

Gelegentliche Verbindungsprobleme bei Wireless-Bridges

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Gründe für häufige Verbindungsprobleme bei Wireless-Bridges](#)

[Funkfrequenzstörungen](#)

[Verwenden Sie die Carrier-Testoption in Bridges, um nach RFI zu suchen.](#)

[Einstellungen für die Übertragungsrate der Wireless-Bridges unter optimiert/falsch](#)

[Fresnel-Zonen und Sichtbereich](#)

[Probleme mit der Antennenausrichtung](#)

[Clear Channel Assessment Parameter \(CCA\)](#)

[Weitere Probleme, die die Leistung von Wireless-Bridges beeinträchtigen](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument werden einige der Hauptgründe für gelegentliche Verbindungsprobleme bei Wireless-Brücken erläutert und die Lösung dieser Probleme erläutert.

Voraussetzungen

Anforderungen

Cisco empfiehlt, einige grundlegende Kenntnisse über Wireless Bridges zu erwerben.

Weitere Referenzen zu Wireless-Bridges finden Sie unter [Wireless - Technischer Support und Dokumentation](#).

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco Aironet Wireless Bridges.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips](#)

Gründe für häufige Verbindungsprobleme bei Wireless-Bridges

Im Folgenden sind die häufigsten Gründe für zeitweilige Verbindungsprobleme bei Wireless-Bridges aufgeführt:

1. [Funkfrequenzstörungen](#)
2. [Unoptimal/Falsch eingestellte Datenrateneinstellungen auf den Wireless Bridges](#)
3. [Problembereiche im Umkreis- und Sichtbereich](#)
4. [Probleme mit der Antennenausrichtung](#)
5. [Clear Channel Assessment Parameter \(CCA\)](#)
6. [Weitere Probleme, die die Leistung von Wireless-Bridges beeinträchtigen](#)

Funkfrequenzstörungen

Bei Funkfrequenzstörungen (Radio Frequency Interference, RFI) handelt es sich um unerwünschte störende HF-Signale, die die ursprünglichen Datensignale von Wireless-Geräten stören. RFI in einem Wireless-Netzwerk kann schädliche Auswirkungen haben, z. B. zeitweilige Verbindungsverluste, schlechter Durchsatz und niedrige Datenraten. Es gibt verschiedene Arten von RFI, die in einer Wireless-Netzwerkumgebung auftreten können. Sie müssen diese RFI-Typen vor der Implementierung von Wireless-Netzwerken berücksichtigen. Zu den RFI-Typen zählen Schmalband-RFI, All-Band-RFI und RFI aufgrund ungünstiger Wetterbedingungen.

- **Narrowband-RFI:** Narrowband-Signale können, abhängig von der Frequenz und Signalstärke, gelegentlich RF-Signale von einem Spreadpektrum-Gerät, z. B. einer Wireless-Bridge, unterbrechen oder sogar unterbrechen. Die beste Methode zur Überwindung des Schmalband-RFI besteht darin, die Quelle des Funksignals zu identifizieren. Sie können Spektrumanalysatoren verwenden, um die Quelle des RF-Signals zu identifizieren. Spektrumanalysatoren sind Geräte, mit denen Sie die Stärke von störenden HF-Signalen erkennen und messen können. Wenn Sie die Quelle identifizieren, können Sie entweder die Quelle entfernen, um RFI zu beseitigen, oder die Quelle richtig schützen. Durch Narrowband-Signale werden die ursprünglichen Daten-RF-Signale (von einer Wireless-Bridge) im gesamten RF-Band nicht unterbrochen. Daher können Sie auch einen alternativen Kanal für die Bridge auswählen, wenn keine schmalbandige HF-Interferenz auftritt. Wenn z. B. unerwünschte Funksignale einen Kanal stören (z. B. Kanal 11), können Sie die Wireless Bridge so konfigurieren, dass sie einen anderen Kanal verwendet, z. B. Kanal 3, bei dem es kein Schmalband-RFI gibt.
- **RFI (All-Band-Funktion)** - Wie der Name bereits andeutet, beinhalten All-Band-Interferenzen unerwünschte Funksignale, die das Daten-RF-Signal im gesamten RF-Band stören. Als All-Band-RFI kann die Interferenz definiert werden, die das gesamte Spektrum abdeckt, das die Funkeinheit nutzt. Das gesamte RF-Band verweist nicht nur auf das ISM-Band. Das RF-Band deckt alle Frequenzbereiche ab, die von den Wireless Bridges verwendet werden. Eine mögliche Ursache für all-Band-Interferenzen, die Sie häufig finden, ist ein Mikrowellenherd. Wenn eine Interferenz für das gesamte Band vorliegt, ist es am besten, eine andere Technologie zu verwenden, z. B. den Umstieg von 802.11b auf 802.11a (das 5-GHz-Band verwendet). Das gesamte Spektrum, das der FHSS nutzt, beträgt 83,5 MHz (das gesamte ISM-Band), während es für DSSS nur 20 MHz (eines der Subbänder) ist. Die

Wahrscheinlichkeit einer Interferenz, die einen Bereich von 20 MHz abdeckt, ist größer als die Wahrscheinlichkeit einer Interferenz, die 83,5 MHz abdeckt. Wenn Sie keine Technologien ändern können, versuchen Sie, die Ursache für die Multiband-Interferenz zu finden und zu beseitigen. Diese Lösung kann jedoch schwierig sein, da Sie das gesamte Spektrum analysieren müssen, um die Störungsquelle zu ermitteln.

- **RFI aufgrund widriger Witterungsbedingungen:** Schwere Wetterbedingungen, z. B. extremer Wind, Nebel oder Smog, können die Leistung von Wireless-Brücken beeinträchtigen und zu temporären Verbindungsproblemen führen. In diesen Situationen können Sie ein Radom verwenden, um eine Antenne vor den Auswirkungen auf die Umwelt zu schützen. Antennen ohne Radomschutz sind anfällig für Umwelteinflüsse und können die Leistung der Brücken beeinträchtigen. Ein häufiges Problem, das auftreten kann, wenn Sie das Radom nicht verwenden, ist das, das durch Regen. Raindrops können sich auf der Antenne ansammeln und die Leistung beeinflussen. Radome schützen eine Antenne auch vor herabfallenden Objekten, wie etwa Eis, das aus einem Overhead-Baum fällt. Mit dem [Cisco Outdoor Bridge Range Berechnungsprogramm](#) können Sie Ihr Klima und Ihr Terrain auswählen. Das Programm kompensiert jegliche Wetterverschlechterung.

CRC-, PLCP-Fehler

CRC- und PLCP-Fehler können aufgrund von Funkfrequenzstörungen auftreten. Je mehr Funkmodule eine Zelle hat (APs, Bridges oder Clients), desto größer sind die Wahrscheinlichkeit, dass diese Fehler auftreten. Eine Zelle ist ein einzelner Kanal (z. B. Kanal 1) oder ein Kanal, der den Kanal überschneidet. Funkschnittstellen sind Halbduplex. Daher sind Funkschnittstellen genau wie Kollisionsnachrichten auf Ethernet. Es gibt einige Gründe für das Auftreten von CRC-Fehlern:

- Paketkollisionen, die aufgrund einer hohen Anzahl von Client-Adaptoren auftreten
- Überlappende Access Point-Abdeckung auf einem Kanal
- Hohe Multipath-Bedingungen durch bounce-Signale
- Vorhandensein weiterer 2,4-GHz-Signale von Geräten wie Mikrowellenherden und Wireless-Mobiltelefonen

Wireless ist ein offeneres Medium als kabelgebundene Netzwerke und unterliegt Umweltauswirkungen. Die Radiowellen werden von umgebenden Objekten abgesprengt, was ein schwächeres oder defektes Signal erzeugen kann. Dies geschieht bei Mobiltelefonen, FM-Funkmodulen und anderen Wireless-Geräten. Je mehr 802.11-Funkmodule und Clients sich in einem Zellbereich befinden, desto höher ist der Konfliktstand und das Potenzial für Neuversuche und CRC-Fehler. Gleiches gilt für kabelgebundene Segmente.

CRC- und PLCP-Fehler (Physical Layer Control Protocol) sind normal, wenn der Datenverkehr über den AP fließt. Sie müssen diese Fehler nur dann als Problem betrachten, wenn die Anzahl der Fehler sehr groß ist. Es folgen einige Parameter, die Sie überprüfen müssen, wenn eine große Anzahl von CRC-Fehlern vorliegt:

1. **Line of Sight (LOS)** - Überprüfen Sie die LOS-Verbindung zwischen Sender und Empfänger, und stellen Sie sicher, dass die LOS-Daten klar sind.
2. **Funkstörungen:** Verwenden Sie einen Kanal mit geringeren Funkstörungen.
3. **Antennen und Kabel:** Stellen Sie sicher, dass die Antennen und Kabel für den Abstand der Funkverbindung geeignet sind.

Cisco empfiehlt eine Standortprüfung, um diese Fehler zu minimieren. Weitere Informationen zur

Bei einer Beeinträchtigung der Kommunikation, bei der die Einheiten auf eine niedrigere Datenrate zurückfallen müssen, kann die für 11 Mbit/s festgelegte Einheit jedoch nicht zurückfallen, und die Kommunikation schlägt fehl. Dies ist eines der häufigsten Probleme im Zusammenhang mit Datenraten. Die Problemlösung besteht in der Verwendung optimierter Datenrateneinstellungen auf den beiden Wireless Bridges.

Sie können die Datenrateneinstellungen verwenden, um die Bridge für den Betrieb mit bestimmten Datenraten einzurichten. Um beispielsweise die Bridge so zu konfigurieren, dass sie nur mit 54 Mbit/s betrieben wird, legen Sie die 54-Mbit/s-Geschwindigkeit auf "Basic" (Grundlegend) fest, und legen Sie die anderen Datenraten auf "Enabled" (Aktiviert) fest. Um die Bridge so einzurichten, dass sie mit 24, 48 und 54 Mbit/s betrieben werden kann, legen Sie 24, 48 und 54 auf "Basic" (Grundlegend) fest, und legen Sie die restlichen Datenraten auf "Enabled" (Aktiviert) fest. Sie können die Bridge auch so konfigurieren, dass die Datenraten automatisch festgelegt werden, um die Reichweite oder den Durchsatz zu optimieren. Wenn Sie einen Bereich für die Datenrateneinstellung eingeben, legt die Bridge die 6-Mbit/s-Rate auf "Basic" (Grundrate) und die anderen Raten auf "Enabled" (Aktiviert) fest. Wenn Sie den Durchsatz für die Datenrateneinstellung eingeben, legt die Bridge alle Datenraten auf "Basic" fest. Weitere Informationen zur Optimierung der Datenrateneinstellungen finden Sie unter [Konfigurieren der Funkdatenraten](#).

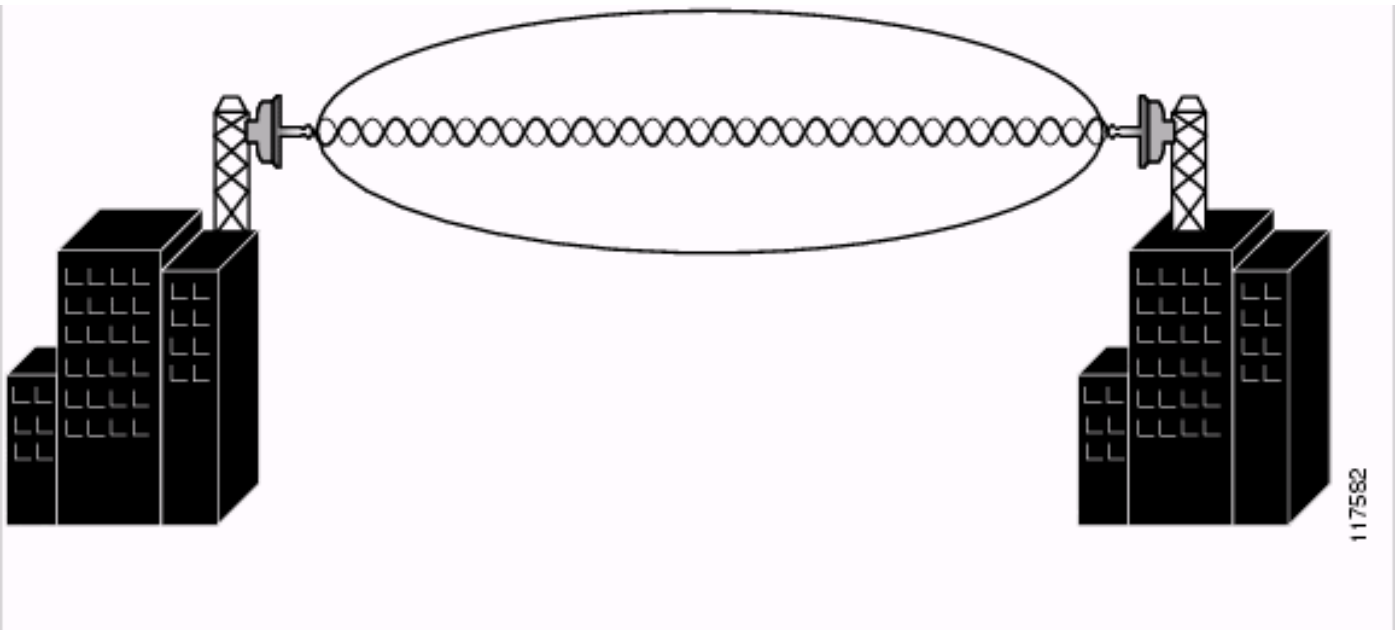
[Fresnel-Zonen und Sichtbereich](#)

Line of Sight (LoS) ist eine scheinbare (unsichtbare) gerade Linie zwischen Sender und Empfänger. Bei Wireless Bridges befindet sich das LoS zwischen den beiden Antennen, die die Bridges verbinden, z. B. eine Root Bridge und eine Non-Root Bridge. Der RF-LoS ist eine scheinbare gerade Linie, da RF-Wellen aufgrund verschiedener Faktoren wie Refraktion, Reflexion und Diffraktion Richtungsänderungen unterliegen. Das Problem besteht darin, dass Fresnel-Zonen RF-LoS beeinflussen können. In einem solchen Szenario kann die Verbindung zwischen den Bridges zeitweilig unterbrochen werden und in einigen Fällen zu einem vollständigen Verlust der Verbindung zwischen den Bridges führen.

Die Fresnel Zone ist ein elliptischer Bereich, der den visuellen Pfad unmittelbar umgibt. Die Fresnel Zone variiert je nach Länge des Signalpfads und der Frequenz des Signals. Eine klare Sichtlinie mit Fresnel Zone-Rand zeigt an, dass der Pfad keine Hindernisse aufweist, die das Signal beeinflussen können. Fresnel-Zonen sind wichtig, und Sie müssen diese Zonen vor der Implementierung eines Wireless Bridge-Netzwerks in Betracht ziehen. Alle Objekte in der Fresnel Zone können das Funksignal stören, was das Signal beeinflusst und eine Änderung des LoS bewirkt. Zu diesen Objekten gehören Bäume, Hügel und Gebäude.

Fresnel Zonen sind frequenzabhängig. Bei den Berechnungen des Bridge-Dienstprogramms wird eine Frequenz von 5,8 GHz verwendet. Technische Details zum Zonenfreigabe für Fresnel finden Sie im Abschnitt *Fresnel Zone* im Bereitstellungsleitfaden für die Cisco Aironet Wireless Bridge der Serie 1400.

Abbildung 2: Fresnel-Bereich



Um diese Probleme zu beheben, stellen Sie sicher, dass zwischen den Root- und Nicht-Root-Bridges visuelle und Radio-LoS vorhanden sind. Stellen Sie sicher, dass die Fresnel Zone durch nichts beeinträchtigt wird. Manchmal müssen Sie die Antennenhöhe erhöhen, um die Fresnel Zone zu löschen. Wenn die Brücken mehr als 10 km voneinander entfernt sind, greift die Krümmung der Erde in die Fresnel Zone ein. Weitere Unterstützung erhalten Sie im [Tool zur Berechnung der Reichweite](#) der [Außenbrücken](#).

[Probleme mit der Antennenausrichtung](#)

Die Antennenausrichtung bezieht sich direkt auf den korrekten LoS zwischen den beiden Brücken. Bei einer korrekten Ausrichtung der Antennen ist der RF-LoS zwischen den Geräten eindeutig, und es treten keine Verbindungsprobleme auf. Wenn Sie Richtantennen für die Kommunikation zwischen zwei Brücken verwenden, müssen Sie die Antennen manuell ausrichten, um einen ordnungsgemäßen Bridge-Betrieb zu gewährleisten. Richtantennen haben die Strahlungswinkel erheblich reduziert. Der Strahlungswinkel für Yagi-Antennen beträgt etwa 25 bis 30 Grad, für Parabolantennen etwa 12,5 Grad. Mithilfe des Bridge-Link-Tests können Sie die Ausrichtung von zwei Antennen messen, nachdem die Bridges zugeordnet wurden. Die Zuordnung zeigt den Antennenpunkt in der allgemeinen Nachbarschaft an, zeigt jedoch keine korrekte Ausrichtung der Antennen an. Der Verbindungstest enthält Informationen, mit denen Sie die Ausrichtung messen können.

Wenn zwei Antennen an den Rändern ihrer Strahlungsmuster ausgerichtet sind, kann die Kommunikation in der Regel marginal sein, da Pakete verloren gehen, die Anzahl der Wiederholungen hoch ist und die Signalstärke gering ist. Wenn jedoch zwei Antennen korrekt ausgerichtet sind, die Kommunikation verbessert und alle Pakete empfangen werden, sind die Anzahl der Wiederholungen geringer und die Signalstärke hoch. Informationen zur grundlegenden Antennenausrichtung und Anleitungen zur Durchführung von Verbindungstests finden Sie im Abschnitt *Grundorientierung* der [Antennen](#) im Abschnitt *Grundausrüstung* der [Antennen](#).

[Clear Channel Assessment Parameter \(CCA\)](#)

CCA ist im Wesentlichen die Einrichtung eines Rauschbodens, unterhalb dessen HF-Eingänge auf der Suche nach einem guten, soliden Signal ignoriert werden. Mit der programmierbaren CCA-Funktion können Wireless Bridges auf eine bestimmte Hintergrundinterferenzstufe konfiguriert werden, die in einer bestimmten Umgebung vorkommt. So wird der Overhead-Konflikt mit anderen

Wireless-Systemen verringert.

Ein CCA-Grenzwert kann die Empfängerempfindlichkeit verringern, indem der absolute Empfangsleistungsgrad geändert wird, über den der Kanal normalerweise als besetzt gilt. Der Standardwert des CCA-Parameters ist 75. Sie können jedoch den CCA-Grenzwert erhöhen, um die Geräusentwicklung in Umgebungen zu reduzieren. CCA-Werte können unabhängig für Root- und Nicht-Root-Bridges festgelegt werden.

Wenn der CCA-Wert nicht richtig konfiguriert ist, kann es zu Unterbrechungen der Verbindung mit Wireless Bridges kommen. Stellen Sie sicher, dass der CCA-Wert nicht auf 0 (null) festgelegt ist und auf den Standardwert nahe dem Standardwert 75 (falls nicht der Standardwert) festgelegt ist. Wireless-Bridges, die Cisco IOS® Software Releases vor 12.3(2)JA ausführen, schlagen einen Fehler auf, durch den der CCA-Standardwert beim Neustart des Geräts auf Null geändert wird. Weitere Informationen zu diesem Fehler und zur Behebung der Fehler finden Sie unter Cisco Bug ID [CSCed46039](#) (nur [registrierte](#) Kunden).

Weitere Probleme, die die Leistung von Wireless-Bridges beeinträchtigen

Die Materialien, durch die das HF-Signal durchdringen kann, können die Leistung der Wireless-Bridge bestimmen. Die Dichte der Materialien, die für den Bau eines Gebäudes verwendet werden, bestimmt die Anzahl der Wände, die das Funksignal durchlassen kann, und hält weiterhin eine ausreichende Abdeckung aufrecht. Die wesentliche Auswirkung auf die Signaldurchdringung ist:

1. Papier- und Vinyl-Wände haben wenig Einfluss auf die HF-Signaldurchdringung.
2. Feste und vorgestanzte Betonwände begrenzen die Signaldurchdringung auf eine oder zwei Wände, ohne dass die Abdeckung beeinträchtigt wird.
3. Betonblockwände begrenzen die Signaldurchdringung auf drei oder vier Wände.
4. Holz oder Gips ermöglichen eine ausreichende Signaldurchdringung für fünf bis sechs Wände.
5. Eine dicke Metallwand bewirkt, dass die Signale ausreflektiert werden, was zu einer schlechten Signaldurchdringung führt.
6. Kettenzaun und Drahtgitter mit einem Abstand von 1 bis 1 ½ Zoll fungieren als ½"-Wellen, die ein 2,4-GHz-Signal blockieren.
7. Wenn Sie eine Wireless Bridge-Verbindung über ein Fenster bereitstellen, kann das Fenster zu einem erheblichen Signalverlust führen. Je nach Art des Glases liegen die typischen Verluste zwischen 5 und 15 dB pro Fenster. Bei der Planung der Antennengewinne und der Energieeinstellungen muss dieser zusätzliche Verlust vorsichtig berücksichtigt werden.
8. Deaktivieren Sie die **Konfiguration** auf der Brücke. Bei der Konfiguration werden mehrere Pakete in einem einzigen Paket zusammengefasst, um den Durchsatz zu erhöhen. Wenn die Bridge mit einer Verbindung mit niedriger Geschwindigkeit auf der kabelgebundenen Seite verbunden wird, stellt dies ein Problem dar. Geben Sie diesen Befehl ein, um die Verkettung zu deaktivieren.

```
bridge(config)#interface dot11radio0  
    bridge(config-if)#no concatenation.
```

9. Bei Wireless-Bridges können zeitweilige Verbindungsprobleme auftreten, oder es kann zu einem Totalverlust der Verbindung zwischen den Kabeln kommen, die die Wireless-Bridges mit dem Power Injector und der Antenne verbinden. Überprüfen Sie zunächst, ob die Kabel ordnungsgemäß angeschlossen sind. Dies ist besonders dann hilfreich, wenn die Wireless-Brücken früher funktionierten, aber plötzlich die Verbindung verloren.

10. CCA ist im Wesentlichen die Einrichtung eines Rauschbodens, unterhalb dessen HF-Eingänge auf der Suche nach einem guten, soliden Signal ignoriert werden. Mit der programmierbaren CCA-Funktion können Wireless Bridges auf eine bestimmte Hintergrundinterferenzstufe konfiguriert werden, die in einer bestimmten Umgebung vorkommt. So wird der Overhead-Konflikt mit anderen Wireless-Systemen verringert. Ein CCA-Grenzwert kann die Empfängerempfindlichkeit verringern, indem der absolute Empfangsleistungsgrad geändert wird, über den der Kanal normalerweise als besetzt gilt. Der Standardwert des CCA-Parameters ist 75. Sie können jedoch den CCA-Grenzwert erhöhen, um die Geräusentwicklung in Umgebungen zu reduzieren. CCA-Werte können unabhängig für Root- und Nicht-Root-Bridges festgelegt werden. Wenn der CCA-Wert nicht richtig konfiguriert ist, kann es zu Unterbrechungen der Verbindung mit Wireless Bridges kommen. Stellen Sie sicher, dass der CCA-Wert nicht auf Null festgelegt ist.

Stellen Sie vor der Implementierung eines Wireless-Netzwerks sicher, dass Sie das Verhalten der Funkwellen durch die verschiedenen Materialien verstehen.

Zugehörige Informationen

- [Wireless - Technischer Support und Dokumentation](#)
- [Fehlerbehebung bei Verbindungen in einem Wireless-LAN-Netzwerk](#)
- [Fehlerbehebung bei Problemen mit der Funkfrequenzkommunikation](#)
- [Cisco Aironet Antenna - Referenzhandbuch](#)
- [RF-Leistungswerte](#)
- [Fehlerbehebung: BR350 Bridges](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)