# 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

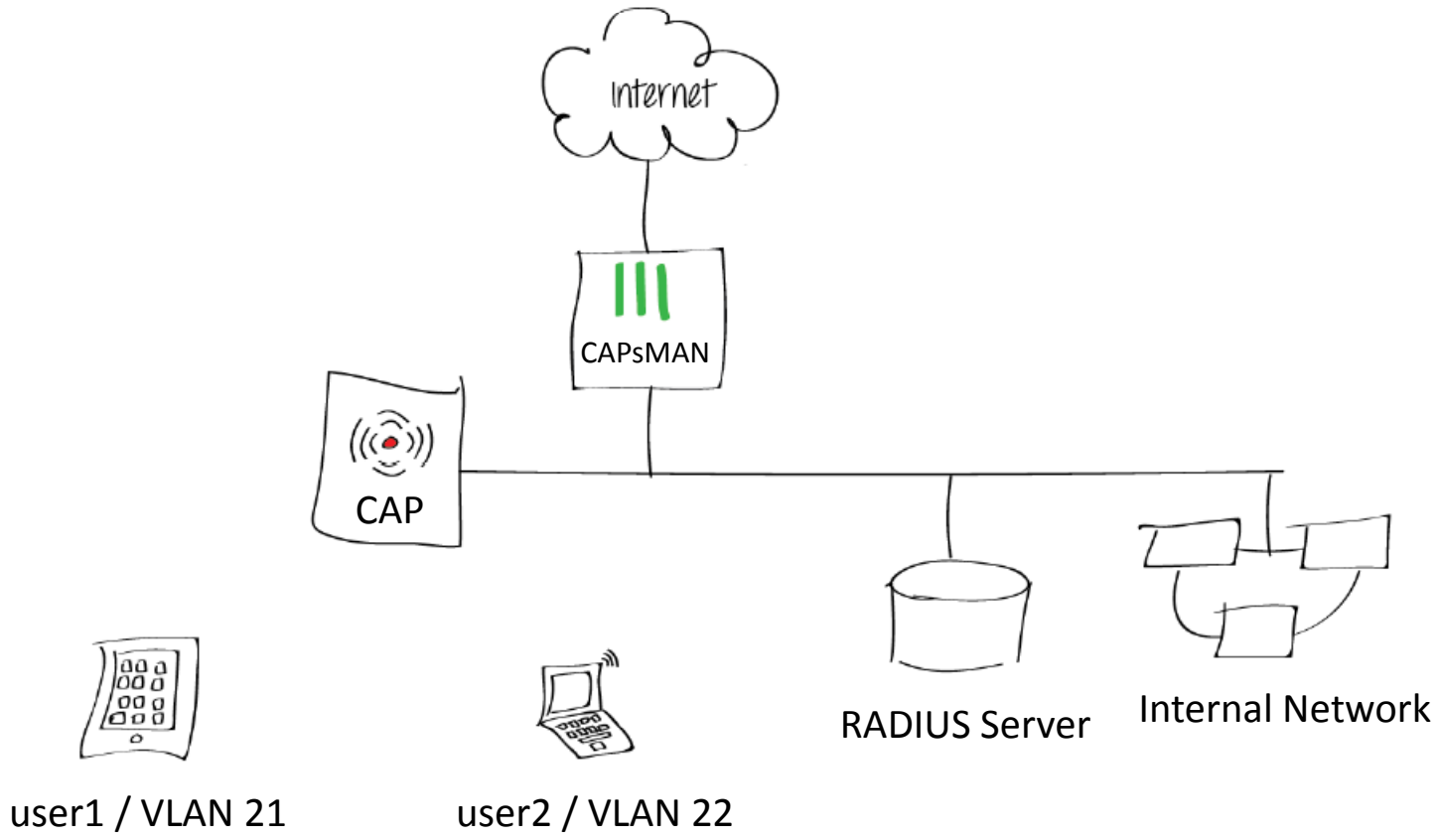

# 802.1X

- 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.

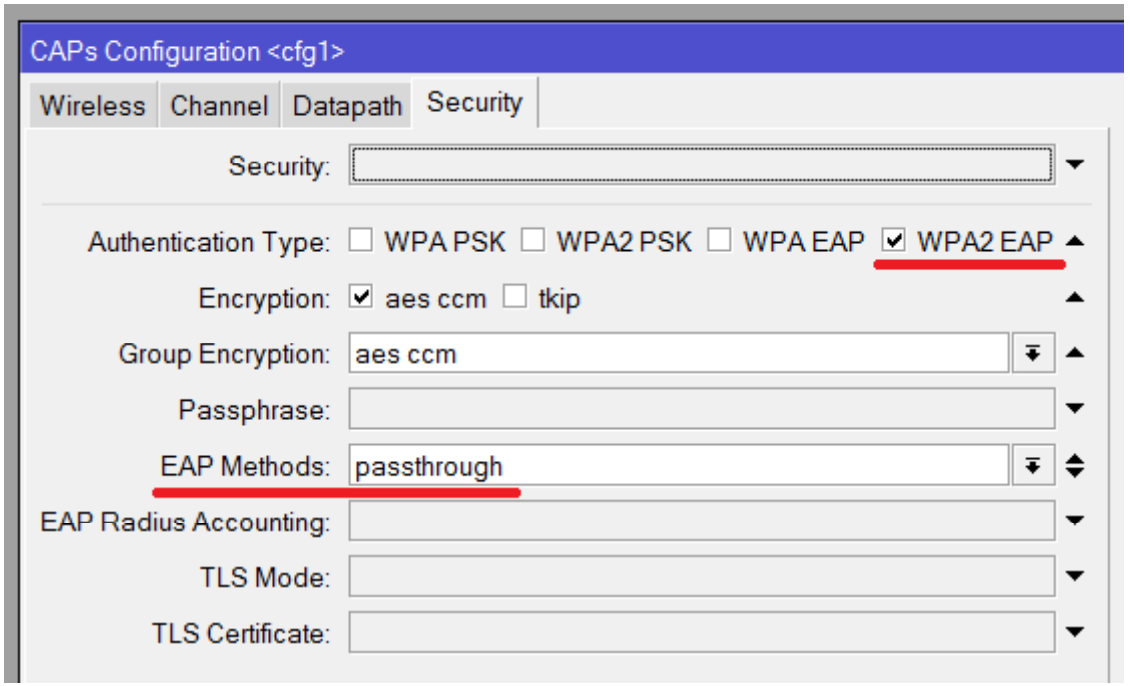
# Dynamic VLAN assignment

- 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

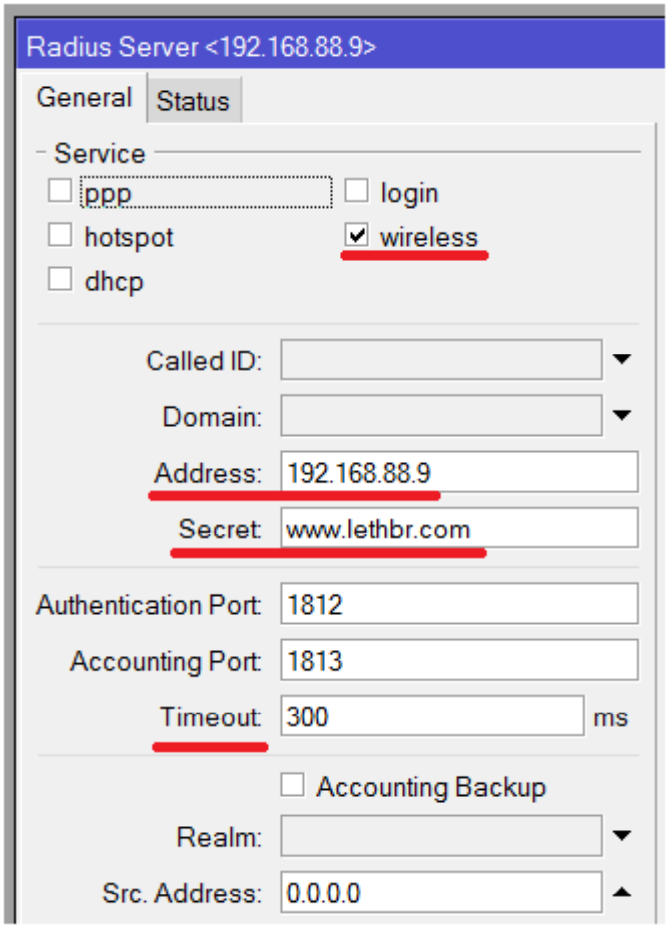


# Security Cfg.



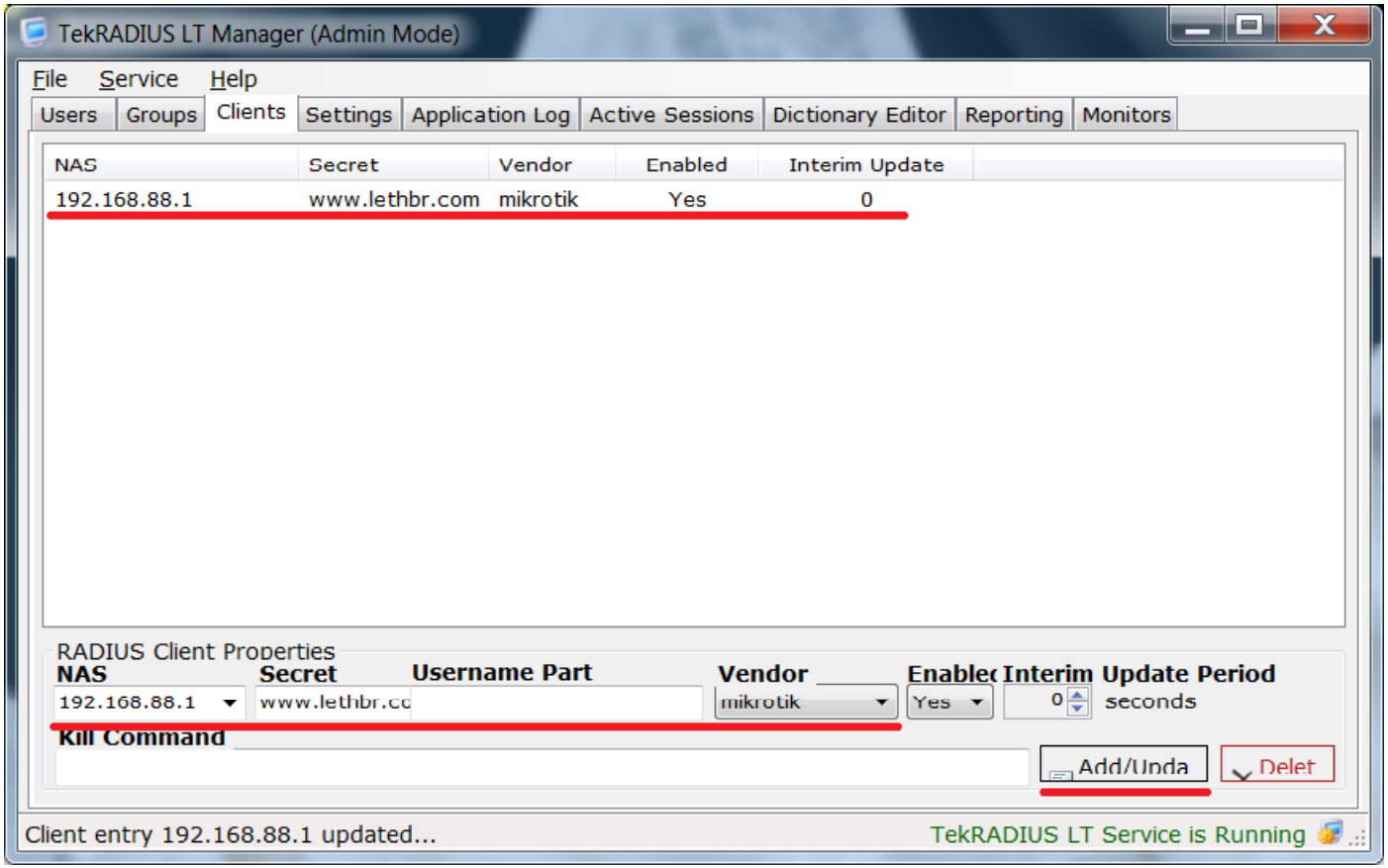

passthrough – Controller will relay authentication process to the RADIUS server.

# Add a RADIUS Server for wireless service

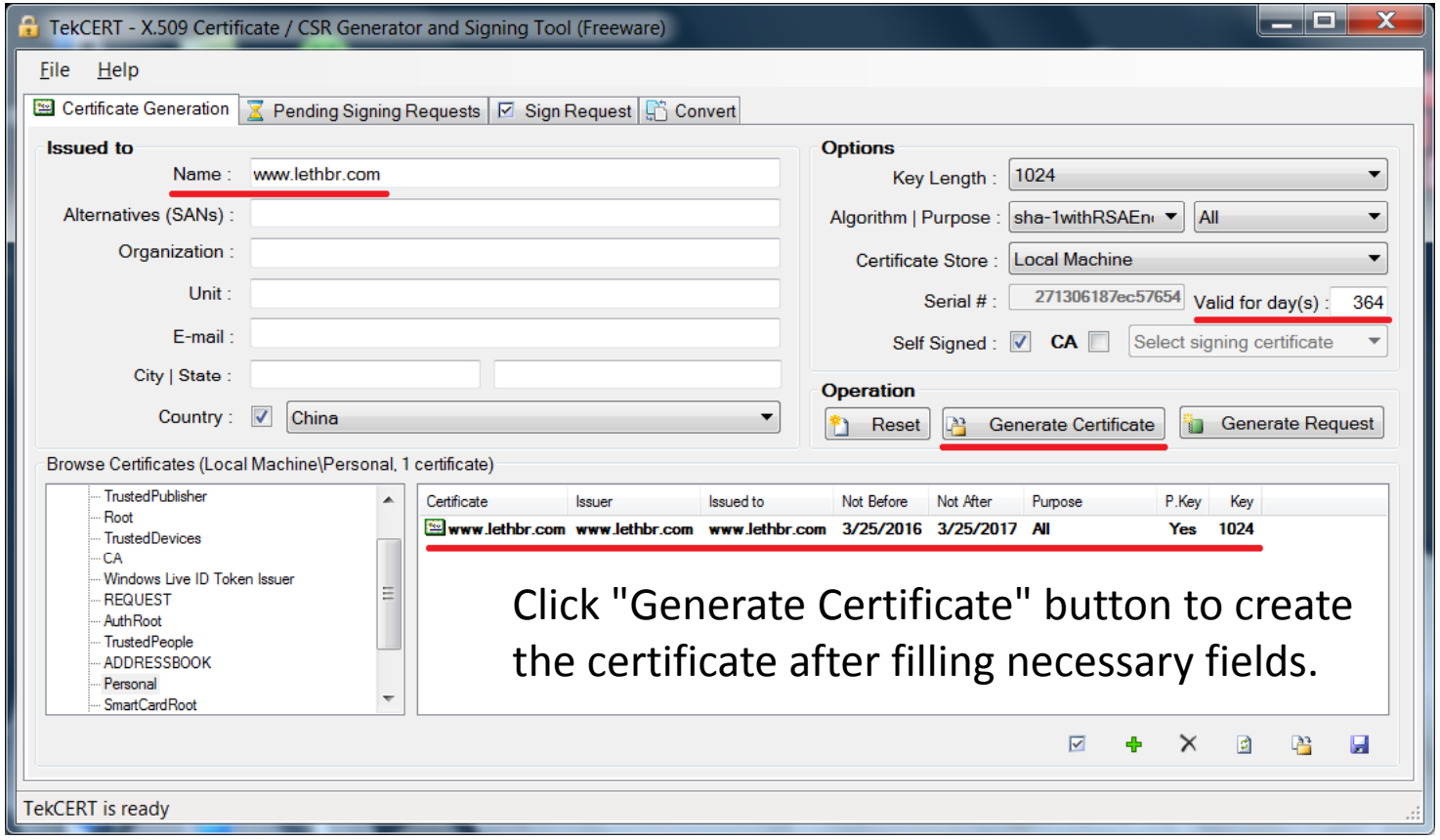



Timeout – defines how much milliseconds can elapse while the answer arrives from the RADIUS server.
If you are using slower connection to RADIUS server, set this timeout higher (3000-5000 ms).

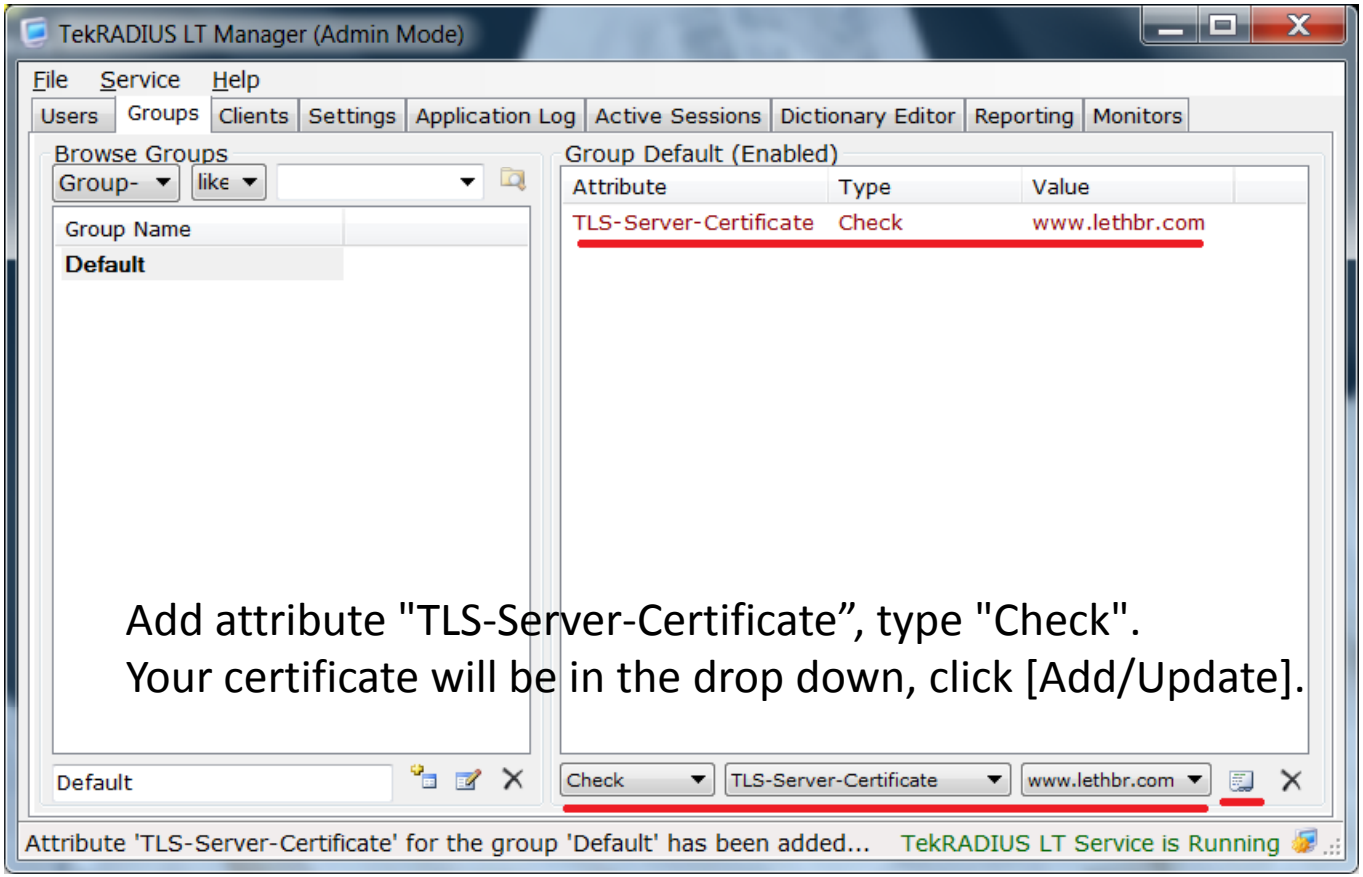
# To create a RADIUS client



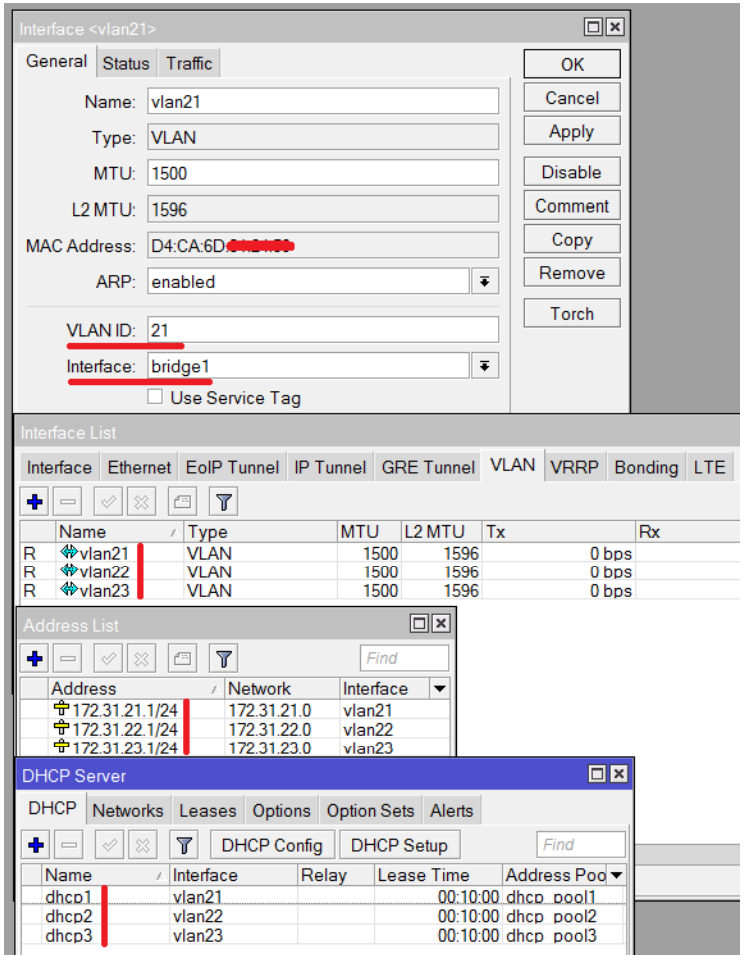
# Create Self Signed Server Certificate



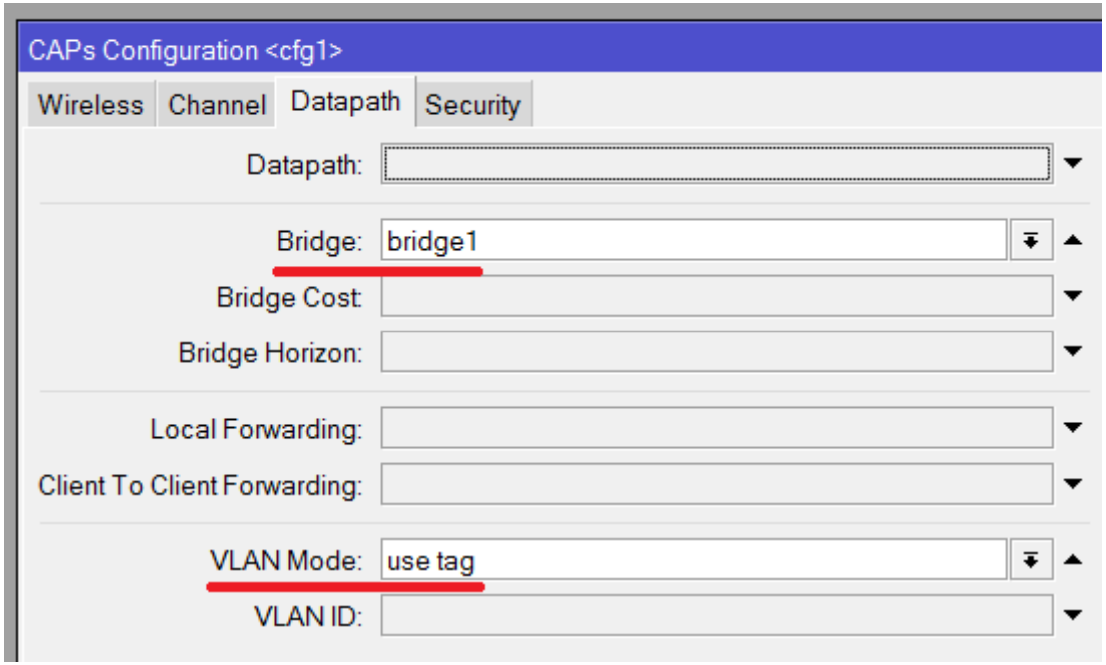
# Import newly created certificate to RADIUS



# VLAN Interfaces



# Datapath




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).

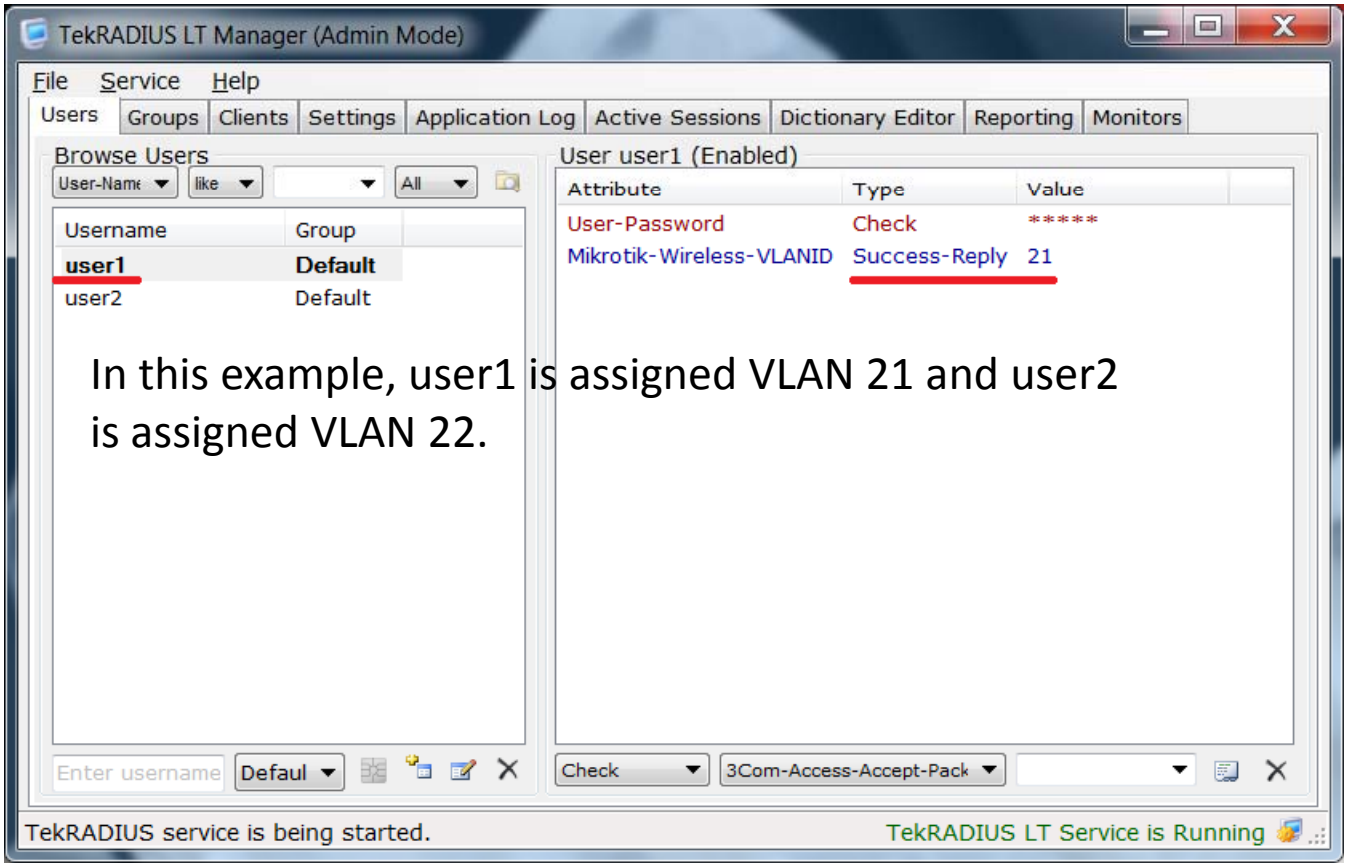
# RADIUS attributes

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

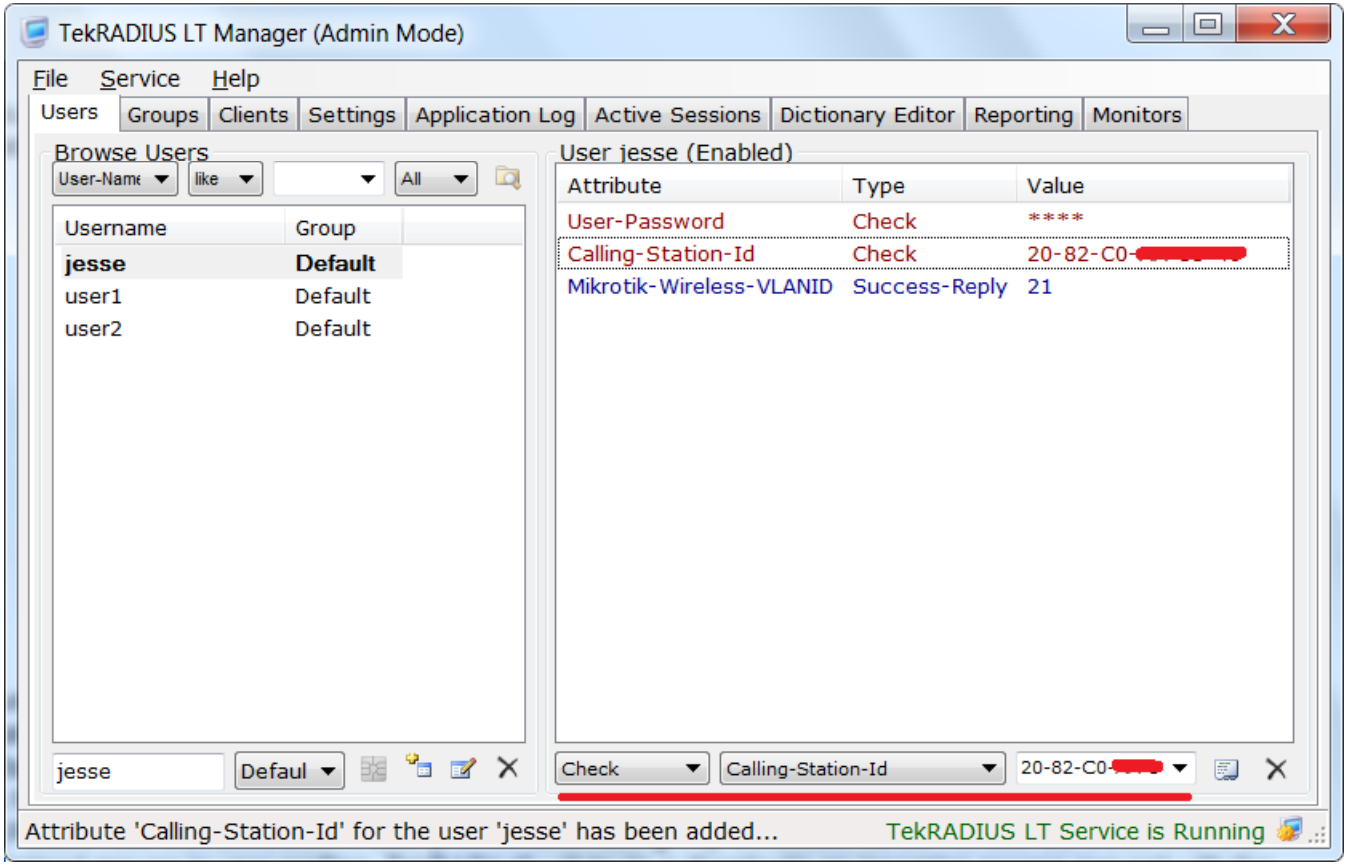
```
ATTRIBUTE       Mikrotik-Wireless-PSK           16  string
ATTRIBUTE       Mikrotik-Total-Limit            17  integer
ATTRIBUTE       Mikrotik-Total-Limit-Gigawords  18  integer
ATTRIBUTE       Mikrotik-Address-List           19  string
ATTRIBUTE       Mikrotik-Wireless-MPKey         20  string
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       Mikortik_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

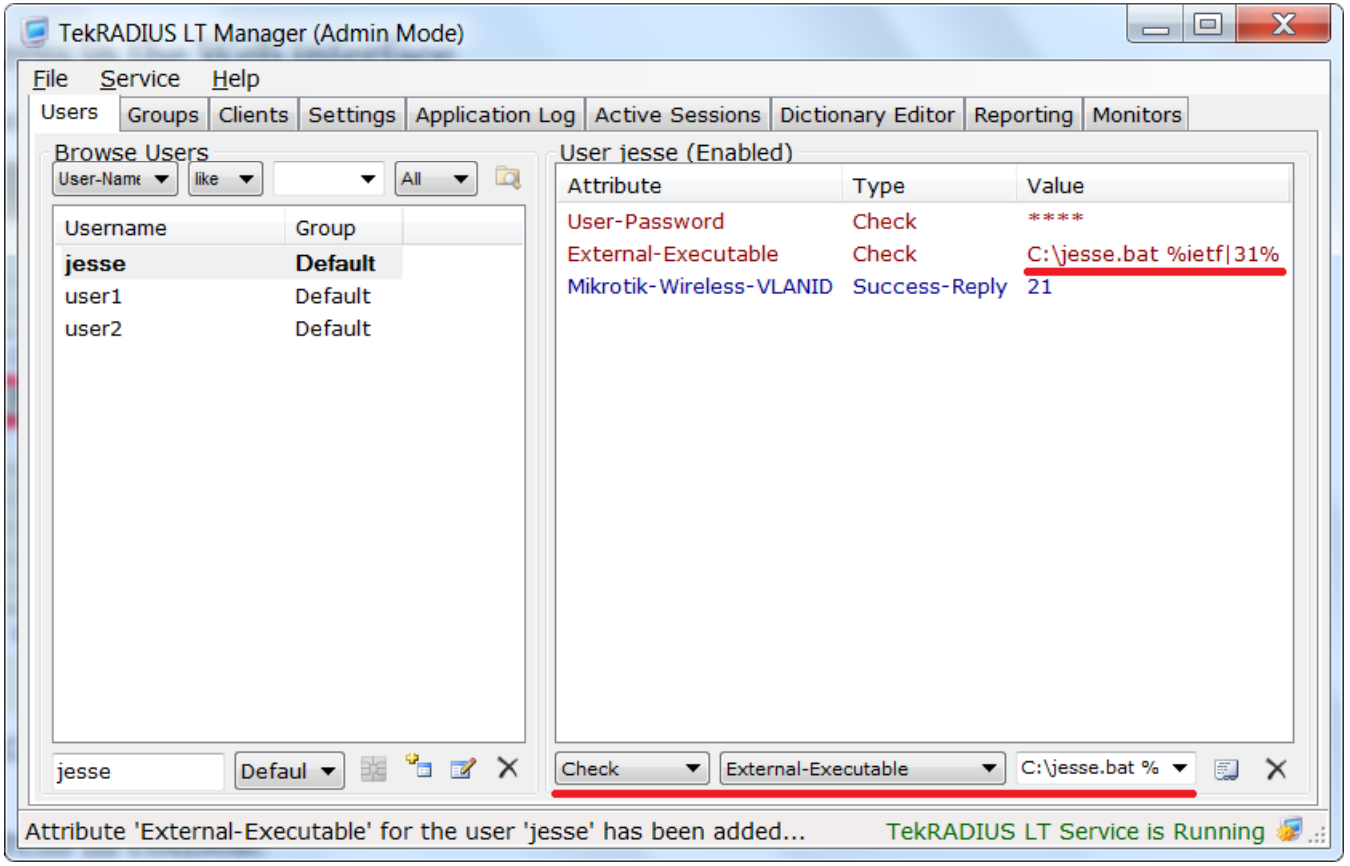
- For each user, add RADIUS attributes which specify the VLAN information to be sent to the CAPsMAN.



# MAC address binding



# Bind multiple MAC addresses to one user



# Bind multiple MAC addresses to one user

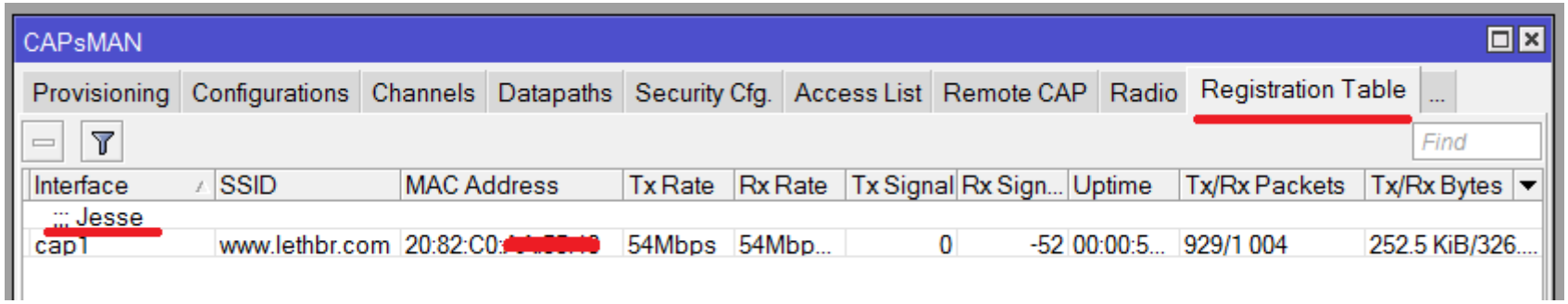
jesse.bat

```
1  @echo off
2
3  IF "%1%" == "20-82-C0-[redacted]" Goto Success
4  IF "%1%" == "B4-CE-F6-[redacted]" Goto Success
5  IF "%1%" == "84-3A-4B-[redacted]" Goto Success
6
7  echo Fail
8  exit /b 1
9
10 :Success
11
12 echo Success
13 exit /b 0
```

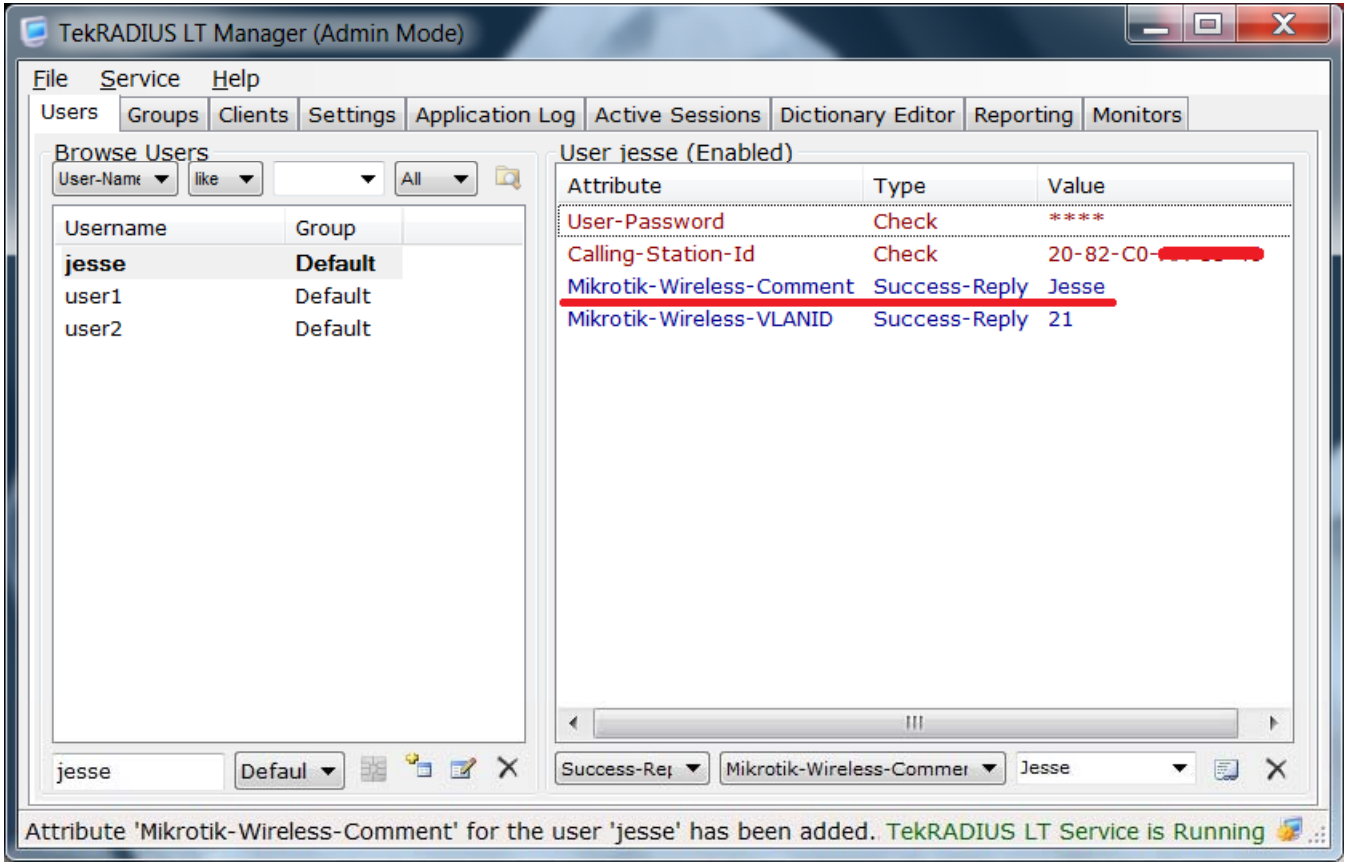
- Phone
- Tablet
- Laptop

# Registration Table

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



# Mikrotik-Wireless-Comment



# 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