

*MikroTik*

A C A D E M Y

# MTCUME outline

CERTIFIED USER MANAGEMENT ENGINEER



Duration: 2 days

Outcomes: This course is aimed at Network engineers and technicians wanting to deploy and support large-scale corporate networks. By the end of this training session, the student will be able to securely manage large-scale RouterOS based network with centralised user management. All participants who pass the exam will receive an official MikroTik MTCUME certification.

By the end of this training session, the student will be able to securely manage large scale RouterOS based networks with centralised user management.

Target Audience: Network engineers and technicians wanting to deploy and support large scale corporate networks with centralised user management.

Course prerequisites: A good working knowledge of TCP/IP Basics is required. You must be MikroTik MTCNA Certified (current or expired certificate is fine) to sit this course.

Title	Objective
<p><b>Module 1</b> PPP</p>	<ul style="list-style-type: none"> <li>• PPP Profile <ul style="list-style-type: none"> <li>• Local and remote addresses</li> <li>• Incoming and outgoing filters</li> <li>• Address list</li> <li>• Change TCP-MSS</li> <li>• Use encryption</li> <li>• Session timeout</li> <li>• Rate-limit configuration</li> <li>• Only-one setting</li> </ul> </li> <li>• PPP Secret <ul style="list-style-type: none"> <li>• Service and Profile</li> <li>• Local and Remote address</li> <li>• Routes configuration</li> <li>• Limit Bytes In/Limit Bytes Out configuration</li> </ul> </li> <li>• IP Pool <ul style="list-style-type: none"> <li>• Set addresses ranges</li> <li>• Next pool options</li> </ul> </li> <li>• <b>Module 1 laboratory</b></li> </ul>
<p><b>Module 2</b> PPTP, LT2P</p>	<ul style="list-style-type: none"> <li>• PPTP and L2TP <ul style="list-style-type: none"> <li>• Theory</li> <li>• Comparison</li> </ul> </li> <li>• PPTP Client configuration <ul style="list-style-type: none"> <li>• Client setup</li> <li>• Set profile</li> <li>• Dial on demand</li> <li>• Add default route and static routes</li> </ul> </li> <li>• PPTP Server configuration <ul style="list-style-type: none"> <li>• Enable server</li> <li>• Setup profiles</li> <li>• Add clients to PPP secret</li> <li>• Set static interfaces for clients</li> </ul> </li> <li>• L2TP Client configuration <ul style="list-style-type: none"> <li>• Client setup</li> <li>• Configure profile</li> <li>• Dial on demand</li> <li>• Add default route and static routes</li> </ul> </li> <li>• L2TP Server configuration <ul style="list-style-type: none"> <li>• Enable server</li> <li>• Set profiles</li> <li>• Add clients to PPP secret</li> <li>• Set Static interfaces for clients</li> </ul> </li> <li>• <b>Module 2 laboratory</b></li> </ul>

<p><b>Module 3</b> PPPoE</p>	<ul style="list-style-type: none"> <li>• PPPoE server and client <ul style="list-style-type: none"> <li>• Theory</li> <li>• Usage environment</li> <li>• Comparison to other PPP protocols</li> </ul> </li> <li>• PPPoE client configuration <ul style="list-style-type: none"> <li>• Client setup</li> <li>• Select interface</li> <li>• Service name</li> <li>• Configure profile</li> </ul> </li> <li>• PPPoE Server configuration <ul style="list-style-type: none"> <li>• Enable PPPoE server</li> <li>• Set profiles</li> <li>• Add clients to PPP secret</li> <li>• Add Static interfaces for clients</li> <li>• Secure server by removing any IP address from PPPoE server interface</li> </ul> </li> <li>• Encryption <ul style="list-style-type: none"> <li>• Set profile without encryption</li> <li>• Set profile with encryption</li> <li>• Configure PPPoE client without encryption</li> </ul> </li> <li>• Interface ECMP <ul style="list-style-type: none"> <li>• Set ECMP routes for PPP interfaces</li> </ul> </li> <li>• <b>Module 3 laboratory</b></li> </ul>
----------------------------------	---

<p><b>Module 4</b> Bridging</p>	<ul style="list-style-type: none"> <li>• L2TP and EoIP <ul style="list-style-type: none"> <li>• Set L2TP tunnel</li> <li>• Set EoIP tunnel</li> <li>• Create bridge and add necessary interfaces to ports</li> <li>• Confirm you have Ethernet connectivity between remote nodes</li> </ul> </li> <li>• L2TP and VPLS <ul style="list-style-type: none"> <li>• Set L2TP tunnel</li> <li>• Set VPLS tunnel</li> <li>• Create bridge and add necessary interfaces to ports</li> </ul> </li> <li>• L2TP and BCP <ul style="list-style-type: none"> <li>• Set L2TP tunnel</li> <li>• Use BCP to bridge PPP interface</li> <li>• Add to bridge necessary interface</li> </ul> </li> <li>• Multilink Protocol <ul style="list-style-type: none"> <li>• Enable multilink by specifying correct MRRU settings</li> <li>• Disable mangle rules for MSS adjustment</li> </ul> </li> <li>• MLPPP (optional) <ul style="list-style-type: none"> <li>• Setup client and specify multiple interfaces for one client</li> <li>• Set PPPoE server with MLPPP support</li> </ul> </li> <li>• <b>Module 4 laboratory</b></li> </ul>
-------------------------------------	---

<p><b>Module 5</b> IPSec</p>	<ul style="list-style-type: none"> <li>• Introduction <ul style="list-style-type: none"> <li>• Theory and concepts</li> <li>• Comparison to other VPN protocols</li> </ul> </li> <li>• IPSec Peer <ul style="list-style-type: none"> <li>• Use different authentication methods</li> <li>• IPSec exchange modes</li> <li>• Encryption and hash algorithms</li> <li>• NAT-Traversal</li> <li>• Lifetime and lifebytes</li> <li>• DPD protocol</li> </ul> </li> <li>• Policy <ul style="list-style-type: none"> <li>• IPSec protocol and action</li> <li>• Tunnels</li> <li>• Generate dynamic Policy</li> </ul> </li> <li>• Proposal <ul style="list-style-type: none"> <li>• Encryption and authentication algorithms</li> <li>• Lifetime</li> <li>• PFS</li> </ul> </li> <li>• Installed-SA <ul style="list-style-type: none"> <li>• Flush SA</li> </ul> </li> <li>• Create IPSec between two routers with NAT <ul style="list-style-type: none"> <li>• Set peer</li> <li>• Set policy</li> <li>• Set NAT rules</li> <li>• Confirm the secure link is established</li> </ul> </li> <li>• <b>Module 5 laboratory</b></li> </ul>
----------------------------------	---

<p><b>Module 6</b> HotSpot</p>	<ul style="list-style-type: none"><li>• Introduction<ul style="list-style-type: none"><li>• Concepts</li><li>• Usage environments</li><li>• Setup HotSpot with default settings</li></ul></li><li>• HotSpot Login Methods<ul style="list-style-type: none"><li>• HTTP CHAP/PAP</li><li>• MAC</li><li>• Cookie</li><li>• HTTPS</li><li>• Trial</li><li>• RADIUS</li></ul></li><li>• Users<ul style="list-style-type: none"><li>• Add users</li><li>• Set MAC-address for user</li><li>• Set MAC-address for username</li><li>• Limit Uptime and Limit Bytes In/Out</li><li>• Reset limits for user</li></ul></li><li>• Monitor Users<ul style="list-style-type: none"><li>• Host Table</li><li>• Active Table</li><li>• SNMP for users</li></ul></li><li>• Profile<ul style="list-style-type: none"><li>• Keepalive timeout</li><li>• Shared users</li><li>• Rate-Limit</li><li>• Address-list</li><li>• Incoming/Outgoing filter</li><li>• Incoming/Outgoing Packet Mark</li></ul></li><li>• Bypass HotSpot<ul style="list-style-type: none"><li>• Walled garden</li><li>• Walled garden IP</li><li>• IP binding</li></ul></li><li>• Customize HotSpot<ul style="list-style-type: none"><li>• Advertisement</li><li>• Customize pages</li></ul></li><li>• <b>Module 6 laboratory</b></li></ul>
------------------------------------	--

<p><b>Module 7</b> RADIUS</p>	<ul style="list-style-type: none"><li>• RADIUS client<ul style="list-style-type: none"><li>• Add radius client</li><li>• Set service</li><li>• Use RADIUS for the specific service</li></ul></li><li>• RADIUS server</li><li>• User manager<ul style="list-style-type: none"><li>• Install the latest user-manager</li><li>• Add routers</li><li>• Add users</li><li>• Set profile</li></ul></li><li>• RADIUS incoming</li><li>• <b>Module 7 laboratory</b></li></ul>
-----------------------------------	---