WMM and VLAN priority

How WMM works

WMM works by dividing traffic into 4 access categories: background, best effort, video, voice. QoS policy (different handling of access categories) is applied on transmitted packets, therefore the transmitting device is treating different packets differently, e.g. AP does not have control over how clients are transmitting packets, and clients do not have control over how AP transmits packets.

Mikrotik AP and client classifies packets based on the priority assigned to them, according to the table (as per WMM specification): 1,2 - background 0,3 - best effort 4,5 - video 6,7 - voice.

To be able to use multiple WMM access categories, not just best effort where all packets with default priority 0 go, priority must be set for those packets. By default, all packets (incoming and locally generated) inside the router have priority 0.

"Better" access category for packet does not necessarily mean that it will be sent over the air before all other packets with the "worse" access category. WMM works by executing the DCF method for medium access with different settings for each access category (EDCF), which basically means that "better" access category has a higher probability of getting access to medium - WMM enabled station can be considered to be 4 stations, one per access category, and the ones with "better" access category use settings that make them more likely to get chance to transmit (by using shorter backoff timeouts) when all are contending for medium. Details can be studied in 802.11e and WMM specifications.

> WMM support can be enabled using the `wmm-support` setting. It only applies to bands B and G. Other bands will have it enabled regardless of this setting

How VLAN priority works

The VLAN priority is a 3-bit field called Priority Code Point (PCP) within a VLAN-tagged header and values are between 0 and 7. It is used for implementing QoS on bridges and switches. MikroTik devices by default are sending VLAN packets (locally generated or encapsulated) with a priority of 0. RouterOS bridge forwards VLAN tagged packets unaltered, which means that received VLAN tagged packets with a certain VLAN priority will leave the bridge with the same VLAN priority. The only exception is when the bridge untags the packet, in this situation VLAN priority is not preserved due to the missing VLAN header.

More details can be studied in the IEEE 802.1p specification.

How to set priority

Priority of packets can be set using `action=set-priority` of IP firewall mangle rules or bridge filter/nat rules. Priority can be set to a specific value or taken from the ingress priority using the `from-ingress` setting. Ingress priority is the priority value that was detected on the incoming packet, if available. Currently, there are 2 sources of ingress priority - priority in the VLAN header and priority from the WMM packet received over a wireless interface. For all other packets ingress priority is 0.

Note that ingress priority value is not automatically copied to IP mangle `priority` value, the correct rule needs to be set up to do this.

There are basically 2 ways to control priority - assign priority with rules with particular matchers (protocol, addresses, etc.) or set it from ingress priority. Both options require setting up correct rules.

This essentially means that if it is not possible or wanted to classify packets by rules, the configuration of the network must be such that the router can extract ingress priority from incoming frames. Remember there are currently 2 sources for this - VLAN tag in packets and received WMM packets.

> Do not mix priority of queues with priority assigned to packets. Priorities of queues work separately and specify the "importance" of the queue and have meaning only within a particular queue setup. Think of packet priority as some kind of mark, that gets attached to the packet by rules. Also take into account that this mark currently is only used for outgoing packets when going over WMM enabled link, and in case VLAN tagged packet is sent out (no matter if that packet is tagged locally or bridged).

Set VLAN or WMM priority based on specific matchers

It is possible to change the VLAN and WMM priorities based on specific matchers in IP mangle or bridge filter/nat rules. In this example, all outgoing ICMP packets will be sent with a VLAN or WMM priority using the IP mangle rule:

```
/ip firewall mangle
add action=set-priority chain=output new-priority=2 protocol=icmp
```

Custom priority mapping

Sometimes certain VLAN or WMM priorities need to be changed or cleared to a default value. We can use the `ingress-priority` matcher in IP mangle or bridge firewall/nat rules to filter only the needed priorities and change them to a different value using the `new-priority` action setting. For example, forwarded VLAN tagged packets over a bridge with a priority of 5, need to be changed to 0.

```
/interface bridge filter
add action=set-priority chain=forward ingress-priority=5 new-priority=0
```

Translating WMM priority to VLAN priority inside a bridge

When a wireless packet is received with an already set WMM priority, the RouterOS bridge does not automatically translate it to a VLAN header. It means, that received wireless packets with WMM priority that gets VLAN tagged by the bridge will be forwarded with a VLAN priority of 0. However, we can use a bridge filter rule with `from-ingress` setting to keep the priority in VLAN packets. For example, we would like to forward wireless packets over ether2 with VLAN 10 header and keep the already set WMM priority (set by wireless client).

```
/interface bridge
add name=bridge1 vlan-filtering=yes
/interface bridge port
add bridge=bridge1 interface=ether2
add bridge=bridge1 interface=wlan2 pvid=10
/interface bridge vlan
add bridge=bridge1 tagged=ether2 vlan-ids=10

# translates WMM priority to VLAN priority
/interface bridge filter
add action=set-priority chain=forward new-priority=from-ingress out-interface=ether2
```

The same situation applies when wireless packets are VLAN tagged by the wireless interface using the `vlan-mode=use-tag` and `vlan-id` settings. You still need to use the same bridge filter rule to translate WMM priority to VLAN priority:

```
/interface wireless
set [ find default-name=wlan2 ] vlan-mode=use-tag vlan-id=10

/interface bridge
add name=bridge1
/interface bridge port
add bridge=bridge1 interface=ether2
add bridge=bridge1 interface=wlan2

 # translates WMM priority to VLAN priority
/interface bridge filter
add action=set-priority chain=forward new-priority=from-ingress out-interface=ether2
```

The same principles apply in the other direction. RouterOS does not automatically translate VLAN priority to WMM priority. The same rule `new-priority=from-ingress` can be used to translate VLAN priority to WMM priority.

RouterOS bridge forwards VLAN tagged packets unaltered, which means that received VLAN tagged packets with a certain VLAN priority will leave the bridge with the same VLAN priority. The only exception is when the bridge untags the packet, in this situation VLAN priority is not preserved due to the missing VLAN header.

Priority from DSCP

Another way of setting VLAN or WMM priority is by using the DSCP field in the IP header, this can only be done by the IP firewall mangle rule with `new-priority=from-dscp` or `new-priority=from-dscp-high-3-bits` settings and `set-priority` action property. Note that DSCP in IP header can have values 0-63, but priority only 0-7. When using the `new-priority=from-dscp` setting, the priority will be 3 low bits of the DSCP value, but when using `new-priority=from-dscp-high-3-bits` the priority will be 3 high bits of DSCP value.

Remember that DSCP can only be accessed on IP packets and DSCP value in IP header should be set somewhere (either by client devices or IP mangle rules).

It is best to set the DSCP value in the IP header of packets on some border router (e.g. main router used for connection to the Internet), based on traffic type e.g. set DSCP value for packets coming from the Internet belonging to SIP connections to 7, and 0 for the rest. This way packets must be marked only in one place. Then all APs on the network can set packet priority from DSCP value with just one rule.

Set VLAN or WMM priority from DSCP

In this example, the AP device will set WMM priority from DSCP when packets are routed through the wireless interface.

```
/ip firewall mangle
add action=set-priority chain=forward new-priority=from-dscp out-interface=wlan2
```

When packets are forwarded through a bridge, to change VLAN/WMM priority from DSCP you have to pass packets through IP firewall mangle rules, to do so set `use-ip-firewall=yes` under the bridge settings.

DSCP from Priority

Similarly, the DSCP value can be set if the received packet contains VLAN or WMM priority. This can be achieved with IP mangle rules with `new-dscp=from-priority` or `new-dscp=from-priority-to-high-3-bits` settings and `change-dscp` action property. Note that priority in VLAN or WMM packets can have values 0-7, but DSCP in IP headers are 0-63. When using the `new-dscp=from-priority` setting, the value of priority will set the 3 low bits of the DSCP, but when using `new-dscp=from-priority-to-high-3-bits` the value of priority will set the 3 high bits of the DSCP.

However, this setting cannot directly use ingress priority from received VLAN or WMM packets. You first need to set priority using IP mangle or bridge filter /nat rules (ingress priority can be used in this case), and only then apply the DSCP rule.

Set DSCP from VLAN or WMM priority

In this example, the AP device needs to set DSCP from WMM priority when packets are routed. First, add a rule to set priority, it will be needed for the DSCP rule to correctly change the DSCP value. This rule can take priority from ingress. Then add the DSCP rule to change its value.

```
/ip firewall mangle
add action=set-priority chain=prerouting in-interface=wlan2 new-priority=from-ingress
add action=change-dscp chain=prerouting in-interface=wlan2 new-dscp=from-priority
```

When packets are forwarded through a bridge, to change DSCP from VLAN/WMM you have to pass packets through IP firewall mangle rules, to do so set `use-ip-firewall=yes` under the bridge settings.

Combining priority setting and handling solutions

Complex networks and different situations can be handled by combining different approaches of carrying priority information to ensure QoS and optimize the use of resources, based on the "building blocks" described above. Several suggestions:

- The fewer number of filter rules in the whole network, the better (faster). Try classifying packets only when necessary, prefer to do that on fast routers as most probably connection tracking will be required.
- Use DSCP to carry priority information in IP packets forwarded in your network, this way you can use it when needed.
- Use VLANs where necessary, as they also carry priority information, make sure Ethernet bridges and switches in the way are not clearing priority information in the VLAN tag.
- Remember that QoS does not improve the throughput of links, it just treats different packets differently, and also that WMM traffic over the wireless link will discriminate regular traffic in the air.

See also

- Packet Flow in RouterOS
- IP mangle
- Bridge firewall