TechTarget | SearchNetworking

E-guide

PRO+ Content

10 Steps to Troubleshooting Wi-Fi Connectivity

In this e-guide

In this e-guide:

In the workplace, wireless connection problems can crop up at any time.

So when you have trouble connecting a smartphone, tablet, laptop or other Wi-Fi client device to an office wireless LAN, what should you do?

In this e-guide, discover 10 step-by-step troubleshooting tips to help with your wireless network connection problems.

In this e-guide

10 steps to troubleshoot wireless connection problems

Lisa Phifer, Owner | Core Competence Inc.

Wireless connection problems can crop up when joining a wireless client to an office network. These step-by-step debugging tips can help.

Step 1: Check WAN and LAN connections

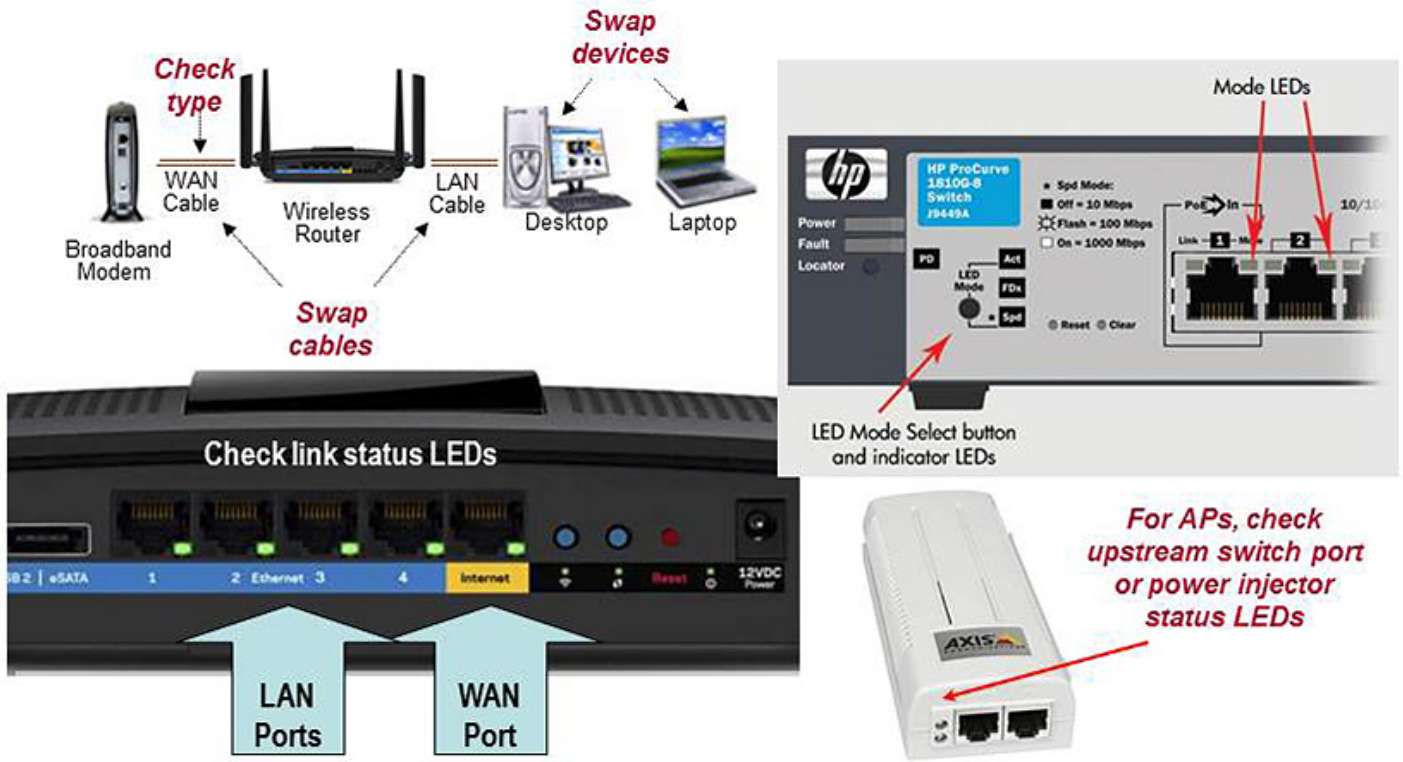
Physical connections are an oft-overlooked common culprit. Check all wireless access point (AP) or wireless router ports to ensure that Ethernet cables are inserted tightly and link status LEDs are green at both ends. If not:

- Verify that devices at both ends of each Ethernet cable are powered on and that ports are enabled. For example, your AP may be connected to a wall port that is disabled, or the upstream switch or modem may be off.
- Try swapping Ethernet cables to isolate a damaged cable or connector.

In this e-guide

- Check your AP or router manual to ensure that you're using the right type of cable. For example, Internet/WAN ports may require crossover cables.
- Connect another Ethernet-capable device, such as a laptop, to the affected AP or router port. If link status LEDs change, the device that you just replaced may be failing link auto-negotiation. Check port configurations at both ends and reconfigure as needed to match speed and duplex mode.

In this e-guide



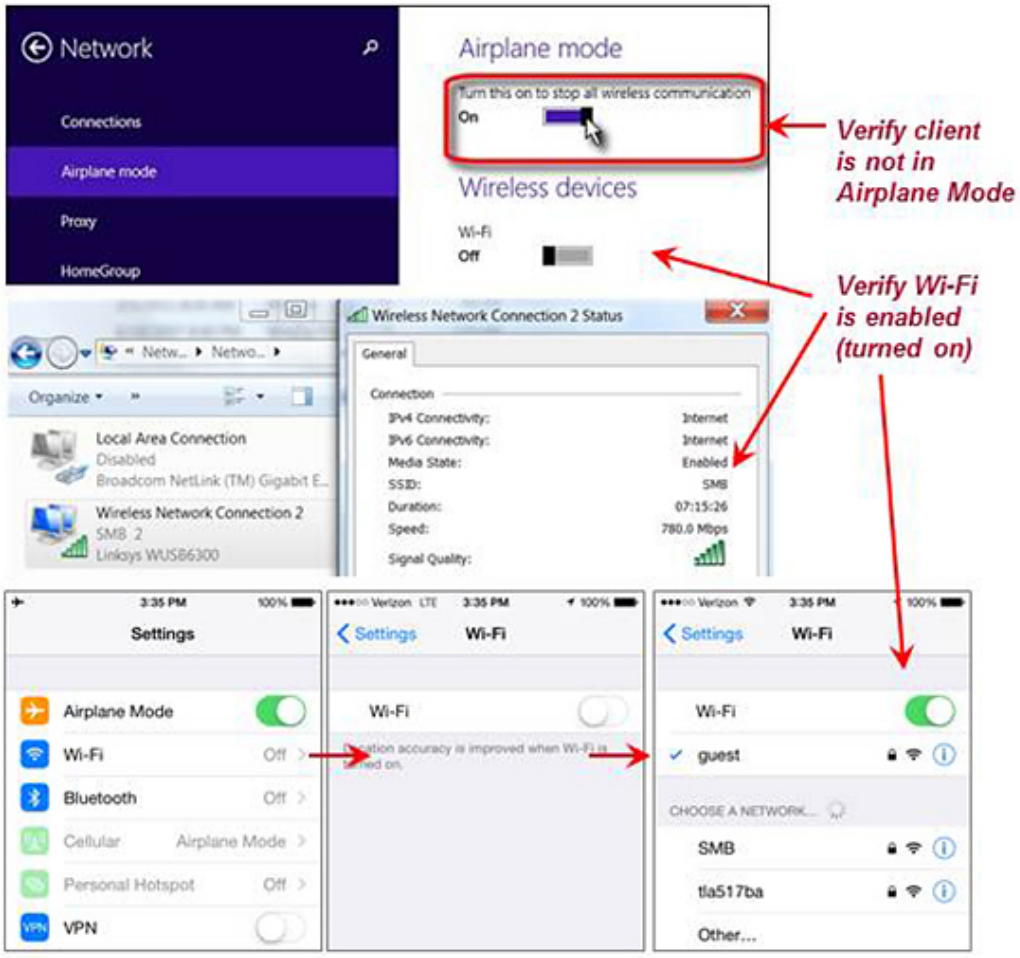
In this e-guide

Step 2: Verify wireless adapter

It might seem obvious, but it's important to ensure the client's Wi-Fi adapter used for network troubleshooting is enabled and ready to connect.

- When using a Windows client, select your wireless network adapter from the Network Connections Control Panel and check to see if its status is *Enabled*. If not, right-click to enable the connection. If this fails when using a laptop, look for a function key or physical button or slider-switch to take the laptop out of airplane mode. If this fails when using a removable client such as a USB adapter, remove and re-insert it.
- When using an Apple iOS client, use the Settings app to verify that your iPhone or iPad is not in airplane mode and that Wi-Fi is on and ready to connect. For further iOS client troubleshooting, see Part 2 of this series.
- On an Android client, use the Settings app in a similar manner to verify that your smartphone or tablet is not in airplane mode and that Wi-Fi is on. For further Android client troubleshooting, see Part 3 of this series.

In this e-guide



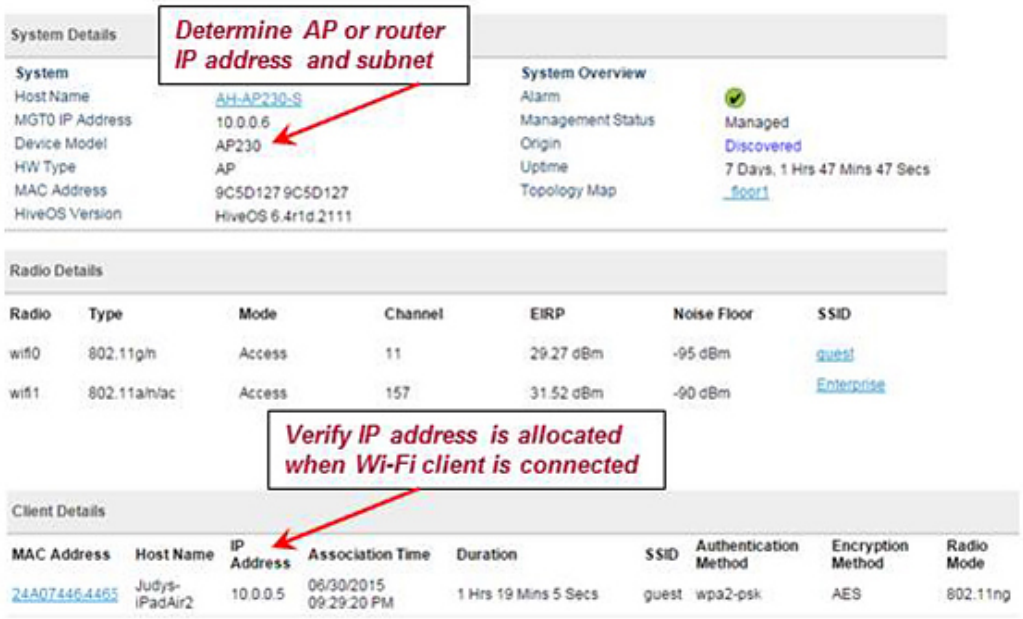
In this e-guide

Step 3: Verify AP and router settings

Use your wireless access point or router's administrative GUI to verify network settings for the wireless network service set identifier (SSID) to which your Wi-Fi client is trying to connect.

- Locate the SSID that you're troubleshooting. On a basic wireless router, there may be just one SSID, or one for each radio band (2.4 GHz and 5 GHz). On a small business or enterprise AP, there may be several SSIDs used to segregate wireless clients and their traffic.
- Identify the IP subnet [and, if applicable, virtual LAN (VLAN) ID] assigned to that SSID. Upon successful connection, your Wi-Fi client should receive a local IP address from this subnet.
- Identify the router or AP's own local IP address that should be reachable through this subnet (and, if applicable, VLAN).
- Check your router's events log or status GUI to verify that an IP address from this subnet is indeed assigned to your Wi-Fi client when it connects.

In this e-guide



System Details

System		System Overview	
Host Name	AH-AP230-S	Alarm	
MGT0 IP Address	10.0.0.6	Management Status	Managed
Device Model	AP230	Origin	Discovered
HW Type	AP	Uptime	7 Days, 1 Hrs 47 Mins 47 Secs
MAC Address	9C5D127 9C5D127	Topology Map	floor1
HiveOS Version	HiveOS 6.4r1d.2111		

Radio Details

Radio	Type	Mode	Channel	EIRP	Noise Floor	SSID
wifi0	802.11g/n	Access	11	29.27 dBm	-95 dBm	guest
wifi1	802.11a/n/ac	Access	157	31.52 dBm	-90 dBm	Enterprise

Client Details

MAC Address	Host Name	IP Address	Association Time	Duration	SSID	Authentication Method	Encryption Method	Radio Mode
24A07446:4465	Judys-iPadAir2	10.0.0.5	06/30/2015 09:29:20 PM	1 Hrs 19 Mins 5 Secs	guest	wpa2-psk	AES	802.11ng

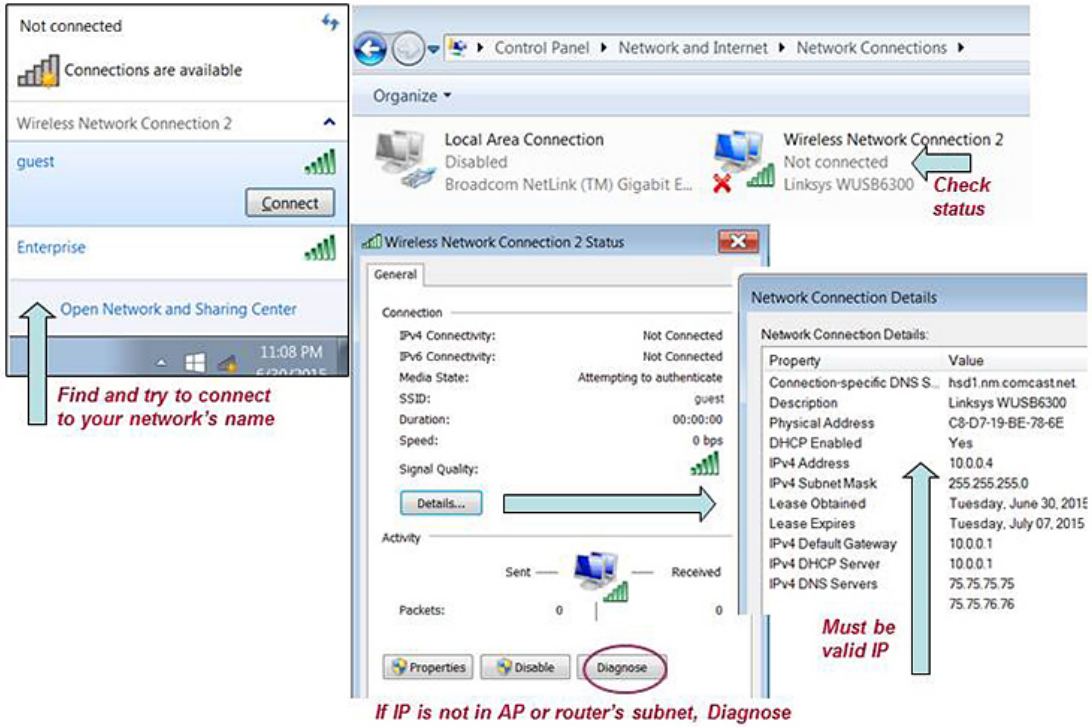
In this e-guide

Step 4: Verify TCP/IP settings

Although we describe using Windows to manage wireless connections here, troubleshooting is conceptually similar when using other kinds of Wi-Fi clients.

- Open the network connections control panel and select your wireless network adapter. If the status is still *Disabled*, return to step 2.
- If status is *Not Connected*, select your wireless network's SSID and click *Connect*. If your network's SSID does not appear in the list or you cannot connect to your network, go to step 8 to debug wireless settings.
- While attempting to connect, status may change briefly to *Authenticating* or *Acquiring Network Address*, then *Connected*. At that point, use Status/Support to determine the client's assigned IP address. If the client's IP is 0.0.0.0 or 169.254.x.x, click *Diagnose*. If that persists, go to step 8.
- Otherwise, if the Wi-Fi client's IP address is not in your AP or router's subnet, use the Properties/Internet (TCP/IP) panel to reconfigure the connection to get an address automatically and repeat step 4.

In this e-guide



In this e-guide

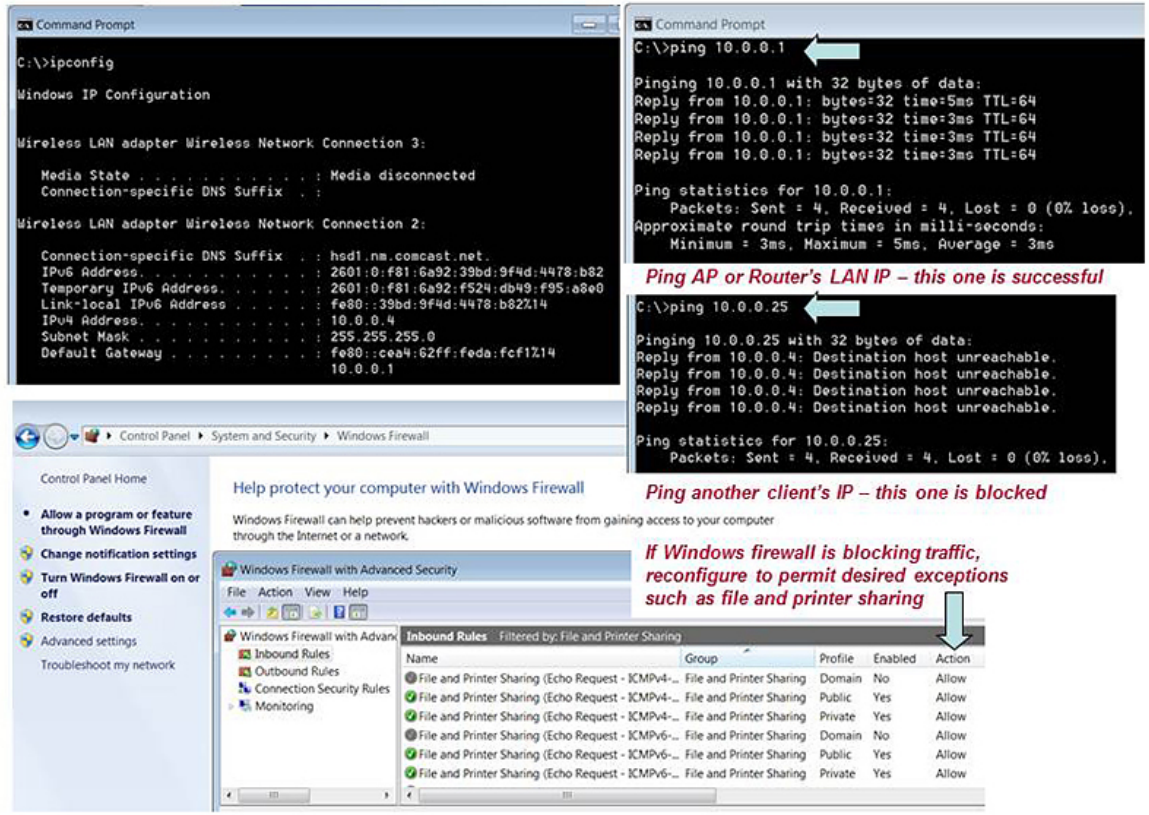
Step 5. Verify network connection with Ping

Once your wireless client has a valid IP address, use ping to verify network connectivity.

Run a Command Prompt window from the wireless client's Start menu and use it to ping your AP or router's IP address with the Internet Control Message Protocol as shown in Figure 5.

- If pinging your AP or router repeatedly fails, skip to step 6.
- If pinging your AP or router is successful, then ping any other wired or wireless LAN client that you wish to share files or printers with. If that ping fails, then the destination may be using a firewall to block incoming messages.
- After disabling the destination's Windows firewall, ping again. If ping is now successful, then the firewall you disabled may also be blocking Windows network protocols. Reconfigure the firewall to permit the traffic you want to exchange between LAN clients. For example, re-enable the firewall and permit inbound file and printer sharing.

In this e-guide



In this e-guide

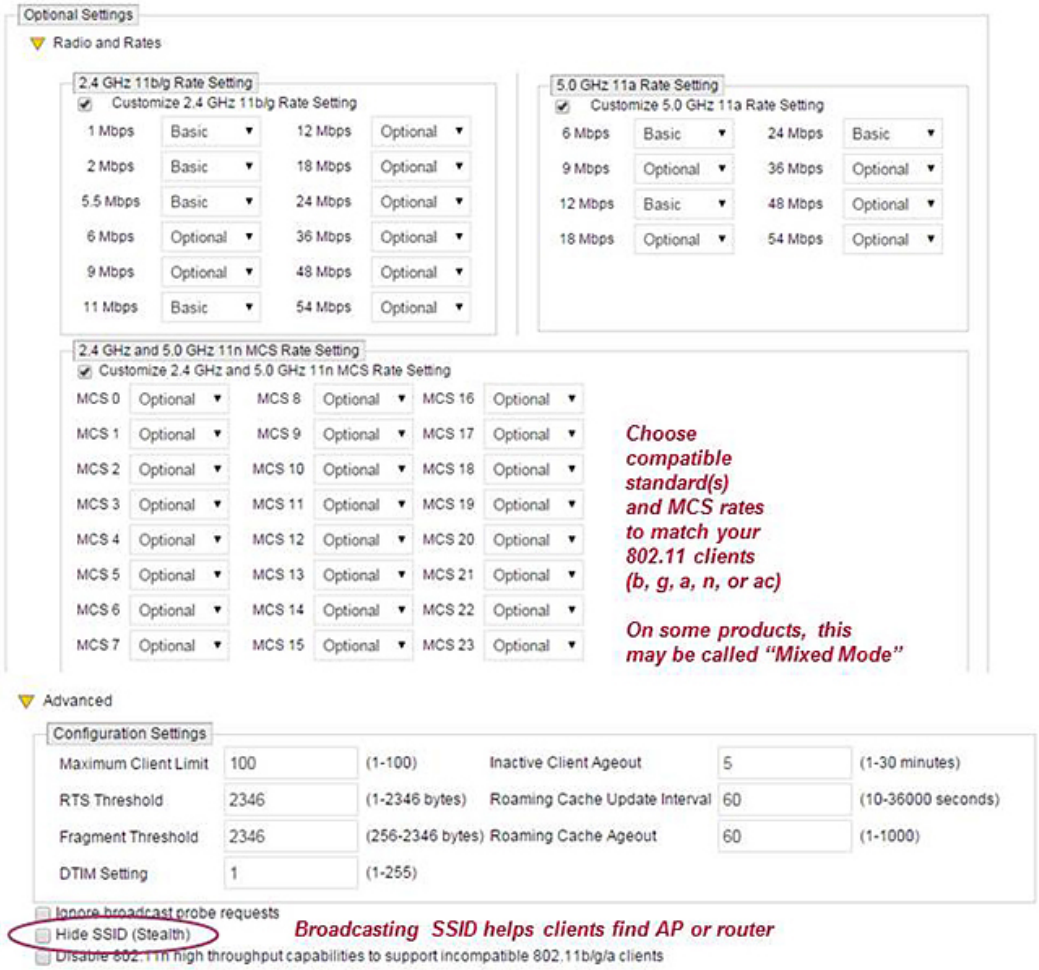
Step 6: Check wireless-specific issues

If your wireless client still cannot connect, get a valid IP address or ping your AP or router, then it's time to consider wireless-specific problems.

The wireless AP or router and client must use compatible 802.11 standards and the same network name (SSID). Use your AP or router's admin GUI to view WLAN settings and compare them to your client's wireless connection parameters.

- If your SSID does not appear in the Client's Available Networks list, enable *SSID broadcasts* on your AP or router. Alternatively, add the SSID to your client's Wireless Networks list, allowing devices to connect even if the SSID is hidden. Be sure to match the SSID exactly, including capitalization.
- 802.11ac, dual-band 802.11n and older 802.11a clients can connect to 802.11ac or 802.11n APs or routers using channels in the 5 GHz band.
- 802.11n and older 802.11b/g clients can also connect to 802.11n APs or routers using channels in the 2.4 GHz band.
- To connect older 802.11a or 802.11b/g clients, enable *Mixed Mode* and slower modulation and coding scheme rates on your AP or router. For example, to connect to 802.11b clients, at least the 11 Mbps rate must be enabled. To connect to 802.11g clients, at least the 54 Mbps rate must be supported. Even slow rates are needed to connect to old clients over longer distances.

In this e-guide



In this e-guide

Step 7: Look for a security mismatch

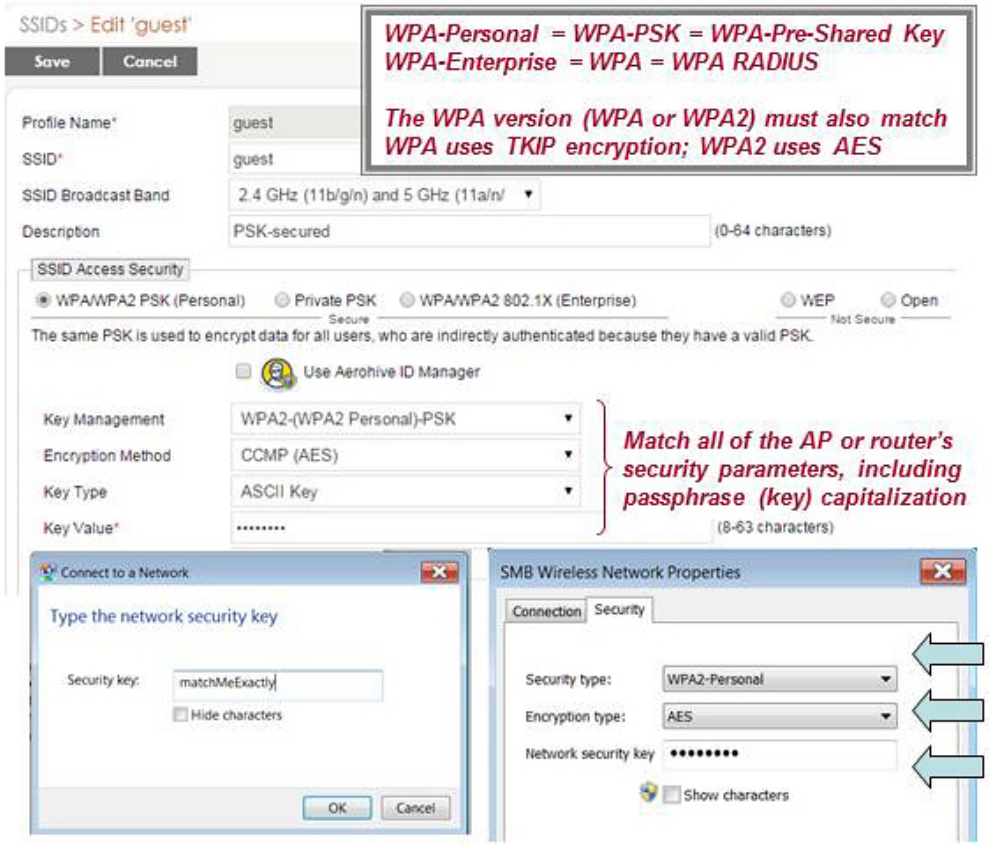
If a matched wireless client and AP or router can "hear" each other but still can't connect or exchange traffic, look for a security mismatch.

The client must support the security mode the AP or router requires: Open, WEP, WPA or WPA2. Unless the WLAN is open (unsecured), the AP or router and client must also have (or dynamically receive) the same keys used to encrypt traffic between them. Compare your AP or router's WLAN security settings to your client's wireless connection properties to match them.

- If your AP or router uses WEP, set the client's encryption to WEP and match the authentication type (open or shared). Copy the AP or router's first WEP key to the client, translating from ASCII to hex if needed.
- If your AP or router uses WPA-Personal, set the client's authentication to WPA-PSK and match the encryption type (TKIP). Enter the same passphrase on both devices Remember: Capitalization counts!
- If your AP or router uses WPA2-Personal, set the client's authentication to WPA2-PSK, match the encryption type (AES) and enter the same passphrase on both devices. If you must support both WPA and WPA2 clients, set your AP or router to allow both TKIP and AES encryption.

In this e-guide

- If your AP or router uses WPA or WPA2-Enterprise, set the client's authentication to WPA or WPA2 respectively, match the encryption type and continue 802.1X set-up in step 8.



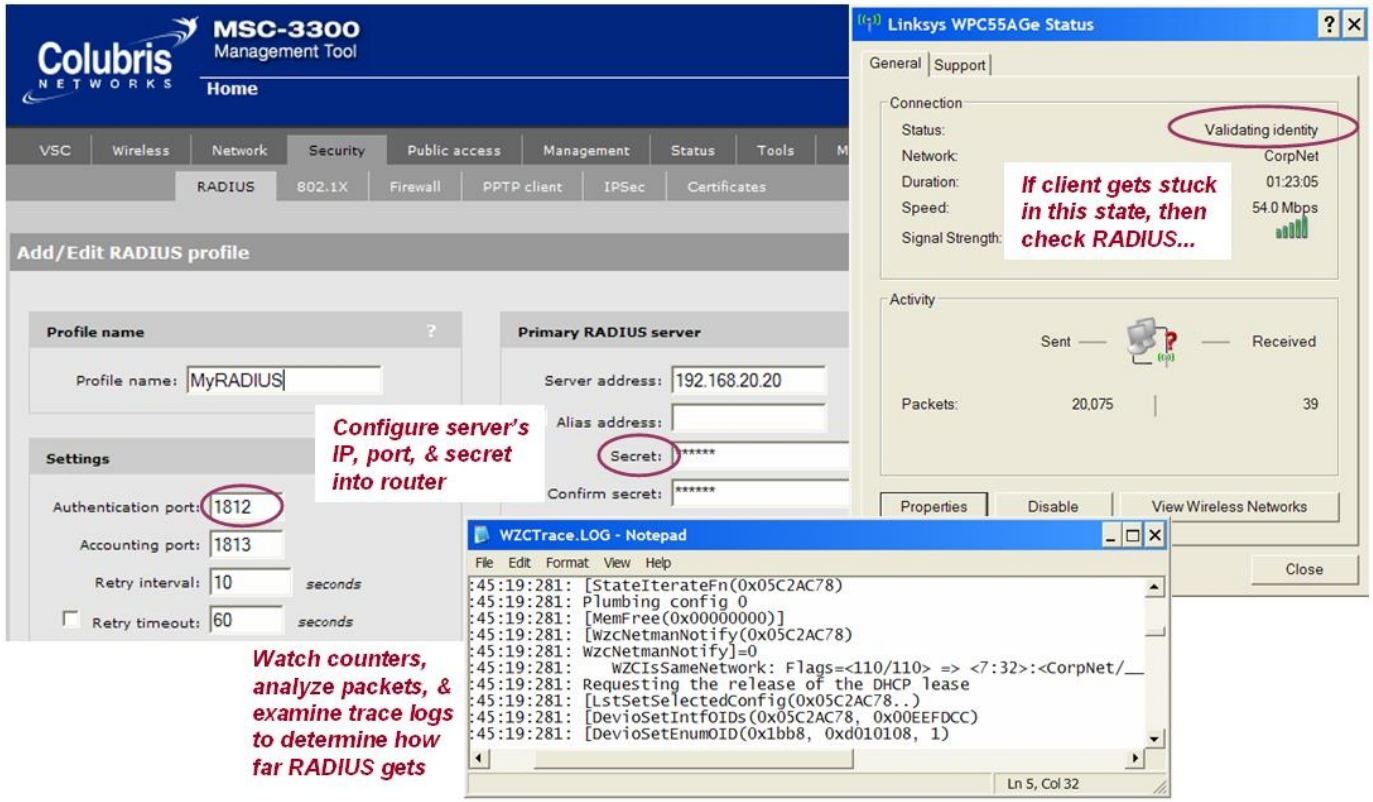
In this e-guide

Step 8: Ensure RADIUS is working

WPA and WPA2-Enterprise log the client into the network and deliver encryption keys using an 802.1X-capable RADIUS server. If you do not already have a RADIUS server, consult this tip. Otherwise, try the following:

- Reconfigure your AP or router and server with a matching RADIUS secret.
- Reconfigure your RADIUS server to accept requests from your AP or router.
- Use ping to verify AP or router-to-RADIUS server network reachability.
- Watch LAN packet counters to verify that RADIUS is being sent, or use a LAN analyzer debug RADIUS protocol issues.

In this e-guide



In this e-guide

Step 9: Check 802.1X EAP and user login

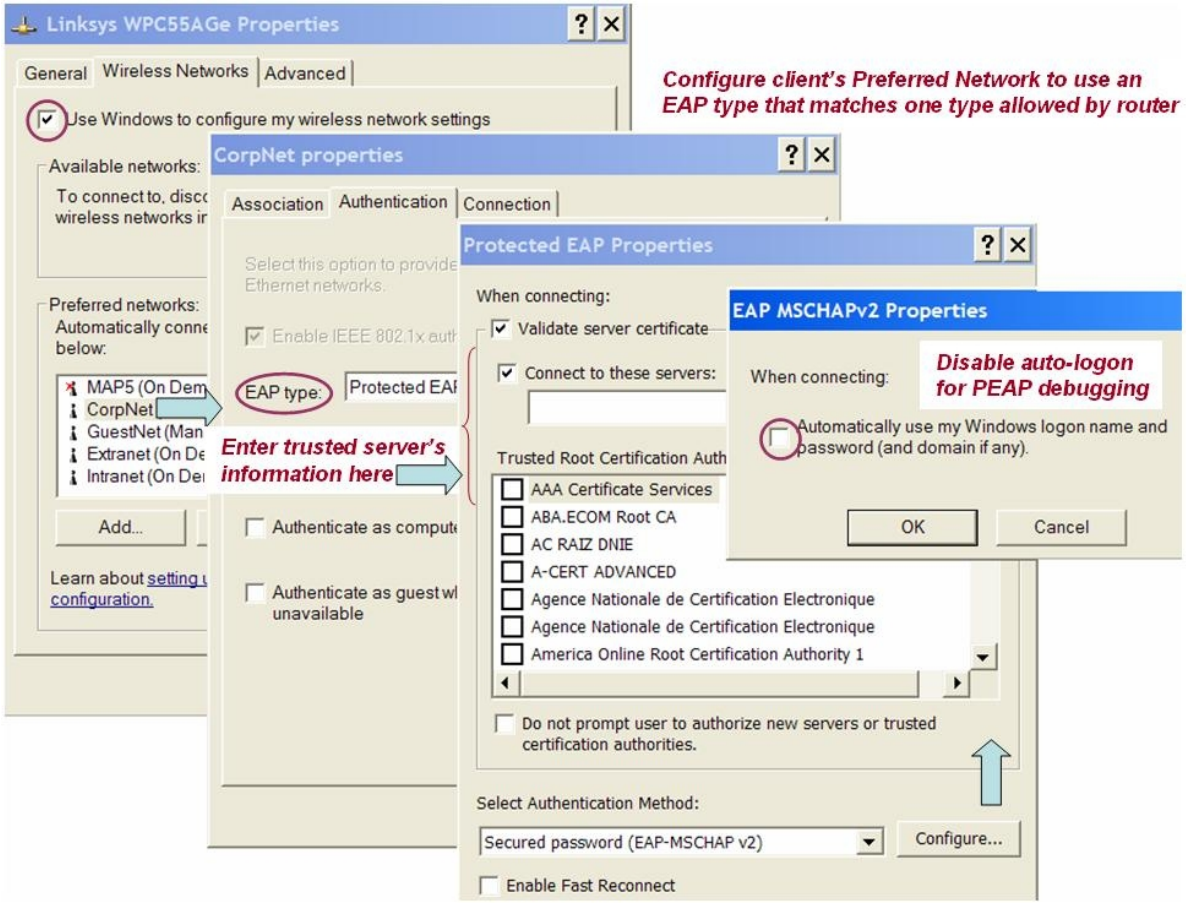
If RADIUS is working but the client's access requests are rejected, look for an 802.1X Extensible Authentication Protocol (EAP) or user login problem.

Your client must support one of the EAP types your server requires and must supply a valid login and password, token, certificate or other kind of credential.

- If your server requires EAP-TLS, select *Smart Card or other Certificate* on the client's Network Properties/Authentication panel.
- If your server requires PEAP, select *Protected EAP* on that panel.
- If your server requires EAP-TTLS or EAP-FAST, install a third-party 802.1X Supplicant program like Cisco's Trust Agent on the client.
- Make sure that client and server EAP-specific properties match, including server certificate Trusted Root Authority, server domain name (optional) and tunneled authentication method (e.g., EAP-MSCHAPv2, EAP-GTC).
- If you are prompted to accept the server's certificate at connect time, examine the certificate carefully, verifying issuer and identity. Never add an unrecognized or suspicious certificate to your trusted list.
- If EAP-TLS problems persist, use a Web browser to inspect the client's certificate and make sure the certificate is valid (e.g., not expired).
- If PEAP problems persist, use CHAP Configure to prevent Windows auto-logon and enter a valid username and password when prompted.

In this e-guide

- If you still haven't spotted the problem, consult your RADIUS server's 802.1X documentation for EAP configuration and debugging hints.



In this e-guide

Step 10: Check intermittent network connectivity issues

Finally, if your wireless client connects and pings successfully, but encounters intermittent network connectivity problems (e.g., some pings work, some fail), you may be experiencing poor signal strength, RF interference, or disconnection caused by AP roaming. See our *Fixing wireless LAN problems* tip for troubleshooting hints.

http://searchnetworking.techtarget.com/feature/Balancing-wireless-LAN-troubleshooting-strategies-for-BYOD

Next article

In this e-guide

Related Content

Check out more of our top tips on Wi-Fi troubleshooting.

How to Troubleshoot Android Wi-Fi Connection Problems

Android smartphone and tablet users now abound in the enterprise, making Android Wi-Fi connection troubleshooting a key element of enterprise wireless network connection management.

How to Troubleshoot iPad and iPhone Wi-Fi Connection Problems

As iPhone and iPad Wi-Fi clients proliferate in the enterprise, IT must troubleshoot Wi-Fi connection problems. Here's how to solve basic iPhone and iPad connection problems.

Discover more at http://SearchNetworking.com/

Images; Fotalia