



Configuring the Radio Network

This chapter describes the procedures for configuring the bridge's radio network.

Here's what you'll find in this chapter:

- [Using the Configuration Radio Menu, page 4-2](#)
- [Establishing an SSID \(Ssid\), page 4-2](#)
- [Selecting the Data Rate and Basic Rate \(Rates, Basic_rates\), page 4-2](#)
- [Setting the World Mode \(World\), page 4-2](#)
- [Using the Configuration Radio IEEE 802.11 Menu \(I80211\), page 4-3](#)
- [Using the Configuration Radio Link Tests Menu \(Linktests\), page 4-6](#)
- [Using the Configuration Radio Extended Menu \(Extended\), page 4-10](#)

Using the Configuration Radio Menu

From the Configuration Radio menu, you can configure the radio network.

Navigation: Choose **Main > Configuration > Radio**

Option	Value	Description
1 - Ssid	["2"]	- Service set identification
2 - Rates	[1_11]	- Allowed bit rates in megabits/second
3 - Basic_rates	[1]	- Basic bit rates in megabits/second
4 - World	[off]	- Enable world mode
5 - 180211	[menu]	- 802.11 parameters
6 - Extended	[menu]	- Extended parameters

Enter an option number or name, "=" main menu, <ESC> previous menu
> _

86612



Caution

Changes to radio parameters take effect immediately. If your Telnet or browser session is accessing the bridge over a radio link, you might lose the session because the bridge may no longer be associated to an access point on the network. If this happens, it may be necessary to change the access point's radio parameters to reestablish the radio link. You can also use a crossover cable to attach the bridge to the Ethernet port on a PC to configure it.

Establishing an SSID (Ssid)

The *Ssid* option establishes a unique identifier that the bridge uses to associate with the access point. The SSID helps client devices distinguish between multiple wireless networks in the same vicinity. The SSID can be any alphanumeric, case-sensitive entry from two to 32 characters long.

Selecting the Data Rate and Basic Rate (Rates, Basic_rates)

The *Rates* option sets the list of data rates at which the bridge will be allowed to send and receive radio packets. The rate may be configured as an inclusive range (1 to 11) or as an individual rate (11).

The *Basic_rates* option determines the rate every radio node in the cell must support. If the basic rate is not supported, the bridge is not allowed to associate. The lowest basic rate controls the rate at which all multicast and broadcast packets are transmitted. The highest basic rate controls the bit rate at which the management packets are transmitted.

Setting the World Mode (World)

The *World* option allows the bridge to automatically inherit channel configuration and output power properties from the Cisco Aironet access point to which it associates. The *World* mode should be enabled when the bridge is used outside the United States.

Using the Configuration Radio IEEE 802.11 Menu (I80211)

Use the Radio IEEE 802.11 menu to configure RTS/CTS and encryption parameters.

Navigation: Choose **Main > Configuration > Radio > I80211**

Configuration Radio I80211 Menu		
Option	Value	Description
1 - Rts	[2048]	- RTS/CTS packet size threshold
2 - Privacy	[menu]	- Privacy configuration

Enter an option number or name, "=" main menu, <ESC> previous menu
> █

44774

Setting the RF Request To Send/Clear To Send (RTS/CTS) Parameter (Rts)

The *Rts* parameter determines the minimum-size transmitted packet that will use the RTS/CTS protocol. The value typed must range from 0 to 2400 bytes. The default is 2048.

This protocol is most useful in infrastructures where the mobile nodes roam so far that the nodes on one side of the cell cannot hear the transmission of the nodes on the other side of the cell.

When the transmitted packet is equal to or larger than the RTS threshold, an RTS packet is sent. The destination node must respond with a CTS packet before the originator can send the real data packet. A node at the far end of a cell detects the RTS to/from the bridge or the CTS to/from the bridge. The node detects how long to block its transmitter to allow the real packet to be received by the bridge. The RTS and CTS are small and, if lost in a collision, they can be retried more quickly and with less overhead than if the whole packet must be retried.

The disadvantage of using RTS/CTS is that for each data packet transmitted that is larger than the threshold size, another packet must be transmitted and received, thereby reducing throughput.

Privacy Menu (Privacy)

Wired Equivalent Privacy (WEP) is an optional IEEE 802.11 feature that provides data confidentiality equivalent to a wired LAN without crypto techniques to enhance privacy. Use WEP to encrypt data signals sent from the bridge to wireless client devices and to decrypt data signals sent from client devices to the bridge.

Navigation: Choose **Main > Configuration > Radio > I80211 > Privacy**

Configuration Radio I80211 Privacy Menu		
Option	Value	Description
1 - Encryption	[off]	- Encrypt radio packets
2 - Auth	[open]	- Authentication mode
3 - Key		- Set the keys
4 - Transmit		- Key number for transmit

Enter an option number or name, "=" main menu, <ESC> previous menu
> █

44775

Steps for Enabling Encryption

It is important that you enable WEP in the following sequence:

1. Set the receive key.
2. Set the transmit key.
3. Set the authentication mode.
4. Turn on encryption.

Setting the Receive Key

The *Key* value establishes the WEP key the bridge uses to receive packets. The value must match the key used by the access point. You can set two levels of encryption: 40-bit and 128-bit. The 40-bit key consists of 10 hexadecimal characters. The 128-bit key consists of 26 hexadecimal characters. The hexadecimal characters may be any combination of 0 through 9, a through f, or A through F. The WEP key can contain combinations of any of these characters. Hexadecimal WEP keys are not case-sensitive.

To set the key, follow these steps:

-
- Step 1** In the Privacy menu, choose **Key**. The following message appears:
- ```
Enter a number [1 to 4]:
```
- Step 2** Enter the number of the key the bridge will use and press **Enter**. The following message appears:
- ```
Enter a key of hex digits:
```
- Step 3** Enter the hexadecimal digits for the key (10 digits for 40-bit encryption or 26 digits for 128-bit encryption) and press **Enter**. The following message appears:
- ```
Enter a key again:
```
- Step 4** Enter the key again for confirmation and press **Enter**. After a few seconds, the Configuration Radio I80211 Privacy prompt appears.
- Step 5** Press **Enter** again to return to the Privacy menu.
- 

### Setting the Transmit Key

The *Transmit* key establishes the WEP key the bridge will use to transmit packets. You can use the key established when you set the key in the procedure above or you can use a different key. If you use a different key, a matching key must be established on the access point.

Follow these steps to set the *Transmit* key:

- 
- Step 1** In the Privacy menu, choose **Transmit**. The following message appears:
- ```
Enter a number [ 1 to 4]:
```
- Step 2** Enter the key number (1, 2, 3, or 4) and press **Enter**.



Note Only one WEP key can be used at a time to transmit.

Setting the Authentication Mode

The *Auth* parameter determines which authentication mode the system uses. Options are *open* or *shared_key*. The following is an explanation of each mode:

- **Open:** allows any access point, regardless of its WEP setting, to authenticate and then attempt to communicate with the bridge. **Open** is the default authentication mode.
- **Shared_key:** instructs the bridge to send a plain-text, shared-key query to any access point attempting to communicate with the bridge. The shared-key setting can leave the bridge open to a known-text attack from intruders, and it is therefore not as secure as the open setting.

To set the authorization mode, follow these steps:

Step 1 In the privacy menu, choose **Auth** and press **Enter**. The following message appears:

```
Enter one of [open, shared_key]:
```

Step 2 Enter a mode and press **Enter**.

Turning on Encryption

The *Encryption* option sets encryption parameters on all data packets except association packets and some control packets. Options are *off*, *on*, *mixed on*, or *mixed off*. The access point must also have encryption active and a key set properly. The following is an explanation of each option:

- **Off:** the default setting that turns off all encryption. The bridge cannot communicate with access points that use WEP.
- **On:** requires all data transfers to be encrypted. The bridge only communicates with access points that use WEP.
- **Mixed on:** means that the bridge always uses WEP when communicating with the access point but that the access point communicates with all devices whether they use WEP or not.
- **Mixed off:** means that the bridge does not use WEP when communicating with the access point, but the access point communicates with all devices whether they use WEP or not.



Caution

If you select *on* or *mixed on* as the WEP category and you are configuring the bridge through its radio link, you will lose connectivity to the bridge if the WEP key is set incorrectly. Be sure the WEP key you set exactly matches the WEP key used on your wireless LAN.

To set the encryption parameters, follow these steps:

Step 1 In the Privacy menu, choose **Encryption**. The following message appears:

```
Enter one of [off, on, mixed_on, mixed_off]:
```

Step 2 Enter the encryption option the bridge will use and press **Enter**.



Caution

The WEP key you use to transmit data must be set to exactly the same value on your access point and your bridge.

Extensible Authentication Protocol (EAP)

Additional wireless security is available when you enable the bridge's EAP feature. See Chapter 3, "Using the Configuration Menu" for details and procedures.

Using the Configuration Radio Link Tests Menu (Linktests)

The *Linktests* option tests the transmission quality between bridge nodes and other nodes on the radio network as well as individual node radio performance.

A link test sends special control packets to a specified destination, which in turn echoes the packets back to the source. Each control packet sent has a sequence number that allows the sender to know whether packets were lost on the way to the destination or on the way back to the source node.

Navigation: Choose **Main > Configuration > Radio > Linktests**

Configuration Radio Linktests Menu		
Option	Value	Description
1 - Strength		- Run a signal strength test
2 - Align		- Antenna alignment test
3 - Multicast		- Run a multicast echo test
4 - Unicast		- Run a unicast echo test
5 - Remote		- Run a remote echo test
6 - Destination	[any]	- Target address
7 - Size	[512]	- Packet size
8 - Count	[100]	- Number of packets to send
9 - Rate	[auto]	- Data rate
01 - Errors		- Radio error statistics
02 - Autotest	[once]	- Auto echo test
03 - Continuous	[0]	- Repeat echo test once started

Enter an option number or name, "=" main menu, <ESC> previous menu
> █

44773

Running a Signal Strength Test (Strength)

The *Strength* option sends a packet once per second to the parent access point. This packet is echoed back to the bridge, which records and displays the RF signal strength associated with that particular node.

Strength tests can be used to quickly verify the link to each radio partner or signal strength can be monitored while aligning directional antennas between two nodes. As the antennas are moved, the signal strength can be monitored to achieve maximum value.

Running an Alignment Test (Align)

The *Align* option breaks the association with the access point and starts monitoring beacons from all access points within radio range. Press any key to stop the test.

This test provides a continuous readout of radio signal parameters between the access point and the bridge to which it is associated. Display parameters include signal strength, signal quality, number of hops to the backbone, load, and the number of clients associated to the access point. Use the test to align directional antennas or to optimize bridge location and orientation.

Running a Multicast Test (Multicast)

The *Multicast* option tests transmission conditions within local radio cells. Packets are sent between the source and destination nodes without any acknowledgments or retries (as unicasts). This test provides a good indication of the raw state of the path to the node because no attempt is made to recover from any radio errors.

Navigation: Choose **Main > Configuration > Radio > Linktests > Multicast**

```

Testing link to Cisco-264be0 with 100 multicast packets of size 512
GOOD ( 0% Lost)

```

	Time msec	Strength		Quality %	
		% In dBm	% Out dBm	In	Out
Sent: 100, Avg: 7	51	-69	255	84	0
Lost to Tgt: 0, Max: 8	68	-61	255	93	0
Lost to Src: 0, Min: 6	42	-74	255	68	0

```

Rates (Src/Tgt) 11Mb: 100/100
Noise level -94dBm, 1 minute Max -94dBm Avg -95dBm
Hit any key to continue ...

```

44771

The time displays in milliseconds. Each packet contains the time it was sent. When a packet is received by the source, the time difference indicates the round-trip time. Longer times indicate full bandwidth of either the processor or the radio.

The signal strength and quality parameters report on the radio signal at the time the packets are received at each end. Signal strength and quality are expressed in decibels referenced to an input signal of one milliwatt of power (dBm) and as a percentage of full power.

Running a Unicast Test (Unicast)

The *Unicast* option tests the path between the bridge and any other Cisco Aironet node in the wired or radio network. The packets are sent with the same error recovery as normal user data, so round-trip times indicate the infrastructure throughput and congestion.

Navigation: Choose **Main > Configuration > Radio > Linktests > Unicast**

```

Testing link to Cisco-264be0 with 100 unicast packets of size 512
GOOD (7% Retries)

```

	Time msec	Strength		Quality %		Retries	
		% In dBm	% Out dBm	In	Out	In	Out
Sent: 100, Avg: 7	66	-61	255	88	0	Tot: 11	4
Lost to Tgt: 0, Max: 12	76	-58	255	93	0	Max: 2	1
Lost to Src: 0, Min: 6	40	-75	255	75	0		

```

Rates (Src/Tgt) 11Mb: 100/100
Noise level -94dBm, 1 minute Max -94dBm Avg -95dBm
Hit any key to continue ...

```

44772

The time displays in milliseconds. Each packet contains the time it was sent. When a packet is received by the source, the time difference indicates the round-trip time. Longer times indicate full bandwidth of either the processor or the radio.

The signal strength and quality parameters report on the radio signal at the time the packets are received at each end. Signal strength and quality are expressed in decibels referenced to an input signal of one milliwatt of power (dBm) and as a percentage of full power.

If the path to the target node was over the radio, the report displays the total number of radio retries necessary to complete the test. A large number of retries indicates radio interference problems.

Running a Remote Link Test (Remote)

The *Remote* option runs a multicast link test between a remote bridge node associated in the infrastructure and its parent access point. You are prompted for the address of the bridge node in order to make a broadcast request. The two remote nodes will run the link test and return the results, which display to the operator locally.

Navigation: Choose **Main > Configuration > Radio > Linktests > Remote**

```
Remote linktest from 00409610d258 to 0040961064de
Sent 100 of 100 512 byte packets, Destination received 90,
Source received 90
```

Specifying the Target Address (Destination)

The *Destination* option indicates the target node address for the link test. You may type an infrastructure address or the string *any*. If you select *any*, the bridge directs the test to the access point to which it is associated. If you type an infrastructure address, it may only be used for the remote or unicast link tests.

Setting the Packet Size and Count (Size, Count)

The *Size* and *Count* options indicate the size and number of packets to be sent. The default values are 100 packets of 512 bytes each. Both the size and the count can be changed. The packet size can be set from 30 to 1450 bytes and the count of the number of packets to transmit can be set from 1 to 999 packets.

When running the link test, use the highest data bit rate possible to test the reliability of your data bit rate and frequency combination. The more packets you send and the larger the packet size, the more accurate the test.



Note

Multiple large packets increase test time.

Rate (Rate)

The *Rate* option allows you to force the link test to transmit packets at only one of the allowed rates, or you can select *auto* to use the highest allowed rate and rate-shift if necessary.

Viewing Errors (Errors)

The *Errors* option views any radio error statistics that occurred during the link test. See Chapter 7, “Viewing Statistics.”

Setting the Automatic Link Test Mode (Autotest)

The *Autotest* option controls the automatic running of a link test whenever a bridge associates to its parent. The test uses the currently configured test parameters which, by default, run a test to the parent node.

- **Off:** an automatic test is never run.
- **Once:** only one test is run the first time the bridge associates to a parent after powering on.
- **Always:** runs the test each time the bridge associates to a parent.

During an automatic link test, the three indicators on the bridge turn green in a cyclic pattern to indicate that a test is in progress. At the end of the test, the indicators are set to a steady pattern for 4 seconds to indicate the test results. The particular pattern that is displayed depends on the percentage of packets lost during the test as shown in Table 4-1:

Table 4-1 Auto Link Test Display Patterns

Radio	Status	Ethernet	% of Packets Lost	Quality
Green	Green	Green	0-2	Excellent
Green	Green	Amber	3-5	Very Good
Green	Green	Off	6-25	Good
Green	Amber	Off	26-50	Satisfactory
Amber	Off	Off	51-75	Fair
Red	Off	Off	76-100	Poor

The Autotest procedure helps determine the placement of bridges. For example, at each prospective location, an installer could cycle the power on the bridge and watch the indicator displays for the results of the link test. As the test begins to fail, the installer could determine the radio range to the infrastructure and adjust the location accordingly.

Continuously Running a Link Test (Continuous)

The *Continuous* option continuously repeats the link tests. If the value for the parameter is zero, the tests are not repeated; otherwise, the value determines the delay (in seconds) between tests.

Using the Configuration Radio Extended Menu (Extended)

The extended radio parameters are not normally modified, but some may have to be changed when certain situations arise.

Navigation: Choose **Main > Configuration > Radio > Extended**

Configuration Radio Extended Menu		
Option	Value	Description
1 - Parentid	[any]	- Parent node Id
2 - Parent_timeout	[off]	- Time to look for specified parent
3 - Count_retry	[64]	- Maximum number transmit retries
4 - Refresh	[100]	- Refresh rate in 1/10 of seconds
5 - Diversity	[on]	- Enable the diversity antennas
6 - Power	[full]	- Transmit power level
7 - Fragment	[2048]	- Maximum fragment size
8 - Options		- Enable radio options

Enter an option number or name, "=" main menu, <ESC> previous menu
> |

44770

Setting the Parent ID (Parentid, Parent_timeout)

The *Parentid* option controls the address with which the bridge associates. If the value is set to *any*, the bridge associates with its best choice of parent based on signal quality and load. If the value is set to a specified infrastructure address, the bridge only associates to the access point assigned that address.

If the *Parent_timeout* option is set to *on*, the lost bridge makes only one attempt to re-associate to the parent access point. If the bridge does not find the requested parent, the bridge stops searching and associates to the best access point. If the *Parent_timeout* is set to *off*, the bridge attempts to re-associate to the parent access point. If the bridge does not find the requested parent, it does not associate with the best access point.

Setting Retry Transmission Time (Count_retry)

The *Count_retry* option establishes a particular level of radio performance by controlling the RF packet retry level. If the retry count is reached, the retry process on this particular packet is stopped. The bridge is disassociated from the access point and then begins scanning for a new parent access point.

The *Count_retry* range is 8 to 64. The default setting is 64. Reduce the retry count field if the bridge is mobile and you want to change from access point to access point very quickly after moving out of range. In non-mobile applications, lowering this parameter could help if there were sources of temporary interference. It would cause the bridge to retry at a later time.

Setting the Refresh Time (Refresh)

The *Refresh* option specifies an amount of time there has been no traffic between the bridge and its parent. If there has been no traffic between the bridge and its parent for the time specified, the bridge sends a special refresh packet to ensure that the parent is still reachable. The value may be set from 5 to 150 tenths of a second. Use the default value unless the bridge is mobile and needs to quickly verify that it has moved out of range (faster than once every 15 seconds).

Diversity (Diversity)

The *Diversity* option enables the dual diversity feature of a bridge equipped with two antennas. This option is not available for bridge models with one captured antenna. For bridge models with two antennas installed, the *Diversity* setting defaults to *on*.

**Caution**

If your bridge is equipped with one antenna, verify that the *Diversity* option is turned off and make sure the antenna is attached to the connector nearest the power connector, as shown in the illustration below. Attaching the antenna to the opposite connector will result in reduced operation.



Setting the Power Level (Power)

The *Power* parameter adjusts the bridge's radio transmitter output power level. The power may be adjusted incrementally from 1 to 100 mW, or set to full. Default power level is full.

Setting Fragment Size (Fragment)

The *Fragment* option determines the largest packet size that may be transmitted. Packets that are larger than this size will be broken into pieces that are transmitted separately and rebuilt on the receiving side.

If there is excessive radio interference or collisions with other nodes, the smaller lost packets can be retried faster and with less impact on the airwaves. The disadvantage is that if there is limited interference, long packets take more time to transmit due to the extra packet overhead and acknowledgments for the fragments.

Set the fragment size between 256 and 2048 bytes. Default fragment size is 2048.

Options (Options)

The *Options* feature is reserved for future system improvements.

