

CIS ACWAPR - User Manual



Table of Contents

Welcome to Custom Integration Solutions.....	5
Overview	5
Package Contents.....	5
Power	5
Device Details.....	6
Ports	6
LED Indicators	6
Buttons.....	6
Wall Mounting	7
Ceiling Mount.....	8
Quick Setup	10
Accessing the Web Interface	11
The Status Page.....	12
Setting the Access Point's Identity.....	13
Undo / Redo	14
Show / Hide Passwords.....	14
Rebooting the Device.....	14
Changing the Default Password.....	15
Setting the Time Zone	15

IP Addressing.....	16
The DHCP Client Tab	16
Renewing the IP Address	16
Setting a Static IP Address	18
Managing Access Points with the Wireless Manager	20
Linking CIS Access Points to the Wi-Fi Manager	20
Viewing the Connected Access Points	22
Viewing Connected Devices	22
Changing the SSID of Managed Access Points	23
Changing the Wi-Fi Password of Managed Access Points	23
Configuring Access Points in Standalone Mode.....	25
Setting the Wi-Fi Password for Standalone Access Points.....	27
Enabling the Guest Network on Standalone Access Points	28
To change the password, click the Security Profiles tab in the Wireless menu. Click the Guest security profile and change the password, just like you did for the main network.	29
View Connected Devices.....	29
Setting up the Access Point as a Repeater.....	29
Tools.....	31
UPnP.....	31
Ping	31
IP Scan	32
Wireless Scanner.....	32
Troubleshooting.....	34
Warranty Information.....	36

Contact Information..... 36

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

CIS wireless access points provide a compact and powerful solution to your home and commercial connectivity needs. The CIS-ACWAPR is an indoor only version of our popular CIS-ACWAP. The 360° coverage pattern makes these access points ideal for business and residential applications. Keep your cable runs hidden by routing the Ethernet cables through an access slot in the rear of the access points.

- The CIS-ACWAPR provides high speed connectivity on the 2.4 and 5 GHz bands with support for wireless standards 802.11 a, b, g, n, and ac.

Package Contents



AP



PoE Injector



DC Adapter



Mounting
Brackets



Screw Kit

Power

The CIS-ACWAPR is powered through PoE on Ether1. Use the included PoE injector or connect it to a router or switch that outputs PoE. You can connect an additional passively powered PoE device to Ether2, and the access point will pass PoE power to it. Be aware that the CIS-ACWAPR can consume up to 24W of power when an additional device is connected.

- The CIS-ACWAPR can accept passive PoE (17-57V) or 802.3af/at power and consumes a maximum of 13W by itself.
- The device can consume up to 24W of power with additional devices connected.
- The device outputs passive PoE at the same voltage that it receives. It outputs up to 500mA at 18-30v, and 400mA at 30-57v.

Device Details



Ports

- Ether1 – Gigabit Ethernet port. Power the access point by supplying PoE to it.
- Ether2 – Connect an additional PoE device/AP to this port. The access point will passthrough PoE to it (passive PoE only). The port acts as a switched/bridged port.

LED Indicators



- USR – flashes when the access point is reset.
- 5G – indicates activity on the 5 GHz radio.
- 2G – indicates activity on the 2.4 GHz radio
- E2 – indicates activity on Ether2.
- E1 – indicates activity on Ether1.
- PoE Out – lights when passing through PoE power to Ether2.
- PWR – lit when the device is powered on.

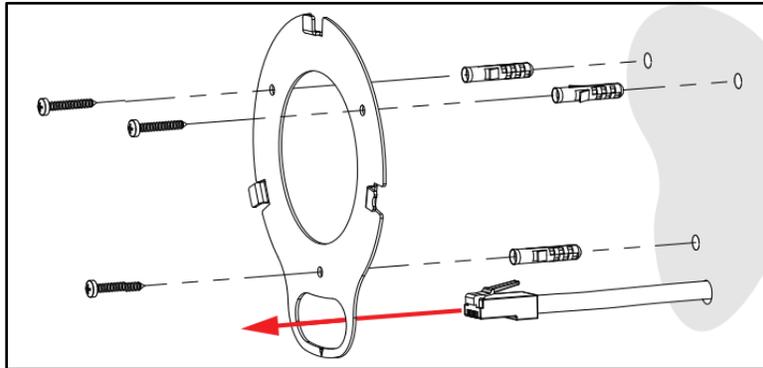
Buttons

Center button: Located on the front of the access point, press the center to enable and disable the LEDs.

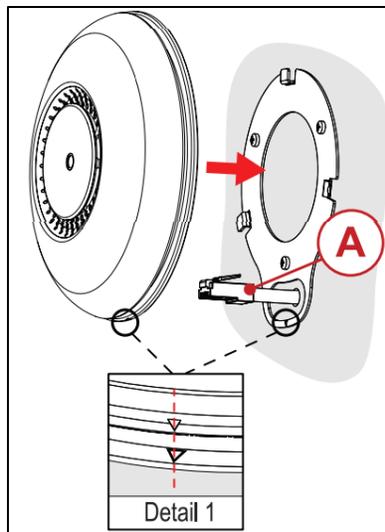
Mode button: Located on the rear of the device, this button also enables and disables the LEDs.

Reset button: This button is located on the rear of the device. 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.

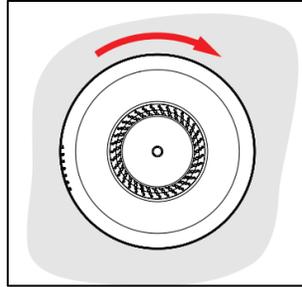
Wall Mounting



1. Drill three holes for the drywall anchors and install them.
2. Drill an additional hole for the Ethernet cable and run it through the bottom of the bracket.

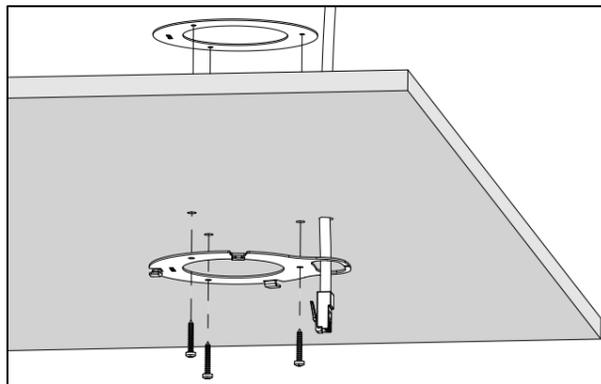


3. Insert the Ethernet cable (A) into Ether1 of the CIS-ACWAPR
4. Mount the access point. Align the marker on the access point to the marker on the bracket.

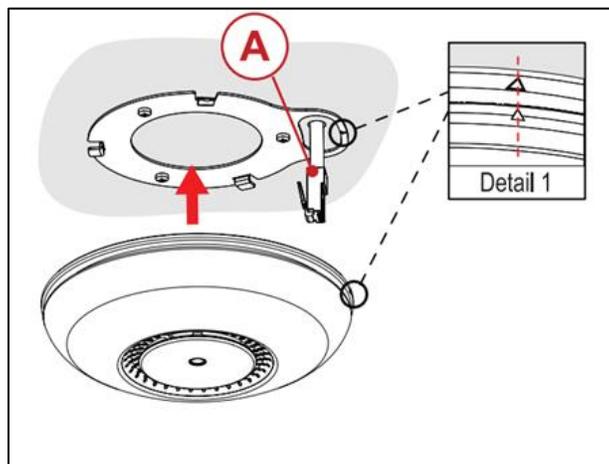


5. Rotate the access point clockwise to secure it.

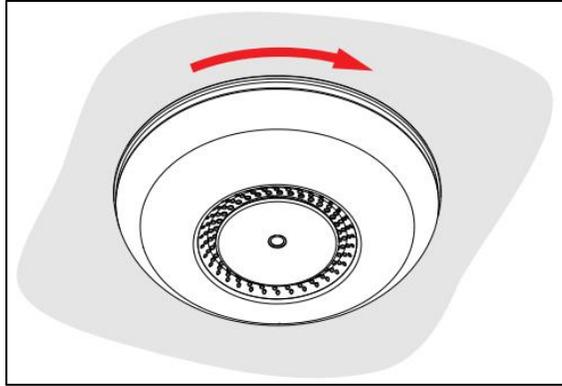
Ceiling Mount



1. Mark and drill three holes for screws, and one for the Ethernet cable.
2. Attach the support bracket on the other side of the ceiling panel and secure it with the screws.



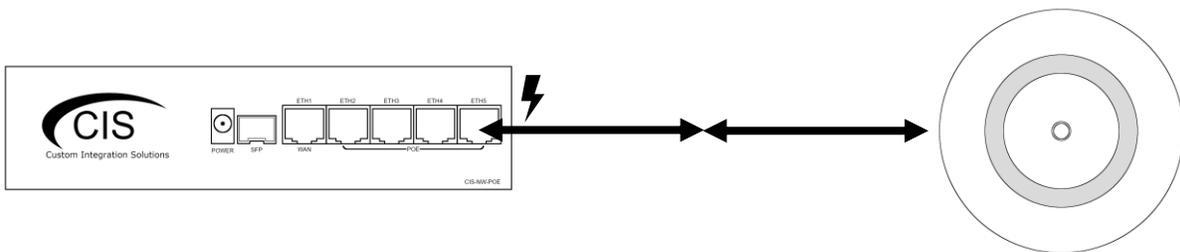
3. Attach the Ethernet cable (A) into Ether1 of the access point.
4. Mount the access point. Align the marker on the access point with the marker on the bracket.



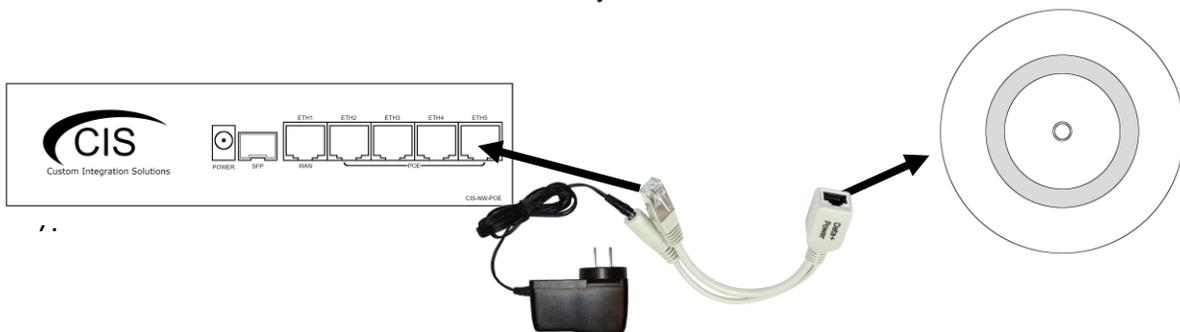
5. Rotate the access point clockwise to secure it in place.

Quick Setup

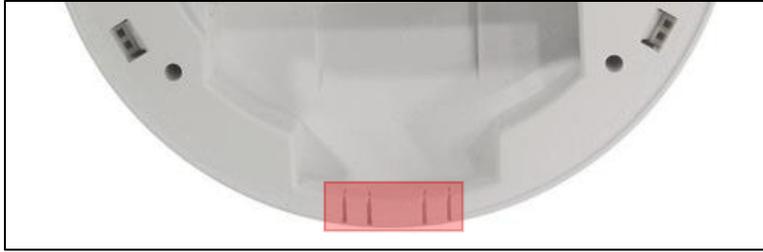
1. Connect the Ethernet cable to the access point and mount it using the instructions on the previous pages.
2. Connect the other end of the Ethernet cable to a router or switch capable of PoE.



3. If a PoE capable router or switch is unavailable, use the included PoE injector.
 - a. Connect the power adapter to the PoE injector.
 - b. Connect the male end of the PoE injector to the router or switch.



4. If necessary, break off the tabs on bottom rear of the access point to route Ethernet cables through.



Accessing the Web Interface

1. Connect your laptop or PC to the router.
2. Obtain the IP address of your access points. If you're using a CIS router, access the web configuration by typing 10.100.1.1 in a web browser (10.100.1.1 is the default, but some systems may be different). Once logged in with the default credentials of **cis** and **integration** as the password, select **IP > DHCP Server** and view the **Leases** tab.

		▲ Address	MAC Address	Active Address	Active MAC Address	Active Host Name	Expires After
-	D	10.100.1.100	64:D1:54:	10.100.1.100	64:D1:54:	CIS-SW-POE4	1d 22:58:20
-	D	10.100.1.101	6C:3B:6B:	10.100.1.101	6C:3B:6B:	CIS-ACWAP	1d 23:59:46

3. Enter the IP address of the access point in the address bar of your web browser.
4. To login, use the default credentials **cis** and **integration** as the password.
5. Integrators may use the Get TeamViewer link if remote assistance is required.

CIS-ACWAP 2.4/5GHz Access Point

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



CIS
Custom Integration Solutions

CIS 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. You can view the identity (name) of the access point you are connected to, view it's public address, the traffic flowing through the device, and identify the MAC addresses of its interfaces.

RouterOS v6.47.7 (stable)
CIS 2.4/5GHz WAP

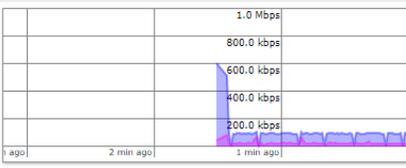
CIS ACWAP 2.4/5GHz Access Point

ISP Public Address	
Public Address	99.1

CIS ACWAP	
Identity	
IP Address	10.100.1.193/24
LAN MAC Address	48:8F:
WLAN MAC Address	48:8F:

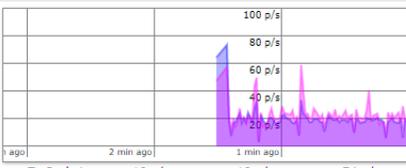
Resources	
CPU Load	0 %
CPU Frequency	716 MHz
CPU Count	4
Rate	1Gbps
Uptime	1d 22:33:49

Byte Graph



— Tx cur: 95.6 kbps avg: 89.9 kbps max: 607.6 kbps
 — Rx cur: 24.2 kbps avg: 23.7 kbps max: 82.2 kbps

Packet Graph



— Tx Packet cur: 18 p/s avg: 18 p/s max: 74 p/s
 — Rx Packet cur: 22 p/s avg: 21 p/s max: 59 p/s

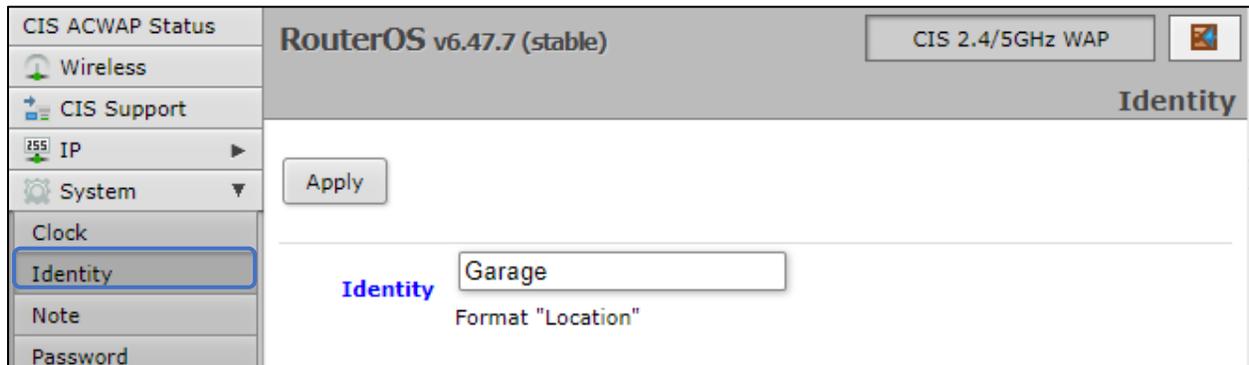
CIS Platinum Support

Support Address 10.255.254.226
 FOR INTEGRATOR PLATINUM SUPPORT PRESENT ACCESS NUMBER

Setting the Access Point's Identity

The identity is used to identify your device on the network. Troubleshooting will become easier when you set the identity correctly. Set the identity of the access point based on its location E.g., Basement.

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



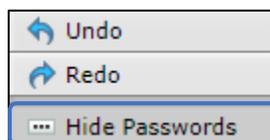
Undo / Redo

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



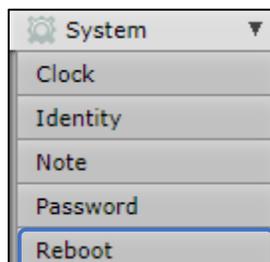
Show / Hide Passwords

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



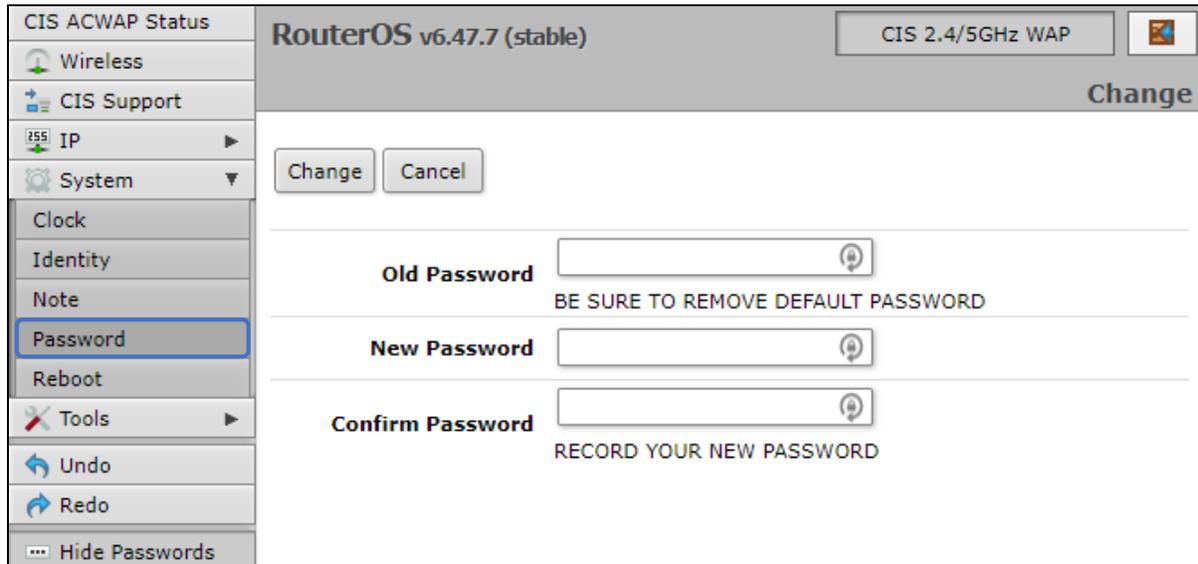
Rebooting the Device

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 ACWAP Status, Wireless, CIS Support, IP, System, Clock, Identity, Note, Password (highlighted), Reboot, Tools, Undo, Redo, and Hide Passwords. The main content area is titled "RouterOS v6.47.7 (stable)" and "CIS 2.4/5GHz WAP". A "Change" button is in the top right corner. Below the title, there are "Change" and "Cancel" buttons. The form contains three password fields: "Old Password" with a hint "BE SURE TO REMOVE DEFAULT PASSWORD", "New Password" with a hint "RECORD YOUR NEW PASSWORD", and "Confirm Password" with a hint "RECORD YOUR NEW PASSWORD". Each field has a password icon on the right side.

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.

CIS ACWAP Status RouterOS v6.47.7 (stable) CIS 2.4/5GHz WAP Clock

Wireless
CIS Support
IP
System
Clock
Identity
Note
Password
Reboot
Tools
Undo
Redo
Hide Passwords

Apply

Time 11:43:18

Date Apr/23/2021

Time Zone Autodetect

Time Zone Name America/Vancouver

IP Addressing

The DHCP Client Tab

The DHCP Client tab will present you with the IP address assigned to your access point from the router. CIS recommends creating a DHCP reservation for access points and other network infrastructure devices.

CIS ACWAP Status RouterOS v6.47.7 (stable) CIS 2.4/5GHz WAP DHCP Client

Wireless
CIS Support
IP
Addresses
DHCP Client
DHCP Server
DNS
Pool
UPnP

1 item

	▲ Interface	IP Address
D	bridge-operations	10.100.1.193/24

Renewing the IP Address

Once you've clicked the entry under the **DHCP Client** option, click the **Renew** button to obtain a new lease.

CIS ACWAP Status

RouterOS v6.47.7 (stable) CIS 2.4/5GHz WAP

Wireless

CIS Support

IP

Addresses

DHCP Client

DHCP Server

DNS

Pool

UPnP

System

Tools

Undo

Redo

Hide Passwords

DHCP Client <bridge-operations>

OK Cancel Apply **Renew**

Status: bound not invalid

Enabled

DHCP

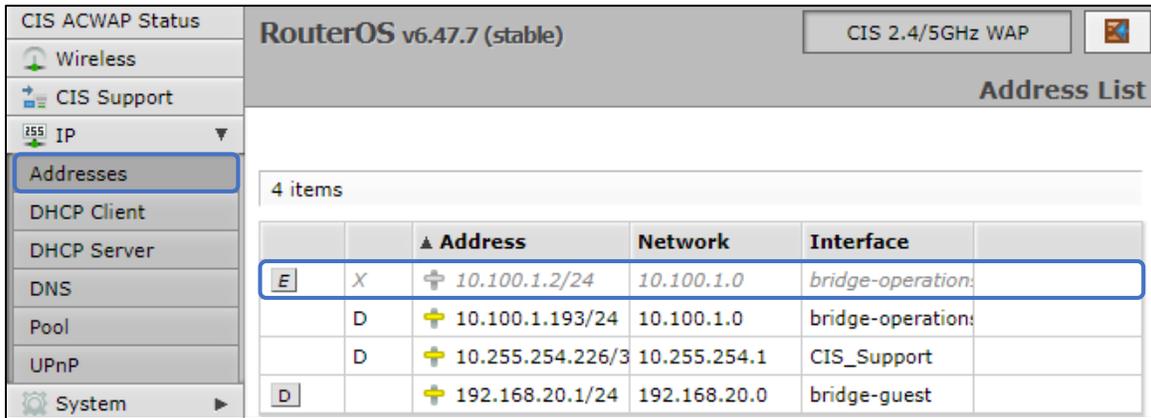
Interface bridge-operations

Status

IP Address 10.100.1.193/24

Setting a Static IP Address

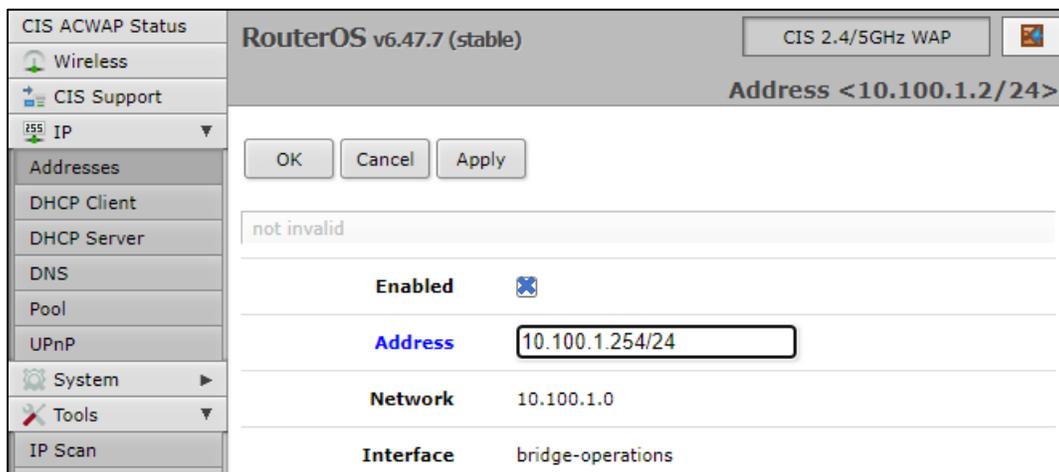
To set a static IP, select the **Addresses** tab under the **IP** section in the toolbar. There is an IP address entry that is disabled by default. Click on it.



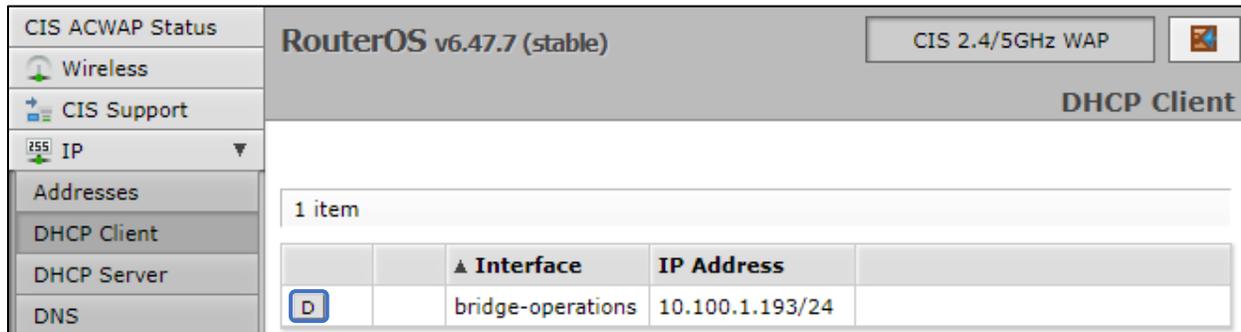
If your network falls in one of the ranges below, you can set the static IP address yourself. If it is outside of these ranges, you must call CIS to have a route created on the access point!

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

Check the **Enabled** box, then enter the IP address you would like to use. It MUST be in the range of your network, and outside of the range of the DHCP pool. The format must include **/24** at the end. This is the subnet mask, which determines how many devices can be connected to this network.



Once the static IP address is set, disable the DHCP client. Go to **IP > DHCP Client** and click on the entry. Click on the small 'D' button to disable it.

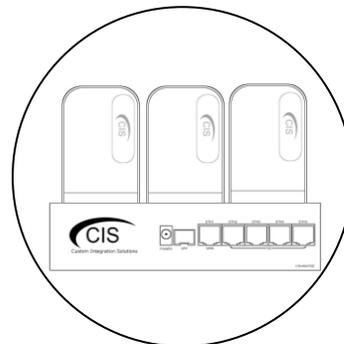


The screenshot shows the RouterOS v6.47.7 (stable) interface. The left sidebar contains a menu with items: CIS ACWAP Status, Wireless, CIS Support, IP (selected), Addresses, DHCP Client, DHCP Server, and DNS. The main content area is titled 'DHCP Client' and shows '1 item' in a list. Below this is a table with the following data:

	▲ Interface	IP Address	
<input type="checkbox"/>	bridge-operations	10.100.1.193/24	

Managing Access Points with the Wireless Manager

All CIS routers include a Wireless Manager that allows you to manage your access points from a single location. All changes to SSIDs, passwords and other options will be propagated to all CIS access points on the network.



Linking CIS Access Points to the Wi-Fi Manager

Select the **Wireless** section in the left toolbar. Under the **WiFi Interfaces** tab, select **Wi-Fi Manager**.

		Name	Type	Actual MTU	Tx
D	S	wlan1-2.4GHz	Wireless (IPQ4019)	1500	0 bps

Check the **Enabled** box, click Apply, then OK.

Enabled

The device will display the message --- managed by CAPsMAN. The Access point is now linked to your CIS router and can be managed through the router's configuration page.

<i>--- managed by CAPsMAN</i>					
E	XS	wlan1-2.4GHz	Wireless (IPQ4019)	1500	0 bps
<i>--- managed by CAPsMAN</i>					
E	XS	wlan2-5GHz	Wireless (IPQ4019)	1500	0 bps

Viewing the Connected Access Points

On your CIS router, select the **Wi-Fi Manager** section in the left toolbar. The active Wi-Fi radios will be displayed.

The screenshot shows the RouterOS v6.47.7 (stable) interface. The left sidebar has 'Wi-Fi Manager' selected. The main area has tabs for 'Interface', 'SSID-Channel', 'WiFi Password', 'Access List', 'WiFi Access Points', and 'Registration Table'. The 'WiFi Access Points' tab is active, showing a table with 1 item:

	▲ Name	Tx	Rx	Tx Packet (p/s)	Rx Packet (p/s)	FP Tx
D	RMB CIS 2.4GHz-RACK	0 bps	0 bps	0	0	0 bps

If you select the **WiFi Access points tab**, you'll be able to view the identity, MAC address and other information of the individual access points.

The screenshot shows the RouterOS v6.47.7 (stable) interface. The left sidebar has 'Wi-Fi Manager' selected. The main area has tabs for 'Interface', 'SSID-Channel', 'WiFi Password', 'Access List', 'WiFi Access Points', and 'Registration Table'. The 'WiFi Access Points' tab is active, showing a table with 1 item:

	▲ Address	Version	Identity	State	Radios
	6C:3B:6B:EA:36:1E	6.47.7	Rack	Run	1

Viewing Connected Devices

Select the **Registration Table** tab to view the connected devices.

The screenshot shows the RouterOS v6.47.7 (stable) interface. The left sidebar has 'Wi-Fi Manager' selected. The main area has tabs for 'Interface', 'SSID-Channel', 'WiFi Password', 'Access List', 'WiFi Access Points', and 'Registration Table'. The 'Registration Table' tab is active, showing a table with 1 item:

	▲ Interface	SSID	MAC Address	Tx Rate	Rx Rate	Tx Signal	Rx Signal	Uptime
-	CIS 2.4GHz-RACK	CIS Guest		52Mbps-20	65Mbps-20	0	-66	00:02:49,24

Changing the SSID of Managed Access Points

Select the **SSID-Channel** tab in the **Wi-Fi Manager** section. Click on the 2.4GHz network.



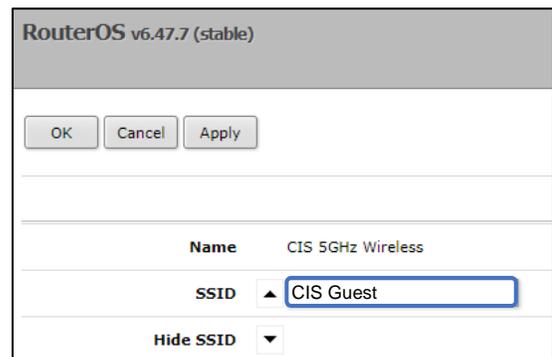
The screenshot shows the RouterOS v6.47.7 (stable) interface. The left sidebar contains navigation options: CIS Router Status, Wi-Fi Manager, Interfaces, IP, System, Tools, Undo, Redo, and Hide Passwords. The main content area is titled "RouterOS v6.47.7 (stable)" and "CIS-NW-POE ROUTER". Below the title are tabs for "Interface", "SSID-Channel", "WiFi Password", "Access List", "WiFi Access Points", and "Registration Table". The "SSID-Channel" tab is selected. It displays a table with 2 items:

	▲ Name	SSID	Hide SSID	Channel
	CIS 2.4GHz Wireless	CIS Guest		2.4GHz Channel 02
	CIS 5GHz Wireless	CIS 5GHz Wireless		5GHz Channel 5180

Enter the name of the SSID in the field. Copy and paste the SSID so that the 5GHz network has the same SSID.



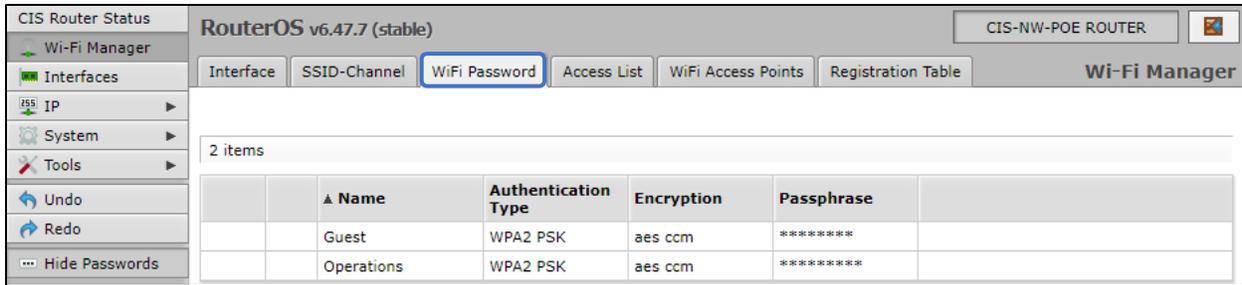
The screenshot shows the RouterOS v6.47.7 (stable) interface for the 2.4GHz network. It features "OK", "Cancel", and "Apply" buttons at the top. Below them, the "Name" field is set to "CIS 2.4GHz Wireless". The "SSID" field is a dropdown menu with "CIS Guest" selected and highlighted with a blue border. The "Hide SSID" field is a dropdown menu with a downward arrow.



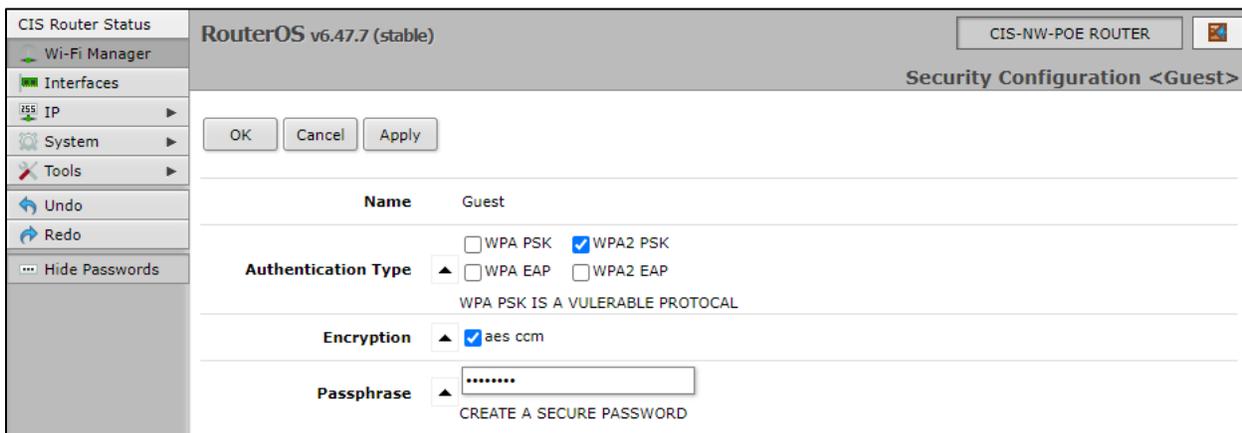
The screenshot shows the RouterOS v6.47.7 (stable) interface for the 5GHz network. It features "OK", "Cancel", and "Apply" buttons at the top. Below them, the "Name" field is set to "CIS 5GHz Wireless". The "SSID" field is a dropdown menu with "CIS Guest" selected and highlighted with a blue border. The "Hide SSID" field is a dropdown menu with a downward arrow.

Changing the Wi-Fi Password of Managed Access Points

Select the **Wi-Fi Password** tab. Click on the network that you'd like to change the password for. If you've purchased a guest network, it will appear here.

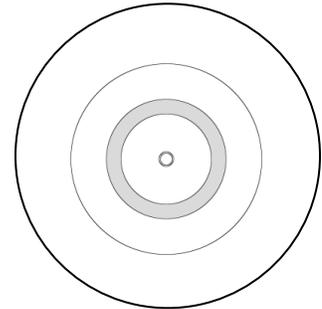


Click on the network you'd like to set the password for, then enter the passphrase in the box below. It is highly recommended you use only **WPA2 PSK** for security purposes. WPA is vulnerable to password cracking.



Configuring Access Points in Standalone Mode

CIS access points can be centrally managed via the Wi-Fi manager on CIS routers, or they can operate as standalone units. This section includes instructions for setting up access points as standalone units.



Setting the SSID

Select the **Wireless** tab from the left toolbar. You can view the networks under the **WiFi** interfaces tab. The 2.4 and 5 GHz bands have their own separate networks you can modify individually. Use the 'E' and 'D' buttons to enable and disable the wireless networks.

The screenshot shows the RouterOS v6.47.7 (stable) interface. The left sidebar has the 'Wireless' tab selected. The main content area shows the 'WiFi Interfaces' tab, with buttons for 'Wi-Fi Manager', 'Setup Repeater', and 'Scanner'. Below these buttons, there is a table with 4 items. The table has columns for Name, Type, Actual MTU, and Tx. The table contains two rows of data:

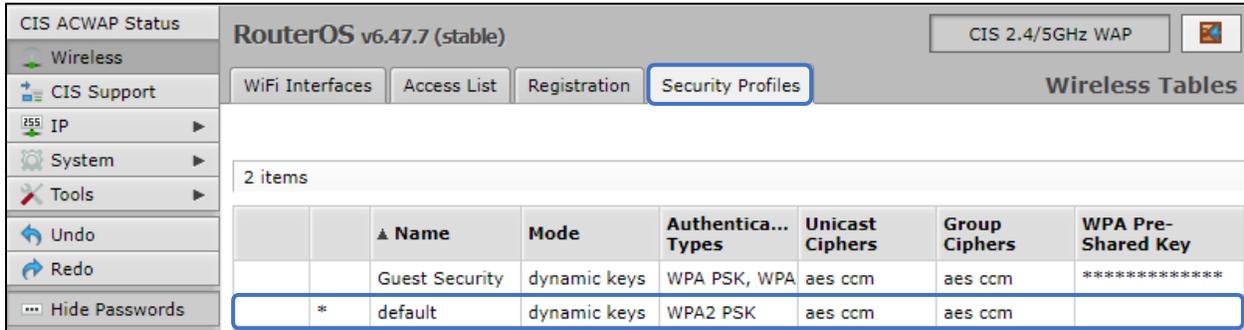
		Name	Type	Actual MTU	Tx
<input type="checkbox"/>	S	wlan1-2.4GHz	Wireless (IPQ4019)	1500	0 bps
<input type="checkbox"/>	S	wlan2-5GHz	Wireless (IPQ4019)	1500	0 bps

Click on one of the networks, then enter your SSID in the **SSID** box. Remember to change it for both the 2.4 GHz network and 5 GHz network! (CIS-ACWAPR only).

Tools ▶ Undo Redo Hide Passwords	running ap not running slave	
	Enabled <input checked="" type="checkbox"/>	
	General	
	Name wlan1-2.4GHz	
	Wireless	
	Band 2GHz-B/G/N ▼	
	Channel Width 20MHz ▼	
	Frequency auto ▼ MHz	
	SSID ▲ CIS AP-AC 2.4	

Setting the Wi-Fi Password for Standalone Access Points

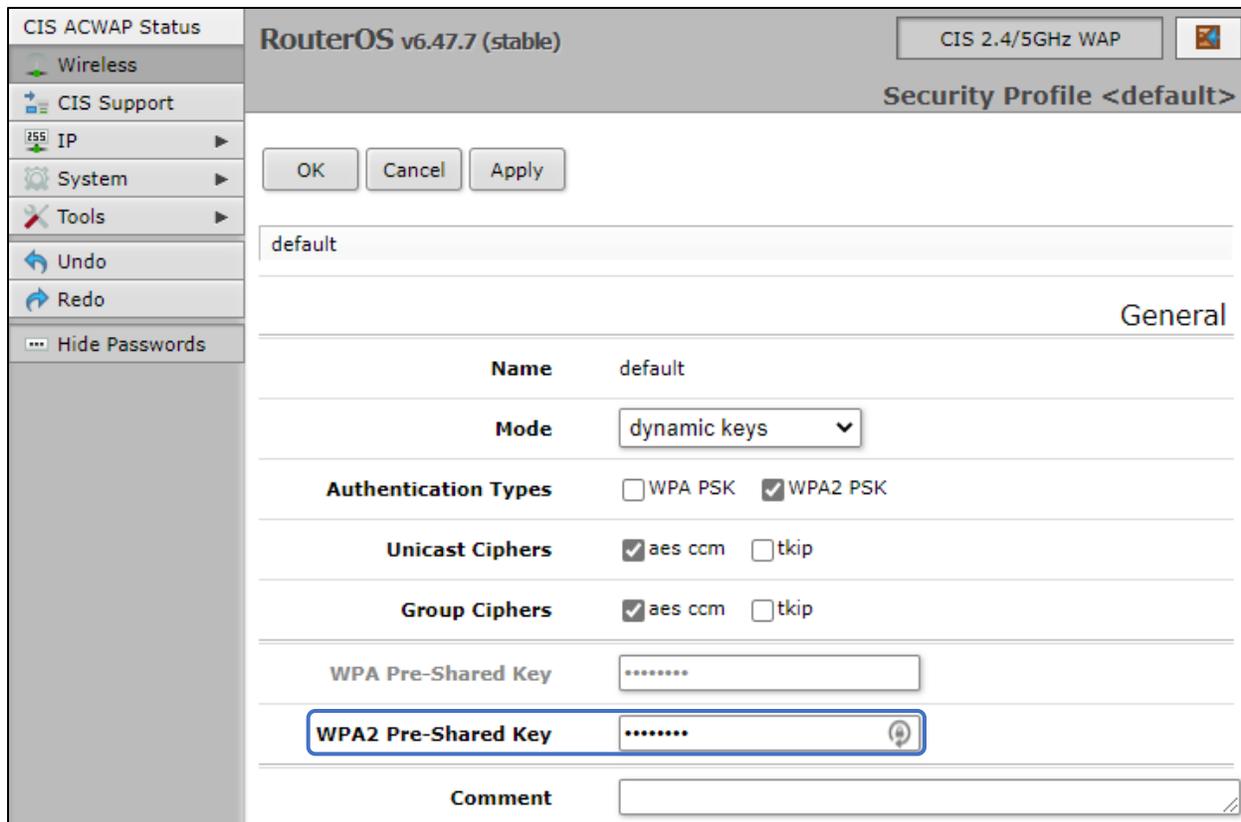
Select the **Security Profiles** tab in the Wireless section. Click on the default network to change the password and security settings.



The screenshot shows the RouterOS v6.47.7 (stable) interface. The 'Security Profiles' tab is selected. The table below shows the configuration for two security profiles:

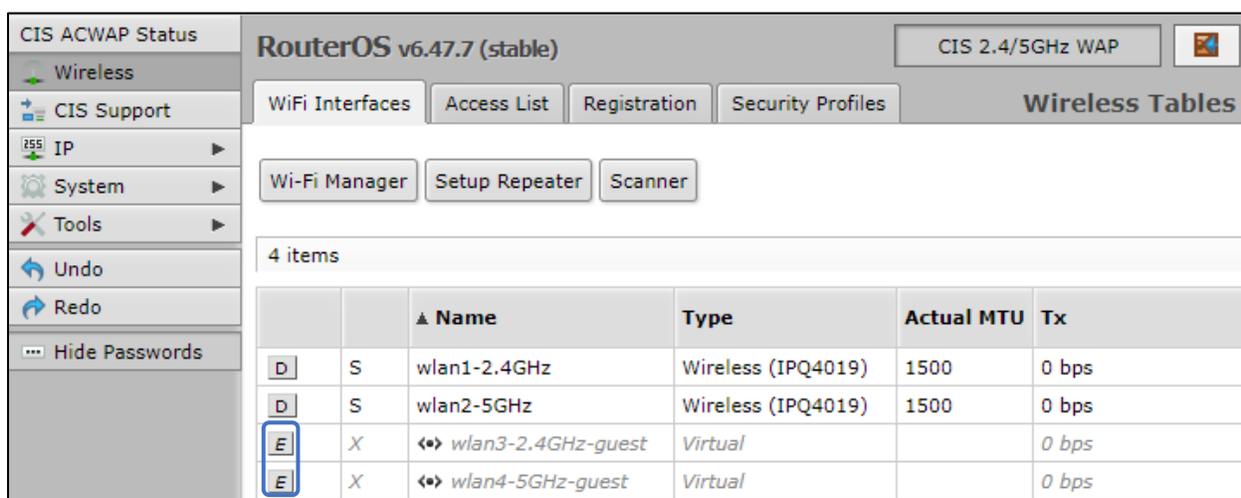
	Name	Mode	Authentica... Types	Unicast Ciphers	Group Ciphers	WPA Pre-Shared Key
	Guest Security	dynamic keys	WPA PSK, WPA	aes ccm	aes ccm	*****
	* default	dynamic keys	WPA2 PSK	aes ccm	aes ccm	

Enter the password in the **WPA2 Pre-Shared Key** field. CIS recommends you leave WPA PSK disabled, as it is a vulnerable protocol. If you have legacy devices that require it, enable it, and copy and paste the password into the WPA Pre-Shared Key field.



Enabling the Guest Network on Standalone Access Points

CIS access points running in standalone mode can run a simple guest network. To enable, click the **E** button in the **WiFi Interfaces** tab of the **Wireless** section. Enable both the 2.4 and 5 GHz networks (CIS-ACWAPR only).



Devices in the guest network will receive different IP addresses and will be isolated from clients on the

main network. Change the SSID by clicking on the virtual network.

Enabled

General

Name wlan3-2.4GHz-guest

Type Virtual

Wireless

Secondary Channel ▼

SSID ▲ CIS AP-AC Guest 2.4

Master Interface wlan1-2.4GHz

Security Profile Guest Security

To change the password, click the **Security Profiles** tab in the Wireless menu. Click the **Guest security profile** and change the password, just like you did for the main network.

View Connected Devices

In the **Wireless** section, click the **Registration** tab to view the connected devices. You can identify them based on their MAC address. You can view the uptime, signal strength, traffic flow, and more.

CIS ACWAP Status RouterOS v6.47.7 (stable) CIS 2.4/5GHz WAP

Wireless WiFi Interfaces Access List **Registration** Security Profiles Wireless Tables

1 item

▲ Radio Name	MAC Address	Interface	Uptime	AP	W...	Last Activity (s)	Tx/Rx Signal Strength (dBm)	Tx Rate	Rx Rate
wlan2-5GHz	C6:D7:41	wlan2-5GHz	00:00:49	no	no	11.310	-67	9Mbps	390Mbps-80MHz/

Setting up the Access Point as a Repeater

In the **Wireless** section, select the **WiFi Interfaces** tab. Click on **Setup Repeater**.

CIS ACWAP Status RouterOS v6.47.7 (stable) CIS 2.4/5GHz WAP

Wireless
CIS Support
IP
System
Tools
Undo
Redo
Hide Passwords

WiFi Interfaces Access List Registration Security Profiles **Wireless Tables**

Wi-Fi Manager **Setup Repeater** Scanner

4 items

		Name	Type	Actual MTU	Tx	Rx	Tx Packet (p/s)
D	S	wlan1-2.4GHz	Wireless (IPQ4019)	1500	0 bps	0 bps	0
D	RS	wlan2-5GHz	Wireless (IPQ4019)	1500	904 bps	0 bps	2
E	X	↔ wlan3-2.4GHz-guest	Virtual		0 bps	0 bps	0
E	X	↔ wlan4-5GHz-guest	Virtual		0 bps	0 bps	0

Display the SSID field by clicking the down arrow next to it. Type the SSID and Passphrase of the wireless network you wish to extend the range of. Click **Start**.

Note: You can only run a repeater on one band at a time. The 2.4 GHz band will offer better range.

IP
System
Tools
Undo
Redo
Hide Passwords

Start Stop Close

Interface wlan2-5GHz

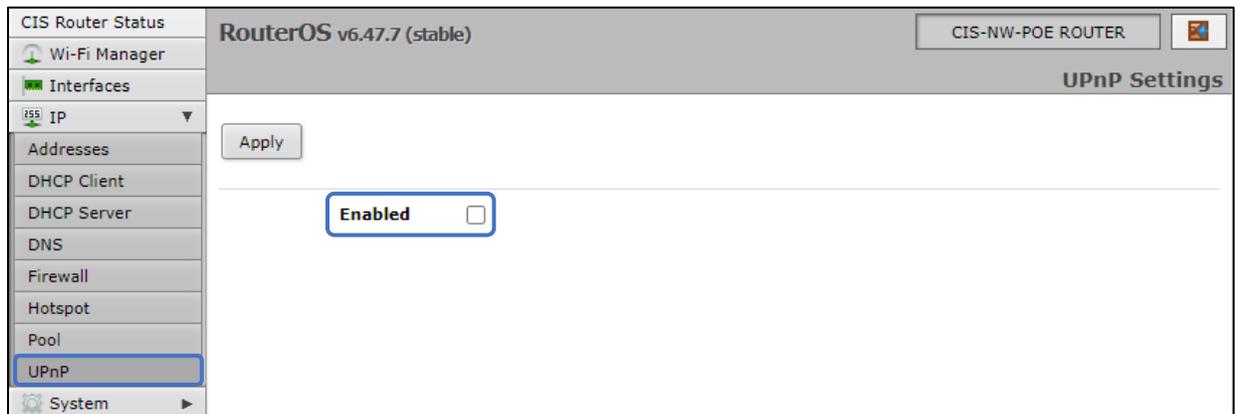
SSID ▲ CIS Guest

Passphrase

Tools

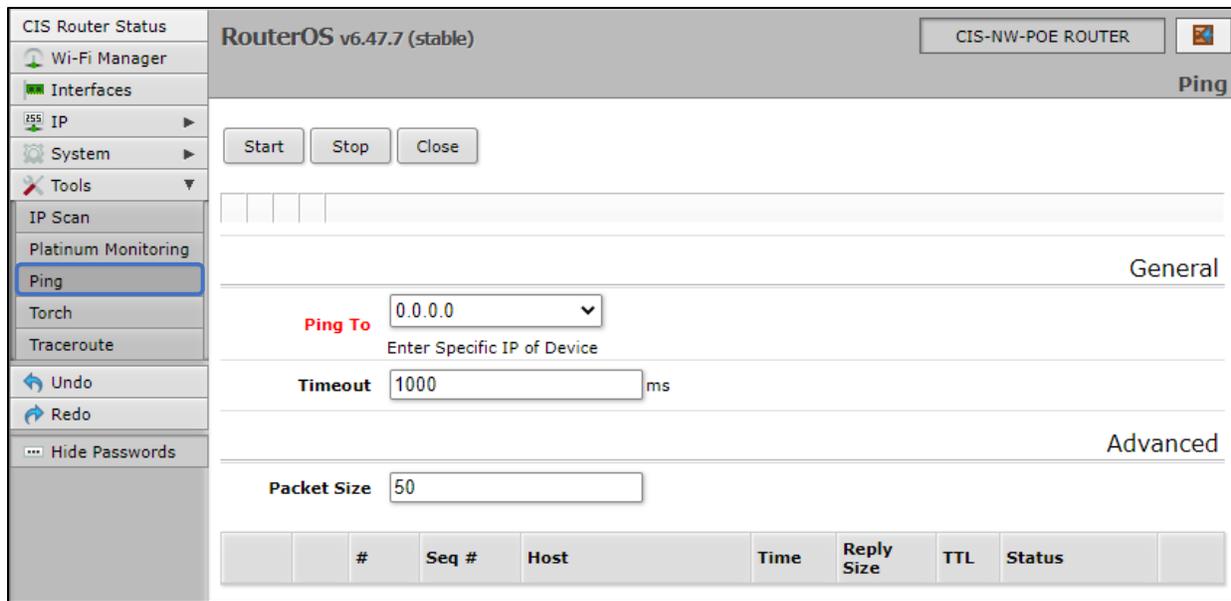
UPnP

Universal Plug and Play enables the discovery 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

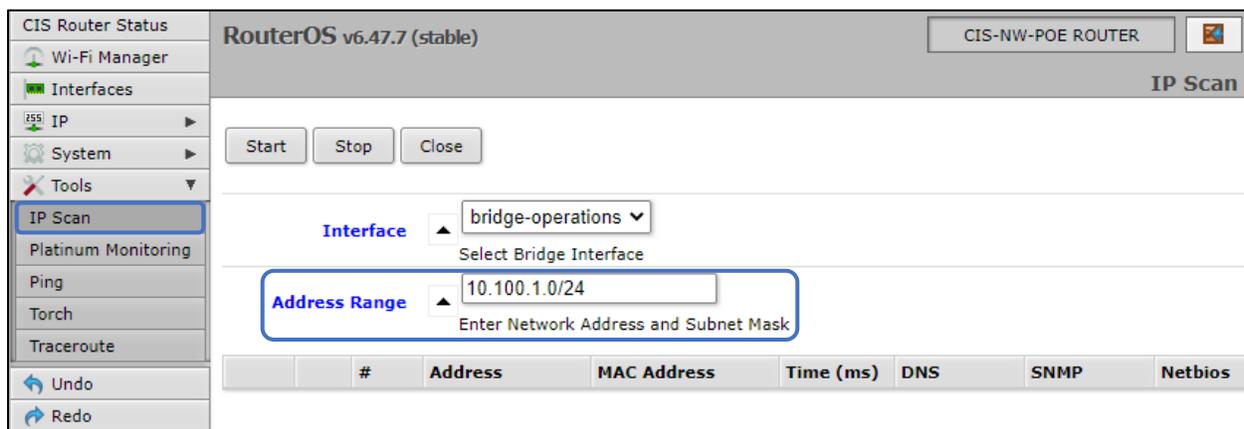
Ping uses Internet Control Message Protocol (ICMP) echo messages to determine if a remote host is active. It will also provide the round-trip time between the hosts. Enter the IP address of the device and select Start to begin.



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 your access point.

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.



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.

Wireless Scanner

You can use the access point to scan for other wireless networks in the area. This is immensely helpful if you need to discover networks that may be interfering with your wireless performance.

Note: You must disable the Wi-Fi manager on the access point prior to using this tool!

From the **Wireless** section, click on the **Scanner** button. Select the interface to use and click **Start**.



Troubleshooting

Symptom	Possible causes
The devices are having trouble maintaining a connection to the wireless network.	<ul style="list-style-type: none"> • Check the signal strength in the registration table. A healthy signal range is between -30 and -75 dB. • Avoid using the 2.4 GHz network when possible, as it is more prone to interference. Use the Scanner tool to detect interfering networks if necessary. • Try changing the channel of the access points. You can do this in the Wi-Fi manager by clicking on the Interface tab, then choose an access point radio. Click the down arrow to show the channel box.
The device won't connect to the wireless network at all.	<ul style="list-style-type: none"> • Ensure the device is in range of the access point. • Temporarily disable all access points except the one closest to the device. Some devices have issues with multiple access points with the same SSID. <ul style="list-style-type: none"> • If this is the case, contact CIS and we will make a separate SSID for these devices that is only broadcast on one access point. • 802.11b is disabled by default. If you have devices that require 802.11b you can enable it in the Wi-Fi manager or contact CIS for assistance. • Ensure that the passphrase is correct.
I am not receiving the speed that I am expecting.	<ul style="list-style-type: none"> • The CIS-ACWAPR has been tested to achieve maximum speeds of approximately 340 mbps in our testing under ideal circumstances. • The vast majority of access points and client devices will not provide or support the full throughput of a 1 Gbps internet connection. • Test the speed of your device when it is plugged into the wired network if possible. Compare the results.

<p>The speed is particularly slow.</p>	<ul style="list-style-type: none"> • Ensure there is adequate coverage throughout the building. • We recommend one access point for every 1000 sq ft for adequate 5 GHz coverage. • The placement of the access point can have a significant impact on performance as well as the nearby materials. The following materials can cause issues with reflecting or absorbing radio frequencies: <table border="1" data-bbox="824 596 1416 1003"> <thead> <tr> <th>Type of Barrier</th> <th>Interference Potential</th> </tr> </thead> <tbody> <tr> <td>Wood</td> <td>Low</td> </tr> <tr> <td>Synthetic material</td> <td>Low</td> </tr> <tr> <td>Glass</td> <td>Low</td> </tr> <tr> <td>Water</td> <td>Medium</td> </tr> <tr> <td>Bricks</td> <td>Medium</td> </tr> <tr> <td>Marble</td> <td>Medium</td> </tr> <tr> <td>Plaster</td> <td>High</td> </tr> <tr> <td>Concrete</td> <td>High</td> </tr> <tr> <td>Bulletproof glass</td> <td>High</td> </tr> <tr> <td>Metal</td> <td>Very high</td> </tr> </tbody> </table> <p>The following are sources of interference that can affect Wi-Fi performance:</p> <ul style="list-style-type: none"> • Microwave ovens. • Power sources – breaker boxes, etc. • Cordless home phones. • Wireless video transmitters. • Wireless speakers. • Poorly shielded cabling. 	Type of Barrier	Interference Potential	Wood	Low	Synthetic material	Low	Glass	Low	Water	Medium	Bricks	Medium	Marble	Medium	Plaster	High	Concrete	High	Bulletproof glass	High	Metal	Very high
Type of Barrier	Interference Potential																						
Wood	Low																						
Synthetic material	Low																						
Glass	Low																						
Water	Medium																						
Bricks	Medium																						
Marble	Medium																						
Plaster	High																						
Concrete	High																						
Bulletproof glass	High																						
Metal	Very high																						
<p>The access point will not turn on.</p>	<ul style="list-style-type: none"> • If using the PoE injector, ensure the data end is connected to the router or switch and the power end to the access point. • If not using the PoE injector, ensure the router or switch is capable of providing PoE. Some devices only support PoE on specific ports. • Faulty cabling or bad terminations can cause issues with PoE. Try plugging the access point directly into the PoE router or switch with a short cable. • CIS routers and switches may have issues detecting PoE devices over long cable lengths. Set the PoE mode to “forced on”. Review the user manuals for instructions. 																						

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



CIS Access Points are in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EC.