

MikroTik RouterOS Training Class



Nikan Network

www.nikannetwork.com

Schedule

- Training day: 9AM - 5PM
- 30 minute Breaks: 10:30AM and 3PM
- 1 hour Lunch: 12:30PM

Course Objective

- Overview of RouterOS software and RouterBoard capabilities
- Hands-on training for MikroTik router configuration, maintenance and basic troubleshooting

About MikroTik

- Router software and hardware manufacturer
- Products used by ISPs, companies and individuals
- Make Internet technologies faster, powerful and affordable to wider range of users

MikroTik's History

- 1995: Established
- 1997: RouterOS software for x86 (PC)
- 2002: RouterBOARD is born
- 2006: First MUM

Where is MikroTik?

- www.mikrotik.com
- www.routerboard.com
- Riga, Latvia, Northern Europe, EU

Where is MikroTik ?



Introduce Yourself

- Please, introduce yourself to the class
 - Your name
 - Your Company
 - Your previous knowledge about RouterOS (?)
 - Your previous knowledge about networking (?)
 - What do you expect from this course? (?)
- Please, remember your class XY number.

MikroTik RouterOS

What is RouterOS ?

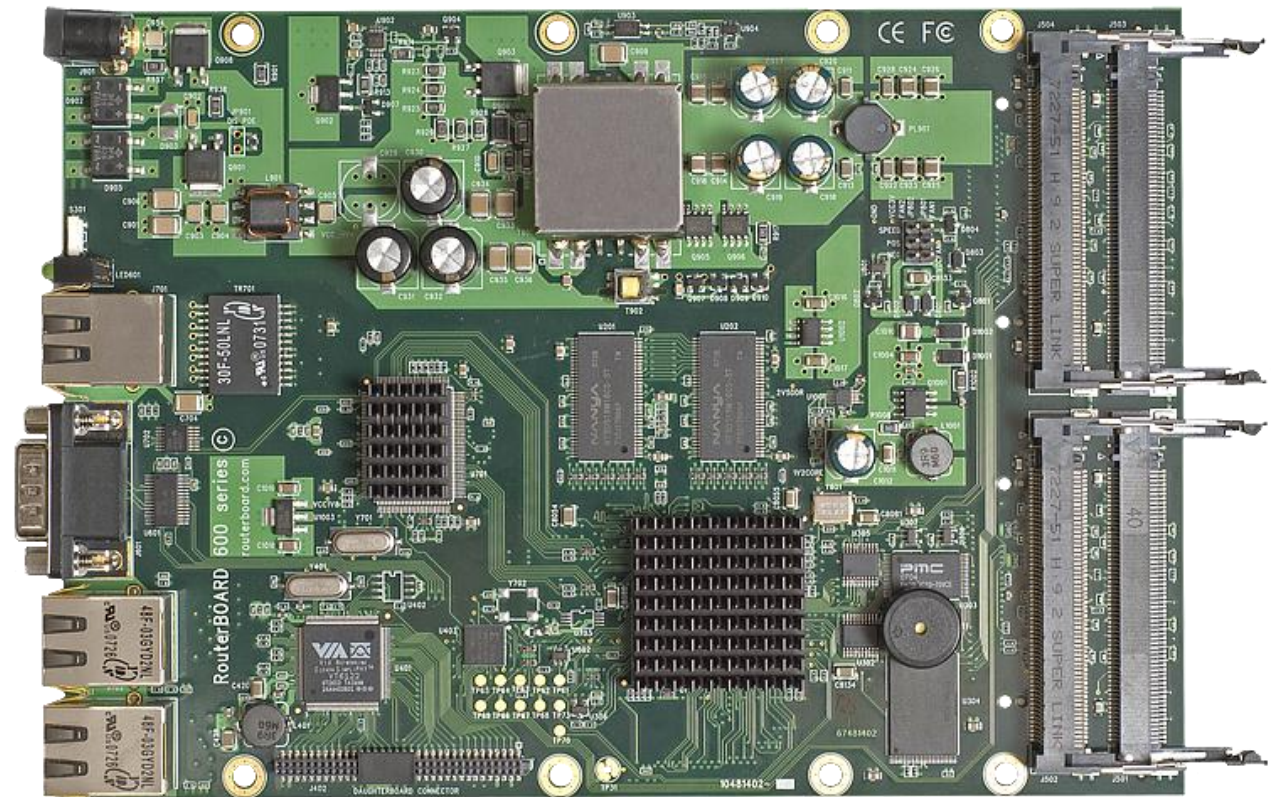
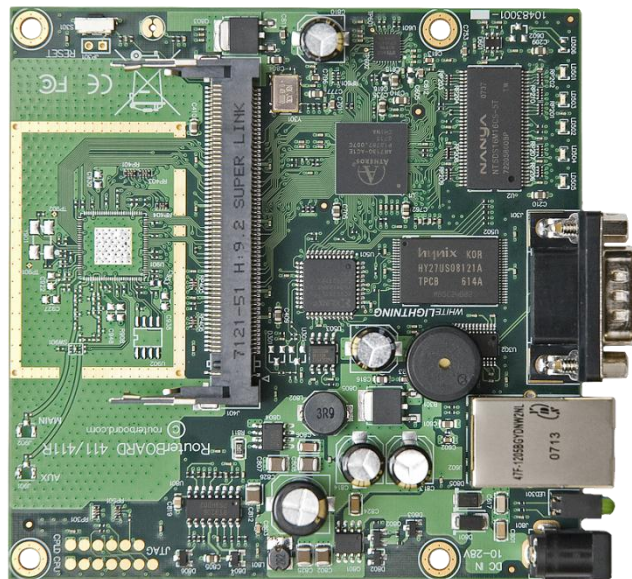
- RouterOS is an operating system that will make your device:
 - a dedicated router
 - a bandwidth shaper
 - a (transparent) packet filter
 - any 802.11a,b/g wireless device

What is RouterOS ?

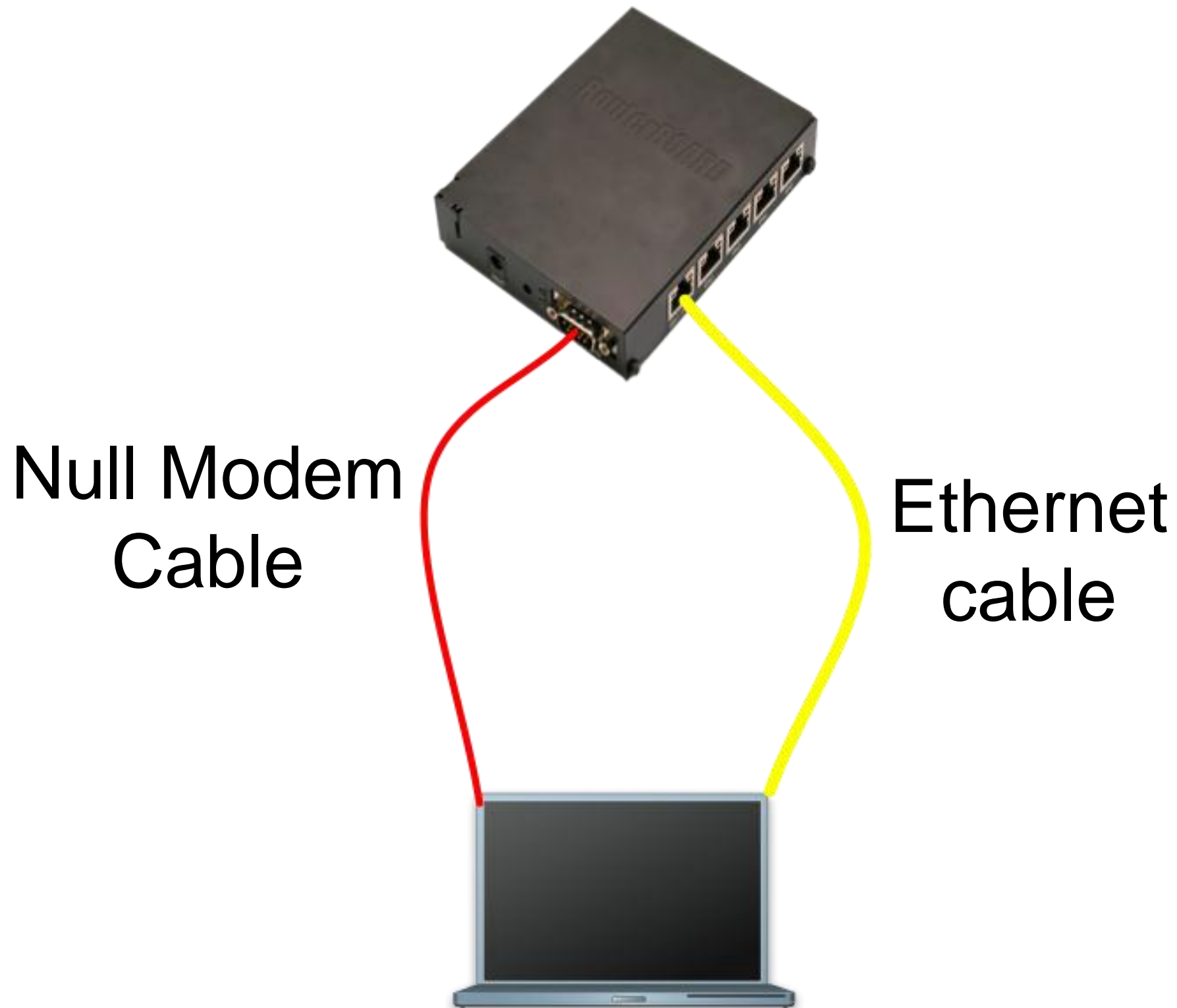
- The operating system of RouterBOARD
- Can be also installed on a PC

What is RouterBOARD ?

- Hardware created by MikroTik
- Range from small home routers to carrier-class access concentrators



First Time Access



Winbox

- The application for configuring RouterOS
- It can be downloaded from www.mikrotik.com

Download Winbox



Routers & Wireless

[home](#) [products](#) [software](#) [wireless](#) [sitemap](#) [s](#)

[Main](#) [Buy](#) [Our customers](#) [About us](#) [Press](#) [Download](#) [Jobs](#)

MikroTik everywhere: [AP](#) | [CPE](#) | [Network Monitor](#) | [Us](#) | [Manag](#)

MUM Poland 2008

RouterOS Software

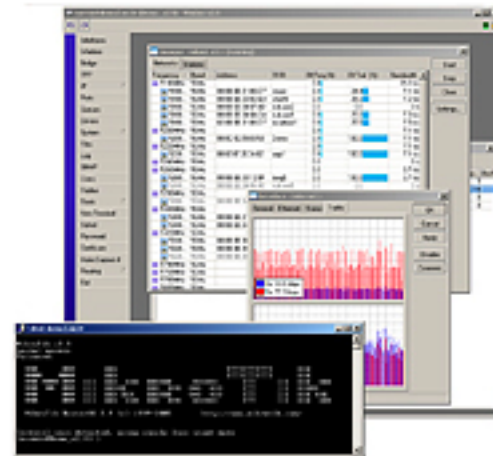
[\[info\]](#) [\[docs\]](#) [\[wiki\]](#) [\[forum\]](#) [\[download\]](#)



The first MikroTik User Meeting (MUM) of 2008 will take place in Poland.

- [registration for MUM](#)
- [registration for training before MUM](#)

MikroTik Training



Major features:

- Best wireless performance
- Improved Nstreme performance
- Powerful QoS control
- P2P traffic filtering
- High availability with VRRP
- Bonding of Interfaces

RouterOS Installation

Netinstall

Download the Netinstall utility to install any RouterOS version. Netinstall uses the packages you can download on the left.

- [Install Help](#)
- [Upgrade Help](#)

Full RouterOS installation packages (requires a [Torrent client](#)):

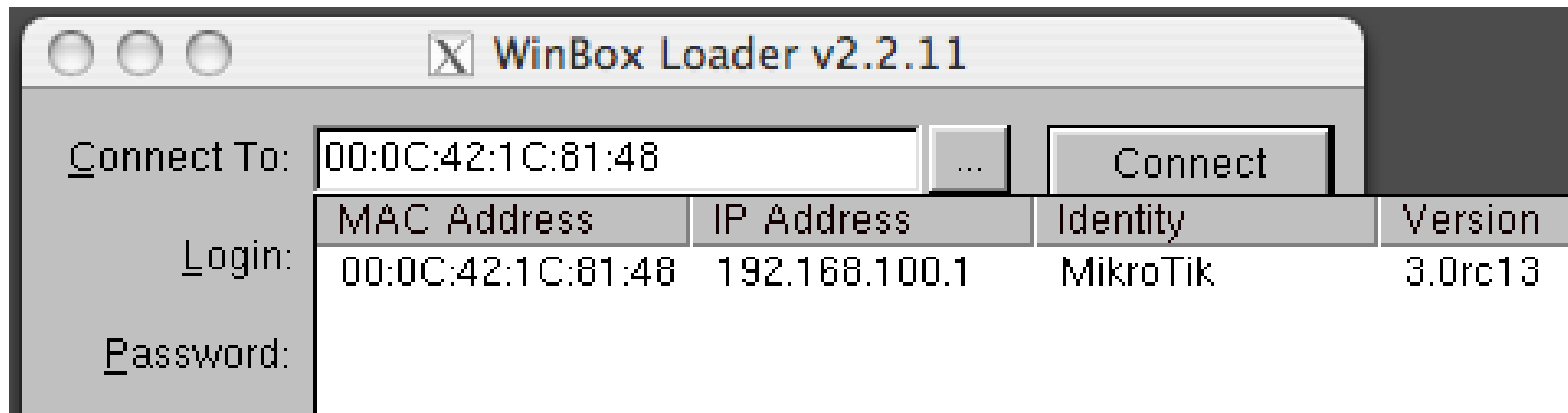
- [RouterOS 2.9.50 Torrent](#)
- [RouterOS 3.0rc13 Torrent](#)

Tools / Utilities

- [Winbox configuration tool 2.2.13](#)
- [The Dude network monitor](#)
- [Trafr sniffer reader for linux](#)
- [Bandwidth test tool for Windows](#)
- [Neighbor viewer for Windows](#)
- [Other tools in the Archive](#)

Connecting

Click on the [...] button to see your router



Communication

- Process of communication is divided into seven layers
- Lowest is physical layer, highest is application layer

Application

Presentation

Session

Transport

Network

Data Link

Physical

MAC address

- It is the unique physical address of a network device
- It's used for communication within LAN
- Example: 00:0C:42:20:97:68

IP

- It is logical address of network device
- It is used for communication over networks
- Example: 159.148.60.20

Subnets

- Range of logical IP addresses that divides network into segments
- Example: 255.255.255.0 or /24

Subnets

- Network address is the first IP address of the subnet
- Broadcast address is the last IP address of the subnet
- They are reserved and cannot be used

CIDR	Subnet Mask	Available Hosts
------	-------------	-----------------

/32	255.255.255.255	
/30	255.255.255.252	4-2
/29	255.255.255.248	8-2
/28	255.255.255.240	16-2
/27	255.255.255.224	32-2
/26	255.255.255.192	64-2
/25	255.255.255.128	128-2
/24	255.255.255.0	256-2

Selecting IP address

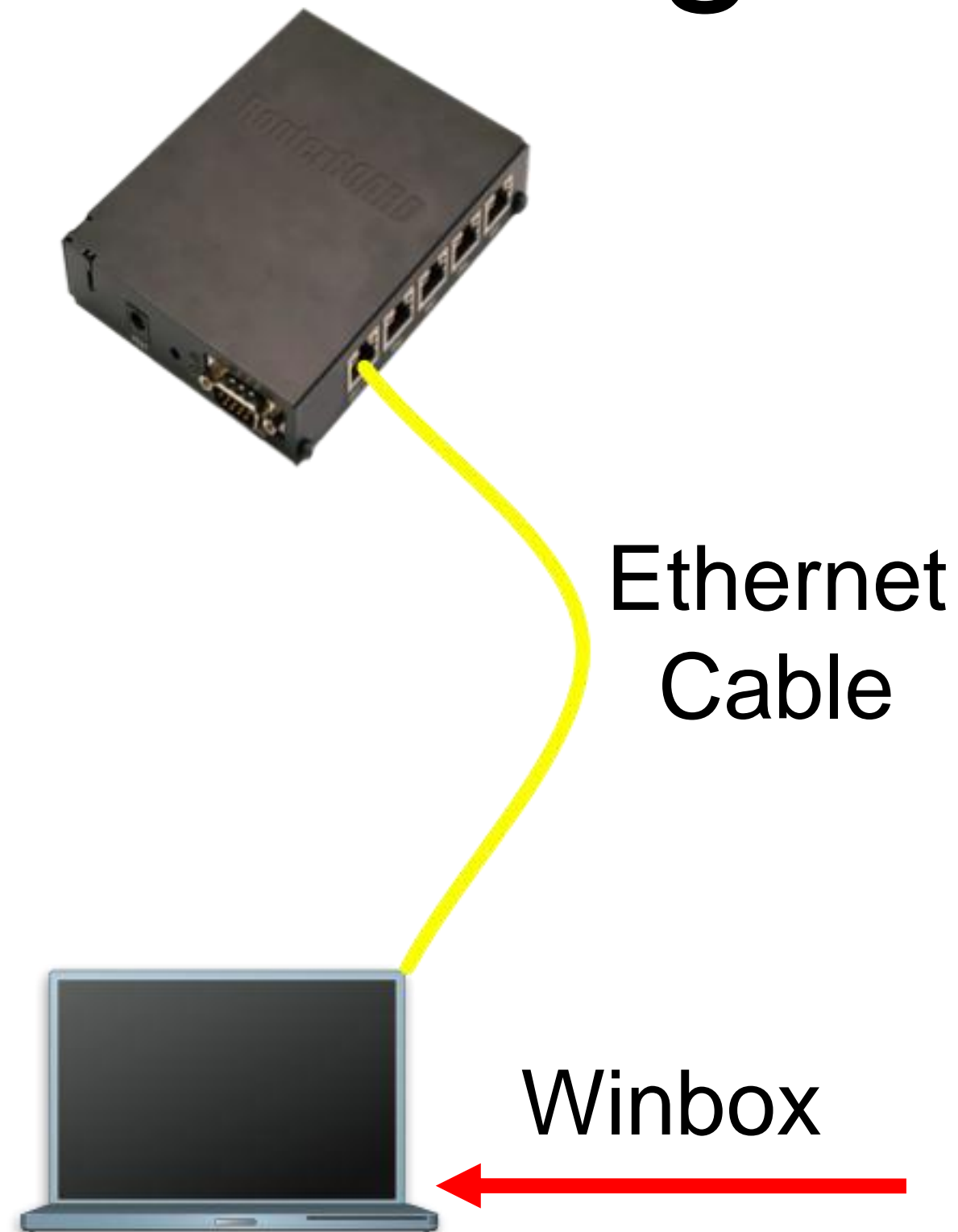
- Select IP address from the same subnet on local networks
- Especially for big network with multiple subnets

Selecting IP address

Example

- Clients use different subnet masks /25 and /26
- **A** has 192.168.0.200/**26** IP address
- **B** use subnet mask /**25**, available addresses 192.168.0.129-192.168.0.254
- **B** should **not** use 192.168.0.129-192.168.0.192
- **B** should use IP address from 192.168.0.193 - 192.168.0.254/25

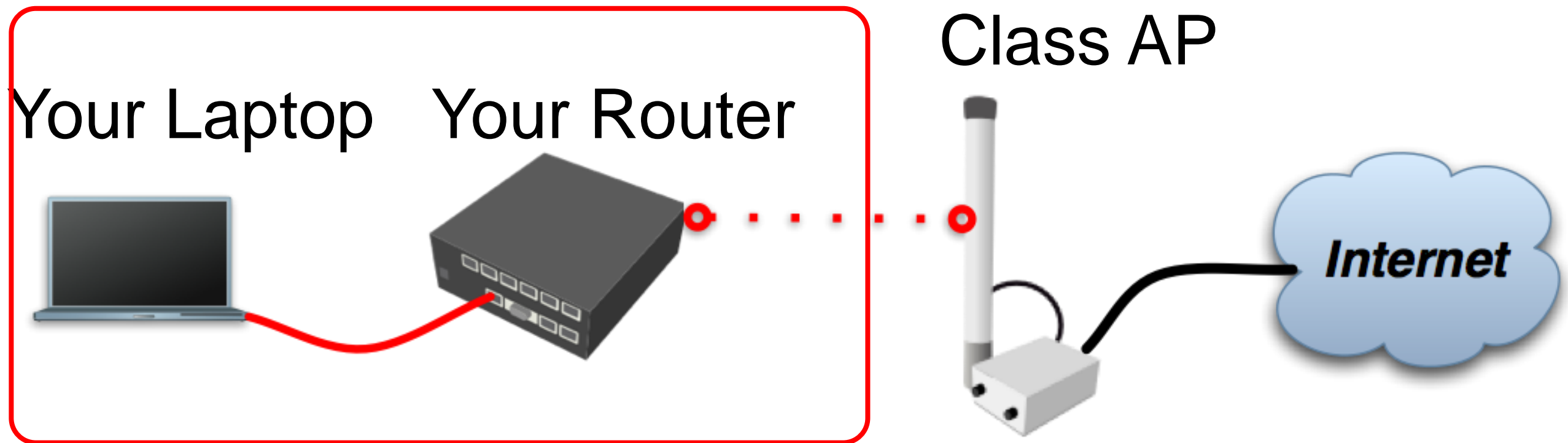
Connecting



Connecting Lab

- Click on the Mac-Address in Winbox
- Default username “admin” and no password

Diagram

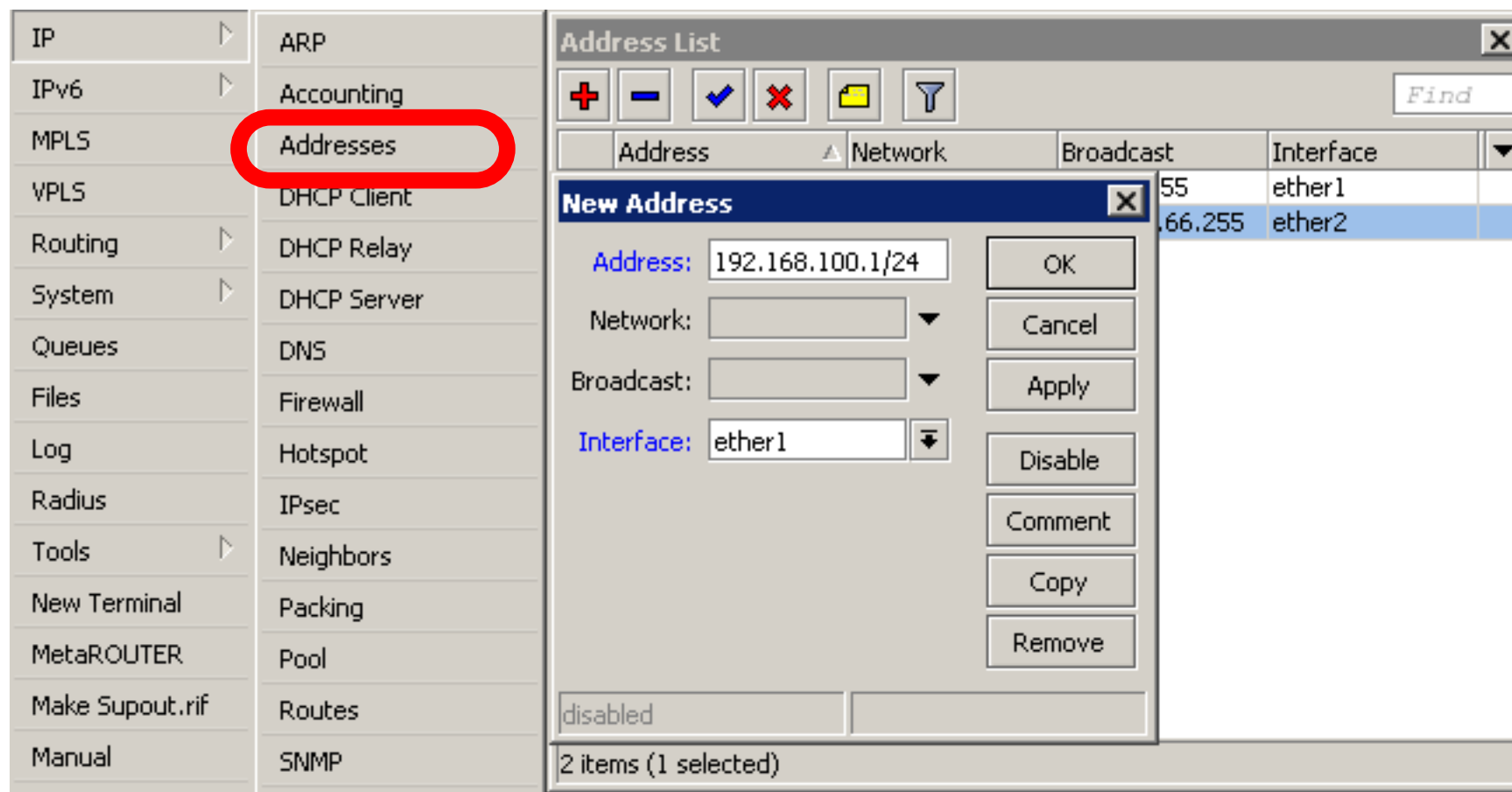


Laptop - Router

- Disable any other interfaces (wireless) in your laptop
- Set 192.168.X.1 as IP address
- Set 255.255.255.0 as Subnet Mask
- Set 192.168.X.254 as Default Gateway

Laptop - Router

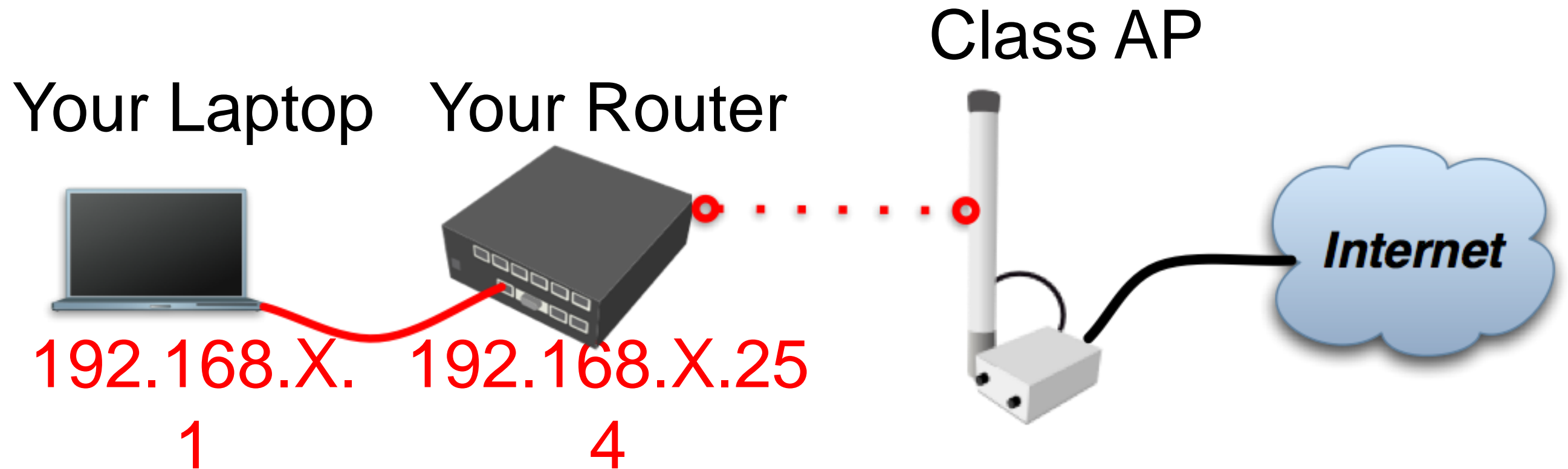
- Connect to router with MAC-Winbox
- Add 192.168.X.254/24 to Ether1



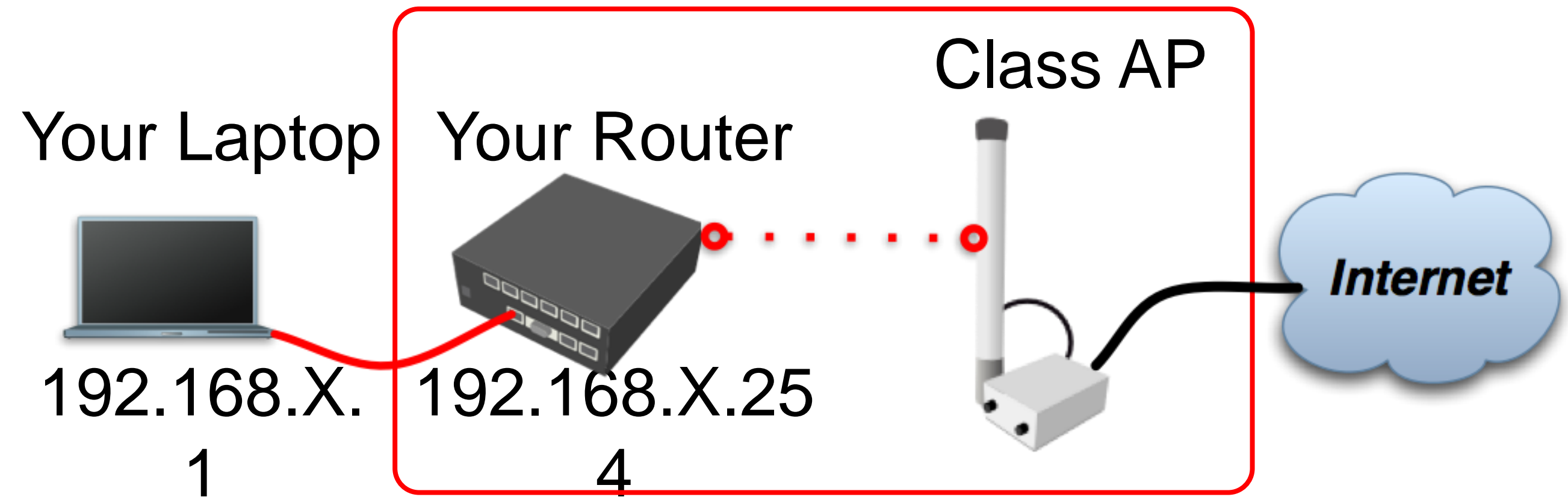
Laptop - Router

- Close Winbox and connect again using IP address
- MAC-address should only be used when there is no IP access

Laptop Router Diagram



Router Internet

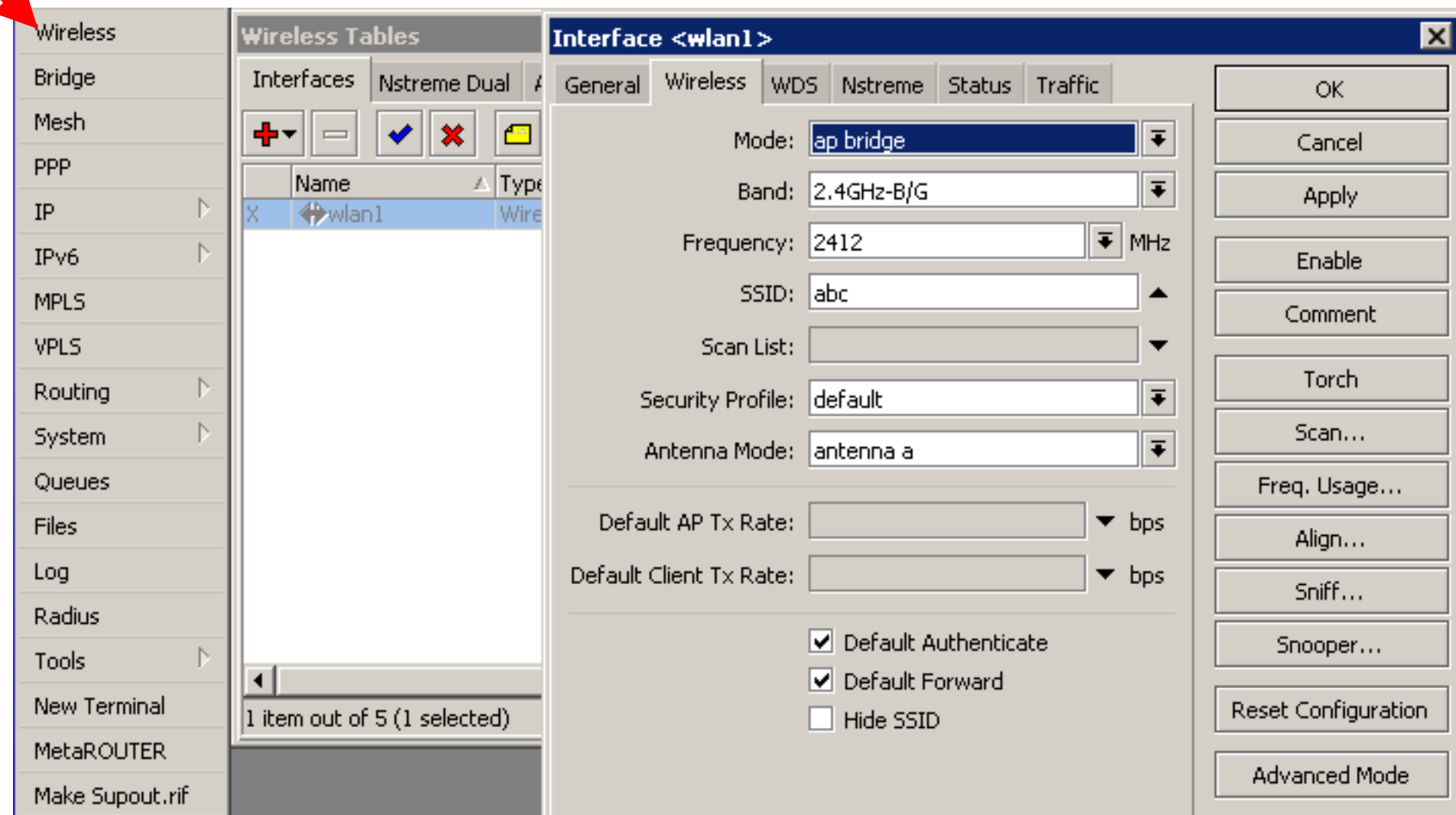


Router - Internet

- The Internet gateway of your class is accessible over wireless - it is an **AP** (access point)
- To connect you have to configure the wireless interface of your router as a **station**

Router - Internet

To configure wireless interface, double-click on it's name



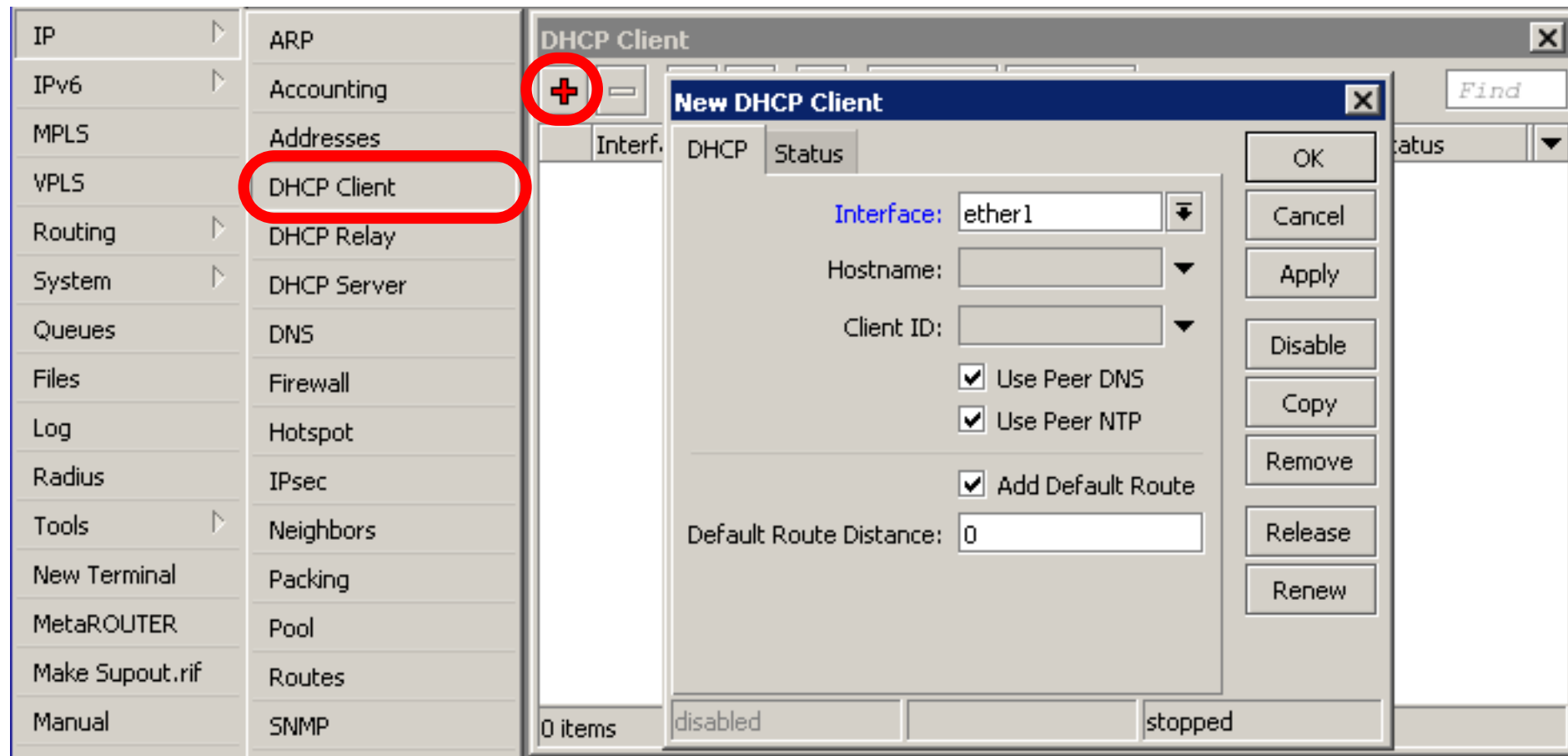
Router - Internet

- To see available AP use **scan** button
- Select **class1** and click on **connect**
- Close the scan window
- You are now connected to AP!
- Remember class SSID **class1**

Router - Internet

- The wireless interface also needs an IP address
- The AP provides automatic IP addresses over DHCP
- You need to enable DHCP client on your router to get an IP address

Router - Internet



Router - Internet

Check Internet
connectivity by
traceroute

Tools ▾

- New Terminal
- MetaROUTER
- Make Supout.rif
- Manual
- Exit

- BTest Server
- Bandwidth Test
- Email
- Flood Ping
- Graphing
- IP Scan
- MAC Server
- Netwatch
- Packet Sniffer
- Ping
- Ping Speed
- Telnet
- Torch
- Traceroute**

Traceroute

Traceroute To:

Packet Size:

Timeout: s

Protocol: ▾

Port:

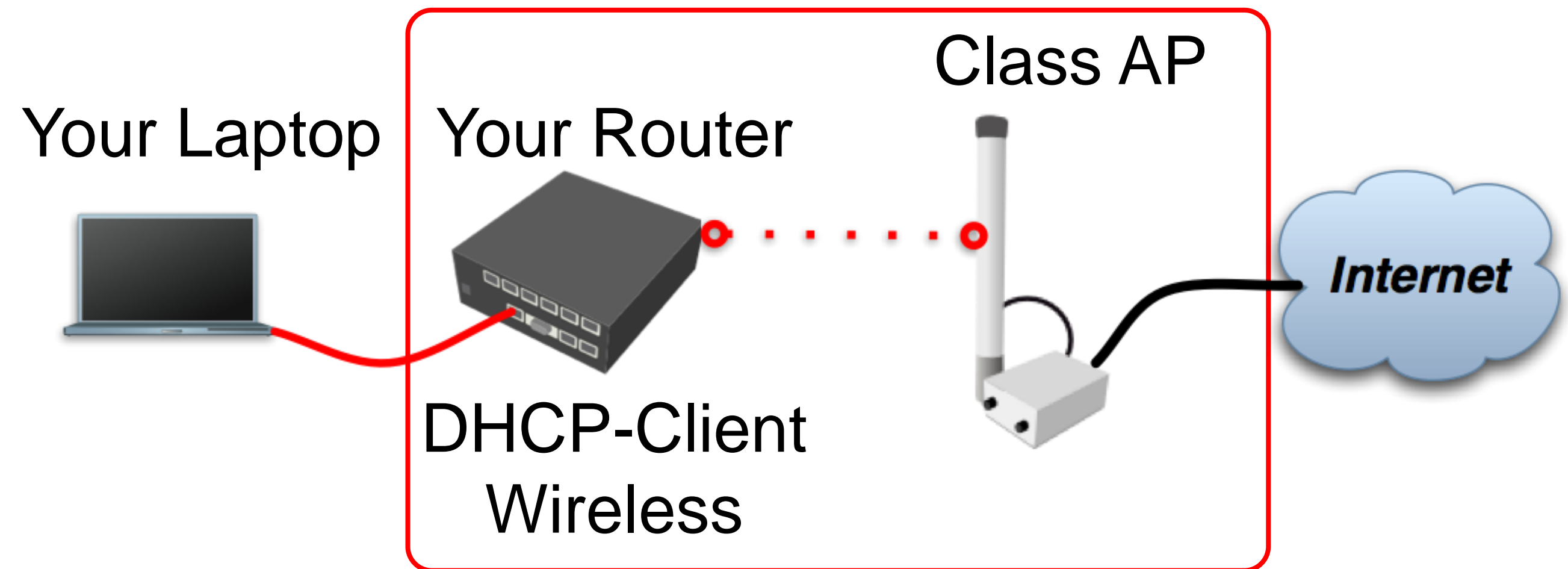
Src. Address: ▾

DSCP: ▾

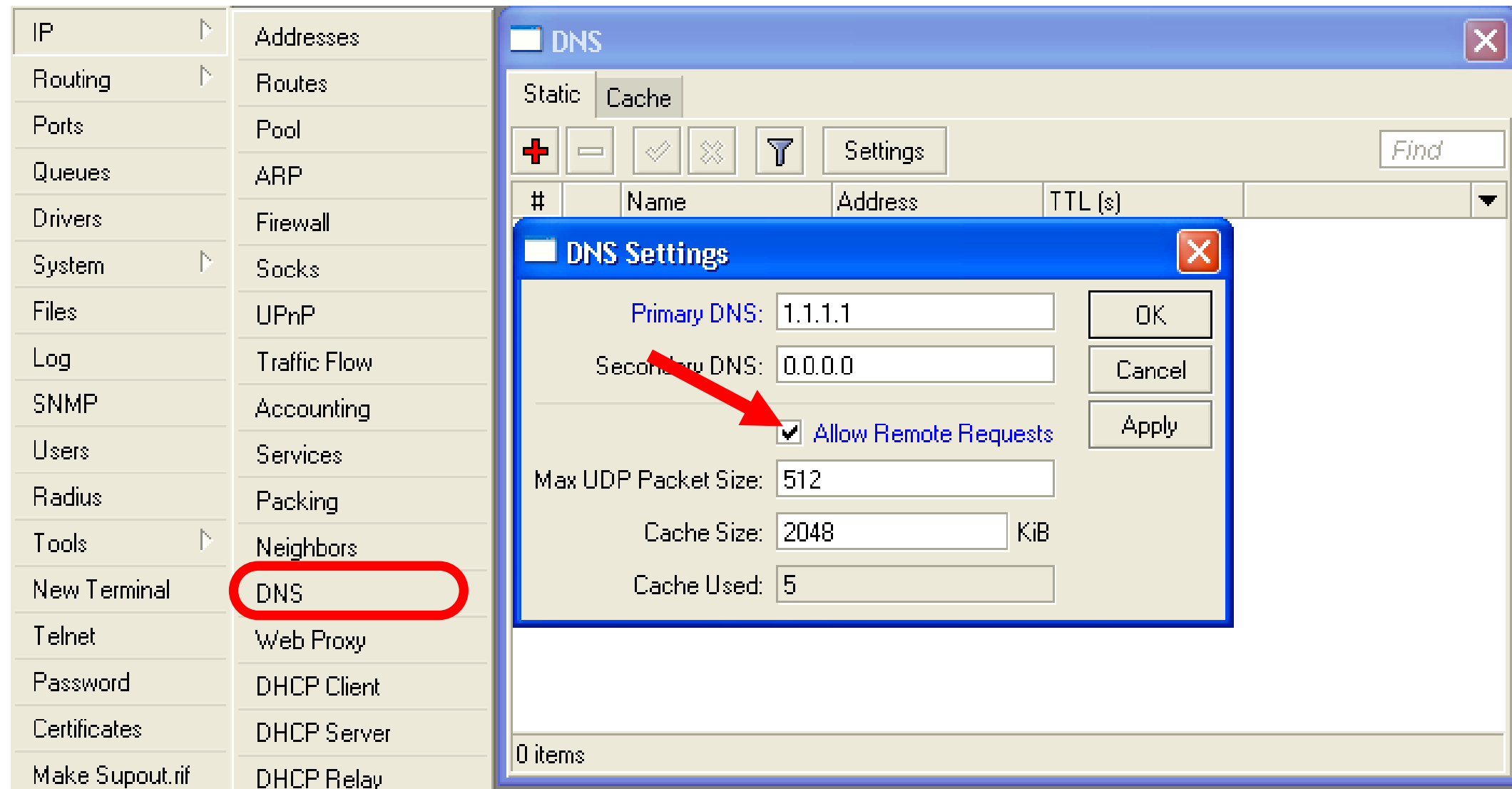
Routing Table: ▾

#	Host	Time 1	Time 2	Time 3
0	10.0.0.1	1ms	1ms	1ms
1	159.148.60.1	1ms	1ms	1ms
2	10.0.0.105	2ms	2ms	2ms
3	10.0.0.201	3ms	4ms	3ms

Router Internet



Laptop - Internet



Your router too can be a DNS server for your local network (laptop)

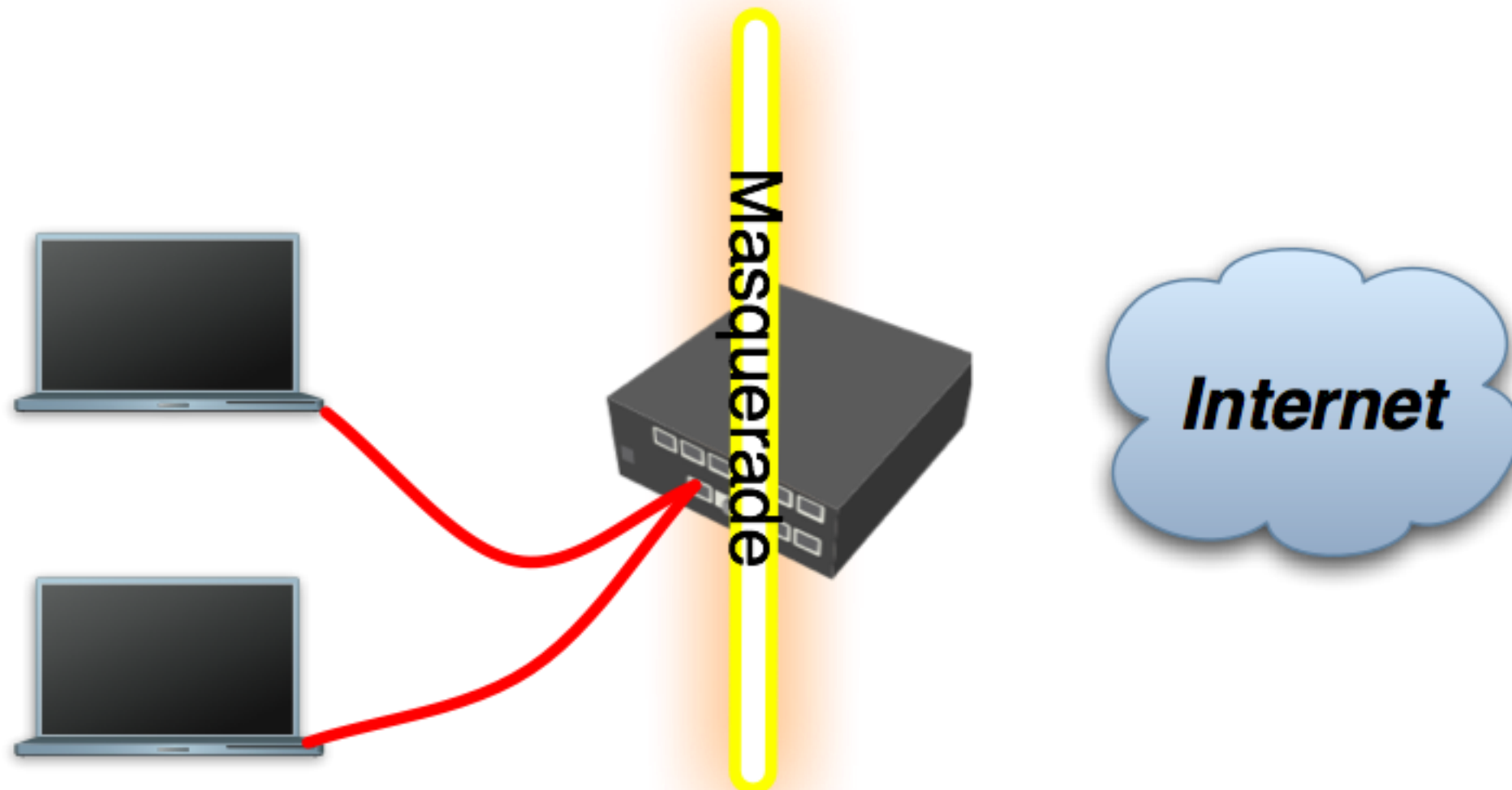
Laptop - Internet

- Tell **your Laptop** to use **your router** as the **DNS** server
- Enter your router IP (192.168.x.254) as the DNS server in laptop network settings

Laptop - Internet

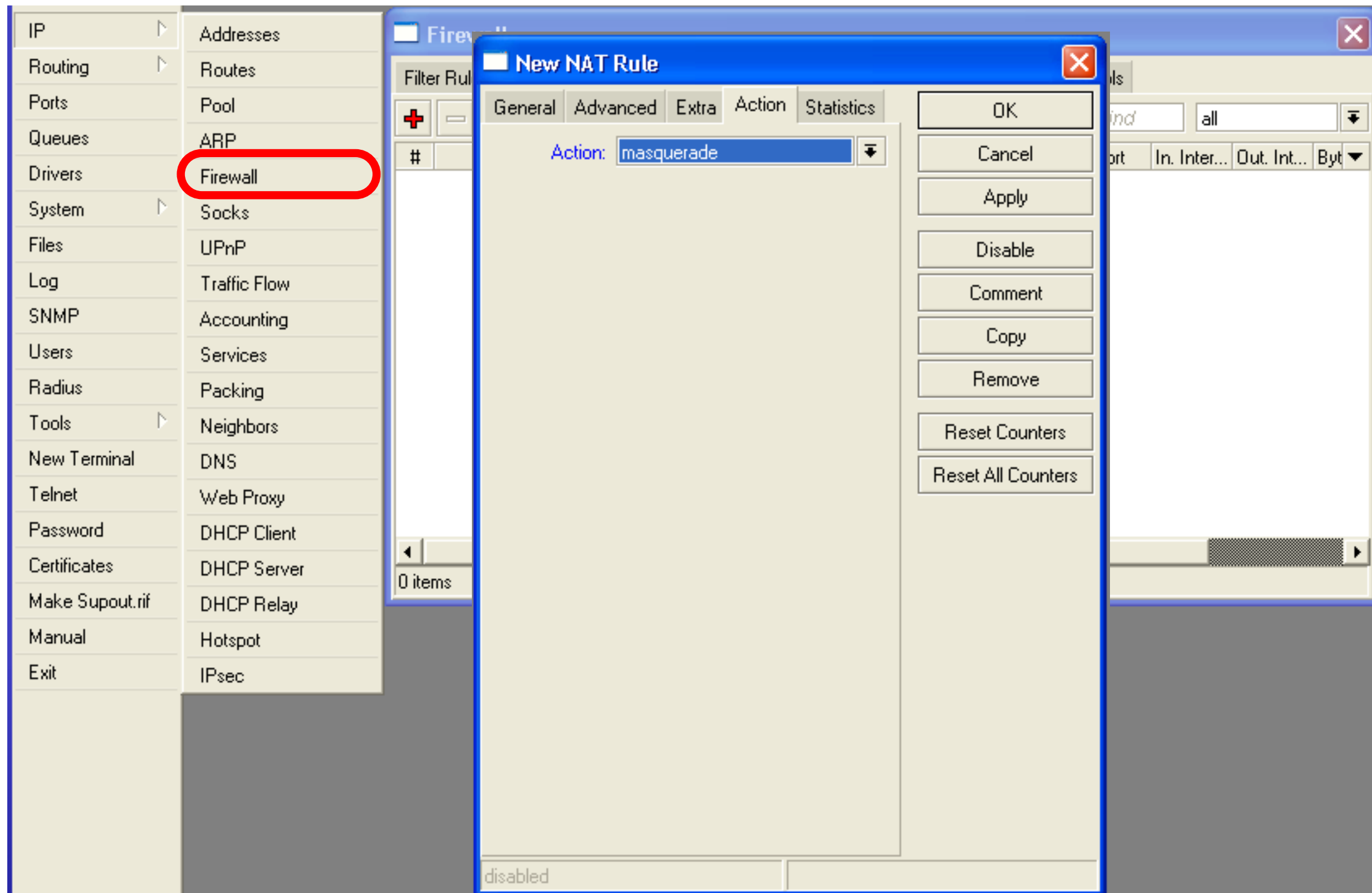
- Laptop can access the router and the router can access the internet, one more step is required
- Make a Masquerade rule to hide your private network behind the router, make Internet work in your laptop

Private and Public space



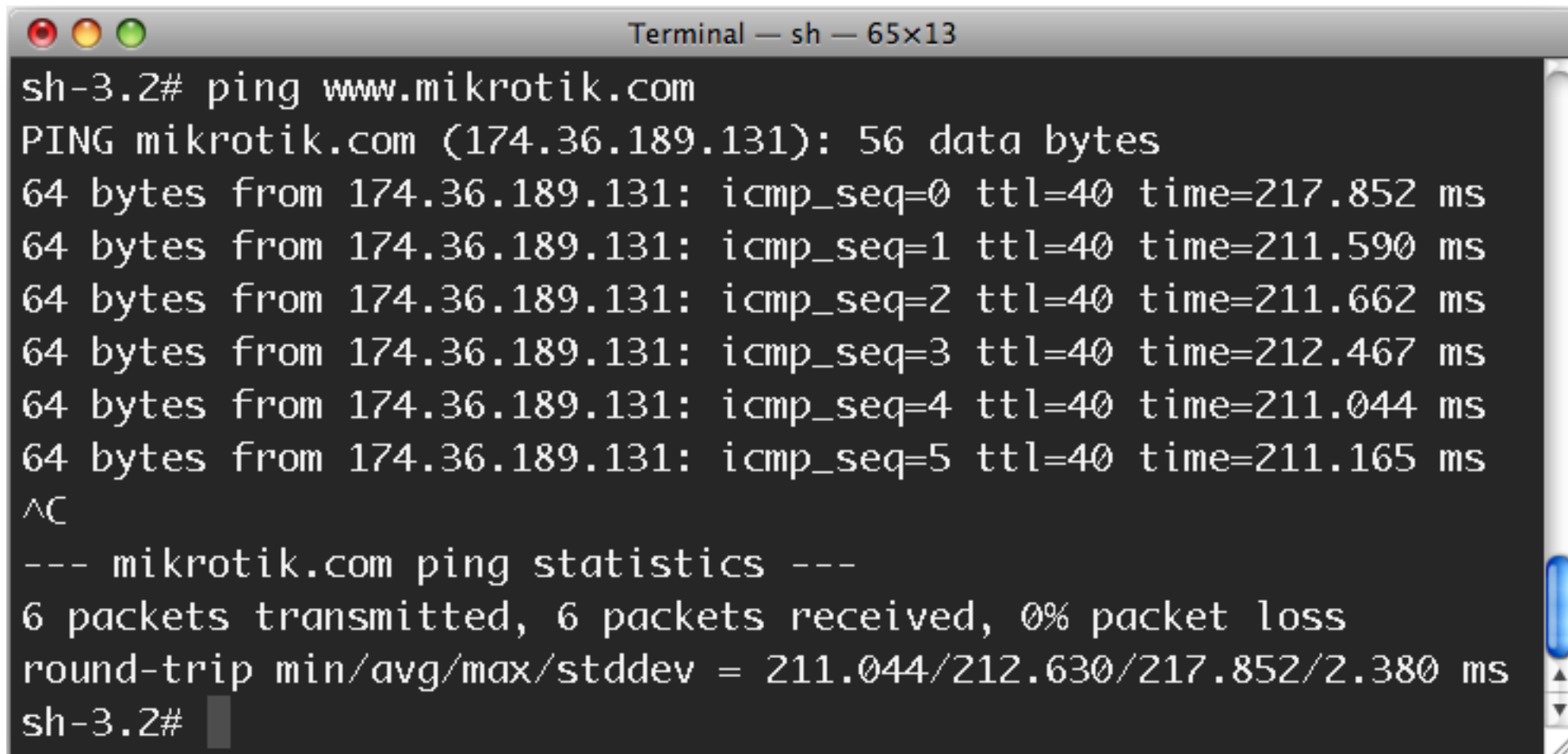
- **Masquerade** is used for Public network access, where private addresses are present
- Private networks include 10.0.0.0-10.255.255.255, 172.16.0.0-172.31.255.255, 192.168.0.0-192.168.255.255

Laptop - Internet



Check Connectivity

Ping www.mikrotik.com from your laptop

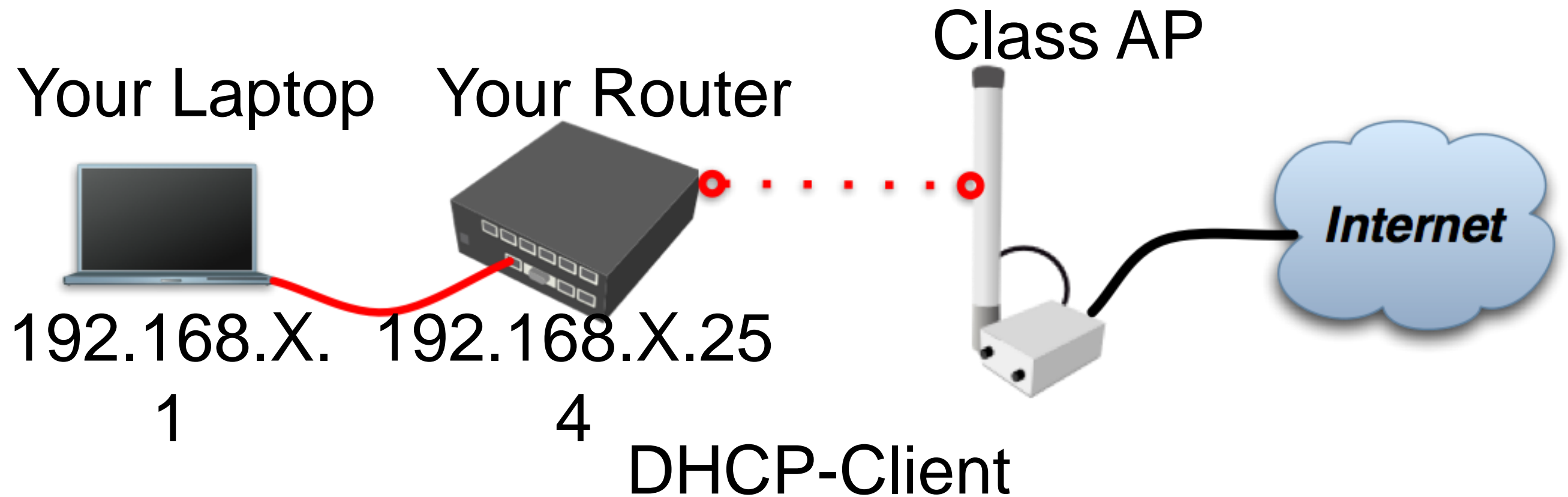
A screenshot of a terminal window titled "Terminal — sh — 65x13". The terminal shows the execution of a ping command to www.mikrotik.com. The output displays six successful ping attempts with varying response times. After the pings, the user presses the Ctrl-C key (indicated by ^C), and the terminal shows the ping statistics, indicating 0% packet loss and providing round-trip time statistics.

```
sh-3.2# ping www.mikrotik.com
PING mikrotik.com (174.36.189.131): 56 data bytes
64 bytes from 174.36.189.131: icmp_seq=0 ttl=40 time=217.852 ms
64 bytes from 174.36.189.131: icmp_seq=1 ttl=40 time=211.590 ms
64 bytes from 174.36.189.131: icmp_seq=2 ttl=40 time=211.662 ms
64 bytes from 174.36.189.131: icmp_seq=3 ttl=40 time=212.467 ms
64 bytes from 174.36.189.131: icmp_seq=4 ttl=40 time=211.044 ms
64 bytes from 174.36.189.131: icmp_seq=5 ttl=40 time=211.165 ms
^C
--- mikrotik.com ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max/stddev = 211.044/212.630/217.852/2.380 ms
sh-3.2#
```

What Can Be Wrong

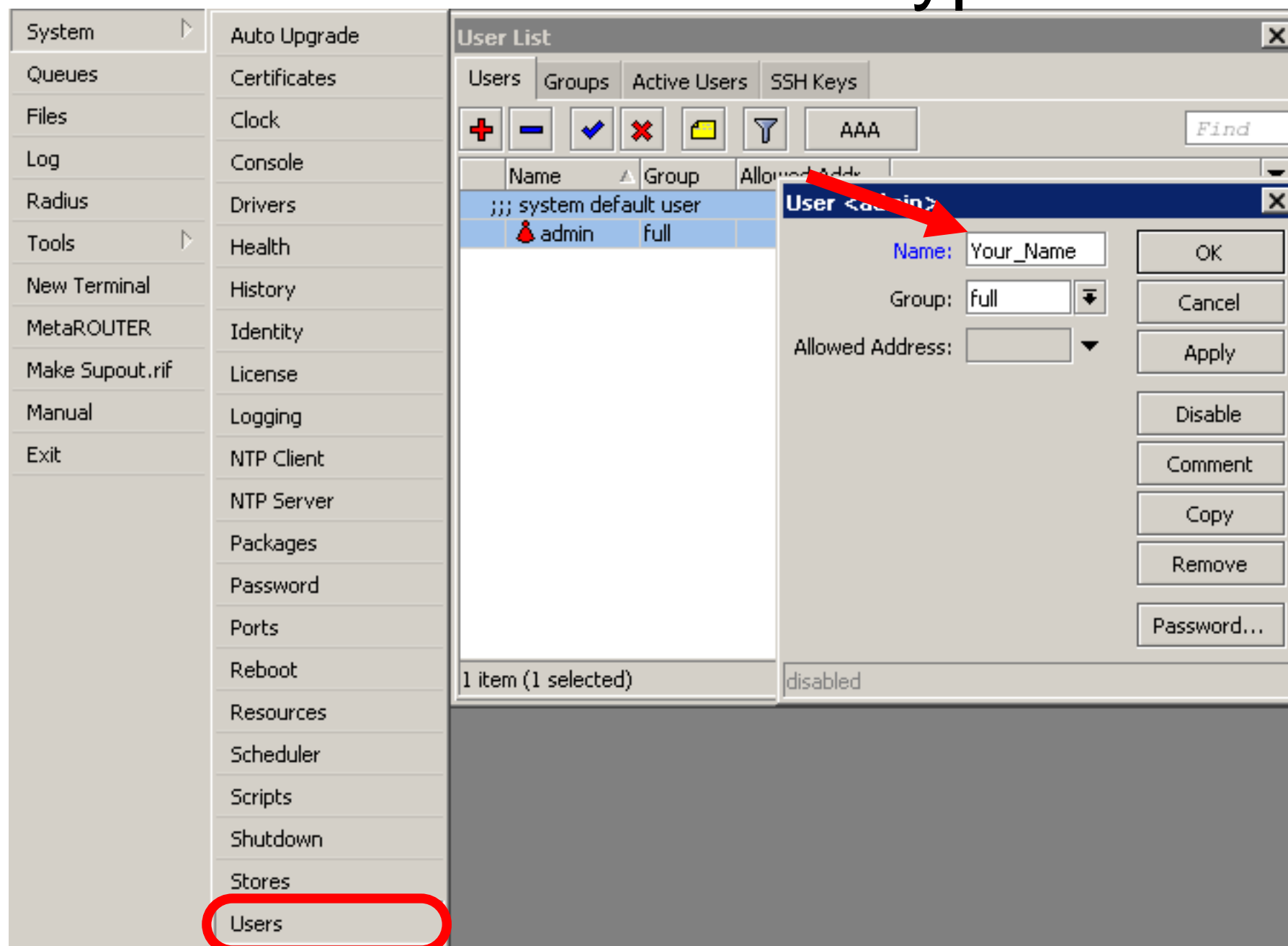
- Router cannot ping further than AP
- Router cannot resolve names
- Computer cannot ping further than router
- Computer cannot resolve names
- Is masquerade rule working
- Does the laptop use the router as default gateway and DNS

Network Diagram



User Management

- Access to the router can be controlled
- You can create different types of users



User Management Lab

LAB

- Add new router user with full access
- Make sure you remember user name
- Make admin user as read-only
- Login with your new user

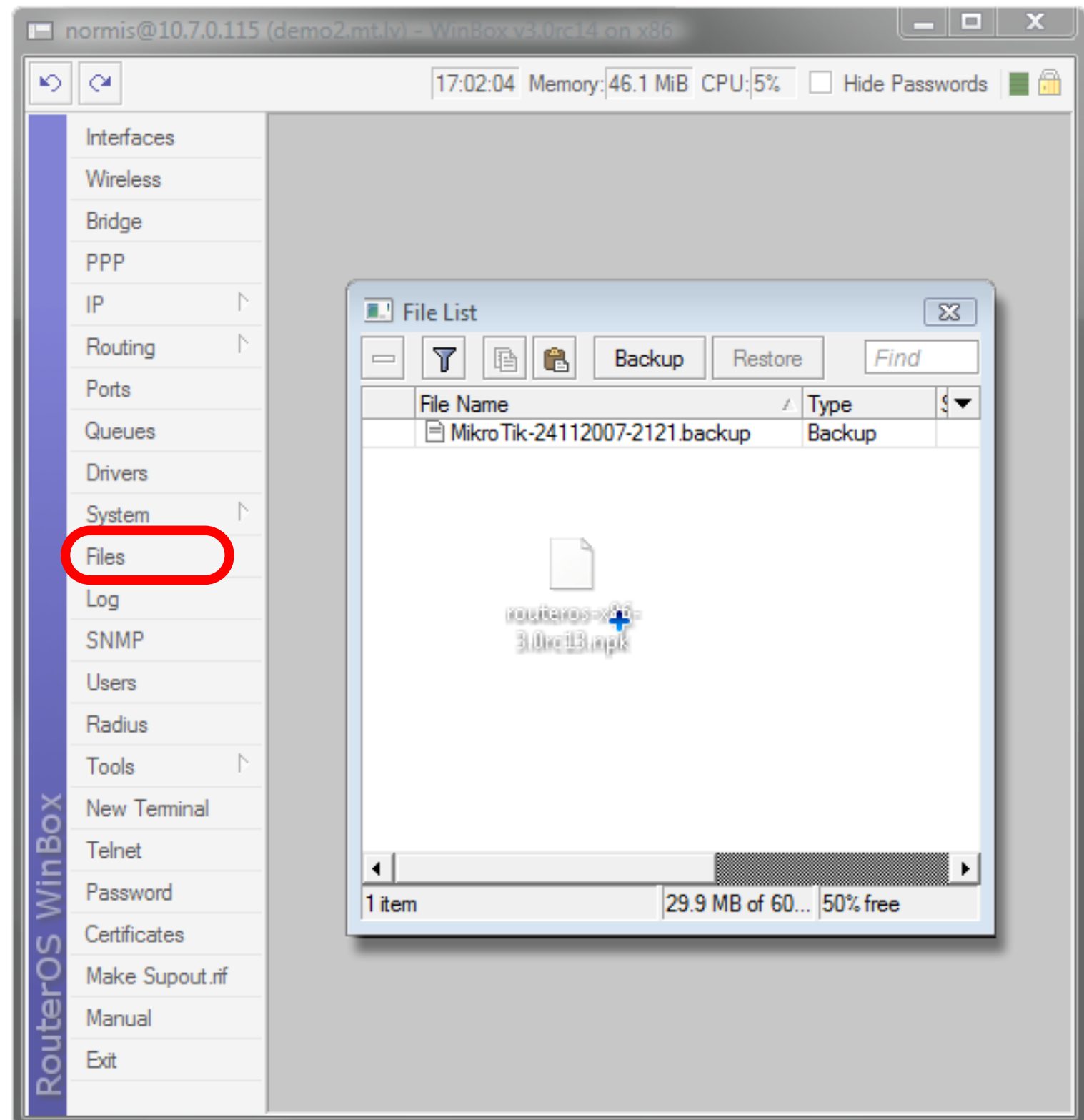
Upgrading Router Lab

LAB

- Download packages from ftp://192.168.200.254
- Upload them to router with Winbox
- Reboot the router
- Newest packages are always available on www.mikrotik.com

Upgrading Router

- Use combined RouterOS package
- Drag it to the Files window



Package Management

RouterOS functions are enabled by packages

The screenshot shows the RouterOS WinBox interface. On the left is a sidebar menu with categories like System, Queues, Files, Log, Radius, Tools, New Terminal, MetaROUTER, Make Supout.rif, Manual, and Exit. The 'Tools' category is expanded, showing sub-items: Auto Upgrade, Certificates, Clock, Console, Drivers, Health, History, Identity, License, Logging, NTP Client, **Packages** (highlighted with a red circle), Password, Ports, and Reboot. The main window displays the 'Package List' dialog. It features a toolbar with buttons: Enable, Disable, Uninstall, Unschedule, Downgrade, and a Find button. Below the toolbar is a table with columns: Name, Version, Build Time, and Scheduled. The table lists 12 installed packages. At the bottom of the dialog, it says '12 items'.

Name	Version	Build Time	Scheduled
routeros-mipsbe	3.27	Jul/16/2009 11:35:45	
advanced-...	3.27	Jul/16/2009 12:33:56	
dhcp	3.27	Jul/16/2009 12:34:03	
hotspot	3.27	Jul/16/2009 12:34:25	
X ipv6	3.27	Jul/16/2009 12:34:21	
ppp	3.27	Jul/16/2009 12:34:08	
routerboard	3.27	Jul/16/2009 12:34:52	
routing	3.27	Jul/16/2009 12:34:10	
X routing-test	3.27	Jul/16/2009 12:34:12	
security	3.27	Jul/16/2009 12:34:01	
system	3.27	Jul/16/2009 12:33:52	
wireless	3.27	Jul/16/2009 12:34:30	

Package Information

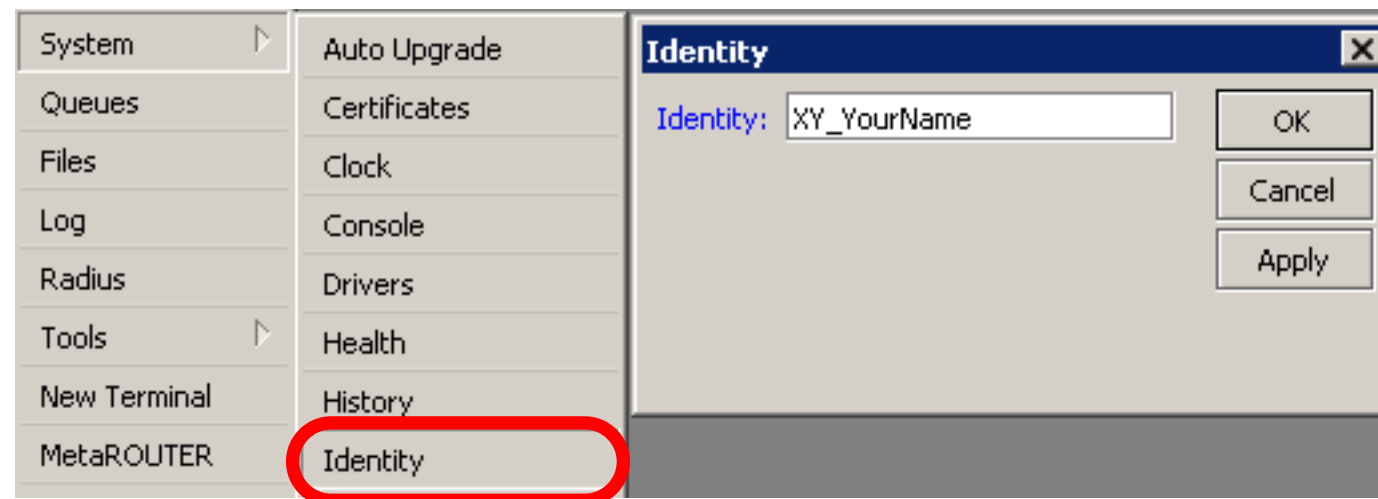
Name	Functions
advanced-tools	Email client, ping, netwatch
dhcp	DHCP Server and Client
hotspot	HotSpot Gateway
ntp	NTP server
ppp	PPP, PPTP, L2TP, PPPoE
routerboard	RouterBOARD specific functions
routing	RIP, OSPF, BGP
security	Secure Winbox, SSH, IPSec
wireless	Wireless 802.11 a/b/g
user-manager	User-Manager management system
ipv6	IPv6

Package Lab

- Disable wireless
- Reboot
- Check interface list
- Enable wireless

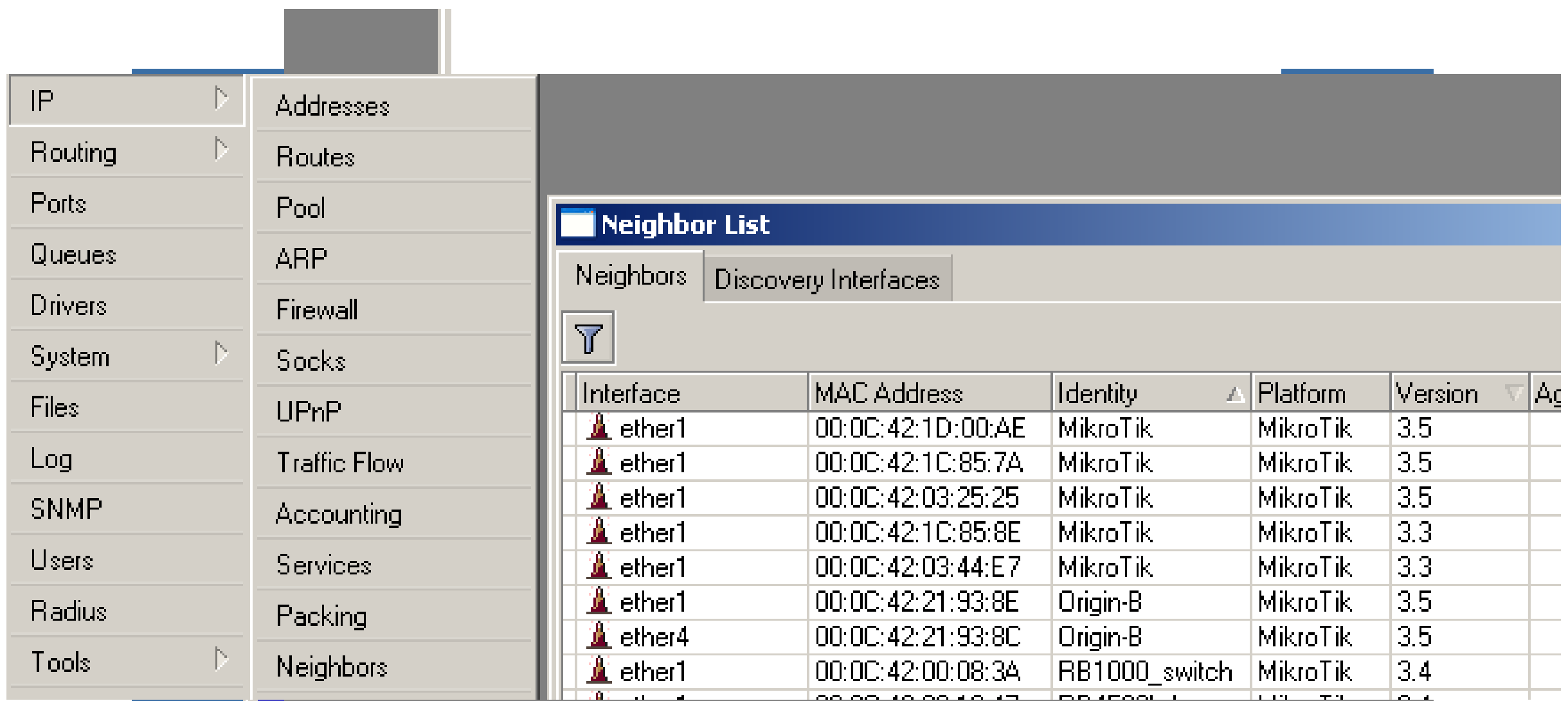
Router Identity

Option to set name for each router



Router Identity

Identity information is shown in different places



The screenshot shows the Mikrotik WinBox interface. On the left is a sidebar menu with categories like IP, Routing, Ports, Queues, Drivers, System, Files, Log, SNMP, Users, Radius, and Tools. The 'Neighbors' option under the 'Tools' category is selected. The main window displays the 'Neighbor List' tab, which shows a table of discovered neighbors. The table has columns for Interface, MAC Address, Identity, Platform, Version, and Age. The data shows several neighbors connected to the 'ether1' interface, mostly identified as 'MikroTik' with version 3.5, and one identified as 'Origin-B' with version 3.5, and another as 'RB1000_switch' with version 3.4.

Interface	MAC Address	Identity	Platform	Version	Age
ether1	00:0C:42:1D:00:AE	MikroTik	MikroTik	3.5	
ether1	00:0C:42:1C:85:7A	MikroTik	MikroTik	3.5	
ether1	00:0C:42:03:25:25	MikroTik	MikroTik	3.5	
ether1	00:0C:42:1C:85:8E	MikroTik	MikroTik	3.3	
ether1	00:0C:42:03:44:E7	MikroTik	MikroTik	3.3	
ether1	00:0C:42:21:93:8E	Origin-B	MikroTik	3.5	
ether4	00:0C:42:21:93:8C	Origin-B	MikroTik	3.5	
ether1	00:0C:42:00:08:3A	RB1000_switch	MikroTik	3.4	

Router Identity Lab

Set **your number + your name** as router identity

NTP

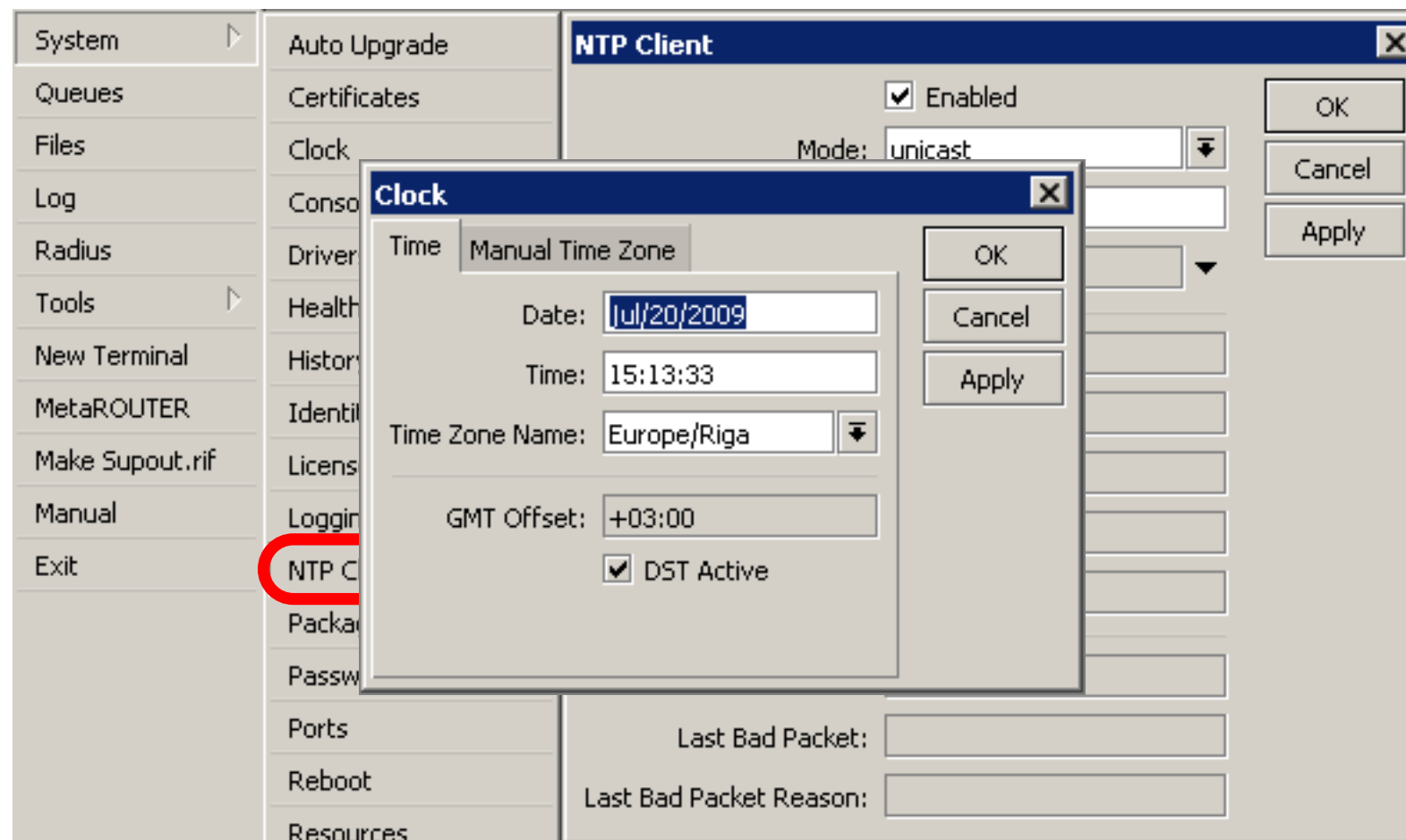
- Network Time Protocol, to synchronize time
- NTP Client and NTP Server support in RouterOS

Why NTP

- To get correct clock on router
- For routers without internal memory to save clock information
- For all RouterBOARDS

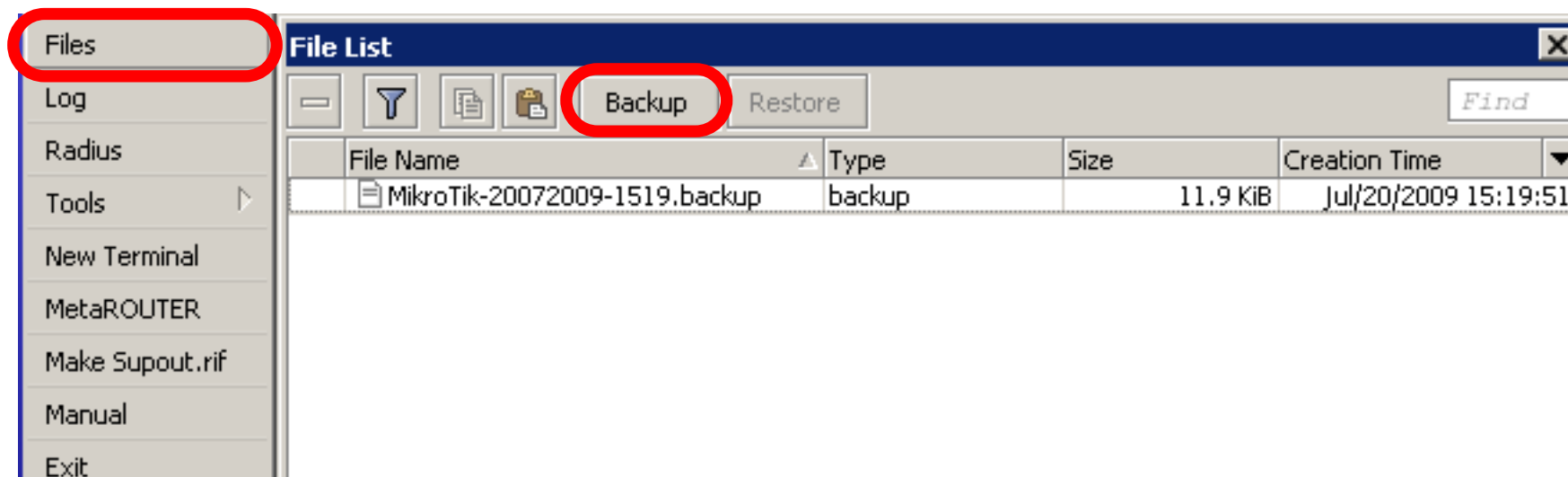
NTP Client

NTP package is not required



Configuration Backup

- You can backup and restore configuration in the Files menu of Winbox
- Backup file is not editable



Configuration Backup

- Additionally use export and import commands in CLI
- Export files are editable
- Passwords are not saved with export

```
/export file=conf-august-2009
```

```
/ ip firewall filter export file=firewall-aug-2009
```

```
/ file print
```

```
/ import [Tab]
```

Backup Lab

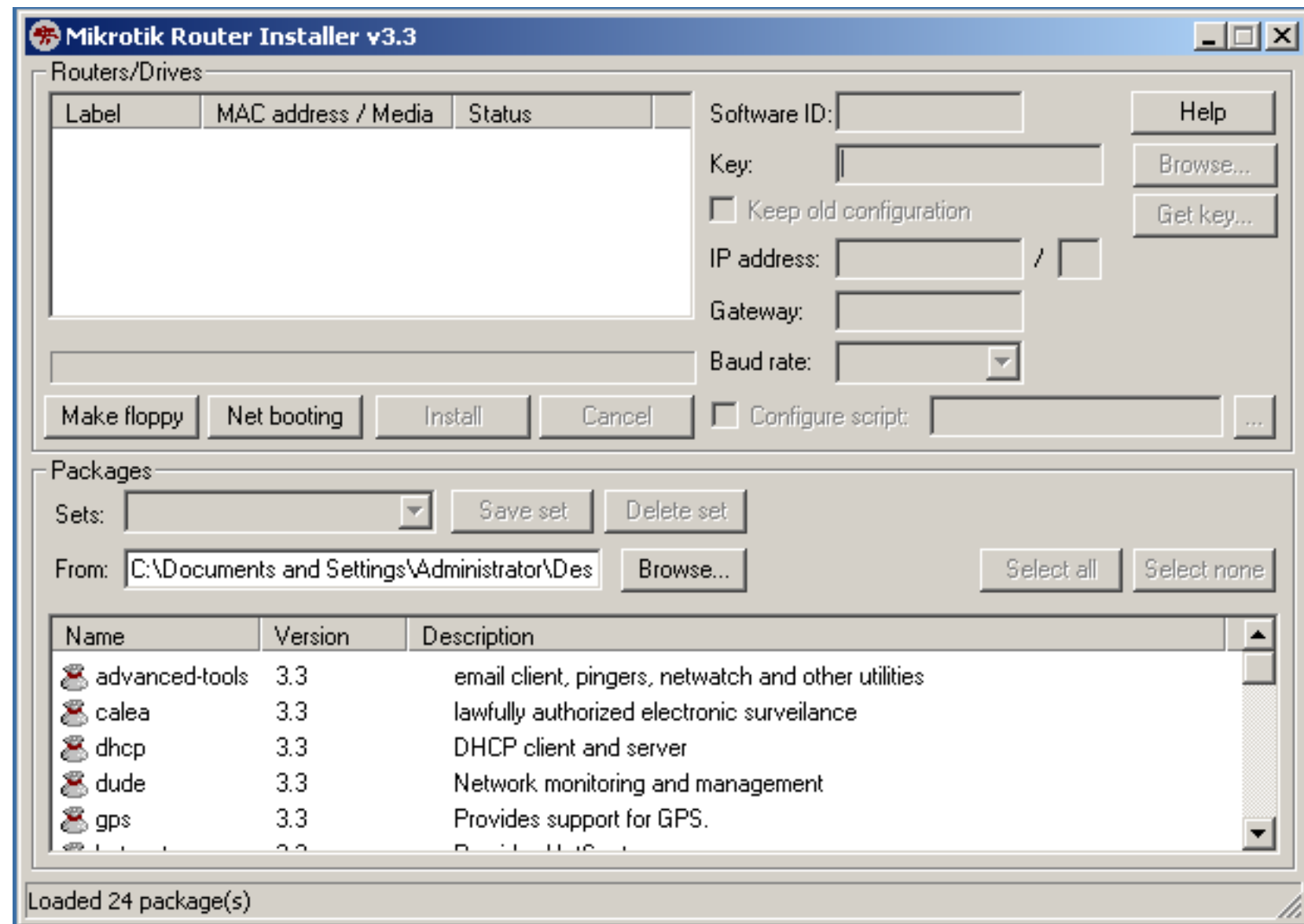
- Create Backup and Export files
- Download them to your laptop
- Open export file with text editor

Netinstall

- Used for installing and reinstalling RouterOS
- Runs on Windows computers
- Direct network connection to router is required or over switched LAN
- Available at www.mikrotik.com

Netinstall

1. List of routers
2. Net Booting
3. Keep old configuration
4. Packages
5. Install



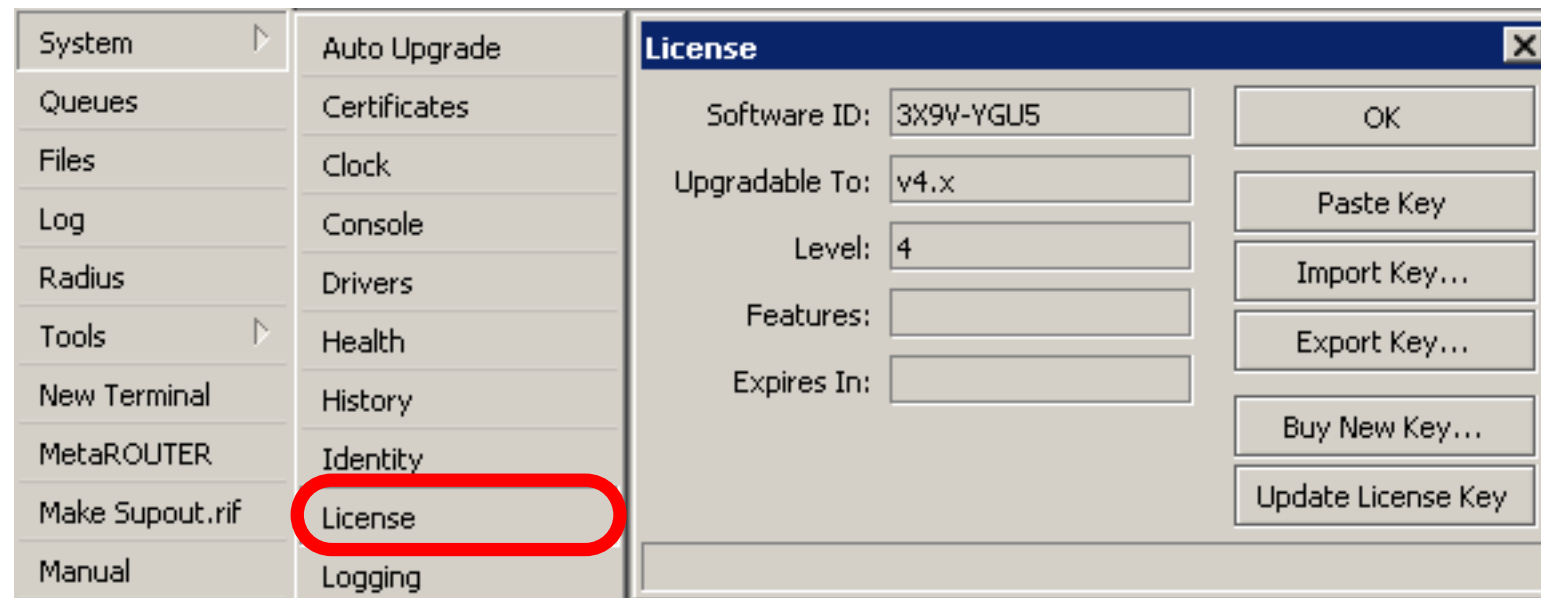
Optional Lab

- Download Netinstall from <ftp://192.168.100.254>
- Run Netinstall
- Enable Net booting, set address 192.168.x.13
- Use null modem cable and Putty to connect
- Set router to boot from Ethernet

RouterOS License

- All RouterBOARDS shipped with license
- Several levels available, no upgrades
- Can be viewed in system license menu
- License for PC can be purchased from mikrotik.com or from distributors

License



Obtain License

MT http://www.mikrotik.com/ Inquisitor

Routers & Wireless

home products software wireless sitemap support buy

Main Buy Our customers About us Press Download Jobs New Account

MikroTik everywhere: AP CPE Network Monitor User Manager HotSpot Gateway Core Router

MUM Poland 2008 RouterOS Software MikroTik News

[info] [docs] [wiki] [forum] [download]

MikroTik Newsletter this week:

- New product
- Winbox improvements
- NASA/NOAA uses RouterOS
- New package files

Issue No.005

RouterBOARD 333: \$180 USD

Login to your account

- registration for MUM
- registration for training before MUM


MikroTik Training

Date	Location	Partner
February 5-6	Prague, Czech Republic	Futureshop
February 7	Prague, Czech Republic	Jaromir Cihak
February 18-22	Yogyakarta, Indonesia	CitraWeb
February 19-22	Ibadan, Nigeria	GDES
February 19-22	Recife/PE, Brazil	MD Brasil
February 25-27	Krakow, Poland	Mikrotik
February 26-29	Cape Town, South Africa	MIRO
	Ratam Island	

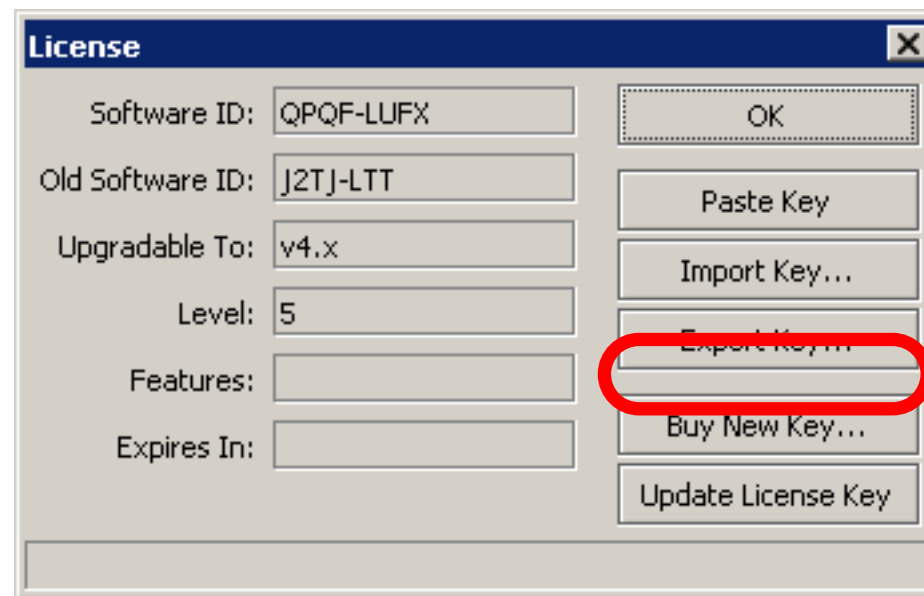
or features:

- Best wireless performance
- Improved Nstreme performance
- Powerful QoS control
- P2P traffic filtering
- High availability with VRRP
- Bonding of Interfaces
- Improved interface
- Smaller and Less resource-hungry
- Tons of other new features
- Advanced Quality of Service
- Stateful firewall, tunnels
- STP bridging with filtering
- High speed 802.11a/b/g wireless with WEP/WPA
- WDS and Virtual AP
- HotSpot for Plug-and-Play access
- RIP, OSPF, BGP routing
- remote WinBox GUI and Web admin
- telnet/mac-telnet/ssh/console admin
- real-time configuration and monitoring

Detailed Description



Update License for 802.11N



- 8-symbol software-ID system is introduced
- **Update key** on existing routers to get full features support (**802.11N**, etc.)

Summary

Useful Links

- www.mikrotik.com - manage licenses, documentation
- forum.mikrotik.com - share experience with other users
- wiki.mikrotik.com - tons of examples

Firewall

Firewall

- Protects your router and clients from unauthorized access
- This can be done by creating rules in Firewall Filter and NAT facilities

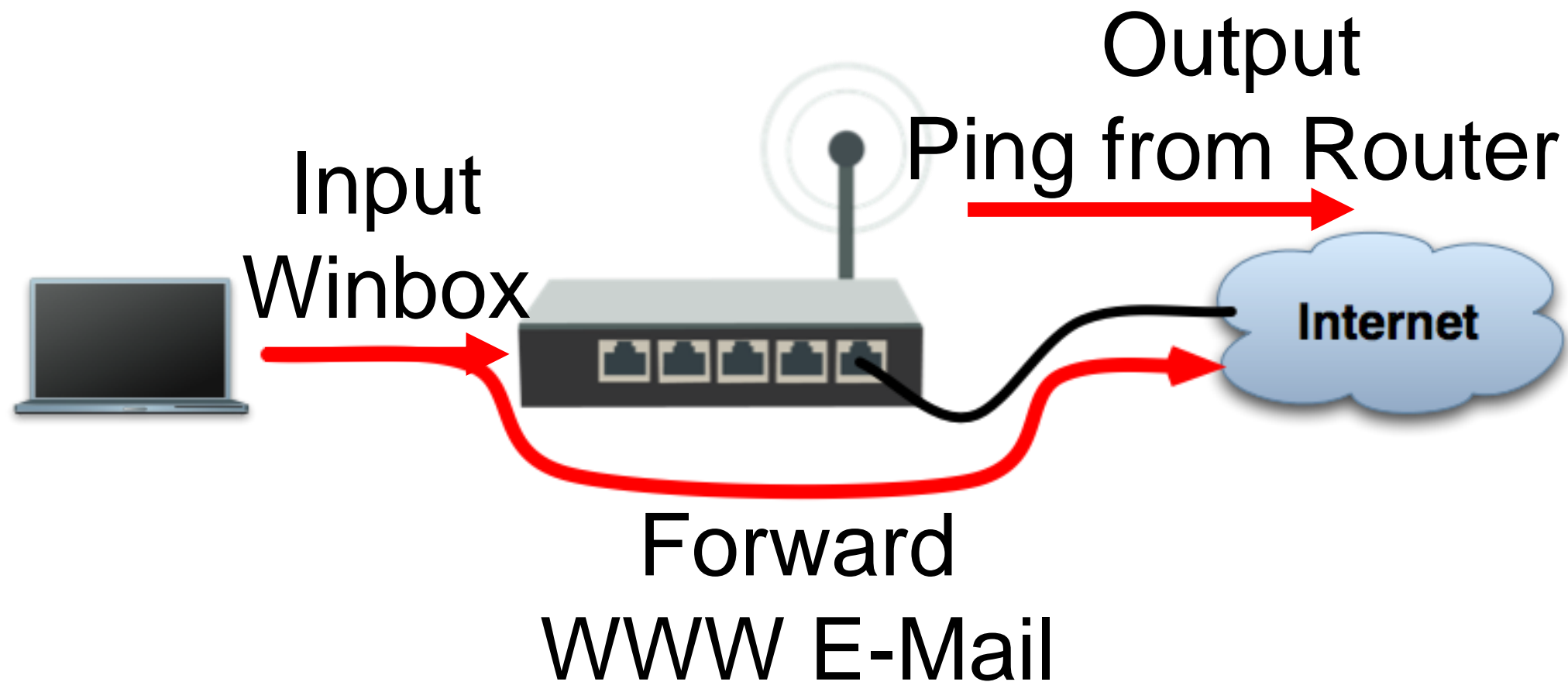
Firewall Filter

- Consists of user defined rules that work on the **IF-Then** principle
- These rules are ordered in Chains
- There are predefined Chains, and User created Chains

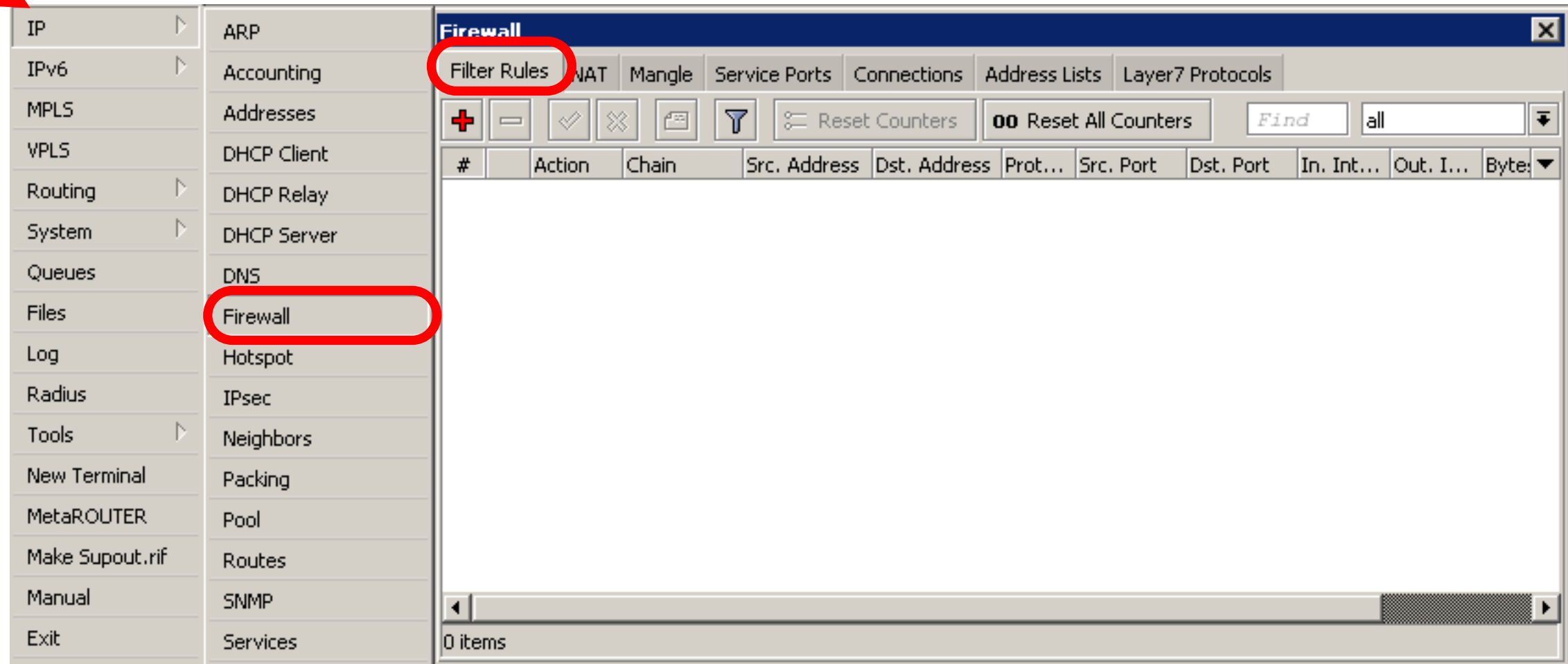
Filter Chains

- Rules can be placed in three default chains
 - input (**to** router)
 - output (**from** router)
 - forward (**trough** the router)

Firewall Chains



Firewall Chains

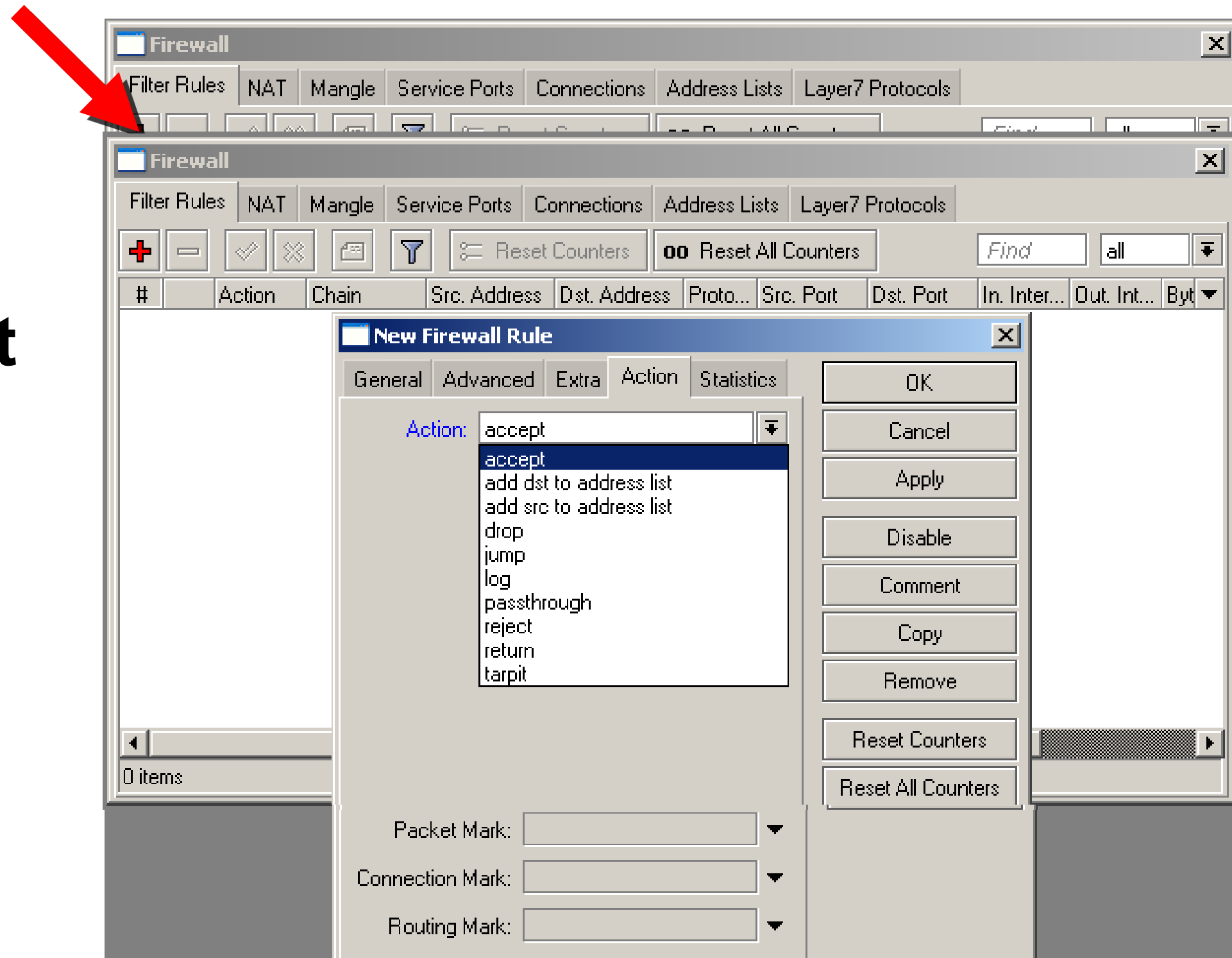


Input

- Chain contains filter rules that protect the **router itself**
- Let's block everyone except your laptop

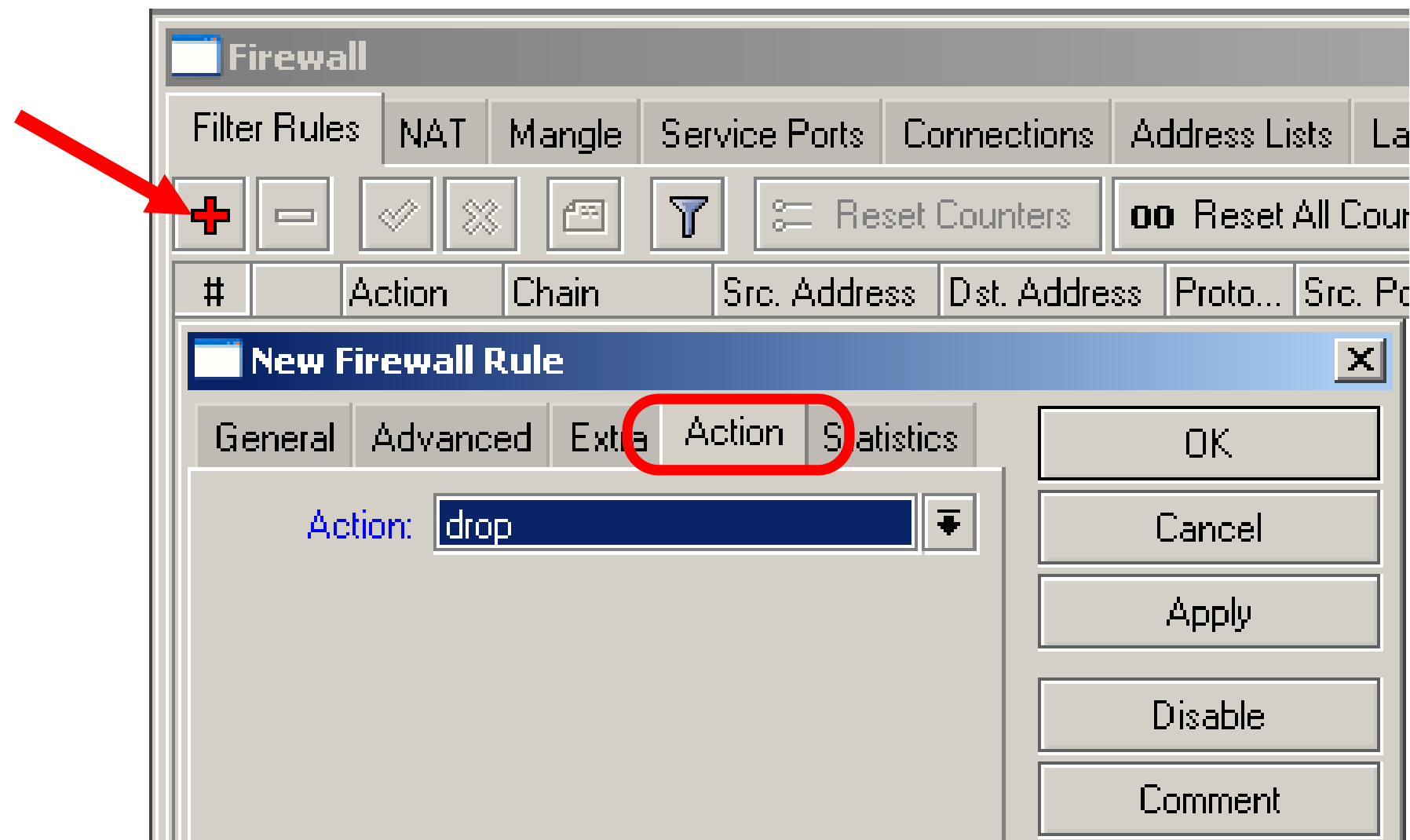
Input

Add an **accept** rule for your Laptop IP address



Input

Add a **drop** rule
in input chain
to drop
everyone else



Input Lab

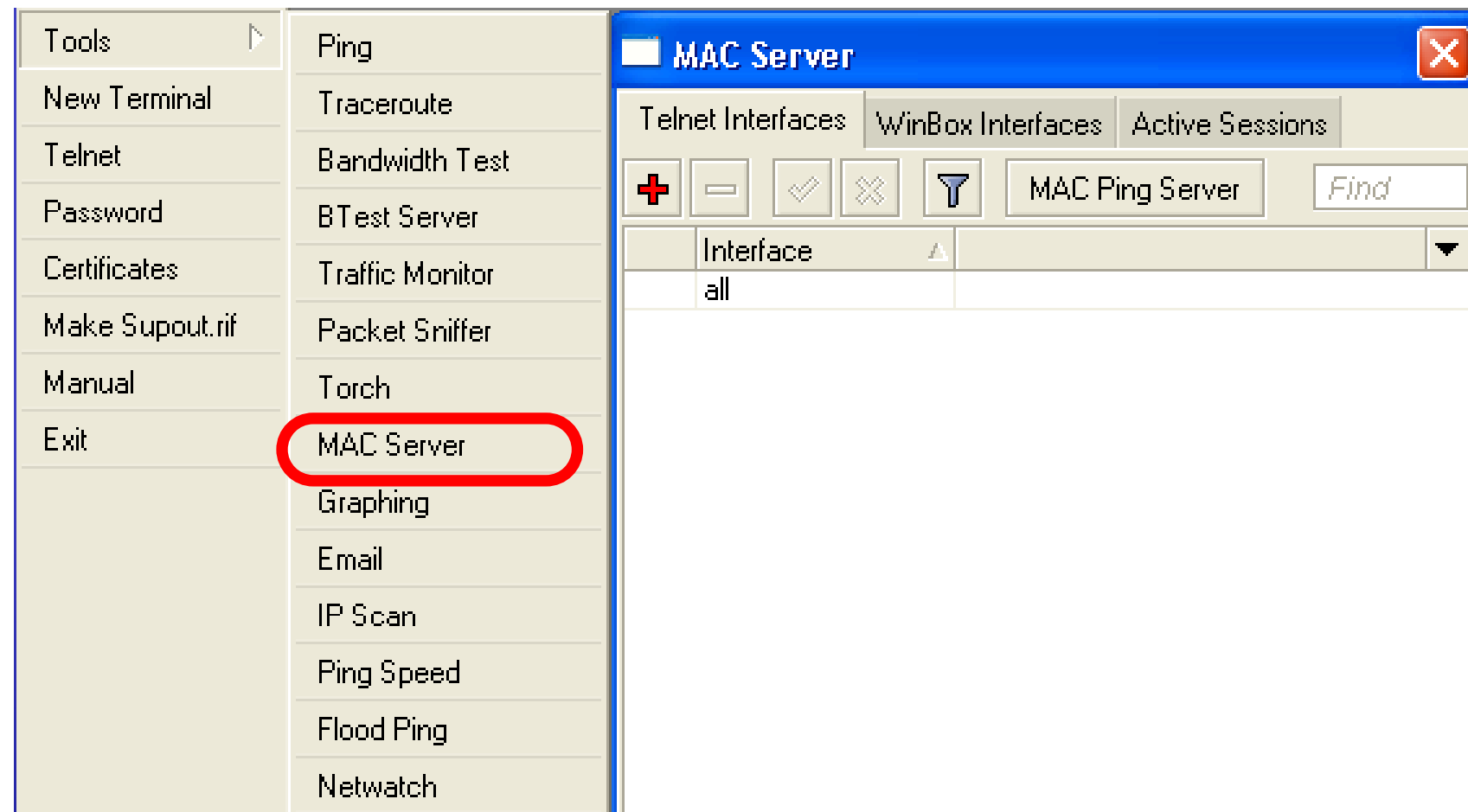
- Change your laptop IP address, 192.168.x.**y**
- Try to connect. The firewall is working
- You can still connect with MAC-address, Firewall Filter is only for IP

Input

- Access to your router is blocked
- Internet is not working
- Because we are blocking DNS requests as well
- Change configuration to make Internet working

Input

- You can disable MAC access in the **MAC Server** menu
- Change the Laptop IP address back to 192.168.X.**1**, and connect with IP

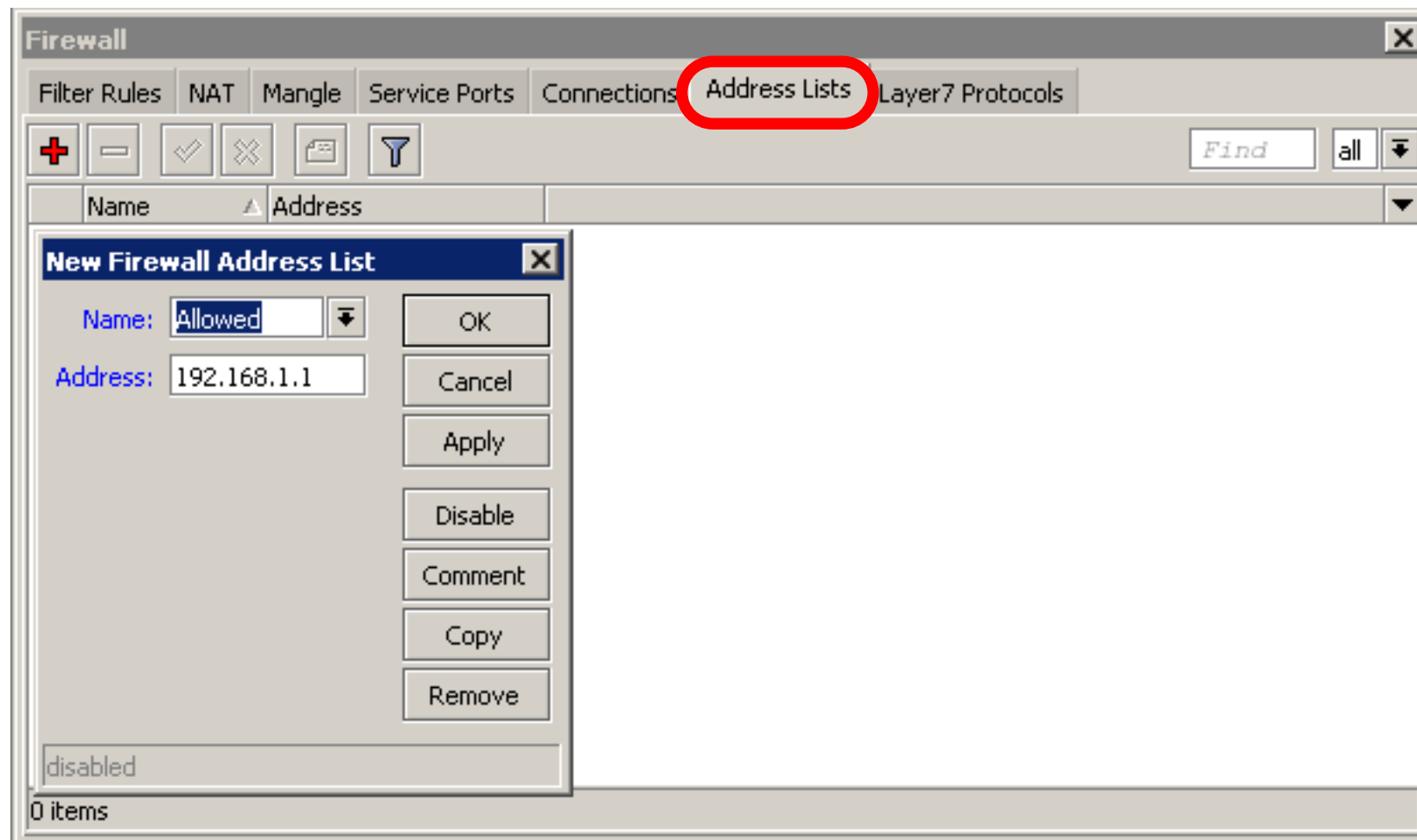


Address-List

- Address-list allows you to filter group of the addresses with one rule
- Automatically add addresses by address-list and then block

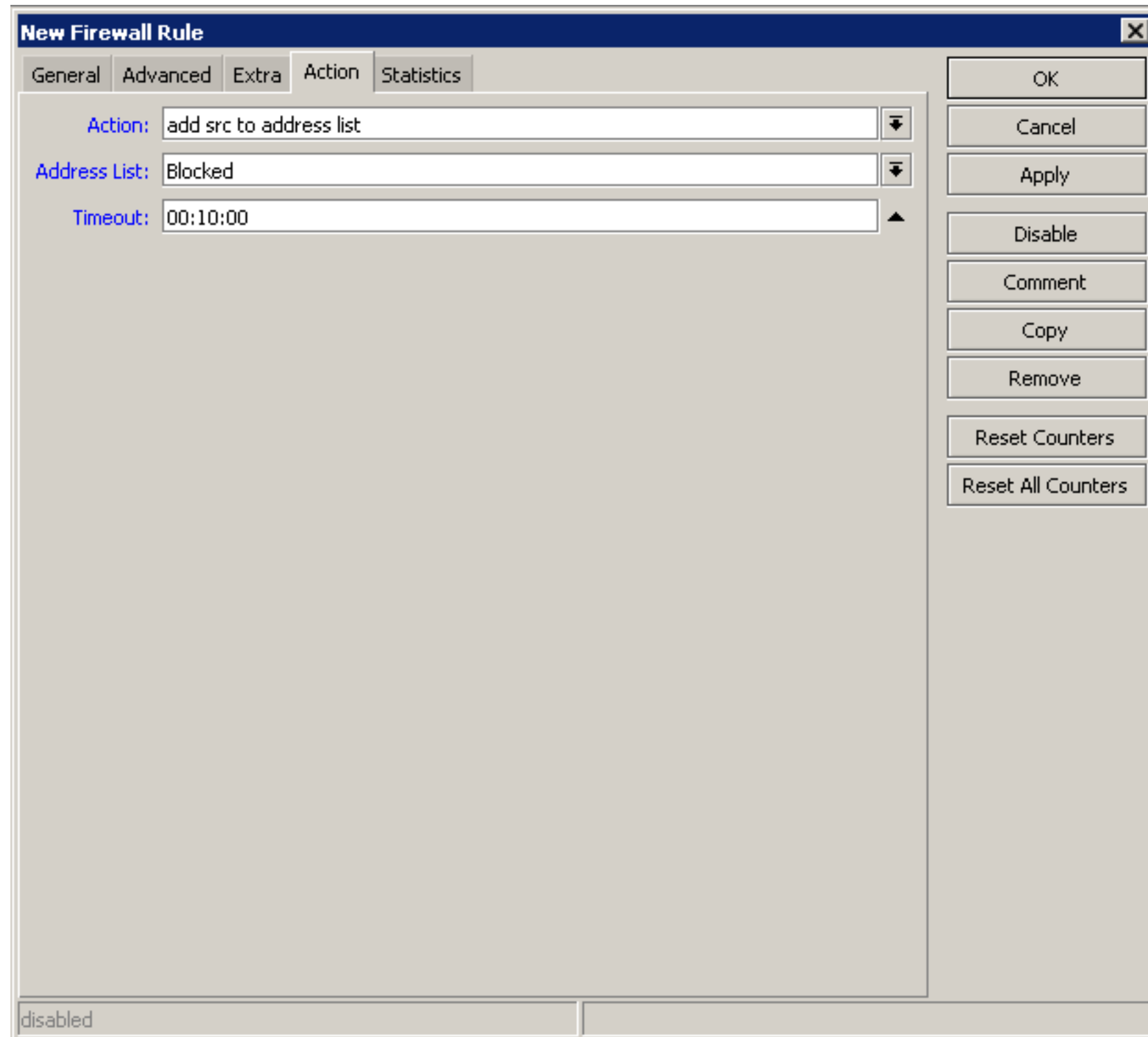
Address-List

- Create different lists
- Subnets, separates ranges, one host addresses are supported



Address-List

- Add specific host to address-list
- Specify timeout for temporary service



Address-List in Firewall

- Ability to block by source and destination addresses

The screenshot shows the 'New Firewall Rule' dialog box with the 'Advanced' tab selected. The 'Src. Address List' field is highlighted with a red circle and contains the text 'Allowed'. Other fields include 'Dst. Address List', 'Layer7 Protocol', 'Content', 'Connection Bytes', 'Per Connection Classifier', 'Src. MAC Address', 'Out. Bridge Port', 'In. Bridge Port', 'Ingress Priority', 'DSCP (TOS)', 'TCP MSS', 'Packet Size', 'Random', 'TCP Flags', 'ICMP Options', and 'IPv4 Options'. The status bar at the bottom indicates 'disabled'.

Address-List Lab

LAB

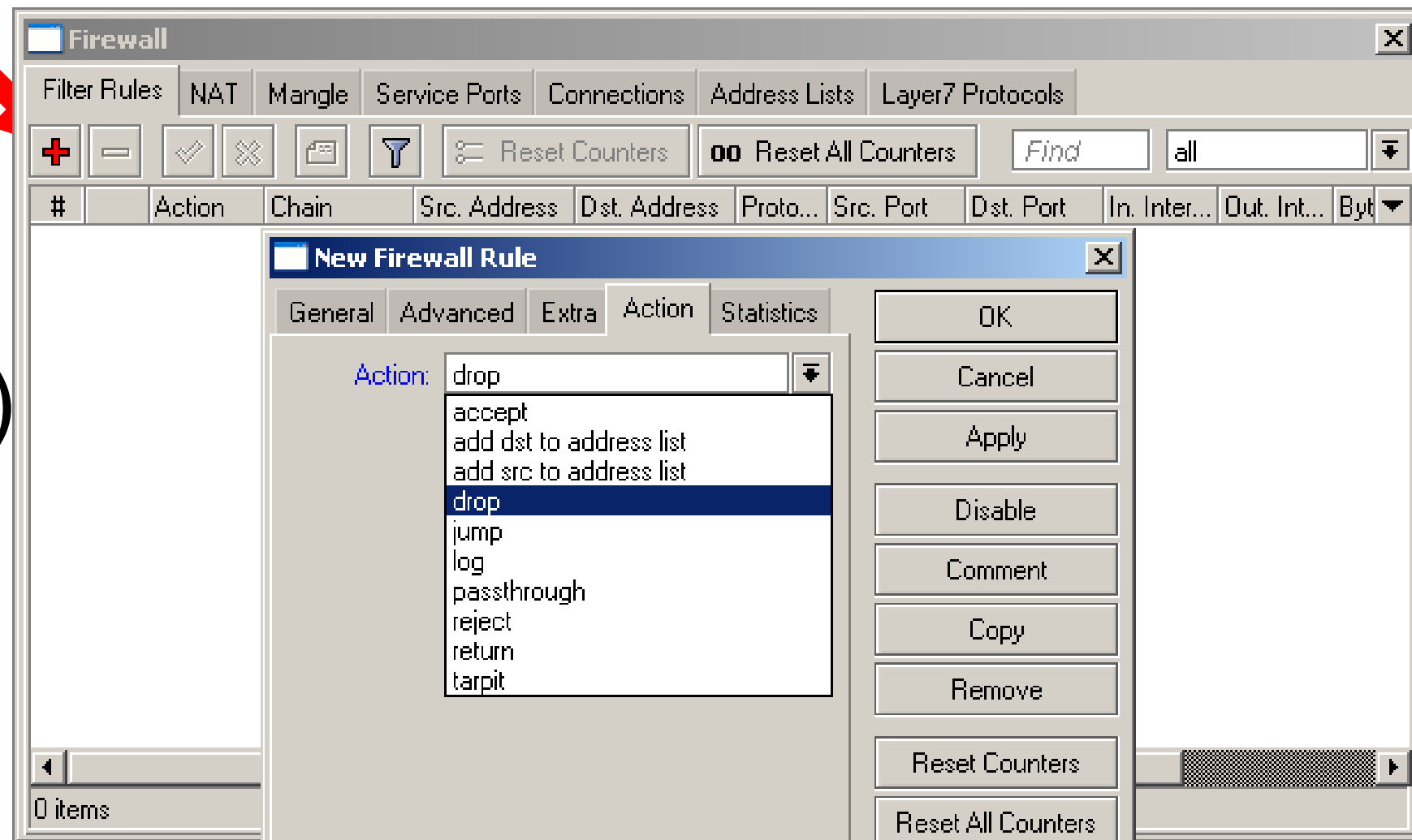
- Create address-list with allowed IP addresses
- Add accept rule for the allowed addresses

Forward

- Chain contains rules that control packets going **through** the router
- Control traffic **to and from the clients**

Forward

- Create a rule that will block TCP port 80 (web browsing)
- Must select protocol to block ports



Forward

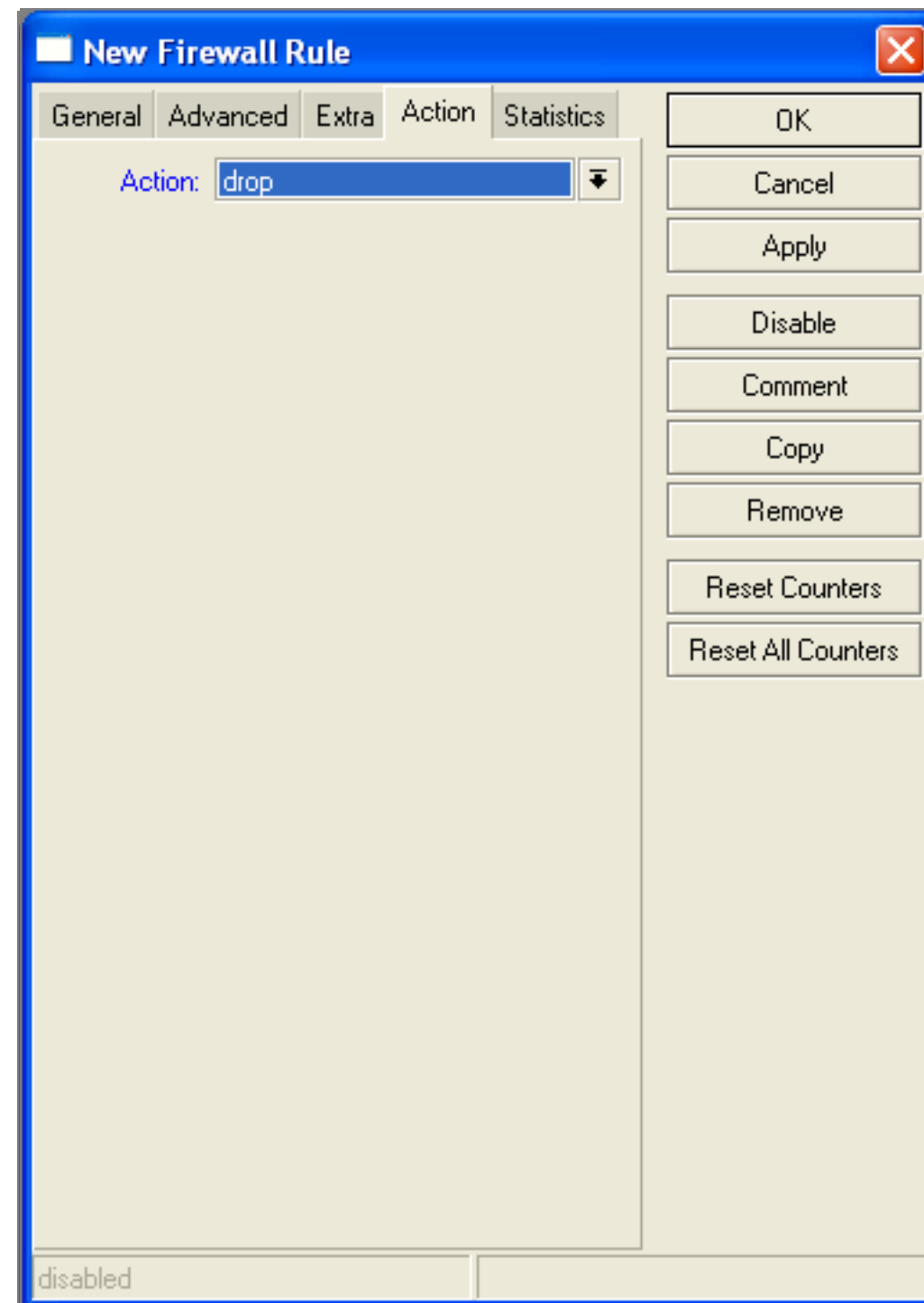
- Try to open www.mikrotik.com
- Try to open <http://192.168.X.254>
- Router web page works because drop rule is for **chain=forward** traffic

List of well-known ports

Port	Protocol	Service
80	TCP	WWW, HTTP
22	TCP	SSH
23	TCP	Telnet
53	TCP/UDP	DNS
21,20	TCP	FTP
8291	TCP	Winbox
123	UDP	NTP
443	TCP	HTTPS, SSL
5678	UDP	MNDP
8080	TCP	MikroTik Proxy
20561	UDP	MAC-Winbox
/1	ICMP	Pings

Forward

Create a rule that
will block client's
p2p traffic



Firewall Log

- Let's log client pings to the router
- Log rule should be added before other **action**

Firewall								
Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols								
+ - [check] [x] [icon] [icon] [00] Reset Counters [00] Reset All Counters								
#	Action	Chain	Protocol	In. Inter...	Out. Int...	Bytes	Packets	
0	log	input	1 (icmp)			4.9 KiB	80	

New Firewall Rule

General

Advanced

Extra

Action

Statistics

Action: log

Log Prefix: ICMP

OK

Cancel

Apply

Disable

Comment

Copy

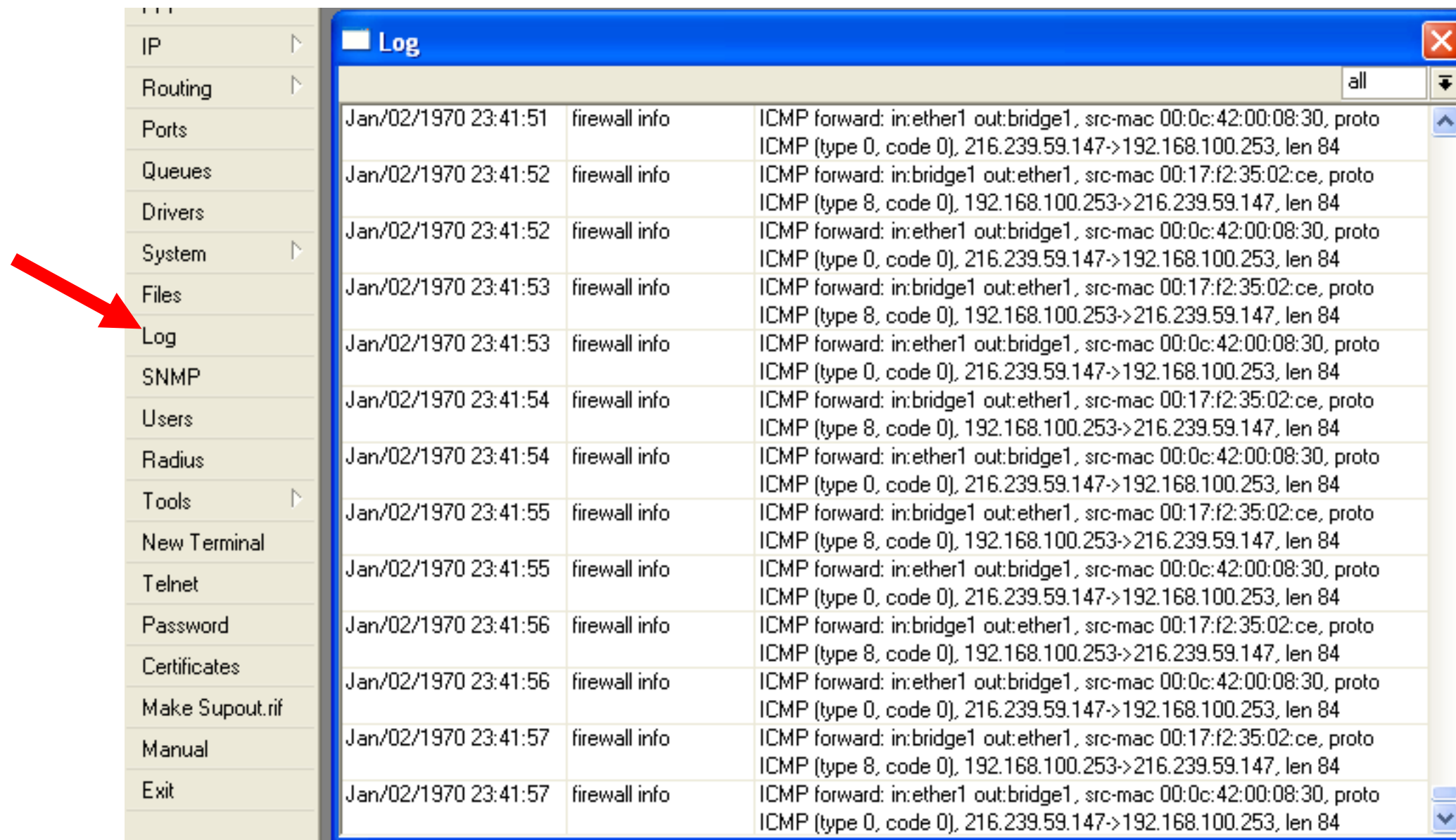
Remove

Reset Counters

Reset All Counters

disabled

Firewall Log



The screenshot shows a network configuration interface with a sidebar on the left and a main window titled 'Log'. The sidebar contains various system settings, and the 'Log' option is highlighted with a red arrow. The main window displays a table of firewall log entries.

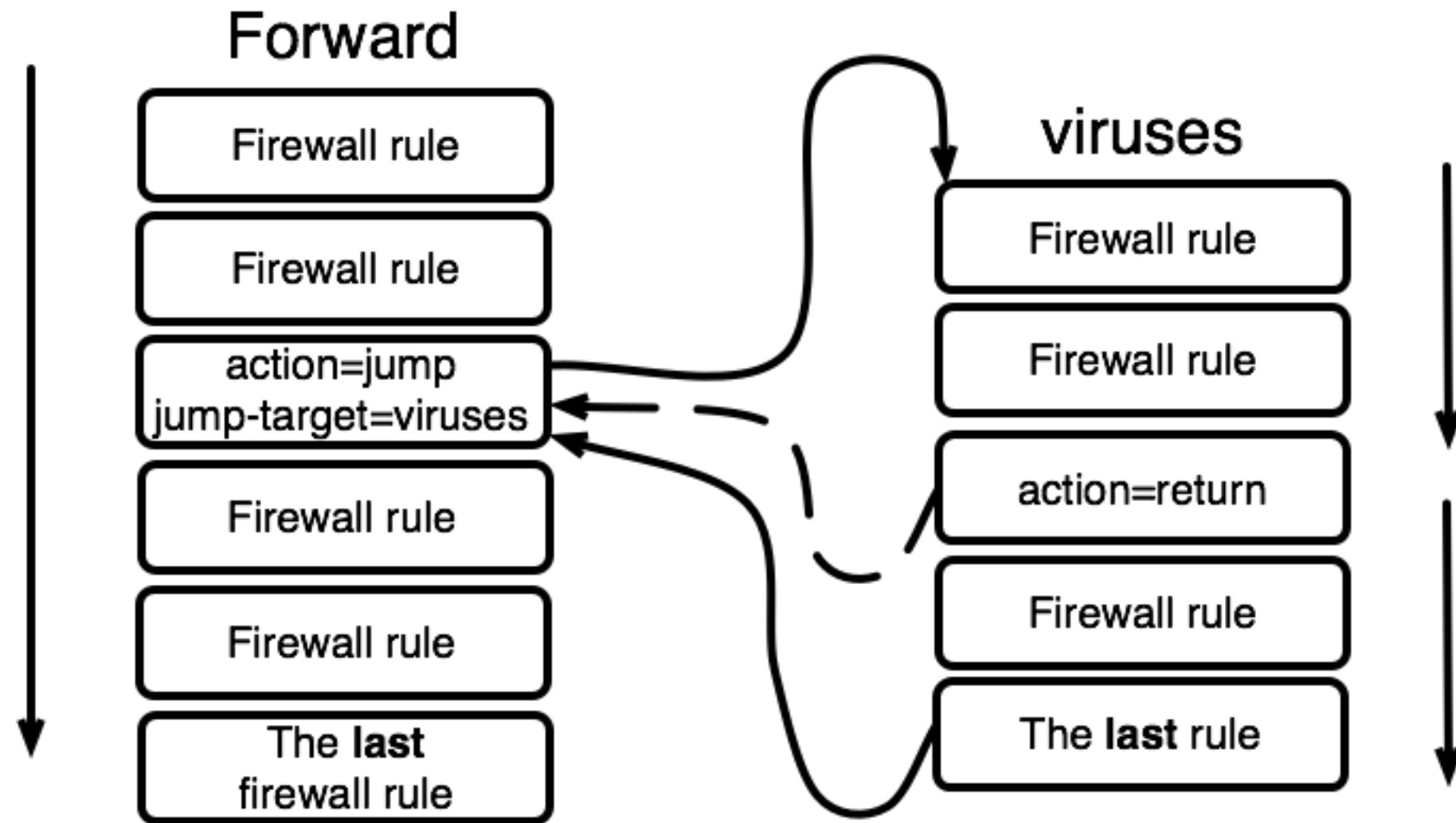
Time	Event	Details
Jan/02/1970 23:41:51	firewall info	ICMP forward: in:ether1 out:bridge1, src-mac 00:0c:42:00:08:30, proto ICMP (type 0, code 0), 216.239.59.147->192.168.100.253, len 84
Jan/02/1970 23:41:52	firewall info	ICMP forward: in:bridge1 out:ether1, src-mac 00:17:f2:35:02:ce, proto ICMP (type 8, code 0), 192.168.100.253->216.239.59.147, len 84
Jan/02/1970 23:41:52	firewall info	ICMP forward: in:ether1 out:bridge1, src-mac 00:0c:42:00:08:30, proto ICMP (type 0, code 0), 216.239.59.147->192.168.100.253, len 84
Jan/02/1970 23:41:53	firewall info	ICMP forward: in:bridge1 out:ether1, src-mac 00:17:f2:35:02:ce, proto ICMP (type 8, code 0), 192.168.100.253->216.239.59.147, len 84
Jan/02/1970 23:41:53	firewall info	ICMP forward: in:ether1 out:bridge1, src-mac 00:0c:42:00:08:30, proto ICMP (type 0, code 0), 216.239.59.147->192.168.100.253, len 84
Jan/02/1970 23:41:54	firewall info	ICMP forward: in:bridge1 out:ether1, src-mac 00:17:f2:35:02:ce, proto ICMP (type 8, code 0), 192.168.100.253->216.239.59.147, len 84
Jan/02/1970 23:41:54	firewall info	ICMP forward: in:ether1 out:bridge1, src-mac 00:0c:42:00:08:30, proto ICMP (type 0, code 0), 216.239.59.147->192.168.100.253, len 84
Jan/02/1970 23:41:55	firewall info	ICMP forward: in:bridge1 out:ether1, src-mac 00:17:f2:35:02:ce, proto ICMP (type 8, code 0), 192.168.100.253->216.239.59.147, len 84
Jan/02/1970 23:41:55	firewall info	ICMP forward: in:ether1 out:bridge1, src-mac 00:0c:42:00:08:30, proto ICMP (type 0, code 0), 216.239.59.147->192.168.100.253, len 84
Jan/02/1970 23:41:56	firewall info	ICMP forward: in:bridge1 out:ether1, src-mac 00:17:f2:35:02:ce, proto ICMP (type 8, code 0), 192.168.100.253->216.239.59.147, len 84
Jan/02/1970 23:41:56	firewall info	ICMP forward: in:ether1 out:bridge1, src-mac 00:0c:42:00:08:30, proto ICMP (type 0, code 0), 216.239.59.147->192.168.100.253, len 84
Jan/02/1970 23:41:57	firewall info	ICMP forward: in:bridge1 out:ether1, src-mac 00:17:f2:35:02:ce, proto ICMP (type 8, code 0), 192.168.100.253->216.239.59.147, len 84
Jan/02/1970 23:41:57	firewall info	ICMP forward: in:ether1 out:bridge1, src-mac 00:0c:42:00:08:30, proto ICMP (type 0, code 0), 216.239.59.147->192.168.100.253, len 84

Firewall chains

- Except of the built-in chains (input, forward, output), custom chains can be created
- Make firewall structure more simple
- Decrease load of the router

Firewall chains in Action

- Sequence of the firewall custom chains
- Custom chains can be for viruses, TCP, UDP protocols, etc.



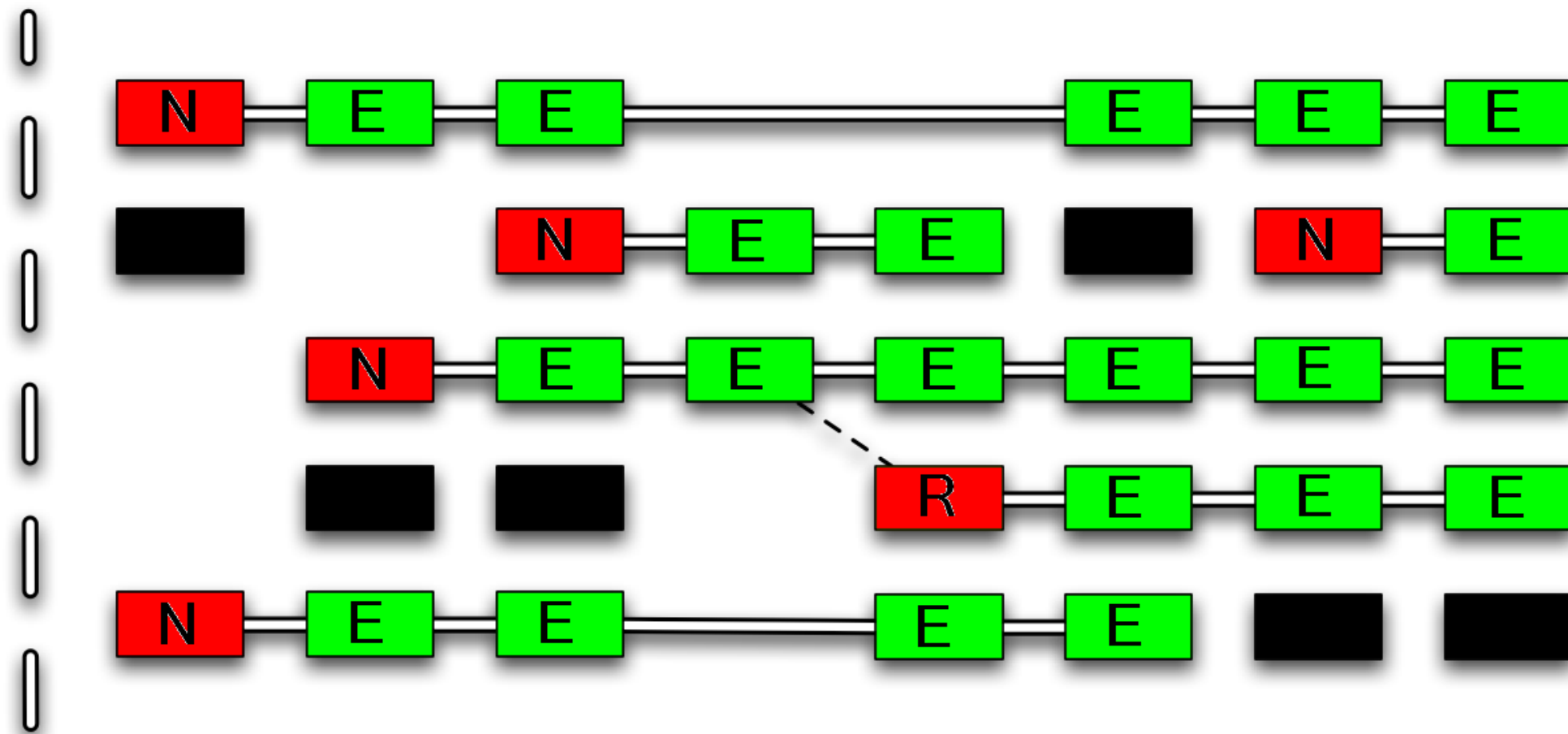
Firewall chain Lab

LAB

- Download viruses.rsc from router (access by FTP)
- Export the configuration by import command
- Check the firewall

Connections

Firewall



invalid

N new

E established

R related

Connection State

- Advise, drop invalid connections
- Firewall should proceed only new packets, it is recommended to exclude other types of states
- Filter rules have the “connection state” matcher for this purpose

Connection State

- Add rule to drop invalid packets
- Add rule to accept established packets
- Add rule to accept related packets
- Let Firewall to work with **new** packets **only**

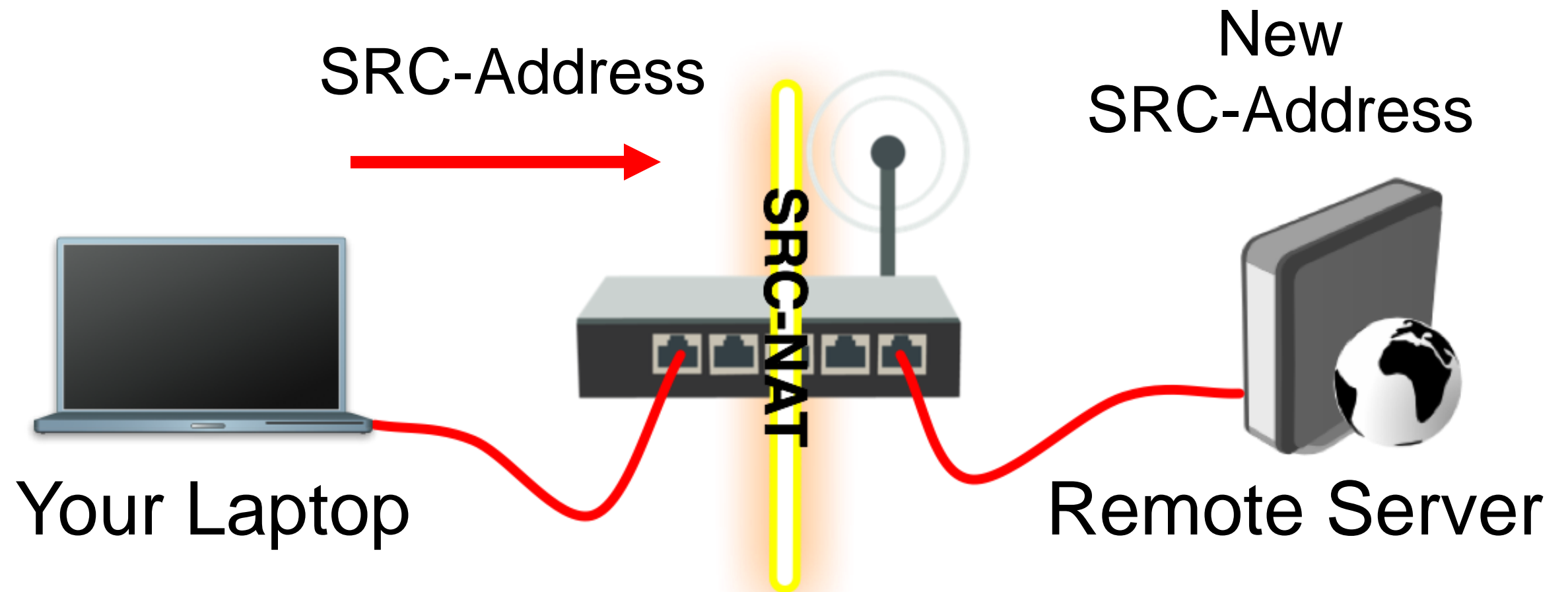
Summary

Network Address Translation

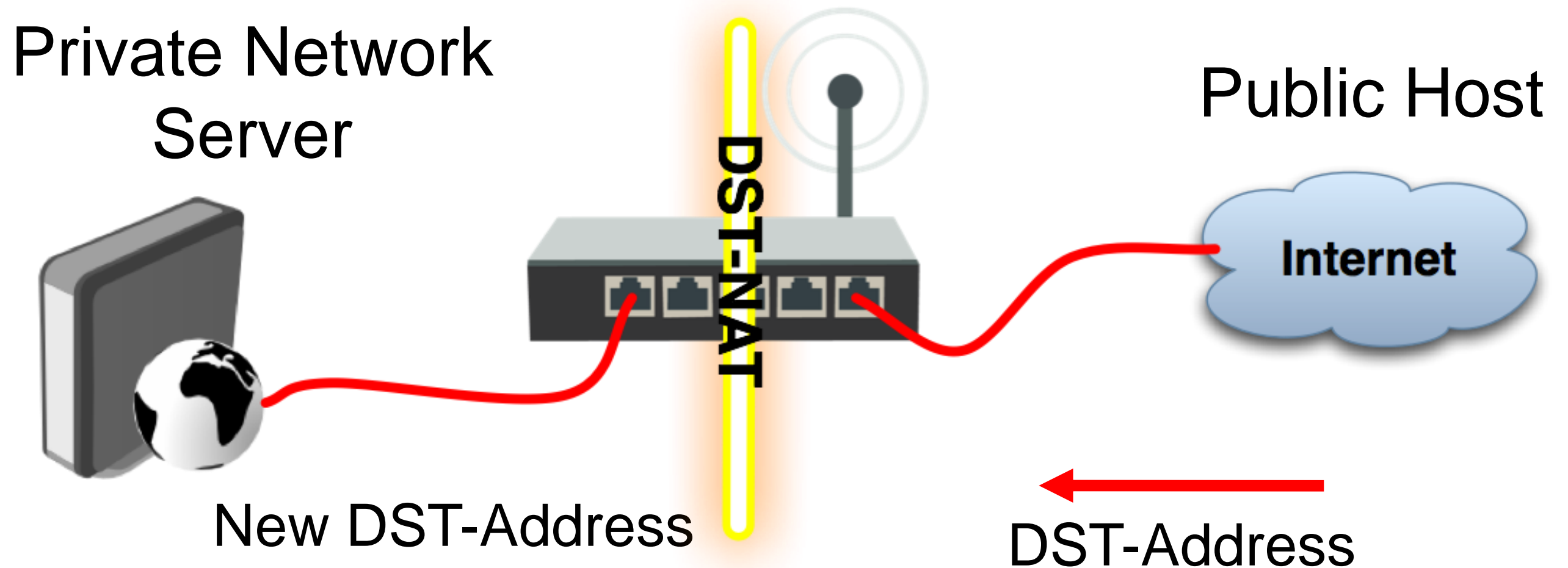
NAT

- Router is able to change **Source** or **Destination** address of packets flowing through it
- This process is called **src-nat** or **dst-nat**

SRC-NAT



DST-NAT



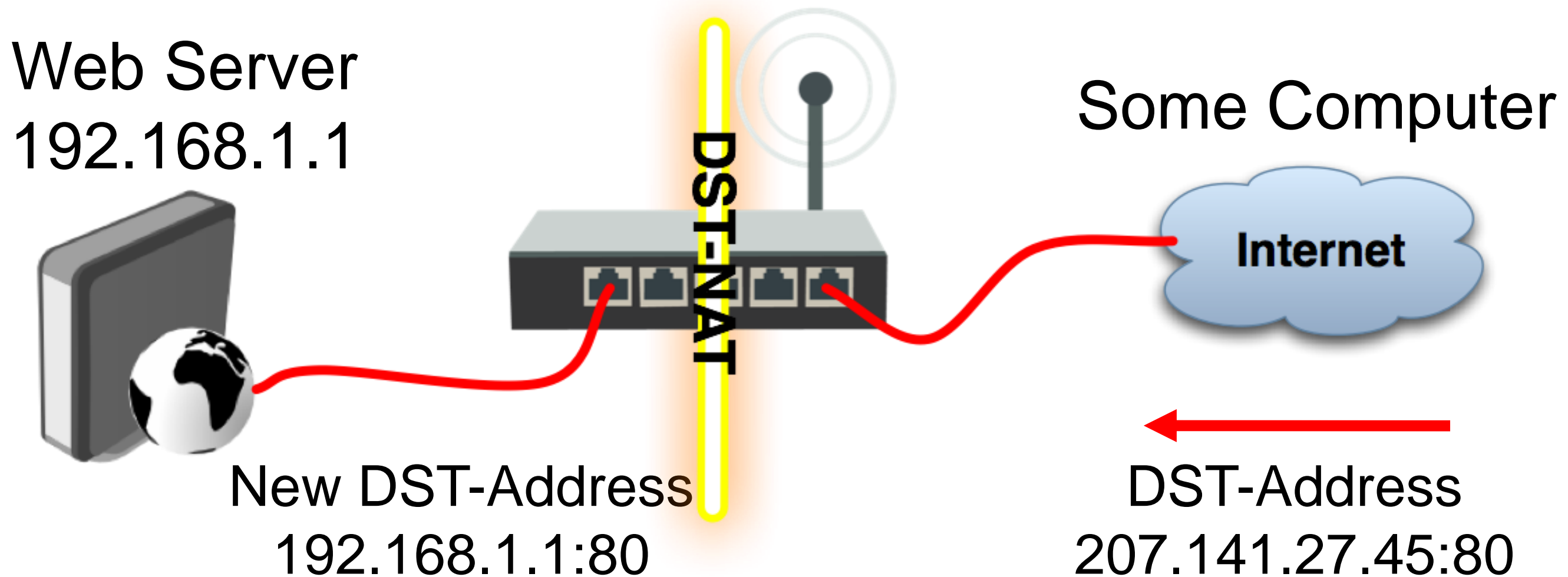
NAT Chains

- To achieve these scenarios you have to order your NAT rules in appropriate chains: **dstnat** or **srcnat**
- NAT rules work on **IF-THEN** principle

DST-NAT

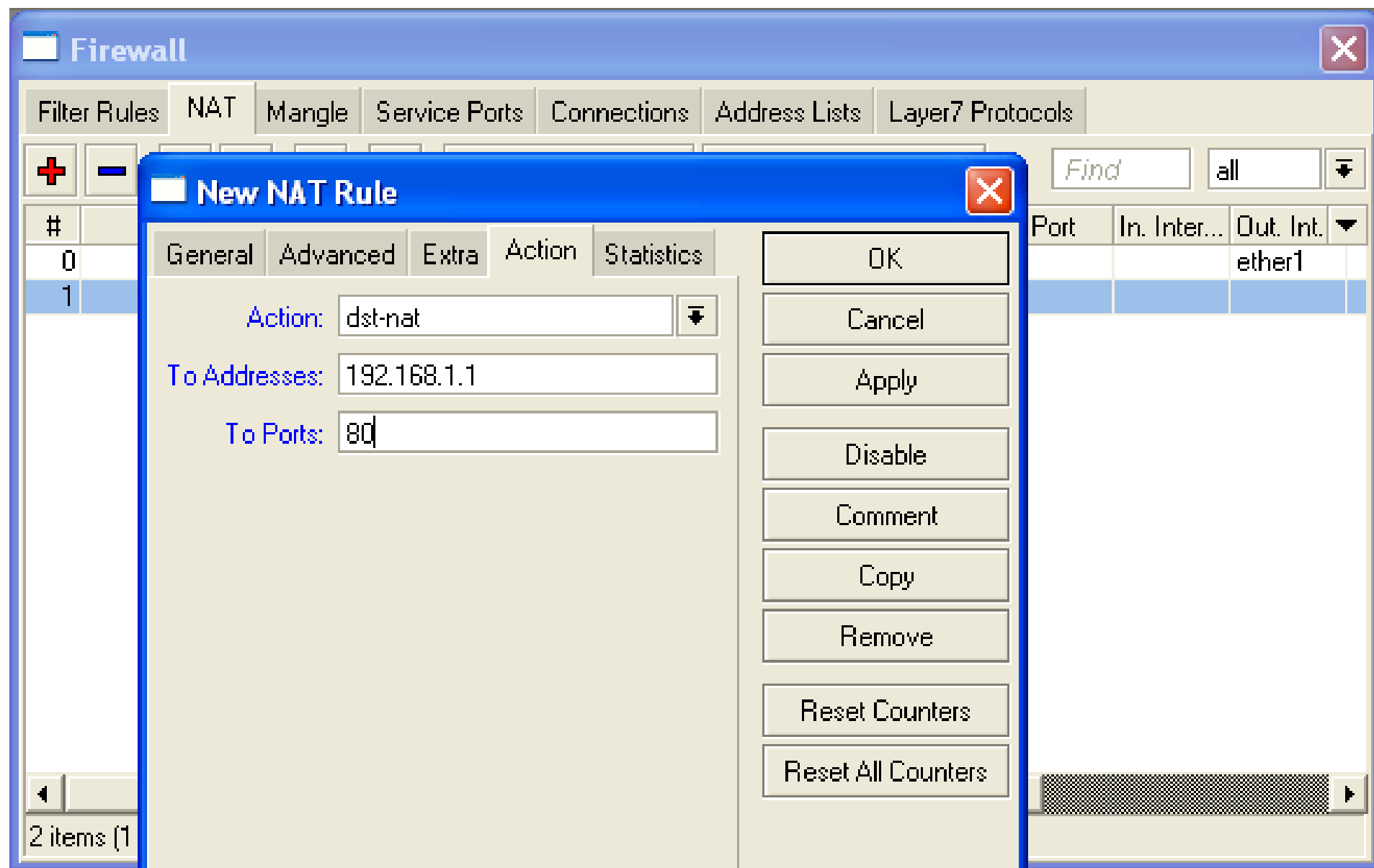
- DST-NAT changes packet's destination address and port
- It can be used to direct internet users to a server in your private network

DST-NAT Example



DST-NAT Example

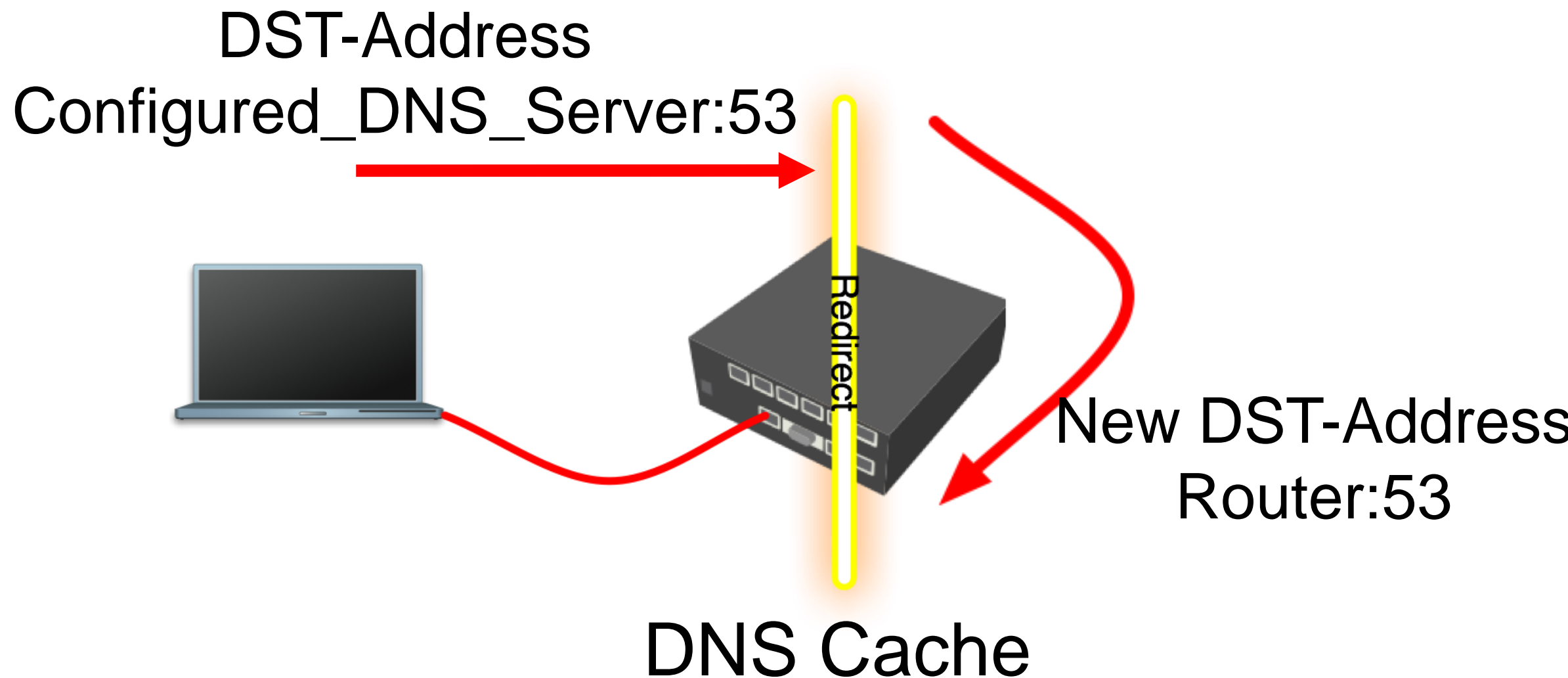
Create a rule to forward traffic to WEB server in private network



Redirect

- Special type of DST-NAT
- This action redirects packets to the router itself
- It can be used for proxying services (DNS, HTTP)

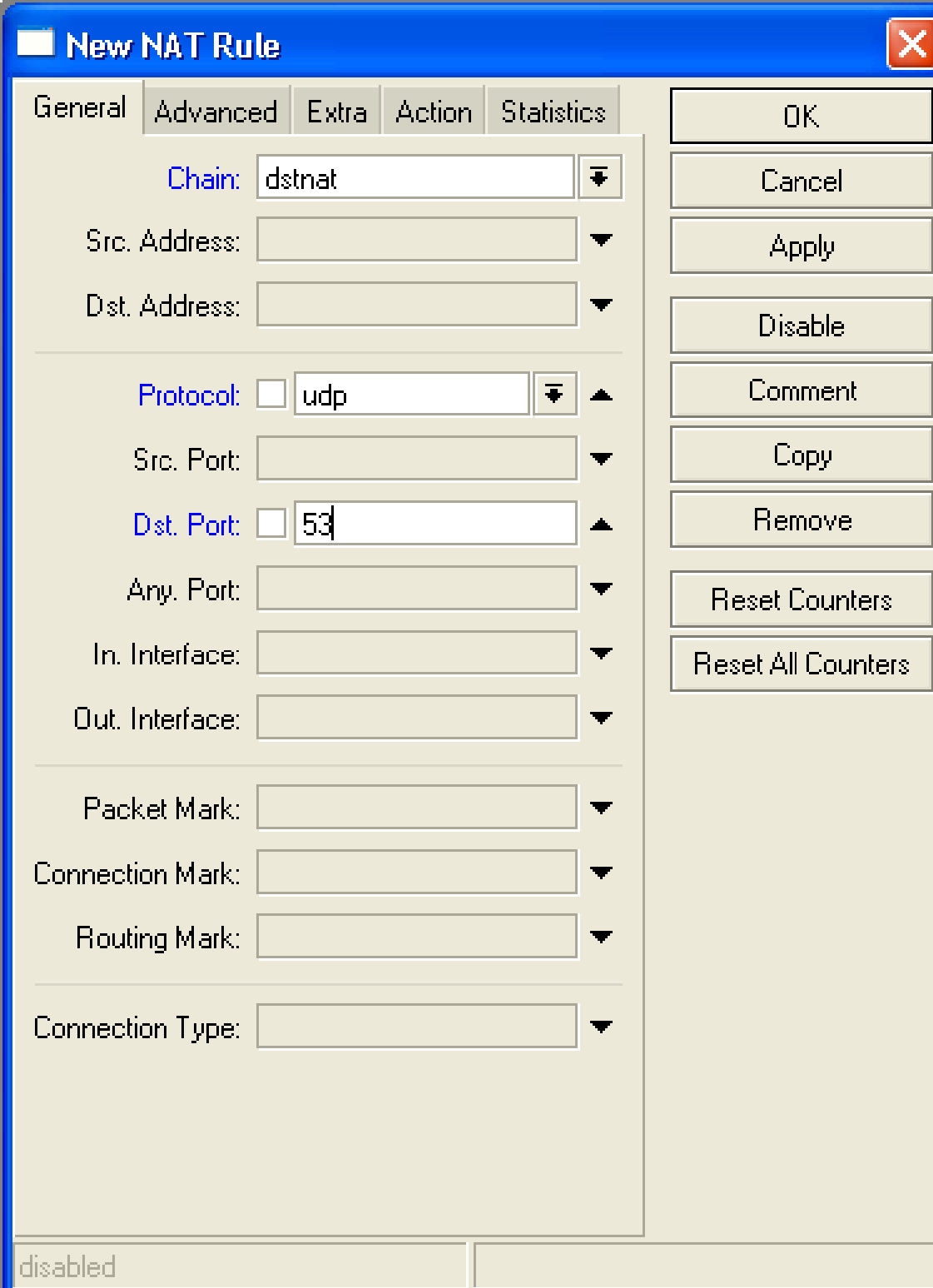
Redirect example



Redirect Example

LAB

- Let's make local users to use Router DNS cache
- Also make rule for **udp** protocol



The image shows a 'New NAT Rule' dialog box with the following fields and options:

- Chain:** dstnat
- Src. Address:** (empty)
- Dst. Address:** (empty)
- Protocol:** ☐ udp
- Src. Port:** (empty)
- Dst. Port:** ☐ 53
- Any. Port:** (empty)
- In. Interface:** (empty)
- Out. Interface:** (empty)
- Packet Mark:** (empty)
- Connection Mark:** (empty)
- Routing Mark:** (empty)
- Connection Type:** (empty)

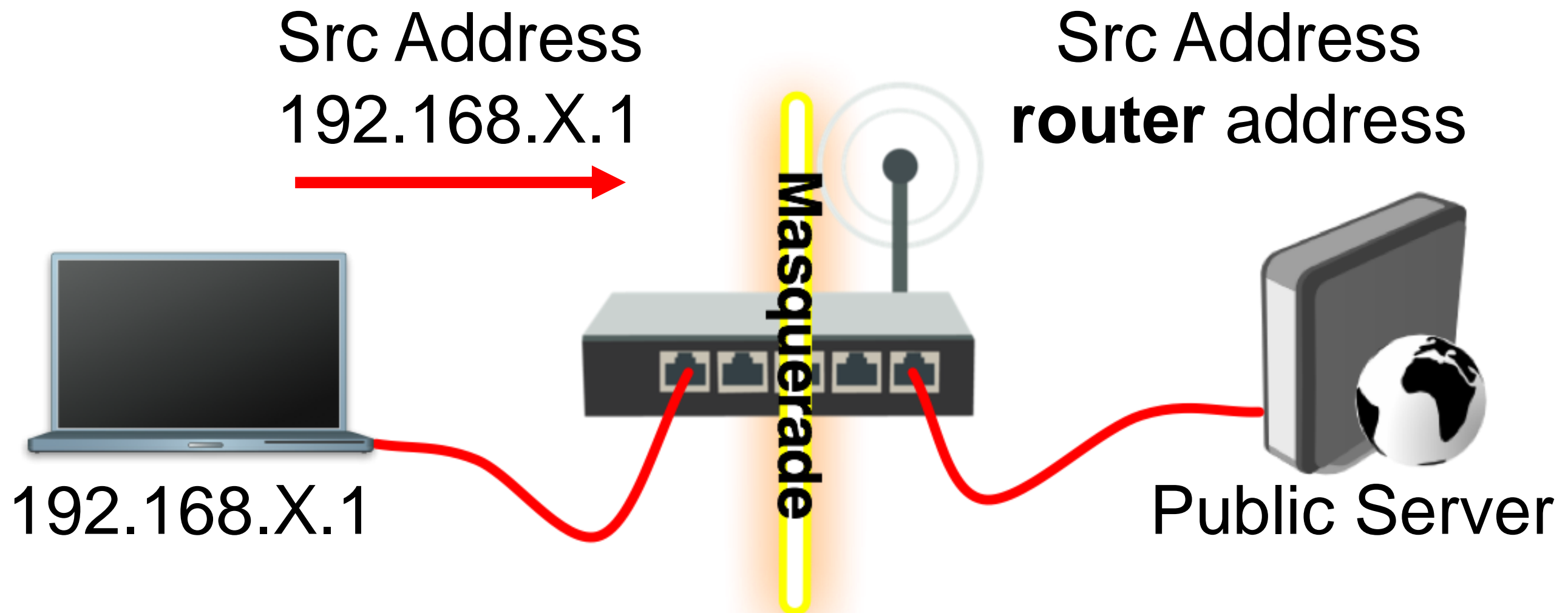
Buttons on the right: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, Reset All Counters.

At the bottom left, the status is 'disabled'.

SRC-NAT

- SRC-NAT changes packet's source address
- You can use it to connect private network to the Internet through public IP address
- **Masquerade** is one type of SRC-NAT

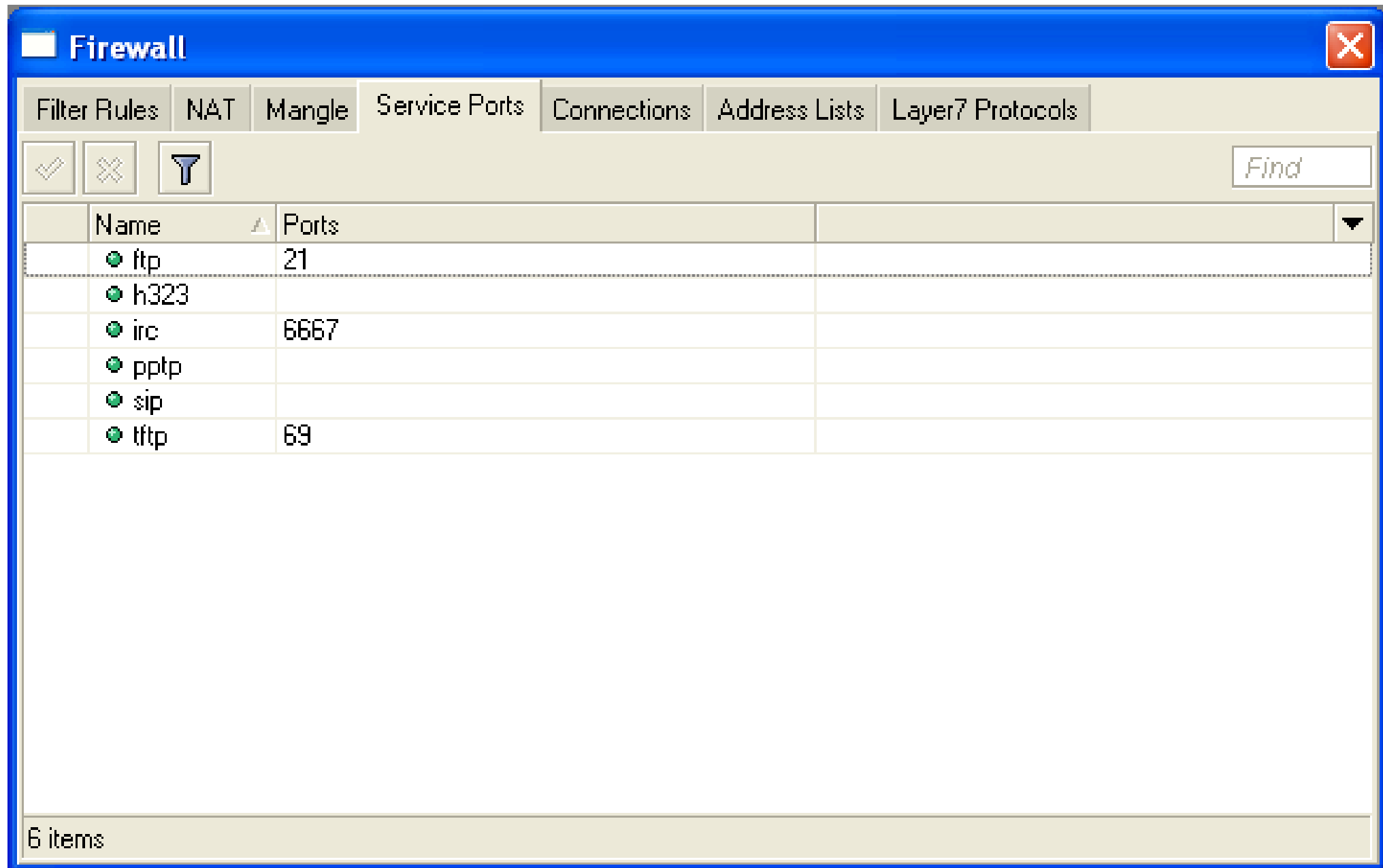
Masquerade



SRC-NAT Limitations

- Connecting to internal servers from outside is not possible (DST-NAT needed)
- Some protocols require NAT helpers to work correctly

NAT Helpers



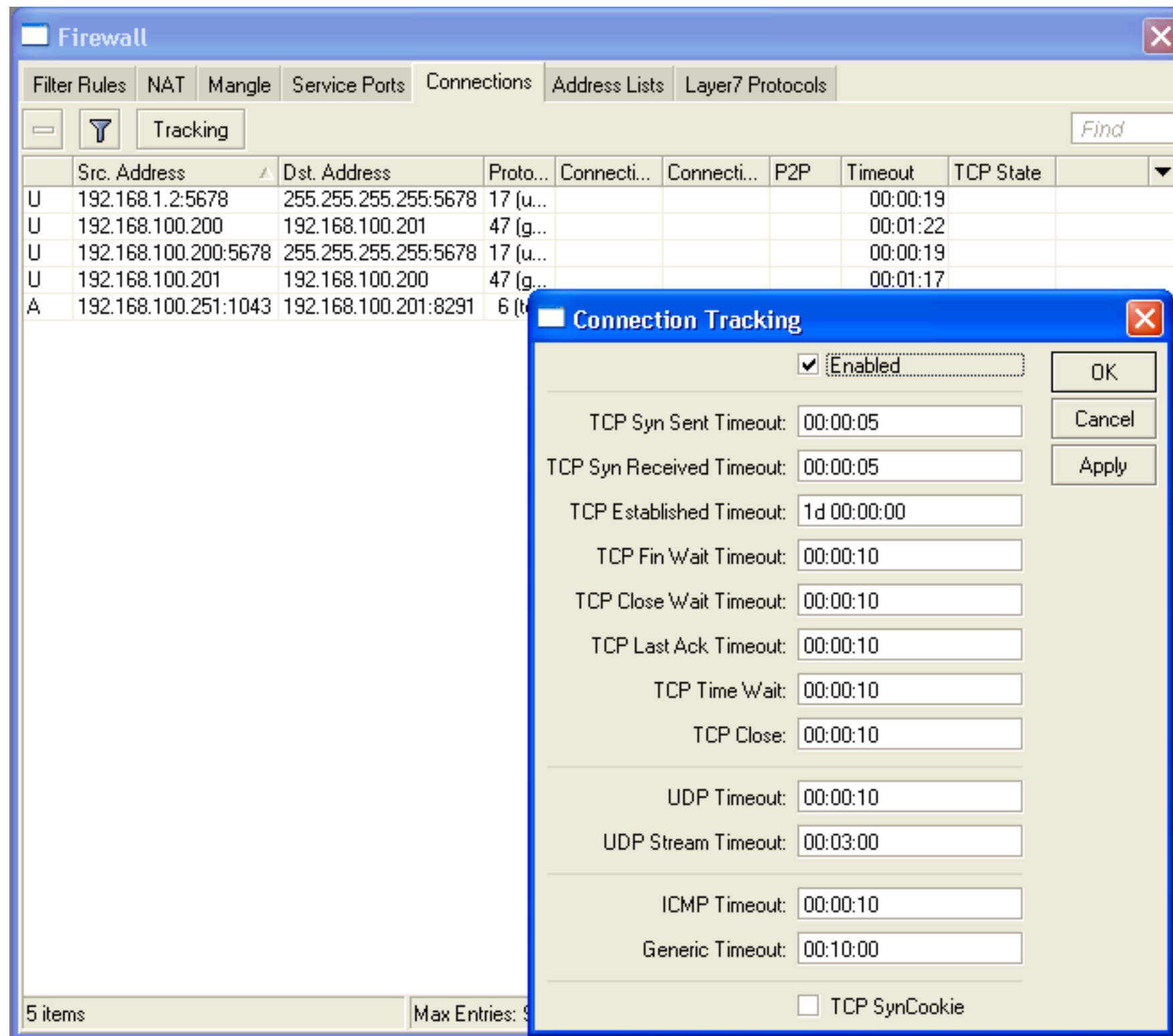
Firewall Tips

- Add comments to your rules
- Use Connection Tracking or Torch

Connection Tracking

- Connection tracking manages information about all active connections.
- It should be enabled for Filter and NAT

Connection Tracking



Torch

The screenshot shows the Torch network monitoring tool. The left sidebar contains a 'Tools' menu with the following options: New Terminal, Telnet, Password, Certificates, Make Supout.tif, Manual, Exit, Ping, Traceroute, Bandwidth Test, BTest Server, Traffic Monitor, Packet Sniffer, Torch, MAC Server, Graphing, Email, IP Scan, Ping Speed, Flood Ping, and Netwatch. The main window is titled 'Torch (running)' and has a blue title bar. It contains two tabs: 'Basic' and 'Filters'. The 'Basic' tab is active and shows the following configuration: Interface: ether3, Entry Timeout: 00:00:03 s. The 'Filters' tab is also visible and shows: Src. Address: 0.0.0.0/0, Dst. Address: 0.0.0.0/0, Protocol: any, Port: any, and VLAN Id: any. On the right side of the main window, there are three buttons: Start, Stop, and Close. Below the configuration fields, there is a 'Find' search bar. At the bottom of the window, there is a table displaying traffic statistics.

	Src. Address	Dst. Address	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...	
	192.168.100.251	192.168.100.201	24.7 kbps	6.7 kbps	8	9	
	192.168.100.200	192.168.100.201	0 bps	184 bps	0	0	

Detailed actual traffic report for interface

Firewall Actions

- Accept
- Drop
- Reject
- Tarpit
- log
- add-src-to-address-list(dst)
- Jump, Return
- Passthrough

NAT Actions

- Accept
- DST-NAT/SRC-NAT
- Redirect
- Masquerade
- Netmap

Summary

Bandwidth Limit

Simple Queue

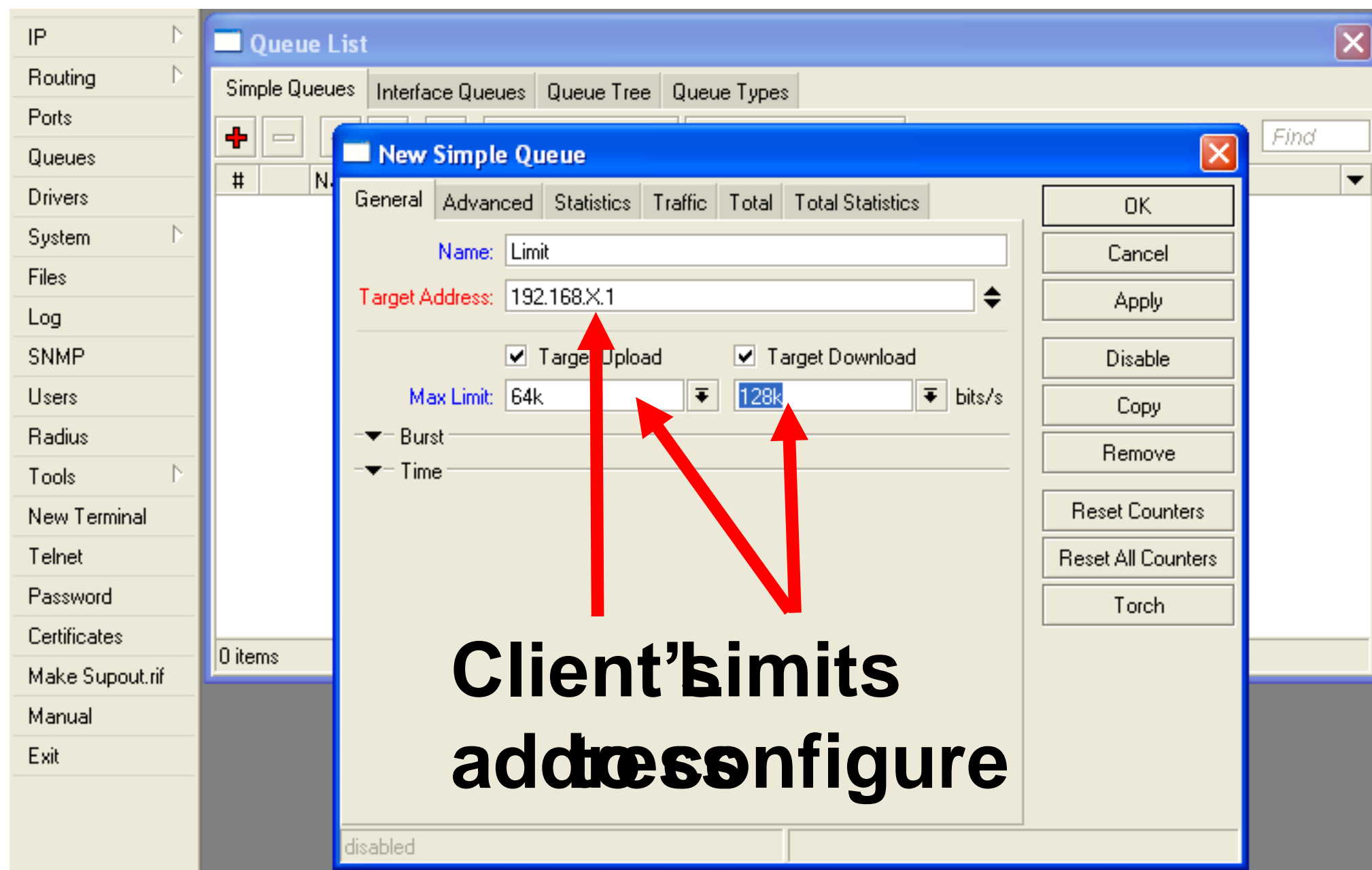
- The easiest way to limit bandwidth:
 - client download
 - client upload
 - client aggregate, download+upload

Simple Queue

- You must use **Target-Address** for Simple Queue
- Rule order is important for queue rules

Simple Queue

- Let's create limitation for your laptop
- 64k Upload, 128k Download



Simple Queue

- Check your limits
- Torch is showing bandwidth rate

Using Torch

- Select local network interface
- See actual bandwidth

Torch

Basic

Interface: ether1

Entry Timeout: 00:00:03 s

Collect

☒ Src. Address ☐ Protocol

☐ Dst. Address ☐ Port

Filters

Src. Address: 192.168.X.1

Dst. Address: 0.0.0.0/0

Protocol: any

Port: any

Find

Src. Address	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
10.5.8.8	917 bps	0 bps	0	0
10.5.8.140	0 bps	254 bps	0	0
10.5.8.51	0 bps	237 bps	0	0
192.168.1.10	0 bps	122 bps	0	0
84.215.125.239	538 bps	1634 bps	2	1

5 items Total Tx: 2.4 kbps Total Rx: 2.2 kbps Total Tx Packet: 2 Total Rx Packet: 1

Set the interface address

Specific Server Limit

LAB

- Let's create bandwidth limit to MikroTik.com
- DST-address is used for this
- Rules order is important

New Simple Queue

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

P2P:

Packet Marks:

Dst. Address:

Interface:

Target Upload: Limit At: bits/s

Target Download: bits/s

Queue Type:

Parent:

Priority:

disabled

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

Specific Server Limit

LAB

- Ping
www.mikrotik.com
- Put MikroTik address to DST-address
- MikroTik address can be used as Target-address too

New Simple Queue

General Advanced Statistics Traffic Total Total Statistics

P2P:

Packet Marks:

Dst. Address:

Interface:

Target Upload Limit At: bits/s

Target Download Limit At: bits/s

Queue Type:

Parent:

Priority:

MikroTik.com Address

disabled

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

Specific Server Limit

LAB

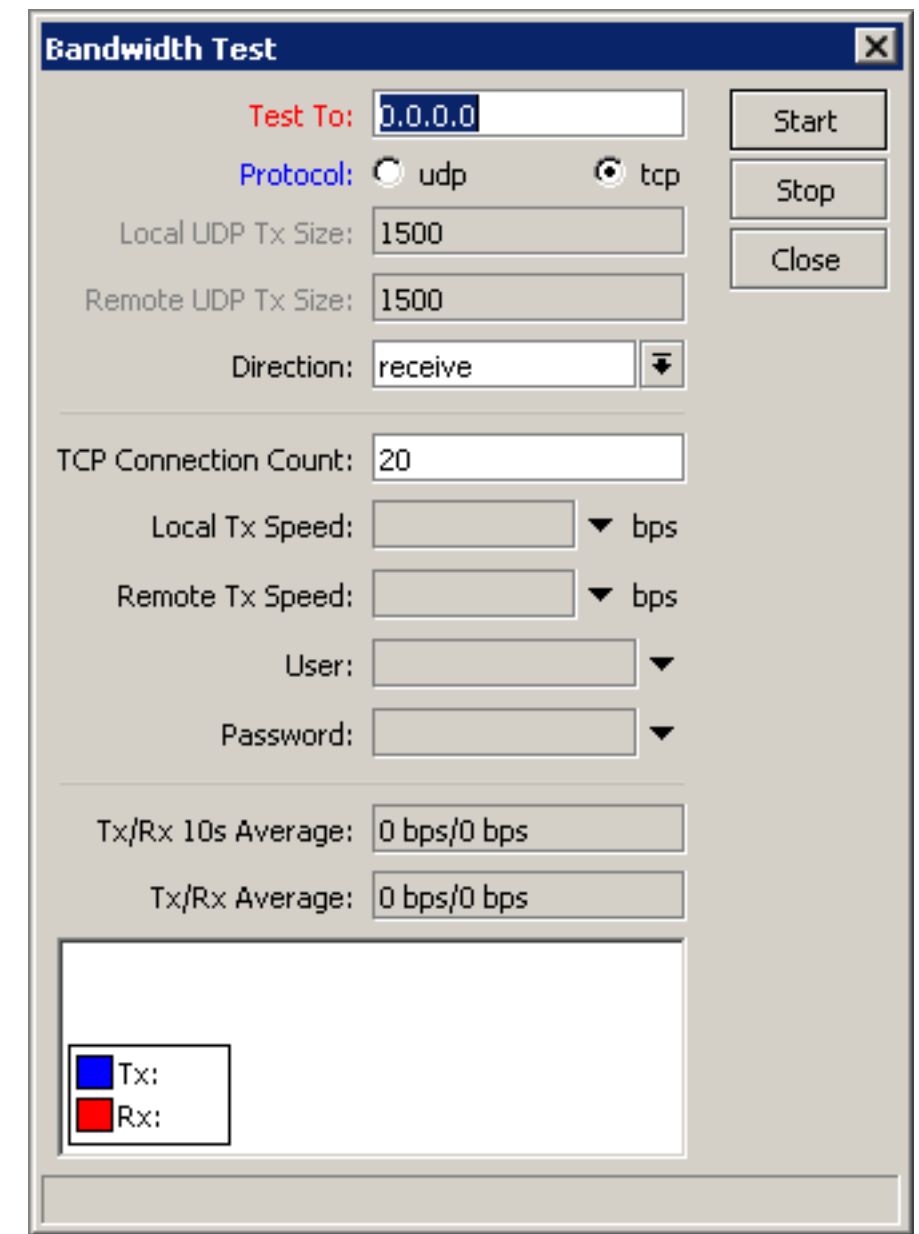
- DST-address is useful to set unlimited access to the local network resources
- Target-address and DST-addresses can be vice versa

Bandwidth Test Utility

- Bandwidth test can be used to monitor throughput to remote device
- Bandwidth test works between two MikroTik routers
- Bandwidth test utility available for Windows
- Bandwidth test is available on MikroTik.com

Bandwidth Test on Router

- Set **Test To** as testing address
- Select protocol
- TCP supports multiple connections
- Authentication might be required



The image shows a 'Bandwidth Test' configuration window. It includes fields for 'Test To' (0.0.0.0), 'Protocol' (tcp selected), 'Local UDP Tx Size' (1500), 'Remote UDP Tx Size' (1500), 'Direction' (receive), 'TCP Connection Count' (20), 'Local Tx Speed', 'Remote Tx Speed', 'User', and 'Password'. It also displays 'Tx/Rx 10s Average' and 'Tx/Rx Average' as 0 bps/0 bps. A legend at the bottom left indicates blue for Tx and red for Rx.

Field	Value
Test To	0.0.0.0
Protocol	tcp
Local UDP Tx Size	1500
Remote UDP Tx Size	1500
Direction	receive
TCP Connection Count	20
Local Tx Speed	
Remote Tx Speed	
User	
Password	
Tx/Rx 10s Average	0 bps/0 bps
Tx/Rx Average	0 bps/0 bps

Bandwidth Server

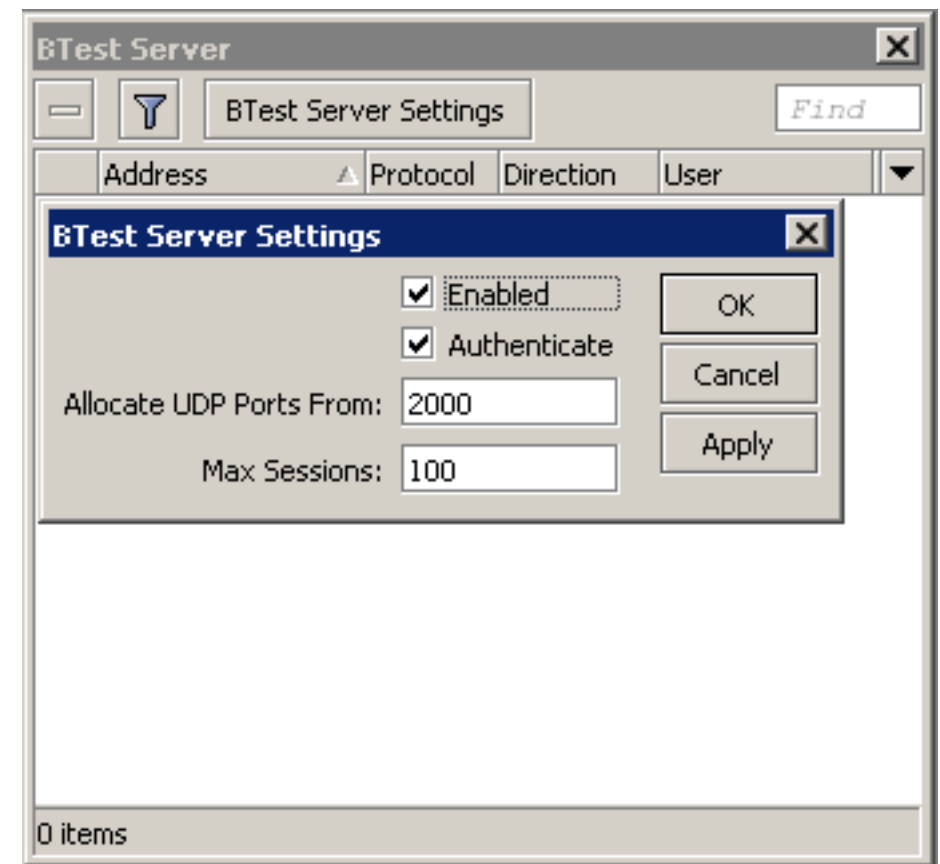
- Set **Test To** as testing address
- Select protocol
- TCP supports multiple connections
- Authentication might be required

The screenshot shows a window titled "Bandwidth Test" with a close button (X) in the top right corner. The window contains the following controls and fields:

- Test To:** A text field containing "0.0.0.0".
- Protocol:** Two radio buttons, "udp" and "tcp". The "tcp" button is selected.
- Local UDP Tx Size:** A text field containing "1500".
- Remote UDP Tx Size:** A text field containing "1500".
- Direction:** A dropdown menu showing "receive".
- TCP Connection Count:** A text field containing "20".
- Local Tx Speed:** A text field with a dropdown arrow, currently showing "bps".
- Remote Tx Speed:** A text field with a dropdown arrow, currently showing "bps".
- User:** A text field with a dropdown arrow.
- Password:** A text field with a dropdown arrow.
- Tx/Rx 10s Average:** A text field showing "0 bps/0 bps".
- Tx/Rx Average:** A text field showing "0 bps/0 bps".
- Start, Stop, Close buttons:** Three buttons stacked vertically on the right side of the window.
- Legend:** A small box at the bottom left containing a blue square labeled "Tx:" and a red square labeled "Rx:".

Bandwidth Test

- Server should be enabled
- It is advised to use enabled **Authenticate**



Traffic Priority

- Let's configure higher priority for queues
- Priority 1 is higher than 8
- There should be at least two priority

Simple Queue <Limit_Neighbor_Bandwidth>

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

P2P:

Packet Marks:

Dst. Address:

Interface:

Target Upload: Limit At: bits/s

Target Download: Limit At: bits/s

Queue Type:

Parent:

Priority:

Set Higher Priority

disabled

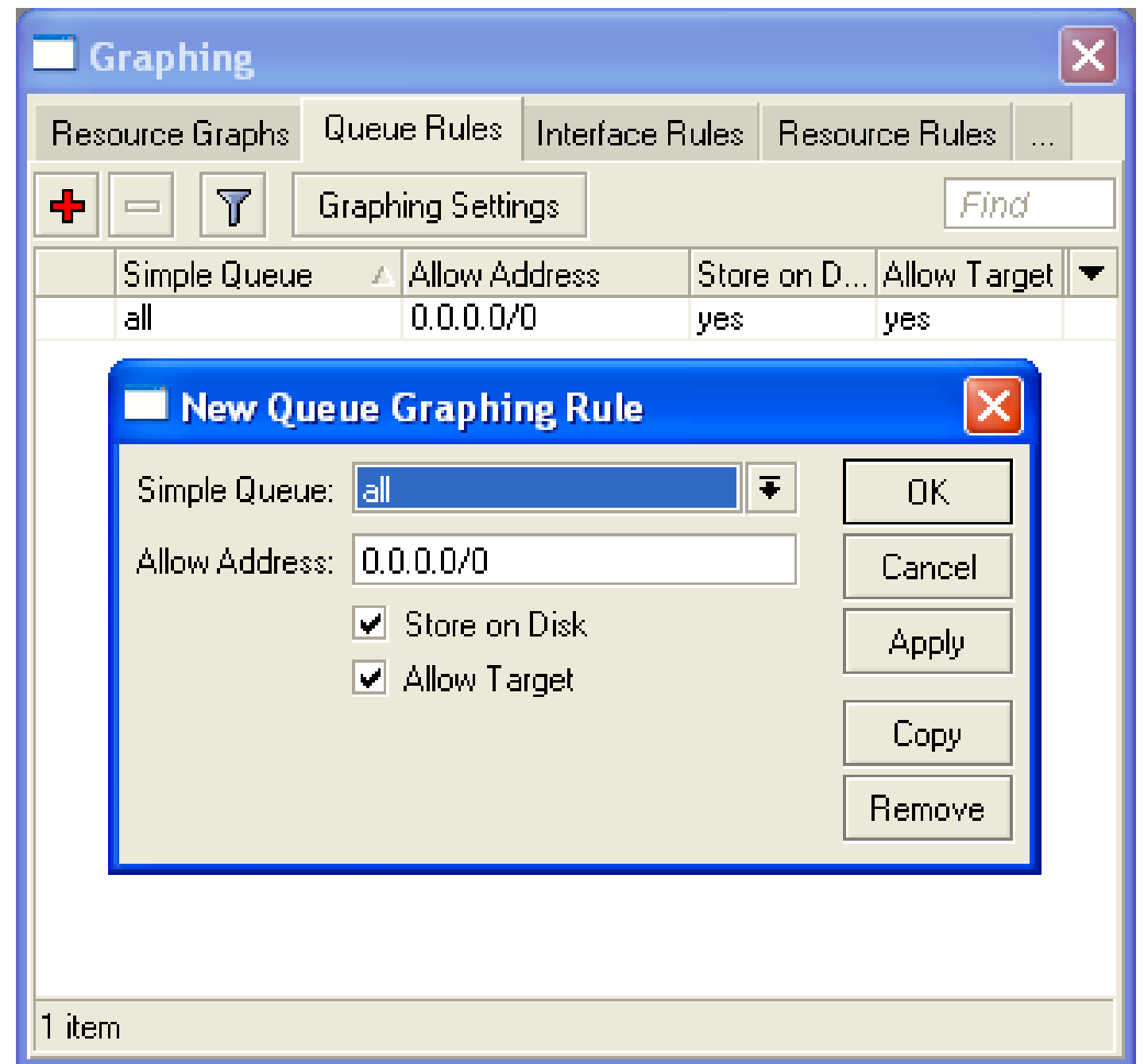
OK
Cancel
Apply
Disable
Copy
Remove
Reset Counters
Reset All Counters
Torch

Simple Queue Monitor

- It is possible to get **graph** for each queue simple rule
- Graphs show how much traffic is passed through queue

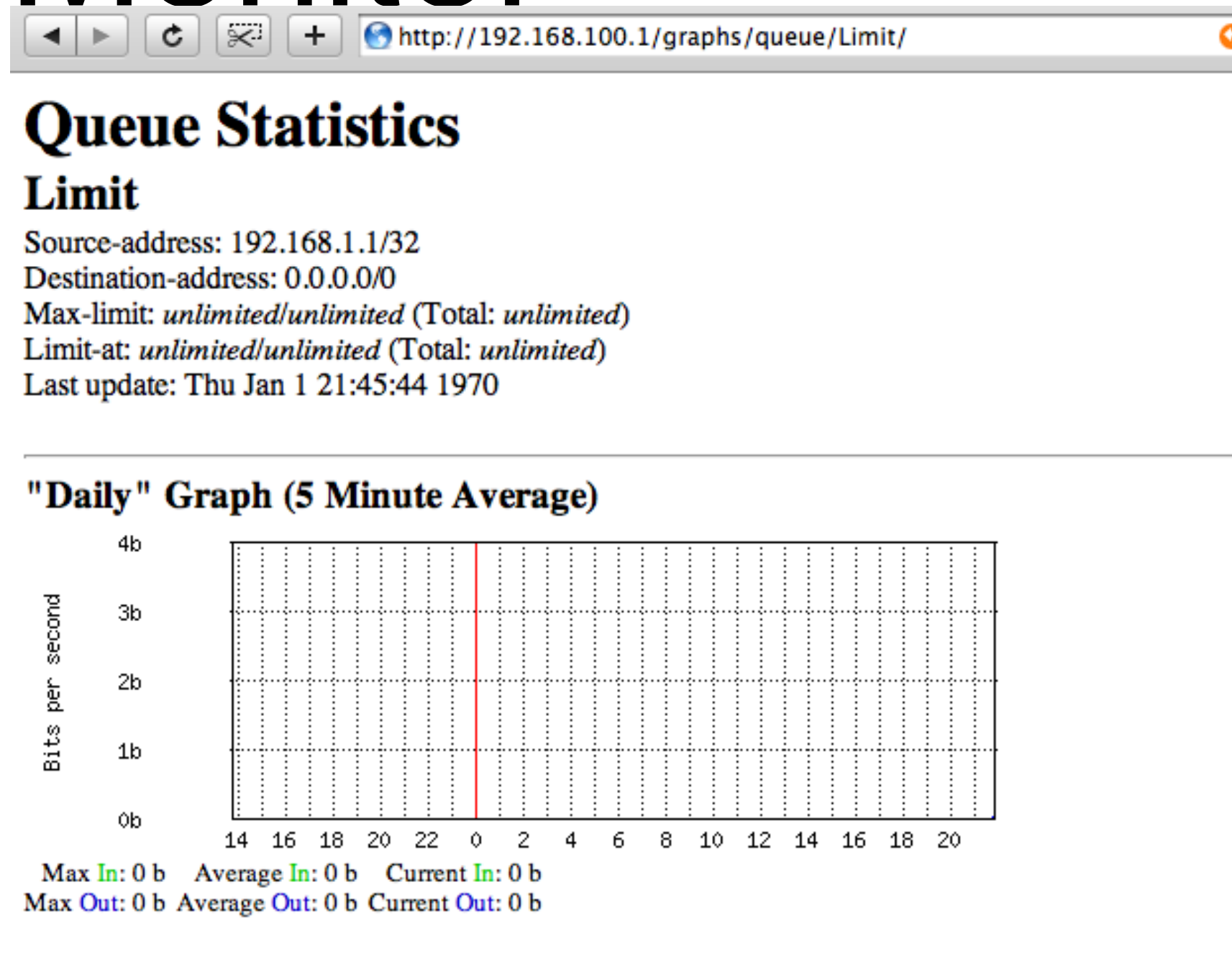
Simple Queue Monitor

Let's enable graphing for Queues



Simple Queue Monitor

- Graphs are available on WWW
- To view graphs
http://router_1_P
- You can give it to your customer



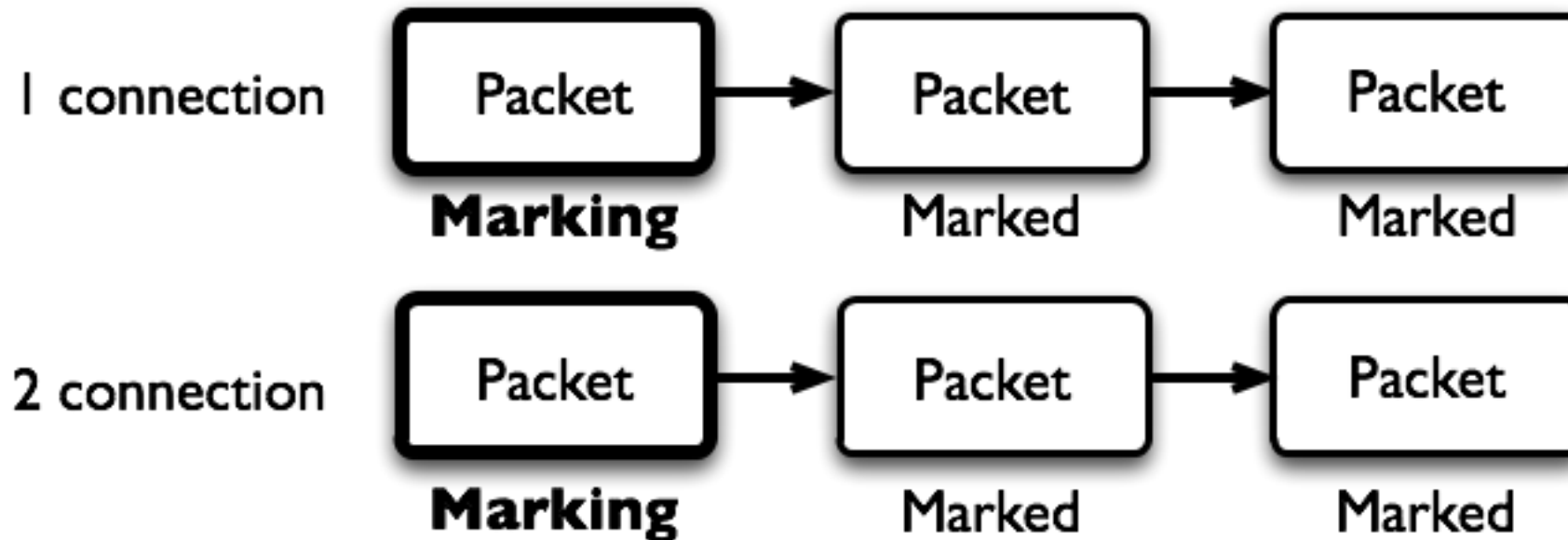
Advanced Queing

Mangle

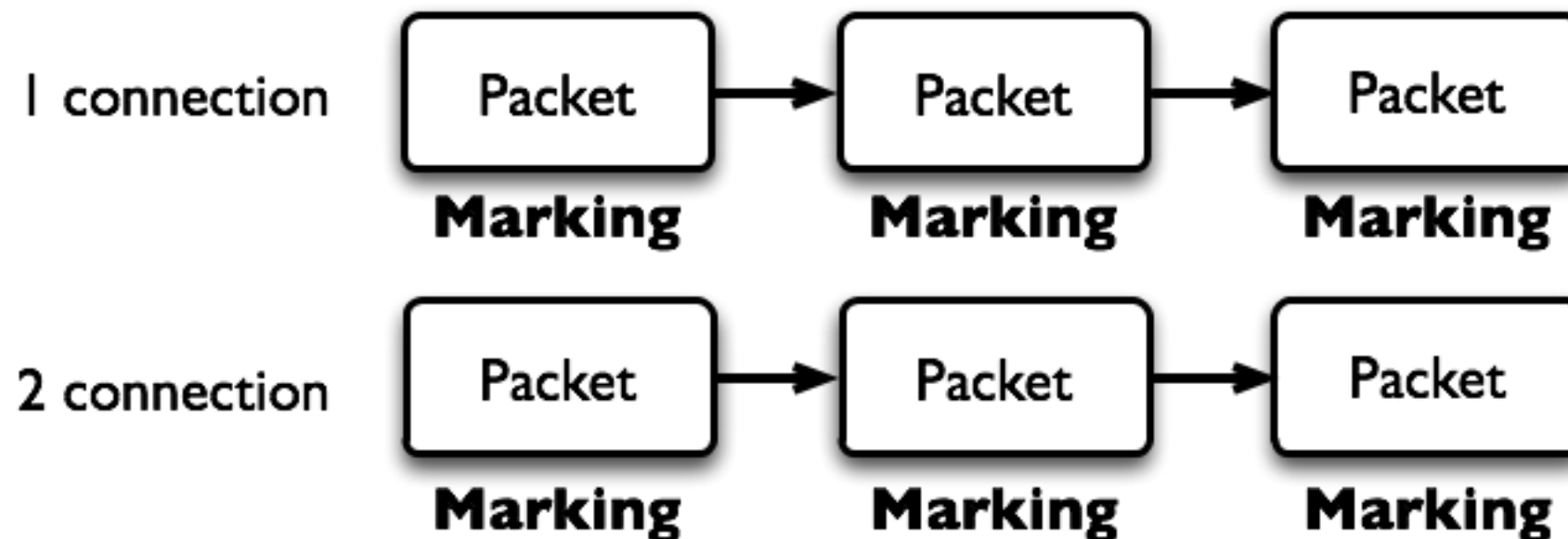
- Mangle is used to mark packets
- Separate different type of traffic
- Marks are active within the router
- Used for queue to set different limitation
- Mangle do not change packet structure (except DSCP, TTL specific actions)

Mangle Actions

Mark-Connection



Mark-Packet



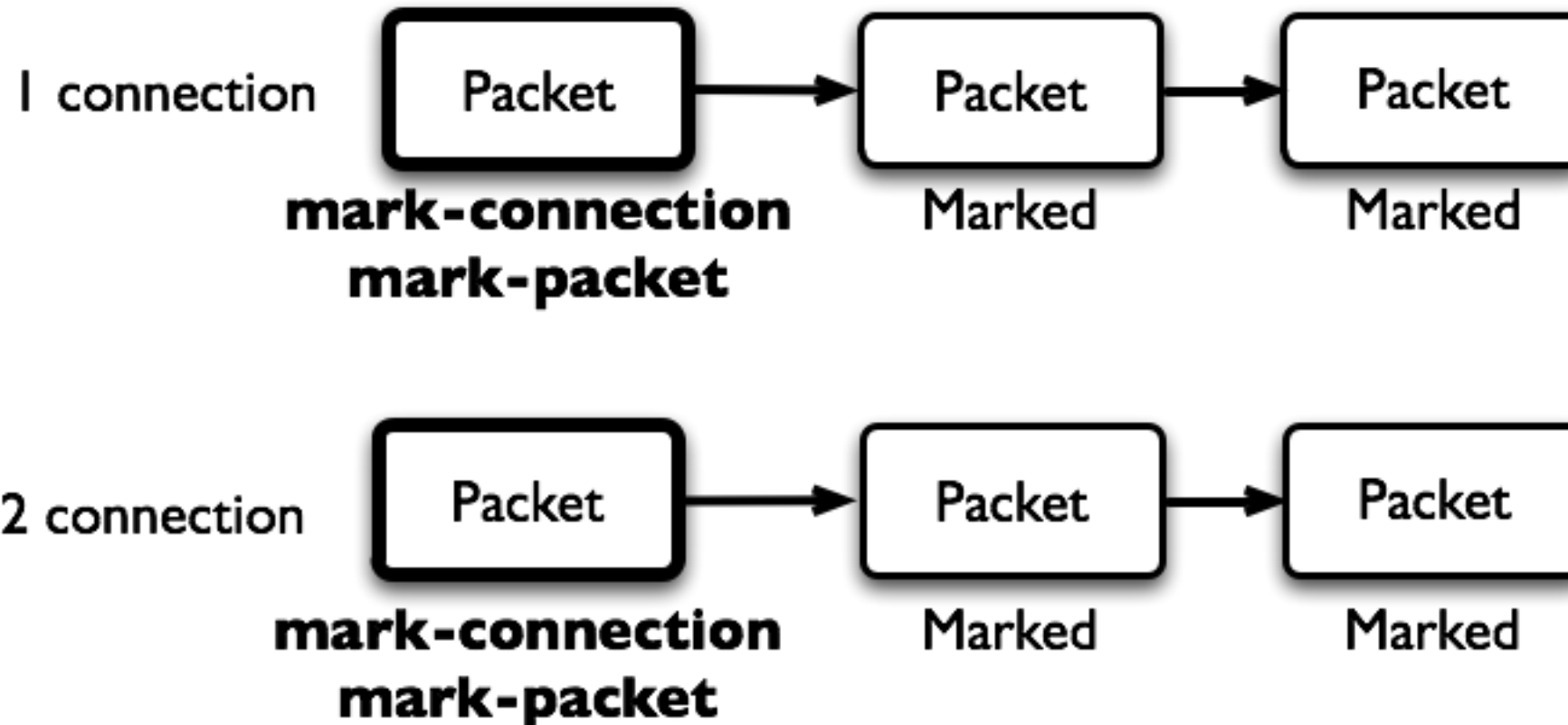
Mangle Actions

- **Mark-connection** uses connection tracking
- Information about new connection added to connection tracking table
- Mark-packet works with packet directly
- Router follows each packet to apply **mark-packet**

Optimal Mangle

- Queues have packet-mark option only

Combine Mark-Connection and Mark-Packet



Optimal Mangle

- Mark new connection with **mark-connection**
- Add **mark-packet** for every **mark-connection**

Mangle Example

- Imagine you have second client on the router network with 192.168.X.55 IP address
- Let's create two different marks (**Gold**, **Silver**), one for your computer and second for 192.168.X.55

Mark Connection

New Mangle Rule

General | Advanced | Extra | Action | Statistics

Chain: forward

Src. Address: ☐ 192.168.X.1

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

Any. Port:

P2P:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark:

Routing Mark:

Connection Type:

Connection State:

disabled

New Mangle Rule

General | Advanced | Extra | Action | Statistics

Action: mark connection

New Connection Mark: Mark User 1

☒ Passthrough

OK

Cancel

Apply

Disable

Comment

Copy

Remove

Reset Counters

Reset All Counters

disabled

Mark Packet

The image displays two side-by-side screenshots of the 'New Mangle Rule' configuration window, showing the 'General' and 'Action' tabs respectively.

Left Screenshot (General Tab):

- Chain:** forward
- Src. Address:**
- Dst. Address:**
- Protocol:**
- Src. Port:**
- Dst. Port:**
- Any. Port:**
- P2P:**
- In. Interface:**
- Out. Interface:**
- Packet Mark:**
- Connection Mark:** ☐ Mark User 1
- Routing Mark:**
- Connection Type:**
- Connection State:**

Right Screenshot (Action Tab):

- Action:** mark packet
- New Packet Mark:** User1
- ☒ Passthrough

Both windows show a 'disabled' status at the bottom. The right window includes a sidebar with buttons: OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, and Reset All Counters.

Mangle Example

LAB

- Add Marks for second user too
- There should be 4 mangle rules for two groups

Advanced Queuing

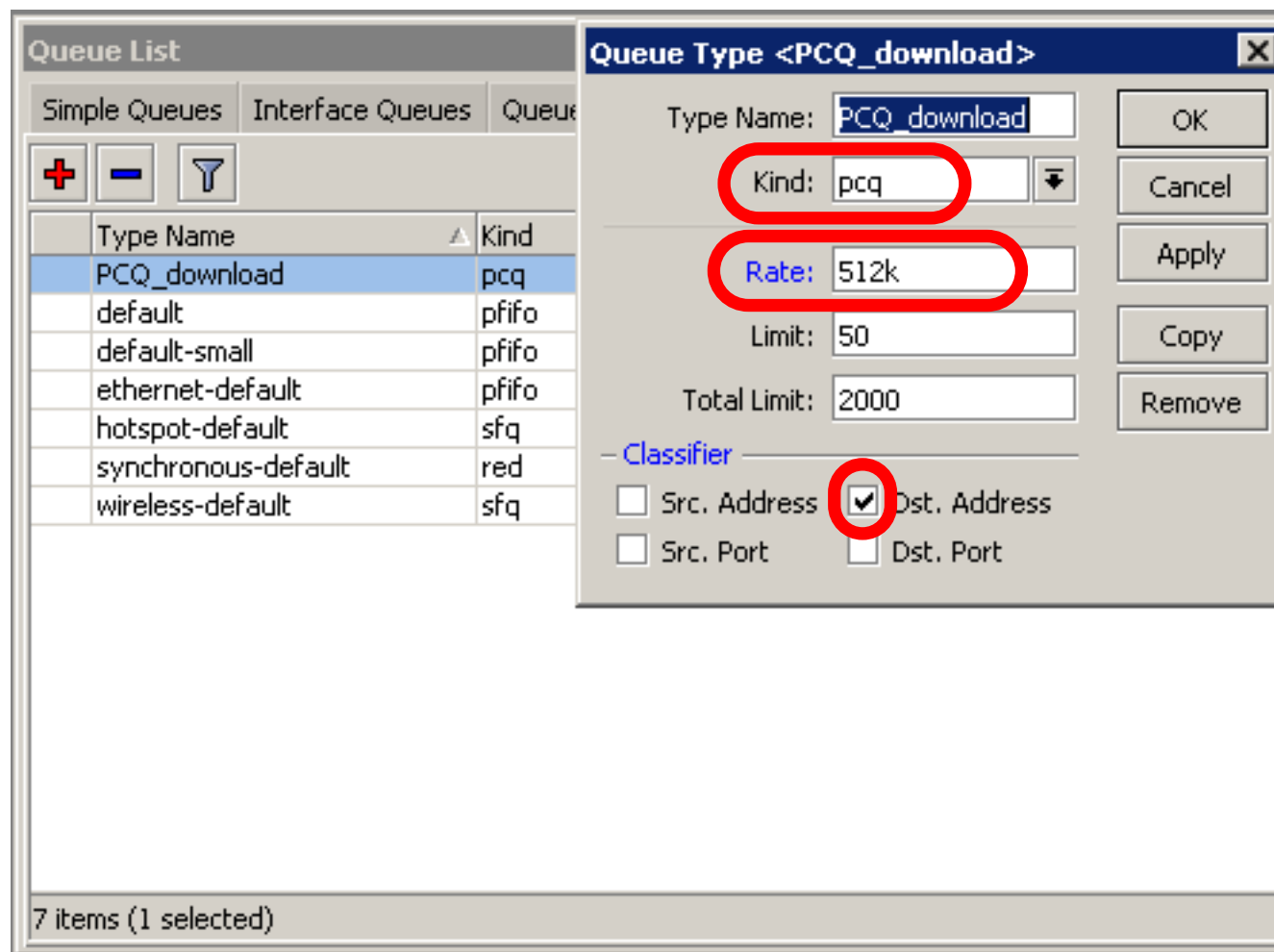
- Replace hundreds of queues with just few
- Set the same limit to any user
- Equalize available bandwidth between users

PCQ

- PCQ is advanced Queue type
- PCQ uses classifier to divide traffic (from client point of view; src-address is upload, dst-address is download)

PCQ, one limit to all

- PCQ allows to set one limit to all users with one queue



One limit to all

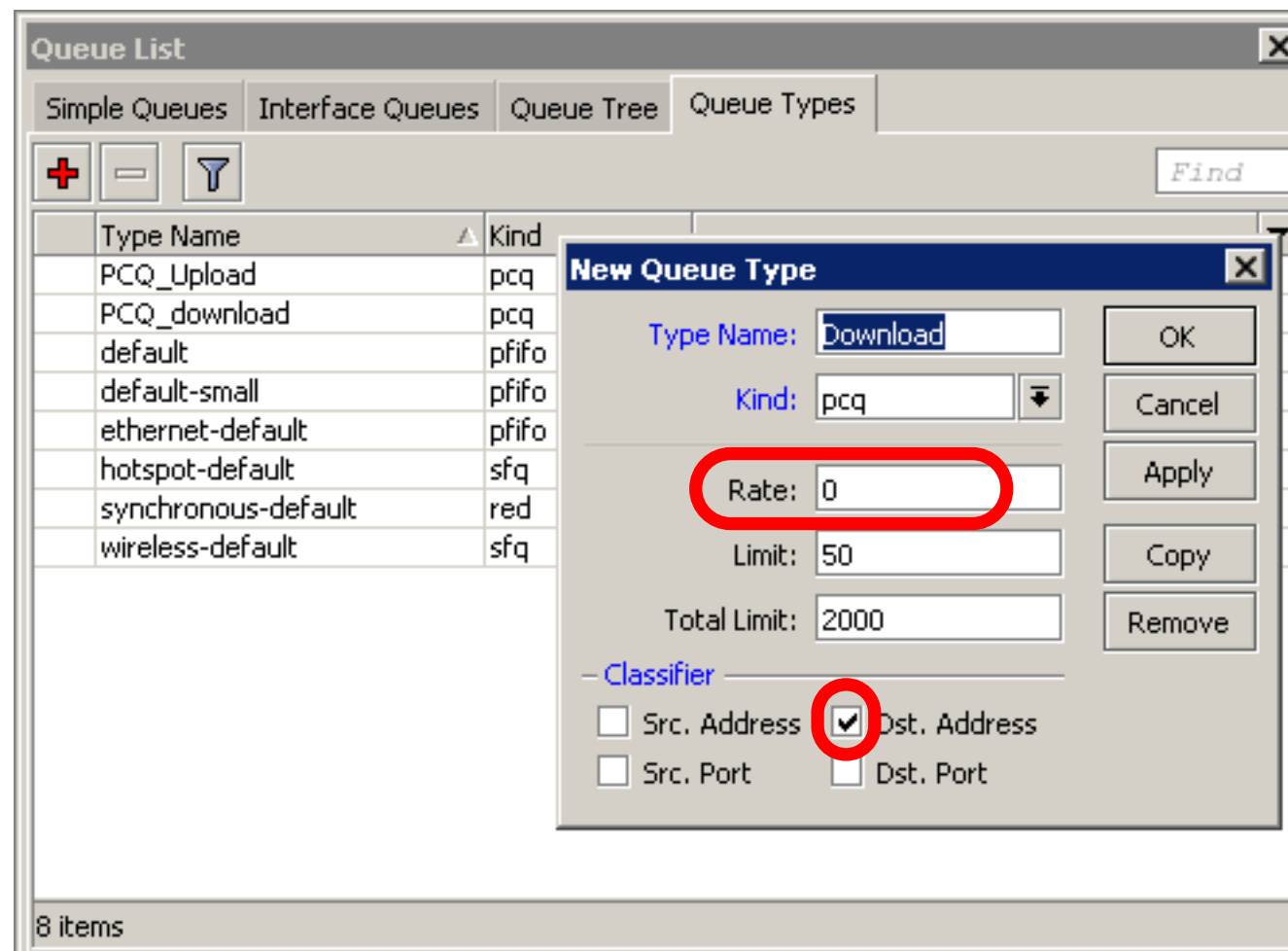
- Multiple queue rules are changed by one

The screenshot shows the 'New Simple Queue' dialog box with the following fields and values:

- General Tab:**
 - P2P: (empty)
 - Packet Marks: (empty)
 - Dst. Address: (empty)
 - Interface: all
 - Target Upload Limit At: unlimited
 - Target Download Limit At: unlimited
 - Queue Type:** PCQ_Upload (highlighted with a red circle)
 - Parent: none
 - Priority: 8
- Buttons:** OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, Reset All Counters, Torch.
- Status:** disabled

PCQ, equalize bandwidth

- Equally share bandwidth between customers



Equalize bandwidth

- 1M upload/2M download is shared between users

The image displays two screenshots of Mikrotik queue configuration windows. The left window is titled 'New Simple Queue' and the right window is titled 'Simple Queue'. Both windows have tabs for 'General', 'Advanced', 'Statistics', 'Traffic', 'Total', and 'Total Statistics'. In the 'New Simple Queue' window, the 'Name' field is 'queue1', the 'Target Address' is '192.168.0.0/24', and the 'Max Limit' is set to '1M' for upload and '2M' for download. In the 'Simple Queue' window, the 'P2P' field is empty, the 'Interface' is 'all', and the 'Limit At' is set to 'unlimited' for both upload and download. The 'Queue Type' is set to 'Upload' and 'Download'. Both windows have buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', 'Reset Counters', 'Reset All Counters', and 'Torch'.

New Simple Queue

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

Name: queue1

Target Address: 192.168.0.0/24

☒ Target Upload ☒ Target Download

Max Limit: 1M 2M bits/s

Burst

Time

disabled

Simple Queue

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

P2P:

Packet Marks:

Address:

Interface: all

Target Upload Target Download

Limit At: unlimited unlimited bits/s

Queue Type: Upload Download

Parent: none

Priority: 8

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

PCQ Lab

- Teacher is going to make PCQ lab on the router
- Two PCQ scenarios are going to be used with mangle

Summary

Wireless

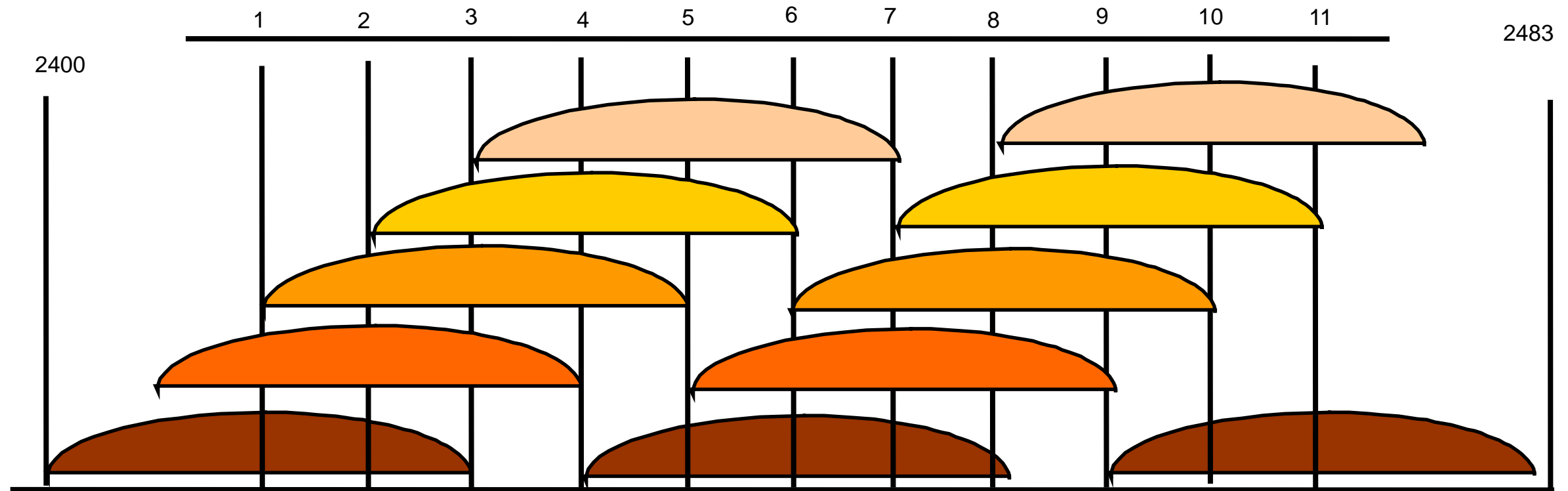
What is Wireless

- RouterOS supports various radio modules that allow communication over the air (2.4GHz and 5GHz)
- MikroTik RouterOS provides a complete support for IEEE 802.11a, 802.11b and 802.11g wireless networking standards

Wireless Standards

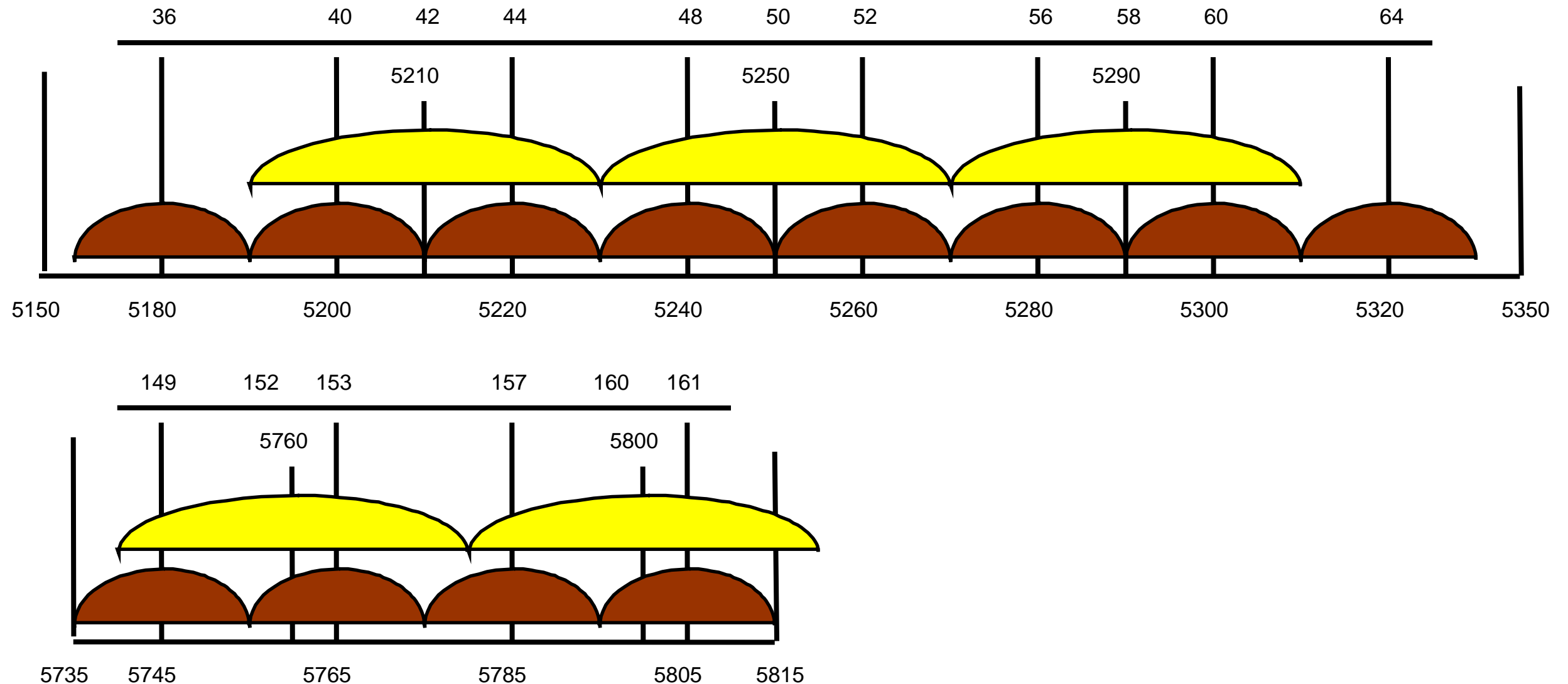
- IEEE 802.11b - 2.4GHz frequencies, 11Mbps
- IEEE 802.11g - 2.4GHz frequencies, 54Mbps
- IEEE 802.11a - 5GHz frequencies, 54Mbps
- IEEE 802.11n - draft, 2.4GHz - 5GHz

802.11 b/g Channels



- (11) 22 MHz wide channels (US)
- 3 non-overlapping channels
- 3 Access Points can occupy same area without interfering

802.11a Channels



- (12) 20 MHz wide channels
- (5) 40MHz wide turbo channels

Supported Bands

All 5GHz (802.11a) and 2.4GHz (802.11b/g),
including small channels

Supported Frequencies

- Depending on your country regulations wireless card might support
 - 2.4GHz: 2312 - 2499 MHz
 - 5GHz: 4920 - 6100 MHz

Apply Country Regulations

Set wireless interface to apply your country regulations

The screenshot shows the Mikrotik WinBox configuration window for the wireless interface <wlan1>. The 'Wireless' tab is active, displaying various settings. The 'Frequency Mode' is set to 'regulatory domain' and the 'Country' is set to 'united states'. The 'Simple Mode' button is highlighted with a red circle. The left sidebar shows the 'Wireless' menu selected.

Field	Value
Mode	ap bridge
Band	2.4GHz-B/G
Frequency	2412 MHz
SSID	abc
Radio Name	000C421B4EE8
Scan List	
Security Profile	default
Frequency Mode	regulatory domain
Country	united states
Antenna Mode	antenna a
Antenna Gain	0 dBi
DFS Mode	none
Proprietary Extensions	post-2.9.25
WMM Support	disabled
Default AP Tx Rate	
Default Client Tx Rate	
Default Authenticate	<input checked="" type="checkbox"/>
Default Forward	<input checked="" type="checkbox"/>
Hide SSID	<input type="checkbox"/>

Buttons: OK, Cancel, Apply, Enable, Comment, Torch, Scan..., Freq. Usage..., Align..., Sniff..., Snooper..., Reset Configuration, Simple Mode (highlighted).

Status: disabled, running, slave, disabled

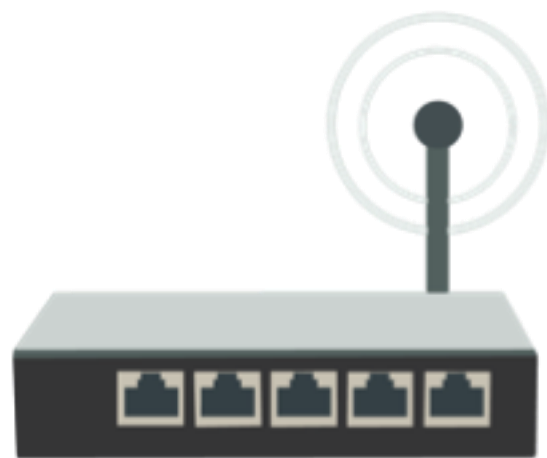
RADIO Name

- We will use RADIO Name for the same purposes as router identity
- Set RADIO Name as **Number+Your Name**

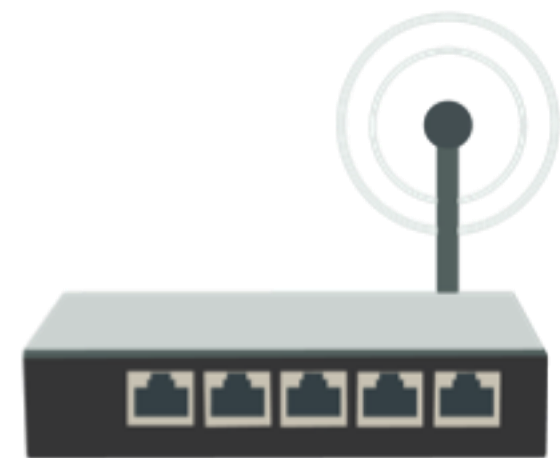
Wireless Network



Wireless
Access Point



**Wireless
Stations**



Station Configuration

- Set Interface **mode=station**
- Select **band**
- Set **SSID**, Wireless Network Identity
- Frequency is **not important** for client, use scan-list

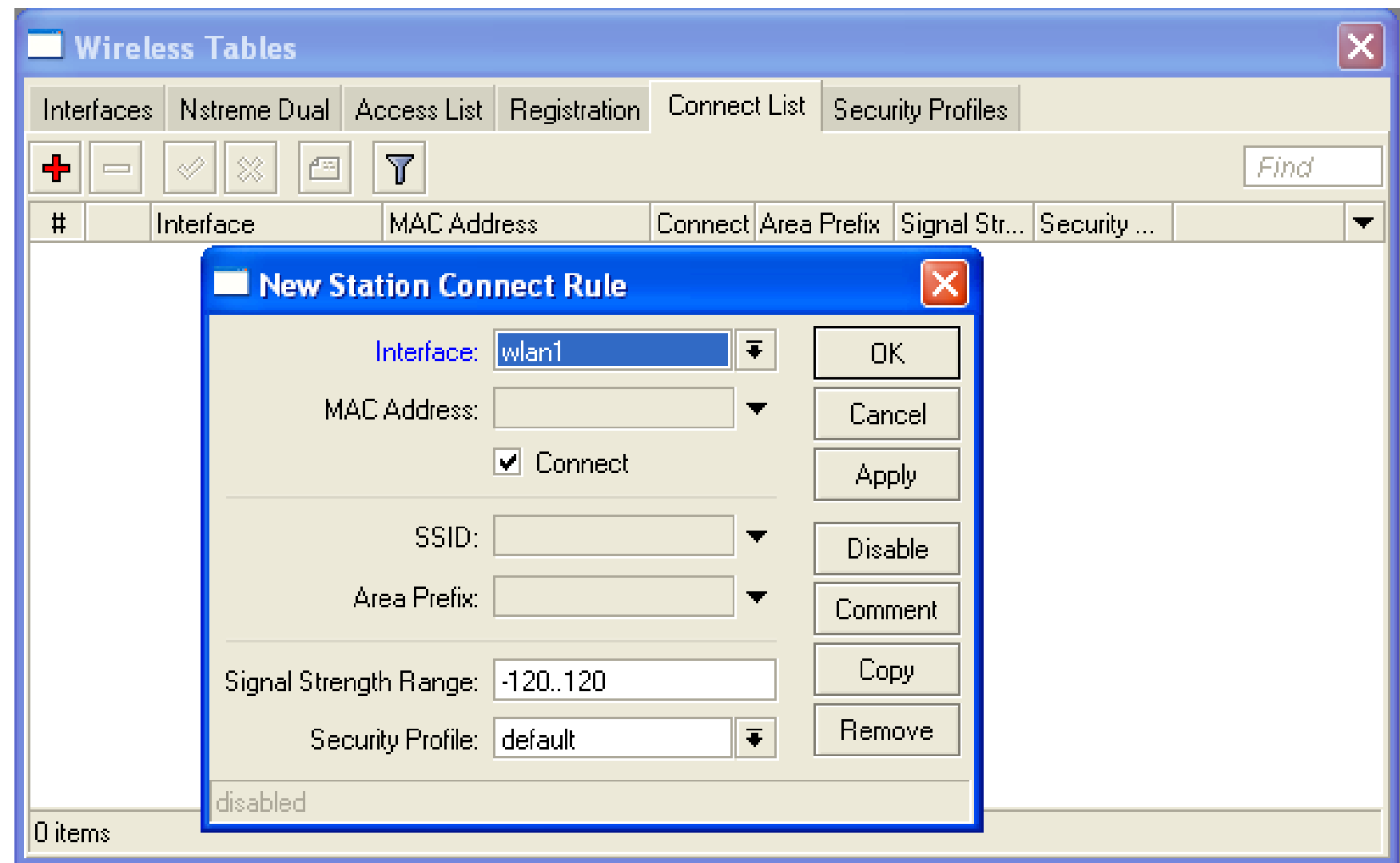
The screenshot shows the 'Interface <wlan1>' configuration window in WinBox, with the 'Wireless' tab selected. The configuration is as follows:

Field	Value
Mode	station
Band	2.4GHz-only-G
Frequency	2422 MHz
SSID	MikroTik
Scan List	
Security Profile	default
Antenna Mode	antenna a
Default AP Tx Rate	
Default Client Tx Rate	
Default Authenticate	<input checked="" type="checkbox"/>
Default Forward	<input checked="" type="checkbox"/>
Hide SSID	<input type="checkbox"/>
Compression	<input type="checkbox"/>

At the bottom, there are four status indicators: disabled, running, slave, and running ap. The 'running' indicator is highlighted.

Connect List

- Set of rules used by station to select access-point

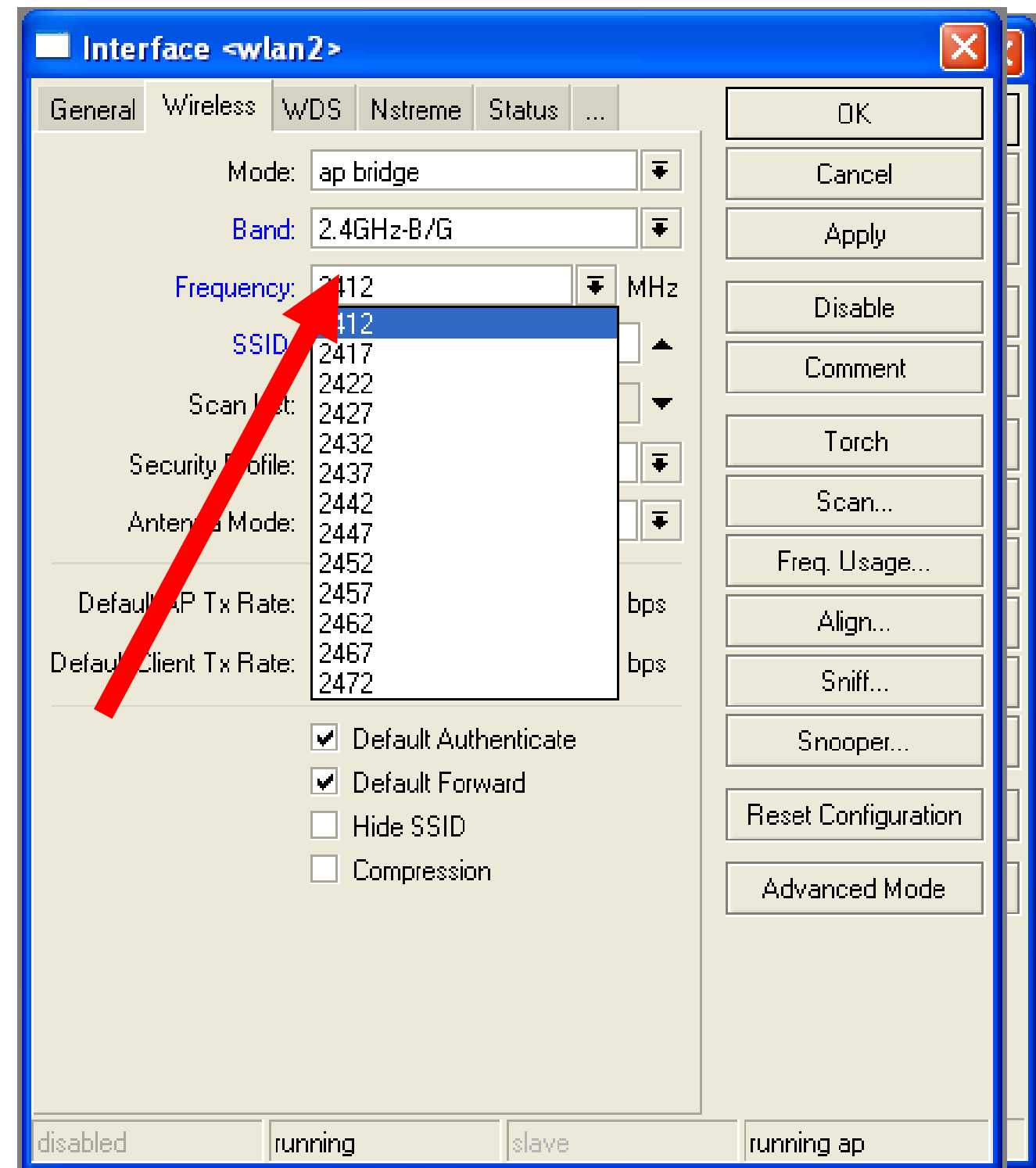


Connect List Lab

- Currently your router is connected to class access-point
- Let's make rule to disallow connection to class access-point
- Use connect-list matchers

Access Point Configuration

- Set Interface **mode=ap-bridge**
- Select **band**
- Set **SSID**, Wireless Network Identity
- Set **Frequency**



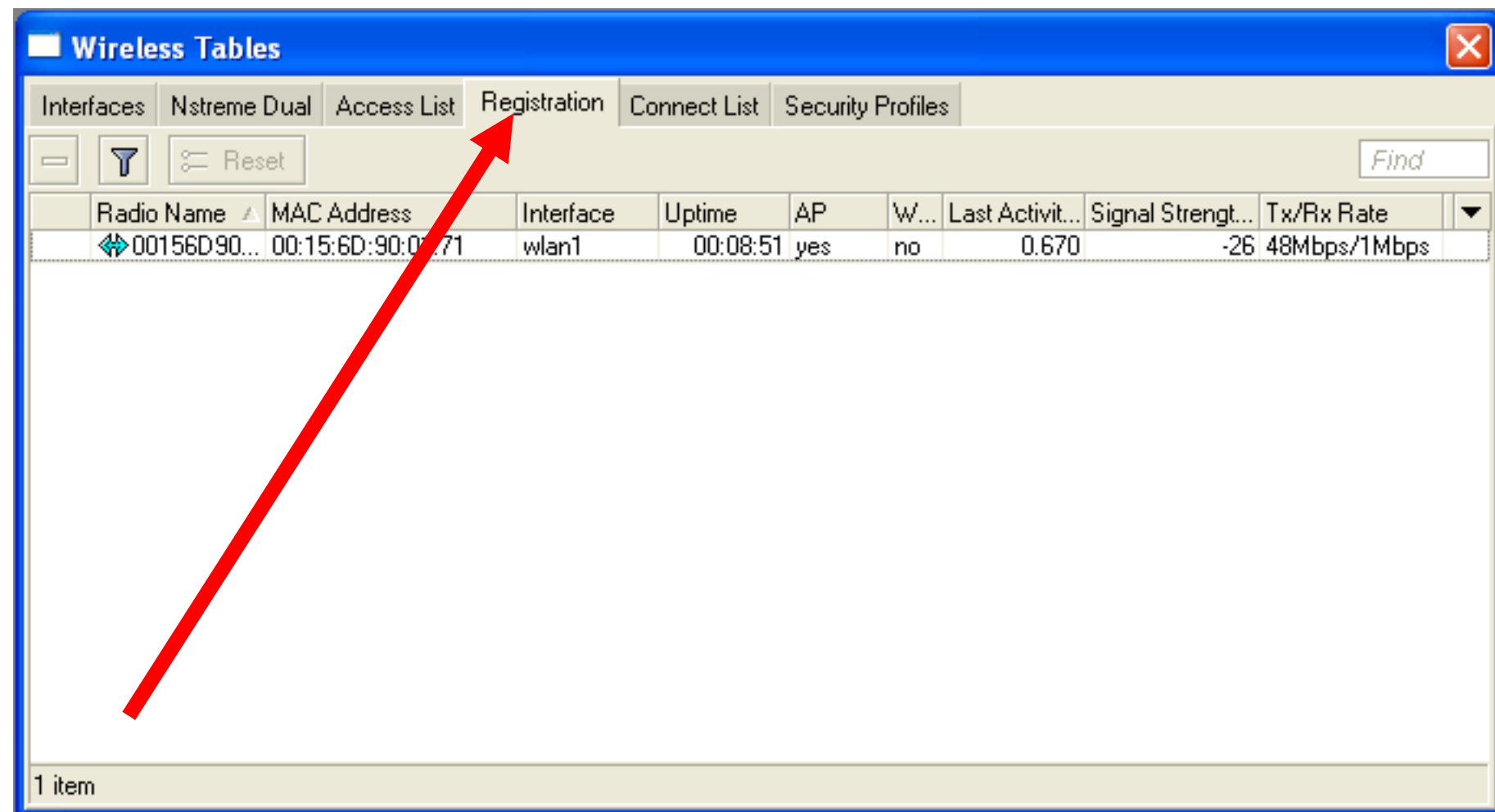
Snooper wireless monitor

- Use **Snooper** to get total view of the wireless networks on used band
- Wireless interface is **disconnected** at this moment

Frequency	Band	Address	SSID	Of Freq. (%)	Of Traf. (%)	Bandwidth
2412	2.4GHz...	00:0B:6B:3...	MikroTik	0.0	0.0	0 b/s
2412	2.4GHz...	00:0C:42:0...	hotspot	0.0	0.0	0 b/s
2412	2.4GHz...	00:0C:42:0...	Kris	0.0	0.0	0 b/s
2412	2.4GHz...	00:0B:6B:4...	hotspot	0.8	8.0	7.2 kb/s
2412	2.4GHz...	00:0C:42:1...	hotspot	0.8	8.0	7.2 kb/s
2427	2.4GHz...			0.0		0 b/s
2452	2.4GHz...			1.8		8.0 kb/s
2447	2.4GHz...			1.4		11.2 kb/s
2437	2.4GHz...			4.0		14.2 kb/s
2412	2.4GHz...	00:0C:42:0...	den	0.5	12.8	4.1 kb/s
2412	2.4GHz...	00:19:5B:...	default	0.7	19.6	5.9 kb/s
2442	2.4GHz...			2.8		18.3 kb/s
2412	2.4GHz...	00:0B:6B:3...	seta	1.0	35.9	8.2 kb/s
2462	2.4GHz...			2.5		20.0 kb/s
2412	2.4GHz...	00:1D:7E:...	linksys_SE...	0.9	26.9	7.3 kb/s
2432	2.4GHz...			4.7		20.8 kb/s
2412	2.4GHz...	00:0E:2E:F...	MY_NEW...	1.1	24.8	10.7 kb/s
2457	2.4GHz...			3.0		24.3 kb/s
2412	2.4GHz...	00:0C:42:0...	stendi	1.0	32.9	8.0 kb/s
2412	2.4GHz...	00:0C:42:0...	stendi	1.0	32.9	8.0 kb/s
2412	2.4GHz...	00:0B:6B:3...	stendi	1.0	34.0	8.3 kb/s
2422	2.4GHz...			7.5		54.4 kb/s
2417	2.4GHz...			9.2		61.8 kb/s
2412	2.4GHz...	00:0C:42:0...		0.0	0.0	0 b/s

Registration Table

- View all connected wireless interfaces

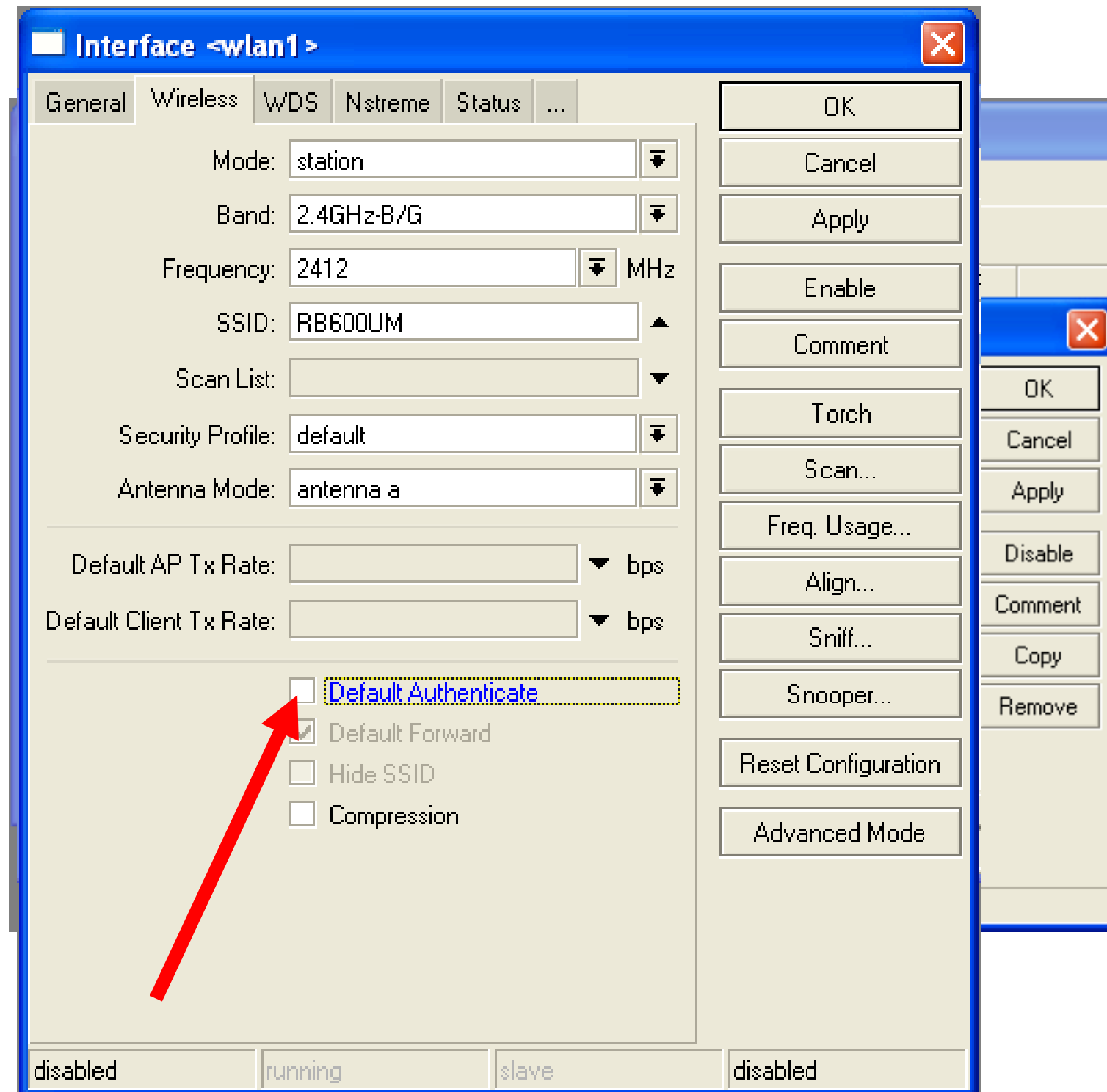


The screenshot shows a window titled 'Wireless Tables' with several tabs: 'Interfaces', 'Nstreme Dual', 'Access List', 'Registration', 'Connect List', and 'Security Profiles'. The 'Registration' tab is selected. Below the tabs is a search bar with a 'Find' button and a 'Reset' button. A table displays the registration information for a single item. The table has columns: 'Radio Name', 'MAC Address', 'Interface', 'Uptime', 'AP', 'W...', 'Last Activit...', 'Signal Strengt...', and 'Tx/Rx Rate'. The data row shows a radio named '00156D90...' with MAC address '00:15:6D:90:00:71' connected to 'wlan1' for 00:08:51, with AP 'yes', W... 'no', Last Activit... '0.670', Signal Strengt... '-26', and Tx/Rx Rate '48Mbps/1Mbps'. A status bar at the bottom indicates '1 item'.

Radio Name	MAC Address	Interface	Uptime	AP	W...	Last Activit...	Signal Strengt...	Tx/Rx Rate
00156D90...	00:15:6D:90:00:71	wlan1	00:08:51	yes	no	0.670	-26	48Mbps/1Mbps

Security on Access Point

- **Access-list** is used to set **MAC-address** security
- Disable **Default-Authentication** to use only **Access-list**



Default Authentication

- **Yes**, Access-List rules are checked, client is able to connect, if there is no deny rule
- **No**, only Access-List rule are checked

Access-List Lab

- Since you have mode=station configured we are going to make lab on teacher's router
- Disable connection for specific client
- Allow connection only for specific clients

Security

- Let's enable encryption on wireless network
- You must use WPA or WPA2 encryption protocols
- All devices on the network should have the same security options

Security

LAB

- Let's create WPA **encryption** for our wireless network
- WPA Pre-Shared Key is **mikrotiktraining**

Wireless Tables

Interfaces Nstreme Dual Access List Registration Connect List Security Profiles

+ - Filter

Name	Mode
default	not

1 item

New Security Profile

General RADIUS EAP Static Keys

Name: profile1

Mode: dynamic keys

Authentication Types

☒ WPA PSK ☒ WPA2 PSK

☐ WPA EAP ☐ WPA2 EAP

Unicast Ciphers

☒ tkip ☒ aes ccm

Group Ciphers

☒ tkip ☒ aes ccm

WPA Pre-Shared Key: *****

WPA2 Pre-Shared Key: *****

Supplicant Identity:

Group Key Update: 00:05:00

Management Protection: allowed

Management Protection Key:

OK Cancel Apply Copy Remove

Configuration Tip

- To view hidden Pre-Shared Key, click on Hide Passwords
- It is possible to view other hidden information, except router password

03:14:52 ☐ Hide Passwords

New Security Profile

General | RADIUS | EAP | Static Keys

Name: Security

Mode: dynamic keys

– Authentication Types –

☒ WPA PSK ☒ WPA2 PSK

☐ WPA EAP ☐ WPA2 EAP

– Unicast Ciphers –

☒ tkip ☐ aes ccm

– Group Ciphers –

☒ tkip ☐ aes ccm

WPA Pre-Shared Key: mikrotiktraining

WPA2 Pre-Shared Key: mikrotiktraining

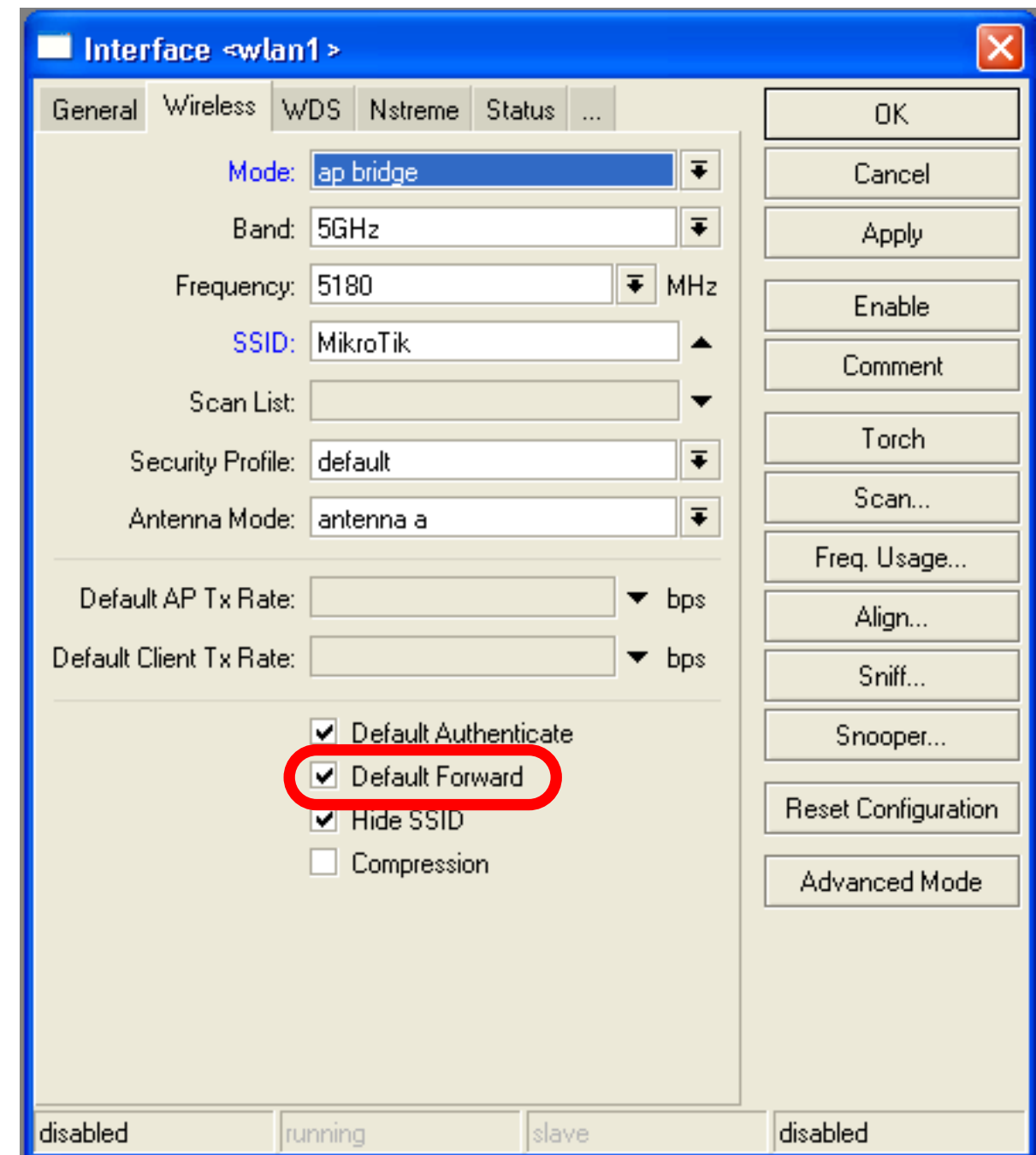
Supplicant Identity:

Group Key Update: 00:05:00

OK Cancel Apply Copy Remove

Drop Connections between clients

Default-Forwarding used
to disable
communications
between clients
connected to the same
access-point



Default Forwarding

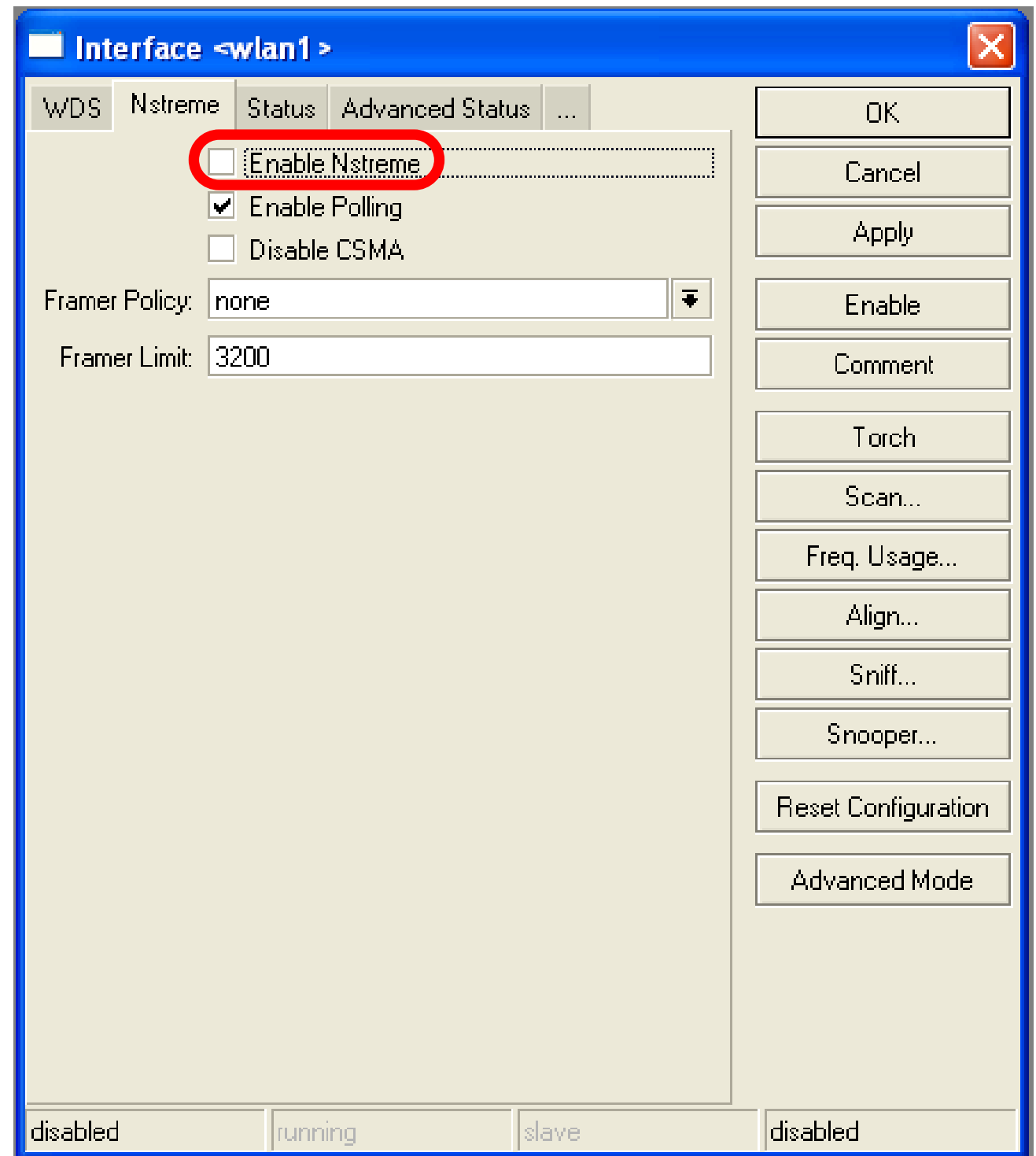
- Access-List rules have higher priority
- Check your access-list if connection between client is working

Nstreme

- MikroTik proprietary wireless protocol
- Improves wireless links, especially long-range links
- To use it on your network, enable protocol **on all** wireless devices of this network

Nstreme Lab

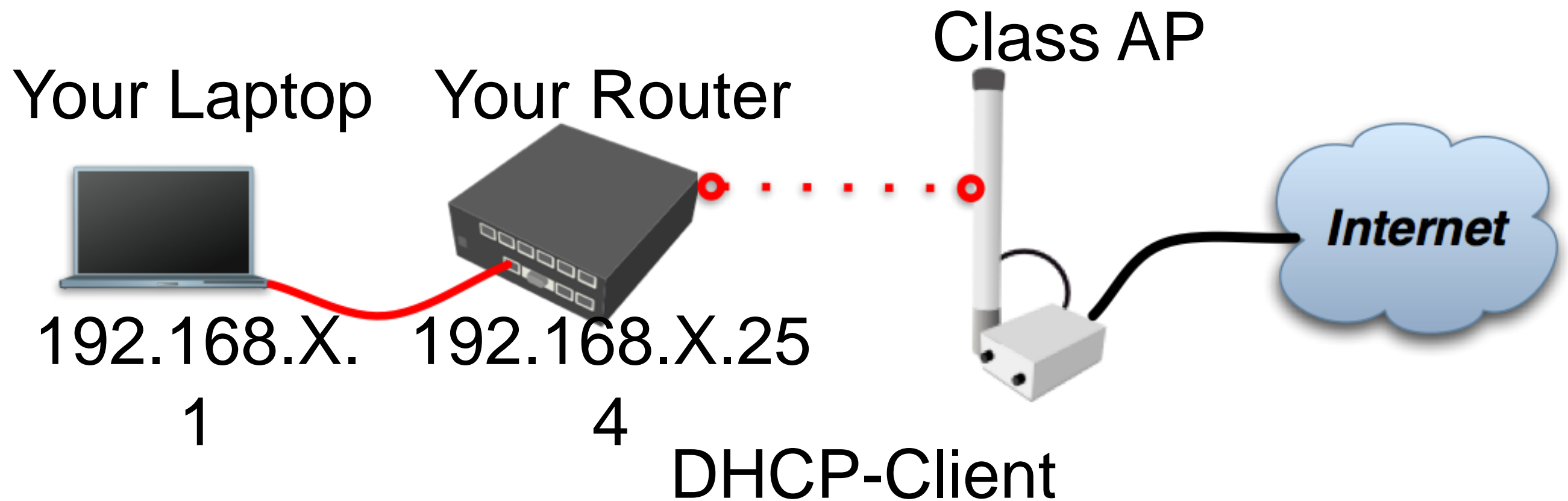
- Enable Nstreme on your router
- Check the connection status
- **Nstreme** should be enabled on **both** routers



Summary

Bridging

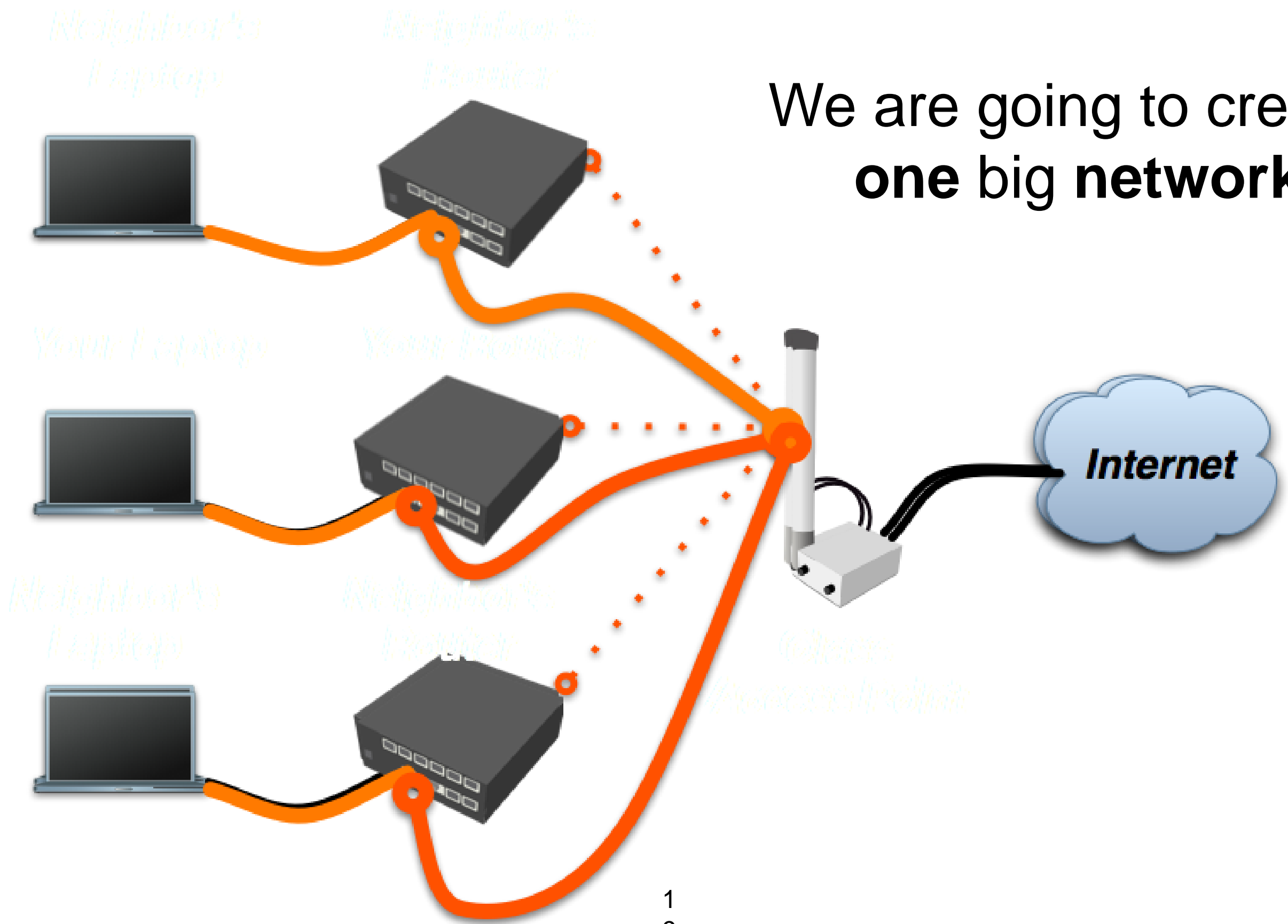
Bridge Wireless Network



Let's get back to our configuration

Bridge Wireless Network

We are going to create
one big network



Bridge

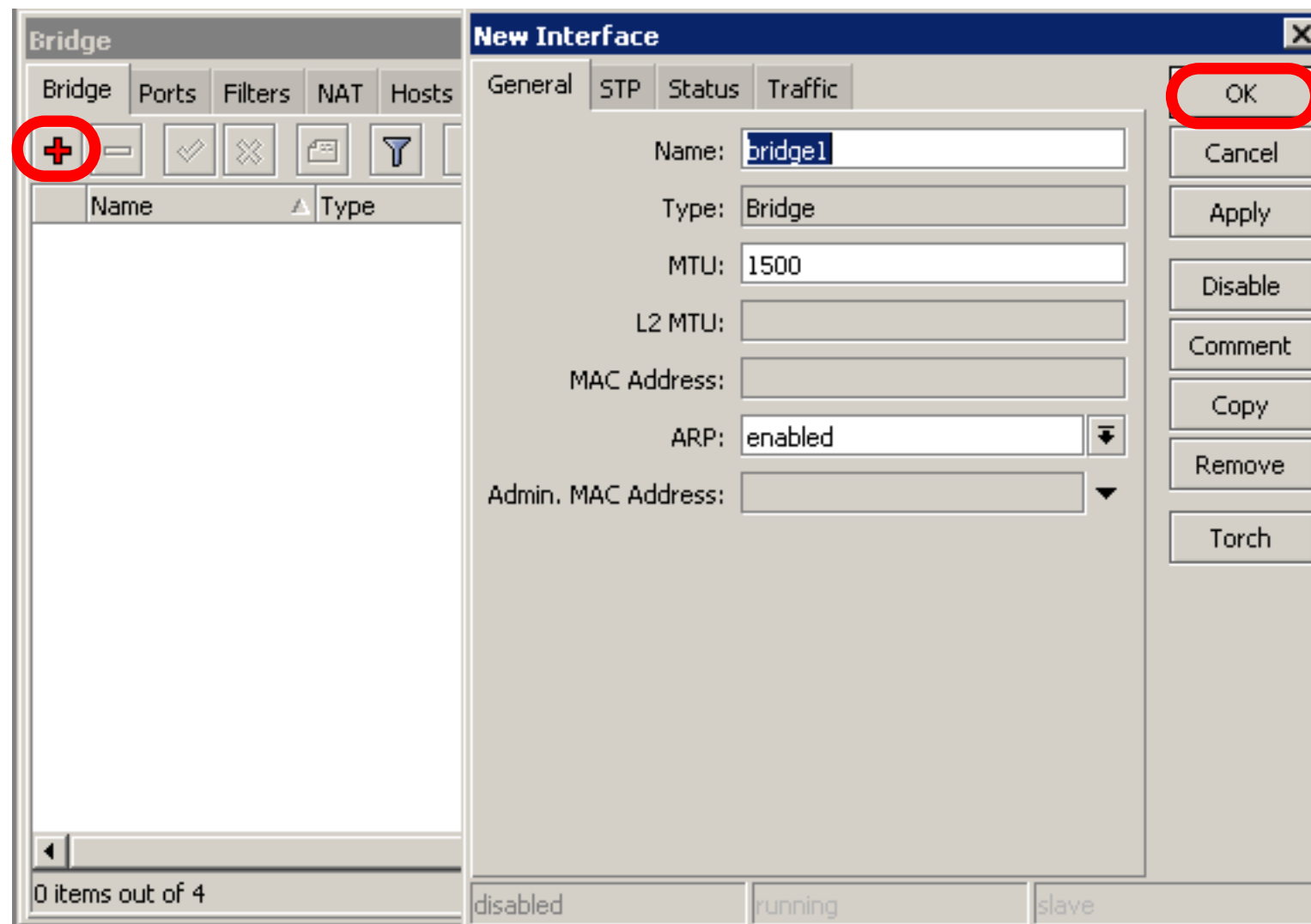
- We are going to bridge local Ethernet interface with Internet wireless interface
- Bridge unites different physical interfaces into one logical interface
- All your laptops will be in the same network

Bridge

- To bridge you need to create bridge interface
- Add interfaces to bridge ports

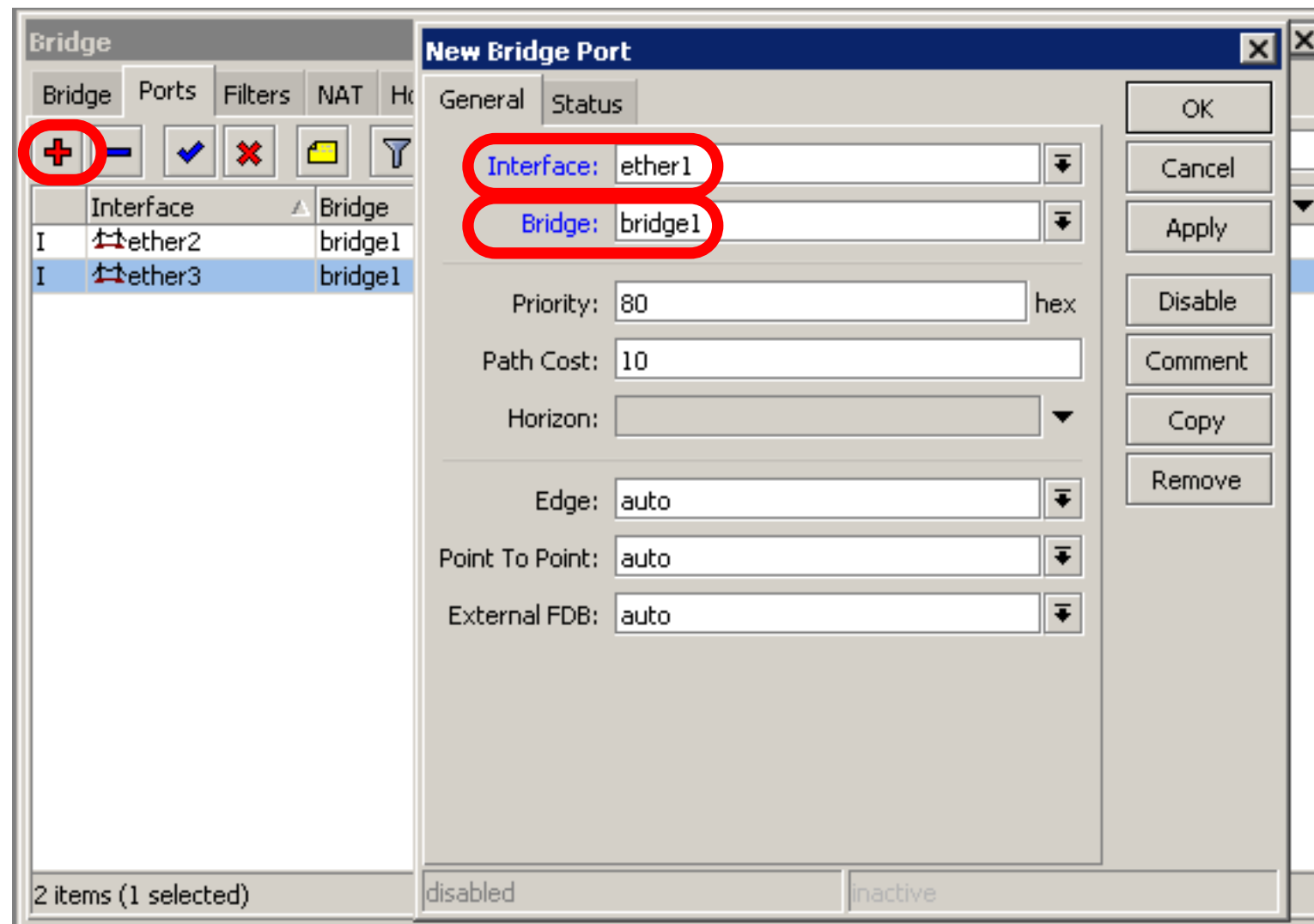
Create Bridge

- Bridge is configured from **/interface bridge** menu



Add Bridge Port

- Interfaces are added to bridge via ports



Bridge

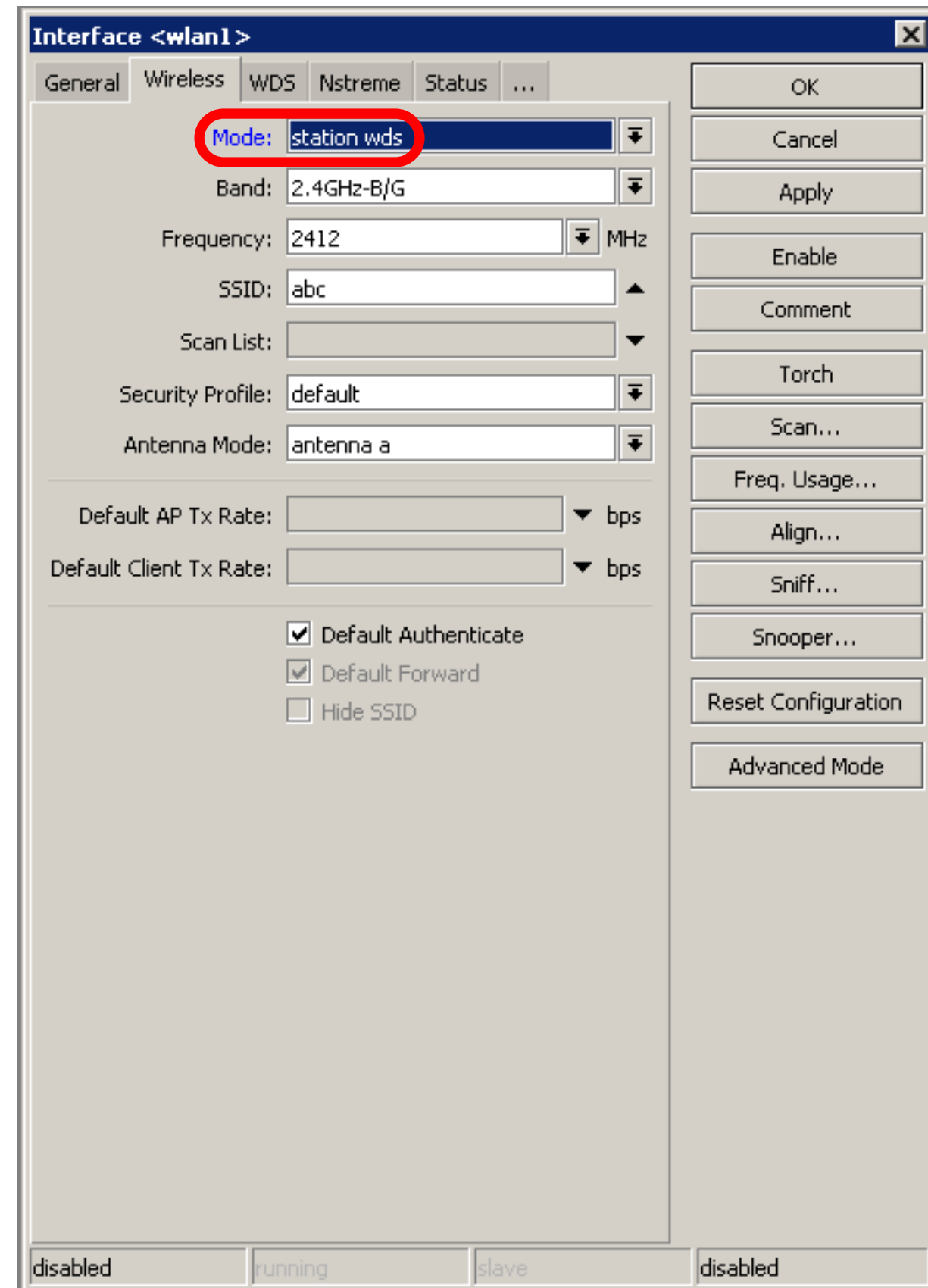
- There are no problems to bridge Ethernet interface
- Wireless Clients (**mode=station**) do not support **bridging** due the limitation of 802.11

Bridge Wireless

- **WDS** allows to add wireless client to **bridge**
- WDS (Wireless Distribution System) enables connection between Access Point and Access Point

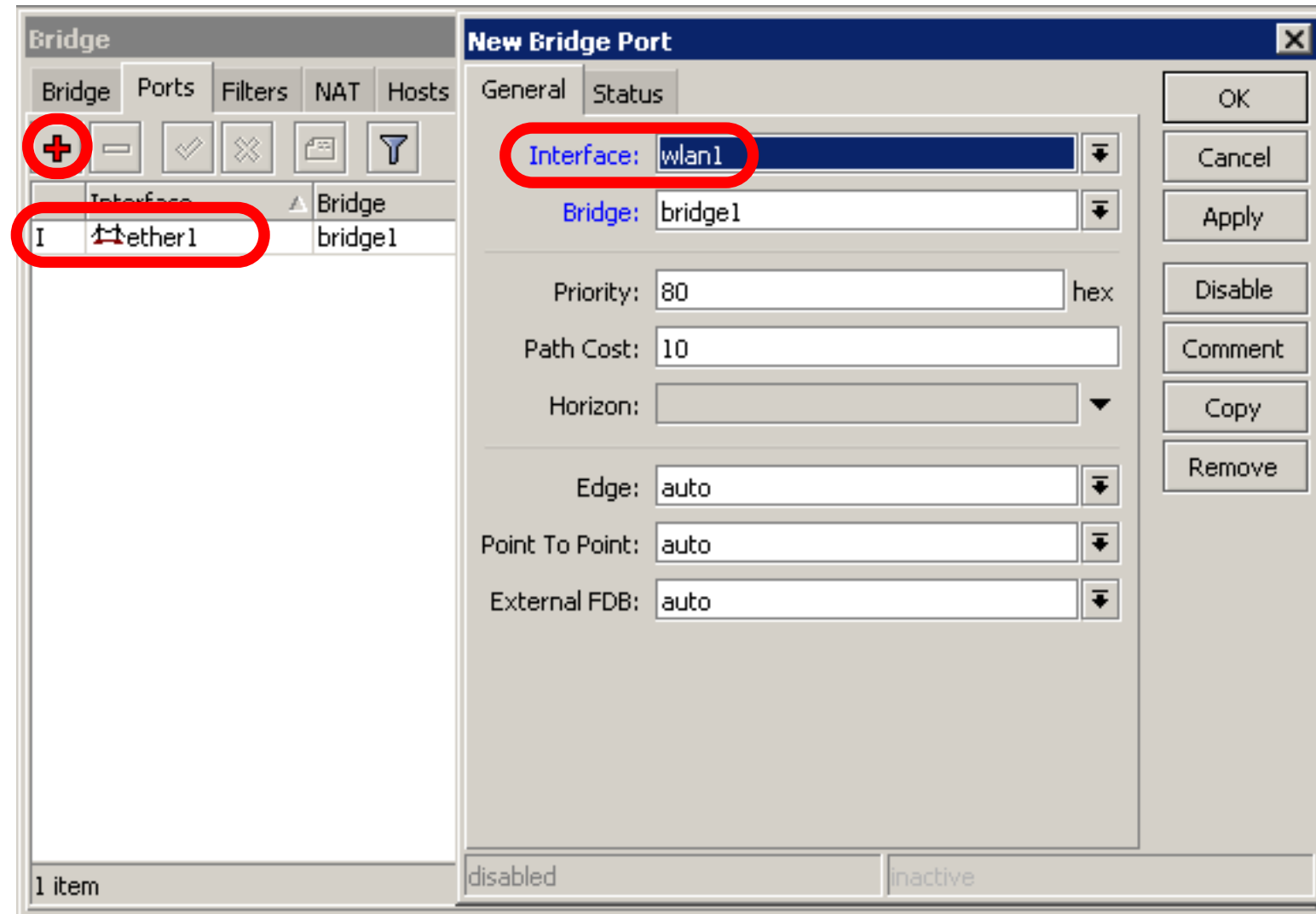
Set WDS Mode

- Station-wds is special station mode with WDS support



Add Bridge Ports

- Add public and local interface to bridge
- Ether1 (local), wlan1 (public)



Access Point WDS

- Enable WDS on AP-bridge, use mode=dynamic-mesh
- WDS interfaces are created on the fly
- Use default bridge for WDS interfaces
- Add Wireless Interface to Bridge

AP-bridge

- Set AP-bridge settings
- Add Wireless interface to **bridge**

Interface <wlan1>

General Wireless WDS Nstreme Status Traffic

Mode: **ap bridge**

Band: 2.4GHz-B/G

Frequency: 2412 MHz

SSID: abc

Scan List:

Security Profile: default

Antenna Mode: antenna a

Default AP Tx Rate: bps

Default Client Tx Rate: bps

☒ Default Authenticate

☒ Default Forward

☐ Hide SSID

OK

Cancel

Apply

Enable

Comment

Torch

Scan...

Freq. Usage...

Align...

Sniff...

Snooper...

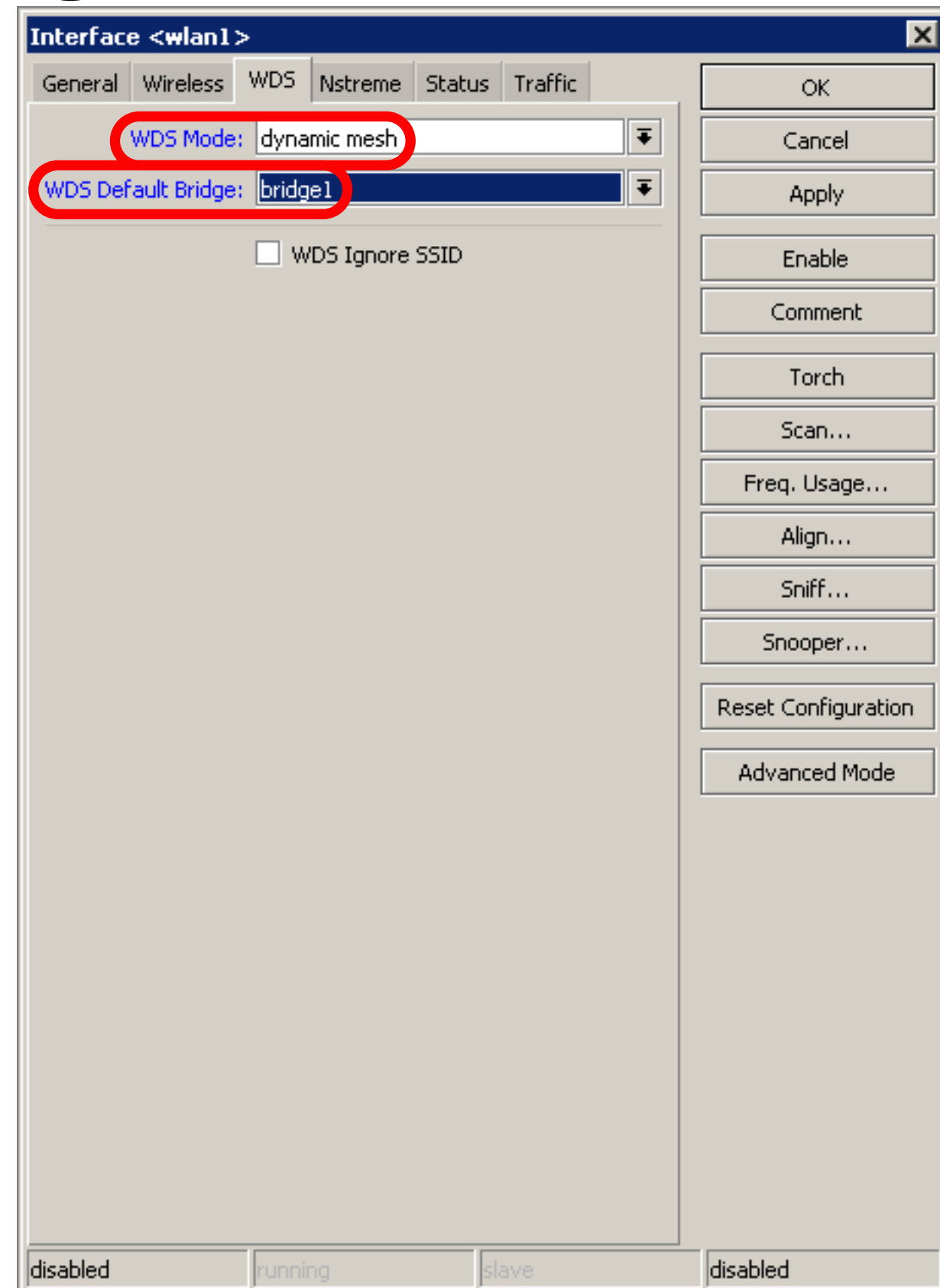
Reset Configuration

Advanced Mode

disabled running slave disabled

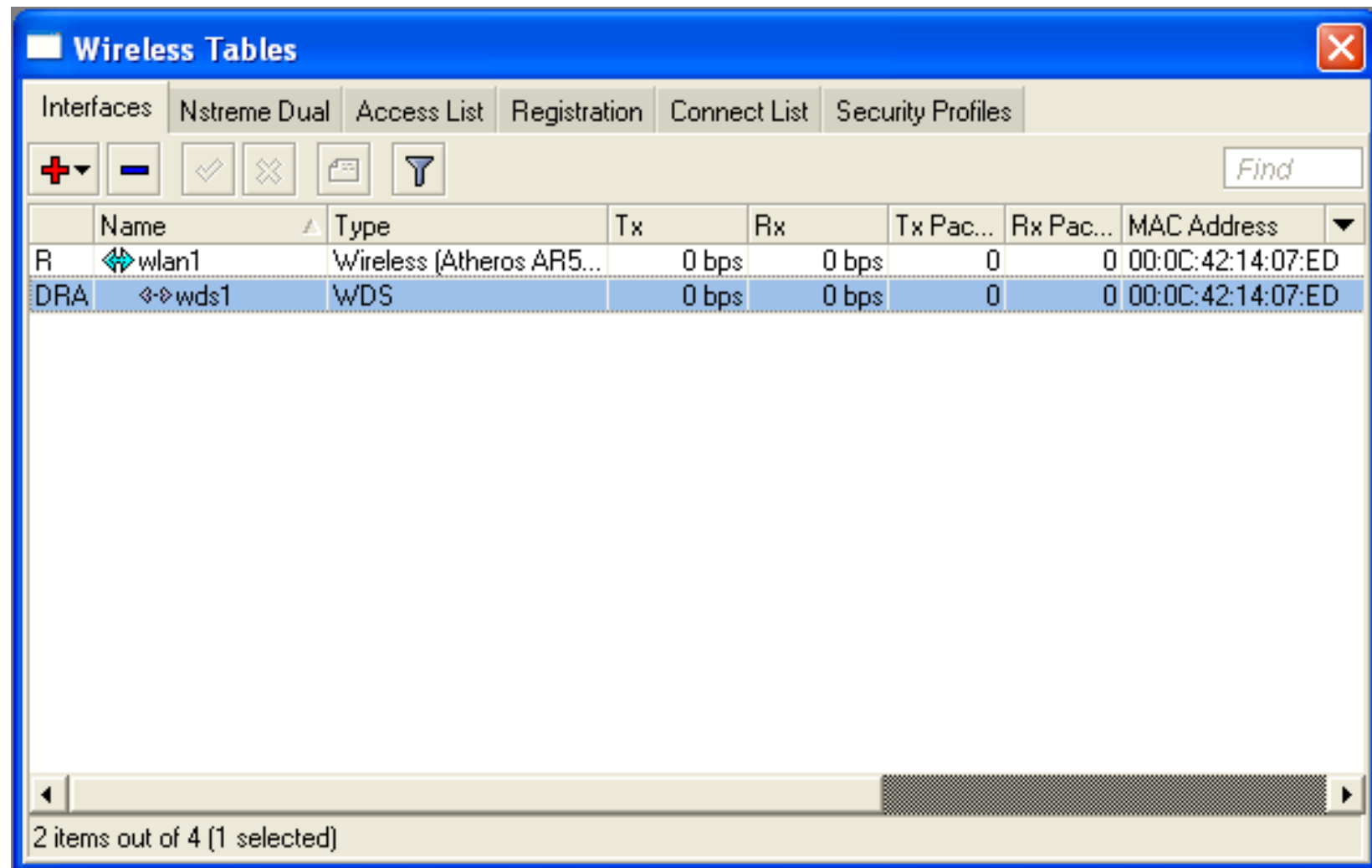
WDS configuration

- Use **dynamic-mesh** WDS mode
- WDS interfaces are created on the fly
- Others AP should use **dynamic-mesh** too



WDS

- WDS link is established
- Dynamic interface is present



	Name	Type	Tx	Rx	Tx Pac...	Rx Pac...	MAC Address
R	wlan1	Wireless (Atheros AR5...	0 bps	0 bps	0	0	00:0C:42:14:07:ED
DRA	wds1	WDS	0 bps	0 bps	0	0	00:0C:42:14:07:ED

WDS Lab

- Delete **masquerade** rule
- Delete **DHCP-client** on router wireless interface
- Use mode=station-wds on router
- Enable DHCP on your laptop
- Can you ping neighbor's laptop

WDS Lab

- Your **Router is Transparent Bridge** now
- You should be able to ping neighbor router and computer now
- Just use correct IP address

Restore Configuration

- To restore configuration manually
 - change back to Station mode
 - Add DHCP-Client on correct interface
 - Add masquerade rule
 - Set correct network configuration to laptop

Summary

Routing

Route Networks

- Configuration is back
- Try to ping neighbor's laptop
- Neighbor's address 192.168.X.1
- We are going to learn how to use route rules to ping neighbor laptop

Route

- **ip route** rules define where packets should be sent
- Let's look at `/ip route` rules

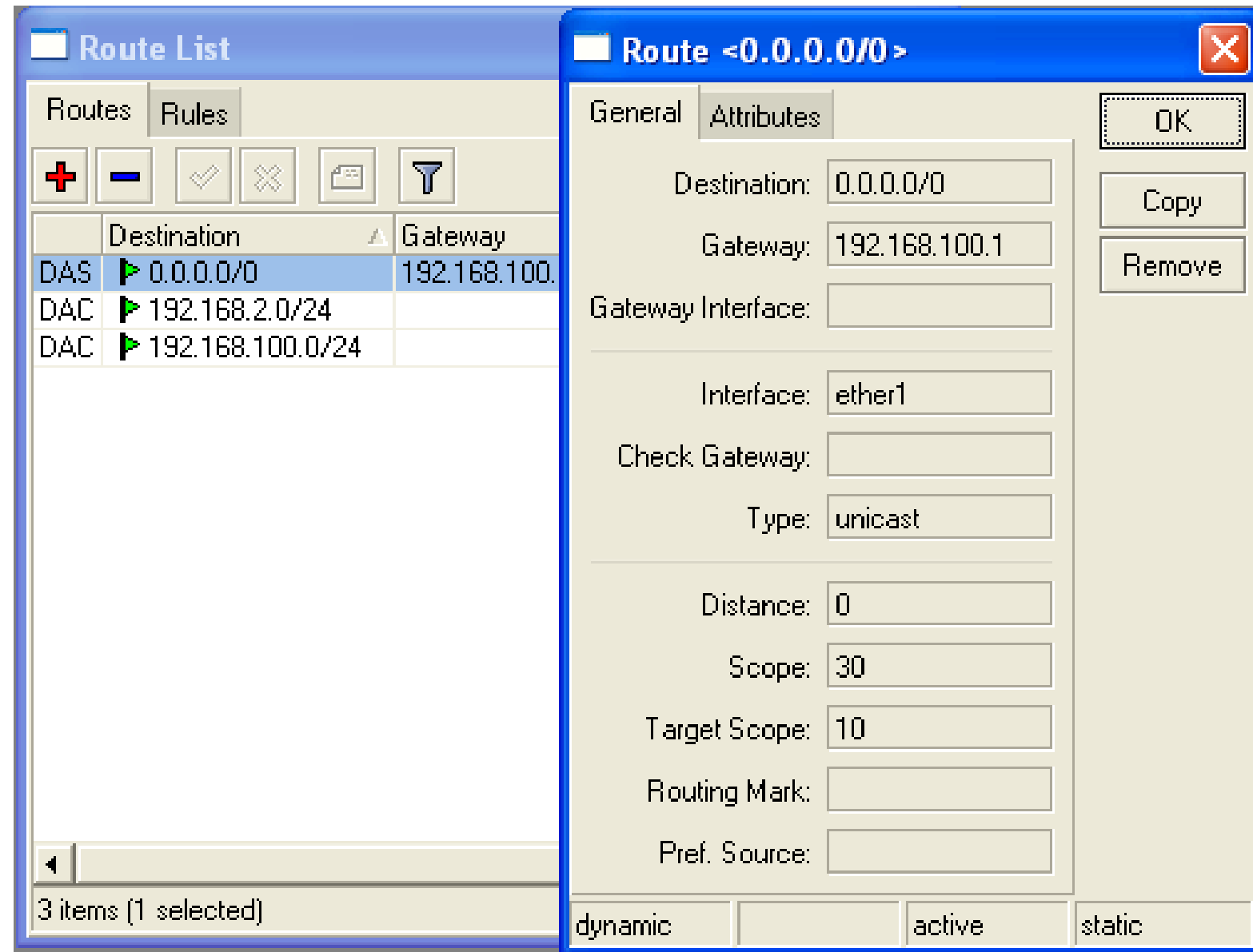
Routes

- **Destination:**
networks
which can be
reached
- **Gateway:**
IP of the next
router to reach
the
destination

	Destination	Gateway	Gateway ...	Interface
DAS	0.0.0.0/0	192.168.100.1		ether1
DAC	192.168.2.0/24			wlan1
DAC	192.168.100.0/24			ether1

Default Gateway

Default gateway:
next hop router
where all (**0.0.0.0**)
traffic is sent

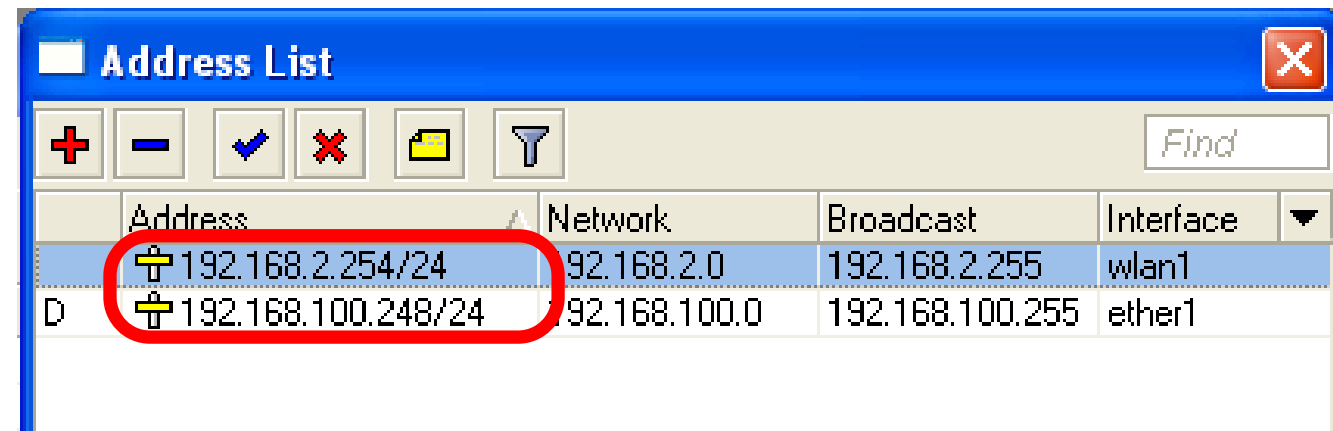


Set Default Gateway Lab

- Currently you have default gateway received from DHCP-Client
- Disable automatic receiving of default gateway in DHCP-client settings
- Add default gateway manually

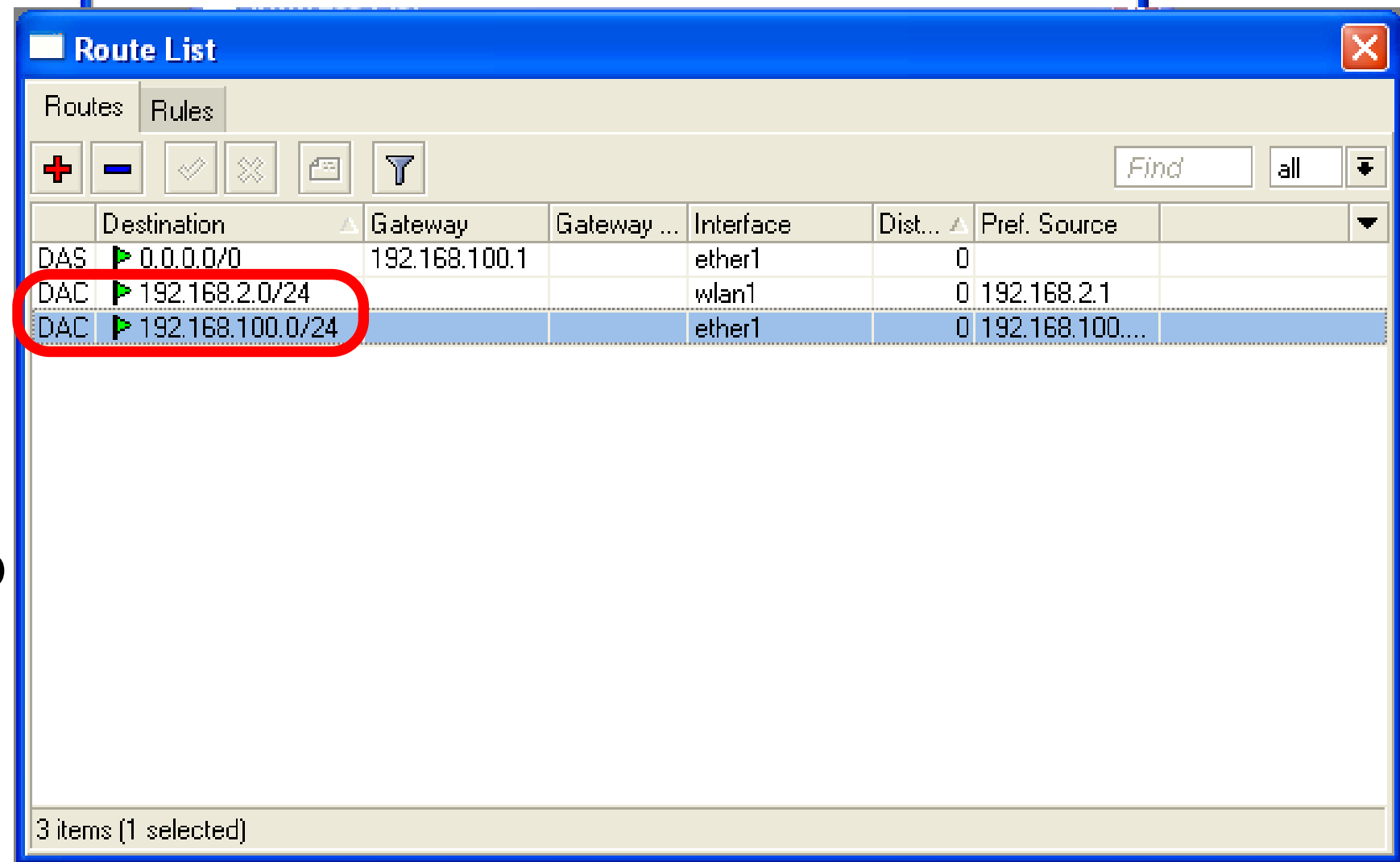
Dynamic Routes

- Look at the other routes
- Routes with **DAC** are added automatically
- **DAC** route comes from IP address configuration



Address List

	Address	Network	Broadcast	Interface
	192.168.2.254/24	192.168.2.0	192.168.2.255	wlan1
D	192.168.100.248/24	192.168.100.0	192.168.100.255	ether1



Route List

	Destination	Gateway	Gateway ...	Interface	Dist...	Pref. Source
DAS	0.0.0.0/0	192.168.100.1		ether1	0	
DAC	192.168.2.0/24			wlan1	0	192.168.2.1
DAC	192.168.100.0/24			ether1	0	192.168.100...

3 items (1 selected)

Routes

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

Static Routes

- Our goal is to ping neighbor laptop
- Static route will help us to achieve this

Static Route

- Static route specifies how to reach specific destination network
- **Default gateway** is also static route, it sends all traffic (destination 0.0.0.0) to host - the gateway

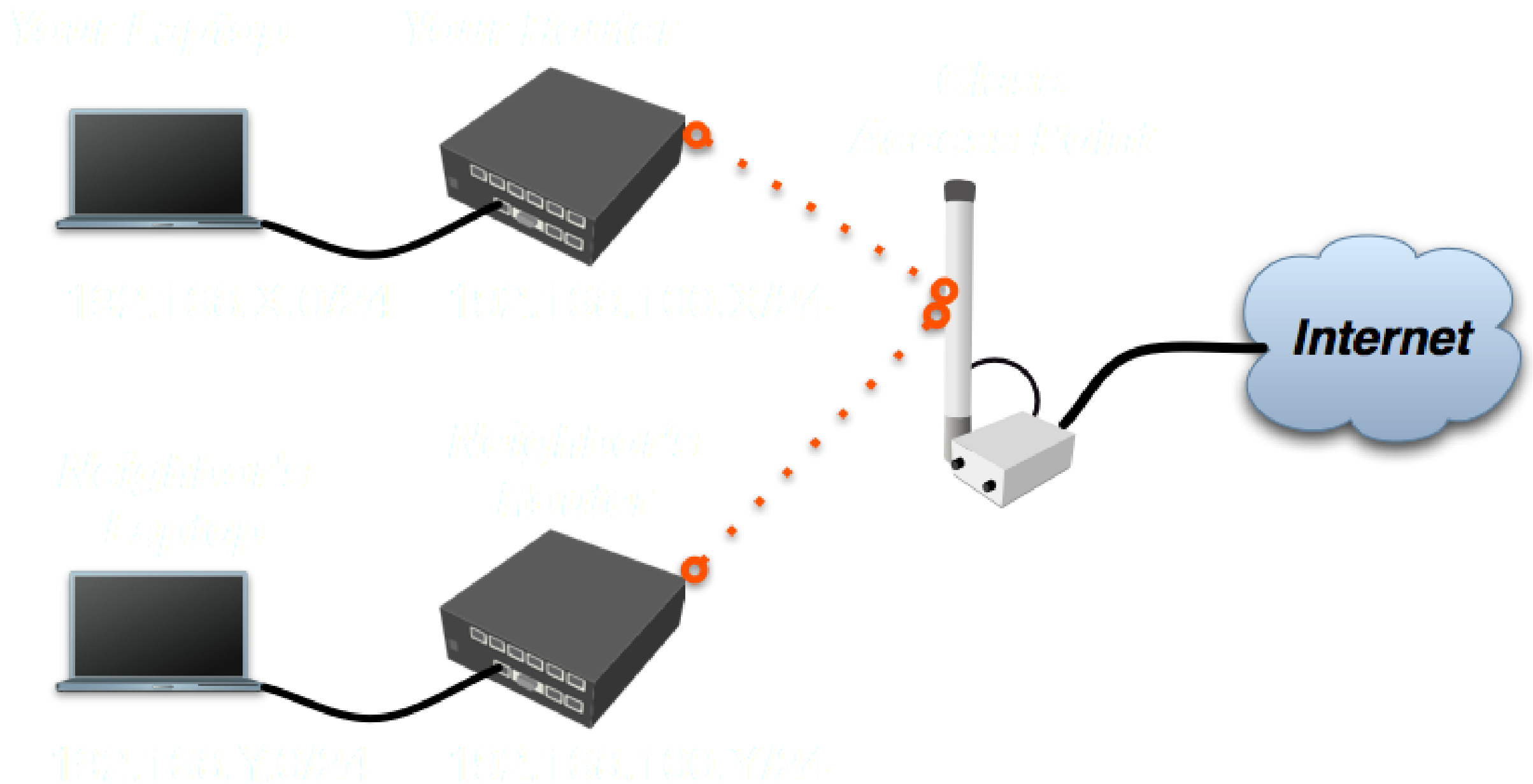
Static Route

- Additional static route is required to reach your neighbor laptop
- Because **gateway** (teacher's router) does not have information about **student's private network**

Route to Your Neighbor

- Remember the network structure
- Neighbor's local network is 192.168.x.0/24
- Ask your neighbor the IP address of their wireless interface

Network Structure

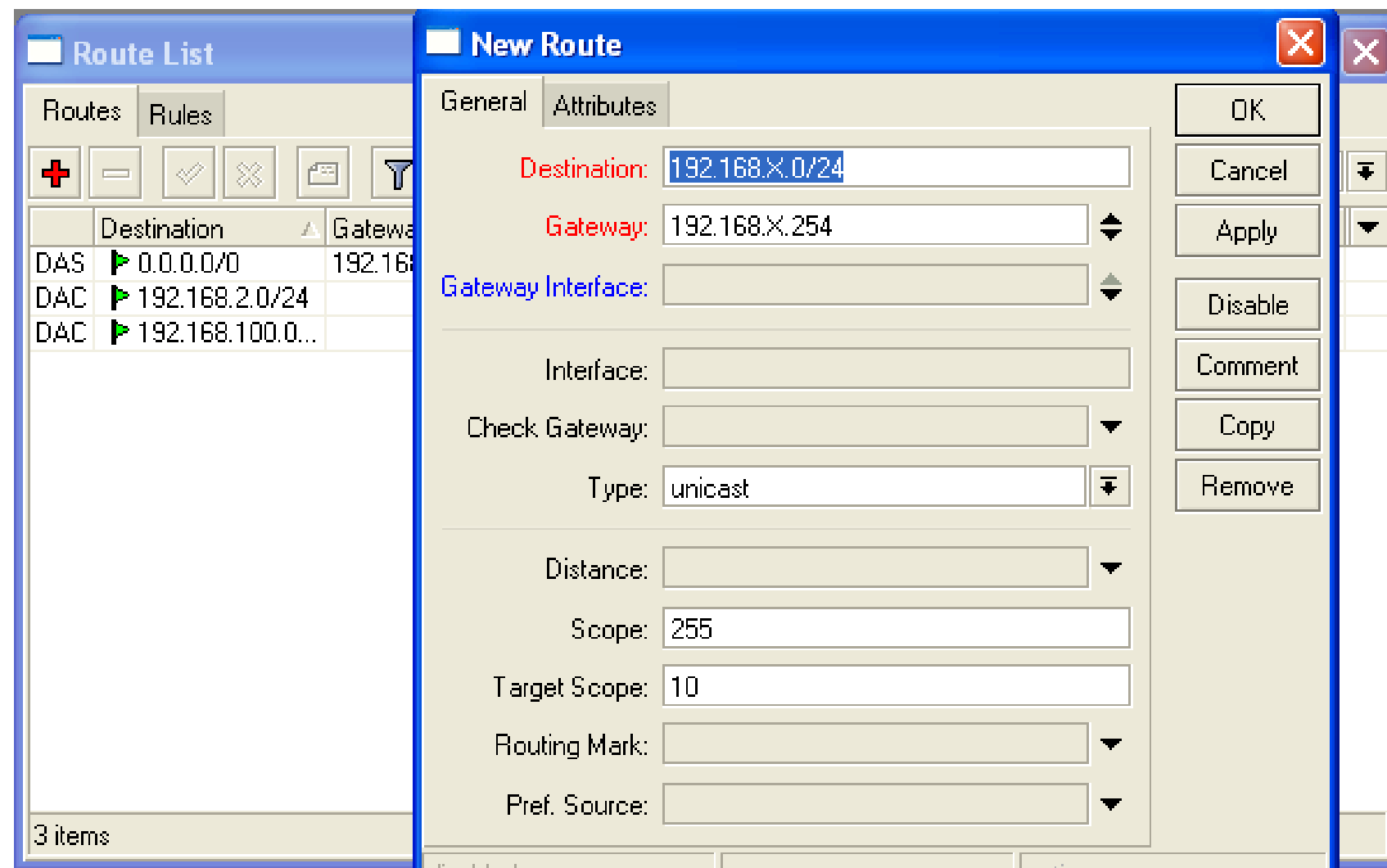


Route To Your Neighbor

- Add one route rule
- Set Destination, **destination** is **neighbor's local network**
- Set Gateway, address which is used to reach destination - **gateway** is IP address of neighbor's router wireless interface

Route Your Neighbor

- Add static route
- Set Destination and Gateway
- Try to ping Neighbor's Laptop



Router To Your Neighbor

You should be able to ping neighbor's laptop
now

Dynamic Routes

- The same configuration is possible with dynamic routes
- Imagine you have to add static routes to all neighbors networks
- Instead of adding tons of rules, dynamic routing protocols can be used

Dynamic Routes

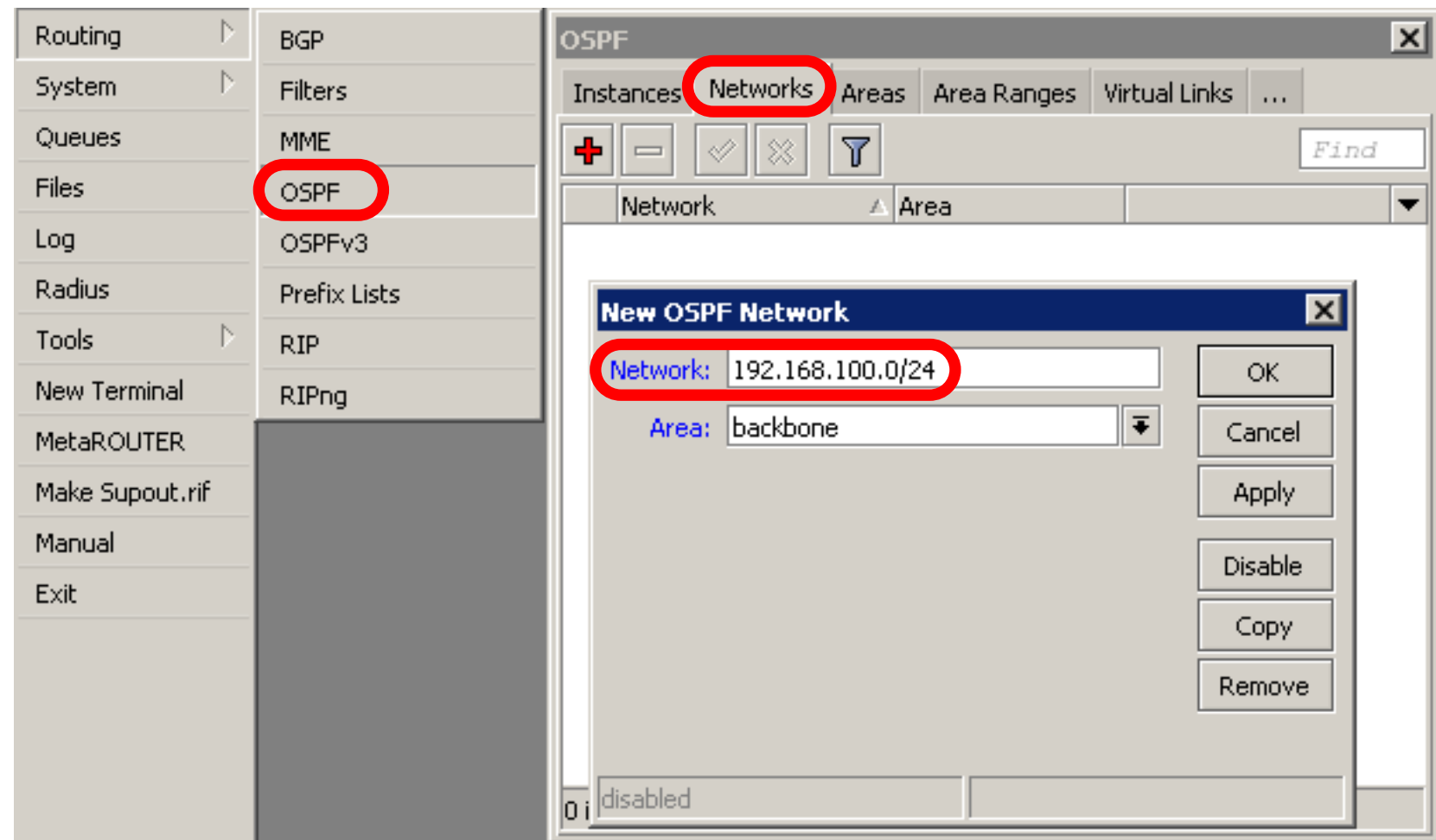
- Easy in configuration, difficult in managing/troubleshooting
- Can use more router resources

Dynamic Routes

- We are going to use OSPF
- OSPF is very fast and optimal for dynamic routing
- Easy in configuration

OSPF configuration

- Add correct network to OSPF
- OSPF protocol will be enabled



OSPF LAB

LAB

- Check route table
- Try to ping other neighbor now
- Remember, additional knowledge required to run OSPF on the big network

Summary

Local Network Management

Access to Local Network

- Plan network design carefully
- Take care of user's local access to the network
- Use RouterOS features to secure local network resources

ARP

- Address Resolution Protocol
- ARP joins together client's IP address with MAC-address
- ARP operates dynamically, but can also be manually configured

ARP Table

ARP table
provides: IP
address,
MAC-address
and Interface

	IP Address	MAC Address	Interface
D	10.5.8.235	00:04:23:8E:BB:64	ether1
D	192.168.100.96	00:17:F2:35:02:CE	ether2
D	192.168.100.200	00:1C:42:C3:26:57	ether2

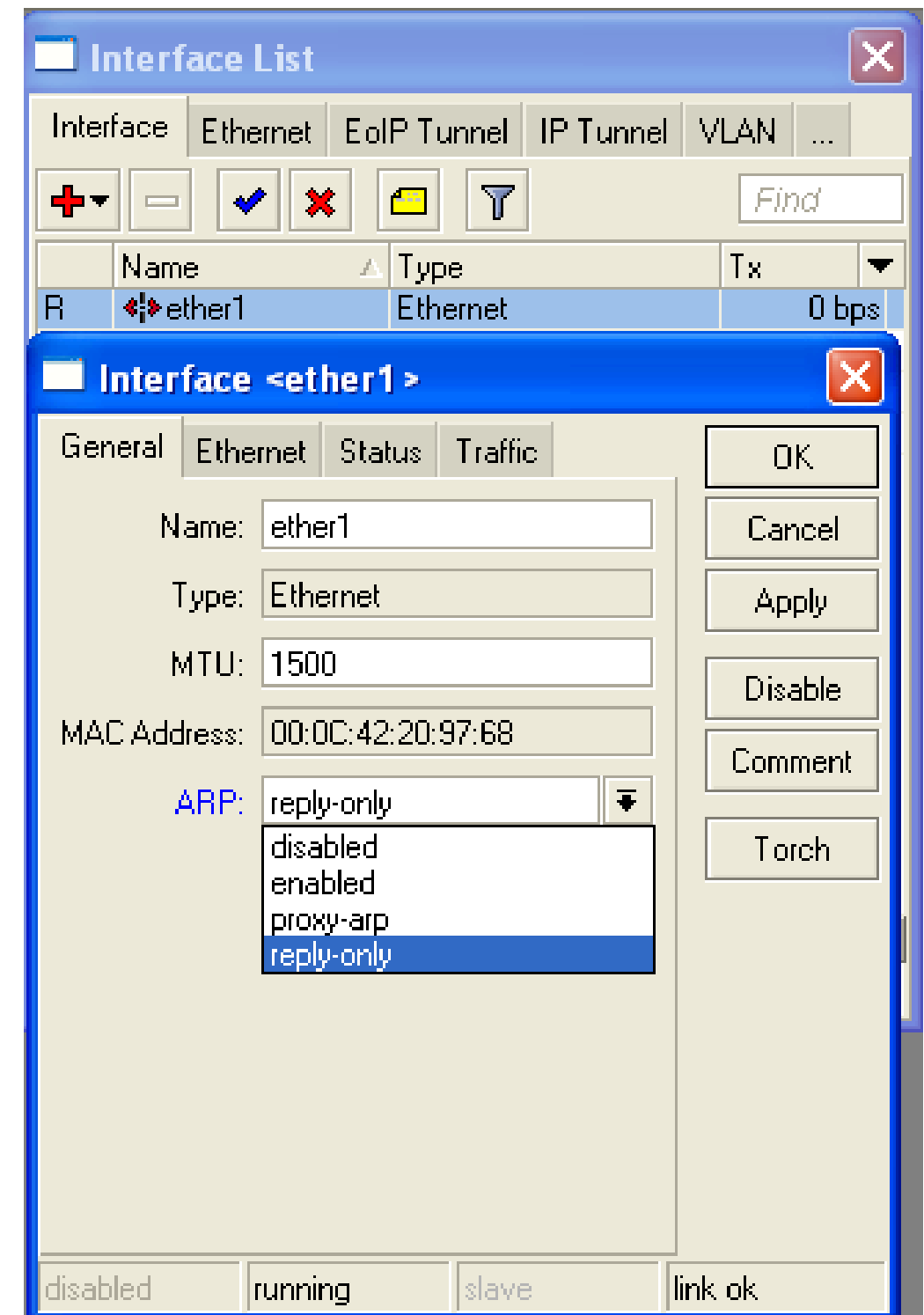
3 items

Static ARP table

- To increase network security ARP entries can be created manually
- Router's client will not be able to access Internet with changed IP address

Static ARP configuration

- Add Static Entry to ARP table
- Set for interface arp=reply-only to disable dynamic ARP creation
- Disable/enable interface or reboot router



Static ARP Lab

- Make your laptop ARP entry as static
- Set arp=reply-only to Local Network interface
- Try to change computer IP address
- Test Internet connectivity

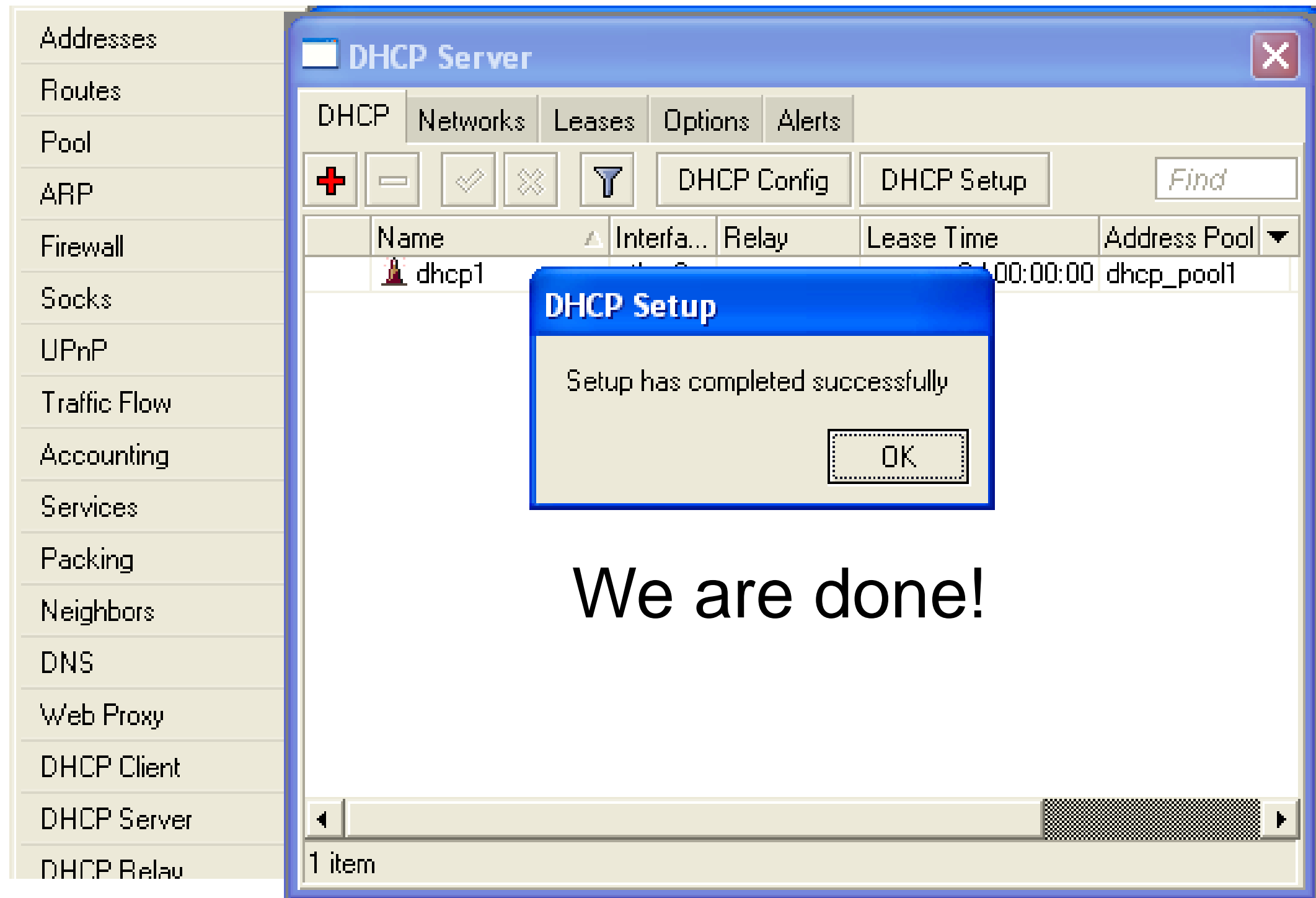
DHCP Server

- Dynamic Host Configuration Protocol
- Used for automatic IP address distribution over local network
- Use DHCP only in secure networks

DHCP Server

- To setup DHCP server you should have IP address on the interface
- Use setup command to enable DHCP server
- It will ask you for necessary information

DHCP-Server Setup



Important

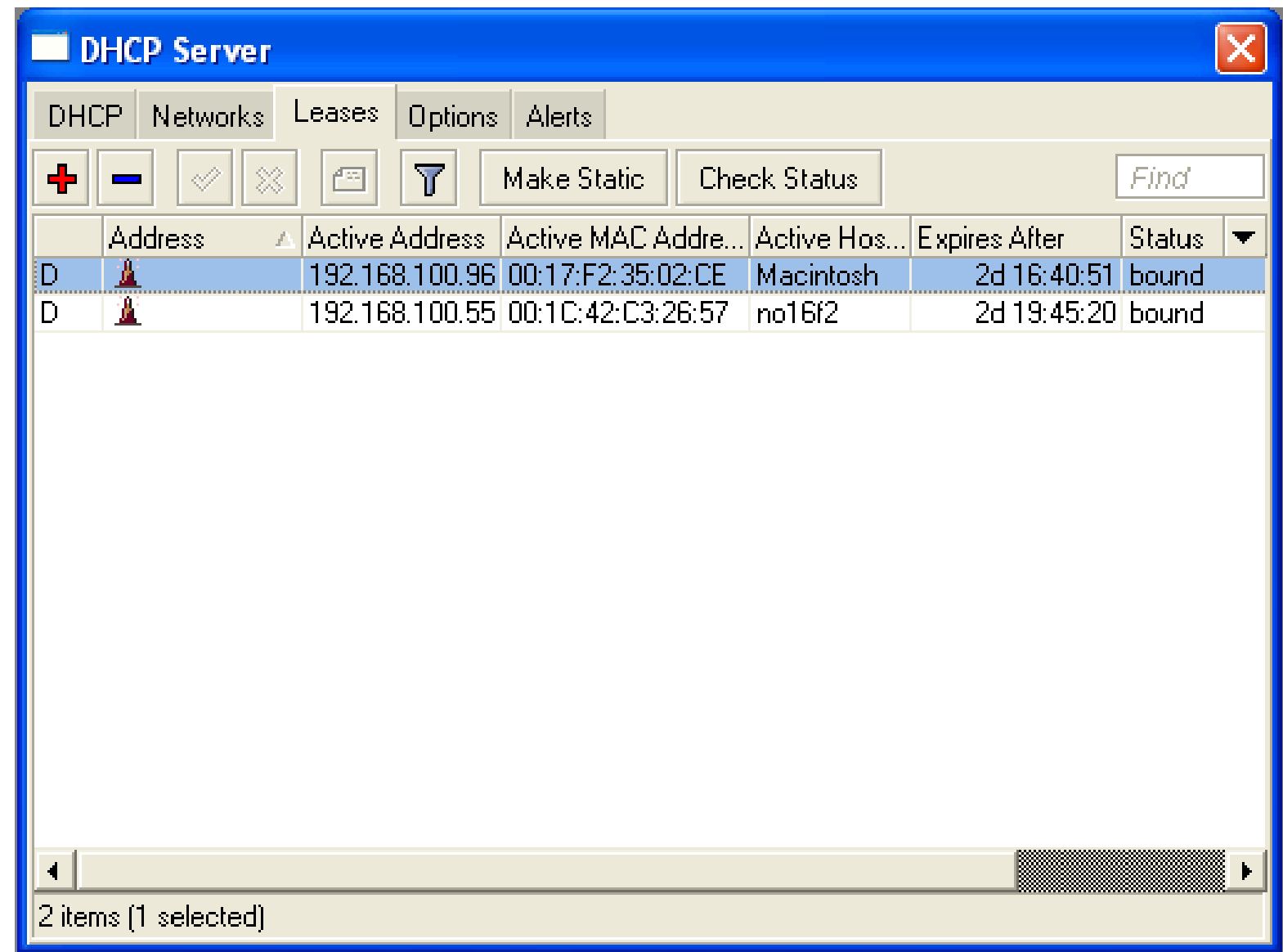
- To configure **DHCP server** on **bridge**, set server on **bridge interface**
- DHCP server will be **invalid**, when it is configured on **bridge port**



DHCP Server Lab

- Setup DHCP server on Ethernet Interface where Laptop is connected
- Change computer Network settings and enable DHCP-client (Obtain an IP address Automatically)
- Check the Internet connectivity

DHCP Server Information

Leases provide
information about
DHCP clients



	Address	Active Address	Active MAC Address	Active Hostname	Expires After	Status
D		192.168.100.96	00:17:F2:35:02:CE	Macintosh	2d 16:40:51	bound
D		192.168.100.55	00:1C:42:C3:26:57	no16f2	2d 19:45:20	bound

2 items (1 selected)

Winbox Configuration Tip

Show or
hide
different
Winbox
columns

The screenshot shows the Winbox DHCP Server configuration window, specifically the 'Leases' tab. The window displays a table of DHCP leases with columns: Address, Active Address, Active MAC Address, Active Host Name, Expires After, and Status. A red arrow points to the 'Status' column header, which has a dropdown menu open. The menu includes options like 'Show Categories', 'Detail Mode', 'Inline Comments', 'Show Columns', 'Find', 'Find Next', 'Select All', and 'Add'. The 'Show Columns' option is selected, and a sub-menu is visible showing a list of columns with checkboxes next to them, indicating which columns are currently displayed.

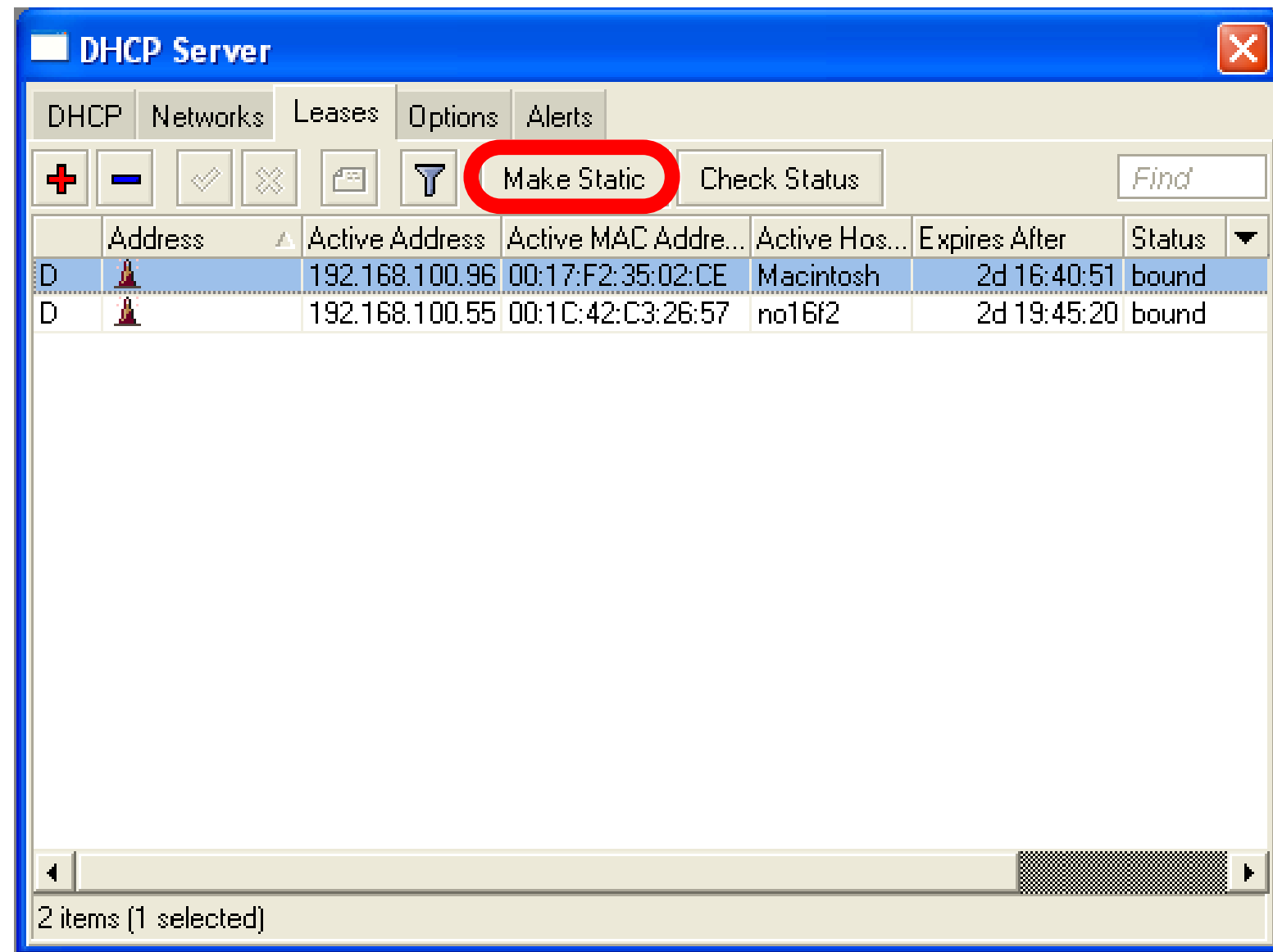
	Address	Active Address	Active MAC Address	Active Host Name	Expires After	Status
D	192.168.100.96	00:17:F2:35:02:CE	Macintosh	2d 16:38:28	bou	
D	192.168.100.55	00:1C:42:C3:26:57	no16f2	2d 19:42:57	bou	

2 items (1 selected)

- Show Categories
- Detail Mode
- Inline Comments
- Show Columns
 - ✓ Address
 - MAC Address
 - Use Src. MAC Address
 - Client ID
 - Server
 - Lease Time
 - Block Access
 - Always Broadcast
 - Rate Limit
 - ✓ Active Address
 - ✓ Active MAC Address
 - Active Client ID
 - ✓ Active Host Name
 - Active Server
 - ✓ Expires After
 - Agent Circuit Id
 - Agent Remote Id
 - ✓ Status
- Find (Ctrl+F)
- Find Next (Ctrl+G)
- Select All (Ctrl+A)
- Add (A)

Static Lease

- We can make lease to be static
- Client will not get other IP address

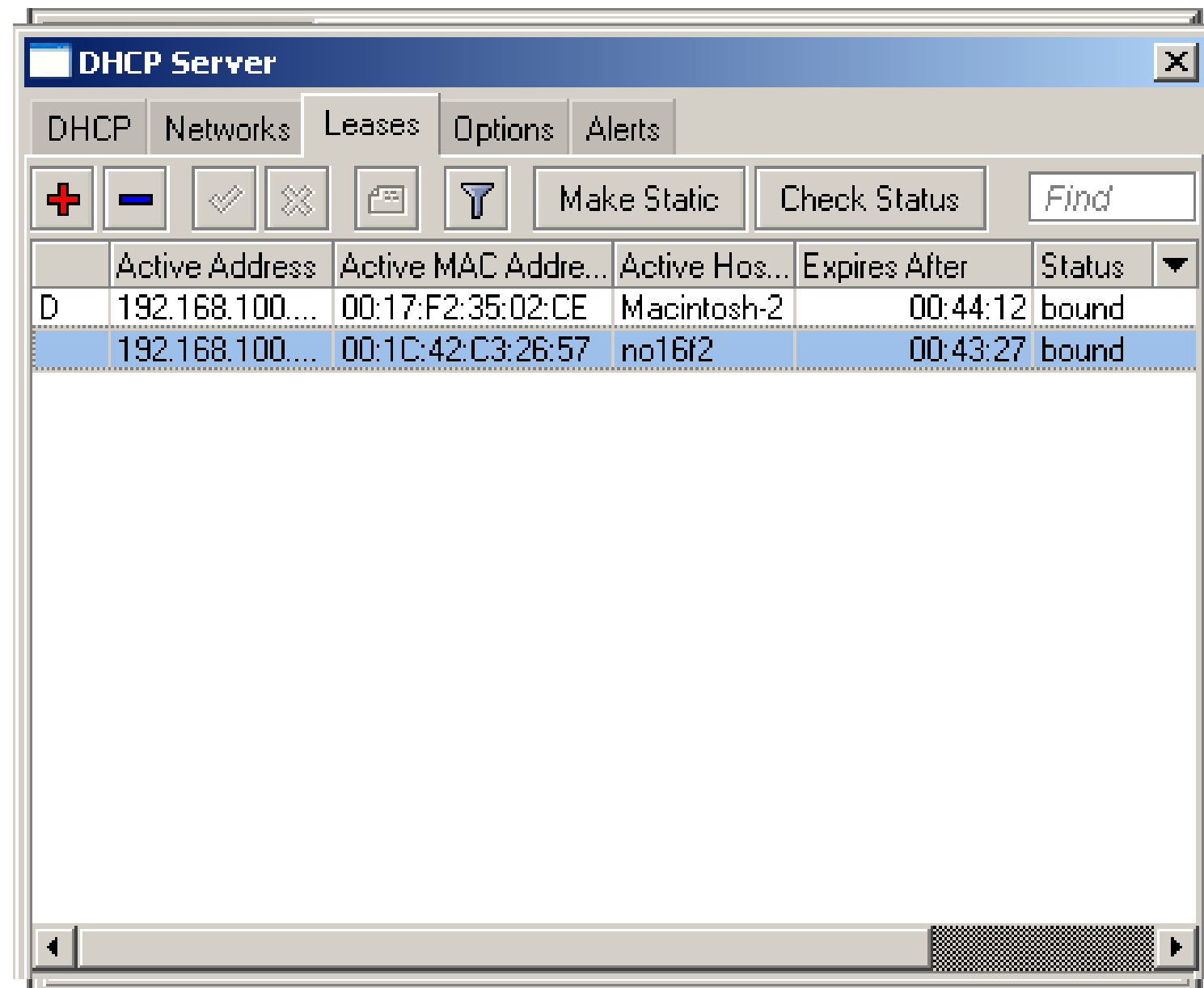


Static Lease

- DHCP-server could run without dynamic leases
- Clients will receive only preconfigured IP address

Static Lease

- Set Address-Pool to static-only
- Create Static leases



HotSpot

HotSpot

- Tool for Instant Plug-and-Play Internet access
- HotSpot provides authentication of clients before access to public network
- It also provides User Accounting

HotSpot Usage

- Open Access Points, Internet Cafes, Airports, universities campuses, etc.
- Different ways of authorization
- Flexible accounting

HotSpot Requirements

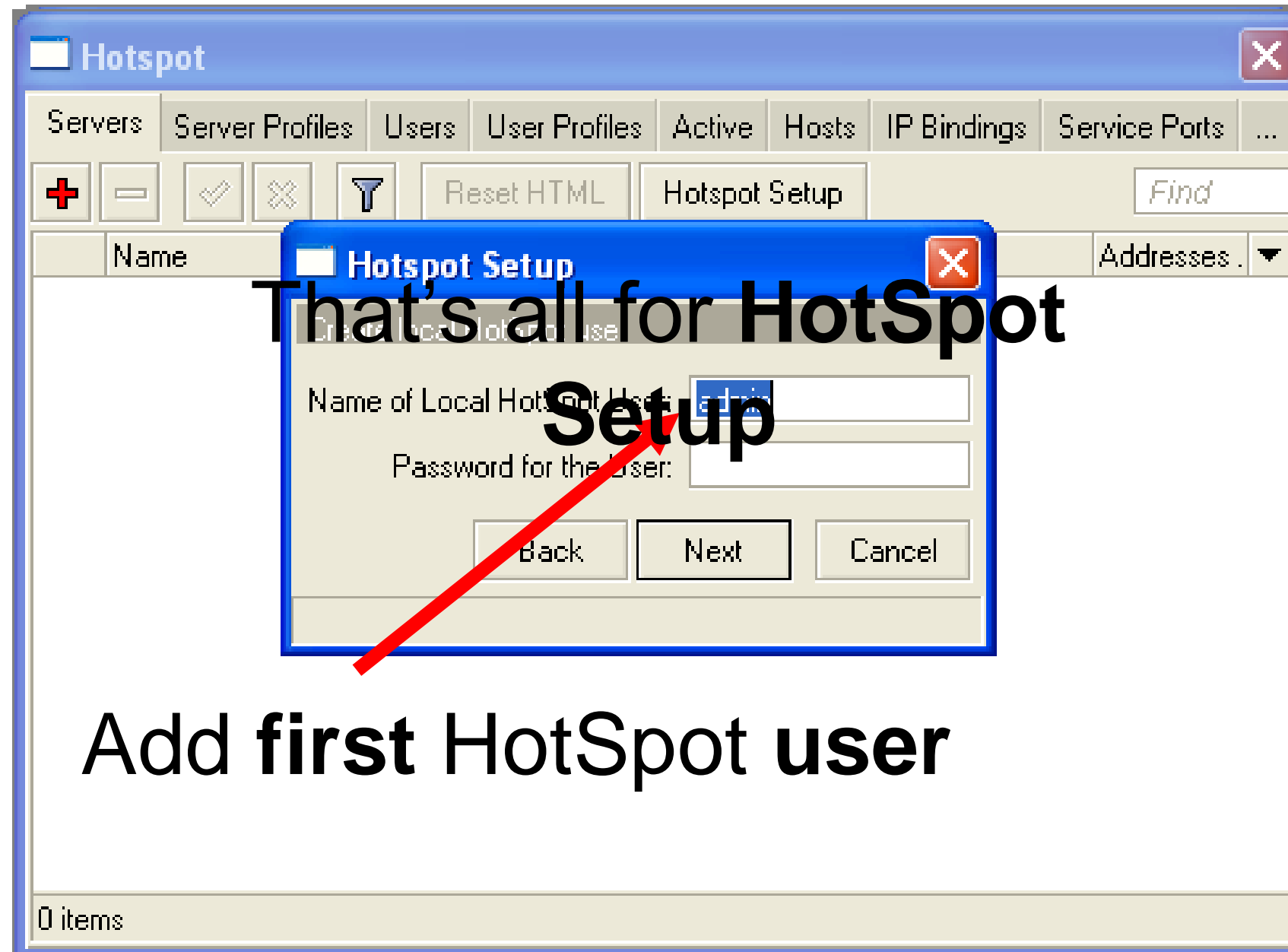
- Valid **IP addresses** on Internet and Local **Interfaces**
- DNS servers addresses added to **ip dns**
- At least one HotSpot user

HotSpot Setup

- HotSpot setup is easy
- Setup is similar to DHCP Server setup

HotSpot Setup

- Run **ip hotspot setup**
- Select Interface
- Proceed to answer the questions



Important Notes

- Users connected to HotSpot interface will be disconnected from the Internet
- Client will have to authorize in HotSpot to get access to Internet

Important Notes

- HotSpot default setup creates additional configuration:
 - **DHCP-Server** on HotSpot Interface
 - **Pool** for HotSpot Clients
 - Dynamic **Firewall** rules (Filter and NAT)

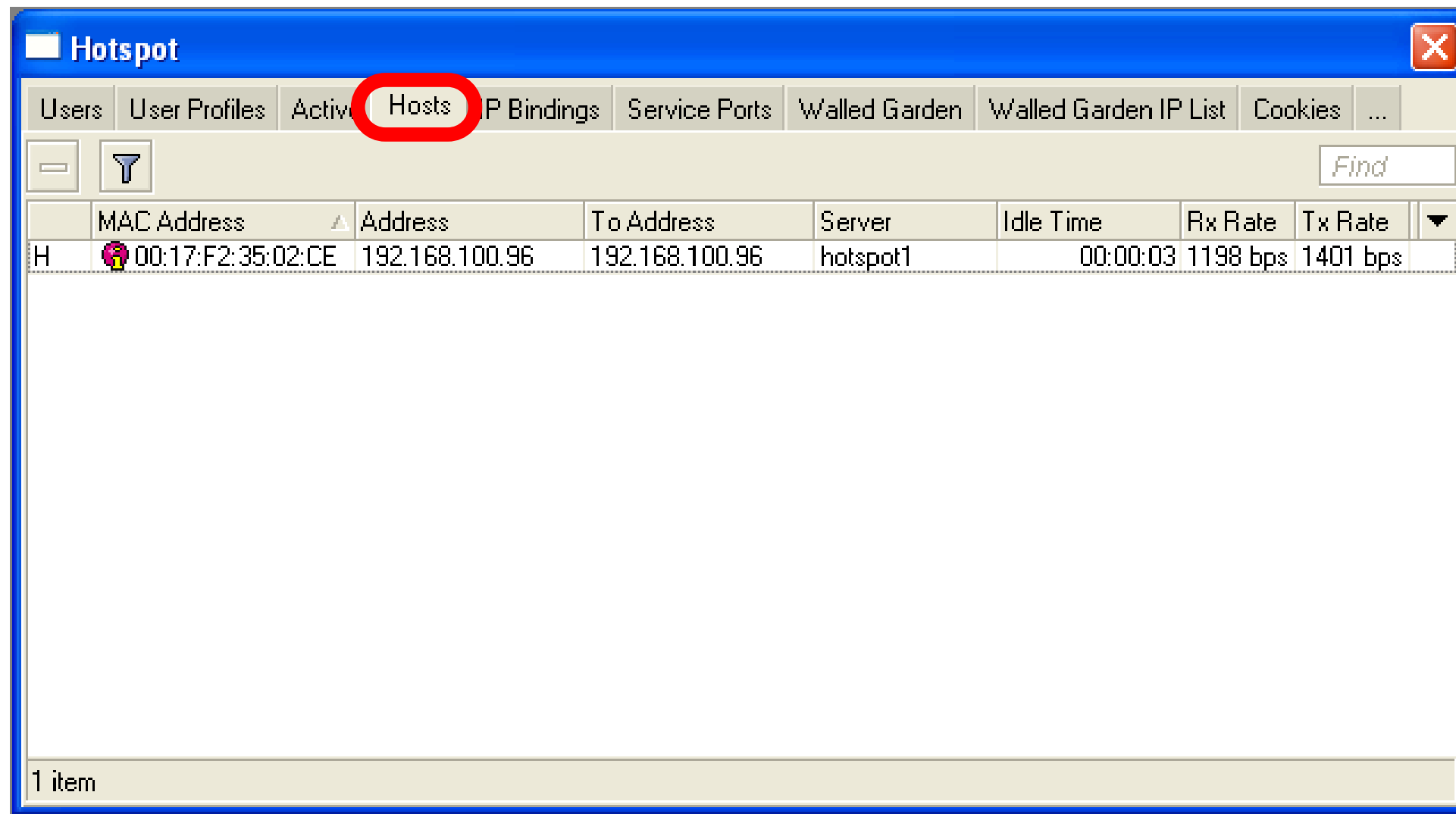
HotSpot Help

- HotSpot login page is provided when user tries to access any web-page
- To logout from HotSpot you need to go to http://router_IP or http://HotSpot_DNS

HotSpot Setup Lab

- Let's create HotSpot on local Interface
- Don't forget HotSpot login and password or you will not be able to get the Internet

HotSpot Network Hosts



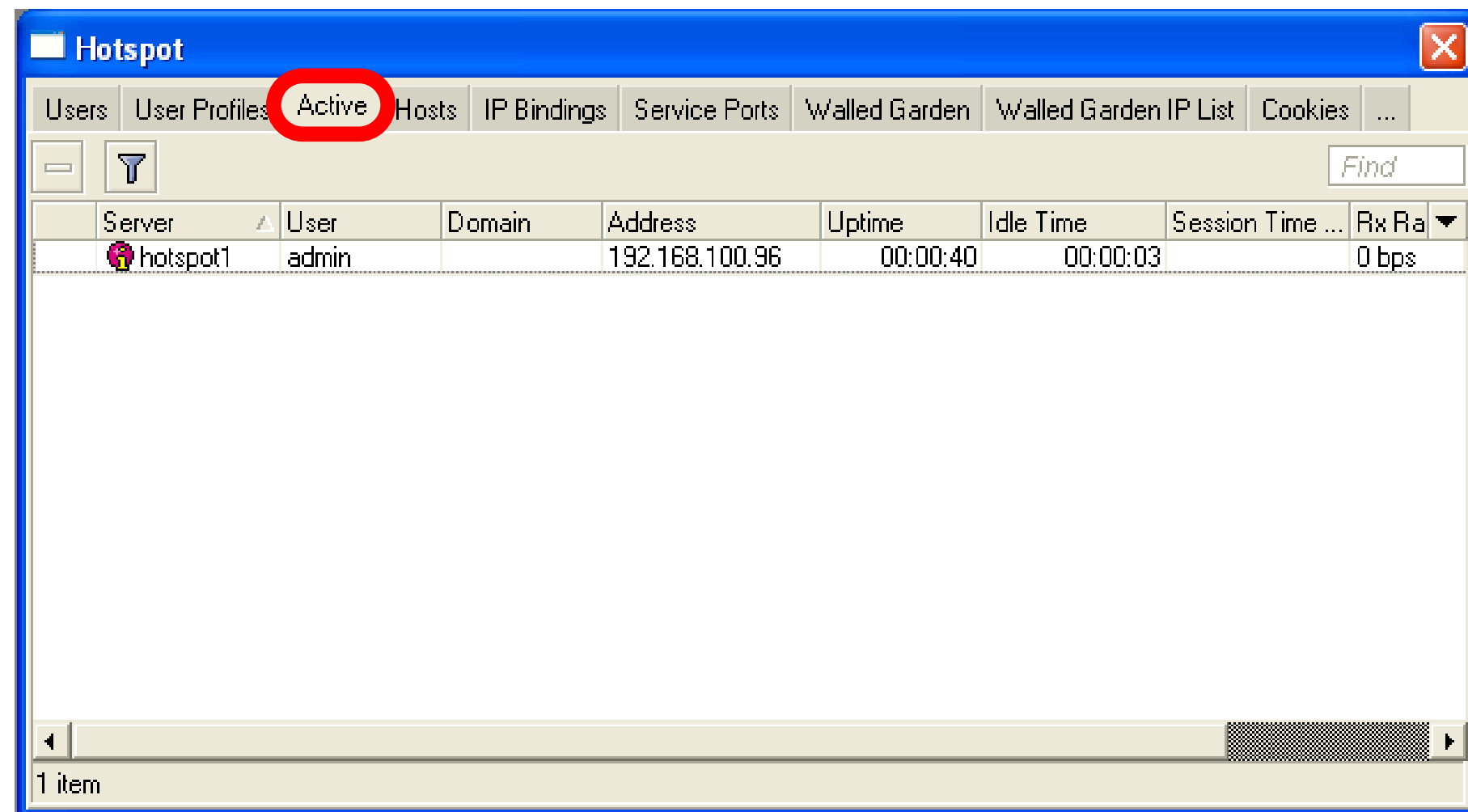
The screenshot shows a web-based management interface for a hotspot. The title bar is blue and says "Hotspot". Below it is a navigation menu with tabs: "Users", "User Profiles", "Active", "Hosts" (which is highlighted with a red circle), "IP Bindings", "Service Ports", "Walled Garden", "Walled Garden IP List", "Cookies", and "...". Below the tabs is a search bar with a "Find" button. The main area is a table with the following columns: "H", "MAC Address", "Address", "To Address", "Server", "Idle Time", "Rx Rate", and "Tx Rate". There is one row of data. At the bottom left, it says "1 item".

H	MAC Address	Address	To Address	Server	Idle Time	Rx Rate	Tx Rate
	00:17:F2:35:02:CE	192.168.100.96	192.168.100.96	hotspot1	00:00:03	1198 bps	1401 bps

Information about clients connected to HotSpot router

HotSpot Active Table

Information
about
authorized
HotSpot clients

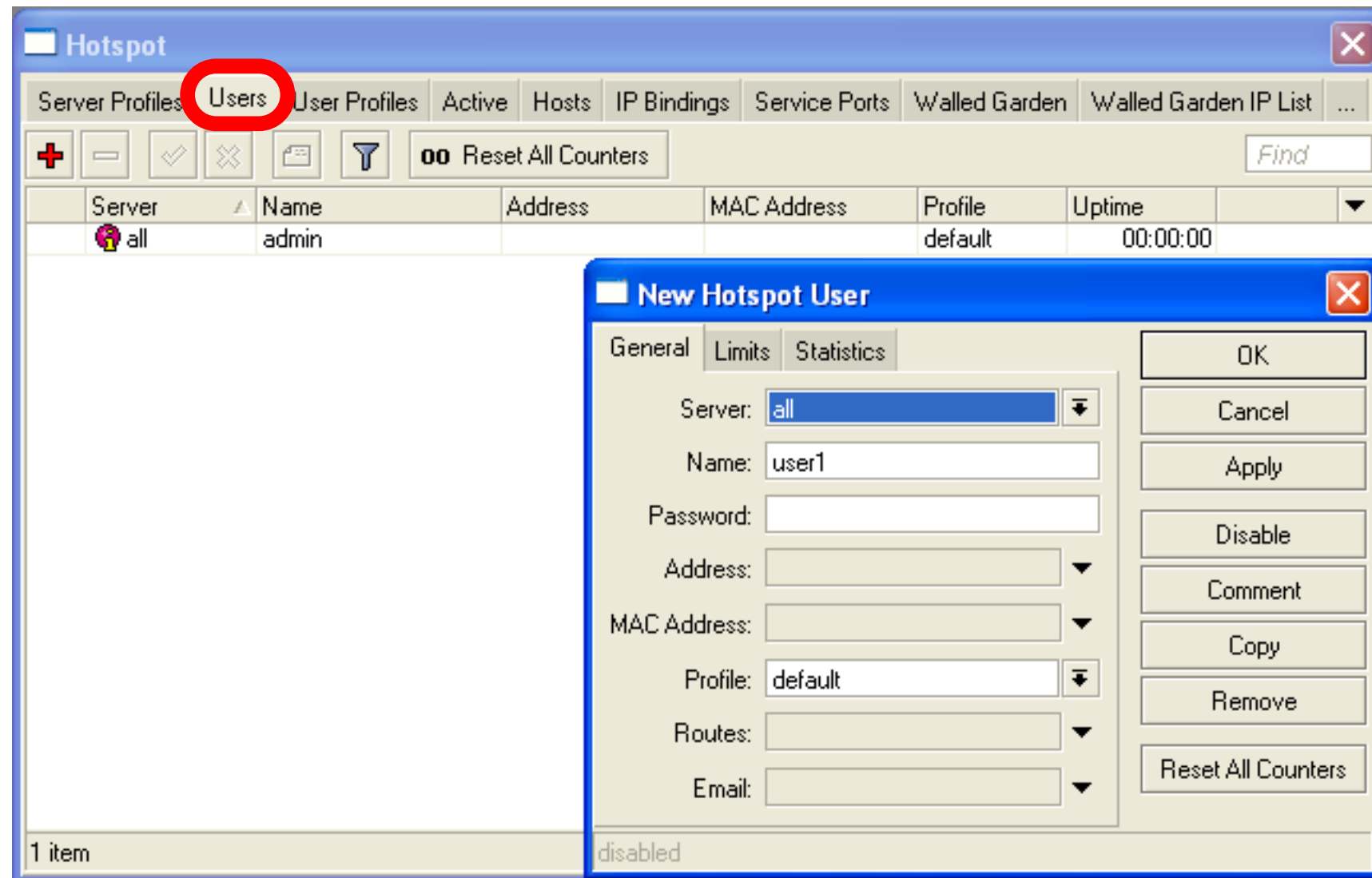


The screenshot shows a window titled "Hotspot" with a blue title bar. Below the title bar is a tabbed interface with tabs for "Users", "User Profiles", "Active", "Hosts", "IP Bindings", "Service Ports", "Walled Garden", "Walled Garden IP List", and "Cookies". The "Active" tab is selected and highlighted with a red circle. Below the tabs is a search bar with a "Find" button. The main area displays a table with the following columns: Server, User, Domain, Address, Uptime, Idle Time, Session Time, and Rx/Rx. The table contains one row of data: Server: hotspot1, User: admin, Domain: (empty), Address: 192.168.100.96, Uptime: 00:00:40, Idle Time: 00:00:03, Session Time: (empty), and Rx/Rx: 0 bps. At the bottom of the window, a status bar indicates "1 item".

Server	User	Domain	Address	Uptime	Idle Time	Session Time	Rx/Rx
hotspot1	admin		192.168.100.96	00:00:40	00:00:03		0 bps

User Management

Add/Edit/Remove
HotSpot users



HotSpot Walled-Garden

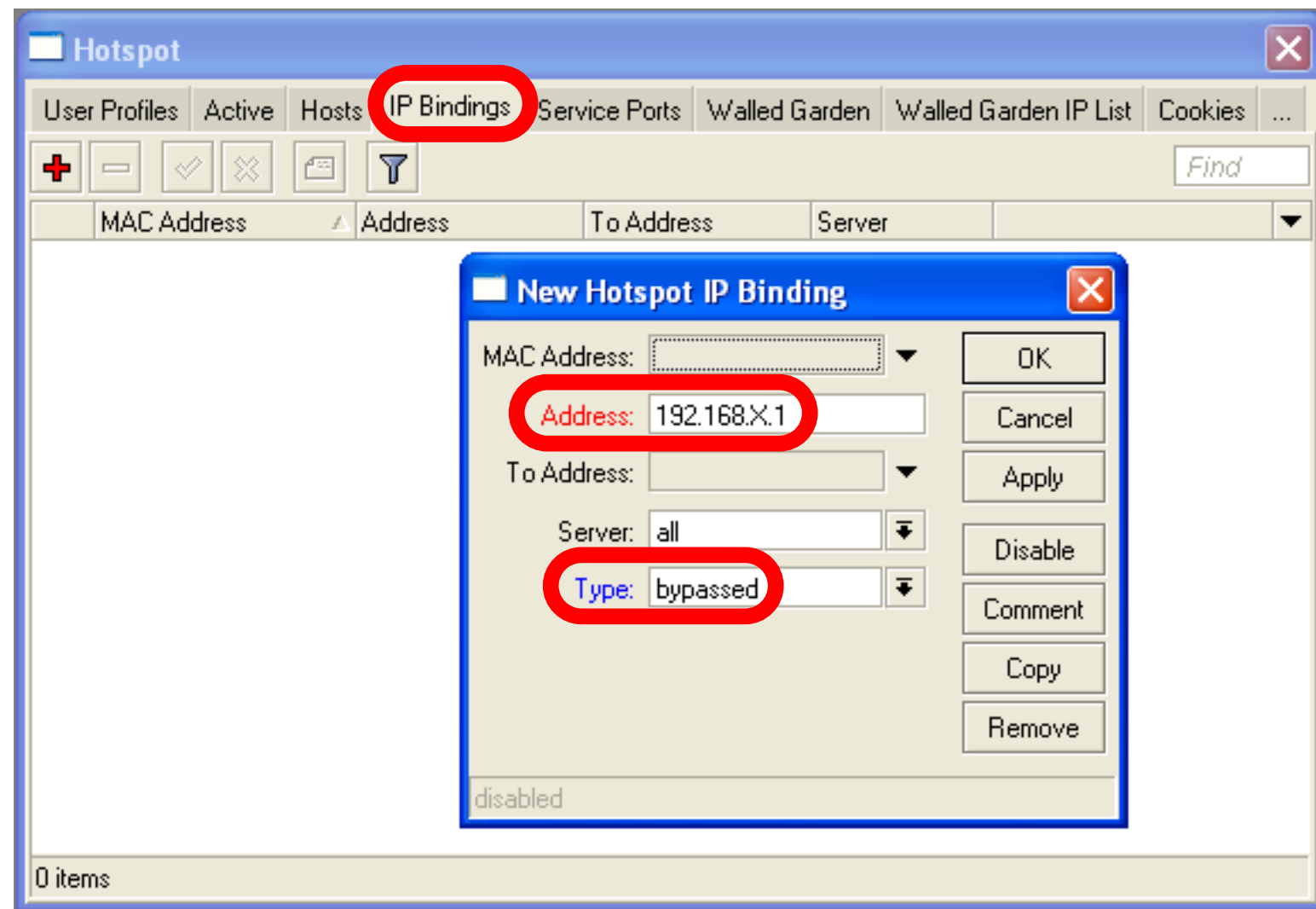
- Tool to get access to specific resources without HotSpot authorization
- Walled-Garden for HTTP and HTTPS
- Walled-Garden IP for other resources (Telnet, SSH, Winbox, etc.)

Allow access to mikrotik.com



Bypass HotSpot

- Bypass specific clients over HotSpot
- VoIP phones, printers, superusers
- IP-binding is used for that

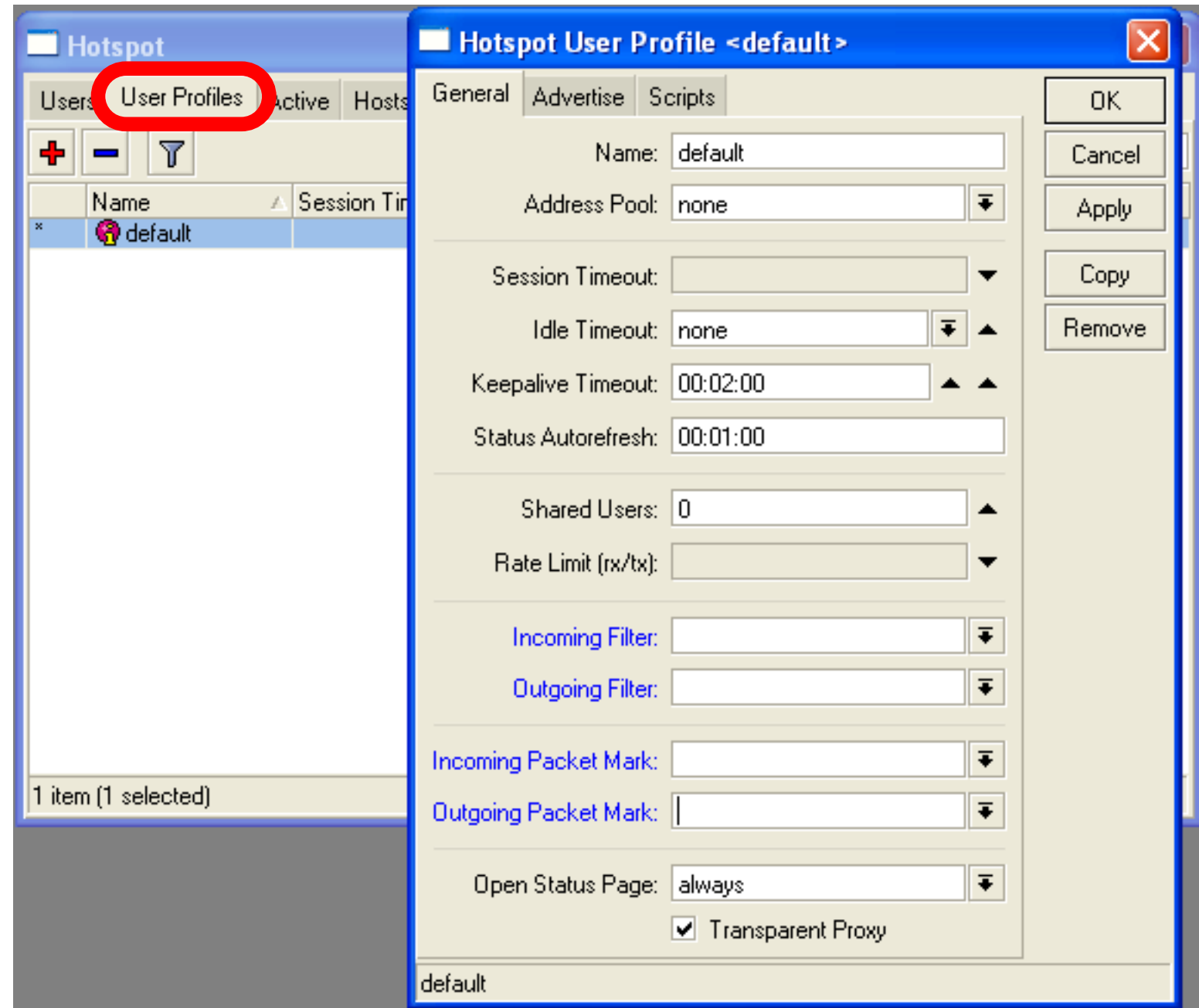


HotSpot Bandwidth Limits

- It is possible to set every HotSpot user with automatic bandwidth limit
- Dynamic queue is created for every client from profile

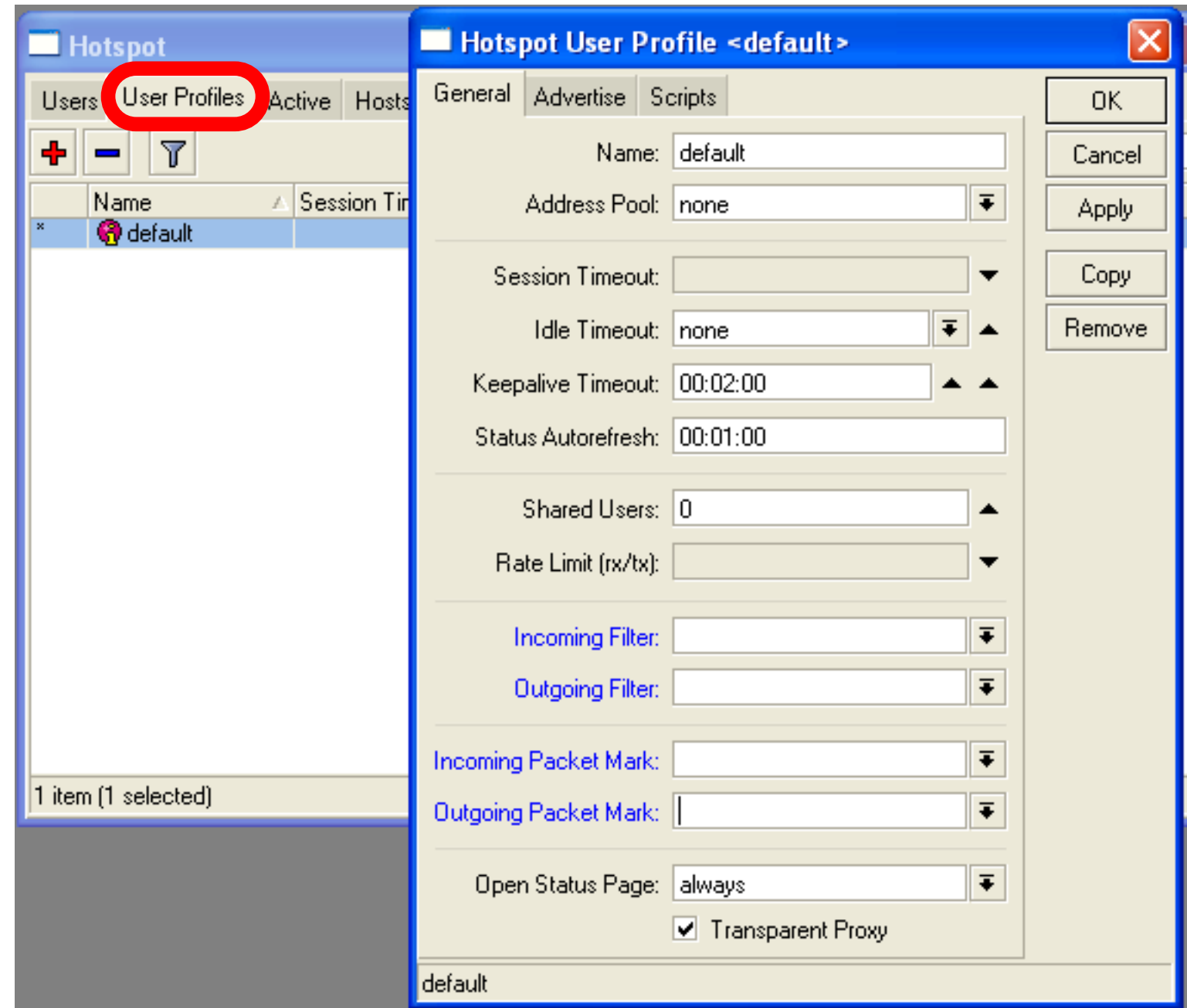
HotSpot User Profile

User Profile - set of options used for specific group of HotSpot clients



HotSpot Advanced Lab

To give each client
64k upload and
128k download, set
Rate Limit



HotSpot Lab

- Add second user
- Allow access to www.mikrotik.com without HotSpot authentication for your laptop
- Add Rate-limit 1M/1M for your laptop

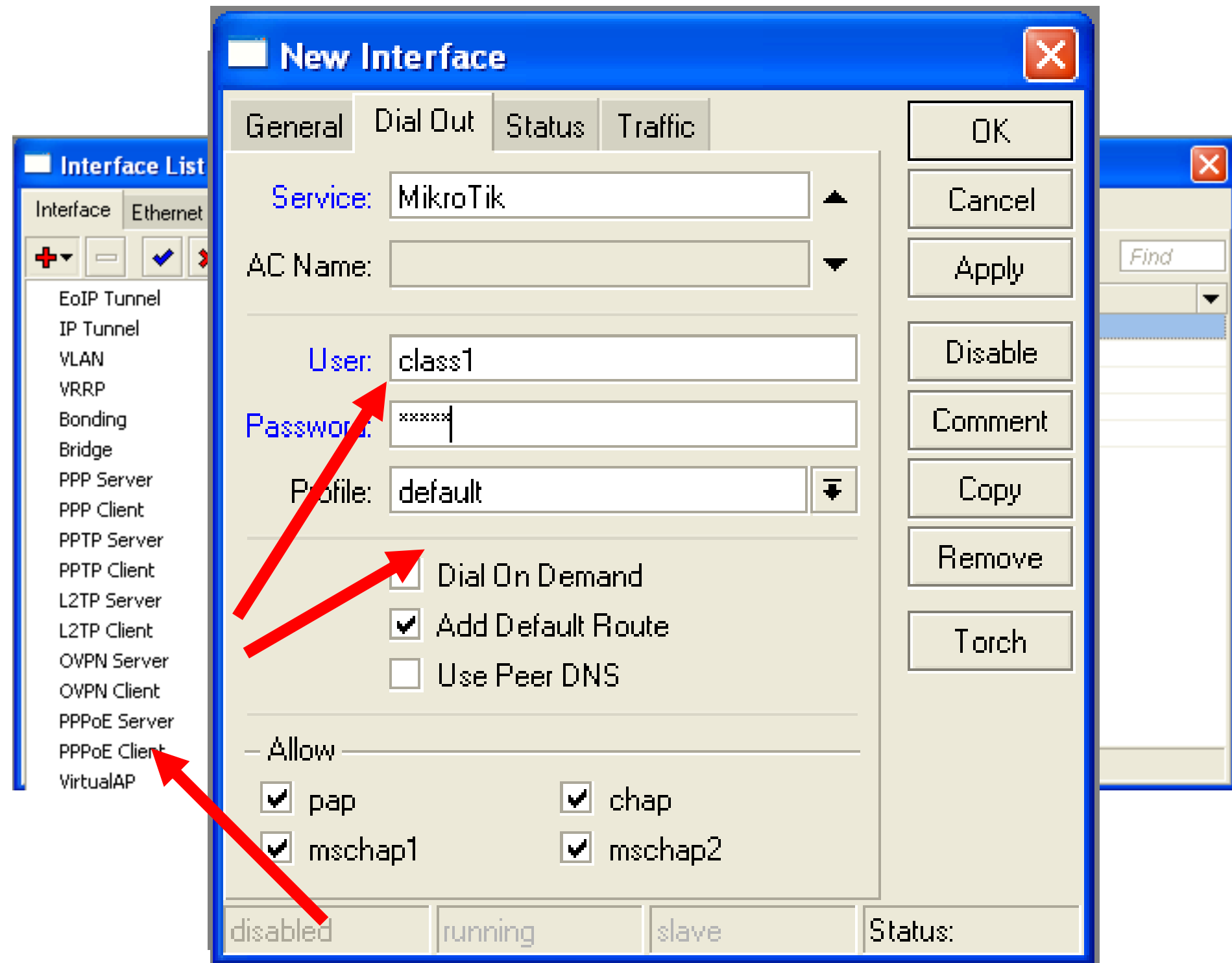
Tunnels

PPPoE

- Point to Point Protocol over Ethernet is often used to control client connections for DSL, cable modems and plain Ethernet networks
- MikroTik RouterOS supports PPPoE client and PPPoE server

PPPoE Client Setup

- Add PPPoE client
- You need to set **Interface**
- Set **Login** and **Password**



PPPoE Client Lab

- Teachers are going to create PPPoE server on their router
- Disable DHCP-client on router's outgoing interface
- Set up PPPoE client on outgoing interface
- Set Username **class**, password **class**

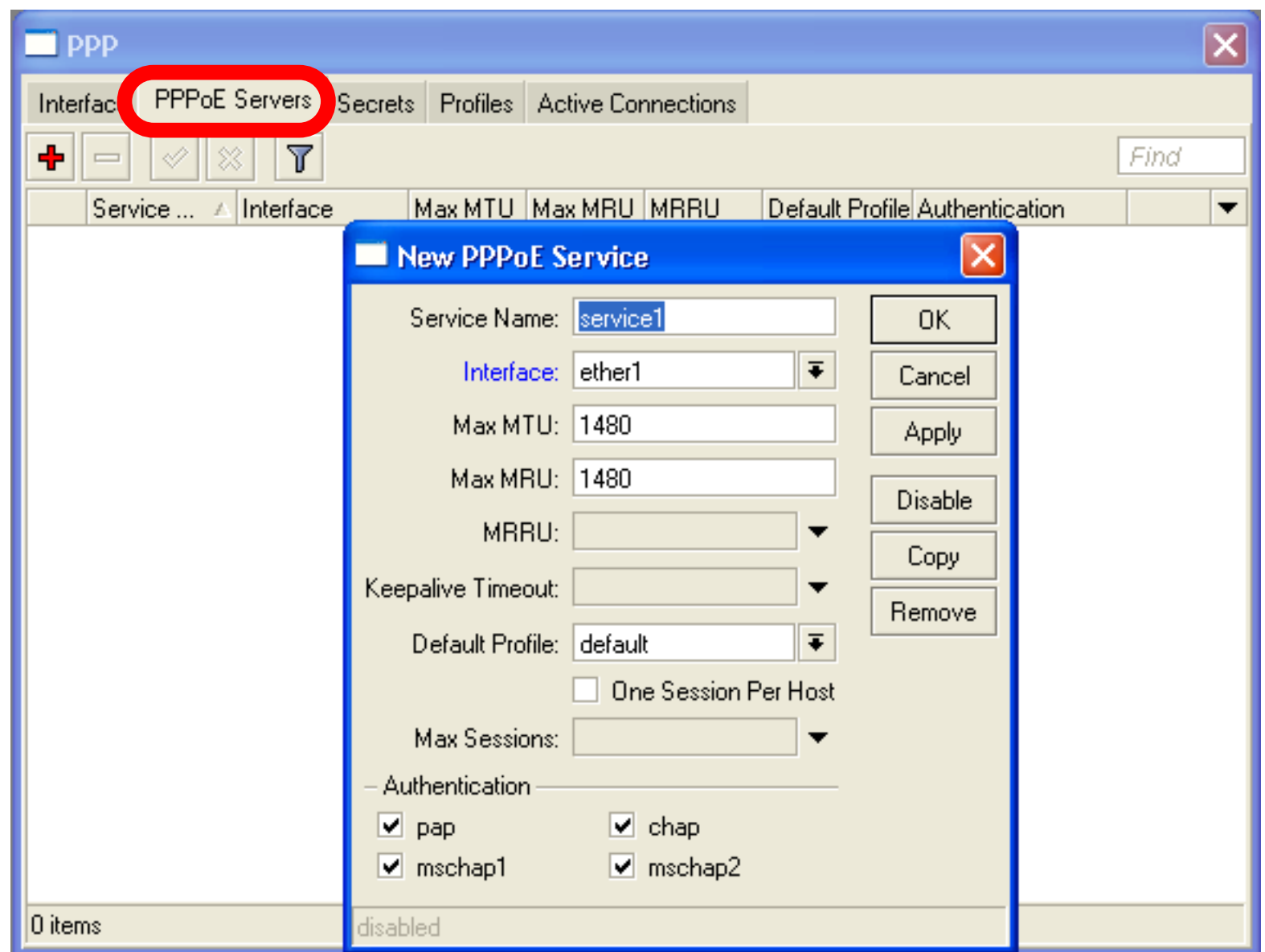
PPPoE Client Setup

- Check PPP connection
- Disable PPPoE client
- Enable DHCP client to restore old configuration

PPPoE Server Setup

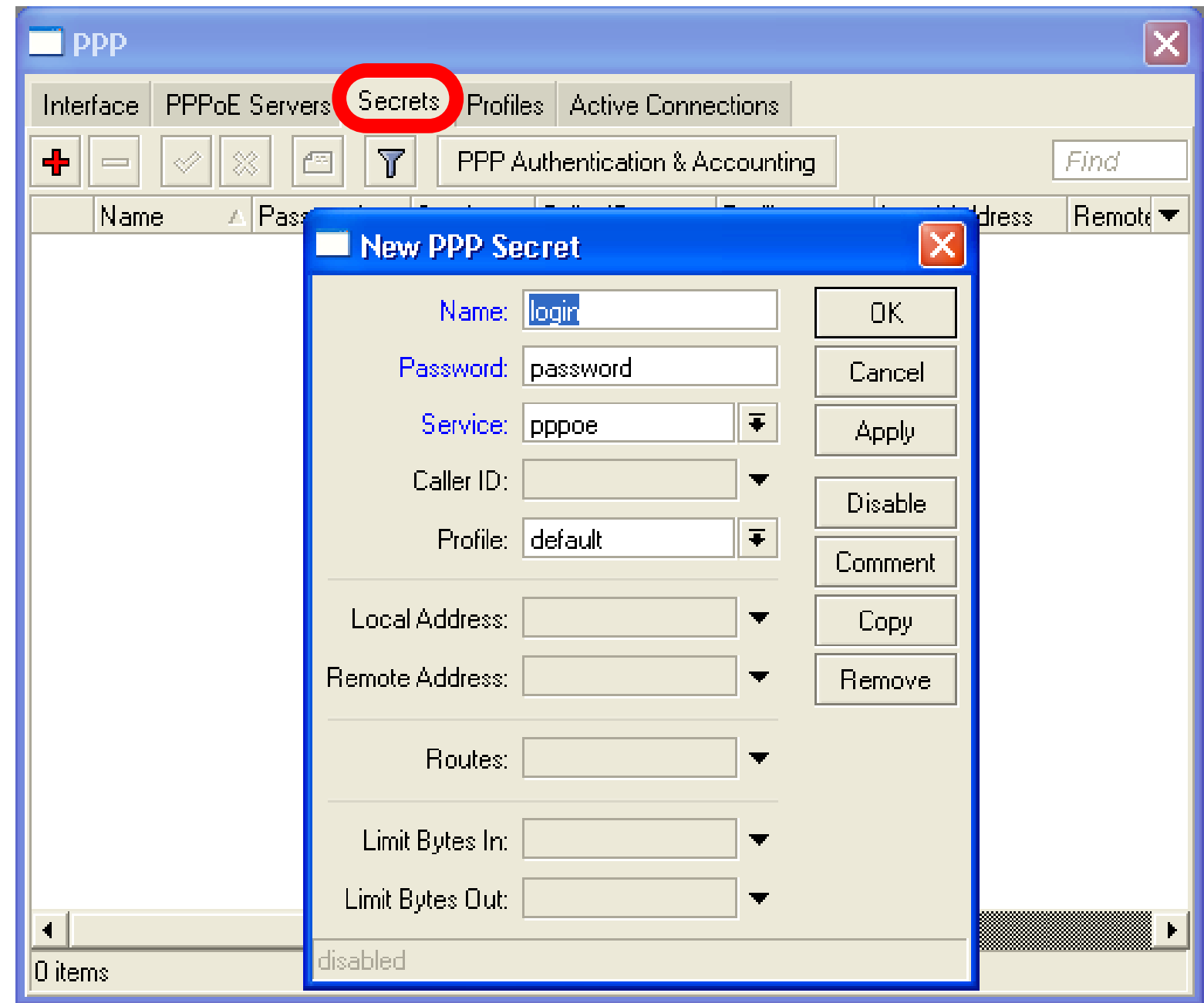
LAB

- Select Interface
- Select Profile



PPP Secret

- User's database
- Add login and Password
- Select service
- Configuration is taken from profile

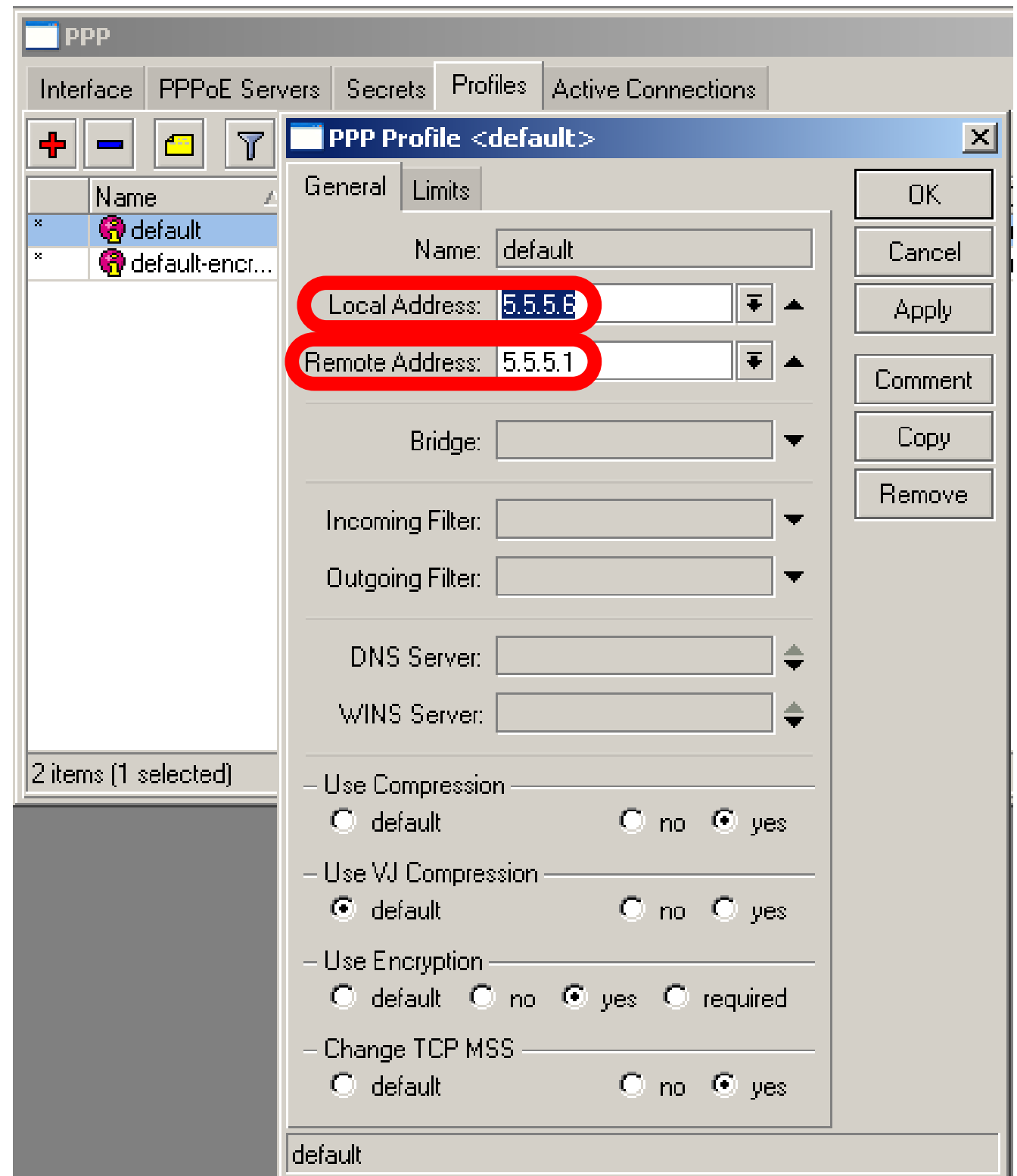


PPP Profiles

- Set of rules used for PPP clients
- The way to set same settings for different clients

PPP Profile

- **Local address -**
Server address
- **Remote Address**
- Client address



PPPoE

- Important, PPPoE server runs on the interface
- PPPoE interface can be without IP address configured
- For security, leave PPPoE interface without IP address configuration

Pools

- Pool defines the range of IP addresses for PPP, DHCP and HotSpot clients
- We will use a pool, because there will be more than one client
- Addresses are taken from pool automatically

Pool

The screenshot displays the Mikrotik WinBox interface. On the left sidebar, the 'Pool' menu item is highlighted with a red circle. The main window shows the 'IP Pool' configuration screen. At the top, there are two tabs: 'Pools' (selected) and 'Used Addresses'. Below the tabs are three icons: a red plus sign, a blue minus sign, and a funnel icon. A 'Find' search box is located on the right. The main area contains a table with the following data:

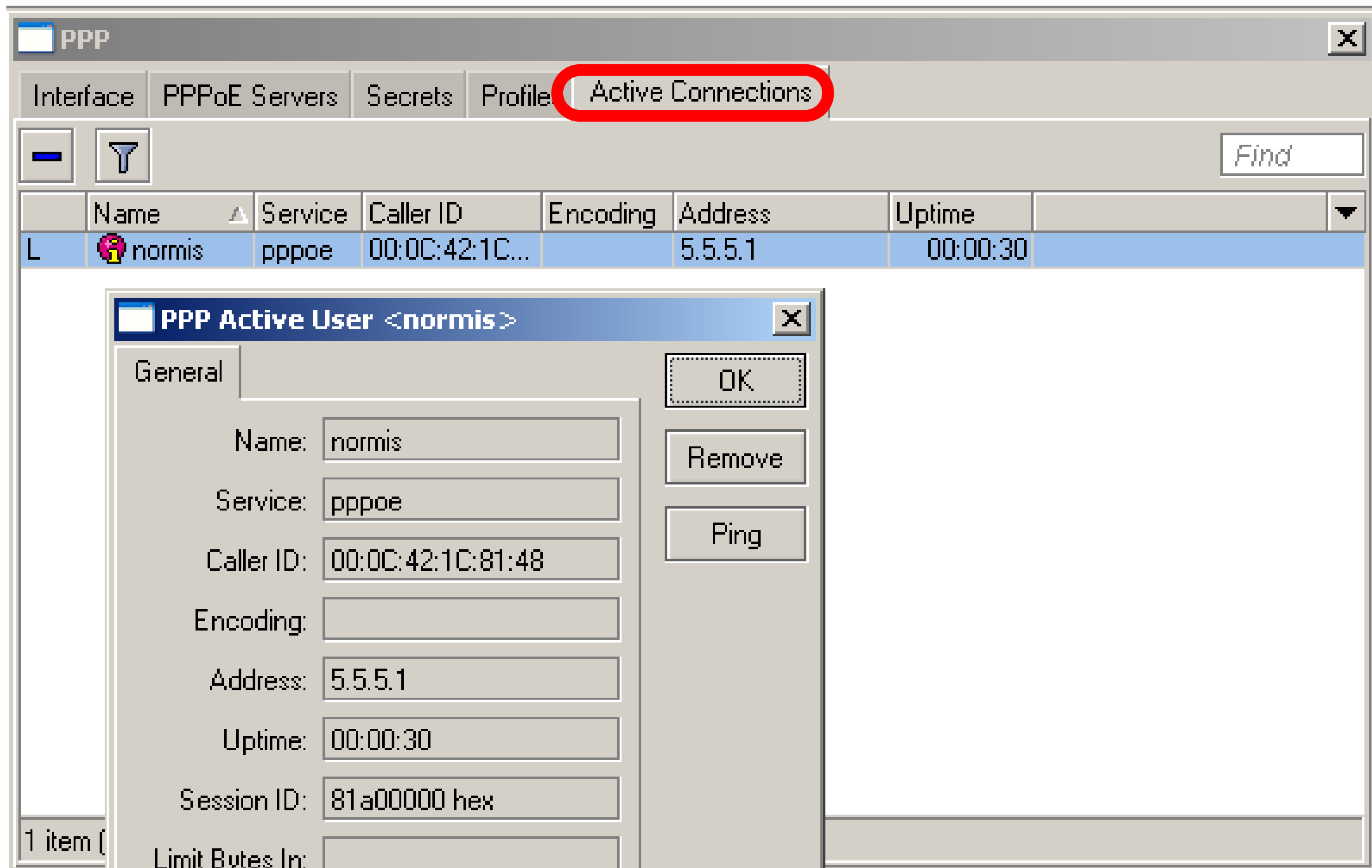
Name	Addresses	Next Pool
Pool	192.168.100.2-192.168.100.254	none

Below the table, a configuration dialog for the selected pool is open. The dialog has the title 'IP Pool <Pool>'. It contains the following fields and buttons:

- Name: Pool
- Addresses: 192.168.100.2-1
- Next Pool: none
- Buttons: OK, Cancel, Apply, Copy, Remove

At the bottom of the main window, a status bar indicates '1 item (1 selected)'.

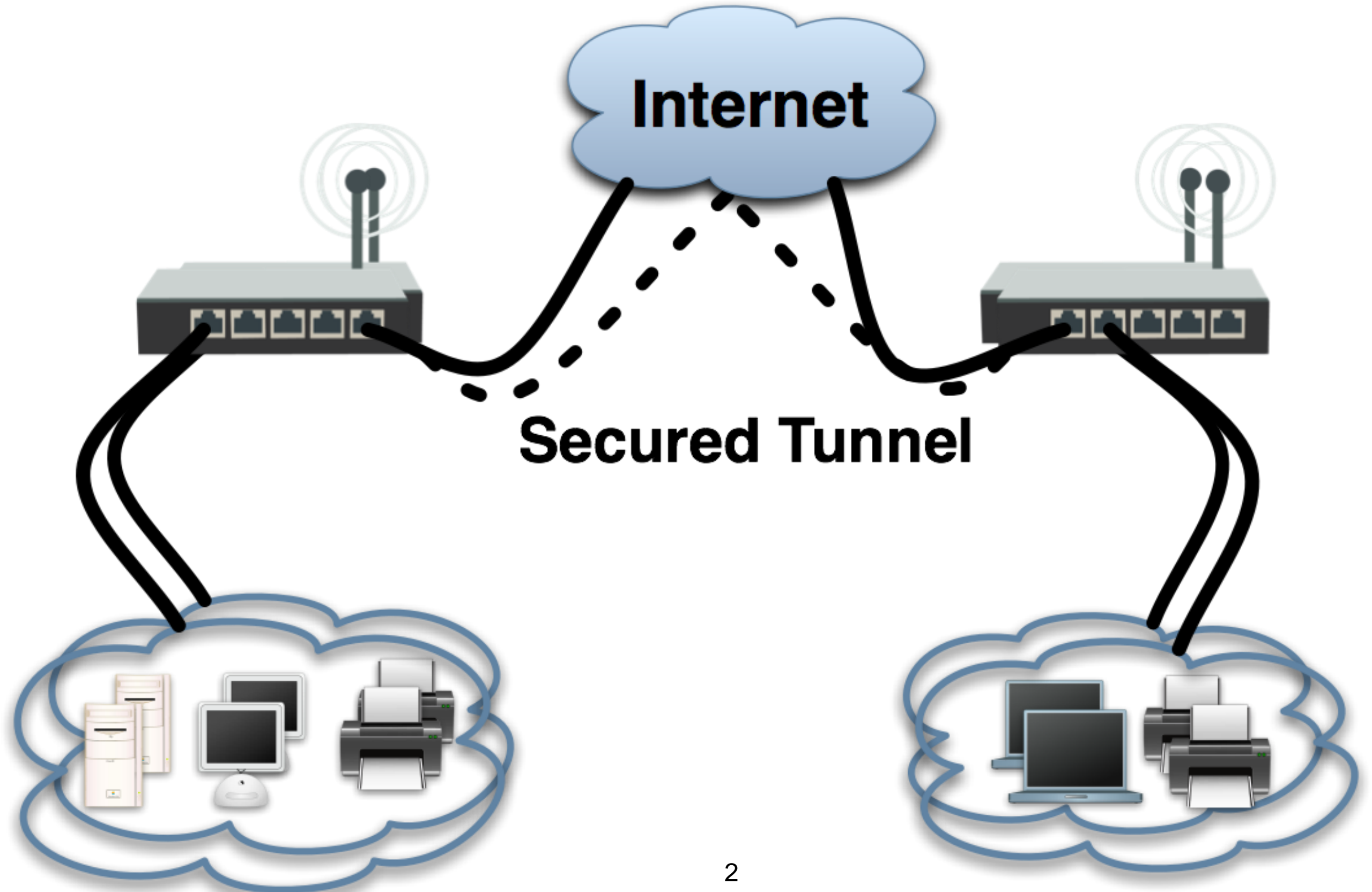
PPP Status



PPTP

- Point to Point Tunnel Protocol provides encrypted tunnels over IP
- MikroTik RouterOS includes support for PPTP client and server
- Used to secure link between Local Networks over Internet
- For mobile or remote clients to access company Local network resources

PPTP

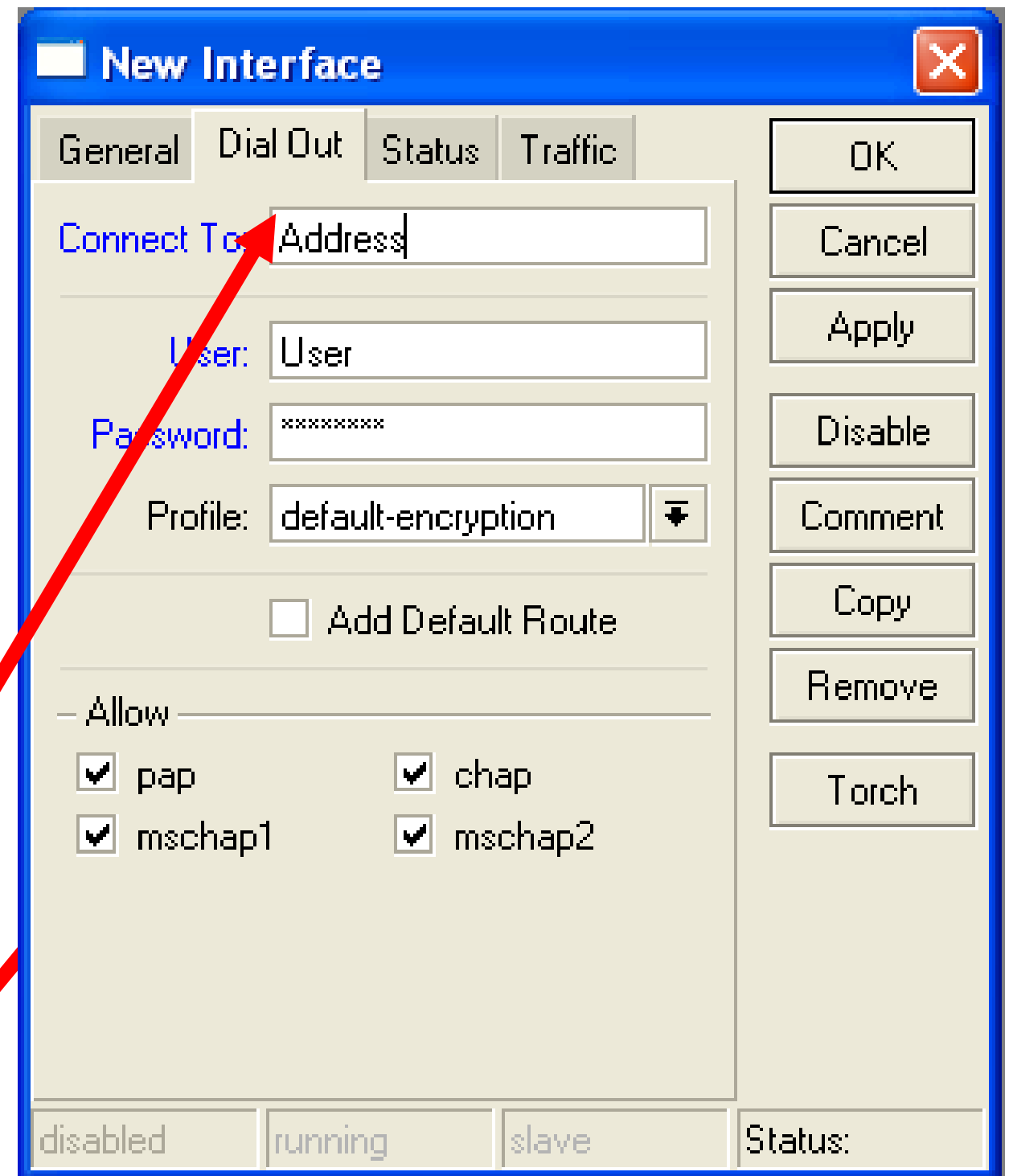


PPTP configuration

- PPTP configuration is very similar to PPPoE
- L2TP configuration is very similar to PPTP and PPPoE

PPTP client

- Add PPTP Interface
- Specify address of PPTP server
- Set login and password



The screenshot shows the 'New Interface' dialog box with the 'Dial Out' tab selected. A red arrow points from the 'Specify address of PPTP server' bullet point to the 'Connect To Address' text box. Another red arrow points from the 'Set login and password' bullet point to the 'User' and 'Password' text boxes. The 'Connect To Address' text box contains the word 'Address'. The 'User' text box contains the word 'User'. The 'Password' text box contains a series of asterisks. The 'Profile' dropdown menu is set to 'default-encryption'. The 'Add Default Route' checkbox is unchecked. The 'Allow' section has four checked options: 'pap', 'chap', 'mschap1', and 'mschap2'. The 'Status' section at the bottom shows 'disabled', 'running', and 'slave' buttons, with 'Status:' text to the right. On the right side of the dialog, there are buttons for 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', 'Remove', and 'Torch'.

New Interface

General Dial Out Status Traffic

Connect To Address

User: User

Password: xxxxxxxx

Profile: default-encryption

☐ Add Default Route

— Allow —

☒ pap ☒ chap

☒ mschap1 ☒ mschap2

disabled running slave Status:

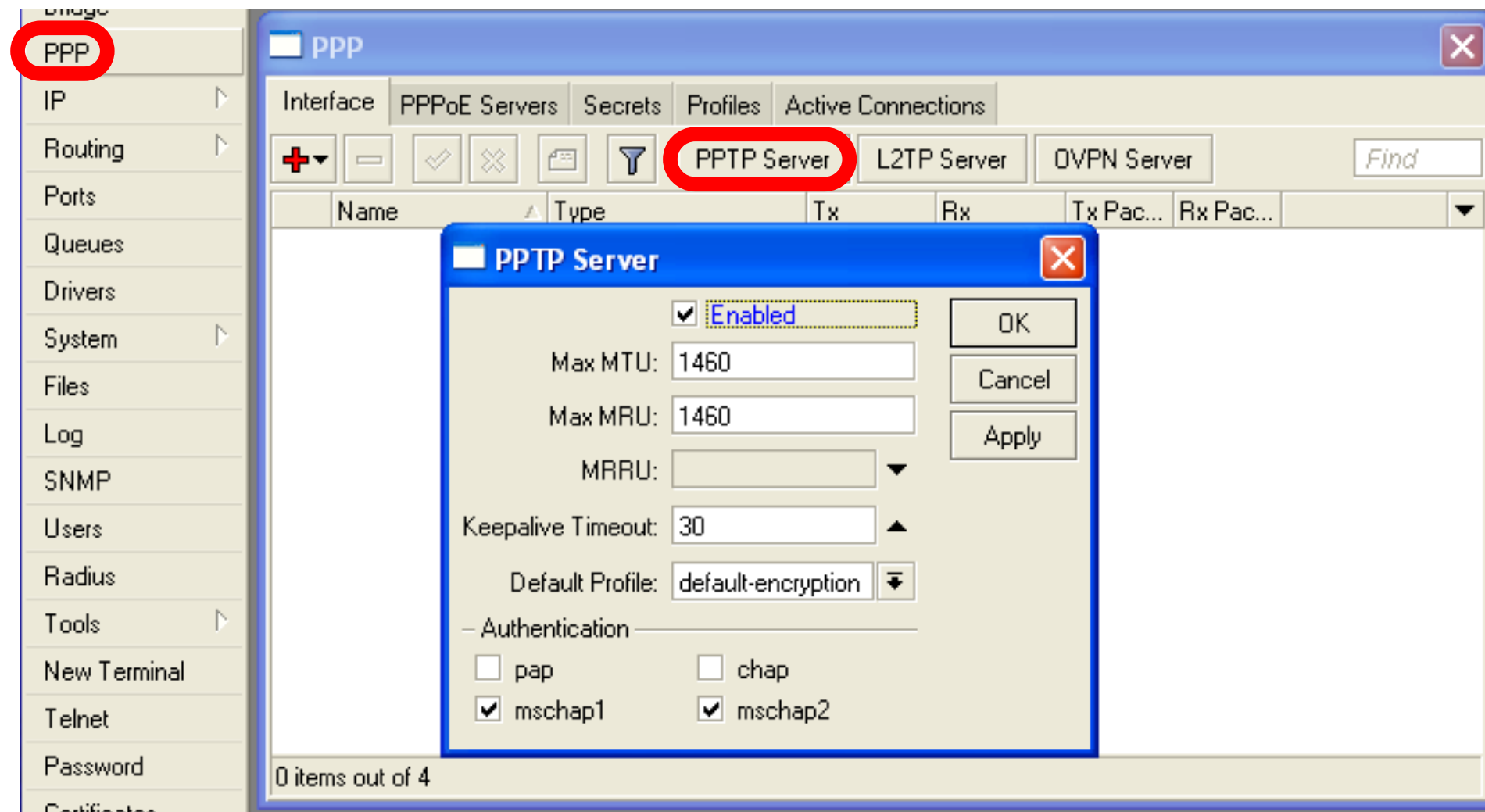
OK Cancel Apply Disable Comment Copy Remove Torch

PPTP Client

- That's all for PPTP client configuration
- Use Add Default Gateway to route all router's traffic to PPTP tunnel
- Use static routes to send specific traffic to PPTP tunnel

PPTP Server

- PPTP Server is able to maintain multiple clients
- It is easy to enable PPTP server



PPTP Server Clients

- PPTP client settings are stored in ppp secret
- ppp secret is used for PPTP, L2TP, PPPoE clients
- ppp secret database is configured on server

PPP Profile

- The same profile is used for PPTP, PPPoE, L2TP and PPP clients

PPTP Lab

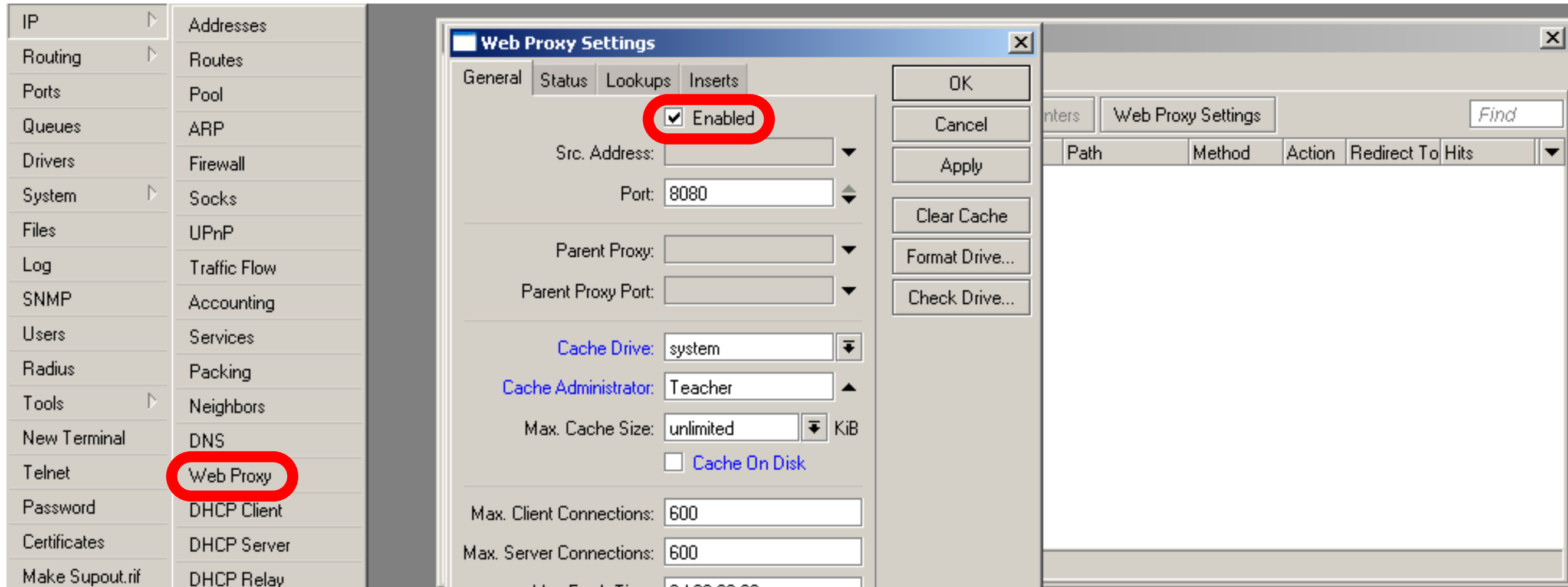
- Teachers are going to create PPTP server on Teacher's router
- Set up PPTP client on outgoing interface
- Use username **class** password **class**
- Disable PPTP interface

Proxy

What is Proxy

- It can speed up WEB browsing by caching data
- HTTP Firewall

Enable Proxy



The main option is **Enable**, other settings are optional

Transparent Proxy

- User need to set additional configuration to browser to use Proxy
- Transparent proxy allows to direct all users to proxy automatically

Transparent Proxy

- DST-NAT rules required for transparent proxy
- HTTP traffic should be redirected to router

The image displays two side-by-side screenshots of the Mikrotik WinBox NAT Rule configuration interface for a rule named "NAT Rule <80>".

Left Screenshot (General Tab):

- Chain:** dstnat (highlighted with a red circle)
- Protocol:** 6 (tcp) (highlighted with a red circle)
- Dst. Port:** 80 (highlighted with a red circle)

Right Screenshot (Action Tab):

- Action:** redirect
- To Ports:** 8080 (highlighted with a red circle)

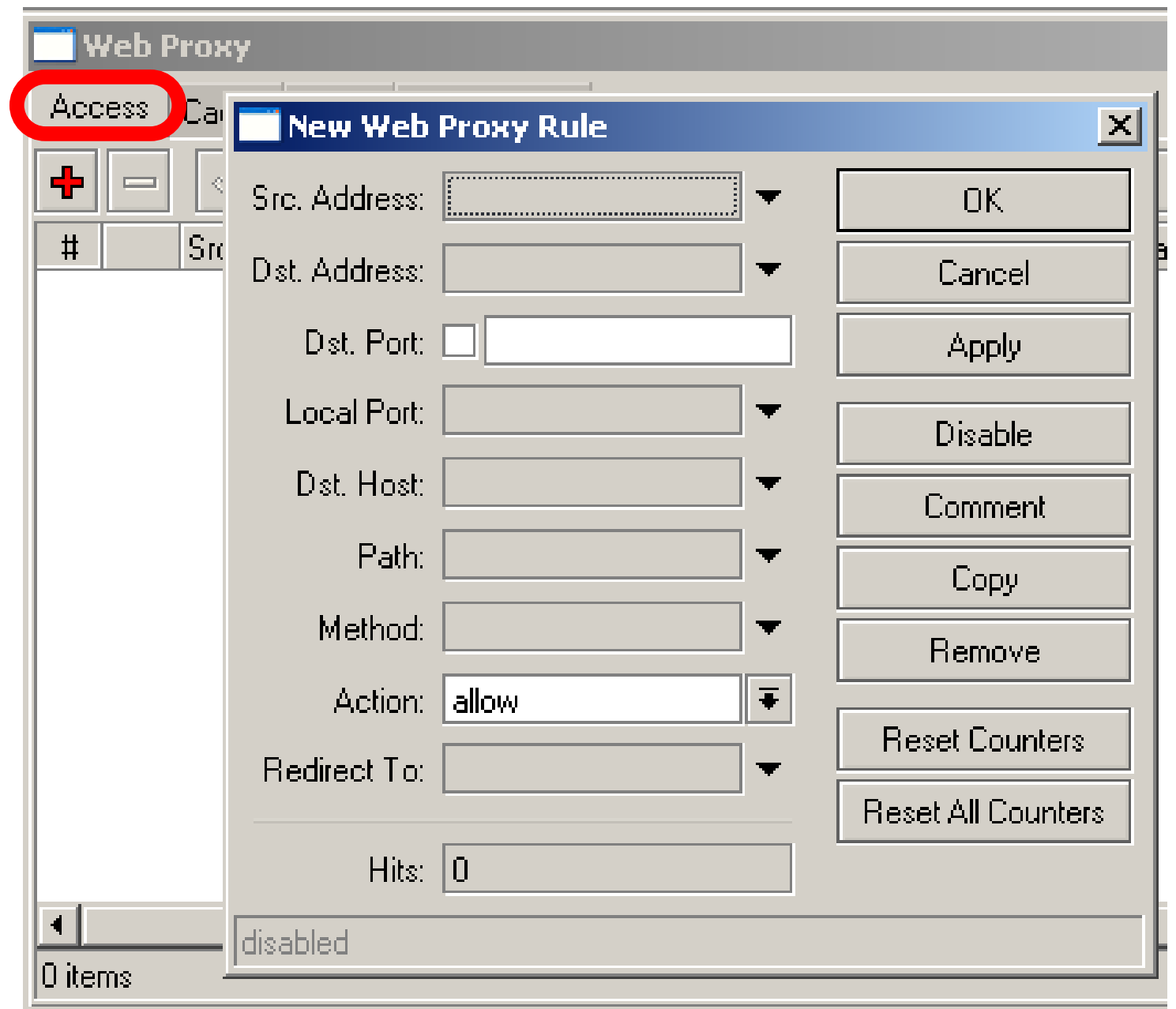
Both windows show the rule is currently **disabled** at the bottom. The right window includes additional tabs (Advanced, Extra, Action, Statistics) and a set of control buttons (OK, Cancel, Apply, Disable, Comment, Copy, Remove, Reset Counters, Reset All Counters) on the right side.

HTTP Firewall

- Proxy access list provides option to filter DNS names
- You can make redirect to specific pages

HTTP Firewall

- Dst-Host, webpage address
(<http://test.com>)
- Path, anything after
<http://test.com/PATH>



HTTP Firewall

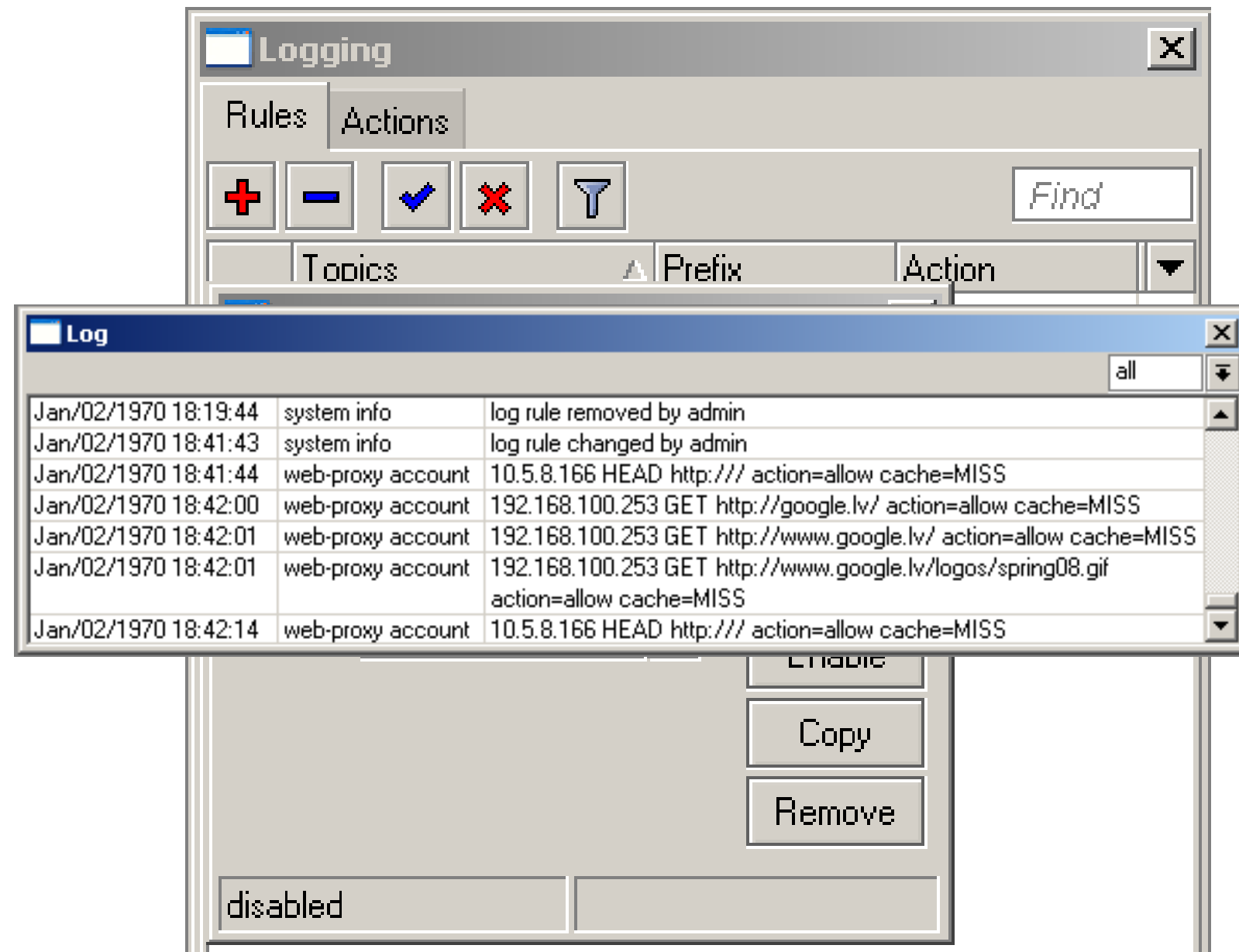
- Create rule to drop access for specific web-page
- Create rule to make redirect from unwanted web-page to your company page

Web-page logging

- Proxy can log visited Web-Pages by users
- Make sure you have enough resources for logs (it is better to send them to remote)

Web-Pages logging

- Add logging rule
- Check logs

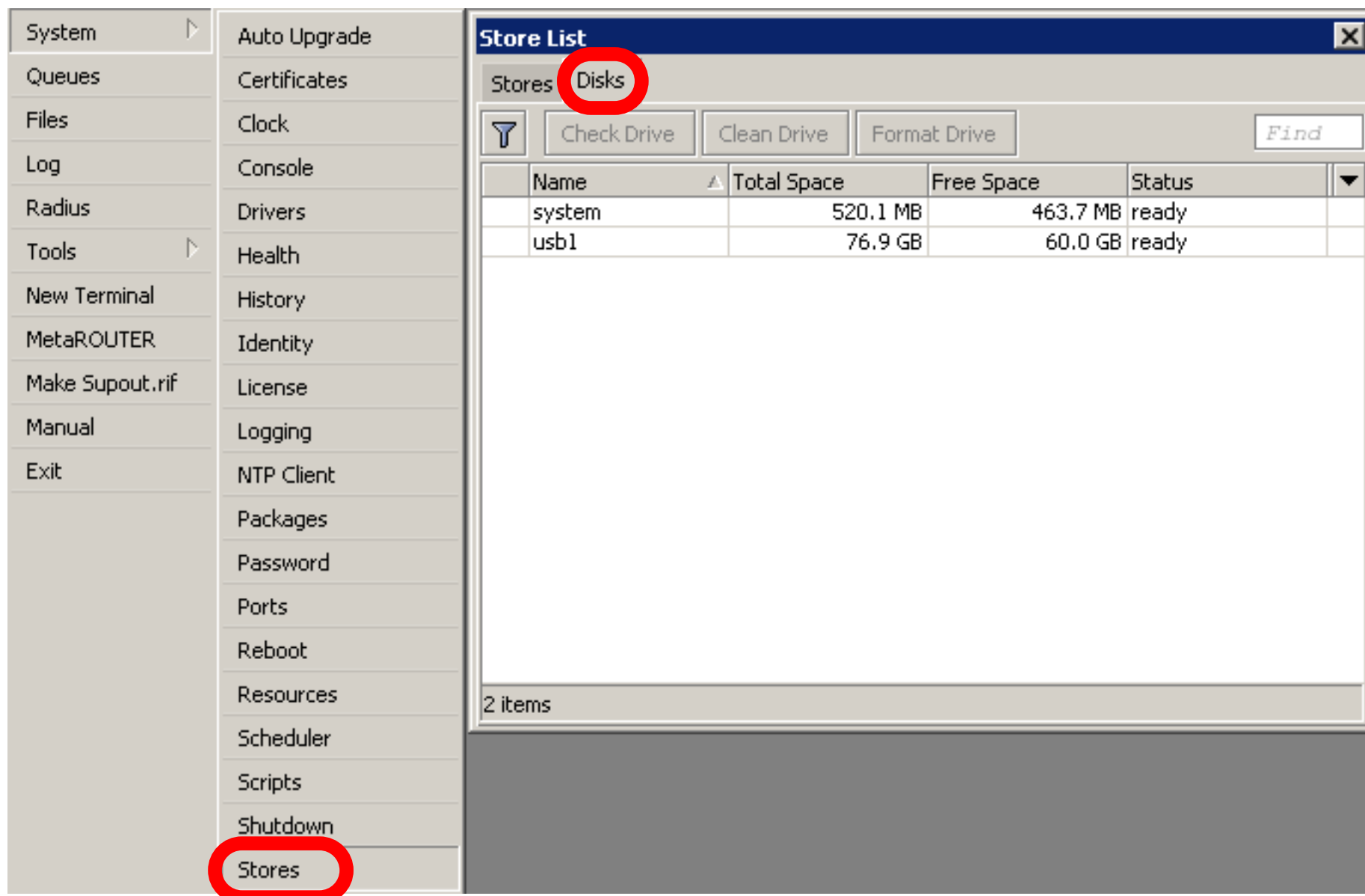


Caching to External

- Cache can be stored on the external drives
- **Store** manipulates all the external drives
- Cache can be stored to IDE, SATA, USB, CF, MicroSD drives

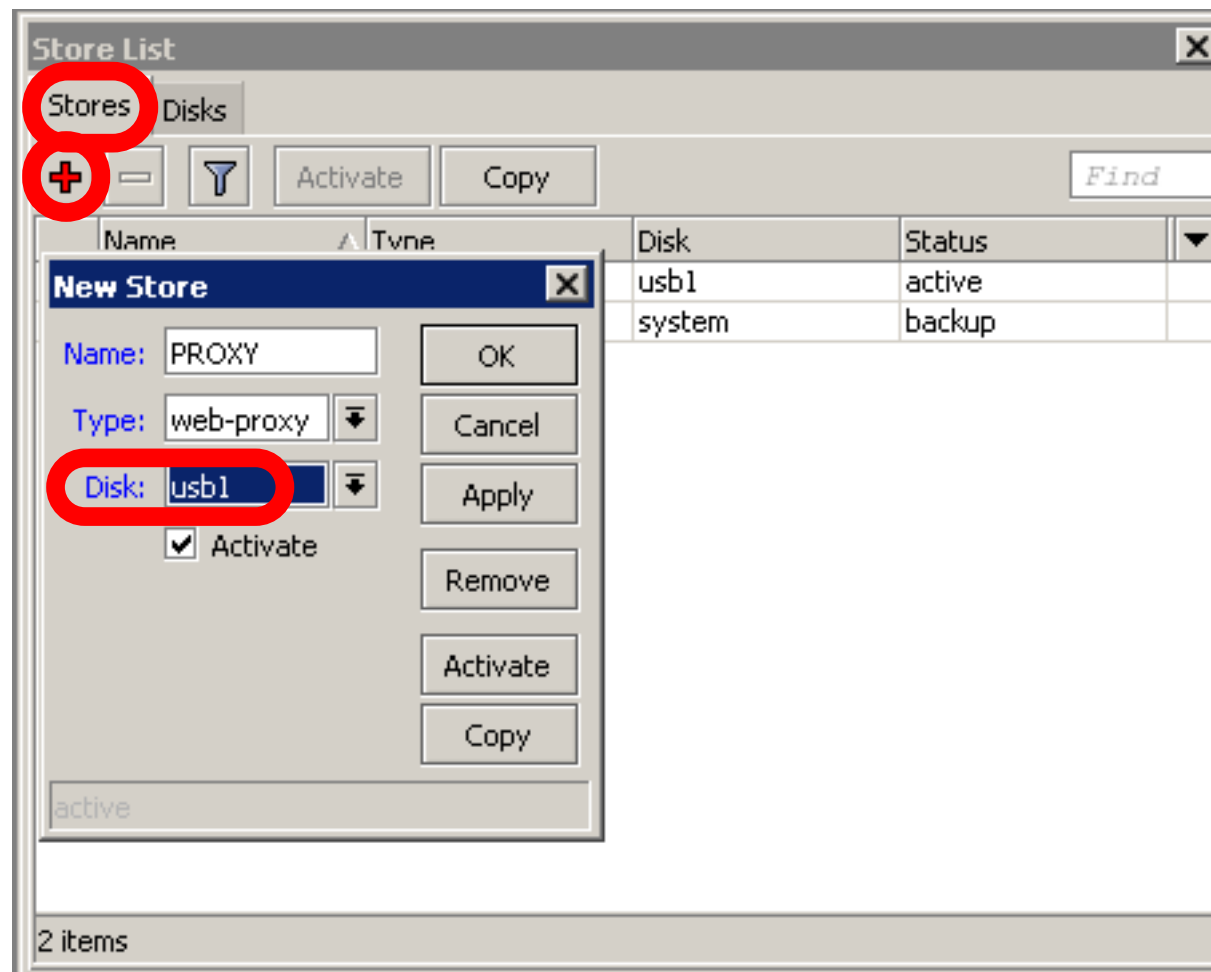
Store

- Manage all external disks
- Newly connected disk should be formatted



Add Store

- Add store to save proxy to external disk
- Store supports proxy, user-manager, dude



Summary

Dude

Dude

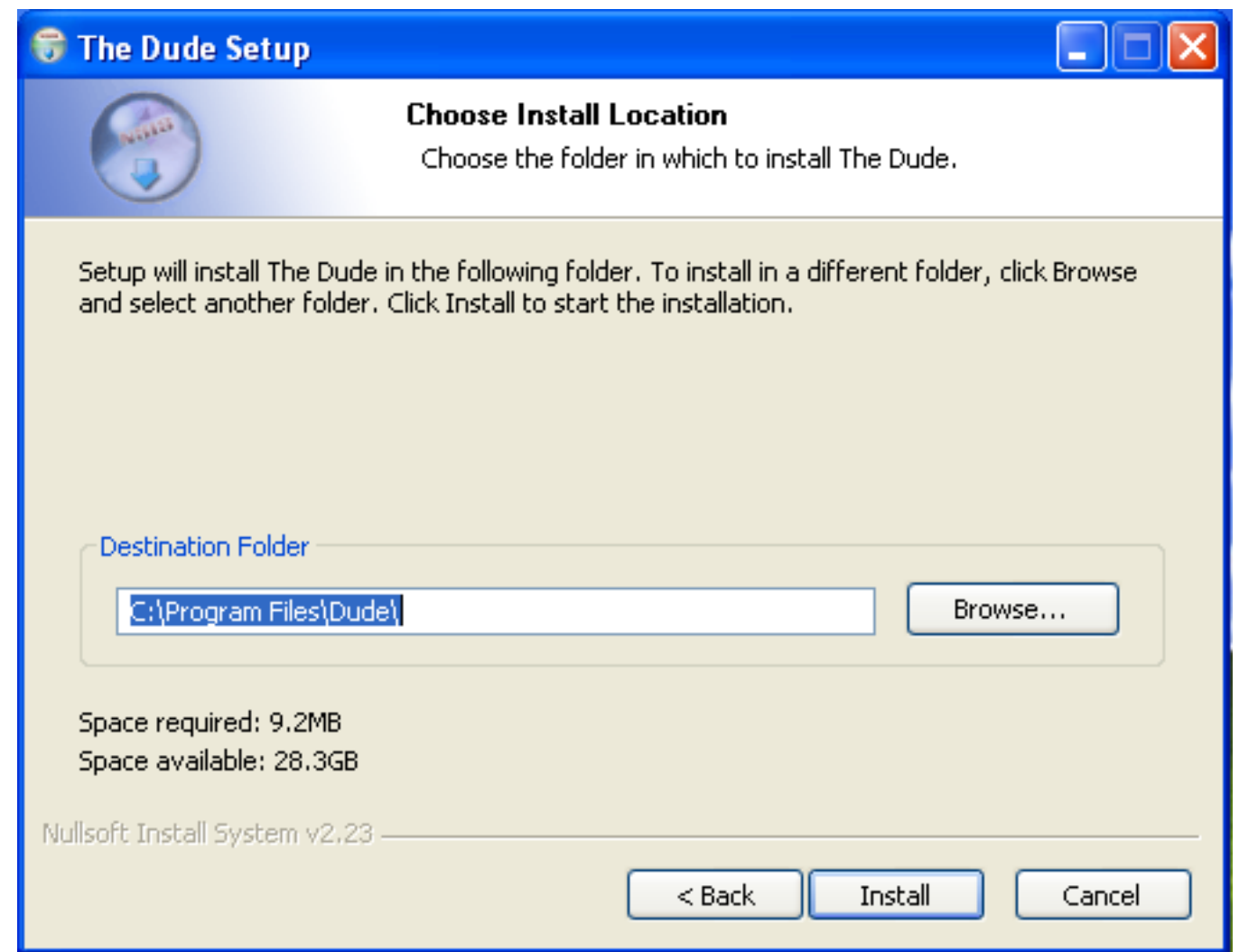
- Network monitor program
- Automatic discovery of devices
- Draw and Layout map of your networks
- Services monitor and alerts
- It is **Free**

Dude

- Dude consists of two parts:
 1. Dude server - the actual monitor program. It does not have a graphical interface. You can run Dude server even on RouterOS
 2. Dude client - connects to Dude server and shows all the information it receives

Dude Install

- Dude is available at www.mikrotik.com
- Install is very easy
- Read and use next button



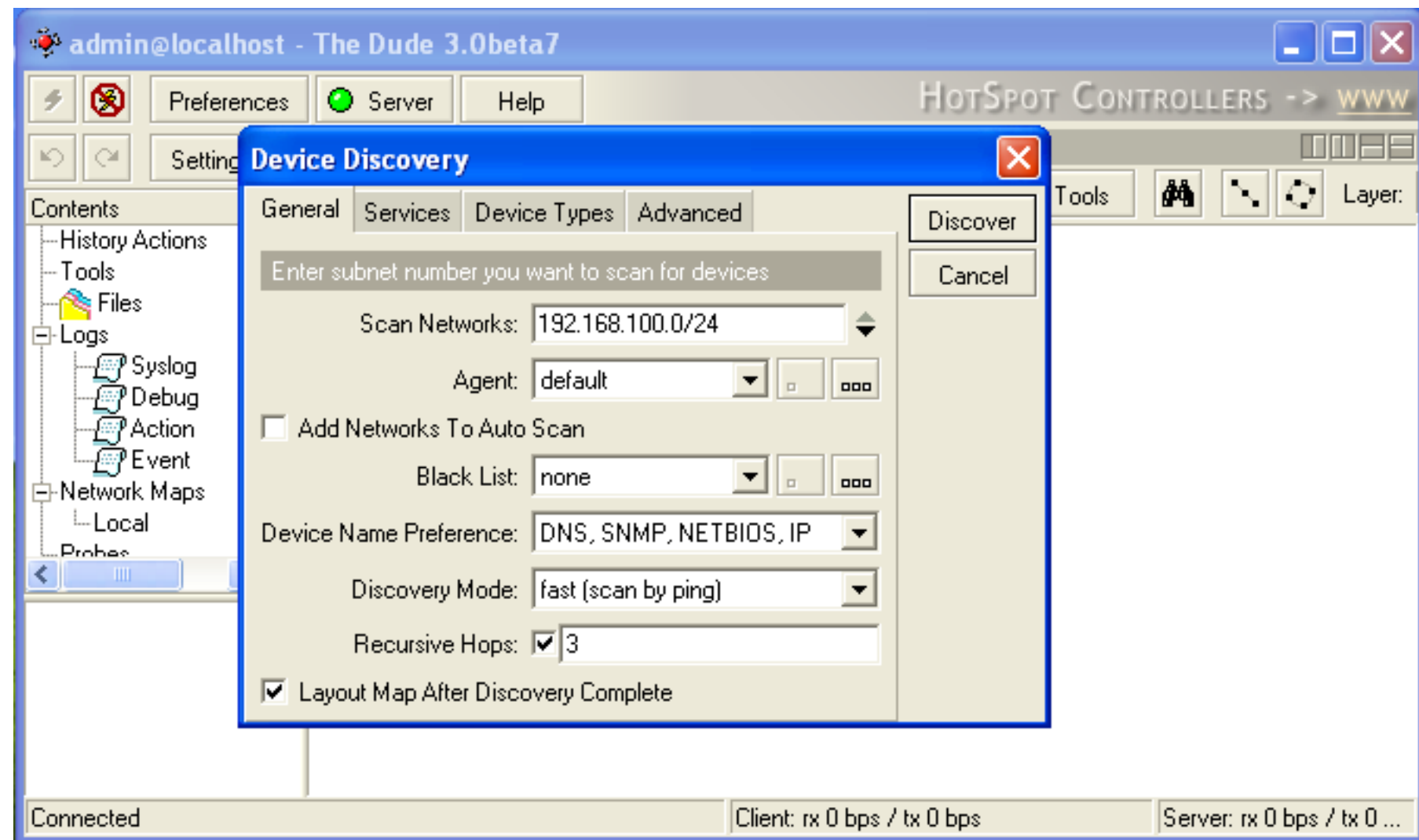
Install **Dude Server** on computer

Dude

- Dude is translated to different languages
- Available on wiki.mikrotik.com

Dude First Launch

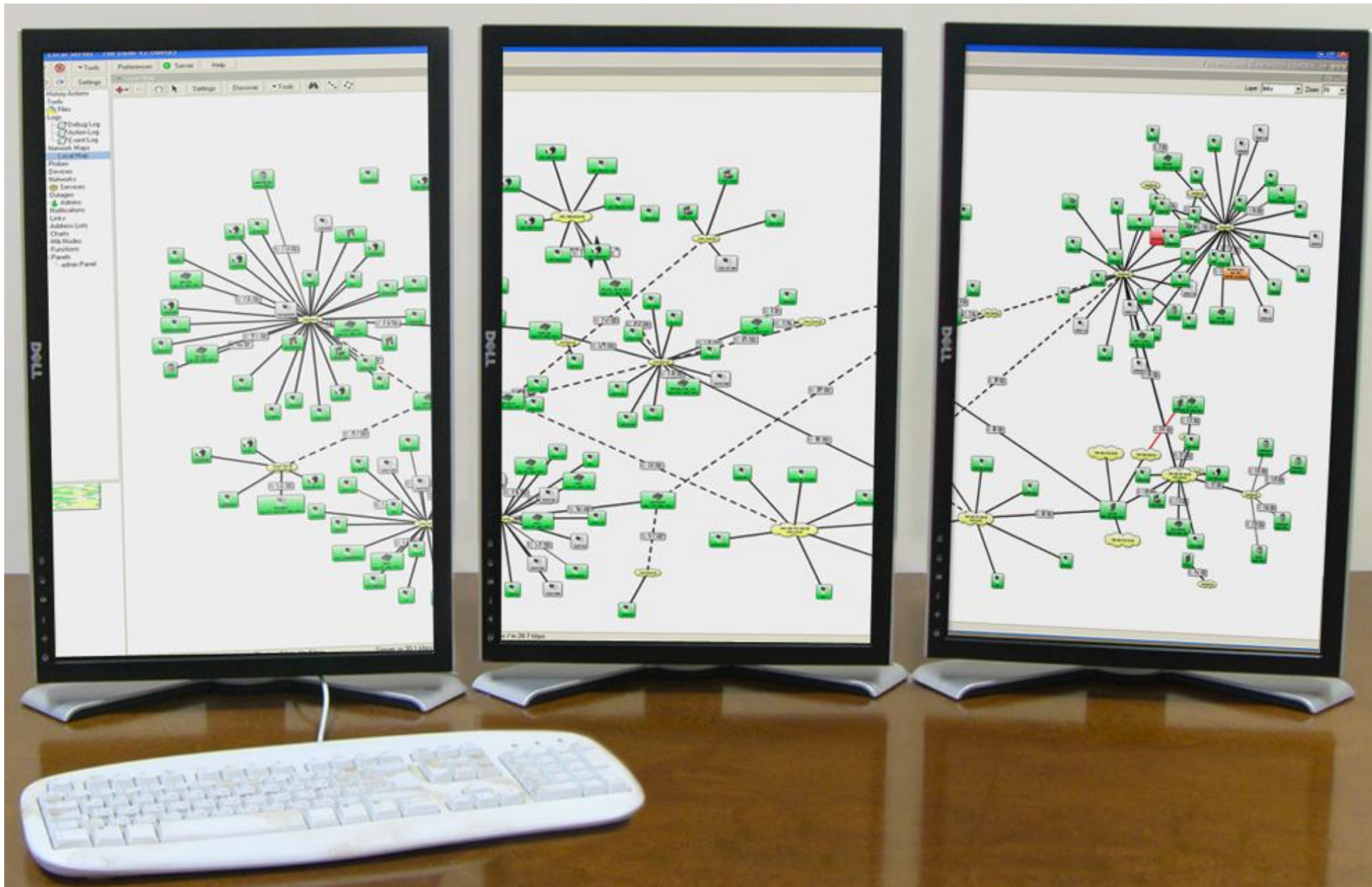
- Discover option is offered for the first launch
- You can discover local network



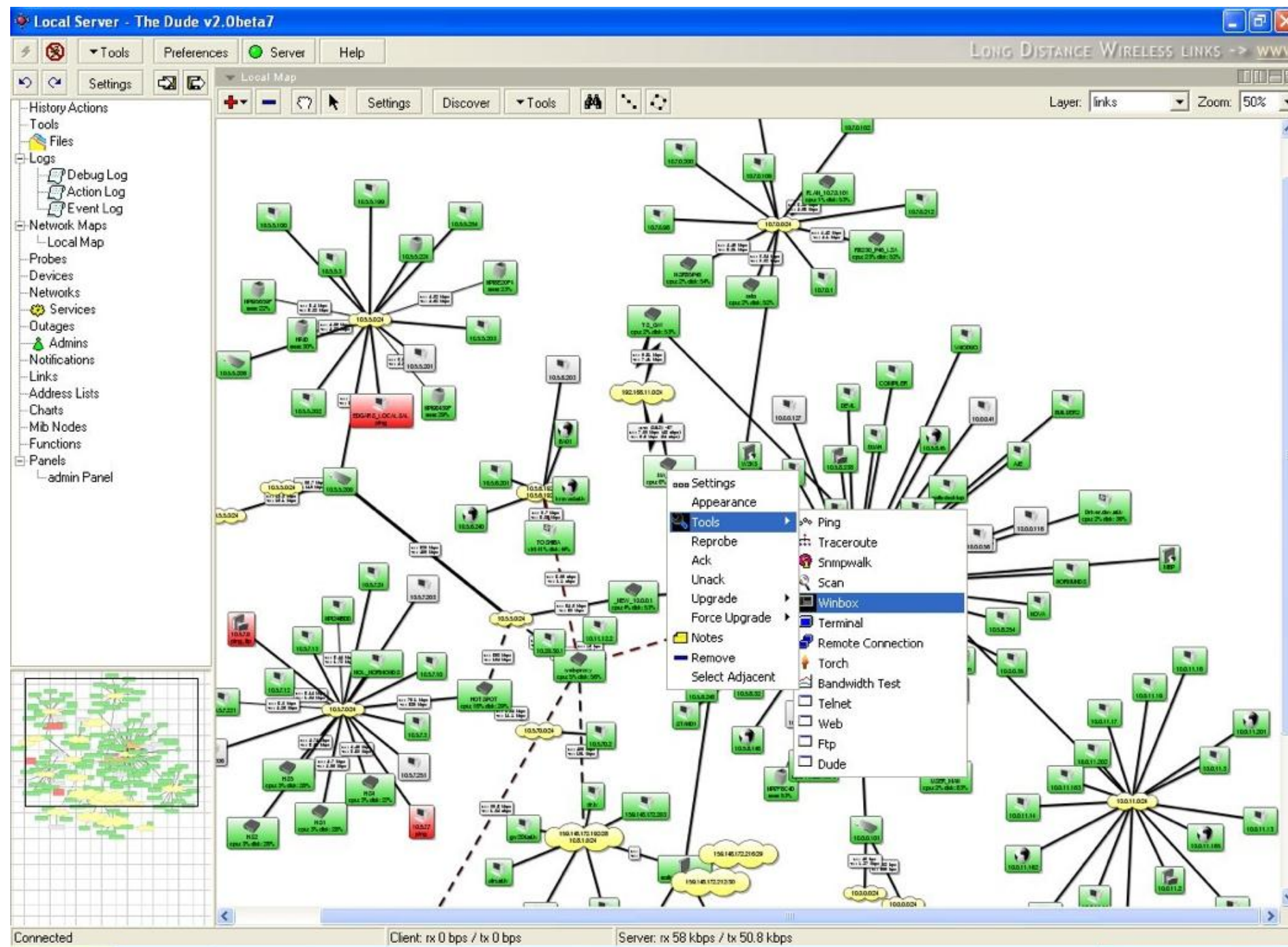
Dude Lab

- Download Dude from `ftp://192.168.100.254`
- Install Dude
- Discover Network
- Add laptop and router
- Disconnect Laptop from Router

Dude Usage



Dude Usage



Troubleshooting

Lost Password

- The only solution to reset password is to reinstall the router

RouterBOARD License

- All purchased licenses are stored in the MikroTik account server
- If your router loses the Key for some reason - just log into mikrotik.com to get it from keys list
- If the key is not in the list use Request Key option

Bad Wireless Signal

- check that the antenna connector is connected 'main' antenna connector
- check that there is no water or moisture in the cable
- check that the default settings for the radio are being used
- Use interface wireless reset-configuration

No Connection

- Try different Ethernet port or cable
- Use reset jumper on RouterBOARD
- Use serial console to view any possible messages
- Use netinstall if possible
- Contact support
(support@mikrotik.com)

Before Certification Test

- Reset the router
- Restore backup or restore configuration
- Make sure you have access to the Internet and to training.mikrotik.com

Certification Test

Certification test

- Go to <http://training.mikrotik.com>
- Login with your account
- Look for US/Dallas Training
- Select Essential Training Test

Instructions