CHAPTER 8

Basic Wireless Device Configuration

This module describes how to configure the autonomous wireless device on the following Cisco Integrated Services Routers (ISRs):

- Cisco 860 Series
- Cisco 880 Series
- Cisco 890 Series

Note To upgrade the autonomous software to Cisco Unified software on the embedded wireless device, see the "Upgrading to Cisco Unified Software" section on page 8-9 for instructions.

The wireless device is embedded 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 port, and perform these procedures to establish connectivity and configure the wireless settings.

- Starting a Wireless Configuration Session, page 8-2
- Configuring Wireless Settings, page 8-4
- Configuring the Access Point in Hot Standby Mode, page 8-9 (Optional)
- Upgrading to Cisco Unified Software, page 8-9
- Related Documentation, page 8-12

Starting a Wireless Configuration Session

Note Before you configure the wireless settings in the router's setup, you must follow these steps to open a session between the router and the access point.

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 or Action	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.
		• The interface is used for communication between the router's console and the wireless device.
		Note 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`
	`or`
	`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 that the internal interface connection will remain open.

	Command or Action	Purpose
Step 4	**interface vlan1** **Example:** `Router(config-if)# interface vlan1`	Specifies the virtual LAN interface for data communication on the internal Gigabit Ethernet 0 (GE0) port to other interfaces. • All the switch ports inherit the default vlan1 interface on the Cisco 860 Series, Cisco 880 Series, and Cisco 890 Series ISRs.

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 interface configuration mode and returns to global configuration mode.

Step 7	**exit**
	Example:
	`Router(config)# exit`
	`Router#`
		Exits the global configuration 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.

Tip To create a Cisco 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 utomatically skip to the **dot11 radio** level in the Cisco IOS software.

Closing the Session

To close the session between the wireless device and the router's console, perform 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 wireless device for the first time, you must start a configuration session between the access point and the router before you attempt to configure the basic wireless settings. See the "Starting a Wireless Configuration Session" section on page 8-2.

Configure the wireless device with the tool that matches the software on the device.

- Cisco IOS Command Line Interface, page 8-5—Autonomous software
- Cisco Express Setup, page 8-4—Unified Software

Note To upgrade to Unified mode from the Autonomous mode, see the "Upgrading to Cisco Unified Software" section on page 8-9 for upgrade instructions.

After upgrading to Cisco Unified Wireless software, use the web-browser tool to configure the device:
http://cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/configuration/guide/scg12410b-chap2-gui.html

Cisco Express Setup

To configure the Unified wireless device, use the web-browser tool:

Step 1 Establish a console connection to the wireless device and get the Bridge-Group Virtual Interface (BVI) IP address by entering the **show interface bvi1 Cisco** IOS command.

Step 2 Open a browser window, and enter the BVI IP address in the browser-window address line. Press **Enter**. 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. For details about using the web-browser configuration page, see the following URL:

http://cisco.com/en/US/docs/wireless/access_point/12.4_10b_JA/configuration/guide/scg12410b-chap4-first.html#wp1103336

Cisco IOS Command Line Interface

To configure the Autonomous wireless device, use the Cisco IOS CLI tool and perform these tasks:

- Configuring the Radio, page 8-5
- Configuring Wireless Security Settings, page 8-5
- Configuring Wireless Quality of Service, page 8-8 (Optional)

Configuring the Radio

Configure the radio parameters on the wireless device to transmit signals in autonomous or Cisco Unified mode. For specific configuration procedures, see Chapter 9, "Configuring Radio Settings".

Configuring Wireless Security Settings

- Configuring Authentication, page 8-5
- Configuring WEP and Cipher Suites, page 8-6
- Configuring Wireless VLANs, page 8-6

Configuring Authentication

Authentication types are tied to the Service Set Identifiers (SSIDs) that are configured for the access point. 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, the client device 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 authentication types rely on an authentication server on your network.

To select an authentication type, see *Authentication Types for Wireless Devices* at:

http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityAuthenticationTypes.html.

To set up a maximum security environment, see *RADIUS and TACACS+ Servers in a Wireless Environment* at:

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 a server failure, 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 Lightweight Extensible Authentication Protocol (LEAP), Extensible Authentication Protocol-Flexible Authentication via Secure Tunneling (EAP-FAST), or MAC-based authentication. The access point performs up to five authentications per second.

Configure the local authenticator access point manually with client usernames and passwords because it does not synchronize its database with RADIUS servers. You can specify a VLAN and a list of SSIDs that a client is allowed to use.

For details about setting up the wireless device in this role, see *Using the Access Point as a Local Authenticator* at:

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 Temporal Key Integrity Protocol (TKIP) provide the greatest security for your wireless LAN. Cipher suites that contain only WEP are the least secure.

For encryption procedures, see *Configuring WEP and Cipher Suites* at:

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 8-7. 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), that are 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.

For more information about wireless VLAN architecture, see *Configuring Wireless VLANs* at:

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 you can configure a unique set of parameters for each SSID. For example, you might use one SSID to allow guests limited access to the network and another SSID to allow authorized users access to secure data.

For more about creating multiple SSIDs, see *Service Set Identifiers* at:

http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/ServiceSetID.html.

Read 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 WPA authentication because the SSIDs use different encryption settings. If the security setting for an SSID conflicts with the settings for another SSID, delete one or more SSIDs to eliminate the conflict.

Security Types

Table 8-1 describes the four security types that you can assign to an SSID.

Table 8-1 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 in a public space, and you should 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: 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* 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 8-1 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 plus EAP, network EAP authentication, no key management, and 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 who are authenticated against a database. Access is through the services of an authentication server. User IP traffic is then encrypted with stronger algorithms than those used in WEP. This setting uses encryption ciphers, TKIP[10], open authentication plus 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 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.`

[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] WPA = 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 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. For more information, see *Hot Standby Access Points* at:

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 performing the following procedures:

- Preparing for the Upgrade, page 8-9
- Performing the Upgrade, page 8-10
- Downgrading the Software on the Access Point, page 8-11
- Recovering Software on the Access Point, page 8-12

Software Prerequisites

- Cisco 890 Series ISRs with embedded access points can be upgraded from autonomous software to Cisco Unified software, if the router is running the IP Base feature set and Cisco IOS 12.4(22)YB software.
- Cisco 880 Series ISRs with embedded access points can be upgraded from autonomous software to Cisco Unified software, if the router is running the advipservices feature set and Cisco IOS 12.4(20)T software.
- To use the embedded access point in a Cisco Unified Architecture, the Cisco Wireless LAN Configuration (WLC) must be running version 5.1 or later.

Preparing for the Upgrade

Perform the tasks in the following sections to prepare for the upgrade:

- Secure an IP Address on the Access Point, page 8-10
- Confirm that the Mode Setting is Enabled, page 8-10

Secure an IP Address on the Access Point

Secure an IP address on the access point so it that 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. The access point then communicates with the WLC and setup option 43 for the controller IP address in the DHCP pool configuration. The following example shows 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: http://www.cisco.com/en/US/docs/wireless/controller/4.0/configuration/guide/ccfig40.html

Confirm that the Mode Setting is Enabled

To confirm that the mode setting is enabled, perform the following steps.

Step 1 Ping the WLC from the router to confirm IP connectivity.

Step 2 Enter the **service-module wlan-ap 0 session** command to establish a session into the access point.

Step 3 Confirm that the access point is running an autonomous boot image.

Step 4 Enter the **show boot** command on the access point to confirm that 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 the autonomous software to Cisco Unified software, follow these steps:

Step 1 To change the access point boot image to a Cisco Unified upgrade image (also known as a *recovery image*), use the **service-module wlan-ap 0 bootimage unified** command, in global configuration mode.

```
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 whether the software license is still eligible.

To identify the access point's boot image path, use the **show boot** command in privileged EXEC mode on the access point console:

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

Step 2 To perform a graceful shutdown and reboot of the access point to complete the upgrade process, use the **service-module wlan-ap 0 reload** command in global configuration mode. Establish a session into the access point, and monitor the upgrade process.

See the "Cisco Express Setup" section on page 8-4 for details about using the GUI configuration page to set up 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 Cisco Unified software, and it seems to be stuck in the recovery mode. What is my next step?

A. If the access point fails to upgrade from autonomous to Unified software, perform the following actions:

- Check to ensure the autonomous access point does not have the static IP address configured on the BVI interface before you boot the recovery image.
- Ping between the router/access point and the WLC to confirm communication.
- Check that the access point and WLC clock (time and date) are set correctly.

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 may attempt to boot and fail or may become stuck in the recovery mode and fail to upgrade to the Unified software. If either occurs, use the **service-module wlan-ap0 reset bootloader** command to return the access point to the bootloader for manual image recovery.

Downgrading the Software on the Access Point

To reset the access point boot to the last autonomous image, use the **service-module wlan-ap0 bootimage autonomous** command in global configuration mode. To reload the access point with the autonomous software image, use the **service-module wlan-ap 0 reload** command.

Recovering Software on the Access Point

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

Caution Use this command with caution. It does not provide an orderly shutdown and consequently may impact file operations that are in progress. Use this command only to recover from a shutdown or a failed state.

Related Documentation

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

- Autonomous Cisco Documentation—Table 8-2
- Cisco Unified Documentation—Table 8-3

Table 8-2 Autonomous Cisco Documentation

Network Design	**Links**
Wireless Overview	Chapter 2, "Wireless Device Overview"
Configuration	**Links**
Configuring the Radio	Chapter 9, "Configuring Radio Settings"
Security	**Links**
Authentication Types for Wireless Devices	This document describes the authentication types that are configured on the access point. http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityAuthenticationTypes.html
RADIUS and TACACS+ Servers in a Wireless Environment	This document describes how to enable and configure the RADIUS and TACACS+ and provides detailed accounting information and flexible administrative control over authentication and authorization processes. RADIUS and TACACS+ are facilitated through AAA[1] and can be enabled only through AAA commands. http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityRadiusTacacs_1.html
Using the Access Point as a Local Authenticator	This document 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. http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityLocalAuthent.html

Table 8-2 Autonomous Cisco Documentation (continued)

Network Design	**Links**
Cipher Suites and WEP	This document describes how to configure the cipher suites required for using WPA and CCKM[2]; WEP; and WEP features including AES[3], MIC[4], TKIP, and broadcast key rotation. http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SecurityCipherSuitesWEP.html
Hot Standby Access Points	This document describes how to configure your wireless device as a hot standby unit. http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/RolesHotStandby.html
Configuring Wireless VLANs	This document describes how to configure an access point to operate with the VLANs set up on a wired LAN. http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/wireless_vlans.html
Service Set Identifiers	In the role of an access point, a wireless device can support up to 16 SSIDs. This document describes how to configure and manage SSIDs on the wireless device. http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/ServiceSetID.html
Administering	**Links**
Administering the Access Point	Chapter 10, “Administering the Wireless Device”
Quality of Service	This document describes how to configure QoS 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. http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/QualityOfService.html
Regulatory Domains and Channels	This document lists the radio channels supported by Cisco access products in the regulatory domains of the world. http://www.cisco.com/en/US/customer/docs/routers/access/wireless/software/guide/RadioChannelFrequencies.html
System Message Logging	This document describes how to configure system message logging on your wireless device. http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/SysMsgLogging.html

[1] AAA = Authentication, Authorization, and Accounting.

[2] CCKM = Cisco Centralized Key Management.

[3] AES = Advanced Encryption Standard.

[4] MIC = Message Integrity Check.

Table 8-3 Cisco Unified Documentation

Network Design	Links
Why Migrate to the Cisco Unified Wireless Network?	http://www.cisco.com/en/US/prod/collateral/wireless/ps5679/ps6548/prod_white_paper0900aecd804f19e3_ps6305_Products_White_Paper.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