



L2TPv2 Tunnel Configuration and Monitoring on cnPilot E Series Access Points

Revision History

Date	Version #	Author(s)	Comments

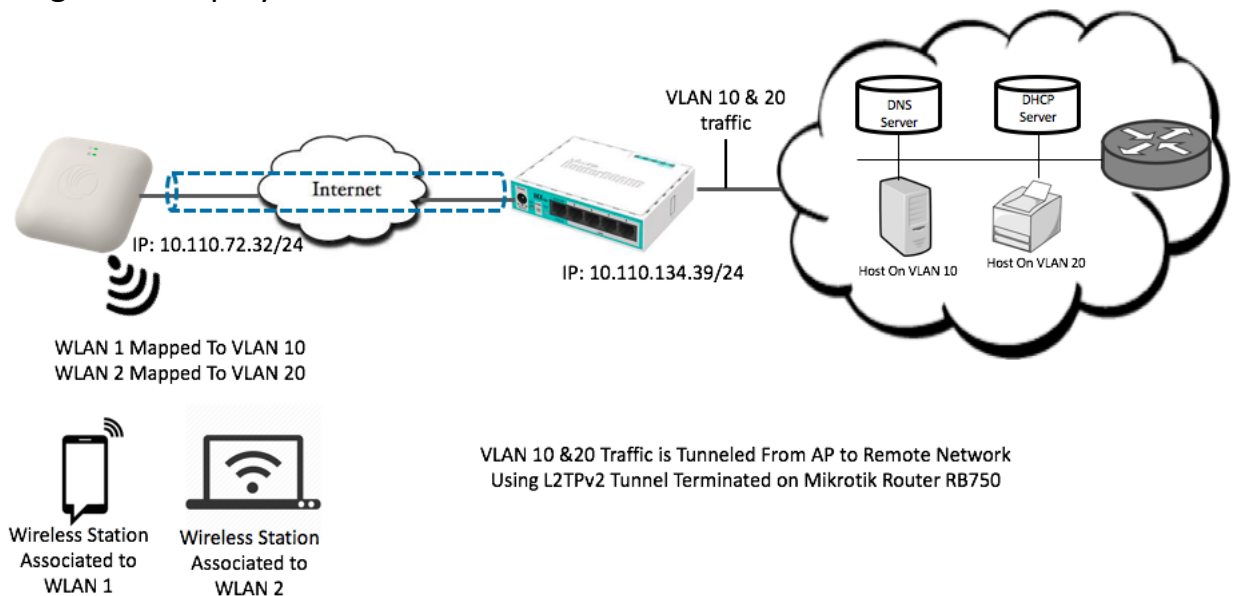
Table of Contents

1. Overview of the document
2. L2TPv2 tunnel configuration between AP and Mikrotik Router
 - 2.1 L2TPv2 Tunnel and WLAN profile configuration on AP
 - 2.2 L2TPv2 Tunnel configuration on Mikrotik router
3. Deployment guidelines

1. Overview of the document

The document will show how to configure and establish L2TPv2 tunnel between AP and Mikrotik router RB750r2 / RB3011UiAS-RM. L2TPv2 tunnel can be used to tunnel the WLAN traffic from AP to remote location. BCP protocol is used to carry WLAN user traffic using PPP session which is established over L2TPv2 tunnel.

The general deployment will look like this



2. L2TPv2 tunnel configuration between AP and Mikrotik Router

It is assumed that AP and Mikrotik router have been configured with the IP addresses, default gateway and reachable over the internet or intranet network.

AP will tag WLAN traffic with the assigned VLAN and will put the traffic on the tunnel interface. Mikrotik router will put the VLAN tagged packet on LAN ports

2.1 L2TPv2 Tunnel and WLAN profile configuration on AP

WLAN 1 profile is configured with VLAN 10 and L2TPv2 tunnel option

The screenshot displays the Cambium Networks cnPilot E400 web interface for configuring a WLAN profile. The left sidebar shows the navigation menu with options like Dashboard, Monitor, Configure, System, Radio, WLAN, Network, Services, Operations, and Troubleshoot. The main content area is titled 'Configure / Wlan' and shows the configuration for 'wlan 1'. The 'Basic' tab is active, displaying fields for Enable (checked), Mesh (Off), SSID (WLAN 1), VLAN (10), Security (WPA2 Pre-shared Keys), Passphrase (masked), Radios (5GHz), Max Clients (127), Client Isolation (unchecked), and Hide SSID (unchecked). A red circle highlights the 'VLAN' field, with a red arrow pointing to it and the text 'WLAN 1 Mapped to VLAN 10'. The 'Advanced' tab is also visible, showing fields for UAPSD (unchecked), QBSS (unchecked), DTIM interval (1), Monitored Host (empty), Band Steering (Disabled), Proxy ARP (checked), Insert DHCP Option82 (unchecked), Tunnel Mode (checked), Fast-Roaming Protocol (Pre-authentication, OKC, 802.11r), and 802.11w State (Disable). A red circle highlights the 'Tunnel Mode' field, with a red arrow pointing to it and the text 'Enable L2TPv2 Tunnel Option On WLAN Configuration'. The 'Save' and 'Cancel' buttons are at the bottom.

WLAN 1 profile CLI configuration

```

wireless wlan 1
  ssid "WLAN 1"
  no shutdown
  vlan 10
  security wpa2-psk
  passphrase $crypt$1$AS6/o+ejaVVEuHJtqGrtm4gtcidqRXC7
  band 5GHz
  dtim-interval 1
  max-associated-client 127
  tunnel-mode
  mac-authentication policy deny
  no guest-access
!

```

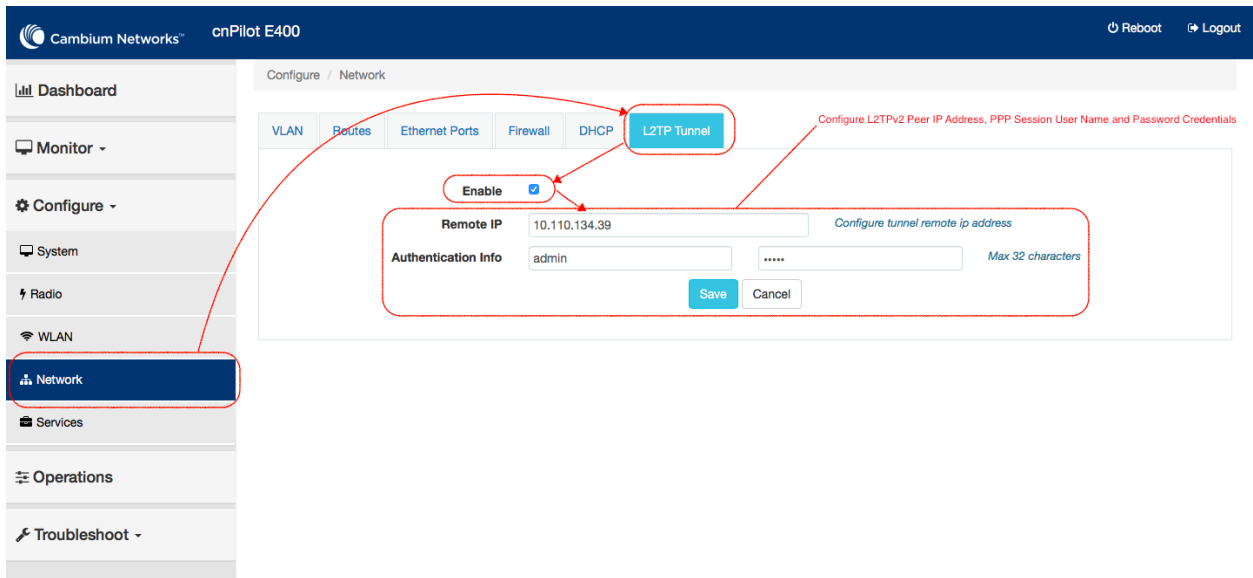
WLAN 2 profile is configured with VLAN 20 and L2TPv2 tunnel option

The screenshot displays the Cambium Networks cnPilot E400 web interface for configuring WLAN 2. The interface is divided into a left sidebar with navigation options (Dashboard, Monitor, Configure, Operations, Troubleshoot) and a main content area. The main content area has a top bar with 'Configure / Wlan' and buttons for 'Edit', 'Delete this Wireless LAN', and 'Create Wireless LAN'. Below this is a tabbed interface with 'Basic', 'Radius Server', 'Guest Access', 'Usage Limits', 'Scheduled Access', 'Access', and 'Passpoint' tabs. The 'Basic' tab is selected, showing various configuration fields. A red circle highlights the 'VLAN' field, which is set to '20'. A red arrow points to this field with the text 'WLAN 2 Mapped To VLAN 20'. Another red circle highlights the 'Tunnel Mode' checkbox in the 'Advanced' section, which is checked. A red arrow points to this checkbox with the text 'Enable L2TPv2 Tunnel Option On WLAN 2'. Other fields include 'Enable' (checked), 'Mesh' (Off), 'SSID' (WLAN 2), 'Security' (WPA2 Pre-shared Keys), 'Passphrase' (masked), 'Radios' (2.4GHz and 5GHz), 'Max Clients' (127), 'Client Isolation' (unchecked), 'Hide SSID' (unchecked), 'UAPSD' (unchecked), 'QBSS' (unchecked), 'DTIM Interval' (1), 'Monitored Host' (empty), 'Band Steering' (Disabled), 'Proxy ARP' (checked), 'Insert DHCP Option82' (unchecked), 'Fast-Roaming Protocol' (Pre-authentication), and '802.11w State' (Disable). At the bottom right are 'Save' and 'Cancel' buttons.

WLAN 2 profile CLI configuration

```
!  
wireless wlan 2  
  ssid "WLAN 2"  
  no shutdown  
  vlan 20  
  security wpa2-psk  
  passphrase $crypt$1$VReLF3zP0jiGUuepVIxS9I7oi/FYrVEB  
  band both  
  dtim-interval 1  
  max-associated-client 127  
  tunnel-mode  
  mac-authentication policy deny  
  no guest-access  
!
```

L2TPv2 tunnel configuration on AP



L2TPv2 Tunnel CLI configuration

```
!
tunnel l2tp
no shutdown
remote-ip 10.110.134.39
auth admin $crypt$1$IT3as4npmJQo1ffYC0+x35Rzd1pae4fz
```

One AP once can see the status of tunnel with command “show tunnel status”

```
MB-E500(config)# show tunnel-status
```

TYPE	REMOTE-IP	STATUS
l2tp	10.110.134.39	Up

```
MB-E500(config)#
```

2.2 L2TPv2 Tunnel configuration on Mikrotik router

Configuration on Mikrotik router (750 RB750r2 hEX lite 5 ports router) involves below 5 steps

- Disable Firewall on WAN interface

- Bridge configuration
- Assigning port to bridge
- Assigning IP address to bridge
- Create PPP profile for bridging
- Add PPP secrets
- Configuring L2TPv2 Server

Disable Firewall configuration on WAN interface:

WebFig v6.36 (stable)

Firewall

Filter Rules NAT Mangle Raw Service Ports Connections Address Lists Layer7 Protocols

Add New Reset All Counters

8 items

#	Action	Chain	Src. Address	Dst. Address	Prot...	Src. Port	Dst. Port	Any. Port	In. Interf...	Out. Interf...	Bytes	Packets
;;; special dummy rule to show fasttrack counters												
0	accept	forward									0 B	0
;;; defconf: accept ICMP												
1	accept	input			1 (icmp)						15.6 KiB	127
;;; defconf: accept established,related												
2	accept	input									8.7 MiB	53 918
;;; defconf: drop all from WAN												
3	drop	input							ether1		0 B	0
;;; defconf: fasttrack												
4	fasttrack	forward									0 B	0
;;; defconf: accept established,related												
5	accept	forward									0 B	0
;;; defconf: drop invalid												
6	drop	forward									0 B	0
;;; defconf: drop all from WAN not DSTNATed												
7	drop	forward							ether1		0 B	0

Disable Firewall on WAN Interface Ether 1

Bridge configuration:

Go to bridge configuration section and add new bridge with below configuration

Interfaces

Bridge

Switch

PPP

Mesh

IP

ARP

Accounting

Addresses

Cloud

DHCP Client

DHCP Relay

DHCP Server

DNS

Firewall

Hotspot

IPsec

Neighbors

Packing

Pool

Routes

SMB

SNMP

Services

Settings

Socks

TFTP

Traffic Flow

UPnP

Web Proxy

MPLS

Routing

OK Cancel Apply Remove Torch

running not slave

Enabled ☒

Name bridge_12tp_tunnel

Type Bridge

MTU Set MTU 1500 Bytes

Actual MTU 1500

L2 MTU 1598

MAC Address 4C:5E:0C:4F:5F:51

ARP enabled

Admin. MAC Address 4C:5E:0C:4F:5F:51

Protocol Mode none stp rstp

Priority 8000 hex

Max Message Age 00:00:20

Forward Delay 00:00:15

Transmit Hold Count 6

Ageing Time 00:05:00

General

STP

Status

Assigning port to bridge:

Go to bridge configuration section and add new port with below configuration

Quick Set

CAPS MAN

Wireless

Interfaces

Bridge

Switch

PPP

Mesh

IP

MPLS

Routing

System

Queues

Files

Log

Radius

Tools

New Terminal

MetaROUTER

Partition

Make Supout.rtf

Undo

Redo

Hide Menu

Hide Passwords

Safe Mode

Design Skin

Manual

WinBox

Graphs

End-User License

WebFig v6.35.4 (stable)

Bridge Port <ether2-master>

OK Cancel Apply Remove

not inactive

Enabled ☒

Interface ether2-master

Bridge bridge_12tp_tunnel

Priority 80 hex

Path Cost 10

Horizon auto

Edge auto

Point To Point auto

External FDB auto

Auto Isolate ☐

Port Number 1

Role designated port

Edge Port ☐

General

Status

Assigning IP address to bridge interface:

Go to IP configuration -> Addresses -> Add new

Quick Set
CAPsMAN
Wireless
Interfaces
Bridge
Switch
PPP
Mesh
IP
ARP
Accounting
Addresses
Cloud
DHCP Client
DHCP Relay

OK Cancel Apply Remove

Select Previously Created Bridge Interface

not invalid Configure IP Address and Mask

Enabled ☒

Address 192.168.88.1/24

Network 192.168.88.0

Interface bridge_l2tp_tunnel

Comment defconf

Create PPP profile for bridging:

Go to PPP Configuration -> Profiles -> Add New settings, please do below configurations

Quick Set
CAPsMAN
Wireless
Interfaces
Bridge
Switch
PPP
Mesh
IP
ARP
Accounting
Addresses
Cloud
DHCP Client
DHCP Relay
DHCP Server
DNS
Firewall
Hotspot
IPsec
Neighbors
Packing
Pool
Routes
SMB
SNMP
Services
Settings
Socks
TFTP
Traffic Flow
UPnP
Web Proxy

WebFig v6.35.4 (stable)

PPP Profile <ppp-bridging>

OK Cancel Apply Remove

Configure PPP profile name and attach previously configured bridge

Name ppp-bridging

Local Address

Remote Address

Bridge bridge_l2tp_tunnel

Bridge Port Priority hex

Bridge Path Cost

Incoming Filter

Outgoing Filter

Address List

DNS Server

WINS Server

Change TCP MSS no yes default

Use UPnP no yes default

Use MPLS no yes required default

Use Compression no yes default

General

Protocols

PPP Secret settings:

Go to PPP Configuration -> Secrets -> Add new settings and do below configuration

WebFig v6.35.4 (stable)

PPP Secret <admin>

OK Cancel Apply Remove

Enabled ☒

Name admin

Password *****

Service any

Caller ID

Profile ppp-bridging

Local Address

Remote Address

Routes

Limit Bytes In

Limit Bytes Out

Last Logged Out Jul/26/2016 07:31:46

Comment

Configure user name and password and map to previously configured PPP profile

Configuring L2TPv2 Server:

Go to PPP Configuration -> Interface -> L2TP Server with the below configuration options

WebFig v6.35.4 (stable)

L2TP Server

OK Cancel Apply

Enabled ☒

Max MTU 1500

Max MRU 1500

MRRU 1600

Keepalive Timeout 30

Default Profile ppp-bridging

Max Sessions

Authentication ☒ mschap2 ☒ mschap1 ☒ chap ☒ pap

Use IPsec ☐

IPsec Secret

Allow Fast Path ☐

Attach previously configured PPP bridge to L2TPv2 interface

This completes Mikrotik router UI configuration for L2TPv2 bridging

One can see the status of L2TPv2 tunnel under Interfaces section

	Name	Type	L2 MTU	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx	FP Rx	FP Tx Packet (p/s)
DRS	<l2tp-admin-4>	L2TP Server Binding		0 bps	0 bps	0	0	0 bps	0 bps	0
R	VLAN10	VLAN	1594	0 bps	0 bps	0	0	0 bps	0 bps	0
R	bridge_l2tp_tunnel	Bridge	1598	0 bps	0 bps	0	0	0 bps	0 bps	0
R	ether1	Ethernet	1598	109.6 kbps	10.3 kbps	11	11	110.0 kbps	11.0 kbps	11
S	ether2-master	Ethernet	1598	0 bps	0 bps	0	0	0 bps	0 bps	0
S	ether3	Ethernet	1598	0 bps	0 bps	0	0	0 bps	0 bps	0
S	ether4	Ethernet	1598	0 bps	0 bps	0	0	0 bps	0 bps	0
S	ether5	Ethernet	1598	0 bps	0 bps	0	0	0 bps	0 bps	0

L2tp-admin-4 is the dynamic tunnel name and double click this one to see more tunnel details

More status and statistics information of the above created tunnel

General	
Name	<l2tp-admin-4>
Type	L2TP Server Binding
L2 MTU	1596
User	admin
Status	
Last Link Up Time	Jul/24/2016 14:54:17
Link Down	0
Uptime	1d 01:11:41
User	admin
Caller ID	10.110.72.32
Encoding	
MTU	1596
MRU	1600

Tunnel name and type will be displayed

Tunnel up time will be displayed

3. Deployment guidelines

- When WLAN profile is configured with L2TPv2 tunnel option, DHCP server, Default gateway and DNS server shall be reachable over the tunnel
- User traffic will not be bridged to local VLAN interface i.e. all the user traffic on that WLAN will be put on to the tunnel only

- On board Captive Portal feature will not work on the tunneled WLAN