CIS-CCR2004 User Manual

Table of Contents

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

The CIS-CCR2004 boasts many upgrades over its predecessor – the CIS-CCR1009. The CPU has been upgraded to a quad-core ARM processor at 1.7 GHz that produces significantly better single-core performance. The RAM has been doubled to 4GB.

The CIS-CCR2004 router is now equipped with 16 Gigabit Ethernet ports and two SFP+ ports – compatible with 1 GB or 10GB SFP modules.

Package Contents

Router

Power Cable (2)

Rack ears (2)

Screws (8)

Power

The CIS-CCR2004 is powered using the supplied IEC power cables. The dual power supplies are removeable and can be replaced should a failure occur. Connect one for standard operation or connect two of them to make use of the redundant power supplies. Connect a cable to a separate circuit, or UPS to maximize uptime.

The device consumes 35 W without any attachments, and up to a maximum of 48 W.

Device Details

Ports

- 16 Gigabit Ethernet ports.
- 2 SFP+ cages.
- Dual power input.
- Console port – disabled.
- USB – disabled, but may provide future functionality, such as LTE modems.

LED Indicators

- USER – An LED that can be customized by CIS. Default is off.
- FAULT – Indicates a failure with the device or its cooling system.
- PWR 1 & 2 – Indicates whether one or both power supplies are connected to power.
- Ethernet LED – Indicates network activity on the Ethernet ports and link speed.
- SFP LEDs – ACT displays network activity. 10G is illuminated should a 10G link be established.

Buttons

Reset button: If you would like to reset the router, it is highly recommended you contact CIS. Resetting your CIS router will remove all custom configuration, including services you may have paid for.

Quick Setup

1. Connect a power cable to one or both power supplies on the back of the router.

2. Connect the ISP's modem to the first port on the front of the router with an Ethernet cable.

3. Connect your remaining devices to the Ethernet ports.

4. (Optional) Use the SFP+ port to connect to a switch.

Accessing the Web Interface

1. Connect the ISP's modem to the first Ethernet port. Connect your laptop to any remaining port on the front of the CIS router (excluding the console port). Ensure your computer is set to DHCP mode.

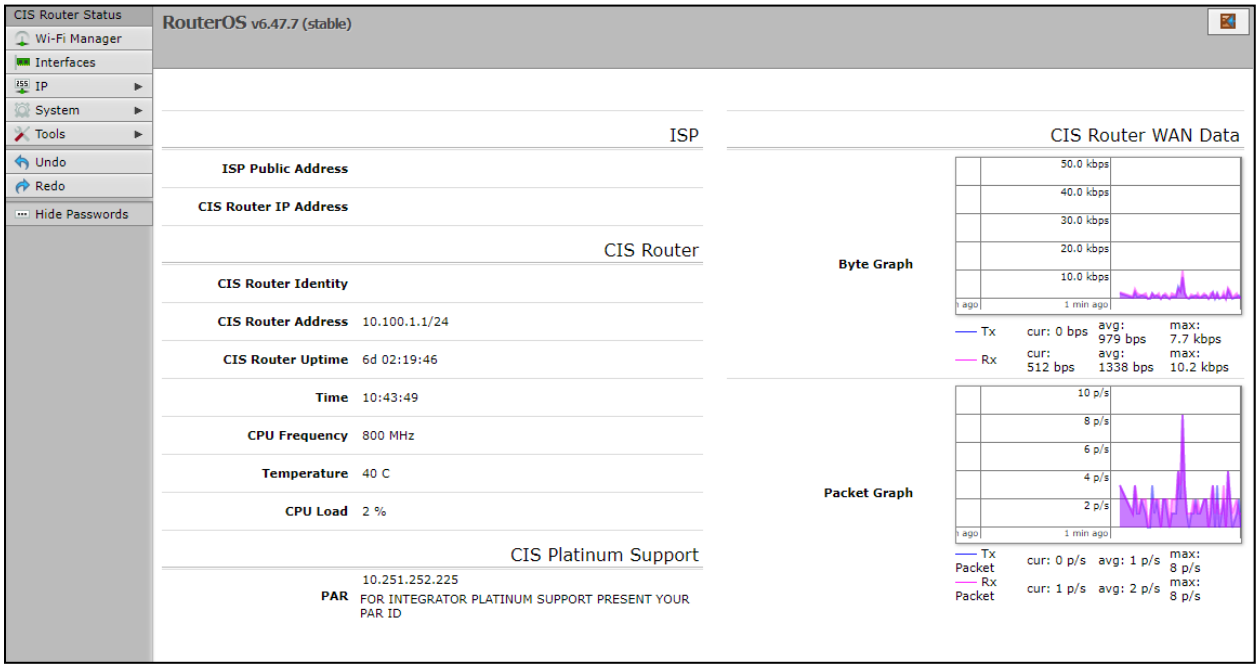
2. In a web browser, navigate to **10.100.1.1** (the default IP address). If you have requested a different network address, enter it or open a command window and use the **ipconfig** command to get the default gateway. Enter this value in the browser.

3. To login, enter the username **cis** and password **integration**.

4. Integrators may use the Get TeamViewer link if remote assistance is required.

The Status Page

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



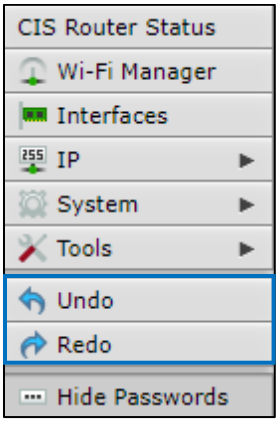
Setting the Router's Identity

The identity is used to identify your device on the network. It is essential to set the router to the name of the client using the format below, as CIS will use it to identify the router when connecting for updates and troubleshooting.

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

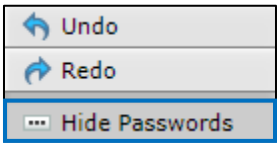
Undo / Redo

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



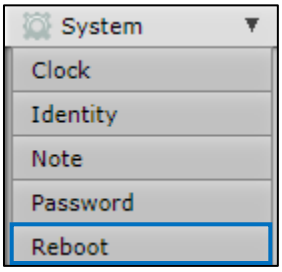
Show / Hide Passwords

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



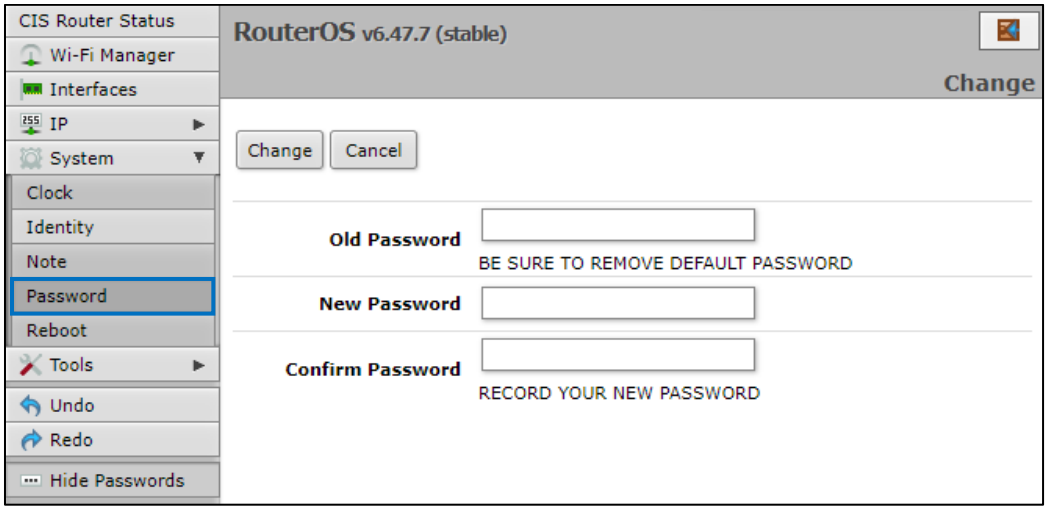
Rebooting the Device

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.



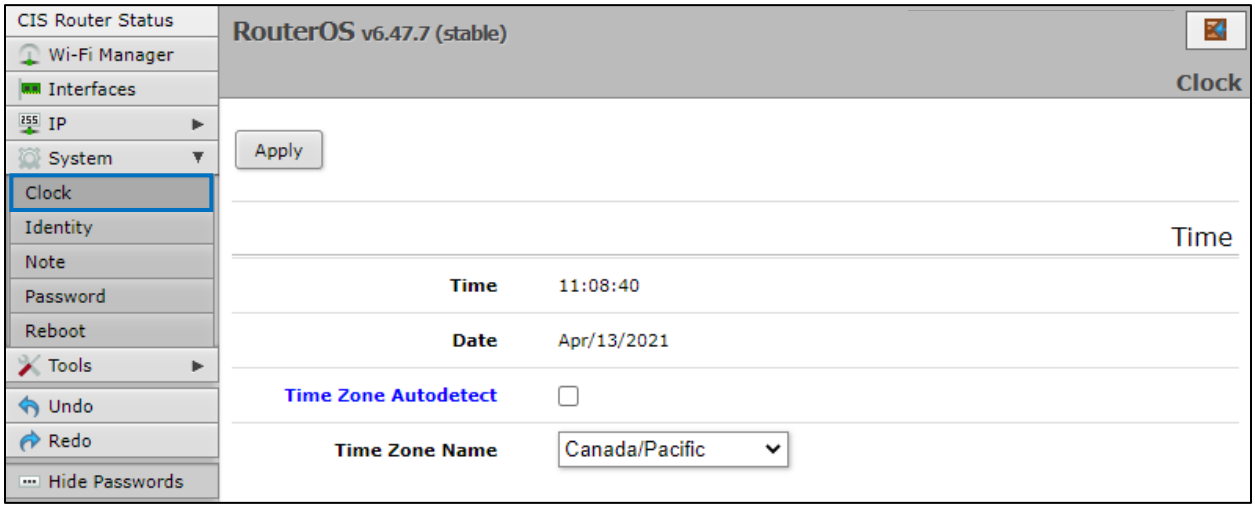
Changing the Default Password

After you log in for the first time, please create a new a 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.



Setting the Time Zone

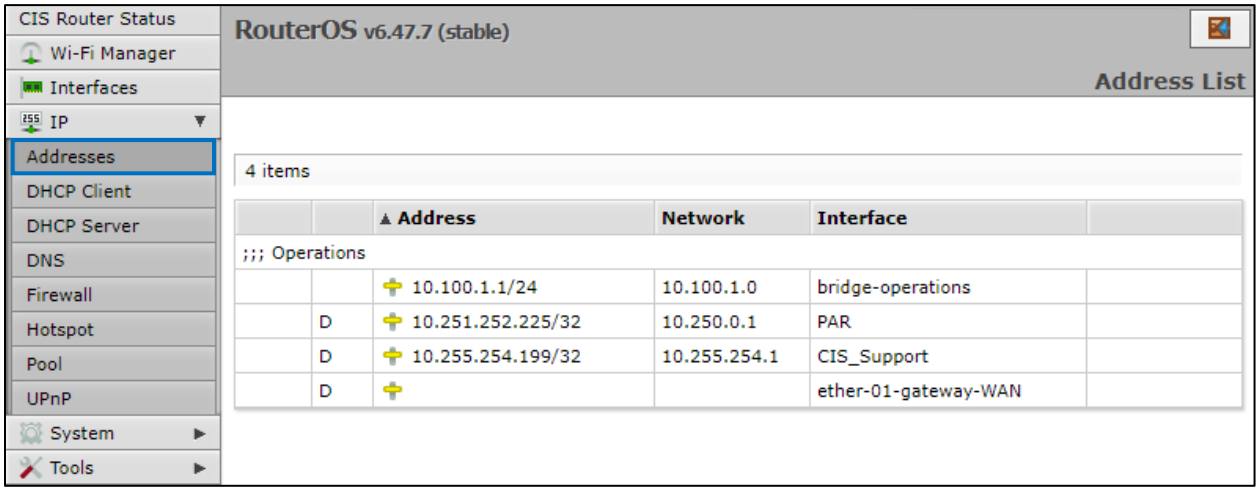
You can find the Clock settings under the System tab in the left toolbar. Select your time zone from the drop-down menu.



IP Addressing

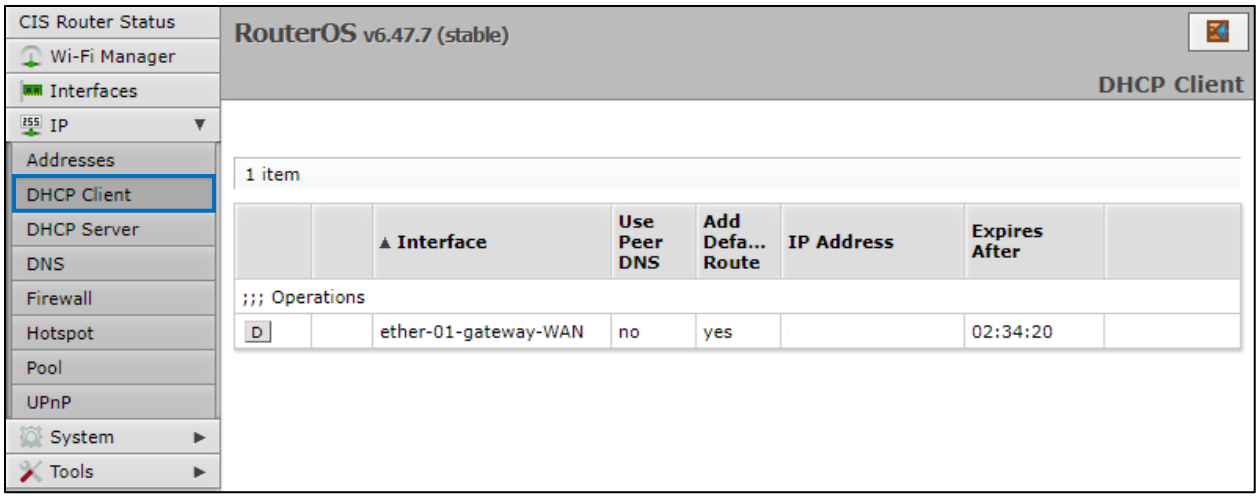
View the Router's IP Addresses

To view the IP addresses assigned to the router, choose the **Addresses** tab in the **IP** section in the left toolbar. You can see the WAN address on ***ether-01-gateway-WAN***, the LAN address assigned to ***bridge-operations***, and either a CIS support address or a PAR address.



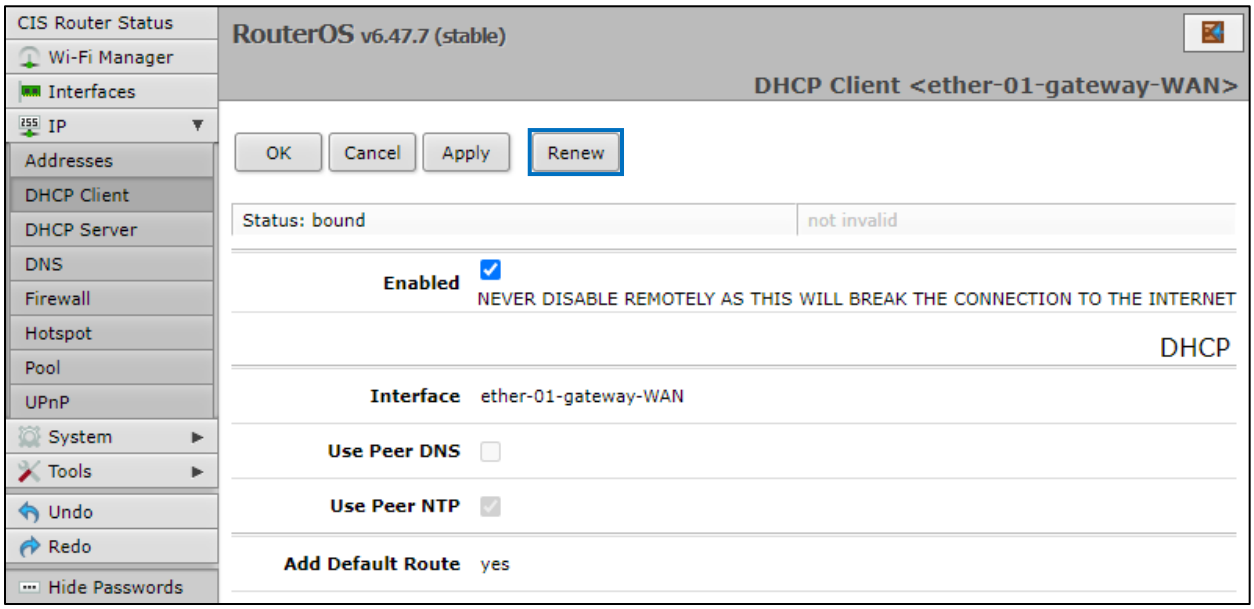
The DHCP Client Tab

The DHCP Client tab will present you with the IP address assigned to your router from the ISP's modem. Click on the entry to see the addresses and DNS servers assigned to your router from the ISP.



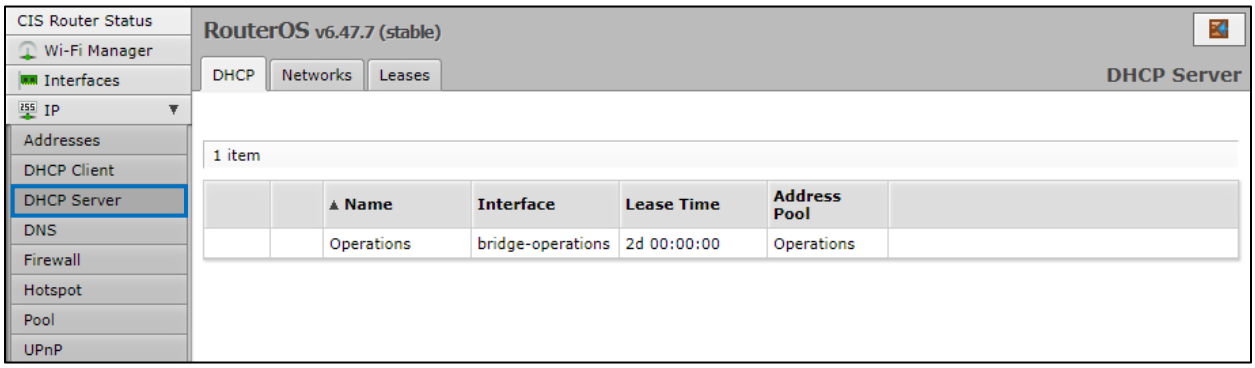
Renewing the WAN IP Address

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

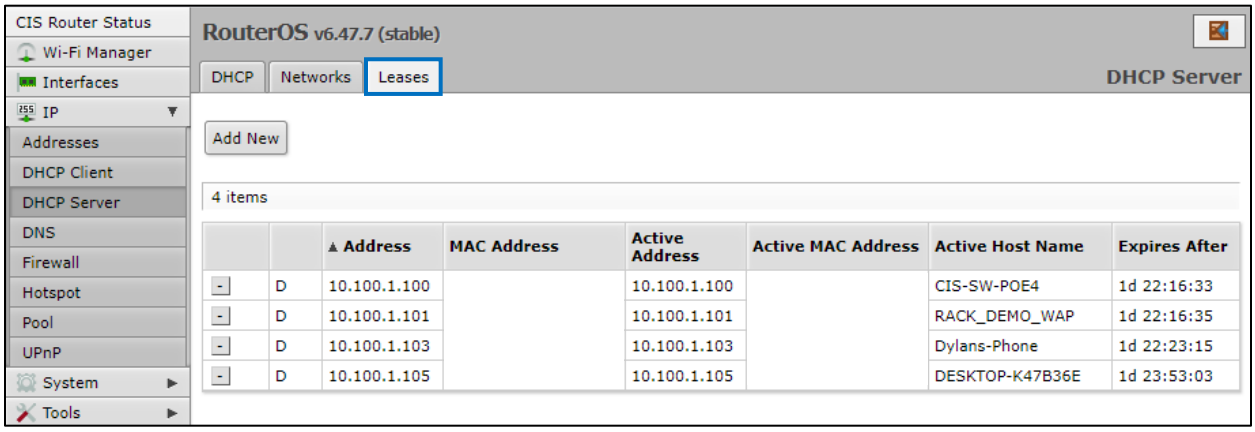


The DHCP Server

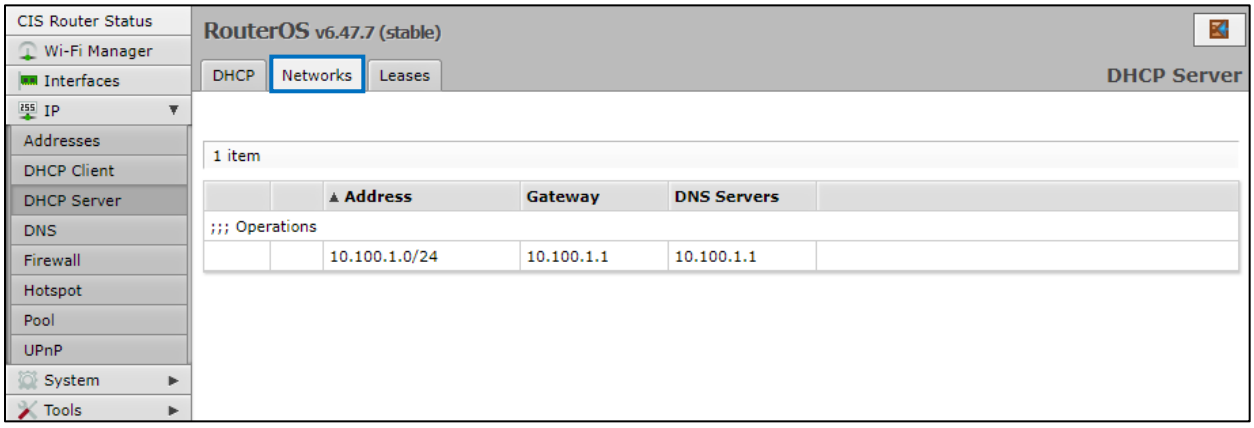
The main page displays the lease time for the DHCP server.



The **Leases** tab displays the IP and MAC addresses of connected devices.



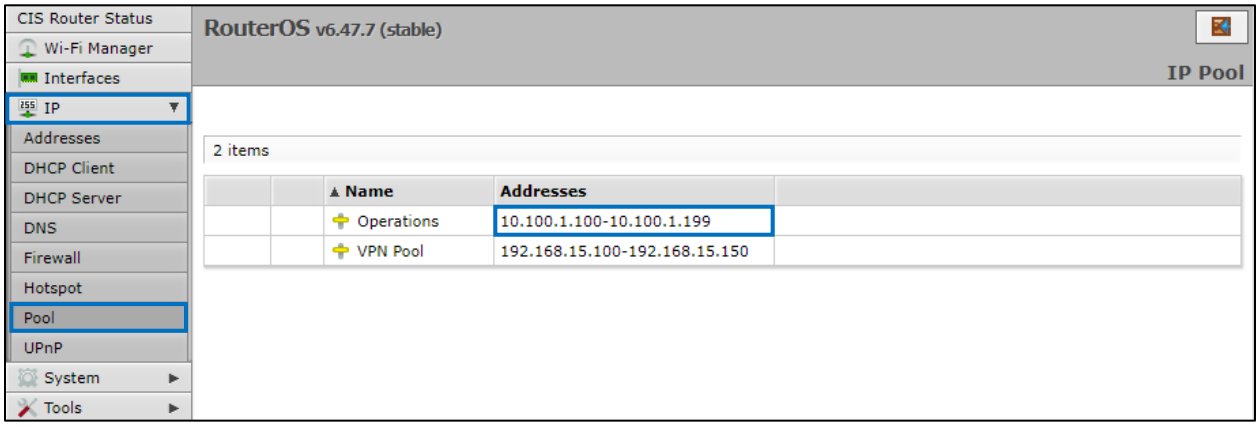
The **Networks** tab displays the gateway and DNS server IP addresses that the connected devices will receive.



Setting a DHCP Reservation

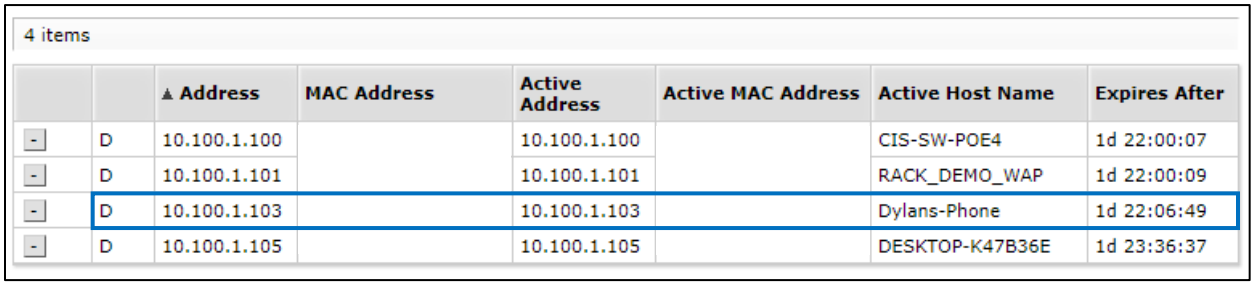
It is highly recommended that static DHCP reservations are created for important networking devices such as switches, access points, automation controllers, NVRs, printers, etc.

1. Before assigning a static IP address, select **IP** > **Pool** from the toolbar. Do not assign any addresses inside of the DHCP pool range. In addition, it is recommended you perform an **IP Scan** to ensure the IP address you wish to assign is unused. See the **Tools** section for more info.

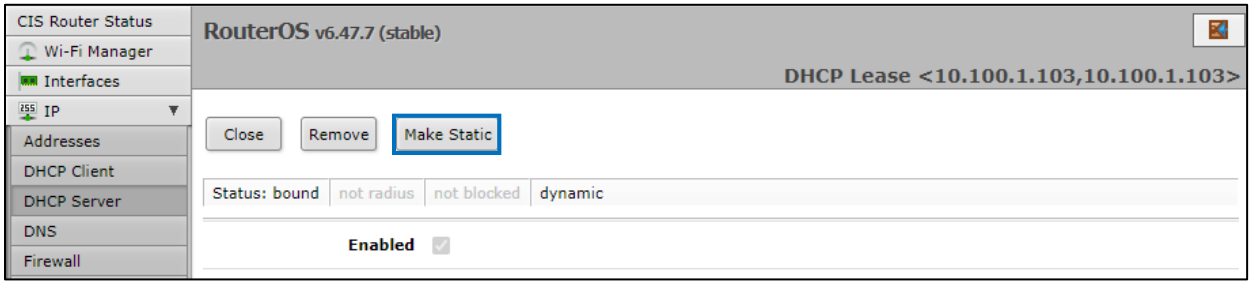


*View the **Operations** pool. You should not reserve addresses between 10.100.1.100 and 10.100.1.199 on this device.*

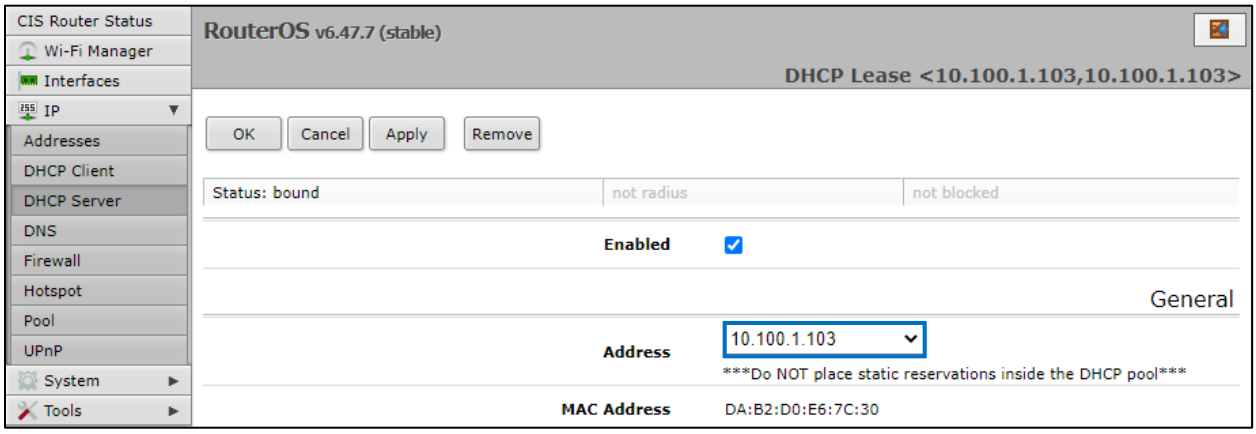
2. Click anywhere on the table entry for the device you wish to create a reservation.



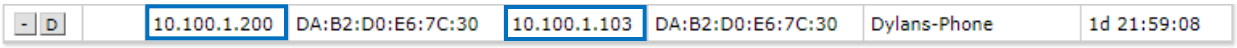
3. Click the **Make Static** button near the top.



4. Select **close**, then click on the same entry in the leases table. You can now edit the IP address.



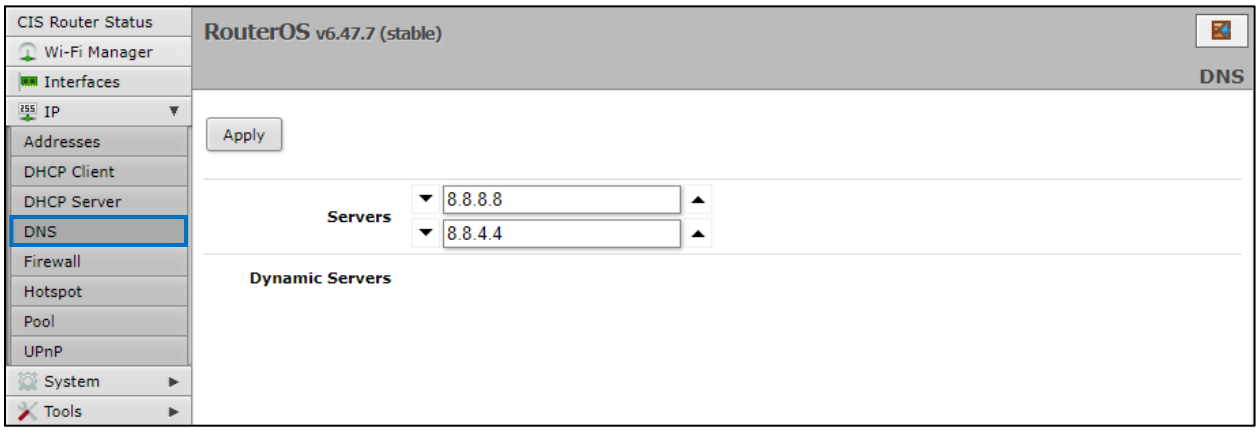
5. Once assigned you will need to renew the lease on the device, disconnect and reconnect it to the network, or reboot it for the new IP address to take effect.



The active IP address will not change until the device requests a new lease.

Changing the DNS Servers

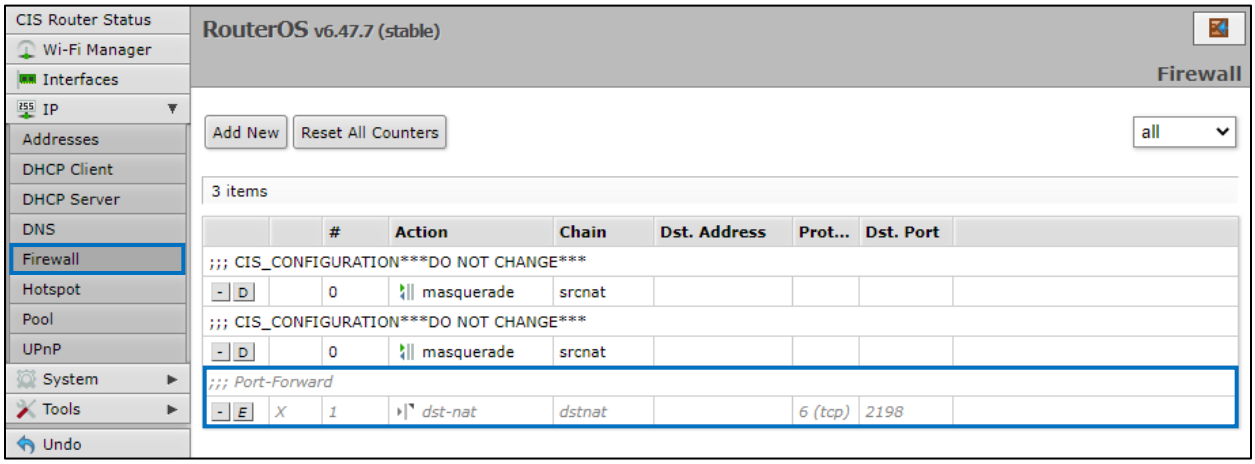
In the **IP** section in the left toolbar, select the **DNS** tab. CIS Routers now use Google DNS by default (8.8.8.8 and 8.8.4.4). To add another server, click the down arrows, and a box will appear below the arrow you have clicked on. To remove a server, click the up arrow next to the box.



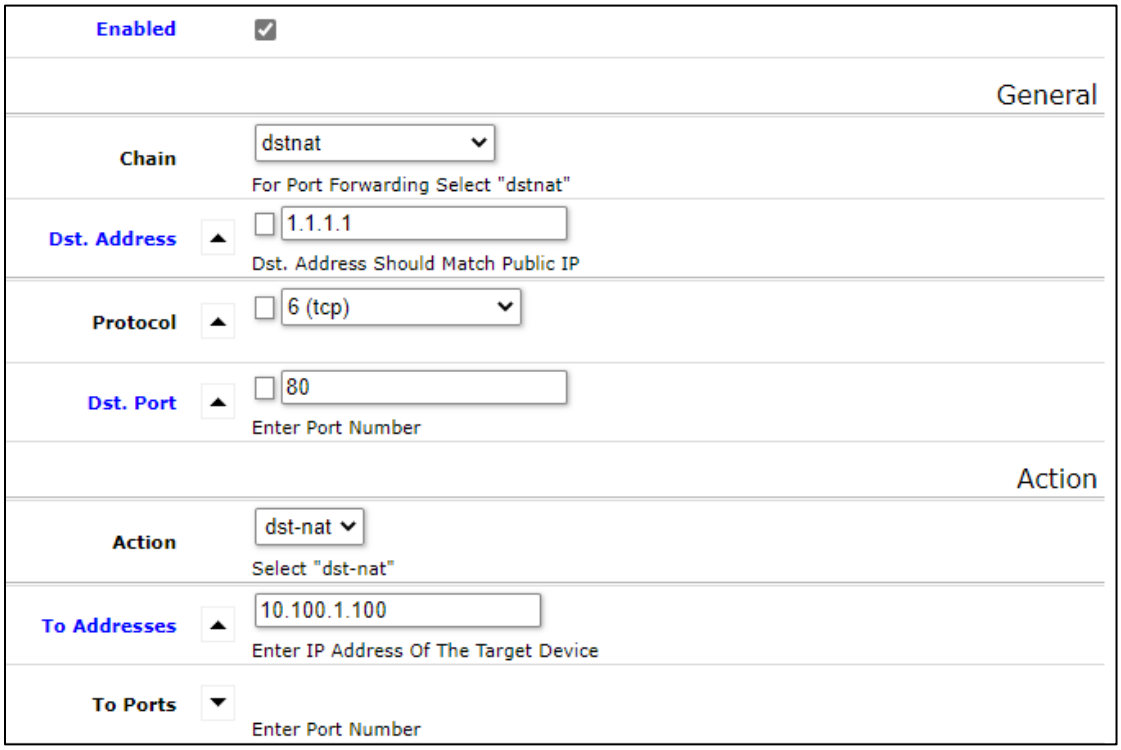
Port Forwarding

Port forwarding allows inbound traffic to a specific port on a desired host. Be careful when using port forwarding, as each port you open may leave the host vulnerable to attack! CIS recommends using a VPN connection instead whenever possible.

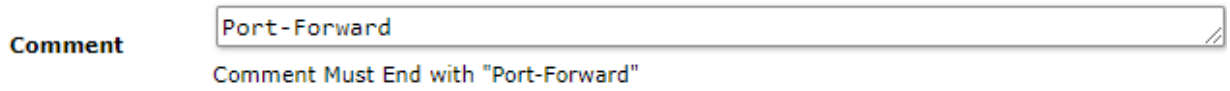
By default, there is a port forwarding rule to use as a template. Select the **Firewall** section in the left tool bar. Click on the **Port-Forward** entry.



Do NOT modify the CIS_CONFIGURATION rules or you may lose internet access!



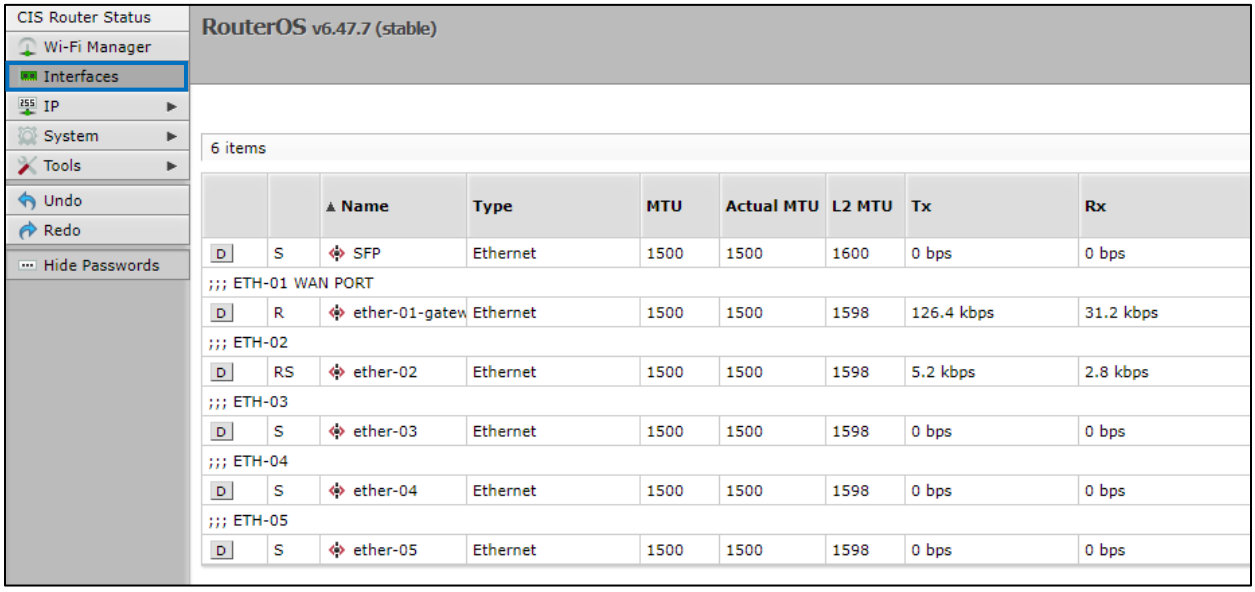
Enabled	Check this box to activate the rule.
Chain	Set to **dstnat**
Dst. Address	The Dst. Address is your public IP address. It will be automatically updated.
Protocol	Select TCP or UDP based on which port you need to open.
Dst. Port	Enter the port(s) to open. You can enter a range (e.g., 5000-6000) or separate multiple ports with commas (e.g., 80, 443, 3389).
Action	Set to **dst-nat**.
To Addresses	Enter the IP address of the device on your network.
To ports	Optional. If you wish for the traffic to be forwarded to a different port on the device, enter it here.
Comment	The comment must be set to **Port-Forward** or the rule will not work!



The comment must end with "Port-Forward" for the rule to work!

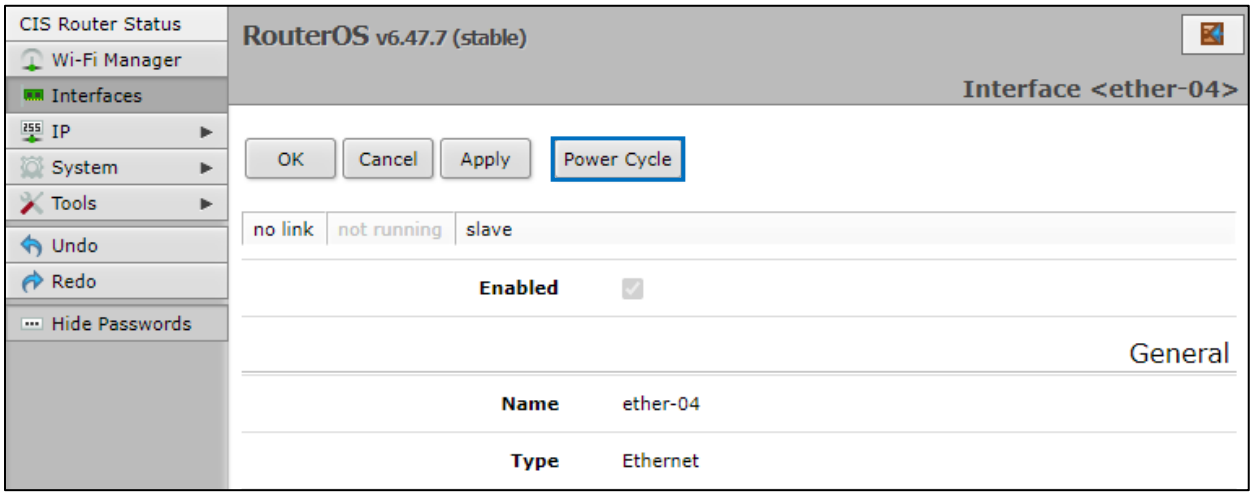
View and Set Interfaces

The Interfaces tab provides an overview of the activity on all ports. You can view the traffic sent and received, MTU settings and more.



Power Cycling an Ethernet Port

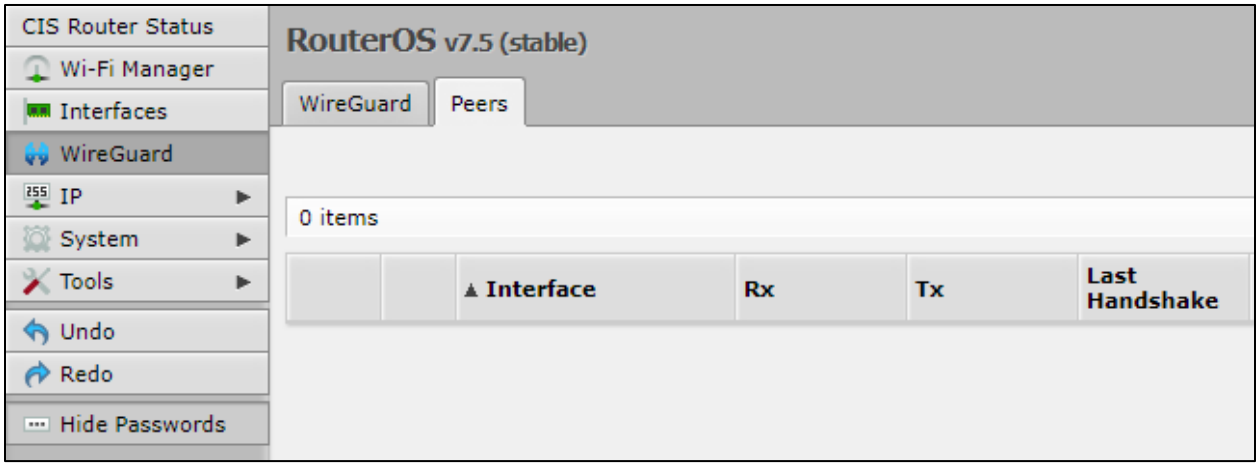
Select an Ethernet port in the table below to view the information for it. Click the **Power Cycle** button to disable, then re-enable the port.



WireGuard

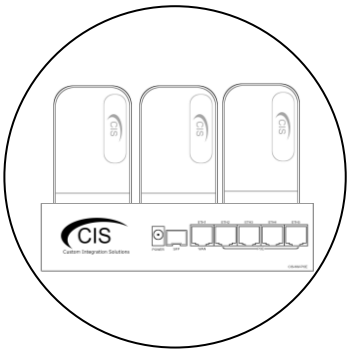
CIS is now offering an alternative to the L2TP VPN. With WireGuard, your clients can access their home network with minimal configuration on their mobile devices. Download the WireGuard app from the app store and scan the QR code provided by CIS. It also works well on Windows PCs and MacOS devices.

Call CIS to activate your WireGuard VPN. Your router will be configured for your devices, and you will be sent the required QR codes to connect them. You can monitor connectivity status and traffic from the **WireGuard** tab.



Managing Access Points with the Wireless Manager

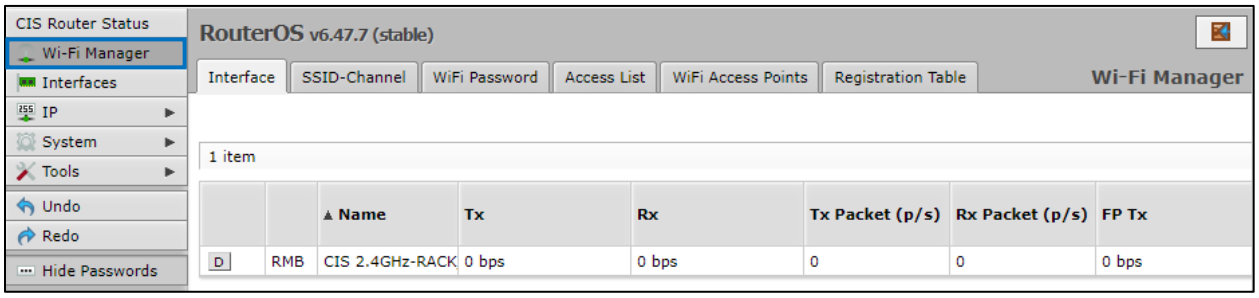
All CIS routers include a Wireless Manager that allows you to manage your access points from a single location. All changes to SSIDs, passwords and other options will be propagated to all CIS access points on the network.



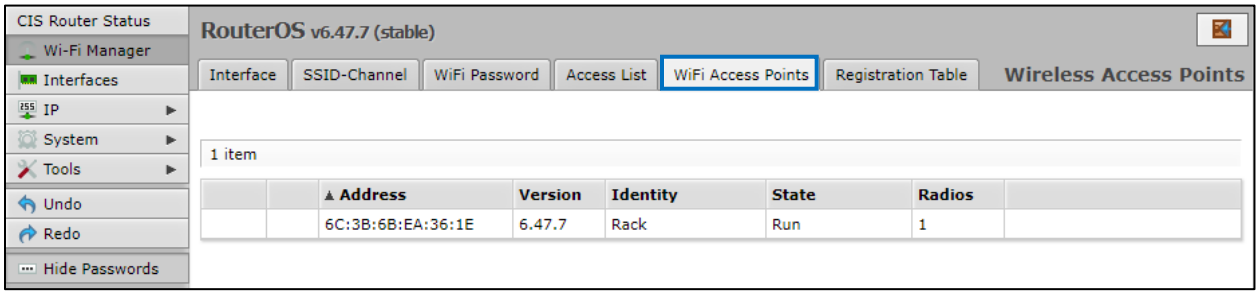
To configure your CIS access point for use with the Wireless Manager, view the manual for the CIS-ACWAP.

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.

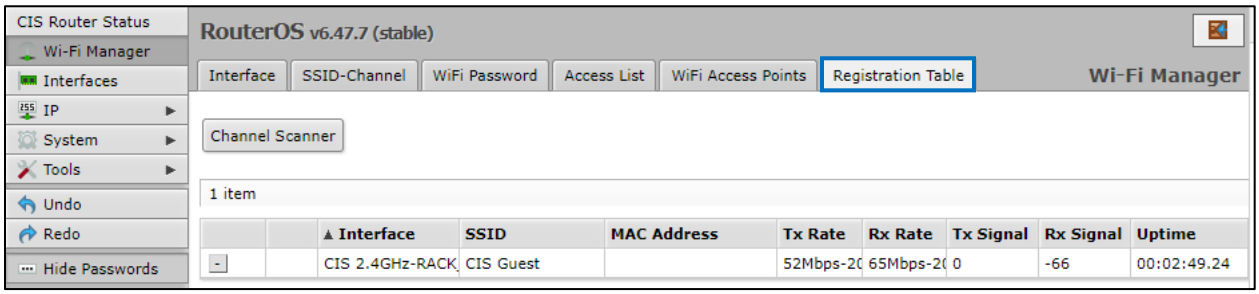


If you select the **WiFi Access points tab**, you'll be able to view the identity, MAC address and other information of the individual access points.



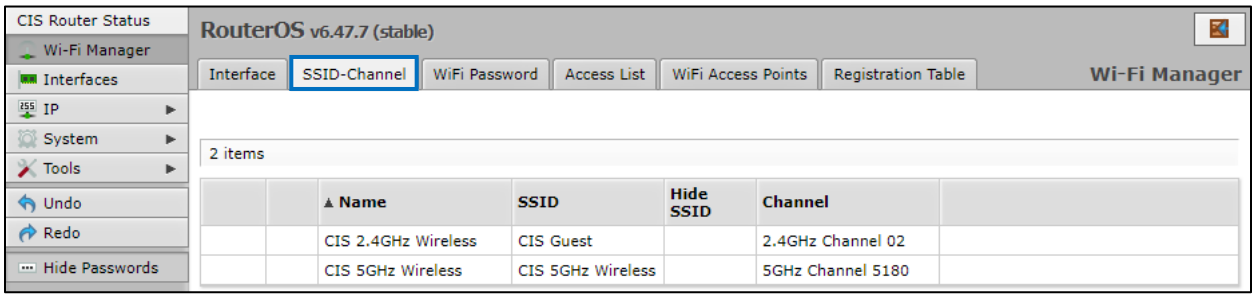
Viewing Connected Devices

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

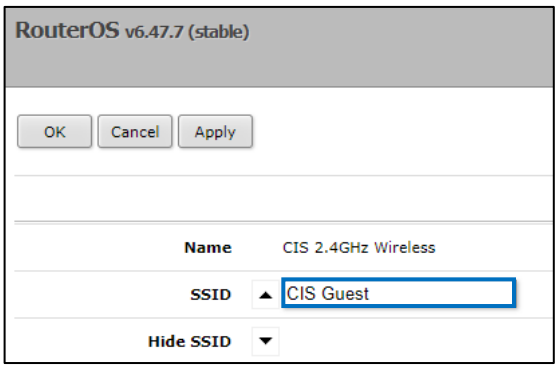


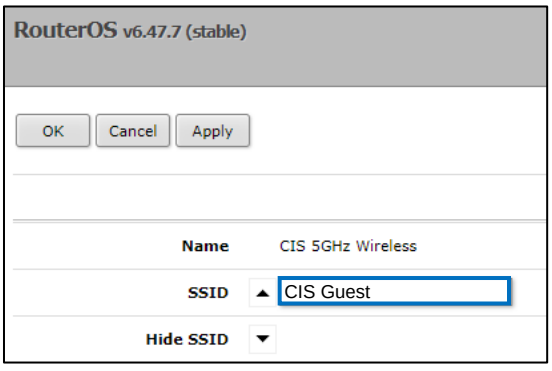
Changing the SSID of Managed Access Points

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



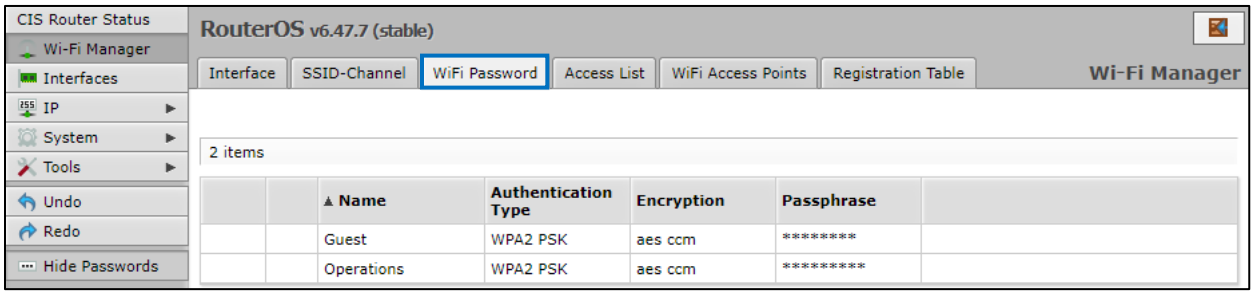
Copy and paste the SSID so that the 5GHz network has the same SSID.



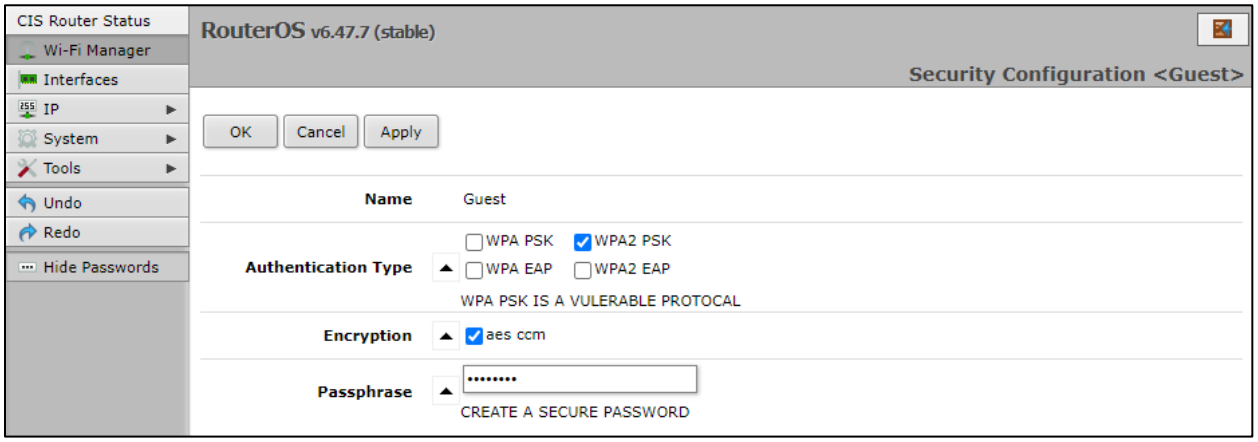


Changing the Wi-Fi Password of Managed Access Points

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.



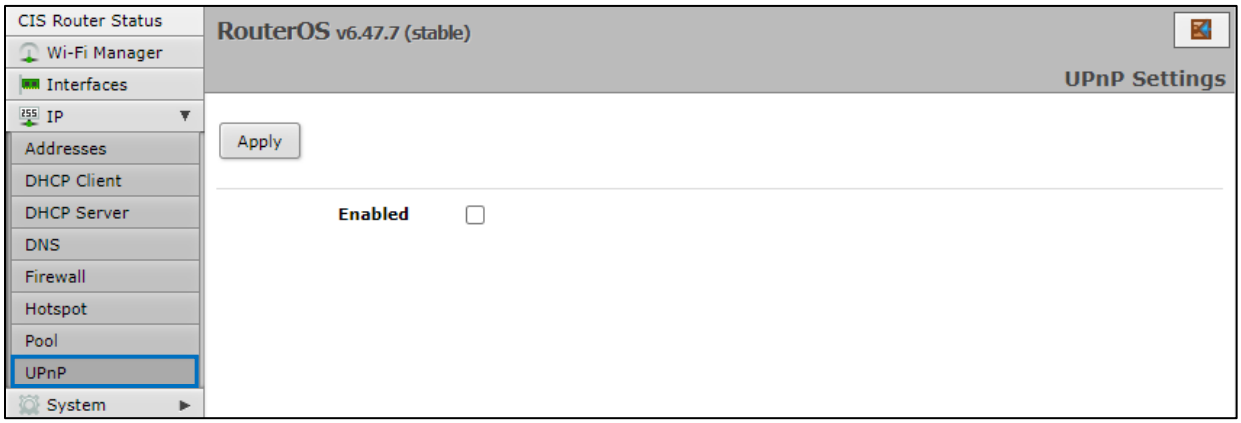
Click on the network you'd like to set the password for, then enter the passphrase in the box below. It is highly recommended you use only **WPA2 PSK** for security purposes. WPA is vulnerable to password cracking.



Tools

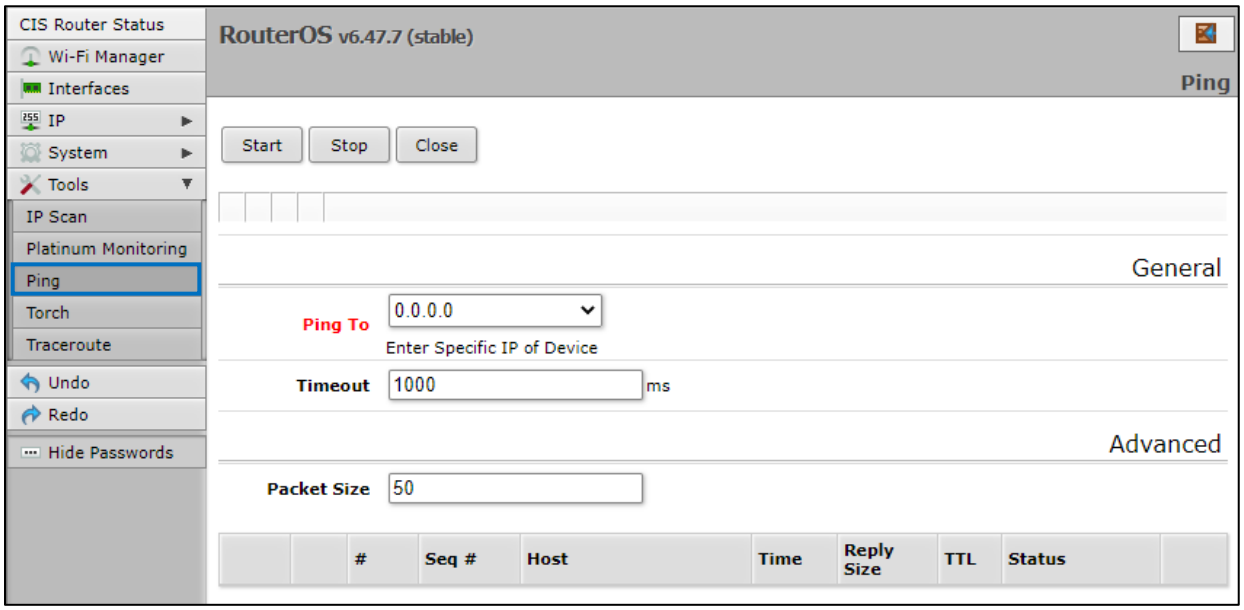
UPnP

Universal Plug and Play enables your router 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

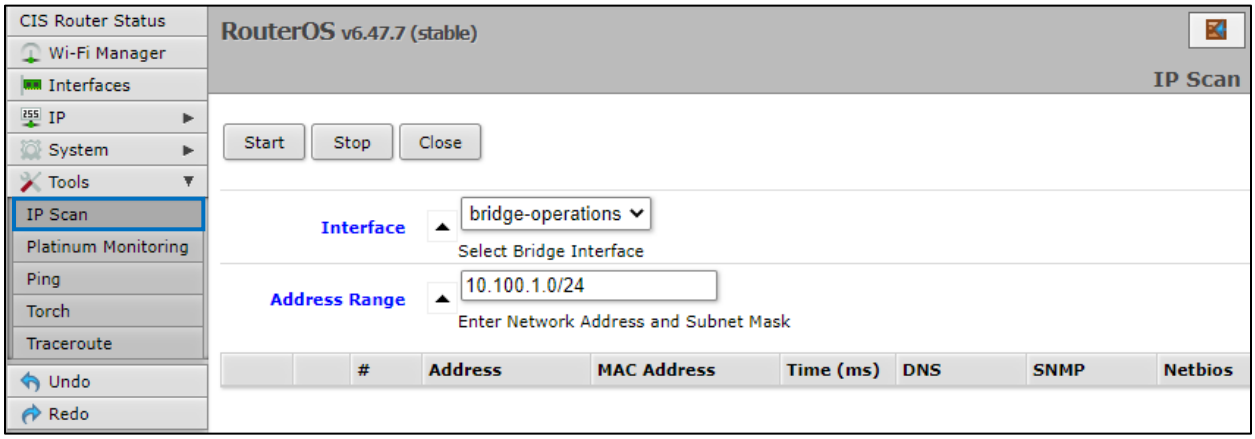
Ping uses Internet Control Message Protocol (ICMP) echo messages to determine if a remote host is active. It will also provide the round-trip time between the hosts. Enter the IP address of the device and select Start to begin.



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 the router.

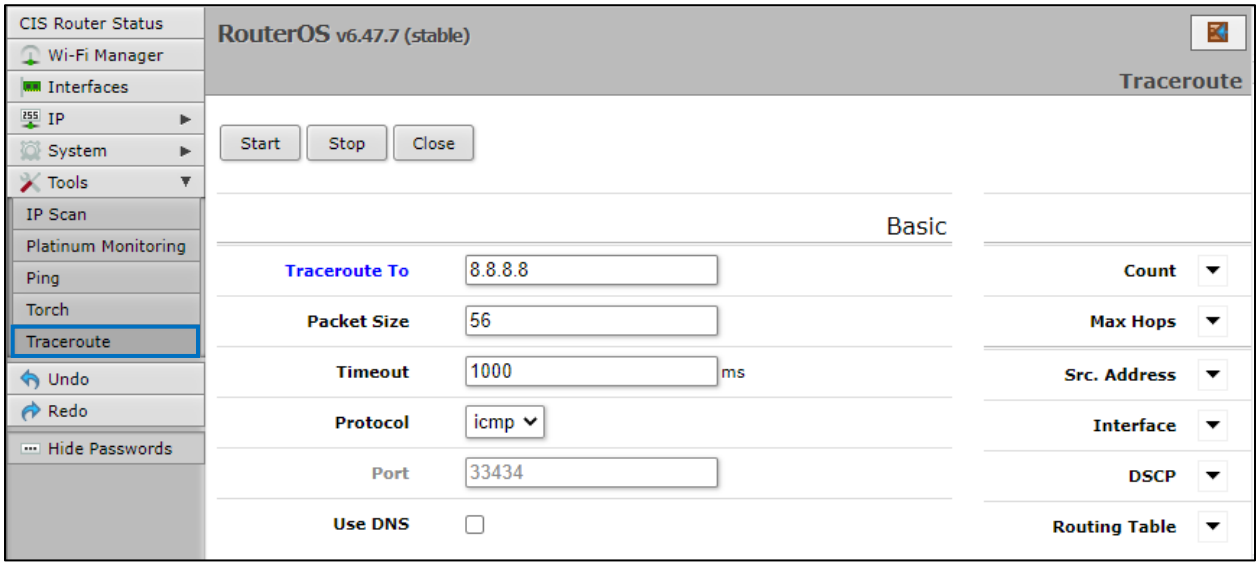
To use the IP scan tool, select the network you wish to scan on (bridge-operations is default), then enter the network address and subnet mask using CIDR notation.



*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.*

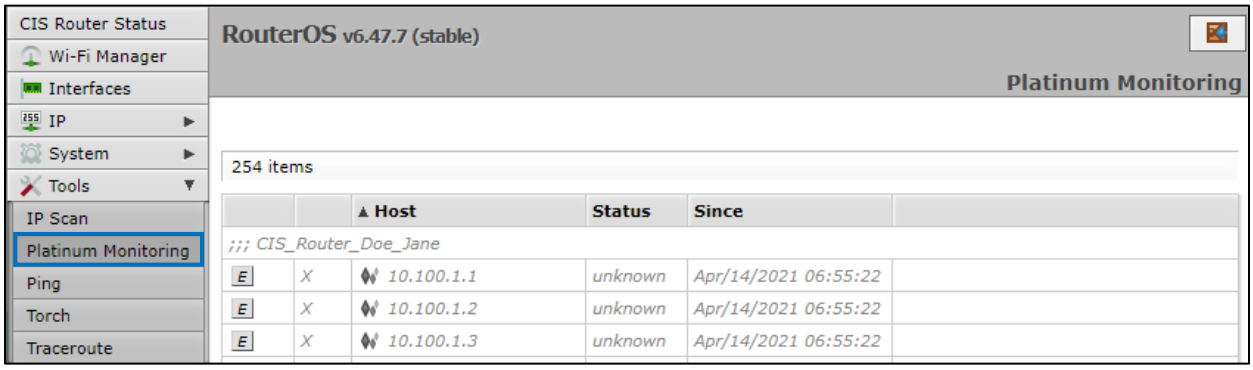
Traceroute

The traceroute tool is used to view the network hops between your router and a destination IP. For basic use, enter the IP address of the host to perform the trace on and click Start.



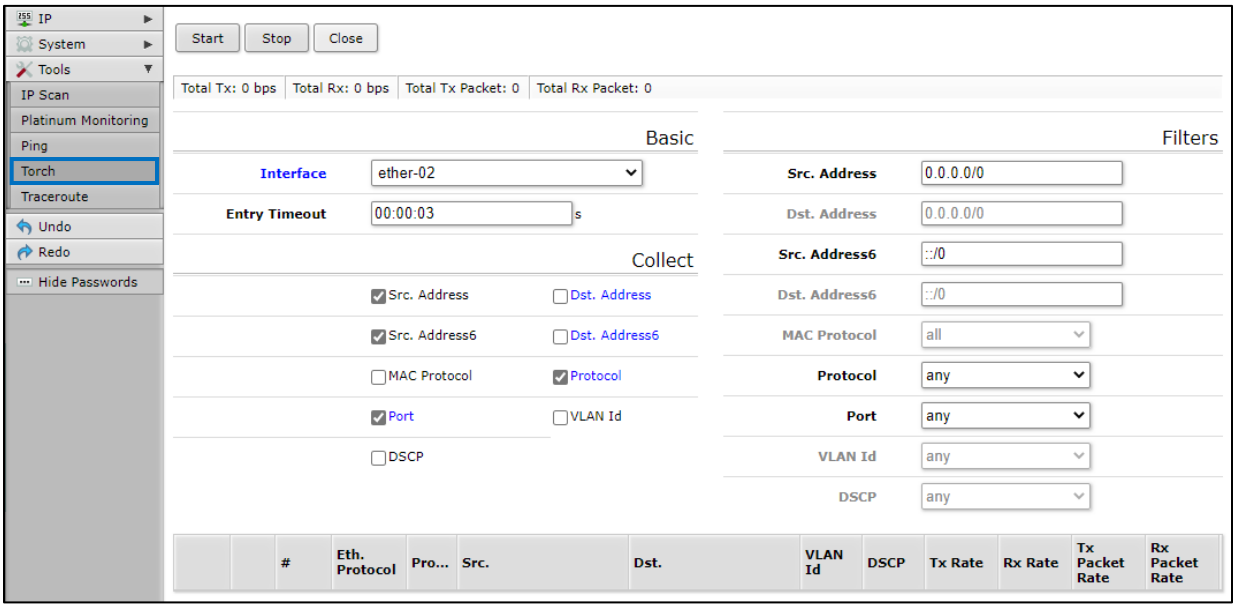
Platinum Monitoring

If the client has a Platinum or PlatinumDN service, they will receive the Platinum Monitoring service, which will send email alerts when key networking equipment at a specified IP address goes offline. You can enable and disable notifications by clicking the **D** or **E** buttons on the left.



Torch

Torch allows you to view packets flowing through an interface. You can obtain information such as the IP addresses, ports, and protocols in use. You can select the interface, and which information to collect. You can specify a source or destination address range or leave these fields blank for all addresses. You can specify by port or protocol as well.



Troubleshooting

Symptom	Possible causes
I cannot access my system using the VPN.	• Ensure the username, password, and secret were copied and pasted correctly and contain no extra characters or spaces. • It is recommended you use a DNS name to connect instead of an IP address, as they are prone to change from time to time. • Your ISP's provided gateway must be in bridge mode for VPN access to work. Consider a PlatinumDN service if this is not possible.
Port Forwarding does not work.	• Review the manual to ensure the configuration is set correctly or call CIS for support. • The ISP's gateway must be in bridge mode or have extra configuration applied.
The client is not getting the speed they are paying the ISP for.	• If you are connected wirelessly, the speed will be affected by the distance from the access point, interference from neighboring networks, the number of devices connected to the access point, the environment surrounding the access point, the device used, and other factors. • With current technologies, wireless access points are not able to perform at the speed of a Gigabit internet connection, especially in a crowded environment.
I cannot access the router's web interface.	Ensure your device is set to receive an IP address via DHCP. If your router's IP address is different than the default, obtain the default gateway address and use that to connect. You can do this using **ipconfig** in a command prompt in Windows.
The router has no internet access.	• Check connections and reboot the router and ISP's gateway. • If the ISP requires a static IP address or PPPoE connection, contact CIS for assistance.

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

CE

The CIS-CCR2004 is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EC.