

UserManager: a free radius server for Wireless, Hotspot, PPP, users and DHCP. (UserManager PlayBook)

by Lorenzo Busatti

DENMARK ON MAY 27, 2016



About me

Lorenzo Busatti

- Founder of Grifonline S.r.l. [ISP] (1997)
- Founder of Linkwave [WISP] (2006)
- MikroTik Trainer [NA,RE,WE,TCE,INE,UME](2010)
- Member of RIPE, AMS-IX, MIX-IT



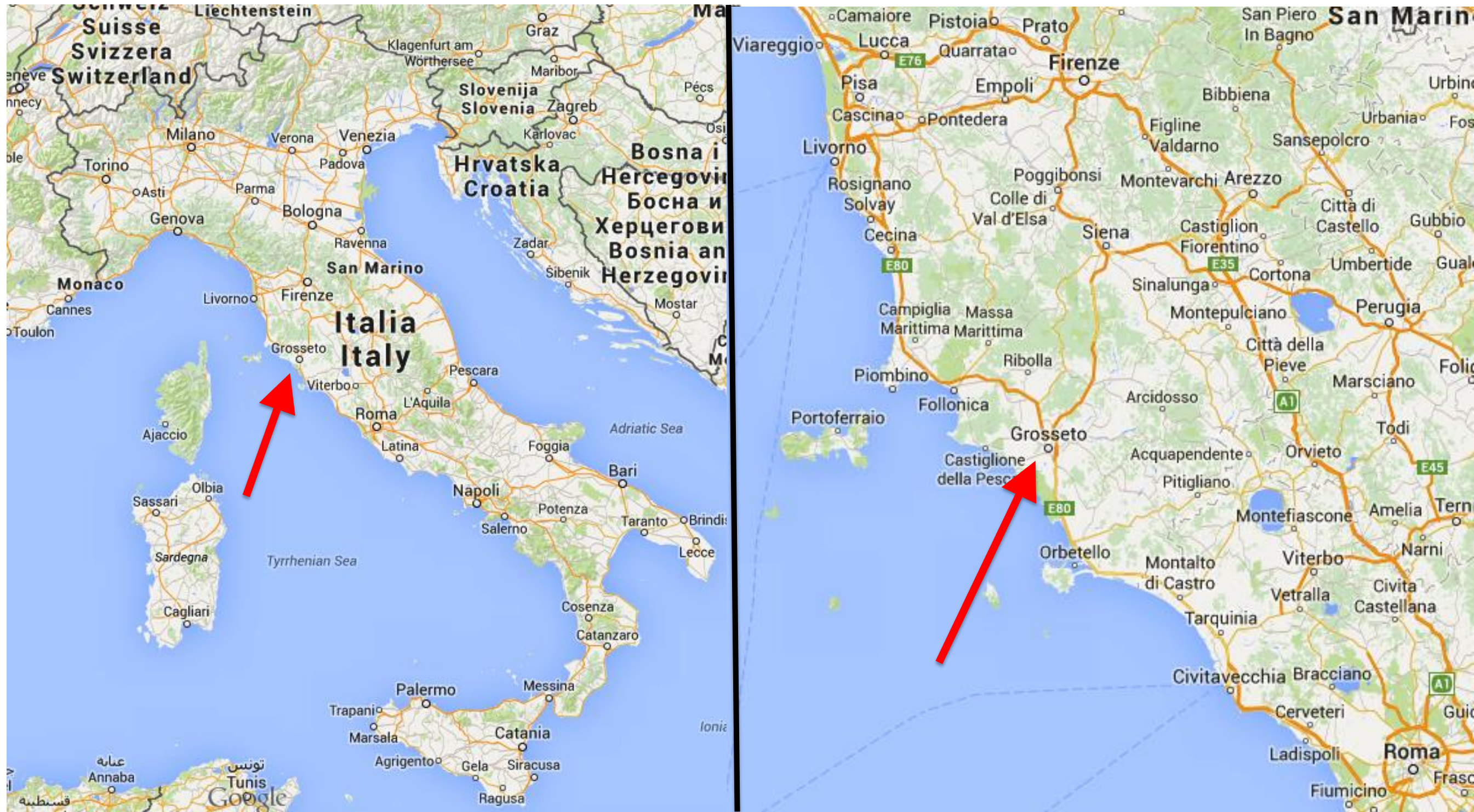
About me

Lorenzo Busatti

- Worldwide Trainer and Consultant, previous experiences in:
- Italy, USA, UnitedArabEmirates, Brasil, Slovenia, Poland, Croatia, Czech Republic, etc



About me





I'm a MikroTik *evangelist*

About me

- Founder (2016) of the



**Non Profit Organization for
High Quality Training Partners**

Dedicated to Max

The UserManager

- Additional “package” for RouterOS;
- A powerful radius server that can be used for managing authentication in:
 - ✓ Hotspot
 - ✓ PPP
 - ✓ RouterOS Users
 - ✓ Wireless
 - ✓ DHCP server

The UserManager

And it's free.



Why this presentation?

Doing trainings the students are used to ask info about radius servers.

The UserManager is not well known

There are reasons for not to use a radius included in RouterOS for free?

Why this presentation?

Is also not well known where RouterOS can ask authentication at a radius server:

Most used:

Hotspot

PPP

Not well known:

RouterOS Users

Wireless *(and in the CAPsMAN)*

DHCP server



Why this presentation?

And now **the** question:

How many are using the
UserManager?

My style

1. I don't have "hours" into the time slot
2. I don't like "boring" presentations

So

- I'll not show you ALL the things about the UserManager (will not be possible);
- You can use the wiki.mikrotik.com
- You can take the MTCUME training class



RADIUS server

The UserManager is a radius server.

Remote Authentication Dial-In User Service

Is a networking protocol that provides
centralized:

Authentication, Authorization, and Accounting (AAA or Triple A), using UDP packets.

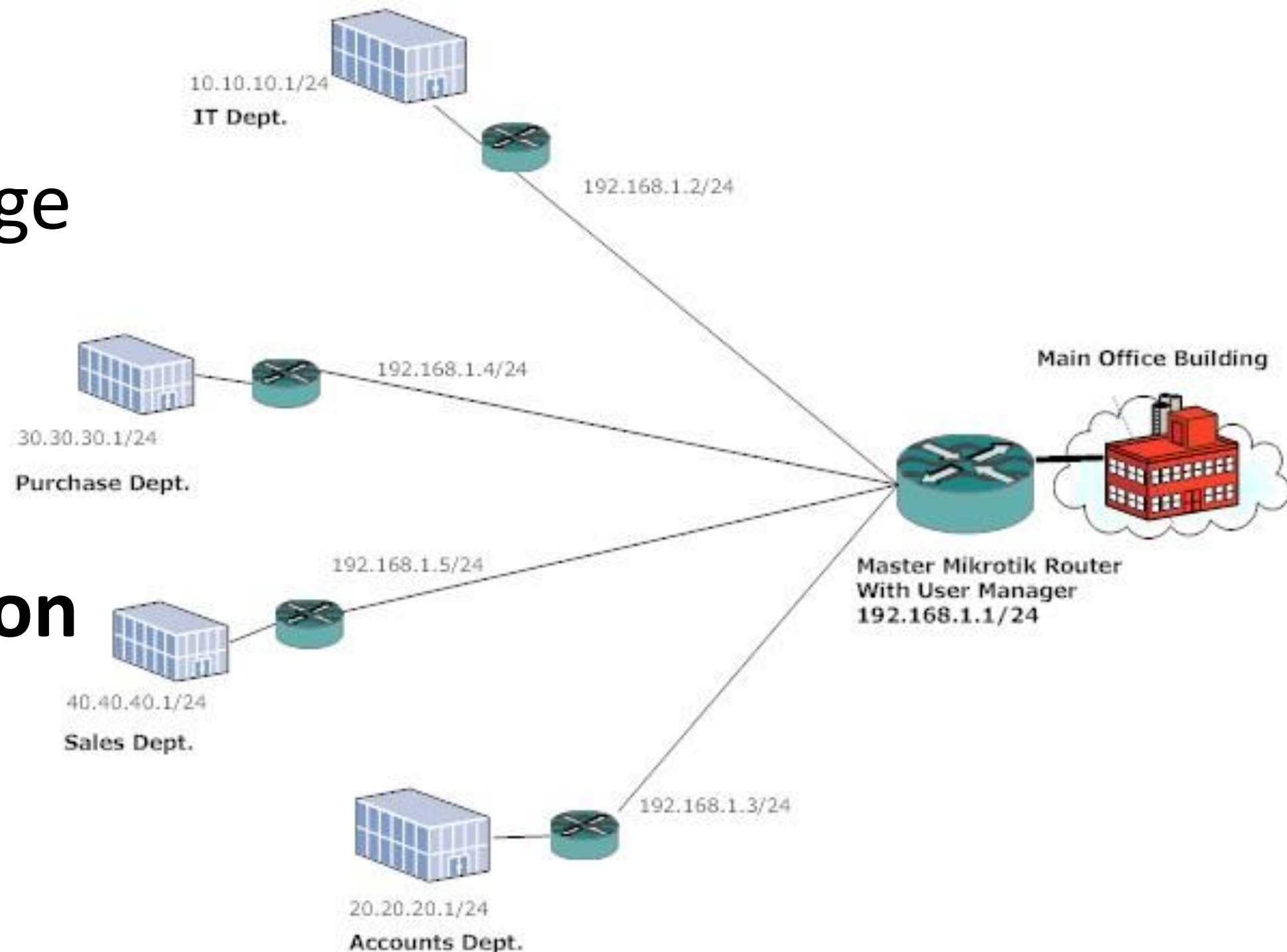
RADIUS server

He will allow

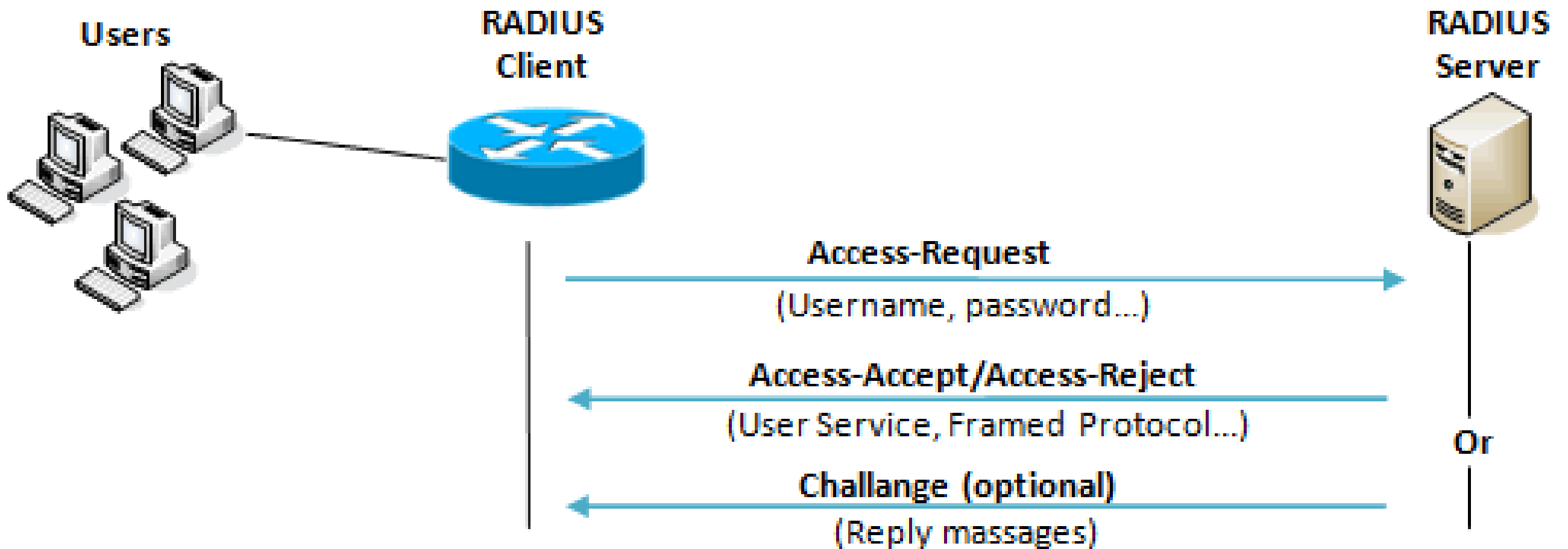
You to manage

Centralized

authentication



RADIUS server

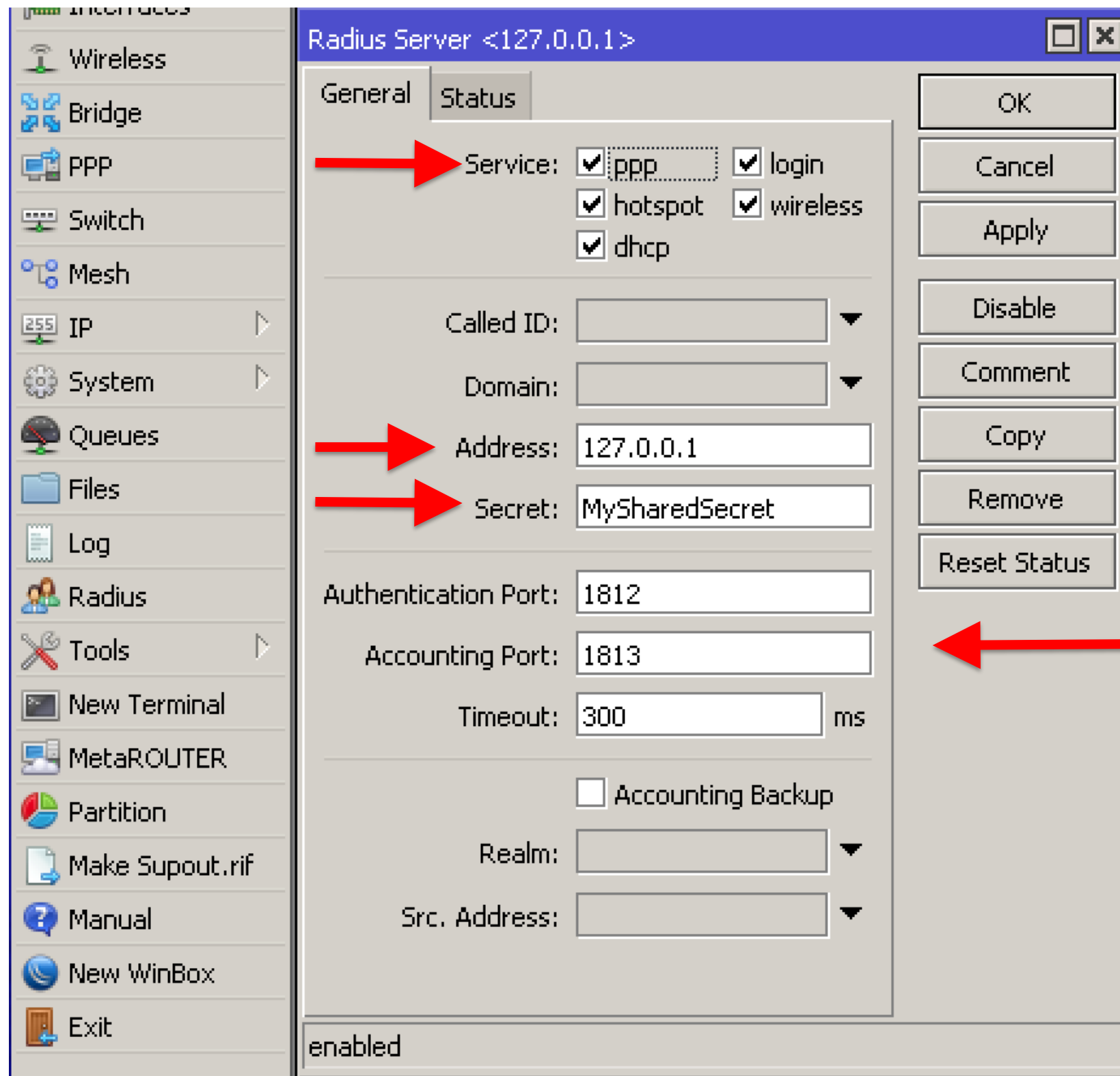


RADIUS client

- RouterOS have a radius client, included in the system;
- Don't require optional packages or special licenses;
- Can ask authentication at ANY standard radius server.
- It's free



RADIUS client



RADIUS client

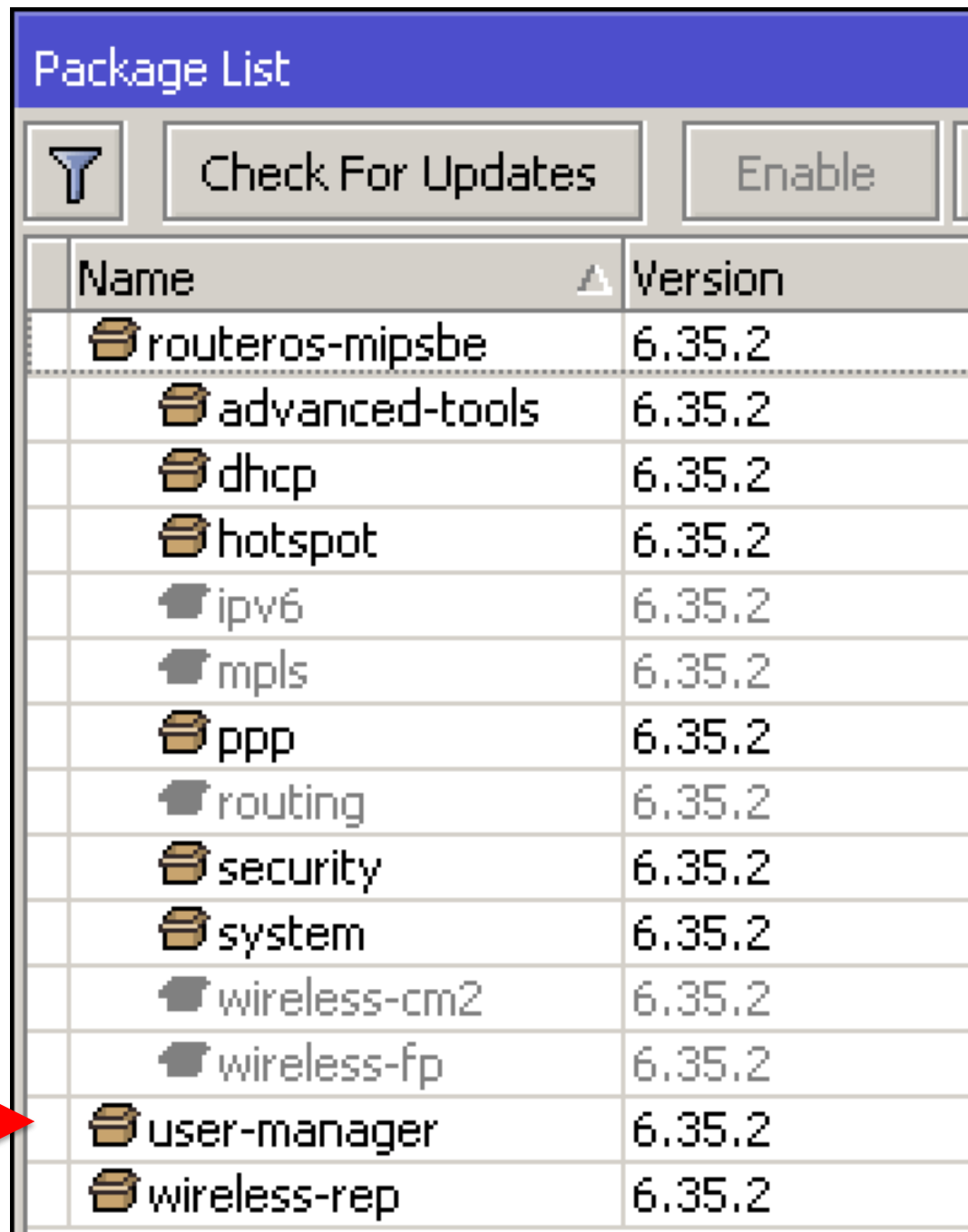
The rules of thumb is:

- RouterOS will use the **LOCAL** users database **FIRST**;
- **THEN** will ask at a **RADIUS** server (if set)

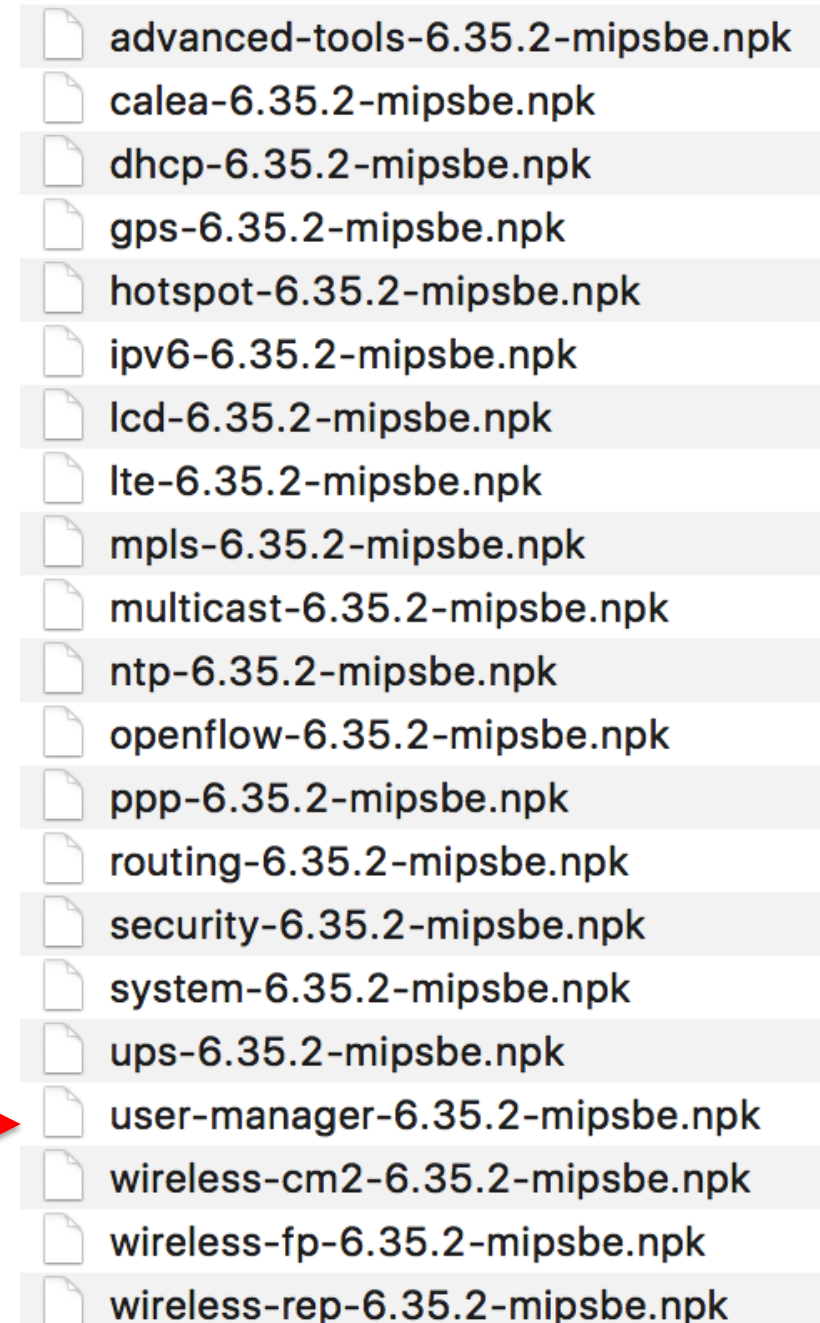


Where is the UserManager?

You have to manually install this optional package:



Name	Version
routeros-mipsbe	6.35.2
advanced-tools	6.35.2
dhcp	6.35.2
hotspot	6.35.2
ipv6	6.35.2
mpls	6.35.2
ppp	6.35.2
routing	6.35.2
security	6.35.2
system	6.35.2
wireless-cm2	6.35.2
wireless-fp	6.35.2
user-manager	6.35.2
wireless-rep	6.35.2

- 
- advanced-tools-6.35.2-mipsbe.npk
 - calea-6.35.2-mipsbe.npk
 - dhcp-6.35.2-mipsbe.npk
 - gps-6.35.2-mipsbe.npk
 - hotspot-6.35.2-mipsbe.npk
 - ipv6-6.35.2-mipsbe.npk
 - lcd-6.35.2-mipsbe.npk
 - lte-6.35.2-mipsbe.npk
 - mpls-6.35.2-mipsbe.npk
 - multicast-6.35.2-mipsbe.npk
 - ntp-6.35.2-mipsbe.npk
 - openflow-6.35.2-mipsbe.npk
 - ppp-6.35.2-mipsbe.npk
 - routing-6.35.2-mipsbe.npk
 - security-6.35.2-mipsbe.npk
 - system-6.35.2-mipsbe.npk
 - ups-6.35.2-mipsbe.npk
 - user-manager-6.35.2-mipsbe.npk**
 - wireless-cm2-6.35.2-mipsbe.npk
 - wireless-fp-6.35.2-mipsbe.npk
 - wireless-rep-6.35.2-mipsbe.npk

Requirements

You can install the UserManager in any RouterBoard with at least 32MB RAM and 2MB free space.

Will work on x86 or CHR also.





Licensing

The UserManager is free, but have different limitations depending your RouterOS license level:

	L3 (CPE)	L4 (WISP)	L5 (WISP)	L6 (Controller)
Max active sessions	10	20	50	Unlimited



The web interface

The screenshot displays the Mikrotik User Manager web interface in a browser window. The browser's address bar shows the URL `192.168.200.1/userman`, with a red arrow pointing to it. The page title is "Mikrotik User Manager: Users". The interface includes a sidebar with navigation options: Routers, Users (selected), Sessions, Customers, Logs, Payments, Profiles, Settings, Reports, 0 A sessions, 0 A users, Advanced search, Maintenance, and Logout. The main content area features a header with "Add", "Edit", and "Generate" buttons, a search bar, and a table with columns: Username, Till time, Total time left, and Actual profile. A "Per page [20]" dropdown is also visible. The table currently contains one row with a checkmark in the first column.

The CLI interface

```
/tool user-manager>
```

```
customer    database    history
```

```
log    payment    profile    router
```

```
session    user    export
```



The User Guide

http://wiki.mikrotik.com/wiki/Manual:User_Manager

Manual:User Manager

(Redirected from [User Manager](#))

Contents [\[hide\]](#)

- 1 Introduction
- 2 Getting started
- 3 Quick start
- 4 Concepts explained
 - 4.1 Common
 - 4.2 Version 4.x test package specific
 - 4.3 Version 3.x specific
- 5 Reference
 - 5.1 Web interface
 - 5.2 Customer page
 - 5.3 User page
 - 5.4 User sign-up
 - 5.5 User payments
 - 5.6 Backup and restore
- 6 Questions and answers



Tips

Don't forget:

- To change the UserManager default password
- That all the users/customers of the UserManager are not shared into RouterOS
- To add routers to be managed
- To create PROFILES (and limitations) BEFORE adding Users

Tips

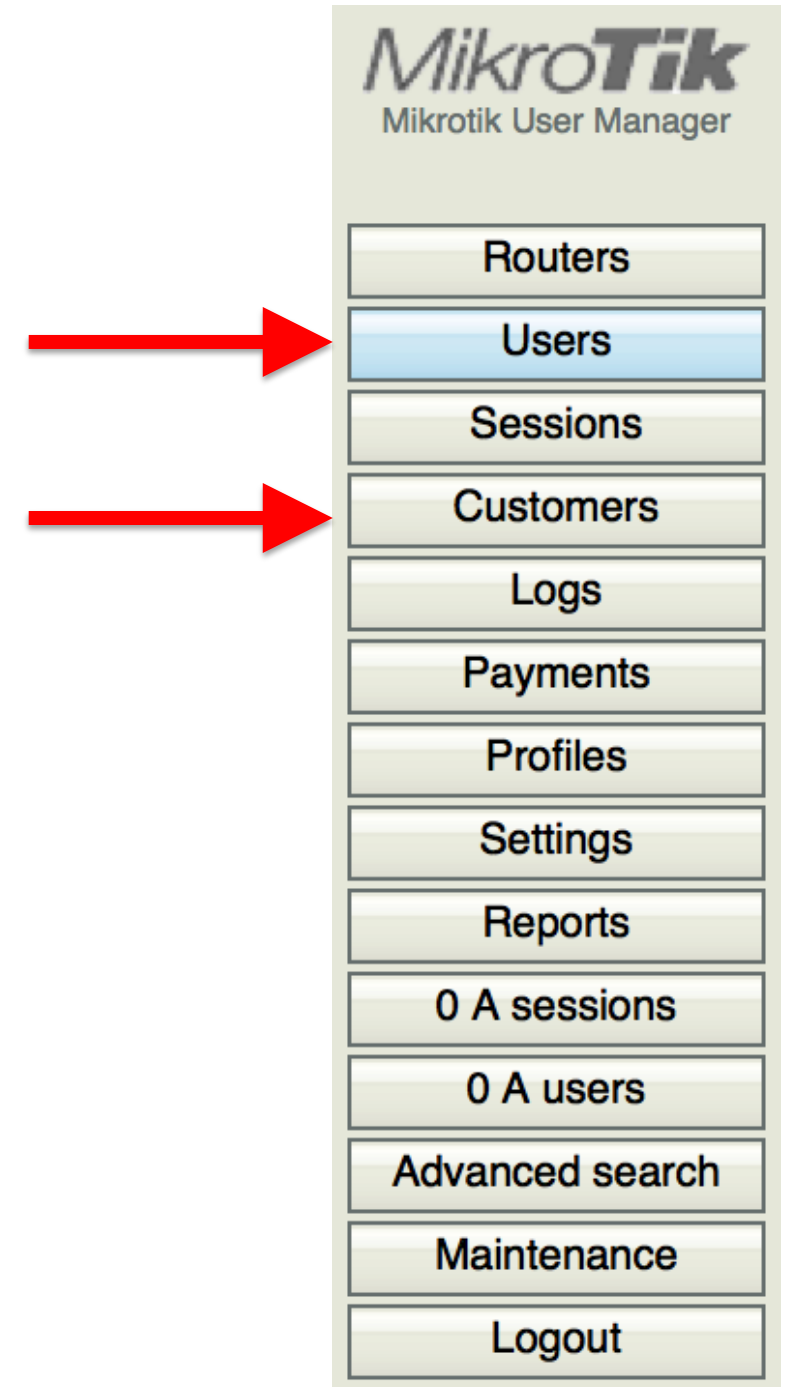
Don't mess up between Users and Customers:

Users

The **users** the Userman will authenticate

Customers

The Userman **administrators**



PPP Services

PPP

Interface | PPPoE Servers | **Secrets** | Profiles | Active Connections | L2TP Secrets

+ - ✓ ✗ [Icon] [Icon] **PPP Authentication & Accounting** ←

Name	Password	Service	Caller ID	Profile	Local Address
0 items					

PPP Authentication & Accounting

Use Radius ←

Accounting

Use Circuit ID in NAS Port ID

Interim Update: [] ▾

OK

Cancel

Apply

PPP Services

Enabling the radius client for the PPP services will be used by ALL the PPP services:

PPPoE, PPTP, L2TP, OVPN, SSTP

You can easily manage VPN authentication via one radius server.

Centralized Management of VPN Servers.

Tips

Radius attributes (replied to the client) will override settings into the Profiles in RouterOS.

PPP Profile <default>

General Protocols Limits Queue Scripts

Session Timeout: []

Idle Timeout: []

Rate Limit (rx/tx): 2M/2M

— Only One —

no yes default

OK Cancel Apply Comment Copy Remove

MikroTik MikroTik User Manager

Routers Users Sessions Customers Logs Payments Profiles Settings Reports 0 A sessions 0 A users Advanced search Maintenance Logout

Profiles Limitations

Profile: profile1

Name: profile1

Name for users: []

Owner: admin

Validity: []

Starts: At first logon

Price: 0.00

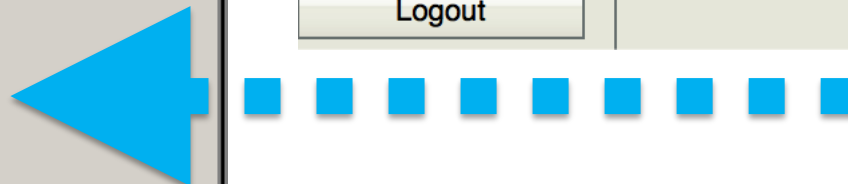
Shared users: not used

Save profile Remove profile

Profile limitations

<input type="checkbox"/>	Active	Constraints
<input type="checkbox"/>	Always	Rate limits: 1M/1M 0/0 0/0 0/0 0 1M/1M

Add new limitation Remove selected limitations



PPP Profile's limitations

Limitation details ✕

▲ Main

Name:

Owner: admin

▲ Limits

Download:

Upload:

Transfer:

Uptime:

▲ Rate limits

Rate limit: Rx	<input type="text"/>	Tx	<input type="text"/>
Burst rate: Rx	<input type="text"/>	Tx	<input type="text"/>
Burst threshold: Rx	<input type="text"/>	Tx	<input type="text"/>
Burst time: Rx	<input type="text"/>	Tx	<input type="text"/>
Min rate: Rx	<input type="text"/>	Tx	<input type="text"/>

Priority:

▲ Constraints

Group name:

IP pool:

Address list:

Group name:

“/user group” for RouterOS users

“/user profile” for HotSpot users



HotSpot Services

The screenshot displays the 'Hotspot' configuration interface. At the top, there are several tabs: 'Servers', 'Server Profiles', 'Users', 'User Profiles', 'Active', 'Hosts', 'IP Bindings', and 'Services'. A red arrow points to the 'Servers' tab. Below the tabs, there are three icons: a plus sign, a minus sign, and a funnel. A table below shows the following data:

Name	DNS Name	HTML Directory	Rate Limit (rx/tx)
default		hotspot	

Below the table, a dialog box titled 'Hotspot Server Profile <default>' is open. It has three tabs: 'General', 'Login', and 'RADIUS'. A red arrow points to the 'RADIUS' tab. The 'RADIUS' tab contains the following settings:

- Use RADIUS
- Default Domain: [Empty]
- Location ID: [Empty]
- Location Name: [Empty]
- MAC Format: XX:XX:XX:XX:XX:XX
- Accounting
- Interim Update: [Empty]
- NAS Port Type: 19 (wireless-802.11)

On the right side of the dialog box, there are five buttons: 'OK', 'Cancel', 'Apply', 'Copy', and 'Remove'. A small '1' is visible in the bottom-left corner of the dialog box.



HotSpot Services

With the radius you can easily manage tons of hotspots with just one user DB.



Centralized Management of HotPot Servers.

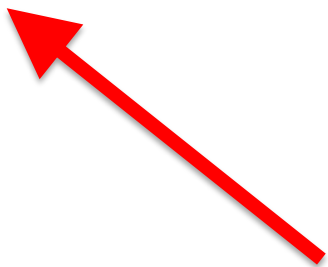
RouterOS Users

One of my favourite Radius client apps.

A question for you:

Do you think is possible to disconnect a RouterOS user from Winbox or CLI ?

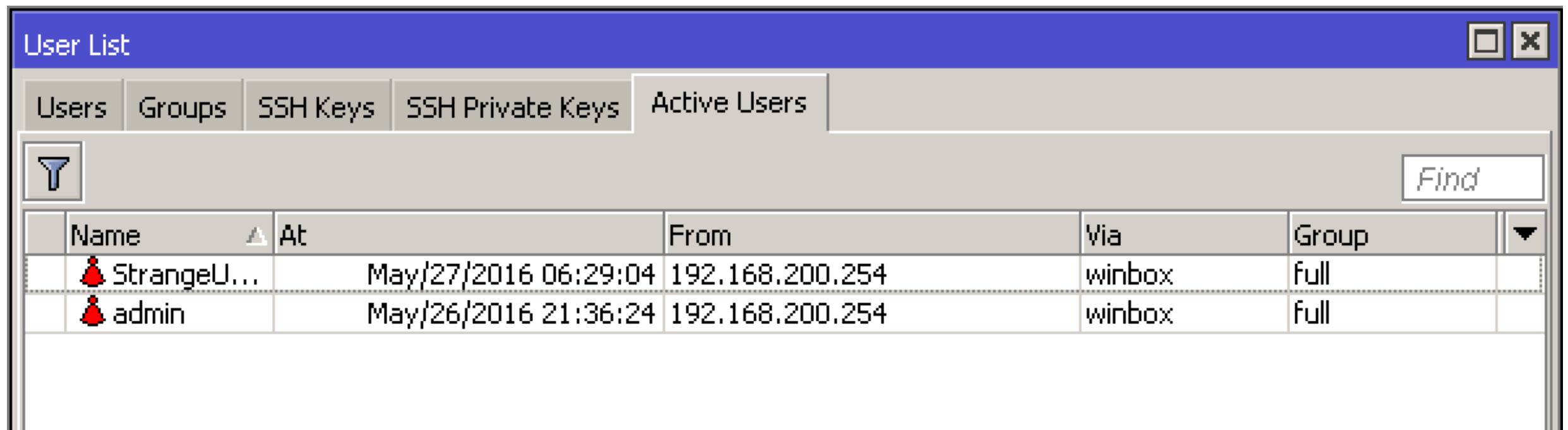
Name	At	From	Via	Group
 admin	May/26/2016 21:36:24	192.168.200.254	winbox	full
 StrangeUser	May/27/2016 06:27:18	192.168.200.254	winbox	full



RouterOS Users

No!

Once connected you can't disconnect them.



The screenshot shows the 'User List' window in RouterOS WinBox. The window has a blue title bar and a tabbed interface with 'Active Users' selected. A search bar with a 'Find' button is located above the table. The table lists two active users:

Name	At	From	Via	Group
StrangeU...	May/27/2016 06:29:04	192.168.200.254	winbox	full
admin	May/26/2016 21:36:24	192.168.200.254	winbox	full

RADIUS client - incoming

The screenshot shows a 'Radius' window with a table of clients. The 'Incoming' button is highlighted with a red arrow. A 'Radius Incoming' dialog box is open, showing configuration options for the selected client. Red arrows point to the 'Accept' checkbox and the 'Port' field.

#	Service	Called ID	Domain	Address	Secret
0	ppp login hotspot wire...			127.0.0.1	MySharedSe...

Radius Incoming

Accept

Port: 1700

Requests: 0

Bad Requests: 0

Acks: 0

Naks: 0

Buttons: OK, Cancel, Apply, Reset Status

1 item

RADIUS client - incoming

Router details ✕

▼ Main

Name: localhost

Owner: admin

IP address: 127.0.0.1

Shared secret: MySharedSecret

Time zone: Parent time zone

Disabled:

Log events: Authorization success
 Authorization failure
 Accounting success
 Accounting failure

▲ Radius incoming

CoA support:

CoA port: 1700

▼ Request statistics

Save



RouterOS Users

The screenshot shows the RouterOS 'User List' interface. At the top, there are tabs for 'Users', 'Groups', 'SSH Keys', 'SSH Private Keys', and 'Active Users'. Below the tabs is a toolbar with icons for adding (+), removing (-), checking (✓), unchecking (✗), deleting (trash), filtering (funnel), and a button labeled 'AAA'. A red arrow points to the 'AAA' button. Below the toolbar is a table with columns: Name, Group, Allowed Address, and Last Log. The table contains two entries: ';; system default user' and 'admin' (with a red tree icon) in the 'Group' column, 'full' in the 'Group' column, and empty cells for 'Allowed Address' and 'Last Log'.

Overlaid on the bottom right is a dialog box titled 'Login Authentication & Accounting'. It has a blue header bar with a close button (X). The dialog contains several options: 'Use RADIUS' (checked), 'Accounting' (checked), 'Interim Update:' (with a dropdown arrow), 'Default Group:' (with a text field containing 'read' and a dropdown arrow), and 'Exclude Groups:' (with a dropdown arrow). On the right side of the dialog are three buttons: 'OK', 'Cancel', and 'Apply'. A red arrow points to the 'Use RADIUS' checkbox.

DHCP Server

Is possible to use the radius for managing DHCP lease by DHCP servers.

Centralized Management of DNS Servers.

DHCP Server

DHCP Server <dhcp1>

Name:

Interface:

Relay:

Lease Time:

Bootp Lease Time:

Address Pool:

Src. Address:

Delay Threshold:

Authoritative:

Bootp Support:

Lease Script:

Add ARP For Leases

Always Broadcast

Use RADIUS

enabled

OK


Cancel

Apply

Disable

Copy

Remove



DHCP Server

User details

▲ Main

Username: 4C:5E:0C:CA:1A:B8

Password:

Disabled:

Owner: admin

▲ Constraints

IP address: 192.168.200.2

Bind on first use

Caller ID:

Shared users: 1

▼ Wireless

▼ Private information

Assign profile: profile1

Add



Wireless Clients

Is possible to use the radius for managing Wireless Clients connecting to an AP.

Will work “against” Access List.

Centralized Management of Wireless Clients.

(and will be possible to disconnect them **by** the radius)

Wireless Clients

New Security Profile

General **RADIUS** EAP Static Keys

MAC Authentication

MAC Accounting

EAP Accounting

Interim Update: 00:00:00

MAC Format: XX:XX:XX:XX:XX:XX

MAC Mode: as username

MAC Caching Time: disabled

OK
Cancel
Apply
Copy
Remove



Wireless Clients

User details

▲ Main

Username: 4C:5E:0C:CA:1A:B8

Password:

Disabled:

Owner: admin

▼ Constraints

▼ Wireless

▼ Private information

Assign profile: profile1

Add



Wireless Clients

User details ✕

▲ Main

Username: 4C:5E:0C:CA:1A:B8

Password:

Disabled:

Owner: admin

▼ Constraints

▲ Wireless

Preshared key: aKeyForThisWirelessClient

Enc key:

Enc algo: AES-CCM

▼ Private information

Assign profile: profile1

Add



CAPsMAN Wireless Clients

Is possible to use the radius for managing Wireless Clients connecting to an AP managed by a CAPsMAN.

(and will be possible to disconnect them **by** the radius)

CAPsMAN Wireless Clients

In this case the radius server will be query by a **CAPs Access List rule**:

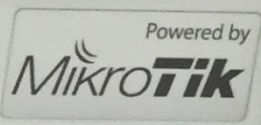
The screenshot shows the CAPsMAN configuration interface. The 'Access List' tab is selected, as indicated by a red arrow. Below the tab is a toolbar with icons for adding, deleting, and filtering rules. A table with columns for '#', 'MAC Address', 'MAC Mask', 'Interface', 'Signal Ra...', 'Action', and 'Client' is visible. Overlaid on this is a 'New CAPs Access Rule' dialog box. The dialog box contains fields for 'MAC Address', 'MAC Mask', 'Interface', 'SSID Regexp', and 'Signal Range'. The 'Action' dropdown is set to 'query radius', highlighted by a red arrow. Other buttons in the dialog include 'OK', 'Cancel', 'Apply', 'Disable', 'Comment', 'Copy', and 'Remove'.

The power of RouterOS

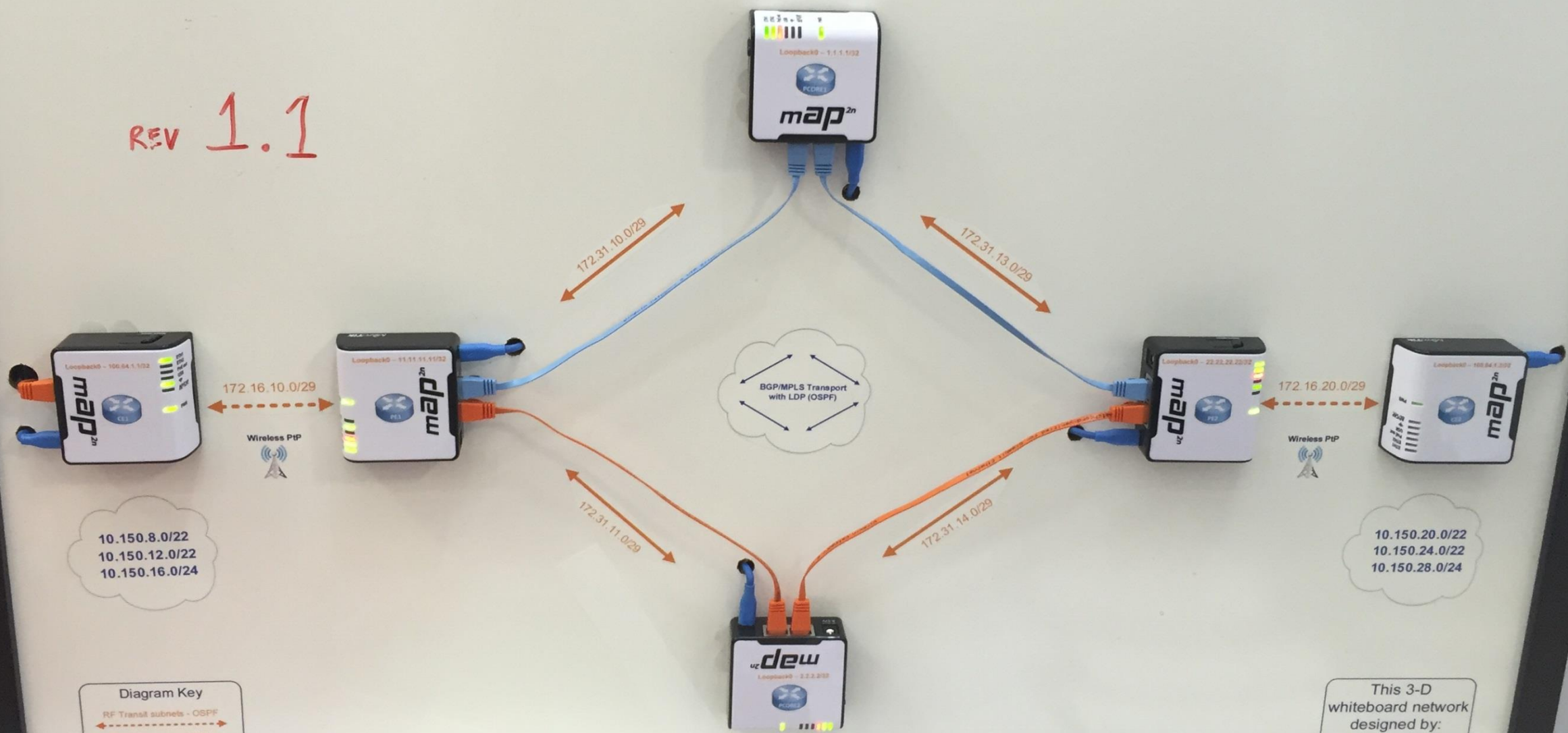
- ALL the functions and his POWER into small devices also!
- APs, firewall, traffic shaper, hotspot, ospf, ... and also MPLS, BGP and the usermanager!
- Awesome!



WORLD'S SMALLEST MPLS ISP

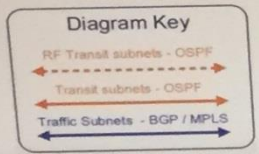


REV 1.1



10.150.8.0/22
10.150.12.0/22
10.150.16.0/24

10.150.20.0/22
10.150.24.0/22
10.150.28.0/24



This 3-D whiteboard network designed by:
ArchiTechs
MANAGED SERVICES



An LSA Type 6 packet walks into a bar and asks the bartender for a drink.

PACKETS

FRAMES

Wrap up

- ✓ I hope you enjoyed my presentation;
- ✓ And from today you'll start to increase to use the UserManager more than before 😊

Thank you!

Q & A

<http://training.grifonline.it>
training@grifonline.it