Last edited on March 10th, 2020

Certified Enterprise Wireless Engineer (MTCEWE)

Training Outline

Duration:	3 days
Objectives:	By the end of this training session, the student will be able to understand major RouterOS Enterprise WiFi features, how WiFi works and implement CAPsMAN into real life WiFi setups.
Target Audience:	Network engineers and technicians wanting to deploy and support: • Corporate WiFi networks based on MikroTik Controlled Access Point system Manager (CAPsMAN) • Simple Layer 2 wireless bridges using MikroTik 60GHz Wireless Wire Technology
Course prerequisites:	MTCNA certificate

Title	Objective

Module 1
Wireless Introduction
	• Wireless routers
	  • RouterBOARD hardware with integrated wireless
	  • MikroTik wireless cards
	• **Module 1 laboratory**

Module 2
RF Wireless Characteristics
	• The RF Radio Spectrum and Electromagnetic Energy
	• Decibels
	• Antenna theory and examples of use
	  • Isotropic
	  • Directional
	  • Omnidirectional
	• Antenna polarization
	• Initial class setup
	• Attenuation/absorption and reflective properties of building materials and how they affect radio signals
	• 2.4/5GHz indoor/outdoor cell sizes and transmitter powers
	• Client roaming
	• RouterOS station roaming setting
	• Co-channel and Adjacent-channel interference
	• Choosing correct access point placement
	• Physical network infrastructure
	• Understanding 'Airtime'
	• **Module 2 laboratory**

Module 3
Wireless Standards
	• 802.11a/b/g/n/ac wireless protocol
	  • 802.11 standards features overview
	  • Bands, channels (frequencies) and channel widths
	  • Scan list
	  • Modulation schemes and MCS data rates
	  • Channel bonding
	  • Frame aggregation overview
	  • Chains (SISO, MIMO and MU-MIMO)
	  • CSMA/CA overview
	  • HW protection (RTS/CTS)
	  • QoS priorities / WMM®
	• Future standards (802.11ax)
	• **Module 3 laboratory**

Module 4 Country / Regulatory Domain Settings in CAPsMAN	• Antenna gain and control of maximum EIRP • Setting antenna gain on CAP • Selecting the country code and purpose of 'installation' setting • Dynamic frequency selection (DFS radar detect) • **Module 4 laboratory**

Module 5 Non CAPsMAN Wireless Modes	• Extending coverage with repeaters and extenders • Bridging with MikroTik 60GHz Wireless Wire products • **Module 5 laboratory**

Module 6 Wireless Security	• Authentication (Open / Shared) • Encryption (WEP, WPA™ TKIP, WPA2™ AES) • Weaknesses of older encryption (WEP / WPA™ TKIP) • Overview of 802.11X (RADIUS and EAP) • Performance difference of TKIP vs. AES • Basic access list (ACL) management • Mitigating against most common known vulnerabilities of 802.11 • **Module 6 laboratory**

Module 7 Wireless Troubleshooting	• Troubleshooting wireless clients • Registration table analysis • TX/RX signal strength • Signal to noise ratio • CCQ, frames and HW frames, hardware retries • Data rates • Analysing the System log for wireless problems • Scan, background scan • Frequency usage • Wireless snooper • Wireless sniffer • **Module 7 laboratory**

Module 8 Wireless Surveys	• Pre-install site surveys • Spectrum analysis overview • Prediction software overview • Post-install validation surveys • **Module 8 laboratory**

Module 9
CAPsMAN v2
	• MikroTik CAPsMAN version 2 features
	• CAP hardware/software requirements
	• L2 (broadcast/multicast) vs L3 (via UDP) CAPs communication methods
	• Using DHCP option 138
	• Configuration of a CAP
	  • CAPsMAN discovery and selection by CAP
	  • Authentication and locking by SSL certificates
	  • Auto certificate & locking
	  • Auto upgrading feature
	  • Securing the CAP configuration
	• CAPsMAN configuration settings (channels, datapaths, security configurations, data rates)
	• Provisioning CAP Interfaces (single and dual band APs)
	• Datapath / local forwarding
	• Dynamic vs static CAP interfaces on CAPsMAN
	• Virtual AP (additional SSIDs)
	• Static interfaces on CAPs (slave virtual interfaces with VLANs)
	• Access list features
	• **Module 9 laboratory**