Troubleshooting a Traditional Cisco Business Wireless Network

Objective

This document will cover some of the areas to analyze when troubleshooting a traditional Cisco wireless network. If you are using a mesh network, check out Troubleshooting a Cisco Business Wireless Mesh Network.

Applicable Devices | Software Version

- WAP121 | 1.0.6.8 (download latest)
- WAP125 | 1.0.3.1 (download latest)
- WAP131 | 1.0.2.17 (download latest)
- WAP150 | 1.1.2.4 (download latest)
- WAP361 | 1.1.2.4 (download latest)
- WAP371 | 1.3.0.7 (download latest)
- WAP551 | 1.2.1.6 (download latest)
- WAP561 | 1.2.1.7 (download latest)
- WAP571 | 1.1.0.3 (download latest)
- WAP571E | 1.1.0.3 (download latest)
- WAP581 | 1.0.3.1 (download latest)

Table of Contents

Introduction

Mesh wireless networks are awesome, but let’s face it, things happen! Just like any wireless network, a number of things can cause problems. Sometimes there is a simple fix, while others might be more complicated.

For optimum performance and reliability, keep these in mind!

1. Make sure the area has full coverage for the expected number of clients and their applications. Additional wireless access points may need to be added in order to smooth out the performance across your total wireless infrastructure.
2. Be aware of the types of applications they may be using (or as an administrator, the types of applications you may allow).
3. Clients running video streaming applications consume more bandwidth than those that may be streaming audio-only programs. Video applications rely on buffering to provide a decent experience.
4. Clients running voice-related applications require immediate service with no delays while not being as bandwidth-intensive. Since there is no buffering with a voice call, it is very important that packets are not dropped.

Ready for some troubleshooting? Let’s dig in!

Connection Problems? Start with the Basics

Check Physical and Environmental Conditions

This is the easiest way to troubleshoot but is often overlooked. Even though these may appear to be obvious, it is good to start with the basics.

1. Is there power to everything?
2. Is all the equipment turned on?
3. Are the cables connected correctly?
4. Do you have a link light on consistently?
5. Could it be a bad cable?
6. Is any of the equipment overheated?
7. Could there be environmental factors such as where it is located?
8. Is there metal or thick walls between the AP and the wireless device?
9. If the client is completely unable to connect, could the client be out of range?

Other Items to Consider

1. Restart the AP.
2. For APs connecting to a switch, check the switch configuration, and verify that the switch is running in good health. The CPU utilization, temperature, and memory utilization should be below the specified threshold levels.
3. On the Web UI, under *Monitoring*, check the *Wireless Dashboard* to gather information on performance and other issues.
4. Make sure all equipment is running the latest version of the firmware.
5. Enable *Bonjour* and *Link Layer Discovery Protocol (LLDP)* on the router if it is available.

6. Enable *Wireless Multicast Forwarding* when available for gaming and streaming applications.
7. Disable *Bandwidth Utilization*.

Number of SSIDs

Every Service Set Identifier (SSID) requires sending a beacon frame every 100 milliseconds (ms), which can eat up a lot of channel utilization.

It is best to limit the total number of SSIDs on the AP to 1-2 SSIDs per radio or per AP if possible.

Check Connectivity Issues

Run Connectivity Tests from the Web User Interface (UI)

The AP must be able to communicate with other devices to be effective. A simple way to check this is to perform a ping.

Ping the AP from at least two clients that are connected (associated) to that particular access point. Access the administration menus of that AP to determine which clients are connected directly.

Ping from the router to the access point IP address to see if end-to-end connectivity is available. Ping from the router to the wireless clients associated with the AP to check if they can be reached from the main network.

For more details on how to ping, click on the most appropriate link:

- Ping, Traceroute, and DNS Lookup on the RV160 and RV260
- DNS Name Lookup and Ping Test on RV320 and RV325 VPN Router Series
- Perform a Diagnostic Evaluation on an RV34x Series Router

Could DHCP Problems be the Issue?

Make sure that the DHCP server is operational and reachable from the Local Area Network (LAN) of the AP.

It’s possible that there are more clients needing an IP address than are available in the DHCP pool. See the section *How to View or Change the Pool of IP Addresses for DHCP* section the article Best Practices for Setting Static IP Addresses on Cisco Business Hardware for more information.

There may be times where too many DHCP addresses are cached, which can also prevent clients from getting an IP address. To learn more about this, check out

Tips to Keep the ARP Table Available for DHCP IP Addressing. Windows Support

If Windows, select your wireless connection from the Network Connections panel and verify that its status is "Enabled."

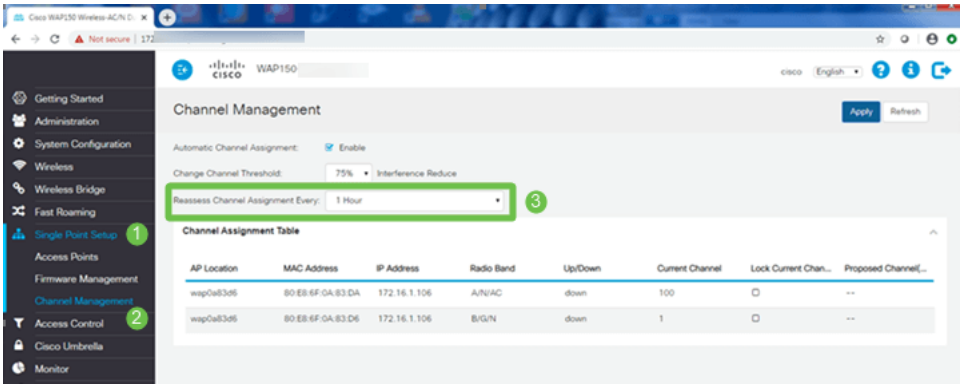
Detailed guidance can be found at the Microsoft Support Forum for troubleshooting wireless network connectivity at the following URL: Fix Wi-Fi connection issues in Windows.

Change Specific Default Settings

There are some default settings that might cause connection issues. You can try changing the following settings.

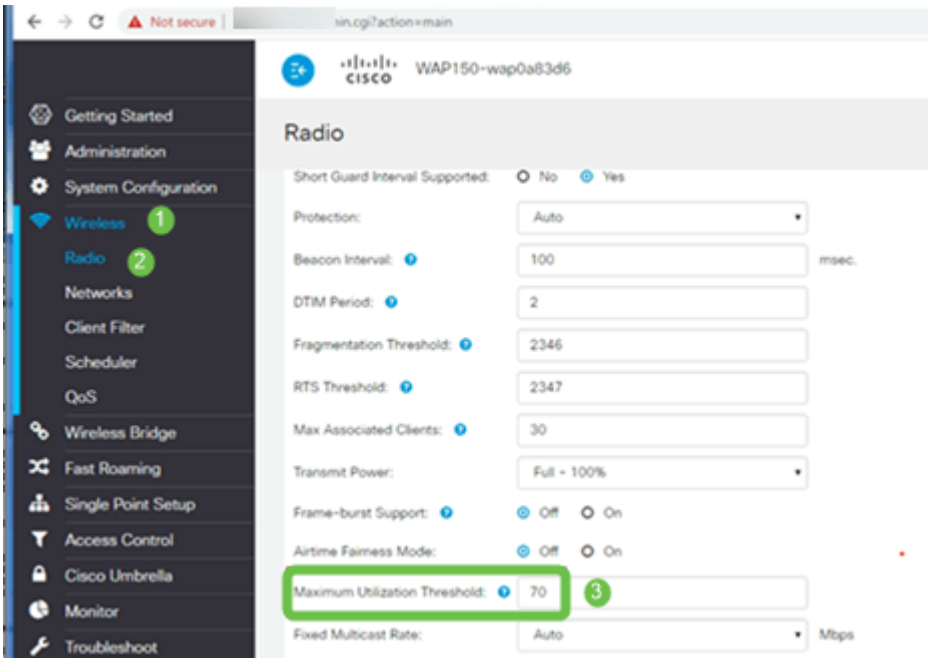
Reassess Channel Assignment

Navigate to **Single Point Setup > Channel Management** page. Under *Reassess Channel Assignment*, adjust the default of *1 Hour* to either *Every 12 hours* or *1 time a day*. This will avoid frequent channel reselection (which will force WLAN client reassociations every 1 hour).



Maximum Utilization Threshold

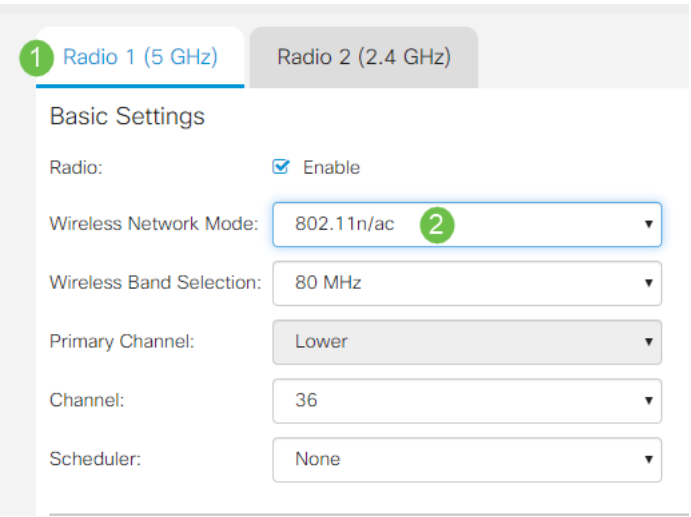
Navigate to **Wireless > Radio**. You are automatically under *Radio 1 (5 GHz).* Under *Maximum Utilization Threshold*, the default of *70* should be changed to **0**.



Radio Settings

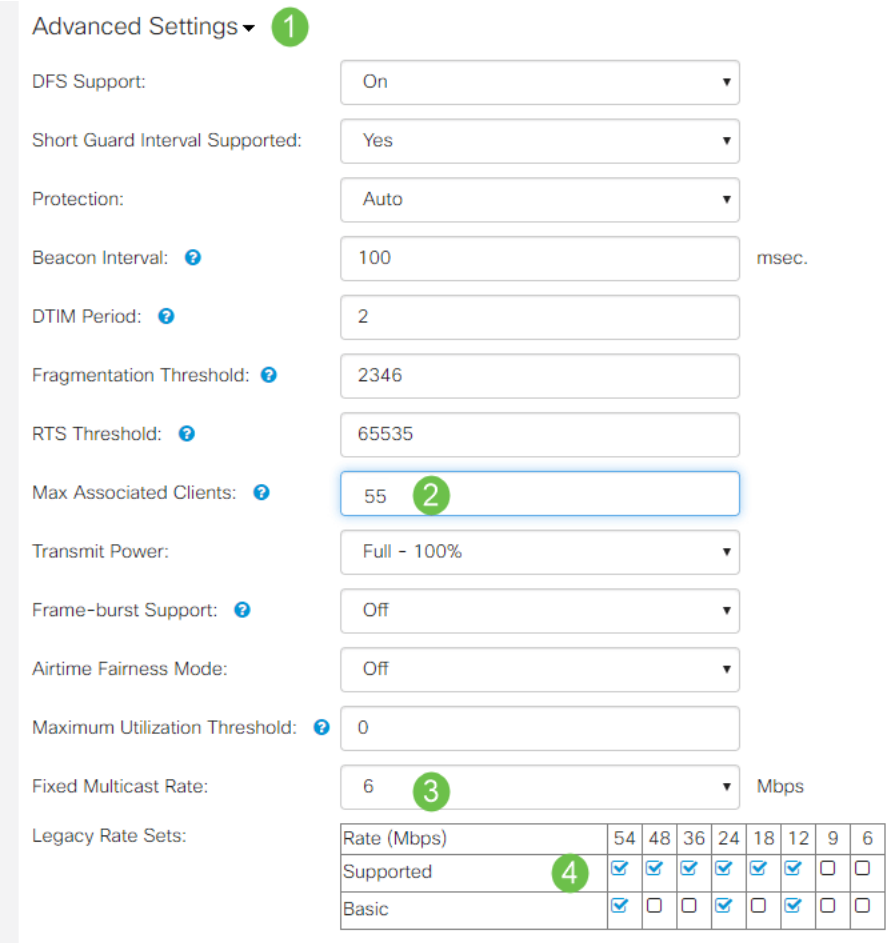
Keep on the *Radio* page under *Radio 1 (5 GHz).*

Set *Wireless Network Mode* to **802.11n/ac**.



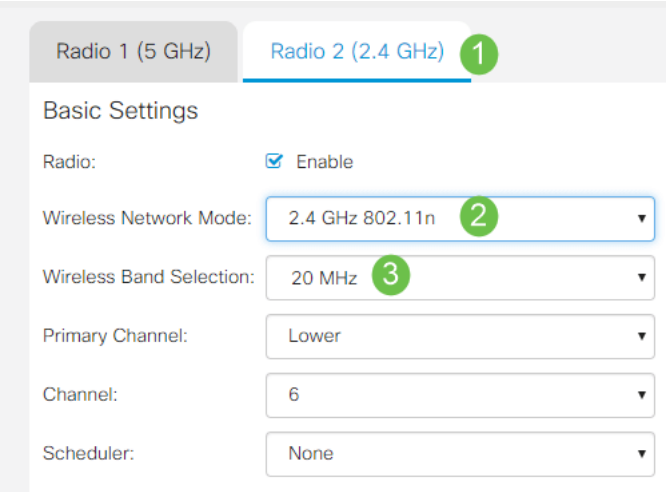
Scroll down to *Advanced Settings* and set the following configurations:

- Under *Max Associated Clients*, lower the default of *200* to **55** or less. For large deployments where there may be more than 20 clients using wireless in the same coverage area, check the datasheet for the access point model in use to check the maximum number of wireless clients supported simultaneously on that AP. If the access point does have the possibility of exceeding its maximum wireless client support, consider adding additional APs in the coverage area and limiting the number of clients a single AP will support
- Change the *Fixed Multicast Rate* to **6**.
- Under *Legacy Rate Sets*, for both *Supported* and *Basic*, uncheck **6** and **9** Mbps.
- Under *Legacy Rate Sets*, for *Basic*, enable **24** and **54**.



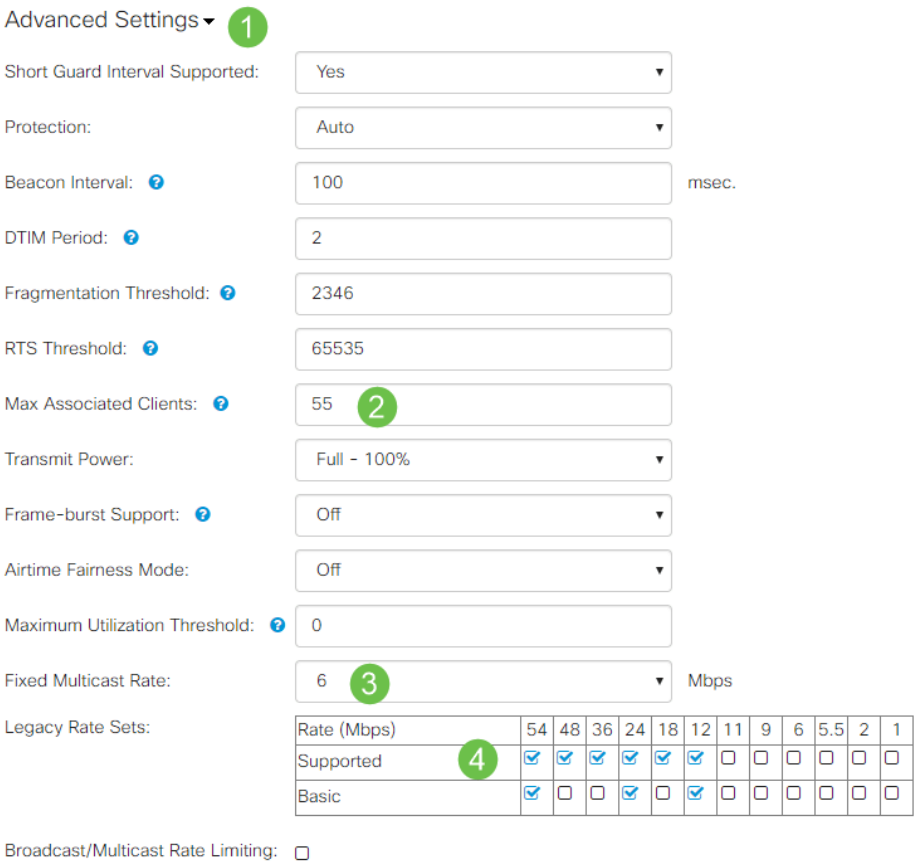
Keep on the *Radio* page and select *Radio 2 (2.4 GHz)*.

Set *Wireless Network Mode* to **2.4 GHz 802.11n** and *Wireless Band Selection* to **20 MHz**.



Scroll down to *Advanced Settings* and set the following configurations:

- Under *Max Associated Clients*, lower the default of *200* to **55** or less.
- Change the *Fixed Multicast Rate* to **6**.
- Under *Legacy Rate Sets*, for both *Supported* and *Basic*, uncheck **1, 2, 5.5, 6, 9,** and **11.** Mbps.
- Under *Legacy Rate Sets*, for *Basic*, enable **12, 24,** and **54**.



Interference Considerations

Possible Interference Problems

Interference can cause issues on wireless networks and can come from more sources than ever before. Microwaves, security cameras, smartwatches, motion detectors, or even fluorescent bulbs can cause interference.

How much they affect the network can depend on many factors including the amount of power emitted if the object is constantly on, or if it is intermittent. The stronger the signal or the more frequently it is on the more problems that can arise.

Rogue APs and rogue clients can cause problems if there are too many on the same channel as well. Voice over IP and streaming of video can cause issues as well.

Interference can be a major inhibitor to wireless performance, creating security vulnerabilities and wireless network instability.

If you would like to learn more about the causes of interference, check out the following articles:

- Manage the Rogue AP Detection List on the WAP125 or WAP581 Access Point
- Configure the Basic Radio Settings on the WAP581
- Enable Spectrum Analysis Mode on a WAP581 Access Point
- Tips for Single Point Setup on a WAP581
- Configure the Advanced Radio Settings on the WAP125 and the WAP581

Signal to Noise Ratio (SNR)

On a real-time application, such as voice or video, it is recommended to have at least a 25 dB SNR versus 20 dB SNR for data application.

Using a standard noise level of -92 dBm, a 25 dB SNR = -67 dBm Received Signal Strength Indicator (RSSI).

Navigate to **Monitoring > Wireless Dashboard** on the Web UI to see inside your network.

The following chart shows the Acceptable Signal Strengths RSSI Value:

Signal Strength	Rating	Description	Required to use
-30 dBm	Amazing	Max achievable signal strength. The client can only be a few feet from the AP to achieve this. Not typical in the real world.	N/A
-67 dBm	Very Good	Minimum signal strength for applications that require very reliable, timely delivery of data packets.	Voice over IP, Voice over WiFi, and streaming video
-70 dBm	Okay	Minimum signal strength for reliable packet delivery.	Email, web
-80 dBm	Not Good	Minimum signal strength for basic connectivity. Packet delivery may be unreliable.	N/A
-90 dBm	Unusable	Approaching or drowning in the noise floor. Any functionality is highly unlikely.	N/A

Look Behind the Curtain

Syslogs

Being aware of events can help ensure the network runs smoothly and prevent failures. Syslogs are useful for network troubleshooting, debugging packet flow, and to monitor events.

These logs can be viewed on the Web User Interface (UI) of the Master AP and if configured, on remote log servers. Events are typically erased from the system when rebooted if they are not saved on a remote server.

If you would like more information, check out these articles:

- Configure System Log Settings on the RV34x Series Router
- Manage the System Logs (Syslogs) on an RV34x Series Router
- Configuring Remote Logging on RV160 and RV260 Routers
- View Logs on an RV Series Router
- System Log Configuration on RV320 and RV325 VPN Router Series

Packet Captures

A packet capture, also known as a PCAP file, is a tool that can be helpful in troubleshooting. It records every packet sent between devices in your network, in real-time. Capturing packets allows you to dig into the details of the network traffic, which can include everything from device negotiation, protocol conversations, failed authentication, and sensitive information transfer. You can see the path of specific traffic flows and every interaction between devices on selected networks. These packets can be saved for further analysis as needed. It's like an x-ray of the network's transfer of packets.

If you would like more information, check out these articles:

- Using Wireshark on a Cisco Business WAP for Packet Analysis: Stream Directly to Wireshark
- Integrating Cloudshark for Packet Analysis on a WAP125 or WAP581
- Configure Packet Capture on a WAP125 or WAP581 Access Point
- Configure Packet Capture on the WAP125

If All Else Fails, Reset to Factory Default Settings

An option of last resort, that should only be done to remedy the most severe issues such as losing the ability to gain access to the management portal, is to perform a hardware reset on the router.

When you reset to factory default settings you lose all configurations. You will need to set up the router again from scratch so make sure you have the connection details.

Reference your hardware administration manual for specific details on how to accomplish a hardware reset.

If your router model is over 5 years old, consider replacement with a modern router to get the latest security and vulnerability patches. Many older routers do not provide further development efforts to keep them updated and patched (just as you would normally do with your PC).

- Reboot and Factory Default Reset on WAP121 and WAP321 Access Points
- Reboot and Reset the Wireless Access Point to Factory Default Settings
- Reboot and Reset the WAP125 and WAP581 to Factory Default Settings
- Reset a CBW AP back to Factory Default Settings

Conclusion

It's hard to tell what helped you fix your connection, but this toolbox of options should have done

the trick!