

Migrating Wi-Fi Tunnel Concentrator from cnMaestro On-Premises to an external solution

[Document subtitle]



[Date]

Cambium

[Company address]

Contents

[Overview. 2](#_Toc61860772)

[L2tp tunnel configuration between cnPilot and Mikrotik 2](#_Toc61860773)

[Introduction 2](#_Toc61860774)

[Topology diagram. 3](#_Toc61860775)

[Configuration on Mikrotik router 4](#_Toc61860776)

[Configuration on cnPilot AP 18](#_Toc61860777)

[Check the status of L2tp tunnel on AP. 20](#_Toc61860778)

[Same configuration can also be done from cnMaestro. 20](#_Toc61860779)

[Tunnel status on Mikrotik**.** 24](#_Toc61860780)

[Dhcp server status on Mikrotik. 25](#_Toc61860781)

[Known Interoperability issues with Mikrotik router 25](#_Toc61860782)

[Scalability 27](#_Toc61860783)

[Setting up EoGRE Tunnel between Cambium cnPilot and Ubuntu 28](#_Toc61860784)

[Topology diagram. 28](#_Toc61860785)

[Ubuntu server configuration 29](#_Toc61860786)

[AP configuration for Eogre tunnel. 30](#_Toc61860787)

[AP UI configuration. 32](#_Toc61860788)

[Configure the GRE tunnel. 33](#_Toc61860789)

[Same configuration can also be done from cnMaestro. 34](#_Toc61860790)

[AP statistics. 34](#_Toc61860791)

[Cli statistics. 34](#_Toc61860792)

[AP UI statistics. 35](#_Toc61860793)

[GRE Packet capture 35](#_Toc61860794)

# Overview.

CnPilot provides two tunneling option, l2tpv2 with BCP & EoGRE tunnel. Both the tunneling mechanism can be used to bridge the Ethernet traffic coming from an end host (wireless client) , and encapsulate the traffic using either EoGRE or L2tpv2 header and forward over an L3 network.  The most widely deployed tunnel is EoGRE because it has less protocol overhead compared to L2tpv2 and works with number of deployment solutions. We have validated EoGRE tunnel between cnPilot access point and linux server.

Since the support for EoGRE tunnel will be deprecated on cnMaestro from 3.x release, Cambium recommends customers to move to either of the two tunneling deployment solutions supported by cnPilot.

Available Tunneling options on cnPilot

* L2tpv2 with BCP  (Tunnel between  Mikrotik & cnPIlot)
* EoGRE   ( Tunnel between Linux server  & cnPilot).

The steps to configure both the tunnel is listed below. The solution can be used to scale up to 100 to 200 tunnels. Scaling of the tunnel depends on the hardware configuration of the Ubuntu server in case of EoGRE and model number of the Mikrotik router.

*NOTE: There is interoperability problem between cnPIlot and Mikrotik if auto-mac feature is enabled on Mikrotik router, so we recommend disabling this feature on Mikrotik to avoid the issue.*

*Please read the interoperability section which explains in detail about the issue.*

# L2tp tunnel configuration between cnPilot and Mikrotik

# 

# 

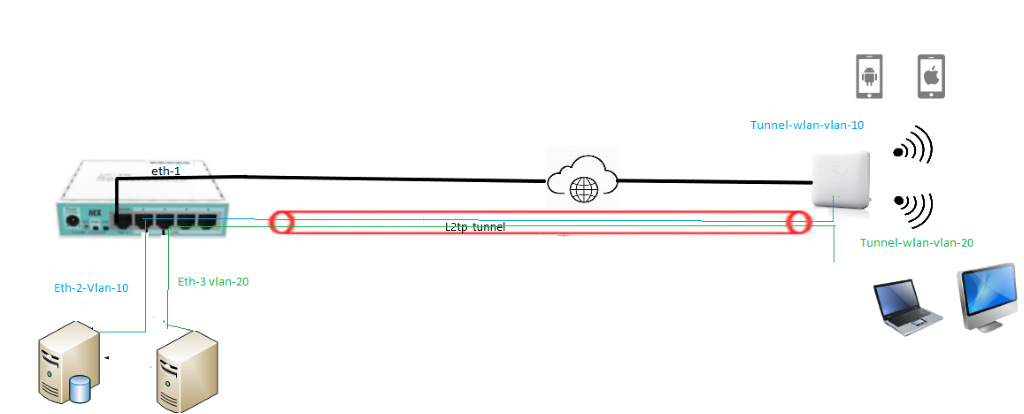
Introduction.

L2tp is a layer 2 tunneling protocol used to tunnel the wlan vlan to centralized tunnel concentrator.

This is the centralized deployment model where the dhcp server for all the wlan vlan will run on the mikrotik router or it can be behind mikrotik. The L2tp tunnel terminates on the mikrotik router and then the user traffic is routed through the wan interface.

## Topology diagram.

----------------------



Topology Details.

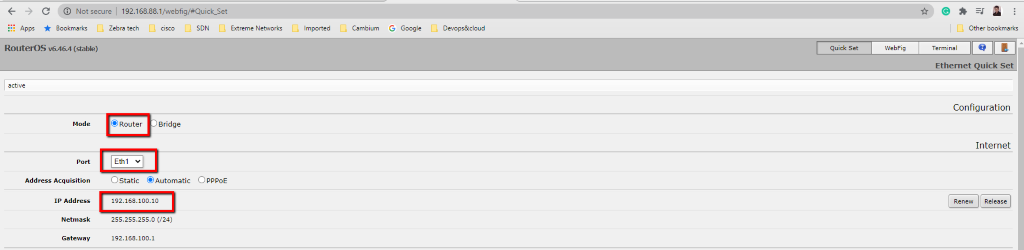
* AP connects to the POE switch and gets ip address from the management vlan.
* User can onboard the AP to cnMaestro and push the configuration from there or can directly open the AP ui and do the wlan configuration.
* Launch the AP ui and configure two wlan.
* Ssid-1 : mapped to vlan 10
* Ssid –2 mapped to vlan 20
* Configure each  wlan in tunnel mode. Steps to configure the wlan is listed below
* Configure L2tp tunnel on the Access point . Steps to the tunnel is listed below.
* Configure the Mikrotik router accept l2tpv2 tunnel request from the Access point. Steps for the configuration is listed below.
* Once the tunnel is established, connect a wireless client to wlan 1, check the wireless client gets ip address and it can reach the default gateway.
* Similarly connect another client to wlan 2 and verify that it can ip address and reach the default gateway.

## Configuration on Mikrotik router

1. Login to MIkrotik router.

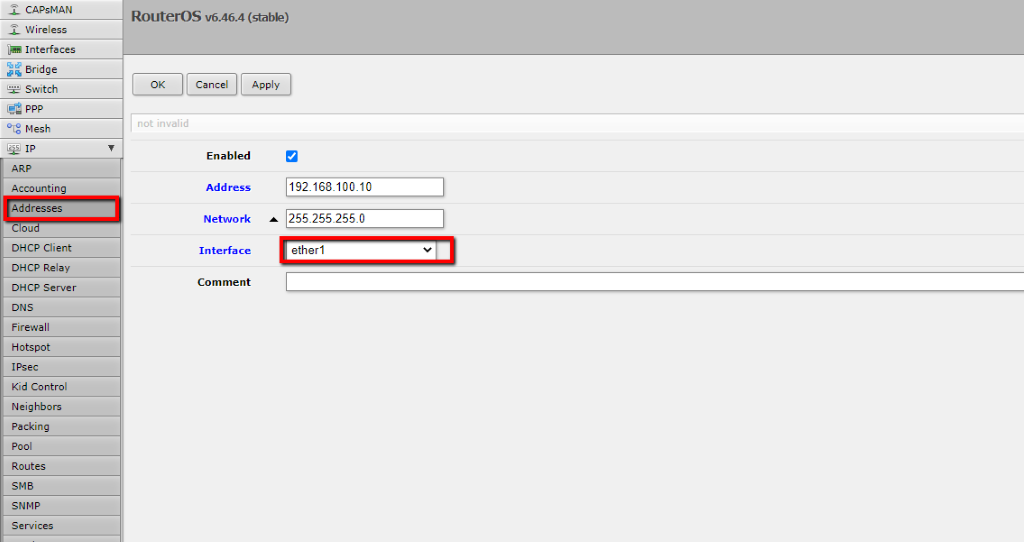
Eth1 interface or the wan interface is assigned ip address dynamically from the network.

Ensure Gateway and mask is learned from the dhcp server.



Or you can manually assing static ip address

Go to Address > ADD NEW > assign the static address to the eth1 interface.



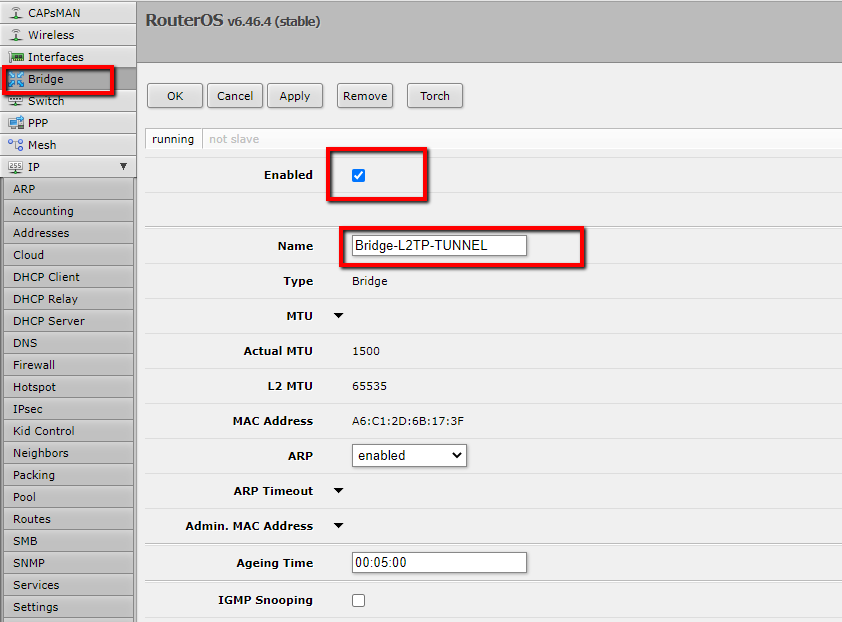
2) Add a bridge interface for L2tp-tunnel.

Go to Bridge > ADD NEW.

Click on Enable check box.

Type the name for the bridge interface “Bridge-L2tp-Tunnel.”

Click Apply OK.



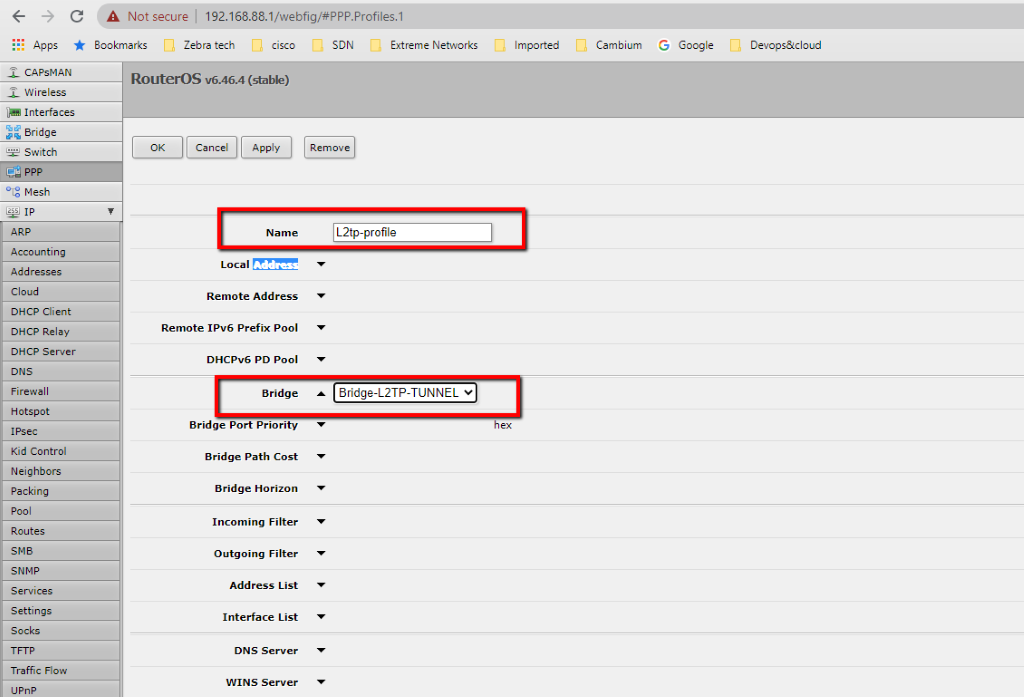
3) configure the L2tp PPP profile.

Click on PPP > profiles >add new

Type the name of the bridge ppp profile “l2tp-profile”

In the Bridge dropdown select the bridge interface as “Bridge-L2TP-Tunnel.”

Click Apply OK.



4)  configure the PPP profile secrets .

      Username and password for the L2tp tunnel.

 Go to PPP > secrets > Add New.

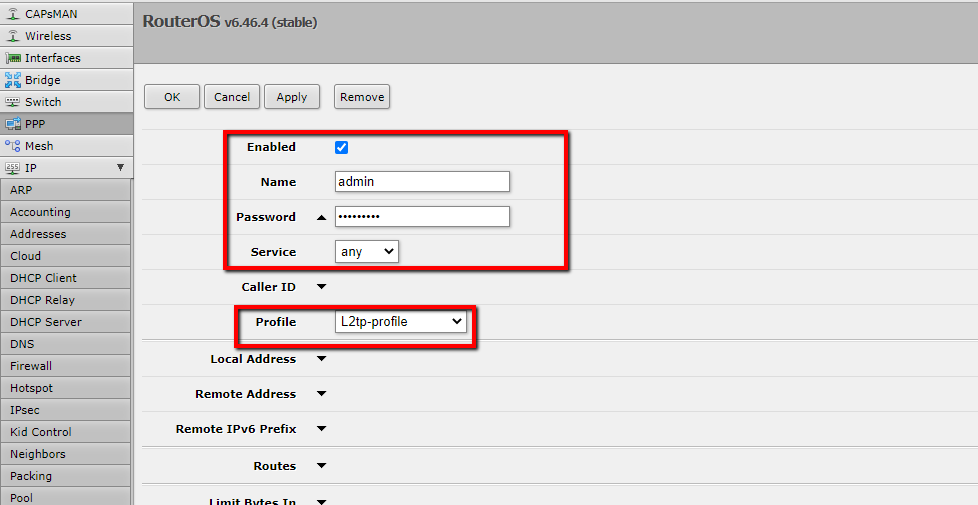
Click on the enable checkbox.

Configure Name as : admin

Password : secret123

Service : Any

Profile : L2tp-profile.



5)  Configure the L2tp server.

Go PPP>L2tp Server .

Click on enable checkbox.

Configure the max MTU as 1460

Configure Max MRU as 1460.

Configure MRRU as 1518.

Select default profile from the drop down as “L2TP-Profile.”

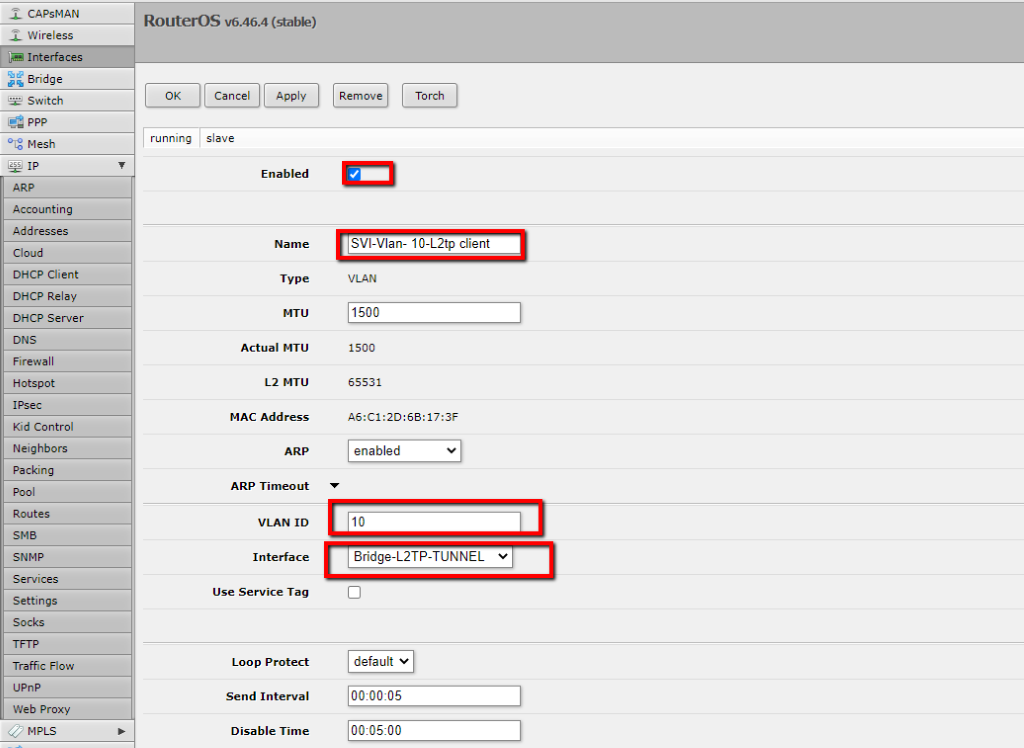
Note: Please set the MTU and MRRU values as suggested to avoid fragmentation

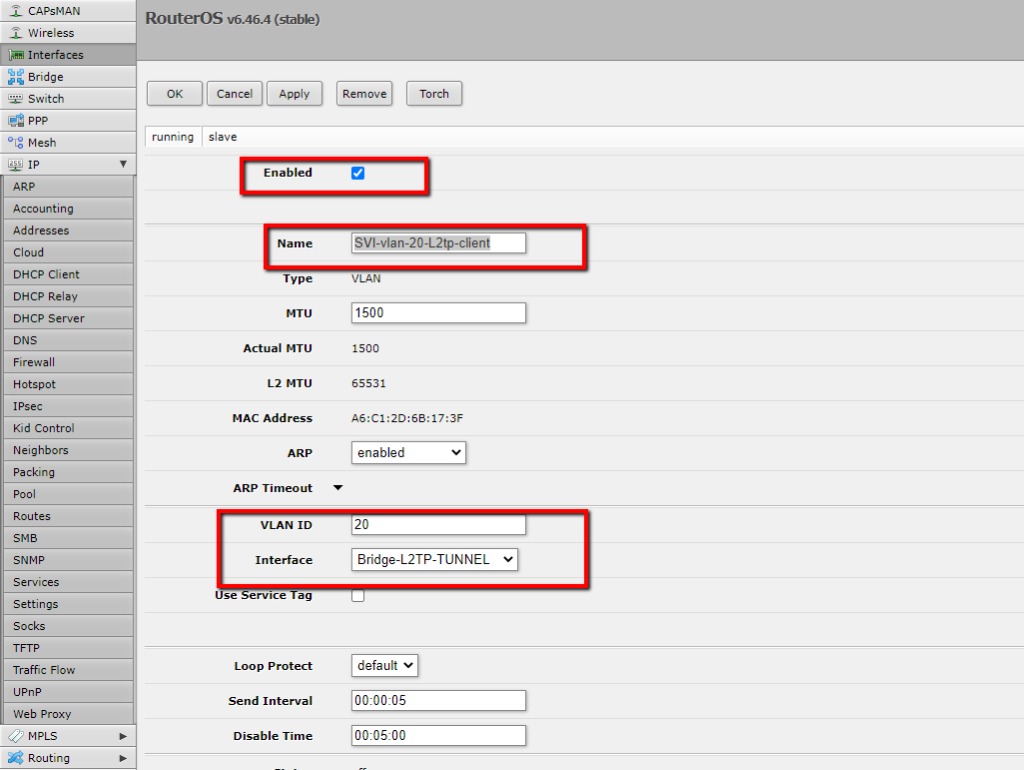


6)  configure the vlan for the wireless client.

* configure two VLAN’s  that will be bridged over the L2TP tunnel.

|  |  |  |
| --- | --- | --- |
| Vlan interface name | Vlan id | Attach to interface |
| SVI-vlan-10-L2tp-client | 10 | Bridge-L2tp-Tunnel |
| SVI-vlan-20-L2tp-client | 20 | Bridge-L2tp-Tunnel |



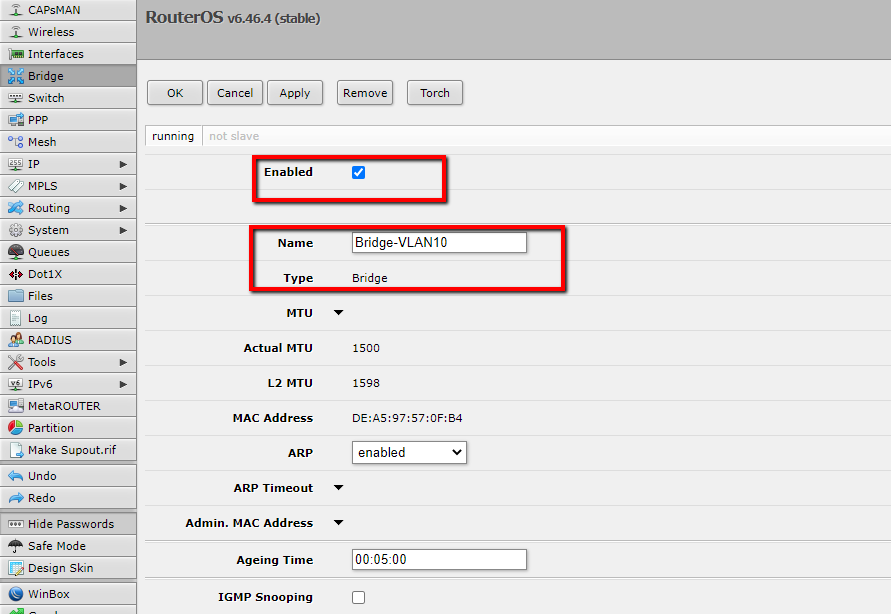


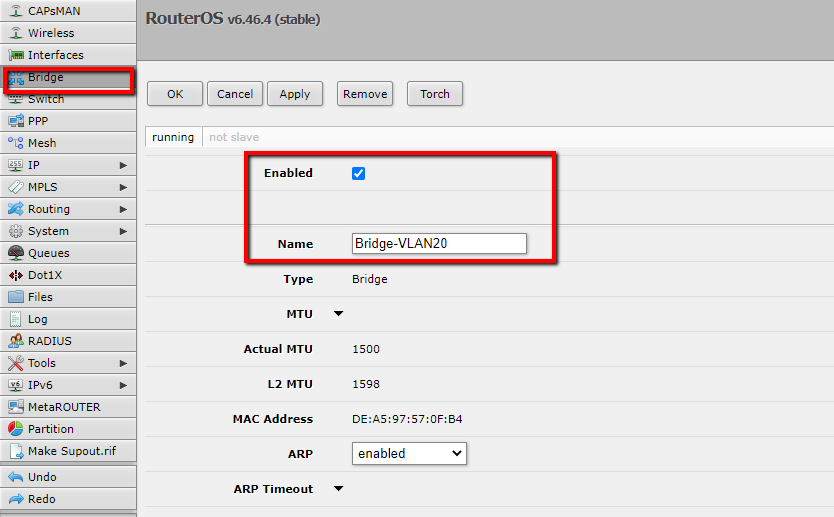
 7) create a bridge  interface for both the client vlan and add ports

      SVI-VLAN-10 mapped to eth2 interface

      SVI-VLAN-20 mapped to eth3 interface.

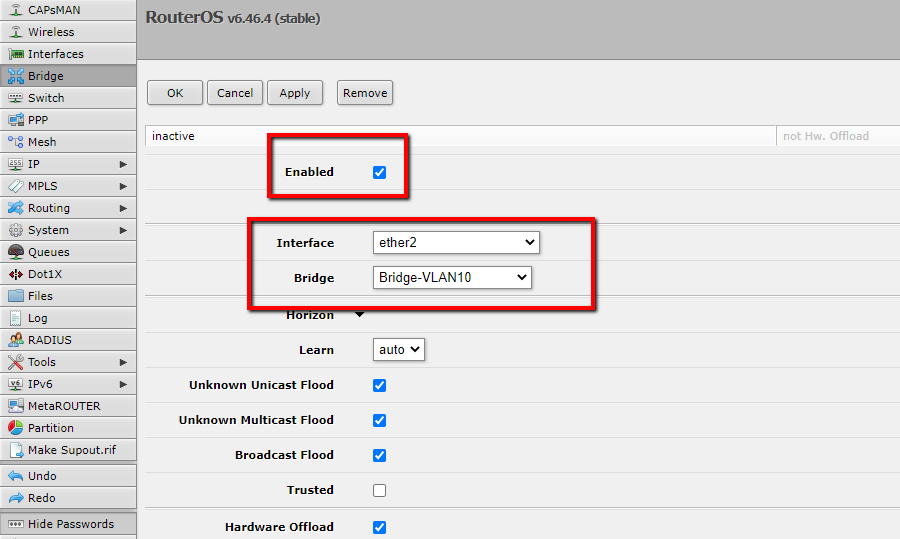
     Go to Bridge > Add New

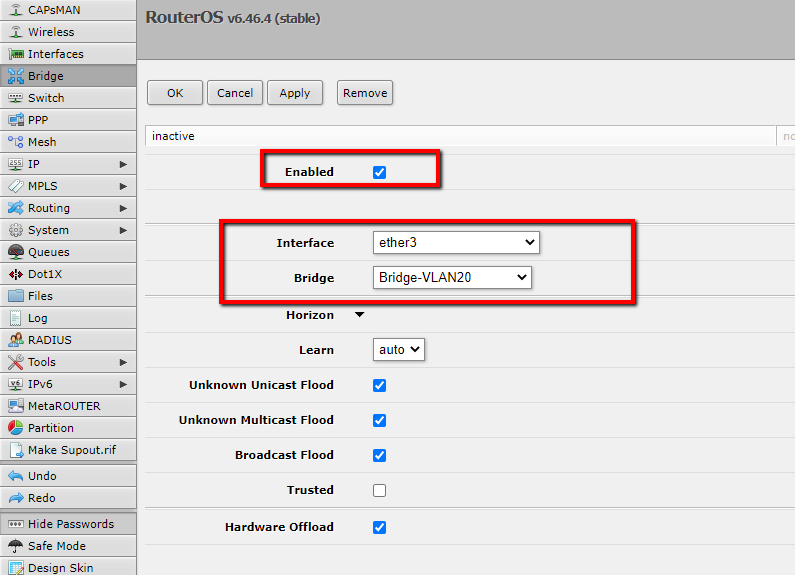




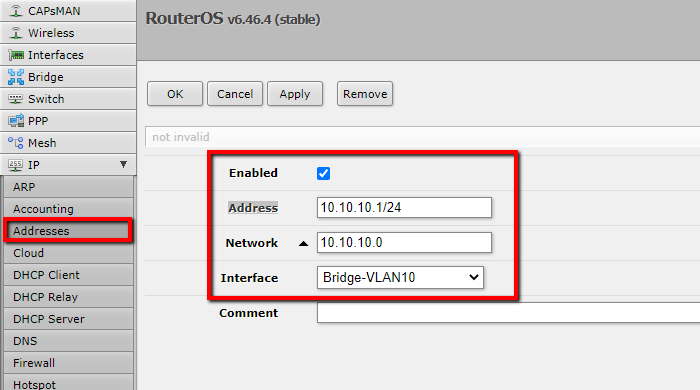
Need to add ports to the bridge interface.

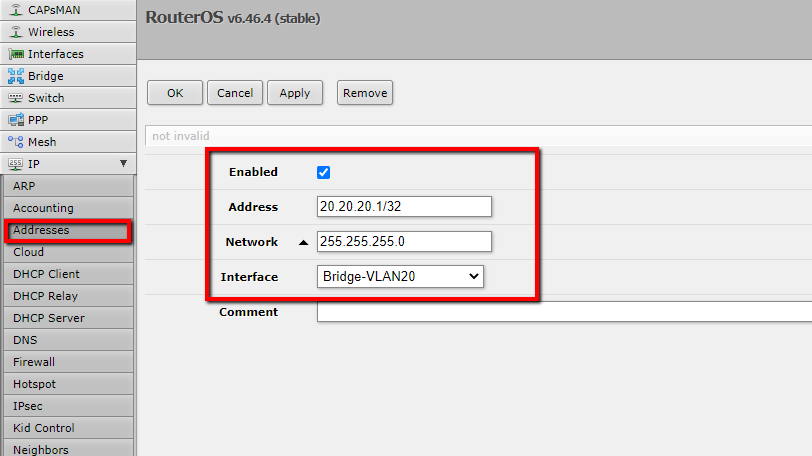
Go to Bridge > ports> Add New.





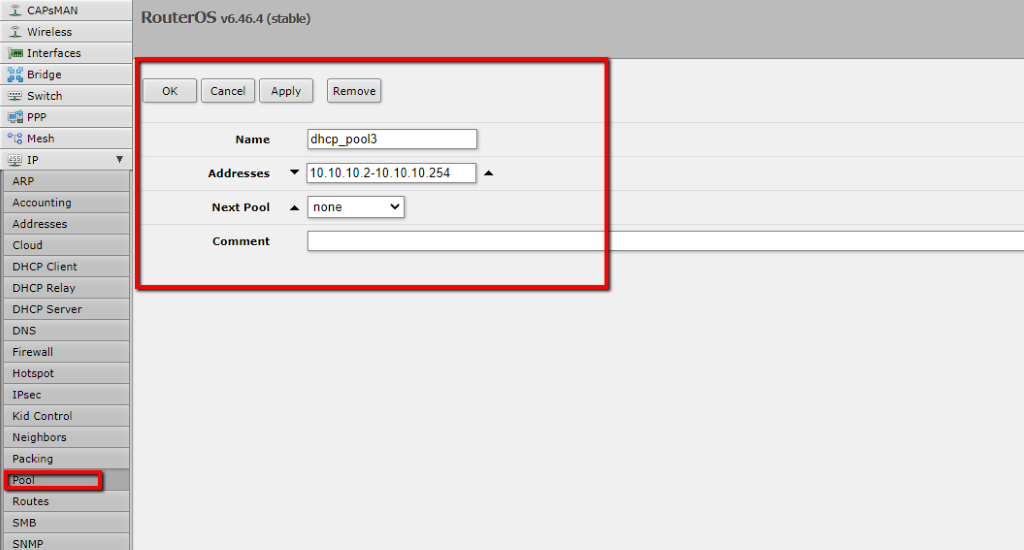
8) Assign ip address to the vlan interface and run dhcp server .

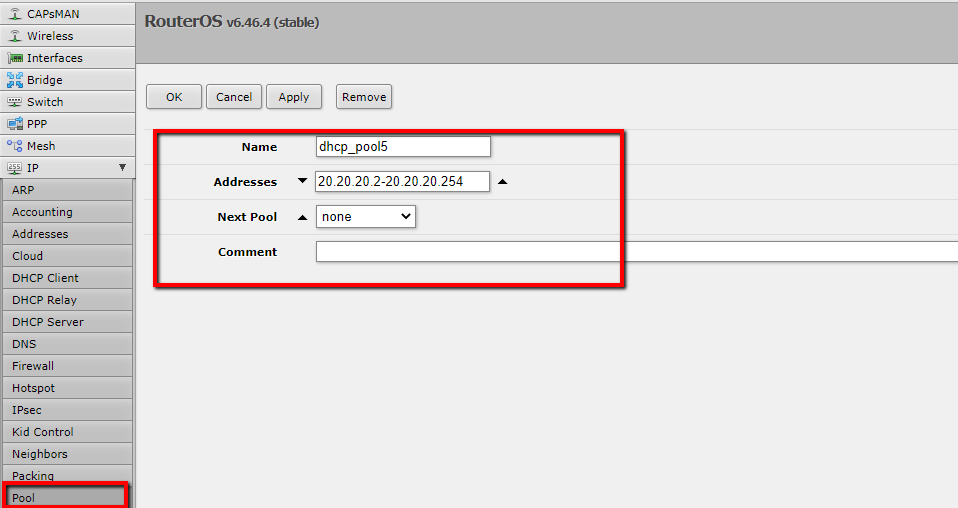




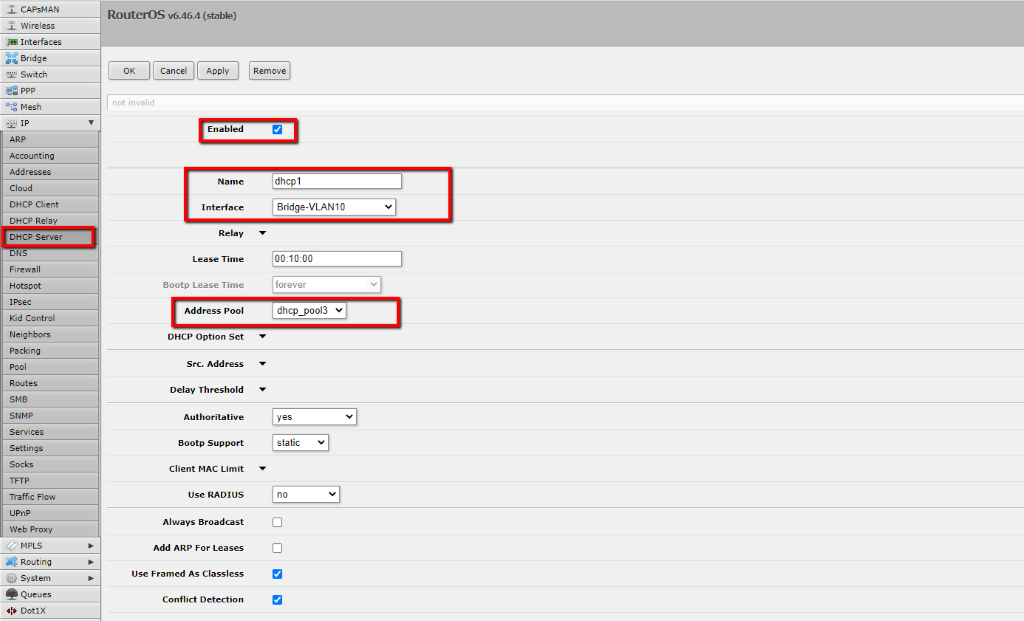
Configure dhcp pool.

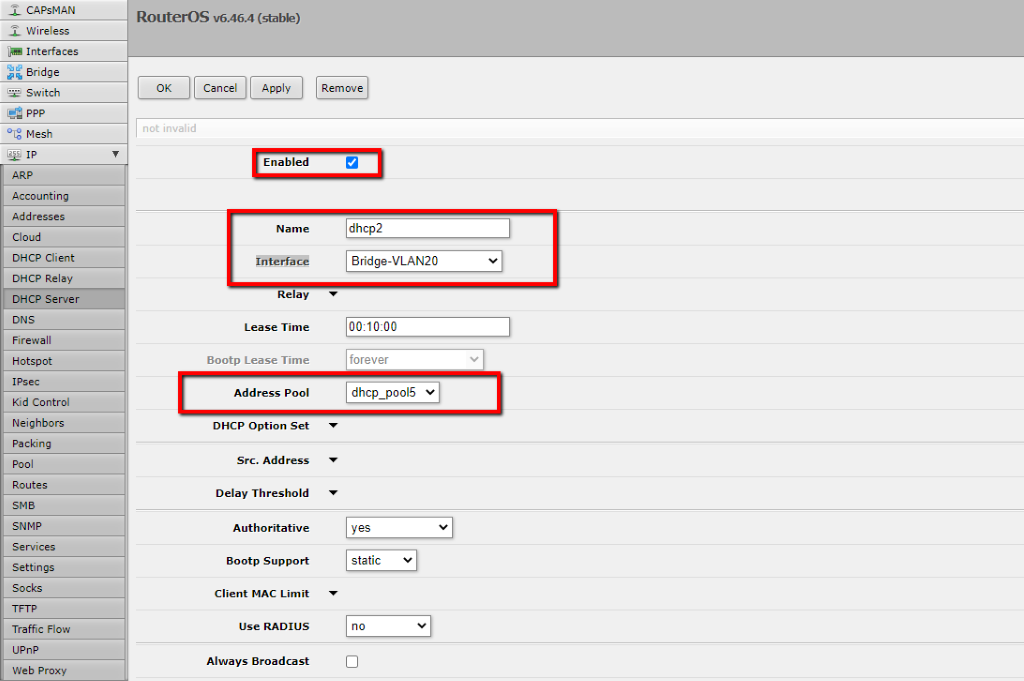
Click on IP > POOL > Add New.





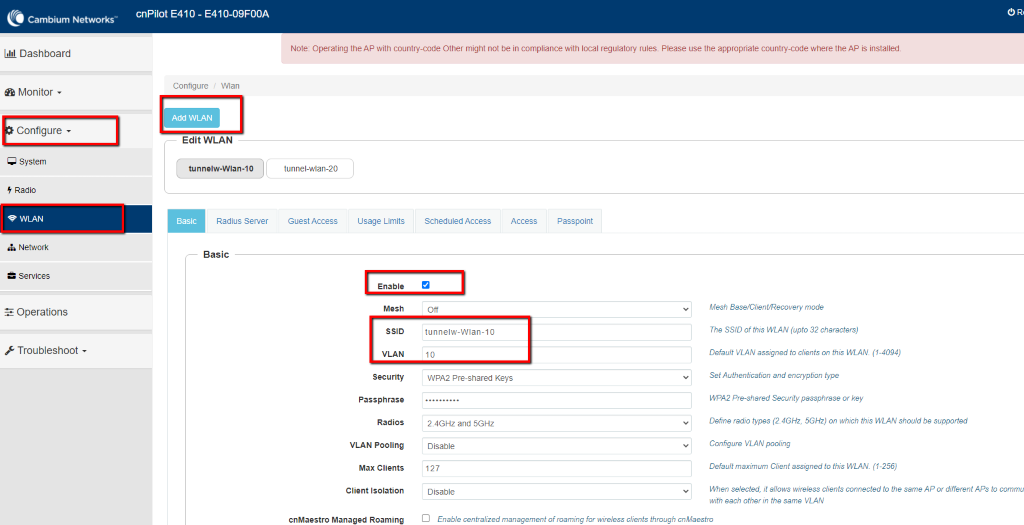
Attach the dhcp pool to the interface.

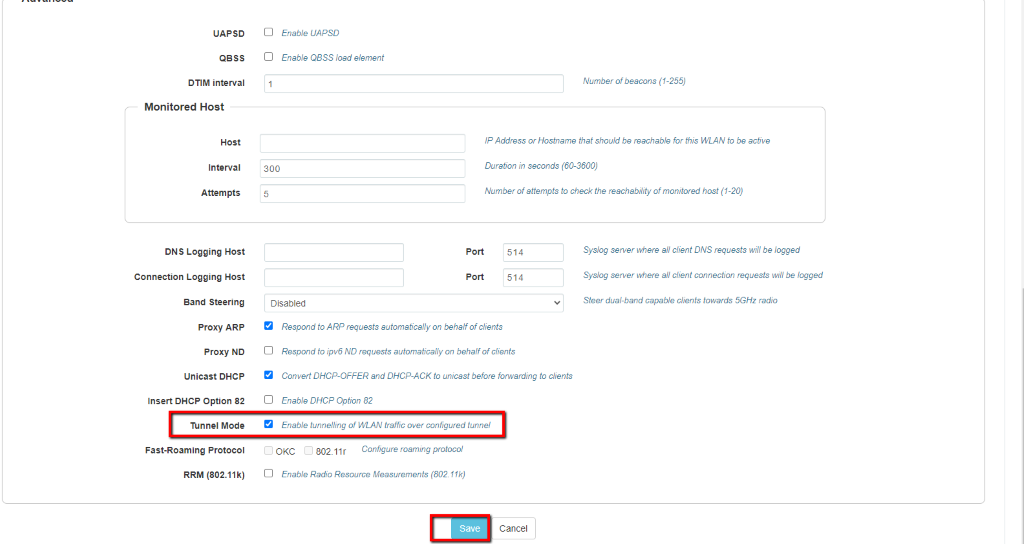


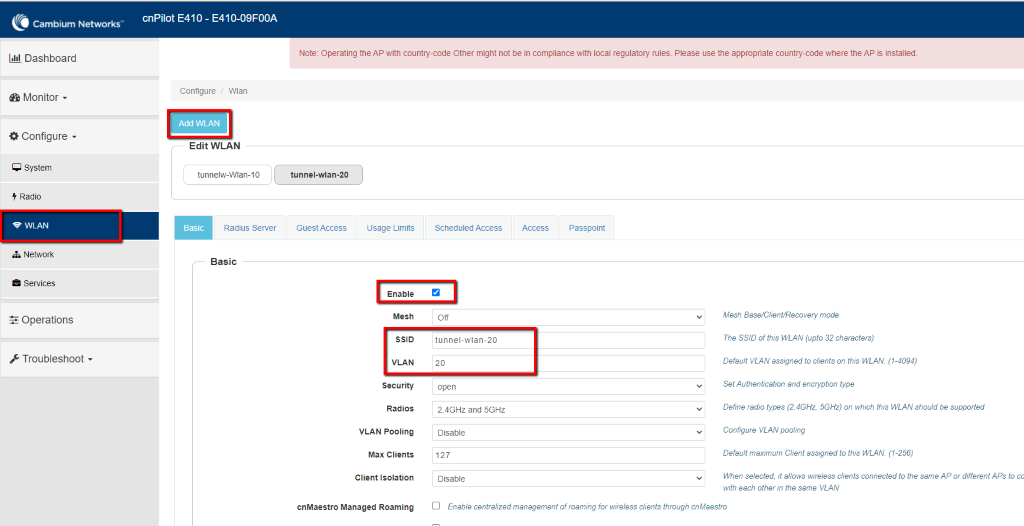


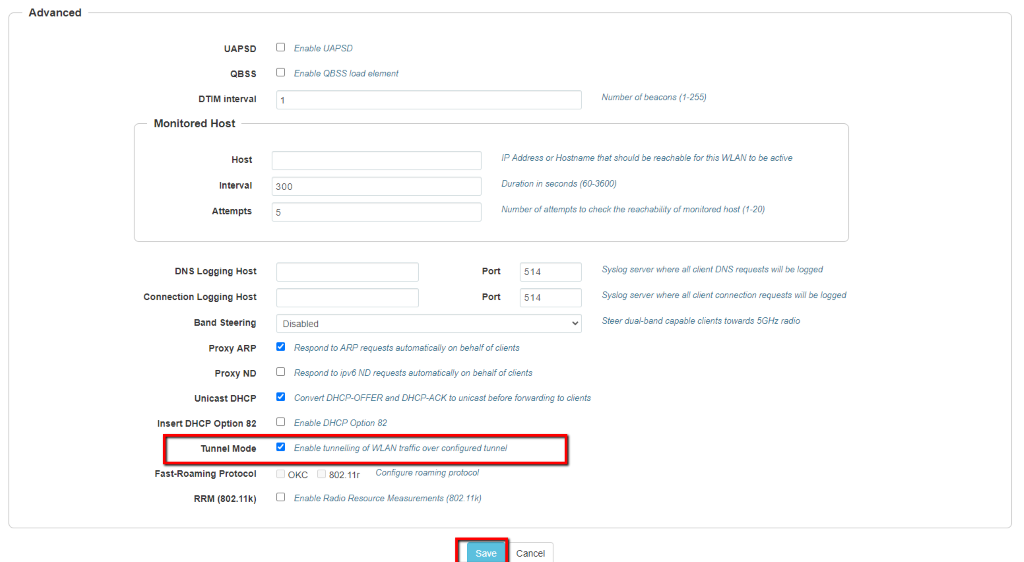
Configuration on cnPilot AP.

Go to configure > Wlan> Add wlan.









Configure L2tp tunnel on cnPilot

Go to configure >Network > Tunnel

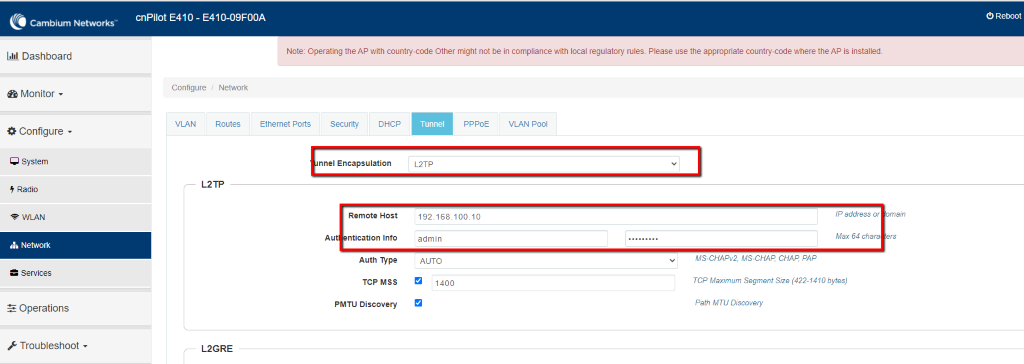
Select l2tp from the dropdown of tunnel ecapsulation.

Type the peer Mikrotik router ip address

Type the authentication username/password for L2tp

Admin/Secret123

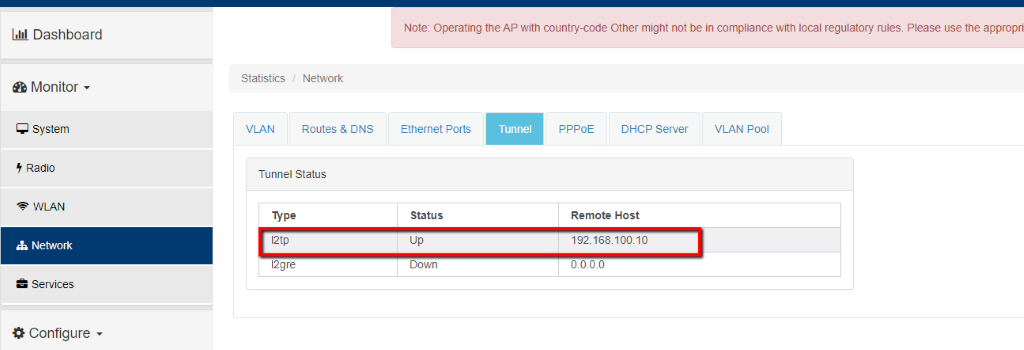
Save the configuraion



## Check the status of L2tp tunnel on AP.

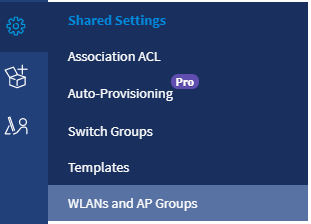
Go to Monitor> Network> Tunnel.

The tunnel status should be “UP”



## Same configuration can also be done from cnMaestro.

Go to shared settings > wlans and AP group.

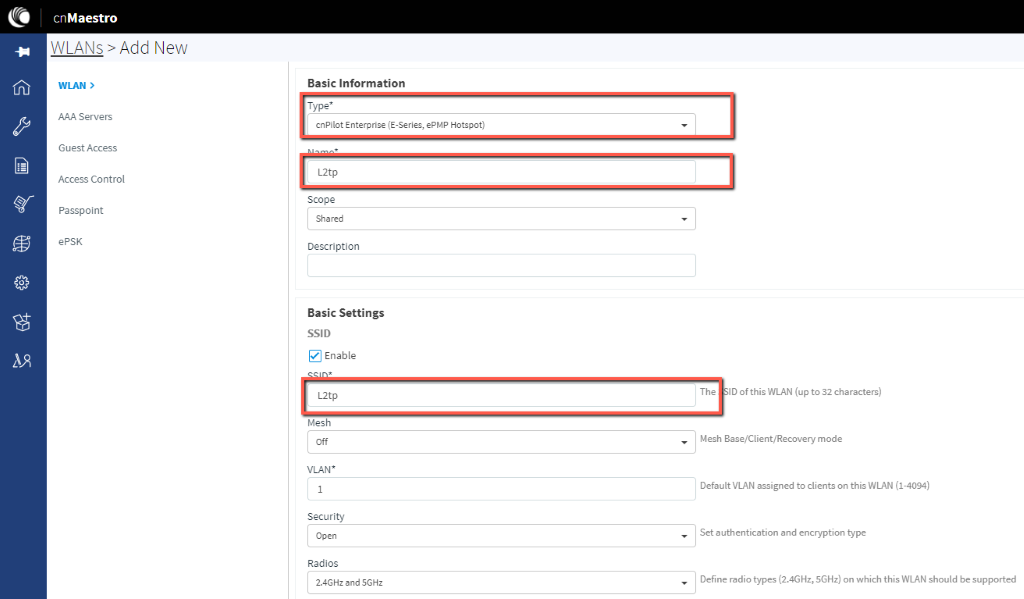


  Create a new Wlan group.

In the type drop down menu , select Eseries , epmp

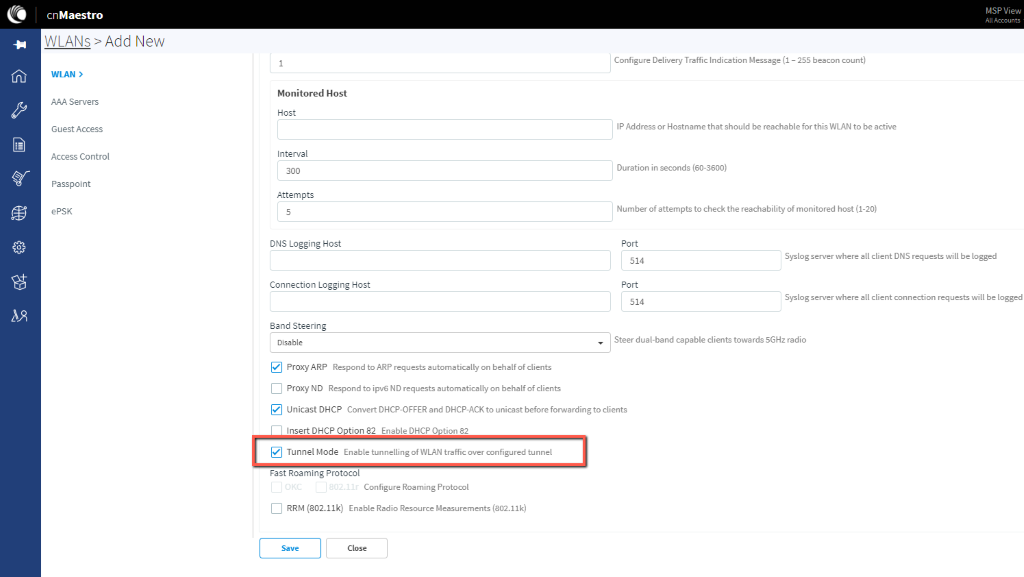
Type the name of the wlan group.

Type the name of the ssid and map the vlan id that needs to be tunneled.



Enable tunneling of user traffic on wlan. Scroll down and click on Advanced.

Check the box “enable tunnel mode”.   save the configuration.



Create a new AP group.

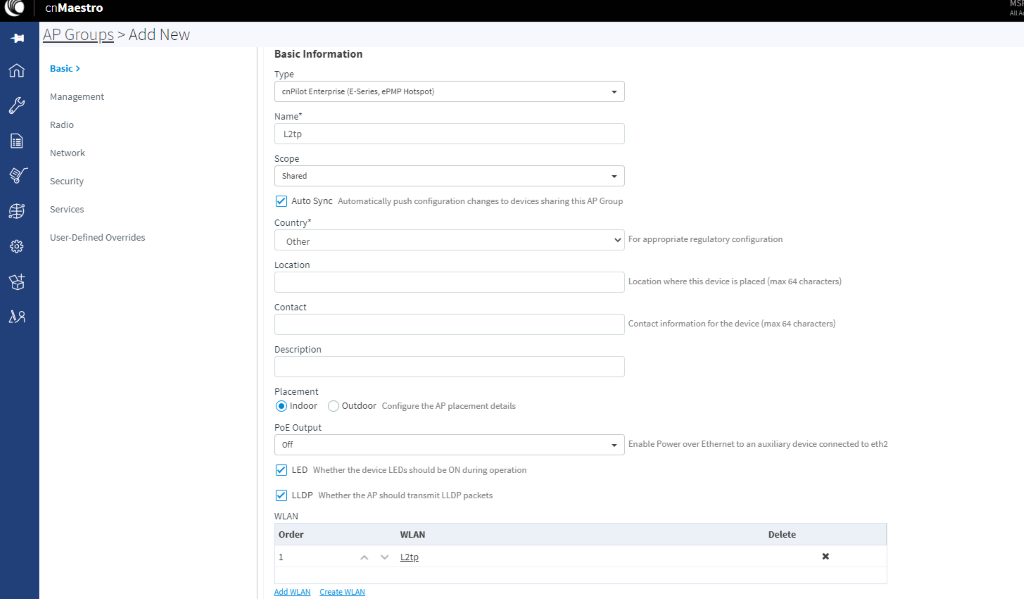
Go to shared settings > wlans and AP group.

Click on AP group tab and click “New AP group.”

From the Type drop down select “ Eseries and ePMP”

Type the name of the AP group and in country select the country based on location.

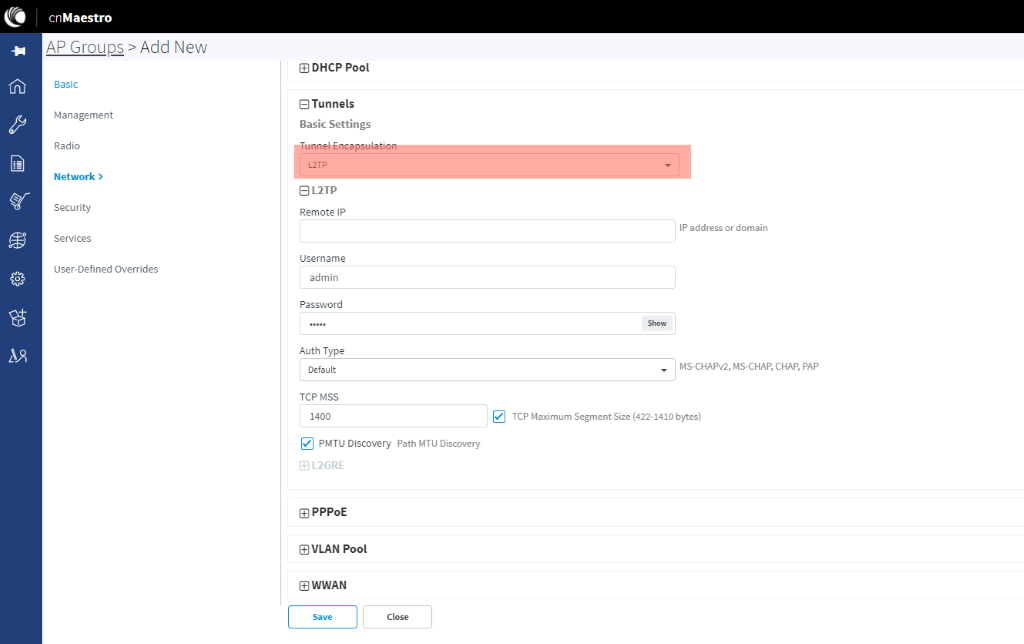
In the wlan section , click add wlan and attached the wlan which was created above.



Go to Network in the left-hand side, Expand tunnels

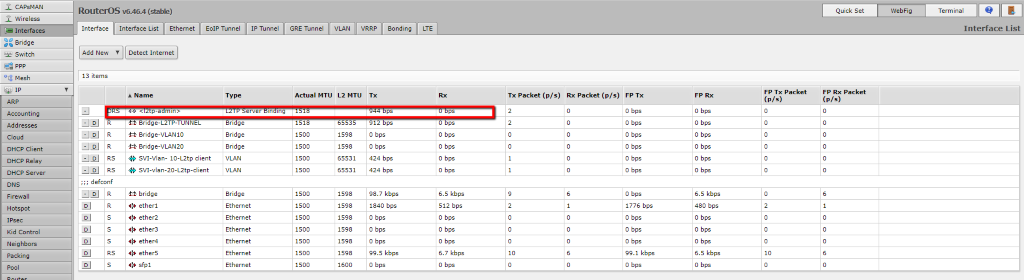
In the tunnel encapsulation select L2tp.

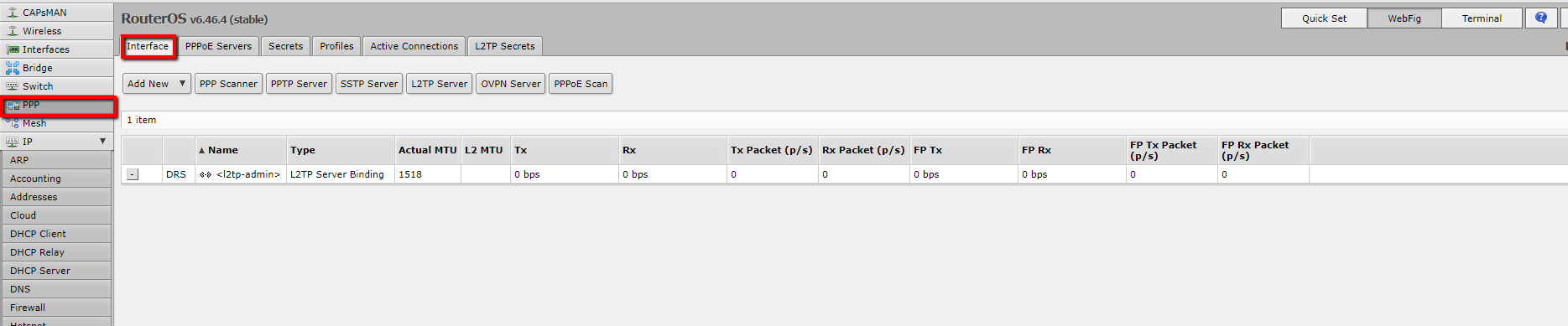
Configure the remote ip address , username & password and save the configuration.

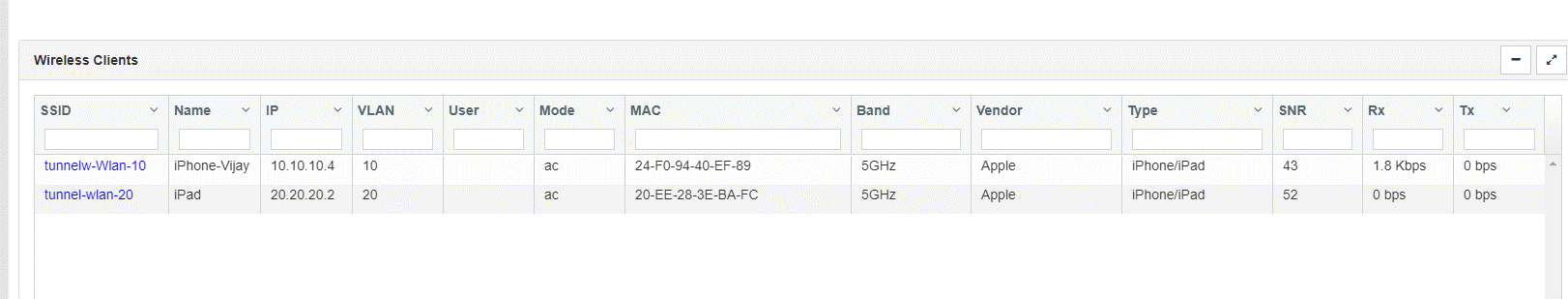


## Tunnel status on Mikrotik**.**

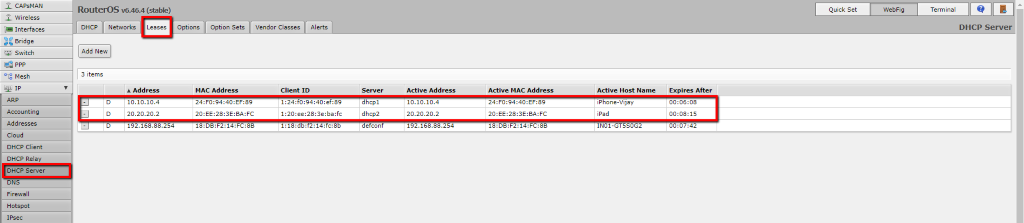
## 







## Dhcp server status on Mikrotik.



## Known Interoperability issues with Mikrotik router

**Problem**

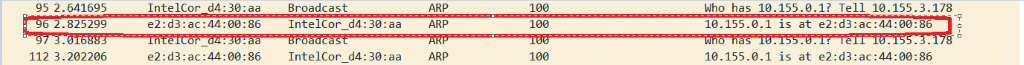
It is observed that whenever the l2tp tunnel is terminated from Mikrotik router, the tunnel is teared  and re-establish. However, after the tunnel is established, the mikrotik router is not able to reach the host behind the cnpilot AP connected to the tunneled wlan.

Please note, this issue will only occur if the client isolation feature is enabled network wide on the cnPilot AP because it caches the gateway mac address on the AP and allows communication between wireless client and gateway and restrict communication from wireless client  to any other mac address on the network.

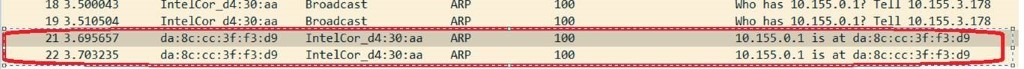
**Root cause analysis.**

After analyzing the packet capture on the access point, we figured out that if tunnel tears down from mikrotik and re-establishes, the mac address of the bridge interface (which is tunneled inside L2tp) on Mikrotik changes. This is because the bridge interface has a default config of  auto-mac  which is enabled . This feature changes the mac address of the bridge interface if the tunnel terminates and re-establishes.

 In the  below packet capture,  the gateway ip is 10.155.0.1 . It reflects the mac address of the gateway before tunnel termination.



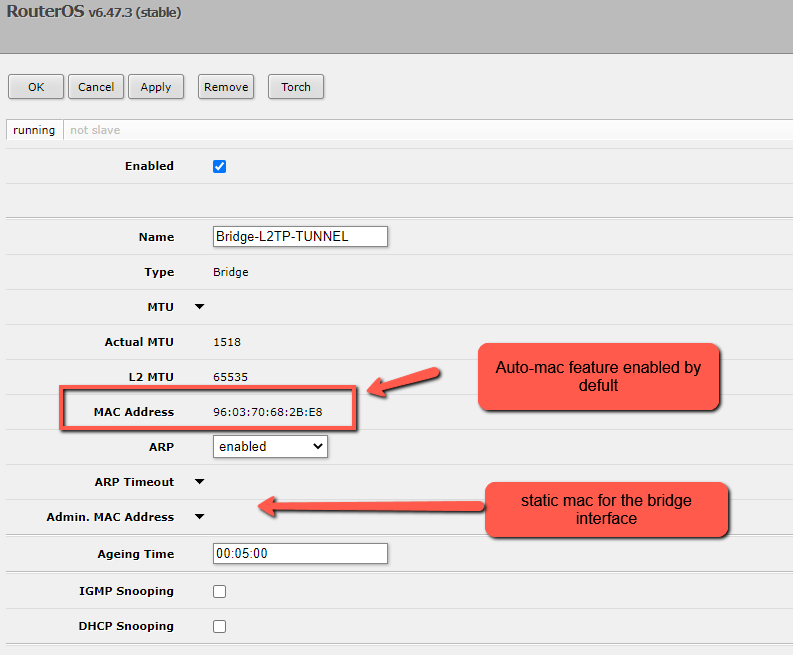
The below capture reflects the mac address of the gateway after tunnel termination.



As you can see the gateway mac is changed. Since client isolation feature is enabled on AP, any traffic originated from this bridge interface will be dropped by AP because the cache on AP is not updated with the new mac of gateway.  The cache on the AP is updated from the dhcp offer packet received form the mikrotik. As the wireless client does not disconnect from the AP, it will not send any dhcp discover to get an offer in reply due to which the cache on the AP will not get updated.

**Solution**

We recommend network administrator to disable auto-mac feature on bridge interface and instead configure the static mac in the field “**admin mac address ”**



## Scalability

Scalability of the L2tpv2 tunnel concentrator depends on Mikrotik model number.

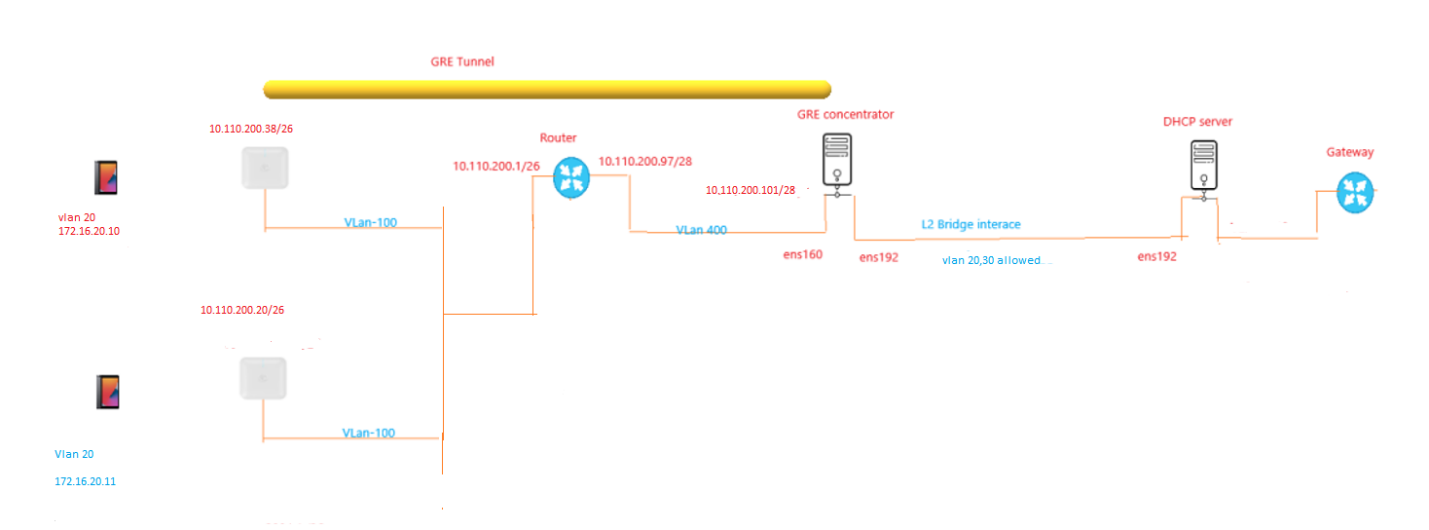
The max number of L2tpv2 tunnel supported on a Mikrotick router can be obtained from the Mikrotik website.

# Setting up EoGRE Tunnel between Cambium cnPilot and Ubuntu

Ubuntu Version.

Please use the latest version 20.04 but the same command can also work on 18.04 or 16.04.

## Topology diagram.



Topology details.

* AP connect to the Management vlan.
* AP is configured with a wlan which is in tunnel mode and mapped to vlan 20.
* Dhcp for vlan 20 is running beyond the gre concentrator.
* Once the configuration is applied, AP sets up GRE tunnel with the concentrator.
* After that client connects to the wlan, it sends a dhcp discover packet
* The AP receives the  dhcp discover packet and encapsulates it with GRE header and sends it to the GRE concentrator.
* After receiving the encapsulated packet , GRE concentrator removes the GRE header and checks the dot1q vlan header and bridges it to the dhcp server.
* Dhcp server does lookup in pool of vlan 20 and then responds with an offer packet, the gre concentrator encapsulate the offer packet with GRE Header and sends it to the AP.
* Ap after receiving the GRE packet, removes the gre header and sends the packet in vlan 20.
* Now the client receives the dhcp offer packet and does the remaining dhcp control packet exchange.
* Once the client is assigned the ip address, it can reach the default gateway.

## Ubuntu server configuration

*ip link add l2gre1 type gretap remote 10.110.200.38 local 10.110.200.101 ttl 255*

*ip link add l2gre2 type gretap remote 10.110.200.20 local 10.110.200.101 ttl 255*

*NOTE : For every remote AP , you need add the IP link add command in the linux gre concentrator.*

*ifconfig l2gre1 up*

*ifconfig l2gre2 up*

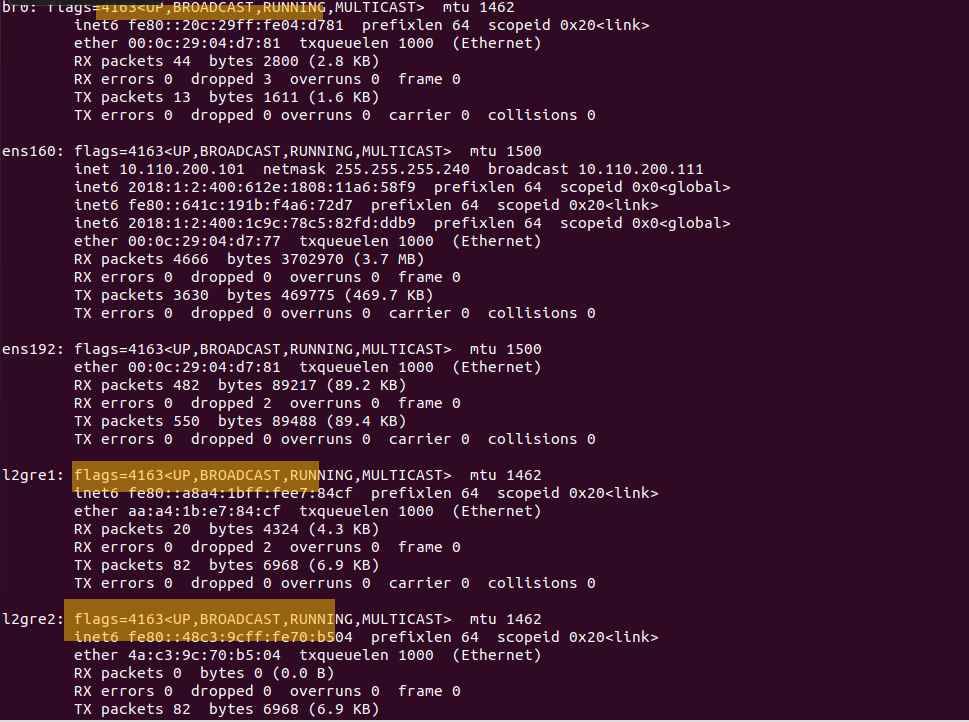
*brctl addbr br0*

*brctl addif br0 l2gre1*

*brctl addif br0 l2gre2*

*brctl addif br0 ens192.*

*ifconfig br0 up*



## AP configuration for Eogre tunnel.

NOTE: Same configuration needs to be applied on both AP1 & AP2.

*!*

*wireless wlan 2*

*ssid "11GRE tunnel-legacy"*

*no shutdown*

*vlan 1020*

*security wpa2-psk*

*no protected-mgmt-frames*

*passphrase $crypt$1$Alqc48hXt8SHL+yfxLEQVRo2PQVIffwR*

*band both*

*dtim-interval 1*

*wpa-group-rekey-interval 3600*

*max-associated-client 127*

*tunnel-mode*

*network-policy-id 0*

*mac-authentication policy deny*

*passpoint interworking access-network-type private*

*no guest-access*

*!*

*!*

*tunnel encapsulation l2gre*

*!*

*tunnel l2gre*

*remote-host 10.110.200.101*

*pmtudisc*

*dscp 0*

*mtu 1460*

*tcp-mss 1410*

*no gre-in-udp*

*no cambium-gre*

*!*

*pppoe server*

*shutdown*

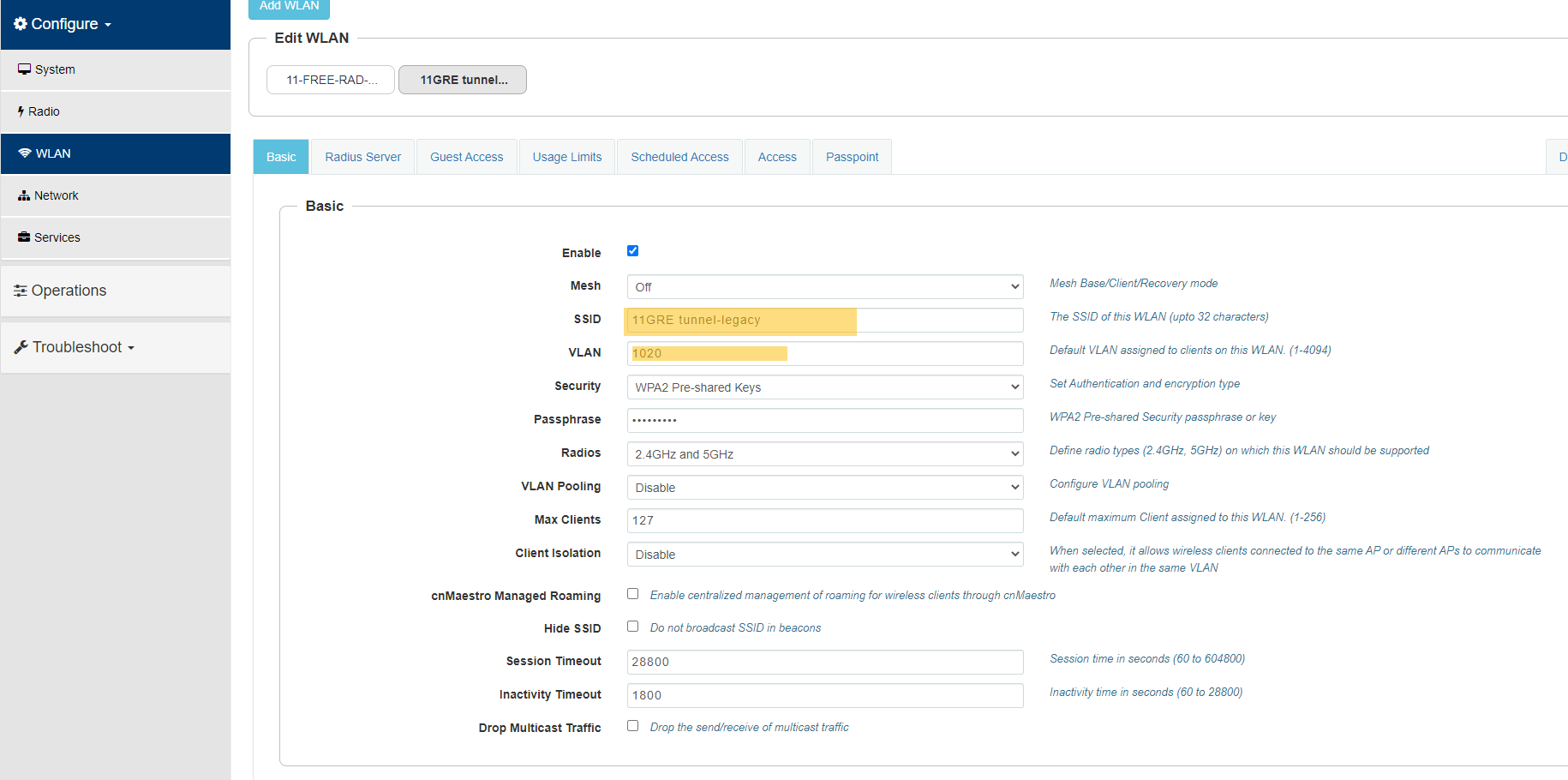
*tcp-mss-clamp*

*management-access*

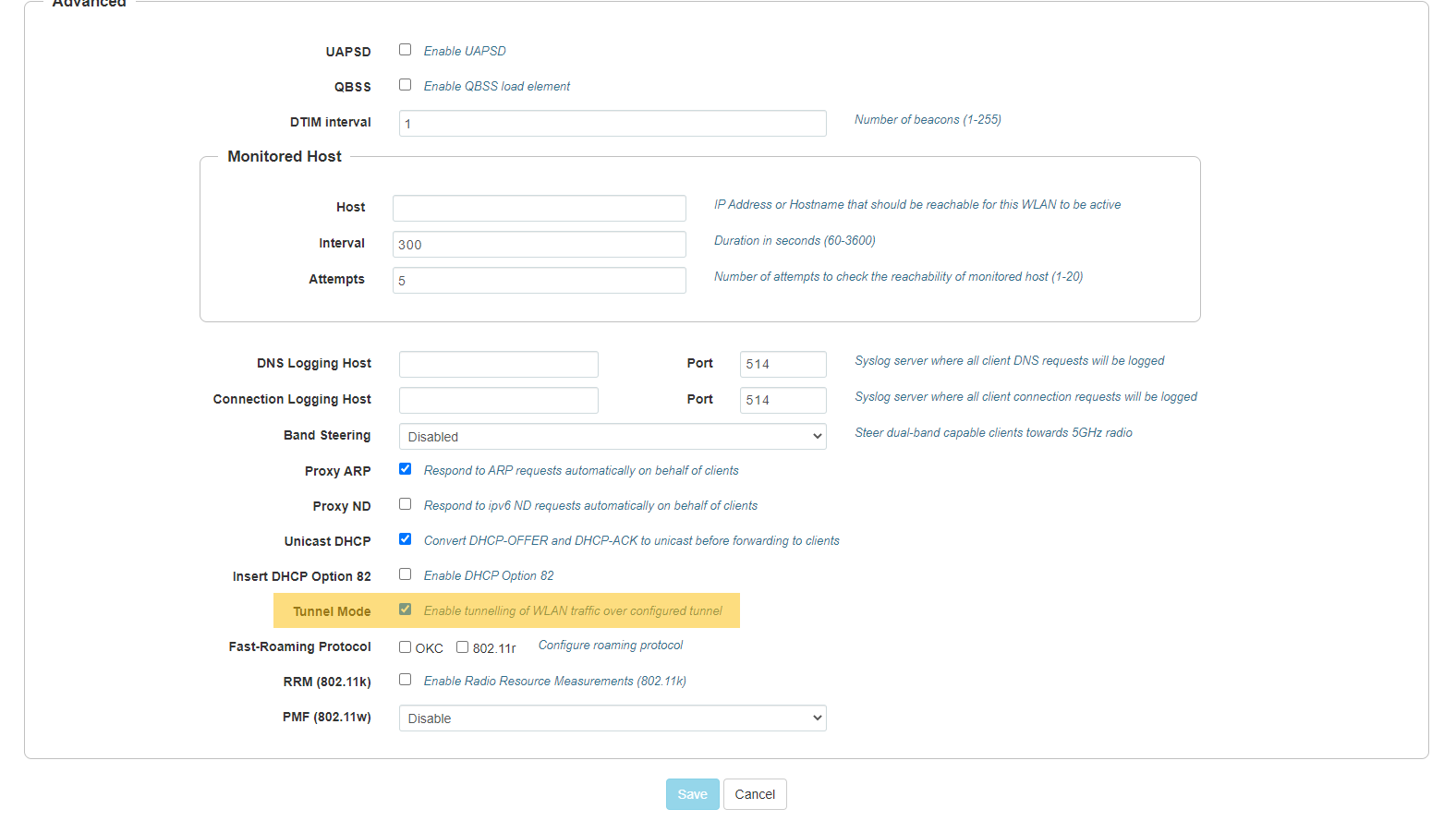
*!*

## AP UI configuration.

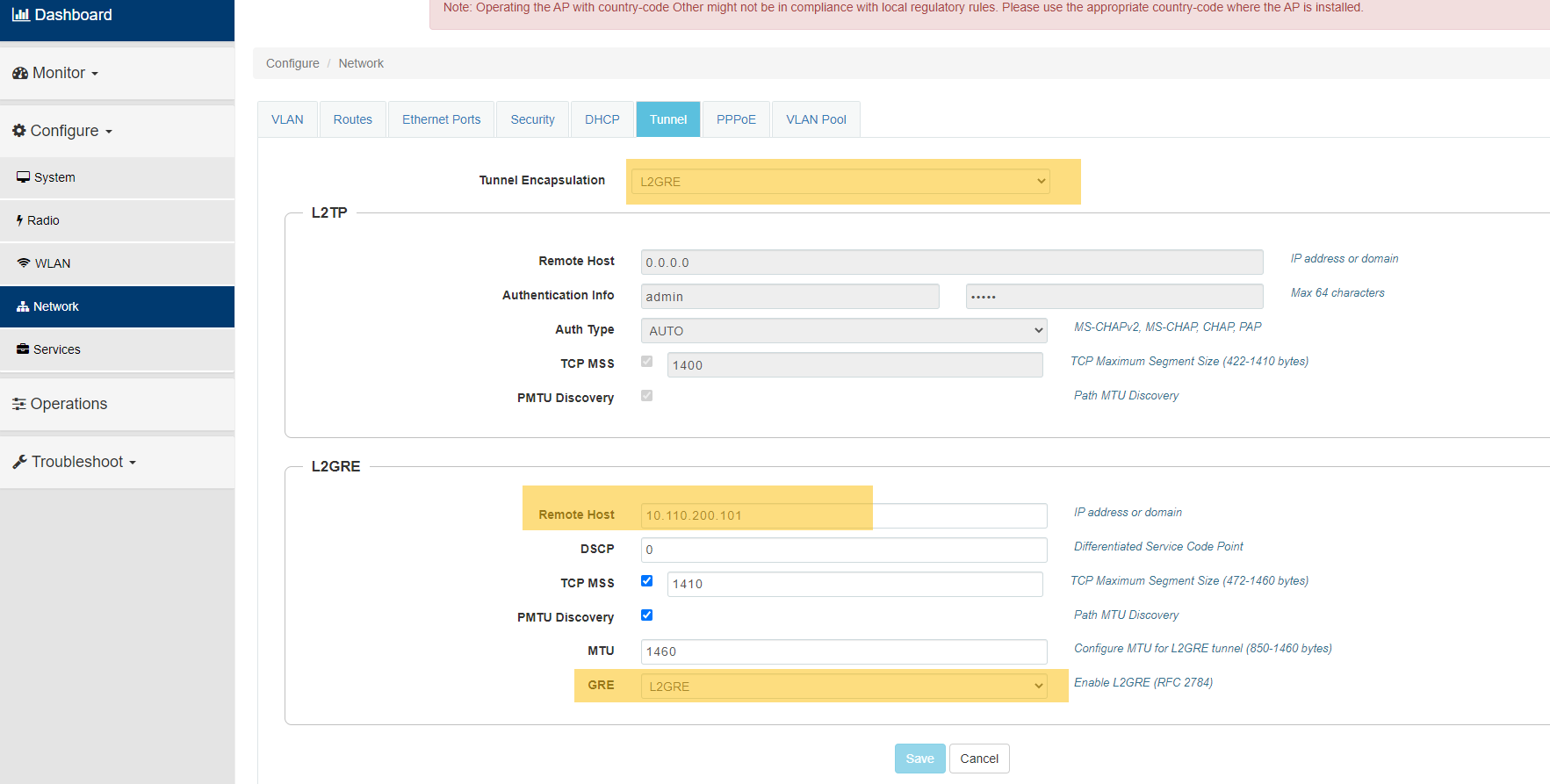
*Configure Wlan*



*Enable tunneling mode.*



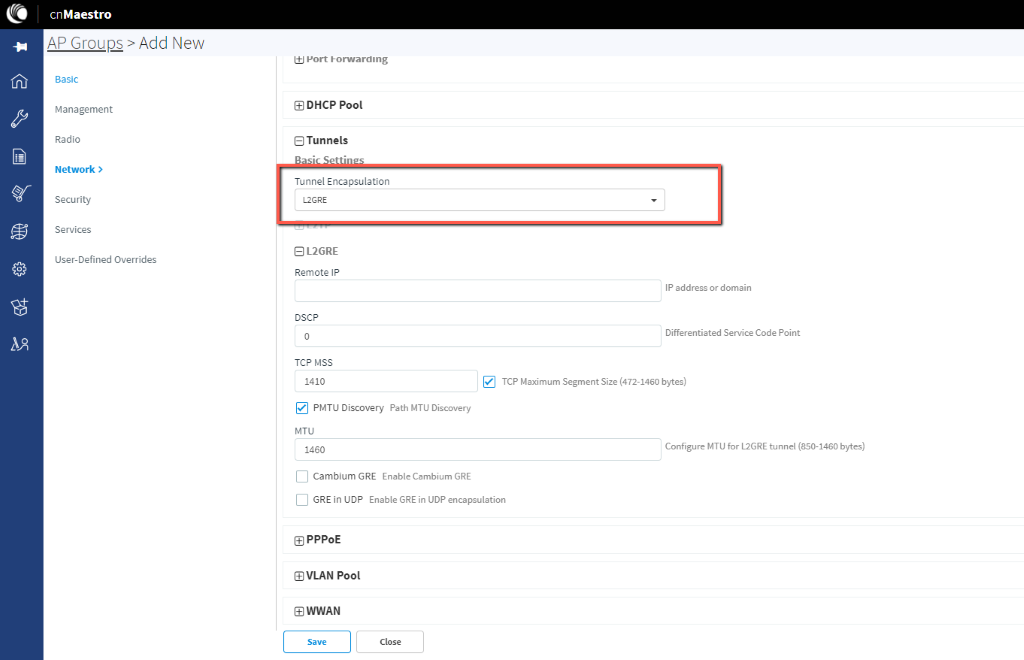
## Configure the GRE tunnel.



## Same configuration can also be done from cnMaestro.

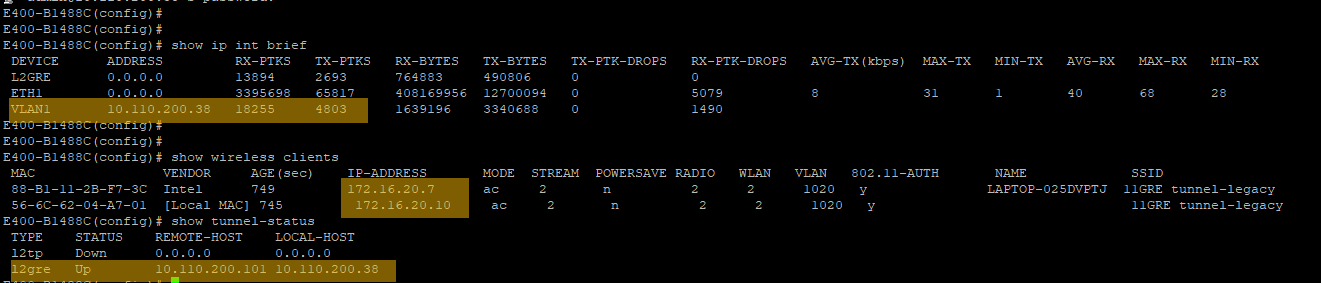
# 

# 

**

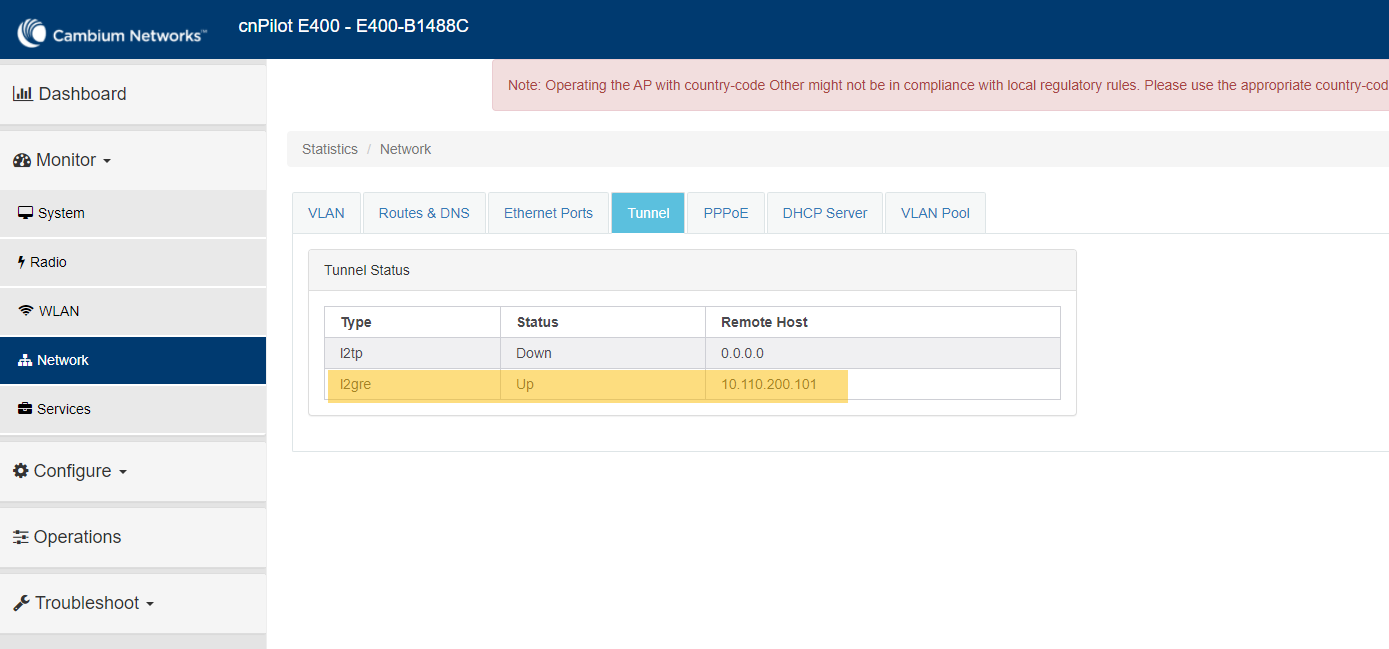
## AP statistics.

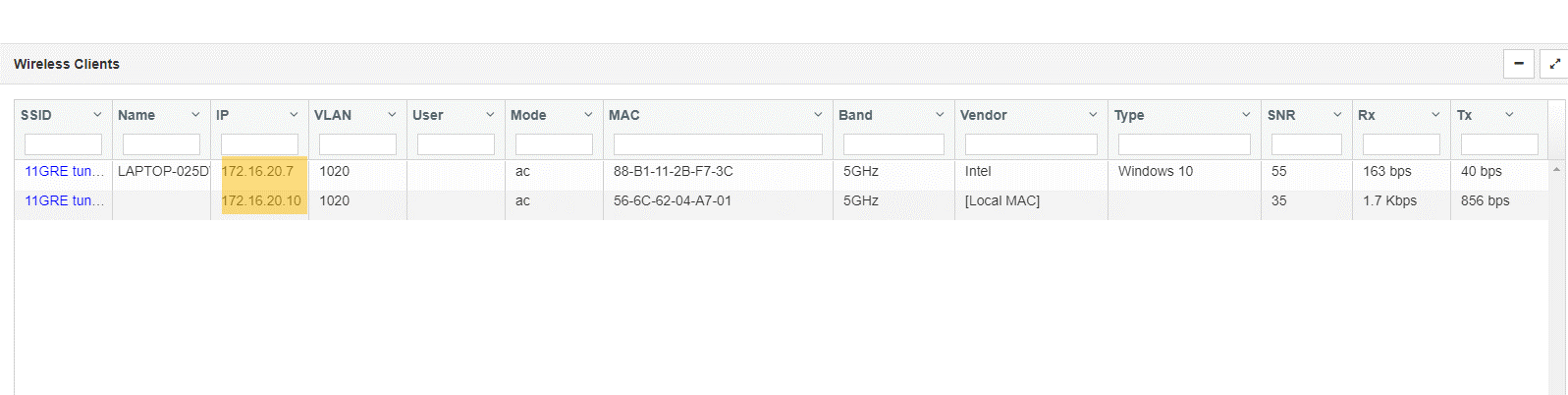
## Cli statistics.



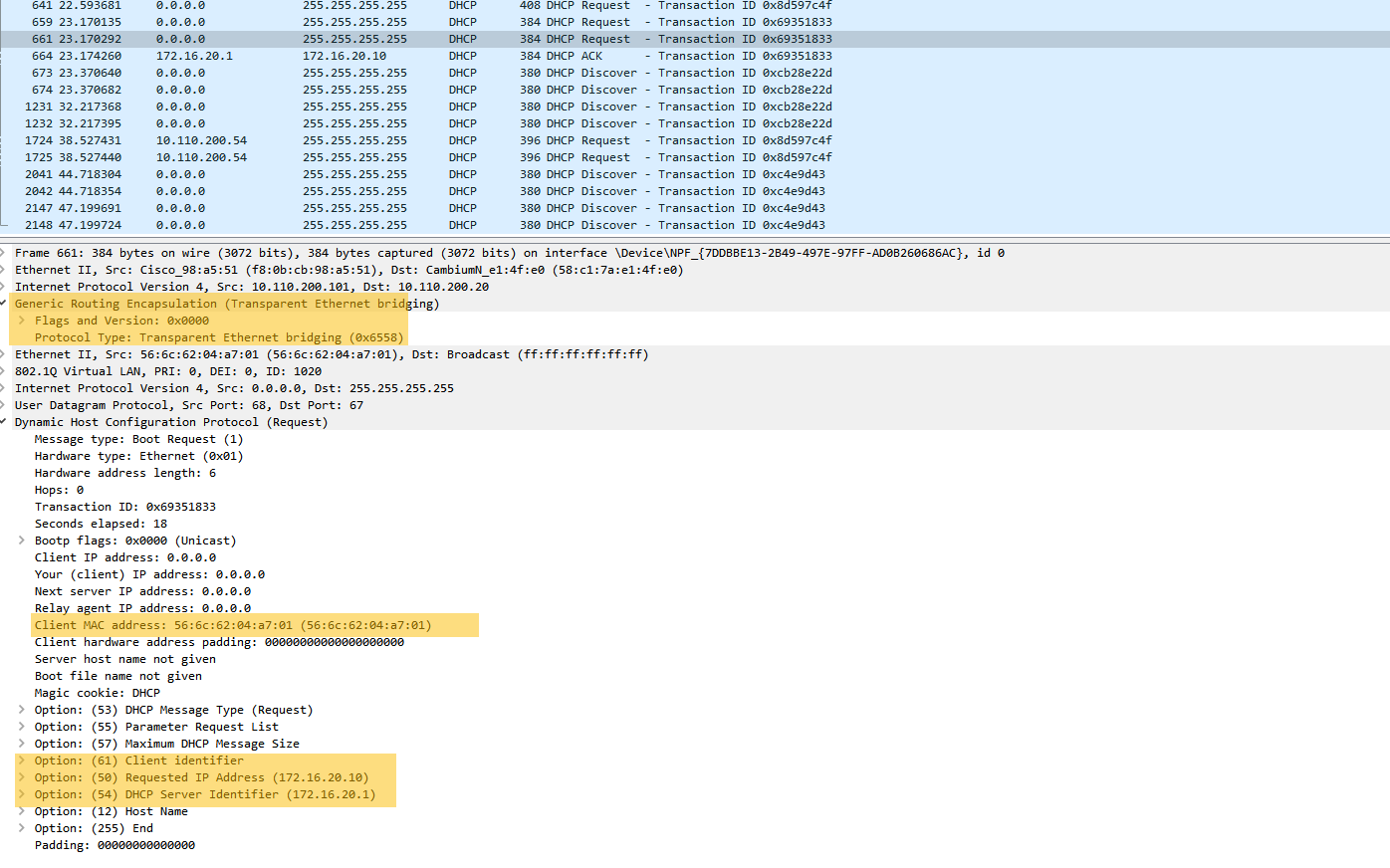
Same stats will be available on AP2.

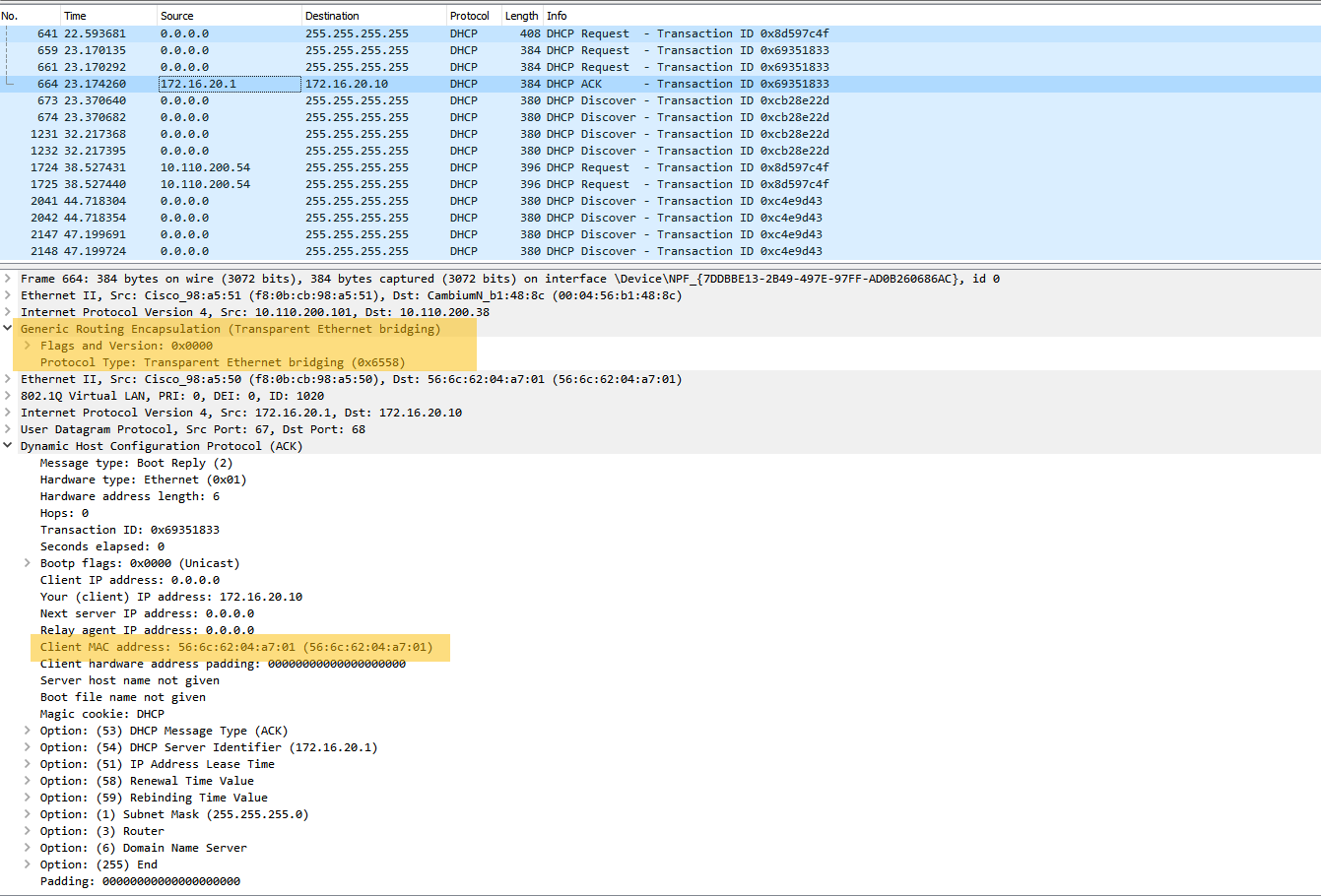
## AP UI statistics.

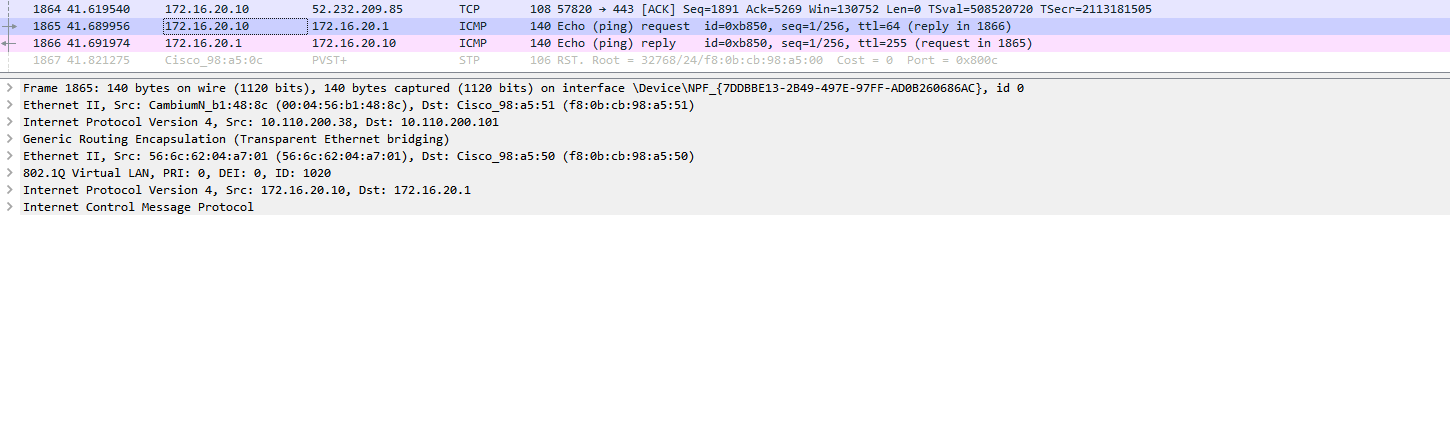




## GRE Packet capture







NOTE

Scalability of the GRE tunnel concentrator depends on the hardware configuration. Ap only supports one tunnel at a time.