

Manual:CAPsMAN with VLANs

From MikroTik Wiki

Contents

- 1 Summary
- 2 Using Local Forwarding Mode
 - 2.1 CAPsMAN Router
 - 2.2 Switch
 - 2.3 CAPs
- 3 Using CAPsMAN Forwarding Mode
 - 3.1 CAPsMAN Router
 - 3.2 CAPs
- 4 Case studies
 - 4.1 Without Virtual APs

Applies
to



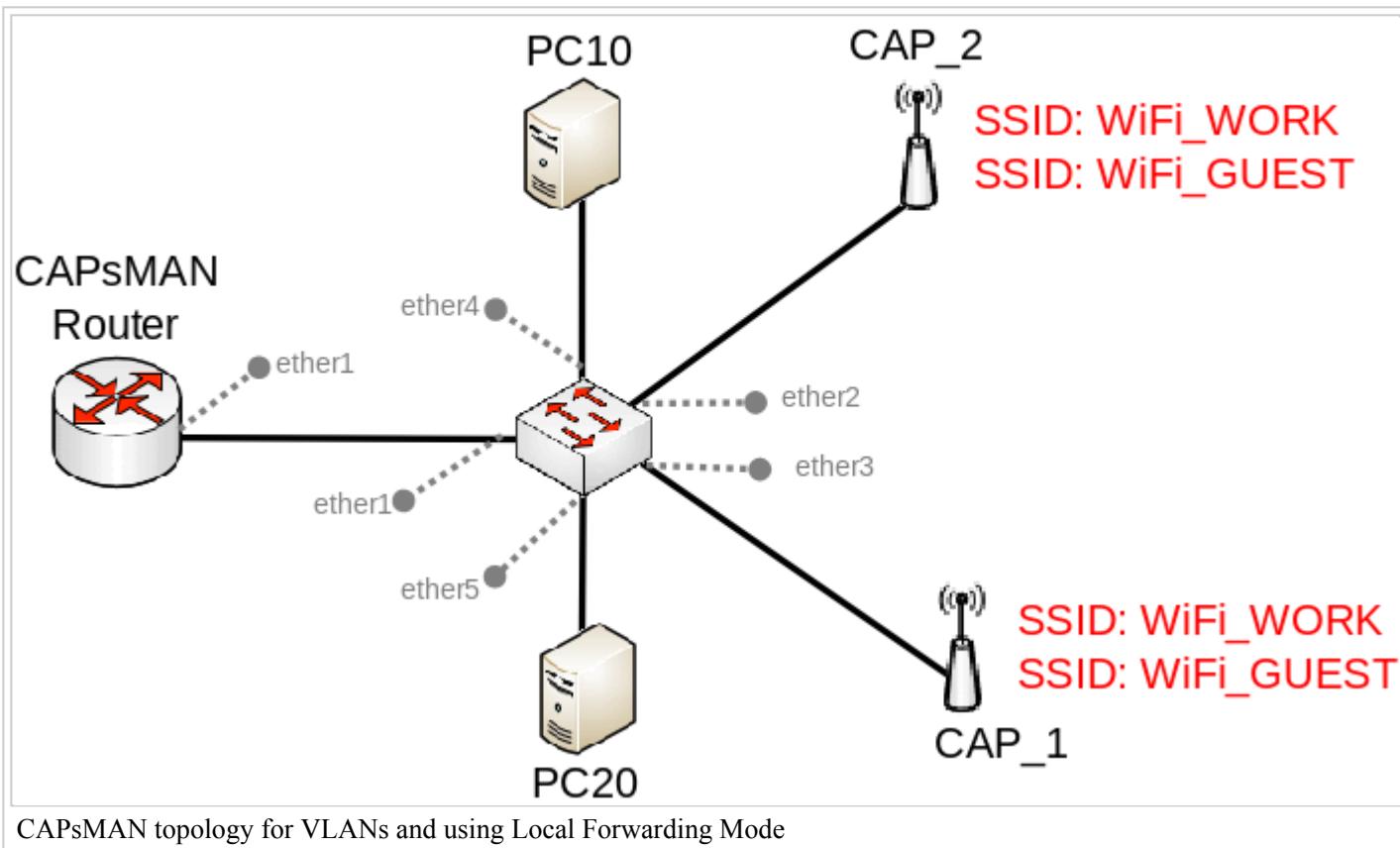
RouterOS: v6.41 +

Summary

It is possible to create centralized Access Point management setup for home or office environment that is scalable to many Access Point, such a setup is quite easy to configure and has been explained in the Simple CAPSMAN setup guide, but for more complex setups VLANs might be required. CAPsMAN has a functionality to assign a certain VLAN ID under certain conditions. This guide will provide an example how assign a VLAN ID to Wireless packets based on the AP, to which a Wireless client connects to. CAPsMAN with VLANs can be achieved either by using Local Forwarding Mode or CAPsMAN Forwarding Mode, the Local Forwarding Mode will provide the possibility to use a switch between your APs and CAPsMAN router to switch packets (to achieve larger throughput), while CAPsMAN Forwarding Mode should be used when all traffic should always be forwarded to the CAPsMAN router (in most cases to filter packets).

In this example we are going to assign all our Wireless clients to **VLAN10**, if they connect to **WiFi_WORK**, and going to assign Wireless clients to **VLAN20**, if they connect to **WiFi_GUEST**. We are going to use Virtual APs along with CAPsMAN to create multiple SSIDs for our Wireless clients to connect to while using a single physical device. An example how to use a single SSID for a single physical device will also be shown by using CAPsMAN provisioning rules.

Using Local Forwarding Mode



CAPsMAN topology for VLANs and using Local Forwarding Mode

In Local Forwarding Mode the CAPsMAN router is distributing the configuration across all CAPs that are being provisioned by the CAPsMAN router. In Local Forwarding Mode traffic is not required to be sent to the CAPsMAN router, rather it can be sent to a different router without involving the CAPsMAN router when forwarding traffic. This mode allows you to tag traffic to a certain VLAN ID before it is being sent to your network from your Wireless client, which adds possibilities to use a switch to limit certain VLAN IDs to certain ports. In Local Forwarding Mode traffic is not encapsulated with a special CAPsMAN header, which can only be removed by a CAPsMAN router.

CAPsMAN Router

- Create appropriate CAP configurations for each VLAN

```
/caps-man configuration
add country=latvia datapath.local-forwarding=yes datapath.vlan-id=10 datapath.vlan-mode=use-tag name=Config_WORK
    security.passphrase=secret_work_password ssid=WiFi_WORK
add country=latvia datapath.local-forwarding=yes datapath.vlan-id=20 datapath.vlan-mode=use-tag name=Config_GUEST
    wpa-psk,wpa2-psk security.passphrase=secret_guest_password ssid=WiFi_GUEST
```

- We are going to create a single CAPsMAN provisioning rule to create the **WiFi_WORK** and the **WiFi_GUEST** SSIDs on a single device, each connect CAP is going to create these SSIDs automatically

```
/caps-man provisioning
add action=create-dynamic-enabled master-configuration=Config_WORK slave-configurations=Config_GUEST
```



Note: You can create even more Virtual APs by adding multiple **slave-configuration**s. That requires multiple CAPsMAN configurations that were created earlier.

- For security reasons, limit the CAPsMAN to a single interface

```
/caps-man manager interface
set [ find default=yes ] forbid=yes
add disabled=no interface=ether1
```

- Enable the CAPsMAN manager

```
/caps-man manager
set enabled=yes
```

- Setup DHCP Server for each VLAN

```
/interface vlan
add interface=ether1 name=VLAN10 vlan-id=10
add interface=ether1 name=VLAN20 vlan-id=20
/ip address
add address=192.168.10.1/24 interface=VLAN10
add address=192.168.20.1/24 interface=VLAN20
/ip pool
add name=dhcp_pool10 ranges=192.168.10.2-192.168.10.254
add name=dhcp_pool20 ranges=192.168.20.2-192.168.20.254
/ip dhcp-server
add address-pool=dhcp_pool10 disabled=no interface=VLAN10 name=dhcp10
add address-pool=dhcp_pool20 disabled=no interface=VLAN20 name=dhcp20
/ip dhcp-server network
add address=192.168.10.0/24 dns-server=8.8.8.8 gateway=192.168.10.1
add address=192.168.20.0/24 dns-server=8.8.8.8 gateway=192.168.20.1
```

Switch

In this example we are going to be using Bridge VLAN Filtering to filter unknown VLANs and to assign other devices to the same networks. Some devices are capable of offloading this to the built-in switch chip, check Basic VLAN switching guide to see how to configure it on different types of devices.

- Setup Bridge VLAN Filtering

```
/interface bridge
add name=bridge1 vlan-filtering=yes
/interface bridge port
add bridge=bridge1 interface=ether1
add bridge=bridge1 interface=ether2
add bridge=bridge1 interface=ether3
add bridge=bridge1 interface=ether4 pvid=10
add bridge=bridge1 interface=ether5 pvid=20
/interface bridge vlan
add bridge=bridge tagged=ether1,ether2,ether3 untagged=ether4,ether5 vlan-ids=10,20
```



Note: In this example untagged traffic is going to be used to communicate between CAPs and CAPsMAN Router. By default, if PVID is not changed, untagged traffic is going to be forwarded between ports that have the same PVID value set (including the default PVID).

CAPs

- Create a bridge and assign a port to it, that is connect to the CAPsMAN Router

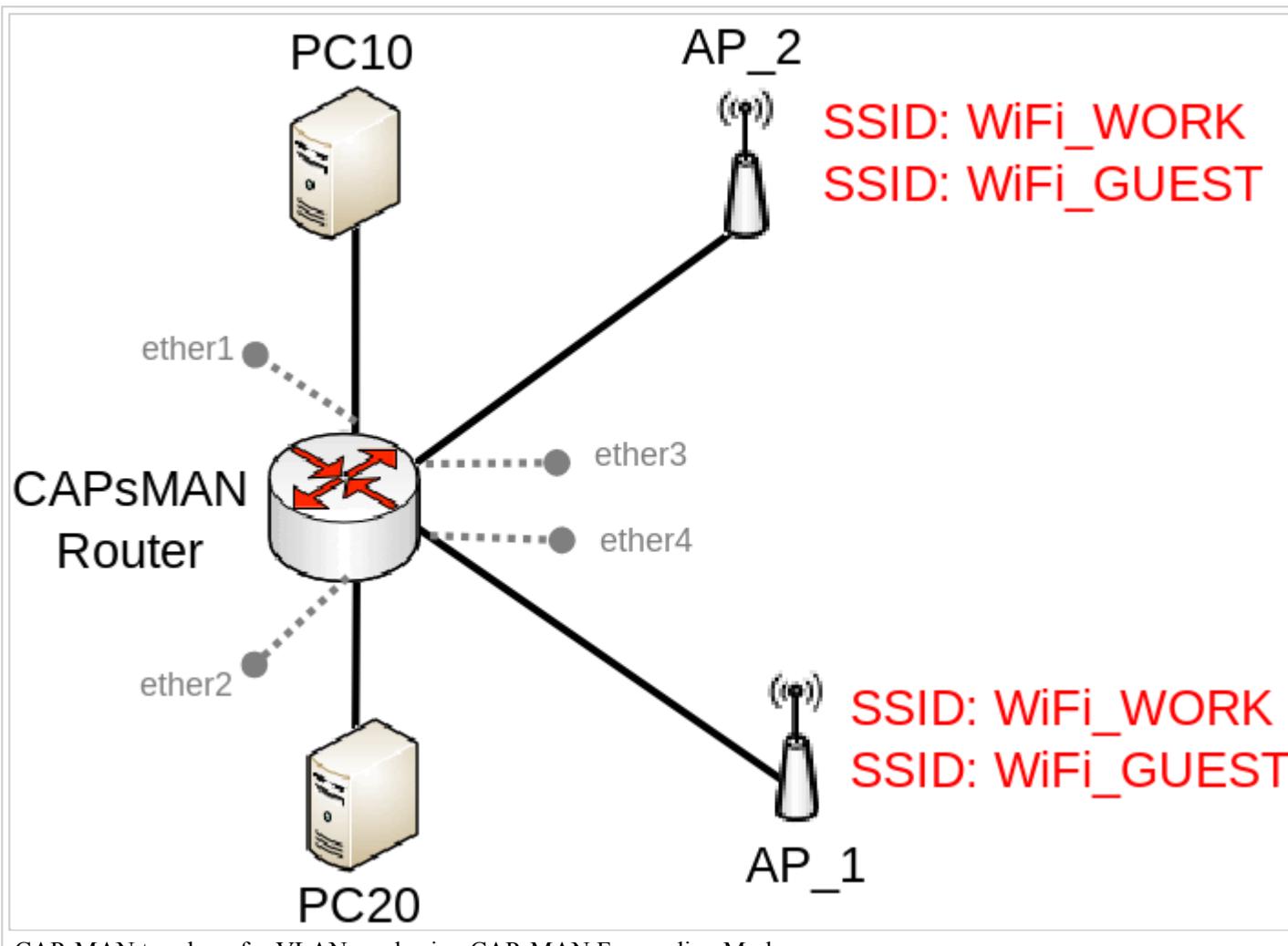
```
/interface bridge  
add name=bridge1  
/interface bridge port  
add bridge=bridge1 interface=ether1
```

- Enable CAP mode on the AP, make sure you specify to use the newly created bridge

```
/interface wireless cap  
set bridge=bridge1 discovery-interfaces=bridge1 enabled=yes interfaces=wlan1
```

That is it! Connect Wireless clients to your APs and check connectivity.

Using CAPsMAN Forwarding Mode



In CAPsMAN Forwarding Mode all traffic that is coming from a CAP is encapsulated with a special CAPsMAN header, which can only be removed by a CAPsMAN router, this means that a switch will not be able to distinguish the VLAN ID set by the CAP since the VLAN tag is also going to be encapsulated. This mode limits the possibility to divert traffic in Layer2 networks, but gives you the possibility to forward traffic from each CAP over Layer3 networks for a distant CAPsMAN router to process the traffic, this mode is useful when you want to control multiple CAPs in remote locations, but want to use a central gateway.

CAPsMAN Router

- Setup Bridge VLAN filtering to limit interfaces to appropriate VLANs

```
/interface bridge
add name=bridge1 vlan-filtering=yes
/interface bridge port
add bridge=bridge1 interface=ether1 pvid=10
add bridge=bridge1 interface=ether2 pvid=20
/interface bridge vlan
add bridge=bridge1 tagged=bridge untagged=ether1,ether2 vlan-ids=10,20
```



Note: CAPsMAN will attach CAP interfaces to the bridge and automatically will add appropriate entries to the bridge VLAN table. Currently this feature is only added in 6.43rc17.

- Create appropriate CAP configurations for each VLAN

```
/caps-man configuration
add country=latvia datapath.bridge=bridge1 datapath.vlan-id=10 datapath.vlan-mode=use-tag name=Config_WORK
  security.passphrase=secret_work_password ssid=WiFi_WORK
add country=latvia datapath.bridge=bridge1 datapath.vlan-id=20 datapath.vlan-mode=use-tag name=Config_GUEST
  security.passphrase=secret_guest_password ssid=WiFi_GUEST
```

- We are going to create a single CAPsMAN provisioning rule to create the **WiFi_WORK** and the **WiFi_GUEST** SSIDs on a single device, each connect CAP is going to create these SSIDs automatically

```
/caps-man provisioning
add action=create-dynamic-enabled master-configuration=Config_WORK slave-configurations=Config_GUEST
```



Note: You can create even more Virtual APs by adding multiple **slave-configuration**s. That requires multiple CAPsMAN configurations that were created earlier.

- For security reasons, limit the CAPsMAN to interfaces. to which CAPs are going to be connected

```
/caps-man manager interface
set [ find default=yes ] forbid=yes
add disabled=no interface=ether3
add disabled=no interface=ether4
```

- Enable the CAPsMAN manager

```
/caps-man manager
set enabled=yes
```

- Setup DHCP Server for each VLAN

```
/interface vlan
add interface=bridge1 name=VLAN10 vlan-id=10
add interface=bridge1 name=VLAN20 vlan-id=20
/ip address
add address=192.168.10.1/24 interface=VLAN10
add address=192.168.20.1/24 interface=VLAN20
/ip pool
add name=dhcp_pool10 ranges=192.168.10.2-192.168.10.254
add name=dhcp_pool20 ranges=192.168.20.2-192.168.20.254
/ip dhcp-server
add address-pool=dhcp_pool10 disabled=no interface=VLAN10 name=dhcp10
add address-pool=dhcp_pool20 disabled=no interface=VLAN20 name=dhcp20
/ip dhcp-server network
add address=192.168.10.0/24 dns-server=8.8.8.8 gateway=192.168.10.1
add address=192.168.20.0/24 dns-server=8.8.8.8 gateway=192.168.20.1
```

CAPs

- Enable CAP mode on each AP, specify which interface is connected to the CAPsMAN router

```
/interface wireless cap
set discovery-interfaces=ether1 enabled=yes interfaces=wlan1
```

That is it! Connect Wireless clients to your APs and check connectivity.

Case studies

Without Virtual APs

Not everyone wants to create Virtual APs since that does decrease the total throughput. If you want to use multiple devices to create multiple SSIDs, then it is possible to assign a certain configuration on a CAP based on its identity. To achieve this you should use CAPsMAN provisioning rules along with RegEx expressions. In this example we are going to assign the **Config_WORK** configuration to CAPs that have identity set to "**AP_WORK_***" and we are going to assign the **Config_GUEST** configuration to CAPs that have identity set to "**AP_GUEST_***". To do this, you simply need to change the CAPsMAN provisioning rules.

- Remove any existing provisioning rules

```
/caps-man provisioning remove [f]
```

- Create new provisioning rules that will assign appropriate configuration on a CAP based on its identity

```
/caps-man provisioning
add action=create-dynamic-enabled identity-regexp=^AP_GUEST_ master-configuration=Config_GUEST
add action=create-dynamic-enabled identity-regexp=^AP_WORK_ master-configuration=Config_WORK
```



Note: Don't forget to set a proper identity on the CAPs since CAPsMAN is going to assign appropriate configuration on the APs based on its identity.

Retrieved from "https://wiki.mikrotik.com/index.php?title=Manual:CAPsMAN_with_VLANs&oldid=31976"

Categories: Bridging and switching | Wireless | Examples

- This page was last edited on 31 August 2018, at 09:54.