

Fehlerbehebung in einem herkömmlichen Cisco Wireless-Netzwerk

Ziel

In diesem Dokument werden einige Bereiche beschrieben, die bei der Fehlerbehebung für ein herkömmliches Cisco Wireless-Netzwerk analysiert werden müssen. Wenn Sie ein Mesh-Netzwerk verwenden, sehen Sie unter [Fehlerbehebung für ein Cisco Business Wireless Mesh Network nach](#).

Unterstützte Geräte | Softwareversion

- WAP121 | 1.0.6.8 ([neueste Version herunterladen](#))
- WAP125 | 1.0.3.1 ([zuletzt heruntergeladen](#))
- WAP131 | 1.0.2.17 ([zuletzt heruntergeladen](#))
- WAP150 | 1.1.2.4 ([zuletzt heruntergeladen](#))
- WAP361 | 1.1.2.4 ([zuletzt heruntergeladen](#))
- WAP371 | 1.3.0.7 ([neueste Version herunterladen](#))
- WAP551 | 1.2.1.6 ([zuletzt heruntergeladen](#))
- WAP561 | 1.2.1.7 ([neueste Version herunterladen](#))
- WAP571 | 1.1.0.3 ([neueste Version herunterladen](#))
- WAP571E | 1.1.0.3 ([neueste Version herunterladen](#))
- WAP581 | 1.0.3.1 ([zuletzt heruntergeladen](#))

Inhalt

- [Für optimale Leistung und Zuverlässigkeit sollten Sie diese berücksichtigen!](#)
- [Verbindungsprobleme? Beginnen Sie mit den Grundlagen](#)
 - [Überprüfen Sie die Gehäusetechnik und Umgebungsbedingungen.](#)
 - [Weitere zu berücksichtigende Elemente](#)
 - [Anzahl der SSIDs](#)
- [Verbindungsprobleme prüfen](#)
 - [Ausführen von Verbindungstests über die Webbenutzeroberfläche \(UI\)](#)
 - [Könnte das Problem DHCP-Probleme sein?](#)
 - [Tipps zur Verfügbarkeit der ARP-Tabelle für die DHCP-IP-Adressierung Windows-Unterstützung](#)
- [Spezifische Standardeinstellungen ändern](#)
 - [Neubewertung der Kanalzuweisung](#)
 - [Maximaler Auslastungsgrenzwert](#)
 - [Funkeinstellungen](#)
- [Überlegungen zu Interferenzen](#)
 - [Mögliche Interferenzprobleme](#)
 - [Signal-Rausch-Verhältnis \(SNR\)](#)
- [Hinter dem Vorhang](#)
 - [Syslogs](#)
 - [Paketerfassung](#)
- [Wenn alle anderen Fehler auftreten, setzen Sie die Standardeinstellungen auf die Werkseinstellungen zurück.](#)

Einführung

Mesh-Wireless-Netzwerke sind fantastisch, aber lassen Sie uns ehrlich sein: Dinge passieren! Ähnlich wie bei jedem Wireless-Netzwerk können auch einige Dinge Probleme verursachen. Manchmal gibt es eine einfache Lösung, während andere komplizierter sein können.

Für optimale Leistung und Zuverlässigkeit sollten Sie diese berücksichtigen!

1. Stellen Sie sicher, dass der Bereich die erwartete Anzahl von Clients und deren Anwendungen vollständig abdeckt. Möglicherweise müssen zusätzliche Wireless Access Points hinzugefügt werden, um die Leistung in Ihrer gesamten Wireless-Infrastruktur zu optimieren.
2. Achten Sie darauf, welche Anwendungstypen sie möglicherweise verwenden (oder als Administrator, welche Anwendungstypen Sie zulassen können).
3. Clients, auf denen Video-Streaming-Anwendungen ausgeführt werden, benötigen mehr Bandbreite als Clients, die nur Audio-Streaming-Programme übertragen. Videoanwendungen basieren auf Pufferung, um ein anständiges Erlebnis zu bieten.
4. Clients, die Anwendungen für die Sprachkommunikation ausführen, benötigen einen sofortigen Service ohne Verzögerungen, ohne dabei die erforderliche Bandbreite beanspruchen zu müssen. Da bei einem Sprachanruf keine Pufferung erfolgt, ist es sehr wichtig, dass Pakete nicht verworfen werden.

Sind Sie bereit für eine Fehlerbehebung? Lass uns eingraben!

Verbindungsprobleme? Beginnen Sie mit den Grundlagen

Überprüfen Sie die Gehäusetechnik und Umgebungsbedingungen.

Dies ist die einfachste Methode zur Fehlerbehebung, wird jedoch häufig übersehen. Auch wenn diese scheinbar offensichtlich sind, ist es gut, mit den Grundlagen zu beginnen.

1. Gibt es Macht für alles?
2. Ist das gesamte Gerät eingeschaltet?
3. Sind die Kabel richtig angeschlossen?
4. Haben Sie durchgängig eine Verbindungsleuchte?
5. Könnte es ein schlechtes Kabel sein?
6. Ist irgendein Gerät überhitzt?
7. Könnte es Umweltfaktoren geben, z. B. wo es sich befindet?
8. Gibt es zwischen dem Access Point und dem Wireless-Gerät Metallwände oder dicke Mauern?
9. Kann der Client außerhalb des Empfangsbereichs liegen, wenn er keine Verbindung herstellen kann?

Weitere zu berücksichtigende Elemente

1. Starten Sie den Access Point neu.
2. Überprüfen Sie bei APs, die mit einem Switch verbunden sind, die Switch-Konfiguration, und überprüfen Sie, ob der Switch ordnungsgemäß funktioniert. Die CPU-Auslastung, die Temperatur und die Speichernutzung sollten unter den angegebenen Schwellenwerten

liegen.

3. Überprüfen Sie auf der Webbenutzeroberfläche unter *Überwachung* das *Wireless Dashboard*, um Informationen über Leistung und andere Probleme zu sammeln.
4. Stellen Sie sicher, dass auf allen Geräten die neueste Version der Firmware ausgeführt wird.
5. Aktivieren Sie *Bonjour* und *Link Layer Discovery Protocol (LLDP)* auf dem Router, sofern diese verfügbar sind.
6. Aktivieren Sie *Wireless Multicast Forwarding*, wenn diese für Spiele- und Streaming-Anwendungen verfügbar ist.
7. *Bandbreitennutzung* deaktivieren.

Anzahl der SSIDs

Jeder Service Set Identifier (SSID) erfordert das Senden eines Beacon-Frames alle 100 Millisekunden (ms), was eine hohe Kanalauslastung verursachen kann.

Es empfiehlt sich, die Gesamtzahl der SSIDs auf dem Access Point auf 1-2 SSIDs pro Funkmodul oder, wenn möglich, pro Access Point zu begrenzen.

Verbindungsprobleme prüfen

Ausführen von Verbindungstests über die Webbenutzeroberfläche (UI)

Der Access Point muss mit anderen Geräten kommunizieren können, um effektiv zu sein. Eine einfache Möglichkeit, dies zu überprüfen, besteht darin, einen Ping auszuführen.

Pingen Sie den Access Point von mindestens zwei Clients, die mit diesem Access Point verbunden (verbunden) sind. Auf die Administrationsmenüs dieses Access Points zugreifen, um zu bestimmen, welche Clients direkt verbunden sind.

Pingen Sie vom Router an die IP-Adresse des Access Points, um festzustellen, ob eine End-to-End-Verbindung verfügbar ist. Pingen Sie vom Router an die Wireless-Clients, die dem Access Point zugeordnet sind, um zu überprüfen, ob sie vom Hauptnetzwerk aus erreichbar sind.

Weitere Informationen zum Ping-Befehl erhalten Sie, wenn Sie auf den entsprechenden Link klicken:

- [Ping-, Traceroute- und DNS-Suche am RV160 und RV260](#)
- [DNS-Namenssuche und Ping-Test auf den VPN-Routern der Serien RV320 und RV325](#)
- [Führen Sie eine Diagnose für einen Router der Serie RV34x durch.](#)

Könnte das Problem DHCP-Probleme sein?

Stellen Sie sicher, dass der DHCP-Server betriebsbereit ist und über das Local Area Network (LAN) des AP erreichbar ist.

Es ist möglich, dass mehr Clients eine IP-Adresse benötigen, als im DHCP-Pool verfügbar sind. Weitere Informationen finden Sie im Abschnitt *Anzeigen oder Ändern des Pools von IP-Adressen für DHCP* im Artikel [Best Practices für das Festlegen statischer IP-Adressen auf Cisco Business Hardware](#).

Es kann vorkommen, dass zu viele DHCP-Adressen zwischengespeichert werden, was Clients auch daran hindern kann, eine IP-Adresse zu erhalten. Weitere Informationen hierzu finden Sie

unter

[Tipps zur Verfügbarkeit der ARP-Tabelle für die DHCP-IP-Adressierung](#) Windows-Unterstützung

Wenn Windows, wählen Sie Ihre Wireless-Verbindung aus dem Bereich Netzwerkverbindungen aus, und überprüfen Sie, ob ihr Status "Enabled" (Aktiviert) lautet.

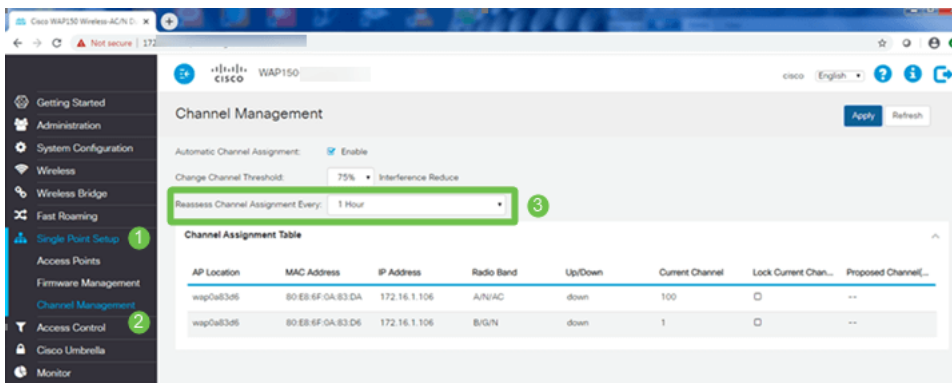
Ausführliche Informationen zur Fehlerbehebung bei Wireless-Netzwerkverbindungen finden Sie im Microsoft Support Forum unter folgender URL: [Beheben Sie Wi-Fi-Verbindungsprobleme in Windows](#).

Spezifische Standardeinstellungen ändern

Es gibt einige Standardeinstellungen, die Verbindungsprobleme verursachen können. Sie können versuchen, die folgenden Einstellungen zu ändern.

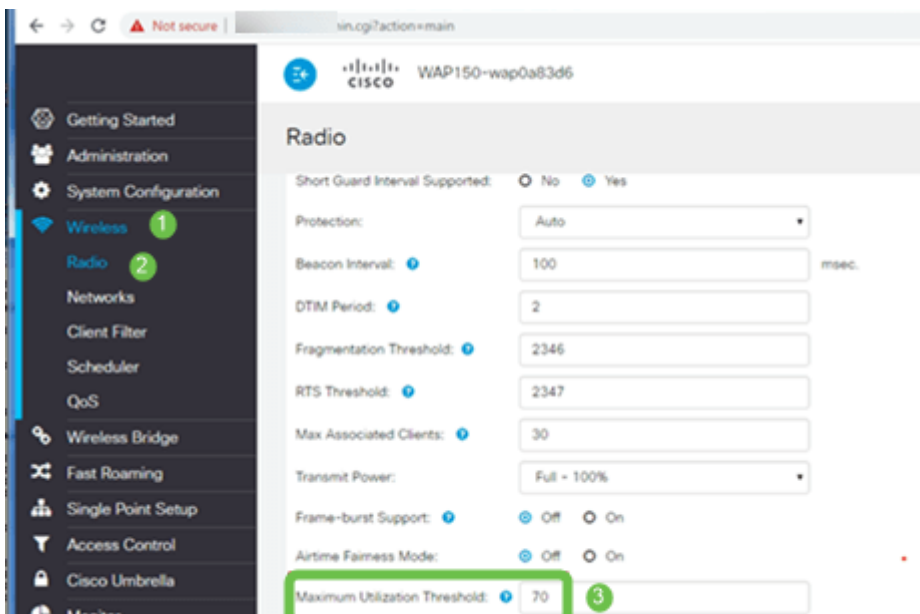
Neubewertung der Kanaluweisung

Navigieren Sie zur Seite **Single-Point-Einrichtung** > **Channel-Management**. Passen Sie unter *Kanaluweisung neu bewerten* den Standardwert von *1 Stunde* entweder *alle 12 Stunden* oder *1 Mal am Tag an*. Dadurch wird eine häufige Neuwahl des Kanals vermieden (wodurch WLAN-Client-Neuzuordnungen alle 1 Stunde erzwungen werden).



Maximaler Auslastungsgrenzwert

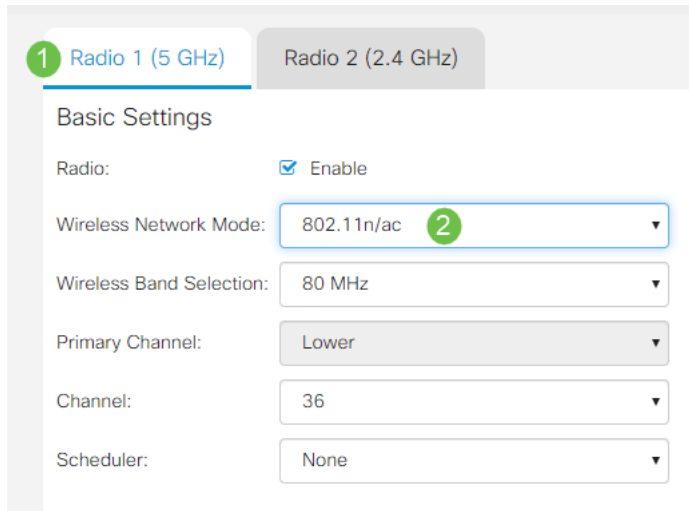
Navigieren Sie zu **Wireless** > **Radio**. Sie befinden sich automatisch unter *Radio 1 (5 GHz)*. Unter *Maximaler Auslastungsgrenzwert* sollte der Standardwert von *70* auf *0* geändert werden.



Funkeinstellungen

Lassen Sie die *Seite Radio (Funkübertragung)* unter *Radio 1 (5 GHz)* geöffnet.

Legen Sie *den Wireless-Netzwerkmodus* auf **802.11n/ac** fest.



1 Radio 1 (5 GHz) Radio 2 (2.4 GHz)

Basic Settings

Radio: Enable

Wireless Network Mode: 802.11n/ac 2

Wireless Band Selection: 80 MHz

Primary Channel: Lower

Channel: 36

Scheduler: None

Scrollen Sie nach unten zu *Erweiterte Einstellungen*, und legen Sie die folgenden Konfigurationen fest:

- Legen Sie unter *Max Associated Clients* den Standardwert von *200* auf **55** oder weniger fest. Bei großen Bereitstellungen, bei denen mehr als 20 Clients im gleichen Abdeckungsbereich Wireless-Verbindungen verwenden können, überprüfen Sie im Datenblatt das verwendete Access Point-Modell, um die maximale Anzahl gleichzeitig auf diesem AP unterstützter Wireless-Clients zu überprüfen. Wenn der Access Point die maximale Unterstützung für Wireless-Clients überschreiten kann, sollten Sie in Betracht ziehen, weitere APs im Abdeckungsbereich hinzuzufügen und die Anzahl der Clients zu begrenzen, die ein einzelner Access Point unterstützt
- Ändern Sie die *Fixed Multicast-Rate* auf **6**.
- Deaktivieren Sie unter *Legacy Rate Sets* für *Unterstützte* und *Basic* die Option **6** und **9 Mbit/s**.
- Aktivieren Sie unter *Legacy Rate Sets* für *Basic (Grundlegende)* **24** und **54**.

Advanced Settings 1

DFS Support: On

Short Guard Interval Supported: Yes

Protection: Auto

Beacon Interval: 100 msec.

DTIM Period: 2

Fragmentation Threshold: 2346

RTS Threshold: 65535

Max Associated Clients: 55 2

Transmit Power: Full - 100%

Frame-burst Support: Off

Airtime Fairness Mode: Off

Maximum Utilization Threshold: 0

Fixed Multicast Rate: 6 3 Mbps

Legacy Rate Sets:

Rate (Mbps)	54	48	36	24	18	12	9	6
Supported	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Basic	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Lassen Sie die Seite *Radio (Funkmodul)* geöffnet, und wählen Sie *Radio 2 (2,4 GHz)*.

Stellen Sie *den Wireless-Netzwerkmodus* auf **2,4 GHz 802.11n** und *Wireless-Frequenzauswahl* auf **20 MHz** ein.

Radio 1 (5 GHz) Radio 2 (2.4 GHz) 1

Basic Settings

Radio: Enable

Wireless Network Mode: 2.4 GHz 802.11n 2

Wireless Band Selection: 20 MHz 3

Primary Channel: Lower

Channel: 6

Scheduler: None

Scrollen Sie nach unten zu *Erweiterte Einstellungen*, und legen Sie die folgenden Konfigurationen fest:

- Legen Sie unter *Max Associated Clients* den Standardwert von 200 auf **55** oder weniger fest.
- Ändern Sie die *Fixed Multicast-Rate* auf **6**.
- Deaktivieren Sie unter *Ältere Ratensätze* für *Unterstützte* und *Basic* die Optionen **1, 2, 5.5, 6, 9** und **11**. Mbit/s
- Aktivieren Sie unter *Legacy Rate Sets* für *Basic* **12,24** und **54**.

Advanced Settings 1

Short Guard Interval Supported: Yes

Protection: Auto

Beacon Interval: 100 msec.

Überlegungen zu Interferenzen

Mögliche Interferenzprobleme

Interferenzen können Probleme in Wireless-Netzwerken verursachen und aus mehr Quellen als je zuvor stammen. Mikrowellen, Sicherheitskameras, Smartwatches, Bewegungsmelder oder sogar Leuchtstofflampen können Interferenzen verursachen.

Wie stark sie sich auf das Netzwerk auswirken, kann von vielen Faktoren abhängen, darunter von der Menge an ausgestrahlter Leistung, wenn das Objekt ständig eingeschaltet ist oder intermittierend ist. Je stärker das Signal ist oder je häufiger es auf die Probleme zutrifft, die auftreten können.

Nicht autorisierte APs und nicht autorisierte Clients können Probleme verursachen, wenn zu viele auf demselben Kanal vorhanden sind. Voice over IP und Video-Streaming können ebenfalls Probleme verursachen.

Interferenzen können die Leistung von Wireless-Netzwerken erheblich beeinträchtigen und Sicherheitsschwachstellen und Instabilität in Wireless-Netzwerken verursachen.

Wenn Sie mehr über die Ursachen von Interferenzen erfahren möchten, lesen Sie die folgenden Artikel:

- [Verwalten der Liste nicht autorisierter APs auf dem WAP125 oder WAP581 Access Point](#)
- [Konfigurieren der grundlegenden Funkeinstellungen des WAP581](#)
- [Aktivieren des Spektrumanalysemodus auf einem WAP581-Access Point](#)
- [Tipps für die Single-Point-Einrichtung eines WAP581](#)
- [Konfigurieren der erweiterten Funkeinstellungen auf dem WAP125 und dem WAP581](#)

Signal-Rausch-Verhältnis (SNR)

Bei Echtzeitanwendungen wie Sprache oder Video wird für Datenanwendungen eine SNR von mindestens 25 dB gegenüber einer SNR von 20 dB empfohlen.

Bei einem Standard-Rauschpegel von -92 dBm entspricht ein SNR von 25 dB = -67 dBm Signalstärke-Indikator (RSSI).

Navigieren Sie zu **Monitoring > Wireless Dashboard** auf der Webbenutzeroberfläche, um das Innere Ihres Netzwerks anzuzeigen.

Das folgende Diagramm zeigt den RSSI-Wert für akzeptable Signalstärken.

Signalstärke	Bewertung	Beschreibung	Erforderliche Verwendung
-30 dBm	Erstaunlich	Maximal erreichbare Signalstärke. Der Client kann nur wenige Meter vom Access Point entfernt sein, um dies zu erreichen. Nicht typisch in der realen Welt.	–
-67 dBm	Sehr gut	Mindestsignalstärke für Anwendungen, die eine sehr zuverlässige und zeitgerechte Bereitstellung von Datenpaketen erfordern.	Voice-over-IP, Voice-over-Wi-Fi und Video-Streaming

-70 dBm	OK	Mindestsignalstärke für eine zuverlässige Paketübermittlung	E-Mail, Web
-80 dBm	Nicht gut	Mindestsignalstärke für grundlegende Verbindungen. Die Paketübermittlung kann unzuverlässig sein. Kommen oder ertrinken Sie im Lärm.	–
-90 dBm	Unbrauchbar	Jede Funktionalität ist sehr unwahrscheinlich.	–

Hinter dem Vorhang

Syslogs

Wenn Sie sich über Ereignisse im Klaren sind, können Sie einen reibungslosen Netzwerkbetrieb sicherstellen und Ausfälle verhindern. Syslogs sind nützlich für die Fehlerbehebung im Netzwerk, das Debuggen des Paketflusses und die Überwachung von Ereignissen.

Diese Protokolle können auf der Webbenutzeroberfläche des Master Access Points und, falls konfiguriert, auf Remote-Protokollservern angezeigt werden. Ereignisse werden normalerweise beim Neustart aus dem System gelöscht, wenn sie nicht auf einem Remote-Server gespeichert werden.

Weitere Informationen finden Sie in den folgenden Artikeln:

- [Konfigurieren der Systemprotokolleinstellungen auf dem Router der Serie RV34x](#)
- [Verwalten der Systemprotokolle \(Syslogs\) auf einem Router der Serie RV34x](#)
- [Konfigurieren der Remoteprotokollierung auf den Routern RV160 und RV260](#)
- [Anzeigen von Protokollen auf einem Router der RV-Serie](#)
- [Konfiguration des Systemprotokolls auf den VPN-Routern der Serien RV320 und RV325](#)

Paketerfassung

Eine Paketerfassung, auch als PCAP-Datei bezeichnet, ist ein Tool, das bei der Fehlerbehebung hilfreich sein kann. Es zeichnet jedes Paket auf, das zwischen Geräten in Ihrem Netzwerk gesendet wird, in Echtzeit. Durch das Erfassen von Paketen können Sie die Details des Netzwerkverkehrs eingehend untersuchen. Dies kann alles von Geräteverhandlung, Protokoll-Kommunikation, fehlgeschlagener Authentifizierung und vertraulicher Datenübertragung umfassen. Sie können den Pfad bestimmter Datenverkehrsflüsse und jede Interaktion zwischen Geräten in ausgewählten Netzwerken sehen. Diese Pakete können bei Bedarf zur weiteren Analyse gespeichert werden. Es ist wie eine Röntgenaufnahme der Paketübertragung im Netzwerk.

Weitere Informationen finden Sie in den folgenden Artikeln:

- [Verwenden von Wireshark auf einem Cisco Business WAP für die Paketanalyse: Direkter Stream zu Wireshark](#)
- [Integration von Cloudshark für die Paketanalyse auf einem WAP125 oder WAP581](#)
- [Konfigurieren der Paketerfassung auf einem WAP125 oder WAP581 Access Point](#)
- [Konfigurieren der Paketerfassung auf dem WAP125](#)

Wenn alle anderen Fehler auftreten, setzen Sie die

Standardeinstellungen auf die Werkseinstellungen zurück.

Eine Option der letzten Instanz, die nur getan werden sollte, um die schwerwiegendsten Probleme wie den Verlust des Zugriffs auf das Management-Portal zu beheben, ist ein Zurücksetzen der Hardware auf den Router.

Beim Zurücksetzen auf die Werkseinstellungen gehen alle Konfigurationen verloren. Sie müssen den Router von Grund auf neu einrichten. Vergewissern Sie sich also, dass Sie die Verbindungsdetails zur Hand haben.

Detaillierte Informationen zum Zurücksetzen der Hardware finden Sie im Hardware-Administrationshandbuch.

Wenn Ihr Router-Modell älter als 5 Jahre ist, sollten Sie einen Ersatz durch einen modernen Router in Betracht ziehen, um die neuesten Sicherheits- und Schwachstellenaktualisierungen zu erhalten. Viele ältere Router bieten keine weiteren Entwicklungsanstrengungen, um sie auf dem neuesten Stand zu halten und Patches zu installieren (so wie dies normalerweise bei Ihrem PC der Fall ist).

- [Neustart und Zurücksetzen der Werkseinstellungen auf WAP121- und WAP321-Access Points](#)
- [Neustarten und Zurücksetzen des Wireless Access Points auf die werkseitigen Standardeinstellungen](#)
- [Neustarten und Zurücksetzen des WAP125 und WAP581 auf die werkseitigen Standardeinstellungen](#)
- [Zurücksetzen eines CBW-Zugangspunkts auf die werkseitigen Standardeinstellungen](#)

Fazit

Es ist schwer zu sagen, was Ihnen geholfen hat, Ihre Verbindung zu reparieren, aber diese Toolbox von Optionen hätte den Trick haben sollen!