Build enterprise wireless with CAPsMAN

Mikrotik User Meeting Melbourne, May 18, 2018

Achmad Mardiansyah
achmad@glcnetworks.com
GLC Networks, Indonesia

www.glcnetworks.com
Agenda

- Introduction
- Enterprise wireless
- How CAPsMAN works
- CAPsMAN features
- CAPsMAN tips
- Suggestion for Mikrotik
- Q & A
What is GLC?

- Garda Lintas Cakrawala (www.glcnetworks.com)
- Based in Bandung, Indonesia
- Areas: Training, IT Consulting
- Certified partner for: Mikrotik, Ubiquity, Linux foundation
- Product: GLC radius manager
- Regular event: webinar (every 2 weeks, see our schedule on website)
About me

- Name: Achmad Mardiansyah
- Base: Bandung, Indonesia
- Linux user since 1999, mikrotik user since 2007,
- Mikrotik Certified Trainer (MTCNA/RE/WE/UME/INE/TCE/IPv6)
- Mikrotik Certified Consultant
- Teacher at Telkom University (Bandung, Indonesia)
- Website contributor: achmadjournal.com, mikrotik.tips, asysadmin.tips
- More info: http://au.linkedin.com/in/achmadmardiansyah
Past experiences

- 2018, Malaysia: integrated monitoring system and bandwidth management for a broadband ISP
- 2017, Libya (north africa): remote wireless migration for a new Wireless ISP
- 2016, United Kingdom: facilitates workshop for a wireless ISP, migrating a bridged to routed network
- 2015, West Borneo: supporting wireless infrastructure project
- 2014, Senegal (west africa): TAC2 engineer for HLR migration from NOKIA to ERICSSON
- 2013, Malaysia: build a wireless network to support an international event
About Telkom University

- Located in Bandung, Indonesia
- 7 Faculties, 27 schools
- Areas: Engineering, Communications, Computing, Business and management, Arts
- 650+ Academic staff, 400+ Administration staff, 20000+ students
- An exchange program
- Runs mikrotik academy program

www.glcnetworks.com
Mikrotik academy @ TEL-U

- Started in 2013
- Embedded into schools curriculum
- 100% hands-on
- Get MTCNA certification

www.glcnetworks.com
Mikrotik in Indonesia

- Very popular product for networking
- Early adopters (beginning of 2000)
- Many schools already join Mikrotik Academy program
- Lots of training classes
- Biggest MUM in the world (3000+ participants, 2-day event)
- Very active community (facebook, telegram, forum, etc)
- What..? you don't know Mikrotik? Where have you been?
Enterprise wireless
Characteristics of enterprise wireless

- Usually indoor, on access network (directly connected to end-user)
- PTMP (point to multi point)
- **Centralised** FCAPS (Fault, Configuration, Authentication, Performance, Security)
- **Enterprise features**: load balancing, better mobility (seamless roaming), security, high availability, authentication, band steering, security
- Example: office, campus, hotel
How CAPsMAN works
About CAPsMAN

- Offers enterprise features: centralised platform to manage AP
- Software based, free to use
- Available since 6.11, CAPsMAN v1 (March 2014)
- Now its CAPsMAN v2 (since 6.22, Nov 2014). Recommended version, not compatible to v1
- CAP: controlled AP
- CAPsMAN: CAP manager (AP controller)
CAPsMAN - CAP connectivity

**Layer 2**
- CAP and CAPsMAN are in the same network

**Layer 3 (recomm.)**
- CAP and CAPsMAN are in different network
CAPsMAN configuration concepts
Channels | datapath | security cfg | rates

### Channels

<table>
<thead>
<tr>
<th>CAP Interface</th>
<th>Provisioning</th>
<th>Configurations</th>
<th>Channels</th>
<th>Datapaths</th>
<th>Security Cfg</th>
</tr>
</thead>
<tbody>
<tr>
<td>f-2412</td>
<td>2412</td>
<td>20MHz</td>
<td>2ghz-g/n</td>
<td>disabled</td>
<td>17</td>
</tr>
<tr>
<td>f-2437</td>
<td>2437</td>
<td>20MHz</td>
<td>2ghz-g/n</td>
<td>disabled</td>
<td>17</td>
</tr>
<tr>
<td>f-2462</td>
<td>2462</td>
<td>20MHz</td>
<td>2ghz-g/n</td>
<td>disabled</td>
<td>17</td>
</tr>
<tr>
<td>f-5745</td>
<td>5745</td>
<td>20MHz</td>
<td>2ghz-g/n</td>
<td>disabled</td>
<td>17</td>
</tr>
</tbody>
</table>

### Datapaths

<table>
<thead>
<tr>
<th>CAP Interface</th>
<th>Provisioning</th>
<th>Configurations</th>
<th>Channels</th>
<th>Datapaths</th>
<th>Security Cfg.</th>
<th>Access List</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>dp-if</td>
<td>yes</td>
<td>no</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>;;; vlan 22</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>dp-if-vlan22</td>
<td>yes</td>
<td>no</td>
<td></td>
<td></td>
<td>use service tag</td>
<td>22</td>
<td></td>
</tr>
</tbody>
</table>

### Security Cfg.

<table>
<thead>
<tr>
<th>CAP Interface</th>
<th>Provisioning</th>
<th>Configurations</th>
<th>Channels</th>
<th>Datapaths</th>
<th>Security Cfg.</th>
<th>Access List</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>wpa-psk-ddsatuvisi</td>
<td>WPA PSK WPA2 ...</td>
<td>aes ccm</td>
<td>aes ccm</td>
<td>*****</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>wpa-psk-old</td>
<td>WPA PSK WPA2 ...</td>
<td>aes ccm</td>
<td>aes ccm</td>
<td>*****</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Rates

<table>
<thead>
<tr>
<th>CAP Interface</th>
<th>Provisioning</th>
<th>Configurations</th>
<th>Channels</th>
<th>Datapaths</th>
<th>Security Cfg.</th>
<th>Access List</th>
<th>Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td>rate-default</td>
<td>9Mbps 12Mbps 18Mbp...</td>
<td>3 4 5 6 7 11 12 13 14... none</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
configuration

www.glcnetworks.com
Provisioning rule

Radio MAC: 00:00:00:00:00:00
Hw. Supported Modes: g
           gn
Identity Regexp: GP-AP-1.3
Common Name Regexp: 10.10.24.2-10.10.31.254
Action: create enabled
Master Configuration: master1-2ghz
Slave Configuration: DDF
Name Format: identity
Name Prefix: enabled
IP Address Ranges: 10.10.24.2-10.10.31.254
ID Identity Regexp: GP-AP-1.3
Action: create enabled
Master Configuration: master1-5ghz
Slave Configuration: DDF
Name Format: identity
Name Prefix: enabled
Master vs slave configuration

**Master**
- Will be used to set basic wireless parameters: Frequency, channel-width, TX power

**Slave**
- Basic wireless parameter will be ignored
- Is used to setup additional SSID (Virtual AP)
CAP interface

**Master Interface**
- Name: GP-AP-1.1-1
- Last Link Down Time: May/17/2018 20:21:02
- Last Link Up Time: May/17/2018 16:00:51
- Link Downs: 5
- Current State: running-ap
- Current Channel: 2412/20 (gn(17dBm))
- Current Rate Set: OFDM:9-54 BW:1x SGI:1x HT:3-7,11-15
- Current Registered Clients: 0
- Current Authorized Clients: 0

**Slave Interface**
- Name: GP-AP-1.1-1-2
- Name: GP-AP-1.1-1-2
Access list

- Is used to control wifi access
- Format:
  - Client matching
  - Action:
    - accept | reject | query radius
  - Connection parameter
CAPsMAN features
Load balancing AP

before

CAPs MAN
POE switch
CAP
15 user
CAP
1 user
CAP
1 user

after

CAPs MAN
POE switch
CAP
6 user
CAP
6 user
CAP
5 user
Roaming

- Unlike GSM, connection to AP is end-user decision, not AP.
- Often, station is **still attached to old AP** even though already moved to new AP.
- What AP can set up a threshold for disassociation (based on signal level).
- On CAPsMAN, we use **access rule**.

![CAPs Access Rule](image)

1. **MAC Address**: [Enter MAC Address]
2. **MAC Mask**: [Enter MAC Mask]
3. **Interface**: [all]
4. **SSID Regexp**: [Enter SSID Regexp]
5. **Signal Range**: 
   - [Enter Signal Range (example: -80..-10 for accept)]
   - [Enter Signal Range (example: -120..-81 for reject)]
6. **Allow Signal Out Of Range**: [00:00:10]
7. **Time**
8. **Action**: [accept]
Datapath (local forwarding)

via bridge

Requires powerful capsman box

Local forwarding = yes

POE switch

ISP

6 user

5 user

6 user

6 user

5 user

Requires powerful capsman box
Datapath (vlan)

no vlan

vlan=22
Datapath (vlan per user)

User1, vlan=11

User2, vlan=22

Need support from radius server which provides vendor attribute
Security: EAP (layer 2 authentication)

- Username and password will be asked on layer 2
- Need support from radius server
MAC based authentication

- It is possible to allow client to connect based on MAC address
- We need support from radius server which contains MAC address database
- Combined with access-list
CAPsMAN tips
CAP: use auto certificate

- Use certificate for **stable** CAP - CAPsMAN connection
- Use “Lock to CAPsMAN” to bind CAP to a particular CAPsMAN
CAP: high availability

- If no connection between CAP and CAPsMAN, station will be disconnected
- Use more than 1 CAPsMAN for high availability
CAPsMAN: upgrade CAP version

- It is recommended to use latest version of RouterOS
- CAPsMAN can upgrade CAP
- CAPs do not need to connect to internet directly
Wireless survey

- Wireless survey is very useful for troubleshooting and verify your wireless setting
Enable client isolation and port isolation

● To gain more airtime, better if we disable client-to-client communication:
  ○ Do not activate “client-to-client forwarding”
  ○ Apply port isolation. Check your switch documentation
  ○ Do not put server on wireless network. Example: wireless printer
Smooth mobility for client

- Maintain layer 3 address. Changing on layer 3 address (ex. renew dhcp-client ip address) will make disconnection time longer.
- Can use flat layer 3 network for whole wireless. Check layer 2 vendor to minimise broadcast traffic
- Can use vlan id per user
Flexible provisioning

- Setup pattern on CAP identity
- Use regex facility on CAPsMAN provisioning
Suggestions for mikrotik
Automatic band steering

- We are encourage users to connect to 5GHz band
- Currently its done manually. Example:
  - 2GHz, SSID = wifi
  - 5GHz, SSID = wifi_faster
- In the future, this process needs to be automatic
Signal visualisation on floor layout

- Similar to wifi survey
- Useful to check wireless settings
- Thedude integration?
Detecting rogue access point

- After all AP are integrated in capsman,
- CAPsMAN can detect a rogue AP in wireless network
- Thedude integration?
EAP support on usermanager

- Currently EAP support is not available on Mikrotik Usermanager
- We use other radius software for EAP authentication
- Perhaps in the future?
Training topics

- Previously, mikrotik wireless product was focusing on outdoor environment, Point-To-Point / Point-To-Multi-Point
- Since CAPsMAN appears, mikrotik is focusing on indoor wireless
- Suggestion for the training track:
  - Mikrotik certified outdoor wireless engineer, focusing on outdoor wireless application
  - Mikrotik certified enterprise wireless engineer, focusing on indoor implementation with CAPsMAN
Interested? Just come to our training...

- **Check schedule on our website**
- More hands-on
- Not only learn the materials, but also sharing experiences, best-practices, and networking
QA
End of slides