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

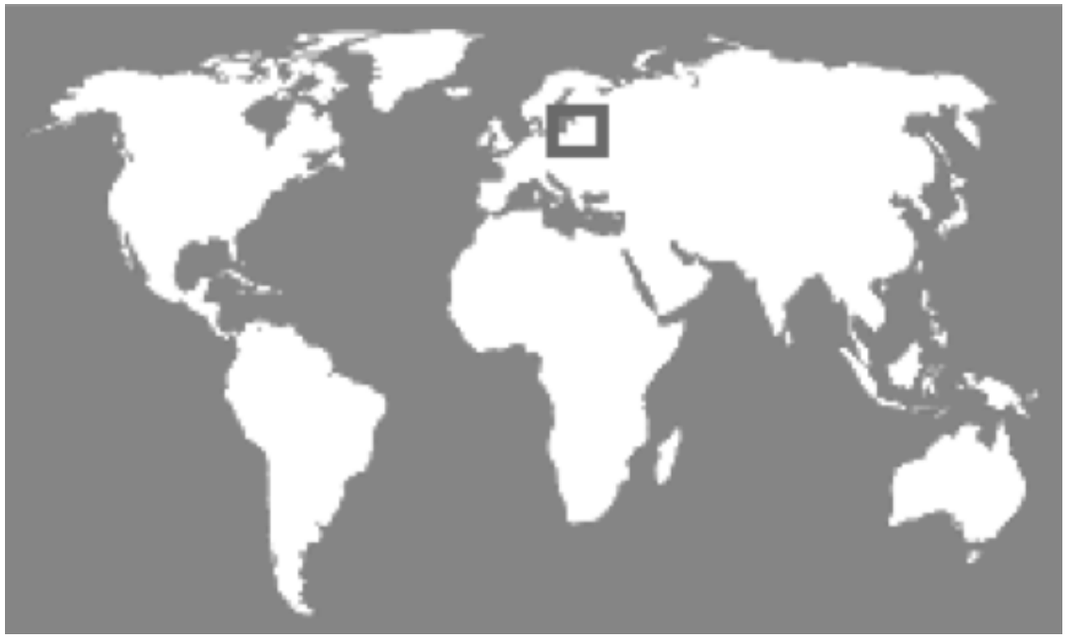
MikroTik's History

- 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 ?

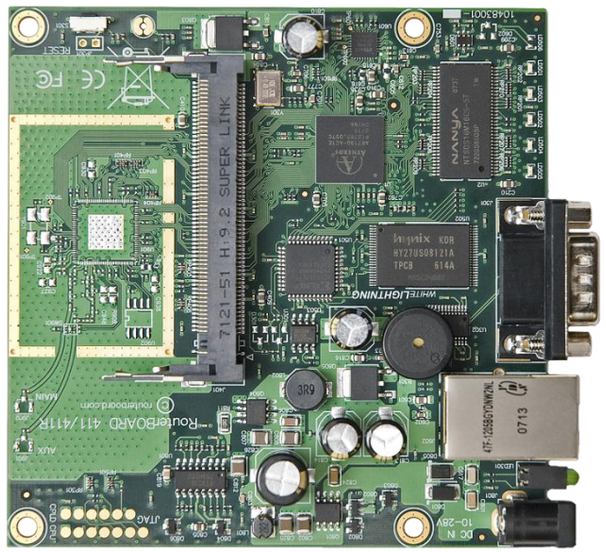
- RouterOS is an operating system that will make your device:
  - a dedicated router
  - a bandwidth shaper
  - a (transparent) packet filter
  - any 802.11a,b/g wireless device

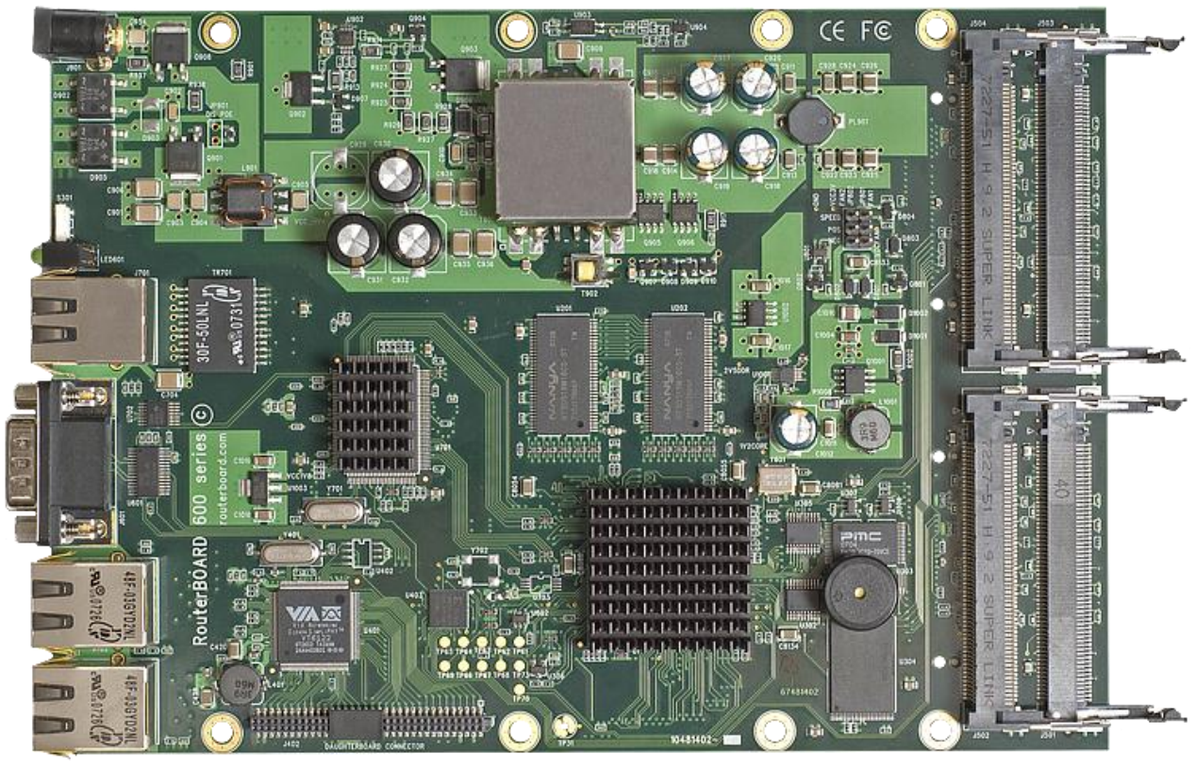
What is RouterOS ?

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

What is RouterBOARD ?

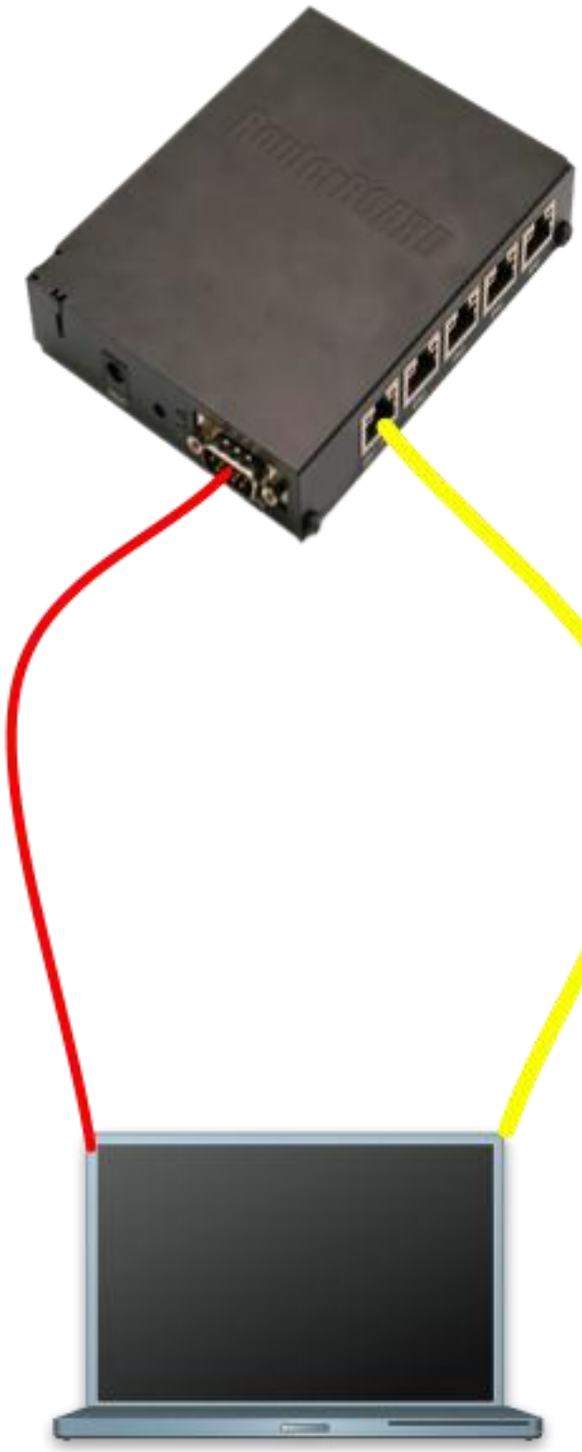
- Hardware created by MikroTik
- Range from small home routers to carrier-class access concentrators





1
2

First Time Access



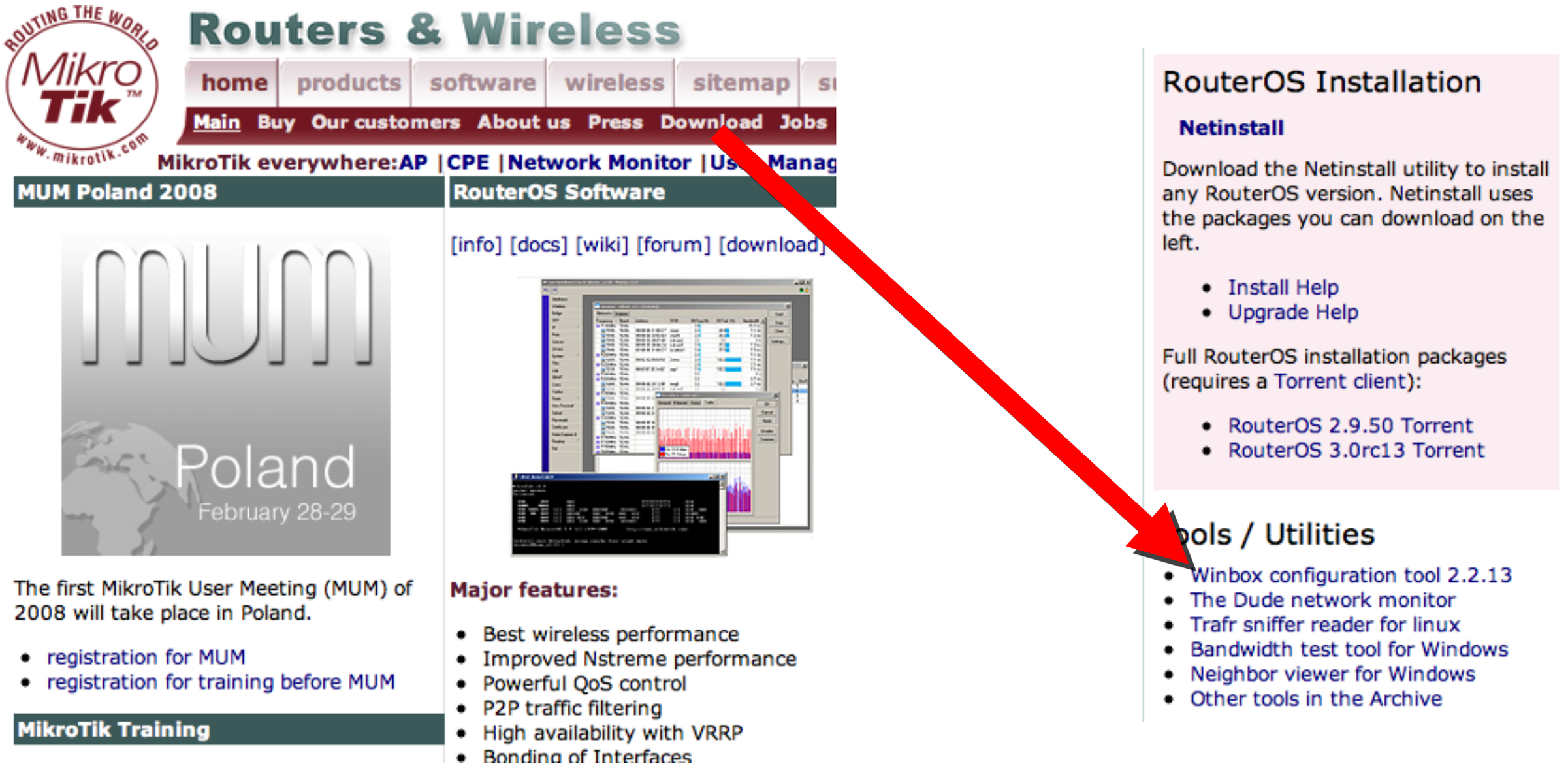
Null Modem Cable

Ethernet cable

Winbox

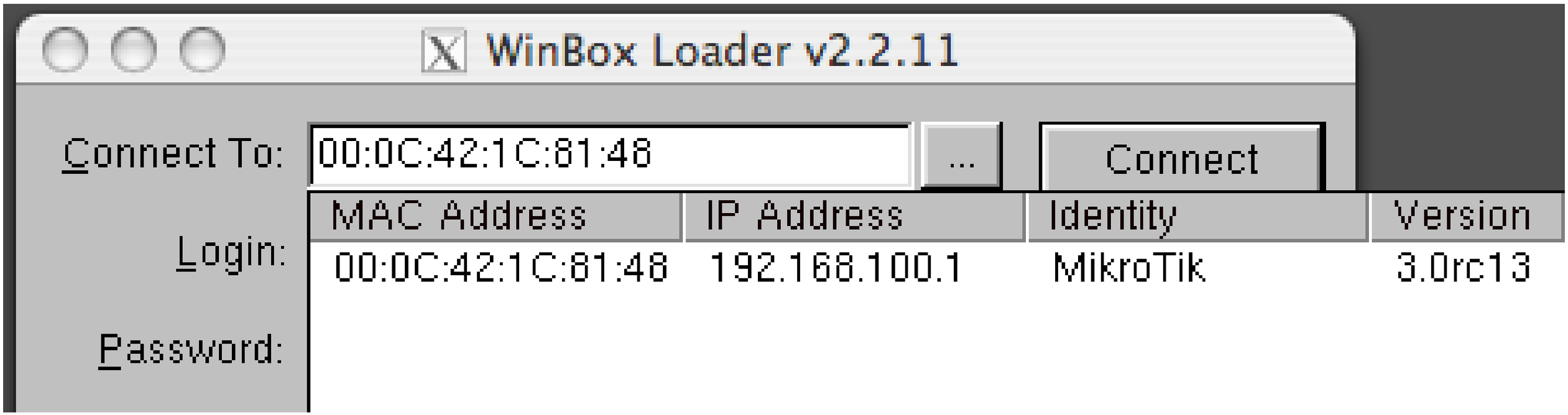
- The application for configuring RouterOS
- It can be downloaded from www.mikrotik.com

Download Winbox



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

Ethernet Cable

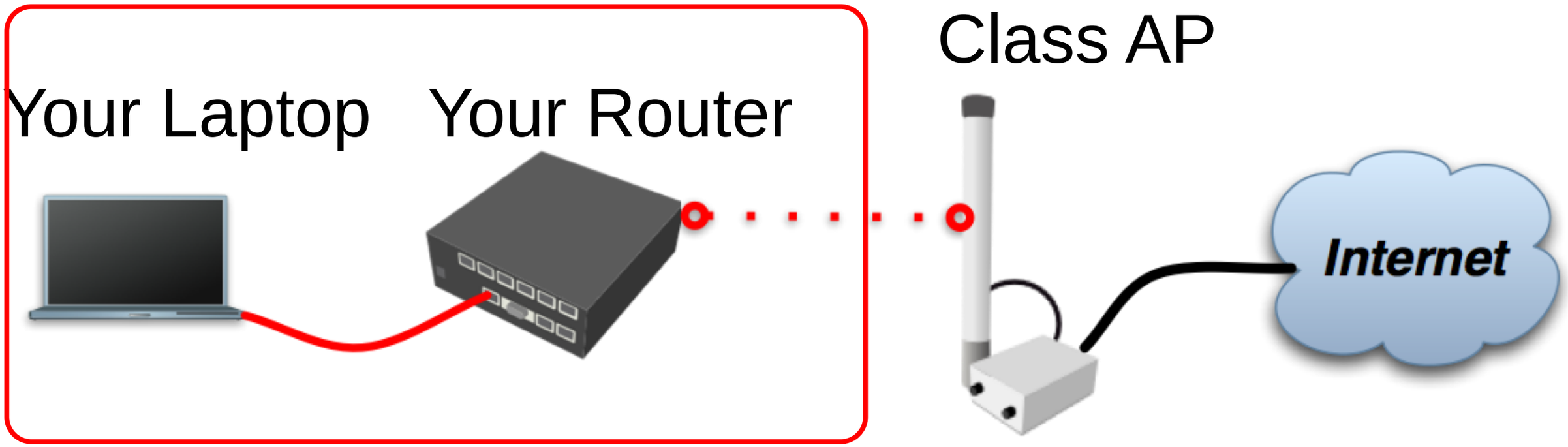
Winbox

Connecting Lab

LAB

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

Diagram

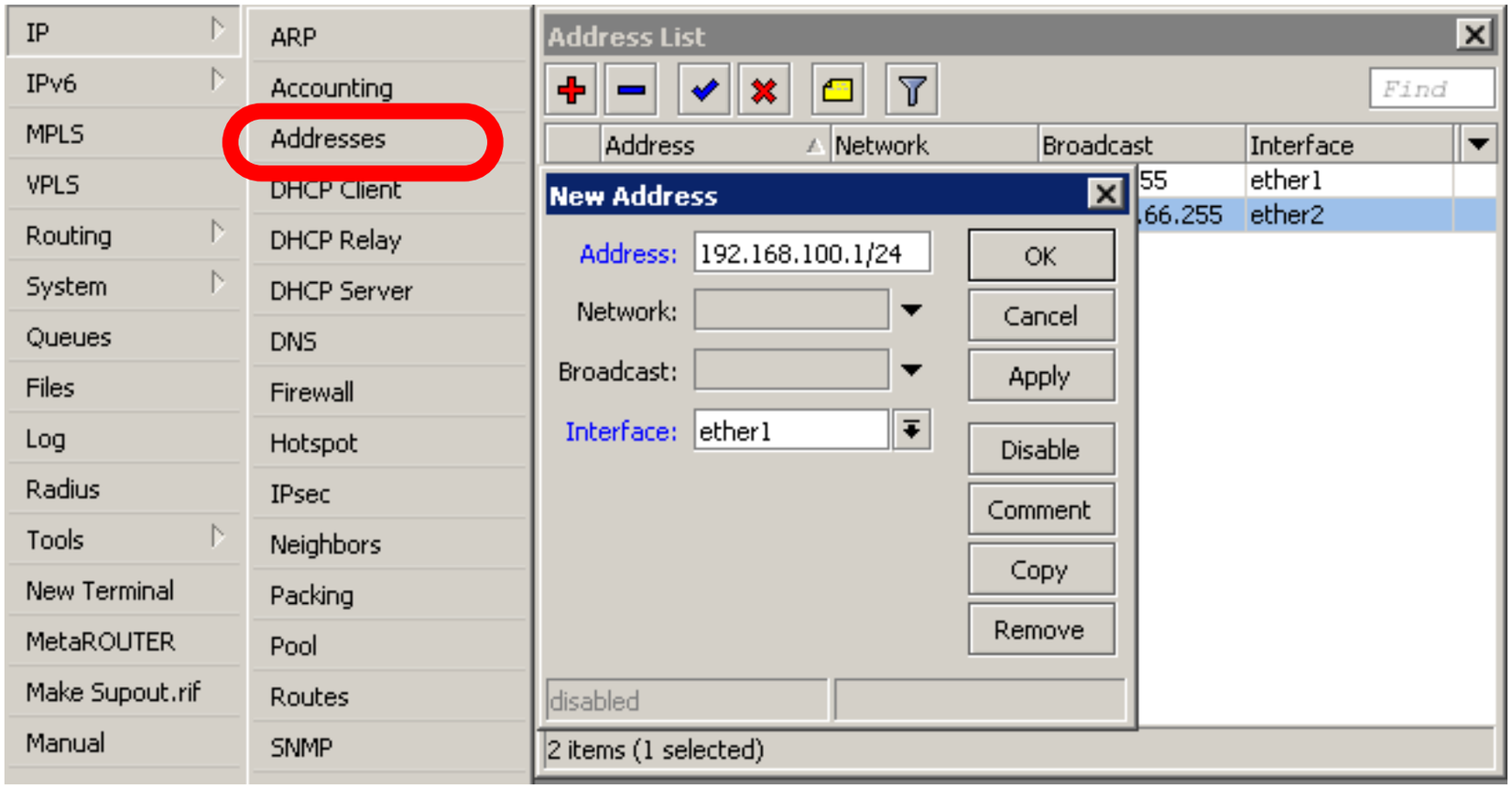


Laptop - Router

- 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**

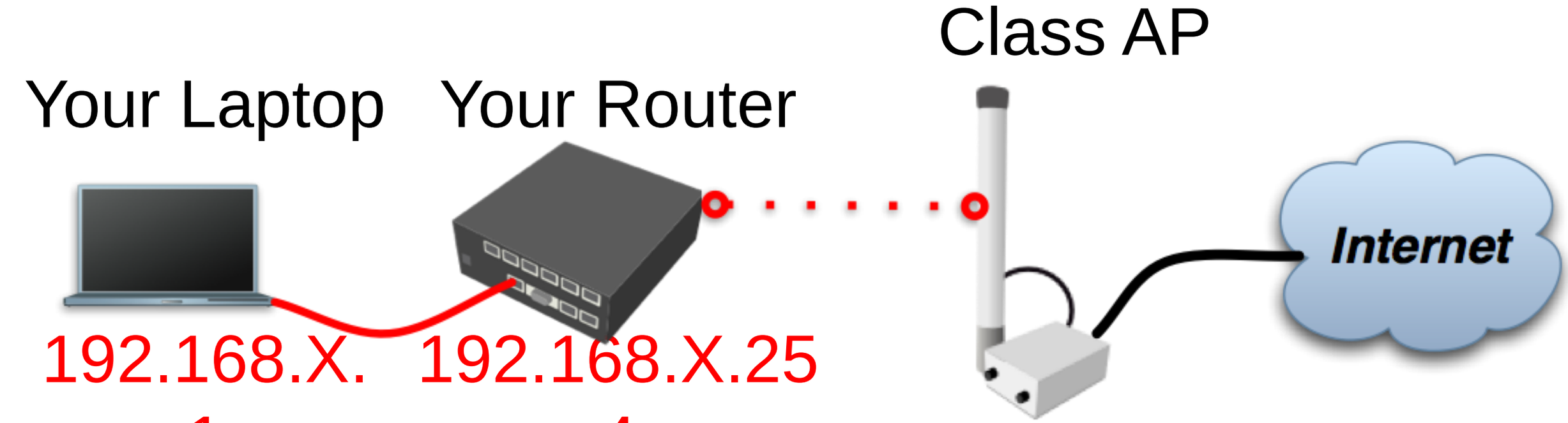
- Connect to router with MAC-Winbox
- Add 192.168.X.254/24 to Ether1



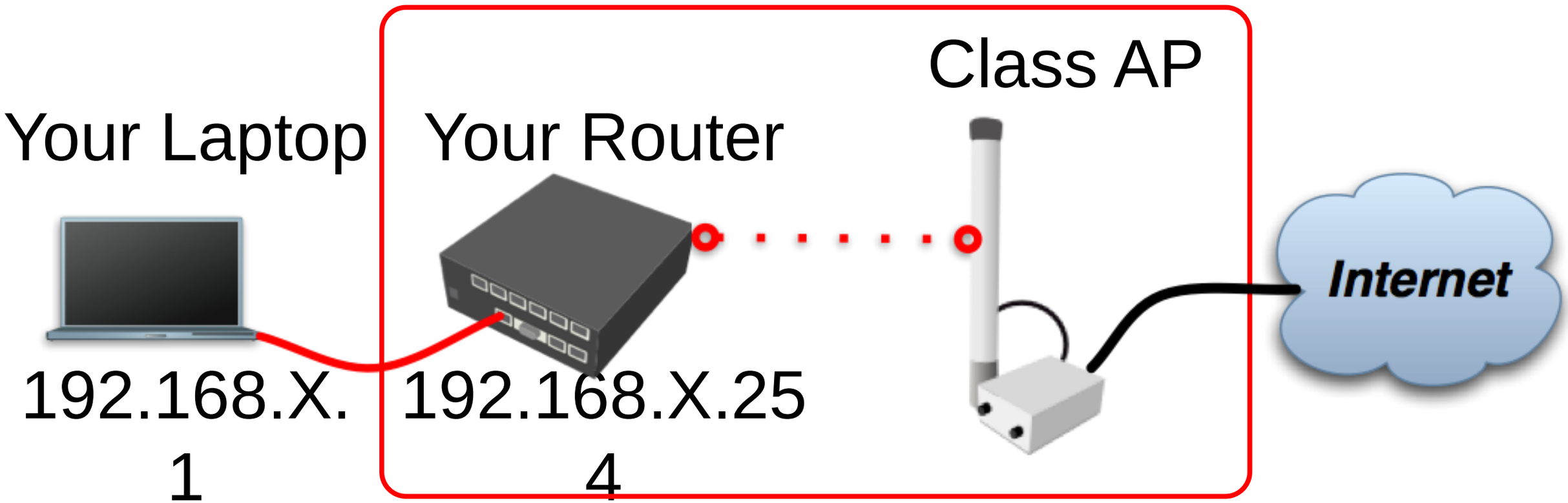
Laptop - **Router**

- 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

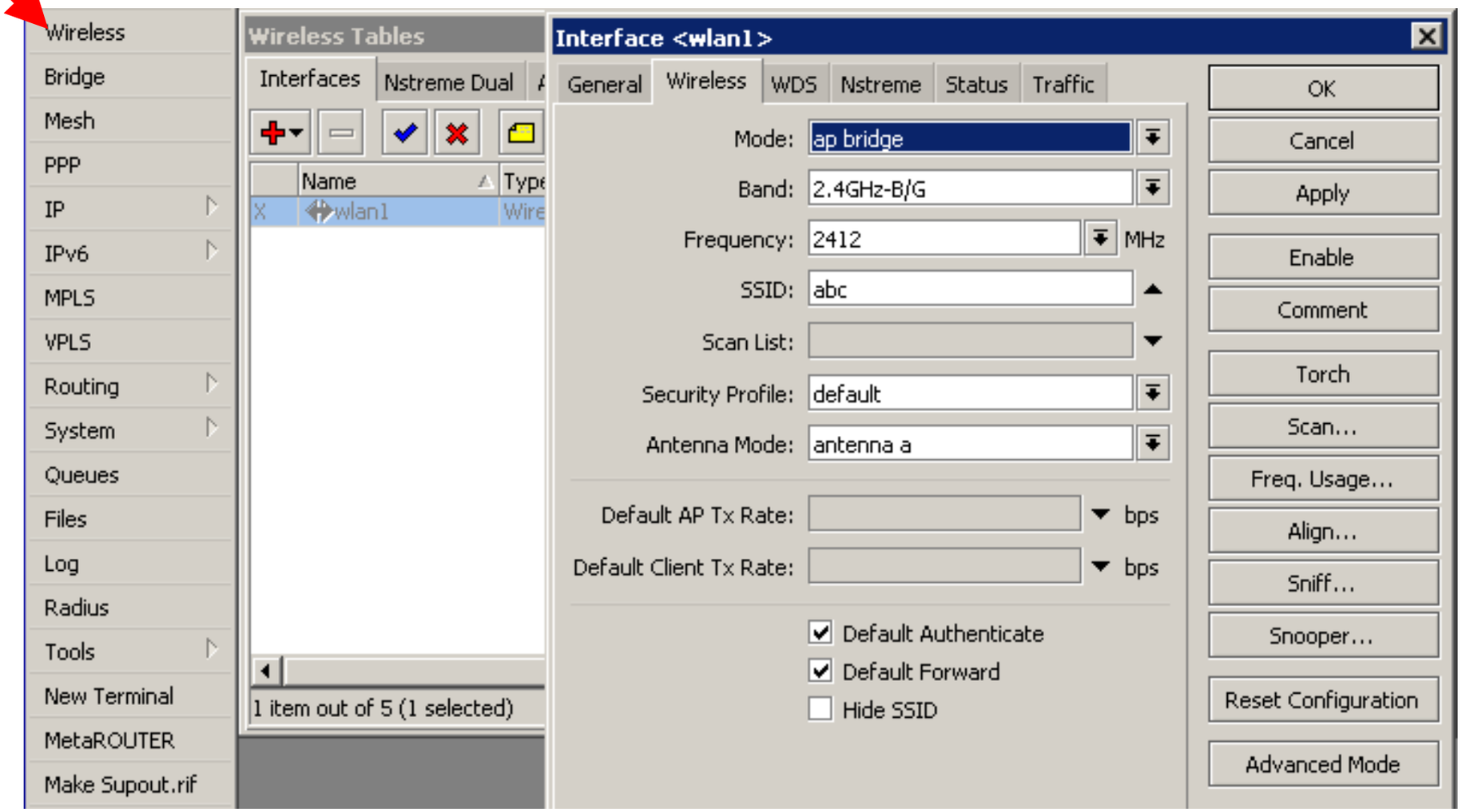


Router - **Internet**

- 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



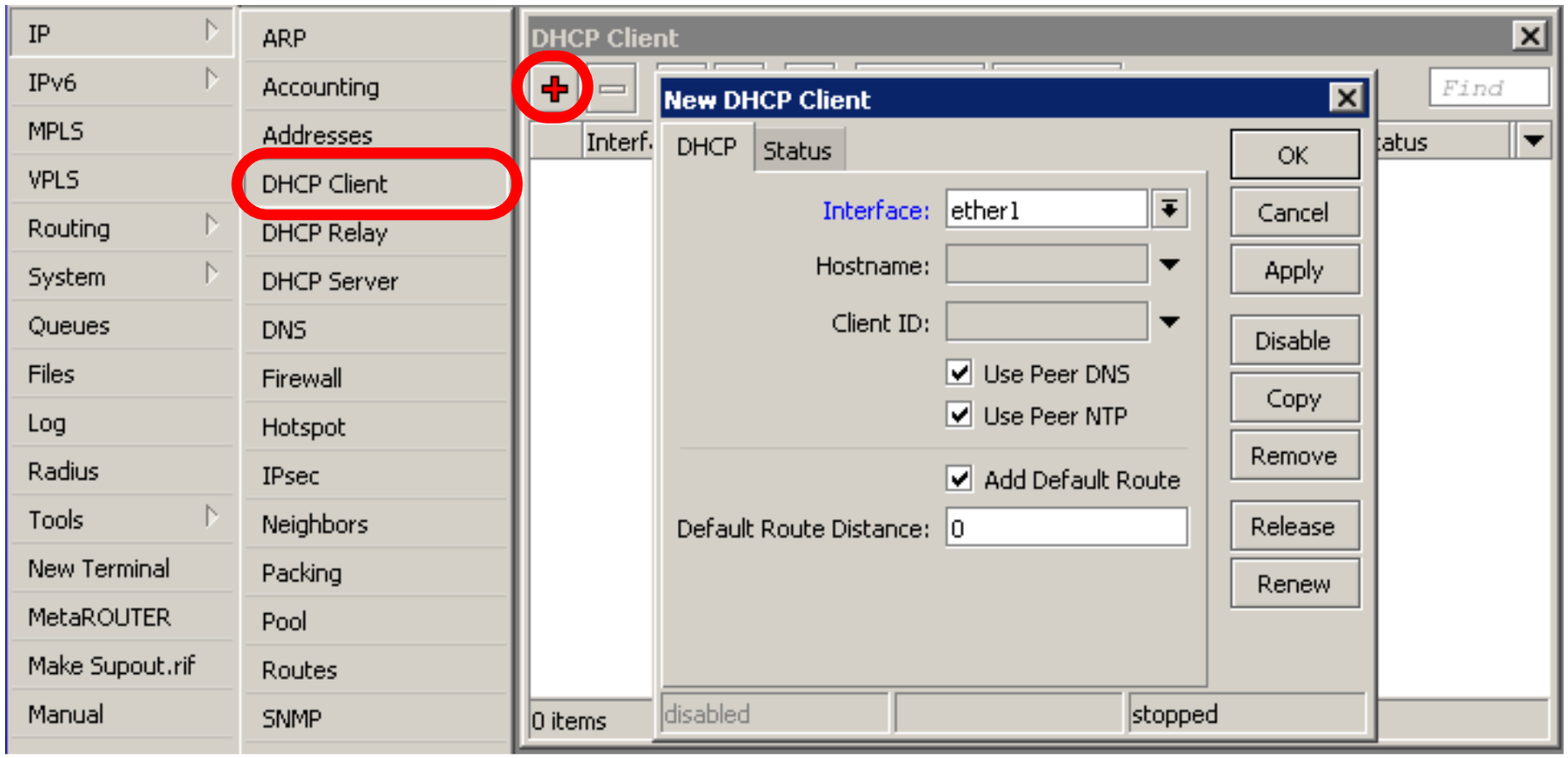
Router - Internet

- 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

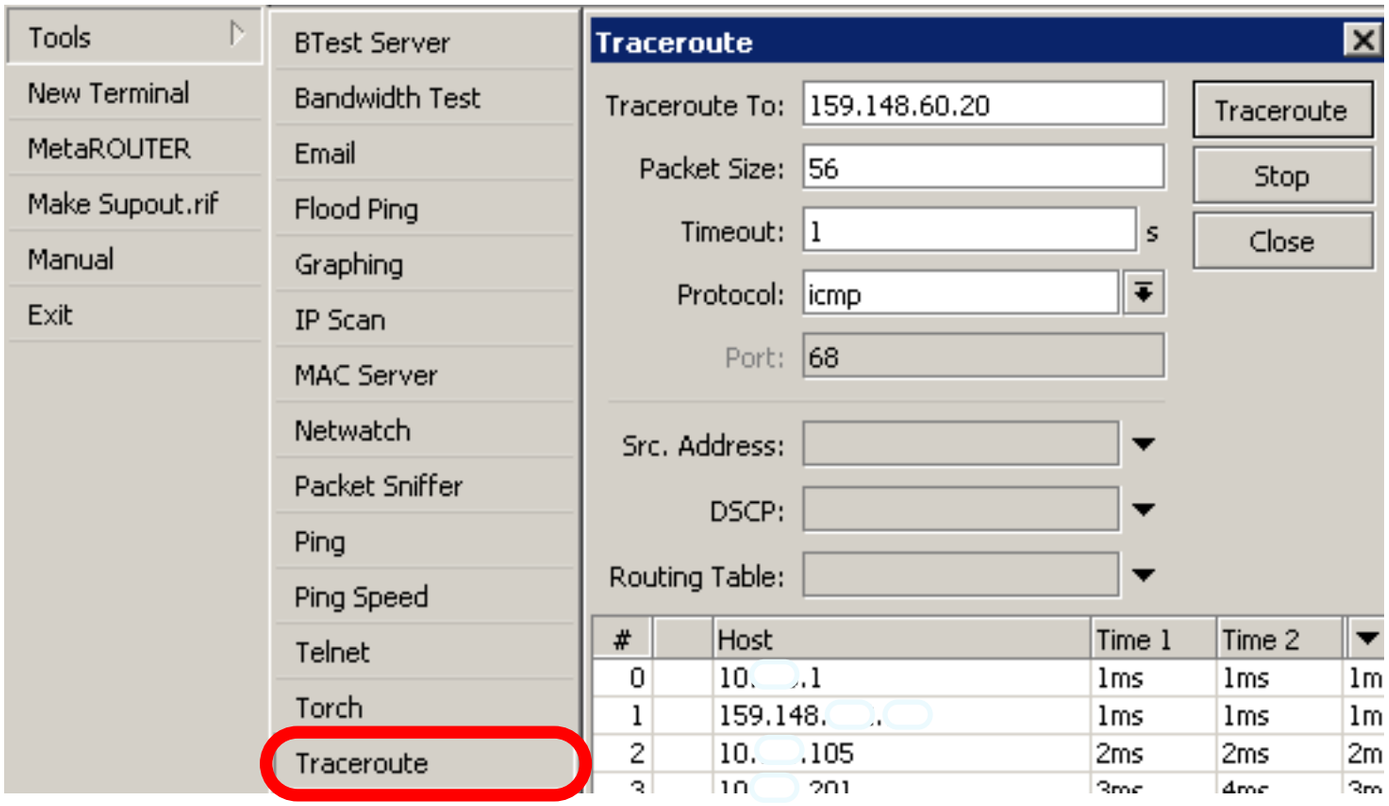
- The wireless interface also needs an IP address
- The AP provides automatic IP addresses over DHCP
- You need to enable DHCP client on your router to get an IP address

Router - Internet

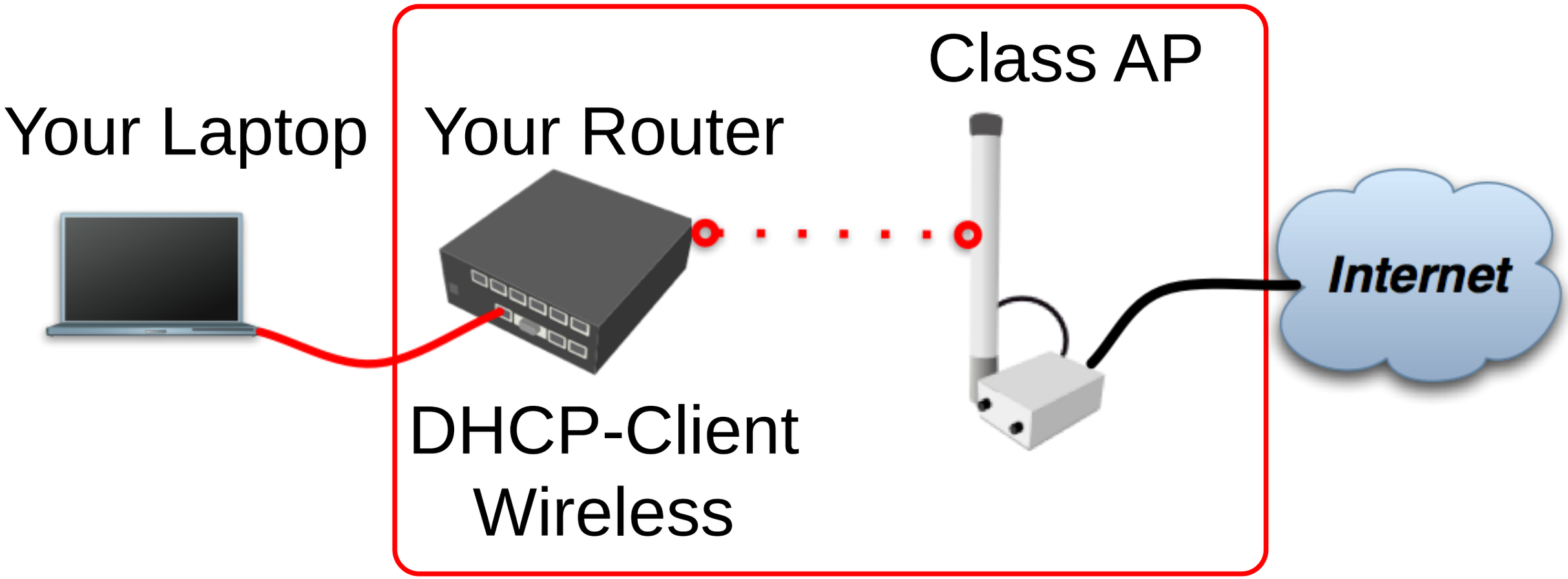


Router - Internet

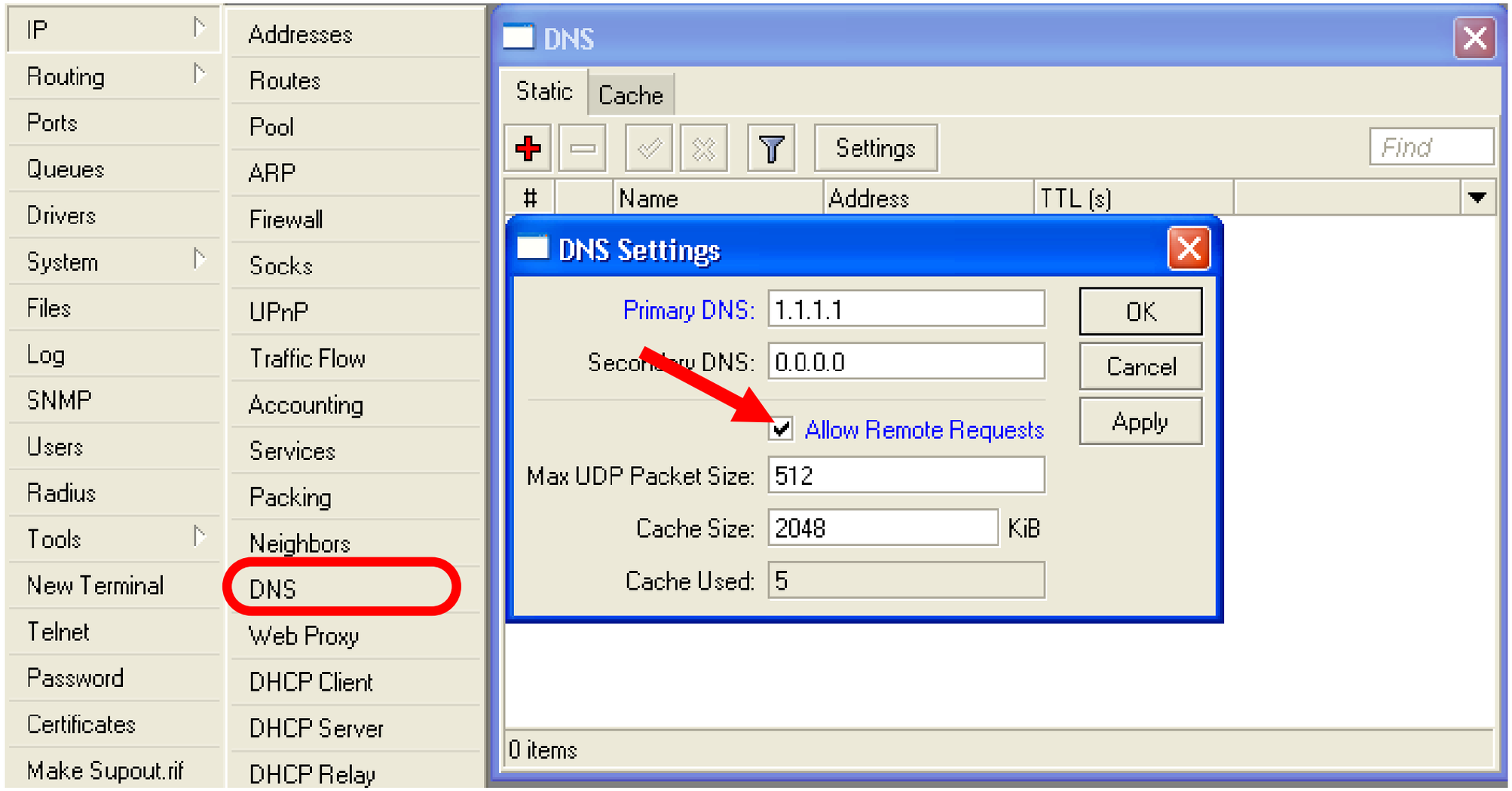
Check Internet connectivity by traceroute



Router Internet



Laptop - Internet



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

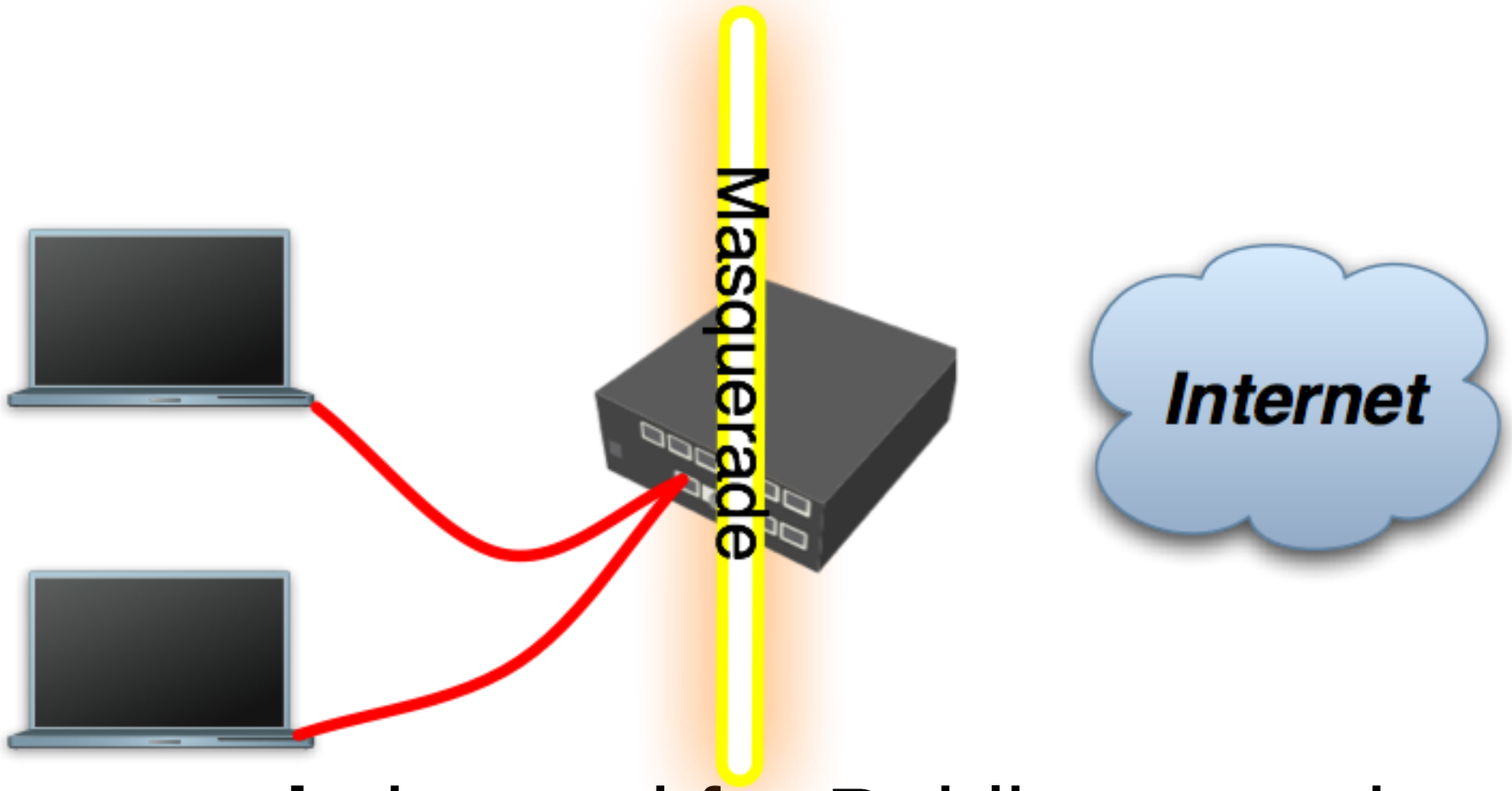
Laptop - Internet

- 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

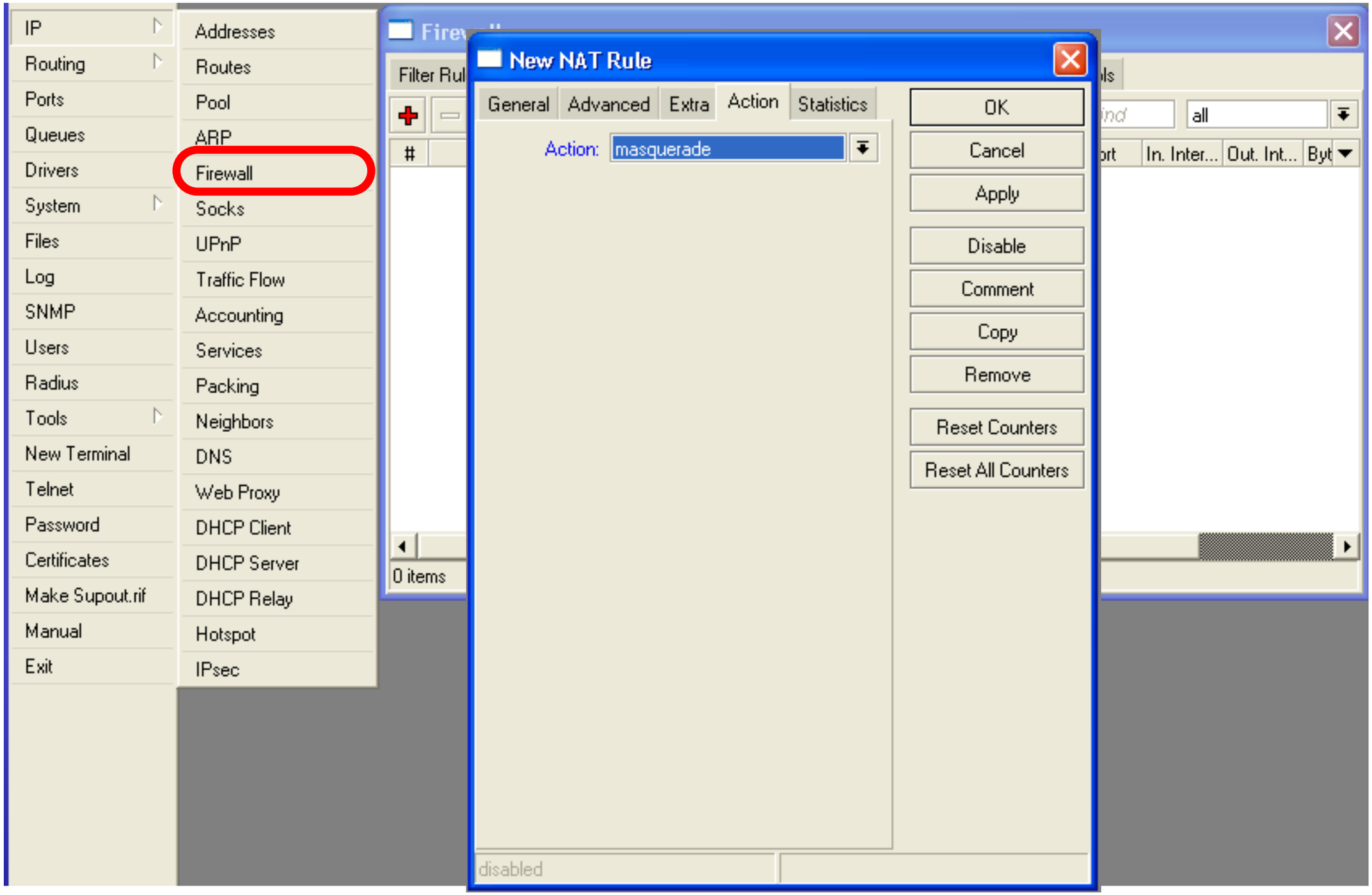
- Laptop can access the router and the router can access the internet, one more step is required
- Make a Masquerade rule to hide your private network behind the router, make Internet work in your laptop

Private and Public space



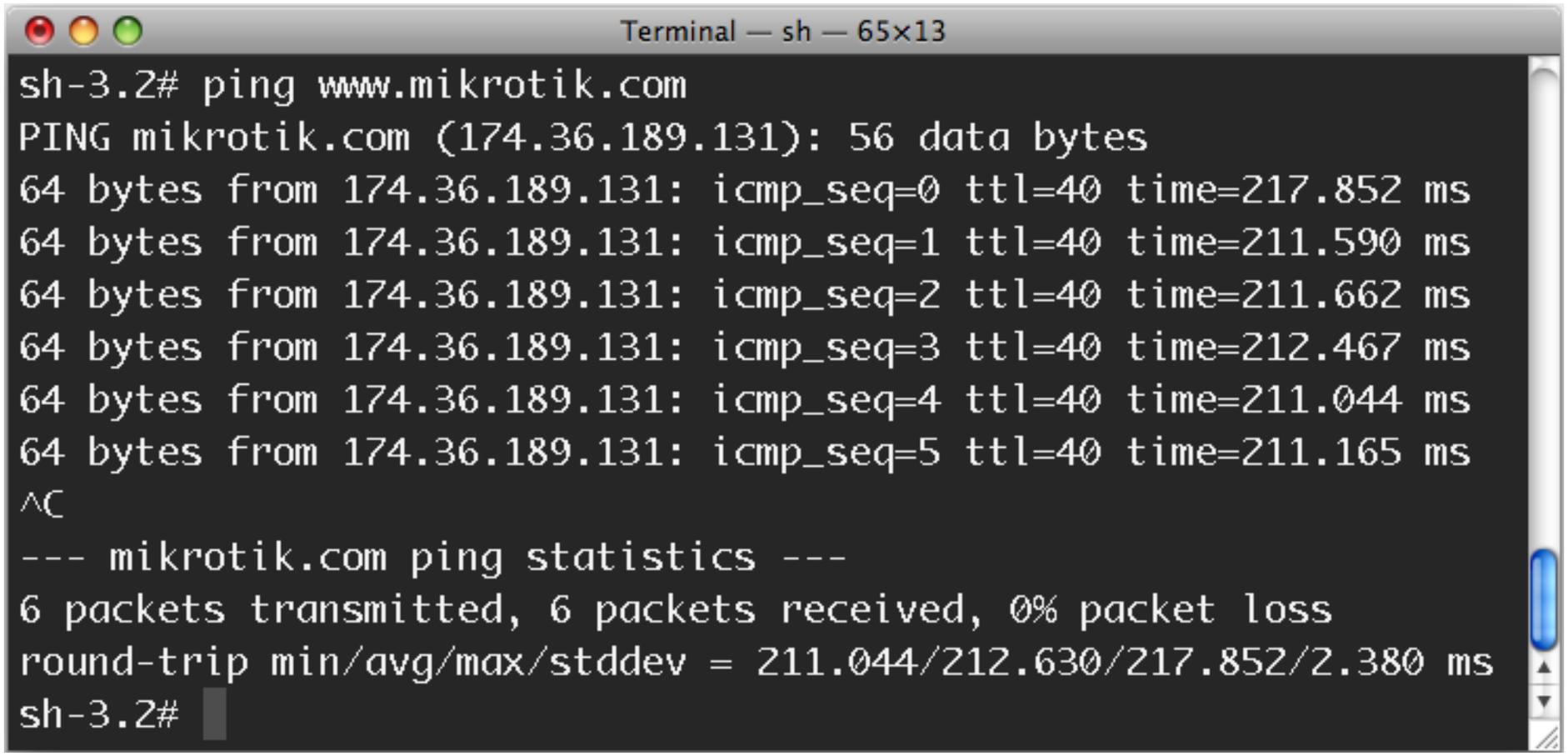
- **Masquerade** is used for Public network access, where private addresses are present
- Private networks include 10.0.0.0-10.255.255.255, 172.16.0.0-172.31.255.255, 192.168.0.0-192.168.255.255

Laptop - Internet



Check Connectivity

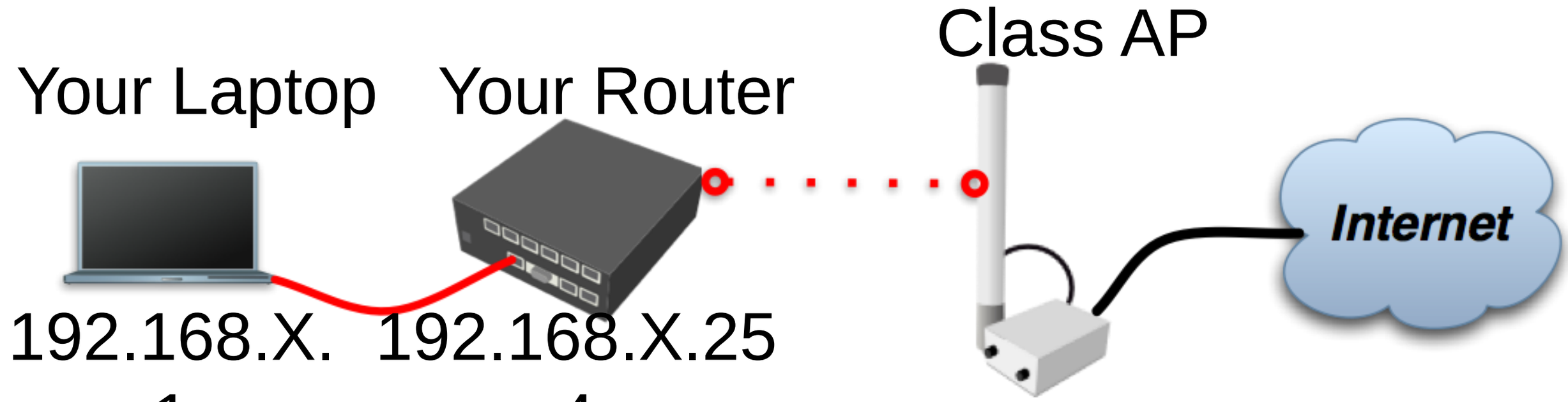
Ping www.mikrotik.com from your laptop



What Can Be Wrong

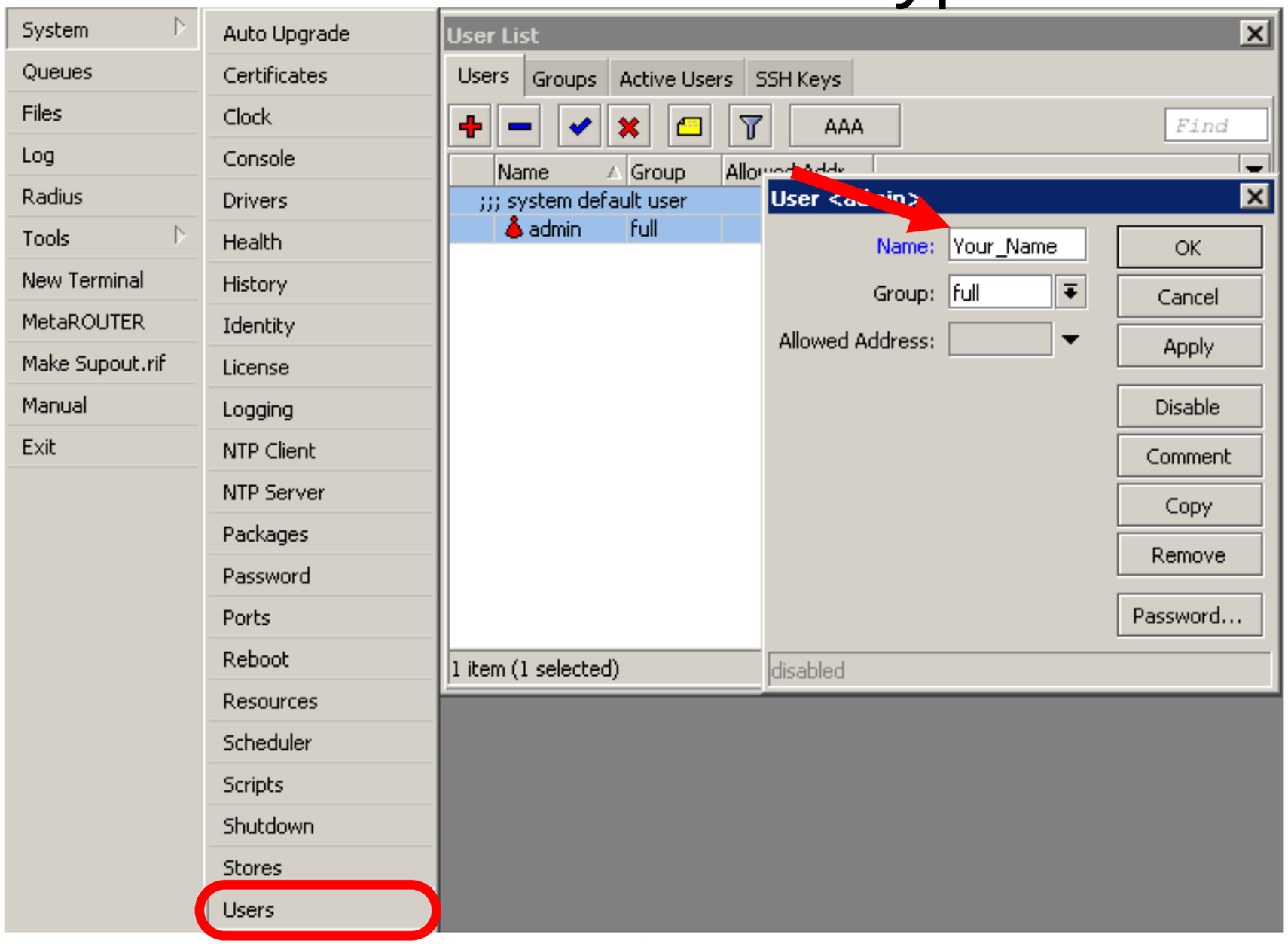
- Router cannot ping further than AP
- Router cannot resolve names
- Computer cannot ping further than router
- Computer cannot resolve names
- Is masquerade rule working
- Does the laptop use the router as default gateway and DNS

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

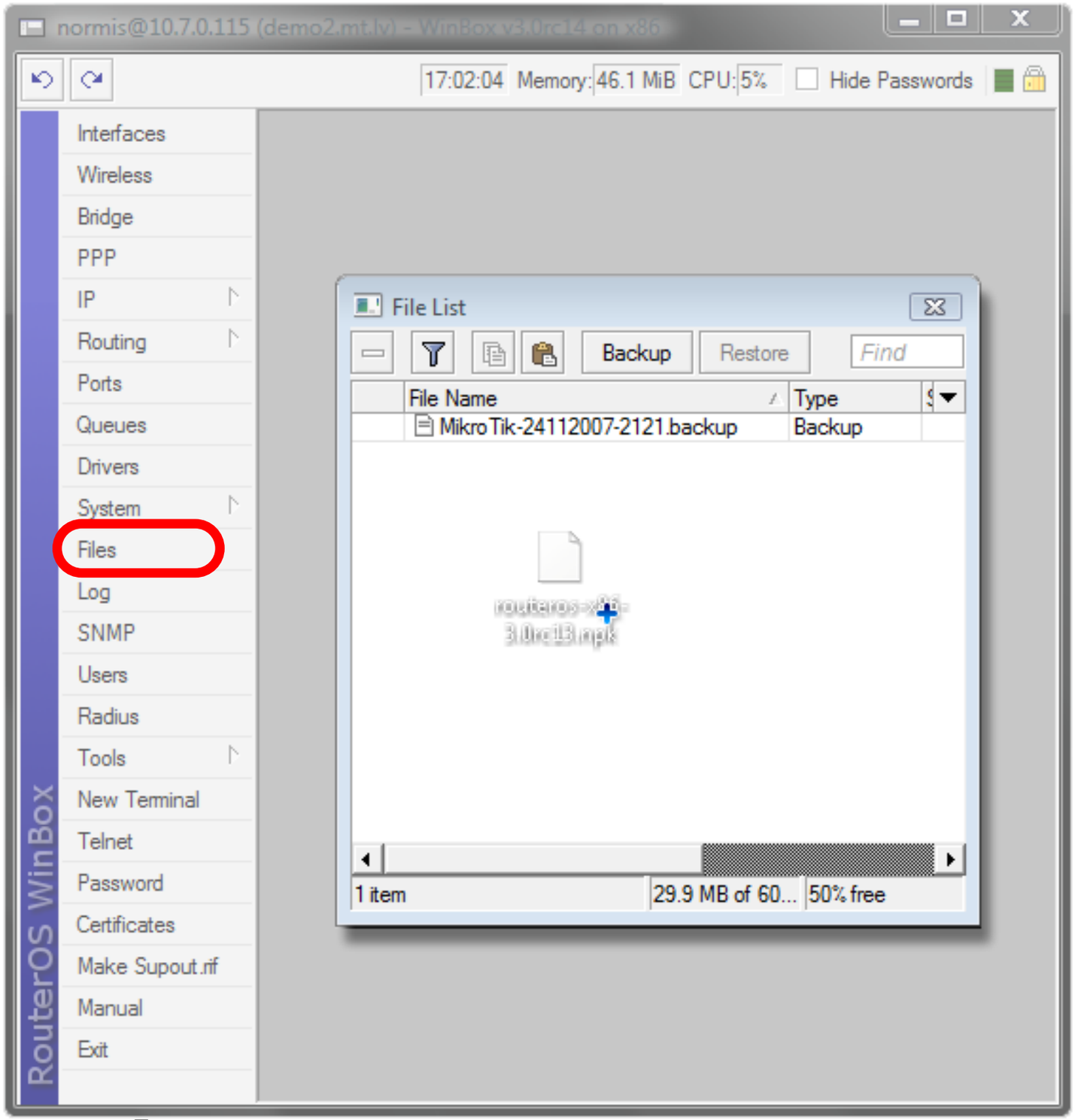
Upgrading Router Lab

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

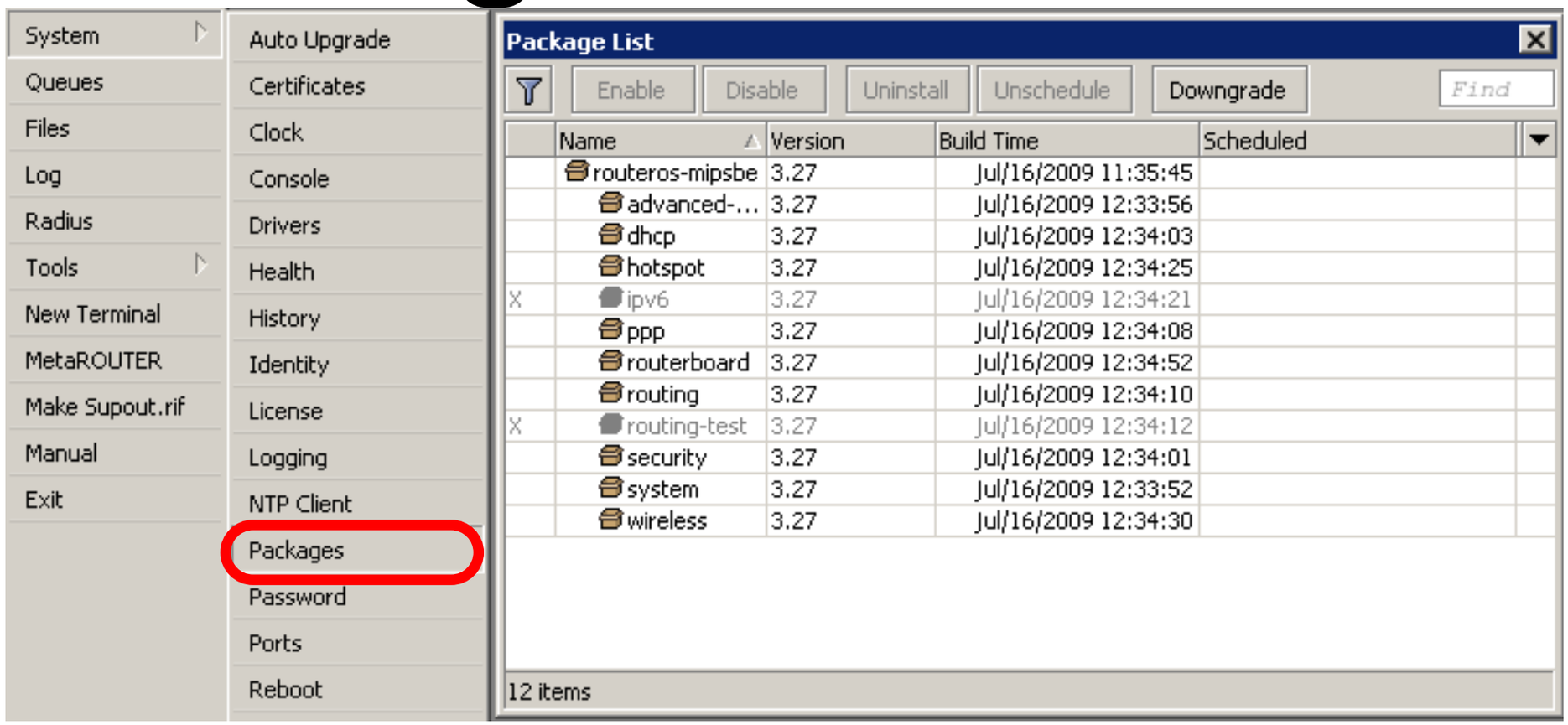
Upgrading Router

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



Package Management

RouterOS functions are enabled by packages



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 802.11a/b/g
user-manager	User-Manager management system
ipv6	IPv6

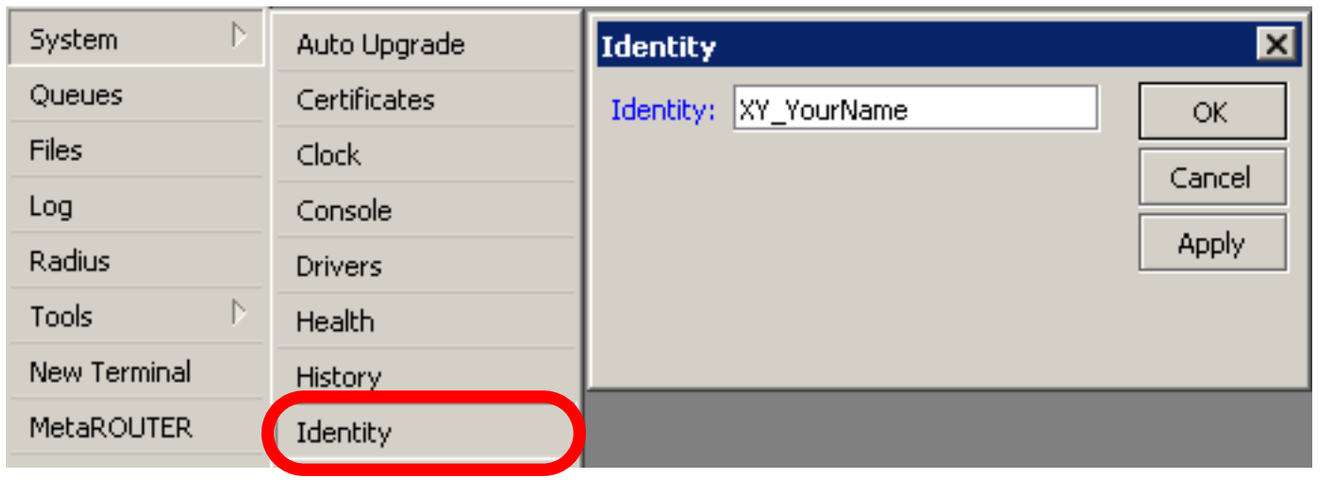
LAB

Package Lab

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

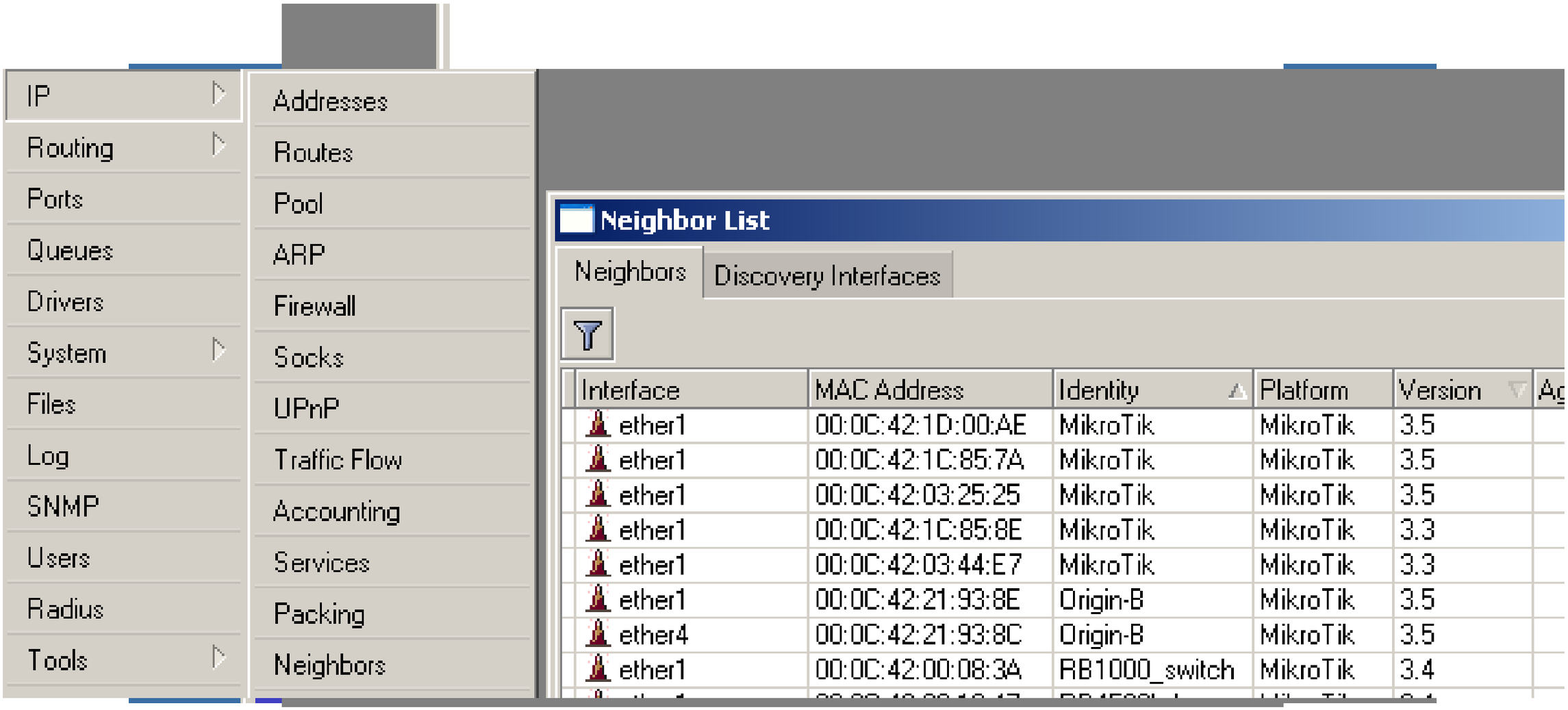
Router Identity

Option to set name for each router



Router Identity

Identity information is shown in different places



Router Identity Lab

LAB

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

NTP

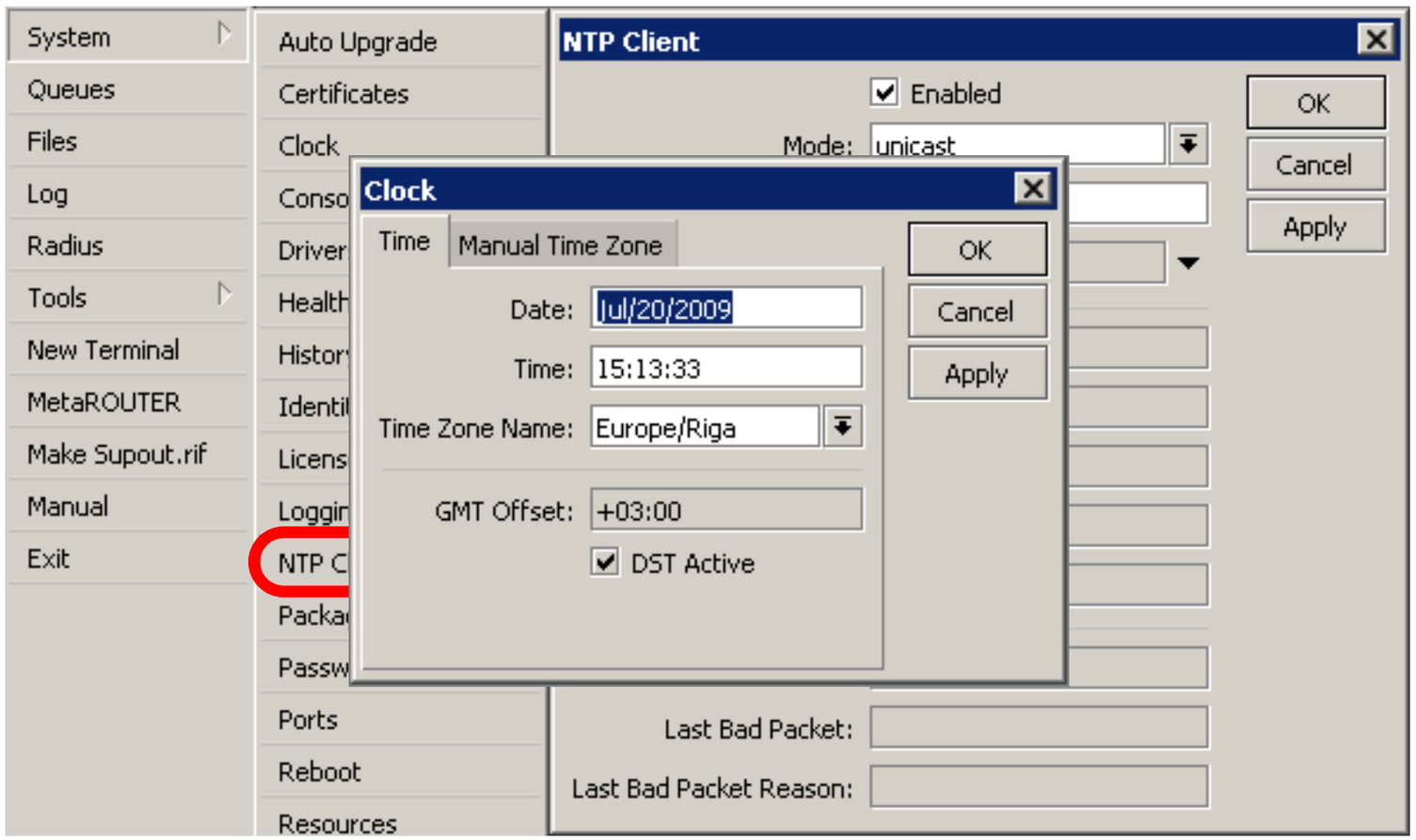
- Network Time Protocol, to synchronize time
- NTP Client and NTP Server support in RouterOS

Why NTP

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

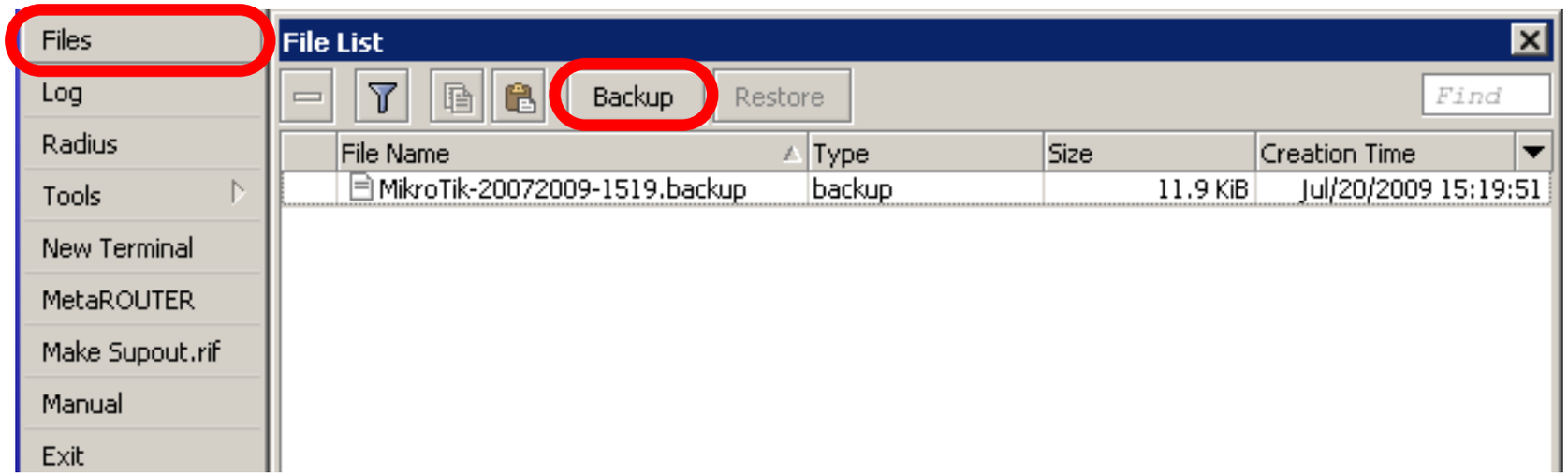
NTP Client

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]
```

LAB

Backup Lab

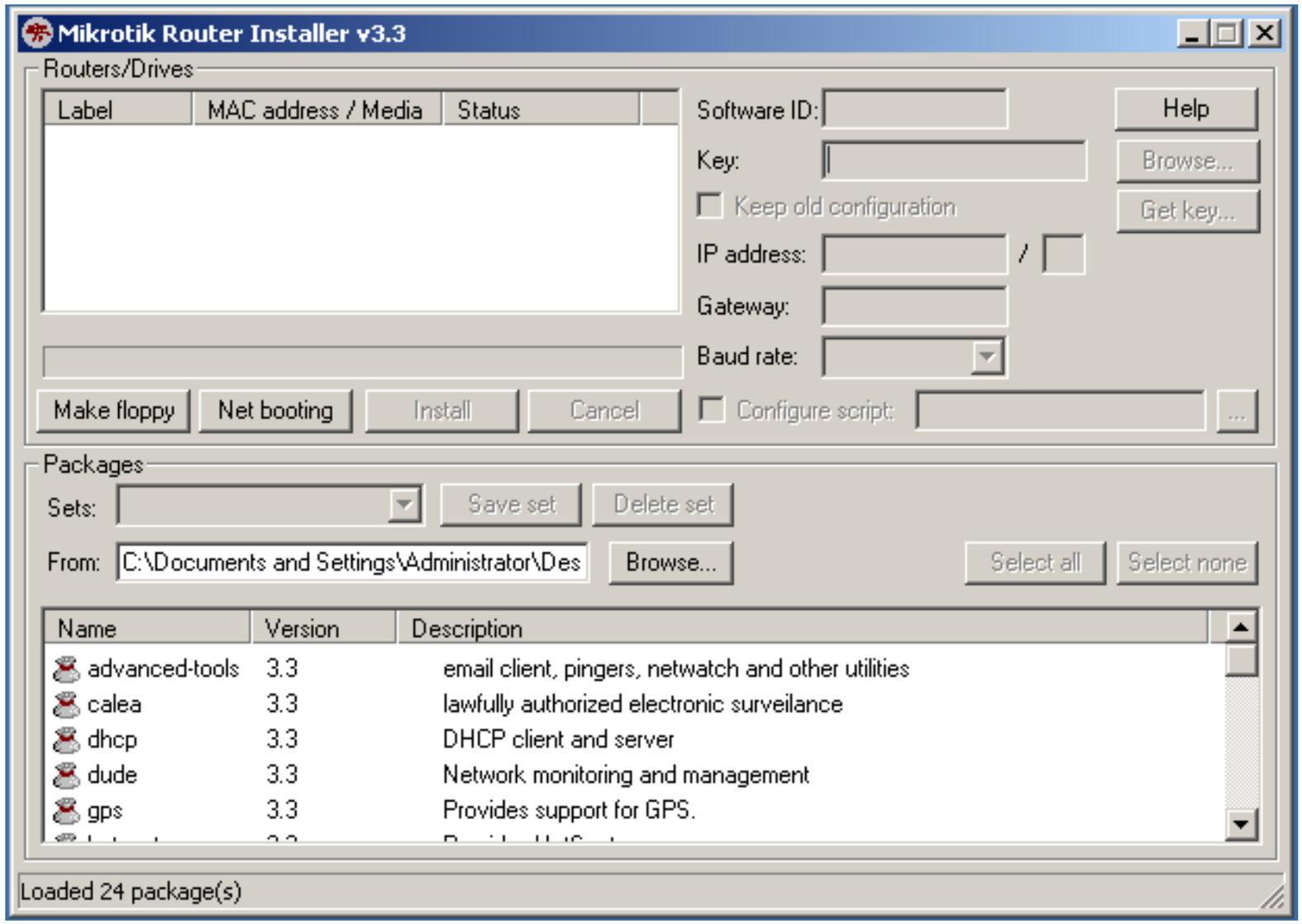
- Create Backup and Export files
- Download them to your laptop
- Open export file with text editor

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



6

LAB

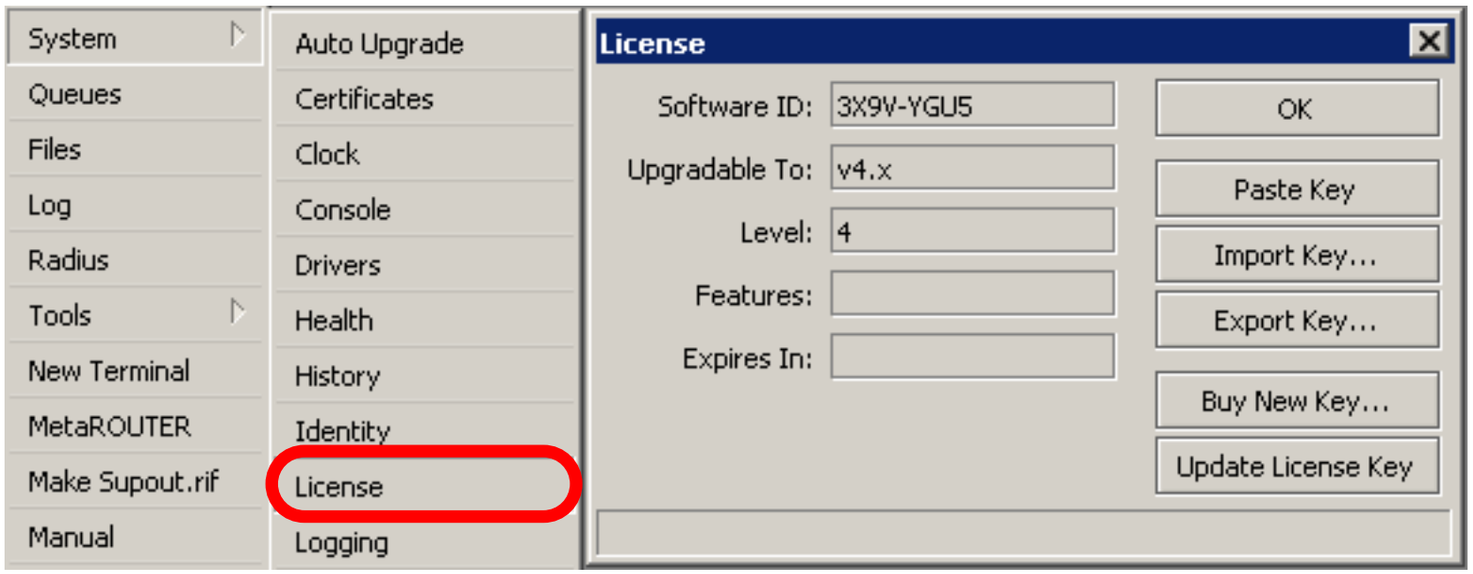
Optional Lab

- 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

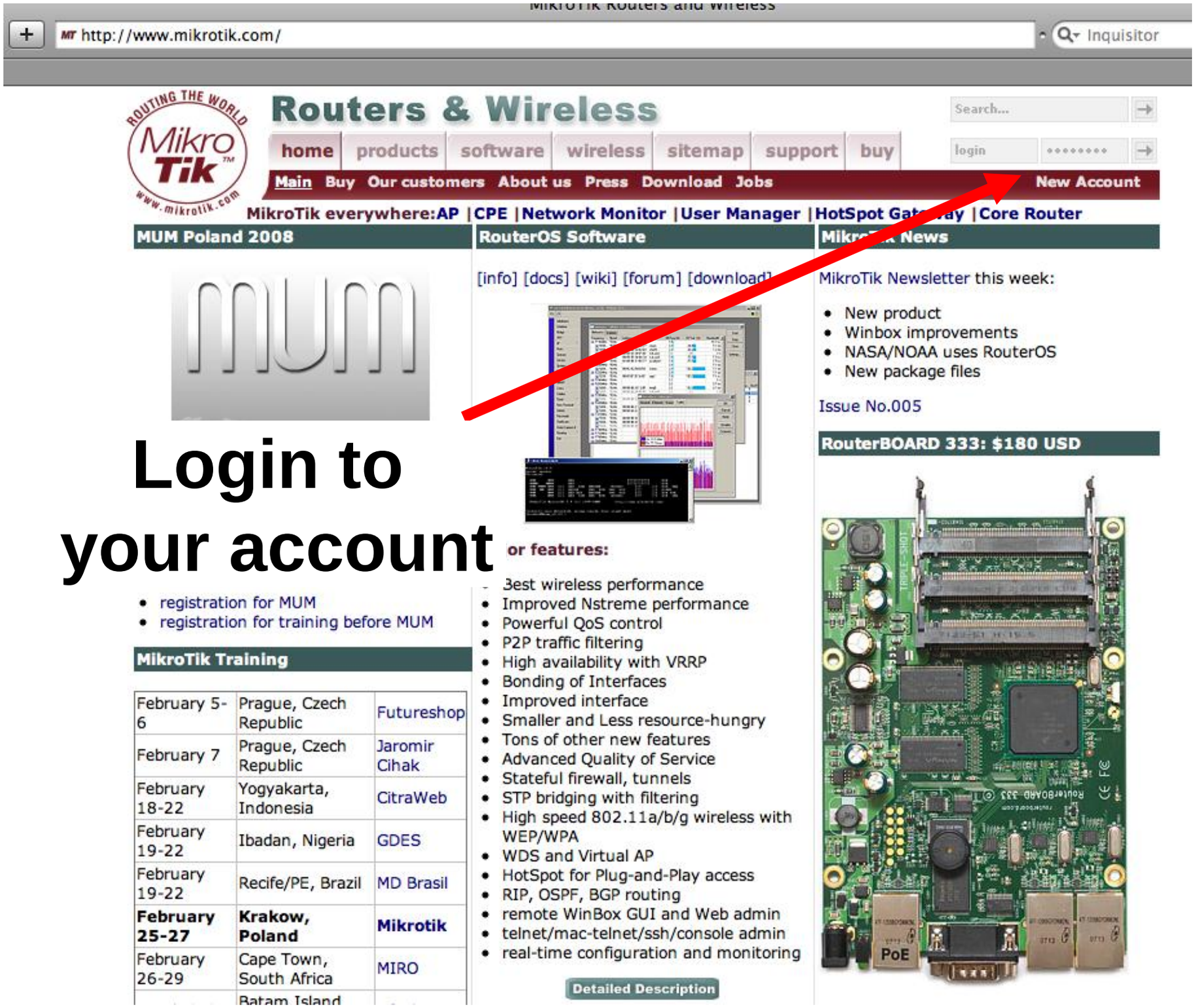
RouterOS License

- 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

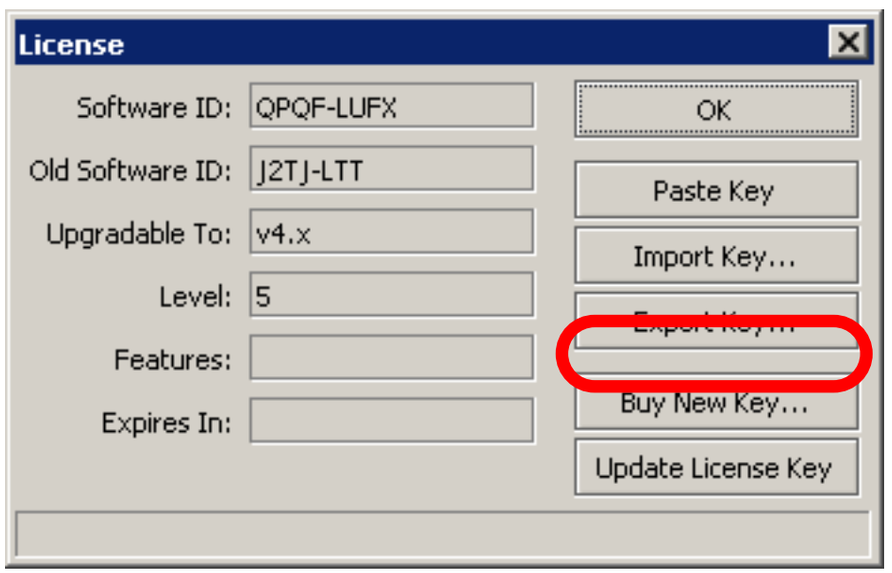
License


System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Make Supout.rif
Manual
Auto Upgrade
Certificates
Clock
Console
Drivers
Health
History
Identity
License
Logging
License
Software ID:
3X9V-YGU5
Upgradable To:
v4.x
Level:
4
Features:
Expires In:
OK
Paste Key
Import Key...
Export Key...
Buy New Key...
Update License Key

Obtain License



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

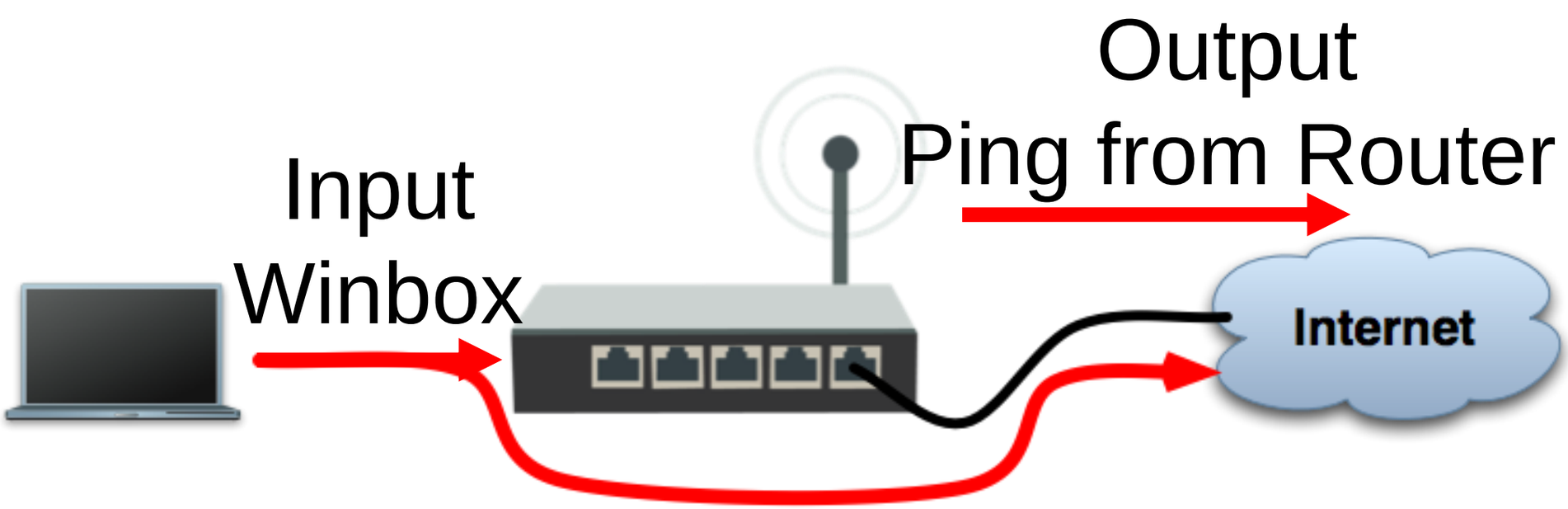
Firewall Filter

- 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

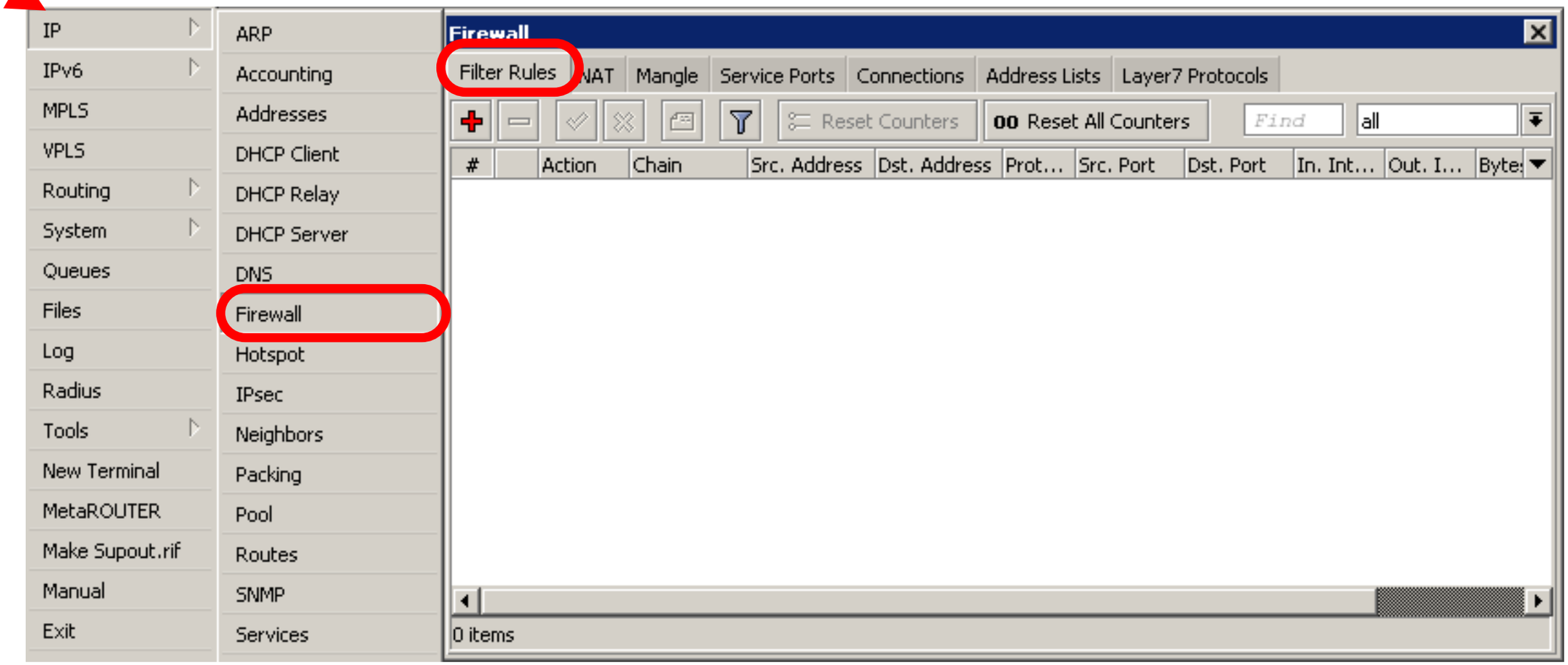
Filter Chains

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

Firewall Chains



Firewall Chains

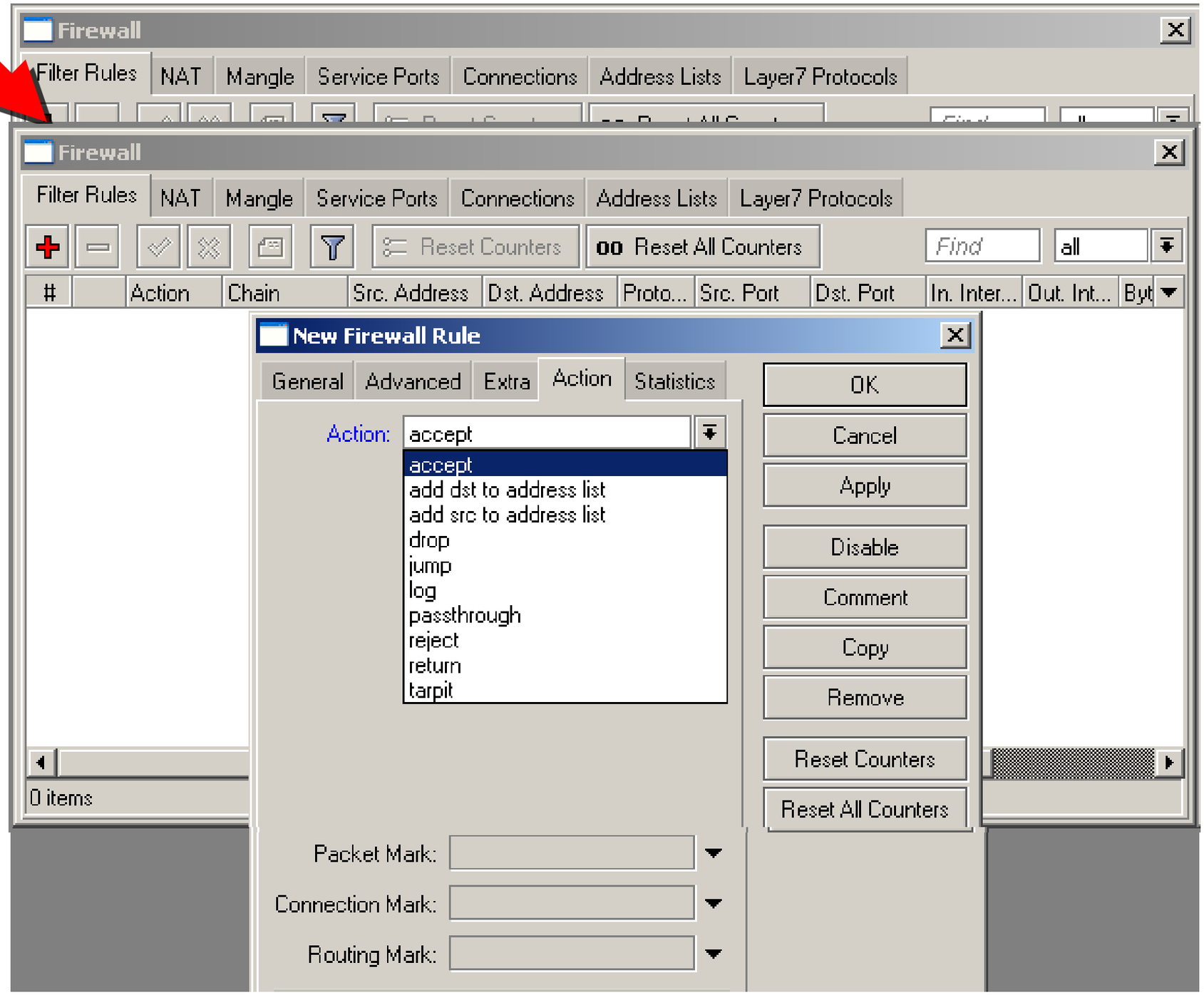


Input

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

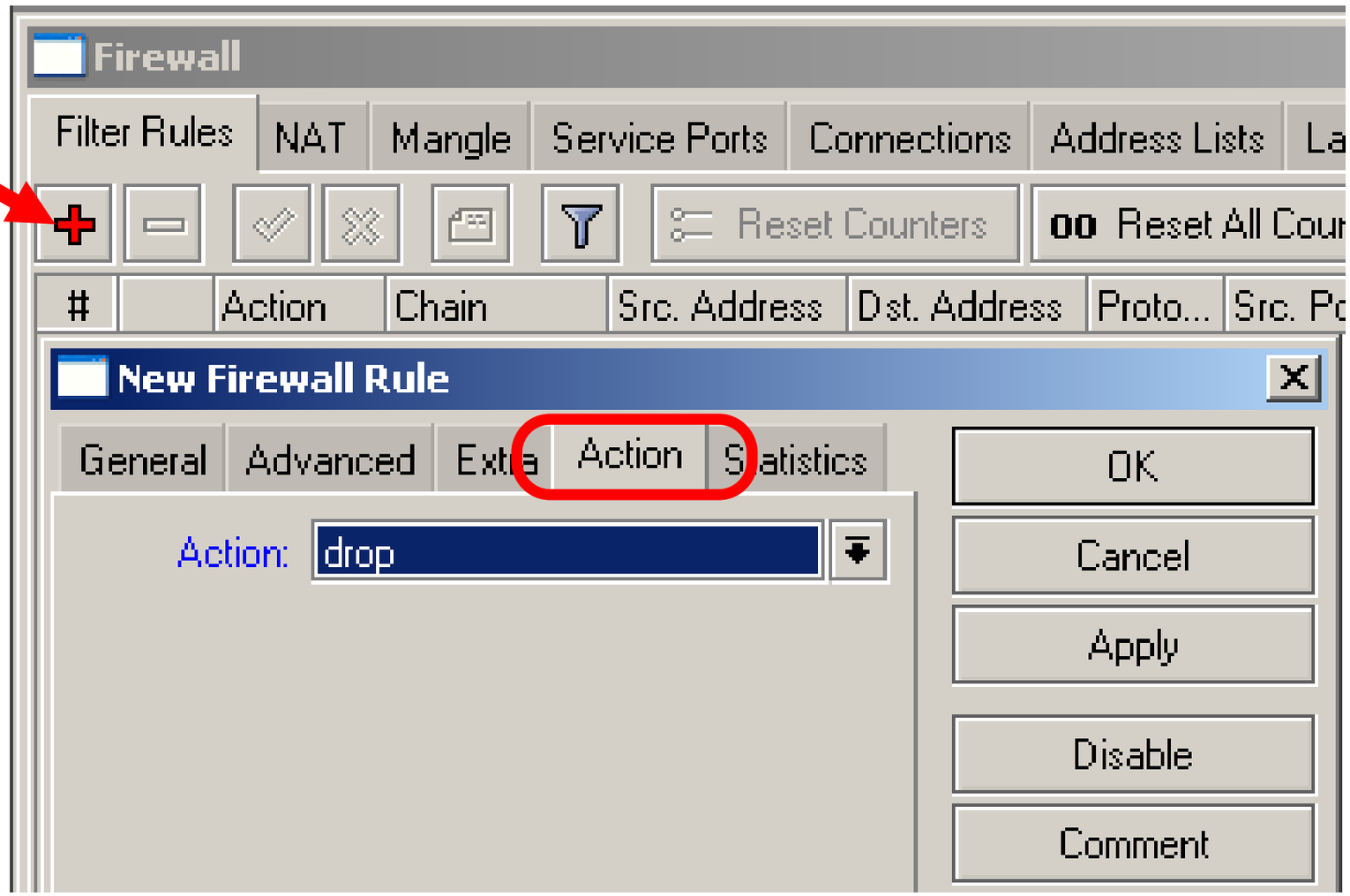
Input

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



Input

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



LAB

Input Lab

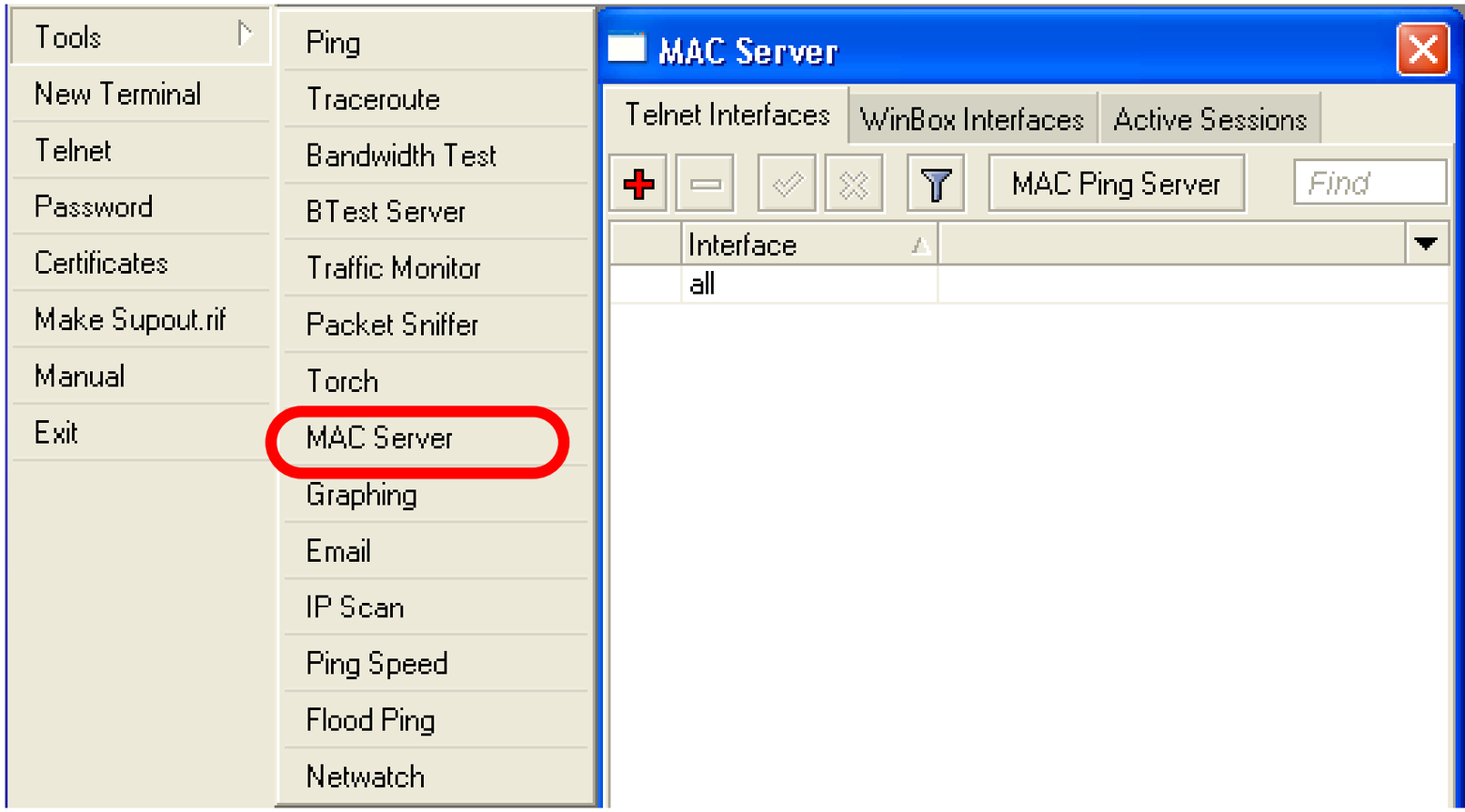
- Change your laptop IP address, 192.168.x.y
- Try to connect. The firewall is working
- You can still connect with MAC-address, Firewall Filter is only for IP

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

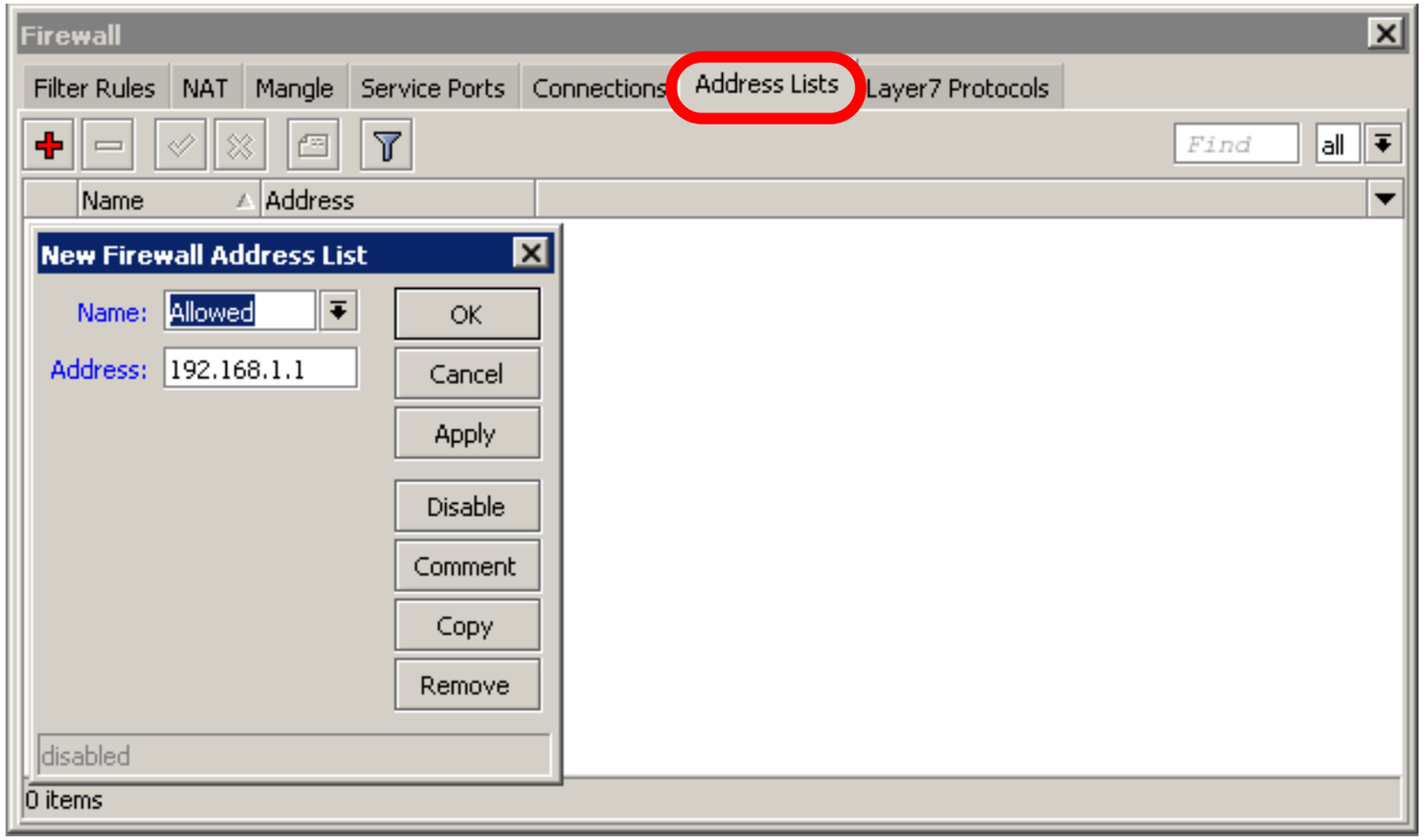


Address-List

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

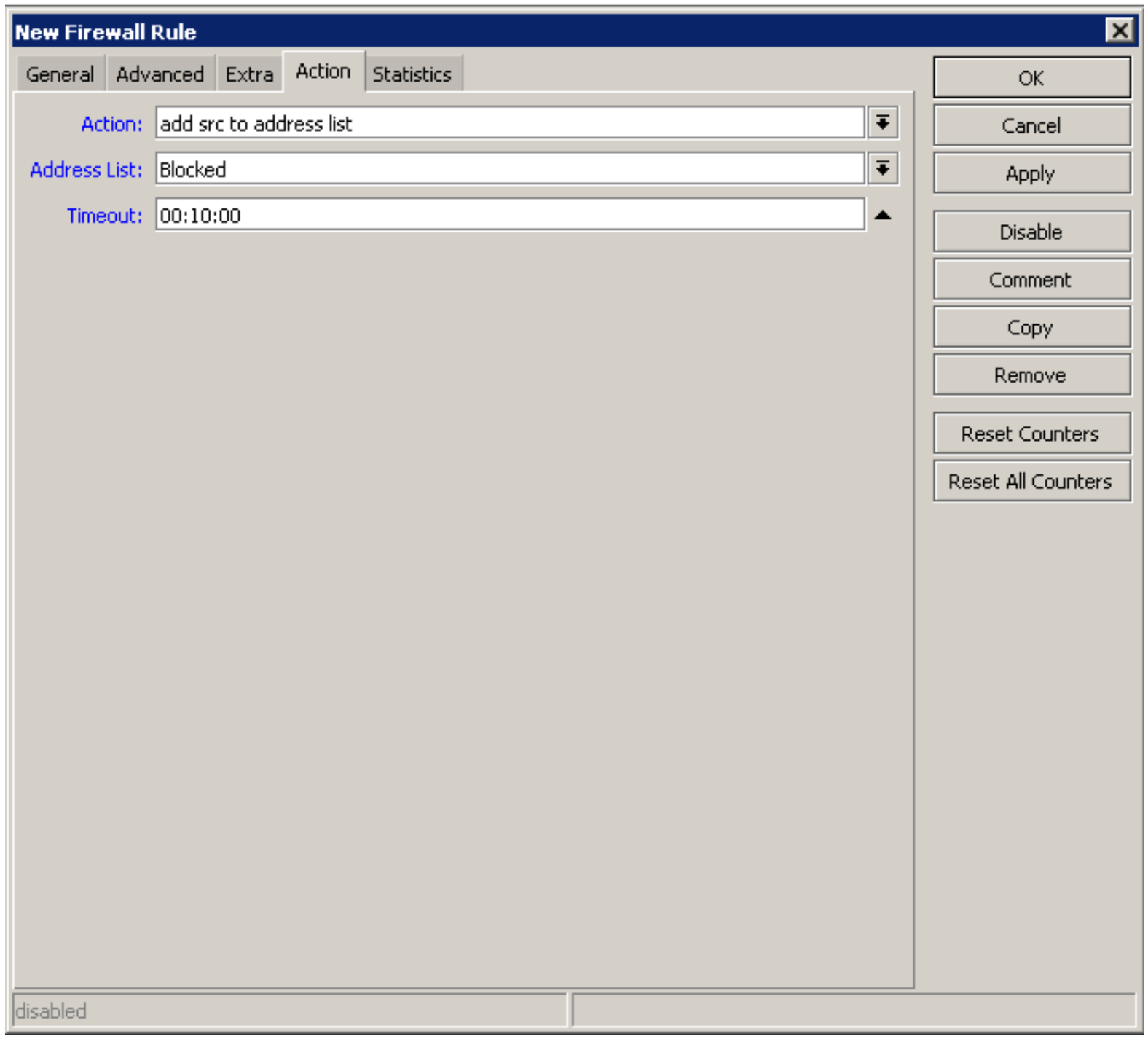
Address-List

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



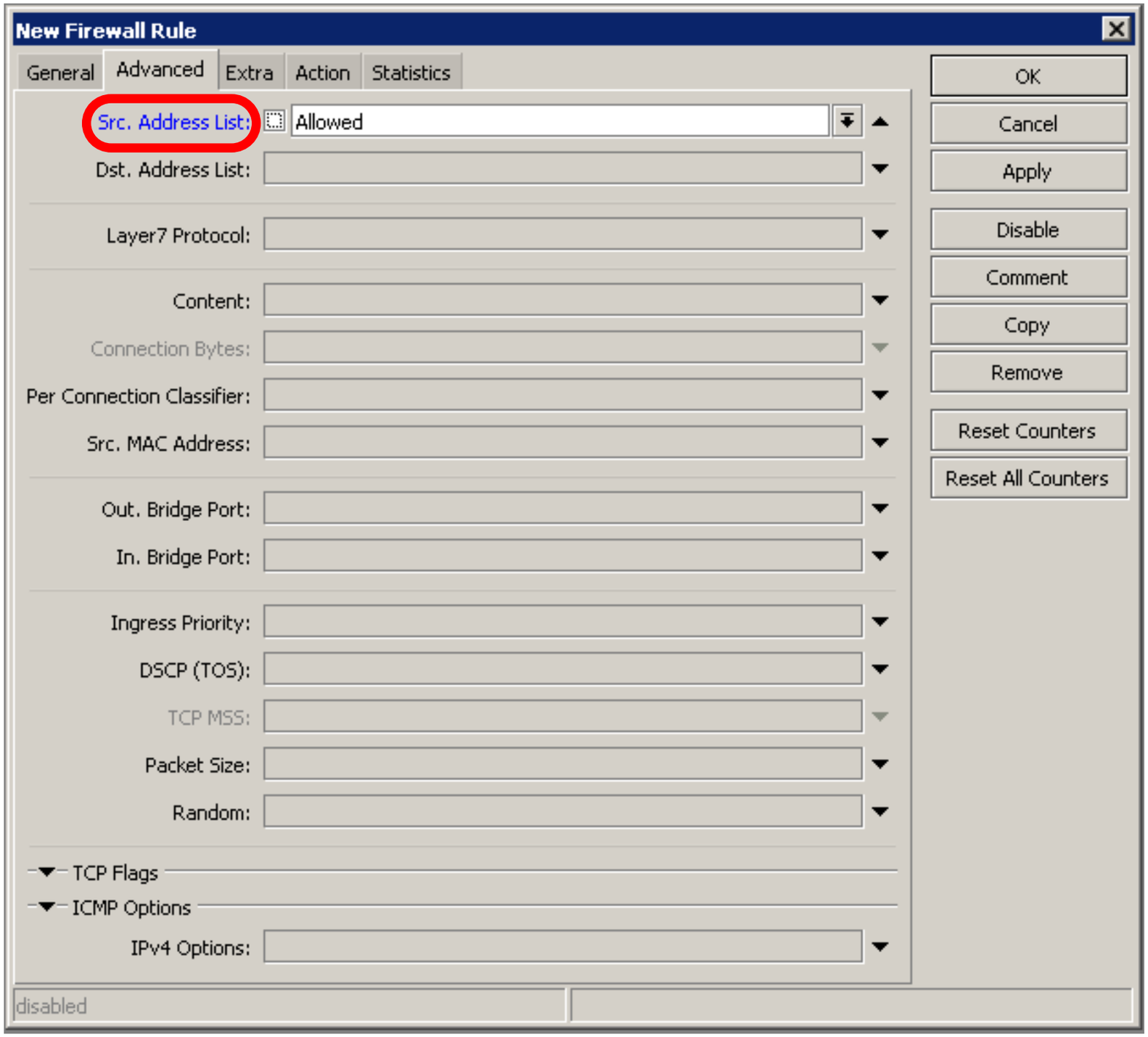
Address-List

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



Address-List in Firewall

- Ability to block by source and destination addresses



Address-List Lab

LAB

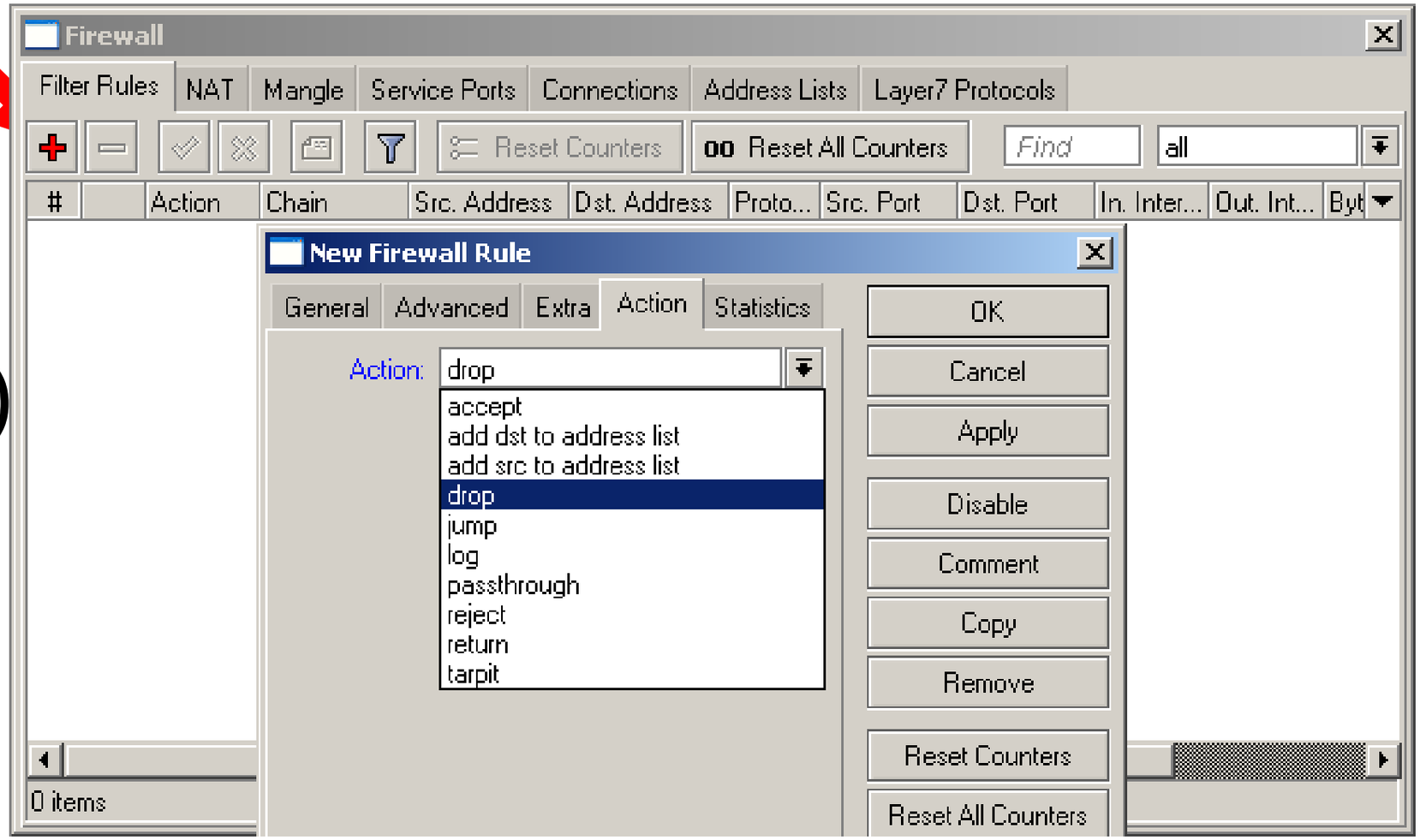
- Create address-list with allowed IP addresses
- Add accept rule for the allowed addresses

Forward

- Chain contains rules that control packets going **trough** 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



LAB

Forward

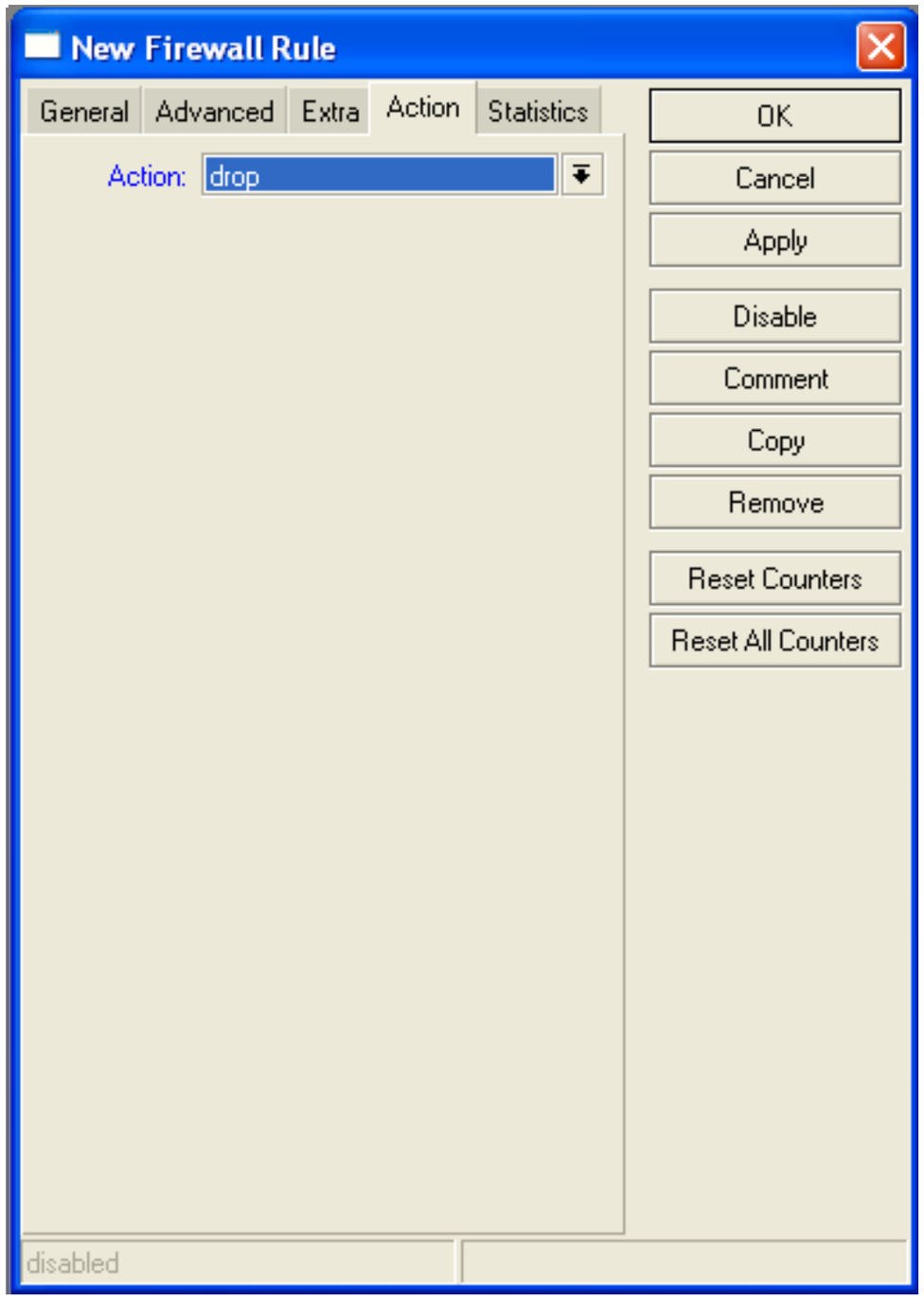
- Try to open www.mikrotik.com
- Try to open http://192.168.X.254
- Router web page works because drop rule is for **chain=forward** traffic

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

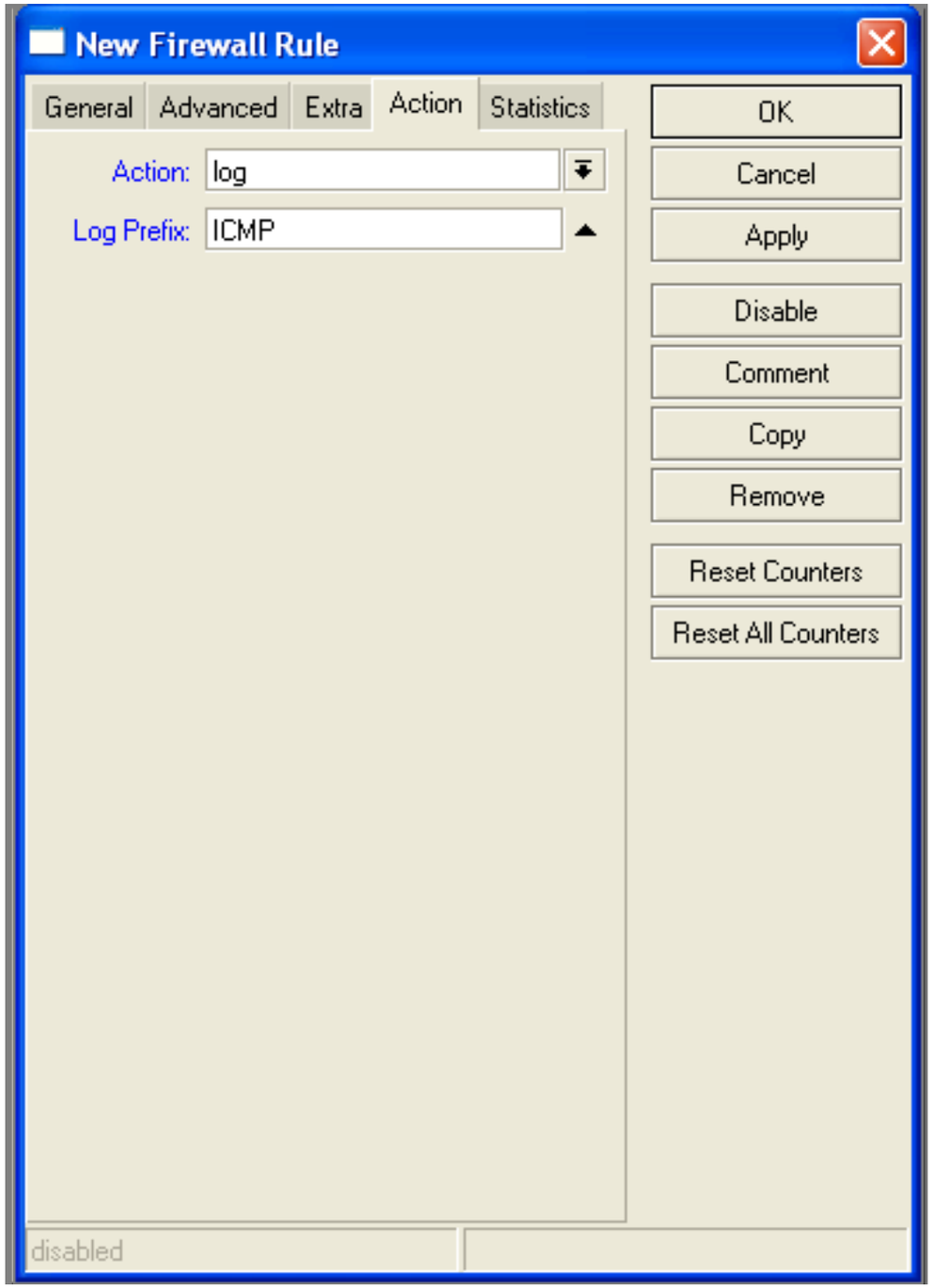
Forward

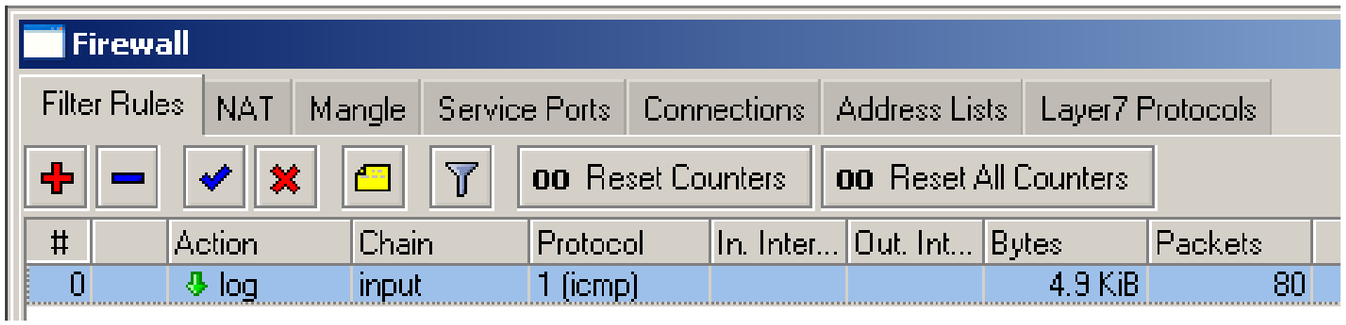
Create a rule that will block client's p2p traffic



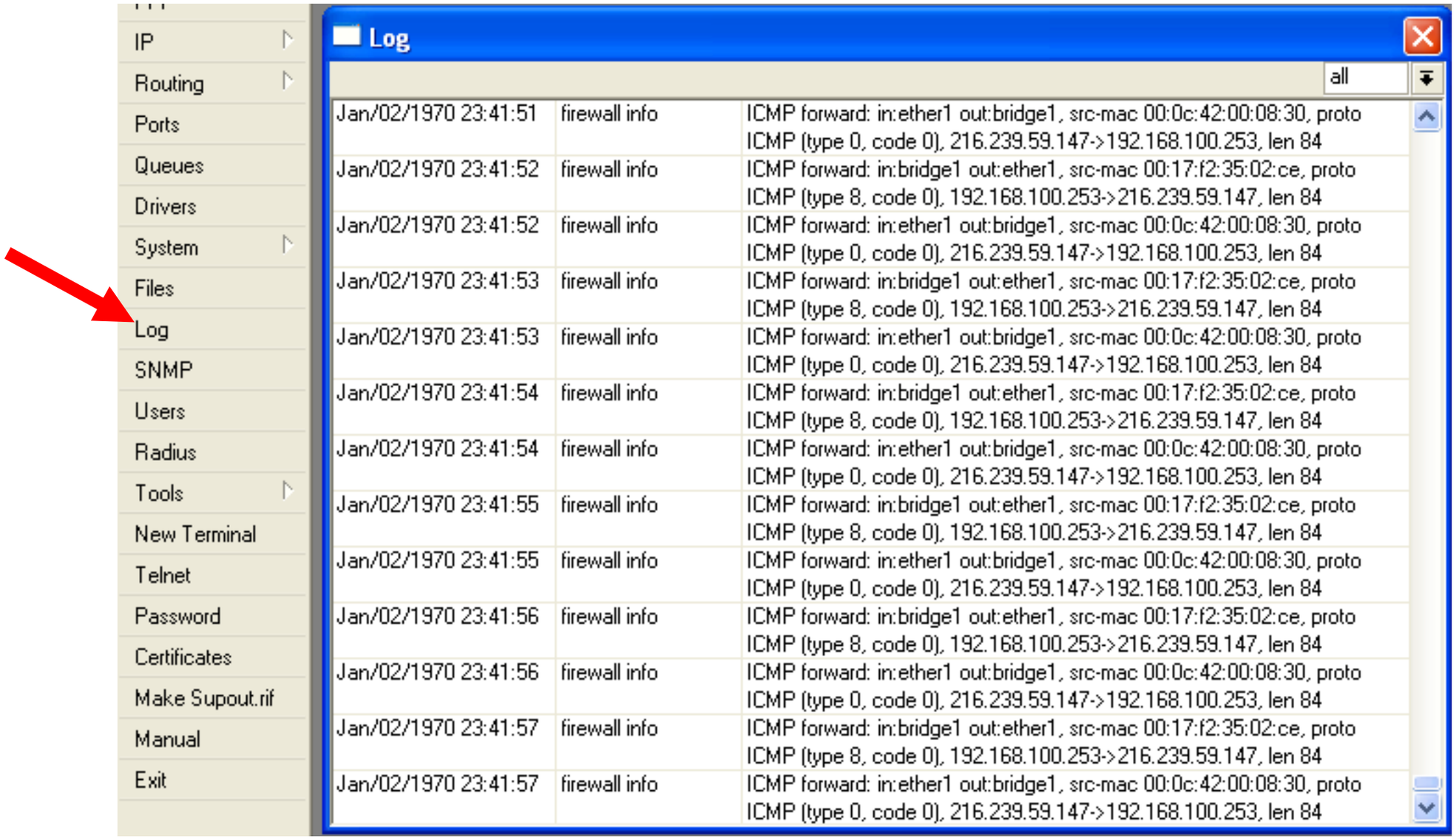
Firewall Log

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





Firewall Log

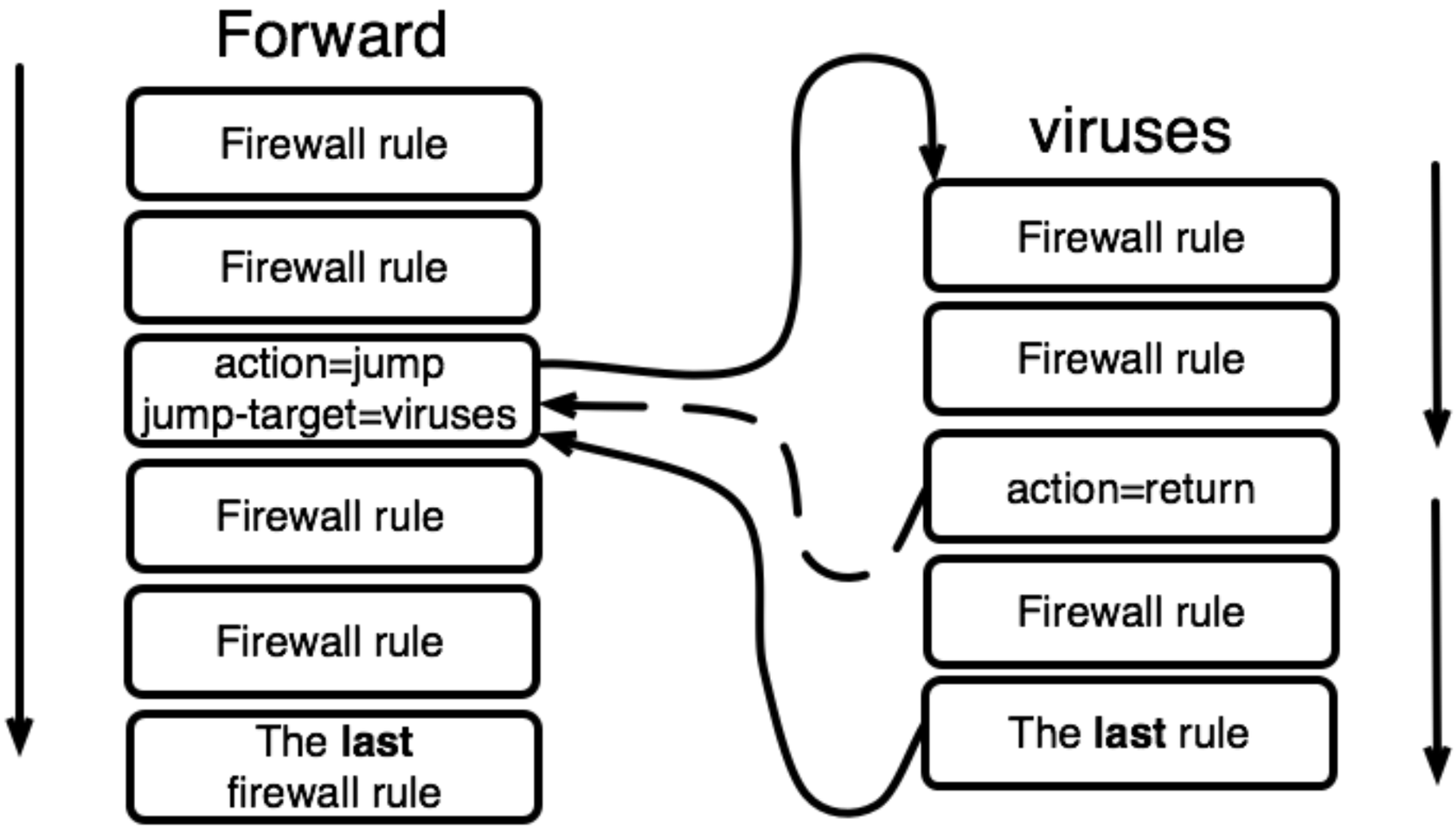


Firewall chains

- 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.

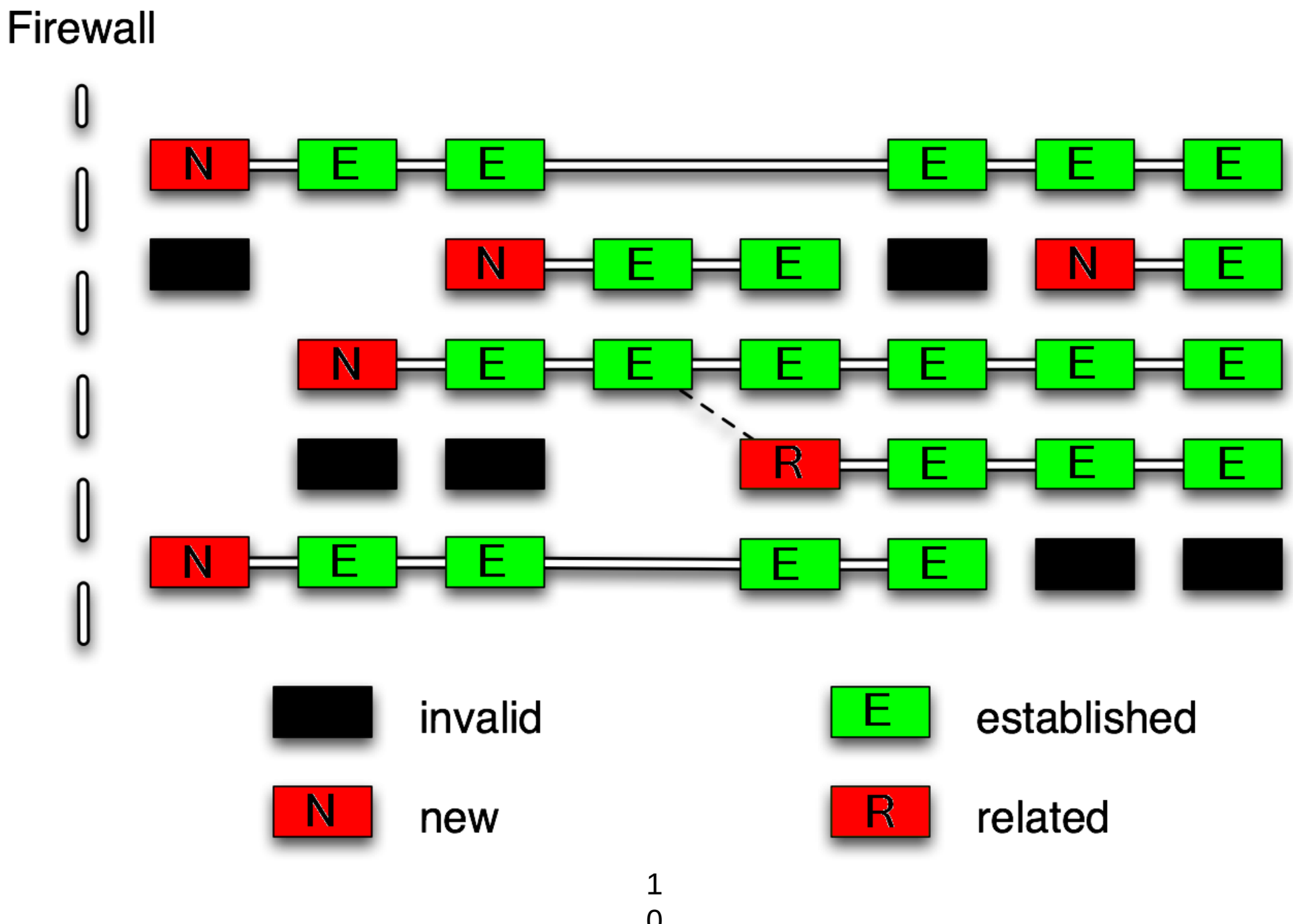


Firewall chain Lab

LAB

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

Connections



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

LAB

- 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**

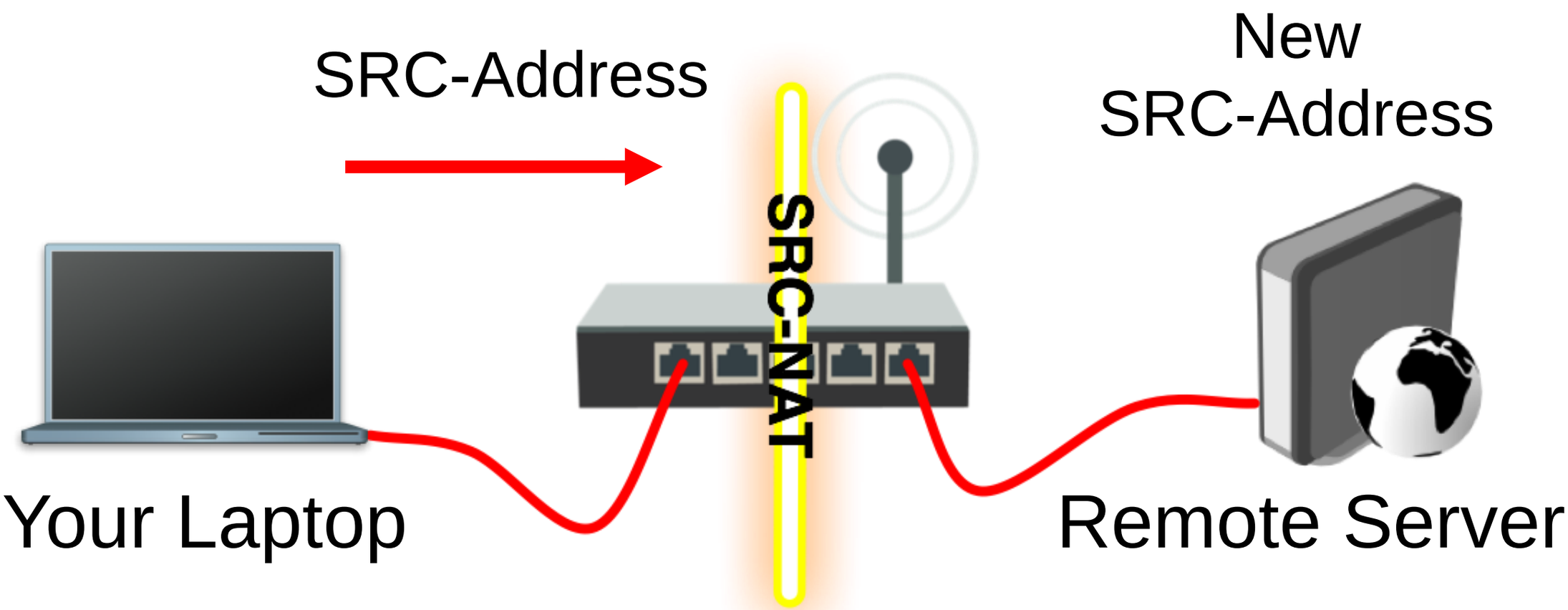
Summary

Network Address Translation

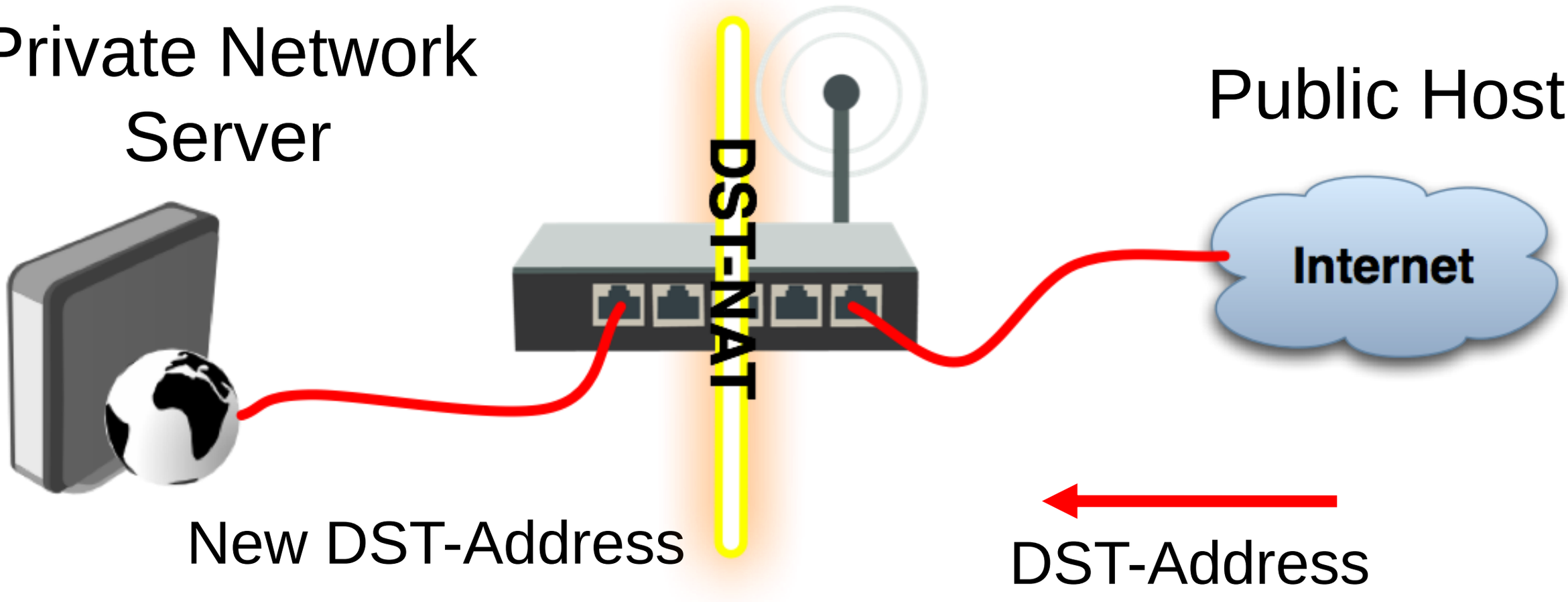
NAT

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

SRC-NAT


SRC-Address
New
SRC-Address
SRC-NAT
Your Laptop
Remote Server

DST-NAT


Private Network
Server
Public Host
DST-NAT
Internet
New DST-Address
DST-Address

NAT Chains

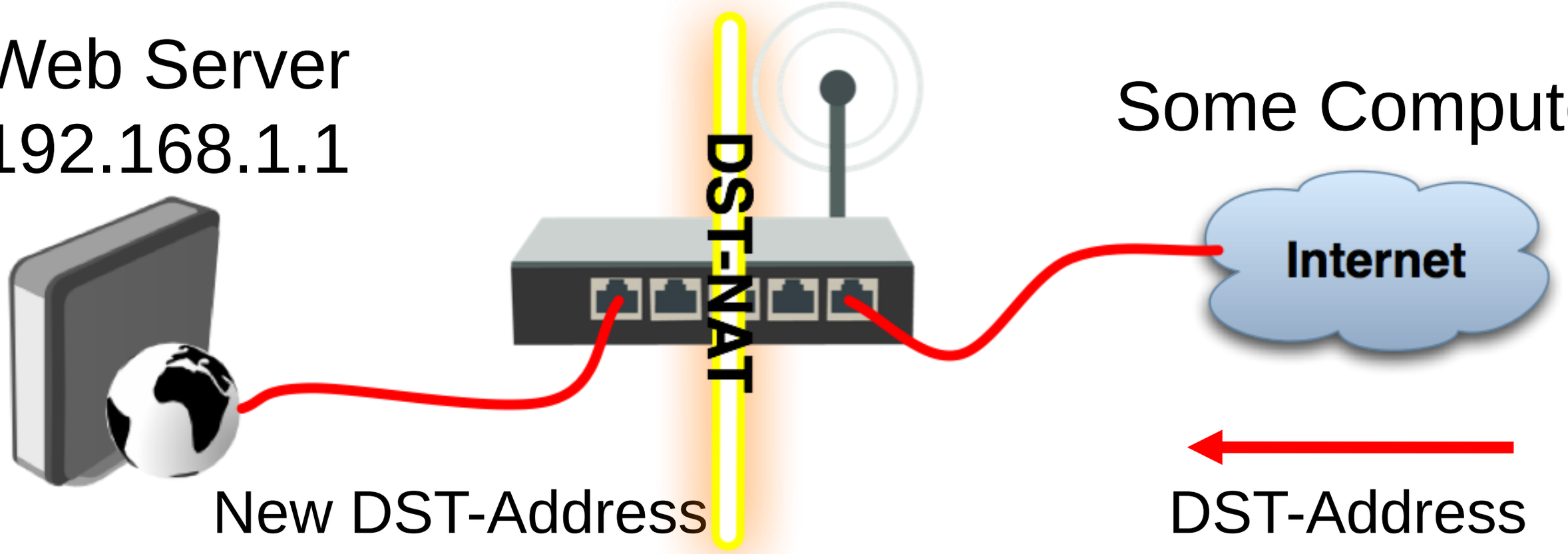
- To achieve these scenarios you have to order your NAT rules in appropriate chains: **dstnat** or **srcnat**
- NAT rules work on **IF-THEN** principle

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

Web Server
192.168.1.1



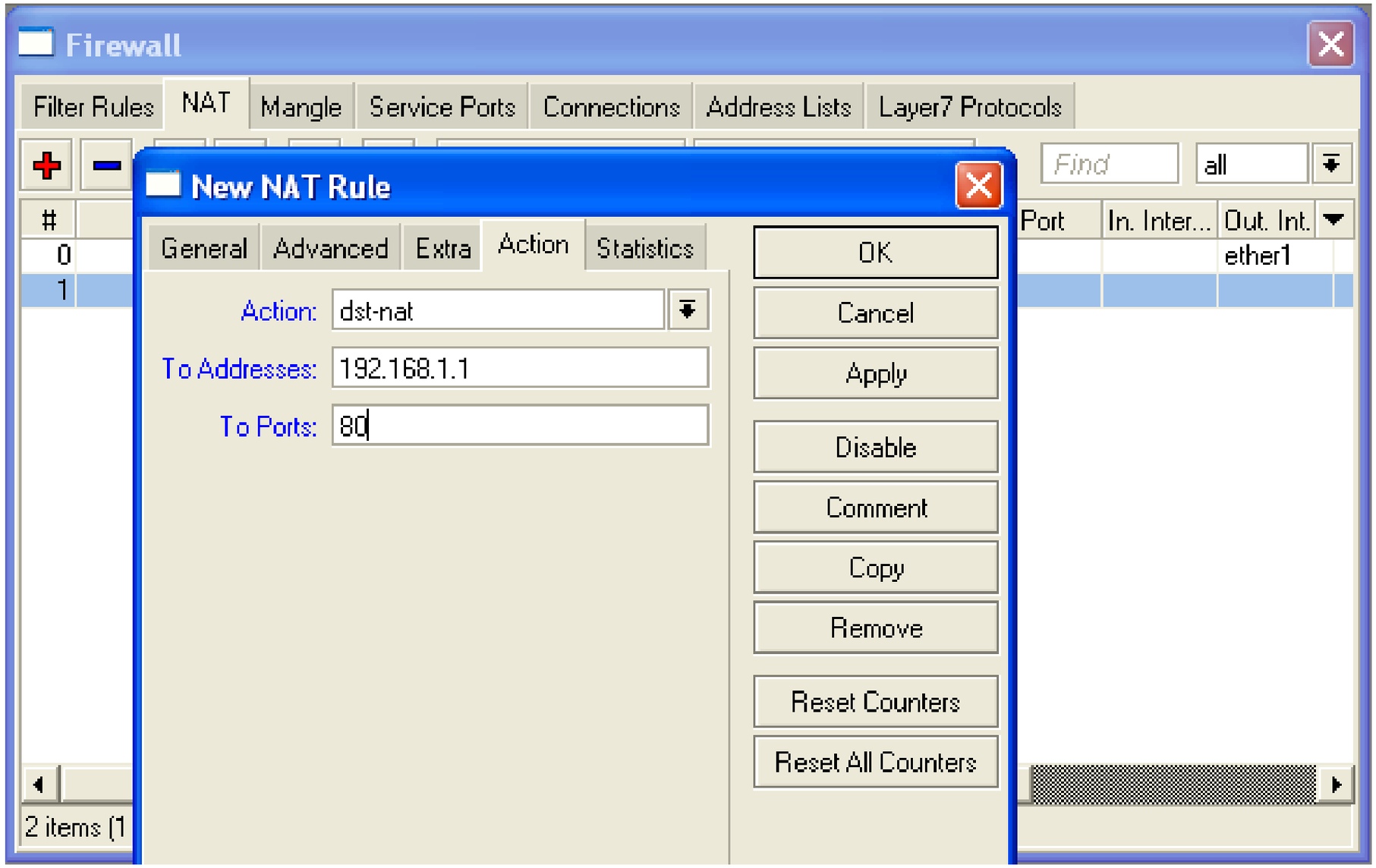
Some Computer

New DST-Address
192.168.1.1:80

DST-Address
207.141.27.45:80

DST-NAT Example

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

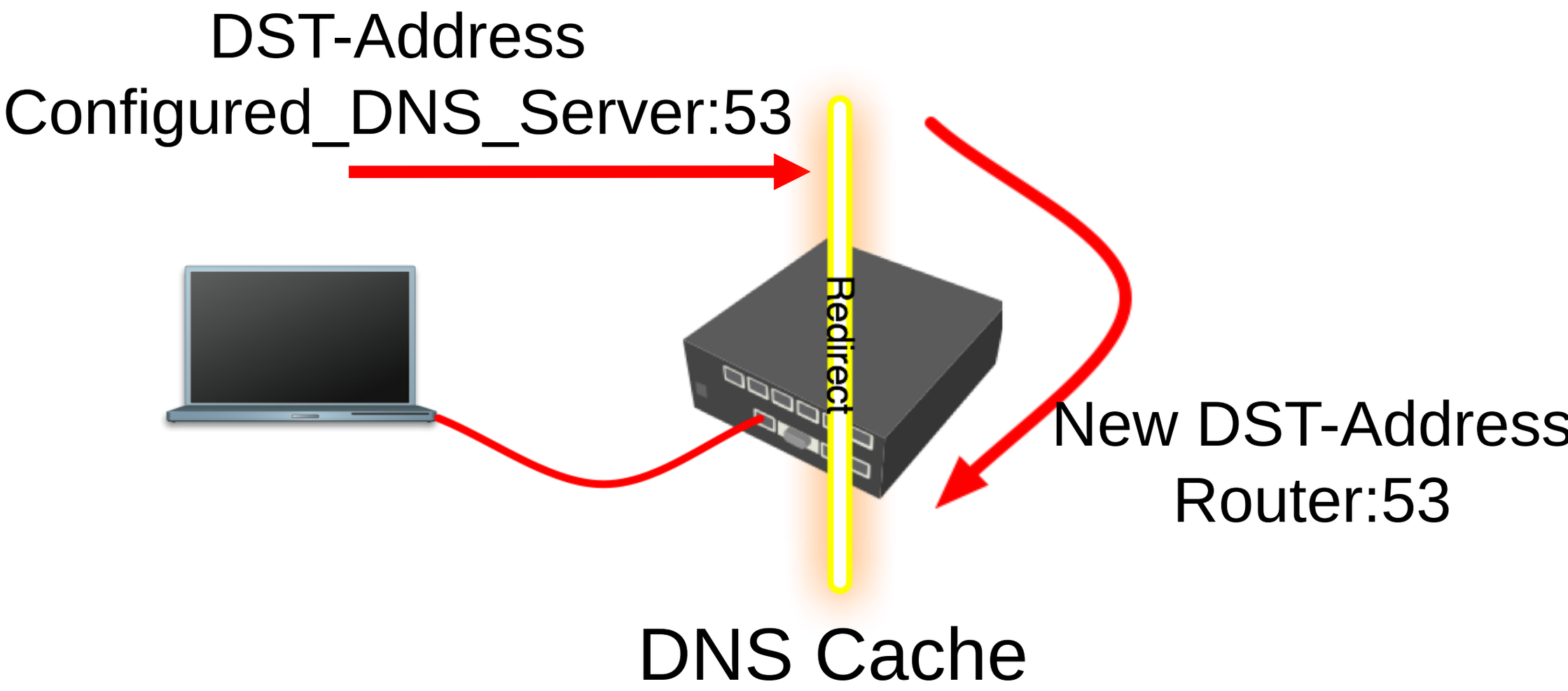


1

Redirect

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

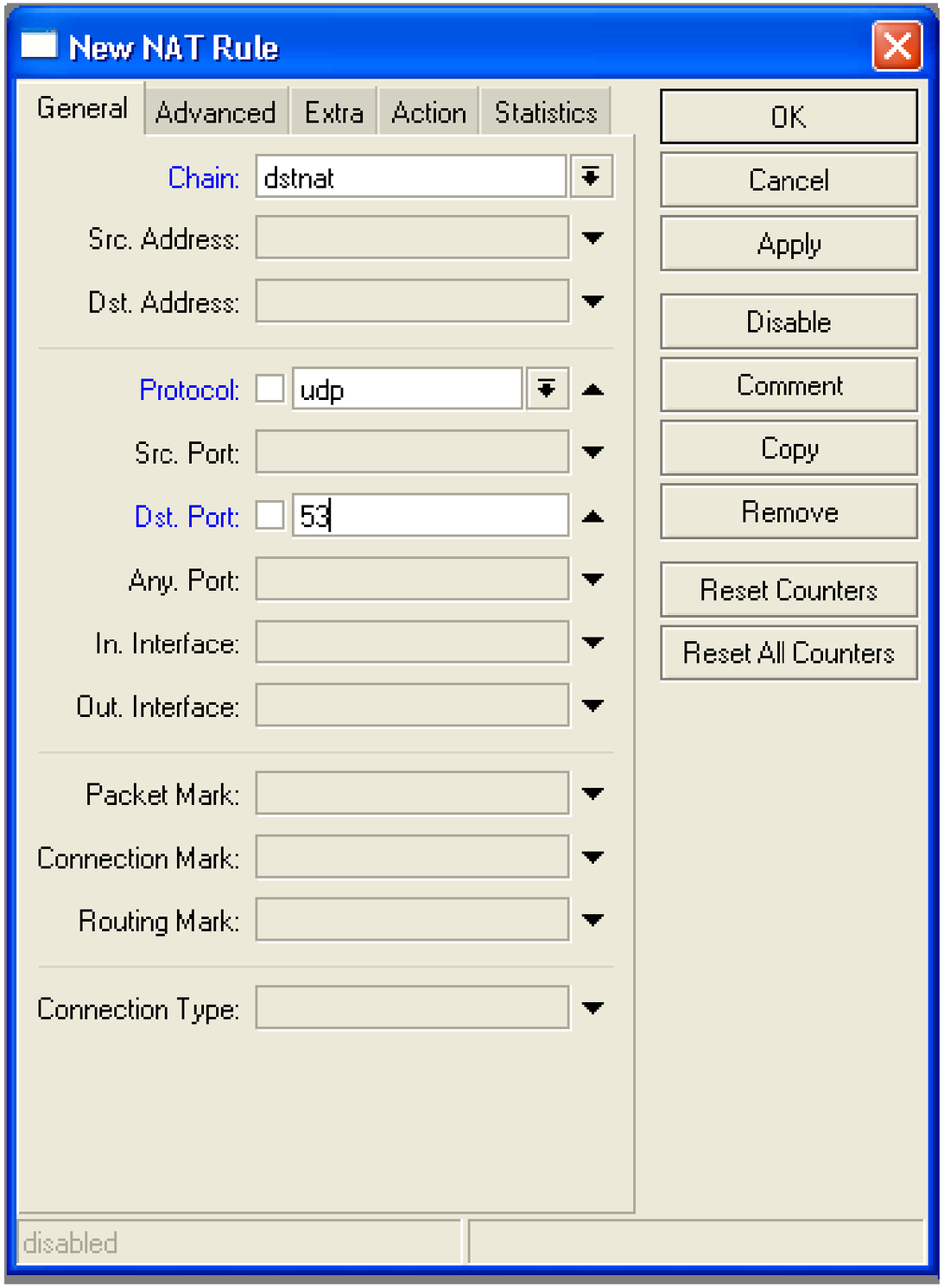
Redirect example



Redirect Example

LAB

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



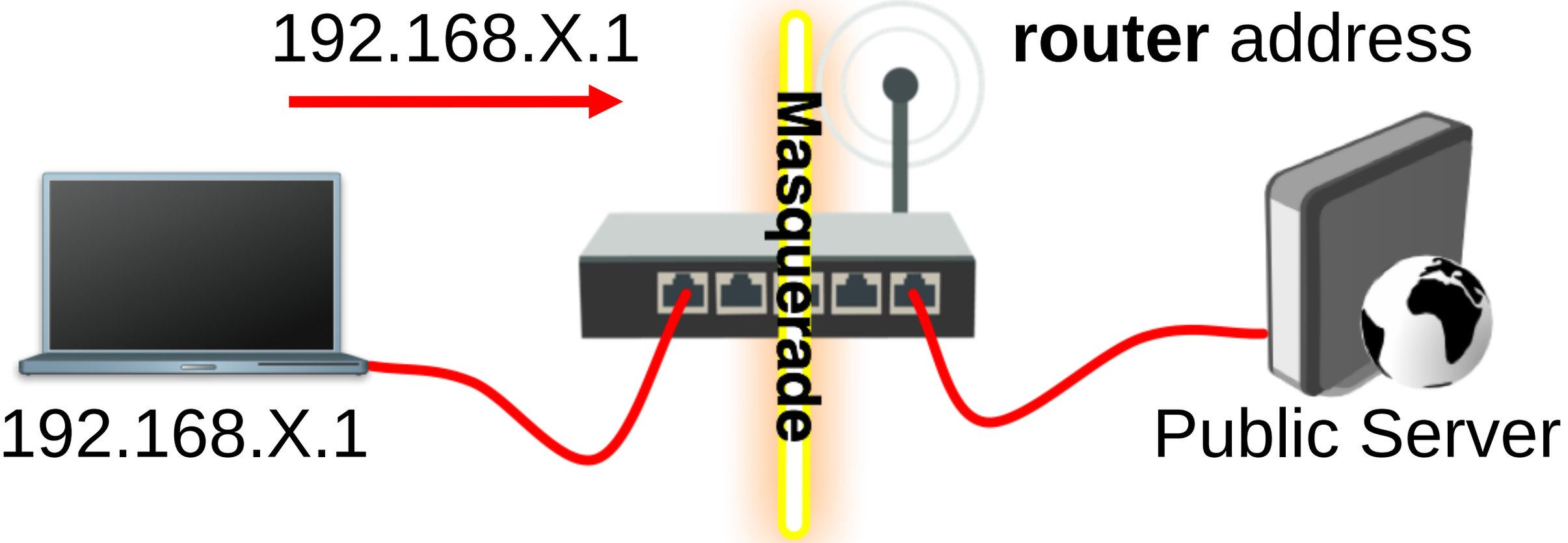
SRC-NAT

- 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 Address
192.168.X.1

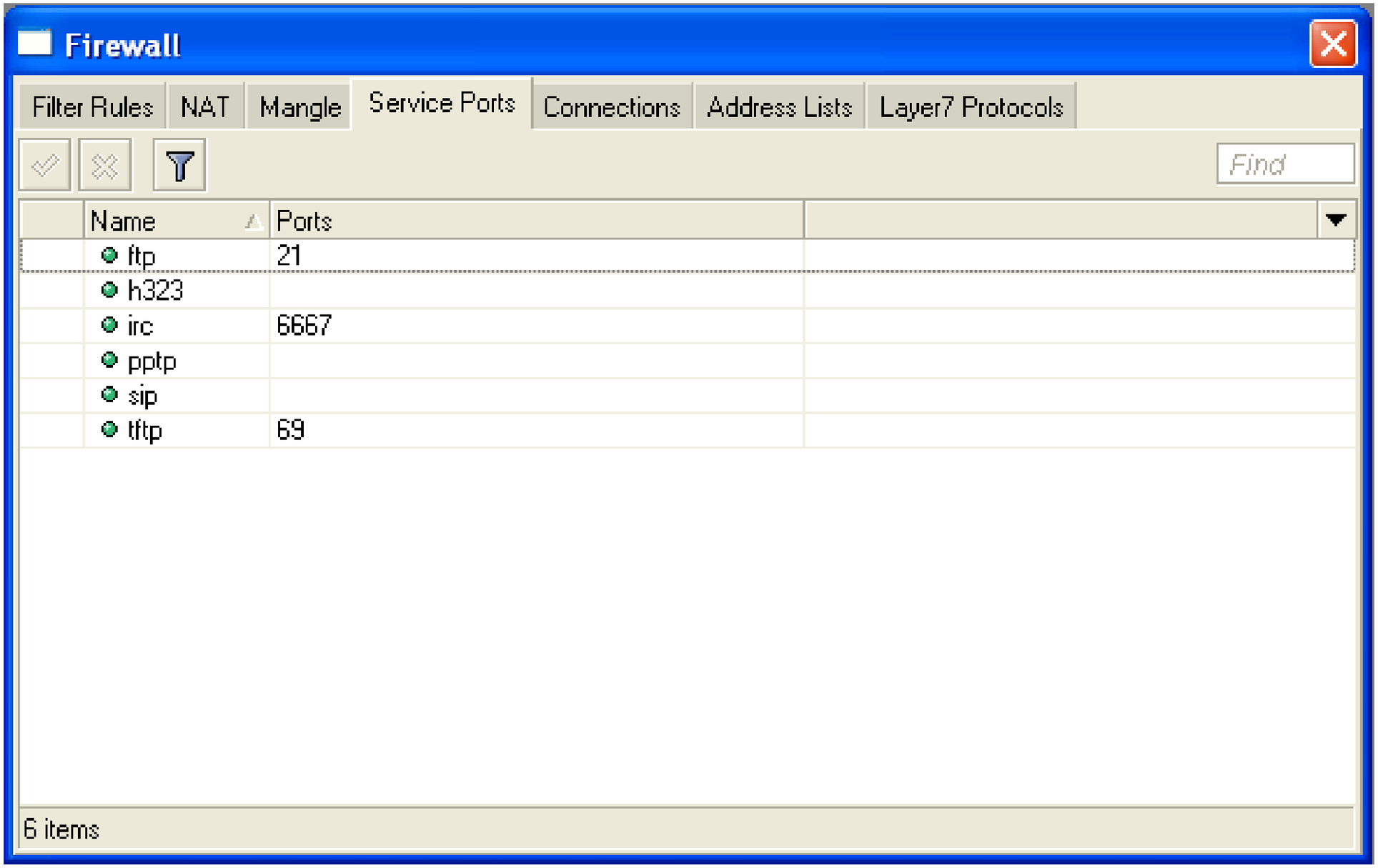
Src Address
router address



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
Filter Rules
NAT
Mangle
Service Ports
Connections
Address Lists
Layer7 Protocols
Find
Name
Ports
ftp
21
h323
irc
6667
pptp
sip
tftp
69
6 items

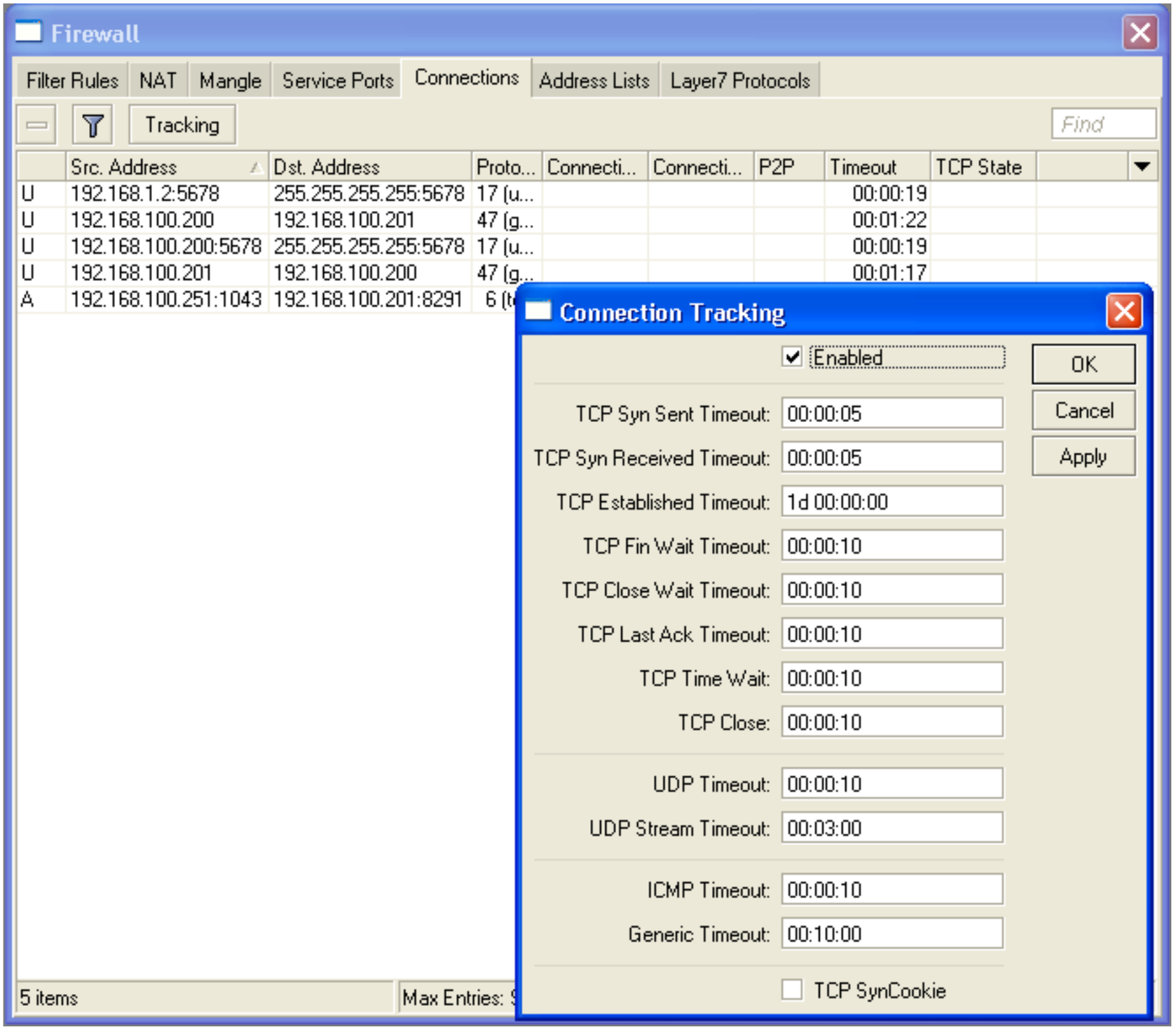
Firewall Tips

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

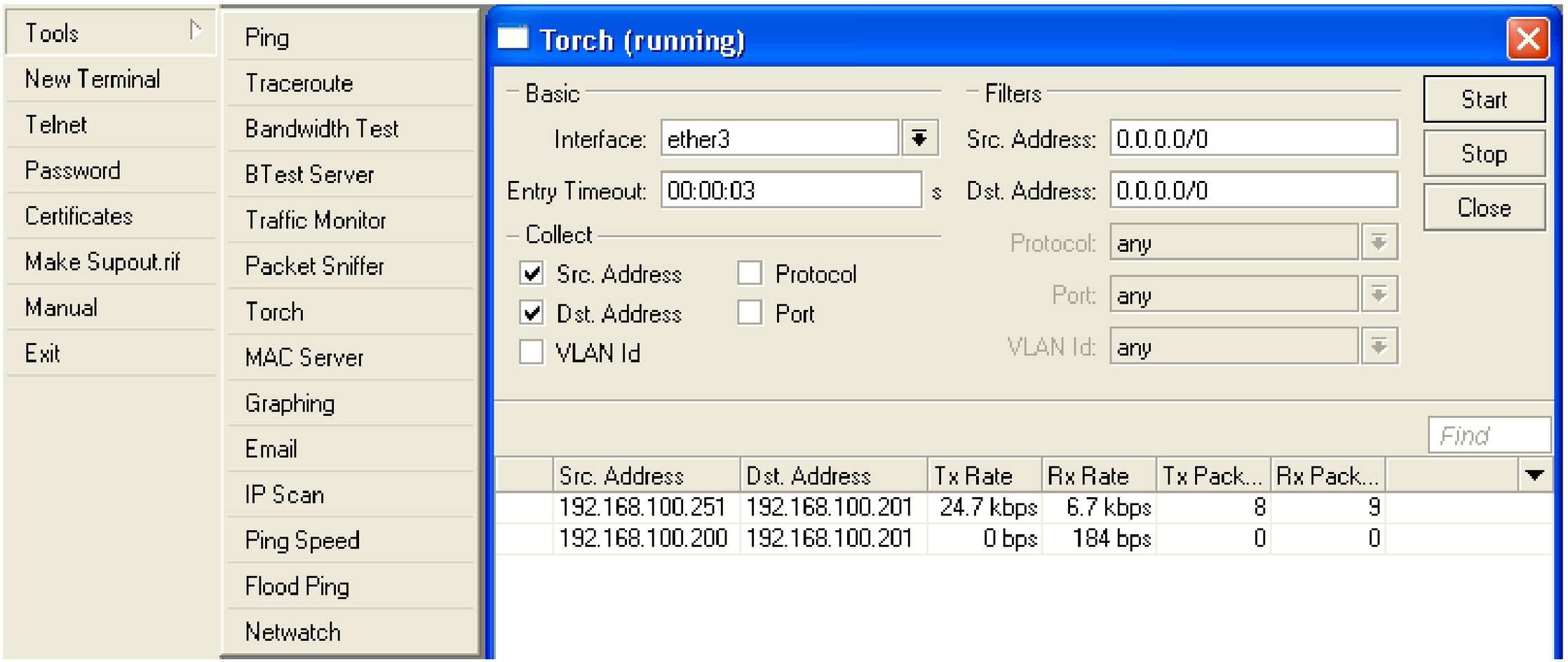
Connection Tracking

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

Connection Tracking



Torch



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

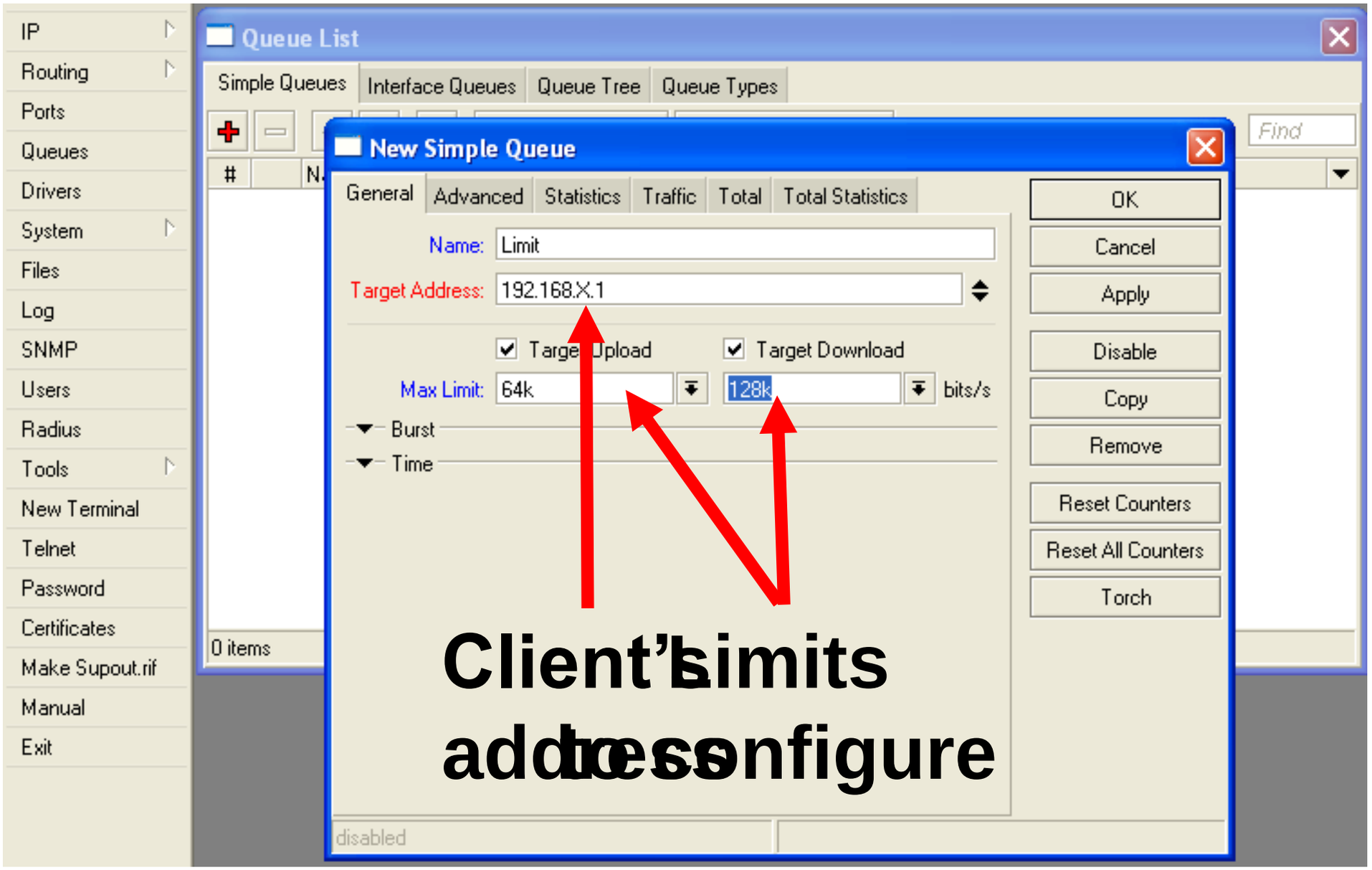
Simple Queue

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

LAB

Simple Queue

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

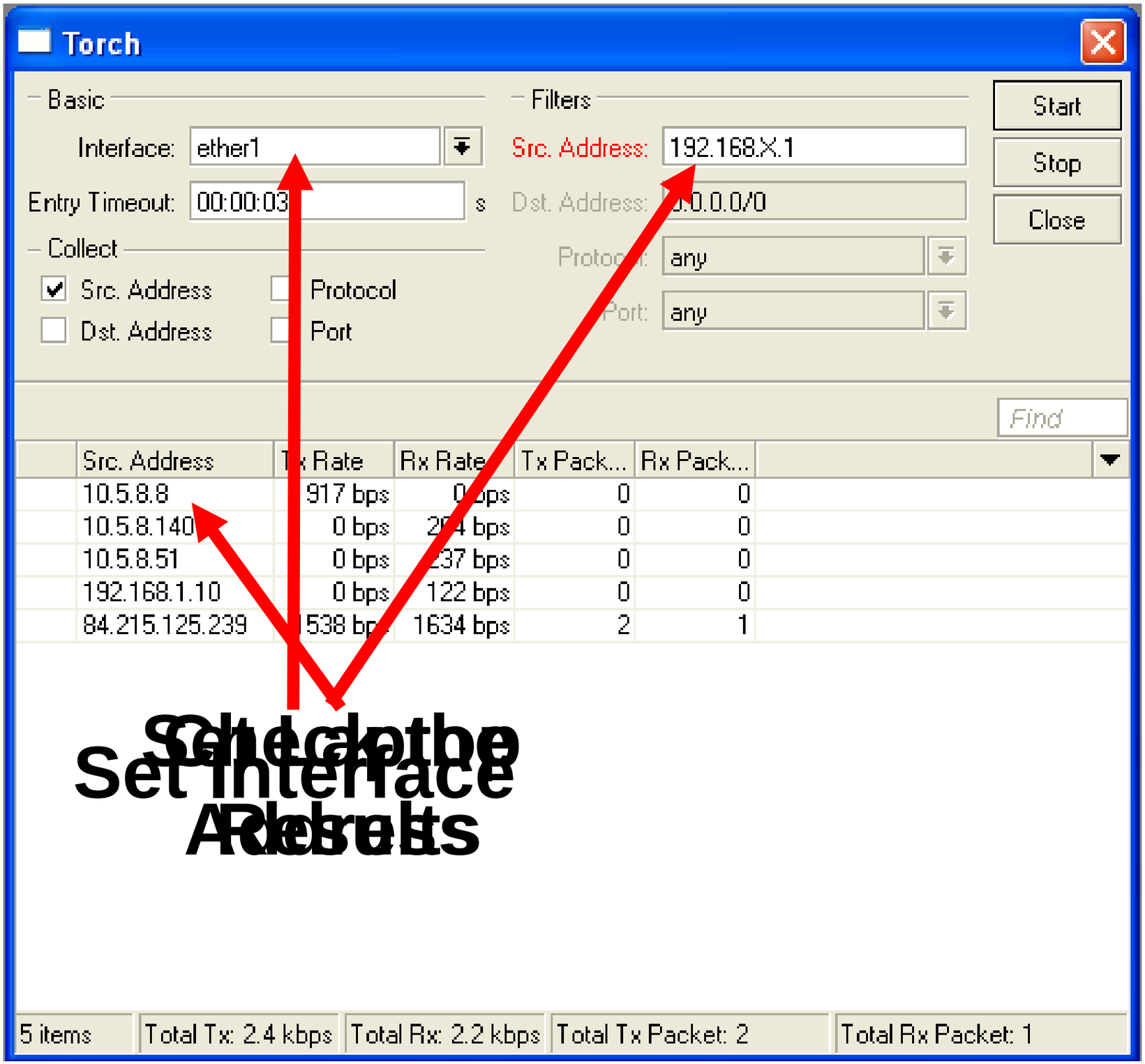


Simple Queue

- Check your limits
- Torch is showing bandwidth rate

Using Torch

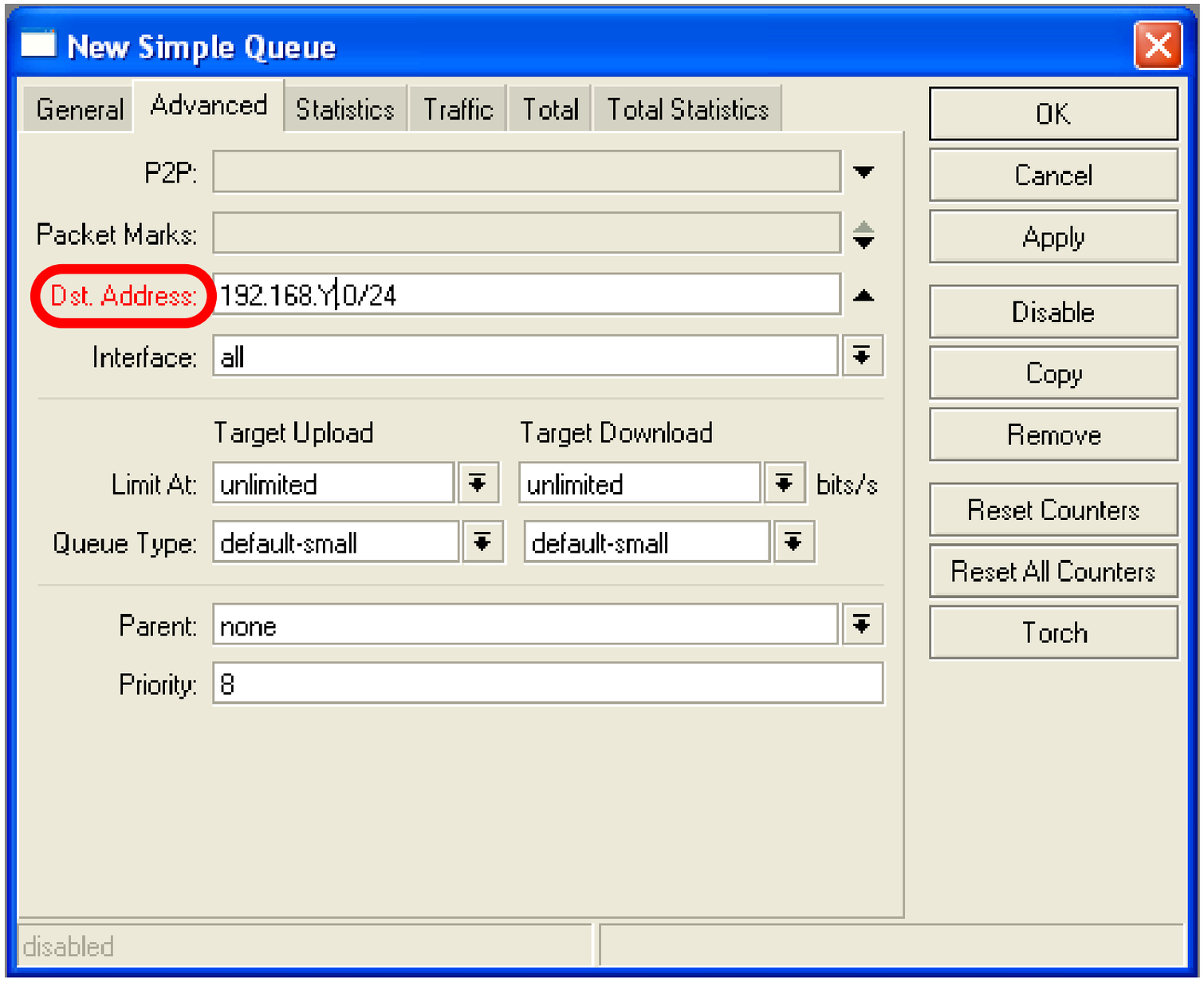
- Select local network interface
- See actual bandwidth



Specific Server Limit

LAB

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

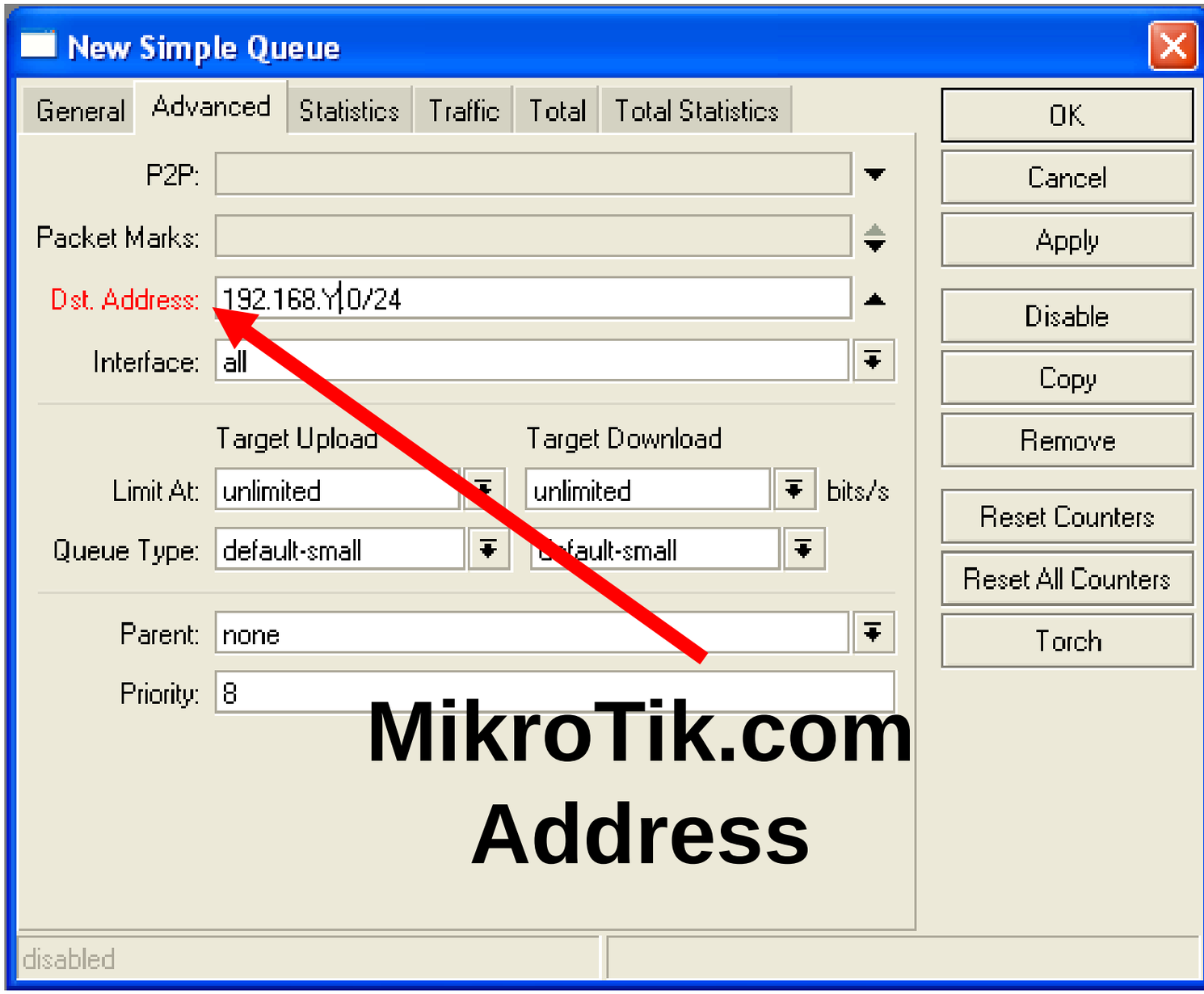


1
3

Specific Server Limit

LAB

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



Specific Server Limit

LAB

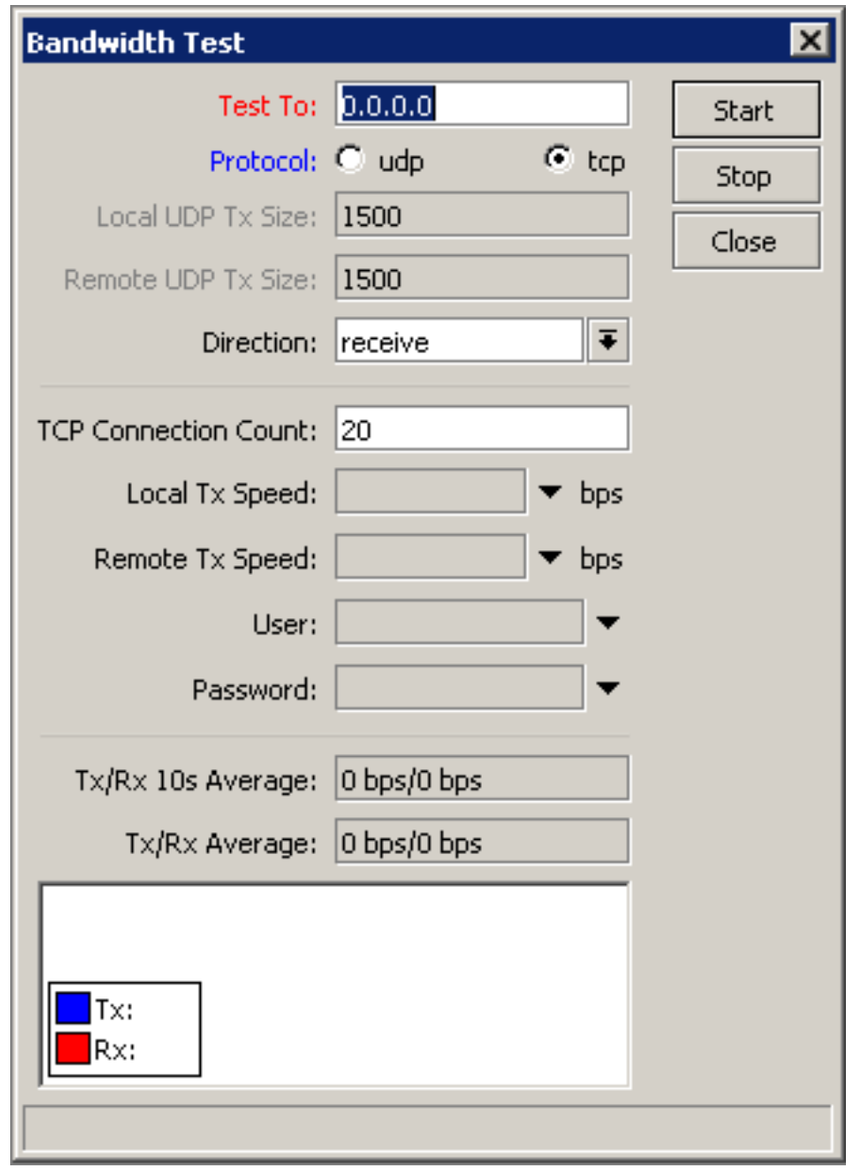
- DST-address is useful to set unlimited access to the local network resources
- Target-address and DST-addresses can be vice versa

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

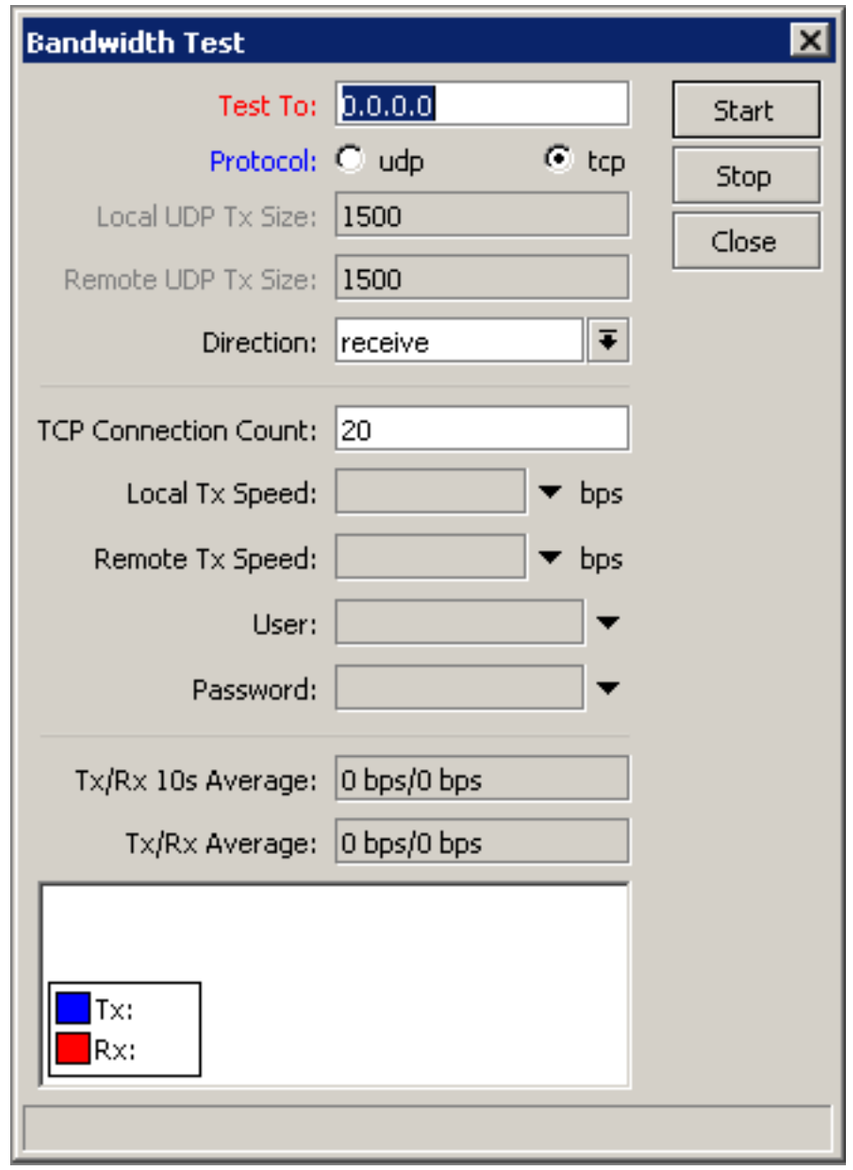
Bandwidth Test on Router

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



Bandwidth Server

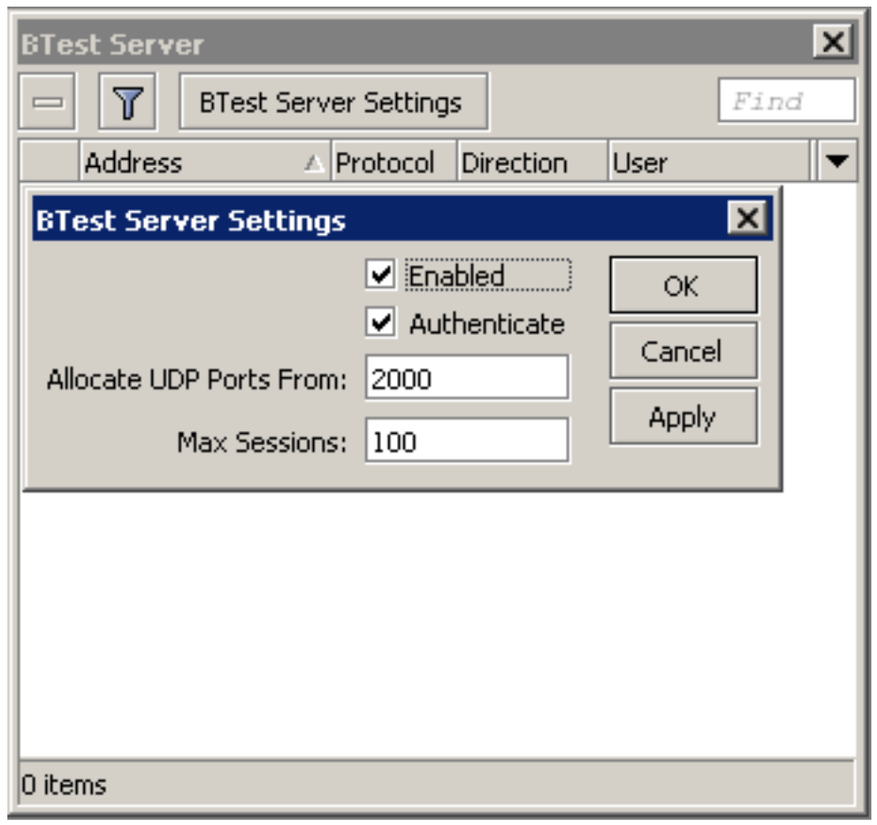
- Set **Test To** as testing address
- Select protocol
- TCP supports multiple connections
- Authentication might be required



LAB

Bandwidth Test

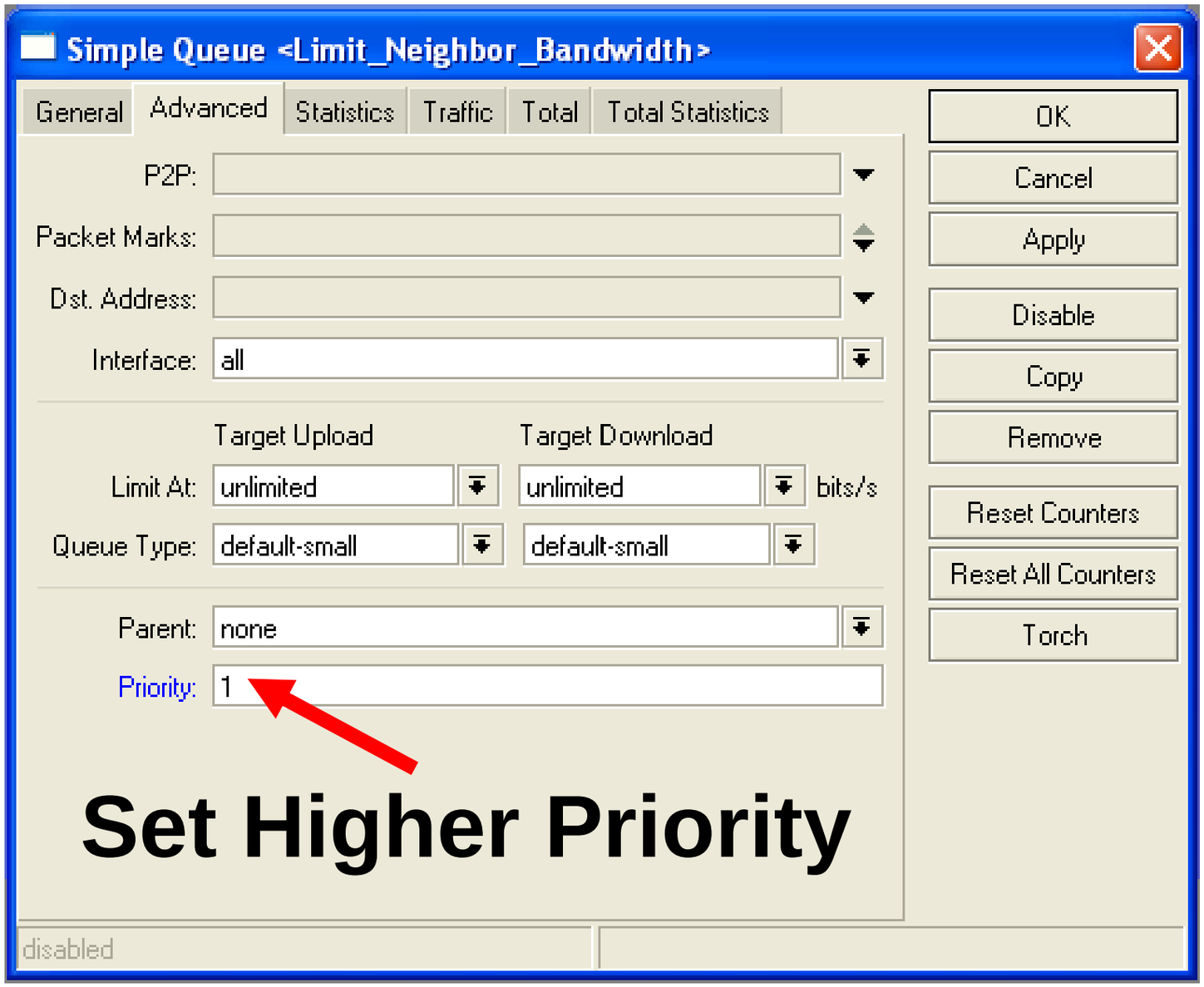
- Server should be enabled
- It is advised to use enabled **Authenticate**



LAB

Traffic Priority

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

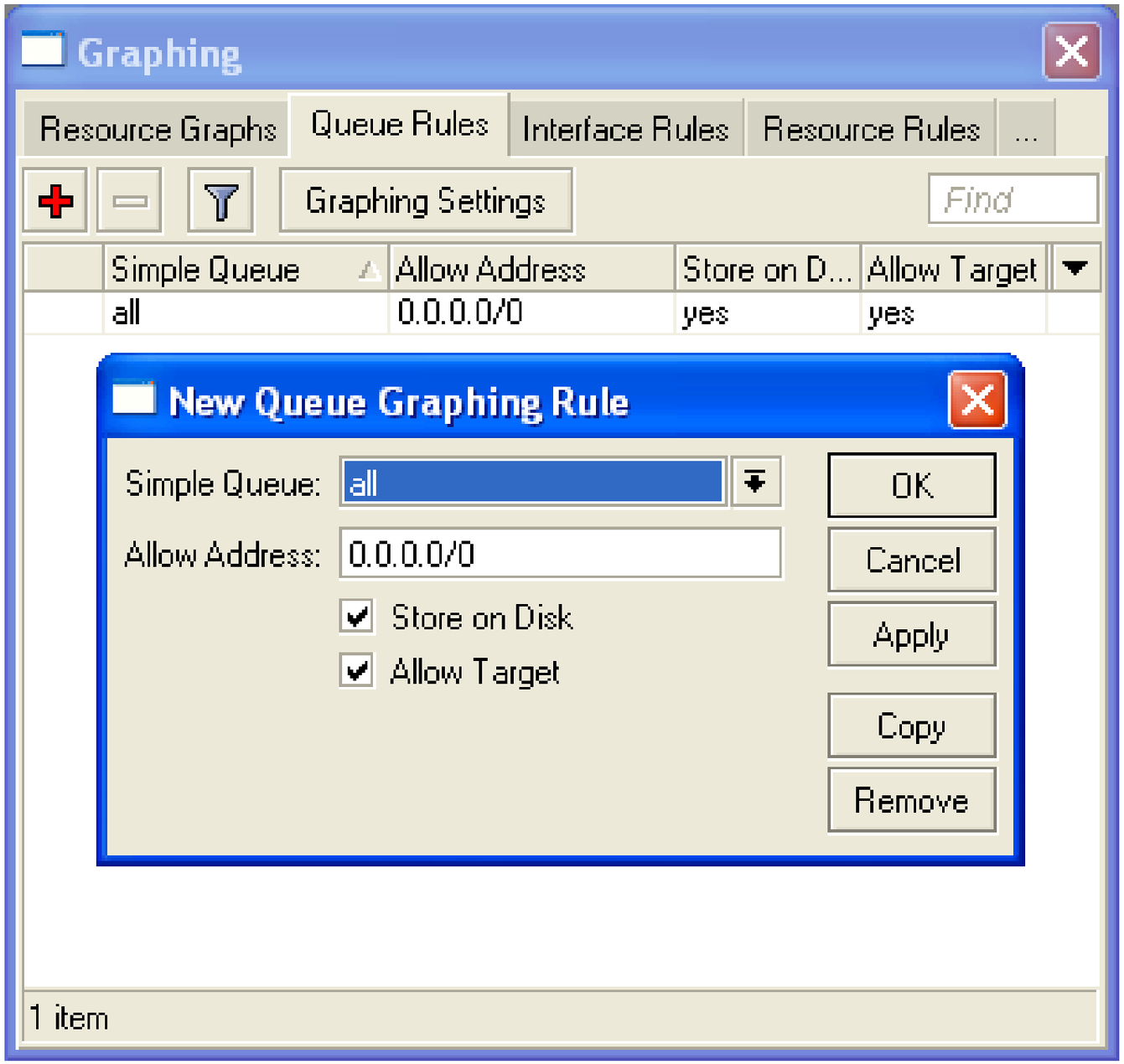


Simple Queue Monitor

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

Simple Queue Monitor

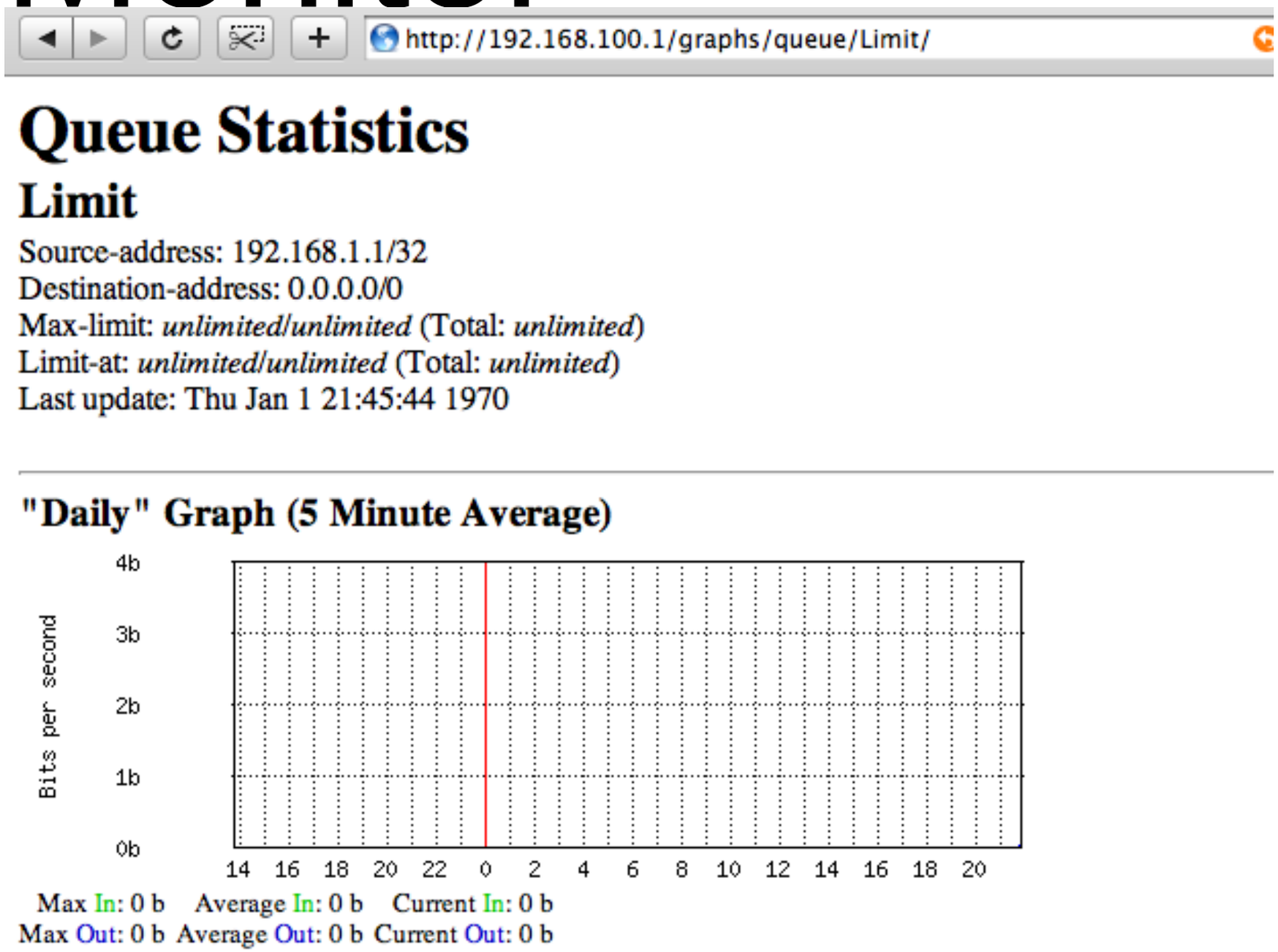
Let's enable graphing for Queues



Simple Queue Monitor

LAB

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

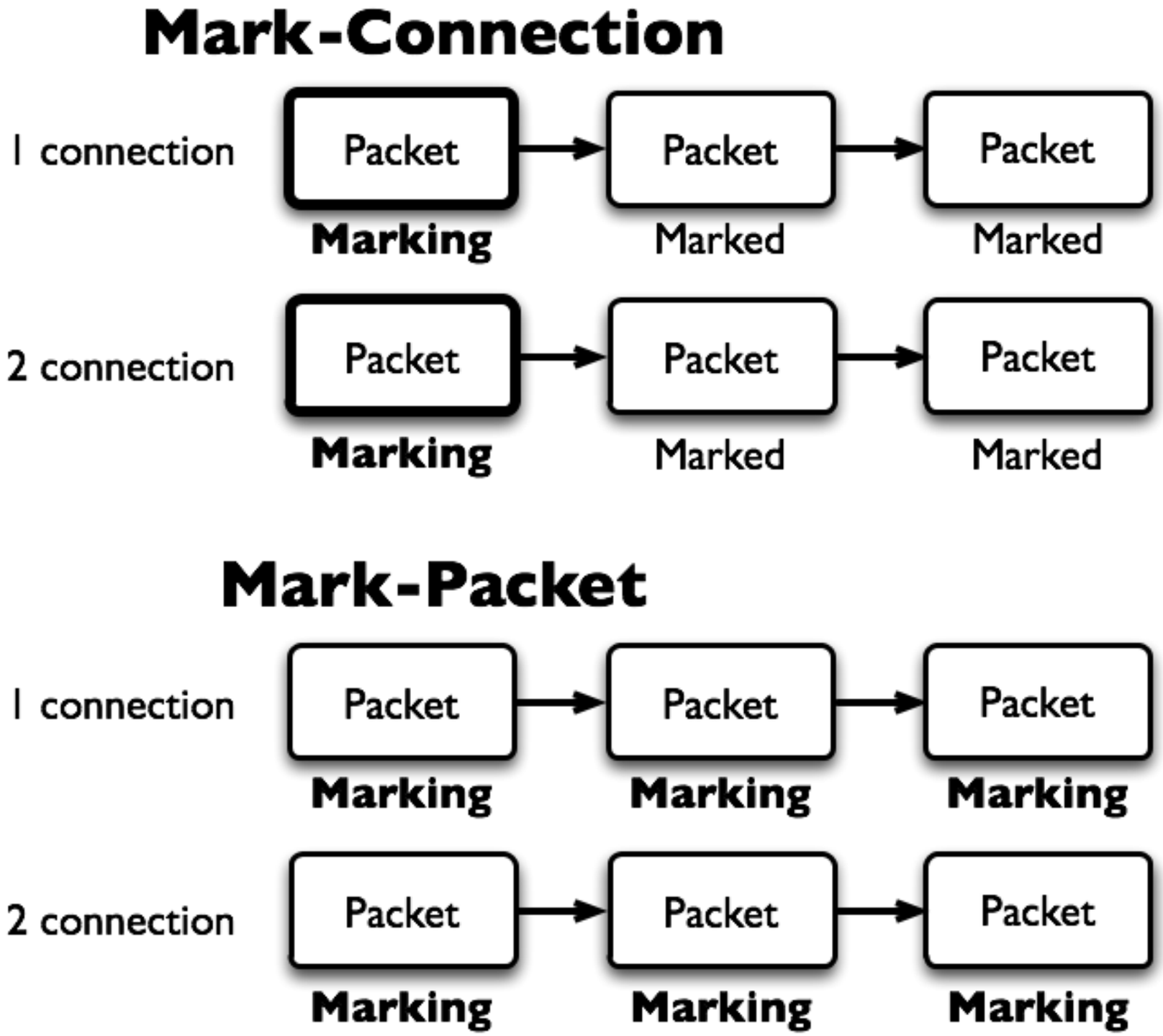


Advanced Queing

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

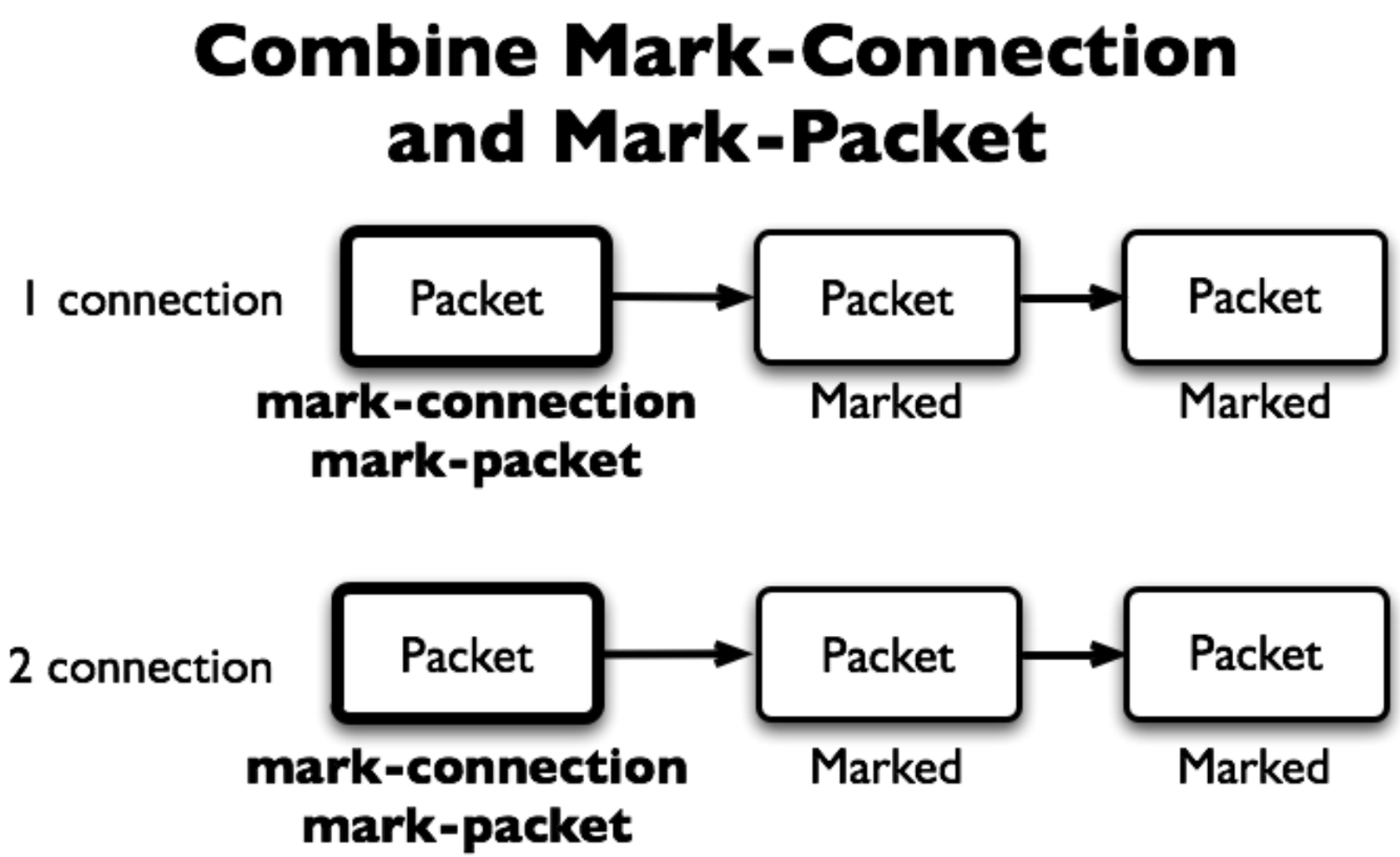


Mangle Actions

- **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



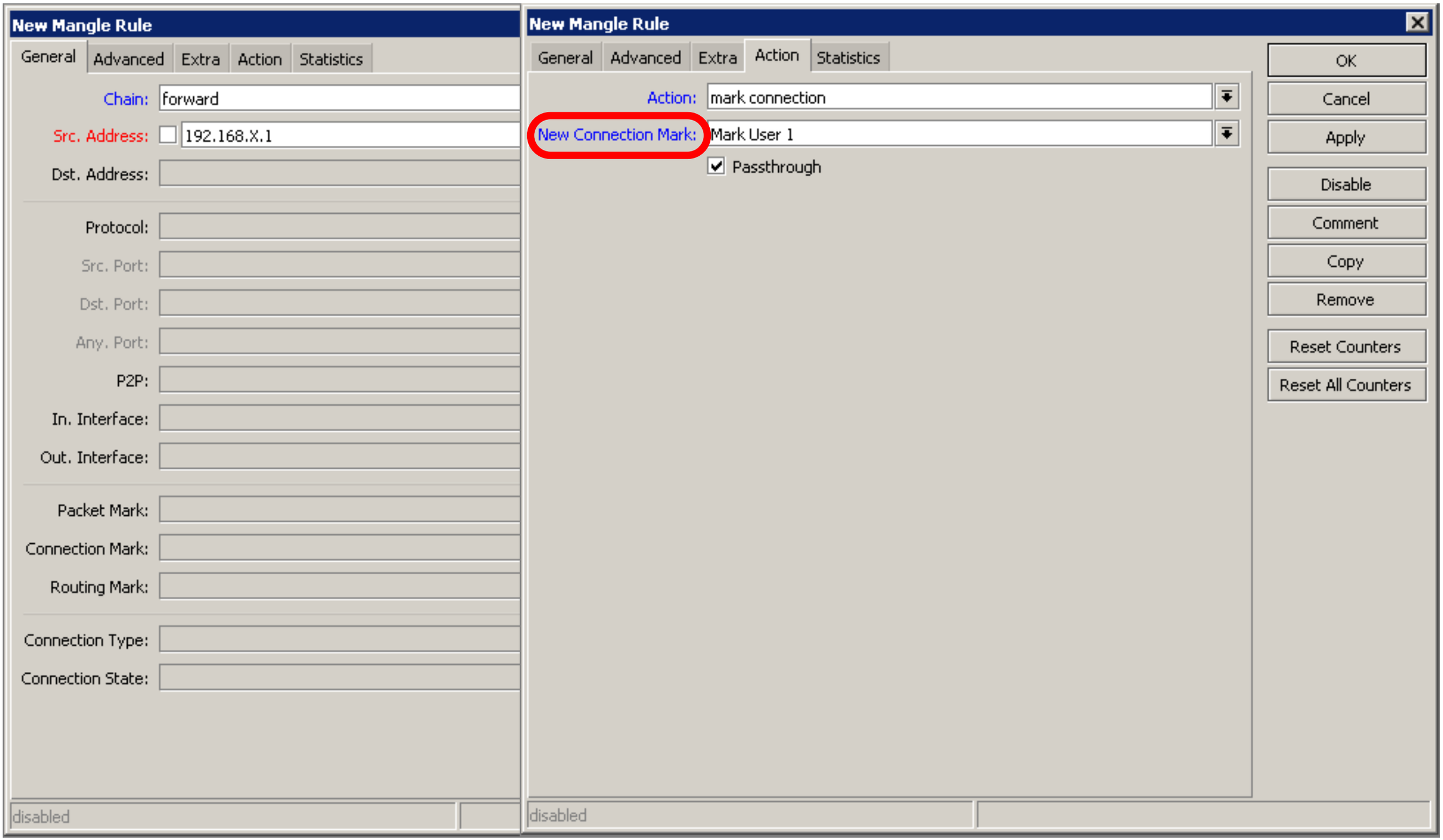
Optimal Mangle

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

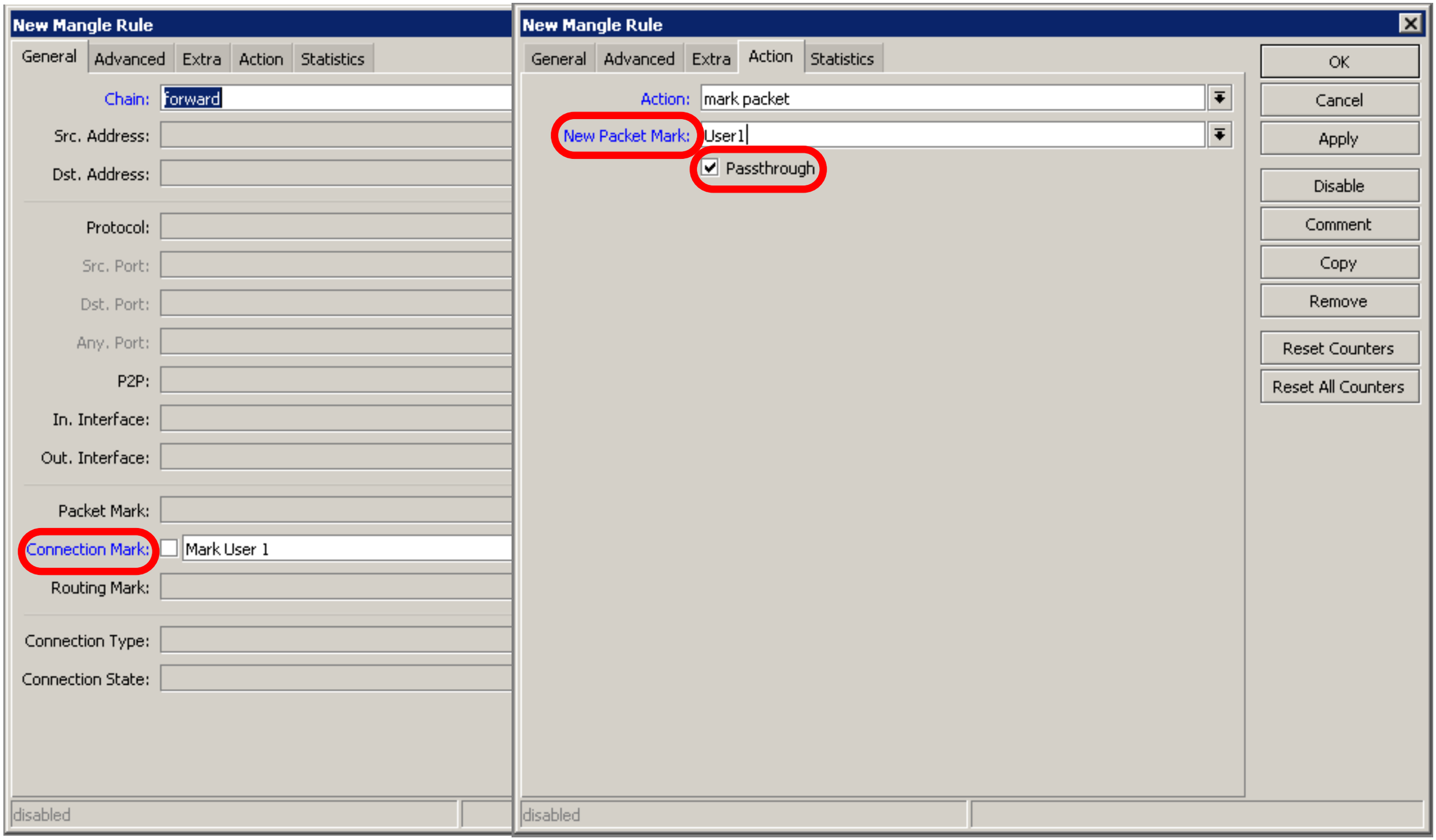
Mangle Example

- 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



Mark Packet


New Mangle Rule
General
Advanced
Extra
Action
Statistics
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:
disabled
New Mangle Rule
General
Advanced
Extra
Action
Statistics
Action: mark packet
New Packet Mark: User1
Passthrough
OK
Cancel
Apply
Disable
Comment
Copy
Remove
Reset Counters
Reset All Counters
disabled

Mangle Example

LAB

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

Advanced Queuing

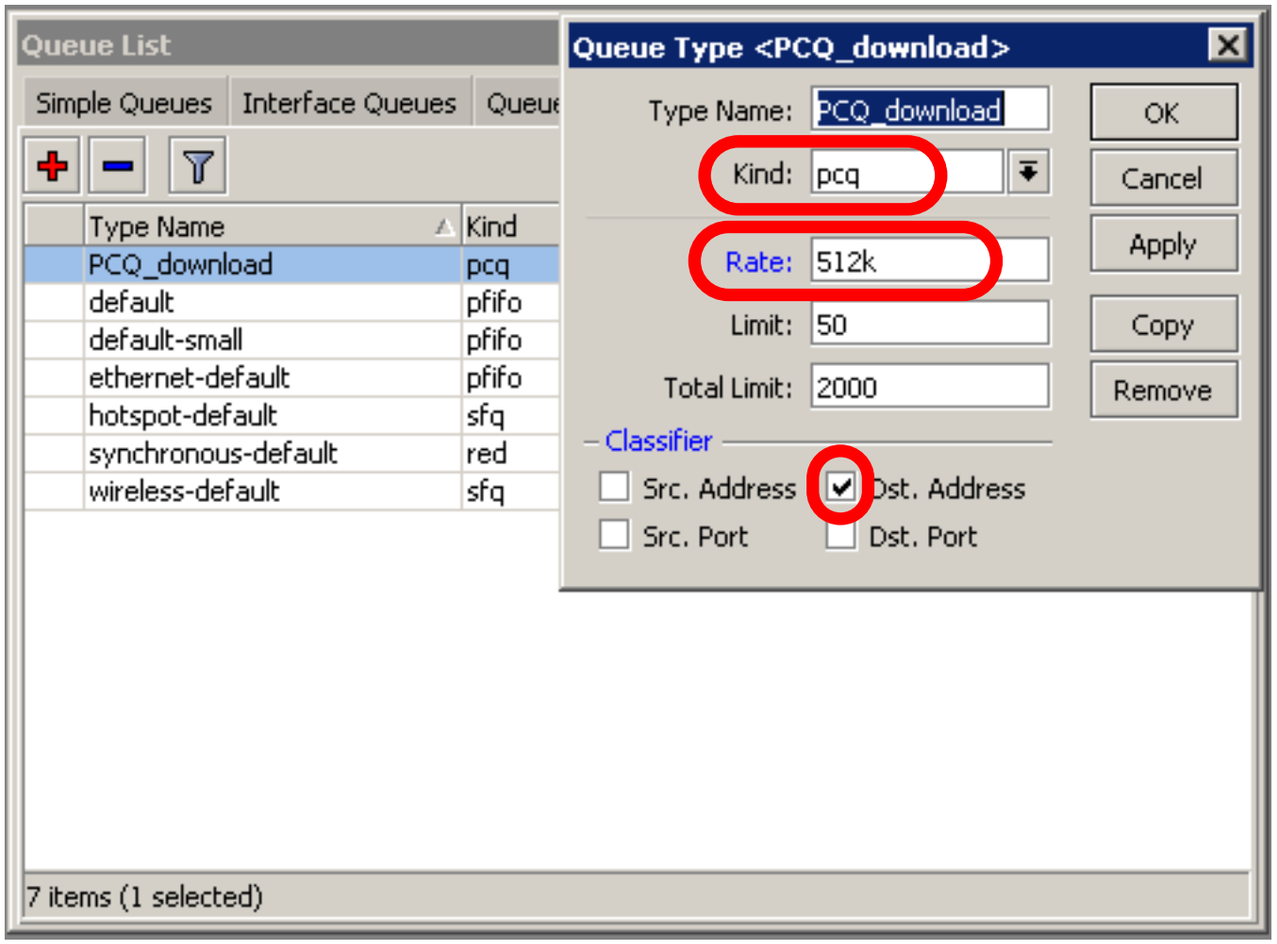
- Replace hundreds of queues with just few
- Set the same limit to any user
- Equalize available bandwidth between users

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)

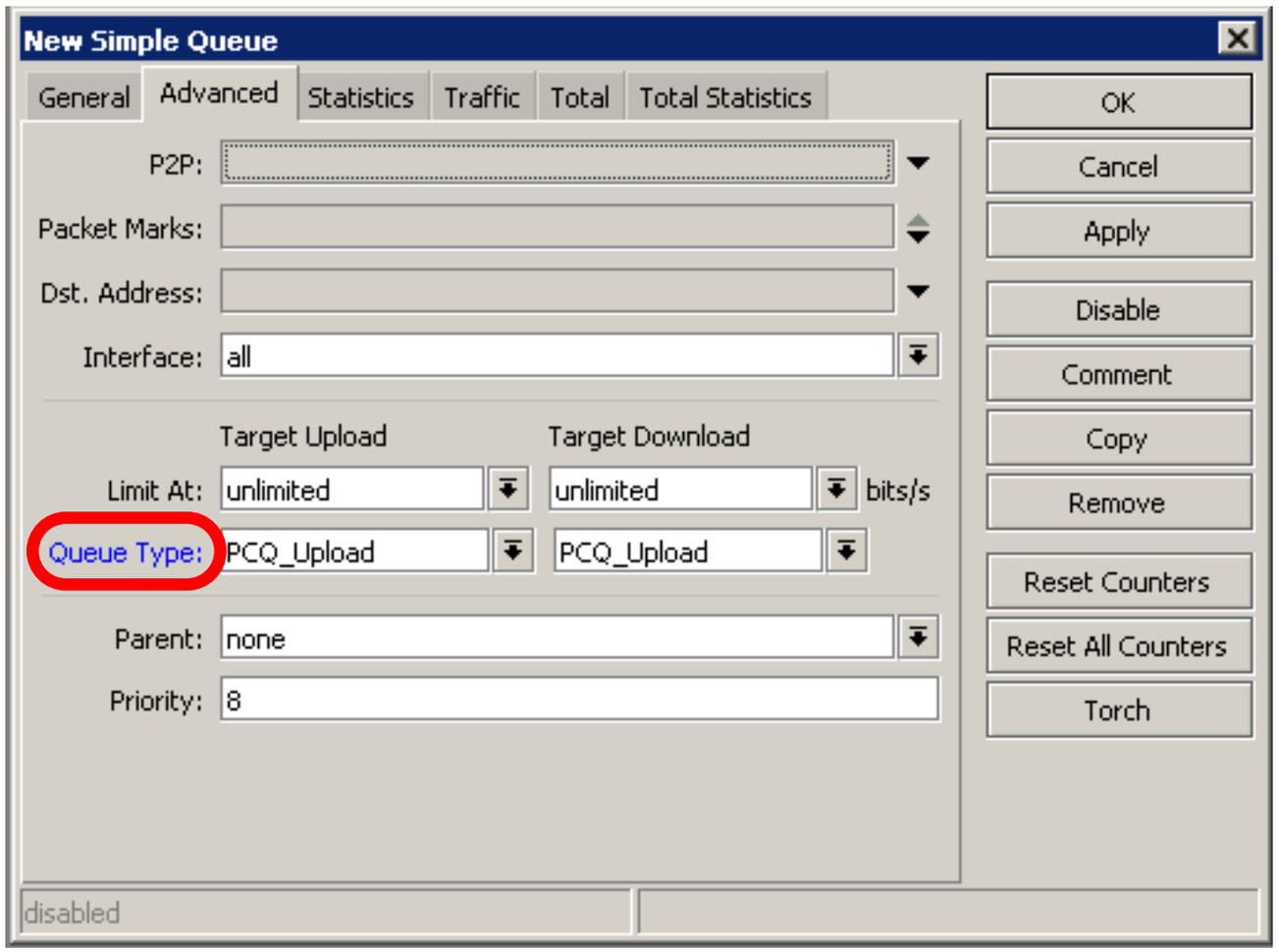
PCQ, one limit to all

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



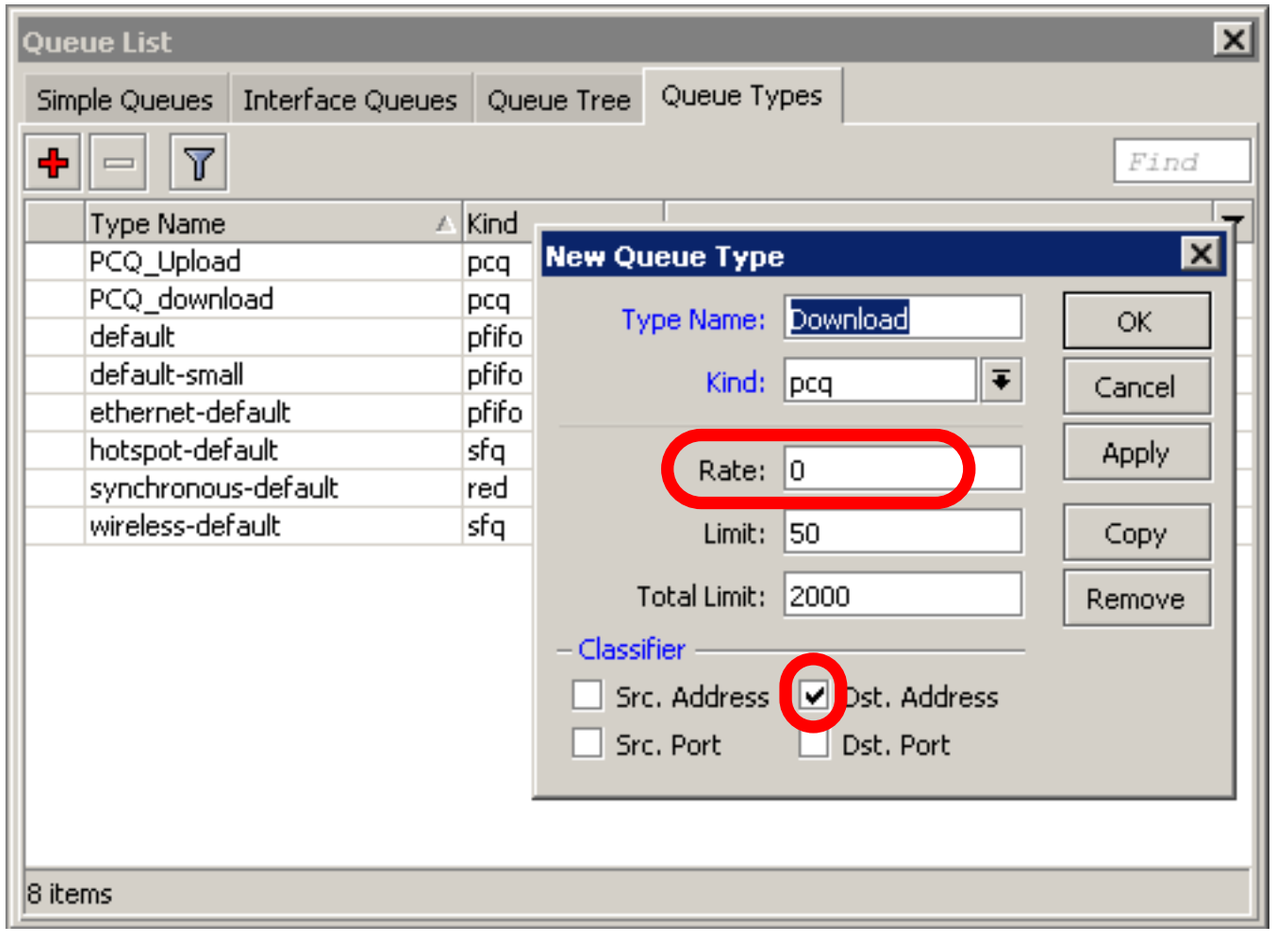
One limit to all

- Multiple queue rules are changed by one



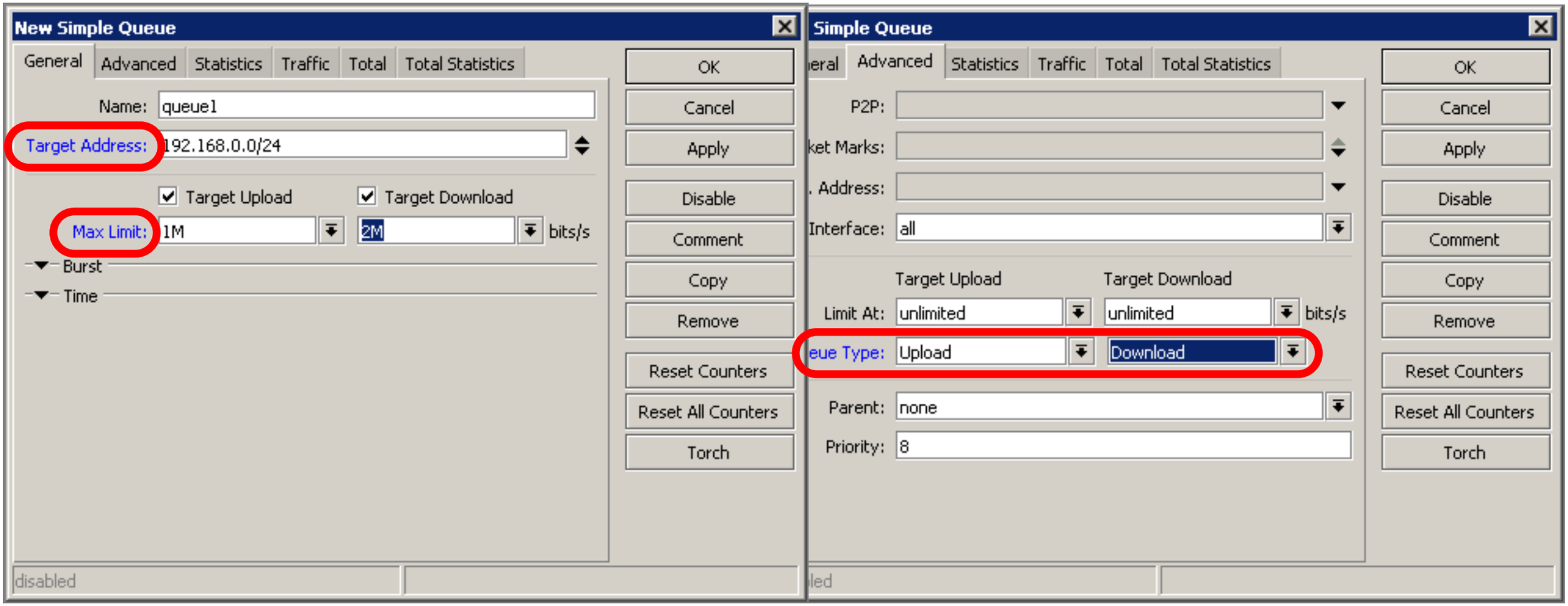
PCQ, equalize bandwidth

- Equally share bandwidth between customers



Equalize bandwidth

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



LAB

PCQ Lab

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

Summary

Wireless

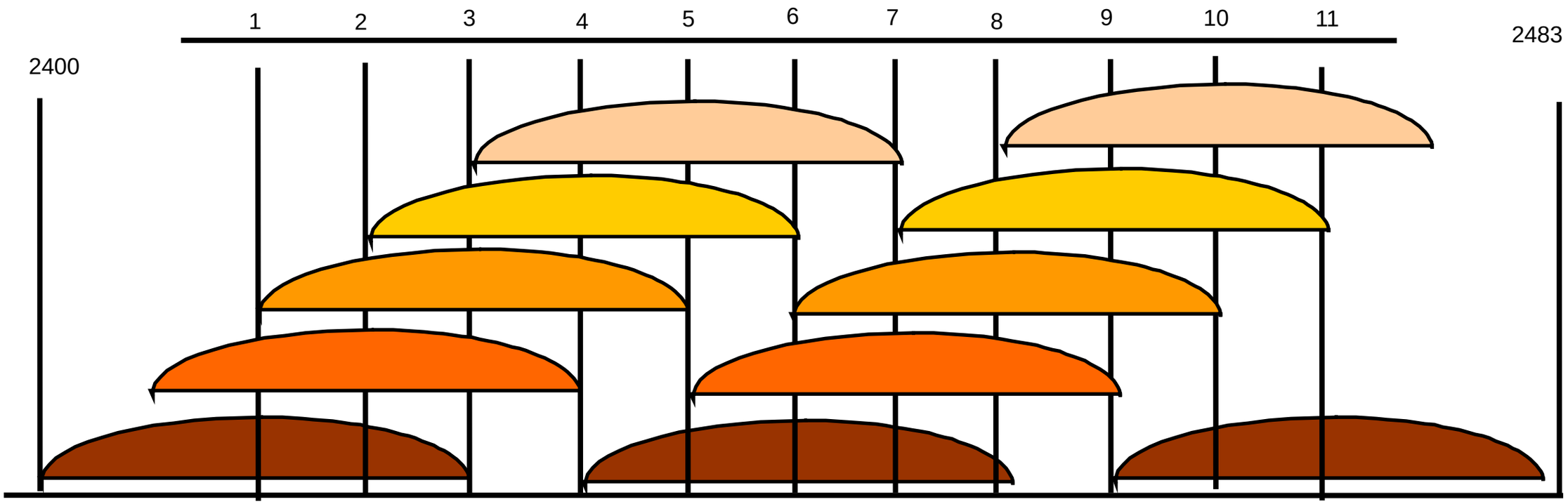
What is Wireless

- 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

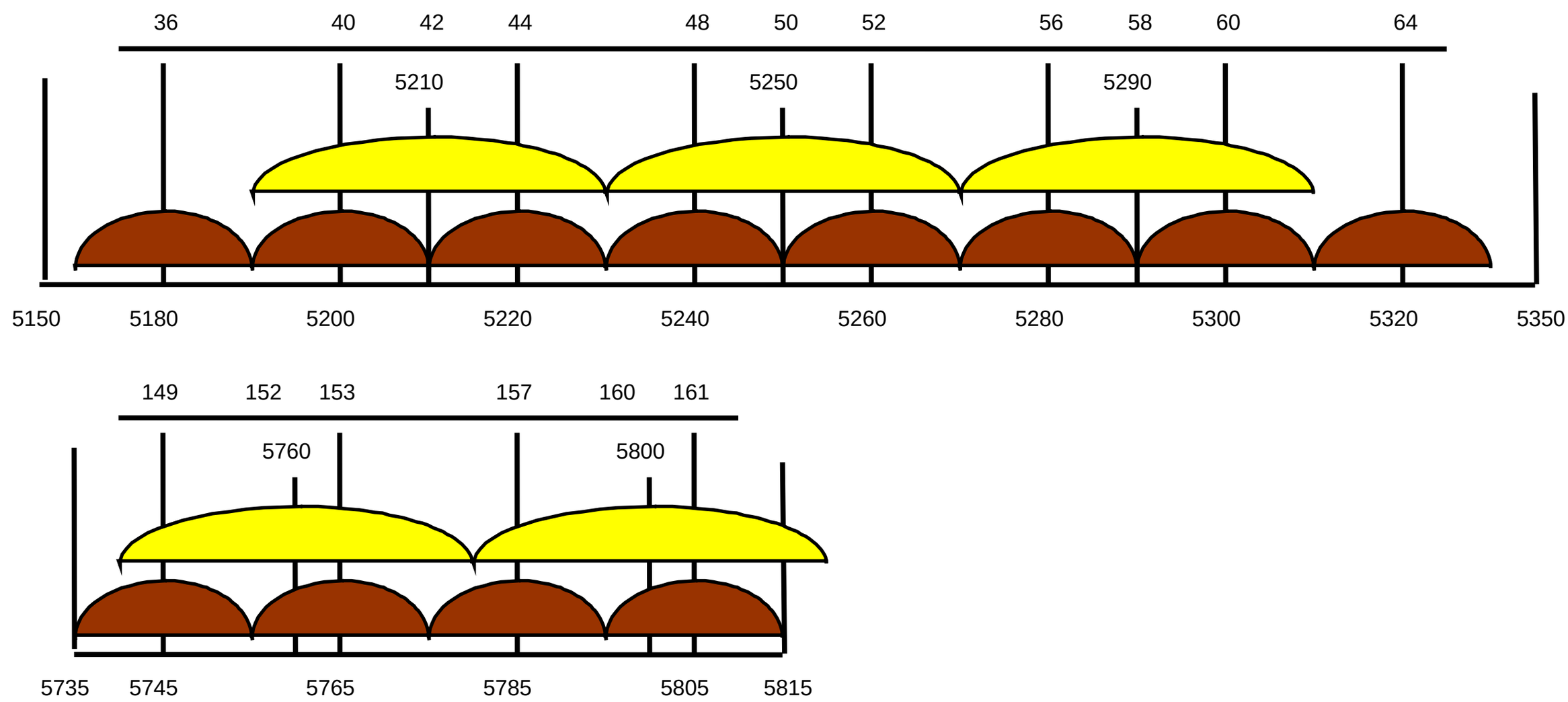
- IEEE 802.11b - 2.4GHz frequencies, 11Mbps
- IEEE 802.11g - 2.4GHz frequencies, 54Mbps
- IEEE 802.11a - 5GHz frequencies, 54Mbps
- IEEE 802.11n - draft, 2.4GHz - 5GHz

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

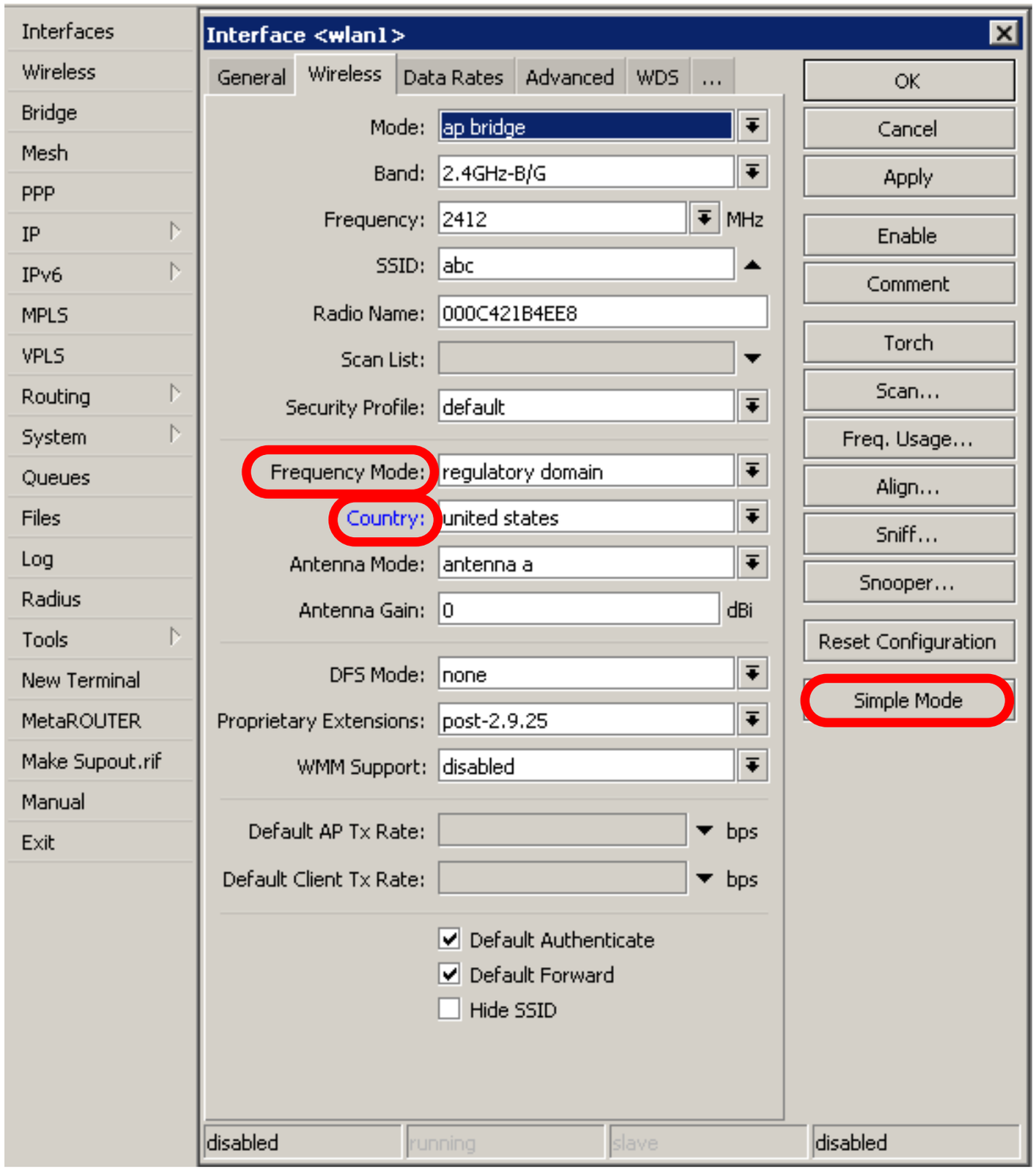
All 5GHz (802.11a) and 2.4GHz (802.11b/g), including small channels

Supported Frequencies

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

Apply Country Regulations

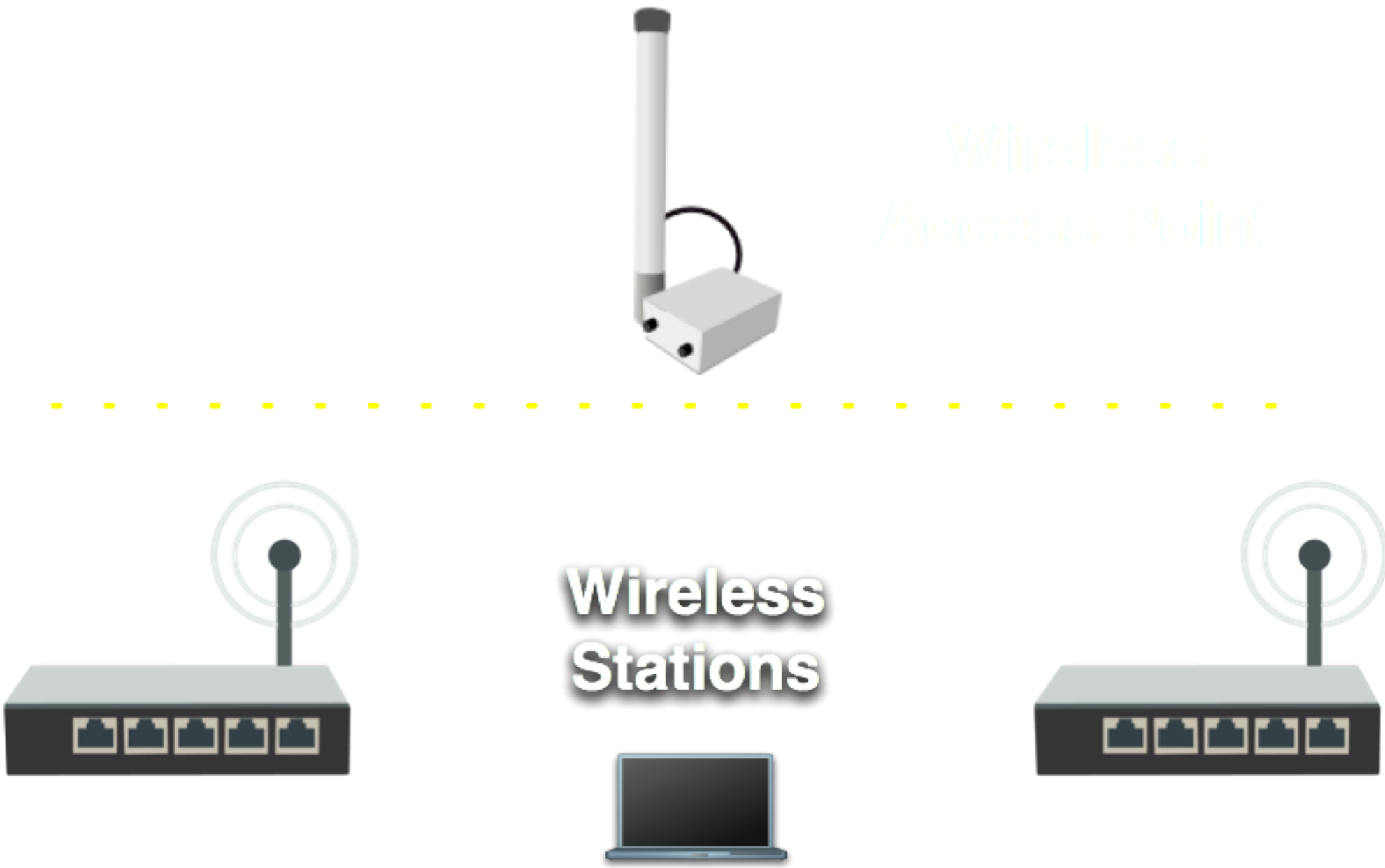
Set wireless interface to apply your country regulations



RADIO Name

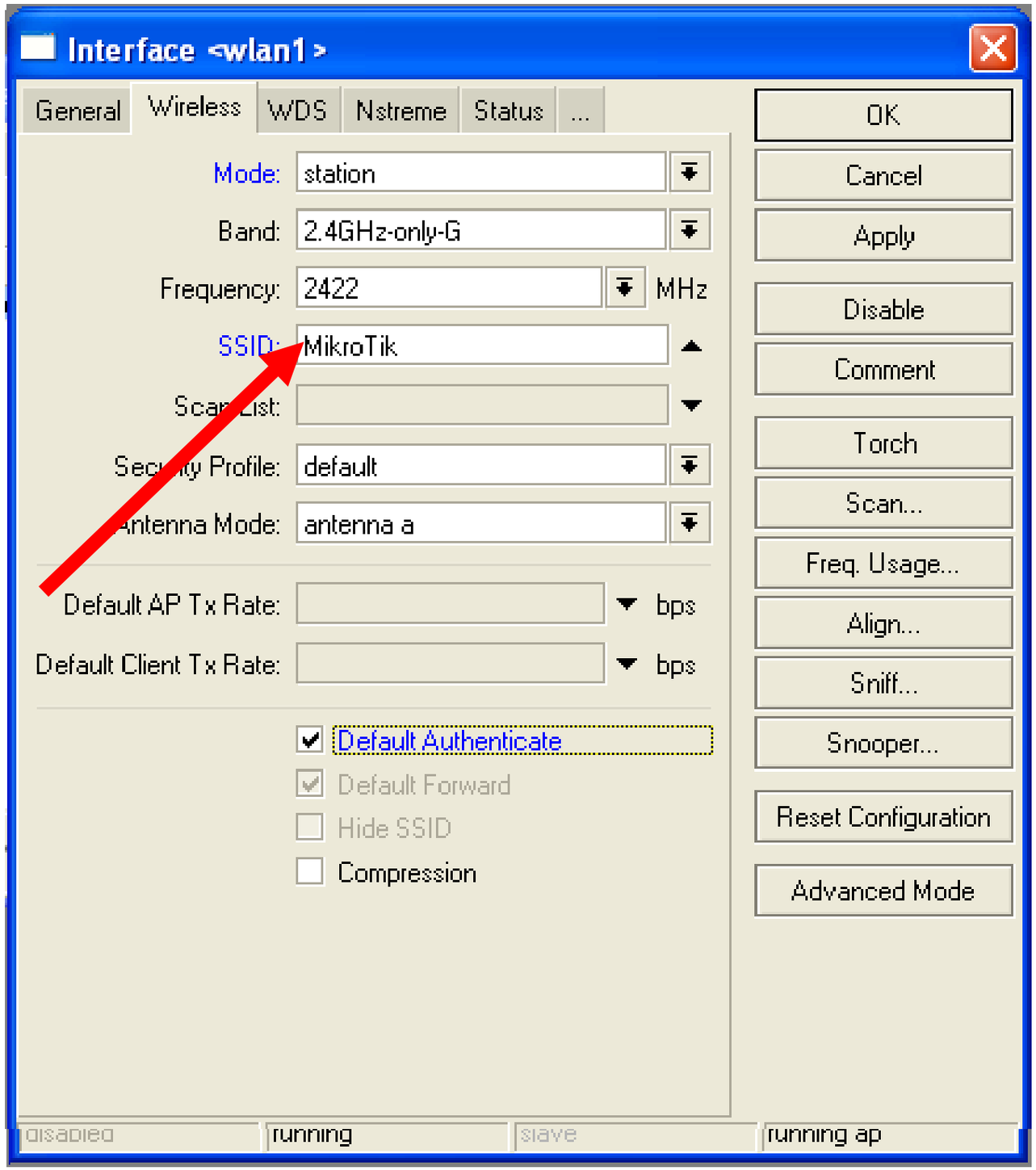
- We will use RADIO Name for the same purposes as router identity
- Set RADIO Name as **Number+Your Name**

Wireless Network



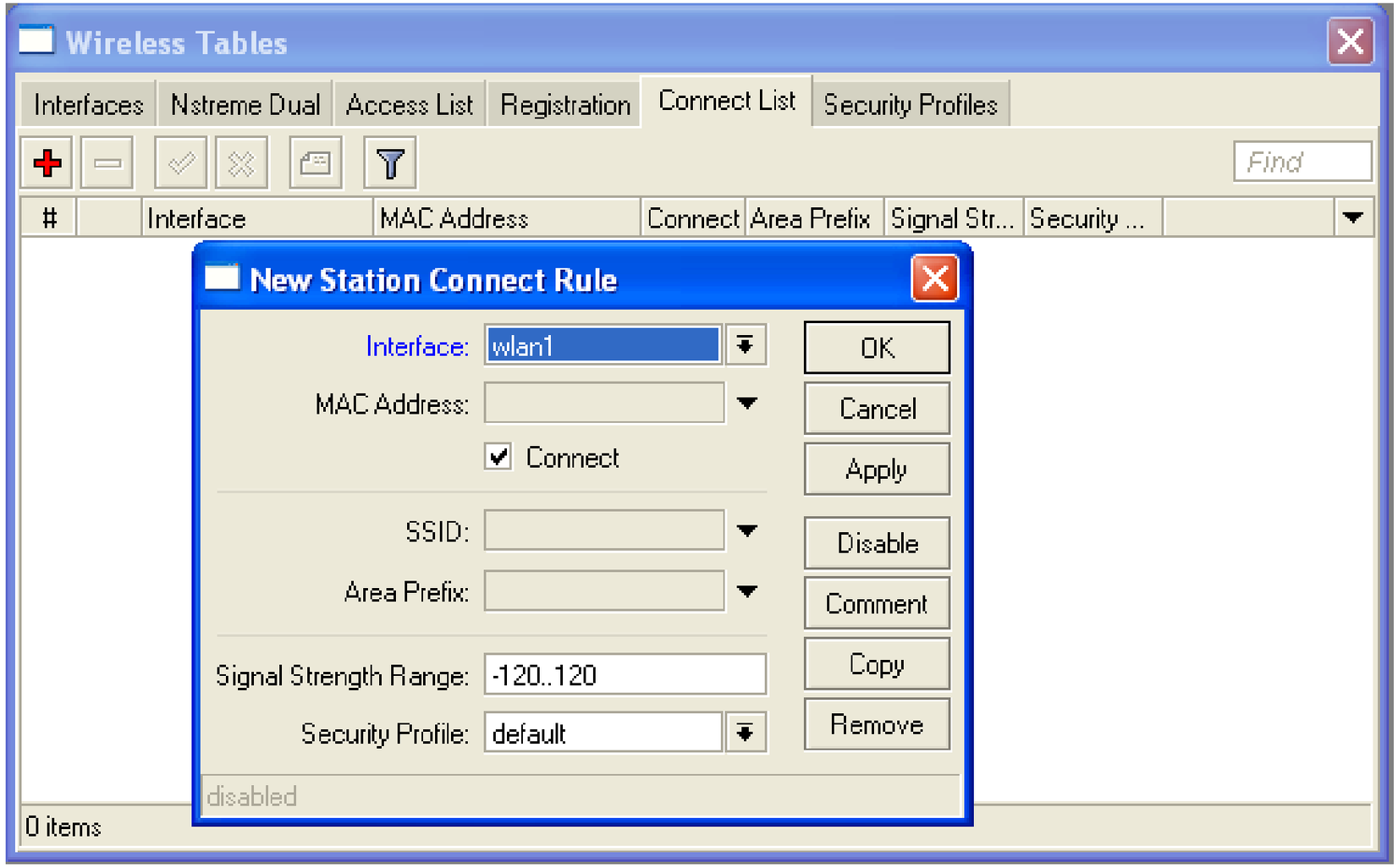
Station Configuration

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



Connect List

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



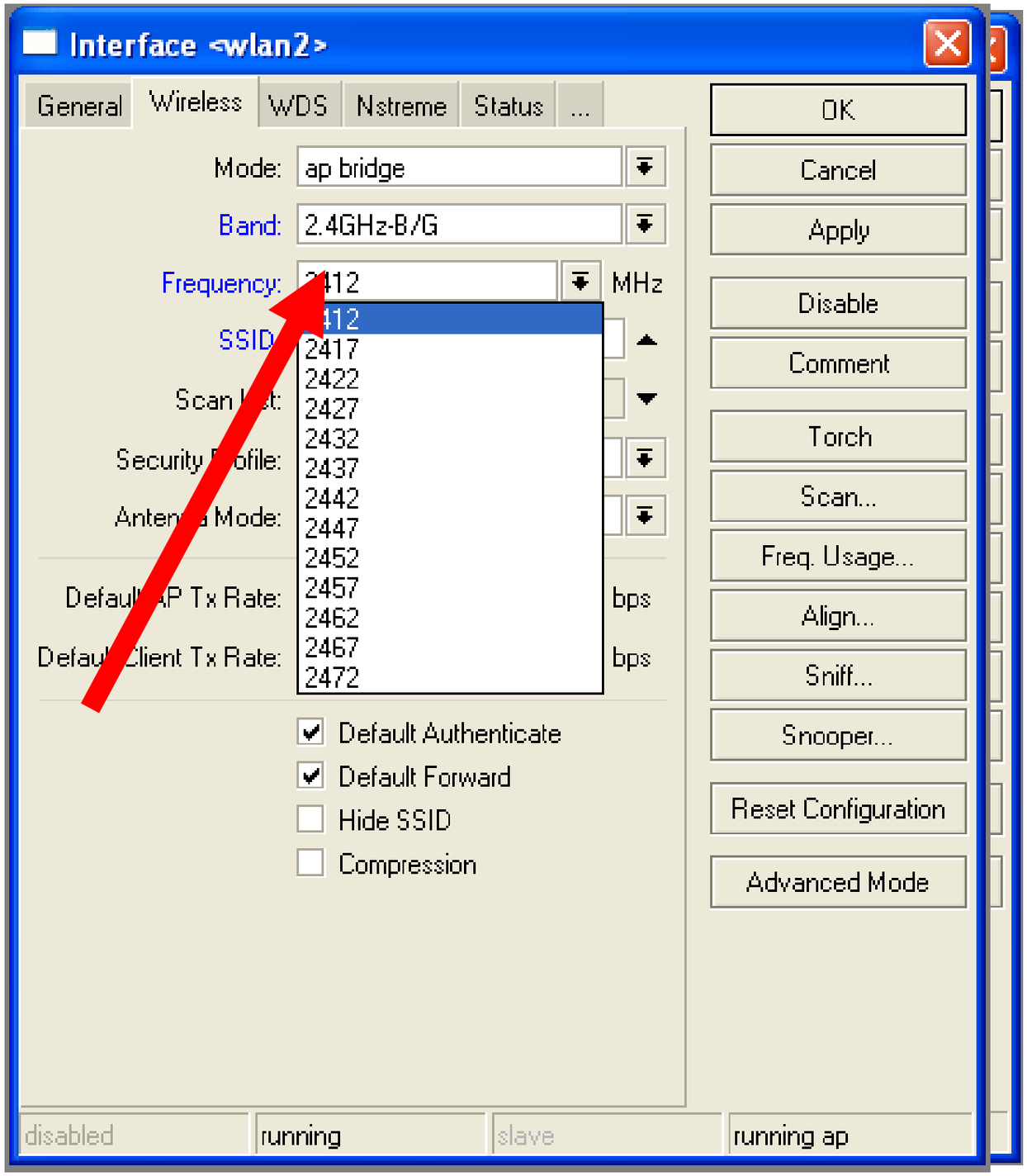
Connect List Lab

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

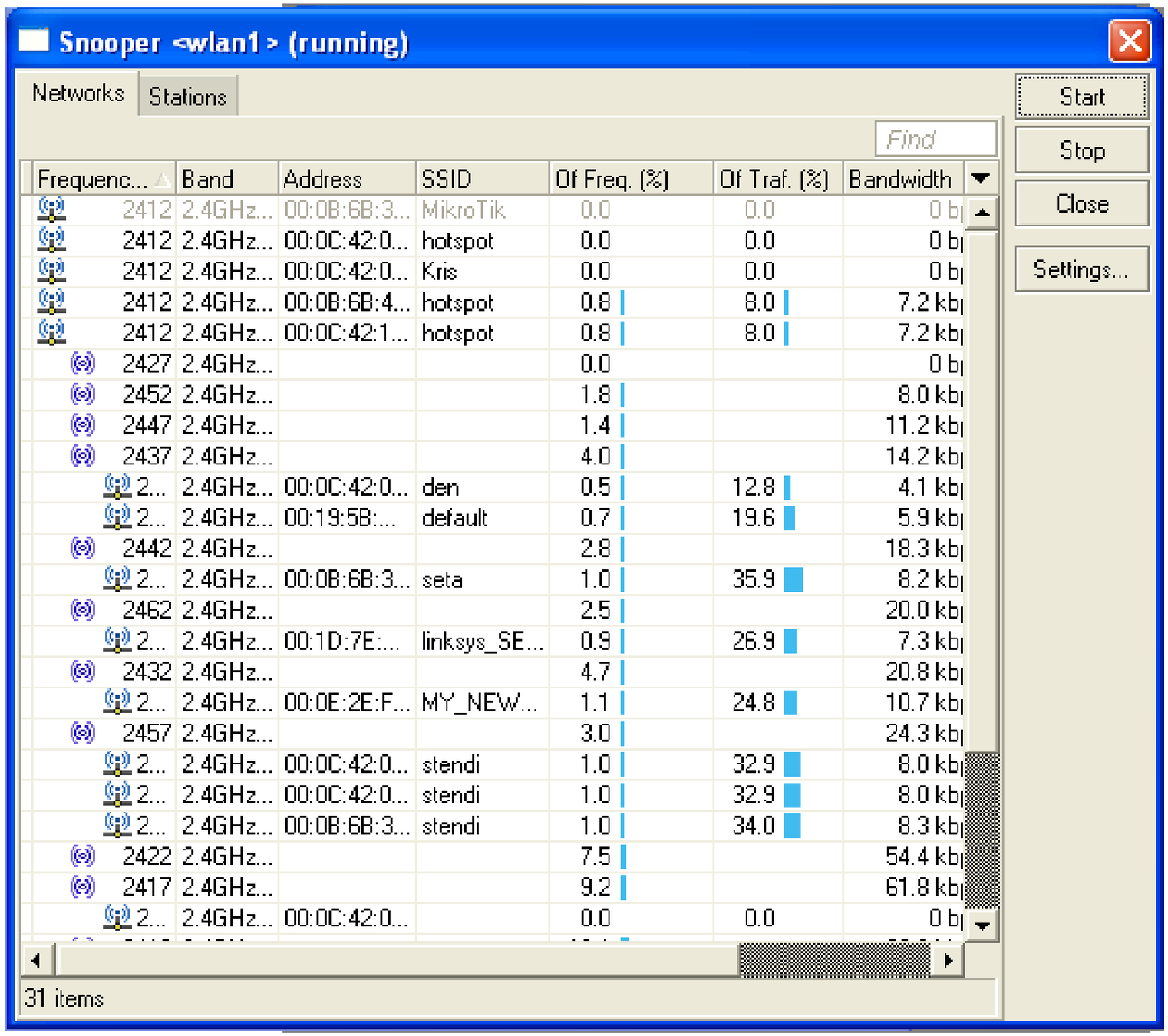
Access Point Configuration

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



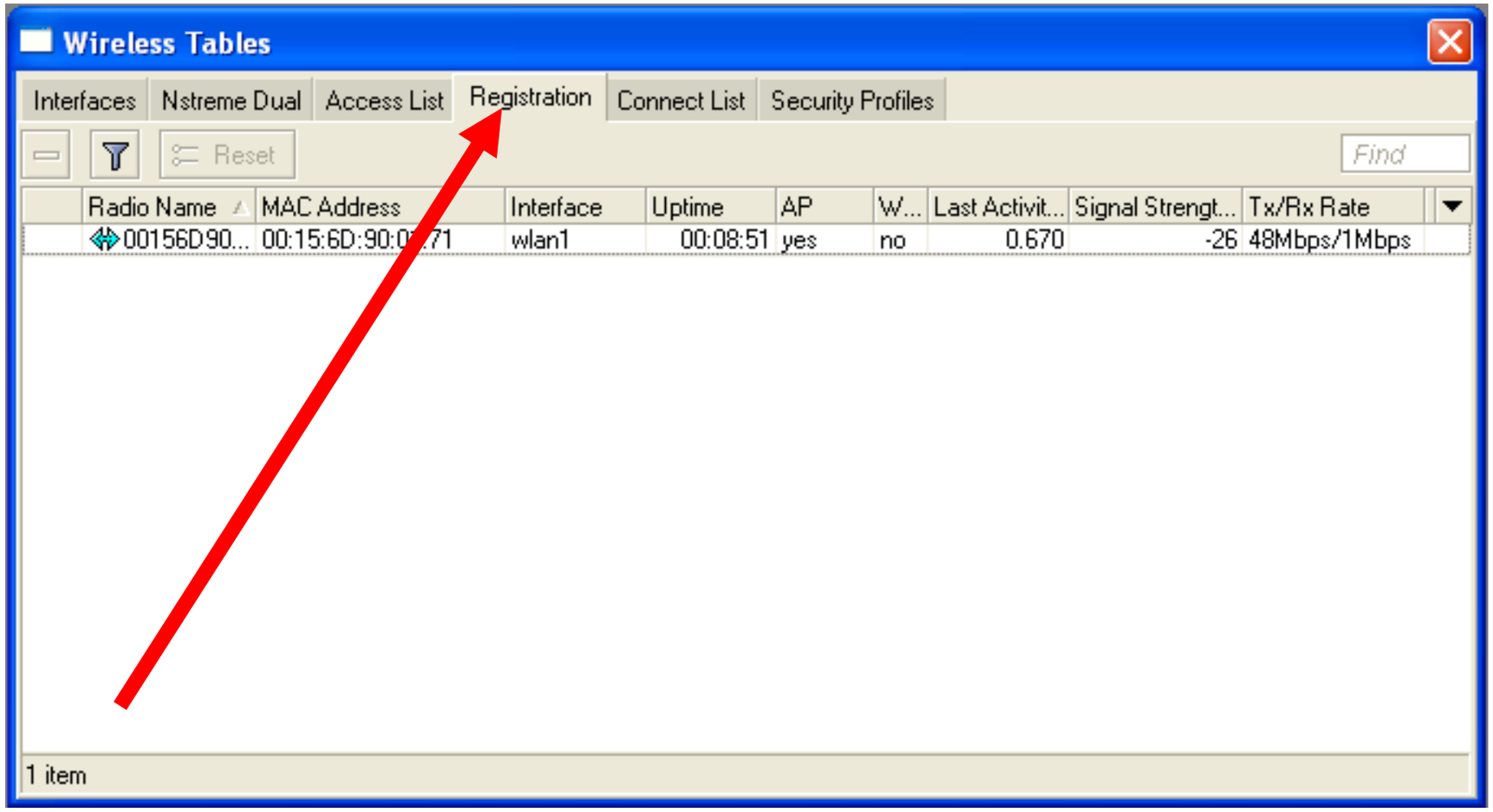
Snooper wireless monitor

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



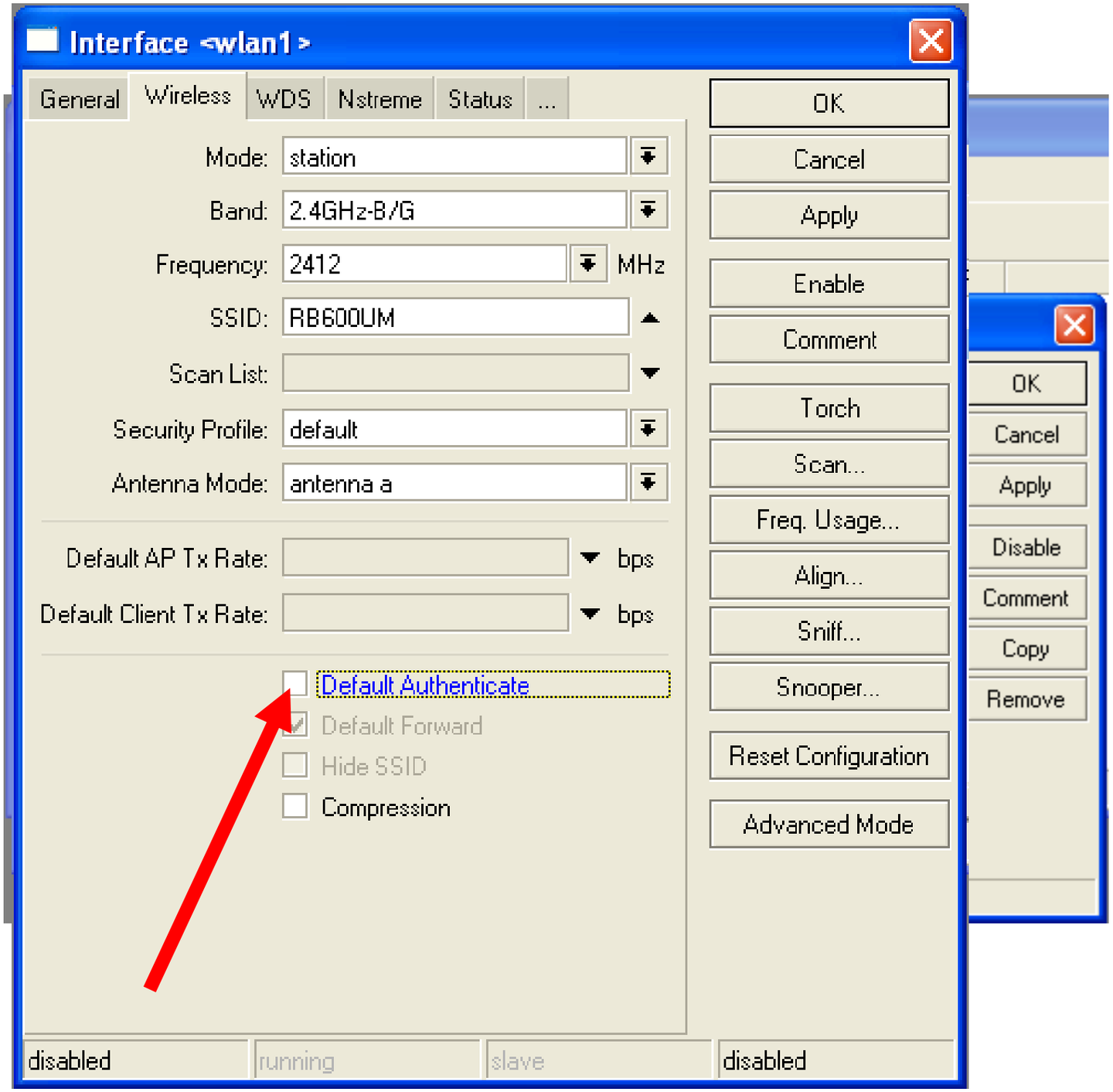
Registration Table

- View all connected wireless interfaces



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

LAB

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

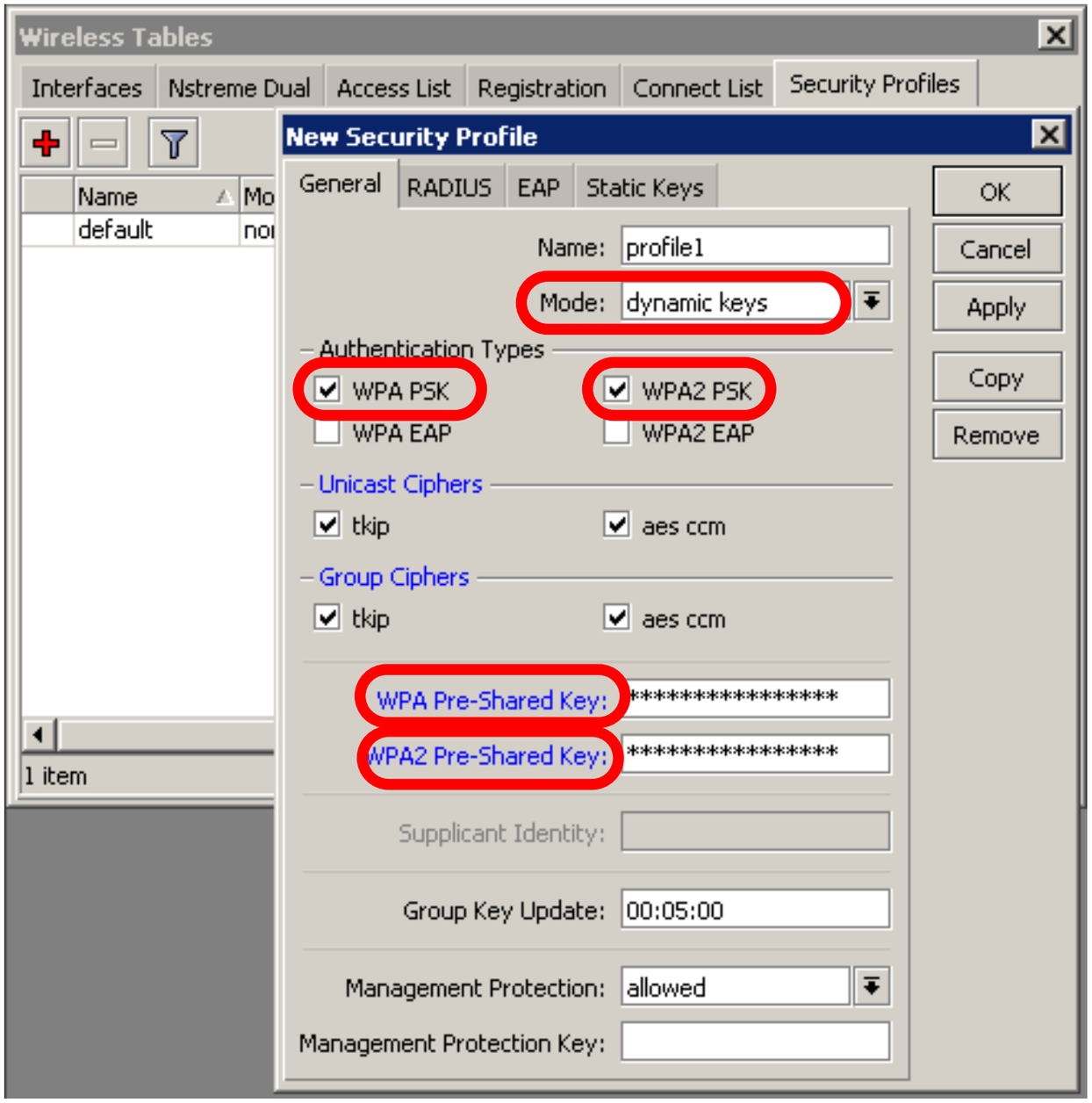
Security

- 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

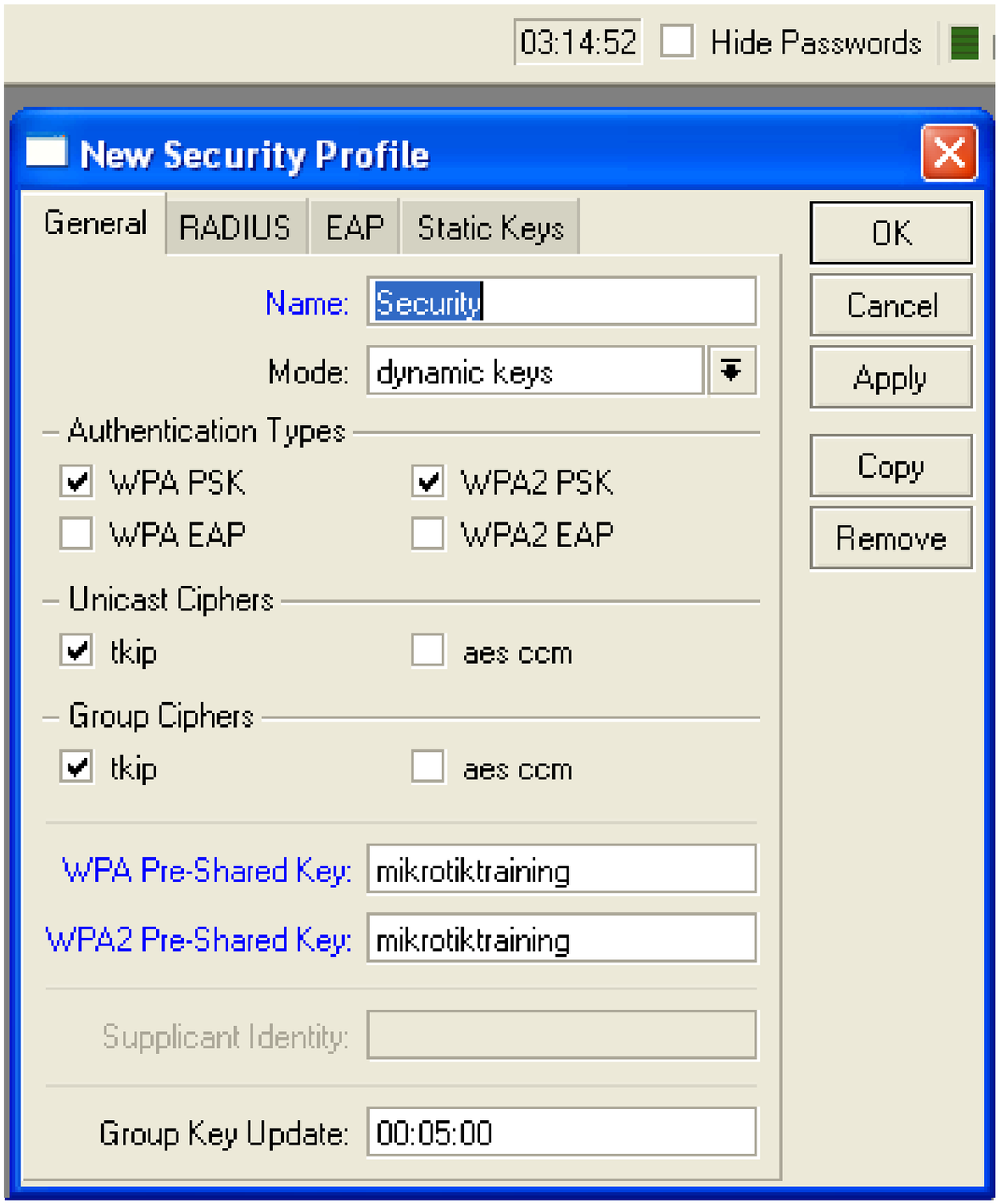
LAB

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



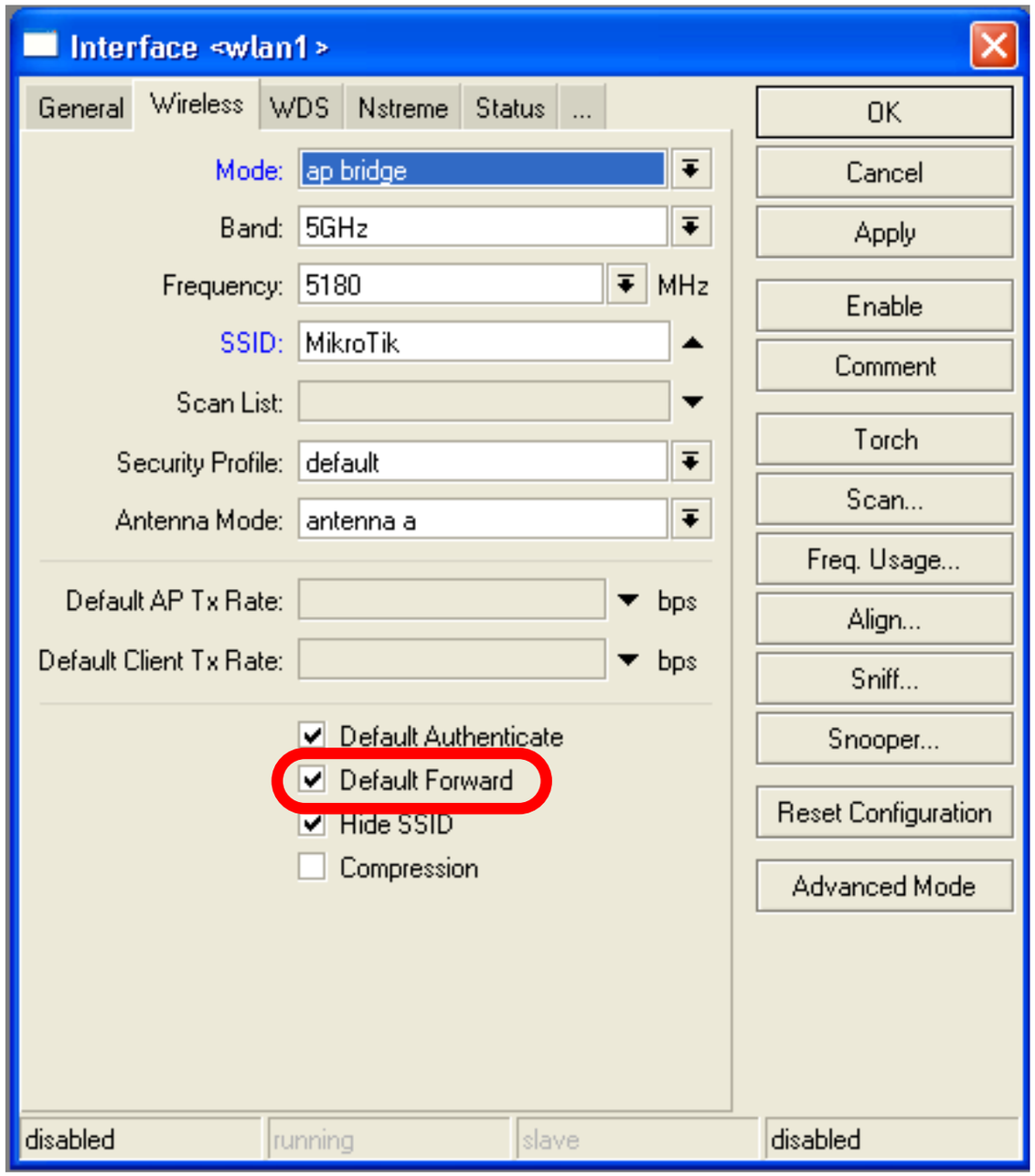
Configuration Tip

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



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

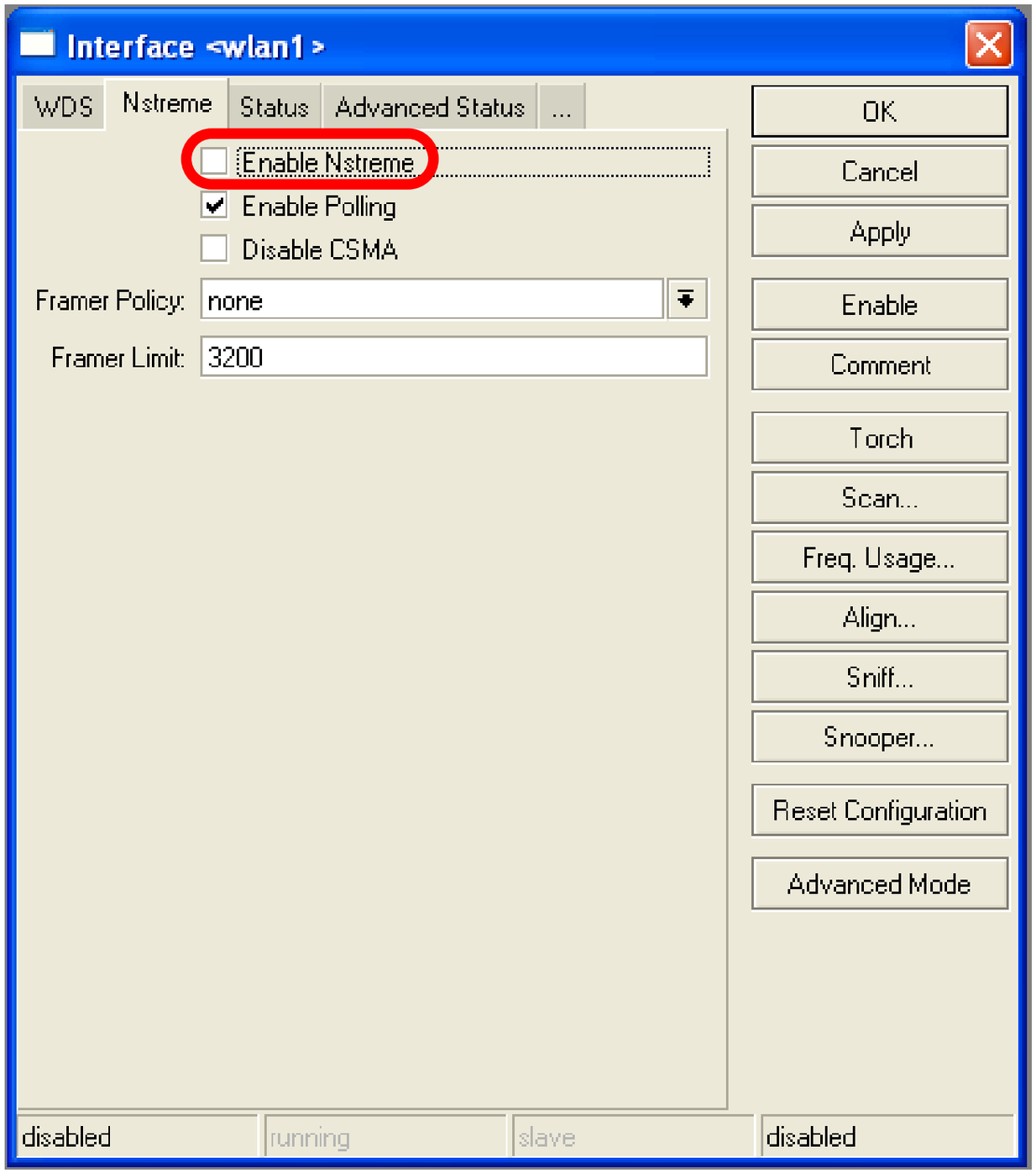
Nstreme

- 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

LAB

Nstreme Lab

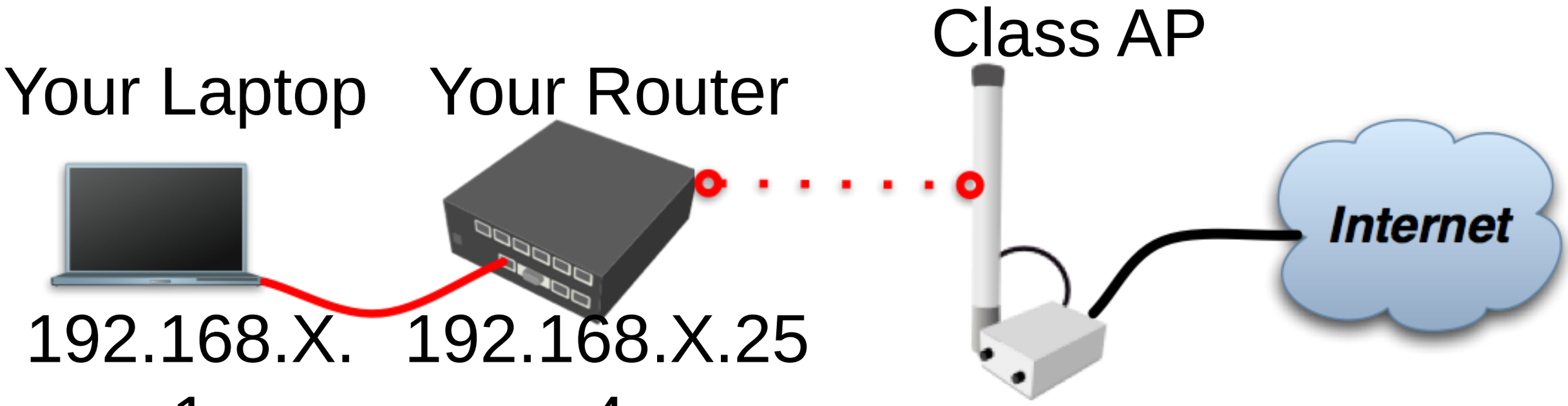
- Enable Nstreme on your router
- Check the connection status
- **Nstreme** should be enabled on **both** routers



Summary

Bridging

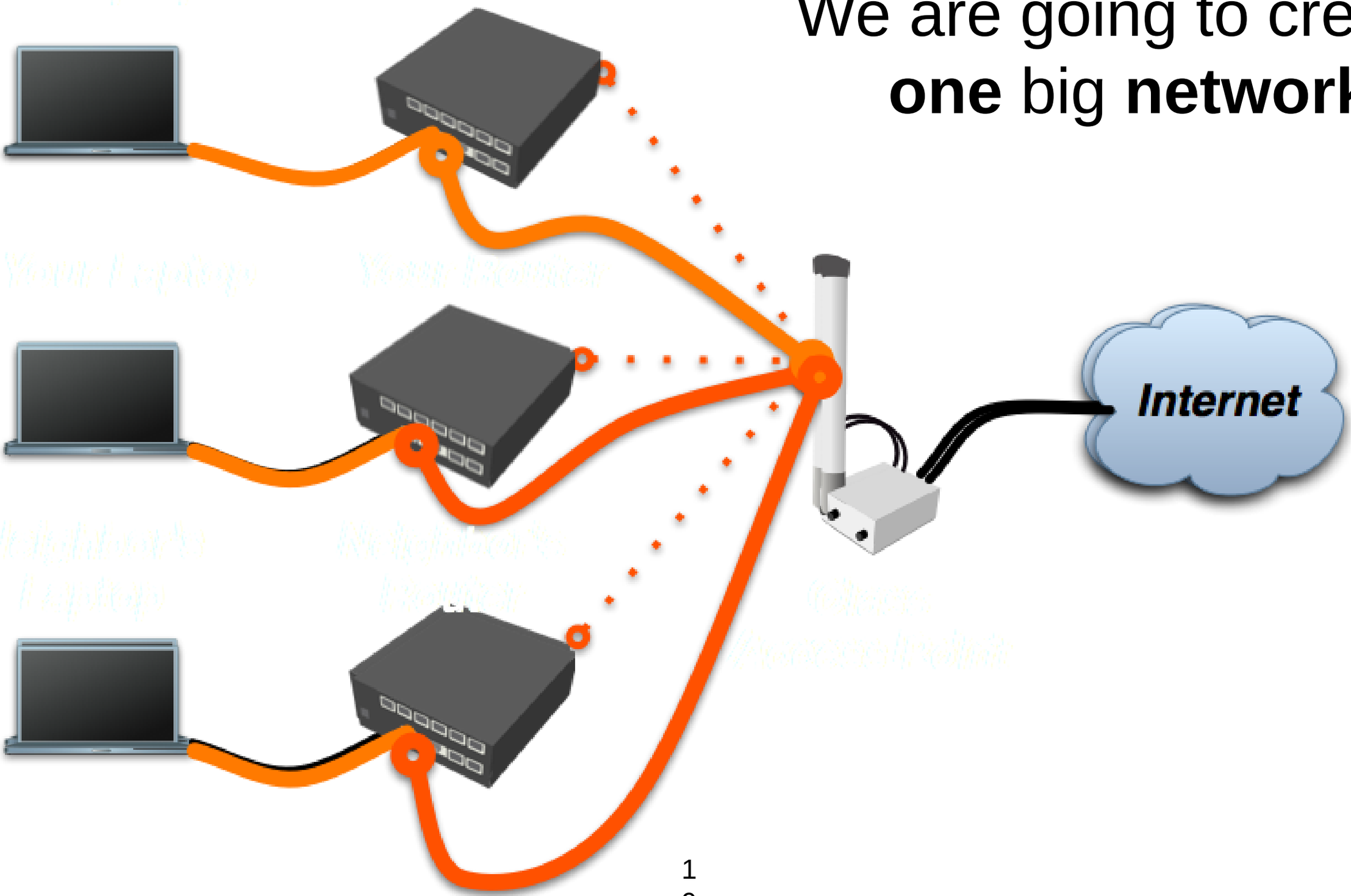
Bridge Wireless Network



Let’s get back to our configuration

Bridge Wireless Network

We are going to create
one big **network**



Bridge

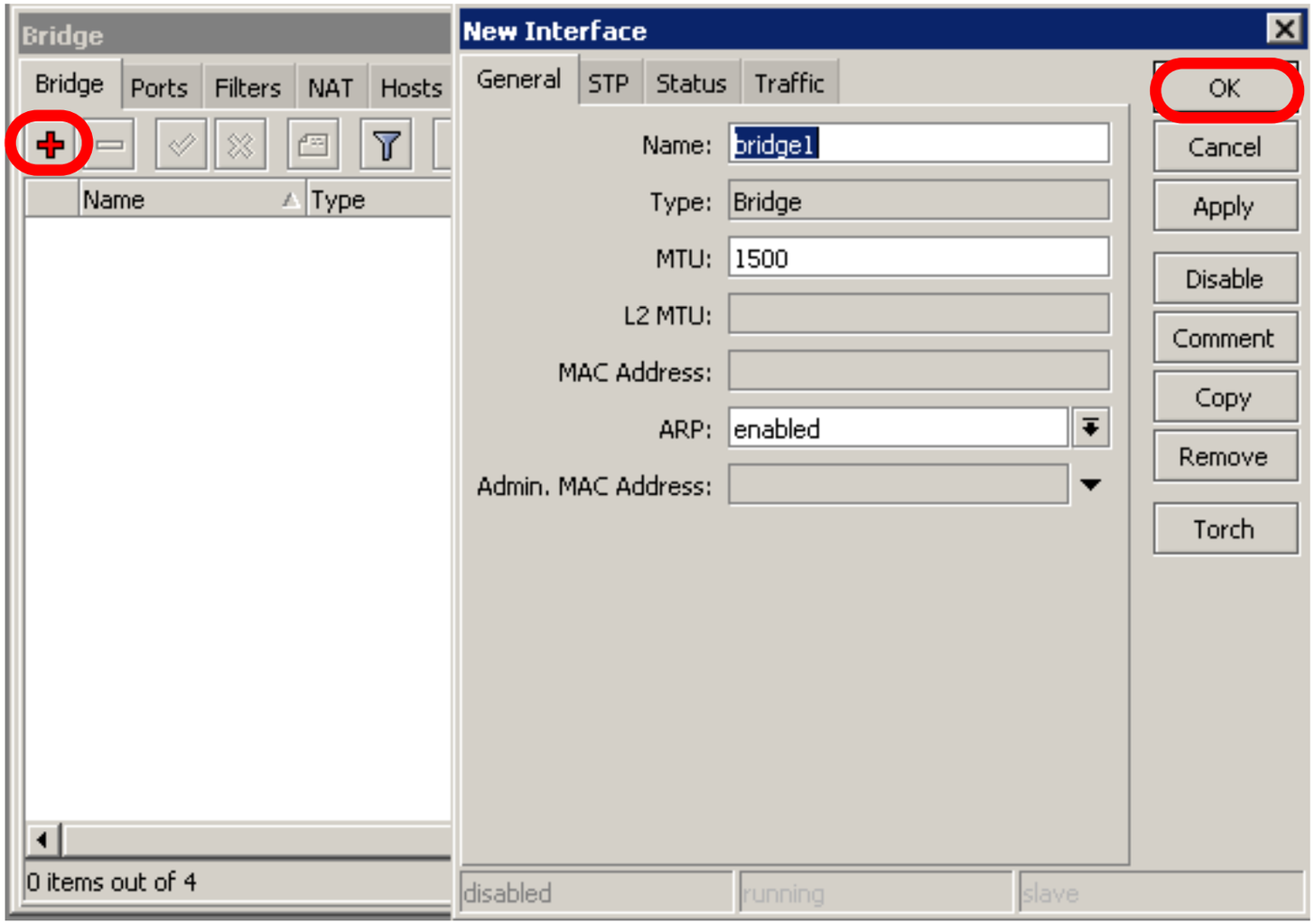
- We are going to bridge local Ethernet interface with Internet wireless interface
- Bridge unites different physical interfaces into one logical interface
- All your laptops will be in the same network

Bridge

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

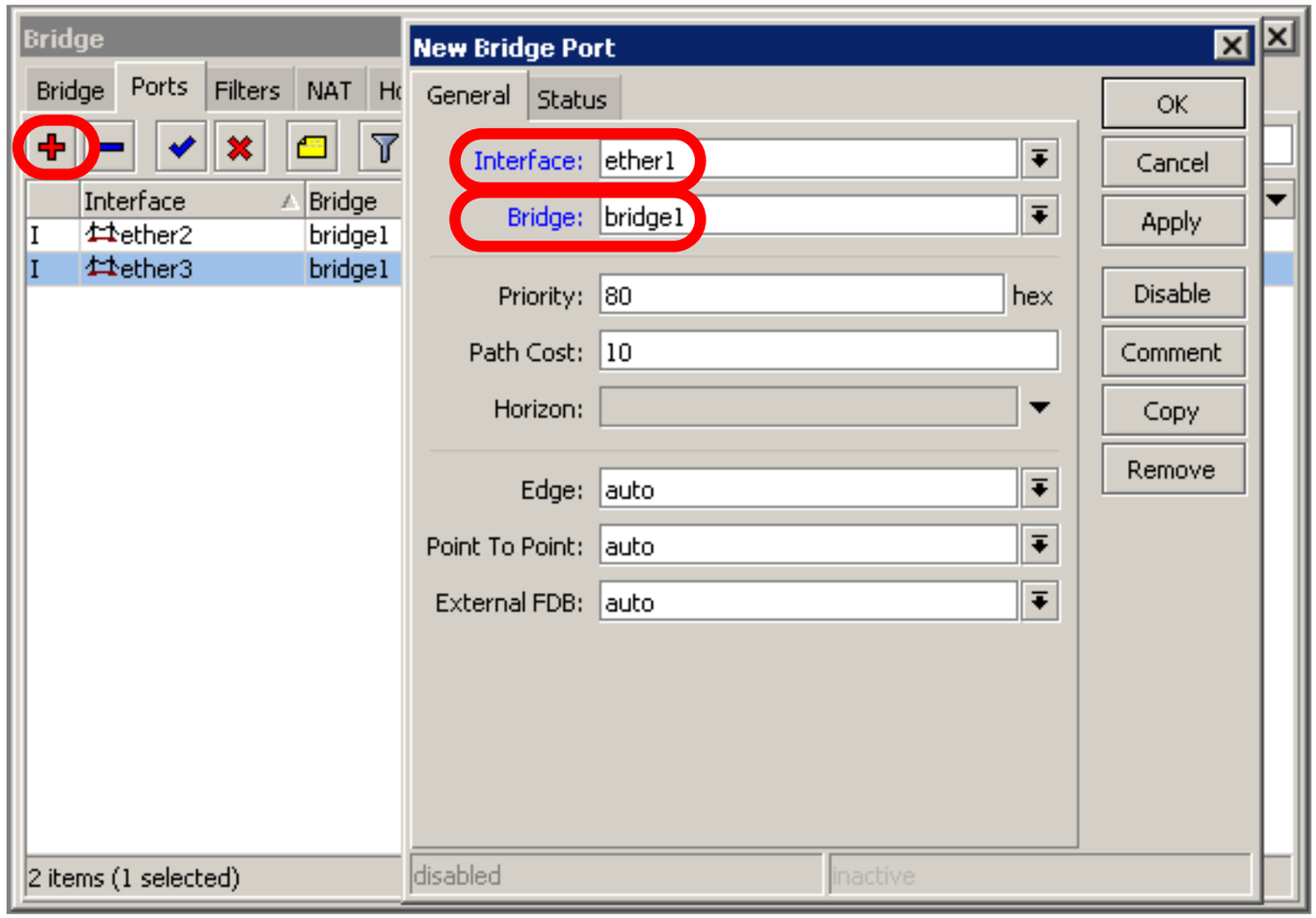
Create Bridge

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



Add Bridge Port

- Interfaces are added to bridge via ports



Bridge

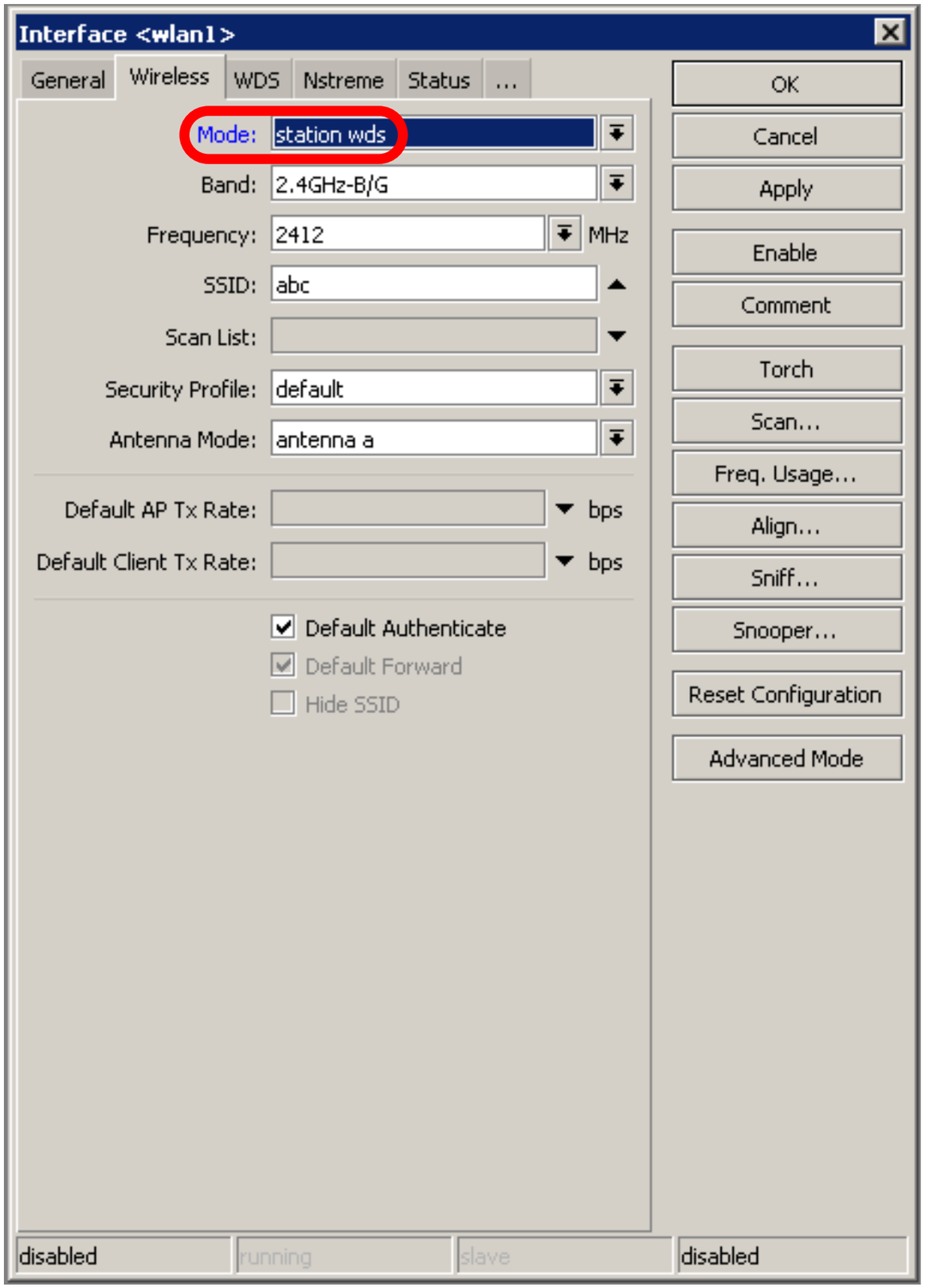
- There are no problems to bridge Ethernet interface
- Wireless Clients (**mode=station**) do not support **bridging** due the limitation of 802.11

Bridge Wireless

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

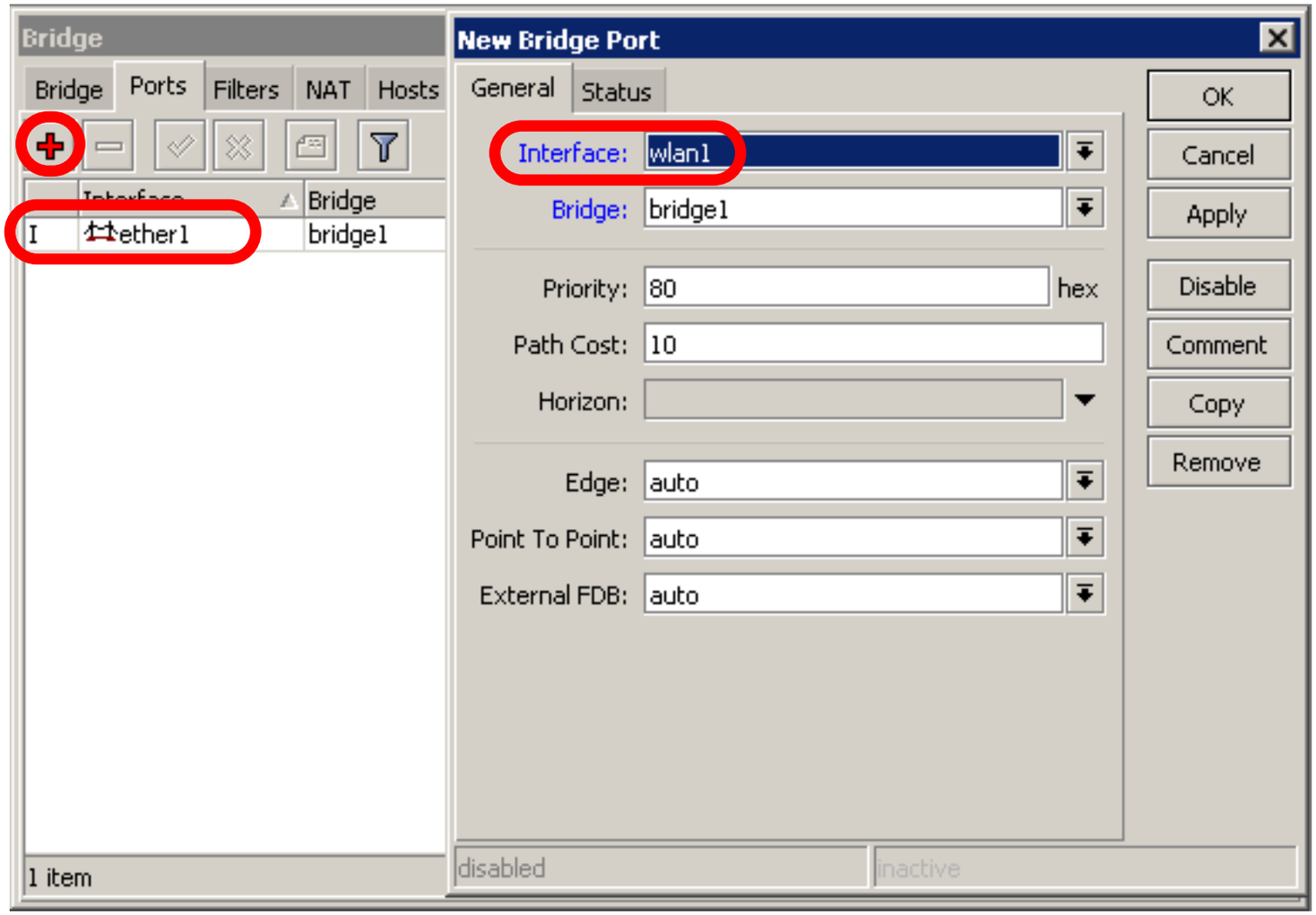
Set WDS Mode

- Station-wds is special station mode with WDS support



Add Bridge Ports

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

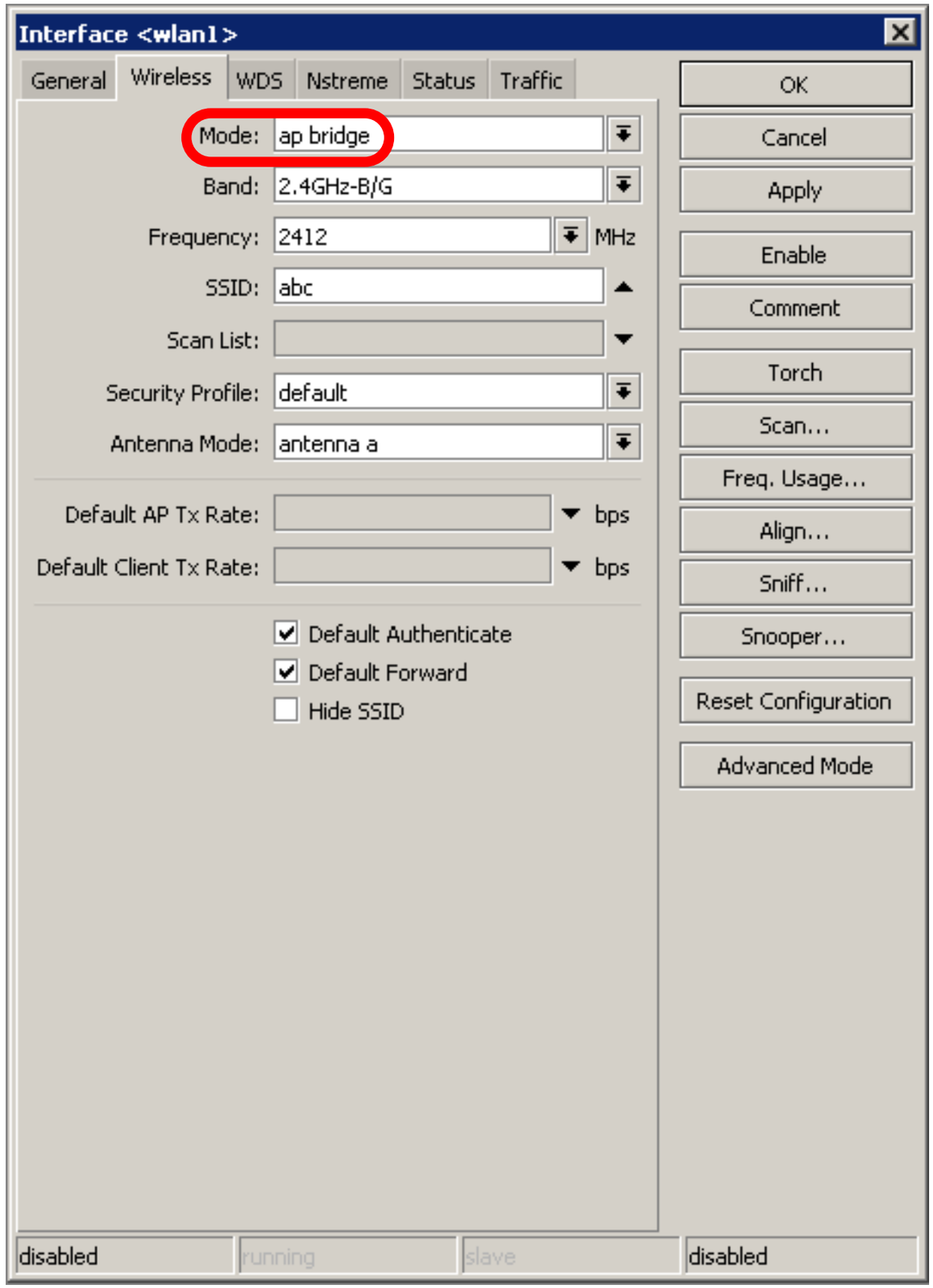


Access Point WDS

- 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

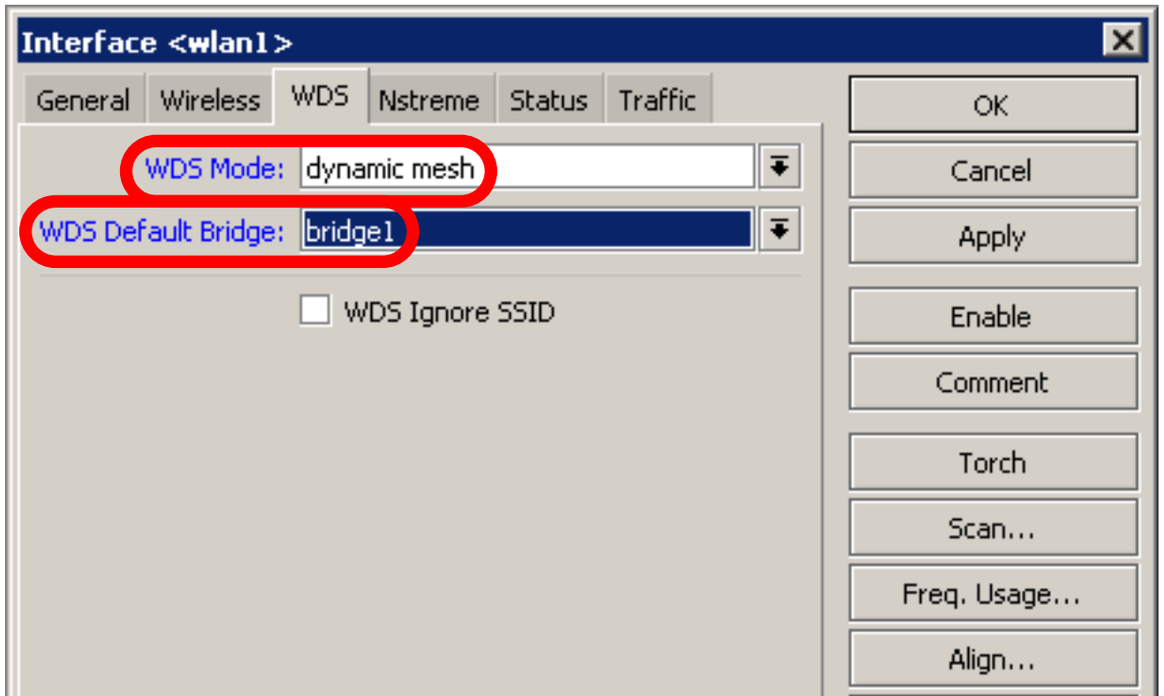
AP-bridge

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



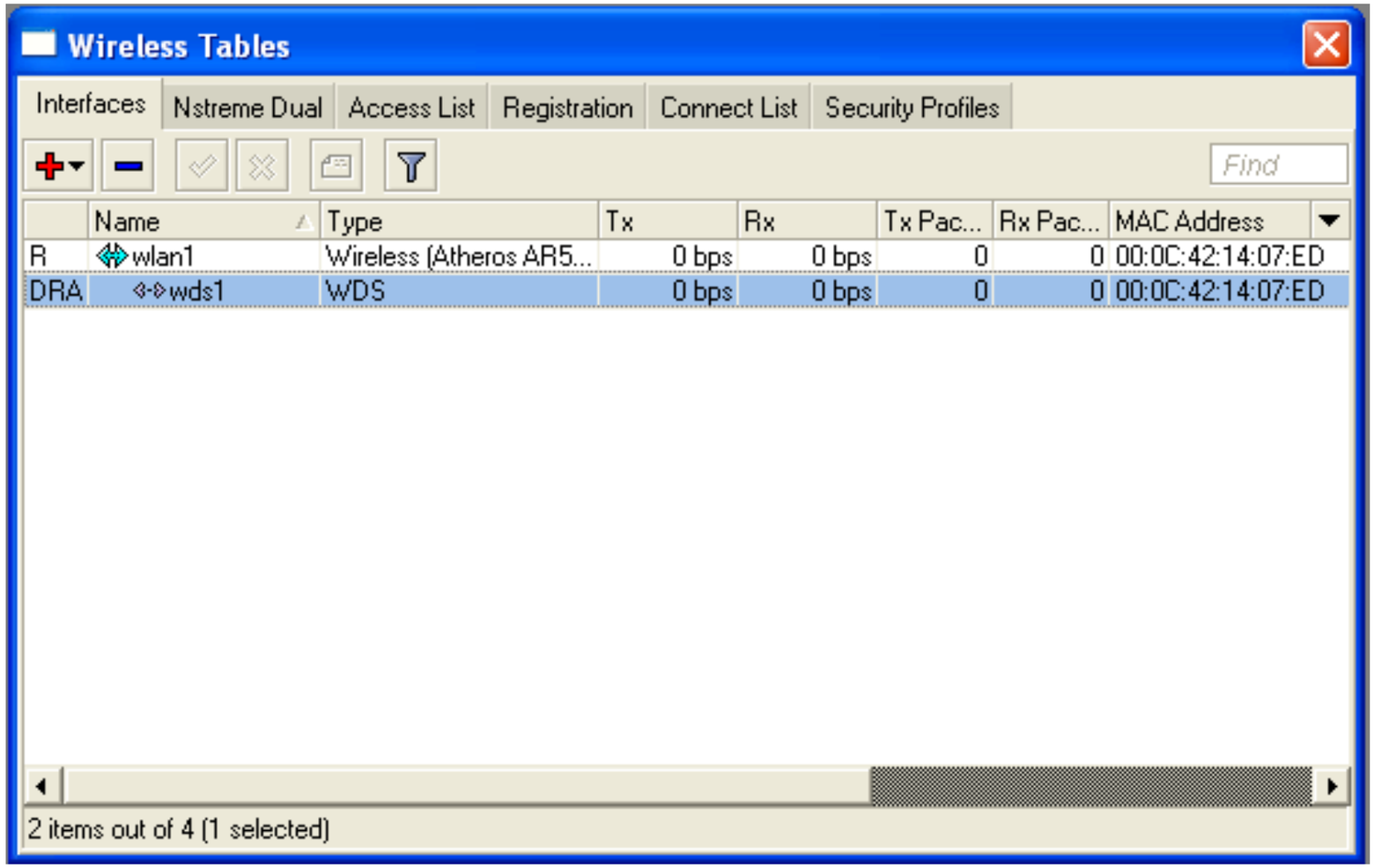
WDS configuration

- 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



LAB

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

LAB

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

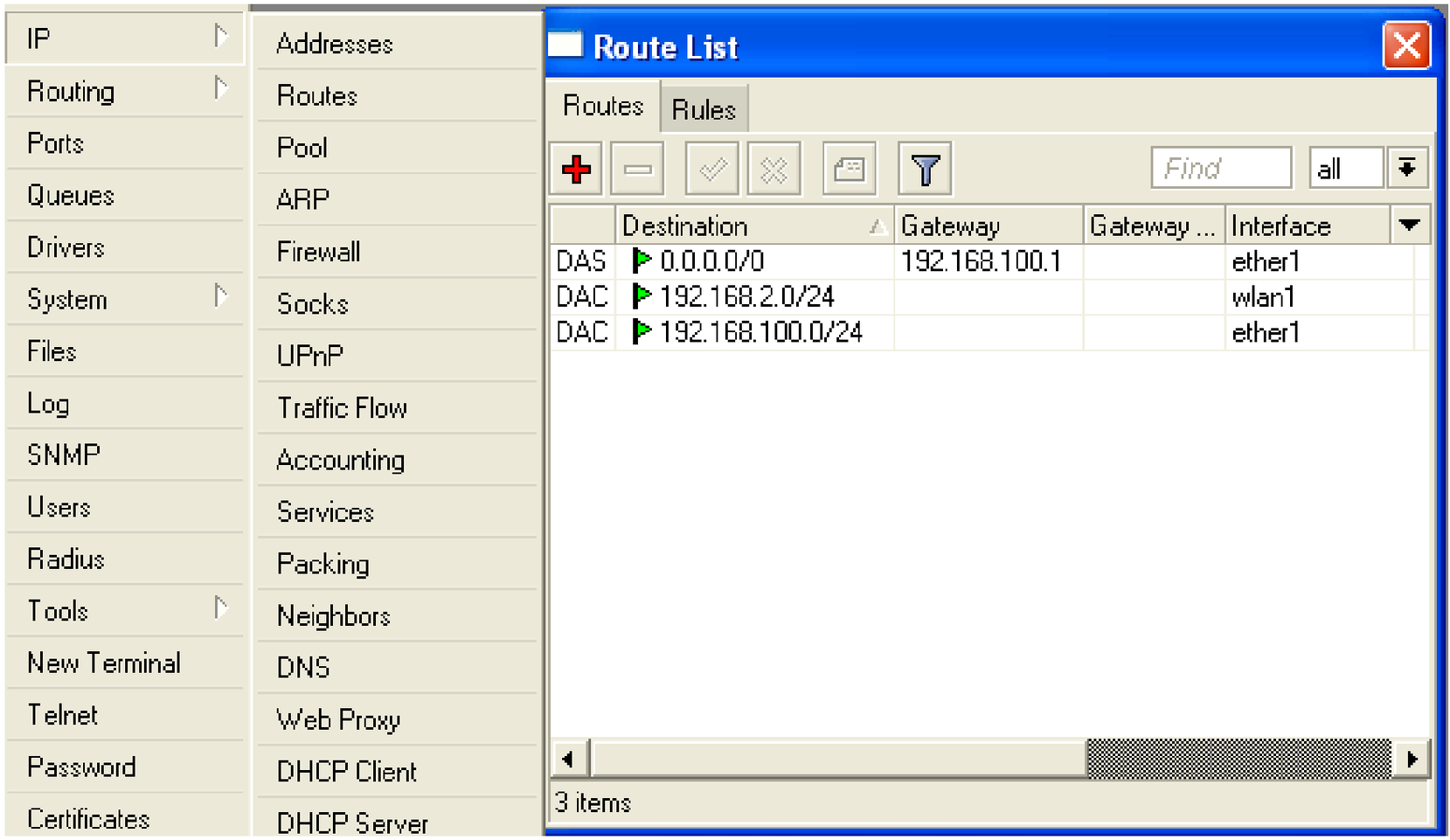
- Configuration is back
- Try to ping neighbor’s laptop
- Neighbor’s address 192.168.X.1
- We are going to learn how to use route rules to ping neighbor laptop

Route

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

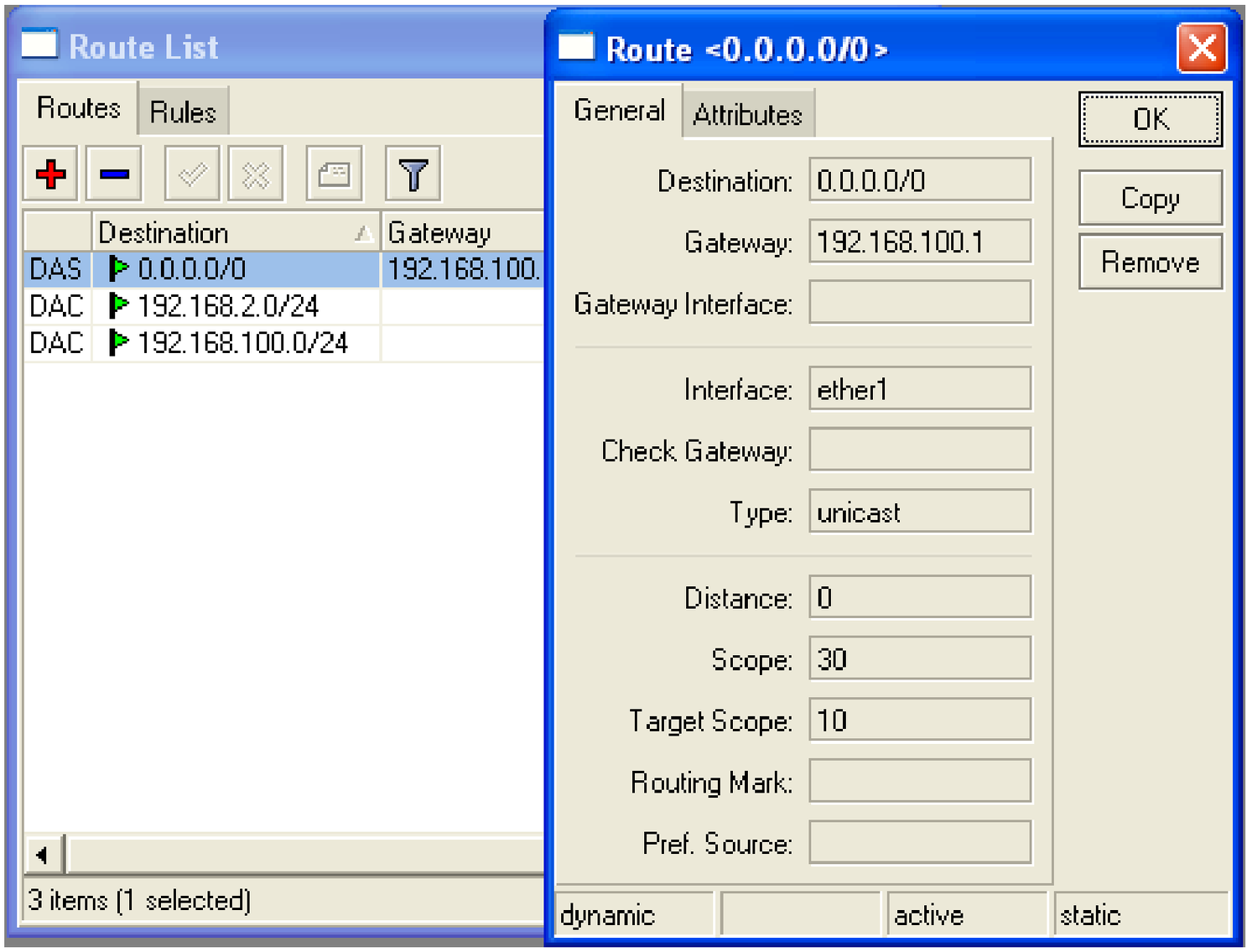
Routes

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



Default Gateway

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

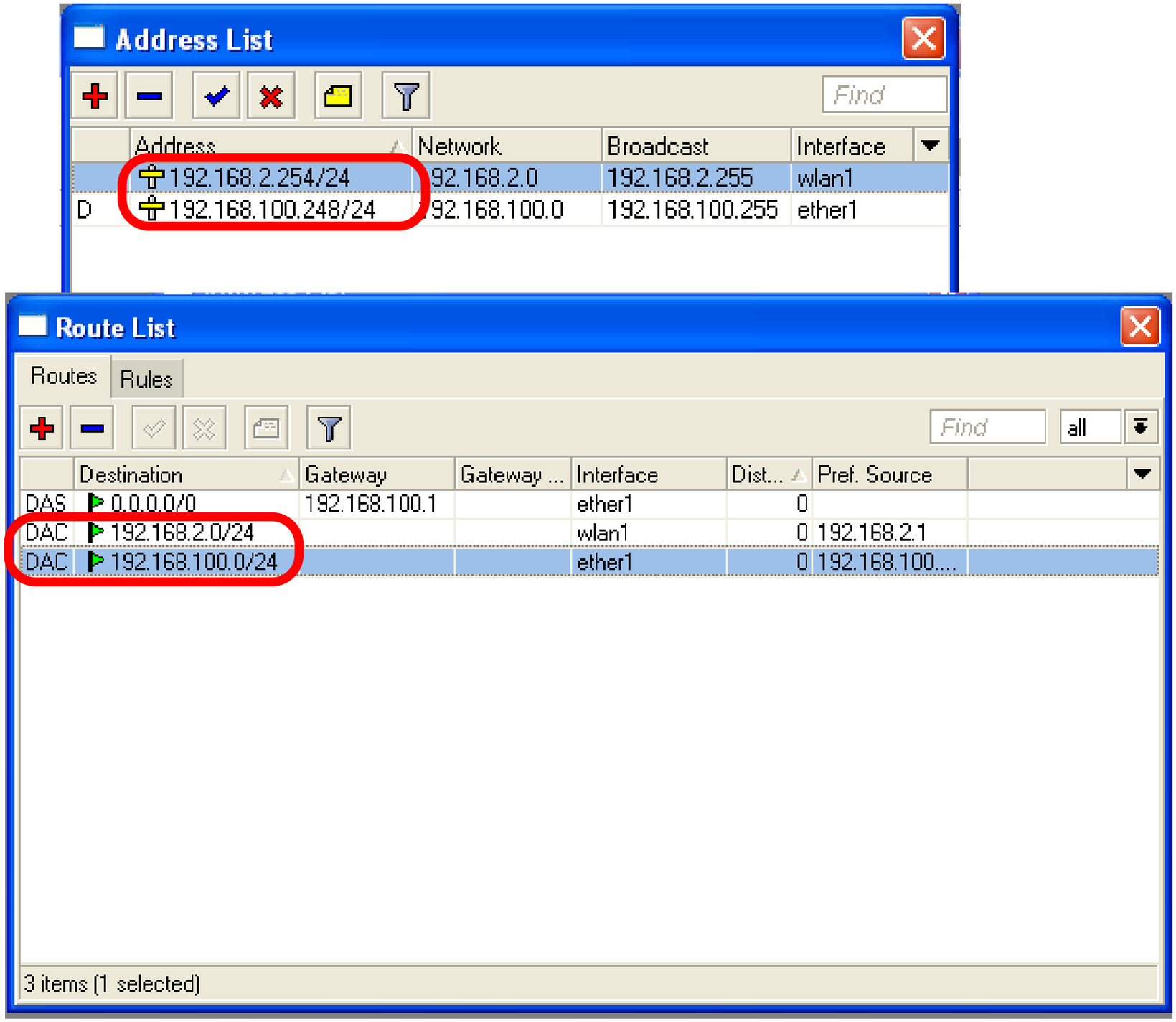


Set Default Gateway Lab

- 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



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

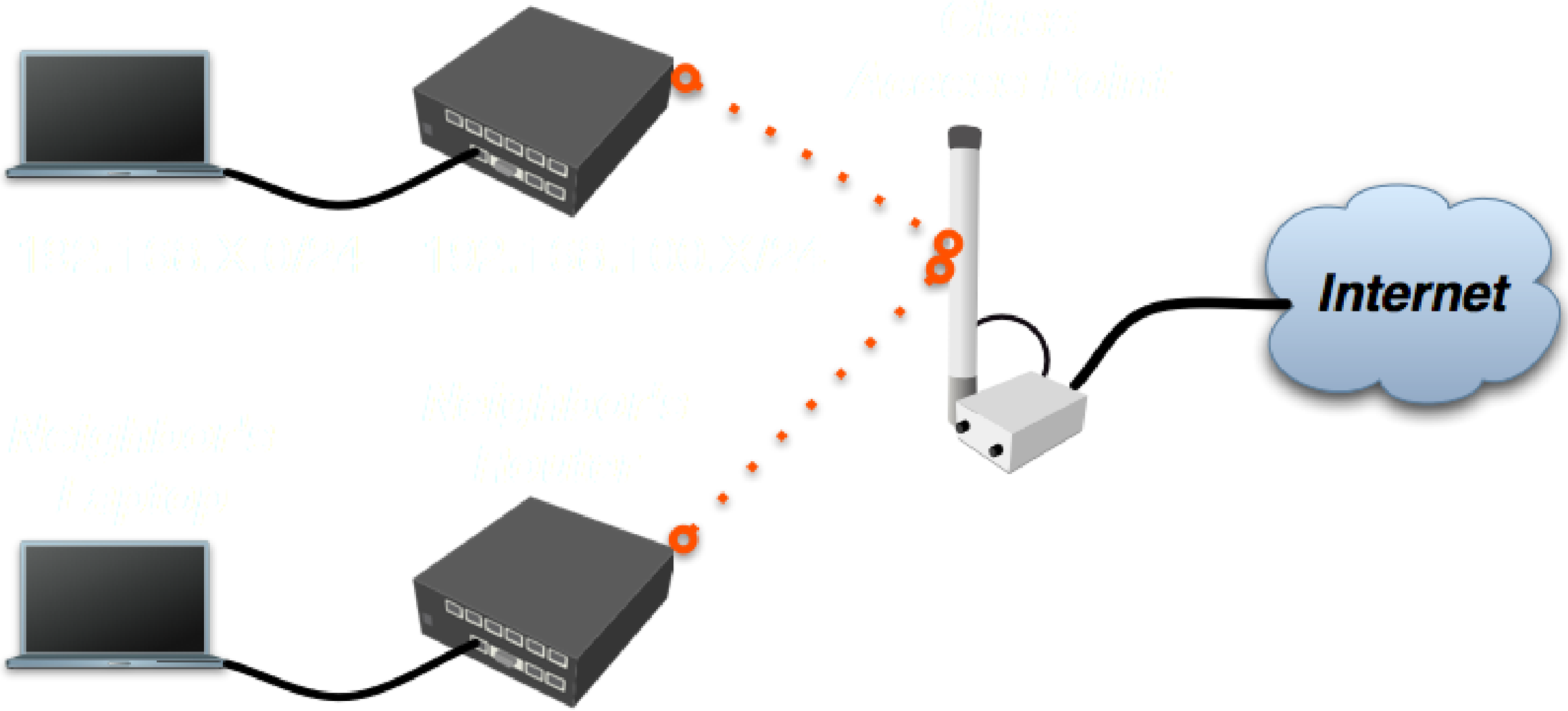
Static Route

- 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

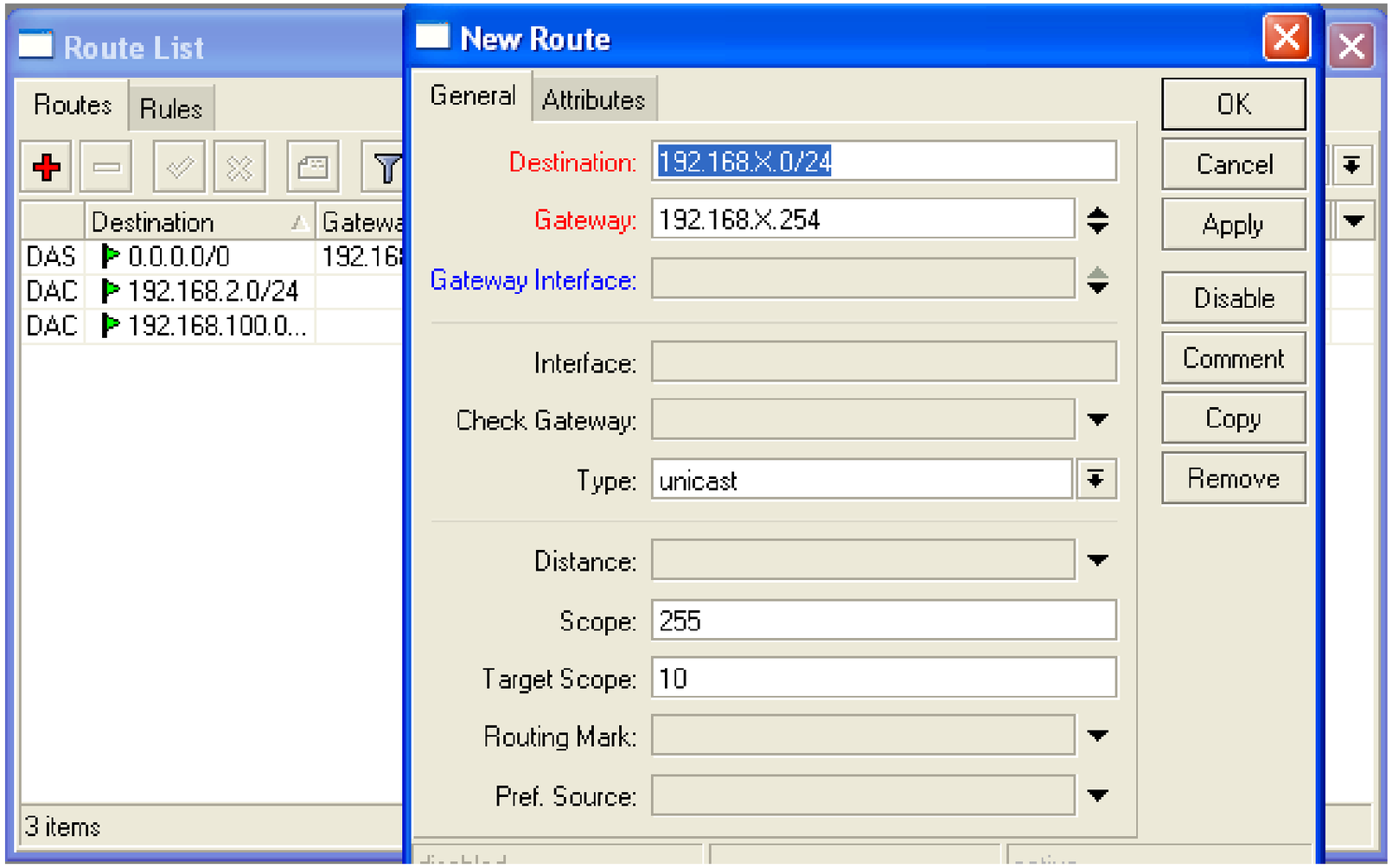
LAB

- 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

LAB

- 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

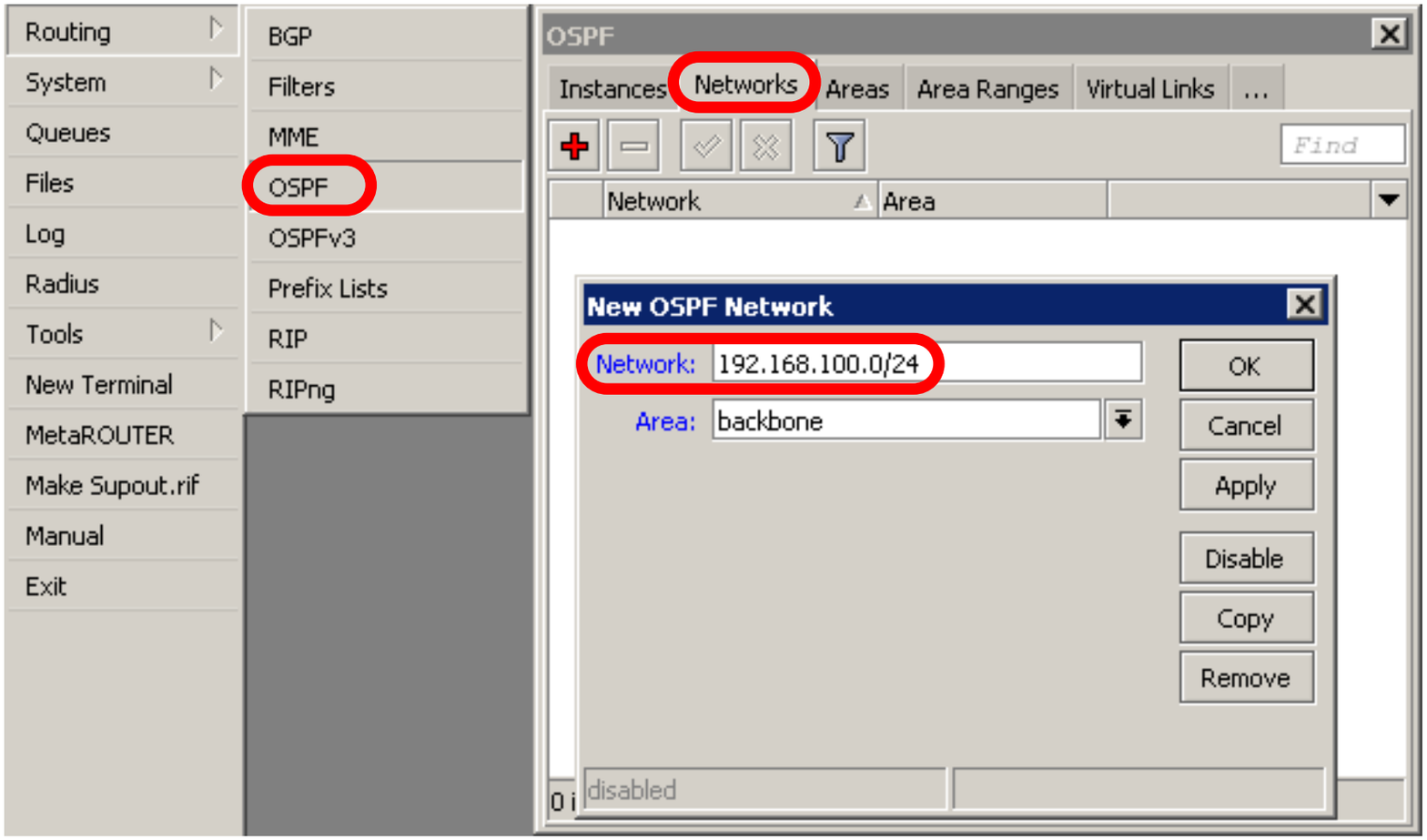
- Easy in configuration, difficult in managing/troubleshooting
- Can use more router resources

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

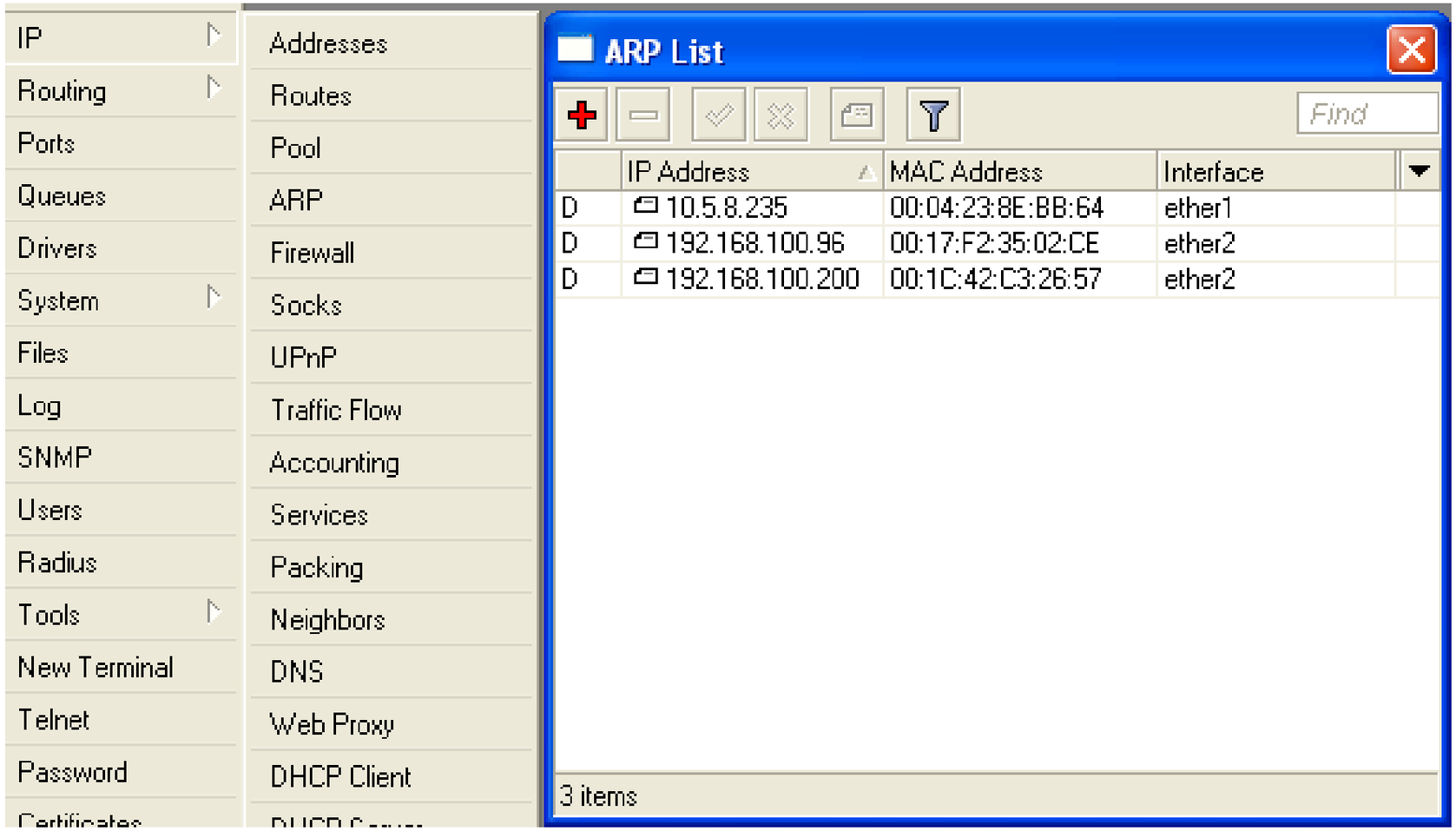
- Plan network design carefully
- Take care of user’s local access to the network
- Use RouterOS features to secure local network resources

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

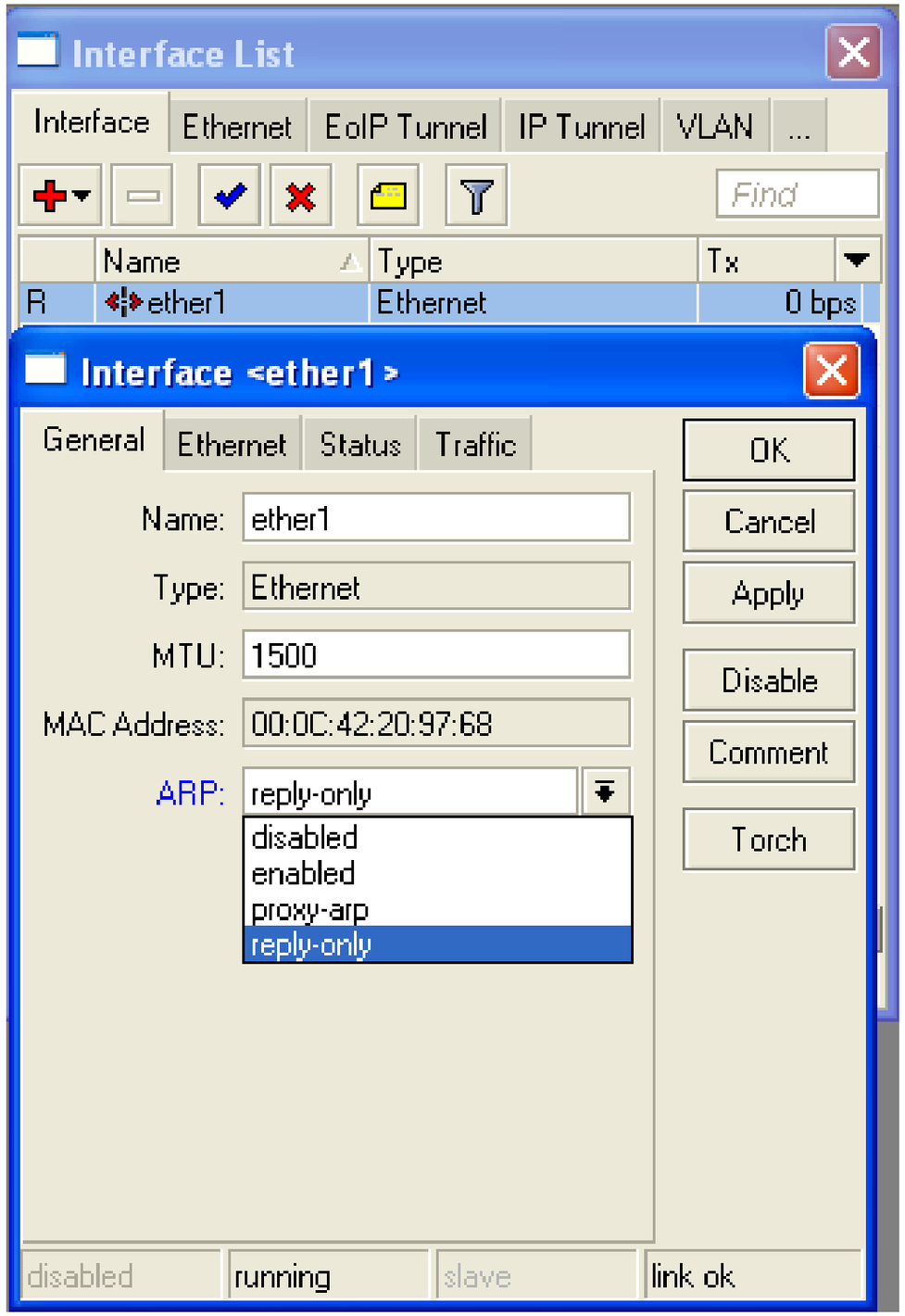


Static ARP table

- To increase network security ARP entries can be crated 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



LAB

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

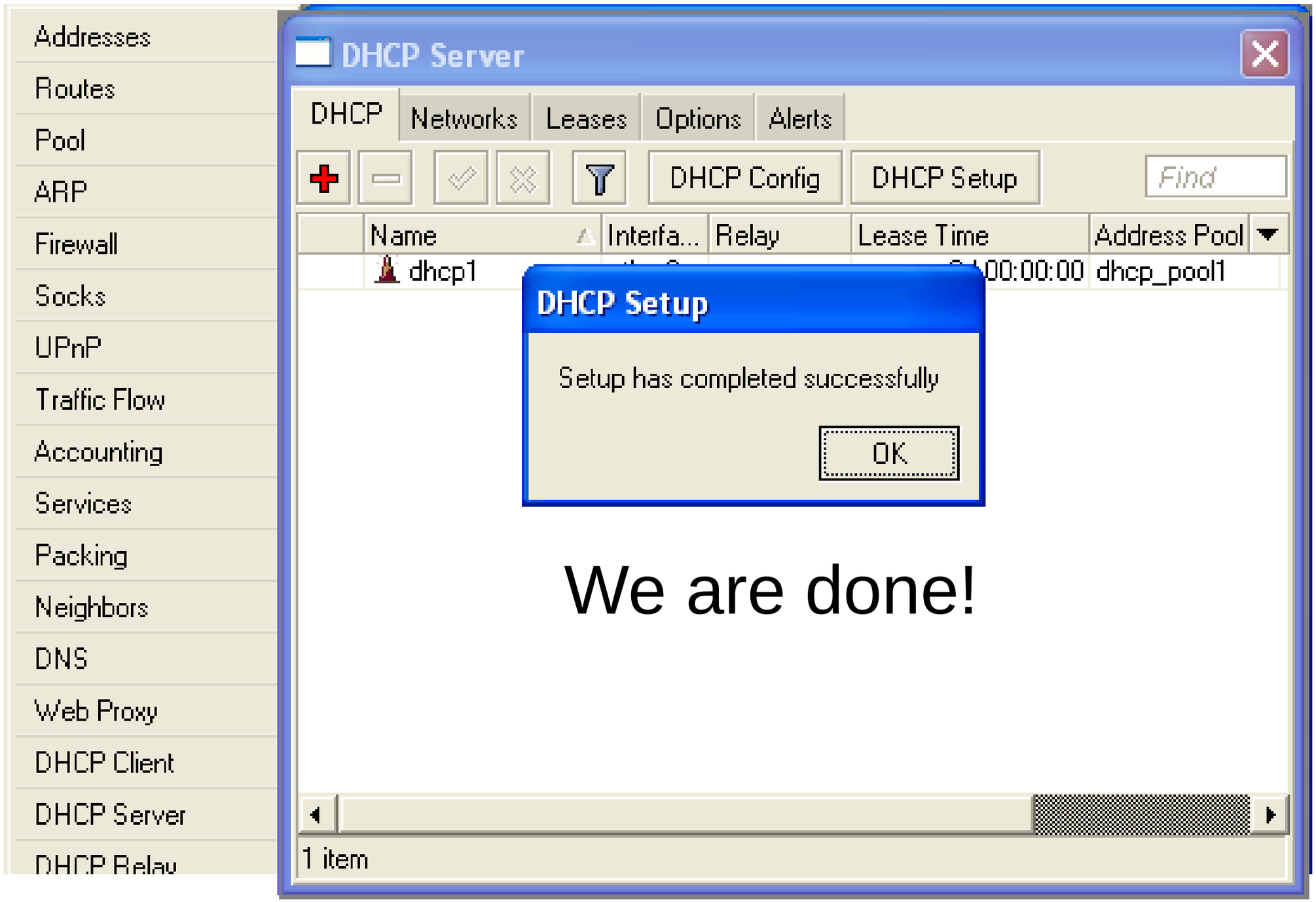
DHCP Server

- 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**

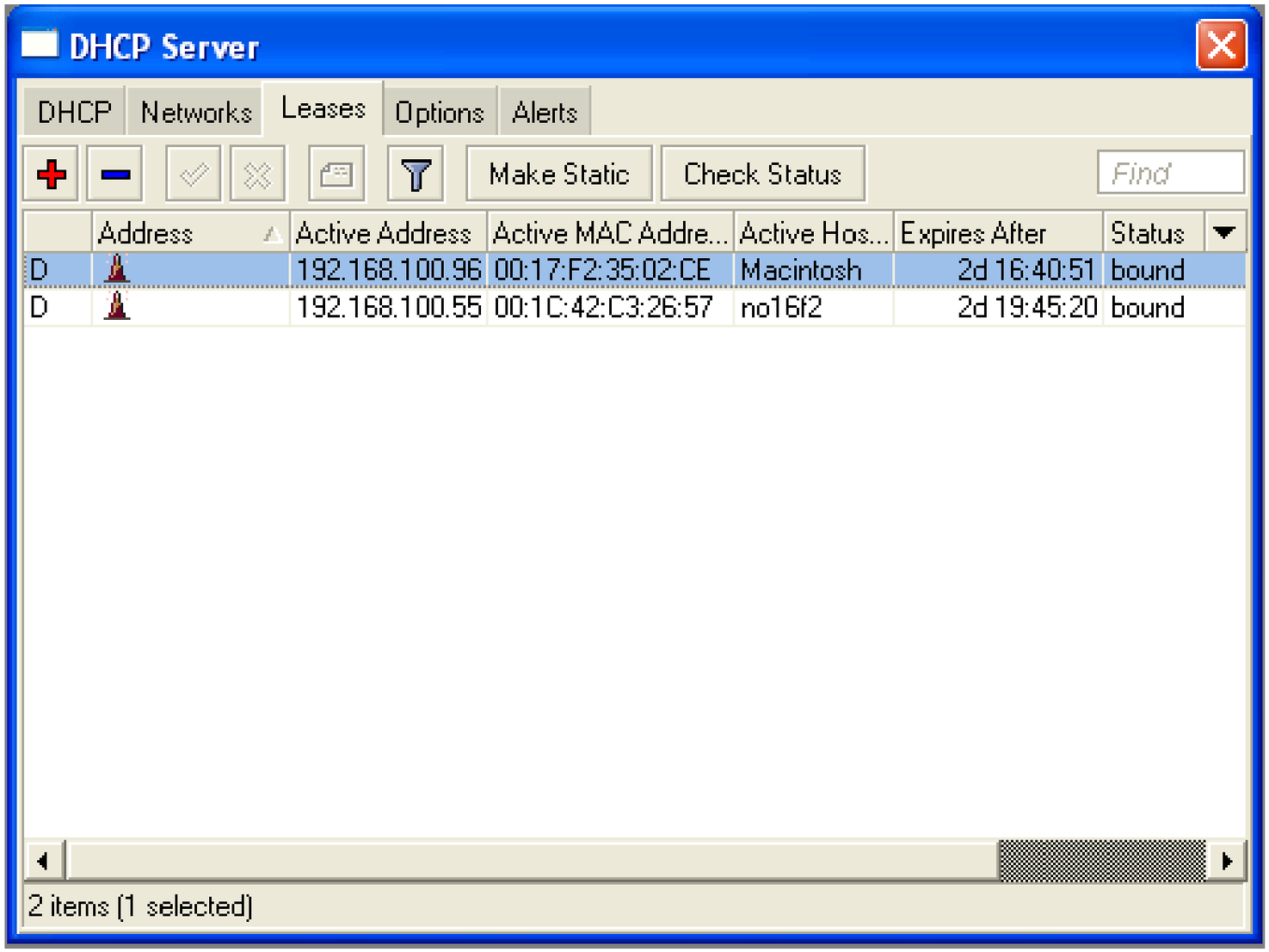
LAB

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

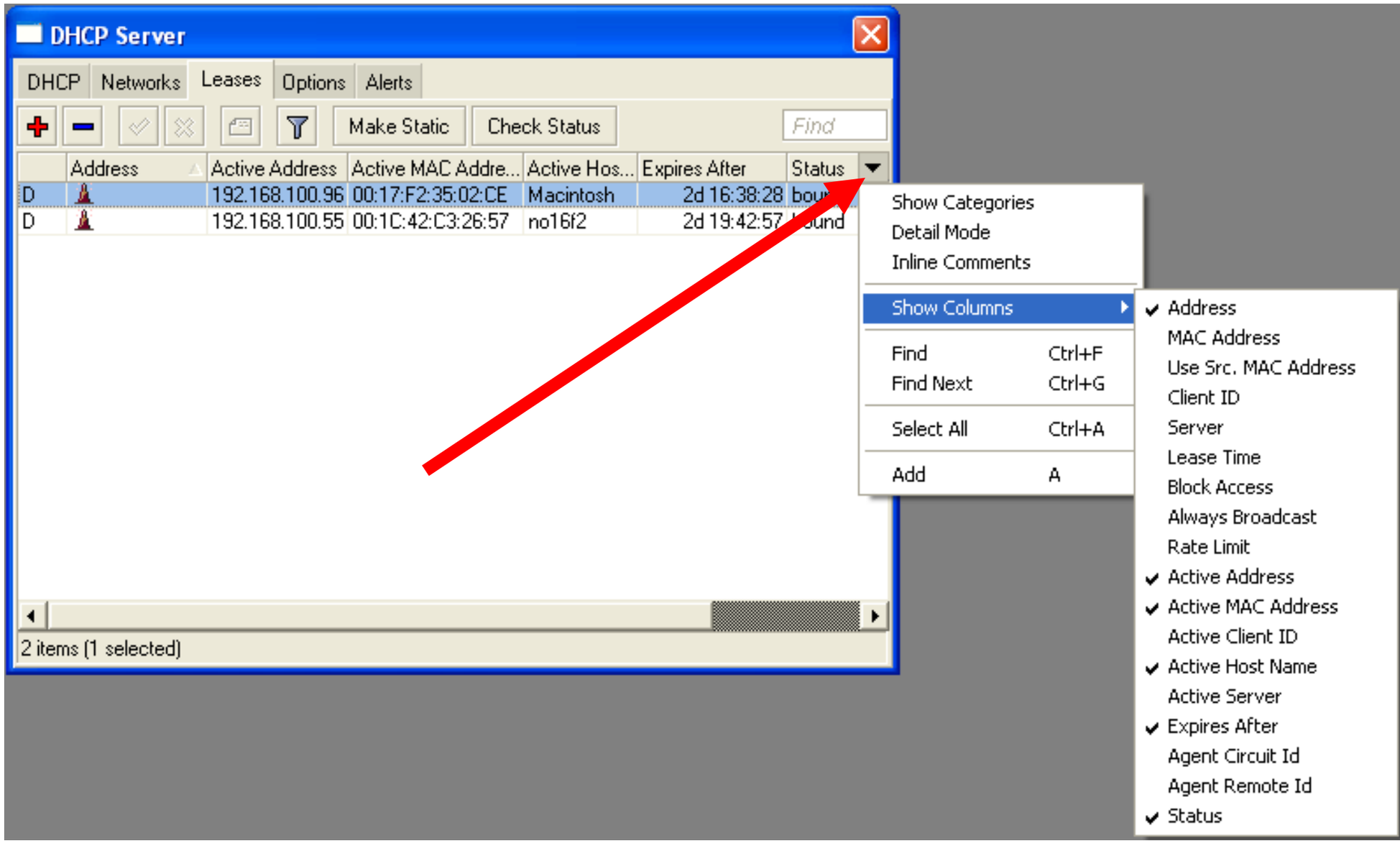
DHCP Server Information

- Leases provide information about DHCP clients



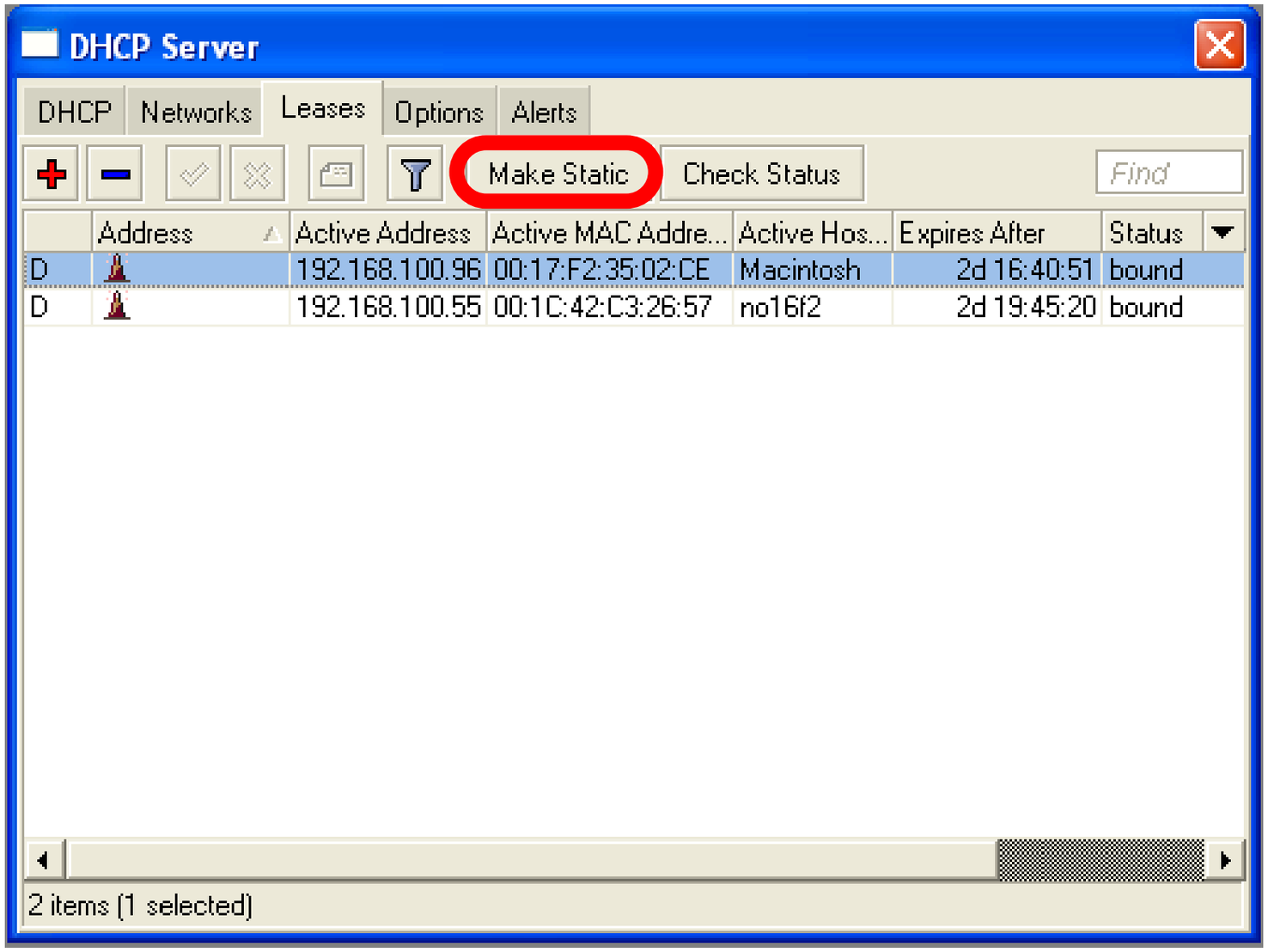
Winbox Configuration Tip

Show or hide different Winbox columns



Static Lease

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



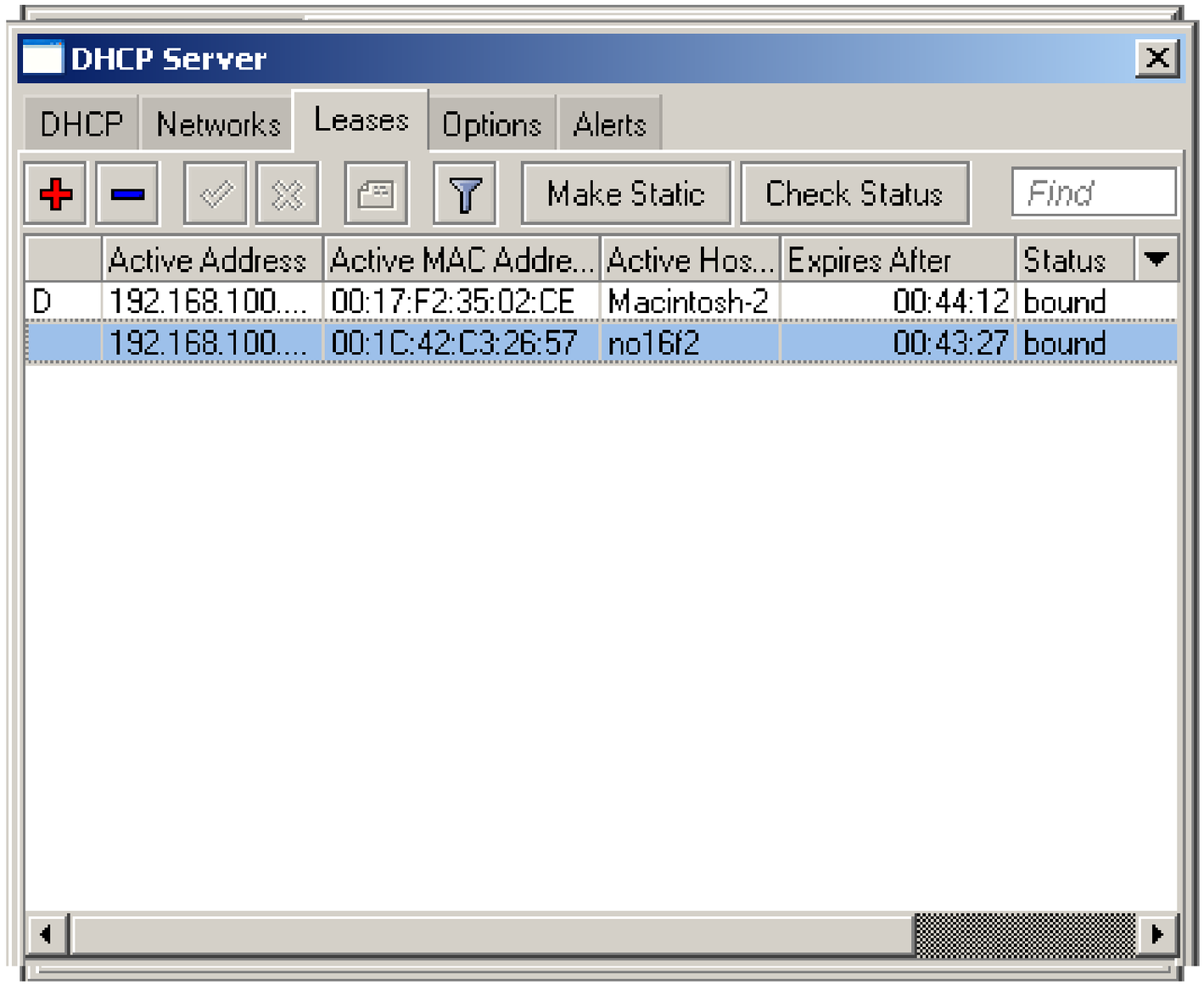
Static Lease

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

LAB

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

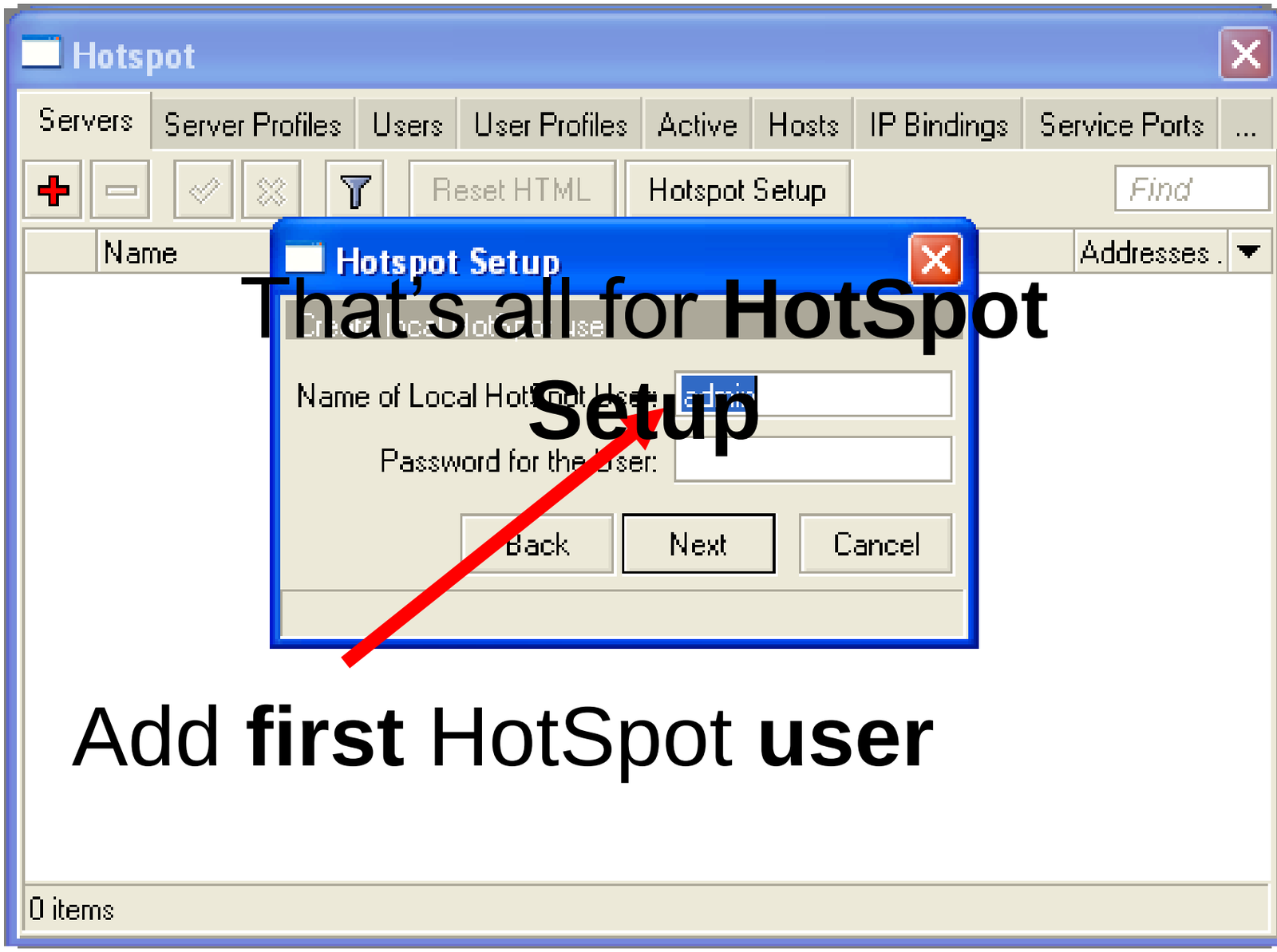
- Valid **IP addresses** on Internet and Local **Interfaces**
- DNS servers addresses added to **ip dns**
- At least one HotSpot user

HotSpot Setup

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

HotSpot Setup

- Run **ip hotspot setup**
- Select Inteface
- 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

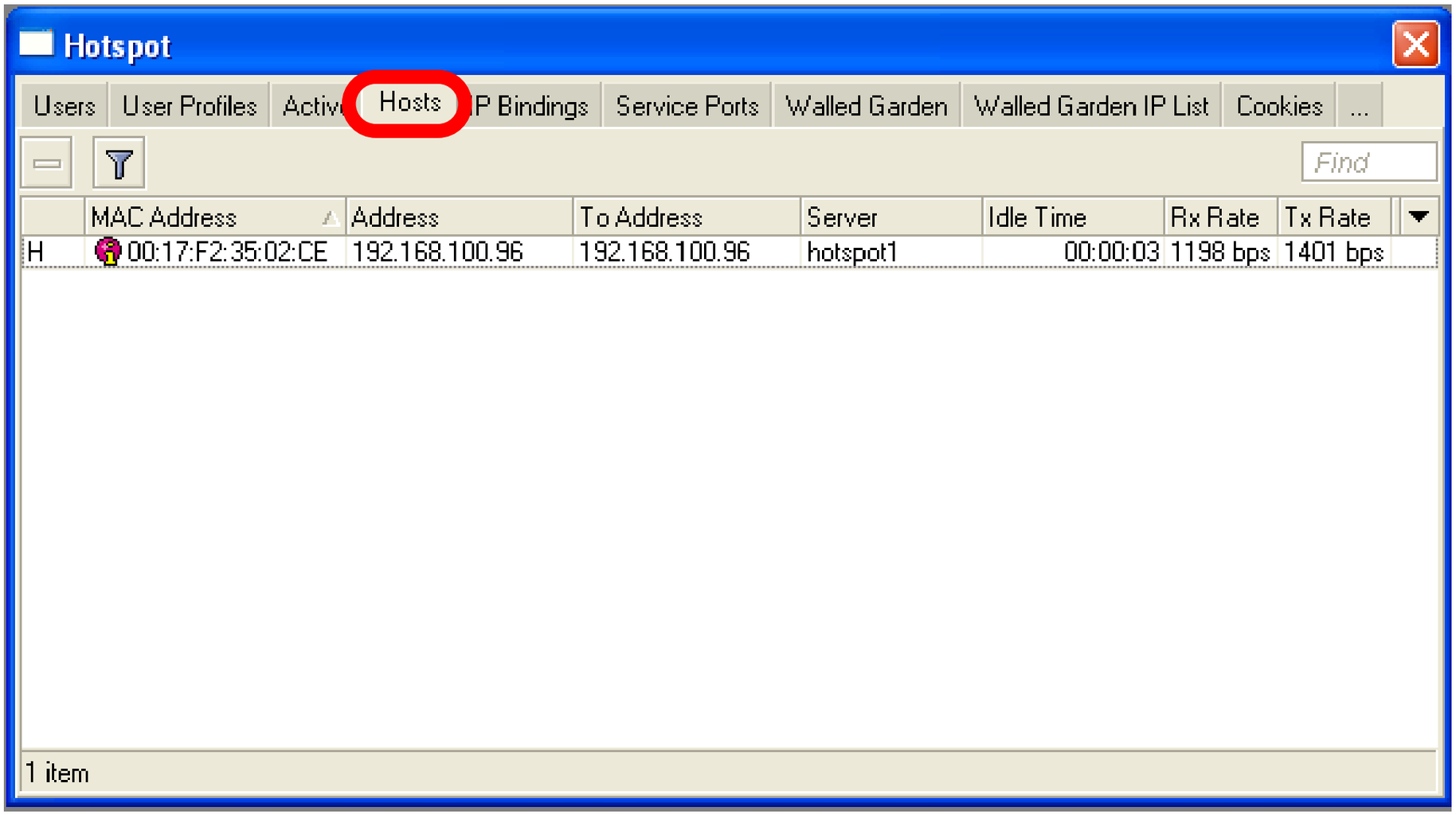
- HotSpot login page is provided when user tries to access any web-page
- To logout from HotSpot you need to go to http://router_IP or http://HotSpot_DNS

LAB

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

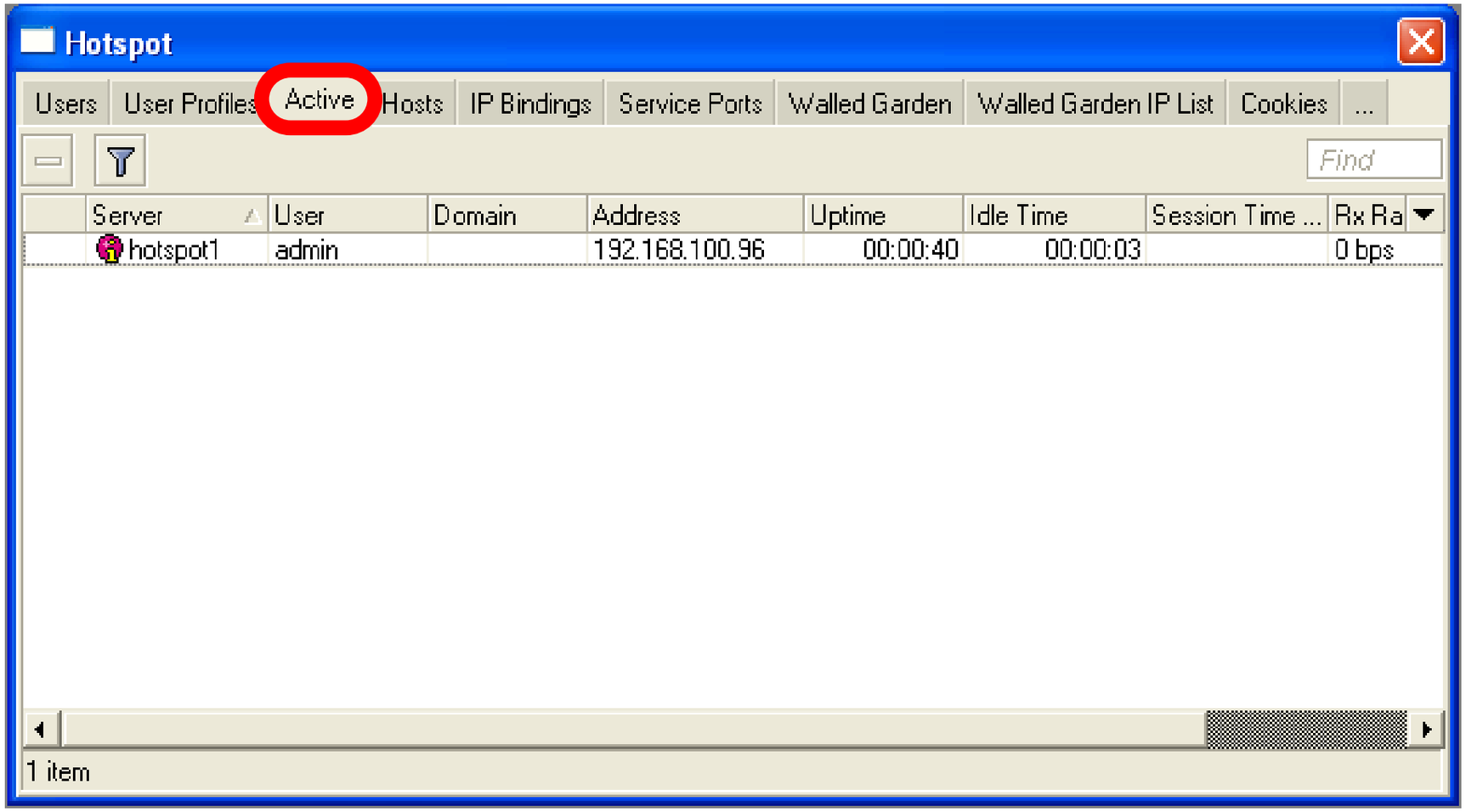
HotSpot Network Hosts



Information about clients connected to HotSpot router

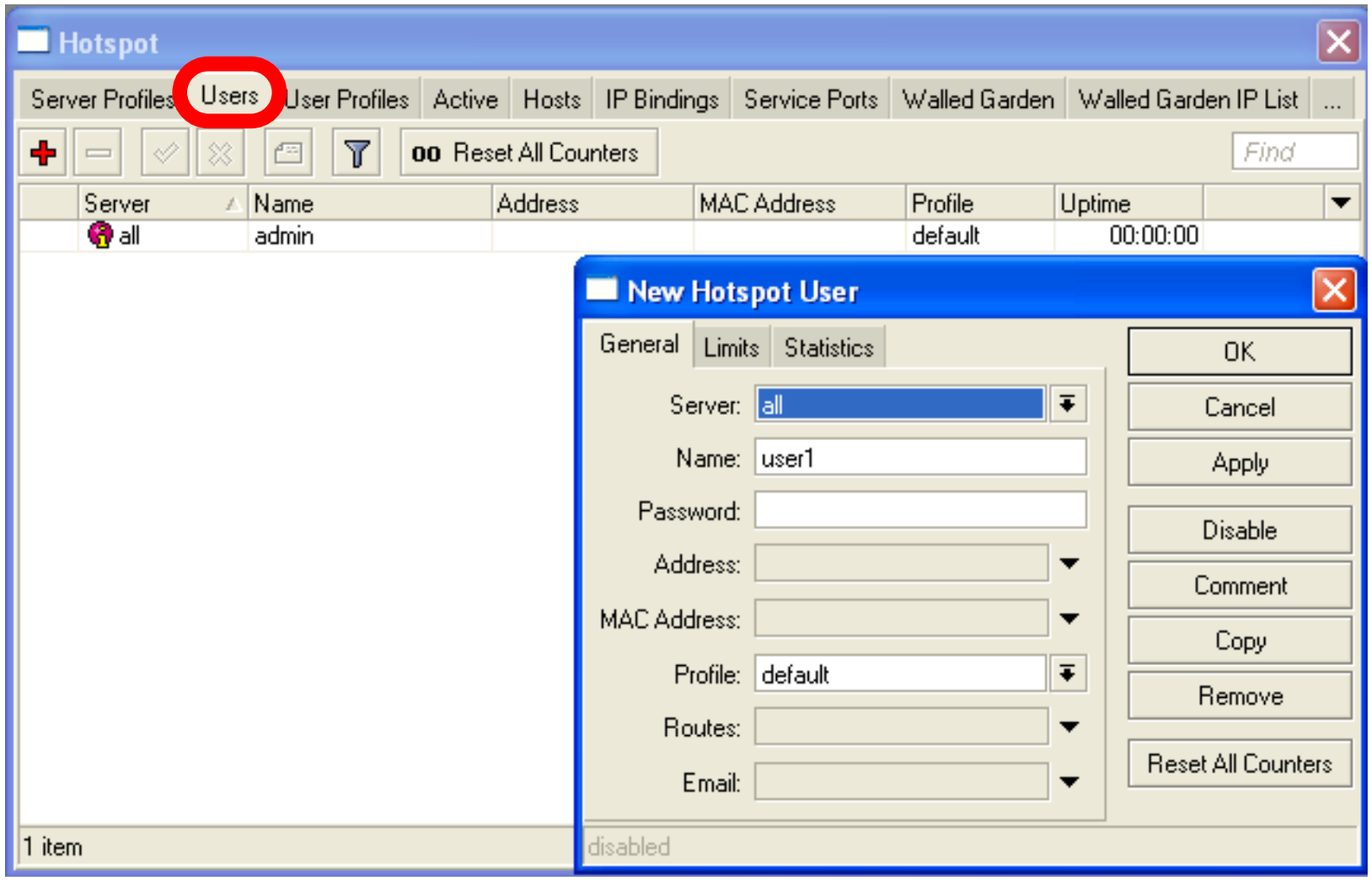
HotSpot Active Table

Information about authorized HotSpot clients



User Management

Add/Edit/Remove HotSpot users

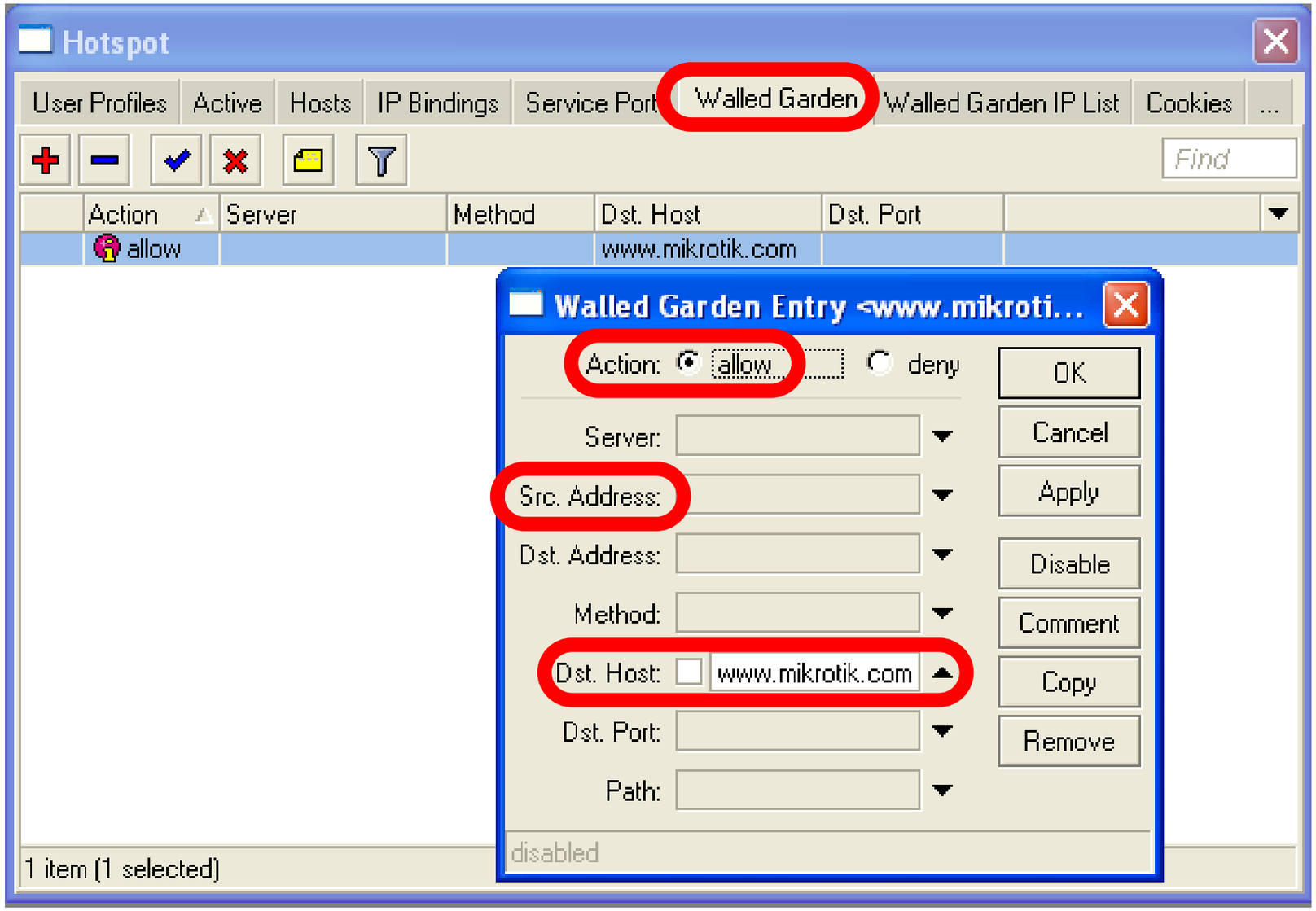


HotSpot Walled-Garden

- 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.)

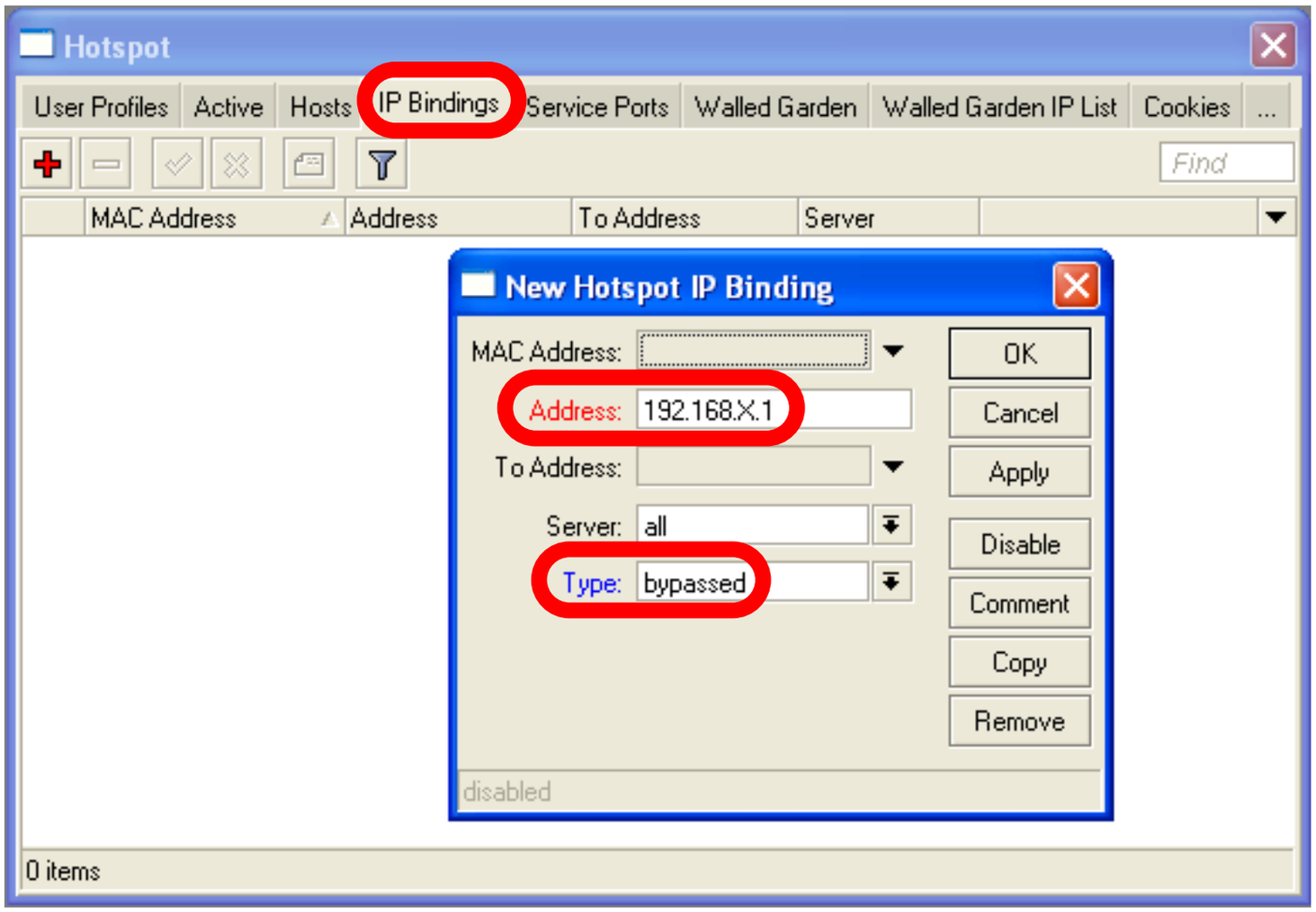
HotSpot Walled-Garden

Allow access to mikrotik.com



Bypass HotSpot

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

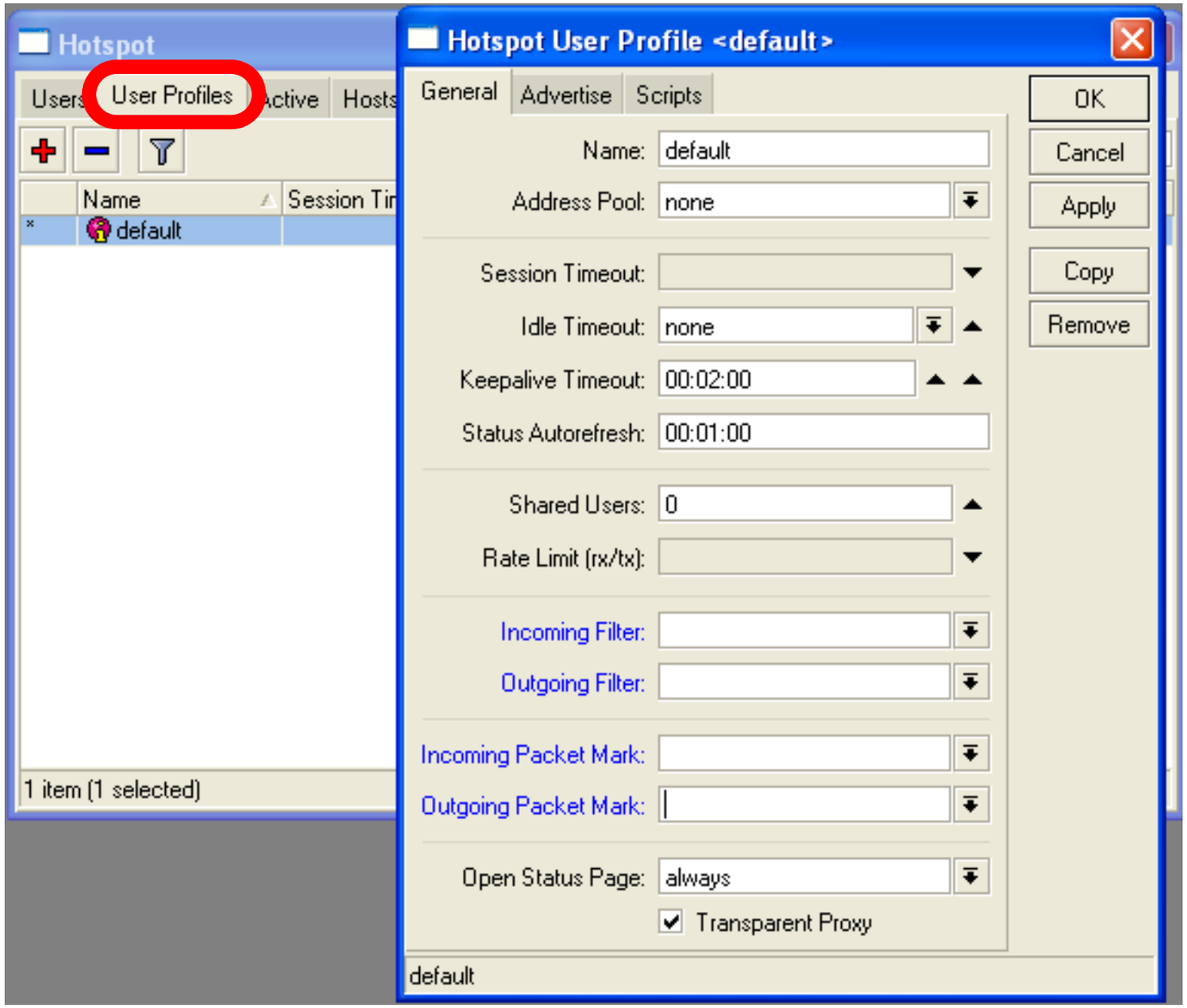


HotSpot Bandwidth Limits

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

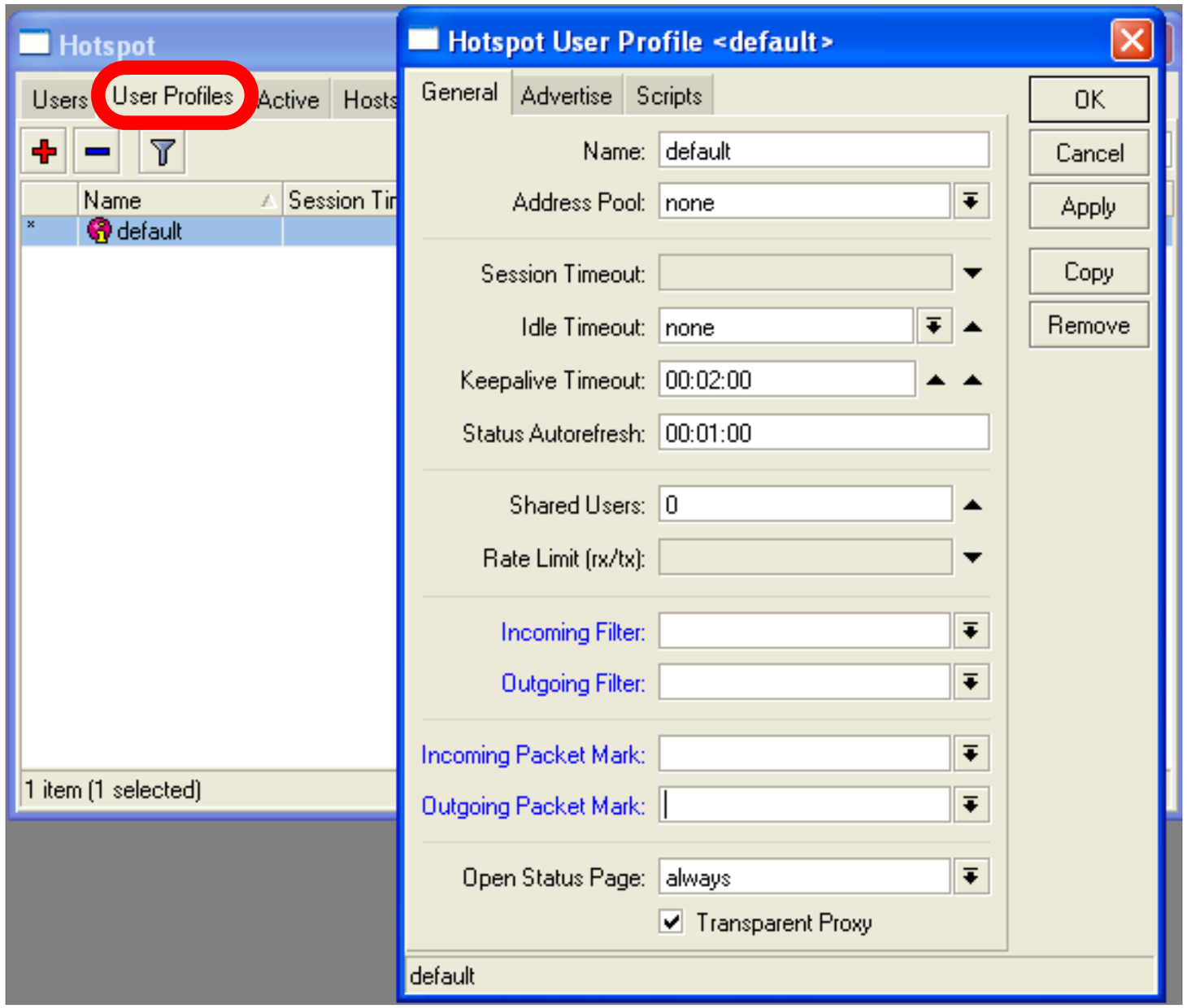
HotSpot User Profile

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**



LAB

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

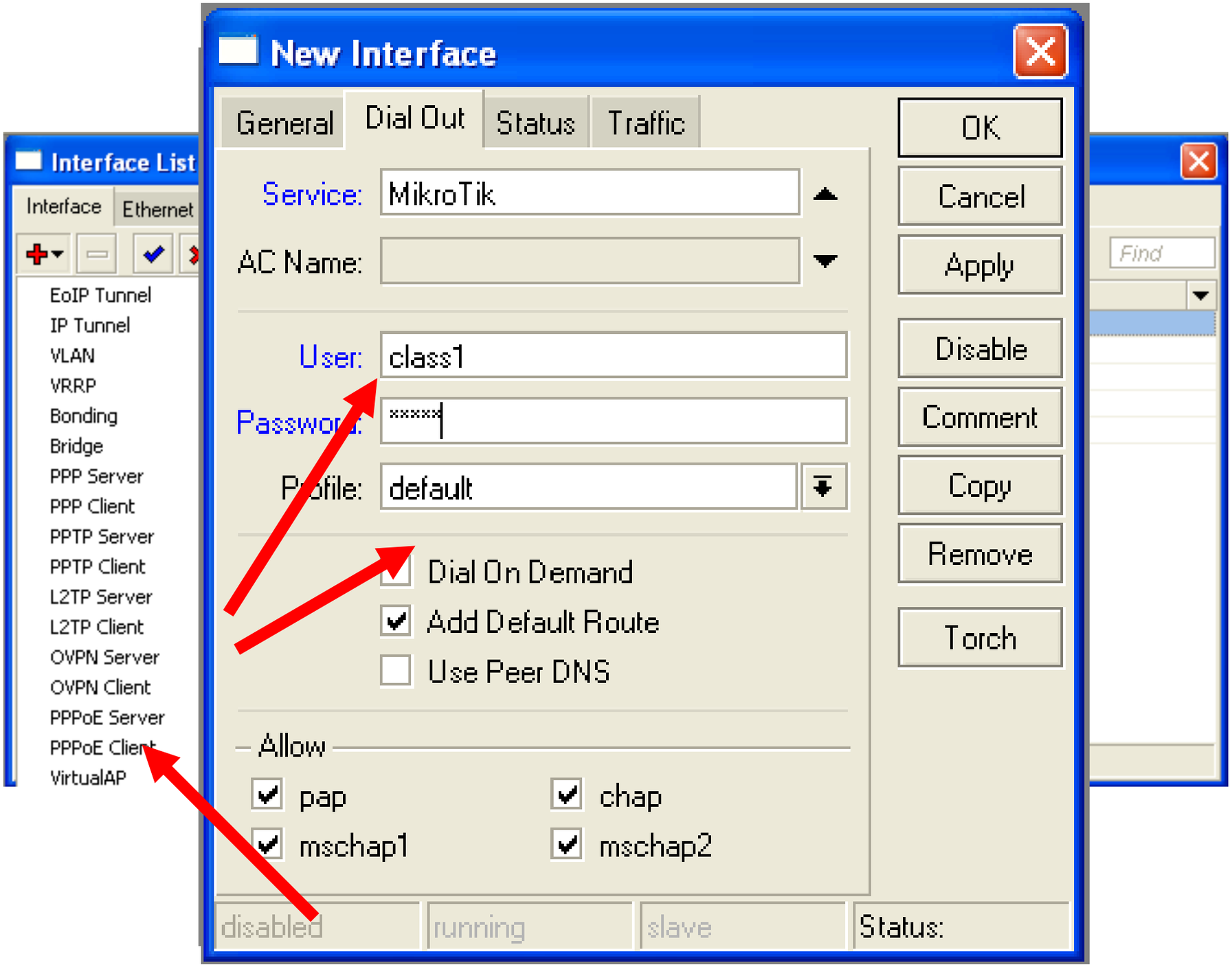
Tunnels

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 **Interace**
- Set **Login** and **Password**



LAB

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**

LAB

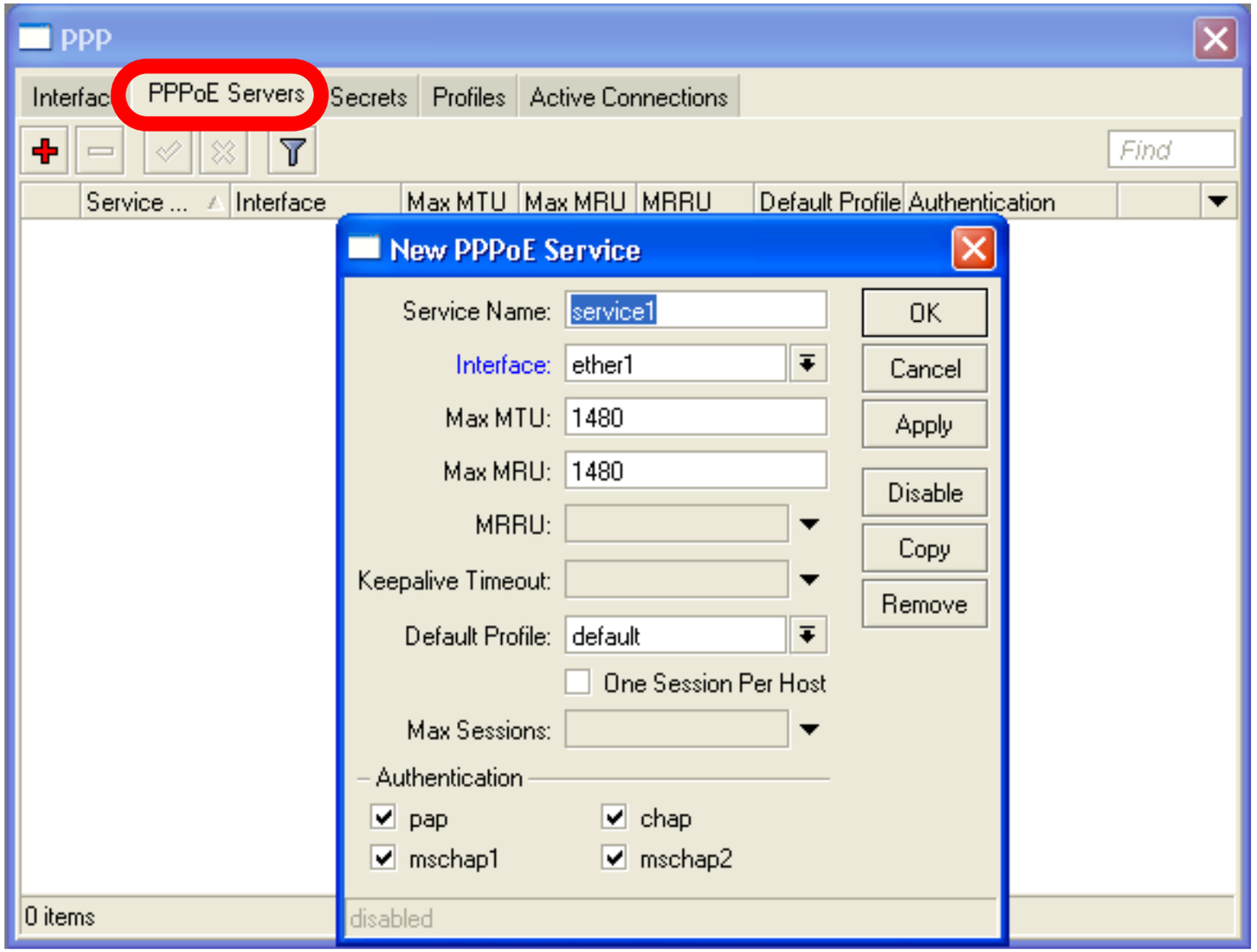
PPPoE Client Setup

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

LAB

PPPoE Server Setup

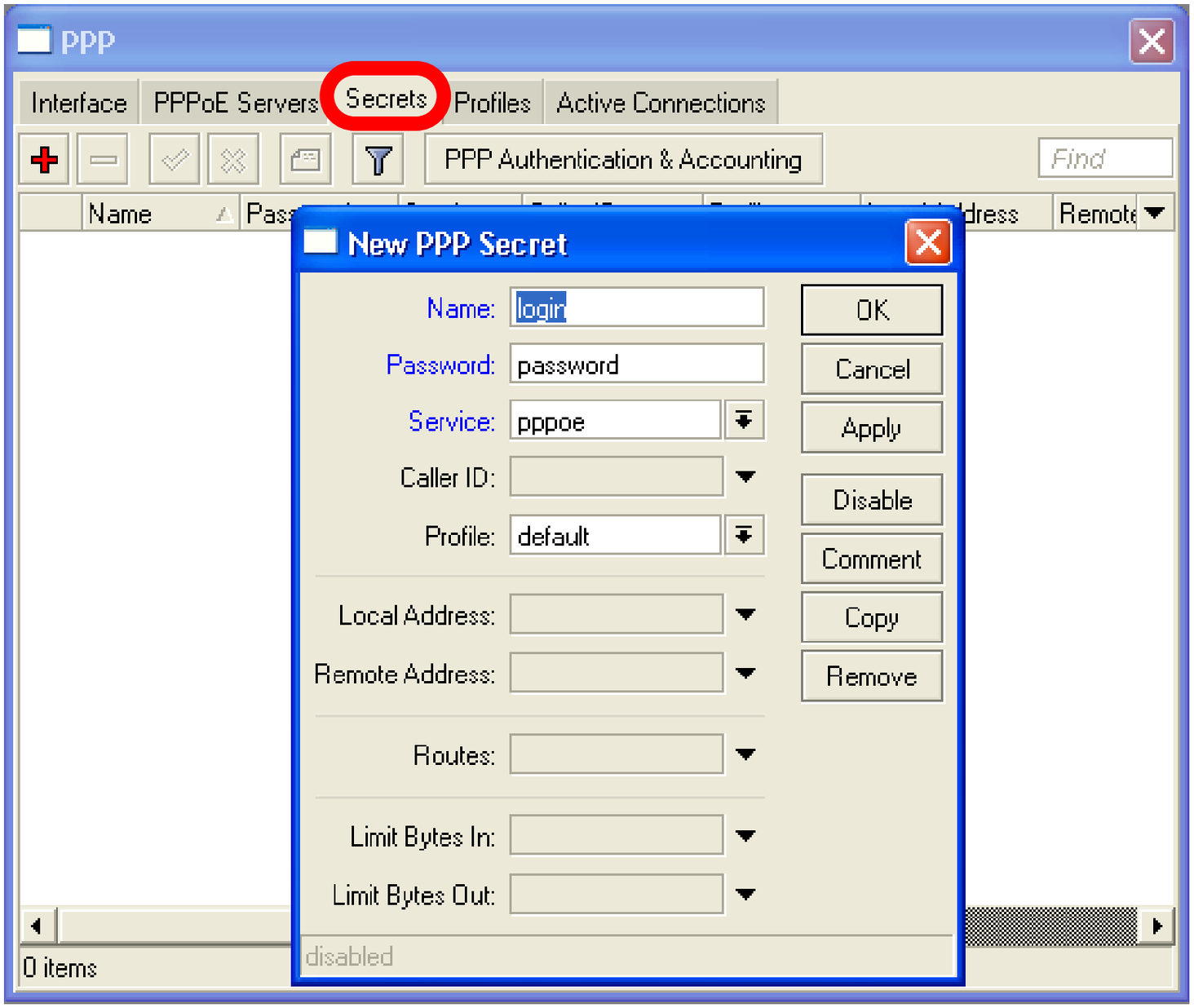
- Select Interface
- Select Profile



LAB

PPP Secret

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

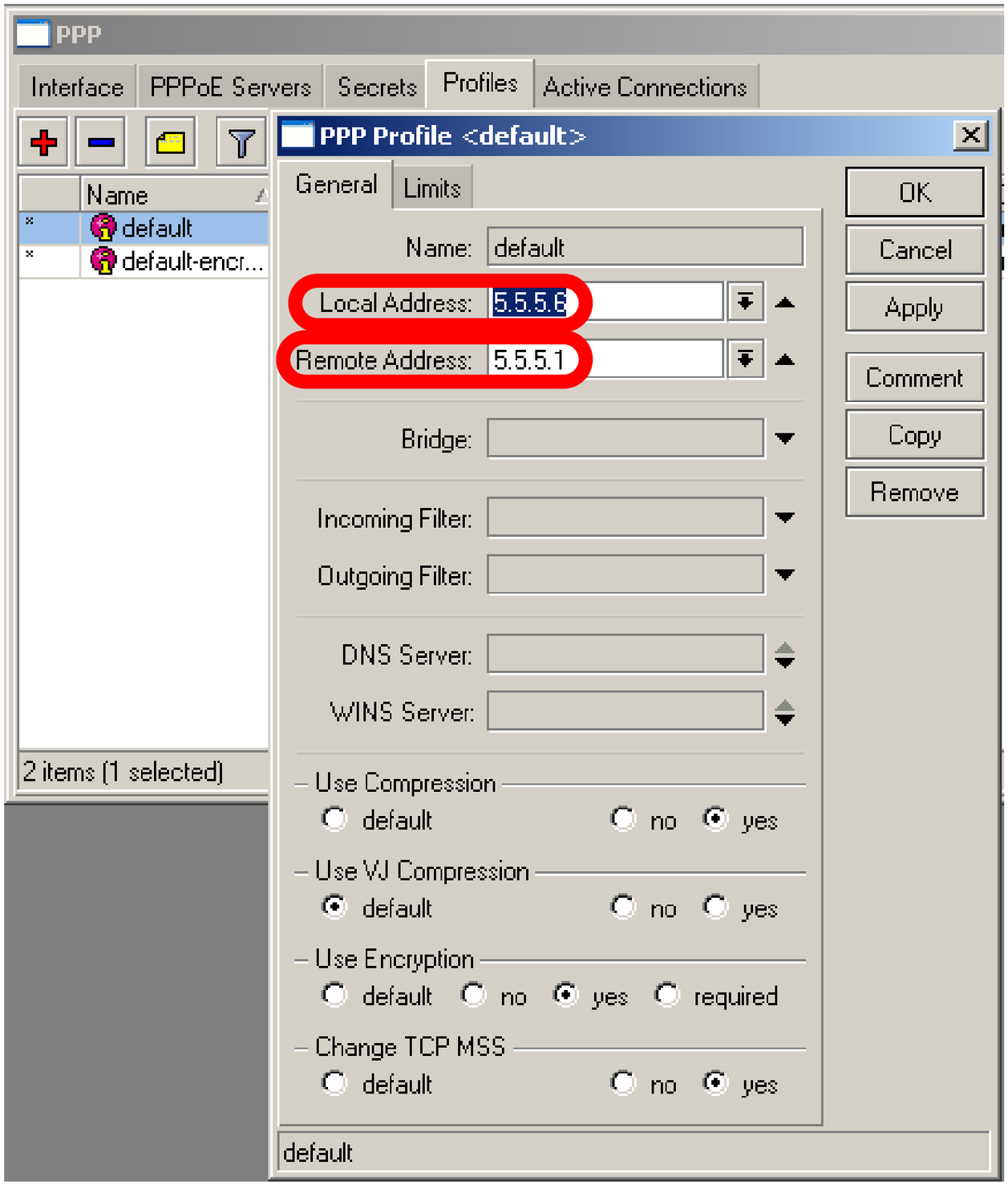


PPP Profiles

- 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



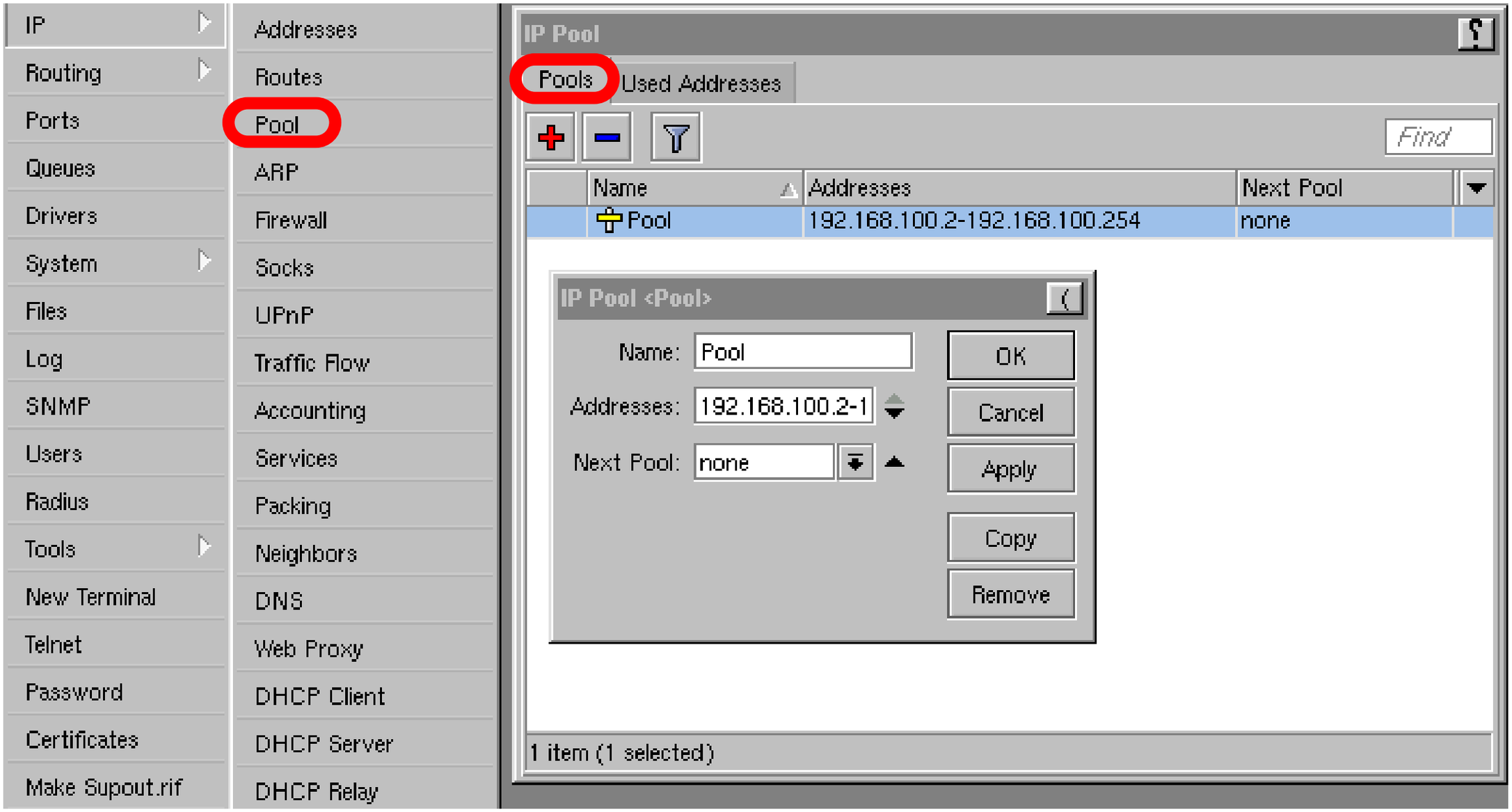
PPPoE

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

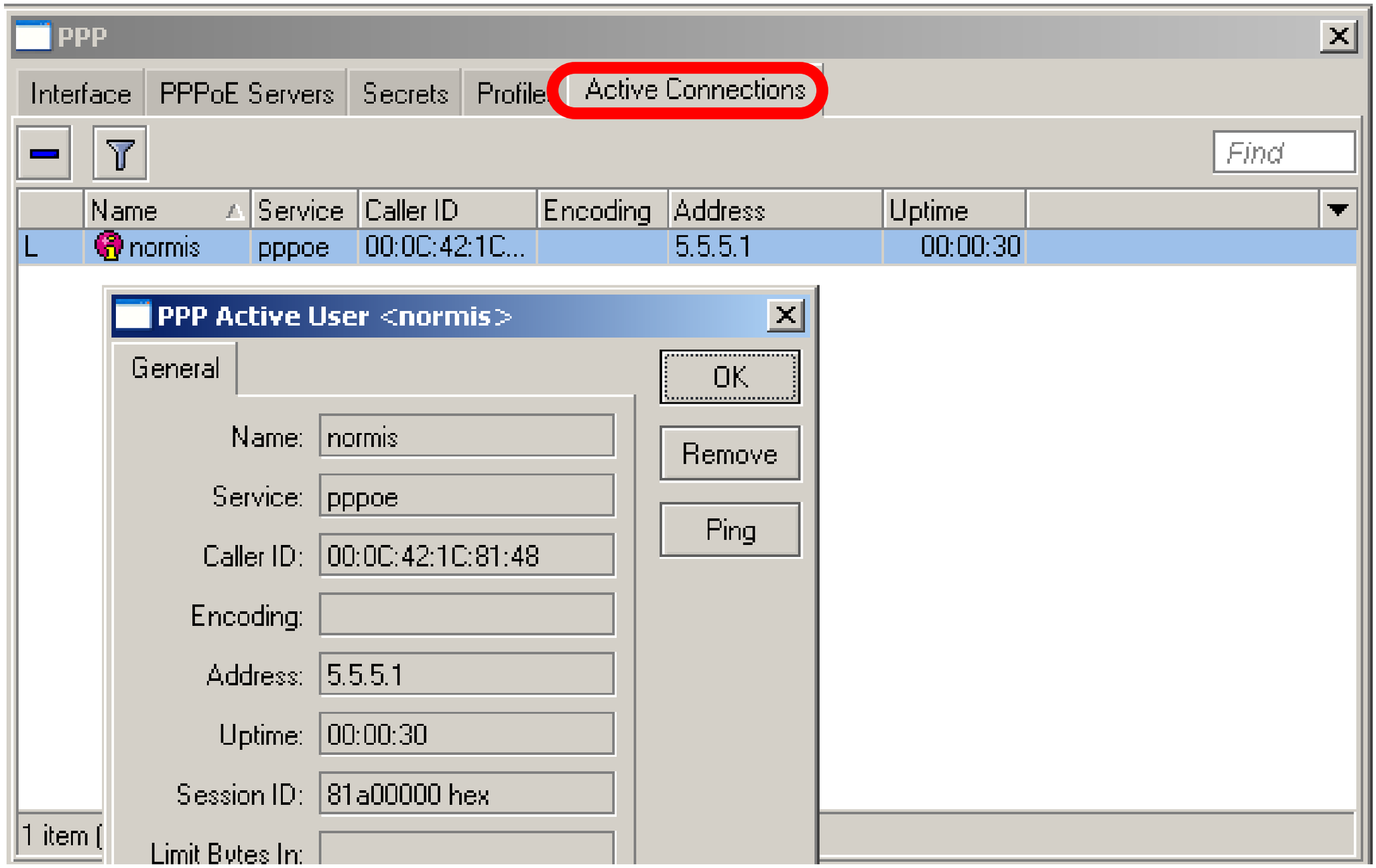
Pools

- 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


IP
Routing
Ports
Queues
Drivers
System
Files
Log
SNMP
Users
Radius
Tools
New Terminal
Telnet
Password
Certificates
Make Supout.rif
Addresses
Routes
Pool
ARP
Firewall
Socks
UPnP
Traffic Flow
Accounting
Services
Packing
Neighbors
DNS
Web Proxy
DHCP Client
DHCP Server
DHCP Relay
IP Pool
Pools
Used Addresses
Find
Name
Addresses
Next Pool
Pool
192.168.100.2-192.168.100.254
none
IP Pool <Pool>
Name:
Pool
Addresses:
192.168.100.2-1
Next Pool:
none
OK
Cancel
Apply
Copy
Remove
1 item (1 selected)

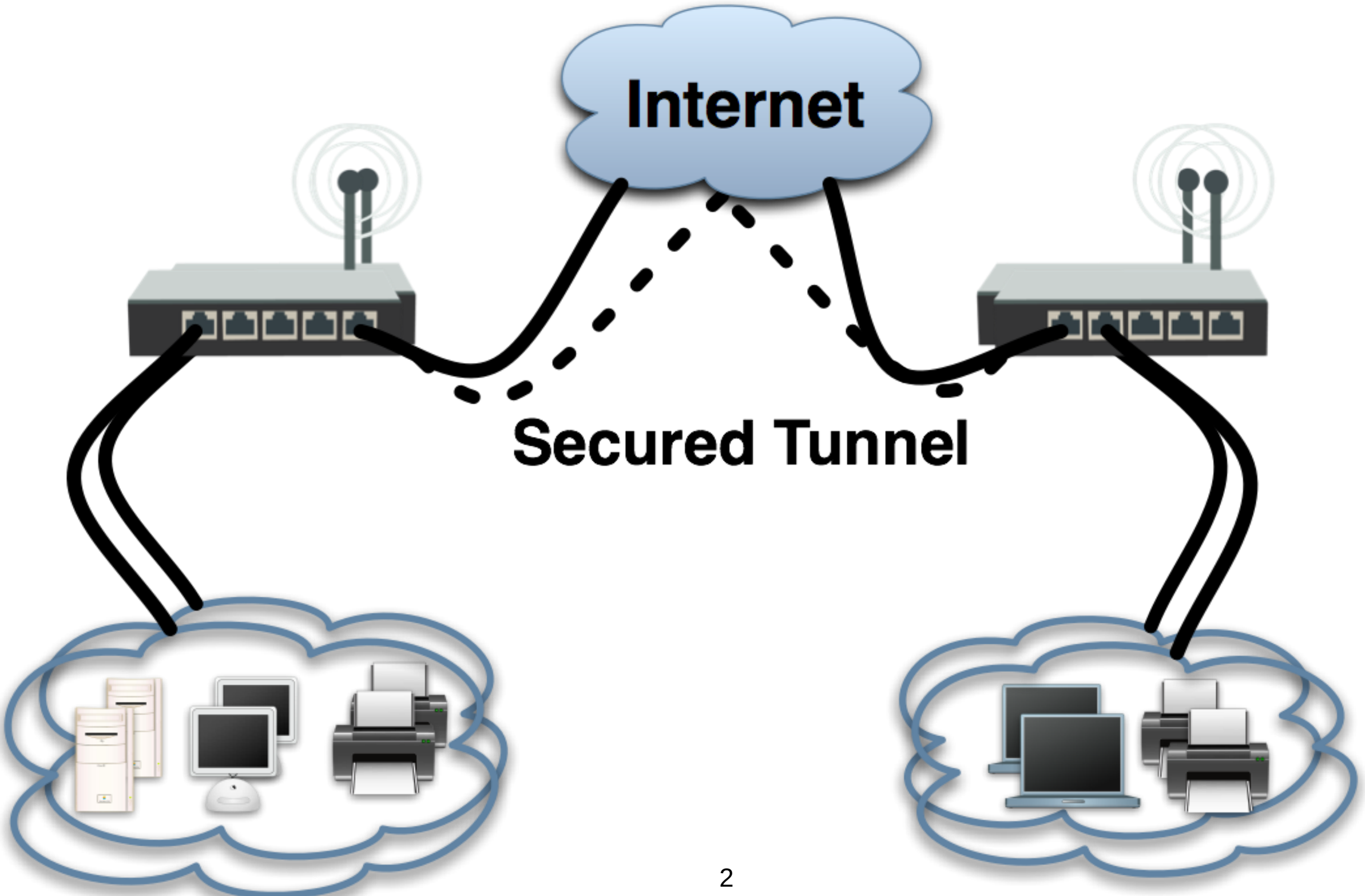
PPP Status


PPP
Interface
PPPoE Servers
Secrets
Profiles
Active Connections
Find
Name
Service
Caller ID
Encoding
Address
Uptime
normis
pppoe
00:0C:42:1C...
5.5.5.1
00:00:30
PPP Active User <normis>
General
OK
Remove
Ping
Name: normis
Service: pppoe
Caller ID: 00:0C:42:1C:81:48
Encoding:
Address: 5.5.5.1
Uptime: 00:00:30
Session ID: 81a00000 hex
Limit Bytes In:
1 item

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

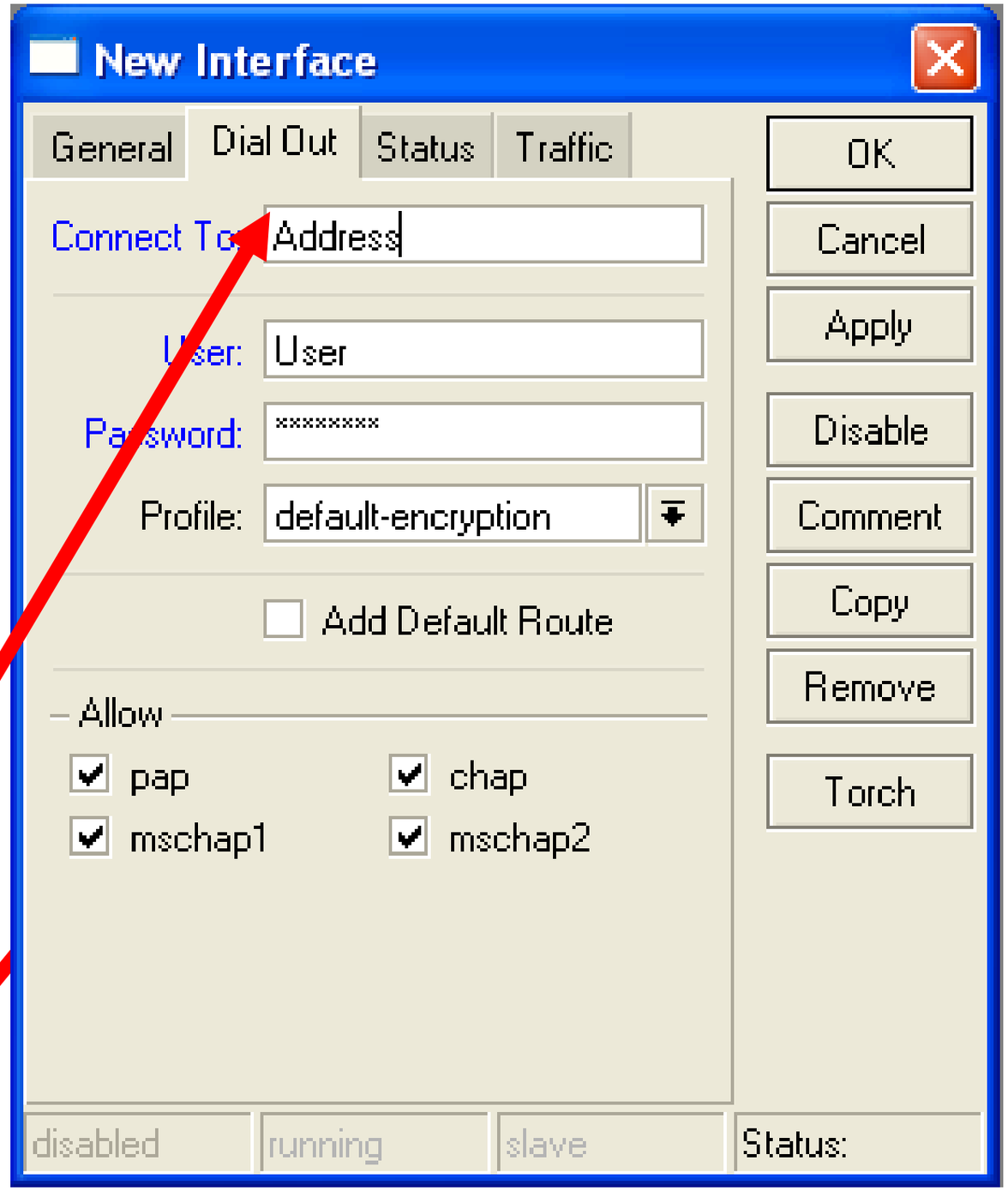


PPTP configuration

- 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

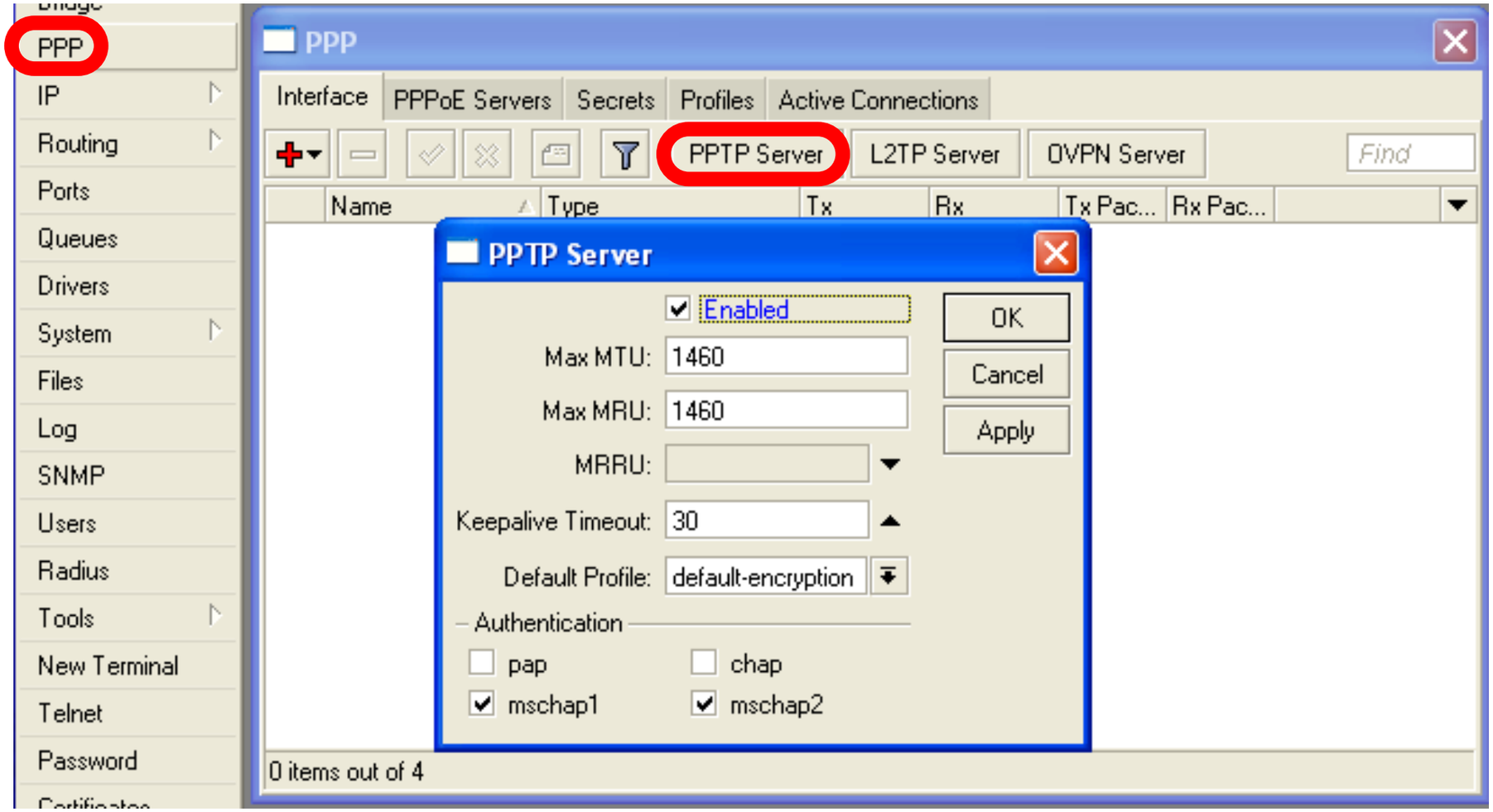


PPTP Client

- 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

LAB

PPTP Lab

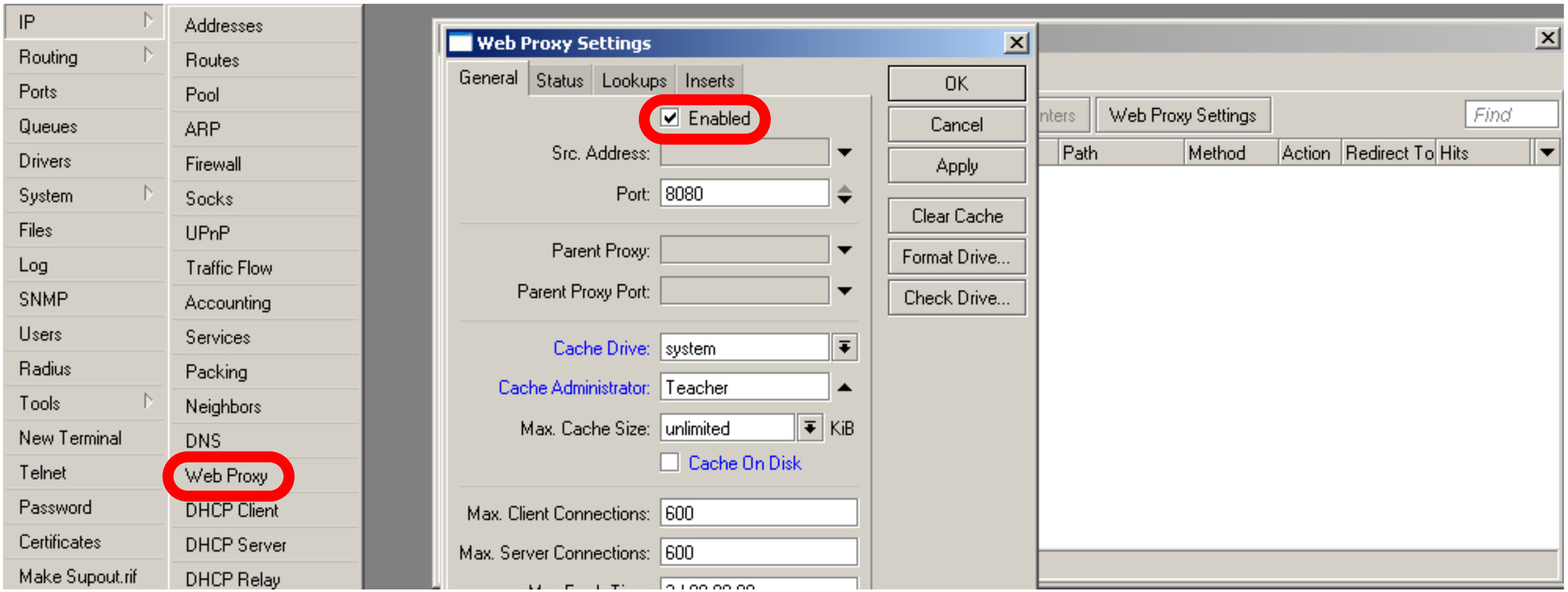
- Teachers are going to create PPTP server on Teacher's router
- Set up PPTP client on outgoing interface
- Use username **class** password **class**
- Disable PPTP interface

Proxy

What is Proxy

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

Enable Proxy



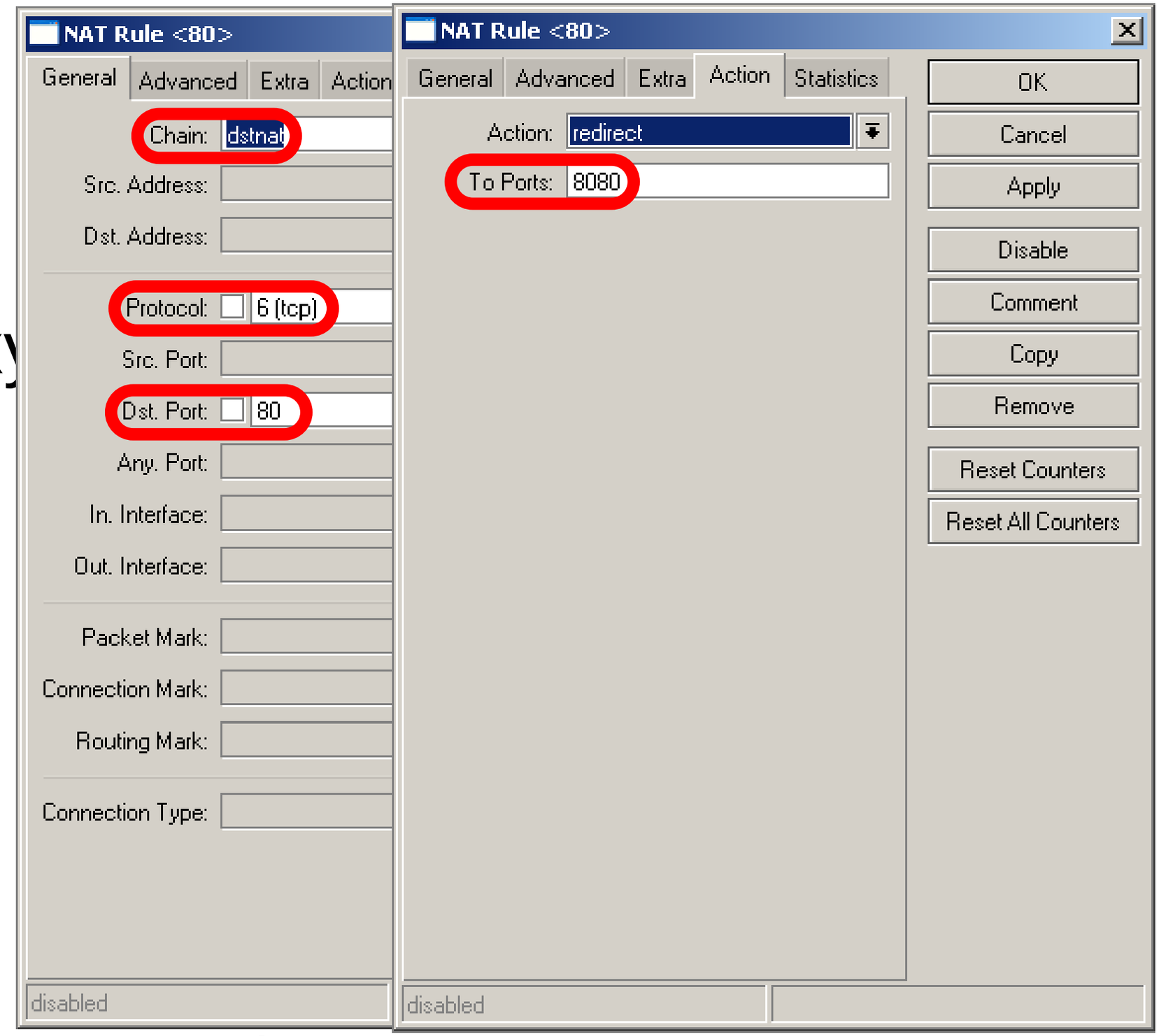
The main option is **Enable**, other settings are optional

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

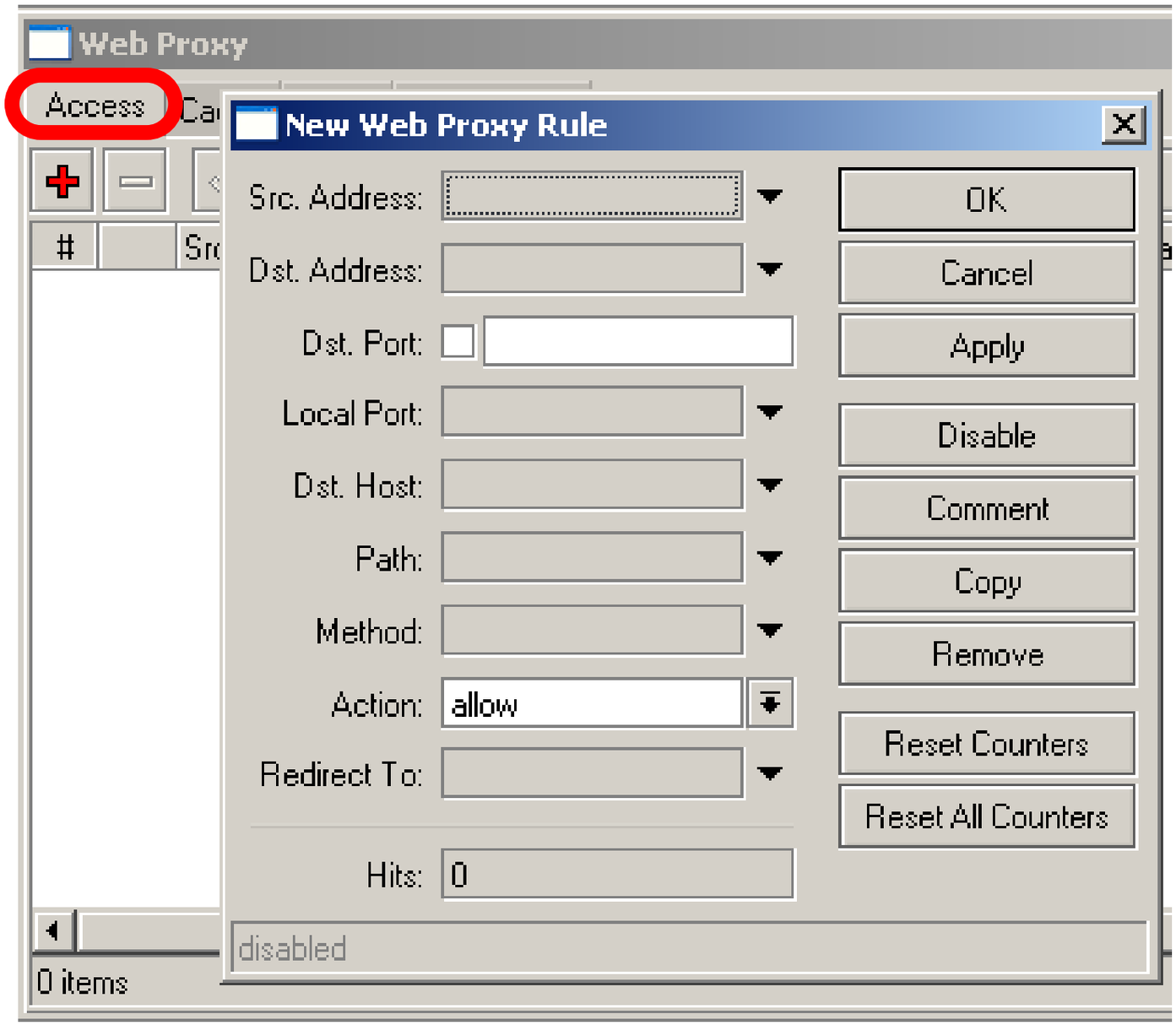


HTTP Firewall

- 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**



LAB

HTTP Firewall

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

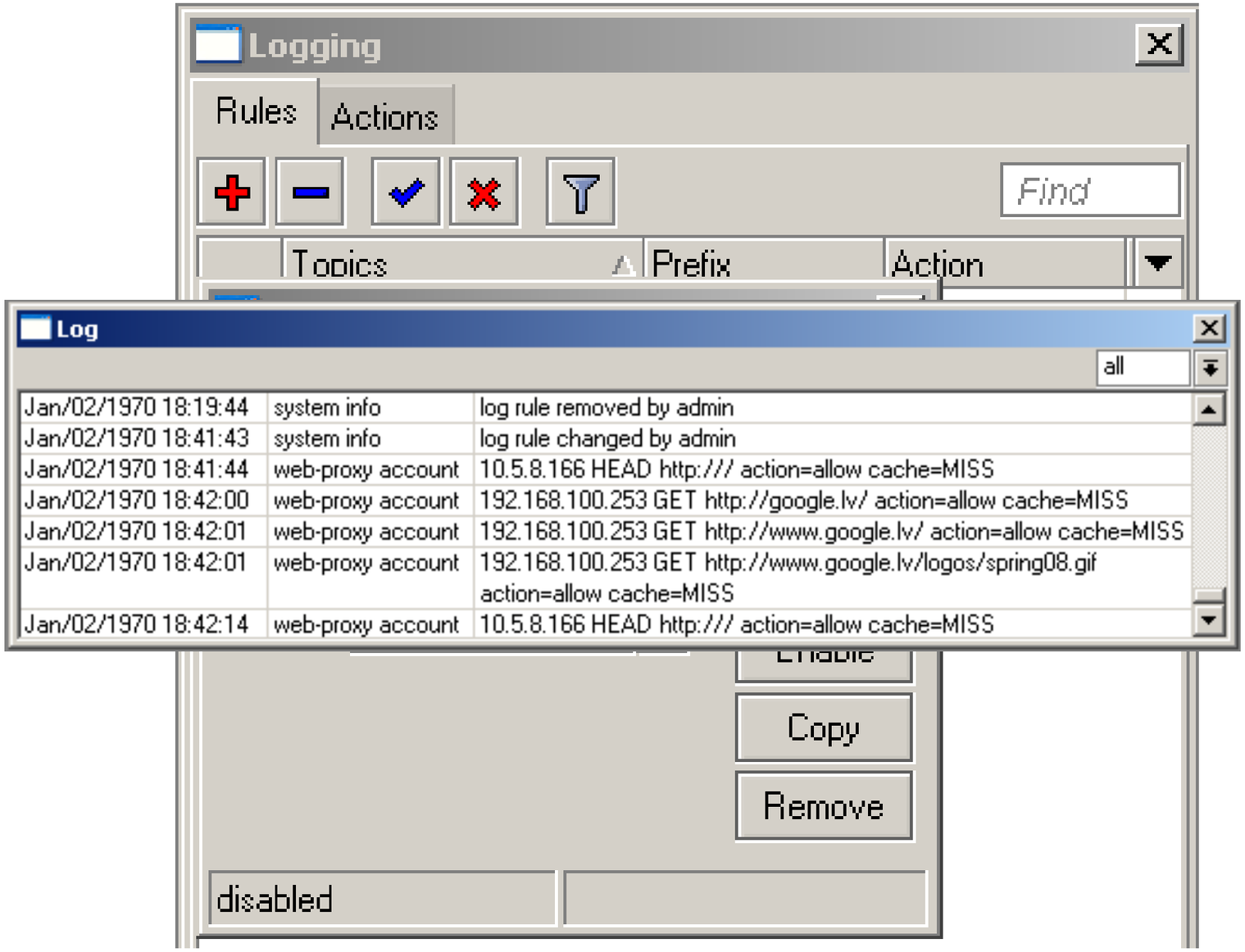
Web-page logging

- 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

LAB

- Add logging rule
- Check logs

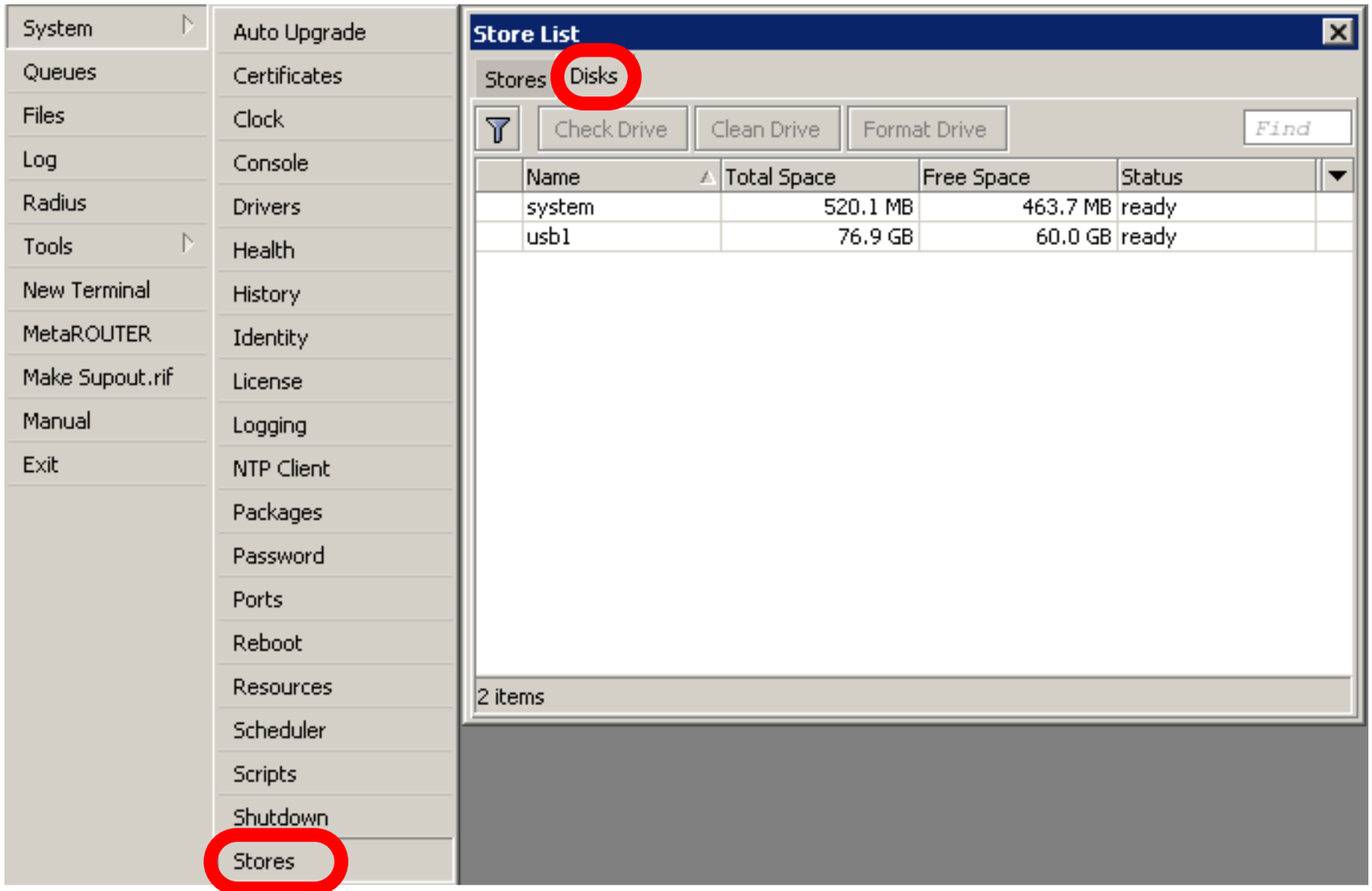


Cashing to External

- 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

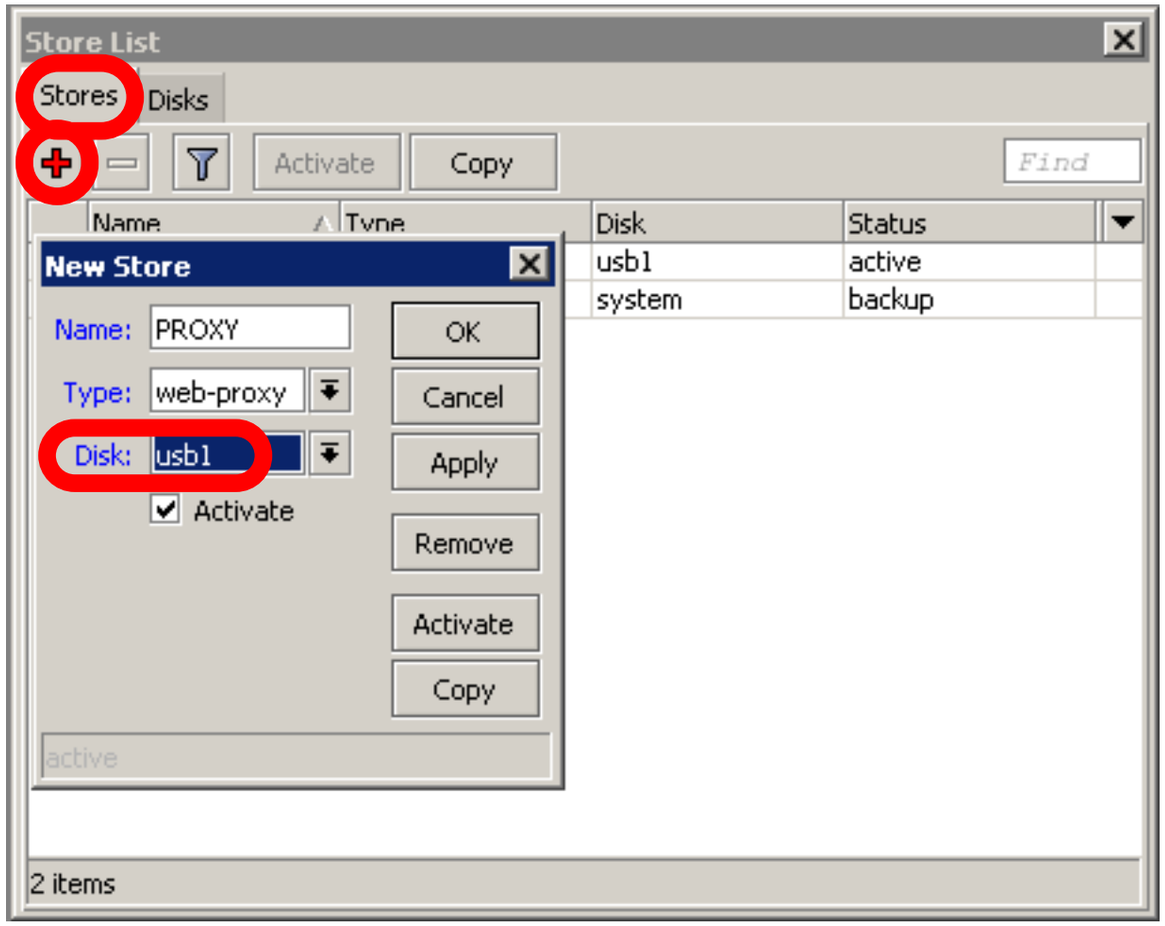
Store

- 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

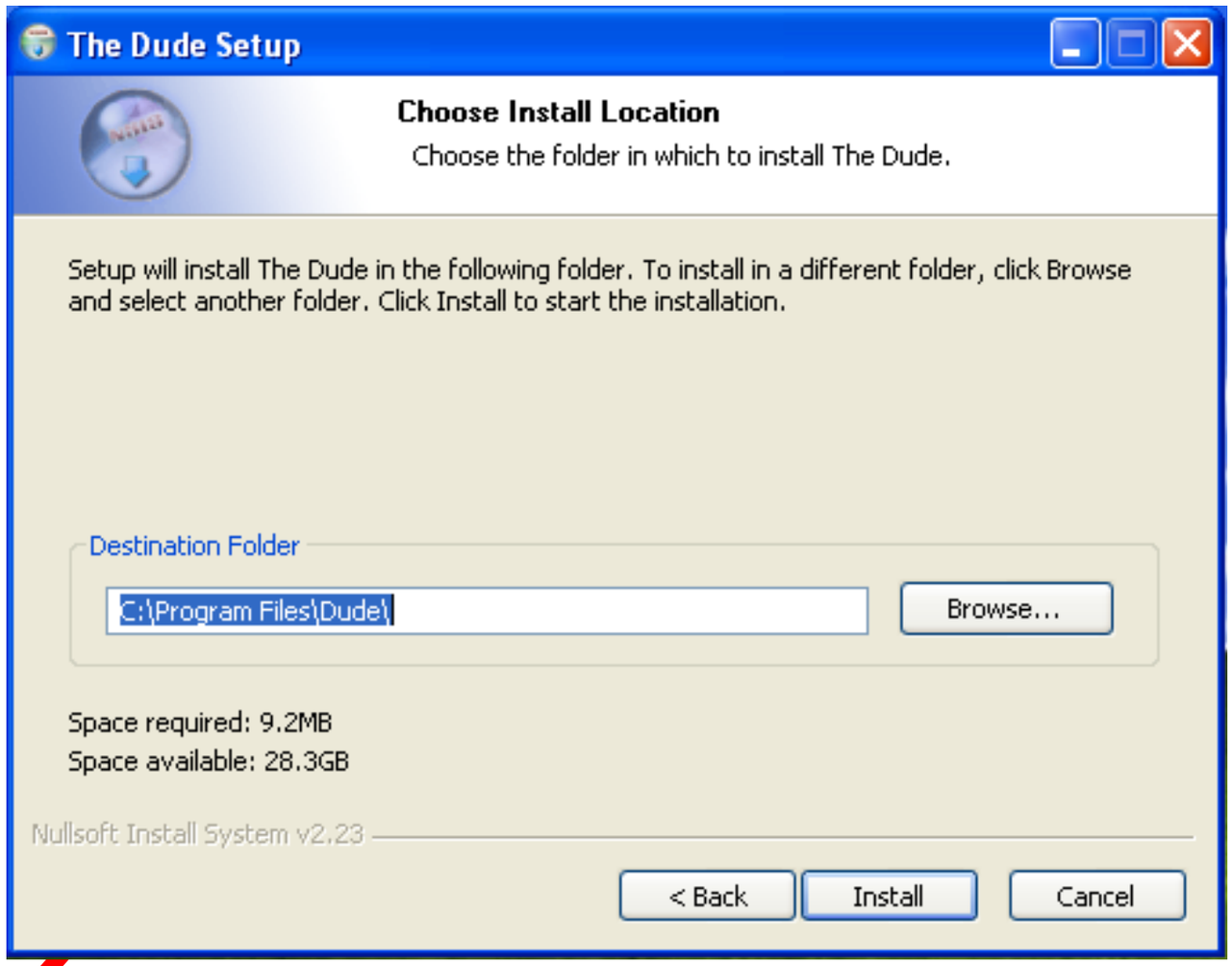
- Network monitor program
- Automatic discovery of devices
- Draw and Layout map of your networks
- Services monitor and alerts
- It is **Free**

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



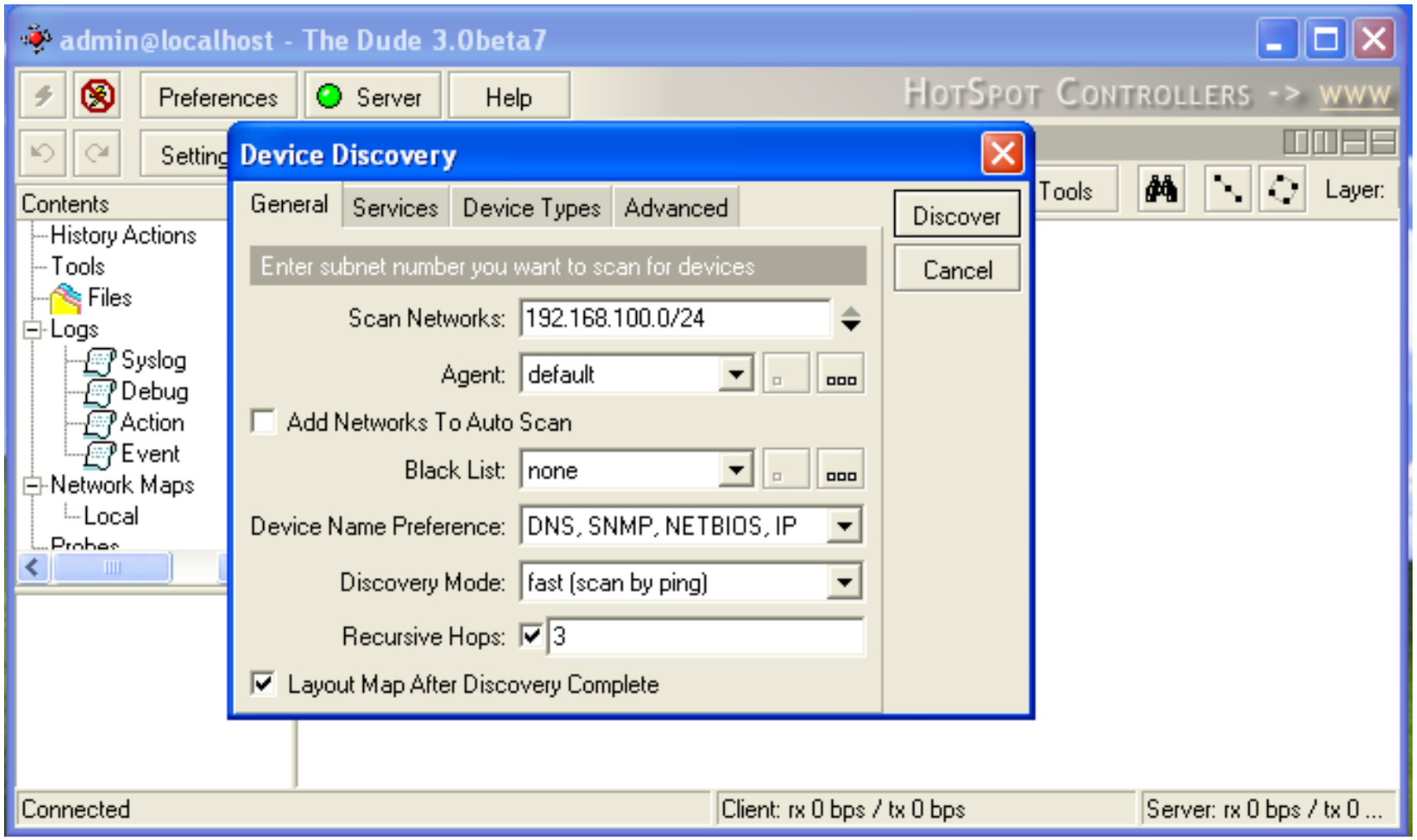
Install **Dude Server** on computer

Dude

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

Dude First Launch

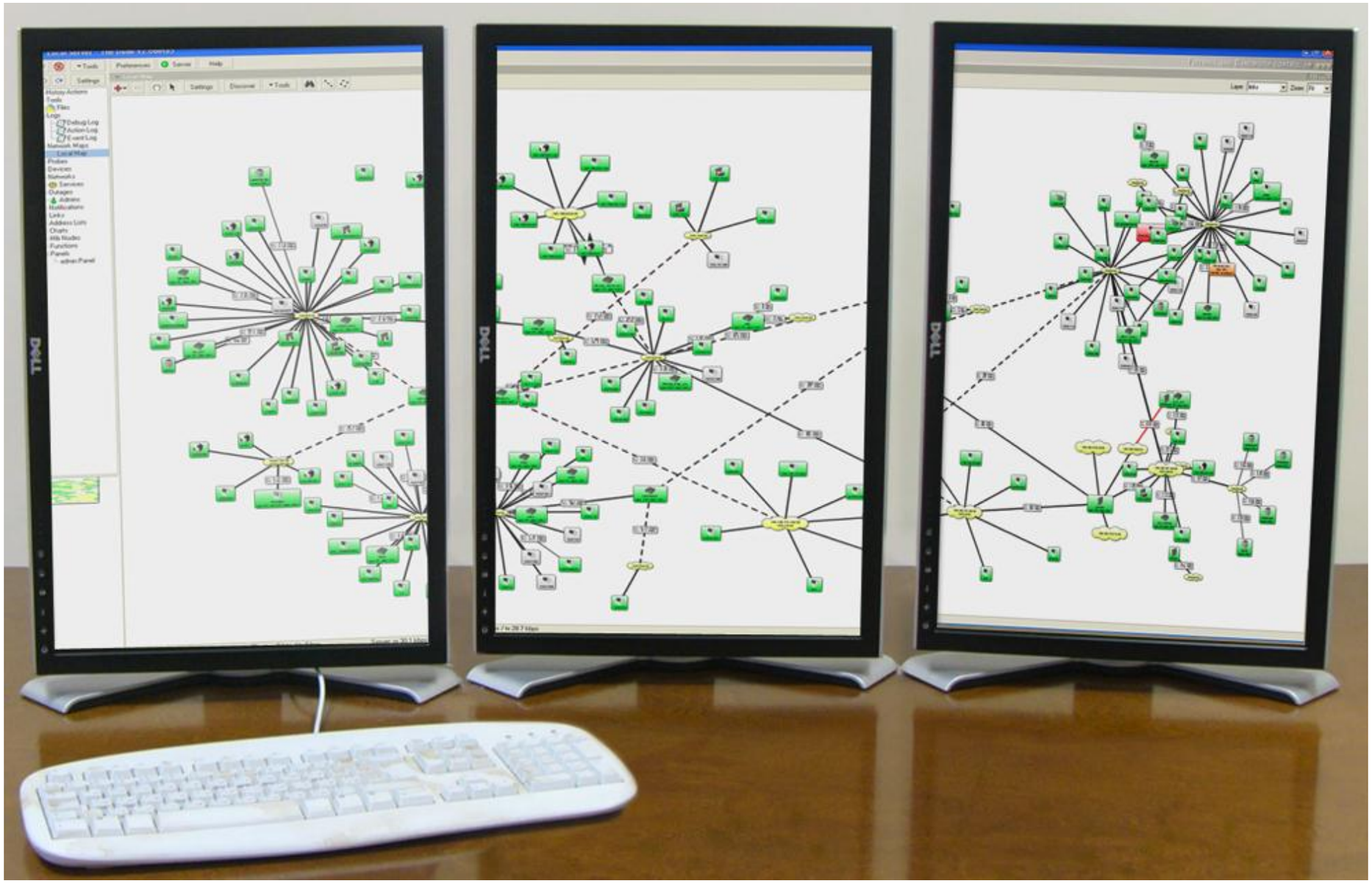
- Discover option is offered for the first launch
- You can discover local network



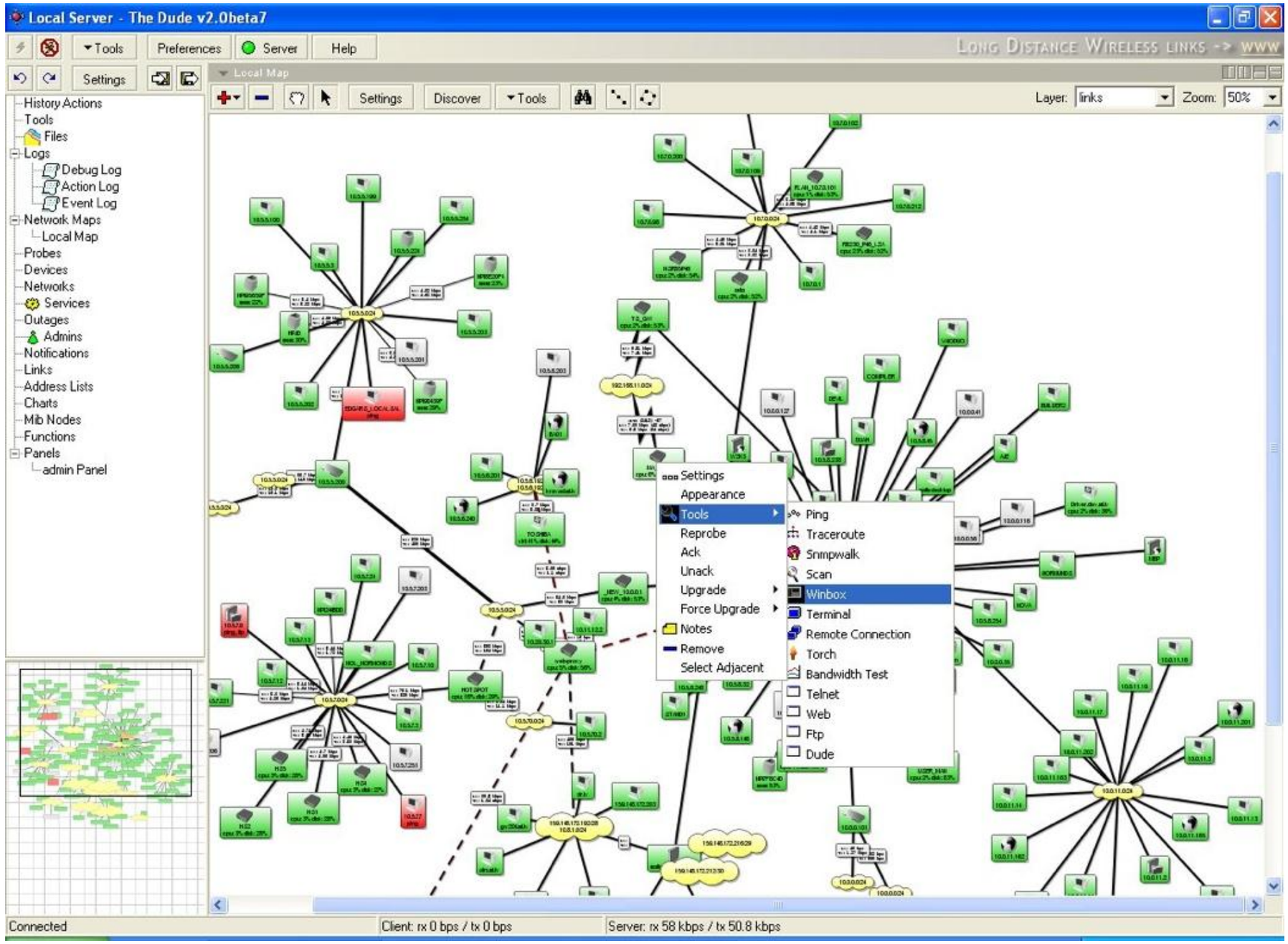
Dude Lab

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

Dude Usage



Dude Usage


Local Server - The Dude v2.0beta7
Tools
Preferences
Server
Help
Long Distance Wireless Links -> www
Settings
Local Map
Settings
Discover
Tools
Layer: links
Zoom: 50%
History Actions
Tools
Files
Logs
Debug Log
Action Log
Event Log
Network Maps
Local Map
Probes
Devices
Networks
Services
Outages
Admins
Notifications
Links
Address Lists
Charts
Mib Nodes
Functions
Panels
admin Panel
Settings
Appearance
Tools
Reprobe
Ack
Unack
Upgrade
Force Upgrade
Notes
Remove
Select Adjacent
Ping
Traceroute
Snmpwalk
Scan
Winbox
Terminal
Remote Connection
Torch
Bandwidth Test
Telnet
Web
Ftp
Dude
Connected
Client: rx 0 bps / tx 0 bps
Server: rx 58 kbps / tx 50.8 kbps

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