CAPsMAN Case Study

Uldis Cerneveksis
MikroTik, Latvia

MUM Brazil
November 2014
CAPsMAN Features

- Centralized management of RouterOS APs
- Dual Band AP support
- Provisioning of APs
- MAC and IP Layer communication with APs
- Certificate support for AP communication
- Full and Local data forwarding mode
- RADIUS MAC authentication
- Custom configuration support
Requirements

- **CAPsMAN**
  - x86 or RouterBOARD based device
  - Newest RouterOS v6 version
  - Wireless-fp package installed and enabled

- **CAP**
  - X86 or RouterBOARD based device
  - Newest RouterOS v6 version
  - Atheros chipset (a/b/g/n/ac) wireless card
  - Wireless-fp package installed and enabled
  - At least Level4 RouterOS license
CAPsMAN Simple Setup
CAPsMAN Simple Setup

- Enable CAPsMAN service
- Create Bridge interface
- Add IP configuration to Bridge interface
- Create CAPsMAN Configuration
- Create Provisioning rule
- Enable CAP mode on the APs
CAPsMAN Simple Setup

- Enable the CAPsMAN service
CAPsMAN Simple Setup

- Create Bridge Interface
CAPsMAN Simple Setup

1. Add IP address
2. Add DHCP Server
3. Add NAT rule
CAPsMAN Simple Setup

- Add New CAPsMAN Configuration
CAPsMAN Simple Setup

- Add new Provisioning rule
CAPsMAN Simple Setup

- Configure the AP to use CAP mode
  - Enable wireless-fp package
  - Enable CAP mode
    - By CAP mode button on some boards
    - By configuration in Wireless CAP menu
CAPsMAN Simple Setup

- Check the Status of the CAPsMAN CAP interface
## CAPsMAN Registration Table

<table>
<thead>
<tr>
<th>Interface</th>
<th>MAC Address</th>
<th>Tx Rate</th>
<th>Rx Rate</th>
<th>Tx Signal</th>
<th>Rx Signal</th>
<th>Uptime</th>
<th>Tx/Rx Packets</th>
<th>Tx/Rx Bytes</th>
</tr>
</thead>
<tbody>
<tr>
<td>OfficeAP3</td>
<td>18:34:51:41:75:CD</td>
<td>65Mbps-20MHz/1S</td>
<td>65Mbps-20MHz/1S</td>
<td>0</td>
<td>-44</td>
<td>00:03:17.70</td>
<td>31395/33212</td>
<td>29.8 MiB/29.5 MiB</td>
</tr>
</tbody>
</table>
Manual Provisioning

- Changing Provisioning rules doesn't effect already configured CAPs, manual Provisioning required:
  - Remove CAP interface
  - Initiate Provision command on the CAP
CAP to CAPsMAN Connection

• MAC Layer2:
  – No IP configuration required
  – CAP and CAPsMAN must be in the same Layer 2 network

• IP (UDP) Layer3:
  – CAP must reach the CAPsMAN using IP protocol
  – Can traverse NAT if necessary

• Management connection between CAP and CAPsMAN is secured using DTLS

• CAP client data traffic is not secured – if necessary additional encryption by using IPSec or encrypted tunnels is needed
CAPsMAN Selection on CAP

- CAP attempts to contact CAPsMAN and build available CAPsMAN list:
  - List of CAPsMAN IPs
  - List of CAPsMAN IPs obtained from DHCP
  - Broadcasting on configured interfaces using IP and MAC Layer

- CAP selects the CAPsMAN based on such rules:
  - If CAPsMAN names setting is matched it will prefer that CAPsMAN earlier in the list
  - MAC layer connectivity to CAPsMAN is preferred over IP connectivity
  - If list is empty it will connect to any available CAPsMAN
CAPsMAN with Layer3

- On the CAP specify the IP address of the CAPsMAN

![CAPsMAN Layer3 Configuration](image)
CAPsMAN selection using Name

- On the CAP specify the CAPsMAN identity name
CAP Identification

- MAC/IP address
- RouterBoard model
- Serial Number of the Board
- RouterOS version
- System Identity
- Main wireless MAC
- State of the CAP
- Provided radio count
CAPsMAN static CAP interface

- No interface name change or setting change after the reboot
- Additional manual setting override
- Copy dynamic interface to make static interface
CAPsMAN VirtualAP Configuration

• Create new Bridge interface and IP configuration for the VirtualAPs or use the same bridge interface as Master AP
• Create a new configuration for the VirtualAP
• Specify the new configuration in Provisioning rule as Slave Configuration
• Remove all CAP interfaces
• Initiate Manual Provisioning on all the CAPs
CAPsMAN VirtualAP Setup

Image of CAPsMAN configuration interface with highlighted sections for "Wireless" and "Datapath" settings.
CAPsMAN VirtualAP Setup
CAPsMAN static VirtualAP
CAPsMAN Access List Features

- MAC Authentication
- Radius Query support
- MAC Mask support
- Signal Range
- Time
- Private Passphrase
- VLAN ID assignment
CAPsMAN Access List

- Allow Apple devices to connect
- Rest of the connections pass to the RADIUS
CAPsMAN Local Forwarding Setup
CAPsMAN Local Forwarding

- Create a Local Forwarding configuration
CAPsMAN Local Forwarding

- Create Provisioning rule
- Move above the default Provisioning rule
CAPsMAN Local Forwarding

- On CAP specify the Bridge interface for CAP or use routing for access to network
CAPsMAN VLAN Assignment
CAPsMAN VLAN Assignment

- When using Local Forwarding CAPsMAN can assign VLAN ID to specific CAP interface or even specific wireless client.
- Create Slave interface with Vlan tag.
CAPsMAN VLAN Assignment

- Create Access List rule for specific client to get tagged to Management Vlan on the same CAP interface
- Move the Access List rule above the previous ones
CAPsMAN VLAN Assignment

• Create VLAN interfaces on the CAPsMAN router interface where the CAPs are connected
CAPsMAN VLAN Assignment

- Assign IPs to VLAN interfaces on CAPsMAN
CAPsMAN Dual Band CAP

- If the Channel settings are not specified it will automatically use the supported band/channel
- If specific Channel settings are required then specific Provisioning rules are required
  - Custom Channel settings
  - Dual band wireless interface support
CAPsMAN Dual Band CAP

- Create 3 configurations:
  - Config for both bands radio
  - Config for 5ghz only radio
  - Config for 2.4ghz only radio
CAPsMAN Dual Band CAP

- Create 3 Provisioning rules
  - For A/N,G/N hardware use Both Bands config
  - For A/N hardware use 5ghz config
  - For G/N hardware use 2.4ghz config
CAPsMAN Dual Band CAP

--- managed by CAPsMAN
--- channel: 5220/20-Ce/an(17dBm), SSID: 5ghz band, CAPsMAN forwarding
X wlan1 Wireless (Atheros AR9... 1600 0 bps 0 bps

--- managed by CAPsMAN
--- channel: 2427/20-Ce/an(30dBm), SSID: 2.4ghz band, CAPsMAN forwarding
X wlan2 Wireless (Atheros AR9... 1600 0 bps 0 bps
CAPsMAN Configuration override

- Configuration overrides Channel setting
- Interface overrides Channel and Configuration setting
CAPsMAN Auto Certificate

- Enable Certificate and CA Certificate on CAPsMAN
CAPsMAN Auto Certificate

- Enable request Certificate on CAP
CAPsMAN Auto Certificate

- Allow CAPsMAN to accept connections only from CAPs with valid certificate
CAP Lock To CAPsMAN

- Enable Lock To CAPsMAN on CAP – certificate is required
CAPsMAN and CAP in one board

- Enable CAPsMAN Manager and create the configuration
- Configure the CAP to look for IP 127.0.0.1
CAPsMAN Antenna-gain

- Antenna-gain value is taken from the CAP interface.
- Must be configured on AP before enable radio in CAP mode.
- Example with 6db antenna-gain and 30db EIRP.
CAPsMAN v2 features

- CAPsMAN automatic upgrade of all CAP clients (configurable)
- Improved CAP<->CAPsMAN data connection protocol
- Added "Name Format" and "Name Prefix" setting for Provision rules
- Improved logging entries when client roams between the CAPs
- Added L2 Path MTU discovery
CAPsMAN v2 compatibility

- CAPsMAN v2 is NOT compatible with current CAPsMAN v1 (CAPsMAN v1 CAP devices will not be able to connect to CAPsMAN v2 and CAPsMAN v2 CAP devices will not be able to connect to CAPsMAN v1).
- Both CAPsMAN and CAP devices should have wireless-cm2 package installed in order to make CAPsMAN v2 system to work.
Upgrade to CAPsMAN v2

- Option1: Install a new temporary CAPsMAN v2 router in the same network where the current CAPsMAN router is and start upgrading CAPs with wireless-cm2 package. All CAPs with the v2 will connect to the new temporary CAPsMAN v2 router. After every CAP is upgraded to v2, upgrade your current CAPsMAN to v2 and then turn off the temporary CAPsMAN v2 router.

- Option2: Upgrade your CAPs and then CAPsMAN to v2 at the same time. In this case you could have little more downtime unless you schedule all the CAPs to reboot/install at the same time.