Configuring the Wi-Fi Interface

This chapter provides details on how to configure the Wi-Fi interface on the Cisco 910 Industrial Routers (hereafter referred to as the router). The Wi-Fi interface helps to provide remote wireless connectivity to a router.

**Note**
The Wi-Fi interface can be configured only on the IR910W-K9 model of Cisco 910 Industrial Routers.

This chapter includes the following sections:
- Information About the Wi-Fi Interface, page 19-1
- Configuring the Wi-Fi Interface, page 19-3
- Monitoring Wi-Fi Information, page 19-9

### Information About the Wi-Fi Interface

This section includes the following information:
- Wi-Fi Modes, page 19-1
- Wi-Fi Settings, page 19-2
- SSID, page 19-2
- Security, page 19-2

### Wi-Fi Modes

- Wi-Fi Access Point, page 19-2
- Wi-Fi Station, page 19-2

**Note**
The Wi-Fi interface can only be set up to perform as a Wi-Fi access point or Wi-Fi client at any one time—it cannot perform both roles simultaneously.
Information About the Wi-Fi Interface

Wi-Fi Access Point

The router’s 2.4GHz Wi-Fi radio interface can function as an access point (AP) that provides connectivity to 802.11 b/g/n devices. This Wi-Fi connectivity allows remote access and diagnostics of the router in the field.

Wi-Fi Station

The Wi-Fi interface can be configured as a Wi-Fi station. This configuration allows the Wi-Fi interface to act as a Wi-Fi client to another access point or repeater. Layer-3 routing is supported over the radio interface. SSIDs are required to be configured on the dot11 interface operating as a Wi-Fi station.

Wi-Fi Settings

The Wi-Fi interface is identified as dot11Radio 0 on the router.

The essential configuration elements are:

- Wi-Fi interface IP address.
- Service set identifier (SSID).
- Authentication type for enabling the router’s Wi-Fi functionality.
- Configuring a passphrase if WPA/WPA2 authentication is selected.

For more information, see the “SSID” section on page 19-2, the “Security” section on page 19-2, and the “Configuring the Wi-Fi Interface” section on page 19-3.

SSID

The WLAN associates a service set identifier (SSID) to the Wi-Fi interface. An SSID must be assigned to the Wi-Fi interface for it to be active in the network.

The SSID can be suppressed such that it is not advertised in the 802.11 beacons. Multiple SSIDs can be configured but the Wi-Fi interface supports only one SSID—only one active SSID can be assigned at a time to the Wi-Fi Interface.

Security

The Wi-Fi interface supports none, Wired Equivalent Privacy (WEP), WPA2, and WPA1/WPA2 mode.

This section contains information about:

- WEP, page 19-2
- WPA2, page 19-3
- WPA1/WPA2, page 19-3

WEP

WEP is the encryption algorithm built into the 802.11 (Wi-Fi) standard. WEP encryption uses the Ron's Code 4 (RC4) Stream Cipher with 40- or 104-bit keys and a 24-bit initialization vector (IV).
As the standard specifies, WEP uses the RC4 algorithm with a 40-bit or 104-bit key and a 24-bit IV. RC4 is a symmetric algorithm because it uses the same key for the encryption and the decryption of data. When WEP is enabled, each radio station has a key. The key is used to scramble the data before transmission of the data through the airwaves. If a station receives a packet that is not scrambled with the appropriate key, the packet is discarded and never delivered to the host.

Two methods of authentication can be used with WEP: Open System authentication and Shared Key authentication.

**WPA2**

WPA2 provides full implementation of the IEEE 802.11i standard for WLANs and supports the enhanced AES-CCMP encryption algorithm.

**WPA1/WPA2**

WPA1/WPA2 mode allows support of WPA/TKIP and WPA2/AES-CCMP clients on a common SSID. The access point advertises the available encryption methods (TKIP, AES-CCMP) on the network, and the Wi-Fi client then selects which security method it wants to employ.

## Configuring the Wi-Fi Interface

You can configure the Wi-Fi interface to AP mode or station mode.

This section includes:

- Configuring Wireless Mode, page 19-3
- Configuring the Wi-Fi Interface for AP Mode, page 19-4
- Configuring the Wi-Fi Interface for Station Mode, page 19-7

### Configuring Wireless Mode

Beginning in privileged EXEC mode, follow these steps to choose AP mode or station mode for the radio interface.

<table>
<thead>
<tr>
<th>Step</th>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>2</td>
<td>interface dot11radio 0</td>
<td>Enter 802.11 radio interface configuration mode, and enter the interface number.</td>
</tr>
<tr>
<td>3</td>
<td>dot11mode {ap</td>
<td>sta auto-connect {on</td>
</tr>
<tr>
<td>4</td>
<td>exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>5</td>
<td>copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>
Chapter 19  Configuring the Wi-Fi Interface

Configuring the Wi-Fi Interface for AP Mode

- Creating an SSID and Binding an AP Profile, page 19-4
- Configuring AP Settings, page 19-4
- Configuring AP Profiles, page 19-6

Creating an SSID and Binding an AP Profile

The service set identifier (SSID) is a unique identifier of the wireless network that wireless networking devices use to establish and maintain wireless connectivity. Multiple access points on a network or sub-network can use the same SSID. An SSID name is case sensitive and can contain up to 32 alphanumeric characters. Do not include spaces in your SSID name.

You must define an SSID for the Wi-Fi interface to activate the interface within the network.

**Note**

Only one active SSID can be associated with the interface.

Beginning in privileged EXEC mode, follow these steps to create an AP profile and associate the radio interface to the profile.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 dot11ap ssid ssid-name</td>
<td>Create 802.11 AP profile.</td>
</tr>
<tr>
<td>Step 3 interface dot11radio 0</td>
<td>Enter 802.11 radio interface configuration mode, and enter the interface number.</td>
</tr>
<tr>
<td>Step 4 ssid ssid-name</td>
<td>Create an SSID.</td>
</tr>
<tr>
<td>Step 5 exit</td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td>Step 6 copy running-config startup-config</td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

This example shows how to associate an SSID to the Wi-Fi interface.

```
Router(config)# configure terminal
Router(config)# dot11ap ssid test-ap
Router(config)# interface dot11radio 0
Router(config-if)# ssid test-ap
```

Configuring AP Settings

Beginning in privileged EXEC mode, follow these steps to configure the AP settings:

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1 configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
<tr>
<td>Step 2 interface dot11radio 0</td>
<td>Enter 802.11 radio interface configuration mode, and enter the interface number.</td>
</tr>
</tbody>
</table>
### Step 3

**Command**: bandwidth {ht20 | ht40}

Configure the bandwidth of the AP. The bandwidth value includes ht20 and ht40.
- ht20—High-throughput 20 MHz.
- ht40—High-throughput 40 MHz.

---

### Step 4

**Command**: speed 2.4g speed-string

Specify the radio data rates.

The *speed-string* value can be one of the following:
- 36.0
- 48.0
- 54.0
- 36.0 48.0
- 48.0 54.0
- 36.0 54.0
- 36.0 48.0 54.0

---

### Step 5

**Command**: short-gi {enable | disable}

Enable or disable the short guard interval which is used to ensure that distinct transmissions occur between the successive data symbols transmitted by a device.

---

### Step 6

**Command**: ssid-hidden {enable | disable}

Enable or disable hiding the SSID when scanning the WLAN.

---

### Step 7

**Command**: ampdu {0 | 1/4 | 1/2 | 1 | 2 | 4 | 8 | 16}

Configure aggregate MAC Protocol Data Unit (A-MPDU), which joins multiple MPDU sub frames with a single leading PHY header.

---

### Step 8

**Command**: ap-isolation {enable | disable}

Enable or disable AP Isolation. AP Isolation effectively creates a virtual network among wireless clients, where each device is an individual entity that cannot communicate with other wireless devices on the same Wi-Fi access point.

---

### Step 9

**Command**: power local value

Set the transmit power for the AP. The value could be 8–17 or maximum.

---

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3  bandwidth {ht20</td>
<td>ht40}</td>
</tr>
<tr>
<td>Step 4  speed 2.4g speed-string</td>
<td>Specify the radio data rates. The <em>speed-string</em> value can be one of the following:</td>
</tr>
<tr>
<td>Step 5  short-gi {enable</td>
<td>disable}</td>
</tr>
<tr>
<td>Step 6  ssid-hidden {enable</td>
<td>disable}</td>
</tr>
<tr>
<td>Step 7  ampdu {0</td>
<td>1/4</td>
</tr>
<tr>
<td>Step 8  ap-isolation {enable</td>
<td>disable}</td>
</tr>
<tr>
<td>Step 9  power local value</td>
<td>Set the transmit power for the AP. The value could be 8–17 or maximum.</td>
</tr>
</tbody>
</table>
Chapter 19  Configuring the Wi-Fi Interface

Configuring AP Profiles

Beginning in privileged EXEC mode, follow these steps to create an AP profile and associate the radio interface to the profile.

Step 10

```
band {5a | 5an | 2.4bg | 2.4bgn}
channel channel_number
```

Specify radio band and channel as following. The country code for United States is US, China is CN, and Japan is JP.

- 2.4bg supports 802.11b, 802.11g
- 2.4bgn supports 802.11b, 802.11g, and 802.11n
- 5a supports 802.11a
- 5an supports 802.11a, 802.11n
- All of 2.4bg/2.4bgn are supported to use in China.
- All of 5a, 5an, 2.4bg, 2.4bgn are supported to use in US and JP.
- CN does not support 5a and 5an Channel
- US 2.4bg and 2.4bgn support Channel 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, and 11.
- JP 2.4bg and 2.4bgn support Channel 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, and 14.
- CN 2.4bg and 2.4bgn support Channel 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13.

Step 11

```
beacon dtim-period value
```

Specify the Delivery traffic indication message (DTIM), which informs the clients about the presence of buffered multicast or broadcast data on the access point. The default value is 1. Value range is 1–100.

Step 12

```
beacon period value
```

Specify the interval between periodic beacons. The default value is 100. Value range is 50–1000.

Step 13

```
rts_threshold value
```

Configure the request to send (RTS) threshold, which specifies the packet size of an RTS transmission. This parameter can help control traffic flow through the access point, especially when there are many clients connected. The default value is 2346. Value range is 1000–2347.

Step 14

```
packet retries value
```

Specify the maximum data retries. Value range is 1–10. Default is 5.

Step 15

```
fragment-threshold value
```

Specify the maximum frame size which wireless device can transmit without fragmenting the frame. The default value is 2346. Value range is 1000–2346.

Step 16

```
exit
```

Return to global configuration mode.

Step 17

```
copy running-config startup-config
```

(Optional) Save your entries in the configuration file.
### Configuring the Wi-Fi Interface

**Creating an STA Profile with an SSID**

Beginning in privileged EXEC mode, follow these steps to create an STA profile with an SSID.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>configure terminal</td>
<td>Enter global configuration mode.</td>
</tr>
</tbody>
</table>
| dot11sta ssid ssid-name | Create a 802.11 STA profile. The length of SSID is 1–32. You can create up to five STA profiles. These characters are not supported: +, \, ], ?, $, TAB, and trailing spaces. Do not use # or ! at the beginning of the SSID name. 
|                     | **Note** Up to ten STA profiles can be connected to an AP.             |
### Chapter 19      Configuring the Wi-Fi Interface

**Configuring the Wi-Fi Interface**

This example shows how to create an STA profile with a WEP key:

```
Router(config)# configure terminal
Router(config)# dot11sta ssid test-sta
Router(config-ap)# wep-key 3 size 128 12345678901234567890123456 transmit-key
```

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Step 3</strong></td>
<td></td>
</tr>
<tr>
<td>`authmode {open</td>
<td>shared}`</td>
</tr>
<tr>
<td></td>
<td>• <strong>open</strong>—Although every user can connect to an AP, the receiver cannot receive any packets from the sender.</td>
</tr>
<tr>
<td></td>
<td>• <strong>shared</strong>—Key-index and password are needed to connect to an AP.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>Only WEP encryption requires to use the <code>authmode</code> command to connect to an AP.</td>
</tr>
<tr>
<td><strong>Step 4</strong></td>
<td></td>
</tr>
<tr>
<td>`encryption {none</td>
<td>wep</td>
</tr>
<tr>
<td><strong>Step 5</strong></td>
<td></td>
</tr>
<tr>
<td>`wep-key 0-3 size {64</td>
<td>128}`</td>
</tr>
<tr>
<td></td>
<td>• For <strong>64</strong>, enter a string of 10 hexadecimal digits or 5 ASCII numbers.</td>
</tr>
<tr>
<td></td>
<td>• For <strong>128</strong>, enter a string of 26 hexadecimal digits or 13 ASCII numbers.</td>
</tr>
<tr>
<td></td>
<td>The encryption is WEP.</td>
</tr>
<tr>
<td></td>
<td>or</td>
</tr>
<tr>
<td>`wpa-psk {hex</td>
<td>ascii}`</td>
</tr>
<tr>
<td></td>
<td>• For <strong>hex</strong>, enter a string of 64 hexadecimal characters.</td>
</tr>
<tr>
<td></td>
<td>• For <strong>ascii</strong>, enter a string of 8 to 63 ASCII characters (including special characters) and numbers.</td>
</tr>
<tr>
<td><strong>Note</strong></td>
<td>In the STA mode, the mode of none, WEP, WPA2, or WPA1WPA2 cannot be automatically detected. And The encryption is WPA-PSK.</td>
</tr>
<tr>
<td><strong>Step 6</strong></td>
<td></td>
</tr>
<tr>
<td><code>priority priority-level</code></td>
<td>Set the priority of the STA profile. The priority level must be an integer larger than 0. A smaller value of priority level refers to a higher priority.</td>
</tr>
<tr>
<td><strong>Step 7</strong></td>
<td></td>
</tr>
<tr>
<td><code>exit</code></td>
<td>Return to global configuration mode.</td>
</tr>
<tr>
<td><strong>Step 8</strong></td>
<td></td>
</tr>
<tr>
<td><code>copy running-config startup-config</code></td>
<td>(Optional) Save your entries in the configuration file.</td>
</tr>
</tbody>
</table>

This example shows how to create an STA profile with a WEP key:

```
Router(config)# configure terminal
Router(config)# dot11sta ssid test-sta
Router(config-ap)# wep-key 3 size 128 12345678901234567890123456 transmit-key
```

### Configuring SSID Scan

To scan the SSIDs, use the `dot11 scan-channel` privileged EXEC command:

The following example shows an sample output of the `dot11 scan-channel 2.4g` command:

```
Router #dot11 scan-channel 2.4g
```

<table>
<thead>
<tr>
<th>#</th>
<th>ch</th>
<th>ss</th>
<th>bssid</th>
<th>SSID</th>
</tr>
</thead>
<tbody>
<tr>
<td>01</td>
<td>001</td>
<td>202</td>
<td>00:23:f8:0a:84:3e</td>
<td>AP999</td>
</tr>
<tr>
<td>02</td>
<td>001</td>
<td>195</td>
<td>00:03:7f:00:00:18</td>
<td>FX_MIS2</td>
</tr>
<tr>
<td>03</td>
<td>001</td>
<td>211</td>
<td>00:03:7f:24:00:08</td>
<td>FX_MIS</td>
</tr>
<tr>
<td>04</td>
<td>001</td>
<td>164</td>
<td>00:1b:0c:65:43:0d</td>
<td>MIS-XB</td>
</tr>
<tr>
<td>05</td>
<td>001</td>
<td>162</td>
<td>00:03:7f:46:01:5f</td>
<td>FX_crd</td>
</tr>
<tr>
<td>06</td>
<td>001</td>
<td>159</td>
<td>00:1b:0c:65:43:0e</td>
<td>voice</td>
</tr>
<tr>
<td>07</td>
<td>001</td>
<td>169</td>
<td>00:22:cf:56:26:80</td>
<td>GW-USMicro300</td>
</tr>
<tr>
<td>08</td>
<td>001</td>
<td>157</td>
<td>00:03:7f:24:00:03</td>
<td>FX_MIS</td>
</tr>
</tbody>
</table>
Connecting To or Disconnecting From an AP

To connect to an AP, use the `dot11sta connect` privileged EXEC command.
To connect to a list of APs, use the `dot11sta exec_connect_prefer` privileged EXEC command.
To disconnect from an AP, use the `dot11sta disconnect ssid` privileged EXEC command.

Checking the STA Connecting Status

To check the STA connection status, use the `dot11sta check_connect_status` privileged EXEC command.

Monitoring Wi-Fi Information

You can display specific statistics of the Wi-Fi settings. Table 19-1 lists the privileged EXEC commands for displaying Wi-Fi information.

<table>
<thead>
<tr>
<th>Command</th>
<th>Purpose</th>
</tr>
</thead>
<tbody>
<tr>
<td>show dot11 mode</td>
<td>Display the radio mode.</td>
</tr>
<tr>
<td>show interfaces dot11radio 0 association</td>
<td>Display the radio association.</td>
</tr>
<tr>
<td>show dot11ap profile {ssid ssid-string</td>
<td>all}</td>
</tr>
<tr>
<td>show dot11sta prefer-list</td>
<td>Display the station prefer list.</td>
</tr>
<tr>
<td>show dot11sta ssid {ssid-string</td>
<td>all}</td>
</tr>
</tbody>
</table>

The following command displays the radio association:

```
Router# show interfaces dot11radio 0 association
uap0  IEEE 802.11-DS  ESSID:"
Mode:Master  Frequency:2.437 GHz  Access Point: Not-Associated
Encryption key:off
Link Quality:0  Signal level:0 Noise level:0
Rx invalid nwid:0  Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0  Invalid misc:0 Missed beacon:0
```

The following command displays the AP profile:

```
Router# show dot11ap profile ssid testap
SSID     Mode       Encryption        WEP Key        WPA Key     Encrypcipher
Authserver Addr port key-----------------------------------------------
-----------------------------------------------
testap
```

The following command displays the station prefer list:

```
Router# show dot11sta prefer-list
```
1. SSID:testap1
2. SSID:testap2
3. SSID:testap3