

Dynamic VLAN Assignment with RADIUS and CAPsMAN Configuration Example

MUM China - April 10, 2016

Jesse Liu, Lethbridge

About Me

- **Jesse Liu, Lethbridge**
 - Over 10 years experience using RouterOS
 - Specialization in Wireless, Tunnel and Routing
 - MikroTik Certified Consultant
 - MikroTik MTCNA, MTCWE, MTCTCE Certifications
 - Cisco CCNP, CCDP Certifications

Special Thanks



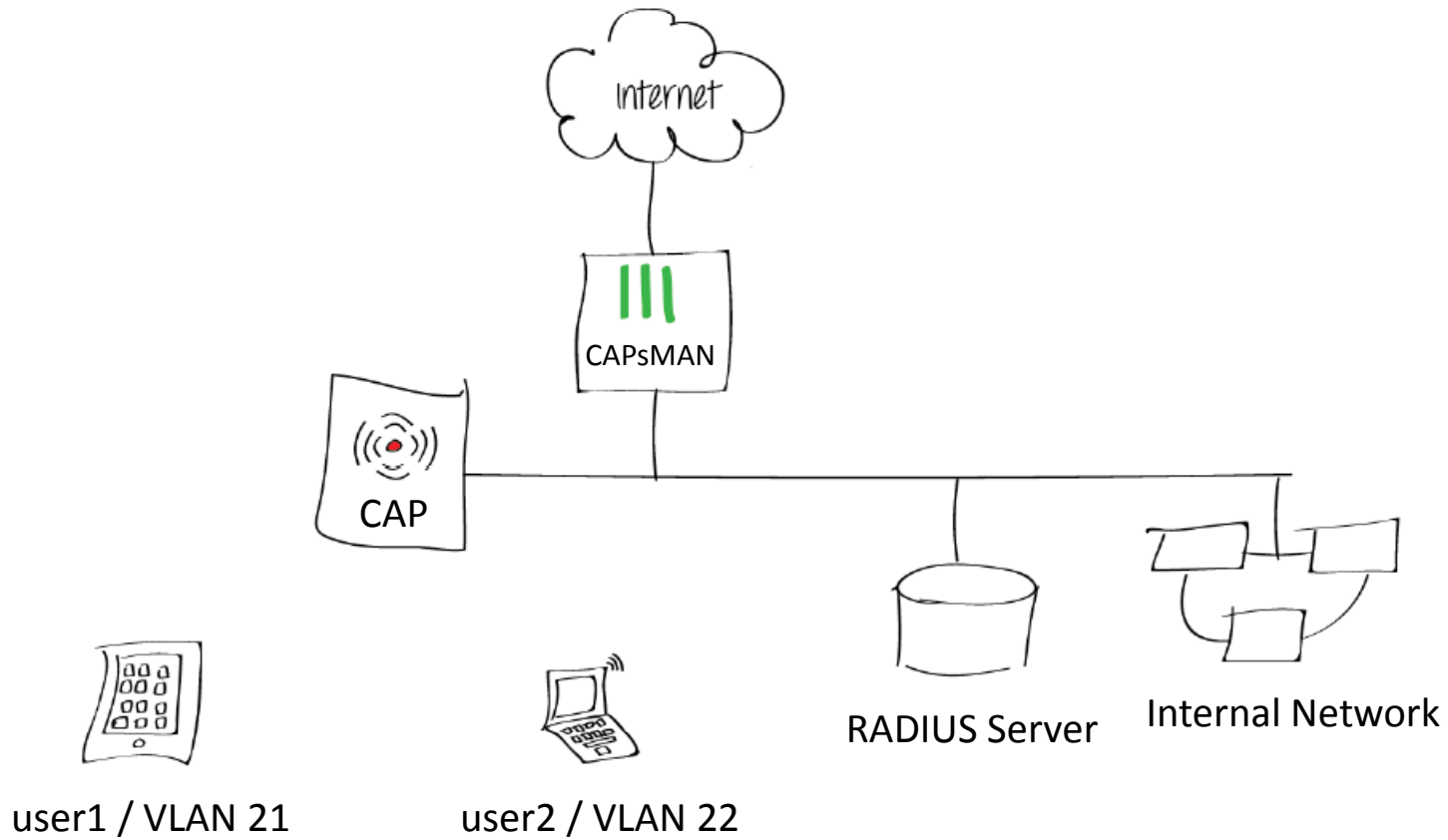
802.1X

- 802.1X is NOT an encryption type. It is basically just a per-user (e.g. username and password) authentication mechanism.
- WPA2 is a security scheme that specifies two main aspects of your wireless security:
 - Authentication: Your choice of PSK ("Personal") or **EAP ("Enterprise")**.
 - Encryption: Always AES-CCMP.

Dynamic VLAN assignment

- VLANs are used to assign wireless users to different networks without requiring the use of multiple SSIDs.
- Each user's VLAN assignment is stored in the user database of the RADIUS server that authenticates the users.

Network Diagram



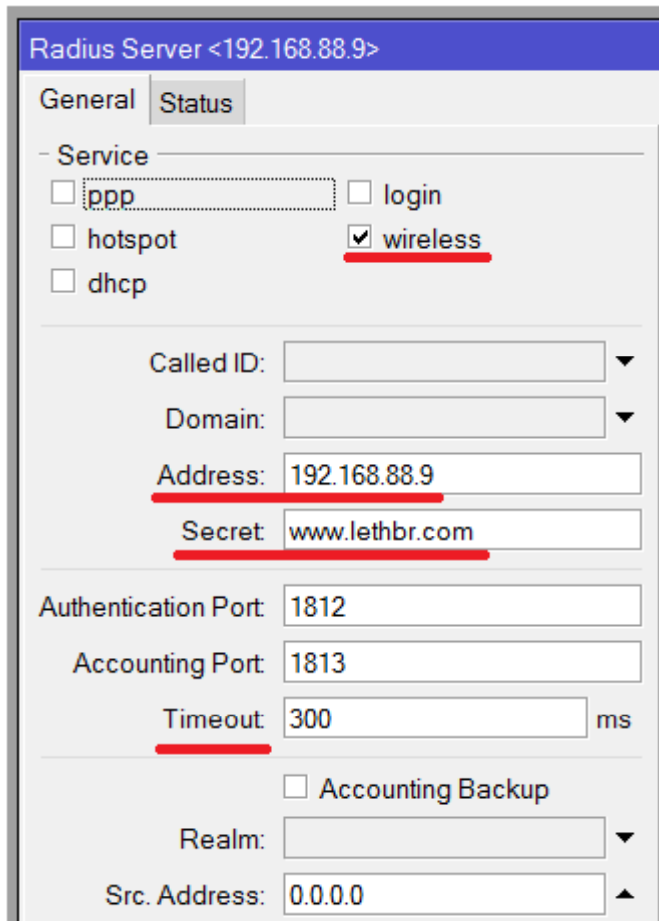
Security Cfg.

The screenshot shows the 'Security' configuration page for CAPs Configuration <cfg1>. The 'Security' tab is selected. The 'Authentication Type' section has 'WPA2 EAP' selected with a red underline. The 'Encryption' section has 'aes ccm' selected. The 'Group Encryption' dropdown is set to 'aes ccm'. The 'EAP Methods' dropdown is set to 'passthrough' with a red underline. Other fields like 'Passphrase', 'EAP Radius Accounting', 'TLS Mode', and 'TLS Certificate' are empty.

Field	Value
Security:	
Authentication Type:	<input type="checkbox"/> WPA PSK <input type="checkbox"/> WPA2 PSK <input type="checkbox"/> WPA EAP <input checked="" type="checkbox"/> WPA2 EAP
Encryption:	<input checked="" type="checkbox"/> aes ccm <input type="checkbox"/> tkip
Group Encryption:	aes ccm
Passphrase:	
EAP Methods:	passthrough
EAP Radius Accounting:	
TLS Mode:	
TLS Certificate:	

passthrough – Controller will relay authentication process to the RADIUS server.

Add a RADIUS Server for wireless service



Radius Server <192.168.88.9>

General Status

- Service

ppp login

hotspot wireless

dhcp

Called ID:

Domain:

Address: 192.168.88.9

Secret: www.lethbr.com

Authentication Port: 1812

Accounting Port: 1813

Timeout: 300 ms

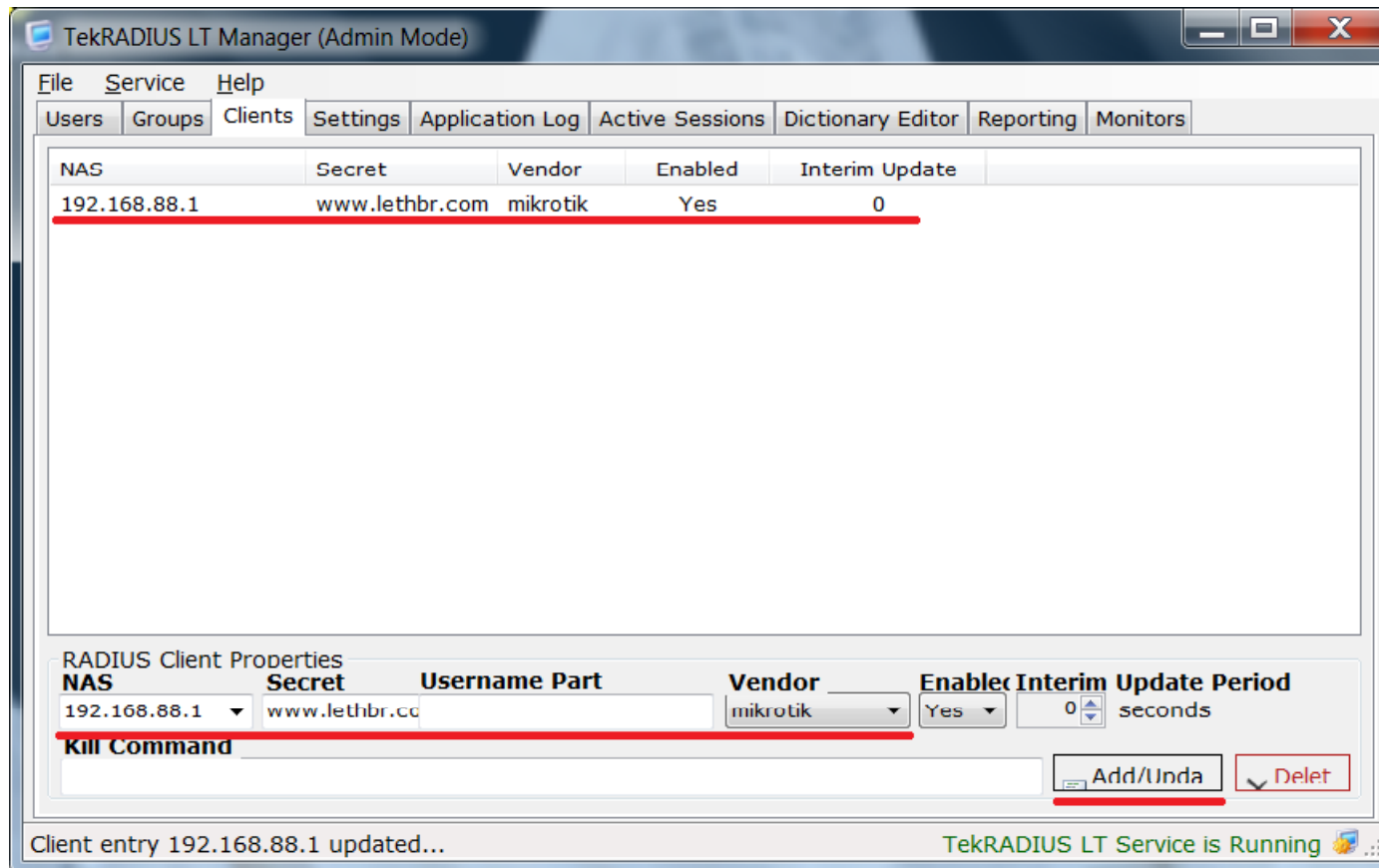
Accounting Backup

Realm:

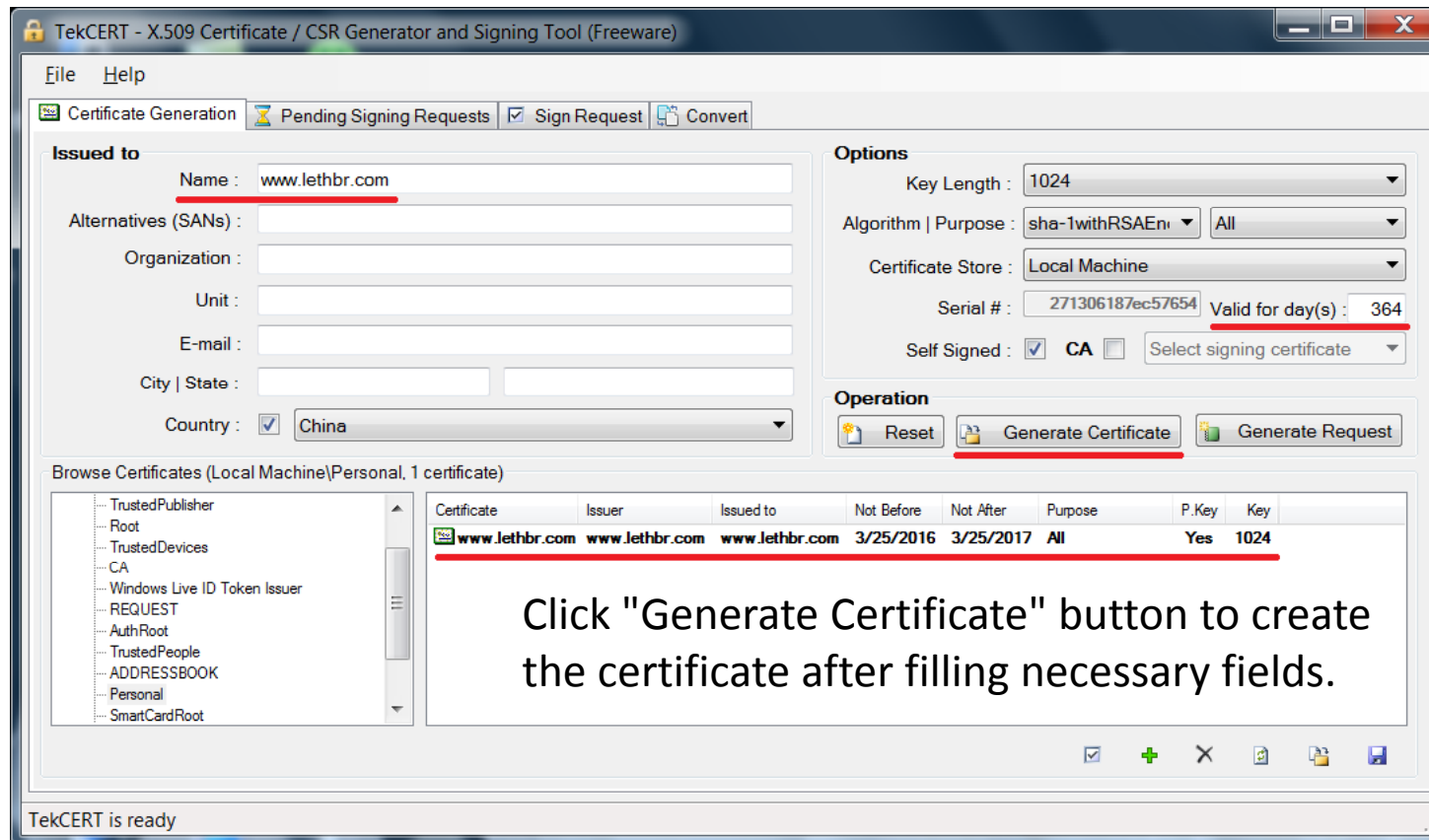
Src. Address: 0.0.0.0

Timeout – defines how much milliseconds can elapse while the answer arrives from the RADIUS server. If you are using slower connection to RADIUS server, set this timeout higher (3000-5000 ms).

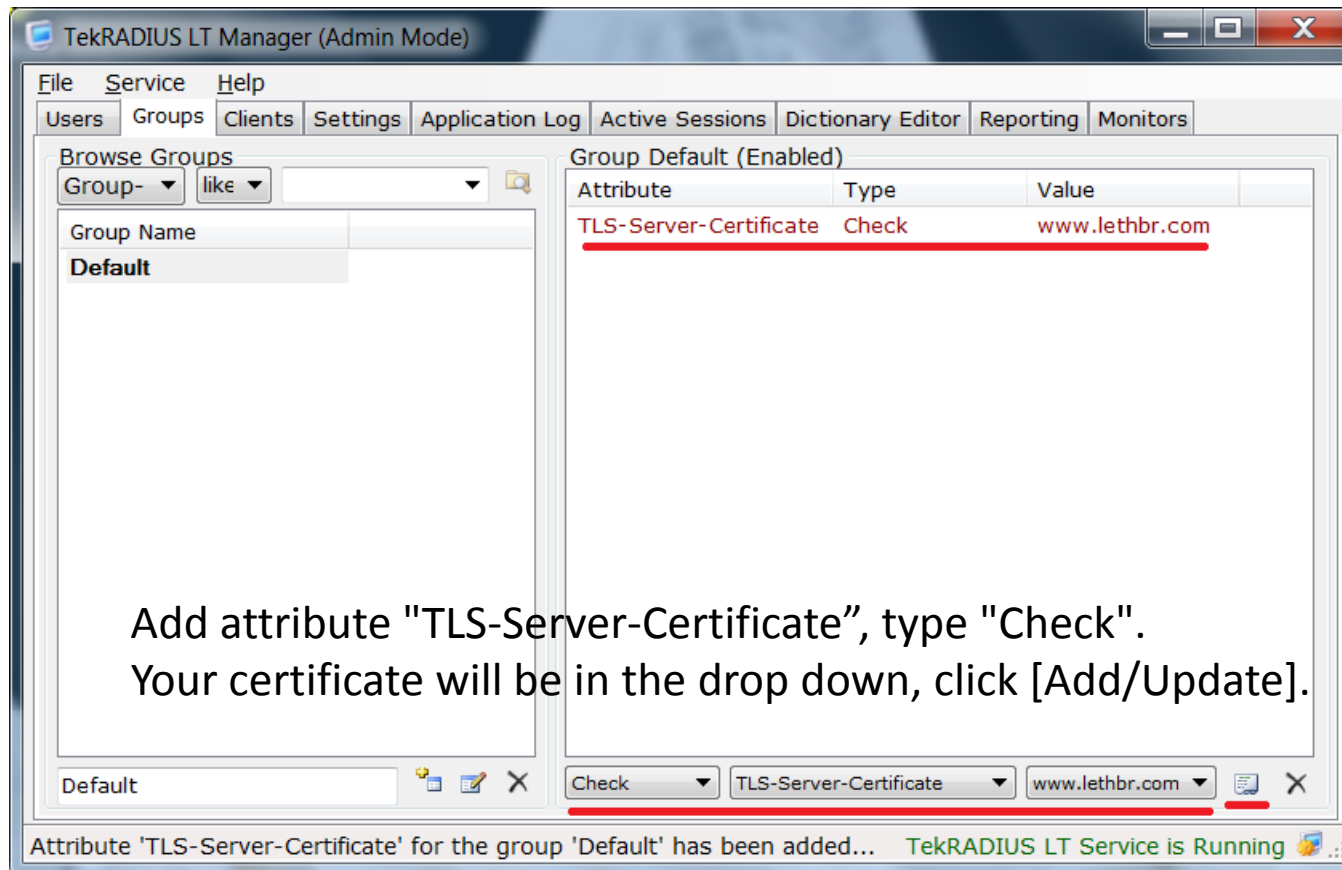
To create a RADIUS client



Create Self Signed Server Certificate



Import newly created certificate to RADIUS



The screenshot shows the TekRADIUS LT Manager (Admin Mode) interface. The 'Groups' tab is active, and the 'Default' group is selected. The 'Group Default (Enabled)' table shows the following attribute:

Attribute	Type	Value
TLS-Server-Certificate	Check	www.lethbr.com

Below the table, the attribute configuration is shown in a form:

Check | TLS-Server-Certificate | www.lethbr.com

A status bar at the bottom of the window displays the message: "Attribute 'TLS-Server-Certificate' for the group 'Default' has been added... TekRADIUS LT Service is Running".

Add attribute "TLS-Server-Certificate", type "Check".
Your certificate will be in the drop down, click [Add/Update].

VLAN Interfaces

Interface <vlan21>

General Status Traffic

Name: vlan21

Type: VLAN

MTU: 1500

L2 MTU: 1596

MAC Address: D4:CA:6D:00:00:00

ARP: enabled

VLAN ID: 21

Interface: bridge1

Use Service Tag

OK
Cancel
Apply
Disable
Comment
Copy
Remove
Torch

Interface List

Interface Ethernet EoIP Tunnel IP Tunnel GRE Tunnel VLAN VRRP Bonding LTE

Name	Type	MTU	L2 MTU	Tx	Rx
R vlan21	VLAN	1500	1596	0 bps	
R vlan22	VLAN	1500	1596	0 bps	
R vlan23	VLAN	1500	1596	0 bps	

Address List

Address	Network	Interface
172.31.21.1/24	172.31.21.0	vlan21
172.31.22.1/24	172.31.22.0	vlan22
172.31.23.1/24	172.31.23.0	vlan23

DHCP Server

DHCP Networks Leases Options Option Sets Alerts

Name	Interface	Relay	Lease Time	Address Pool
dhcp1	vlan21		00:10:00	dhcp_pool1
dhcp2	vlan22		00:10:00	dhcp_pool2
dhcp3	vlan23		00:10:00	dhcp_pool3

Datapath

CAPs Configuration <cfg1>

Wireless Channel Datapath Security

Datapath:

Bridge: bridge1

Bridge Cost:

Bridge Horizon:

Local Forwarding:

Client To Client Forwarding:

VLAN Mode: use tag

VLAN ID:

Enables and specifies type of VLAN tag to be assigned to interface (causes all received data to get tagged with VLAN tag and allows interface to only send out data tagged with given tag).

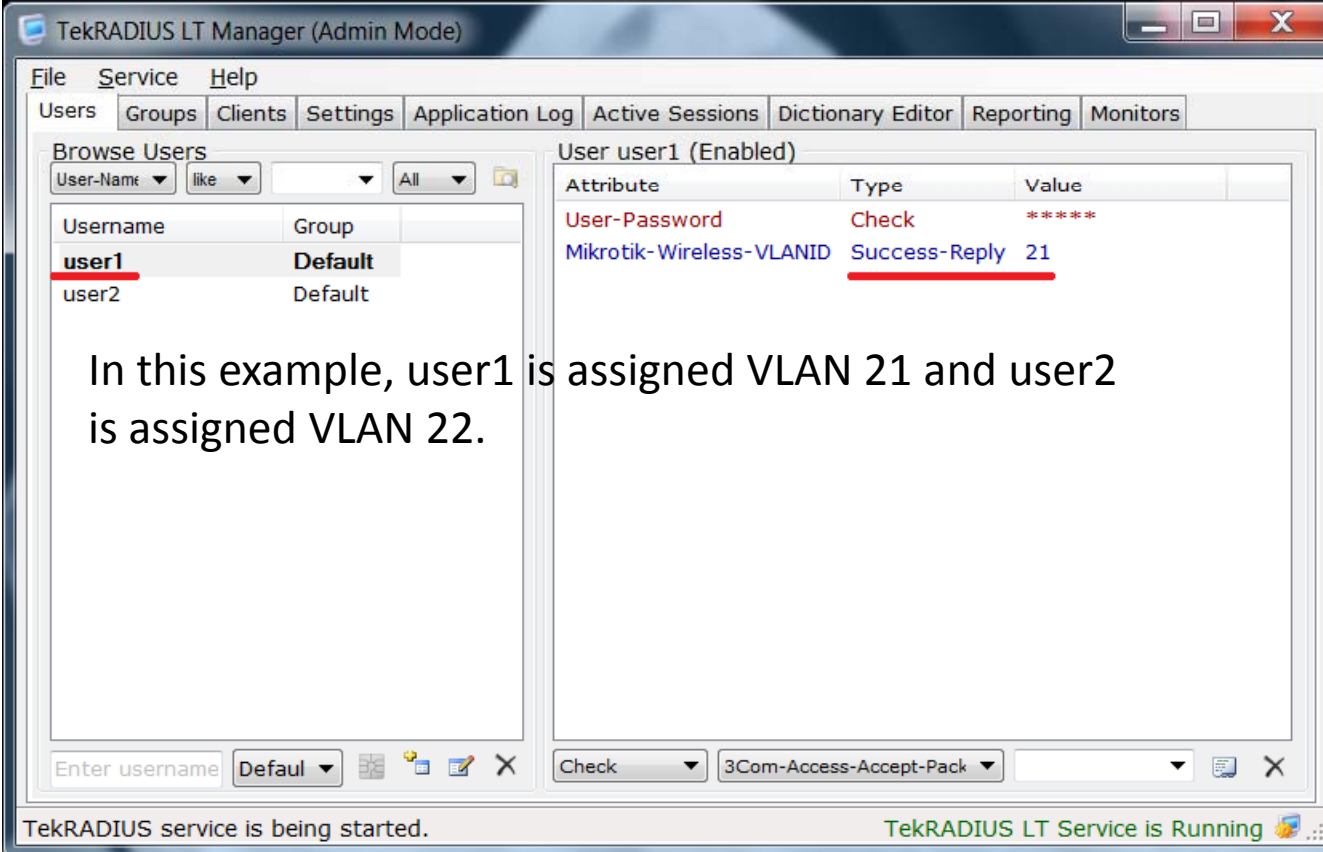
RADIUS attributes

- The RADIUS attributes used for the VLAN ID assignment are:

ATTRIBUTE	Mikrotik-Wireless-PSK	16	string
ATTRIBUTE	Mikrotik-Total-Limit	17	integer
ATTRIBUTE	Mikrotik-Total-Limit-Gigawords	18	integer
ATTRIBUTE	Mikrotik-Address-List	19	string
ATTRIBUTE	Mikrotik-Wireless-MPKey	20	string
ATTRIBUTE	Mikrotik-Wireless-Comment	21	string
ATTRIBUTE	Mikrotik-Delegated-IPv6-Pool	22	string
ATTRIBUTE	Mikrotik_DHCP_Option_Set	23	string
ATTRIBUTE	Mikrotik_DHCP_Option_Param_STR1	24	string
ATTRIBUTE	Mikrotik_DHCP_Option_Param_STR2	25	string
ATTRIBUTE	Mikrotik_Wireless_VLANID	26	integer
ATTRIBUTE	Mikrotik_Wireless_VLANIDtype	27	integer
ATTRIBUTE	Mikrotik_Wireless_Minsignal	28	string
ATTRIBUTE	Mikrotik_Wireless_Maxsignal	29	string

Specifies the VLAN ID

- For each user, add RADIUS attributes which specify the VLAN information to be sent to the CAPsMAN.



The screenshot shows the TekRADIUS LT Manager (Admin Mode) interface. The 'Users' tab is active, and the 'Browse Users' section shows a list of users. The 'user1' entry is highlighted, and its details are shown in the 'User user1 (Enabled)' section. The 'Mikrotik-Wireless-VLANID' attribute is set to 'Success-Reply 21'.

Attribute	Type	Value
User-Password	Check	*****
Mikrotik-Wireless-VLANID	Success-Reply	21

In this example, user1 is assigned VLAN 21 and user2 is assigned VLAN 22.

TekRADIUS service is being started. TekRADIUS LT Service is Running

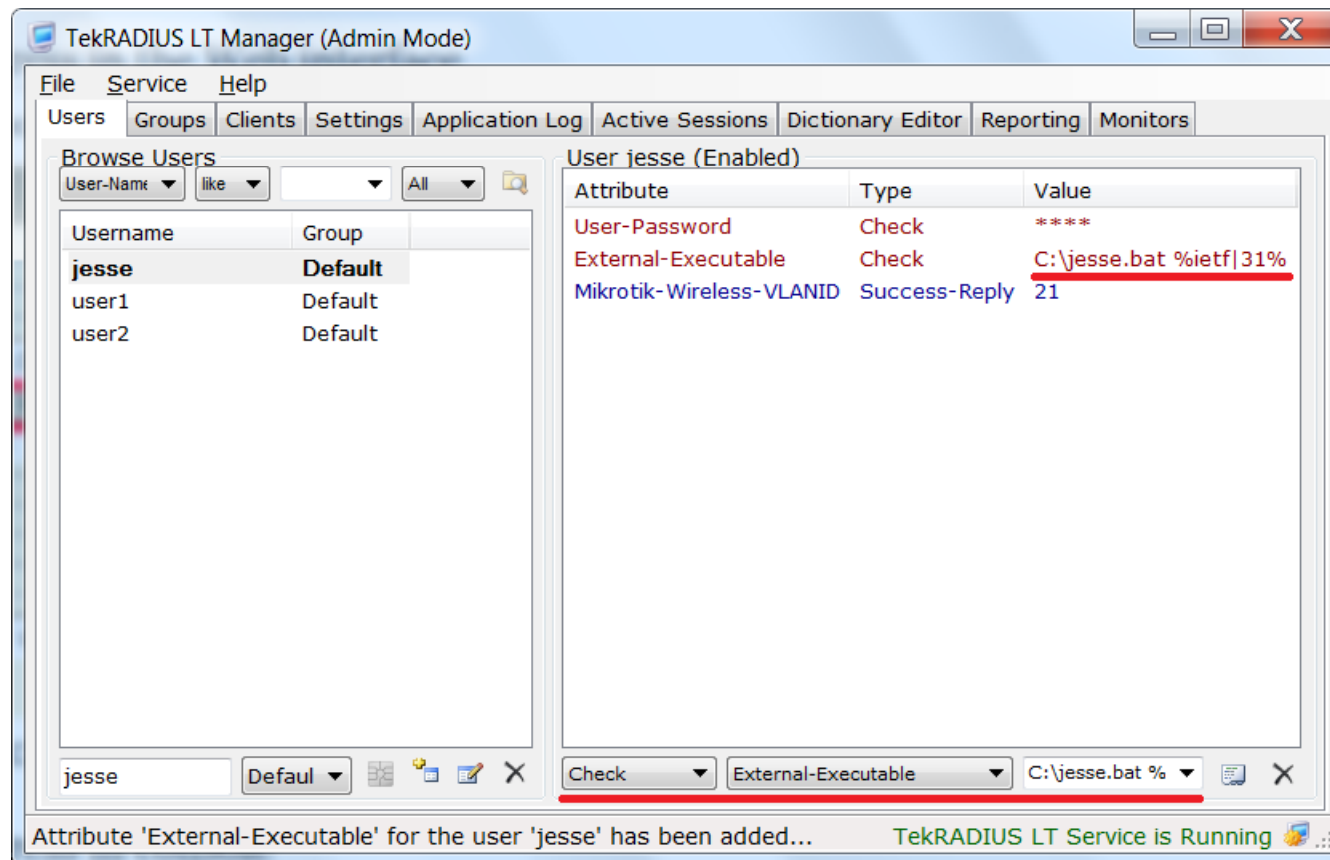
MAC address binding

The screenshot shows the TekRADIUS LT Manager (Admin Mode) interface. The 'Users' tab is active, and the 'Browse Users' section shows a list of users. The user 'jesse' is selected, and the 'User jesse (Enabled)' details are displayed on the right. The details include a table of attributes and their values.

Attribute	Type	Value
User-Password	Check	****
Calling-Station-Id	Check	20-82-C0- XXXXXXXXXX
Mikrotik-Wireless-VLANID	Success-Reply	21

At the bottom of the window, a status bar displays the message: "Attribute 'Calling-Station-Id' for the user 'jesse' has been added..." and "TekRADIUS LT Service is Running".

Bind multiple MAC addresses to one user



Bind multiple MAC addresses to one user

```
jesse.bat x
1 @echo off
2
3 IF "%1%" == "20-82-C0-11-55-18" Goto Success - Phone
4 IF "%1%" == "B4-CE-F6-57-81-88" Goto Success - Tablet
5 IF "%1%" == "84-3A-4B-07-00-50" Goto Success - Laptop
6
7 echo Fail
8 exit /b 1
9
10 :Success
11
12 echo Success
13 exit /b 0
```

Registration Table

- Description of an entry. Comment is taken from RADIUS attributes if specified.

The screenshot shows the CAPsMAN web interface with the 'Registration Table' tab selected. The table contains the following data:

Interface	SSID	MAC Address	Tx Rate	Rx Rate	Tx Signal	Rx Sign...	Uptime	Tx/Rx Packets	Tx/Rx Bytes
cap1	www.lethbr.com	20:82:C0:...	54Mbps	54Mbps	0	-52	00:00:5...	929/1 004	252.5 KiB/326....

Mikrotik-Wireless-Comment

The screenshot shows the TekRADIUS LT Manager (Admin Mode) interface. The main window is titled "TekRADIUS LT Manager (Admin Mode)" and has a menu bar with "File", "Service", and "Help". Below the menu bar are several tabs: "Users", "Groups", "Clients", "Settings", "Application Log", "Active Sessions", "Dictionary Editor", "Reporting", and "Monitors".

The "Users" tab is active, showing a "Browse Users" section on the left and a "User jesse (Enabled)" section on the right. The "Browse Users" section has a search bar with "User-Name" and "like" dropdowns, and a "All" dropdown. Below it is a table with columns "Username" and "Group".

Username	Group
jesse	Default
user1	Default
user2	Default

The "User jesse (Enabled)" section shows a table with columns "Attribute", "Type", and "Value".

Attribute	Type	Value
User-Password	Check	****
Calling-Station-Id	Check	20-82-C0- [REDACTED]
<u>Mikrotik-Wireless-Comment</u>	Success-Reply	Jesse
Mikrotik-Wireless-VLANID	Success-Reply	21

At the bottom of the window, there is a status bar with the text: "Attribute 'Mikrotik-Wireless-Comment' for the user 'jesse' has been added. TekRADIUS LT Service is Running".

EAP-TLS

- For RouterOS client, EAP-TLS is possible only.
- For RouterOS AP - to clients any EAP method is possible.

More information at:
<http://mum.mikrotik.com/2016/CN/agenda>

Thank you for participating