CHAPTER 4

Basic Wireless Device Configuration

This chapter describes how to configure the autonomous wireless device on the Cisco 880 Series Integrated Services Router (ISR).

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 4-9 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 4-2
- Closing the Session, page 4-3
- Configuring Wireless Settings, page 4-4
- Configuring the Access Point in Hot Standby Mode, page 4-9 (Optional)
- Upgrading to Cisco Unified Software, page 4-9
- Images Supported, page 4-13
- Related Documentation, page 4-13

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 CLI.

SUMMARY STEPS

1. **interface wlan-ap0**
2. **ip address** *subnet mask*
3. **no shutdown**
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. The interface 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`
	
	`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 shutdown** **Example:** `router(config-if)# no shutdown`	Specifies that the internal interface connection remains open.

	Command	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 880 Series ISR.
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 interface 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.

Closing the Session

To close the session between the wireless device and the router's console, follow these steps:

Wireless Device

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

Router

1. Type the **disconnect** command.
2. Press **Enter.**

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 4-2.

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

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

Note If you are running the wireless device in autonomous mode and would like to upgrade to Unified mode, see the "Upgrading to Cisco Unified Software" section on page 4-9 for upgrade instructions.

After upgrading to Cisco Unified Wireless software, use the web-browser interface to configure the device at the following URL: 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 autonomous 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 username.

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://www.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 to perform the following tasks:

- Configuring the Radio, page 4-5
- Configuring Wireless Security Settings, page 4-5
- Configuring Wireless Quality of Service, page 4-8 (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 the "Configuring Radio Settings" section on page 5-1.

Configuring Wireless Security Settings

- Configuring Authentication, page 4-5
- Configuring Access Point as Local Authenticator, page 4-6
- Configuring WEP and Cipher Suites, page 4-6
- Configuring Wireless VLANs, page 4-6
- Assigning SSIDs, page 4-7

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.

You 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 4-7. 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.

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 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 4-1 describes the four security types that you can assign to an SSID.

Table 4-1 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.	—
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 the MAC address. For more information, see C*ipher 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. For instructions, see *Using the Access Point as a Local Authenticator* at 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 4-1 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 key 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. Users' 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 key 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 offline 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 4-9
- Performing the Upgrade, page 4-11
- Upgrading AP bootloader, page 4-12
- Downgrading the Software on the Access Point, page 4-12
- Recovering Software on the Access Point, page 4-13

Software Prerequisites

- Cisco 880 Series ISRs with embedded access points are eligible to upgrade from autonomous software to Cisco Unified software if the router is running the advipservices feature set and Cisco IOS Release15.2(4)M1 or later versions.
- To use the embedded access point in a Cisco Unified Architecture, the Cisco Wireless LAN Configuration (WLC) must be running the minimum versions for single radio (Cisco IOS Release 7.0.116.0 or later versions) and dual radio (Cisco IOS Release 7.2.110.0 or later versions).

Preparing for the Upgrade

To prepare for the upgrade, peform the following tasks:

- Secure an IP Address on the Access Point, page 4-10
- Confirm that the Mode Setting is Enabled, page 4-10

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 bootup. The host router provides the access point DHCP server functionality through the DHCP pool. 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 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, follow these 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 a sample output for the command:

```
# show boot
BOOT path-list:      flash:ap802-k9w7-mx.124/ap802-k9w7-mx.124
Config file:         flash:/config.txt
Private Config file: flash:/private-config
Enable Break:          no
Manual Boot:         yes
HELPER path-list:    no
NVRAM/Config file
buffer size:   32768
Mode Button:    on
Radio Core TFTP:
ap#
```

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*), issue the **service-module wlan-ap 0 bootimage unified** command in global configuration mode.

```
Router# configure 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, check whether the advipservices or advipsevices_npe software license is enabled or not.

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:/ap802-rcvk9w8-mx/ap802-rcvk9w8-mx
```

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

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 appears 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.
- Issue a 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 does 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.

Upgrading AP bootloader

For AP802, the bootloader is available as part of the host router image. To upgrade the bootloader, perform the following steps:

Step 1 Verify the WLAN AP bootloader bundled with the host router image running on the first core using the **show platform version** command.

```
Router# show platform version
Platform Revisions/Versions :
.
WLAN AP Boot loader (bundled):
AP802 Boot Loader (AP802-BOOT-M) Version 12.4(25e)JA1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Compiled Wed 30-May-12 03:46 by prod_rel_team
```

Step 2 Open a session between the router and the WLAN AP.

For information on how to open a session between a router and an access point, see the "Starting a Wireless Configuration Session" section on page 4-2.

Step 3 Verify the version of the WLAN AP bootloader.

At the WLAN AP bootloader, use the **version** command.

```
ap: version
AP802 Boot Loader (AP802-BOOT-M) Version 12.4(25e)JA1, RELEASE SOFTWARE (fc1)
Technical Support: http://www.cisco.com/techsupport
Compiled Wed 30-May-12 03:46 by prod_rel_team
```

At the WLAN AP IOS, use the show version command.

```
ap# show version
.
BOOTLDR: AP802 Boot Loader (AP802-BOOT-M) Version 12.4(25e)JA1, RELEASE SOFTWARE (fc1)
<snip>
Configuration register is 0xF
```

Step 4 Upgrade the bootloader using the following commands:

```
Router# service-module wlan-ap 0 upgrade bootloader
Router# service-module wlan-ap 0 reset
```

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 privileged EXEC mode on the host router running on the first core. To reload the access point with the autonomous software image, use the **service-module wlan-ap 0 reload** command.

```
Router# configure terminal
Router(config)# service-module wlan-ap 0 bootimage autonomous
Router(config)# end
Router# write
Router# service-module wlan-ap 0 reload
```

Recovering Software on the Access Point

To recover the image on the access point, use the **service-module wlan-ap0 reset bootloader** command in privileged EXEC 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.

Images Supported

For information on images supported on the Cisco 880 Series ISRs, see the "Images Supported" section on page 1-11.

Related Documentation

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

- Autonomous Mode Documentation—Table 4-2
- Unified Mode Documentation—Table 4-3

Table 4-2 Autonomous Mode Documentation

Autonomous Mode	Links	Description
Network Design		
Wireless Overview	Wireless Device Overview	Describes the roles of the wireless device on the network.
Cisco IOS Command Reference for Cisco Aironet Access Points and Bridges Versions 12.4(25d)JA and 12.3(8)JEE	http://www.cisco.com/en/US/docs/wireless/access_point/12.4.25d.JA/Command/reference/cr12425d-preface.html	Describes the Cisco IOS Release 12.4(25d)JA and Cisco IOS Release 12.3(8)JEE commands for configuring Cisco Aironet access points and bridges.
Configuration		
Configuring the Radio	Configuring Radio Settings	Describes how to configure the wireless radio.
Security		
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.

Table 4-2 Autonomous Mode Documentation (continued)

Autonomous Mode	Links	Description
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[3] 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 when using WPA[4] and CCKM[5]; WEP[6]; and WEP features including AES[7], MIC[8], TKIP[9], 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[10]. This document describes how to configure and manage SSIDs on the wireless device.
Administering		
Quality of Service	http://www.cisco.com/en/US/docs/routers/access/wireless/software/guide/QualityOfService.html	Describes how to configure QoS[11] 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. AAA = Authentication, Authorization, and Accounting.
4. WPA = Wireless Protected Access.
5. CCKM = Cisco Centralized Key Management.
6. WEP = Wired Equivalent Privacy.
7. AES = Advanced Encryption Standard.
8. MIC = Message Integrity Check.
9. TKIP = Temporal Key Integrity Protocol.
10. SSID = service set identifiers.
11. QoS = quality of service.

Table 4-3 Unified Mode 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
Single-Radio AP802	
Cisco Wireles LAN Controller Configuration Guide, Release 7.0.116.0	http://www.cisco.com/en/US/docs/wireless/controller/7.0MR1/configuration/guide/cg_controller_setting.html
Dual-Radio AP802	
Cisco Unified Wireless Network Software Release 7.2.110.0 (7.2 Maintenance Release 1)	http://www.cisco.com/en/US/prod/collateral/wireless/ps6302/ps8322/ps10315/product_bulletin_c25-707629.html