

CIS-CRS328-24P User Manual



Table of Contents

Welcome to Custom Integration Solutions	4
Overview.....	4
Package Contents.....	4
Power.....	4
PoE Output	4
Device Details.....	5
Ports.....	5
LED Indicators.....	5
Buttons	5
Input Power Requirements	5
Quick Setup.....	6
Setup and Accessing the Web Interface	7
The Status Page.....	8
Setting the Switch's Identity.....	8
Undo / Redo	9
Show / Hide Passwords	9
Rebooting the Device.....	9
Changing the Default Password	10
Setting the Time Zone.....	10
IP Addressing	11
View the Switch's IP Addresses	11
CIS Support.....	11
Renewing the IP Address	12
Setting a Static IP address.....	13
Interfaces	15
Power Cycling an Ethernet Port	15

VLANs.....	16
Purchase VLAN configuration.....	16
Changing the VLAN on a Port on a Preconfigured System.....	16
Manually Configuring the Switch for VLANs	17
Step 1 – Enable VLAN Filtering on the Bridge	17
Step 2 – Assign the Trunk Port(s)	18
Step 3 – Assign Ports to VLANs.....	19
Multicast Filtering – Prior to 6.48	20
Multicast Filtering – 6.48 and Newer	21
Multicast Querier	21
PoE Information and Settings.....	22
Enable/Disable PoE.....	22
Tools.....	23
UPnP.....	23
Ping.....	23
IP Scan	24
Troubleshooting.....	25
Warranty Information.....	26
Contact Information.....	26

Welcome to Custom Integration Solutions

Thank you for purchasing CIS devices. Our solutions make it easy for integrators to deploy networks in home and business settings with minimal configuration. Our support team is here to assist with setting up equipment and answering your network related questions.

Overview

Package Contents



Switch



Power cable



Rack ears (2)



Screws (8)

Power

The unit is equipped with one IEC type AC power input, which accepts 100–240 V power (~ 50/60 Hz 7 A max).

The power consumption of this device under maximum load is up to 494 W with attachments, 44 W without attachments.

PoE Output

The CIS-CRS328-24P can supply PoE to external devices. The output voltage will be selected automatically, depending on the voltage the connected device requires. The device can power both 802.3af/at devices and devices that accept passive PoE power. If necessary, the output voltage can be switched manually.

By default, the PoE mode is set to auto. It will not damage non-PoE devices and will auto-detect devices with PoE support and their required voltage. Once a PoE device is detected, it will be powered and the PoE LEDs will turn on.

The PoE out ports are grouped in three PoE out groups of 8 ports each. The total PoE limit is 450w (150w per 8 port group). Each port can provide up to 30 W with high voltage output, and 26.5 W with low voltage output.

Device Details



Ports

- 24 Gigabit Ethernet ports (With Auto MDI/X – You can use straight-through or cross-over cables for connecting devices to the switch).
- 4 SFP+ cages, which accept both 1.25 Gb SFP and 10 Gb SFP+ modules.
- RJ45 serial port–disabled by default.

LED Indicators

- PWR LED – lit when the switch is powered on.
- USR LED – an LED that can be customized to display different information.
- The top row LEDs indicate PoE out status. A green LED indicates that the respective port uses low voltage, a red LED indicates high voltage.
 - A flashing green LED – indicates a problem with a low voltage device.
 - A flashing red LED – indicates a problem with a high voltage device.
- The bottom row LEDs indicate Ethernet and SFP port activity.
- FAN FAULT LED – indicates a problem with the cooling fans.
- PoE FAULT LED – indicates the switch has exceeded the overall maximum PoE output limit. Port PoE-out priorities work in 3 independent sections (8 ports each) and an overload will occur in any section that breaches 150 watts of consumption.

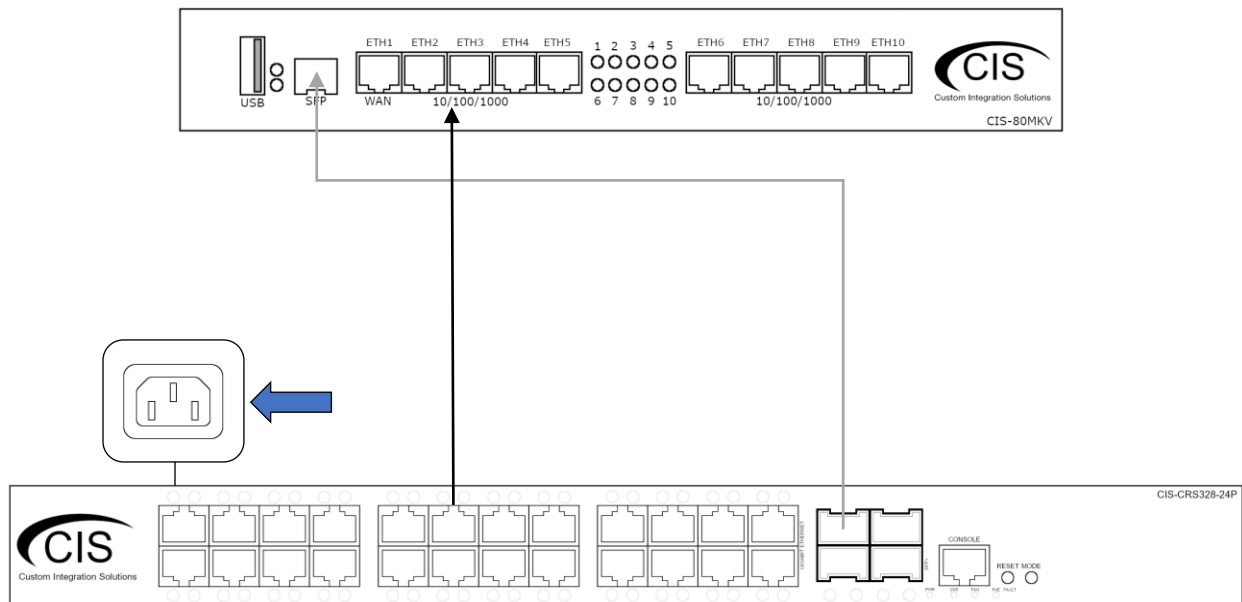
Buttons

Reset button: This button is located on the side next to the USB port. Hold this button while the device is powered off, then apply power. Keeping holding until the USR LED light starts flashing, (5 seconds) then release the button to reset to the default CIS configuration. You can use this procedure if you have forgotten the password to access the device, or simply wish to return the unit to its default configuration state.

Input Power Requirements

Supported input voltage–100V AC–240V AC.

Quick Setup



1. Connect the included power cable to the connector on the back of the switch.
2. Connect the switch to the router with an Ethernet cable or SFP cable. Do not connect both cables at the same time.
3. Connect your network devices to the remaining ports on the switch.

Setup and Accessing the Web Interface

1. Connect the switch to your router using either an Ethernet or SFP cable. Do not connect both to the router.
2. Connect your laptop or PC to any remaining Ethernet port on the front of the CIS switch (excluding the console port). You can also access the web interface plugged directly into the router.
3. To access the web interface, you must obtain the IP address assigned to the switch. Access your router's configuration page, then find the IP address assigned to the switch in the DHCP leases.
4. Launch a web browser and navigate to the IP address of the switch. To login, enter the username **cis** and password **integration**.
5. Integrators may use the Get TeamViewer link if remote assistance is required.

CIS-CRS328-24P Switch

You have connected to a switch. Administrative access only. If this device is not in your possession, please contact your local network administrator.

CIS
Custom Integration Solutions

CIS Login:


Login: Login

Password:

 Smart Router

 CIS Store

 Get TeamViewer

 Owners Guide

 Like us on Facebook!

© Custom Integration Solutions

The Status Page

The status page provides basic diagnostic information. There is a CIS Support Address should you require assistance. The switch's Identity will show you which device you are accessing on your network. You can view uptime, memory usage and load on the CPU.

CIS Switch Status RouterOS v6.47.7 (stable)

ISP Public Address

CIS Switch Identity

CIS Switch Uptime 00:22:01

CIS Switch Address 10.100.1.2/24

CPU Load 11 %

Total Memory 128.0 MiB

Free Memory 106.6 MiB

CIS Platinum Support

CIS Support Address 10.255.255.95
FOR INTEGRATOR PLATINUM SUPPORT PRESENT
YOUR CIS SUPPORT ADDRESS ACCESS NUMBER

Byte Graph

Packet Graph

Setting the Switch's Identity

The identity is used to identify your device on the network. If you have multiple switches of the same model, it is recommended you use a naming scheme to identify them.

The **Identity** setting can be found in the **System** tab in the left toolbar.

CIS Switch Status RouterOS v6.47.7 (stable)

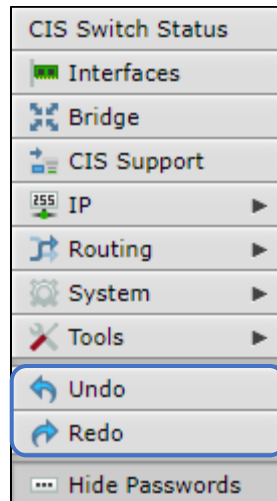
Identity

Apply

Identity "Switch Identity"

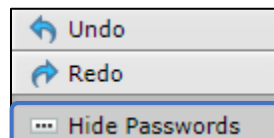
Undo / Redo

Undo and Redo buttons are located in the left toolbar. You may use them to quickly undo/redo any changes made to configuration.



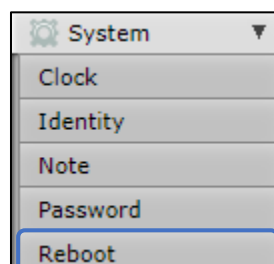
Show / Hide Passwords

Selecting the **Hide Passwords** button in the left toolbar will toggle the displaying of passwords related to Wi-Fi, Hotspot, and more.



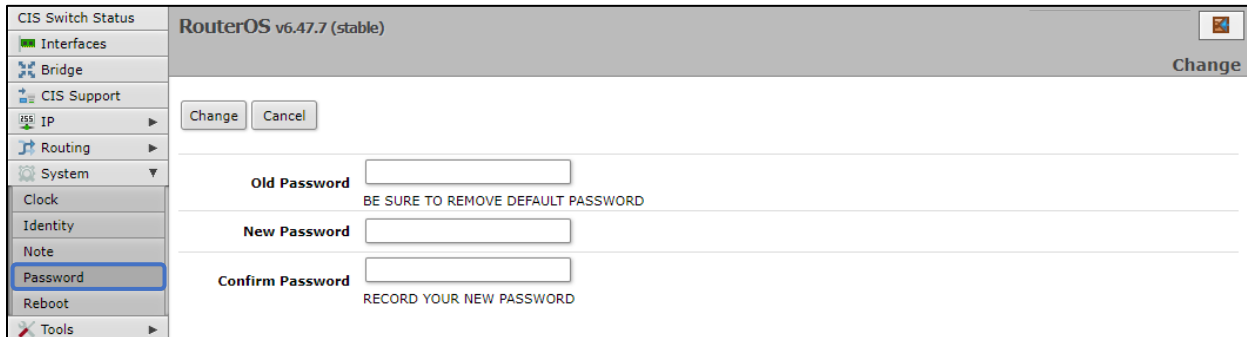
Rebooting the Device

If you are having ongoing issues with your network and suspect a reboot will help, the **Reboot** option can be found in the **System** tab in the left toolbar. Clicking reboot will ask for confirmation before proceeding.



Changing the Default Password

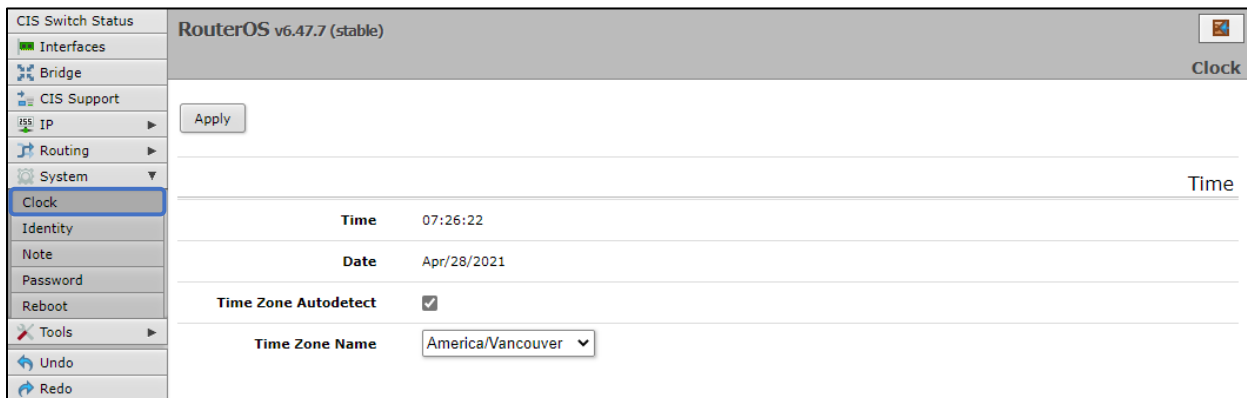
After you log in for the first time, please create a new password to increase the security of the device. Enter the old password in the top field and a secure password in the new and confirm password fields.



The screenshot shows the RouterOS v6.47.7 (stable) web interface. The left sidebar contains a menu with the following items: CIS Switch Status, Interfaces, Bridge, CIS Support, IP, Routing, System, Clock, Identity, Note, Password (highlighted), Reboot, and Tools. The main content area is titled "RouterOS v6.47.7 (stable)" and has a "Change" button in the top right corner. Below the title, there are two buttons: "Change" and "Cancel". The form contains three password fields: "Old Password" (with a warning "BE SURE TO REMOVE DEFAULT PASSWORD" below it), "New Password", and "Confirm Password" (with a warning "RECORD YOUR NEW PASSWORD" below it).

Setting the Time Zone

You can find the Clock settings under the System tab in the left toolbar. Select your time zone from the drop-down menu.

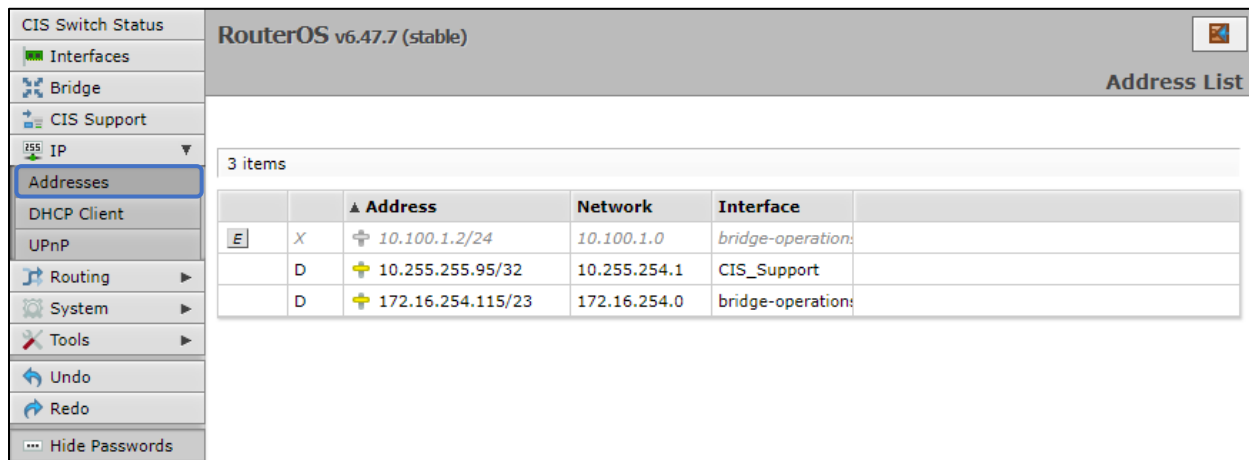


The screenshot shows the RouterOS v6.47.7 (stable) web interface with the "Clock" settings page. The left sidebar menu is the same as in the previous screenshot, but "Clock" is highlighted. The main content area is titled "RouterOS v6.47.7 (stable)" and has a "Clock" button in the top right corner. Below the title, there is an "Apply" button. The form displays the following settings: "Time" (07:26:22), "Date" (Apr/28/2021), "Time Zone Autodetect" (checked), and "Time Zone Name" (America/Vancouver, shown in a dropdown menu).

IP Addressing

View the Switch's IP Addresses

By default, the switch will acquire an IP address through DHCP. You can view the IP addresses in the **IP > Addresses** section. In the picture below, there is an entry for a static address (optional), an entry for your support IP address (if the support tunnel is enabled), and an entry for the IP address received via DHCP.

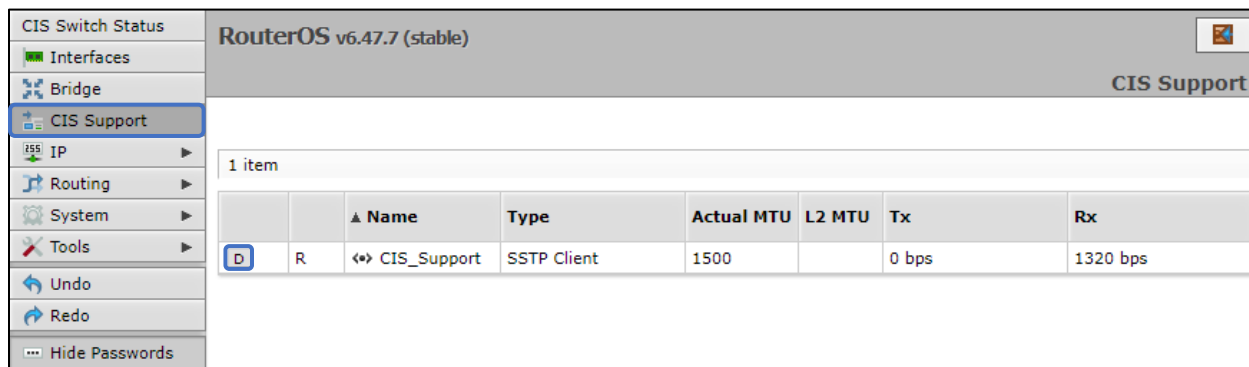


The screenshot shows the RouterOS v6.47.7 (stable) interface. The left sidebar has the 'IP' menu expanded to 'Addresses'. The main panel is titled 'Address List' and shows 3 items in a table:

		▲ Address	Network	Interface	
<input type="checkbox"/>	X	<input type="checkbox"/> 10.100.1.2/24	10.100.1.0	bridge-operation:	
<input type="checkbox"/>	D	<input type="checkbox"/> 10.255.255.95/32	10.255.254.1	CIS_Support	
<input type="checkbox"/>	D	<input type="checkbox"/> 172.16.254.115/23	172.16.254.0	bridge-operation:	

CIS Support

With the CIS Support tunnel activated, the CIS team can make configuration changes, push updates, and troubleshoot your network. Press the button to the left of the entry. "D" stands for disable, while "E" stands for enable.

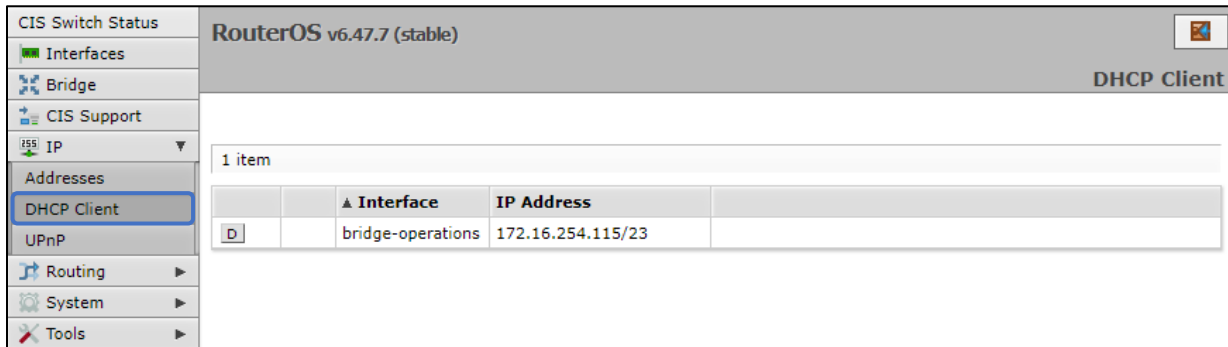


The screenshot shows the RouterOS v6.47.7 (stable) interface. The left sidebar has the 'CIS Support' menu selected. The main panel is titled 'CIS Support' and shows 1 item in a table:

		▲ Name	Type	Actual MTU	L2 MTU	Tx	Rx
<input type="checkbox"/>	R	<input type="checkbox"/> CIS_Support	SSTP Client	1500		0 bps	1320 bps

Renewing the IP Address

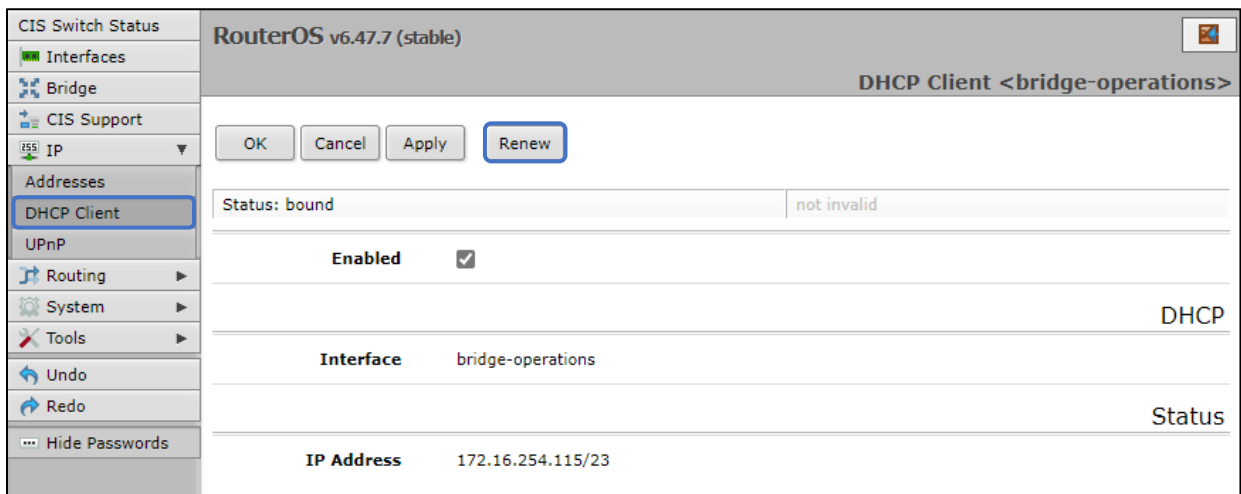
To renew the IP address, select the **DHCP Client** section under the **IP** tab.



The screenshot shows the RouterOS v6.47.7 (stable) interface. The left sidebar has the 'DHCP Client' option selected under the 'IP' tab. The main content area shows a table with one entry:

	▲ Interface	IP Address	
D	bridge-operations	172.16.254.115/23	

Click on the entry to bring up the options. Click the **Renew** button to obtain a new lease.

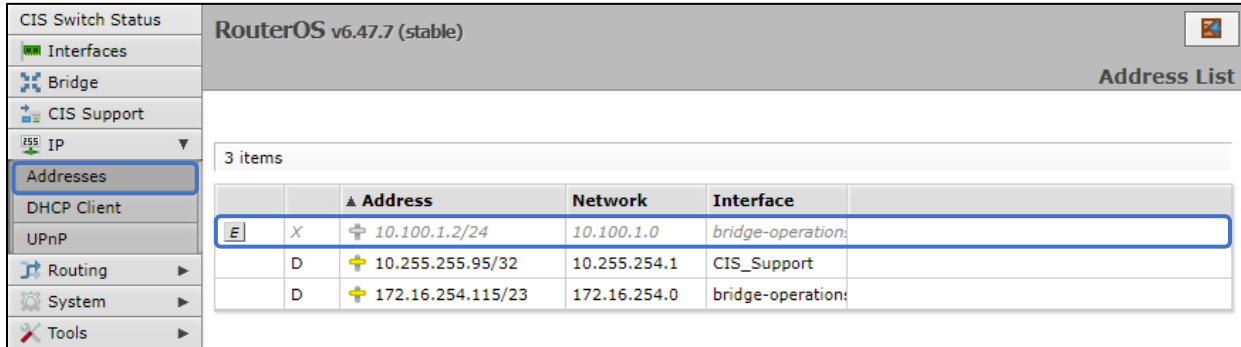


The screenshot shows the configuration options for the DHCP Client on the 'bridge-operations' interface. The 'Renew' button is highlighted. The configuration includes:

- Buttons: OK, Cancel, Apply, Renew
- Status: bound | not invalid
- Enabled:
- Interface: bridge-operations
- IP Address: 172.16.254.115/23

Setting a Static IP address

To set a static IP, select **Addresses** from the **IP** tab. Click on the field containing the disabled IP address.

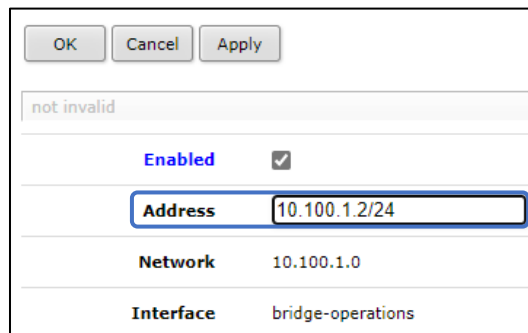


		▲ Address	Network	Interface
E	X	10.100.1.2/24	10.100.1.0	bridge-operations
	D	10.255.255.95/32	10.255.254.1	CIS_Support
	D	172.16.254.115/23	172.16.254.0	bridge-operations

If your network falls in one of the ranges below, you can set the static IP address yourself. If it is outside of these ranges, you must call CIS to have a route created!

Available address ranges:			
172.16.1.0/24	10.100.1.0/24	192.168.1.0/24	192.168.0.0/24

Enter the IP address to assign to the switch. Ensure that it is outside of the DHCP pool, and not in use by other devices. The format must include **/24** at the end. This is the subnet mask, which determines how many devices can be connected to this network.



OK Cancel Apply

not invalid

Enabled

Address 10.100.1.2/24

Network 10.100.1.0

Interface bridge-operations

Once you have set the static IP address, disable the DHCP client. Go to the **DHCP Client** tab located under **IP** in the toolbar. Click the "D" to disable the DHCP client.

	▲ Interface	IP Address
<input type="checkbox"/> D	bridge-operations	172.16.254.115/23

Interfaces

To view the interface status, select **Interfaces**, then the **Ethernet** tab. The Ethernet tab provides an overview of the activity on all ports. You can view the traffic sent and received, the status of PoE, PoE settings, PoE priority and current being drawn by PoE devices.

The screenshot shows the RouterOS v6.48 (stable) web interface. The left sidebar contains navigation options: CIS Switch Status, Interfaces, CIS Support, Bridge, IP, Routing, System, Tools, Undo, Redo, and Hide Passwords. The main content area is titled 'RouterOS v6.48 (stable)' and 'Interface List'. A 'Power Cycle' button is visible. Below it, a table displays 6 items:

		▲ Name	Type	MTU	L2 MTU	Tx	Rx
<input type="checkbox"/>	S	⚡ SFP-01	Ethernet	1500	1600	0 bps	0 bps
;;; TRUNK							
<input type="checkbox"/>	RS	⚡ ether-01	Ethernet	1500	1598	102.9 kbps	26.3 kbps
<input type="checkbox"/>	S	⚡ ether-02	Ethernet	1500	1598	0 bps	0 bps
<input type="checkbox"/>	S	⚡ ether-03	Ethernet	1500	1598	0 bps	0 bps
<input type="checkbox"/>	S	⚡ ether-04	Ethernet	1500	1598	0 bps	0 bps
<input type="checkbox"/>	RS	⚡ ether-05	Ethernet	1500	1598	3.5 kbps	5.8 kbps

Power Cycling an Ethernet Port

Click the **Power Cycle** button in the Interfaces > Ethernet section. Select the port and duration, then click **Power Cycle**.

The screenshot shows the RouterOS v6.48 (stable) web interface with the 'Power Cycle' dialog box open. The dialog has a 'Power Cycle' button and a 'Cancel' button. Below the buttons, there are two fields: 'Interface' with a dropdown menu showing 'ether-02' and 'Duration' with a text input field containing '5' and a 's' unit indicator.

VLANs

VLANs provide isolation between your network devices. This can keep traffic from designated devices secure and restricted from other devices on the network and reduce the overall congestion. It is highly recommended to deploy VLANs for VoIP applications and systems that handle sensitive data.

Purchase VLAN configuration

For a complete VLAN model, the router, access points and switching all require additional configuration.

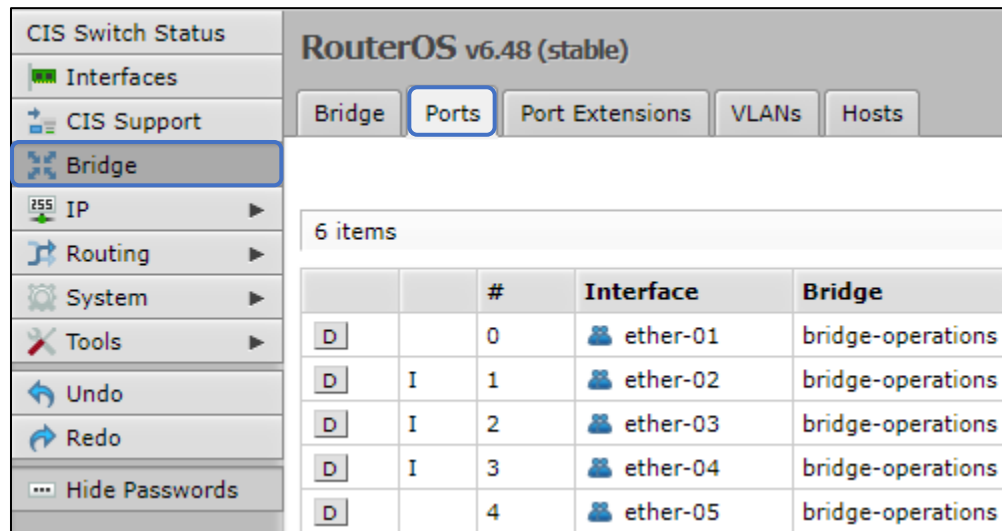
VLANs and additional networks are available on the CIS Store.

<https://www.custom-integration-solutions.com/store/cis-vlan-interface/>

<https://www.custom-integration-solutions.com/store/cis-additional-network/>

Changing the VLAN on a Port on a Preconfigured System

Select **Bridge** from the left toolbar, then click on the **Ports** tab. Select the port you wish to change the VLAN on.



The screenshot shows the RouterOS v6.48 (stable) configuration interface. The left sidebar contains a menu with options: CIS Switch Status, Interfaces, CIS Support, Bridge (selected), IP, Routing, System, Tools, Undo, Redo, and Hide Passwords. The main area is titled "RouterOS v6.48 (stable)" and has tabs for Bridge, Ports (selected), Port Extensions, VLANs, and Hosts. Below the tabs, there is a table with 6 items. The table has columns for #, Interface, and Bridge. The data rows are:

	#	Interface	Bridge
D	0	ether-01	bridge-operations
D	I 1	ether-02	bridge-operations
D	I 2	ether-03	bridge-operations
D	I 3	ether-04	bridge-operations
D	I 4	ether-05	bridge-operations

Enter the VLAN you wish the port to be a member of in the **PVID** field.

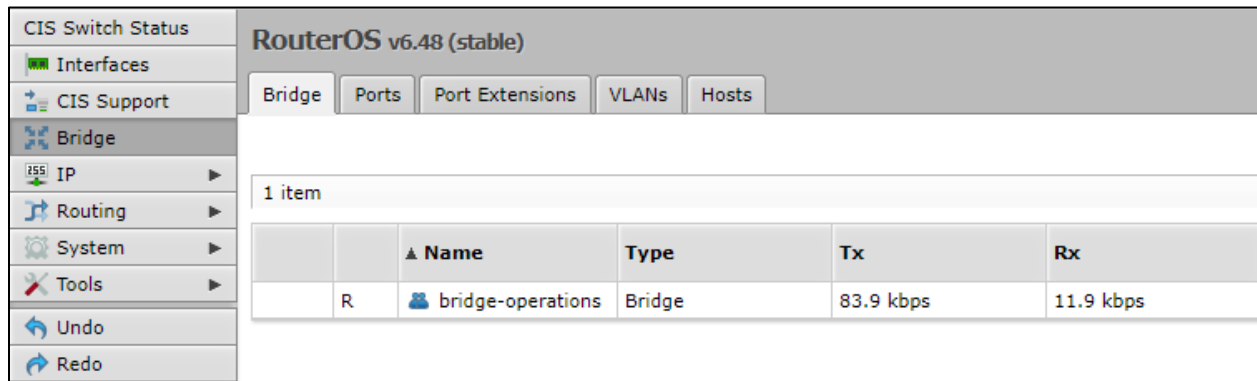
PVID

Manually Configuring the Switch for VLANs

When you purchase a VLAN configuration from CIS, these configuration changes will already be implemented. If you wish to implement these changes yourself, follow the instructions below.

Step 1 – Enable VLAN Filtering on the Bridge

Select **Bridge** from the left toolbar. Select the bridge entry.



CIS Switch Status RouterOS v6.48 (stable)

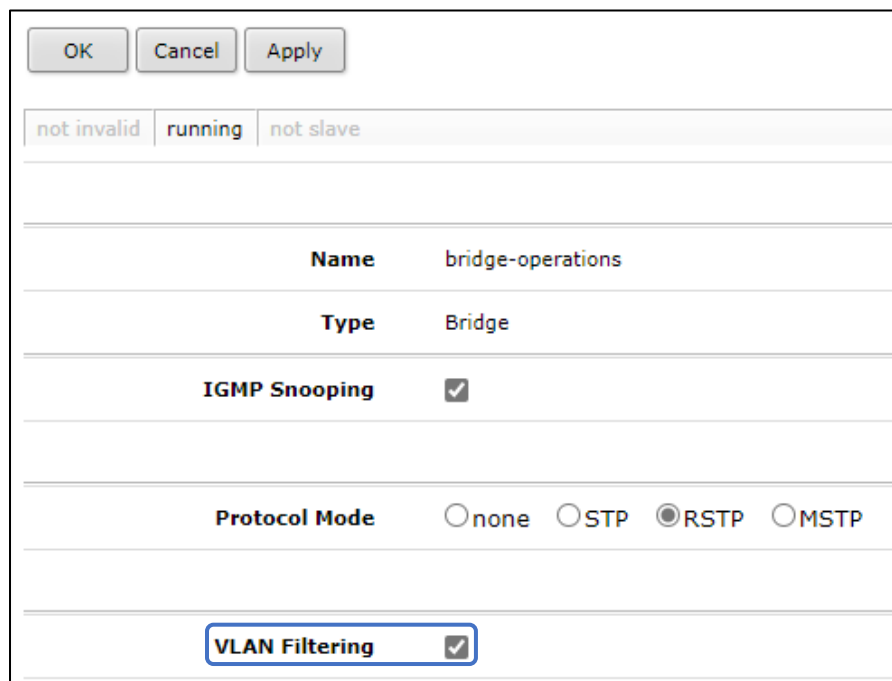
Interfaces
CIS Support
Bridge
IP
Routing
System
Tools
Undo
Redo

Bridge Ports Port Extensions VLANs Hosts

1 item

	▲ Name	Type	Tx	Rx
R	bridge-operations	Bridge	83.9 kbps	11.9 kbps

Enable the **VLAN Filtering** option. Click Apply, then OK.



OK Cancel Apply

not invalid running not slave

Name bridge-operations

Type Bridge

IGMP Snooping

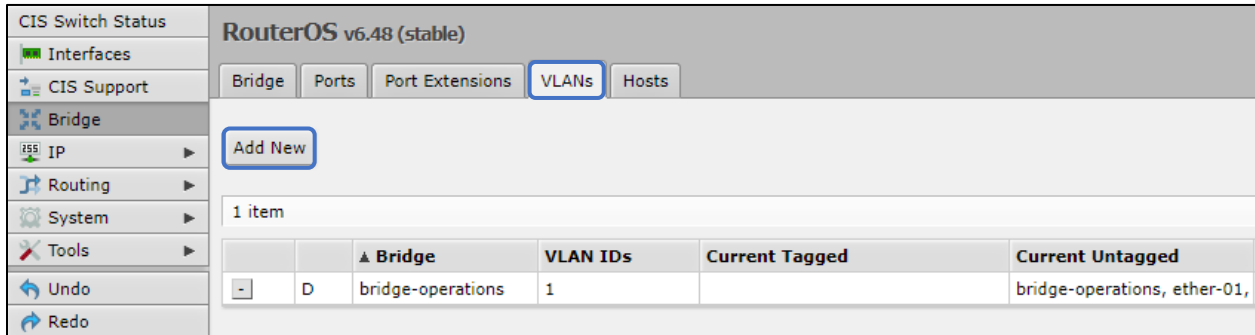
Protocol Mode none STP RSTP MSTP

VLAN Filtering

Step 2 – Assign the Trunk Port(s)

Trunk ports carry traffic from all VLANs between your switches and routers. You must configure a trunk port between the router and the switch.

With **Bridge** selected in the left toolbar, select the **VLANs** tab. Click **Add New**.



CIS Switch Status RouterOS v6.48 (stable)

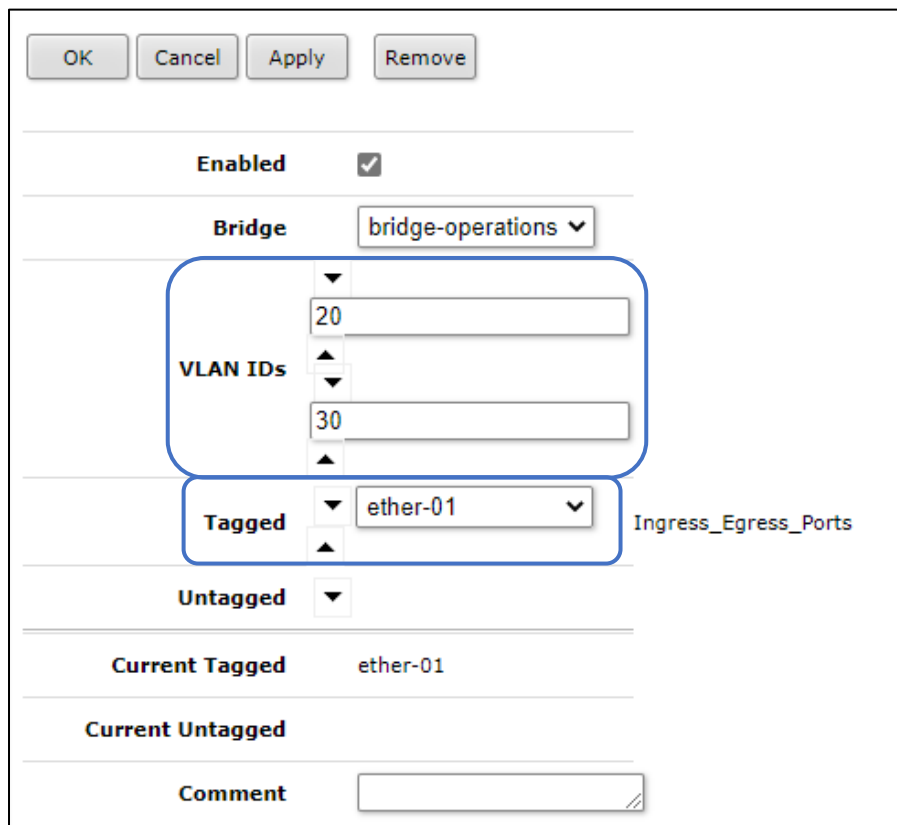
Bridge Ports Port Extensions **VLANs** Hosts

Bridge Add New

1 item

	▲ Bridge	VLAN IDs	Current Tagged	Current Untagged
-	D bridge-operations	1		bridge-operations, ether-01,

Enter the VLAN IDs the trunk will carry. You should enter the VLAN ID of every VLAN that will be present on the network. Use the up/down arrows to add and remove VLAN IDs. Set each trunk port to be **Tagged**.



OK Cancel Apply Remove

Enabled

Bridge bridge-operations

VLAN IDs

20

30

Tagged ether-01 Ingress_Egress_Ports

Untagged

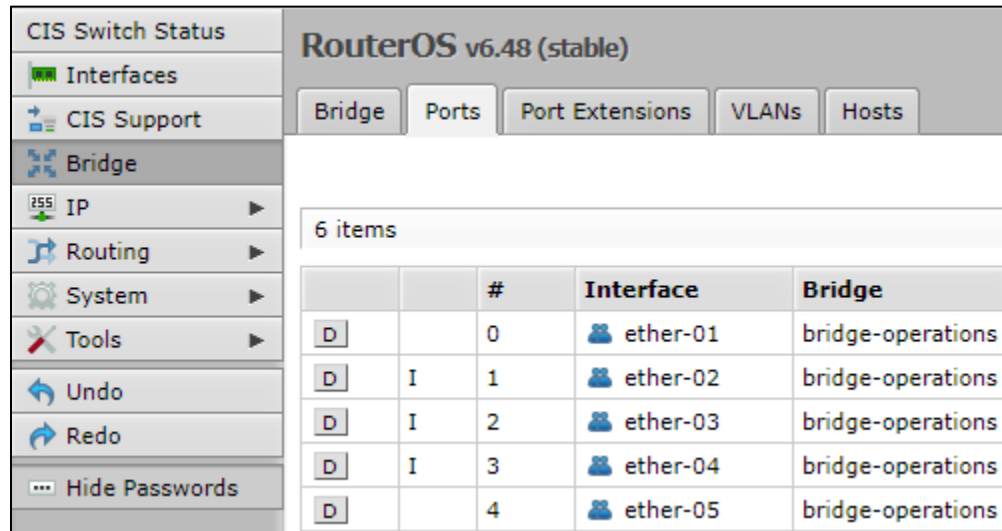
Current Tagged ether-01

Current Untagged

Comment

Step 3 – Assign Ports to VLANs

The ports that connect to your devices will be “untagged” ports or access ports. The final step is to set which VLAN they will be a member of. With the **Bridge** section selected in the left toolbar, select the **Ports** tab. Click on a port below.



		#	Interface	Bridge
D		0	ether-01	bridge-operations
D	I	1	ether-02	bridge-operations
D	I	2	ether-03	bridge-operations
D	I	3	ether-04	bridge-operations
D		4	ether-05	bridge-operations

Enter the VLAN number in the **PVID** field and click Apply, then OK.

PVID	<input type="text" value="20"/>
-------------	---------------------------------

Multicast Filtering – Prior to 6.48

Multicast traffic conserves network resources. If one device were to send a single stream of data to multiple other devices on the network, it would take many times the amount of bandwidth. Multicast traffic reduces the load on the transmitting device by duplicating the traffic instead.

However, the switches in the system must be configured to handle multicast traffic or the network can become flooded with this traffic. Without a solution in place, this traffic will be sent to every port – often bringing the network down. Use the following methods to prevent this from happening.

Note: This method is deprecated and will be removed in future firmware versions!

On systems prior to version 6.48:

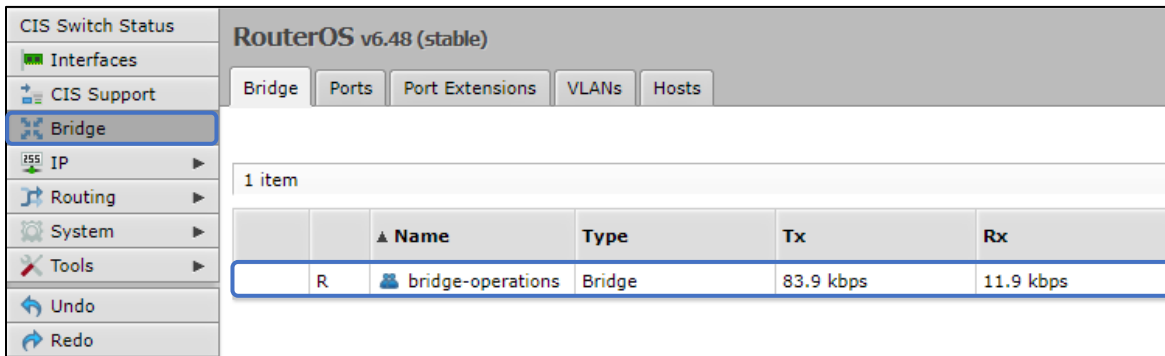
Select the **Interfaces** option from the left toolbar. Select the **Interface List** tab. Enable the MAC Filter for each port that will receive multicast traffic and **ONLY** the ports that will receive multicast traffic.

The screenshot shows the RouterOS v6.48 (stable) web interface. The left sidebar has the 'Interfaces' menu item selected. The main content area shows the 'Interface List' tab for the 'Ethernet' section. A 'Lists' button is visible. Below it, a table displays 4 items. The table has columns for 'List' and 'Interface'. Each row shows a 'MAC FILTER' applied to a specific interface (ether-02, ether-03, ether-04, ether-05). The 'List' column contains an 'E' icon, an 'X' icon, and the text 'MAC FILTER'. The 'Interface' column contains the interface name.

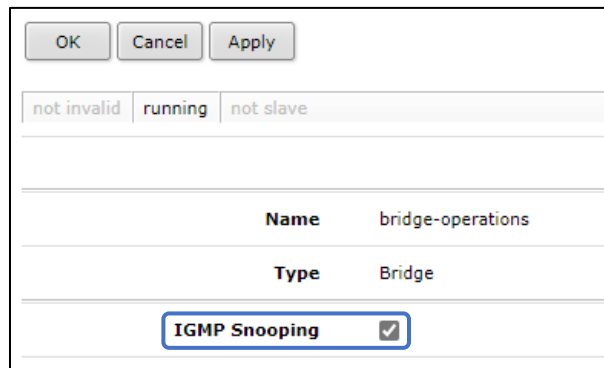
		▲ List	Interface
<input checked="" type="checkbox"/>	X	MAC FILTER	ether-02
<input checked="" type="checkbox"/>	X	MAC FILTER	ether-03
<input checked="" type="checkbox"/>	X	MAC FILTER	ether-04
<input checked="" type="checkbox"/>	X	MAC FILTER	ether-05

Multicast Filtering – 6.48 and Newer

Switches 6.48 and newer only – By enabling **IGMP Snooping**, multicast traffic will be automatically forwarded to only the devices that request it. Select the **Bridge** option from the left toolbar. Click on the bridge entry.



Enable **IGMP Snooping**. Click Apply, then OK.



Multicast Querier

The multicast querier option is required for many multicast systems to function correctly. With this enabled, the switch will periodically check to determine if devices are still requiring a multicast stream.



PoE Information and Settings

PoE-Out Modes:

Auto-on mode (default)

When selected, auto-on mode checks for resistance on the host device and will automatically supply power to devices that require it. It will not damage non-PoE devices.

Forced-on mode

When selected, the switch applies power on pins 4,5 (+) and 7,8 (-), even if no cable is attached.

Be careful plugging non-PoE devices into a port when Forced-on is selected. **You may damage your device!**

Off mode

When selected, the switch will not supply power to connected devices.

PoE-Out limitations

The total PoE limit is 450w (150w per 8 port group). Each port can provide up to 30 W with high voltage output, and 26.5 W with low voltage output.

Enable/Disable PoE

Select the port from the **Interfaces** tab. Change the PoE Out option accordingly.

		PoE
PoE Out	auto on	▼
PoE Priority	10	
Power Cycle Ping Enabled	<input type="checkbox"/>	
Power Cycle Interval		
PoE Out Status	powered on	
PoE Out Current	120 mA	
PoE Out Voltage		
PoE Out Power	6.7 W	

Tools

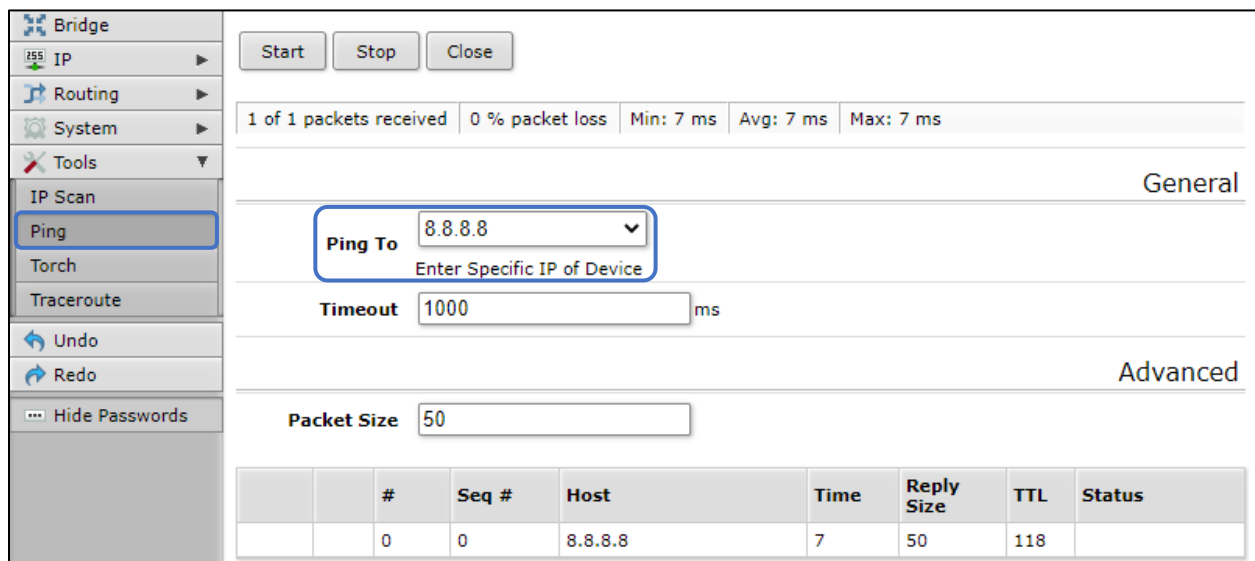
UPnP

Universal Plug and Play enables your switch to easily discover other devices located on the network and vice-versa. If you require UPnP, select it under the **IP** tab in the toolbar, then enable it. UPnP has implications on the security of the device, and it is recommended you leave it disabled unless required.



Ping

Ping uses Internet Control Message Protocol (ICMP) echo messages to determine if a remote device is active. It will also provide the round-trip time between the hosts. Enter the IP address of the device and select Start to begin. Ping devices on your network to see if they are online, or ping devices over the internet to confirm connectivity. Google's DNS server at 8.8.8.8 is a common target.



IP Scan

The IP scan tool locates devices on the network. It can also locate devices that have a static IP set internally if they are on the same network as the switch.

To use the IP scan tool, select the network you wish to scan on (bridge-operations is default), then enter the network address and subnet mask using CIDR notation.

The screenshot shows the RouterOS v6.47.7 (stable) IP Scan tool interface. The sidebar on the left contains navigation options: CIS Router Status, Wi-Fi Manager, Interfaces, IP, System, Tools, IP Scan (highlighted), Platinum Monitoring, Ping, Torch, and Traceroute. The main area has a 'Start' button, 'Stop' button, and 'Close' button. Below these are two dropdown menus: 'Interface' (set to 'bridge-operations') and 'Address Range' (set to '10.100.1.0/24'). The 'Address Range' field is highlighted with a blue border. At the bottom, a table header is visible with columns: #, Address, MAC Address, Time (ms), DNS, SNMP, and Netbios.

Select **bridge-operations** and enter **10.100.1.0/24** as the address range. You may have multiple interfaces and address ranges depending on your configuration. Most use a /24 network size.

Troubleshooting

Symptom	Possible causes
The PoE access point, switch, or other powered device will not turn on.	<ul style="list-style-type: none"> • Try changing the PoE mode to “forced on” from the interfaces menu. Remember, never force PoE on a non-PoE device! • Select the appropriate voltage when setting the power to “forced on”. 802.3af/at devices will require “high” voltage.
I can’t get VLANs to work correctly.	<ul style="list-style-type: none"> • The router must be configured to work with VLANs for most operations. • Ensure the trunk ports are tagged correctly. • Contact CIS for assistance.
I can’t get a connection when using the SFP port.	<ul style="list-style-type: none"> • CIS recommends DAC SFP cables such as the CIS-SFP-001 and 003, though other SFP modules are compatible. • Try a different SFP port. Two ports are set at 10 Gbit and the other two are set at 1 Gbit to maximize compatibility. • Ensure the SFP cables are inserted completely. There should be a slight click as they are inserted. They will slide in most of the way when upside down but will not fit completely. • Check the interface status. Click Interfaces, then the Ethernet tab. Click on the SFP port in question. Determine if it is passing traffic. Consider disabling auto negotiation and setting the speed and duplex manually.
I can’t enable IGMP Snooping, etc.	<ul style="list-style-type: none"> • Some features are unavailable before firmware version 6.48. Contact CIS to perform a firmware upgrade your equipment.

Warranty Information

Custom Integration Solutions™ products have a 2-Year Limited Warranty. This warranty includes parts and labor repairs on all components found to be defective in material or workmanship under normal conditions of use. This warranty shall not apply to products that have been abused, modified, or disassembled. Products to be repaired under this warranty must be returned to Custom Integration Solutions™ or a designated service center with prior notification and an assigned return authorization (RA) number.

Contact Information

Web: www.custom-integration-solutions.com

Phone: Technical Support - (888) 976-3651

Email: activations@custom-integration-solutions.com



The CIS-CRS328-24P is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EC.