Cisco 500 Series Wireless Express Mobility Controller Configuration Guide

Software Release 1.5
February 2008

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Customer Order Number:
Text Part Number: OL-15283-01

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses used in this document are not intended to be actual addresses. Any examples, command display output, and figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Cisco 500 Series Wireless Express Mobility Controller Configuration Guide

CONTENTS

CHAPTER 3

CHAPTER 4

CHAPTER 5

CHAPTER 6

CHAPTER 7

Preface

This preface provides an overview of the *Cisco 500 Series Wireless Express Mobility Controller Configuration Guide*, *Software Release 1.5*, references related publications, and explains how to obtain other documentation and technical assistance, if necessary.

Audience

This guide is for the networking professional who installs and manages these devices. To use this guide, you should be familiar with the concepts and terminology of wireless LANs.

Purpose

This guide describes how to configure the Cisco 526 Wireless Express Mobility Controller (hereafter referred to as the *WLC526* or the *controller*) and Cisco 521 Wireless Express Access Points using the Cisco Configuration Assistant (hereafter referred to as the *CCA*).

Note This version of the *Cisco 500 Series Wireless Express Mobility Controller Configuration Guide* pertains specifically to CCA software release1.5. If you are using an earlier version of CCA software, you might notice differences in features, functionality, and GUI windows (for instructions on obtaining the latest CCA software, refer to the "Obtaining and Installing CCA" section on page 1.

Conventions

This publication uses these conventions to convey instructions and information:

Command descriptions use these conventions:

- Commands and keywords are in boldface text.
- Arguments for which you supply values are in italic.
- Square brackets ([ ]) mean optional elements.
- Braces ({ }) group required choices, and vertical bars (|) separate the alternative elements.
- Braces and vertical bars within square brackets ([{ | }]) mean a required choice within an optional element.

Interactive examples use these conventions:

- Terminal sessions and system displays are in screen font.
- Information you enter is in **boldface**.
- Nonprinting characters, such as passwords or tabs, are in angle brackets (< >).

Notes and cautions use these conventions and symbols:

Note Means reader take note. Notes contain helpful suggestions or references to materials not contained in this manual.

Caution Means reader be careful. In this situation, you might do something that could result in equipment damage or loss of data.

Abbreviations and Acronyms

Table 1 lists the abbreviations and acronyms for Cisco products and services included in this guide.

Table 1 Abbreviations and Acronyms Used in This Guide

Abbreviation or Acronym Used	Additional References (generic or collective)	Cisco Product or Service Name
AP521	autonomous access point Cisco 500 series access point	Cisco 521 Wireless Express Access Point
Cat3750	DHCP server	Cisco Catalyst 3750 Series Switch
CCA		Cisco Configuration Assistant
CE520	switch Catalyst Express 500 Series Switches	Cisco Catalyst Express 520 Series Switch
CLI		Command Line Interface
CUWN		Cisco Unified Wireless Network
GUI	controller GUI	controller web-browser interface
LAP521	lightweight access point controller-based access point	Cisco 521 Wireless Express Lightweight Access Point
RRM		radio resource management (feature)
SBCS		Cisco Smart Business Communications System
UC500	UC500 devices	Cisco UC500 series appliances
WCS		Cisco Wireless LAN Control System
WLC526	controller Wireless Express 500 series controllers	Cisco 526 Wireless Express Mobility Controller

Related Documentation

This guide assumes that you are installing your WLC526 within the Cisco Smart Business Communications System. The following documents provide information about system components and include configuration procedures:

- *Quick Start Guide: Cisco 526 Wireless Express Mobility Controller*—Contains basic installation and configuration instructions for the WLC526.
- *Cisco Smart Business Communications System Setup Guide*—Contains instructions for installing, configuring, and monitoring the SBCS. You should use this document to configure all the components of the smart business system (referred to as the "Smart Doc" in some documents).
- *Cisco Unified Communications 500 Series for Small Business Getting Started Guide*—Provides basic installation and setup instructions for the UC500 appliance.
- *Getting Started Guide for the Catalyst Express 520 Switches*—Provides basic installation and setup instructions for the CE520 switch.
- *User Guide for the Catalyst Express 520 Switches*—Provides advanced configuration information for the CE520 switch.
- *Cisco Configuration Assistant Quick Start Guide*—Contains basic installation and configuration instructions for the CCA.
- *Quick Start Guide: Cisco 521 Wireless Express Access Point*—Contains mounting instructions for the AP521.

Follow these steps to obtain these documents on Cisco.com:

Step 1 Browse to http://www.cisco.com/en/US/products/hw/wireless/.

Step 2 Scroll down to the **Cisco Mobility Express** section.

Step 3 Select the link for the wireless express component you need. The Introduction window for that component appears.

Step 4 The product documentation is available in the **Support box**. Download the appropriate document.

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.

Translated Warning

Statement 1071—Warning Definition

Warning

IMPORTANT SAFETY INSTRUCTIONS

This warning symbol means danger. You are in a situation that could cause bodily injury. Before you work on any equipment, be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. Use the statement number provided at the end of each warning to locate its translation in the translated safety warnings that accompanied this device. Statement 1071

SAVE THESE INSTRUCTIONS

Waarschuwing

BELANGRIJKE VEILIGHEIDSINSTRUCTIES

Dit waarschuwingssymbool betekent gevaar. U verkeert in een situatie die lichamelijk letsel kan veroorzaken. Voordat u aan enige apparatuur gaat werken, dient u zich bewust te zijn van de bij elektrische schakelingen betrokken risico's en dient u op de hoogte te zijn van de standaard praktijken om ongelukken te voorkomen. Gebruik het nummer van de verklaring onderaan de waarschuwing als u een vertaling van de waarschuwing die bij het apparaat wordt geleverd, wilt raadplegen.

BEWAAR DEZE INSTRUCTIES

Varoitus

TÄRKEITÄ TURVALLISUUSOHJEITA

Tämä varoitusmerkki merkitsee vaaraa. Tilanne voi aiheuttaa ruumiillisia vammoja. Ennen kuin käsittelet laitteistoa, huomioi sähköpiirien käsittelemiseen liittyvät riskit ja tutustu onnettomuuksien yleisiin ehkäisytapoihin. Turvallisuusvaroitusten käännökset löytyvät laitteen mukana toimitettujen käännettyjen turvallisuusvaroitusten joukosta varoitusten lopussa näkyvien lausuntonumeroiden avulla.

SÄILYTÄ NÄMÄ OHJEET

Attention

IMPORTANTES INFORMATIONS DE SÉCURITÉ

Ce symbole d'avertissement indique un danger. Vous vous trouvez dans une situation pouvant entraîner des blessures ou des dommages corporels. Avant de travailler sur un équipement, soyez conscient des dangers liés aux circuits électriques et familiarisez-vous avec les procédures couramment utilisées pour éviter les accidents. Pour prendre connaissance des traductions des avertissements figurant dans les consignes de sécurité traduites qui accompagnent cet appareil, référez-vous au numéro de l'instruction situé à la fin de chaque avertissement.

CONSERVEZ CES INFORMATIONS

Warnung **WICHTIGE SICHERHEITSHINWEISE**

Dieses Warnsymbol bedeutet Gefahr. Sie befinden sich in einer Situation, die zu Verletzungen führen kann. Machen Sie sich vor der Arbeit mit Geräten mit den Gefahren elektrischer Schaltungen und den üblichen Verfahren zur Vorbeugung vor Unfällen vertraut. Suchen Sie mit der am Ende jeder Warnung angegebenen Anweisungsnummer nach der jeweiligen Übersetzung in den übersetzten Sicherheitshinweisen, die zusammen mit diesem Gerät ausgeliefert wurden.

BEWAHREN SIE DIESE HINWEISE GUT AUF.

Avvertenza **IMPORTANTI ISTRUZIONI SULLA SICUREZZA**

Questo simbolo di avvertenza indica un pericolo. La situazione potrebbe causare infortuni alle persone. Prima di intervenire su qualsiasi apparecchiatura, occorre essere al corrente dei pericoli relativi ai circuiti elettrici e conoscere le procedure standard per la prevenzione di incidenti. Utilizzare il numero di istruzione presente alla fine di ciascuna avvertenza per individuare le traduzioni delle avvertenze riportate in questo documento.

CONSERVARE QUESTE ISTRUZIONI

Advarsel **VIKTIGE SIKKERHETSINSTRUKSJONER**

Dette advarselssymbolet betyr fare. Du er i en situasjon som kan føre til skade på person. Før du begynner å arbeide med noe av utstyret, må du være oppmerksom på farene forbundet med elektriske kretser, og kjenne til standardprosedyrer for å forhindre ulykker. Bruk nummeret i slutten av hver advarsel for å finne oversettelsen i de oversatte sikkerhetsadvarslene som fulgte med denne enheten.

TA VARE PÅ DISSE INSTRUKSJONENE

Aviso **INSTRUÇÕES IMPORTANTES DE SEGURANÇA**

Este símbolo de aviso significa perigo. Você está em uma situação que poderá ser causadora de lesões corporais. Antes de iniciar a utilização de qualquer equipamento, tenha conhecimento dos perigos envolvidos no manuseio de circuitos elétricos e familiarize-se com as práticas habituais de prevenção de acidentes. Utilize o número da instrução fornecido ao final de cada aviso para localizar sua tradução nos avisos de segurança traduzidos que acompanham este dispositivo.

GUARDE ESTAS INSTRUÇÕES

¡Advertencia! **INSTRUCCIONES IMPORTANTES DE SEGURIDAD**

Este símbolo de aviso indica peligro. Existe riesgo para su integridad física. Antes de manipular cualquier equipo, considere los riesgos de la corriente eléctrica y familiarícese con los procedimientos estándar de prevención de accidentes. Al final de cada advertencia encontrará el número que le ayudará a encontrar el texto traducido en el apartado de traducciones que acompaña a este dispositivo.

GUARDE ESTAS INSTRUCCIONES

Varning! **VIKTIGA SÄKERHETSANVISNINGAR**

Denna varningssignal signalerar fara. Du befinner dig i en situation som kan leda till personskada. Innan du utför arbete på någon utrustning måste du vara medveten om farorna med elkretsar och känna till vanliga förfaranden för att förebygga olyckor. Använd det nummer som finns i slutet av varje varning för att hitta dess översättning i de översatta säkerhetsvarningar som medföljer denna anordning.

SPARA DESSA ANVISNINGAR

Figyelem **FONTOS BIZTONSÁGI ELOÍRÁSOK**

Ez a figyelmezeto jel veszélyre utal. Sérülésveszélyt rejto helyzetben van. Mielott bármely berendezésen munkát végezte, legyen figyelemmel az elektromos áramkörök okozta kockázatokra, és ismerkedjen meg a szokásos balesetvédelmi eljárásokkal. A kiadványban szereplo figyelmeztetések fordítása a készülékhez mellékelt biztonsági figyelmeztetések között található; a fordítás az egyes figyelmeztetések végén látható szám alapján keresheto meg.

ORIZZE MEG EZEKET AZ UTASÍTÁSOKAT!

Предупреждение **ВАЖНЫЕ ИНСТРУКЦИИ ПО СОБЛЮДЕНИЮ ТЕХНИКИ БЕЗОПАСНОСТИ**

Этот символ предупреждения обозначает опасность. То есть имеет место ситуация, в которой следует опасаться телесных повреждений. Перед эксплуатацией оборудования выясните, каким опасностям может подвергаться пользователь при использовании электрических цепей, и ознакомьтесь с правилами техники безопасности для предотвращения возможных несчастных случаев. Воспользуйтесь номером заявления, приведенным в конце каждого предупреждения, чтобы найти его переведенный вариант в переводе предупреждений по безопасности, прилагаемом к данному устройству.

СОХРАНИТЕ ЭТИ ИНСТРУКЦИИ

警告 重要的安全性说明

此警告符号代表危险。您正处于可能受到严重伤害的工作环境中。在您使用设备开始工作之前，必须充分意识到触电的危险，并熟练掌握防止事故发生的标准工作程序。请根据每项警告结尾提供的声明号码来找到此设备的安全性警告说明的翻译文本。

请保存这些安全性说明

警告 安全上の重要な注意事項

「危険」の意味です。人身事故を予防するための注意事項が記述されています。装置の取り扱い作業を行うときは、電気回路の危険性に注意し、一般的な事故防止策に留意してください。警告の各国語版は、各注意事項の番号を基に、装置に付属の「Translated Safety Warnings」を参照してください。

これらの注意事項を保管しておいてください。

주의 중요 안전 지침

이 경고 기호는 위험을 나타냅니다. 작업자가 신체 부상을 일으킬 수 있는 위험한 환경에 있습니다. 장비에 작업을 수행하기 전에 전기 회로와 관련된 위험을 숙지하고 표준 작업 관례를 숙지하여 사고를 방지하십시오. 각 경고의 마지막 부분에 있는 경고문 번호를 참조하여 이 장치와 함께 제공되는 번역된 안전 경고문에서 해당 번역문을 찾으십시오.

이 지시 사항을 보관하십시오.

تحذير إرشادات الأمان الهامة

يوضح رمز التحذير هذا وجود خطر. وهذا يعني أنك متواجد في مكان قد ينتج عنه التعرض لإصابات. قبل بدء العمل، احذر مخاطر التعرض للصدمات الكهربائية وكن على علم بالإجراءات القياسية للحيلولة دون وقوع أي حوادث. استخدم رقم البيان الموجود في أخر كل تحذير لتحديد مكان ترجمته داخل تحذيرات الأمان المترجمة التي تأتي مع الجهاز. قم بحفظ هذه الإرشادات

Upozorenje **VAŽNE SIGURNOSNE NAPOMENE**

Ovaj simbol upozorenja predstavlja opasnost. Nalazite se u situaciji koja može prouzročiti tjelesne ozljede. Prije rada s bilo kojim uređajem, morate razumjeti opasnosti vezane uz električne sklopove, te biti upoznati sa standardnim načinima izbjegavanja nesreća. U prevedenim sigurnosnim upozorenjima, priloženima uz uređaj, možete prema broju koji se nalazi uz pojedino upozorenje pronaći i njegov prijevod.

SAČUVAJTE OVE UPUTE

Upozornění

DŮLEŽITÉ BEZPEČNOSTNÍ POKYNY

Tento upozorňující symbol označuje nebezpečí. Jste v situaci, která by mohla způsobit nebezpečí úrazu. Před prací na jakémkoliv vybavení si uvědomte nebezpečí související s elektrickými obvody a seznamte se se standardními opatřeními pro předcházení úrazům. Podle čísla na konci každého upozornění vyhledejte jeho překlad v přeložených bezpečnostních upozorněních, která jsou přiložena k zařízení.

USCHOVEJTE TYTO POKYNY

Προειδοποίηση

ΣΗΜΑΝΤΙΚΕΣ ΟΔΗΓΙΕΣ ΑΣΦΑΛΕΙΑΣ

Αυτό το προειδοποιητικό σύμβολο σημαίνει κίνδυνο. Βρίσκεστε σε κατάσταση που μπορεί να προκαλέσει τραυματισμό. Πριν εργαστείτε σε οποιοδήποτε εξοπλισμό, να έχετε υπόψη σας τους κινδύνους που σχετίζονται με τα ηλεκτρικά κυκλώματα και να έχετε εξοικειωθεί με τις συνήθεις πρακτικές για την αποφυγή ατυχημάτων. Χρησιμοποιήστε τον αριθμό δήλωσης που παρέχεται στο τέλος κάθε προειδοποίησης, για να εντοπίσετε τη μετάφρασή της στις μεταφρασμένες προειδοποιήσεις ασφαλείας που συνοδεύουν τη συσκευή.

ΦΥΛΑΞΤΕ ΑΥΤΕΣ ΤΙΣ ΟΔΗΓΙΕΣ

אזהרה

הוראות בטיחות חשובות

סימן אזהרה זה מסמל סכנה. אתה נמצא במצב העלול לגרום לפציעה. לפני שתעבוד עם ציוד כלשהו, עליך להיות מודע לסכנות הכרוכות במעגלים חשמליים ולהכיר את הנהלים המקובלים למניעת תאונות. השתמש במספר ההוראה המסופק בסופה של כל אזהרה כד לאתר את התרגום באזהרות הבטיחות המתורגמות שמצורפות להתקן.

שמור הוראות אלה

Opomena

ВАЖНИ БЕЗБЕДНОСНИ НАПАТСТВИЈА

Симболот за предупредување значи опасност. Се наоѓате во ситуација што може да предизвика телесни повреди. Пред да работите со опремата, бидете свесни за ризикот што постои кај електричните кола и треба да ги познавате стандардните постапки за спречување на несреќни случаи. Искористете го бројот на изјавата што се наоѓа на крајот на секое предупредување за да го најдете неговиот период во преведените безбедносни предупредувања што се испорачани со уредот.

ЧУВАЈТЕ ГИ ОВИЕ НАПАТСТВИЈА

Ostrzeżenie **WAŻNE INSTRUKCJE DOTYCZĄCE BEZPIECZEŃSTWA**

Ten symbol ostrzeżenia oznacza niebezpieczeństwo. Zachodzi sytuacja, która może powodować obrażenia ciała. Przed przystąpieniem do prac przy urządzeniach należy zapoznać się z zagrożeniami związanymi z układami elektrycznymi oraz ze standardowymi środkami zapobiegania wypadkom. Na końcu każdego ostrzeżenia podano numer, na podstawie którego można odszukać tłumaczenie tego ostrzeżenia w dołączonym do urządzenia dokumencie z tłumaczeniami ostrzeżeń.

NINIEJSZE INSTRUKCJE NALEŻY ZACHOWAĆ

Upozornenie **DÔLEŽITÉ BEZPEČNOSTNÉ POKYNY**

Tento varovný symbol označuje nebezpečenstvo. Nachádzate sa v situácii s nebezpečenstvom úrazu. Pred prácou na akomkoľvek vybavení si uvedomte nebezpečenstvo súvisiace s elektrickými obvodmi a oboznámte sa so štandardnými opatreniami na predchádzanie úrazom. Podľa čísla na konci každého upozornenia vyhľadajte jeho preklad v preložených bezpečnostných upozorneniach, ktoré sú priložené k zariadeniu.

USCHOVAJTE SI TENTO NÁVOD

Opozorilo **POMEMBNI VARNOSTNI NAPOTKI**

Ta opozorilni simbol pomeni nevarnost. Nahajate se v situaciji, kjer lahko pride do telesnih poškodb. Preden pričnete z delom na napravi, se morate zavedati nevarnosti udara električnega toka, ter tudi poznati preventivne ukrepe za preprečevanje takšnih nevarnosti. Uporabite obrazložitveno številko na koncu posameznega opozorila, da najdete opis nevarnosti v priloženem varnostnem priročniku.

SHRANITE TE NAPOTKE!

警告 重要安全性指示

此警告符號代表危險，表示可能造成人身傷害。使用任何設備前，請留心電路相關危險，並熟悉避免意外的標準作法。您可以使用每項警告後的聲明編號，查詢本裝置隨附之安全性警告譯文中的翻譯。

請妥善保留此指示

CHAPTER 1

Overview

This chapter provides an overview of the Cisco 526 Wireless Express Mobility Controller components and features. It contains these sections:

System Overview

The Cisco 526 Wireless Express Mobility Controller (also referred to as the *WLC526* or just the *controller*) is a network appliance that is optimized for secure transmission of data, voice, and video as part of the Cisco Mobility Express solution of the Cisco Smart Business Communications System (SBCS).

Some of the features available in the controller-based architecture of the Cisco Mobility Express Solution include:

- Centralized management—Cisco Configuration Assistant (also referred to as *CCA*) enables users to quickly and easily set-up and manage clients, access points, and network policies through a single wizard interface and predefined configuration templates.
- Radio resource management—Features such as quality of service (QoS) and load balancing optimize traffic of voice, video, and data, thus optimizing bandwidth.
- Up to eight virtual networks—This allows one physical infrastructure to be segmented for multiple uses—such as by organization, security level, voice or data requirement, and so on. One network can also be configured as a secure guest network.
- Mobility management—Allows movement from one access point to another without losing a connection.
- Mobility services—Supports advanced mobility services traditionally reserved for enterprise businesses, including:
  - Standards-based security
  - Secure guest access
  - Optimized voice over Wi-Fi

The Cisco Mobility Express Solution

The Cisco Mobility Express solution comprises access points, mobility controllers, and a configuration assistant that is tailored to the needs of businesses with fewer than 250 employees.

Figure 1-1 shows the Cisco Mobility Express Solution elements.

Figure 1-1 Cisco Mobility Express Solution Elements

The Cisco 521 Wireless Express Access Point

The Cisco 521 Wireless Express Access Point is a single-band 802.11g access point that features business-class management, security, and scalability. It supports high-performance wireless connectivity in carpeted offices and similar environments. They can be deployed in two modes—standalone or controller-based:

- Standalone (referred to as an *AP521* access point)—Up to three AP521 access points can be deployed to provide wireless connectivity between the devices and the rest of the network. In this configuration, the access points are managed individually through the CCA.
- Controller-based (referred to as a *lightweight* or *LAP521* access point)—Up to 12 LAP521 access points (six per wireless LAN controller) can be deployed and become multifunctional. In addition to offering connectivity, the access points allow the controller to monitor all wireless activities through them. In this configuration, they are managed by the controller through the CCA.

Note Cisco 500 series access points can associate only with Cisco 500 series controllers. Because the needs of Cisco Mobility Express customers are different than those of enterprise customers, these access points do not operate with other controllers.

For more information about Cisco 521 Wireless Express Access Points, refer to the *Quick Start Guide: Cisco 521 Wireless Express Access Point.*

The Cisco 526 Wireless Express Mobility Controller

The WLC526 controller is easy to deploy, use, and maintain. The CCA interface and the automated Radio Resources Management (RRM) tool configure the access points automatically to avoid interference or coverage gaps while maximizing the bandwidth available. If the controller detects an access point failure or a point of interference, it immediately takes action tuning the radio power or frequency of surrounding access points to compensate and maintain business continuity without affecting the devices connected to the wireless network.

A single WLC526 controller supports up to six LAP521 access points. A second WLC526 controller can be added to the network to support redundancy or to increase capacity to 12 access points, or both.

Cisco Configuration Assistant

The CCA is a PC-based user interface created specifically for small-to-medium businesses with limited networking resources and IT expertise. CCA manages the entire Smart Business Communications System portfolio, including Cisco Mobility Express devices (see previous section) and these SBCS devices:

- Cisco UC500 series appliances (UC500)—The UC500 includes voice and messaging features, Public Switched Telephone Networks and Internet connectivity, integrated network security, and an optional integrated WLAN access point to provide basic WLAN coverage in a small office space.
- Catalyst Express 500 Series Switches (CE520)—These fixed-configuration, Layer 2-managed Ethernet switches include wire-speed Fast Ethernet and Gigabit Ethernet connectivity, integrated security, QoS, and Power-over-Ethernet (PoE) features.
- Cisco Unified IP Phones—The full Cisco Unified IP Phone portfolio is supported, including the Cisco Unified IP Communicator and wireless IP phones.

Remote Configuring and Monitoring Capability

Cisco Monitor Director and Cisco Monitor Director Agent provide monitoring and reporting tools that give network integrators real-time access to their supported customer networks. CCA supports remote configuration. For more information about Cisco Monitor Director and Agent, refer to the *Quick Start Guide for Cisco Monitor Director 1.1 (Cisco Smart Business Communications System Release*).

WLC526 Controller Overview

This section outlines the features and specifications of the WLC526 controller.

Features and Benefits

Table 1-1 lists the features and benefits of the WLC526 controller.

Table 1-1 Features and Benefits of the WLC526 controller

Features	Benefits
Secure network access for guest users	Secure guest access enables you to easily create and manage a virtual guest network with a Web login portal page for users such as customers, vendors, and contractors. Visitors can have Internet access while safely partitioned from the sensitive corporate LAN.
Support for Cisco voice-over-WLAN optimization	Voice-over-WLAN optimization is a package of features that deliver quality of service, call admission control, and fast, secure inter-access-point handoff to improve the quality of a wireless voice infrastructure.
Easy management tool	Within CCA are Smart Assist features that enable plug-and-play functionality and optimize network settings.
Support for Cisco Lightweight Access Point Protocol (LWAPP)	Uses Cisco LWAPP for communication between Cisco 500 series access points and WLC526 controllers to simplify deployment and management, and to automate functions required for seamless wireless coverage.
Support for up to 6 access points per controller and up to 2 controllers per network for a total of 12 access points	The wireless network easily expands as business requirements for additional wireless coverage and mobility services increase.
Multi-access-point Radio Resource Management (RRM)	RRM automatically optimizes radio coverage and capacity while working around potential points of interference. This real-time radio coordination simplifies deploying multiple access points.
Secure authentication mechanism support	Supports a wide range of authentication mechanisms to enable scalable security architectures and minimizes security interoperability problems (see the "Security/Authentication Standards" section on page 1-5)
Wired/wireless network virtualization	Supports the use of up to 8 SSID/VLANs so that one physical WLAN infrastructure can be safely shared by users, applications, or organizations with different network and security requirements.

WLC526 Controller Specifications

Table 1-2 lists product specifications for the WLC526 controller.

Table 1-2 WLC526 Controller Specifications

Item	Specification
Physical Interfaces	• Two 10/100 Ethernet ports for uplink and management • Two USB console ports (future expansion) • One RJ-45 serial port for direct console access
Wired/Switching/Routing protocols	• IEEE 802.3 10BASE-T • IEEE 802.3u 100BASE-TX • IEEE 802.1Q VLAN tagging
Management Options	• CCA software (recommended primary interface) • Controller web-browser interface • Limited command-line interface for troubleshooting using Telnet, SSH, or console port access
Security/Authentication Standards	• None/Open • MAC Filtering • WPA/Network EAP • WPA-PSK/Open with EAP • Protected EAP • EAP- TLS • EAP-SIM • WEP/Open • WPA/Open with EAP • WPA-PSK/Network EAP • WPA2/AES CCMP • Cisco LEAP • EAP Generic Token Card
RADIUS Authentication	• IEEE 802.1x RADIUS authentication (external RADIUS server required)
Multiple Service Set Identifiers (SSIDs)	• Eight SSIDs supported (each access point may support multiple SSIDs) • One SSID broadcast in SSID beacon
Support for Cisco Secure Guest Access through CCA	• Guest SSID/VLAN • Auto-expiring guest user accounts • Custom guest login page
Support for Voice-over-WLAN Optimization	• Quality of service • Call admission control • Fast inter-access point hand-off • Other optimization features designed to improve the quality of a wireless voice infrastructure

Configuration Options

Like many Cisco devices, the WLC526 controller can be configured and operated through more than one interface. They are:

- Cisco Configuration Assistant (CCA)
- Controller web-browser interface (GUI)
- Command-line interface (CLI)

This section explains use and limitations of each interface.

Using the Cisco Configuration Assistant

The CCA is your primary tool to install, set up, configure, and monitor all the Cisco Smart Business Communications System devices. Many common tasks are automated, simplified, or guided to help you to establish and administer a safe, optimized wireless network.

Note There is no charge to download or use this software. For information about downloading and installing CCA, refer to *Getting Started with Cisco Configuration Assistant 1.5*.

The following sections highlight some of the setup and configuration tools available in CCA.

Device Setup Wizard

The CCA Device Setup Wizard guides you through the steps for making devices ready to use and ready for CCA to manage. For more information about using the Device Setup Wizard, see Chapter 2, "Adding a WLC526 Controller and LAP521 Access Points."

Note The CCA Device Setup Wizard supports WLC526 controllers running software versions 4.2 and above. For controllers running earlier versions, see the "Using the Controller Web-Browser Interface (GUI)" section on page 1-8.

Cisco Smart Assist

CCA includes Cisco Smart Assist features with plug-and-play functionality. Smart Assist features reduce the time it takes to set up devices and applications and optimize your network settings. Cisco Smart Assist features include:

- Default configurations to allow auto discovery of supported devices
- Private branch exchange (PBX) configuration on the Cisco UC500 series appliance
- Firewall activation included in the default configuration
- Automatic assignment of phone extensions
- Password and VLAN synchronization for supported system devices
- Predefined configuration templates that automate SSID policy configuration, minimizing the number of parameters required to complete configuration

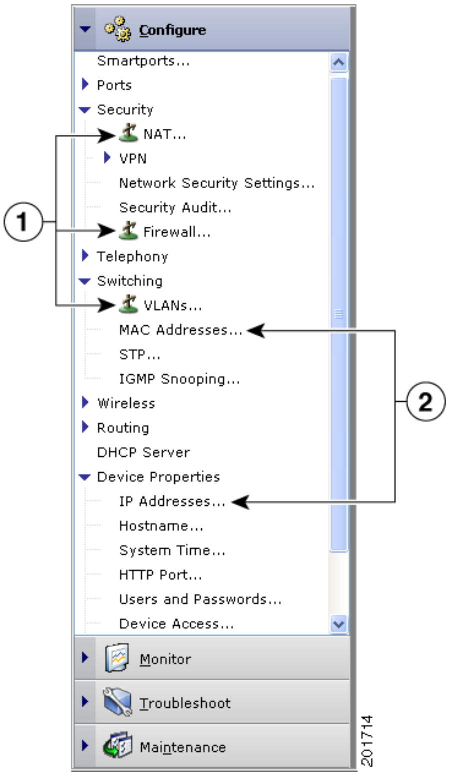
- Easy WLAN monitoring through a single-screen snapshot view of all WLAN network elements and statistics
- Extensive online help for configuring common client devices.

CCA Guide Mode and CCA Expert Mode

Most of the choices on the feature bar, toolbar, and popup menus open feature windows or guide steps. Feature windows are compact—all your options are presented together, without explanatory words. To see explanations, click **Help**. Guide steps, on the other hand, present one option at a time and explain what to do for that option. When you use feature windows, you are in *expert mode*; when you use guide steps, you are in *guide mode*.

CCA is in expert mode by default. The features that you see on the feature bar with an icon beside them can also be shown in guide mode (see Figure 1-2). To access guide mode, choose **Guide** on the Application menu before you select a task. To return to expert mode, choose **Expert** on the Application menu, then select the task.

Figure 1-2 Guide Mode Signposts



1	Examples of features that are available in guide mode and expert mode	**2**	Examples of features that are available only in expert mode

Smartport Support for Catalyst Express 500 Series Switches

CCA recognizes and supports Cisco Smartport technology, a collection of pretested, Cisco-recommended baseline configuration templates for CE520 switches. The Smartports Advisor detects connected Cisco Smart Business Communications System devices and suggests recommended network configuration, QoS, security, and multicast settings.

CCA detects where you have not used Smartports to configure a device connection and alerts you from the Event Notification window. You can configure the connection either manually or based on suggestions provided by CCA. Open the Smartports window to either select a role to apply, or use Smartports to suggest a role to apply.

Note The CCA Smartports option is accessible when there is one or more 520 series switch connected to the network.

Using the Controller Web-Browser Interface (GUI)

The controller web-browser interface (referred to generically as the *GUI*) is part of the embedded software of the WLC526 and has a different but overlapping set of features and capabilities from the CCA. Use the controller GUI for the following tasks:

- **Controller setup**—Use this interface when a WLC526 controller running software versions 4.0 or 4.1 powers on for the first time. The GUI Setup Wizard guides you through the necessary steps for basic controller configuration. For information about this process, refer to the *Quick Start Guide: Cisco 526 Wireless Express Mobility Controller*.

  Note WLC526 controllers running software releases 4.2 and later can use the CCA Device Setup Wizard.

- **Advanced configuration tasks**—IT professionals who have experience with Cisco GUIs can also use the Wireless Express 500 series controller GUI to perform a number of advanced configuration tasks that cannot be done in the current version of CCA. GUI-only tasks include:
  - Advanced monitor and client statistics
  - Advanced WLAN configuration options
  - Advanced QoS settings
  - Advanced WLAN layer 2 and 3 settings
  - Controller advanced interface settings
  - Controller advanced CDP settings
  - Controller advanced DHCP settings
  - Wireless advanced access point configuration settings
  - Wireless advanced access point QoS, timers, and regulatory settings
  - Wireless advanced RRM configuration
  - Security advanced configuration settings
  - Advanced MAC filtering
  - Advanced security for client management

- Advanced client exclusion policies
- Advanced security for access point management
- Advanced SNMP configuration
- Advanced controller management configuration
- Guest Lobby Administrator configuration
- Advanced controller troubleshooting configuration
- Advanced log configurations
- Advanced controller file management configuration options

For help with these and other advanced configuration tasks, refer to the GUI online help.

Using the Command-Line Interface

Use the controller command line interface (CLI) if you are experienced using Cisco CLI commands and want to display system parameters or access debugging information (see Example 1-1).

Example 1-1 CLI Command Output Example

```
(Cisco Controller) >show stats switch summary

Packets Received Without Error.................. 443557435
Broadcast Packets Received...................... 73998045
Packets Received With Error..................... 0
Packets Transmitted Without Error............... 468934
Broadcast Packets Transmitted................... 2341
Transmit Packet Errors.......................... 0
Address Entries Currently In Use................ 2
VLAN Entries Currently In Use................... 1
Time Since Counters Last Cleared................ 76 day 6 hr 38 min 23 sec

(Cisco Controller) >
```

Note The WLC526 controller is simple to install and operate; therefore, the controller CLI consists of a limited number of primarily **show** and **debug** commands.

CHAPTER 2

Adding a WLC526 Controller and LAP521 Access Points

This chapter provides instructions on adding a WLC526 controller and controller-based LAP521 access points to your network using CCA. These sections are provided in this chapter:

Obtaining and Installing CCA

If you have not already installed CCA, go to the following Cisco.com URL, click **Download Software** and follow the instructions:

http://www.cisco.com/en/US/products/ps7287/index.html

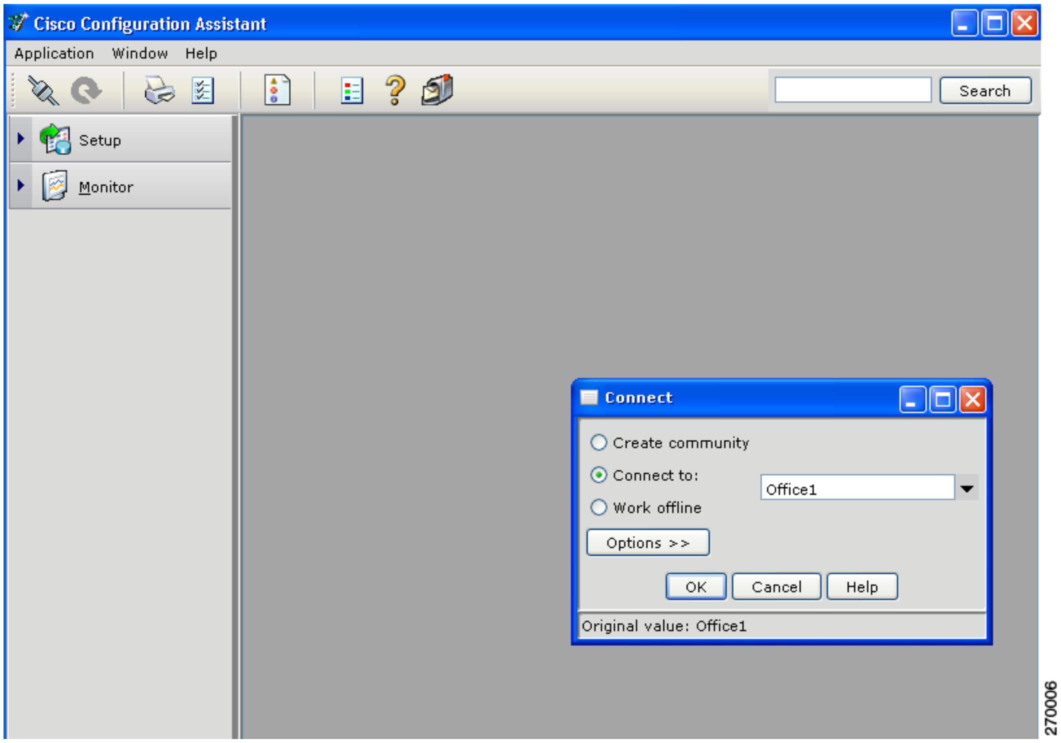
For CCA installation instructions, refer to *Getting Started with Cisco Configuration Assistant 1.5*:

http://www.cisco.com/en/US/products/ps7287/prod_installation_guides_list.html

Starting CCA

Double-click the CCA icon on your desktop to start the application and the CCA window appears (see Figure 2-1).

Figure 2-1 CCA Window



○ Create community
● Connect to: Office1
○ Work offline

Original value: Office1

For additional information about the CCA interface, windows, icons, or menus, refer to Ge*tting Started with Cisco Configuration Assistant 1.5*.

Adding a New Controller

You can use CCA to add and configure your controller. CCA provides a device setup wizard to simplify the configuration process.

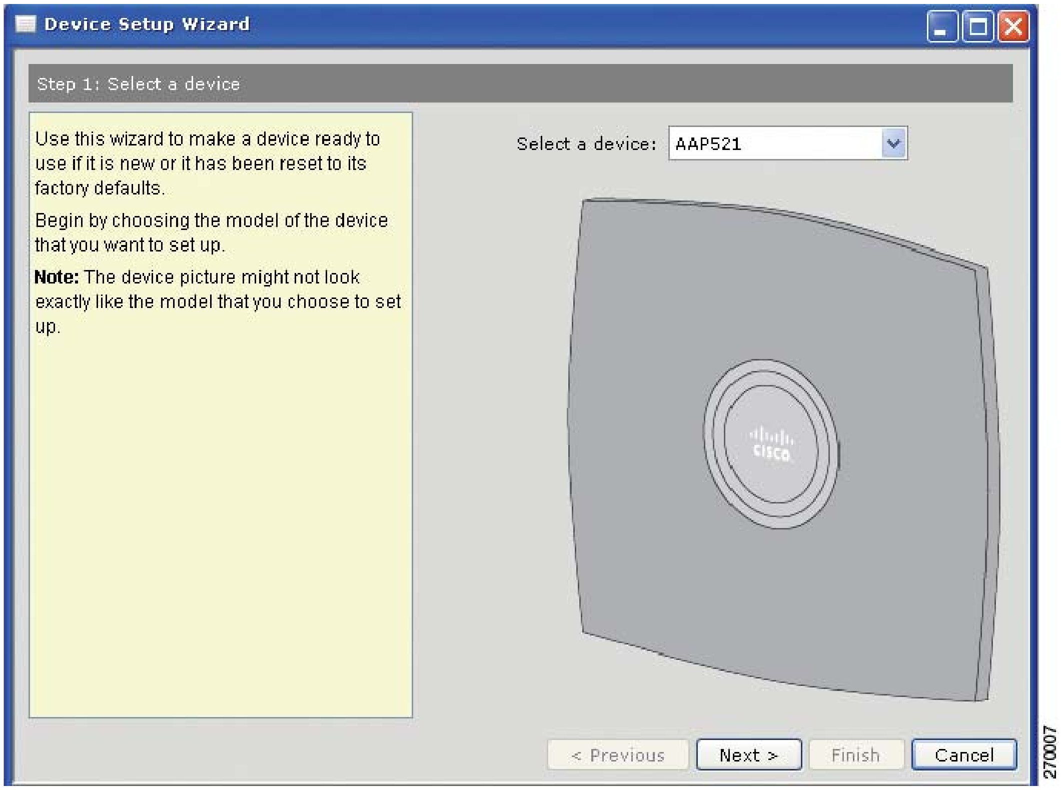
Note The CCA device setup wizard only supports WLC526 Release 4.2 controllers.

The Ethernet adapter on your PC must be configured to automatically receive an IP address from a DHCP server (see the "Verifying and Configuring Your Ethernet Adapter" section on page 2-9).

Follow these instructions to use the device setup wizard to configure a new controller.

Step 1 To start the wizard, click **Setup** > **Device Setup Wizard.** The Step 1: Select a Device window appears (see Figure 2-2).

Figure 2-2 Step 1: Select a Device Window



Device Setup Wizard

Step 1: Select a device

Use this wizard to make a device ready to use if it is new or it has been reset to its factory defaults.

Begin by choosing the model of the device that you want to set up.

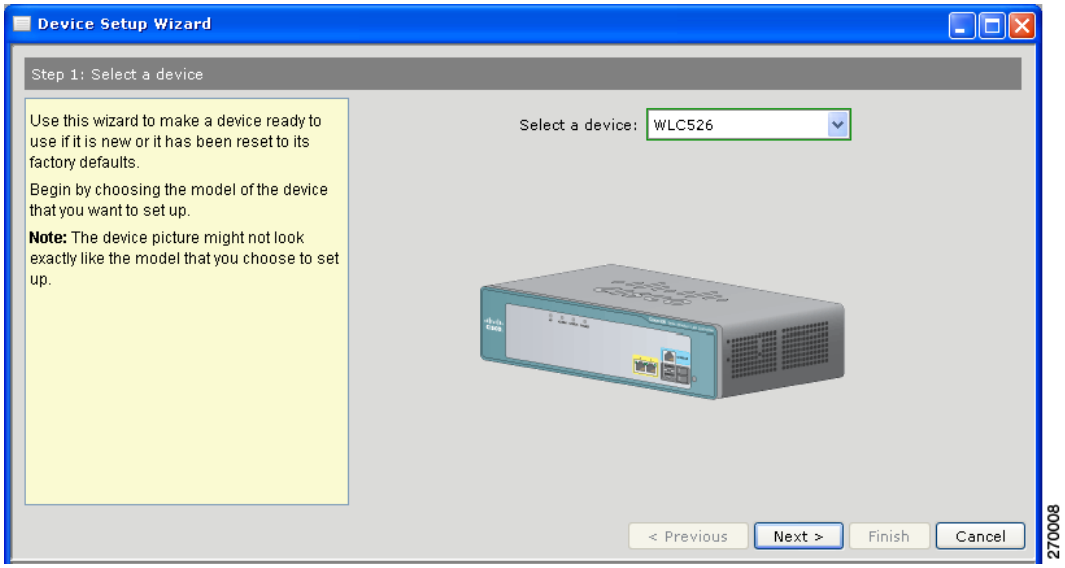
Note: The device picture might not look exactly like the model that you choose to set up.

Select a device: AAP521

Perform these operations:

a. In the Select a device field, click the drop down arrow and choose **WLC526**. Figure 2-3 appears showing the controller.

Figure 2-3 Step 1 with WLC526 Selected



Device Setup Wizard

Step 1: Select a device

Use this wizard to make a device ready to use if it is new or it has been reset to its factory defaults.

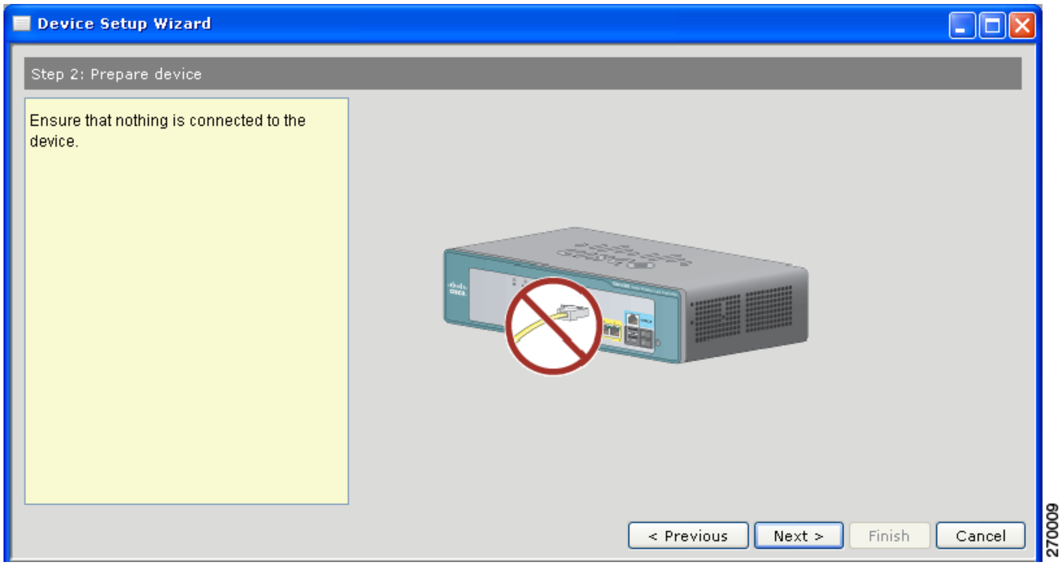
Begin by choosing the model of the device that you want to set up.

Note: The device picture might not look exactly like the model that you choose to set up.

Select a device: WLC526

b. Click **Next** and the Step 2: Prepare a device window appears (see Figure 2-4

Figure 2-4 Step 2: Prepare a Device Window



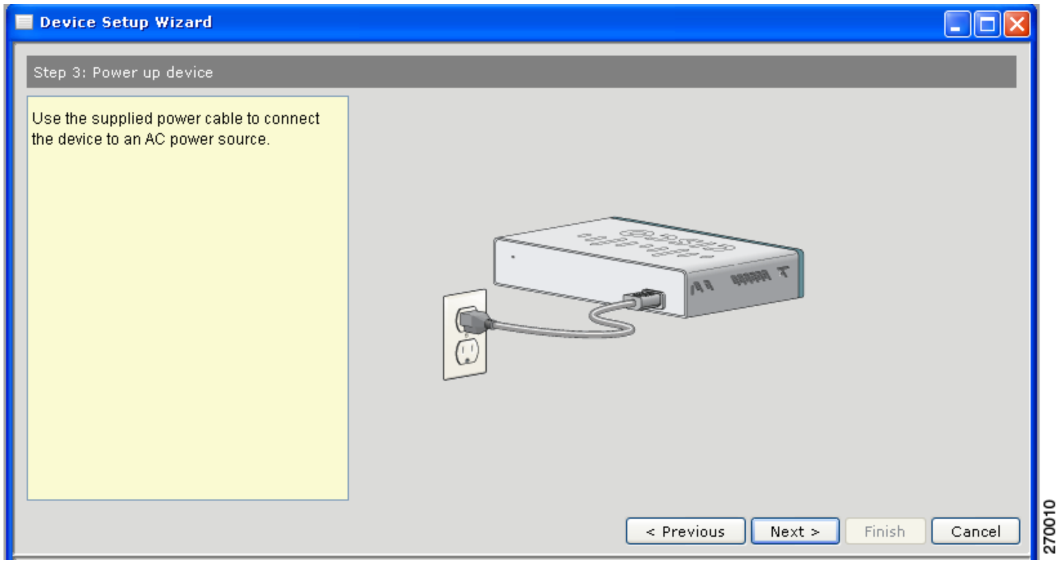
Device Setup Wizard

Step 2: Prepare device

Ensure that nothing is connected to the device.

Step 2 Verify that an Ethernet cable is not connected to any of the controller ports and click **Next**. The Step 3: Power up a device window appears (see Figure 2-5).

Figure 2-5 Step 3: Power Up Device Widow



Device Setup Wizard

Step 3: Power up device

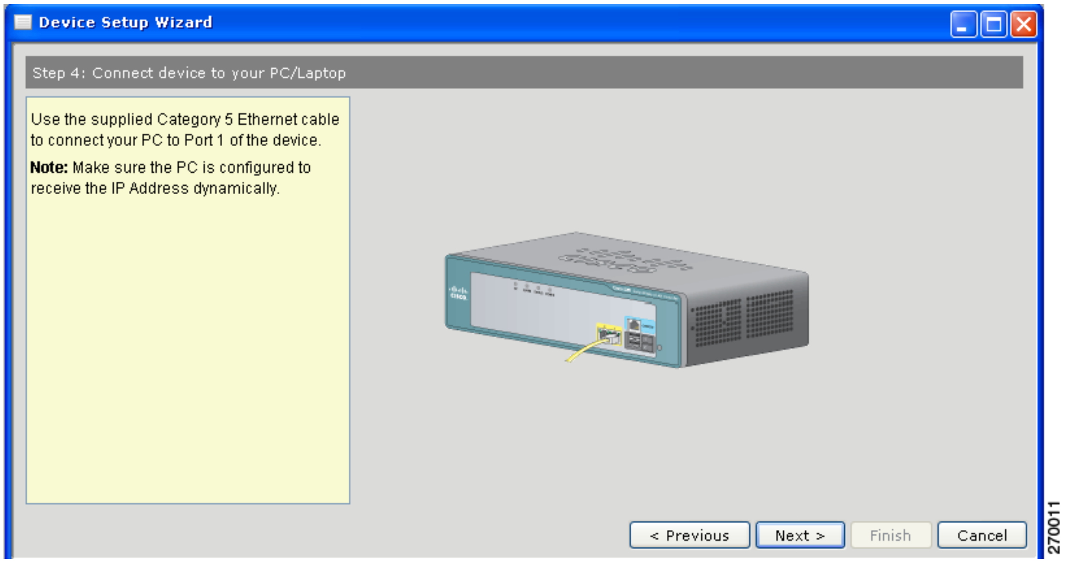
Use the supplied power cable to connect the device to an AC power source.

Step 3 Perform these operations:

a. Connect an AC power cable to the controller.

b. When the power LED turns green, click **Next.** The Step 4: Connect your device to your PC/Laptop window appears (see Figure 2-6).

Figure 2-6 Step 4: Connect Device to Your PC/Laptop Window



Step 4: Connect device to your PC/Laptop

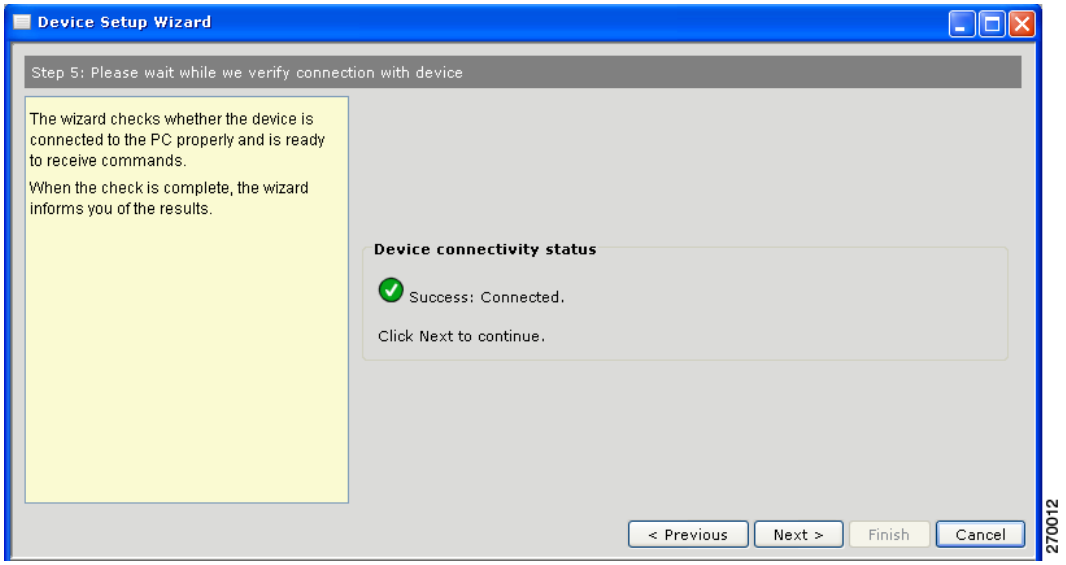
Use the supplied Category 5 Ethernet cable to connect your PC to Port 1 of the device.

Note: Make sure the PC is configured to receive the IP Address dynamically.

Step 4 Connect a Category 5 Ethernet cable from your PC and to Port 1 on the controller.

Step 5 When the wizard verifies successful connection, the Step 5: Verify Connection with Device window displays a successful connection message (see Figure 2-7).

Figure 2-7 Step 5: Verify Connection with Device Window



Step 5: Please wait while we verify connection with device

The wizard checks whether the device is connected to the PC properly and is ready to receive commands.

When the check is complete, the wizard informs you of the results.

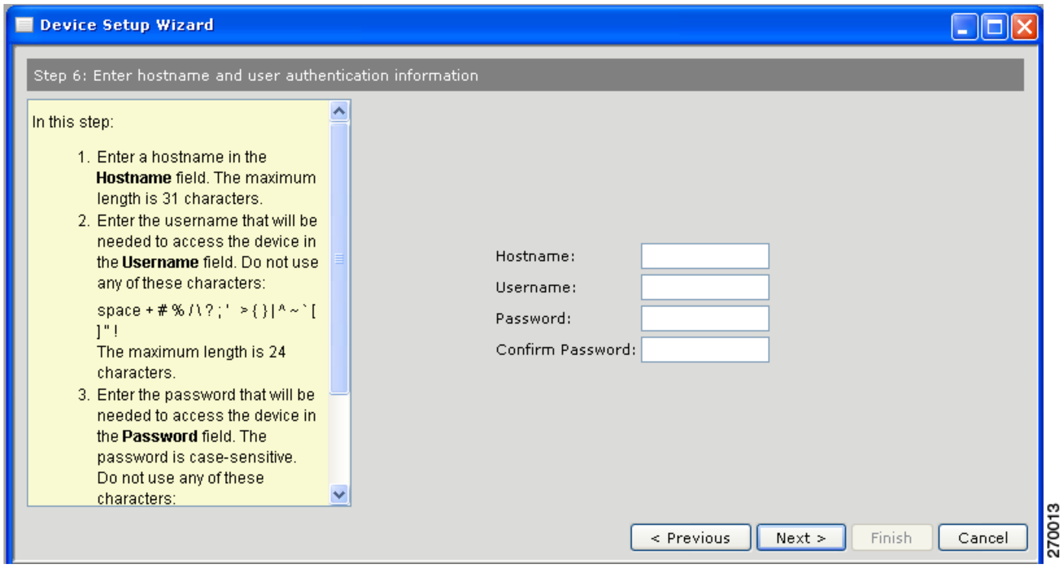
Device connectivity status

✓ Success: Connected.

Click Next to continue.

Step 6 Click Next and the Step 6 Enter Hostname and User Authentication Information window appears (see Figure 2-8).

Figure 2-8 Step 6: Enter Hostname and User Authentication Information Window



Step 6: Enter hostname and user authentication information

In this step:

1. Enter a hostname in the **Hostname** field. The maximum length is 31 characters.
2. Enter the username that will be needed to access the device in the **Username** field. Do not use any of these characters:

   space + # % / \ ? ; ' > { } | ^ ~ ` [ ] " !

   The maximum length is 24 characters.
3. Enter the password that will be needed to access the device in the **Password** field. The password is case-sensitive. Do not use any of these characters:

Hostname:

Username:

Password:

Confirm Password:

Step 7 Perform these operations:

a. Enter a name for the controller (up to 31 ASCII characters) in the Hostname field.

Note The user name cannot contain these characters: space + # % / \ ? ; ' < > { } | ^ ~ [ ] ` " !

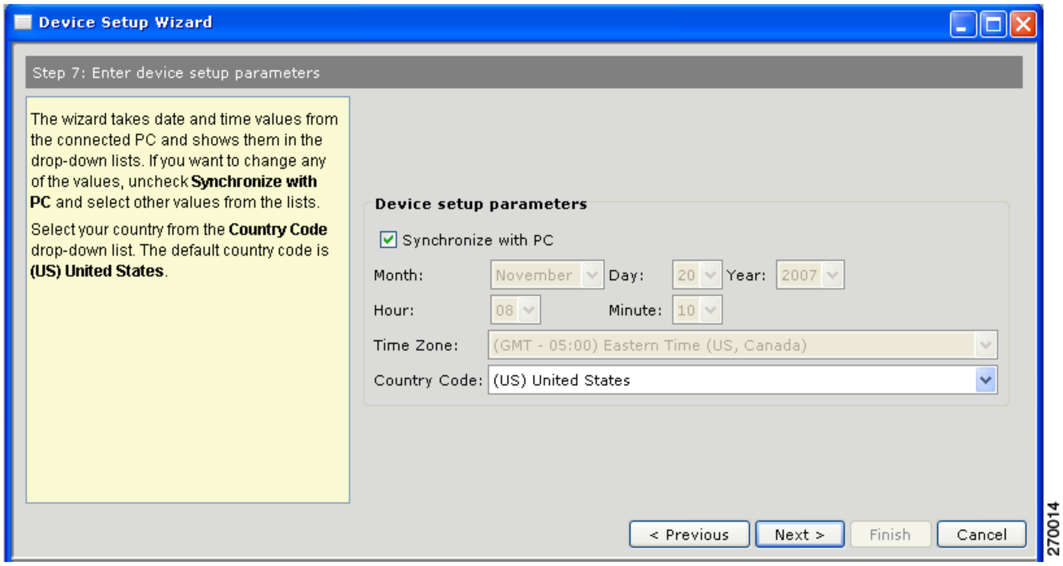
b. Enter the administrator password (up to 24 ASCII characters) into the Password field.

Note The password cannot contain these characaters: space + ? / \ < > # % { } | ^ ~ [ ] ` "
space + ? / \ < > # % { } | ^ ~ [ ] ` "

c. Repeat the administrator password in the Confirm password field.

d. Click **Next** and the Enter Device Setup Parameters window appears (see Figure 2-9).

Figure 2-9 Step 7 Enter Device Setup Parameters Window



Device Setup Wizard

Step 7: Enter device setup parameters

The wizard takes date and time values from the connected PC and shows them in the drop-down lists. If you want to change any of the values, uncheck **Synchronize with PC** and select other values from the lists.

Select your country from the **Country Code** drop-down list. The default country code is **(US) United States**.

Device setup parameters

☑ Synchronize with PC

Month: November Day: 20 Year: 2007

Hour: 08 Minute: 10

Time Zone: (GMT - 05:00) Eastern Time (US, Canada)

Country Code: (US) United States

Step 8 Perform these operations:

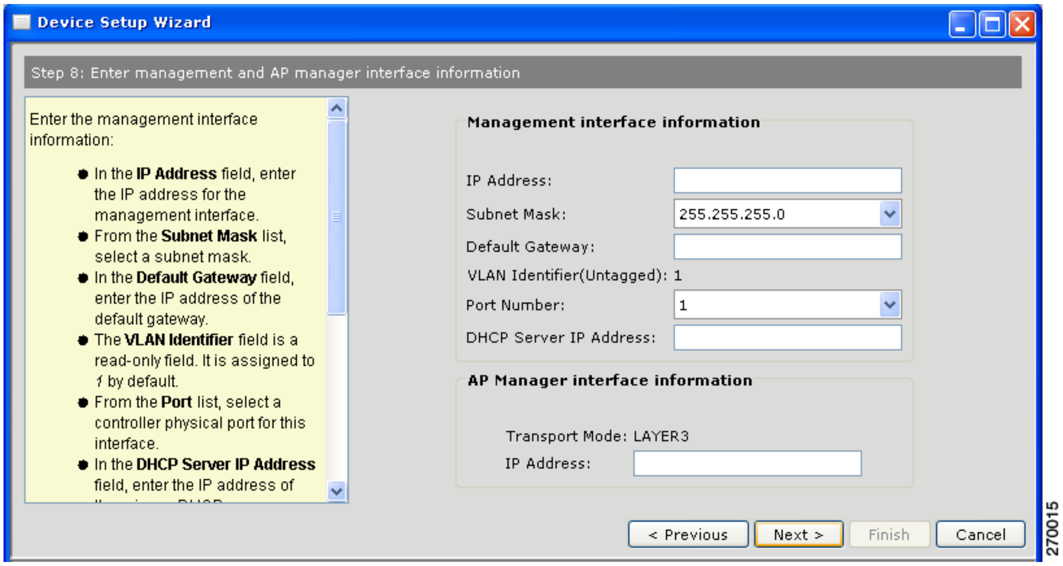
a. Accept the default setting to synchronize the controller time with your PC, or uncheck the Synchronize with PC box.

b. If you unchecked the Synchronize with PC checkbox, configure the month, date, year, hour and minute by clicking the appropriate drop-down arrows and choosing the desired settings.

c. Accept the default US country code or click the drop-down arrow and choose the desired country code setting.

d. Click **Next** and the Step 8 Management and AP Manager Interface Information window appears (see Figure 2-10).

Figure 2-10 Step 8: Management and AP Manager Interface Information Window



Device Setup Wizard

Step 8: Enter management and AP manager interface information

Enter the management interface information:

- In the **IP Address** field, enter the IP address for the management interface.
- From the **Subnet Mask** list, select a subnet mask.
- In the **Default Gateway** field, enter the IP address of the default gateway.
- The **VLAN Identifier** field is a read-only field. It is assigned to *1* by default.
- From the **Port** list, select a controller physical port for this interface.
- In the **DHCP Server IP Address** field, enter the IP address of

Management interface information

IP Address:

Subnet Mask: 255.255.255.0

Default Gateway:

VLAN Identifier(Untagged): 1

Port Number: 1

DHCP Server IP Address:

AP Manager interface information

Transport Mode: LAYER3

IP Address:

Step 9 For the management interface, perform these operations:

a. Enter the IP address of the management interface.

b. Accept the default subnet mask or enter a new subnet mask in the Subnet Mask field.

c. Enter the IP address of the default gateway (or router) in the Default Gateway field.

Note The VLAN identifier is set to 0 for an untagged VLAN. This setting cannot be changed with the CCA. This setting must be the same on the switch.

d. Accept the default controller port 1 setting or click the drop-down arrow to choose port 2. These ports are located on the controller front panel and are used to connect the controller to the network.

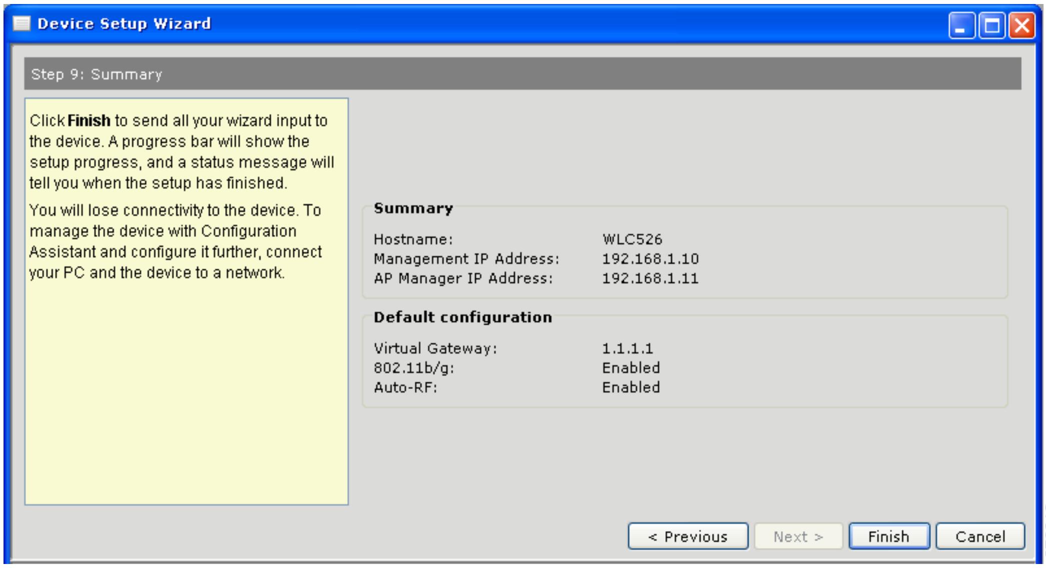
e. Enter the IP address of the DHCP server in the DHCP Server IP Address field.

Note The default for the Transport Mode is Layer 3 and cannot be changed with the CCA.

f. For the AP Manager interface, enter the IP address for the AP Manager in the IP Address field.

g. Click **Next** and the Step 9 Summary window appears (see Figure 2-11).

Figure 2-11 Step 9 Summary Window



Device Setup Wizard

Step 9: Summary

Click **Finish** to send all your wizard input to the device. A progress bar will show the setup progress, and a status message will tell you when the setup has finished.

You will lose connectivity to the device. To manage the device with Configuration Assistant and configure it further, connect your PC and the device to a network.

Summary

Hostname:	WLC526
Management IP Address:	192.168.1.10
AP Manager IP Address:	192.168.1.11

Default configuration

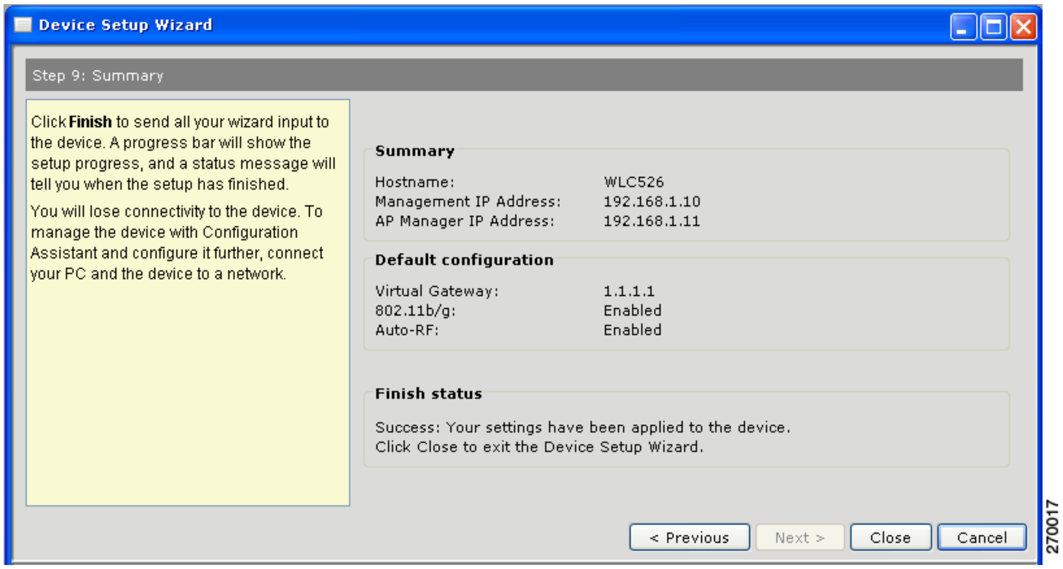
Virtual Gateway:	1.1.1.1
802.11b/g:	Enabled
Auto-RF:	Enabled

Step 10 Carefully review the summary settings and perform one of these operations:

a. If the summary is incorrect or you desire to make changes, click **Previous** and the previous window appears.

b. If the summary is correct, click **Finish** and the wizard begins to transfer the configuration information to the controller (a progress bar appears). When the transfer is complete, the wizard indicates the finish status on the window (see Figure 2-12).

Figure 2-12 Step 9 Summary Window Finish Status



Click **Finish** to send all your wizard input to the device. A progress bar will show the setup progress, and a status message will tell you when the setup has finished.

You will lose connectivity to the device. To manage the device with Configuration Assistant and configure it further, connect your PC and the device to a network.

Summary

Hostname:	WLC526
Management IP Address:	192.168.1.10
AP Manager IP Address:	192.168.1.11

Default configuration

Virtual Gateway:	1.1.1.1
802.11b/g:	Enabled
Auto-RF:	Enabled

Finish status

Success: Your settings have been applied to the device.
Click Close to exit the Device Setup Wizard.

Step 11 Click **Close** to exit the wizard.

Step 12 Remove your PC's Ethernet cable from the controller.

Note Prior to using your PC and CCA to monitor your network, you need to reconfigure your PC Ethernet adapter to a static IP address within the subnet of your network.

Step 13 Mount your access point in the desired location. For mounting information refer to the *Quick Start Guide: Cisco 526 Wireless Express Mobility Controller*.

Step 14 Connect a Category 5 Ethernet cable from the controller management interface port (1 or 2 as configured in Step 9, above) to your switch.

Your controller is now configured and ready to accept access point connections.

Verifying and Configuring Your Ethernet Adapter

To verify that your Ethernet adapter is configured to receive an IP address from a DHCP server on a Windows-based PC, follow these instructions:

Step 1 Click **Start** > **Control Panel** > **Network Connections**.

Step 2 Right-click on your Ethernet adapter and choose **Properties**.

Step 3 Scroll down the list of items and click **Internet Protocol (TCP/IP)**.

Step 4 Click **Properties** and the Internet Protocol (TCP/IP) Properties screen appears.

Step 5 Ensure that **Obtain an IP address automatically** is checked.

Step 6 Click **OK**.

Step 7 Click **OK** on your Ethernet adapter properties screen.

Configuring your Ethernet Adapter to a Static IP Address

To configure your Ethernet adapter to a static IP address on a Windows-based PC, follow these instructions:

Step 1 Click **Start** > **Control Panel** > **Network Connections**.

Step 2 Right-click on your Ethernet adapter and choose **Properties**.

Step 3 Scroll down the list of items and click **Internet Protocol (TCP/IP)**.

Step 4 Click **Properties** and the Internet Protocol (TCP/IP) Properties screen appears.

Step 5 Check *Use the following IP address.*

Step 6 Enter the IP address, the subnet mask, and the default gateway IP address in the corresponding fields.

Step 7 Click **OK**.

Step 8 Click **OK** on your Ethernet adapter properties screen.

Verifying the IP Address of your Ethernet Adapter

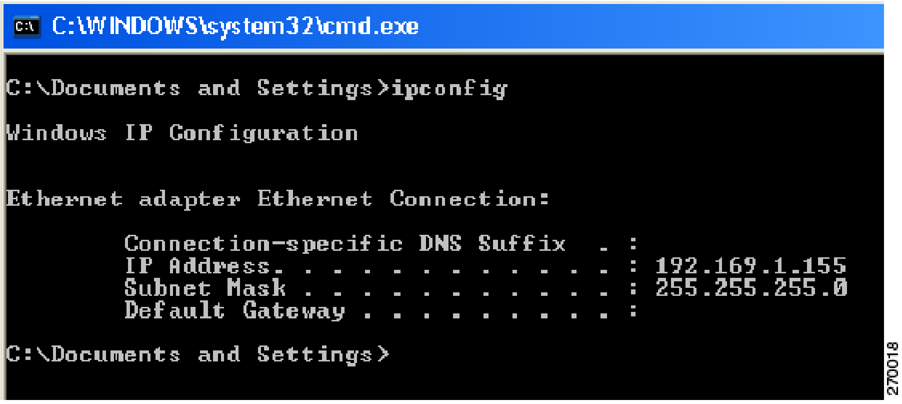
The IP address of your Ethernet adapter must be configured within the same subnet as your system components for use with CCA. To verify the IP address of your Ethernet adapter on a Windows-based PC, follow these instructions:

Step 1 Click **Start** > **Run** and the Run pop-up window appears.

Step 2 Type **cmd** in the Open field and click **OK. The cmd.exe** pop-up window appears.

Step 3 In the pop-up window, type **ipconfig** and press **Enter** (see **Figure 2-13**).

Figure 2-13 IPCONFIG Results Window



```
C:\Documents and Settings>ipconfig

Windows IP Configuration


Ethernet adapter Ethernet Connection:

        Connection-specific DNS Suffix  . :
        IP Address. . . . . . . . . . . . : 192.169.1.155
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :

C:\Documents and Settings>
```

Step 4 After verifying the IP address of your Ethernet adapter, close the window by clicking the Red X box.

Adding LAP521 Access Points

Each WLC526 controller supports up to six controller-based LAP521 access points. For additional information on mounting the access points, refer to the *Quick Start Guide: Cisco 521 Wireless Express Access Point* at this Cisco.com URL:

http://www.cisco.com/en/US/docs/wireless/access_point/521/quick/guide/a521qsg.html

You must connect your LAP521 access points to a switch to enable communications with a controller.

Note The WLC526 controller supports only controller-based LAP521 access points. It does not support Cisco Aironet lightweight access points, such as the 1000, 1130, 1200, 1240, 1250, 1300, 1500, or 1520 series access points.

Note The switch ports to which you connect your access points must be configured as access point *smart ports*. You can use CCA or the switch web-browser interface to configure the switch ports.

The access points can be powered by PoE from your switch, by a power injector, or by a power module. On power up, the access points begin a discovery process that automatically connects them with your controller. The discovery process is indicated by the Status LED indicator on the access point blinking green, red, and amber. When the access point associates with the controller, the Status LED changes to light green. For more information about the LED color codes, refer to the *Quick Start Guide: Cisco 521 Wireless Express Access Point.*

When the LAP521 associates to the WLC526, the controller automatically downloads the latest operating system and configures the access point.

CHAPTER 3

Creating and Connecting to a Community

This chapter describes how to create a community of devices and describes how to connect to a community using the CCA. This chapter contains these sections:

Community Overview

This section provides only a brief overview of communities. For additional information on CCA and communities refer to the *Getting Started with Cisco Configuration Assistant* document available on Cisco.com at this URL:

http://www.cisco.com/en/US/products/ps7287/prod_installation_guides_list.html

CCA manages device groups called communities. In a community, every device must have an IP address. CCA communicates directly with all members of the community, so an HTTPS link is possible with every member.

Characteristics of a Community

In addition to offering the security of HTTPS links, a community has these characteristics:

- It can contain up to 25 SBCS devices, including the UC500, CE520, WLC526 controllers, and stand-alone AP521 access points. Specific limitations include:
  - Five routers
  - Three AP521 autonomous wireless access points
  - Two wireless controllers (which can control up to an additional 12 AP521 access points
  - As many Cisco IP phones as there are available switch ports in the network
- Because every member has an IP address, if you lose communication with a member, you can still communicate with other members.
- A basic set of networking tasks is supported for community members, including routers and access points. The tasks are
  - Managing user access

- Upgrading software
- Saving a running configuration
- Backing up and restoring a configuration
- Managing the system time
- Getting system message notifications
- Changing the HTTP port number
- Getting an inventory report

Creating a Community

You can create a community in either of these ways:

- When you launch CCA, you can use the Connect window that appears.
- Choose **Application** > **Communities** from the menu bar and use the Communities window that appears.
- Choose **Application** > **Connect** and use the Connect window that appears.
- Click the Connect icon on the tool bar and use the Connect window that appears.

Community Limits

Table 3-1 lists the limits on the number of specific device types that can be supported in a community.

Table 3-1 Limits on the Number of Specific Device Types in a Community

Device Type	Limit
Catalyst Express 500 Series Switches	15
Cisco UC500 series appliance	5
Wireless Express 500 series controllers	2
Autonomous AP521 access points	3

IP phones do not count toward the 25-device community limit. You can connect as many IP phones as there are switch ports in the community’s UC500 appliances and CE500 switches.

If you exceed the device limits, you cannot manage the community until you remove enough devices to comply with the limits.

There is no limit to the number of communities that CCA can manage.

Creating a Community of Devices Using the Connect Window

When you launch CCA, two windows open: the CCA window, which contains the user interface, and the Connect window.

CCA starts in a disconnected mode, it is not connected to a community or a standalone device. In this mode, you see the menu bar in the CCA window and only the Setup and Monitor options of the feature bar. The feature bar is populated with device features only when CCA is connected to a community.

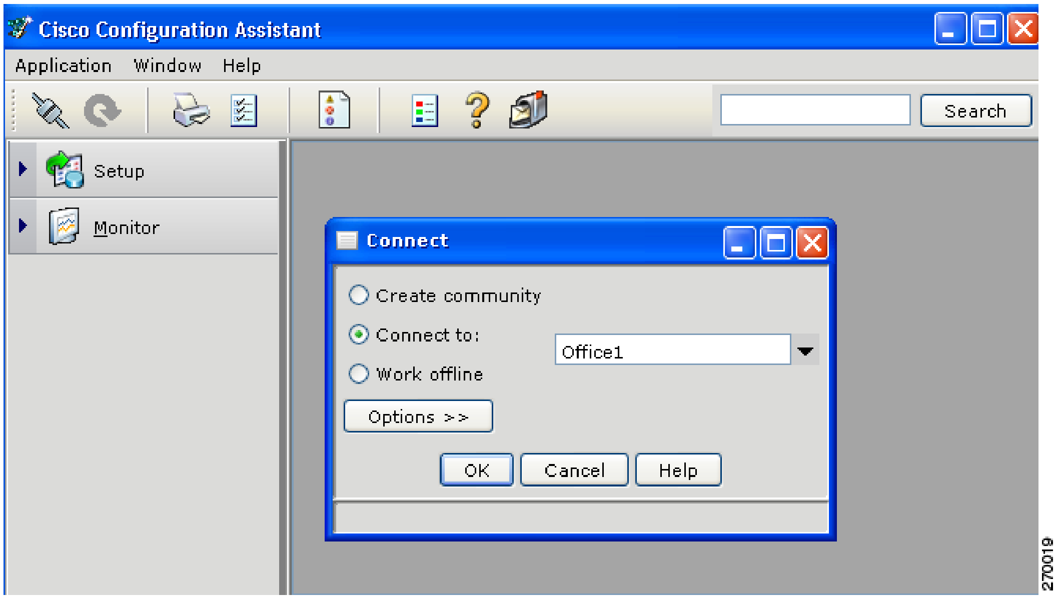
The Connect window gives you these choices:

- Creating a new community. You first create the community and then connect to it.
- Connecting to an existing community or to a standalone device.
- Working offline. When you are offline, only the Voice feature is available on the feature bar. You can specify options for voice communication, save them, and retrieve them in a later session, when you do connect to a community or a standalone device.

To use the Connect window to create a new community of devices, follow these instructions:

Step 1 Check **Create community** in the Connect window (see Figure 3-1).

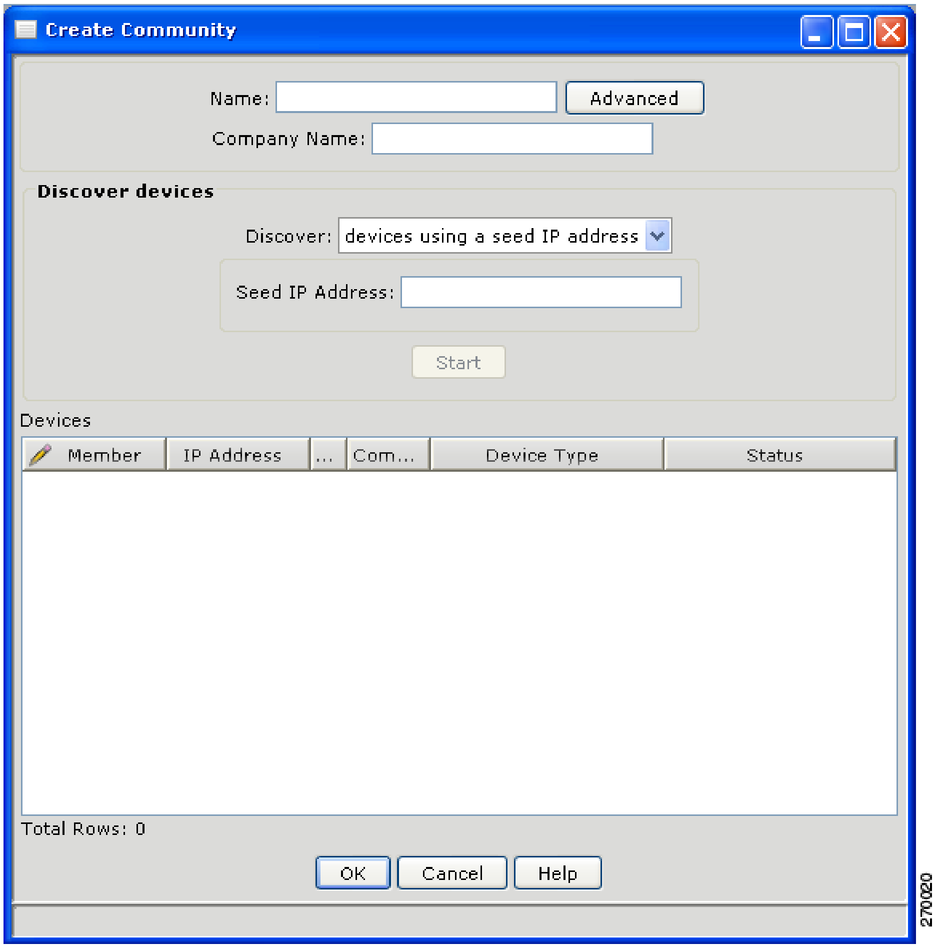
Figure 3-1 Connect Window



○ Create community
● Connect to: Office1
○ Work offline

Step 2 Click **OK** and the Create Community window appears (see Figure 3-2).

Figure 3-2 Create Community Window



Discover: devices using a seed IP address

Total Rows: 0

Step 3 Enter the community name in the Name field (up to 64 characters, A-Z, a-z, 0-9, hyphen, and underscore).

Step 4 (Optional) Enter your company name, your organization, or any other identifying text in the Company Name field. The text is used as the default SSID (service set identifier) for your network.

Step 5 CCA uses the information from the Discovery option to discover devices and their neighbors using the Cisco Discovery Protocol (CDP). The discovered devices and their neighbors are added to your community. Choose a discover option by clicking the drop-down arrow in the Discover field and enter the requested information as listed below:

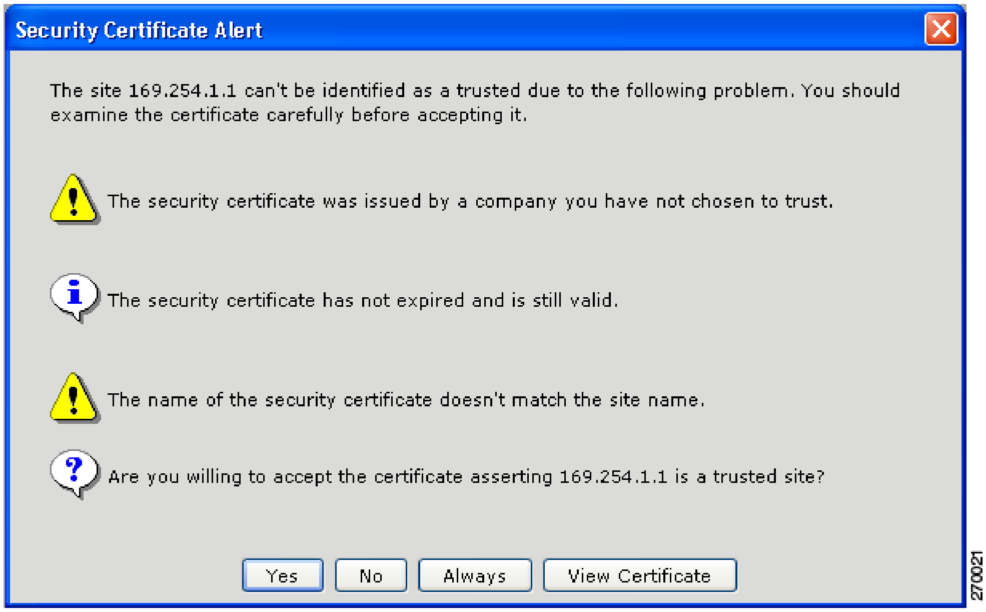
- A single device by IP address—Enter the IP address of the device you want CCA to discover.
- Devices using a seed IP address—(default) Enter the IP address of a device with neighbors that you want CCA to discover.
- Devices on a subnet—Enter the IP address and a subnet mask.
- Devices in an IP address range—Enter the start and end IP addresses of the range.

Step 6 Click **Start**. CCA begins the discovery process and displays a progress bar. When devices are discovered, CCA includes the discovered devices in the Device table.

Step 7 If a pop-up window appears that indicates the expected amount of time for the discovery process, click **Yes** or **No** to continue.

Step 8 If a Security Certificate Alert pop-up window appears (see Figure 3-3) to indicate that a certificate site cannot be identified as a trusted site, you might want to examine the certificate by clicking **View Certificate**. After examining the certificate, click **Yes**, **No**, or **Always**.

Figure 3-3 Security Certificate Alert Pop-Up Window



Security Certificate Alert

The site 169.254.1.1 can't be identified as a trusted due to the following problem. You should examine the certificate carefully before accepting it.

The security certificate was issued by a company you have not chosen to trust.

The security certificate has not expired and is still valid.

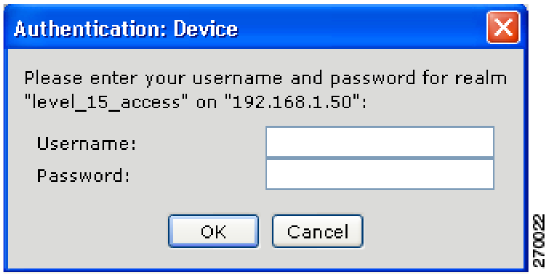
The name of the security certificate doesn't match the site name.

Are you willing to accept the certificate asserting 169.254.1.1 is a trusted site?

Step 9 If an Authentication: Device pop-up windows appears (see Figure 3-4), enter the administrative username and password for the indicated device.

Note For the WLC526 controller and the CE500 switch, the default username and password are both *admin*.

Figure 3-4 Authentication: Device Pop-Up Window



Authentication: Device

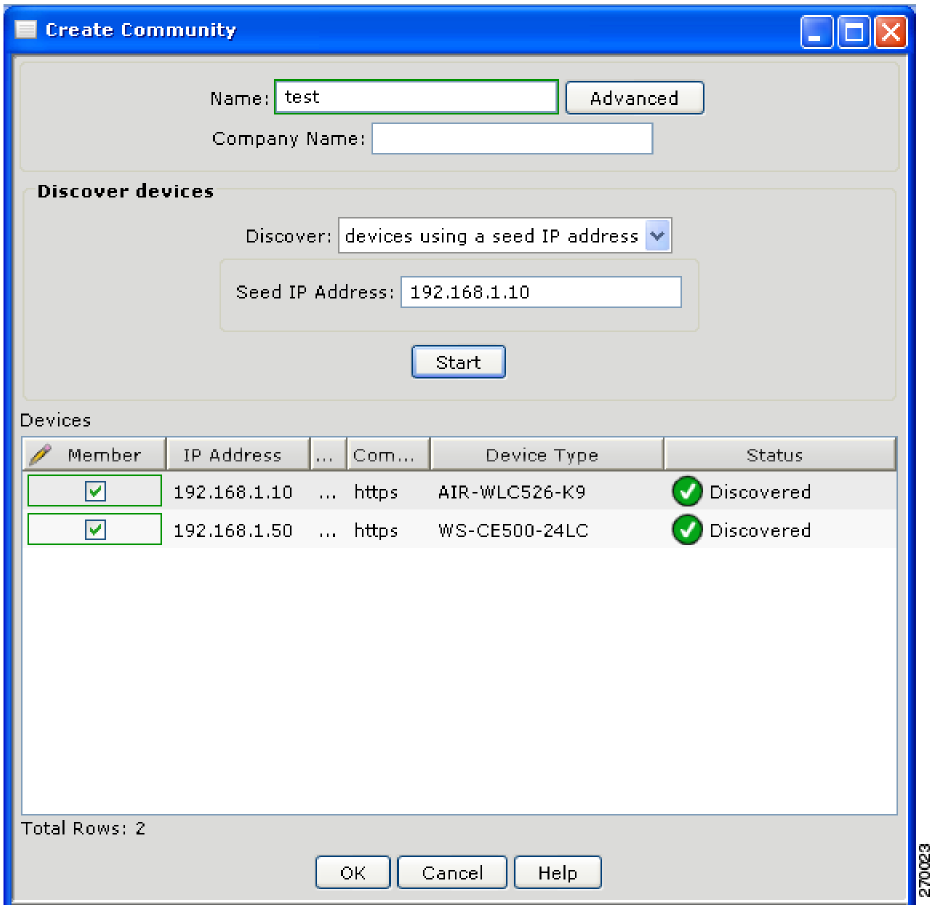
Please enter your username and password for realm "level_15_access" on "192.168.1.50":

Username:

Password:

When the discovery process complete, the discovered devices are listed in the Devices table (see Figure 3-5).

Figure 3-5 Discovered Community Devices



Name: test

Company Name:

Discover devices

Discover: devices using a seed IP address

Seed IP Address: 192.168.1.10

Devices

Member	IP Address	...	Com...	Device Type	Status
☑	192.168.1.10	...	https	AIR-WLC526-K9	✓ Discovered
☑	192.168.1.50	...	https	WS-CE500-24LC	✓ Discovered

Total Rows: 2

Step 10 Click **Ok**.

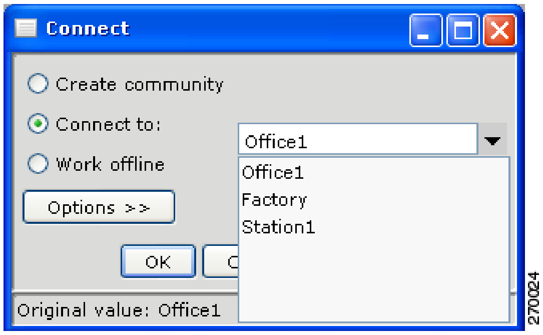
Connecting To a Community

When you connect to a community, you can use CCA to communicate with and manage all of the members. To connect to a community using the Connect window, follow these instructions:

Step 1 Check **Connect to** in the Connect window (see Figure 3-1).

Step 2 Click the drop-down arrow and choose from the list of configured communities (see Figure 3-6).

Figure 3-6 ***Community Drop-Down List***



Connect

○ Create community

● Connect to: Office1

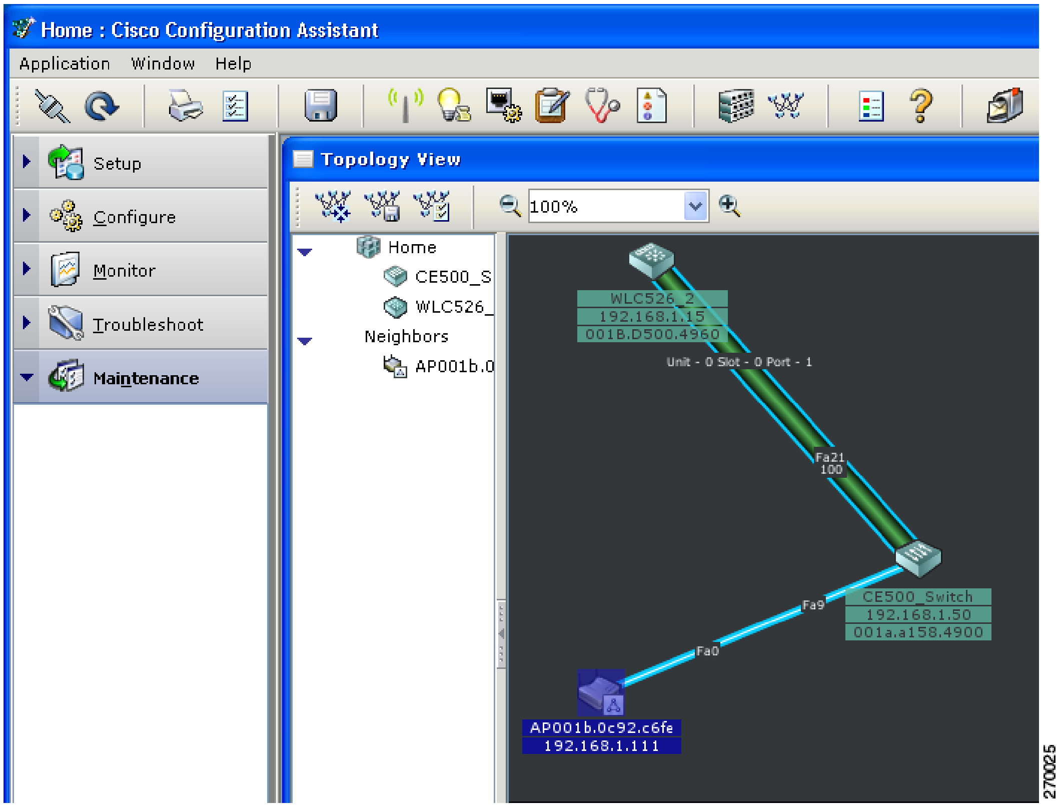
○ Work offline

Office1
Factory
Station1

Original value: Office1

Step 3 Click **OK**. CCA displays a discovery progress bar on the lower left side of the screen. When CCA completes the discovery process, the Topology View window appears (see Figure 3-7).

Figure 3-7 ***Topology View Window***



The topology shows the devices discovered, their connections, the connection ports, and other information for the community that you specified. CCA provides topology options that specify the information displayed for a device. To change the information displayed, right click on the information and choose **Topology Options**.

Note After CCA has connected to a community, the Feature bar expands to cover additional device feature options.

CHAPTER 4

Creating and Modifying WLANs and VLANs

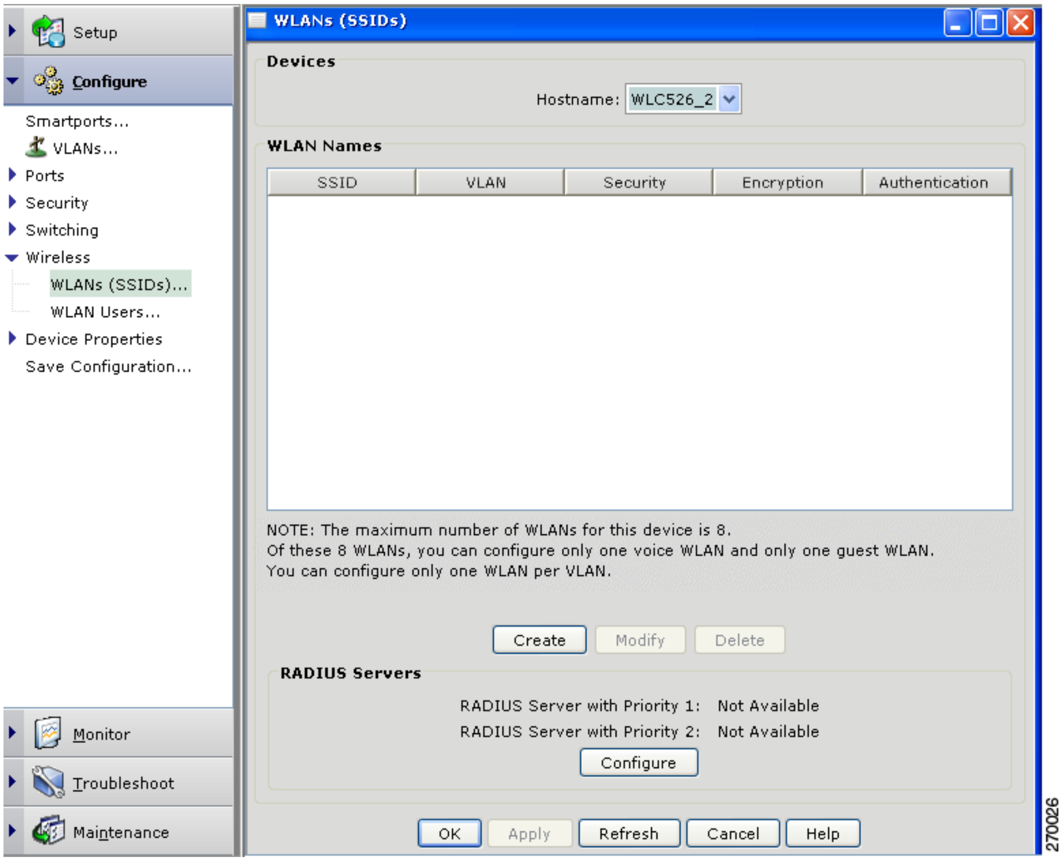
This chapter describes how to use CCA to create and modify wireless LANs (WLANs) and virtual LANs (VLANs). The chapter contains these sections:

Creating a New WLAN

This section describes how to use CCA to create a new WLAN. Follow these steps to create a new WLAN:

Step 1 Click **Configure** > **Wireless** > **WLANs (SSID) and the WLANs (SSID) window appears (see Figure 4-1).**

Figure 4-1 WLAN (SSIDs) Window



Hostname: WLC526_2

SSID	VLAN	Security	Encryption	Authentication

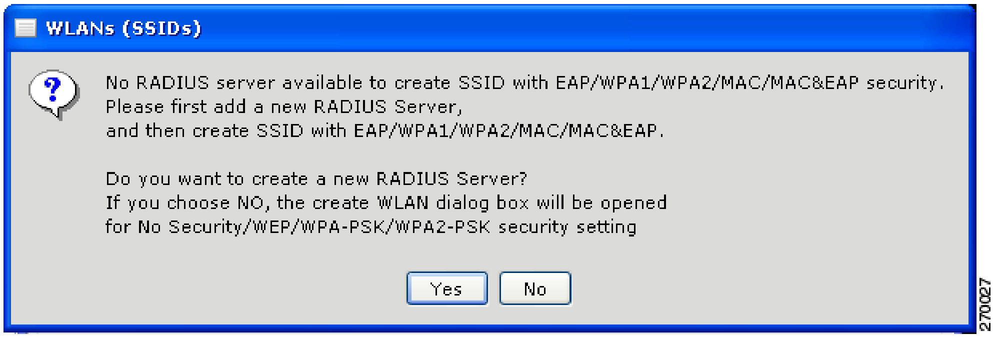
NOTE: The maximum number of WLANs for this device is 8.
Of these 8 WLANs, you can configure only one voice WLAN and only one guest WLAN.
You can configure only one WLAN per VLAN.

RADIUS Server with Priority 1: Not Available
RADIUS Server with Priority 2: Not Available

Step 2 Click **the Hostname drop-down arrow and choose the controller that you want to configure.**

If you fail to configure a RADIUS server, a WLANs (SSIDs) pop-up window appears to indicate that you should create a new RADIUS server (see Figure 4-2).

Figure 4-2 RADIUS Server Required display

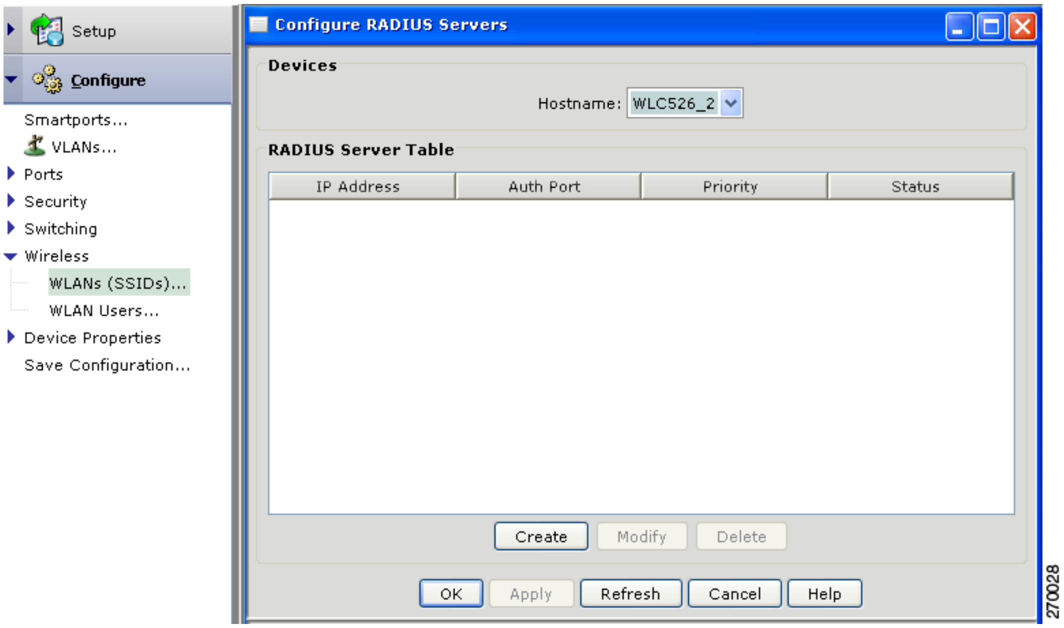


No RADIUS server available to create SSID with EAP/WPA1/WPA2/MAC/MAC&EAP security.
Please first add a new RADIUS Server,
and then create SSID with EAP/WPA1/WPA2/MAC/MAC&EAP.

Do you want to create a new RADIUS Server?
If you choose NO, the create WLAN dialog box will be opened
for No Security/WEP/WPA-PSK/WPA2-PSK security setting

Step 3 Click **Configure** and the Configure RADIUS Servers window appears (see Figure 4-3).

Figure 4-3 Configure RADIUS Servers Window

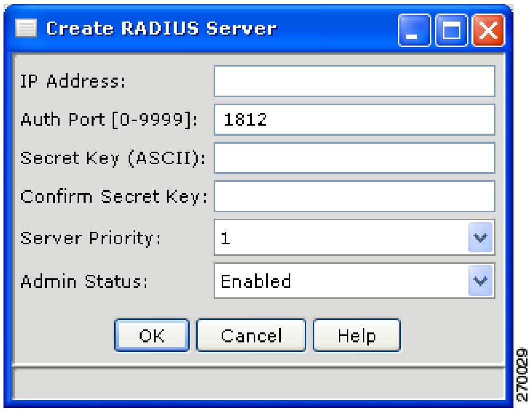


Hostname: WLC526_2

IP Address	Auth Port	Priority	Status

Step 4 Click **Create** and the Create RADIUS Server window appears (see Figure 4-4).

Figure 4-4 Create RADIUS Server Configuration Window



IP Address:

Auth Port [0-9999]: 1812

Secret Key (ASCII):

Confirm Secret Key:

Server Priority: 1

Admin Status: Enabled

Step 5 Perform these operations:

a. Enter the RADIUS server IP address in the IP Address field.

b. Enter the RADIUS server secret key in ASCII in the Secret Key (ASCII) field.

c. Reenter the secret key in the Confirm Secret Key field.

d. Click the Server Priority drop-down arrow and choose the priority (1 or 2). The primary server is used first and is specified by a priority of 1. The secondary server is used when the primary server cannot be reached and is specified by a priority of 2.

e. Click the Admin Status drop-down arrow and choose **Enabled** (default) or **Disabled**.

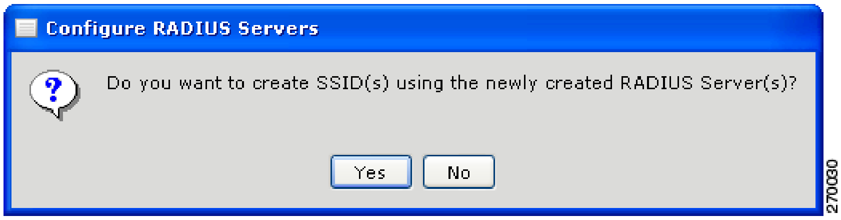
f. Click **OK** and the RADIUS Server entry is listed in the RADIUS server table.

Step 6 Click **Apply** and the RADIUS server configuration information is saved.

Step 7 To configure a secondary RADIUS server, repeat Steps 5 and 6.

Step 8 When done entering RADIUS servers information, click **OK** and a pop-up message (see Figure 4-5) appears asking if you want to create SSIDs using the RADIUS server.

Figure 4-5 Configure RADIUS Server Pop-Up Message



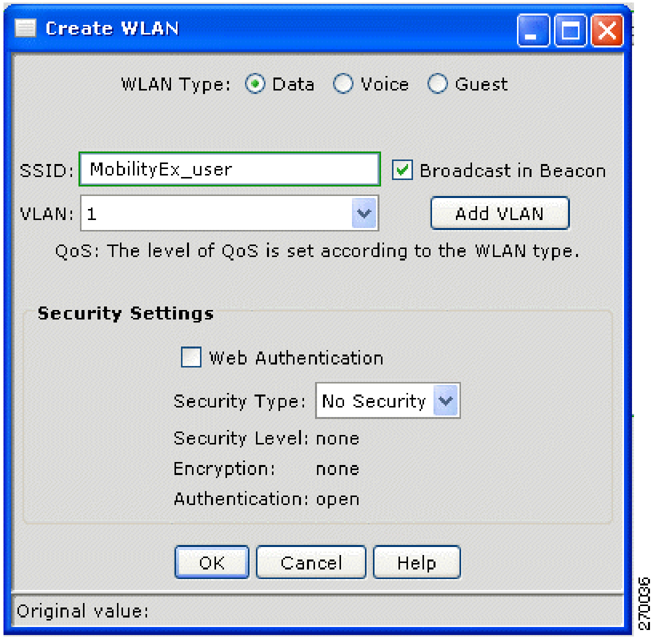
Configure RADIUS Servers

Do you want to create SSID(s) using the newly created RADIUS Server(s)?

Step 9 Click **Yes** on the pop-up message and the WLANs (SSIDs) window appear again (see Figure 4-1).

Step 10 Click **Create** to create a WLAN and Figure 4-6 appears.

Figure 4-6 Create WLAN Window



Create WLAN

WLAN Type: ● Data ○ Voice ○ Guest

SSID: MobilityEx_user ☑ Broadcast in Beacon

VLAN: 1

QoS: The level of QoS is set according to the WLAN type.

Security Settings

□ Web Authentication

Security Type: No Security

Security Level: none

Encryption: none

Authentication: open

Original value:

Step 11 Choose the WLAN type by checking **Data**, **Voice**, or **Guest**.

> **Note** For voice or data WLAN types, the VLAN ID is automatically selected.

Step 12 Enter an SSID in the SSID field (up to 32 alphanumeric characters without spaces).

> **Note** For the guest WLAN type, the SSID can contain a space character but not a leading or trailing space character.

Step 13 Uncheck **Broadcast in Beacon** if you don’t want the SSID included in the beacon packets.

Step 14 Accept the VLAN or click the drop-down arrow to choose another configured VLAN.

Step 15 To add a VLAN, click **Add VLAN** (for instructions on adding a VLAN refer to the "Adding a VLAN" section on page 4-10).

Step 16 Check **Web Authentication** if you want to create a guest or employee user. This option is enabled by default for Guest WLANs.

Step 17 Click the Security Type drop-down arrow and choose one of these security options:

- **No Security**—This is the least secure option. Select it only for an SSID that is used in a public place (guest SSID), and associate it with a VLAN that restricts access to your network. There is no encryption, and the authentication type is open authentication.
- **WEP**—This security setting requires that the access point and the client device (a device that connects to the wireless device such as a laptop or a PC) share the same WEP key to keep the communication private.
- **EAP**—This security setting enables IEEE 802.1X authentication and requires you to select the IP address of a RADIUS server. The encryption type is WEP, and the authentication type is IEEE 802.1x.
- **WPA**—This security setting is more secure than the EAP setting. It enables WPA authentication and requires you to select the IP address of a RADIUS server. Client devices that associate with the access point by using this SSID must be WPA-capable.
- **WPA-PSK**—Select this security setting when you want to use the WPA encryption and you do not have access to a RADIUS server. It requires that the access point and the client device share the same WPA-PSK. The key can be from 8 to 63 characters long.
- **WPA2**—This security setting is more secure than the WPA setting. It enables WPA2 authentication and requires you to select the IP address of a RADIUS server. Client devices that associate with the access point by using this SSID must be WPA2-capable.
- **WPA2-PSK**—Select this security setting when you want to use WPA2 encryption and you do not have access to a RADIUS server. It requires that the access point and the client device share the same WPA2-PSK. The key can be from 8 to 63 characters long. The authentication type is WPA2-PSK.
- **MAC**—Select this security setting when you want to authenticate client devices by using MAC address-based authentication. There is no encryption, and the authentication type is IEEE 802.1x.

Step 18 If you choose WEP security, perform these steps:

a. In the Authentication field, click the drop-down arrow and choose **Open** or **shared key**.

b. In the Key Format field, click the drop-down arrow and choose **Hex** or **ASCII**.

c. Click the Hex Key field drop-down arrow and choose **1**, **2**, **3**, **4**.

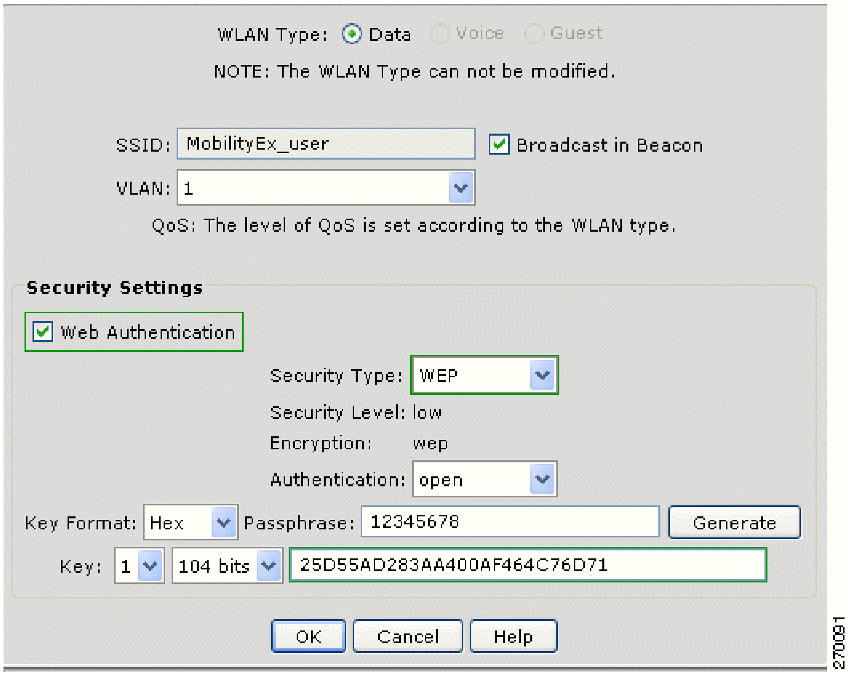
d. Click the key size drop-down arrow and choose one of these options:

   - **104 bits**—Requires 13 ASCII characters or 26 Hex digits.
   - **40 bits**—Requires 5 ASCII characters or 20 Hex digits.

e. If you selected a hex key format, choose one of these options:

   - Enter the encryption key (see key size above).
   - Enter a passphrase (8 to 63 characters) and click **Generate for the encryption key to be automatically created** (see Figure 4-7).

Figure 4-7 Passphrase and Auto-Generated Hex Key



WLAN Type: ● Data ○ Voice ○ Guest

NOTE: The WLAN Type can not be modified.

SSID: MobilityEx_user ☑ Broadcast in Beacon

VLAN: 1

QoS: The level of QoS is set according to the WLAN type.

Security Settings

☑ Web Authentication

Security Type: WEP

Security Level: low

Encryption: wep

Authentication: open

Key Format: Hex Passphrase: 12345678

Key: 1 104 bits 25D55AD283AA400AF464C76D71

Step 19 If you choose WPA security, perform these steps:

a. Click the Encryption drop-down arrow and choose **aes** or **tkip**.

b. Click the Authentication drop-down arrow and choose one of these authentication options:

- **802.1x** (default)
- `Fast roaming (CCKM)`
- **802.1x, fast roaming (CCKM)**

Step 20 If you choose WPA-PSK, WPA2, or WPA2-PSK security, perform these steps:

a. Click the Encryption drop-down arrow and choose **AES** or **TKIP**.

Note The authentication is WPA-PSK, WPA2-PSK, or WPA2-PSK corresponding to the security type.

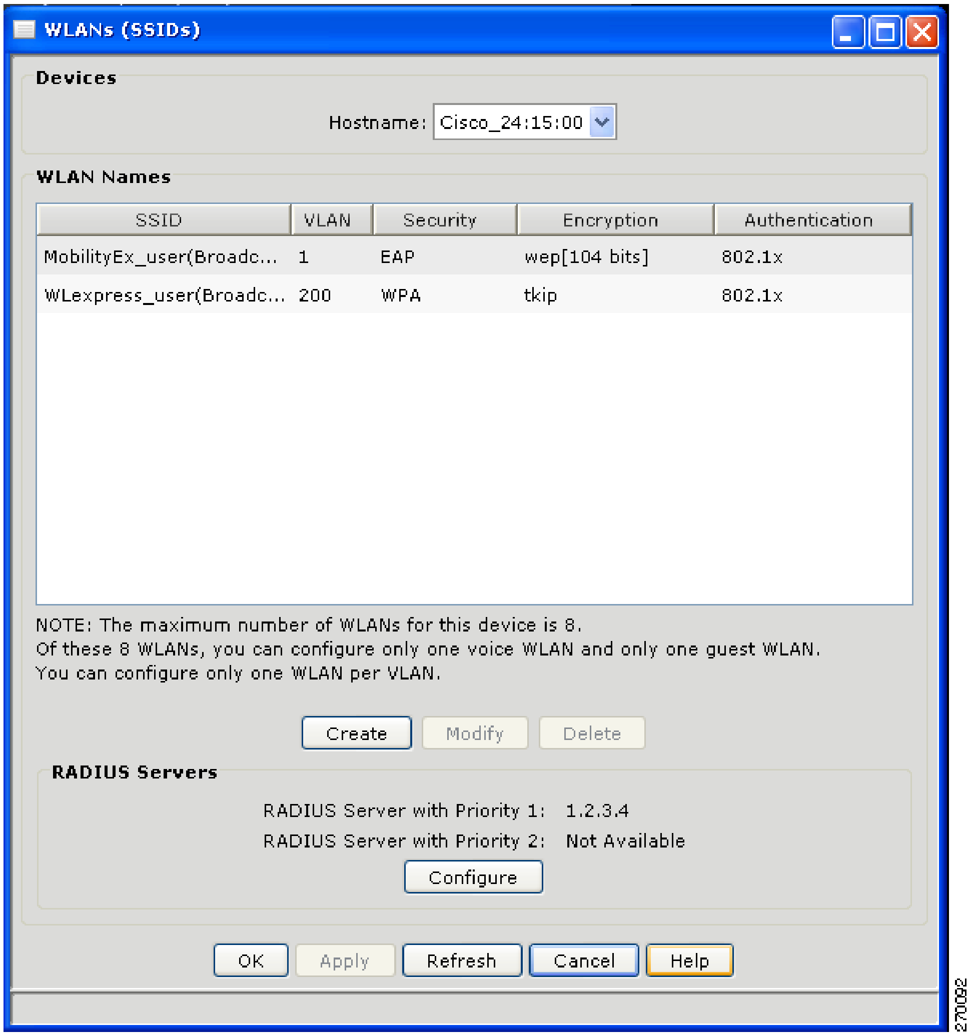
b. Enter the WPA pre-shared key (8 to 63 characters long).

Step 21 If you selected a voice WLAN type, choose one of these voice CAC types:

- **Wireless MultiMedia Policy**—(Default) requires client devices to use WMM.
- **7920 CAC (AP and Client)**—Supports Cisco 7920 IP telephones on your network.

Step 22 Click **OK and the specified WLAN information is visible in the WLAN Names list (see Figure 4-8).**

Figure 4-8 WLAN List



Hostname: Cisco_24:15:00

SSID	VLAN	Security	Encryption	Authentication
MobilityEx_user(Broadc...	1	EAP	wep[104 bits]	802.1x
WLexpress_user(Broadc...	200	WPA	tkip	802.1x

NOTE: The maximum number of WLANs for this device is 8.
Of these 8 WLANs, you can configure only one voice WLAN and only one guest WLAN.
You can configure only one WLAN per VLAN.

RADIUS Servers

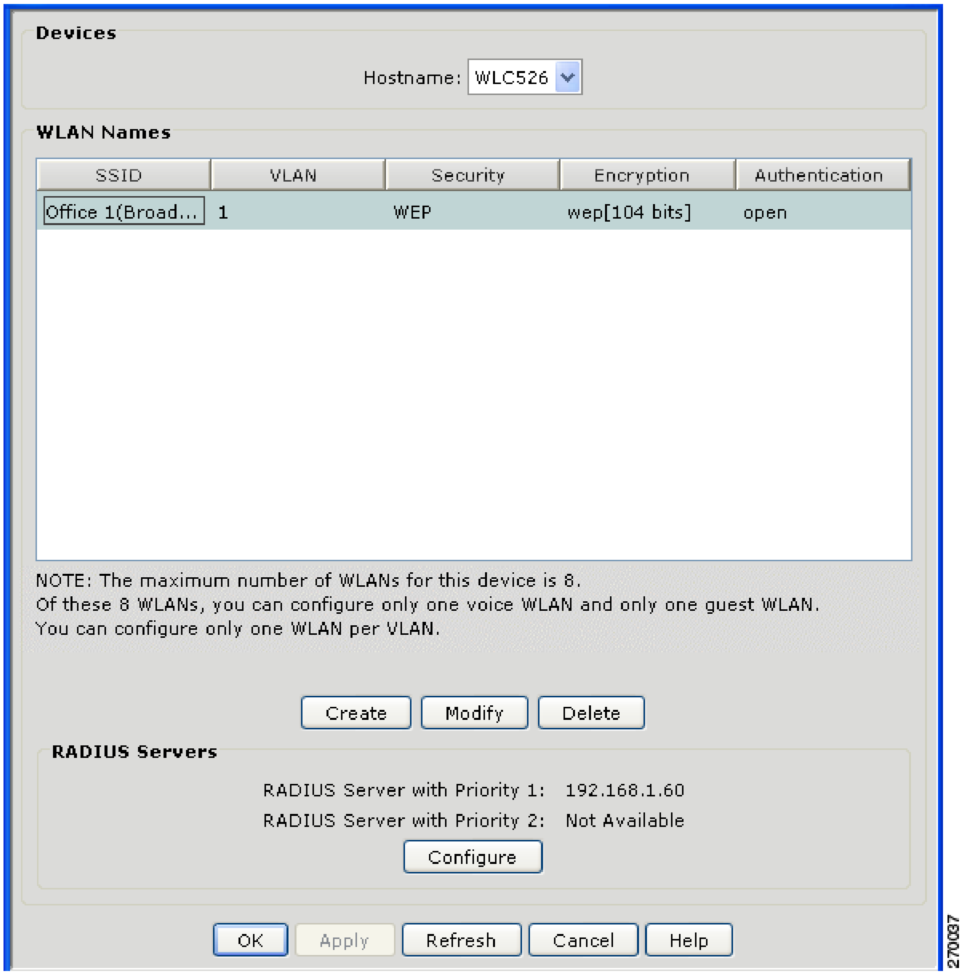
RADIUS Server with Priority 1: 1.2.3.4
RADIUS Server with Priority 2: Not Available

Modify a WLAN

To modify a WLAN, follow these steps:

Step 1 Click **Configure** > **Wireless** > **WLANs** and the WLANs window appears (see Figure 4-12):

Figure 4-9 WLAN Window with Defined WLANs



Devices

Hostname: WLC526

WLAN Names

SSID	VLAN	Security	Encryption	Authentication
Office 1(Broad...	1	WEP	wep[104 bits]	open

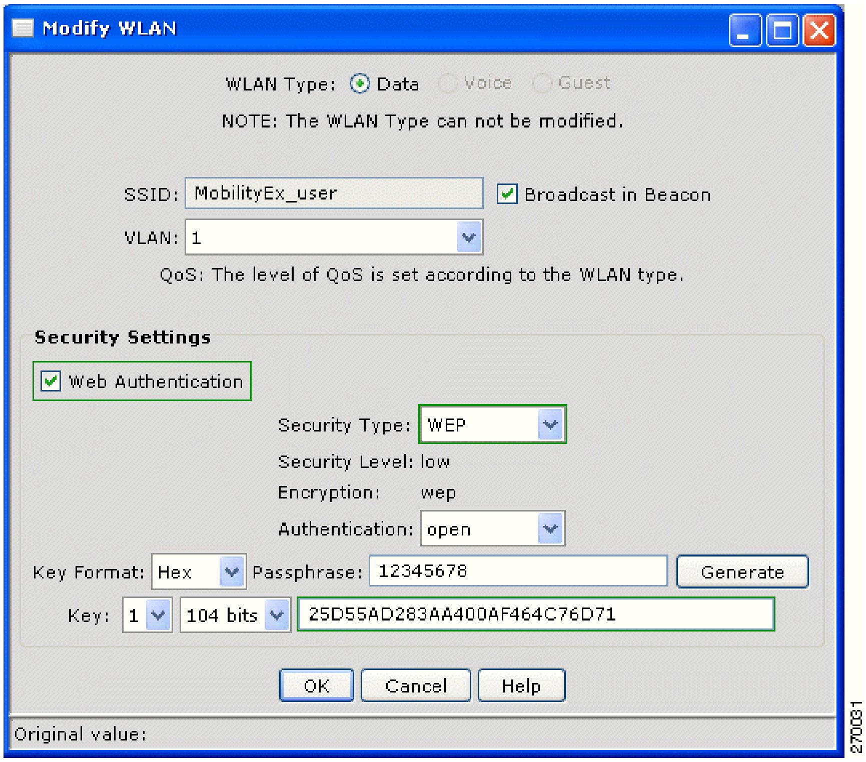
NOTE: The maximum number of WLANs for this device is 8.
Of these 8 WLANs, you can configure only one voice WLAN and only one guest WLAN.
You can configure only one WLAN per VLAN.

RADIUS Servers

RADIUS Server with Priority 1: 192.168.1.60
RADIUS Server with Priority 2: Not Available

Step 2 Click **Modify** and Figure 4-10 appears.

Figure 4-10 Modify WLAN Window



Modify WLAN

WLAN Type: ● Data ○ Voice ○ Guest

NOTE: The WLAN Type can not be modified.

SSID: MobilityEx_user ☑ Broadcast in Beacon

VLAN: 1

QoS: The level of QoS is set according to the WLAN type.

Security Settings

☑ Web Authentication

Security Type: WEP

Security Level: low

Encryption: wep

Authentication: open

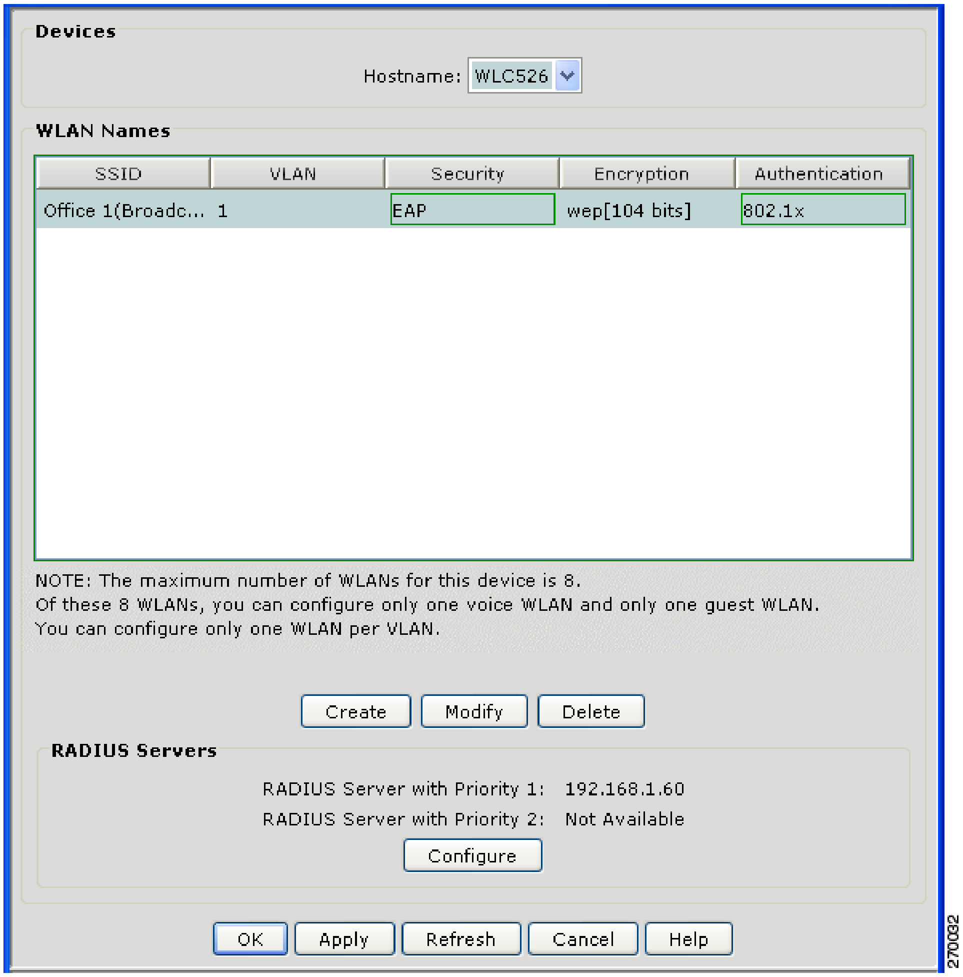
Key Format: Hex Passphrase: 12345678

Key: 1 104 bits 25D55AD283AA400AF464C76D71

Original value:

Step 3 Change the WLAN information as needed and then click **OK**. Figure 4-11 appears with the changed information.

Figure 4-11 WLAN Window with Modified Information



Devices

Hostname: WLC526

WLAN Names

SSID	VLAN	Security	Encryption	Authentication
Office 1(Broadc...	1	EAP	wep[104 bits]	802.1x

NOTE: The maximum number of WLANs for this device is 8.
Of these 8 WLANs, you can configure only one voice WLAN and only one guest WLAN.
You can configure only one WLAN per VLAN.

RADIUS Servers

RADIUS Server with Priority 1: 192.168.1.60
RADIUS Server with Priority 2: Not Available

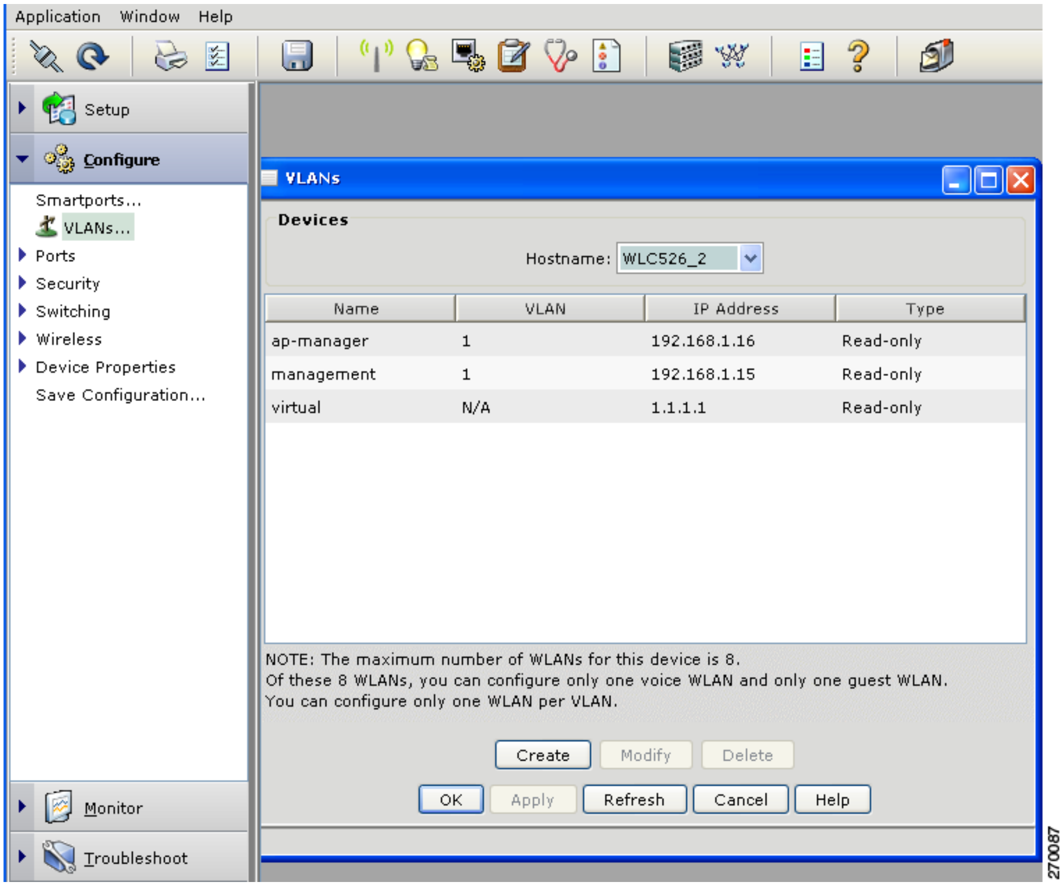
Step 4 Click **OK**.

Adding a VLAN

To add a new VLAN, follow these steps:

Step 1 Click **Configure** > **Wireless** > **VLANs** and the VLANs window appears (see Figure 4-12):

Figure 4-12 VLANs Window with Existing VLANs



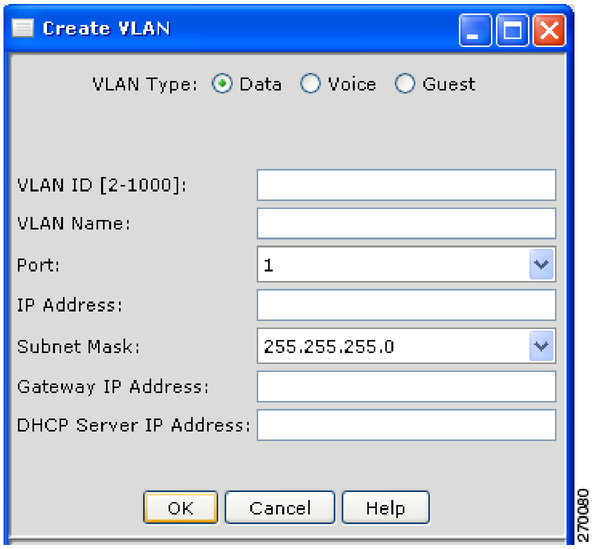
Hostname: WLC526_2

Name	VLAN	IP Address	Type
ap-manager	1	192.168.1.16	Read-only
management	1	192.168.1.15	Read-only
virtual	N/A	1.1.1.1	Read-only

NOTE: The maximum number of WLANs for this device is 8.
Of these 8 WLANs, you can configure only one voice WLAN and only one guest WLAN.
You can configure only one WLAN per VLAN.

Step 2 Click Create and the Create VLANs window appears (see Figure 4-13).

Figure 4-13 Create VLAN Window



VLAN Type: ● Data ○ Voice ○ Guest

VLAN ID [2-1000]:	
VLAN Name:	
Port:	1
IP Address:	
Subnet Mask:	255.255.255.0
Gateway IP Address:	
DHCP Server IP Address:	

Step 3 Perform these steps:

a. Enter a VLAN ID value (2 to 1000) into the VLAN ID field.

b. Accept the auto generated VLAN name or enter a unique name in the VLAN Name field.

c. Accept the displayed controller Port number or click the drop-down arrow and choose **2**.

d. Enter an IP address for the VLAN in the IP Address field.

e. Accept the displayed subnet mask or enter a new subnet mask value.

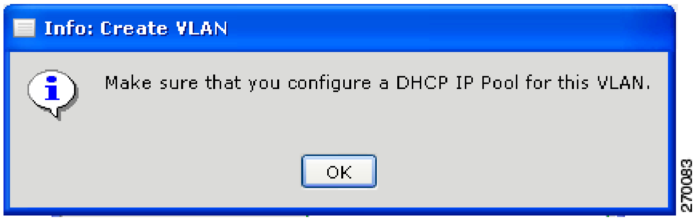
f. Enter the IP address for the Gateway (or router) in the Gateway IP Address field.

g. Enter the IP address for the DHCP server in the DHCP Server IP Address field.

h. When you reviewed your entries, click **OK**.

Step 4 When the pop-up message appears that indicates you should configure a DHCP server with IP addresses for the VLAN subnet (see Figure 4-14), you should record the reminder and click **OK**.

Figure 4-14 Info: Create VLAN Message Reminder

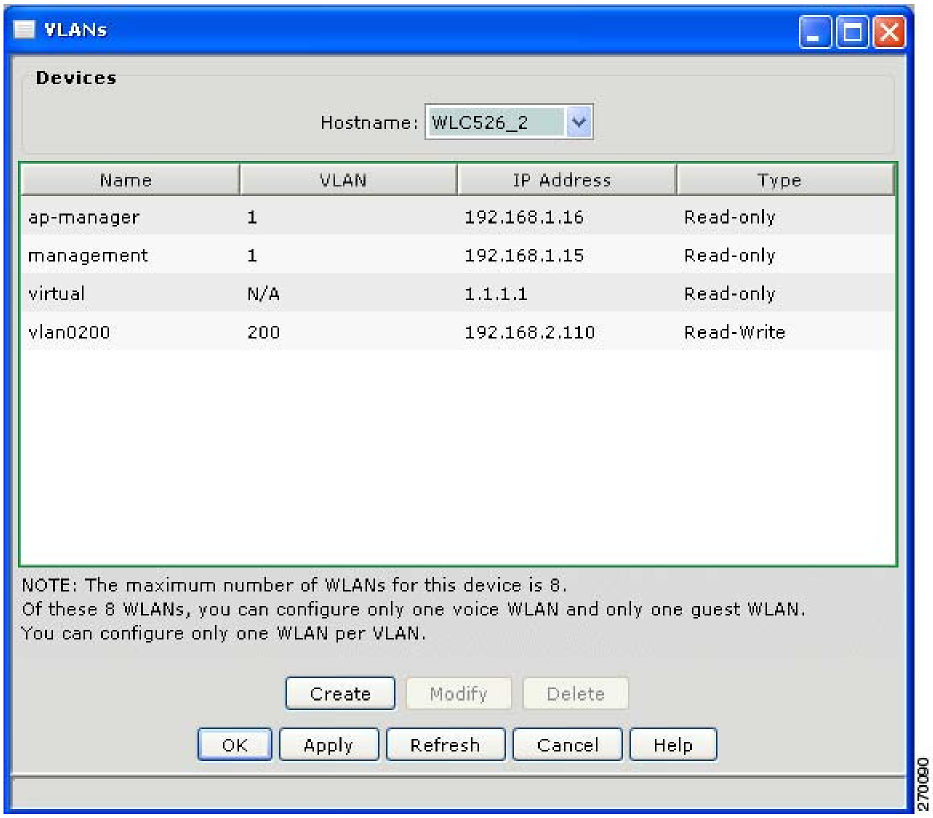


Info: Create VLAN

Make sure that you configure a DHCP IP Pool for this VLAN.

The VLANs window (see Figure 4-15) appears and contains the added VLAN.

Figure 4-15 VLANs Window with the New VLAN



Hostname: WLC526_2

Name	VLAN	IP Address	Type
ap-manager	1	192.168.1.16	Read-only
management	1	192.168.1.15	Read-only
virtual	N/A	1.1.1.1	Read-only
vlan0200	200	192.168.2.110	Read-Write

NOTE: The maximum number of WLANs for this device is 8.
Of these 8 WLANs, you can configure only one voice WLAN and only one guest WLAN.
You can configure only one WLAN per VLAN.

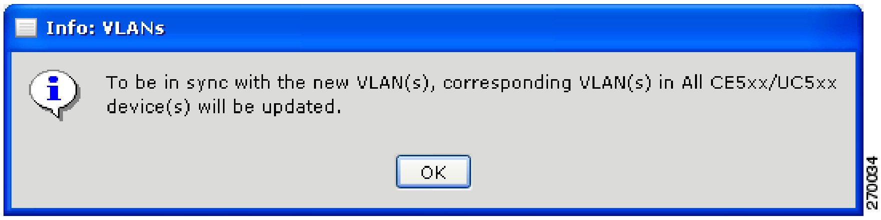
Step 5 If you need to add more VLANS, click **Apply** and repeat Steps 2 through Step 4.

Step 6 When you have finished adding VLANs, click **OK**.

Step 7 If CCA detects an error or a conflict with a settings already configured in the switch, a pop-up message appears indicating you should revise the field indicated with a red box. Make necessary corrections and click **OK**.

Step 8 If a pop-up message appears (see Figure 4-16) that indicates the corresponding VLANs in all switches will be updated, click **OK**.

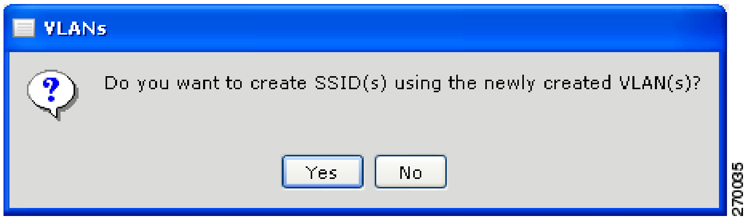
Figure 4-16 VLANs Pop-Up Message



To be in sync with the new VLAN(s), corresponding VLAN(s) in All CE5xx/UC5xx device(s) will be updated.

Step 9 When a pop-up message appears (see Figure 4-17) that asks if you want to create an SSID using the VLAN data, click **Yes or No**.

Figure 4-17 Create SSID Prompt



Do you want to create SSID(s) using the newly created VLAN(s)?

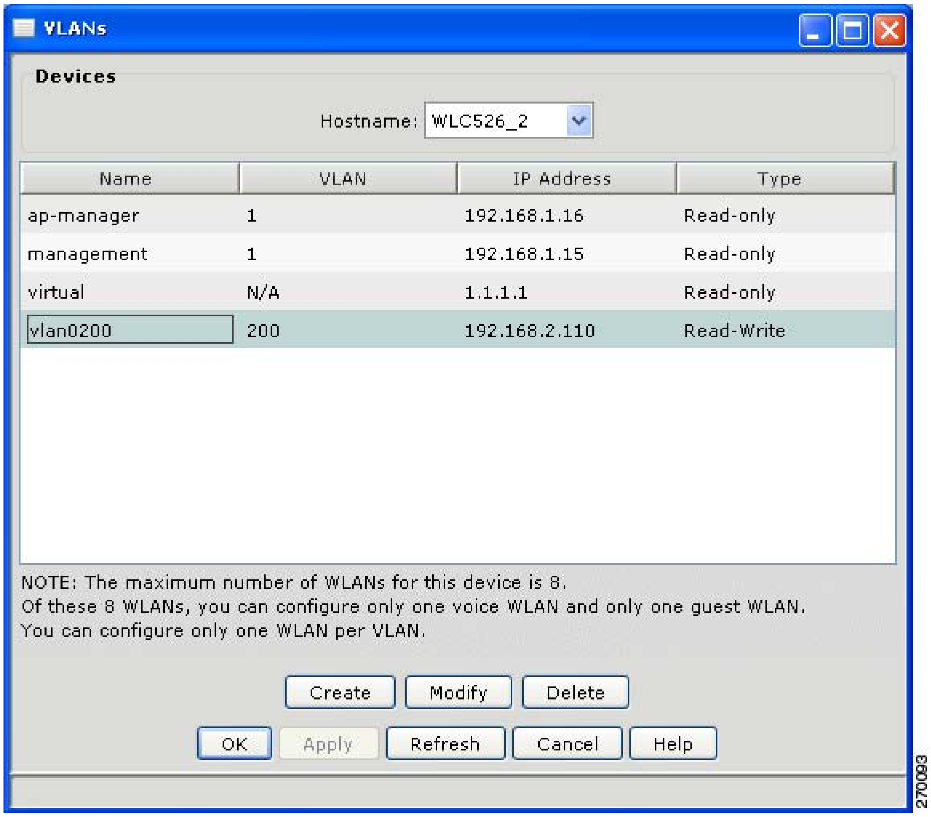
Step 10 If you choose Yes to create an SSID, go to Step 10 in the Create WLAN section to enter the new SSID information.

Modifying a VLAN

To modify an existing VLAN, follow these steps:

Step 1 Click **Configure** > **Wireless** > **VLANs** and the VLANs window appears (see Figure 4-18):

Figure 4-18 VLANs Window with Existing VLANS



Hostname: WLC526_2

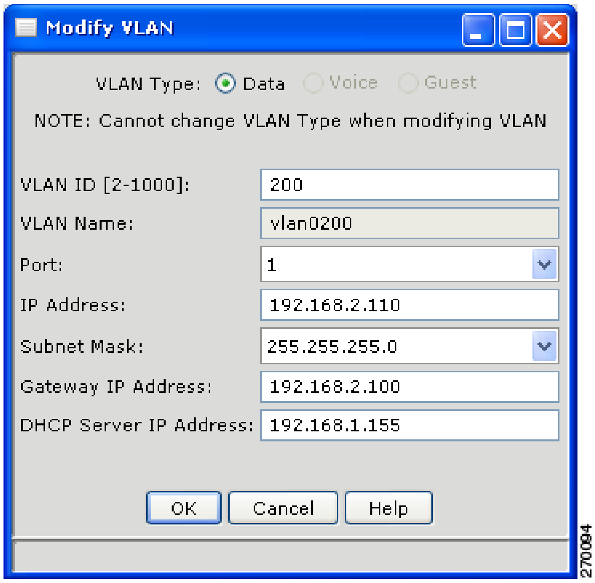
Name	VLAN	IP Address	Type
ap-manager	1	192.168.1.16	Read-only
management	1	192.168.1.15	Read-only
virtual	N/A	1.1.1.1	Read-only
vlan0200	200	192.168.2.110	Read-Write

NOTE: The maximum number of WLANs for this device is 8.
Of these 8 WLANs, you can configure only one voice WLAN and only one guest WLAN.
You can configure only one WLAN per VLAN.

Step 2 Click the VLAN that you want to modify to highlight it (see Figure 4-18).

Step 3 Click **Modify** and the Modify VLAN window appears (see Figure 4-19).

Figure 4-19 Modify VLAN Window



VLAN Type: ● Data ○ Voice ○ Guest

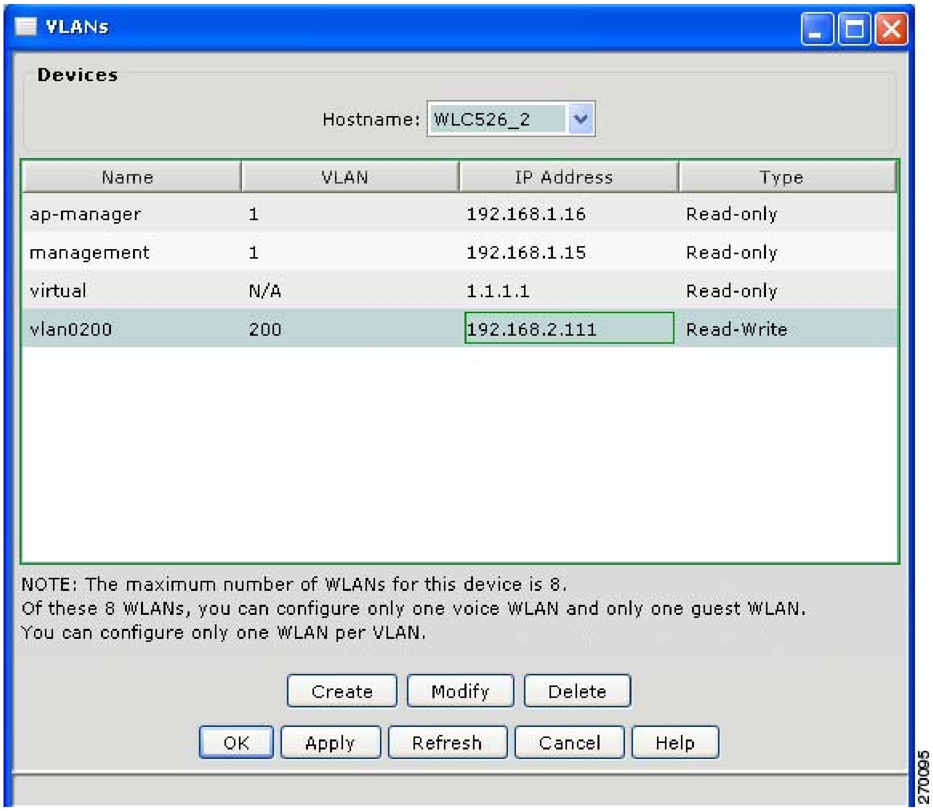
NOTE: Cannot change VLAN Type when modifying VLAN

VLAN ID [2-1000]: 200
VLAN Name: vlan0200
Port: 1
IP Address: 192.168.2.110
Subnet Mask: 255.255.255.0
Gateway IP Address: 192.168.2.100
DHCP Server IP Address: 192.168.1.155

Step 4 Use the left mouse button to highlight the data you want to modify, then enter the desired data.

Step 5 When you have finished modifying the data fields, click **OK.** Figure 4-20 **appears and contains the revised VLAN.**

Figure 4-20 VLANs Window with Revised VLAN



Hostname: WLC526_2

Name	VLAN	IP Address	Type
ap-manager	1	192.168.1.16	Read-only
management	1	192.168.1.15	Read-only
virtual	N/A	1.1.1.1	Read-only
vlan0200	200	192.168.2.111	Read-Write

NOTE: The maximum number of WLANs for this device is 8.
Of these 8 WLANs, you can configure only one voice WLAN and only one guest WLAN.
You can configure only one WLAN per VLAN.

Step 6 If you need to revise additional VLANs, click **Apply** and repeat Step 2 through Step 5.

Step 7 When you have finished modifying the VLANs, click **OK**.

CHAPTER 5

Controller Software Upgrade

This chapter describes how to upgrade WLC526 controller software using CCA. This chapter contains these sections:

- Obtaining the Controller Software Image, page 5-1
- Upgrading Controller Software, page 5-1

Obtaining the Controller Software Image

Prior to attempting a software upgrade, you must obtain the software image for your controllers and autonomous access points. The latest software images are available for download from Cisco.com at this URL:

http://www.cisco.com/en/US/products/ps7320/index.html

Click **Software Download** and follow the prompts to obtain the latest WLC526 controller software image. Save the software images to your hard drive.

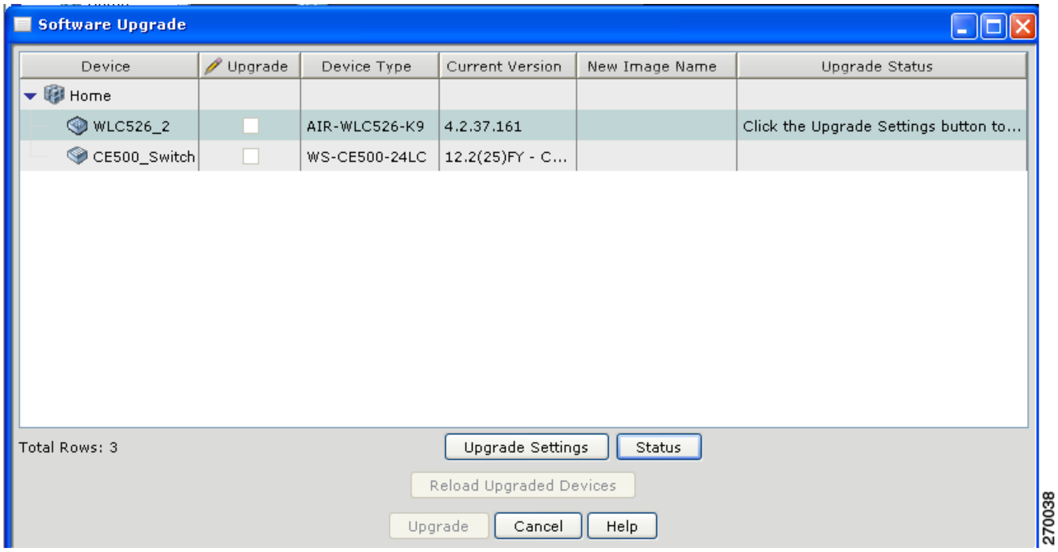
Upgrading Controller Software

CCA enables you to upgrade software on a single device or to simultaneously upgrade the software on multiple devices. This section will describe how to upgrade your controller software using the feature bar software upgrade option.

Follow these steps to upgrade your controller software:

Step 1 Click **Maintenance** > **Software Upgrade** and Figure 5-1 appears.

Figure 5-1 Controller Software Upgrade Window

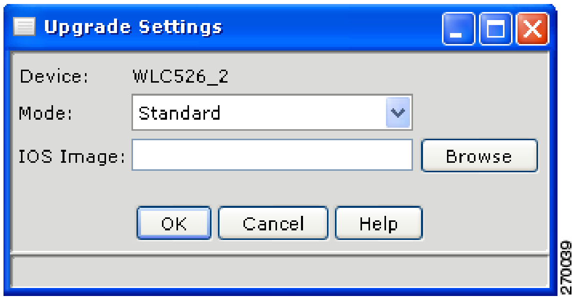


Device	Upgrade	Device Type	Current Version	New Image Name	Upgrade Status
Home					
WLC526_2	□	AIR-WLC526-K9	4.2.37.161		Click the Upgrade Settings button to...
CE500_Switch	□	WS-CE500-24LC	12.2(25)FY - C...		

Total Rows: 3

Step 2 Highlight your switch and click **Upgrade Settings**. Figure 5-2 appears.

Figure 5-2 Upgrade Settings Window



Device: WLC526_2

Mode: Standard

IOS Image:

Step 3 Click the drop-down arrow in the Mode field and choose **Standard** or **Remote TFTP Server**.

Step 4 If you selected Standard, enter the path/filename of the controller software image in the IOS Image field or click **Browse** and navigate to the controller software image file on your hard drive.

Step 5 If you selected Remote TFTP Server, perform these steps:

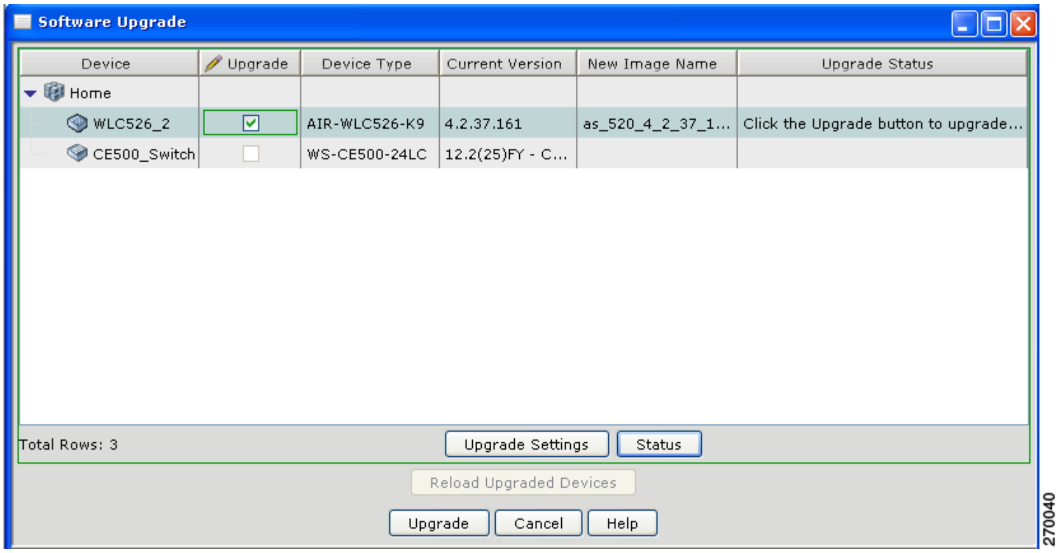
a. Enter the filename of the controller software image in the IOS Image field.

b. Enter the TFTP server IP address in the corresponding field.

> **Note** The controller software image file must be in your TFTP server download directory.

Step 6 Click OK and Figure 5-3 appears.

Figure 5-3 ***Controller Upgrade Selected***



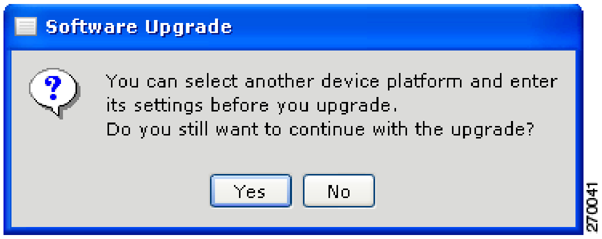
Software Upgrade

Device	Upgrade	Device Type	Current Version	New Image Name	Upgrade Status
Home					
WLC526_2	☑	AIR-WLC526-K9	4.2.37.161	as_520_4_2_37_1...	Click the Upgrade button to upgrade...
CE500_Switch	□	WS-CE500-24LC	12.2(25)FY - C...		

Total Rows: 3

Step 7 Click **Upgrade** and Figure 5-4 appears.

Figure 5-4 ***Software Upgrade Pop Up Message***



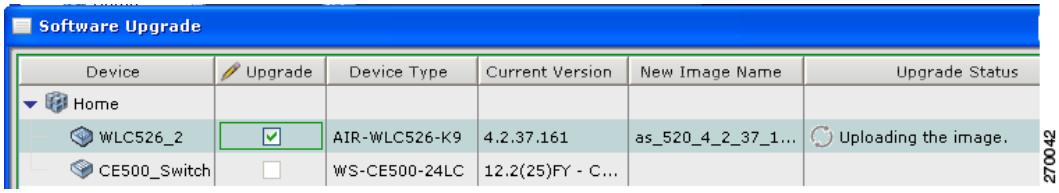
Software Upgrade

You can select another device platform and enter its settings before you upgrade.
Do you still want to continue with the upgrade?

Step 8 Click one of these options:

- **Yes—to continue with the software upgrade.** Figure 5-5 **appears.**
- **No**—to specify upgrade options for another device. Go to Step 6 to enter additional upgrade information.

Figure 5-5 ***Loading the Controller Image***



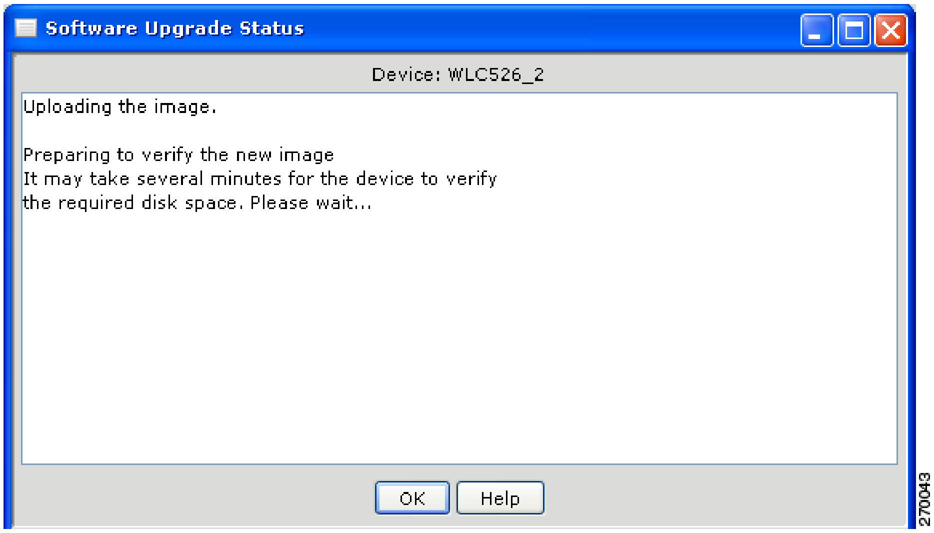
Software Upgrade

Device	Upgrade	Device Type	Current Version	New Image Name	Upgrade Status
Home					
WLC526_2	☑	AIR-WLC526-K9	4.2.37.161	as_520_4_2_37_1...	Uploading the image.
CE500_Switch	□	WS-CE500-24LC	12.2(25)FY - C...		

The upgrade status field indicates CCA is uploading the software image to the controller.

You can click **Status at any time to view status information (see** Figure 5-2).

Figure 5-6 Software Upgrade Status Information



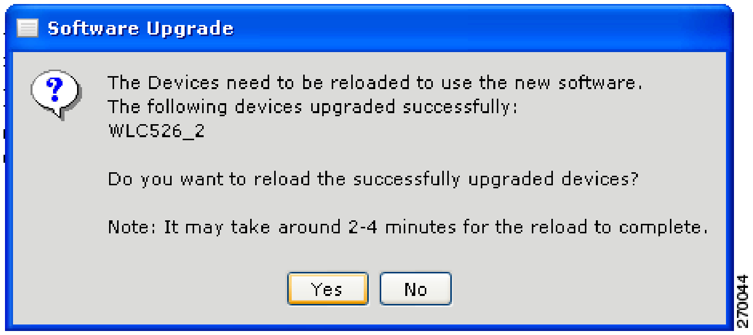
Device: WLC526_2

```
Uploading the image.

Preparing to verify the new image
It may take several minutes for the device to verify
the required disk space. Please wait...
```

When the controller software upgrade is completed, a pop-up message (Figure 5-7) appears and indicates the successful upgrade of the controller. The message indicates that the controller must be reloaded to use the new software and asks if you want to reload the software.

Figure 5-7 Software Upgrade Pop-Up Message



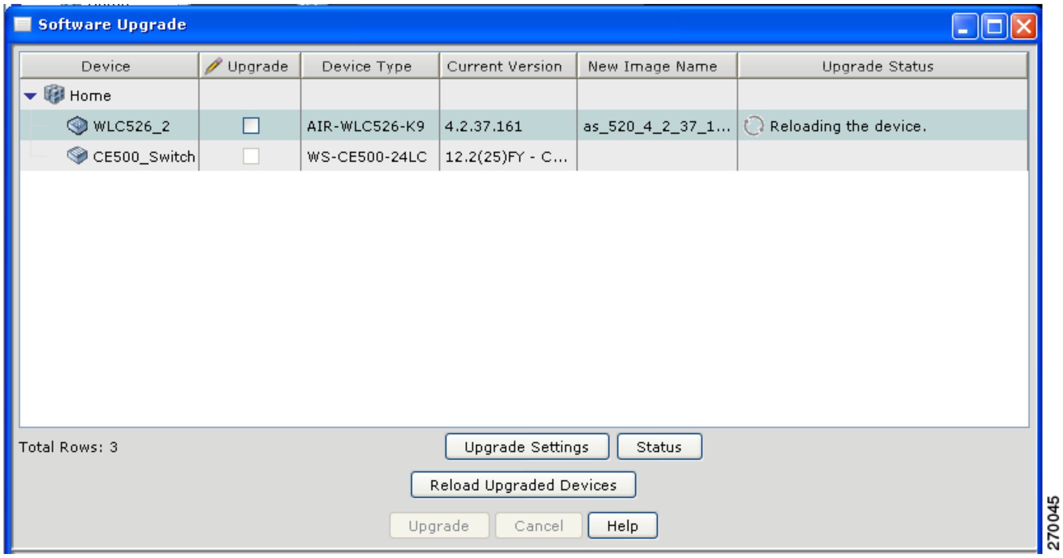
The Devices need to be reloaded to use the new software.
The following devices upgraded successfully:
WLC526_2

Do you want to reload the successfully upgraded devices?

Note: It may take around 2-4 minutes for the reload to complete.

Step 9 Click **Yes** to reload the controller and Figure 5-8 appears indicating the controller is being reloaded.

Figure 5-8 Reloading the Controller

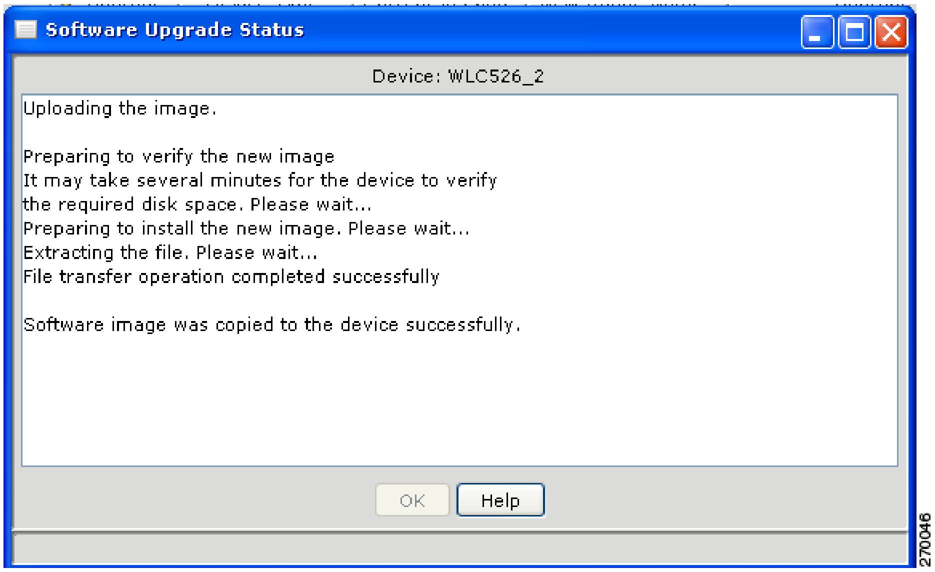


Device	Upgrade	Device Type	Current Version	New Image Name	Upgrade Status
Home					
WLC526_2	□	AIR-WLC526-K9	4.2.37.161	as_520_4_2_37_1...	Reloading the device.
CE500_Switch	□	WS-CE500-24LC	12.2(25)FY - C...		

Total Rows: 3

Step 10 If you click Status, Figure 5-9 appears and indicates the reload status.

Figure 5-9 Reload Status Information



Device: WLC526_2

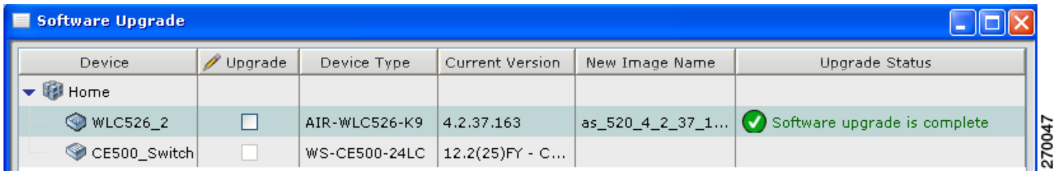
```
Uploading the image.

Preparing to verify the new image
It may take several minutes for the device to verify
the required disk space. Please wait...
Preparing to install the new image. Please wait...
Extracting the file. Please wait...
File transfer operation completed successfully

Software image was copied to the device successfully.
```

When the reload completes, Figure 5-10 appears and indicates the upgrade status is successful.

Figure 5-10 Software Upgrade Complete



Device	Upgrade	Device Type	Current Version	New Image Name	Upgrade Status
Home					
WLC526_2	□	AIR-WLC526-K9	4.2.37.163	as_520_4_2_37_1...	✓ Software upgrade is complete
CE500_Switch	□	WS-CE500-24LC	12.2(25)FY - C...		

Step 11 After reviewing the information provided in the window, close the window by clicking the red X button the top right of the window.

CHAPTER 6

Restarting, Resetting, Backing Up, and Restoring the Controller

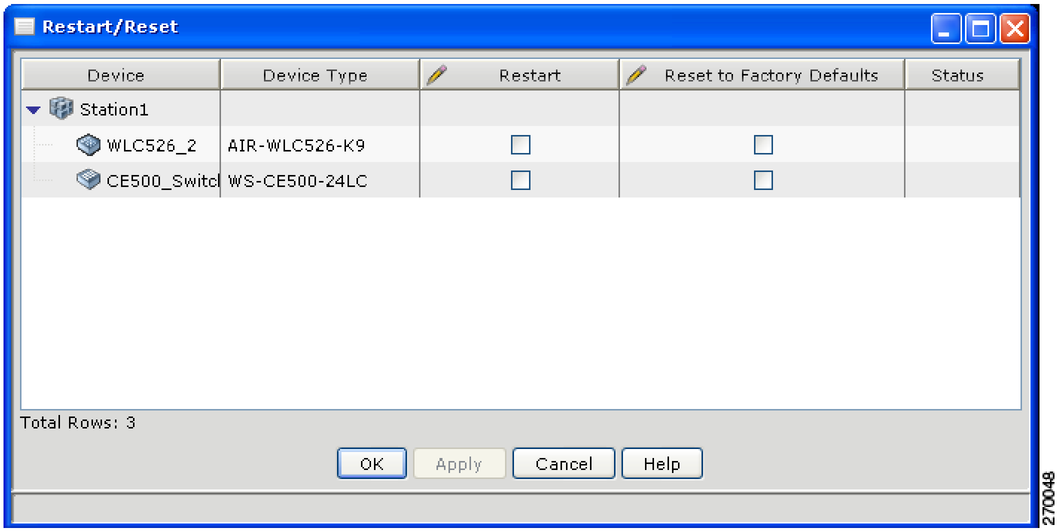
This chapter describes how to restart the controller, reset the controller to factory defaults, backup the controller configuration, and restore the controller configuration. The chapter contains these sections:

Restarting the Controller Using CCA

Follow these instructions to restart the controller using CCA:

Step 1 Click **Maintenance** > **Restart/Reset** and Figure 6-1 appears.

Figure 6-1 Restart and Reset Device Selections

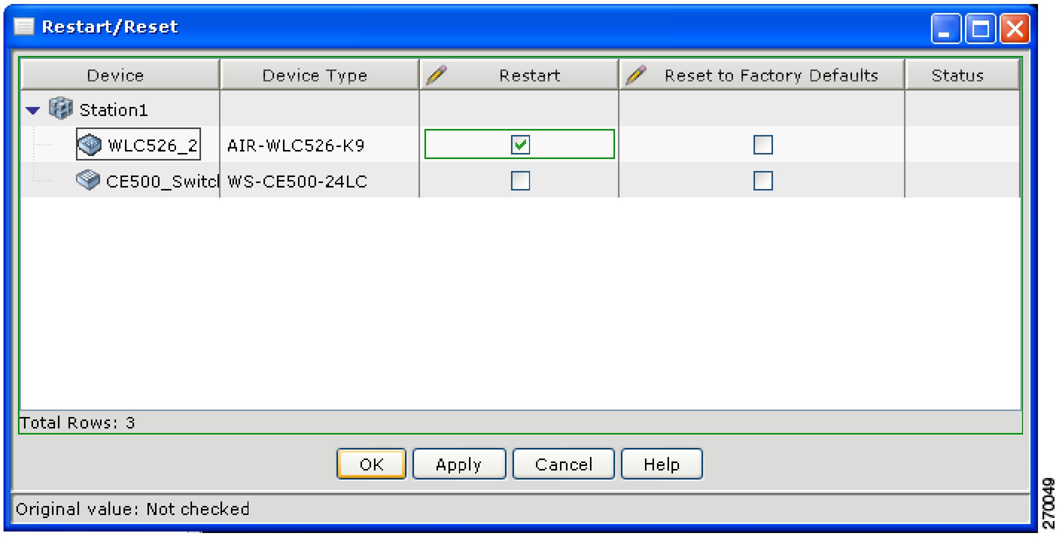


Device	Device Type	Restart	Reset to Factory Defaults	Status
Station1				
WLC526_2	AIR-WLC526-K9	□	□	
CE500_Switcl	WS-CE500-24LC	□	□	

Total Rows: 3

Step 2 For your controller, check **Restart**. Figure 6-2 appears and shows the controller restart check box has been checked.

Figure 6-2 Restart Check Box



Device	Device Type	Restart	Reset to Factory Defaults	Status
Station1				
WLC526_2	AIR-WLC526-K9	☑	□	
CE500_Switcl	WS-CE500-24LC	□	□	

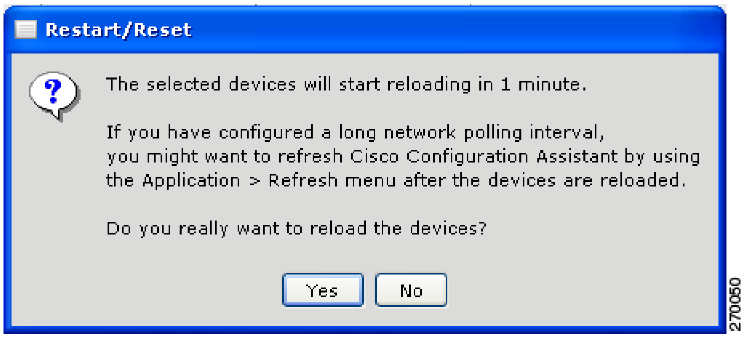
Total Rows: 3

Original value: Not checked

Step 3 If you need to restart another controller, click **Apply** and return to Step 2.

Step 4 Click **OK** and a pop-up message appears (see Figure 6-3**).** The message indicates the controller(s) will reload in approximately 1 minute. The message also indicates that you might need to refresh the CCA screen by clicking Application > Refresh after the controllers are restarted.

Figure 6-3 Reload Confirmation Pop-Up Message



Restart/Reset

The selected devices will start reloading in 1 minute.

If you have configured a long network polling interval,
you might want to refresh Cisco Configuration Assistant by using
the Application > Refresh menu after the devices are reloaded.

Do you really want to reload the devices?

Step 5 Click **Yes** to begin the reset process.

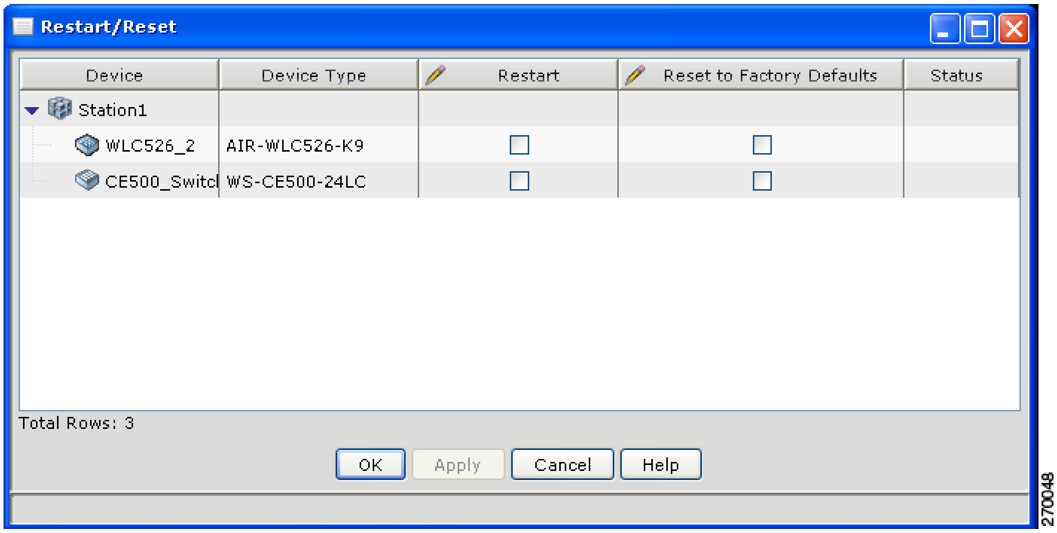
When the controller reset completes, the window closes automatically.

Resetting the Controller to Factory Default Values Using CCA

To reset the controller to factory default values using the CCA, follow these instructions:

Step 1 Click **Maintenance** > **Restart/Reset** and Figure 6-4 appears.

Figure 6-4 Restart/Reset Window



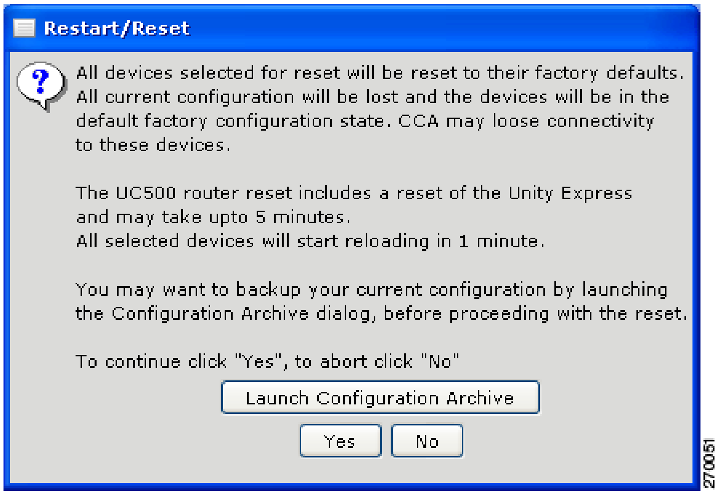
Restart/Reset

Device	Device Type	Restart	Reset to Factory Defaults	Status
Station1				
WLC526_2	AIR-WLC526-K9	□	□	
CE500_Switc	WS-CE500-24LC	□	□	

Total Rows: 3

Step 2 On the controller line, check **Reset to Factory Defaults**. Figure 6-5 appears and indicates the reset will being in approximately 1 minute for the selected devices. The message indicates CCA will loose connectivity with the controller after it has been reset to factory defaults. To reconfigure the controller, go to the "Adding a New Controller" section on page 2-2.

Figure 6-5 Restart/Reset Message



All devices selected for reset will be reset to their factory defaults. All current configuration will be lost and the devices will be in the default factory configuration state. CCA may loose connectivity to these devices.

The UC500 router reset includes a reset of the Unity Express and may take upto 5 minutes.
All selected devices will start reloading in 1 minute.

You may want to backup your current configuration by launching the Configuration Archive dialog, before proceeding with the reset.

To continue click "Yes", to abort click "No"

Step 3 If you want to backup your current controller configuration, go to the "Backing Up the Controller Configuration" section on page 6-4 for additional instructions.

Step 4 If you want to continue with the reset of the controller, click **Yes**.

When the reset process is complete, CCA returns to the main CCA screen displaying the Topology View. If you click the Refresh icon, CCA refreshes the topology view and the previously configured controller is shown not connected to the switch. CCA also detects the unconfigured controller with a default IP address of 192.168.1.1 connected to the controller. To configure the controller, go to the "Adding a New Controller" section on page 2-2.

Backing Up the Controller Configuration

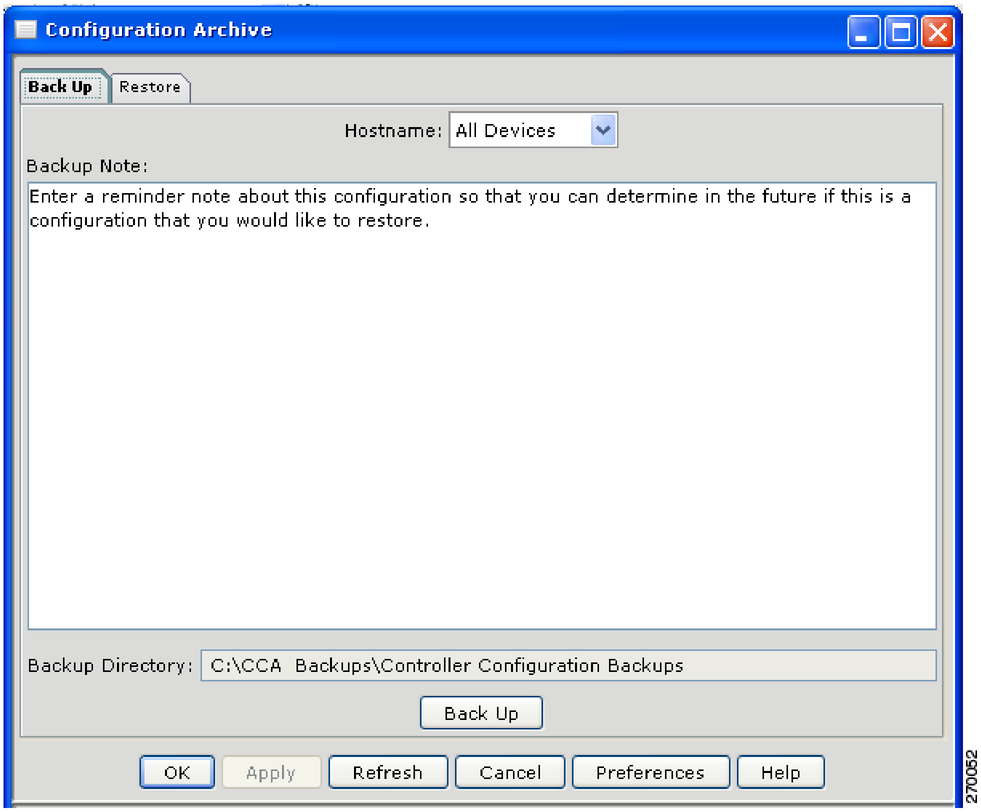
You can backup the controller configuration during the process of resetting the controller to defaults or from the Maintenance options. This section describes both methods of backing up the controller configuration.

Note On CCA Release 1.5, the CCA restore function only supports backup files created using CCA Release 1.5. You cannot use backup files created with CCA Release 1.1. CCA Release 1.1 supports binary configuration files, but CCA Release 1.5 and higher supports XML configuration files.

To back up a controller configuration, follow these steps:

Step 1 Click **Launch Configuration Archive** from the Restart/Reset pop-up message window or click **Maintenance** > **Configuration Archive**. Figure 6-6 appears.

Figure 6-6 Configuration Archive Backup Option



Hostname: All Devices

Backup Note: Enter a reminder note about this configuration so that you can determine in the future if this is a configuration that you would like to restore.

Backup Directory: C:\CCA Backups\Controller Configuration Backups

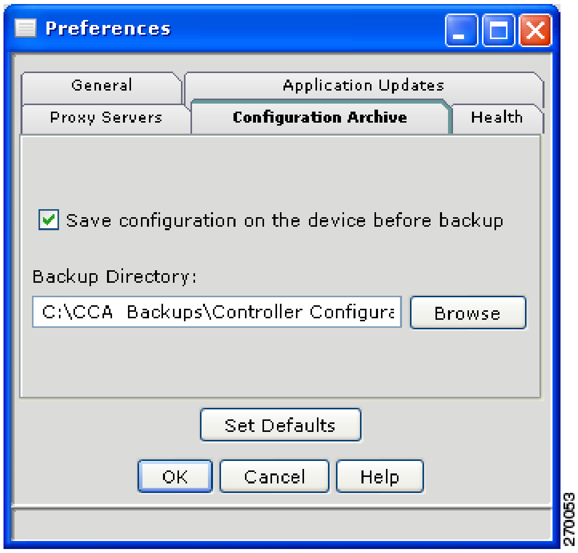
Step 2 Click the drop-down arrow in the Hostname field and choose the controller that you want to backup the configuration.

Step 3 Enter a backup description about the controller and the configuration that you are backing up in the Backup Note field.

Step 4 If you want to change the Backup Directory location, follow these steps:

a. click **Preferences** and the Preferences Window appears (see Figure 6-7).

Figure 6-7 Preferences Window



☑ Save configuration on the device before backup

Backup Directory:

C:\CCA Backups\Controller Configur

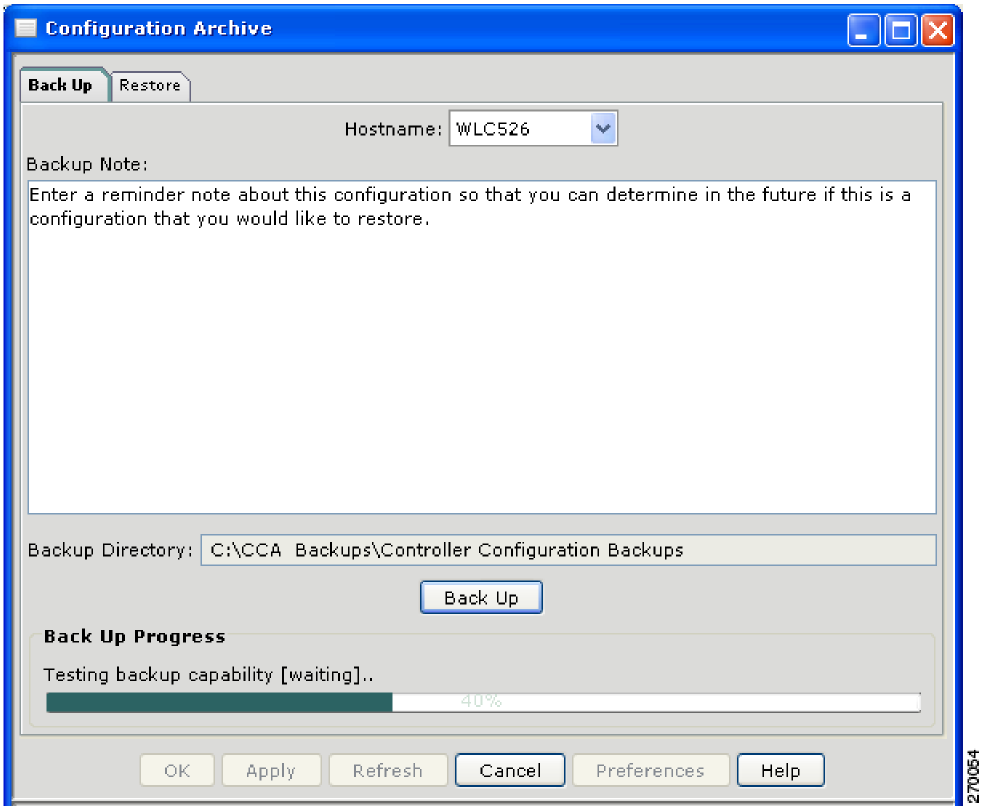
b. Click **Browse**. The Select Folder window appears.

c. Navigate to the desired backup directory folder on your hard drive and click **Select**.

d. Click **Ok** on the Preferences window.

Step 5 When the Configuration Archive window reappears, click **Backup** and Figure 6-8 appears. A backup progress bar appears indicating the progress of the backup.

Figure 6-8 Backup Progress

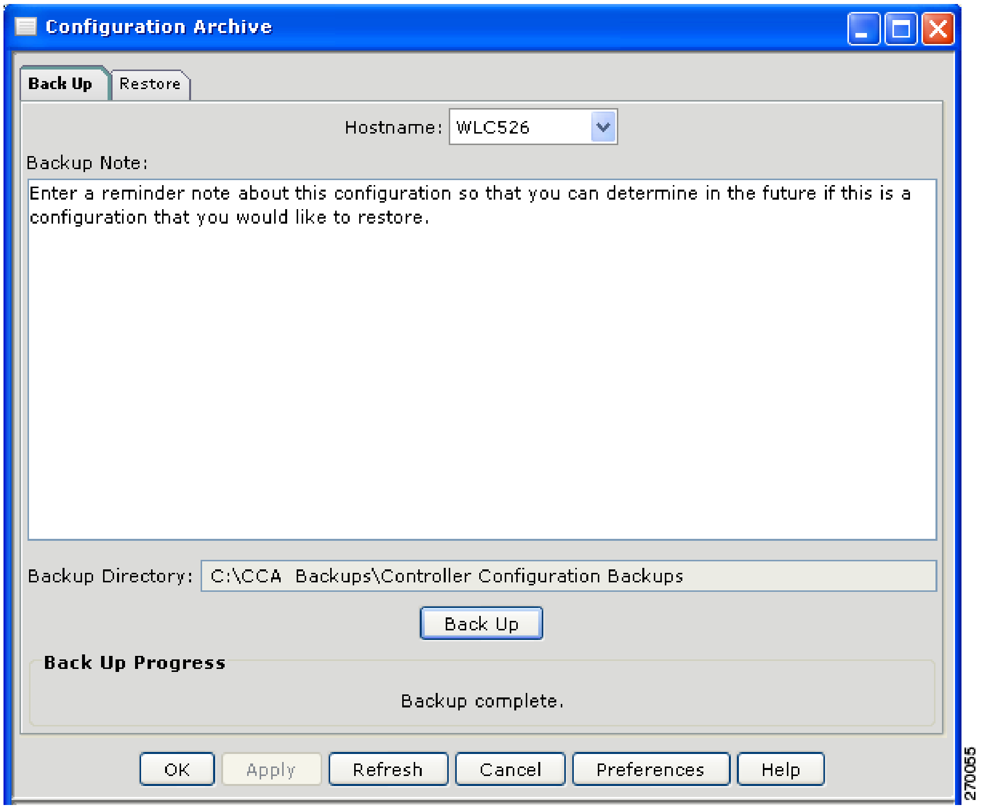


Enter a reminder note about this configuration so that you can determine in the future if this is a configuration that you would like to restore.

Testing backup capability [waiting]..

A backup complete message appears when the backup is complete (see Figure 6-9).

Figure 6-9 Backup Complete Message



Hostname: WLC526

Backup Note:

Enter a reminder note about this configuration so that you can determine in the future if this is a configuration that you would like to restore.

Backup Directory: C:\CCA Backups\Controller Configuration Backups

Backup complete.

Step 6 Click **OK**.

Step 7 If you started the backup process by clicking the Launch Configuration Archive button, the Restart/Reset window reappears. To continue resetting the controller to factory defaults, go to Step 4 of the reset process.

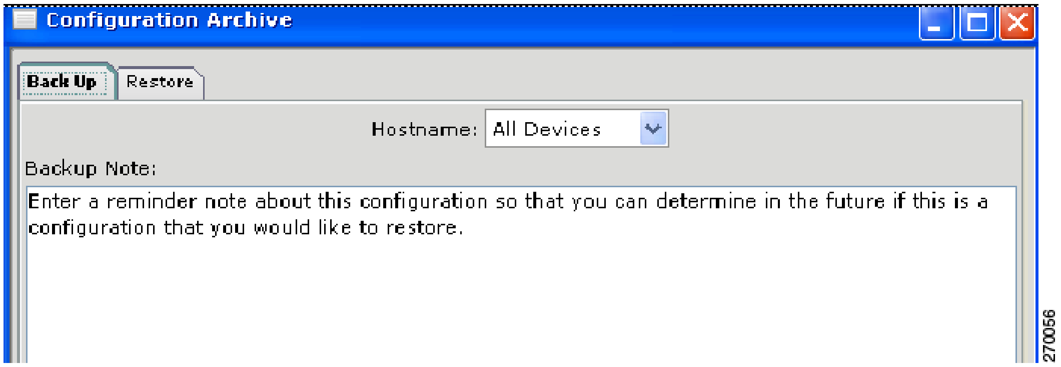
Restoring the Controller Configuration

To restore a previously backed up controller configuration, follow these steps:

Note On CCA Release 1.5, the CCA restore function only supports backup files created using CCA Release 1.5. You cannot use backup files created with CCA Release 1.1. CCA Release 1.1 supports binary configuration files, but CCA Release 1.5 and higher supports XML configuration files.

Step 1 Click **Maintenance** > **Configuration Archive** and Figure 6-10 appears.

Figure 6-10 Configuration Archive Window



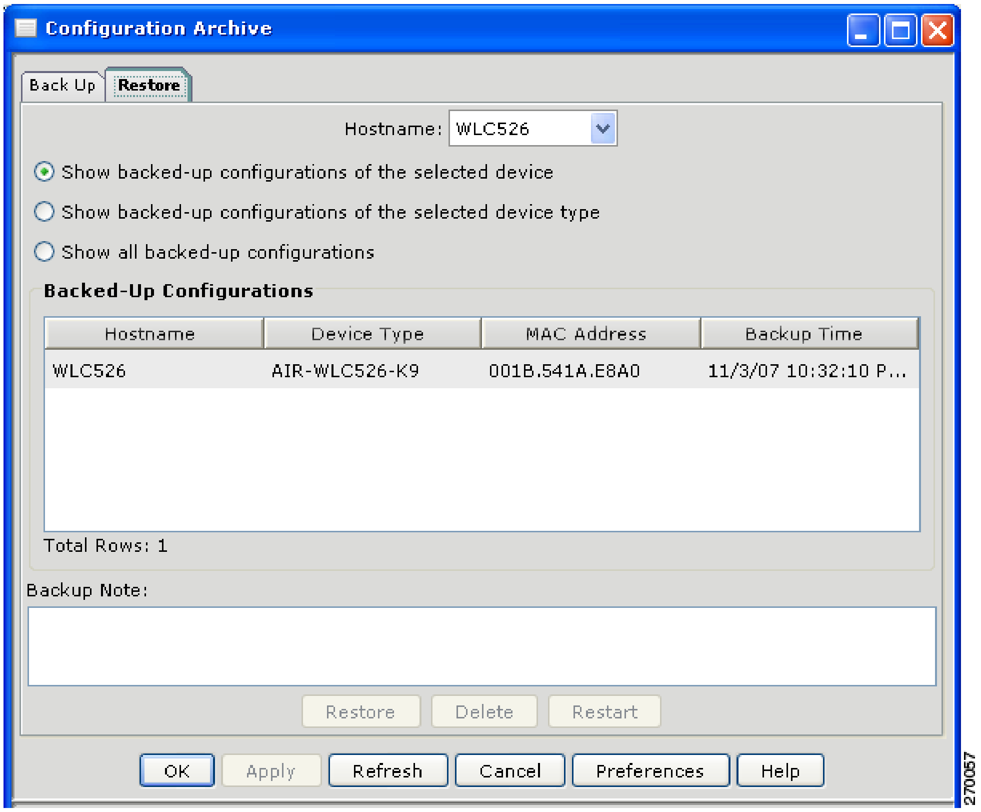
Hostname: All Devices

Backup Note:

Enter a reminder note about this configuration so that you can determine in the future if this is a configuration that you would like to restore.

Step 2 Click the **Restore tab** and Figure 6-11 appears.

Figure 6-11 Restore Window



Hostname: WLC526

● Show backed-up configurations of the selected device

○ Show backed-up configurations of the selected device type

○ Show all backed-up configurations

Backed-Up Configurations

Hostname	Device Type	MAC Address	Backup Time
WLC526	AIR-WLC526-K9	001B.541A.E8A0	11/3/07 10:32:10 P...

Total Rows: 1

Backup Note:

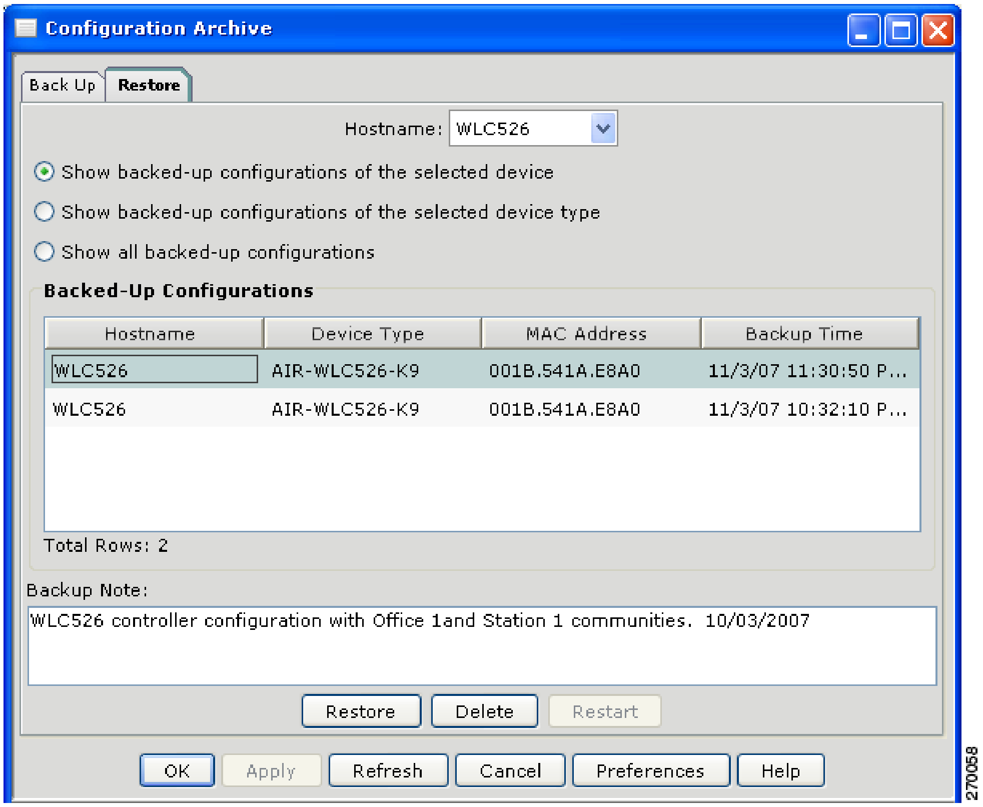
Step 3 Click the drop-down arrow in the Hostname field and choose your controller from the list.

Step 4 Choose one of these backup options:

- **Show backed-up configurations of the selected device**—displays only the backed-up configurations for the controller you selected.
- **Show backed-up configurations of the selected device type**—displays all the backed-up configurations for all controllers in your community.
- **Show all backed-up configurations**—displays all the backed-up configurations in the backup directory.

Figure 6-12 appears.

Figure 6-12 Restore Window with the Chosen Selection



Configuration Archive

Hostname: WLC526

● Show backed-up configurations of the selected device

○ Show backed-up configurations of the selected device type

○ Show all backed-up configurations

Backed-Up Configurations

Hostname	Device Type	MAC Address	Backup Time
WLC526	AIR-WLC526-K9	001B.541A.E8A0	11/3/07 11:30:50 P...
WLC526	AIR-WLC526-K9	001B.541A.E8A0	11/3/07 10:32:10 P...

Total Rows: 2

Backup Note:

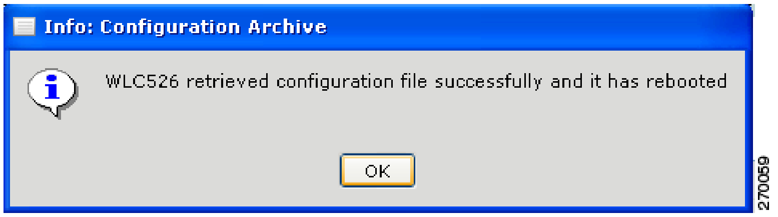
WLC526 controller configuration with Office 1and Station 1 communities. 10/03/2007

Step 5 Choose one of the listed backup-configurations by clicking the controller's hostname. Review the backup note field for information about the backup configuration.

Step 6 Click **Restore** and a progress bar appears indicating the restore progress. A description above the restore progress bar indicates the controller being restored. This will take a few minutes to complete.

When the restoration is complete, a pop-up message appears (see Figure 6-13) and indicates the controller was successfully restored and has been rebooted.

Figure 6-13 Configuration Archive Pop-Up Message



Info: Configuration Archive

WLC526 retrieved configuration file successfully and it has rebooted

Step 7 Click **OK on the pop-up message**.

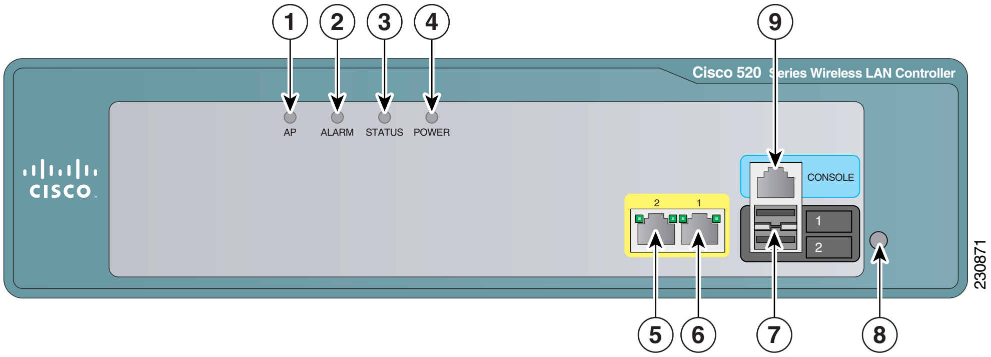
Step 8 If you need to restore another controller, repeat Steps 3 to 7.

Step 9 When you are finished restoring controller configurations, click **OK on the Configuration Archive window**.

Manually Restarting the Controller Using the Reset Button

The Reset button on the controller's front panel becomes active after the controller boots. You can use the Reset button to reset power or to reset the configuration to factory defaults.

Figure 6-14 WLC526 Front Panel



1	AP LED	**6**	Distribution port 1
2	Alarm LED	**7**	USB ports (not used)
3	Status LED	**8**	Reset button
4	Power LED	**9**	Console port
5	Distribution port 2		

To restart the controller using the Reset button, follow these instructions:

Step 1 Place a straightened paper clip into the **Reset** button hole (see Figure 6-14).

Step 2 While observing the controller LEDs, gently push and hold the **Reset** button with the paper clip.

Step 3 When the Status LED turn amber, release the **Reset** button by removing the paper clip.

Step 4 The controller configuration settings are not reset. If you have configured the controller, it reboots and loads the active configuration. If you have not configured the controller, the startup wizard GUI appears.

Manually Resetting the Controller to Factory Defaults

To reset the controller to factory defaults using the Reset button, follow these instructions:

Step 1 Place a straightened paper clip into the **Reset** button hole (see Figure 6-14).

Step 2 While observing the controller LEDs, gently push and hold the **Reset** button with the paper clip.

Step 3 When the Alarm LED turns green, release the **Reset** button by removing the paper clip.

Step 4 The controller power cycles and reboots. The controller configuration settings are reset to factory defaults and the startup wizard GUI appears.

CHAPTER 7

Adding Guest Access with Web Authentication

This chapter describes how to add guest access with web authentication and contains these sections:

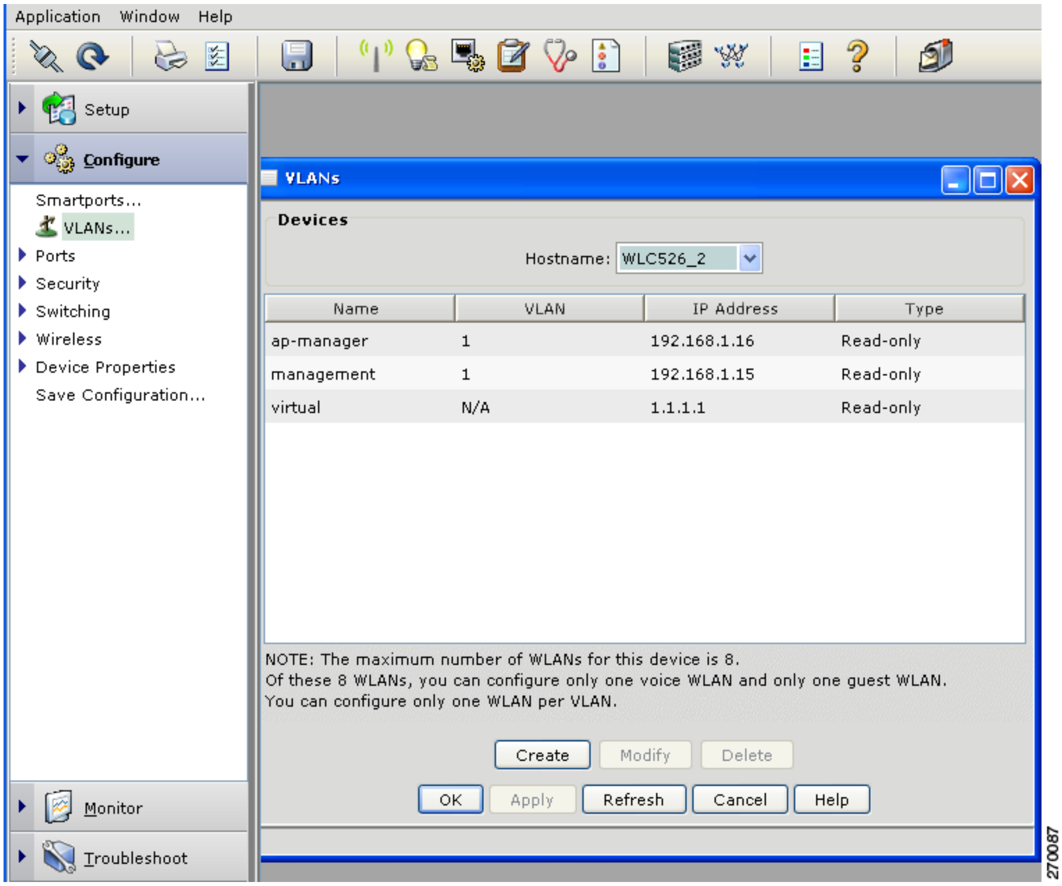
- Adding a Guest Access VLAN, page 7-1
- Creating a New SSID for the Guest VLAN, page 7-6
- Adding a Guest User, page 7-9

Adding a Guest Access VLAN

To add a guest access VLAN, follow these steps:

Step 1 Click **Configure** > **VLANs** and Figure 7-1 appears.

Figure 7-1 VLAN Window



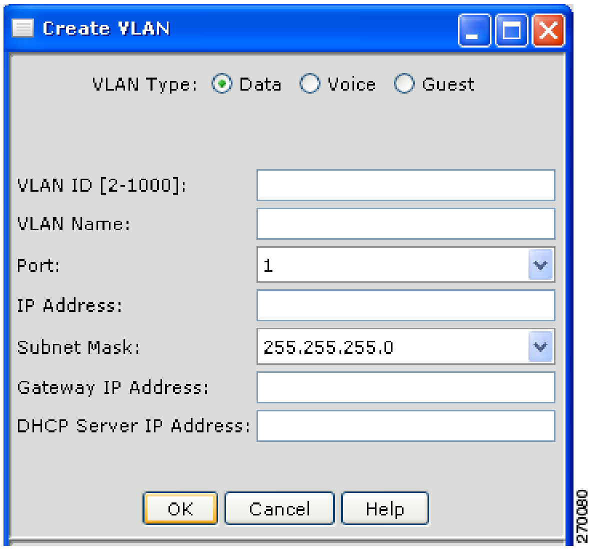
Hostname: WLC526_2

Name	VLAN	IP Address	Type
ap-manager	1	192.168.1.16	Read-only
management	1	192.168.1.15	Read-only
virtual	N/A	1.1.1.1	Read-only

NOTE: The maximum number of WLANs for this device is 8.
Of these 8 WLANs, you can configure only one voice WLAN and only one guest WLAN.
You can configure only one WLAN per VLAN.

Click **Create** and Figure 7-2 appears.

Figure 7-2 Create VLAN Window



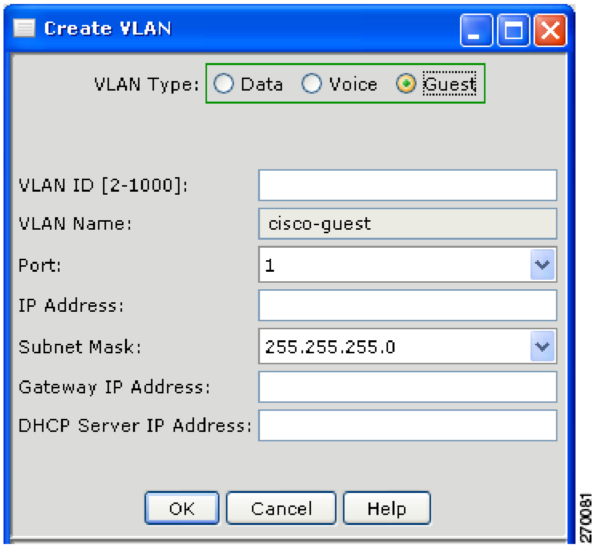
VLAN Type: ● Data ○ Voice ○ Guest

VLAN ID [2-1000]:	
VLAN Name:	
Port:	1
IP Address:	
Subnet Mask:	255.255.255.0
Gateway IP Address:	
DHCP Server IP Address:	

Step 2 Click **Guest** for a guest VLAN and Figure 7-3 appears.

> **Note** For a Guest VLAN type, the VLAN name field is set with a predefined VLAN name (*cisco-guest*) and cannot be changed.

Figure 7-3 Create Guest VLAN Window



Create VLAN

VLAN Type: ○ Data ○ Voice ● Guest

VLAN ID [2-1000]:

VLAN Name: cisco-guest

Port: 1

IP Address:

Subnet Mask: 255.255.255.0

Gateway IP Address:

DHCP Server IP Address:

Step 3 Perform these steps:

a. In the VLAN ID field, enter the VLAN ID that you want to associate with the guest VLAN. Use an ID in the range 2 to 1000. Do not enter 1; this ID is reserved.

> **Note** For Guest VLAN types, the VLAN name field is set with a predefined VLAN name that is based on the selected VLAN type. It cannot be changed.

b. From the Port list, select a port (1 or 2) for the VLAN. The default is 1.

c. In the IP Address field, enter an IP address for the VLAN.

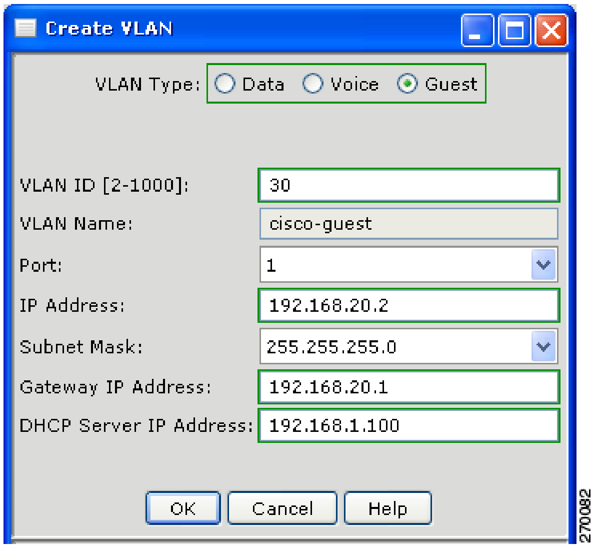
d. From the Subnet Mask list, accept the default or click the drop-down arrow and choose the subnet mask for the VLAN. The default is 255.255.255.0.

e. In the Gateway IP Address field, enter the IP address of the default gateway.

f. In the DHCP Server IP Address field, enter the IP address of the DHCP server.

g. When you complete this window (see Figure 7-4), click **OK** to save your changes and to close the window.

Figure 7-4 Typical Guest VLAN Data



VLAN Type: ○ Data ○ Voice ● Guest

VLAN ID [2-1000]: 30

VLAN Name: cisco-guest

Port: 1

IP Address: 192.168.20.2

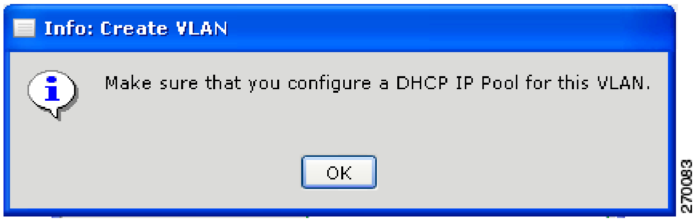
Subnet Mask: 255.255.255.0

Gateway IP Address: 192.168.20.1

DHCP Server IP Address: 192.168.1.100

A create VLAN pop-up message (Figure 7-5) appears.

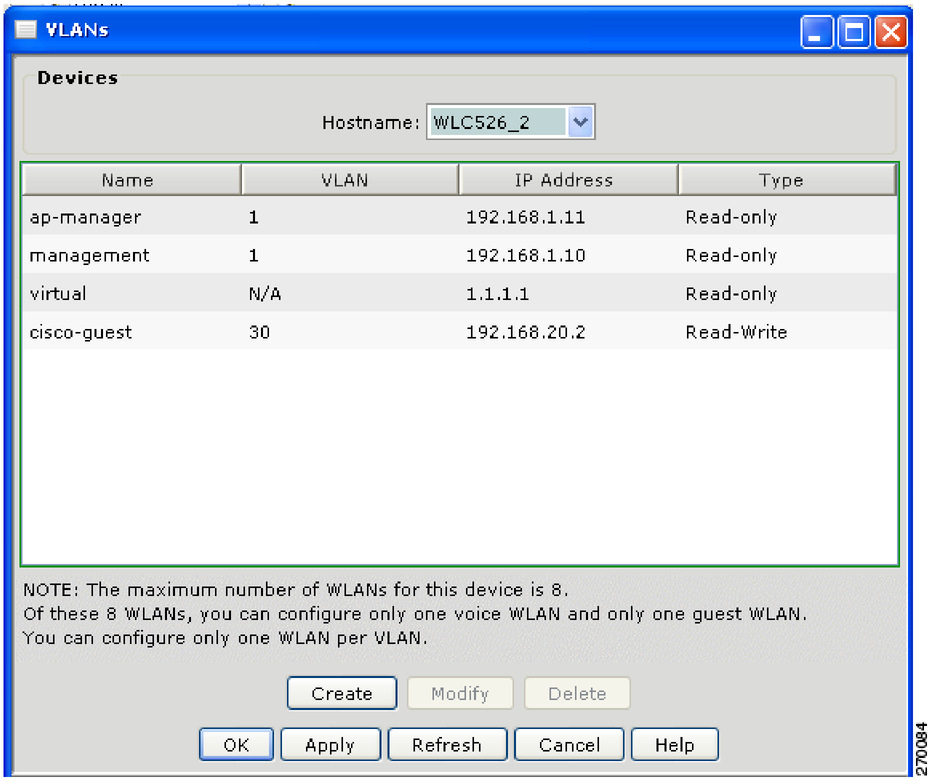
Figure 7-5 Create VLAN Pop-Up Message



Make sure that you configure a DHCP IP Pool for this VLAN.

Step 4 Click **OK** and Figure 7-6 appears and lists the new guest VLAN.

Figure 7-6 VLANs Window with Guest VLAN Added



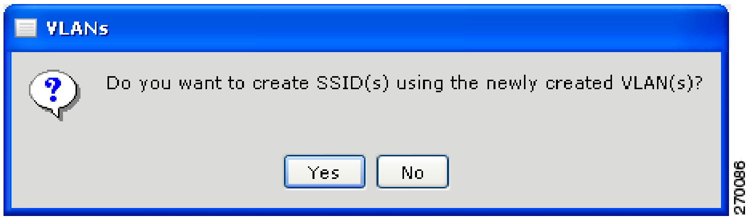
Hostname: WLC526_2

Name	VLAN	IP Address	Type
ap-manager	1	192.168.1.11	Read-only
management	1	192.168.1.10	Read-only
virtual	N/A	1.1.1.1	Read-only
cisco-guest	30	192.168.20.2	Read-Write

NOTE: The maximum number of WLANs for this device is 8.
Of these 8 WLANs, you can configure only one voice WLAN and only one guest WLAN.
You can configure only one WLAN per VLAN.

Step 5 Click **OK** and a VLANs pop-up message appears (Figure 7-7) asking if you want to create an SSID using the new VLAN.

Figure 7-7 VLANs Pop-UP SSID Message



Do you want to create SSID(s) using the newly created VLAN(s)?

Step 6 Click **Yes** to create an SSID for the guest VLAN and Figure 7-8 appears. Go to Step 1.

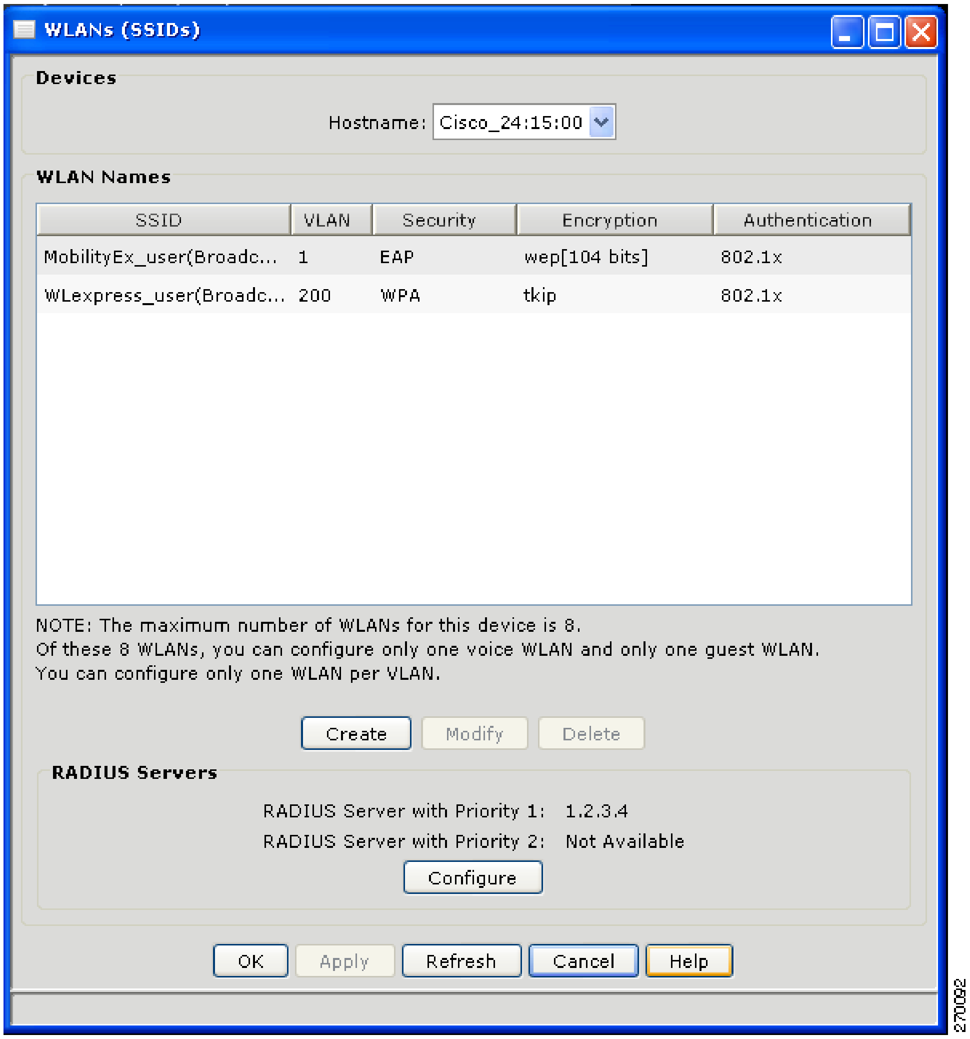
Creating a New SSID for the Guest VLAN

To create a new SSID for the guest VLAN, follow these instructions:

Step 1 Figure 7-8 appears after clicking Yes on the VLANs pop-up SSID message (see Figure 7-7).

Note You can also click **Wireless** > **WLAN (SSIDs)** to add a guest WLAN SSID and Figure 7-8 appears.

Figure 7-8 WLAN (SSIDs) Window



WLANs (SSIDs)

Devices

Hostname: Cisco_24:15:00

WLAN Names

SSID	VLAN	Security	Encryption	Authentication
MobilityEx_user(Broadc...	1	EAP	wep[104 bits]	802.1x
WLexpress_user(Broadc...	200	WPA	tkip	802.1x

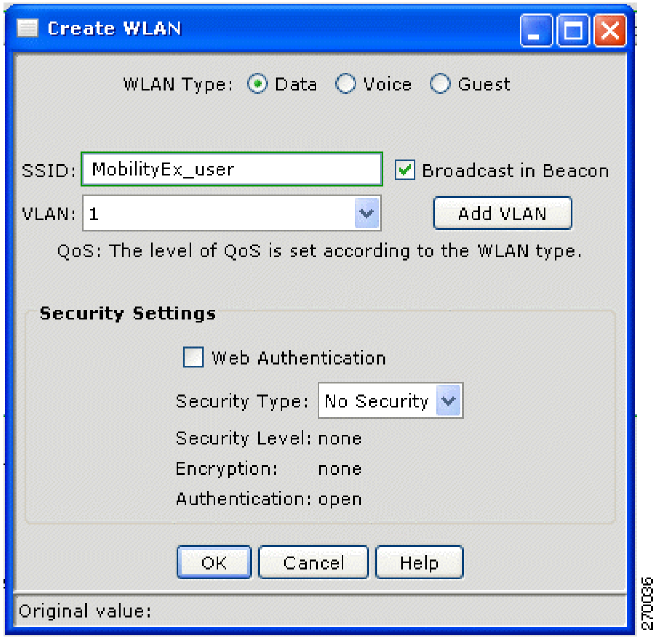
NOTE: The maximum number of WLANs for this device is 8.
Of these 8 WLANs, you can configure only one voice WLAN and only one guest WLAN.
You can configure only one WLAN per VLAN.

RADIUS Servers

RADIUS Server with Priority 1: 1.2.3.4
RADIUS Server with Priority 2: Not Available

Step 2 Click **Create** to create a new WLAN and Figure 7-9 appears.

Figure 7-9 Create WLAN Window



Create WLAN

WLAN Type: ● Data ○ Voice ○ Guest

SSID: MobilityEx_user ☑ Broadcast in Beacon

VLAN: 1 Add VLAN

QoS: The level of QoS is set according to the WLAN type.

Security Settings

□ Web Authentication

Security Type: No Security

Security Level: none

Encryption: none

Authentication: open

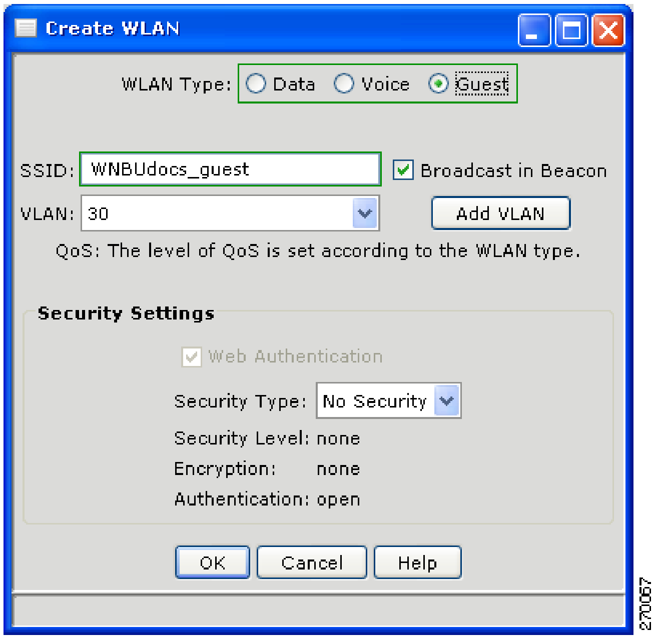
OK Cancel Help

Original value:

Use the window to create a new SSID and to specify the security settings.

Step 3 Click **Guest** to create a guest WLAN and Figure 7-10 appears.

Figure 7-10 Create Guest WLAN Window



Create WLAN

WLAN Type: ○ Data ○ Voice ● Guest

SSID: WNBUdocs_guest ☑ Broadcast in Beacon

VLAN: 30 Add VLAN

QoS: The level of QoS is set according to the WLAN type.

Security Settings

☑ Web Authentication

Security Type: No Security

Security Level: none

Encryption: none

Authentication: open

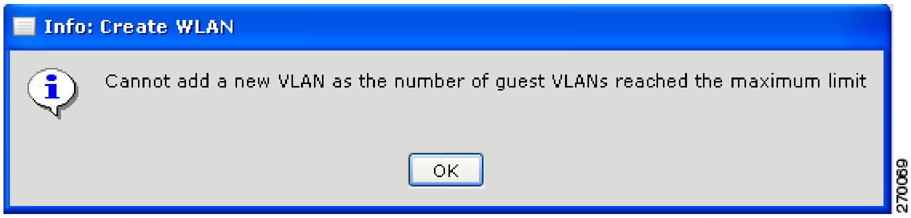
OK Cancel Help

On a guest WLAN, these options are automatically configured and cannot be changed:

- The default guest VLAN selected. Only one guest VLAN can be created.

- If you click the Add VLAN button, Figure 7-11 appears indicating the maximum number of VLANs has been reached.

Figure 7-11 Add VLAN Pop-Up Message



Info: Create WLAN

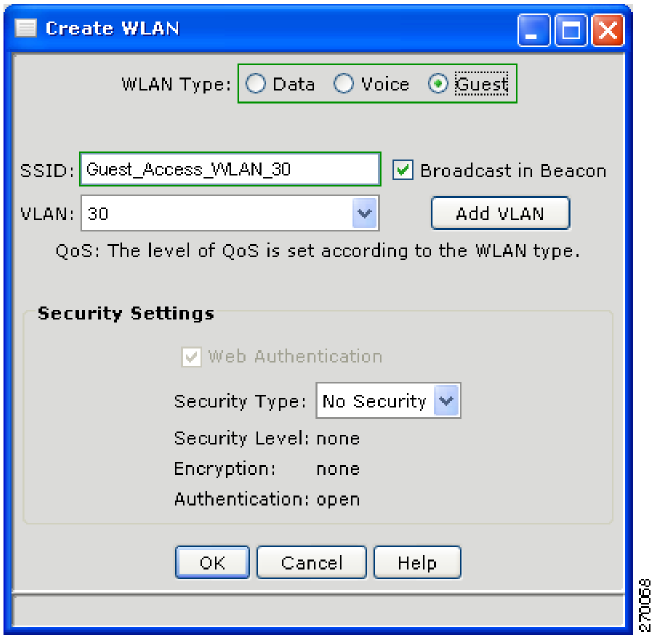
Cannot add a new VLAN as the number of guest VLANs reached the maximum limit

- Web Authentication is selected.
- The Security Type field is automatically set to No Security.
- No encryption is configured.
- Open authentication is configured.

Step 4 Perform these steps:

a. Accept the default guest WLAN SSID or enter a new SSID (see Figure 7-12). The SSID can be up to 32 alphanumeric characters.

Figure 7-12 New Guest SSID Configured



Create WLAN

WLAN Type: ○ Data ○ Voice ● Guest

SSID: Guest_Access_WLAN_30 ☑ Broadcast in Beacon

VLAN: 30

QoS: The level of QoS is set according to the WLAN type.

Security Settings

☑ Web Authentication

Security Type: No Security

Security Level: none

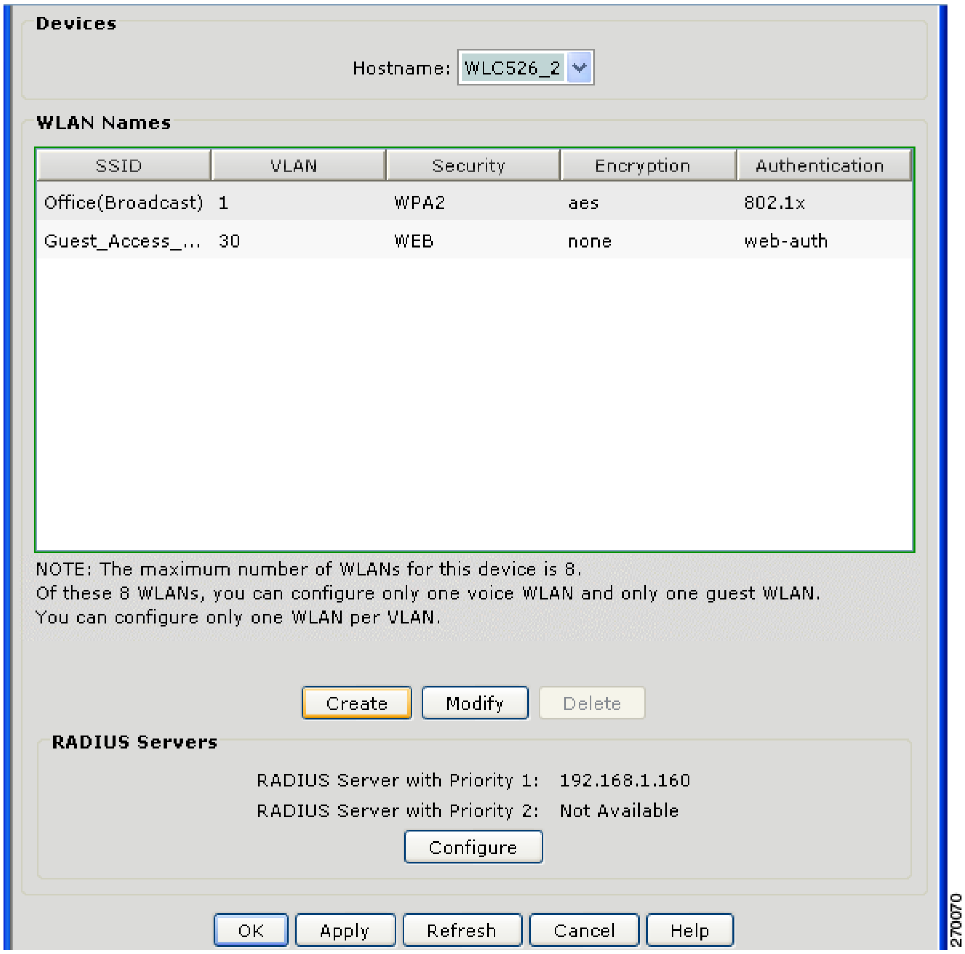
Encryption: none

Authentication: open

b. Accept or uncheck the default Broadcast in Beacon setting. When checked, the guest WLAN SSID is broadcast in beacon messages so that the devices that do not specify an SSID can associate (establish a wireless connection) with the access point. Only the guest SSID can be included in the beacon.

c. When finished, click **OK** and WLANs Window (Figure 7-13) reappears with the new guest WLAN added.

Figure 7-13 WLANs Window with New Guest WLAN



Devices

Hostname: WLC526_2

WLAN Names

SSID	VLAN	Security	Encryption	Authentication
Office(Broadcast)	1	WPA2	aes	802.1x
Guest_Access_...	30	WEB	none	web-auth

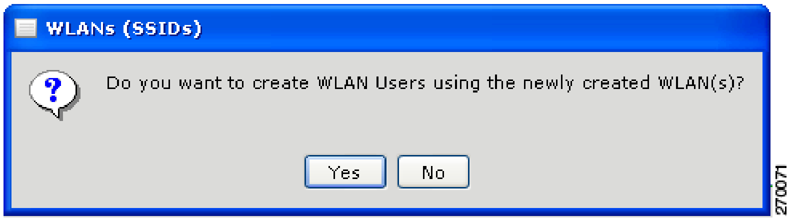
NOTE: The maximum number of WLANs for this device is 8.
Of these 8 WLANs, you can configure only one voice WLAN and only one guest WLAN.
You can configure only one WLAN per VLAN.

RADIUS Servers

RADIUS Server with Priority 1: 192.168.1.160
RADIUS Server with Priority 2: Not Available

Step 5 Click **OK** and a pop-up message (Figure 7-14) appears asking if you want to create WLAN users for the new WLAN.

Figure 7-14 WLAN Pop-Up Message



WLANs (SSIDs)

Do you want to create WLAN Users using the newly created WLAN(s)?

Step 6 Click **Yes** to add new guest users and Figure 7-15 appears. Go to Step 1.

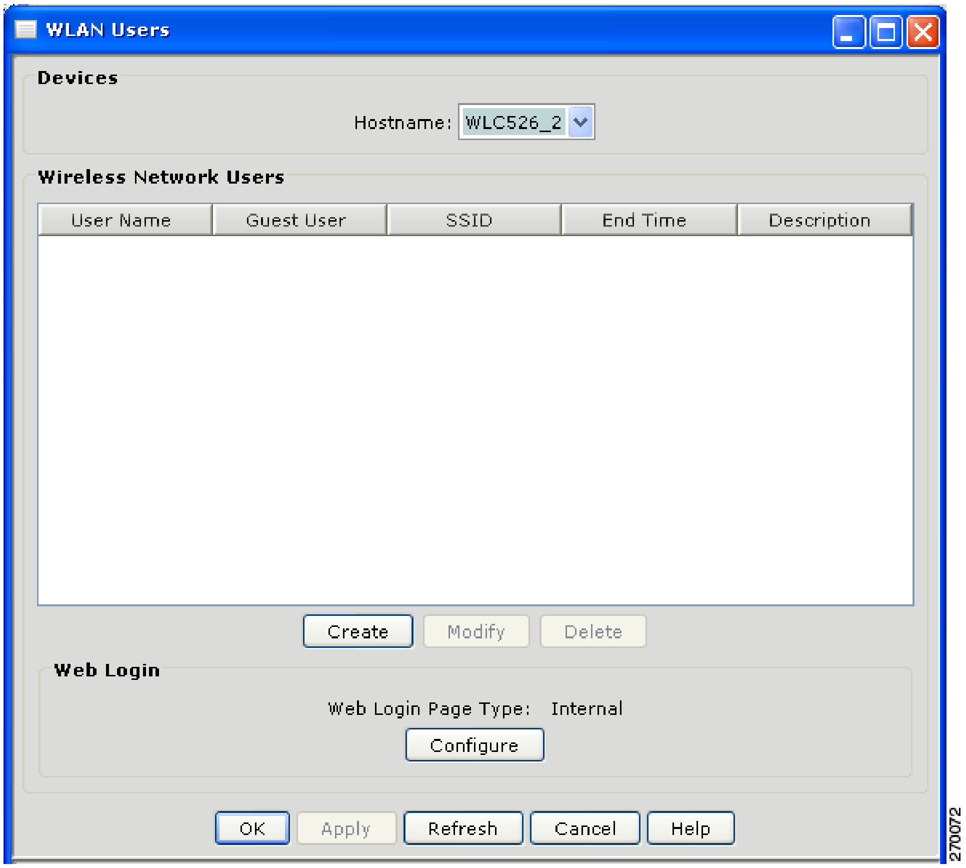
Adding a Guest User

To add a guest user, follow these instructions:

Step 1 Figure 7-15 appears after clicking Yes on the WLAN (SSIDs) pop-up message (see Figure 7-14).

Note You can also click **Wireless** > **WLAN Users** to add guest users and Figure 7-15 appears.

Figure 7-15 WLAN Users Window



WLAN Users

Devices

Hostname: WLC526_2

Wireless Network Users

User Name	Guest User	SSID	End Time	Description

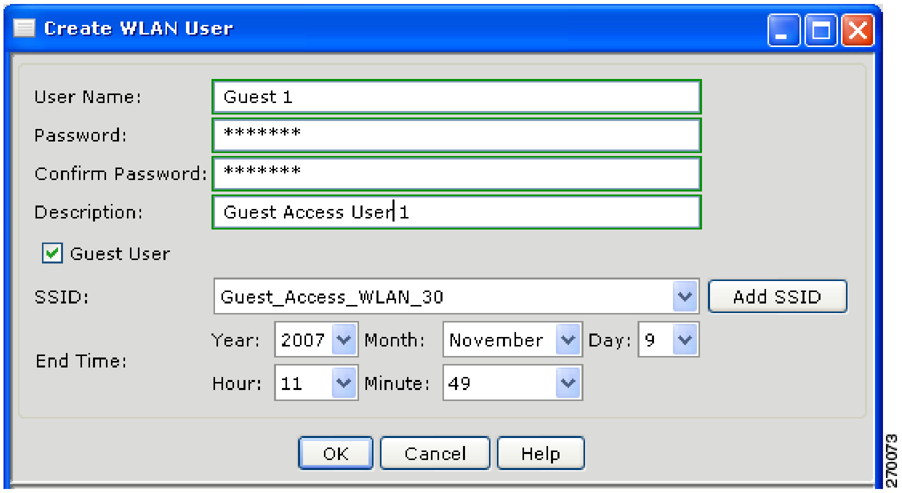
Web Login

Web Login Page Type: Internal

Step 2 Click the drop-down arrow in the Hostname field and choose your controller.

Step 3 Click **Create** and Figure 7-16 appears.

Figure 7-16 Create WLAN User Window



Create WLAN User

User Name: Guest 1

Password: *******

Confirm Password: *******

Description: Guest Access User 1

☑ Guest User

SSID: Guest_Access_WLAN_30

End Time: Year: 2007 Month: November Day: 9 Hour: 11 Minute: 49

Step 4 Perform these steps:

a. Enter a user name (up to 49 alphanumeric characters) in the User Name field.

b. Enter a password (up to 24 alphanumeric characters) in the Password field.

c. Reenter the password in the Confirm Password field.

d. Enter a description of the user in the Description field.

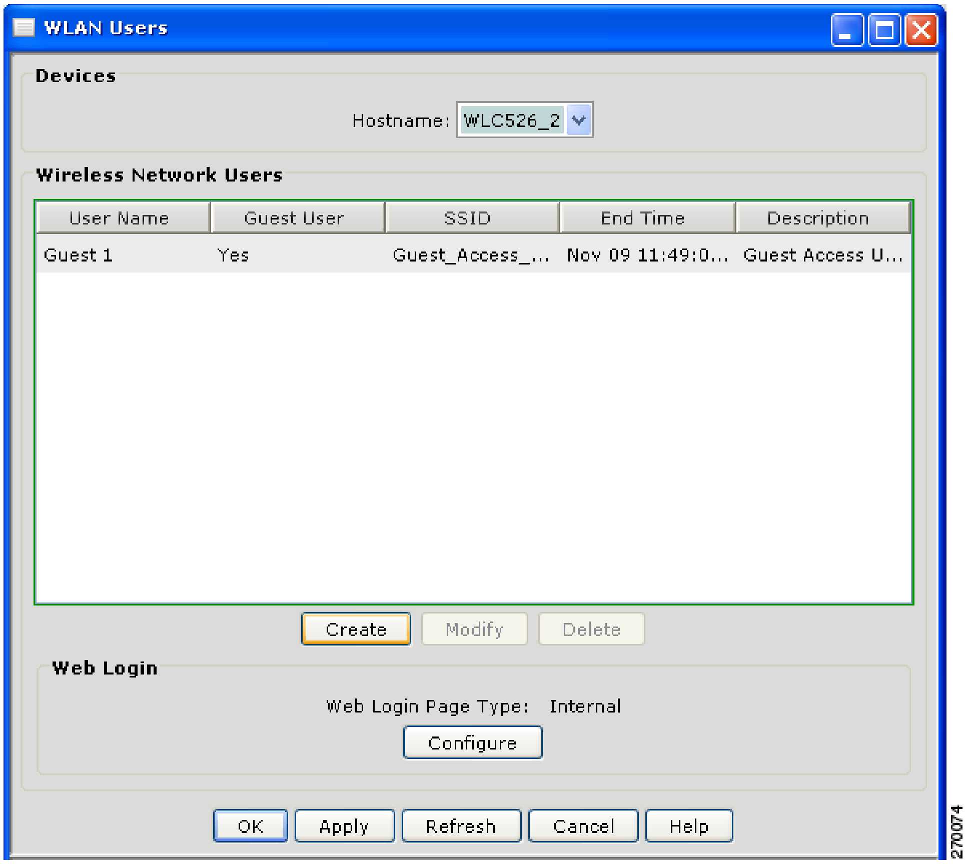
e. Ensure Guest User is checked.

Note For guest accounts, the SSID cannot be changed. If there is a guest SSID already present and if you click the Add SSID button, a pop-up SSID message appears and indicates that you cannot add a new SSID.

f. Accept the default values for the End Time or change the values.

g. When complete, click **OK** and Figure 7-17 appears.

Figure 7-17 New Guest User



WLAN Users

Devices

Hostname: WLC526_2

Wireless Network Users

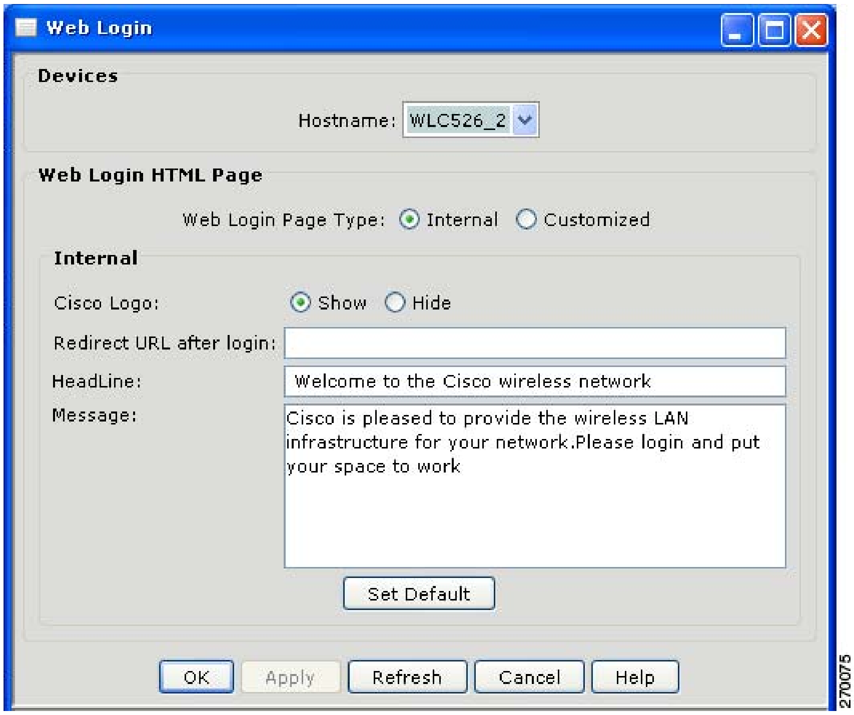
User Name	Guest User	SSID	End Time	Description
Guest 1	Yes	Guest_Access_...	Nov 09 11:49:0...	Guest Access U...

Web Login

Web Login Page Type: Internal

Step 5 Click **Configure** to configure the web login page and Figure 7-18 appears.

Figure 7-18 Web Login Window



Devices

Hostname: WLC526_2

Web Login HTML Page

Web Login Page Type: ● Internal ○ Customized

Internal

Cisco Logo: ● Show ○ Hide

Redirect URL after login:

HeadLine: Welcome to the Cisco wireless network

Message: Cisco is pleased to provide the wireless LAN infrastructure for your network.Please login and put your space to work

Step 6 Click the drop-down arrow in the Hostname field and choose your controller.

Step 7 Check **Internal** or **Customized** in the Web Login Page Type field.

Step 8 If you checked Internal, perform these steps:

a. Check **Show** to display the Cisco logo or check **Hide to hide the** Cisco logo.

b. In the Redirect URL after Login field, enter a URL to which the user will be redirected after logging in. The URL format is *www.companyname.com* and can contain up to 254 characters.

c. In the Headline field, enter the login page headline or summary, up to 127 characters. The default is *Welcome to the Cisco wireless network*.

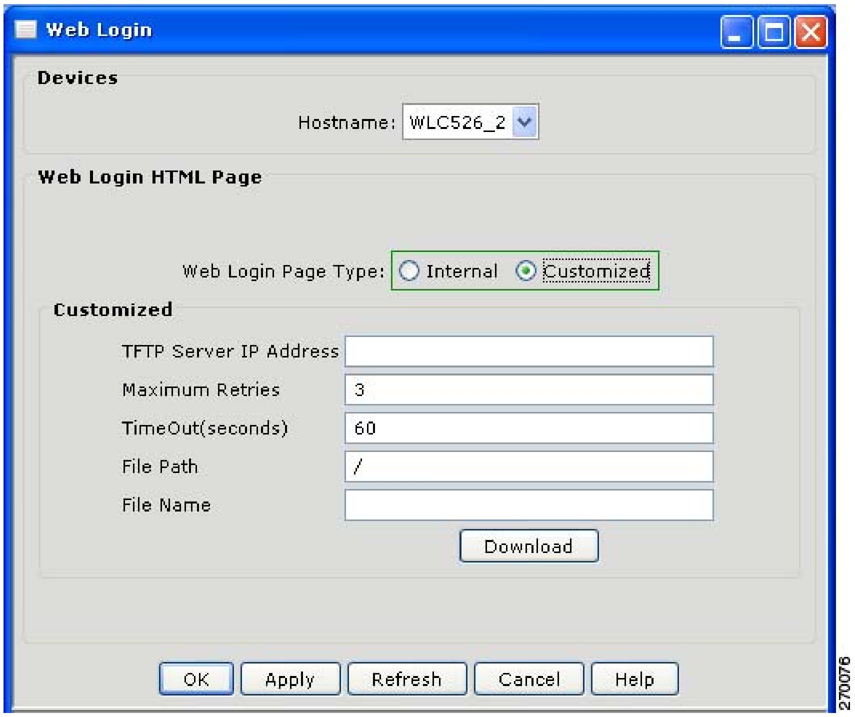
d. In the message field, enter the message text up to 2047 characters. The default message is shown in Figure 7-18.

e. Click **Set Default** to use the default settings.

f. When complete, click **OK and a** web login pop-up message appears (see Figure 7-20). Go to Step 10.

Step 9 If you checked Customized, Figure 7-19 appears.

Figure 7-19 Web Login Customized Window



Web Login

Devices

Hostname: WLC526_2

Web Login HTML Page

Web Login Page Type: ○ Internal ● Customized

Customized

TFTP Server IP Address

Maximum Retries 3

TimeOut(seconds) 60

File Path /

File Name

Perform these steps:

a. In the TFTP Server IP Address field, enter the IP address of the TFTP server where the customized Web authentication bundle file exists.

> **Note** The TFTP server cannot be located on the same computer as the CCA application, because they both use the same communication port.

b. In the Maximum Retries field, enter the number of attempts that the WCS526 controller tries to load the web authentication file from the TFTP server on a failure. The default value is 3.

c. In the Timeout (seconds) field, enter the timeout period (in seconds). If the WLC526 controller is not able to start downloading the file within this time period, loading does not occur.

d. In the File Path field, enter the path of the web authentication file on the TFTP server. The default value is a slash (/).

e. In the File Name field, enter the name of the file to be transferred.

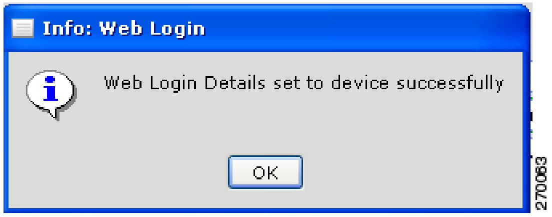
f. Click **Download** to download the customized login file.

> **Note** If you click **OK** or **Apply**, the download starts and the customized login file is applied to the device.

> **Note** The download process takes at least 3 minutes and overwrites the existing login file.

g. When you complete this window, click **OK** to save your changes and to close the window. A web login pop-up message appears (see Figure 7-20).

Figure 7-20 Web Login Pop-Up Message



Info: Web Login

Web Login Details set to device successfully

Step 10 Click **OK** and the CCA main window appears.

CHAPTER 8

Adding Employee Access with Web Authentication

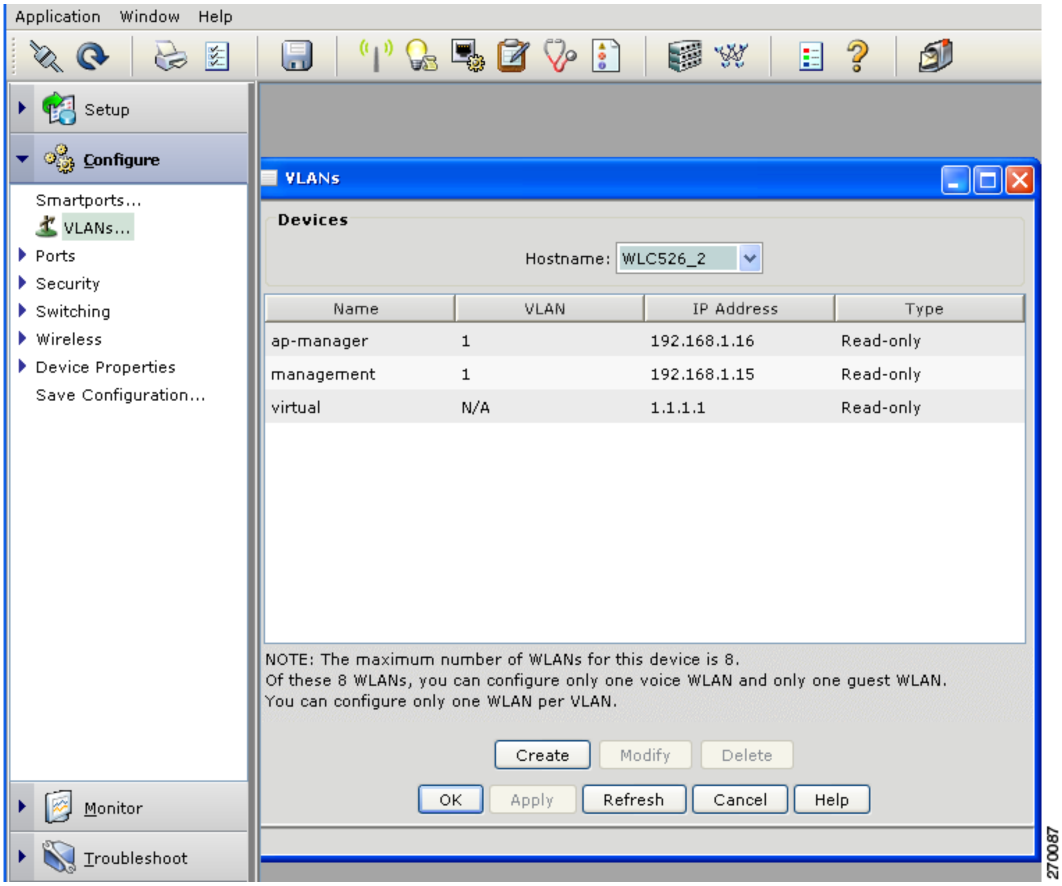
This chapter describes how to add employee access with web authentication and contains these sections:

Adding an Employee Access VLAN

To add an employee access VLAN, follow these steps:

Step 1 Click **Configure** > **VLANs** and Figure 8-1 appears.

Figure 8-1 VLANs Window



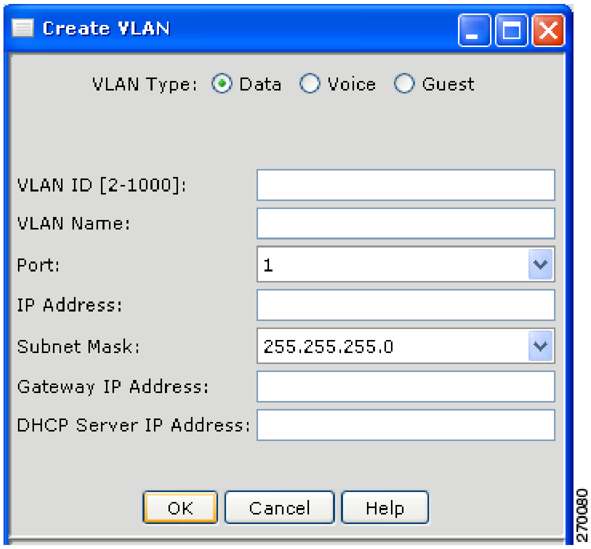
Hostname: WLC526_2

Name	VLAN	IP Address	Type
ap-manager	1	192.168.1.16	Read-only
management	1	192.168.1.15	Read-only
virtual	N/A	1.1.1.1	Read-only

NOTE: The maximum number of WLANs for this device is 8.
Of these 8 WLANs, you can configure only one voice WLAN and only one guest WLAN.
You can configure only one WLAN per VLAN.

Step 2 Click **Create** and Figure 8-2 appears.

Figure 8-2 Create VLAN Window



VLAN Type: ● Data ○ Voice ○ Guest

VLAN ID [2-1000]:
VLAN Name:
Port: 1
IP Address:
Subnet Mask: 255.255.255.0
Gateway IP Address:
DHCP Server IP Address:

Step 3 Accept the Data selection in the VLAN Type field.

Step 4 Perform these steps:

a. In the VLAN ID field, enter the VLAN ID that you want to associate with the employee access VLAN. Use an ID in the range 2 to 1000. Do not enter 1; this ID is reserved.

b. In the VLAN Name field, accept the default name or enter a different name for the VLAN.

c. From the Port list, select a port (1 or 2) for the VLAN. The default is 1.

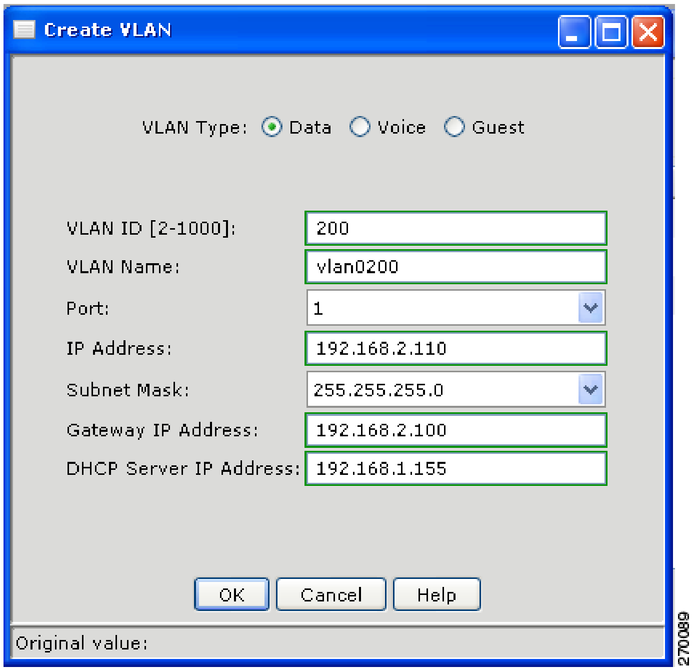
d. In the IP Address field, enter an IP address for the VLAN.

e. From the Subnet Mask list, accept the default or click the drop-down arrow and choose the subnet mask for the VLAN. The default is 255.255.255.0.

f. In the Gateway IP Address field, enter the IP address of the default gateway.

g. In the DHCP Server IP Address field, enter the IP address of the DHCP server.

Figure 8-3 Typical Employee Access VLAN Data



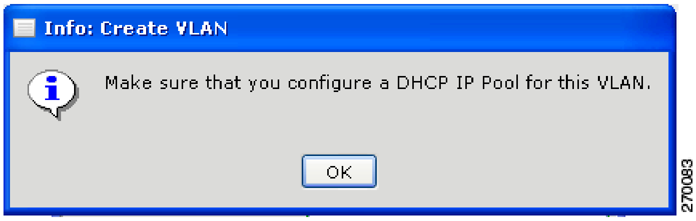
VLAN Type: ● Data ○ Voice ○ Guest

VLAN ID [2-1000]: 200
VLAN Name: vlan0200
Port: 1
IP Address: 192.168.2.110
Subnet Mask: 255.255.255.0
Gateway IP Address: 192.168.2.100
DHCP Server IP Address: 192.168.1.155

Original value:

h. When you complete this window (see Figure 8-3), click **OK** to save your changes and to close the window. A create VLAN pop-up message (Figure 8-4) appears.

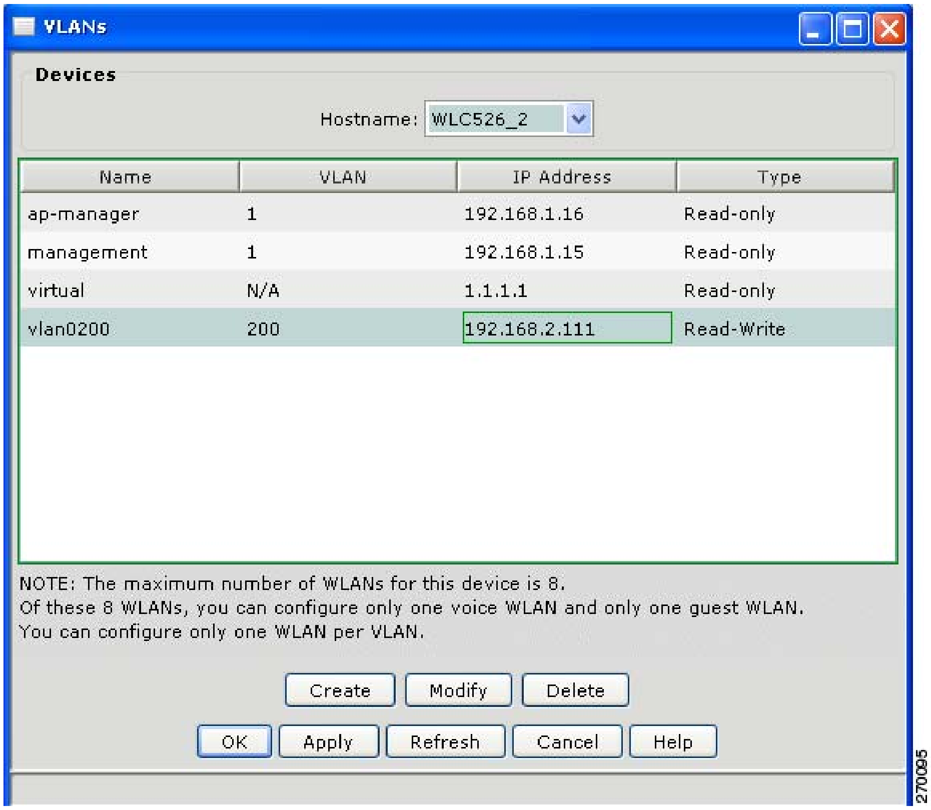
Figure 8-4 Create VLAN Pop-Up Message



Make sure that you configure a DHCP IP Pool for this VLAN.

Step 5 Click **OK** and Figure 8-5 appears and lists the new employee VLAN.

Figure 8-5 VLANs Window with Employee VLAN Added



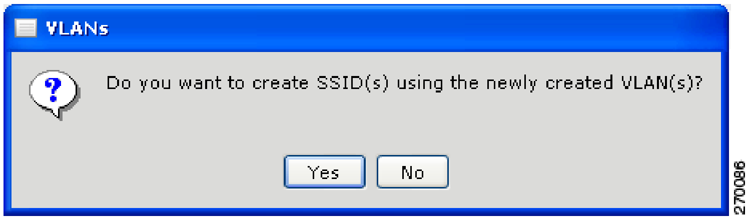
Hostname: WLC526_2

Name	VLAN	IP Address	Type
ap-manager	1	192.168.1.16	Read-only
management	1	192.168.1.15	Read-only
virtual	N/A	1.1.1.1	Read-only
vlan0200	200	192.168.2.111	Read-Write

NOTE: The maximum number of WLANs for this device is 8.
Of these 8 WLANs, you can configure only one voice WLAN and only one guest WLAN.
You can configure only one WLAN per VLAN.

Step 6 Click **OK** and another VLANs pop-up message appears (Figure 8-6) asking if you want to create an SSID using the new VLAN.

Figure 8-6 VLANs Pop-UP SSID Message



Do you want to create SSID(s) using the newly created VLAN(s)?

Step 7 Click **Yes** to create an SSID for the employee VLAN and Figure 8-7 appears. Go to Step 1.

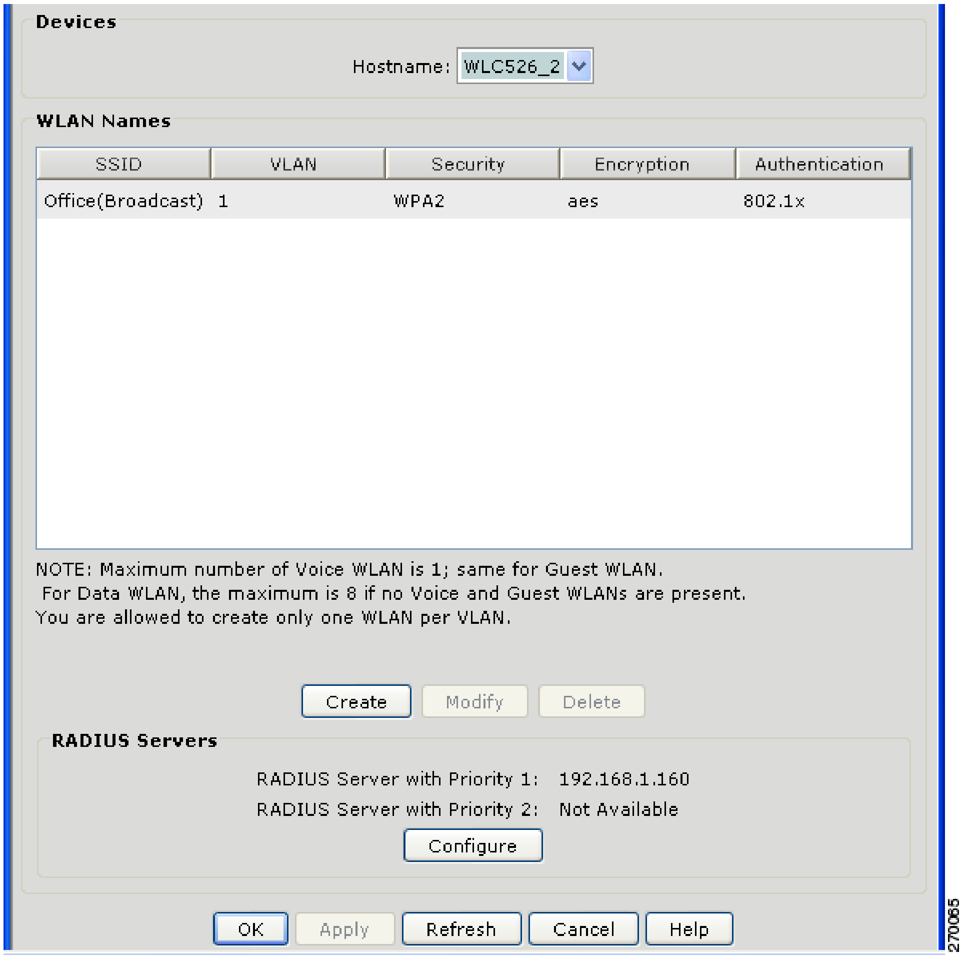
Creating a New WLAN SSID for the Employee VLAN

To create a new WLAN SSID for the employee VLAN, follow these instructions:

Step 1 Figure 8-7 appears after clicking Yes on the VLANs pop-up SSID message (Figure 8-6).

Note You can also click **Wireless** > **WLAN (SSIDs)** to add a employee access WLAN SSID and Figure 8-7 appears.

Figure 8-7 WLAN (SSIDs) Window



Devices

Hostname: WLC526_2

WLAN Names

SSID	VLAN	Security	Encryption	Authentication
Office(Broadcast)	1	WPA2	aes	802.1x

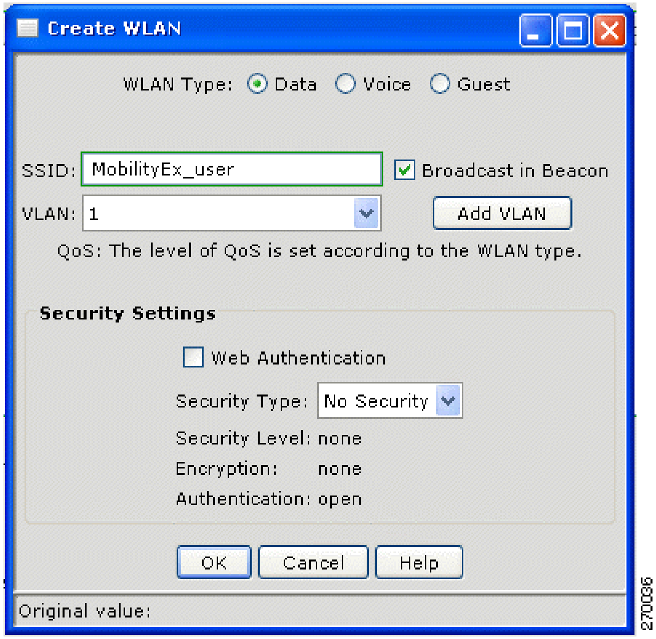
NOTE: Maximum number of Voice WLAN is 1; same for Guest WLAN.
For Data WLAN, the maximum is 8 if no Voice and Guest WLANs are present.
You are allowed to create only one WLAN per VLAN.

RADIUS Servers

RADIUS Server with Priority 1: 192.168.1.160
RADIUS Server with Priority 2: Not Available

Step 2 Click **Create** to create a new WLAN and Figure 8-8 appears.

Figure 8-8 Create WLAN Window



Create WLAN

WLAN Type: ● Data ○ Voice ○ Guest

SSID: MobilityEx_user ☑ Broadcast in Beacon

VLAN: 1 Add VLAN

QoS: The level of QoS is set according to the WLAN type.

Security Settings

□ Web Authentication

Security Type: No Security

Security Level: none

Encryption: none

Authentication: open

OK Cancel Help

Original value:

Use the window to create a new WLAN SSID and to specify the security settings.

Step 3 Accept the default SSID or enter a new SSID value in the SSID field. The SSID can be up to 32 alphanumeric characters.

Step 4 Check **Broadcast in Beacon** if you want to broadcast the SSID so that the devices that do not specify an SSID can associate (establish a wireless connection) with the access point. Only one SSID can be included in the beacon (the employee access WLAN SSID).

Step 5 From the VLAN list, select the data VLAN ID that you want to associate with the SSID.

Step 6 If you click **Add VLAN**, the Add VLAN window appears that enables you to add a new VLAN. To do this, see "Adding an Employee Access VLAN" section on page 8-1.

Step 7 Check **Web Authentication**.

Step 8 Click the Security Type drop-down arrow and choose one of these security options:

- **No Security**—This is the least secure option. Select it only for an SSID that is used in a public place (guest SSID), and associate it with a VLAN that restricts access to your network. There is no encryption, and the authentication type is open authentication.
- **WEP**—This security setting requires that the access point and the client device (a device that connects to the wireless device such as a laptop or a PC) share the same WEP key to keep the communication private.
- **EAP**—This security setting enables IEEE 802.1X authentication and requires you to select the IP address of a RADIUS server. The encryption type is WEP, and the authentication type is IEEE 802.1x.
- **WPA**—This security setting is more secure than the EAP setting. It enables WPA authentication and requires you to select the IP address of a RADIUS server. Client devices that associate with the access point by using this SSID must be WPA-capable.
- **WPA-PSK**—Select this security setting when you want to use the WPA encryption and you do not have access to a RADIUS server. It requires that the access point and the client device share the same WPA-PSK. The key can be from 8 to 63 characters long.

- **WPA2**—This security setting is more secure than the WPA setting. It enables WPA2 authentication and requires you to select the IP address of a RADIUS server. Client devices that associate with the access point by using this SSID must be WPA2-capable.
- **WPA2-PSK**—Select this security setting when you want to use WPA2 encryption and you do not have access to a RADIUS server. It requires that the access point and the client device share the same WPA2-PSK. The key can be from 8 to 63 characters long. The authentication type is WPA2-PSK.
- **MAC**—Select this security setting when you want to authenticate client devices by using MAC address-based authentication. There is no encryption, and the authentication type is IEEE 802.1x.

Step 9 If you choose WEP security, perform these steps:

a. In the Authentication field, click the drop-down arrow and choose **open** or **shared key**.
   - Open authentication—an authentication method that allows any device to authenticate and then attempts to communicate with the access point.
   - Shared key authentication—an authentication method in which the access point sends an unencrypted challenge text string to any device attempting to communicate with it. If the challenge text is correctly encrypted, the access point allows the requesting device to authenticate.

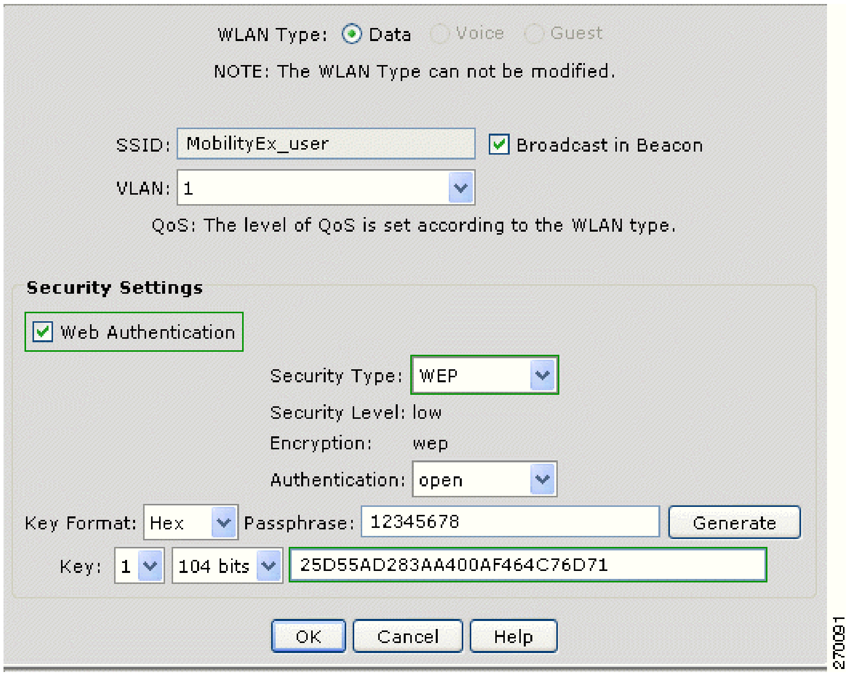
b. In the Key Format field, click the drop-down arrow and choose **Hex** or **ASCII**.

c. Click the Hex Key field drop-down arrow and choose **1**, **2**, **3**, **4**.

d. Click the key size drop-down arrow and choose one of these options:
   - **104 bits**—Requires 13 ASCII characters or 26 Hex digits.
   - **40 bits**—Requires 5 ASCII characters or 20 Hex digits.

e. If you selected a hex key format, choose one of these options:
   - Enter the encryption key (see key size above).
   - Enter a passphrase (8 to 63 characters) and click **Generate for the encryption key to be automatically created** (see Figure 8-9).

Figure 8-9 ***Passphrase and Auto-Generated Hex Key***



WLAN Type: ● Data ○ Voice ○ Guest

NOTE: The WLAN Type can not be modified.

SSID: MobilityEx_user ☑ Broadcast in Beacon

VLAN: 1

QoS: The level of QoS is set according to the WLAN type.

Security Settings

☑ Web Authentication

Security Type: WEP

Security Level: low

Encryption: wep

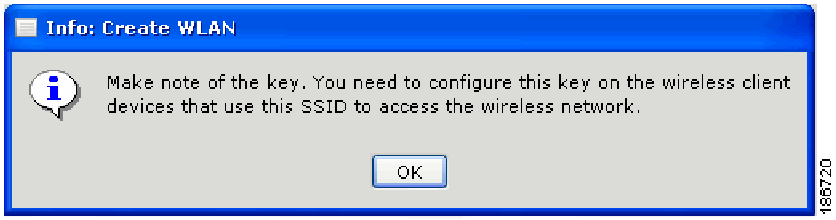
Authentication: open

Key Format: Hex Passphrase: 12345678

Key: 1 104 bits 25D55AD283AA400AF464C76D71

> **Note** When you click the Generate key, a pop-up window appears, reminding you to make note of the key in a safe place (see Figure 8-10).

Figure 8-10 ***Generate Button Pop-Up Message***



Info: Create WLAN

Make note of the key. You need to configure this key on the wireless client devices that use this SSID to access the wireless network.

f. Skip to Step 12 to finish the configuration.

Step 10 If you choose WPA security, perform these steps:

a. Click the Encryption drop-down arrow and choose one of these options:

- **AES**—Advanced Encryption Standard is a block cipher that can encrypt and decrypt data using keys of 128, 192, or 256 bits.
- **TKIP**—Temporal Key Integrity Protocol is an encryption that defends against an attack on WEP in which the intruder uses an unencrypted segment called the initialization vector (IV) in encrypted packets to calculate the WEP key.

b. Click the Authentication drop-down arrow and choose one of these authentication options:

- **802.1x** (default)
- **Fast roaming**

- **802.1x with fast roaming**

c. Skip to Step 12 to finish the configuration.

Step 11 If you choose WPA-PSK, WPA2, or WPA2-PSK security, perform these steps:

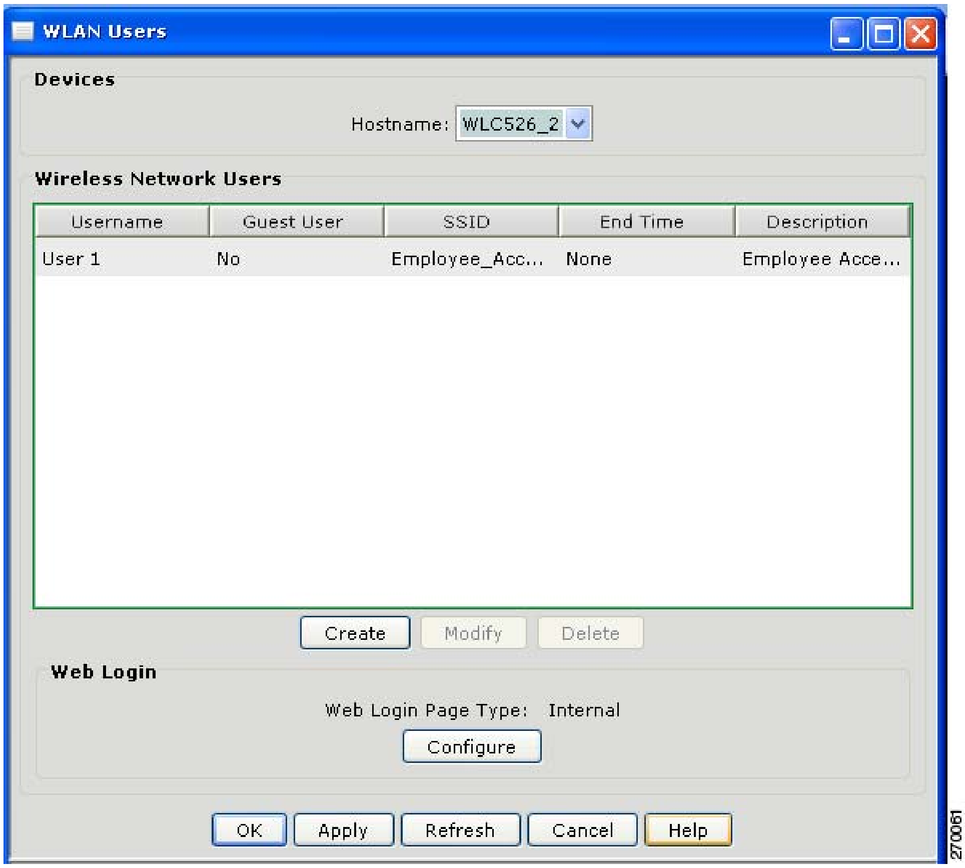
a. Click the Encryption drop-down arrow and choose **aes** or **tkip**.

Note The authentication is wpa-psk, wpa2-psk, or WPA2-PSK corresponding to the security type.

b. Enter the WPA pre-shared key (8 to 63 characters long).

Step 12 When finished, click **OK** and WLANs Window (Figure 8-11) reappears with the new employee WLAN SSID added.

Figure 8-11 WLANs Window with New Employee WLAN SSID



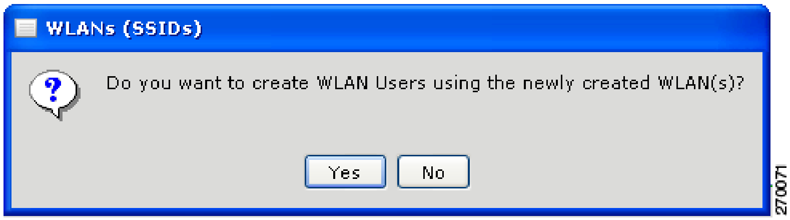
Hostname: WLC526_2

Username	Guest User	SSID	End Time	Description
User 1	No	Employee_Acc...	None	Employee Acce...

Web Login Page Type: Internal

Step 13 Click **OK** and a pop-up message (Figure 8-12) appears asking if you want to create WLAN users for the new WLAN.

Figure 8-12 WLAN (SSIDs) Pop-Up Message


WLANs (SSIDs)

Do you want to create WLAN Users using the newly created WLAN(s)?

Step 14 Click **Yes** to add new employee users and Figure 8-13 appears. Go to Step 1.

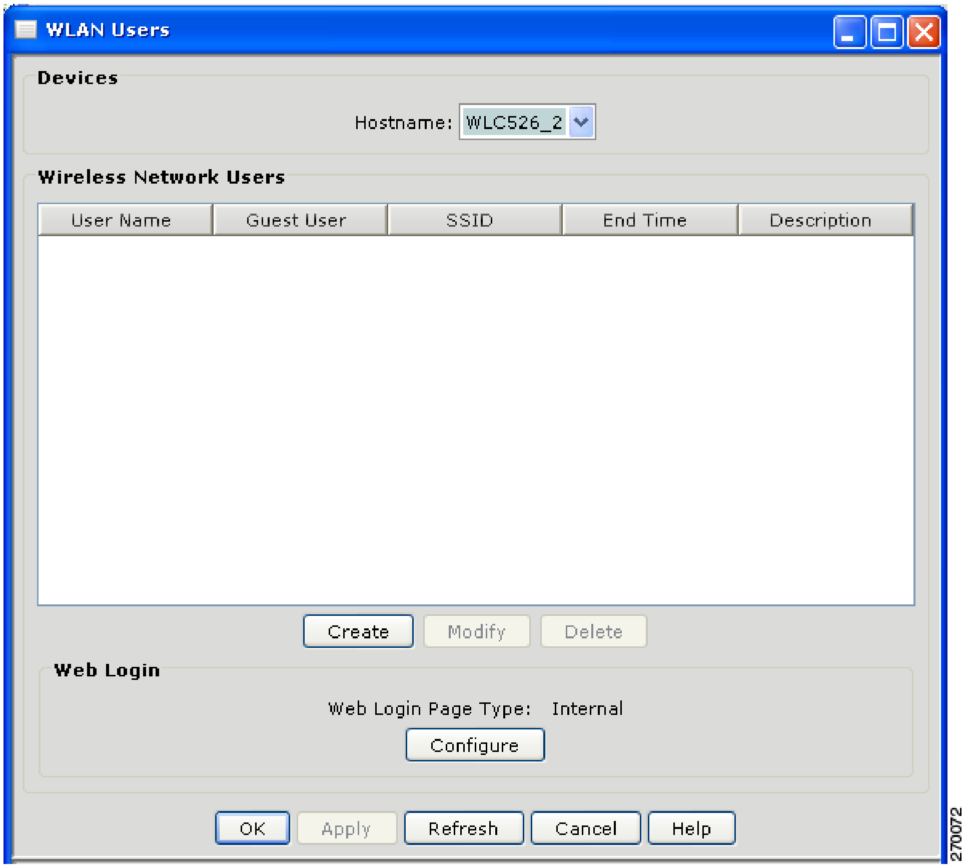
Adding an Employee User

To add an employee access user, follow these instructions:

Step 1 Figure 8-13 appears after clicking Yes on the WLAN (SSIDs) pop-up message (see Figure 8-12).

Note You can also click **Wireless** > **WLAN Users** to add employee users and Figure 8-12 appears.

Figure 8-13 WLAN Users Window



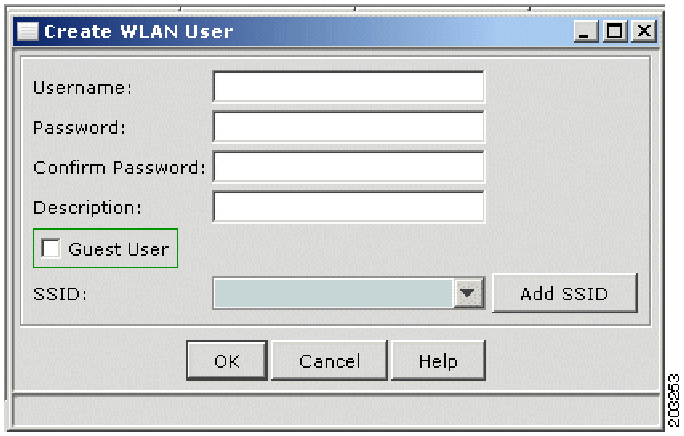
Hostname: WLC526_2

Web Login Page Type: Internal

Step 2 Click the drop-down arrow in the Hostname field and choose your controller.

Step 3 Click **Create** and Figure 8-14 appears.

Figure 8-14 Create WLAN User Window



Step 4 Perform these steps:

a. Enter a user name (up to 49 alphanumeric characters) in the User Name field.

b. Enter a password (up to 24 alphanumeric characters) in the Password field.

c. Reenter the password in the Confirm Password field.

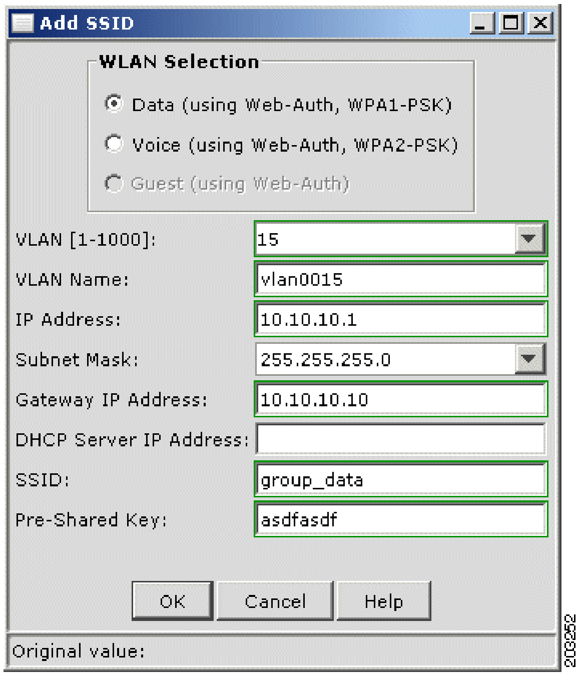
d. Enter a description of the user in the Description field.

e. Uncheck **Guest User**, if necessary.

f. Accept the displayed SSID or click the down-arrow and choose the desired employee access SSID.

Note If no SSID is present in the drop-down list, click **Add SSID**, and complete the Add SSID window and click OK. See Figure 8-15.

Figure 8-15 Add SSID window for employee user



Add SSID

WLAN Selection

● Data (using Web-Auth, WPA1-PSK)

○ Voice (using Web-Auth, WPA2-PSK)

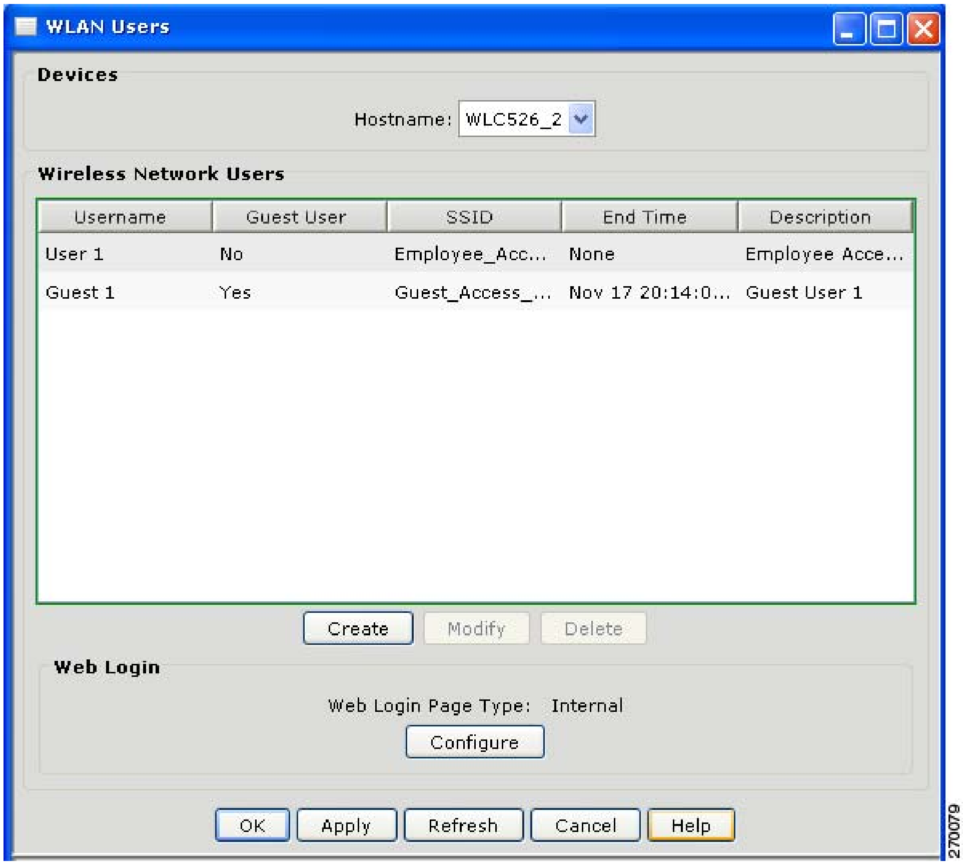
○ Guest (using Web-Auth)

VLAN [1-1000]:	15
VLAN Name:	vlan0015
IP Address:	10.10.10.1
Subnet Mask:	255.255.255.0
Gateway IP Address:	10.10.10.10
DHCP Server IP Address:	
SSID:	group_data
Pre-Shared Key:	asdfasdf

Original value:

g. When complete, click **OK** and Figure 8-16 appears.

Figure 8-16 New Employee User



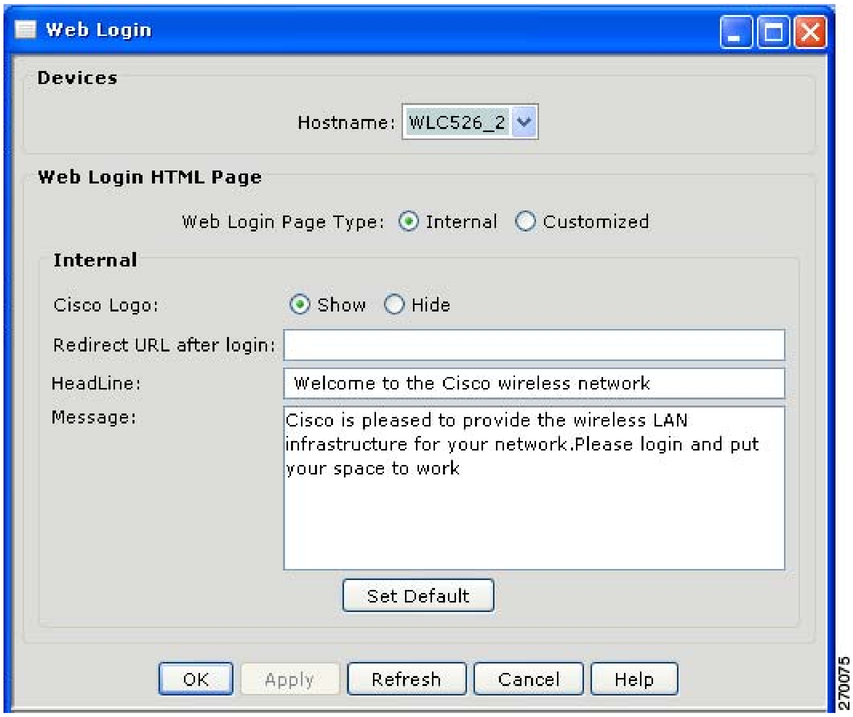
Hostname: WLC526_2

Username	Guest User	SSID	End Time	Description
User 1	No	Employee_Acc...	None	Employee Acce...
Guest 1	Yes	Guest_Access_...	Nov 17 20:14:0...	Guest User 1

Web Login Page Type: Internal

Step 5 Click **Configure** to configure the web login page and Figure 8-17 appears.

Figure 8-17 Web Login Window



Web Login

Devices

Hostname: WLC526_2

Web Login HTML Page

Web Login Page Type: ● Internal ○ Customized

Internal

Cisco Logo: ● Show ○ Hide

Redirect URL after login:

HeadLine: Welcome to the Cisco wireless network

Message: Cisco is pleased to provide the wireless LAN infrastructure for your network.Please login and put your space to work

Step 6 Click the drop-down arrow in the Hostname field and choose your controller.

Step 7 Check **Internal** or **Customized** in the Web Login Page Type field.

Step 8 If you checked Internal, perform these steps:

a. Check **Show** to display the Cisco logo or check **Hide to hide the** Cisco logo.

b. In the Redirect URL after Login field, enter a URL to which the user will be redirected after logging in. The URL format is *www.companyname.com* and can contain up to 254 characters.

c. In the Headline field, enter the login page headline or summary, up to 127 characters. The default is *Welcome to the Cisco wireless network*.

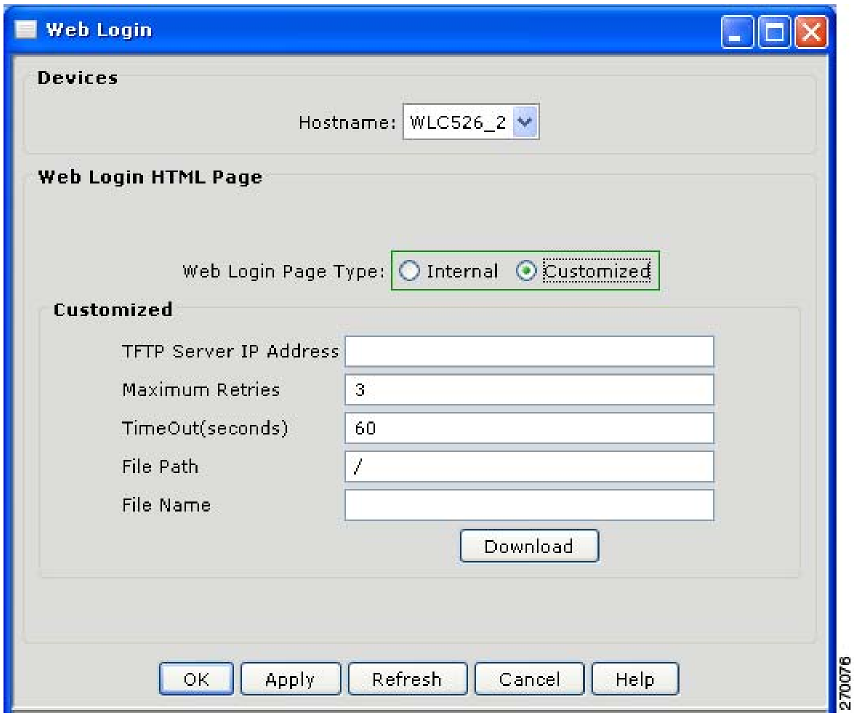
d. In the message field, enter the message text up to 2047 characters. The default message is shown in Figure 8-17.

e. If you want to revert to the default settings, click **Set Default**.

f. When complete, click **OK and a** web login pop-up message appears (see Figure 8-19). Go to Step 10.

Step 9 If you checked Customized, Figure 8-18 appears.

Figure 8-18 Web Login Customized Window



Web Login

Devices

Hostname: WLC526_2

Web Login HTML Page

Web Login Page Type: ○ Internal ● Customized

Customized

TFTP Server IP Address:

Maximum Retries: 3

TimeOut(seconds): 60

File Path: /

File Name:

Perform these steps:

a. In the TFTP Server IP Address field, enter the IP address of the TFTP server where the customized Web authentication bundle file exists.

Note The TFTP server cannot be located on the same computer as the CCA application, because they both use the same communication port.

b. In the Maximum Retries field, enter the number of attempts that the WCS526 controller tries to load the web authentication file from the TFTP server on a failure. The default value is 3.

c. In the Timeout (seconds) field, enter the timeout period (in seconds). If the WLC526 controller is not able to start downloading the file within this time period, loading does not occur.

d. In the File Path field, enter the path of the web authentication file on the TFTP server. The default value is a slash (/).

e. In the File Name field, enter the name of the file to be transferred.

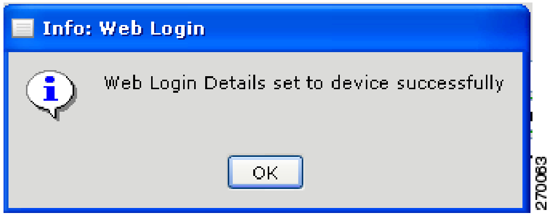
f. Click **Download** to download the customized login file.

Note If you click **OK** or **Apply**, the download starts and the customized login file is applied to the device.

Note The download process takes at least 3 minutes and overwrites the existing login file.

g. When you complete this window, click **OK** to save your changes and to close the window. A web login pop-up message appears (see Figure 8-19).

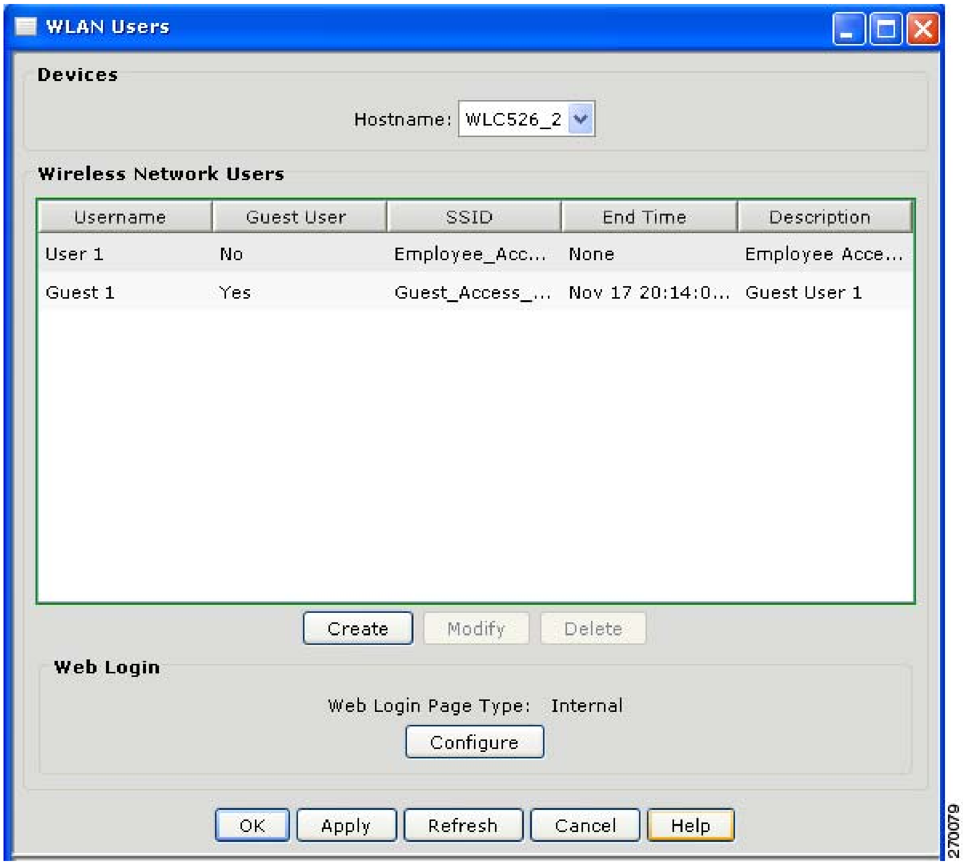
Figure 8-19 Web Login Pop-Up Message



Web Login Details set to device successfully

Step 10 Click **OK** and the WLAN Users window reappears (see Figure 8-20).

Figure 8-20 Create WLAN User Window



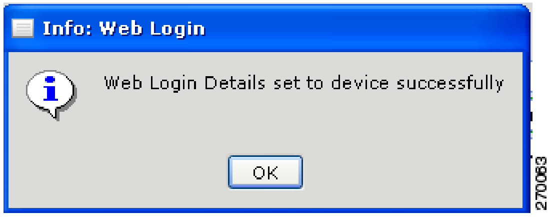
Hostname: WLC526_2

Username	Guest User	SSID	End Time	Description
User 1	No	Employee_Acc...	None	Employee Acce...
Guest 1	Yes	Guest_Access_...	Nov 17 20:14:0...	Guest User 1

Web Login Page Type: Internal

Step 11 Click **OK** and Figure 8-21 appears.

Figure 8-21 Web Login Details Message



Web Login Details set to device successfully

Step 12 Click **OK** and the CCA main window appears.

CHAPTER 9

Adding Voice Access with Web Authentication

This chapter describes how to add voice access with web authentication and contains these sections:

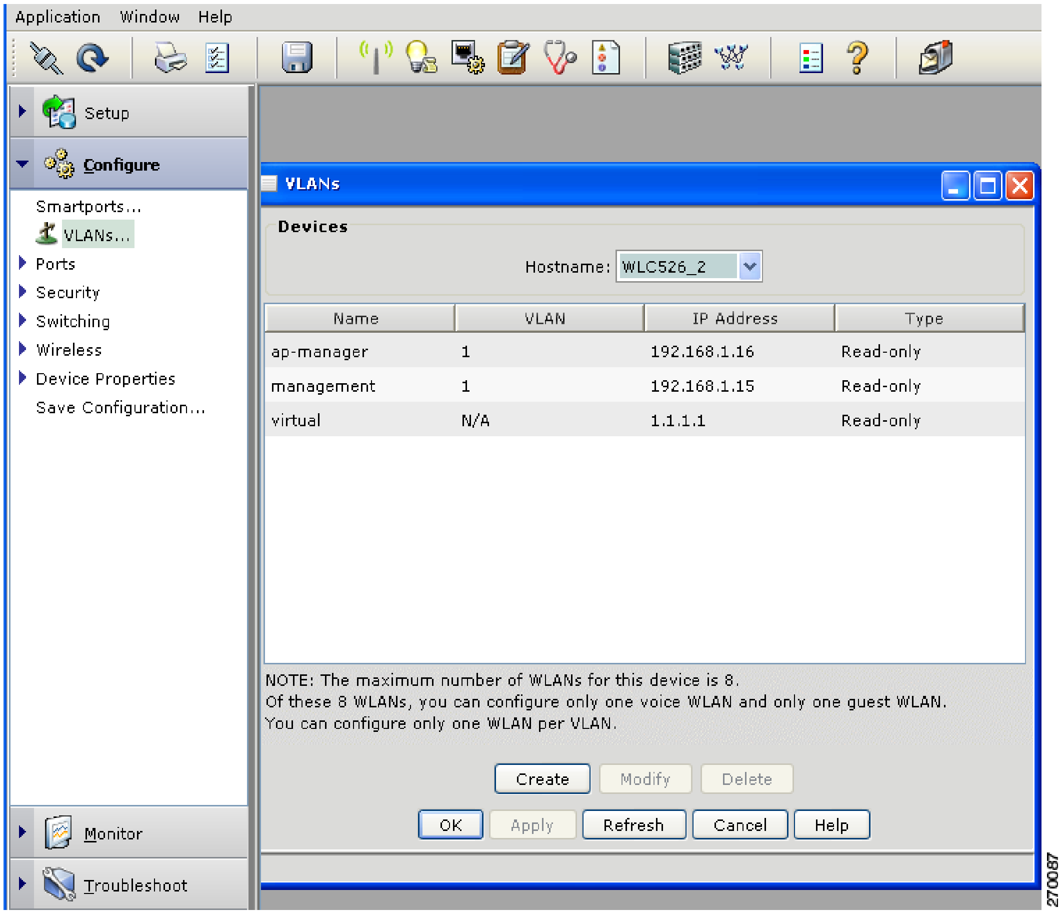
- Adding a Voice-Enabled VLAN, page 9-2
- Creating a New SSID for the Voice VLAN, page 9-6

Adding a Voice-Enabled VLAN

To add a voice-enabled VLAN, follow these steps:

Step 1 Click **Configure** > **VLANs** and Figure 9-1 appears.

Figure 9-1 VLAN Window



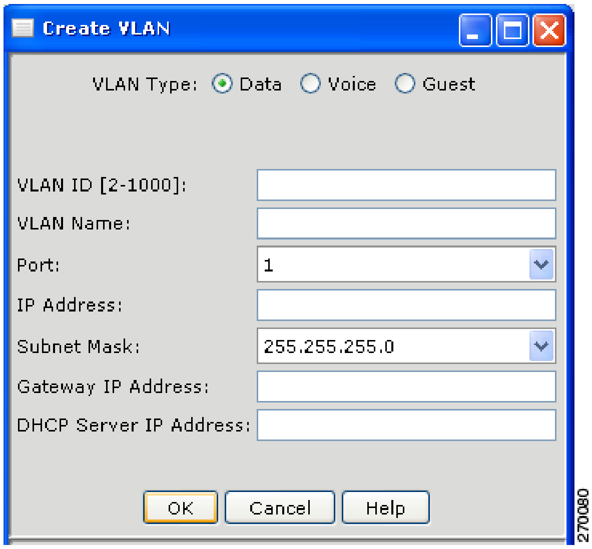
Hostname: WLC526_2

Name	VLAN	IP Address	Type
ap-manager	1	192.168.1.16	Read-only
management	1	192.168.1.15	Read-only
virtual	N/A	1.1.1.1	Read-only

NOTE: The maximum number of WLANs for this device is 8.
Of these 8 WLANs, you can configure only one voice WLAN and only one guest WLAN.
You can configure only one WLAN per VLAN.

Click **Create** and Figure 9-2 appears.

Figure 9-2 Create VLAN Window



Create VLAN

VLAN Type: ● Data ○ Voice ○ Guest

VLAN ID [2-1000]:

VLAN Name:

Port: 1

IP Address:

Subnet Mask: 255.255.255.0

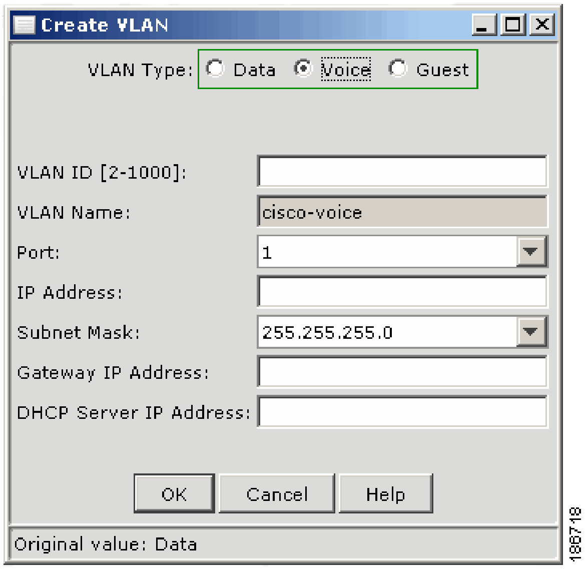
Gateway IP Address:

DHCP Server IP Address:

Step 2 Click **Voice** for a voice VLAN and Figure 9-3 appears.

Note For a Voice VLAN type, the VLAN name field is set with a predefined VLAN name (*cisco-voice*) and cannot be changed.

Figure 9-3 Create Voice VLAN Window



Create VLAN

VLAN Type: ○ Data ● Voice ○ Guest

VLAN ID [2-1000]:

VLAN Name: cisco-voice

Port: 1

IP Address:

Subnet Mask: 255.255.255.0

Gateway IP Address:

DHCP Server IP Address:

Original value: Data

Step 3 Perform these steps:

a. In the VLAN ID field, enter the VLAN ID that you want to associate with the voice VLAN. Use an ID in the range 2 to 1000. Do not enter 1; this ID is reserved.

Note For Voice VLAN types, the VLAN name field is set with a predefined VLAN name that is based on the selected VLAN type. It cannot be changed.

b. From the Port list, select a port (1 or 2) for the VLAN. The default is 1.

c. In the IP Address field, enter an IP address for the VLAN.

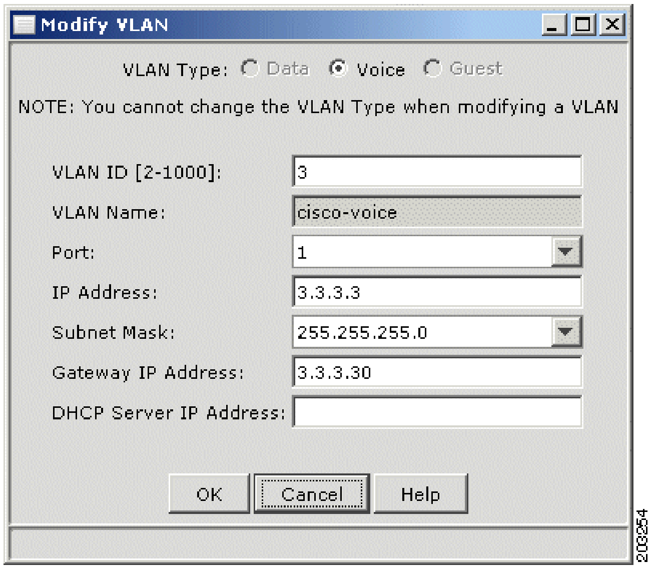
d. From the Subnet Mask list, accept the default or click the drop-down arrow and choose the subnet mask for the VLAN. The default is 255.255.255.0.

e. In the Gateway IP Address field, enter the IP address of the default gateway.

f. In the DHCP Server IP Address field, enter the IP address of the DHCP server.

g. When you complete this window (see Figure 9-4), click **OK** to save your changes and to close the window.

Figure 9-4 Typical Voice VLAN Data



Modify VLAN

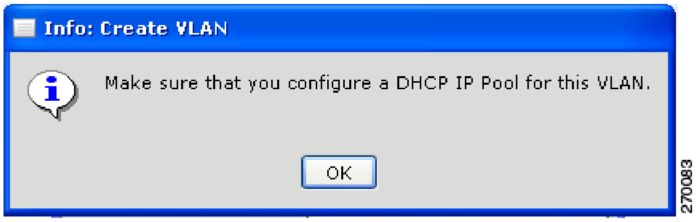
VLAN Type: ○ Data ● Voice ○ Guest

NOTE: You cannot change the VLAN Type when modifying a VLAN

VLAN ID [2-1000]:	3
VLAN Name:	cisco-voice
Port:	1
IP Address:	3.3.3.3
Subnet Mask:	255.255.255.0
Gateway IP Address:	3.3.3.30
DHCP Server IP Address:	

A create VLAN pop-up message (Figure 9-5) appears.

Figure 9-5 Create VLAN Pop-Up Message

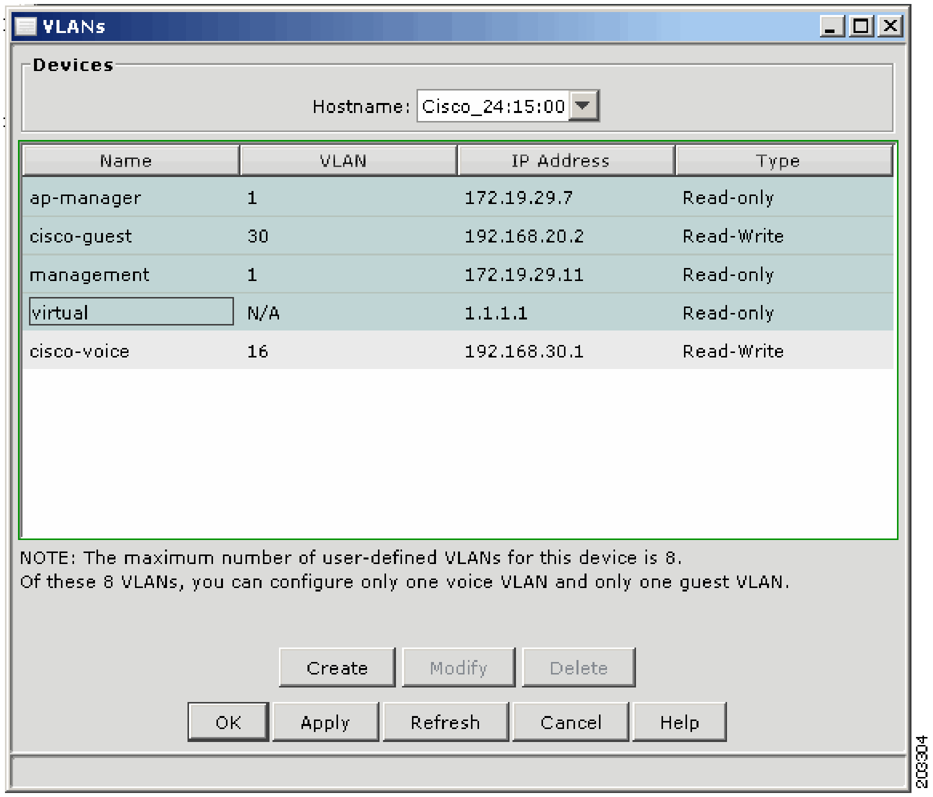


Info: Create VLAN

Make sure that you configure a DHCP IP Pool for this VLAN.

Step 4 Click **OK** and Figure 9-6 appears and lists the new voice VLAN.

Figure 9-6 VLANs Window with Voice VLAN Added



VLANs

Devices

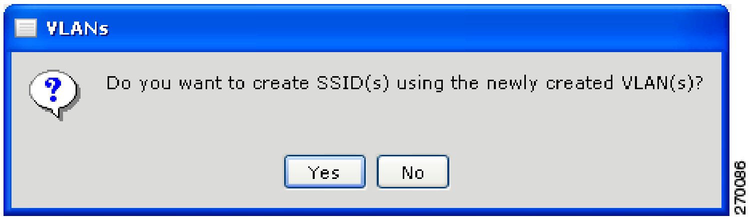
Hostname: Cisco_24:15:00

Name	VLAN	IP Address	Type
ap-manager	1	172.19.29.7	Read-only
cisco-guest	30	192.168.20.2	Read-Write
management	1	172.19.29.11	Read-only
virtual	N/A	1.1.1.1	Read-only
cisco-voice	16	192.168.30.1	Read-Write

NOTE: The maximum number of user-defined VLANs for this device is 8.
Of these 8 VLANs, you can configure only one voice VLAN and only one guest VLAN.

Step 5 Click **OK** and a VLANs pop-up message appears (Figure 9-7) asking if you want to create an SSID using the new VLAN.

Figure 9-7 VLANs Pop-UP SSID Message



VLANs

Do you want to create SSID(s) using the newly created VLAN(s)?

Step 6 Click **Yes** to create an SSID for the voice VLAN and Figure 9-8 appears. Go to Step 1.

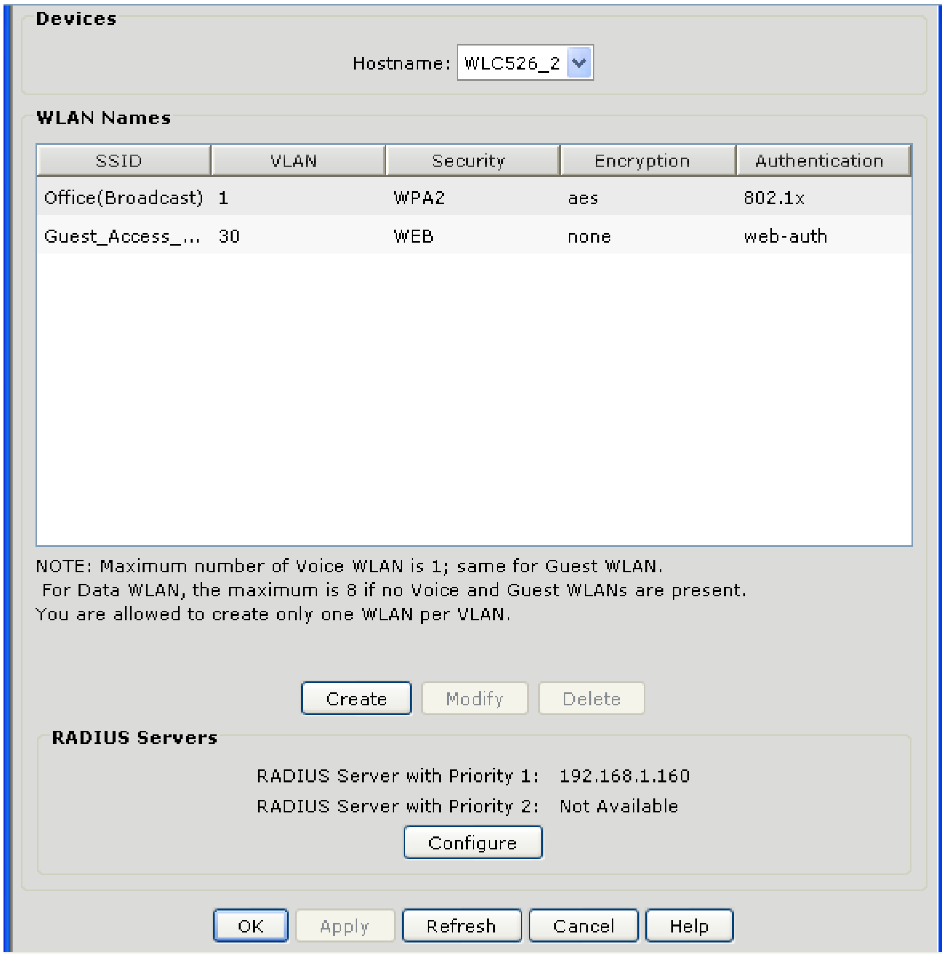
Creating a New SSID for the Voice VLAN

To create a new SSID for the voice VLAN, follow these instructions:

Step 1 Figure 9-8 appears after clicking Yes on the VLANs pop-up SSID message (see Figure 9-7).

Note You can also click **Wireless** > **WLAN (SSIDs)** to add a voice WLAN SSID and Figure 9-8 appears.

Figure 9-8 WLAN (SSIDs) Window



Devices

Hostname: WLC526_2

WLAN Names

SSID	VLAN	Security	Encryption	Authentication
Office(Broadcast)	1	WPA2	aes	802.1x
Guest_Access_...	30	WEB	none	web-auth

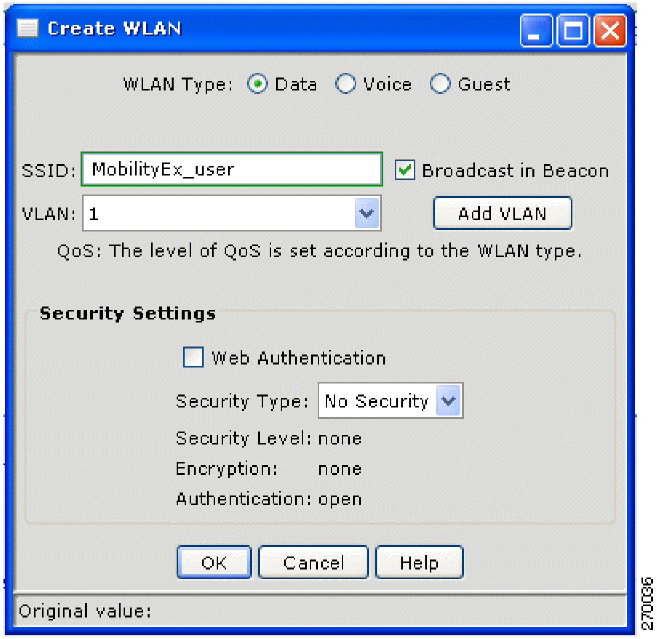
NOTE: Maximum number of Voice WLAN is 1; same for Guest WLAN.
For Data WLAN, the maximum is 8 if no Voice and Guest WLANs are present.
You are allowed to create only one WLAN per VLAN.

RADIUS Servers

RADIUS Server with Priority 1: 192.168.1.160
RADIUS Server with Priority 2: Not Available

Step 2 Click **Create** to create a new WLAN and Figure 9-9 appears.

Figure 9-9 Create WLAN Window



WLAN Type: ● Data ○ Voice ○ Guest

SSID: MobilityEx_user ☑ Broadcast in Beacon

VLAN: 1

QoS: The level of QoS is set according to the WLAN type.

Security Settings

□ Web Authentication

Security Type: No Security

Security Level: none

Encryption: none

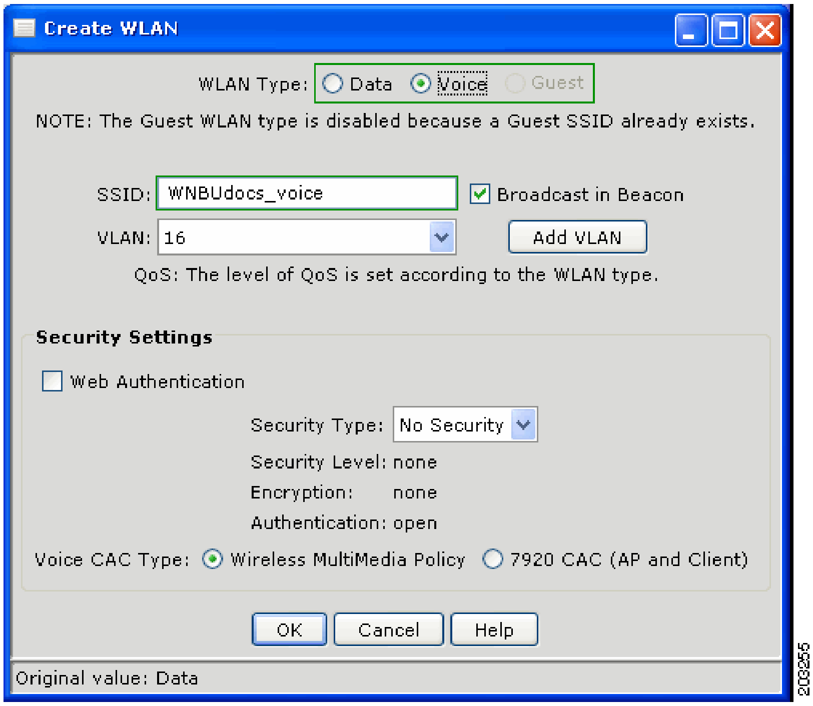
Authentication: open

Original value:

Use the window to create a new SSID and to specify the security settings.

Step 3 Click **Voice** to create a voice WLAN and Figure 9-10 appears.

Figure 9-10 Create Voice WLAN Window



WLAN Type: ○ Data ● Voice ○ Guest

NOTE: The Guest WLAN type is disabled because a Guest SSID already exists.

SSID: WNBUdocs_voice ☑ Broadcast in Beacon

VLAN: 16

QoS: The level of QoS is set according to the WLAN type.

Security Settings

□ Web Authentication

Security Type: No Security

Security Level: none

Encryption: none

Authentication: open

Voice CAC Type: ● Wireless MultiMedia Policy ○ 7920 CAC (AP and Client)

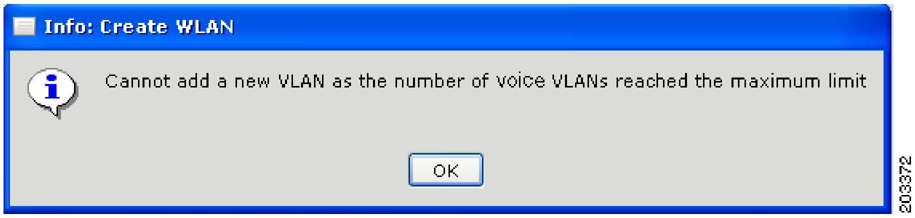
Original value: Data

On a voice WLAN, these options are automatically configured and cannot be changed:

- The default voice VLAN selected. Only one voice VLAN can be created.

  - If you click the Add VLAN button, Figure 9-11 appears indicating the maximum number of VLANs has been reached.

Figure 9-11 Add VLAN Pop-Up Message



Info: Create WLAN

Cannot add a new VLAN as the number of voice VLANs reached the maximum limit

Step 4 Check **Web Authentication**.

Step 5 Click the Security Type drop-down arrow and choose one of these security options:

- **No Security**—This is the least secure option. Select it only for an SSID that is used in a public place (guest SSID), and associate it with a VLAN that restricts access to your network. There is no encryption, and the authentication type is open authentication.
- **WEP**—This security setting requires that the access point and the client device (a device that connects to the wireless device such as a laptop or a PC) share the same WEP key to keep the communication private.
- **EAP**—This security setting enables IEEE 802.1X authentication and requires you to select the IP address of a RADIUS server. The encryption type is WEP, and the authentication type is IEEE 802.1x.
- **WPA**—This security setting is more secure than the EAP setting. It enables WPA authentication and requires you to select the IP address of a RADIUS server. Client devices that associate with the access point by using this SSID must be WPA-capable.
- **WPA-PSK**—Select this security setting when you want to use the WPA encryption and you do not have access to a RADIUS server. It requires that the access point and the client device share the same WPA-PSK. The key can be from 8 to 63 characters long.
- **WPA2**—This security setting is more secure than the WPA setting. It enables WPA2 authentication and requires you to select the IP address of a RADIUS server. Client devices that associate with the access point by using this SSID must be WPA2-capable.
- **WPA2-PSK**—Select this security setting when you want to use WPA2 encryption and you do not have access to a RADIUS server. It requires that the access point and the client device share the same WPA2-PSK. The key can be from 8 to 63 characters long. The authentication type is WPA2-PSK.
- **MAC**—Select this security setting when you want to authenticate client devices by using MAC address-based authentication. There is no encryption, and the authentication type is IEEE 802.1x.

Step 6 If you choose WEP security, perform these steps:

a. In the Authentication field, click the drop-down arrow and choose **open** or **shared key**.

  - Open authentication—an authentication method that allows any device to authenticate and then attempts to communicate with the access point.
  - Shared key authentication—an authentication method in which the access point sends an unencrypted challenge text string to any device attempting to communicate with it. If the challenge text is correctly encrypted, the access point allows the requesting device to authenticate.

b. In the Key Format field, click the drop-down arrow and choose **Hex** or **ASCII**.

c. Click the Hex Key field drop-down arrow and choose **1**, **2**, **3**, **4**.

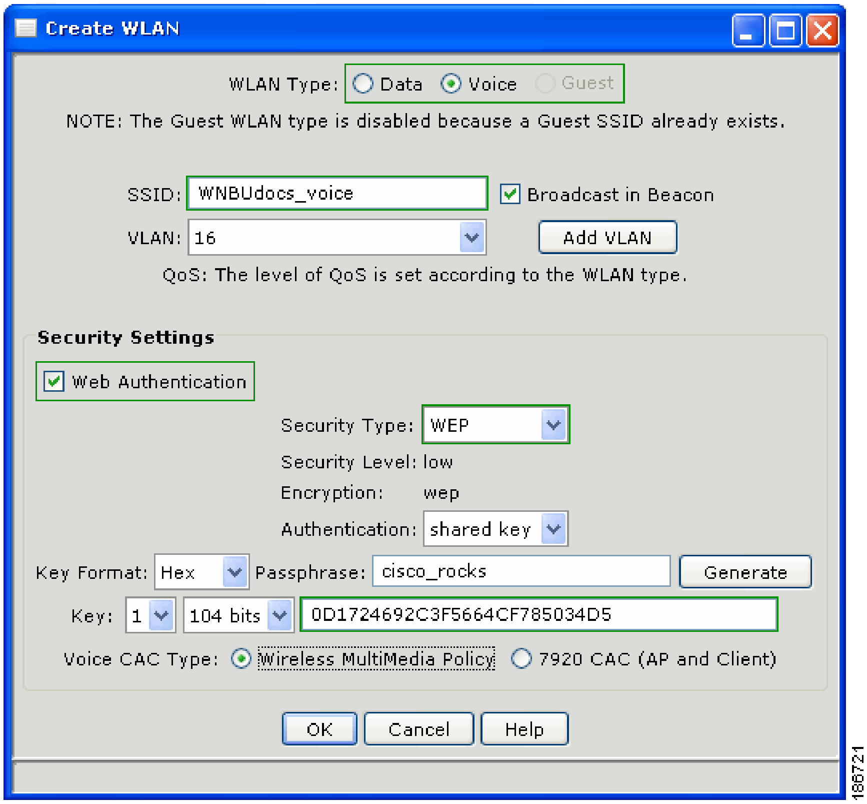
d. Click the key size drop-down arrow and choose one of these options:

- **104 bits**—Requires 13 ASCII characters or 26 Hex digits.
- **40 bits**—Requires 5 ASCII characters or 20 Hex digits.

e. If you selected a hex key format, choose one of these options:

- Enter the encryption key (see key size above).
- Enter a passphrase (8 to 63 characters) and click **Generate for the encryption key to be automatically created** (see Figure 9-12).

Figure 9-12 Configuring WEP Security with Generated Encryption Key



WLAN Type: ○ Data ● Voice ○ Guest

NOTE: The Guest WLAN type is disabled because a Guest SSID already exists.

SSID: WNBUdocs_voice ☑ Broadcast in Beacon

VLAN: 16

QoS: The level of QoS is set according to the WLAN type.

Security Settings

☑ Web Authentication

Security Type: WEP

Security Level: low

Encryption: wep

Authentication: shared key

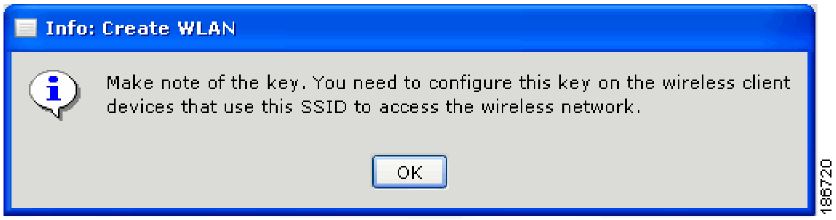
Key Format: Hex Passphrase: cisco_rocks

Key: 1 104 bits 0D1724692C3F5664CF785034D5

Voice CAC Type: ● Wireless MultiMedia Policy ○ 7920 CAC (AP and Client)

Note When you click the Generate key, a pop-up window appears, reminding you to make note of the key in a safe place (see Figure 9-13).

Figure 9-13 WEP Key Reminder Message



Info: Create WLAN

Make note of the key. You need to configure this key on the wireless client devices that use this SSID to access the wireless network.

f. Skip to Step 9 to finish the configuration.

Step 7 If you choose WPA security, perform these steps:

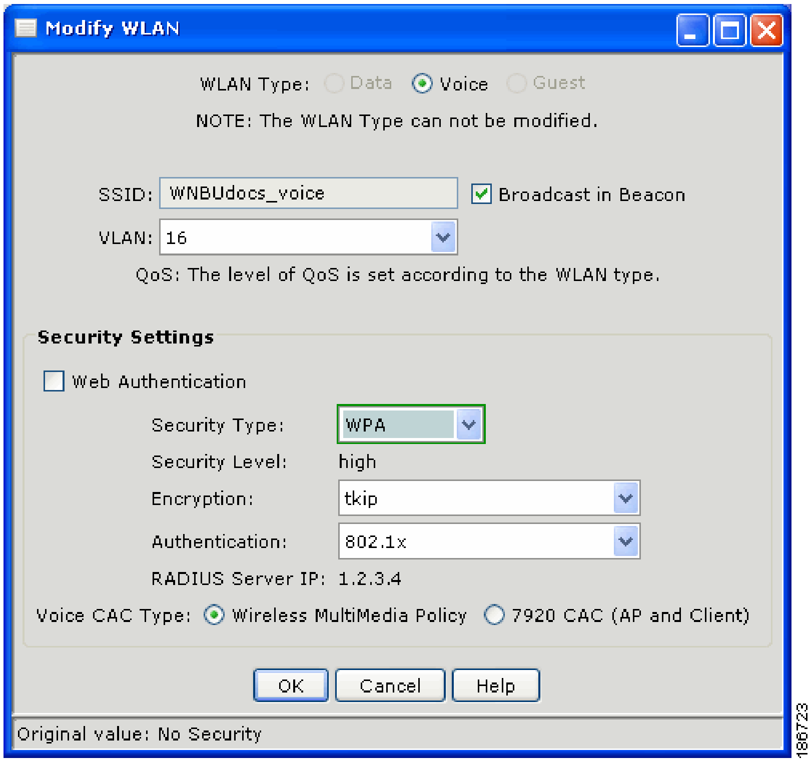
a. Click the Encryption drop-down arrow and choose one of these options:

- **AES**—Advanced Encryption Standard is a block cipher that can encrypt and decrypt data using keys of 128, 192, or 256 bits.
- **TKIP**—Temporal Key Integrity Protocol is an encryption that defends against an attack on WEP in which the intruder uses an unencrypted segment called the initialization vector (IV) in encrypted packets to calculate the WEP key.

b. Click the Authentication drop-down arrow and choose one of these authentication options (**see Figure 9-14**):

- **802.1x** (default)
- **Fast roaming**
- **802.1x with fast roaming**

Figure 9-14 Configuring WPA Security Type



Modify WLAN

WLAN Type: ○ Data ● Voice ○ Guest

NOTE: The WLAN Type can not be modified.

SSID: WNBUdocs_voice ☑ Broadcast in Beacon

VLAN: 16

QoS: The level of QoS is set according to the WLAN type.

Security Settings

□ Web Authentication

Security Type: WPA

Security Level: high

Encryption: tkip

Authentication: 802.1x

RADIUS Server IP: 1.2.3.4

Voice CAC Type: ● Wireless MultiMedia Policy ○ 7920 CAC (AP and Client)

Original value: No Security

c. Skip to Step 9 to finish the configuration.

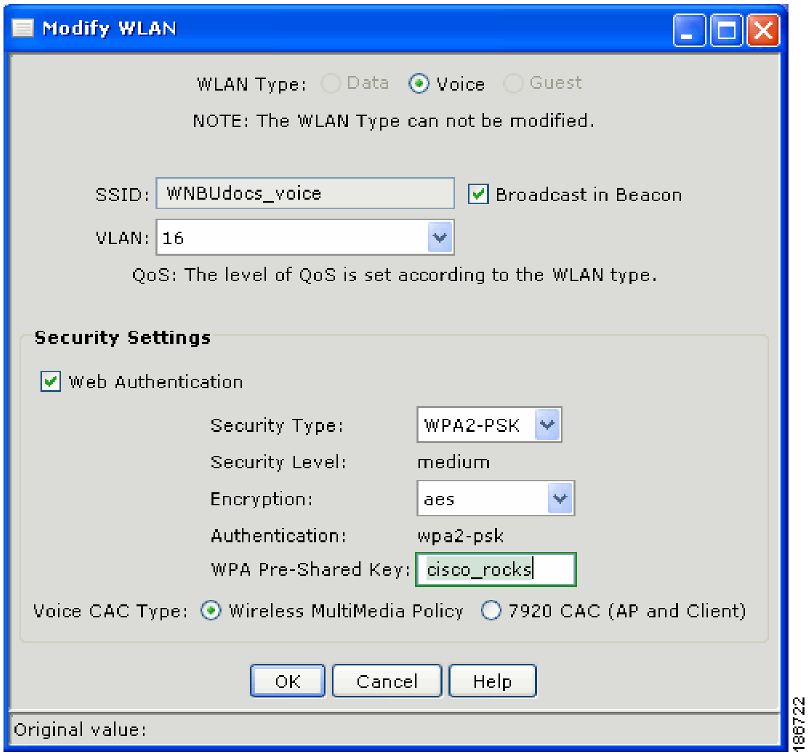
Step 8 If you choose WPA-PSK, WPA2, or WPA2-PSK security, perform these steps:

a. Click the Encryption drop-down arrow and choose **aes** or **tkip** (**see Figure 9-15**).

Note The authentication is WPA-PSK, WPA2-PSK, or WPA2-PSK, corresponding to the security type.

b. Enter the WPA pre-shared key (8 to 63 characters long).

Figure 9-15 Configuring WPA2-PSK Security Type



Modify WLAN

WLAN Type: ○ Data ● Voice ○ Guest

NOTE: The WLAN Type can not be modified.

SSID: WNBUdocs_voice ☑ Broadcast in Beacon

VLAN: 16

QoS: The level of QoS is set according to the WLAN type.

Security Settings

☑ Web Authentication

Security Type: WPA2-PSK

Security Level: medium

Encryption: aes

Authentication: wpa2-psk

WPA Pre-Shared Key: cisco_rocks

Voice CAC Type: ● Wireless MultiMedia Policy ○ 7920 CAC (AP and Client)

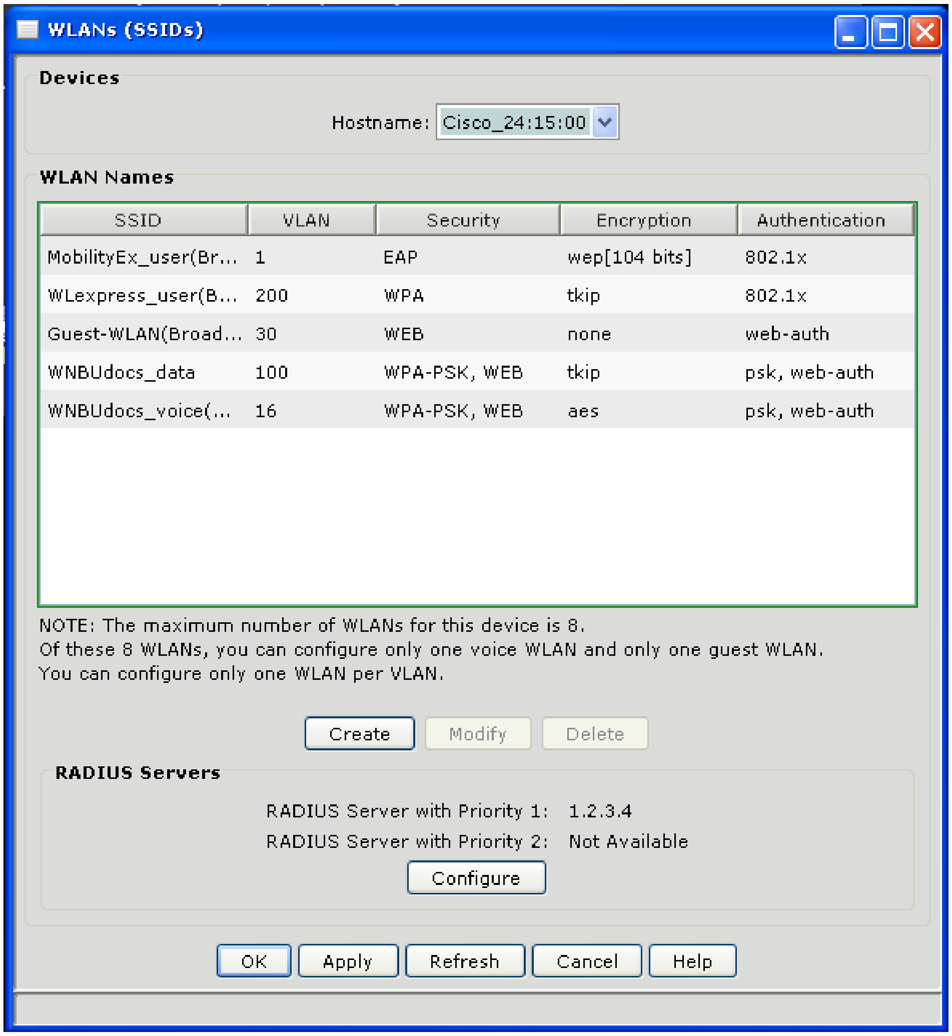
Original value:

Step 9 From the **Voice CAC type** area, select **Wireless MultiMedia Policy**, which requires client devices to use WMM, or select **7920 CAC (AP and Client)**, which supports Cisco 7920 IP telephones on your network. The default setting is Wireless Multimedia Policy.

Note Do not select Wireless Multimedia Policy if you use Cisco 7920 phones on your network.

Step 10 When finished, click **OK** and the WLANs Window (Figure 9-16) reappears with the voice WLAN SSID added.

Figure 9-16 New Voice SSID Configured



Hostname: Cisco_24:15:00

SSID	VLAN	Security	Encryption	Authentication
MobilityEx_user(Br...	1	EAP	wep[104 bits]	802.1x
WLexpress_user(B...	200	WPA	tkip	802.1x
Guest-WLAN(Broad...	30	WEB	none	web-auth
WNBUdocs_data	100	WPA-PSK, WEB	tkip	psk, web-auth
WNBUdocs_voice(...	16	WPA-PSK, WEB	aes	psk, web-auth

NOTE: The maximum number of WLANs for this device is 8.
Of these 8 WLANs, you can configure only one voice WLAN and only one guest WLAN.
You can configure only one WLAN per VLAN.

RADIUS Server with Priority 1: 1.2.3.4
RADIUS Server with Priority 2: Not Available

Step 11 Click **OK**.

APPENDIX A

Configuring DHCP Option 43 for Cisco 520 Series Access Points

This appendix describes the steps needed to configure DHCP Option 43 on an enterprise DHCP server, such as a Cisco Catalyst 3750 series switch, for use with the Cisco 520 series access points (AP521 and LAP521). This appendix contains these sections:

Overview

This section contains a DHCP Option 43 configuration example on an enterprise DHCP server, such as a Cisco Catalyst 3750 series switch, for use with Cisco 520 series access points. For other DHCP server implementations, consult their product documentation for configuring DHCP Option 43. In Option 43, you should use the IP address of the controller web-browser interface (GUI).

Note DHCP Option 43 is limited to one access point type per DHCP pool (AP521 or LAP521). You must configure a separate DHCP pool for each access point type.

The Cisco 520 series access points use the type-length-value (TLV) format for DHCP Option 43. DHCP servers must be programmed to return the option based on the access point's DHCP Vendor Class Identifier (VCI) string (DHCP Option 60). The VCI strings for the Cisco 520 series is listed in Table A-1:

Table A-1 Cisco 520 Series Lightweight Access Point VCI String

Access Point	Vendor Class Identifier (VCI)
LAP521 lightweight access point	Cisco AP c520

The format of the TLV block for 520 series access points is listed below:

- Type: 0xf1 (decimal 241)
- Length: Number of controller IP addresses * 4
- Value: List of WLC management interfaces

Configuring Option 43 for Cisco 520 Series Access Points

To configure DHCP Option 43 for Cisco 520 series access points in the embedded Cisco IOS DHCP server, follow these steps:

Step 1 Enter configuration mode at the Cisco IOS CLI.

Step 2 Create the DHCP pool, including the necessary parameters such as default router and name server. A DHCP scope example is as follows:

```
ip dhcp pool <pool name>
network <IP Network> <Netmask>
default-router <Default router>
dns-server <DNS Server>

Where:
    <pool name> is the name of the DHCP pool, such as LAP521
    <IP Network> is the network IP address where the controller resides, such as 10.0.15.1
    <Netmask> is the subnet mask, such as 255.255.255.0
    <Default router> is the IP address of the default router, such as 10.0.0.1
    <DNS Server> is the IP address of the DNS server, such as 10.0.10.2
```

Step 3 Add the option 60 line using the following syntax:

```
option 60 ascii "VCI string"
```

For the *VCI string*, use the value from Table A-1. The quotation marks must be included.

Step 4 Add the option 43 line using the following syntax:

```
option 43 hex <hex string>
```

The *hex string* is assembled by concatenating the TLV values shown below:

Type + *Length* + *Value*

Type is always *f1(hex)*. *Length* is the number of controller management IP addresses times 4 in hex. *Value* is the IP address of the controller listed sequentially in hex.

For example, suppose that there are two controllers with GUI IP addresses 10.126.126.2 and 10.127.127.2. The type is *f1(hex)*. The length is *2 * 4 = 8 = 08 (hex)*. The IP addresses translate to *0a7e7e02* and *0a7f7f02*. Assembling the string then yields *f1080a7e7e020a7f7f02*. The resulting Cisco IOS command added to the DHCP scope is listed below:

```
option 43 hex f1080a7e7e020a7f7f02
```

APPENDIX B

Converting an Autonomous Access Point

This appendix provides instructions for using CCA to convert an *autonomous* AP521 access point into a controller-based (or *lightweight*) LAP521 access point. The appendix contains these sections:

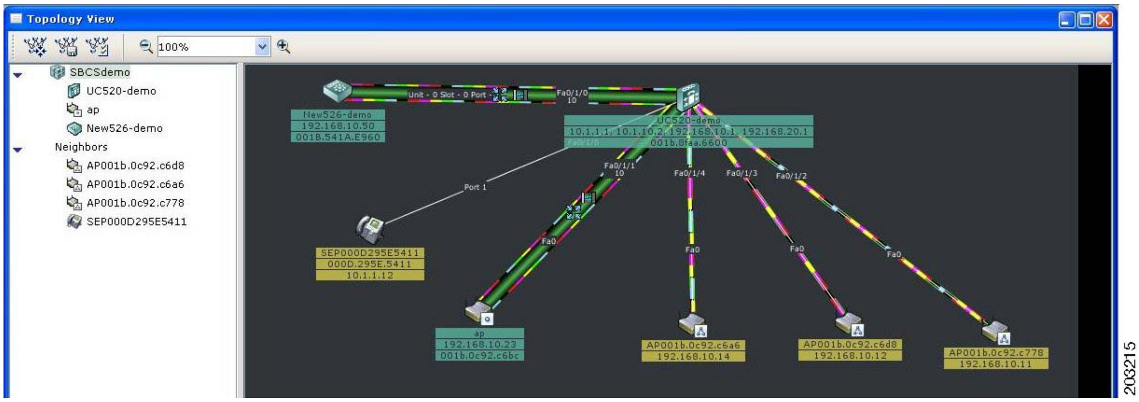
Verifying the Software Version of the AP521 Access Point

Prior to obtaining the conversion image file for your access point, you must verify the software version. To verify the software version of the access point, follow these steps:

Step 1 Check the topology view of your network to ensure an AP521 access point is available (see Figure B-3).

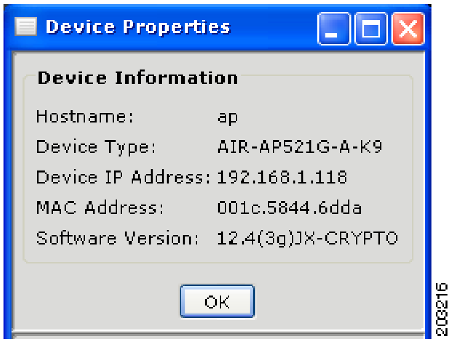
> **Note** An AP521 access point is identified by a circle icon in a small box next to the access point, such as the access point with an IP address of 192.168.10.23 in Figure B-1.

Figure B-1 Topology View Containing an AP521 Access Point



Step 2 Right click on the AP521 access point and choose Properties in the pop-up. Figure B-2 appears.

Figure B-2 AP521 Access Point Properties



Hostname: ap
Device Type: AIR-AP521G-A-K9
Device IP Address: 192.168.1.118
MAC Address: 001c.5844.6dda
Software Version: 12.4(3g)JX-CRYPTO

Step 3 Record the software version of your access point.

Note The access point conversion image must be chosen to match the current software version of your AP521 access point.

Obtaining the AP521 Access Point Conversion Image File

The AP521 access point conversion image file is located on Cisco.com. To obtain the conversion image file on Cisco.com, follow these instructions:

Step 1 Use your Internet browser to access the Cisco Software Center on Cisco.com at the following URL:

http://www.cisco.com/en/US/products/ps7319/index.html

Step 2 Click **Download Software** in the Support box.

Note You must register or be a registered user of Cisco.com to download software.

Step 3 Click **Yes** on the Security Alert pop-up message.

Step 4 Click **IOS Software**.

Step 5 On the Log In page, enter your Cisco.com username and password and click **Log In**.

Step 6 Click **Cisco 500 Series Wireless Express Access Points** under Cisco Mobility Express.

Step 7 Click **Cisco 521 Wireless Express Access Point**.

Step 8 Under Latest Releases, click the software version that matches your AP521 access point, such as **12.4.3g-JX2(ED)** for an access point with 12.4.3g.JX or 12.4.3g.JX2 software.

Step 9 Click **Wireless LAN LWAP RECOVERY**.

Step 10 Click **DOWNLOAD** to obtain the conversion image file.

Step 11 Read and accept the terms and conditions of the Software License Agreement.

Step 12 Click **Save** to download your image file (such as c529-rcvk9w8-tar.124-3g.JX2.tar) to your hard disk.

Step 13 Select the desired download location on your hard disk and click **Save**.

Note Save the copy of the image file to the PC where CCA is installed if you plan to use the **Standard Mode** when converting the access points (see Figure B-6 on page B-5); save the copy to a remote TFTP server if you plan to use **Remote TFTP Server** mode (See Figure B-7 on page B-5).

Step 14 When the download completes, click **Close**.

Step 15 Close your browser.

Using CCA to Convert an AP521 Access Point

CCA can be used to convert an AP521 access point into a lightweight LAP521 access point.

Caution The CCA conversion process is a one-way process. CCA can only convert an AP521 into an LAP521. **CCA cannot reconvert an access point back to autonomous operation**.

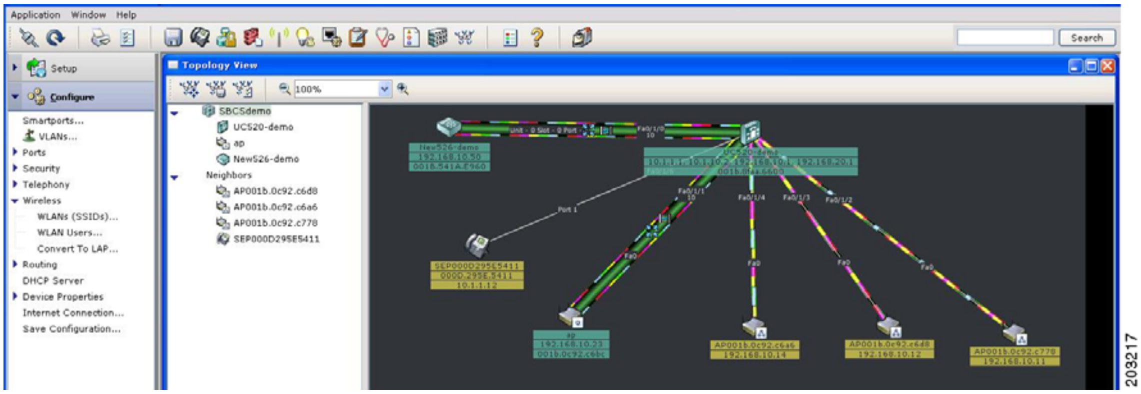
To convert an AP521 using CCA, follow these steps:

Step 1 Check the topology view of your network to ensure an autonomous AP521 is available, such as Figure B-3.

Note An autonomous access point is identified by a circle icon in a small box next to the access point, such as the AP521 with an IP address of 192.168.10.23 in Figure B-3.

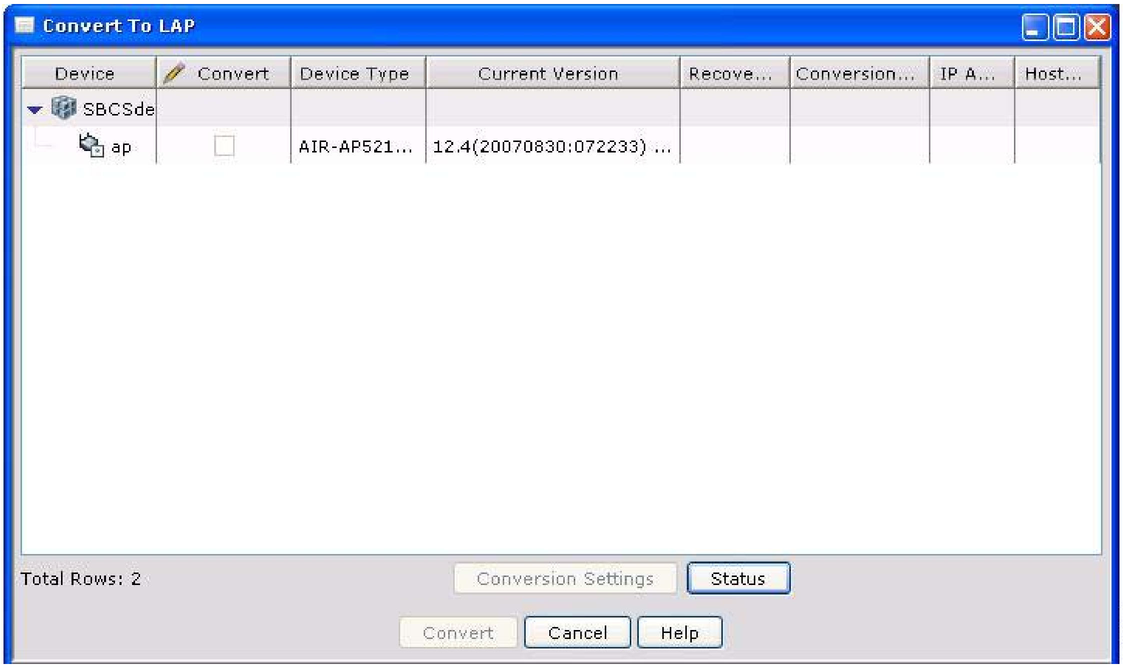
Note An AP521 must be added to the community, before the Convert to LAP option is visible.

Figure B-3 Network Topology View



Step 2 Click **Configure** > **Wireless** > **Convert to LAP** and Figure B-4 appears.

Figure B-4 Convert to LAP Window



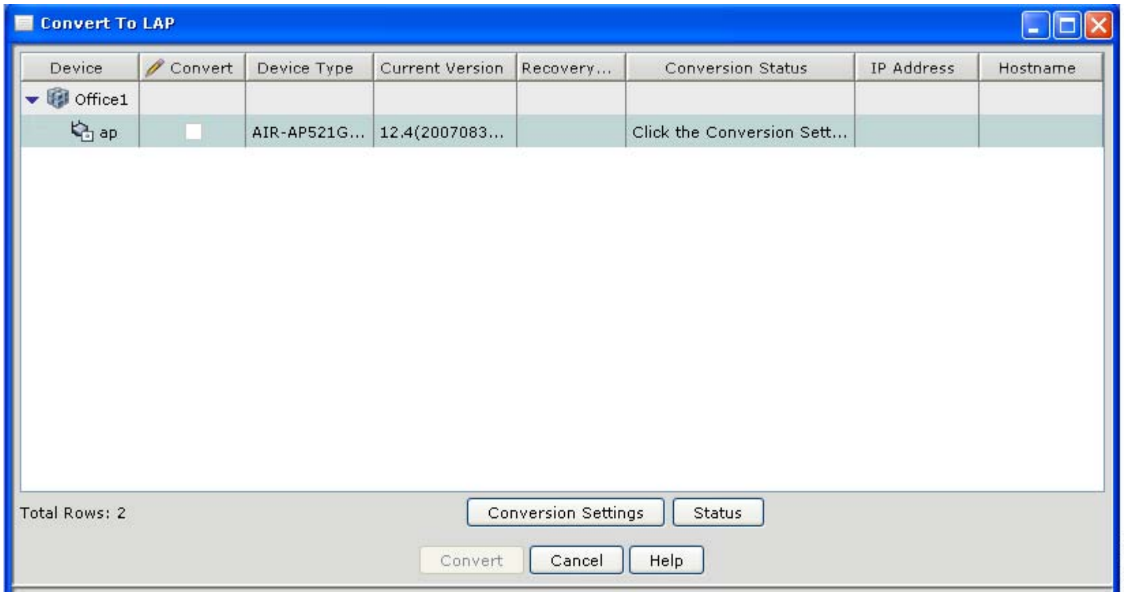
Device	Convert	Device Type	Current Version	Recove...	Conversion...	IP A...	Host...
SBCSde							
ap	□	AIR-AP521...	12.4(20070830:072233) ...				

Step 3 Click on the target access point to highlight the line. Figure B-5 appears.

You can choose multiple AP521 access points by pressing the shift or control key on your PC keyboard while clicking multiple access points.

Note When converting multiple autonomous access points, your DHCP server must be able to handle multiple requests and sessions simultaneously.

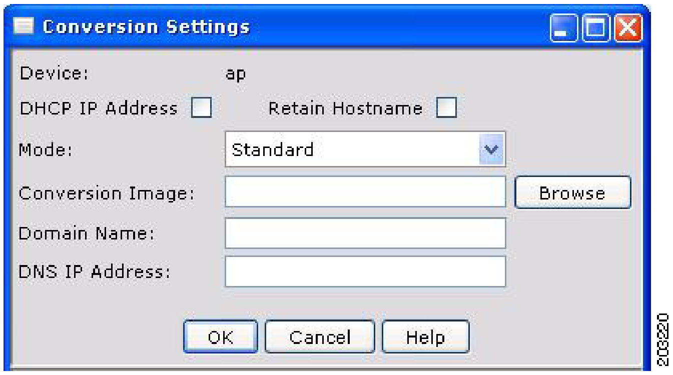
Figure B-5 Highlighted Access Point



Device	Convert	Device Type	Current Version	Recovery...	Conversion Status	IP Address	Hostname
Office1							
ap	□	AIR-AP521G...	12.4(2007083...		Click the Conversion Sett...		

Step 4 Click **Conversion Settings** and Figure B-6 appears.

Figure B-6 Conversion Settings Window



Conversion Settings

Device: ap

DHCP IP Address □ Retain Hostname □

Mode: Standard

Step 5 If you want the converted access point to obtain a new IP address using DHCP, check **DHCP IP Address**.

> **Note** If you check the **DHCP IP Address** box, the Domain Name and DNS IP Address fields will be filled in from the corresponding DHCP server.

Step 6 If you want to keep the access point hostname, check **Retain Hostname**.

Step 7 Click the drop-down arrow in the Mode field and choose **Standard** to use a conversion image that is stored locally on your PC, otherwise choose **Remote TFTP Server** to use TFTP to access a remote conversion image.

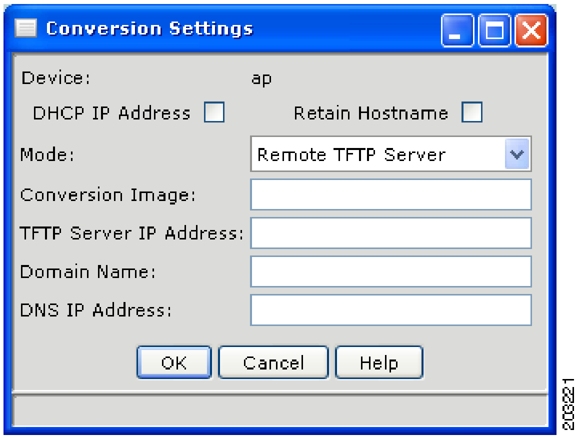
Step 8 If you choose Standard, enter the path and filename for the conversion image in the Conversion Image field or click **Browse** to locate the conversion image file on your PC.

Step 9 If you choose Remote TFTP Server, perform these steps (see Figure B-7):

a. In the Conversion Image field, enter the path and filename for the remote conversion image.

b. In the TFTP Server IP Address field, enter the IP address for your TFTP server.

Figure B-7 Remote TFTP Server Conversion Settings



Conversion Settings

Device: ap

DHCP IP Address □ Retain Hostname □

Mode: Remote TFTP Server

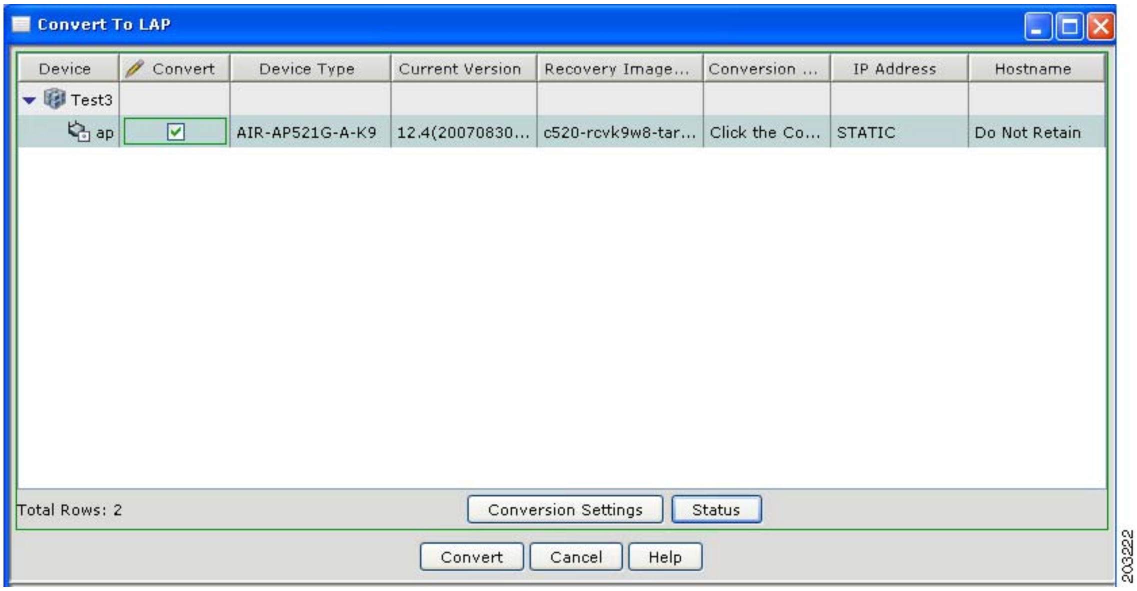
Step 10 In the Domain Name field, enter the domain name for your network (if used).

Step 11 In the DNS IP address field, enter the IP address for your DNS server (if used).

Note If you check the **DHCP IP Address** box, the Domain Name and DNS IP Address fields will be filled in from the corresponding DHCP server.

Step 12 Click **OK** to save your settings and Figure B-8 appears and contains your conversion settings.

Figure B-8 Conversion Setting Information Incorporated



Device	Convert	Device Type	Current Version	Recovery Image...	Conversion ...	IP Address	Hostname
Test3							
ap	☑	AIR-AP521G-A-K9	12.4(20070830...	c520-rcvk9w8-tar...	Click the Co...	STATIC	Do Not Retain

Total Rows: 2

Step 13 Click **Convert** to begin the autonomous access point conversion process. This process will take approximately 1 to 2 minutes per access point to complete.

Note Do not remove power or the Ethernet cable from the access point during the conversion process or the conversion process will be aborted. You can check the conversion status by clicking **Status**.

Step 14 Click **Yes** on the pop-up message indicating that multiple access points can be converted.

Step 15 Click **OK** on the pop-up message indicating that the devices need to be reloaded.

Note The converted access point icon disappears from the topology view until the new software image is loaded from the controller and the LAP521 access point gets an IP address. The process might take a minute or more before the access point appears in the topology as an LAP521 access point.

Note When an autonomous AP521 access point is converted to controller-based operation using the CCA, the access point properties screen continues to indicate that the access point is an AIR-AP521G-A-K9 after the conversion. This is in agreement with the product label on the access point. However, the CCA displays a small triangle icon next to the converted access point to indicate that the access point is now operating as a controller-based LAP521 access point.

APPENDIX C

Deployment Recommendations and Feature List

This appendix provides deployment recommendations and a list of supported and unsupported features for the Cisco 526 Wireless Express Mobility Controller. The appendix contains these sections:

- Deployment Recommendations, page C-1
- Software Feature List for the WLC526 Controller, page C-2

Deployment Recommendations

The Cisco Mobility Express is an integral part of the Cisco Smart Business Communications System (SBCS), and comprises the mobility solution tools, including the WLC526 controller and Cisco 500 series access points. All elements of the SBCS share intuitive GUI-based management tools (such as CCA, Cisco Smart Assist, and Cisco Monitor Director) for quick and easy network setup and network management. These solutions reduce the time and effort required by small and medium businesses (SMBs) to install and operate their network, thus allowing them to focus more time on their core business.

As a targeted solution for small and medium businesses, Mobility Express and SBCS are not designed for mid-market and enterprise deployments. Use Table C-1 to verify that Mobility Express is the correct solution for your business.

Table C-1 Comparison of Cisco Mobility Express and Cisco Unified Wireless Network Solutions

Feature Group	Cisco Mobility Express	Cisco Unified Wireless Network
Target Customer Segment	SMBs (250 employees or less) requiring low deployment costs and minimal management overhead for the wireless functionality that most small businesses need.	Mid-market and enterprise businesses (250 employees or more) who employ IT professionals to administer their network, and require advanced features and customization ability
Management	• Cisco Configuration Assistant (CCA), a GUI-based management system designed for simplicity and practical SMB configurations • Controller web-browser interface (GUI) • Limited command-line interface (CLI) • Remote monitoring with Cisco Monitor Director and Cisco Monitor Director Agent	• Wireless LAN Control System (WCS), a sophisticated network management and monitoring system designed for the CUWN • Controller GUI • Full CLI • Remote monitoring

Table C-1 Comparison of Cisco Mobility Express and Cisco Unified Wireless Network Solutions (continued)

Feature Group	Cisco Mobility Express	Cisco Unified Wireless Network
Scalability / Upgrade path	• Access points can be deployed in autonomous mode for basic wireless connectivity[1] • Add one or two WLC526 controllers to scale and optimize a network with centralized management and advanced features • Advanced mobility services (secure wireless guest access, voice over Wi-Fi) available on demand through CCA	• Scalable from small to very large deployments • Robust interoperability between many IOS-based wireless devices
Capacity	• No limit on unmanaged autonomous access points (up to network capacity) • Manage up to 3 autonomous access points using CCA • Manage up to 6 controller-based access points per controller and 2 controllers per network • 1 mobility group	• Flexible architecture – n+1 scalability • Up to 30,000 access points using Cisco WCS Navigator • 24 controllers per mobility group with 72 controllers per network maximum
Security	• Data encryption • Client authentication	• SNMP support • Data encryption • Client authentication • Intrusion detection and prevention
Roaming	• 2 controllers within the mobility group • Operate in ISO Layer 3 mode	• 24 controllers per mobility group • Operate in ISO Layer 3 mode
Mobility Applications	• Voice over Wi-Fi capability • Guest access configurable through CCA and controller GUI	• Voice over Wi-Fi capability • Guest access configurable through WCS and controller GUI • Location-based services

[1] SBCS 500-series devices are not interoperable with other access points and controllers

Software Feature List for the WLC526 Controller

Table C-2 compares the Cisco Mobility Express (CME) features of the WLC526 controller with the features available on the Cisco Unified Wireless Network controllers.

Table C-2 Cisco Mobility Express and CUWN Wireless Controller Feature Comparison

Wireless Controller Features	CME	CUWN
Feature is supported	X	
Feature is not supported	—	
Cisco Configuration Assistant	X	—

Table C-2 Cisco Mobility Express and CUWN Wireless Controller Feature Comparison

Wireless Controller Features	CME	CUWN
VLAN synchronization	X	—
Controller GUI	X	X
Zero-touch lightweight access point support	X	X
Layer 3 support	X	X
Multiple WLANs	X	X
Multiple VLANs (dynamic interfaces)	X	X
Security: WEP, WPA, WPA2, MAC, ACL	X	X
RADIUS 802.1x authentication	X	X
Voice over WLAN-ready	X	X
WMM support	X	X
Layer 2 and 3 roaming	X	X
Wireless guest user access	X	X
Internal and customizable web portal support	X	X
Lobby admin support (GUI)	X	X
Auto RM support (auto RF)	X	X
Wireless protection policies	X	X
Rogue detection (GUI)	X	X
Multiple countries support	X	X
802.11b/g support	X	X
802.11a/n support	—	X
CLI configuration	limited	X
WCS support	—	X
Location Base services	—	X
Mesh support	—	X
SNMP support	—	X
H-REAP support	—	X
Local EAP	—	X
Internal DHCP server	—	X
Wired guest user access	—	X
AP monitor/sniffer mode support	—	X
Intrusion protection services	—	X
Multicast support	—	X
Third-party security certificate support	—	X

INDEX