

CRS1xx/2xx series switches

- [Summary](#)
- [Cloud Router Switch models](#)
- [Abbreviations and Explanations](#)
- [Port Switching](#)
 - [Multiple switch groups](#)
- [Global Settings](#)
- [Port Settings](#)
- [Forwarding Databases](#)
 - [Unicast FDB](#)
 - [Multicast FDB](#)
 - [Reserved FDB](#)
- [VLAN](#)
 - [VLAN Table](#)
 - [Egress VLAN Tag](#)
 - [Ingress/Egress VLAN Translation](#)
 - [Protocol Based VLAN](#)
 - [MAC Based VLAN](#)
 - [1:1 VLAN Switching](#)
- [Port Isolation/Leakage](#)
- [Trunking](#)
- [Quality of Service](#)
 - [Shaper](#)
 - [Ingress Port Policer](#)
 - [QoS Group](#)
 - [DSCP QoS Map](#)
 - [DSCP To DSCP Map](#)
 - [Policer QoS Map](#)
- [Access Control List](#)
 - [ACL Policer](#)
- [See also](#)

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. See [Cloud Router Switch configuration examples](#)



This article applies to CRS1xx and CRS2xx series switches and not to CRS3xx series switches. For CRS3xx series devices, read the [CRS3xx, CRS5xx series switches and CCR2116, CCR2216 routers](#) manual.

Features	Description
Forwarding	<ul style="list-style-type: none">• 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	<ul style="list-style-type: none"> • Various types of mirroring: <ul style="list-style-type: none"> ◦ Port-based mirroring ◦ VLAN-based mirroring ◦ MAC-based mirroring • 2 independent mirroring analyzer ports
VLAN	<ul style="list-style-type: none"> • Fully compatible with IEEE802.1Q and IEEE802.1ad VLAN • 4k active VLANs • Flexible VLAN assignment: <ul style="list-style-type: none"> ◦ 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	<ul style="list-style-type: none"> • 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	<ul style="list-style-type: none"> • 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)	<ul style="list-style-type: none"> • Flexible QoS classification and assignment: <ul style="list-style-type: none"> ◦ Port-based ◦ MAC-based ◦ VLAN-based ◦ Protocol-based ◦ PCP/DEI based ◦ DSCP based ◦ ACL based • QoS remarking and remapping for QoS domain translation between a service provider and client networks • Overriding of each QoS assignment according to the configured priority
Shaping and Scheduling	<ul style="list-style-type: none"> • 8 queues on each physical port • Shaping per port, per queue, per queue group
Access Control List	<ul style="list-style-type: none"> • 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 the protocol header fields

Cloud Router Switch models

This table clarifies the 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

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 enqueueing or dropping.

Port Switching

In order to set up port switching on CRS1xx/2xx series switches, check the [Bridge Hardware Offloading](#) page.



Dynamic reserved VLAN entries (VLAN4091; VLAN4090; VLAN4089; etc.) are created in the CRS switch when switched port groups are added when a hardware offloaded bridge is created. These VLANs are necessary for internal operation and have lower precedence than user-configured VLANs.

Multiple switch groups

The CRS1xx/2xx series switches allow you to use multiple bridges with hardware offloading, this allows you to easily isolate multiple switch groups. This can be done by simply creating multiple bridges and enabling hardware offloading.



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



CRS1xx/2xx series switches are capable of running multiple hardware offloaded bridges with (R)STP enabled, but it is not recommended since the device is not designed to run multiple (R)STP instances on a hardware level. To isolate multiple switch groups and have (R)STP enabled you should isolate port groups with port isolation profile configuration.

Global Settings

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

Sub-menu: `/interface ethernet switch`

Property	Description
name (<i>string value</i> ; Default: switch1)	Name of the switch.
bridge-type (<i>customer-vid-used-as-lookup-vid / service-vid-used-as-lookup-vid</i> ; 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 (<i>yes / no</i> ; Default: yes)	Globally enables or disables MAC level isolation. Once enabled, the switch will check the source and destination MAC address entries and their isolation-profile from the unicast forwarding table. By default, the switch will learn MAC addresses and place them into a <code>promiscuous</code> isolation profile. Other isolation profiles can be used when creating static unicast entries. If the source or destination MAC address is located on a <code>promiscuous</code> isolation profile, the packet is forwarded. If both source and destination MAC addresses are located on the same <code>community1</code> or <code>community2</code> isolation profile, the packet is forwarded. The packet is dropped when the source and destination MAC address isolation profile is <code>isolated</code> , or when the source and destination MAC address isolation profiles are from different communities (e.g. source MAC address is <code>community1</code> and destination MAC address is <code>community2</code>). When MAC level isolation is globally disabled, the isolation is bypassed.
use-svid-in-one2one-vlan-lookup (<i>yes / no</i> ; Default: no)	Whether to use service VLAN id for 1:1 VLAN switching lookup.
use-cvid-in-one2one-vlan-lookup (<i>yes / no</i> ; Default: yes)	Whether to use customer VLAN id for 1:1 VLAN switching lookup.
multicast-lookup-mode (<i>dst-ip-and-vid-for-ipv4 / dst-mac-and-vid-always</i> ; Default: dst-ip-and-vid-for-ipv4)	Lookup mode for IPv4 multicast bridging. <ul style="list-style-type: none"> <code>dst-mac-and-vid-always</code> - For all packet types lookup key is destination MAC and VLAN id. <code>dst-ip-and-vid-for-ipv4</code> - 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 (<i>time interval</i> ; Default: 5m)	Timeout for Unicast FDB entries.
override-existing-when-ufdb-full (<i>yes / no</i> ; 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 (<i>ports</i> ; 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 (<i>ports</i> ; Default: none)	Ports that drop invalid and other port VLAN id frames.
unknown-vlan-lookup-mode (<i>ivl / svl</i> ; Default: svl)	Lookup and learning mode for packets with invalid VLAN.
forward-unknown-vlan (<i>yes / no</i> ; Default: yes)	Whether to allow forwarding VLANs that are not members of the VLAN table.

Property	Description
bypass-vlan-ingress-filter-for (<i>protocols</i> ; Default: none)	Protocols that 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 (<i>protocols</i> ; Default: none)	Protocols that are excluded from Ingress Port Policing. (arp, dhcpv4, dhcpv6, eapol, igmp, mld, nd, pppoe-discovery, ripv1)
bypass-l2-security-check-filter-for (<i>protocols</i> ; ; Default: none)	Protocols that are excluded from Policy rule security check. (arp, dhcpv4, dhcpv6, eapol, igmp, mld, nd, pppoe-discovery, ripv1)

Property	Description
ingress-mirror0 (<i>port trunk,format</i> ; Default: none,modified)	The first ingress mirroring analyzer port or trunk and mirroring format: <ul style="list-style-type: none"> analyzer-configured - The packet is the same as the packet to the destination. VLAN format is modified based on the VLAN configurations of the analyzer port. modified - The packet is the same as the packet to the 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 the edge port.
ingress-mirror1 (<i>port trunk,format</i> ; Default: none,modified)	The second ingress mirroring analyzer port or trunk and mirroring format: <ul style="list-style-type: none"> analyzer-configured - The packet is the same as the packet to the destination. VLAN format is modified based on the VLAN configurations of the analyzer port. modified - The packet is the same as the packet to the 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 the edge port.
ingress-mirror-ratio (<i>1/32768..1/1</i> ; Default: 1/1)	The proportion of ingress mirrored packets compared to all packets.
egress-mirror0 (<i>port trunk,format</i> ; Default: none,modified)	The first egress mirroring analyzer port or trunk and mirroring format: <ul style="list-style-type: none"> analyzer-configured - The packet is the same as the packet to the destination. VLAN format is modified based on the VLAN configurations of the analyzer port. modified - The packet is the same as the packet to the 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 the edge port.

egress-mirror1 (<i>port trunk,format</i> ; Default: no ne,modified)	The second egress mirroring analyzer port or trunk and mirroring format: <ul style="list-style-type: none"> analyzer-configured - The packet is the same as the packet to the destination. VLAN format is modified based on the VLAN configurations of the analyzer port. modified - The packet is the same as the packet to the 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 the edge port.
egress-mirror-ratio (<i>1/32768..1/1</i> ; Default: 1/1)	Proportion of egress mirrored packets compared to all packets.
mirror-egress-if-ingress-mirrored (<i>yes / no</i> ; Default: no)	When a packet is applied to both ingress and egress mirroring, only ingress mirroring is performed on the packet, if this setting is disabled. If this setting is enabled both mirroring types are applied.
mirror-tx-on-mirror-port (<i>yes / no</i> ; Default: no)	
mirrored-packet-qos-priority (<i>0..7</i> ; Default: 0)	Remarkd priority in mirrored packets.
mirrored-packet-drop-precedence (<i>drop green red yellow</i> ; Default: green)	Remarkd drop precedence in mirrored packets. This QoS attribute is used for mirrored packet enqueueing or dropping.
fdb-uses (<i>mirror0 mirror1</i> ; Default: mirror0)	Analyzer port used for FDB-based mirroring.
vlan-uses (<i>mirror0 mirror1</i> ; Default: mirror0)	Analyzer port used for VLAN-based mirroring.

Port Settings

Sub-menu: `/interface ethernet switch port`

Property	Description
vlan-type (<i>edge-port network-port</i> ; 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 (<i>yes / no</i> ; Default: no) isolation-leakage-profile-override isolation-leakage-profile (<i>0..31</i> ;))	Custom port profile for port isolation/leakage configurations. <ul style="list-style-type: none"> 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 (<i>yes / no</i> ; Default: !learn-override) learn-limit (<i>1..1023</i> ; Default: !learn-limit)	Enable or disable MAC address learning and set MAC limit on the port. MAC learning limit is disabled by default when <code>!learn-override</code> and <code>!learn-limit</code> . Property <code>learn-override</code> is replaced with <code>learn</code> under <code>/interface ethernet bridge port</code> menu since RouterOS v6.42.
drop-when-ufdb-entry-src-drop (<i>yes / no</i> ; Default: yes)	Enable or disable to drop packets when UFDB entry has action <code>src-drop</code> .
allow-unicast-loopback (<i>yes / no</i> ; 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 (<i>yes / no</i> ; 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 (<i>copy-to-cpu drop forward redirect-to-cpu</i> ; Default: forward)	Action for packets when UFDB already contains static entry with such MAC but with a different port.
drop-dynamic-mac-move (<i>yes / no</i> ; Default: no)	Prevents MAC relearning until UFDB timeout if MAC is already learned on other port.

Property	Description
allow-fdb-based-vlan-translate (<i>yes / no</i> ; Default: no)	Enable or disable MAC-based VLAN translation on the port.
allow-mac-based-service-vlan-assignment-for (<i>all-frames / none / tagged-frame-only / untagged-and-priority-tagged-frame-only</i> ; Default: none)	Frame type for which applies MAC-based service VLAN translation.
allow-mac-based-customer-vlan-assignment-for (<i>all-frames / none / tagged-frame-only / untagged-and-priority-tagged-frame-only</i> ; Default: none)	Frame type for which applies MAC-based customer VLAN translation.
default-customer-pcp (<i>0..7</i> ; Default: 0)	Default customer PCP of the port.
default-service-pcp (<i>0..7</i> ; Default: 0)	Default service PCP of the port.
pcp-propagation-for-initial-pcp (<i>yes / no</i> ; Default: no)	Enables or disables PCP propagation for initial PCP assignment on ingress. <ul style="list-style-type: none"> • 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 (<i>yes / no</i> ; Default: no)	Whether to filter untagged frames on the port.
filter-priority-tagged-frame (<i>yes / no</i> ; Default: no)	Whether to filter tagged frames with priority on the port.
filter-tagged-frame (<i>yes / no</i> ; Default: no)	Whether to filter tagged frames on the port.

Property	Description
egress-vlan-tag-table-lookup-key (<i>according-to-bridge-type / egress-vid</i> ; Default: egress-vid)	Egress VLAN table (VLAN Tagging) lookup: <ul style="list-style-type: none"> • 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 (<i>tagged / unmodified / untagged</i> ; Default: unmodified)	Egress VLAN tagging action on the port.
egress-pcp-propagation (<i>yes / no</i> ; Default: no)	Enables or disables egress PCP propagation. <ul style="list-style-type: none"> • 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 (<i>mirror0 / mirror1 / none</i> ; Default: none)	Analyzer port for port-based ingress mirroring.

ingress-mirroring-according-to-vlan (<i>yes / no</i> ; Default: no)	
egress-mirror-to (<i>mirror0 / mirror1 / none</i> ; Default: none)	Analyzer port for port-based egress mirroring.

Property	Description
qos-scheme-precedence (<i>da-based / dscp-based / ingress-acl-based / pcp-based / protocol-based / sa-based / vlan-based</i> ; Default: pcp-based, sa-based, da-based, dscp-based, protocol-based, vlan-based)	Specifies applied QoS assignment schemes on ingress of the port. <ul style="list-style-type: none"> • da-based • dscp-based • ingress-acl-based • pcp-based • protocol-based • sa-based • vlan-based
pcp-or-dscp-based-qos-change-dei (<i>yes / no</i> ; Default: no)	Enable or disable PCP or DSCP based DEI change on port.
pcp-or-dscp-based-qos-change-pcp (<i>yes / no</i> ; Default: no)	Enable or disable PCP or DSCP based PCP change on port.
pcp-or-dscp-based-qos-change-dscp (<i>yes / no</i> ; Default: no)	Enable or disable PCP or DSCP based DSCP change on port.
dscp-based-qos-dscp-to-dscp-mapping (<i>yes / no</i> ; Default: yes)	Enable or disable DSCP to internal DSCP mapping on port.
pcp-based-qos-drop-precedence-mapping (<i>PCP/DEI-range:drop-precedence</i> ; 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 (<i>PCP/DEI-range:DEI</i> ; 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 (<i>PCP/DEI-range:DEI</i> ; 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 (<i>PCP/DEI-range:DEI</i> ; 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 (<i>PCP/DEI-range:DEI</i> ; 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 (<i>priority-range:queue</i> ; Default: 0-15:0,1:1,2:2,3:3)	Internal priority (0..15) mapping to queue (0..7) per port.
per-queue-scheduling (<i>Scheduling-type:Weight</i> ; 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 (<i>yes / no</i> ; Default: ingress-customer-tpid-override) ingress-customer-tpid (<i>0..10000</i> ; Default: 0x8100)	Ingress customer TPID override allows accepting specific frames with a custom customer tag TPID. Default value is for tag of 802.1Q frames.
egress-customer-tpid-override (<i>yes / no</i> ; Default: egress-customer-tpid-override) egress-customer-tpid (<i>0..10000</i> ; Default: 0x8100)	Egress customer TPID override allows custom identification for egress frames with a customer tag. Default value is for tag of 802.1Q frames.
ingress-service-tpid-override (<i>yes / no</i> ; Default: ingress-service-tpid-override) ingress-service-tpid (<i>0..10000</i> ; Default: 0x88A8)	Ingress service TPID override allows accepting specific frames with a custom service tag TPID. Default value is for service tag of 802.1AD frames.
egress-service-tpid-override (<i>yes / no</i> ; Default: egress-service-tpid-override) egress-service-tpid (<i>0..10000</i> ; Default: 0x88A8)	Egress service TPID override allows custom identification for egress frames with a service tag. Default value is for service tag of 802.1AD frames.

Property	Description
custom-drop-counter-includes (<i>counters</i> ; Default: none)	Custom include to count dropped packets for switch port custom-drop-packet counter. <ul style="list-style-type: none"> • 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 (<i>counters</i> ; 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. <ul style="list-style-type: none"> • red • yellow • green • queue0 • ... • queue7

queue-custom-drop-counter1-includes (<i>counters</i> ; 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. <ul style="list-style-type: none"> • red • yellow • green • queue0 • ... • queue7
policy-drop-counter-includes (<i>counters</i> ; Default: none)	Custom include to count dropped packets for switch port policy-drop-packet counter. <ul style="list-style-type: none"> • ingress-policing • ingress-acl • egress-policing • egress-acl

Forwarding Databases

Unicast FDB

The unicast forwarding database supports up to 16318 MAC entries.

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

Property	Description
action (<i>action</i> ; Default: forward)	Action for UFDB entry: <ul style="list-style-type: none"> • 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 (<i>yes / no</i> ; Default: no)	Enables or disables Unicast FDB entry.
isolation-profile (<i>community1 community2 isolated promiscuous</i> ; Default: promiscuous)	MAC level isolation profile.
mac-address (<i>MAC address</i>)	The action command applies to the packet when the destination MAC or source MAC matches the entry.
mirror (<i>yes / no</i> ; Default: no)	Enables or disables mirroring based on source MAC or destination MAC.
port (<i>port</i>)	Matching port for the Unicast FDB entry.
qos-group (<i>none</i> ; Default: none)	Defined QoS group from QoS group menu.

svl (<i>yes / no</i> ; Default: no)	Unicast FDB learning mode: <ul style="list-style-type: none"> • 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 (<i>0..4095</i>)	Unicast FDB lookup/learning VLAN id.

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 learned and can only be configured.

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

Property	Description
address (<i>X.X.X.X / XX:XX:XX:XX:XX:XX</i>)	Matching IP address or MAC address for multicast packets.
bypass-vlan-filter (<i>yes / no</i> ; Default: no)	Allow to bypass VLAN filtering for matching multicast packets.
disabled (<i>yes / no</i> ; Default: no)	Enables or disables Multicast FDB entry.
ports (<i>ports</i>)	Member ports for multicast traffic.
qos-group (<i>none</i> ; Default: none)	Defined QoS group from QoS group menu.
svl (<i>yes / no</i> ; Default: no)	Multicast FDB learning mode: <ul style="list-style-type: none"> • 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 (<i>0..4095</i> ; Default: 0)	Multicast FDB lookup VLAN id. If VLAN learning mode is IVL, VLAN id is lookup id, otherwise VLAN id = 0.

Reserved FDB

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

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

Property	Description
action (<i>copy-to-cpu / drop / forward / redirect-to-cpu</i> ; Default: forward)	Action for RFDB entry: <ul style="list-style-type: none"> • 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 (<i>yes / no</i> ; Default: no)	Allow to bypass Ingress Port Policer for matching packets.
bypass-ingress-vlan-filter (<i>yes / no</i> ; Default: no)	Allow to bypass VLAN filtering for matching packets.
disabled (<i>yes / no</i> ; Default: no)	Enables or disables Reserved FDB entry.
mac-address (<i>MAC address</i> ; Default: 00:00:00:00:00:00)	Matching MAC address for Reserved FDB entry.
qos-group (<i>none</i> ; Default: none)	Defined QoS group from QoS group menu.

VLAN

VLAN Table

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.

Sub-menu: `/interface ethernet switch vlan`

Property	Description
disabled (<i>yes / no</i> ; Default: no)	Indicate whether the VLAN entry is disabled. Only enabled entry is applied to lookup process and forwarding decision.
flood (<i>yes / no</i> ; 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 (<i>yes / no</i> ; Default: no)	Enable the ingress mirror per VLAN to support the VLAN-based mirror function.
learn (<i>yes / no</i> ; Default: yes)	Enables or disables source MAC learning for VLAN.
ports (<i>ports</i>)	Member ports of the VLAN.
qos-group (<i>none</i> ; Default: none)	Defined QoS group from QoS group menu.
svl (<i>yes / no</i> ; Default: no)	FDB lookup mode for lookup in UFDB and MFDB. <ul style="list-style-type: none">• 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 (<i>0..4095</i>)	VLAN id of the VLAN member entry.

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.

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

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

Ingress/Egress VLAN Translation

The Ingress VLAN Translation table allows for up to 15 entries for each port. One or multiple fields can be selected from the packet header for lookup in the Ingress VLAN Translation table. The S-VLAN or C-VLAN or both configured in the first matched entry are 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 (<i>any priority-tagged-or-tagged tagged untagged-or-tagged</i> ; Default: any)	Type of frames with customer tag for which VLAN translation rule is valid.
disabled (<i>yes no</i> ; 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 (<i>yes no</i> ; Default: no)	Enables or disables PCP propagation. <ul style="list-style-type: none"> • 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 (<i>ports</i>)	Matching switch ports for VLAN translation rule.
protocol (<i>protocols</i> ; Default: none)	Matching Ethernet protocol. (<i>only for Ingress VLAN Translation</i>)
sa-learning (<i>yes no</i> ; Default: no)	Enables or disables source MAC learning after VLAN translation. (<i>only for Ingress VLAN Translation</i>)
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 (<i>any priority-tagged-or-tagged tagged untagged-or-tagged</i> ; 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: <ul style="list-style-type: none"> • Untagged traffic • Tagged traffic • Tagged traffic with priority set • VLAN 0 traffic • VLAN 0 traffic with priority set
priority-tagged-or-tagged	Accepts: <ul style="list-style-type: none"> • Tagged traffic • Tagged traffic with priority set • VLAN 0 traffic • VLAN 0 traffic with priority set
tagged	Accepts: <ul style="list-style-type: none"> • Tagged traffic • Tagged traffic with priority set

untagged-or-tagged	Accepts: <ul style="list-style-type: none"> • Untagged traffic • Tagged traffic • Tagged traffic with priority set
---------------------------	---

 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

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

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

Property	Description
disabled (<i>yes / no</i> ; Default: no)	Enables or disables Protocol Based VLAN entry.
frame-type (<i>ethernet llc rfc-1042</i> ; Default: ethernet)	Encapsulation type of the matching frames.
new-customer-vid (<i>0..4095</i> ; Default: 0)	The new customer VLAN id which replaces original customer VLAN id for the specified protocol. If set to 4095, then traffic is dropped.
new-service-vid (<i>0..4095</i> ; Default: 0)	The new service VLAN id which replaces the original service VLAN id for the specified protocol.
ports (<i>ports</i>)	Matching switch ports for Protocol-based VLAN rule.
protocol (<i>protocol</i> ; Default: 0)	Matching protocol for Protocol-based VLAN rule.
qos-group (<i>none</i> ; Default: none)	Defined QoS group from QoS group menu.
set-customer-vid-for (<i>all none tagged untagged-or-priority-tagged</i> ; Default: all)	Customer VLAN id assignment command for different packet type.
set-qos-for (<i>all none tagged untagged-or-priority-tagged</i> ; Default: none)	Frame type for which QoS assignment command applies.
set-service-vid-for (<i>all none tagged untagged-or-priority-tagged</i> ; Default: all)	Service VLAN id assignment command for different packet type.

MAC Based VLAN

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

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

Property	Description
disabled (<i>yes / no</i> ; Default: no)	Enables or disables MAC Based VLAN entry.
new-customer-vid (<i>0..4095</i> ; 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 (<i>0..4095</i> ; Default: 0)	The new service VLAN id which replaces original service VLAN id for matched packets.
src-mac-address (<i>MAC address</i>)	Matching source MAC address for MAC based VLAN rule.



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

1:1 VLAN Switching

1:1 VLAN switching can be used to replace the regular L2 bridging for matched packets. When a packet hits a 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.

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

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

Port Isolation/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.

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

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

Property	Description
disabled (<i>yes / no</i> ; Default: no)	Enables or disables port isolation/leakage entry.
flow-id (<i>0..63</i> ; Default: none)	
forwarding-type (<i>bridged; routed</i> ; Default: bridged,routed)	Matching traffic forwarding type on Cloud Router Switch.
mac-profile (<i>community1 community2 isolated promiscuous</i> ; Default: none)	Matching MAC isolation/leakage profile.

port-profile (<i>0..31</i> ; Default: none)	Matching Port isolation/leakage profile.
ports (<i>ports</i> ; Default: none)	Isolated/leaked ports.
protocol-type (<i>arp; nd; dhcpv4; dhcpv6; ripv1</i> ; Default: arp,nd,dhcpv4,dhcpv6,ripv1)	Included protocols for isolation/leakage.
registration-status (<i>known; unknown</i> ; Default: known,unknown)	Registration status for matching packets. Known are present in UFDB and MFDB, unknown are not.
traffic-type (<i>unicast; multicast; broadcast</i> ; Default: unicast,multicast,broadcast)	Matching traffic type.
type (<i>dst src</i> ; Default: src)	Lookup type of the isolation/leakage entry: <ul style="list-style-type: none"> • src - Entry applies to ingress packets of the ports. • dst - Entry applies to egress packets of the ports.
vlan-profile (<i>community1 community2 isolated promiscuous</i> ; Default: none)	Matching VLAN isolation/leakage profile.

Trunking

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. 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.

Sub-menu: /interface ethernet switch trunk

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

Quality of Service

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.

Sub-menu: /interface ethernet switch shaper

Property	Description
burst (<i>integer</i> ; Default: 100k)	Maximum data rate which can be transmitted while the burst is allowed.
disabled (<i>yes / no</i> ; Default: no)	Enables or disables traffic shaper entry.
meter-unit (<i>bit / packet</i> ; Default: bit)	Measuring units for traffic shaper rate.
port (<i>port</i>)	Physical port for traffic shaper.
rate (<i>integer</i> ; Default: 1M)	Maximum data rate limit.

target (<i>port queueX wrr-groupX</i> ; Default: port)	<p>Three levels of shapers are supported on each port (including CPU port):</p> <ul style="list-style-type: none"> • Port level - Entry applies to the 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 the port. • Queue level - Entry applies to one of the 8 queues (queue0 - queue7) on the port.
---	--

Ingress Port Policer

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

Property	Description
burst (<i>integer</i> ; Default: 100k)	Maximum data rate which can be transmitted while the burst is allowed.
disabled (<i>yes / no</i> ; Default: no)	Enables or disables ingress port policer entry.
meter-len (<i>layer-1 layer-2 layer-3</i> ; Default: layer-1)	<p>Packet classification which sets the packet byte length for metering.</p> <ul style="list-style-type: none"> • 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 (<i>bit / packet</i> ; Default: bit)	Measuring units for traffic ingress port policer rate.
new-dei-for-yellow (<i>0..1 remap</i> ; Default: none)	Remarkd DEI for exceeded traffic if yellow-action is remark.
new-dscp-for-yellow (<i>0..63 remap</i> ; Default: none)	Remarkd DSCP for exceeded traffic if yellow-action is remark.
new-pcp-for-yellow (<i>0..7 remap</i> ; Default: none)	Remarkd PCP for exceeded traffic if yellow-action is remark.
packet-types (<i>packet-types</i> ; Default: all types from description)	Matching packet types for which ingress port policer entry is valid.
port (<i>port</i>)	Physical port or trunk for ingress port policer entry.
rate (<i>integer</i>)	Maximum data rate limit.
yellow-action (<i>drop forward remark</i> ; Default: drop)	Performed action for exceeded traffic.

QoS Group

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

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

Property	Description
dei (<i>0..1</i> ; Default: none)	The new value of DEI for the QoS group.
disabled (<i>yes / no</i> ; Default: no)	Enables or disables protocol QoS group entry.
drop-precedence (<i>drop green red yellow</i> ; Default: green)	Drop precedence is internal QoS attribute used for packet enqueueing or dropping.
dscp (<i>0..63</i> ; Default: none)	The new value of DSCP for the QoS group.
name (<i>string value</i> ; Default: groupX)	Name of the QoS group.
pcp (<i>0..7</i> ; Default: none)	The new value of PCP for the QoS group.
priority (<i>0..15</i> ; 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

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

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

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

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.

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

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

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.



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



Due to hardware limitations, it is not possible to match broadcast/multicast traffic on specific ports. You should use port isolation, drop traffic on ingress ports or use VLAN filtering to prevent certain broadcast/multicast traffic from being forwarded.

Sub-menu: /interface ethernet switch acl

ACL condition part for MAC-related fields of packets.

Property	Description
disabled (<i>yes / no</i> ; Default: no)	Enables or disables ACL entry.
table (<i>egress / ingress</i> ; Default: ingress)	Selects policy table for incoming or outgoing packets.
invert-match (<i>yes / no</i> ; Default: no)	Inverts whole ACL rule matching.
src-ports (<i>ports,trunks</i>)	Matching physical source ports or trunks.
dst-ports (<i>ports,trunks</i>)	Matching physical destination ports or trunks. It is not possible to match broadcast/multicast traffic on the egress port due to a hardware limitation.
mac-src-address (<i>MAC address/Mask</i>)	Source MAC address and mask.
mac-dst-address (<i>MAC address/Mask</i>)	Destination MAC address and mask.
dst-addr-registered (<i>yes / no</i>)	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 (<i>802.2 arp homeplug-av ip ip-or-ipv6 ipv6 ipx lldp loop-protect mpls-multicast mpls-unicast non-ip packing-compr packing-simple pppoe pppoe-discovery rarp service-vlan vlan or integer: 0..65535 decimal format or 0x0000-0xffff hex format</i>)	<p>Ethernet payload type (MAC-level protocol)</p> <ul style="list-style-type: none"> • 802.2 - 802.2 Frames (0x0004) • arp - Address Resolution Protocol (0x0806) • homeplug-av - HomePlug AV MME (0x88E1) • ip - Internet Protocol version 4 (0x0800) • ip-or-ipv6 - IPv4 or IPv6 (0x0800 or 0x86DD) • ipv6 - Internet Protocol Version 6 (0x86DD) • ipx - Internetwork Packet Exchange (0x8137) • lldp - Link Layer Discovery Protocol (0x88CC) • loop-protect - Loop Protect Protocol (0x9003) • mpls-multicast - MPLS multicast (0x8848) • mpls-unicast - MPLS unicast (0x8847) • non-ip - Not Internet Protocol version 4 (not 0x0800) • packing-compr - Encapsulated packets with compressed IP packing (0x9001) • packing-simple - Encapsulated packets with simple IP packing (0x9000) • pppoe - PPPoE Session Stage (0x8864) • pppoe-discovery - PPPoE Discovery Stage (0x8863) • rarp - Reverse Address Resolution Protocol (0x8035) • service-vlan - Provider Bridging (IEEE 802.1ad) & Shortest Path Bridging IEEE 802.1aq (0x88A8) • vlan - VLAN-tagged frame (IEEE 802.1Q) and Shortest Path Bridging IEEE 802.1aq with NNI compatibility (0x8100)
drop-precedence (<i>drop green red yellow</i>)	Matching internal drop precedence. Valid only in egress table.
custom-fields	

ACL condition part for VLAN-related fields of packets.

Property	Description
lookup-vid (<i>0..4095</i>)	VLAN id used in lookup. It can be changed before reaching the 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 the 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 the 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)	<ul style="list-style-type: none"> • 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 sent to new destination ports if they match the ACL conditions.
new-dst-ports (ports,trunks)	If the action is "send-to-new-dst-ports", then this property sets which ports/trunks are the new destinations.

mirror-to (<i>mirror0 mirror1</i>)	Mirroring destination for ACL packets.
policer (<i>policer</i>)	Applied ACL Policer for ACL packets.
src-mac-learn (<i>yes / no</i>)	Whether to learn source MAC of the matched ACL packets. Valid only in the ingress policy table.
new-service-vid (<i>0..4095</i>)	New service VLAN id for ACL packets.
new-service-pcp (<i>0..7</i>)	New service PCP for ACL packets.
new-service-dei (<i>0..1</i>)	New service DEI for ACL packets.
new-customer-vid (<i>0..4095</i>)	New customer VLAN id for ACL packets. If set to 4095, then traffic is dropped.
new-customer-pcp (<i>0..7</i>)	New customer PCP for ACL packets.
new-customer-dei (<i>0..1</i>)	New customer DEI for ACL packets.
new-dscp (<i>0..63</i>)	New DSCP for ACL packets.
new-priority (<i>0..15</i>)	New internal priority for ACL packets.
new-drop-precedence (<i>drop green red yellow</i>)	New internal drop precedence for ACL packets.
new-registered-state (<i>yes / no</i>)	Whether to modify packet status. YES sets packet status to registered, NO - unregistered. Valid only in the ingress policy table.
new-flow-id (<i>0..63</i>)	

Filter bypassing part for ACL packets.

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

ACL Policer

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

Property	Description
name (<i>string</i> ; Default: policerX)	Name of the Policer used in ACL.
yellow-rate (<i>integer</i>)	Maximum data rate limit for packets with yellow drop precedence.
yellow-burst (<i>integer</i> ; Default: 0)	Maximum data rate which can be transmitted while the burst is allowed for packets with yellow drop precedence.
red-rate (<i>integer</i> ; Default: 0)	Maximum data rate limit for packets with red drop precedence.
red-burst (<i>integer</i> ; Default: 0)	Maximum data rate which can be transmitted while the burst is allowed for packets with red drop precedence.
meter-unit (<i>bit packet</i> ; Default: bit)	Measuring units for ACL traffic rate.

meter-len (<i>layer-1 layer-2 layer-3</i> ; Default: layer-1)	Packet classification which sets the packet byte length for metering. <ul style="list-style-type: none"> • 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 (<i>yes no</i> ; Default: no)	YES makes policer to take into account pre-colored drop precedence, NO - ignores drop precedence.
bucket-coupling (<i>yes no</i> ; Default: no)	
yellow-action (<i>drop forward remark</i> ; Default: drop)	Performed action for exceeded traffic with yellow drop precedence.
new-dei-for-yellow (<i>0..1 remap</i>)	New DEI for yellow drop precedence packets.
new-pcp-for-yellow (<i>0..7 remap</i>)	New PCP for yellow drop precedence packets.
new-dscp-for-yellow (<i>0..63 remap</i>)	New DSCP for yellow drop precedence packets.
red-action (<i>drop forward remark</i> ; Default: drop)	Performed action for exceeded traffic with red drop precedence.
new-dei-for-red (<i>0..1 remap</i>)	New DEI for red drop precedence packets.
new-pcp-for-red (<i>0..7 remap</i>)	New PCP for red drop precedence packets.
new-dscp-for-red (<i>0..63 remap</i>)	New DSCP for red drop precedence packets.

See also

- [CRS1xx/2xx series switches examples](#)
- [CRS Router](#)
- [CRS1xx/2xx VLANs with Trunks](#)
- [Basic VLAN switching](#)
- [Bridge Hardware Offloading](#)
- [Spanning Tree Protocol](#)
- [IGMP Snooping](#)
- [DHCP Snooping and Option 82](#)
- [MTU on RouterBOARD](#)
- [Layer2 misconfiguration](#)