Configuring the Wireless Device

The following sections describe how to configure the wireless device on the Cisco 1941W integrated services router (ISR):

Note You can upgrade the software on the device to Cisco Unified software. See the "Upgrading to Cisco Unified Software" section on page 255.

Note The wireless device is embedded on the router and does not have an external console port for connections. To configure the wireless device, use a console cable to connect a personal computer to the host router's Console serial port, and follow the instruction to establish a configuration session.

Starting a Wireless Configuration Session

Enter the following commands in global configuration mode on the router's Cisco IOS command-line interface (CLI).

SUMMARY STEPS

1. **interface wlan-ap0**
2. **ip address** ***subnet mask***
3. **no shut**
4. **interface vlan1**
5. **ip address** ***subnet mask***
6. **exit**
7. **exit**
8. **service-module wlan-ap 0 session**

DETAILED STEPS

	Command	Purpose

Step 1	**interface wlan-ap0**
	
	Example:
	`router(config)# interface wlan-ap0`
	`router(config-if)#`
		Defines the router's console interface to the wireless device. It is used for communication between the router's Console and the wireless device.
		Always use port 0.
		The following message appears:
		`The wlan-ap 0 interface is used for managing the embedded AP. Please use the` **`service-module wlan-ap 0 session`** `command to console into the embedded AP.`

Step 2	**ip address** *subnet mask*
	
	Example:
	`router(config-if)# ip address 10.21.0.20 255.255.255.0`
	
	Example:
	`router(config-if)# ip unnumbered vlan1`
		Specifies the interface IP address and subnet mask.
		Note The IP address can be shared with the IP address assigned to the Cisco Integrated Services Router by using the **ip unnumbered vlan1** command.

Step 3	**no shut** **Example:** `router(config-if)# no shut`	Specifies the internal interface connection remains open.
Step 4	**interface vlan1** **Example:** `router(config-if)# interface vlan1`	Specifies the virtual LAN interface for data communication on the internal GE0[1] port to other interfaces.
Step 5	**ip address** *subnet mask* **Example:** `router(config-if)# ip address 10.10.0.30 255.255.255.0`	Specifies the interface IP address and subnet mask.

Step 6	**exit**
	
	Example:
	`router(config-if)# exit`
	`router(config)#`
		Exits the mode.

	Command	Purpose

Step 7	**exit**
	
	Example:
	`router(config)# exit`
	`router#`
		Exits the mode.

Step 8	**service-module wlan-ap 0 session**
	
	Example:
	`router# service-module wlan-ap0 session`
	`Trying 10.21.0.20, 2002 ... Open`
	
	`ap>`
		Opens the connection between the wireless device and the router's console.

1. GE0 = Gigabit Ethernet 0

Tip If you want to create an IOS software alias for the Console to session into the wireless device, enter the **alias exec dot11radio service-module wlan-ap 0 session** command at the EXEC prompt. After entering this command, you automatically skip to the **dot11 radio** level in the IOS.

Closing the Session

To close the session between the wireless device and the router's console, perform both of the following steps.

Wireless Device

1. **Control-Shift-6 x**

Router

2. **disconnect**
3. Press **Enter** twice.

Configuring Wireless Settings

Note If you are configuring the autonomous wireless device for the first time, start a configuration session between the router and the access point before attempting to configure basic wireless settings. See the "Starting a Wireless Configuration Session" section on page 247.

Configure the wireless device with the appropriate software tool.

- Unified software—Cisco Express Setup, page 250
- Autonomous software—Cisco IOS CLI, page 250

Cisco Express Setup

To configure the Cisco Unified wireless device use the web-browser Cisco Express Setup tool:

Step 1 Establish a Console connection to the wireless device and get the BVI IP address by entering the **show interface bvi1 IOS** command.

Step 2 Open a browser window and enter the BVI IP address in the browser-window address line. Press enter and an Enter Network Password window appears.

Step 3 Enter your username. *Cisco* is the default User Name.

Step 4 Enter the wireless device password. *Cisco* is the default password. The Summary Status page appears. See the following URL for details about using the web-browser configuration page: http://cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/configuration/guide/scg12410b-chap4-first.html#wp1103336

Cisco IOS CLI

To configure the Autonomous wireless device, establish a session between the router and the access point, then use the Cisco IOS CLI tool:

- Configuring the Radio, page 250
- Configuring Wireless Security Settings, page 251
- Configuring Wireless Quality of Service, page 254 (Optional)
- Configuring the Access Point in Hot Standby Mode, page 255 (Optional)

Configuring the Radio

Configure the radio parameters on the wireless device to transmit signals. See Chapter 16, “Configuring Radio Settings,” for specific configuration procedures.

Configuring Wireless Security Settings

Configuring Authentication

Authentication types are tied to the Service Set Identifiers (SSIDs) that are configured for the access point. If you want to serve different types of client devices with the same access point, configure multiple SSIDs.

Before a wireless client device can communicate on your network through the access point, it must authenticate to the access point by using open or shared-key authentication. For maximum security, client devices should also authenticate to your network using MAC-address or Extensible Authentication Protocol (EAP) authentication. Both of these authentication types rely on an authentication server on your network.

See *Authentication Types for Wireless Devices* at Cisco.com to select an authentication type: http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityAuthenticationTypes.html

See *RADIUS and TACACS+ Servers in a Wireless Environment* at Cisco.com to set up a maximum security environment: http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityRadiusTacacs_1.html.

Configuring Access Point as Local Authenticator

To provide local authentication service or backup authentication service for a WAN link failure or circumstance where a server fails, you can configure an access point to act as a local authentication server. The access point can authenticate up to 50 wireless client devices using Light Extensible Authentication Protocol (LEAP), Extensible Authentication Protocol-Flexible Authentication Secure Tunneling (EAP-FAST), or MAC-based authentication. The access point performs up to five authentications per second.

You configure the local authenticator access point manually with client user names and passwords because it does not synchronize its database with Remote Authentication Dial-In User Service (RADIUS) servers. You can specify a VLAN and a list of SSIDs that a client is allowed to use.

See *Using the Access Point as a Local Authenticator* at Cisco.com for details about setting up the wireless device in this role: http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityLocalAuthent.html

Configuring WEP and Cipher Suites

Wired Equivalent Privacy (WEP) encryption scrambles the data transmitted between wireless devices to keep the communication private. Wireless devices and their wireless client devices use the same WEP key to encrypt and decrypt data. WEP keys encrypt both unicast and multicast messages. Unicast messages are addressed to one device on the network. Multicast messages are addressed to multiple devices on the network.

Cipher suites are sets of encryption and integrity algorithms designed to protect radio communication on your wireless LAN. You must use a cipher suite to enable Wi-Fi Protected Access (WPA) or Cisco Centralized Key Management (CCKM).

Cipher suites that contain TKIP provide the best security for your wireless LAN. Cipher suites that contain only WEP are the least secure.

See *Configuring WEP and Cipher Suites* for encryption procedures:
http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityCipherSuitesWEP.html

Configuring Wireless VLANs

If you use VLANs on your wireless LAN and assign SSIDs to VLANs you can create multiple SSIDs by using any of the four security settings defined in the "Security Types" section on page 253. A VLAN can be thought of as a broadcast domain that exists within a defined set of switches. A VLAN consists of a number of end systems, either hosts or network equipment (such as bridges and routers), connected by a single bridging domain. The bridging domain is supported on various pieces of network equipment such as LAN switches that operate bridging protocols between them with a separate group of protocols for each VLAN.

See *Configuring Wireless VLANs* at Cisco.com for more about wireless VLAN architecture:
http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/wireless_vlans.html

Note If you do not use VLANs on your wireless LAN, the security options that you can assign to SSIDs are limited because the encryption settings and authentication types are linked on the Express Security page.

Assigning SSIDs

You can configure up to 16 SSIDs on a wireless device in the role of an access point and configure a unique set of parameters for each SSID. For example, you might use one SSID to allow guests to have limited access to the network and another SSID to allow authorized users to have access to secure data.

See *Service Set Identifiers* at Cisco.com for more about creating multiple SSIDs,
http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/ServiceSetID.html.

Note Without VLANs, encryption settings (WEP and ciphers) apply to an interface, such as the 2.4-GHz radio, and you cannot use more than one encryption setting on an interface. For example, when you create an SSID with static WEP with VLANs disabled, you cannot create additional SSIDs with Wi-Fi Protected Access (WPA) authentication because the SSIDs use different encryption settings. If you find that the security setting for an SSID conflicts with the settings for another SSID, you can delete one or more SSIDs to eliminate the conflict.

Security Types

Table 1 describes the four security types that you can assign to an SSID.

Table 1 Types of SSID Security

Security Type	Description	Security Features Enabled
No Security	This is the least secure option. You should use this option only for SSIDs used in a public space and assign it to a VLAN that restricts access to your network.	None.
Static WEP Key	This option is more secure than no security. However, static WEP keys are vulnerable to attack. If you configure this setting, you should consider limiting association to the wireless device based on MAC address. See *Cipher Suites and WEP* at Cisco.com for configuration procedures, http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityCipherSuitesWEP.html . Or If your network does not have a RADIUS server, consider using an access point as a local authentication server. See *Using the Access Point as a Local Authenticator* at Cisco.com for instructions, http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityLocalAuthent.html.	Mandatory WEP. Client devices cannot associate using this SSID without a WEP key that matches the wireless device key.

Table 1 Types of SSID Security (continued)

Security Type	Description	Security Features Enabled
EAP[1] Authentication	This option enables 802.1X authentication (such as LEAP[2], PEAP[3], EAP-TLS[4], EAP-FAST[5], EAP-TTLS[6], EAP-GTC[7] EAP-SIM[8], and other 802.1X/EAP based products) This setting uses mandatory encryption, WEP, open authentication + EAP, network EAP authentication, no key management, RADIUS server authentication port 1645. You are required to enter the IP address and shared secret for an authentication server on your network (server authentication port 1645). Because 802.1X authentication provides dynamic encryption keys, you do not need to enter a WEP key.	Mandatory 802.1X authentication. Client devices that associate using this SSID must perform 802.1X authentication. If radio clients are configured to authenticate using EAP-FAST, open authentication with EAP should also be configured. If you do not configure open authentication with EAP, the following warning message appears: `SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.`
WPA[9]	This option permits wireless access to users authenticated against a database through the services of an authentication server, then encrypts their IP traffic with stronger algorithms than those used in WEP. This setting uses encryption ciphers, TKIP[10], open authentication + EAP, network EAP authentication, key management WPA mandatory, and RADIUS server authentication port 1645. As with EAP authentication, you must enter the IP address and shared secret for an authentication server on your network (server authentication port 1645).	Mandatory WPA authentication. Client devices that associate using this SSID must be WPA-capable. If radio clients are configured to authenticate using EAP-FAST, open authentication with EAP should also be configured. If you don't configure open authentication with EAP, the following message appears: `SSID CONFIG WARNING: [SSID]: If radio clients are using EAP-FAST, AUTH OPEN with EAP should also be configured.`

1. EAP = Extensible Authentication Protocol.
2. LEAP = Lightweight Extensible Authentication Protocol.
3. PEAP = Protected Extensible Authentication Protocol.
4. EAP-TLS = Extensible Authentication Protocol - Transport Layer Security.
5. EAP-FAST = Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling.
6. EAP-TTLS = Extensible Authentication Protocol-Tunneled Transport Layer Security.
7. EAP-GTC = Extensible Authentication Protocol--Generic Token Card.
8. EAP-SIM = Extensible Authentication Protocol--Subscriber Identity Module.
9. WA = Wi-Fi Protected Access.
10. TKIP = Temporal Key Integrity Protocol.

Configuring Wireless Quality of Service

Configuring Quality of Service (QoS) can provide preferential treatment to certain traffic at the expense of other traffic. Without QoS, the device offers best-effort service to each packet, regardless of the packet contents or size. It sends the packets without any assurance of reliability, delay bounds, or throughput. To configure quality of service (QoS) for your wireless device, see *Quality of Service in a Wireless Environment* at:
http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/QualityOfService.html.

Configuring the Access Point in Hot Standby Mode

In hot standby mode, an access point is designated as a backup for another access point. The standby access point is placed near the access point that it monitors and is configured exactly like the monitored access point. The standby access point associates with the monitored access point as a client and sends Internet Access Point Protocol (IAPP) queries to the monitored access point through the Ethernet and radio ports. If the monitored access point fails to respond, the standby access point comes online and takes the monitored access point's place in the network.

Except for the IP address, the standby access point's settings should be identical to the settings on the monitored access point. If the monitored access point goes off line and the standby access point takes its place in the network, matching settings ensure that client devices can switch easily to the standby access point. See *Hot Standby Access Points* at Cisco.com for more information: http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/RolesHotStandby.html.

Upgrading to Cisco Unified Software

To run the access point in Cisco Unified mode, upgrade the software by following these major steps:

- Preparing for the Upgrade, page 255
- Performing the Upgrade, page 256
- Downgrading the Software on the Access Point, page 257
- Recovering Software on the Access Point, page 257

Software Prerequisites

- Cisco 1941W ISRs are eligible to upgrade to Cisco Unified software, if the router is running IP Base feature set and Cisco IOS Release 15.0(1)M.
- To use the embedded access point in a Cisco Unified Architecture, the Cisco wireless LAN controller (WLC) must be running version 5.1 or later.

Preparing for the Upgrade

Perform these tasks to prepare for the upgrade:

- Secure an IP Address on the Access Point, page 255
- Prior to the Upgrade, page 256

Secure an IP Address on the Access Point

Secure an IP address on the access point so it can communicate with the WLC and download the Unified image upon boot up. The host router provides the access point DHCP server functionality through the DHCP pool. Then the access point communicates with the WLC and setup option 43 for the controller IP address in the DHCP pool configuration. The following is a sample configuration:

```
ip dhcp pool embedded-ap-pool
network 60.0.0.0 255.255.255.0
dns-server 171.70.168.183
default-router 60.0.0.1
option 43 hex  f104.0a0a.0a0f   (single WLC IP address(10.10.10.15) in hex format)
int vlan1
ip address 60.0.0.1 255.255.255.0
```

For more information about the WLC discovery process, see *Cisco Wireless LAN Configuration Guide* at Cisco.com:
http://www.cisco.com/en/US/docs/wireless/controller/4.0/configuration/guide/ccfig40.html

Prior to the Upgrade

Perform the following steps.

1. Ping the WLC from the router to confirm IP connectivity.
2. Enter the **service-module wlan-ap 0 session** command to establish a session with the access point.
3. Confirm that the access point is running an autonomous boot image.
4. Enter the **show boot** command on the access point to confirm the mode setting is enabled. The following is sample output for the command:

```
Autonomous-AP# show boot
BOOT path-list:      flash:ap801-k9w7-mx.124-10b.JA3/ap801-k9w7-mx.124-10b.JA3
Config file:         flash:/config.txt
Private Config file: flash:/private-config
Enable Break:        yes
Manual Boot:         yes
HELPER path-list:
NVRAM/Config file
buffer size:   32768
Mode Button:    on
```

Performing the Upgrade

To upgrade to Unified software, follow these steps:

Step 1 Issue the **service-module wlan-ap 0 bootimage unified** command to change the access point boot image to the Unified upgrade image, which is also known as a *recovery image*.

```
Router# conf terminal
Router(config)# service-module wlan-ap 0 bootimage unified
Router(config)# end
```

Note If the **service-module wlan-ap 0 bootimage unified** command does not work successfully, check to see whether the software license is still eligible.

On the access point console, use the **show boot** command to identify the access point's boot image path:

```
autonomous-AP# show boot
BOOT path-list:      flash:/ap801-rcvk9w8-mx/ap801-rcvk9w8-mx
```

Step 2 Issue the **service-module wlan-ap 0 reload** command to perform a graceful shutdown and reboot the access point and complete the upgrade process. Session into the access point and monitor the upgrade process.

See the "Cisco Express Setup" section on page 250 for details about using the Web-based configuration page to configure the wireless device settings.

Troubleshooting an Upgrade or Reverting the AP to Autonomous Mode

Q. My access point failed to upgrade from autonomous software to Unified software and it appears to be stuck in the recovery mode. What is my next step?

A. Check the following items:

- Is the IP address on the BVI interface on the same subnet as the WLC?
- Can you ping the WLC from the router/access point to confirm connectivity?
- Is the access point set to the current date and time? Use the **show clock** command to confirm this information.

Q. My access point is attempting to boot, but it keeps failing. Why?
My access point is stuck in the recovery image and will not upgrade to the Unified software. Why?

A. The access point is stuck in recovery mode and you must use the **service-module wlan-ap0 reset bootloader** command to return the access point back to bootloader for manual image recovery.

Downgrading the Software on the Access Point

Use the **service-module wlan-ap0 bootimage autonomous** command to reset the access point BOOT back to the last autonomous image. Use the **service-module wlan-ap 0 reload** command to reload the access point with the autonomous software image.

Recovering Software on the Access Point

To recover the image on the access point, use the **service-module wlan-ap0 reset bootloader** command. This command returns the access point to the bootloader for manual image recovery.

Caution Use this command with caution. Use this command only to recover from a shutdown or failed state.

Related Documentation

See the following documentation for additional autonomous and unified configuration information:

- Autonomous Documentation—Table 2
- Unified Documentation—Table 3

Table 2 Autonomous Documentation

Network Design	Links	Description
Wireless Overview	"Wireless Device Overview"	Describes the roles of the wireless device on the network.
Configuration	**Links**	
Configuring the Radio	"Configuring Radio Settings"	Describes how to configure the wireless radio.
Security	**Links**	
Authentication Types for Wireless Devices	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityAuthenticationTypes.html	Describes the authentication types that are configured on the access point.
RADIUS and TACACS+ Servers in a Wireless Environment	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityRadiusTacacs_1.html	Describes how to enable and configure the RADIUS[1] and TACACS+[2] and provides detailed accounting information and flexible administrative control over authentication and authorization processes. RADIUS and TACACS+ are facilitated through AAA and can be enabled only through AAA commands.
Using the Access Point as a Local Authenticator	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityLocalAuthent.html	Describes how to use a wireless device in the role of an access point as a local authenticator, serving as a standalone authenticator for a small wireless LAN, or providing backup authentication service. As a local authenticator, the access point performs LEAP, EAP-FAST, and MAC-based authentication for up to 50 client devices.
Cipher Suites and WEP	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityCipherSuitesWEP.html	Describes how to configure the cipher suites required for using WPA[3] and CCKM[4]; WEP[5]; and WEP features including AES[6], MIC[7], TKIP[8], and broadcast key rotation.
Hot Standby Access Points	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/RolesHotStandby.html	Describes how to configure your wireless device as a hot standby unit.
Configuring Wireless VLANs	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/wireless_vlans.html	Describes how to configure an access point to operate with the VLANs set up on a wired LAN.
Service Set Identifiers	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/ServiceSetID.html	In the role of an access point, a wireless device can support up to 16 SSIDs[9]. This document describes how to configure and manage SSIDs on the wireless device.
Administering	**Links**	**Description**
Administering the Access Point	"Administering the Wireless Device"	Describes how to administer the wireless device on the network.

Table 2 Autonomous Documentation (continued)

Quality of Service	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/QualityOfService.html	Describes how to configure QoS[10] on your Cisco wireless interface. With this feature, you can provide preferential treatment to certain traffic at the expense of other traffic. Without QoS, the device offers best-effort service to each packet, regardless of the packet contents or size. It sends the packets without any assurance of reliability, delay bounds, or throughput.
Regulatory Domains and Channels	http://www.cisco.com/en/US/docs/routers/access/800/860-880-890/software/configuration/guide/scg_chanels.html	Lists the radio channels supported by Cisco access products in the regulatory domains of the world.
System Message Logging	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SysMsgLogging.html	Describes how to configure system message logging on your wireless device.

1. RADIUS = Remote Authentication Dial-In User Service
2. TACACS+ = Terminal Access Controller Access Control System Plus
3. WPA = Wireless Protected Access
4. CCKM = Cisco Centralized Key Management
5. WEP = Wired Equivalent Privacy
6. AES = Advanced Encryption Standard
7. MIC = Message Integrity Check
8. TKIP = Temporal Key Integrity Protocol
9. SSID = service set identifiers
10. QoS = quality of service

Table 3 Unified Documentation

Network Design	Links
Why Migrate to the Cisco Unified Wireless Network?	http://www.cisco.com/en/US/solutions/ns175/networking_solutions_products_genericcontent0900aecd805299ff.html
Wireless LAN Controller (WLC) FAQ	http://www.cisco.com/en/US/products/ps6366/products_qanda_item09186a008064a991.shtml
Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges, versions 12.4(10b) JA and 12.3(8) JEC	http://www.cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/command/reference/cr2410b.html
Cisco Aironet 1240AG Access Point Support Documentation	http://www.cisco.com/en/US/docs/wireless/access_point/1240/quick/guide/ap1240qs.html
Cisco 4400 Series Wireless LAN Controllers Support Documentation	http://www.cisco.com/en/US/products/ps6366/tsd_products_support_series_home.html