# MikroTik RouterOS Training
# User Management

Vahid Shahbazian fard jahromy www.LearnMikroTik.ir

## Schedule

- 09:00 – 10:30 Morning Session I
  - 10:30 – 11:00 Morning Break
- 11:00 – 12:30 Morning Session II
  - 12:30 – 13:30 Lunch Break
- 13:30 – 15:00 Afternoon Session I
  - 15:00 – 15:30 Afternoon Break
- 15:30 – 17:00 (18:00) Afternoon Session II




## Instructor

- Vahid Shahbazian fard jahromy
  - Training, Support & Consultant
  - Specialization: Wireless, Firewall, The Dude, Routing, Monitoring Techniques




## Housekeeping

- Course materials
- Routers, cables
- Break times and lunch




## Course Objective

- Provide knowledge and hands-on training for MikroTik RouterOS basic and advanced user management capabilities for any size networks
- Upon completion of the course you will be able to plan, implement, adjust and debug user management configurations implemented by MikroTik RouterOS




## Topics Overview

- Point-to-Point Protocols
  - PPP Profile, PPP Secret
  - PPTP and L2TP
  - User Access Control
  - PPP interface Bridging
    - Bridge Control Protocol
    - PPP Multi-link Protocol

## Topics Overview (Cont.)

- Hotspot
  - Hotspot Setup
  - Hotspot Login Methods
  - Universal clients
  - Users
  - Group of Users
  - Server Configuration
  - Exceptions
  - Accounting

## Topics Overview (Cont.)

- RADIUS
  - RADIUS client
  - RADIUS server
    - User Manager
  - RADIUS incoming
- IPsec
  - IPsec Introduction
  - Transport mode vs. Tunnel mode

## 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: X=_____ Y=_____

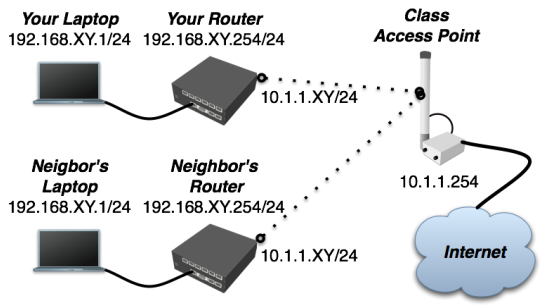
 

## Class Setup Lab.

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

## Class Setup



## Class setup Lab (cont.)

- Set system identity of the board and wireless radio name to “XY_<your_name>”. Example: “88_Shahbazian”
- 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)

## Point-to-Point Protocols

PPTP, PPPoE, L2TP, BCP, MLPPP, MRRU, Interface routing, Dynamic address-lists, Dynamic simple queues



PPP Profile, PPP Secret

## LOCAL USER DATABASE

## Point-to-Point protocol tunnels

- little bit sophisticated in configuration
- Capable of authentication and data encryption
- Such tunnels are:
  - PPPoE (Point-to-Point Protocol over Ethernet)
  - PPTP (Point-to-Point Tunneling Protocol)
  - L2TP (Layer 2 Tunneling Protocol)
  - OVPN (Open Virtual Private Network)
  - SSTP (Secure Socket Tunneling Protocol)
- You should create user information before
- creating any tunnels

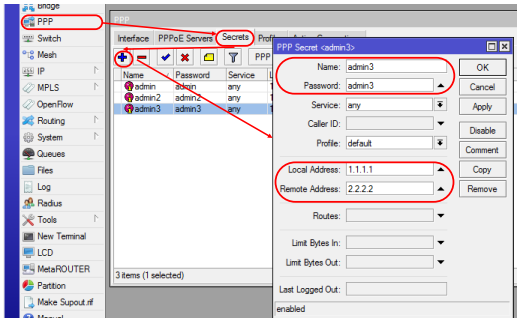
 

## PPP Secret

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

## PPP Secret



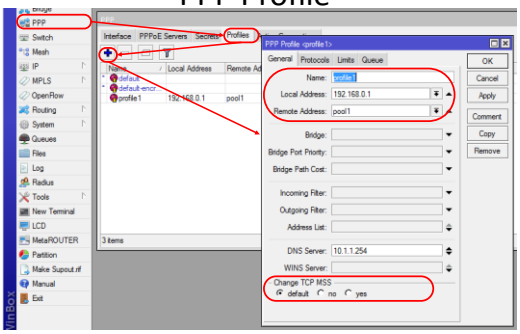

 

## PPP Profile and IP Pools

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

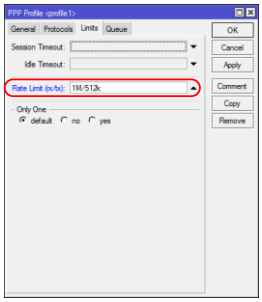
 

## PPP Profile





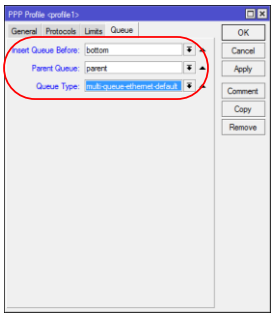

## Dynamic Simple Queues



- It is possible to assign specific limit to each group belonging to the same PPP profile
- Every time new user connects RouterOS will create new simple queue
- This option can be acquired from RADIUS server



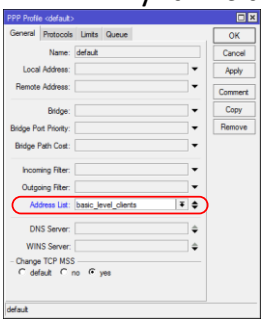

## Dynamic Simple Queues (Cont.)



- It is possible to select
  - Dynamic Queue order
  - Parent Queue
  - Queue Type




## Dynamic address-list



- It is also possible to implement custom QoS structures
- Every time new user connects RouterOS will create new address-list entry
- Address-list then can be utilized by mange facility for packet marking.




## Change TCP MSS

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




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

## PPTP AND L2TP

## PPTP Tunnels

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

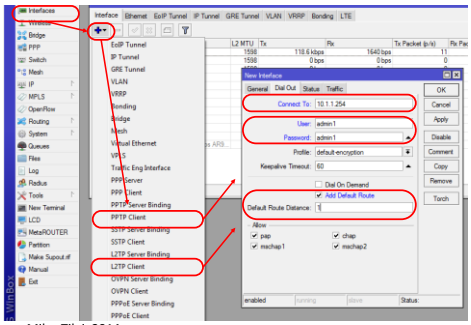



## L2TP Tunnels

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




## Creating PPTP/L2TP Client





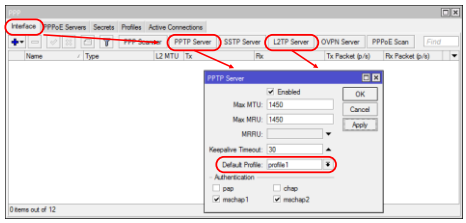


## PPTP Client Lab

- Create PPTP client
  - Server Address: 10.1.2.1
  - User: class
  - Password: class
  - Add default route = yes
- Make necessary adjustments to access the internet




## Creating PPTP/L2TP server







## PPTP Server Lab

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

## Optional: Advanced VPN Lab

- Restore system backup
- Create secure L2TP tunnel with your neighbor
- Create EoIP tunnel over the L2TP tunnel
- Bridge your networks together!




Point to Point Protocol over Ethernet

## USER ACCESS CONTROL




## User Access Control

- Controlling the Hardware
  - Static IP and ARP entries
  - DHCP for assigning IP addresses and managing ARP entries
- Controlling the Users
  - PPPoE requires PPPoE client configuration
  - Hotspot redirects client request to the sign-up page
  - PPTP requires PPTP client configuration

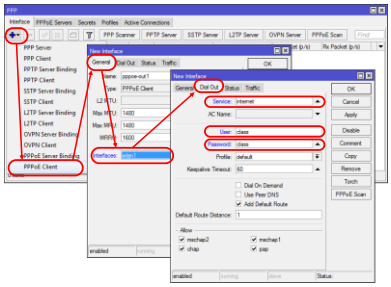



## PPPoE tunnels

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




## PPPoE client






## PPPoE Client Lab

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

## PPPoE Client Status

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




## * PPPoE Lab with Encryption *

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

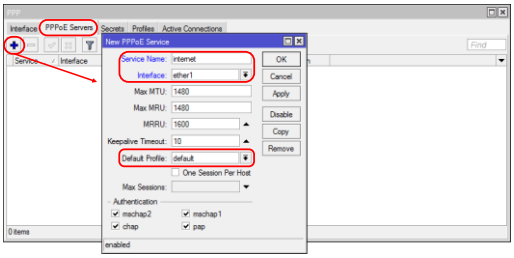



## PPPoE Server

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




## Creating PPPoE server (service)







## PPPoE Server Lab

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




PPP BCP (Bridge Control Protocol)
PPP MP (Multi-link Protocol)

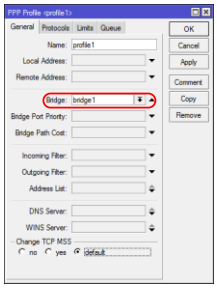
## PPP INTERFACE BRIDGING

## PPP Bridge Control Protocol

- RouterOS now have BCP support for all async. PPP, PPTP, L2TP & PPPoE (not ISDN) interfaces
- BCP allows to bridge Ethernet packets through the PPP link
- BCP is independent part of PPP tunnel - It is not related to IP address of PPP interface
- Bridging and routing over PPP link can happen at the same time, independently.




## Setting up BCP




- Bridge must be specified the PPP profiles on ***both*** sides of the tunnel
- Note that PPP interface don't have any MAC addresses – so your bridge must have a MAC address before you add PPP to the bridge




## PPP MTU Problem

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




## PPP Multi-link Protocol

- PPP Multi-link Protocol allows divide packet to multiple channels therefore increasing possible MTU and MRU (up to 65535 bytes)
- MLPPP can be created:
  - over single physical link – where multiple channels run on the same link
  - over multiple physical links - where multiple channels run on the multiple link

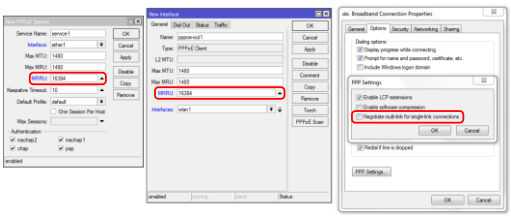



## MRRU

- To enable PPP Multi-link Protocol over single link you must specify MRRU option
- If both sides support this feature there are no need for MSS adjustment (in firewall mangle)
- MRRU is less CPU expensive that 2 mangle rules per client if you have more that 30 clients
- In MS Windows you must enable "Negotiate multi-link for single link connections" option




## PPP Multi-link Protocol



## PPP Bridging Lab

- **Restore default system backup**
- Create PPP tunnel with your neighbour(s)
- Bridge PPP tunnels with your local interface
- Ensure that MTU and MRU of the PPP link is at least 1518 byte (size of Ethernet frame)
- Check the configuration using ping tool with different packet size




## MLPPP

- MikroTik RouterOS have multi-link PPP over multiple links client support starting from V3.10
- Server support will be added some time in the future
- To enable MLPPP just assign multiple interfaces for the same PPP client.
- Note:
  - all PPP lines must have same user name and password
  - Server must have support for MLPPP




## Interface ECMP Routing

- In case you have more that one PPP connection from the same server, but MLPPP is impossible (different user names, server support missing) it is possible to use Interface routing
- Simple IP address routing is impossible all PPP connections have the same gateway IP address
- To enable interface routing just specify all PPP interfaces as route gateway-interface
- Works only on PPP interfaces.




## Hotspot

Overview & Setup, Users & Groups, Universal clients, Server configurations, Exceptions, Accounting



Introduction Hotspot

## HOTSPOT OVERVIEW




## Hotspot Overview

- Tool for Instant **Plug-and-Play** Internet access
- Hotspot provides **authentication** of clients before access to public network
- Walled-garden to allow resources **without** authentication
- It also provides User **Accounting**
- Transparent **proxy**

## Hotspot Usage

- Open Access Points, Internet Cafes, Airports, universities campuses, etc.
- Different ways of authorization
- Flexible accounting
- Anywhere Authorization or Accounting are required




## Hotspot Operation

- Client can use **wrong network** configuration **settings**, Hotspot server translates them to correct ones
- **No** Internet available **before** Hotspot authorization
- **Exceptions** are added to walled-garden and /ip hotspot ip-binding




## Hotspot Operation

- Enter username/password in Hotspot login page to get the Internet
- Other login methods available
- Different accounting options




How to setup Hotspot

## HOTSPOT SETUP




## Hotspot Requirements
(Before setup)

- Valid IP address configuration on local (Hotspot) and Public (Internet) interfaces
- DNS servers added in /ip dns
- One Hotspot user (added by setup command)

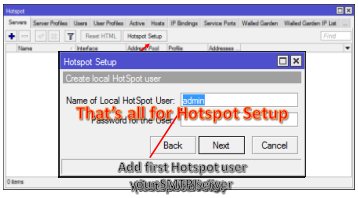



## Hotspot Setup

- Setup is launched by the command, **/ip hotspot setup**
- Use /ip hotspot setup for Hotspot server setup, **strongly recommended**
- All configuration settings can be added manually

## Hotspot Setup

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







## Important Notes

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




## Configuration Created

- Additional configuration is created in different sections by Hotspot setup
- Hotspot default setup creates additional configuration:
  - **DHCP-Server** on Hotspot Interface
  - **Pool** for Hotspot Clients
  - Dynamic **Firewall rules** (Filter and NAT)
- No additional configuration necessary with /ip hotspot setup




## Common Mistakes

- Hotspot on bridge, configure server on **bridge interface** not on the bridge port (hotspot can not run on slave interface)
- Correct **DNS name** for Hotspot server **FQDN required**
- **arp=enabled** for the interface




## 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://routerIP or http://HotSpotDNS




## Hotspot 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
- Make sure you get to the Internet

## Remember

- Access to public networks is blocked (Internet, Winbox to the router)
- Login to the Hotspot to get the Internet
- Login by Hotspot page

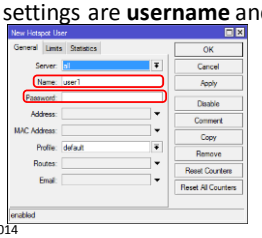



## USERS




## Hotspot users

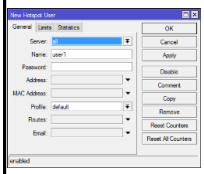
- Users are added and managed from */ip hotspot user*
- Required settings are **username** and **password**







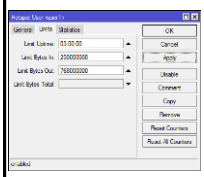
## Users Settings



- **Server**, Hotspot server user belongs to
- **Name**, client username
- **Password**, user's password
- **Address**, Hotspot IP address to be used by client
- **MAC-address**, login only from the specific MAC-address
- **Profile**, user's profile name




## Users Limits



- **Uptime**, time allowed to be online for user
- **Bytes In**, bytes user can upload
- **Bytes Out**, bytes user can download
- **Bytes Total** = Bytes In + Bytes Out

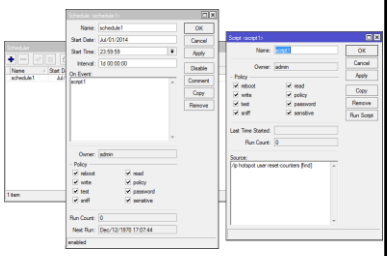



## Users lab

- Add additional Hotspot user
- Set this user to login only from your laptop
- Restrict user to 5 hours 1Gb upload and 1Gb download per day

## Daily users

- For the previous lab, use **scheduler** and simple **script**
- */ip hotspot user reset-counters* command to reset uptime



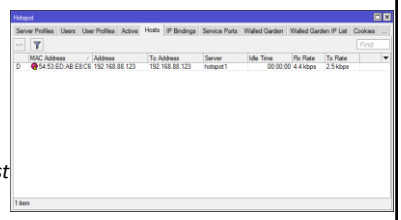



## MONITOR USERS



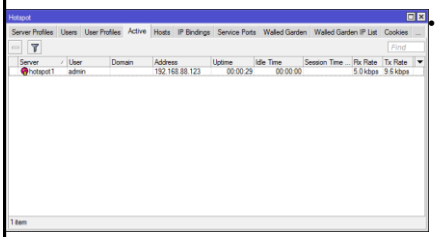

## Hotspot Network Hosts

- Information about clients connected to Hotspot interface shown in */ip hotspot host*






## Authorized Users



- Authorized users are shown in */ip hotspot active*




## HOTSPOT LOGIN METHODS

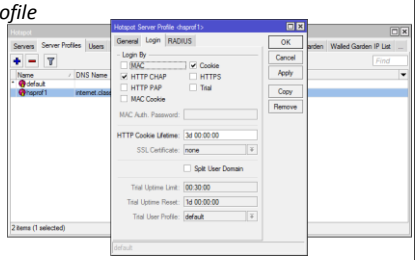



## Login Methods

- HTTP CHAP, HTTP PAP
- HTTPS
- MAC-Address
- Cookie
- Trial method

## Login Configuration

- */ip hotspot profile* stores **Login Method** configuration






## HTTP CHAP, PAP

- Login page is shown for users
- login/password is necessary to get Internet
- CHAP, CHAP challenge for login, enabled browser's JavaScript
- PAP, login in plain text for legacy browsers





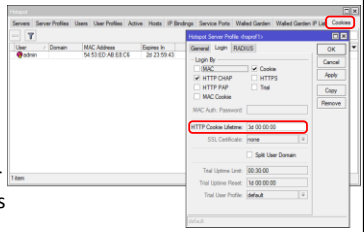
## HTTPS

- **Login page** is shown for users
- Authorization is encrypted by **SSL** protocol
- **Certificate** should be imported to router



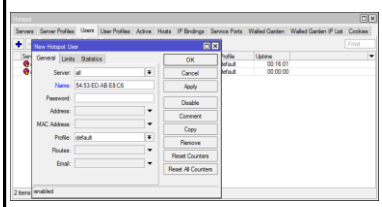

## Cookie

- Cookie is sent to client, after successful HTTP login
- Hotspot does not ask for login/password for second time access






## MAC-Address

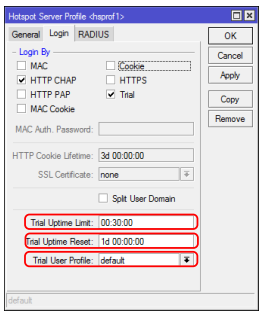


- Avoid Hotspot login page
- Add MAC-address as username
- Authentication occurs, as user is connected to the Hotspot




## Trial

- Use Hotspot free of charge for the period
- Set usage time over specific period



## Login Methods Lab

- Enable cookie login for 2 days lifetime
- Enable trial for 1 hour over 24 hours
- Enable MAC-address authentication for your laptop




## Hotspot Sequence

| | |
|---|---|
| Universal Client | • User is connected to the Router<br>• IP address is translated, if necessary |
| MAC-Address | • MAC-address users authentication |
| HTTP, HTTPS | • Login page is shown for user |
| Cookie | • Cookie used for second HTTP login |




## Exceptions Sequence

| | |
|---|---|
| IP-Binding | • Present on Universal client level |
| Walled-Garden | • Allow access to specific resources |




## Hotspot Logout

- Logout from Hotspot to stop accounting
- Logout from **login** page, http://hotspot or http://router_ip
- After **keepalive** timeout reached

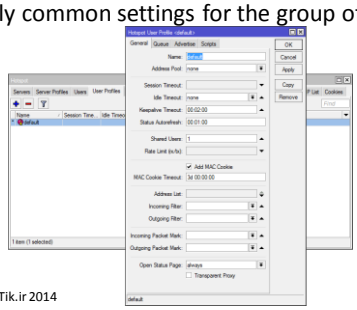



## GROUP OF USERS

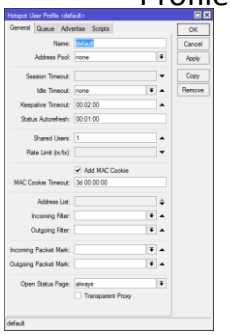



## User Profile

- To apply common settings for the group of users



## Profile Settings

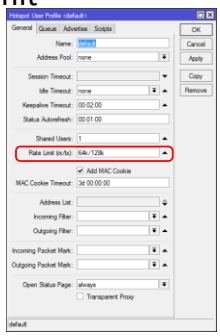


- **Address-Pool**, to enable universal client
- **Session Timeout**, user is logged out after this time
- **Keepalive Timeout**, detects whether client is reachable
- **Shared Users**, allowed simultaneous logins with the same username



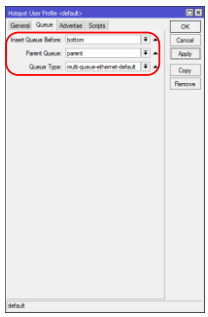

## Rate Limit

- Bandwidth limit for Hotspot clients
- Creates **dynamic** simple queue
- Syntax, rx-rate[/tx-rate] [rx-burstrate[/tx-burst-rate] [rx-burstthreshold[/tx-burst-threshold] [rxburst-time[/tx-burst-time] [priority][rx-rate-min[/tx-rate-min]]]]
- **rx** client's upload, **tx** client's download





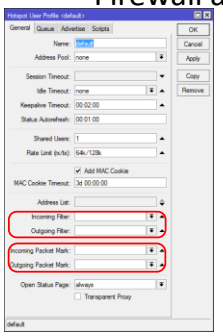

## Rate Limit (Continue)



- It is possible to select
  - Dynamic Queue order
  - Parent Queue
  - Queue Type




## Firewall and Mangle

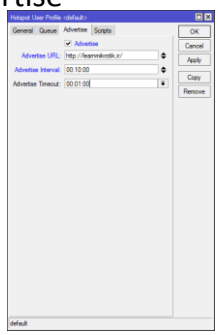


- **Filter**, check users through the specific firewall filter chain
- **Packet Mark**, to set mangle mark for the users
- Add **jump** from built-in chains (input, forward, output) to hotspot chain



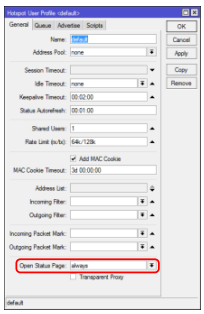

## Advertise

- To show advertise web-page after period of time
- Internet is blocked, if not shown
- Popup blockers can disturb advertise





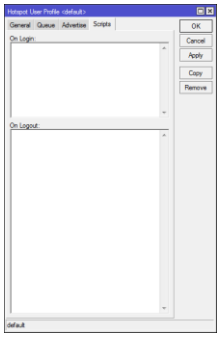

## Alternative Advertising



- Put the advertisement information to status page
- HTML knowledge required to modify alogin.html (status)
- Open-status page=always, shows status page for all clients

## Scripts

- Execute scripts on Hotspot user login and logout







## User Profile Lab

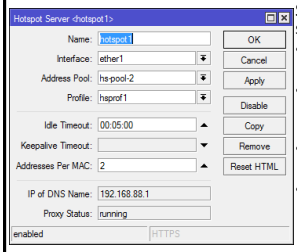
- Set max-limit=1M/2M limit-at=512k/1M priority=3 for every Hotspot user
- Log Hotspot users traffic in firewall chain=log
- Set static queue and make sure they are before dynamic all the time




## SERVER CONFIGURATION




## Hotspot server




Server's menu lists all Hotspot servers

- **Interface**, specifies interface Hotspot is configured on
- **Address-Pool**, Universal client for non-authorized clients
- **Timeouts**, timeouts for unauthorized clients
- **Addresses-Per-Mac**, number of IP addresses allowed per one MAC address

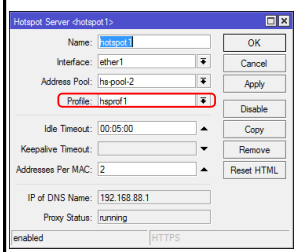



## Hotspot Server Lab

- Create Bridge on the router between Hotspot interface and unused interface
- Modify Hotspot servers settings appropriately



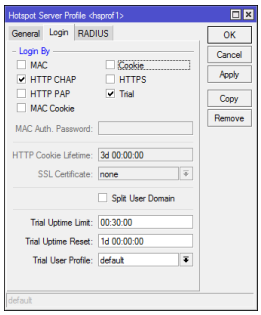

## Hotspot Server




- **Profile**, contains all settings for the Hotspot server

## Login

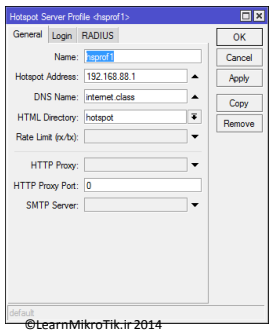
- Hotspot login method selection
- Additional authentication settings
- Trial User configuration







## Server Profile

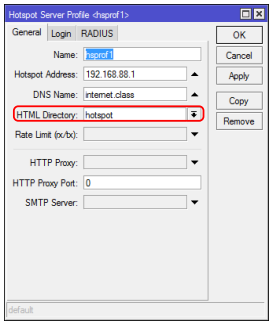



- **DNS name**, Hotspot server DNS name, use FQDN
- **Rate-Limit**, set bandwidth limit for the entire Hotspot server
- **HTTP proxy**, parent proxy settings
- **SMTP server**, to redirect e-mails to your mail server




## Hotspot Customization

- HTML-directory, sets location of the Hotspot server files
- Use FTP client to get Hotspot login page files





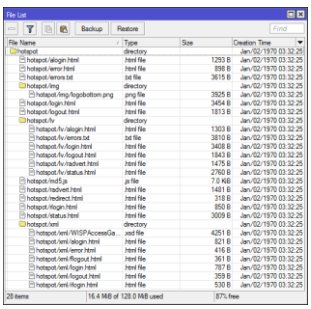


## Hotspot pages

- redirect.html - redirect users to another url
- login.html - login page shown to a user
- md5.js – Java script for MD5 password hashing
- status.html - statistics for the client
- logout.html - logout page
- error.html - error page
- You can put necessary information with basic HTML knowledge




## Customize Hotspot




- */ip hotspot reset-html <hotspotX>*, command to get back **default** login page




## Hotspot Profile Lab

- Set Trial Login on the Hotspot server
- Set DNS-Name for Hotspot, use it to login and logout
- Modify Hotspot page to login without login and password

## Previous Lab

- Get login.html page from ftp://router
- Open login.html with text editor




## Page Modifications

- Change two lines
  - <type="text" value="$(username)> to
    - <input type="hidden" name="username" value="yourname"?>
  - <input type="password">
    - <input type="hidden" name=password value="password">




## Login without password

- No login/password required
- Put advertising information or any information for user to accept
- Increase shared-users




## EXCEPTIONS




## Hotspot Exceptions

- Hotspot blocks connection to the Internet
- Servers, switches, telephony terminals perhaps do not have browser for the login
- There are few ways to bypass HotSpot authentication

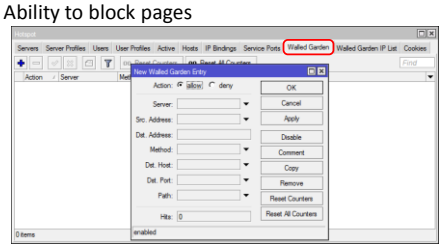



## Hotspot Walled-Garden

- 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.)

## Walled-Garden

- Access for HTTP and HTTPS pages without authentication
- Ability to block pages







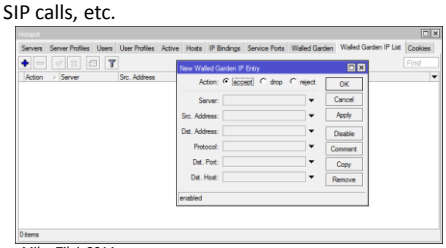
## Walled-Garden

- **Src. address**, Hotspot client address
- **Dst. address**, HTTP/HTTPs IP address
- **Dst. Host**, DNS name, example www.test.com
- **Path**, www.test.com/path




## Walled-Garden IP

- Bypass other services without authentication
- Bypass for protocols and ports, SSH, Telnet, Winbox, SIP calls, etc.





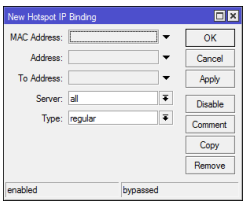


## IP Binding

- Allows full Hotspot bypass for the user
- Static Universal client (one-to-one NAT) translations
- Block unauthorized hosts or networks




## One-to-One NAT

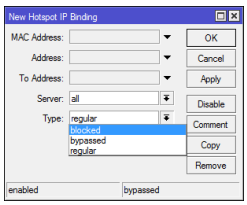



- **Address**, Hotspot client address
- **To Address**, new address of the Hotspot client




## IP Binding types

- **regular**, no action for the client
- **bypassed**, client is bypassed without authentication
- **blocked**, block access for the client or network



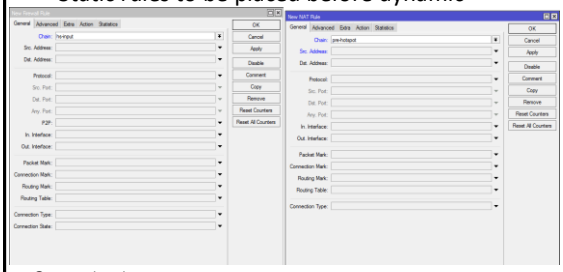
## Firewall rules

- Hotspot setup creates dynamic firewall rules
- Static rules are moved to the bottom after reboot
- Special chain available for placing static rules over dynamic




## Filter and NAT

- Static rules to be placed before dynamic






## Firewall rules

- Jump rules are red, because there is no rules in custom chain
- Red rules does not make any problem for HotSpot or firewall operation




## Exceptions lab

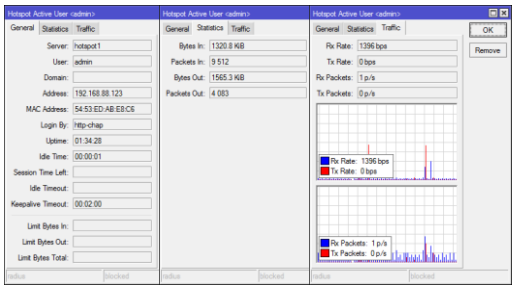
- Set **www.mikrotik.com** without authentication
- Set **SSH** without authentication
- Block **Telnet** for all Hotspot users
- Set access for Hotspot **only** for users with local network IP address




## ACCOUNTING




## Accounting



# SNMP

- Information provided by SNMP