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

Internet

CAPsMAN

CAP

RADIUS Server

Internal Network

user1 / VLAN 21

user2 / VLAN 22
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

Click "Generate Certificate" button to create the certificate after filling necessary fields.
Import newly created certificate to RADIUS

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

<table>
<thead>
<tr>
<th>ATTRIBUTE</th>
<th>Value</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mikrotik-Wireless-PSK</td>
<td>16</td>
<td>string</td>
</tr>
<tr>
<td>Mikrotik-Total-Limit</td>
<td>17</td>
<td>integer</td>
</tr>
<tr>
<td>Mikrotik Total Limit Gigawords</td>
<td>10</td>
<td>intgr</td>
</tr>
<tr>
<td>Mikrotik-Address-List</td>
<td>19</td>
<td>string</td>
</tr>
<tr>
<td>Mikrotik-Wireless-MPKey</td>
<td>20</td>
<td>string</td>
</tr>
<tr>
<td>Mikrotik-Wireless-Comment</td>
<td>21</td>
<td>string</td>
</tr>
<tr>
<td>Mikrotik Delegated IPv6 Pool</td>
<td>22</td>
<td>string</td>
</tr>
<tr>
<td>Mikrotik_DHCP_Option_Set</td>
<td>23</td>
<td>string</td>
</tr>
<tr>
<td>Mikrotik_DHCP_Option_Param_STR1</td>
<td>24</td>
<td>string</td>
</tr>
<tr>
<td>Mikrotik_DHCP_Option_Param_STR2</td>
<td>25</td>
<td>string</td>
</tr>
<tr>
<td>Mikrotik Wireless_VLANID</td>
<td>26</td>
<td>integer</td>
</tr>
<tr>
<td>Mikrotik_Wireless_VLANIDtype</td>
<td>27</td>
<td>integer</td>
</tr>
<tr>
<td>Mikrotik_Wireless_Minsignal</td>
<td>28</td>
<td>string</td>
</tr>
<tr>
<td>Mikrotik_Wireless_Maxsignal</td>
<td>29</td>
<td>string</td>
</tr>
</tbody>
</table>
Specifies the VLAN ID

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

In this example, user1 is assigned VLAN 21 and user2 is assigned VLAN 22.
MAC address binding
Bind multiple MAC addresses to one user
Bind multiple MAC addresses to one user

```bat
@echo off
IF "%1" == "20-82-C0-2A-51-20" Goto Success
IF "%1" == "B4-CE-F6-C5-2B-88" Goto Success
IF "%1" == "84-3A-4B-C9-C1-72" Goto Success

echo Fail
exit /b 1

:Success

echo Success
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