Manual:CRS1xx/2xx series switches

From MikroTik Wiki

Contents

Applies to

RouterOS: v6.12 +

Summary

The Cloud Router Switch series are highly integrated switches with high performance MIPS CPU and feature-rich packet processor. The CRS switches can be designed into various Ethernet applications including unmanaged switch, Layer 2 managed switch, carrier switch and wireless/wired unified packet processing.

Warning: This article applies to CRS1xx and CRS2xx series switches and not to CRS3xx series switches. For CRS3xx series devices read the CRS3xx series switches manual.

Features	Description
Forwarding	▪ Configurable ports for switching or routing ▪ Full non-blocking wirespeed switching ▪ Up to 16k MAC entries in Unicast FDB for Layer 2 unicast forwarding ▪ Up to 1k MAC entries in Multicast FDB for multicast forwarding ▪ Up to 256 MAC entries in Reserved FDB for control and management purposes ▪ All Forwarding Databases support IVL and SVL ▪ Configurable Port based MAC learning limit ▪ Jumbo frame support (CRS1xx: 4064 Bytes; CRS2xx: 9204 Bytes) ▪ IGMP Snooping support

Mirroring	▪ Various types of mirroring:
	  ▪ Port based mirroring
	  ▪ VLAN based mirroring
	  ▪ MAC based mirroring
	▪ 2 independent mirroring analyzer ports

VLAN	▪ Fully compatible with IEEE802.1Q and IEEE802.1ad VLAN
	▪ 4k active VLANs
	▪ Flexible VLAN assignment:
	  ▪ Port based VLAN
	  ▪ Protocol based VLAN
	  ▪ MAC based VLAN
	▪ From any to any VLAN translation and swapping
	▪ 1:1 VLAN switching - VLAN to port mapping
	▪ VLAN filtering

Port Isolation and Leakage	▪ Applicable for Private VLAN implementation ▪ 3 port profile types: Promiscuous, Isolated and Community ▪ Up to 28 Community profiles ▪ Leakage profiles allow bypassing egress VLAN filtering
Trunking	▪ Supports static link aggregation groups ▪ Up to 8 Port Trunk groups

- Up to 8 member ports per Port Trunk group
- Hardware automatic failover and load balancing

Quality of Service (QoS)

- Flexible QoS classification and assignment:
  - Port based
  - MAC based
  - VLAN based
  - Protocol based
  - PCP/DEI based
  - DSCP based
  - ACL based
- QoS remarking and remapping for QoS domain translation between service provider and client networks
- Overriding of each QoS assignment according to the configured priority

Shaping and Scheduling

- 8 queues on each physical port
- Shaping per port, per queue, per queue group

Access Control List

- Ingress and Egress ACL tables
- Up to 128 ACL rules (limited by RouterOS)
- Classification based on ports, L2, L3, L4 protocol header fields
- ACL actions include filtering, forwarding and modifying of the protocol header fields

Cloud Router Switch models

This table clarifies main differences between Cloud Router Switch models.

Model	Switch Chip	CPU	Wireless	SFP+ port	Access Control List	Jumbo Frame (Bytes)
CRS105-5S-FB	**QCA-8511**	**400MHz**	**-**	**-**	+	**9204**
CRS106-1C-5S	**QCA-8511**	**400MHz**	**-**	**-**	+	**9204**
CRS112-8G-4S	**QCA-8511**	**400MHz**	**-**	**-**	+	**9204**
CRS210-8G-2S+	**QCA-8519**	**400MHz**	**-**	+	+	**9204**
CRS212-1G-10S-1S+	**QCA-8519**	**400MHz**	**-**	+	+	**9204**
CRS226-24G-2S+	**QCA-8519**	**400MHz**	**-**	+	+	**9204**
CRS125-24G-1S	**QCA-8513L**	**600MHz**	**-**	**-**	**-**	**4064**
CRS125-24G-1S-2HnD	**QCA-8513L**	**600MHz**	+	**-**	**-**	**4064**
CRS109-8G-1S-2HnD	**QCA-8513L**	**600MHz**	+	**-**	**-**	**4064**

Cloud Router Switch configuration examples

Abbreviations and Explanations

CVID - Customer VLAN id: inner VLAN tag id of the IEEE 802.1ad frame

SVID - Service VLAN id: outer VLAN tag id of the IEEE 802.1ad frame

IVL - Independent VLAN learning - learning/lookup is based on both MAC addresses and VLAN IDs.

SVL - Shared VLAN learning - learning/lookup is based on MAC addresses - not on VLAN IDs.

TPID - Tag Protocol Identifier

PCP - Priority Code Point: a 3-bit field which refers to the IEEE 802.1p priority

DEI - Drop Eligible Indicator

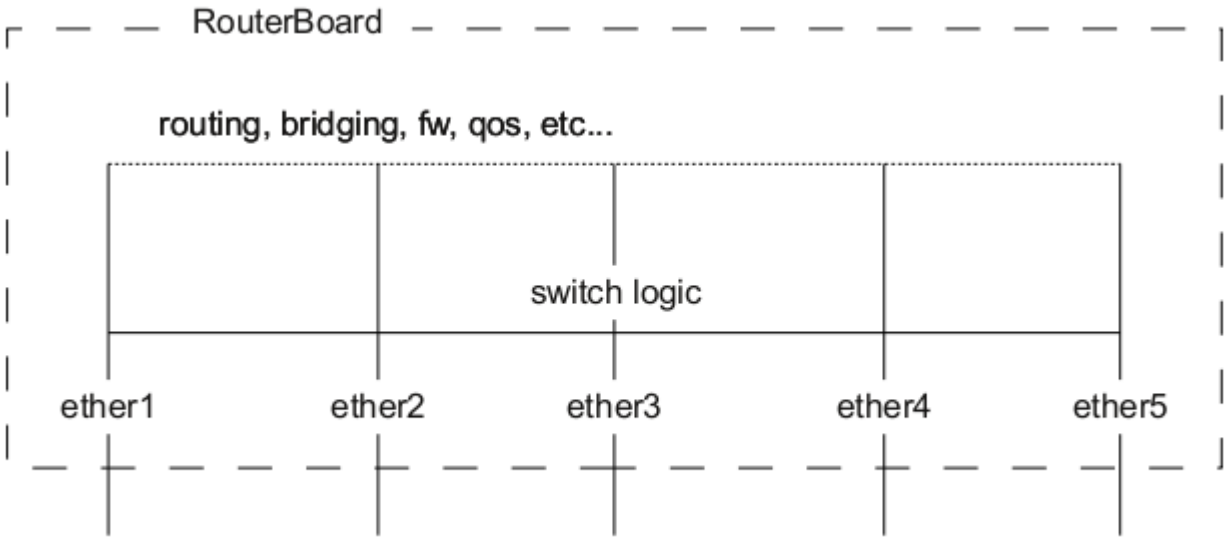
DSCP - Differentiated services Code Point

Drop precedence - internal CRS switch QoS attribute used for packet enqueuing or dropping.

Port Switching

Similarly to other RouterBoards, port switching on CRS allows wire-speed traffic forwarding among a group of ports, like the ports were a regular Ethernet switch. This feature is configurable by setting a "master-port" property to one or more ports in `/interface ethernet menu`. The "master-port" will be the port through which the RouterOS will communicate to all ports in the group. Interfaces which have the "master-port" specified become isolated - no traffic can be received and no traffic can be sent out directly from RouterOS.

Here is a general diagram of RouterBoard with a five port switch chip:



A packet that is received by one of the ports always passes through the switch logic first. Switch logic decides to which ports the packet should be going to. Passing packet "up" or giving it to RouterOS is also called sending it to switch chip's "CPU" port. It means at that point switch forwards the packet to CPU port the packet starts to get processed by RouterOS as incoming packet of the "master-port". If the packet does not have to go to "CPU" port, it is handled entirely by switch logic, does not require any CPU resources and happens at wire-speed.

Additionally, CRS series switches support multiple "master-port" configurations and have no port selection limitations for a port group which makes possible many various switched port combinations with all CRS switch interfaces. But no port can be in more than one switch group.

For example, consider a CRS125 switch with 24 Ethernet interfaces and 1 SFP interface:

```
[admin@MikroTik] > interface ethernet print
Flags: X - disabled, R - running, S - slave
 #    NAME            MTU MAC-ADDRESS       ARP        MASTER-PORT          SWITCH
 0 R  ether1         1500 D4:CA:6D:F9:FE:2F enabled    none                 switch1
 1    ether2         1500 D4:CA:6D:F9:FE:30 enabled    none                 switch1
 2    ether3         1500 D4:CA:6D:F9:FE:31 enabled    none                 switch1
 3    ether4         1500 D4:CA:6D:F9:FE:32 enabled    none                 switch1
 4 R  ether5         1500 D4:CA:6D:F9:FE:33 enabled    none                 switch1
 5 R  ether6         1500 D4:CA:6D:F9:FE:34 enabled    none                 switch1
 6    ether7         1500 D4:CA:6D:F9:FE:35 enabled    none                 switch1
 7    ether8         1500 D4:CA:6D:F9:FE:36 enabled    none                 switch1
...
22    ether23        1500 D4:CA:6D:F9:FE:45 enabled    none                 switch1
23 R  ether24        1500 D4:CA:6D:F9:FE:46 enabled    none                 switch1
24    sfp1           1500 D4:CA:6D:F9:FE:47 enabled    none                 switch1
```

And there are configured 3 switch groups: 1) ether2, ether3, ether4, ether5, ether6; 2) ether13, ether14, ether15, ether16, ether17, ether18, ether19, ether20; 3) ether21, ether22, ether23, ether24, sfp1.

Ports ether1, ether7-ether12 are not switched in this example, they remain as independent router ports.

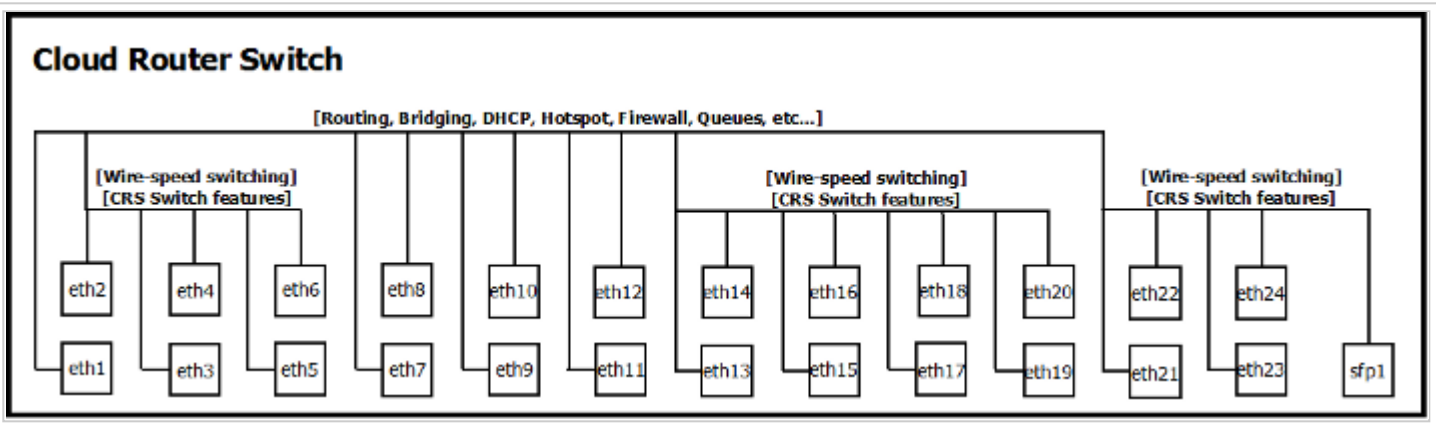
```
[admin@MikroTik] /interface ethernet>
set ether3,ether4,ether5,ether6 master-port=ether2
[admin@MikroTik] /interface ethernet>
set ether14,ether15,ether16,ether17,ether18,ether19,ether20 master-port=ether13
[admin@MikroTik] /interface ethernet>
set ether22,ether23,ether24,sfp1 master-port=ether21

[admin@MikroTik] /interface ethernet> print
```

```
Flags: X - disabled, R - running, S - slave
 #    NAME            MTU MAC-ADDRESS       ARP        MASTER-PORT          SWITCH
 0 R  ether1         1500 D4:CA:6D:F9:FE:2F enabled    none                 switch1
 1 R  ether2         1500 D4:CA:6D:F9:FE:30 enabled    none                 switch1
 2  S ether3         1500 D4:CA:6D:F9:FE:31 enabled    ether2               switch1
 3  S ether4         1500 D4:CA:6D:F9:FE:32 enabled    ether2               switch1
 4 RS ether5         1500 D4:CA:6D:F9:FE:33 enabled    ether2               switch1
 5 RS ether6         1500 D4:CA:6D:F9:FE:34 enabled    ether2               switch1
 6    ether7         1500 D4:CA:6D:F9:FE:35 enabled    none                 switch1
 7    ether8         1500 D4:CA:6D:F9:FE:36 enabled    none                 switch1
 8    ether9         1500 D4:CA:6D:F9:FE:37 enabled    none                 switch1
 9    ether10        1500 D4:CA:6D:F9:FE:38 enabled    none                 switch1
10    ether11        1500 D4:CA:6D:F9:FE:39 enabled    none                 switch1
11    ether12        1500 D4:CA:6D:F9:FE:3A enabled    none                 switch1
12 R  ether13        1500 D4:CA:6D:F9:FE:3B enabled    none                 switch1
13  S ether14        1500 D4:CA:6D:F9:FE:3C enabled    ether13              switch1
14  S ether15        1500 D4:CA:6D:F9:FE:3D enabled    ether13              switch1
15 RS ether16        1500 D4:CA:6D:F9:FE:3E enabled    ether13              switch1
16  S ether17        1500 D4:CA:6D:F9:FE:3F enabled    ether13              switch1
17  S ether18        1500 D4:CA:6D:F9:FE:40 enabled    ether13              switch1
18  S ether19        1500 D4:CA:6D:F9:FE:41 enabled    ether13              switch1
19  S ether20        1500 D4:CA:6D:F9:FE:42 enabled    ether13              switch1
20 R  ether21        1500 D4:CA:6D:F9:FE:43 enabled    none                 switch1
21  S ether22        1500 D4:CA:6D:F9:FE:44 enabled    ether21              switch1
22  S ether23        1500 D4:CA:6D:F9:FE:45 enabled    ether21              switch1
23 RS ether24        1500 D4:CA:6D:F9:FE:46 enabled    ether21              switch1
24  S sfp1           1500 D4:CA:6D:F9:FE:47 enabled    ether21              switch1
```

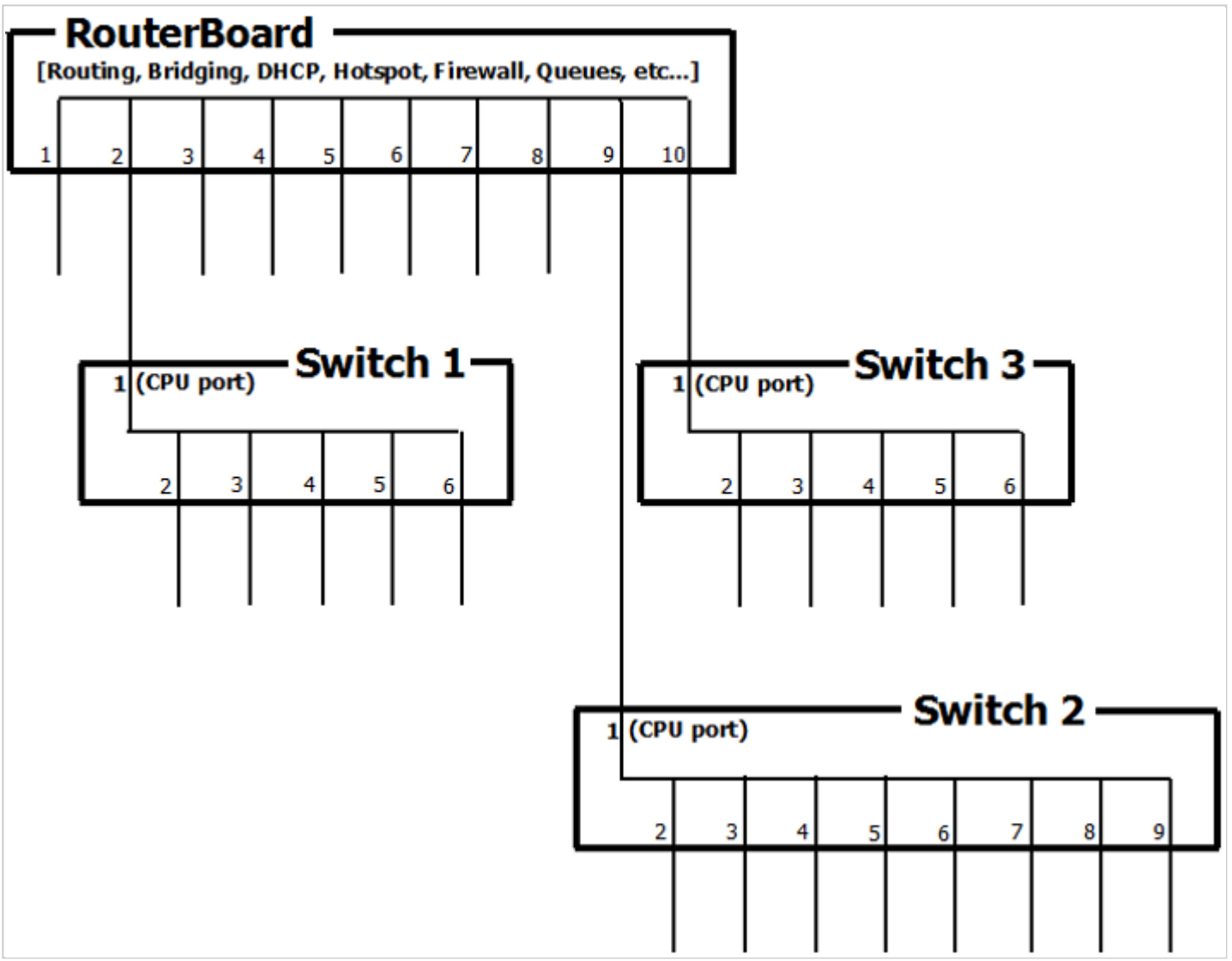
Now ether2 is the “master-port” of the group 1, ether13 – of the group 2 and ether21 – of the group 3.

Note: Previously a link was detected only on interfaces with a physical connection, but now since the ether2, ether13 and ether21 have connection to CPU, the running flag is propagated to them, as well.



CRS Port Switching Example

In essence this configuration is the same as if you had a RouterBoard with 10 Ethernet interfaces and 3 switches:



CRS Port Switching Logic

Note: Dynamic reserved VLAN entries (VLAN4091; VLAN4090; VLAN4089; etc.) are created in CRS switch when switched port groups are added by setting new master-ports. These VLANs are necessary for internal operation and have lower precedence than user configured VLANs.

Note: Multiple master-port configuration is designed as fast and simple port isolation solution, but it limits a part of VLAN functionality supported by CRS switch-chip. For advanced configurations use one master-port within CRS switch chip for all ports, configure VLANs and isolate port groups with port isolation profile configuration.

Bridge Hardware Offloading

More details about the bridge hardware offloading feature can be found in the Bridge Hardware Offloading section.

Global Settings

Sub-menu: `/interface ethernet switch`

CRS switch chip is configurable from the `/interface ethernet switch` console menu.

Property	Description
name (*string value*; Default: **switch1**)	Name of the switch.
bridge-type (*customer-vid-used-as-lookup-vid* | *service-vid-used-as-lookup-vid*; Default: **customer-vid-used-as-lookup-vid**)	Bridge type defines which VLAN tag is used as Lookup-VID. Lookup-VID serves as the VLAN key for all VLAN-based lookup.
mac-level-isolation (*yes* | *no*; Default: **yes**)	Enables or disables MAC level isolation.
use-svid-in-one2one-vlan-lookup (*yes* | *no*; Default: **no**)	Whether to use service VLAN id for 1:1 VLAN switching lookup.
use-cvid-in-one2one-vlan-lookup (*yes* | *no*; Default: **yes**)	Whether to use customer VLAN id for 1:1 VLAN switching lookup.
multicast-lookup-mode (*dst-ip-and-vid-for-ipv4* | *dst-mac-and-vid-always*; Default:**dst-ip-and-vid-for-ipv4**)	Lookup mode for IPv4 multicast bridging. - `dst-mac-and-vid-always` - For all packet types lookup key is destination MAC and VLAN id. - `dst-ip-and-vid-for-ipv4` - For IPv4 packets lookup key is destination IP and VLAN id. For other packet types lookup key is destination MAC and VLAN id.
unicast-fdb-timeout (*time interval*; Default: **5m**)	Timeout for Unicast FDB entries.
override-existing-when-ufdb-full (*yes* | *no*; Default: **no**)	Enable or disable to override existing entry which has the lowest aging value when UFDB is full.

Property	Description
drop-if-no-vlan-assignment-on-ports (*ports*; Default: **none**)	Ports which drop frames if no MAC-based, Protocol-based VLAN assignment or Ingress VLAN Translation is applied.
drop-if-invalid-or-src-port--not-member-of-vlan-on-ports (*ports*; Default: **none**)	Ports which drop invalid and other port VLAN id frames.
unknown-vlan-lookup-mode (*ivl* | *svl*; Default: **svl**)	Lookup and learning mode for packets with invalid VLAN.

forward-unknown-vlan (*yes* | *no*; Default: **yes**)	Whether to allow forwarding VLANs which are not members of VLAN table.

Property	Description
bypass-vlan-ingress-filter-for (*protocols*; Default: **none**)	Protocols which are excluded from Ingress VLAN filtering. These protocols are not dropped if they have invalid VLAN. (arp, dhcpv4, dhcpv6, eapol, igmp, mld, nd, pppoe-discovery, ripv1)
bypass-ingress-port-policing-for (*protocols*; Default: **none**)	Protocols which are excluded from Ingress Port Policing. (arp, dhcpv4, dhcpv6, eapol, igmp, mld, nd, pppoe-discovery, ripv1)
bypass-l2-security-check-filter-for (*protocols*; Default: **none**)	Protocols which are excluded from Policy rule security check. (arp, dhcpv4, dhcpv6, eapol, igmp, mld, nd, pppoe-discovery, ripv1)

Property	Description
ingress-mirror0 (*port* | *trunk,format*; Default: **none,modified**)	The first ingress mirroring analyzer port or trunk and mirroring format: - `analyzer-configured` - The packet is same as the packet to destination. VLAN format is modified based on the VLAN configurations of the analyzer port. - `modified` - The packet is same as the packet to destination. VLAN format is modified based on the VLAN configurations of the egress port. - `original` - Traffic is mirrored without any change to the original incoming packet format. But service VLAN tag is stripped in edge port.
ingress-mirror1 (*port* | *trunk,format*; Default: **none,modified**)	The second ingress mirroring analyzer port or trunk and mirroring format: - `analyzer-configured` - The packet is same as the packet to destination. VLAN format is modified based on the VLAN configurations of the analyzer port. - `modified` - The packet is same as the packet to destination. VLAN format is modified based on the VLAN configurations of the egress port. - `original` - Traffic is mirrored without any change to the original incoming packet format.

	But service VLAN tag is stripped in edge port.
ingress-mirror-ratio (*1/32768..1/1*; Default: **1/1**)	Proportion of ingress mirrored packets compared to all packets.
egress-mirror0 (*port* | *trunk,format*; Default: **none,modified**)	The first egress mirroring analyzer port or trunk and mirroring format: ▪ `analyzer-configured` - The packet is same as the packet to destination. VLAN format is modified based on the VLAN configurations of the analyzer port. ▪ `modified` - The packet is same as the packet to destination. VLAN format is modified based on the VLAN configurations of the egress port. ▪ `original` - Traffic is mirrored without any change to the original incoming packet format. But service VLAN tag is stripped in edge port.
egress-mirror1 (*port* | *trunk,format*; Default: **none,modified**)	The second egress mirroring analyzer port or trunk and mirroring format: ▪ `analyzer-configured` - The packet is same as the packet to destination. VLAN format is modified based on the VLAN configurations of the analyzer port. ▪ `modified` - The packet is same as the packet to destination. VLAN format is modified based on the VLAN configurations of the egress port. ▪ `original` - Traffic is mirrored without any change to the original incoming packet format. But service VLAN tag is stripped in edge port.
egress-mirror-ratio (*1/32768..1/1*; Default: **1/1**)	Proportion of egress mirrored packets compared to all packets.
mirror-egress-if-ingress-mirrored (*yes* | *no*; Default: **no**)	When packet is applied to both ingress and egress mirroring, if this setting is disabled, only ingress mirroring is performed on the packet; if this setting is enabled both mirroring types are applied.
mirror-tx-on-mirror-port (*yes* | *no*; Default: **no**)	
mirrored-packet-qos-priority (*0..7*; Default: **0**)	Remarked priority in mirrored packets.
mirrored-packet-drop-precedence (*drop* | *green* | *red* | *yellow*; Default: **green**)	Remarked drop precedence in mirrored packets. This QoS attribute is used for mirrored packet enqueuing or dropping.

fdb-uses (*mirror0* | *mirror1*; Default: **mirror0**)	Analyzer port used for FDB-based mirroring.
vlan-uses (*mirror0* | *mirror1*; Default: **mirror0**)	Analyzer port used for VLAN-based mirroring.

Port Settings

Sub-menu: `/interface ethernet switch port`

Property	Description
vlan-type (*edge-port* | *network-port*; Default: **network-port**)	Port VLAN type specifies whether VLAN id is used in UFDB learning. Network port learns VLAN id in UFDB, edge port does not - VLAN 0. It can be observed only in IVL learning mode.
isolation-leakage-profile-override (*yes* | *no*; Default: **!isolation-leakage-profile-override**) **isolation-leakage-profile** (*0..31*;)	Custom port profile for port isolation/leakage configurations. ▪ Port-level isolation profile 0. Uplink port - allows the port to communicate with all ports in the device. ▪ Port-level isolation profile 1. Isolated port - allows the port to communicate only with uplink ports. ▪ Port-level isolation profile 2 - 31. Community port - allows communication among the same community ports and uplink ports.
learn-override (*yes* | *no*; Default: **!learn-override**) **learn-limit** (*1..1023*; Default: **!learn-limit**)	Enable or disable MAC address learning and set MAC limit on the port. MAC learning limit is disabled by default when !learn-override and !learn-limit
drop-when-ufdb-entry-src-drop (*yes* | *no*; Default: **yes**)	Enable or disable to drop packets when UFDB entry has action `src-drop`.
allow-unicast-loopback (*yes* | *no*; Default: **no**)	Unicast loopback on port. When enabled, it permits sending back when source port and destination port are the same one for known unicast packets.
allow-multicast-loopback (*yes* | *no*; Default: **no**)	Multicast loopback on port. When enabled, it permits sending back when source port and destination port are the same for registered multicast or broadcast packets.
action-on-static-station-move (*copy-to-cpu* | *drop* | *forward* | *redirect-to-cpu*; Default: **forward**)	Action for packets when UFDB already contains static entry with such MAC but with a different port.

drop-dynamic-mac-move (*yes* | *no*; Default: **no**)	Prevents MAC relearning until UFDB timeout if MAC is already learned on other port.

Property	Description
allow-fdb-based-vlan-translate (*yes* | *no*; Default: **no**)	Enable or disable MAC-based VLAN translation on the port.
allow-mac-based-service-vlan-assignment-for (*all-frames* | *none* | *tagged-frame-only* | *untagged-and-priority-tagged-frame-only*; Default: **none**)	Frame type for which applies MAC-based service VLAN translation.
allow-mac-based-customer-vlan-assignment-for (*all-frames* | *none* | *tagged-frame-only* | *untagged-and-priority-tagged-frame-only*; Default: **none**)	Frame type for which applies MAC-based customer VLAN translation.
default-customer-pcp (*0..7*; Default: **0**)	Default customer PCP of the port.
default-service-pcp (*0..7*; Default: **0**)	Default service PCP of the port.
pcp-propagation-for-initial-pcp (*yes* | *no*; Default: **no**)	Enables or disables PCP propagation for initial PCP assignment on ingress. ▪ If the port `vlan-type` is Edge port, the service PCP is copied from the customer PCP. ▪ If the port `vlan-type` is Network port, the customer PCP is copied from the service PCP.
filter-untagged-frame (*yes* | *no*; Default: **no**)	Whether to filter untagged frames on the port.
filter-priority-tagged-frame (*yes* | *no*; Default: **no**)	Whether to filter tagged frames with priority on the port.
filter-tagged-frame (*yes* | *no*; Default: **no**)	Whether to filter tagged frames on the port.

Property	Description
egress-vlan-tag-table-lookup-key (*according-to-bridge-type* | *egress-vid*; Default: **egress-vid**)	Egress VLAN table (VLAN Tagging) lookup: ▪ `egress-vid` - Lookup VLAN id is CVID when Edge port is configured, SVID when Network port is configured.

	▪ according-to-bridge-type - Lookup VLAN id is CVID when customer VLAN bridge is configured, SVID when service VLAN bridge is configured. Customer tag is unmodified for Edge port in service VLAN bridge.
egress-vlan-mode (*tagged* | *unmodified* | *untagged*; Default: **unmodified**)	Egress VLAN tagging action on the port.
egress-pcp-propagation (*yes* | *no*; Default: **no**)	Enables or disables egress PCP propagation. ▪ If the port vlan-type is Edge port, the service PCP is copied from the customer PCP. ▪ If the port vlan-type is Network port, the customer PCP is copied from the service PCP.

Property	Description
ingress-mirror-to (*mirror0* | *mirror1* | *none*; Default: **none**)	Analyzer port for port-based ingress mirroring.
ingress-mirroring-according-to-vlan (*yes* | *no*; Default: **no**)	
egress-mirror-to (*mirror0* | *mirror1* | *none*; Default: **none**)	Analyzer port for port-based egress mirroring.

Property	Description
qos-scheme-precedence (*da-based* | *dscp-based* | *ingress-acl-based* | *pcp-based* | *protocol-based* | *sa-based* | *vlan-based*; Default: **pcp-based, sa-based, da-based, dscp-based, protocol-based, vlan-based**)	Specifies applied QoS assignment schemes on ingress of the port. ▪ da-based ▪ dscp-based ▪ ingress-acl-based ▪ pcp-based ▪ protocol-based ▪ sa-based ▪ vlan-based
pcp-or-dscp-based-qos-change-dei (*yes* | *no*; Default: **no**)	Enable or disable PCP or DSCP based DEI change on port.
pcp-or-dscp-based-qos-change-pcp (*yes* | *no*; Default: **no**)	Enable or disable PCP or DSCP based PCP change on port.
pcp-or-dscp-based-qos-change-dscp (*yes* | *no*; Default: **no**)	Enable or disable PCP or DSCP based DSCP change on port.

dscp-based-qos-dscp-to-dscp-mapping (*yes* | *no*; Default: **yes**)	Enable or disable DSCP to internal DSCP mapping on port.
pcp-based-qos-drop-precedence-mapping (*PCP/DEI-range:drop-precedence*; Default: **0-15:green**)	The new value of drop precedence for the PCP/DEI to drop precedence (drop | green | red | yellow) mapping. Multiple mappings allowed separated by comma e.g. "0-7:yellow,8-15:red".
pcp-based-qos-dscp-mapping (*PCP/DEI-range:DEI*; Default: **0-15:0**)	The new value of DSCP for the PCP/DEI to DSCP (0..63) mapping. Multiple mappings allowed separated by comma e.g. "0-7:25,8-15:50".
pcp-based-qos-dei-mapping (*PCP/DEI-range:DEI*; Default: **0-15:0**)	The new value of DEI for the PCP/DEI to DEI (0..1) mapping. Multiple mappings allowed separated by comma e.g. "0-7:0,8-15:1".
pcp-based-qos-pcp-mapping (*PCP/DEI-range:DEI*; Default: **0-15:0**)	The new value of PCP for the PCP/DEI to PCP (0..7) mapping. Multiple mappings allowed separated by comma e.g. "0-7:3,8-15:4".
pcp-based-qos-priority-mapping (*PCP/DEI-range:DEI*; Default: **0-15:0**)	The new value of internal priority for the PCP/DEI to priority (0..15) mapping. Multiple mappings allowed separated by comma e.g. "0-7:5,8-15:15".

Property	Description
priority-to-queue (*priority-range:queue*; Default: **0-15:0,1:1,2:2,3:3**)	Internal priority (0..15) mapping to queue (0..7) per port.
per-queue-scheduling (*Scheduling-type:Weight*; Default: **wrr-group0:1,wrr-group0:2,wrr-group0:4,wrr-group0:8,wrr-group0:16,wrr-group0:32,** **wrr-group0:64,wrr-group0:128**)	Set port to use either strict or weighted round robin policy for traffic shaping for each queue group, each queue is separated by a comma.

Property	Description
ingress-customer-tpid-override (*yes* | *no*; Default:**!ingress-customer-tpid-override**)	Ingress customer TPID override allows accepting specific frames with a custom customer tag TPID. Default value is for tag of 802.1Q frames.
ingress-customer-tpid (*0..10000*; Default: **0x8100**)	
egress-customer-tpid-override (*yes* | *no*; Default: **!egress-customer-tpid-override**)	Egress customer TPID override allows custom identification for egress frames with a customer tag. Default value is for tag of 802.1Q frames.
egress-customer-tpid (*0..10000*; Default: **0x8100**)	
ingress-service-tpid-override (*yes* | *no*; Default:	Ingress service TPID override allows accepting

!ingress-service-tpid-override)	specific frames with a custom service tag TPID. Default value is for service tag of 802.1AD frames.
`ingress-service-tpid` (*0..10000*; Default: **0x88A8**)	
`egress-service-tpid-override` (*yes* | *no*; Default:	Egress service TPID override allows custom identification for egress frames with a service tag. Default value is for service tag of 802.1AD frames.
!egress-service-tpid-override)	
`egress-service-tpid` (*0..10000*; Default:	
0x88A8)	

Property	Description
`custom-drop-counter-includes` (*counters*; Default: **none**)	Custom include to count dropped packets for switch port `custom-drop-packet` counter. ▪ **device-loopback** ▪ **fdb-hash-violation** ▪ **exceeded-port-learn-limitation** ▪ **dynamic-station-move** ▪ **static-station-move** ▪ **ufdb-source-drop** ▪ **host-source-drop** ▪ **unknown-host** ▪ **ingress-vlan-filtered**
`queue-custom-drop-counter0-includes` (*counters*; Default: **none**)	Custom include to count dropped packets for switch port `tx-queue-custom0-drop-packet` and bytes for `tx-queue-custom0-drop-byte` counters. ▪ **red** ▪ **yellow** ▪ **green** ▪ **queue0** ▪ **...** ▪ **queue7**
`queue-custom-drop-counter1-includes` (*counters*; Default: **none**)	Custom include to count dropped packets for switch port `tx-queue-custom1-drop-packet` and bytes for `tx-queue-custom1-drop-byte` counters. ▪ **red** ▪ **yellow** ▪ **green** ▪ **queue0** ▪ **...** ▪ **queue7**
`policy-drop-counter-includes` (*counters*; Default:	Custom include to count dropped packets for switch

none)	port `policy-drop-packet` counter. ▪ **ingress-policing** ▪ **ingress-acl** ▪ **egress-policing** ▪ **egress-acl**

Forwarding Databases

Unicast FDB

Sub-menu: `/interface ethernet switch unicast-fdb`

The unicast forwarding database supports up to 16318 MAC entries.

Property	Description
`action` (*action*; Default: **forward**)	Action for UFDB entry: ▪ `dst-drop` - Packets are dropped when their destination MAC match the entry. ▪ `dst-redirect-to-cpu` - Packets are redirected to CPU when their destination MAC match the entry. ▪ `forward` - Packets are forwarded. ▪ `src-and-dst-drop` - Packets are dropped when their source MAC or destination MAC match the entry. ▪ `src-and-dst-redirect-to-cpu` - Packets are redirected to CPU when their source MAC or destination MAC match the entry. ▪ `src-drop` - Packets are dropped when their source MAC match the entry. ▪ `src-redirect-to-cpu` - Packets are redirected to CPU when their source MAC match the entry.
`disabled` (*yes* | *no*; Default: **no**)	Enables or disables Unicast FDB entry.
`isolation-profile` (*community1* | *community2* | *isolated* | *promiscuous*; Default: **promiscuous**)	MAC level isolation profile.
`mac-address` (*MAC address*)	The `action` command applies to the packet when the destination MAC or source MAC matches the entry.
`mirror` (*yes* | *no*; Default: **no**)	Enables or disables mirroring based on source MAC or destination MAC.
`port` (*port*)	Matching port for the Unicast FDB entry.
`qos-group` (*none*; Default: **none**)	Defined QoS group from QoS group menu.

svl (*yes* | *no*; Default: **no**)	Unicast FDB learning mode: ▪ Shared VLAN Learning (svl) - learning/lookup is based on MAC addresses - not on VLAN IDs. ▪ Independent VLAN Learning (ivl) - learning/lookup is based on both MAC addresses and VLAN IDs.
vlan-id (*0..4095*)	Unicast FDB lookup/learning VLAN id.

Multicast FDB

Sub-menu: `/interface ethernet switch multicast-fdb`

CRS125 switch-chip supports up to 1024 entries in MFDB for multicast forwarding. For each multicast packet, destination MAC or destination IP lookup is performed in MFDB. MFDB entries are not automatically learnt and can only be configured.

Property	Description
address (*X.X.X.X* | *XX:XX:XX:XX:XX:XX*)	Matching IP address or MAC address for multicast packets.
bypass-vlan-filter (*yes* | *no*; Default: **no**)	Allow to bypass VLAN filtering for matching multicast packets.
disabled (*yes* | *no*; Default: **no**)	Enables or disables Multicast FDB entry.
ports (*ports*)	Member ports for multicast traffic.
qos-group (*none*; Default: **none**)	Defined QoS group from QoS group menu.
svl (*yes* | *no*; Default: **no**)	Multicast FDB learning mode: ▪ Shared VLAN Learning (svl) - learning/lookup is based on MAC addresses - not on VLAN IDs. ▪ Independent VLAN Learning (ivl) - learning/lookup is based on both MAC addresses and VLAN IDs.
vlan-id (*0..4095*; Default: **0**)	Multicast FDB lookup VLAN id. If VLAN learning mode is IVL, VLAN id is lookup id, otherwise VLAN id = 0.

Reserved FDB

Sub-menu: `/interface ethernet switch reserved-fdb`

Cloud Router Switch supports 256 RFDB entries. Each RFDB entry can store either Layer2 unicast or multicast MAC address with specific commands.

Property	Description
action (*copy-to-cpu* | *drop* | *forward* | *redirect-to-cpu*; Default: **forward**)	Action for RFDB entry: - copy-to-cpu - Packets are copied to CPU when their destination MAC match the entry. - drop - Packets are dropped when their destination MAC match the entry. - forward - Packets are forwarded when their destination MAC match the entry. - redirect-to-cpu - Packets are redirected to CPU when their destination MAC match the entry.
bypass-ingress-port-policing (*yes* | *no*; Default: **no**)	Allow to bypass Ingress Port Policer for matching packets.
bypass-ingress-vlan-filter (*yes* | *no*; Default: **no**)	Allow to bypass VLAN filtering for matching packets.
disabled (*yes* | *no*; Default: **no**)	Enables or disables Reserved FDB entry.
mac-address (*MAC address*; Default: **00:00:00:00:00:00**)	Matching MAC address for Reserved FDB entry.
qos-group (*none*; Default: **none**)	Defined QoS group from QoS group menu.

VLAN

VLAN Table

Sub-menu: `/interface ethernet switch vlan`

The VLAN table supports 4096 VLAN entries for storing VLAN member information as well as other VLAN information such as QoS, isolation, forced VLAN, learning, and mirroring.

Property	Description
disabled (*yes* | *no*; Default: **no**)	Indicate whether the VLAN entry is disabled. Only enabled entry is applied to lookup process and forwarding decision.
flood (*yes* | *no*; Default: **no**)	Enables or disables forced VLAN flooding per VLAN. If the feature is

	enabled, the result of destination MAC lookup in the UFDB or MFDB is ignored, and the packet is forced to flood in the VLAN.
ingress-mirror (*yes* | *no*; Default: **no**)	Enable the ingress mirror per VLAN to support the VLAN-based mirror function.
learn (*yes* | *no*; Default: **yes**)	Enables or disables source MAC learning for VLAN.
ports (*ports*)	Member ports of the VLAN.
qos-group (*none*; Default: **none**)	Defined QoS group from QoS group menu.
svl (*yes* | *no*; Default: **no**)	FDB lookup mode for lookup in UFDB and MFDB. ▪ Shared VLAN Learning (svl) - learning/lookup is based on MAC addresses - not on VLAN IDs. ▪ Independent VLAN Learning (ivl) - learning/lookup is based on both MAC addresses and VLAN IDs.
vlan-id (*0..4095*)	VLAN id of the VLAN member entry.

Egress VLAN Tag

Sub-menu: `/interface ethernet switch egress-vlan-tag`

Egress packets can be assigned different VLAN tag format. The VLAN tags can be removed, added, or remained as is when the packet is sent to the egress port (destination port). Each port has dedicated control on the egress VLAN tag format. The tag formats include:

- Untagged
- Tagged
- Unmodified

The Egress VLAN Tag table includes 4096 entries for VLAN tagging selection.

Property	Description
disabled (*yes* | *no*; Default: **no**)	Enables or disables Egress VLAN Tag table entry.
tagged-ports (*ports*)	Ports which are tagged in egress.
vlan-id (*0..4095*)	VLAN id which is tagged in egress.

Ingress/Egress VLAN Translation

The Ingress VLAN Translation table allows for up to 16 entries for each port. One or multiple fields can be selected from packet header for lookup in the Ingress VLAN Translation table. The S-VLAN or C-VLAN or both configured in the first matched entry is assigned to the packet.

Sub-menu: `/interface ethernet switch ingress-vlan-translation`

Sub-menu: `/interface ethernet switch egress-vlan-translation`

Property	Description
customer-dei (*0..1*; Default: **none**)	Matching DEI of the customer tag.
customer-pcp (*0..7*; Default: **none**)	Matching PCP of the customer tag.
customer-vid (*0..4095*; Default: **none**)	Matching VLAN id of the customer tag.
customer-vlan-format (*any* | *priority-tagged-or-tagged* | *tagged* | *untagged-or-tagged*; Default:**any**)	Type of frames with customer tag for which VLAN translation rule is valid.
disabled (*yes* | *no*; Default: **no**)	Enables or disables VLAN translation entry.
new-customer-vid (*0..4095*; Default: **none**)	The new customer VLAN id which replaces matching customer VLAN id. If set to 4095 and ingress VLAN translation is used, then traffic is dropped.
new-service-vid (*0..4095*; Default: **none**)	The new service VLAN id which replaces matching service VLAN id.
pcp-propagation (*yes* | *no*; Default: **no**)	Enables or disables PCP propagation. ▪ If the port type is Edge, the customer PCP is copied from the service PCP. ▪ If the port type is Network, the service PCP is copied from the customer PCP.
ports (*ports*)	Matching switch ports for VLAN translation rule.
protocol (*protocols*; Default: **none**)	Matching Ethernet protocol. *(only for Ingress VLAN Translation)*
sa-learning (*yes* | *no*; Default: **no**)	Enables or disables source MAC learning after VLAN translation. *(only for Ingress VLAN Translation)*
service-dei (*0..1*; Default: **none**)	Matching DEI of the service tag.
service-pcp (*0..7*; Default: **none**)	Matching PCP of the service tag.
service-vid (*0..4095*; Default: **none**)	Matching VLAN id of the service tag.
service-vlan-format (*any* | *priority-tagged-or-tagged* | *tagged* | *untagged-or-tagged*; Default:**any**)	Type of frames with service tag for which VLAN translation rule is valid.

Below is a table of traffic that triggers a rule that has a certain VLAN format set, note that traffic that is tagged with VLAN ID 0 is a special case that is also taken into account.

Property	Description
any	Accepts: ▪ Untagged traffic ▪ Tagged traffic ▪ Tagged traffic with priority set ▪ VLAN 0 traffic ▪ VLAN 0 traffic with priority set
priority-tagged-or-tagged	Accepts: ▪ Tagged traffic ▪ Tagged traffic with priority set ▪ VLAN 0 traffic ▪ VLAN 0 traffic with priority set
tagged	Accepts: ▪ Tagged traffic ▪ Tagged traffic with priority set
untagged-or-tagged	Accepts: ▪ Untagged traffic ▪ Tagged traffic ▪ Tagged traffic with priority set

Warning: If `VLAN-format` is set to `any`, then `customer-vid/service-vid` set to `0` will trigger the switch rule with VLAN 0 traffic. In this case the switch rule will be looking for untagged traffic or traffic with VLAN 0 tag, only `untagged-or-tagged` will filter out VLAN 0 traffic in this case.

Protocol Based VLAN

Sub-menu: `/interface ethernet switch protocol-based-vlan`

Protocol Based VLAN table is used to assign VID and QoS attributes to related protocol packet per port.

Property	Description
disabled (*yes* | *no*; Default: **no**)	Enables or disables Protocol Based VLAN entry.

frame-type (*ethernet* | *llc* | *rfc-1042*; Default: **ethernet**)	Encapsulation type of the matching frames.
new-customer-vid (*0..4095*; Default: **0**)	The new customer VLAN id which replaces original customer VLAN id for specified protocol. If set to 4095, then traffic is dropped.
new-service-vid (*0..4095*; Default: **0**)	The new service VLAN id which replaces original service VLAN id for specified protocol.
ports (*ports*)	Matching switch ports for Protocol based VLAN rule.
protocol (*protocol*; Default: **0**)	Matching protocol for Protocol based VLAN rule.
qos-group (*none*; Default: **none**)	Defined QoS group from QoS group menu.
set-customer-vid-for (*all* | *none* | *tagged* | *untagged-or-priority-tagged*; Default: **all**)	Customer VLAN id assignment command for different packet type.
set-qos-for (*all* | *none* | *tagged* | *untagged-or-priority-tagged*; Default: **none**)	Frame type for which QoS assignment command applies.
set-service-vid-for (*all* | *none* | *tagged* | *untagged-or-priority-tagged*; Default: **all**)	Service VLAN id assignment command for different packet type.

MAC Based VLAN

Sub-menu: `/interface ethernet switch mac-based-vlan`

MAC Based VLAN table is used to assign VLAN based on source MAC.

Property	Description
disabled (*yes* | *no*; Default: **no**)	Enables or disables MAC Based VLAN entry.
new-customer-vid (*0..4095*; Default: **0**)	The new customer VLAN id which replaces original service VLAN id for matched packets. If set to 4095, then traffic is dropped.
new-service-vid (*0..4095*; Default: **0**)	The new service VLAN id which replaces original service VLAN id for matched packets.
src-mac-address (*MAC address*)	Matching source MAC address for MAC based VLAN rule.

Note: All CRS1xx/2xx series switches support up to 1024 MAC Based VLAN table entries.

1:1 VLAN Switching

Sub-menu: `/interface ethernet switch one2one-vlan-switching`

1:1 VLAN switching can be used to replace the regular L2 bridging for matched packets. When a packet hits an 1:1 VLAN switching table entry, the destination port information in the entry is assigned to the packet. The matched destination information in UFDB and MFDB entry no longer applies to the packet.

Property	Description
customer-vid (*0..4095*; Default: **0**)	Matching customer VLAN id for 1:1 VLAN switching.
disabled (*yes* | *no*; Default: **no**)	Enables or disables 1:1 VLAN switching table entry.
dst-port (*port*)	Destination port for matched 1:1 VLAN switching packets.
service-vid (*0..4095*; Default: **0**)	Matching customer VLAN id for 1:1 VLAN switching.

Port Isolation/Leakage

Sub-menu: `/interface ethernet switch port-isolation`

Sub-menu: `/interface ethernet switch port-leakage`

The CRS switches support flexible multi-level isolation features, which can be used for user access control, traffic engineering and advanced security and network management. The isolation features provide an organized fabric structure allowing user to easily program and control the access by port, MAC address, VLAN, protocol, flow and frame type. The following isolation and leakage features are supported:

- Port-level isolation
- MAC-level isolation
- VLAN-level isolation
- Protocol-level isolation
- Flow-level isolation
- Free combination of the above

Port-level isolation supports different control schemes on source port and destination port. Each entry can be programmed with access control for either source port or destination port.

- When the entry is programmed with source port access control, the entry is

applied to the ingress packets.

- When the entry is programmed with destination port access control, the entry

is applied to the egress packets.

Port leakage allows bypassing egress VLAN filtering on the port. Leaky port is allowed to access other ports for various applications such as security, network control and management. Note: When both isolation and leakage is applied to the same port, the port is isolated.

Property	Description
disabled (*yes* | *no*; Default: **no**)	Enables or disables port isolation/leakage entry.
flow-id (*0..63*; Default: **none**)	
forwarding-type (*bridged; routed*; Default: **bridged,routed**)	Matching traffic forwarding type on Cloud Router Switch.
mac-profile (*community1* | *community2* | *isolated* | *promiscuous*; Default: **none**)	Matching MAC isolation/leakage profile.
port-profile (*0..31*; Default: **none**)	Matching Port isolation/leakage profile.
ports (*ports*; Default: **none**)	Isolated/leaked ports.
protocol-type (*arp; nd; dhcpv4; dhcpv6; ripv1*; Default: **arp,nd,dhcpv4,dhcpv6,ripv1**)	Included protocols for isolation/leakage.
registration-status (*known; unknown*; Default: **known,unknown**)	Registration status for matching packets. Known are present in UFDB and MFDB, unknown are not.
traffic-type (*unicast; multicast; broadcast*; Default: **unicast,multicast,broadcast**)	Matching traffic type.
type (*dst* | *src*; Default: **src**)	Lookup type of the isolation/leakage entry: ▪ src - Entry applies to ingress packets of the ports. ▪ dst - Entry applies to egress packets of the ports.
vlan-profile (*community1* | *community2* | *isolated* | *promiscuous*; Default: **none**)	Matching VLAN isolation/leakage profile.

Trunking

Sub-menu: `/interface ethernet switch trunk`

The Trunking in the Cloud Router Switches provides static link aggregation groups with hardware automatic failover and load balancing. IEEE802.3ad and IEEE802.1ax compatible Link Aggregation Control Protocol is not supported yet. Up to 8 Trunk groups are supported with up to 8 Trunk member ports per Trunk group. CRS Port Trunking calculates transmit-hash based on all following parameters: L2 src-dst MAC + L3 src-dst IP + L4 src-dst Port.

Property	Description
disabled (*yes* | *no*; Default: **no**)	Enables or disables port trunking entry.
member-ports (*ports*)	Member ports of the Trunk group.
name (*string value*; Default: **trunkX**)	Name of the Trunk group.

Quality of Service

Shaper

Sub-menu: `/interface ethernet switch shaper`

Traffic shaping restricts the rate and burst size of the flow which is transmitted out from the interface. The shaper is implemented by a token bucket. If the packet exceeds the maximum rate or the burst size, which means no enough token for the packet, the packet is stored to buffer until there is enough token to transmit it.

Property	Description
burst (*integer*; Default: **100k**)	Maximum data rate which can be transmitted while the burst is allowed.
disabled (*yes* | *no*; Default: **no**)	Enables or disables traffic shaper entry.
meter-unit (*bit* | *packet*; Default: **bit**)	Measuring units for traffic shaper rate.
port (*port*)	Physical port for traffic shaper.
rate (*integer*; Default: **1M**)	Maximum data rate limit.
target (*port* | *queueX* | *wrr-groupX*; Default: **port**)	Three levels of shapers are supported on each port (including CPU port): ▪ `Port level` - Entry applies to port of the switch-chip. ▪ `WRR group level` - Entry applies to one of the 2 Weighted Round Robin queue groups (wrr-group0, wrr-group1) on port. ▪ `Queue level` - Entry applies to one of the 8 queues (queue0 - queue7) on port.

Ingress Port Policer

Sub-menu: `/interface ethernet switch ingress-port-policer`

Property	Description
burst (*integer*; Default: **100k**)	Maximum data rate which can be transmitted while the burst is allowed.
disabled (*yes* | *no*; Default: **no**)	Enables or disables ingress port policer entry.
meter-len (*layer-1* | *layer-2* | *layer-3*; Default: **layer-1**)	Packet classification which sets the packet byte length for metering.

	▪ `layer-1` - includes entire layer-2 frame + FCS + inter-packet gap + preamble. ▪ `layer-2` - includes layer-2 frame + FCS. ▪ `layer-3` - includes only layer-3 + ethernet padding without layer-2 header and FCS.
`meter-unit` (*bit* | *packet*; Default: **bit**)	Measuring units for traffic ingress port policer rate.
`new-dei-for-yellow` (*0..1* | *remap*; Default: **none**)	Remarked DEI for exceeded traffic if yellow-action is remark.
`new-dscp-for-yellow` (*0..63* | *remap*; Default: **none**)	Remarked DSCP for exceeded traffic if yellow-action is remark.
`new-pcp-for-yellow` (*0..7* | *remap*; Default: **none**)	Remarked PCP for exceeded traffic if yellow-action is remark.
`packet-types` (*packet-types*; Default: **all types from description**)	Matching packet types for which ingress port policer entry is valid.
`port` (*port*)	Physical port or trunk for ingress port policer entry.
`rate` (*integer*)	Maximum data rate limit.
`yellow-action` (*drop* | *forward* | *remark*; Default: **drop**)	Performed action for exceeded traffic.

QoS Group

Sub-menu: `/interface ethernet switch qos-group`

The global QoS group table is used for VLAN-based, Protocol-based and MAC-based QoS group assignment configuration.

Property	Description
`dei` (*0..1*; Default: **none**)	The new value of DEI for the QoS group.
`disabled` (*yes* | *no*; Default: **no**)	Enables or disables protocol QoS group entry.
`drop-precedence` (*drop* | *green* | *red* | *yellow*; Default: **green**)	Drop precedence is internal QoS attribute used for packet enqueuing or dropping.
`dscp` (*0..63*; Default: **none**)	The new value of DSCP for the QoS group.
`name` (*string value*; Default: **groupX**)	Name of the QoS group.
`pcp` (*0..7*; Default: **none**)	The new value of PCP for the QoS group.
`priority` (*0..15*; Default: **0**)	Internal priority is a local significance of priority for classifying traffics to different egress queues on a port. (1 is highest, 15 is lowest)

DSCP QoS Map

Sub-menu: `/interface ethernet switch dscp-qos-map`

The global DSCP to QOS mapping table is used for mapping from DSCP of the packet to new QoS attributes configured in the table.

Property	Description
dei (*0..1*)	The new value of DEI for the DSCP to QOS mapping entry.
drop-precedence (*drop* | *green* | *red* | *yellow*)	The new value of Drop precedence for the DSCP to QOS mapping entry.
pcp (*0..7*)	The new value of PCP for the DSCP to QOS mapping entry.
priority (*0..15*)	The new value of internal priority for the DSCP to QOS mapping entry.

DSCP To DSCP Map

Sub-menu: `/interface ethernet switch dscp-to-dscp`

The global DSCP to DSCP mapping table is used for mapping from the packet's original DSCP to new DSCP value configured in the table.

Property	Description
new-dscp (*0..63*)	The new value of DSCP for the DSCP to DSCP mapping entry.

Policer QoS Map

Sub-menu: `/interface ethernet switch policer-qos-map`

Property	Description
dei-for-red (*0..1*; Default: **0**)	Policer DEI remapping value for red packets.
dei-for-yellow (*0..1*; Default: **0**)	Policer DEI remapping value for yellow packets.
dscp-for-red (*0..63*; Default: **0**)	Policer DSCP remapping value for red packets.
dscp-for-yellow (*0..63*; Default: **0**)	Policer DSCP remapping value for yellow packets.

pcp-for-red (*0..7*; Default: **0**)	Policer PCP remapping value for red packets.
pcp-for-yellow (*0..7*; Default: **0**)	Policer PCP remapping value for yellow packets.

Access Control List

Note: See Summary section for Access Control List supported Cloud Router Switch devices.

Access Control List contains of ingress policy and egress policy engines and allows to configure up to 128 policy rules (limited by RouterOS). It is advanced tool for wire-speed packet filtering, forwarding, shaping and modifying based on Layer2, Layer3 and Layer4 protocol header field conditions.

ACL

Sub-menu: `/interface ethernet switch acl`

ACL condition part for MAC related fields of packets.

Property	Description
disabled (*yes* | *no*; Default: **no**)	Enables or disables ACL entry.
table (*egress* | *ingress*; Default: **ingress**)	Selects policy table for incoming or outgoing packets.
invert-match (*yes* | *no*; Default: **no**)	Inverts whole ACL rule matching.
src-ports (*ports,trunks*)	Matching physical source ports or trunks.
dst-ports (*ports,trunks*)	Matching physical destination ports or trunks.
mac-src-address (*MAC address/Mask*)	Source MAC address and mask.
mac-dst-address (*MAC address/Mask*)	Destination MAC address and mask.
dst-addr-registered (*yes* | *no*)	Defines whether to match packets with registered state - packets which destination MAC address is in UFDB/MFDB/RFDB. Valid only in egress table.
mac-protocol (*802.2* | *arp* | *ip* | *ipv6* | *ipx* | *length* | *mpls-multicast* | *mpls-unicast* | *pppoe* | *pppoe-discovery* | *rarp* | *vlan or integer: 0..65535 decimal format or 0x0000-0xffff hex format*)	Ethernet payload type (MAC-level protocol) ▪ **802.2** ▪ **arp** - Type 0x0806 - ARP ▪ **ip** - Type 0x0800 - IPv4 ▪ **ipv6** - Type 0x86dd - IPv6 ▪ **ipx** - Type 0x8137 - "Internetwork Packet Exchange" ▪ **mpls-multicast** - Type 0x8848 - MPLS Multicast ▪ **mpls-unicast** - Type 0x8847 - MPLS Unicast ▪ **ppoe** - Type 0x8864 - PPPoE Session

	▪ **ppoe-discovery** - Type 0x8863 - PPPoE Discovery ▪ **rarp** - Type 0x8035 - Reverse ARP ▪ **vlan** - Type 0x8100 - 802.1Q tagged VLAN
drop-precedence (*drop* | *green* | *red* | *yellow*)	Matching internal drop precedence. Valid only in egress table.
custom-fields	

ACL condition part for VLAN related fields of packets.

Property	Description
lookup-vid (*0..4095*)	VLAN id used in lookup. It can be changed before reaching egress table.
service-vid (*0-4095*)	Matching service VLAN id.
service-pcp (*0..7*)	Matching service PCP.
service-dei (*0..1*)	Matching service DEI.
service-tag (*priority-tagged* | *tagged* | *tagged-or-priority-tagged* | *untagged*)	Format of the service tag.
customer-vid (*0-4095*)	Matching customer VLAN id.
customer-pcp (*0..7*)	Matching customer PCP.
customer-dei (*0..1*)	Matching customer DEI.
customer-tag (*priority-tagged* | *tagged* | *tagged-or-priority-tagged* | *untagged*)	Format of the customer tag.
priority (*0..15*)	Matching internal priority. Valid only in egress table.

ACL condition part for IPv4 and IPv6 related fields of packets.

Property	Description
ip-src (*IPv4/0..32*)	Matching source IPv4 address.
ip-dst (*IPv4/0..32*)	Matching destination IPv4 address.
ip-protocol (*tcp* | *udp* | *udp-lite* | *other*)	IP protocol type.
src-l3-port (*0-65535*)	Matching Layer3 source port.
dst-l3-port (*0-65535*)	Matching Layer3 destination port.
ttl (*0* | *1* | *max* | *other*)	Matching TTL field of the packet.
dscp (*0..63*)	Matching DSCP field of the packet.
ecn (*0..3*)	Matching ECN field of the packet.

fragmented (*yes* | *no*)	Whether to match fragmented packets.
first-fragment (*yes* | *no*)	YES matches not fragmented and the first fragments, NO matches other fragments.
ipv6-src (*IPv6/0..128*)	Matching source IPv6 address.
ipv6-dst (*IPv6/0..128*)	Matching destination IPv6 address.
mac-isolation-profile (*community1* | *community2* | *isolated* | *promiscuous*)	Matches isolation profile based on UFDB. Valid only in egress policy table.
src-mac-addr-state (*dynamic-station-move* | *sa-found* | *sa-not-found* | *static-station-move*)	Defines whether to match packets with registered state - packets which destination MAC address is in UFDB/MFDB/RFDB. Valid only in egress policy table.
flow-id (*0..63*)	

ACL rule action part.

Property	Description
action (*copy-to-cpu* | *drop* | *forward* | *redirect-to-cpu* | *send-to-new-dst-ports*; Default: **forward**)	▪ `copy-to-cpu` - Packets are copied to CPU if they match the ACL conditions. ▪ `drop` - Packets are dropped if they match the ACL conditions. ▪ `forward` - Packets are forwarded if they match the ACL conditions. ▪ `redirect-to-cpu` - Packets are redirected to CPU if they match the ACL conditions. ▪ `send-to-new-dst-ports` - Packets are send to new destination ports if they match the ACL conditions.
new-dst-ports (*ports,trunks*)	If action is "send-to-new-dst-ports", then this property sets which ports/trunks is the new destination.
mirror-to (*mirror0* | *mirror1*)	Mirroring destination for ACL packets.
policer (*policer*)	Applied ACL Policer for ACL packets.
src-mac-learn (*yes* | *no*)	Whether to learn source MAC of the matched ACL packets. Valid only in ingress policy table.
new-service-vid (*0..4095*)	New service VLAN id for ACL packets.
new-service-pcp (*0..7*)	New service PCP for ACL packets.
new-service-dei (*0..1*)	New service DEI for ACL packets.
new-customer-vid (*0..4095*)	New customer VLAN id for ACL packets. If set to 4095, then traffic is dropped.

new-customer-pcp (*0..7*)	New customer PCP for ACL packets.
new-customer-dei (*0..1*)	New customer DEI for ACL packets.
new-dscp (*0..63*)	New DSCP for ACL packets.
new-priority (*0..15*)	New internal priority for ACL packets.
new-drop-precedence (*drop* | *green* | *red* | *yellow*)	New internal drop precedence for ACL packets.
new-registered-state (*yes* | *no*)	Whether to modify packet status. YES sets packet status to registered, NO - unregistered. Valid only in ingress policy table.
new-flow-id (*0..63*)	

Filter bypassing part for ACL packets.

Property	Description
attack-filter-bypass (*yes* | *no*; Default: **no**)	
ingress-vlan-filter-bypass (*yes* | *no*; Default: **no**)	Allows to bypass ingress VLAN filtering in VLAN table for matching packets. Applies only to ingress policy table.
egress-vlan-filter-bypass (*yes* | *no*; Default: **no**)	Allows to bypass egress VLAN filtering in VLAN table for matching packets. Applies only to ingress policy table.
isolation-filter-bypass (*yes* | *no*; Default: **no**)	Allows to bypass Isolation table for matching packets. Applies only to ingress policy table.
egress-vlan-translate-bypass (*yes* | *no*; Default: **no**)	Allows to bypass egress VLAN translation table for matching packets.

ACL Policer

Sub-menu: `/interface ethernet switch acl policer`

Property	Description
name (*string*; Default: **policerX**)	Name of the Policer used in ACL.
yellow-rate (*integer*)	Maximum data rate limit for packets with yellow drop precedence.
yellow-burst (*integer*; Default: **0**)	Maximum data rate which can be transmitted while the burst is allowed for packets with yellow drop precedence.
red-rate (*integer*); Default: **0**)	Maximum data rate limit for packets with red drop precedence.

red-burst (*integer*; Default: **0**)	Maximum data rate which can be transmitted while the burst is allowed for packets with red drop precedence.
meter-unit (*bit* | *packet*; Default: **bit**)	Measuring units for ACL traffic rate.
meter-len (*layer-1* | *layer-2* | *layer-3*; Default: **layer-1**)	Packet classification which sets the packet byte length for metering. - `layer-1` - includes entire layer-2 frame + FCS + inter-packet gap + preamble. - `layer-2` - includes layer-2 frame + FCS. - `layer-3` - includes only layer-3 + ethernet padding without layer-2 header and FCS.
color-awareness (*yes* | *no*; Default: **no**)	YES makes policer to take into account pre-colored drop precedence, NO - ignores drop precedence.
bucket-coupling (*yes* | *no*; Default: **no**)	
yellow-action (*drop* | *forward* | *remark*; Default: **drop**)	Performed action for exceeded traffic with yellow drop precedence.
new-dei-for-yellow (*0..1* | *remap*)	New DEI for yellow drop precedence packets.
new-pcp-for-yellow (*0..7* | *remap*)	New PCP for yellow drop precedence packets.
new-dscp-for-yellow (*0..63* | *remap*)	New DSCP for yellow drop precedence packets.
red-action (*drop* | *forward* | *remark*; Default: **drop**)	Performed action for exceeded traffic with red drop precedence.
new-dei-for-red (*0..1* | *remap*)	New DEI for red drop precedence packets.
new-pcp-for-red (*0..7* | *remap*)	New PCP for red drop precedence packets.
new-dscp-for-red (*0..63* | *remap*)	New DSCP for red drop precedence packets.

[Top | Back to Content **]**