CENTRALIZATION OF WIRELESS NETWORK MANAGEMENT WITH MIKROTIK CAPSMAN

MUM Ho Chi Minh, Vietnam

April 2017

About me

- My name: Binh Nguyen Dang Thai
- Email: binhndt@uranus.com.vn
- Cellphone: +84 909006026
- Website: http://uranus.com.vn
- Support website: http://forum.uranus.com.vn
- Own: URANUS INFORMATION SYSTEM COMPANY

Objective

- Centralizing management MikroTik access point with CAPsMAN.
- Integrating wireless network into LAN.

CAPsMAN Features

- Centralized management of RouterOS (ROS) 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
- VLAN Aware
- Template Based - Profile

Overview

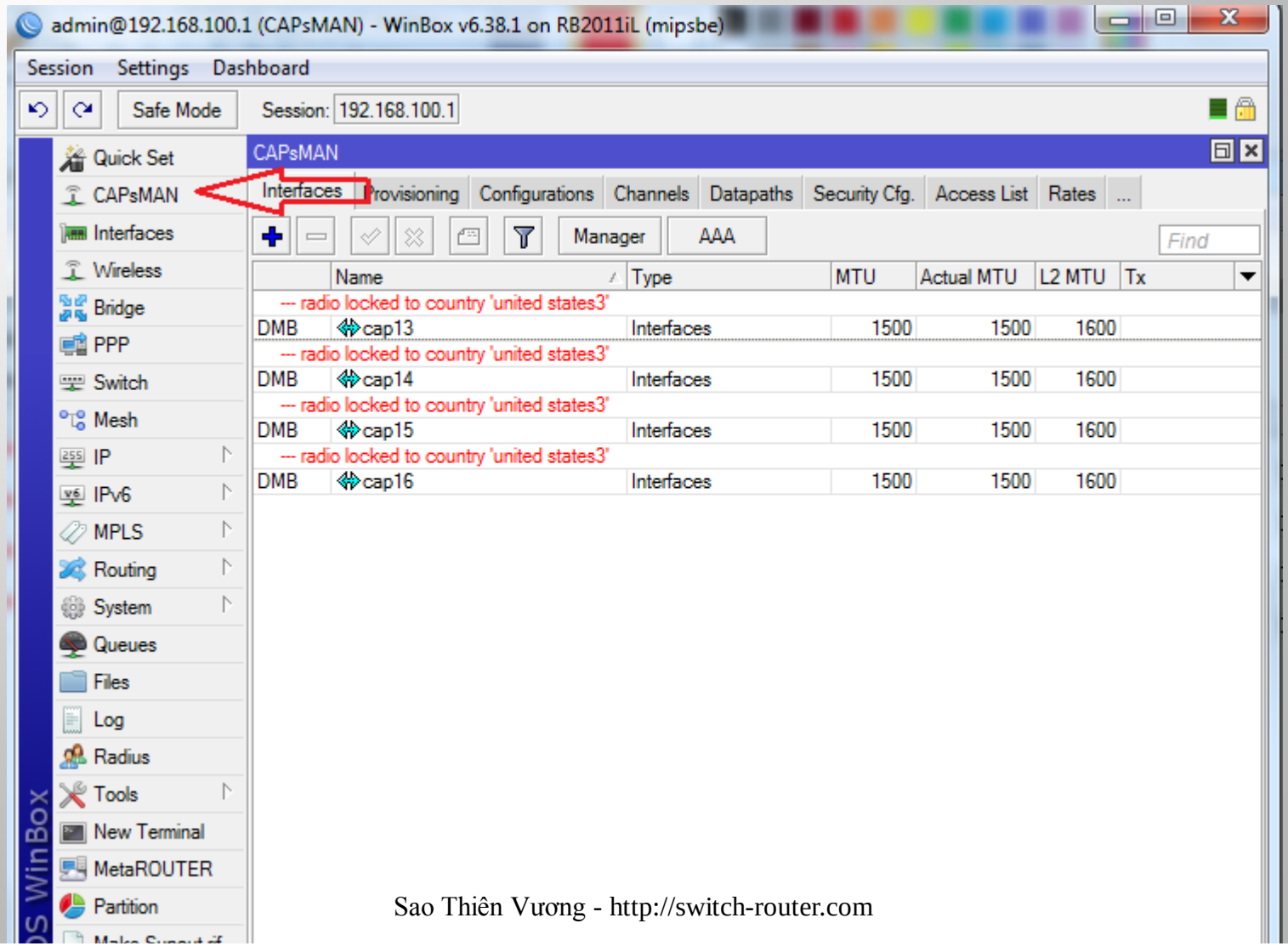
CAPsMAN (Controlled AP System Manager)

- Centralized wireless network management
- Data Processing, (if necessary) (by default)
- Manage Configuration of APs
- Manage Client authentication

Works on any ROS Device from Version 6.22rc7 for CAPsMAN v2

Wireless package is required from ROS 6.38.1

Overview

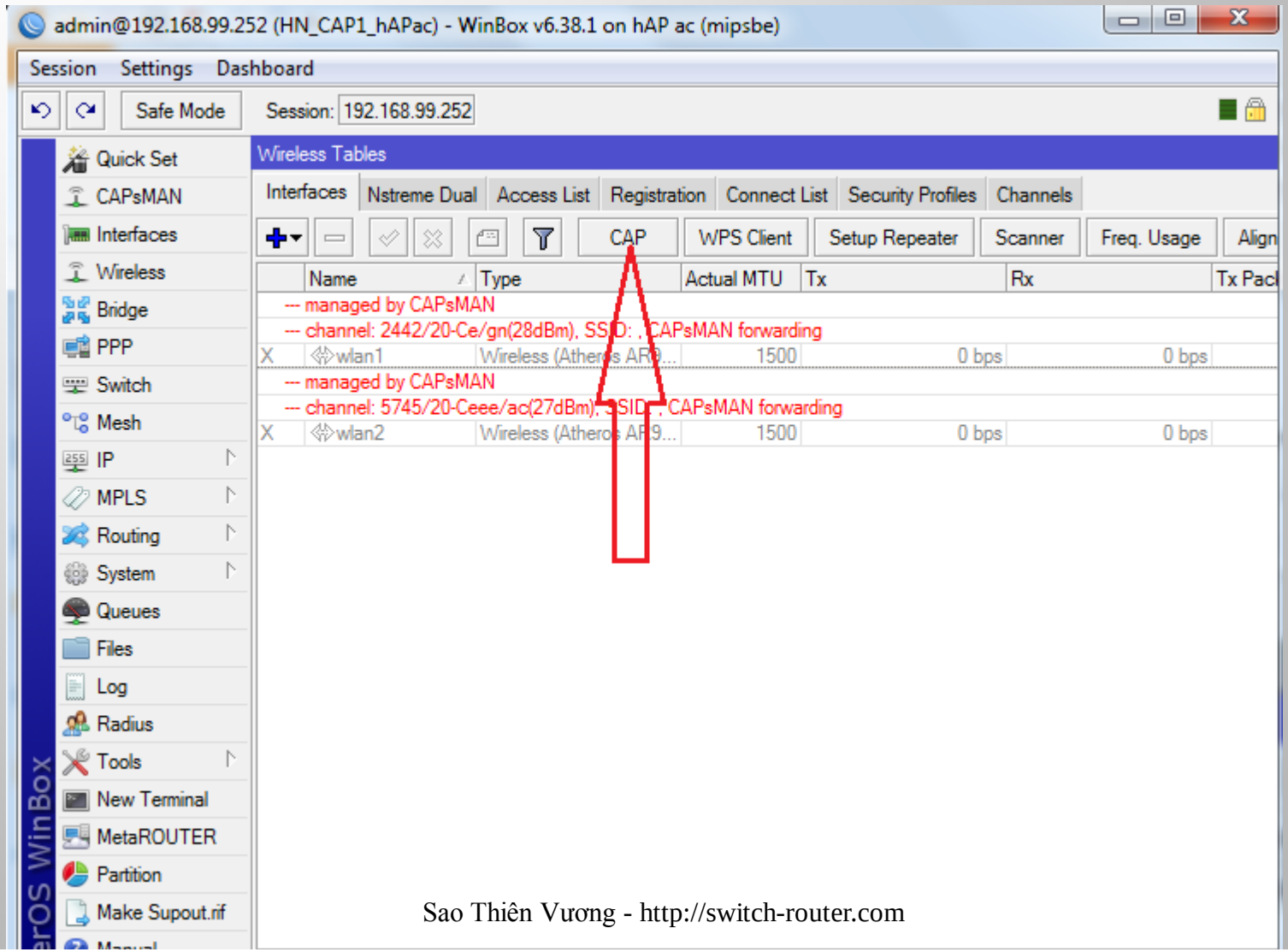

admin@192.168.100.1 (CAPsMAN) - WinBox v6.38.1 on RB2011iL (mipsbe)
Session Settings Dashboard
Safe Mode
Session: 192.168.100.1
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
IPv6
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
CAPsMAN
Interfaces
Provisioning
Configurations
Channels
Datapaths
Security Cfg.
Access List
Rates
Manager
AAA
Find
Name
Type
MTU
Actual MTU
L2 MTU
Tx
--- radio locked to country 'united states3'
DMB cap13 Interfaces 1500 1500 1600
--- radio locked to country 'united states3'
DMB cap14 Interfaces 1500 1500 1600
--- radio locked to country 'united states3'
DMB cap15 Interfaces 1500 1500 1600
--- radio locked to country 'united states3'
DMB cap16 Interfaces 1500 1500 1600

Overview

CAP (Controlled Access Point)

- Provide wireless connectivity
- Wireless link layer encryption / decryption

Overview


admin@192.168.99.252 (HN_CAP1_hAPac) - WinBox v6.38.1 on hAP ac (mipsbe)
Session
Settings
Dashboard
Safe Mode
Session: 192.168.99.252
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.rif
RouterOS WinBox
Wireless Tables
Interfaces
Nstreme Dual
Access List
Registration
Connect List
Security Profiles
Channels
CAP
WPS Client
Setup Repeater
Scanner
Freq. Usage
Align
Name
Type
Actual MTU
Tx
Rx
Tx Pacl
--- managed by CAPsMAN
--- channel: 2442/20-Ce/gn(28dBm), SSID: , CAPsMAN forwarding
X
wlan1
Wireless (Atheros AR9...
1500
0 bps
0 bps
--- managed by CAPsMAN
--- channel: 5745/20-Ceee/ac(27dBm), SSID: , CAPsMAN forwarding
X
wlan2
Wireless (Atheros AR9...
1500
0 bps
0 bps

CAP to CAPsMAN Connection

Management connection can be established using

- MAC layer protocols (layer2)
- IP layer protocols (layer3)

Secured by DTLS (datagram transport layer security)

CAP can pass client data connection to manager

- Data connection is **not secured**
- **IPSec** or **encrypted tunnels** is needed for data security

CAP to CAPsMAN Connection

MAC layer connection feature (layer2)

- No IP configuration is necessary on CAP
- Both must be on the same layer2 segment
- Either Physical or virtual (layer 2 tunnels)

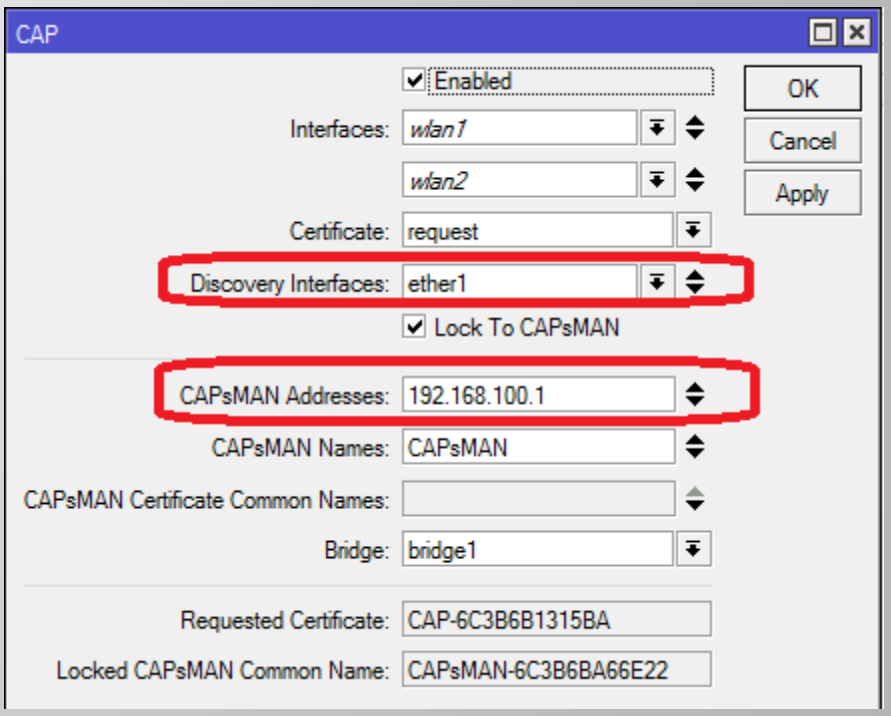
IP layer (UDP) connection feature (layer 3)

- Can traverse NAT if necessary.
- UDP port 5246,5247
- If they are not on the same L2 segment, CAP must be provisioned with the CAPsMAN's IP

CAP to CAPsMAN Connection

During Discovery process, CAP attempt to contact CAPsMAN using:

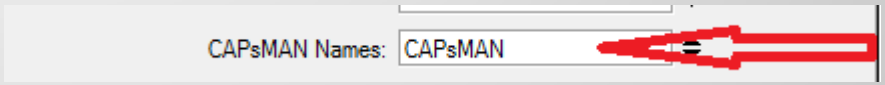
- Configured list of manager IP address
- List of CAPsMAN IPs obtained from DHCP server
- Broadcasting on configured interface using both IP and MAC layer protocols



CAP to CAPsMAN Connection

After building the list of available Manager, CAP select CAPsMAN based on:

- Caps-man-names option (Manager Identity)(if specified)



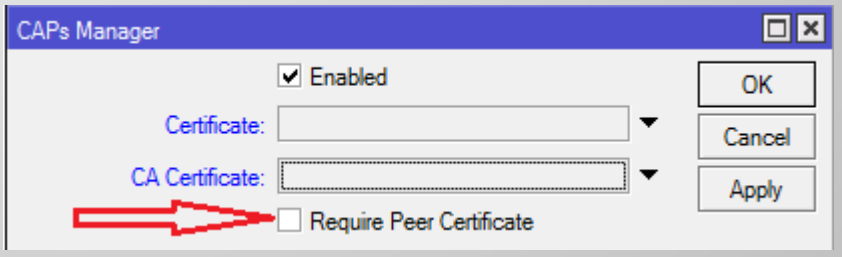
- Suitable manager with MAC layer connectivity is preferred to manager with IP connectivity

CAP to CAPsMAN Connection

After Manager is selected, CAP attempts to establish DTLS connection. There are the following authentication modes possible:

- no certificates on CAP and CAPsMAN - no authentication
- Certification configuration only on CAPsMAN

  (**require-peer-certificate=no** on CAPsMAN)



- Certificate configured on both (mutual authentication)

  (**require-peer-certificate=yes** on CAPsMAN)

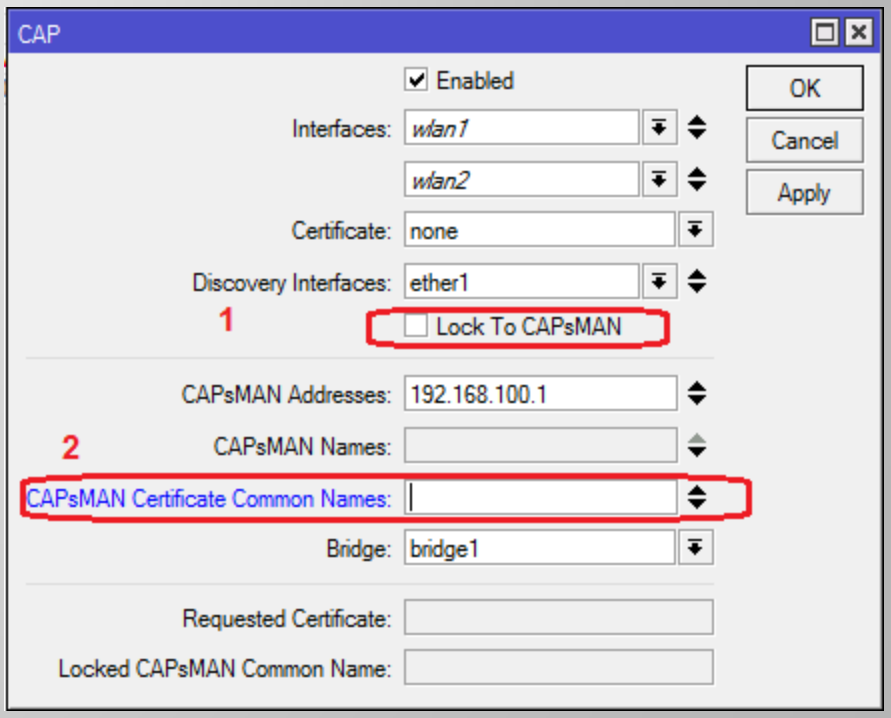
CAP to CAPsMAN Connection

CAP Auto locking to CAPsMAN:

- CAP can be configured to automatically lock to CAPsMAN by: 1

(Use of certificate is mandatory for locking to work)

- CAP can be manually locked to CAPsMAN by: 2



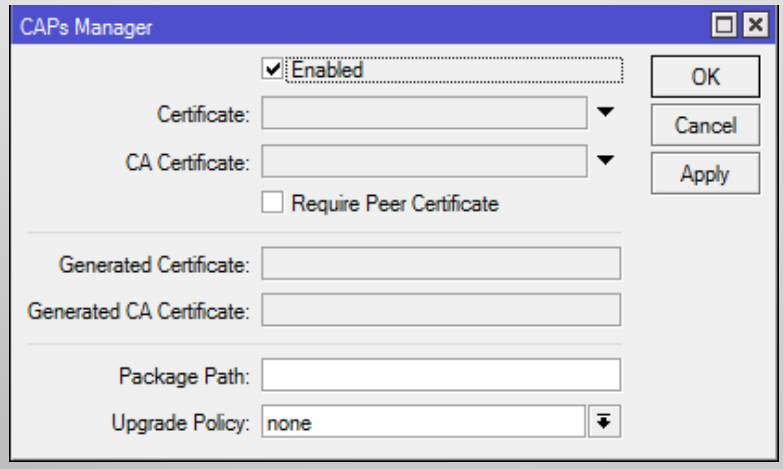
Auto Certificates

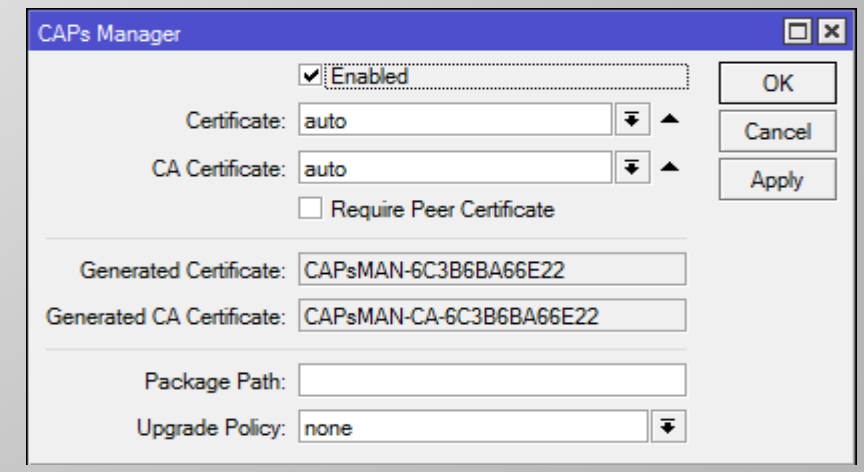
- CAPsMAN can be configured to generate necessary certificates automatically
- CAP can be configured to request certificate from CAPsMAN

Auto Certificates

CAPsMAN Auto certificate configuration:

- Certificate: 1. if set to **none**, will operate in no-certificate mode; 2. If set to **auto**, will attempt to issue certificate to itself
- ca-certificate: 1. If set to **none**, will not be able to issue certificate to itself or sign certificate requests from CAPs; 2. If set to **auto**, will generate self-signed CA certificate



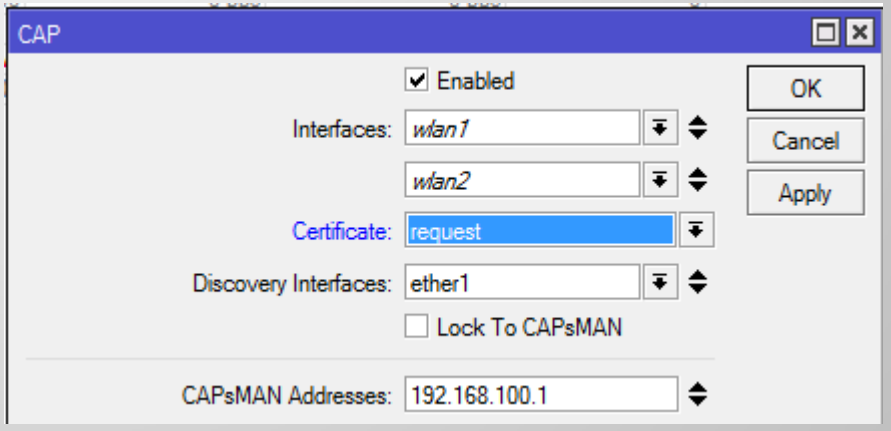


Feb/14/2017 11:20:13	memory	system, info	CAPsMAN configuration changed by admin
Feb/14/2017 11:20:20	memory	certificate, info	generated CA certificate: CAPsMAN-CA-6C3B6BA66E22
Feb/14/2017 11:20:21	memory	certificate, debug	trust store updated
Feb/14/2017 11:20:36	memory	certificate, info	generated certificate CAPsMAN-6C3B6BA66E22:201B414BEEB7AE44::::: key-size:2048 usage:d valid:24854 for CA CAPsMAN-CA

Auto Certificates

CAP Auto certificate configuration:

- CAP must be configured with setting **certificate = request**



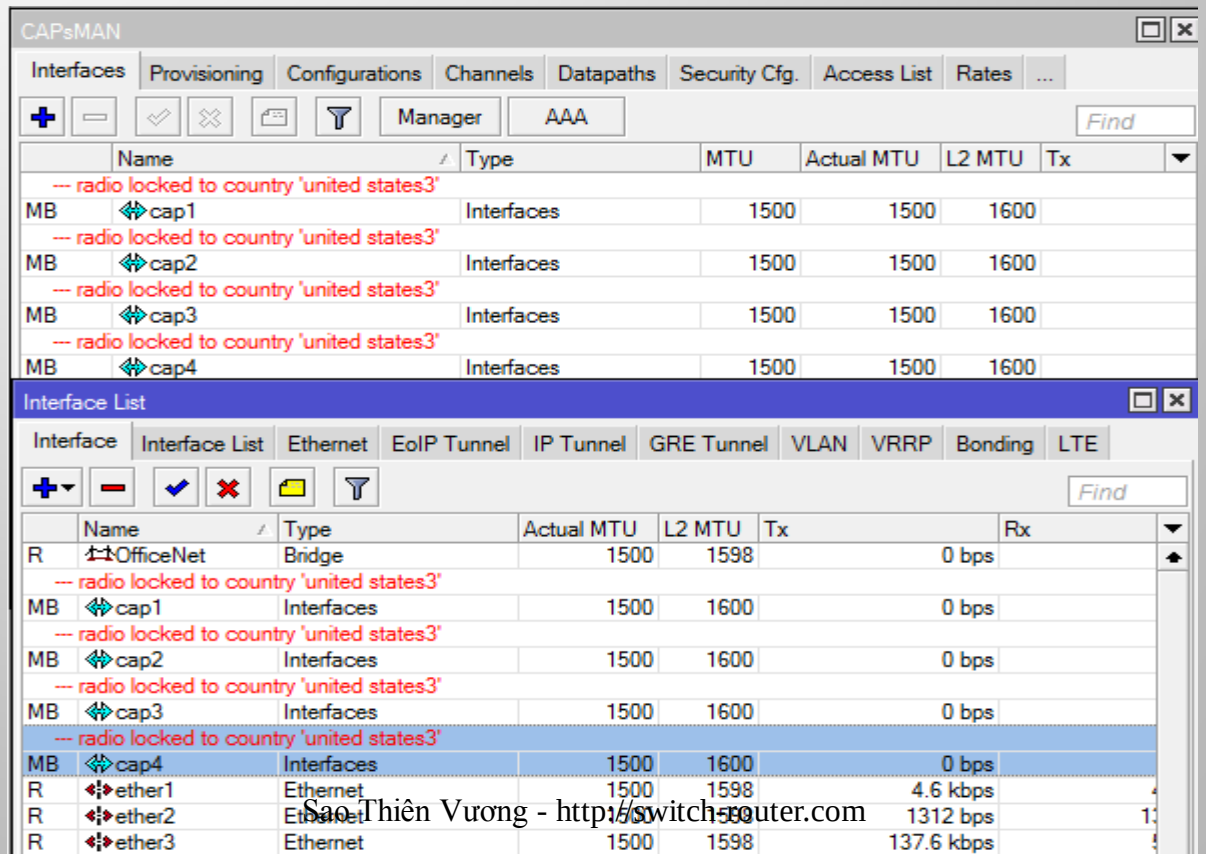
Auto Certificates

- CAP will initially generate private key and certificate request
- After connection establishment, CAP will request CAPsMAN to sign its certificate
- CAPsMAN will send CA certificate and newly issued certificate
- CAP will import these certificates in its certificate store

Feb/14/2017 11:39:40	memory	system, info	CAP configuration changed by admin
Feb/14/2017 11:39:41	memory	caps, debug	CAP None->Discover
Feb/14/2017 11:39:41	memory	caps, debug	CAP discovery target list:
Feb/14/2017 11:39:41	memory	caps, debug	::ffff:192.168.100.1:5246
Feb/14/2017 11:39:44	memory	caps, debug	CAP discovery over, results:
Feb/14/2017 11:39:44	memory	caps, debug	CAPsMAN (::ffff:192.168.100.1:5246)
Feb/14/2017 11:39:44	memory	caps, debug	CAP Discover->Select
Feb/14/2017 11:39:44	memory	caps, info	CAP selected CAPsMAN CAPsMAN (::ffff:192.168.100.1:5246)
Feb/14/2017 11:39:44	memory	caps, debug	CAP Select->Connect
Feb/14/2017 11:39:45	memory	caps, info	CAP connected to CAPsMAN (::ffff:192.168.100.1:5246), CommonName 'CAPsMAN-6C3B6BA66E22'
Feb/14/2017 11:39:45	memory	caps, debug	CAP Connect->Join
Feb/14/2017 11:39:45	memory	caps, info	imported CAP CA certificate
Feb/14/2017 11:39:45	memory	caps, info	imported CAP certificate
Feb/14/2017 11:39:45	memory	caps, info	CAP joined CAPsMAN (::ffff:192.168.100.1:5246)
Feb/14/2017 11:39:45	memory	caps, debug	CAP Join->Joined

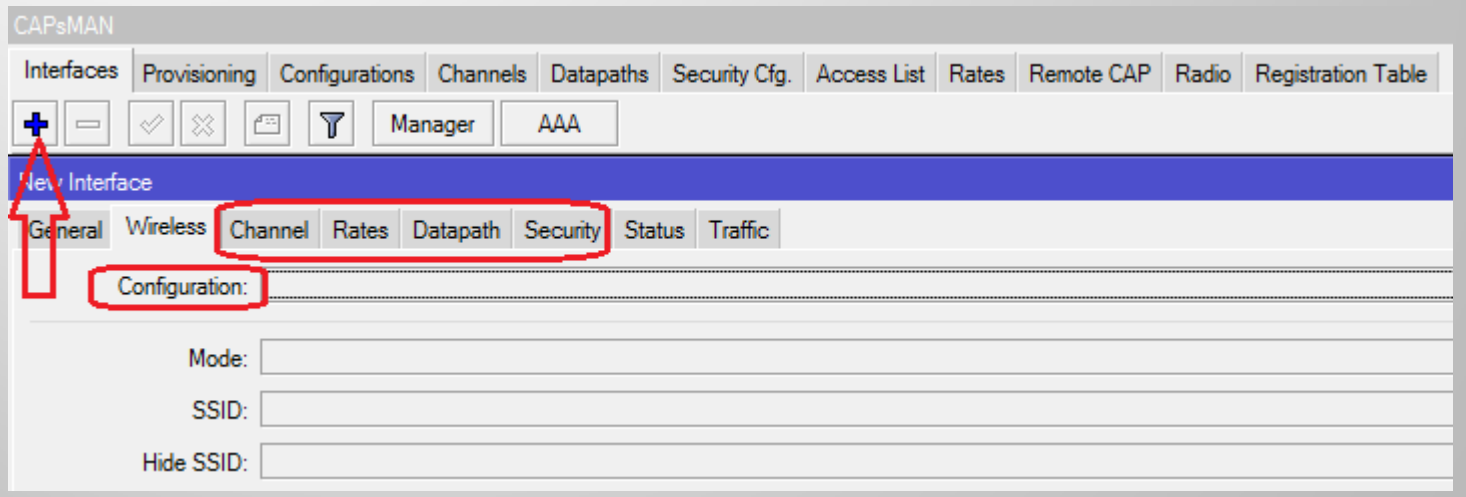
CAPsMAN Configuration

- Each wireless interface on a CAP that is under CAPsMAN control appears as a virtual interface on the CAPsMAN



CAPsMAN Configuration

Many wireless interface settings are able to be grouped together into named groups ('profiles') that simplifies the reuse of configuration



CAPsMAN Configuration

Interface Settings and Profiles:

- Channel - channel related settings
- Datapath - data forwarding related settings.
- Security - security related settings, such as allowed authentication types or passphrase
- Rates – rate related settings
- Configuration - main wireless settings profile, includes settings such as SSID, and additionally binds together other setting profiles

Any profile setting can be overridden directly in an Interface Settings for maximum flexibility

Interface Types

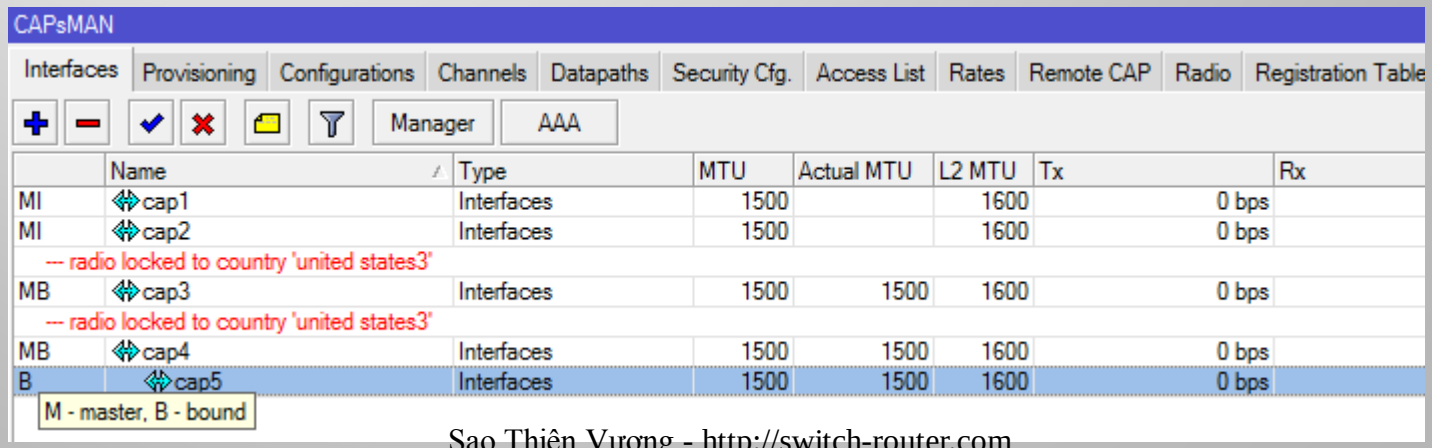
There are 2 types of interfaces:

- Master Interface: Holds the configuration for an actual wireless interface (Physical CAPs)

  Master interfaces will become operational if it's enabled

- Slave Interface: Holds the configuration for a Virtual AP (Virtual CAPs)

  Slave interfaces will become operational only if both Master and Slave interfaces are enabled



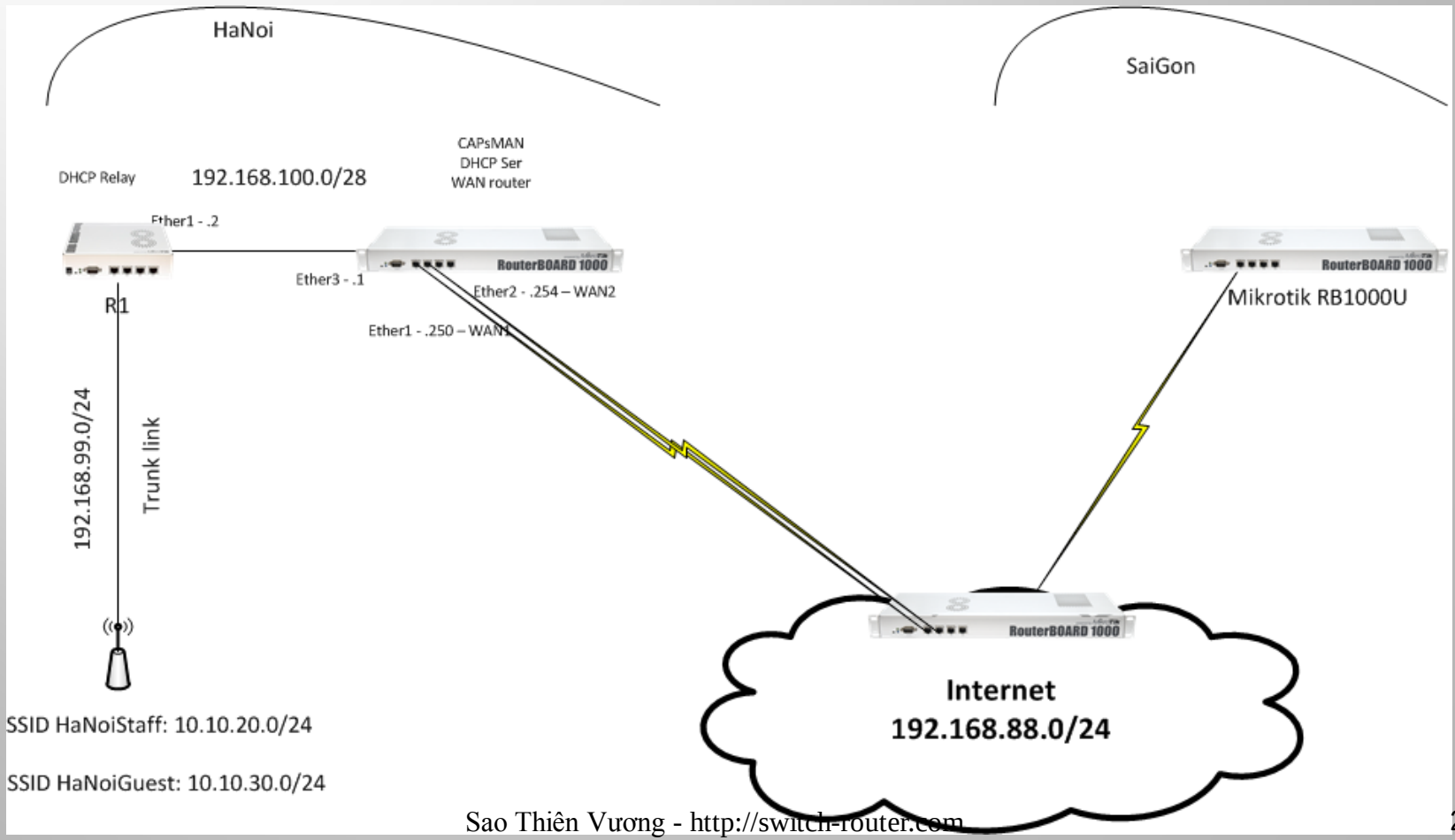
Interface Types

Interfaces on CAPsMAN can be configured:

- Statically: Stored in RouterOSconfiguration and will persist across reboots
- Dynamically: exist only while a particular CAP is connected to CAPsMAN

Network topology

- Network topology for LAB



Network topology

- My “real” LAB

Deployment

Requirements:

- Wireless LAN with 2 SSIDs for Staff and Guest
- Centralized Guest traffic for management.
- Unified Staff SSID with VLAN for Staff in corporate network.

Network information

- OSPF dynamic routing for Networks on R1 & WAN router.
- Network for Guest: 10.10.30.0/24
- Network for Staff: 10.10.20.0/24; VLAN ID 20

Deployment

WAN router:

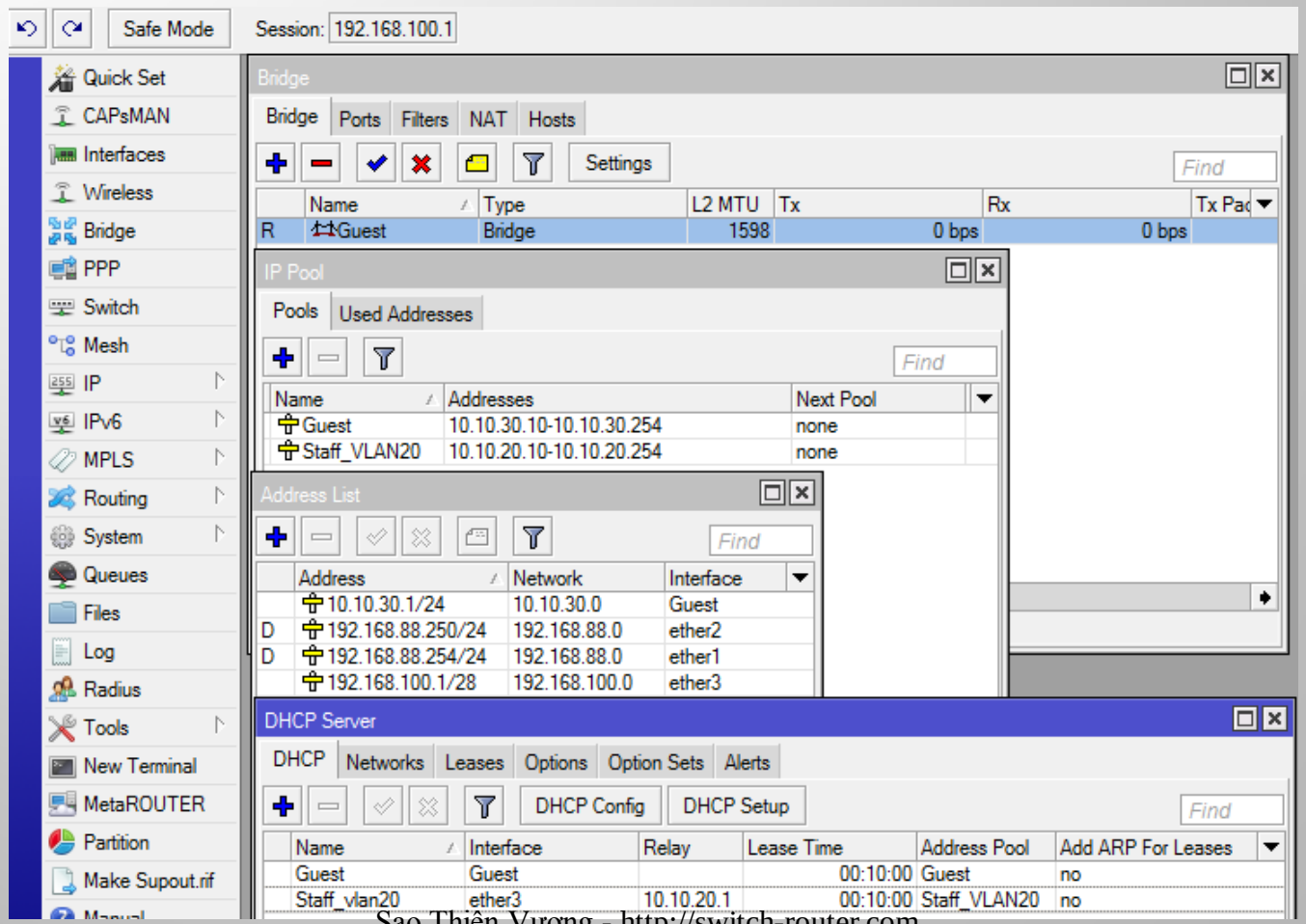
- Create Bridge interface for Guest
- Add IP configuration to Bridge interface
- Add DHCP server for Guest and DHCP for Staff

R1 router

- Create Bridge interface for Staff
- Add IP configuration to Bridge interface
- Add DHCP relay for Staff
- Trunk ports for APs

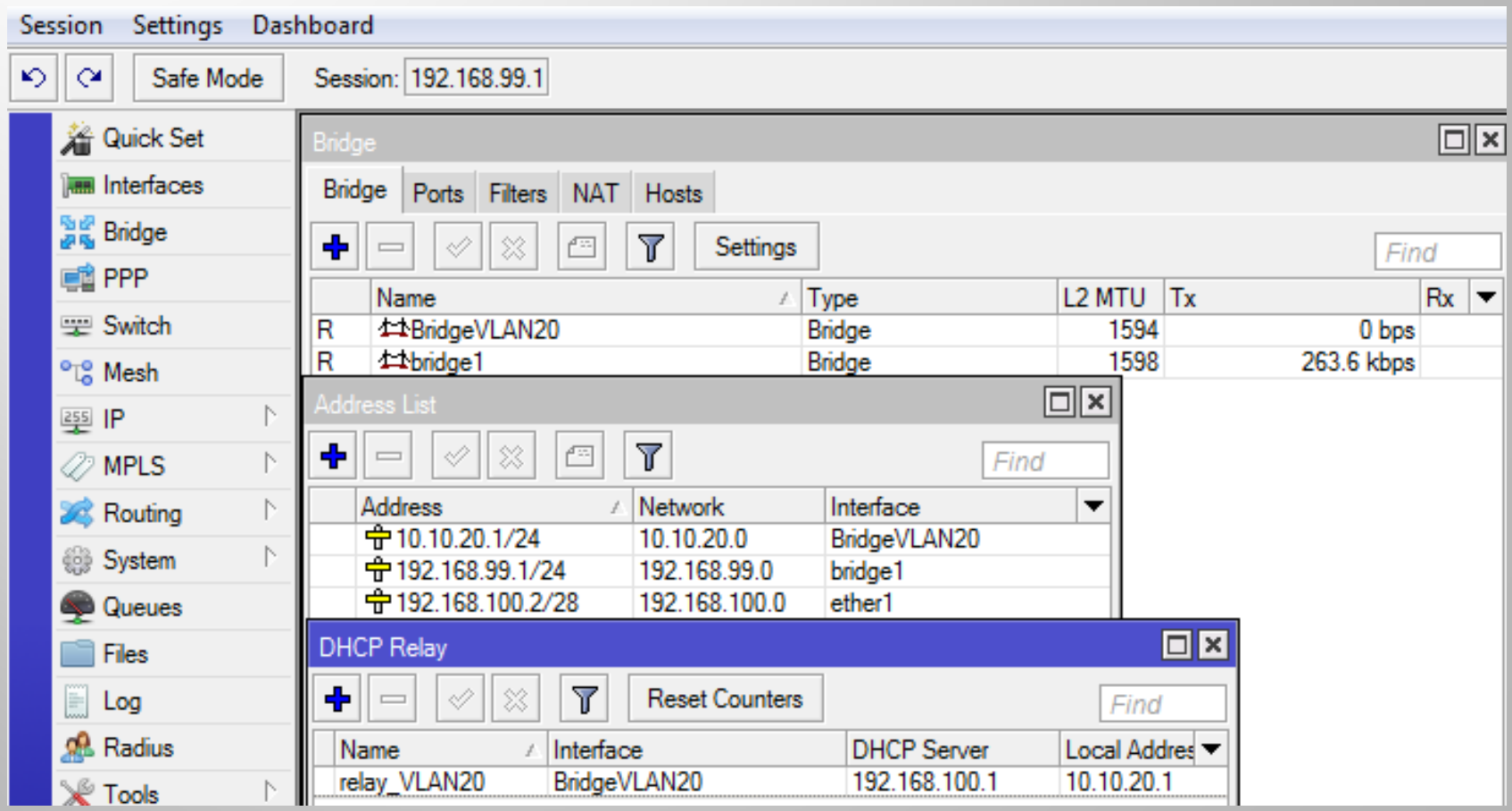
Deployment

- WAN router:



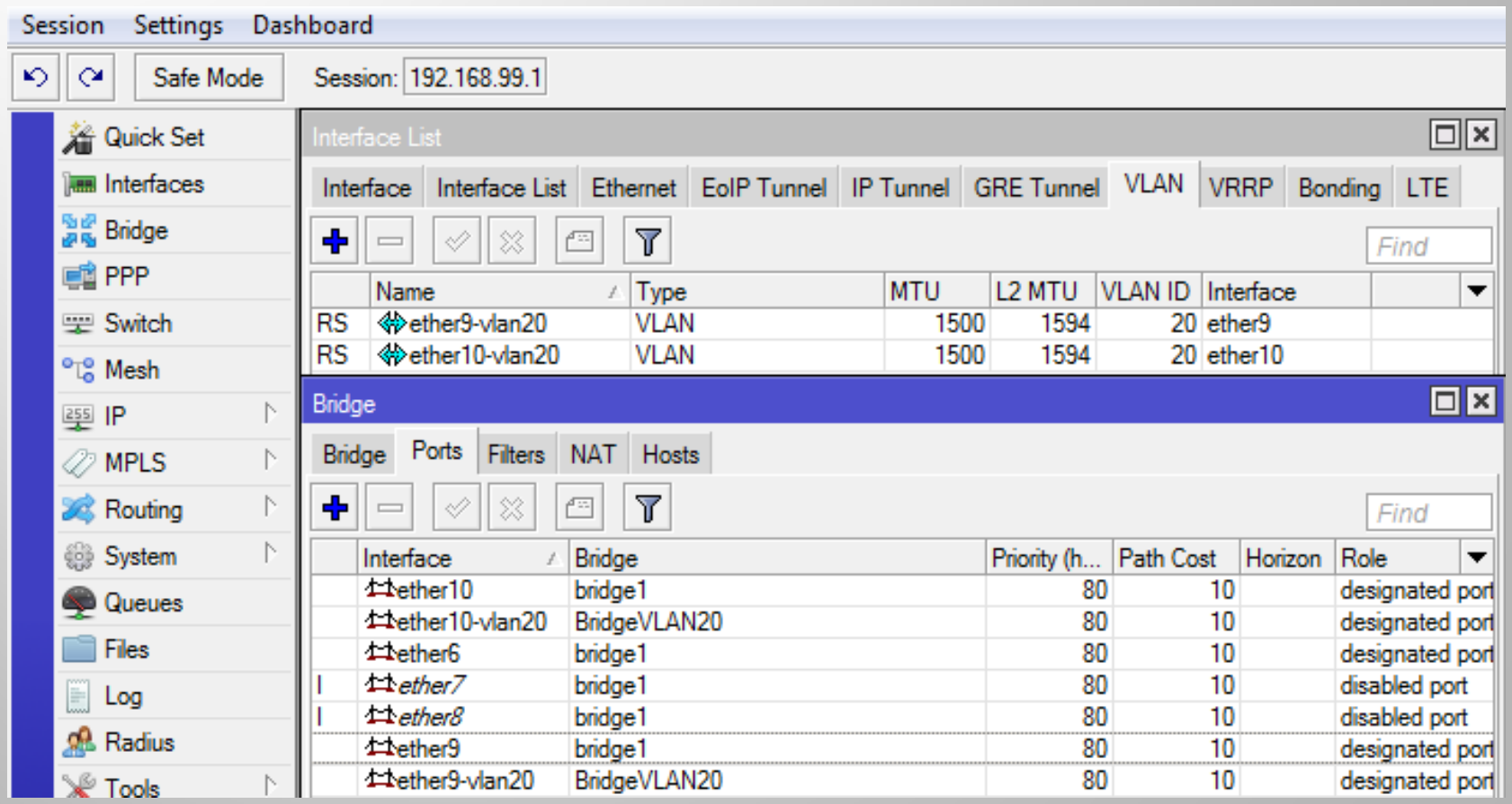
Deployment

- R1 router



Deployment

- R1 router – trunking ports



Deployment

CAPsMAN Setup

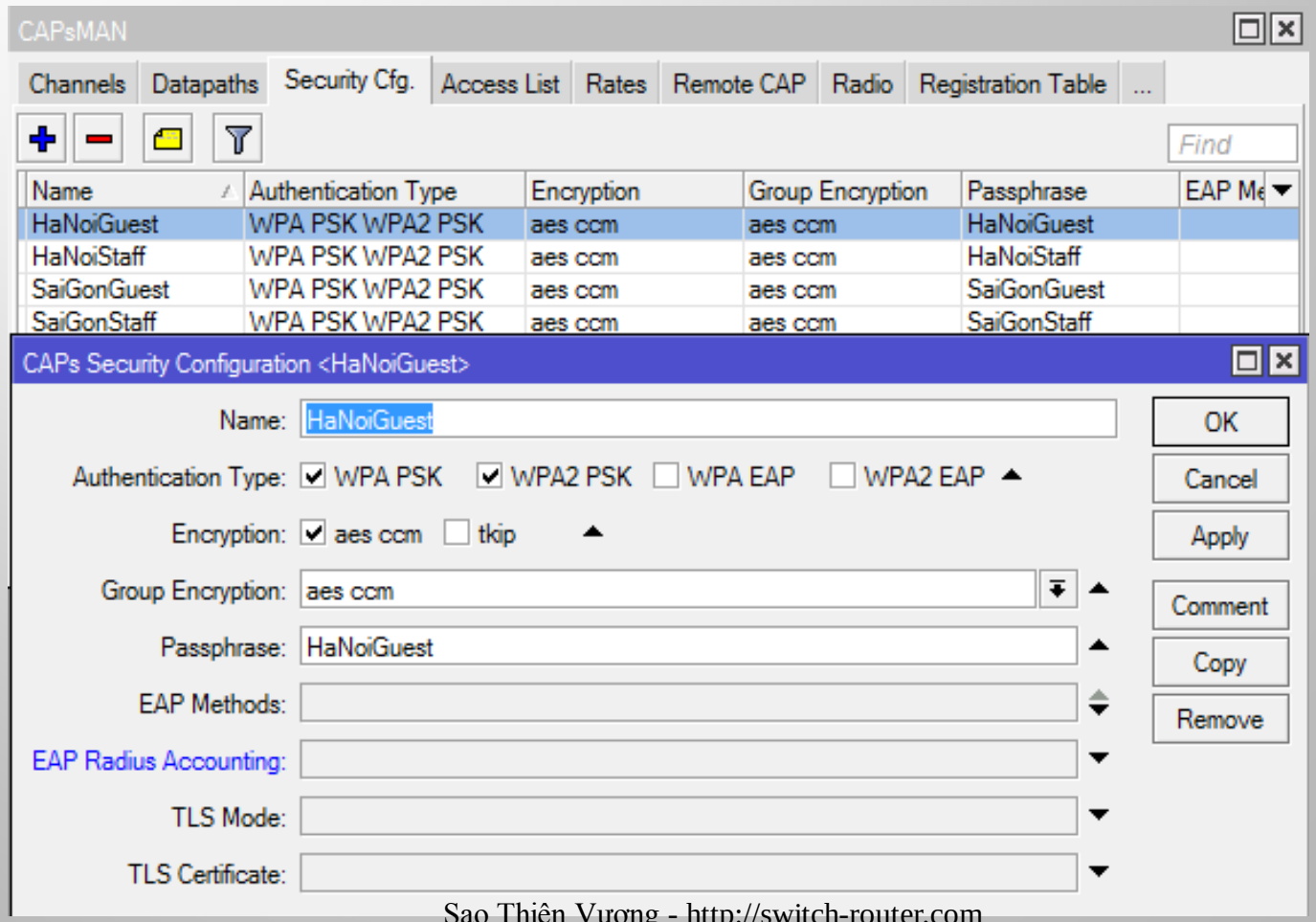
- Enable CAPsMAN service
- Enable certificate and CA certificate auto on CAPsMAN
- Create CAPsMAN Configuration
- Create Provisioning rule

CAP Setup

- Enable CAP mode on the APs
- Enable certificate request on the APs
- Set Identity APs

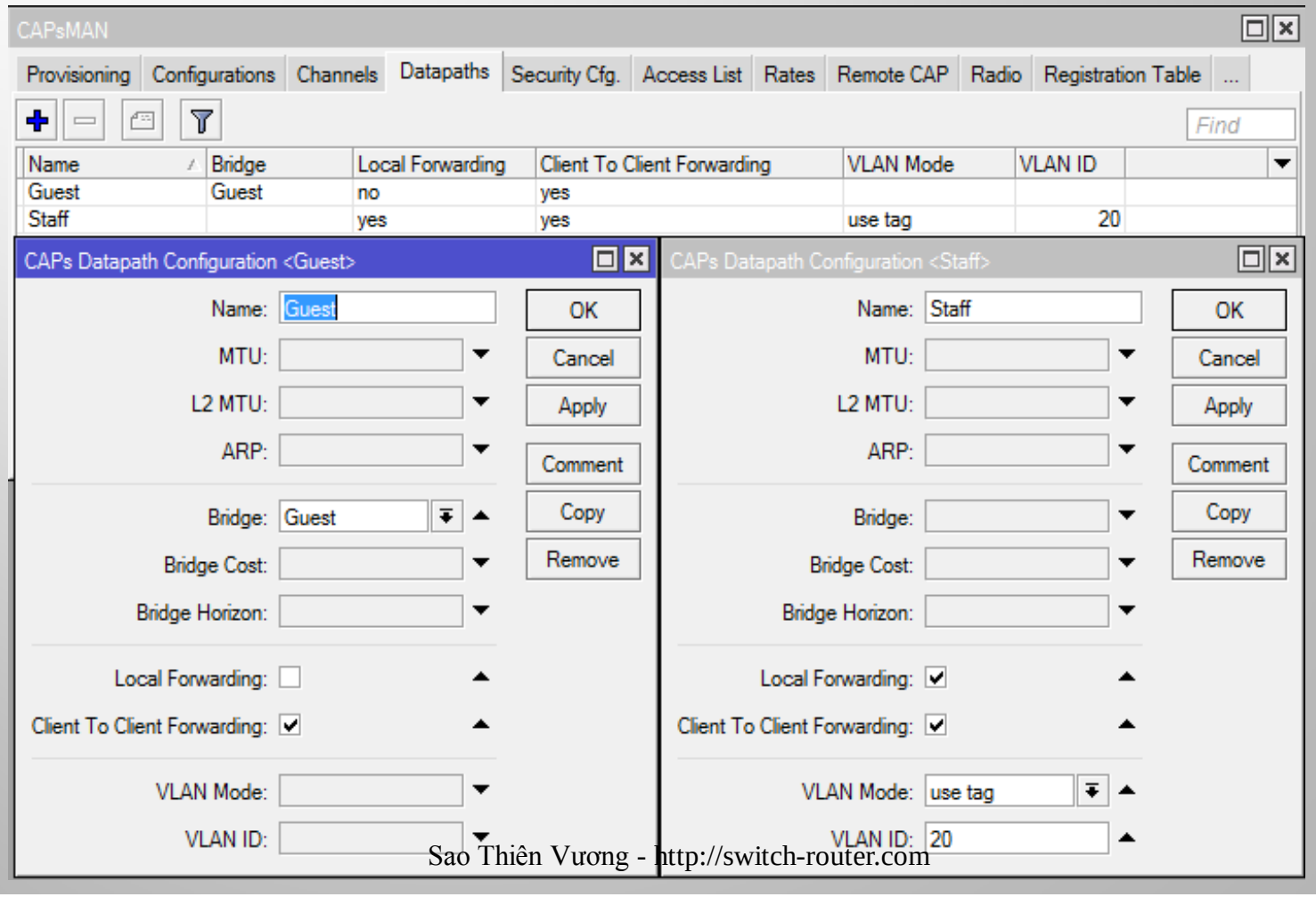
CAPsMAN Setup

- Security Profiles



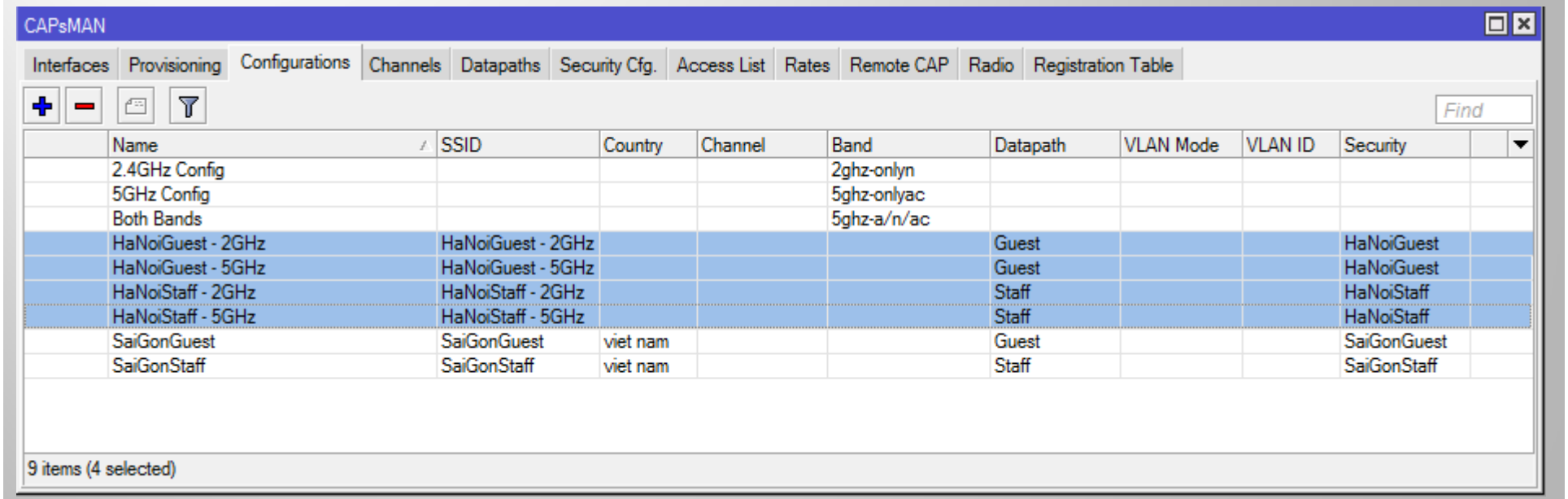
CAPsMAN Setup

- Datapath profiles



CAPsMAN Setup

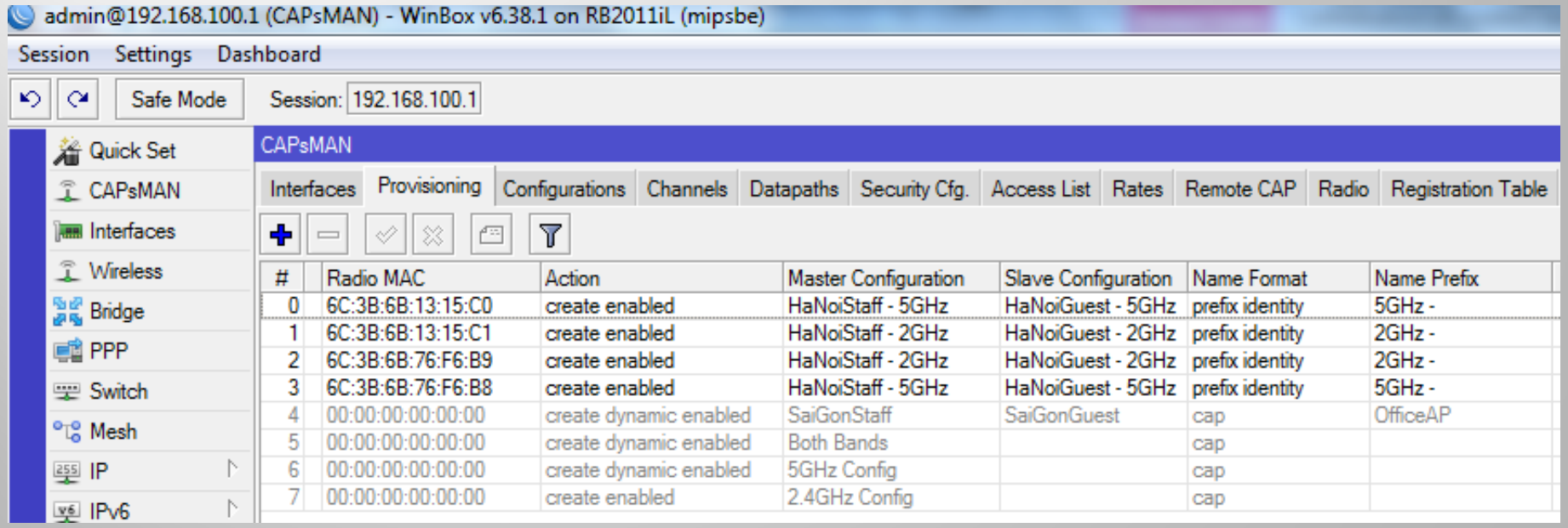
- Configuration profiles



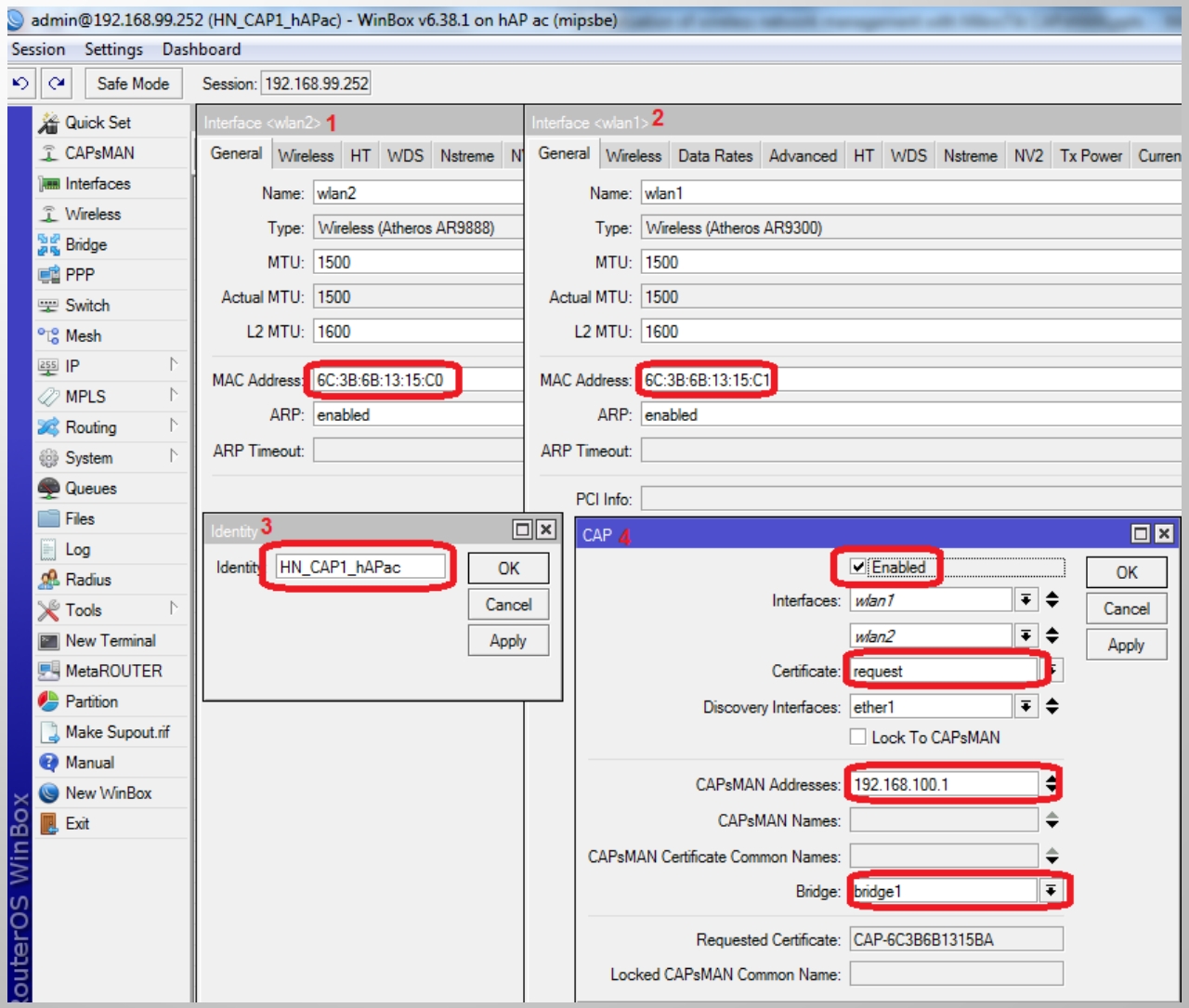
CAPsMAN Setup

APs provisioning

- **Provisioning** is the process of connecting a new **APs** to wireless network

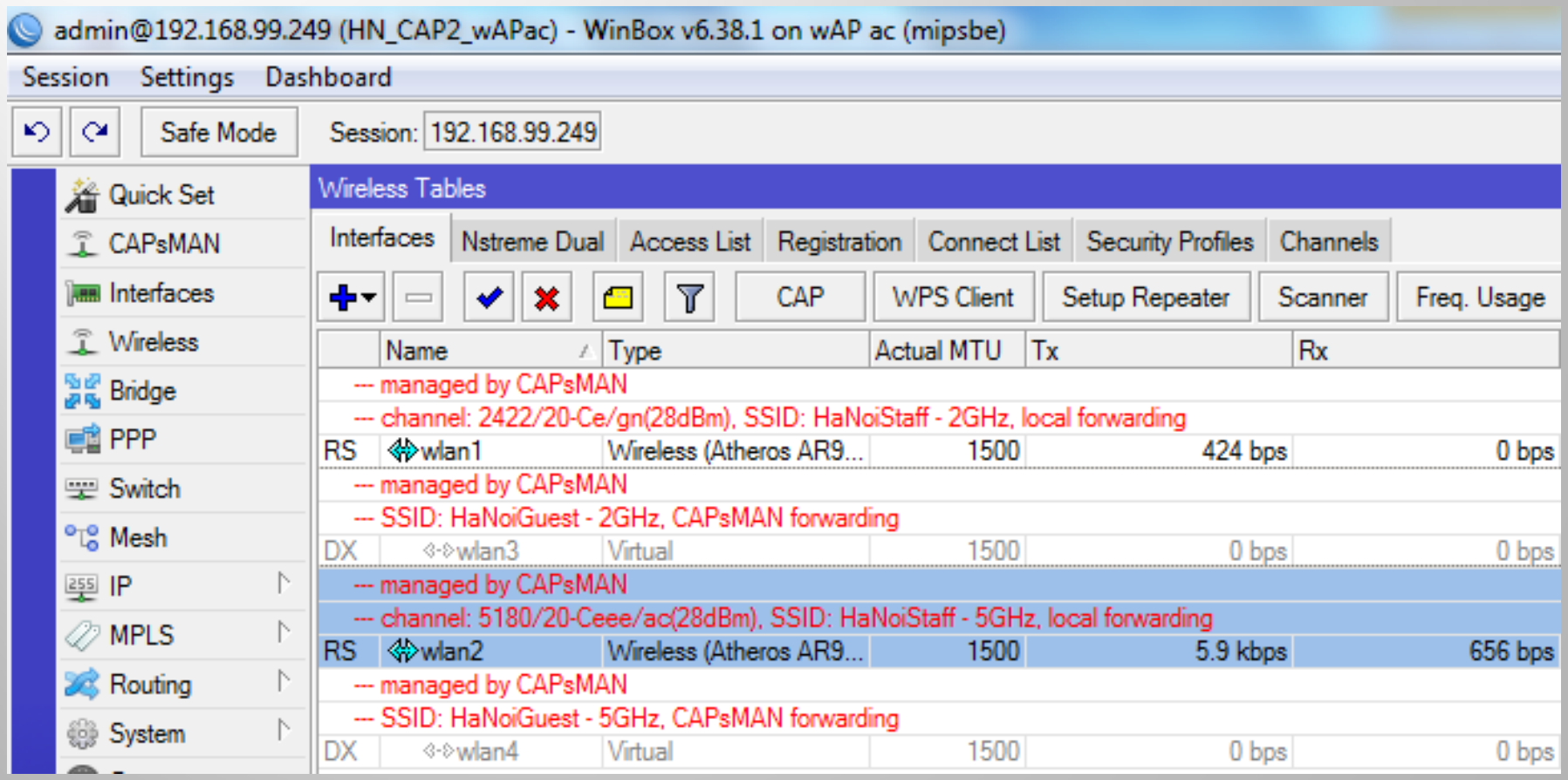


CAP setup


admin@192.168.99.252 (HN_CAP1_hAPac) - WinBox v6.38.1 on hAP ac (mipsbe)
Session Settings Dashboard
Safe Mode
Session: 192.168.99.252
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.rif
Manual
New WinBox
Exit
RouterOS WinBox
Interface <wlan2> 1
General Wireless HT WDS Nstreme
Name: wlan2
Type: Wireless (Atheros AR9888)
MTU: 1500
Actual MTU: 1500
L2 MTU: 1600
MAC Address: 6C:3B:6B:13:15:C0
ARP: enabled
ARP Timeout:
Interface <wlan1> 2
General Wireless Data Rates Advanced HT WDS Nstreme NV2 Tx Power
Name: wlan1
Type: Wireless (Atheros AR9300)
MTU: 1500
Actual MTU: 1500
L2 MTU: 1600
MAC Address: 6C:3B:6B:13:15:C1
ARP: enabled
ARP Timeout:
PCI Info:
Identity 3
Identity: HN_CAP1_hAPac
OK
Cancel
Apply
CAP 4
Enabled
Interfaces: wlan1
wlan2
Certificate: request
Discovery Interfaces: ether1
Lock To CAPsMAN
CAPsMAN Addresses: 192.168.100.1
CAPsMAN Names:
CAPsMAN Certificate Common Names:
Bridge: bridge1
Requested Certificate: CAP-6C3B6B1315BA
Locked CAPsMAN Common Name:
OK
Cancel
Apply

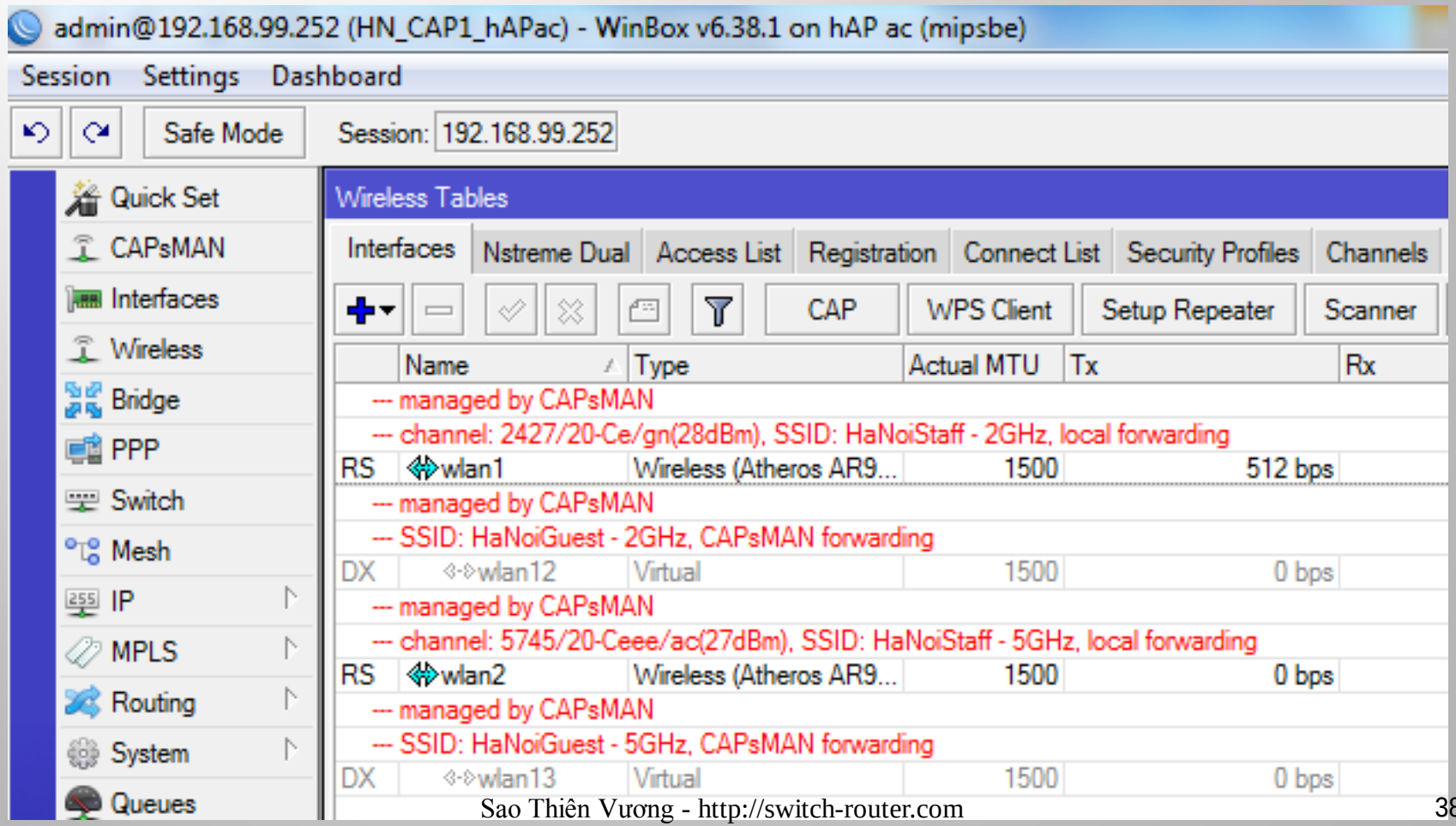
Result

CAP2


admin@192.168.99.249 (HN_CAP2_wAPac) - WinBox v6.38.1 on wAP ac (mipsbe)
Session Settings Dashboard
Safe Mode
Session: 192.168.99.249
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Wireless Tables
Interfaces
Nstreme Dual
Access List
Registration
Connect List
Security Profiles
Channels
CAP
WPS Client
Setup Repeater
Scanner
Freq. Usage
Name
Type
Actual MTU
Tx
Rx
--- managed by CAPsMAN
--- channel: 2422/20-Ce/gn(28dBm), SSID: HaNoiStaff - 2GHz, local forwarding
RS wlan1 Wireless (Atheros AR9... 1500 424 bps 0 bps
--- managed by CAPsMAN
--- SSID: HaNoiGuest - 2GHz, CAPsMAN forwarding
DX wlan3 Virtual 1500 0 bps 0 bps
--- managed by CAPsMAN
--- channel: 5180/20-Ceee/ac(28dBm), SSID: HaNoiStaff - 5GHz, local forwarding
RS wlan2 Wireless (Atheros AR9... 1500 5.9 kbps 656 bps
--- managed by CAPsMAN
--- SSID: HaNoiGuest - 5GHz, CAPsMAN forwarding
DX wlan4 Virtual 1500 0 bps 0 bps

Result

- CAP1


admin@192.168.99.252 (HN_CAP1_hAPac) - WinBox v6.38.1 on hAP ac (mipsbe)
Session
Settings
Dashboard
Safe Mode
Session: 192.168.99.252
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Wireless Tables
Interfaces
Nstreme Dual
Access List
Registration
Connect List
Security Profiles
Channels
CAP
WPS Client
Setup Repeater
Scanner
Name
Type
Actual MTU
Tx
Rx
--- managed by CAPsMAN
--- channel: 2427/20-Ce/gn(28dBm), SSID: HaNoiStaff - 2GHz, local forwarding
RS wlan1 Wireless (Atheros AR9... 1500 512 bps
--- managed by CAPsMAN
--- SSID: HaNoiGuest - 2GHz, CAPsMAN forwarding
DX wlan12 Virtual 1500 0 bps
--- managed by CAPsMAN
--- channel: 5745/20-Ceee/ac(27dBm), SSID: HaNoiStaff - 5GHz, local forwarding
RS wlan2 Wireless (Atheros AR9... 1500 0 bps
--- managed by CAPsMAN
--- SSID: HaNoiGuest - 5GHz, CAPsMAN forwarding
DX wlan13 Virtual 1500 0 bps

Result

- CAPsMAN – radio

CAPsMAN

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

Provision

	Radio MAC	Remote CAP Name	Remote CAP Identity	Interface
P	6C:3B:6B:13:15:C1	CAP-6C3B6B1315BA	HN_CAP1_hAPac	2GHz - -HN_CAP1_hAPac-1
P	6C:3B:6B:76:F6:B9	CAP-6C3B6B76F6B7	HN_CAP2_wAPac	*2GHz - -HN_CAP2_wAPac-1*
P	6C:3B:6B:13:15:C0	CAP-6C3B6B1315BA	HN_CAP1_hAPac	5GHz - -HN_CAP1_hAPac-1
P	6C:3B:6B:76:F6:B8	CAP-6C3B6B76F6B7	HN_CAP2_wAPac	*5GHz - -HN_CAP2_wAPac-1*

CAPsMAN – Remote CAP

CAPsMAN

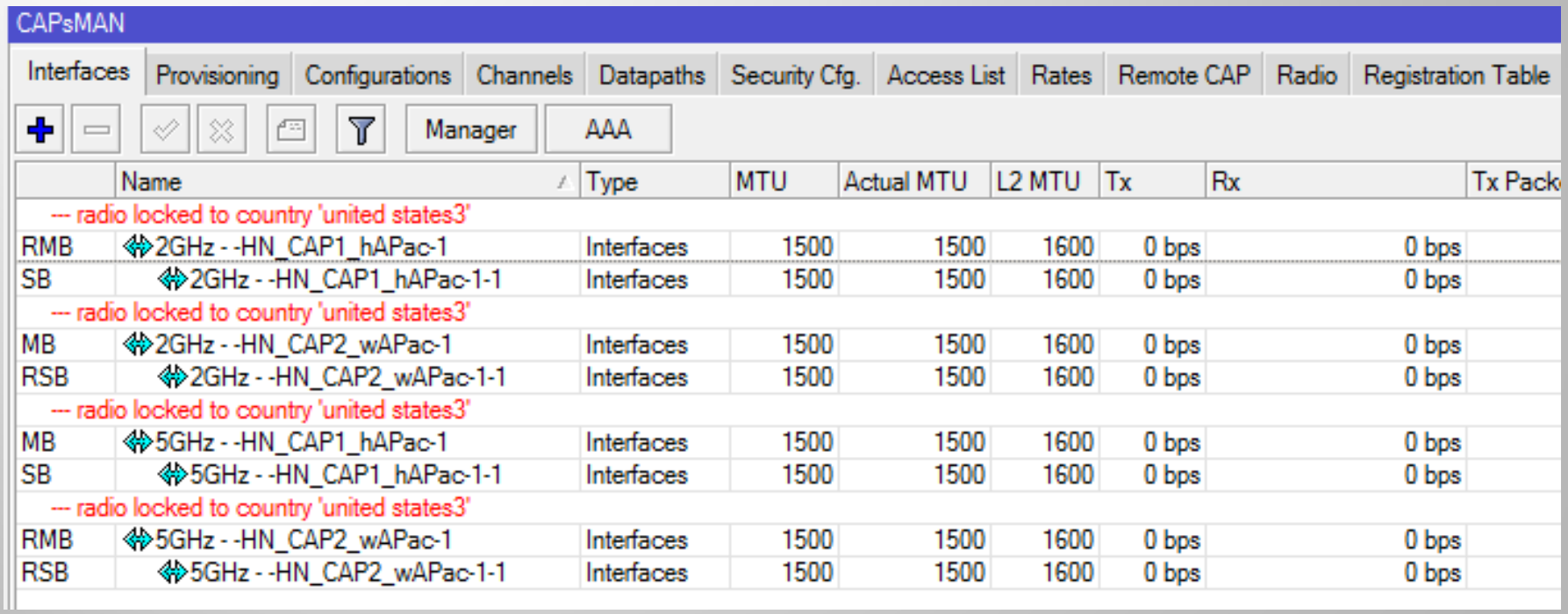
Interfaces | Provisioning | Configurations | Channels | Datapaths | Security Cfg. | Access List | Rates | Remote CAP | Radio | Registration Table

Provision | Upgrade | Set Identity

Address	Name	Board	Serial	Version	Identity	Base MAC	State	Radios
192.168.99.249	CAP-6C3B6B76F6B7	RBwAPG-5HacT2HnD	711E06609BF8	6.38.1	HN_CAP2_wAPac	6C:3B:6B:76:F6:B7	Run	2
192.168.99.252	CAP-6C3B6B1315BA	RB962UiGS-5HacT2HnT	67630668E90F	6.38.1	HN_CAP1_hAPac	6C:3B:6B:13:15:BA	Run	2

Result

- CAPsMAN – Interfaces



	Name	Type	MTU	Actual MTU	L2 MTU	Tx	Rx	Tx Pack
	--- radio locked to country 'united states3'							
RMB	2GHz - -HN_CAP1_hAPac-1	Interfaces	1500	1500	1600	0 bps	0 bps	
SB	2GHz - -HN_CAP1_hAPac-1-1	Interfaces	1500	1500	1600	0 bps	0 bps	
	--- radio locked to country 'united states3'							
MB	2GHz - -HN_CAP2_wAPac-1	Interfaces	1500	1500	1600	0 bps	0 bps	
RSB	2GHz - -HN_CAP2_wAPac-1-1	Interfaces	1500	1500	1600	0 bps	0 bps	
	--- radio locked to country 'united states3'							
MB	5GHz - -HN_CAP1_hAPac-1	Interfaces	1500	1500	1600	0 bps	0 bps	
SB	5GHz - -HN_CAP1_hAPac-1-1	Interfaces	1500	1500	1600	0 bps	0 bps	
	--- radio locked to country 'united states3'							
RMB	5GHz - -HN_CAP2_wAPac-1	Interfaces	1500	1500	1600	0 bps	0 bps	
RSB	5GHz - -HN_CAP2_wAPac-1-1	Interfaces	1500	1500	1600	0 bps	0 bps	

Result

- CAPsMAN – Registration Table

CAPsMAN

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

Interface	SSID	MAC Address	Tx Rate	Rx Rate	Tx Signal	Rx Signal	Uptime	Tx/Rx Packets	Tx/Rx Bytes
2GHz - -HN_CAP1_hAPac-1	HaNoiStaff - 2GHz	34:23:87:49:3A:C7	135Mbps-40MHz/1S	135Mbps-40MHz/1S	0	-57	00:17:24....	21 002/18 294	20.0 MiB/2744.9 ...
2GHz - -HN_CAP2_wAPac-1-1	HaNoiGuest - 2GHz	7C:61:93:10:DB:DE	11Mbps	1Mbps	0	-49	00:17:57....	10/257	1948 B/12.1 KiB
5GHz - -HN_CAP2_wAPac-1	HaNoiStaff - 5GHz	A0:04:60:2D:B0:0A	702Mbps-80MHz/2S	866.6Mbps-80MHz/2S/SGI	0	-38	00:19:40....	5 678/5 965	3553.3 KiB/627.9...

- DHCP – leases

DHCP Server

DHCP | Networks | Leases | Options | Option Sets | Alerts

Check Status

	Address	MAC Address	Client ID	Server	Active Address	Active MAC Addre...	Active Host Name
D	10.10.20.253	34:23:87:49:3A:C7	1:34:23:87:49:3a:c7	Staff_vlan20	10.10.20.253	34:23:87:49:3A:C7	mai-PC
D	10.10.20.254	A0:04:60:2D:B0:0A	1:a0:4:60:2d:b0:a	Staff_vlan20	10.10.20.254	A0:04:60:2D:B0:0A	T430
D	10.10.30.252	40:6F:2A:1F:B7:0F		Guest	10.10.30.252	40:6F:2A:1F:B7:0F	BLACKBERRY-Z10
D	10.10.30.253	7C:61:93:10:DB:DE		Guest	10.10.30.253	7C:61:93:10:DB:DE	Android_356299045134572

Additional configuration

- Enable Require Peer Certificate to prevent rouge APs associate with CAPsMAN
- Enable auto or manual Lock to CAPsMAN to prevent rouge CAPsMANs
- Firewall rules for Guest traffic only access Internet

Questions?

THANK YOU!