

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

The screenshot shows the WinBox interface for CAPsMAN configuration. The left sidebar contains a tree view with categories like Quick Set, CAPsMAN, Interfaces, Wireless, Bridge, PPP, Switch, Mesh, IP, IPv6, MPLS, Routing, System, Queues, Files, Log, Radius, Tools, New Terminal, MetaROUTER, and Partition. The main area is titled 'CAPsMAN' and has tabs for Interfaces, Provisioning, Configurations, Channels, Datapaths, Security Cfg., Access List, and Rates. The 'Interfaces' tab is active, showing a table of interfaces. A red arrow points to the 'Interfaces' tab. The table has columns for Name, Type, MTU, Actual MTU, L2 MTU, and Tx. Each row represents a DMB interface (cap13 to cap16) with a warning: '-- radio locked to country 'united states3''. The MTU for all interfaces is 1500, Actual MTU is 1500, and L2 MTU is 1600.

Name	Type	MTU	Actual MTU	L2 MTU	Tx
DMB cap13	Interfaces	1500	1500	1600	
DMB cap14	Interfaces	1500	1500	1600	
DMB cap15	Interfaces	1500	1500	1600	
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

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 Pack
	-- 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	

erOS WinBox

Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.tif
Manual

Sao Thiên Vương - <http://switch-router.com>

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

The screenshot shows a configuration window titled "CAP" with the following settings:

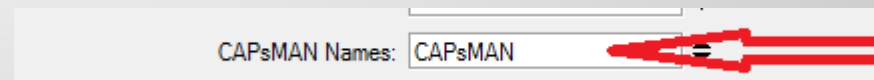
- Enabled
- Interfaces: *wlan1*, *wlan2*
- Certificate: *request*
- Discovery Interfaces: *ether1* (highlighted with a red box)
- Lock To CAPsMAN
- CAPsMAN Addresses: *192.168.100.1* (highlighted with a red box)
- CAPsMAN Names: *CAPsMAN*
- CAPsMAN Certificate Common Names: (empty)
- Bridge: *bridge1*
- Requested Certificate: *CAP-6C3B6B1315BA*
- Locked CAPsMAN Common Name: *CAPsMAN-6C3B6BA66E22*

Buttons: OK, Cancel, Apply

CAP to CAPsMAN Connection

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

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

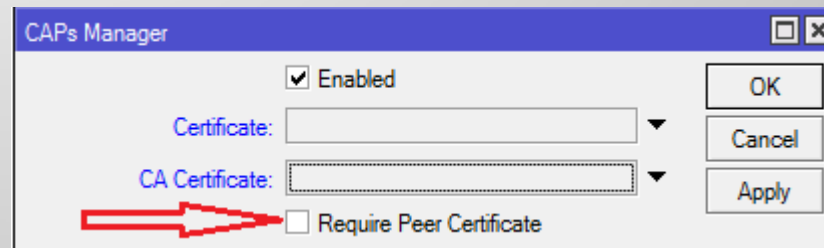


- ▣ Suitable manager with MAC layer connectivity is preferred to manager with IP connectivity

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

The screenshot shows the 'CAP' configuration window. The 'Enabled' checkbox is checked. The 'Interfaces' field contains 'wan1' and 'wan2'. The 'Certificate' field is set to 'none'. The 'Discovery Interfaces' field is set to 'ether1'. The 'Lock To CAPsMAN' checkbox is unchecked and highlighted with a red box, with a red '1' next to it. The 'CAPsMAN Addresses' field is set to '192.168.100.1'. The 'CAPsMAN Names' field is empty. The 'CAPsMAN Certificate Common Names' field is empty and highlighted with a red box, with a red '2' next to it. The 'Bridge' field is set to 'bridge1'. The 'Requested Certificate' and 'Locked CAPsMAN Common Name' fields are empty.

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

The screenshot shows the 'CAPs Manager' configuration window. The 'Enabled' checkbox is checked. The 'Certificate' and 'CA Certificate' dropdown menus are empty. The 'Require Peer Certificate' checkbox is unchecked. The 'Generated Certificate' and 'Generated CA Certificate' fields are empty. The 'Package Path' field is empty. The 'Upgrade Policy' dropdown is set to 'none'. Buttons for 'OK', 'Cancel', and 'Apply' are visible.

The screenshot shows the 'CAPs Manager' configuration window after configuration. The 'Enabled' checkbox is checked. The 'Certificate' and 'CA Certificate' dropdown menus are set to 'auto'. The 'Require Peer Certificate' checkbox is unchecked. The 'Generated Certificate' field contains 'CAPsMAN-6C3B6BA66E22'. The 'Generated CA Certificate' field contains 'CAPsMAN-CA-6C3B6BA66E22'. The 'Package Path' field is empty. The 'Upgrade Policy' dropdown is set to 'none'. Buttons for 'OK', 'Cancel', and 'Apply' are visible.

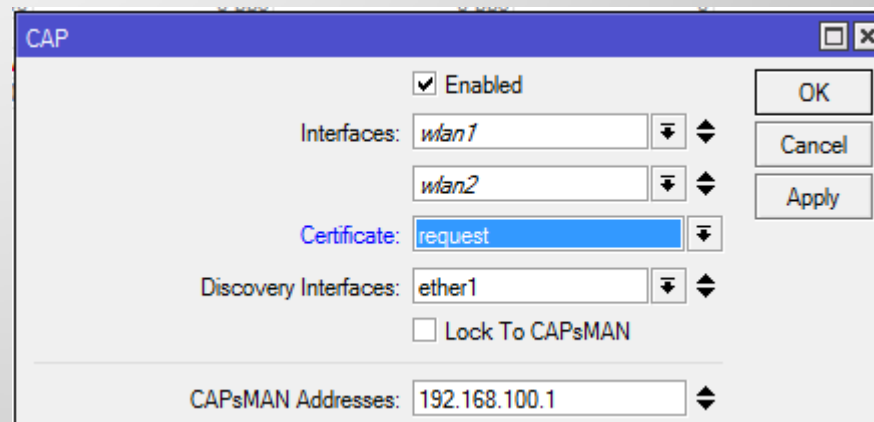
Feb/14/2017 11:20:13	memory	system, info	CAPsMAN configuration changed by admin
Feb/14/2017 11:20:20	memory	certificate, info	generated CA certificate: CAPsMAN-CA-6C3B6BA66E22
Feb/14/2017 11:20:21	memory	certificate, debug	trust store updated
Feb/14/2017 11:20:36	memory	certificate, info	generated certificate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

Sao Thien Vuong - <http://switch-router.com>

Auto Certificates

CAP Auto certificate configuration:

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



The screenshot shows a configuration window titled "CAP". It contains the following settings:

- Enabled
- Interfaces: *wlan1* (dropdown), *wlan2* (dropdown)
- Certificate: *request* (dropdown)
- Discovery Interfaces: *ether1* (dropdown)
- Lock To CAPsMAN
- CAPsMAN Addresses: *192.168.100.1* (dropdown)

Buttons: OK, Cancel, Apply

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

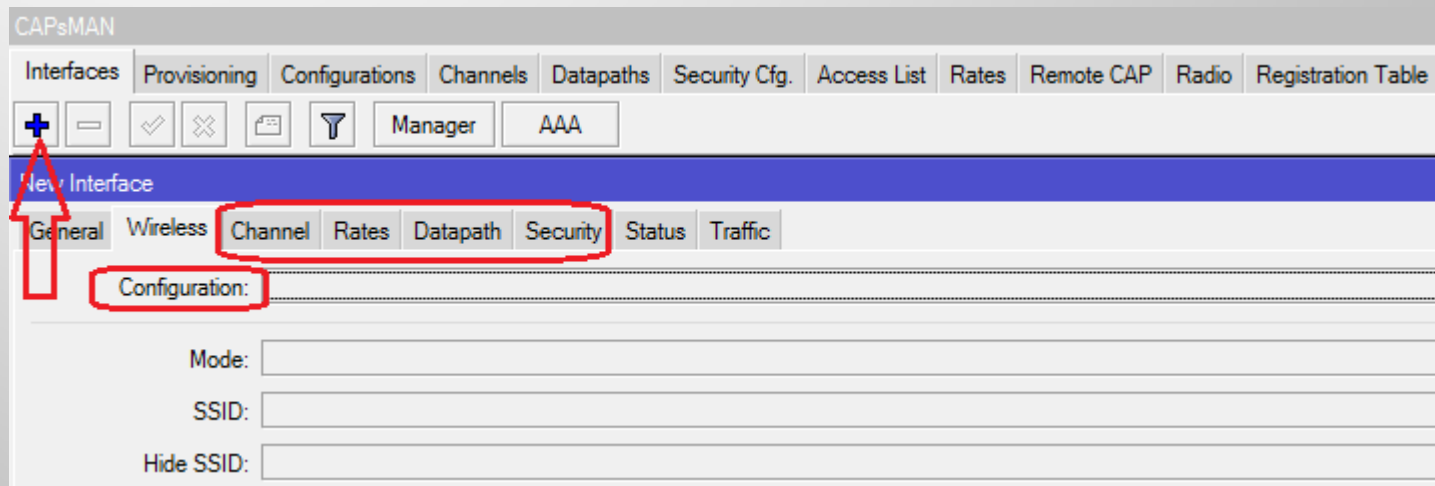
The screenshot displays the CAPsMAN configuration interface. The top window shows a list of virtual interfaces under the 'Interfaces' tab. Below it, the 'Interface List' window provides a detailed view of the system's interfaces.

Name	Type	MTU	Actual MTU	L2 MTU	Tx
--- radio locked to country 'united states3'					
MB cap1	Interfaces	1500	1500	1600	
--- radio locked to country 'united states3'					
MB cap2	Interfaces	1500	1500	1600	
--- radio locked to country 'united states3'					
MB cap3	Interfaces	1500	1500	1600	
--- radio locked to country 'united states3'					
MB cap4	Interfaces	1500	1500	1600	

Interface	Name	Type	Actual MTU	L2 MTU	Tx	Rx
R	OfficeNet	Bridge	1500	1598		0 bps
--- radio locked to country 'united states3'						
MB	cap1	Interfaces	1500	1600		0 bps
--- radio locked to country 'united states3'						
MB	cap2	Interfaces	1500	1600		0 bps
--- radio locked to country 'united states3'						
MB	cap3	Interfaces	1500	1600		0 bps
--- radio locked to country 'united states3'						
MB	cap4	Interfaces	1500	1600		0 bps
R	ether1	Ethernet	1500	1598		4.6 kbps
R	ether2	Ethernet	1500	1598		1312 bps
R	ether3	Ethernet	1500	1598		137.6 kbps

CAPsMAN Configuration

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



The screenshot displays the CAPsMAN configuration interface. At the top, there is a navigation bar with tabs for 'Interfaces', 'Provisioning', 'Configurations', 'Channels', 'Datapaths', 'Security Cfg.', 'Access List', 'Rates', 'Remote CAP', 'Radio', and 'Registration Table'. Below this, there is a toolbar with icons for adding (+), removing (-), saving (checkmark), deleting (X), and a filter icon, along with buttons for 'Manager' and 'AAA'. A red arrow points to the '+' icon. The main area shows a 'New Interface' dialog box with tabs for 'General', 'Wireless', 'Channel', 'Rates', 'Datapath', 'Security', 'Status', and 'Traffic'. The 'Channel' tab is selected and highlighted with a red box. Below the tabs, there is a 'Configuration:' label with a red box around it, followed by input fields for 'Mode:', 'SSID:', and 'Hide SSID:'.

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

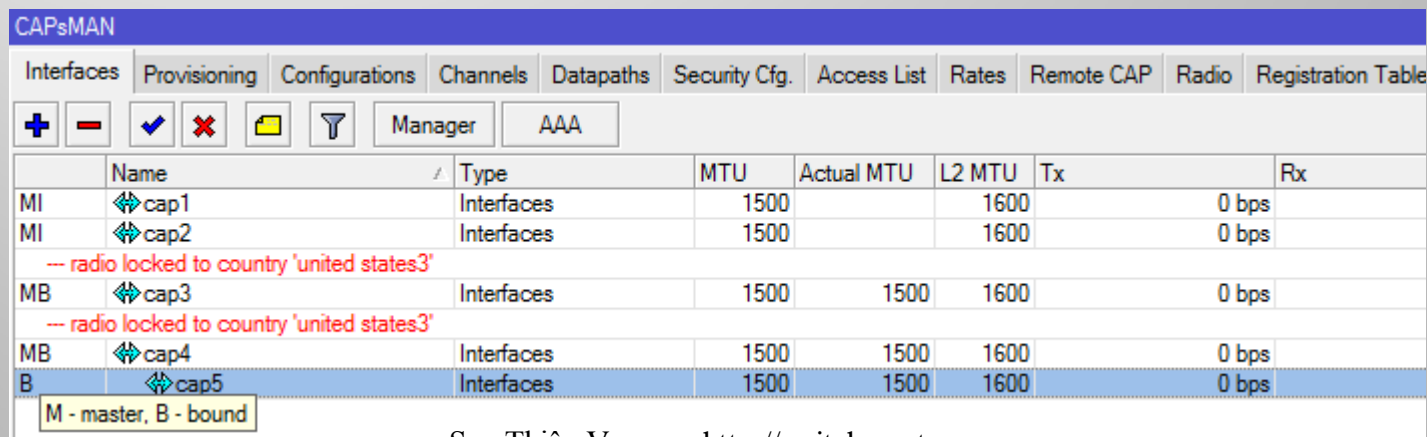
There are 2 types of interfaces:

- ❑ 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



The screenshot shows the CAPsMAN configuration interface with a table of interface configurations. The table has columns for Name, Type, MTU, Actual MTU, L2 MTU, Tx, and Rx. The interfaces are listed as follows:

Name	Type	MTU	Actual MTU	L2 MTU	Tx	Rx
MI cap1	Interfaces	1500		1600		0 bps
MI cap2	Interfaces	1500		1600		0 bps
-- radio locked to country 'united states3'						
MB cap3	Interfaces	1500	1500	1600		0 bps
-- radio locked to country 'united states3'						
MB cap4	Interfaces	1500	1500	1600		0 bps
B cap5	Interfaces	1500	1500	1600		0 bps

A legend at the bottom left indicates: M - master, B - bound.

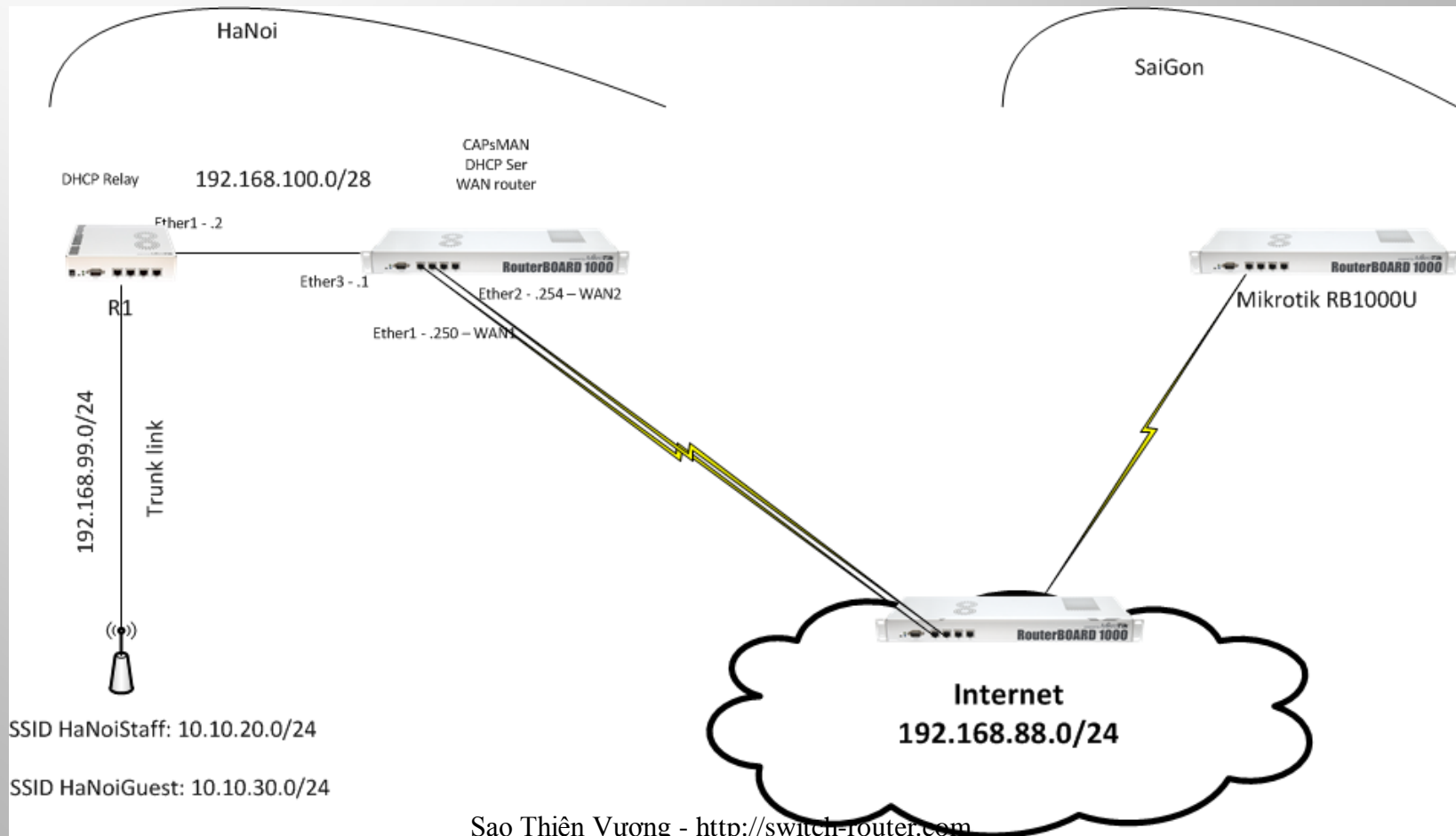
Interface Types

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:

Safe Mode Session: 192.168.100.1

Bridge

Name	Type	L2 MTU	Tx	Rx	Tx Pac
Guest	Bridge	1598	0 bps	0 bps	

IP Pool

Name	Addresses	Next Pool
Guest	10.10.30.10-10.10.30.254	none
Staff_VLAN20	10.10.20.10-10.10.20.254	none

Address List

Address	Network	Interface
10.10.30.1/24	10.10.30.0	Guest
D 192.168.88.250/24	192.168.88.0	ether2
D 192.168.88.254/24	192.168.88.0	ether1
D 192.168.100.1/28	192.168.100.0	ether3

DHCP Server

Name	Interface	Relay	Lease Time	Address Pool	Add ARP For Leases
Guest	Guest		00:10:00	Guest	no
Staff_vlan20	ether3	10.10.20.1	00:10:00	Staff_VLAN20	no

Deployment

▣ R1 router

Session Settings Dashboard

Safe Mode Session: 192.168.99.1

Quick Set
Interfaces
Bridge
PPP
Switch
Mesh
IP
MPLS
Routing
System
Queues
Files
Log
Radius
Tools

Bridge

Bridge Ports Filters NAT Hosts

+ - ✓ ✗ Settings Find

	Name	Type	L2 MTU	Tx	Rx
R	↕↕BridgeVLAN20	Bridge	1594	0 bps	
R	↕↕bridge1	Bridge	1598	263.6 kbps	

Address List

+ - ✓ ✗ Find

Address	Network	Interface
↕ 10.10.20.1/24	10.10.20.0	BridgeVLAN20
↕ 192.168.99.1/24	192.168.99.0	bridge1
↕ 192.168.100.2/28	192.168.100.0	ether1

DHCP Relay

+ - ✓ ✗ Reset Counters Find

Name	Interface	DHCP Server	Local Address
relay_VLAN20	BridgeVLAN20	192.168.100.1	10.10.20.1

Deployment

- ▣ R1 router – trunking ports

The screenshot displays a network configuration interface with a sidebar on the left and a main content area. The sidebar includes options like Quick Set, Interfaces, Bridge, PPP, Switch, Mesh, IP, MPLS, Routing, System, Queues, Files, Log, Radius, and Tools. The main content area is divided into two sections: 'Interface List' and 'Bridge'.

Interface List

Interface	Name	Type	MTU	L2 MTU	VLAN ID	Interface
RS	ether9-vlan20	VLAN	1500	1594	20	ether9
RS	ether10-vlan20	VLAN	1500	1594	20	ether10

Bridge

Interface	Bridge	Priority (h...)	Path Cost	Horizon	Role
ether10	bridge1	80	10		designated port
ether10-vlan20	BridgeVLAN20	80	10		designated port
ether6	bridge1	80	10		designated port
ether7	bridge1	80	10		disabled port
ether8	bridge1	80	10		disabled port
ether9	bridge1	80	10		designated port
ether9-vlan20	BridgeVLAN20	80	10		designated port

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

The screenshot displays the CAPsMAN configuration interface. The main window has tabs for Channels, Datapaths, Security Cfg., Access List, Rates, Remote CAP, Radio, and Registration Table. Below the tabs are icons for adding, deleting, saving, and filtering, along with a search field labeled 'Find'. A table lists the security profiles:

Name	Authentication Type	Encryption	Group Encryption	Passphrase	EAP Methods
HaNoiGuest	WPA PSK WPA2 PSK	aes ccm	aes ccm	HaNoiGuest	
HaNoiStaff	WPA PSK WPA2 PSK	aes ccm	aes ccm	HaNoiStaff	
SaiGonGuest	WPA PSK WPA2 PSK	aes ccm	aes ccm	SaiGonGuest	
SaiGonStaff	WPA PSK WPA2 PSK	aes ccm	aes ccm	SaiGonStaff	

A secondary window titled 'CAPs Security Configuration <HaNoiGuest>' is open, showing the configuration for the selected profile:

- Name: HaNoiGuest
- Authentication Type: WPA PSK WPA2 PSK WPA EAP WPA2 EAP
- Encryption: aes ccm tkip
- Group Encryption: aes ccm
- Passphrase: HaNoiGuest
- EAP Methods: (empty)
- EAP Radius Accounting: (empty)
- TLS Mode: (empty)
- TLS Certificate: (empty)

Buttons on the right side of the configuration dialog include OK, Cancel, Apply, Comment, Copy, and Remove.

CAPsMAN Setup

▣ Datapath profiles

The screenshot displays the CAPsMAN web interface. At the top, there are tabs for Provisioning, Configurations, Channels, Datapaths, Security Cfg., Access List, Rates, Remote CAP, Radio, and Registration Table. The 'Datapaths' tab is active, showing a table of profiles:

Name	Bridge	Local Forwarding	Client To Client Forwarding	VLAN Mode	VLAN ID
Guest	Guest	no	yes		
Staff		yes	yes	use tag	20

Below the table, two configuration windows are open:

- CAPs Datapath Configuration <Guest>**:
 - Name: Guest
 - MTU: []
 - L2 MTU: []
 - ARP: []
 - Bridge: Guest
 - Bridge Cost: []
 - Bridge Horizon: []
 - Local Forwarding:
 - Client To Client Forwarding:
 - VLAN Mode: []
 - VLAN ID: []
- CAPs Datapath Configuration <Staff>**:
 - Name: Staff
 - MTU: []
 - L2 MTU: []
 - ARP: []
 - Bridge: []
 - Bridge Cost: []
 - Bridge Horizon: []
 - Local Forwarding:
 - Client To Client Forwarding:
 - VLAN Mode: use tag
 - VLAN ID: 20

CAPsMAN Setup

- ▣ Configuration profiles

The screenshot shows the CAPsMAN web interface with the 'Configurations' tab selected. The table below lists the configuration profiles. Four profiles are selected, indicated by blue highlighting.

Name	SSID	Country	Channel	Band	Datapath	VLAN Mode	VLAN ID	Security
2.4GHz Config				2ghz-onlyn				
5GHz Config				5ghz-onlyac				
Both Bands				5ghz-a/n/ac				
HaNoiGuest - 2GHz	HaNoiGuest - 2GHz				Guest			HaNoiGuest
HaNoiGuest - 5GHz	HaNoiGuest - 5GHz				Guest			HaNoiGuest
HaNoiStaff - 2GHz	HaNoiStaff - 2GHz				Staff			HaNoiStaff
HaNoiStaff - 5GHz	HaNoiStaff - 5GHz				Staff			HaNoiStaff
SaiGonGuest	SaiGonGuest	viet nam			Guest			SaiGonGuest
SaiGonStaff	SaiGonStaff	viet nam			Staff			SaiGonStaff

9 items (4 selected)

CAPsMAN Setup

APs provisioning

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

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

CAPsMAN

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

#	Radio MAC	Action	Master Configuration	Slave Configuration	Name Format	Name Prefix
0	6C:3B:6B:13:15:C0	create enabled	HaNoiStaff - 5GHz	HaNoiGuest - 5GHz	prefix identity	5GHz -
1	6C:3B:6B:13:15:C1	create enabled	HaNoiStaff - 2GHz	HaNoiGuest - 2GHz	prefix identity	2GHz -
2	6C:3B:6B:76:F6:B9	create enabled	HaNoiStaff - 2GHz	HaNoiGuest - 2GHz	prefix identity	2GHz -
3	6C:3B:6B:76:F6:B8	create enabled	HaNoiStaff - 5GHz	HaNoiGuest - 5GHz	prefix identity	5GHz -
4	00:00:00:00:00:00	create dynamic enabled	SaiGonStaff	SaiGonGuest	cap	OfficeAP
5	00:00:00:00:00:00	create dynamic enabled	Both Bands		cap	
6	00:00:00:00:00:00	create dynamic enabled	5GHz Config		cap	
7	00:00:00:00:00:00	create enabled	2.4GHz Config		cap	

CAP setup

The screenshot displays the WinBox configuration interface for a MikroTik device. The main window shows the configuration for two wireless interfaces, wlan2 and wlan1. The left sidebar contains a navigation menu with options like 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, and Exit.

Interface <wlan2> 1 Configuration:

- General tab selected
- 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: (empty)

Interface <wlan1> 2 Configuration:

- General tab selected
- 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: (empty)
- PCI Info: (empty)

Identity 3 Configuration:

- Identity: HN_CAP1_hAPac

CAP 4 Configuration:

- Enabled:
- Interfaces: wlan1, wlan2
- Certificate: request
- Discovery Interfaces: ether1
- Lock To CAPsMAN:
- CAPsMAN Addresses: 192.168.100.1
- CAPsMAN Names: (empty)
- CAPsMAN Certificate Common Names: (empty)
- Bridge: bridge1
- Requested Certificate: CAP-6C3B6B1315BA
- Locked CAPsMAN Common Name: (empty)

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

+ - ✓ ✗ [icon] [icon] 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

CAPsMAN								
Interfaces								
Provisioning								
Configurations								
Channels								
Datapaths								
Security Cfg.								
Access List								
Rates								
Remote CAP								
Radio								
Registration Table								
+ - ✓ ✗ ☰ ☷ Manager AAA								
	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/SGL	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

+ - ✓ ✗ [icon] [icon] Check Status

	Address	MAC Address	Client ID	Server	Active Address	Active MAC Address	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!