WISP / Industrial/ Residential, Marinas Deployment, Using MikroTik CapsMan With Best Features

By Shakeel Khan
Dreams Network & Technology Pvt (Ltd)
Pakistan
About Me

- **Name:** Shakeel Khan
- **Education:** Bachelors In Engineering
- **Position:** Technical Product Manager

**Trainings:**
- Only Mikrotik Trainer & Consultant In Pakistan From **USA**
- MTCNA (**MikroTik Certified Network Associate**)
- MTCWE (**MikroTik Certified Wireless Engineer**)
- MTCTCE (**MikroTik Certified Traffic Control Engineer**)
- UBWS (**Ubiquiti Broadband Wireless Specialist**)
- UBWA V2 (**Ubiquiti Broadband Wireless Admin**)
- UBWE (**Ubiquiti Enterprise Wireless Admin Ubiquiti Broadband Wireless Admin**)
- VoIP YEASTAR
About Company

- Started in 2003
- We are Master Distributor for:
  - IT Managed Services
  - E & I Managed Services
  - Training & Consultancy
  - M2M Solutions
  - Security Solutions
  - Electrical & Instrumentation Solutions with SCADA
Presentation Objectives

- Best Possible Understanding Of Centralized Management System WIFI Hotspots
- Modes of Wireless Networks
- Applications of Wireless Networks
- Centralized Management
- Mikrotik’s CAPsMAN & its Deployment
- Questions & Answers
Modes Of Wireless Networks

PTP (Point to Point):
- Required for long distance links
- High throughput (BACKHUAL PURPOSE)

PTMP (Point to Multi Point):
- Mostly in WISP’s (One To Many)
- Shared link with multiple users
- Cheap compared to point to point

Centralized Managed Wireless Network (Enterprise Hotspots)
- To provide wireless coverage for the roaming/fixed stations
- Highly managed
Advantages & Disadvantage of Wireless Networks

Advantages:
- Required minimum time for installation
- Low cost
- High availability

Disadvantages / Limitations:
- Bandwidth limitations
- Regulatory limitations (Where Applicable)
Mostly Applications of Wireless Network

- Wireless ISPs
- Wireless CCTV
- Wireless VoIP
- Wireless Advertisements
- Wireless SCADA
- Wireless Data Networks
Why We Need Centralized Managed System?

- For high availability of network
- One click management
- One windows statics of network

Applications:
- Hospitals
- Universities
- Industries
- Malls and cafe
- Homes / Apartments
- Ports and container terminals
Conventional problems

- Conventionally, 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 Manpower if we need to changes something for the enterprise WLAN Setups i.e Appartment As Shown.
Solution

- Using Mikrotik Capsman
  It Shall Fix All conventional Problems.
Solution with MIKROTIK CAPsMAN (Success Story)
Reason to use MIKROTIK CAPsMAN

- Highly flexible
- Reliable
- No additional license required (Comes Free With Routerboard Hardware)
- Highly scalable
- CAP can be any MIKROTIK hardware with at least one wireless interface
- 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
- Easy availability
- Low cost
Component of CAPs Management System

- **CAPsMAN**
  - x86 or RouterBOARD based device
  - Newest RouterOS version
  - Wireless-cm2 package installed and enabled

- **CAP**
  - X86 or RouterBOARD based device
  - Newest RouterOS v6 version
  - Atheros chipset (a/b/g/n/ac) wireless card
  - Wireless-cm2 package installed and enabled
  - At least Level4 RouterOS license
CAPsMAN Simple Setup

- **cAP**: cAP is the Controlled Access Point, a device that is managed by the CAPsMAN manager.
- **SXT**: These are devices in the building.
- **CLIENT BUILDING**: This is the client building.
- **WIRELESS DEVICES**: Devices are connected to cAP.
- **CLOUD CORE ROUTER**: This device is the CAPsMAN controller. It is connected to the client building over the wireless link managed by two SXT devices. All cAP devices in the building are controlled by the CAPsMAN. It sees all connected client computers, and manages all settings of the Access Points (cAPs) in that building.
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.
Enable CAPsMAN service
Create Bridge interface
Add IP configuration to Bridge interface
Run DHCP Server with NAT
Create CAPsMAN Configuration
Create Provisioning rule
Enable CAP mode on the Aps
Efficient Roaming Configuration TIP
Specific Brand Allow Only Without Authentication
CAPsMAN Setup LAB
CAPsMAN Setup LAB

1. Bridge with bridge 1 selected
2. Address List showing 192.168.1.0/24
3. DHCP Server with dhcp 1 interface selected
4. Firewall with NAT interface selected
CAPsMAN Setup LAB
CAPsMAN Setup LAB Complete
CAP to CAPsMAN Connection

- **MAC Layer2:**
  - No IP configuration required
  - CAP an 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.
How Cap Selects CAPsMAN

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.
CAP Configuration on AP LAB
Make sure that the latest package of firmware should be updated
CAP Connected with CAPsMAN LAB
CAP Radio Table on CAPsMAN
CAP Identification On Capsman

- MAC / IP Address
- RouterBoard model
- Serial Number of the Board
- RouterOS version
- System Identity
- Main wireless MAC
- State of the CAP
- Provided radio count
Station Registered on CAPsMAN
CAPsMAN Access List Features

- MAC Authentication
- Radius Query support
- MAC Mask support
- Signal Range
- Time
- Private Passphrase
- VLAN ID assignment
Efficient Roaming Configuration TIP
Efficient Roaming Configuration TIP
MAC Authentication

- By using this rule you can reject the undesired stations only
Brand Based Authentication

- By using this rule you can allow selected Brands Via Mac Orders
Our Contact details

- Official Address: C-89 2nd Floor Gulshan-e-Hadeed Phase-I, Karachi, Pakistan-75010
- Lahore

- Official Phone: 021-34710763 Ext : 301
  - Private Cell: +923018212944
- Official Website: www.dreamsnw.com
- Official E-mail: info@dreamnw.com
- http://www.mikrotiktrainings.com/

- Facebook : https://www.facebook.com/DreamsNetworkTechnology
Questions & Answers


Gift For First Two Questioners

http://www.mikrotiktrainings.com/