

MikroTik RouterOS Training Class

MTCNA

May 4-8 2013
Qom, IRAN

NikanNetwork

<http://www.nikannetwork.com>

Vahid Shahbazian

www.LearnMikroTik.ir

Schedule

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

2

Course Objective

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

3

About MikroTik

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

4

MikroTik's History

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

5

Where is MikroTik?

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

6

Where is MikroTik ?



7

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.

8

MikroTik RouterOS

9

What is RouterOS ?

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

10

What is RouterOS ?

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

11

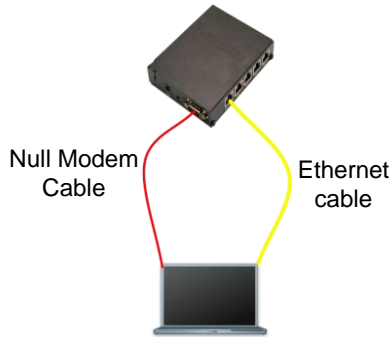
What is RouterBOARD?

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



12

First Time Access



13

Winbox

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

14

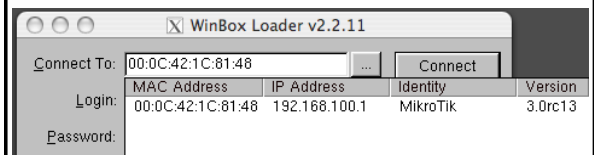
Download Winbox



15

Connecting

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



16

Communication

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

17

Application

Presentation

Session

Transport

Network

Data Link

Physical

18

MAC address

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

19

IP

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

20

Subnets

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

21

Subnets

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

22

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

23

Selecting IP address

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

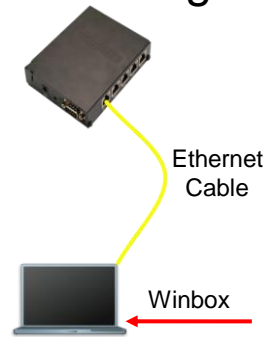
24

Selecting IP address Example

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

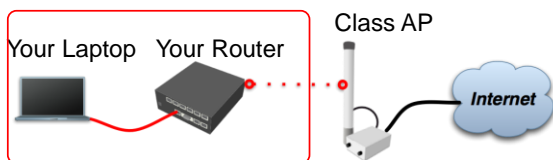
25

Connecting



26

Diagram



27

Laptop - Router

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

28

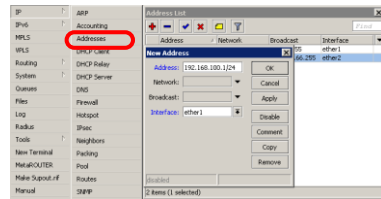
Connecting Lab

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

29

Laptop - Router

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



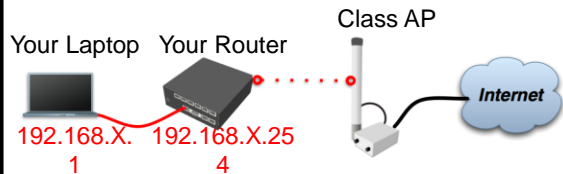
30

Laptop - Router

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

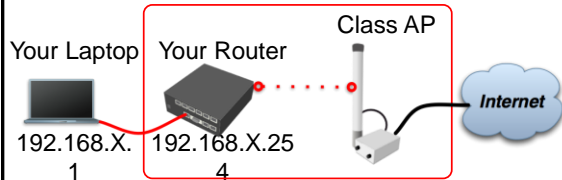
31

Laptop Router Diagram



32

Router Internet



33

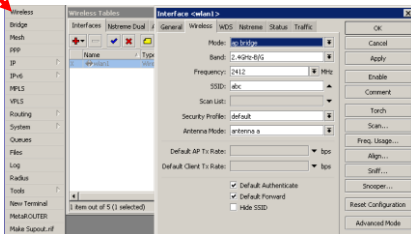
Router - Internet

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

34

Router - Internet

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



35

Router - Internet

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

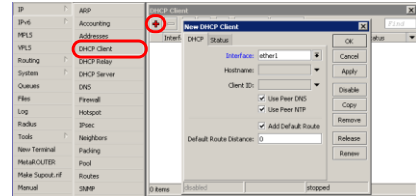
36

Router - Internet

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

37

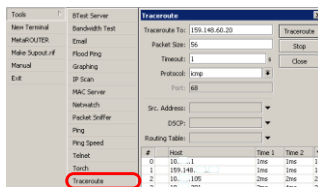
Router - Internet



38

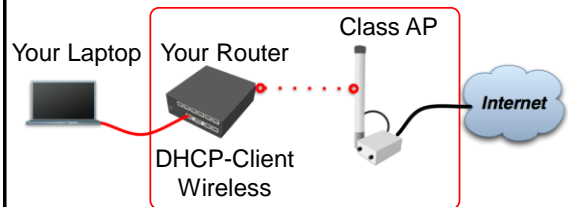
Router - Internet

Check Internet connectivity by traceroute



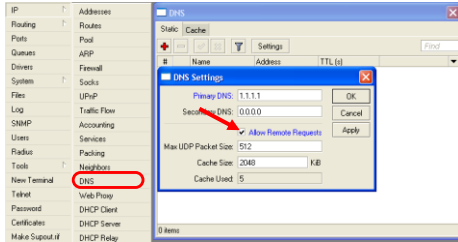
39

Router Internet



40

Laptop - Internet



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

41

Laptop - Internet

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

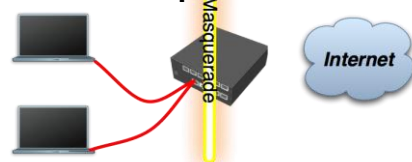
42

Laptop - Internet

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

43

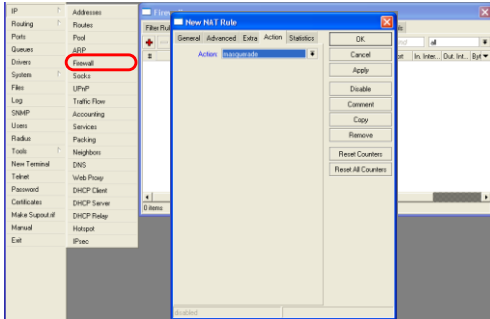
Private and Public space



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

44

Laptop - Internet



45

Check Connectivity

Ping www.mikrotik.com from your laptop

```
Terminal - sh - 65x13
sh-3.2# ping www.mikrotik.com
PING mikrotik.com (174.36.189.131): 56 data bytes
64 bytes from 174.36.189.131: icmp_seq=0 ttl=40 time=217.852 ms
64 bytes from 174.36.189.131: icmp_seq=1 ttl=40 time=211.590 ms
64 bytes from 174.36.189.131: icmp_seq=2 ttl=40 time=211.662 ms
64 bytes from 174.36.189.131: icmp_seq=3 ttl=40 time=212.467 ms
64 bytes from 174.36.189.131: icmp_seq=4 ttl=40 time=211.044 ms
64 bytes from 174.36.189.131: icmp_seq=5 ttl=40 time=211.165 ms
^C
--- mikrotik.com ping statistics ---
6 packets transmitted, 6 packets received, 0% packet loss
round-trip min/avg/max/stddev = 211.044/212.630/217.852/2.380 ms
sh-3.2#
```

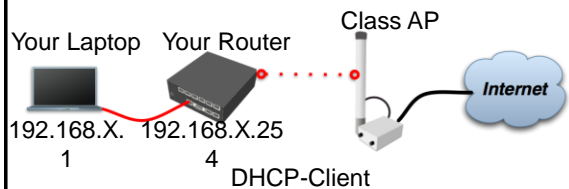
46

What Can Be Wrong

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

47

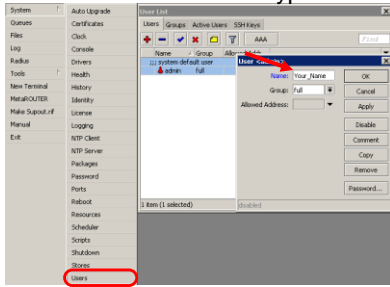
Network Diagram



48

User Management

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



49

User Management Lab

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

50

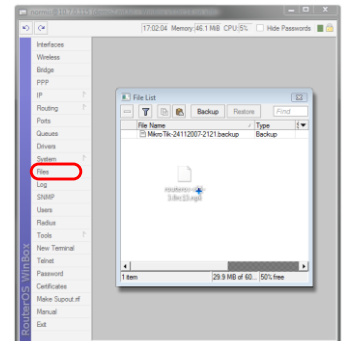
Upgrading Router Lab

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

51

Upgrading Router

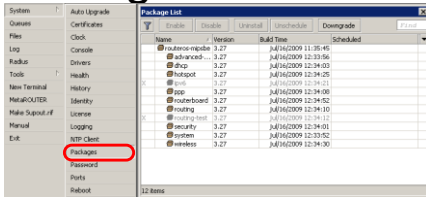
- Use combined RouterOS package
- Drag it to the Files window



52

Package Management

RouterOS functions are enabled by packages



53

Package Information

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

54

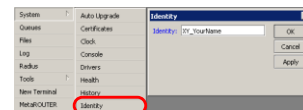
Package Lab

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

55

Router Identity

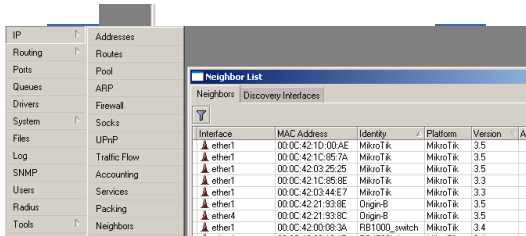
Option to set name for each router



56

Router Identity

Identity information is shown in different places



| Interface | MAC Address | Identity | Platform | Version | Age |
|-----------|-------------------|---------------|----------|---------|-----|
| ether1 | 00:0C:42:1D:00:A2 | MikroTik | MikroTik | 3.5 | |
| ether1 | 00:0C:42:1C:85:7A | MikroTik | MikroTik | 3.5 | |
| ether1 | 00:0C:42:03:25:25 | MikroTik | MikroTik | 3.5 | |
| ether1 | 00:0C:42:1C:85:8E | MikroTik | MikroTik | 3.3 | |
| ether1 | 00:0C:42:03:44:E7 | MikroTik | MikroTik | 3.3 | |
| ether1 | 00:0C:42:21:93:9E | Origin-B | MikroTik | 3.5 | |
| ether4 | 00:0C:42:21:93:8C | Origin-B | MikroTik | 3.5 | |
| ether1 | 00:0C:42:00:08:3A | RB1000_switch | MikroTik | 3.4 | |

57

Router Identity Lab

Set your number + your name as router identity

58

NTP

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

59

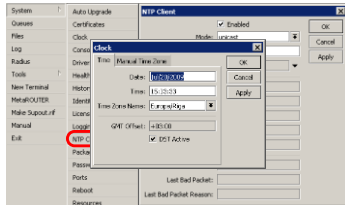
Why NTP

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

60

NTP Client

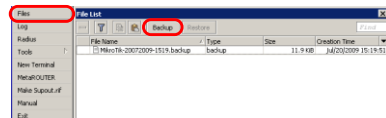
NTP package is not required



61

Configuration Backup

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



62

Configuration Backup

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

```
/export file=conf-august-2009
/ip firewall filter export file=firewall-aug-2009
/file print
/import [Tab]
```

63

Backup Lab

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

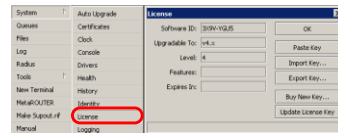
64

RouterOS License

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

65

License



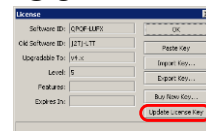
66

Obtain License



67

Update License for 802.11N



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

68

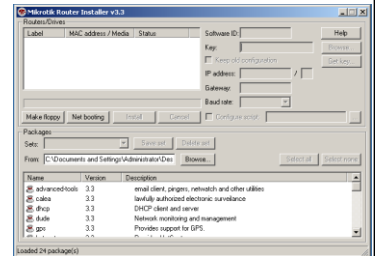
Netinstall

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

69

Netinstall

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



70

Optional Lab

LAB

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

71

Summary

72

Useful Links

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

73

Firewall

74

Firewall

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

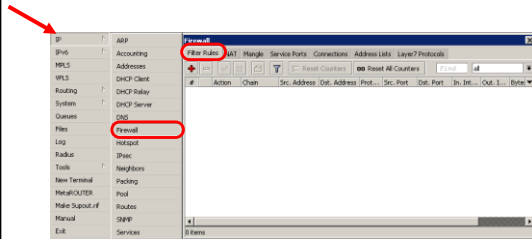
75

Firewall Filter

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

76

Firewall Chains



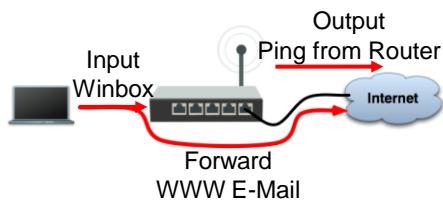
77

Filter Chains

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

78

Firewall Chains



79

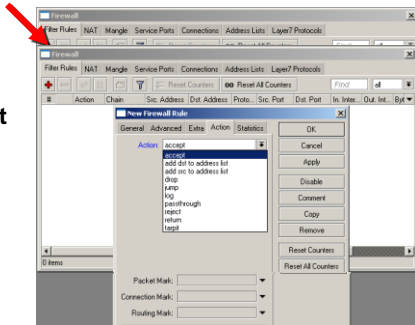
Input

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

80

Input

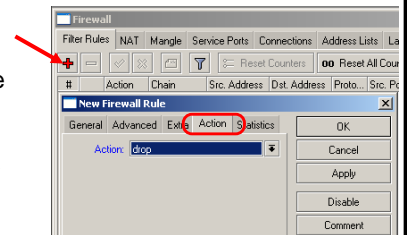
Add an **accept** rule for your Laptop IP address



81

Input

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



82

Input Lab

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

83

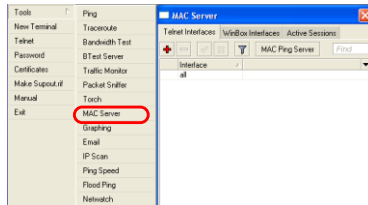
Input

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

84

Input

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



85

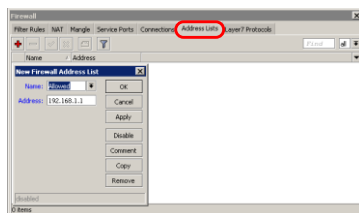
Address-List

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

86

Address-List

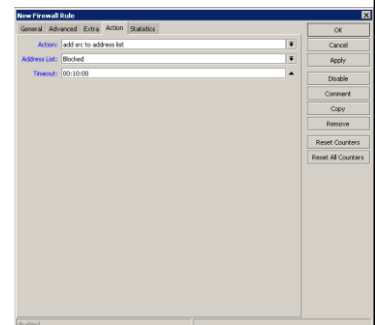
- Create different lists
- Subnets, separates ranges, one host addresses are supported



87

Address-List

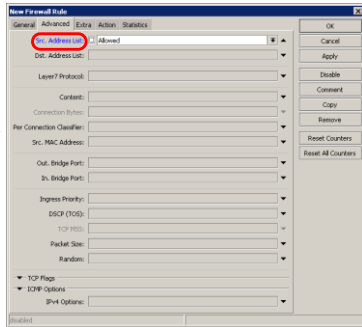
- Add specific host to address-list
- Specify timeout for temporary service



88

Address-List in Firewall

- Ability to block by source and destination addresses



89

Address-List Lab

LAB

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

90

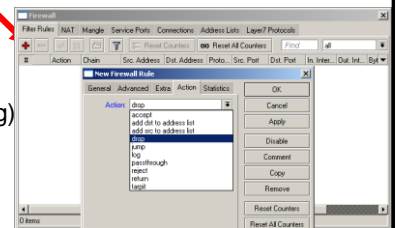
Forward

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

91

Forward

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



92

Forward

LAB

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

93

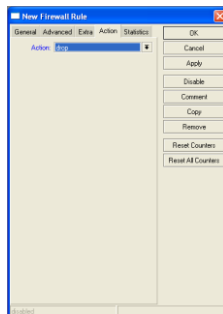
List of well-known ports

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

94

Forward

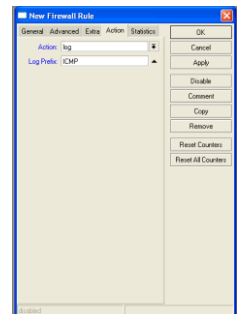
Create a rule that will block client's p2p traffic



95

Firewall Log

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



96

Firewall

[illegible]

Firewall chains

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

98

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

Firewall chains in Action

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

Forward

Firewall rule

Firewall rule

action=jump
jump-target=viruses

Firewall rule

Firewall rule

The last
firewall rule

viruses

Firewall rule

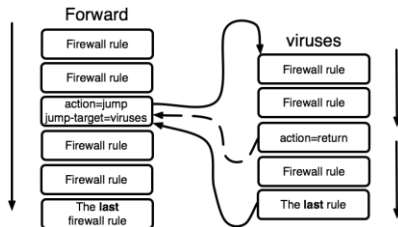
Firewall rule

action=return

Firewall rule

The last rule

99



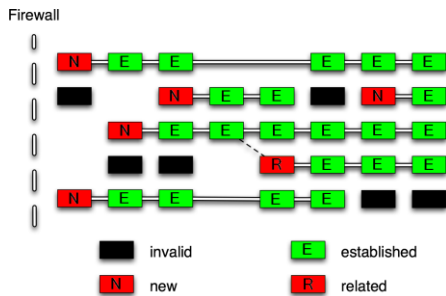
Firewall chain Lab

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

100

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

Connections



101

Connection State

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

102

Connection State

LAB

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

103

Summary

104

Network Address Translation

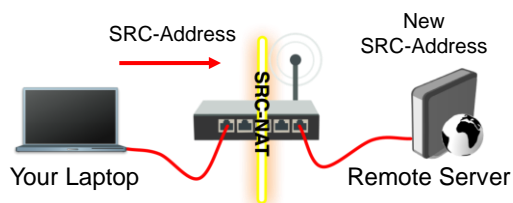
105

NAT

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

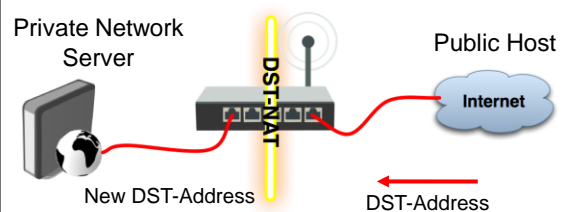
106

SRC-NAT



107

DST-NAT



108

NAT Chains

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

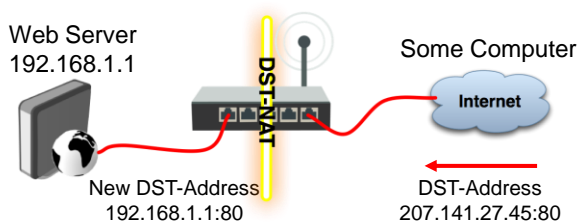
109

DST-NAT

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

110

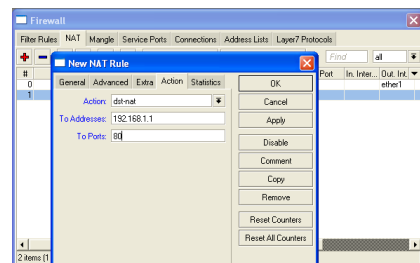
DST-NAT Example



111

DST-NAT Example

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



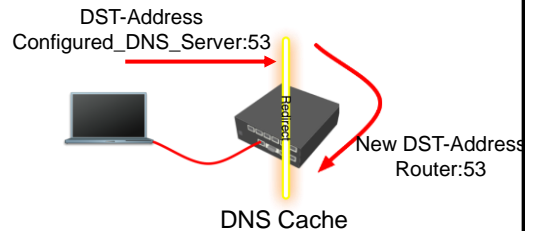
112

Redirect

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

113

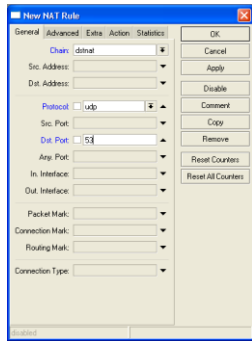
Redirect example



114

Redirect Example

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



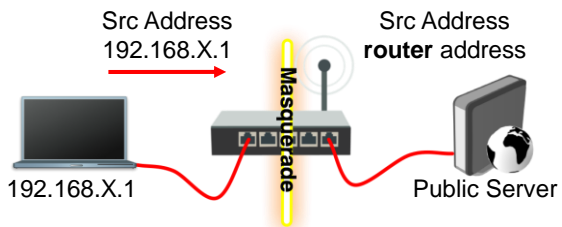
115

SRC-NAT

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

116

Masquerade



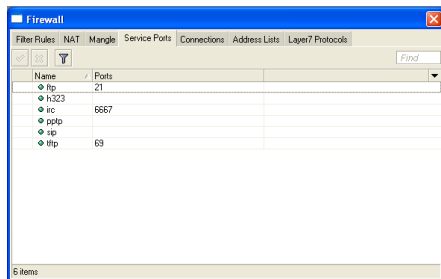
117

SRC-NAT Limitations

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

118

NAT Helpers



119

Firewall Tips

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

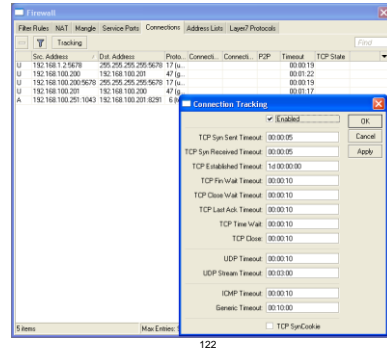
120

Connection Tracking

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

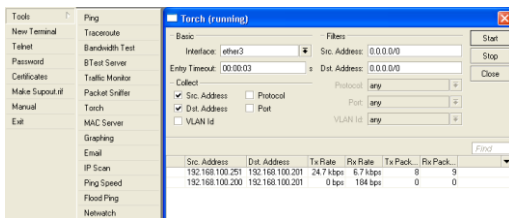
121

Connection Tracking



122

Torch



Detailed actual traffic report for interface

123

Firewall Actions

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

124

NAT Actions

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

125

Summary

126

Bandwidth Limit

127

Simple Queue

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

128

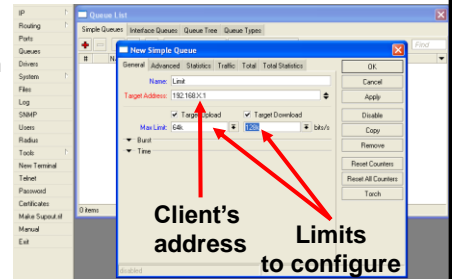
Simple Queue

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

129

Simple Queue

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



130

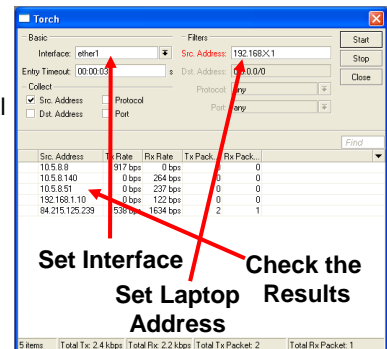
Simple Queue

- Check your limits
- Torch is showing bandwidth rate

131

Using Torch

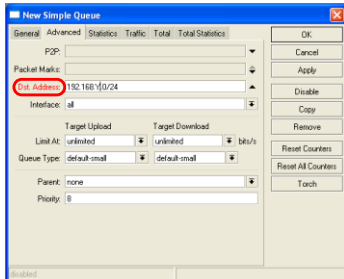
- Select local network interface
- See actual bandwidth



132

Specific Server Limit

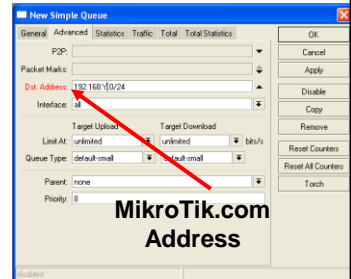
- Let's create bandwidth limit to MikroTik.com
- DST-address is used for this
- Rules order is important



133

Specific Server Limit

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



134

Specific Server Limit

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

135

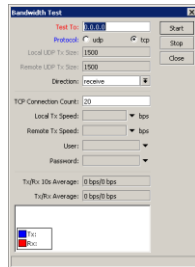
Bandwidth Test Utility

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

136

Bandwidth Test on Router

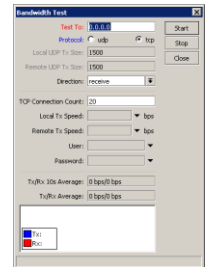
- Set **Test To** as testing address
- Select protocol
- TCP supports multiple connections
- Authentication might be required



137

Bandwidth Server

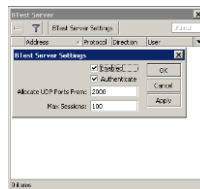
- Set **Test To** as testing address
- Select protocol
- TCP supports multiple connections
- Authentication might be required



138

Bandwidth Test

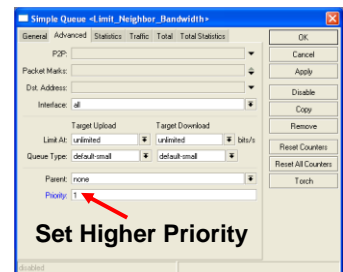
- Server should be enabled
- It is advised to use enabled **Authenticate**



139

Traffic Priority

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



140

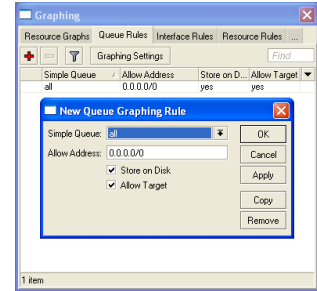
Simple Queue Monitor

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

141

Simple Queue Monitor

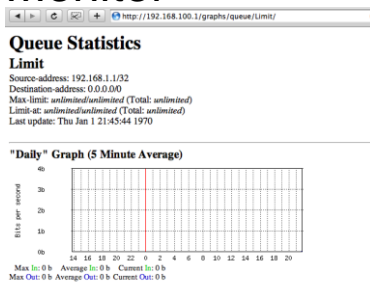
Let's enable graphing for Queues



142

Simple Queue Monitor

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



143

Advanced Queuing

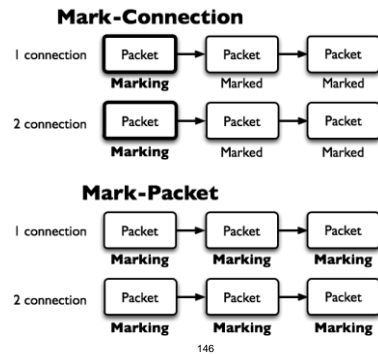
144

Mangle

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

145

Mangle Actions



146

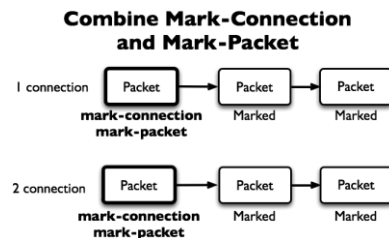
Mangle Actions

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

147

Optimal Mangle

- Queues have packet-mark option only



148

Optimal Mangle

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

149

Mangle Example

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

150

Mark Connection

The screenshot shows the 'New Mangle Rule' dialog box. The 'Chain' is set to 'forward'. The 'Src. Address' is '192.168.X.1'. The 'Action' is 'mark-connection'. The 'Mark User' is 'User 1'. The 'Passthrough' checkbox is checked. The 'Connection Marks' section is empty.

151

Mark Packet

The screenshot shows the 'New Mangle Rule' dialog box. The 'Chain' is set to 'forward'. The 'Src. Address' is '192.168.X.1'. The 'Action' is 'mark-packet'. The 'Mark User' is 'User 1'. The 'Passthrough' checkbox is checked. The 'Packet Marks' section is empty.

152

Mangle Example

LAB

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

153

Advanced Queuing

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

154

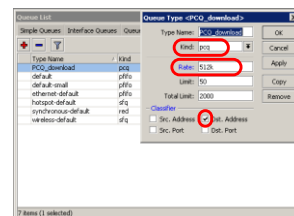
PCQ

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

155

PCQ, one limit to all

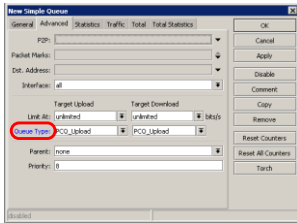
- PCQ allows to set one limit to all users with one queue



156

One limit to all

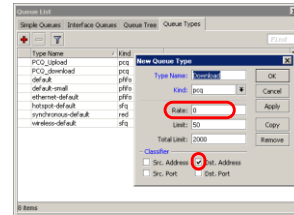
- Multiple queue rules are changed by one



157

PCQ, equalize bandwidth

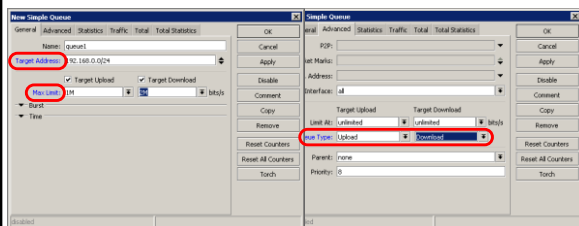
- Equally share bandwidth between customers



158

Equalize bandwidth

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



159

PCQ Lab

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

160

Summary

161

Wireless

162

What is Wireless

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

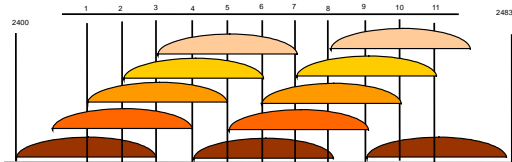
163

Wireless Standards

- IEEE 802.11b - 2.4GHz frequencies, 11Mbps
- IEEE 802.11g - 2.4GHz frequencies, 54Mbps
- IEEE 802.11a - 5GHz frequencies, 54Mbps
- IEEE 802.11n - 2.4GHz - 5GHz, 300Mbps

164

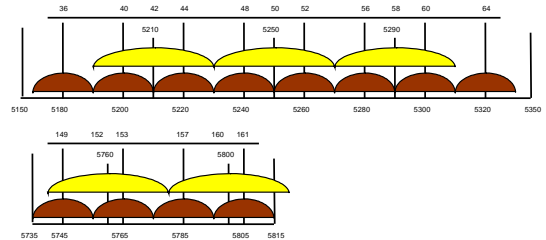
802.11 b/g Channels



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

165

802.11a Channels



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

166

Supported Bands

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

167

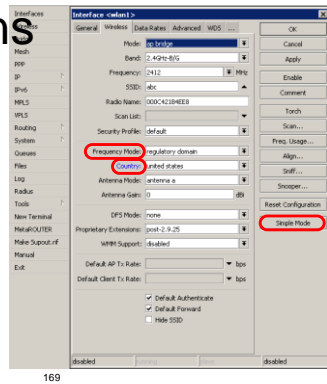
Supported Frequencies

- Depending on your country regulations wireless card might support
 - 2.4GHz: 2192 - 2734 MHz
 - 5GHz: 4800 - 6100 MHz

168

Apply Country Regulations

Set wireless interface to apply your country regulations



169

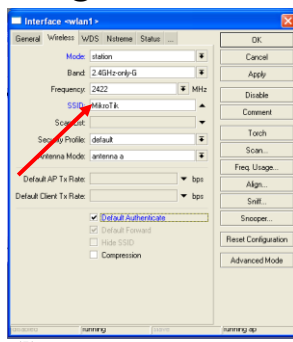
Wireless Network



170

Station Configuration

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



171

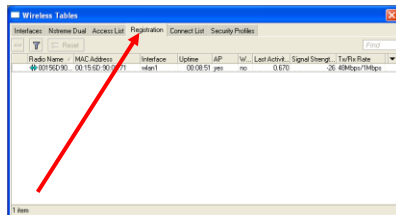
RADIO Name

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

172

Registration Table

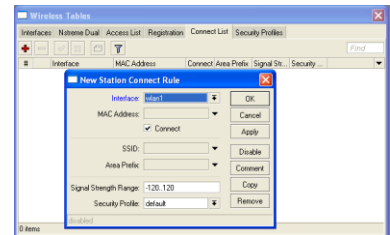
- View all connected wireless interfaces



173

Connect List

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



174

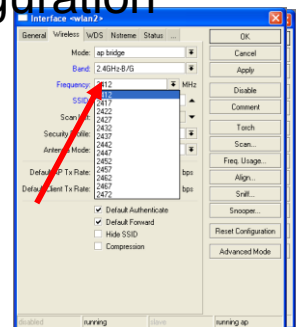
Connect List Lab

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

175

Access Point Configuration

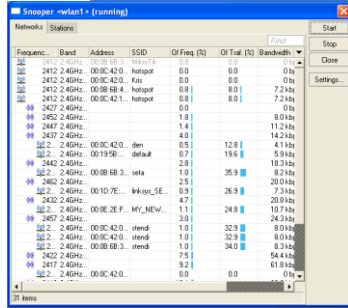
- Set Interface **mode=ap-bridge**
- Select **band**
- Set **SSID**, Wireless Network Identity
- Set **Frequency**



176

Snooper wireless monitor

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

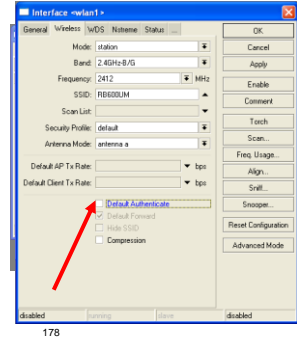


| Network | Station | Frequency | Band | Address | SSID | Of Freq (%) | Of Total (%) | Bandwidth |
|---------|---------|-------------------|----------|---------|------|-------------|--------------|-----------|
| 2412 | 2.4GHz | 00:0C:42:00:00:00 | Hotspot | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| 2412 | 2.4GHz | 00:0C:42:00:00:00 | Kiss | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| 2412 | 2.4GHz | 00:0B:68:40:00:00 | Hotspot | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| 2412 | 2.4GHz | 00:0C:42:11:00:00 | Hotspot | 0.0 | 0.0 | 0.0 | 0.0 | 0.0 |
| 2402 | 2.4GHz | 00:0C:42:00:00:00 | den | 0.5 | 12.8 | 4.1 | 1.0 | 0.0 |
| 2402 | 2.4GHz | 00:19:0E:00:00:00 | default | 0.7 | 19.8 | 5.9 | 1.0 | 0.0 |
| 2402 | 2.4GHz | 00:0B:68:30:00:00 | seta | 1.0 | 25.9 | 8.2 | 1.0 | 0.0 |
| 2402 | 2.4GHz | 00:10:7E:00:00:00 | mkysa_SE | 2.5 | 26.9 | 7.3 | 1.0 | 0.0 |
| 2402 | 2.4GHz | 00:0E:2E:F0:00:00 | MY_NEW | 4.7 | 24.8 | 10.7 | 1.0 | 0.0 |
| 2402 | 2.4GHz | 00:0C:42:00:00:00 | stend | 1.0 | 32.9 | 8.0 | 1.0 | 0.0 |
| 2402 | 2.4GHz | 00:0C:42:00:00:00 | stend | 1.0 | 32.9 | 8.0 | 1.0 | 0.0 |
| 2402 | 2.4GHz | 00:0B:68:30:00:00 | stend | 1.0 | 34.0 | 8.3 | 1.0 | 0.0 |
| 2402 | 2.4GHz | 00:0C:42:00:00:00 | stend | 7.5 | 54.4 | 16.4 | 1.0 | 0.0 |
| 2402 | 2.4GHz | 00:0C:42:00:00:00 | stend | 9.2 | 61.6 | 18.6 | 1.0 | 0.0 |

177

Security on Access Point

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



178

Default Authentication

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

179

Access-List Lab

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

180

Security

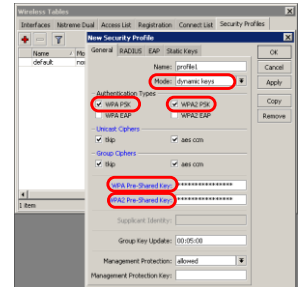
- Let's enable encryption on wireless network
- You must use WPA or WPA2 encryption protocols
- All devices on the network should have the same security options

181

Security

LAB

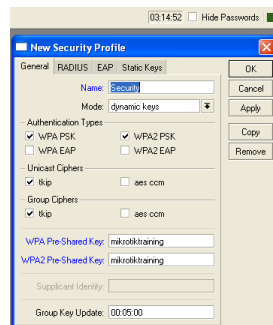
- Let's create WPA **encryption** for our wireless network
- WPA Pre-Shared Key is **mikrotiktraining**



182

Configuration Tip

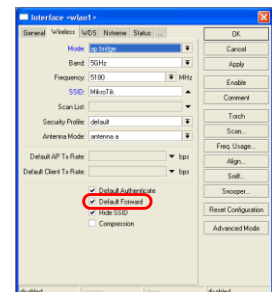
- To view hidden Pre-Shared Key, click on Hide Passwords
- It is possible to view other hidden information, except router password



183

Drop Connections between clients

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



184

Default Forwarding

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

185

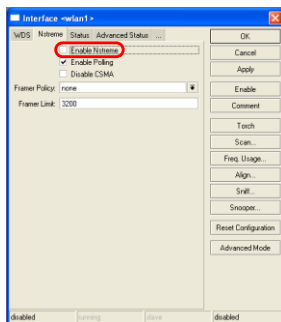
Nstreme

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

186

Nstreme Lab

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



187

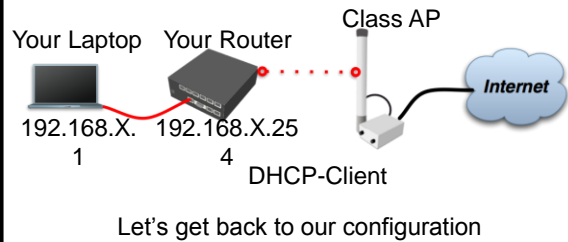
Summary

188

Bridging

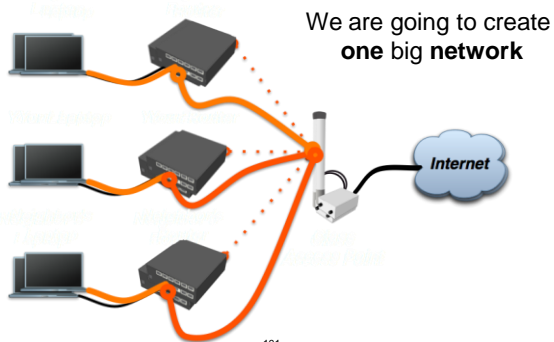
189

Bridge Wireless Network



190

Bridge Wireless Network



191

Bridge

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

192

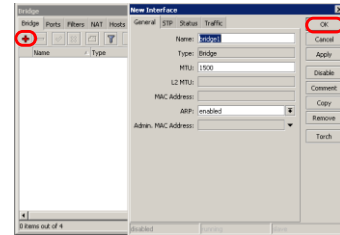
Bridge

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

193

Create Bridge

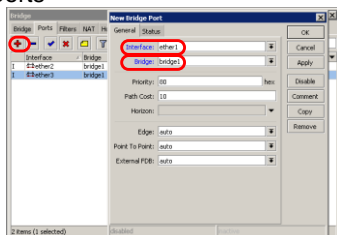
- Bridge is configured from **/interface bridge** menu



194

Add Bridge Port

- Interfaces are added to bridge via ports



195

Bridge

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

196

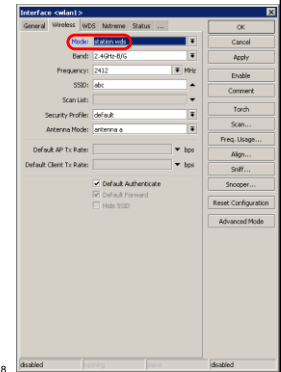
Bridge Wireless

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

197

Set WDS Mode

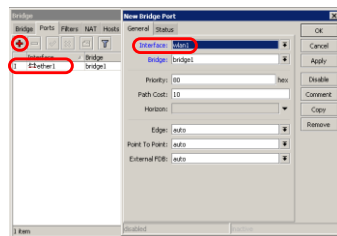
- Station-wds is special station mode with WDS support



198

Add Bridge Ports

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



199

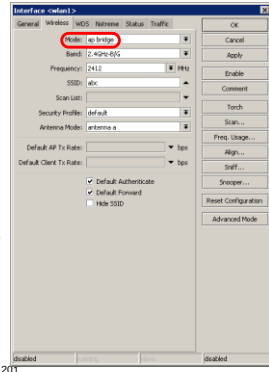
Access Point WDS

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

200

AP-bridge

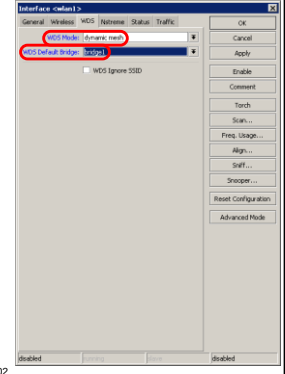
- Set AP-bridge settings
- Add Wireless interface to **bridge**



201

WDS configuration

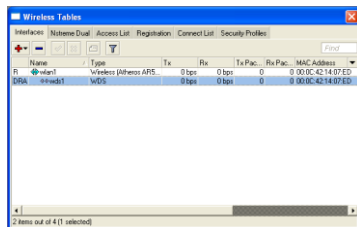
- Use **dynamic-mesh** WDS mode
- WDS interfaces are created on the fly
- Others AP should use **dynamic-mesh** too



202

WDS

- WDS link is established
- Dynamic interface is present



203

WDS Lab

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

204

WDS Lab

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

205

Restore Configuration

LAB

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

206

Summary

207

Routing

208

Route Networks

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

209

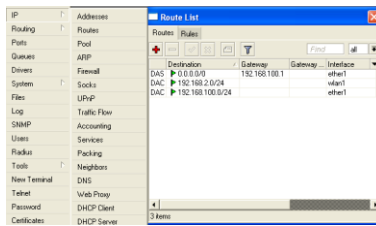
Route

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

210

Routes

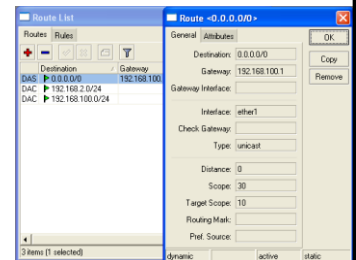
- **Destination:** networks which can be reached
- **Gateway:** IP of the next router to reach the destination



211

Default Gateway

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



212

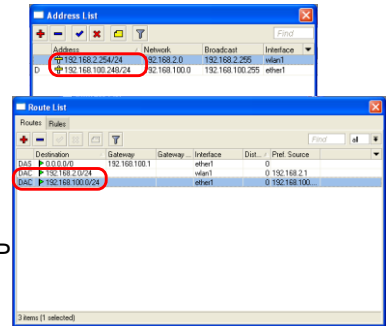
Set Default Gateway Lab

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

213

Dynamic Routes

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



214

Routes

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

215

Static Routes

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

216

Static Route

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

217

Static Route

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

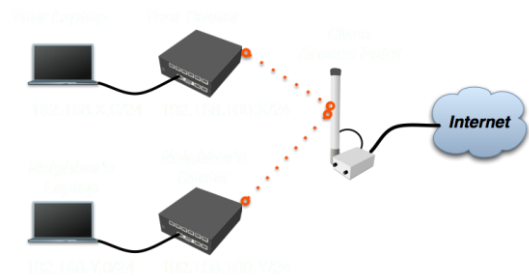
218

Route to Your Neighbor

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

219

Network Structure



220

Route To Your Neighbor

LAB

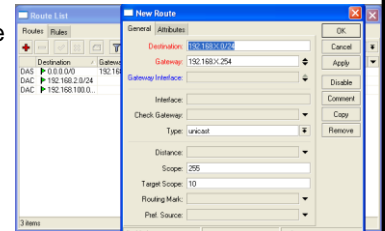
- Add one route rule
- Set Destination, **destination** is **neighbor's local network**
- Set Gateway, address which is used to reach destination - **gateway** is IP address of neighbor's router wireless interface

221

Route Your Neighbor

LAB

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



222

Router To Your Neighbor

You should be able to ping neighbor's laptop now

223

Dynamic Routes

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

224

Dynamic Routes

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

225

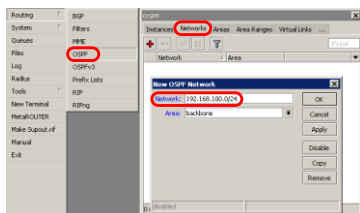
Dynamic Routes

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

226

OSPF configuration

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



227

OSPF LAB

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

228

Summary

229

Local Network Management

230

Access to Local Network

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

231

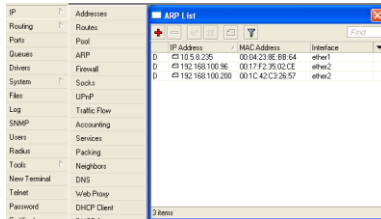
ARP

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

232

ARP Table

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



| IP Address | MAC Address | Interface |
|-----------------|-------------------|-----------|
| 10.5.5.235 | 00:04:23:8E:8B:64 | ether1 |
| 192.168.100.16 | 00:17:F2:39:02:C1 | ether2 |
| 192.168.100.200 | 00:1C:42:C3:38:57 | ether2 |

233

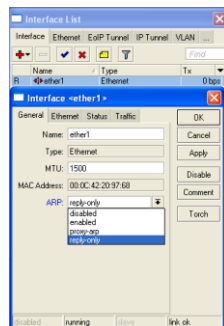
Static ARP table

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

234

Static ARP configuration

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



235

Static ARP Lab

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

236

DHCP Server

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

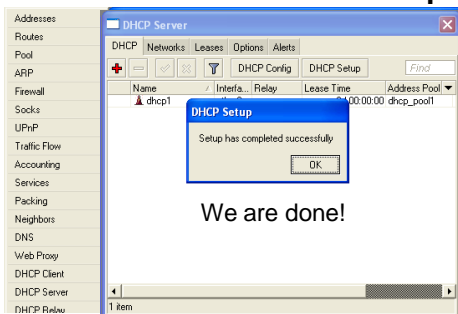
237

DHCP Server

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

238

DHCP-Server Setup



239

Important

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

240

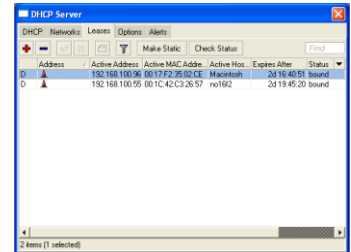
DHCP Server Lab

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

241

DHCP Server Information

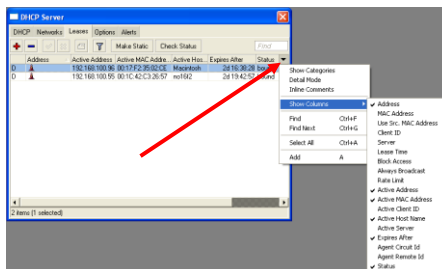
Leases provide information about DHCP clients



242

Winbox Configuration Tip

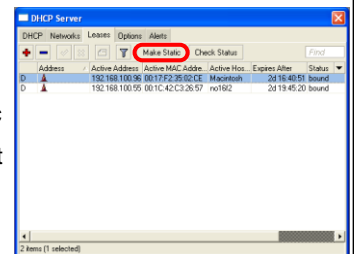
Show or hide different Winbox columns



243

Static Lease

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



244

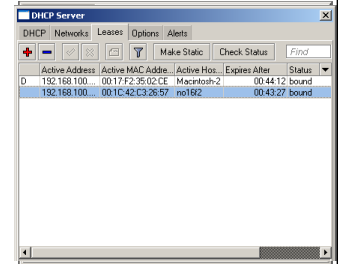
Static Lease

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

245

Static Lease

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



246

HotSpot

247

HotSpot

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

248

HotSpot Usage

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

249

HotSpot Requirements

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

250

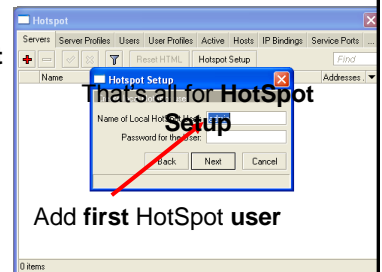
HotSpot Setup

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

251

HotSpot Setup

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



252

Important Notes

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

253

HotSpot Help

- HotSpot login page is provided when user tries to access any web-page
- To logout from HotSpot you need to go to <http://router IP> or <http://HotSpot DNS>

254

HotSpot Setup Lab

LAB

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

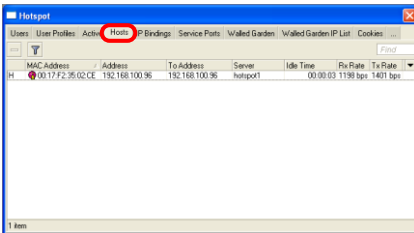
255

Important Notes

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

256

HotSpot Network Hosts

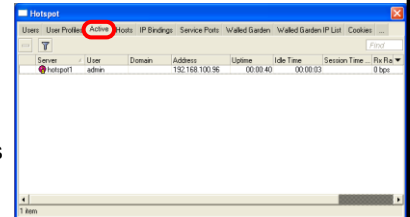


Information about clients connected to HotSpot router

257

HotSpot Active Table

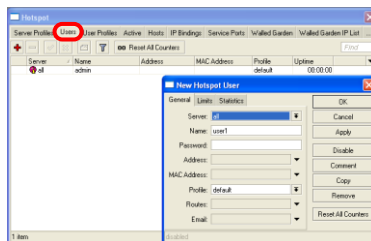
Information about authorized HotSpot clients



258

User Management

Add/Edit/Remove HotSpot users



259

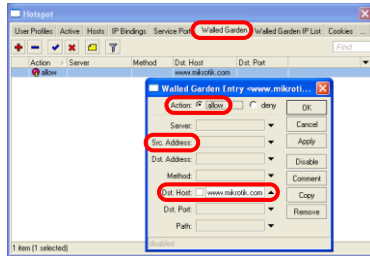
HotSpot Walled-Garden

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

260

HotSpot Walled-Garden

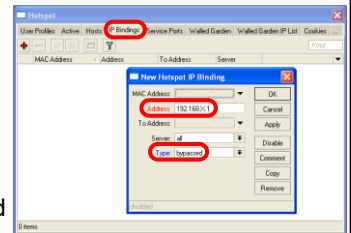
Allow access to
mikrotik.com



261

Bypass HotSpot

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



262

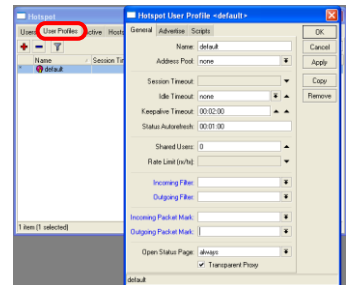
HotSpot Bandwidth Limits

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

263

HotSpot User Profile

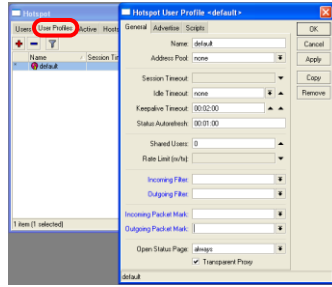
User Profile - set of options used for specific group of HotSpot clients



264

HotSpot Advanced Lab

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



265

HotSpot Lab

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

266

Tunnels

267

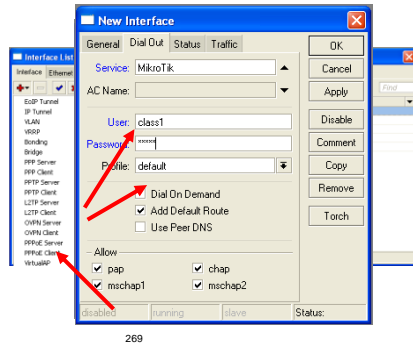
PPPoE

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

268

PPPoE Client Setup

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



269

PPPoE Client Lab

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

270

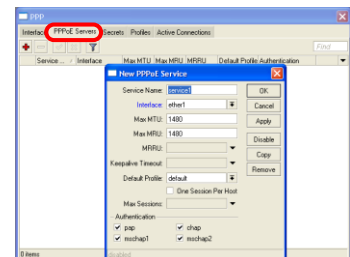
PPPoE Client Setup

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

271

PPPoE Server Setup

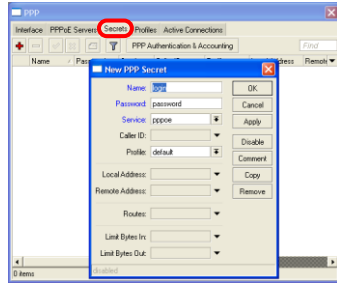
- Select Interface
- Select Profile



272

PPP Secret

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



273

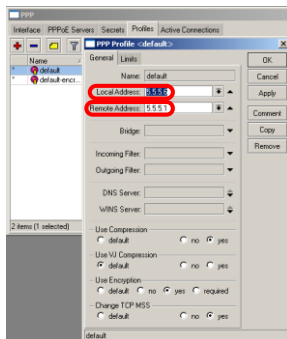
PPP Profiles

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

274

PPP Profile

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



275

PPPoE

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

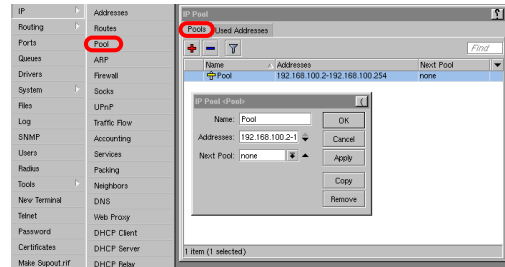
276

Pools

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

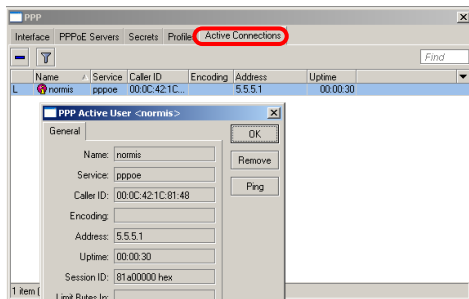
277

Pool



278

PPP Status

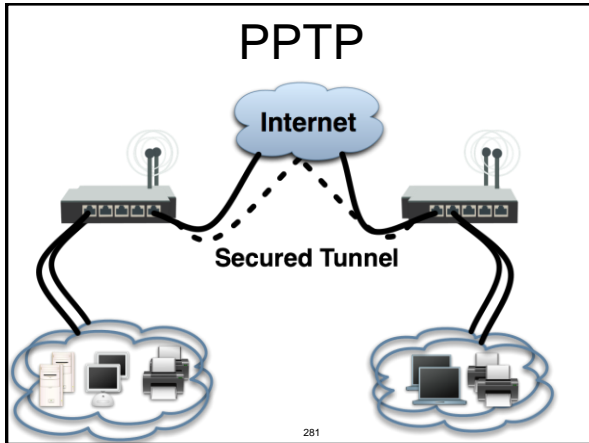


279

PPTP

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

280



PPTP configuration

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

282

PPTP client

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

283

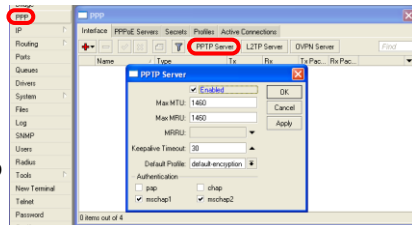
PPTP Client

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

284

PPTP Server

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



285

PPTP Server Clients

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

286

PPP Profile

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

287

PPTP Lab

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

288

LAB

Proxy

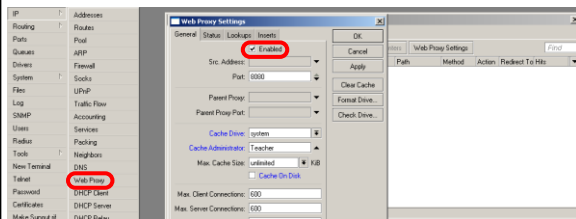
289

What is Proxy

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

290

Enable Proxy



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

291

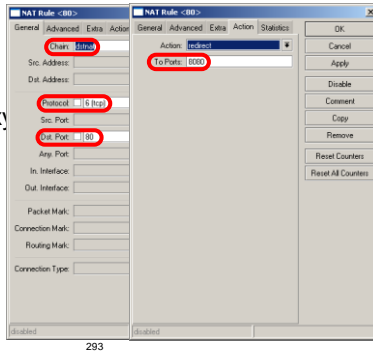
Transparent Proxy

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

292

Transparent Proxy

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



293

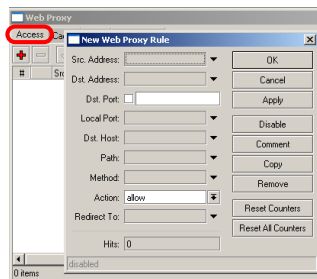
HTTP Firewall

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

294

HTTP Firewall

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



295

HTTP Firewall

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

296

LAB

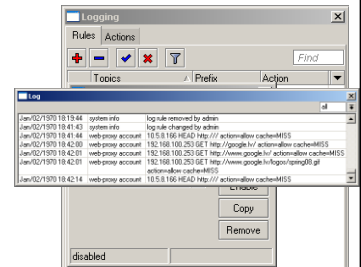
Web-page logging

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

297

Web-Pages logging

- Add logging rule
- Check logs



298

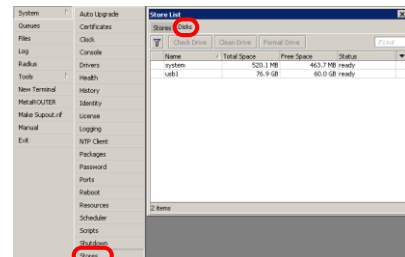
Caching to External

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

299

Store

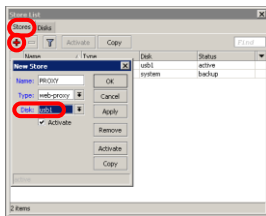
- Manage all external disks
- Newly connected disk should be formatted



300

Add Store

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



301

Summary

302

Dude

303

Dude

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

304

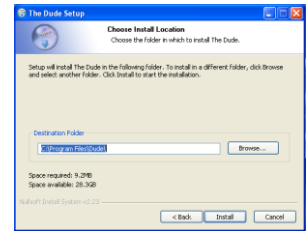
Dude

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

305

Dude Install

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



306

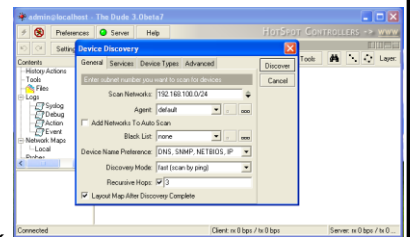
Dude

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

307

Dude First Launch

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



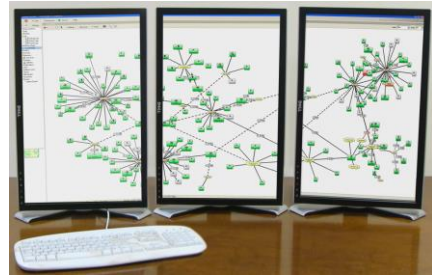
308

Dude Lab

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

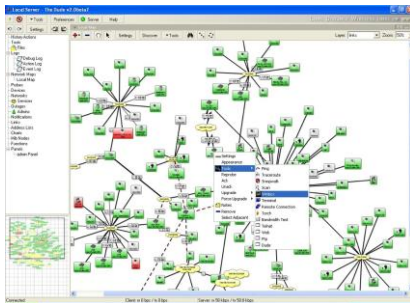
309

Dude Usage



310

Dude Usage



311

Troubleshooting

312

Lost Password

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

313

RouterBOARD License

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

314

Bad Wireless Signal

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

315

No Connection

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

316

Before Certification Test

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

317

Certification Test

318

Certification test

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

319

Instructions

320