

qm command (QoS configuration)

 Successfully pass the free certification exam at IW Academy and become an Infinet Certified Engineer.

[To the certification exam](#)

- [Description](#)
- [Parameters](#)
- [Examples](#)

Description

QoS (Quality of Service) is a convenient and flexible mechanism, allows to manipulate data streams going through the device. Allows to create up to 200 logical channels characterized by different properties (such as priority levels and data transfer rates), and then assign data streams to these logical channels according to special rules of assignment. Packets going through different channels are thus modifying their own properties as well as properties of their respective data flows.

Syntax:

```
option [no]rtp [no]dot1p [no]dscp [no]tos [no]tcbp [no]icmp
      [no]tunnel [no]pppoe [no]mpls [no]selfqos [no]auto [no]ipfw


classN {max=N} | {clear}

chN [max=N[%]|0] [classN] [ceil=N[%]|0] [ceilprio=N|0] [latency=N|0]
  [[add]pri=[N] | setpri=[N]] [[no]strict]] [pps=N|0] [to=ADDR]
  [vlan=[N|-1]] [dot1p=[N|-1]] [dscp=[N|-1]] [info="STRING"]
  clear

stat [full] [clear]
del  RULE_NUMBER
dump RULE_NUMBER
mov  RULE_A RULE_B
rearrange [STEP]
add[out] [NUM] [IFNAME] chN rules...

rules: [{setpri|addpri}=[N]] [pass]
  [vlan={N|any|$ACL}] [dot1p=N] [swg=N] [ether={X|any}] [dscp=N|tos=N] [prf]
  -f "pcap filter expression"
  |
  PROTO from [not] ADDR [PORTs] to [not] ADDR [PORTs]

PROTO: [all] | tcp | udp | icmp | arp | proto NUMBER
ADDR:  IP | $LOCAL | $ROUTE | $ACL | mac x:x:x:x:x:x }
PORTS: NUM[:NUM] [NUM] ...
```

 **CAUTION**

Parameter values shall be put after their keywords (if any) without blanks, as shown above; no blank may be put before or after "=".

Parameters

Parameter	Description
-----------	-------------

**NOTE**

For all auto-prioritization functions the "*addpri*" argument must be used. Thus, priorities will be set in the following order:

1. the dot1p priority ("*addpri*");
2. the priority set by "*qm*" rule ("*addpri*" or "*setpri*");
3. the "*dscp*" / "*tos*" priority, if it is higher than current ("*addpri*");
4. the value, that is set to the channel ("*addpri*" или "*setpri*").

The same order will be applied for outgoing packets if corresponding rules are configured.

- "*no/strict*" – applies the "Strict Priority" policy to all queues (packets from a queue with lower priority are not processed before a queue with higher priority is not empty). By default "Weighted Fair Queuing" policy is used (even if a queue with higher priority is not empty packets from other queues will be processed in a distinct sequence relative to a higher priority queue. For example, 4 packets from queue with priority 1, 1 packet from the queue with priority 2, 8 packets from queue priority 1, 1 packet from the queue with priority 3).
- "*pps=N/d*" – sets the limit for the packets per second for the specified channel. The "0" value disables the parameter.
- "*to=ADDR*" – redirects the whole stream to the specified IP-address irrespectively of the present routing conditions. The specified address shall be directly attainable through one of the router interfaces (without additional routing). This may be useful when the router serves as a network access unit, and two or more different clients want to access different providers through one unit.
- "*vlan=N/-1*" – sets VLAN ID (value range: 0-4095). The "-1" value removes the argument.
- "*dot1p=N/-1*" – prioritization of packets labeled IEEE 802.1p (valid values are from 0 to 7). The "-1" value removes the argument.
- "*dscp=N/-1*" – prioritization of DSCP (valid values are from 0 to 63). The "-1" value removes the argument.
- "*classN*" – assigns service class "*N*" to the channel. This additional parameter relates to the above defined data rate limitation, making it flexible: when the total bandwidth of this service class is not fully used, the extra bandwidth may be granted to such channel, thus exceeding its predefined data rate limit, up to full load of the class. When, there are several such channels competing for extra bandwidth, it is equally divided between them.

**CAUTION**

Exception: on the H02 platform, if there are several channels competing for extra bandwidth of their parent class, the bandwidth is divided between them proportionally to their respective predefined data rate limits.

- "*info=STRING*" – allows user to set up a string description for the QoS channel.
- "*clear*" – removes current configuration of channel.

**NOTE**





If several of the above parameters are specified in the same command then rate limitation is applied first then redirection and priority last. If "*vlan*" and "*dot1p*" parameters are specified in the same command then "*vlan*" is processed first.


Each channel can be assigned a priority (0...16). Once assigned, a priority will be automatically recognized by every node inside MINT network.

Channel	Priority
BACKGROUND	16
REGULAR Best Effort	15
BUSINESS6	14
BUSINESS5	13
BUSINESS4	12
BUSINESS3	11
BUSINESS2	10
BUSINESS1	9
QOS4	8
QOS3	7
QOS2	6
QOS1	5
VIDEO2	4
VIDEO	3
VOICE	2
CONTROL	1
NETCRIT	0

Packets that have no priority are labeled as "*REGULAR Best Effort=15*" and processed accordingly.

Packets classification can also be performed using "*pcap*" rules.

	<div>  CAUTION </div> <p>Real prioritization within MINT network is conducted by priority, given by "<i>pri=N</i>" parameters. A DSCP label is transparently transmitted through the MINT network in any mode. A 802.1p priority is transparently transmitted only in switch mode of the MINT network. If necessary, for packets leaving the MINT network required "<i>dot1p</i>" and "<i>dscp</i>" parameters can be assigned by the operator.</p>
stat [full] [clear]	<p>Displays statistics of the specific channel (only for channels with specified rate limitation):</p> <ul style="list-style-type: none"> "full" – allows viewing enhanced statistics. "clear" – resets statistics. <pre>qm ch1 max=128 cur=127 packets=12345 (1234) bytes=1234567 (12345)</pre> <div>  NOTE </div> <p>The "<i>qm stat</i>" command displays PPS (Packets Per Second) statistics only if the limit for the packets per second is set for the specified channel (<i>qm chN pps=N</i>).</p>
del RULE_NUMBER	Deletes the specified rule from the list.
dump RULE_NUMBER	Displays the compiled pseudo-code of the PCAP rule. Allows to check visually the complexity / optimality or the correctness of the rule.
mov RULE_A RULE_B	Changes the number of the rule from "A" to "B".
rearrange [STEP]	Renums all rules with the given increment " <i>STEP</i> " (default is 5). The " <i>config show</i> " command displays rules number.
add[out] [NUM] [IFNAME] chN rules..	<p>Allows to add an ingress/egress packet to / from the device that satisfies the channel "<i>N</i>" rule.</p> <ul style="list-style-type: none"> "add" - processing of ingress packets to the device. "out" – processing of egress packets from the device. "num" – the sequence number in the list of rules (optional parameter). "IFNAME" – an interface name through which packets enter\leave the device (optional parameter). <div>  NOTE </div> <p>All manipulations with packet headers, for example changing of dscp and 802.1p label, are possible only by using the "<i>qm addout</i>" command, i.e. only for leaving the device packets.</p>
rules: [{setpri=addpri=[N]} [pass] [vlan=[N any{\$ACL}] [dot1p=N] [swg=N] [ether=X any]] [dscp=N] [tos=N] [prf] -f "pcap filter expression"]	<p>The rules syntax fully corresponds to the syntax of the "<i>ipfw</i>" command (see "<i>ipfw command (IP Firewall)</i>" section).</p> <div>  NOTE </div> <p>Each packet passing through the system is checked if it matches rules strictly in order, from the first to the last, until there is a rule that satisfies the properties of the packet.</p> <ul style="list-style-type: none"> "setpri=[N]" – sets priority level of the packet no matter what priority it had before. "addpri=[N]" – increase the priority level of the packet to the specified value only if the new priority is higher than initial. "pass" – allows to "skip" the rule, perform related activities and continue browsing other rules in the list. "log" – includes filter action records in the system log (optional parameter). "vlan=" – allows to analyze VLAN ID (values range 0-4095): <ul style="list-style-type: none"> "N" – the filter will pass tagged packets with the specified tag "N". "any" – the filter will pass all tagged packets with any VLAN ID. "\$ACL" – the filter will pass tagged packets with the VLAN tags, listed as "\$ACL" (description of the ACL lists see in section «Access Control Lists (<i>*acl</i>) command)). "dot1p=N" – allows to analyze 802.1p priority (values range 0-7). "swg=N" – allows to analyze a switching group number. "ether=X any" – allows to analyze a packet type. If option "any" is enabled, the filter will pass packets of all types. "dscp=N" – allows to analyze the DSCP tag (values range 0-63). "tos=N" – allows to analyze the TOS tag. "prf" – enables filtration of PRF interface generated traffic. "-f "pcap filter expression" – allows to use PCAP-filters.
PROTO from [not] ADDR [PORTs] to [not] ADDR [PORTs]	<p>Specify a direction of transmission from and / or to:</p> <ul style="list-style-type: none"> "from" – source IP-address. "to" – destination IP-address. "not" – negative prefix, can be used after "from" and "to" keywords, it will be applied to the specified IP-address only, not for ports. "ADDR" – source or destination IP-address. The syntax depends on the "proto" field. If "proto" specified as "all" or "icmp", than "ADDR" defines an address information. If "proto" specified as "udp" or "tcp", than "ADDR" defines an address information and an optional list of ports. An address information is specified as IP-address and optional subnet mask. A subnet mask can be specified as prefix or as a numeric value (<i>nnn.nnn.nnn.nnn</i>). <p>Possible options:</p> <pre>nn . nn . nn . nn nn . nn . nn . nn : xxx . xxx . xxx . xxx nn . nn . nn . nn / NN</pre> <p>The "0/0" record includes all possible IP-addresses.</p>

PROTO: <i>[all] tcp udp icmp arp proto NUMBER</i>	The limitation is based on the compliance with a certain protocol. Possible values: TCP, UDP, ICMP, ARP or numeric value of the protocol. ARP-packets are allowed for all IP-addresses and for ranges of IP-addresses, which are specified in the permit filters, even if these filters are created for other types of packets.
ADDR: <i>IP \$LOCAL \$ROUTE \$ACL mac x:x:x:x:x:x }</i>	<p>It is possible to group all the necessary addresses into the appropriate access list and set the name of this list as an IP-address (<i>\$ACLRULE</i>). There are several predefined dynamic lists:</p> <ul style="list-style-type: none"> "<i>\$LOCAL</i>" – a list that includes all the local addresses belonging to this router. It can be used to make easier filters records that restrict / allow access to the device. "<i>\$ROUTE</i>" – a list that contains the current system routing table, except for the "<i>default route</i>". Matching the address from this list means that there is an exact route for this address and the default route will not be used. "<i>\$ACL</i>" – a list of IP-addresses or networks, to which this rule will be applied. "<i>mac x:x:x:x:x:x</i>" – for interfaces which have physical ethernet MAC-address, the numeric MAC-address value with the "<i>mac</i>" keyword as a prefix can be used. However, for incoming filters, you can specify only the source MAC-address, and for outgoing ones only the destination MAC-address. The "<i>\$BS</i>" keyword can be used, in this case the real MAC-address of the base station sector will be used. <div style="border: 1px solid #f9e79f; padding: 10px; margin-top: 10px;"> <p> NOTE</p> <p>Rules that use MAC-addresses for ingress packets will be processed before all the other rules, and rules for egress packets will be processed last.</p> </div>
PORTS: <i>NUM[:NUM] [NUM] ...</i>	Filters traffic by port numbers. It is possible to use a list of ports to specify multiple ports in one command. The first item of the list of ports can specify a range of numbers from smaller to greater, separated by a colon.

Examples

Limit all outgoing traffic on the subscriber terminal to 64 Kbps.

```
qm ch1 max=64
qm add eth0 ch1 all from 0/0 to 0/0
```

Set to the "*1.1.1.0/24*" network traffic higher priority than for all other data streams.

```
qm ch1 pri=5
qm add ch1 all from 1.1.1.0/24 to 0/0
qm add ch1 all from 0/0 to 1.1.1.0/24
```

Set to the "*1.1.1.0/24*" network traffic lower priority than for all other data streams. Take attention on the rules order. The last rule that each packet meets should be at the end of the list.

```
qm ch1 pri=5
qm ch2 pri=10
qm add ch2 all from 1.1.1.0/24 to 0/0
qm add ch2 all from 0/0 to 1.1.1.0/24
qm add ch1 all from 0/0 to 0/0
```

Network subscribers:

- "*1.1.1.0/24*" should make connection through the "*10.10.10.10*" provider.
- "*2.2.2.0/24*" should use the "*20.20.20.20*" provider.

In case of more complicated topology when providers routers are not reachable from this node, it is necessary to configure tunnels to providers first, then make redirection.

```
qm ch1 to=10.10.10.10
qm ch2 to=20.20.20.20
qm add ch1 all from 1.1.1.0/24 to 0/0
qm add ch2 all from 2.2.2.0/24 to 0/0
```

Disable automatic prioritization of real time packets and enable automatic prioritization of packets labeled with TOS.

```
qm option -rtsp tos
```

Increase the priority of all packets to the value "N" in case if "N" is higher than the current priority.

```
qm ch1 addpri=N
```

Set the priority level "N" to all packets.

```
qm ch1 setpri=N
```

Channel 1 resets DSCP labels and 802.1p priorities.

```
qm ch1 dscp=0 dot1p=-1
```

Channel 2 sets the "QM_PRIO_BUSINESS1" priority and DSCP 31 label.

```
qm ch2 pri=9 dscp=31
```

Pass all traffic through channel 1 to reset all priorities.

```
qm add ch1 pass all from 0/0 to 0/0
```

Forward TCP part of the traffic to the channel 2.

```
qm add ch2 tcp from X.X.X.0/24 to 0/0
```

Forward the UDP part of the traffic to the channel 3.

```
qm add ch3 udp from X.X.X.0/24 PORT to 0/0
```

The remaining traffic will be processed as a non-priority and directed to the channel 4.

```
qm add ch4 all from 0/0 to 0/0
```

Set 802.1p priority to packets from channel 25.

```
qm ch25 dot1p=5
```

Set 802.1p priority and VLAN ID for channel 26. The VLAN header will be added automatically in case it is missing.

```
qm ch26 vlan=7 dot1p=4
```

Forward egress packets assigned to the "eth0" interface and labeled with the DSCP 11, to the channel 25.

```
qm addout eth0 ch25 dscp=11 from 0/0 to 0/0
```

Forward egress UDP packets assigned to the "eth0" interface to the channel 25 and label them as DSCP 51.

```
qm ch25 dscp=51
qm addout eth0 ch25 udp from 0/0 to 0/0
```

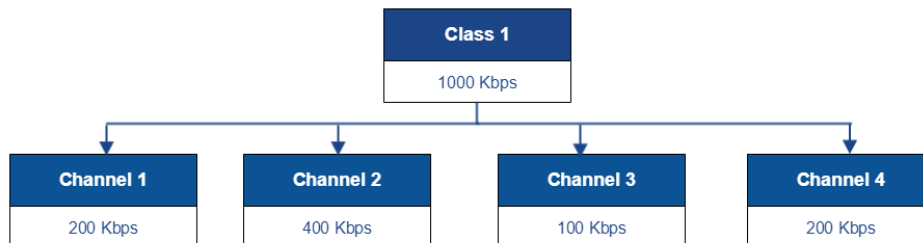
The example of using PCAP filters for packet classification: all ICMP-traffic will be added to the channel 5 directed from or to nodes "1.1.1.1" and "1.1.1.5".

```
qm add ch5 -f "icmp and host (1.1.1.1 or 1.1.1.5)"
```

The example of using service class.

```
qm class1 max=1000
qm ch1 max=200 ceil=1000 class1
qm ch2 max=400 ceil=1000 class1
qm ch3 max=100 ceil=300 class1
qm ch4 max=200 ceil=300 class1
```

As a result of these commands the hierarchy as in the picture below will appear:



- Assign the maximum throughput 1000 Kbps for parent class "Class 1".
- Throughput of the "Class 1" is distributed between "Channel 1", "Channel 2", "Channel 3" and "Channel 4" with appropriate bandwidth values and the maximum non-guaranteed rate: in case if the "Class 1" bandwidth is not fully used, then the "Channel 1" and the "Channel 2" rates can increase up to 1000 Kbps, the "Channel 3" and the "Channel 4" increase up to 300 Kbps.