

A decorative horizontal bar featuring a repeating pattern of white and blue squares, resembling a binary code or digital data stream.



1010101010101010101010101

Par reči o predavaču

- IT/IS Manager u Algotech d.o.o.
- U IT industriji od 1991. godine
- Usmerenje ka Windows poslovnim mrežama i bezbednosti informacija
- Sertifikati za Microsoft, CompTIA, NICE
- Autor dve knjige o mrežama
- Sa Mikrotik ruterima radi od 2005. godine
- Fokus na kontroli pristupa i automatizaciji rada

O čemu ćemo pričati

- Kontrola pristupa resursima i protoka saobraćaja
- Upravljanje mrežama sa stalnim i povremenim korisnicima
- Odgovor – Mikrotik HotSpot i Mikrotik User Manager



Mikrotik HotSpot

Šta je Mikrotik HotSpot?

- Mikotik HotSpot je servis koji upravlja pristupom mrežnim lokacijama i resursima van lokalne mreže
- Ne obezbeđuje zaštitne funkcije kao što je šifrovanje saobraćaja
- Nema potrebe za klijentskom aplikacijom
- HotSpot servis može da kontroliše sledeće interfejse:
 - Ethernet portovi (bakar/optika)
 - Wireless kartice (bežične mreže)
 - Bridge interfejsi (na nivou celog bridža)

Kako vrši funkciju?

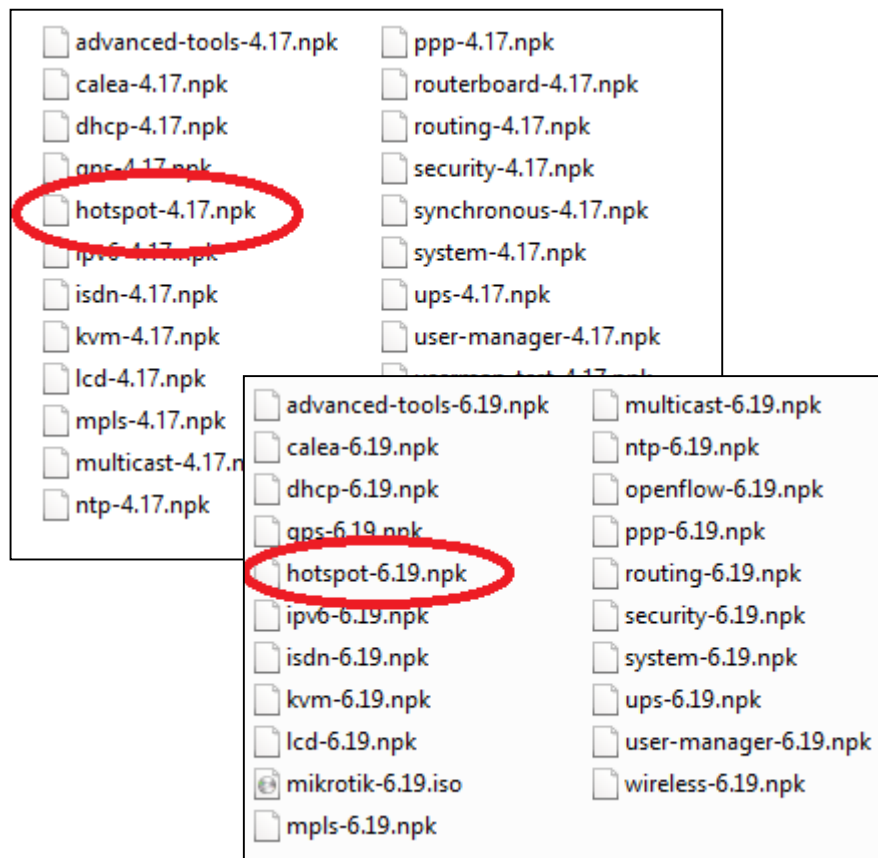
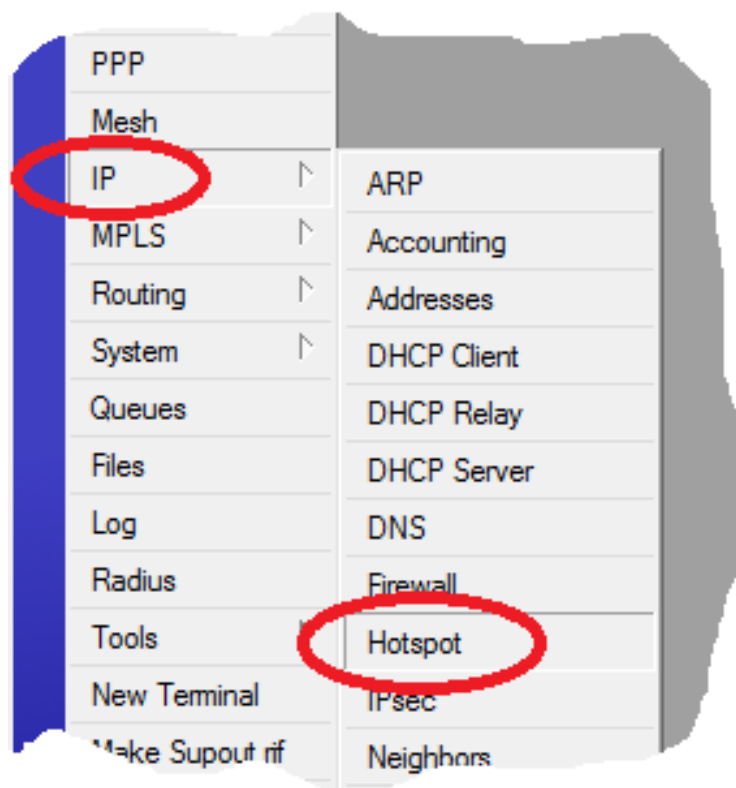
- Gejtvej vrši identifikaciju korisnika prilikom prve HTTP ili HTTPS sesije iz bilo kog pretraživača na bilo kom operativnom sistemu
- Gejtvej upravlja korisničkim nalozima, vremenima sesija, dozvolama pristupa
- Nalozi mogu da budu u lokalnoj bazi ili na RADIUS serveru
- Može da kontrolišete protok saobraćaja na nivou porta ili korisnika

Gde možemo da upotrebimo ovo rešenje?

- Svuda!
- Verzija RouterOS-a nije bitna
- Potencijalni korisnik je svako ko ima potrebe za nekim vidom kontrole mrežnog pristupa
- Probni režim daje dodatne mogućnosti korisniku

Gde se nalazi HotSpot?

- Svi RouterBOARD-ovi od verzije 3.x imaju preinstaliran HotSpot
- x86 verzija zahteva da se ovaj servis instalira kao poseban paket



- HotSpot i User Manager zahtevaju sledeće licencne nivoe:

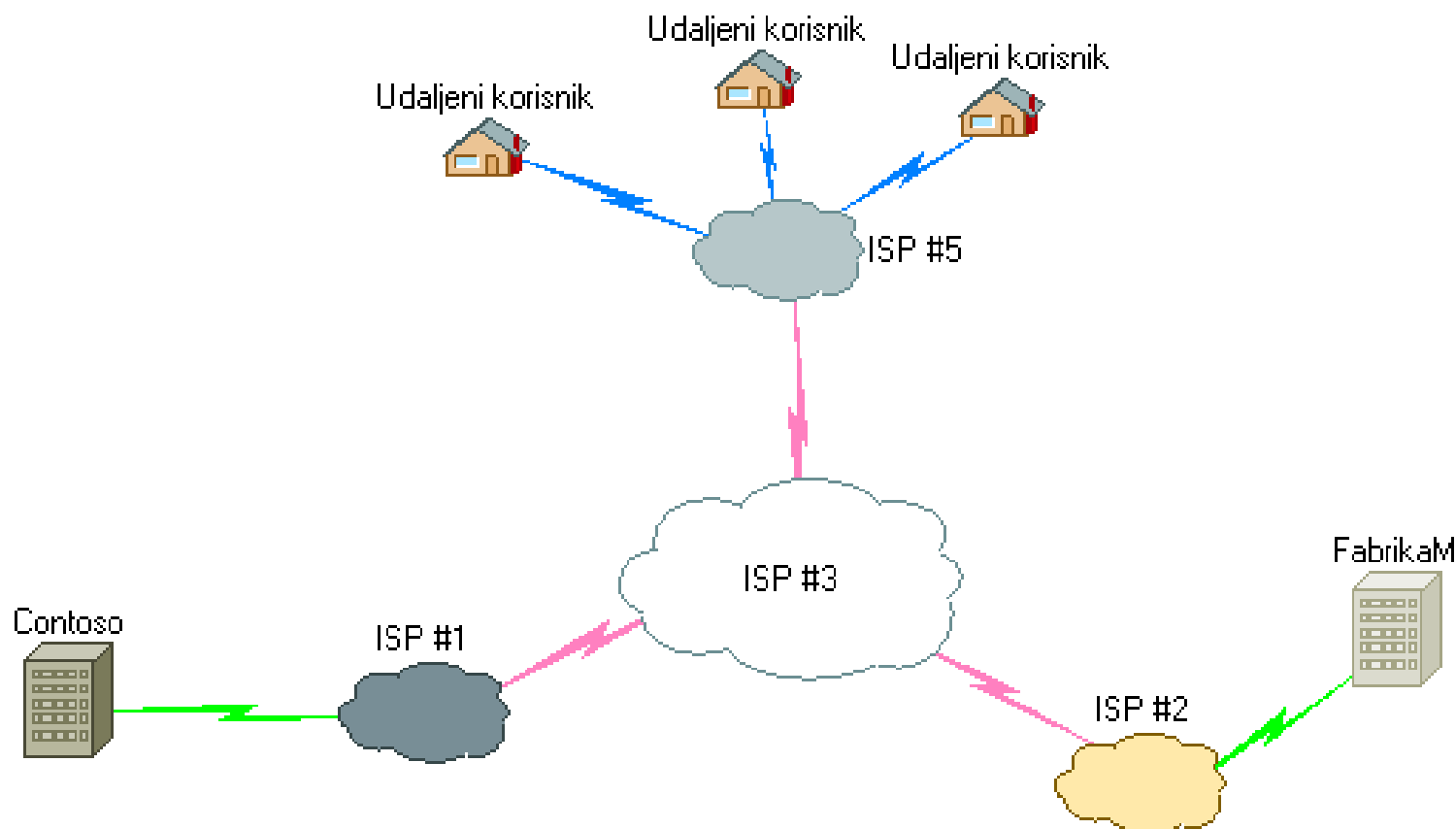
<i>Nivo (level)</i>	<i>HotSpot</i>	<i>User Manager</i>
<i>0 (24h demo)</i>	<i>Bez ograničenja</i>	<i>Bez ograničenja</i>
<i>1 (demo)</i>	<i>nema</i>	<i>nema</i>
<i>3 (CPE)</i>	<i>1</i>	<i>10</i>
<i>4</i>	<i>200</i>	<i>20</i>
<i>5</i>	<i>500</i>	<i>50</i>
<i>6</i>	<i>Bez ograničenja</i>	<i>Bez ograničenja</i>



Naša laboratorija

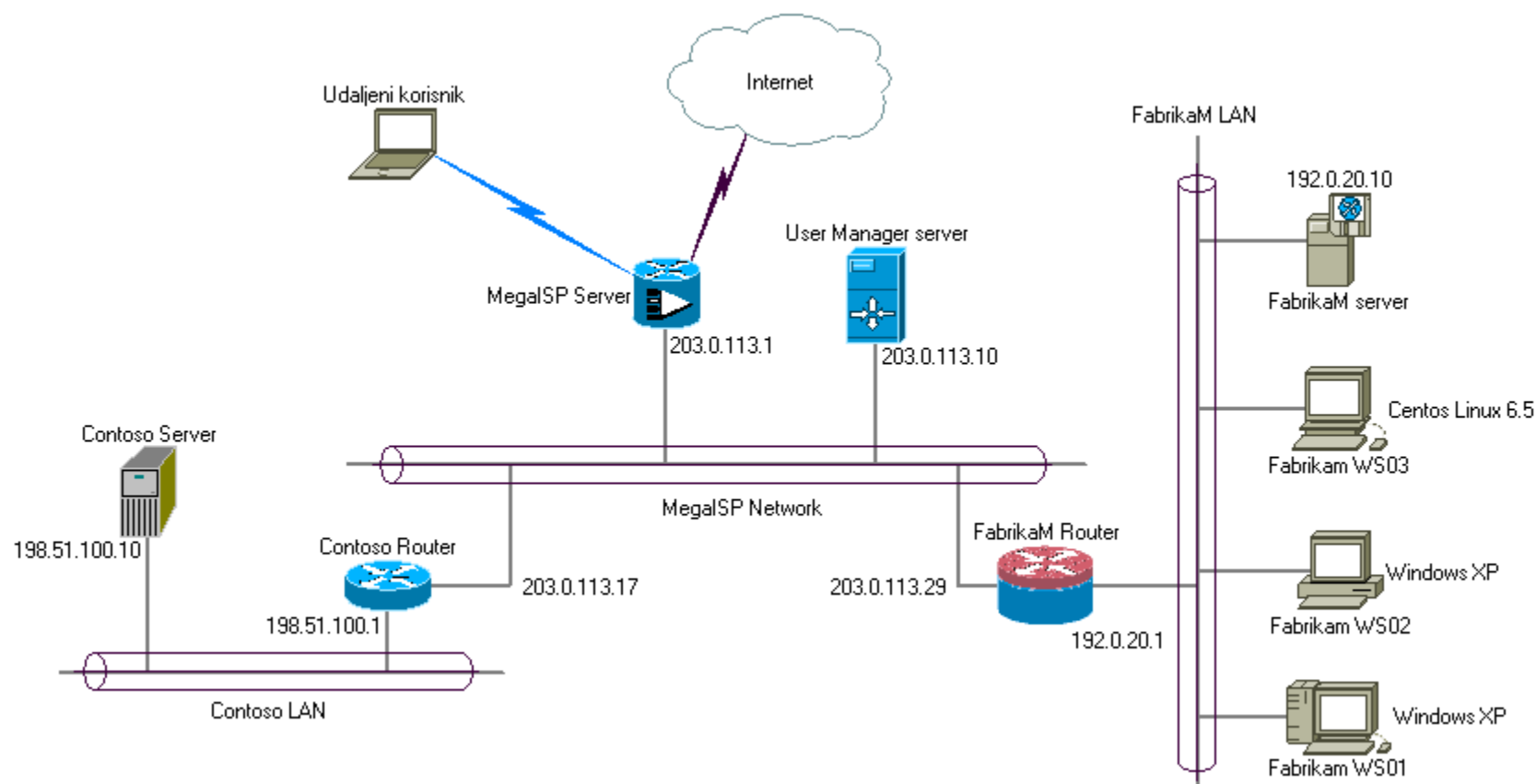
Scenario koji simuliramo

- Simulirali smo povezivanje više organizacija i ISP-ova



Naša laboratorija

- Sve funkcije smo simulirali u virtuelnom okruženju

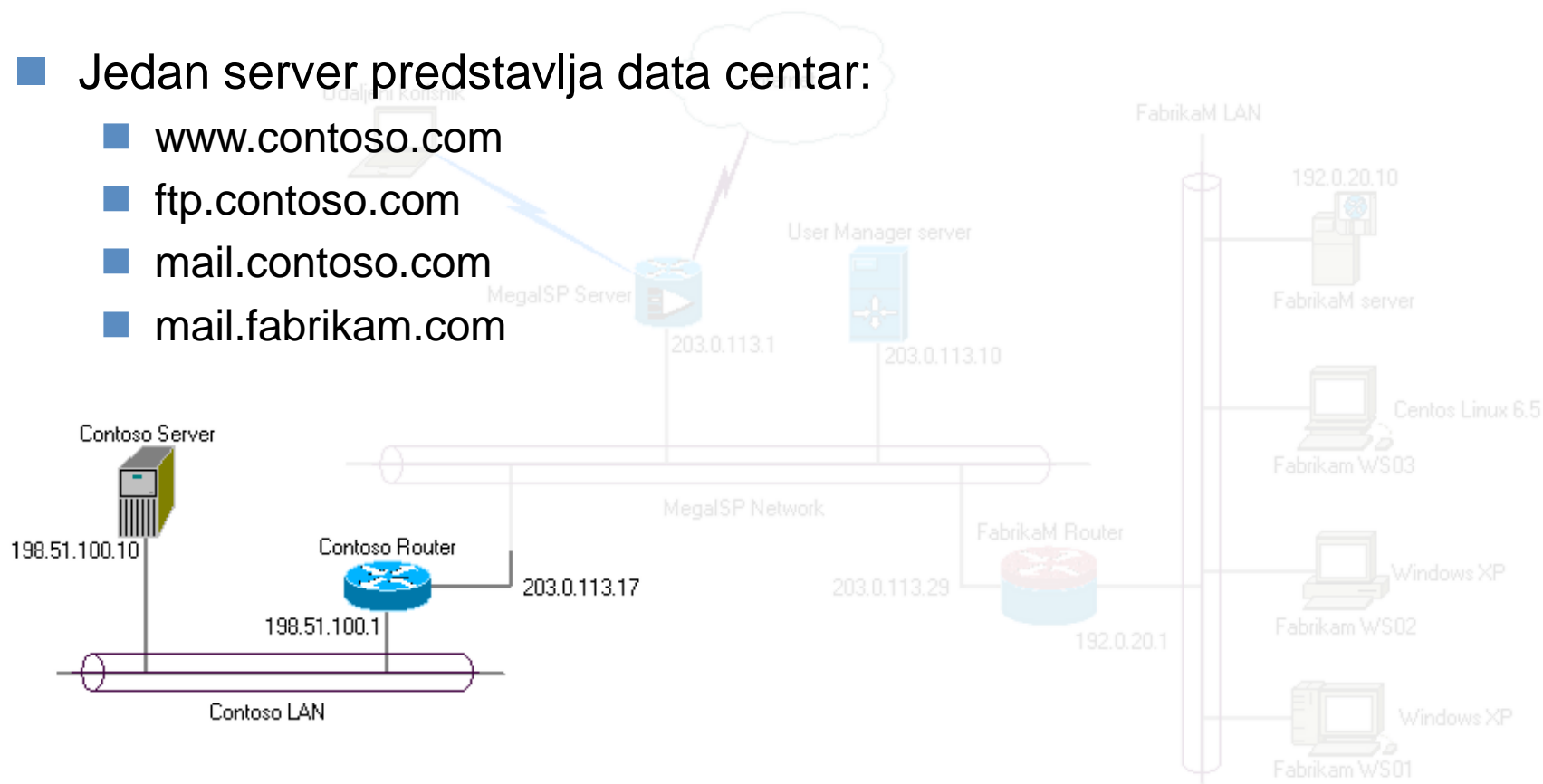


Mreža Contoso

■ „Mother“

■ Jedan server predstavlja data centar:

- www.contoso.com
- ftp.contoso.com
- mail.contoso.com
- mail.fabrikam.com



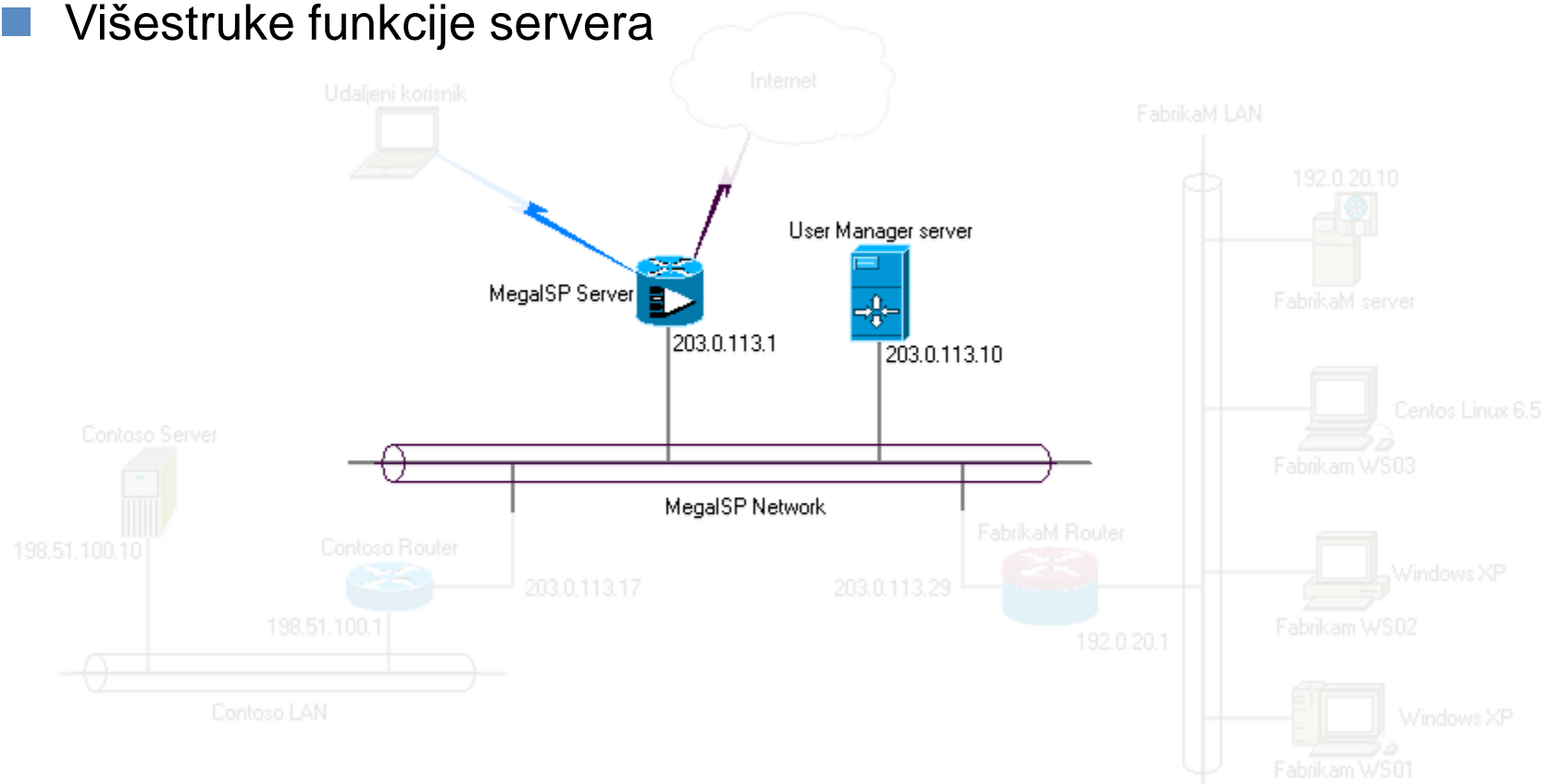
FabrikaM deo

- Kontrolišemo Internet pristup
- Korisnik želi najbolje korišćenje Internet pristupa
- Neke stanice moraju da komuniciraju bez ograničenja



MegaSP deo

- Ovaj segment simulira sva povezivanja preko Interneta
- Višestruke funkcije servera



Naša mreža bez HotSpota

- Postavili smo celu laboratoriju bez ograničenja i testirali rad

The screenshot displays a virtual lab environment with several windows open:

- POP3 Service:** A window showing a list of mailboxes. The table below is circled in red:

Mailbox Name	Size of Mailbox	Messages	State
contoso_admin	11 KB	22	Unlocked
contoso_user...	0 KB	0	Unlocked
contoso_user...	0 KB	0	Unlocked

- Quick'n Easy FTP Server 3.0 Lite:** A window showing server status and logs. The logs show a client connection from 192.0.20.10.
- C:\inetpub\ftproot:** A file explorer window showing backup files. The files below are circled in red:

Name	Size	Type	Date Modified	Attributes
Fabrikam_server.backup	5 KB	BACKUP File	9/16/2014 11:00 AM	A
Mikrotik-15092014-1541.backup	5 KB	BACKUP File	9/16/2014 10:45 AM	A
Mikrotik-15092014-1700.backup	4 KB	BACKUP File	9/16/2014 11:08 AM	A

- Mozilla Firefox:** A browser window showing the Contoso website.
- Microsoft Internet Explorer:** A browser window showing the Contoso website.
- Inbox - Outlook Express:** A window showing an email from Walter Bishop to Peter Bishop with the subject "Hello".



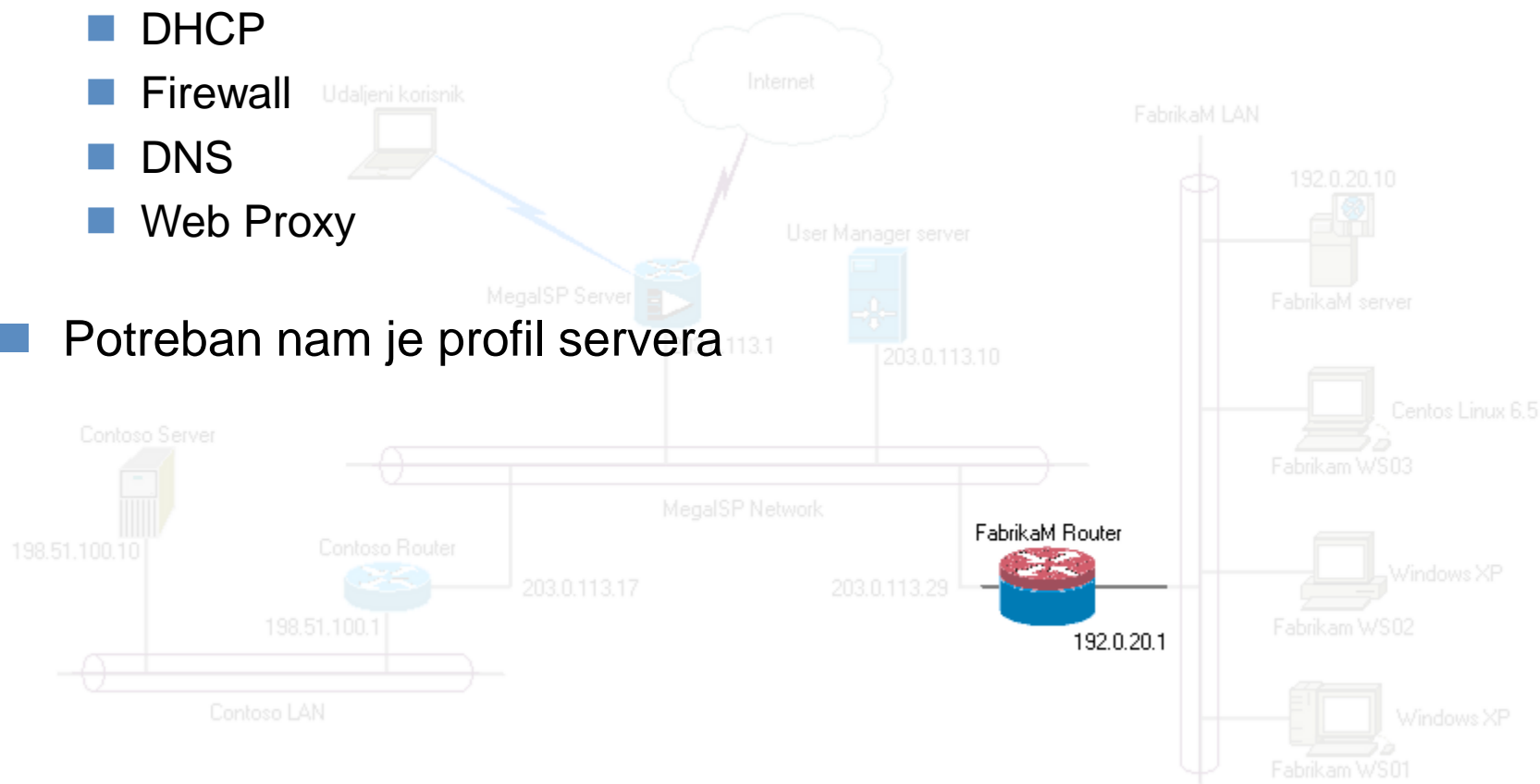
Priprema HotSpot-a

Pre podešavanja

■ HotSpot utiče na rad više servisa:

- DHCP
- Firewall
- DNS
- Web Proxy

■ Potreban nam je profil servera



HotSpot Server Profile

- IP > Hotspot > Server Profiles
- Profil sadrži opšta podešavanja
- Obratiti pažnju ako se postavljaju ograničenja protoka

The image displays three sequential screenshots of the 'Hotspot Server Profile <default>' configuration window, illustrating the different tabs available for setting up a hotspot server profile.

General Tab: This tab contains fields for basic profile information and server settings. The 'Name' field is set to 'default'. Other fields include 'Hotspot Address', 'DNS Name', 'HTML Directory' (set to 'hotspot'), 'Rate Limit (px/bx)', 'HTTP Proxy', 'HTTP Proxy Port' (set to '0'), and 'SMTP Server'.

Login Tab: This tab is used to configure authentication methods. The 'Login By' section shows options for 'MAC', 'Cookie' (checked), 'HTTP CHAP' (checked), 'HTTPS', 'HTTP PAP', and 'Trial'. It also includes fields for 'MAC Auth. Password', 'HTTP Cookie Lifetime' (set to '3d 00:00:00'), 'SSL Certificate' (set to 'none'), 'Split User Domain' (unchecked), 'Trial Uptime Limit' (set to '00:30:00'), 'Trial Uptime Reset' (set to '1d 00:00:00'), and 'Trial User Profile' (set to 'default').

RADIUS Tab: This tab is for configuring RADIUS authentication and accounting. The 'Use RADIUS' checkbox is unchecked. Fields include 'Default Domain', 'Location ID', 'Location Name', 'MAC Format' (set to 'XX:XX:XX:XX:XX:XX'), 'Accounting' (checked), 'Interim Update', and 'NAS Port Type' (set to '19 (wireless-802.11)').

Podešavanje HotSpot servera

- IP > Hotspot > Servers
- U okviru podešavanja servera moramo da podesimo interfejs
- Potreban nam je profil u kome su sva ostala podešavanja

The image displays three sequential screenshots of the Mikrotik WinBox interface for configuring a Hotspot server.

First Screenshot: New Hotspot Server
This window shows the initial configuration. The 'Name' field is set to 'FabrikaM_HotSpot'. The 'Interface' is 'ether1'. The 'Address Pool' is 'FabrikaM_pool' (highlighted with a red circle). The 'Profile' is 'default' (highlighted with a red circle). Other fields like 'Idle Timeout', 'Keepalive Timeout', 'Addresses Per MAC', 'IP of DNS Name' (0.0.0.0), and 'Proxy Status' are visible.

Second Screenshot: New Hotspot Server
This is a duplicate of the first screenshot, showing the same configuration fields with 'Address Pool' and 'Profile' highlighted by red circles.

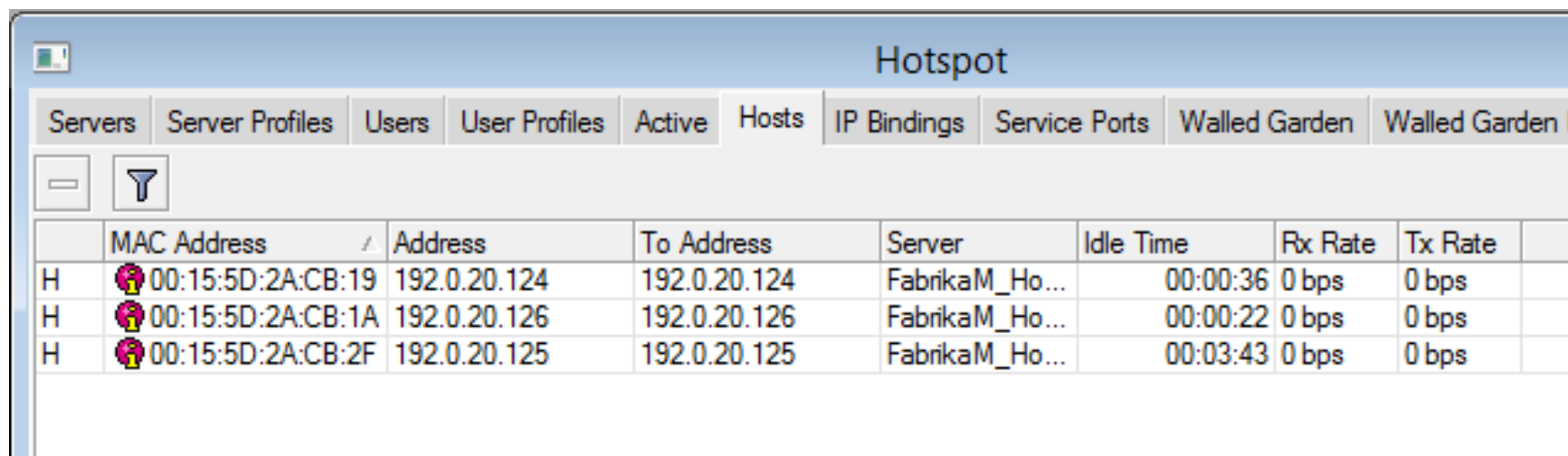
Third Screenshot: Hotspot Server <FabrikaM_HotSpot>
This window shows the configuration for the specific server. The 'Name' is 'FabrikaM_HotSpot'. The 'Interface' is 'ether1'. The 'Address Pool' is 'FabrikaM_pool'. The 'Profile' is 'default'. The 'IP of DNS Name' is '0.0.0.0'. The 'Proxy Status' is set to 'running' (highlighted with a red circle). On the right side, the 'Apply' button is highlighted with a red rectangle. Other buttons like 'OK', 'Cancel', 'Disable', 'Copy', 'Remove', and 'Reset HTML' are also visible.



Pokretanje HotSpot-a

HotSpot stanice

- IP > Hotspot > Hosts
- HotSpot će pokazati sve stanice koje imaju HTTP ili HTTPS sesije



	MAC Address	Address	To Address	Server	Idle Time	Rx Rate	Tx Rate
H	00:15:5D:2A:CB:19	192.0.20.124	192.0.20.124	FabrikaM_Ho...	00:00:36	0 bps	0 bps
H	00:15:5D:2A:CB:1A	192.0.20.126	192.0.20.126	FabrikaM_Ho...	00:00:22	0 bps	0 bps
H	00:15:5D:2A:CB:2F	192.0.20.125	192.0.20.125	FabrikaM_Ho...	00:03:43	0 bps	0 bps

HotSpot pravila u zaštitnom zidu

- HotSpot će ubaciti svoja pravila u podešavanja zaštitnog zida

Firewall											
Filter Rules NAT Mangle Service Ports Connections Address Lists Layer7 Protocols											
+ - ✓ ✗ [icon] [icon] Reset Counters 00 Reset All Counters Find all											
#	Action	Chain	Src. Address	Dst. Address	Protocol	Src. Port	Dst. Port	In. Inter...	Out. Int...	Bytes	Packets
0 D	jump	forward								900 B	9
1 D	jump	forward								0 B	0
2 D	jump	input								9.7 KB	94
3 DI	jump	hs-input								0 B	0
4 D	✓ acc...	hs-input			17 (udp)		64872			856 B	14
5 D	✓ acc...	hs-input			6 (tcp)		64872-64875			6.8 KB	62
6 D	jump	hs-input								2109 B	18
7 D	✗ reject	hs-unauth			6 (tcp)					60 B	1
8 D	✗ reject	hs-unauth								2949 B	26
9 D	✗ reject	hs-unauth-to								0 B	0
... place hotspot rules here											
10 X	pas...	unused-hs...								0 B	0

Filter Rules NAT Mangle Service Ports											
+ - ✓ ✗ [icon] [icon]											
#	Action	Chain	Src.								
0 D	jump	dstnat									
1 DI	jump	hotspot			17 (u...	53				488 B	8
2 D	⇄ redir...	hotspot			6 (tcp)	53				0 B	0
3 D	⇄ redir...	hotspot			6 (tcp)	80				216 B	4
4 D	⇄ redir...	hotspot			6 (tcp)	443				0 B	0
5 D	⇄ redir...	hotspot			6 (tcp)					216 B	4
6 D	jump	hotspot			6 (tcp)					0 B	0
7 D	jump	hotspot			6 (tcp)					156 B	3
8 D	⇄ redir...	hs-unauth			6 (tcp)	80				3128	0
9 D	⇄ redir...	hs-unauth			6 (tcp)	8080				0 B	0
10 D	⇄ redir...	hs-unauth			6 (tcp)	443				0 B	0
11 D	⇄ redir...	hs-unauth			6 (tcp)					0 B	0
12 DI	jump	hs-unauth			6 (tcp)	25				0 B	0
13 D	⇄ redir...	hs-auth			6 (tcp)					0 B	0
14 DI	jump	hs-auth			6 (tcp)	25				0 B	0
... place hotspot rules here											
15 X	pas...	unused-hs...								0 B	0

Šta se dešava sa stanicama?

- Sve stanice su izgubile pristup resursima izvan mreže
- DNS upiti će nastaviti da rade

```
C:\>nslookup
*** Can't find server name for address 192.0.20.1: Non-existent domain
*** Default servers are not available
Default Server: UnKnown
Address: 192.0.20.1

> www.contoso.com
Server: UnKnown
Address: 192.0.20.1

Non-authoritative answer:
Name: www.contoso.com
Address: 198.51.100.10

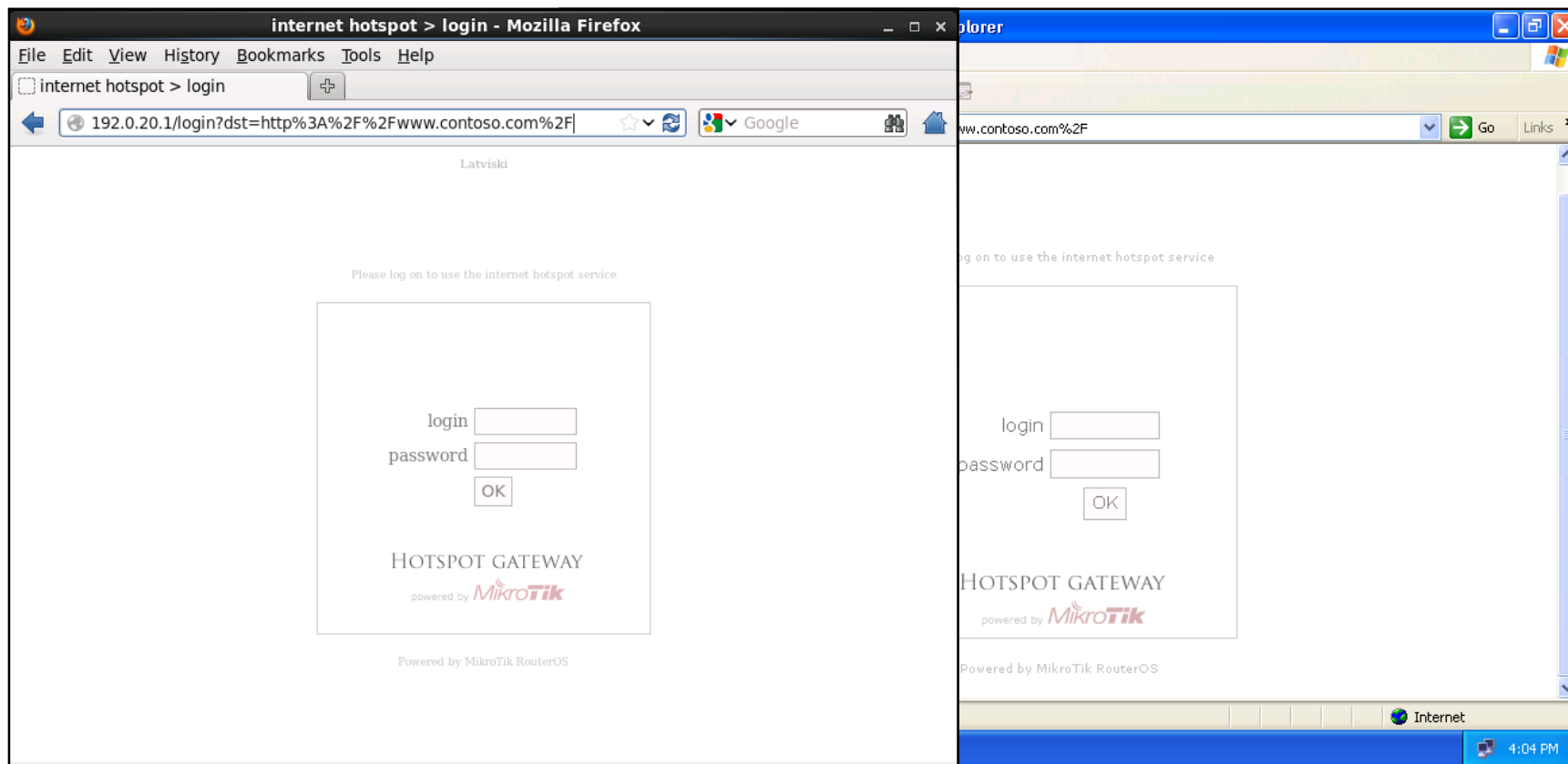
> www.fabrikam.com
Server: UnKnown
Address: 192.0.20.1

Non-authoritative answer:
Name: www.fabrikam.com
Address: 192.0.20.10

>
```


Blokiran saobraćaj

- Pretraživači otvaraju HotSpot stranicu za prijavu
- Korisnik mora da unese ime i šifru za izlaz iz mreže



Blokiran saobraćaj (II deo)

- I server na statičkoj IP je blokiran
- Radi samo saobraćaj koji ne prolazi kroz HotSpot

```
[admin@MikroTik] >
[admin@FabrikaM Server] > ping www.contoso.com
invalid value for argument address
[admin@FabrikaM Server] > ping [/resolve www.cont
failure
[admin@FabrikaM Server] > ping 198.51.100.10 cou
198.51.100.10 ping timeout
198.51.100.10 ping timeout
198.51.100.10 ping timeout
198.51.100.10 ping timeout
4 packets transmitted, 0 packets received, 100% p
[admin@FabrikaM Server] > ping 192.0.20.1 count=4
192.0.20.1 ping timeout
192.0.20.1 ping timeout
192.0.20.1 ping timeout
192.0.20.1 ping timeout
4 packets transmitted, 0 packets received, 100% packet loss
[admin@FabrikaM Server] > ping 192.0.20.126 count=4
192.0.20.126 64 byte ping: ttl=128 time=3 ms
192.0.20.126 64 byte ping: ttl=128 time<1 ms
192.0.20.126 64 byte ping: ttl=128 time<1 ms
192.0.20.126 64 byte ping: ttl=128 time<1 ms
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0/0.7/3 ms
[admin@FabrikaM Server] >
```

```
1  name="FTP_Upload" owner="admin"
   policy=ftp,reboot,read,write,policy,test,winbox,password,sniff,sensitive
   last-started=sep/16/2014 15:10:57 run-count=2
   source=
     /system backup save name=fabrikam_server.backup

     :delay 2

     /tool fetch address=198.51.100.10 mode=ftp dst-path=fabrikam_server.bac>

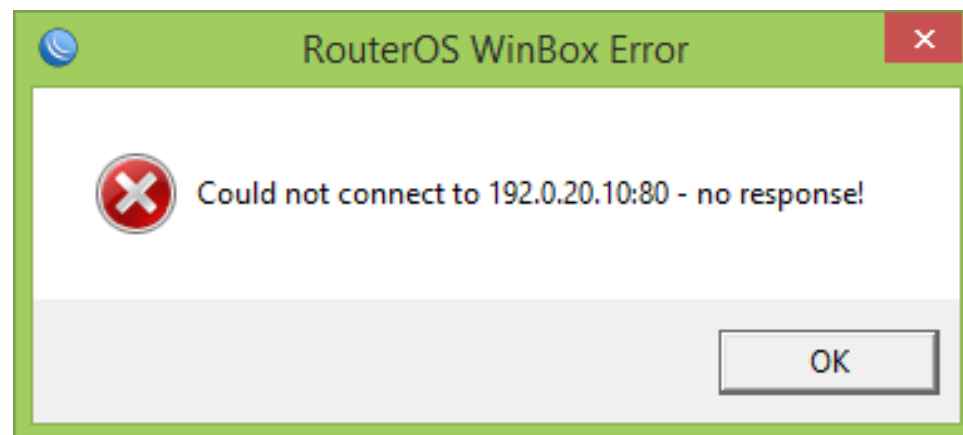
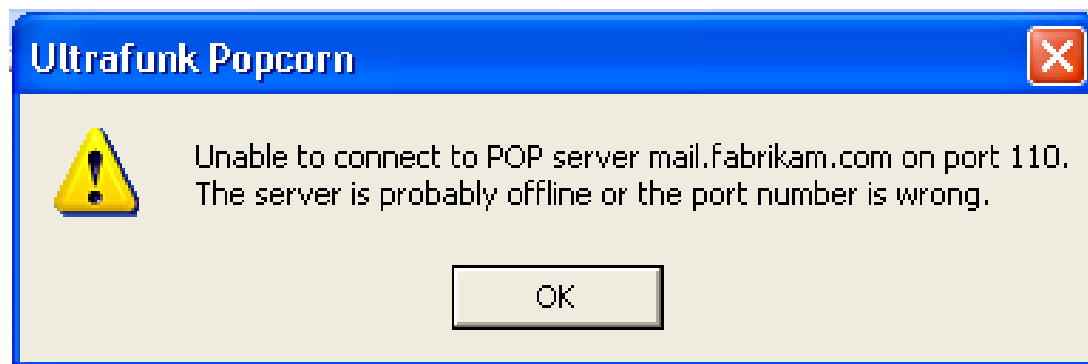
     :delay 5

     /tool e-mail send to=contoso_admin@contoso.com subject="Backup Upload" >

[admin@FabrikaM Server] > system script run FTP_Upload
Saving system configuration
Configuration backup saved
status: failed
failure: connection failed
[admin@FabrikaM Server] >
```

Blokiran saobraćaj (III deo)

- HotSpot automatski blokira sve portove/servise
- Time se blokiraju i dolazne konekcije





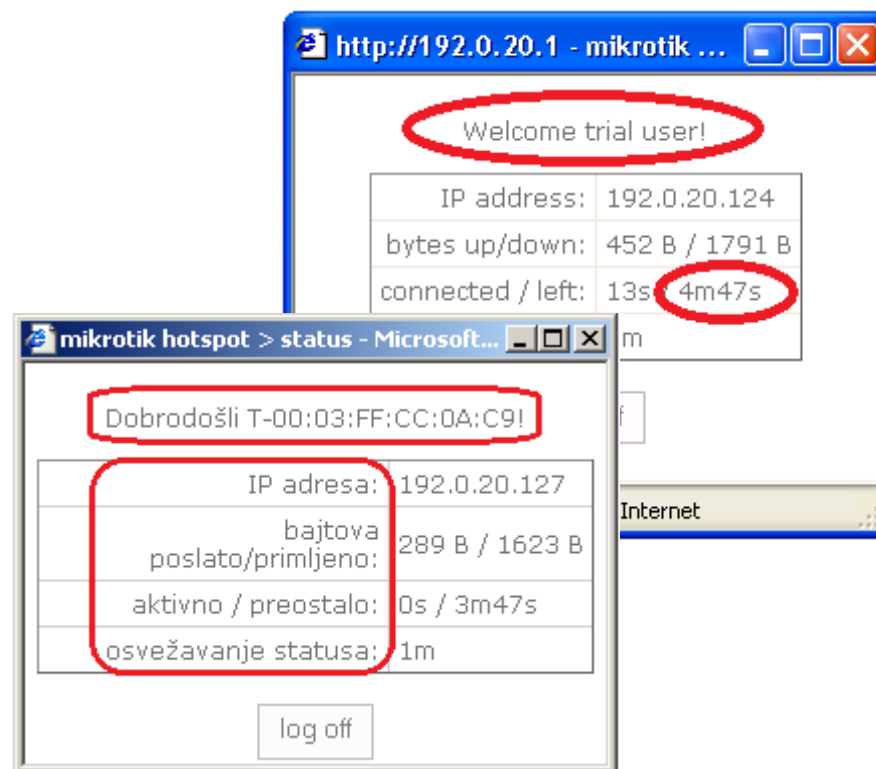
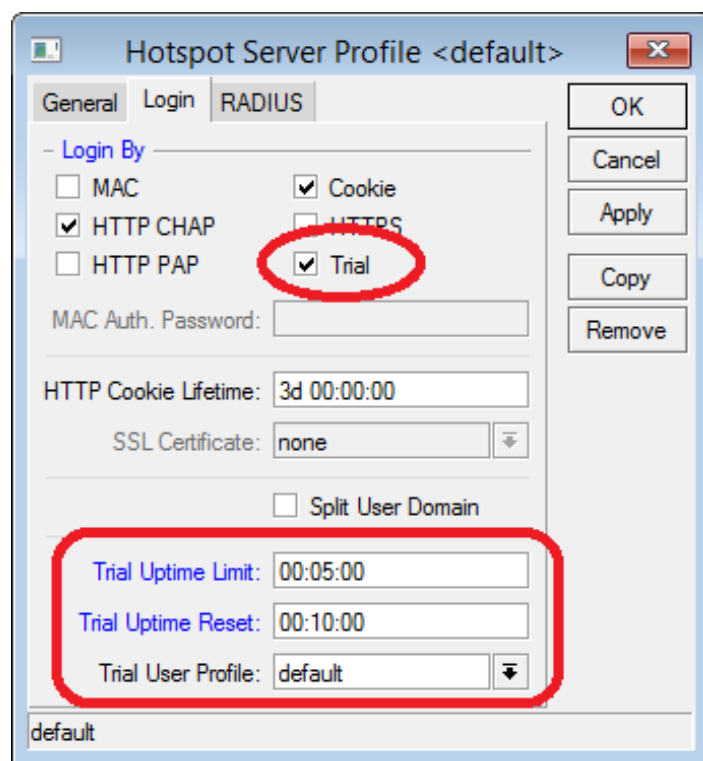
Zaobilaženje HotSpot-a

Kako korisnik može da zaobiđe HotSpot?

- HotSpot se ne može zaobići
- Administrator kontroliše prolaz
- Mehanizmi za prolaz bez autorizacije
 - Probni period
 - Walled garden i Walled garden IP
 - IP Bindings

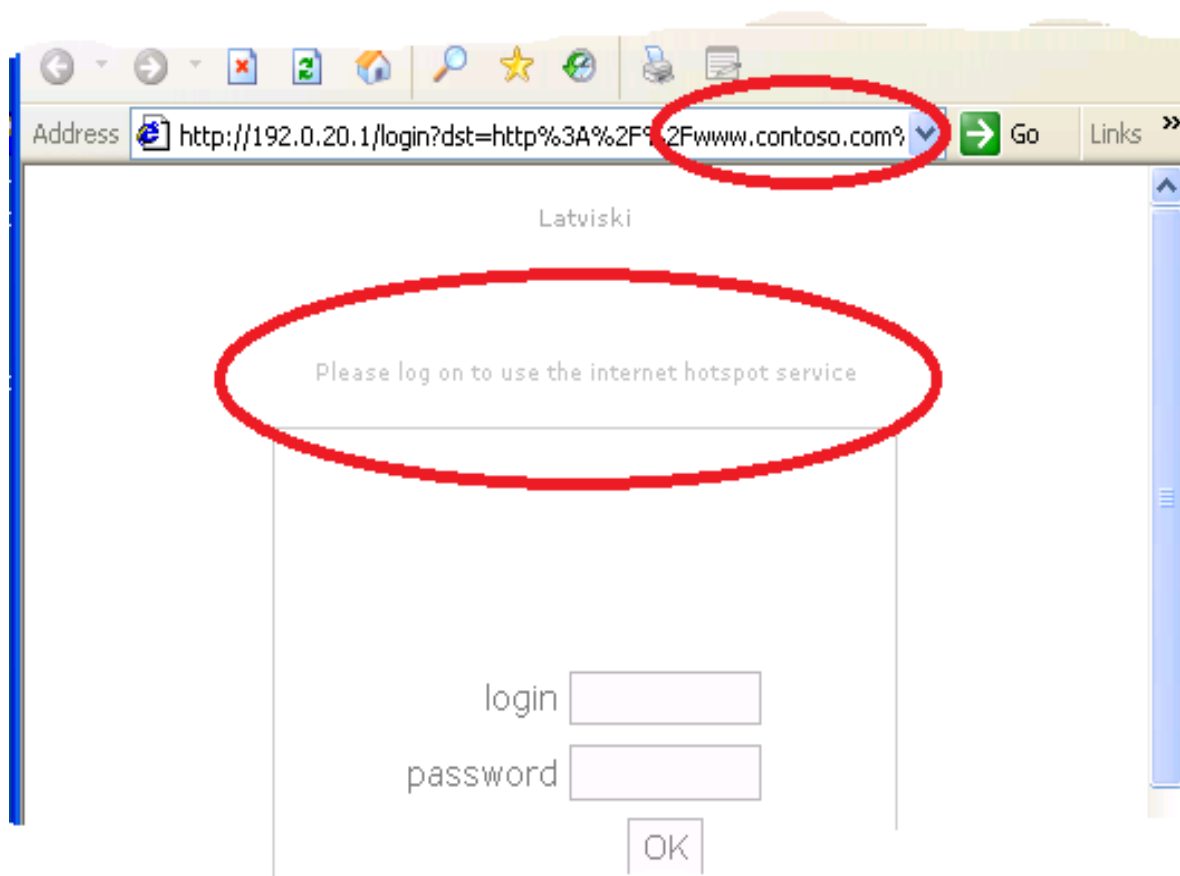
Probni period – poklon korisniku

- Možemo pokloniti korisnicima neko vreme na Internetu
- Na stanici za prijavu se dobija link za probni period



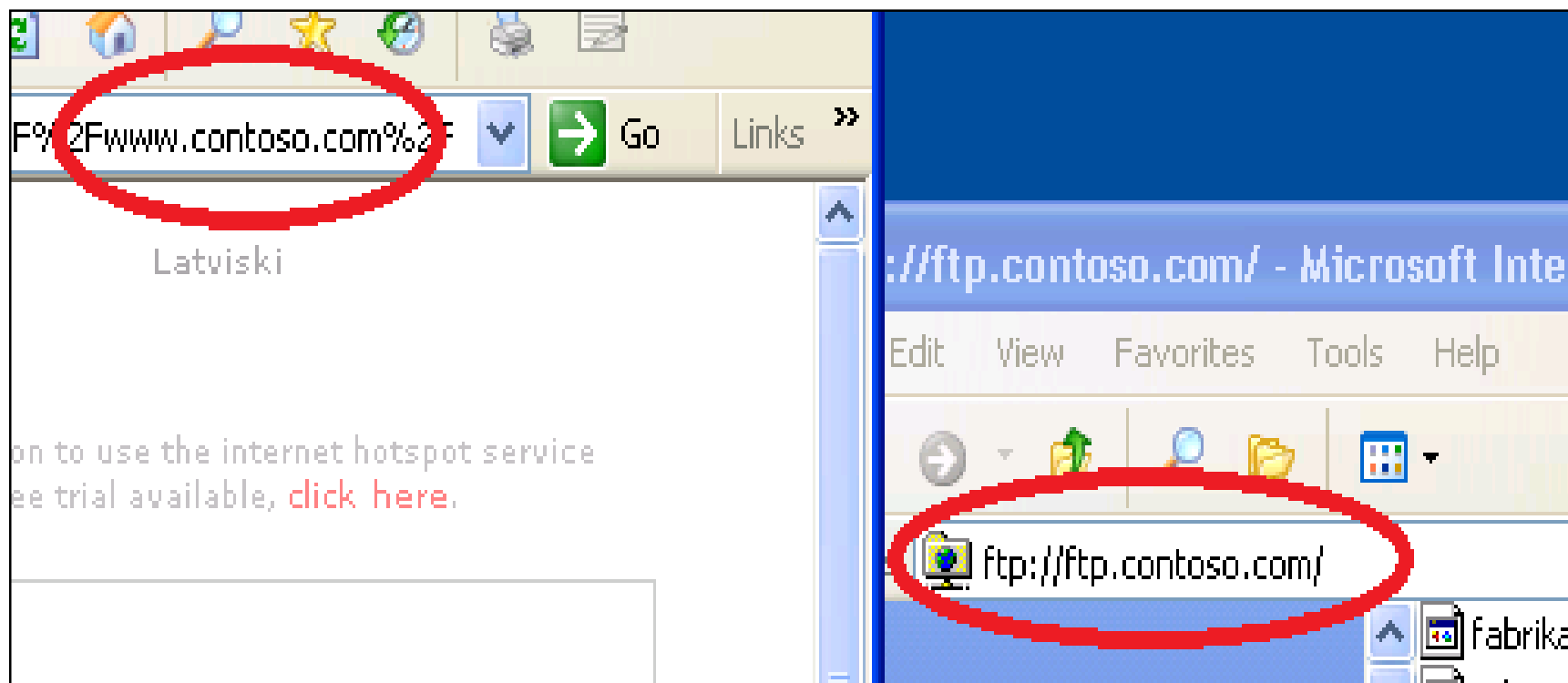
Kraj probnog perioda

- Na kraju probnog perioda se zatvaraju sve sesije
- Korisnik se vraća na stranicu za prijavu



Walled Garden i Walled Garden IP

- Walled Garden pravila dozvoljavaju pristup resursima bez prijave na HotSpot.
- Walled Garden neće blokirati autorizovanog korisnika.



Kako da dodamo servise u Walled Garden?

- Svaki servis opisujemo jednoznačno

Hotspot

Servers Server Profiles Users User Profiles Active Hosts IP Bindings Service Ports Walled Garden Walled Garden IP List

+ - ✓ ✗ 📁 🔍

Action	Server	Src. Address	Dst. Address	Protocol	Dst. Port	Dst. Host
accept	FabrikaM_HotSpot					ftp.contoso.com
accept	FabrikaM_HotSpot			6 (tcp)	110	mail.fabrikam.com
accept	FabrikaM_HotSpot			6 (tcp)	25	mail.fabrikam.com

Contoso Server
198.51.100.10

Contoso LAN
198.51.100.1

Walled Garden IP Entry <mail.fabrikam...>

Action: ☒ accept ☐ drop ☐ reject

Server: ☐ FabrikaM_HotSpot

Src. Address:

Dst. Address:

Protocol: ☐ 6 (tcp)

Dst. Port: ☐ 25

Dst. Host: mail.fabrikam.com

disabled

OK Cancel Apply Disable Comment Copy Remove

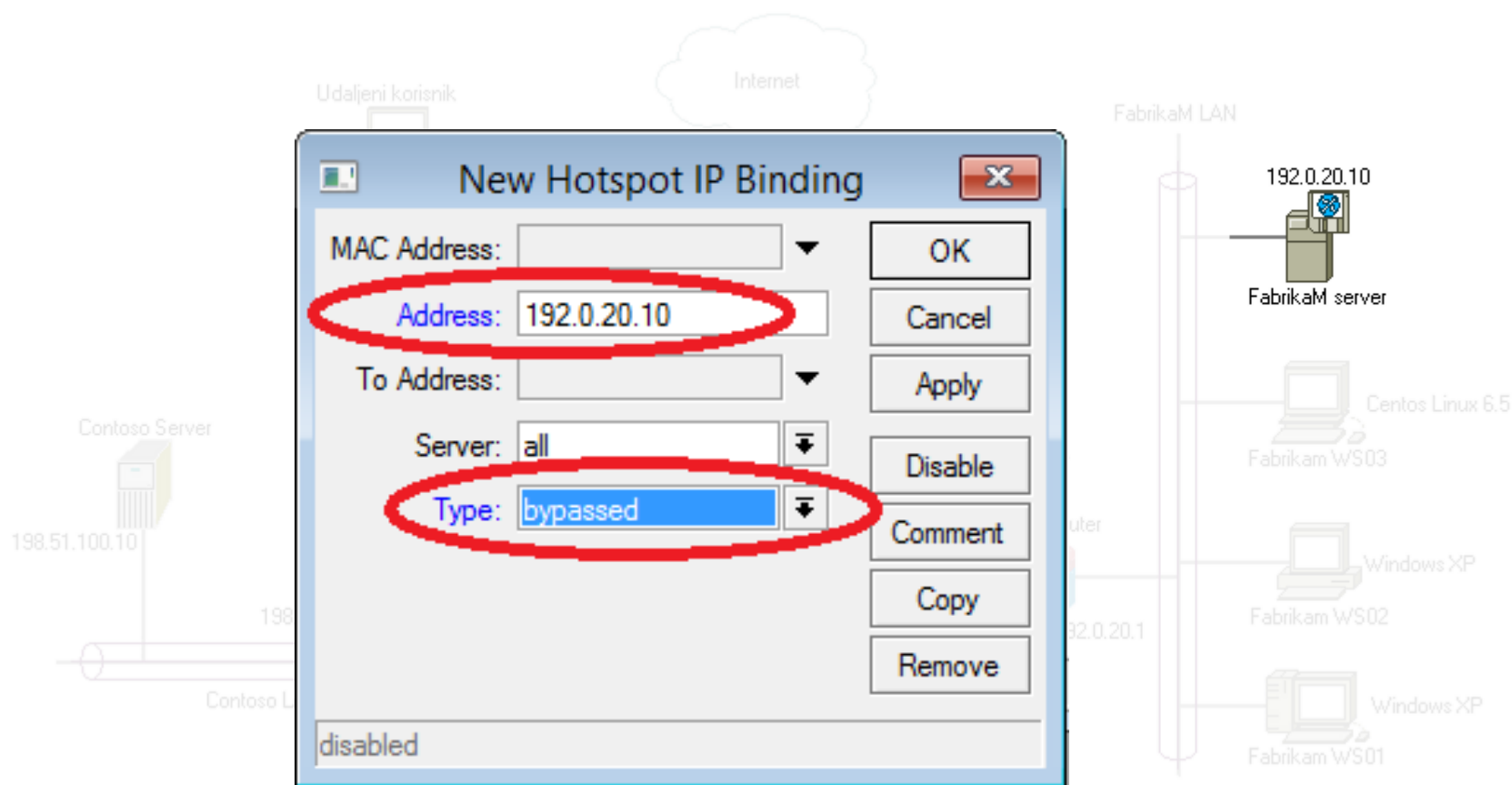
Fabrikam WS03
Centos Linux 6.5

Fabrikam WS02
Windows XP

Fabrikam WS01
Windows XP

Mehanizam za zaobilazanje HotSpota

- IP Bindings dozvoljava hostu da prođe kroz HotSpot bez prijave





Korisnički nalozi

Korisnički nalozi za HotSpot

- Korisnici moraju da se prijave na HotSpot
- Lokalna baza naloga ili RADIUS server
- Osnovna podešavanja se postavljaju kroz profile

HotSpot User Profile

- IP > Hotspot > User Profiles
- HotSpot User Profile omogućava podešavanje zajedničkih parametara za naloge korisnika
- Obratiti pažnju na ograničenja koja se postavljaju

Hotspot User Profile <default>

General Advertise Scripts

Name: default

Address Pool: none

Session Timeout:

Idle Timeout: none

Keepalive Timeout: 00:02:00

Status Autorefresh: 00:01:00

Shared Users: 1

Rate Limit (px/bx):

Address List:

Incoming Filter:

Outgoing Filter:

Incoming Packet Mark:

Outgoing Packet Mark:

Open Status Page: always

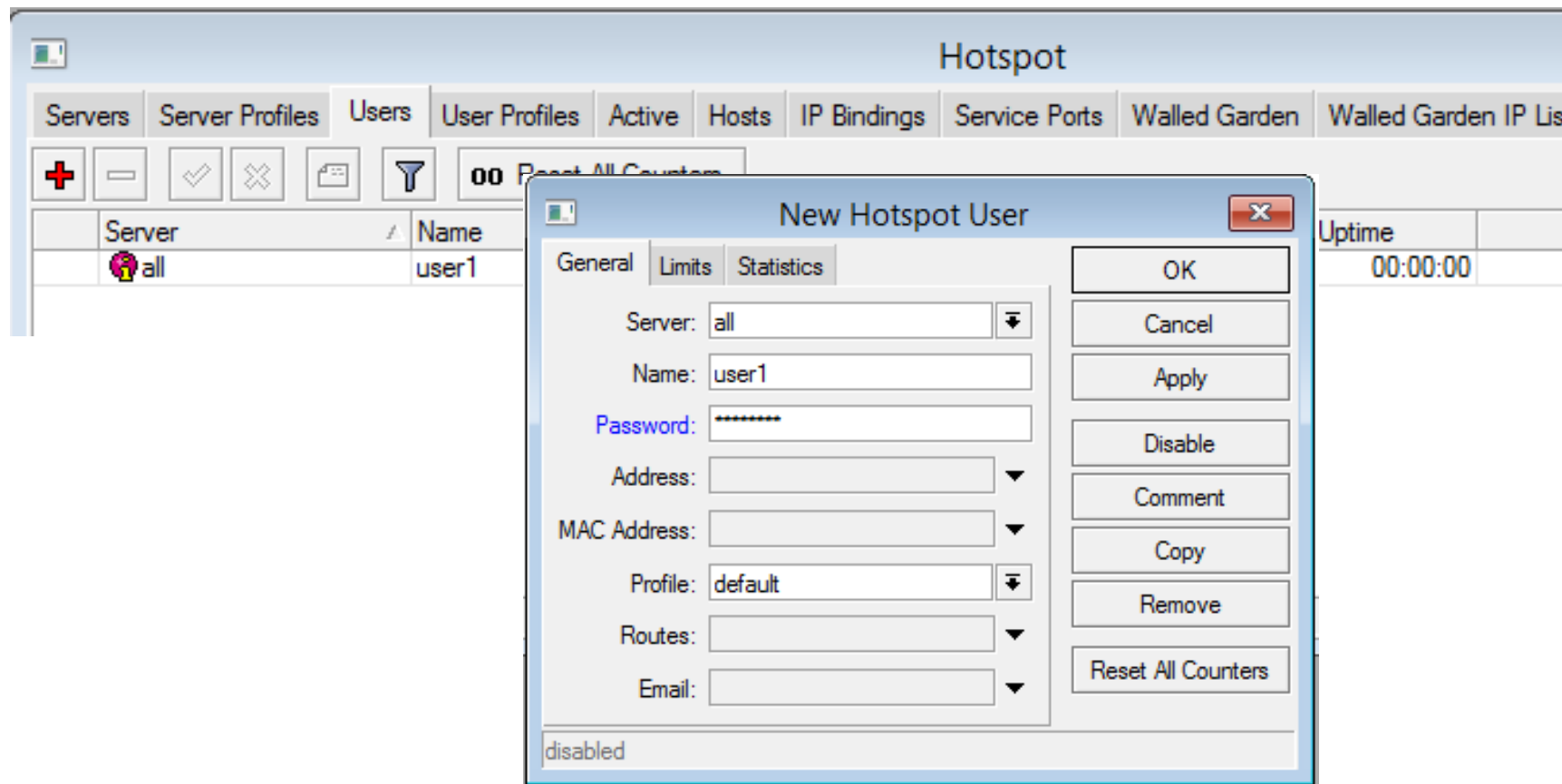
☐ Transparent Proxy

OK Cancel Apply Copy Remove

default

HotSpot korisnički nalozi

- Preko IP > Hotspot > Users pravimo naloge u lokalnoj bazi

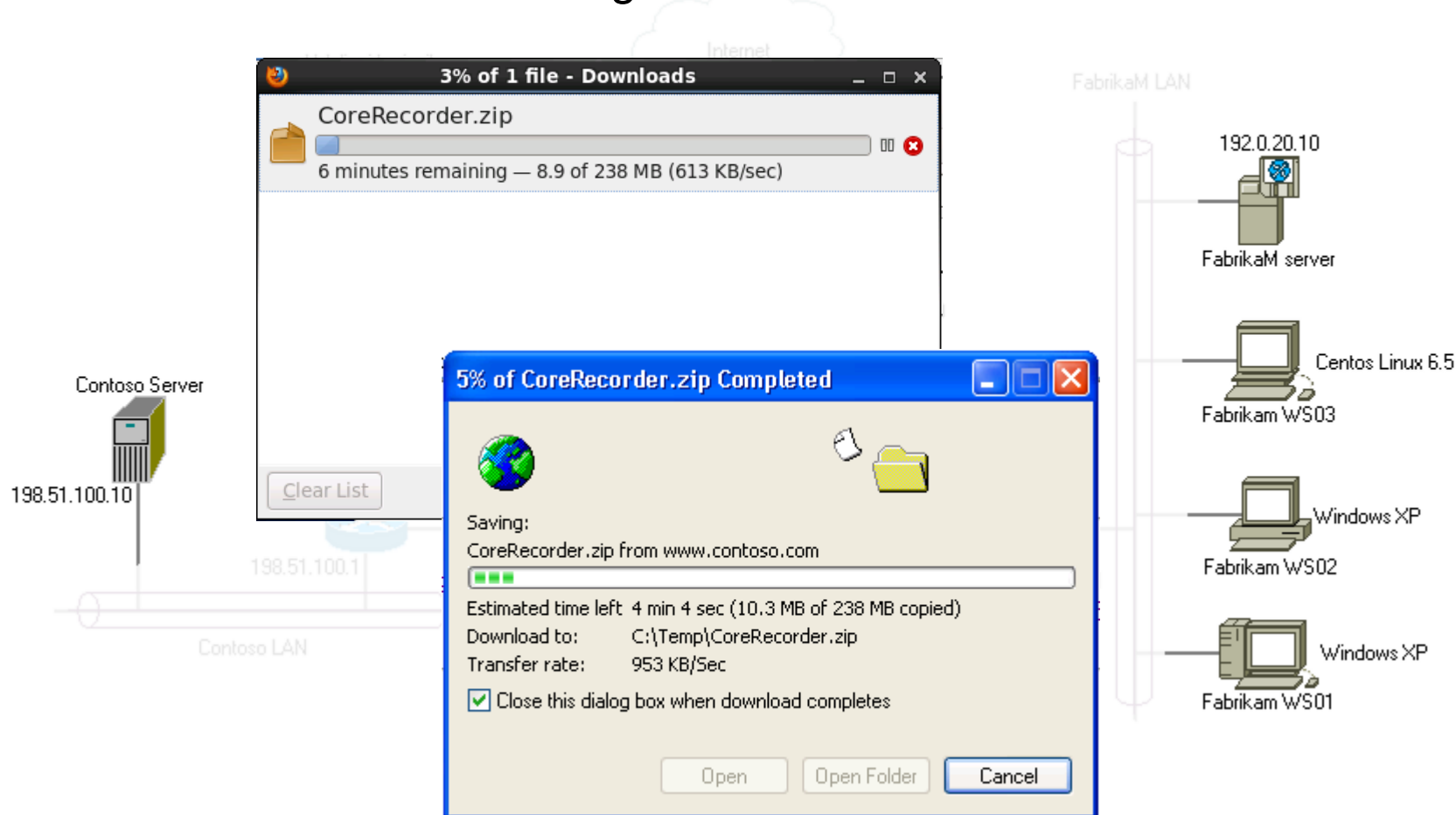




Kontrola protoka

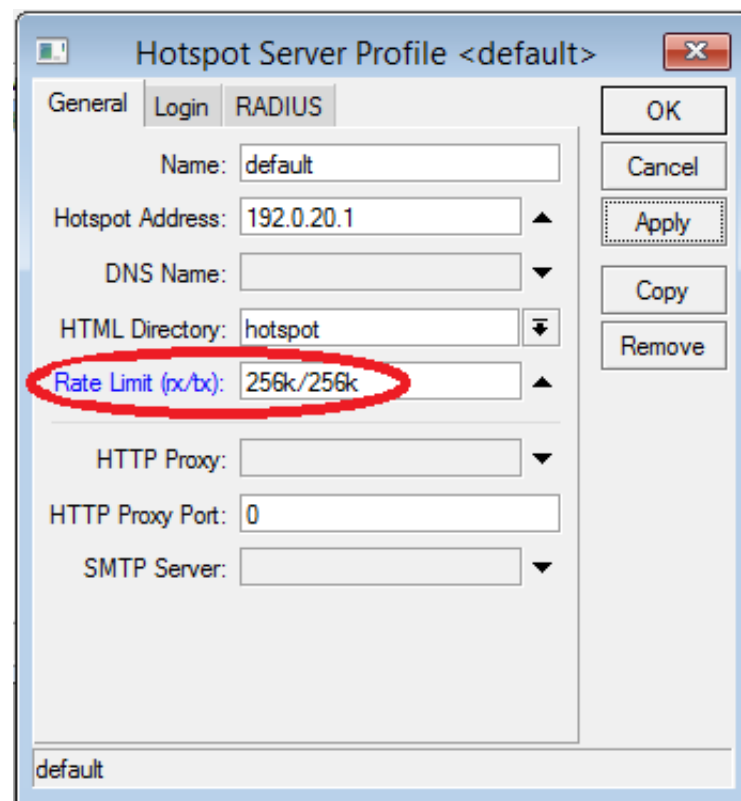
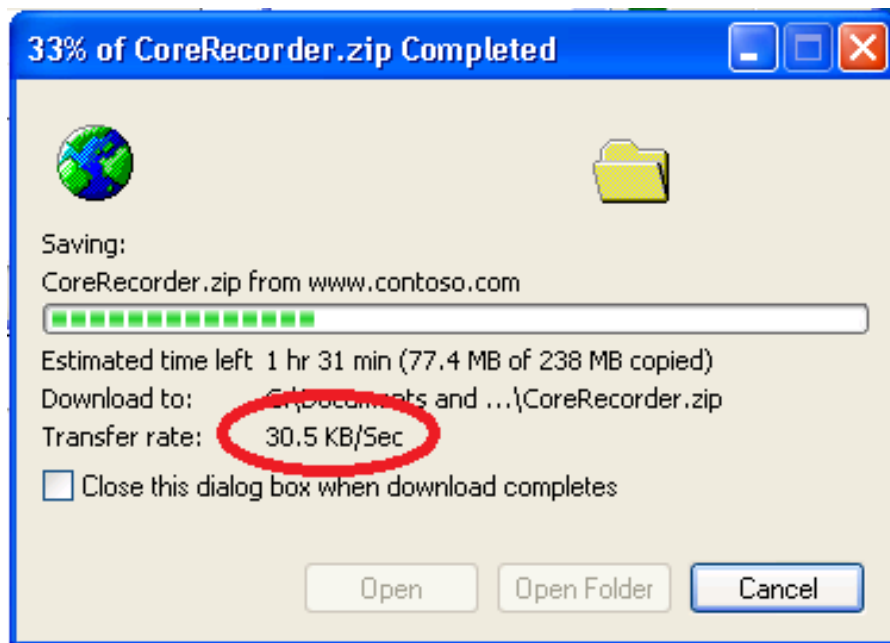
Protok bez ograničenja

- Klijenti skidaju punom brzinom
- Jedan korisnik može da zaguši ceo link



Ograničenje protoka po HotSpot-u

- Ograničava se ukupan protok kroz HotSpot
- Svi korisnici dele taj protok



HotSpot i Queue

- Ceo HotSpot je samo jedan Queue

The image shows two overlapping windows from the Mikrotik WinBox interface. The background window is titled 'Queue List' and displays a table with queue configurations. The foreground window is titled 'Hotspot Server Profile <default>' and shows configuration options for a hotspot profile, with the 'Rate Limit (rx/tx)' field circled in red.

Queue List Window:

#	Name	Target Address	Rx Max Limit	Tx Max Limit	Packet ...
0 D	hs-<FabrikaM_HotSpot>		512k	512k	

1 item | 33.8 KiB queued | 23 packets queued

Hotspot Server Profile <default> Window:

General | Login | RADIUS

Name: default

Hotspot Address: 192.0.20.1

DNS Name:

HTML Directory: hotspot

Rate Limit (rx/tx): 512k/512k

HTTP Proxy:

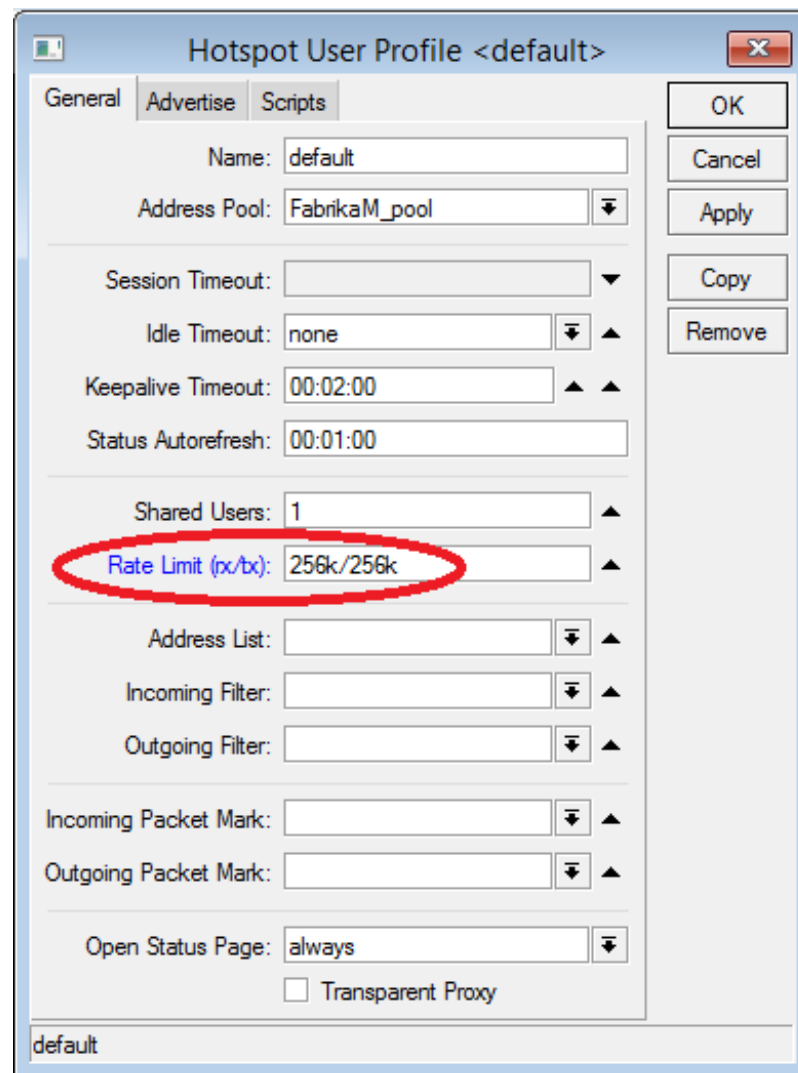
HTTP Proxy Port: 0

SMTP Server:

default

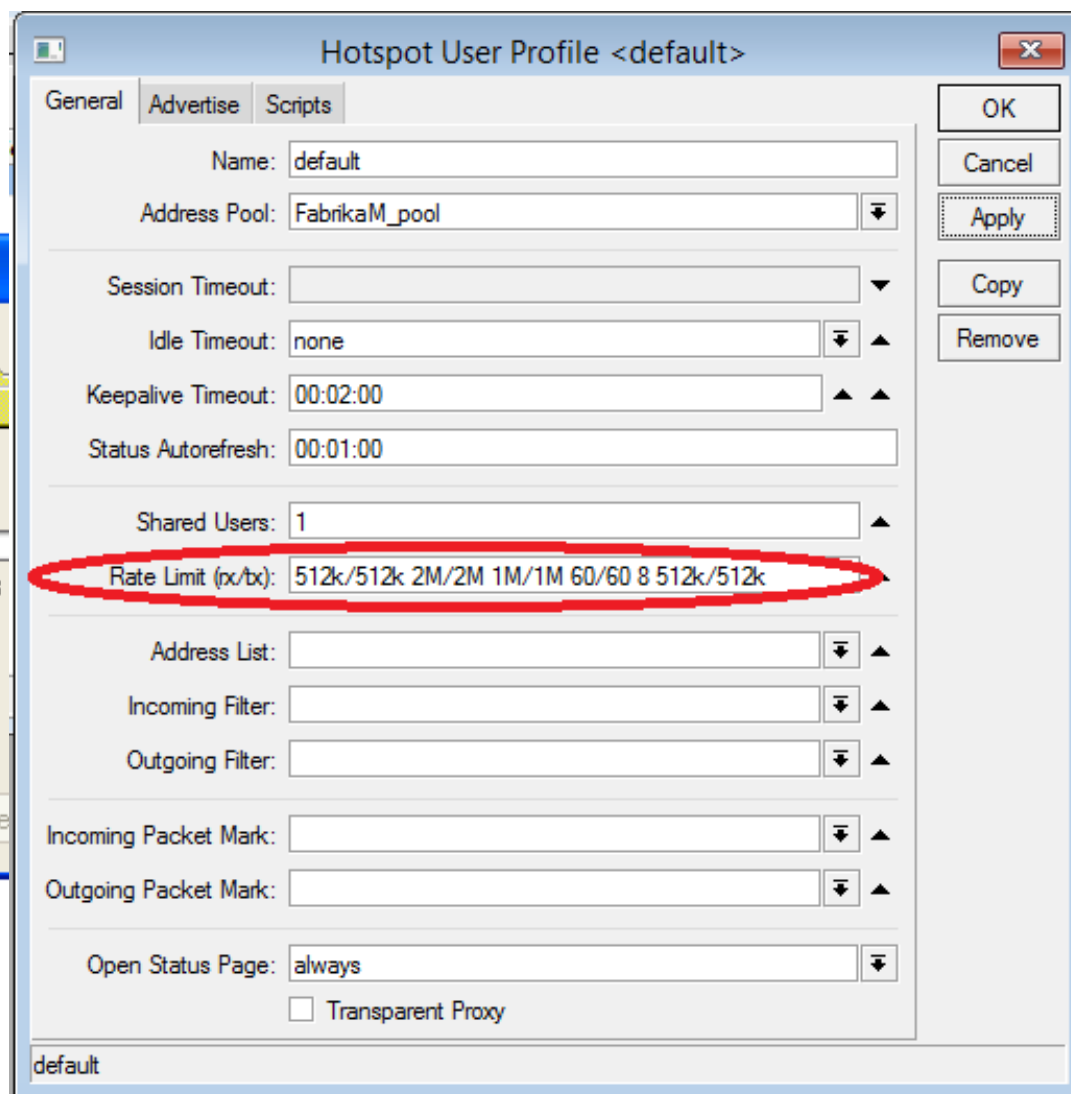
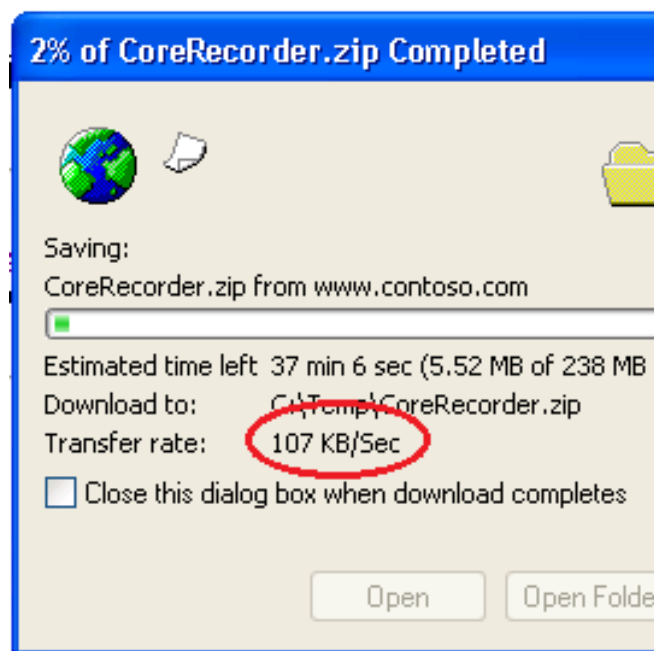
Protok po korisniku

- Možemo da ograničimo protok po korisniku
- Ograničenje je deo profila

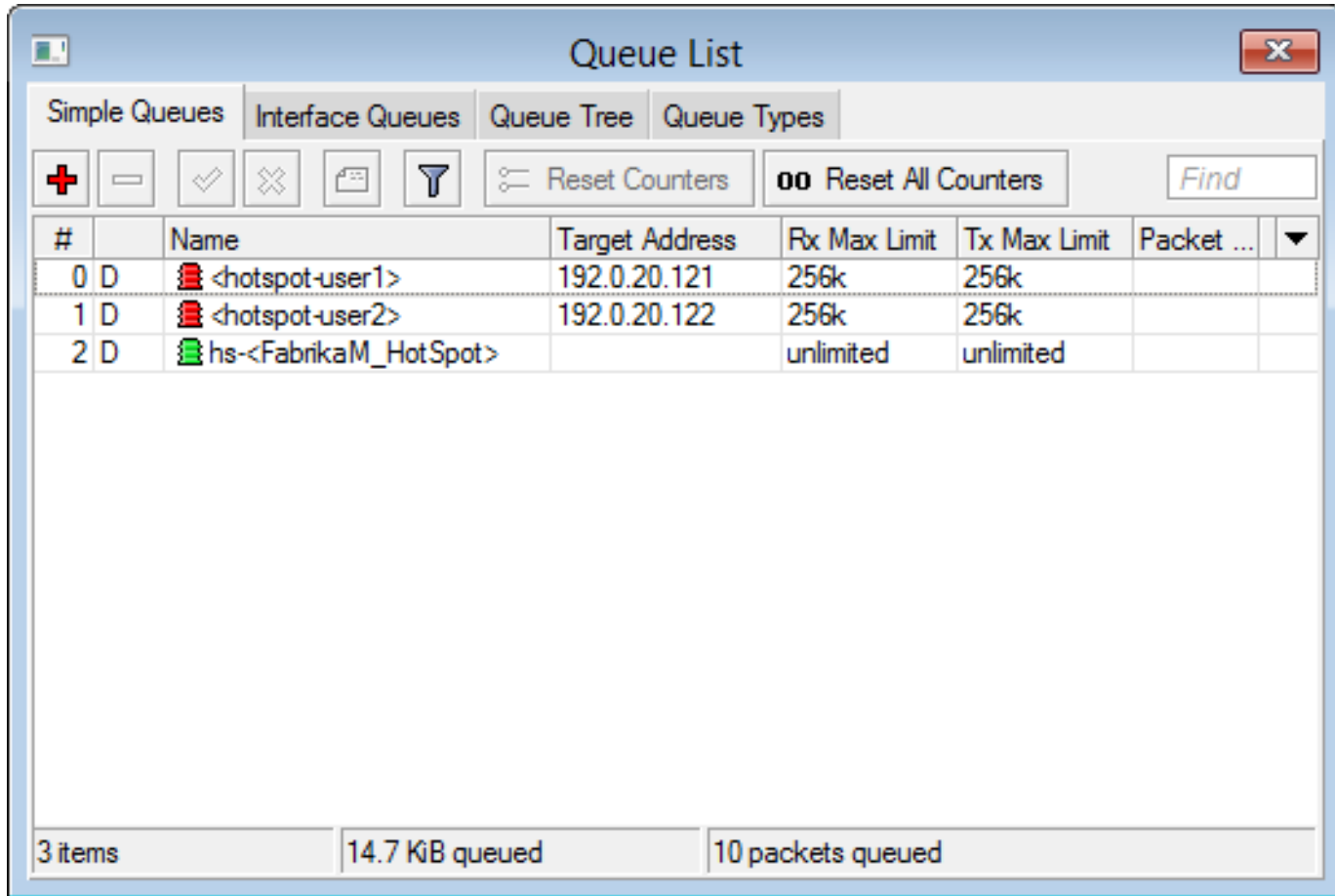


Varijabilni protokol

- Protokol se menja u vremenu



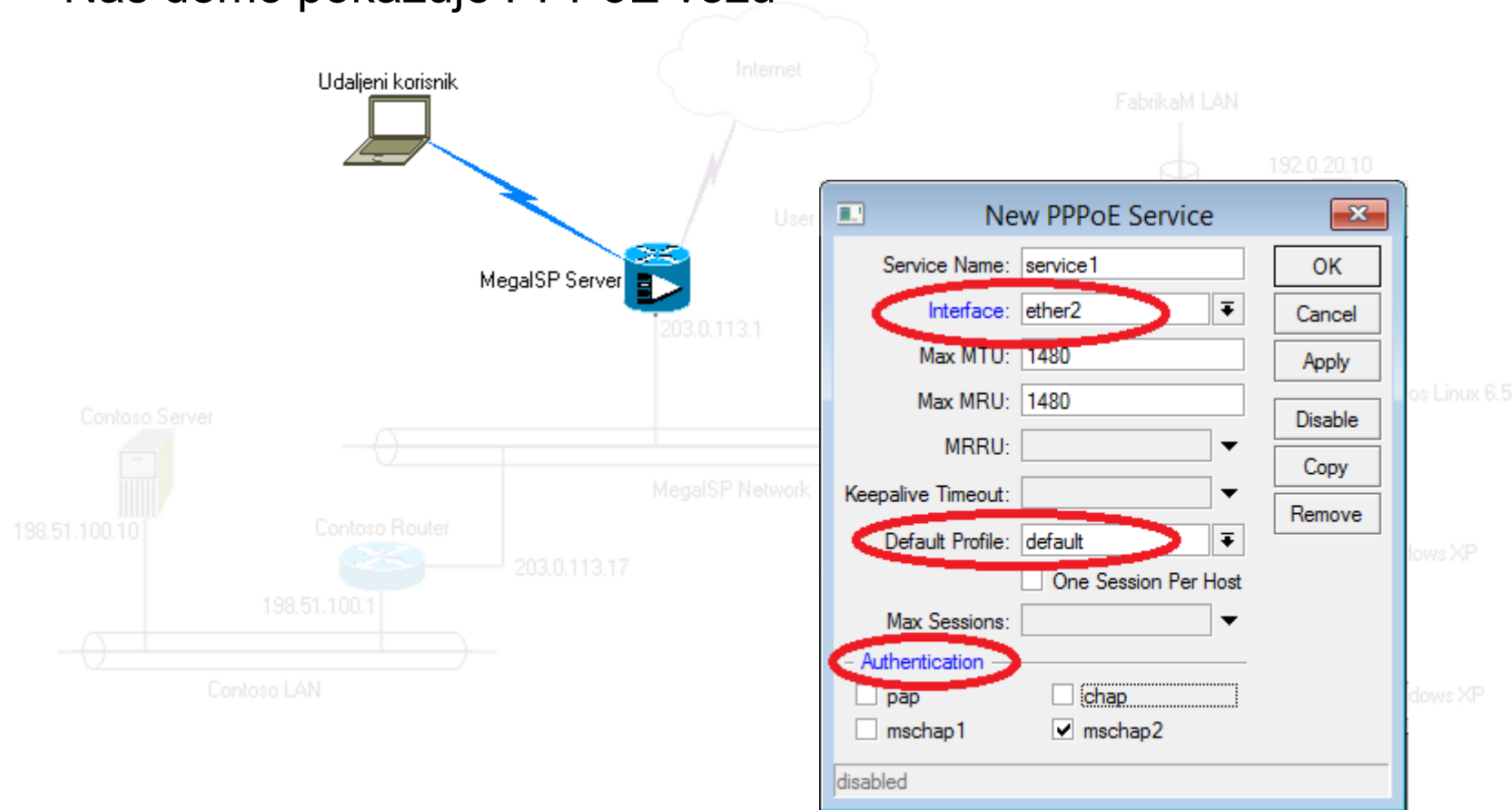
- Svaki korisnik dobija svoj queue



PPP servizi

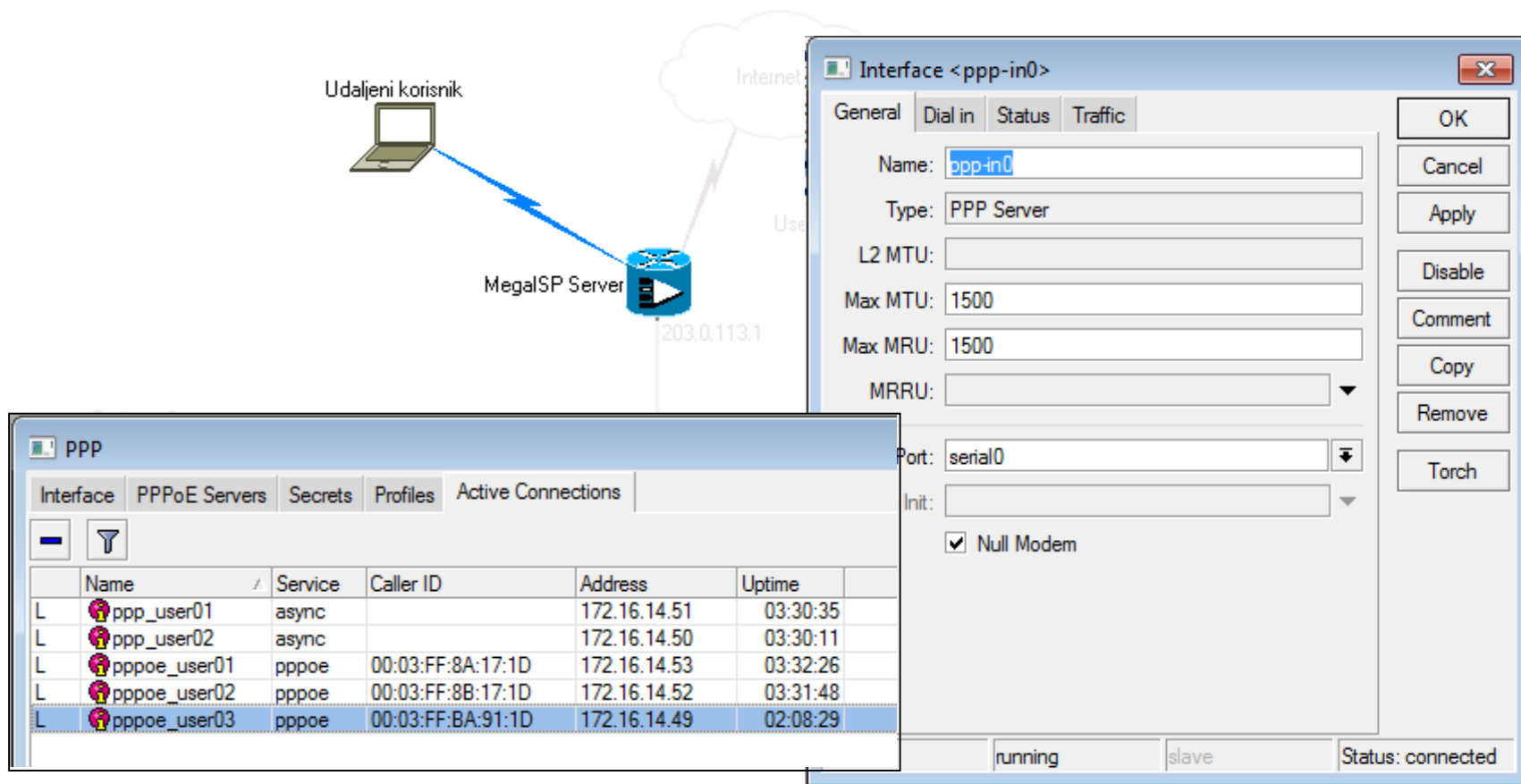
Udaljeni korisnici

- Udaljeni korisnik se prijavljuje preko nekog PPP servisa
- Naš demo pokazuje PPPoE vezu



Udaljeni korisnici (II)

- A imamo i dva korisnika preko modema



The diagram illustrates a network setup where a laptop, labeled 'Udaljeni korisnik' (Remote user), connects to a 'MegalSP Server' via a blue lightning bolt representing a modem connection. The server is connected to an 'Internet' cloud and has the IP address '203.0.113.1'. Below the diagram, two windows from a network management application are shown.

The 'PPP' window displays the 'Active Connections' tab with the following table:

	Name	Service	Caller ID	Address	Uptime
L	ppp_user01	async		172.16.14.51	03:30:35
L	ppp_user02	async		172.16.14.50	03:30:11
L	pppoe_user01	pppoe	00:03:FF:8A:17:1D	172.16.14.53	03:32:26
L	pppoe_user02	pppoe	00:03:FF:8B:17:1D	172.16.14.52	03:31:48
L	pppoe_user03	pppoe	00:03:FF:BA:91:1D	172.16.14.49	02:08:29

The 'Interface <ppp-in0>' window shows the configuration for the 'ppp-in0' interface. The 'General' tab is active, showing the following settings:

- Name: ppp-in0
- Type: PPP Server
- L2 MTU: (empty)
- Max MTU: 1500
- Max MRU: 1500
- MRRU: (empty)
- Port: serial0
- Init: (empty)
- ☒ Null Modem

Buttons on the right include OK, Cancel, Apply, Disable, Comment, Copy, Remove, and Torch. At the bottom, the status is shown as 'running', 'slave', and 'Status: connected'.

PPP nalozi

- PPP servisi imaju svoj lokalnu bazu

The screenshot shows the 'PPP Secret <pppuser01>' dialog box. The 'Name' field is set to 'pppoe_user01' and the 'Password' field is filled with asterisks. The 'Service' is set to 'any', 'Caller ID' is empty, and 'Profile' is set to 'default'. The 'Local Address' and 'Remote Address' fields are empty. The 'Routes' field is empty. The 'Limit Bytes In' and 'Limit Bytes Out' fields are empty. The status at the bottom is 'disabled'. Buttons on the right include OK, Cancel, Apply, Disable, Comment, Copy, and Remove.

The screenshot shows the 'PPP Profile <default>' dialog box. The 'Name' field is set to 'default'. The 'Local Address' field is set to '172.16.14.1' and the 'Remote Address' field is set to 'pppoe_pool'. The 'Bridge' field is empty. The 'Incoming Filter', 'Outgoing Filter', and 'Address List' fields are empty. The 'DNS Server' and 'WINS Server' fields are empty. The 'Use Compression' section has 'default' selected. The 'Use VJ Compression' section has 'default' selected. The 'Use Encryption' section has 'default' selected. The 'Change TCP MSS' section has 'yes' selected. Buttons on the right include OK, Cancel, Apply, Comment, Copy, and Remove.



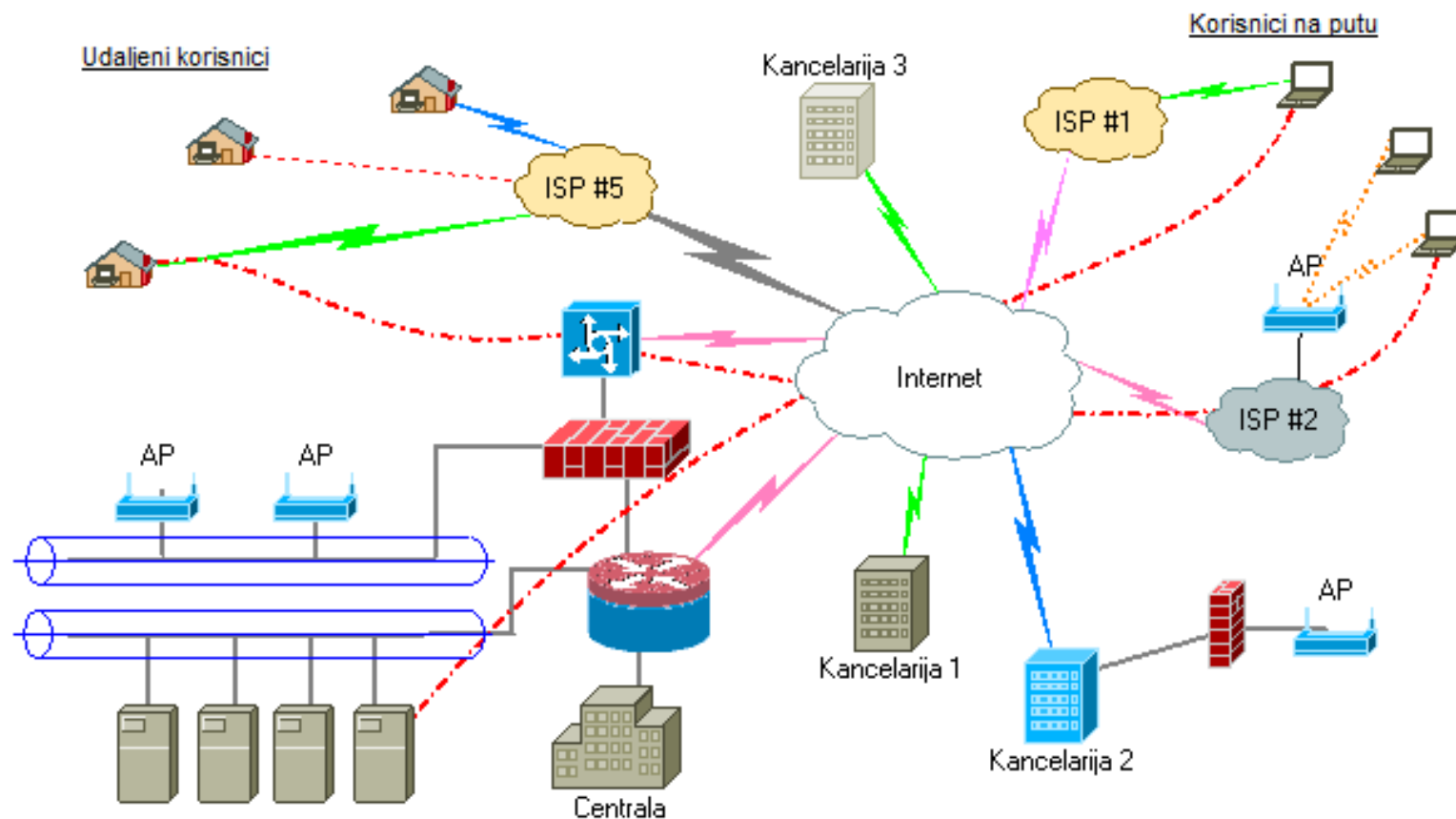
Mikrotik User Manager

Šta je to Mikrotik User Manager?

- Mikrotik User Manager je RADIUS server
- Jedan User Manager server - više klijenata
- Web aplikacija
- Centralizovana administracija naloga

Slučaj za User Manager

- Svuda gde je potrebna centralizovana administracija korisnika



Ograničenja User Managera

- Zahteva minimalno 32MB RAM i 2MB na disku
- Zahteva dosta prostora na disku za dnevnike aktivnosti
- RouterOS i User Manager moraju biti iste verzije
- Može značajno da optereti procesor na RouterBOARD-u
- Preporuka je da se koristi verzija 4.xx ili kasnija



Podešavanje User Manager-a

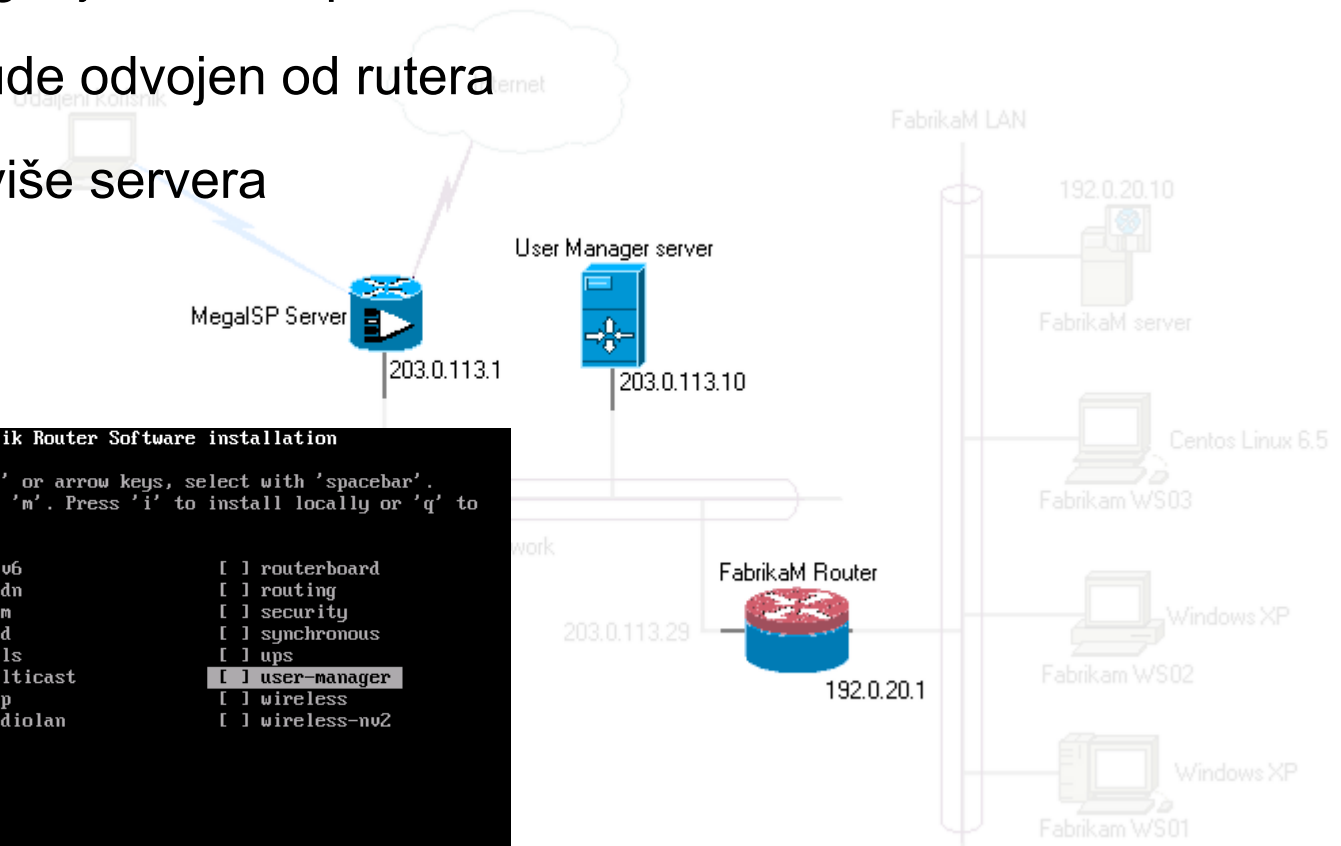
Instalacija paketa

- User Manager je dodatni paket
- Može da bude odvojen od rutera
- Opslužuje više servera

```
Welcome to MikroTik Router Software installation
Move around menu using 'p' and 'n' or arrow keys, select with 'spacebar'.
Select all with 'a', minimum with 'm'. Press 'i' to install locally or 'q' to
cancel and reboot.

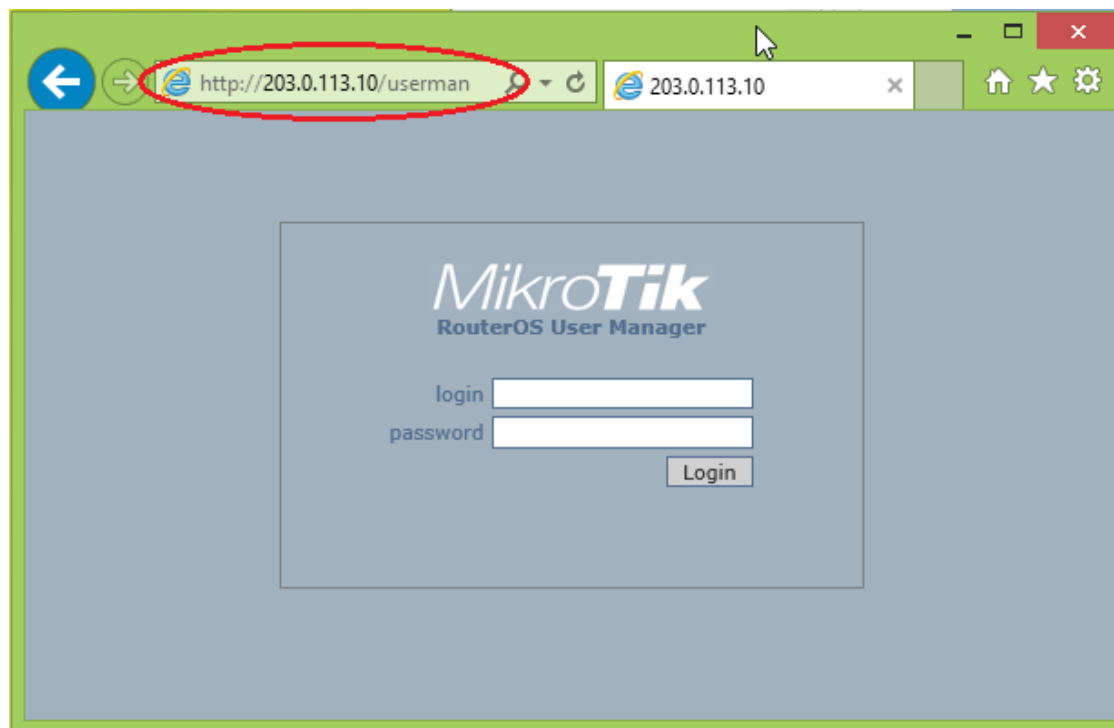
[X] system          [ ] ipv6          [ ] routerboard
[ ] ppp             [ ] isdn          [ ] routing
[ ] dhcp            [ ] kvm           [ ] security
[ ] advanced-tools  [ ] lcd           [ ] synchronous
[ ] arlan           [ ] mpls          [ ] ups
[ ] calea           [ ] multicast    [ ] user-manager
[ ] gps             [ ] ntp           [ ] wireless
[ ] hotspot         [ ] radiolan       [ ] wireless-nv2

user-manager (depends on system):
RouterOS User Manager service
```



Kako upravljati servisom?

- User Manager ima svoju Web stranicu
- `http(s)://um_server/userman`
- Komandna linija `/tool user-manager`



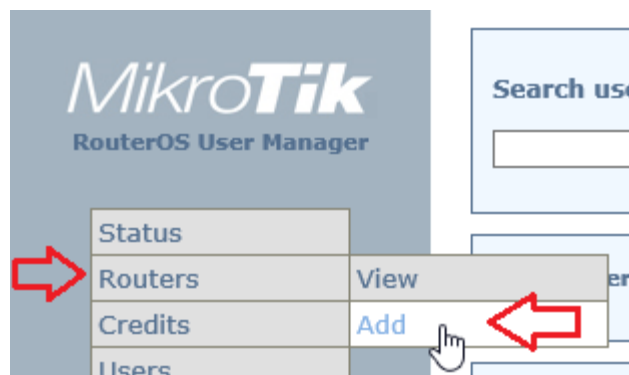
User Manager administrator

- Glavni nalog je admin
- Nalog nema lozinku

The screenshot shows the MikroTik RouterOS User Manager web interface in a browser window. The address bar shows the URL `http://203.0.113.10/userman`. The page has a green header bar with the MikroTik logo and the text "RouterOS User Manager". On the left, there is a sidebar menu with links: Status, Routers, Credits, Users, Sessions, Customers, Reports, Logs, and Logout. The main content area is divided into three sections. The top section is titled "Search users" and contains a text input field and a "Search" button. The middle section shows "Active users: 0" and a "Show" button. The bottom section shows "Active sessions: 0" and a "Show" button. On the right, there is a large form titled "Add users". It contains several fields: "Number of users:" with a value of 1, "Rate limits:" with a plus sign, "Uptime limit:" with a value of 0s, "Group:" with an empty field, "Pool name:" with an empty field, "Download limit:" with an empty field, "Upload limit:" with an empty field, and "Transfer limit:" with an empty field. Below these fields are two checkboxes: "Prepaid:" with a dropdown menu showing "no credits available", and "Generate CSV file" and "Generate vouchers" both checked. At the bottom right of the form is an "Add" button.

Dodajemo ruter

- Definišemo rutere koji mogu da pristupe



The 'Add router' dialog box is shown. It contains the following fields and options:

- Name:** MegaISP
- IP Address:** 203.0.113.1
- Shared Secret:** radius123
- Log events:**
 - ☒ Authorisation ok
 - ☒ Authorisation failed
 - ☐ Accounting ok
 - ☒ Accounting failed

An 'Add' button is located at the bottom right of the dialog.

The 'Routers' table displays a list of configured routers. Below the table, there is an 'Edit' button and a 'Search' input field.

<input type="checkbox"/>	▽ Name △	▽ IP Address △	▽ Shared secret △	Log events
<input type="checkbox"/>	FabrikaM	203.0.113.29	radius123	auth ok & auth fail & acct fail
<input type="checkbox"/>	MegaISP	203.0.113.1	radius123	auth ok & auth fail & acct fail

Per page: 20

Edit [input field] Search

Disable

Enable

Remove

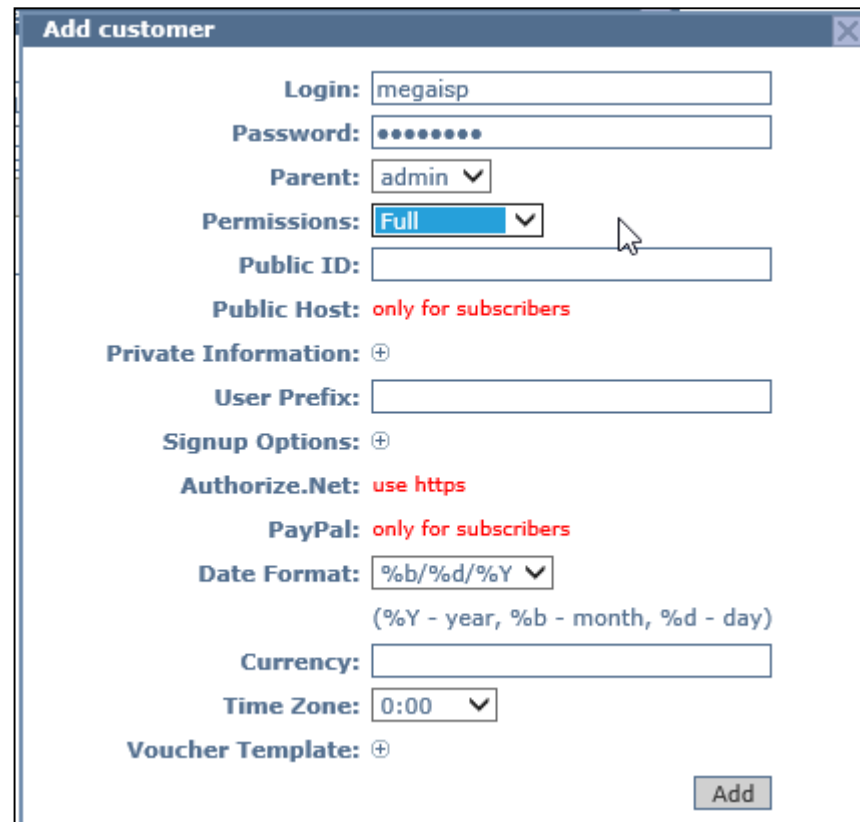
Reset counters

Korisnički nivoi u User Manageru

- User manager poznaje tri nivoa korisnika:
 - Subscriber
 - Customer
 - User
- Grafičko okruženje omogućava samo:
 - Customer
 - User

Dodajemo customer-a

- Customer je administrator
- Svi customer-i su ravnopravni
- Administriraju:
 - korisnike
 - uređaje
 - vaučere



Add customer

Login: megaisp

Password: ●●●●●●

Parent: admin ▼

Permissions: Full ▼

Public ID:

Public Host: only for subscribers

Private Information: +

User Prefix:

Signup Options: +

Authorize.Net: use https

PayPal: only for subscribers

Date Format: %b/%d/%Y ▼
(%Y - year, %b - month, %d - day)

Currency:

Time Zone: 0:00 ▼

Voucher Template: +

Add

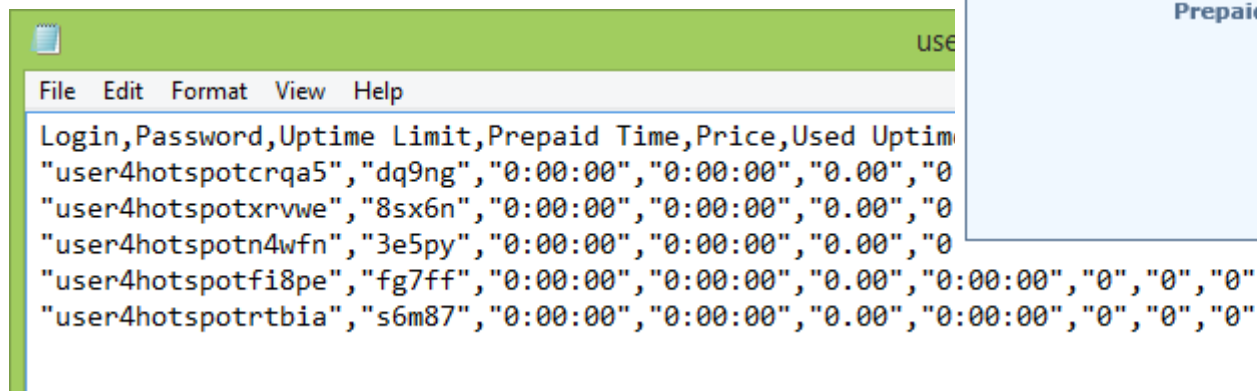
Privilegije customer-a

- Postoje 4 nivoa privilegija koje možemo zadati:
 - Owner
 - Full
 - Read-Write
 - Read
- Owner se automatski dodeljuje svakom subscriber-u
- U zavisnosti od podele posla, Customer nalog dobija neki od ostalih nivoa
- Detaljna tabela prava po nivou privilegija se nalazi na Web stranici http://wiki.mikrotik.com/wiki/User_Manager/Permissions

Dodajemo korisnike

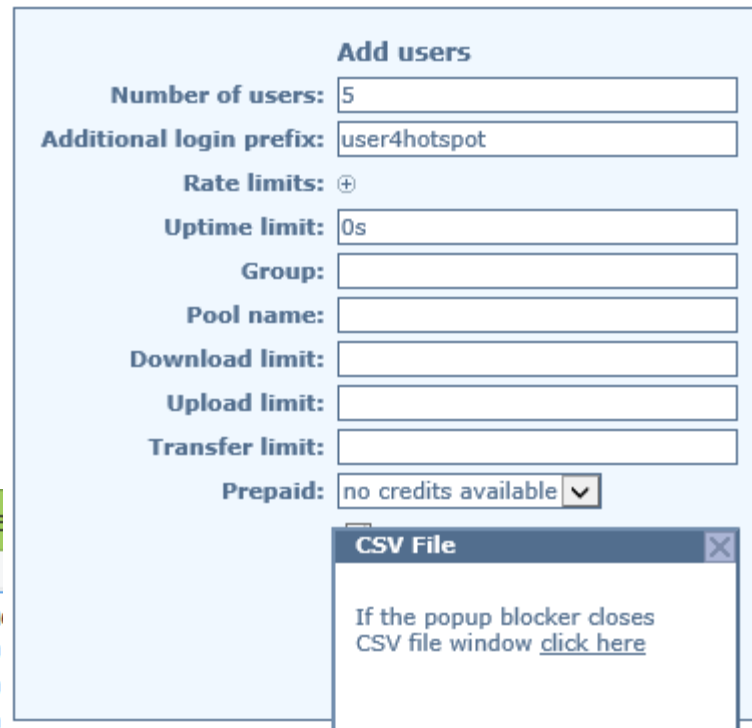
■ Korisnici se mogu dodati:

- pojedinačno
- u grupi (batch mode)



A screenshot of a text editor window with a green title bar and menu bar (File, Edit, Format, View, Help). The text content is a CSV file with the following data:

Login	Password	Uptime Limit	Prepaid Time	Price	Used Uptime
"user4hotspotcrqa5"	"dq9ng"	"0:00:00"	"0:00:00"	"0.00"	"0"
"user4hotspotxrvwe"	"8sx6n"	"0:00:00"	"0:00:00"	"0.00"	"0"
"user4hotspotn4wfn"	"3e5py"	"0:00:00"	"0:00:00"	"0.00"	"0"
"user4hotspotfi8pe"	"fg7ff"	"0:00:00"	"0:00:00"	"0.00"	"0:00:00", "0", "0", "0"
"user4hotspotrtbia"	"s6m87"	"0:00:00"	"0:00:00"	"0.00"	"0:00:00", "0", "0", "0"



A screenshot of a web form titled "Add users". The form contains the following fields and options:

- Number of users:** 5
- Additional login prefix:** user4hotspot
- Rate limits:** ⊕
- Uptime limit:** 0s
- Group:** (empty text box)
- Pool name:** (empty text box)
- Download limit:** (empty text box)
- Upload limit:** (empty text box)
- Transfer limit:** (empty text box)
- Prepaid:** no credits available (dropdown menu)

A "CSV File" popup window is overlaid on the bottom right of the form, containing the text: "If the popup blocker closes CSV file window [click here](#)".

Kredit za korisnike

- Kredit – plaćeni pristup
- Vremensko ograničenje
- Sa ili bez produženja

Credits				
				Per page: 20 ▼
<input type="checkbox"/>	▽ Name △	▽ Time △	▽ Full Price △	▽ Extended Price △
<input type="checkbox"/>	Test	5m	10.00	10.00
Remove			Search	

Users							
							Per page: 20 ▼
<input type="checkbox"/>	▽ Username △	▽ Prepaid △	▽ Used △	Left	▽ Price △	▽ Download △	▽ Upload △
<input type="checkbox"/>	user4hotspotcrqa5	5m	13m:13s	0s	10.00	45.8 MiB	748.0 KiB
<input type="checkbox"/>	user4hotspotxrvwe	unlimited	0s	0s	0.00	0 B	0 B
<input type="checkbox"/>	user4hotspotn4wfn	unlimited	0s	0s	0.00	0 B	0 B
<input type="checkbox"/>	user4hotspotfi8pe	1h	0s	1h	100.00	0 B	0 B
<input type="checkbox"/>	user4hotspotrtbia	unlimited	0s	0s	0.00	0 B	0 B
<input type="checkbox"/>	user4pppoe01	unlimited	39m:5s	0s	0.00	748 B	1976 B
Edit		Extend	Generate			Search	

Ali ja želim moje naloge

- Treba napraviti novog subscriber-a
- Svaki subscriber vidi svoje uređaje, administratore, korisnike, kredite, sesije, izveštaje
- Subscriber se dodaje iz komandne linije

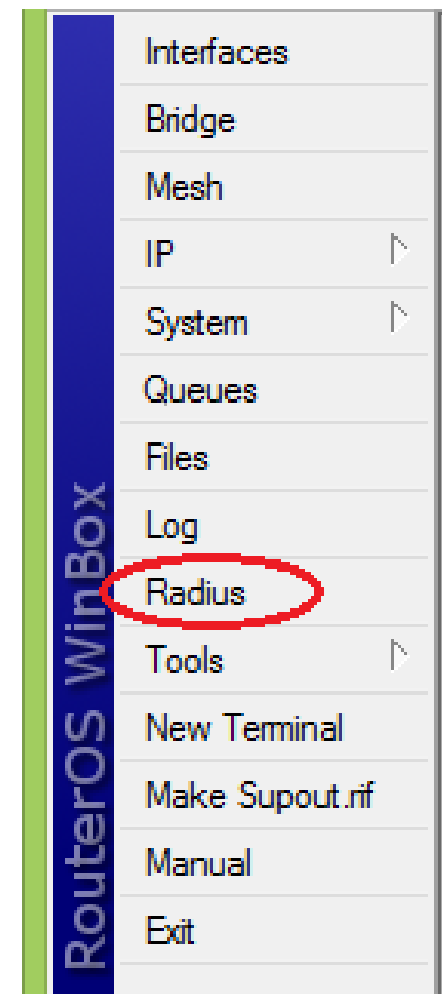
```
/tool user-manager customer add login=megaisp password=password permissions=owner
```

```
[admin@MikroTik] /tool user-manager customer> print
Flags: X - disabled
0  subscriber=admin login="admin" password="" time-zone="+00:00" permissions=owner parent=admin signup-allowed=no
   paypal-allowed=no paypal-secure-response=no paypal-accept-pending=no
1  subscriber=megaisp login="megaisp" password="password" time-zone="+00:00" permissions=owner parent=megaisp
   signup-allowed=no paypal-allowed=no paypal-secure-response=no paypal-accept-pending=no
2  subscriber=fabrikam login="fabrikam" password="password" time-zone="+00:00" permissions=owner parent=fabrikam
   signup-allowed=no paypal-allowed=no paypal-secure-response=no paypal-accept-pending=no
[admin@MikroTik] /tool user-manager customer>
```


RADIUS klient

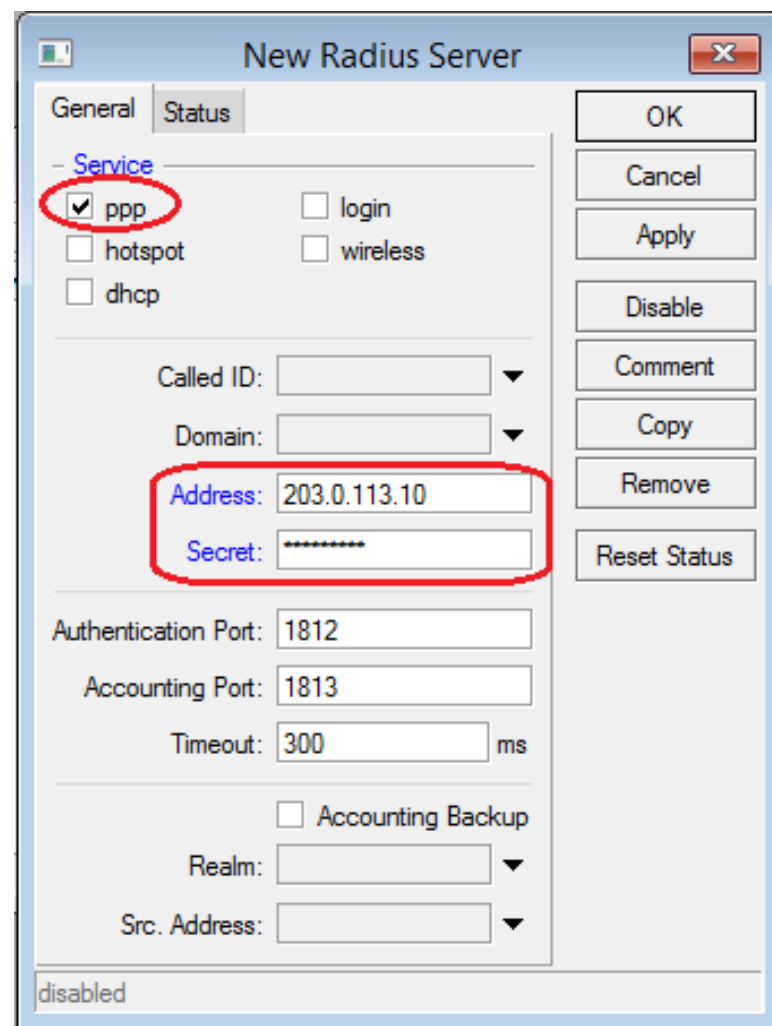
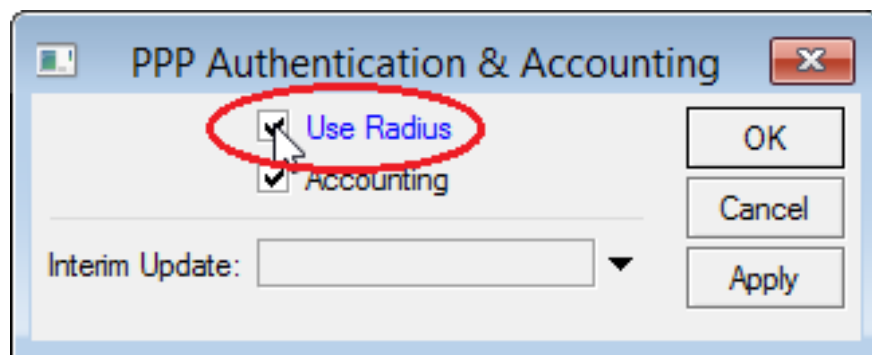
Mikrotik RADIUS klijent

- Mikrotik ima ugrađen RADIUS klijent
- Klijent komunicira sa serverom u ime servisa:
 - HotSpot
 - PPP/PPTP/L2TP/PPPoE
 - DHCP
 - Wireless
 - RouterOS pristup



RADIUS klijent za PPP servise

- U PPP AAA se omogući korišćenje RADIUS servisa
- Podesi se ugrađeni RADIUS klijent za PPP servis



RADIUS klijent za HotSpot servis

- U HotSpot profilu se omogući RADIUS autentifikacija
- Podesi se ugrađeni RADIUS klijent

The screenshot shows the 'Hotspot Server Profile <default>' dialog box with the 'RADIUS' tab selected. The 'Use RADIUS' checkbox is checked and circled in red. Below it, the 'Default Domain' is empty. The 'Location ID' and 'Location Name' fields are empty. The 'MAC Format' is set to 'XX:XX:XX:XX:XX:XX'. The 'Accounting' checkbox is checked. The 'Interim Update' field is empty. The 'NAS Port Type' is set to 'ethernet' and is circled in red. The 'default' profile name is shown at the bottom.

The screenshot shows the 'New Radius Server' dialog box with the 'General' tab selected. The 'Service' section has the 'hotspot' checkbox checked and circled in red. The 'Address' field is set to '203.0.113.10' and the 'Secret' field is filled with asterisks; both are circled in red. The 'Authentication Port' is 1812, 'Accounting Port' is 1813, and 'Timeout' is 300 ms. The 'Accounting Backup' checkbox is unchecked. The 'Realm' and 'Src. Address' fields are empty. The 'disabled' status is shown at the bottom.

RADIUS autentifikuje korisnike

- Svi klijenti se autentikuju kroz RADIUS (User Manager)

The screenshot shows the 'PPP Active User <pppoe_user01>' dialog box. The 'Service' field is circled in red and contains the value 'pppoe'. Below the dialog, the 'PPP' interface window shows a table of active users. The 'RADIUS' label in the interface is also circled in red. The table lists several users, with the last three being pppoe users.

	Name	Service	Caller ID	Address	Uptime
L	ppp_user01	async		172.16.14.51	03:41:00
L	ppp_user02	async		172.16.14.50	03:40:36
R	pppoe_user01	pppoe	00:03:FF:8A:17:1D	172.16.14.53	00:01:32
R	pppoe_user02	pppoe	00:03:FF:8B:17:1D	172.16.14.52	00:01:58
R	pppoe_user03	pppoe	00:03:FF:8A:91:1D	172.16.14.49	00:02:24

The screenshot shows the 'Hotspot Active User <user4hotspotcra...>' dialog box. The 'radius' label at the bottom is circled in red. The dialog displays various fields for user authentication and session management.

General Statistics Traffic

Server: FabrikaM_HotSpot
User: user4hotspotcra5
Domain:
Address: 192.0.20.122
MAC Address: 00:15:5D:2A:CB:1A
Login By: http-chap
Uptime: 00:00:26
Idle Time: 00:00:12
Session Time Left:
Idle Timeout:
Keepalive Timeout: 00:02:00
Limit Bytes In:
Limit Bytes Out:
Limit Bytes Total:

radius blocked

User manager za krajnjeg korisnika

- [http\(s\)://ip_servera/user](http(s)://ip_servera/user)
- Krajnji korisnik ima uvid u svoj nalog

The screenshot displays the MikroTik RouterOS User Manager web interface. The left sidebar contains the MikroTik logo and navigation links for Status, Settings, and Logout. The main content area is divided into three sections: Summary, Credits, and Sessions.

Summary

- Prepaid Time: 30m
- Total price: 60.00
- Uptime Limit: 0s
- Uptime Used: 21m28s
- Download Used: 45.8 MiB
- Upload Used: 758.3 KiB

Credits

Duration	Price	Start Time	Used Time	End Time
5m	10.00	Sep/23/2014 17:12:34	5m	Sep/23/2014 17:17:34
5m	10.00	Sep/23/2014 17:20:11	1m:29s	Sep/23/2014 17:25:11
5m	10.00	Sep/23/2014 17:30:17	5m	Sep/23/2014 17:35:17
5m	10.00	Sep/23/2014 17:35:18	1m:46s	Sep/23/2014 17:40:18
5m	10.00	Sep/23/2014 17:40:18	0s	Sep/23/2014 17:45:18
5m	10.00	Sep/23/2014 17:45:18	0s	Sep/23/2014 17:50:18

Sessions

ID	From Time	Till Time	Uptime	Download	Upload
<input type="checkbox"/> 3	Sep/23/2014 17:02:00	Sep/23/2014 17:08:36	6m:35s	25.9 MiB	421.2 KiB
<input type="checkbox"/> 4	Sep/23/2014 17:10:54	Sep/23/2014 17:12:31	1m:38s	6.6 KiB	2.1 KiB
<input type="checkbox"/> 5	Sep/23/2014 17:12:34	Sep/23/2014 17:17:34	5m	19.9 MiB	324.6 KiB
<input type="checkbox"/> 6	Sep/23/2014 17:20:11	Sep/23/2014 17:21:40	1m:29s	6.6 KiB	1968 B
<input type="checkbox"/> 7	Sep/23/2014 17:30:17	Sep/23/2014 17:35:17	5m	17.6 KiB	5.7 KiB
<input type="checkbox"/> 8	Sep/23/2014 17:35:18	Sep/23/2014 17:37:03	1m:46s	7.2 KiB	2.6 KiB
<input type="checkbox"/> 9	Sep/23/2014 17:37:22	Sep/23/2014 17:37:22	0s	0 B	0 B

Korisnički portal u višeklijentskom okruženju

- http://ip_servera/user?subs=PublisherID
- PublisherID se zadaje za prvi Customer nalog

Edit customer

Login:

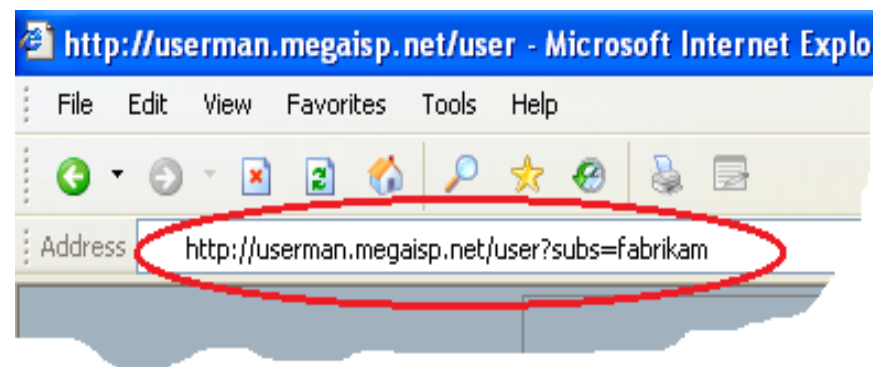
Password:

Parent: ▼

Permissions: ▼

Public ID:

Public Host:



Address **http://userman.megaisp.net/user**

MikroTik
RouterOS User Manager

Status
Settings
Logout

First Name:

Last Name:

Phone:

Location:

Email:

Change password (leave blank to keep the old one):
New password:

Zaključak

Pričali smo o ovome

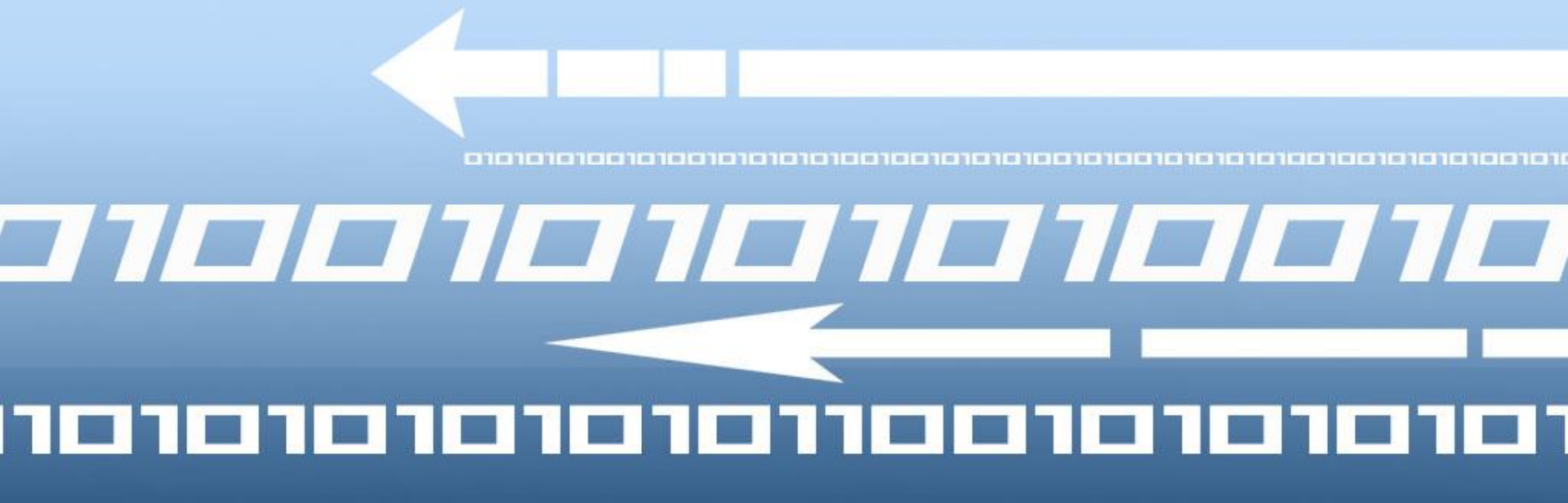
- Smanjite troškove Interneta – kontrolirajte protok
- Prenesite deo administracije na lokalnog administratora ili krajnjeg korisnika
- Sprečite upad u bežičnu mrežu i zloupotrebe
- Odgovor – Mikrotik HotSpot i Mikrotik User Manager

Šta dalje?

- Konsultujte korisničko uputstvo
- Pogledajte Mikrotik Wiki za više informacija i studije slučaja
- Kontaktirajte predavača na adrese e-pošte:

sstanisic@algotech.rs

s.stanisic@beotel.net



Hvala na pažnji !!!