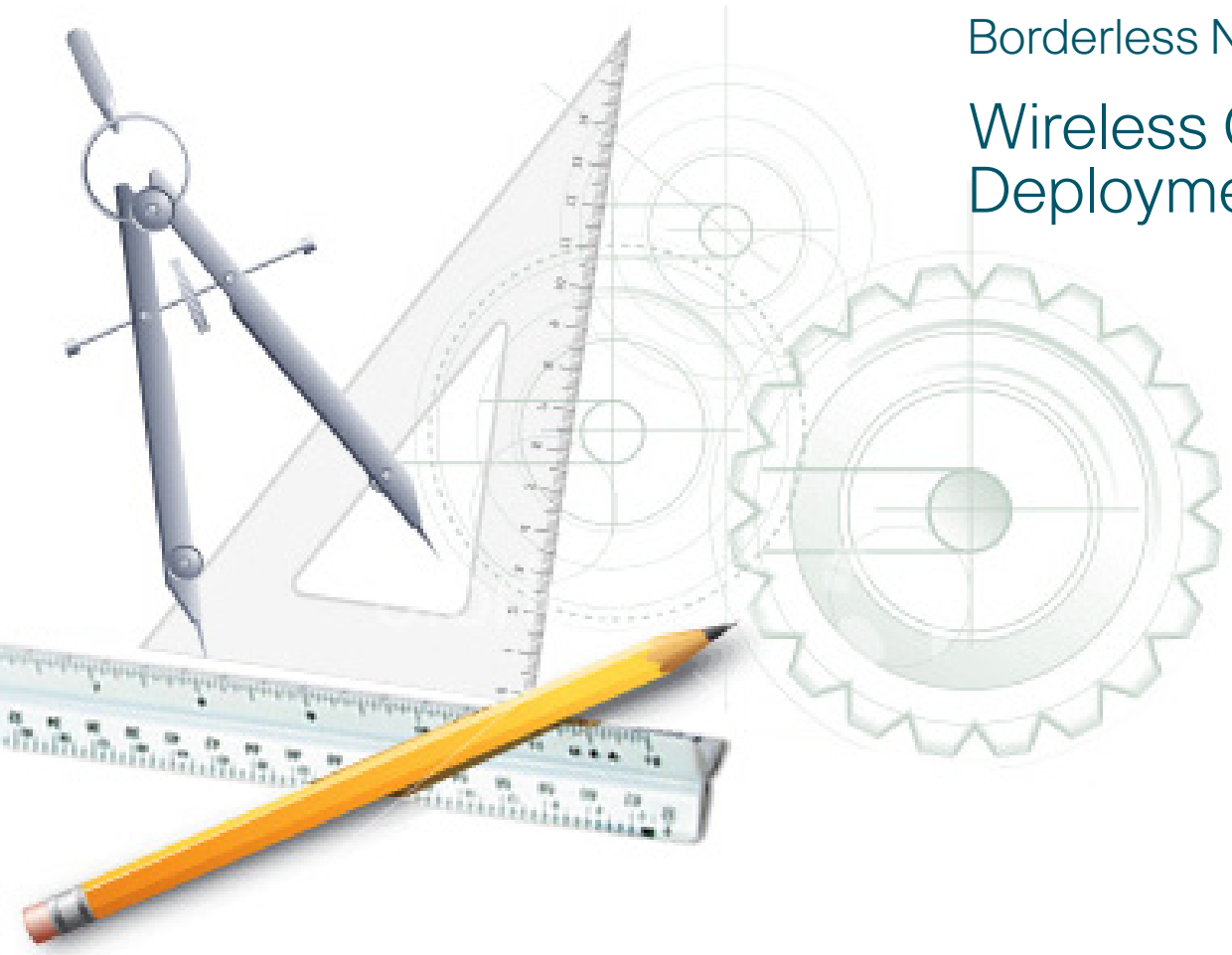


Smart Business Architecture

Borderless Networks for Enterprise Organizations

Wireless CleanAir Deployment Guide

Revision: H2CY10

Table Of Contents

This document is for the reader who:

- Wants a general understanding of Radio Resource management.
- Understands the challenges of the unlicensed Radio Spectrum.
- Has already read the Smart Business Architecture Foundation for Enterprise Organizations Deployment Guide and is looking for a Wireless Network Management Solution.
- Has an existing network and needs guidance on how to add Wireless and Radio Spectrum Management.
- Wants to better understand how to react to unforeseen Wireless Network challenges.

Who Should Read This Guide

This guide should be of interest to anyone in an enterprise organization who wants to understand the benefits of using the Wireless Network Management, Cisco's Wireless Control System (WCS), and the Wireless Control System Navigator offerings, to learn how to choose among them, and to find out how to purchase one of these products.

The audience also includes technology resellers who want to understand more about the Cisco Wireless offerings and to learn how to become a Cisco Wireless authorized partner.

This guide does not require any specific technical background other than gen-eral computer experience.

Using this Collaboration Guide

This guide is a concise reference on Wireless Network Management and is organized into the following sections:

The **Introduction** outlines the issues the Cisco Wireless Control System and Navigator can solve within your organization and the capabilities it provides to solve them.

The **Technology Overview** section introduces Cisco Wireless Control System and describes how it is delivered as Software as a Service (SaaS).

The **Cisco Wireless Control System (WCS) and Navigator Solutions Overview** section discusses the various Wireless Network Management solution offerings, the differences between them, and how to decide which one is right for you.

How to Get Cisco Wireless Control System points you to the correct resource to order Cisco WCS or Navigator for your organization.

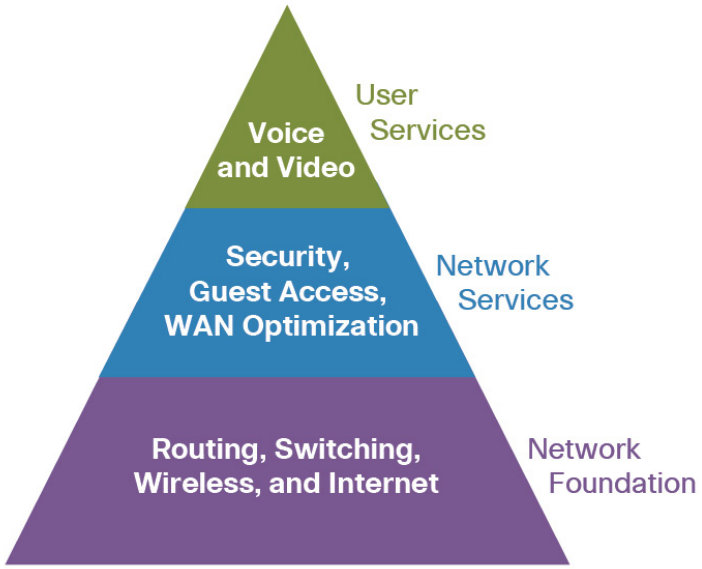
Additional Information

This guide is a companion document to the Borderless Network Architecture for Enterprise Customers Design Guide and Deployment Guide.

The Cisco Borderless Architecture for Enterprise Customers is a prescriptive architecture that delivers an easy-to-use, flexible, and scalable network with wired, wireless, security, WAN optimization, and unified communication com-ponents. The architecture eliminates the challenges of integrating the various network components by using a standardized design that is reliable and has comprehensive support offerings.

The Cisco Smart Business Architecture for Enterprise Customers is designed to address the common requirements of organizations with 2000 to 10000 employees. Each organization is unique, however, and so are its requirements. Because of that, the Cisco Borderless Network Architecture was built so that additional capabilities could be added without redesigning the network.

Figure 1. Network Services, Services and Foundation



One way that the Cisco Borderless Network Architecture accomplishes this extensibility is by breaking down the architecture into three primary layers: **Net-work Foundation, Network Services,** and **User Services.** See Figure 1.

The Cisco Wireless Control System is a User Service. User Services are the services or applications we use everyday and interact with directly. They range from picking up the phone to use the phone service, to reading our email using the email service. How well a User Service interacts with the Network Service impacts how it performs when a user actually uses it, which makes Wireless Network management an imperative for a healthy network.

Reliable Network Services provided by the Cisco Smart Business Architecture such as the Internet connection, WAN infrastructure, and security help ensure a business can rely on applications such as web conferencing for critical collaboration.

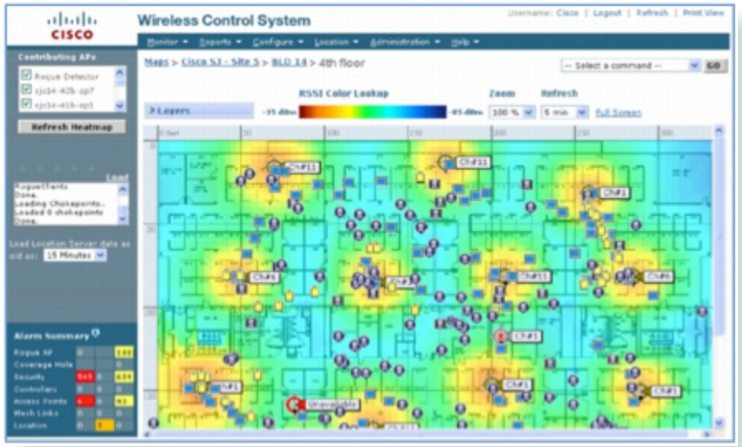
To learn more about Cisco Borderless Network Architecture, visit:
http://www.cisco.com/go/smartarchitecture or
http://www.cisco.com/go/partner/smartarchitecture

Business Overview

The challenges of running a wired data network are beyond the expectations of most other jobs. The challenges go beyond simply adding a machine and handing it over to the desktop IT department or to the end user to leverage as they desire. With the numerous challenges that arise with any application, the network is always the easiest entity to blame for failure. Now add a wireless data network to the picture and the challenges and skill set required to maintain and troubleshoot the network triple. Wireless networking brings a new set of unknowns that a wired network never had to address.

The Cisco Wireless Control System (WCS) with CleanAir Technology allow the Network Administration IT staff to visually see how well their network is performing, troubleshoot client connectivity remotely, manage wireless network resources, and analyze interference devices from anywhere in the world and more. The real power of Cisco WCS with ClearnAir combined with CleanAir access points is the ability to visually represent the radio environment to the network administrator to better manage and troubleshoot issues before they become issues.

Figure 2. WCS Heat Map



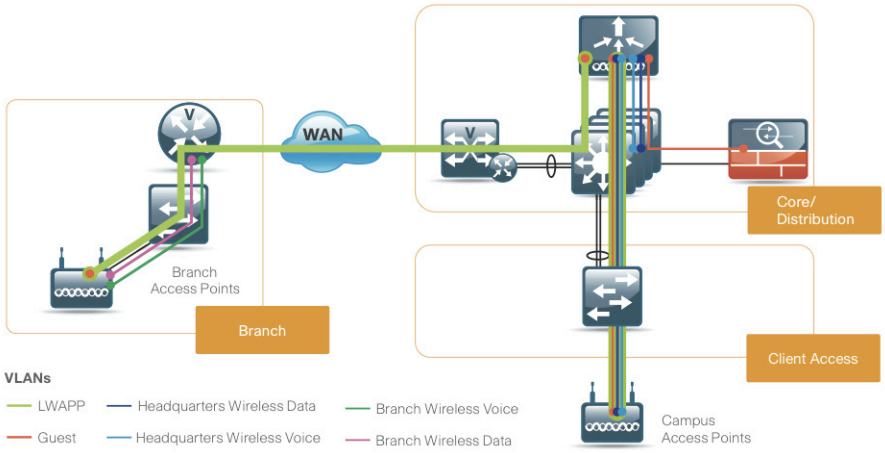
Radio is the manipulation of the magnetic field that is invisible to the naked eye. Without running expensive site surveys with a spectrum expert every hour and minute of every day, the network administrator cannot tell what is happening in the user space. The Wireless Control system collects the data from all the Wireless LAN Controllers (WLC) in the network, while each CleanAir access point does a spectrum sweep of the environment and alerts the administrator of any potentially negative issue before a user creates a call ticket in the network call center.

The CleanAir Access Point

Unlicensed bands need to be proactively managed. Wi-Fi is no longer a convenience technology used for casual web surfing or simple connectivity from conference rooms. With 802.11n, wireless performance is now on par with wired networks where businesses as well as hospitals rely on the wireless network for mission-critical and patient-critical applications. With limited IT resources, lack of tools, and lack of RF expertise, the CleanAir access point with Integrated Spectrum hardware can fill the RF expertise gap and limit or eliminate network downtime.

With Event Driven Radio Resource Management, an issue within the wireless radio network can be identified and mitigated without any user interaction. Alerts can be sent out via email as well as through syslog to make the network IT staff aware of the mitigated issue and alert them to watch for other issues, enforce the company radio policy, or do both.

Figure 3. Simplified Network Diagram



Technology Overview

Cisco CleanAir Technology

Cisco CleanAir is the integration of Cisco Spectrum Expert technology with a Cisco access point. Before Cisco CleanAir was available, operators had to walk around with an instrument to detect chosen signals and physically locate the device. Cisco CleanAir helps to automate these tasks within the system management function by adding additional intelligence over Spectrum Expert, and thereby augmenting the overall experience by proactively reclaiming control over the spectrum.

The components of a basic Cisco CleanAir technology are the Wireless LAN Controller and the Cisco 3500 Series access points. To take advantage of the entire Cisco CleanAir feature, the Cisco WCS can display in real time the data retrieved from Cisco CleanAir. Adding the Mobility Services Engine (which is addressed in a separate guide) further enhances the available features and provides the history and location of specific interference devices.

Wireless Control System

Cisco WCS enables you to configure and monitor one or more controllers and associated access points, to monitor and troubleshoot radio technology, and to visually display Cisco CleanAir data to the network administrator. Cisco WCS includes the same configuration, performance monitoring, security, fault management, and accounting options used at the controller level and adds a graphical view of multiple controllers and managed access points.

Cisco WCS runs on Windows 2003/SP2, Windows 2003 R2/SP2 32-bit installations, and Red Hat Linux Enterprise Server 5.0 32-bit installations. On both Windows and Linux, Cisco WCS runs as a service, which runs continuously and resumes running after a reboot. The configuration in this guide runs the Windows 2003 Operating System within a virtual machine and leverages VMware ESXi 4.0 within the data center.

Mobility Services Engine

The Mobility Service Engine (MSE) can run multiple related or independent services such as location and wireless IDS/IPS services, the CleanAir database functionality, as well as future services. The MSE is an independent appliance and is leveraged by the Cisco WCS. The MSE and the services it supports are discussed in another supplemental guide.

Location or Context-Aware

The Cisco location service solution (also referred to as the context-aware service) provides the capability to determine the physical location of a tracked entity in the network and additional contextual information such as the serial number of the tracked entity. The tracked entity can be a wireless endpoint, a wired endpoint (a phone or PC), a wired switch, or a wireless controller. Location information is critical for wired endpoints. For example, a phone in the lobby of an office building can have different policies from a phone in a conference room or in an employee office. Today, the policies are statically administered based on the MAC address and not based on the location of the endpoint itself. Knowing the location of a wired entity provides additional intelligence to push the right set of policies to tracked devices based not only on the user's credentials and MAC address, but also on the location of the device. This document does not cover the location service solution; this information is presented in a different supplemental guide.

Configuration Details

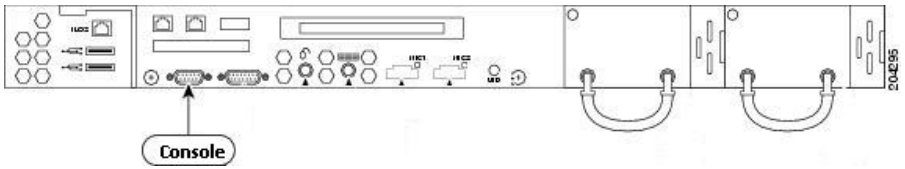
This Cisco Wireless Control System requires having Windows 2003 Server loaded, and within the SBA architecture, we have loaded Windows 2003 Server on a VMware ESXi 4.0 platform. This document leverages the standard server configuration that supports up to 2000 Cisco Aironet lightweight access points, 1000 standalone access points, and 450 Cisco wireless LAN controllers. A low-end server can support up to 500 Cisco Aironet lightweight access points, 200 standalone access points, and 125 Cisco wireless LAN controllers. This information can help you determine your network needs and future growth. No matter what your organization requires, it is the same Cisco Wireless Control System software that runs on different hardware, as described in the product Release Notes.

Install the Mobility Service Engine

The Mobility Solutions Engine (MSE) can be leveraged within the CleanAir solution to create an Interference History. Many issues that occur in the day-to-day operations of a Wireless Network are intermittent and often hard to track down. Leveraging the power of the MSE, you can track an issue by the time of day and build upon the historical data that can help mitigate these difficult, if not impossible, network interference devices.

Initial Configuration of the MSE

Step 1: Connect your console cable to the console port of the MSE.



Step 2: Power on the Mobility Services Engine.

Step 3: Follow the on-screen prompts and provide the following required information in this order:

1. Hostname
2. IP address
3. Network mask
4. Default gateway
5. DNS server IP address
6. Login banner
7. SSH password

(WCS Username and Password is used by the WCS for secure communication)

8. WCS communication username
9. WCS communication password (which must have two uppercase and two lowercase characters, two digits, and two special characters to be accepted)

Provide the following optional information:

1. NTP server IP address
2. Second Ethernet IP address

List of Procedures for a Successful WCS Deployment

This section lists the tasks that must be completed for a successful deployment.

1. Installation
   a. Install Cisco Wireless Control System on a VMware ESXi 4.0 virtual machine
2. Licensing
   a. Install the appropriate license to bring Cisco WCS online
3. Wireless LAN controller
   a. Add Wireless LAN controller(s) to Cisco WCS
4: Add Mobility Service Engine to Wireless Control System
5. Building and Floorplan
   a. Add the building or site to Cisco WCS
   b. Add individual floorplans to each building
   c. Place each access point on the floorplan map
6. Configuring the Cisco Wireless Solution for CleanAir
   a. Enable Event-Driven Radio Resource Management

Procedure 1: Installation

The installation steps outlined in this section are typical for most applications and perhaps intuitive to most users. With every installation, knowing up front what you need to have ready is essential for a quick and easy installation experience. With the Cisco Wireless Control System, planning the hostname ahead of time when building the machine makes for a logical and easy-to-troubleshoot network. For the actual installation of the Cisco Wireless Control System service, keep the following information handy for a smooth installation process.

1. HTTP, HTTPS, and health monitor port information
   a. We will use the default ports, however, consult your security policy to be sure your company policy is to use default ports
2. Root password
3. FTP file folder on local machine
4. TFTP file folder on local machine
5. Installation folder (a default folder will be chosen under Program Files)

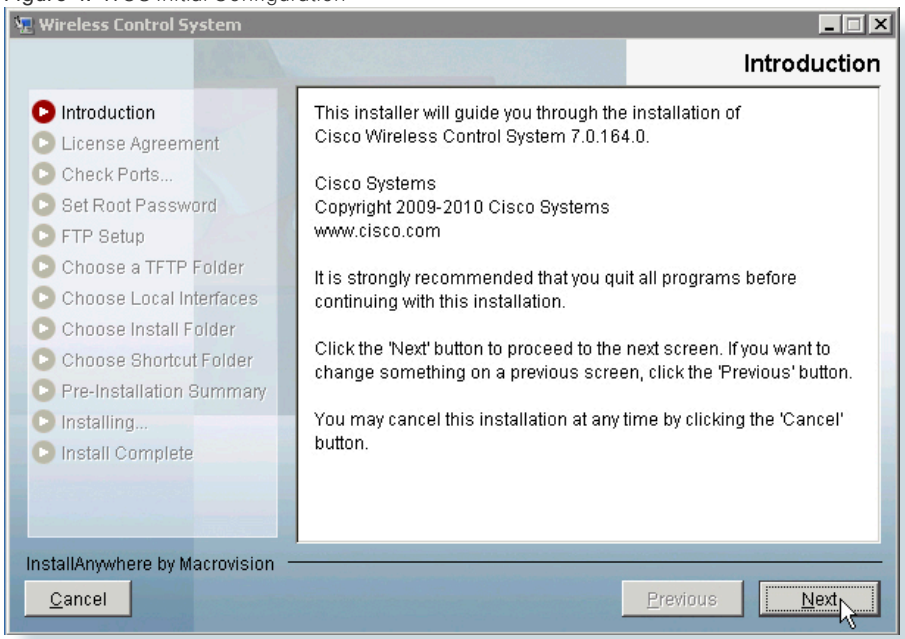
Run Application

Double-click the Cisco WCS application that you downloaded from Cisco.com. It should have a name similar to the following:

```
WCS-STANDARD-K9-7.0.164.0.exe
```

You see the introductory screen as shown here.

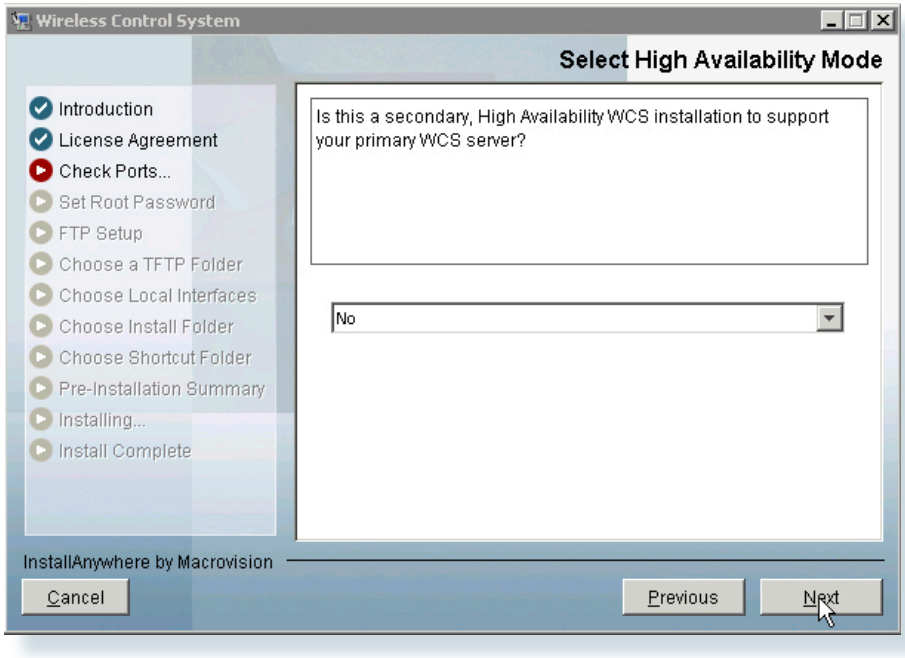
Figure 4. WCS Initial Configuration



The introduction summarizes the application you downloaded and prompts you to move to the next screen. You must accept the license agreement and click **Next**.

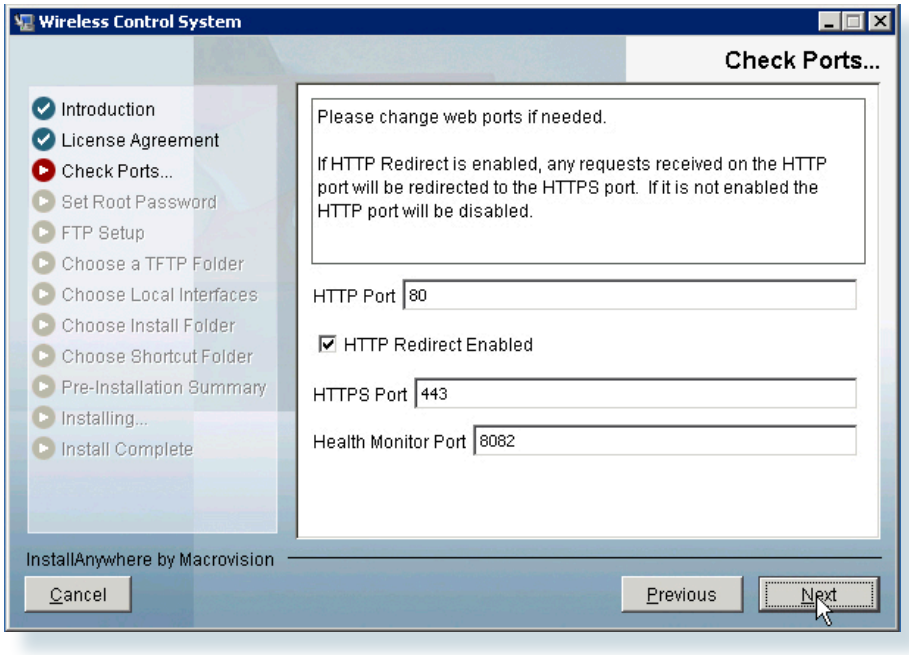
The installer checks for any previous installations. It asks if this installation is for High Availability or is being built as a secondary WCS. We do not set up a secondary or High Availability installation in this guide; however, you can do this simply by repeating this installation and selecting **Yes**.

Figure 5. High Availability Mode Selection



The next two screens prompt you to either accept the default ports or assign alternative ports for access services on your Cisco WCS. Unless your security policy specifies something different, click **Next**.

Figure 6. Port Configuration

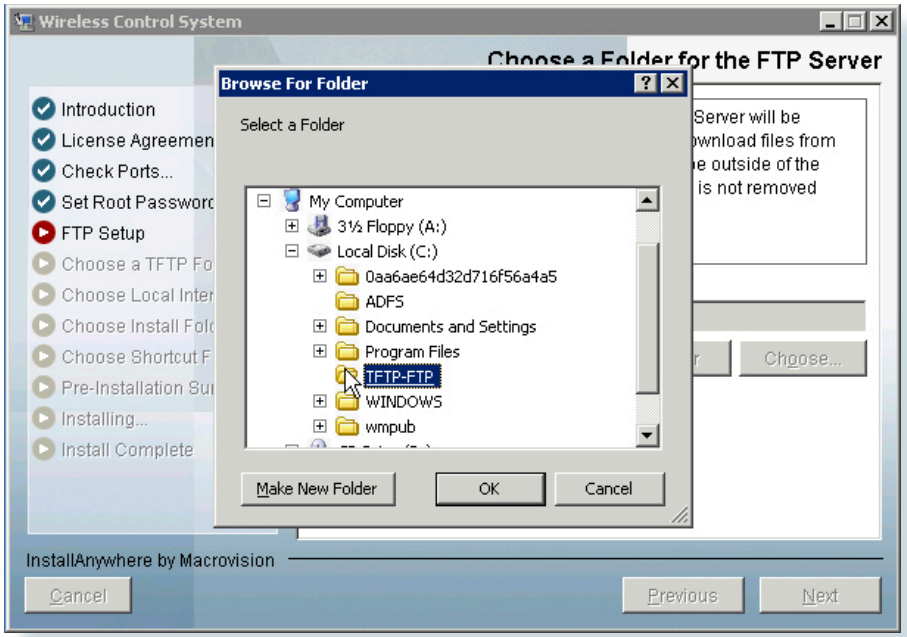


You must define the root password next. This password is the locally defined administration password. The password will be checked for strength; however, password strength should follow your security policy. The root password is only used for the local administrator.

Figure 7. Root Password

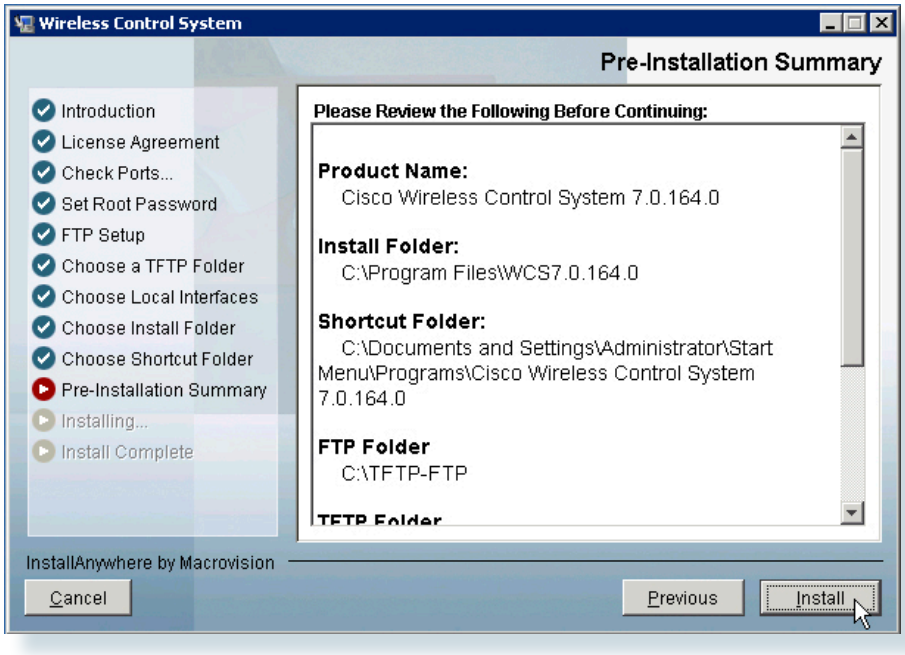
Choose your FTP folder, TFTP folder, and the installation folder on the local machine for WCS. As a pre-check, we created an FTP folder and a separate TFTP folder for this function and allowed the default folder for the Cisco WCS installation.

Figure 8. File Folder Selection



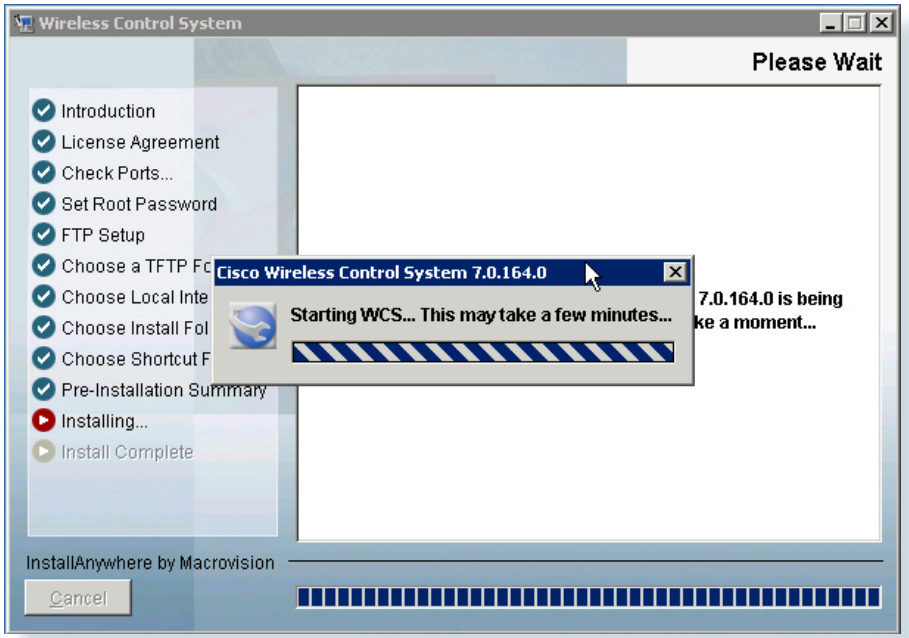
Click **Next** on the installation icon folder options to get to the installation summary. Review your choices before the installation begins.

Figure 9. Installation Summary



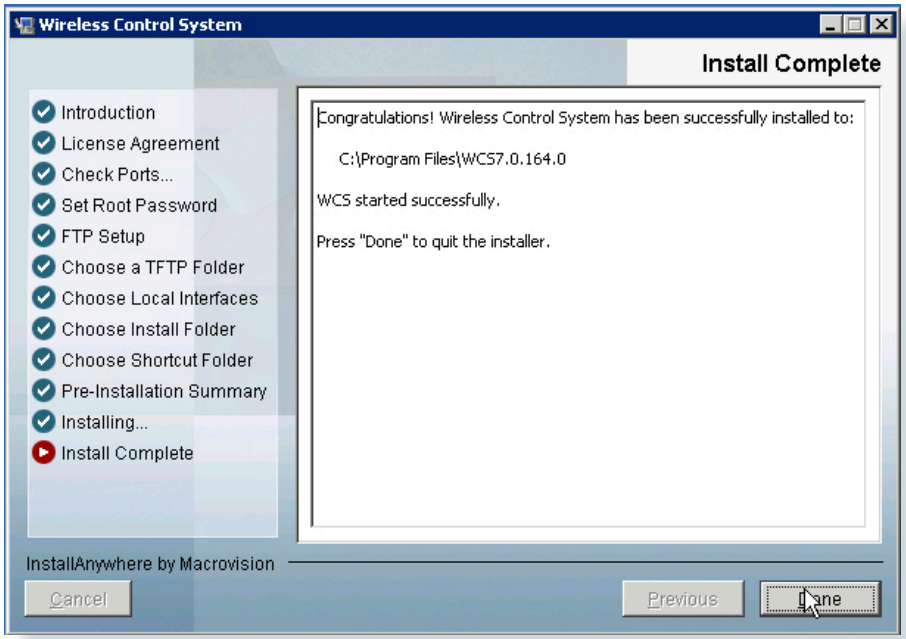
Once the installation completes, you can start Cisco WCS services.

Figure 10. Starting WCS for the First Time



Click **Done** to close the installation application. You are now running Cisco WCS.

Figure 11. Installation Complete



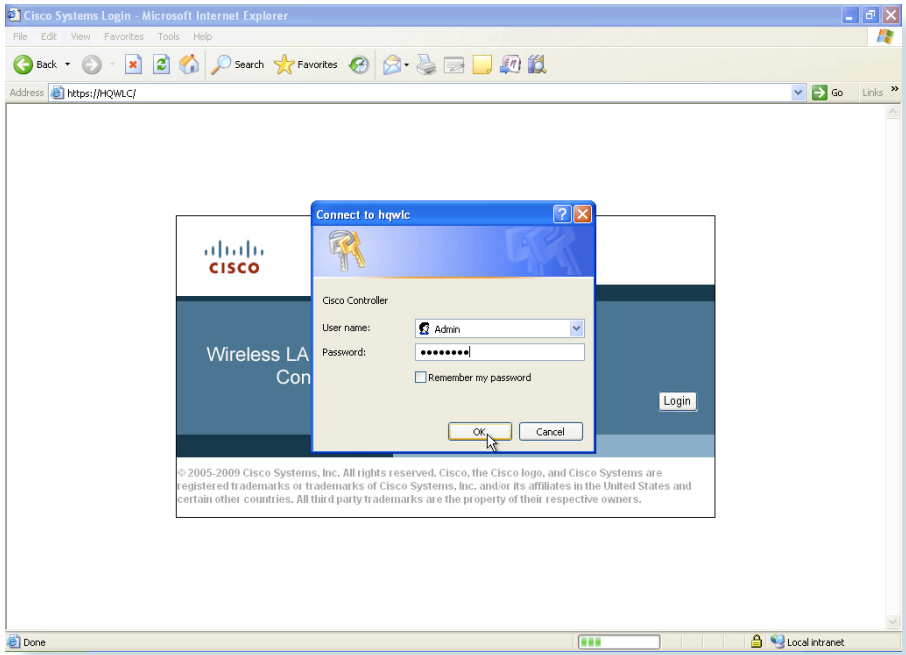
Procedure 2: Licensing

Cisco Wireless Control System (WCS) is licensed by the number of access points and services you desire. For this guide, we upload a license that includes Spectrum Intelligence as a service and 250 access points

Summary of Steps to Install the License

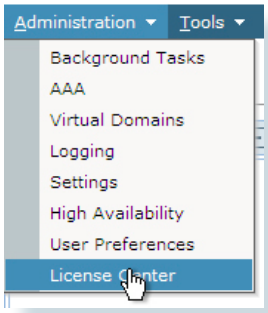
1. Save the license file (.lic) to a temporary directory on your hard drive. (You will receive an email from Cisco with an attached license file.)
2. Open a browser and in the location or address field, enter the following URL and replace the IP address with the IP address or host name of the Cisco WCS server: https: // <IP address>. In our example, we have Cisco WCS installed at 10.4.200.19
   https:// 10.4.200.19
3. Log into the Cisco WCS server as system administrator. (Be aware that usernames and passwords are case-sensitive.)

Figure 12. WCS Login Screen



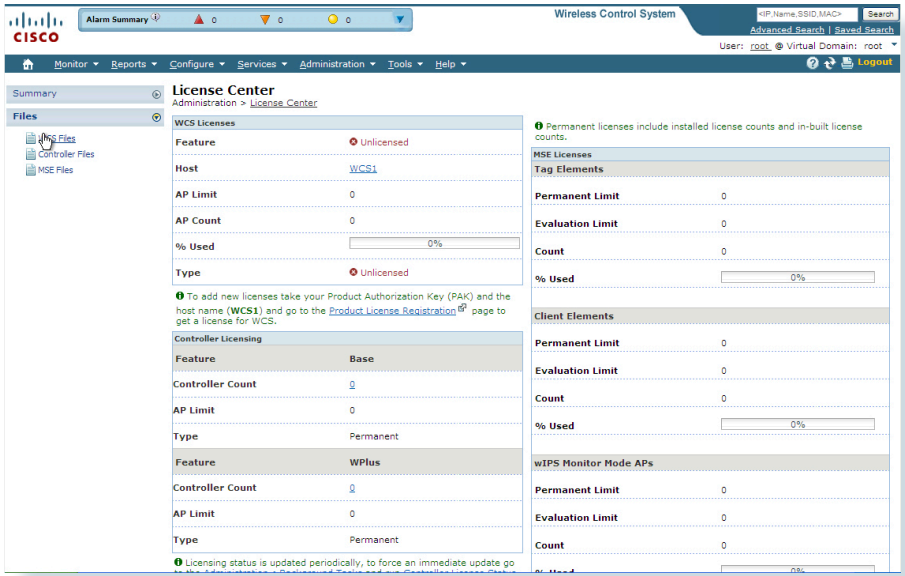
4. From the **Administration** menu, select **License Center**.

Figure 13. Navigate to License Center



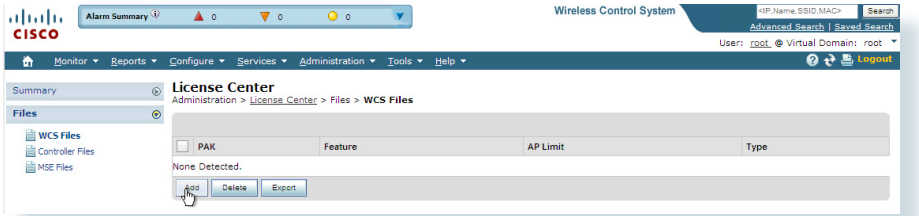
5. On the right, select **Files** and then select **WCS Files**.

Figure 14. License Center, Add PAK



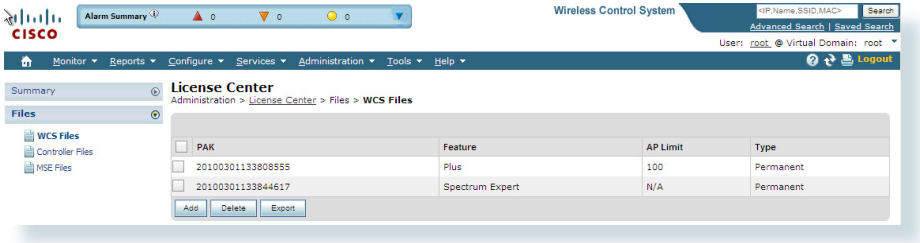
6. Under **PAK**, select **Add**, and click **Choose File** to navigate to the location where you saved the .lic file.

Figure 15. Add New PAK



7. Click **Upload**. The Cisco WCS server then imports the license.
8. Repeat this step for each additional license you have received.

Figure 16. Importing License Files



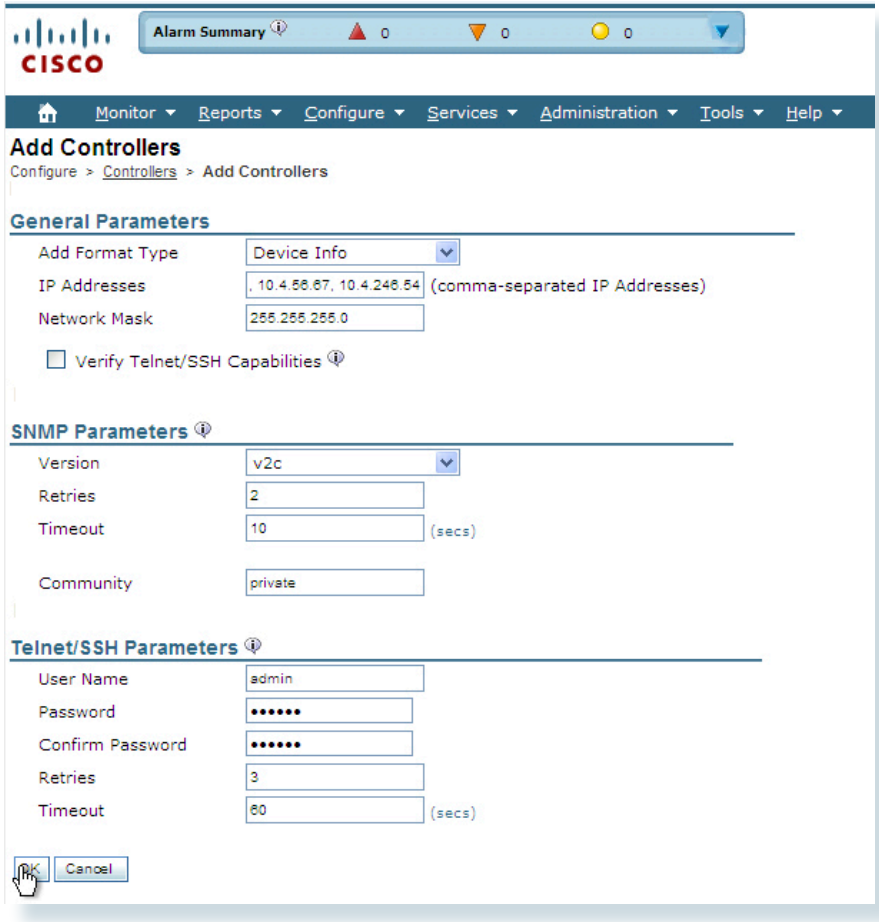
Once completed, all your license files should appear as shown in Figure 15. To verify that your license files do indeed provide the access point count and the services you ordered, return to the **Administration** menu and select **License Center**. We uploaded both Spectrum Intelligence as a service and as a single 100AP license as shown in Figure 16.

Procedure 3: Add Wireless LAN Controller(s) to Cisco WCS

Each controller must be added to Cisco WCS so the network can be monitored and centrally managed. This process is very simple, but necessary.

Navigate to **Configure** and then to **Controllers**, which should bring you to an empty list of controllers as shown in Figure 17. From the drop-down list on the right, select **Add Controllers...** and click **Go**. You are prompted to enter the Controller(s) IP address(es). (Enter all your controller IP addresses separated by a comma as shown in this example: 10.4.56.64, 10.4.56.65, 10.4.56,66, 10.4.246.54.) Use the default settings for all other parameters including the Telnet/SSH password.

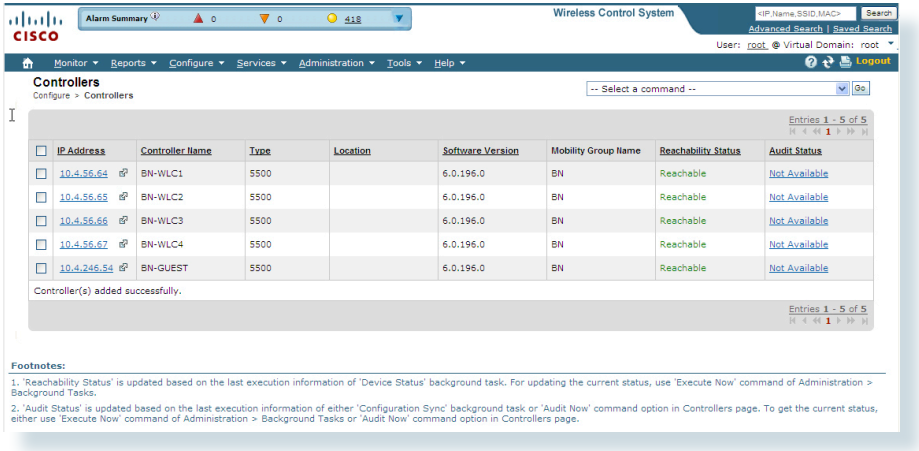
Figure 17. Add Controllers



NOTE: You may enter every controller IP address separated by a comma, or you can select a comma-delimited (CSV) spreadsheet with the IP addresses of your controllers. In our example, we selected a single controller by IP address to allow for clarification.

Click **OK**, which tests for connectivity to each controller you have specified and provides you with a list of your controllers, their hostname, and an indication if they are reachable as shown in Figure 18.

Figure 18. List of Controllers



IP Address	Controller Name	Type	Location	Software Version	Mobility Group Name	Reachability Status	Audit Status
10.4.56.64	BN-WLC1	5500		6.0.196.0	BN	Reachable	Not Available
10.4.56.65	BN-WLC2	5500		6.0.196.0	BN	Reachable	Not Available
10.4.56.66	BN-WLC3	5500		6.0.196.0	BN	Reachable	Not Available
10.4.56.67	BN-WLC4	5500		6.0.196.0	BN	Reachable	Not Available
10.4.246.54	BN-GUEST	5500		6.0.196.0	BN	Reachable	Not Available

To Audit the Controller immediately, select the hyperlink next to your controller initially labeled **Not Available** and then click **Audit Now**.

Upgrade Controllers for CleanAir Support

CleanAir software support for the 3502 access points and the integrated Spectrum Expert hardware begins with 7.0.98.0 or later. Managing multiple controllers with Cisco WCS is important and the ability to upgrade all five controllers simultaneously shows the true power of the Cisco Wireless Control System, this upgrade process can be then scheduled and streamlined to maximize network uptime.

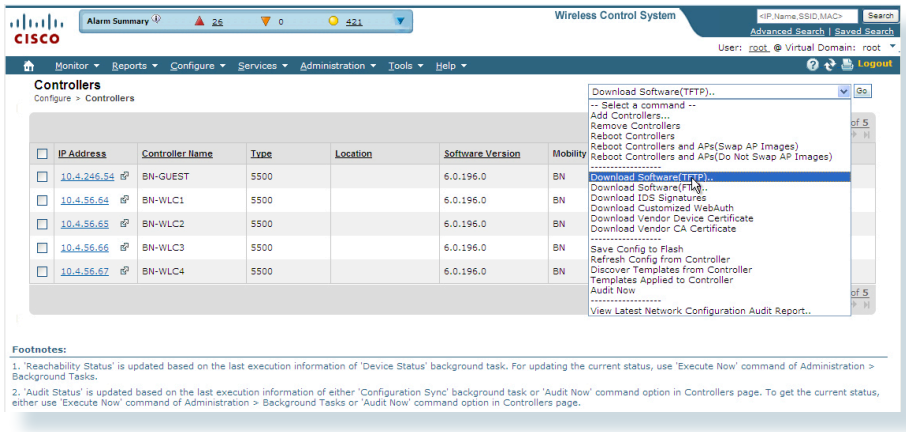
Step 1: Log into Cisco WCS

Step 2: Navigate to **Configure > Controllers**.

Step 3: Select **All Controllers**.

Step 4: From the drop-down list at the right, select **Download Software (TFTP)** and **Go**.

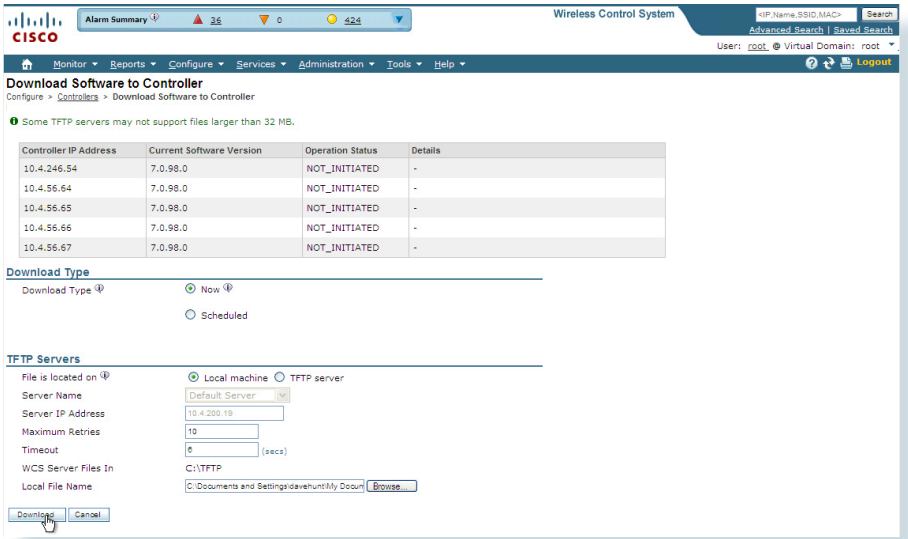
Figure 19. Download Software via TFTP



Step 5: Answer the software controller prompts:

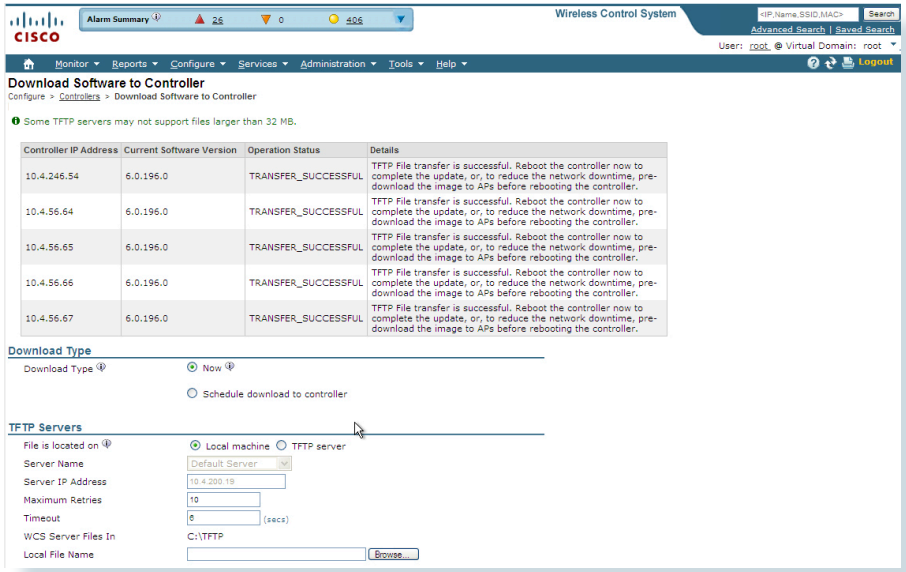
1. Keep **Download Type Now** Selected.
2. Keep **File is located on ... Local Machine** Selected.
3. Leave **Maximum Retries** and **Timeout** at their default values.
4. From **Browse**, select the file **AIR-CT5500-K9-7-0-98-0.aes** and click **OK**.
5. Click **Download**.

Figure 20. Download Software to All Machines



Once the file is uploaded to every controller, you must reboot these controllers. You can do the reboot process all at once, which does not allow traffic during the upgrade, or you can schedule your controllers to reboot in a logical fashion to keep wireless connectivity available during this change opportunity.

Figure 21. Transfer Complete, Reboot Controller to Continue



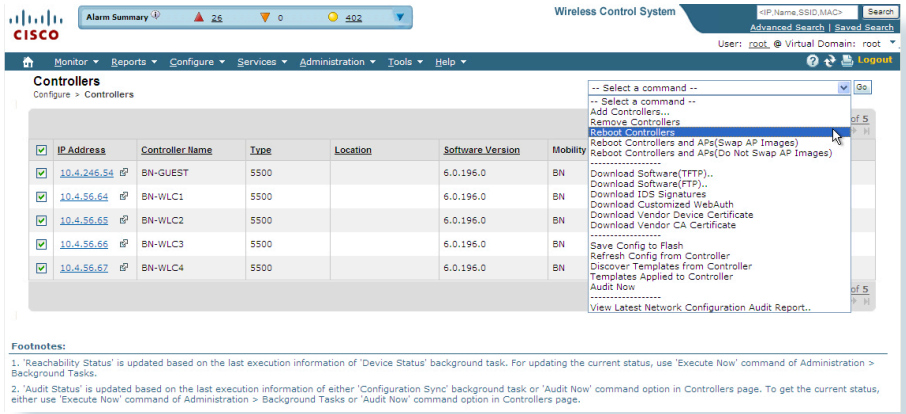
Step 1: Log into Cisco WCS.

Step 2: Navigate to **Configure > Controllers**.

Step 3: Select **All Controllers**.

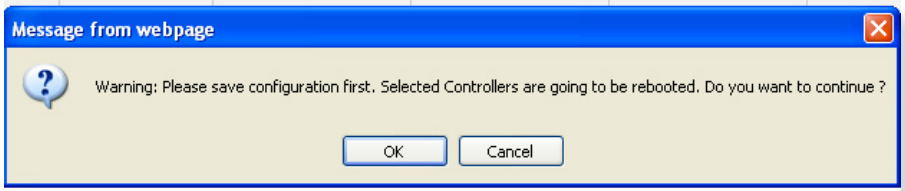
Step 4: From the right drop-down list, select **Reboot Controllers**.

Figure 22. Reboot Controller



Step 5: Click **OK** to the Warning "**Warning: Please save configuration first. Selected Controllers are going to be rebooted. Do you want to continue?**"

Figure 23. Warning: You Are About to Reload Your Controller!



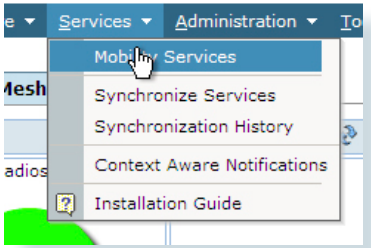
Procedure 4: Add the Mobility Service Engine to the Wireless Control System

You must add the Mobility Service Engine to the Wireless Control System. Using the WCS Comunication username and password that you used earlier will allow Cisco WCS to poll the MSE database for historical context information. At a later time, Wireless Intrusion Prevention System services can be added if needed.

Step 1: Log into WCS.

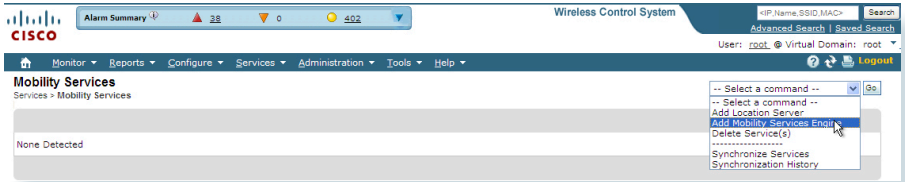
Step 2: Navigate to **Services > Mobility Services**.

Figure 24. New Mobility Service



Step 3: From the drop-down list, select **Add Mobility Services Engine** and click **Go**.

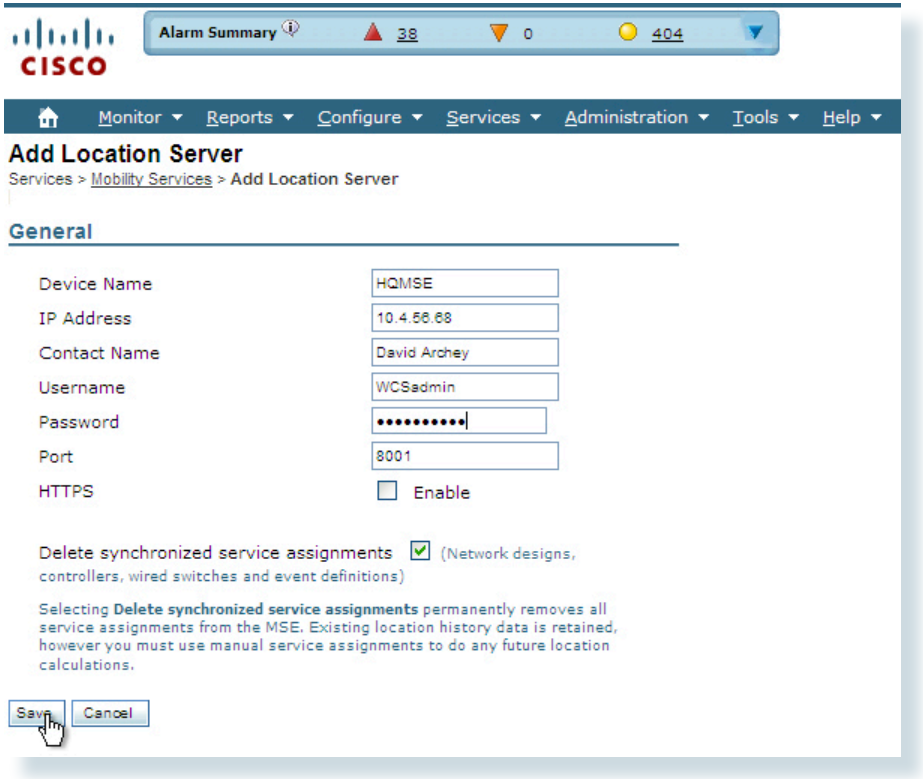
Figure 25. Add Mobility Service Engine



Step 4: Enter the following information and click **Save**:

1. Device name
2. IP address
3. Contact name
4. Username (WCS communication username)
5. Password (WCS communication password)
6. Port (accept the default)

Figure 26. Define New MSE and Communication Credentials



Step 5: Check the **Context Aware Service** check box and click **Save**.

Figure 27. Select Mobility Engine Services

Procedure 5: Building and Floor Plan

The real advantage to any management system is the presentation of the information, which you can then use to make informed decisions. The Cisco Wireless Control System brings visibility to the radio spectrum, which allows the administrator to see the coverage that is provided to the users. Including the building and floorplans in Cisco WCS creates the visibility to this otherwise unknown or convoluted data that the network provides.

Adding the First Campus and Building

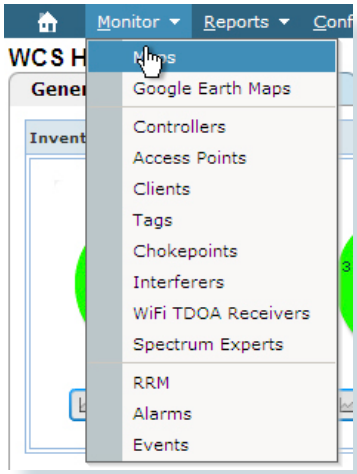
Every organizational method starts by categorizing the approach; with the Cisco Wireless Control System, the approach is familiar. Even though you may only have one building today, you may end up with another building, or perhaps each Campus is a single building today, but could have more buildings tomorrow. The campus, building, floor approach makes it easy to understand as you dig for more information and peel away the layers to find what you are looking for.

NOTE: You need to know the dimension of the campus picture you are bringing into the system so that you can scale the drawing appropriately as each building and floor are added.

Step 1: Log into the Wireless Control System.

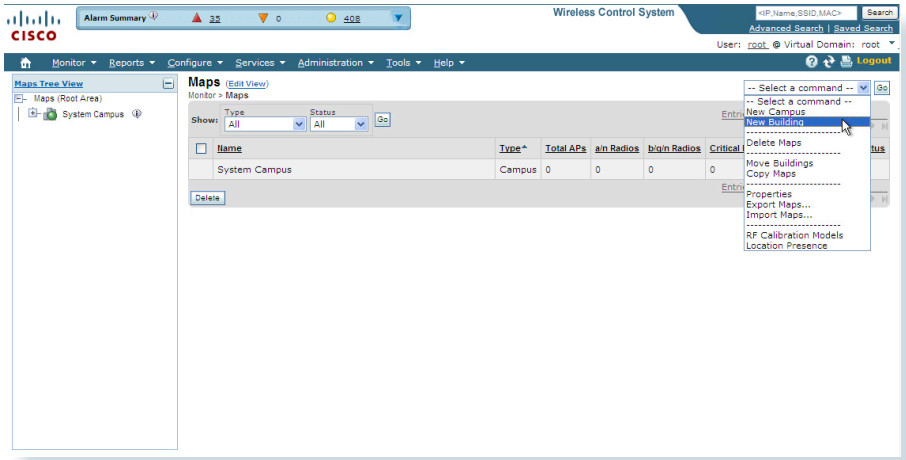
Step 2: Navigate to **Monitor > Maps**.

Figure 28. Finding Building Maps



Step 3: From the drop-down list, select **New Building** and click **Go**.

Figure 29. New Building



Step 4: Create name, contact name, and characteristics of the building:

Building Name: BN-Headquarters

Contact: Ben O'Brien

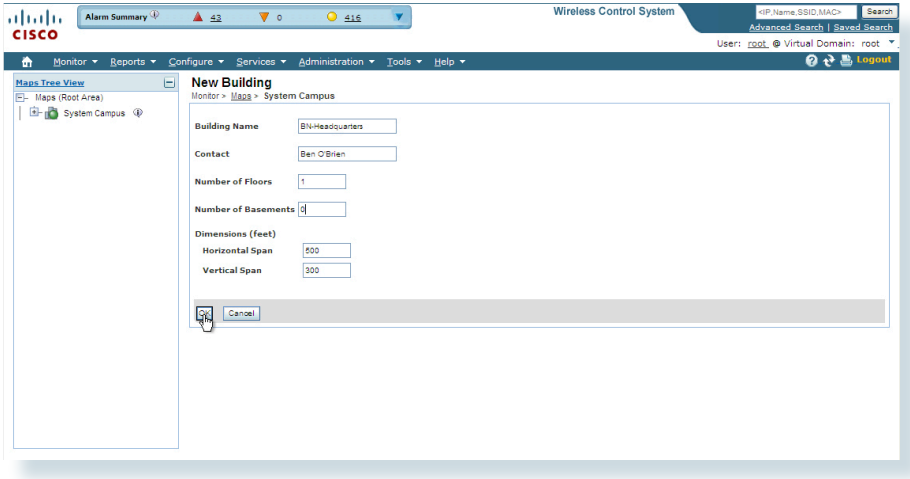
Number of floors: 1

Number of Basements: 0

Horizontal Span (feet): 500

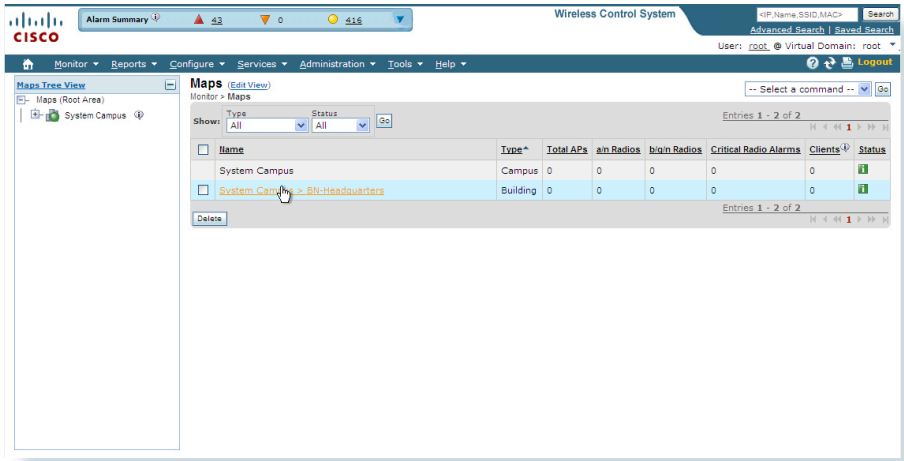
Vertical Span (feet): 300

Figure 30. Building Details



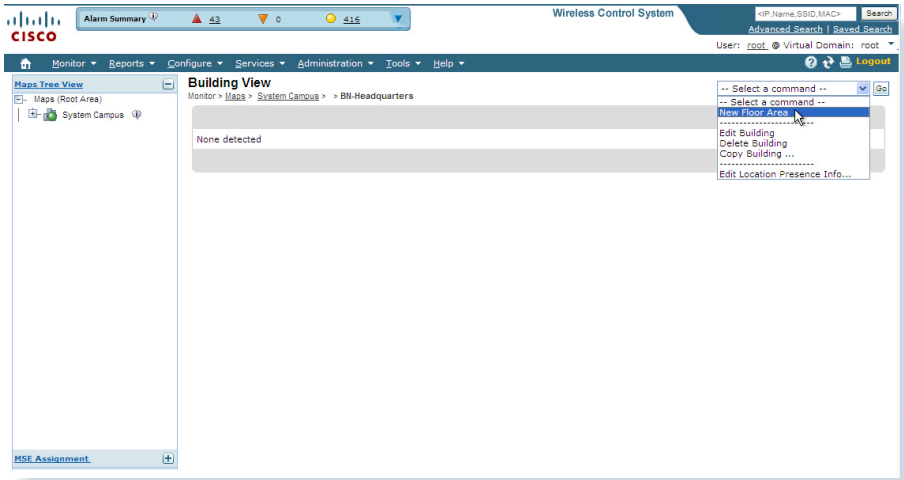
Step 5: Select your newly created building.

Figure 31. Select New Campus



Step 6: Select **New Floor Area** from the drop-down menu and click **Go**.

Figure 32. New Floor Area



Step 7: Create a floor name, contact name, floor number, and a description of the area. Select the floor plan image. Click **Next**:

Floor Area Name: BN-Headqaurters

Contact: Ben O'Brien

Floor: 1 (selected from drop-down list)

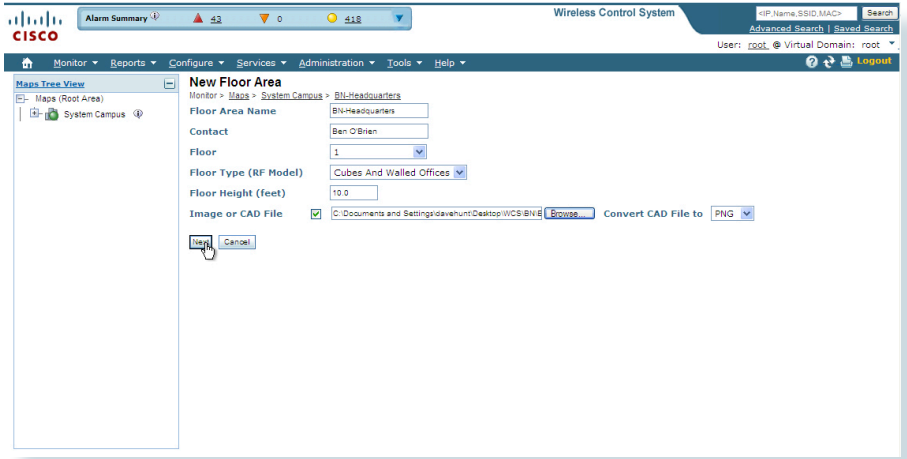
Floor Type (RF Model): Cubes And Walled Offices (select from the drop-down list)

Floor Height (feet): 10.0

Image or CAD File: C:\Documents and Settings\BN-Headquarters.png

Convert CAD File to: PNG (Accept the default drop-down selection)

Figure 33. New Floor Details and Image Upload



Step 8: Verify your new floor area details and image and click **OK**.

Figure 34. Verify New Floor Details

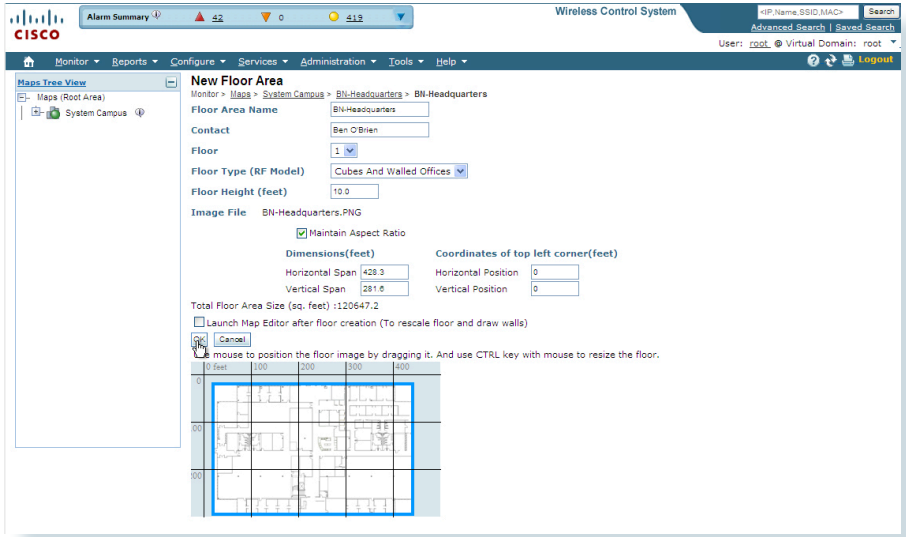
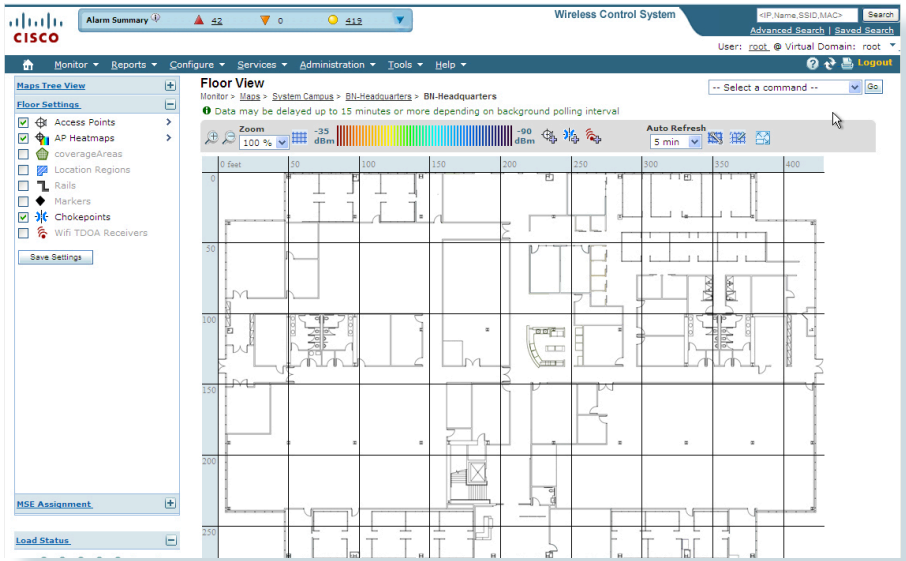


Figure 35. Floor View



Place Access Points

The final piece of the puzzle is to place the access points at the proper location on your individual floorplans. The Wireless LAN Controllers that work in conjunction with the Cisco Wireless Control System give an accurate view and device location, if you take the time to place your access points where they actually are located.

Step 1: Log into Cisco WCS.

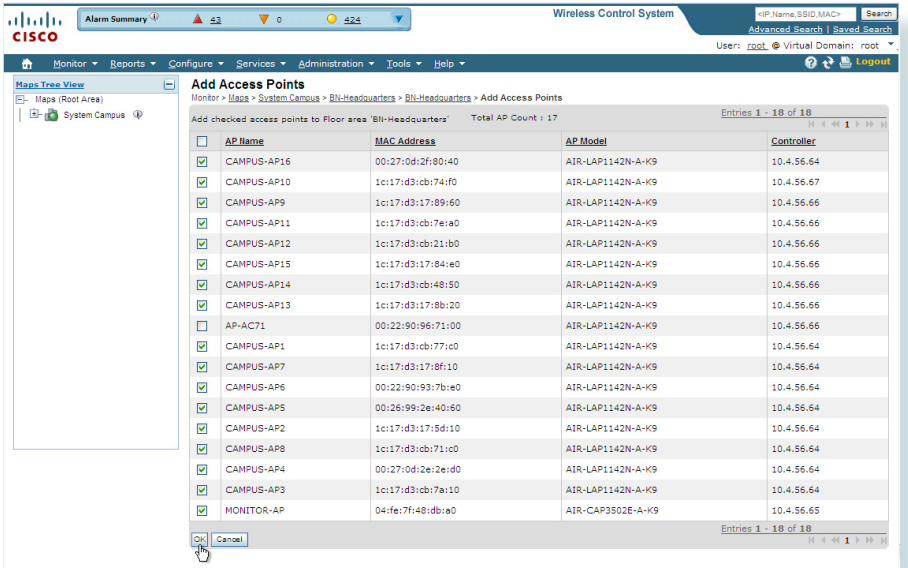
Step 2: Navigate to **Monitor > Maps**.

Step 3: Select your new Floor plan, **BN-Headquarters**.

Step 4: From the right drop-down list, select **Add Access Points** and click **Go**.

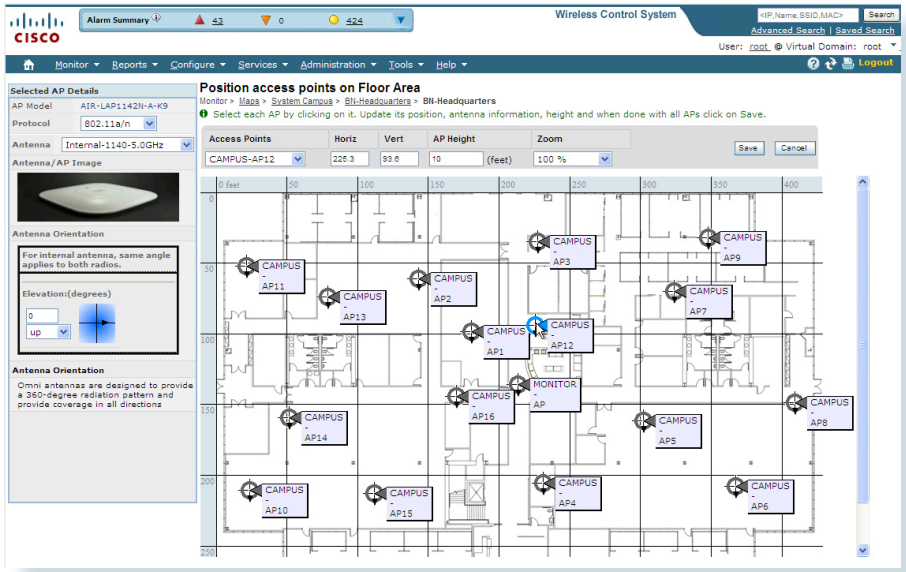
Step 5: Select access points that are registered with the system but not yet placed for the headquarters building.

Figure 36. Select APs to Place on New Floor



Step 6: Carefully place each access point as close to its real position in the building as possible and click **Save**.

Figure 37. AP Placement



NOTE: You must now wait while the system calculates the heatmaps from the placement and floorplan area.

Configuring the Cisco Wireless Solution for CleanAir

The Wireless LAN controller with the connected Cisco AIR-CAP3500 access points is immediately CleanAir capable. The Wireless LAN controllers can give you immediate information about your environment. Where the WCS can take a network view, the WLC only displays data retrieved from the locally connected CleanAir access points.

With the Cisco Wireless Control System in the network, all management will be handled at the WCS. Management can be done at each controller, but we do not recommend this. With the CleanAir access point operating from the wireless LAN Controller, we can log into the Cisco Wireless Control System and configure our controller to support CleanAir.

Event-Driven Radio Resource Management (EDRRM)

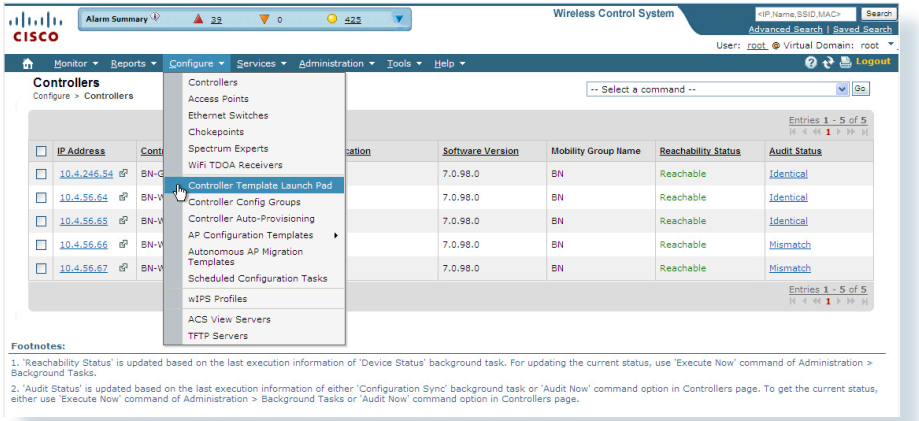
Event-Driven RRM is a feature that allows an access point that is in distress to bypass normal RRM intervals and immediately change channels. A CleanAir access point always monitors AirQuality (AQ), and reports on AQ in 15 second intervals. AirQuality is a better metric than relying on normal Wi-Fi chip noise measurements because AQ only reports on classified interference devices. That makes AQ a reliable metric in that we know what is reported is not because of Wi-Fi energy (and hence is not a transient normal spike).

The key benefit of the EDRRM is very fast action time (30 seconds). If an interferer is operating on an active channel and is causing enough AQ degradation that it triggers EDRRM, then no clients will be able to use that access point or channel. The only thing to do is get the access point off that channel. The EDRRM feature is not enabled by default and must be enabled. This process has two steps: enable CleanAir and then enable Event-Driven RRM.

Step 1: Log into Cisco WCS.

Step 2: Navigate to **Configure > Controller Template Launch Pad**.

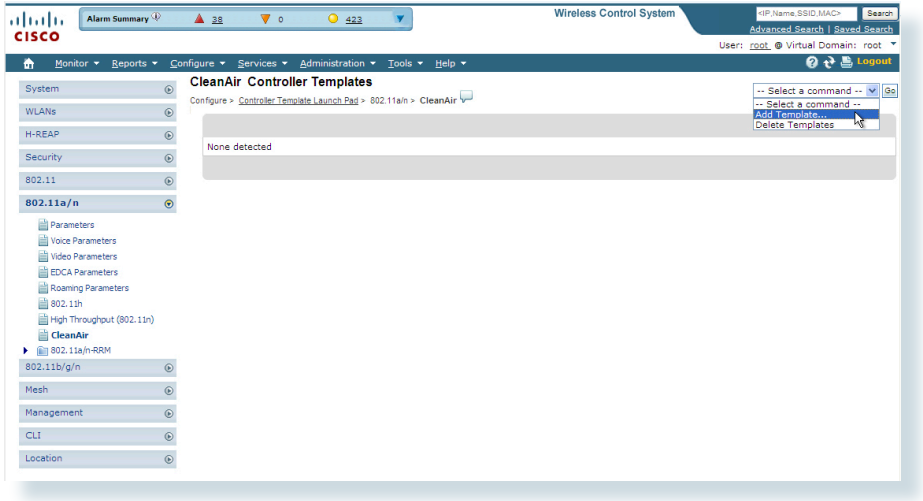
Figure 38. Controller Templates



Step 3: Navigate to **802.11a/n > CleanAir**.

Step 4: From the drop-down list, select **Add Template**.

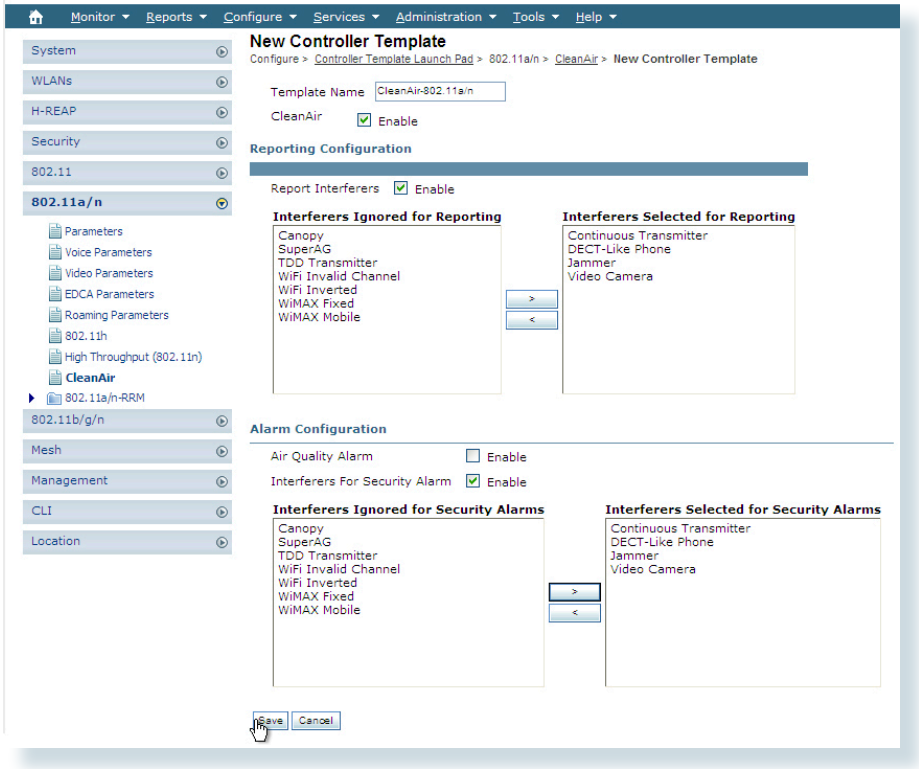
Figure 39. Add 802.11a/n CleanAir Template



Step 5: Create a template name (for example, CleanAir-802.11a/n) and provide the following information:

1. Check the **CleanAir Enable** check box.
2. Check the **Report Interferers Enable** check box.
3. Add Continuous Transmitter, DECT-Like Phone, Jammer and Video Camera to **Interferers Selected for Reporting**.
4. Check the **Interferers For Security Alarm Enable** check box.
5. Add Continuous Transmitter, DECT-Like Phone, Jammer and Video Camera to **Interferers Selected for Security Alarms**
6. Select **Save**.

Figure 40. 802.11a/n CleanAir Parameters



Step 6: Select **Apply to Controllers....**

Step 7: Select ALL Controllers and click **OK**.

Step 8: Navigate to **Configure > Controller Template Launch Pad**.

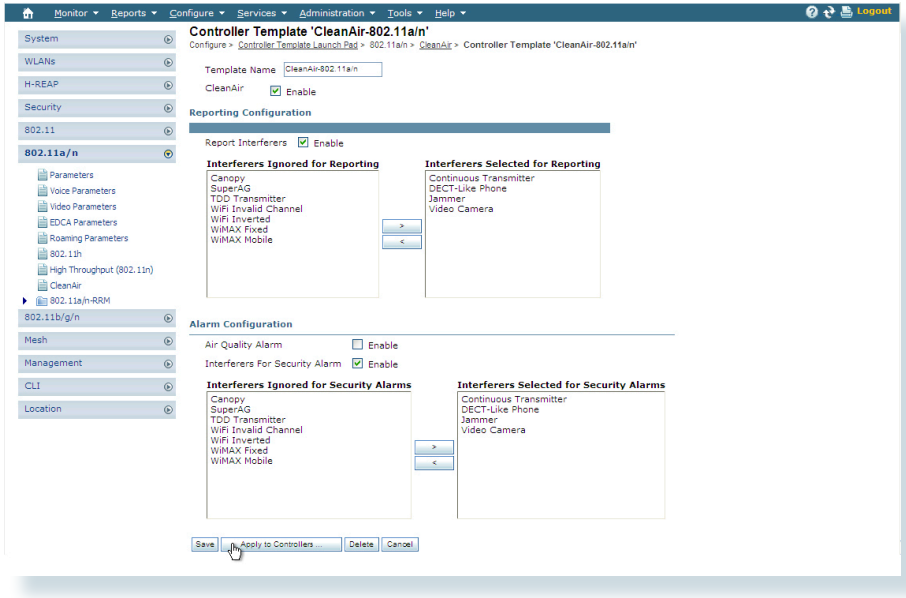
Step 9: Navigate to **802.11b/g/n > CleanAir**.

Step 10: From the drop-down list, select **Add Template**.

Step 11: Create a template name (for example, CleanAir-802.11b/g/n) and provide the following information:

1. Check the **CleanAir Enable** check box.
2. Check the **Report Interferers Enable** check box.
3. Add Continuous Transmitter, DECT-Like Phone, Jammer, Microwave Oven and Video Camera to **Interferers Selected for Reporting**.
4. Check the **Interferers For Security Alarm Enable** check box.
5. Add Continuous Transmitter, DECT-Like Phone, Jammer, Microwave Oven and Video Camera to **Interferers Selected for Security Alarms**.
6. Click **Save**.

Figure 41. 802.11b/g/n CleanAir Parameters



Step 12: Select **Apply to Controllers....**

Step 13: Select **ALL Controllers** and click **OK**.

Enable Event Driven Radio Resource Management

Step 1: Navigate to **Configure > Controller Template Launch Pad**.

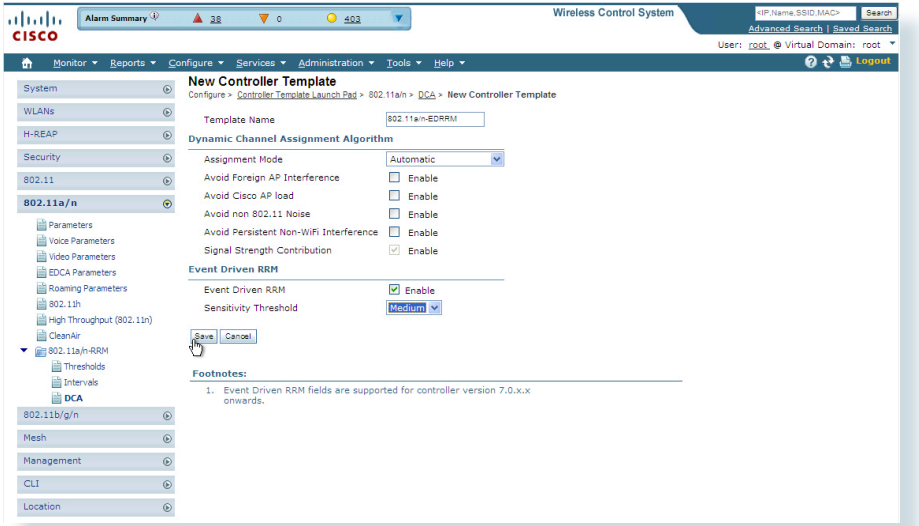
Step 2: From the left menu, navigate to **802.11a/n > 802.11a/n-RRM > DCA**.

Step 3: Select **Add Template**.

Step 4: Create a template name as follows:

1. Check the **Event Driven RRM Enable** check box.
2. Change the **Sensitivity Threshold** to **Medium**.
3. Click **Save**.

Figure 42. 802.11a/n Event Driven Enable



Step 5: Select **Apply to Controllers....**

Step 6: Leave **Apply to controllers selected directly** and check **All Controllers** and click **OK**.

Step 7: Navigate to **Configure > Controller Template Launch Pad**.

Step 8: From the left menu, navigate to **802.11b/g/n > 802.11b/g/n-RRM > DCA**.

Step 9: Select **Add Template**.

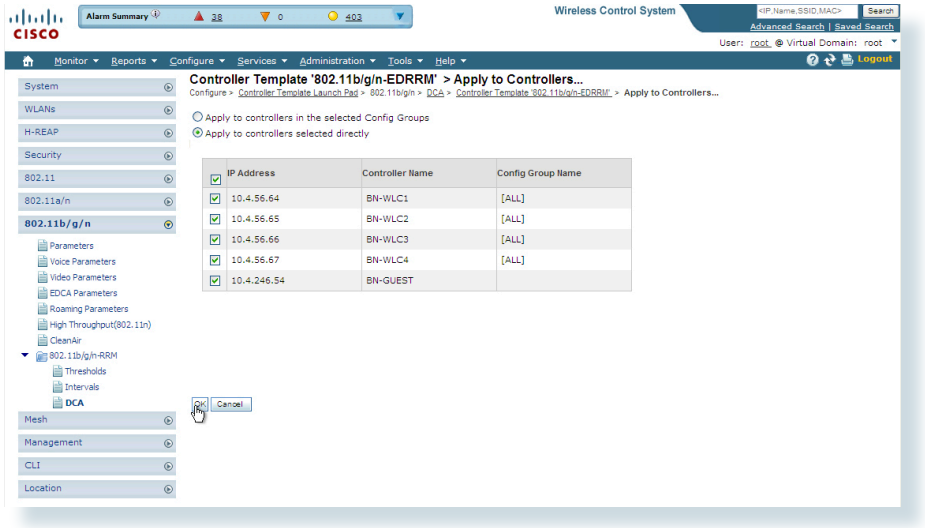
Step 10: Create a template name as follows:

1. Check the **Event Driven RRM Enable** check box.
2. Change the **Sensitivity Threshold** to **Medium**.
3. Click **Save**.

Step 11: Select **Apply to Controllers...**.

Step 12: Leave **Apply to controllers selected directly** and check **All Controllers** and click **OK**.

Figure 43. Apply to All Controllers



Troubleshooting with CleanAir

The real power of CleanAir is that a network administrator can be on one continent while the Wi-Fi spectrum in another office on the other side of the planet can be analyzed directly. The 3500 access points can be put in SE-Connect mode and used as a virtual remote interface for the knowledgeable engineer no matter where this valuable human resource is located. By changing the role of your CleanAir access point and connecting the Spectrum Expert 4.0 software, the Wi-Fi network administrator can now view the environment directly. There is no longer a need to fly expensive personnel onsite to troubleshoot physical layer issues that are unknown and challenging and, too often, intermittent issues.

Accessing Remote CleanAir for Spectrum Connect

When the call for assistance arrives, it is almost certainly to be in a location that does not have the knowledgeable human resources to troubleshoot, identify, and fix the issue. Wi-Fi radios are designed to send and receive Wi-Fi signals, but they do not have the capability to identify non-Wi-Fi radio interferers such as microwave ovens, DECT phones, analog wireless cameras, or even radio jammers. The specialized radios in the CleanAir radio can identify and, with triangulation, can locate where these devices are located.

When the call comes in, it is always important to identify as many facts about the issue to make informed decisions. The information can be the location of the problem (for example, “the street side of the building does not have connectivity”) and time of day (for example, “the issue is pronounced at lunch time”). With as much information from the end user as possible, it is now time to look at the radio environment because the system shows that clients are connecting and WCS indicates AirQuality has dropped...

Configure Spectrum Connect

The CleanAir-capable access point must be changed from either Monitor Mode or Local Mode of operation to Spectrum Connect Mode.

Step 1: Log into the Wireless LAN Controller

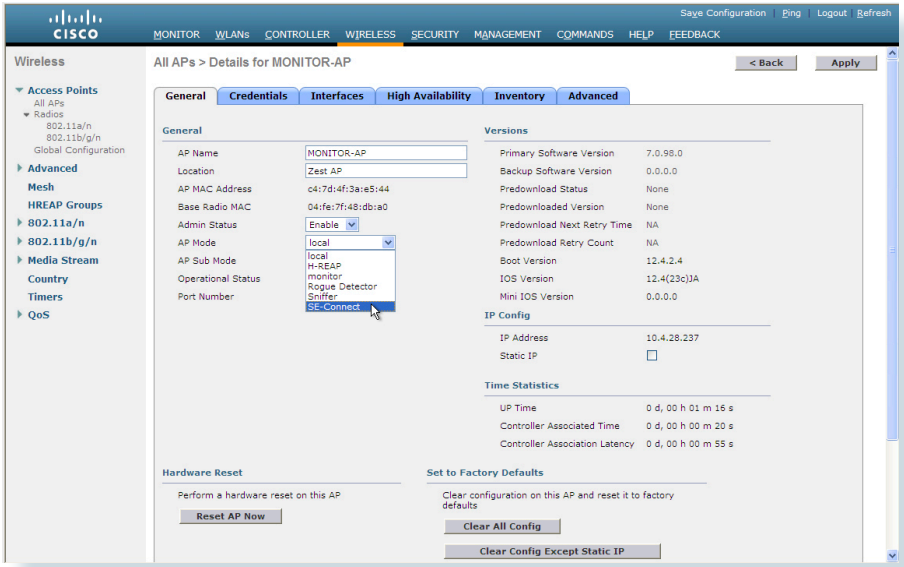
Step 2: Navigate to **WIRELESS**.

Step 3: Select the closest CleanAir AP to the suspected issue.

Step 4: From the drop-down list next to **AP Mode**, change to **SE-Connect**.

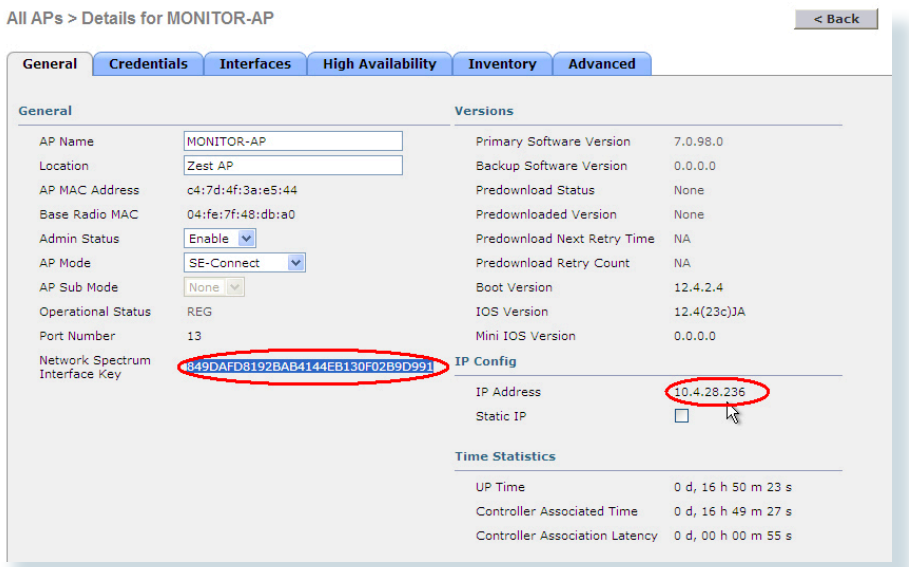
Step 5: Click **Apply** and wait for the access point to reboot and reconnect to the Wireless LAN Controller.

Figure 44. Change Mode



Step 6: Copy the **Network Spectrum Interface Key** and the CleanAir access point IP address.

Figure 45. Capture Network Key and IP Address



Step 7: On a Supported Windows platform with Cisco Spectrum Expert Connect (4.0 or greater) installed, launch Spectrum Expert.

Figure 46. Launch Spectrum Expert

Step 8: Select the **Radial Button Remote Sensor**:

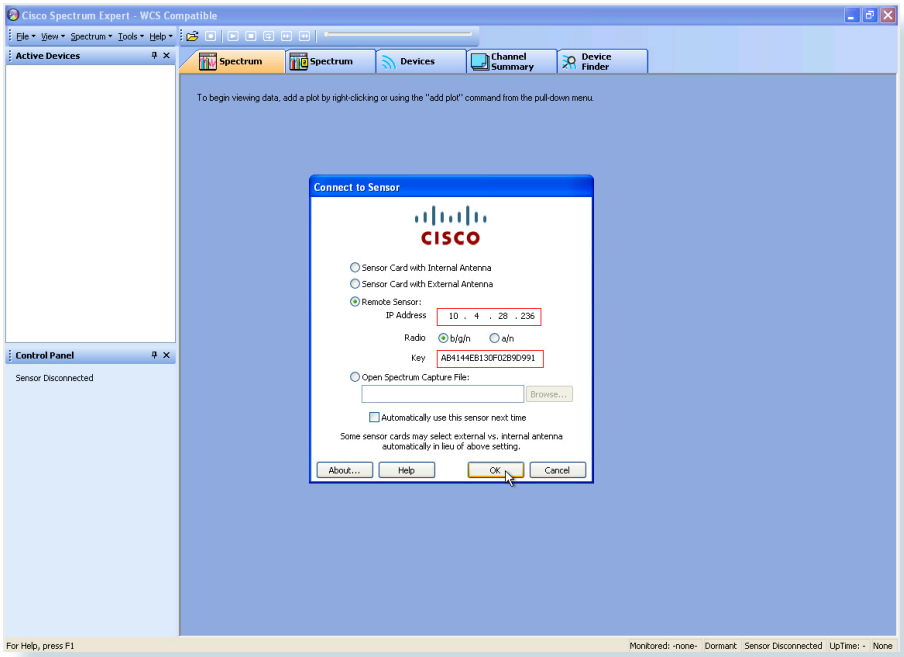
Step 8A: Enter the IP address of the CleanAir access point

Step 8B: Enter the Network Spectrum Interface Key of the CleanAir access point.

Step 8C: Select either 2.4 GHz by selecting the **b/g/n** radial button or the 5 GHz by selecting the **a/n** radial button.

Step 8D: Click **OK**.

Figure 47. Enter Remote CleanAir Details

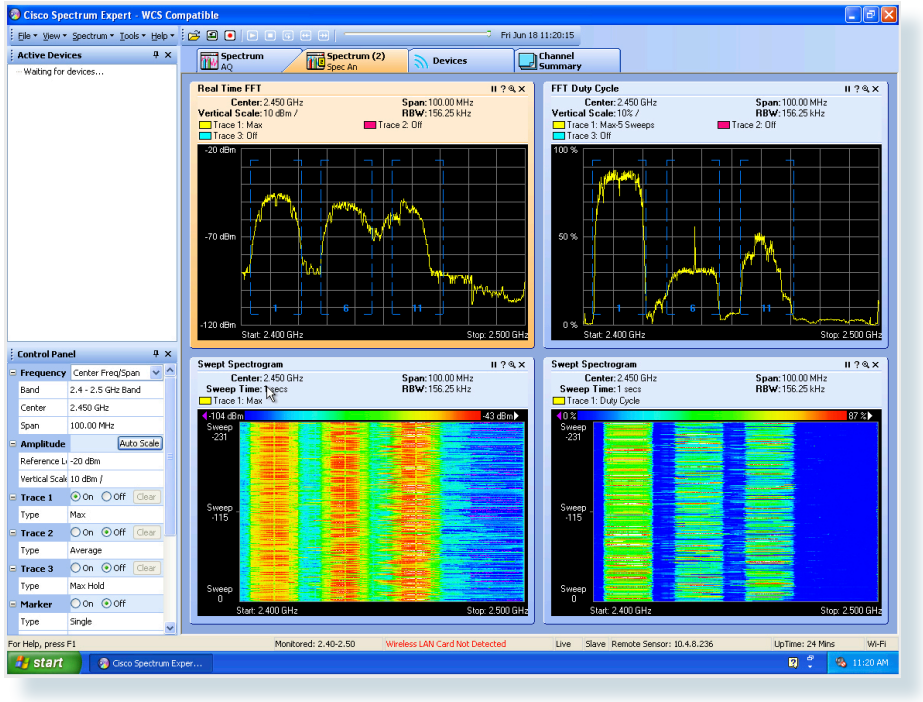


The connected Windows machine now connects to the remote CleanAir access point on UDP port 37540 if you selected b/g or on UDP port 37550 if you selected a/n during preceding setup steps. If connection problems occur, verify that you can ping the CleanAir access point and that there are no port-blocking network devices that may be blocking the necessary UDP port information.

Remote Spectrum

The remote sensor capability is the ability to get real-time, physical layer spectrum data without having to drive or fly onsite. Figure 48 illustrates this capability in a Wi-Fi-only environment, and gives you an understanding of what is really happening in your remote environment.

Figure 48. 2.4 GHz Spectrum Using the CleanAir Access Point as the Remote Sensor



NOTE: Observe in Figure 48 that the Windows XP Spectrum Expert device does not detect a Wireless LAN card and that the remote sensor is at 10.4.28.236.

Appendix A: Parts List

Functional Area	Product	Part Numbers	Software Version
Headquarters	Cisco WCS	WCS-STANDARD-K9 WCS-APBASE-100 WCS-ADV-SI-SE-10= (optional)	7.0.164.0
	Cisco Wireless LAN Controller	AIR-CT5508-100-K9	7.0.98.0
	Cisco Access Point	AIR-CAP3502E-A-K9	7.0.98.0
	Cisco Access Point	AIR-CAP3502I-A-K9	7.0.98.0
	Cisco Access Point	AIR-LAP1142-A-K9	7.0.98.0
	Cisco Spectrum Expert	AIR-CSCO-SE-WIFI-C	4.0.60
	Cisco Mobility Service Engine	AIR-MSE-3350-K9	7.0.105.0

Revision History

Date	Engineer	Explanation/Description
12 March 2010	Davehunt	Initial creation
9 May 2010	Davehunt	Updated for CleanAir
21 May 2010	Davehunt	Moved CleanAir into SBA and updated screenshots
18 June 2010	Davehunt	Updated to current CCO Release software and added Spectrum Connect configuration with SE Software 4.0.60.0

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**

C07-614628-00 08/10