CAPsMAN Features

MUM Istanbul-Turkey

May 2014

Mani Raissdana

M.IT.S Co. (www.mits-co.com)

Mani Raissdana

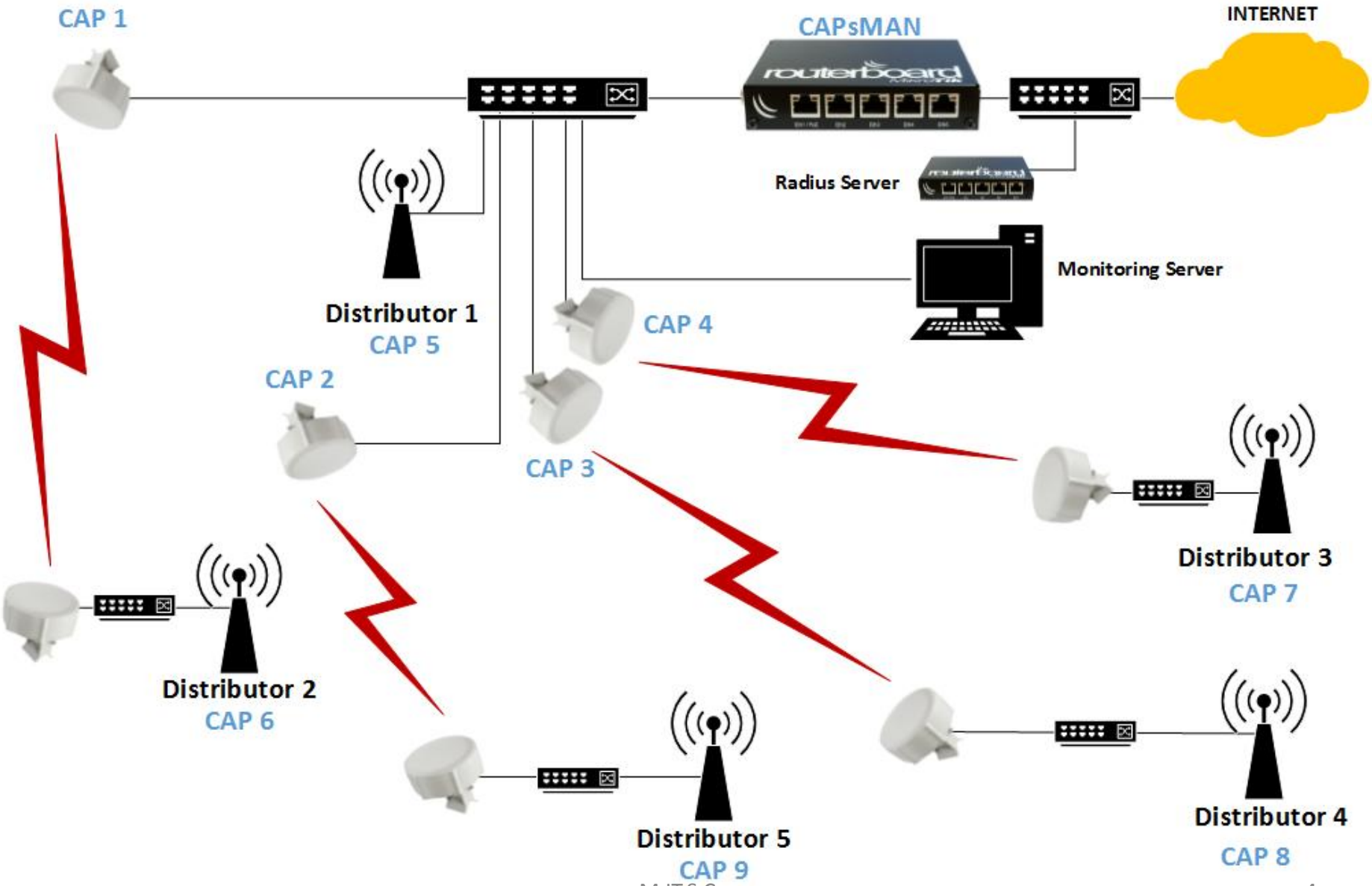
- MikroTik Certified Trainer (since 2011)
- M.IT.S Co CTO (MikroTik Sales & Training Partner)
- Own a WISP (MikroTik Wireless Platform)

CAPsMAN Features

Topics

- CAPsMAN Overview
- CAP to CAPsMAN Connection
- Auto Certificate
- CAP & CAPsMAN Configuration
- Interface Types
- Radio Provisioning
- Datapath Configuration
- Access List
- Registration Table

CAP to CAPsMAN Network Diagram



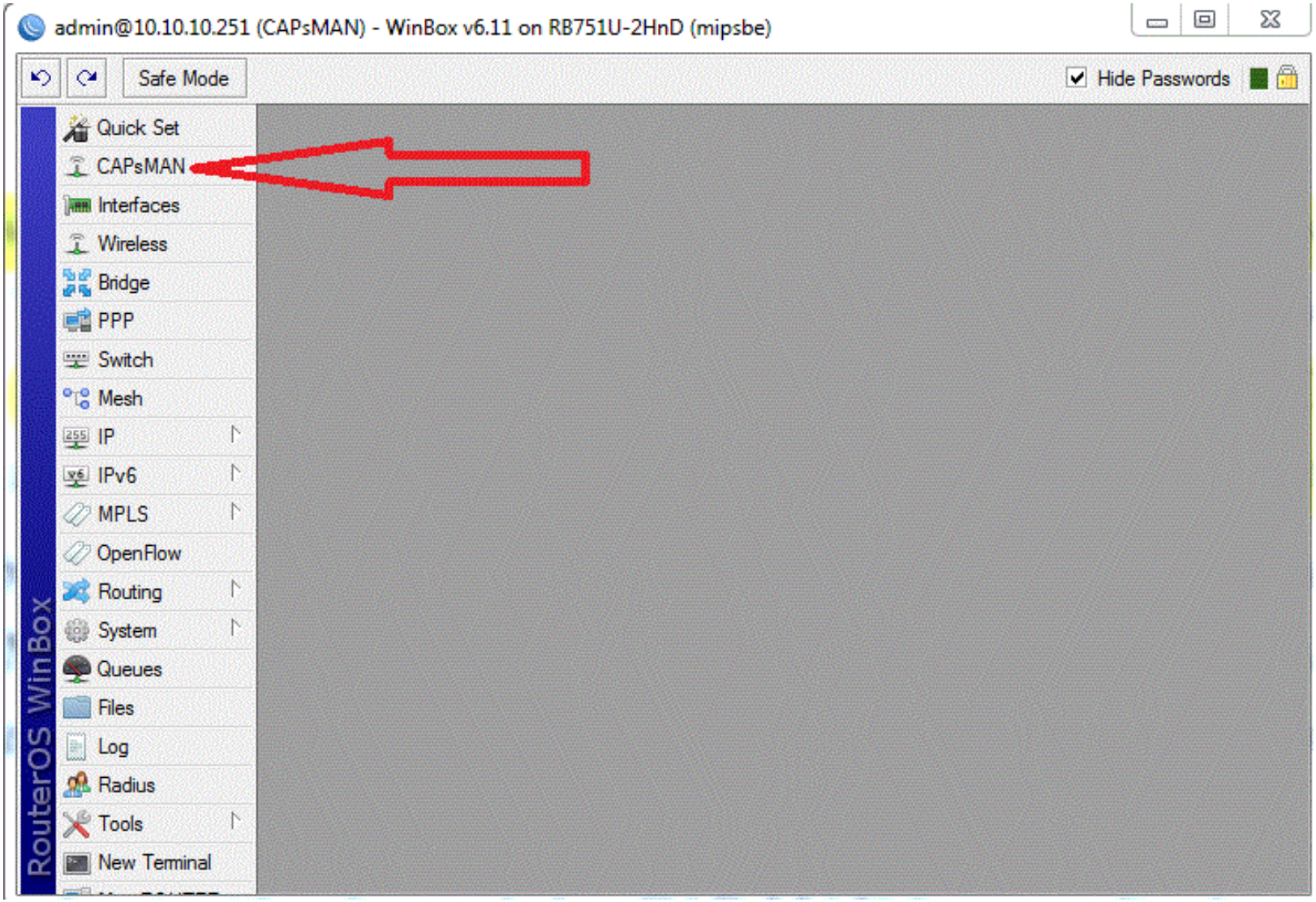
Overview

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 RouterOS Device from Version 6.11

Overview

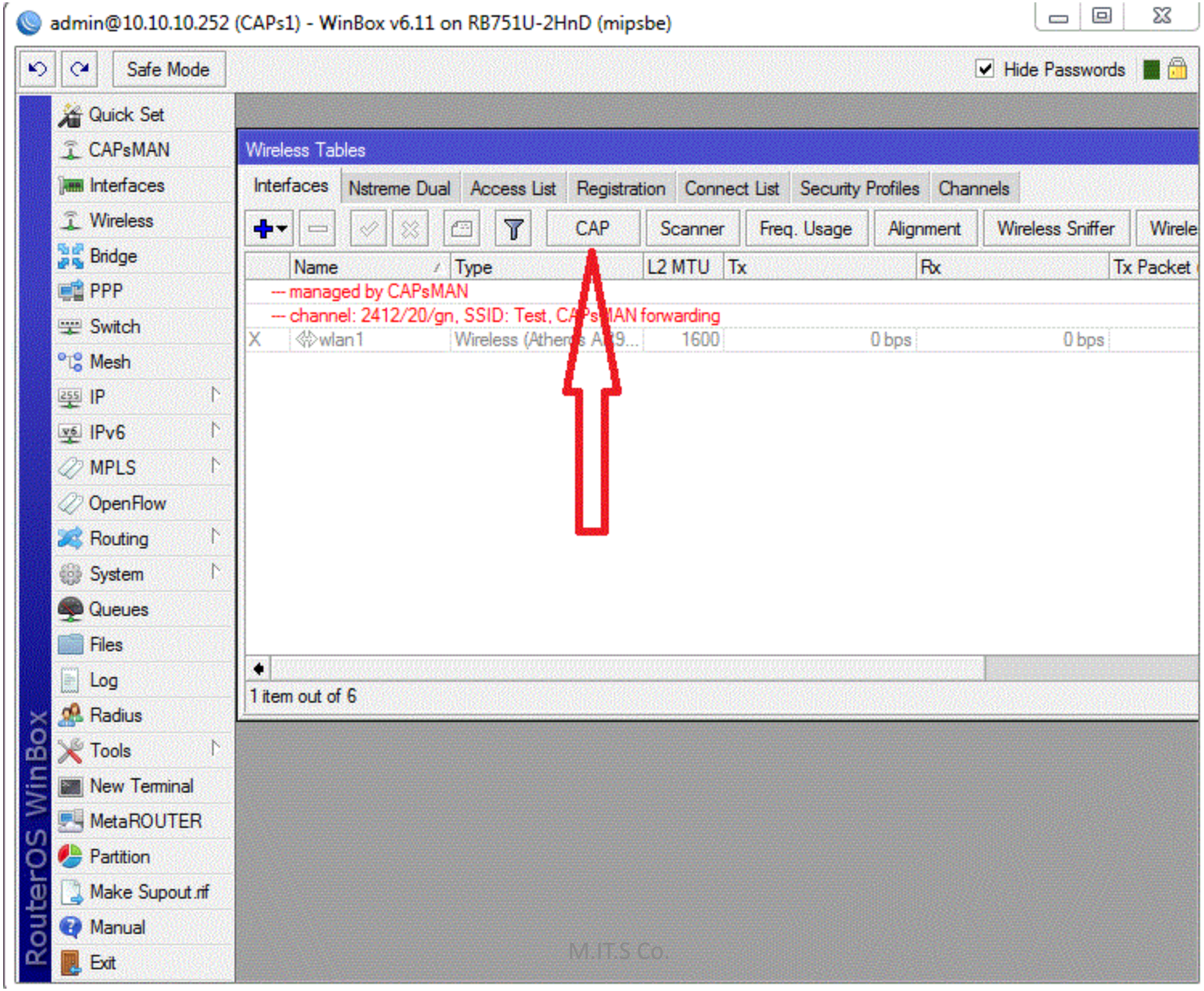

admin@10.10.10.251 (CAPsMAN) - WinBox v6.11 on RB751U-2HnD (mipsbe)
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
IPv6
MPLS
OpenFlow
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
RouterOS WinBox

Overview

CAP (Controlled Access Point)

- Provide wireless connectivity
- Wireless link layer encryption/decryption

Overview


admin@10.10.10.252 (CAPs1) - WinBox v6.11 on RB751U-2HnD (mipsbe)
Safe Mode
Hide Passwords
Quick Set
CAPsMAN
Interfaces
Wireless
Bridge
PPP
Switch
Mesh
IP
IPv6
MPLS
OpenFlow
Routing
System
Queues
Files
Log
Radius
Tools
New Terminal
MetaROUTER
Partition
Make Supout.rif
Manual
Exit
RouterOS WinBox
Wireless Tables
Interfaces
Nstreme Dual
Access List
Registration
Connect List
Security Profiles
Channels
CAP
Scanner
Freq. Usage
Alignment
Wireless Sniffer
Name
Type
L2 MTU
Tx
Rx
Tx Packet
managed by CAPsMAN
channel: 2412/20/gn, SSID: Test, CAPsMAN forwarding
X
wlan1
Wireless (Atheros AR9...
1600
0 bps
0 bps
1 item out of 6

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
- They must be reachable using IP protocol
- If they are not on the same L2 segment, CAP must be provisioned with the CAPsMAN's IP

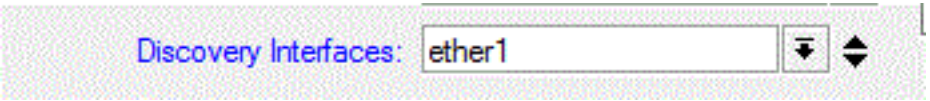
(Because IP multicast based discovery does not work over L3)

CAP to CAPsMAN Connection

After Discovery process, CAP attempt to contact CAPsMAN using:

- Configured list of manager IP address

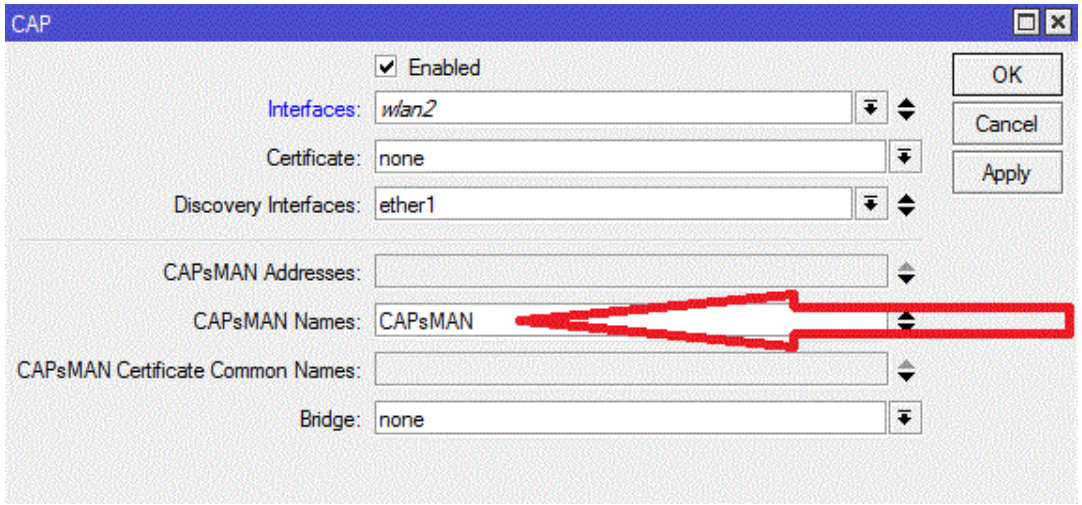
- List of CAPsMAN IPs obtained from DHCP server
- Broadcasting on configured interface using both IP and MAC layer protocols



CAP to CAPsMAN Connection

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

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



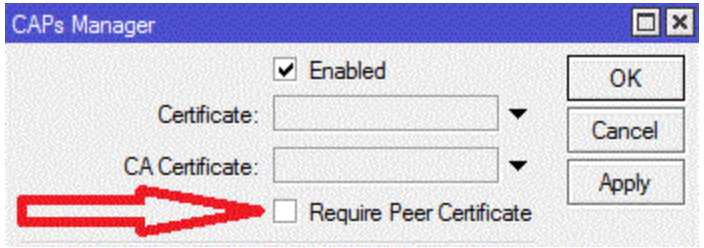
- Suitable manager with MAC layer connectivity is preferred to manager with IP connectivity

CAP to CAPsMAN Connection

Possible authentication mode to establish DTLS:

- No certificate on CAP & CAPsMAN (no Authentication)
- Certification configuration only on CAPsMAN

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



- Certificate configured on both (mutual authentication)

  (**caps-man-certificate-common-names** must specified on CAP)

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

CAP to CAPsMAN Connection

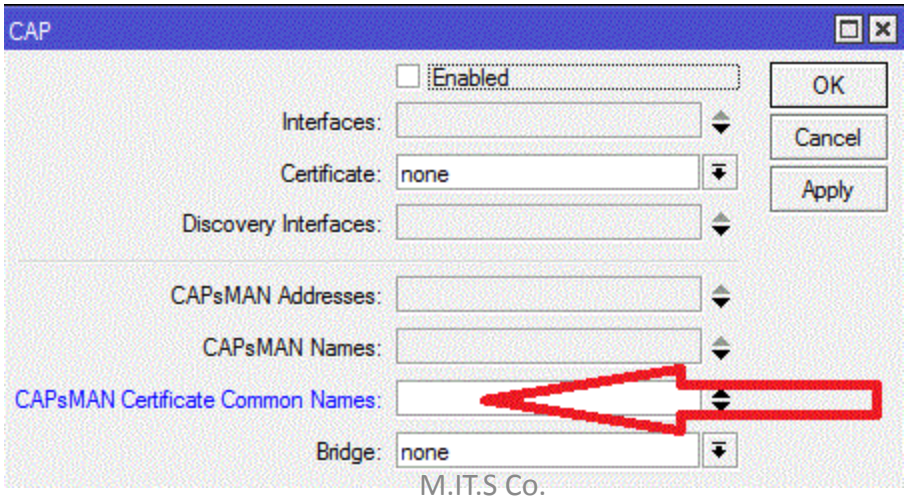
CAP Auto locking to CAPsMAN:

- CAP can be configured to automatically lock to CAPsMAN

```
[admin@CAP] > /interface wireless cap set lock-to-caps-man=yes
```

(Use of certificate is mandatory for locking to work)

- CAP can be manually locked to CAPsMAN by:



Auto Certificate

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

- Automatic certification do not provide full public key infrastructure
- Manual certification distribution or SCEP must be used

Auto Certificate

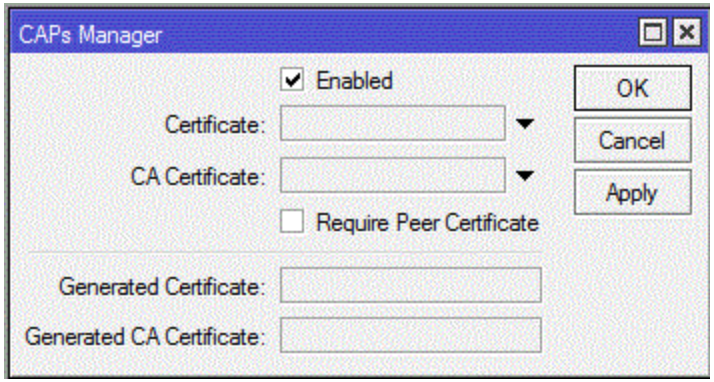
CAPsMAN Auto certificate configuration:

- **Certificate:**

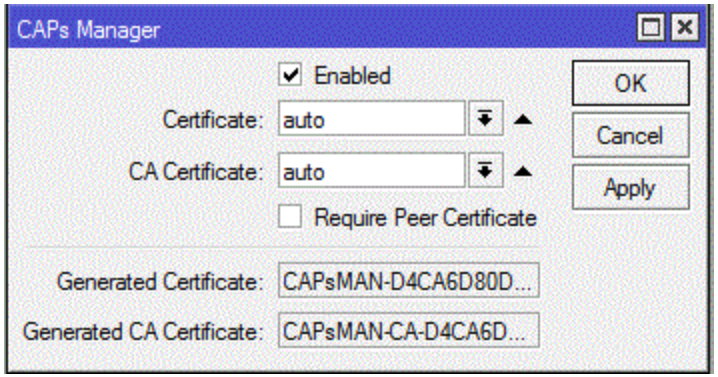
1. **If set to none:** Manager will operate in no-certificate mode
2. **If set to Auto:** Manager will attempt to issue certificate to itself

- **CA Certificate:**

1. **If set to none:** will not be able to issue certificate to itself
2. **If set to Auto:** Manager will generate self-signed CA certificate



1



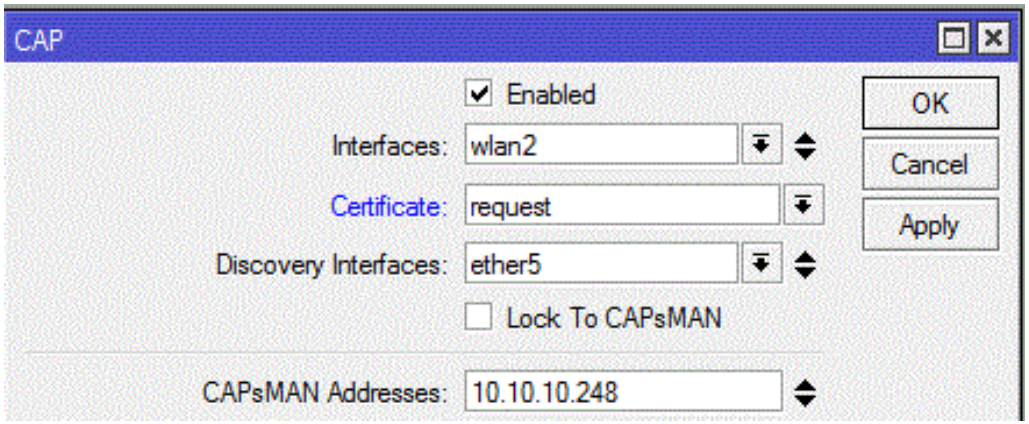
2

Auto Certificate

CAP Auto certificate configuration:

- CAP must be configured to request certificate

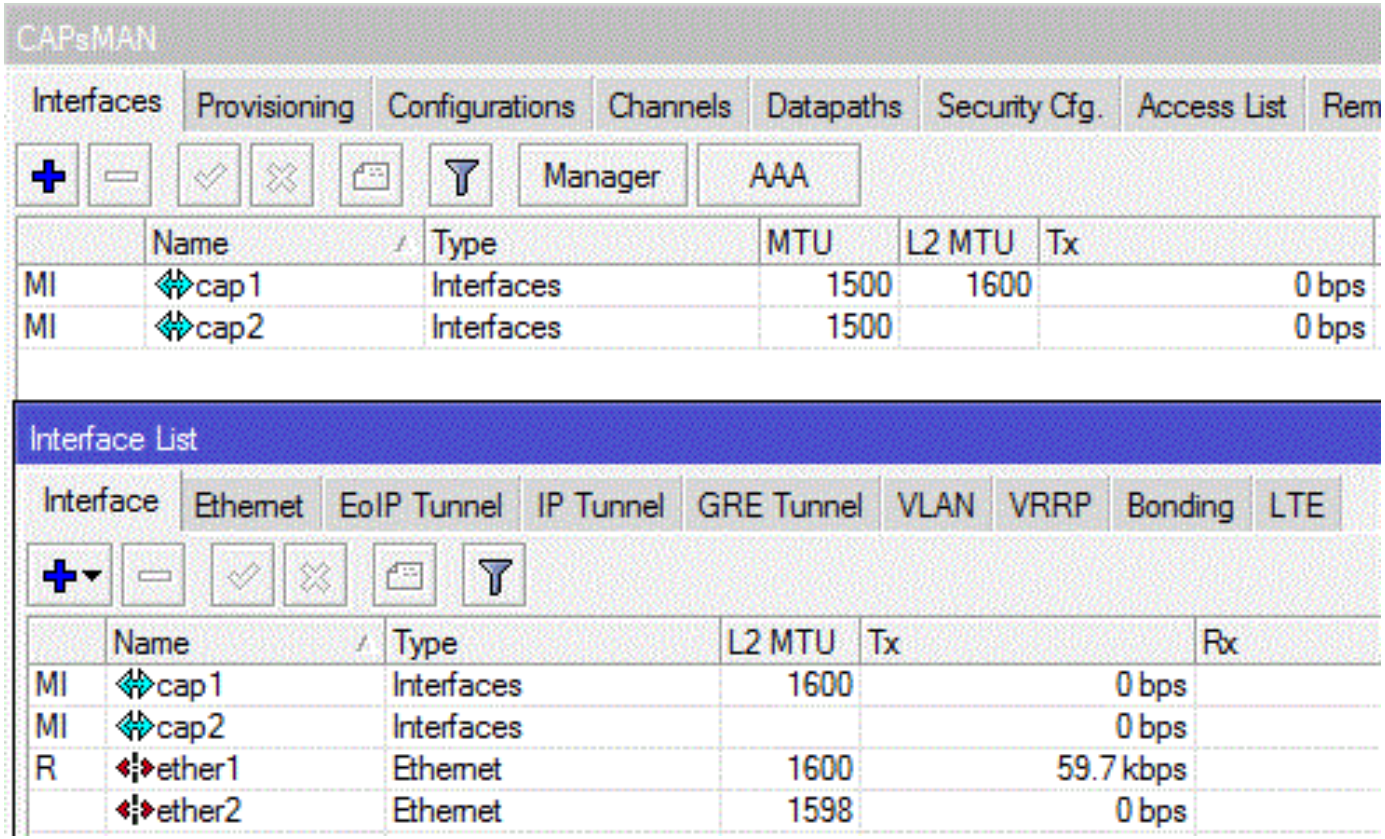
```
[admin@CAPs1] /interface wireless cap> set certificate=request
```



- 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

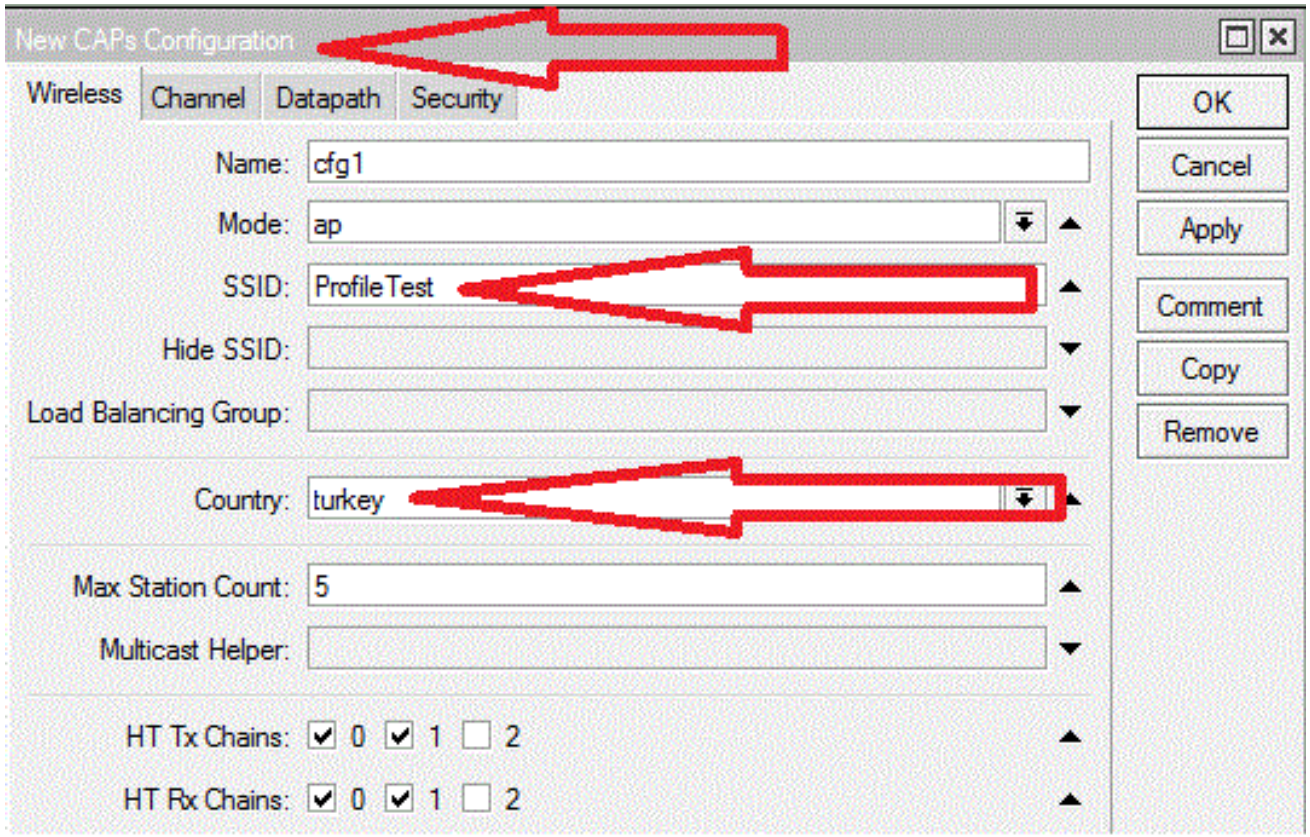
CAP & CAPsMAN Configuration

- CAP's Interfaces, under Manager's Control, appears as a virtual interface on the CAPsMAN



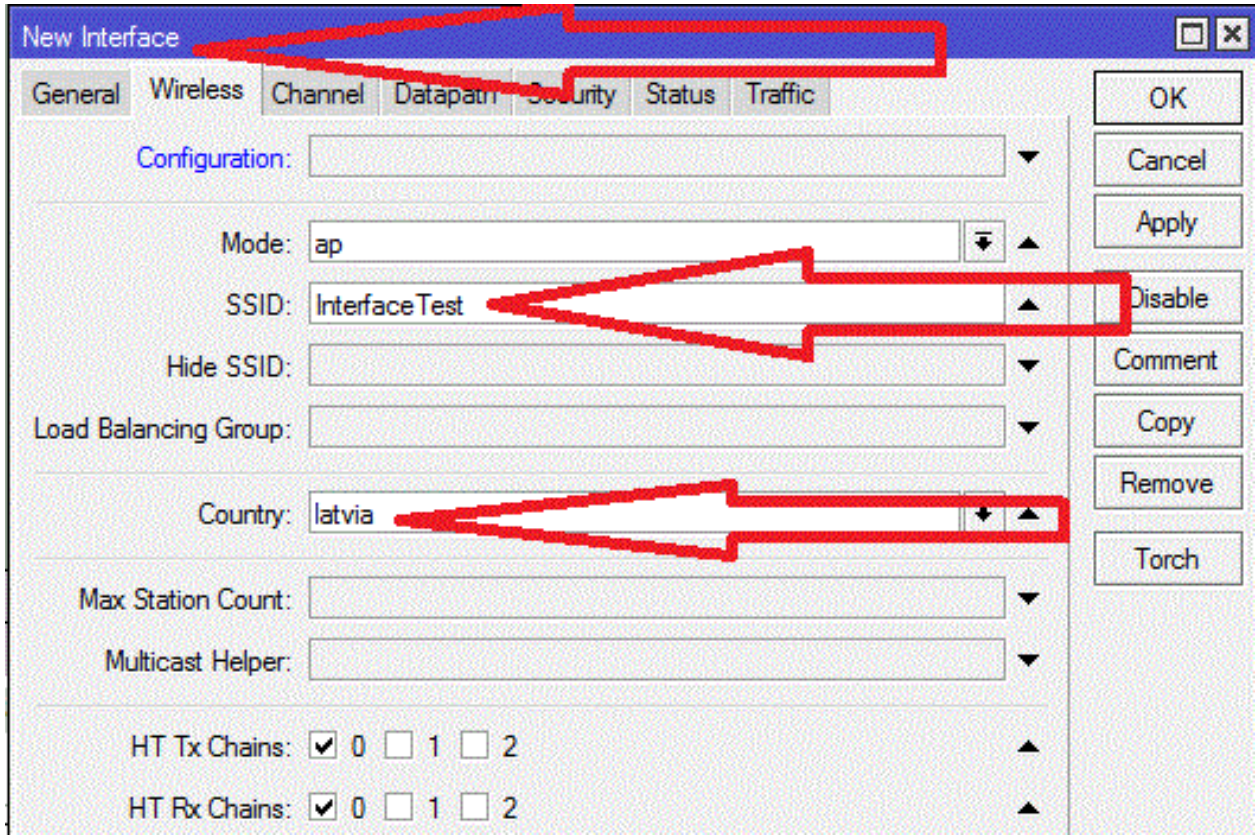
CAP & CAPsMAN Configuration

- Wireless interface settings can be grouped together as “Profile”
- Simply can reuse configuration on other CAP’s interfaces



CAP & CAPsMAN Configuration

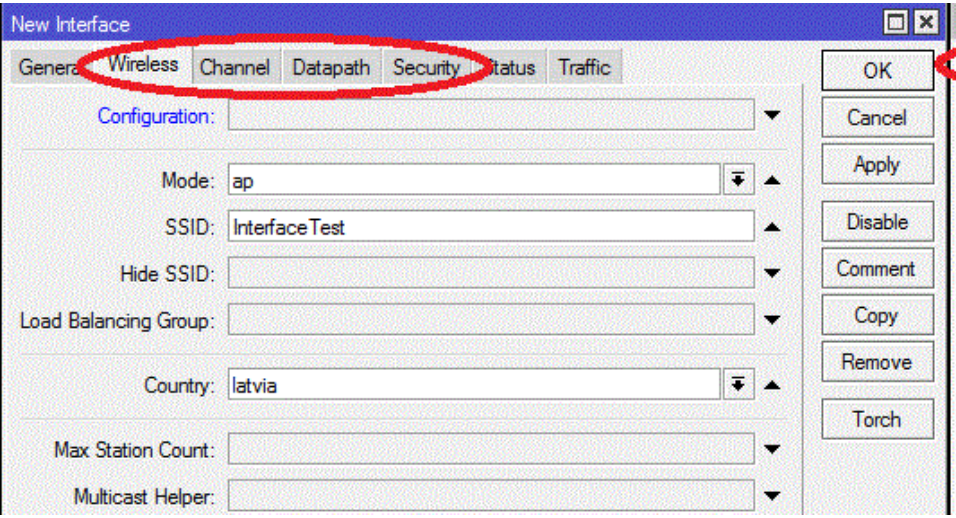
- Any profile settings can be overridden directly in an interface configuration for maximum flexibility

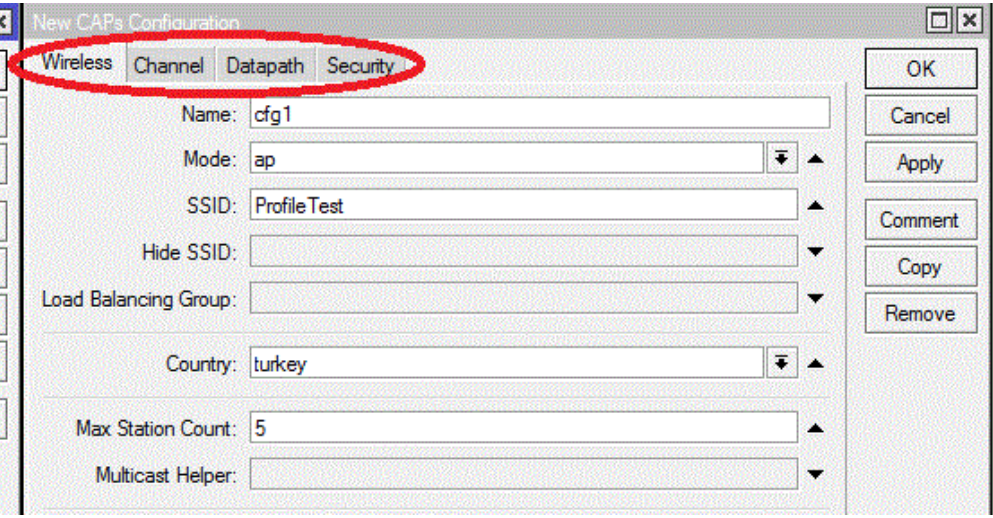


CAP & CAPsMAN Configuration

Interface Settings and Profiles:

- **Wireless:** main wireless settings group, such as SSID etc…
- **Channel:** Channel related settings such as frequency and width
- **Datapath:** Data forwarding related settings
- **Security:** Security related settings, such as allowed authentication types or passphrase





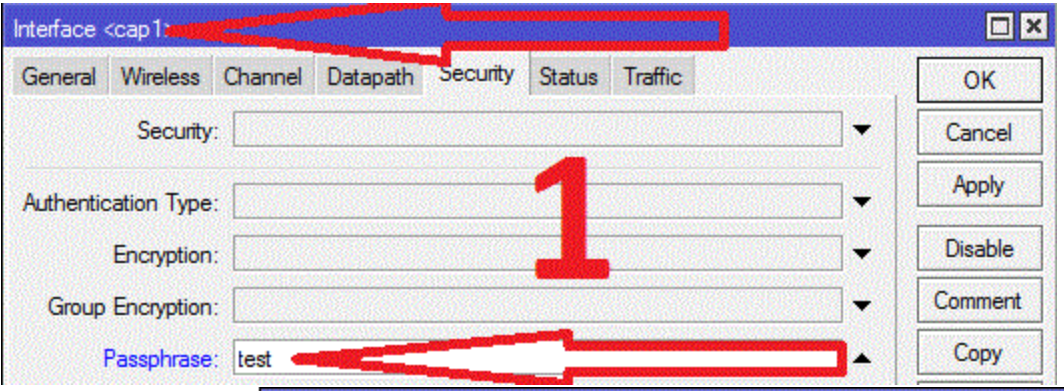
CAP & CAPsMAN Configuration

Interface Settings and Profiles:

- Configuration is organized in hierarchical structure with interface
- Higher level setting value overrides a lower level Value

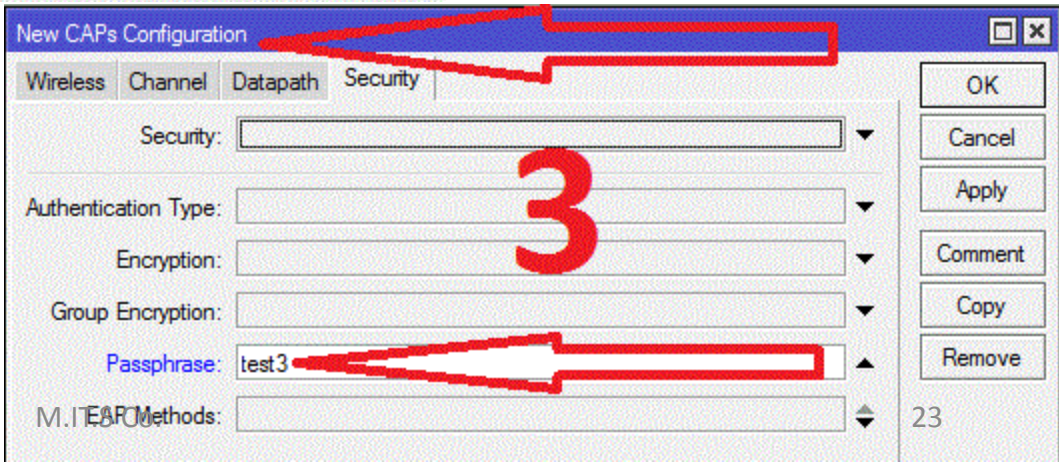
1. Interface Settings (Higher Level)
2. CAPsMAN Settings
3. Configuration settings (Lower level)

CAP & CAPsMAN Configuration



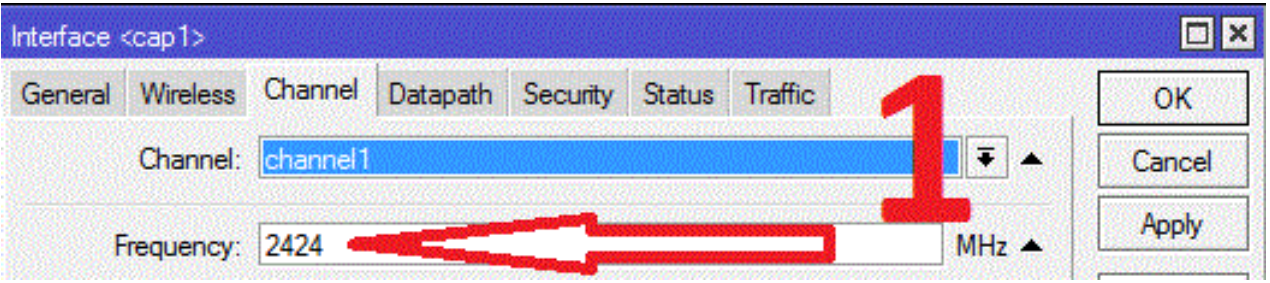
Interface Settings

CAPsMAN Settings

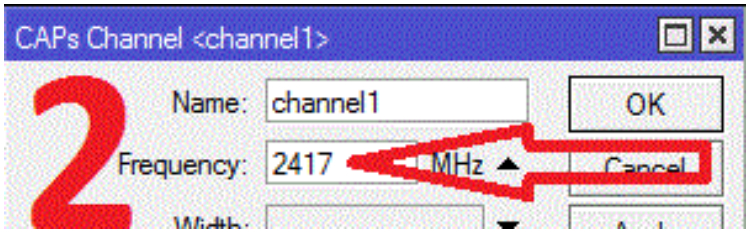


Configuration settings

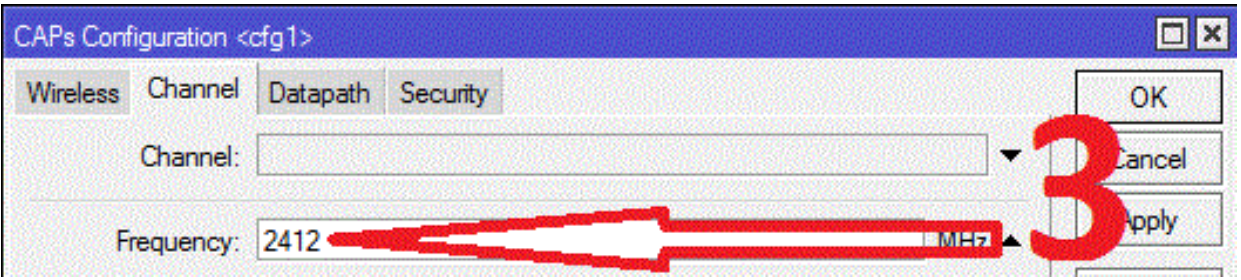
CAP & CAPsMAN Configuration



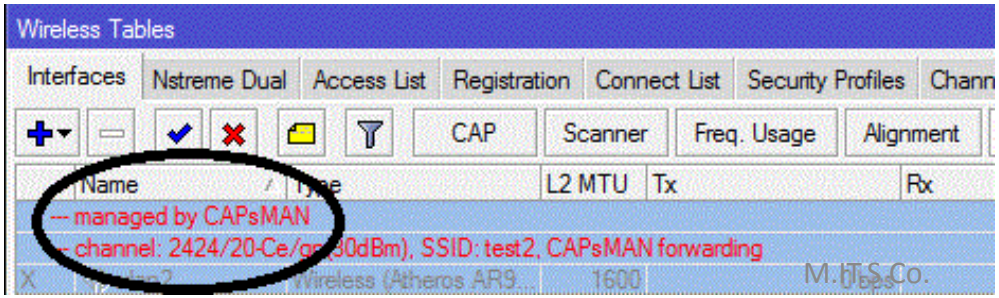
Interface Settings



CAPsMAN Settings



Configuration settings



Result

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 RouterOS configuration and will persist across reboots
- **Dynamically:** exist only while a particular CAP is connected to CAPsMAN

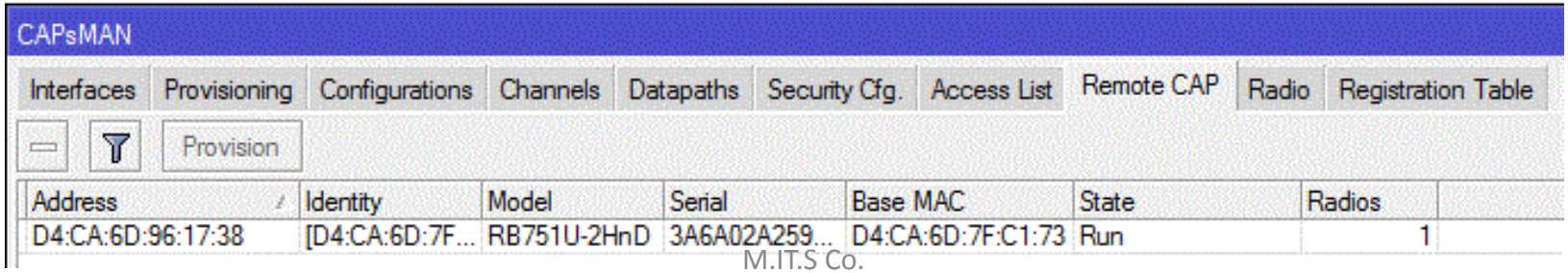
Radio Provisioning

CAPsMAN distinguishes between CAPs based on an Identifier

The Identifier is generated based on:

- **If CAP provides a certificate:** Identifier is set to the Common Name field in the certificate
- **If CAP doesn't provide a certificate:** Identifier is based on Base-MAC provided by CAP in the form of : XX:XX:XX:XX:XX:XX

When DTLS connection successfully established, CAPsMAN makes sure there is no stale connection with CAP using the same identifier

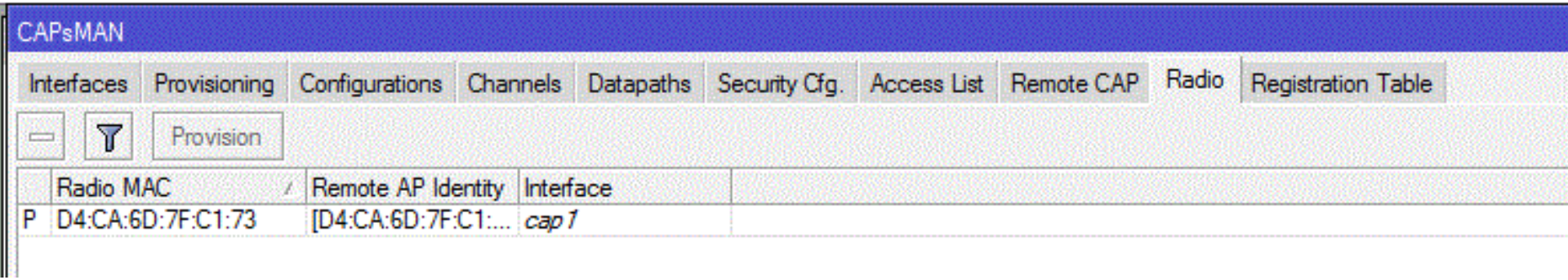


Radio Provisioning

CAPsMAN distinguishes between physical interfaces (radios) based on their built-in MAC address (radio-mac)

So it’s impossible to manage two radios with the same MAC Address

Radio currently managed by CAPsMAN

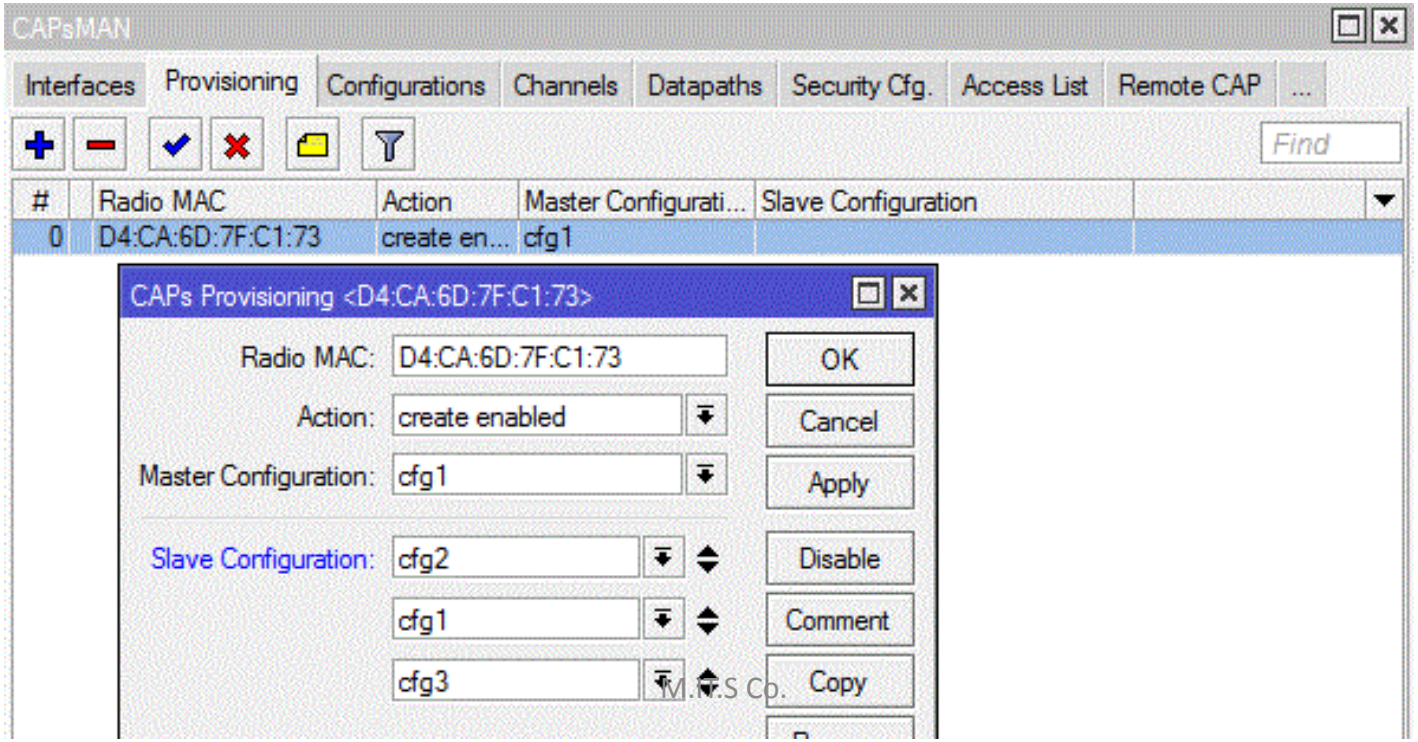


- **Remote CAP:** can be physical or Virtual AP
- **Radio:** Actual Wireless interface (Physical)

Radio Provisioning

When CAP Connects, CAPsMAN at first tries to bind each Cap radio to master interface based on radio-mac

- **If appropriate interface is found:** radio gets setup using master and slave interface configuration , now interfaces are considered bound to radio and radio is considered provisioned
- **If no matching master interface is found:** CAPsMAN executes “provisioning rules”



Datapath Configuration

Datapath settings control data forwarding related aspects

There are 2 major forwarding modes:

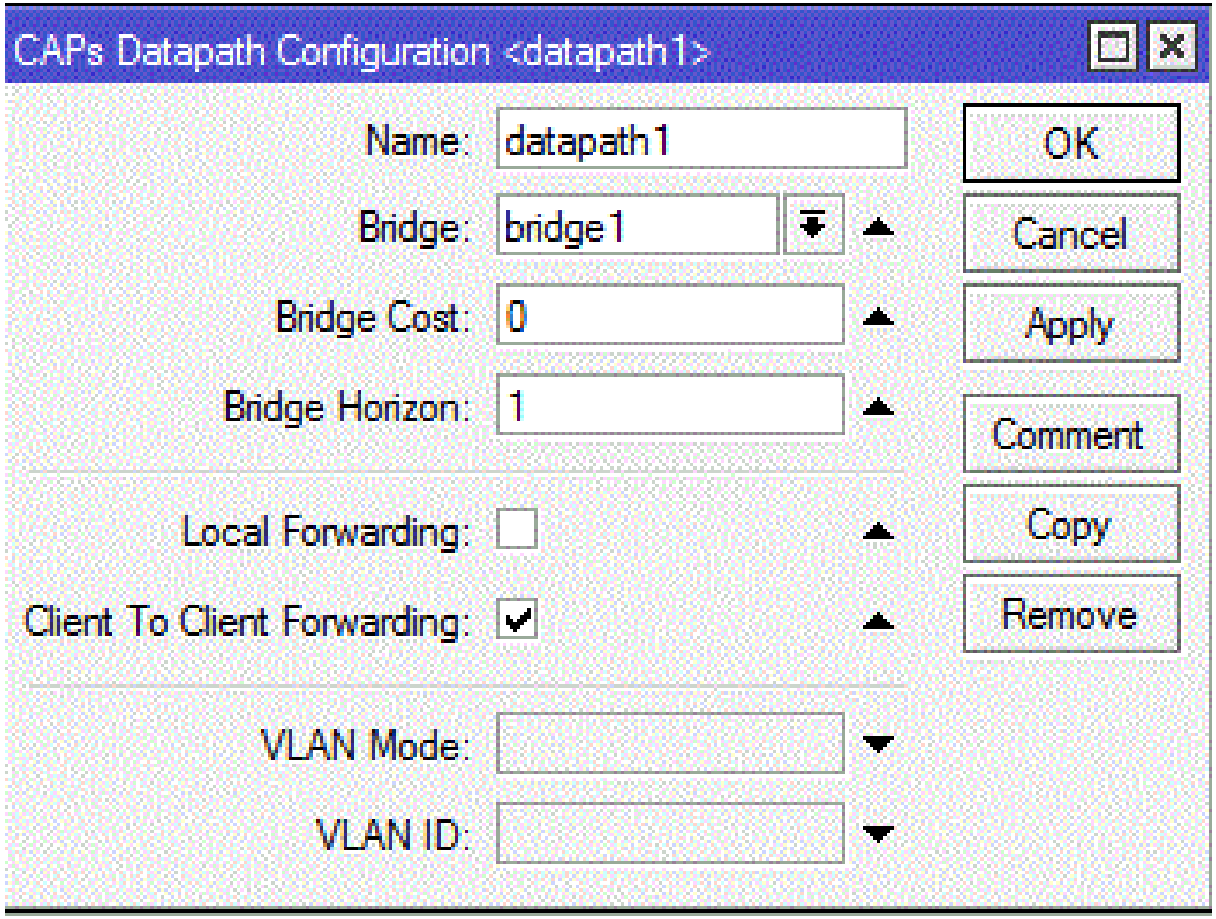
1. **Local forwarding mode:** where CAP is locally forwarding data to and from wireless interface

2. **Manager forwarding mode:** where CAP sends to CAPsMAN all data received over wireless and only sends out the data received from CAPsMAN (Even client-to-client forwarding is controlled and performed by CAPsMAN)

Forwarding mode is configured on a per-interface basis,
Master or Slave interfaces can have different forwarding mode

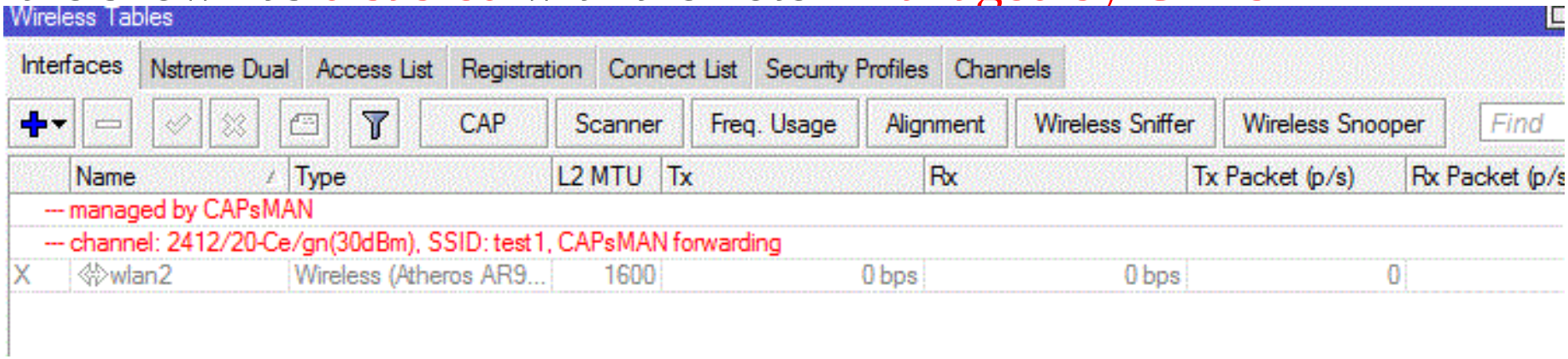
Datapath Configuration

Most of the datapath settings are used only when in manager forwarding mode, because in local forwarding mode CAPsMAN does not have control over data forwarding

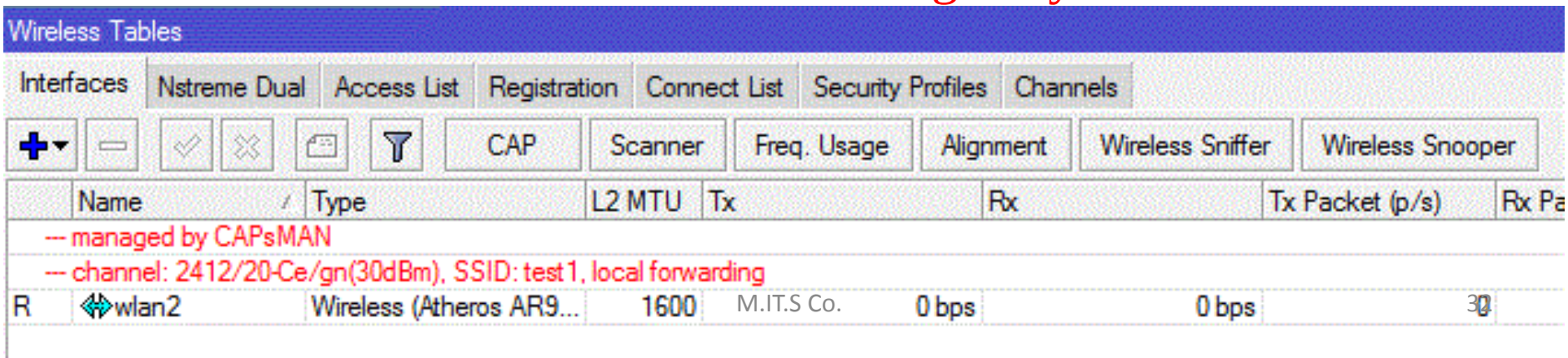


Datapath Configuration

- The CAP wireless interface that are managed by CAPsMAN and also traffic is being forwarded to CAPsMAN (manager forwarding mode), are shown as disabled with the note “Managed by CAPsMAN”

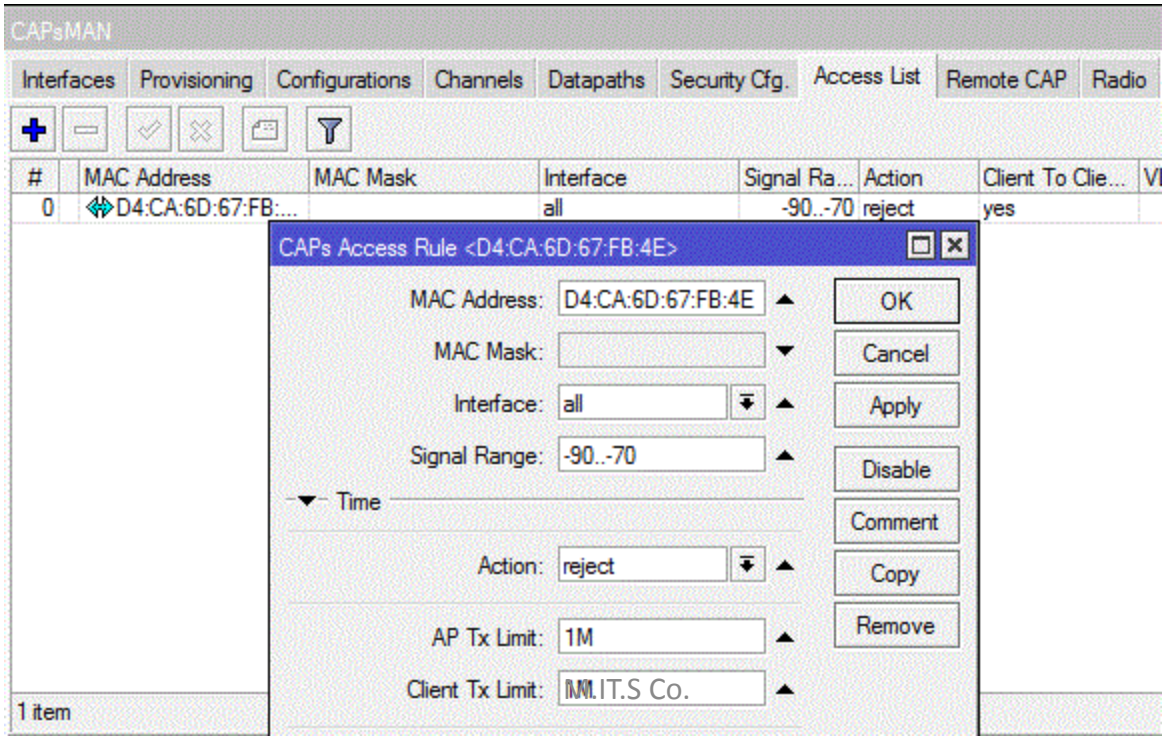


- Those interfaces that are in local forwarding mode (traffic is locally managed by CAP and only management is done by CAPsMAN)are not shown as disabled but the note “Managed by CAPsMAN” is shown



Access List

- Access List on CAPsMAN is an ordered list of rules that is used to allow/deny clients to connect to any CAP under CAPsMAN control
- When client attempts to connect to a CAP that is controled by CAPsMAN, CAP forwards that request to CAPsMAN, as a part of registration process
- CAPsMAN consults access list to determine if client should be allowed to connect or should reject it

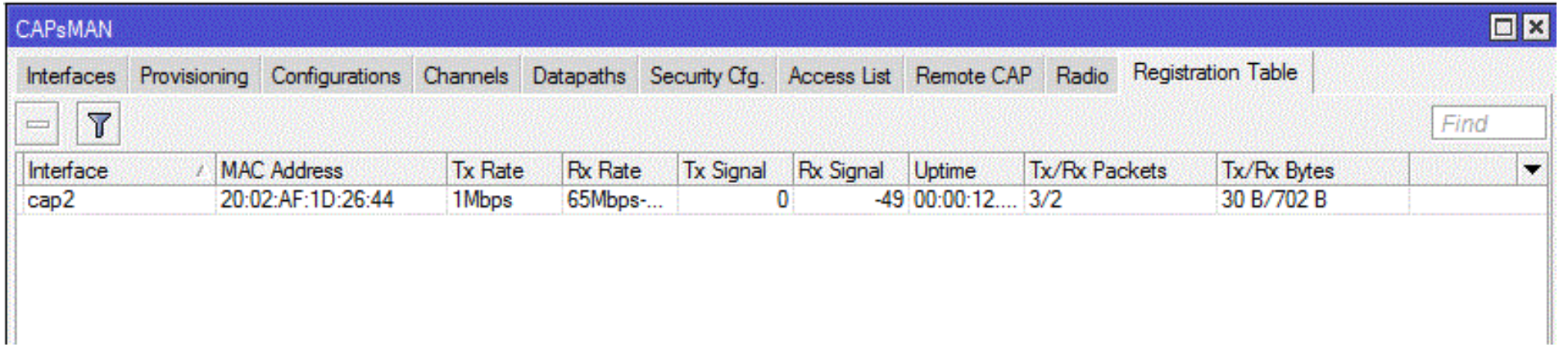


Registration Table

- Registration table contain a list of clients that are connected to radios controlled by CAPsMAN

- This menu is available on **/caps-manager registration-table** menu

```
[admin@CAPsMAN] /caps-man registration-table> pr
 # INTERFACE                    MAC-ADDRESS       UPTIME                RX-SIGNAL
```



My Contact Details

Official Phone: +98 (21) 88 400 717
Private Cell: +98 (912) 149 7009
International Cell: +37259431151
Skype: mani_raissdana
m.raissdana@mits-co.com
raissdana.mani@gmail.com
www.mits-co.com

mani_raissdana mikrotikiran @mani_raissdana Mani Raissdana

Any Questions?????????

Enjoy MUM

Good Luck