MikroTik RouterOS Training

Routing

© MikroTik 2008

Instructors

- Ziad Sobri, MTCNA, MTCRE, MTCTCE, MTCWE, MTCUME, MTCINE, MikroTik Certified Trainer, MikroTik Academy Trainer, MikroTik Academy Coordinator
- Working with RouterOS since 2007
- Other Certifications :
  - Cisco Certified Network Associate (CCNA)
  - Juniper Network Certified Internetworking Associate (JNCIA), Juniper Network Certified Internetworking Specialist – Service Provider (JNCIS-SP)
  - Ubiquiti Broadband Wireless Specialist (UBWS), Ubiquiti Broadband Wireless Admin (UBWA), Ubiquiti Enterprise Wireless Admin (UEWA), Ubiquiti Certified Trainer

Housekeeping

- Course materials
- Routers, cables
- Break times and lunch
- Restrooms and smoking area locations

Course Objective

- Provide thorough knowledge and hands-on training for MikroTik RouterOS basic and advances routing capabilities for small and medium size networks
- Upon completion of the course you will be able to plan, implement, adjust and debug routed MikroTik RouterOS network configurations.

Introduce Yourself

- Please, introduce yourself to the class
  - Your name
  - Your Company
  - Your previous knowledge about RouterOS
  - Your previous knowledge about networking
  - What do you expect from this course?

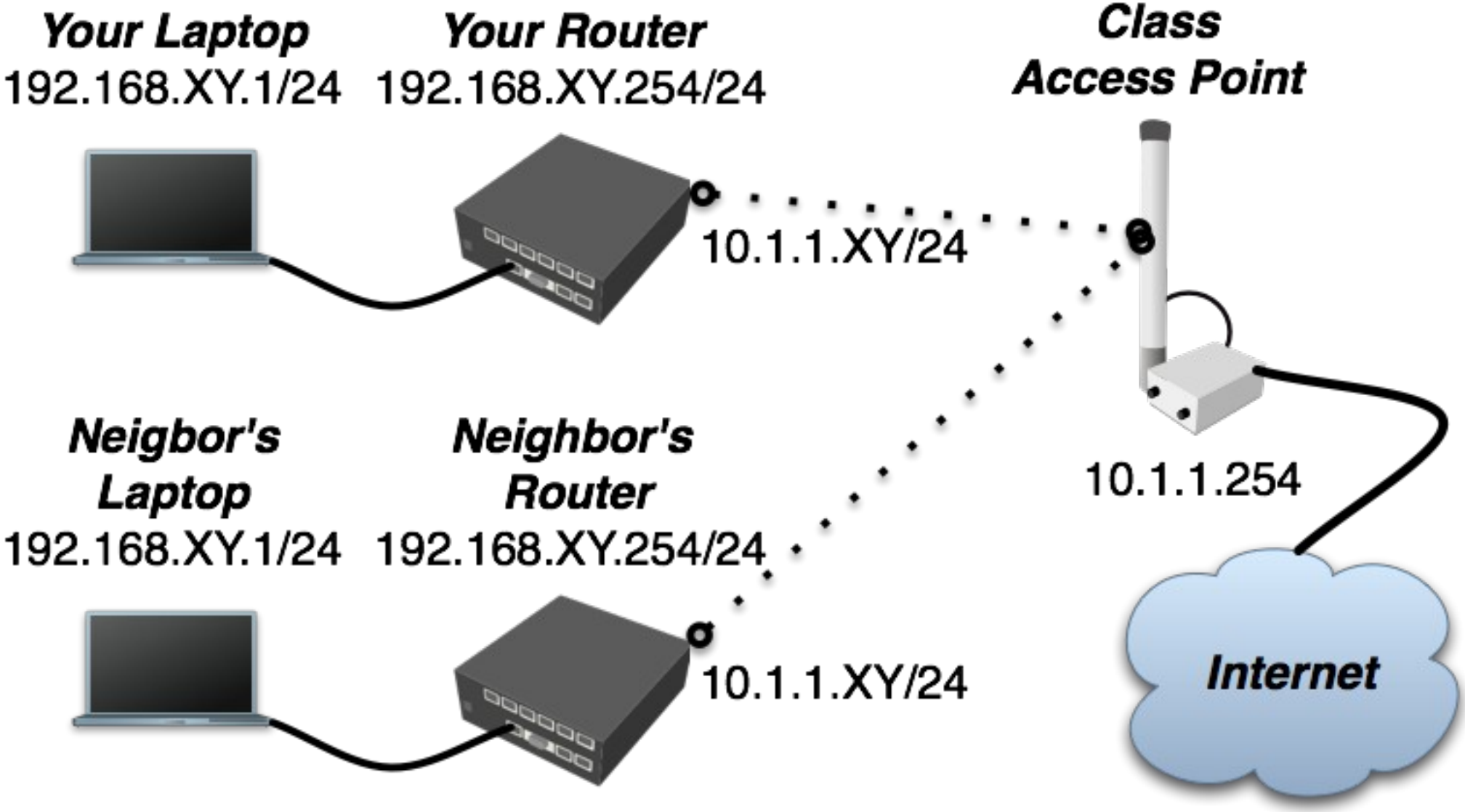
- Please, remember your class XY number.
  (X is number of the row, Y is your seat number in the row)

My number is:_____

Class Setup Lab

- Create an 192.168.XY.0/24 Ethernet network between the laptop (.1) and the router (.254)
- Connect routers to the AP SSID “ap_rb532”
- Assign IP address 10.1.1.XY/24 to the wlan1
- Main GW and DNS address is 10.1.1.254
- Gain access to the internet from your laptops via local router
- Create new user for your router and change “admin” access rights to “read”

Class Setup


Your Laptop
192.168.XY.1/24
Your Router
192.168.XY.254/24
Class
Access Point
10.1.1.XY/24
10.1.1.254
Neigbor's
Laptop
192.168.XY.1/24
Neighbor's
Router
192.168.XY.254/24
10.1.1.XY/24
Internet

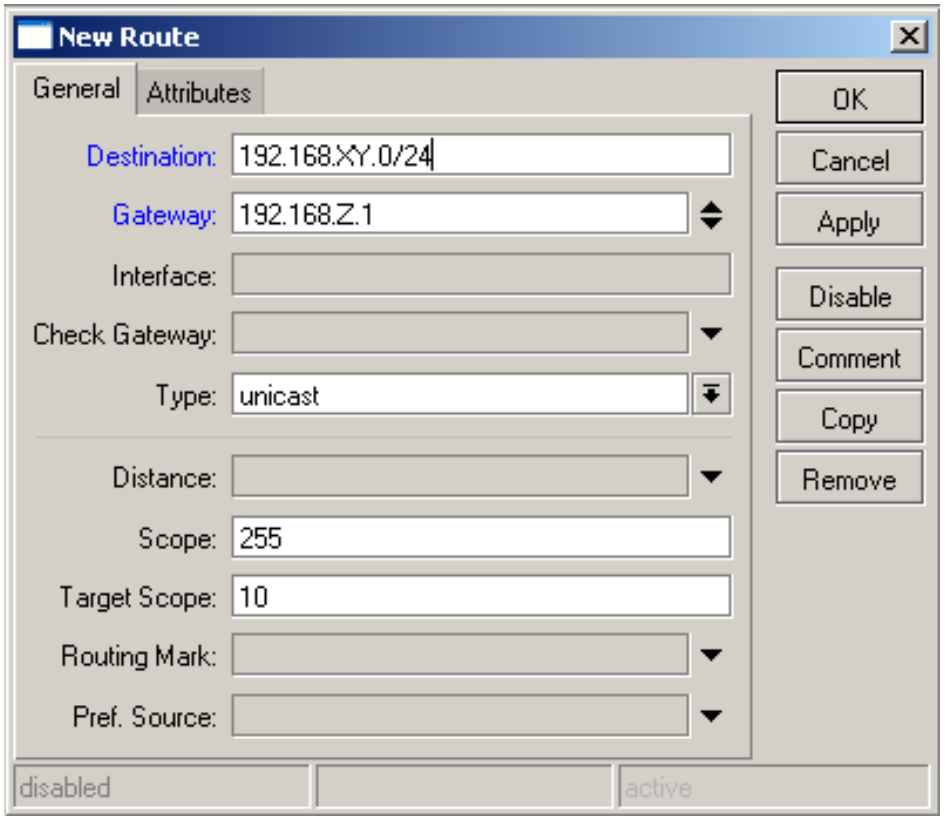
Class setup Lab (cont.)

- Set system identity of the board and wireless radio name to “XY_<your_name>”. Example: ***“00_Janis”***
- Upgrade your router to the latest Mikrotik RouterOS version
- Upgrade your Winbox loader version
- Set up NTP client – use 10.1.1.254 as server
- Create a configuration **backup** and copy it to the laptop (it will be default configuration)

Simple Routing

Distance, Policy Routing, ECMP, Scope, Dead-End and Recursive Next-Hop Resolving

Simple Static Route

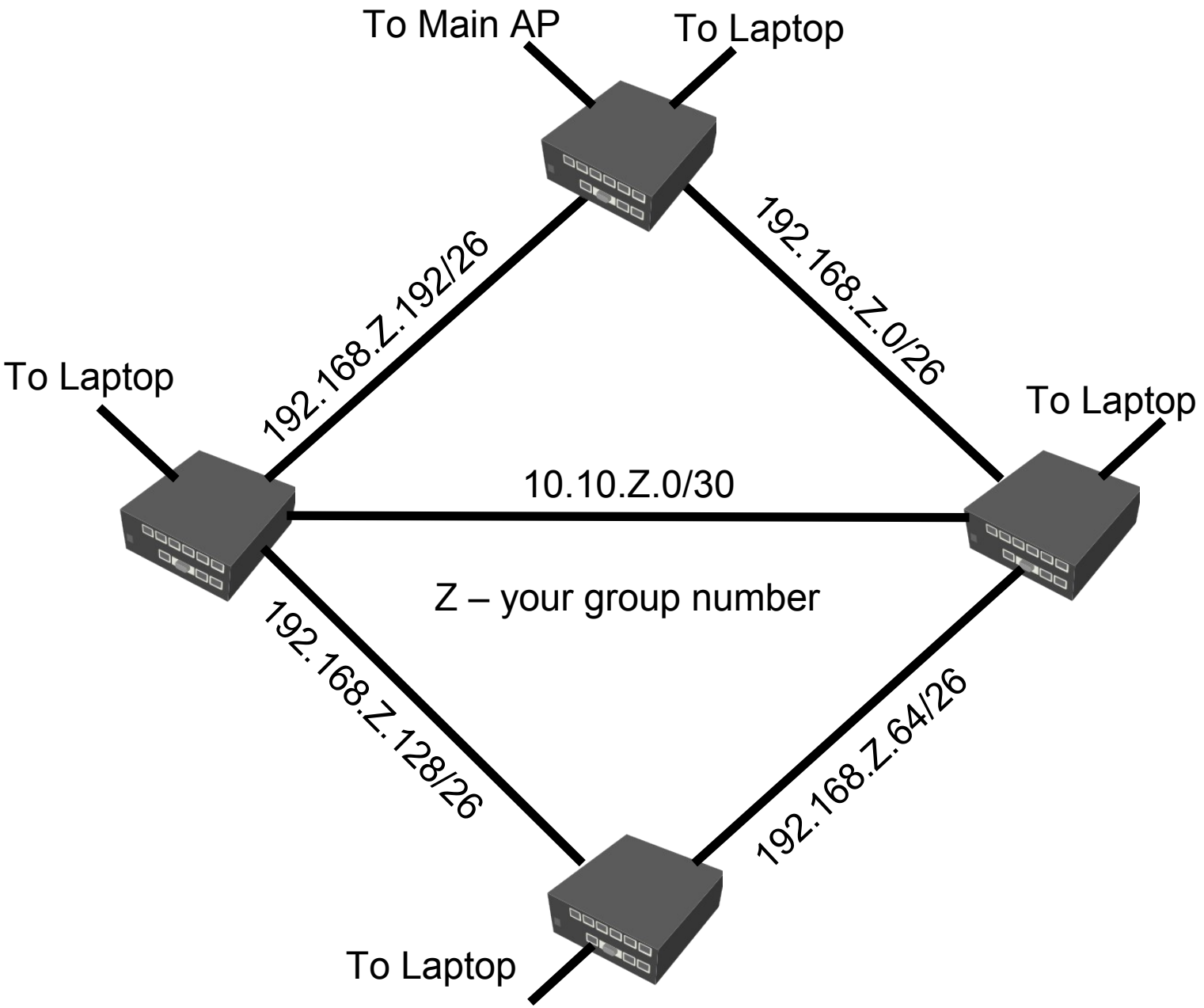


- Only one gateway for a single network
- More specific routes in the routing table have higher priority than less specific
- Route with destination network 0.0.0.0/0 basically means “everything else”

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

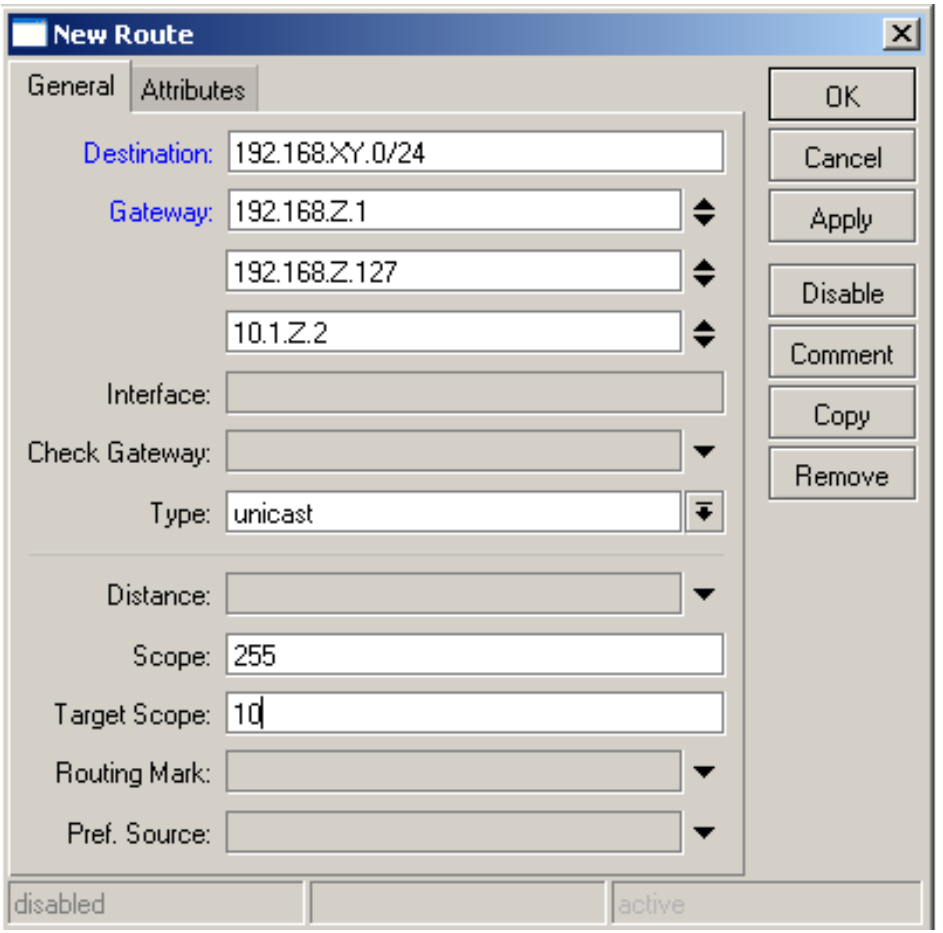
IP Network Structure



Questions!

- Is it possible to manually create routes that will ensure
  - load balancing
  - failover
  - best path
- Is it possible to create routes in this situation?
- Lets take a look!

ECMP Routes



- 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
- Same gateway can be written several times!!

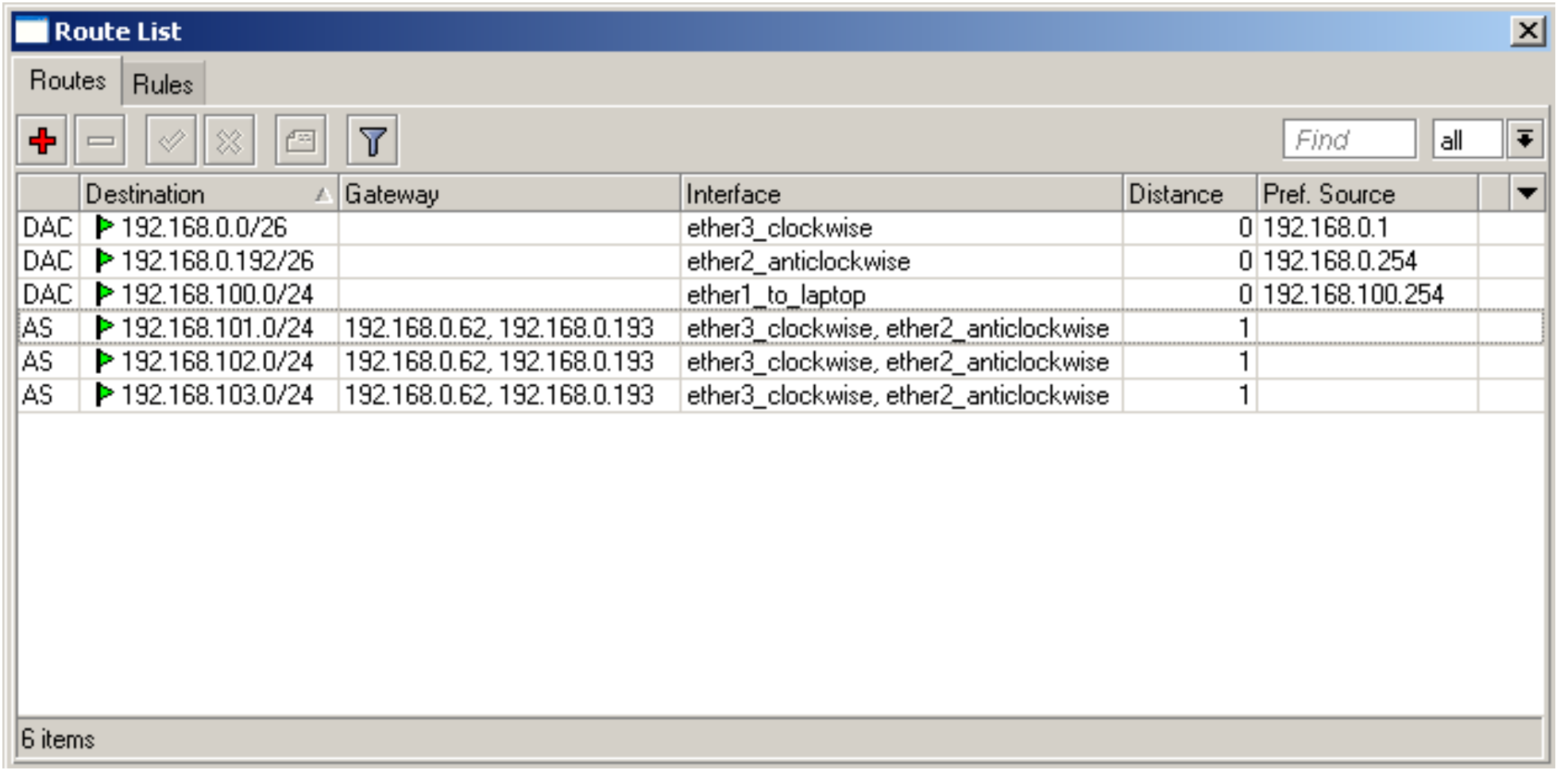
“Check-gateway” Option

- You can set 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
- If Check-gateway option is enabled on one route it will affect all routes with that gateway.

ECMP Lab

- To avoid routing loops
  - Only one participant creates ECMP to every 192.168.XY.0/24 network with “check-gateway”
  - Other participants adjust simple routes to reach each other without routes though the first participant
- Check the redundancy
- Use traceroute to examine the setup
- Use “Undo” to get back pre-lab configuration - **only then proceed to next participant and start over**

Configuration Example



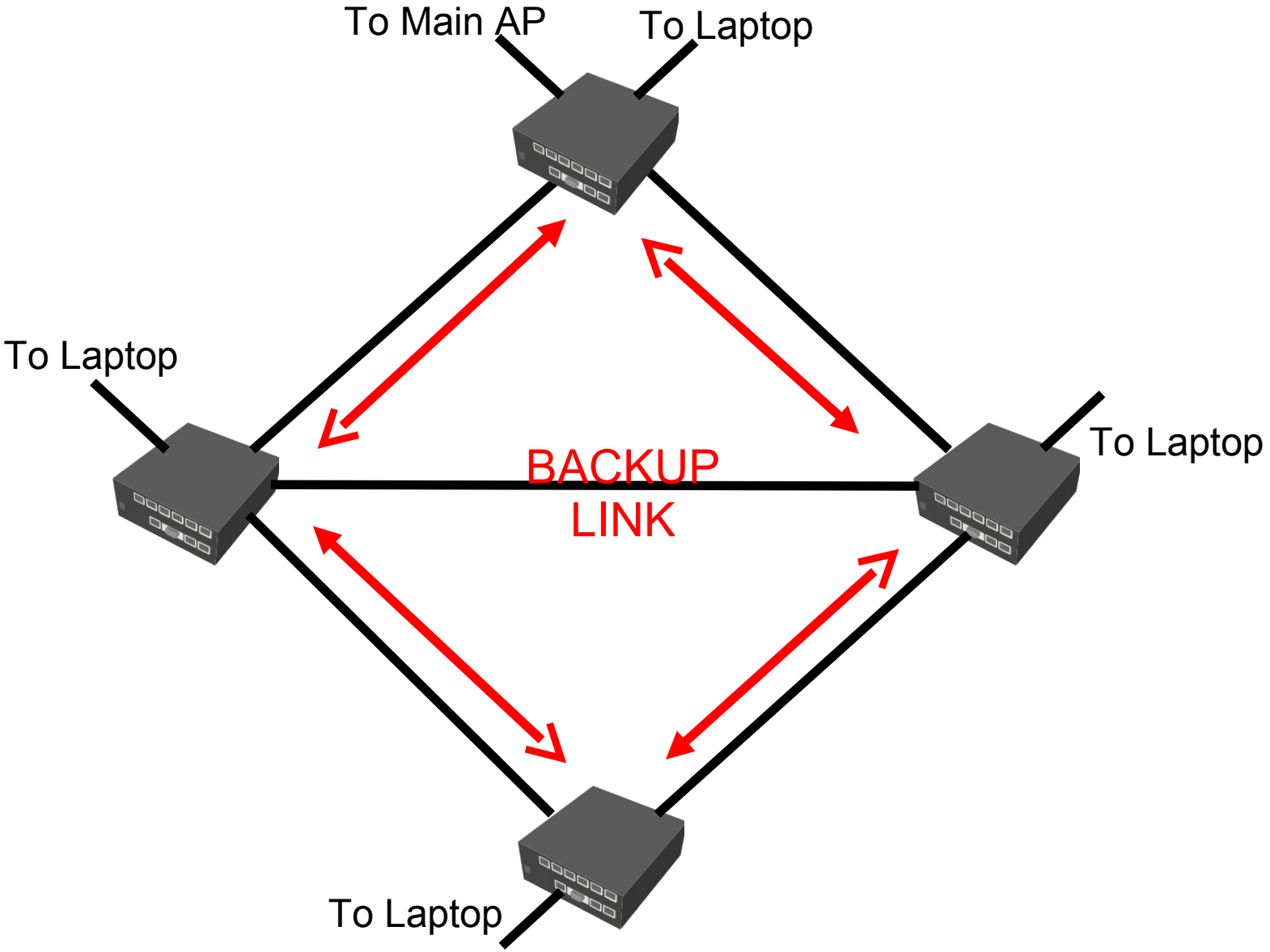
“Distance” Option

- 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

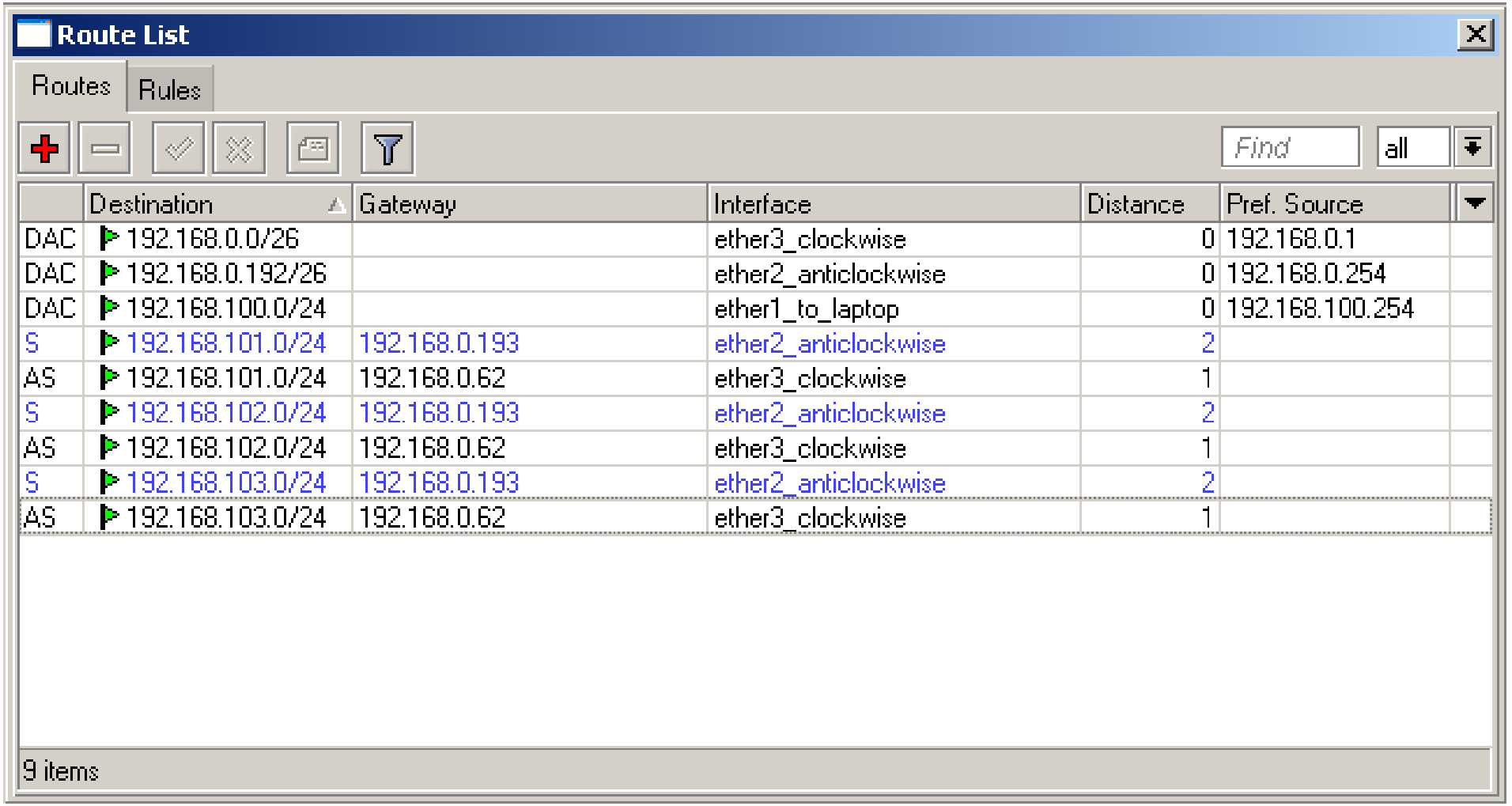
Route Distance Lab

- Create 2 separate routes for each participants local network:
  - One route clockwise with Distance=1
  - One route anticlockwise with Distance=2
- Check the redundancy by disabling clockwise gateway IP addresses
- Use traceroute to examine the setup

Route Distance Lab



Configuration Example



Observed Behaviour

- Traffic has no problems to pass clockwise
- In the case of “check-gateway” failure only affected router will pass traffic anticlockwise – every other router will continue to send it clockwise
- Solution:
  - If traffic starts to go anticlockwise, it should be routed anticlockwise until it reaches destination

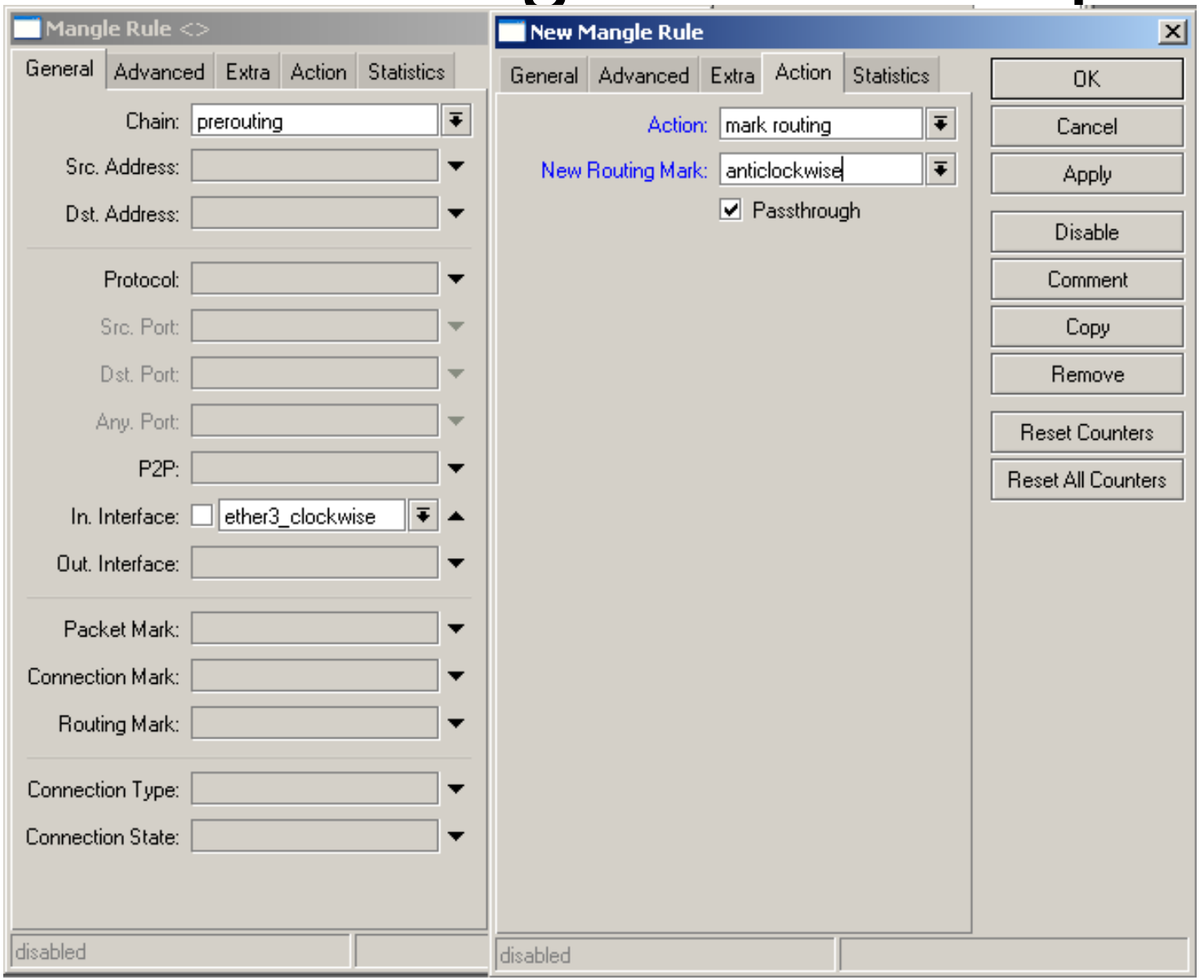
Routing Mark

- To assign specific traffic to the route – traffic must be identified by routing mark
- Routing marks can be assigned by IP firewall mangle facility **only in** chains prerouting and output
- Packets with the routing mark will be ignored by main routing table, if there is at least one route for that routing mark (if none main routing table will be used)
- Each packet can have only one routing mark

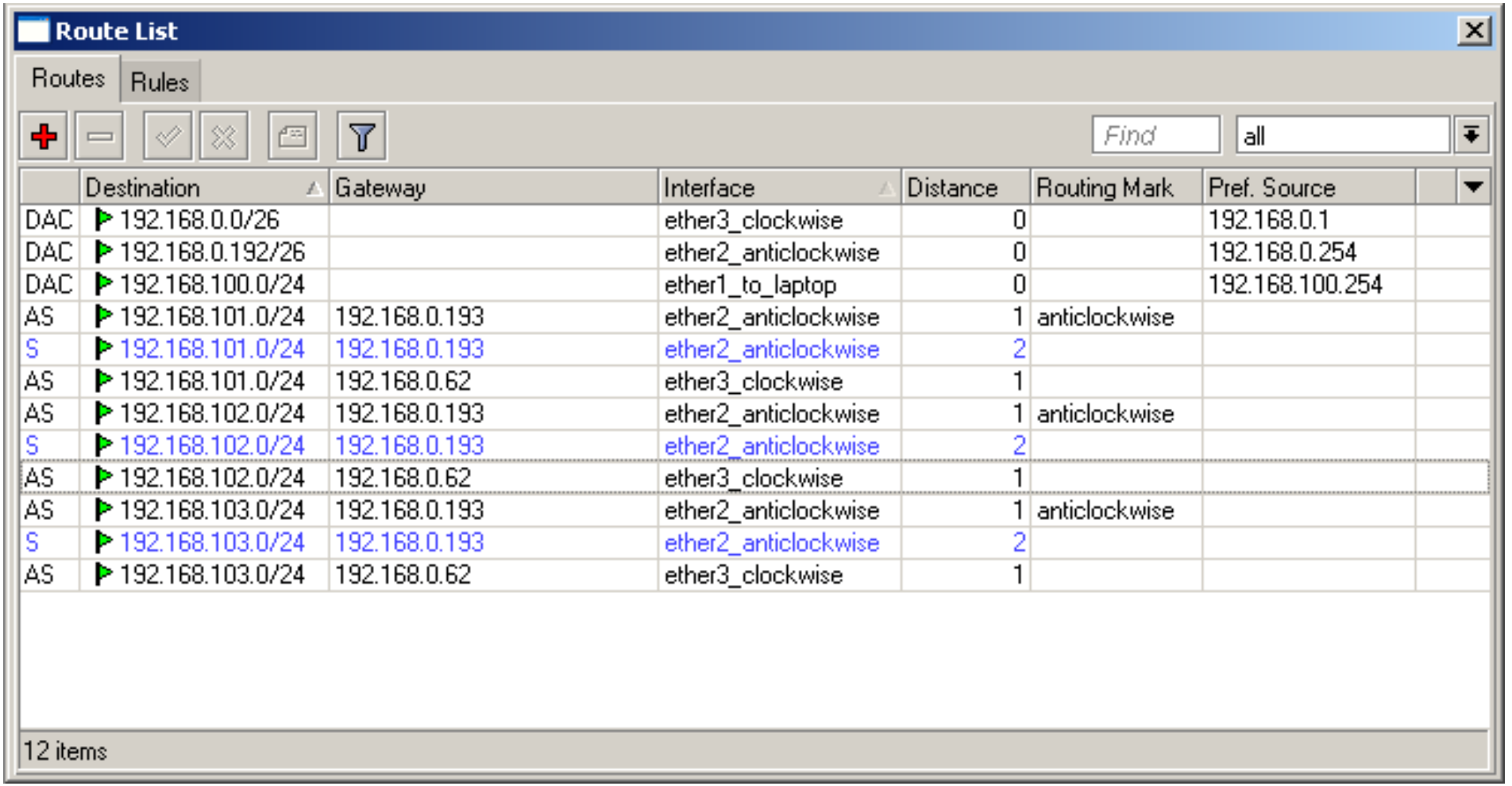
Routing Policy Lab

- Mark all traffic that passes the router (chain prerouting) in anticlockwise direction
- Create a route for marked traffic (use routing-mark option) and send it in anticlockwise direction
- Check the redundancy by disabling clockwise gateway IP addresses
- Use traceroute to examine the setup

Mark Routing Rule Example



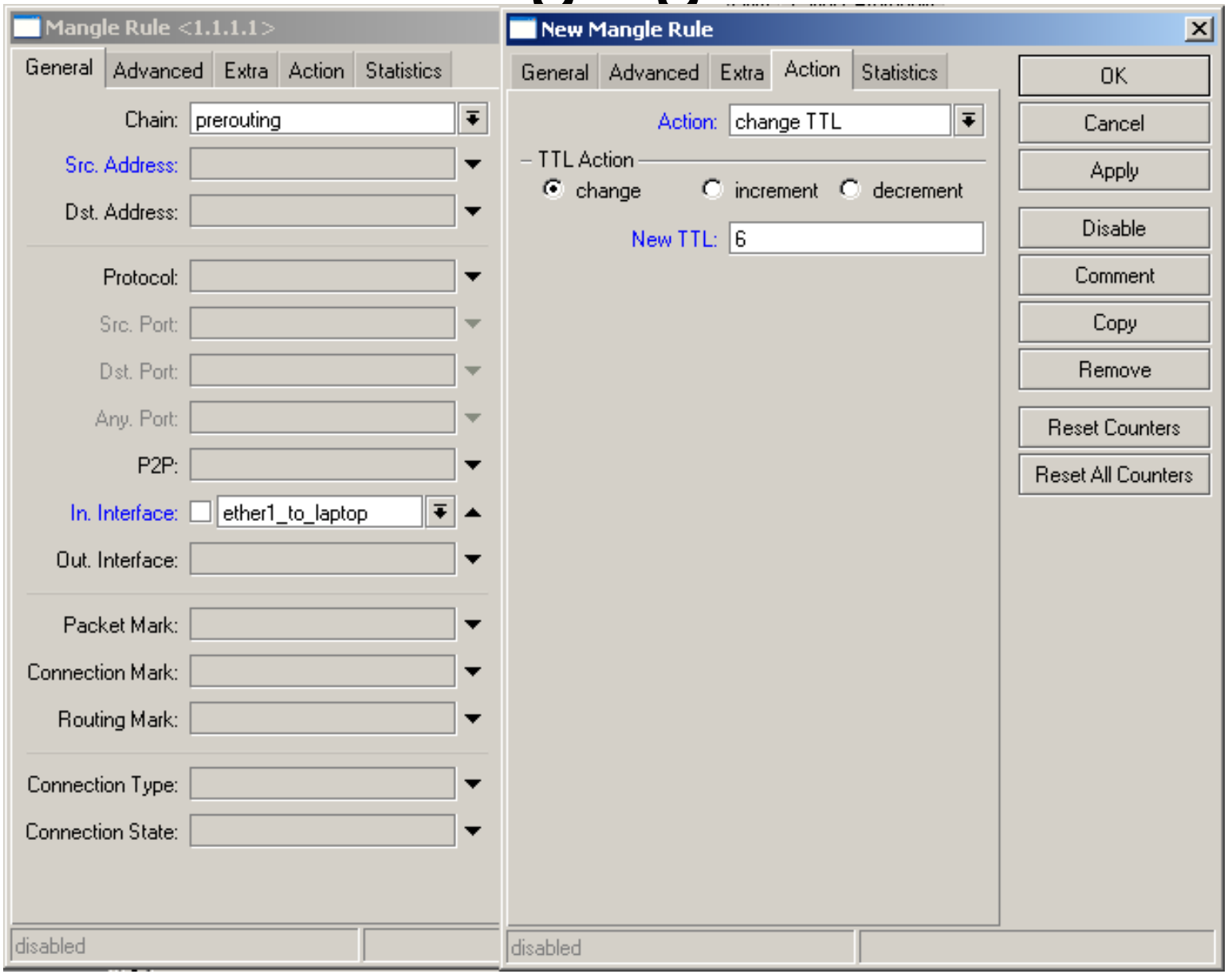
Configuration Example



Time To Live (TTL)

- TTL is a limit of Layer3 devices that IP packet can experience before it should be discarded
- TTL default value is 64 and each router reduce value by one **just before** forwarding decision
- TTL can be adjusted in **IP firewall mange** facility
- Router will not pass traffic to the next device if it receives IP packet with TTL=1
- Useful application: eliminate possibility for clients to create masqueraded networks

Changing TTL



Recursive Next-hop Resolving

- It is possible to specify gateway to network even if gateway is not directly reachable – by using recursive next-hop resolving from any existing route
- Useful for setups where middle section between your router and the gateway is not constant (iBGP for example)
- One route must be in **scope** of other route for recursive next-hop resolving to work

Scope/Target-Scope

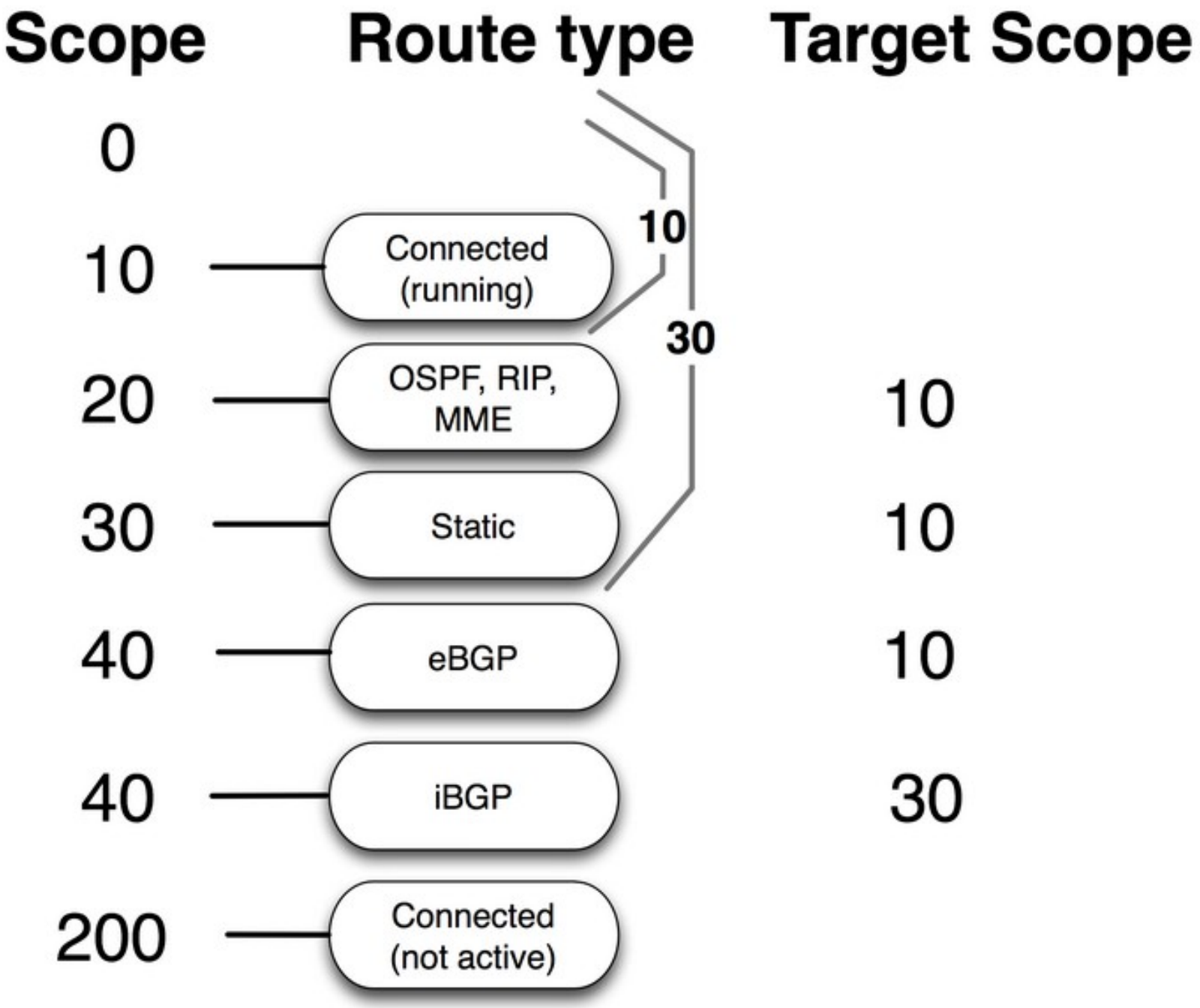
- Route's scope contains all routes that “scope” value is less or equal to its “target-scope” value

Example:

0 ADC dst-address=1.1.1.0/24 pref-src=1.1.1.1
interface=ether1 scope=10 target-scope=0

1 A S dst-address=2.2.2.0/24 gateway=1.1.1.254
interface=ether1 scope=30 target-scope=10

2 A S dst-address=3.3.3.0/24 gateway=2.2.2.254
interface=ether1 scope=30 **target-scope=30**


Scope
Route type
Target Scope
0
10
20
30
40
40
200
Connected (running)
OSPF, RIP, MME
Static
eBGP
iBGP
Connected (not active)
10
30
10
10
10
30

Other Options

- **“Type” option** allows to create dead-end (blackhole/prohibit/unreachable)routes to block some networks to be routed further in the network
- **“Preferred Source” option** points preferred router source address for locally originated packets

Clean-up Lab

- Delete all mangle rules
- Delete all IP routes
- Leave all IP addresses and network structure intact

Open Shortest Path First (OSPF)

Areas, Costs, Virtual links,
Route Redistribution and Aggregation

© MikroTik 2008

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)

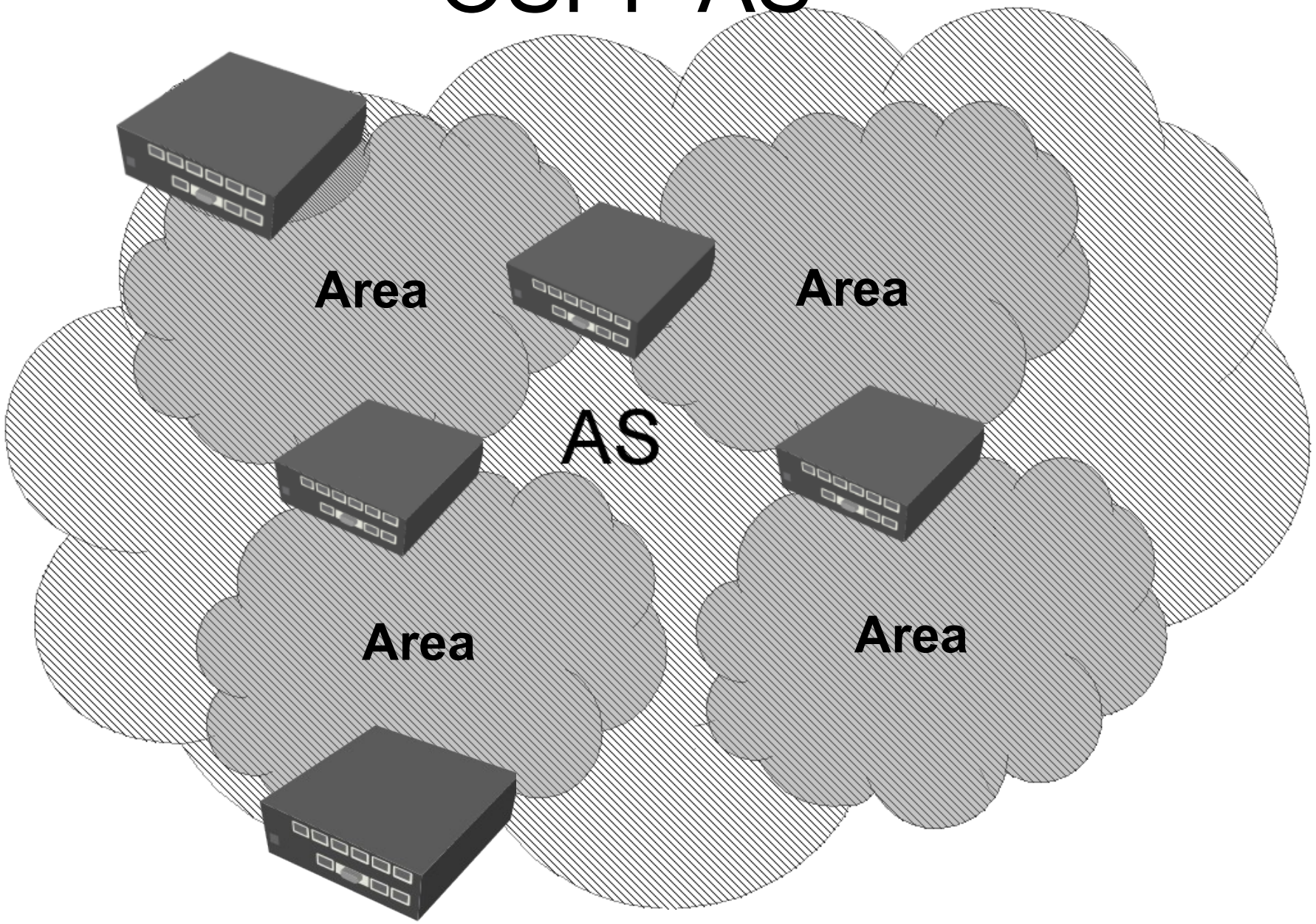
- An autonomous system is a collection of IP networks and routers under the control of one entity (OSPF, iBGP ,RIP) that presents a common routing policy to rest of the network
- AS is identified by 16 bit number (0 - 65535)
  - Range from 1 to 64511 for use in the Internet
  - Range from 64512 to 65535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

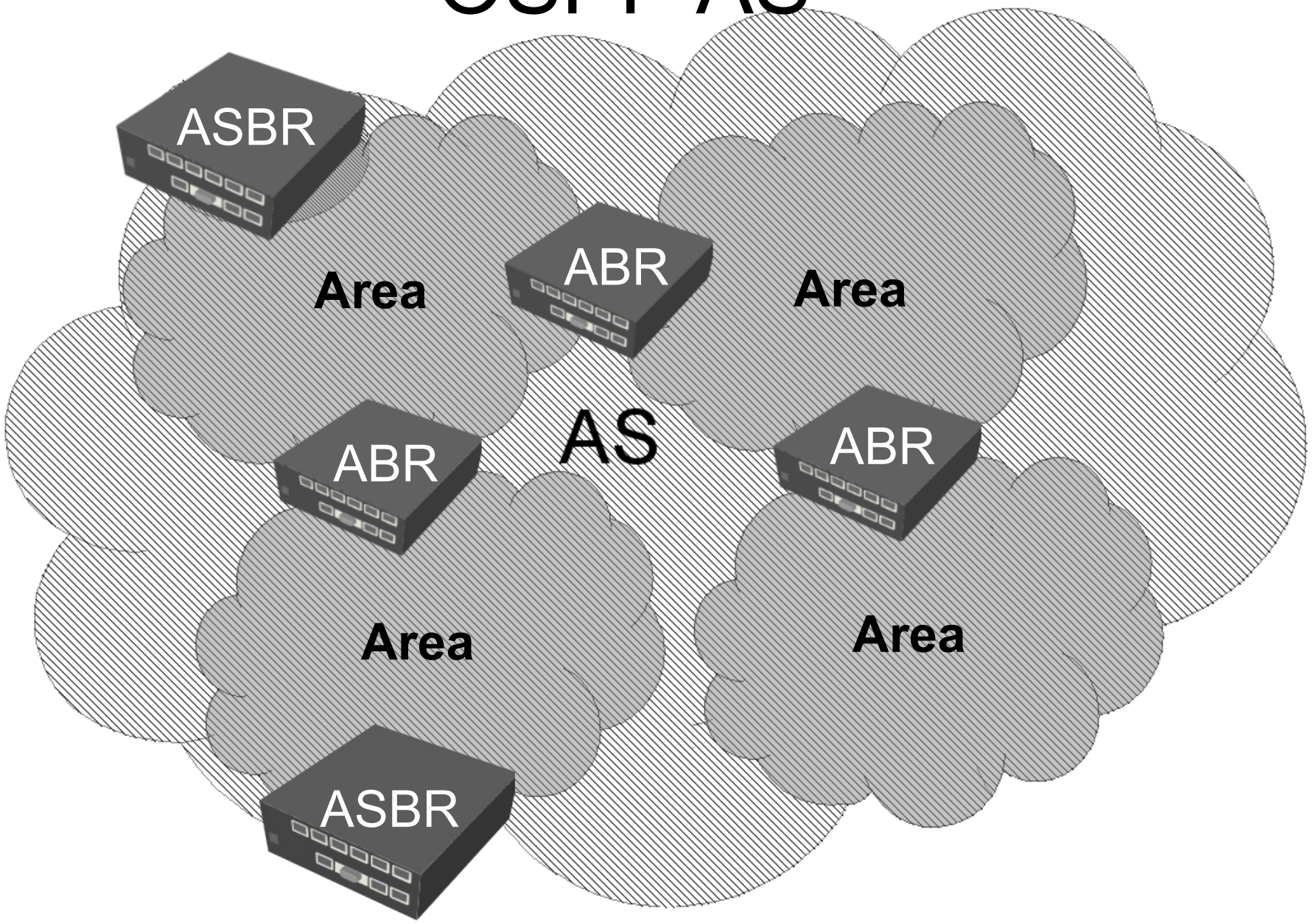
OSPF AS



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

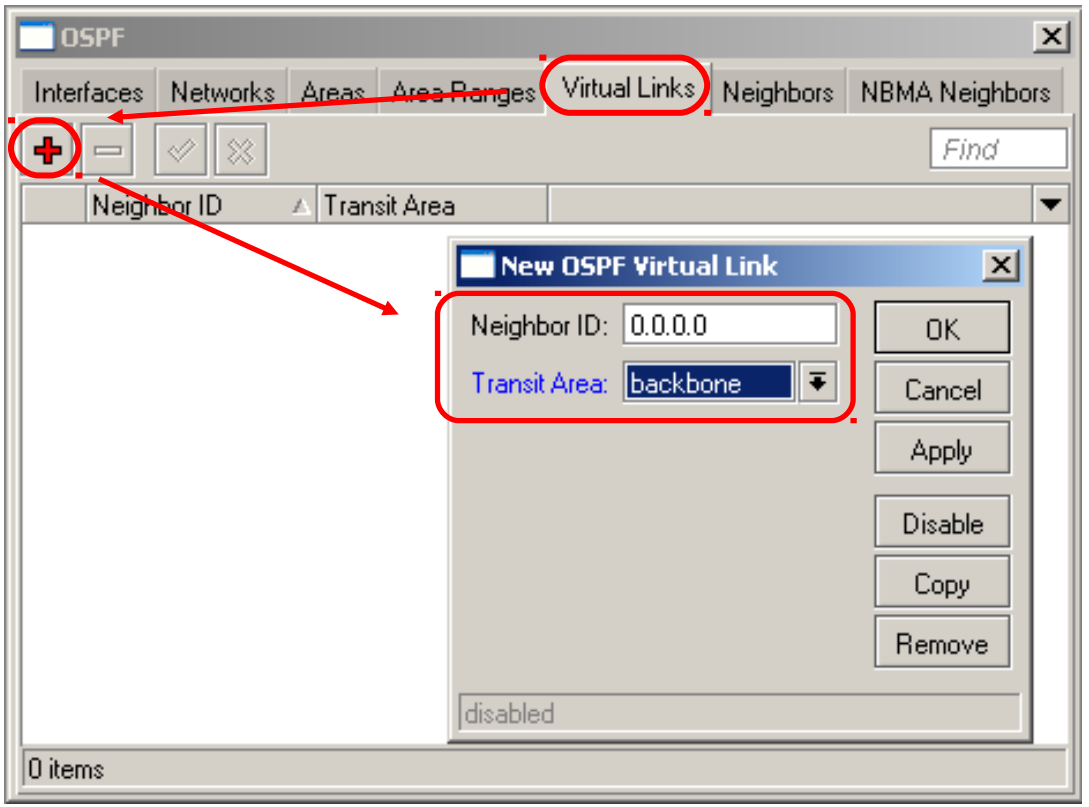
OSPF AS



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)

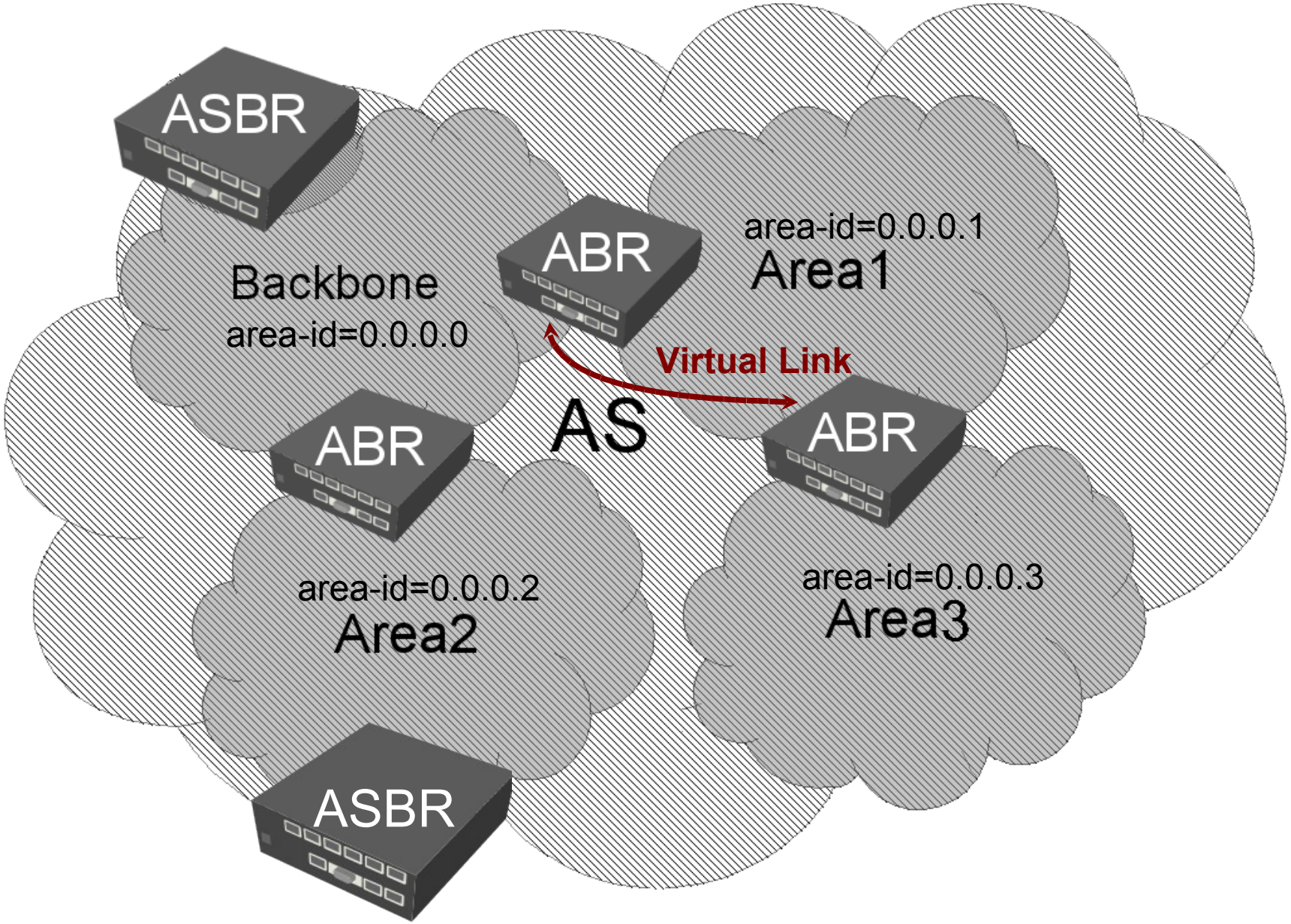
Virtual Links



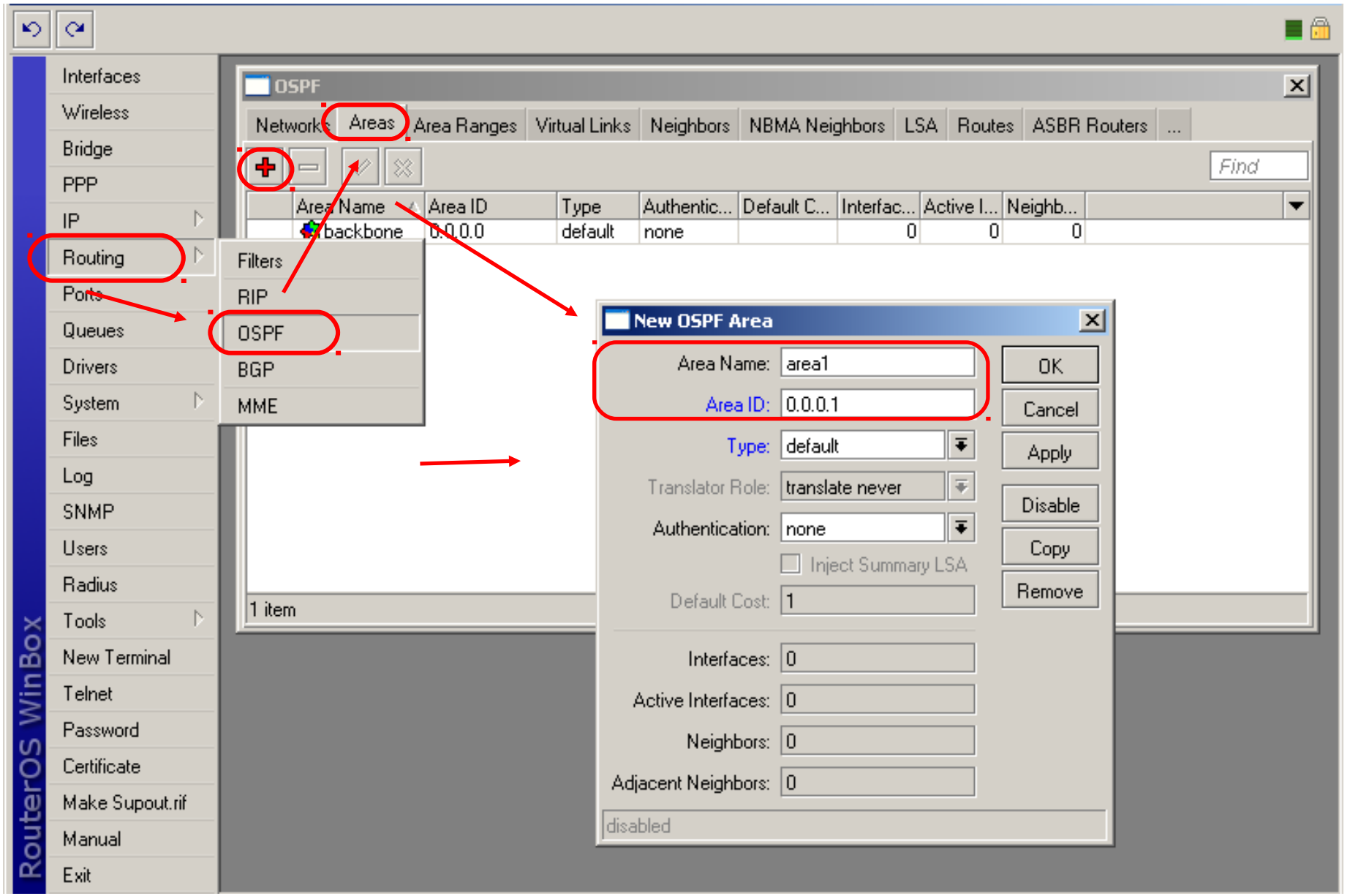
- Used to connect remote areas to the backbone area through a non-backbone area

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

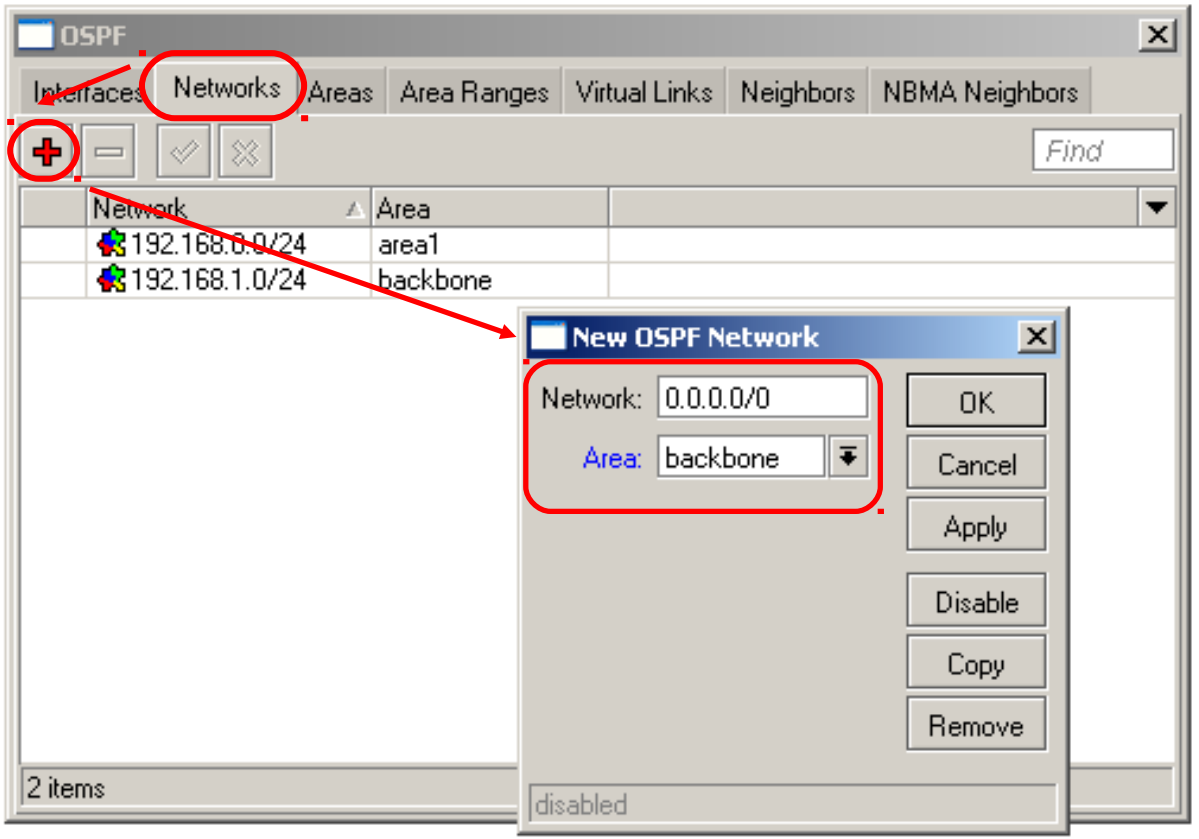
OSPF AS


ASBR
ABR
area-id=0.0.0.1
Area1
Backbone
area-id=0.0.0.0
Virtual Link
AS
ABR
ABR
area-id=0.0.0.2
Area2
area-id=0.0.0.3
Area3
ASBR

OSPF Areas


RouterOS WinBox
Interfaces
Wireless
Bridge
PPP
IP
Routing
Ports
Queues
Drivers
System
Files
Log
SNMP
Users
Radius
Tools
New Terminal
Telnet
Password
Certificate
Make Supout.rif
Manual
Exit
Filters
RIP
OSPF
BGP
MME
OSPF
Networks
Areas
Area Ranges
Virtual Links
Neighbors
NBMA Neighbors
LSA
Routes
ASBR Routers
...
Find
Area Name
Area ID
Type
Authentic...
Default C...
Interfac...
Active I...
Neighb...
backbone
0.0.0.0
default
none
0
0
0
1 item
New OSPF Area
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
disabled
OK
Cancel
Apply
Disable
Copy
Remove

OSPF Networks

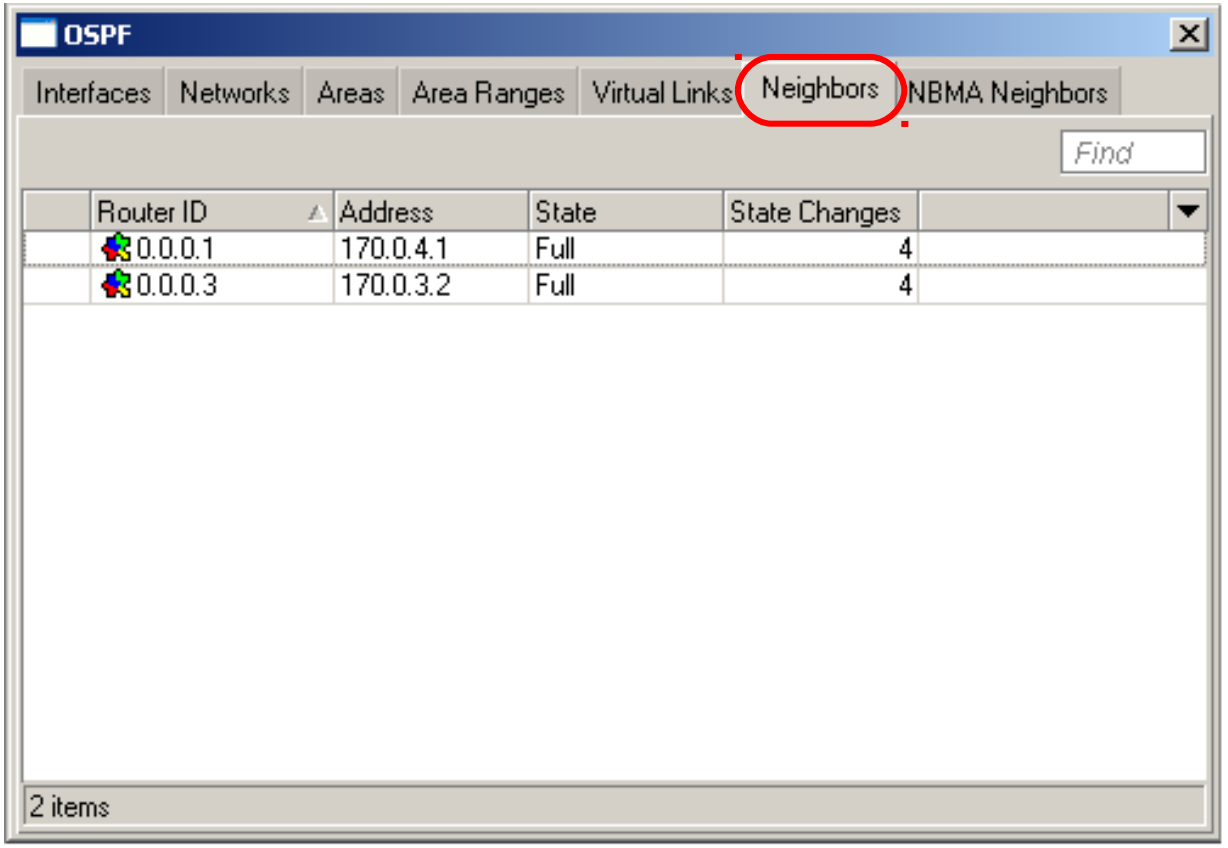


- It is necessary to specify networks and associated areas where to look for other OSPF routers

- 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



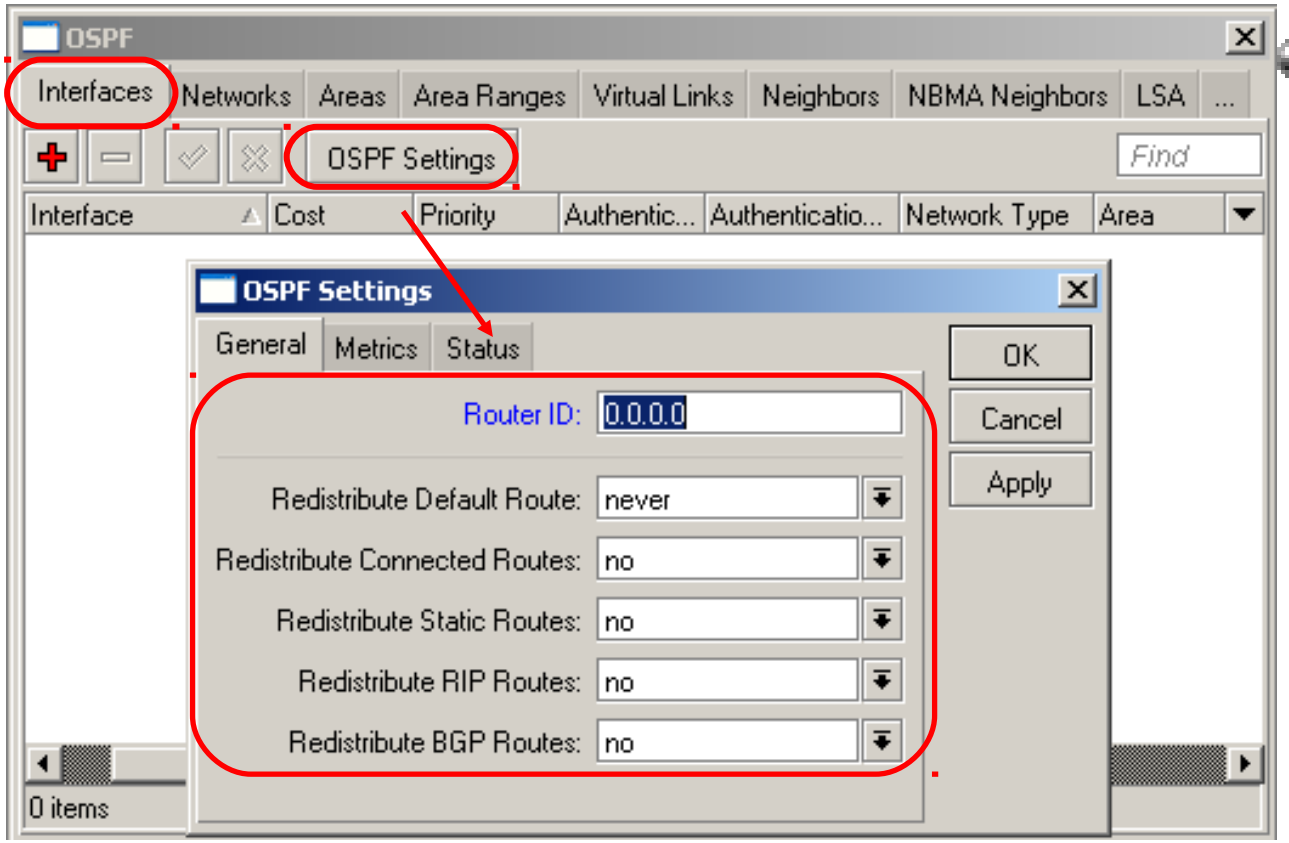
- Down,Attempt,Init,Loading,ExStart,Exchange: not completely running!

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 and routing tables

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

OSPF Settings

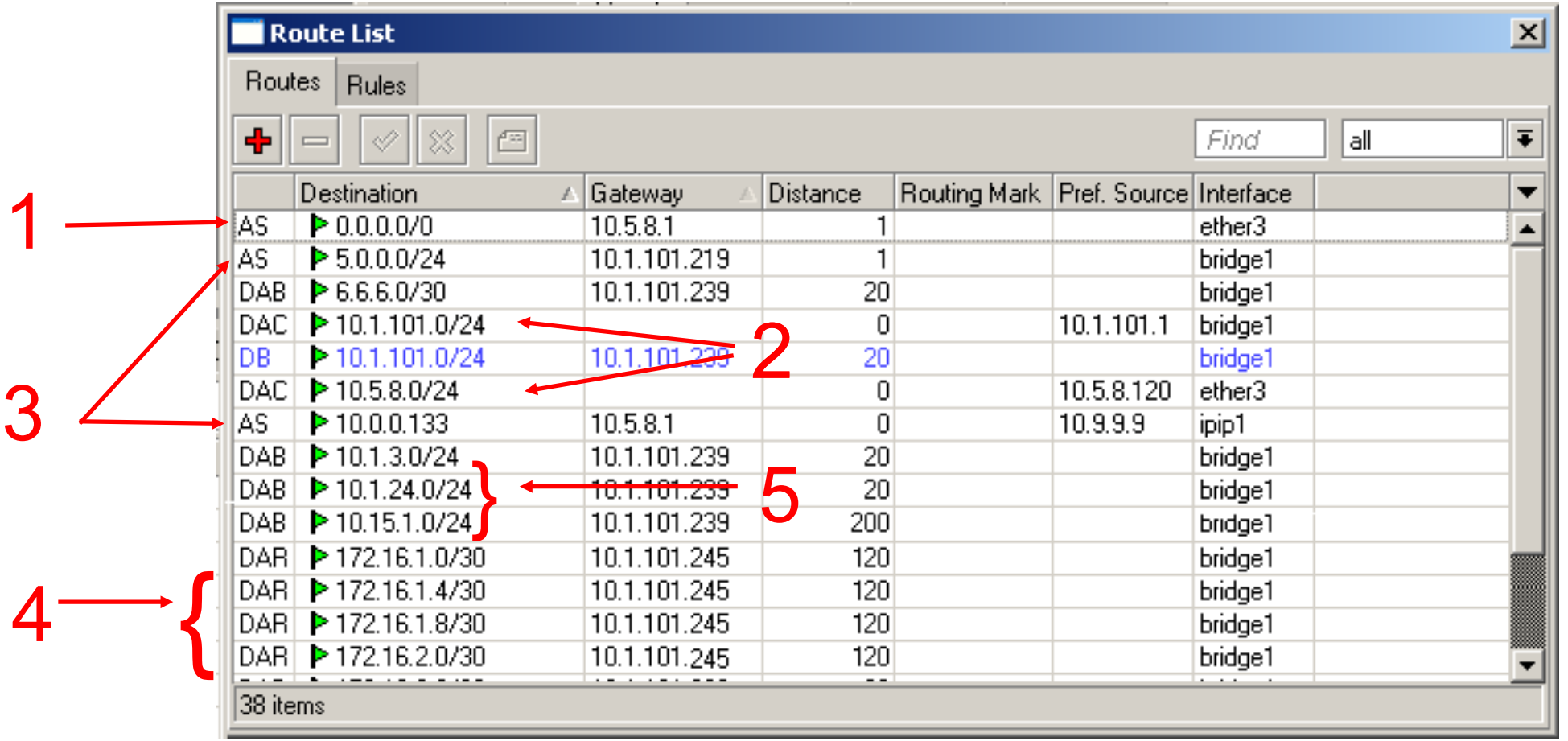


- Router ID must be unique within the AS

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

What to Redistribute?

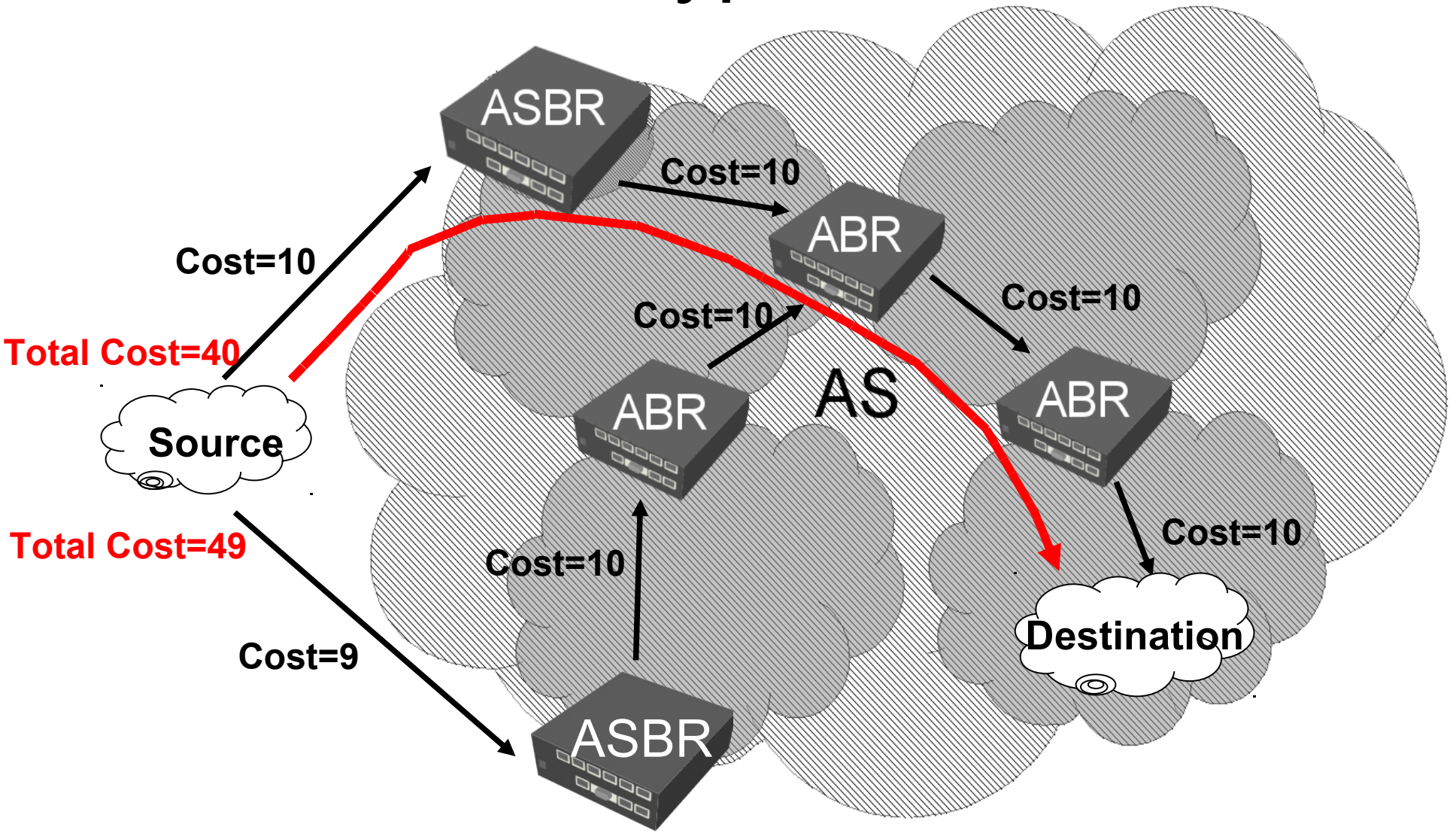
- Default route is not considered as static route



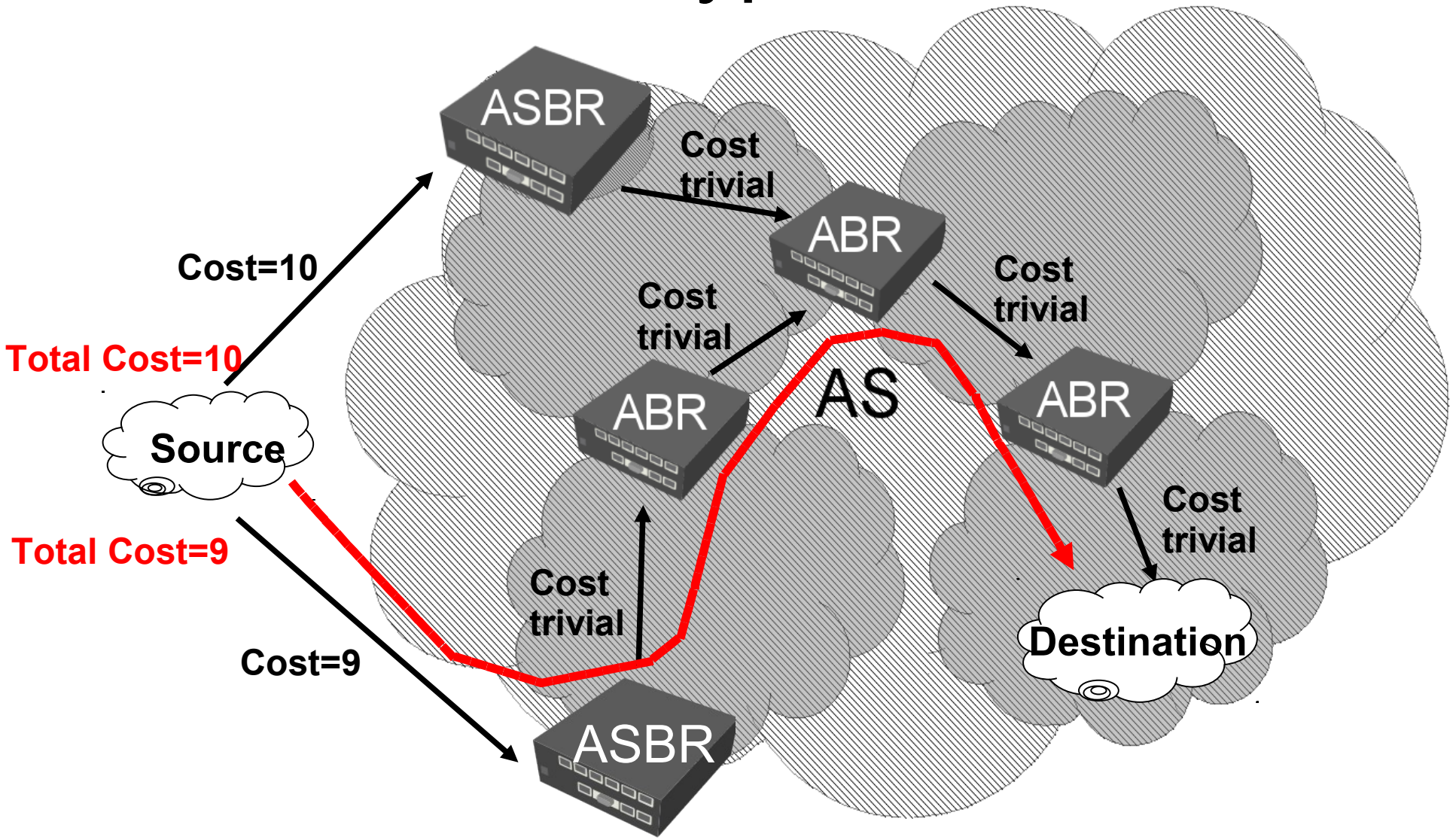
Redistribution Settings

- **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



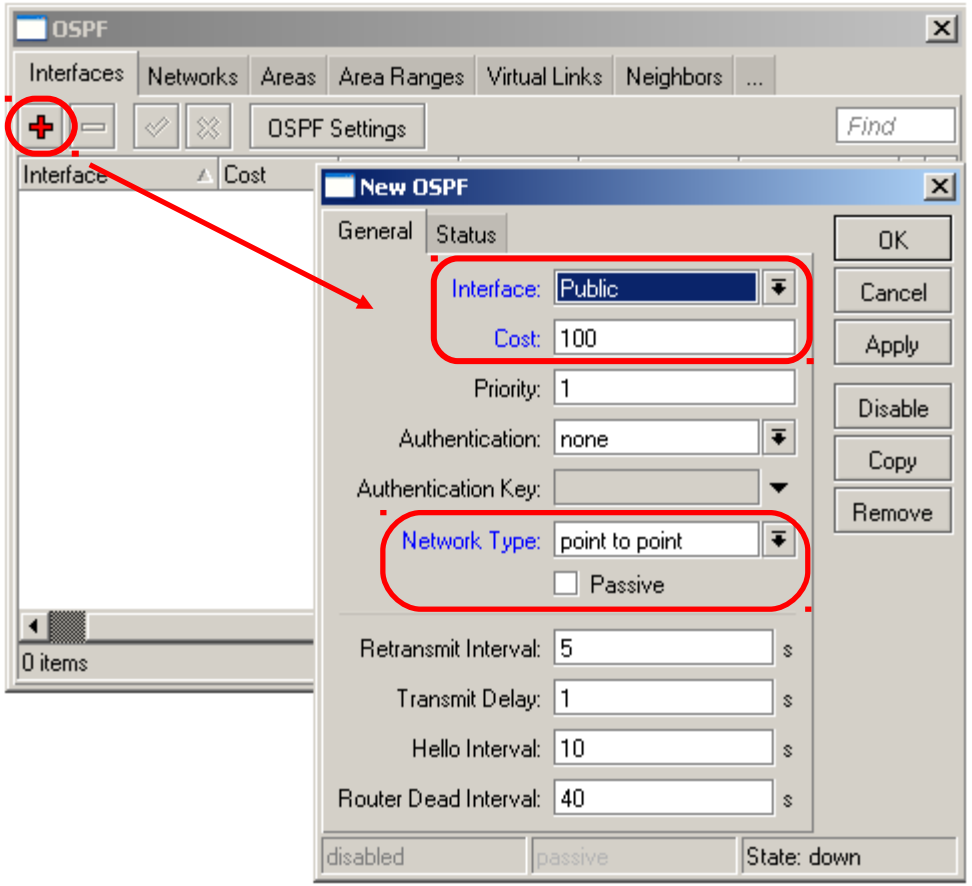
Redistribution Lab

- 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

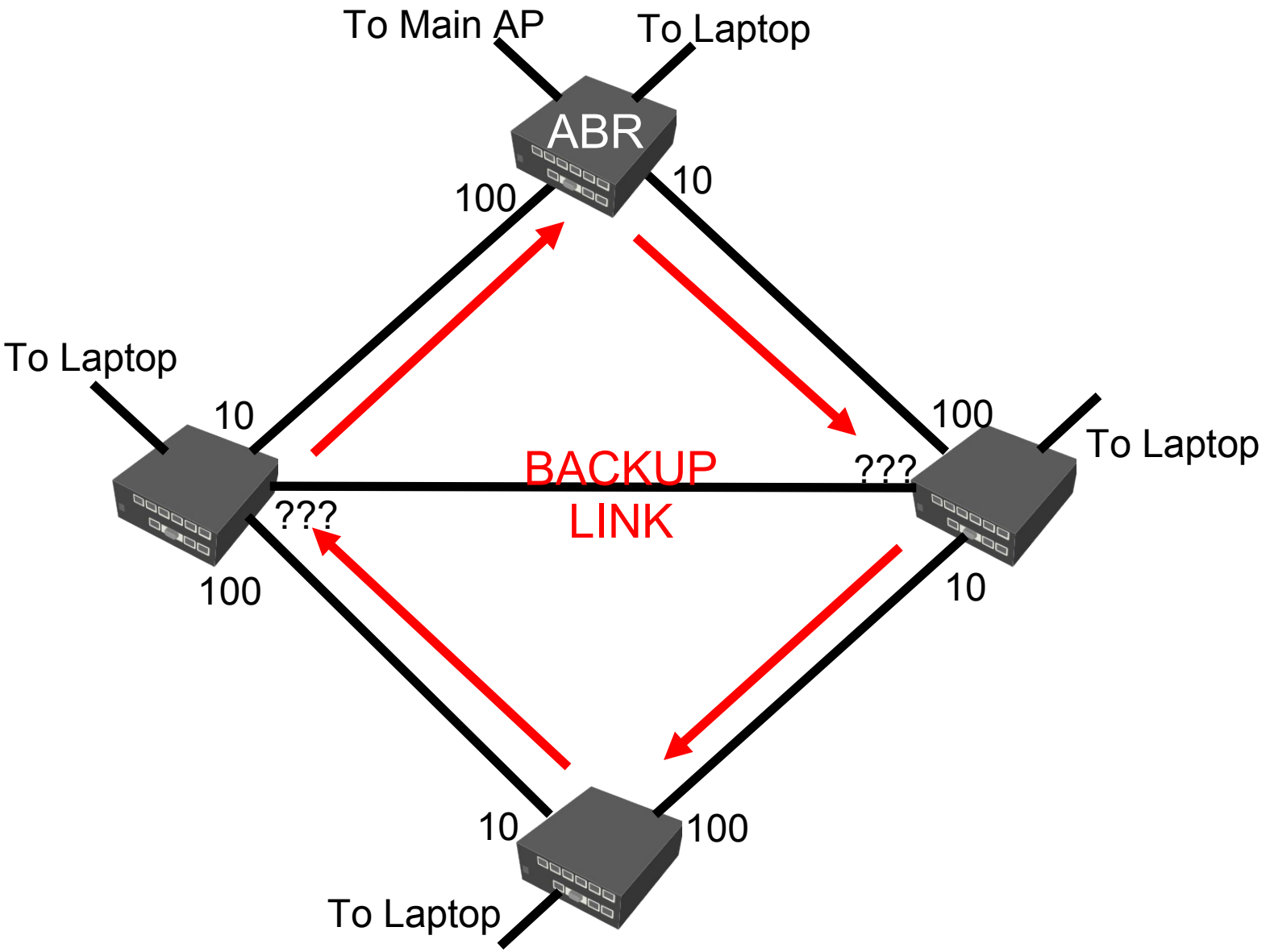
Designated Routers

- 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

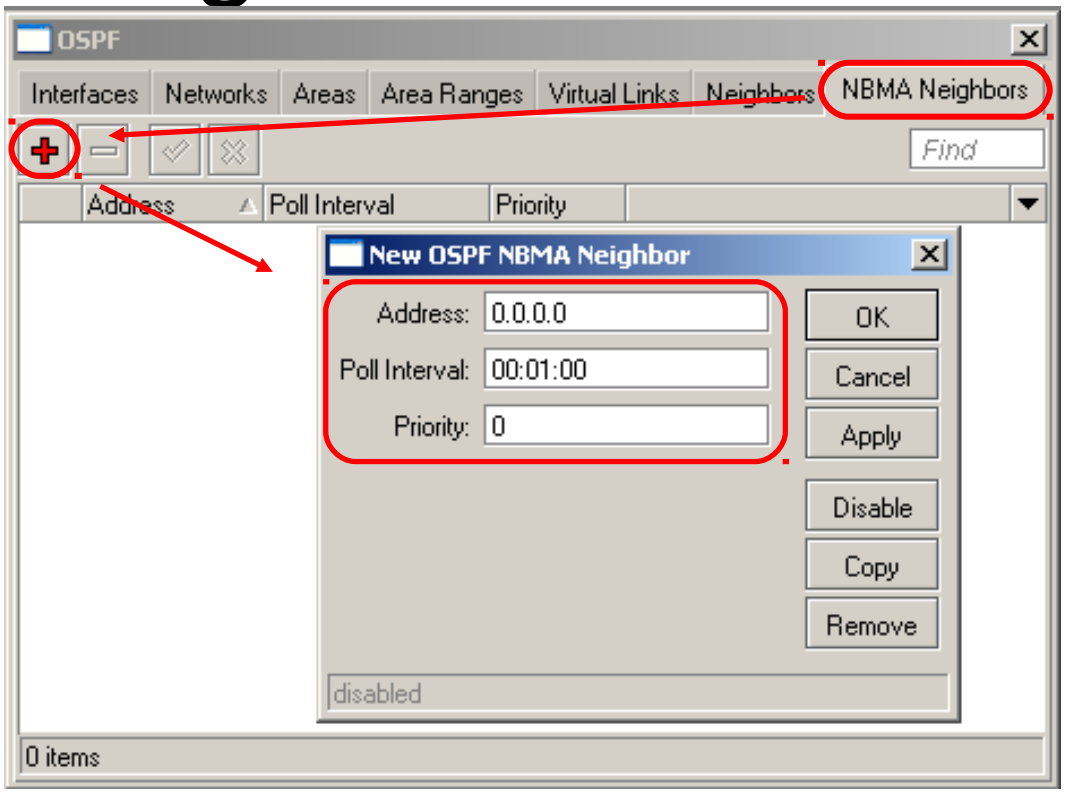
- Choose correct network type for all OSPF interfaces
- Assign costs (next slide) to ensure one way traffic in the area
- Check your routing table for ECMP routes
- Assign necessary costs so backup link will be used only when some other link fails
- Check OSPF network redundancy!
- Ensure ABR to be DR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

Costs


To Main AP
To Laptop
ABR
100
10
To Laptop
10
100
To Laptop
BACKUP
LINK
???
???
100
10
10
100
To Laptop

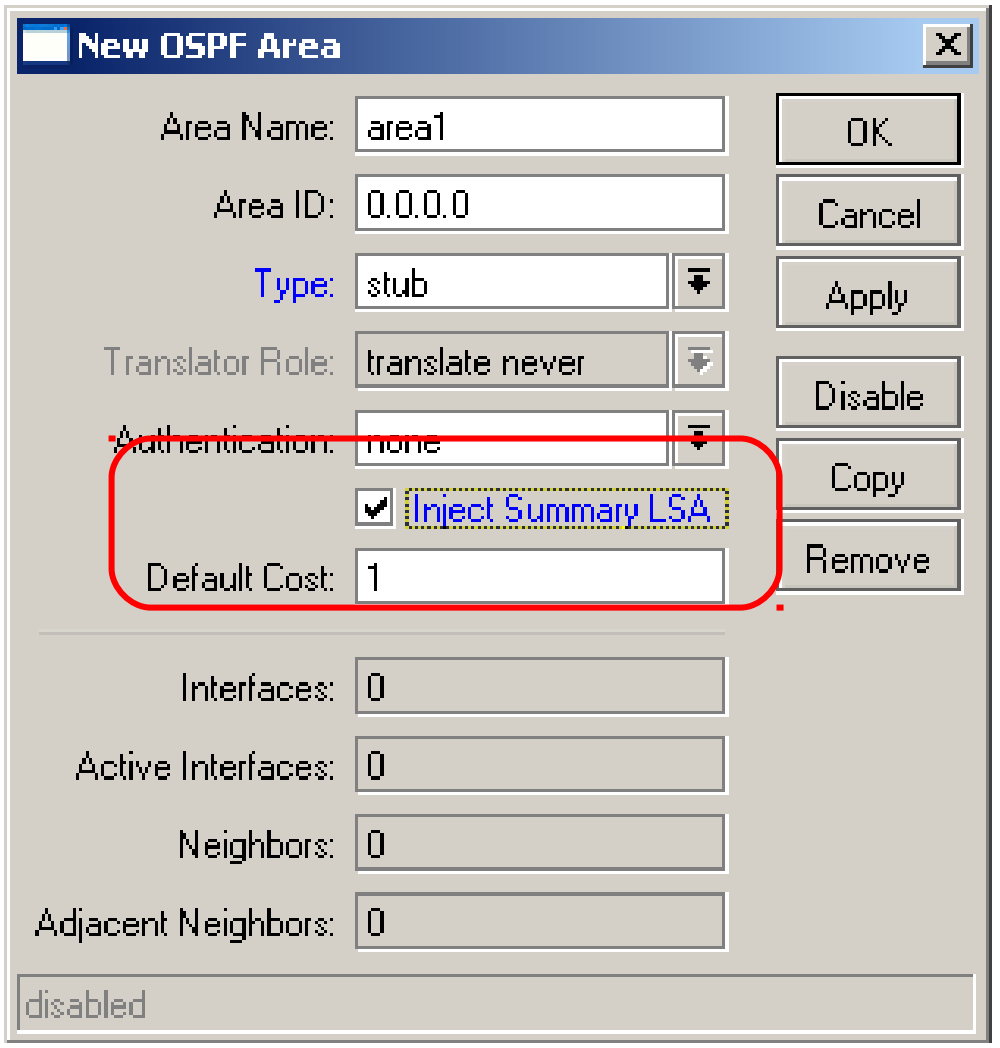
NBMA Neighbors

- 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

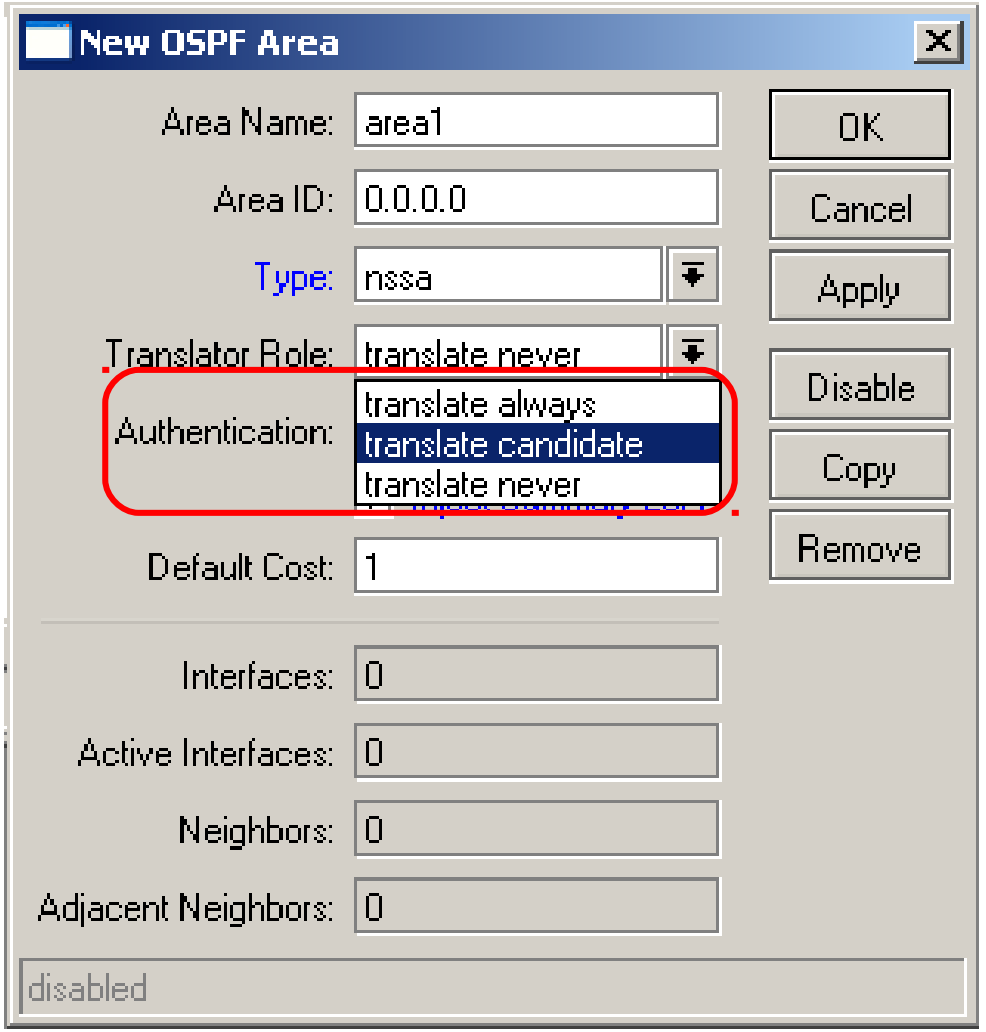


- A stub area is an area which does not receive AS external routes.
- Typically all routes to external AS networks can be replaced by one default route. - this route will be created automatically distributed by ABR

Stub area (2)

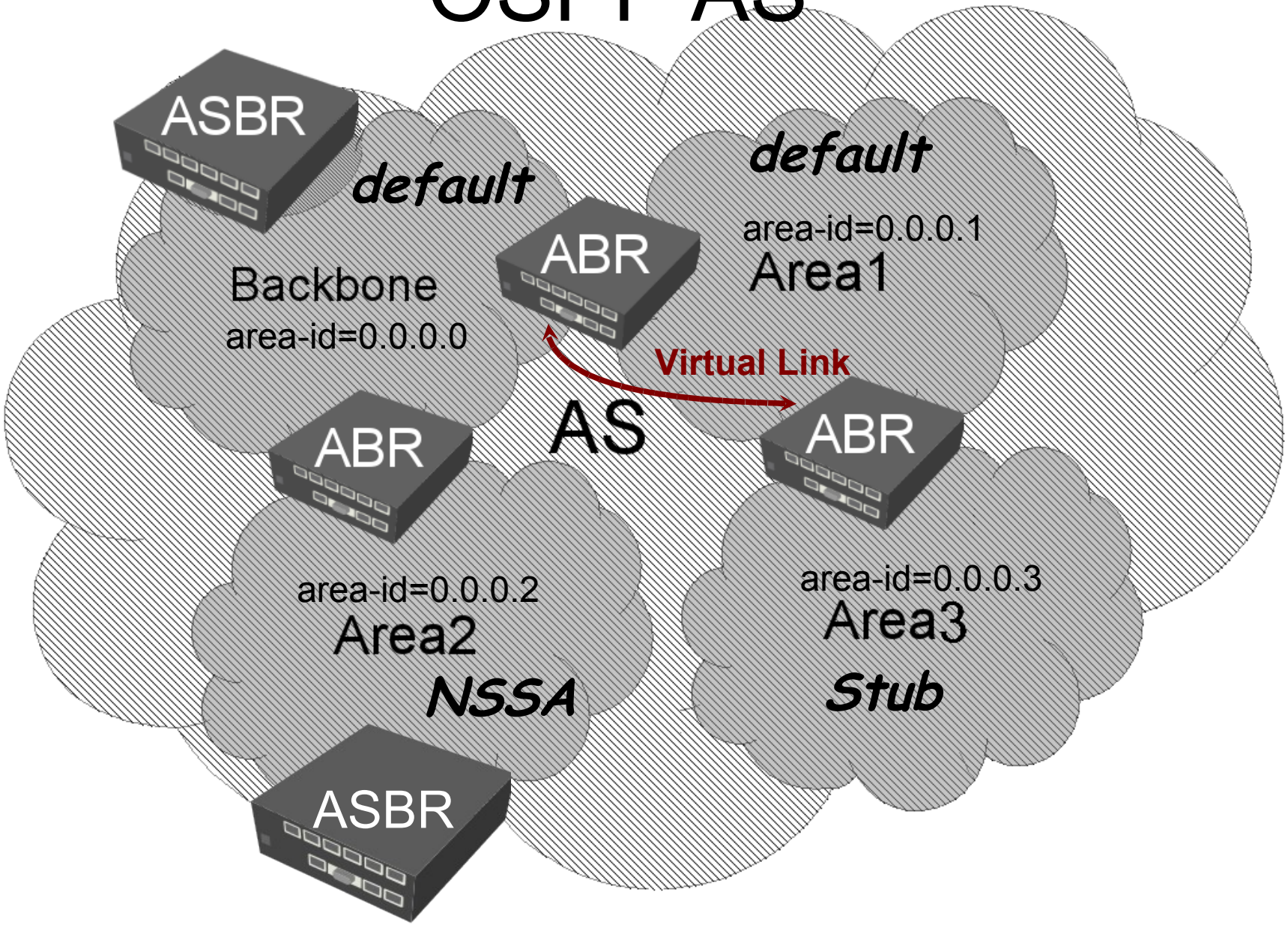
- «Inject Summary LSA» option allows to collect separate backbone or other area router Link State Advertisements (LSA) and inject it to the stub area
- Enable «Inject Summary LSA» option only on ABR
- «Inject Summary LSA» is not a route aggregation
- «Inject Summary LSA» cost is specified by«Default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

Not-So-Stubby Area (NSSA)



- 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


ASBR
default
default
area-id=0.0.0.1
Area1
ABR
Backbone
area-id=0.0.0.0
Virtual Link
AS
ABR
ABR
area-id=0.0.0.2
Area2
NSSA
area-id=0.0.0.3
Area3
Stub
ASBR

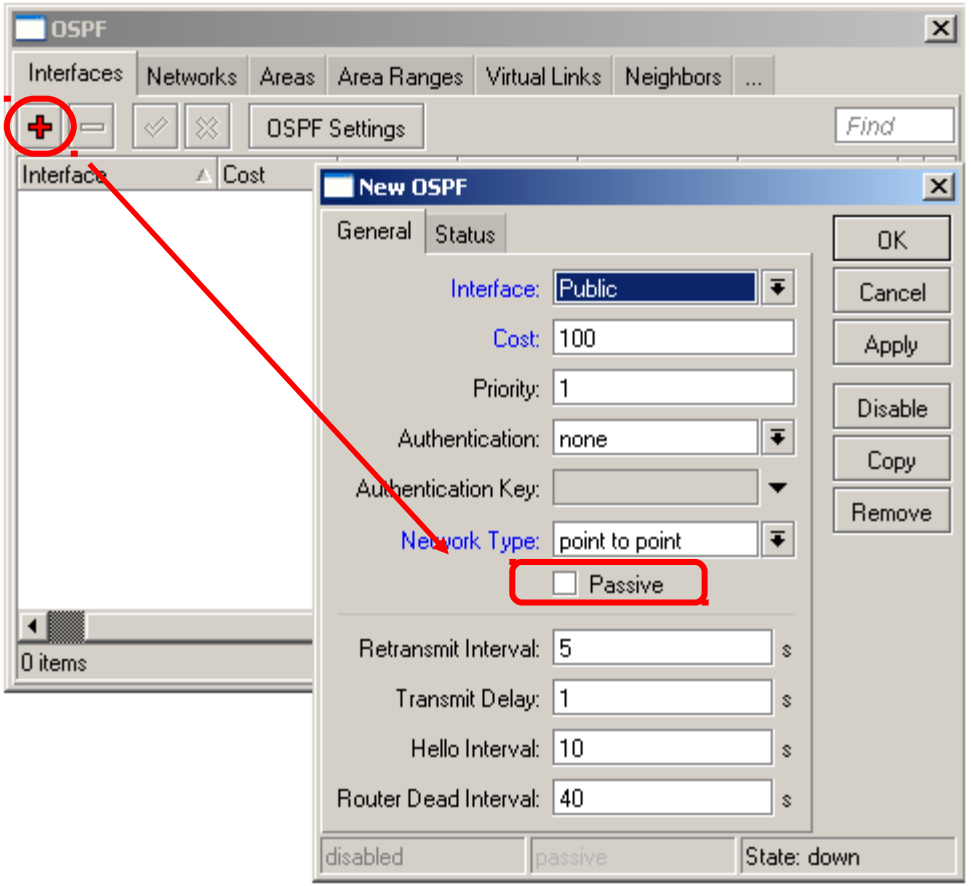
Area Type Lab

- 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

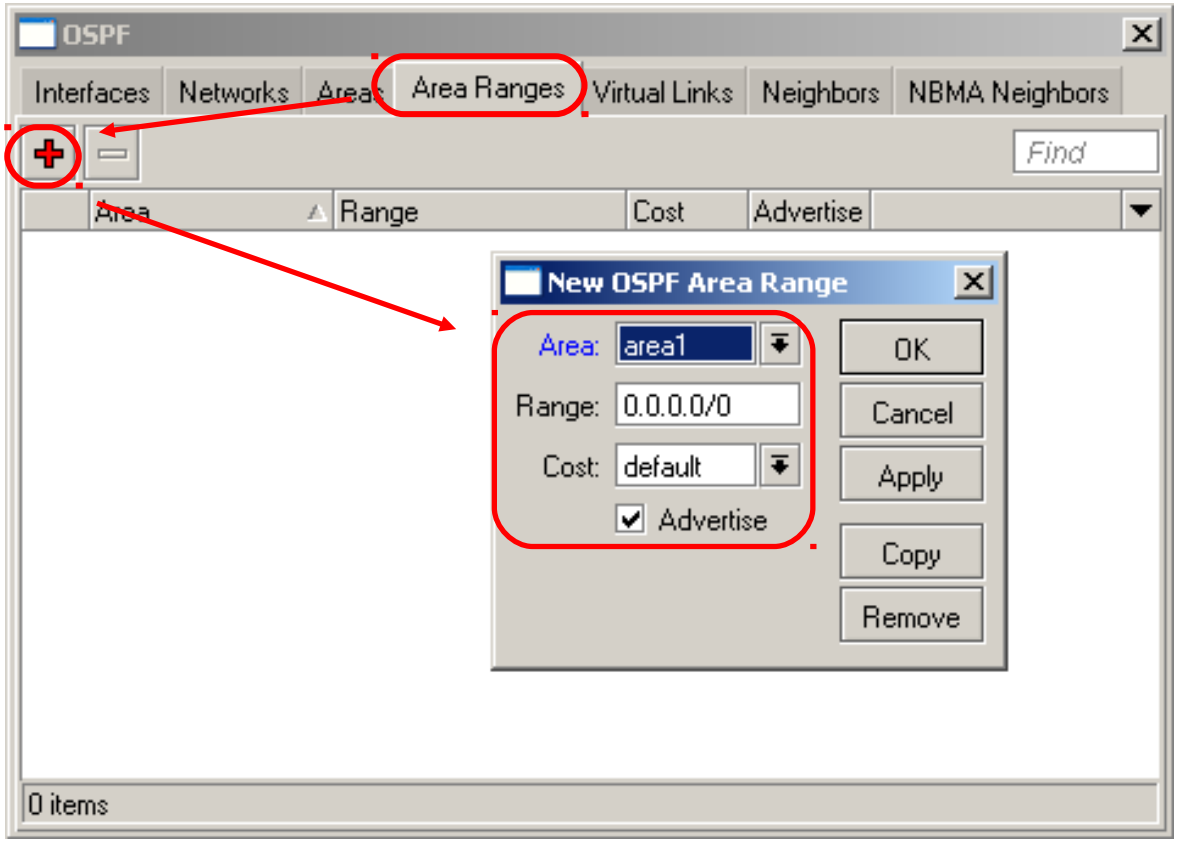


- It is necessary to assign client networks to the area or else stub area will consider those networks as external.
- It is a security issue!!!

- 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 or delete them
- 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

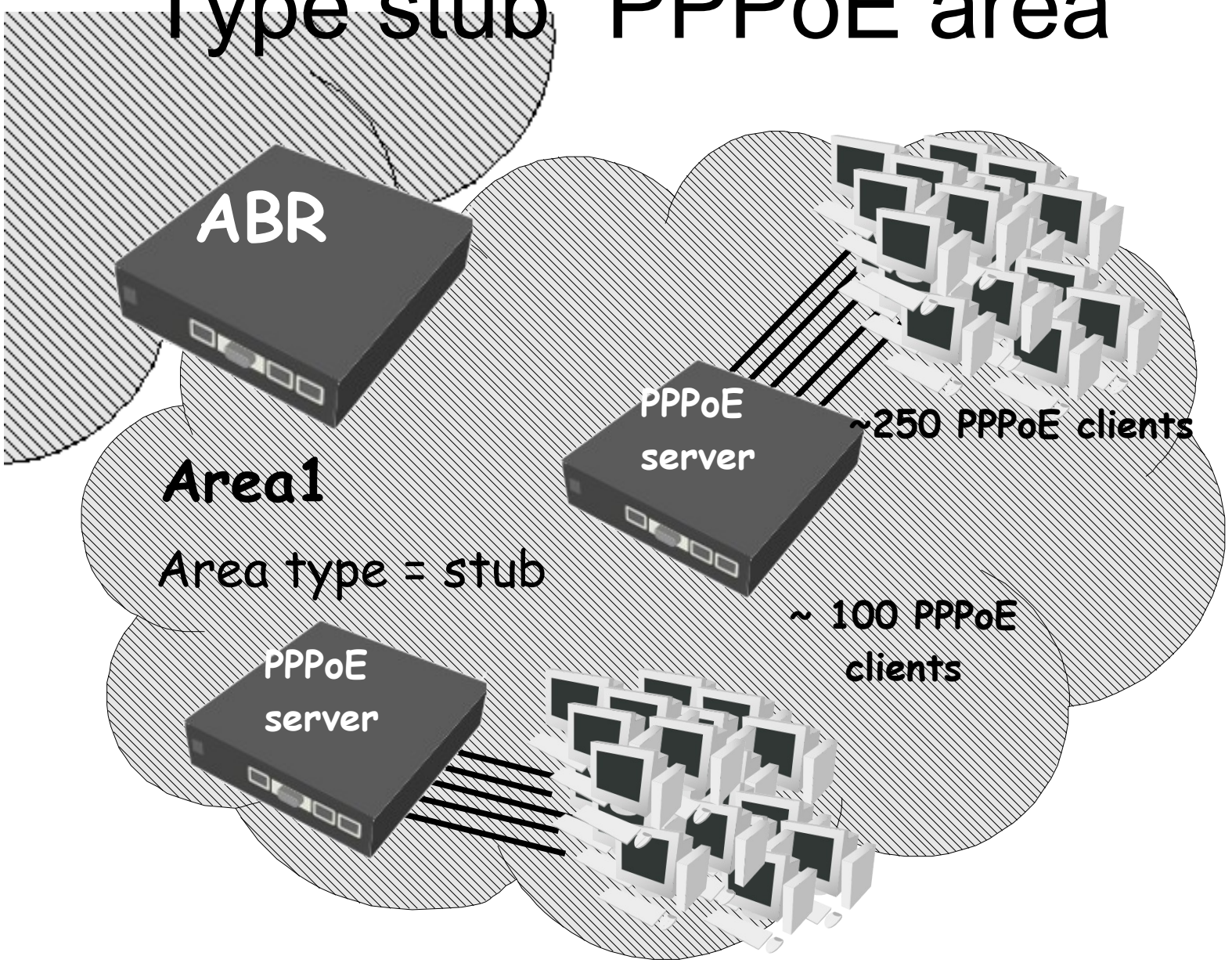
Summary

- 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 route aggregation as much as possible

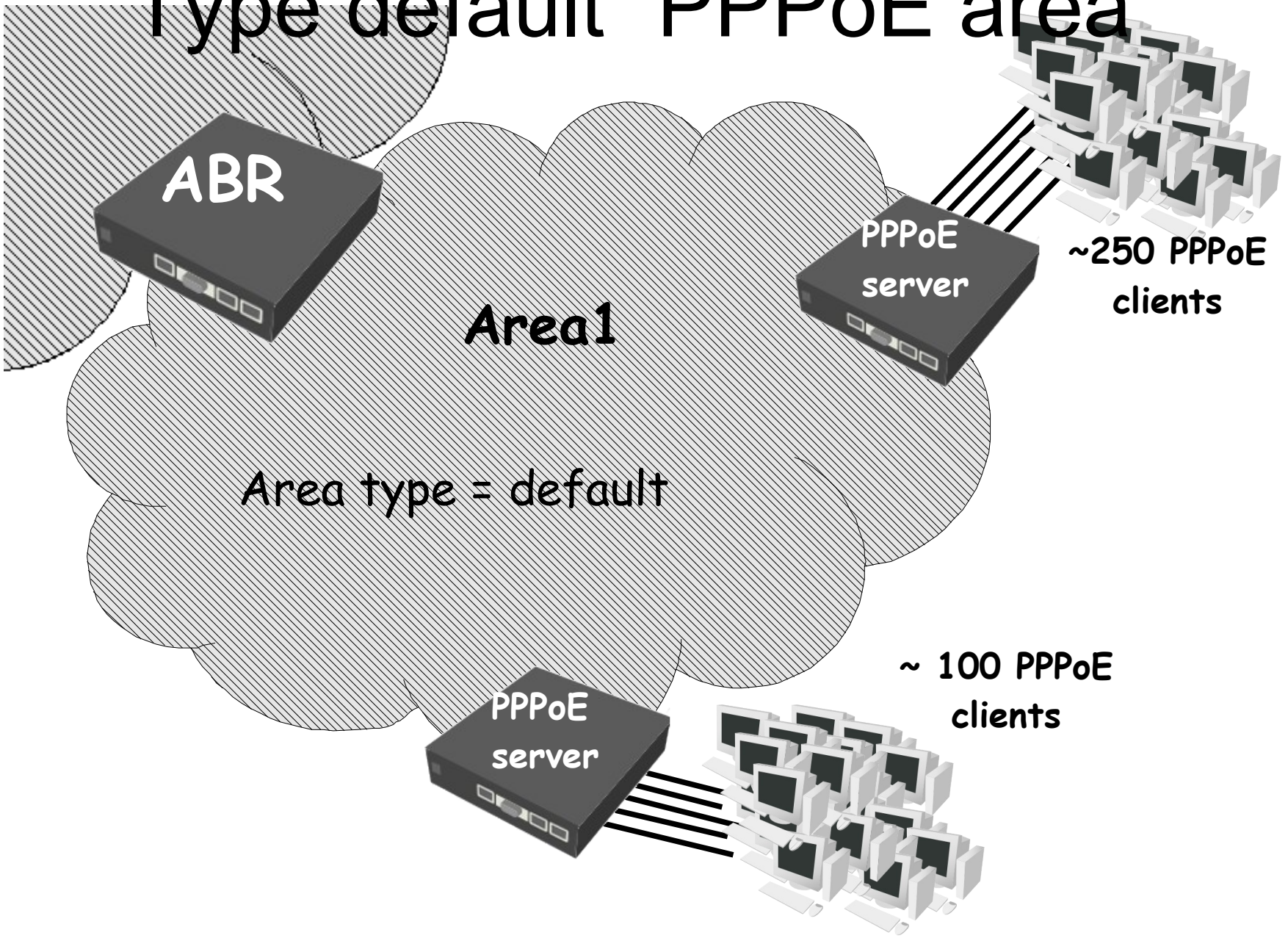
OSPF and Dynamic VPN Interfaces

- 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)

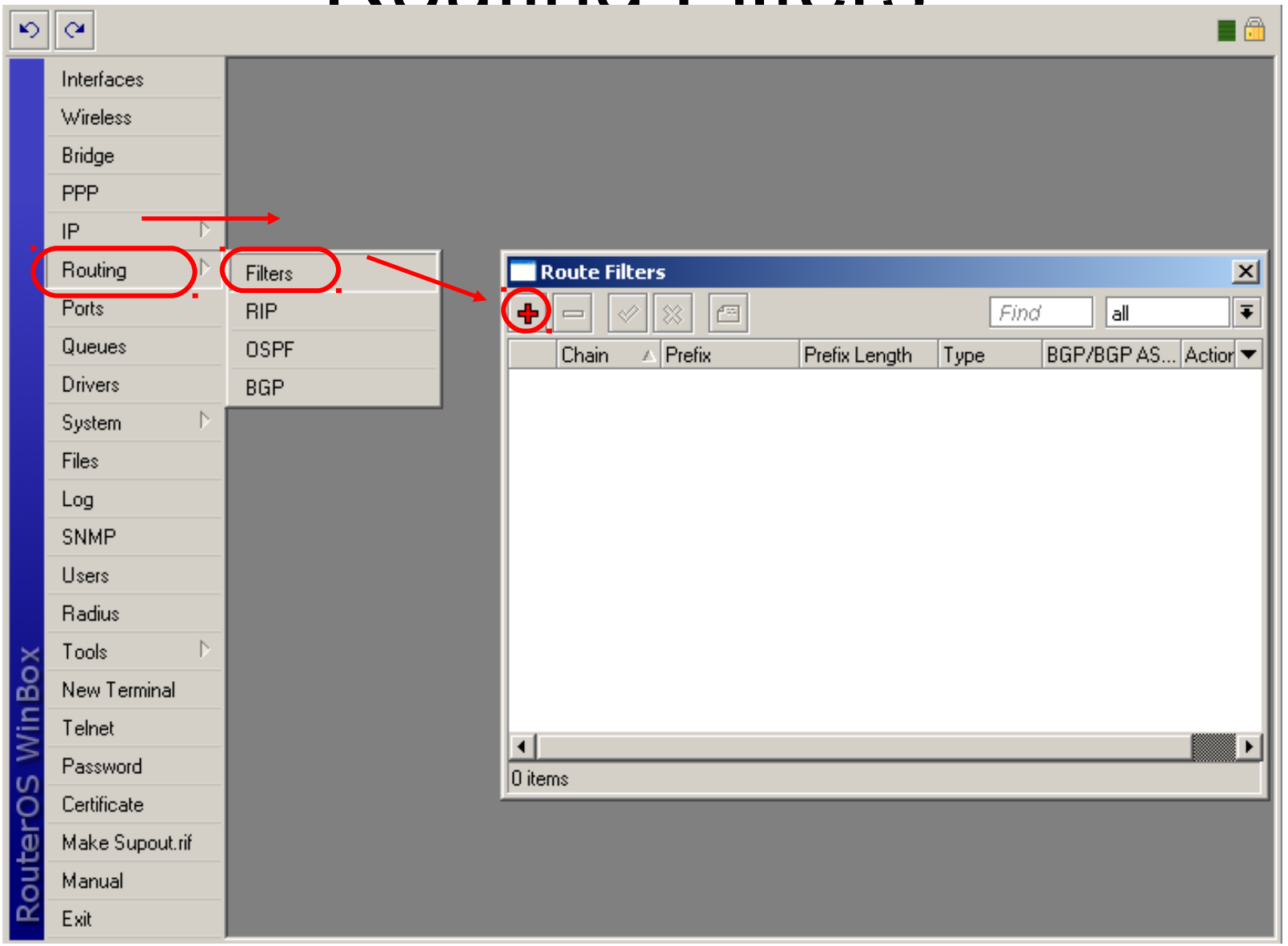
- Give a solution for each problem mentioned previously if used area type is “stub”

- 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)

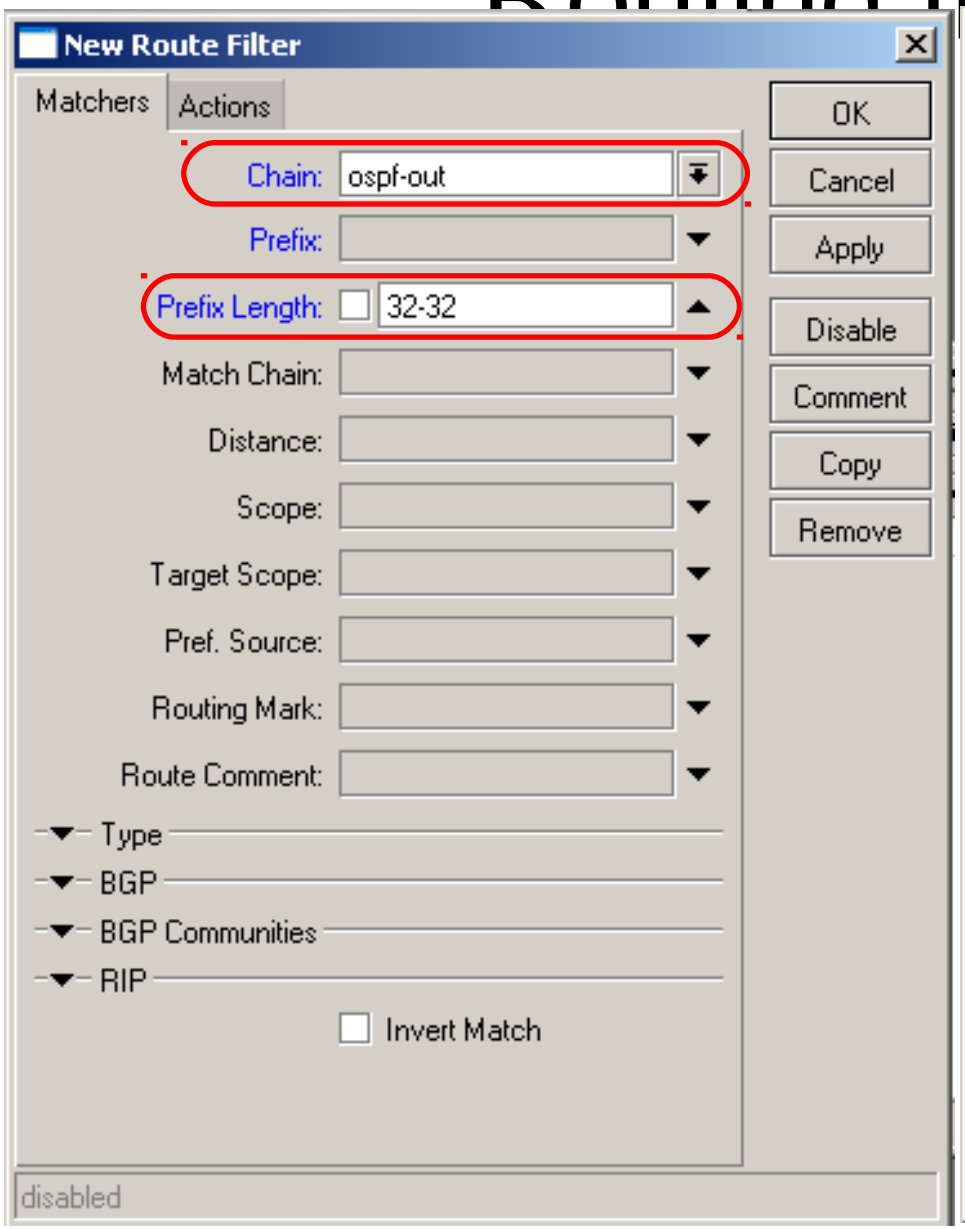
Routing Filters

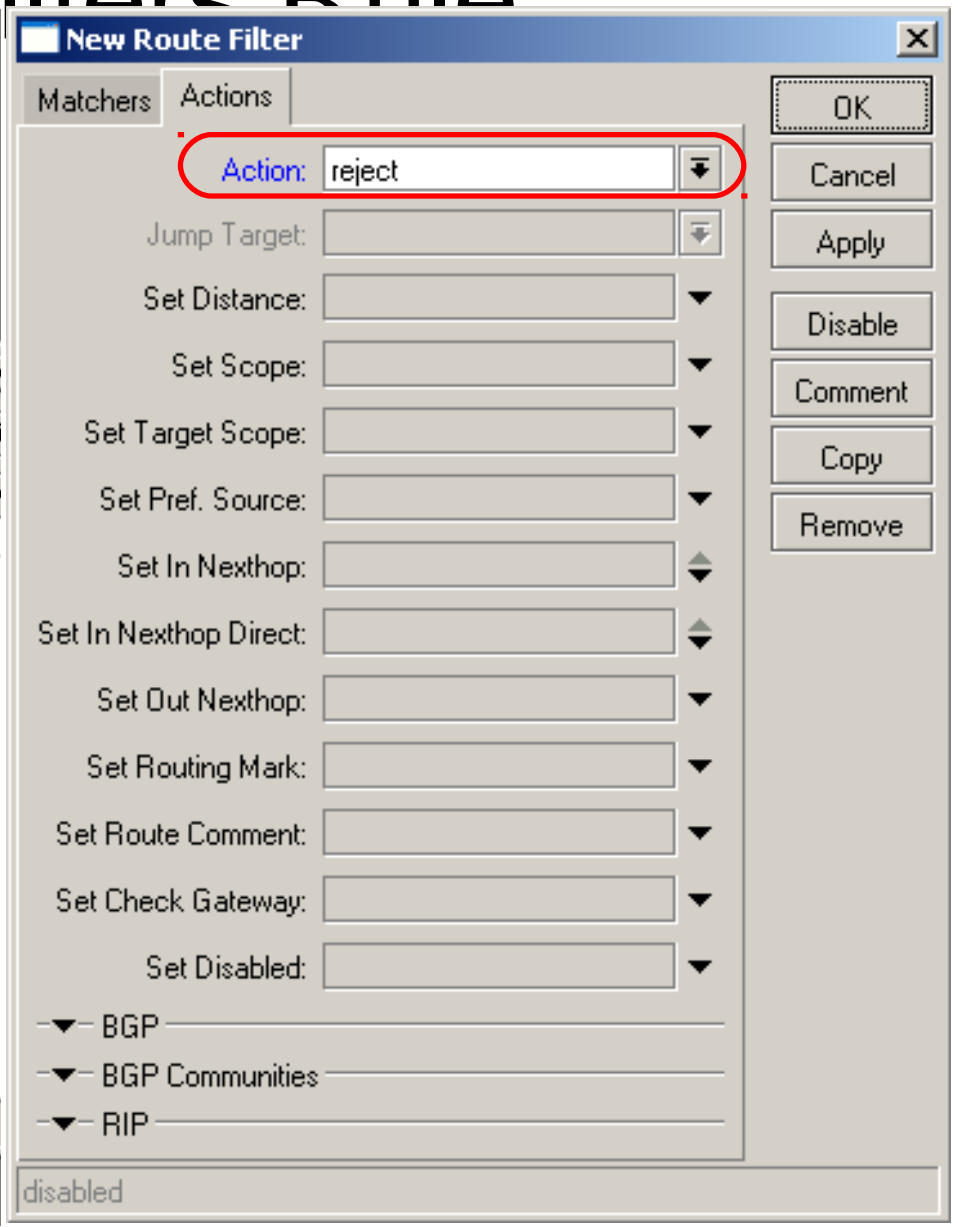


Routing Filters and VPN

- 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





Routing and point-to-point interface

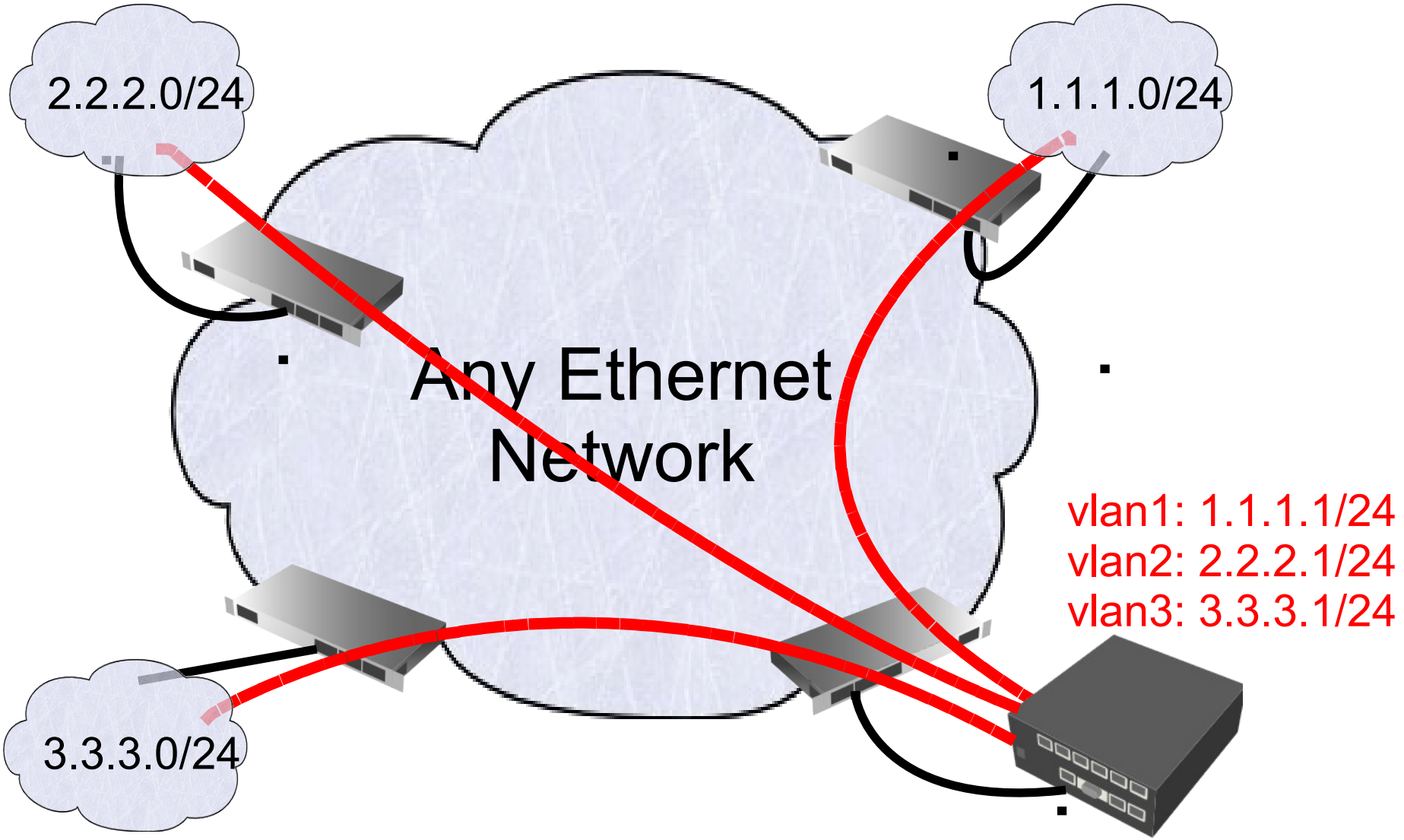
VLAN, IPIP, EOIP,point-to-point addressing

© MikroTik 2008

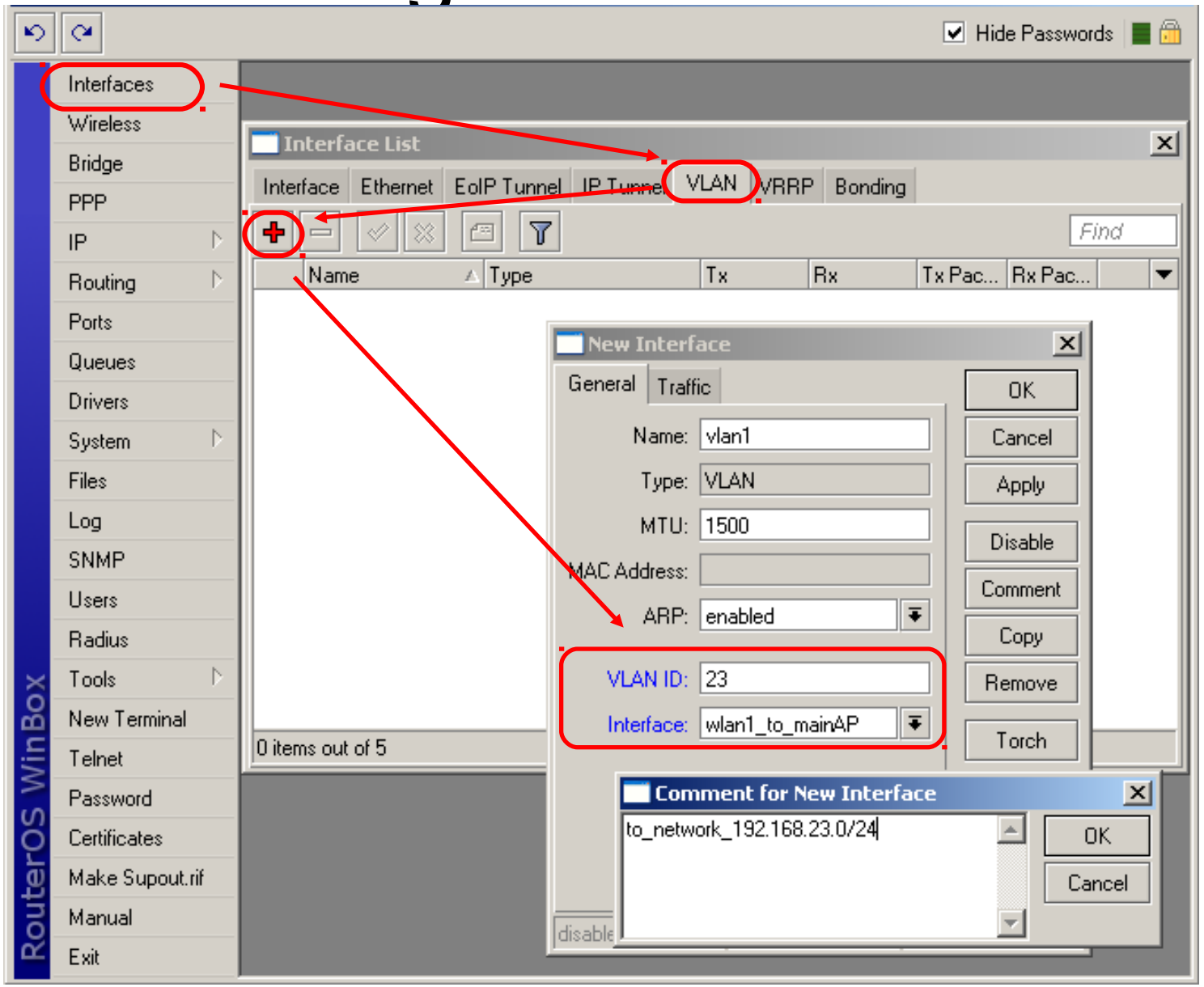
Virtual LAN (802.1Q)

- Virtual LAN (VLAN) allows network devices to be grouped into independent subgroups even if they are located on the same LAN segment
- For routers to communicate the VLAN ID must be the same for VLAN interfaces
- Ports on the router supports multiple (up to 250) Virtual LANs on a single ethernet interface
- VLAN can be configurated over other VLAN interface - “Q-in-Q” (from 802.1**Q**)

VLAN Example



Creating VLAN Interface



VLAN on Switch

- VLAN-compliant switch ports can be assigned to one or several groups based on VLAN tag
- Switch port in each group can be set to
  - Tagged mode – allows to add group's VLAN tag on transmit and allows to receive frames with this tag
  - Untagged mode – allows to remove this group VLAN tag on transmit, and allows to receive only untagged packets
  - <Undefined> – port have no relation to this group
- Trunk port - tagged port for several VLAN groups

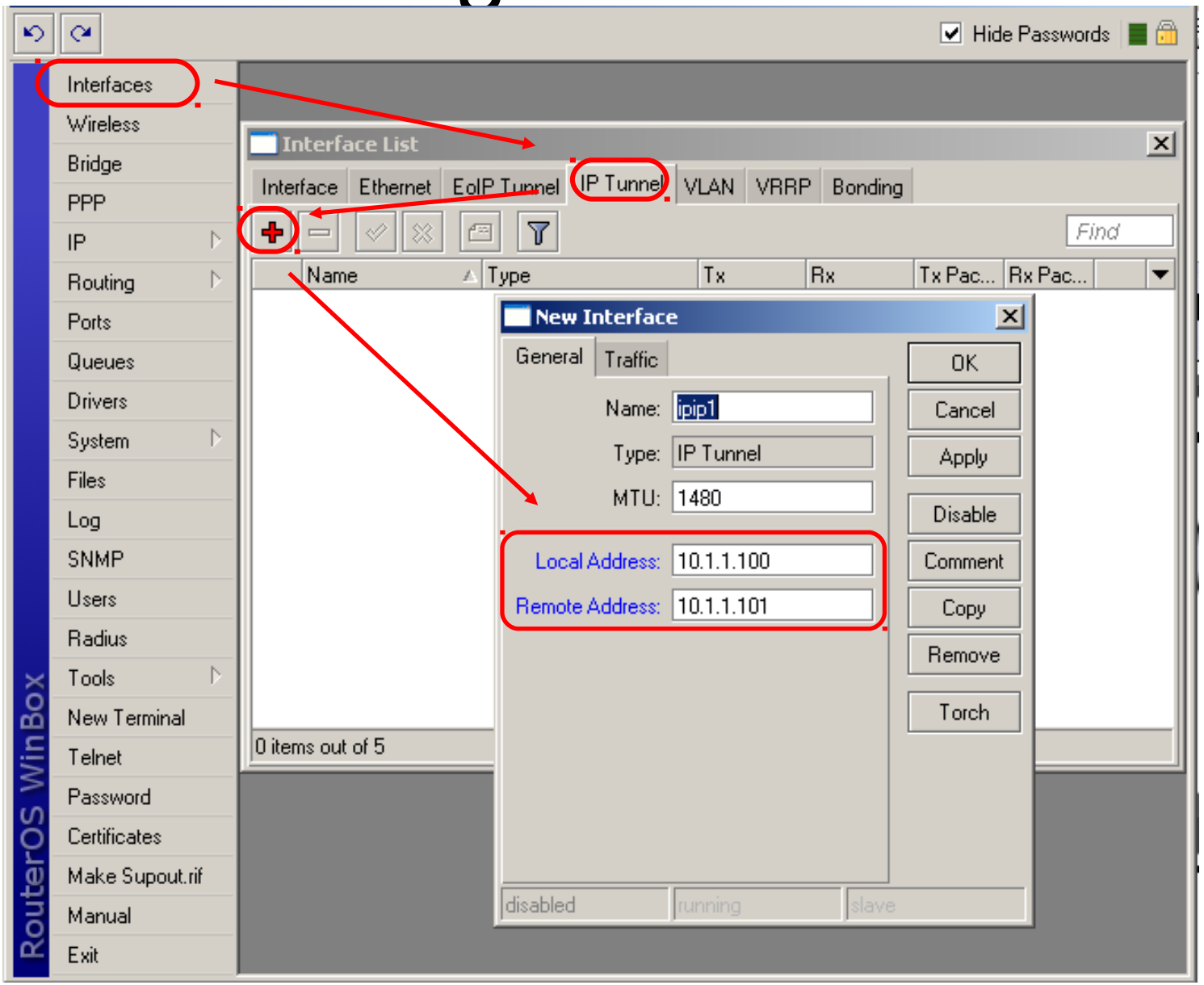
VLAN Lab

- Restore default backup
- Create the group of 4
- Connect together using wireless - one AP, 3 clients
- Create VLAN link to each participant
- Assign /30 networks to VLAN links and check them

IPIP

- IP protocol 4/IPIP allows to create tunnel by encapsulating IP packets in IP packets and sending over to another router
- IPIP is Layer-3 tunnel – it can not be bridged
- RouterOS implements IPIP tunnels according to RFC 2003 – it should be compatible with other vendor IPIP implementations
- To create a tunnel you must specify address of the local and remote router on both sides of the tunnel

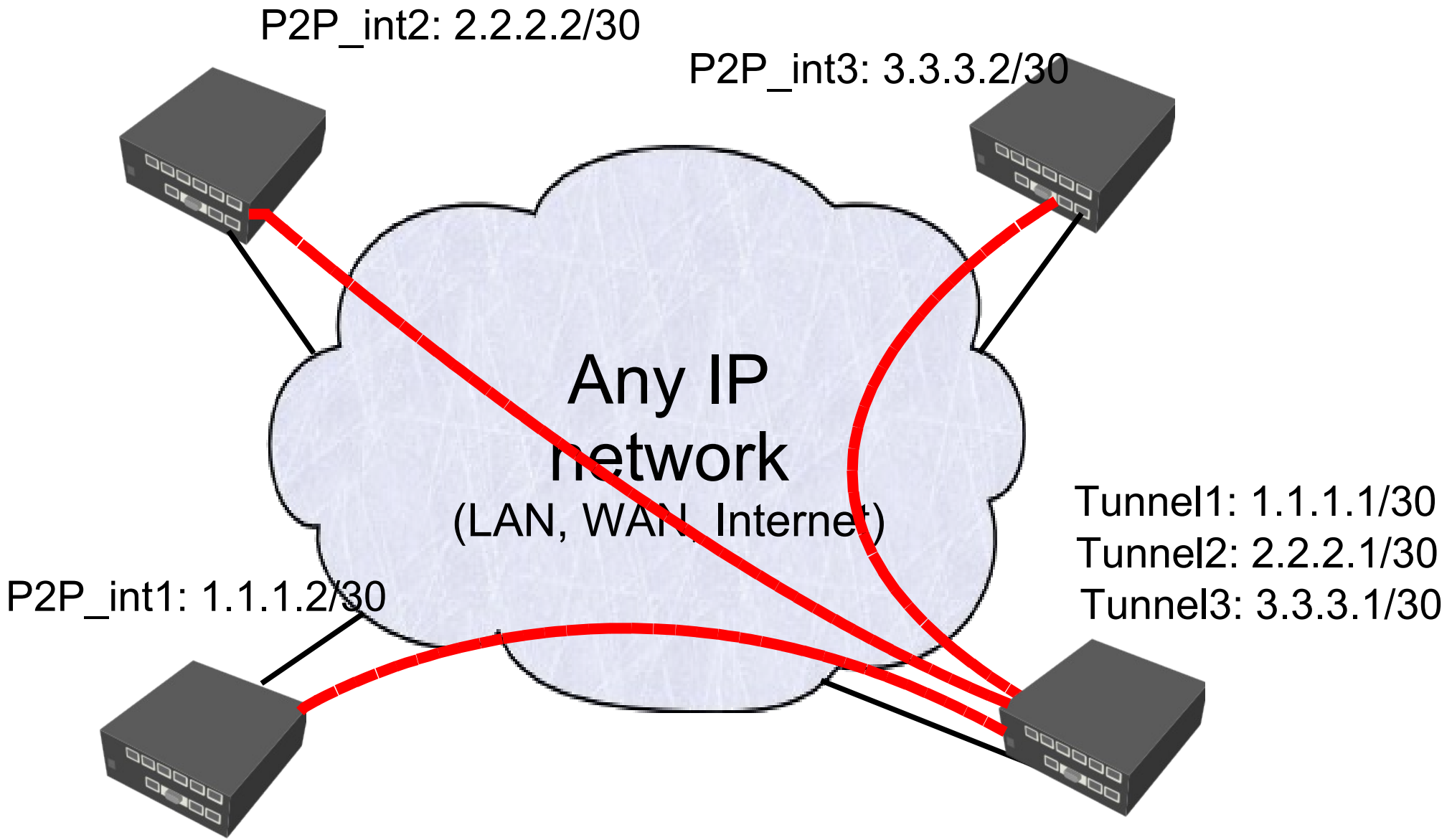
Creating IPIP Interface



IPIP Lab

- Replace all VLANs (from previous lab) with IPIP tunnels
- Check that you are able to ping remote address before creating a tunnel to it
- Assign /30 IP addresses (from previous lab) to IPIP interfaces and check all tunnels

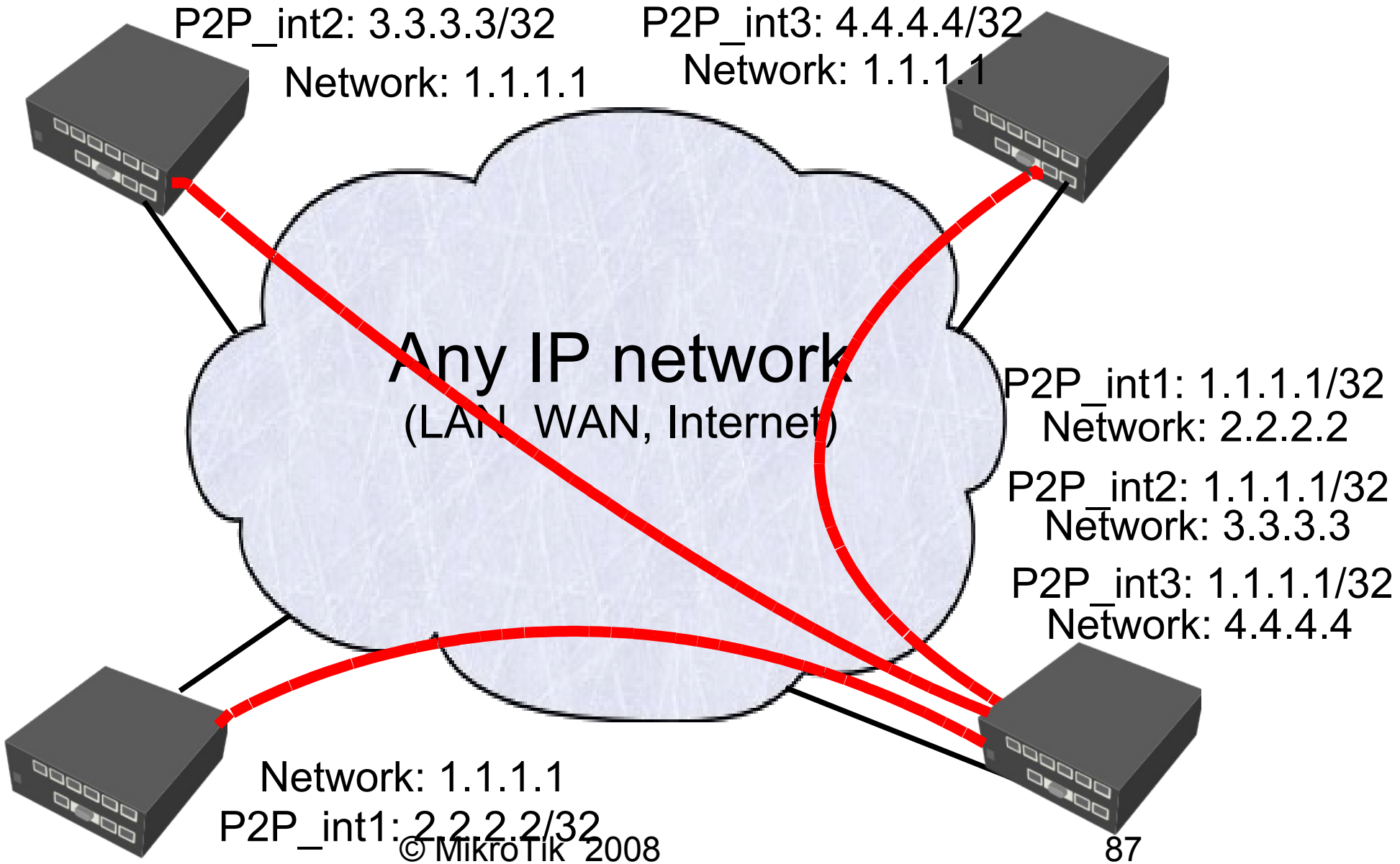
/30 Addressing



Point-to-point Addressing

- Point-to-point addressing utilizes only two IPs per link while /30 utilizes four IPs
- There is no broadcast address, but network address must be set manually to the opposite IP address. Example:
  - Router1: address=1.1.1.1/32, network=2.2.2.2
  - Router2: address=2.2.2.2/32, network=1.1.1.1
- There can be identical /32 addresses on the router – each address will have different connected route

Point-to-point Addressing



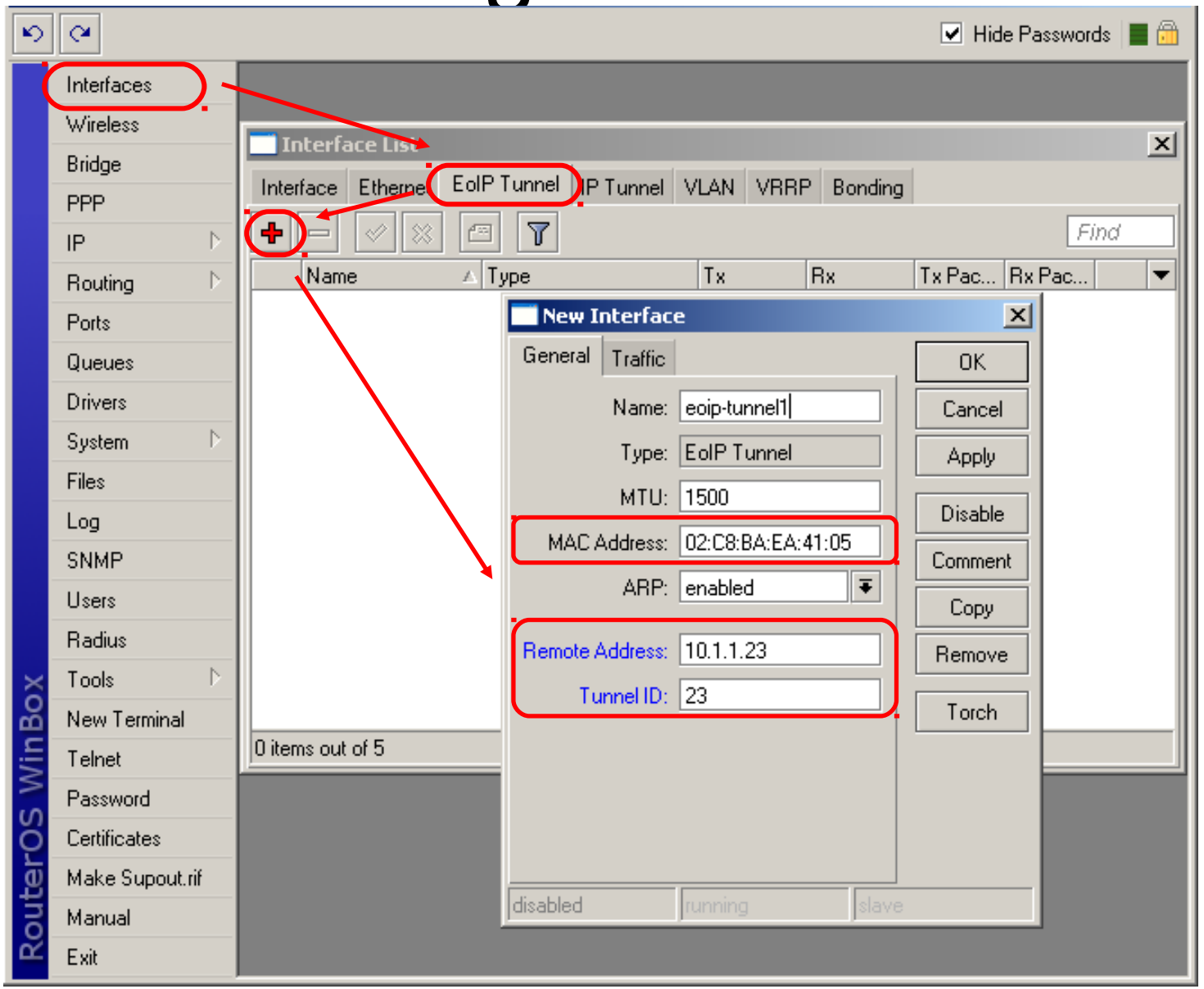
Addressing Lab

- Replace all /30 addresses on IPIP interfaces (from previous lab) with /32 point-to-point addresses.
- Ensure that every other participant will be able to ping you by IP address XY.XY.XY.XY via all IPIP tunnels
- Analyse how much IP addresses were utilized on IPIP tunnels for whole group setup!

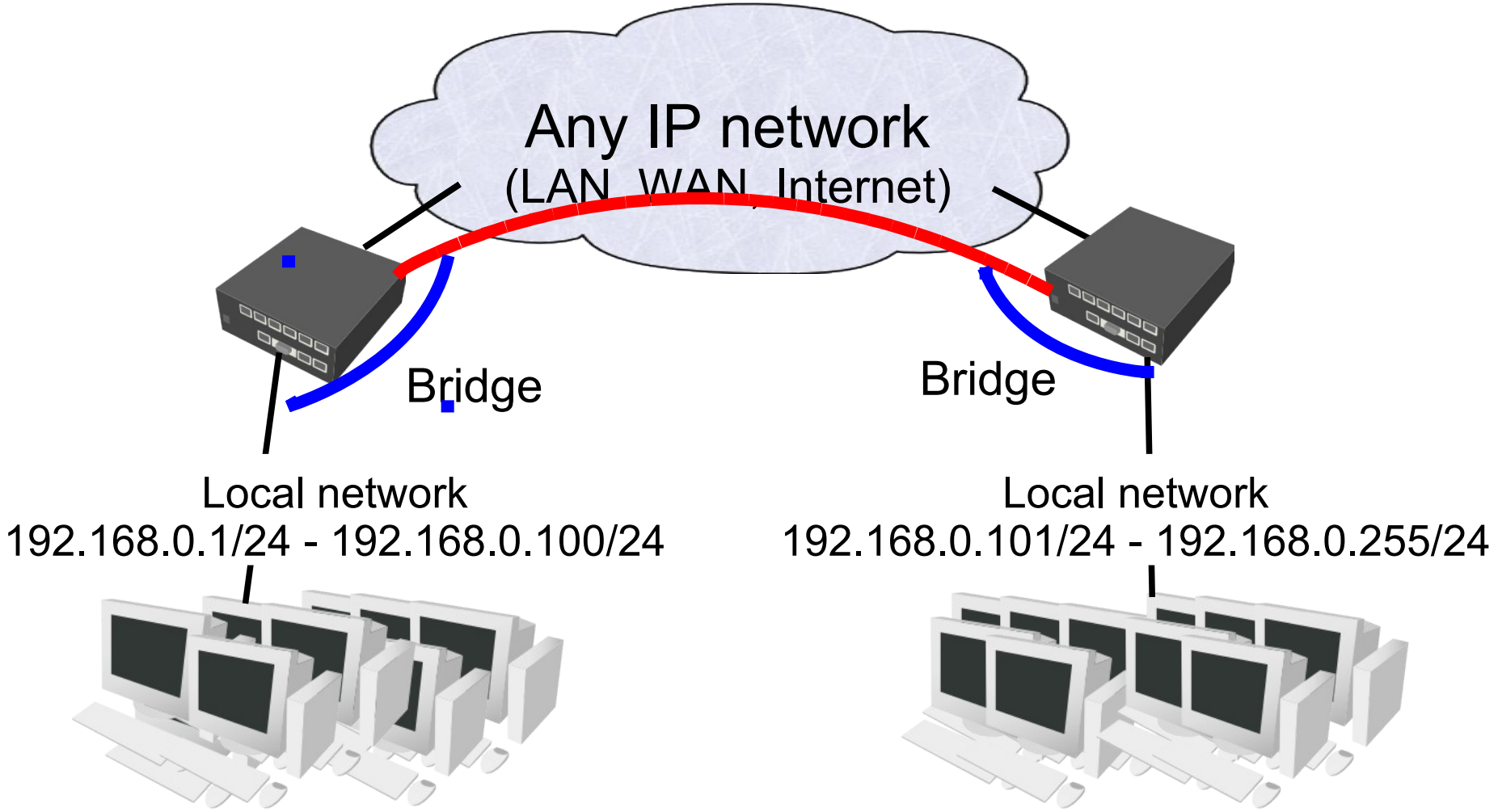
Ethernet Over IP (EOIP) Tunnel

- IP protocol 47/GRE allows to create tunnel by encapsulating Ethernet frames in IP packets and sending over to another router
- MikroTik proprietary protocol
- EOIP is Layer-2 tunnel – it can be bridged
- To create a tunnel you must specify remote router's address and choose unique Tunnel ID
- Check that your EOIP interface have different MAC-address than on opposite side.

Creating EoIP Tunnel



EOIP and Bridging



EoIP Lab

- Replace all IPIP tunnels (from previous lab) with EOIP tunnels
- Check that you are able to ping remote address before creating a tunnel to it
- Bridge all EoIP interfaces with local interface
- Check Winbox Loader neighbour discovery feature (“...” button)