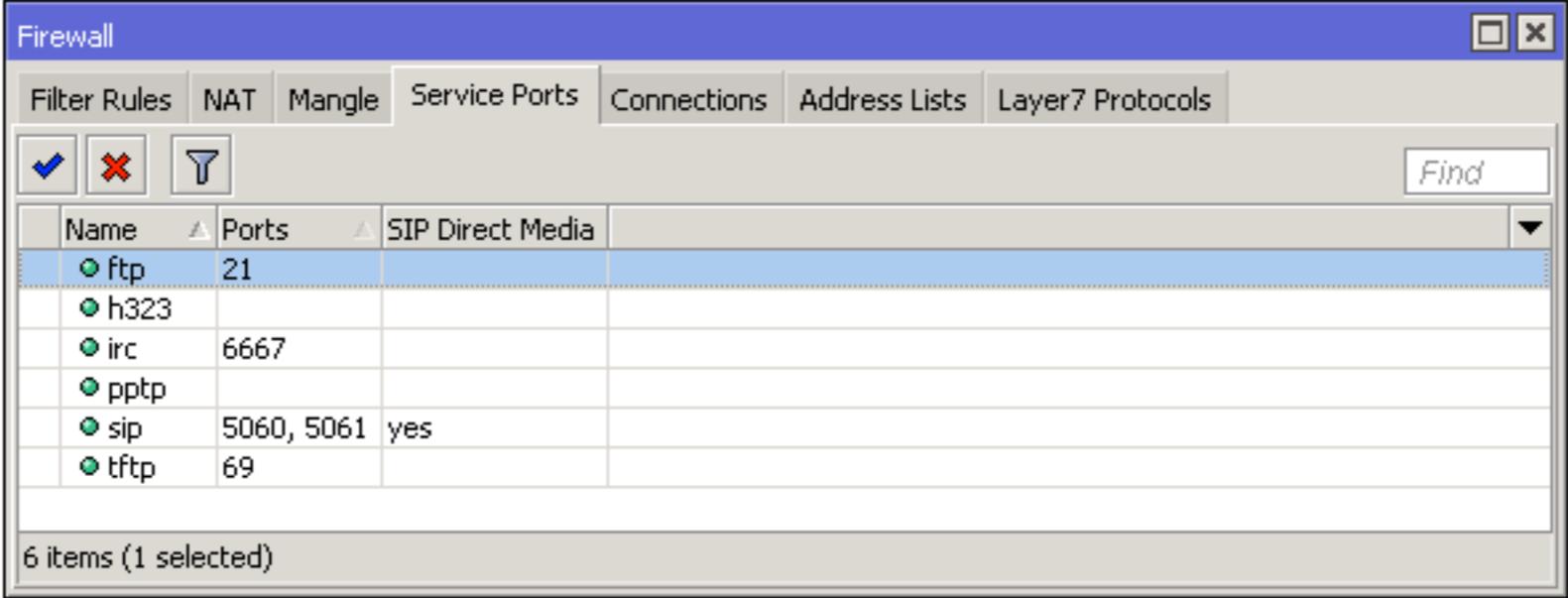
- **Masquerade** is a special type of srcnat

Src NAT

- srcnat action src-nat is meant for rewriting source IP address and/or port
- Example: two companies (A and B) have merged. Internally both use the same address space (172.16.0.0/16). They will set up a segment using a different address space as a buffer, both networks will require src-nat and dst-nat rules.

NAT Helpers

- Some protocols require so-called NAT helpers to work correctly in a NAT'd network



The screenshot shows the Mikrotik WinBox interface for configuring NAT helpers. The 'Service Ports' tab is active, displaying a table of protocols. The 'ftp' protocol is selected.

Name	Ports	SIP Direct Media
ftp	21	
h323		
irc	6667	
pptp		
sip	5060, 5061	yes
tftp	69	

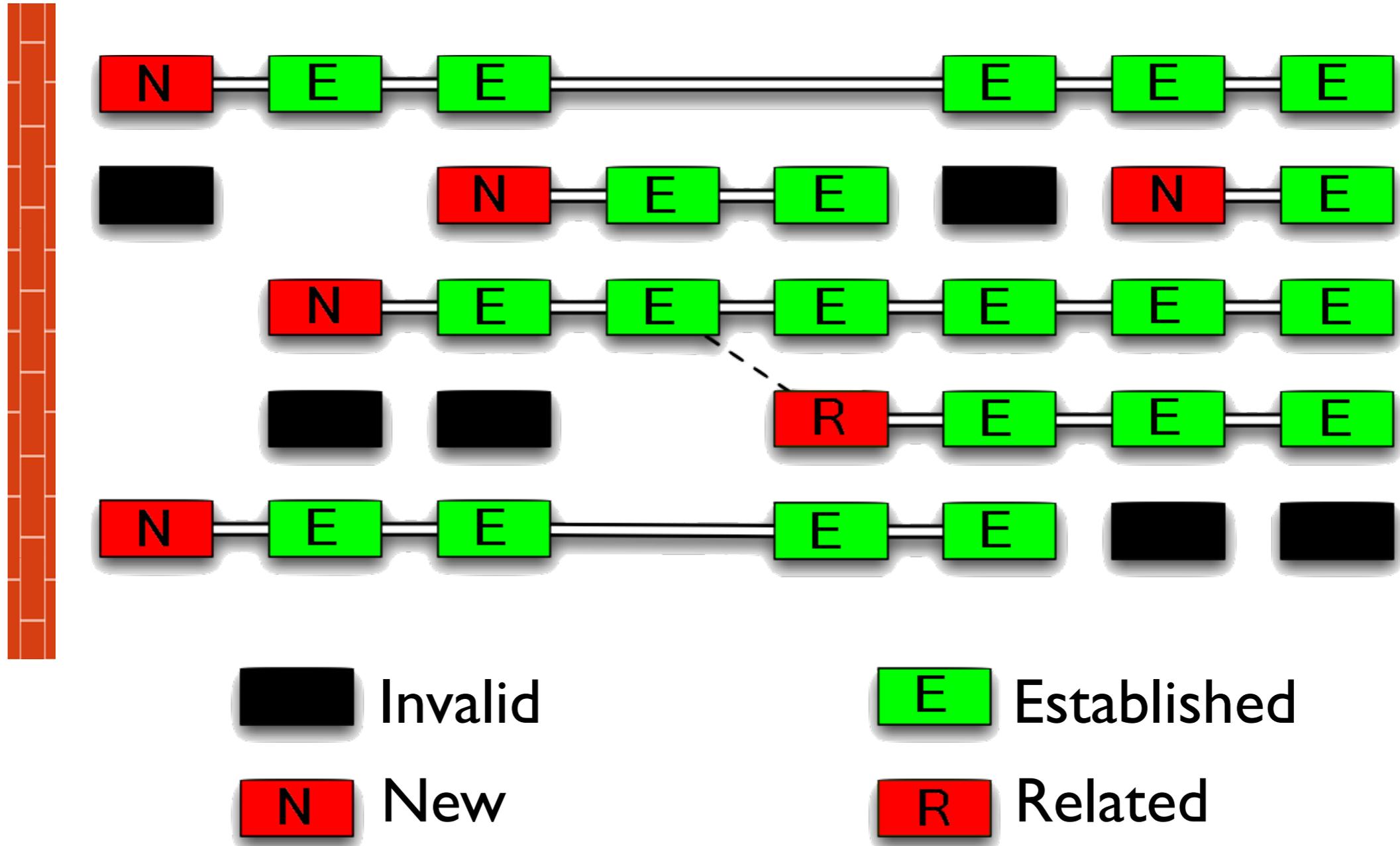
6 items (1 selected)

IP → Firewall → Service Ports

Connections

- **New** - packet is opening a new connection
- **Established** - packet belongs to already known connection
- **Related** - packet is opening a new connection but it has a relation to already known connection
- **Invalid** - packet does not belong to any of known connections

Connections



Connection Tracking

- Manages information about all active connections
- Has to be enabled for NAT and Filter to work
- Note: connection state \neq TCP state

Connection Tracking

The screenshot shows the Mikrotik WinBox interface. The main window is titled 'Firewall' and has several tabs: Filter Rules, NAT, Mangle, Service Ports, Connections, Address Lists, and Layer7 Protocols. The 'Connections' tab is active, showing a table of active connections. A 'Tracking' button is visible above the table. The 'Connection Tracking' dialog box is open on the right, showing various timeout settings for TCP and UDP connections.

	Src. Address	Dst. Address	Protocol	Connection Mark	Timeout	TCP State
C	192.168.199.200:17500	255.255.255.255:17500	17 (udp)		00:00:09	
SACFs	192.168.199.200:11785	213.199.179.172:40035	17 (udp)		00:00:30	
SACFs	192.168.199.200:11785	213.199.179.157:40023	17 (udp)		00:02:35	
SACFs	192.168.199.200:11785	213.199.179.153:40025	17 (udp)		00:00:30	
C	192.168.199.200:17500	192.168.199.255:17500	17 (udp)		00:00:09	
SAC	192.168.199.200:59898	192.168.199.254:8291	6 (tcp)		23:59:59	established
SACFs	192.168.199.200:62355	191.235.128.131:443	6 (tcp)		00:00:09	close
SACFs	192.168.199.200:11785	157.56.52.44:40026	17 (udp)		00:00:30	
SACFs	192.168.199.200:11785	157.56.52.29:40021	17 (udp)		00:02:32	
SACFs	192.168.199.200:11785	157.55.235.172:40018	17 (udp)		00:02:30	
SACFs	192.168.199.200:11785	157.55.235.172:40002	17 (udp)		00:02:35	
SACFs	192.168.199.200:11785	157.55.235.157:40021	17 (udp)		00:02:32	
SACFs	192.168.199.200:11785	157.55.235.146:40005	17 (udp)		00:00:27	
SACFs	192.168.199.200:11785	157.55.130.176:40035	17 (udp)		00:02:32	
SACFs	192.168.199.200:11785	157.55.56.148:40032	17 (udp)		00:02:32	
SACFs	192.168.199.200:11785	152.236.66.231:48760	17 (udp)		00:02:32	
SACFs	192.168.199.200:11785	111.221.77.174:40003	17 (udp)		00:02:32	
SACFs	192.168.199.200:11785	111.221.77.170:40013	17 (udp)		00:00:31	

41 items (1 selected) Max Entries: 88080

Connection Tracking

Enabled: auto

TCP Syn Sent Timeout: 00:00:05

TCP Syn Received Timeout: 00:00:05

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

TCP Max Retransmit Timeout: 00:05:00

TCP Unacked Timeout: 00:05:00

UDP Timeout: 00:00:10

UDP Stream Timeout: 00:03:00

ICMP Timeout: 00:00:10

Generic Timeout: 00:10:00

IP → Firewall → Connections

FastTrack

- 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

FastTrack

Without	With
360Mbps	890Mbps
Total CPU usage 100%	Total CPU usage 86%
44% CPU usage on firewall	6% CPU usage on firewall

* Tested on RB2011 with a single TCP stream

- For more info see [FastTrack wiki page](#)

Module 6

Summary



Certified Network Associate (MTCNA)

Module 7

QoS

Quality of Service

- QoS is the overall performance of a network, particularly the performance seen by the users of the network
- RouterOS implements several QoS methods such as traffic speed limiting (shaping), traffic prioritisation and other

Speed Limiting

- Direct control over inbound traffic is not possible
- But it is possible to do it indirectly by dropping incoming packets
- TCP will adapt to the effective connection speed

Simple Queue

- Can be used to easy limit the data rate of:
 - Client's download (\downarrow) speed
 - Client's upload (\uparrow) speed
 - Client's total speed ($\downarrow + \uparrow$)

Simple Queue

Queue List

Simple Queues Interface Queues Queue Tree Queue Types

+ - ✓ ✕ 📄 🔍 Reset Counters 00 Reset All Counters Find

#	Name	Target	Upload Max Limit	Download Max Limit	Packet Marks	Total Max Limit (bits/s)
---	------	--------	------------------	--------------------	--------------	--------------------------

New Simple Queue

General Advanced Statistics Traffic Total Total Statistics

Name: queue1

Target: 192.168.199.200

Dst.:

	Target Upload	Target Download
Max Limit:	256k	512k
Burst Limit:	unlimited	unlimited
Burst Threshold:	unlimited	unlimited
Burst Time:	0	0

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

enabled

Specify client

Specify Max Limit
for the client

Queues → New Simple Queue(+)

- Disable Firewall FastTrack rule for Simple Queue to work

Torch

- Real-time traffic monitoring tool

Set interface →

Set laptop address ←

Observe the traffic →

Eth. Protocol	Protocol	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
800 (ip)	6 (tcp)	192.168.199.200:55369	205.251.219.190:80 (http)			242.2 kbps	8.8 kbps	20	16
800 (ip)	6 (tcp)	192.168.199.200:54832	192.168.199.254:8291 (winbox)			17.0 kbps	1584 bps	3	3

2 items (1 selected) | Total Tx: 259.3 kbps | Total Rx: 10.4 kbps | Total Tx Packet: 23 | Total Rx Packet: 19

Tools → Torch

Simple Queue

- Create speed limit for your laptop (192.168.XY.200)
- Set upload speed 128k, download speed 256k
- Open www.mikrotik.com/download and download current RouterOS version
- Observe the download speed

Simple Queue

- Instead of setting limits to the client, traffic to the server can also be throttled

Set Target to any →
Set Dst. to server address →

Simple Queue <queue1>

General Advanced Statistics Traffic Total Total Statistics

Name: queue1

Target: 0.0.0.0/0

Dst.: 1.2.3.4

	Target Upload	Target Download
Max Limit:	128k	256k
Burst Limit:	unlimited	unlimited
Burst Threshold:	unlimited	unlimited
Burst Time:	0	0

enabled

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

Queues

Simple Queue

- Using ping tool find out the address of www.mikrotik.com
- Modify existing simple queue to throttle connection to the mikrotik.com server
- Download [MTCNA outline](#)
- Observe the download speed

Guaranteed Bandwidth

- Used to make sure that the client will always get minimum bandwidth
- Remaining traffic will be split between clients on first come first served basis
- Controlled using **Limit-at** parameter

Guaranteed Bandwidth

Set limit at



Simple Queue <129>

General Advanced Statistics Traffic Total Total Statistics

Packet Marks:

Target Upload Target Download

Limit At: 1M 1M bits/s

Priority: 8 8

Queue Type: default-small default-small

Parent: parent

enabled

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

Queues → Simple Queue → Edit → Advanced

- The client will have guaranteed bandwidth 1Mbit download and upload

Guaranteed Bandwidth

- Example:
 - Total bandwidth: 10Mbits
 - 3 clients, each have guaranteed bandwidth
 - Remaining bandwidth split between clients

Guaranteed Bandwidth

#	Name	Target	Upload Max Limit	Upload Limit At	Upload Priority	Upload
0	parent	192.168.199.128/29	10M	unlimited	8	10.0 Mbps
1	129	192.168.199.129	10M	1M	8	1496.2 kbps
3	130	192.168.199.130	10M	4M	8	5.9 Mbps
2	131	192.168.199.131	10M	2M	8	2.6 Mbps

4 items 0 B queued 0 packets queued

**Guranteed
bandwidth**

**Actual
bandwidth**

Queues

Burst

- Used to allow higher data rates for a short period of time
- Useful for HTTP traffic - web pages load faster
- For file downloads Max Limit restrictions still apply

Burst

**Set burst limit,
threshold and
time**

Simple Queue <queue1 >

General | Advanced | Statistics | Traffic | Total | Total Statistics

Name: queue1

Target: 192.168.199.200

Dst.:

	Target Upload	Target Download
Max Limit:	256k	512k
bits/s		
-▲- Burst		
Burst Limit:	4M	4M
bits/s		
Burst Threshold:	2M	2M
bits/s		
Burst Time:	16	16
s		
-▼- Time		

enabled

Queues → Simple Queue → Edit

Burst

- **Burst limit** - max upload/download data rate that can be reached during the burst
- **Burst time** - time (sec), over which the average data rate is calculated (this is NOT the time of actual burst).
- **Burst threshold** - when average data rate exceeds or drops below the threshold the burst is switched off or on

Burst

- Modify the queue that was created in previous LAB
- Set burst limit to 4M for upload and download
- Set burst threshold 2M for upload and download
- Set burst time 16s for upload and download

Burst

- Open www.mikrotik.com, observe how fast the page loads
- Download the newest RouterOS version from [MikroTik download page](#)
- Observe the download speed with torch tool

Per Connection Queuing

- Queue type for optimising large QoS deployments by limiting per ‘sub-stream’
- Substitute multiple queues with one
- Several classifiers can be used:
 - source/destination IP address
 - source/destination port

Per Connection Queuing

- Rate - max available data rate of each sub-stream
- Limit - queue size of single sub-stream (KiB)
- Total Limit - max amount of queued data in all sub-streams (KiB)

PCQ Example

- Goal: limit all clients to 1 Mbps download and 1 Mbps upload bandwidth
- Create 2 new queue types
 - 1 for Dst Address (download limit)
 - 1 for Src Address (upload limit)
- Set queues for LAN and WAN interfaces

PCQ Example

The screenshot shows the Mikrotik Queue List and Queue Type configuration interface. On the left, the 'Queue List' window displays a table of queue types. The 'Queue Types' tab is active, showing a list of 12 items. The 'client-up' queue type is selected. Two configuration windows are open: 'Queue Type <client-up>' and 'Queue Type <client-down>'. Red arrows point from the 'client-up' entry in the list to the 'client-up' configuration window, and from the 'client-down' entry to the 'client-down' configuration window. The configuration windows show fields for Type Name, Kind, Rate, Limit, Total Limit, Burst Rate, Burst Threshold, Burst Time, and Classifier. The 'client-up' window has 'Src. Address' checked in the Classifier, while the 'client-down' window has 'Dst. Address' checked. The 'Queue List' window shows the following table:

Type Name	Kind
client-down	pcq
client-up	pcq
default	pfifo
default-small	pfifo
ethernet-default	pfifo
hotspot-default	sfq
multi-queue-ethernet-default	mq pfifo
only-hardware-queue	none
pcq-download-default	pcq
pcq-upload-default	pcq
synchronous-default	red
wireless-default	sfq

Queues → Queue Type → New Queue Type(+)

PCQ Example

Interface	Queue Type	Default Queue Type
ether1-gateway	only-hardware-queue	only-hardware-queue
ether2-master-local	only-hardware-queue	only-hardware-queue
ether3-slave-local	only-hardware-queue	only-hardware-queue
ether4-slave-local	only-hardware-queue	only-hardware-queue
ether5-slave-local	only-hardware-queue	only-hardware-queue
wlan1	only-hardware-queue	wireless-default

6 items (1 selected)

WAN interface →

Interface: wlan1
Queue Type: client-up
Default Queue Type: wireless-default

OK Cancel Apply

LAN interface →

Interface: ether2-master-local
Queue Type: client-down
Default Queue Type: only-hardware-queue

OK Cancel Apply

Queues → Interface Queues

PCQ Example

- All clients connected to the LAN interface will have 1Mbps upload and download limit

The screenshot shows the Mikrotik Torch (Running) window. The 'Basic' tab is selected, showing the interface 'ether2-master-local' and an entry timeout of 00:00:03. The 'Collect' tab shows checkboxes for 'Src. Address', 'Dst. Address', 'MAC Protocol', 'Protocol', 'DSCP', 'Src. Address6', 'Dst. Address6', 'Port', and 'VLAN Id'. The 'Filters' tab shows various filters set to 'any'. The table below shows three active connections:

Eth. ...	Pro...	Src.	Dst.	VLAN Id	DSCP	Tx Rate	Rx Rate	Tx Pack...	Rx Pack.
800 (ip)		192.168.199.200	85.254.250.18			956.8 kbps	27.9 kbps	79	5
800 (ip)		192.168.199.200	45.58.74.161			30.4 kbps	979.5 k...	56	10
800 (ip)		192.168.199.200	192.168.199.254			13.9 kbps	3.1 kbps	3	

The summary bar at the bottom shows: Total Tx: 1005.3 kbps, Total Rx: 1023.0 kbps, Total Tx Packet: 144, Total Rx Packet: 181. A red arrow points to the 'Total Tx' field.

Tools → Torch

PCQ Example

- The trainer will create two pcq queues and limit all clients (student routers) to 512Kbps upload and download bandwidth
- Try download newest RouterOS version from www.mikrotik.com and observe the download speed with torch tool

Module 7

Summary



Certified Network Associate (MTCNA)

Module 8

Tunnels

Point-to-Point Protocol

- Point-to-Point Protocol (PPP) is used to establish a tunnel (direct connection) between two nodes
- PPP can provide connection authentication, encryption and compression
- RouterOS supports various PPP tunnels such as PPPoE, SSTP, PPTP and others

PPPoE

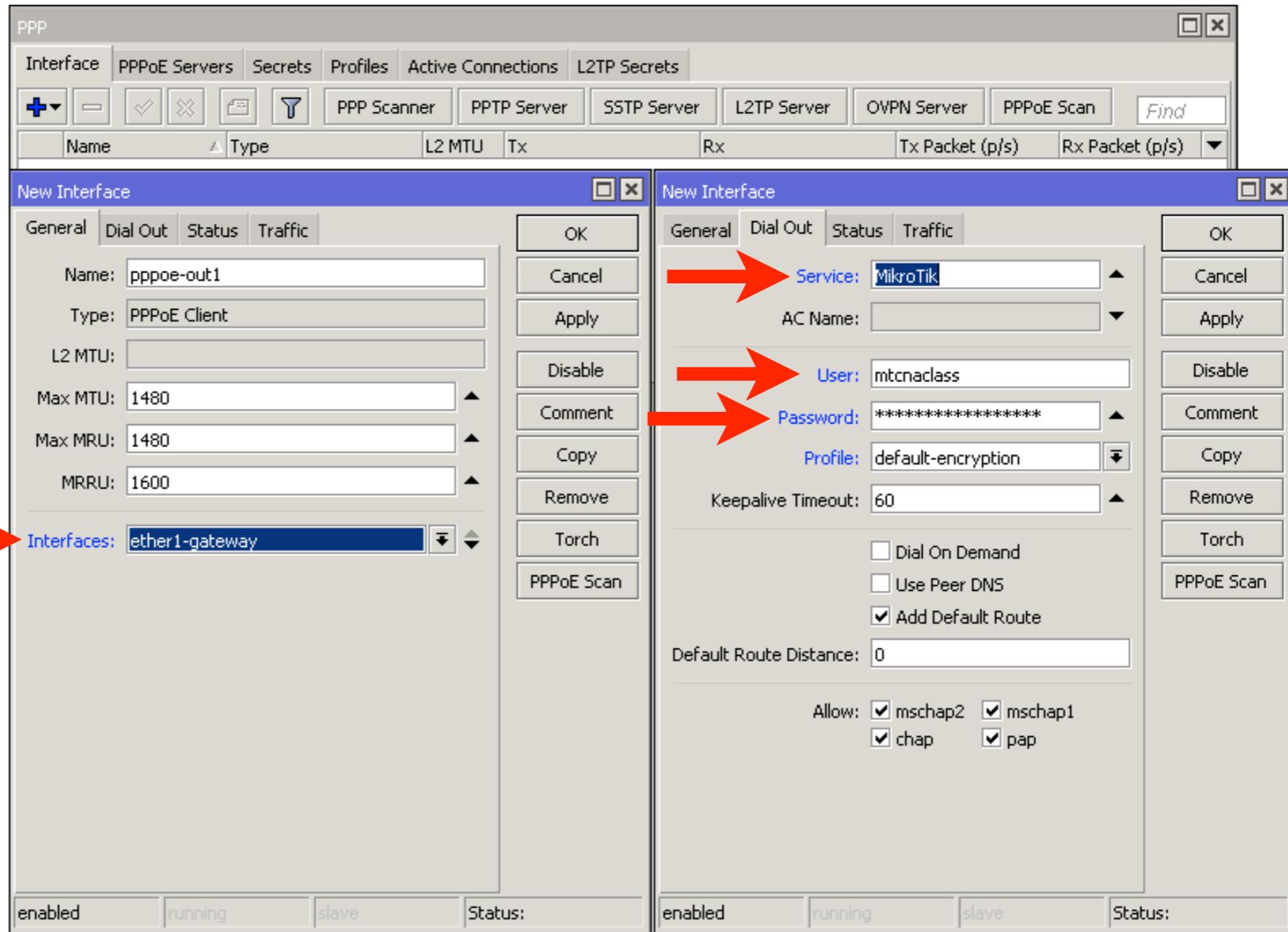
- Point-to-Point Protocol over Ethernet is a layer 2 protocol which is used to control access to the network
- Provides authentication, encryption and compression
- PPPoE can be used to hand out IP addresses to the clients

PPPoE

- Most desktop operating systems have PPPoE client installed by default
- RouterOS supports both PPPoE client and PPPoE server (access concentrator)

PPPoE Client

**Set
interface,
service,
username,
password**



PPP → New PPPoE Client(+)

PPPoE Client

- If there are more than one PPPoE servers in a broadcast domain **service name** should also be specified
- Otherwise the client will try to connect to the one which responds first

PPPoE Client

- The trainer will create a PPPoE server on his/her router
- Disable the DHCP client on your router
- Set up PPPoE client on your router's outgoing interface
- Set username **mtcna** class password **mtcna**

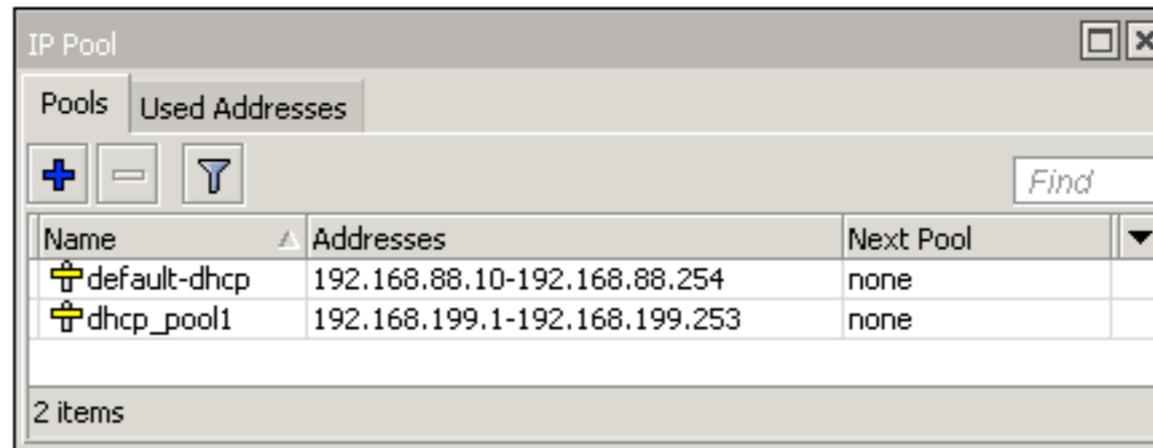
PPPoE Client

- Check PPPoE client status
- Check that the connection to the Internet is available
- When done, disable PPPoE client
- Enable DHCP client to restore previous configuration

IP Pool

- Defines the range of IP addresses for handing out by RouterOS services
- Used by DHCP, PPP and HotSpot clients
- Addresses are taken from the pool automatically

IP Pool

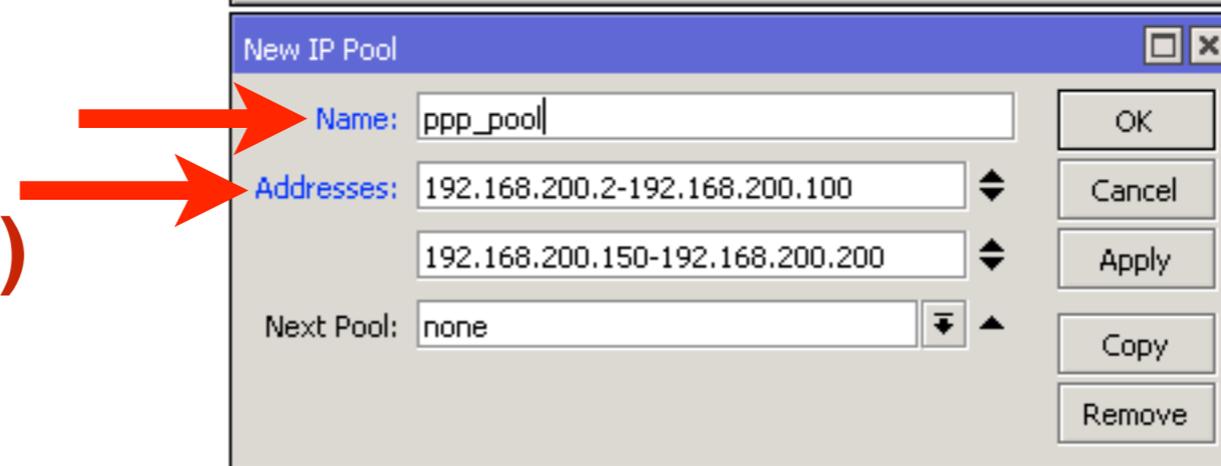


The screenshot shows the 'IP Pool' window with two tabs: 'Pools' and 'Used Addresses'. The 'Pools' tab is active, displaying a table with the following data:

Name	Addresses	Next Pool
default-dhcp	192.168.88.10-192.168.88.254	none
dhcp_pool1	192.168.199.1-192.168.199.253	none

Below the table, it indicates '2 items'.

Set the pool name and address range(s)



The 'New IP Pool' dialog box is shown with the following fields and values:

- Name: ppp_pool
- Addresses: 192.168.200.2-192.168.200.100 and 192.168.200.150-192.168.200.200
- Next Pool: none

Buttons on the right include OK, Cancel, Apply, Copy, and Remove. Two red arrows point from the text 'Set the pool name and address range(s)' to the 'Name' and 'Addresses' fields respectively.

IP → Pool → New IP Pool(+)

PPP Profile

- Profile defines rules used by PPP server for its clients
- Method to set the same settings for multiple clients

PPP Profile

PPP

Interface PPPoE Servers Secrets Profiles Active Connections L2TP Secrets

Name	Local Address	Remote Address	Bridge	Rate Limit (rx/tx)	Only One
default					default
default-encryption					default

New PPP Profile

General Protocols Limits Queue Scripts

Name: profile1

Local Address: 192.168.200.1

Remote Address: ppp_pool

Bridge: ppp_pool

Bridge Port Priority: []

Bridge Path Cost: []

Incoming Filter: []

Outgoing Filter: []

Address List: []

DNS Server: []

WINS Server: []

Change TCP MSS

no yes default

Use UPnP

no yes default

New PPP Profile

General Protocols Limits Queue Scripts

Use MPLS

no yes required default

Use Compression

no yes default

Use Encryption

no yes required default

Set the local and remote address of the tunnel

It is suggested to use encryption

PPP → Profiles → New PPP Profile(+)

PPP Secret

- Local PPP user database
- Username, password and other user specific settings can be configured
- Rest of the settings are applied from the selected PPP profile
- PPP secret settings override corresponding PPP profile settings

PPP Secret

Set the username, password and profile. Specify service if necessary

The screenshot shows the Mikrotik PPP configuration interface. The 'Secrets' tab is selected. A 'New PPP Secret' dialog box is open, allowing the configuration of a new secret. The fields are as follows:

- Name: client1
- Password: masked with asterisks
- Service: any
- Caller ID: (empty)
- Profile: profile1
- Local Address: (empty)
- Remote Address: (empty)
- Routes: (empty)
- Limit Bytes In: (empty)
- Limit Bytes Out: (empty)
- Last Logged Out: (empty)

The 'enabled' checkbox at the bottom is checked. Red arrows point to the Name, Password, and Profile fields.

PPP → Secrets → New PPP Secret(+)

PPPoE Server

- PPPoE server runs on an interface
- Can not be configured on an interface which is part of a bridge
- Either remove from the bridge or set up PPPoE server on the bridge
- For security reasons IP address should not be used on the interface on which PPPoE server is configured

PPPoE Server

Set the service name, interface, profile and authentication protocols

The screenshot shows the MikroTik WinBox interface for configuring PPPoE servers. The 'PPP' menu is open, and the 'PPPoE Servers' tab is selected. A table lists existing services, and a 'New PPPoE Service' dialog box is open. The dialog box contains the following fields and options:

- Service Name:** `pppoe_server` (indicated by a red arrow)
- Interface:** `ether5` (indicated by a red arrow)
- Max MTU:** `1480`
- Max MRU:** `1480`
- MRRU:** `1600`
- Keepalive Timeout:** `10`
- Default Profile:** `profile1` (indicated by a red arrow)
- One Session Per Host
- Max Sessions:** (empty dropdown)
- Authentication:** `mschap2`, `mschap1`, `chap`, `pap` (indicated by a red arrow)

Buttons on the right include OK, Cancel, Apply, Disable, Copy, and Remove. The status at the bottom is 'enabled'.

PPP Status

- Information about currently active PPP users

The screenshot displays the Mikrotik WinBox interface for PPP management. The 'Active Connections' tab is selected, showing a table with one active user:

Name	Service	Caller ID	Encoding	Address	Uptime
client1	pppoe	00:1E:C2:FB:F8:36		192.168.200.100	00:01:01

Below the table, a 'PPP Active User <client1>' dialog box is open, showing the following details:

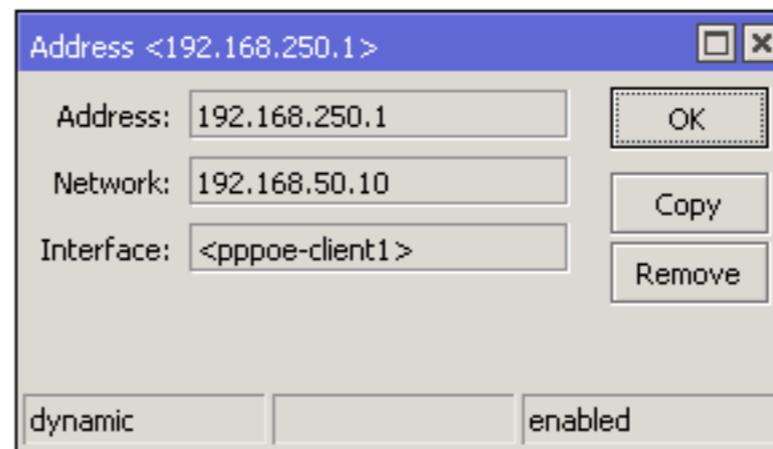
- Name: client1
- Service: pppoe
- Caller ID: 00:1E:C2:FB:F8:36
- Encoding: (empty)
- Address: 192.168.200.100
- Uptime: 00:01:01
- Session ID: 81900000 hex
- Limit Bytes In: (empty)
- Limit Bytes Out: (empty)

The dialog box also includes 'OK', 'Remove', and 'Ping' buttons. The 'local' user is listed at the bottom of the dialog.

PPP → Active Connections

Point-to-Point Addresses

- When a connection is made between the PPP client and server, /32 addresses are assigned
- For the client network address (or gateway) is the other end of the tunnel (router)



A screenshot of a MikroTik configuration window titled "Address <192.168.250.1>". The window contains three input fields: "Address" with the value "192.168.250.1", "Network" with the value "192.168.50.10", and "Interface" with the value "<pppoe-client1>". To the right of these fields are three buttons: "OK", "Copy", and "Remove". At the bottom of the window, there are two dropdown menus: the first is set to "dynamic" and the second is set to "enabled".

Point-to-Point Addresses

- Subnet mask is not relevant when using PPP addressing
- PPP addressing saves 2 IP addresses
- If PPP addressing is not supported by the other device, /30 network addressing should be used

PPPoE Server

- Set up PPPoE server on an unused LAN interface (e.g. eth5) of the router
- Remove eth5 from the switch (set master port: none)
- Check that the interface is not a port of the bridge
- Check that the interface has no IP address

PPPoE Server

- Create an IP pool, PPP profile and secret for the PPPoE server
- Create the PPPoE server
- Configure PPPoE client on your laptop
- Connect your laptop to the router port on which the PPPoE server is configured

PPPoE Server

- Connect to PPPoE server
- Check that the connection to the Internet is available
- Connect to the router using MAC WinBox and observe PPP status
- Disconnect from the PPPoE server and connect the laptop back to previously used port

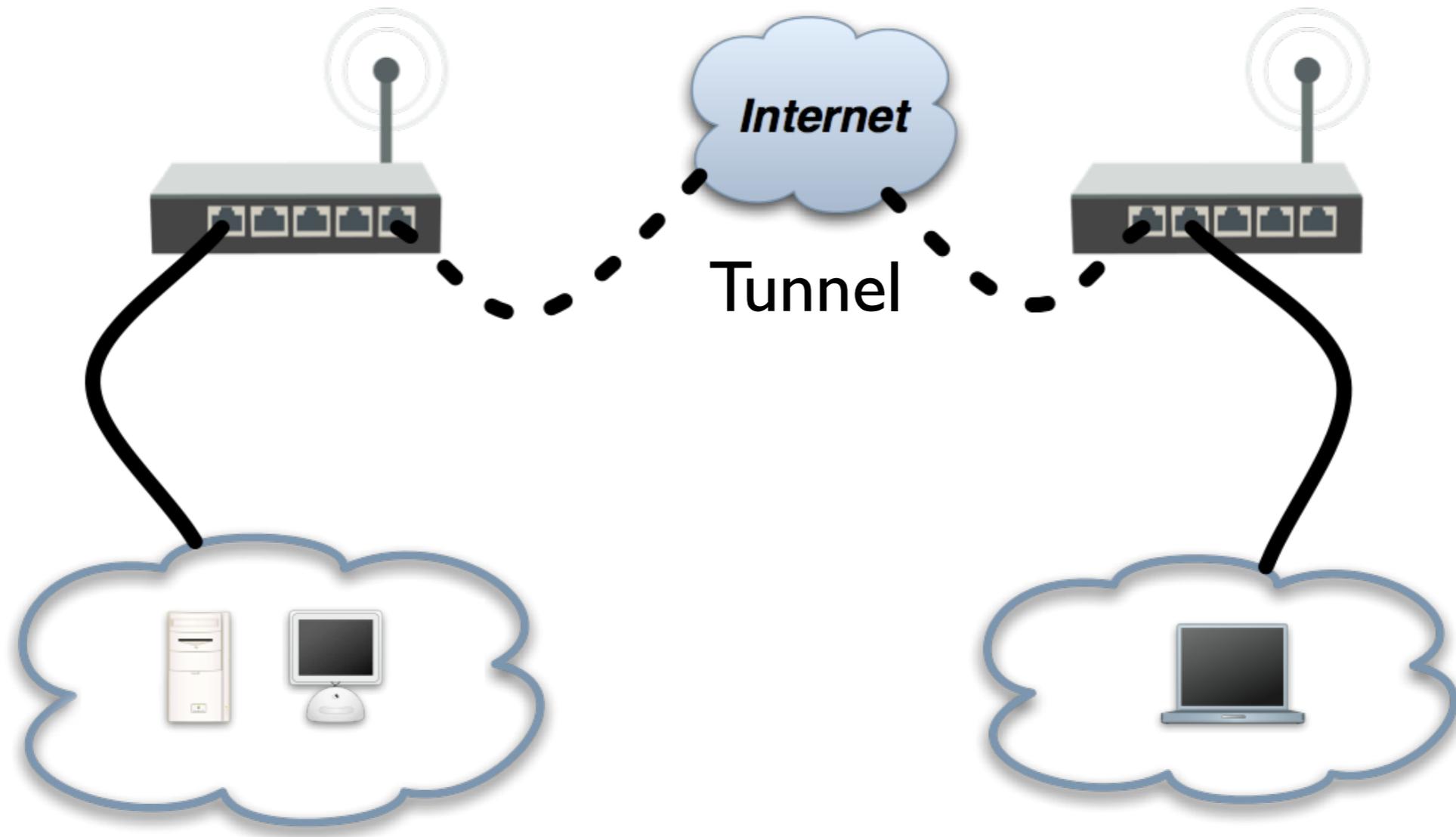
PPTP

- Point-to-point tunnelling protocol (PPTP) provides encrypted tunnels over IP
- Can be used to create secure connections between local networks over the Internet
- RouterOS supports both PPTP client and PPTP server

PPTP

- Uses port tcp/1723 and IP protocol number 47 - GRE (Generic Routing Encapsulation)
- NAT helpers are used to support PPTP in a NAT'd network

PPP Tunnel



PPTP Client

Set name,
PPTP server
IP address,
username,
password

The screenshot shows the MikroTik WinBox interface for configuring a new PPTP Client. The 'New Interface' dialog is open, and the 'General' tab is selected. The 'Name' field is set to 'pptp-out1'. The 'Type' is 'PPTP Client'. The 'Connect To' field is set to '1.2.3.4'. The 'User' is 'pptpclient1' and the 'Password' is masked with asterisks. The 'Profile' is 'default-encryption'. The 'Keepalive Timeout' is 60. The 'Allow' section has checkboxes for 'mschap2', 'mschap1', 'chap', and 'pap', all of which are checked. The 'Status' bar at the bottom shows 'enabled', 'running', 'slave', and 'Status:'.

PPP → New PPTP Client(+)

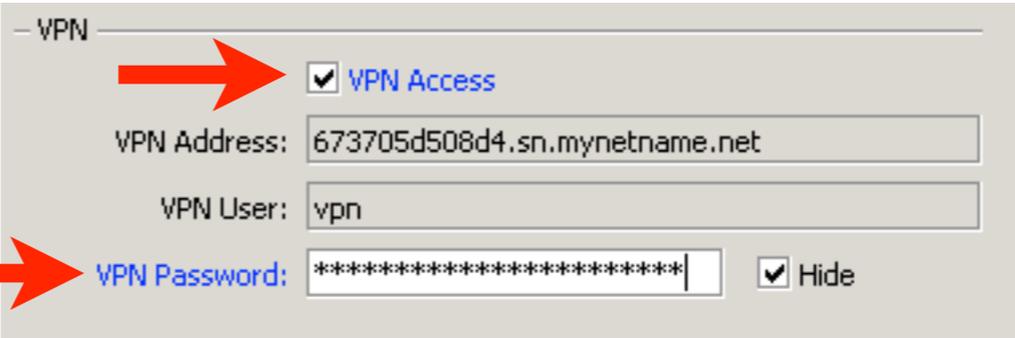
PPTP Client

- Use Add Default Route to send all traffic through the PPTP tunnel
- Use static routes to send specific traffic through the PPTP tunnel
- Note! PPTP is not considered secure anymore - use with caution!
- Instead use SSTP, OpenVPN or other

PPTP Server

- RouterOS provides simple PPTP server setup for administrative purposes
- Use QuickSet to enable VPN Access

**Enable VPN
access and
set VPN
password**



– VPN

VPN Access

VPN Address: 673705d508d4.sn.mynetname.net

VPN User: vpn

VPN Password: ***** Hide

SSTP

- Secure Socket Tunneling Protocol (SSTP) provides encrypted tunnels over IP
- Uses port tcp/443 (the same as HTTPS)
- RouterOS supports both SSTP client and SSTP server
- SSTP client available on Windows Vista SP1 and later versions

SSTP

- Open Source client and server implementation available on Linux
- As it is identical to HTTPS traffic, usually SSTP can pass through firewalls without specific configuration

SSTP Client

Set name,
SSTP server
IP address,
username,
password

The screenshot displays the Mikrotik WinBox interface for configuring SSTP Client interfaces. The main window shows a list of interfaces with columns for Name, Type, L2 MTU, Tx, Rx, Tx Packet (p/s), and Rx Packet (p/s). Two 'New Interface' windows are open, showing the configuration for two SSTP Client interfaces.

Left Window (General Tab):

- Name: sstp-out1
- Type: SSTP Client
- L2 MTU: [empty]
- Max MTU: 1500
- MRRU: 1600

Right Window (Dial Out Tab):

- Connect To: 1.2.3.4
- Port: 443
- Proxy: [empty]
- Proxy Port: 443
- Certificate: none
- Verify Server Certificate
- Verify Server Address From Certificate
- PFS
- User: sstpclient1
- Password: [masked]
- Profile: default-encryption
- Keepalive Timeout: 60
- Dial On Demand
- Add Default Route
- Default Route Distance: 0
- Allow: mschap2, mschap1, chap, pap

SSTP Client

- Use Add Default Route to send all traffic through the SSTP tunnel
- Use static routes to send specific traffic through the SSTP tunnel

SSTP Client

- No SSL certificates needed to connect between two RouterOS devices
- To connect from Windows, a valid certificate is necessary
- Can be issued by internal certificate authority (CA)

PPTP/SSTP

- Pair up with your neighbor
- One of you will create PPTP server and SSTP client, the other - SSTP server and PPTP client
- Reuse previously created IP pool, PPP profile and secret for the servers
- Create client connection to your neighbor's router

PPTP/SSTP

- Check firewall rules. Remember PPTP server uses port tcp/1723 and GRE protocol, SSTP port tcp/443
- Ping your neighbor's laptop from your laptop (not pinging)
- WHY? (answer on the next slide)

PPTP/SSTP

- There are no routes to your neighbors internal network
- Both create static routes to the other's network, set PPP client interface as a gateway
- Ping your neighbor's laptop from your laptop (should ping)

PPP

- In more detail PPPoE, PPTP, SSTP and other tunnel protocol server and client implementations are covered in MTCRE and MTCINE MikroTik certified courses
- For more info see: <http://training.mikrotik.com>

Module 8

Summary



Certified Network Associate (MTCNA)

Module 9

Misc

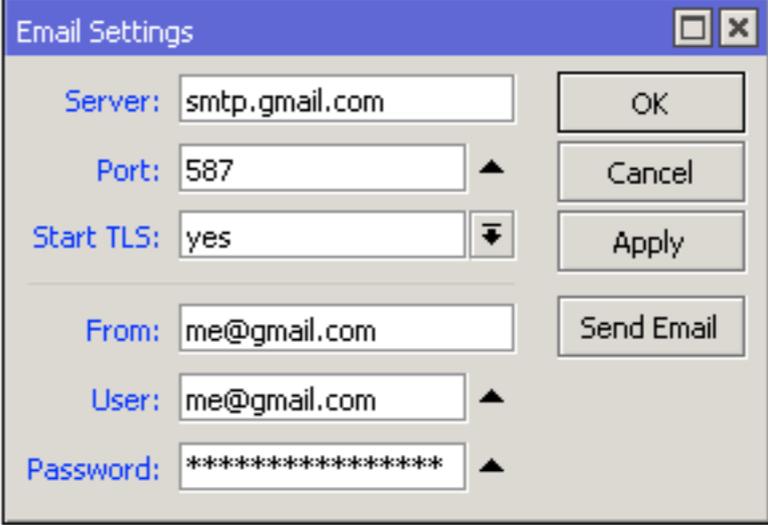
RouterOS Tools

- RouterOS provides various utilities that help to administrate and monitor the router more efficiently



E-mail

- Allows to send e-mails from the router
- For example to send router backup



Tools → Email

```
/export file=export
/tool e-mail send to=you@gmail.com\
  subject="$[/system identity get name] export"\
  body="$[/system clock get date]\
  configuration file" file=export.rsc
```

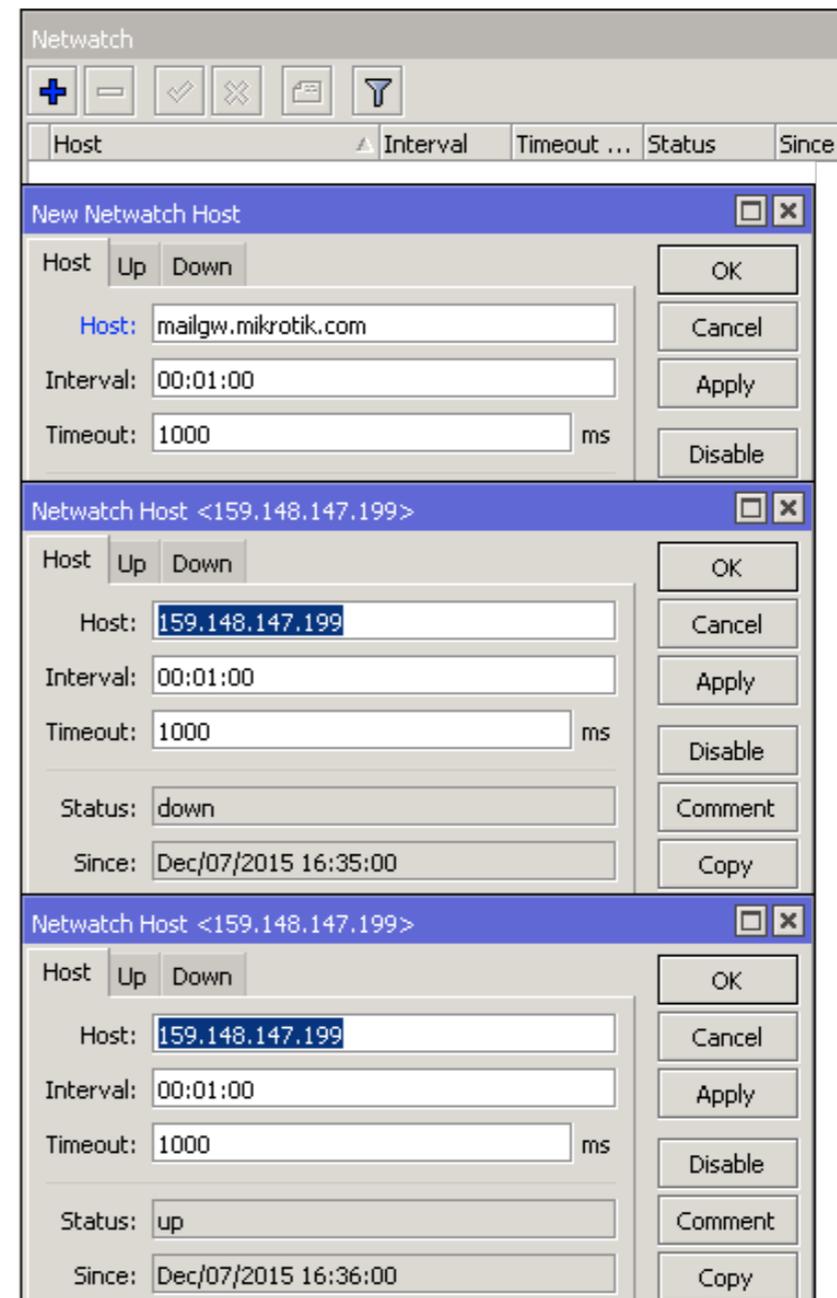
A script to make an export file and send it via e-mail

E-mail

- Configure your SMTP server settings on the router
- Export the configuration of your router
- Send it to your e-mail from the RouterOS

Netwatch

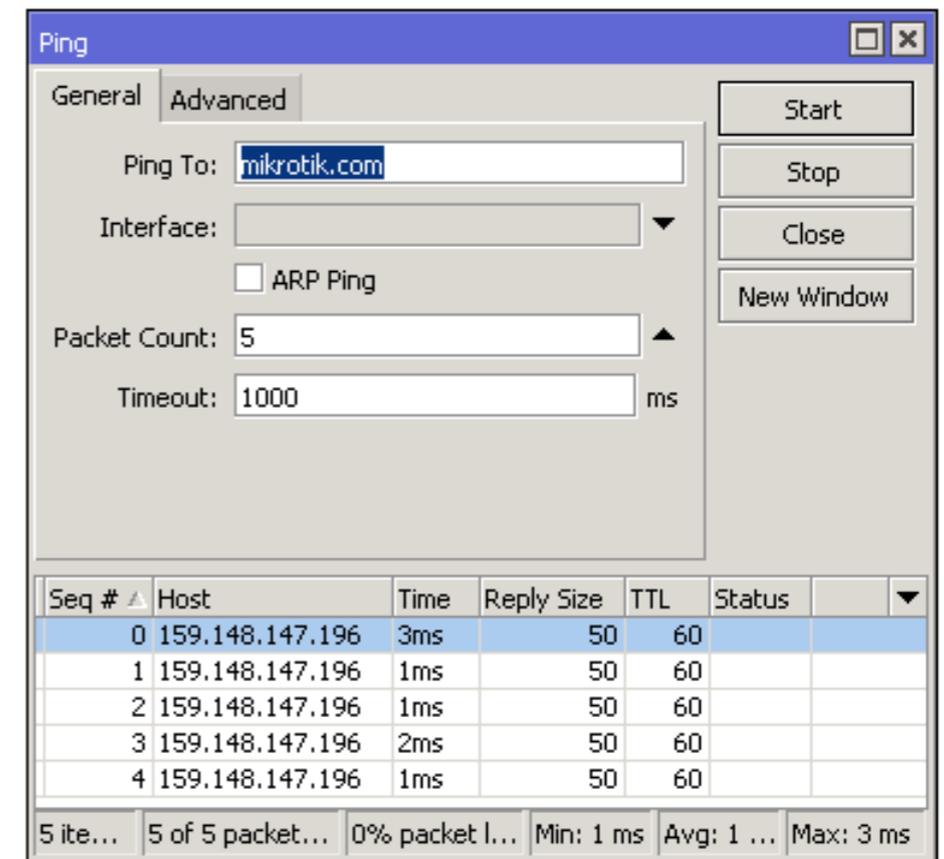
- Monitors state of hosts on the network
- Sends ICMP echo request (ping)
- Can execute a script when a host becomes unreachable or reachable



Tools → Netwatch

Ping

- Used to test the reachability of a host on an IP network
- To measure the round trip time for messages between source and destination hosts
- Sends ICMP echo request packets



Tools → Ping

Ping

- Ping your laptop's IP address from the router
- Click 'New Window' and ping www.mikrotik.com from the router
- Observe the round trip time difference

Traceroute

- Network diagnostic tool for displaying route (path) of packets across an IP network
- Can use icmp or udp protocol

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

- Traceroute To: latvia.lv
- 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]

Hop	Host	Loss	Sent	Last	Avg.	Best	Worst	Std. Dev.	History	Status
1	95.68.96.1	0.0%	466	4.7ms	5.3	0.9	40.2	2.9		
2	195.122.0.174	0.0%	466	10.4ms	11.3	3.2	57.5	3.0		
3	83.231.187.189	0.0%	466	17.5ms	16.2	10.4	19.5	14.1		
4	129.250.7.12	0.0%	466	44.4ms	45.5	43.8	55.0	44.5		
5	129.250.4.186	0.2%	466	52.5ms	53.0	48.8	112.3	52.9		
6	129.250.6.26	0.0%	466	47.8ms	48.0	45.7	146.4	46.9		
7	129.250.6.229	0.0%	466	47.8ms	48.3	45.7	103.1	46.7		
8	82.112.115.162	0.0%	466	50.8ms	50.6	47.7	99.8	48.9		
9	54.239.100.108	0.0%	466	53.8ms	66.1	53.1	142.0	66.5		<MPLS:L=574140,E=0 L=304224,E=0,T=1>
10	54.239.100.119	0.0%	466	57.3ms	55.1	49.2	113.0	54.7		<MPLS:L=304224,E=0>
11	176.32.106.34	0.0%	466	59.0ms	55.5	49.1	140.7	54.8		<MPLS:L=307552,E=0>
12	178.236.0.227	0.0%	466	53.0ms	55.0	49.2	90.6	54.7		
13	178.236.0.196	0.0%	466	55.5ms	56.1	49.6	116.7	54.8		<MPLS:L=641064,E=0>
14	178.236.1.17	0.2%	466	59.1ms	57.7	49.6	94.9	56.5		
15	54.77.166.239	0.0%	466	59.2ms	58.1	49.7	107.3	58.3		

15 items (1 selected)

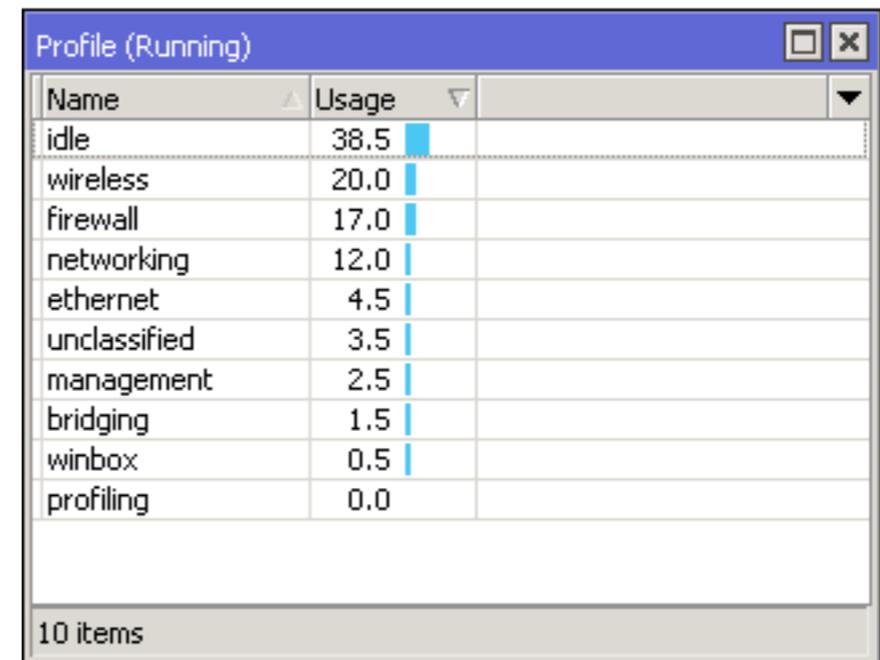
Tools → Traceroute

Traceroute

- Choose a web site in your country and do a traceroute to it
- Click 'New Window' and do a traceroute to www.mikrotik.com
- Observe the difference between the routes

Profile

- Shows CPU usage for each RouterOS running process in real time
- idle - unused CPU resources
- For more info see [Profile wiki page](#)



The screenshot shows a window titled "Profile (Running)" with a table of CPU usage for various processes. The table has two columns: "Name" and "Usage". The usage values are shown as percentages with corresponding blue progress bars.

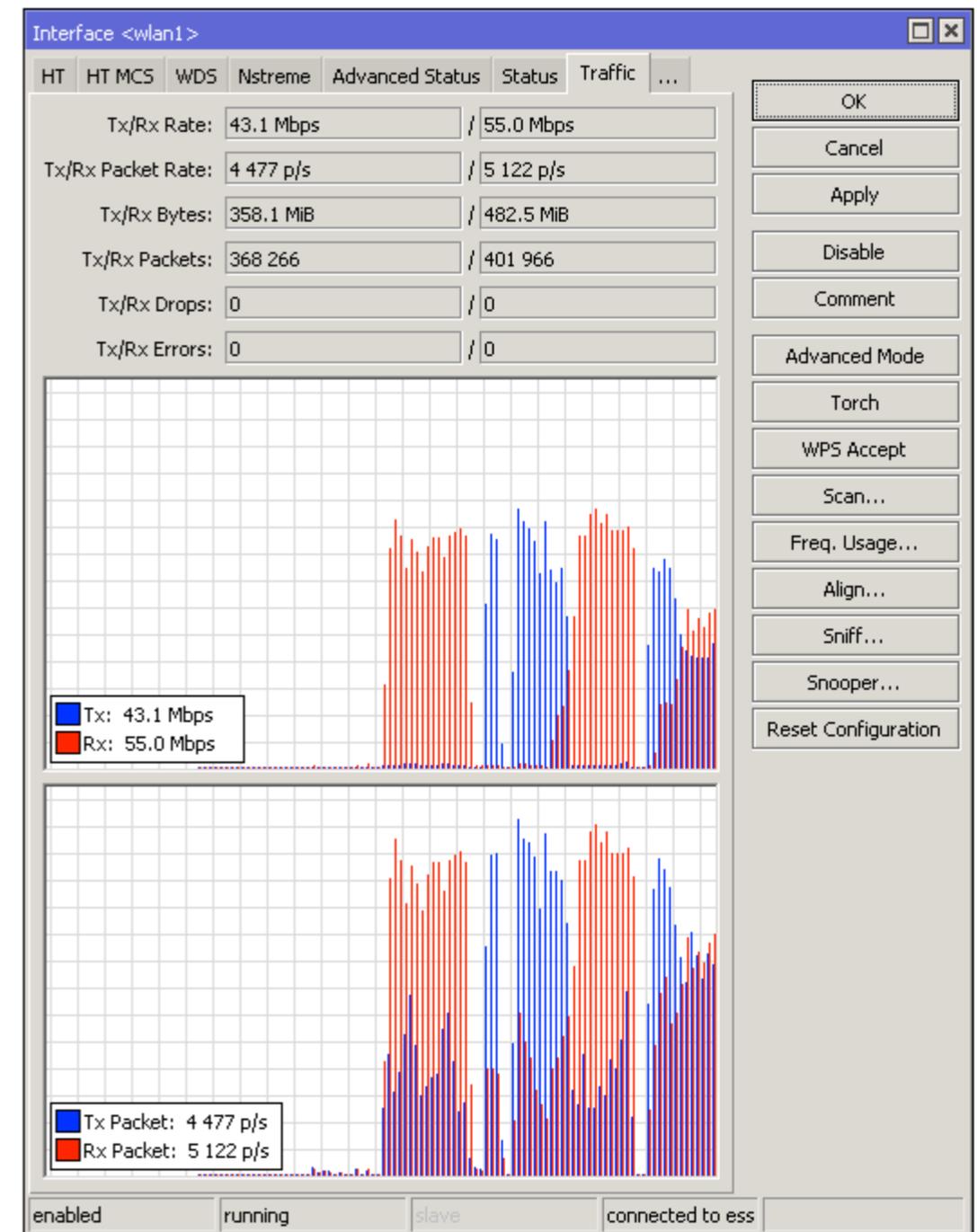
Name	Usage
idle	38.5
wireless	20.0
firewall	17.0
networking	12.0
ethernet	4.5
unclassified	3.5
management	2.5
bridging	1.5
winbox	0.5
profiling	0.0

10 items

Tools → Profile

Interface Traffic Monitor

- Real time traffic status
- Available for each interface in traffic tab
- Can also be accessed from both WebFig and command line interface



Interfaces → wlan1 → Traffic

Torch

- Real-time monitoring tool
- Can be used to monitor the traffic flow through the interface
- Can monitor traffic classified by IP protocol name, source/destination address (IPv4/IPv6), port number

Torch

The screenshot shows the Mikrotik Torch tool interface. The 'Basic' tab is active, showing the interface set to 'bridge-local' and an entry timeout of '00:00:03'. The 'Collect' section has checkboxes for 'Src. Address', 'Dst. Address', 'MAC Protocol', 'Protocol', 'DSCP', 'Src. Address6', 'Dst. Address6', 'Port', and 'VLAN Id'. The 'Filters' section shows 'Src. Address' as '192.168.199.200', 'Dst. Address' as '159.148.147.196', 'MAC Protocol' as 'all', 'Protocol' as 'tcp', 'Port' as 'https', 'VLAN Id' as 'any', and 'DSCP' as 'any'. On the right, there are buttons for 'Start', 'Stop', 'Close', and 'New Window'. Below the configuration is a table of traffic statistics.

Eth. Protocol	Protocol	Src.	Dst.	Tx Rate	Rx Rate	Tx Packet Rate	Rx Packet Rate
800 (ip)	6 (tcp)	192.168.199.200:58658	159.148.147.196:443 (https)	757.3 kbps	54.9 kbps	68	52
800 (ip)	6 (tcp)	192.168.199.200:58656	159.148.147.196:443 (https)	303.5 kbps	51.1 kbps	28	27
800 (ip)	6 (tcp)	192.168.199.200:58659	159.148.147.196:443 (https)	296.5 kbps	40.9 kbps	29	26
800 (ip)	6 (tcp)	192.168.199.200:58655	159.148.147.196:443 (https)	171.4 kbps	54.0 kbps	22	23
800 (ip)	6 (tcp)	192.168.199.200:58661	159.148.147.196:443 (https)	63.2 kbps	22.5 kbps	6	8
800 (ip)	6 (tcp)	192.168.199.200:58662	159.148.147.196:443 (https)	47.7 kbps	22.4 kbps	6	8
800 (ip)	6 (tcp)	192.168.199.200:58657	159.148.147.196:443 (https)	0 bps	0 bps	0	0

7 items Total Tx: 1639.8 kbps Total Rx: 245.9 kbps Total Tx Packet: 159 Total Rx Packet: 144

Tools → Torch

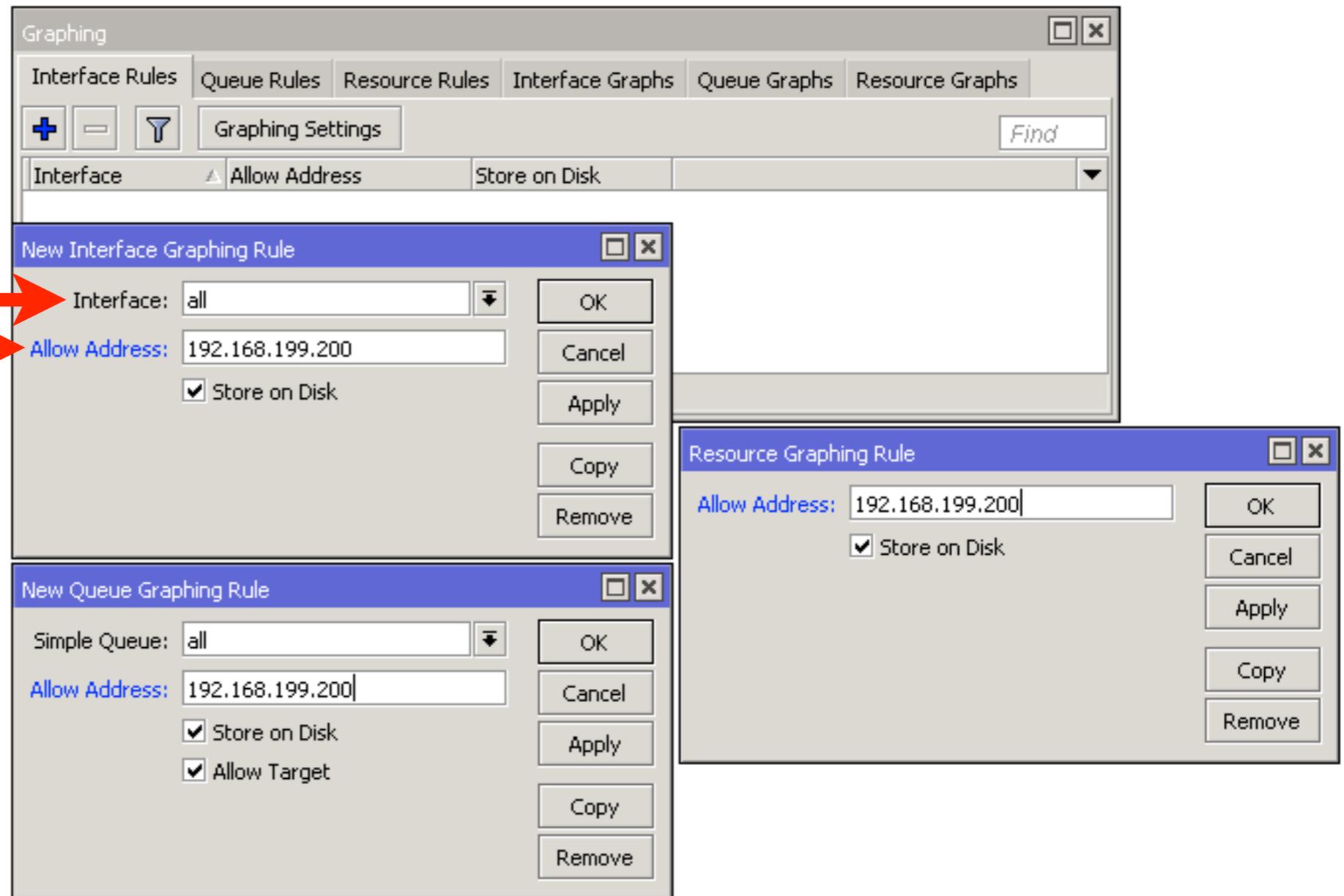
- Traffic flow from the laptop to the mikrotik.com web server HTTPS port

Graphs

- RouterOS can generate graphs showing how much traffic has passed through an interface or a queue
- Can show CPU, memory and disk usage
- For each metric there are 4 graphs - daily, weekly, monthly and yearly

Graphs

Set specific interface to monitor or leave all, set IP address/subnet which will be able to access the graphs



Tools → Graphing

Graphs

Traffic and system resource graphing

[CPU usage](#)
[Memory usage](#)
[Disk usage](#)

You have access to 4 queues:

[129](#)
[130](#)
[131](#)
[parent](#)

You have access to 7 interfaces:

[ether1-gateway](#)
[ether2-master-local](#)
[ether3-slave-local](#)
[ether4-slave-local](#)
[ether5](#)
[wlan1](#)
[bridge-local](#)

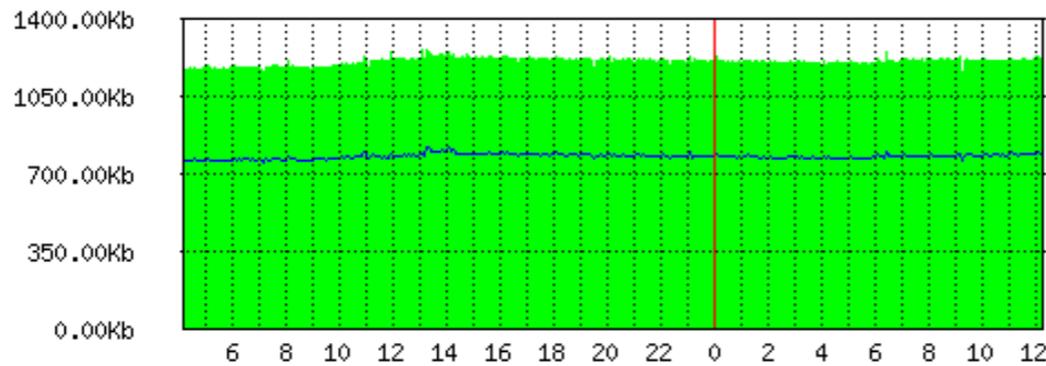
- Available on the router: http://router_ip/graphs

Graphs

Interface <ether1-gateway> Statistics

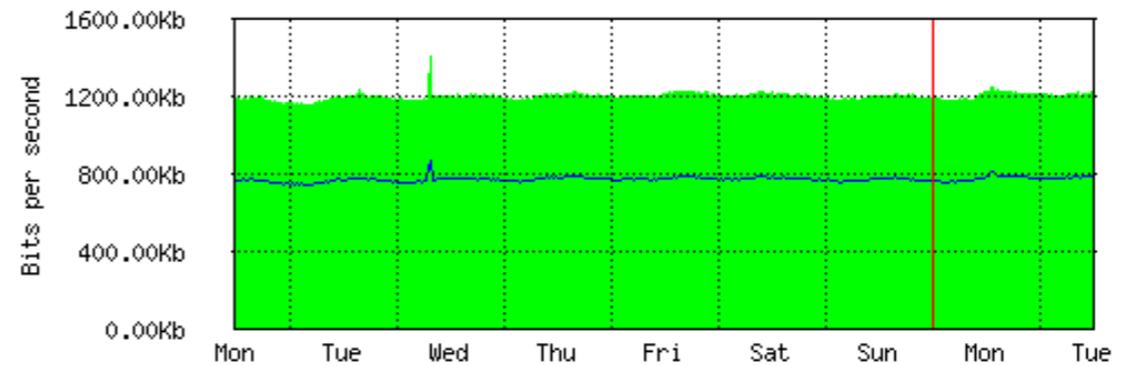
• Last update: Wed Dec 31 23:59:59 2015

"Daily" Graph (5 Minute Average)



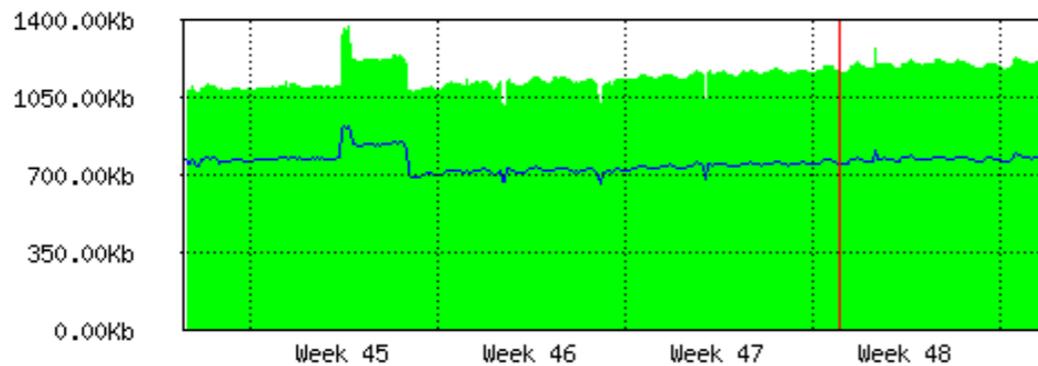
Max In: 1.26Mb; Average In: 1.21Mb; Current In: 1.22Mb;
Max Out: 821.58Kb; Average Out: 780.56Kb; Current Out: 793.75Kb;

"Weekly" Graph (30 Minute Average)



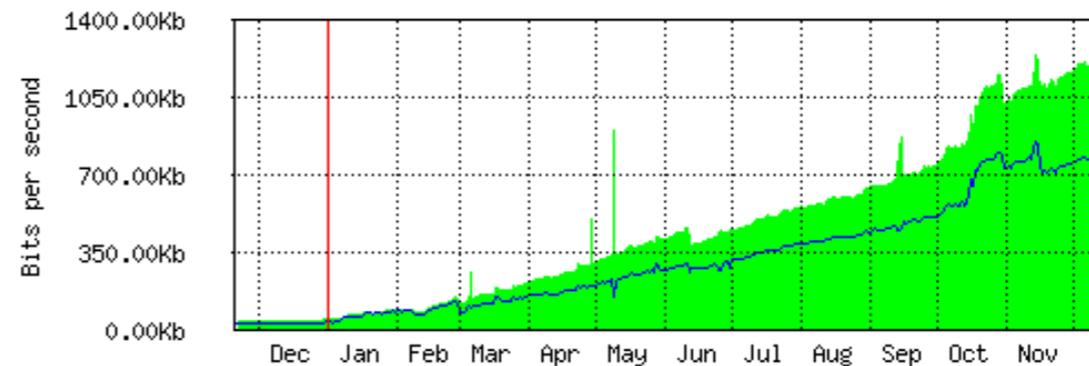
Max In: 1.41Mb; Average In: 1.20Mb; Current In: 1.22Mb;
Max Out: 872.20Kb; Average Out: 772.71Kb; Current Out: 792.54Kb;

"Monthly" Graph (2 Hour Average)



Max In: 1.37Mb; Average In: 1.15Mb; Current In: 1.21Mb;
Max Out: 922.93Kb; Average Out: 757.19Kb; Current Out: 786.12Kb;

"Yearly" Graph (1 Day Average)



Max In: 1.24Mb; Average In: 445.51Kb; Current In: 1.20Mb;
Max Out: 850.52Kb; Average Out: 303.36Kb; Current Out: 772.42Kb;

Graphs

- Enable interface, queue and resource graphs on your router
- Observe the graphs
- Download a large file from the Internet
- Observe the graphs

SNMP

- Simple Network Management Protocol (SNMP)
- Used for monitoring and managing devices
- RouterOS supports SNMP v1, v2 and v3
- SNMP write support is available only for some settings

SNMP

The image displays three overlapping windows from the Mikrotik WinBox interface:

- SNMP Settings:** A configuration window with the following fields:
 - Enabled
 - Contact Info: John Doe
 - Location: classroom
 - Engine ID: (empty)
 - Trap Target: (empty)
 - Trap Community: 7TqCJMga
 - Trap Version: 3
 - Trap Generators: (empty)
 - Trap Interfaces: (empty)
- SNMP Communities:** A table listing configured communities:

Name	Addresses	Security	Read Access	Write Access
7TqCJMga	0.0.0.0/0	authorized	yes	no
- SNMP Community <7TqCJMga>:** A detailed configuration window for the selected community:
 - Name: 7TqCJMga
 - Addresses: 0.0.0.0/0
 - Security: authorized
 - Read Access
 - Write Access
 - Authentication Protocol: MD5
 - Encryption Protocol: DES
 - Authentication Password: *****
 - Encryption Password: *****

Tools → SNMP

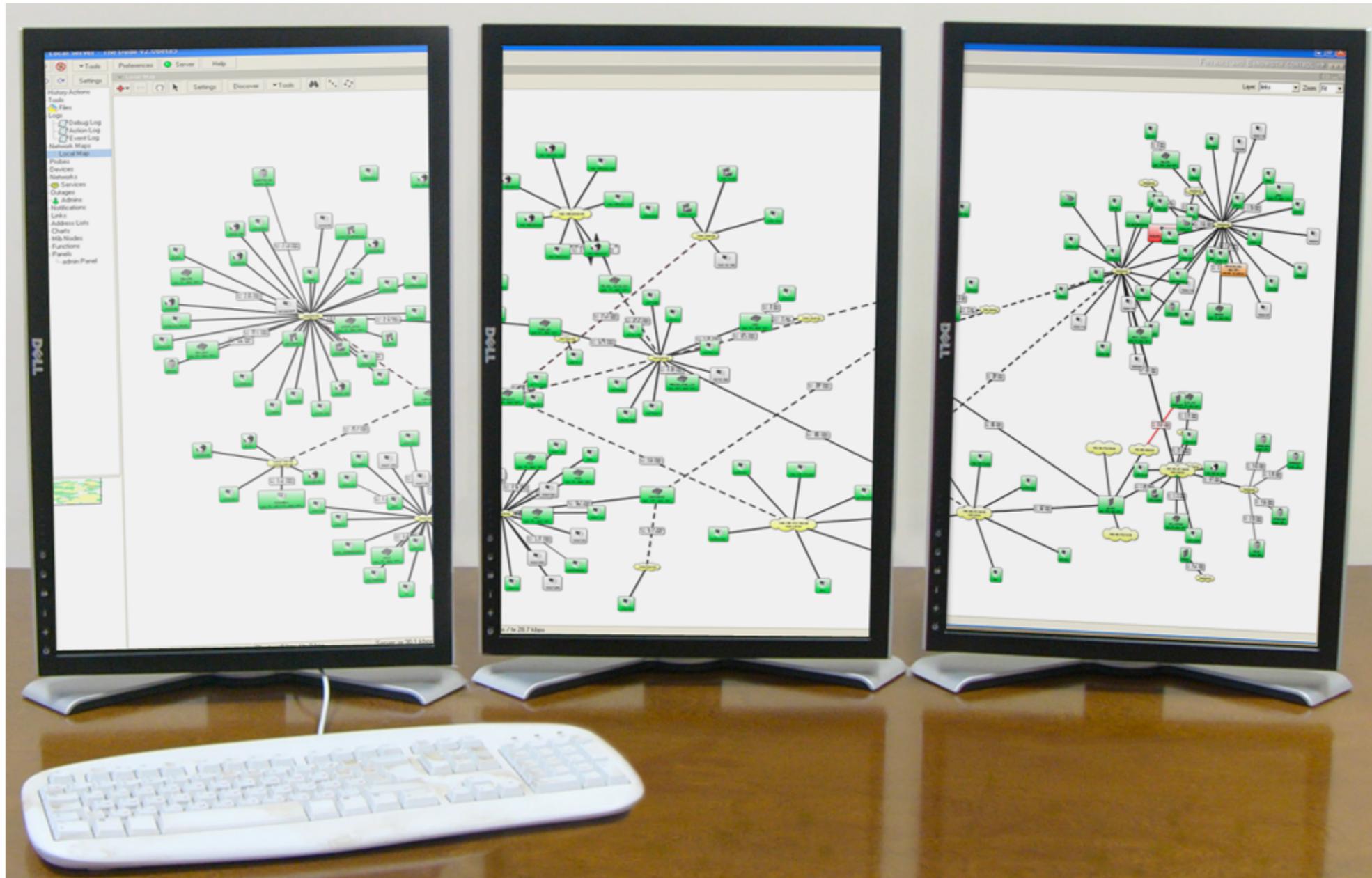
The Dude

- Application by MikroTik which can dramatically improve the way you manage your network environment
- Automatic discovery and layout map of devices
- Monitoring of services and alerting
- Free of charge

The Dude

- Supports SNMP, ICMP, DNS and TCP monitoring
- Server part runs on RouterOS (CCR, CHR or x86)
- Client on Windows (works on Linux and OS X using Wine)
- For more info see [The Dude wiki page](#)

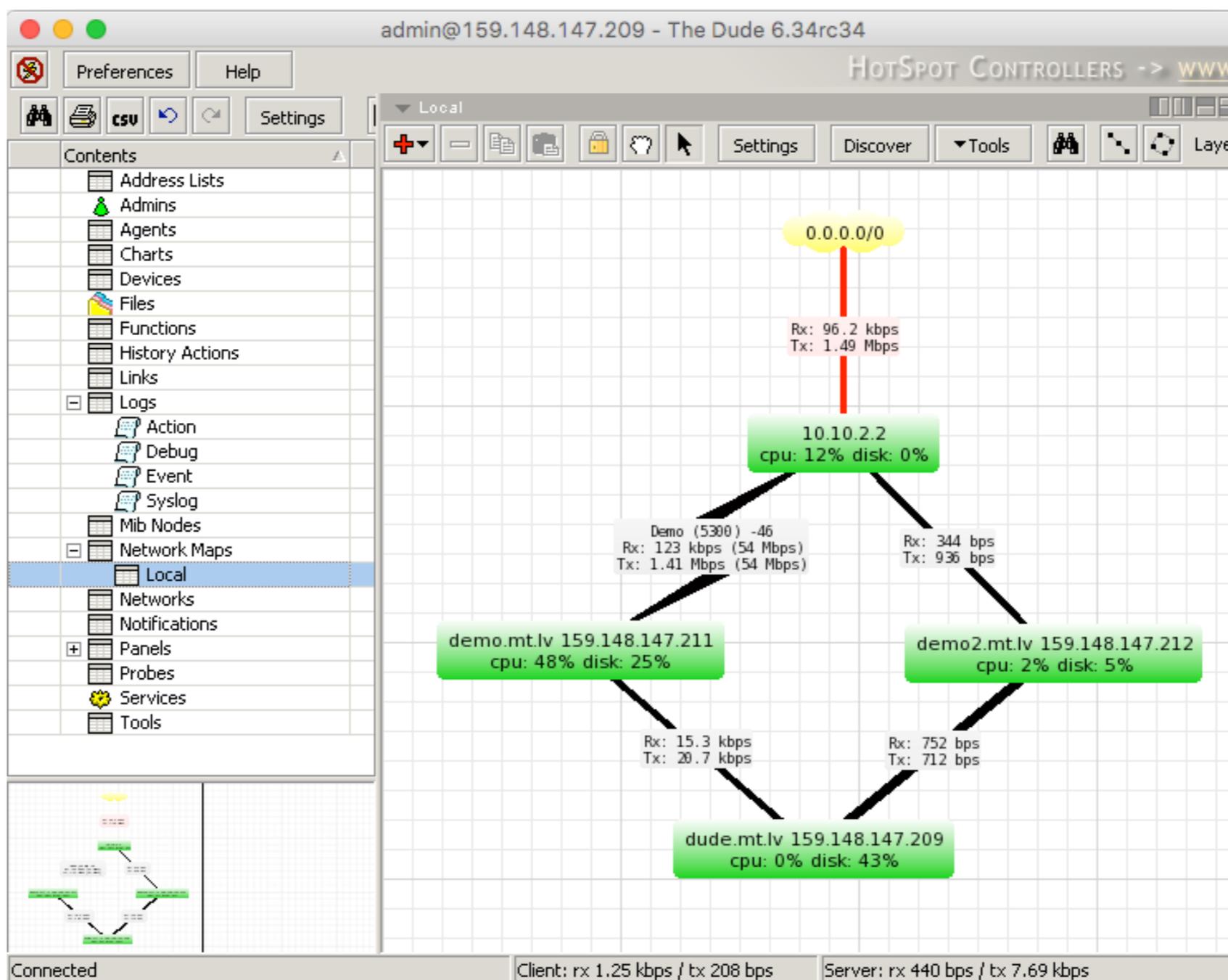
The Dude



The Dude

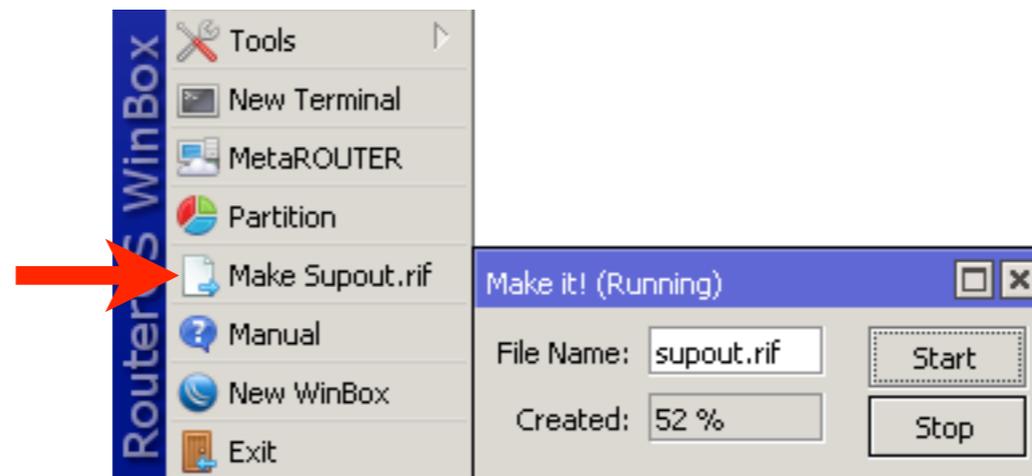
- Download the Dude client for Windows from mikrotik.com/download page
- Install and connect to MikroTik Dude demo server: **dude.mt.lv**
- Observe the Dude

The Dude



Contacting Support

- In order for MikroTik support to be able to help better, few steps should be taken beforehand
- Create support output file (supout.rif)



Contacting Support

- autosupout.rif can be created automatically in case of hardware malfunction
- Managed by watchdog process
- Before sending to MikroTik, support output file contents can be viewed in your [mikrotik.com account](#)
- For more info see [Support Output File and Watchdog](#) wiki pages

System Logs

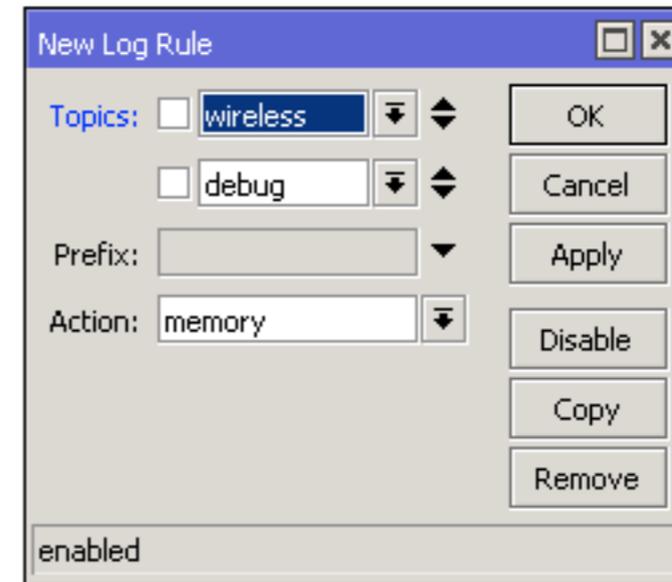
- By default RouterOS already logs information about the router
- Stored in memory
- Can be stored on disk
- Or sent to a remote syslog server

Topics	Prefix	Action
* critical		echo
* error		memory
* info		memory
* warning		memory

System → Logging

System Logs

- To enable detailed logs (debug), create a new rule
- Add debug topic



System → Logging → New Log Rule

Time	Action	Topic	Message
Dec/10/2015 11:14:42	memory	interface, info	ether2-master-local link up (speed 100M, full duplex)
Dec/10/2015 11:14:42	memory	wireless, debug	wlan1: must select network
Dec/10/2015 11:14:42	memory	wireless, debug	64:66:B3:40:E6:5E: on 2412 AP: yes SSID Maximums caps 0x431 rates 0xCCK:1-11 OFDM:6-54 BW:1x-2x SGI:1x-2x HT:0-7 basic 0xCCK:1-11 MT: no
Dec/10/2015 11:14:42	memory	wireless, debug	00:0C:42:00:63:60: on 2412 AP: yes SSID Rb751-cap-test caps 0x431 rates 0xCCK:1-11 OFDM:6-54 basic 0xCCK:1-11 MT: yes
Dec/10/2015 11:14:42	memory	wireless, debug	D4:CA:6D:CE:4F:03: on 2412 AP: yes SSID 48 caps 0x431 rates 0xCCK:1-11 OFDM:6-54 BW:1x SGI:1x HT:0-15 basic 0xCCK:1-11 MT: yes
Dec/10/2015 11:14:42	memory	wireless, debug	D4:CA:6D:A2:7E:D4: on 2412 AP: yes SSID Anrijs-2011 caps 0x431 rates 0xCCK:1-11 OFDM:6-54 BW:1x SGI:1x HT:0-15 basic 0xCCK:1-11 MT: yes
Dec/10/2015 11:14:42	memory	wireless, debug	00:0B:6B:30:7F:A6: on 2412 AP: yes SSID raivis caps 0x431 rates 0xCCK:1-11 OFDM:6-54 basic 0xCCK:1-11 MT: yes
Dec/10/2015 11:14:42	memory	wireless, debug	00:0C:42:62:B6:58: on 2422 AP: yes SSID Rukis caps 0x431 rates 0xCCK:1 basic 0xCCK:1 MT: yes
Dec/10/2015 11:14:42	memory	wireless, debug	4C:5E:0C:50:5A:8B: on 2422 AP: yes SSID Hotspot caps 0x411 rates 0xCCK:1-11 OFDM:6-54 BW:1x HT:0-7 basic 0xCCK:1-11 MT: yes
Dec/10/2015 11:14:42	memory	wireless, debug	D4:CA:6D:FA:02:C0: on 2422 AP: yes SSID jAP caps 0x431 rates 0xCCK:1-11 OFDM:6-54 BW:1x-2x SGI:1x-2x HT:0-15 basic 0xCCK:1-11 MT: yes
Dec/10/2015 11:14:42	memory	wireless, debug	D4:CA:6D:E2:64:7B: on 2427 AP: yes SSID MikroTik-E2647B caps 0x431 rates 0xCCK:1-11 OFDM:6-54 BW:1x-2x SGI:1x-2x HT:0-23 basic 0xCCK:1-11 MT: yes
Dec/10/2015 11:14:42	memory	wireless, debug	D4:CA:6D:2E:3C:F5: on 2427 AP: yes SSID R caps 0x421 rates 0xCCK:1-11 OFDM:6-54 BW:1x SGI:1x HT:0-7 basic 0xCCK:1-11 MT: yes

Contacting Support

- Before contacting support@mikrotik.com check these resources
- wiki.mikrotik.com - RouterOS documentation and examples
- forum.mikrotik.com - communicate with other RouterOS users
- mum.mikrotik.com - MikroTik User Meeting page - presentations videos

Contacting Support

- It is suggested to add meaningful comments to your rules, items
- Describe as detailed as possible so that MikroTik support team can help you better
- Include your network diagram
- For more info [see support page](#)

Module 9

Summary

MTCNA

Summary

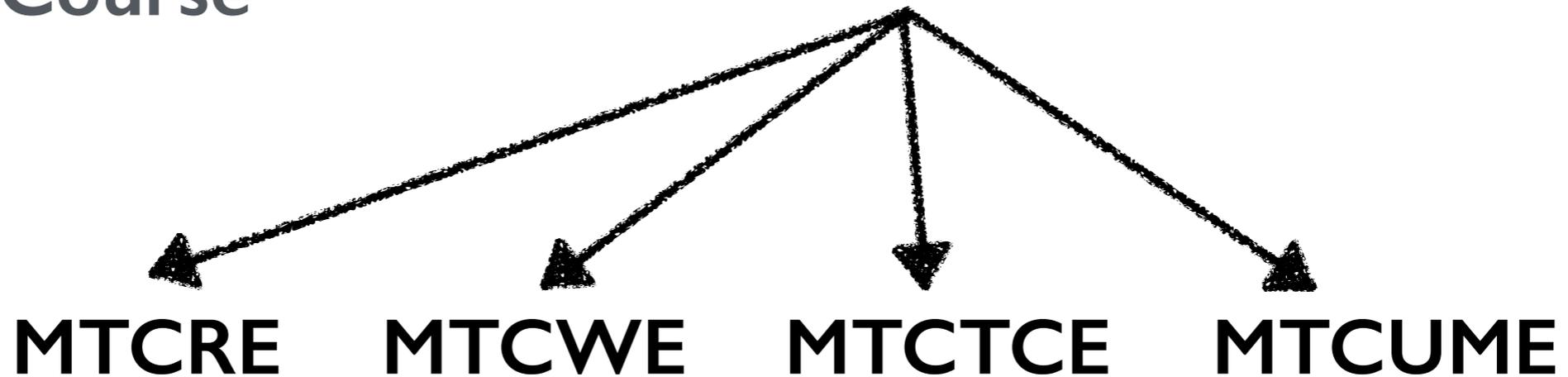
MikroTik Certified

Courses

Introduction
Course



MTCNA



For more info see: <http://training.mikrotik.com>

Certification Test

- If needed reset router configuration and restore from a backup
- Make sure that you have an access to the www.mikrotik.com training portal
- Login with your account
- Choose **my training sessions**
- Good luck!