

10 Steps to Troubleshooting Wi-Fi Connectivity



In this e-guide

10 steps to troubleshoot wireless connection problems p. 2

Related Content p. 22

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 p. 2

Related Content p. 22

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

■ [10 steps to troubleshoot wireless connection problems](#) p. 2

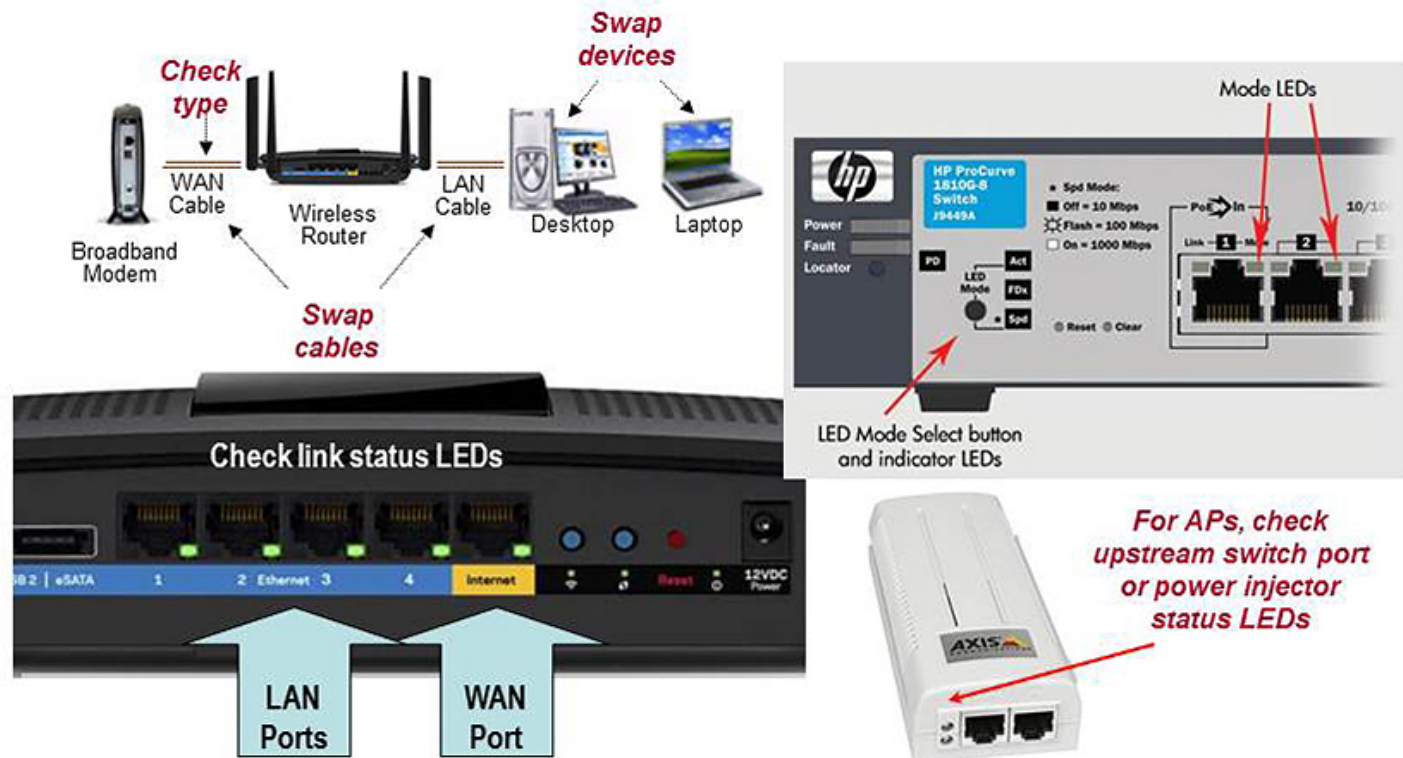
■ [Related Content](#) p. 22

- 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

10 steps to troubleshoot wireless connection problems p. 2

Related Content p. 22



In this e-guide

10 steps to troubleshoot wireless connection problems p. 2

Related Content p. 22

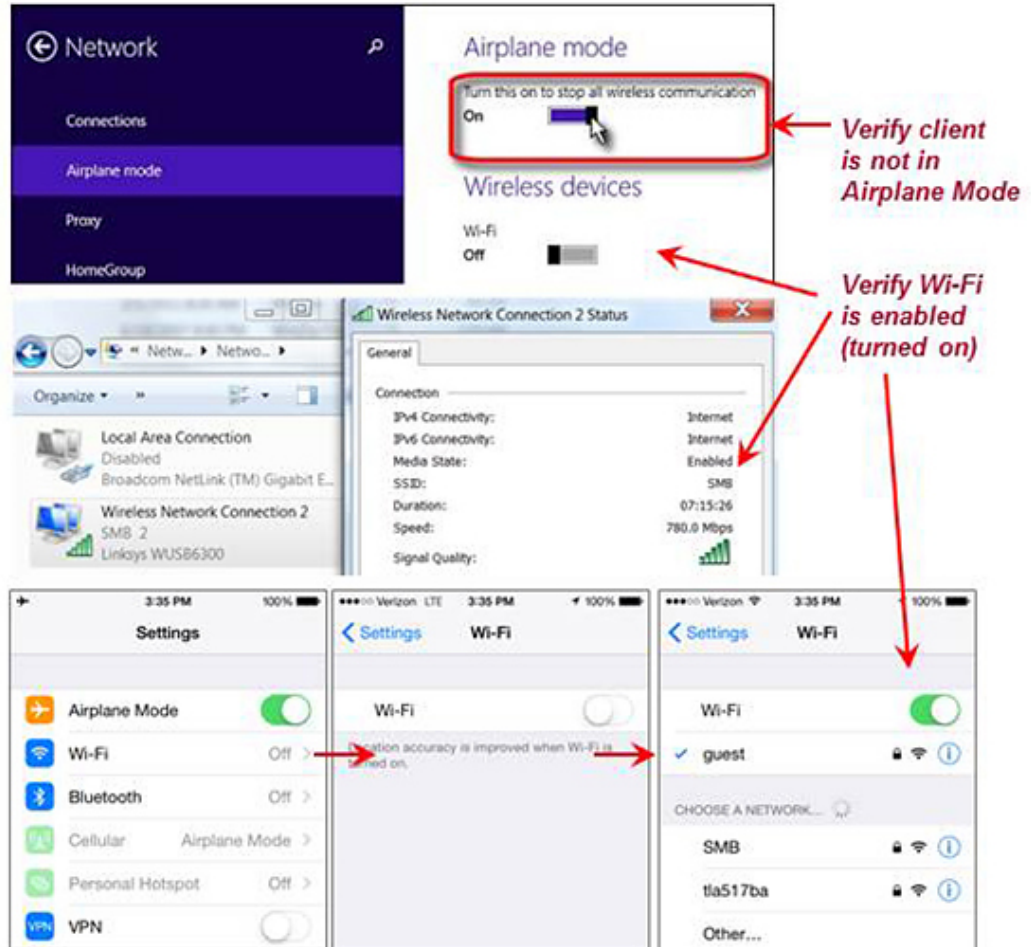
Step 2: Verify wireless adapter

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

- 10 steps to troubleshoot wireless connection problems p. 2
- Related Content p. 22



In this e-guide

■ [10 steps to troubleshoot wireless connection problems](#) p. 2

■ [Related Content](#) p. 22

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

10 steps to troubleshoot wireless connection problems p. 2

Related Content p. 22

System Details

<table border="0"> <tr><td>System</td><td></td></tr> <tr><td>Host Name</td><td>AH-AP230-S</td></tr> <tr><td>MGT0 IP Address</td><td>10.0.0.6</td></tr> <tr><td>Device Model</td><td>AP230</td></tr> <tr><td>HW Type</td><td>AP</td></tr> <tr><td>MAC Address</td><td>9C5D1279C5D127</td></tr> <tr><td>HiveOS Version</td><td>HiveOS 6.4r1d2111</td></tr> </table>	System		Host Name	AH-AP230-S	MGT0 IP Address	10.0.0.6	Device Model	AP230	HW Type	AP	MAC Address	9C5D1279C5D127	HiveOS Version	HiveOS 6.4r1d2111	<table border="0"> <tr><td>System Overview</td><td></td></tr> <tr><td>Alarm</td><td>✔</td></tr> <tr><td>Management Status</td><td>Managed</td></tr> <tr><td>Origin</td><td>Discovered</td></tr> <tr><td>Uptime</td><td>7 Days, 1 Hrs 47 Mins 47 Secs</td></tr> <tr><td>Topology Map</td><td>_floor1</td></tr> </table>	System Overview		Alarm	✔	Management Status	Managed	Origin	Discovered	Uptime	7 Days, 1 Hrs 47 Mins 47 Secs	Topology Map	_floor1
System																											
Host Name	AH-AP230-S																										
MGT0 IP Address	10.0.0.6																										
Device Model	AP230																										
HW Type	AP																										
MAC Address	9C5D1279C5D127																										
HiveOS Version	HiveOS 6.4r1d2111																										
System Overview																											
Alarm	✔																										
Management Status	Managed																										
Origin	Discovered																										
Uptime	7 Days, 1 Hrs 47 Mins 47 Secs																										
Topology Map	_floor1																										

Determine AP or router IP address and subnet

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

Verify IP address is allocated when Wi-Fi client is connected

Client Details

MAC Address	Host Name	IP Address	Association Time	Duration	SSID	Authentication Method	Encryption Method	Radio Mode
24A074464465	Judy's- 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

10 steps to troubleshoot wireless connection problems p. 2

Related Content p. 22

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

- 10 steps to troubleshoot wireless connection problems p. 2
- Related Content p. 22

The screenshot shows the Windows Network Connections control panel window and the Wireless Network Connection 2 Status window. Annotations include:

- An arrow pointing to the 'Connect' button in the Network Connections window with the text: *Find and try to connect to your network's name*
- An arrow pointing to the 'Wireless Network Connection 2' icon in the Network Connections window with the text: *Check status*
- An arrow pointing from the 'Details...' button in the Status window to the 'Network Connection Details' pane with the text: *Must be valid IP*

Property	Value
Connection-specific DNS S...	hsd1.nm.comcast.net
Description	Linksys WUSB6300
Physical Address	C8-D7-19-BE-78-6E
DHCP Enabled	Yes
IPv4 Address	10.0.0.4
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Tuesday, June 30, 2015
Lease Expires	Tuesday, July 07, 2015
IPv4 Default Gateway	10.0.0.1
IPv4 DHCP Server	10.0.0.1
IPv4 DNS Servers	75.75.75.75 75.75.76.76

If IP is not in AP or router's subnet, Diagnose

In this e-guide

10 steps to troubleshoot wireless connection problems p. 2

Related Content p. 22

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

- 10 steps to troubleshoot wireless connection problems p. 2
- Related Content p. 22

Command Prompt - ipconfig

```

C:\>ipconfig

Windows IP Configuration

Wireless LAN adapter Wireless Network Connection 3:

    Media State . . . . . : Media disconnected
    Connection-specific DNS Suffix . . . . . :

Wireless LAN adapter Wireless Network Connection 2:

    Connection-specific DNS Suffix . . . . . : hsd1.nm.comcast.net.
    IPv6 Address. . . . . : 2601:0:f81:6a92:39bd:9f4d:4478:b82
    Temporary IPv6 Address. . . . . : 2601:0:f81:6a92:fs24:db49:f95:a8e0
    Link-local IPv6 Address . . . . . : fe80::39bd:9f4d:4478:b82%14
    IPv4 Address. . . . . : 10.0.0.4
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::ce94:62ff:feda:fcf1%14
    10.0.0.1
    
```

Command Prompt - Ping 10.0.0.1

```

C:\>ping 10.0.0.1

Pinging 10.0.0.1 with 32 bytes of data:
Reply from 10.0.0.1: bytes=32 time=5ms TTL=64
Reply from 10.0.0.1: bytes=32 time=3ms TTL=64
Reply from 10.0.0.1: bytes=32 time=3ms TTL=64
Reply from 10.0.0.1: bytes=32 time=3ms TTL=64

Ping statistics for 10.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 3ms, Maximum = 5ms, Average = 3ms
    
```

Ping AP or Router's LAN IP – this one is successful

Command Prompt - Ping 10.0.0.25

```

C:\>ping 10.0.0.25

Pinging 10.0.0.25 with 32 bytes of data:
Reply from 10.0.0.4: Destination host unreachable.
Reply from 10.0.0.4: Destination host unreachable.
Reply from 10.0.0.4: Destination host unreachable.
Reply from 10.0.0.4: Destination host unreachable.

Ping statistics for 10.0.0.25:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    
```

Ping another client's IP – this one is blocked

Windows Firewall - Inbound Rules

Name	Group	Profile	Enabled	Action
File and Printer Sharing (Echo Request - ICMPv4-...)	File and Printer Sharing	Domain	No	Allow
File and Printer Sharing (Echo Request - ICMPv4-...)	File and Printer Sharing	Public	Yes	Allow
File and Printer Sharing (Echo Request - ICMPv4-...)	File and Printer Sharing	Private	Yes	Allow
File and Printer Sharing (Echo Request - ICMPv6-...)	File and Printer Sharing	Domain	No	Allow
File and Printer Sharing (Echo Request - ICMPv6-...)	File and Printer Sharing	Public	Yes	Allow
File and Printer Sharing (Echo Request - ICMPv6-...)	File and Printer Sharing	Private	Yes	Allow

If Windows firewall is blocking traffic, reconfigure to permit desired exceptions such as file and printer sharing

In this e-guide

10 steps to troubleshoot wireless connection problems p. 2

Related Content p. 22

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

10 steps to troubleshoot wireless connection problems p. 2

Related Content p. 22

Optional Settings

▼ Radio and Rates

2.4 GHz 11b/g Rate Setting

Customize 2.4 GHz 11b/g Rate Setting

1 Mbps	Basic	12 Mbps	Optional
2 Mbps	Basic	18 Mbps	Optional
5.5 Mbps	Basic	24 Mbps	Optional
6 Mbps	Optional	36 Mbps	Optional
9 Mbps	Optional	48 Mbps	Optional
11 Mbps	Basic	54 Mbps	Optional

5.0 GHz 11a Rate Setting

Customize 5.0 GHz 11a Rate Setting

6 Mbps	Basic	24 Mbps	Basic
9 Mbps	Optional	36 Mbps	Optional
12 Mbps	Basic	48 Mbps	Optional
18 Mbps	Optional	54 Mbps	Optional

2.4 GHz and 5.0 GHz 11n MCS Rate Setting

Customize 2.4 GHz and 5.0 GHz 11n MCS Rate Setting

MCS 0	Optional	MCS 8	Optional	MCS 16	Optional
MCS 1	Optional	MCS 9	Optional	MCS 17	Optional
MCS 2	Optional	MCS 10	Optional	MCS 18	Optional
MCS 3	Optional	MCS 11	Optional	MCS 19	Optional
MCS 4	Optional	MCS 12	Optional	MCS 20	Optional
MCS 5	Optional	MCS 13	Optional	MCS 21	Optional
MCS 6	Optional	MCS 14	Optional	MCS 22	Optional
MCS 7	Optional	MCS 15	Optional	MCS 23	Optional

Choose compatible standard(s) and MCS rates to match your 802.11 clients (b, g, a, n, or ac)

On some products, this may be called "Mixed Mode"

▼ Advanced

Configuration Settings

Maximum Client Limit	100	(1-100)	Inactive Client Ageout	5	(1-30 minutes)
RTS Threshold	2346	(1-2346 bytes)	Roaming Cache Update Interval	60	(10-36000 seconds)
Fragment Threshold	2346	(256-2346 bytes)	Roaming Cache Ageout	60	(1-1000)
DTIM Setting	1	(1-255)			

Ignore broadcast probe requests

Hide SSID (Stealth) Broadcasting SSID helps clients find AP or router

Disable 802.11n high throughput capabilities to support incompatible 802.11b/g/a clients

In this e-guide

■ [10 steps to troubleshoot wireless connection problems](#) p. 2

■ [Related Content](#) p. 22

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

- 10 steps to troubleshoot wireless connection problems p. 2
- Related Content p. 22

- 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.

The image shows a network configuration interface for an SSID named 'guest'. The 'SSID Access Security' section is set to 'WPA/WPA2 PSK (Personal)'. The 'Key Management' is 'WPA2-(WPA2 Personal)-PSK', 'Encryption Method' is 'CCMP (AES)', and 'Key Type' is 'ASCII Key'. A text box explains: 'WPA-Personal = WPA-PSK = WPA-Pre-Shared Key' and 'WPA-Enterprise = WPA = WPA RADIUS'. Another text box states: 'The WPA version (WPA or WPA2) must also match WPA uses TKIP encryption; WPA2 uses AES'. A third text box notes: 'Match all of the AP or router's security parameters, including passphrase (key) capitalization'. Below, a 'Connect to a Network' dialog shows the security key 'matchMeExactly'. To the right, the 'SMB Wireless Network Properties' window shows 'Security type' set to 'WPA2-Personal', 'Encryption type' set to 'AES', and the 'Network security key' field with the same passphrase 'matchMeExactly'. Arrows point from the text boxes to the corresponding settings in the client window.

In this e-guide

■ [10 steps to troubleshoot wireless connection problems](#) p. 2

■ [Related Content](#) p. 22

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

10 steps to troubleshoot wireless connection problems p. 2

Related Content p. 22

The screenshot displays the Colubris Management Tool interface for an MSC-3300. The 'Add/Edit RADIUS profile' window is open, showing the configuration for a profile named 'MyRADIUS'. The 'Primary RADIUS server' section is configured with the following details:

- Server address: 192.168.20.20
- Alias address: (empty)
- Secret: *****
- Confirm secret: *****

The 'Settings' section shows the following configuration:

- Authentication port: 1812
- Accounting port: 1813
- Retry interval: 10 seconds
- Retry timeout: 60 seconds

Overlaid on the RADIUS configuration is a red text box that reads: **Configure server's IP, port, & secret into router**. Another red text box is overlaid on the authentication port field, reading: **Watch counters, analyze packets, & examine trace logs to determine how far RADIUS gets**.

To the right, the 'Linksys WPC55A Ge Status' window shows the connection status. The status is 'Validating identity', which is circled in red. A red text box overlaid on this status reads: **If client gets stuck in this state, then check RADIUS...**. The activity section shows 20,075 packets sent and 39 packets received.

At the bottom, a 'WZCTrace.LOG - Notepad' window displays the following log entries:

```
:45:19:281: [StateIterateFn(0x05C2AC78)]
:45:19:281: Plumbing config 0
:45:19:281: [MemFree(0x00000000)]
:45:19:281: [WzcNetmanNotify(0x05C2AC78)]
:45:19:281: WzcNetmanNotify]=0
:45:19:281: WZCISameNetwork: Flags=<110/110> => <7:32>:<CorpNet/_
:45:19:281: Requesting the release of the DHCP lease
:45:19:281: [LstSetSelectedConfig(0x05C2AC78..)]
:45:19:281: [DevioSetIntfOIDs(0x05C2AC78, 0x00EEFDCC)]
:45:19:281: [DevioSetEnumOID(0x1bb8, 0xd010108, 1)]
```

In this e-guide

10 steps to troubleshoot wireless connection problems p. 2

Related Content p. 22

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

- 10 steps to troubleshoot wireless connection problems p. 2
- Related Content p. 22

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

Configure client's Preferred Network to use an EAP type that matches one type allowed by router

Disable auto-logout for PEAP debugging

Enter trusted server's information here

//////
In this e-guide

■ 10 steps to troubleshoot wireless connection problems p. 2

■ Related Content p. 22

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

10 steps to troubleshoot wireless connection problems p. 2

Related Content p. 22

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; Fotolia

©2017 TechTarget. No part of this publication may be transmitted or reproduced in any form or by any means without written permission from the publisher.