Centralised Wireless Network Management Using Mikrotik CAPsMAN

by Chan Ty
Innovative Technology Training Centre (ITTC)
www.ittc.edu.kh

About ITTC

- Mikrotik Training Centre
  - MTCNA
  - MTCRE
  - MTCTCE
  - MTCINE
  - MTCWE
  - MTCUME

About Me

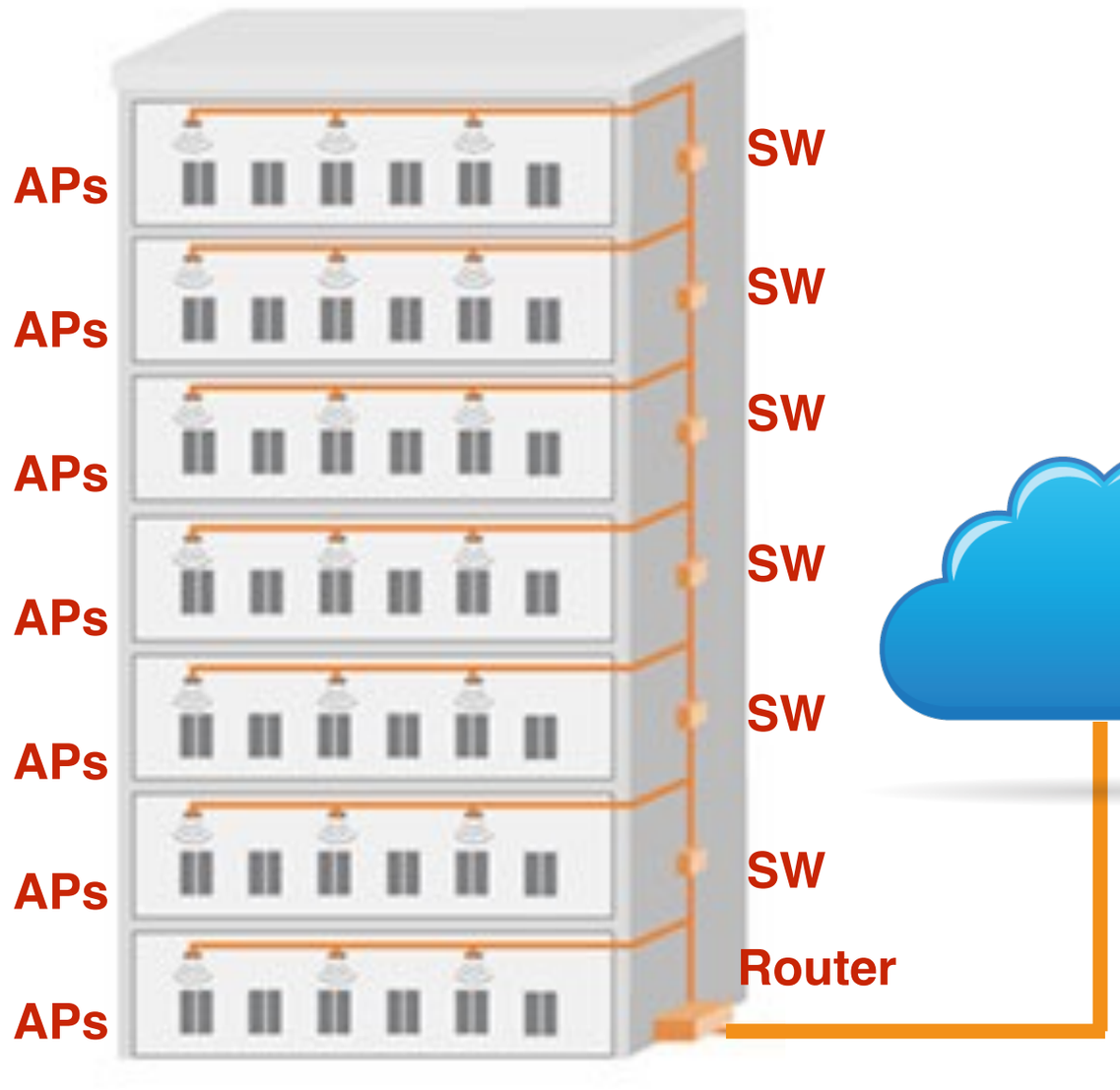
- Chan Ty
- Mikrotik Certified Trainer
  - MTCNA, MTCRE, MTCTCE, MTCINE
- Working at MekongNet as NOC Manager and Director at ITTC
- Mostly focusing on Routing, Switching and QoS

Challenge

- Traditionally, administering wireless Access Point is done individually one by one

- Administrator has to make sure that the configurations are the same for all APs like SSID, Security, Access List, Policy, etc.

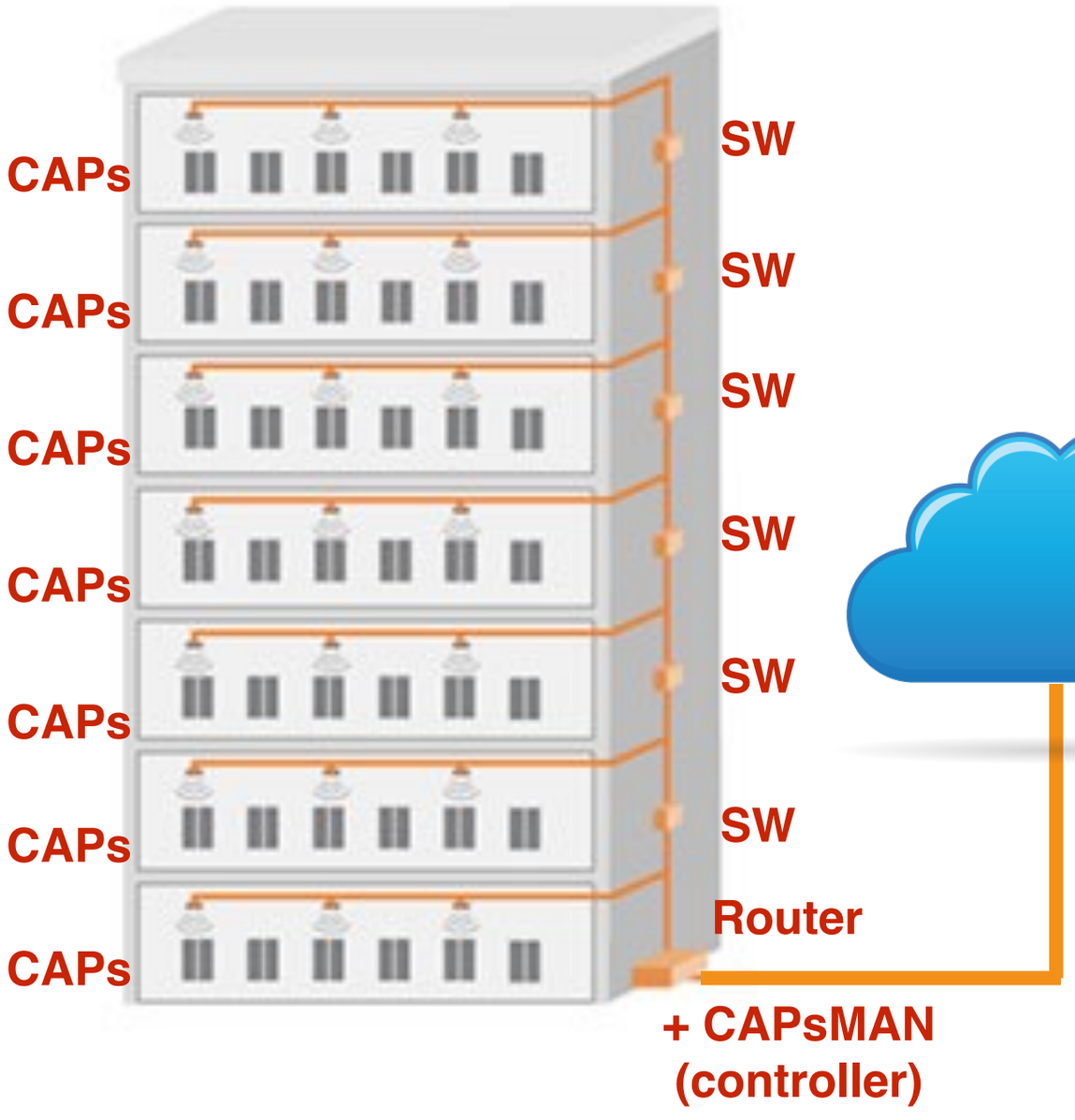
- That needs more time and affords if we have want o changes something for the whole WLAN



Solution

- Since RouterOS v6.11, Mikrotik introduced a feature called Controlled Access Point system MANager (**CAPsMAN**)

- CAPsMan allows centralisation of wireless network management (SSID, Access List, Security,……) and/or data processing (Firewall, QoS, Routing,…)



CAPsMAN Features

- Centralised management of RouterOS Access Point
- 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

- **CAPsMAN v2** (since v6.22rc7)
  - CAPsMAN automatic upgrade of all CAP client (configurable)
  - Improved CAP<>CAPsMAN data connection protocol
  - Add “Name Format” and “Name Prefix” setting for provisioning rules
  - Improve logging entries when client roams between the CAPs
  - Add L2 Path MTU discovery
- CAPsMAN v1 and CAPsMAN v2 is **NOT** compatible

Requirements

- **CAPsMAN**
  - x86 or RouterBoard based device
  - Newest RouterOS version
  - **Wireless-fp** installed and enabled
- **CAP**
  - x86 or RouterBoard based device
  - Newest RouterOS version
  - Atheros chipset (a/b/g/n/ac) wireless card
  - **Wireless-fp** installed and enabled
  - At least Level 4 RouterOS license

CAP to CAPsMAN Connection

- **MAC Layer 2**
  - No IP Configuration Required
  - CAP and CAPsMAN must be in the same Layer 2 Network
- **IP (UDP) Layer 3**
  - CAP must reach the CAPsMAN using IP Protocol
  - CAP can passthrough NAT

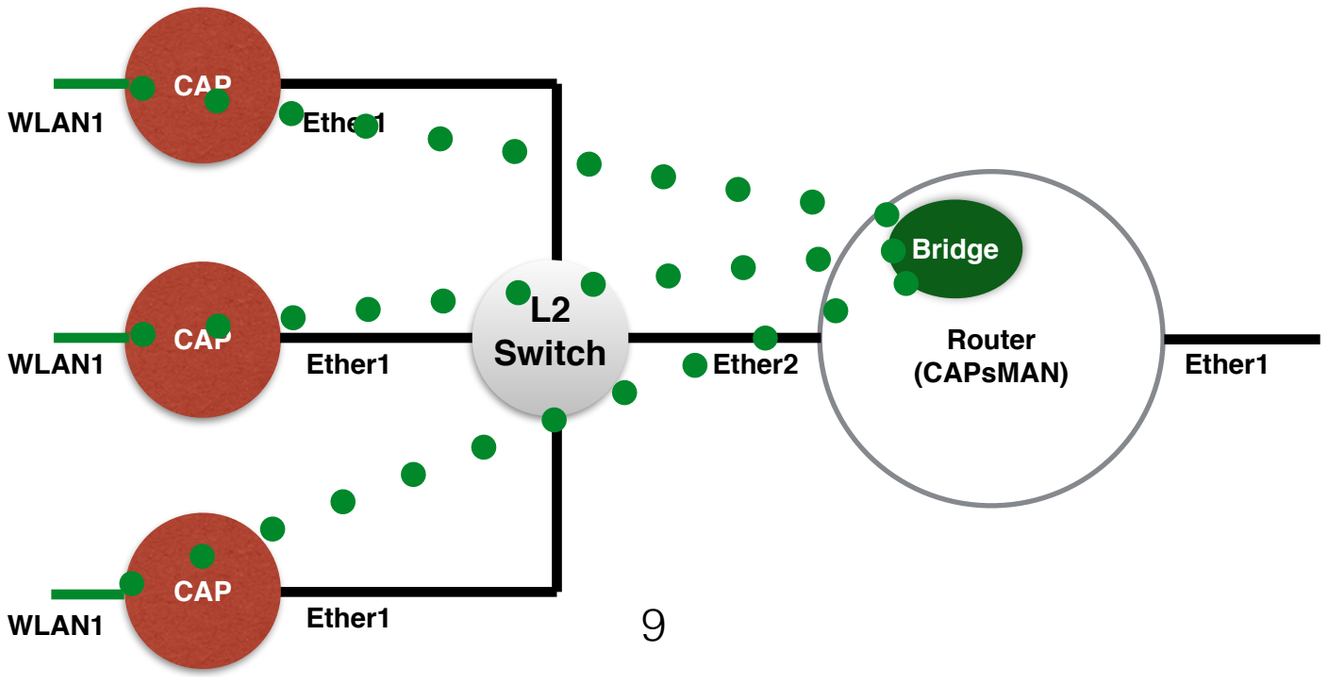
Simple Setup

- **CAPsMAN**

  1. Enable CAPsMAN service
  2. Create and add IP configuration to Bridge interface
  3. Create CAPsMAN Configuration
  4. Create Provisioning rule

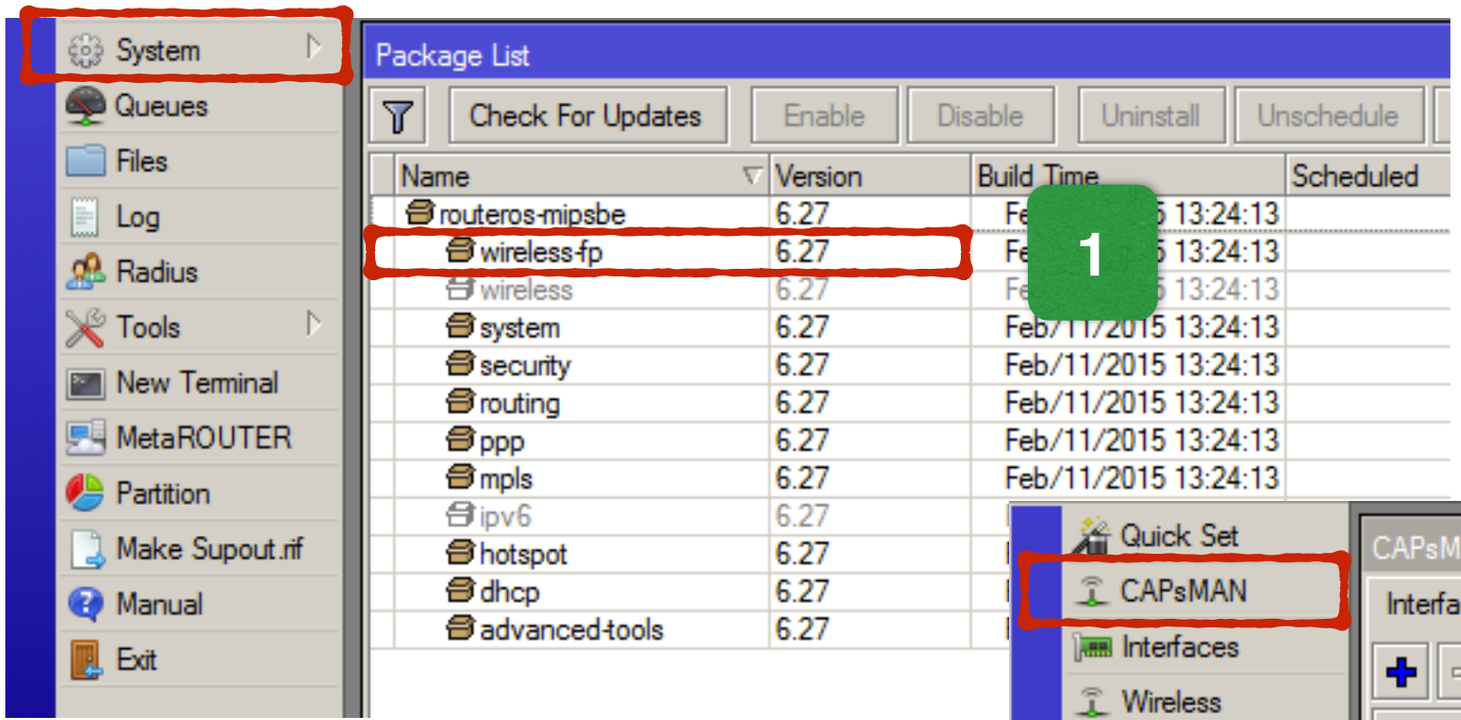
- **CAP**

  5. Enable CAP mode on APs



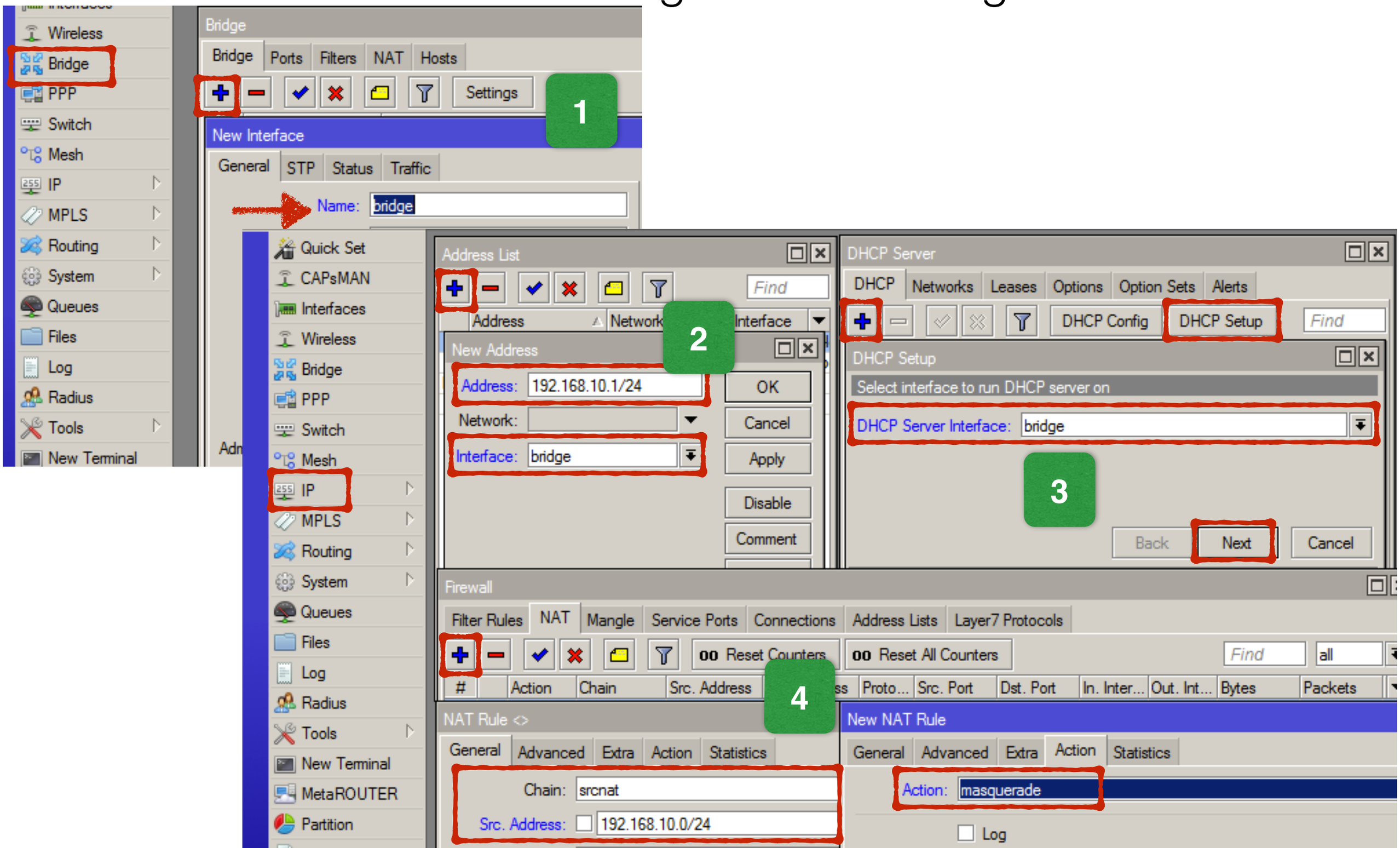
Simple Setup

1. Enable CAPsMAN service



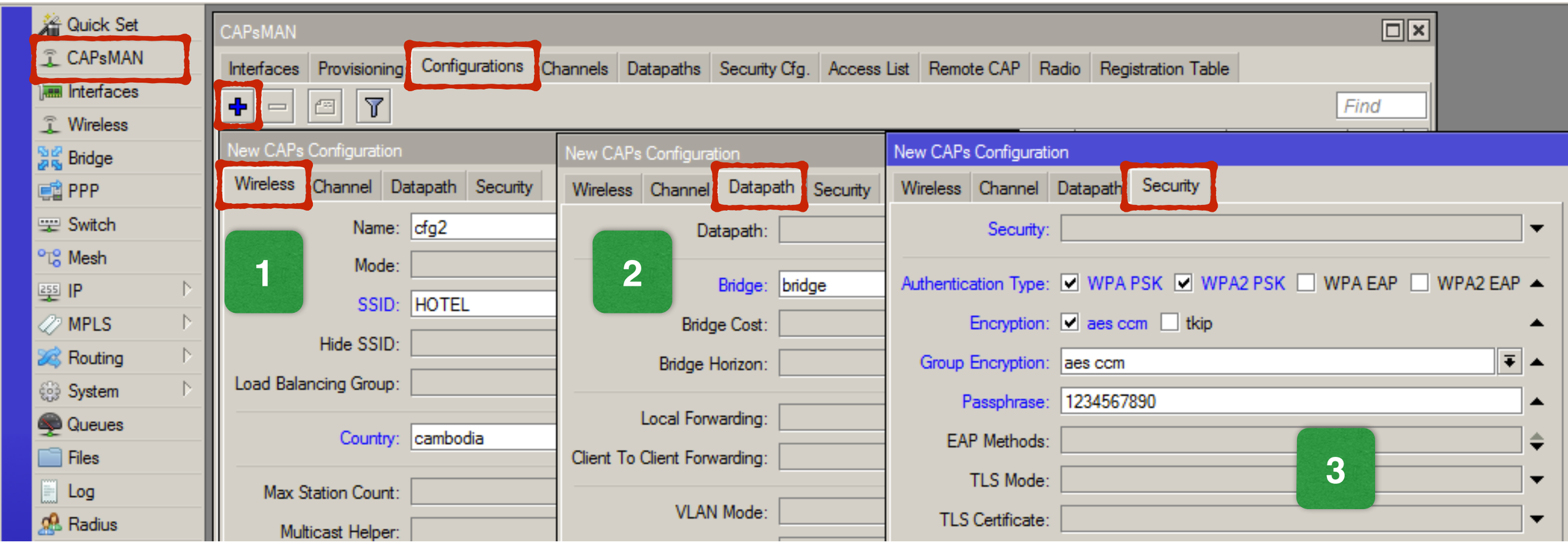
Simple Setup

2. Create and add IP configuration to Bridge interface



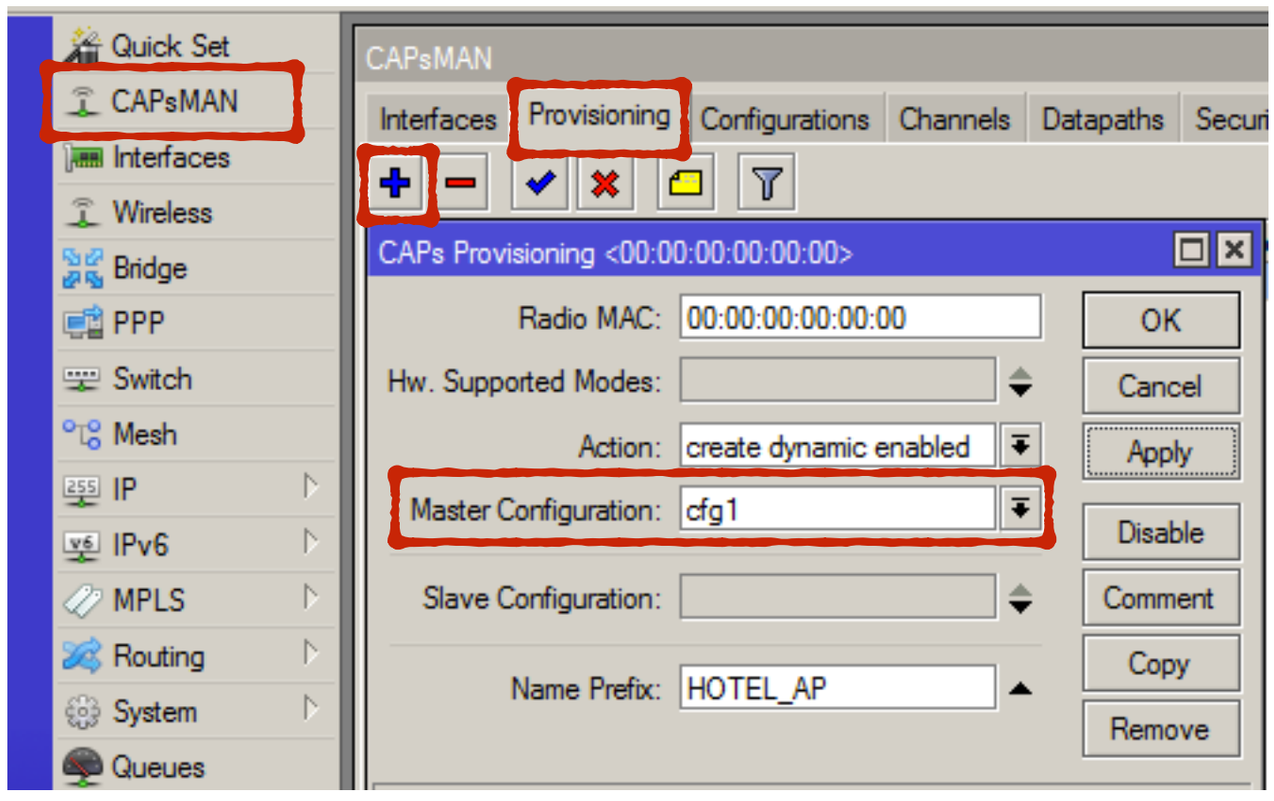
Simple Setup

3. Add new CAPsMAN configuration



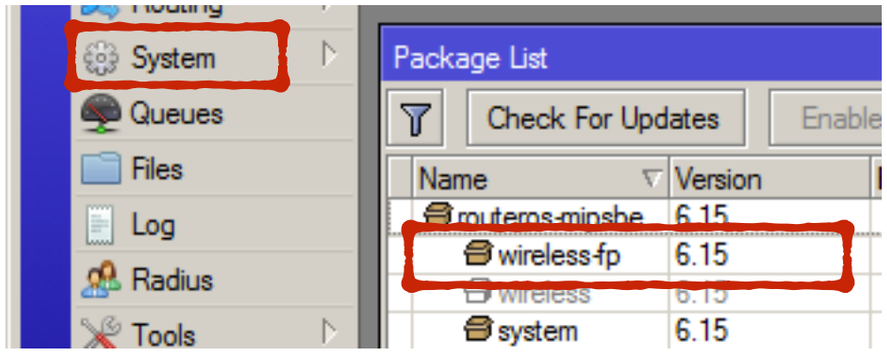
Simple Setup

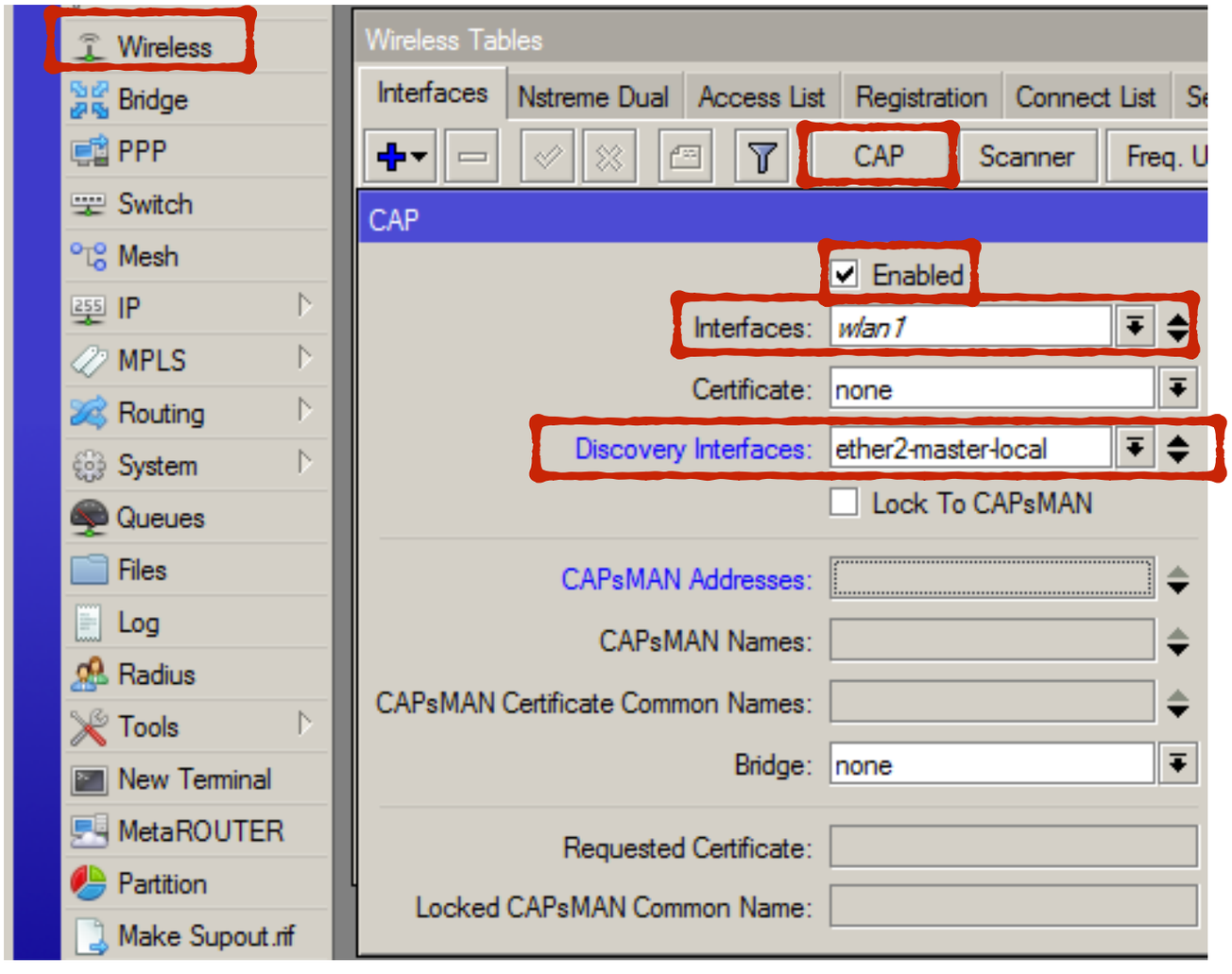
4. Add new Provisioning rule



Simple Setup

5. Enable CAP on AP





Verify on CAPsMAN

CAPsMAN

Interfaces | Provisioning | Configurations | Channels | Datapaths | Security Cfg. | Access List | Remote CAP | Radio | Registration Table

Manager | AAA

	Name	Type	MTU	L2 MTU	Tx	Rx	Tx...	Rx...	SSID	Country	Bridge	Current State	Current Channel
DRSMB	HOTEL_AP1	Interfaces	1500	1600	1544 bps	1336 bps	2	2	HOTEL	cambodia	bridge	running-ap	2452/20-Ce/gn(20dBm)
DRSMB	HOTEL_AP2	Interfaces	1500	1600	1456 bps	0 bps	2	0	HOTEL	cambodia	bridge	running-ap	2452/20-Ce/gn(20dBm)
DRSMB	HOTEL_AP3	Interfaces	1500	1600	1456 bps	0 bps	2	0	HOTEL	cambodia	bridge	running-ap	2452/20-Ce/gn(20dBm)

CAPsMAN

Interfaces | Provisioning | Configurations | Channels | Datapaths | Security Cfg. | Access List | Remote CAP | Radio | Registration Table

Provision

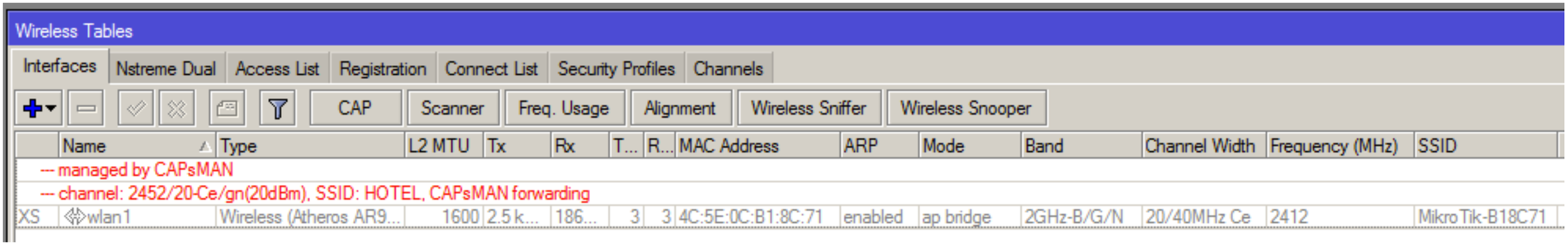
Address	Name	Board	Serial	Version	Identity	Base MAC	State	Radios
4C:5E:0C:B1:72:81	[4C:5E:0C:B1...	RB951Ui-2HnD	4AC90451A9...	6.18	RB	4C:5E:0C:B1:72:85	Run	1
:ffff:127.0.0.1	[D4:CA:6D:F1...	RB951Ui-2HnD	4AC802B657...	6.27	CAPsMAN	D4:CA:6D:F1:2A:E9	Run	1
:ffff:172.16.0.253	[4C:5E:0C:B1...	RB951G-2HnD	4F4404764FAA	6.15	RB	4C:5E:0C:B1:8C:71	Run	1

CAPsMAN

Interfaces | Provisioning | Configurations | Channels | Datapaths | Security Cfg. | Access List | Remote CAP | Radio | Registration Table

Interface	MAC Address	Tx Rate	Rx Rate	Tx Signal	Rx Signal	Uptime	Tx/Rx Packets	Tx/Rx Bytes
HOTEL_AP1	10:0B:A9:50:8F:F8	26Mbps-...	65Mbps-...	0	-43	00:01:52....	132/320	13.5 KiB/26.1 KiB
HOTEL_AP2	68:A8:6D:53:99:5C	2Mbps	130Mbps...	0	-42	00:02:20....	18/18	1392 B/944 B
HOTEL_AP3	68:A8:6D:53:99:5C	26Mbps-...	117Mbps...	0	-38	00:02:46....	32/134	3238 B/23.9 KiB

Verify on CAP



Control Packet Capture

3	2.492580	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x6ae9236e
4	2.497199	172.16.0.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x6ae9236e
5	2.498244	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x6ae9236e
6	2.499281	172.16.0.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x6ae9236e
7	2.501290	172.16.0.253	255.255.255.255	MNDP	140	Source port: 5678 Destination port: 5678
8	2.501406	Routerbo_b1:8c:6d	CDP/VTP/DTP/PAgP/UDLD	CDP	94	Device ID: CAP Port ID: bridge-local
9	3.145429	Routerbo_b1:8c:6d	Spanning-tree-(for-bridges)	STP	60	RST. Root = 32768/0/4c:5e:0c:b1:8c:6d Cost = 0 Port = 0x8001
10	4.155528	Routerbo_b1:8c:6d	Broadcast	ARP	60	Who has 172.16.0.1? Tell 172.16.0.253
11	4.155616	Routerbo_f1:2a:e8	Routerbo_b1:8c:6d	ARP	42	172.16.0.1 is at d4:ca:6d:f1:2a:e8
12	4.155744	172.16.0.253	172.16.0.1	CAPWAP	324	CAPWAP-Control - Discovery Request
13	4.157206	172.16.0.1	172.16.0.253	CAPWAP	131	CAPWAP-Control - Discovery Response
14	5.147707	Routerbo_b1:8c:6d	Spanning-tree-(for-bridges)	STP	60	RST. Root = 32768/0/4c:5e:0c:b1:8c:6d Cost = 0 Port = 0x8001
15	7.097289	172.16.0.253	172.16.0.1	DTLSv1.	192	Client Hello
16	7.149990	Routerbo_b1:8c:6d	Spanning-tree-(for-bridges)	STP	60	RST. Root = 32768/0/4c:5e:0c:b1:8c:6d Cost = 0 Port = 0x8001
17	7.542002	172.16.0.1	172.16.0.253	DTLSv1.	90	Hello Verify Request
18	7.542765	172.16.0.253	172.16.0.1	DTLSv1.	208	Client Hello
19	7.544226	172.16.0.1	172.16.0.253	DTLSv1.	694	Server Hello, Server Key Exchange[Malformed Packet]
20	8.402777	172.16.0.253	172.16.0.1	DTLSv1.	412	Client Key Exchange, Change Cipher Spec, Encrypted Handshake Message
21	8.851843	172.16.0.1	172.16.0.253	DTLSv1.	125	Server Hello
22	8.852296	172.16.0.1	172.16.0.253	DTLSv1.	590	Server Key Exchange[Malformed Packet]
23	8.852416	172.16.0.1	172.16.0.253	DTLSv1.	71	Server Hello Done
24	8.856020	172.16.0.1	172.16.0.253	DTLSv1.	320	New Session Ticket, Change Cipher Spec, Encrypted Handshake Message
25	8.859590	172.16.0.253	172.16.0.1	DTLSv1.	1363	Application Data
26	8.860212	172.16.0.253	172.16.0.1	DTLSv1.	659	Application Data

3	2.572181	0.0.0.0	255.255.255.255	DHCP	342	DHCP Discover - Transaction ID 0x1a55b1b9
4	2.576525	172.16.1.1	255.255.255.255	DHCP	342	DHCP Offer - Transaction ID 0x1a55b1b9
5	2.577622	0.0.0.0	255.255.255.255	DHCP	342	DHCP Request - Transaction ID 0x1a55b1b9
6	2.578436	172.16.1.1	255.255.255.255	DHCP	342	DHCP ACK - Transaction ID 0x1a55b1b9
8	5.026378	172.16.1.254	255.255.255.255	CAPWAP	326	CAPWAP-Control - Discovery Request
9	5.027840	Routerbo_f1:2a:e7	Broadcast	ARP	42	Who has 172.16.1.254? Tell 172.16.1.1
11	5.028093	Routerbo_b1:72:81	Routerbo_f1:2a:e7	ARP	60	172.16.1.254 is at 4c:5e:0c:b1:72:81
12	5.028120	172.16.1.1	172.16.1.254	CAPWAP	131	CAPWAP-Control - Discovery Response
33	9.559227	Routerbo_b1:72:81	Routerbo_f1:2a:e7	0x88bc	60	Ethernet II
34	9.559268	Routerbo_f1:2a:e7	Routerbo_b1:72:81	0x88bc	53	Ethernet II
75	39.890289	Routerbo_b1:72:81	Routerbo_f1:2a:e7	0x88bc	60	Ethernet II
76	39.890330	Routerbo_f1:2a:e7	Routerbo_b1:72:81	0x88bc	53	Ethernet II

Data Packet Capture

```
 969 57.324377  216.58.221.78                192.168.10.5                   HTTP          1284 HTTP/1.1 302 Found  (text/html)
 762 48.304069  192.168.10.5                 216.58.221.78                  TLSv1.2       1270 Application Data
1861 64.837957  216.58.221.67                192.168.10.5                   TLSv1.2       1263 Application Data
 973 57.406591  192.168.10.5                 216.58.221.67                  HTTP          1243 GET /?gws_rd=cr&ei=r14zVezIIKWymAWhtoDQCQ HTTP/1.1

⊞ Frame 969: 1284 bytes on wire (10272 bits), 1284 bytes captured (10272 bits)
⊞ Ethernet II, Src: Routerbo_f1:2a:e8 (d4:ca:6d:f1:2a:e8), Dst: Routerbo_b1:8c:6d (4c:5e:0c:b1:8c:6d)
⊞ Internet Protocol Version 4, Src: 172.16.0.1 (172.16.0.1), Dst: 172.16.0.253 (172.16.0.253)
⊞ User Datagram Protocol, Src Port: 5247 (5247), Dst Port: 57182 (57182)
⊞ Control And Provisioning of Wireless Access Points
⊞ Ethernet II, Src: Routerbo_f1:2a:e5 (d4:ca:6d:f1:2a:e5), Dst: IntelCor_50:8f:f8 (10:0b:a9:50:8f:f8)
⊞ Internet Protocol Version 4, Src: 216.58.221.78 (216.58.221.78), Dst: 192.168.10.5 (192.168.10.5)
⊞ Transmission Control Protocol, Src Port: 80 (80), Dst Port: 49382 (49382), Seq: 1, Ack: 1090, Len: 1180
⊟ Hypertext Transfer Protocol
  ⊞ HTTP/1.1 302 Found\r\n
Location: http://www.google.com.kh/?gws_rd=cr&ei=r14zVezIIKWymAWhtoDQCQ\r\n
```

```
 910 57.088778  Routerbo_b1:72:81          Routerbo_f1:2a:e7              0x88bc     1510 Ethernet II
 908 57.053175  Routerbo_b1:72:81          Routerbo_f1:2a:e7              0x88bc     1510 Ethernet II
 907 57.052935  Routerbo_b1:72:81          Routerbo_f1:2a:e7              0x88bc     1510 Ethernet II
 860 52.837004  Routerbo_b1:72:81          Routerbo_f1:2a:e7              0x88bc     1510 Ethernet II
 842 52.791851  Routerbo_b1:72:81          Routerbo_f1:2a:e7              0x88bc     1510 Ethernet II
 661 46.798638  Routerbo_b1:72:81          Routerbo_f1:2a:e7              0x88bc     1510 Ethernet II
 646 46.691592  Routerbo_b1:72:81          Routerbo_f1:2a:e7              0x88bc     1510 Ethernet II
 879 52.882855  Routerbo_f1:2a:e7          Routerbo_b1:72:81              0x88bc     1440 Ethernet II
 877 52.882010  Routerbo_f1:2a:e7          Routerbo_b1:72:81              0x88bc     1440 Ethernet II
 875 52.880624  Routerbo_f1:2a:e7          Routerbo_b1:72:81              0x88bc     1440 Ethernet II
 874 52.879233  Routerbo_f1:2a:e7          Routerbo_b1:72:81              0x88bc     1440 Ethernet II

⊞ Frame 907: 1510 bytes on wire (12080 bits), 1510 bytes captured (12080 bits)
⊟ Ethernet II, Src: Routerbo_b1:72:81 (4c:5e:0c:b1:72:81), Dst: Routerbo_f1:2a:e7 (d4:ca:6d:f1:2a:e7)
  ⊞ Destination: Routerbo_f1:2a:e7 (d4:ca:6d:f1:2a:e7)
  ⊞ Source: Routerbo_b1:72:81 (4c:5e:0c:b1:72:81)
    Type: Unknown (0x88bc)
⊟ Data (1496 bytes)
    Data: d9d605d400104000000000000d4ca6df12ae5100ba9508ff8...
    [Length: 1496]
```

Question ?

សូមអរគុណ

saum arkoun

Thank You