

CSS106 (RB260) series Manual

- [Features](#)
- [Connecting to the switch](#)
- [Interface Overview](#)
- [System](#)
 - [Password and Backup](#)
- [Link](#)
 - [PoE](#)
- [SFP](#)
- [Forwarding](#)
- [RSTP](#)
- [Statistics, Errors](#)
- [VLAN and VLANs](#)
 - [VLAN Configuration Examples](#)
 - [Trunk and Access Ports](#)
 - [Trunk and Hybrid Ports](#)
 - [Management access](#)
- [Hosts](#)
 - [Static Hosts](#)
- [IGMP Groups](#)
- [SNMP](#)
- [ACL](#)
- [Reset](#)

Features

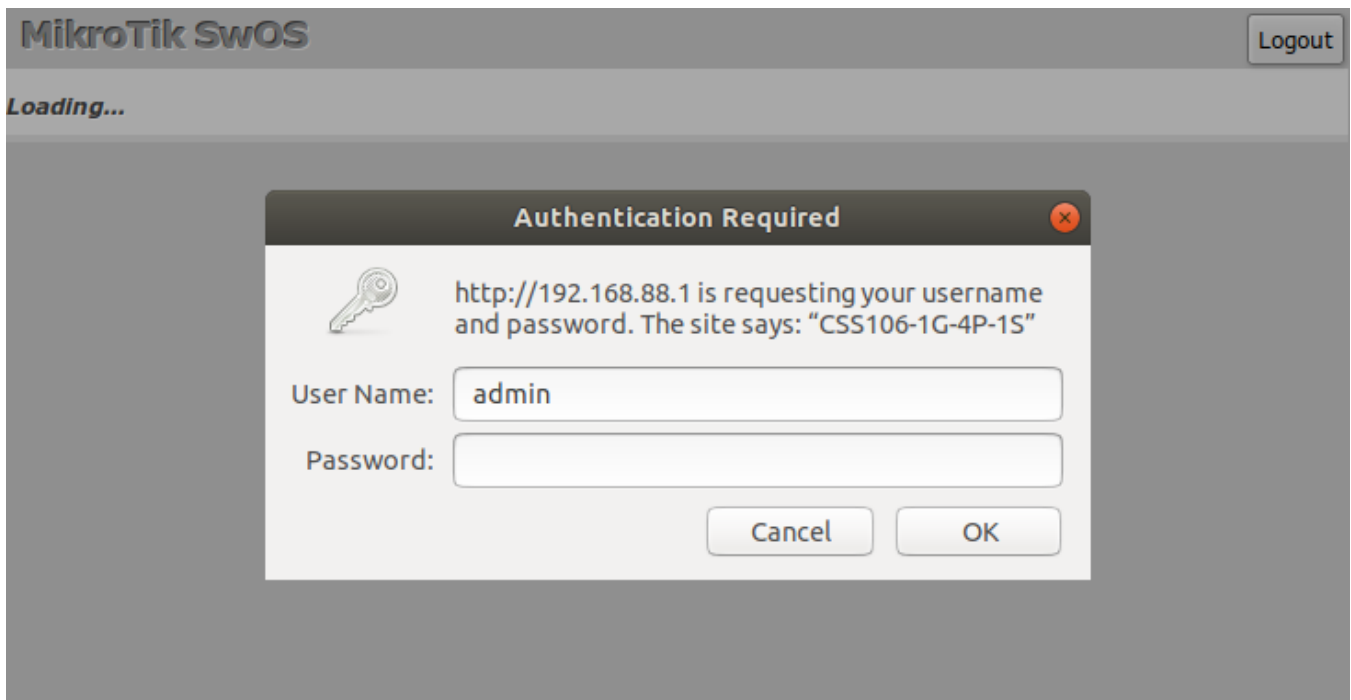
Features	Description
Forwarding	<ul style="list-style-type: none">• Full non-blocking wirespeed switching• Up to 2k MAC entries in the Host table• Forwarding Database works based on SVL or IVL• Port Isolation• Port Lock• Jumbo frame support - 9198 bytes
Spanning Tree Protocol	<ul style="list-style-type: none">• RSTP support
Multicast Forwarding	<ul style="list-style-type: none">• IGMP Snooping support
Mirroring	<ul style="list-style-type: none">• Port-based mirroring
VLAN	<ul style="list-style-type: none">• Fully compatible with IEEE802.1Q• Port-based VLAN• VLAN filtering
Quality of Service (QoS)	<ul style="list-style-type: none">• Ingress traffic limiting (by ACL)• Egress traffic limiting

Access Control List

- Ingress ACL tables
- Up to 32 ACL rules (limited by SwOS)
- Classification based on ports, L2, L3, L4 protocol header fields
- ACL actions include filtering, forwarding, and modifying the protocol header fields

Connecting to the switch

Open your web browser and enter the IP address of your switch (192.168.88.1 by default) and a login screen will appear. The switch can also run a DHCP client, see if a different IP address has been assigned by the DHCP server.



SwOS default IP address: **192.168.88.1**, user name: **admin** and there is no password.



[MikroTik Neighbor Discovery](#) can be used to discover the IP address of the Mikrotik switch. LLDP is not supported.

Interface Overview

SwOS interface menu consists of several tabs: Link, SFP, Forwarding, RST, Statistics, Errors, VLAN, VLANs, Hosts, IGMP Groups, SNMP, ACL, System and Upgrade.

Description of buttons in SwOS configuration tool:

- **Append** - add a new item to the end of the list
- **Apply All** - applies current configuration changes
- **Cut** - removes an item from the list
- **Clear** - reset properties of the item
- **Discard Changes** - removes unsaved configuration
- **Insert** - add a new item to the list (places it before current item)
- **Sort** - sort VLAN table by VLAN-IDs; sort host table by MAC addresses
- **Change Password** - changes the password of the switch
- **Logout** - logout from the current switch
- **Reboot** - reboot the switch
- **Reset Configuration** - reset configuration back to factory defaults

- **Choose File** - browse for upgrade or backup file
- **Upgrade** - upgrade the firmware of the switch using the selected file
- **Download & Upgrade** - automatically try to download and upgrade the firmware, the PC which is running a web browser should be able to access the Internet
- **Restore Backup** - restore switch using a selected backup file
- **Save Backup** - generate and download backup file from the switch

i Each RouterBOARD switch series have their own firmware which cannot be installed on other series models! CSS106-5G-1S (RB260GS) and CSS106-1G-4P-1S (RB260GSP) supports SwOS v2.0 and newer. When upgrading the device, it will first load primary firmware and then make an upgrade. In case a wrong firmware file is chosen, the device will continue to operate with primary firmware and you will be able to choose the correct file.

System

System Tab performs the following functions:

- General information about switch
- Switch management
- Configuration reset
- Backup and restore configuration

i SwOS uses a simple algorithm to ensure TCP/IP communication - it just replies to the same IP and MAC address packet came from. This way there is no need for Default Gateway on the device itself.

MikroTik SwOS


Link
SFP
Forwarding
RSTP
Statistics
Errors
VLAN
VLANs
Hosts
IGMP Groups
SNMP
ACL
System
Upgrade

General

Address Acquisition	DHCP with fallback ▼
Static IP Address	192.168.88.1
Identity	MikroTik
Allow From	
Allow From Ports	<input checked="" type="checkbox"/> 1 <input checked="" type="checkbox"/> 2 <input checked="" type="checkbox"/> 3 <input checked="" type="checkbox"/> 4 <input checked="" type="checkbox"/> 5 <input checked="" type="checkbox"/> SFP
Allow From VLAN	
Watchdog	<input checked="" type="checkbox"/>
Independent VLAN Lookup	<input type="checkbox"/>
IGMP Snooping	<input type="checkbox"/>
Mikrotik Discovery Protocol	<input checked="" type="checkbox"/>
Port1 PoE In Long Cable	<input type="checkbox"/>
MAC Address	64:d1:54:c4:02:92
Serial Number	7A5607973F1F
Board Name	CSS106-1G-4P-1S

Property	Description
Address Acquisition	Specify which address acquisition method to use: <ul style="list-style-type: none"> • DHCP with fallback - switch is trying to request an IP address from a DHCP server. If the requests are unsuccessful, then the switch can be accessed using a Static IP Address value • static - address is set as a Static IP Address value • DHCP only - switch uses DHCP client to acquire address
Static IP Address	IP address of the switch in case of Address Acquisition is set as DHCP with fallback or static
Identity	Name of the switch (for Mikrotik neighbor discovery protocol)
Allow From	IP address or network from which the switch is accessible. Default value is '0.0.0.0/0' - any address.
Allow From Ports	List of switch ports from which the service is accessible
Allow From VLAN	VLAN ID from which the service is accessible. Make sure to first configure VLANs and VLAN pages
Watchdog	Enable or disable system watchdog. It will reset CPU of the switch in case of fault condition
Independent VLAN Lookup	Enable or disable independent VLAN lookup in the Host table for packet forwarding
IGMP Snooping	Enable or disable IGMP Snooping
IGMP Fast Leave	Enables or disables IGMP fast leave feature on the switch port. This property only has an effect when IGMP Snooping is enabled
Mikrotik Discovery Protocol	Enable or disable Mikrotik neighbor discovery protocol
Port1 PoE In Long Cable	If enabled, it will turn off short detection on all PoE out ports to allow the use of longer ethernet cables. This is potentially dangerous setting and should be used with caution. (CSS106-1G-4P-1S model)
MAC Address	MAC address of the switch (read-only)
Serial Number	Serial number of the switch (read-only)
Board Name	MikroTik model name (read-only)
Voltage	Shows the input voltage measured in volts (read-only, CSS106-1G-4P-1S model)
Temperature	Shows PCB temperature in celsius temperature scale (read-only, CSS106-1G-4P-1S model)

Password and Backup

 Using SFP+ 1m/3m DAC cable or S-RJ01 module, the device always shows that the link is established even if nothing is connected on another end.

 The switch supports Jumbo frames up to 9198 bytes. Manually decreasing the MTU settings is not supported for SwOS devices.

PoE

PoE settings change Power over Ethernet output on CSS106-1G-4P-1S port2-port5 and show PoE status and measurements.

PoE					
PoE Out	auto	off	auto	on	
PoE Priority	1	2	3	4	
PoE Status	disabled	powered on	disabled	waiting for load	powered on
PoE Current	58mA			86mA	
PoE Power	1.364W			2.022W	
<div>Discard ChangesApply All</div>					

Property	Description
PoE Out	Sets PoE out mode of the port: <ul style="list-style-type: none">• off - all detection and PoE out is turned off• auto - detection is done regarding resistance on the spare pairs to check if the port has PoE capability. For a port to be turned on measured value should be within a range from 3kΩ to 26.5kΩ• on - PoE out is enabled regardless of the resistance on the port. <i>Use this with caution as that can damage connected equipment!</i>• calibr - manual port PoE out recalibration. It may be necessary if there are occasional problems with powering connected devices.
PoE Priority	Port priority for PoE out supply. If the installation is going over available power budgeted, the port with the lowest priority is going to be turned off first. 1 - the highest priority port; 4 - the lowest priority port
PoE Status	Current PoE out status of the port: <ul style="list-style-type: none">• disabled - PoE out is turned off• waiting for load - "auto" mode detects out of range resistance to turn on PoE out• powered on - PoE out is turned on• short circuit - if it is detected, PoE out is turned off to ensure that there is no additional damage on the powered device and no damage on powering device• voltage too low - not enough voltage supplied to turn on the device with PoE out• current too low - not enough current supplied to turn on the device with PoE out• waiting for cable disconnect - manual recalibration with "calibr" has detected connected device and waits for disconnection to complete the recalibration process
PoE Current	Shows current usage on the port measured in milliamperes
PoE Power	Shows PoE out power on the port measured in watts

SFP

The SFP tab allows you to monitor the status of SFP modules.

MikroTik SwOS

Logout

Link

SFP

Forwarding

RSTP

Statistics

Errors

VLAN

VLANs

Hosts

IGMP Groups

SNMP

ACL

System

Upgrade

Vendor

Mikrotik

Part Number

S-31DLC20D

Revision

Serial

S1T31251001985

Date

15-03-20

Type

1310nm single-mode fiber

Status

Temperature

61C

Voltage

3.3156V

Tx Bias

22.9mA

Tx Power

-6.543dBm

Rx Power

-11.373dBm

Forwarding

Forwarding Tab provides advanced forwarding options among switch ports, port isolation, port locking, port mirroring and egress bandwidth limit features. Ingress rate per port and rate for broadcast traffic can be configured with [Access Control List](#) by setting **Rate**. ACL must have one port per entry to provide bandwidth limiting properly.

	Port1	Port2	Port3	Port4	Port5	SFP
Forwarding						
From Port 1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
From Port 2	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
From Port 3	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
From Port 4	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
From Port 5	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
From SFP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Port Lock						
Port Lock	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Lock On First	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Port Mirroring						
Mirror Ingress	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Mirror Egress	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Mirror To	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Bandwidth Limit						
Egress Rate	<input type="text"/>	<input type="text" value="250M"/>	<input type="text" value="70M"/>	<input type="text"/>	<input type="text" value="30M"/>	<input type="text"/>
						<input type="button" value="Discard Changes"/> <input type="button" value="Apply All"/>

Property	Description
Forwarding	Forwarding table - allows or restricts traffic flow between specific ports
Port Lock	<ul style="list-style-type: none"> Port Lock - Enables or disables MAC address learning on this port. When the option is enabled, it will restrict MAC address learning and static MAC addresses should be configured Lock On First - enable or disable MAC address learning on this port (MAC address from the first received packet will still be learned)
Port Mirroring	<ul style="list-style-type: none"> Mirror Ingress - whether traffic entering this port must be copied and forwarded to the mirroring target port Mirror Egress - whether traffic leaving this port must be copied and forwarded to the mirroring target port Mirror To - mirroring target port
Bandwidth Limit	<ul style="list-style-type: none"> Egress Rate - limit traffic leaving this port (bps)

RSTP

Per-port and global RSTP configuration and monitoring are available in the RSTP menu.

Link	SFP	Forwarding	RSTP	Statistics	Errors	VLAN	VLANs	Hosts	IGMP Groups	SNMP	ACL	System	Upgrade
------	-----	------------	------	------------	--------	------	-------	-------	-------------	------	-----	--------	---------

Per Port

	Port1	Port2	Port3	Port4	Port5	SFP
RSTP	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Mode	RSTP	RSTP	RSTP	RSTP	RSTP	RSTP
Role	designated	root	alternate	disabled	designated	disabled
Root Path Cost		4	19			
Type	edge	point-to-point	point-to-point	edge	edge	edge
State	forwarding	forwarding	discarding	forwarding	forwarding	forwarding

[Discard Changes](#)
[Apply All](#)

General

Bridge Priority (hex)	<input type="text" value="9000"/>
Port Cost Mode	<input type="button" value="short"/> ▼
Root Bridge	1000.64:d1:54:c7:3a:58

[Discard Changes](#)
[Apply All](#)

Property	Description
RSTP	Enable or disable STP/RSTP functionality on this port
Mode	Shows STP/RSTP functionality mode on a specific port (read-only): <ul style="list-style-type: none"> • RSTP • STP
Role	Shows specific port role (read-only): <ul style="list-style-type: none"> • root - port that is facing towards the root bridge and will be used to forward traffic from/to the root bridge • alternate - port that is facing towards root bridge, but is not going to forward traffic (a backup for root port) • backup - port that is facing away from the root bridge, but is not going to forward traffic (a backup for non-root port) • designated - port that is facing away from the root bridge and is going to forward traffic • disabled - port that is not strictly part of STP (RSTP functionality is disabled)
Root Path Cost	Shows root path cost for ports that are facing root bridge (read-only)
Type	<ul style="list-style-type: none"> • edge - ports that are not supposed to receive any BPDUs, should be connected to end station (read-only) • point-to-point - ports that operates in full-duplex links, can be part of STP and operate in forwarding state (read-only)
State	Shows each port state (read-only): <ul style="list-style-type: none"> • forwarding - port participates in traffic forwarding and is learning MAC addresses, is receiving BPDUs • discarding - port does not participate in traffic forwarding and is not learning MAC addresses, is receiving BPDU • learning - port does not participate in traffic forwarding, but is learning MAC addresses
Bridge Priority (hex)	RSTP bridge priority for Root Bridge selection

Port Cost Mode	<p>There are two methods for automatically detecting RSTP port cost depending on link speed.</p> <ul style="list-style-type: none">• short: 10G - 2; 1G - 4; 100M - 10; 10M - 100• long: 10G - 2000; 1G - 20000; 100M - 200000; 10M - 2000000
Root Bridge	The priority and MAC address of the selected Root Bridge in the network (read-only)

Statistics, Errors

Provides detailed information about received and transmitted packets.

	Port1	Port2	Port3	Port4	Port5	SFP
Rate						
Rx Rate	0	0	0	0	0	0
Rx Packet Rate	0	0	0	0	0	0
Tx Rate	0	0	0	0	0	0
Tx Packet Rate	0	0	0	0	0	0
Rx						
Bytes	460272502	464168684	1173481	0	0	0
Total Packets	2877155	3317536	2386	0	0	0
Unicasts	200988	716885	2364	0	0	0
Broadcasts	2603412	2550772	22	0	0	0
Multicasts	72755	49879	0	0	0	0
64	160874	697714	1066	0	0	0
65-127	2145476	2067319	22	0	0	0
128-255	37092	66710	28	0	0	0
256-511	497552	483929	2	0	0	0
512-1023	36101	222	1240	0	0	0
1024-1518	60	1642	28	0	0	0
1519-max	0	0	0	0	0	0
Tx						
Bytes	485105983	446676827	413699	0	0	0
Total Packets	3368062	2921848	3560	0	0	0
Unicast Packets	766764	245919	2705	0	0	0
Broadcasts	2551823	2604200	139	0	0	0
Multicasts	49475	71729	716	0	0	0
64	711989	274205	2682	0	0	0
65-127	2068282	2111608	471	0	0	0
128-255	67887	36993	43	0	0	0
256-511	516006	497279	24	0	0	0
512-1023	1904	1703	340	0	0	0
1024-1518	1994	60	0	0	0	0
1519-max	0	0	0	0	0	0


	Port1	Port2	Port3	Port4	Port5	SFP
Rx						
Pauses	0	0	0	0	0	0
Total Errors	0	0	0	0	0	0
FCS Errors	0	0	0	0	0	0
Align Errors	0	0	0	0	0	0
Runts	0	0	0	0	0	0
Fragments	0	0	0	0	0	0
Too Long	0	0	0	0	0	0
Overflows	0	0	0	0	0	0
Tx						
Pauses	0	0	0	0	0	0
Total Errors	0	0	0	0	0	0
Underruns	0	0	0	0	0	0
Too Long	0	0	0	0	0	0
Collisions	0	0	0	0	0	0
Excessive Collisions	0	0	0	0	0	0
Multiple Collisions	0	0	0	0	0	0
Single Collisions	0	0	0	0	0	0
Excessive Deferred	0	0	0	0	0	0
Deferred	0	0	0	0	0	0
Late Collisions	0	0	0	0	0	0

VLAN and VLANs

VLAN configuration for switch ports.

	Port1	Port2	Port3	Port4	Port5	SFP
Ingress						
VLAN Mode	optional ▾	enabled ▾	strict ▾	strict ▾	strict ▾	strict ▾
VLAN Receive	any ▾	only tagged ▾	only untagged ▾	only untagged ▾	only untagged ▾	any ▾
Default VLAN ID	1	1	200	300	400	1
Force VLAN ID	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Egress						
VLAN Header	leave as is ▾	leave as is ▾	leave as is ▾	leave as is ▾	leave as is ▾	leave as is ▾
						<div>Discard Changes</div> <div>Apply All</div>

Property	Description
VLAN Mode	<p>VLAN mode for ingress port:</p> <ul style="list-style-type: none"> disabled - VLAN table is not used. switch ignores VLAN tag part of tagged packets optional - Handle packets with VLAN tag ID that is not present in VLAN table just like packets without VLAN tag enabled - Drop packets with VLAN tag ID that is not present in VLAN table. Packets without VLAN tag are treat as tagged packets with Default VLAN ID strict - Same as enable, but also checks VLAN support for inbound interface (drop packets with VLAN tag ID and ingress port that are not present in VLAN table)
VLAN Receive	<p>Defines the type of allowed packets on ingress port:</p> <ul style="list-style-type: none"> any - allows tagged and untagged packets on a certain port only tagged - allows only packets with a VLAN tag only untagged - allows only packets without a VLAN tag
Default VLAN ID	the switch will treat both untagged and "Default VLAN ID" tagged ingress packets as they are tagged with this VLAN ID. It is also used to untag egress traffic if the packet's VLAN ID matches "Default VLAN ID". The VLAN tag itself will only be added if there is <code>VLAN Header = add if missing</code> specified on the egress port
Force VLAN ID	Whether to apply Default VLAN ID to incoming packets with VLAN tag
VLAN Header	<ul style="list-style-type: none"> leave as is - if VLAN header is present it remains unchanged always strip - if VLAN header is present it is removed from the packet add if missing - if VLAN header is not present it is added to the packet (VLAN ID will be Default VLAN ID of ingress port)

 CSS106 devices running SwOS version 2.12 can filter RSTP BPDU packets when enabling VLAN filtering on ports (VLAN Mode **enabled** or **strict**). With SwOS version 2.13, it is recommended to set VLAN Receive to **any** on trunk ports.

 VLAN modes **enabled** and **strict** require VLAN ID 1 in VLANs table to allow access of untagged traffic to switch itself.

VLAN table specifies forwarding rules for packets that have an IEEE 802.1Q tag. Basically, the table contains entries that map specific VLAN tag IDs to a group of one or more ports. Packets with VLAN tags leave switch through one or more ports that are set in the corresponding table entry. VLAN table works together with destination MAC lookup to determine egress ports. VLAN table supports up to 250 entries.

Link

SFP

Forwarding

RSTP

Statistics

Errors

VLAN

VLANs

Hosts

IGMP Groups

SNMP

ACL

System

Upgrade

VLAN ID	IVL	IGMP Snooping	Port1	Port2	Port3	Port4	Port5	SFP		
<div>100</div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div>not a member</div>	<div>add if missing</div>	<div>always strip</div>	<div>not a member</div>	<div>not a member</div>	<div>not a member</div>	<div>Cut</div>	<div>Insert</div>
<div>200</div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div>not a member</div>	<div>add if missing</div>	<div>not a member</div>	<div>always strip</div>	<div>not a member</div>	<div>not a member</div>	<div>Cut</div>	<div>Insert</div>
<div>300</div>	<div><div></div><div></div></div>	<div><div></div><div></div></div>	<div>not a member</div>	<div>leave as is</div>	<div>leave as is</div>	<div>leave as is</div>	<div>leave as is</div>	<div>leave as is</div>	<div>Cut</div>	<div>Insert</div>

Append

Sort

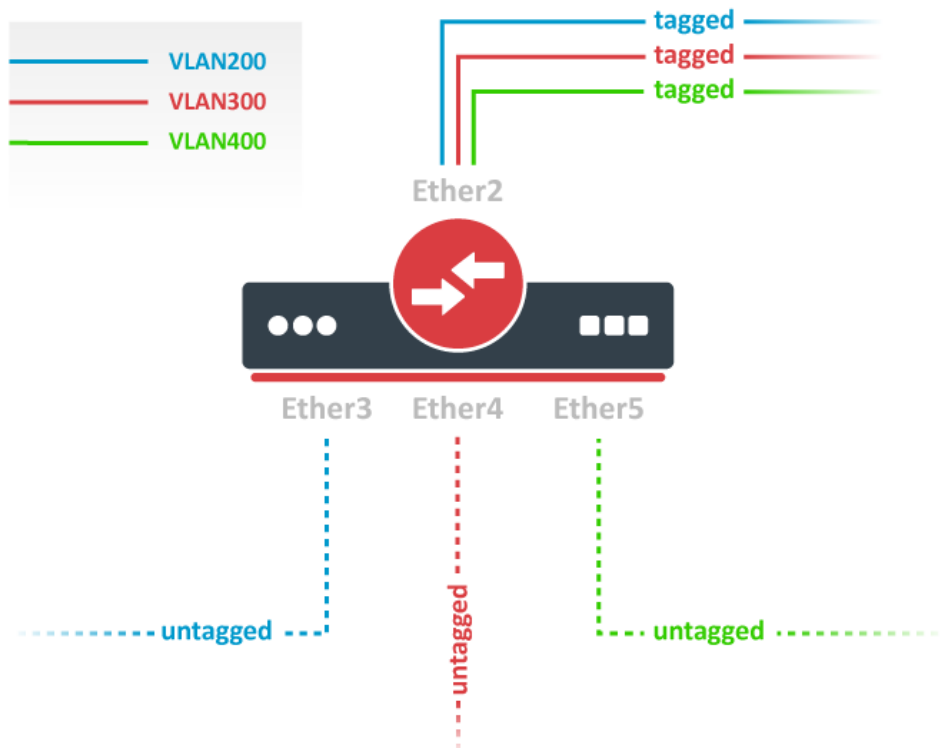
Discard Changes

Apply All

Property	Description
VLAN ID	VLAN ID of the packet
IVL	Enables or disables independent VLAN learning (IVL)
IGMP Snooping	Enables or disables IGMP Snooping on the defined VLAN. When enabled, the switch will listen to IGMP Join and Leave requests from the defined VLAN and only forward traffic to ports, which have sent IGMP membership requests from the defined VLAN. When disabled, the switch will flood all VLAN member ports with Multicast traffic.
Ports	Each port has individual <i>VLAN header</i> options for each VLAN ID. Depending on <i>VLAN mode</i> if lookup is done in this table, the egress action of packets is processed by this option. The egress option from the VLAN tab is ignored.

VLAN Configuration Examples

Trunk and Access Ports



1. In the System menu enable independent VLAN learning (IVL).

MikroTik SwOS Logout

Link SFP Forwarding RSTP Statistics Errors VLAN VLANs Hosts IGMP Groups SNMP ACL **System** Upgrade

General

Address Acquisition DHCP with fallback ▾

Static IP Address 192.168.88.1

Identity MikroTik

Allow From

Allow From Ports ☒ 1 ☒ 2 ☒ 3 ☒ 4 ☒ 5 ☒ SFP

Allow From VLAN

Watchdog ☒

Independent VLAN Lookup ☒

IGMP Snooping ☐

IGMP Fast Leave ☐ ☐ ☐ ☐ ☐

Mikrotik Discovery Protocol ☒

Port1 PoE In Long Cable ☐

MAC Address 64:d1:54:c4:02:92

Serial Number 7A5607973F1F

Board Name CSS106-1G-4P-1S

2. In the VLANs menu add VLAN entries, specify port membership, and enable IVL. The default "leave as is" port setting can be used, the tagging and untagging behavior can be changed with the "Default VLAN ID" setting, see the next step.

MikroTik SwOS

Logout

LinkSFPForwardingRSTPStatisticsErrorsVLANVLANsHostsIGMP GroupsSNMPACLSYSTEMUpgrade

VLAN ID	IVL	IGMP Snooping	Port1	Port2	Port3	Port4	Port5	SFP
200	<input checked="" type="checkbox"/>	<input type="checkbox"/>	not a member	leave as is	leave as is	not a member	not a member	not a member
300	<input checked="" type="checkbox"/>	<input type="checkbox"/>	not a member	leave as is	not a member	leave as is	not a member	not a member
400	<input checked="" type="checkbox"/>	<input type="checkbox"/>	not a member	leave as is	not a member	not a member	leave as is	not a member

AppendSortDiscard ChangesApply All

3. In the VLAN menu configure Default VLAN ID on planned access ports (untagged), select the correct VLAN Receive setting (Port2 only tagged, Port3-5 only untagged), and enable strict VLAN filtering to ensure only allowed VLANs can pass through the ports.

MikroTik SwOS

Logout

LinkSFPForwardingRSTPStatisticsErrorsVLANVLANsHostsIGMP GroupsSNMPACLSYSTEMUpgrade

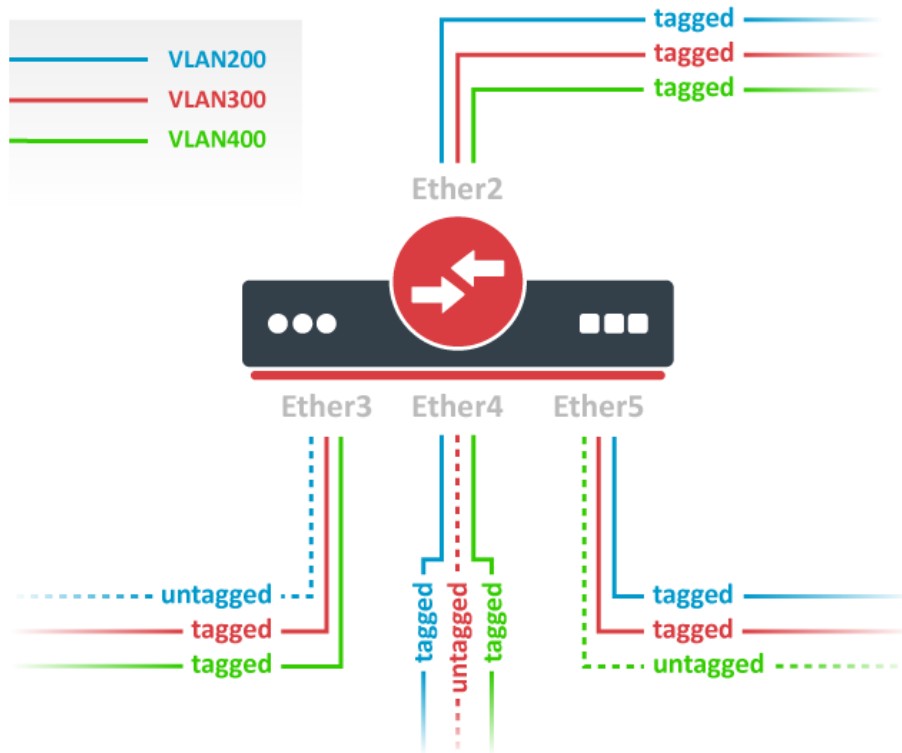
	Port1	Port2	Port3	Port4	Port5	SFP
Ingress						
VLAN Mode	optional	strict	strict	strict	strict	optional
VLAN Receive	any	only tagged	only untagged	only untagged	only untagged	any
Default VLAN ID	1	1	200	300	400	1
Force VLAN ID	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Egress						
VLAN Header	leave as is	leave as is	leave as is	leave as is	leave as is	leave as is

Discard ChangesApply All

!

CSS106 devices running SwOS version 2.12 can filter RSTP BPDU packets when enabling VLAN filtering on ports (VLAN Mode **enabled** or **strict**). With SwOS version 2.13, it is recommended to set VLAN Receive to **any** on trunk ports.

Trunk and Hybrid Ports



1. In the System menu enable independent VLAN learning (IVL).

MikroTik SwOS Logout

Link SFP Forwarding RSTP Statistics Errors VLAN VLANs Hosts IGMP Groups SNMP ACL **System** Upgrade

General

Address Acquisition DHCP with fallback ▾

Static IP Address 192.168.88.1

Identity MikroTik

Allow From

Allow From Ports ☒ 1 ☒ 2 ☒ 3 ☒ 4 ☒ 5 ☒ SFP

Allow From VLAN

Watchdog ☒

Independent VLAN Lookup ☒

IGMP Snooping ☐

IGMP Fast Leave ☐ ☐ ☐ ☐ ☐

Mikrotik Discovery Protocol ☒

Port1 PoE In Long Cable ☐

MAC Address 64:d1:54:c4:02:92

Serial Number 7A5607973F1F

Board Name CSS106-1G-4P-1S

2. In the VLANs menu add VLAN entries, specify port membership, and enable IVL. The default "leave as is" port setting can be used, the tagging and untagging behavior can be changed with the "Default VLAN ID" setting, see the next step.

MikroTik SwOS

Logout

LinkSFPForwardingRSTPStatisticsErrorsVLANVLANsHostsIGMP GroupsSNMPACLSYSTEMUpgrade

VLAN ID	IVL	IGMP Snooping	Port1	Port2	Port3	Port4	Port5	SFP
200	<input checked="" type="checkbox"/>	<input type="checkbox"/>	not a member	leave as is	leave as is	leave as is	leave as is	not a member
300	<input checked="" type="checkbox"/>	<input type="checkbox"/>	not a member	leave as is	leave as is	leave as is	leave as is	not a member
400	<input checked="" type="checkbox"/>	<input type="checkbox"/>	not a member	leave as is	leave as is	leave as is	leave as is	not a member

AppendSortDiscard ChangesApply All

3. In the VLAN menu configure Default VLAN ID on planned hybrid ports (for untagged VLAN), select the correct VLAN Receive setting (Port2 only tagged, Port3-5 any), and enable strict VLAN filtering to ensure only allowed VLANs can pass through the ports.

MikroTik SwOS

Logout

LinkSFPForwardingRSTPStatisticsErrorsVLANVLANsHostsIGMP GroupsSNMPACLSYSTEMUpgrade

Port1	Port2	Port3	Port4	Port5	SFP
Ingress					
VLAN Mode	strict	strict	strict	strict	optional
VLAN Receive	only tagged	any	any	any	any
Default VLAN ID	1	200	300	400	1
Force VLAN ID	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Egress					
VLAN Header	leave as is	leave as is	leave as is	leave as is	leave as is

Discard ChangesApply All

!

CSS106 devices running SwOS version 2.12 can filter RSTP BPDU packets when enabling VLAN filtering on ports (VLAN Mode **enabled** or **strict**). With SwOS version 2.13, it is recommended to set VLAN Receive to **any** on trunk ports.

Management access

In this example, switch management access on VLAN 200 will be created. The configuration scheme is the same as "Trunk and Access Ports" and 1., 2., 3. configuration steps are identical. The additional 4th step requires specifying the management VLAN ID in the System menu. After applying the configuration, the switch will only respond to tagged VLAN 200 packets on Port2 and untagged packets on Port3. The DHCP client will also work in the specified VLAN ID.

MikroTik SwOS
Logout

Link
SFP
Forwarding
RSTP
Statistics
Errors
VLAN
VLANs
Hosts
IGMP Groups
SNMP
ACL
System
Upgrade

General

Address Acquisition
DHCP with fallback

Static IP Address
192.168.88.1

Identity
MikroTik

Allow From

Allow From Ports
☒ 1
☒ 2
☒ 3
☒ 4
☒ 5
☒ SFP

Allow From VLAN
200

Watchdog
☒

Independent VLAN Lookup
☒

IGMP Snooping
☐

IGMP Fast Leave
☐
☐
☐
☐
☐
☐

Mikrotik Discovery Protocol
☒

Port1 PoE In Long Cable
☐

MAC Address
64:d1:54:c4:02:92

Serial Number
7A5607973F1F

Board Name
CSS106-1G-4P-1S



Changing management VLAN can completely disable access to the switch management if VLAN settings are not correctly configured. Save a configuration backup before changing this setting and use [Reset](#) in case management access is lost.

Hosts

This table represents dynamically learned MAC address to port mapping entries. It can contain two kinds of entries: dynamic and static. Dynamic entries get added automatically, this is also called a learning process: when a switch receives a packet from a certain port, it adds the packet's source MAC address X and port it received the packet from to host table, so when a packet comes in with destination MAC address X it knows to which port it should forward the packet. If the destination MAC address is not present in the host table then it forwards the packet to all ports in the group (flood). Dynamic entries take about 5 minutes to time out.



CSS106 series switches support 2048 host table entries.

Port	MAC	VLAN ID
Port1	64:d1:54:c4:02:92	
Port1	cc:2d:e0:e4:b3:38	
Port1	cc:2d:e0:e4:b3:38	200
Port1	cc:2d:e0:e4:b3:38	300
Port1	cc:2d:e0:e4:b3:3a	
Port1	e4:8d:8c:73:6f:ef	
Port2	cc:2d:e0:e4:b3:3c	100
Port4	6c:3b:6b:7b:f9:07	400

Property	Description
Port	Ports the packet should be forwarded to (read-only)
MAC	Learned MAC address (read-only)
VLAN ID	Learned VLAN ID (read-only)

Static Hosts

Static entries will take over dynamic if dynamic entry with same mac-address already exists. Also by adding a static entry you get access to some more functionality.

Port1	Port2	Port3	Port4	Port5	SFP	MAC	VLAN ID	Drop	Mirror	
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="00:01:29:ff:1d:cc"/>	<input type="text" value="1"/>	<input type="checkbox"/>	<input type="checkbox"/>	Insert Cut
<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="text" value="00:0c:42:70:ff:96"/>	<input type="text" value="200"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	Insert Cut
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="text" value="ff:ff:ff:ff:ff:ff"/>	<input type="text" value="1"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	Insert Cut
										Append Sort Discard Changes Apply All

Property	Description
Ports	Ports the packet should be forwarded to
MAC	MAC address
VLAN ID	VLAN ID
Drop	Packet with certain MAC address coming from certain ports can be dropped
Mirror	Packet can be cloned and sent to mirror-target port

IGMP Groups

IGMP Snooping which controls multicast streams and prevents multicast flooding is implemented in SwOS starting from version 2.5. The feature allows a switch to listen in the IGMP conversation between hosts and routers.

First, enable the option under the System tab.

LinkSFPForwardingRSTPStatisticsErrorsVLANVLANsHostsIGMP GroupsSNMPACLSYSTEMUpgrade

General

Address Acquisition

DHCP with fallback

Static IP Address

192.168.88.1

Identity

MikroTik

Allow From

Allow From Ports

☒1☒2☒3☒4☒5

SFP

Allow From VLAN

Watchdog

☒

Independent VLAN Lookup

☐

IGMP Snooping

☒

Mikrotik Discovery Protocol

☒

MAC Address

6c:3b:6b:e2:97:cc

Serial Number

7A5706FD804E

Board Name

CSS106-5G-1S

Available IGMP snooping data can be found under IGMP Group tab.

LinkSFPForwardingRSTPStatisticsErrorsVLANVLANsHostsIGMP GroupsSNMPACLSYSTEMUpgrade

Group Address	VLAN	Member Ports
229.1.1.2		Port3 Port5

Possibility to enable or disable IGMP Snooping for specific VLAN ID.

LinkSFPForwardingRSTPStatisticsErrorsVLANVLANsHostsIGMP GroupsSNMPACLSYSTEMUpgrade

VLAN ID	IVL	IGMP Snooping	Port1	Port2	Port3	Port4	Port5	SFP
30	<input type="checkbox"/>	<input checked="" type="checkbox"/>	not a member	add if missing	always strip	not a member	always strip	not a member
40	<input type="checkbox"/>	<input type="checkbox"/>	not a member	add if missing	not a member	always strip	not a member	not a member

AppendSortDiscard ChangesApply All

SNMP

SwOS supports SNMP v1 and v2c (the Response for GetRequest, GetNextRequest and GetBulkRequest) and uses IF-MIB, SNMPv2-MIB, BRIDGE-MIB and MIKROTIK-MIB (only for health, PoE-out and SFP diagnostics). SNMP traps and writing SwOS configuration are not supported.

Available SNMP data:

- System information
- System uptime
- Port status
- Interface statistics
- Host table information

Enabled	<input checked="" type="checkbox"/>
Community	<input type="text" value="public"/>
Contact Info	<input type="text"/>
Location	<input type="text"/>
<div>Discard Changes Apply All</div>	

Property	Description
Enabled	Enable or disable SNMP service
Community	SNMP community name
Contact Info	Contact information for the NMS
Location	Location information for the NMS

ACL

An access control list (ACL) rule table is a very powerful tool allowing wire-speed packet filtering, forwarding, and VLAN tagging based on L2, L3, and L4 protocol header field conditions. SwOS allows you to implement a limited number of access control list rules (32 simple rules (only L2 conditions are used); 16 rules where both L2 and L3 conditions are used; or 8 advanced rules where all L2,L3, and L4 conditions are used). Each rule contains a conditions part and an action part.

From: ☐ 1 ☒ 2 ☐ 3 ☐ 4 ☐ 5 ☐ SFP
Clear Cut Insert

MAC Src:
MAC Dst:
Ethertype: hex

VLAN:
VLAN ID:
Priority:

IP Src:
IP Dst:
Protocol:
DSCP:

☒ Redirect To ☐ 1 ☐ 2 ☐ 3 ☒ 4 ☐ 5 ☐ SFP
☐ Mirror
Rate:
Set VLAN ID:
Priority:

From: ☒ 1 ☒ 2 ☒ 3 ☒ 4 ☒ 5 ☒ SFP
Clear Cut Insert

MAC Src:
MAC Dst:
Ethertype: hex

VLAN:
VLAN ID:
Priority:

IP Src:
IP Dst:
Protocol:
DSCP:

☐ Redirect To ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ SFP
☐ Mirror
Rate:
Set VLAN ID:
Priority:

Append Discard Changes Apply All

Conditions parameters

Property	Description
From	The port that packet came in from
MAC Src	Source MAC address and mask
MAC Dst	Destination MAC address and mask
Ethertype	Protocol encapsulated in the payload of an Ethernet Frame
VLAN	VLAN header presence: <ul style="list-style-type: none"> any present not present
VLAN ID	VLAN tag ID
Priority	Priority in VLAN tag
IP Src (IP/netmask:port)	Source IPv4 address, netmask, and L4 port number
IP Dst (IP/netmask:port)	Destination IPv4 address, netmask, and L4 port number
Protocol	IP protocol
DSCP	IP DSCP field

Action parameters

Property	Description
Redirect To	Whether to force new destination ports (If "Redirect To" is enabled and no ports are specified in "Redirect To Ports", a packet will be dropped)
Redirect To Ports	Redirect destination ports

Mirror	Clones packet and sends it to mirror-target port
Rate	Limits bandwidth (bps)
Set VLAN ID	Changes the VLAN tag ID, if VLAN tag is present
Priority	Changes the VLAN tag priority bits, if VLAN tag is present

Reset

The CSS106-5G-1S and CSS106-1G-4P-1S have built-in backup SwOS firmware which can be loaded in case standard firmware breaks or upgrade fails:

- Holding Reset button for few seconds while the device is booting will reset configuration and load backup firmware.
- After loading backup firmware, it is possible to connect to 192.168.88.1 (or leased address from a DHCP server) using web browser and install new SwOS firmware.