

MikroTik RouterOS Training Advanced Class

Routing

Simple Routing, ECMP, OSPF, Policy
Routing,

Simple Static Route

New Route

General | Attributes

Destination: 192.168.XY.0/24

Gateway: 192.168.Z.1

Interface:

Check Gateway:

Type: unicast

Distance:

Scope: 255

Target Scope: 10

Routing Mark:

Pref. Source:

OK
Cancel
Apply
Disable
Comment
Copy
Remove

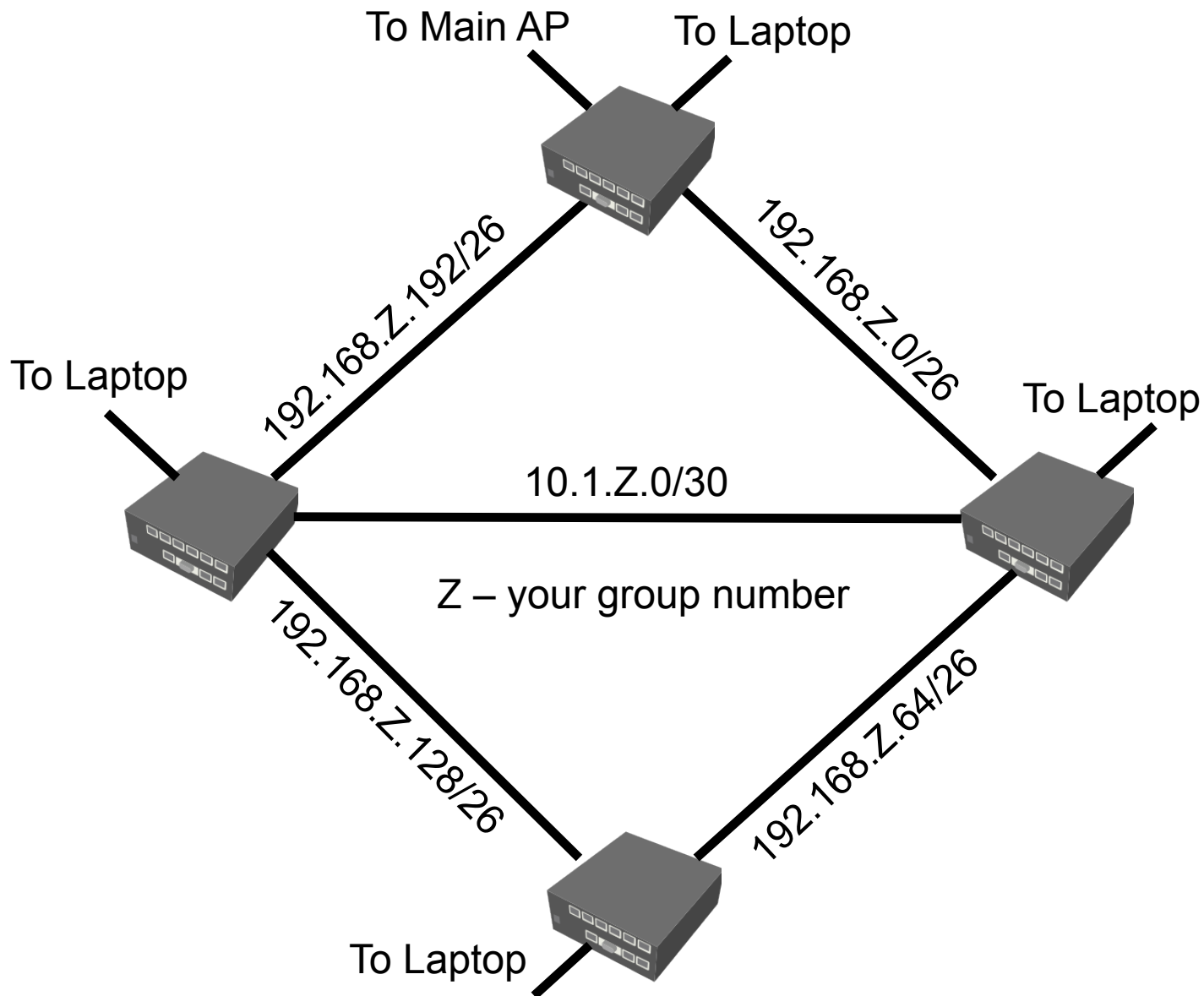
disabled active

- Only one gateway for a single network
- More specific routes in the routing table have higher priority than less specific
- Route with destination network 0.0.0.0/0 basically means “everything else”

Simple Routing Lab

- Ask teacher to join you in a group of 4 and assign specific group number “Z”
- Use any means necessary (cables, wireless) to create IP network structure from the **next slide**
- Remove any NAT (masquerade) rules from your routers
- By using simple static routes only ensure connectivity between laptops, and gain access to the internet.

IP Network Structure



ECMP Routes

The screenshot shows a 'New Route' dialog box with the following fields and values:

- Destination: 192.168.XY.0/24
- Gateway: 192.168.Z.1
- Gateway: 192.168.Z.127
- Gateway: 10.1.Z.2
- Interface: (empty)
- Check Gateway: (empty)
- Type: unicast
- Distance: (empty)
- Scope: 255
- Target Scope: 10
- Routing Mark: (empty)
- Pref. Source: (empty)

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

At the bottom: disabled (selected), active

- ECMP (Equal Cost Multi Path) routes have more than one gateway to the same remote network
- Gateways will be used in Round Robin per SRC/DST address combination

“Check-gateway” option

- It is possible to force router to check gateway reachability using ICMP (ping) or ARP protocols
- If gateway is unreachable in a simple route – the route will become inactive
- If one gateway is unreachable in an ECMP route, only the reachable gateways will be used in the Round Robin algorithm

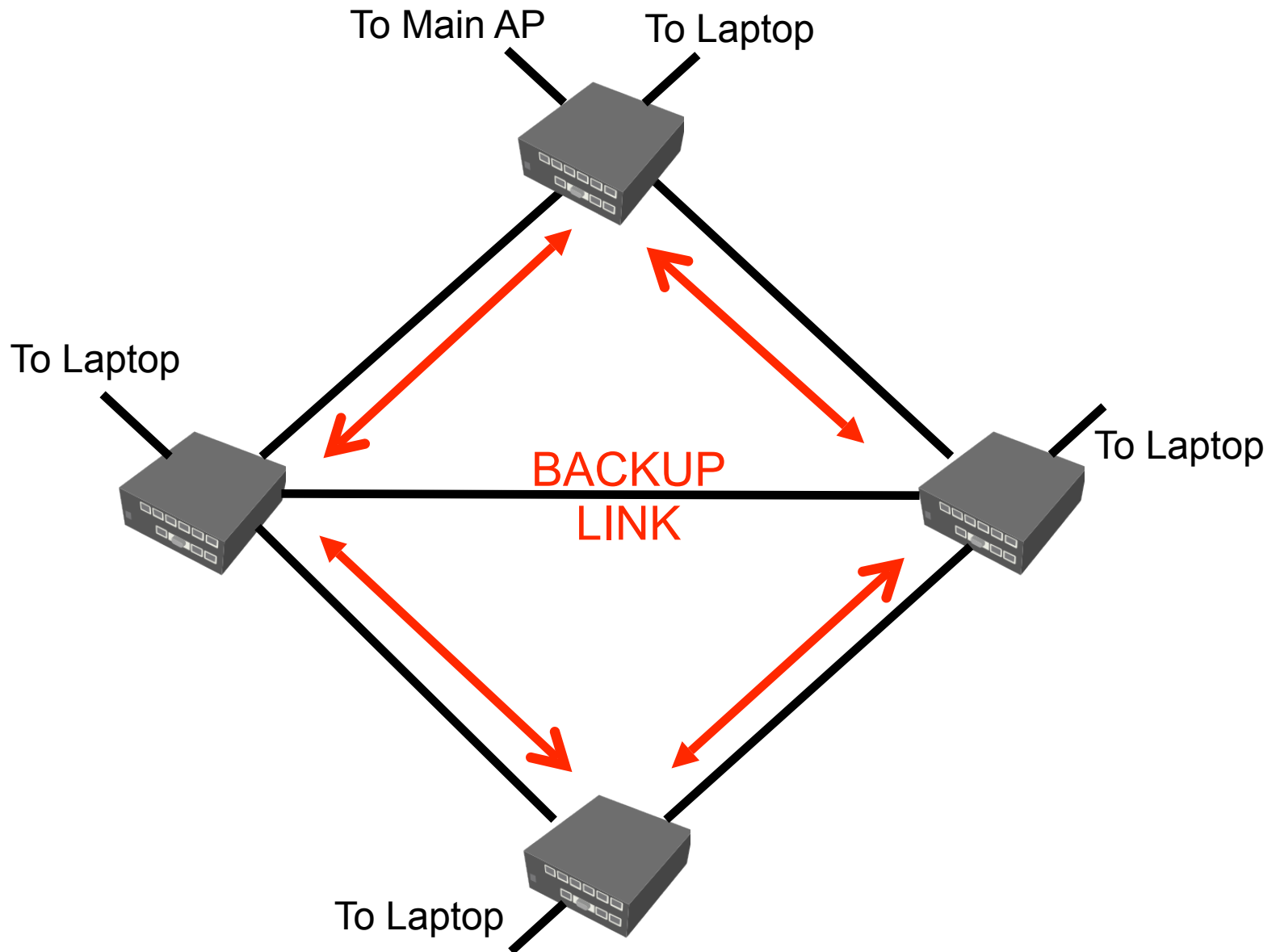
“Distance” option

- It is possible to prioritize one route over another if they both point to the same network using “distance” option.
- When forwarding a packet, the router will use the route with the lowest distance and reachable gateway

ECMP Routing Lab

- Remake your previously created routes, so that there are two gateways to each of the other participant's local networks 192.168.XY.0/24 and to the Internet
- Also ensure that “backup link” (next slide) will be used only when all other ways are not accessible

Advanced Routing



Open Shortest Path First (OSPF)

Areas, Costs, Virtual links,
Route Redistribution and Aggregation

OSPF Protocol

- Open Shortest Path First protocol uses a link-state and Dijkstra algorithm to build and calculate the shortest path to all known destination networks
- OSPF routers use IP protocol 89 for communication with each other
- OSPF distributes routing information between the routers belonging to a single autonomous system (AS)

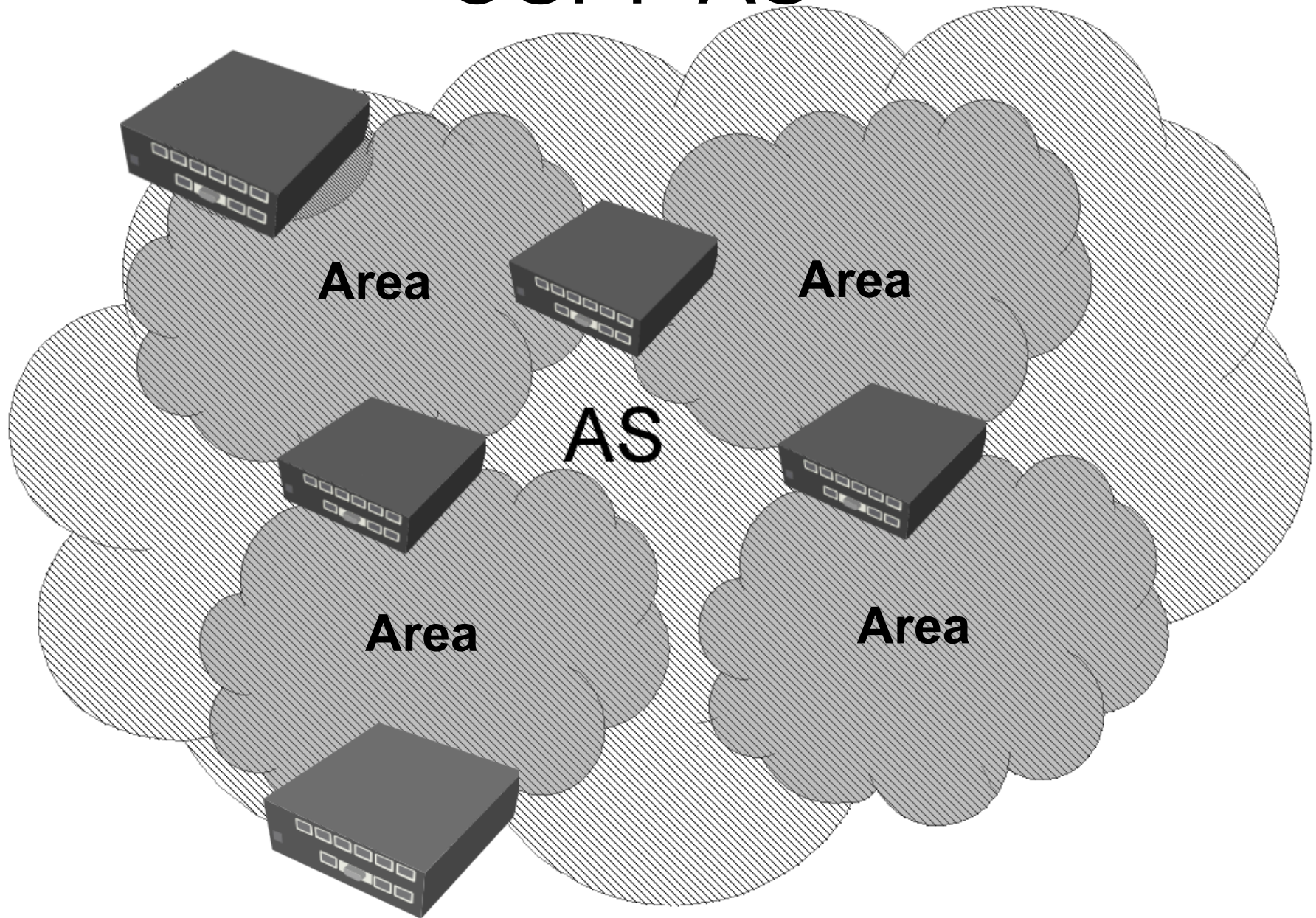
Autonomous System (AS)

- An autonomous system is a collection of IP networks and routers under the control of one entity (OSPF, iBGP ,RIP) that presents a common routing policy to rest of the network
- AS is identified by 16 bit number (0 - 65535)
 - ◆ Range from 1 to 64511 for use in the Internet
 - ◆ Range from 64512 to 65535 for private use

OSPF Areas

- OSPF allows collections of routers to be grouped together (<80 routers in one group)
- The structure of an area is invisible from the outside of the area.
- Each area runs a separate copy of the basic link-state routing algorithm
- OSPF areas are identified by 32-bit (4-byte) number (0.0.0.0 – 255.255.255.255)
- Area ID must be unique within the AS

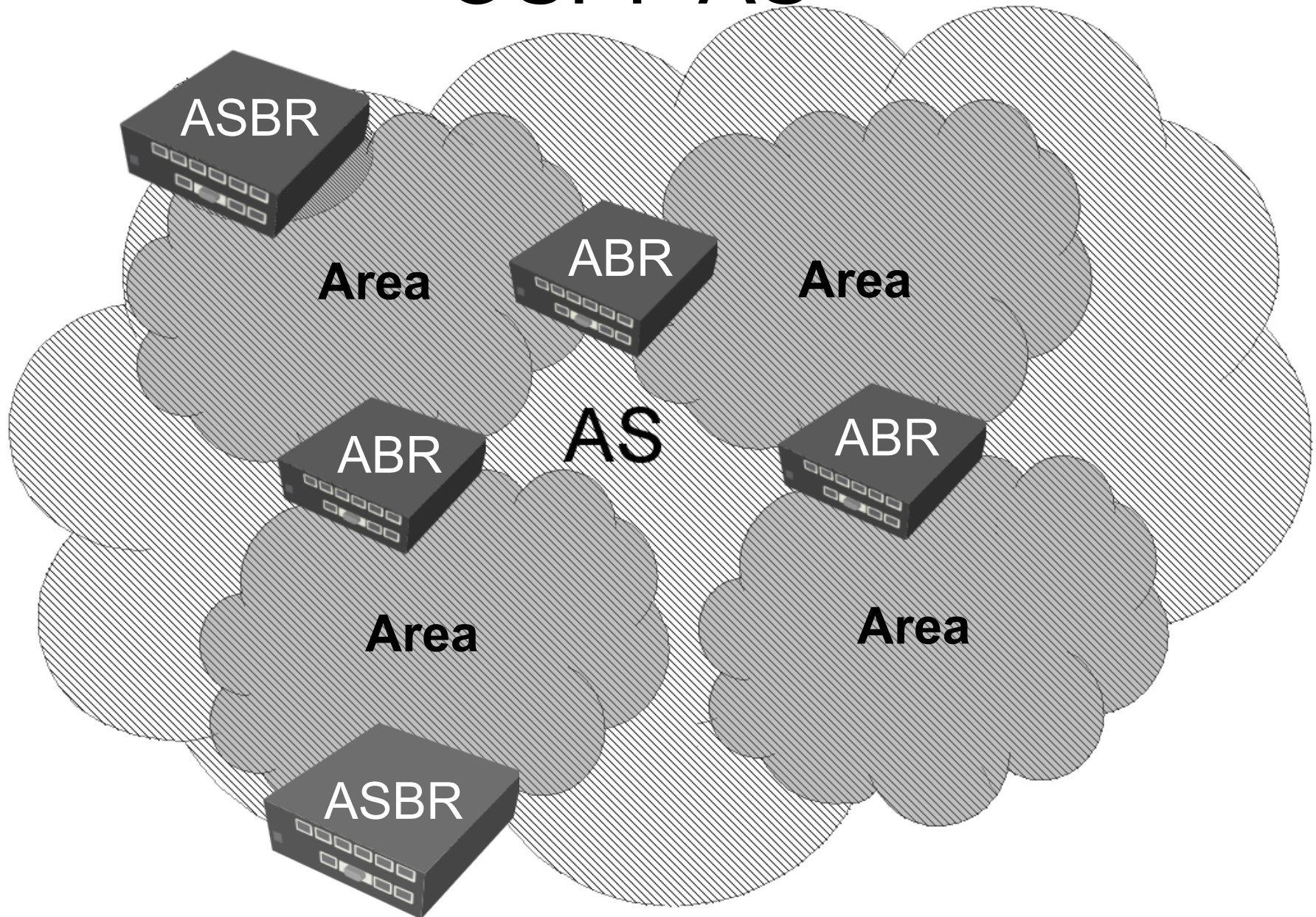
OSPF AS



Router Types

- Autonomous System Border Router (ASBR) - a router that is connected to more than one AS.
 - ◆ An ASBR is used to distribute routes received from other ASes throughout its own AS
- Area Border Router (ABR) - a router that is connected to more than one OSPF area.
 - ◆ An ABR keeps multiple copies of the link-state database in memory, one for each area
- Internal Router (IR) – a router that is connected only to one area

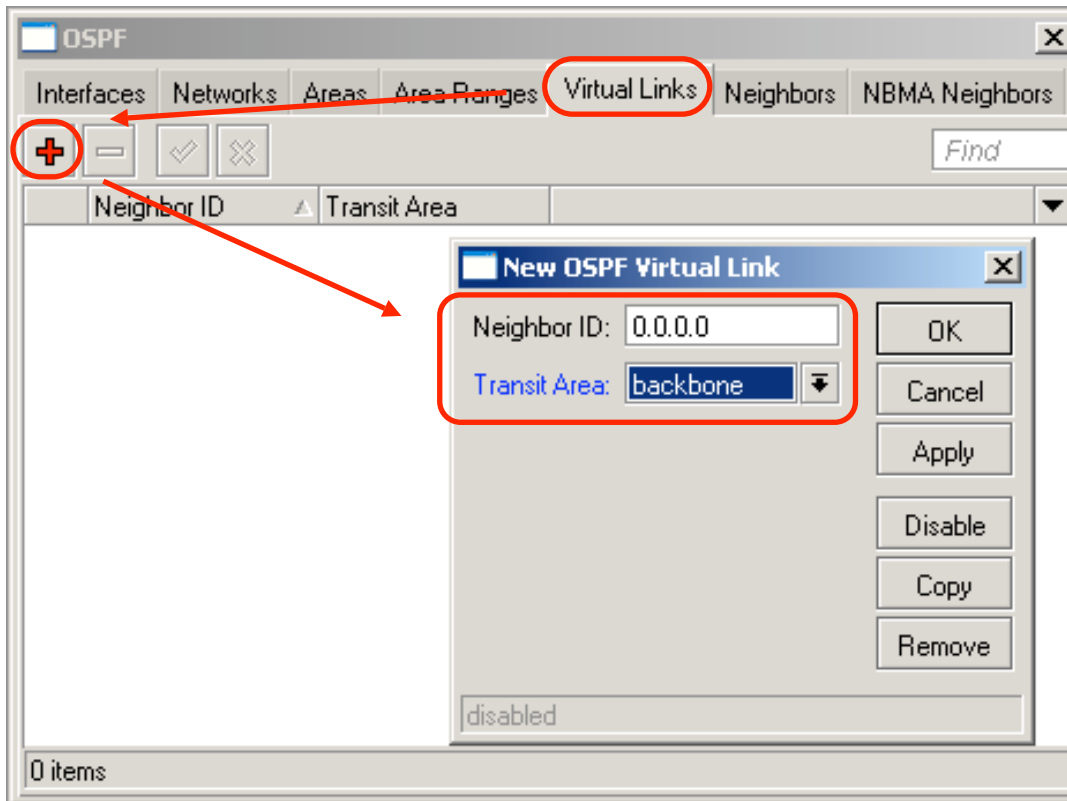
OSPF AS



Backbone Area

- The backbone area (area-id=0.0.0.0) forms the core of an OSPF network
- The backbone is responsible for distributing routing information between non-backbone areas
- Each non-backbone area must be connected to the backbone area (directly or using virtual links)

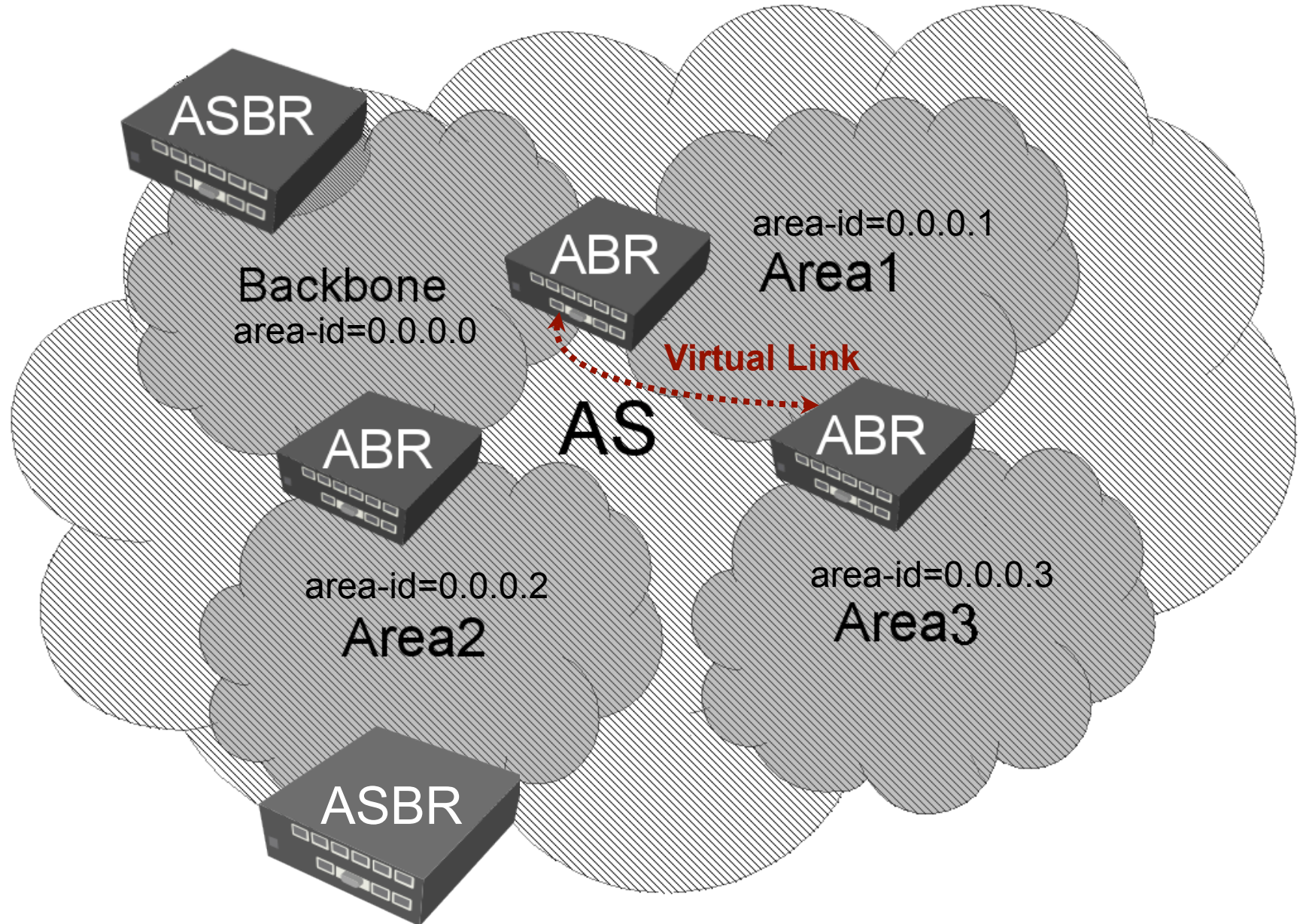
Virtual Links



- Used to connect remote areas to the backbone area through a non-backbone area

- Also Used to connect two parts of a partitioned backbone area through a non-backbone area

OSPF AS



OSPF Areas

The screenshot illustrates the configuration of OSPF areas in RouterOS WinBox. The left sidebar shows the 'RouterOS WinBox' menu with 'Routing' and 'OSPF' highlighted. The main window displays the OSPF configuration interface, where the 'Areas' tab is selected. A table lists the current OSPF areas:

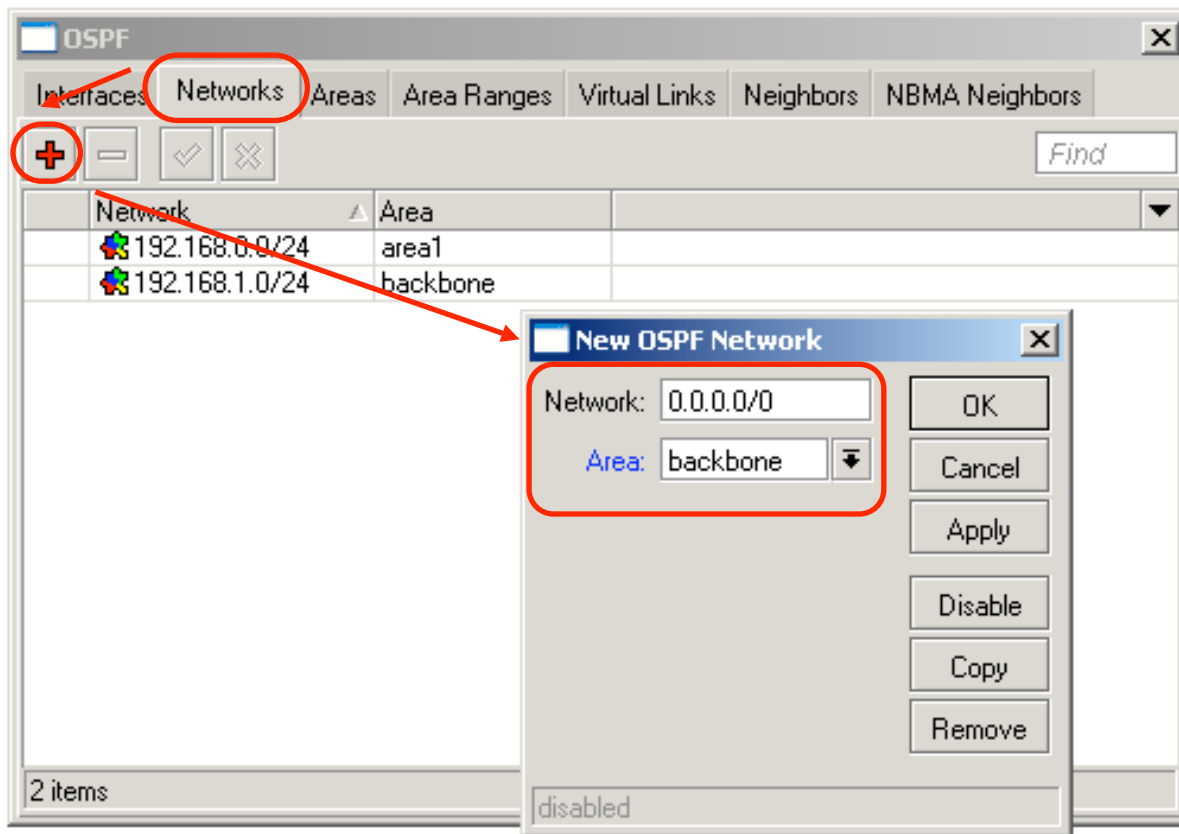
Area Name	Area ID	Type	Authentic...	Default C...	Interfac...	Active I...	Neighb...
backbone	0.0.0.0	default	none		0	0	0

A 'New OSPF Area' dialog box is open, showing the following configuration:

- Area Name: area1
- Area ID: 0.0.0.1
- Type: default
- Translator Role: translate never
- Authentication: none
- Inject Summary LSA
- Default Cost: 1
- Interfaces: 0
- Active Interfaces: 0
- Neighbors: 0
- Adjacent Neighbors: 0

The 'disabled' status is shown at the bottom of the dialog box.

OSPF Networks



- It is necessary to specify networks and associated areas where to look for other OSPF routers

- You should use exact networks from router interfaces (do not aggregate them)

OSPF Neighbour States

- **Full:** link state databases completely synchronized

- **2-Way:** bidirectional communication established

- Down, Attempt, Init, Loading, ExStart, Exchange: not completely running!

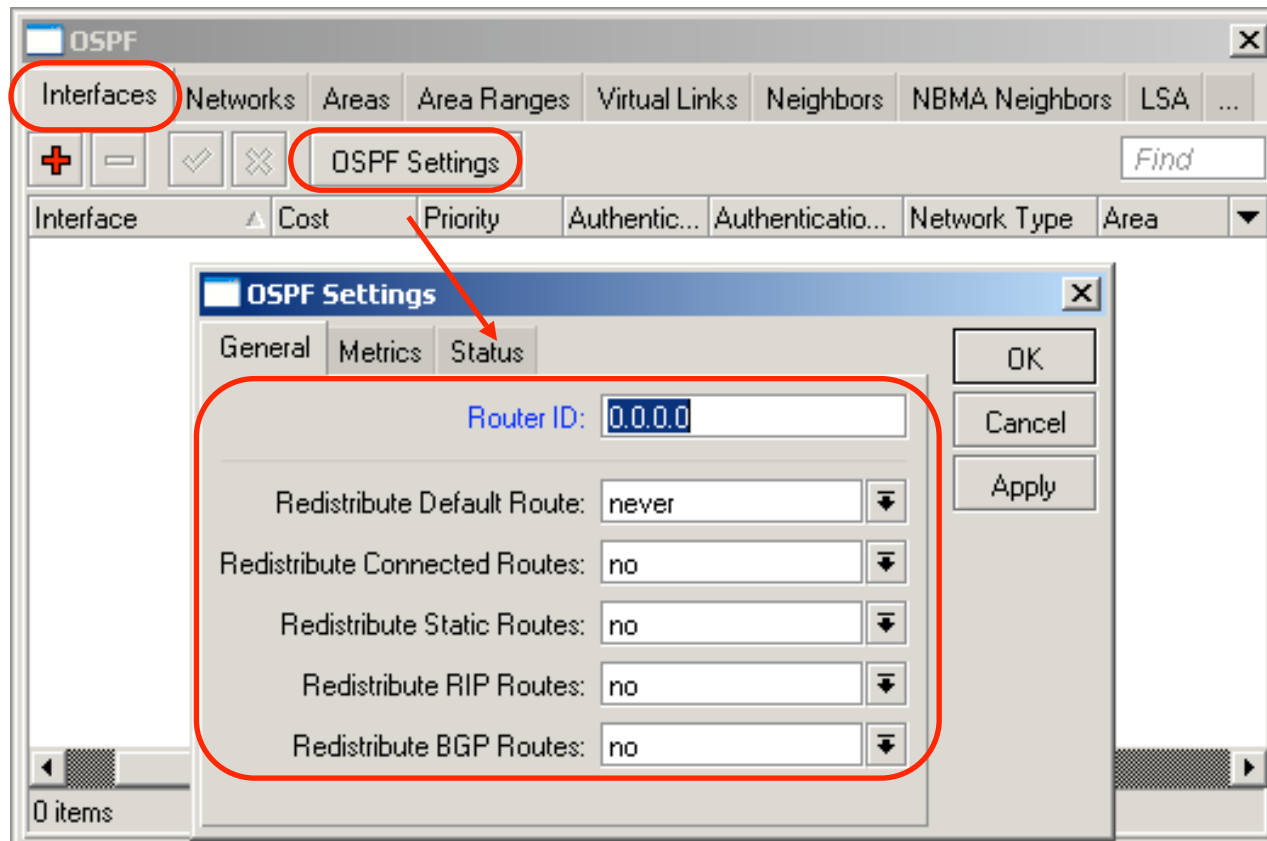
Router ID	Address	State	State Changes
0.0.0.1	170.0.4.1	Full	4
0.0.0.3	170.0.3.2	Full	4

OSPF Area Lab

- Create your own area
 - ◆ area name «Area<Z>»
 - ◆ area-id=0.0.0.<Z>
- Assign networks to the areas
- Check your OSPF neighbors

- Owner of the ABR should also configure backbone area and networks
- Main AP should be in ABR's OSPF neighbor list

OSPF Settings



● Router ID must be unique within the AS

- Router ID can be left as 0.0.0.0 then largest IP address assigned to the router will be used

What to Redistribute?

- Default route is not considered as static route

Route List

Routes Rules

Find all

	Destination	Gateway	Distance	Routing Mark	Pref. Source	Interface
1	AS 0.0.0.0/0	10.5.8.1	1			ether3
	AS 5.0.0.0/24	10.1.101.219	1			bridge1
	DAB 6.6.6.0/30	10.1.101.239	20			bridge1
	DAC 10.1.101.0/24		0		10.1.101.1	bridge1
	DB 10.1.101.0/24	10.1.101.239	20			bridge1
	DAC 10.5.8.0/24		0		10.5.8.120	ether3
3	AS 10.0.0.133	10.5.8.1	0		10.9.9.9	ipip1
	DAB 10.1.3.0/24	10.1.101.239	20			bridge1
	DAB 10.1.24.0/24	10.1.101.239	20			bridge1
	DAB 10.15.1.0/24	10.1.101.239	200			bridge1
	DAR 172.16.1.0/30	10.1.101.245	120			bridge1
4	DAR 172.16.1.4/30	10.1.101.245	120			bridge1
	DAR 172.16.1.8/30	10.1.101.245	120			bridge1
	DAR 172.16.2.0/30	10.1.101.245	120			bridge1

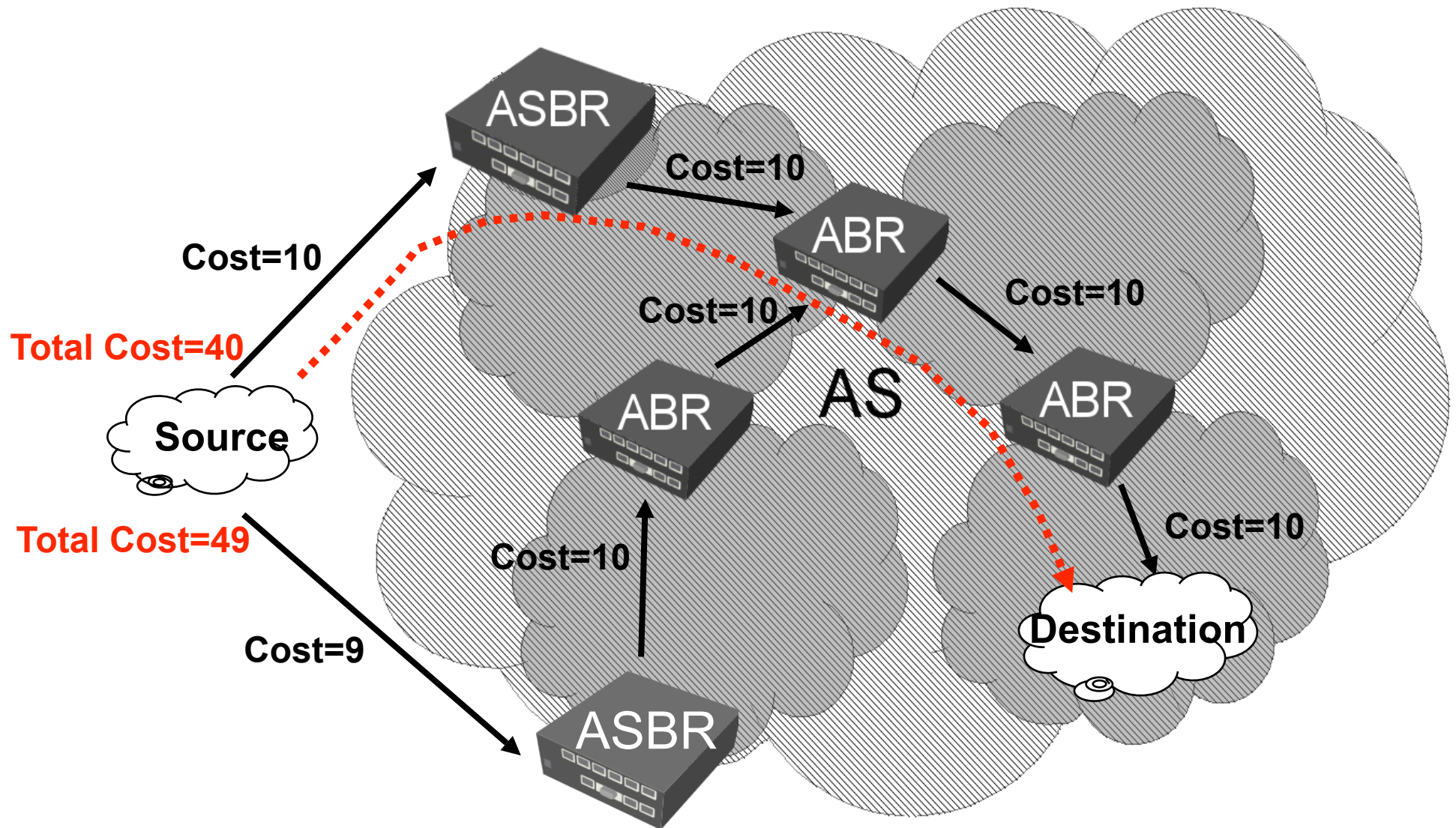
38 items

Annotations: 1 points to the first row. 2 points to the Gateway column. 3 points to the AS 10.0.0.133 row. 4 points to the DAR rows. 5 points to the Gateway column for the DAB 10.1.24.0/24 row.

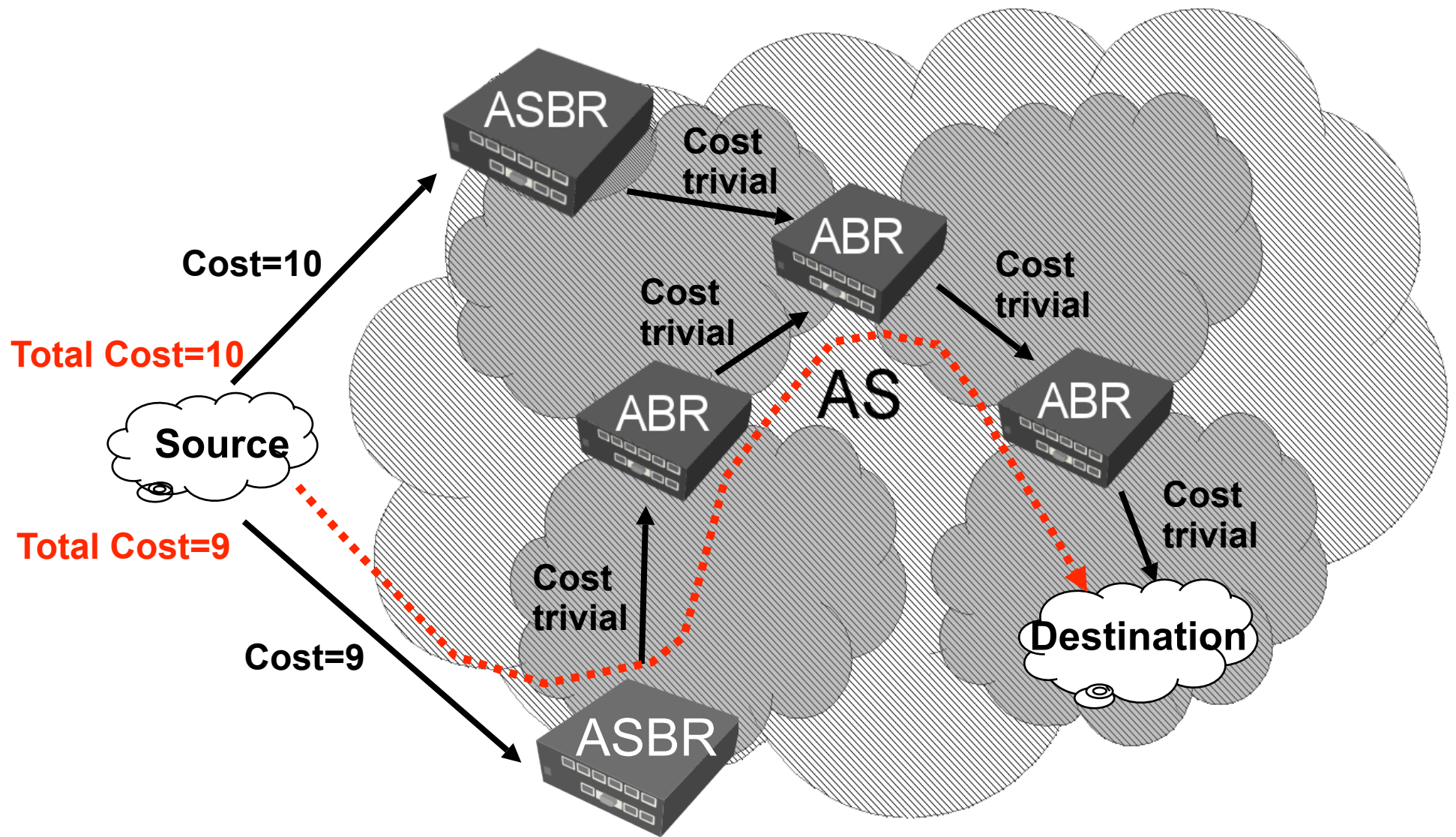
Redistribution Settings

- **if-installed** - send the default route only if it has been installed (static, DHCP, PPP, etc.)
- **always** - always send the default route
- **as-type-1** – remote routing decision to this network will be made based on the sum of the external and internal metrics
- **as-type-2** – remote routing decision to this network will be made based only on external metrics (internal metrics will become trivial)

External Type 1 Metrics



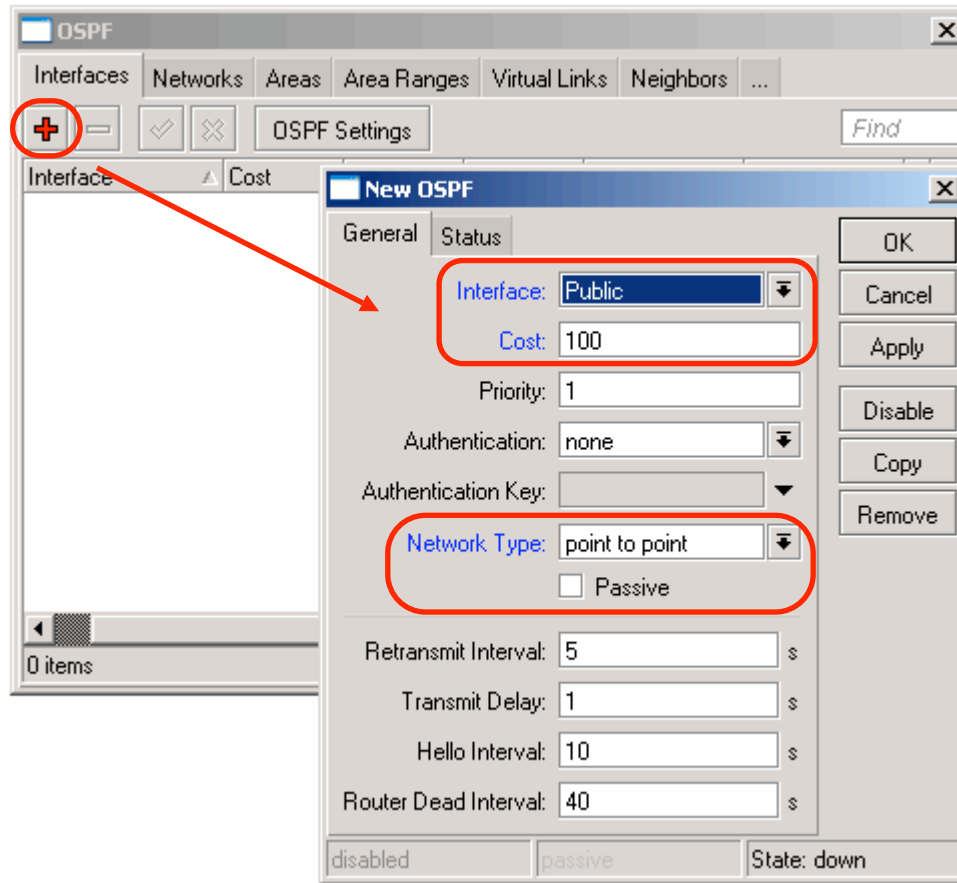
External Type 2 Metrics



Redistribution Lab

- Enable type 1 redistribution for all connected routes
- Take a look at the routing table
- Add one static route to 172.16.XY.0/24 network
- Enable type 1 redistribution for all static routes
- Take a look at the routing table

Interface Cost



- All interfaces have default cost of 10
- To override default setting you should add new entry in interface menu

- Choose correct network type for the interface

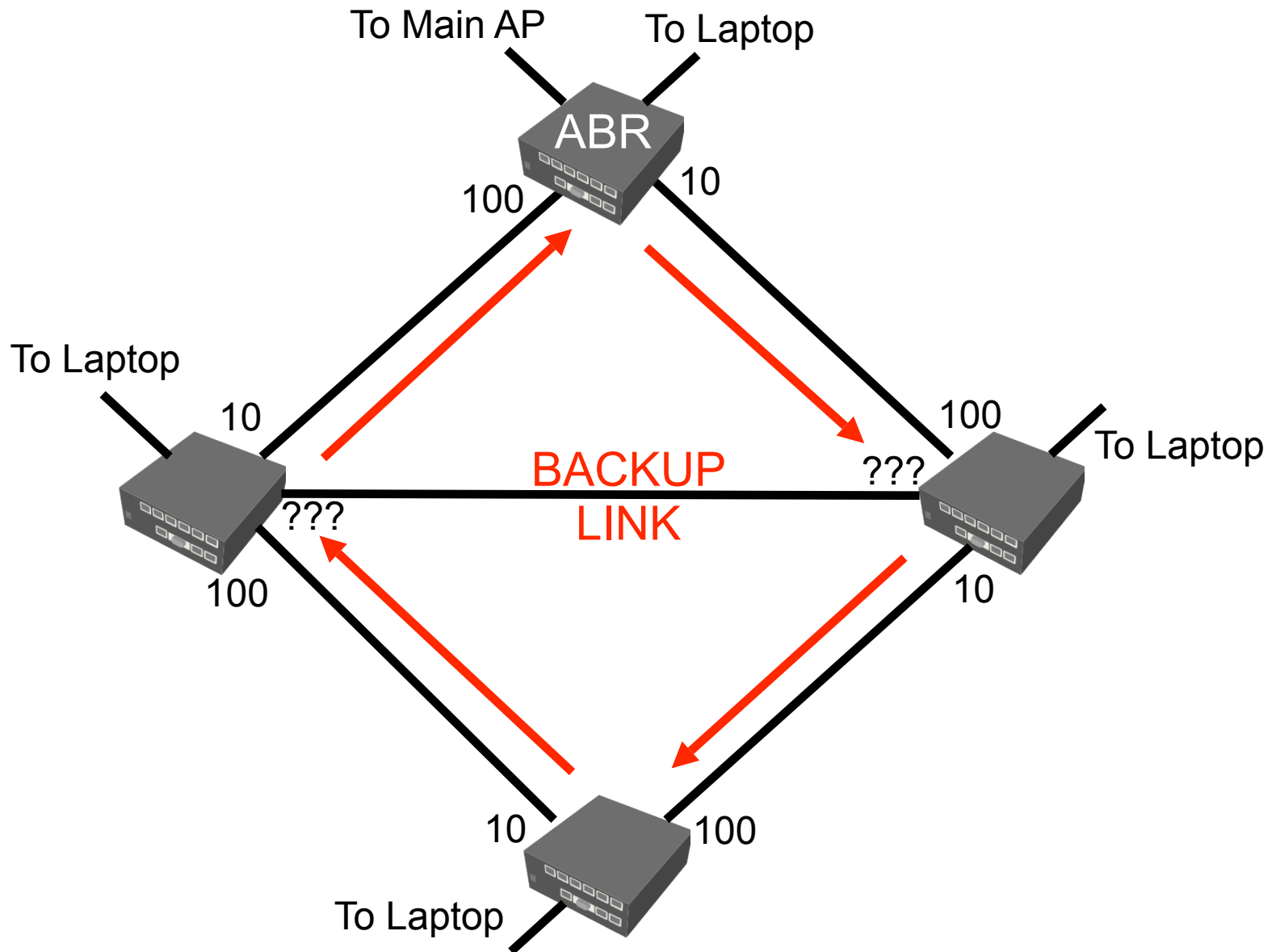
Designated Routers

- To reduce OSPF traffic in NBMA and broadcast networks, a single source for routing updates was introduced - Designated Router (DR)
- DR maintains a complete topology table of the network and sends the updates to the others
- Router with the highest priority (previous slide) will be elected as DR
- Router with next priority will be elected as Backup DR (BDR)
- Router with priority 0 will never be DR or BDR

OSPF Interface Lab

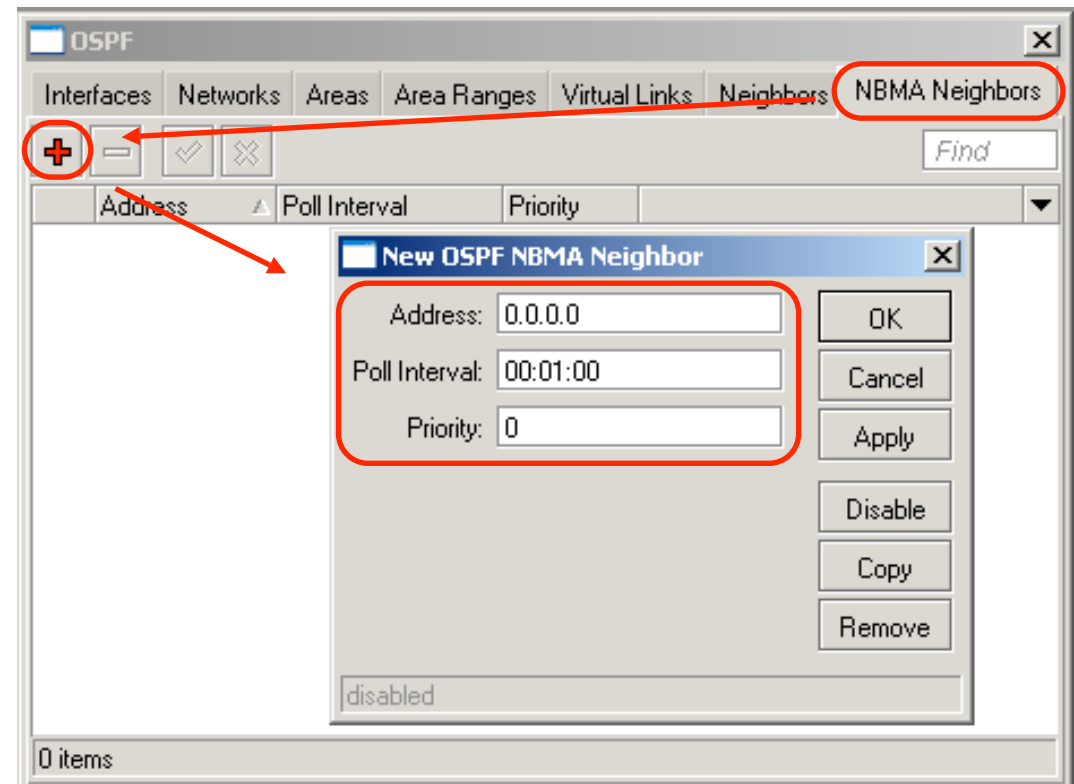
- Choose correct network type for all OSPF interfaces
- Assign costs (next slide) to ensure one way traffic in the area
- Check your routing table for ECMP routes
- Assign necessary costs so backup link will be used only when some other link fails
- Check OSPF network redundancy!
- Ensure ABR to be DR your area, but not in backbone area

Costs



NBMA Neighbors

- For non-broadcast networks it is necessary to specify neighbors manually



- The priority determines the neighbor chance to be elected as a Designated router

Stub Area

The screenshot shows a 'New OSPF Area' dialog box with the following configuration:

- Area Name: area1
- Area ID: 0.0.0.0
- Type: stub
- Translator Role: translate never
- Authentication: none
- Inject Summary LSA (highlighted with a red box)
- Default Cost: 1
- Interfaces: 0
- Active Interfaces: 0
- Neighbors: 0
- Adjacent Neighbors: 0

Buttons on the right include OK, Cancel, Apply, Disable, Copy, and Remove. The dialog is currently disabled, as indicated by the 'disabled' text at the bottom left.

- A stub area is an area which does not receive AS external routes.
- Typically all routes to external AS networks can be replaced by one default route. - this route will be created automatically distributed by ABR

Stub area (2)

- «Inject Summary LSA» option allows to collect separate backbone or other area router Link State Advertisements (LSA) and inject it to the stub area
- Enable «Inject Summary LSA» option only on ABR
- «Inject Summary LSA» is not a route aggregation
- «Inject Summary LSA» cost is specified by «Default area cost» option

Not-So-Stubby Area (NSSA)

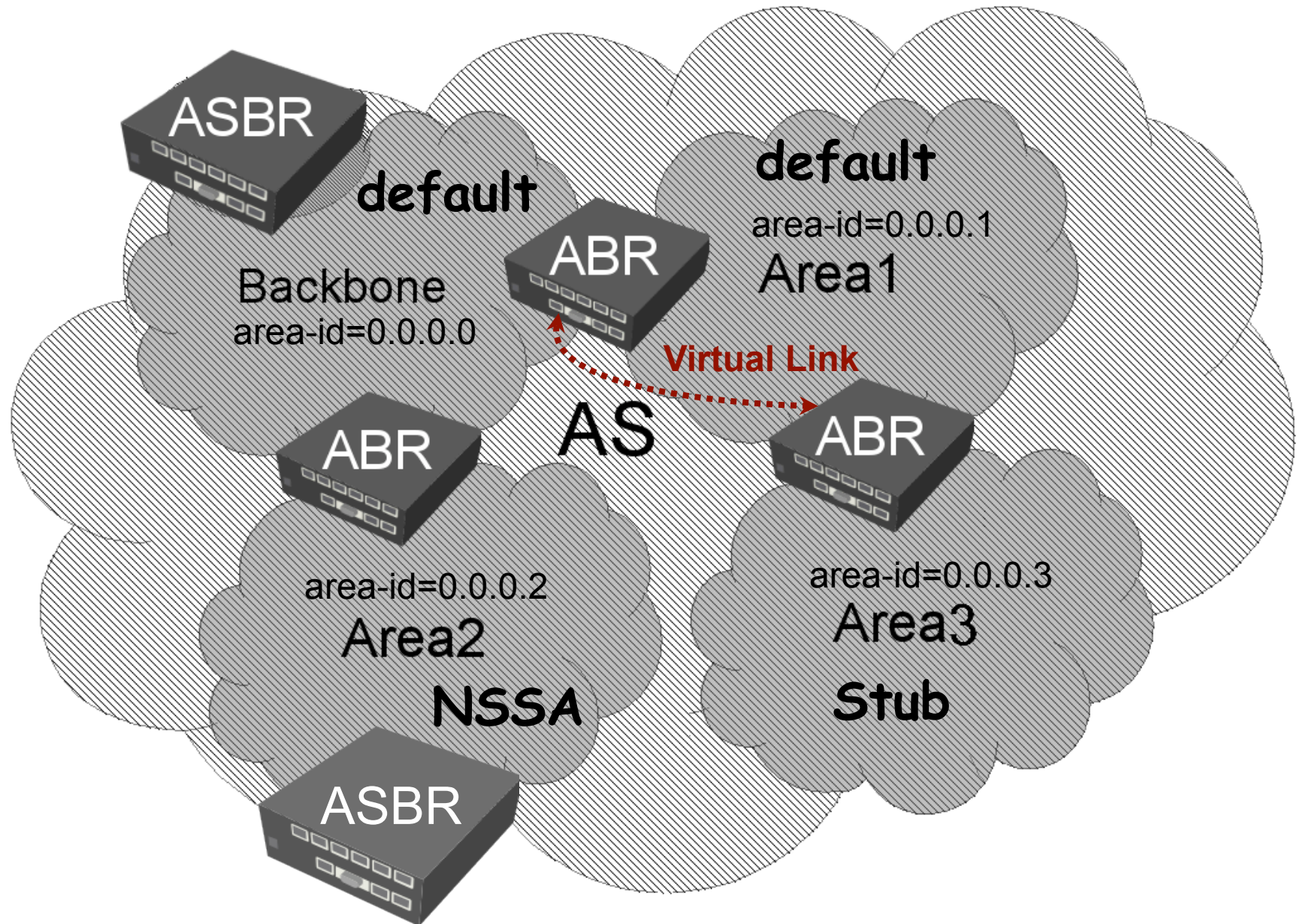
The screenshot shows the 'New OSPF Area' dialog box with the following configuration:

- Area Name: area1
- Area ID: 0.0.0.0
- Type: nssa
- Translator Role: translate never
- Authentication: translate candidate (highlighted)
- Default Cost: 1
- Interfaces: 0
- Active Interfaces: 0
- Neighbors: 0
- Adjacent Neighbors: 0

The 'Authentication' dropdown menu is open, showing three options: 'translate always', 'translate candidate' (highlighted), and 'translate never'.

- NSSA is a type of **stub area** that is able to transparently inject AS external routes to the backbone.
- «Translator role» option allow to control which ABR of the NSSA area will act as a relay from ASBR to backbone area

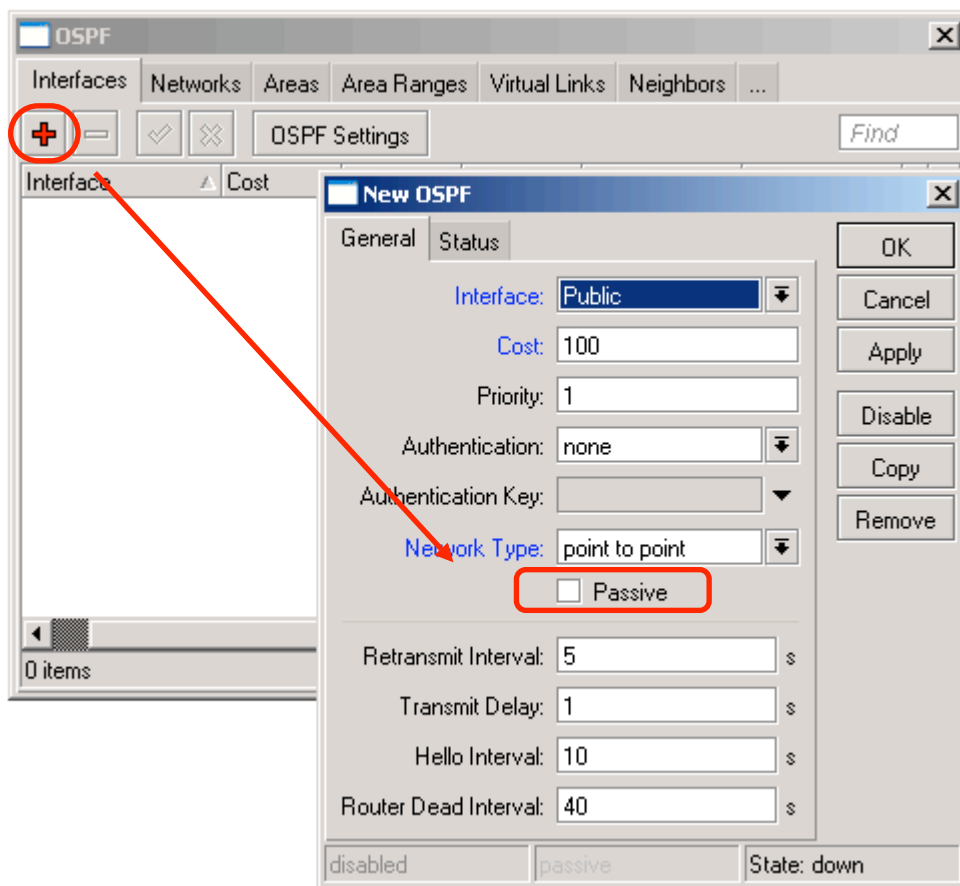
OSPF AS



Area Type Lab

- Set your area type to «stub»
- Check your routing table for changes!
- Make sure that default route redistribution on the ABR is set to «never»
- Set «Inject Summary LSA» option
 - ◆ on the ABR to «enable»
 - ◆ on the IR to «disable»

Passive interface

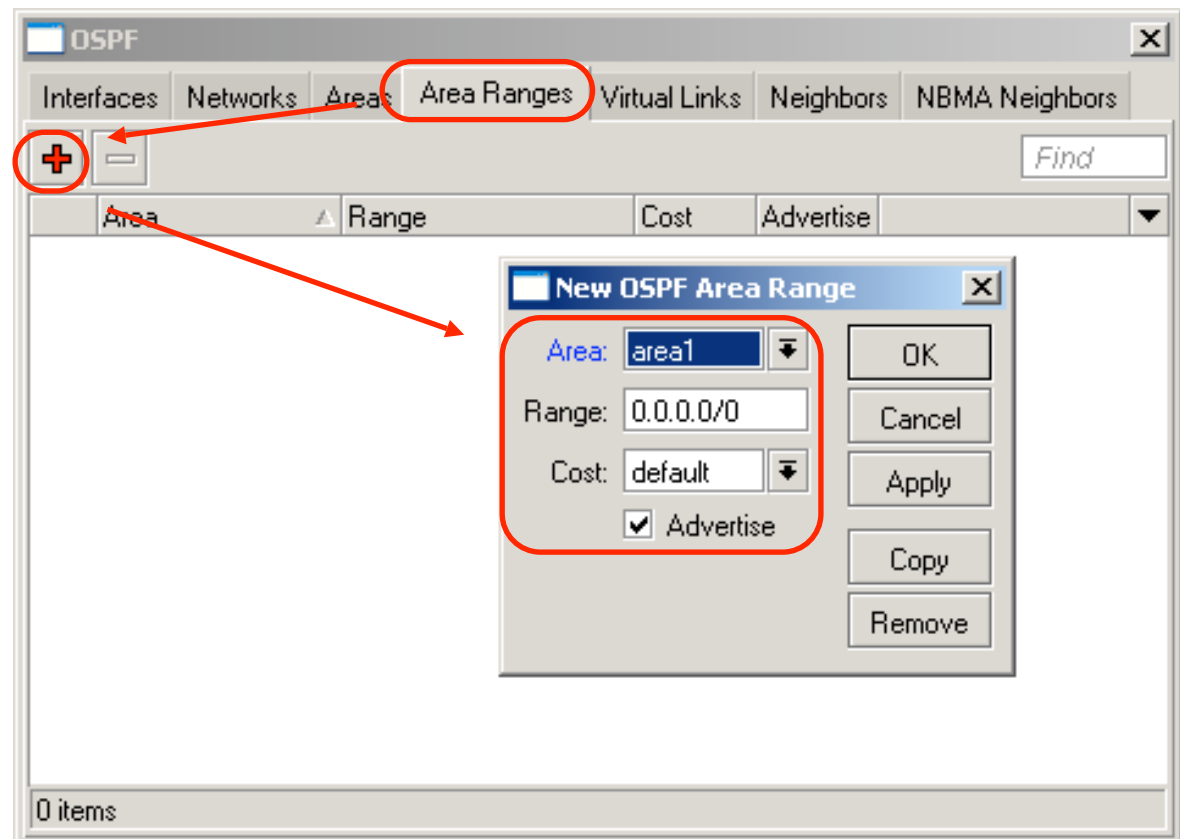


- It is necessary to assign client networks to the area or else stub area will consider those networks as external.
- It is a security issue!!!

- Passive option allow you to disable OSPF “Hello” protocol on client interfaces

Area Ranges

- Address ranges are used to aggregate (replace) network routes from within the area into one single route
- It is possible then to advertise this aggregate route or drop it
- It is possible to assign specific cost to aggregate route



Route Aggregation Lab

- Advertise only one 192.168.Z.0/24 route instead of four /26 (192.168.Z.0/26, 192.168.Z.64/26, 192.168.Z.128/26, 192.168.Z.192/26) into the backbone
- Stop advertising backup network to the backbone
- Check the Main AP's routing table

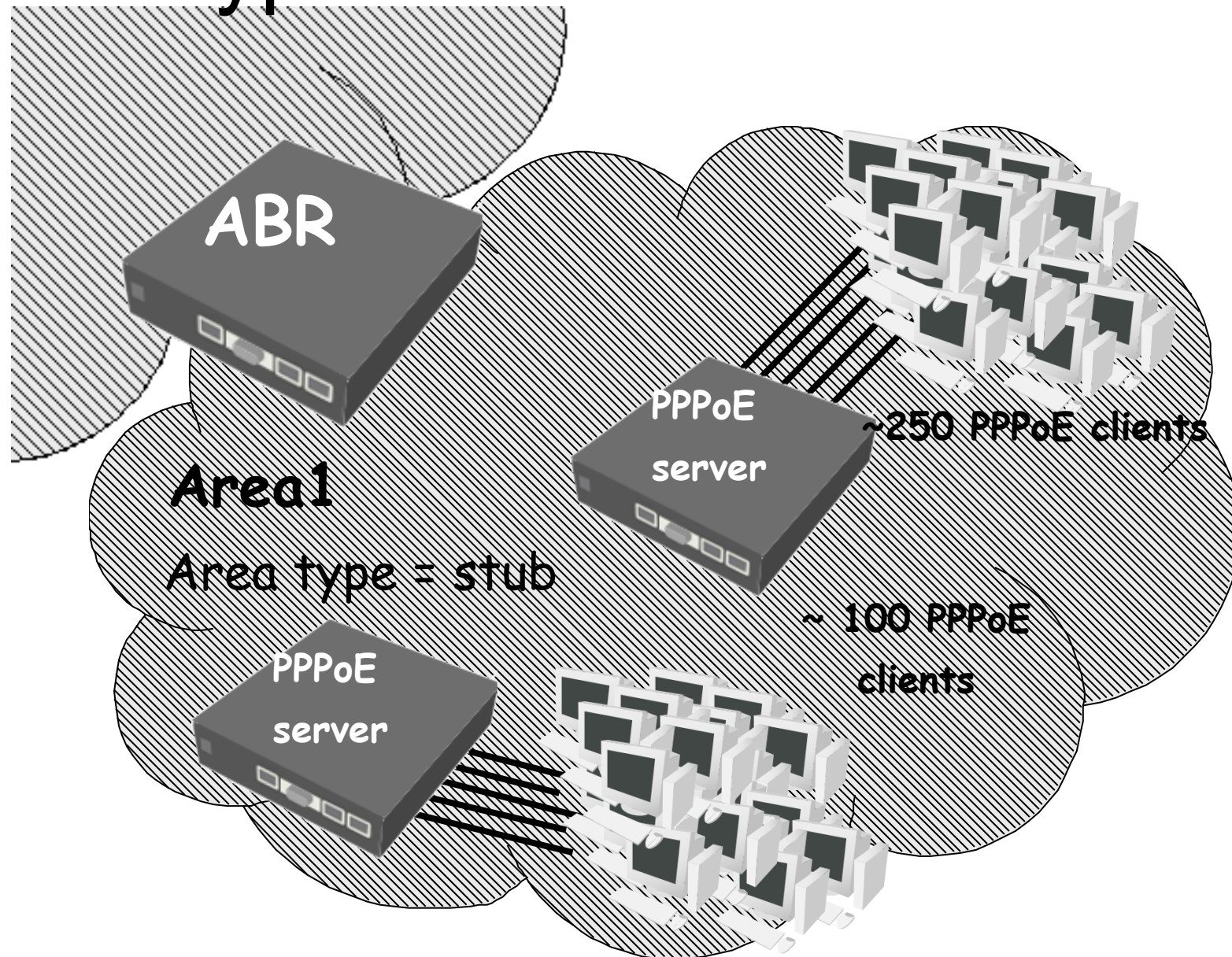
Summary

- For securing your OSPF network
 - ◆ Use authentication keys (for interfaces and areas)
 - ◆ Use highest priority (255) to designated router
 - ◆ Use correct network types for the area
- To increase performance of OSPF network
 - ◆ Use correct area types
 - ◆ Use “Summary LSA” for stub areas
 - ◆ Use route aggregation as much as possible

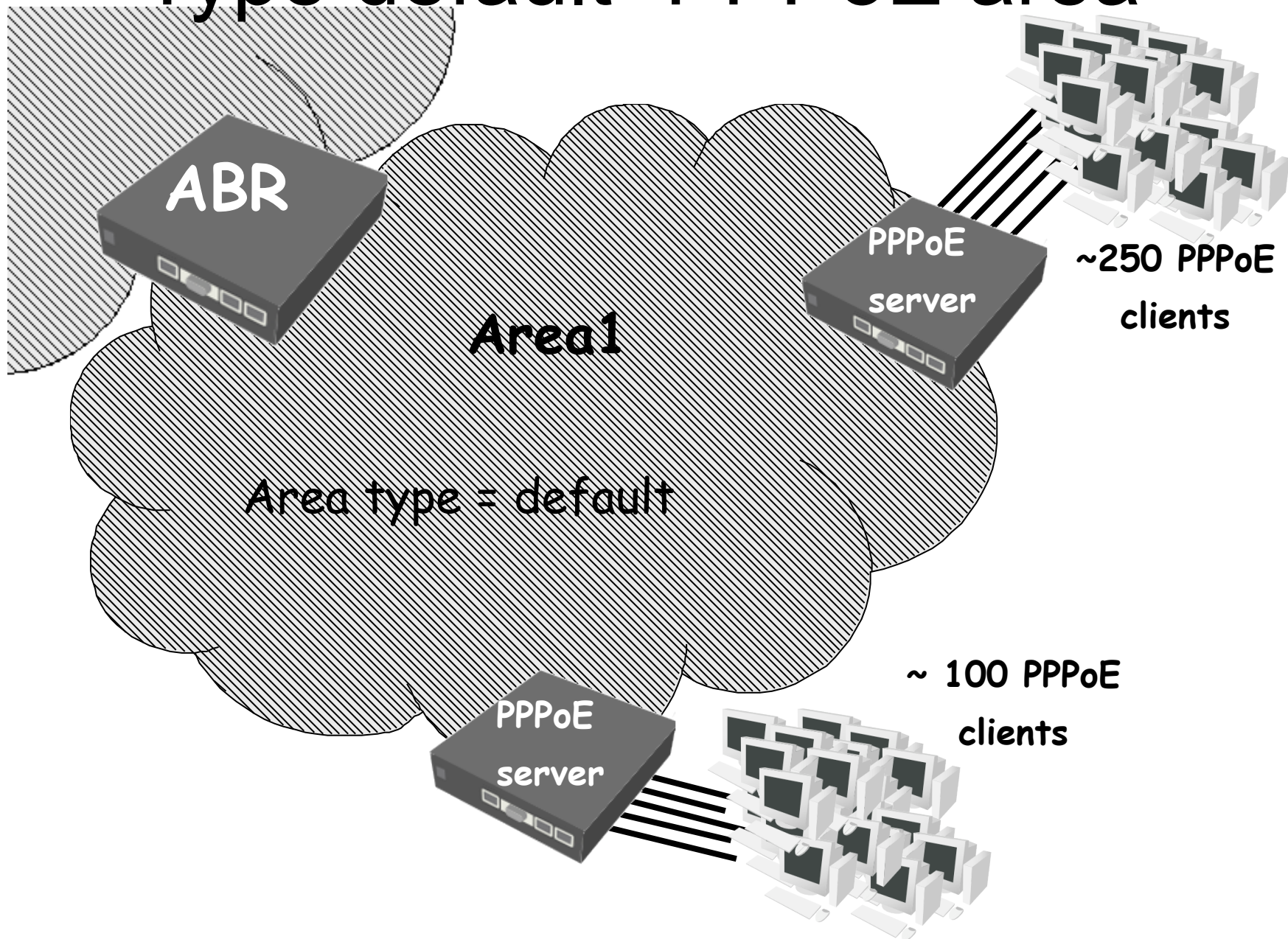
OSPF and Dynamic VPN Interfaces

- Each dynamic VPN interface
 - ◆ creates a new /32 Dynamic, Active, Connected (DAC) route in the routing table when appears
 - ◆ removes that route when disappears
- Problems:
 - ◆ Each of these changes results in OSPF update, if redistribute-connected is enabled (update flood in large VPN networks)
 - ◆ OSPF will create and send LSA to each VPN interface, if VPN network is assigned to any OSPF area (slow performance)

Type stub “PPPoE area”



Type default “PPPoE area”



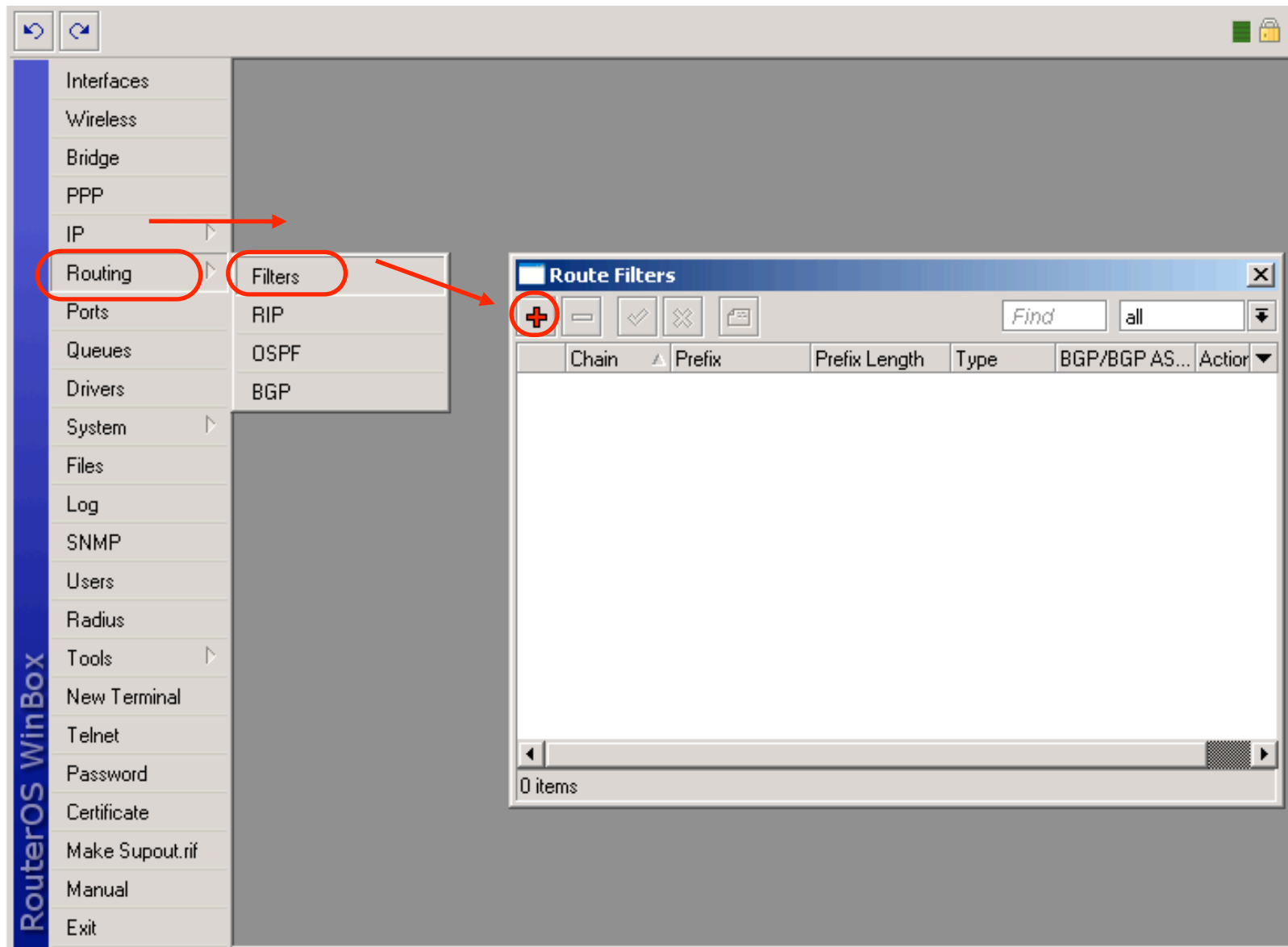
“PPPoE area” Lab (discussion)

- Give a solution for each problem mentioned previously if used area type is “stub”
- Try to find a solution for each problem mentioned previously if used area type is “default”

OSPF Routing Filters

- The routing filters may be applied to incoming and outgoing OSPF routing update messages
 - ◆ Chain “ospf-in” for all incoming routing update messages
 - ◆ Chain “ospf-out” for all outgoing routing update messages
- Routing filters can manage only **external** OSPF routes (routes for the networks that are **not** assigned to any OSPF area)

Routing Filters



Routing Filters and VPN

- It is possible to create a routing filter rule to restrict all /32 routes from getting into the OSPF
- It is necessary to have one aggregate route to this VPN network :
 - ◆ By having address from the aggregate VPN network to the any interface of the router
 - ➔ Suggestion: place this address on the interface where VPN server is running
 - ➔ Suggestion: use network address, the clients will not be able to avoid your VPN service then
 - ◆ By creating static route to the router itself

Routing filters Rule

New Route Filter

Matchers Actions

Chain: ▼

Prefix: ▼

Prefix Length: ▲

Match Chain: ▼

Distance: ▼

Scope: ▼

Target Scope: ▼

Pref. Source: ▼

Routing Mark: ▼

Route Comment: ▼

▼ Type _____

▼ BGP _____

▼ BGP Communities _____

▼ RIP _____

Invert Match

OK

Cancel

Apply

Disable

Comment

Copy

Remove

disabled

New Route Filter

Matchers Actions

Action: ▼

Jump Target: ▼

Set Distance: ▼

Set Scope: ▼

Set Target Scope: ▼

Set Pref. Source: ▼

Set In Nexthop: ▲▼

Set In Nexthop Direct: ▲▼

Set Out Nexthop: ▼

Set Routing Mark: ▼

Set Route Comment: ▼

Set Check Gateway: ▼

Set Disabled: ▼

▼ BGP _____

▼ BGP Communities _____

▼ RIP _____

OK

Cancel

Apply

Disable

Comment

Copy

Remove

disabled

Bridging

Bridge, Admin MAC, Bridge ports, Bridge
firewall, STP and RSTP

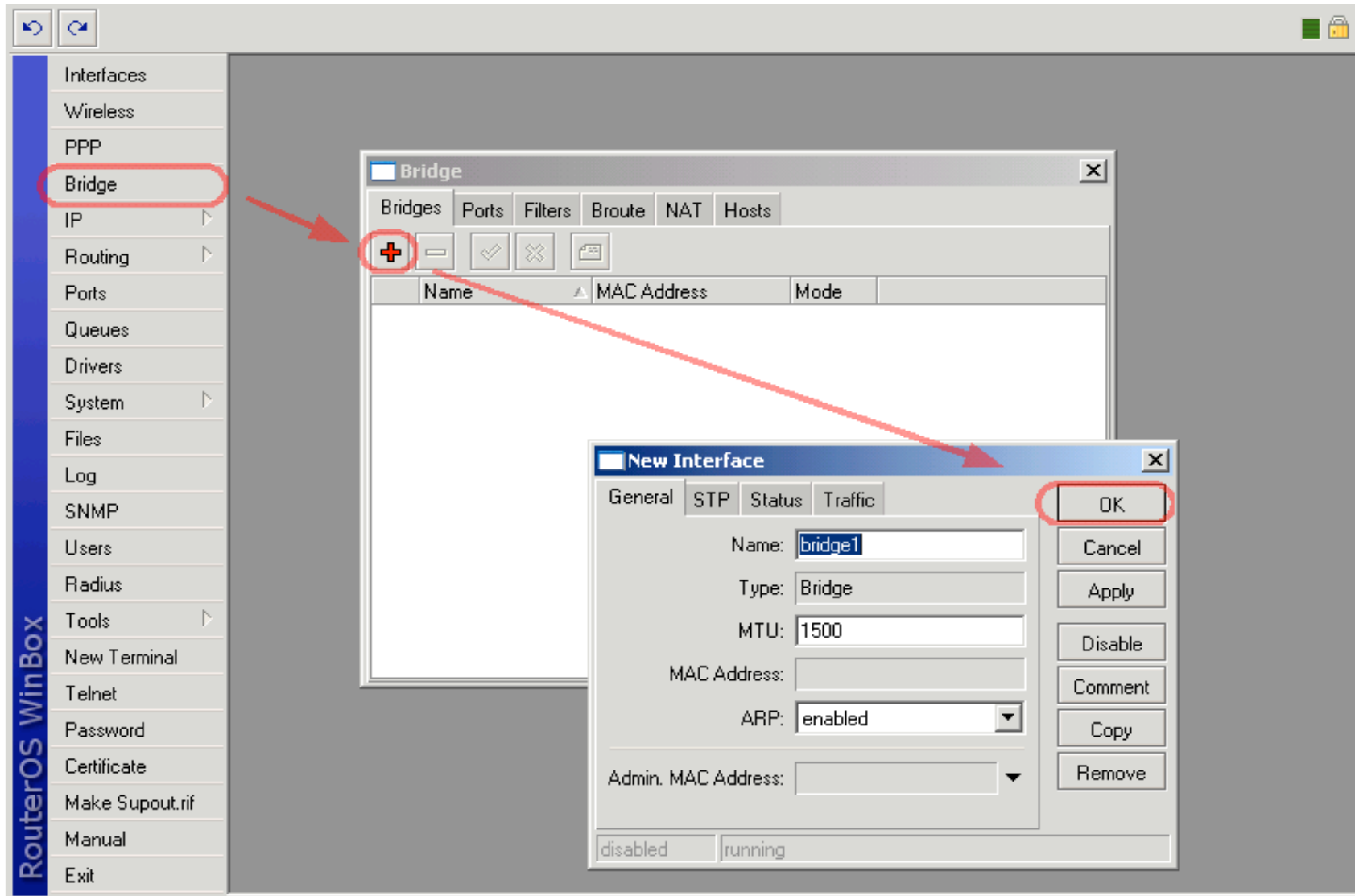
Bridge

- Ethernet-like networks can be connected together using OSI Layer 2 bridges
- The bridge feature allows interconnection of hosts connected to separate LANs as if they were attached to a single LAN segment
- Bridges extend the broadcast domain and increase the network traffic on bridged LAN

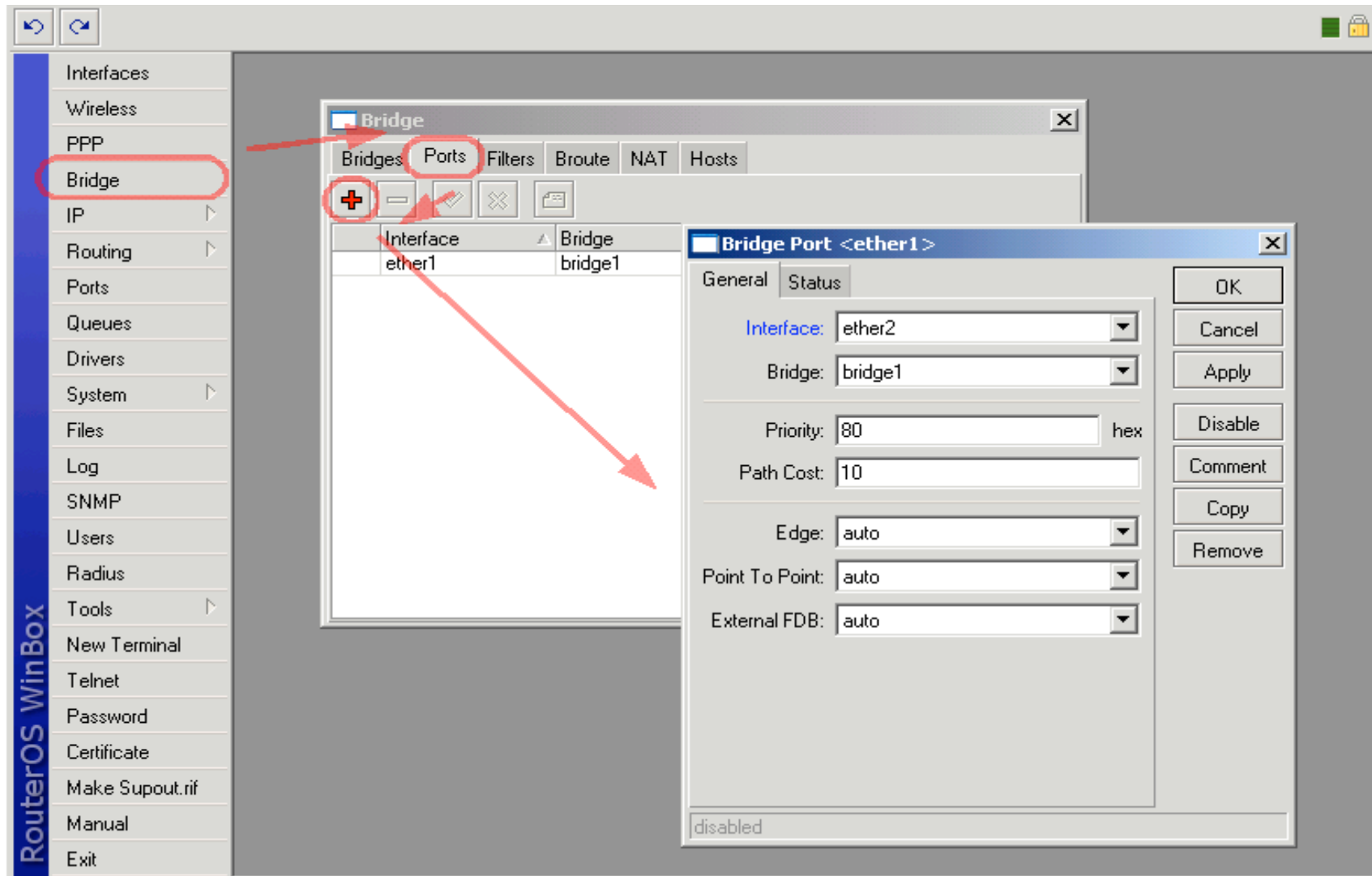
Bridge Configuration

- Bridge is a virtual interface in RouterOS
- Several bridges can be created
 - ◆ `/interface bridge add name=bridge1`
- Interfaces are assigned as ports to a bridge
 - ◆ `/interface bridge port add interface=ether1
bridge=bridge1`
 - ◆ `/interface bridge port add interface=ether2
bridge=bridge1`

Creating a Bridge



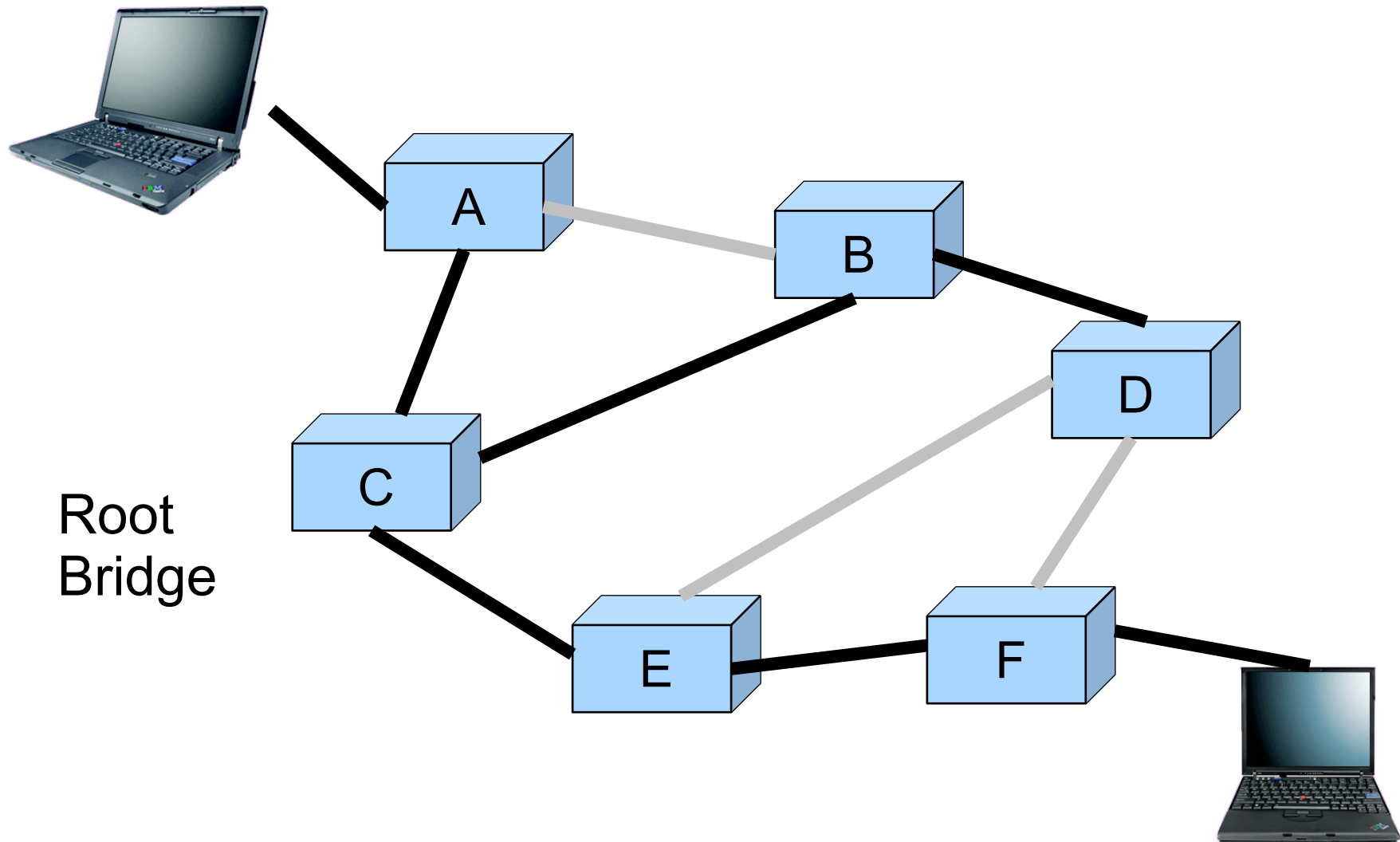
Assigning Ports to the Bridge



Spanning Tree Protocol

- The Spanning Tree Protocol (STP)
 - ◆ is defined by IEEE Standard 802.1D
 - ◆ provides a loop free topology for any bridged LAN
 - ◆ discovers an optimal spanning tree within the mesh network and disables the links that are not part of the tree, thus eliminating bridging loops

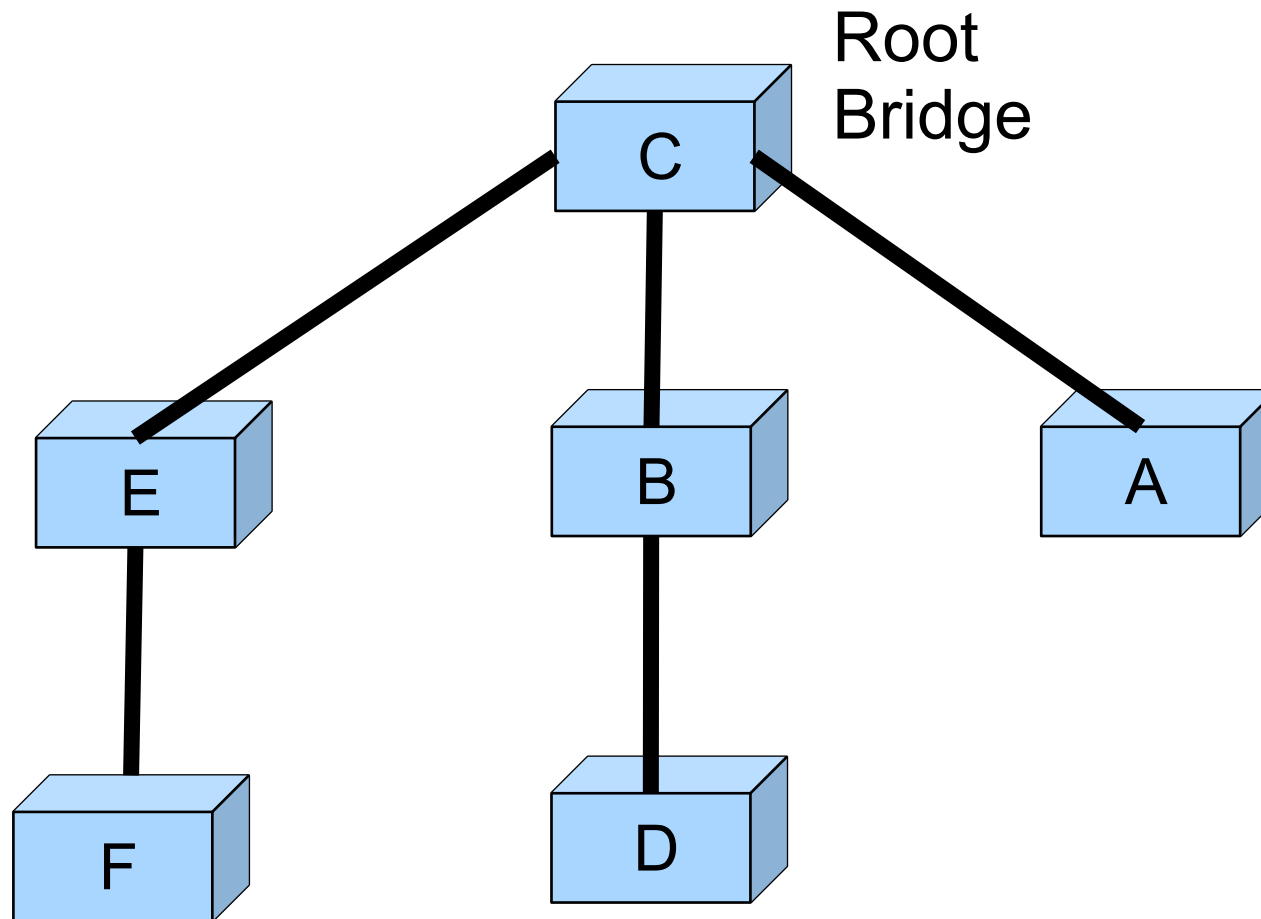
STP in Action



STP Root Bridge

- Lowest priority
- Lowest ID (MAC address)
- Central point of the topology
- Each bridge calculates shortest path to the Root Bridge

Spanning Tree



Rapid Spanning Tree Protocol

- Rapid Spanning Tree Protocol (RSTP)
 - ◆ is an evolution of the STP
 - ◆ provides for faster spanning tree convergence after a topology change than STP
- rstp-bridge-test package is required for the RSTP feature to be available in RouterOS

RSTP Bridge Port Roles

- Lowest priority for looped ports
- Root port – a path to the root bridge
- Alternative port – backup root port
- Designated port – forwarding port
- Backup port – backup designated port

Routed Networks vs Bridging

- Routers do not forward broadcast frames
- Communication loops and their resultant broadcast storms are no longer a design issue in routed networks
- Redundant media and meshed topologies can offer traffic load sharing and more robust fault tolerance than bridged network topologies

Bridge Firewall

- The bridge firewall implements packet filtering and thereby provides security functions that are used to manage data flow to, from and through bridge
- Elements of bridge firewall are:
 - ◆ Bridge Filter
 - ◆ Bridge Network Address Translation (NAT)
 - ◆ Bridge Broute

Bridge Filter

- Bridge filter has three predefined chains, input, forward, and output
- Example application is filtering broadcast traffic

Bridge NAT

- Bridge network address translation (NAT)
 - ◆ provides ways for changing source/destination MAC addresses of the packets traversing a bridge
 - ◆ has two built-in chains
 - ➔ src-nat
 - ➔ dst-nat
- Bridge NAT can be used for ARP

Bridge Broute

- Bridge Broute
 - ◆ makes bridge a brouter - router that performs routing on some of the packets, and bridging - on others
 - ◆ has one predefined chain, brouting, which is traversed right after a packet enters an enslaved interface before "Bridging Decision"
- For example, IP can be routed, and everything else bridged (IPX)

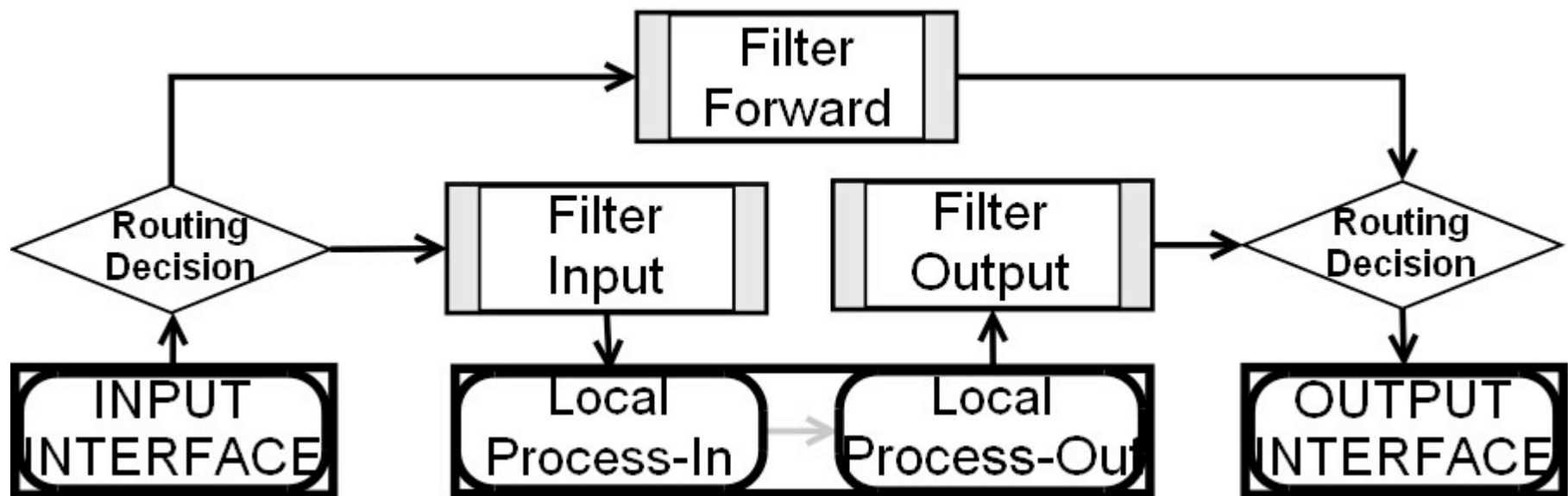
Firewall

Firewall filters,
Network Intrusion Detection System (NIDS),
Network Address Translation (NAT)

Firewall Filters Structure

- Firewall filter rules are organized in chains
- There are default and user-defined chains
- There are three default chains
 - ◆ **input** – processes packets sent to the router
 - ◆ **output** – processes packets sent by the router
 - ◆ **forward** – processes packets sent through the router
- Every user-defined chain should subordinate to at least one of the default chains

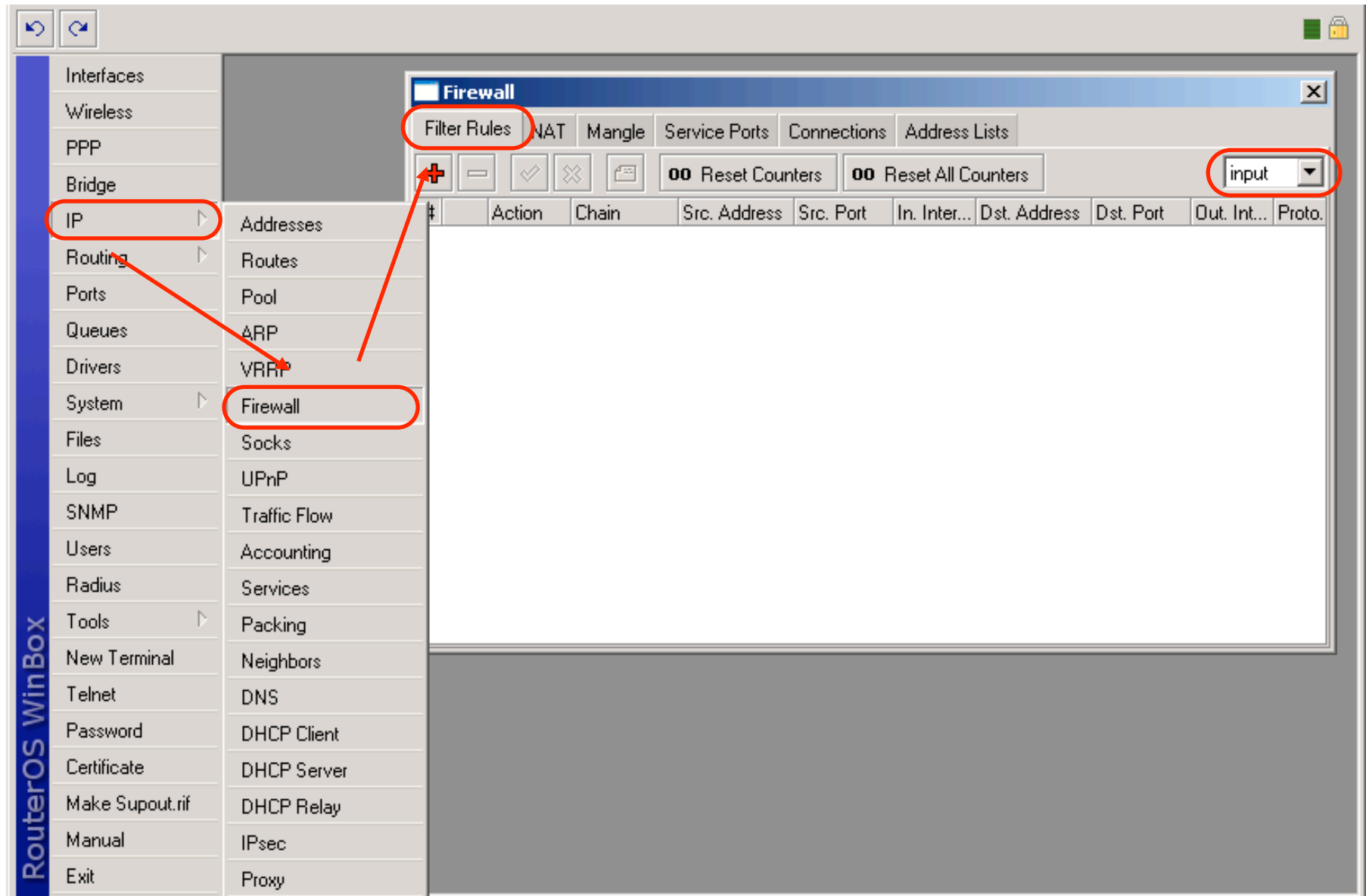
Firewall Filter Structure Diagram



Firewall Filters

- The firewall filter facility is a tool for packet filtering
- Firewall filters consist from the sequence of IF-THEN rules
 - 0) IF <condition(s)> THEN <action>
 - 1) IF <condition(s)> THEN <action>
 - 2) IF <condition(s)> THEN <action>
- If a packet doesn't meet all the conditions of the rule, it will be sent on to the next rule.
- If a packet meet all the conditions of the rule, specified action will be performed on it.

Filter Rules – Winbox View

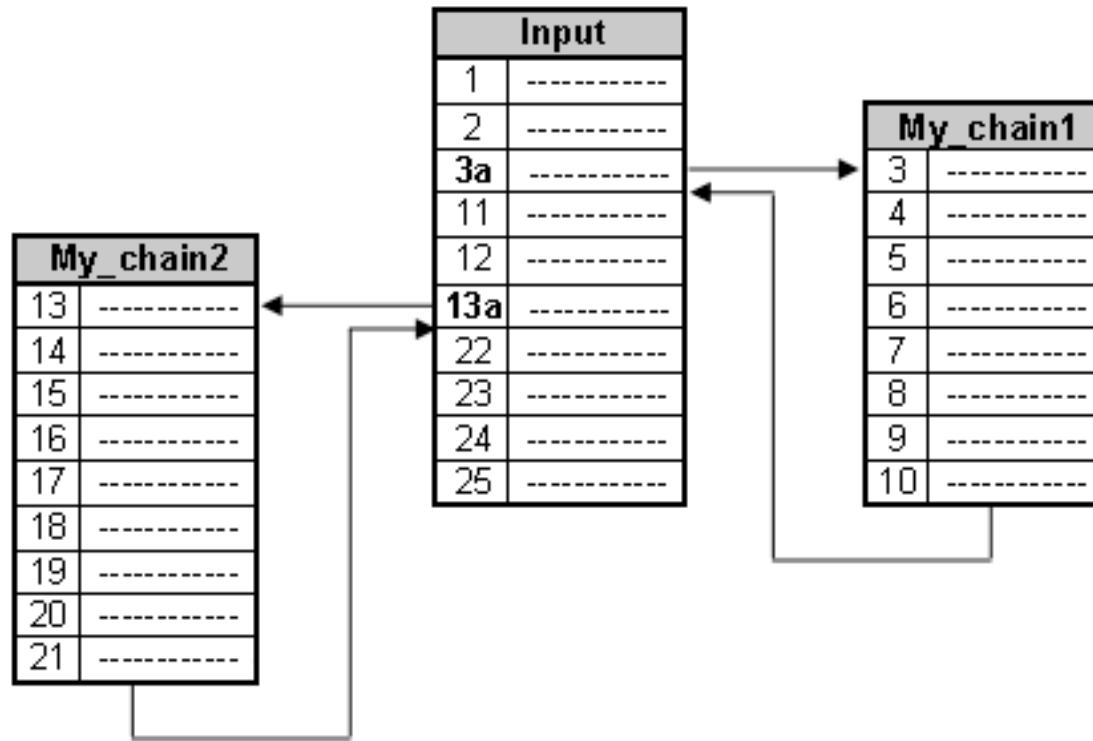


Firewall Filter Chains

- You can direct traffic to user-defined chains using action **jump** (and direct it back to the default chain using action **return**)
- Users can add any number of chains
- User-defined chains are used to optimize the firewall structure and make it more readable and manageable
- User-defined chains help to improve performance by reducing the average number of processed rules per packet

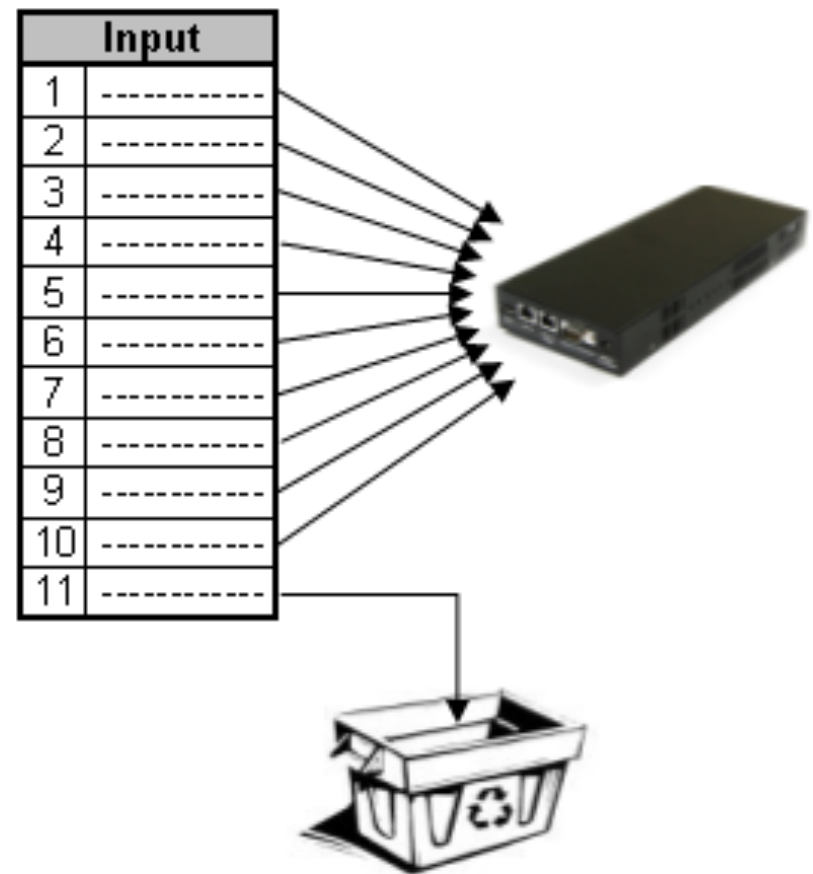
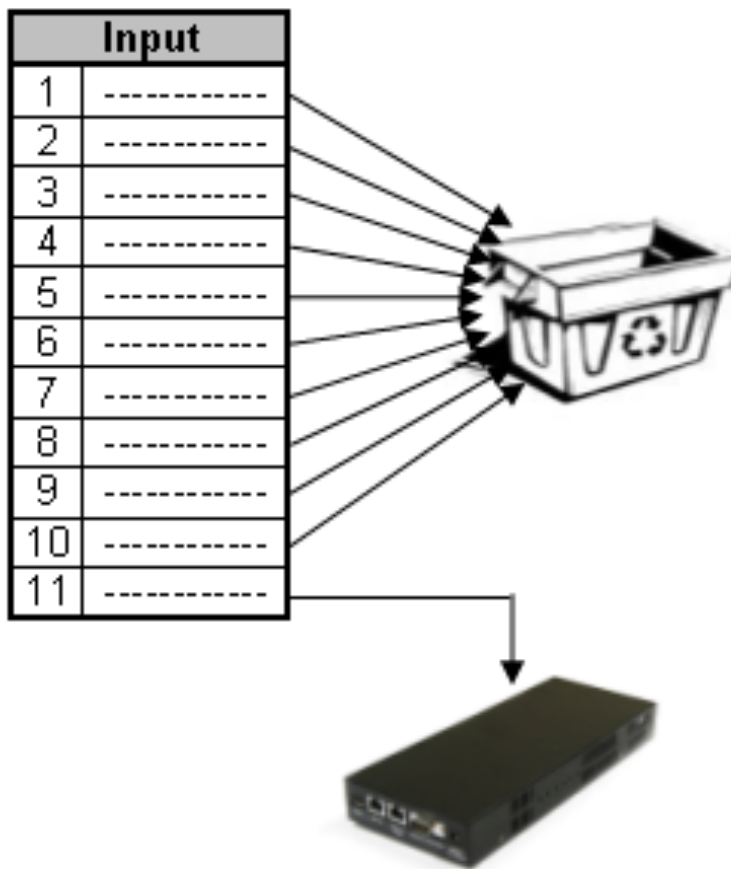
User-Defined Chains

Input	
1	-----
2	-----
3	-----
4	-----
5	-----
6	-----
7	-----
8	-----
9	-----
10	-----
11	-----
12	-----
13	-----
14	-----
15	-----
16	-----
17	-----
18	-----
19	-----
20	-----
21	-----
22	-----
23	-----
24	-----
25	-----



Firewall Building Tactics

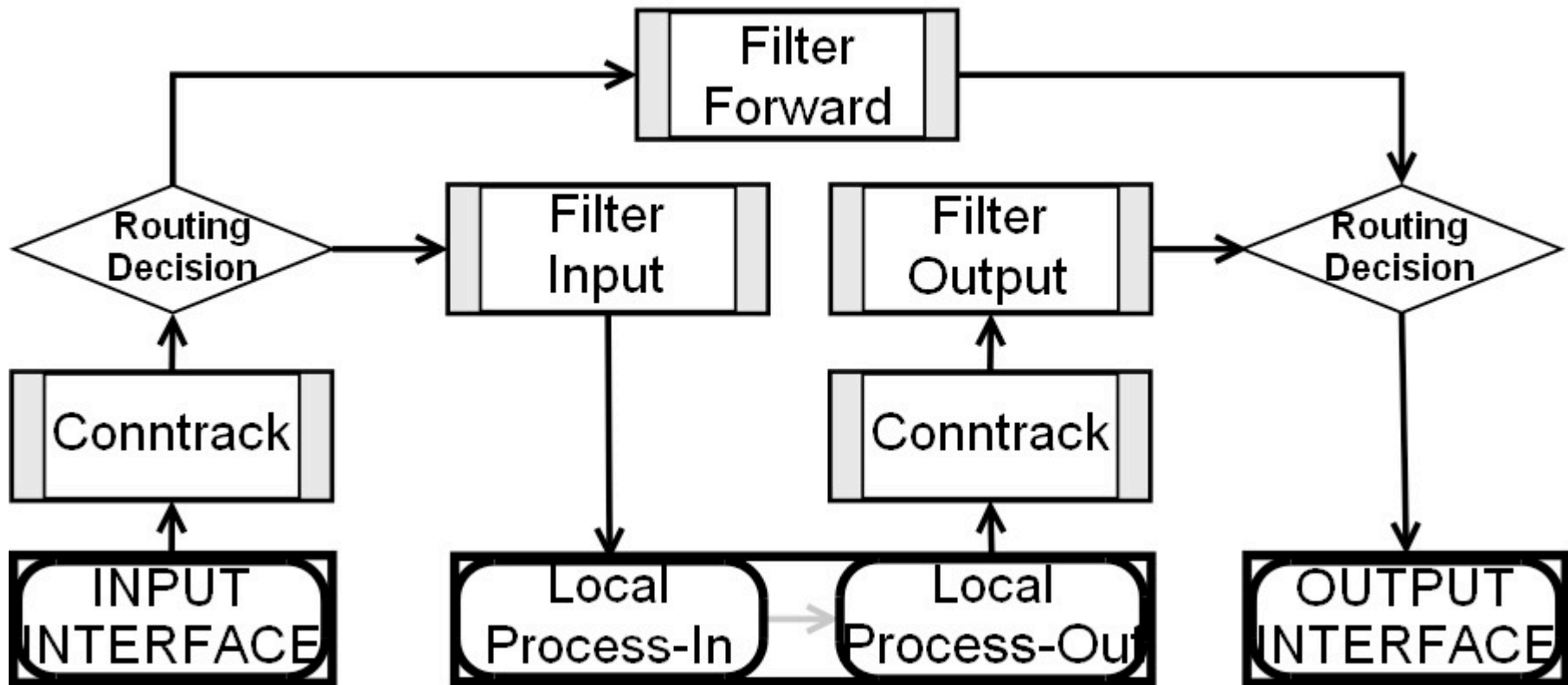
- Drop all unneeded, accept everything else
- Accept only needed, drop everything else



Connection Tracking

- Connection Tracking (or Conntrack) system is the heart of firewall, it gathers and manages information about **all** active connections.
- By disabling the conntrack system you will lose functionality of the NAT and most of the filter and mangle conditions.
- Each conntrack table entry represents bidirectional data exchange
- Conntrack takes a lot of CPU resources (disable it, if you don't use firewall)

Conntrack Placement



Conntrack – Winbox View

The screenshot shows the Winbox Firewall configuration interface. The 'Connections' tab is selected, and the 'Tracking' sub-tab is active. A table of active connections is displayed, with columns for Src. Address, Dst. Address, and Protocol. A red arrow points from the 'Tracking' sub-tab to the 'Connection Tracking' dialog box. The dialog box is titled 'Connection Tracking' and has a checked 'Enabled' checkbox. It contains various timeout settings for TCP and UDP connections, along with an 'ICMP Timeout' and a 'Generic Timeout'. The 'TCP SynCookie' checkbox is unchecked. The dialog also has 'OK', 'Cancel', and 'Apply' buttons. On the right side of the dialog, there is a list of connection entries with their respective timeout values.

Src. Address	Dst. Address	Prot
A 192.168.1.71:1818	217.199.111.8:411	6 (tc
192.168.1.71:9183	217.132.237.251:14642	17 (
A 192.168.1.71:9183	217.132.191.159:9183	17 (
U 192.168.1.71:9183	217.132.112.154:9183	17 (
A 192.168.1.71:9183	217.132.55.45:9183	17 (
192.168.1.71:9183	217.132.35.226:9183	17 (
A 192.168.1.98:1033	213.238.245.47:4263	6 (tc
A 192.168.1.71:9183	213.182.221.64:9183	17 (
192.168.1.71:9183	213.140.19.124:56516	17 (
A 192.168.1.71:9183	212.246.84.168:9183	17 (
192.168.1.71:9183	212.149.193.39:9183	17 (
192.168.1.71:9183	212.149.156.10:9183	17 (
U 192.168.1.71:9183	212.149.137.236:9183	17 (
192.168.1.71:9183	212.54.15.132:9183	17 (
A 192.168.1.71:9183	203.100.21.228:9183	17 (
192.168.1.71:9183	195.244.142.157:9183	17 (
192.168.1.71:9183	195.244.141.182:9183	17 (
A 192.168.1.71:3268	195.178.92.45:11469	6 (tc
A 192.168.1.71:9183	195.13.175.200:64149	17 (
192.168.1.71:9183	195.2.119.182:9183	17 (
U 192.168.1.71:9183	193.109.211.203:59465	17 (
A 192.168.1.71:9183	193.95.232.16:9183	17 (
A 192.168.1.71:9183	193.95.216.149:9181	17 (
A 192.168.1.71:9183	193.77.236.191:9183	17 (

Total Entries: 208 Max Entries: 36864

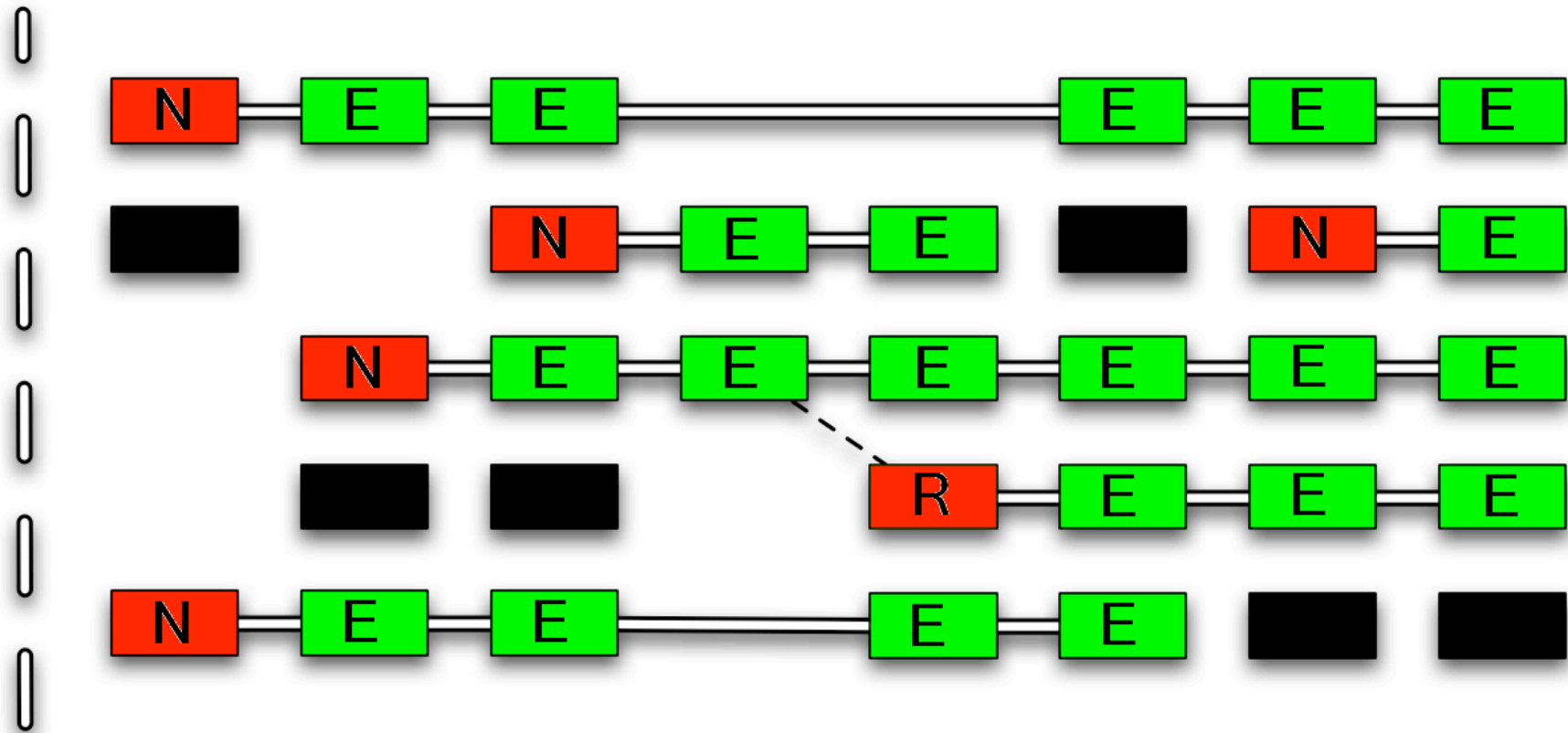
imeout
23:59:58
00:00:07
00:01:56
00:00:08
00:02:51
00:00:04
18:33:56
00:01:12
00:00:01
00:00:59
00:00:01
00:00:08
00:00:05
00:00:06
00:02:40
00:00:05
00:00:08
23:59:58
00:01:34
00:00:04
00:00:03
00:02:02
00:01:34
00:01:12

Condition: Connection State

- Connection state is a status assigned to each packet by conntrack system:
 - ◆ New – packet is opening a new connection
 - ◆ Related – packet is also opening a new connection, but it is in some kind of relation to an already established connection
 - ◆ Established – packet belongs to an already known connection
 - ◆ Invalid – packet does not belong to any of the known connections
- Connection state \neq TCP state

Connection State

Firewall



 invalid

 established

 new

 related

First Rule Example

```
/ip firewall filter add chain=input connection-state=invalid \  
action=drop comment="Drops invalid packets"
```

The screenshot shows the 'Firewall Rule' configuration window with the 'General' tab selected. The 'Chain' dropdown is set to 'input' and the 'Connection State' dropdown is set to 'invalid'. Both dropdowns are circled in red. The 'Status' indicator at the bottom left shows 'disabled'.

The screenshot shows the 'Firewall Rule' configuration window with the 'Action' tab selected. The 'Action' dropdown is set to 'drop' and is circled in red. The 'Comment' button is also circled in red. The 'Status' indicator at the bottom left shows 'disabled'.

Chain Input

Protecting the router – allowing only necessary services from reliable source addresses with agreeable load

Chain Input Lab

- Create 3 rules to ensure that only connection-state **new** packets will proceed through the input filter
 - ◆ **Drop** all connection-state **invalid** packets
 - ◆ **Accept** all connection-state **established** packets
 - ◆ **Accept** all connection-state **related** packets
- Create 2 rules to ensure that only you will be able to connect to the router
 - ◆ **Accept** all packets from your laptop IP
 - ◆ **Drop** everything else

Firewall Maintenance

- Write comment for each firewall rule, to make your firewall more manageable
- Look at the rule counters, to determine rule activity
- Change rule position to get necessary order
- Use action “passthrough” to determine amount of traffic before applying any action
- Use action “log” to collect detailed information about traffic

Action "log"

The screenshot shows the RouterOS WinBox interface. On the left is a vertical menu with the following items: Interfaces, Wireless, PPP, Bridge, IP, Routing, Ports, Queues, Drivers, System, Files, Log (highlighted with a red circle), SNMP, Users, Radius, Tools, New Terminal, Telnet, Password, Certificate, Make Supout.rif, Manual, and Exit. The main window displays a 'Log' window with a dropdown menu set to 'all'. The log entries are as follows:

Date/Time	Event Type	Details
Feb/19/2007 12:58:58	firewall info	input: in:local_ether1 out:(none), src-mac 00:08:0d:26:c8:52, proto TCP (ACK), 10.1.100.251:2553->10.1.100.254:8291, len 40
Feb/19/2007 12:58:58	firewall info	input: in:public_ether3 out:(none), src-mac 00:19:d1:0e:cf:3a, proto UDP, 10.5.8.53:32768->10.5.8.123:161, len 81
Feb/19/2007 12:58:58	firewall info	input: in:public_ether3 out:(none), src-mac 00:19:d1:0e:cf:3a, proto UDP, 10.5.8.53:32768->10.5.8.123:161, len 82
Feb/19/2007 12:58:58	firewall info	input: in:public_ether3 out:(none), src-mac 00:19:d1:0e:cf:3a, proto UDP, 10.5.8.53:32768->10.5.8.123:161, len 82
Feb/19/2007 12:58:58	firewall info	input: in:public_ether3 out:(none), src-mac 00:19:d1:0e:cf:3a, proto UDP, 10.5.8.53:32768->10.5.8.123:161, len 82
Feb/19/2007 12:58:58	firewall info	input: in:local_ether1 out:(none), src-mac 00:0c:42:03:01:40, proto UDP, 0.0.0.0:5678->255.255.255.255:5678, len 96
Feb/19/2007 12:58:58	firewall info	input: in:local_ether1 out:(none), src-mac 00:08:0d:26:c8:52, proto TCP (ACK), 10.1.100.251:1207->10.1.100.254:8291, len 40
Feb/19/2007 12:58:58	firewall info	input: in:local_ether1 out:(none), src-mac 00:08:0d:26:c8:52, proto TCP (ACK), 10.1.100.251:2553->10.1.100.254:8291, len 40
Feb/19/2007 12:58:59	firewall info	input: in:public_ether3 out:(none), src-mac 00:0c:42:0a:88:be, proto UDP, 10.5.8.120:5678->255.255.255.255:5678, len 100
Feb/19/2007 12:58:59	firewall info	input: in:local_ether1 out:(none), src-mac 00:08:0d:26:c8:52, proto TCP (ACK), 10.1.100.251:1207->10.1.100.254:8291, len 40
Feb/19/2007 12:58:59	firewall info	input: in:local_ether1 out:(none), src-mac 00:08:0d:26:c8:52, proto TCP (ACK), 10.1.100.251:2553->10.1.100.254:8291, len 40
Feb/19/2007 12:58:59	firewall info	input: in:local_ether1 out:(none), src-mac 00:08:0d:26:c8:52, proto TCP (ACK), 10.1.100.251:1207->10.1.100.254:8291, len 40
Feb/19/2007 12:58:59	firewall info	input: in:local_ether1 out:(none), src-mac 00:08:0d:26:c8:52, proto TCP (ACK), 10.1.100.251:2553->10.1.100.254:8291, len 40

RouterOS Services

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

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

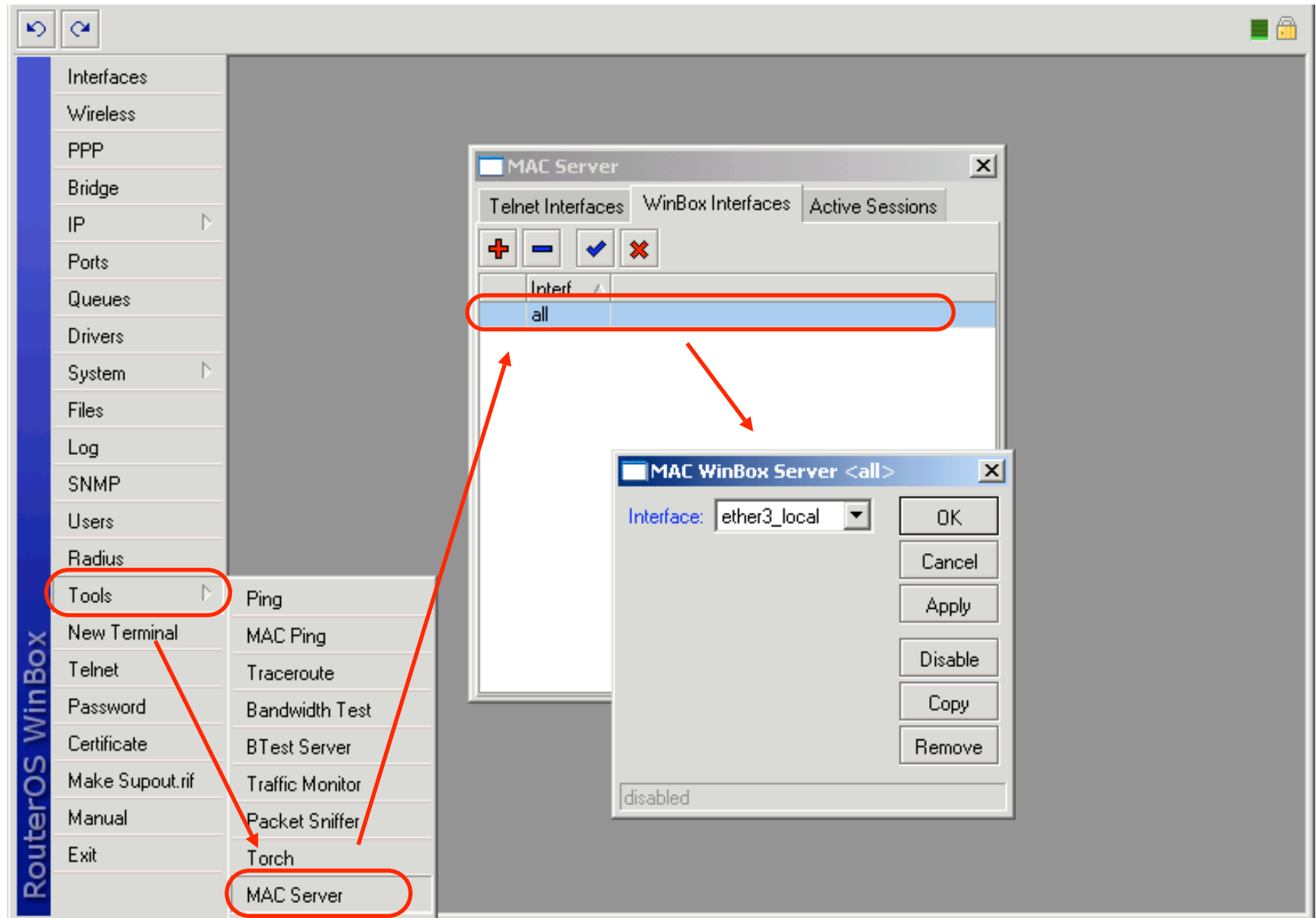
RouterOS Services Lab

- Create rules to allow only necessary RouterOS services to be accessed from the public network
- Use action “log” to determine those services
- Create rule to allow winbox, ssh and telnet connection from the teacher's network (10.1.2.0/24)
- Arrange rules accordingly
- Write comment for each firewall rule

Important Issue

- Firewall filters do not filter MAC level communications
- You should turn off MAC-telnet and MAC-Winbox features at least on the public interface
- You should disable network discovery feature, so that the router do not reveal itself anymore (“/ip neighbor discovery” menu)

MAC-telnet and MAC-winbox



Chain Forward

Protecting the customers from viruses and
protecting the Internet from the customers

Chain Forward Lab

- Create 3 rules to ensure that only connection-state **new** packets will proceed through the chain forward (same as in the Chain Input Lab)
- Create rules to close most popular ports of viruses
 - ◆ **Drop** TCP and UDP port range 137-139
 - ◆ **Drop** TCP and UDP port 445

Virus Port Filter

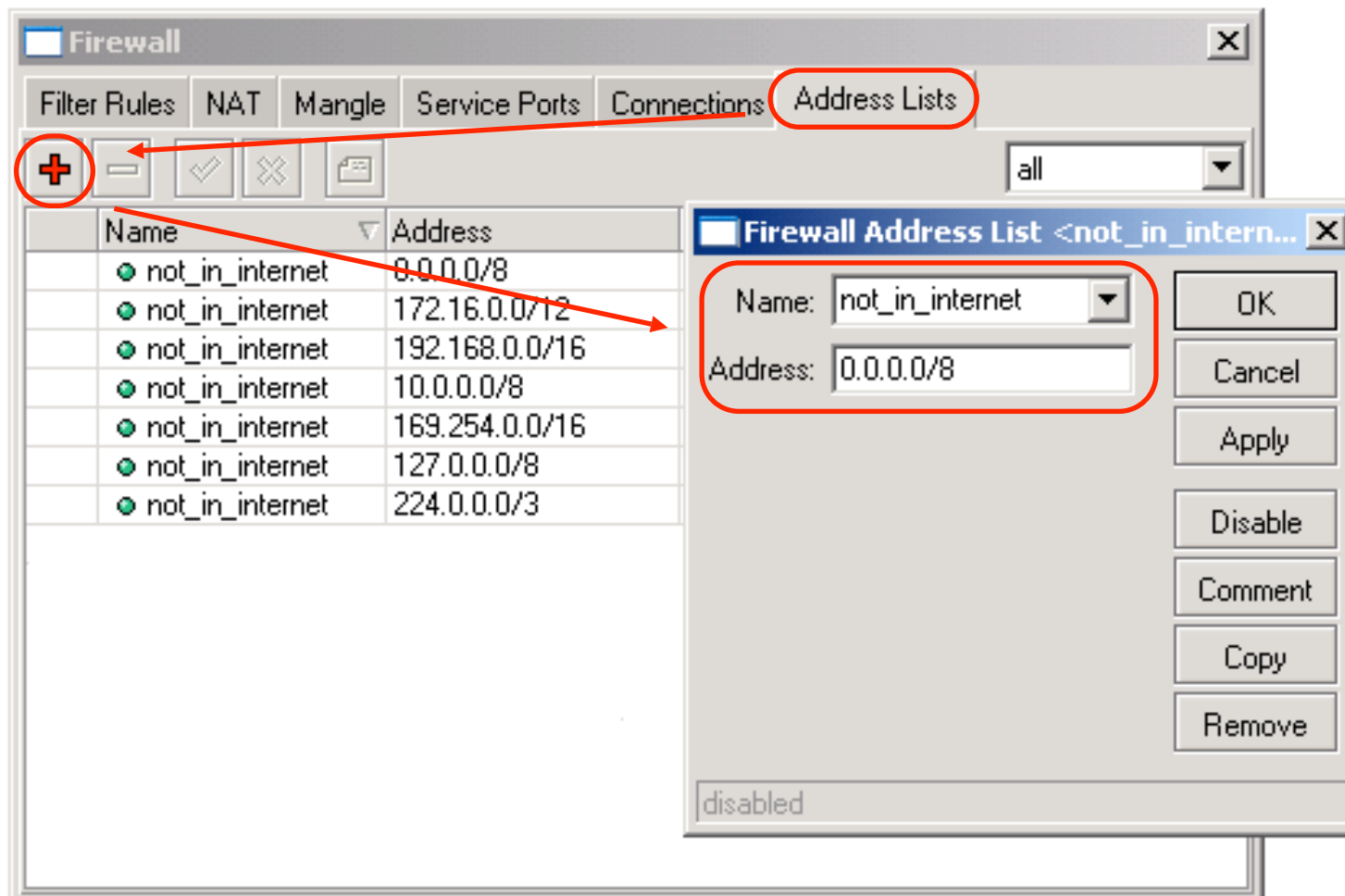
- At the moment there are few hundreds active trojans and less than 50 active worms
- You can download the complete “virus port blocker” chain (~330 drop rules with ~500 blocked virus ports) from <ftp://admin@10.1.1.254>
- Some viruses and trojans use standard services ports and can **not** be blocked.

Bogon IPs

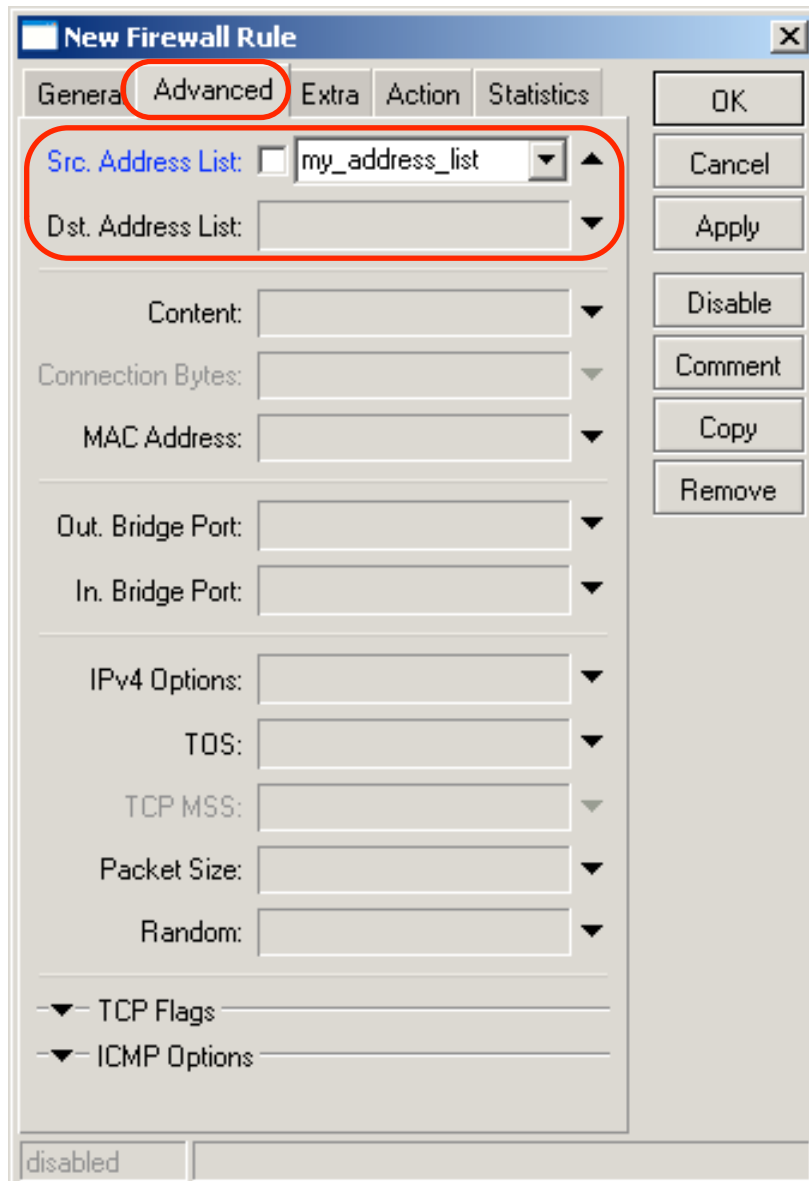
- There are ~4,3 billion IPv4 addresses
- There are several IP ranges restricted in public network
- There are several of IP ranges reserved (not used at the moment) for specific purposes
- There are lots of unused IP ranges!!!
- You can find information about all unused IP ranges at:
<http://www.cidr-report.org/as2.0/#Bogons>

Address List Lab

- Make an address list of the most common bogon IP addresses



Address List Options



- Instead of creating one filter rule for each IP network address, you can create only one rule for IP address list.
- Use “Src./Dst. Address List” options
- Create an address list in “/ip firewall address-list” menu

Address Filtering Lab

- Allow packets to enter your network only from the valid Internet addresses
- Allow packets to enter your network only to the valid customer addresses
- Allow packets to leave your network only from the valid customers addresses
- Allow packets to leave your network only to the valid Internet addresses

User-defined Chains

Firewall structure, chain reusability

ICMP Protocol

- Internet Control Message Protocol (ICMP) is basic network troubleshooting tool, it should be allowed to bypass the firewall
- Typical IP router uses only five types of ICMP messages (type:code)
 - ◆ For PING - messages **0:0** and **8:0**
 - ◆ For TRACEROUTE – messages **11:0** and **3:3**
 - ◆ For Path MTU discovery – message **3:4**
- Any other type ICMP messages should be blocked

ICMP Message Rule Example

The screenshot shows the 'Firewall Rule' configuration window with the 'General' tab selected. The 'Chain' dropdown is set to 'ICMP' and the 'Protocol' dropdown is set to '1 (icmp)'. Both are circled in red. The status bar at the bottom indicates the rule is 'disabled'.

Firewall Rule

General | Advanced | Extra | Action | Statistics

Chain: ICMP

Src. Address:

Dst. Address:

Protocol: 1 (icmp)

Src. Port:

Dst. Port:

P2P:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark:

Routing Mark:

Connection State:

Connection Type:

disabled

The screenshot shows the 'Firewall Rule' configuration window with the 'Advanced' tab selected. The 'ICMP Options' section is expanded, showing 'ICMP Type' set to '8 (echo request)' and 'ICMP Code' checked with '0'. Both the 'Advanced' tab and the 'ICMP Options' section are circled in red. The status bar at the bottom indicates the rule is 'disabled'.

Firewall Rule

General | Advanced | Extra | Action | Statistics

Src. Address List:

Dst. Address List:

Content:

Connection Bytes:

MAC Address:

Out. Bridge Port:

In. Bridge Port:

IPv4 Options:

TOS:

TCP MSS:

Packet Size:

Random:

TCP Flags:

ICMP Options

ICMP Type: 8 (echo request)

ICMP Code: 0

disabled

ICMP Chain Lab

- Make a new chain – ICMP
 - ◆ **Accept 5** necessary ICMP messages
 - ◆ **Drop** all other ICMP packets
- Move all ICMP packets to the ICMP chain
 - ◆ Create an action “**jump**” rule in the chain Input
 - ◆ Place it accordingly
 - ◆ Create an action “**jump**” rule in the chain Forward
 - ◆ Place it accordingly

ICMP Jump Rule

New Firewall Rule

General | Advanced | Extra | Action | Statistics

Chain: forward

Src. Address:

Dst. Address:

Protocol: 1 (icmp)

Src. Port:

Dst. Port:

P2P:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark:

Routing Mark:

Connection State:

Connection Type:

disabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove

New Firewall Rule

General | Advanced | Extra | Action | Statistics

Action: jump

Jump Target: ICMP

disabled

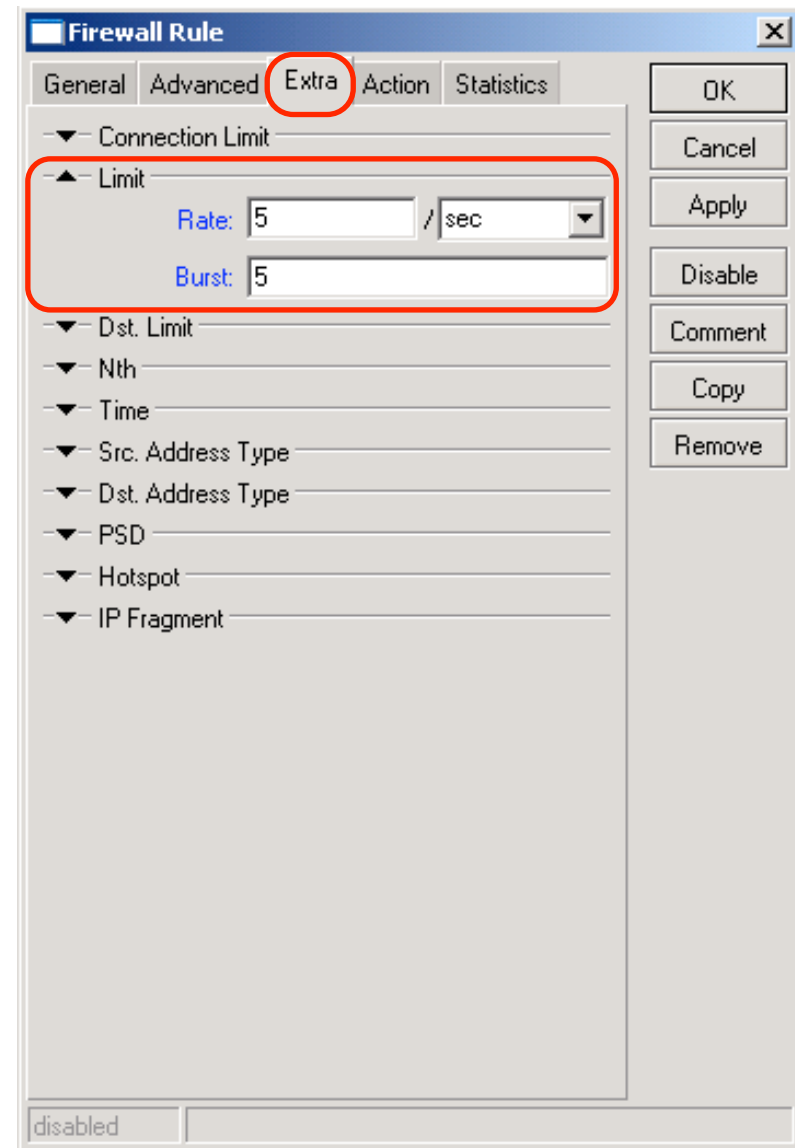
OK
Cancel
Apply
Disable
Comment
Copy
Remove

Network Intrusion Types

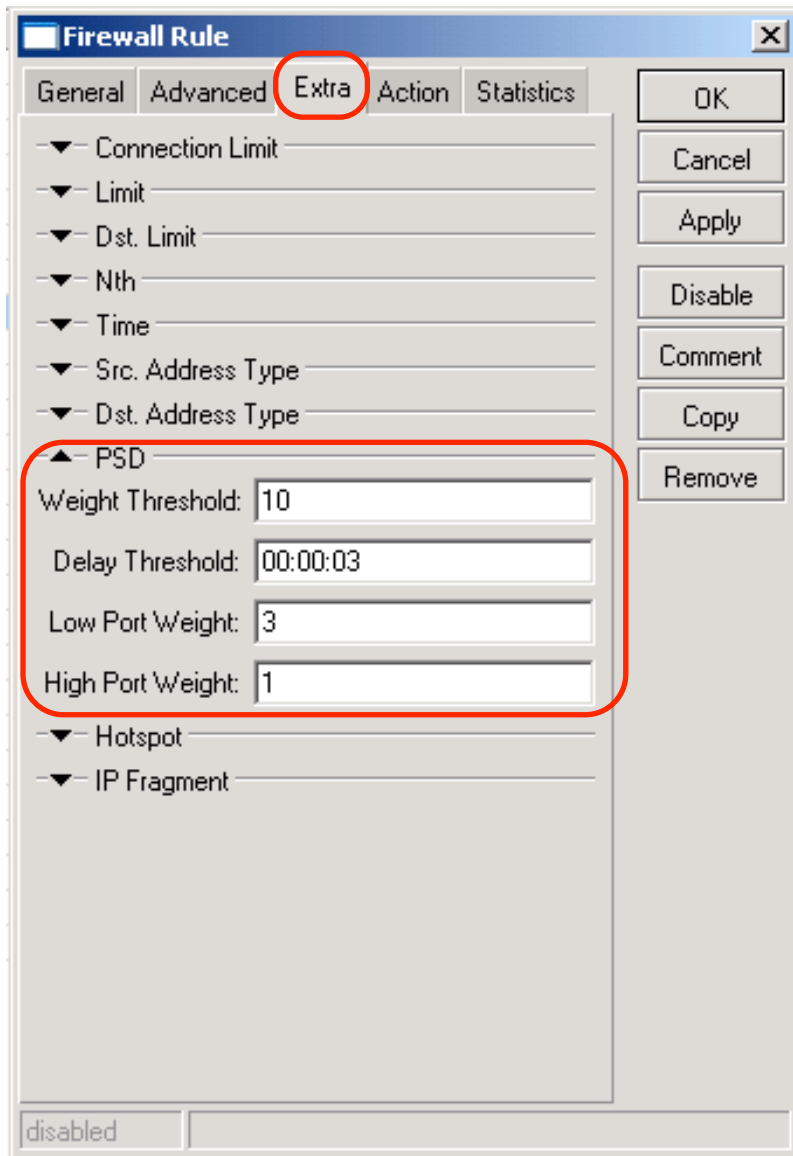
- Network intrusion is a serious security risk that could result not only in temporary service denial, but also in total refusal of network service
- We can point out 4 major network intrusion types:
 - ◆ Ping flood
 - ◆ Port scan
 - ◆ DoS attack
 - ◆ DDoS attack

Ping Flood

- Ping flood usually consists of loads of random ICMP messages
- With “limit” condition it is possible to bound the rule match rate to a given limit
- This condition is often used with action “log”



Port Scan



- Port Scan is sequential TCP (UDP) port probing
- PSD (Port scan detection) works only for TCP protocol
- Low ports
 - ◆ From 0 to 1023
- High ports
 - ◆ From 1024 to 65535

Intrusion Protection Lab

- Adjust all 5 accept rules in the chain ICMP to match rate 5 packets per second with 5 packet burst possibility
- Create PSD protection
 - ◆ Create a PSD drop rule in the chain Input
 - ◆ Place it accordingly
 - ◆ Create a PSD drop rule in the chain Forward
 - ◆ Place it accordingly

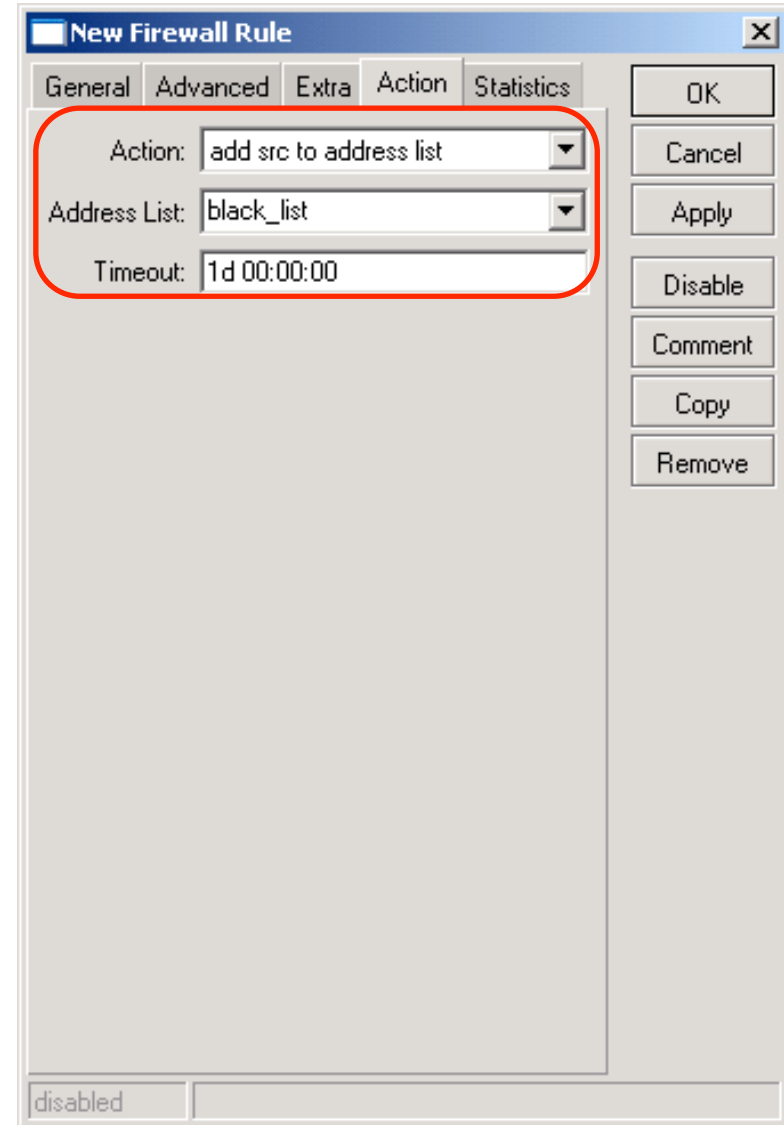
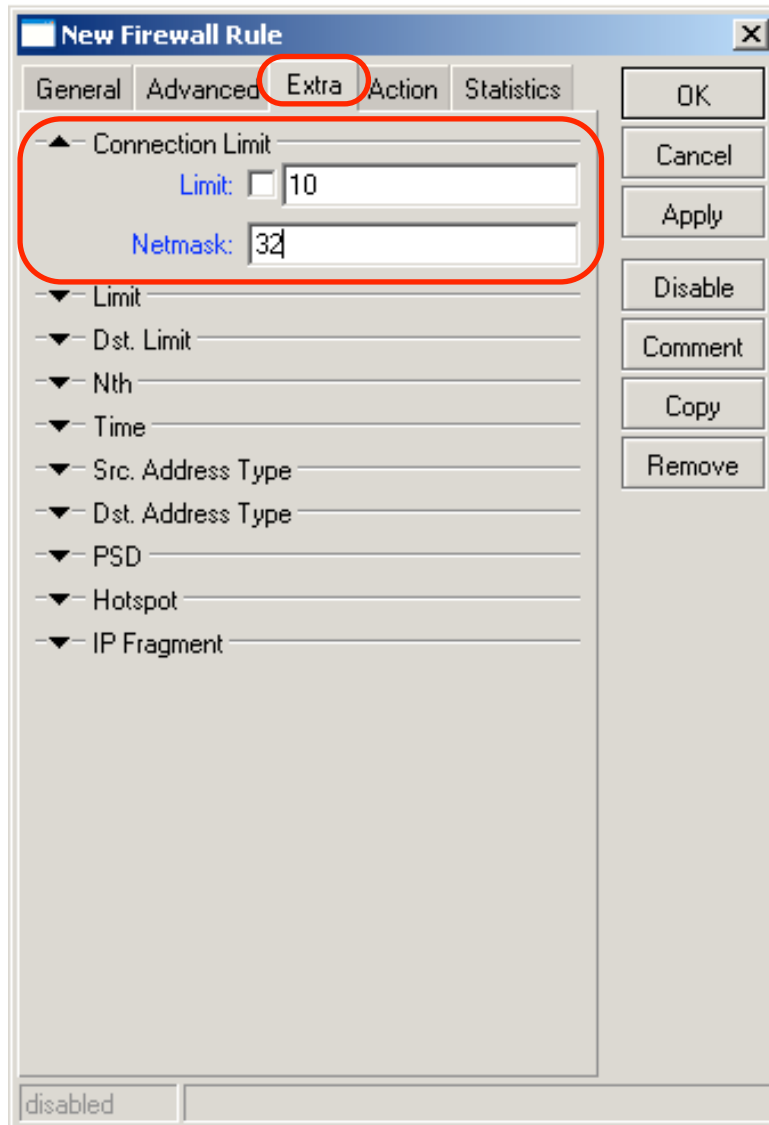
DoS Attacks

- Main target for DoS attacks is consumption of resources, such as CPU time or bandwidth, so the standard services will get Denial of Service (DoS)
- Usually router is flooded with TCP/SYN (connection request) packets. Causing the server to respond with a TCP/SYN-ACK packet, and waiting for a TCP/ACK packet.
- Mostly DoS attackers are virus infected customers

DoS Attack Protection

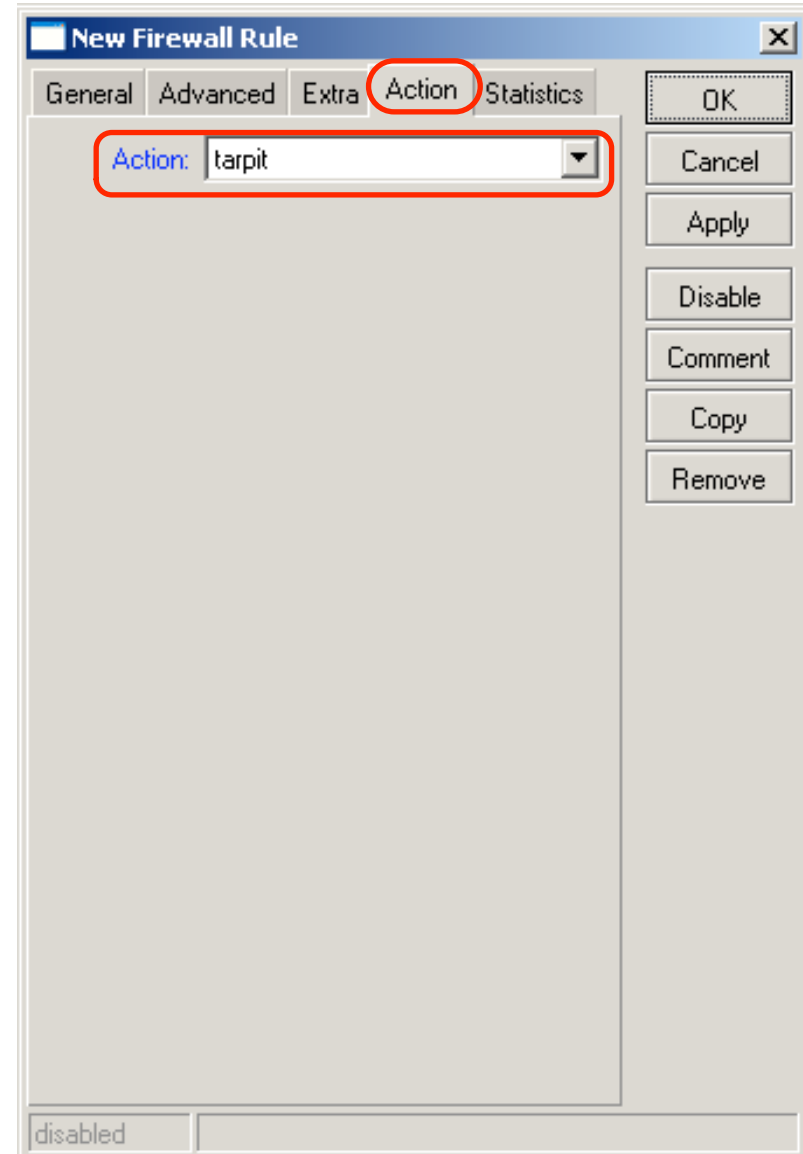
- All IP's with more than 10 connections to the router should be considered as DoS attackers
- With every dropped TCP connection we will allow attacker to create new connection
- We should implement DoS protection into 2 steps:
 - ◆ Detection - Creating a list of DoS attackers on the basis of connection-limit
 - ◆ Suppression – applying restrictions to the detected DoS attackers

DoS Attack Detection



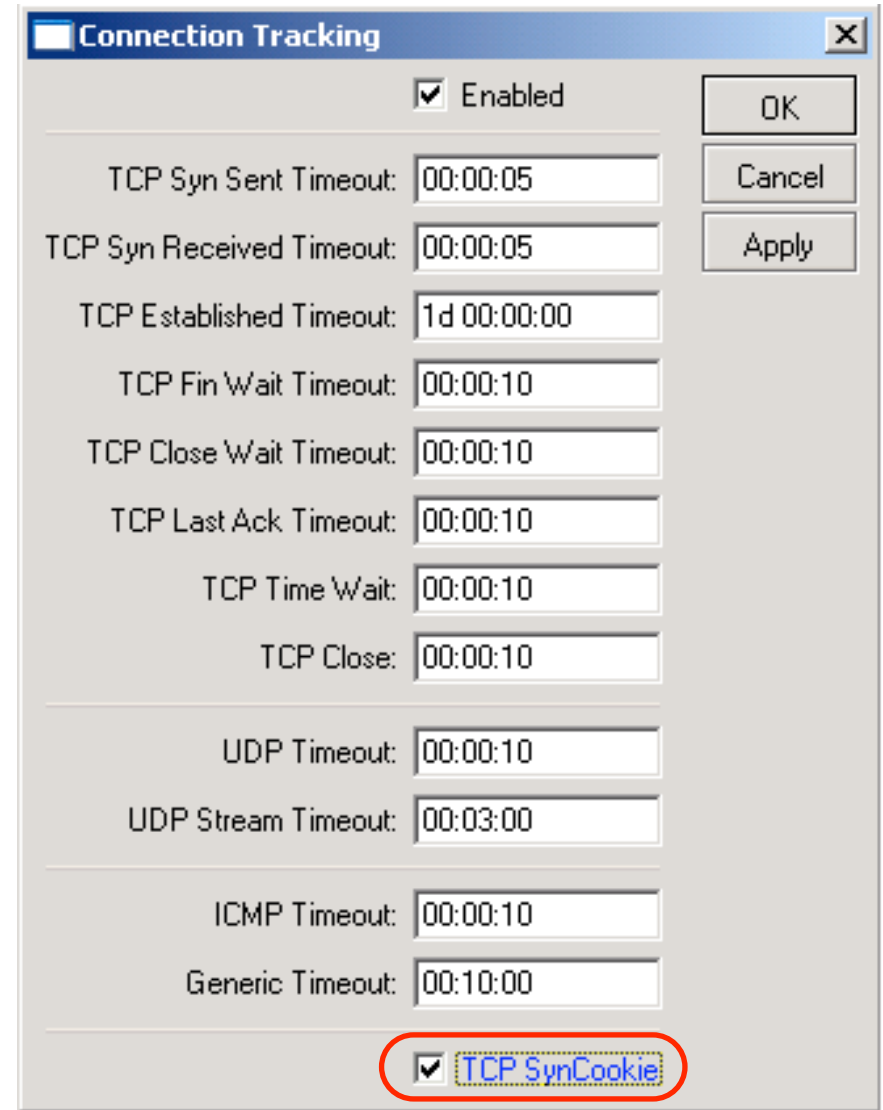
DoS Attack Suppression

- To bound the attacker from creating a new connections, we will use action “tarpit”
- We must place this rule before the detection rule or else address-list entry will rewrites all the time



DDoS attacks

- A Distributed Denial of Service attack is very similar to DoS attack only it occurs from **multiple** compromised systems
- Only thing that could help is “TCPSyn Cookie” option in conntrack system



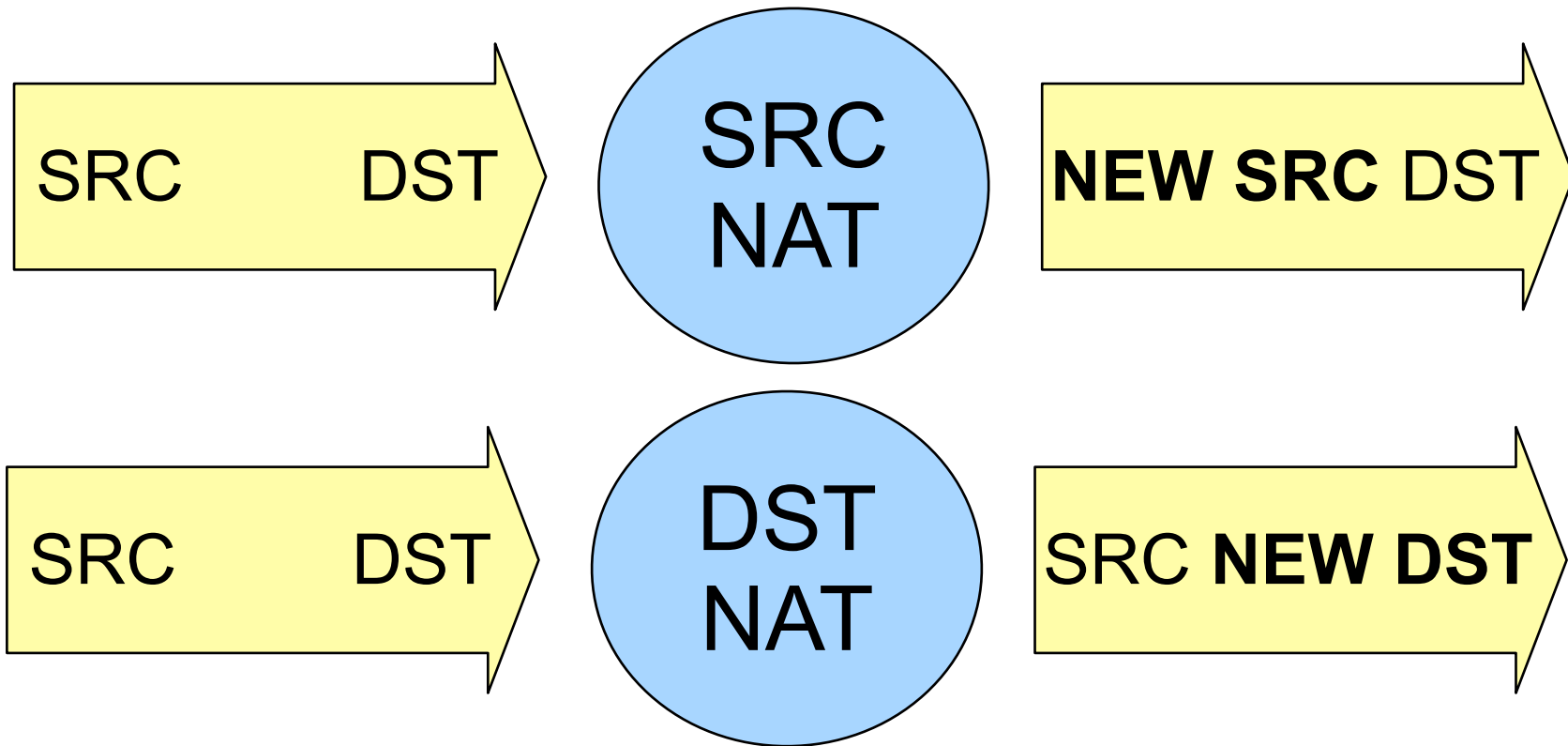
Network Address Translation (NAT)

Destination NAT, Source NAT, NAT traversal

NAT Types

- As there are two IP addresses and ports in an IP packet header, there are two types of NAT
 - ◆ The one, which rewrites source IP address and/or port is called source NAT (src-nat)
 - ◆ The other, which rewrites destination IP address and/or port is called destination NAT (dst-nat)
 - ◆ Firewall NAT rules process only the first packet of each connection (connection state “new” packets)

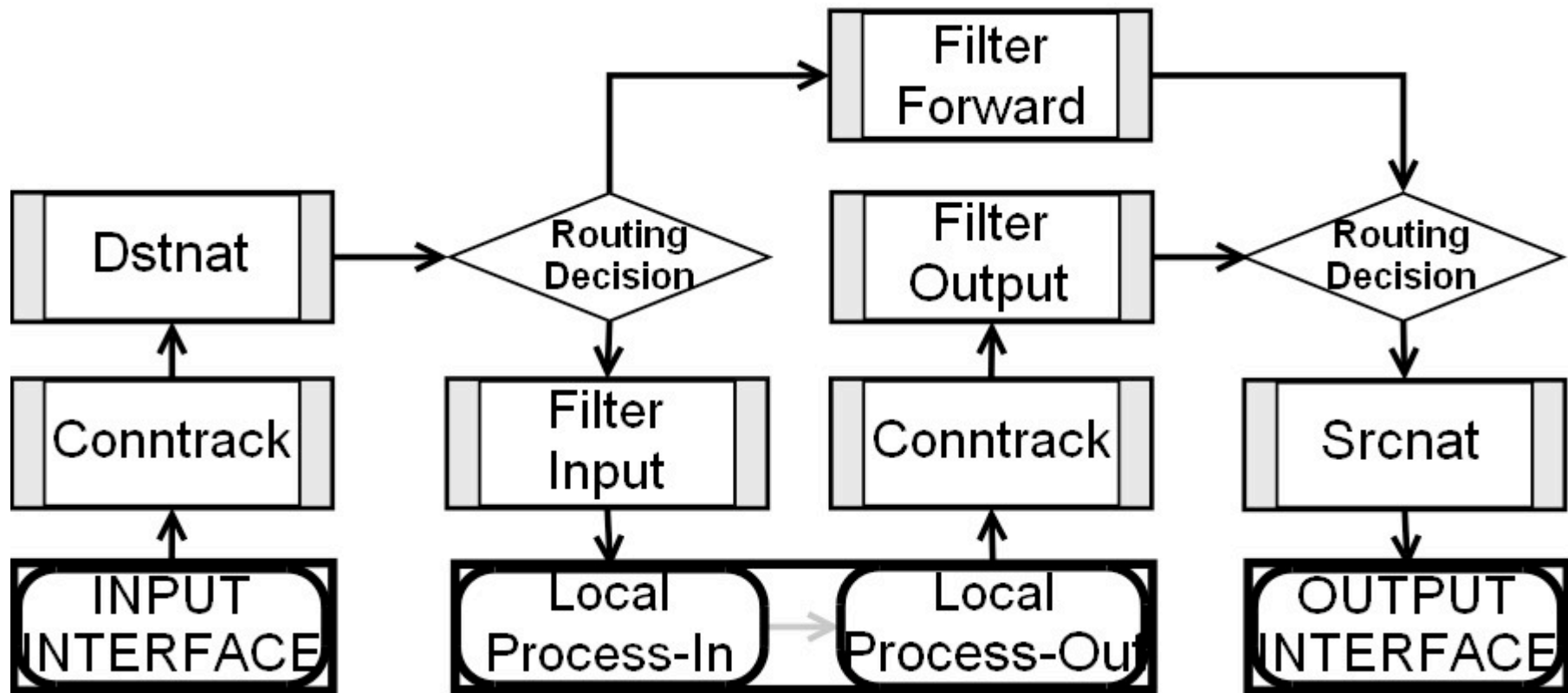
NAT Type Diagrams



Firewall NAT Structure

- Firewall NAT rules are organized in chains
- There are two default chains
 - ◆ **dstnat** – processes traffic sent to and through the router, before it divides in to “input” and “forward” chain of firewall filter.
 - ◆ **srcnat** – processes traffic sent from and through the router, after it merges from “output” and “forward” chain of firewall filter.
- There are also user-defined chains

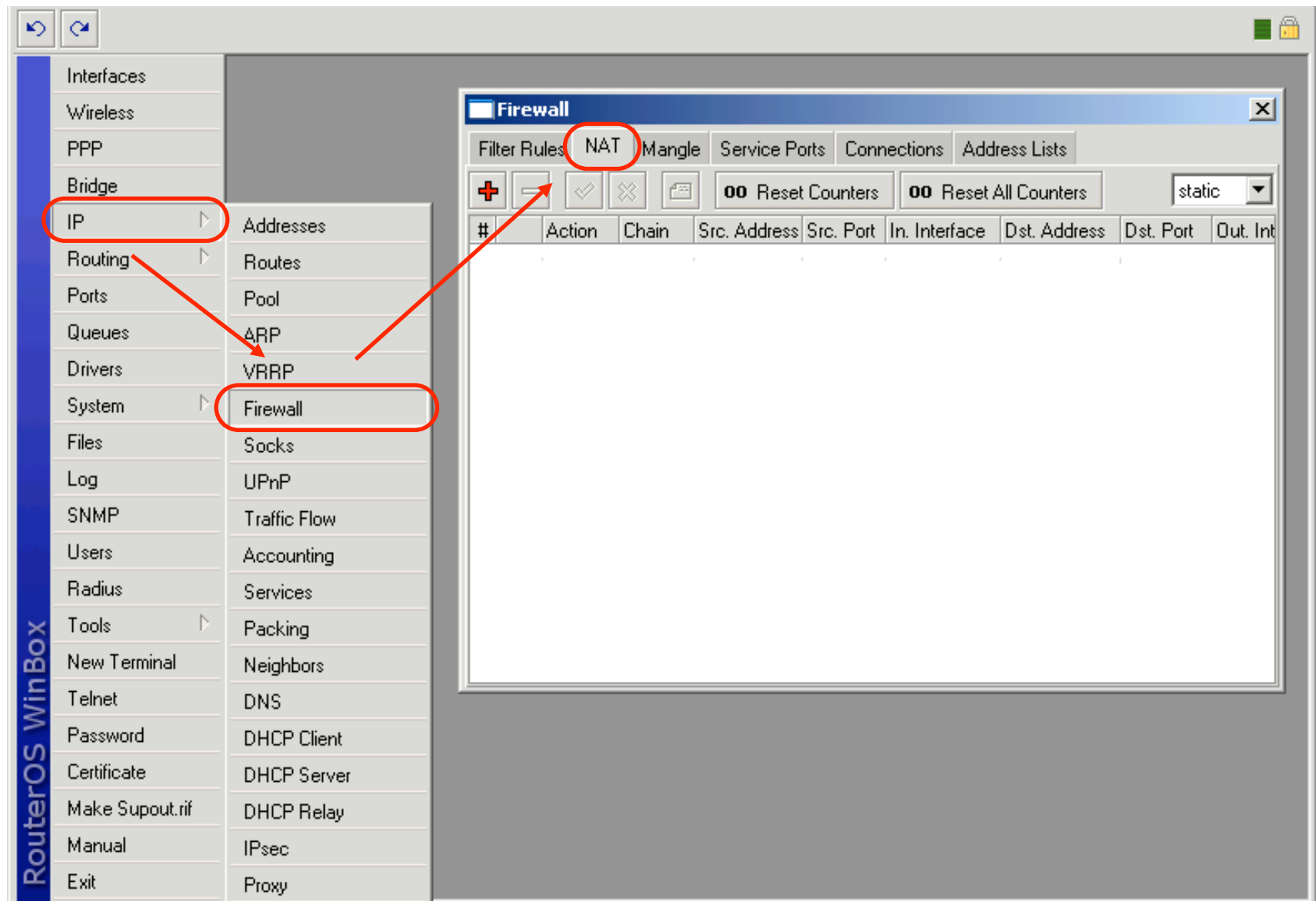
IP Firewall Diagram



Firewall NAT

- The firewall NAT facility is a tool for rewriting packet's header information.
- Firewall NAT consist from the sequence of IF-THEN rules
 - 0) IF <condition(s)> THEN <action>
 - 1) IF <condition(s)> THEN <action>
 - 2) IF <condition(s)> THEN <action>
- If a packet doesn't meet all the conditions of the rule, it will be sent on to the next rule.
- If a packet meet all the conditions of the rule, specified action will be performed on it.

NAT Rules - Winbox View



NAT Actions

- There are 6 specific actions in the NAT
 - ◆ dst-nat
 - ◆ redirect
 - ◆ src-nat
 - ◆ masquarade
 - ◆ netmap
 - ◆ same
- There are 7 more actions in the NAT, but they are exactly the same as in firewall filters

Src-nat

- Action “src-nat” changes packet's source address and/or port to specified address and/or port
- This action can take place only in chain srcnat
- Typical application: hide specific LAN resources behind specific public IP address

Src-nat Rule Example

The screenshot shows the 'New NAT Rule' dialog box with the 'General' tab selected. The 'Chain' dropdown is set to 'srcnat'. The 'Src. Address' field contains '192.168.XY.0/24'. The 'Dst. Address' field is empty. The 'Protocol', 'Src. Port', and 'Dst. Port' fields are also empty. The 'In. Interface', 'Out. Interface', 'Packet Mark', 'Connection Mark', 'Routing Mark', and 'Connection Type' fields are empty. The 'disabled' status is shown at the bottom left. The 'Action' tab is highlighted with a red circle.

New NAT Rule [X]

General | Advanced | Extra | Action | Statistics

Chain: srcnat

Src. Address: 192.168.XY.0/24

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark:

Routing Mark:

Connection Type:

disabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove

The screenshot shows the 'New NAT Rule' dialog box with the 'Action' tab selected. The 'Action' dropdown is set to 'src-nat'. The 'To Addresses' field contains '10.1.1.XY'. The 'To Ports' field contains '0-65535'. The 'disabled' status is shown at the bottom left. The 'General' tab is highlighted with a red circle.

New NAT Rule [X]

General | Advanced | Extra | Action | Statistics

Action: src-nat

To Addresses: 10.1.1.XY

To Ports: 0-65535

disabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove

Masquerade

- Action “masquerade” changes packet's source address router's address and specified port
- This action can take place only in chain srcnat
- Typical application: hide specific LAN resources behind one dynamic public IP address

Masquerade Rule Example

The screenshot shows the 'New NAT Rule' dialog box with the 'General' tab selected. The 'Chain' is set to 'srcnat' and 'Src. Address' is '192.168.XY.0/24'. Other fields like 'Dst. Address', 'Protocol', 'Src. Port', 'Dst. Port', 'In. Interface', 'Out. Interface', 'Packet Mark', 'Connection Mark', 'Routing Mark', and 'Connection Type' are empty. The 'disabled' checkbox is checked. The 'Action' tab is visible but not selected.

New NAT Rule

General | Advanced | Extra | Action | Statistics

Chain: srcnat

Src. Address: 192.168.XY.0/24

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark:

Routing Mark:

Connection Type:

disabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove

The screenshot shows the 'New NAT Rule' dialog box with the 'Action' tab selected. The 'Action' is set to 'masquerade'. The 'disabled' checkbox is checked. The 'General' tab is visible but not selected.

New NAT Rule

General | Advanced | Extra | Action | Statistics

Action: masquerade

disabled

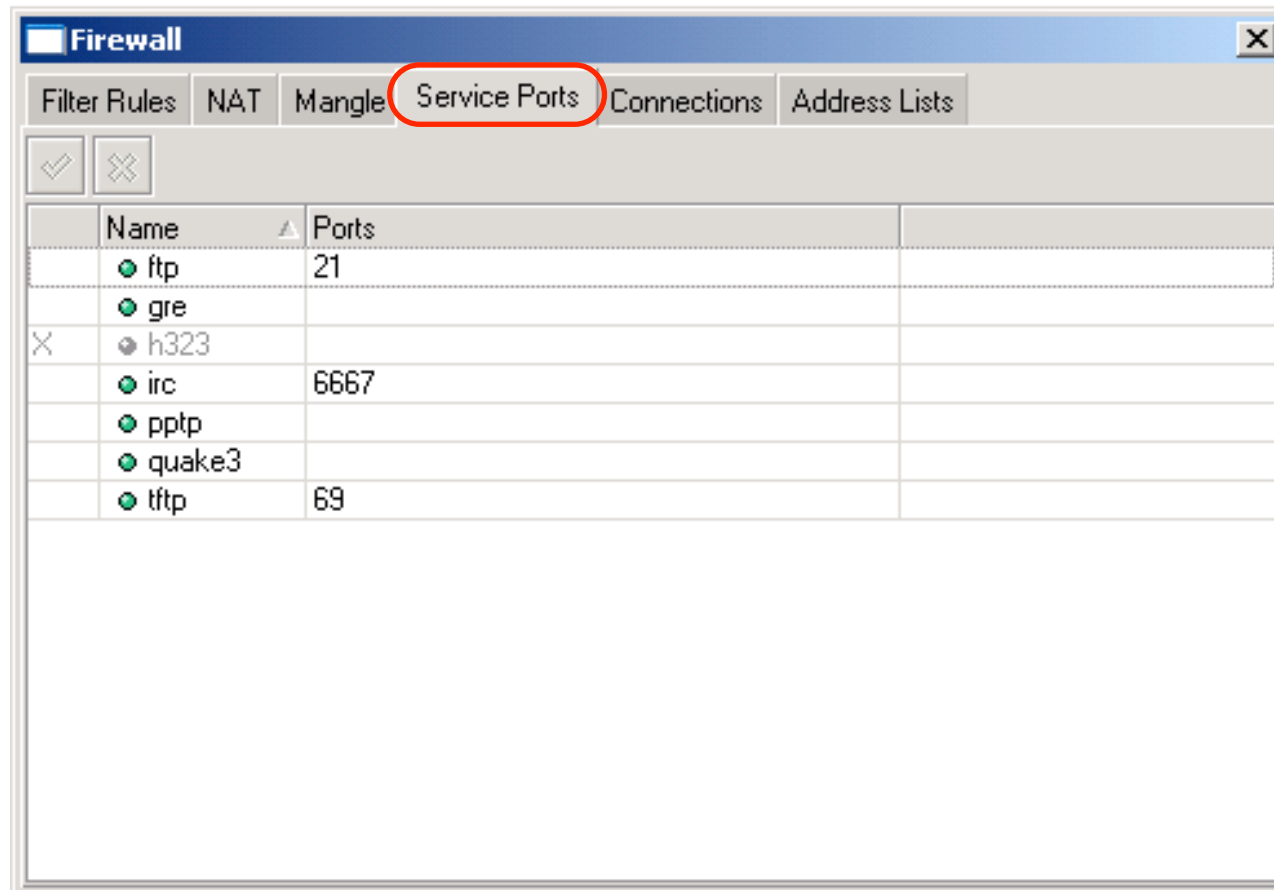
OK
Cancel
Apply
Disable
Comment
Copy
Remove

Source NAT Issues

- Hosts behind a NAT-enabled router do not have true end-to-end connectivity:
 - ◆ connection initiation from outside is not possible
 - ◆ some TCP services will work in “passive” mode
 - ◆ src-nat behind several IP addresses is unpredictable
 - ◆ some protocols will require so-called NAT helpers to work correctly (NAT traversal)

NAT Helpers

- You can specify ports for existing NAT helpers, but you can not add new helpers



Src-nat Lab

- You have been assigned one “public” IP address 172.16.0.XY/32
- Assign it to the wireless interface
- Add src-nat rule to “hide” your private network 192.168.XY.0/24 behind the “public” address
- Connect from your laptop using winbox, ssh, or telnet via your router to the main gateway 10.1.1.254
- Check the IP address you are connecting from (use “/user active print” on the main gateway)

Dst-nat

- Action “dst-nat” changes packet's destination address and port to specified address and port
- This action can take place only in chain dstnat
- Typical application: ensure access to local network services from public network

Dst-nat Rule Example

The screenshot shows the 'New NAT Rule' dialog box with the 'General' tab selected. The 'Chain' is set to 'dstnat'. The 'Dst. Address' is '10.1.1.XY/32'. The 'Protocol' is '6 (tcp)'. The 'Dst. Port' is '25'. The 'Status' is 'disabled'.

New NAT Rule [X]

General | Advanced | Extra | Action | Statistics

Chain: dstnat

Src. Address: []

Dst. Address: 10.1.1.XY/32

Protocol: 6 (tcp)

Src. Port: []

Dst. Port: 25

In. Interface: []

Out. Interface: []

Packet Mark: []

Connection Mark: []

Routing Mark: []

Connection Type: []

disabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove

The screenshot shows the 'New NAT Rule' dialog box with the 'Action' tab selected. The 'Action' is 'dst-nat'. The 'To Addresses' is '192.168.XY.100'. The 'To Ports' is '25'. The 'Status' is 'disabled'.

New NAT Rule [X]

General | Advanced | Extra | Action | Statistics

Action: dst-nat

To Addresses: 192.168.XY.100

To Ports: 25

disabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove

Redirect

- Action “redirect” changes packet's destination address to router's address and specified port
- This action can take place only in chain dstnat
- Typical application: transparent proxying of network services (DNS,HTTP)

Redirect Rule Example

The screenshot shows the 'New NAT Rule' dialog box with the 'General' tab selected. The 'Chain' is set to 'dstnat'. The 'Dst. Address' is '10.1.1.XY/32'. The 'Protocol' is '6 (tcp)'. The 'Dst. Port' is '80'. The 'In. Interface' has a 'Set to default' tooltip. The status at the bottom is 'disabled'.

New NAT Rule

General | Advanced | Extra | Action | Statistics

Chain: dstnat

Src. Address:

Dst. Address: 10.1.1.XY/32

Protocol: 6 (tcp)

Src. Port:

Dst. Port: 80

In. Interface: Set to default

Out. Interface:

Packet Mark:

Connection Mark:

Routing Mark:

Connection Type:

disabled

The screenshot shows the 'New NAT Rule' dialog box with the 'Action' tab selected. The 'Action' is set to 'redirect'. The 'To Ports' is '8080'. The status at the bottom is 'disabled'.

New NAT Rule

General | Advanced | Extra | Action | Statistics

Action: redirect

To Ports: 8080

disabled

Redirect Lab

- Capture all TCP and UDP port 53 packets originated from your private network 192.168.XY.0/24 and redirect them to the router itself.
- Set your laptop's DNS server to some random IP address
- Clear your router's DNS cache
- Try to open a previously unseen Internet page
- Take a look at the DNS cache of the router

Dst-nat Lab

- Capture all TCP port 80 (HTTP) packets originated from your private network 192.168.XY.0/24 and change destination address to 10.1.2.1 using dst-nat rule
- Clear your browser's cache on the laptop
- Try browsing the Internet

Netmap and Same

- **Netmap** - creates a static 1:1 mapping of one set of IP addresses to another one. Often used to distribute public IP addresses to hosts on private networks
- **Same** - gives a particular client the same source/destination IP address from the supplied range for any connection. Used for services that expect constant IP address for multiple connections from the same client

Firewall Mangle

IP packet marking and IP header fields adjustment

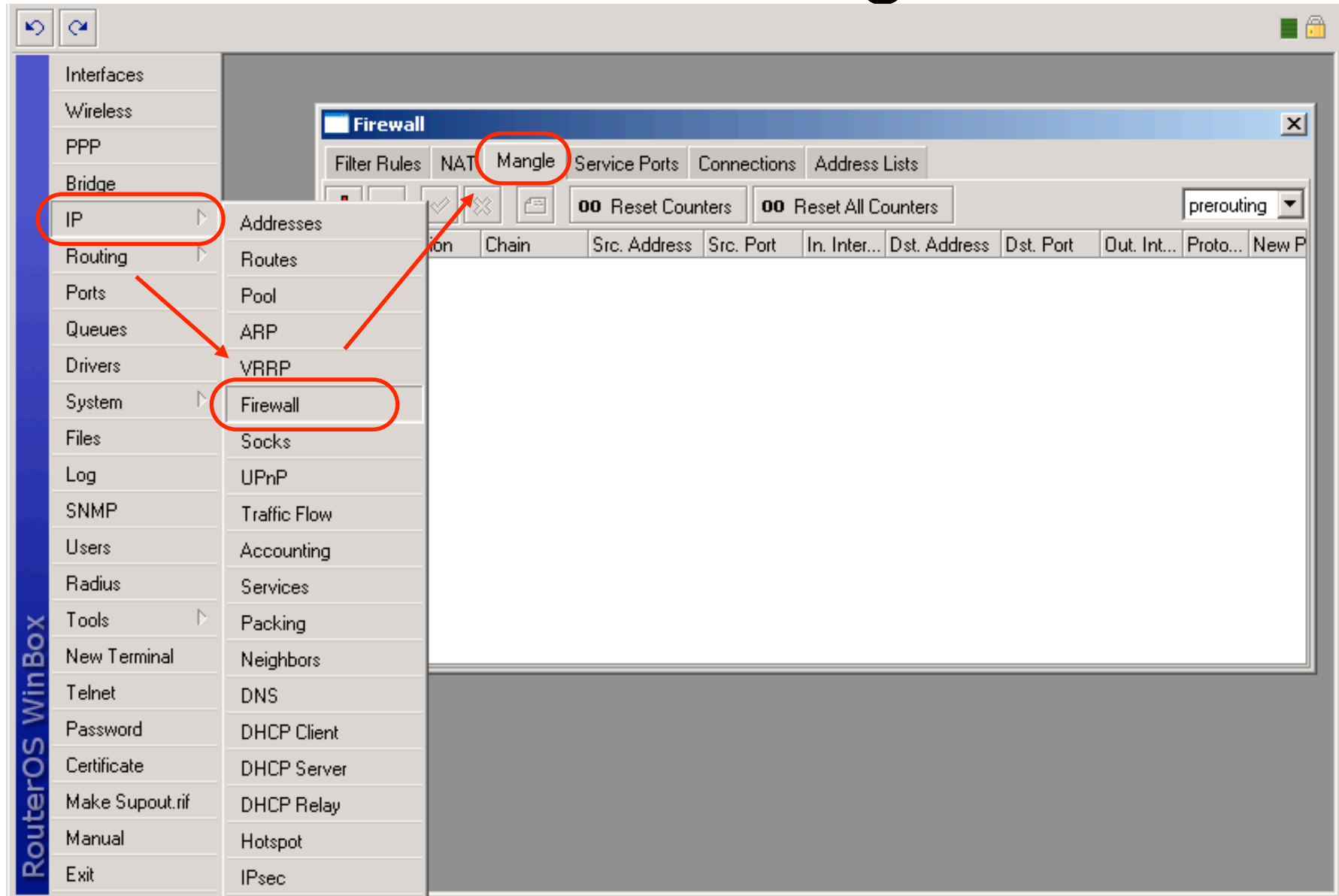
What is Mangle?

- The mangle facility allows to mark IP packets with special marks.
- These marks are used by other router facilities to identify the packets.
- Additionally, the mangle facility is used to modify some fields in the IP header, like TOS (DSCP) and TTL fields.

Firewall Mangle

- The firewall filter facility is a tool for packet marking
- Firewall filters consist from the sequence of IF-THEN rules
 - 0) IF <condition(s)> THEN <action>
 - 1) IF <condition(s)> THEN <action>
 - 2) IF <condition(s)> THEN <action>
- If a packet doesn't meet all the conditions of the rule, it will be sent on to the next rule.
- If a packet meet all the conditions of the rule, specified action will be performed on it.

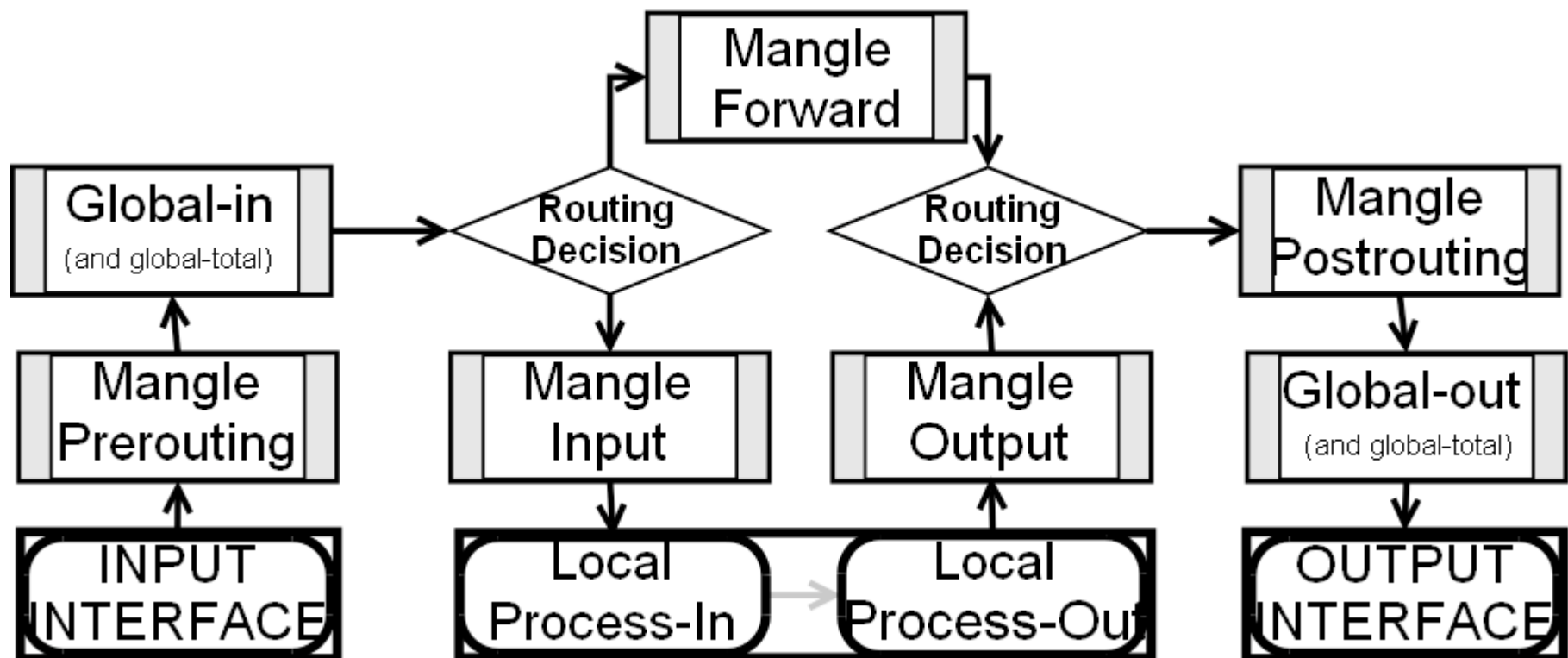
Firewall Mangle



Mangle Structure

- Mangle rules are organized in chains
- There are five built-in chains:
 - ◆ Prerouting- making a mark before Global-In queue
 - ◆ Postrouting - making a mark before Global-Out queue
 - ◆ Input - making a mark before Input filter
 - ◆ Output - making a mark before Output filter
 - ◆ Forward - making a mark before Forward filter
- New user-defined chains can be added, as necessary

Mangle and Queue Diagram (simple)



Mangle actions

- There are 7 more actions in the mangle:
 - ◆ **mark-connection – mark connection (from a single packet)**
 - ◆ **mark-packet – mark a flow (all packets)**
 - ◆ **mark-routing - mark packets for policy routing**
 - ◆ **change MSS - change maximum segment size of the packet**
 - ◆ **change TOS - change type of service**
 - ◆ **change TTL - change time to live**
 - ◆ **strip IPv4 options**

Marking Connections

- Use mark connection to identify one or group of connections with the specific connection mark
- Connection marks are stored in the connection tracking table
- There can be only one connection mark for one connection.
- Connection tracking helps to associate each packet to a specific connection (connection mark)

Mark Connection Rule

Mangle Rule <->any:80>

General | **Advanced** | Extra | Action | Statistics

Chain: prerouting

Src. Address:

Dst. Address:

Protocol: 6 (tcp)

Src. Port:

Dst. Port: 80

P2P:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark:

Routing Mark:

Connection State:

Connection Type:

disabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove

Mangle Rule <->any:80>

General | Advanced | Extra | **Action** | Statistics

Action: mark connection

New Connection Mark: HTTP_conn

Passthrough

disabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove

Marking Packets

- Packets can be marked
 - ◆ Indirectly. Using the **connection tracking** facility, based on previously created **connection marks** (faster)
 - ◆ Directly. Without the **connection tracking** - no connection marks necessary, router will compare **each** packet to a given conditions (this process imitates some of the connection tracking features)

Mark Packet Rule

New Mangle Rule

General | Advanced | Extra | Action | Statistics

Chain: prerouting

Src. Address:

Dst. Address:

Protocol:

Src. Port:

Dst. Port:

P2P:

In. Interface:

Out. Interface:

Packet Mark:

Connection Mark: HTTP_conn

Routing Mark:

Connection State:

Connection Type:

disabled

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

New Mangle Rule

General | Advanced | Extra | Action | Statistics

Action: mark packet

New Packet Mark: HTTP_packets

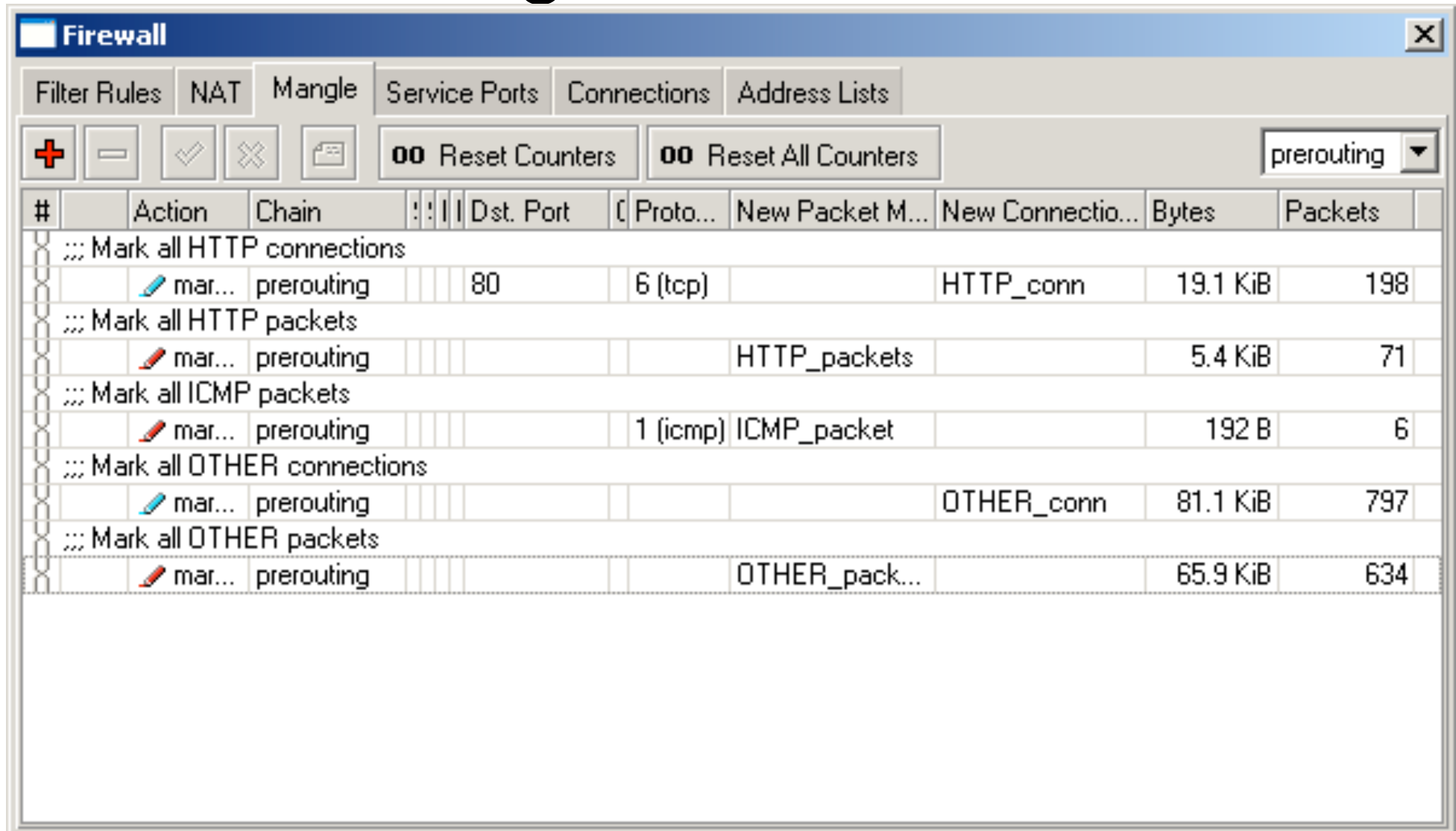
Passthrough

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

Mangle Lab

- Mark all HTTP connections
- Mark all packets from HTTP connections
- Mark all ICMP packets
- Mark all other connections
- Mark all packets from other connections
- Check the configuration

Mangle Lab Result



The screenshot shows the Mikrotik WinBox Firewall Mangle configuration window. The 'prerouting' chain is selected. The table below displays the configuration and statistics for several mangle rules.

#	Action	Chain	Dst. Port	Proto...	New Packet M...	New Connectio...	Bytes	Packets
::: Mark all HTTP connections								
	mar...	prerouting	80	6 (tcp)		HTTP_conn	19.1 KiB	198
::: Mark all HTTP packets								
	mar...	prerouting				HTTP_packets	5.4 KiB	71
::: Mark all ICMP packets								
	mar...	prerouting		1 (icmp)		ICMP_packet	192 B	6
::: Mark all OTHER connections								
	mar...	prerouting				OTHER_conn	81.1 KiB	797
::: Mark all OTHER packets								
	mar...	prerouting				OTHER_pack...	65.9 KiB	634

MikroTik RouterOS – QoS

Quality of Service

Simple limitation using Simple Queues.
Traffic marking using Firewall Mangle.
Traffic prioritization using Queue Tree.

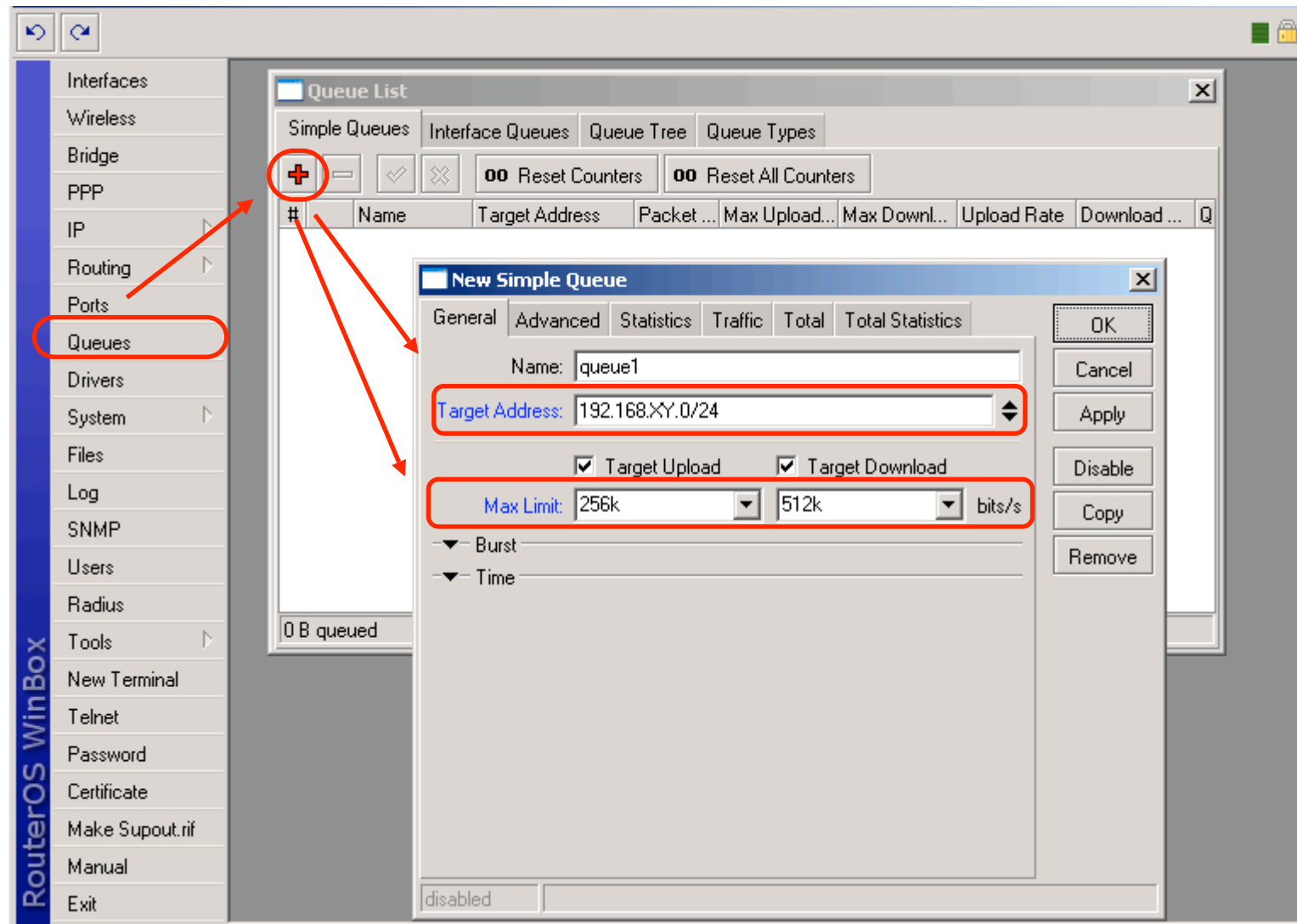
Speed Limiting

- Forthright control over data rate of inbound traffic is impossible
- The router controls the data rate indirectly by dropping incoming packets
- TCP protocol adapts itself to the effective connection speed
- Simple Queue is the easiest way to limit data rate

Simple Queues

- Simple queues make data rate limitation easy. One can limit:
 - ◆ Client's rx rate (client's download)
 - ◆ Client's tx rate (client's upload)
 - ◆ Client's tx + rx rate (client's aggregate)
- While being easy to configure, Simple Queues give control over all QoS features

Simple Limitation



Simple Queue Lab

- **Restore configuration backup (slide 12)**
- Create on simple queue to limit your local network's upload/download data rate to 256Kbps/512Kbps
- Check the limitation!
- Create another simple queue to limit your laptop's upload/download data rate to 64Kbps/128Kbps
- Check the limitation!
- Reorder queues

Limitation and QoS

- QoS is not only limitation!
- QoS is an attempt to use the existing resources rationally (it is not of an interest not to use all the available speed)
- QoS balances and prioritizes the traffic flow and prevents monopolizing the (always too narrow) channel. That is why it is called “Quality of Service”

QoS Basic Principles

- QoS is implemented not only by limitations, but by additional queuing mechanism like:
 - ◆ Burst
 - ◆ Dual limitation
 - ◆ Queue hierarchy
 - ◆ Priority
 - ◆ Queue discipline
- Queuing disciplines control the order and speed of packets going out through the interface

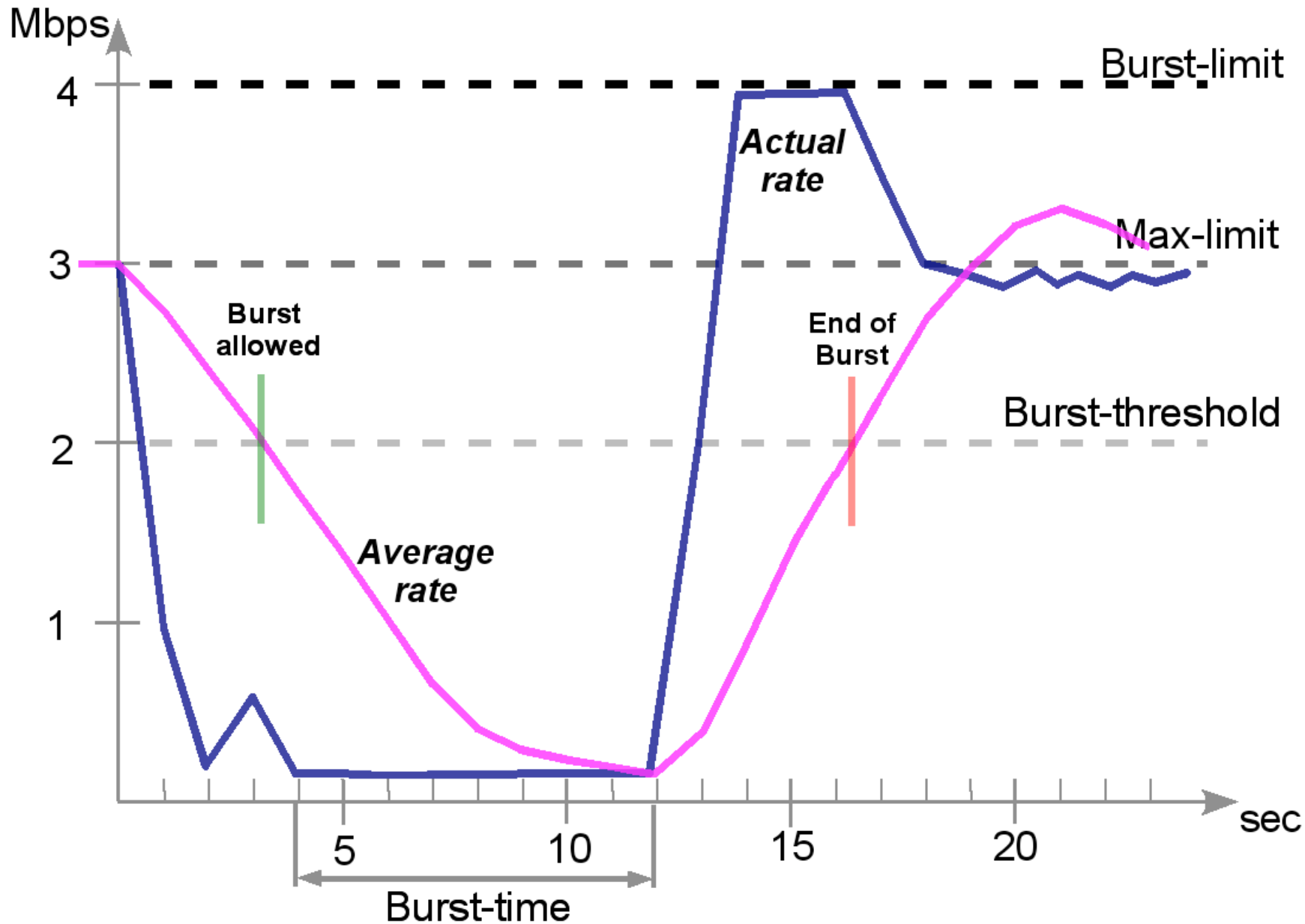
Burst

- Burst is one of the means to ensure QoS
- Bursts are used to allow higher data rates for a short period of time
- If an average data rate is less than **burst-threshold**, burst could be used (actual data rate can reach **burst-limit**)
- Average data rate is calculated from the last **burst-time** seconds

Average Data Rate

- Average data rate is calculated as follows:
 - ◆ **burst-time** is being divided into 16 periods
 - ◆ router calculates the **average data rate** of each class over these small periods
- Note, that the **actual burst period** is not equal to the burst-time. It can be several times shorter than the burst-time depending on the max-limit, burst-limit, burst-threshold, and actual data rate history (see the graph example on the next slide)

Limitation with Burst



Limitation with Burst

The screenshot displays the RouterOS WinBox interface. On the left sidebar, the 'Queues' menu item is highlighted with a red oval. In the main window, the 'Queue List' window is open, showing a table with columns: #, Name, Target Address, Packet ..., Max Upload..., Max Downl..., Upload Rate, and Download ... A red circle highlights the '+' icon in the toolbar above the table. A red arrow points from this icon to the 'New Simple Queue' dialog box. In this dialog, the 'Burst' section is highlighted with a red oval, showing the following settings:

- Burst Limit: 128k (upload), 256k (download) bits/s
- Burst Threshold: 32k (upload), 64k (download) bits/s
- Burst Time: 20 (upload), 20 (download) s

Other settings in the 'New Simple Queue' dialog include:

- Name: laptop_queue
- Target Address: 192.168.XY.1
- Max Limit: 64k (upload), 128k (download) bits/s
- Target Upload and Target Download are checked.

The 'Queue List' window also shows '0 B queued' at the bottom left and 'disabled' at the bottom right.

Burst Lab

- Delete all previously created queues
- Create a queue to limit your laptop upload/download to 64Kbps/128Kbps
- Set burst to this queue
 - ◆ **burst-limit** up to 128Kbps/256Kbps
 - ◆ **burst-threshold** 32Kbps/64Kbps
 - ◆ **burst-time** 20 seconds
- Use bandwidth-test to test the limitations

Advanced Burst Lab

- Try to set burst-threshold for this queue to the 128Kbps/256Kbps
- Try to set burst-threshold for this queue to the 64Kbps/128Kbps
- Try to set burst-threshold for this queue to the 16Kbps/32Kbps
- State the optimal burst configuration

Interface Traffic Monitor

- Open up interface menu in WinBox to see tx/rx rates per interface
- Open up any interface and select the “Traffic” tab to see the graphs
- Use the “monitor-traffic” command in terminal to get the traffic data per one or more interfaces, for example:
 - ◆ `/interface monitor-traffic ether1`
 - ◆ `/interface monitor-traffic ether1,ether2,ether3`

Interface Traffic Monitor

10d 21:54:24 Memory: 13.6 MiB CPU: 7%

RouterOS WinBox

Interfaces

Wireless

PPP

Bridge

IP

Routing

Ports

Queues

Drivers

System

Files

Log

SNMP

Users

Radius

Tools

New Terminal

Telnet

Password

Certificate

Make Supout.rif

Manual

Exit

Interface List

	Name	Type	MTU	Tx Rate	Rx Rate	Tx Packet Rate	Rx Packet Rate
R	bridge1_hata	Bridge	1500	149.0 kbps	871.7 kbps	80	100
R	ether1_DMZ	Ethernet	1500	6.4 kbps	14.3 kbps	3	24
R	ether2_DSL	Ethernet	1500	881.6 kbps	149.2 kbps	99	79
R	ether3_LAN	Ethernet	1500	149.0 kbps	883.7 kbps	80	100
	wlan1_hata	Wireless (Atheros A...	1500	0 bps	0 bps	0	0

Torch Tool

- Torch tool offers more detailed actual traffic report for the interface
- It's easier to use the torch in WinBox:
 - ◆ Go to “Tools” > “Torch”
 - ◆ Select an interface to monitor and click “Start”
 - ◆ Use “Stop” and “Start” to freeze/continue
 - ◆ Refine the output by selecting protocol and port
 - ◆ Double-click on specific IP address to fill in the Src. Or Dst. Address field (0.0.0.0/0 is for any address)

Torch Tools

Torch (running)

- Basic
 Interface: ether3_LAN
 Entry Timeout: 00:00:03 s

- Filters
 Src. Address: 0.0.0.0/0
 Dst. Address: 0.0.0.0/0
 Protocol: any
 Port: any

- Collect
 Src. Address Protocol
 Dst. Address Port

Start
Stop
Close

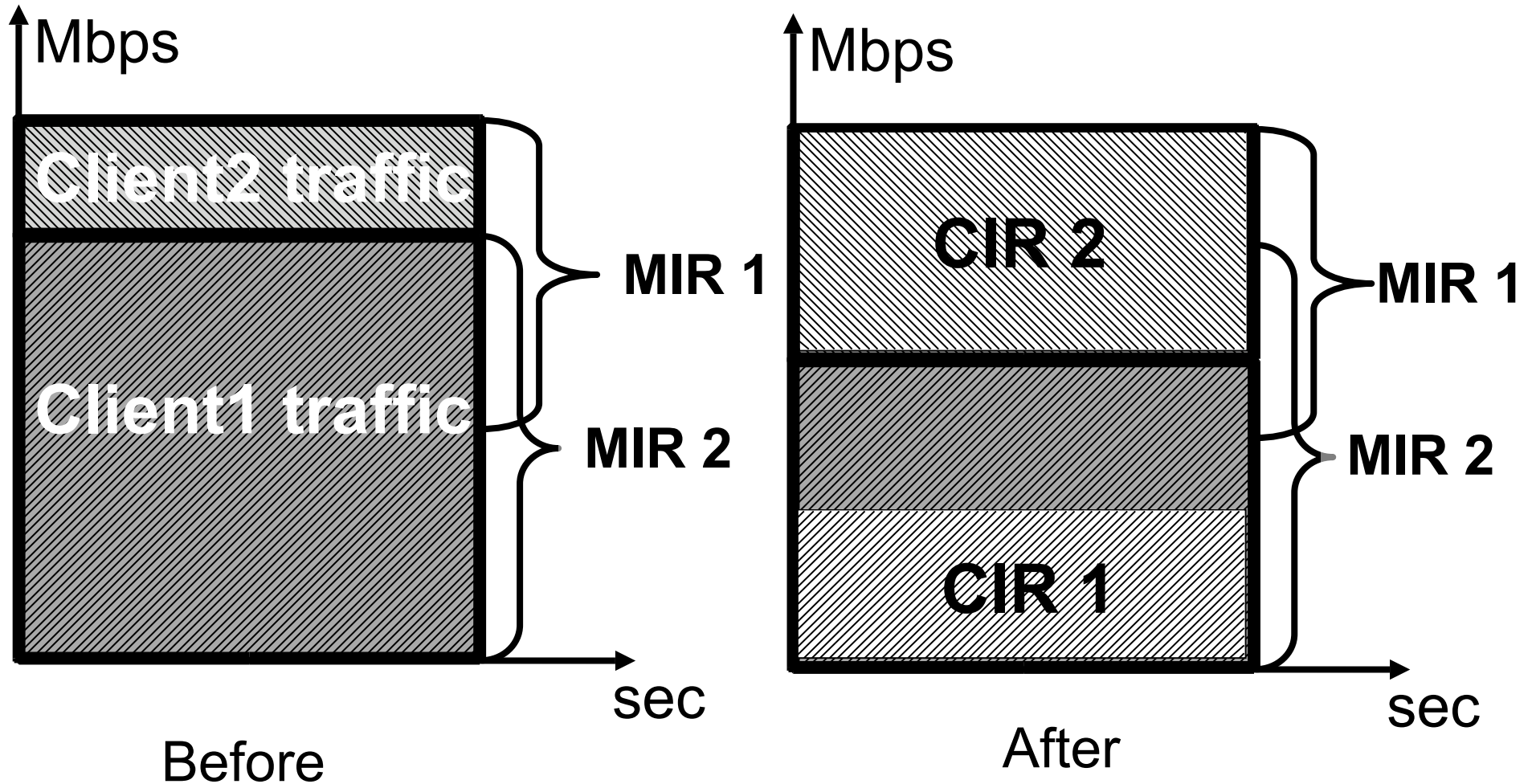
	Eth. ...	Protocol	Src. Address	Src. Port	Dst. Address	Dst. Port	Tx Rate	Rx Rate	Tx Pack...	Rx Pack...
	0 (ip)	6 (tcp)	192.168.1.85	50011	62.136.157.69	4901	2.0 kbps	75.5 kbps	5	6
	0 (ip)	6 (tcp)	192.168.1.85	50011	213.112.9.103	38689	1810 bps	64.2 kbps	4	6
	0 (ip)	6 (tcp)	192.168.1.85	50011	74.13.124.9	50000	1672 bps	62.4 kbps	4	6
	0 (ip)	6 (tcp)	192.168.1.85	50011	83.95.249.222	56070	53.3 kbps	61.6 kbps	8	8
	0 (ip)	6 (tcp)	192.168.1.85	50011	88.91.146.113	47426	31.2 kbps	48.7 kbps	5	6
	0 (ip)	6 (tcp)	192.168.1.85	50011	82.135.96.210	45154	12.5 kbps	44.4 kbps	4	4
	0 (ip)	6 (tcp)	192.168.1.85	50011	84.52.27.45	49149	684 bps	42.0 kbps	1	3
	0 (ip)	6 (tcp)	192.168.1.85	50011	88.114.166.181	4291	778 bps	41.9 kbps	2	3
	0 (ip)	6 (tcp)	192.168.1.85	50011	81.216.151.87	33152	1122 bps	40.3 kbps	2	4
	0 (ip)	6 (tcp)	192.168.1.85	50011	71.245.157.146	61667	20.7 kbps	36.2 kbps	3	3
	0 (ip)	6 (tcp)	192.168.1.85	50011	203.211.88.95	42141	1149 bps	35.0 kbps	1	3
	0 (ip)	6 (tcp)	192.168.1.85	50011	84.57.238.105	54405	21.9 kbps	32.9 kbps	5	5
	0 (ip)	6 (tcp)	192.168.1.85	50011	125.238.51.204	2989	629 bps	29.8 kbps	1	2
	0 (ip)	6 (tcp)	192.168.1.85	50011	67.116.155.233	32807	1048 bps	28.0 kbps	1	2
	0 (ip)	6 (tcp)	192.168.1.85	50011	212.244.76.131	8163	661 bps	28.0 kbps	1	2
	0 (ip)	6 (tcp)	192.168.1.85	50011	148.160.184.134	29580	320 bps	28.0 kbps	1	2
	0 (ip)	6 (tcp)	192.168.1.85	50011	67.174.235.189	32459	106 bps	28.0 kbps	0	2
	0 (ip)	6 (tcp)	192.168.1.85	50011	85.23.16.41	52753	320 bps	23.8 kbps	1	2
	0 (ip)	6 (tcp)	192.168.1.85	50011	66.66.164.152	4922	212 bps	20.0 kbps	0	1

Total Tx: 187.7 kbps Total Rx: 939.5 kbps Total Tx Packet: 73 Total Rx Packet: 98

Dual Limitation

- Advanced, better QoS
- Dual limitation has two rate limits:
 - ◆ **CIR (Committed Information Rate)** – in worst case scenario a flow will get its **limit-at** no matter what (assuming we can actually send so much data)
 - ◆ **MIR (Maximal Information Rate)** – in best case scenario a flow can get up to **max-limit** if there is spare bandwidth

Dual Limitation Example



Dual Limitation Lab

- Create one queue for limiting your laptop's communication with the first test server
 - ◆ limit-at 86Kbps/172Kbps
 - ◆ max-limit to 172Kbps/384Kbps
 - ◆ dst-address <first test server>
- Create one queue for limiting your laptop's communication with the second test server
 - ◆ limit-at 86Kbps/172Kbps
 - ◆ max-limit to 172Kbps/384Kbps
 - ◆ dst-address <second test server>

Parent Queue

- It is hard for the router to detect exact speed of Internet connection
- To optimize usage of your Internet resources and to ensure desired QoS operation you should assign maximal available connection speed manually
- To do so, you should create one parent queue with strict speed limitation and assign all your queues to this parent queue

Parent Queue

New Simple Queue [X]

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

Name:

Target Address:

Target Upload Target Download

Max Limit:

▼ Burst

▼ Time

disabled

Simple Queue <main_queue> [X]

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

P2P:

Packet Mark:

Dst. Address:

Interface:

Target Upload Target Download

Limit At: bits/s

Queue Type:

Parent:

Priority:

disabled

OK
Cancel
Apply
Disable
Copy
Remove

Dual Limitation Lab

- Create a parent queue
 - ◆ max-limit to 256Kbps/512Kbps
- Assign both previously created queues to the parent queue
 - ◆ Set parent option to “main_queue”
- Test the limitations

First Child Queue

New Simple Queue

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

Name: Child_queue1

Target Address: 192.168.XY.1

Target Upload Target Download

Max Limit: 172k 348K bits/s

▼ Burst

▼ Time

disabled

New Simple Queue

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

P2P: [dropdown]

Packet Mark: [dropdown]

Dst. Address: <first test server address>

Interface: all [dropdown]

Limit At: 86k 172k bits/s

Queue Type: default-small default-small

Parent: main_queue [dropdown]

Priority: 8

disabled

Second Child Queue

New Simple Queue

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

Name: Child_queue2

Target Address: 192.168.XY.1

Target Upload Target Download

Max Limit: 172k 348K bits/s

▼ Burst

▼ Time

disabled

OK
Cancel
Apply
Disable

New Simple Queue

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

P2P: [dropdown]

Packet Mark: [dropdown]

Dst. Address: <second test server address>

Interface: all [dropdown]

Target Upload Target Download

Limit At: 86k 172k bits/s

Queue Type: default-small default-small [dropdown]

Parent: main_queue [dropdown]

Priority: 8

disabled

OK
Cancel
Apply
Disable
Copy
Remove

Priority

- 8 is the lowest priority, 1 is the highest
- Numeric difference between priorities is irrelevant (two queues with priorities 1 and 8, will have same relation as two queues with priorities 1 and 2)
- Queue with higher priority will reach its CIR before the queue with lower priority
- Queue with higher priority will reach its MIR before the queue with lower priority

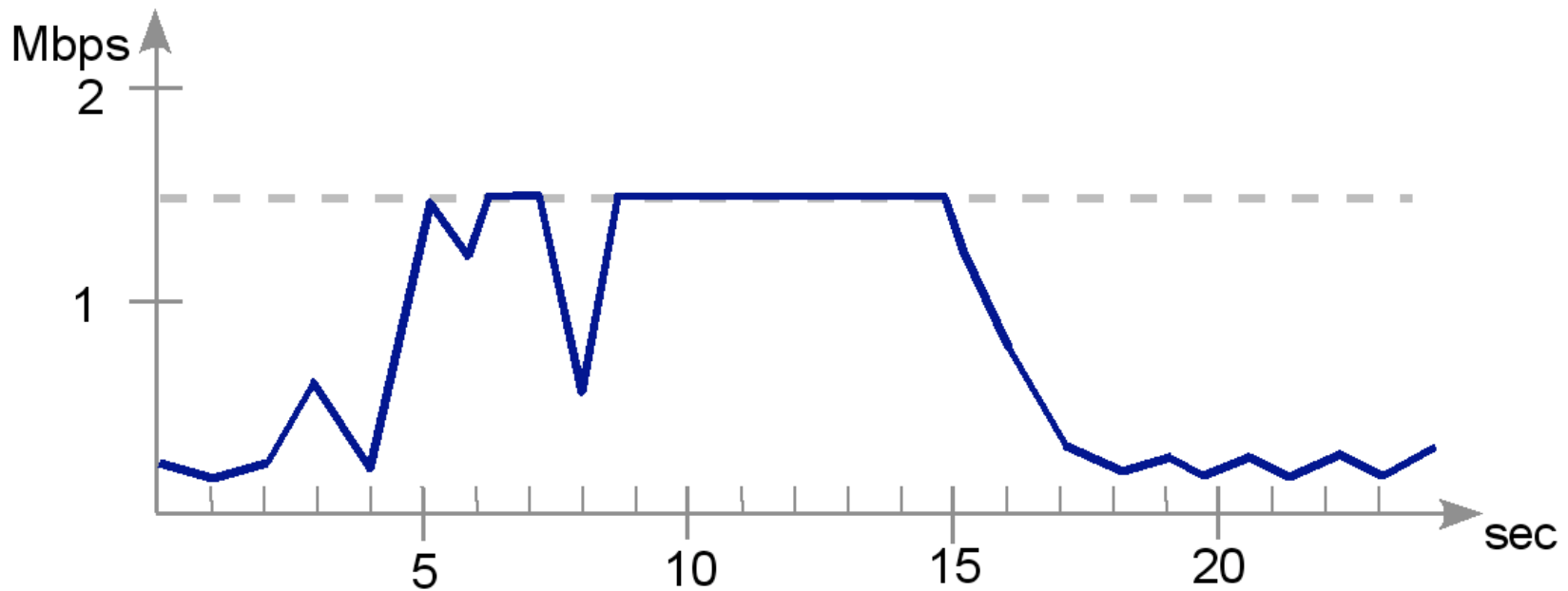
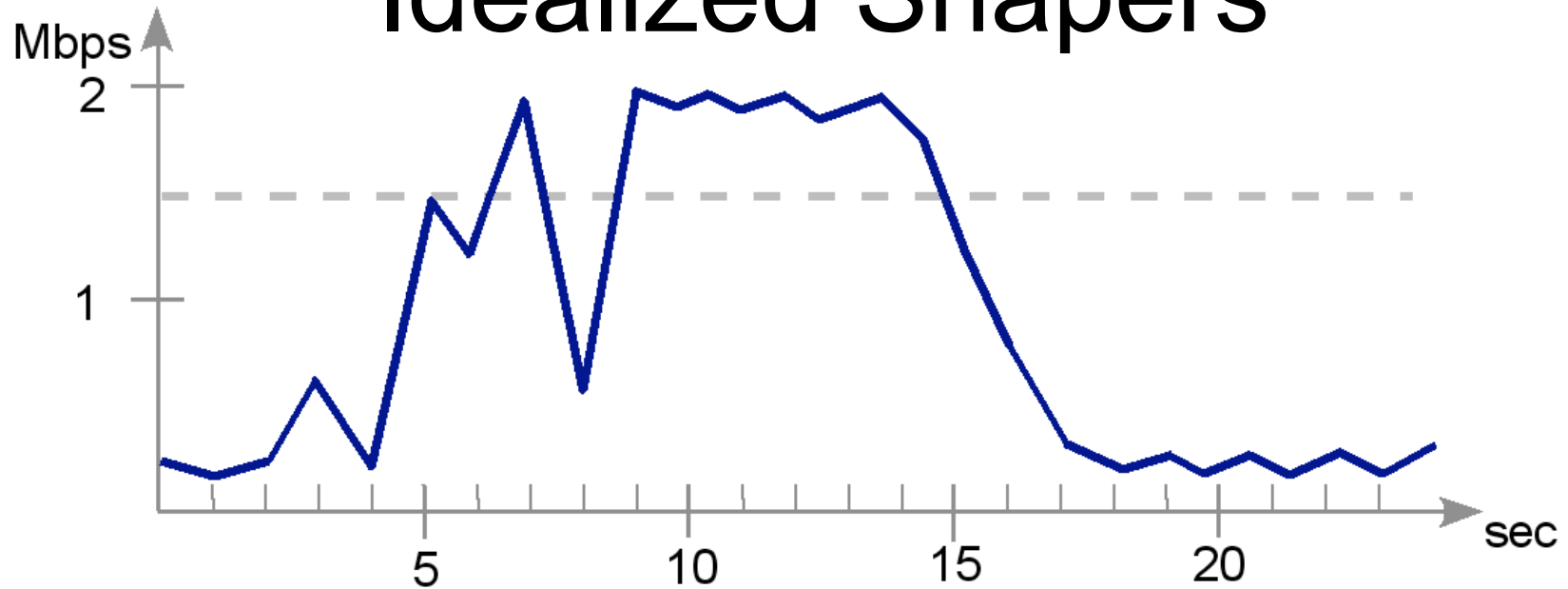
Priority Lab

- Adjust priorities in the “Dual Limitation Lab”
- Check the limitations!

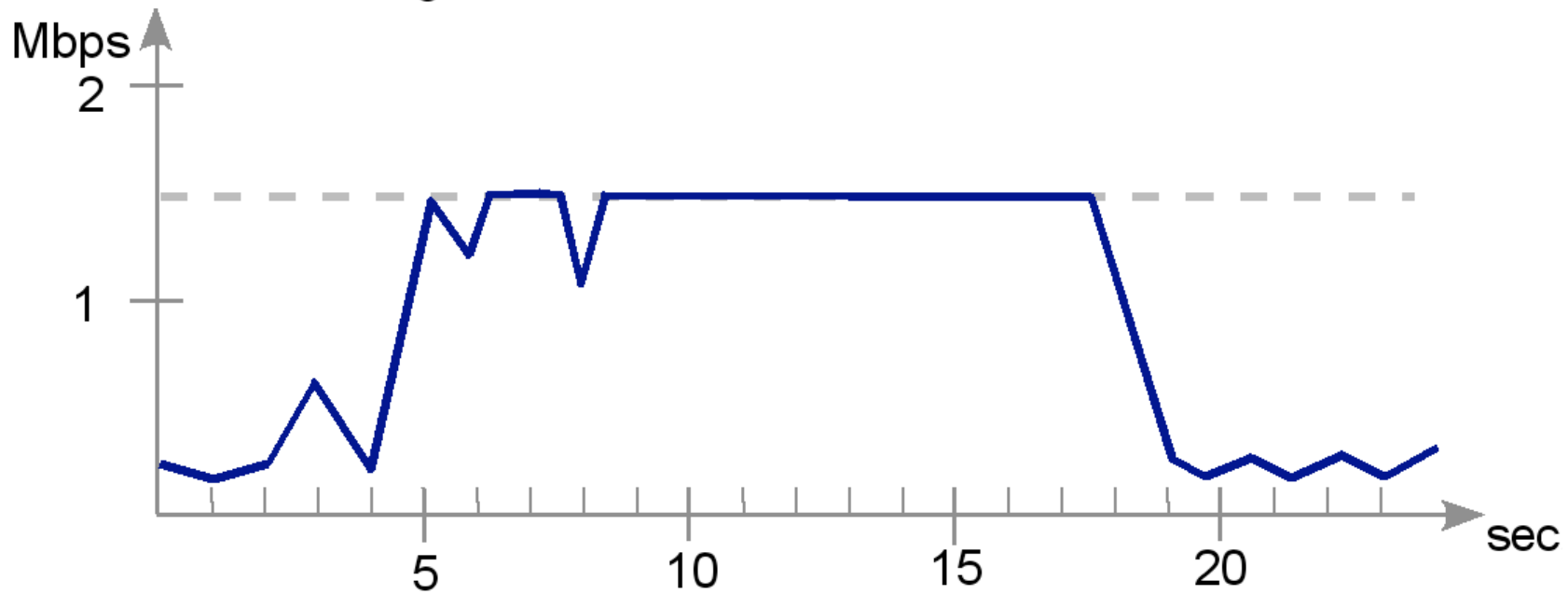
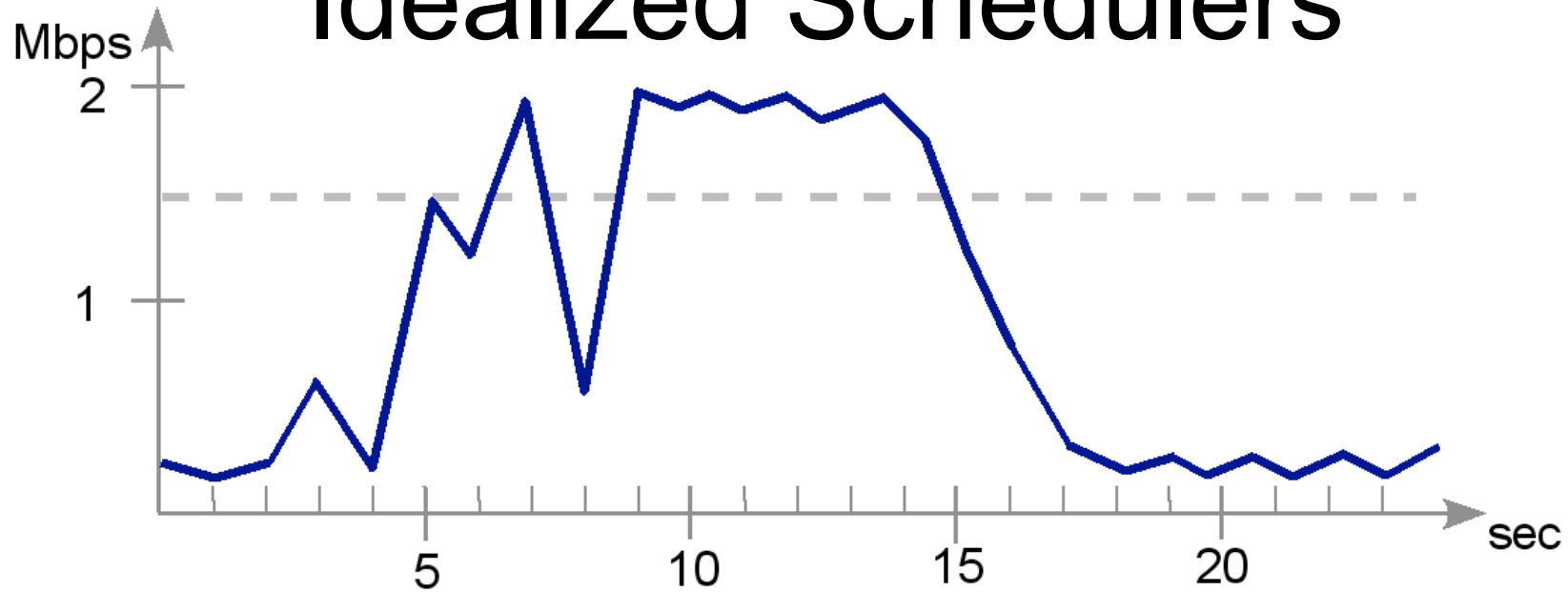
Queue Disciplines

- Queuing disciplines can be classified into two groups by their influence on the traffic flow – schedulers and shapers
- Scheduler queues reorder the packet flow. These disciplines limit the number of waiting packets, not the data rate
- Shaper queues control data flow speed. They can also do a scheduling job

Idealized Shapers



Idealized Schedulers



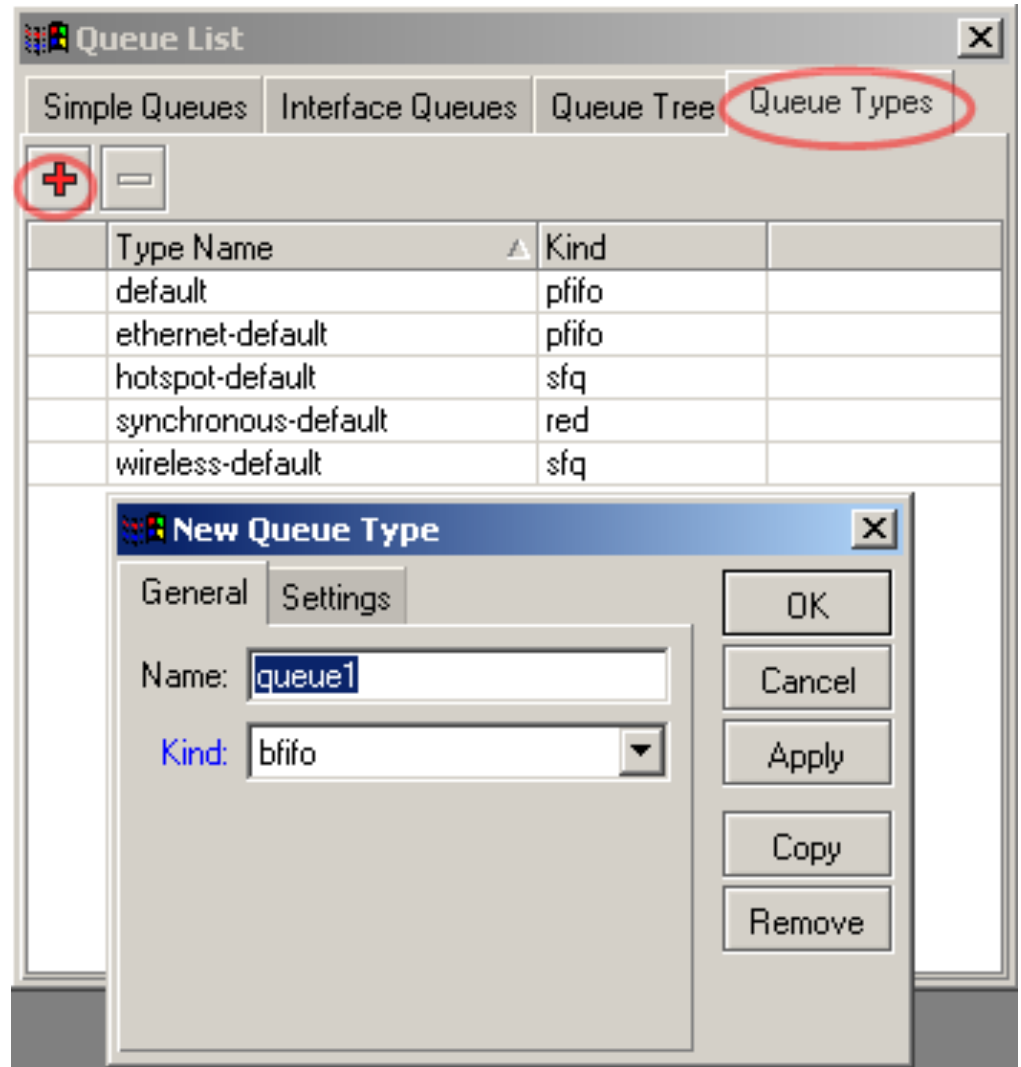
Queue types

- Scheduler queues

- ◆ BFIFO
- ◆ PFIFO
- ◆ RED
- ◆ SFQ

- Shaper queues

- ◆ PCQ



FIFO algorithm



- PFIFO and BFIFO
- FIFO queuing disciplines do not change packet order, instead they accumulate packets until a defined limit is reached

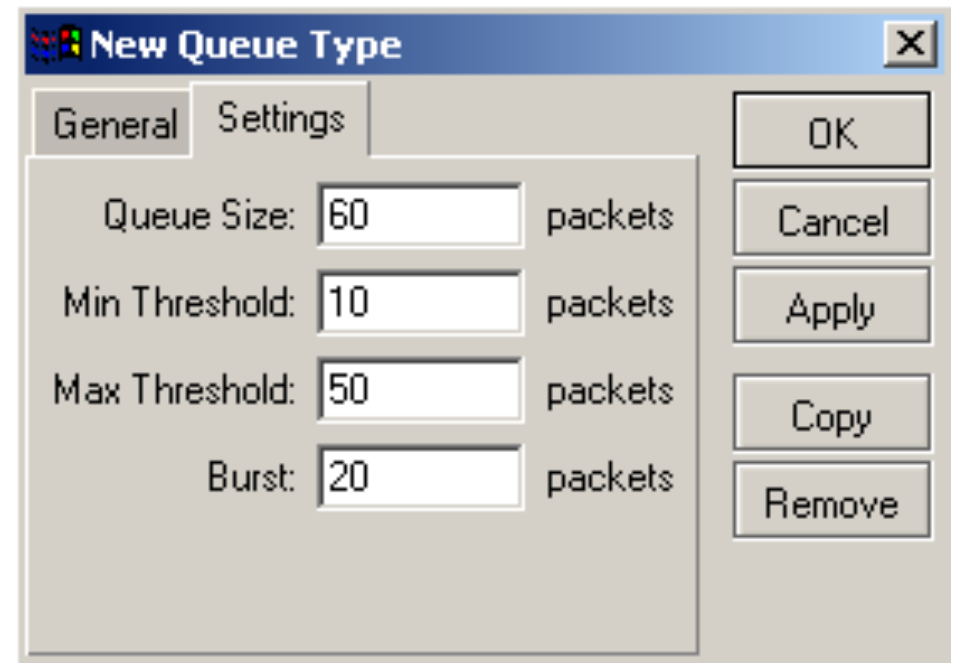
RED algorithm

- Random Early Detect (Random Early Drop)
- Does not limit the speed; indirectly equalizes users' data rates when the channel is full
- When the average queue size reaches min-threshold, RED randomly chooses which arriving packet to drop
- If the average queue size reaches max-threshold, all packets are dropped
- Ideal for TCP traffic limitation

RED algorithm



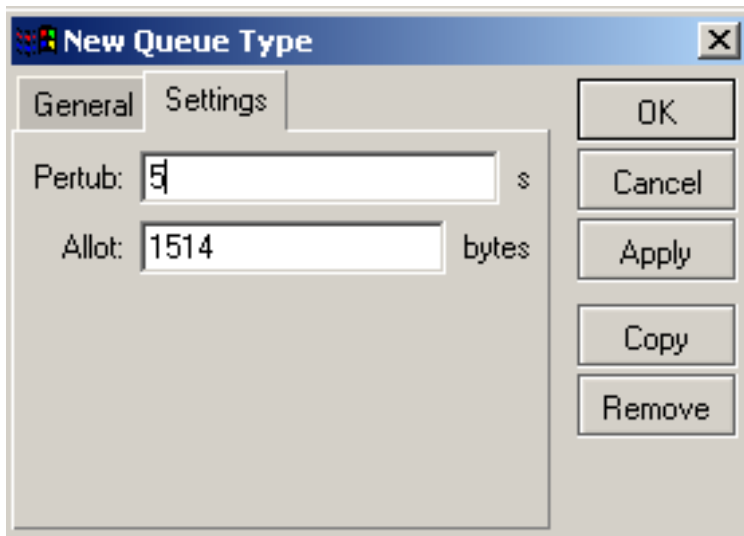
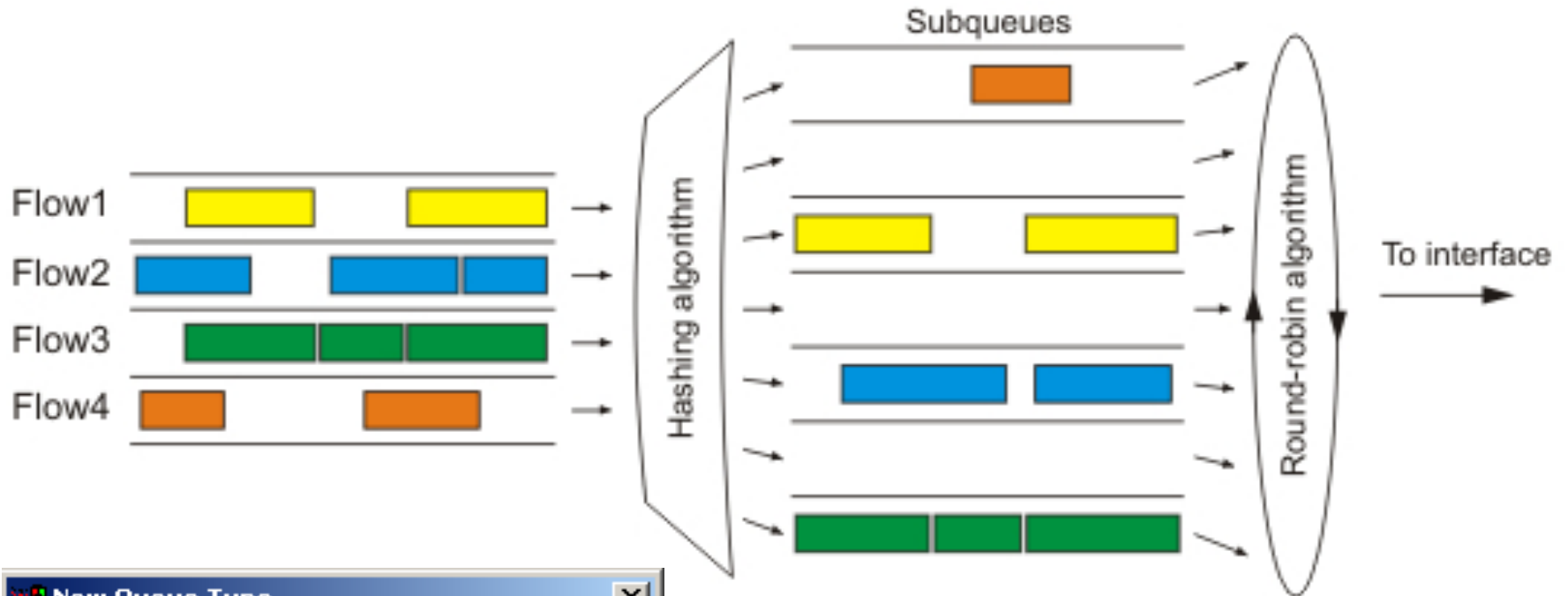
- If real queue size is much greater than max-threshold, then all excess packets are dropped



SFQ algorithm

- Stochastic Fairness Queuing (SFQ) cannot limit traffic at all. Its main idea is to equalize traffic flows when your link is completely full.
- The fairness of SFQ is ensured by hashing and round-robin algorithms
- Hashing algorithm is able to divide the session traffic into up to 1024 sub queues. It can hold up to 128 packets in memory simultaneously
- The round-robin algorithm dequeues bytes from each sub queue in a turn

SFQ algorithm



- After perturb seconds the hashing algorithm changes and divides the session traffic to different subqueues

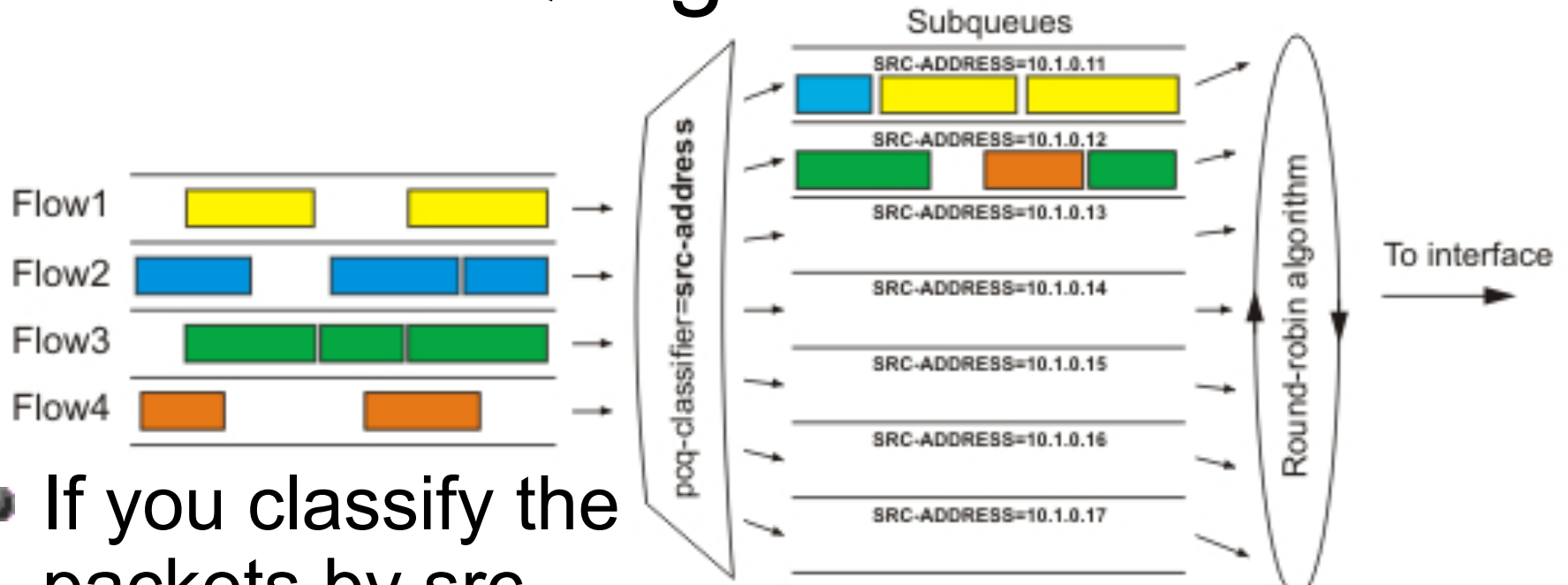
SFQ Example

- SFQ should be used for equalizing similar connection
- Usually used to manage information flow to or from the servers, so it can offer services to every customer
- Ideal for p2p limitation - it is possible to place strict limitation without dropping connections

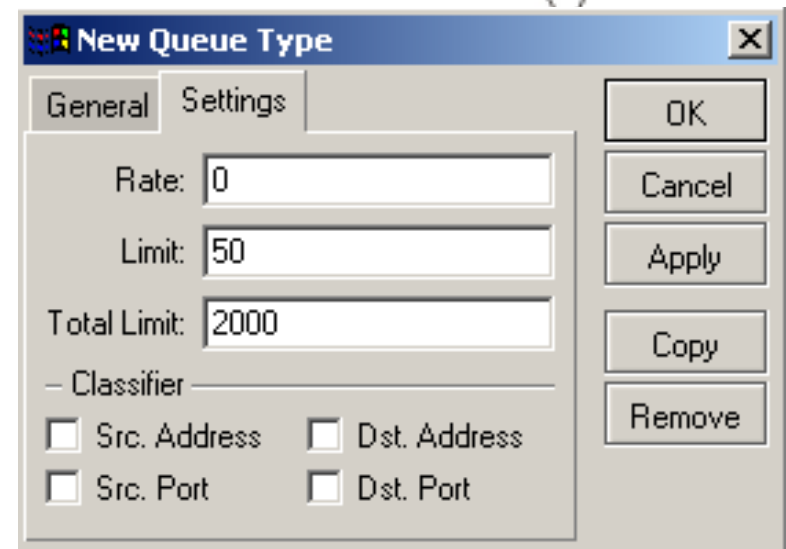
PCQ algorithm

- Per Connection Queue allows to choose classifiers (one or more of src-address, dst-address, src-port, dst-port)
- PCQ does not limit the number of sub flows
- It is possible to limit the maximal data rate that is given to each of the current sub flows
- PCQ is memory consumptive!!

PCQ algorithm



- If you classify the packets by src-address then all packets with different source IP addresses will be grouped into different subqueues

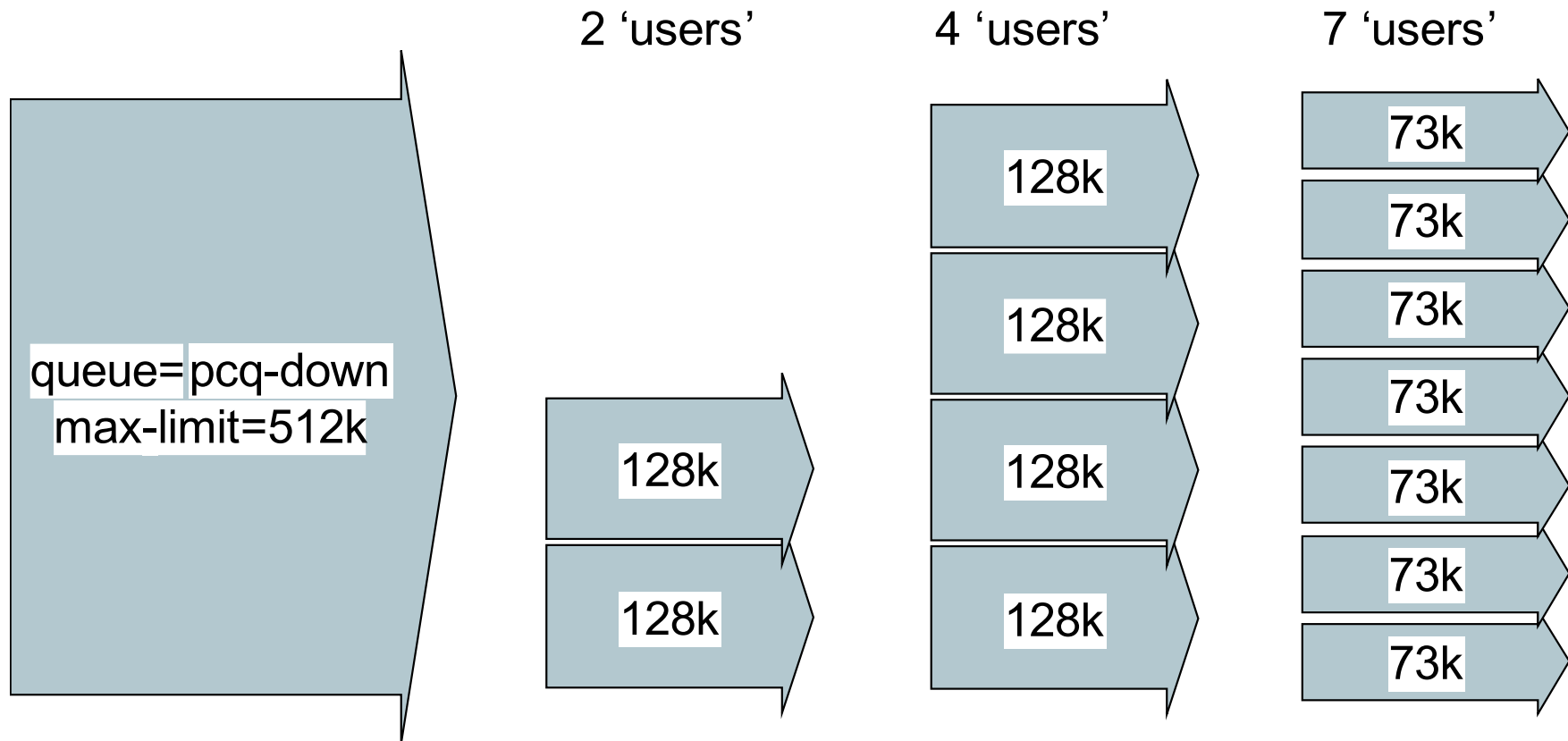


PCQ example

- If 'limit-at' and 'max-limit' are set to '0', then the subqueues can take up all bandwidth available for the parent
- Set the PCQ Rate to '0', if you do not want to limit subqueues, i.e, they can use the bandwidth up to 'max-limit', if available

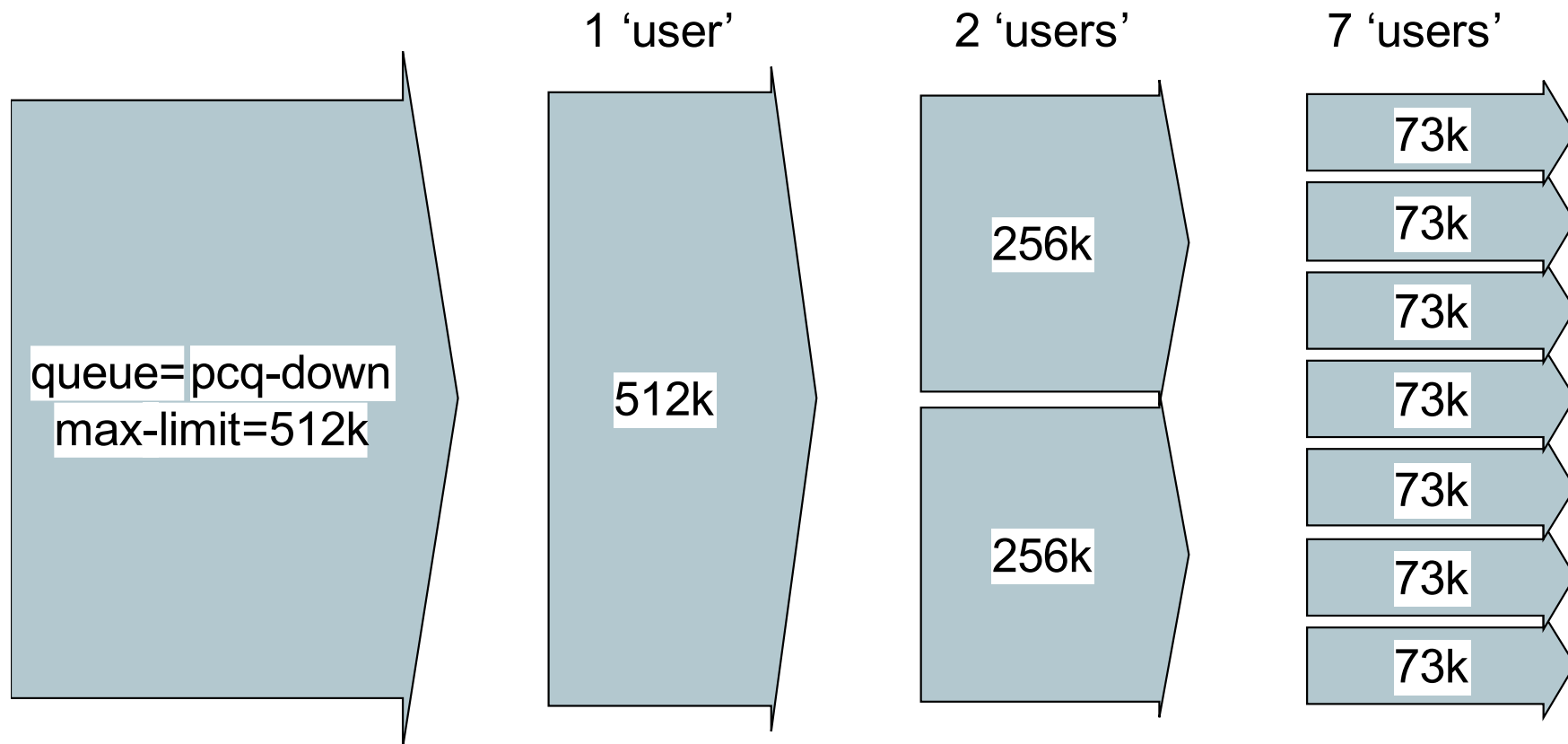
PCQ in Action

- pcq-rate=128000



PCQ in Action (cont.)

- pcq-rate=0



Queue Type Lab

- Try RED algorithm in the last configuration
- Check the limitations!
- Try SFQ algorithm
- Check the limitations!
- Watch the teachers demonstration about PCQ

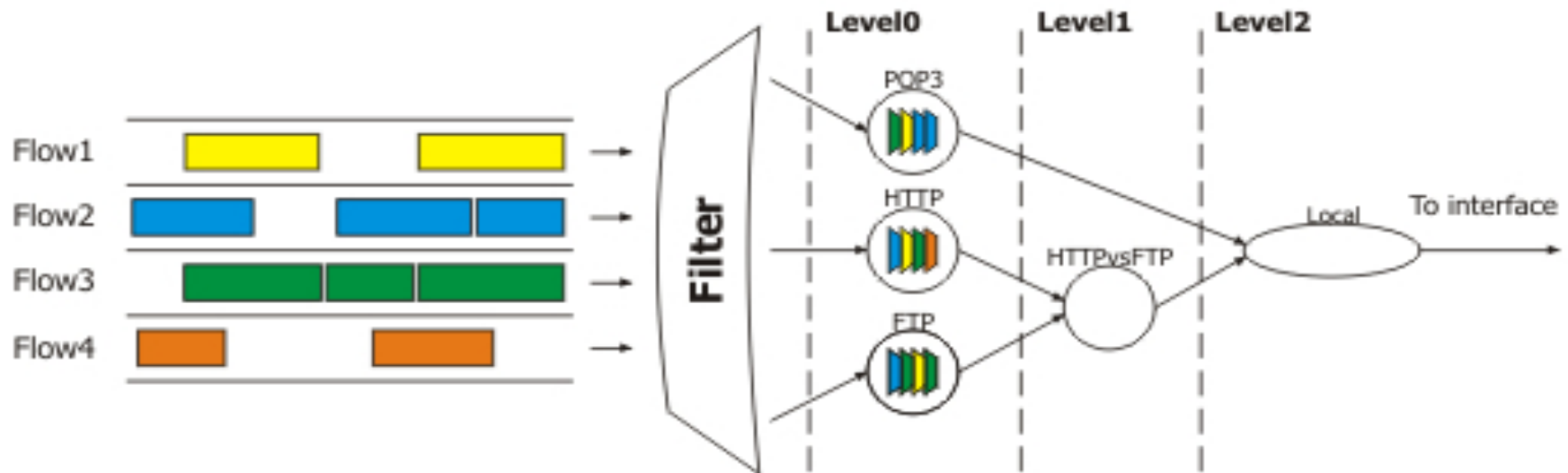
HTB

Hierarchical Token Bucket

HTB

- HTB mentioned before is not managed like other queues
- HTB is a hierarchical queuing discipline.
- HTB is able to prioritize and group traffic flows
- HTB is not co-existing with another queue on an interface – there can only be one queue and HTB is the one.

HTB Algorithm

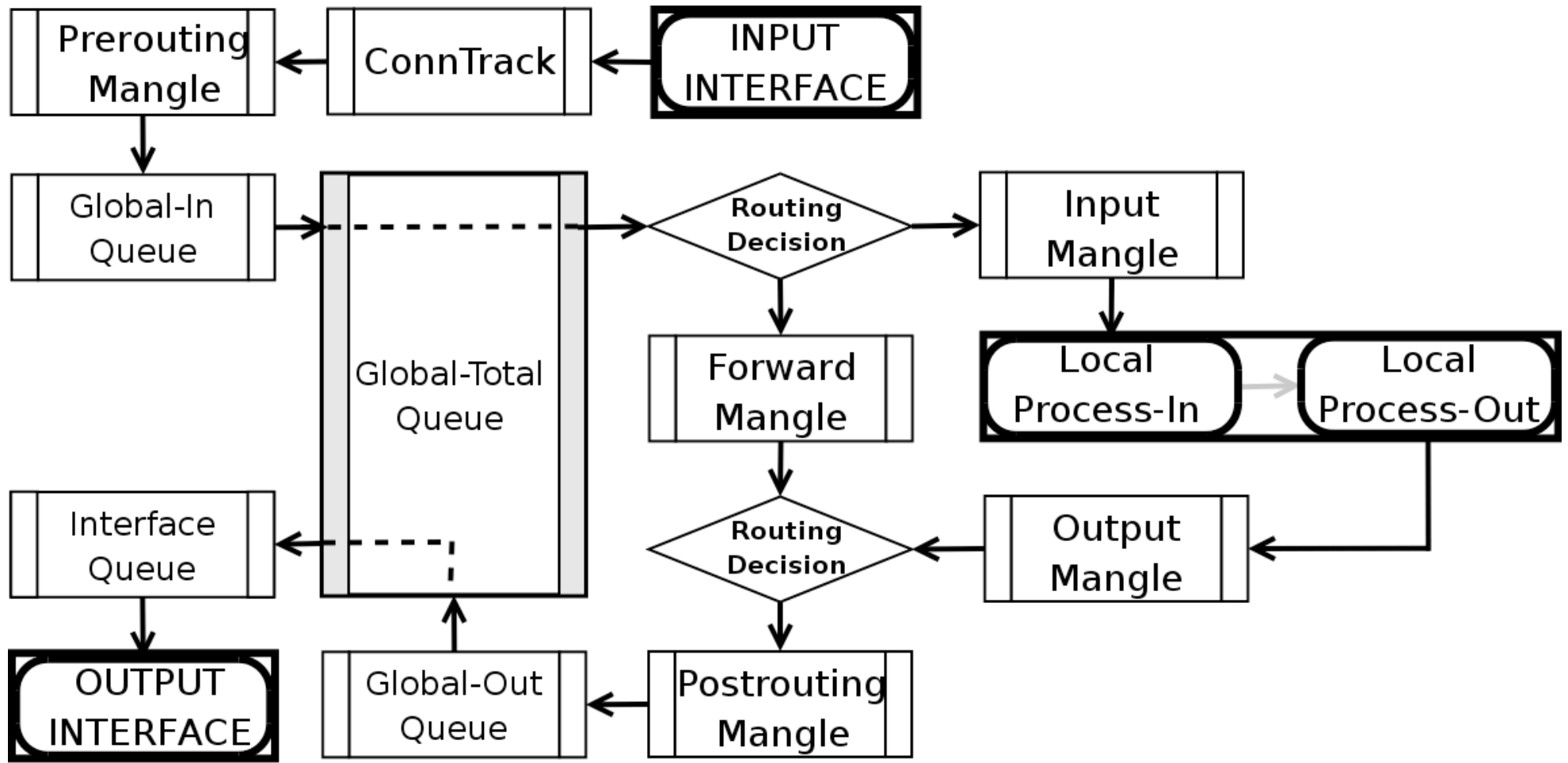


All the circles are queuing disciplines – a packet storage with a flow management algorithm (FIFO, RED, SFQ or PCQ)

HTB

- There are 3 HTB trees maintained by RouterOS:
 - ◆ global-in
 - ◆ global-total
 - ◆ global-out
- And one more for each interface

Mangle and HTB



HTB (cont.)

- When packet travels through the router, it passes all 4 HTB trees
- When packet travels to the router, it passes only global-in and global-total HTB.
- When packet travels from the router, it passes global-out, global-total and interface HTB.

HTB Algorithm

- In order of priority HTB satisfies all “limit-at”s for leaf classes
- When the “limit-at” is reached the class becomes “yellow”
- When the “max-limit” is reached the class becomes “red”

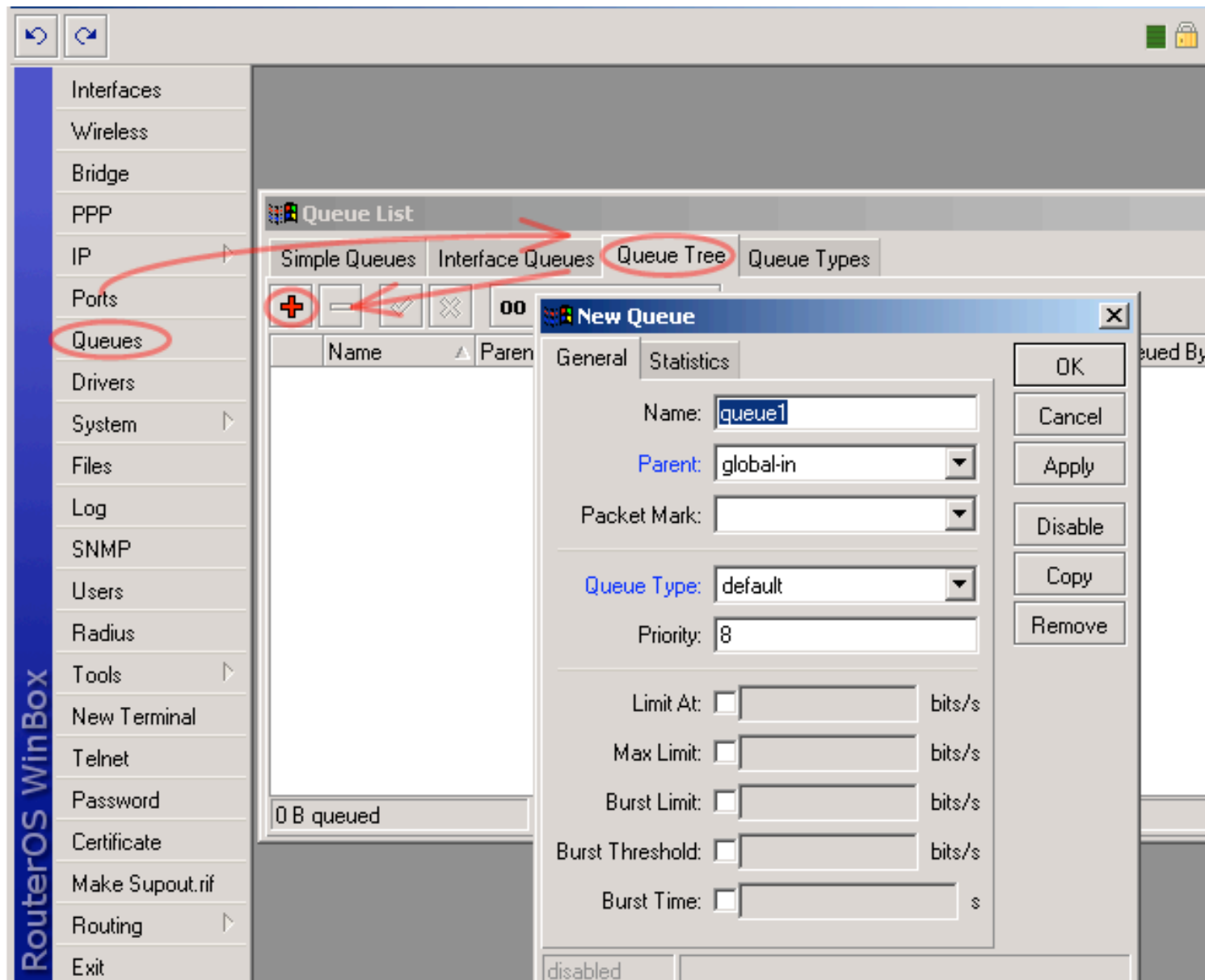
HTB Algorithm

- Some attributes of HTB classes :
 - ◆ limit-at
 - ◆ max-limit
 - ◆ priority
- Simple queues are executed by the HTB facility in “global-out” ('direct' queue), “global-in” ('reverse' queue) and “global-total” ('total' queue) trees

Queue Tree

Another way to manage the traffic

Tree Queue



Queue Tree and Simple Queues

- Tree queue can be placed in 4 different places:
 - ◆ Global-in (“direct” part of simple queues are placed here automatically)
 - ◆ Global-out (“total” part of simple queues are placed here automatically)
 - ◆ Global-total (“reverse” part simple queues are placed here automatically)
 - ◆ Interface queue
- If placed in same place Simple queue will take traffic before Queue Tree

Queue Tree

- Queue tree is only one directional. There must be one queue for download and one for upload
- Queue tree queues work only with packet marks. These marks should be created in the firewall mangle
- Queue tree allows to build complex queue hierarchies





Queue Tree Lab









- Create queue tree:
 - ◆ Create a main queue
 - ◆ Create child queue for ICMP
 - ◆ Create child queue for HTTP
 - ◆ Create child queue for OTHER
- Consume all the available traffic using bandwidth-test and check the ping response times
- Set highest priority to ICMP
- Check the ping response times

Queue Tree Lab Result

Queue List

Simple Queues Interface Queues **Queue Tree** Queue Types

    **00** Reset Counters **00** Reset All Counters

Name	Parent	Packet Mark	Limit At	Max Limit	F
 main_download	local_ether3		0	512k	
 HTTP_download	main_download	HTTP_packets	256k	512k	
 ICMP_download	main_download	ICMP_packet	50k	100k	
 OTHER_download	main_download	OTHER_packets	0	512k	
 main_upload	public_ether1		0	256k	
 HTTP_upload	main_upload	HTTP_packets	128k	256k	
 ICMP_upload	main_upload	ICMP_packet	50k	100k	
 OTHER_upload	main_upload	OTHER_packets	0	256k	

Wireless and Tunnels

Wireless Concepts, Encryption, User Manager,
WDS and Mesh, nStreme Protocol, VLAN,
PPPoE, PPTP, L2TP, IPSec

MikroTik RouterOS – Wireless

Wireless Concepts, Encryption, WDS and Mesh,
NStreme Protocol

Wireless Interface Mode Settings

- bridge/ap-bridge – AP mode; bridge mode supports only one client
- station – a regular client (can **not** be bridged)
- station-pseudobridge/station-pseudobridge-clone – client, which can be bridged (implements MAC address translation)
- alignment-only – for positioning antennas
- nstreme-dual-slave – card will be used in nstreme-dual interface
- wds-slave – works as ap-bridge mode but adapts to the WDS peers frequency
- station-wds – client, which can be bridged (AP should support WDS feature)

Wireless Station

- Joins a Service Set
- Follows the Access Point within the Scan List
- Restrictions based on Connect List

Finding Access Points

The image shows two windows from Mikrotik WinBox. The top window is titled "Interface <wlan1>" and is on the "Wireless" tab. It shows configuration for a wireless interface with the following settings:

- Mode: station
- Band: 2.4GHz-B/G
- Frequency: 2432 MHz
- SSID: AP2G
- Radio Name: 000C420CB283

The bottom window is titled "Scan <wlan1> (running)" and displays a table of detected access points. The table has columns for Address, SSID, Band, Frequency, Signal strength, Radio Name, and Router OS version. The entry for SSID "AP2G" is selected.

	Address	SSID	Band	Frequ...	Signa...	Radio Name	RouterO...
AB	00:02:6F:08:53:18		2.4GHz-G	2432	-41		
AB	00:02:6F:33:C7:B1	MikroTik	2.4GHz-G	2412	-89		
ABR	00:02:6F:45:15:43	AP2G	2.4GHz-G	2432	-65	00026F451543	3.0beta7
ABR	00:08:6B:31:52:69	tests	2.4GHz-G	2452	-93	000B6B315269	2.9.27
ABP	00:08:6B:37:56:94	hotspot	2.4GHz-G	2412	-54	HotSpot2	3.0beta6
ABR	00:08:6B:37:5B:B4	dzintars	2.4GHz-G	2442	-79	testa_ruters	2.8.28
BR	00:08:6B:37:62:70	MikroTik	2.4GHz-G	2412	-95	000B6B376270	2.9.17
ABP	00:08:6B:37:67:0D	hotspot	2.4GHz-G	2412	-47	HotSpotMain	3.0beta5
ABR	00:08:6B:4D:02:29	ap_laptop	2.4GHz-G	2412	-91	000B6B4D0229	2.9.39
ABP	00:08:6B:4D:03:6B	hotspot	2.4GHz-G	2412	-71	HotSpot4	3.0beta6
ABP	00:08:6B:4D:03:99	hotspot	2.4GHz-G	2412	-78	HotSpot5	3.0beta6
ABP	00:08:6B:4D:04:2A	hotspot	2.4GHz-G	2412	-75	HotSpot1	3.0beta6
ABR	00:0C:42:05:01:39	test_ap	2.4GHz-G	2412	-90	000C42050139	2.9.19
ABR	00:0C:42:05:05:8A	Uldim2	2.4GHz-G	2457	-67	000C4205058A	3.0beta6
ABR	00:0C:42:05:06:F3	Demo	2.4GHz-G	2452	-94	000C420506F3	2.9.39

22 items (1 selected)

Buttons: Start, Stop, Close, Connect

Alignment Tool

The screenshot displays the 'Alignment <wlan1> (running)' window. It features a table with columns for Address, SSID, Rx Quality, Avg. Rx Quality, Last Rx, Tx Quality, Last Tx, and Correct (%). The table lists 12 items, with the third item (Address: 00:02:6F:45:15:43, SSID: AP2G) selected. To the right of the table are buttons for Start, Stop, Close, and Settings... A 'Find' search box is also present.

	Address	SSID	Rx Quality	Avg. Rx Quality	Last Rx	Tx Quality	Last Tx	Correct (%)
	00:02:6F:01:CE:2A		-58	-62	0.50		0.00	0
A	00:02:6F:08:53:18		-52	-52	0.08		0.00	0
	00:02:6F:45:15:43	AP2G	-65	-65	0.03	-60	0.03	96
A	00:08:6B:37:5B:...	dzintars	-88	-88	21.65		0.00	0
	00:0C:42:05:01:11		-83	-78	1.20		0.00	0
A	00:0C:42:0C:0A:...	Uldim3	-95	-95	6.40		0.00	0
A	00:0E:2E:40:89:A7	MY AP	-95	-94	8.60		0.00	0
	00:11:50:F6:E5:A3		-88	-77	0.20		0.00	0
	00:14:A4:36:99:00		-46	-48	13.88			
	00:15:6D:53:4D:...		-89	-89	31.01			
A	00:16:B6:D9:53:...	linksys	-70	-71	0.02			
A	02:0B:6B:37:67:...	hot	-85	-85	2.09			

12 items (1 selected)

Wireless Alignment Settings

- Frame Size: 200
- Active Mode
- Receive All
- Filter MAC Address: 00:00:00:00:00:00
- SSID All
- Frames per Second: 1

Buttons: OK, Cancel, Apply

Wireless Sniffer Tool

Sniffer <wlan1 >

Processed Packets: 1055

Memory Size: 9.0 KiB

Memory Saved Packets: 150

Memory Over Limit Packets: 905

File Size: 0 B

File Saved Packets: 0

File Overlimit Packets: 0

Stream Dropped Packets: 0

Stream Sent Packets: 0

File Limit: 10 KiB

Memory Limit: 10 KiB

Sniffed Wireless Packets

Find

	Time (s)	Interfa...	Band	Frequ...	Signal ...	Rate	Dst.	Src.	Type
	0.298	wlan1	2.4GHz-G	2412	-53	48Mbps	00:0B:6B:4D:04:2A	00:0B:6B:37:67:0D	data
	0.299	wlan1	2.4GHz-G	2412	-57	48Mbps	00:0B:6B:4D:04:2A	00:0B:6B:37:67:0D	data
	0.301	wlan1	2.4GHz-G	2412	-59	48Mbps	00:0B:6B:4D:04:2A	00:0B:6B:37:67:0D	data
	0.302	wlan1	2.4GHz-G	2412	-76	36Mbps	00:0B:6B:37:67:0D	00:0B:6B:4D:04:2A	data
	0.304	wlan1	2.4GHz-G	2412	-58	48Mbps	00:0B:6B:4D:04:2A	00:0B:6B:37:67:0D	data
	0.304	wlan1	2.4GHz-G	2412	-56	36Mbps	00:0B:6B:4D:04:2A	00:0B:6B:37:67:0D	data
	0.304	wlan1	2.4GHz-G	2412	-55	36Mbps	00:0B:6B:4D:04:2A	00:0B:6B:37:67:0D	data
	0.305	wlan1	2.4GHz-G	2412	-75	36Mbps	00:0B:6B:37:67:0D	00:0B:6B:4D:04:2A	data
	0.306	wlan1	2.4GHz-G	2412	-77	36Mbps	00:0B:6B:37:67:0D	00:0B:6B:4D:04:2A	data
	0.313	wlan1	2.4GHz-G	2412	-88	1Mbps	FF:FF:FF:FF:FF:FF	00:0B:6B:4D:02:29	beacon
	0.315	wlan1	2.4GHz-G	2412	-75	36Mbps	00:0B:6B:37:67:0D	00:0B:6B:4D:04:2A	data
	0.326	wlan1	2.4GHz-G	2412	-89	1Mbps	FF:FF:FF:FF:FF:FF	00:02:6F:33:C7:B1	beacon
	0.329	wlan1	2.4GHz-G	2412	-67	1Mbps	FF:FF:FF:FF:FF:FF	00:0B:6B:4D:03:6B	beacon
	0.334	wlan1	2.4GHz-G	2412	-53	1Mbps	FF:FF:FF:FF:FF:FF	00:0B:6B:37:56:94	beacon
	0.336	wlan1	2.4GHz-G	2412	-70	1Mbps	FF:FF:FF:FF:FF:FF	00:0B:6B:4D:04:2A	beacon

150 items (1 selected)

Wireless Standards

- IEEE 802.11b
 - ◆ 2.4GHz, 22MHz bandwidth
 - ◆ 11Mbit max air rate
- IEEE 802.11g
 - ◆ 2.4GHz, 22MHz bandwidth
 - ◆ 802.11b compatibility mode
 - ◆ 54Mbit max air rate
- IEEE 802.11a
 - ◆ 5GHz, 20MHz bandwidth
 - ◆ 54Mbit max air rate

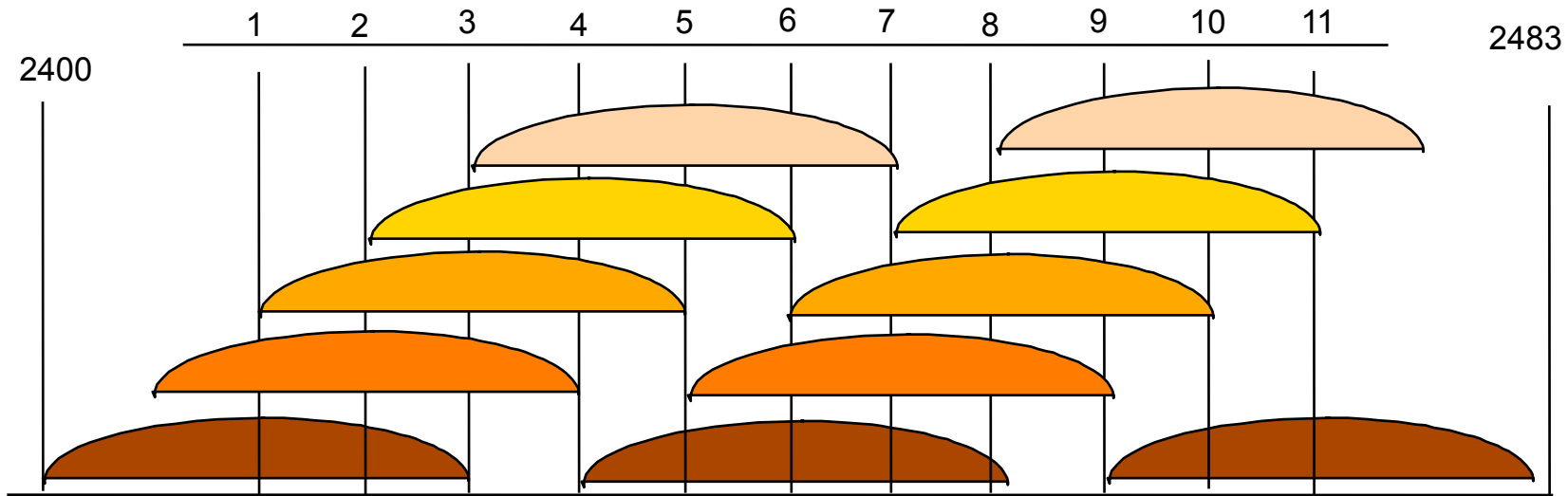
Band Variations

- Double channel (40MHz) – 108Mbit max air rate
 - ◆ 2.4ghz-g-turbo
 - ◆ 5ghz-turbo
- Half channel (10MHz) – 27Mbit max air rate
 - ◆ 2ghz-10mhz
 - ◆ 5ghz-10mhz
- Quarter channel (5MHz) – 13.5Mbit max air rate
 - ◆ 2ghz-5mhz
 - ◆ 5ghz-5mhz

Supported Frequencies

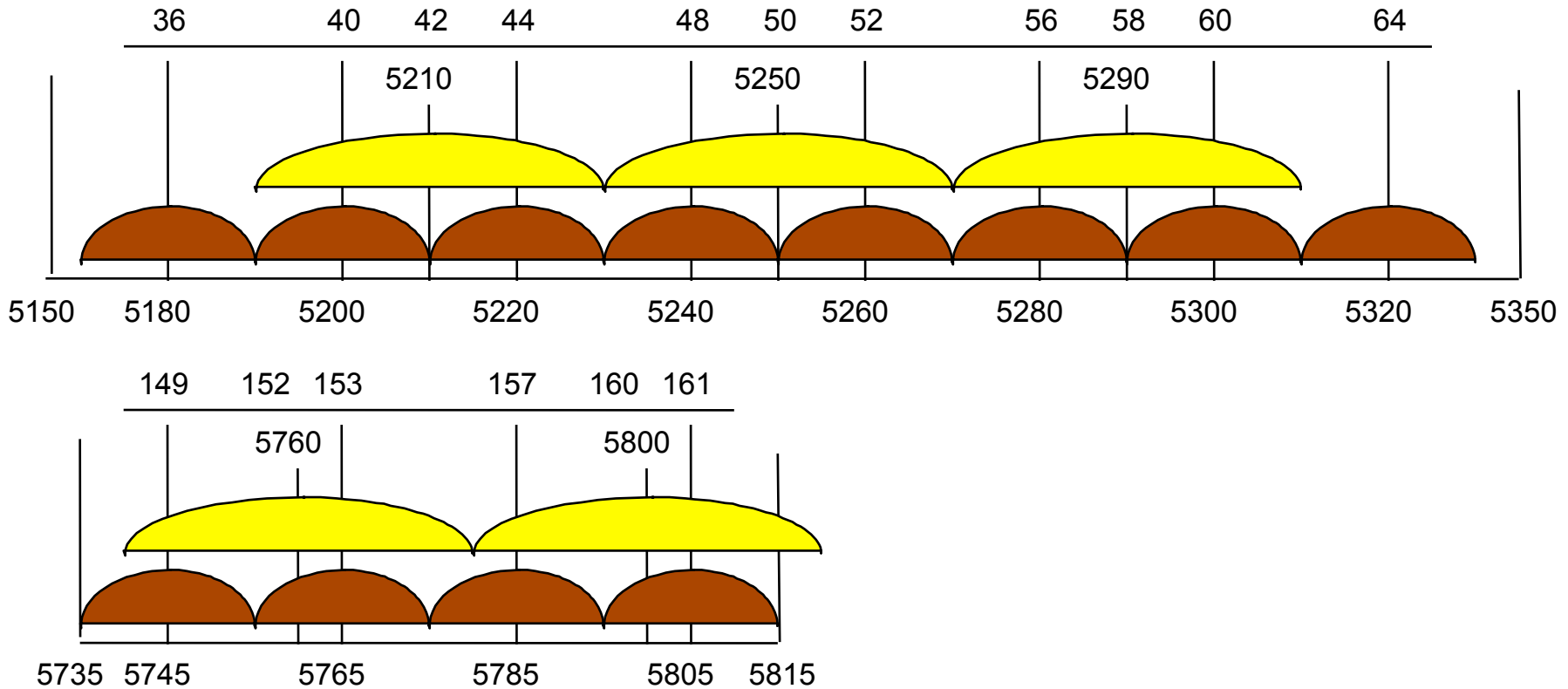
- Wireless cards usually support the following frequencies:
 - ◆ For all 2.4GHz bands: 2192-2539MHz
 - ◆ For all 5GHz bands: 4920-6100MHz
- Your country regulations allow only particular frequency ranges
- Custom frequency license unlocks all frequencies supported by the wireless hardware

Channels- 802.11b/g



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

Channels- 802.11a



- 12 channels, 20 MHz wide
- 5 turbo channels, 40MHz wide

Winbox: Wireless Regulations

The screenshot displays the RouterOS WinBox interface. On the left sidebar, the 'Wireless' menu item is circled in red. A red arrow points from this menu to the 'Wireless Tables' table in the main panel. The table has columns for 'Interface', 'Radio Name', and 'MAC'. The entry for 'wlan1' is circled in red, with its MAC address '000C4205001C' also circled. Another red arrow points from this entry to the 'Interface <wlan1>' configuration window. In this window, the 'Wireless' tab is active, and a red box highlights the regulatory settings: 'Frequency Mode' (regulatory domain), 'Country' (latvia), 'Antenna Gain' (3 dBi), 'DFS Mode' (radar detect), and 'Proprietary Extensions' (post-2.9.25). Other settings visible include 'Radio Name' (0_Teacher), 'Mode' (ap bridge), 'SSID' (ap_rb532), 'Band' (5GHz), 'Frequency' (5180), and 'Security Profile' (default). The status bar at the bottom of the window shows 'disabled', 'running', and 'running ap' options.

Wireless Regulations

- To follow all the regulations in your wireless communication domain you must specify:
 - ◆ **Country** where wireless system will operate
 - ◆ **Frequency mode** as regulatory domain – you will be able to use only allowed channels with allowed transmit powers
 - ◆ **Antenna gain** of antenna attached to this router
 - ◆ **DFS mode** – periodically will check for less used frequency and change to it
 - ◆ **(Proprietary-extensions to post-2.9.25)**

Wireless Country Settings Lab

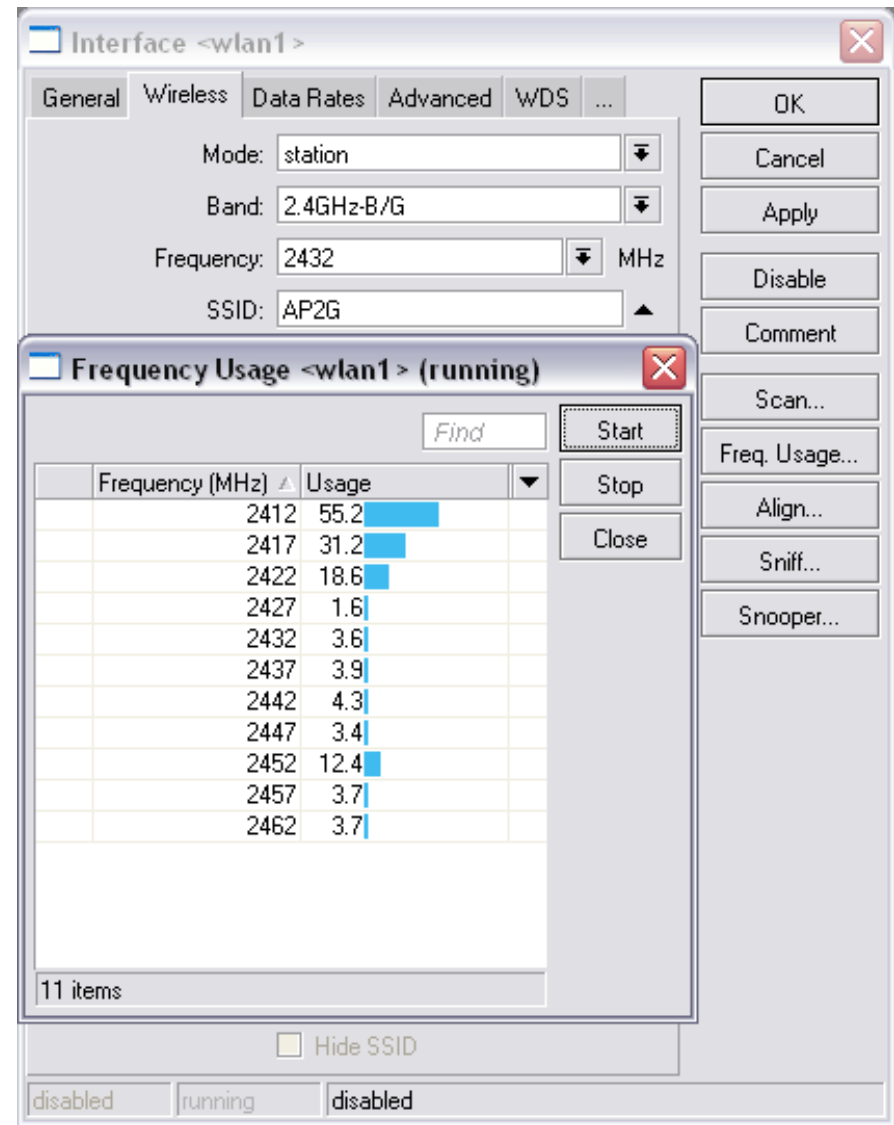
- Open terminal
- Issue “/interface wireless info print” command
- Change country to “australia”
- Issue “/interface wireless info print” command
- Compare results
- Set country back to 'no_country_set'

Access Point

- Creates wireless infrastructure
- Participates in Wireless Area
- Expects stations to follow its frequency (DFS)
- Authentication based on Access List

Frequency Usage Tool

- Frequency Usage Monitor looks only for IEEE 802.11 frames
- Interface is disabled during the Frequency usage monitor



Wireless Snooper Tool

Snooper <wlan1> (running)

Networks Stations

Find

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

35 items (1 selected)

Start Stop Close Settings...

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

General Beacon Mikrotik

OK Cancel

Frequency: 2432 MHz

Band: 2.4GHz-B/G

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

SSID: AP2G

Of Freq.: 12.8 %

Of Traf.: 83.4 %

Bandwidth: 3.7 Mbps

Stations: 2

SSID source: beacon

Supported Rates: 1Mbps 2Mbps 5.5Mbps...

Basic Rates: 1Mbps 2Mbps 5.5Mbps...

Capabilities: ess short-preamble

Wireless AP/Station Lab

- Work in pairs to make AP/Station connection with your neighbor's router
- Create a AP on the wlan1 interface in 5Ghz band with SSID “apXY” where XY is your number
- On wlan2 interface create a station to connect to your neighbor's AP (you need to know the neighbor's AP SSID)
- Make a backup from this configuration

Registration Table

Wireless Tables

Interfaces Access List **Registration** Connect List Security Profiles

← Copy to Access List 00 Reset

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

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

General Signal Nstreme Statistics

Radio Name: X_unknown

MAC Address: 00:0C:42:05:00:1C

Interface: wlan1

Uptime: 00:01:37

Ack. Timeout: 25 us

RouterOS Version: 2.9.XX

AP Tx Limit:

Client Tx Limit:

Last IP:

AP
 WDS

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

General **Signal** Nstreme Statistics

Last Activity: 0.000 s

Signal Strength: -58 dBm

Tx Signal Strength: -53 dBm

Signal To Noise: 37 dB

Tx/Rx CCQ: 93/95 %

Signal Strengths

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

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

General Signal Nstreme **Statistics**

Tx/Rx Rate: 54Mbps

Tx/Rx Packets: 550/794745

Tx/Rx Bytes: 41576/1202538377

Tx/Rx Frames: 550/794804

Tx/Rx Frame Bytes: 38630/1197770772

Tx/Rx Hw Frames: 550/794813

Tx/Rx Hw. Frame Bytes: 51830/1216846302

OK
Cancel

Access Management

- *default-forwarding* (on AP) – whether the wireless clients may communicate with each other directly (access list may override this setting for some particular clients)
- *default-authentication* – enables AP to register a client even if it is not in access list. In turn for client it allows to associate with AP not listed in client's connect list

Wireless Access List

- Individual settings for each client in access list will override the interface default settings
- Access list entries can be made from the registration table entries by using action 'Copy to Access List'
- Access list entries are ordered, just like in firewall
- Matching by all interfaces “interface=all”
- “Time” - works just like in firewall

Wireless Access list

The screenshot displays a network configuration window titled "Wireless Tables". It features several tabs: "Interfaces", "Nstreme Dual", "Access List", "Registration", "Connect List", and "Security Profiles". The "Access List" tab is active, showing a table with two entries. The first entry is selected.

MAC Address	Interface	Signal Str...	Authentication	Forwarding
00:0C:42:0C:0A:ED	wlan1	-120..120	no	no
00:0C:42:0C:0A:ED	wlan1	-120..120	yes	yes

Below the table, it indicates "2 items (1 selected)".

An "AP Access Rule" dialog box is open for the selected rule. It contains the following fields and options:

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

Buttons on the right side of the dialog include: OK, Cancel, Apply, Disable, Comment, Copy, and Remove.

Wireless Access List

AP Access Rule <00:0C:42:0C:0A:ED> ✖

MAC Address:

Interface: ▾

Signal Strength Range:

AP Tx Limit: ▲

Client Tx Limit: ▲

Authentication

Forwarding

Private Key: ▾ 0x

Private Pre Shared Key:

Time:

disabled

OK
Cancel
Apply
Disable
Comment
Copy
Remove

Wireless Access List Lab

- Check if the neighbor's wireless router is connected to your AP interface (wlan1)
- Disable the default interface settings on wlan1: default-forwarding, default-authentication
- Make sure that nobody is connected to your AP
- Add access list entry with your neighbor's MAC address and make sure it connects

Wireless RADIUS Authentication

The screenshot shows the Mikrotik WinBox interface. At the top, there is a 'Wireless Tables' window with tabs for 'Interfaces', 'Nstreme Dual', 'Access List', 'Registration', 'Connect List', and 'Security Profiles'. Below the tabs is a table with columns: Name, Mode, Authentication..., Unicast Ciphers, Group Ciphers, and WPA Pre-Shared Key. The table contains one row with 'default' in the Name column and 'none' in the Mode column. Below the table is a 'Security Profile <default>' dialog box. The dialog has tabs for 'General', 'RADIUS', 'EAP', and 'Static Keys'. The 'RADIUS' tab is selected. The 'Name' field is 'default' and the 'Mode' is 'none'. There are sections for 'Authentication Types', 'Unicast Ciphers', and 'Group Ciphers', each with checkboxes for 'WPA PSK', 'WPA EAP', 'WPA2 PSK', 'WPA2 EAP', 'tkip', and 'aes ccm'. There are also fields for 'WPA Pre-Shared Key', 'WPA2 Pre-Shared Key', 'Supplicant Identity' (set to 'MikroTik'), and 'Group Key Update' (set to '00:05:00'). Buttons for 'OK', 'Cancel', 'Apply', 'Copy', and 'Remove' are on the right.

This screenshot shows the 'Security Profile <default>' dialog box with the 'RADIUS' tab selected. The 'Name' and 'Mode' fields are the same as in the previous screenshot. The 'Authentication Types' section has 'MAC Authentication' and 'MAC Accounting' checked, and 'EAP Accounting' unchecked. The 'Interim Update' field is set to '00:00:00'. The 'MAC Format' field is set to 'XX:XX:XX:XX:XX:XX'. The 'MAC Mode' field is set to 'as username'. The 'OK', 'Cancel', 'Apply', 'Copy', and 'Remove' buttons are visible on the right side of the dialog.

Wireless Connect List

- Allow or deny clients from connecting to specific AP by using Connect list
- Connect list entries can be made from the registration table entries by using action 'Copy to Access List'
- Connect list entries are ordered, just like in firewall
- Used also for WDS links

Wireless Connect List

New Station Connect Rule

Interface: wlan1

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

Connect

SSID: AP2G

Area Prefix:

Signal Strength Range: -120..120

Security Profile: default

OK
Cancel
Apply
Disable
Comment
Copy
Remove

disabled

1

New Station Connect Rule

Interface: wlan1

MAC Address:

Connect

SSID: AP2G

Area Prefix:

Signal Strength Range: -75..120

Security Profile: default

OK
Cancel
Apply
Disable
Comment
Copy
Remove

disabled

2

New Station Connect Rule

Interface: wlan1

MAC Address:

Connect

SSID:

Area Prefix:

Signal Strength Range: -120..120

Security Profile: default

OK
Cancel
Apply
Disable
Comment
Copy
Remove

disabled

3

Wireless Connect List

Wireless Tables

Interfaces Nstreme Dual Access List Registration Connect List Security Profiles

+ - ✓ ✗ 📁 Find

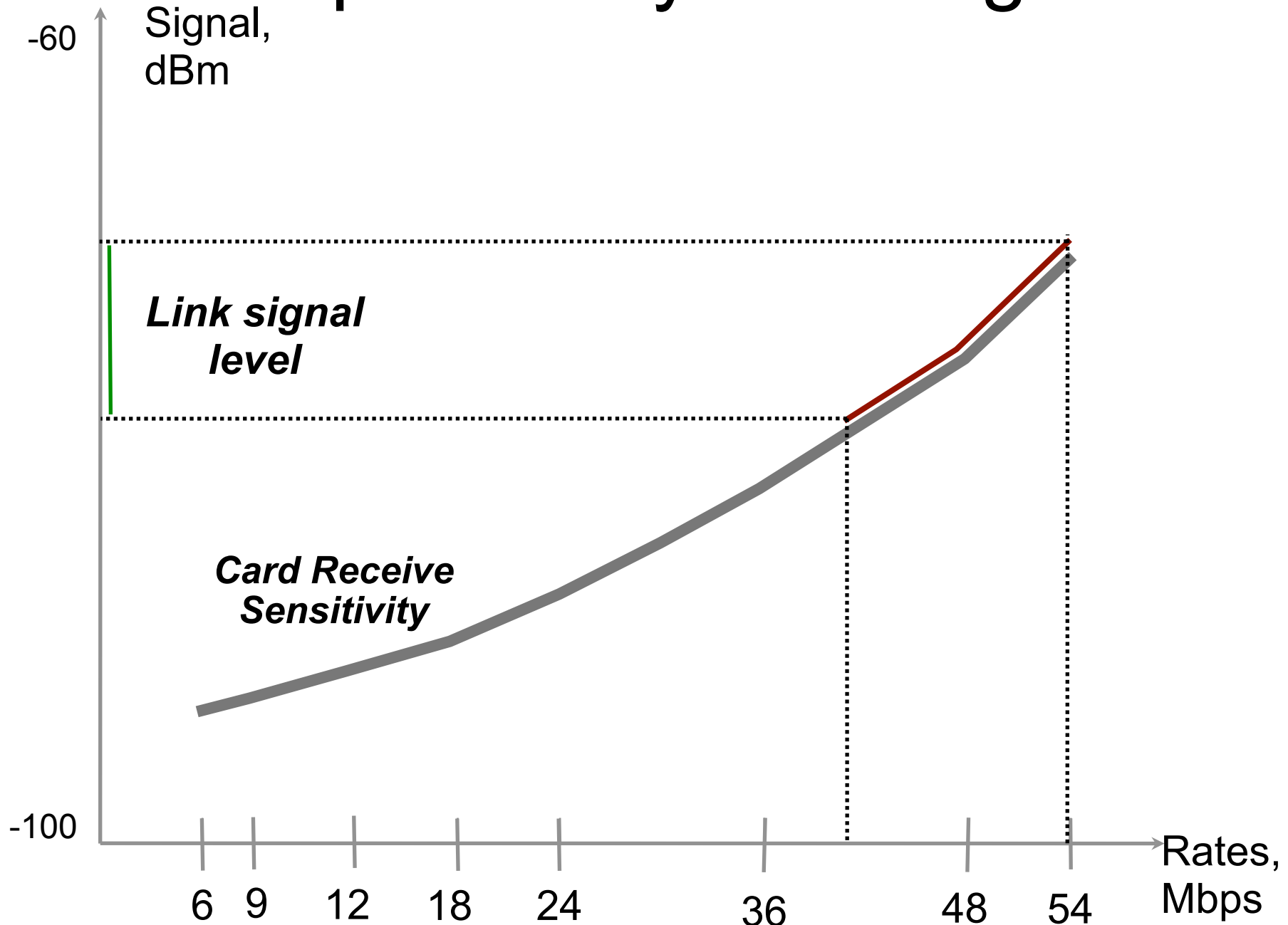
#	Interface	MAC Address	Connect	Area Prefix	Signal Str...	Security ...
0	wlan1	00:02:6F:45:15:43	yes		-120..120	default
1	wlan1		yes		-75..120	default
2	wlan1		no		-120..120	default

3 items (1 selected)

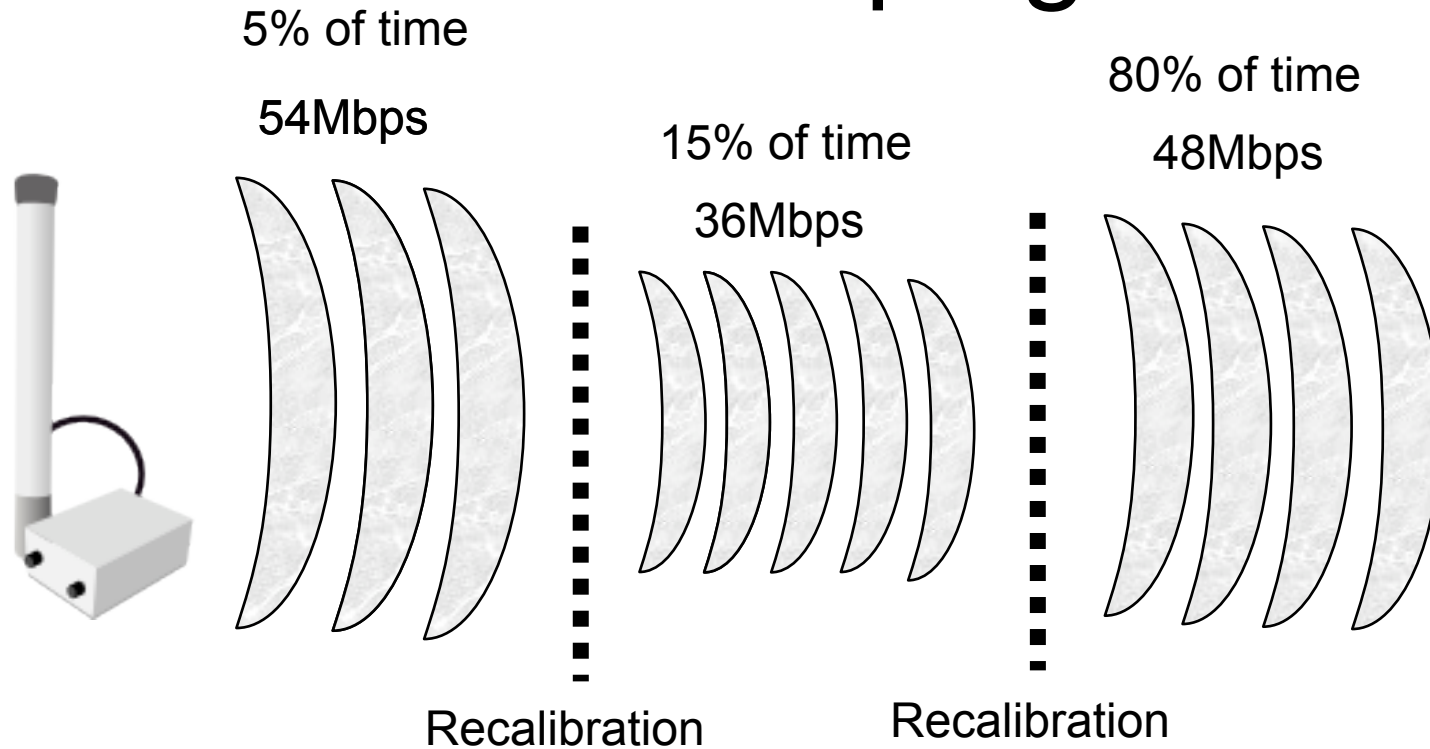
Wireless Connect List Lab

- On the AP interface (wlan1) set SSID to “CHAOS”
- On the Station interface (wlan2) leave the SSID field empty
- Add connect list entry for wlan2 interface to connect to your neighbor's AP (you will need the neighbor's AP MAC address)

Rate Dependency from Signal Level



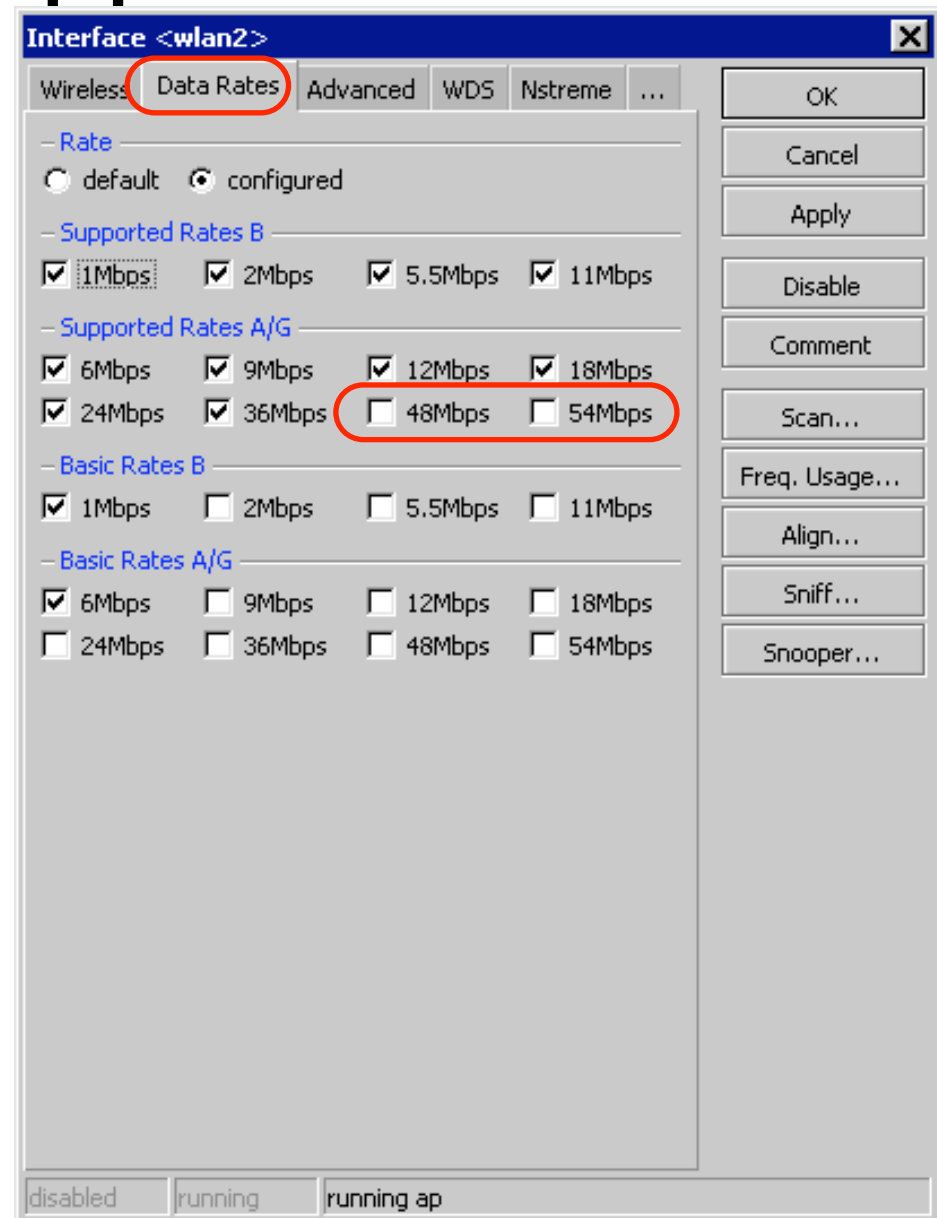
Rate Jumping



- You can optimize link performance, by avoiding rate jumps, in this case link will work more stable at 36Mbps rate

Basic and Supported Rates

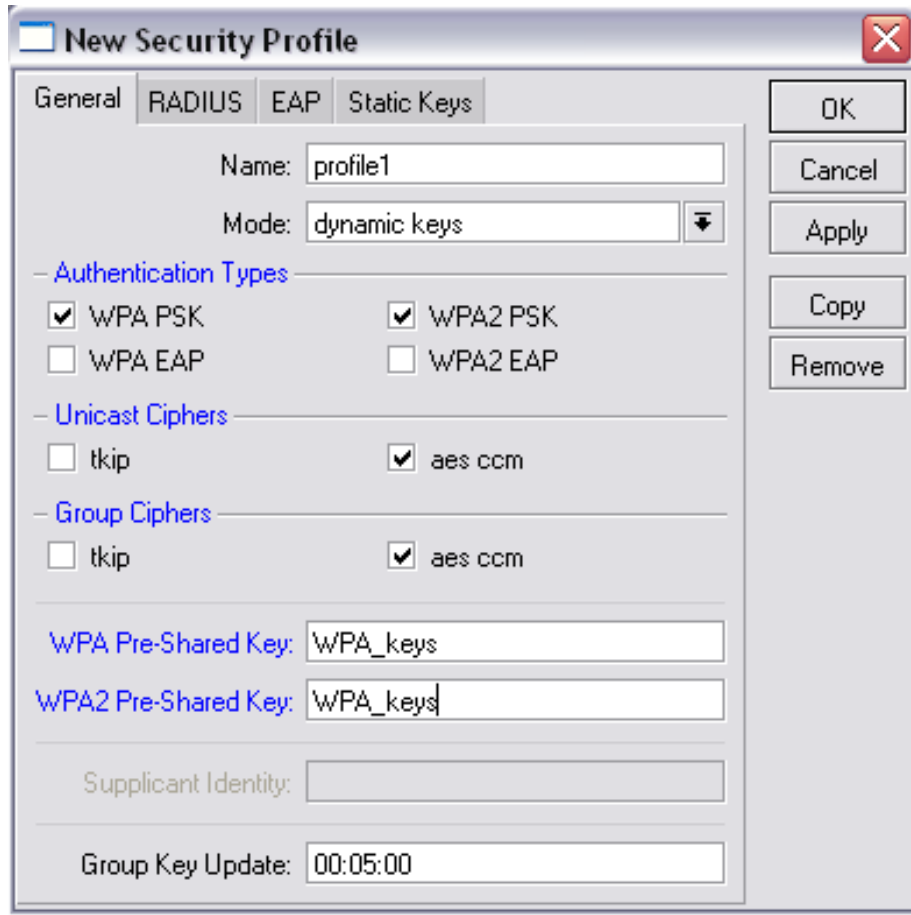
- Supported rates – client data rates
- Basic rates – link management data rates
- If router can't send or receive data at basic rate – link goes down



Wireless MultiMedia (WMM)

- 4 transmit queues with priorities:
 - ◆ 1,2 – background
 - ◆ 0,3 – best effort
 - ◆ 4,5 – video
 - ◆ 6,7 – voice
- Priorities set by
 - ◆ Bridge or IP firewall
 - ◆ Ingress (VLAN or WMM)
 - ◆ DSCP

Wireless Encryption



New Security Profile

General | RADIUS | EAP | Static Keys

Name: profile1

Mode: dynamic keys

Authentication Types

WPA PSK WPA2 PSK
 WPA EAP WPA2 EAP

Unicast Ciphers

tkip aes ccm

Group Ciphers

tkip aes ccm

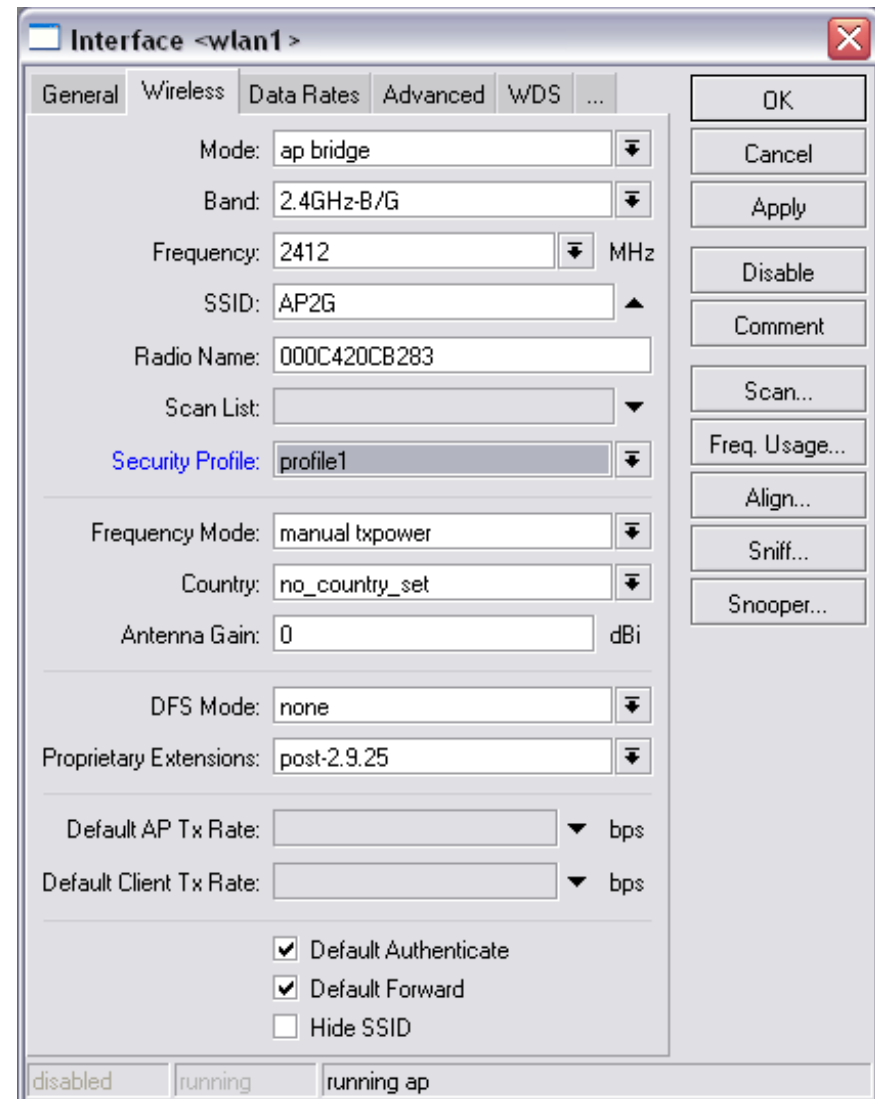
WPA Pre-Shared Key: WPA_keys

WPA2 Pre-Shared Key: WPA_keys

Supplicant Identity:

Group Key Update: 00:05:00

OK, Cancel, Apply, Copy, Remove



Interface <wlan1>

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

Mode: ap bridge

Band: 2.4GHz-B/G

Frequency: 2412 MHz

SSID: AP2G

Radio Name: 000C420CB283

Scan List:

Security Profile: profile1

Frequency Mode: manual txpower

Country: no_country_set

Antenna Gain: 0 dBi

DFS Mode: none

Proprietary Extensions: post-2.9.25

Default AP Tx Rate: bps

Default Client Tx Rate: bps

Default Authenticate
 Default Forward
 Hide SSID

disabled | running | running ap

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

Wireless Encryption

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

OK Cancel Apply Copy Remove

New Security Profile

General | RADIUS | EAP | Static Keys

EAP Methods: passthrough

TLS Mode: no certificates

TLS Certificate: none

OK Cancel Apply Copy Remove

Wireless Encryption Lab

- Create a new security profile with options:
mode=dynamic-keys
authentication-type=wpa2-psk
group/unicast ciphers=aes-ccm
wpa2-key=wireless
- Apply the new profile to wlan1 and check if the neighbors wireless client connects

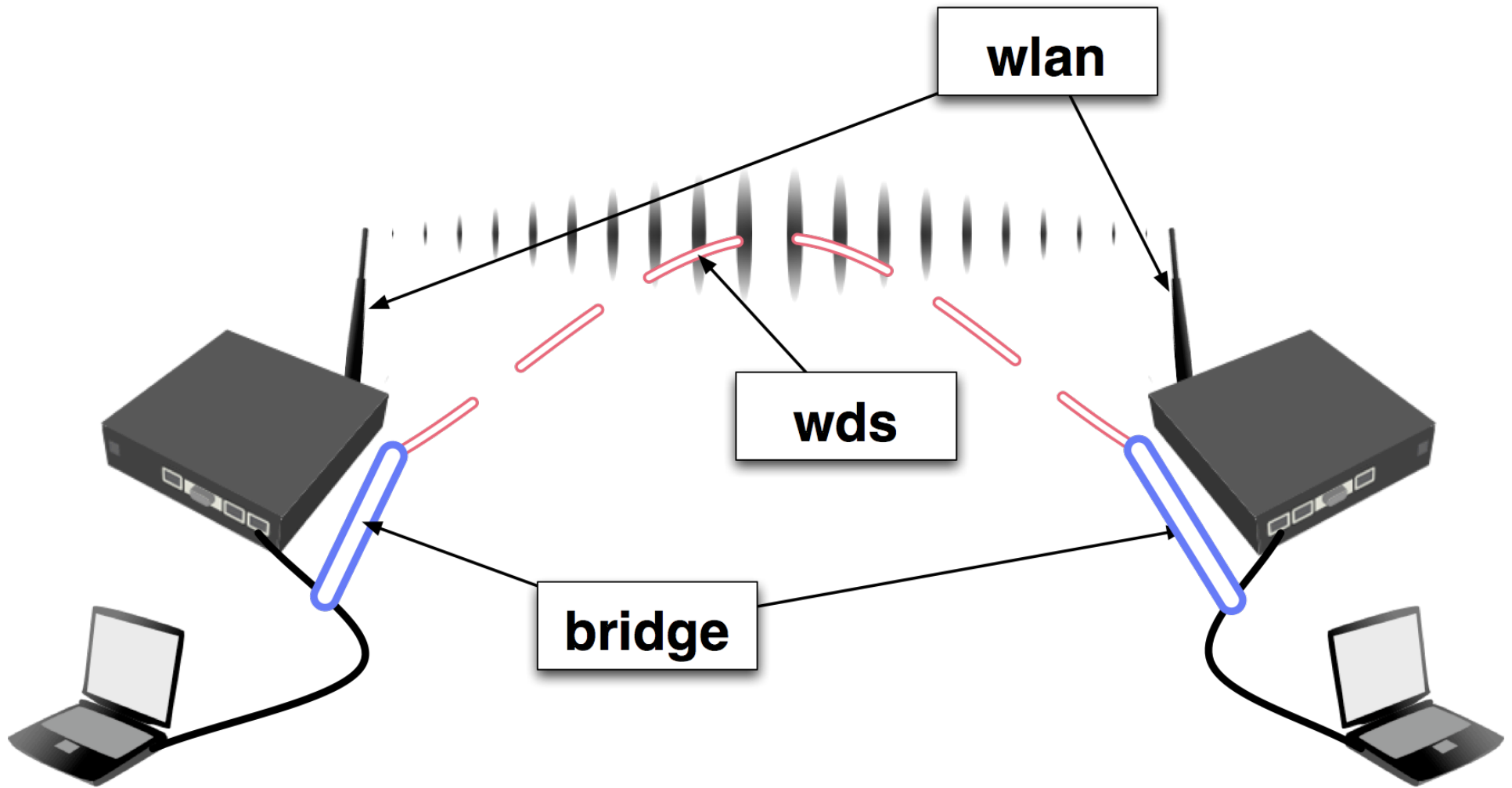
Wireless Distribution System

- WDS (Wireless Distribution System) allows packets to pass from one AP to another, just as if the APs were ports on a wired Ethernet switch
- APs must use the same band and SSID and operate on the same frequency in order to connect to each other
- WDS is used to make bridged networks across the wireless links and to extend the span of the wireless network

Wireless Distribution System

- WDS link can be created between wireless interfaces in several mode variations:
 - ◆ bridge/ap-bridge – bridge/ap-bridge
 - ◆ bridge/ap-bridge – wds-slave
 - ◆ bridge/ap-bridge – station-wds
- You must disable DFS setting when using WDS with more than one AP

Simple WDS Topologies

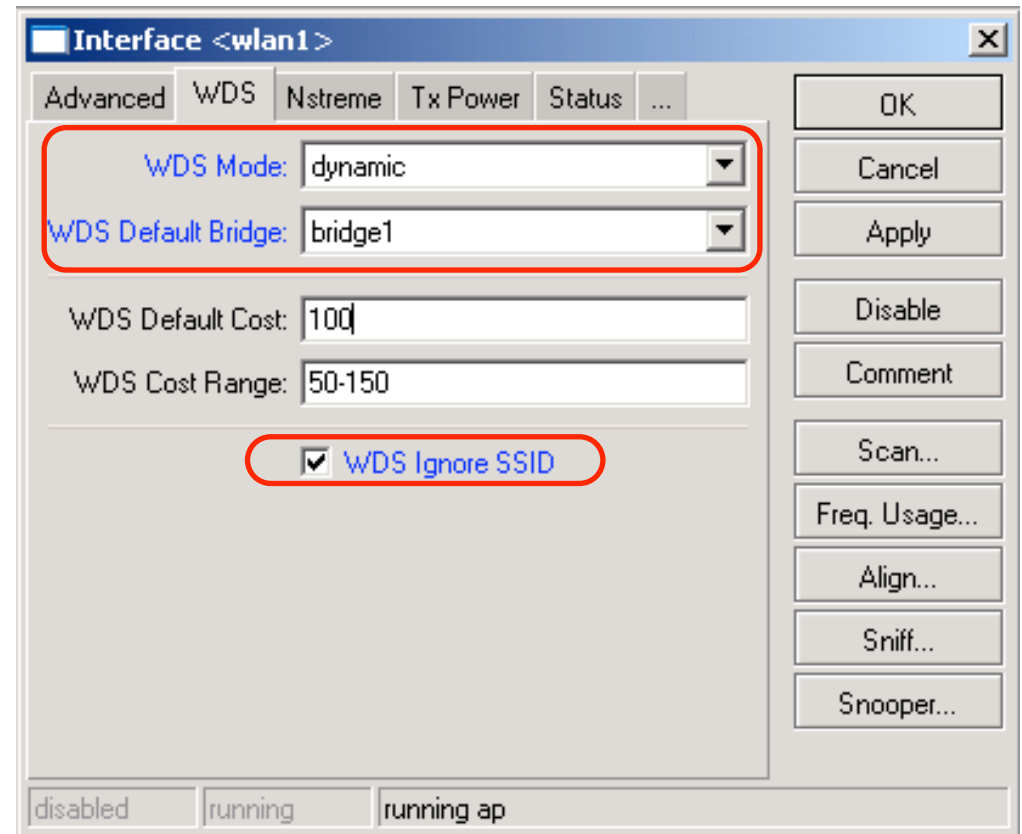


Dynamic WDS Interface

- It is created 'on the fly' and appears under wds menu as a dynamic interface ('D' flag)
- When the link between WDS devices goes down, attached IP addresses will slip off from WDS interface
- Specify “wds-default-bridge” parameter and attach IP addresses to the bridge

Dynamic WDS Configuration

- WDS can be created between two APs, both must have WDS (static or dynamic) feature enabled
- APs must have same SSID or the “WDS ignore SSID” feature enabled
- We must create a bridge to use dynamic wds feature



Bridge Creation

The screenshot shows the RouterOS WinBox interface. On the left sidebar, the 'Bridge' menu item is highlighted with a red circle. An arrow points from this menu item to a '+' icon in the Bridge management window. Another arrow points from the '+' icon to the 'rstp' radio button in the 'Interface <bridge1>' configuration window.

Bridge Management Window

Name	MAC Address	Mode
R bridge1	00:00:00:0...	none

Interface <bridge1> Configuration Window

General STP Status Traffic

Protocol Mode

none stp **rstp**

Priority: 8000 hex

Max Message Age: 00:00:20

Forward Dealy: 00:00:15

Transmit Hold Count: 6

Ageing Time: 00:05:00

disabled running

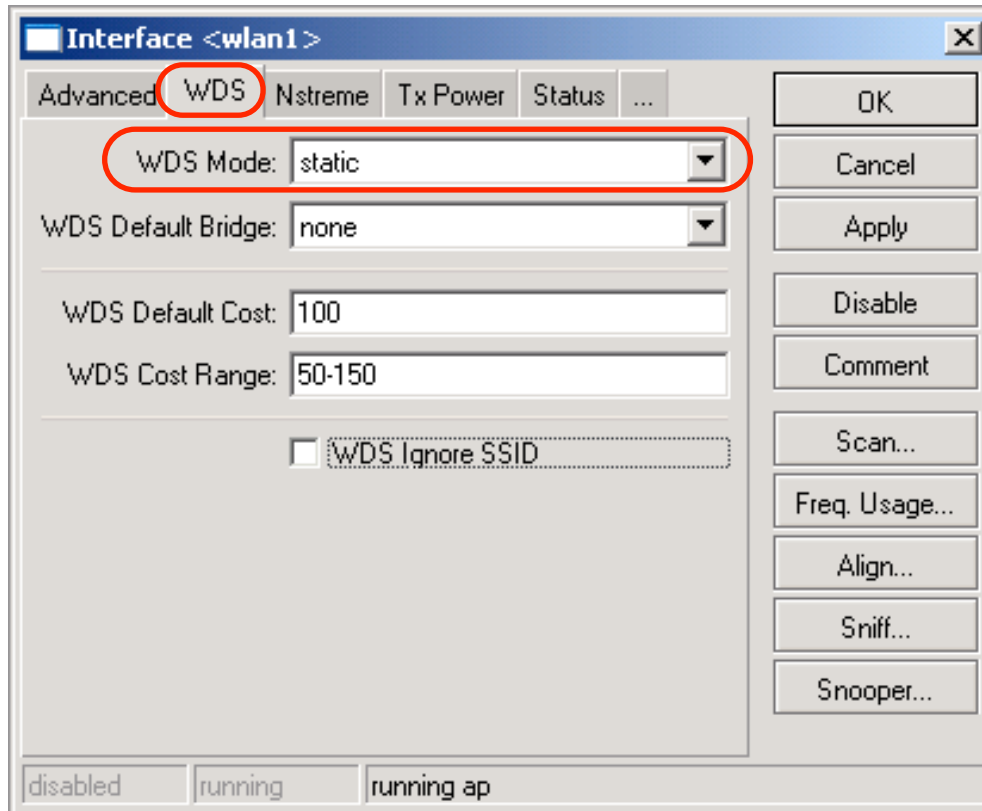
Dynamic WDS Lab

- Create a bridge interface with protocol-mode=rstp
- Make sure that wlan1 interface is set to “ap-bridge” mode and choose with your neighbor an equal SSID
- Enable the dynamic WDS mode on the wlan1 and specify the default-wds-bridge option to use bridge1
- Add 10.1.1.XY/24 IP to the bridge interface
- Check your network: From Your router try to ping neighbors router
- Optional: Add ether1 to the bridge and change laptops IP to 10.1.1.1XY/24

Static WDS

- It should be created manually
- It requires the destination MAC address and master interface parameters to be specified manually
- Static WDS interfaces never disappear, unless you disable or remove them

Static WDS



- To use static WDS use “ap-bridge” mode
- Set WDS mode to “static” and WDS default bridge to “none”
- Create static WDS interfaces

Static WDS Interface

Wireless Tables

Interfaces Access List Registration Connect List Security Profiles

+ - ✓ ✗

VirtualAP	Type	MTU	MAC Address	Mode	Band	Frequency	SSID
WDS	Wireless (Athero...	1500					
Nstreme Dual	Wireless (Athero...	1500					
R wlan1	Wireless (Athero...	1500					
RA wds1	WDS	1500					

New Interface

General WDS Traffic

Master Interface: wlan1

WDS Address: <clients MAC address>

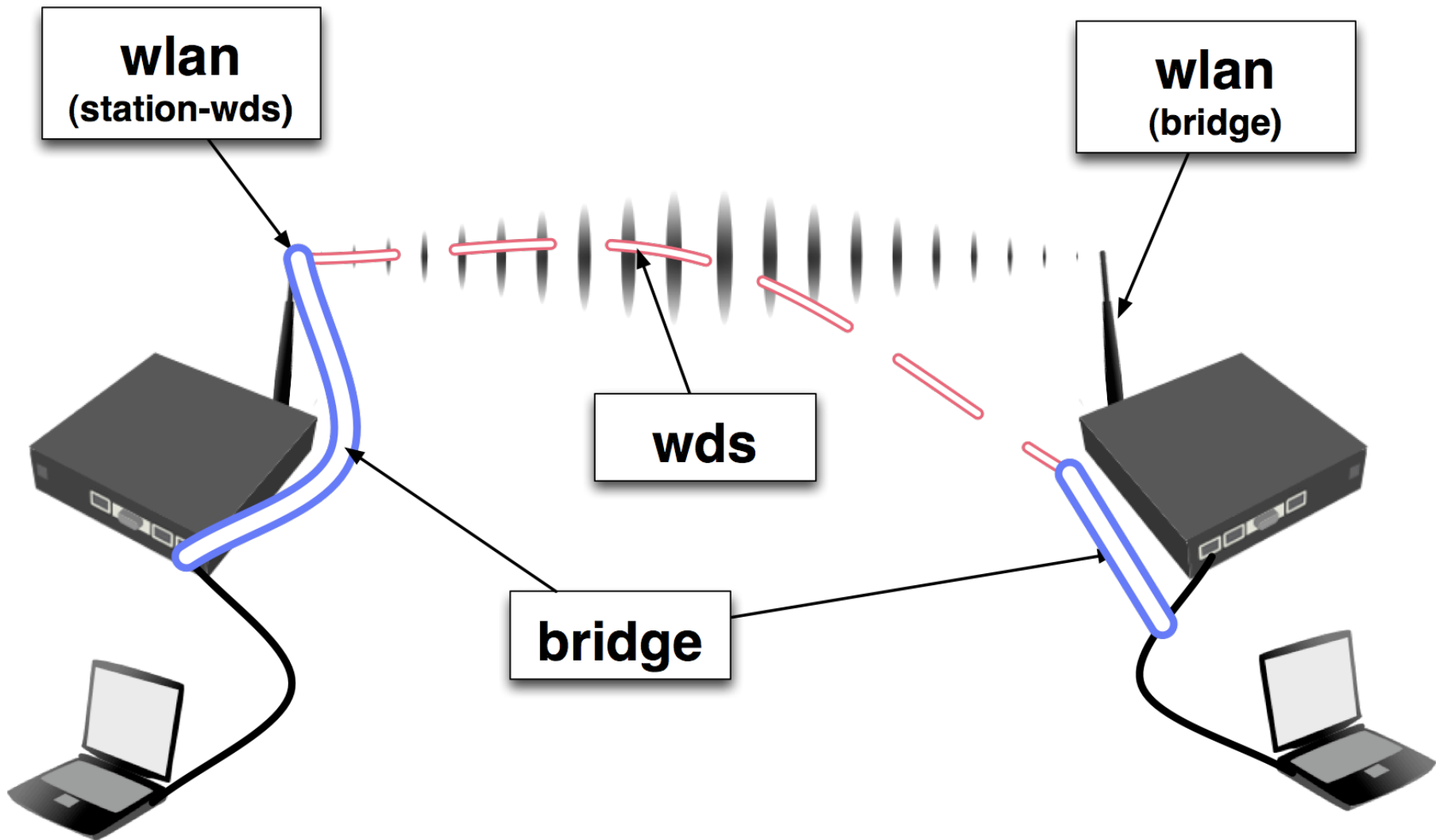
OK Cancel Apply Disable Comment

disabled running

Static WDS Lab

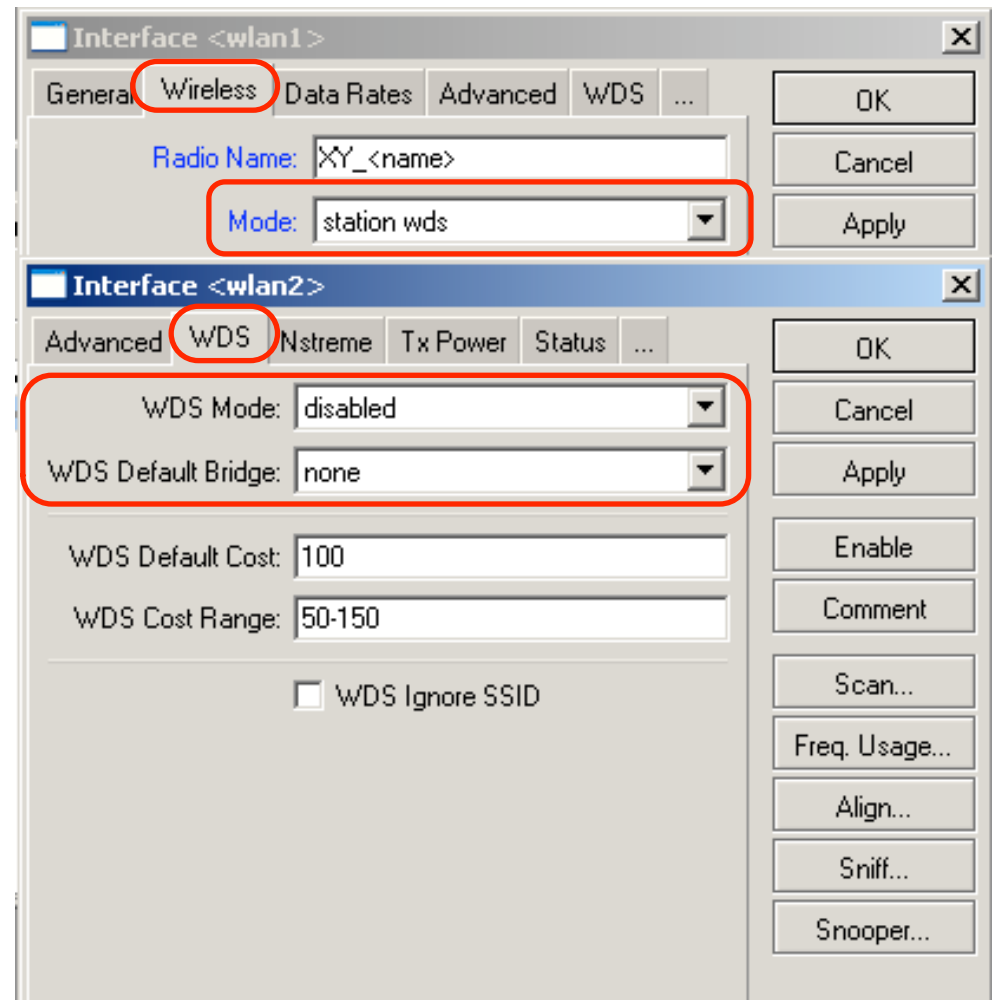
- Adjust setup from the previous lab, to use WDS static mode
 - ◆ Configure your wireless card accordingly
 - ◆ Create the static WDS interface
 - ◆ Add necessary ports to the bridge
- Optional: Add ether1 to the bridge and change laptops IP to 10.1.1.1XY/24

Station-WDS



Station-WDS

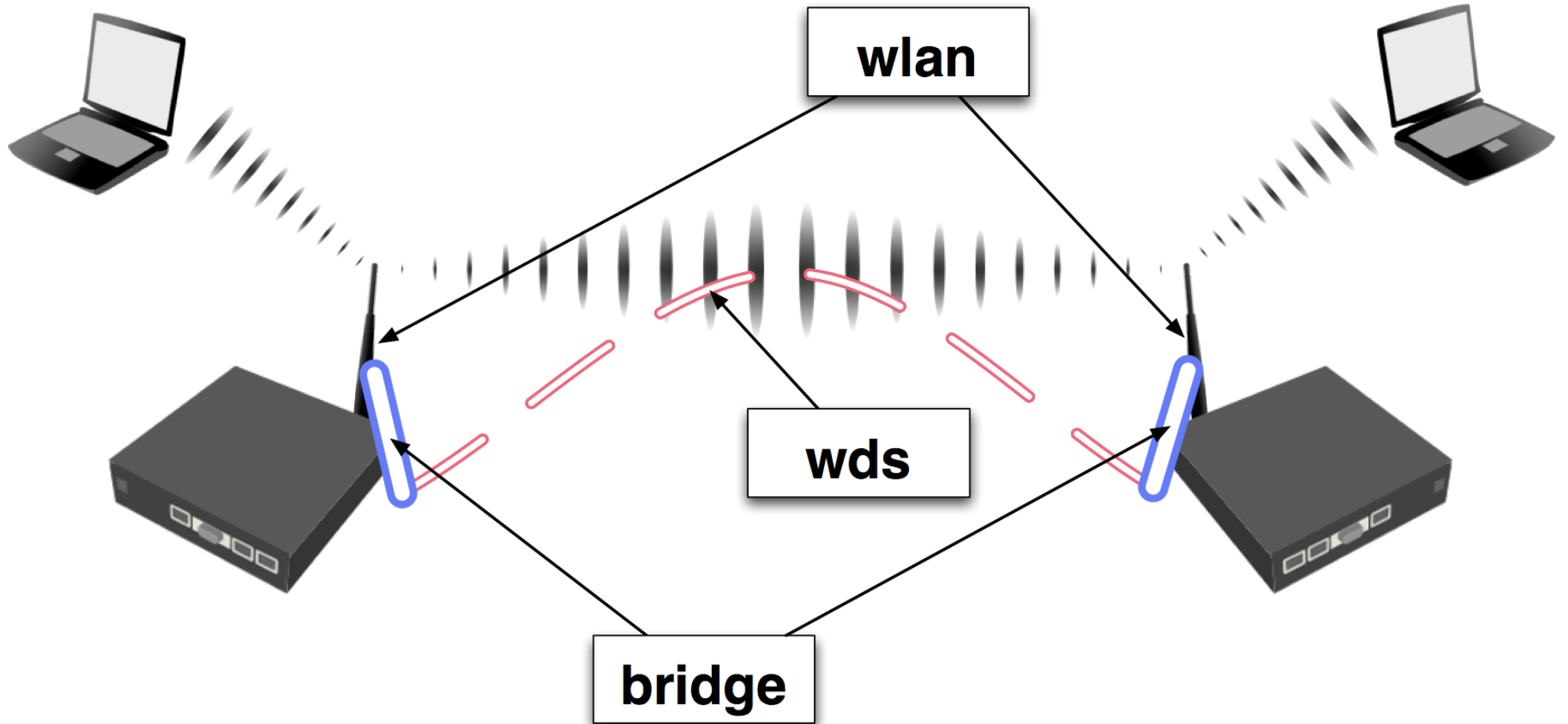
- Use station-wds mode to create clients with WDS capabilities
- WDS-mode must be disabled on the wireless card
- Now your wireless interface will work in the bridge



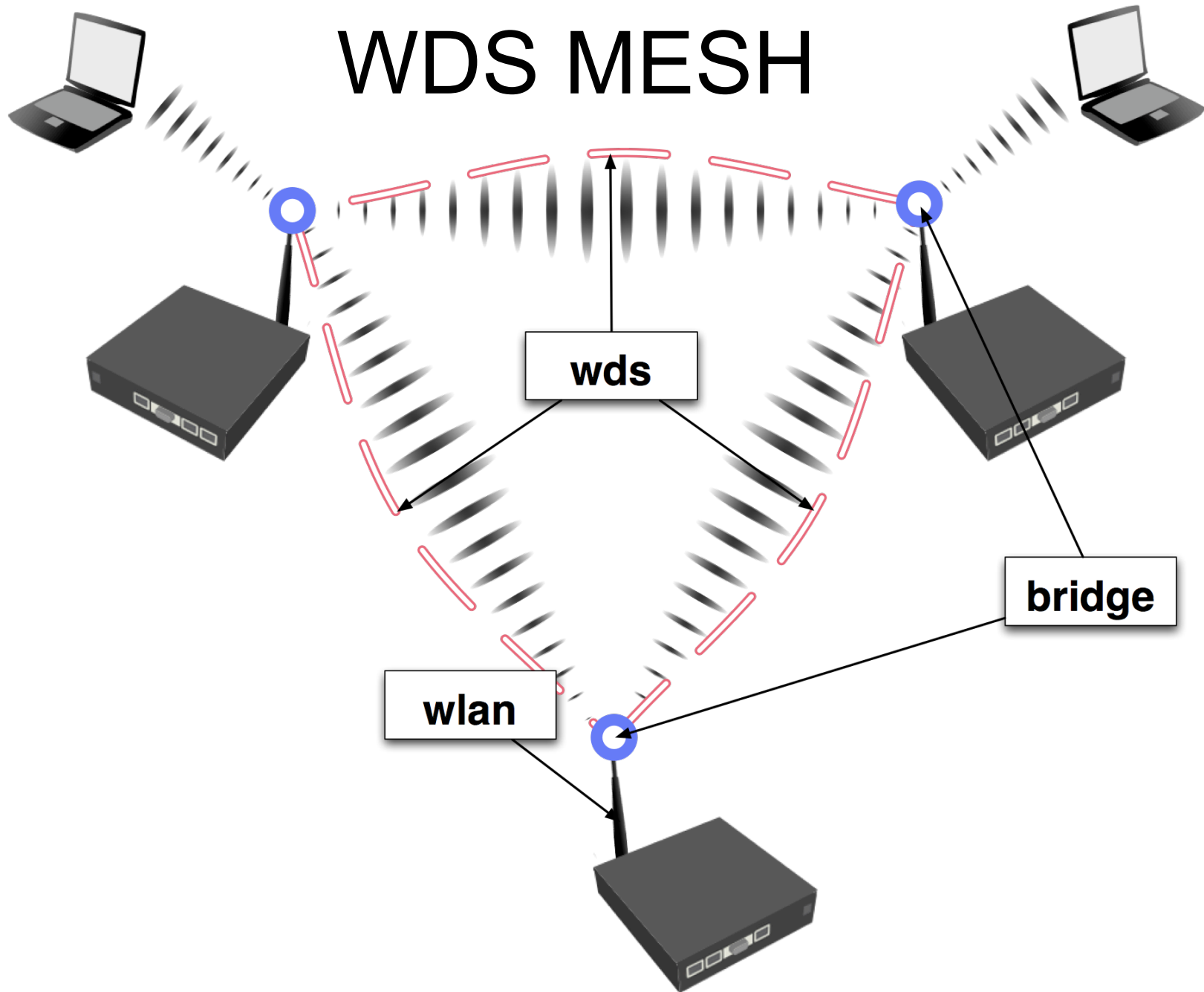
Station-WDS Lab

- Adjust setup from the previous lab, to use only one router as access point and other router as station with WDS capability
- Optional: Switch places (AP becomes client, client becomes AP) and repeat the setup.
- Optional: Add ether1 to the bridge and change laptops IP to 10.1.1.1XY/24

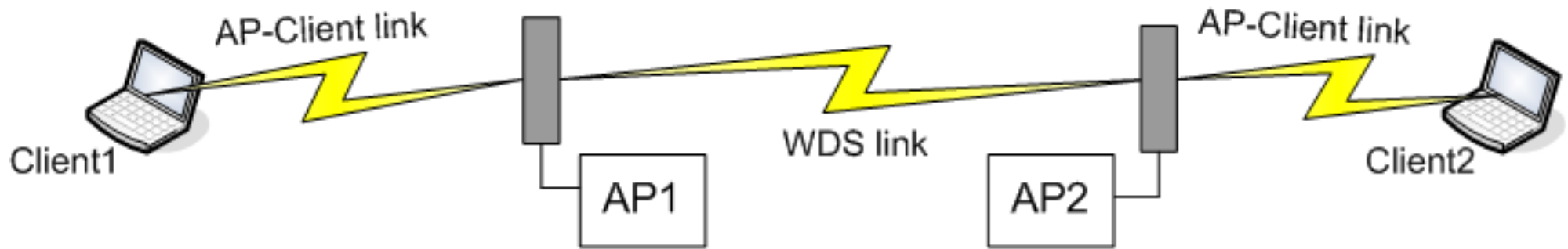
Simple MESH using WDS



WDS MESH

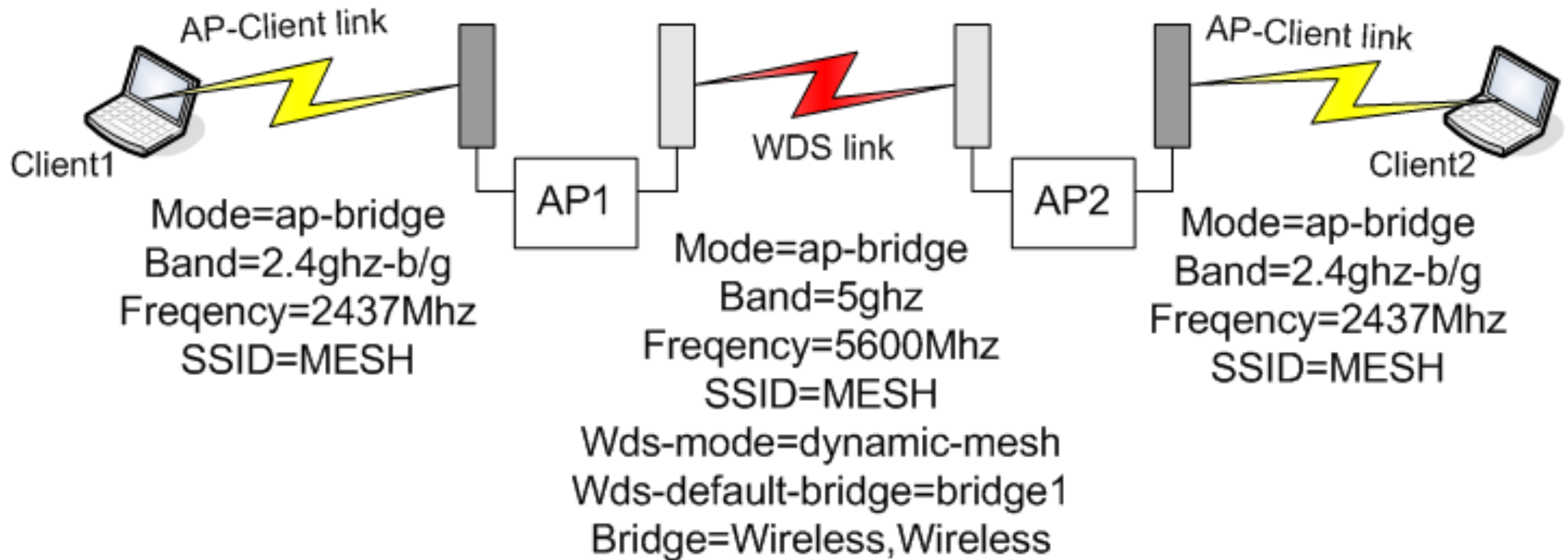


Simple MESH

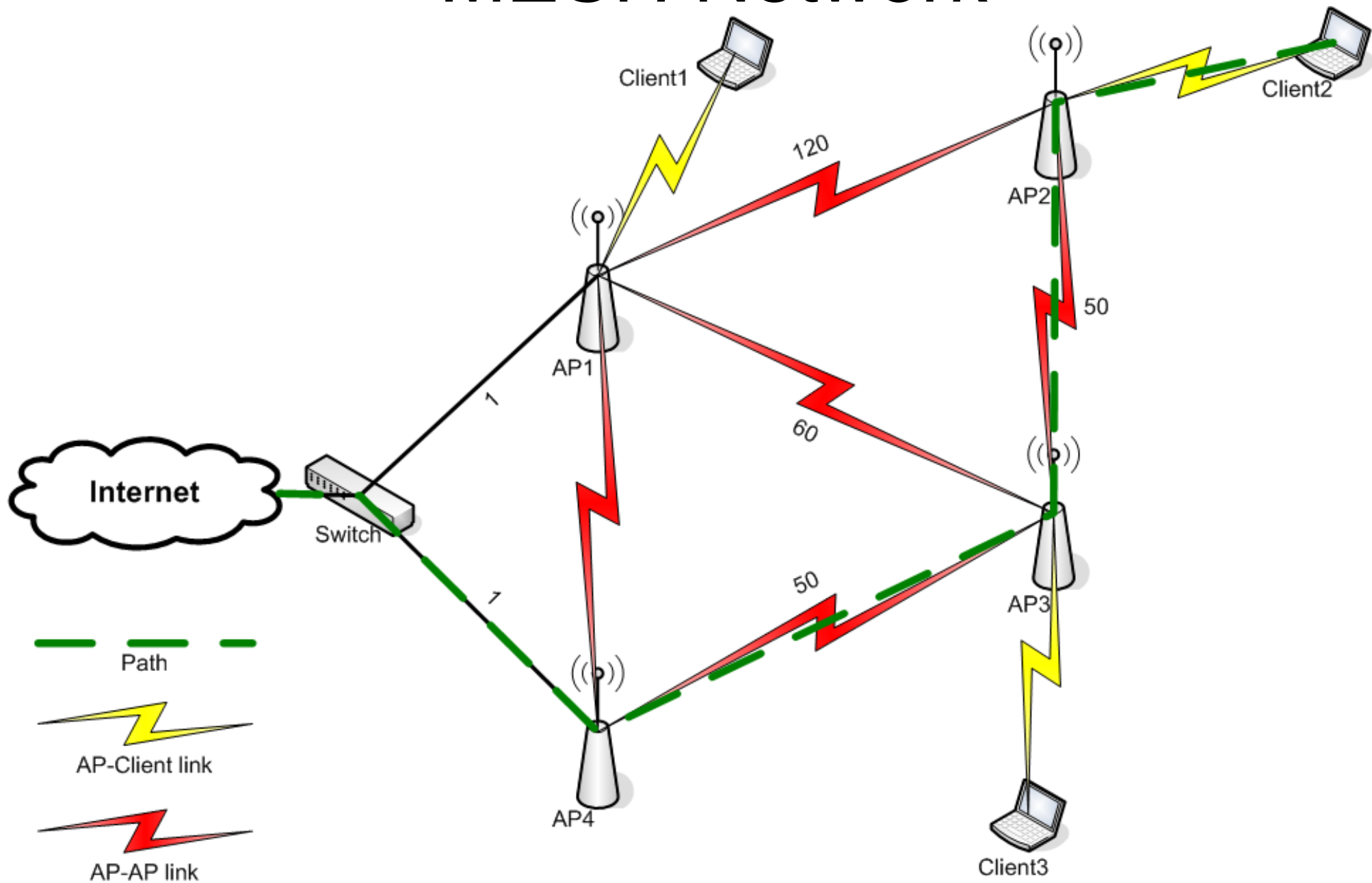


Mode=ap-bridge
Band=2.4ghz-b/g
Frequency=2437Mhz
SSID=MESH
Wds-mode=dynamic-mesh
Wds-default-bridge=bridge1
Bridge=Wireless

Dual Band MESH

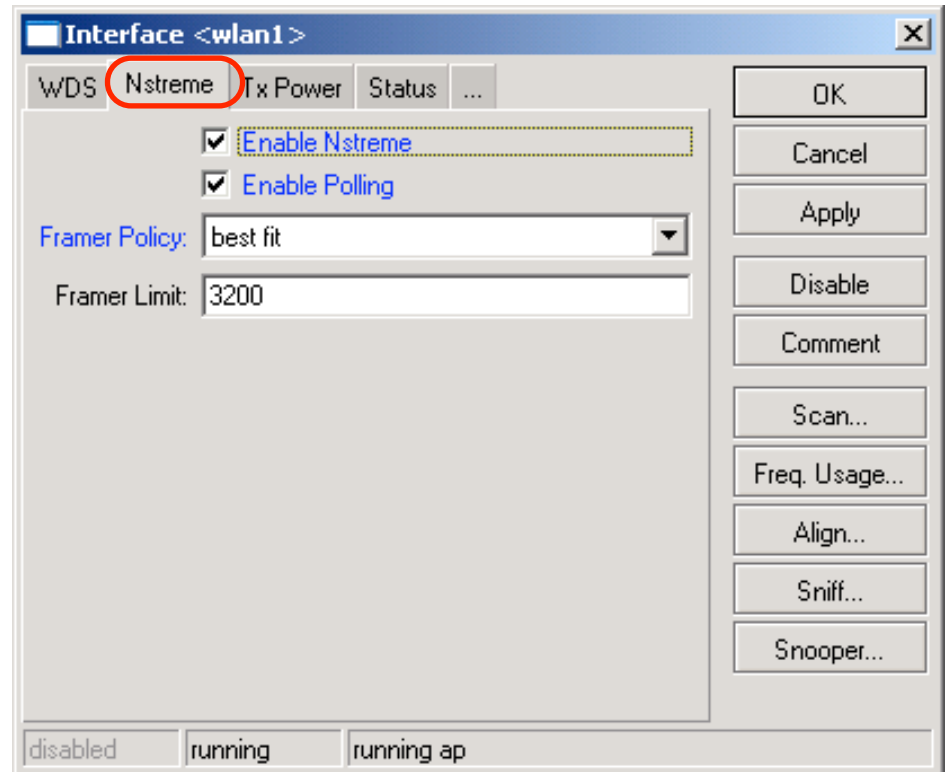


MESH Network



MikroTik Nstreme

- Nstreme is MikroTik's proprietary (i.e., incompatible with other vendors) wireless protocol created to improve point-to-point and point-to-multipoint wireless links.



Nstreme Protocol

Benefits of Nstreme protocol:

- Client polling
- Very low protocol overhead per frame allowing super-high data rates
- No protocol limits on link distance
- No protocol speed degradation for long link distances
- Dynamic protocol adjustment depending on traffic type and resource usage

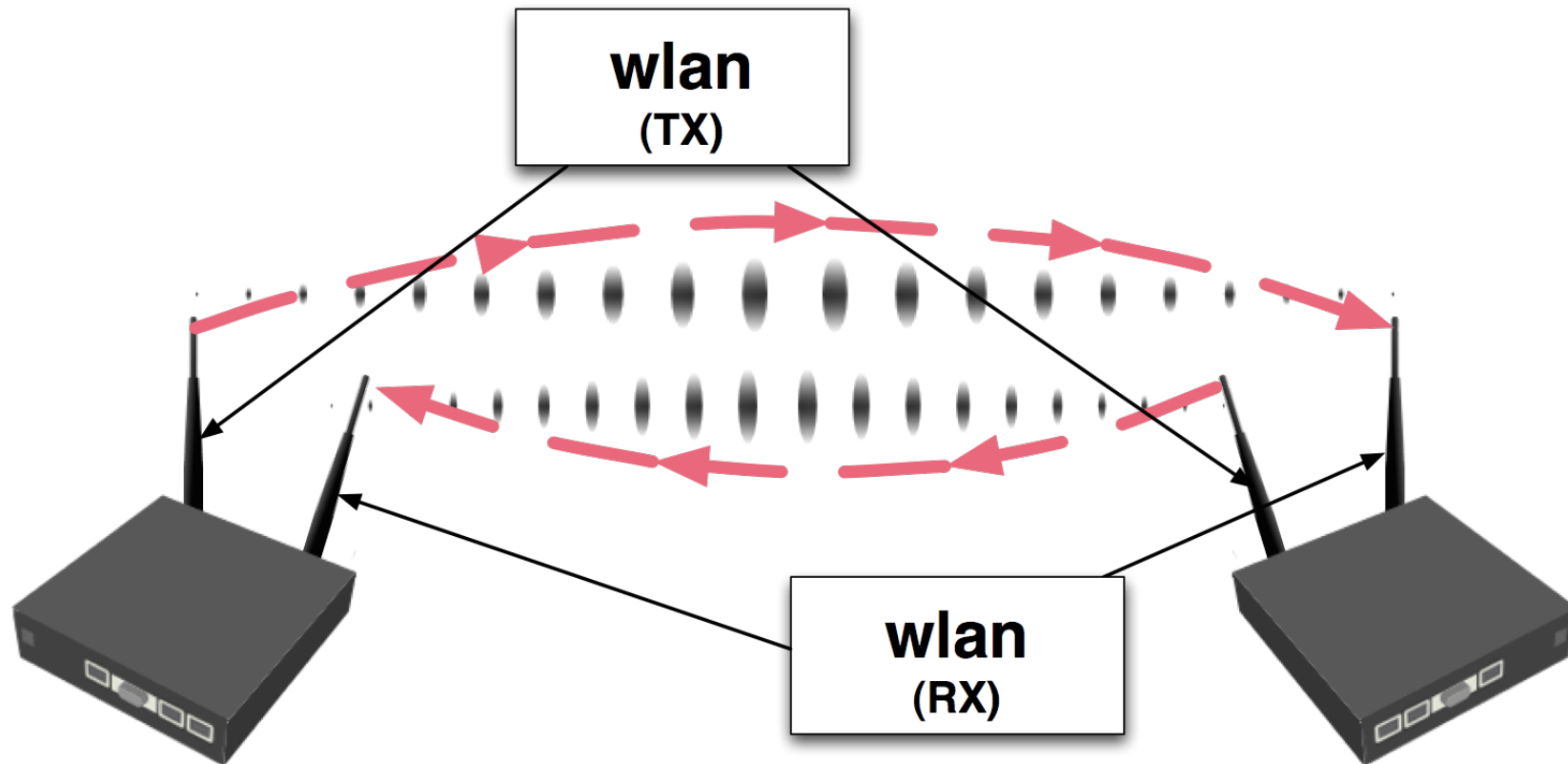
Nstreme Protocol: Frames

- ◆ framer-limit - maximal frame size
- ◆ framer-policy - the method how to combine frames.
There are several methods of framing:
 - ➔ none - do not combine packets
 - ➔ best-fit - put as much packets as possible in one frame, until the limit is met, but do not fragment packets
 - ➔ exact-size - same as best-fit, but with the last packet fragmentation
 - ➔ dynamic-size - choose the best frame size dynamically

Nstreme Lab

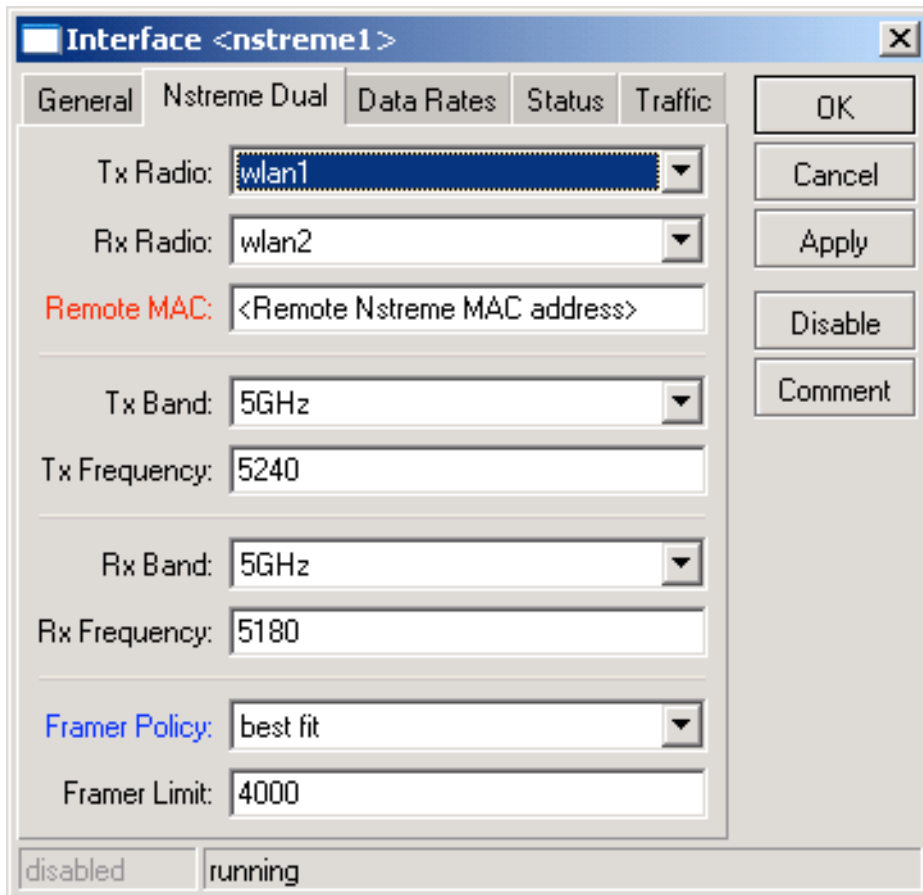
- **Restore configuration backup file**
- Route your private network together with your neighbor's network
- Enable N-streme and check link productivity with different framer polices

Nstreme Dual Protocol



- MikroTik proprietary (i.e., incompatible with other vendors) wireless protocol that works with a pair of wireless cards (Atheros chipset cards only) – one transmitting, one receiving

Nstreme Dual Interface



- Set both wireless cards into “nstreme_dual_slave” mode
- Create Nstreme dual interface (press “plus” button in wireless interface window)
- Use framer policy only if necessary

VPN

Virtual Private Networks

EoIP
PPTP, L2TP
PPPoE

VPN Benefits

- Enable communications between corporate private LANs over
 - ◆ Public networks
 - ◆ Leased lines
 - ◆ Wireless links
- Corporate resources (e-mail, servers, printers) can be accessed securely by users having granted access rights from outside (home, while travelling, etc.)

EoIP

Ethernet over IP

EOIP (Ethernet Over IP) tunnel

- MikroTik proprietary protocol.
- Simple in configuration
- Don't have authentication or data encryption capabilities
- Encapsulates Ethernet frames into IP protocol 47/gre packets, thus EOIP is capable to carry MAC-addresses
- EOIP is a tunnel with bridge capabilities

Creating EoIP Tunnel

The screenshot shows the RouterOS WinBox interface. The left sidebar contains a menu with the following items: Interfaces, Wireless, PPP, Bridge, IP, Routing, Ports, Queues, Drivers, System, Files, Log, SNMP, Users, Radius, Tools, New Terminal, Telnet, Password, Certificate, Make Supout.rif, Manual, and Exit. The 'Interfaces' menu item is highlighted with a red circle. A red arrow points from this circle to a '+' icon in the 'Interface List' window. Another red circle highlights the '+' icon, and a red arrow points from it to the 'EoIP Tunnel' option in a dropdown menu. The 'Interface List' window contains a table with columns: Type, MTU, Tx Rate, Rx Rate, Tx Pac..., and Rx Pac... The table lists several Ethernet interfaces with MTU 1500 and 0 bps for Tx and Rx rates. A 'New Interface' dialog box is open, showing the configuration for a new EoIP tunnel. The dialog has two tabs: 'General' and 'Traffic'. The 'General' tab is active, showing the following fields: Name: eoip-tunnel1, Type: EoIP, MTU: 1500, MAC Address: FE:7A:59:E5:D2:BF (highlighted with a red circle), ARP: enabled, Remote Address: 10.1.1.XZ (highlighted with a red circle), and Tunnel ID: 23 (highlighted with a red circle). The 'Traffic' tab is currently disabled. The dialog also features buttons for OK, Cancel, Apply, Disable, Comment, Copy, and Remove.

Type	MTU	Tx Rate	Rx Rate	Tx Pac...	Rx Pac...
Ethernet	1500	0 bps	0 bps	0	0
Ethernet	1500	0 bps	0 bps	0	0
Ethernet	1500	0 bps	0 bps	0	0
Ethernet	1500	0 bps	0 bps	0	0
Ethernet	1500	0 bps	0 bps	0	0
Ethernet	1500	0 bps	0 bps	0	0
Ethernet	1500	0 bps	0 bps	0	0
Ethernet	1500	0 bps	0 bps	0	0
Ethernet	1500	0 bps	0 bps	0	0
Wireless	1500	0 bps	0 bps	0	0
Wireless	1500	0 bps	0 bps	0	0

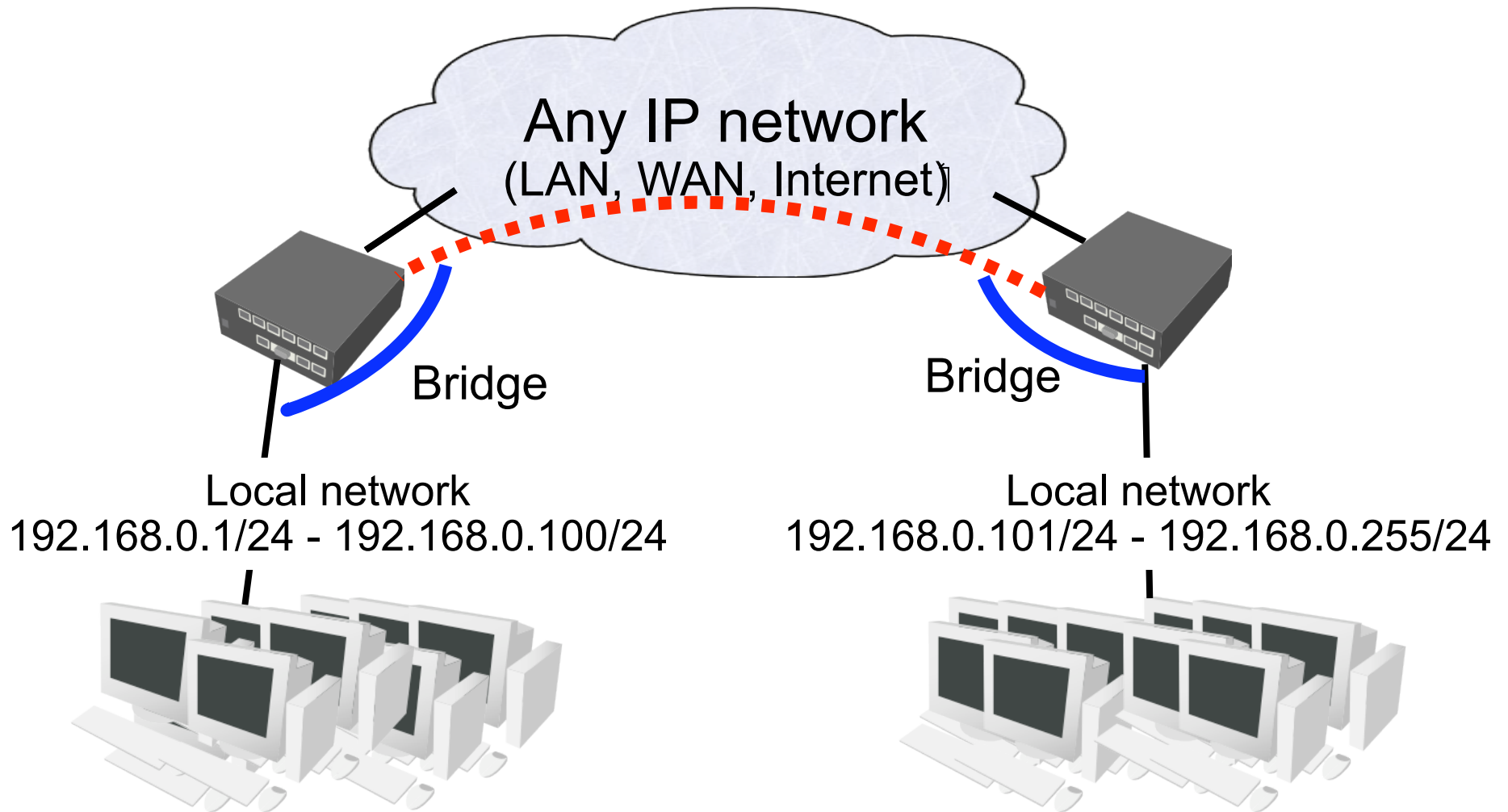
Creating EoIP Tunnel

- Check that you are able to ping remote address before creating a tunnel to it
- Make sure that your EoIP tunnel will have unique MAC-address (it should be from EF:xx:xx:xx:xx:xx range)
- Tunnel ID on both ends of the EoIP tunnel must be the same – it helps to separate one tunnel from other

EoIP and Bridging

- EoIP Interface can be bridged with any other EoIP or Ethernet-like interface.
- Main use of EoIP tunnels is to transparently bridge remote networks.
- EoIP protocol does not provide data encryption, therefore it should be run over encrypted tunnel interface, e.g., PPTP or PPPoE, if high security is required.

EOIP and Bridging



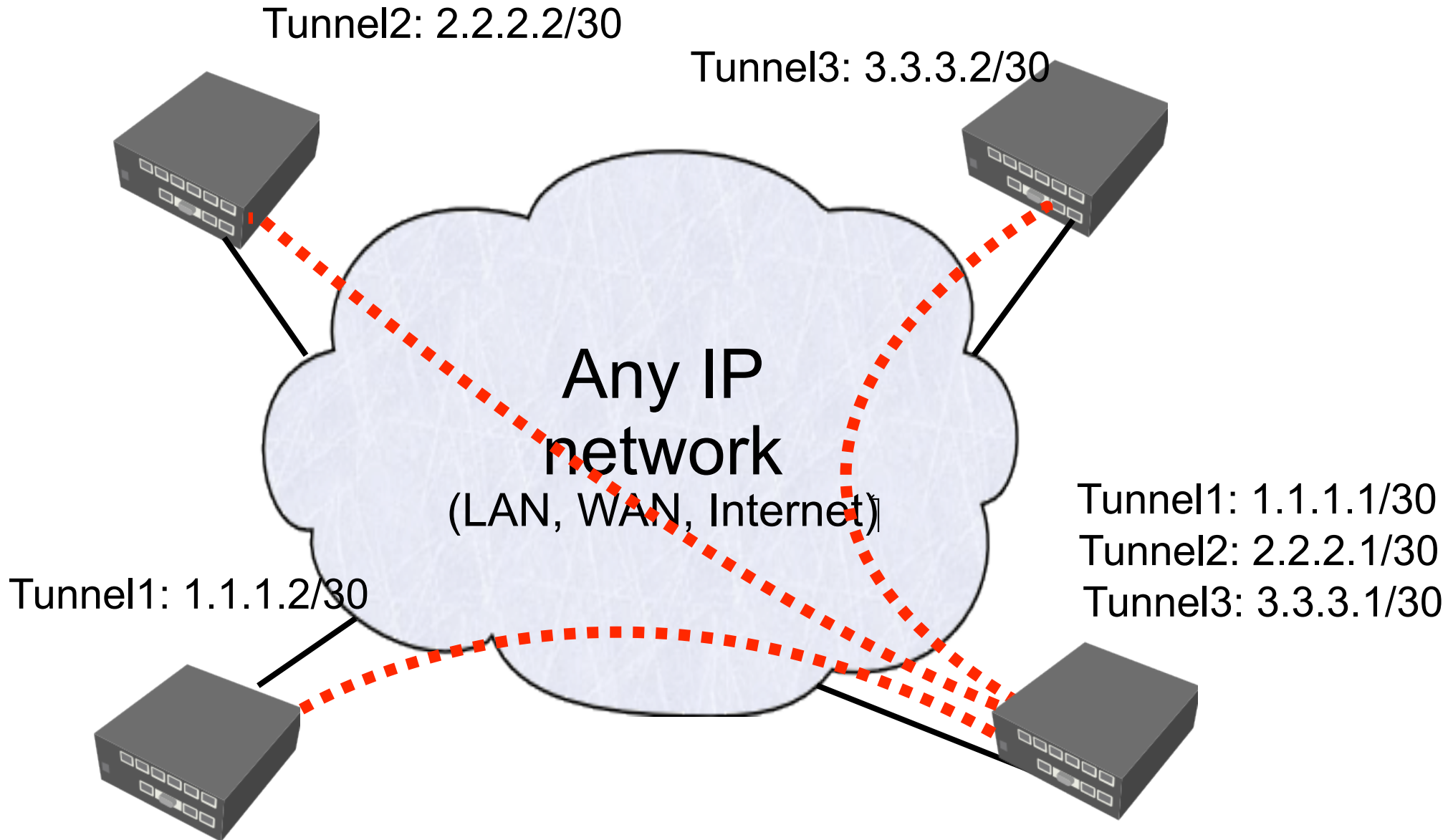
EoIP Lab

- **Restore default system backup**
- Create EoIP tunnel with your neighbor(s)
- Transfer to /22 private networks – this way you will be in the same network with your neighbor, and local addresses will remain the same
- Bridge your private networks via EoIP

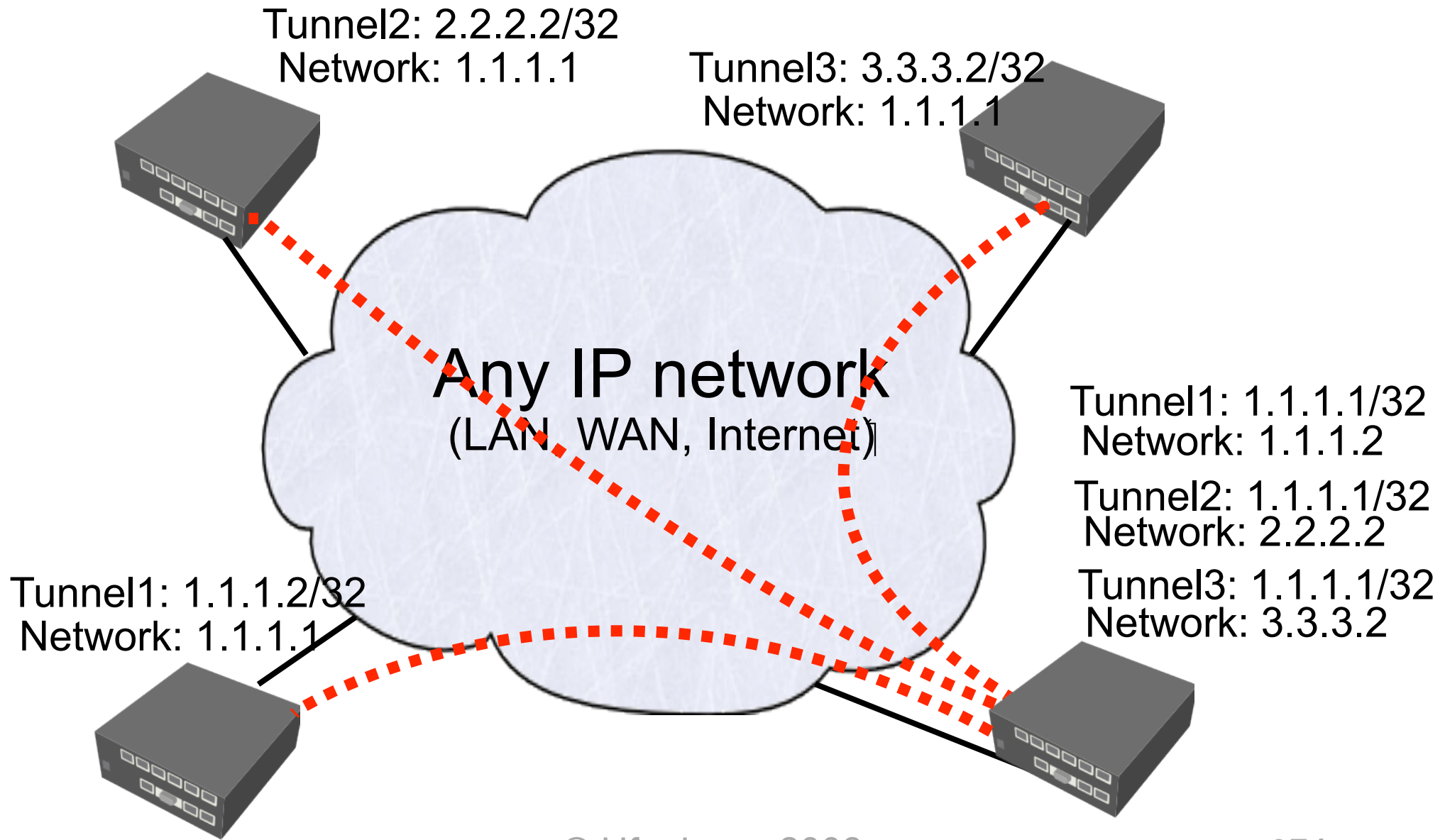
/32 IP Addresses

- IP addresses are added to the tunnel interfaces
- Use /30 network to save address space, for example:
 - ◆ 10.1.6.1/30 and 10.1.6.2/30 from network 10.1.6.0/30
- It is possible to use point to point addressing, for example:
 - ◆ 10.1.6.1/32, network 10.1.7.1
 - ◆ 10.1.7.1/32, network 10.1.6.1

EoIP and /30 Routing



EoIP and /32 Routing



Local User Database

PPP Profile, PPP Secret

Point-to-Point protocol tunnels

- A little bit sophisticated in configuration
- Capable of authentication and data encryption
- Such tunnels are:
 - ◆ PPPoE (Point-to-Point Protocol over Ethernet)
 - ◆ PPTP (Point-to-Point Tunneling Protocol)
 - ◆ L2TP (Layer 2 Tunneling Protocol)
- You should create user information before creating any tunnels

PPP Secret

- PPP secret (aka local PPP user database) stores PPP user access records
- Make notice that user passwords are displayed in the plain text – anyone who has access to the router are able to see all passwords
- It is possible to assign specific /32 address to both ends of the PPTP tunnel for this user
- Settings in **/ppp secret** user database override corresponding **/ppp profile** settings

PPP Secret

The screenshot shows the RouterOS WinBox interface. The left sidebar has 'PPP' selected. The main window shows the 'Secrets' tab with a table of secrets. A dialog box titled 'PPP Secret <admin3>' is open, showing the configuration for the 'admin3' secret.

Name	Password	Service
admin	admin	any
admin2	admin2	any
admin3	admin3	any

PPP Secret <admin3> configuration:

- Name: admin3
- Password: admin3
- Service: any
- Caller ID:
- Profile: default
- Local Address: 1.1.1.1
- Remote Address: 2.2.2.4
- Routes:
- Limit Bytes In:
- Limit Bytes Out:

PPP Profile and IP Pools

- PPP profiles define default values for user access records stored under **/ppp secret** submenu
- PPP profiles are used for more than 1 user so there must be more than 1 IP address to give out - we should use IP pool as “Remote address” value
- Value “default” means – if option is coming from RADIUS server it won't be overridden

PPP Profile

The screenshot displays the RouterOS WinBox interface. On the left, the 'RouterOS WinBox' menu is visible, with 'PPP' highlighted. The main window shows the 'PPP' configuration page, with the 'Profiles' tab selected. A table lists existing profiles:

Name	Local Address	Remote Address
* default		
* default-encr...		

The 'New PPP Profile' dialog is open, showing the following configuration:

- Name: profile1
- Local Address: 192.168.0.1
- Remote Address: dhcp_pool1
- Bridge: (empty)
- Incoming Filter: (empty)
- Outgoing Filter: (empty)
- DNS Server: 10.1.1.254
- WINS Server: (empty)
- Use Compression: default no yes
- Use VJ Compression: default no yes
- Use Encryption: default no yes required
- Change TCP MSS: default no yes

Change TCP MSS

- Big 1500 byte packets have problems going through the tunnels because:
 - ◆ Standard Ethernet MTU is 1500 bytes
 - ◆ PPTP and L2TP tunnel MTU is 1460 bytes
 - ◆ PPPOE tunnel MTU is 1488 bytes
- By enabling “change TCP MSS option, dynamic mangle rule will be created for each active user to ensure right size of TCP packets, so they will be able to go through the tunnel

PPTP and L2TP

Point-to-Point Tunnelling Protocol and
Layer 2 Tunnelling Protocol

PPTP Tunnels

- PPTP uses TCP port 1723 and IP protocol 47/
GRE
- There is a PPTP-server and PPTP-clients
- PPTP clients are available for and/or included
in almost all OS
- You must use PPTP and GRE “NAT helpers” to
connect to any public PPTP server from your
private masqueraded network

L2TP Tunnels

- PPTP and L2TP have mostly the same functionality
- L2TP traffic uses UDP port 1701 only for link establishment, further traffic is using any available UDP port
- L2TP don't have problems with NATed clients – it don't required “NAT helpers”
- Configuration of the both tunnels are identical in RouterOS

Creating PPTP/L2TP Client

The screenshot shows the RouterOS WinBox interface. The 'Interfaces' menu is open, and the 'New Interface' dialog is displayed. The 'PPTP Client' option is selected in the menu, and the 'New Interface' dialog is open to the 'General' tab. The configuration fields are as follows:

- Server Address: 10.1.1.254
- User: admin1
- Password: admin1
- Profile: default
- Add Default Route

The 'Dial Out' tab is also visible, showing options for authentication:

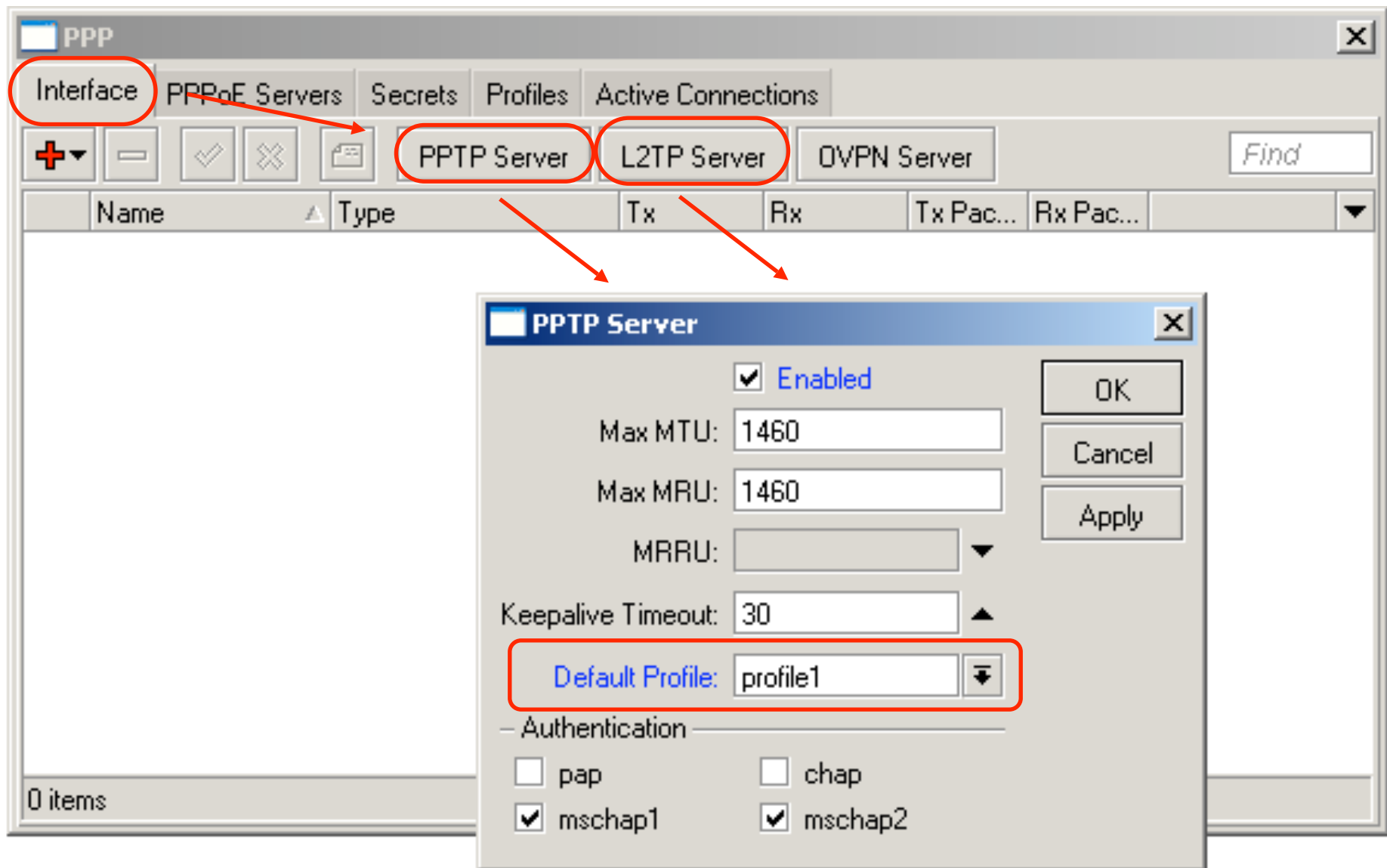
- pap
- mschap1
- chap
- mschap2

The 'Status' tab shows the interface is currently 'disabled'.

PPTP Client Lab

- **Restore system backup (slide 12)**
- **Create PPTP client**
 - ◆ Server Address: 10.1.2.1
 - ◆ User: admin
 - ◆ Password: admin
 - ◆ Add default route = yes
- **Make necessary adjustments to access the internet**

Creating PPTP/L2TP server



PPTP Server Lab

- Create a PPTP server
- Create one user in PPP Secret
- Configure your laptop to connect to your PPTP server
- Make necessary adjustments to access the Internet via the tunnel
- Create PPP Profile for the router to use encryption
- Configure PPTP-client on the laptop accordingly

Optional: Advanced VPN Lab

- **Restore system backup (slide 12)**
- Create secure L2TP tunnel with your neighbor
- Create EoIP tunnel over the L2TP tunnel
- Bridge your networks together!

User Access Control

- Controlling the Hardware

- ◆ Static IP and ARP entries
- ◆ DHCP for assigning IP addresses and managing ARP entries

- Controlling the Users

- ◆ PPPoE requires PPPoE client configuration
- ◆ HotSpot redirects client request to the sign-up page
- ◆ PPTP requires PPTP client configuration

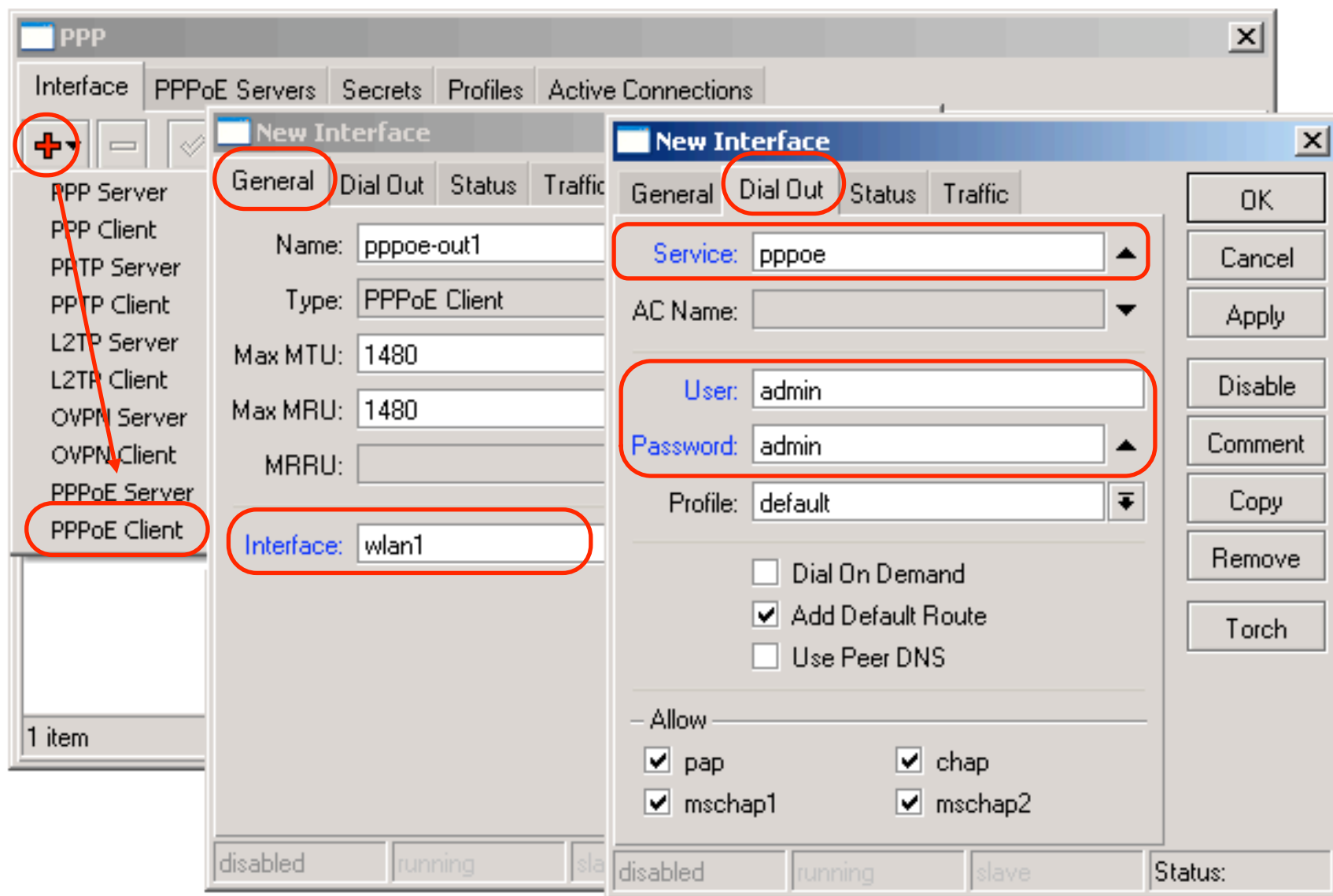
PPPoE

Point-to-Point Protocol over Ethernet

PPPoE tunnels

- PPPoE works in OSI 2nd (data link) layer
- PPPoE is used to hand out IP addresses to clients based on the user authentication
- PPPoE requires a dedicated access concentrator (server), which PPPoE clients connect to.
- Most operating systems have PPPoE client software. Windows XP has PPPoE client installed by default

PPPoE client



PPPoE Client Lab

- **Restore default system backup**
- **Create PPTP client**
 - ◆ Interface: wlan1
 - ◆ Service:pppoe
 - ◆ User: admin
 - ◆ Password: admin
 - ◆ Add default route = yes
- **Make necessary adjustments to access the internet**

PPPoE Client Status

- Check your PPPoE connection
 - ◆ Is the interface enabled?
 - ◆ Is it “connected” and running (R)?
 - ◆ Is there a dynamic (D) IP address assigned to the pppoe client interface in the IP Address list?
 - ◆ What are the netmask and the network address?
 - ◆ What routes do you have on the pppoe client interface?
- See the “Log” for troubleshooting!

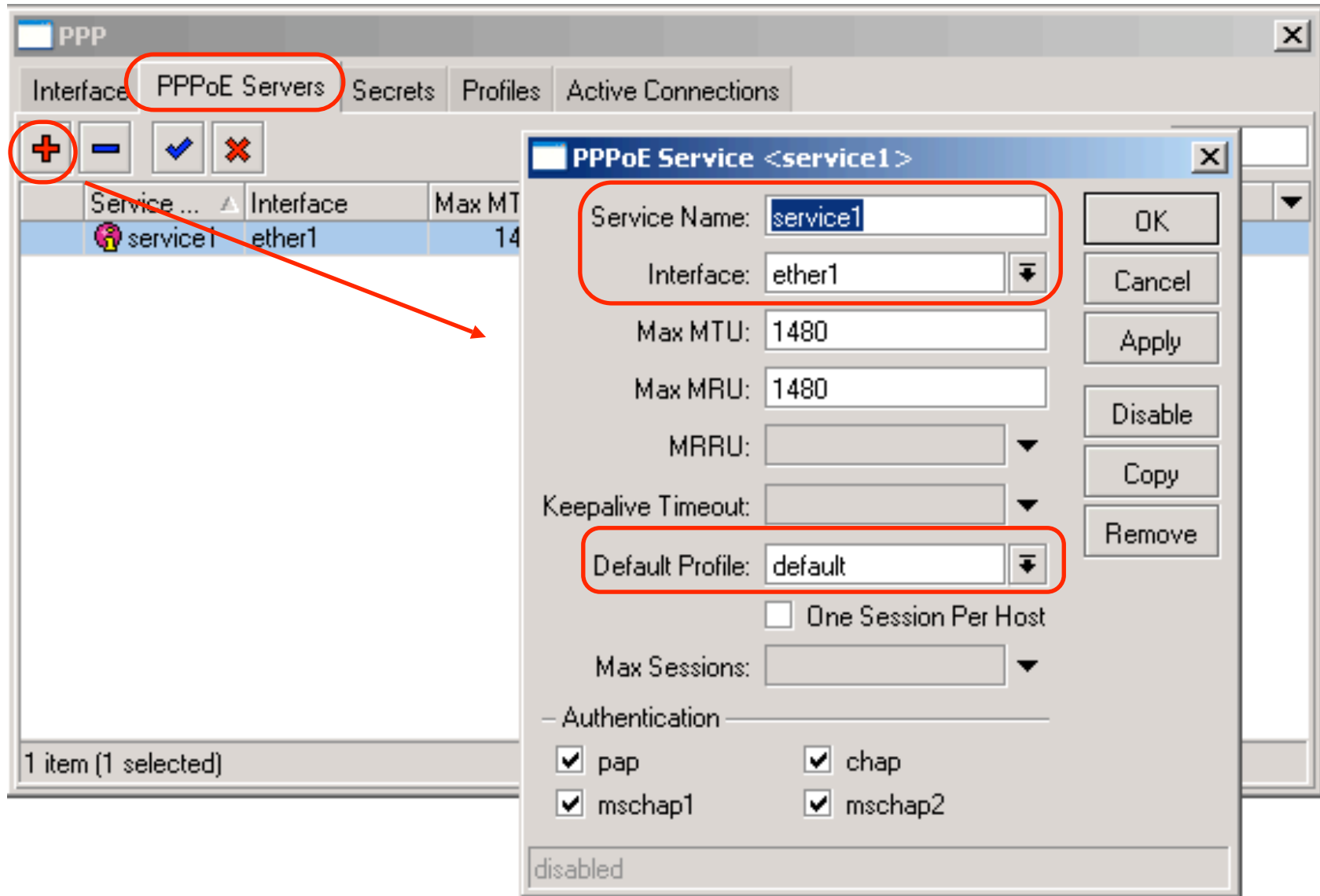
* PPPoE Lab with Encryption *

- The PPPoE access concentrator is changed to use encryption now
- You should use encryption, either
 - ◆ change the ppp profile used for the pppoe client to 'default-encryption', or,
 - ◆ modify the ppp profile used for the pppoe client to use encryption
- See if you get the pppoe connection running

PPPoE Server

- PPPoE server accepts PPPoE client connections on a given interface
- Clients can be authenticated against
 - ◆ the local user database (ppp secrets)
 - ◆ a remote RADIUS server
 - ◆ a remote or a local MikroTik User Manager database
- Clients can have automatic data rate limitation according to their profile

Creating PPPoE server (service)



PPPoE Server Lab

- Create a PPPoE server
- Create one user in PPP Secret
- Configure your laptop to connect to your PPPoE server
- Make necessary adjustments to access the internet via the tunnel
- Create PPP Profile for the router to use encryption
- Configure PPPoE-client on the laptop accordingly

PPP interface Bridging

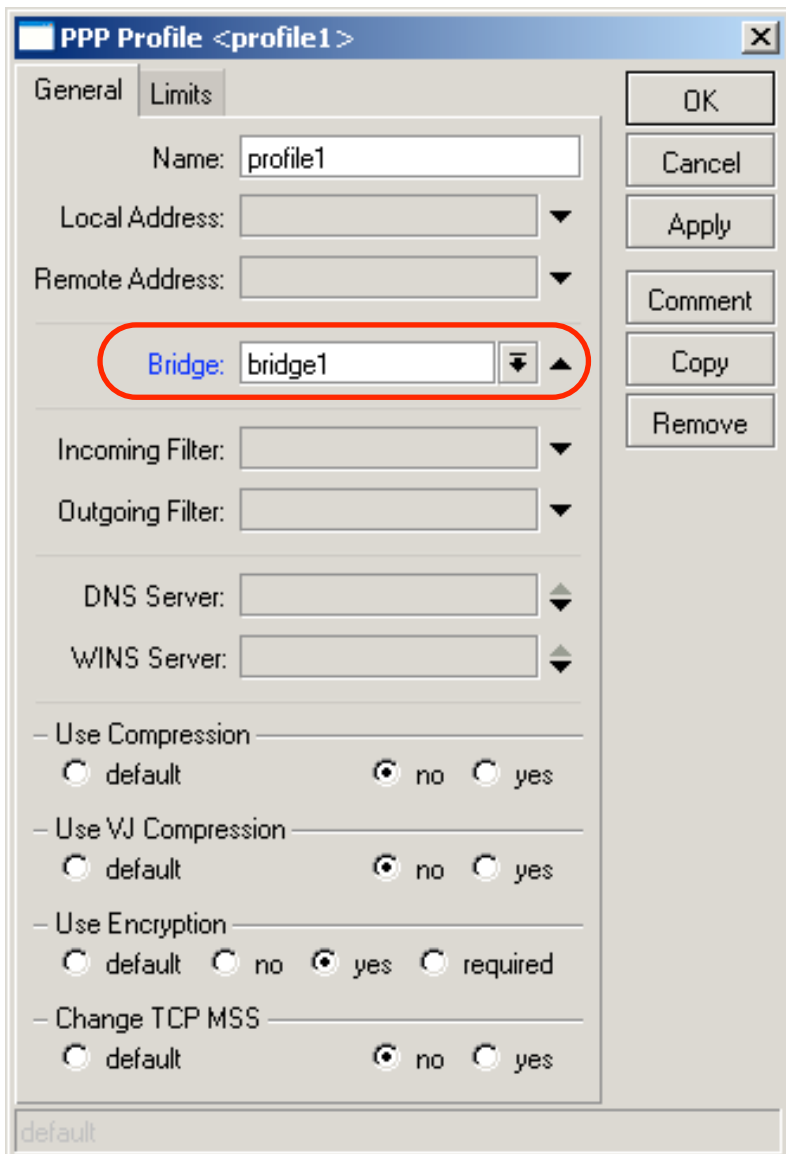
PPP BCP (Bridge Control Protocol)

PPP MP (Multi-link Protocol)

PPP Bridge Control Protocol

- RouterOS now have BCP support for all async. PPP, PPTP, L2TP & PPPoE (not ISDN) interfaces
- If BCP is established, PPP tunnel does not require IP address
- Bridged Tunnel IP address (if present) does not apply to whole bridge – it stays only on PPP interface (routed IP packets can go through the tunnel as usual)

Setting up BCP



- You must specify bridge option in the ppp profiles on **both** ends of the tunnel.
- The bridge **must** have manually set MAC address, or at least one regular interface in it, because ppp interfaces do not have MAC addresses.

PPP Bridging Problem

- PPP interface MTU is smaller than standard Ethernet interface
- It is impossible to fragment Ethernet frames – tunnels must have inner algorithm how to encapsulate and transfer Ethernet frames via link with smaller MTU
- EOIP have encapsulation algorithm enabled by default, PPP interfaces doesn't
- PPP interfaces can utilize PPP Multi-link Protocol to encapsulate Ethernet frames

PPP Multi-link Protocol

- PPP Multi-link Protocol allows to open multiple simultaneous channels between systems
- It is possible to split and recombine packets, between several channels – resulting in increase the effective maximum receive unit (MRU)
- To enable PPP Multi-link Protocol you must specify MRU option
- In MS Windows you must enable "Negotiate multi-link for single link connections" option

PPP Multi-link Protocol

The image displays three overlapping configuration windows from Mikrotik WinBox:

- PPPoE Service <service1>**: Shows Service Name: service1, Interface: ether1, Max MTU: 1480, Max MRU: 1480, and MRRU: 65535 (circled in red).
- Interface <pppoe-out1>**: Shows Name: pppoe-out1, Type: PPPoE Client, Max MTU: 1480, Max MRU: 1480, and MRRU: 65535 (circled in red). The interface is ether1.
- mikrotik Properties**: Shows the Networking tab selected. The Type of VPN is set to Automatic. The Settings button is circled in red. The PPP Settings sub-window is open, showing:
 - Enable LCP extensions
 - Enable software compression
 - Negotiate multi-link for single link connections (circled in red)

PPP Bridging Lab

- **Restore default system backup**
- Create PPP tunnel with your neighbor(s)
- Bridge PPP tunnels with your local interface
- Ensure that MTU and MRU of the PPP link is at least 1500 byte
- Check the configuration using ping tool with different packet size
- **BTW – using PPP MP (even without bridging) it is possible to avoid MSS changes and all MSS related problems**

HotSpot

Plug-and-Play Access

HotSpot

- HotSpot is used for authentication in local network
- Authentication is based on HTTP/HTTPS protocol meaning it can work with any Internet browser
- HotSpot is a system combining together various independent features of RouterOS to provide the so called 'Plug-and-Play' access

How does it work?

- User tries to open a web page
- Router checks if the user is already authenticated in the HotSpot system
- If not, user is redirected to the HotSpot login page
- User specifies the login information

Please log on to use the mikrotik hotspot service



A screenshot of a web-based login form for Mikrotik HotSpot. The form is enclosed in a rectangular border. At the top, it says "Please log on to use the mikrotik hotspot service". Below this, there are two input fields: "login" with the text "anyuser" and "password" with a series of asterisks. Below the password field is an "OK" button. At the bottom of the form is the Mikrotik logo in red.

Powered by mikrotik routers © 2005 mikrotik

How does it work?

- If the login information is correct, then the router
 - ◆ authenticates the client in the Hotspot system;
 - ◆ opens the requested web page;
 - ◆ opens a status pop-up window
- The user can access the network through the HotSpot gateway

Welcome anyuser!

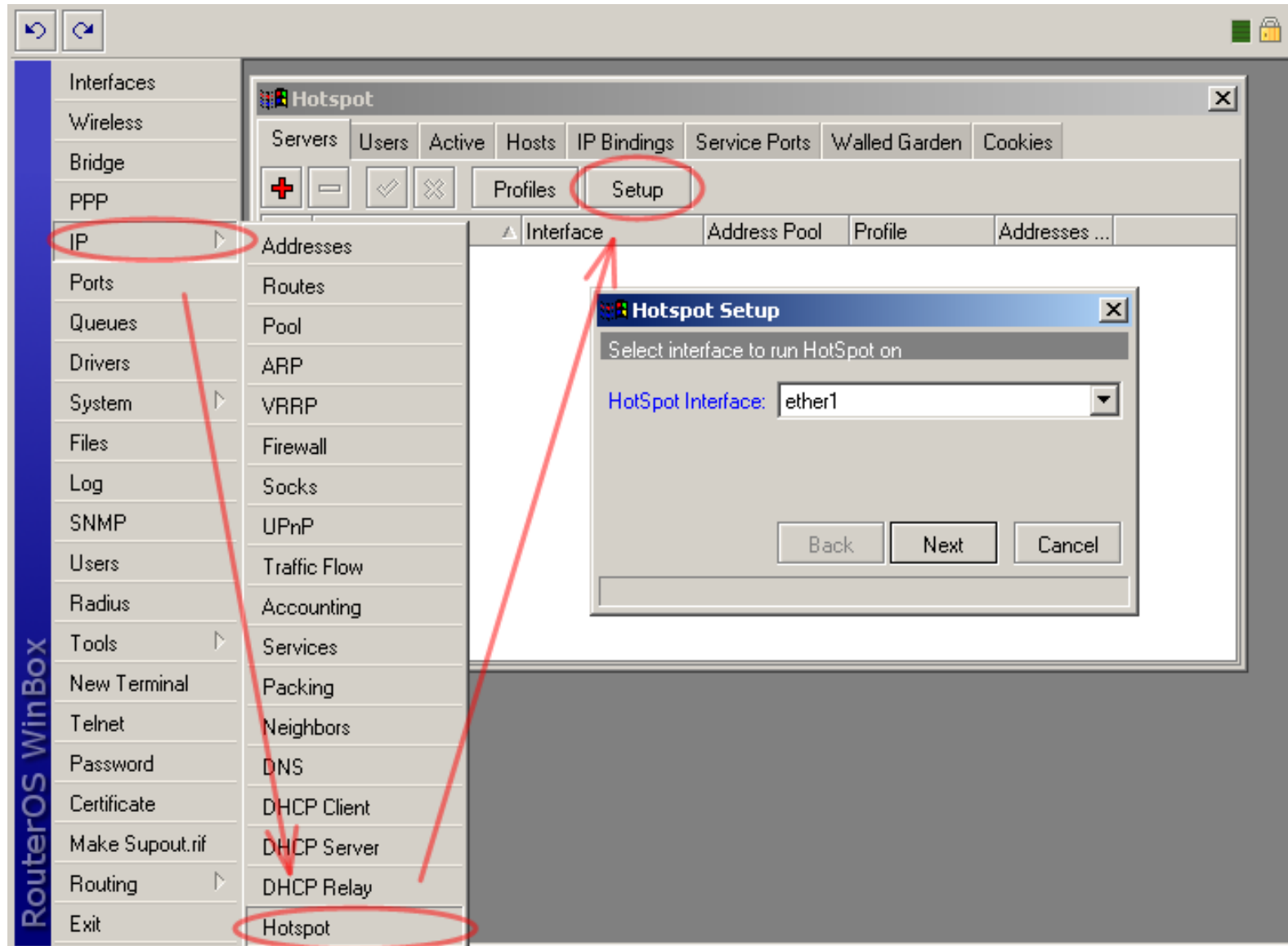
IP address:	10.1.100.1
bytes up/down:	23.1 KiB / 43.5 KiB
connected:	40s
status refresh:	1m

log off

HotSpot Features

- User authentication
- User accounting by time, data transmitted/received
- Data limitation
 - ◆ by data rate
 - ◆ by amount
- Usage restrictions by time
- RADIUS support
- Walled garden

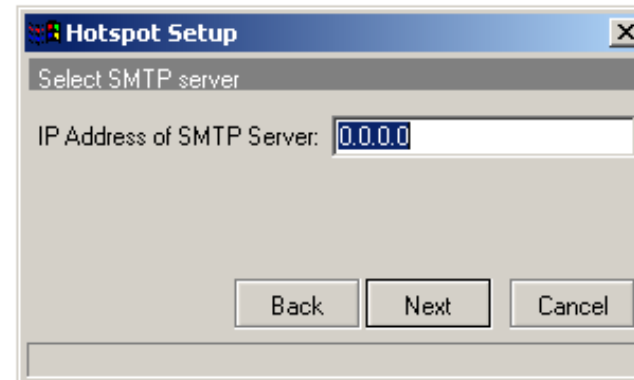
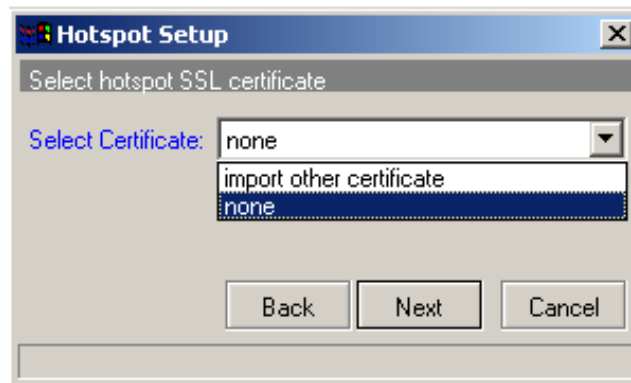
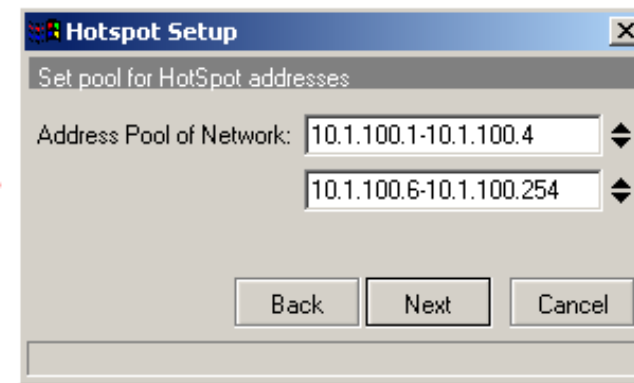
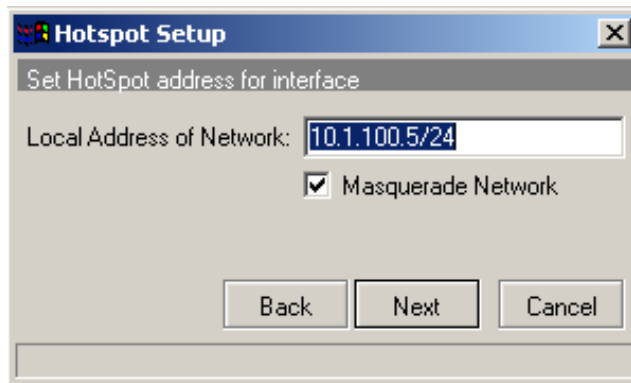
HotSpot Setup Wizard (Step 1)



HotSpot Setup Wizard

- Start the HotSpot setup wizard and select interface to run the HotSpot on
- Set address on the HotSpot interface
- Choose whether to masquerade hotspot network or not
- Select address pool for the HotSpot
- Select HotSpot SSL certificate if HTTPS is required

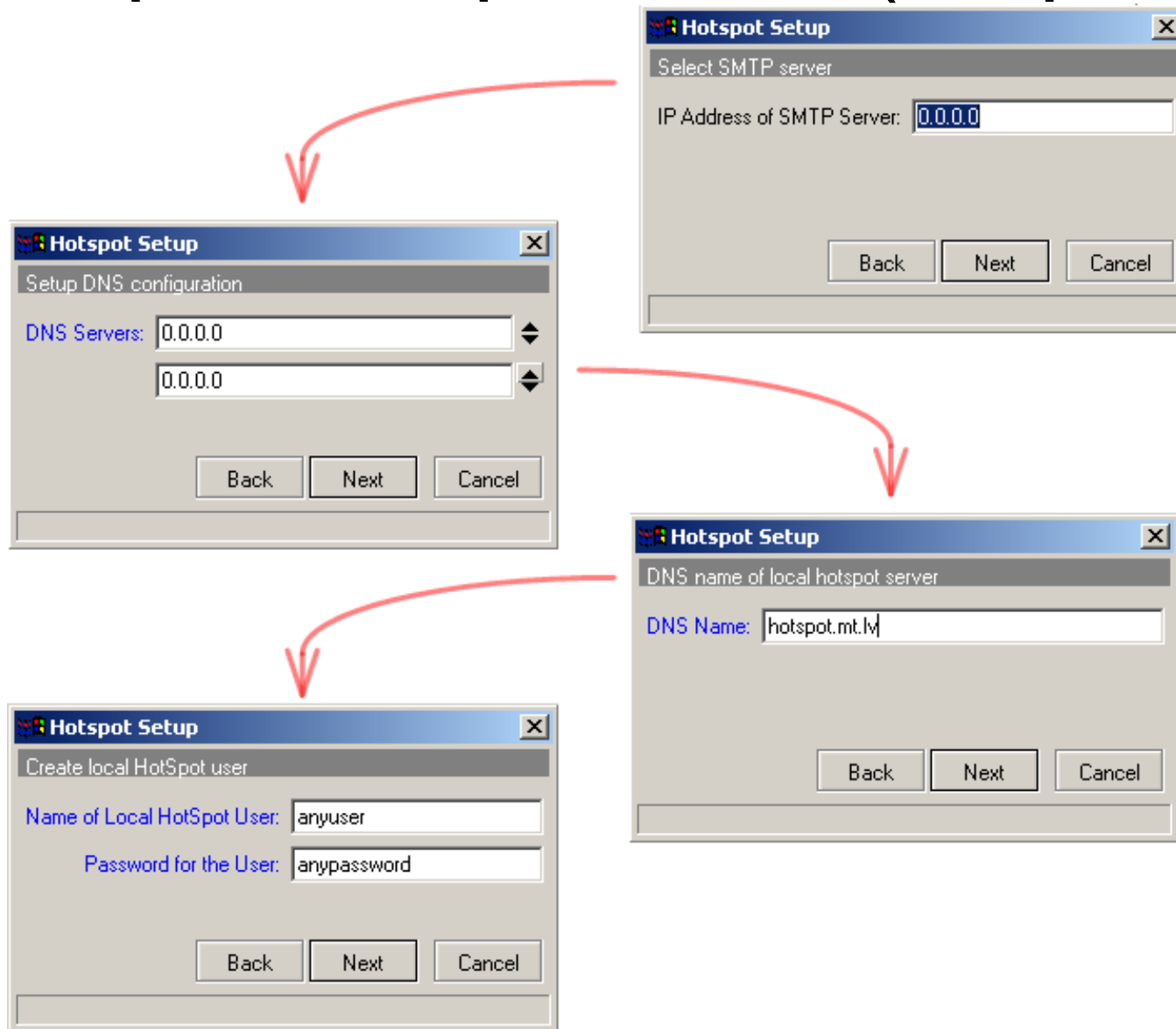
HotSpot Setup Wizard (Step 2-5)



HotSpot Setup Wizard

- Select SMTP server to automatically redirect outgoing mails to local SMTP server, so the clients need not to change their outgoing mail settings
- Specify DNS servers to be used by the router and HotSpot users
- Set DNS name of the local HotSpot server
- Finally the wizard allows to create one HotSpot user

HotSpot Setup Wizard (Step 5-8)



HotSpot Setup Wizard Lab

- Create simple Hotspot server for your private network using HotSpot Setup Wizard
- Login and check the setup!
- Logout
- Type any random IP, netmask, gateway, DNS values on your Laptop network configuration
- Login and check the setup!

HotSpot Server Setup Wizard

- The preferred way to configure HotSpot server
- Automatically creates configuration entries in
 - ◆ /ip hotspot
 - ◆ /ip hotspot profile
 - ◆ /ip hotspot users
 - ◆ /ip pool
 - ◆ /ip dhcp-server
 - ◆ /ip dhcp-server networks
 - ◆ /ip firewall nat (dynamic rules)
 - ◆ /ip firewall filter (dynamic rules)

HotSpot Servers

The screenshot shows the RouterOS WinBox interface. The left sidebar contains a menu with 'Hotspot' circled in red. The main window displays the 'Hotspot' configuration page, with the 'Servers' tab selected and also circled in red. A '+' icon in the toolbar is circled in red, with a red arrow pointing to the 'Hotspot Server <hs-ether1>' dialog box. The dialog box contains the following fields:

- Name: hs-ether1
- Interface: ether1
- Address Pool: hs-pool-1
- Profile: hsprof1
- Idle Timeout: 00:05:00
- Keepalive Timeout:
- Addresses Per MAC: 2
- IP of DNS Name: 0.0.0.0

Buttons on the right side of the dialog include OK, Cancel, Apply, Disable, Copy, Remove, and Reset HTML.

HotSpot Servers Profiles

- HotSpot server profiles are used for common server settings. Think of profiles as of server groups
- You can choose 6 different authentication methods in profile settings

HotSpot Server Profiles

The screenshot displays the Mikrotik WinBox interface for configuring Hotspot Server Profiles. The main window has tabs for Servers, Users, Active, Hosts, IP Bindings, Service Ports, Walled Garden, and Cookies. Below these are buttons for adding (+), removing (-), checking (✓), unchecking (✗), Profiles, and Setup. A table lists existing profiles:

Name	DNS Name	HTML Directory	Rate Limit
default		hotspot	
hsprof1		hotspot	

Two 'New Hotspot Server Profile' dialog boxes are shown. The left one is on the 'General' tab, and the right one is on the 'Login' tab. Red circles highlight the 'Profiles' button in the main window, the '+' button in the profile list, the 'General' tab in the left dialog, and the 'Login' tab in the right dialog. Red arrows indicate the flow from the main window to the dialog and from the list to the dialog.

General Tab (Left Dialog):

- Name: hsprof2
- Hotspot Address:
- DNS Name:
- HTML Directory: hotspot
- Rate Limit (rx/tx):
- HTTP Proxy:
- HTTP Proxy Port:
- SMTP Server:

Login Tab (Right Dialog):

- Login By:
 - MAC
 - Cookie
 - HTTP CHAP
 - HTTPS
 - HTTP PAP
 - Trial
- HTTP Cookie Lifetime: 3d 00:00:00
- SSL Certificate: none
- Split User Domain
- Trial Uptime Limit: 00:30:00
- Trial Uptime Reset: 1d 00:00:00
- Trial User Profile: default

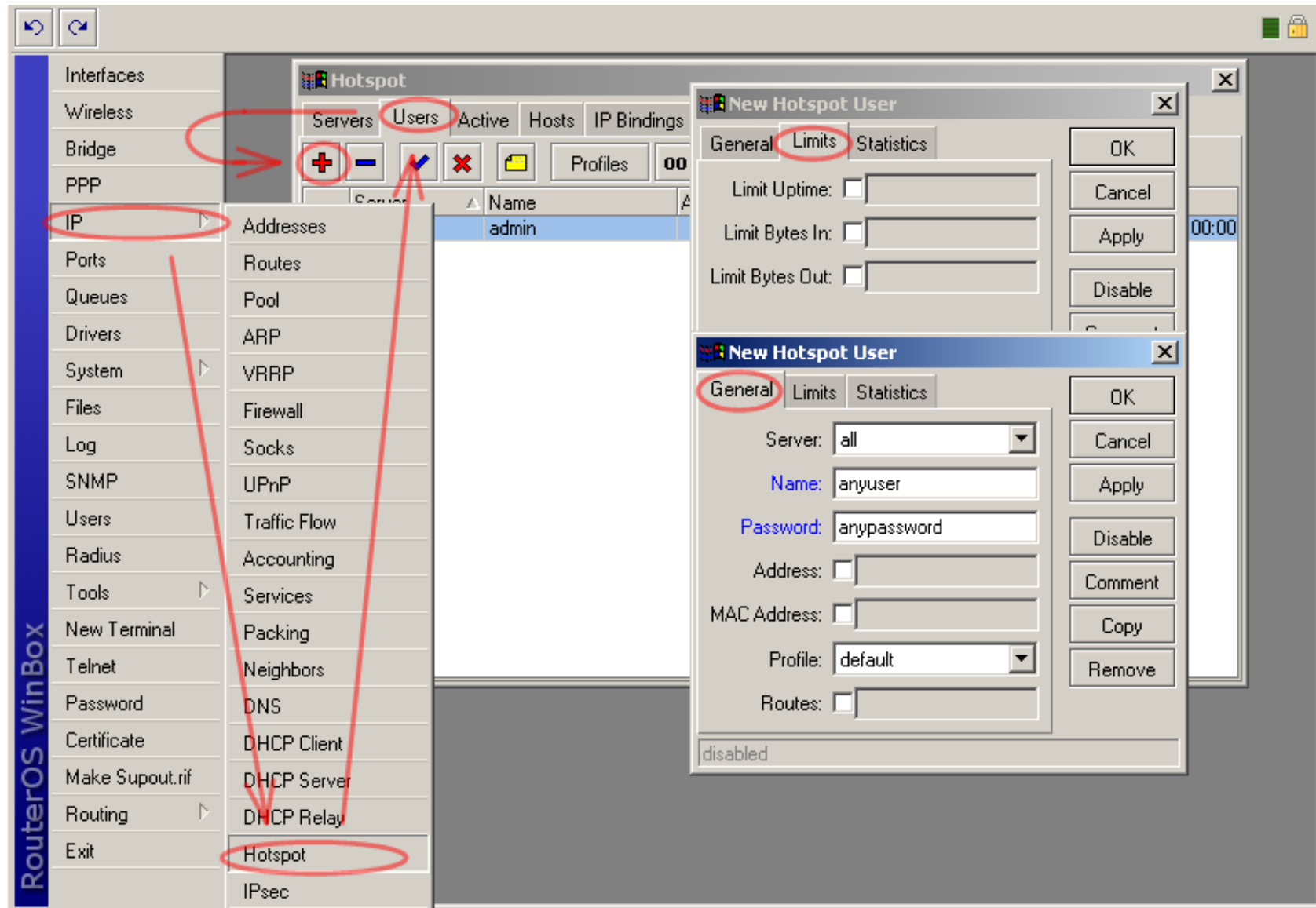
HotSpot Authentication Methods

- ◆ HTTP PAP - simplest method, which shows the HotSpot login page and expects to get the user credentials in plain text (maximum compatibility mode)
- ◆ HTTP CHAP - standard method, which includes CHAP computing for the string which will be sent to the HotSpot gateway.
- ◆ HTTPS – plain text authentication using SSL protocol to protect the session

HotSpot Authentication Methods

- ◆ HTTP cookie - after each successful login, a cookie is sent to the web browser and the same cookie is added to active HTTP cookie list. This method may only be used together with HTTP PAP, HTTP CHAP or HTTPS methods
- ◆ MAC address - authenticates clients as soon as they appear in the hosts list, using client's MAC address as user name
- ◆ Trial - does not require authentication for a certain amount of time

HotSpot Users



HotSpot Users

- Bind username, password and profile for a particular client
- Limit a user by uptime, bytes-in and bytes-out
- Assign an IP address for the client
- Permit user connections only from particular MAC address

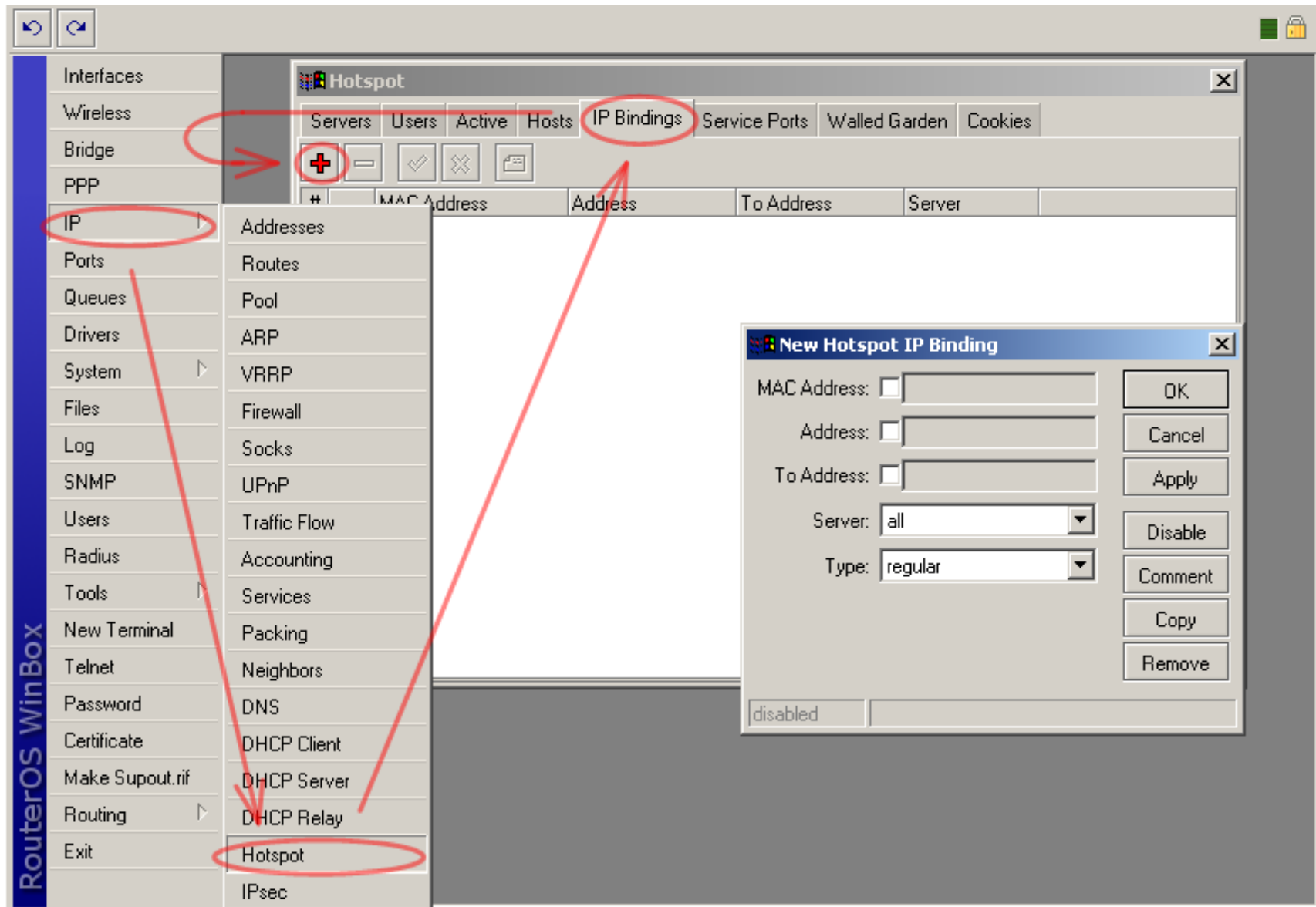
HotSpot User Profiles

The screenshot displays the RouterOS WinBox interface. The left sidebar shows the 'Hotspot' menu item circled in red. A red arrow points from this menu item to the 'New Hotspot User Profile' dialog box. The dialog box is open, showing the 'General' tab. The 'Name' field is set to 'uprof1', the 'Address Pool' is 'hs-pool-1', the 'Session Timeout' is unchecked, the 'Idle Timeout' is set to 'none', the 'Keepalive Timeout' is '00:02:00', the 'Status Autorefresh' is '00:01:00', 'Shared Users' is '1', and 'Rate Limit' is unchecked. The 'Incoming Filter' and 'Outgoing Filter' are both empty. The 'Incoming Packet Mark' and 'Outgoing Packet Mark' are also empty. The 'Open Status Page' is set to 'always'. The 'Transparent Proxy' checkbox is unchecked. The 'OK', 'Cancel', 'Apply', 'Copy', and 'Remove' buttons are visible on the right side of the dialog box.

HotSpot User Profiles

- Store settings common to groups of users
- Allow to choose firewall filter chains for incoming and outgoing traffic check
- Allow to set a packet mark on traffic of every user of this profile
- Allow to rate limit users of the profile

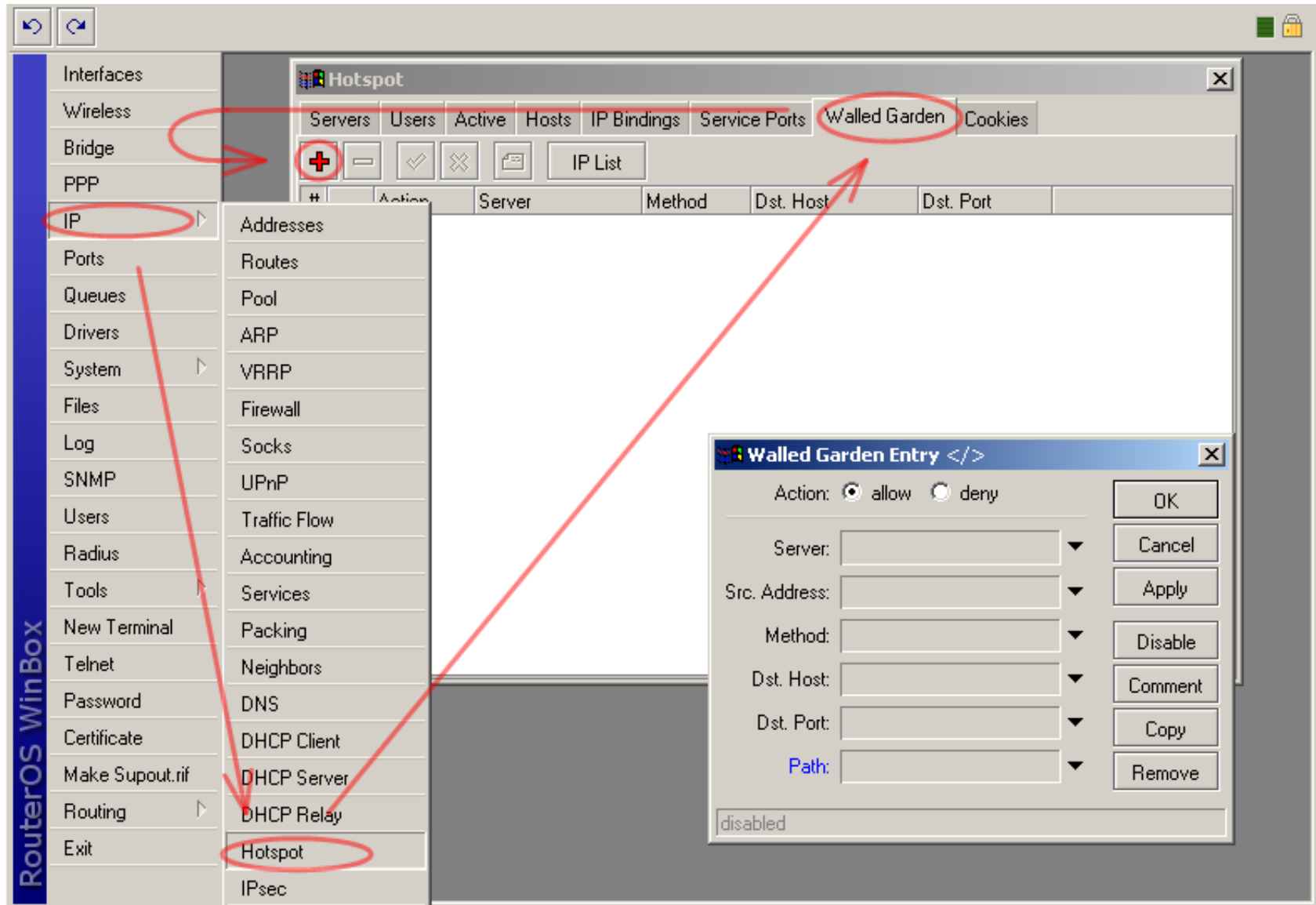
HotSpot IP Bindings



HotSpot IP Bindings

- Setup static NAT translations based on either
 - ◆ the original IP address (or IP network),
 - ◆ the original MAC address.
- Allow some addresses to bypass HotSpot authentication. Usefully for providing IP telephony or server services.
- Completely block some addresses.

HotSpot HTTP-level Walled Garden



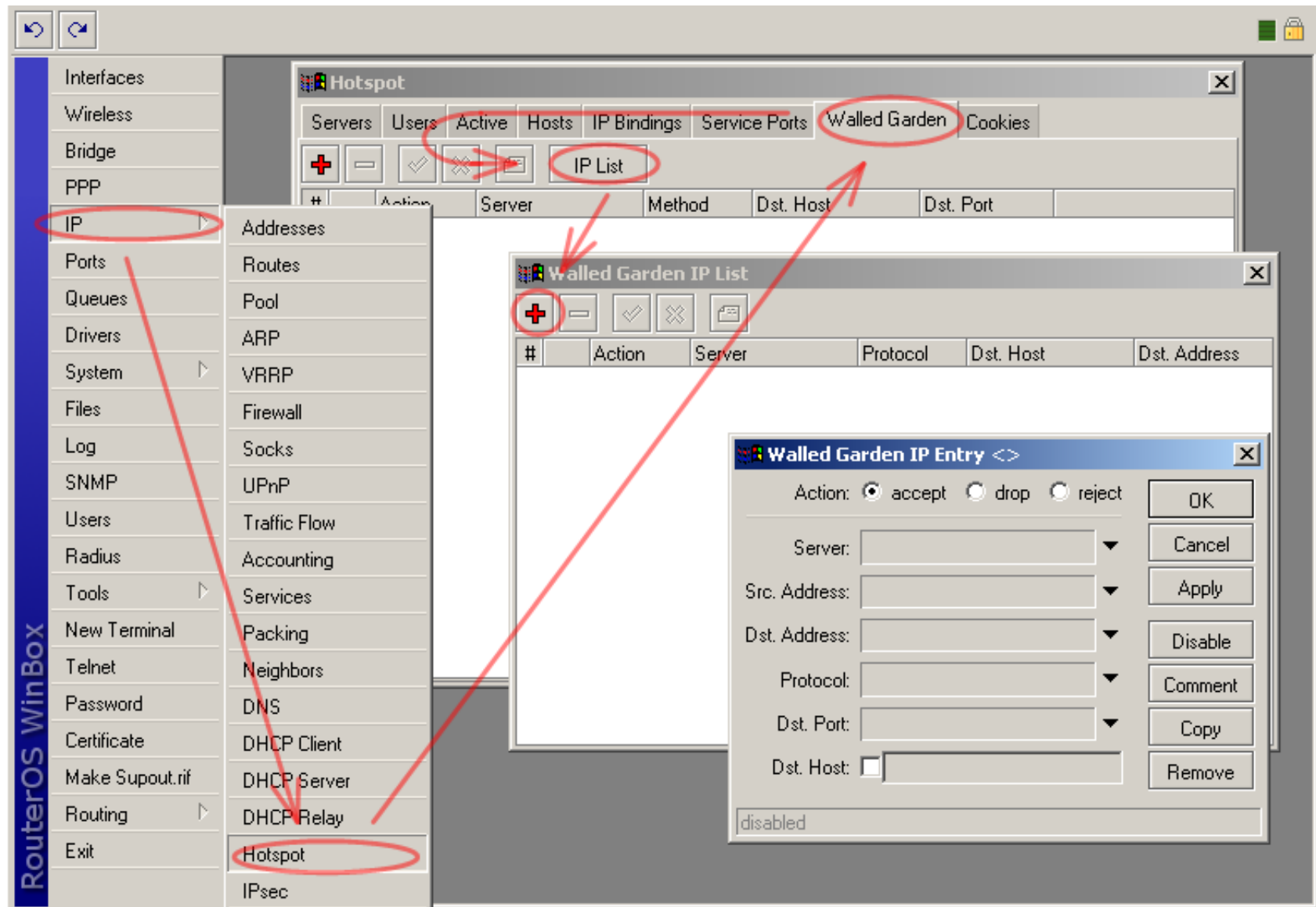
HotSpot HTTP-level Walled Garden

- Walled garden allows to bypass HotSpot authentication for some resources
- HTTP-level Walled Garden manages HTTP and HTTPS protocols
- HTTP-level Walled Garden works like Web-proxy filtering, you can use the same HTTP methods and same regular expressions to make an URL string

HotSpot IP-level Walled Garden

- IP-level Walled Garden works on the IP level, use it like IP firewall filter

HotSpot IP-level Walled Garden



Hotspot Lab

- Allow access to the www.mikrotik.com without the Hotspot authentication
- Allow access to your router's IP without the Hotspot authentication
- Create another user with 10MB download limitation.
- Check this user!
- Allow your laptop to bypass the Hotspot.


Login Page Customization

- There are HTML template pages on the router FTP for each active HotSpot profile
- Those HTML pages contains variables which will be replaced with the actual information by the HotSpot before sending to the client
- It is possible to modify those pages, but you must directly download HTML pages from the FTP to modify them correctly

Customized Page Example


```
$(if chap-id)
$(endif)
```

LATVISKI `$(if error)$(error)$(endif)`




Welcome to the Hotel
HotSpot service

To use this service you must ask
reception for user name and password.



`$(if trial == 'yes')`Also you can try
hotspot service with a trial user, [click
here](#).`$(endif)`



User name:
Password:

User Manager for HotSpot

- Centralized Authorization and Accounting system
- Works as a RADIUS server
- Built in MikroTik RouterOS as a separate package

Requirements for User Manager

- x86 based router with MikroTik RouterOS v2.9.x
- Router with at least 32MB RAM
- Free 2MB of HDD space
- RouterOS Level 4 license for more than 10 active sessions (in RouterOS v2.9.x)

Features

- User Authorization using PAP,CHAP
- Multiple subscriber support and permission management
- Credits/Prepaid support for users
- Rate-limit attribute support
- User friendly WEB interface support
- Report generation by time/amount
- Detailed sessions and logs support
- Simple user adding and voucher printing support

New Features

- User Authorization using MSCHAPv1,MSCHAPv2
- User status page
- User sign up system
- Support for decimal places in credits
- Authorize.net and PayPal payment gateway support
- Database backup feature
- License changes in RouterOS v3.0 for active users:
 - ◆ Level3 – 10 active users
 - ◆ Level4 – 20 active users
 - ◆ Level5 – 50 active users
 - ◆ Level6 – Unlimited active users

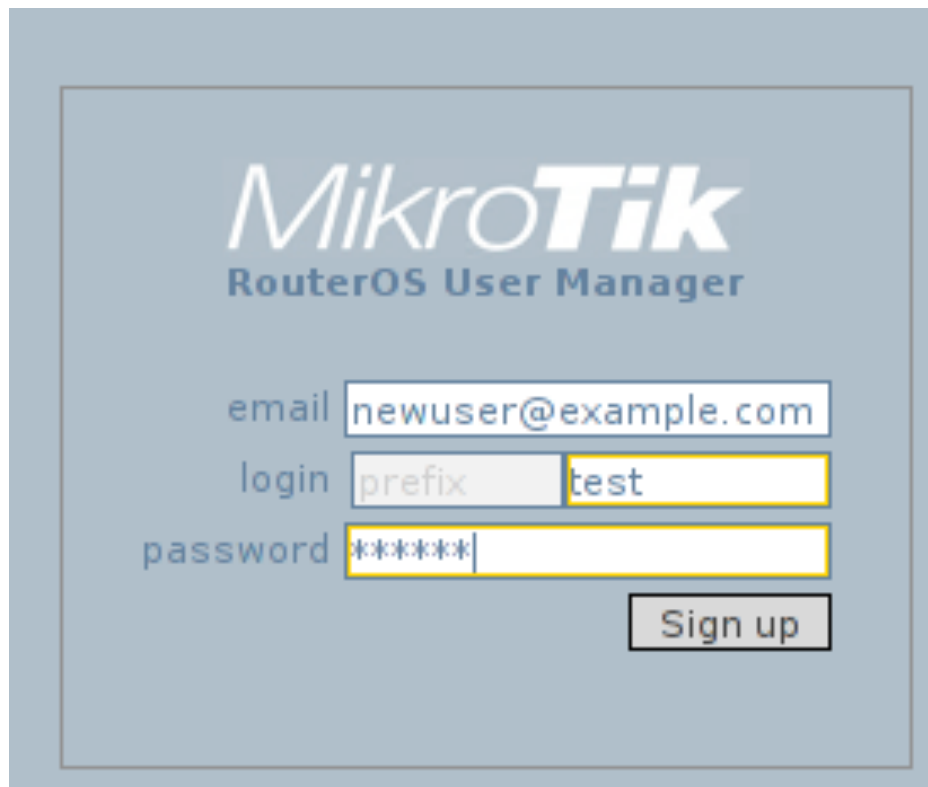
Supported Services

- Hotspot user authorization
- PPP/PPtP/PPPoE users authorization,
Encryption also supported
- DHCP MAC authorization
- Wireless MAC authorization
- RouterOS users authorization

User Manager Usage

- Hotels
- Airports
- Cafés
- Universities
- Companies
- ISPs

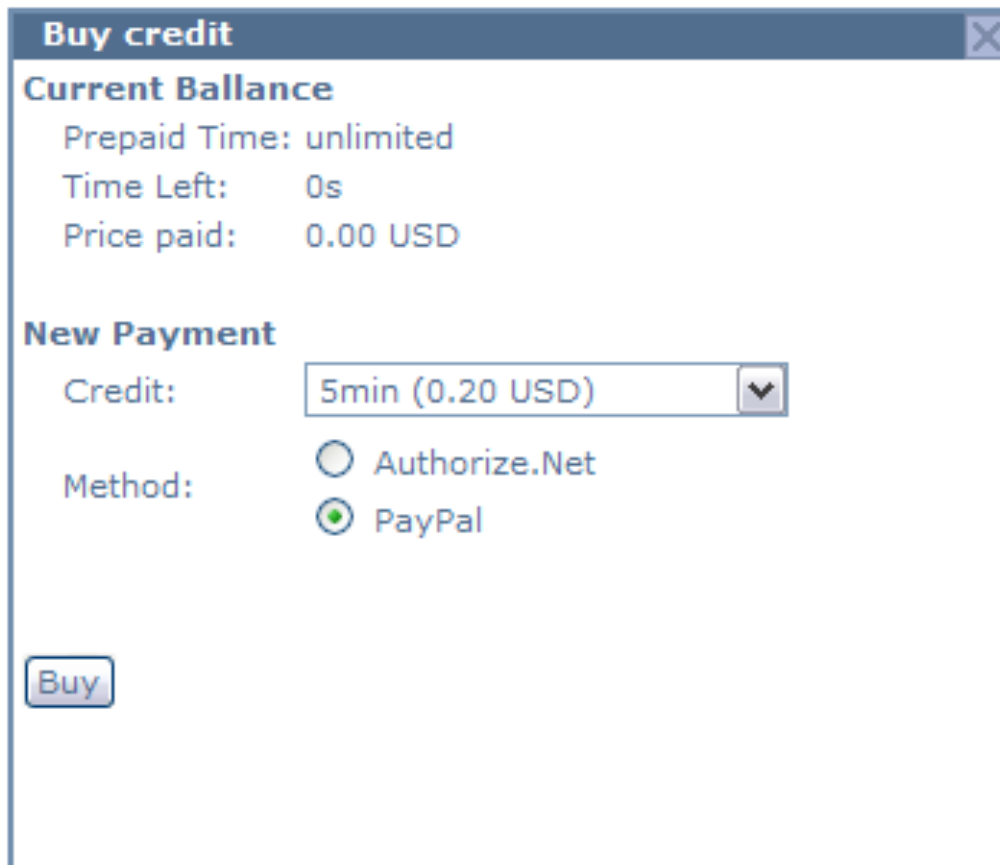
User Signup



The image shows a screenshot of the MikroTik RouterOS User Manager interface. At the top, the MikroTik logo is displayed in white and blue, with the text "RouterOS User Manager" below it. Below the logo, there are three input fields: "email" with the value "newuser@example.com", "login" with the value "prefix" and "test" (the "test" part is highlighted in yellow), and "password" with the value "*****" (the "*****" part is highlighted in yellow). A "Sign up" button is located at the bottom right of the form.

User can create a new account by filling out the form. An account activation email will be sent to the users email address

Buying Prepaid Credit Time



Buy credit

Current Balance

Prepaid Time: unlimited
Time Left: 0s
Price paid: 0.00 USD

New Payment

Credit: 5min (0.20 USD) ▼

Method: Authorize.Net
 PayPal

Buy

Authorize.net/PayPal payment support for buying a credit

Payment data (such as credit card number and expiry date) is sent directly from user's computer to payment gateway and is not captured by User Manager. User Manager processes only response about the payment result from the payment gateway.

Future plans

- Still in development – BETA
- New improved User Manager WEB interface
- Radius Incoming (RFC3576)
- Your suggestions are welcome...
support@mikrotik.com