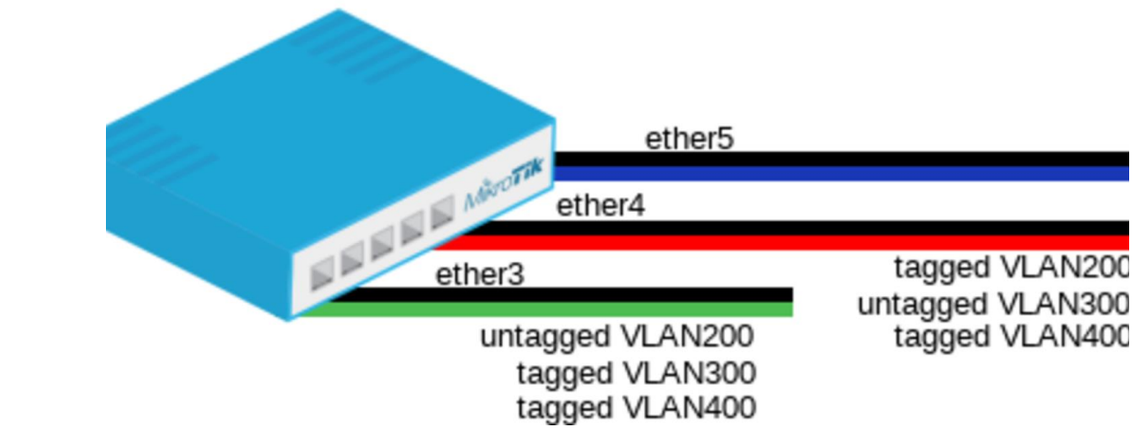
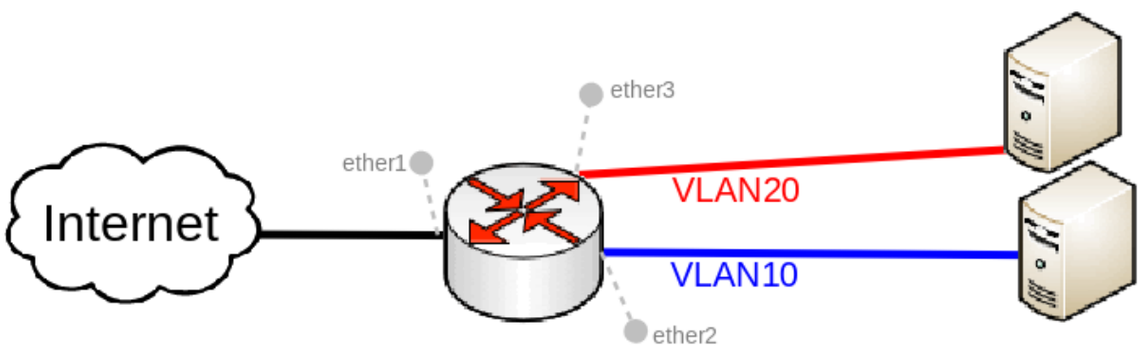
MikroTik VLAN Configuration

released 2020





Port switching

For this type of configuration to work, you must switch all required ports together:

```
/interface bridge
add name=bridge1

/interface bridge port
add bridge=bridge1 interface=ether2 hw=yes
add bridge=bridge1 interface=ether3 hw=yes
```

DHCP and NAT

Create a VLAN interface for each VLAN ID and assign an IP address on it:

```
/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
```

Setup a DHCP Server for each VLAN:

```
/ip pool
add name=POOL10 ranges=192.168.10.100-192.168.10.200
add name=POOL20 ranges=192.168.20.100-192.168.20.200
/ip dhcp-server
add address-pool=POOL10 disabled=no interface=VLAN10 name=DHCP10
add address-pool=POOL20 disabled=no interface=VLAN20 name=DHCP20
```

```
/ip dhcp-server network
add address=192.168.10.0/24 dns-server=8.8.8.8,8.8.4.4 gateway=192.168.10.1
add address=192.168.20.0/24 dns-server=8.8.8.8,8.8.4.4 gateway=192.168.20.1
```

Enable NAT on the device:

```
/ip firewall nat
add action=masquerade chain=srcnat out-interface=ether1
```

VLAN switching

Add each port to the VLAN table and allow these ports to access the CPU in order to make DHCP and routing work:

```
/interface ethernet switch vlan
add independent-learning=yes ports=ether2,switch1-cpu switch=switch1 vlan-id=10
add independent-learning=yes ports=ether3,switch1-cpu switch=switch1 vlan-id=20
```

Specify each port to be as an access port, enable secure VLAN mode on each port and on the switch1-cpu port:

```
/interface ethernet switch port
set ether2 default-vlan-id=10 vlan-header=always-strip vlan-mode=secure
set ether3 default-vlan-id=20 vlan-header=always-strip vlan-mode=secure
set switch1-cpu vlan-mode=secure
```

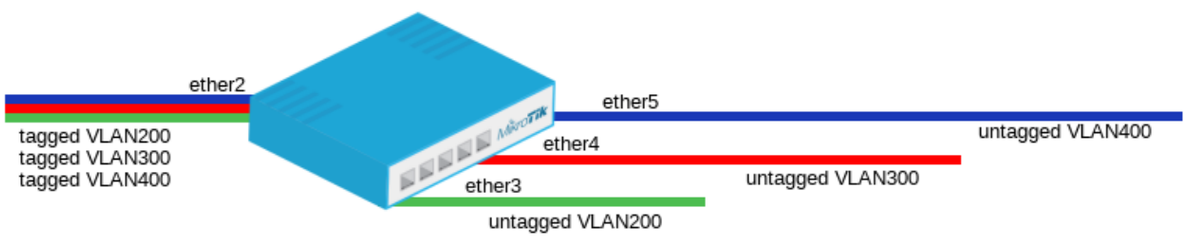
Isolated VLANs

If your device has a rule table, then you can limit access between VLANs on a hardware level. As soon as you add an IP address on the VLAN interface you enable interVLAN routing, but this can be limited on a hardware level yet preserving DHCP Server and other router related services' functionality. To do so, use these ACL rules:

```
/interface ethernet switch rule
add dst-address=192.168.20.0/24 new-dst-ports="" ports=ether2 switch=switch1
add dst-address=192.168.10.0/24 new-dst-ports="" ports=ether3 switch=switch1
```

VLAN Example 1 (Trunk and Access Ports)

RouterBOARDs with Atheros switch chips can be used for 802.1Q Trunking. This feature in RouterOS v6 is supported by **QCA8337, Atheros8316, Atheros8327, Atheros8227** and **Atheros7240** switch chips.
In this example **ether3**, '**ether4** and **ether5** interfaces are access ports, while **ether2** is a trunk port. VLAN IDs for each access port: ether3 - 200, ether4 - 300, ether5 - 400.



Switch together the required ports:

```
/interface bridge
add name=bridge1

/interface bridge port
add bridge=bridge1 interface=ether2 hw=yes
add bridge=bridge1 interface=ether3 hw=yes
add bridge=bridge1 interface=ether4 hw=yes
add bridge=bridge1 interface=ether5 hw=yes
```

Add VLAN table entries to allow frames with specific VLAN IDs between ports:

```
/interface ethernet switch vlan
add ports=ether2,ether3 switch=switch1 vlan-id=200
add ports=ether2,ether4 switch=switch1 vlan-id=300
add ports=ether2,ether5 switch=switch1 vlan-id=400
```

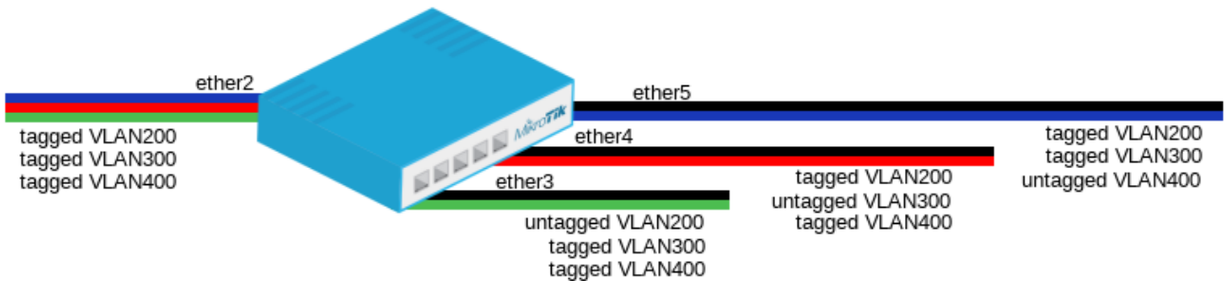
Assign *vlan-mode* and *vlan-header* for each port and also *default-vlan-id* on ingress for each access port:

```
/interface ethernet switch port
set ether2 vlan-mode=secure vlan-header=add-if-missing
set ether3 vlan-mode=secure vlan-header=always-strip default-vlan-id=200
set ether4 vlan-mode=secure vlan-header=always-strip default-vlan-id=300
set ether5 vlan-mode=secure vlan-header=always-strip default-vlan-id=400
```

- Setting `vlan-mode=secure` ensures strict use of VLAN table.
- Setting `vlan-header=always-strip` for access ports removes VLAN header from frame when it leaves the switch chip.
- Setting `vlan-header=add-if-missing` for trunk port adds VLAN header to untagged frames.
- *default-vlan-id* specifies what VLAN ID is added for untagged ingress traffic of the access port.

VLAN Example 2 (Trunk and Hybrid Ports)

VLAN Hybrid ports which can forward both tagged and untagged traffic are supported only by some Gigabit switch chips (**QCA8337, Atheros8327**)



Switch together the required ports:

```
/interface bridge
add name=bridge1
/interface bridge port
add bridge=bridge1 interface=ether2 hw=yes
add bridge=bridge1 interface=ether3 hw=yes
add bridge=bridge1 interface=ether4 hw=yes
add bridge=bridge1 interface=ether5 hw=yes
```

Add VLAN table entries to allow frames with specific VLAN IDs between ports.

```
/interface ethernet switch vlan
add ports=ether2,ether3,ether4,ether5 switch=switch1 vlan-id=200
add ports=ether2,ether3,ether4,ether5 switch=switch1 vlan-id=300
add ports=ether2,ether3,ether4,ether5 switch=switch1 vlan-id=400
```

In switch port menu set *vlan-mode* on all ports and also *default-vlan-id* on planned hybrid ports:

```
/interface ethernet switch port
set ether2 vlan-mode=secure vlan-header=leave-as-is
set ether3 vlan-mode=secure vlan-header=leave-as-is default-vlan-id=200
set ether4 vlan-mode=secure vlan-header=leave-as-is default-vlan-id=300
set ether5 vlan-mode=secure vlan-header=leave-as-is default-vlan-id=400
```

- `vlan-mode=secure` will ensure strict use of VLAN table.
- *`default-vlan-id`* will define VLAN for untagged ingress traffic on port.
- In QCA8337 and Atheros 8327 chips when `vlan-mode=secure` is used, it ignores switch port *vlan-header* options. VLAN table entries handle all the egress tagging/untagging and works as `vlan-`

`header=leave-as-is` on all ports. It means what comes in tagged, goes out tagged as well, only *default-vlan-id* frames are untagged at the egress of port.

Management access configuration

In these examples there will be shown examples for multiple scenarios, but each of these scenarios require you to have switched ports. Below you can find how to switch multiple ports:

```
/interface bridge
add name=bridge1

/interface bridge port
add interface=ether1 bridge=bridge1 hw=yes
add interface=ether2 bridge=bridge1 hw=yes
```

In these examples it will be assumed that **ether1** is the trunk port and **ether2** is the access port, for configuration as the following:

```
/interface ethernet switch port
set ether1 vlan-header=add-if-missing
set ether2 default-vlan-id=100 vlan-header=always-strip

/interface ethernet switch vlan
add ports=ether1,ether2,switch1-cpu switch=switch1 vlan-id=100
```

Tagged

In order to make the device accessible only from a certain VLAN, you need to create a new VLAN interface on the bridge interface and assign an IP address to it:

```
/interface vlan
add name=VLAN-MGMT vlan-id=99 interface=bridge1

/ip address
add address=192.168.99.1/24 interface=VLAN-MGMT
```

Specify from which interfaces it is allowed to access the device:

```
/interface ethernet switch vlan
add ports=ether1,switch1-cpu switch=switch1 vlan-id=99
```

Note: Only specify trunk ports in this VLAN table entry, it is not possible to allow access to the CPU with tagged traffic through an access port since the access port will tag all ingress traffic with the specified `default-vlan-id` value.

When VLAN table is configured, you can enable `vlan-mode=secure` to limit access to the CPU:

```
/interface ethernet switch port
set ether1 vlan-header=add-if-missing vlan-mode=secure
set ether2 default-vlan-id=100 vlan-header=always-strip vlan-mode=secure
set switch1-cpu vlan-header=leave-as-is vlan-mode=secure
```

Untagged

In order to make the device accessible from the access port, create a VLAN interface with the same VLAN ID as set in `default-vlan-id`, for example VLAN 100, and add an IP address to it:

```
/interface vlan
add name=VLAN100 vlan-id=100 interface=bridge1

/ip address
add address=192.168.100.1/24 interface=VLAN100
```

Specify which access (untagged) ports are allowed to access the CPU:

```
/interface ethernet switch vlan
add ports=ether1,ether2,switch1-cpu switch=switch1 vlan-id=100
```

Warning: Most commonly an access (untagged) port is accompanied with a trunk (tagged) port. In case of untagged access to the CPU, you are forced to specify both the access port and the trunk port, this gives access to the CPU from the trunk port as well. Not always this is desired and Firewall might be required on top of VLAN filtering.

When VLAN table is configured, you can enable `vlan-mode=secure` to limit access to the CPU:

```
/interface ethernet switch port
set ether1 vlan-header=add-if-missing vlan-mode=secure
set ether2 default-vlan-id=100 vlan-header=always-strip vlan-mode=secure
set switch1-cpu vlan-header=leave-as-is vlan-mode=secure
```

Note: To setup management port using untagged traffic on a device with the **Atheros7240** switch chip, you will need to set `vlan-header=add-if-missing` for the CPU port.

Untagged from tagged port

It is possible to allow access to the device from the trunk (tagged) port with untagged traffic. To do so, assign an IP address on the bridge interface:

```
/ip address
add address=10.0.0.1/24 interface=bridge1
```

Specify which ports are allowed to access the CPU. Use `vlan-id` that is used in `default-vlan-id` for switch-cpu and trunk ports, by default it is set to 0 or 1.

```
/interface ethernet switch vlan
add ports=ether1,switch1-cpu switch=switch1 vlan-id=1
```

When VLAN table is configured, you can enable `vlan-mode=secure` to limit access to the CPU:

```
/interface ethernet switch port
set ether1 default-vlan-id=1 vlan-header=add-if-missing vlan-mode=secure
set switch1-cpu default-vlan-id=1 vlan-header=leave-as-is vlan-mode=secure
```

Note: This configuration example is not possible for devices with the **Atheros8316** and **Atheros7240** switch chips.

Note: For devices with **QCA8337** and **Atheros8327** switch chips it is possible to use any other `default-vlan-id` as long as it stays the same on switch-cpu and trunk ports. For devices with **Atheros8227** switch chip only `default-vlan-id=0` can be used and trunk port must use `vlan-header=leave-as-is`.

Source:
Please note: Content directly copied from the following pages.
https://wiki.mikrotik.com/wiki/Manual:Switch_Router
https://wiki.mikrotik.com/wiki/Manual:Switch_Chip_Features#Setup_Examples

URL:
https://danservices.com.au/support/mikrotik-vlan-configuration-2020/

TKJ Department
SMK Informatika Wonosobo
Jl. Mayjend. Bambang Sugeng No. 1
Wonosobo, Jawa Tengah, Indonesia

mikrotik.smkinka-wsb.sch.id
tkj.smkinka-wsb.sch.id