

# Intermittent Connectivity Issues in Wireless Bridges

Document ID: 66090

---

## Introduction

### Prerequisites

Requirements

Components Used

Conventions

### Reasons for Intermittent Connectivity Issues in Wireless Bridges

Radio Frequency Interference

Use the Carrier Test Option in Bridges to Check for RFI

Sub-Optimal/Incorrect Data Rate Settings on the Wireless Bridges

Fresnel Zones and Line of Sight Issues

Problems with Antenna Alignment

Clear Channel Assessment Parameter (CCA)

Other Issues That Degrade the Performance of Wireless Bridges

### Related Information

---

## Introduction

This document explains some of the main reasons for intermittent connectivity issues with wireless bridges, and how to resolve these issues.

## Prerequisites

### Requirements

Cisco recommends that you have some basic knowledge of wireless bridges.

Refer to [Wireless – Technical Support & Documentation](#) for more references on wireless bridges.

### Components Used

The information in this document is based on Cisco Aironet Wireless bridges.

### Conventions

Refer to [Cisco Technical Tips Conventions](#) for more information on document conventions.

## Reasons for Intermittent Connectivity Issues in Wireless Bridges

Here are the common reasons for intermittent connectivity issues in wireless bridges:

1. Radio Frequency Interference
2. Sub-optimal/Incorrect Data Rate Settings on the Wireless Bridges
3. Fresnel Zone and Line of Sight Issues

4. Problems with Antenna Alignment
5. Clear Channel Assessment Parameter (CCA)
6. Other Issues that Degrade the Performance of Wireless Bridges

## Radio Frequency Interference

Radio Frequency Interference (RFI) involves the presence of unwanted interfering RF signals that disrupt the original data signals from wireless devices. RFI in a wireless network can lead to adverse effects, for example, intermittent connectivity loss, poor throughput, and low data rates. There are different types of RFI that can occur in a wireless network environment, and you must take these RFI types into consideration before you implement wireless networks. RFI types include narrowband RFI, all-band RFI, and RFI due to adverse weather conditions.

- **Narrowband RFI** Narrowband signals, depending on the frequency and signal strength, can intermittently interrupt or even disrupt RF signals from a spread spectrum device, such as a wireless bridge. The best way to overcome narrowband RFI is to identify the source of the RF signal. You can use Spectrum analyzers to identify the source of the RF signal.

Spectrum analyzers are devices that you can use to identify and measure the strength of interfering RF signals. When you identify the source, you can either remove the source to eliminate RFI, or shield the source properly. Narrowband signals do not disrupt original data RF signals (from a wireless bridge) across the entire RF band. Therefore, you can also choose an alternate channel for the bridge where no narrowband RF interference occurs. For example, if unwanted RF signals disrupt one channel, say channel 11, you can configure the wireless bridge to use another channel, say channel 3, where there is no narrowband RFI.

- **All-band RFI** As the name suggests, all-band interference involves any unwanted RF signal that interferes with the data RF signal across the entire RF band. All-band RFI can be defined as the interference that covers the whole spectrum that the radio uses. The entire RF band does not point to the ISM band alone. The RF band covers any band of frequencies that the wireless bridges use.

A possible source of all-band interference that you can find commonly is a microwave oven. When all-band interference is present, the best possible solution is to use a different technology, for example, move from 802.11b to 802.11a (which uses the 5GHz band). Also, the whole spectrum that the radio uses is 83.5 MHz in FHSS (the whole ISM band), while for DSSS it is only 20 MHz (one of the sub-bands). The chances of an interference that covers a range of 20 MHz are greater than the chances of an interference that covers 83.5 MHz. If you cannot change technologies, try to find and eliminate the source of the all-band interference. However, this solution can be difficult, because you have to analyze the entire spectrum to track the source of the interference.

- **RFI Due to Adverse Weather Conditions** Severely adverse weather conditions, for example, extreme wind, fog, or smog can affect the performance of wireless bridges, and lead to intermittent connectivity issues. In these situations, you can use a radome to protect an antenna from the environmental effects. Antennas that do not have radome protection are vulnerable to environmental effects, and can cause degradation to the performance of the bridges. A common problem that can occur if you do not use the radome is the one due to rain. Raindrops can accumulate on the antenna and affect performance. Radomes also protect an antenna from falling objects, such as ice that falls from an overhead tree. With the Cisco Outdoor Bridge Range Calculation Utility, you can choose your climate and terrain, and the program compensates for any degradation in weather.

### CRC, PLCP errors

CRC errors and PLCP errors can occur due to Radio Frequency interference. The more radios a cell has (APs, Bridges or Clients), the more are the chances of the occurrence of these errors. A cell means a single channel (for example, channel 1) or a channel that overlaps the channel. Radio interfaces are half duplex. Therefore, radio interfaces are just like collision messages on Ethernet. Here are some reasons for the occurrence of CRC

errors:

- Packet collisions that occur due to a dense population of client adapters
- Overlapping access point coverage on a channel
- High multipath conditions due to bounced signals
- Presence of other 2.4-GHz signals from devices like microwave ovens and wireless handset phones

Wireless is a more open medium than wired networks, and is subject to environmental effects. The radio waves bounce off surrounding objects, which can create a weaker or broken signal. This happens with cell phones, FM radios, and other wireless devices. The more 802.11 radios and clients are in a cell area, higher is the contention level and the potential for retries and CRC errors. The same applies to wired segments.

CRC and PLCP (Physical Layer Control Protocol) errors are normal when traffic flows through the AP. You do not need to consider these errors to be an issue unless the number of errors is very large. Here are some parameters you must check if there is a large number of CRC errors:

1. **Line of Sight (LOS)** Check the LOS between the transmitter and the receiver, and ensure that the LOS is clear.
2. **Radio Interference** Use a channel that has lower radio interference.
3. **Antennas and Cables** Ensure that the antennas and cables are appropriate for the distance of the radio link.

Cisco recommends a site survey in order to minimize these errors. Refer to Performing a Site Survey for more information on Site Survey.

## Use the Carrier Test Option in Bridges to Check for RFI

Cisco wireless bridges can also analyze different channels to detect RFI. The carrier busy test helps to view the activity in the RF spectrum. The carrier busy test is available on bridges, and enables you to view the radio spectrum. Figure 1 shows the carrier busy test on the BR500. The numbers 12, 17, 22, and so on represent the 11 frequencies that the bridge uses. For example, 12 represents the frequency 2412 MHz. The asterisk (\*) indicate the activity on each frequency. Whenever possible, choose the frequency with the least activity to reduce chances of interference. Refer to Performing a Carrier Busy Test for more information on how to perform Carrier Test.

**Figure 1 Carrier Busy Test on the BR500**

```
Aironet BR500E V8.24          CARRIER BUSY / FREQUENCY
TechSupp_4800

*
*
*  *
*  *  *
*  *  *
*  *  *
*  *  *  *  *
*  *  *  *  *
*  *  *  *  *  *  *  *  *  *
*  *  *  *  *  *  *  *  *  *
1 1 2 2 3 3 4 4 5 5 6
2 7 2 7 2 7 2 7 2 7 2

Highest point = 35% utilization

Enter space to redisplay, q[uit] ::
```

## Sub-Optimal/Incorrect Data Rate Settings on the Wireless Bridges

Wireless bridges can run into connectivity issues if you configure the bridges with sub-optimal or incorrect data rate settings. If you configure the data rates incorrectly on wireless bridges, the bridges fail to communicate. A typical example is a scenario where one of the bridges is configured for a fixed data rate, for example, 11 Mbps, and the other bridge is configured with a data rate of 5 Mbps.

Normally, the bridge always attempts to transmit at the highest data rate set to basic, also called "require", on the browser-based interface. In case of obstacles or interference, the bridge steps down to the highest rate that allows data transmission. If one of the two bridges has a data rate of 11 Mbps set, and the other is set to "use any rate", the two units communicate at 11 Mbps. However, in case of some impairment in the communication that requires the units to fall back to a lower data rate, the unit set for 11 Mbps cannot fall back, and communications fail. This is one of the most common problems that relate to data rates. The workaround is to use optimized data rate settings on the two wireless bridges.

You can use the data rate settings to set up the bridge to operate at specific data rates. For example, in order to configure the bridge to operate at 54 Mbps service only, set the 54 Mbps rate to basic, and set the other data rates to enabled. In order to set up the bridge to operate at 24, 48, and 54 Mbps, set 24, 48, and 54 to basic, and set the rest of the data rates to enabled. You can also configure the bridge to set the data rates automatically to optimize either range or throughput. When you enter a range for the data rate setting, the bridge sets the 6 Mbps rate to basic and the other rates to enabled. When you enter throughput for the data rate setting, the bridge sets all data rates to basic. Refer to *Configuring Radio Data Rates* for more information on how to optimize the data rate settings.

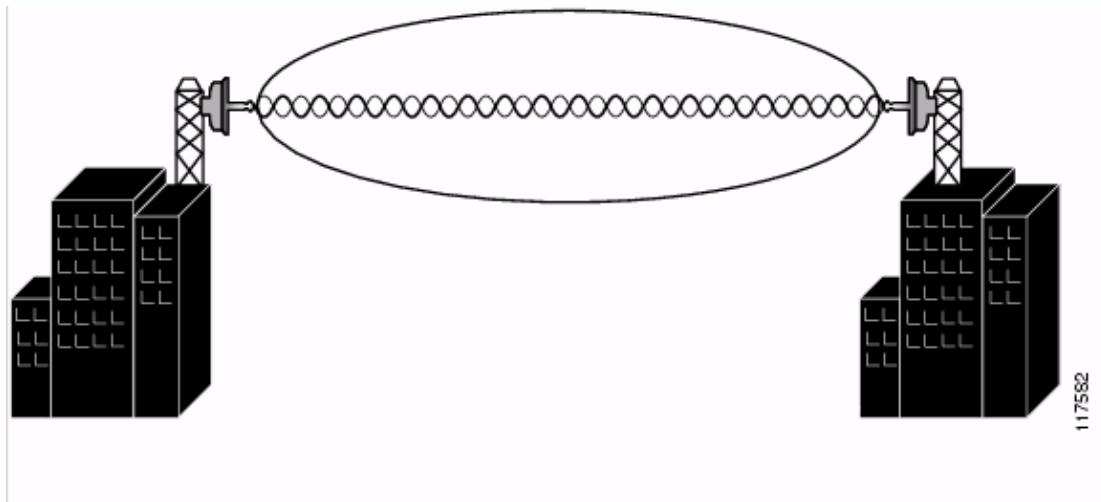
## Fresnel Zones and Line of Sight Issues

Line of Sight (LoS) is an apparent (invisible) straight line between the transmitter and receiver. In the case of wireless bridges, the LoS is between the two antennas that connect the bridges, for example a root bridge and a non-root bridge. The RF LoS is an apparent straight line because RF waves are subject to changes in direction due to various factors that include refraction, reflection, and diffraction. The problem is that Fresnel Zones can affect RF LoS. In such a scenario, the connectivity between the bridges can be intermittent, and in some cases, can lead to complete loss of connectivity between the bridges.

The Fresnel Zone is an elliptical area immediately surrounding the visual path. The Fresnel Zone varies depending on the length of the signal path and the frequency of the signal. A clear line of sight, with Fresnel Zone margin, indicates that the path has no obstructions that can affect the signal. Fresnel Zones are important, and you need to consider these zones before the implementation of any wireless bridged network. Any objects in the Fresnel Zone can interfere with the RF signal, which affects the signal, and causes a change in the LoS. These objects include trees, hills, and buildings.

Fresnel zones are frequency dependent. A frequency of 5.8GHz is used in the bridge utility calculations. Refer to the *Fresnel Zone* section of the Cisco Aironet 1400 Series Wireless Bridge Deployment Guide for technical details on fresnel zone clearance.

### Figure 2 Fresnel Zone



In order to resolve these issues, make sure that there is visual and radio LoS between the root and non-root bridges. Check to ensure that nothing obstructs the Fresnel Zone. Sometimes, you need to raise the antenna height in order to clear the Fresnel Zone. If the bridges are more than six miles apart, the curvature of the earth encroaches on the Fresnel Zone. Refer to the Outdoor Bridge Range Calculation Utility for additional assistance.

## Problems with Antenna Alignment

Antenna alignment directly relates to the proper LoS between the two bridges. In case of proper alignment of the antennas, the RF LoS between the devices is clear and connectivity problems do not occur. When you use directional antennas to communicate between two bridges, you must manually align the antennas for proper bridge operation. Directional antennas have greatly reduced radiation angles. The radiation angle for yagi antennas is approximately 25 to 30 degrees, and for parabolic dish antennas, the radiation angle is approximately 12.5 degrees. You can use the bridge link test to help measure the alignment of two antennas after the bridges are associated. The association indicates the antennas point in the general vicinity of each other, but does not indicate proper alignment of antennas. The link test provides information you can use to gauge the alignment.

Typically, when two antennas are aligned to the edges of their radiation patterns, communication can be marginal, as packets are lost, retry counts are high, and signal strength is low. However, when two antennas are properly aligned, communication improves, and all packets are received, retry counts are lower, and signal strength is high. Refer to the *Basic Antenna Alignment* section of Antenna Basics for information on basic antenna alignment, and for instructions on how to perform link tests.

## Clear Channel Assessment Parameter (CCA)

CCA is essentially the establishment of a noise floor below which it ignores RF inputs, in search of a good, solid signal. With the programmable CCA feature, wireless bridges can be configured to a particular background interference level found in a specific environment, for reduced overhead contention with other wireless systems.

A CCA threshold can decrease the receiver sensitivity by changing the absolute receive power level above which the channel is normally considered busy. The default value of the CCA parameter is 75. However, you can increase the CCA threshold to reduce noise in environments. CCA values can be set independently for root and non-root bridges.

There might be intermittent connectivity losses with wireless bridges if the CCA value is not configured correctly. Ensure that the CCA value is not set to zero and is set to the value close to the default value of 75 if

not the default value. Wireless bridges that run Cisco IOS® Software Releases earlier than 12.3(2)JA hit a bug which changes the default CCA value to zero upon reboot of the device. Refer to Cisco bug ID CSCed46039 (registered customers only) for more information on this bug and the workaround.

## Other Issues That Degrade the Performance of Wireless Bridges

The materials that the RF signal can penetrate can determine the performance of the wireless bridge. The density of the materials used in the construction of a building determine the number of walls the RF signal can pass through and still maintain adequate coverage. Material impact on signal penetration are:

1. Paper and vinyl walls have little effect on RF signal penetration.
2. Solid and pre-cast concrete walls limit signal penetration to one or two walls without degrading coverage.
3. Concrete and concrete block walls limit signal penetration to three or four walls.
4. Wood or drywall allows for adequate signal penetration for five or six walls.
5. A thick metal wall causes signals to reflect off, resulting in poor signal penetration.
6. Chain link fence and wire mesh with 1 to 1½" spacing act as ½" waves that block a 2.4 GHz signal.
7. When you deploy a wireless bridge link through a window, the window glass can introduce significant signal loss. Typical losses range from 5 to 15 dB per window, depending upon the type of glass. Your deployment plan must take this extra loss into account conservatively when you plan antenna gains and power settings.
8. Disable **Concatenation** on the bridge. Concatenation is the process where multiple packets are aggregated into a single packet to increase the throughput. When the bridge connects to a low speed link on the wired side this poses a problem. Issue this command in order to disable concatenation.

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

9. Wireless bridges can experience intermittent connectivity problems or total loss of connectivity if there is loose connectivity between the cables that connect the wireless bridges to the power injector and the antenna. As a first step, check if the cables are connected properly. This especially helps in cases where the wireless bridges were working previously but suddenly lost connectivity.
10. CCA is essentially the establishment of a noise floor below which it ignores RF inputs, in search of a good, solid signal. With the programmable CCA feature, wireless bridges can be configured to a particular background interference level found in a specific environment, for reduced overhead contention with other wireless systems. A CCA threshold can decrease the receiver sensitivity by changing the absolute receive power level above which the channel is normally considered busy. The default value of the CCA parameter is 75. However, you can increase the CCA threshold to reduce noise in environments. CCA values can be set independently for root and non-root bridges. There might be intermittent connectivity losses with wireless bridges if the CCA value is not configured correctly. Ensure that the CCA value is not set to zero.

Before you implement a wireless network, make sure that you understand the behavior of RF waves through the different materials.

---

## Related Information

- **Wireless – Technical Support & Documentation**
- **Troubleshooting Connectivity in a Wireless LAN network**
- **Troubleshooting Problems affecting Radio Frequency Communication**
- **Cisco Aironet Antenna Reference Guide**
- **RF Power Values**
- **Troubleshooting BR350 Bridges**
- **Technical Support & Documentation – Cisco Systems**

---

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Jan 21, 2008

Document ID: 66090

---