Deploying and Troubleshooting Cisco Wireless LAN Controllers:

A Practical Guide to Working with the Cisco Unified Wireless Solution

Mark Gress
Javier Contreras Albesa

ciscopress.com

Deploying and Troubleshooting Cisco Wireless LAN Controllers

Mark L. Gress, CCIE 25539

Lee Johnson

Cisco Press

800 East 96th Street

Indianapolis, IN 46240

Deploying and Troubleshooting Cisco Wireless LAN Controllers

Mark L. Gress, CCIE 25539 and Lee Johnson

Published by:
Cisco Press
800 East 96th Street
Indianapolis, IN 46240 USA

Printed in the United States of America

First Printing November 2009

Library of Congress Cataloging-in-Publication data is on file.

ISBN-13: 978-1-58705-814-1

ISBN-10: 1-58705-814-6

Warning and Disclaimer

This book is designed to provide information about the Cisco Unified Wireless Network (CUWN) solution pertaining to understanding and troubleshooting wireless LAN Controllers (WLC) and access points (AP). The information contained in this book, in conjunction with real-world experience, also provides an excellent self-study resource for the CCIE Wireless exam. Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied.

The information is provided on an “as is” basis. The authors, Cisco Press, and Cisco Systems, Inc. shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the discs or programs that may accompany it.

The opinions expressed in this book belong to the author and are not necessarily those of Cisco Systems, Inc.

Trademark Acknowledgments

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Cisco Press or Cisco Systems, Inc., cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Feedback Information

At Cisco Press, our goal is to create in-depth technical books of the highest quality and value. Each book is crafted with care and precision, undergoing rigorous development that involves the unique expertise of members from the professional technical community.

Readers' feedback is a natural continuation of this process. If you have any comments regarding how we could improve the quality of this book or otherwise alter it to better suit your needs, you can contact us through email at feedback@ciscopress.com. Please make sure to include the book title and ISBN in your message.

We greatly appreciate your assistance.

Corporate and Government Sales

The publisher offers excellent discounts on this book when ordered in quantity for bulk purchases or special sales, which may include electronic versions and/or custom covers and content particular to your business, training goals, marketing focus, and branding interests. For more information, please contact: **U.S. Corporate and Government Sales** 1-800-382-3419 corpsales@pearsontechgroup.com

For sales outside the United States please contact: **International Sales** international@pearsoned.com

Publisher: Paul Boger

Associate Publisher: Dave Dusthimer

Executive Editor: Mary Beth Ray

Managing Editor: Patrick Kanouse

Senior Development Editor: Christopher Cleveland

Project Editor: Mandie Frank

Editorial Assistant: Vanessa Evans

Cover and Interior Designer: Louisa Adair

Composition: Mark Shirar

Indexer: Ken Johnson

Cisco Representative: Eric Ullanderson

Cisco Press Program Manager: Anand Sundaram

Technical Editors: Dmitry Khalyavin and Fabian Riesen

Copy Editor: Karen A. Gill

Proofreader: Jovana San Nicolas-Shirley

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.**

About the Authors

Mark L. Gress, CCIE 25539, is an escalation engineer at the Cisco Systems Technical Assistance Center (TAC) in Research Triangle Park, North Carolina, where he has worked since 2005. He has been troubleshooting complex wireless networks since the birth of the Cisco Wireless LAN Controller (WLC) as a TAC engineer, a technical lead for the Enterprise Wireless team, and now as an escalation engineer supporting the complete Cisco line of wireless products. Mark has diagnosed problems in some of the largest Cisco wireless deployments and has provided training for TAC teams around the world. He has also contributed to numerous design guides, application notes, and white papers. As one of the highest contributors of identifying and assisting in defect resolution, his work has led to increases in overall product quality and stability. Mark graduated summa cum laude with a bachelors of science in both computer information systems and business management from North Carolina Wesleyan College. For more than ten years, Mark has been professionally involved in the networking industry.

Lee Johnson is currently a wireless specialist on the RTP Wireless TAC team at Cisco. He has been troubleshooting wireless networks, including both autonomous and controller-based infrastructures, since 2006. Lee troubleshoots complex wireless issues in Cisco customer networks around the world. He has been dispatched to customer sites to address critical accounts and represented Cisco at Networkers. He also provides training and documentation for fellow Cisco engineers in both wireless and nonwireless TAC groups. Lee works closely with the wireless development group at Cisco to improve product quality and the customer experience with the WLC. He holds a bachelor of science degree in biology from the University of North Carolina at Chapel Hill.

About the Contributing Author

Javier Contreras Albesa, CCIE Security, is a member of the escalation team for the Wireless Business Unit, at Cisco Systems in Spain, where he has worked since 2005. Since the introduction of the Wireless LAN Controllers, he has been an escalation engineer on the TAC in Belgium and now interfaces between post-sales support and development responsible for supporting the European region. Javier has been involved on most support cases for the region and several priority cases worldwide. He has been a significant contributor to quality improvement on different wireless products. He has published several whitepapers and application notes and is the main developer on the WLC Config Analyzer, a tool used to simplify the support on WLC deployments. Javier graduated in computer information systems in Venezuela. For more than 12 years, Javier has been involved in networking, security consultancy, and the wireless industry.

About the Technical Reviewers

Dmitry Khalyavin is the lead engineer in Cisco's Wireless Network Business Unit escalation team. He has six years of experience working with design, implementation, management, and troubleshooting of the complete line of Cisco's wireless product offerings. He holds a bachelor's degree in computer science from Polytechnic Institute of New York University.

Fabian Riesen is Technical Leader at Cisco Systems' TAC in Switzerland. He joined Cisco in 1999 as a project engineer. He owns a Swiss-Engineer degree from the University of Applied Sciences Winterthur/Zurich* with specialization in Software Engineering and Transmission Technologies. He is CCIE ISP-Dial and CCIE Wireless No. 6268.

Dedications

I would like to dedicate this book to my loving wife, Kameron, and children, Taylor, Trinity, and Tanner. They are the root to my strength and dedication that constantly moves me forward in life. They have dealt with me through tough times and made personal sacrifices so I could achieve more. No matter what, they have always been there for me, and for that I will always love them and be extremely grateful.

I would also like to make a special dedication to my doctor, one of the best in the world, Dr. David Paul Adams. With his medical expertise, he has assisted me in accepting the physical limitations I have struggled with throughout this process, giving me my life back so I can continue to accomplish special tasks and achieve what others cannot. I truly do not know where I would be without his understanding, compassion, and support.

I would also like to make a special dedication to my brother, Michael Gress. I am very proud of him for everything he has achieved and hope one day that I can be as good as a person as he is.

Finally my father, Larry Gress—not only is he a terrific father but also my best friend! Thank you for bringing me into this world and all your help!

—Mark L. Gress

I would like to dedicate this book to my wife, Lisa, and children, Tyler and Kasey. Without your love and support, I might never have been able to finish it. Lisa, thanks for putting up with me and taking care of the family while I was engrossed in this project.

—Lee Johnson

Acknowledgments

Mark and Lee would like to thank both Fabi Riesen and Dmitry Khalyavin for providing their expert technical knowledge in reviewing this book. Their comments and suggestions were invaluable in making this book complete and accurate. Thanks for keeping us on our toes with the latest features and configuration settings.

Thanks to Fabi Riesen for his contributing work. Fabi is a great technical resource and certainly helped lighten the load for us to make sure this book reached completion in a timely manner.

We also want to thank the Cisco Press team for this book. Mary Beth Ray, Christopher Cleveland, and Mandie Frank kept us on track and inline to get this work done. Thanks for putting up with us!

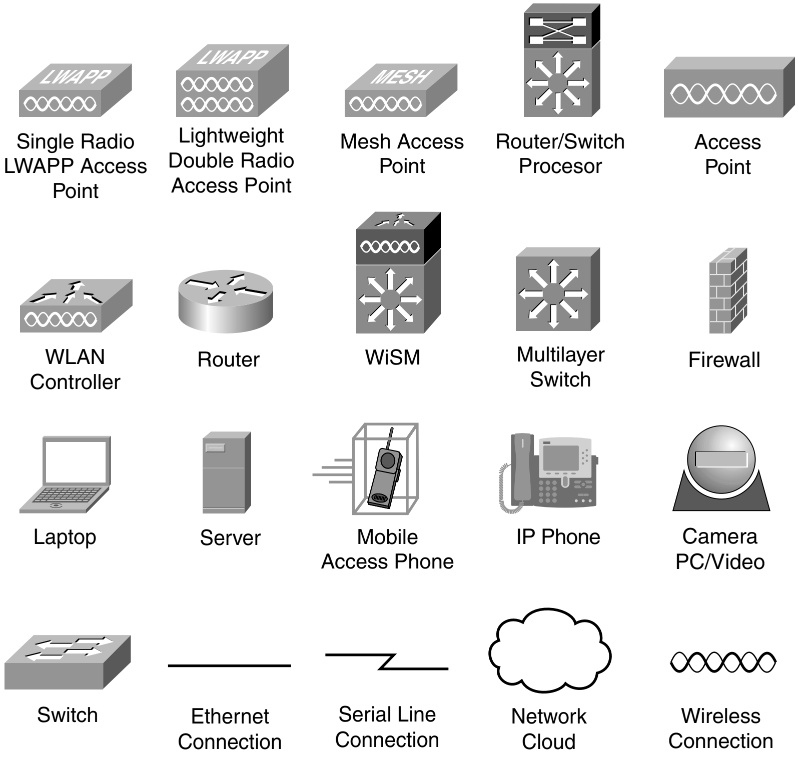
Lee would like to thank Mark Gress for approaching him and giving him the opportunity to work on this book. It was definitely a learning experience!

Mark and Lee would like to thank Jason Fitzgerald, manager of the RTP Wireless Technical Assistance Center, for giving us the opportunity to prove we are the best of the best at what we do! Without his encouragement and support, this book would not have been possible.

Contents at a Glance

Contents

Icons Used in This Book



Command Syntax Conventions

The conventions used to present command syntax in this book are the same conventions used in the *IOS Command Reference*. The *Command Reference* describes these conventions as follows:

- **Boldface** indicates commands and keywords that are entered literally as shown. In actual configuration examples and output (not general command syntax), boldface indicates commands that are manually input by the user (such as a **show** command).
- *Italic* indicates arguments for which you supply actual values.
- Vertical bars (|) separate alternative, mutually exclusive elements.
- Square brackets ([ ]) indicate an optional element.
- Braces ({ }) indicate a required choice.
- Braces within brackets ([{ }]) indicate a required choice within an optional element.

Introduction

Wireless networking is a fast-evolving technology. Long gone are the days when companies view wireless access as a perk. Along with a dial tone, more and more companies view wireless connectivity as a given network resource. Information technology (IT) professionals are required to fully understand the latest wireless products and features to properly implement a wireless solution. Companies and standards bodies are designing and offering certification programs so candidates can prove their wireless knowledge and benefit the organization.

The Cisco Unified Wireless Network (CUWN) solution is a bleeding-edge wireless technology platform that most wireless professionals need to be familiar with to properly install, configure, and troubleshoot.

Goals

The goal of this book is to give you the necessary knowledge to install, configure, and troubleshoot Cisco wireless controller–based networks in a technically proficient and concise manner. Although this book tries to cover the topics in an in-depth manner, it would be impossible to cover all possible network scenarios that might exist. You should be able to take this information and apply it to any network issue and determine the underlying cause and resolve it. A wireless problem is going to fall into one or more of the following categories: configuration mistake, radio frequency (RF) issue, client issue, wired network issue, or bug. Basic wireless knowledge is assumed in this book, so some wireless topics are glossed over at a high level.

Although not specifically designed to help you pass the CCIE Wireless written and lab exams, this book does provide you with real-world configuration and troubleshooting examples. Understanding the basic configuration practices, how the products are designed to function, the feature sets, and what to look for while troubleshooting these features will be invaluable to anyone wanting to pass the CCIE Wireless exams.

Who Should Read This Book?

This book is designed for senior wireless networking professionals who will be installing, configuring, and maintaining Cisco wireless controllers and access points (AP).

How This Book Is Organized

Although this book can be read cover to cover, it is designed so that you can flip directly to the particular chapter that discusses the topic you are interested in. Chapter 1, “Troubleshooting Strategy and Implementation,” provides the basis on how to develop a solid troubleshooting method that you can apply to any of the following subjects covered in the remaining core Chapters 2 through 15. The appendixes provide a list of debug commands, payload information, and information on the next generation of Cisco wireless controllers.

The core chapters, 2 through 15, cover the following topics:

- **Chapter 2, "Wireless LAN Controllers and Access Points"**: This chapter discusses the different wireless controller and AP models and the differences between them. It also covers hardware and software requirements.
- **Chapter 3, "Introduction to LWAPP"**: This chapter discusses the basic concepts behind the Lightweight Access Point Protocol (LWAPP).
- **Chapter 4, "The CAPWAP Protocol"**: This chapter covers the Control and Provising of Wireless Access Points (CAPWAP) protocol, including session establishment, troubleshooting the discovery and join process, and CAPWAP communication.
- **Chapter 5, "Network Design Considerations"**: This chapter covers physical and logical install and design considerations for the controllers and APs. It covers controller failover, access layer, distribution layer, service block controller installations, WAN considerations, and dense access point deployments and location.
- **Chapter 6, "Understanding the Troubleshooting Tools"**: This chapter covers the options and possibilities for troubleshooting wired and wireless issues within your deployments.
- **Chapter 7, "Deploying and Configuring the Wireless LAN Controller"**: This chapter explains how to deploy and configure the Wireless LAN Controller (WLC) for connectivity with APs using multiple AP-Managers and link aggregation (LAG). The chapter also covers how to troubleshoot some of the more common WLC issues.
- **Chapter 8, "Access Point Registration"**: This chapter covers the AP registration process for a controller and the methods for AP discovery and troubleshooting.
- **Chapter 9, "Mobility"**: This chapter discusses intra-, inter-, Layer 2, and Layer 3 controller roaming and troubleshooting. It also covers AP mobility between controllers.
- **Chapter 10, "Troubleshooting Client-Related Issues"**: This chapter covers general client information, client associations, debugs on the client, use of wireless and wired sniffer traces, local AP debugs, and interpreting the output of **debug client** on the controller command-line interface (CLI).
- **Chapter 11, "Wireless Voice"**: This chapter examines proper voice deployment guidelines, configuring the controller for voice depolyments, common voice-related troubleshooting methods, and proper quality of service (QoS) for wireless voice deployments.
- **Chapter 12, "Radio Resource Management"**: This chapter examines the auto-RF feature of the controllers and how RF groups and group leaders are elected. It also covers dynamic channel assignment, transmit power control, coverage hole detection, and Radio Resource Management (RRM) guidelines, enhancements, and troubleshooting.
- **Chapter 13, "H-REAP"**: This chapter covers Hybrid Remote Edge Access Point (H-REAP) configuration and troubleshooting, differences between REAP and H-REAP, Split MAC versus Local MAC, H-REAP modes of operation, configuration, and troubleshooting.

- **Chapter 14, "Guest Networking":** This chapter covers web authentication and how it works, auto-anchoring (guest tunneling), wired guest access, guest profiles, QoS profiles for guest users, and custom web authentication pages and certificates and how to troubleshoot them.
- **Chapter 15, "Mesh":** This chapter discusses wireless mesh APs, the different mesh code releases, deployment guidelines, mesh routing, parent selection, configuration, Ethernet bridging, and troubleshooting.
- **Appendix A, "Debugging Commands":** This appendix covers Comprehensive debug command list and usage guide for WLCs covering all versions of code. The debug commands also include Remote AP debugs and other debugs that will aid in troubleshooting almost every issue possible!
- **Appendix B, "LWAPP and CAPWAP Payloads":** This appendix is a comprehensive list of specific payloads and their uses. The Vendor Specific Payload message element is used to communicate vendor specific information between the WTP and the access controller (AC). Also included are payloads sent in LWAPP messages and the corresponding ones that will be sent in CAPWAP messages.

Chapter 1

Troubleshooting Strategy and Implementation

When you think about a wireless network, especially one involving Lightweight Access Point Protocol (LWAPP) or Control and Provisioning of Wireless Access Points (CAPWAP), the topology can be profoundly large. The challenge of troubleshooting a wireless issue can be intimidating to any seasoned engineer. The issue might not even be wireless, but ultimately it can affect all wireless connectivity or the quality of the connection. The question is a simple one, but at this point, it might be the most difficult: Where do I start or how do I begin?

Developing a Troubleshooting Strategy

Developing a troubleshooting strategy can be a life saver. Usually strategies work well on issues that have been around for awhile or that are intermittent. Depending on the issue, your strategy might change to best suit what is currently going on. No matter which way you look at it, the best choice is to have a plan ready to go. You can always modify your strategy if the parameters of the problem change while you're troubleshooting. It's easier to be in a situation in which your strategy needs extensive modification than to be without one.

Production Versus Nonproduction Outages

A network problem typically falls into one of the following two types of categories, either of which can fit into a production or nonproduction outage:

- **Outage renders the network completely useless or inoperable:** Believe it or not, this does provide some positive aspects to troubleshooting. Network activity that would usually require a maintenance or change window can now be accomplished at any time because the network is down. A network-down scenario is usually easier to identify and fix because the issue is constant.
- **Outage renders the network partially impaired:** Issues that fall into this category are usually smaller in magnitude, but not always. For example, your wireless laptop

users might be able to access all network resources with the exception of the printers. Another example would be if your 7921 voice users have degraded voice quality. Users can still receive and place calls, but it might be difficult to understand the other party.

Step 1: Gathering Data About the Problem

No matter what issue you encounter, the one resource that helps any situation is information about the issue and knowledge of the environment. Information aids in your understanding of what you are potentially dealing with—the scope, magnitude, and other facets that could be influencing the issue at hand. No matter what problem you start to troubleshoot, information gathering should always be the first step. In most cases you do not even realize you have done that.

Step 2: Identifying the Problem

Identifying and isolating the problem can be a major headache in itself, especially in a centralized wireless network using LWAPP and CAPWAP.

Wired networks alone can encompass quite a few network resources. Figure 1-1 shows an example of what you might see in a typical wireless network setup.

If you add the components of a wireless network to a wired network, you have a rather large plethora of network resources:

- Multiple LANs
- Large LANs
- Multiple VLANS (Inter-VLAN routing)
- WANs
- Routing protocols
- Multicast
- Hot Standby Routing Protocol (HSRP)
- Ether Channel

This list is just a small example of the wireless network resources and issues you need to investigate on top of the existing wired devices. Do not forget that this is a wireless deployment and that you also have to look at the wireless pieces:

- Interference
- Access points (APs)
- Controllers
- Antennas

- Authentication equipment (RADIUS servers, APs, or Wireless LAN Controllers [WLC], and so on)
- Client-related problems

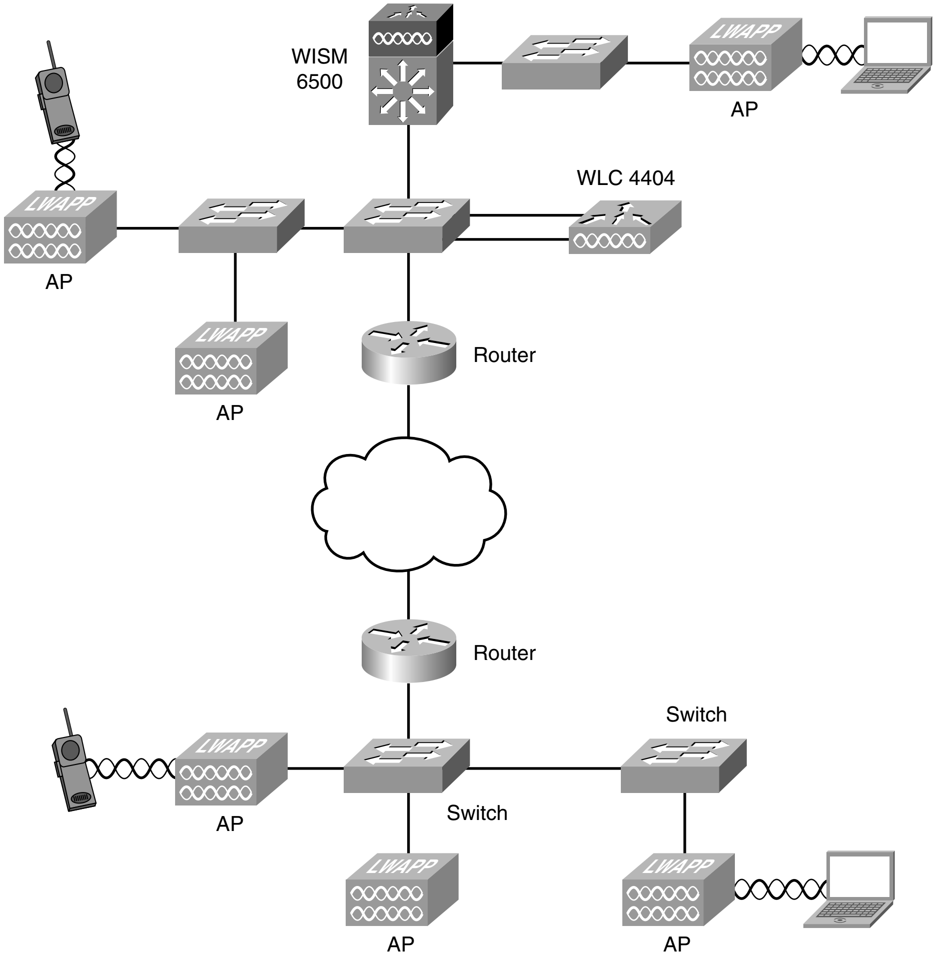


Figure 1-1 *Resources in a Typical Network*

Step 3: Isolating the Problem

A key piece of troubleshooting is to potentially identify the source of the issue. A networking topology can be a valuable tool in assisting you to do so. Judging from all the items listed previously, you have a lot of work cut out for yourself. You should always keep in mind that, while narrowing the list of possible culprits, you should never permanently rule out anything. At some point you might have to revisit the same resource that you looked at initially. Anyone who has been involved with troubleshooting networking-related issues for some time has been a part of a problem that was misdiagnosed or at some point had to claim responsibility for an incorrect action or identification of the problem.

A valuable piece of advice to remember is to always look at the big picture when searching for the root cause of the problem. Never let the symptoms of the problem mislead you.

Network Topology

A network topology can be a great visual roadmap of all the routes and equipment that are used. A network topology can isolate the issue even further and once again inform you of what pieces are or are not involved.

One of the most important steps is to develop a network diagram of the current network on which you are troubleshooting the issue. This can really put the network and its components into perspective. To build your network topology, use network diagram drawing software such as Microsoft Visio, SmartDraw, or similar tools. After the foundation is built, you can update it when needed. This can prove to be useful, especially if you have to contact a third-party support vendor. Your network topology is at your disposal and benefits others. Ideally, when troubleshooting, this drawing is already present or is included in any service requests.

What does the network diagram need to contain? The answer to this question can vary depending on the network size and type. This assists in tracking and being able to quickly connect to any device in the network. What is going to be useful in helping you solve the issue? Consider the following commonly used items:

- Device type diagrams (routers, switches, and so on)
- Model numbers
- IP addresses
- Subnets, VLANs, and so on
- Routing areas
- Protocols (Frame Relay, ATM, and so on)
- Interfaces, port numbers, and so on
- Software version
- Passwords

In addition, for the wireless portion of the network, you might need the following to generate a comprehensive topology:

- Mobility groups
- Radio frequency (RF) groups

- Radiation patterns of APs
- Access point channel information
- Access point power information
- Physical barriers or RF barriers
- AP group VLANs (if applicable)

Note AP group VLANs, along with WLAN override, have replaced the AP group functionality in version 5.2.

You can also generate this information by using a Wireless Control System (WCS) if you have one. The WCS and the Wireless Location Appliance, as seen in Figure 1-2, can be useful in many ways. The Cisco 3300 Series Mobility Services Engine is a combination of hardware and software. The Mobility Services Engine is an appliance-based solution that supports a suite of software services to provide centralized and scalable service delivery. The Mobility Services Engine transforms the wireless LAN into a mobility network by abstracting the application layer from the network layer, effectively allowing for the delivery of mobile applications across different types of networks.

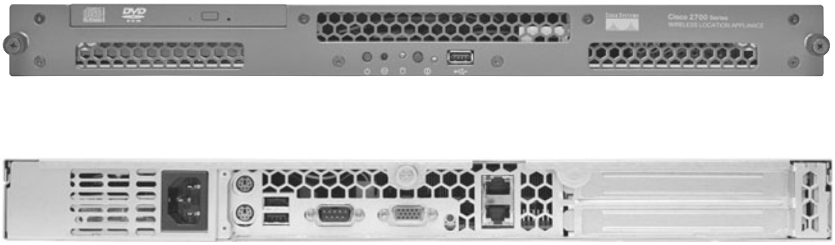


Figure 1-2 *Cisco Wireless Control System and Wireless Location Appliance*

Note The 2700 (wireless location appliance) has been deprecated and is being replaced by the 3300 Series Mobility Services Engine.

The WCS contains useful information and can be quite helpful.

However, because of the real-time necessity of information gathering, WCS can be suboptimal at times when troubleshooting. WCS takes snapshots at configured intervals to update its database. If any changes are made, the administrator has to wait until the next update interval or manually submit an update to see the change. WCS is not needed for a wireless network. WCS is a management standalone database that operates on a server. It acts as a third-party device and is passive unless used otherwise for configuration changes and so on. Figure 1-3 demonstrates how WCS is integrated into networks.

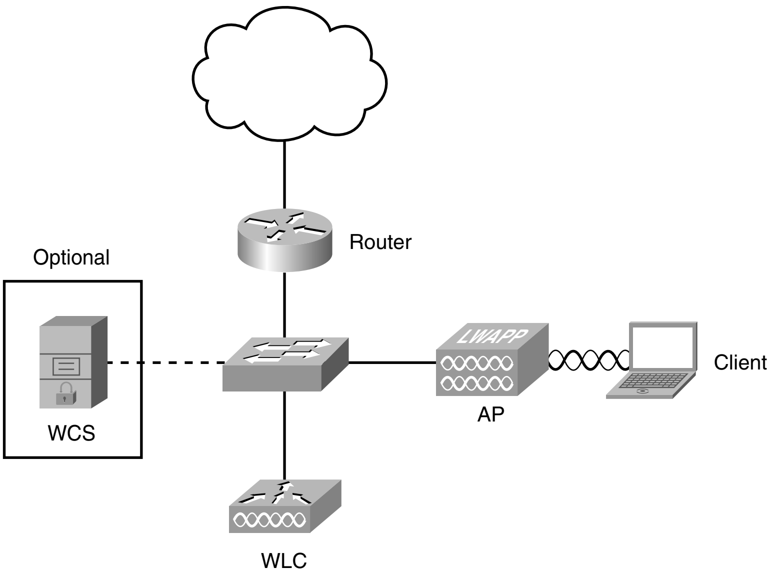


Figure 1-3 *Cisco Wireless Control System Integrated into a Network*

Depending on the size of the network, you might have multiple topology pages and maps. Always remember that there is nothing wrong with this—having too much information is not a bad position to be in. Obviously, everything listed is not required or set in stone; items are listed to give you a good starting point or items additional options to consider. You should always get as much information as needed to troubleshoot your issue.

Gathering General Information

Information is valuable in any form or fashion and is always vital. The best way to determine what information you might need for your network issue is to imagine that you are talking to someone over the phone. That is usually the most challenging environment because you are not physically there. Imagine what questions you would ask to educate yourself so you could provide the next course of action(s) or help solve the problem. This list can give you an idea of the potential information that is going to be needed. If you are the network administrator/owner, you must obtain the following information:

- Details about what the user actually experienced or is currently experiencing
- Information about the scope of the issue and how many users are affected
- Frequency of the issue
- Configurations of devices
- A network topology
- Any error messages, message logs, or sys log information

- Debug requirements
- MAC addresses/IP addresses for debugs or any other utility/application that might need them
- Any additional information/resources for the next troubleshooting steps

This is a good list to get you started. By no means is this list set in stone; you should modify it to fit the issue. If you have to contact a third party for support, it is beneficial to have this information, and in many cases, this information can decrease network outage time. It all comes down to what works for you.

You will encounter network issues that you simply will not have sufficient or the right kind of information to even begin troubleshooting. In many cases, you will need multiple tools set up or in place so when the problem happens again you can collect all the necessary elements. The key element is that in many network issues, additional work will be needed to gain the informational components to proceed to the next step in troubleshooting. This step might be acquiring additional informational resources or corrective action of the issue.

Frequency of the Issue

When discussing time with regard to a problem, you must consider a few factors. Time can be a valuable asset when trying to troubleshoot an issue. The frequency of the problem is important if the entire network is not down. Some issues that you can run into might occur only once a month. This can help set expectations on what information to acquire during the time the issue exists. The problem duration is also valuable because you know what can and cannot be done during this time frame.

In summary, you need to answer four questions in the most accurate and efficient manner:

- How long has the problem been going on?
- When did it start?
- How often does it occur?
- When the problem occurs, how long does it last?

The answers to these questions provide valuable information for the troubleshooting process. They also direct action for the next step you need to take in solving the problem. A subsequent question might be this: Were there network changes before or at the time the problem started? You open the door for numerous other questions while educating yourself, taking one step closer to the problem solution.

Step 4: Analyzing the Data Collected About the Problem

Now that you have collected data from various sources, you must analyze it to find the root cause or workaround for your problem. In many scenarios, you will find that your support vendor will ask or obtain this information to aid in efforts to troubleshoot. If part of your plan is to engage your support vendor, it is a good idea to have already gathered this information. This saves you quite a bit of time in the long run. In addition, it decreases the overall time to locate and resolve the issue you are having. For any piece of hardware, get to know your supporting vendor and what this person might or might not ask.

Tip Get to know your vendor and what this person might ask to help solve your issue. Having this material ahead of time reduces troubleshooting and resolution time.

Another good idea is to get experience and knowledge of the common troubleshooting tools that you might use to aid in problem resolution. An example of this is using sniffer tools to read packet captures or the debugging system of the WLC.

Narrow the List of Possible Causes

After you analyze the collected information data from monitoring tools, logs, and so on, you are in a position to logically narrow the list of possible causes of your problem. It is usually a good idea to start large and then work your way down to something more manageable. When problem identification is at a point that you can reasonably apply additional test methods, you can thoroughly investigate that particular cause and really put it to the test. In many cases, it is as easy as using common sense to reduce the list by 50 percent to 75 percent.

Determining the Proper Troubleshooting Tool

A plethora of troubleshooting tools is available. Most products sold on the market usually contain their own troubleshooting tools, debugs, or some form of diagnostic system. The large number of troubleshooting tools can make it extremely difficult to select which ones are best suited for the job. This book lays out the best tools, debugs, and troubleshooting tips to help you solve most issues that may arise. That way you are better prepared for whatever problem might surface—expected or unexpected.

Summary

Most network issues are reported with a generic description. For example, "All users on the wireless network are experiencing slow response to an application." You must be logical when reporting and troubleshooting the problem. It will be difficult to troubleshoot every user if someone reports that all users are experiencing latency. In many cases, there will be a working model and a nonworking model. A few examples would be a problem on a particular switch. If you had multiple switches in your network, you could compare the working switch to the switch that had the issue. The nice approach to this model is that even if you do not have any idea what is occurring, you can always take a packet capture of the working and nonworking switch and compare packet to packet. In another example, you could look at a problem with a client PC. You would start by listing the difference between the working and nonworking machine.

Tip When comparing equipment, try to find pieces that are close or identical.

You want to try to find machines that are inherently close to each other. The differences between each piece of equipment could invalidate your research and results.

After you have the list of differences between a working and nonworking PC, examine each difference by itself. You do this by removing the differences one at a time. If you remove more than one, you run the risk of solving the problem, without knowing which difference was the cause. One major flaw in the strategy is that you do not always have an accurate picture of the correctly running machine.

Troubleshooting methodology is critical when any network problem arises. You need to have the quickest and most efficient method in your head and at your fingertips. The difference could cost you resources and considerable time.

Chapter 2

Wireless LAN Controllers and Access Points

Cisco access points (AP) provide a way to extend wired networks or install network components where normal physical wiring cannot be installed. APs also provide an alternative solution to networking at a fraction of the cost. Cisco wireless solutions offer secure, manageable, and reliable wireless connectivity with exceptional range and performance. Cisco wireless solutions are offered in two mechanisms:

- A standalone device that interacts directly with the wired network.
- A two-part system that relies on a controller. APs talk directly to a controller or central-based piece of equipment, and this device interacts directly with the wired network.

Each mechanism is Wi-Fi certified for interoperability that offers support for various client devices. Both deployment mechanisms support 802.11a/b/g/n connectivity for indoor and outdoor environments. Many controllers and APs exist, a good portion of which were the creations of the autonomous or the controller technology. By the end of this book, you will have learned what product was intended for what solution and what will suit your business needs. However, you need to dig in and learn a little about the history before you begin.

Wireless LAN Controller Platforms

A range of models can work with any platform you have. The idea of the Wireless LAN Controller (WLC) is to simplify the deployment and operation of wireless networks. It is intended to offer a higher level of security, AP radio frequency (RF) management, single point of management, and mobility services.

The WLC also offers a variety of services, some of which are specific to the model of the controller. Later on in this chapter, you will learn about the functionality differences between the platforms. The main solution is data and voice networks. Within these networks, the WLC can provide wireless and wired guest services, location tracking, quality of service (QoS), and other varieties of 802.11a/b/g/n services. Everything mentioned here and more will be discussed in the future pages of this book.

Current Production WLCs

The controller models differ by their uplink interface size/speed and the number of APs they support. They also vary to a degree with the type of equipment that they interface with. The sections that follow briefly describe the current line of WLCs.

Cisco 5500 Series WLCs

The Cisco 5508, as pictured in Figure 2-1, is the most powerful WLC to date. It offers reliable performance, enhanced flexibility, and zero service loss for mission-critical wireless. This WLC platform was developed with the new 802.11n standard that offers up to nine times the performance of 802.11a/g networks.

Figure 2-1 *Cisco 5508 WLC*

The main improvements and new capabilities that the Cisco 5508 offers over the other controllers are as follows:

- Maximum Performance and Scalability:

  Support for up to 250 APs and 7000 clients

  Nine times the performance of 802.11a/g networks

  Ability to manage 250 APs simultaneously
- Improved Mobility and Services:

  Reliable connections even in the most demanding environments

  Larger mobility domain for more simultaneous client associations

  Uninterrupted network access when roaming

  Consistent streaming video and reliable, toll-quality voice
- Licensing Flexibility and Investment Protection:

  Option to add additional APs and feature licenses over time

  Optional WPLUS software, which supports the Cisco OfficeExtend solution and Enterprise Wireless Mesh

Cisco Catalyst 6500 Series Wireless Services Module

The Wireless Integrated Service Module (WiSM), as shown in Figure 2-2, is a card that fits in the 6500 chassis and actually houses two 4400 controllers on one blade. Each WLC actually supports 150 APs, allowing for a total of 300 APs. Each WLC in the WiSM has its own console port for access. This was the added benefit of purchasing a WiSM over two separate standalone 4404s—the additional 100 APs. This was the largest controller made until production of the 5508 WLC. Of course, there are plans for devices supporting far greater numbers of APs, such as the 5508.

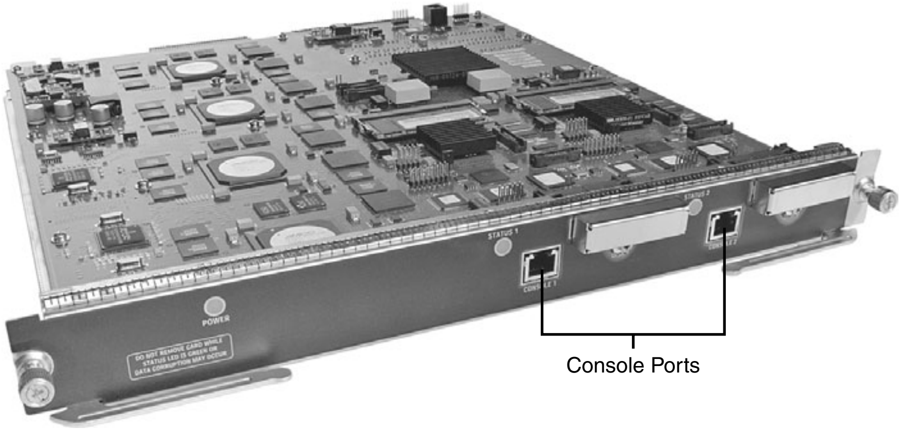


Figure 2-2 *Wireless Integrated Service Module*

The WiSM is typically referred to as the replacement for the Wireless LAN Services Module (WLSM). Cisco offered a trade-in program when the WiSM first came out as a way to increase migration to the WiSM.

Cisco Catalyst 3750G Integrated WLC

The WLC integrated 3750G takes the same approach as the WiSM but on a smaller scale. It is a single 4404 built into a 3750G switch. It is often referred to as the foxhound. The switch has 24 Ethernet 10/100/1000 ports with IEEE 802.3af and Cisco prestandard Power over Ethernet (PoE). It supports up to 50 APs. Figure 2-3 shows the 3750G integrated WLC.

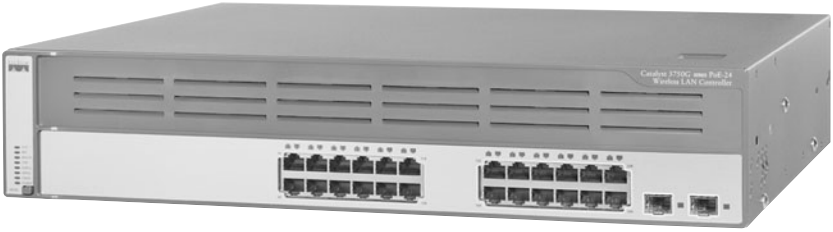


Figure 2-3 *3750G Integrated WLC*

Cisco 4400 Series WLCs

The 4400 series WLCs come in two models—the 4402 and the 4404, as shown in Figure 2-4. The 4402 has two gigabit connections, whereas the 4404 has four. The 4402 is sold in variants that support up to 50 APs, whereas the 4404 supports up to 100 APs.

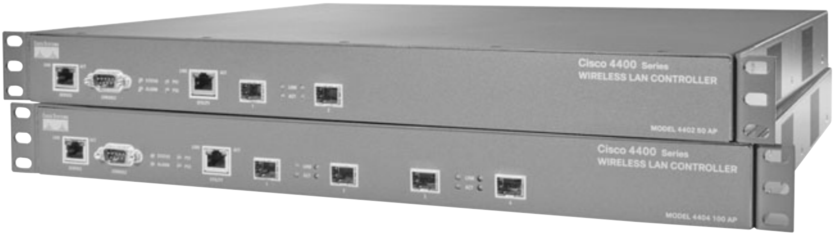


Figure 2-4 *4402 and 4404 WLCs*

Cisco 2100 Series WLCs

There are three models of the Cisco 2100 series WLCs shown in Figure 2-5. Each model correlates to the number of APs that it can support—2106, 2112, and 2125. The 2106 supports six APs, whereas the 2125 supports 25. There was a large architectural change between the old 2006 controller and the 2100 series controllers. The 2106 is now built on the ASA5505 platform. This offers much more functionality and capability than the 2006.

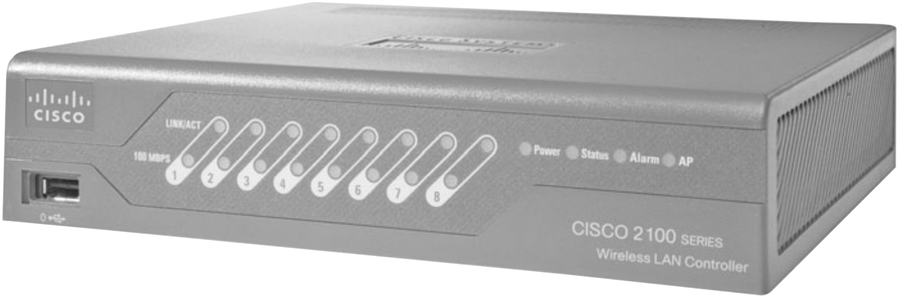


Figure 2-5 *2100 Series WLC*

Cisco Wireless LAN Controller Module

The Cisco Wireless LAN Controller Module (WLCM), shown in Figure 2-6, supports up to 25 Cisco Aironet APs and is supported on the Cisco 2800 and 3800 ISRs and 3700 series router. The WLCM is basically a 2106 sitting on a card that slides into a router. The WLCM is offered in four models: one that supports 6, 8, 12, and 25 APs.

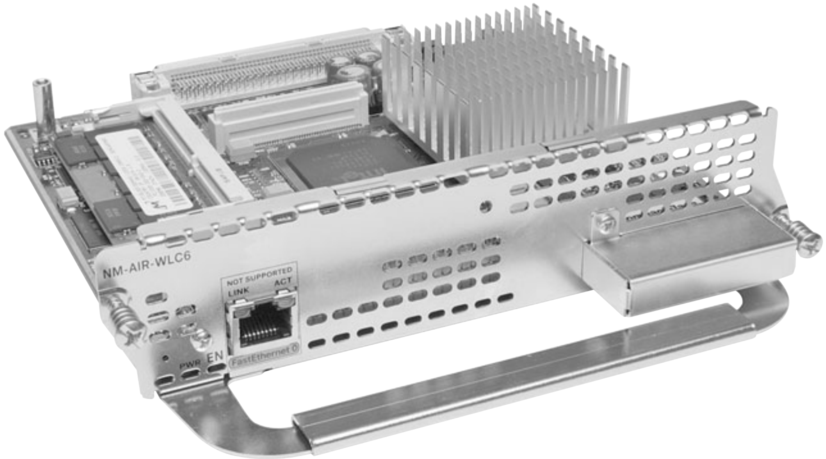


Figure 2-6 *WLCM*

Previous WLCMs

To understand how and why the current models were produced, you need to know the history of the products and the companies they came from. The acquisition of Airespace marked the Cisco entrance into the centrally controlled managed solution, which was selling and gaining ground much faster than the standalone AP approach. These models can be identified with the Airespace labeling even though they were sold as Cisco units. The units eventually were sold with the Cisco branding.

The newer brands are a bit different from their older counterparts. When Airespace introduced its line of controllers, one of its intentions was for the WLC to function like a switch. Customers were to use these controllers to plug their APs directly into the controller's ports. This design had its benefits and flaws. The design of these models restricted the overall design and implementation of wireless because you had to plug the APs directly into the unit. This is why you no longer see models like the 2000 or 4000 series WLCs.

This limited scalability from the product line was one of the major selling points and advantages over the typical standalone IOS-based APs. When applying this concept, the APs had to be located close to the controller and were limited to the length of the Ethernet cable.

The scalability factor is the understanding that you can have a network of any size and plug the APs into the network at any location regardless of geography. One AP might be located in Ohio and another in North Carolina. As long as they have IP connectivity back to the WLC, they establish communication with the controller and register. We will discuss the registration process in more detail in Chapter 8, "Access Point Registration."

Cisco 3500 Series WLCs

The 3504 WLC was the first generation small controller. It is similar to the 2006 in design, but it does not have the same hardware resources as the 2006. It contains less memory than the 2006 and similar models. The 2006 was a direct replacement for the 3504 and had improved hardware, although both were cosmetically identical. You have probably never run across these models unless you have been buying this equipment since Airespace started.

Tip You can install a 3504 image on a 2006, but you cannot install a 2006 image on a 3504 because the 2006 contains more memory than the 3504.

Cisco 4000 Series WLCs

The 4000 series had a few different models, including the 4012 and the 4024. The 12 and 24 were actually the number of 10/100 Ethernet ports that were located on the front of the box. These units did have one or two gigabit ports on the back of the box: 2-port SX or 1-port TX. The ports were also PoE, which was a nice feature. In addition, the units had console, service, and utility ports. The utility ports were always reserved for future users but ended up never providing functionality.

Cisco 2000 Series WLCs

The 2006 was the only model of 2000 series WLCs. The 6 referred to the number of APs it supported. This was and still is the smallest controller built as far as the number of APs supported. The 2006 had a 10/100 uplink that you could plug into a switch, enabling it to function like a larger WLC. The 2006 also had four Ethernet ports, a console port, and a utility port. What was unusual about the 2006 was the idea behind it. The model was built with the idea that people did not have to have a switch for it to work; they could plug the APs directly into the unit. Of course, it is difficult to do this when only four 10/100 Ethernet ports exist. Furthermore, one of the Ethernet ports had to be used as an uplink back to provide network connectivity, leaving only three ports. The 2006 did not have network processing units (NPU); it was more software based and limited to what it actually could do. The 2006 drawbacks were addressed with the release of the 2106, which is discussed in more detail in Chapter 5, “Network Design Considerations.”

Cisco 4100 Series WLCs

The 4100 series WLC was the first hybrid or migration over to the 4402 or 4404s that exist today. Having numerous Ethernet ports all over the box and plugging the APs directly into the box were finally abandoned. These changes were definitely huge benefits because they affected scalability to a high degree.

The 4100 series had one or two ports: one active and one standby. The 4400 utilized SFP modules instead of the 10/100 Ethernet ports.

Functionality Differences Between WLCs

There is actually a great deal of functionality difference in software depending on the model of the controller. If you do not understand the terminology or feature at this point, you will learn more as you progress through the book.

These software features are not supported on the 2000, 2100, and Network Module Controller (NMC) series controllers. The majority of these features *are* supported on the other WLC models:

- PoE for 2100 series controllers. PoE has only two designated ports.
- Service port (separate out-of-band management 10/100-Mbps Ethernet interface). The 2000 and 2100 series WLC does not contain a physical service port.
- Multicast is not supported on APs that are connected directly to the local port of a 2000 or 2100 series controller.
- VPN termination (such as IPsec and Layer 2 Tunneling Protocol [L2TP]) is not supported. IPsec is supported only on 3.2 code on the 4100/4400 models with a VPN module.
- Termination of guest controller tunnels is not supported. (Origination of guest controller tunnels is supported.) This is also known as a *mobility anchor*. The smaller WLC models cannot function as an anchor.
- External web authentication web server list is not supported.
- Layer 2 Lightweight Access Point Protocol (LWAPP) Transport mode is not supported. The 2000 series, 2100 series, and NMC are only L3 capable.

- Spanning tree is not supported.
- Port mirroring is not supported. This feature was originally designed for the multiport WLC platforms in mind. It is similar to a span session on a switch.
- Cranite is not supported.
- Fortress is not supported.
- AppleTalk is not supported.
- QoS per-user bandwidth contracts is not supported.
- IPv6 pass-through is not supported.
- Link aggregation (LAG) or ether channel is not supported.
- Multicast unicast Replication mode is not supported.

The Foxhounds (the 3750s with the built in 4402s) and WiSMs are only capable of link aggregation (LAG). This is also known as EtherChannel. Another point to remember is that the EtherChannel is not capable of channel negotiation; I am referring to Link Aggregation Control Protocol (LACP) or Port Aggregation Protocol (PAgP).

Tip LAG on the WLC does not support LACP or PAgP. Its mode is simply on: "Channel group mode ON." Also, the load-balancing algorithm is src-dst-ip:

```
switch(config)#port-channel load-balance src-dst-ip
```

The channel group mode is simply in the "ON" state. If your WLC is running LAG or ether channel, it must be in Layer 3 mode. All the 2000, 2100, and NMCs are only capable of Layer 3 mode. When Layer 2 or Layer 3 is referred to in the context, it is referring to the lwapp transport mode, and it is strictly a controller function. For now the only point of interest you need to know about Layer 2 and Layer 3 LWAPP transport mode is that in Layer 3 mode an AP-Manager interface is needed/created. The exception is the 5500 series, which does not require an AP-Manager. The management interface handles the AP communication. In addition, the transport mode is specific to LWAPP and has nothing to do with Control and Provisioning of Wireless Access Points (CAPWAP). In Layer 2 LWAPP mode, the APs do not require IP addresses but must be in the same subnet/network as the controller. There is also no AP-Manager interface configured on the WLC.

Note Layer 2 and Layer 3 WLC transport modes are specific only to LWAPP. CAPWAP operates only at Layer 3.

WLC Hardware and Software Requirements

The size of the wireless network you want to have determines the requirements. The first piece of hardware is a controller. You have to decide on the number of APs you want to have in your network. You also need to plan what applications you want to support over wireless. Some controller models support the same number of APs, but the hardware underneath is somewhat different. For instance, Cisco produces a WLC2125 and a WLC4402-25. Therefore, the question comes down to 4402 versus 2125, because both support 25 APs. The 4400 has two network processing units (NPU) and additional resources that the 2100 does not. The 2100 does not have an NPU but in its place has a smaller processor, and for the most part everything is handled in software. There is a phenomenal difference as far as the packet processing rate between the 4400 and the 2100. Neither video nor voice applications on a large scale would be possible for the 2125. The uplink is a 10/100 Ethernet cable, so you are restricted to this bottleneck. Chapter 5 goes much more into architecture of the devices, but the general idea is that a controller is required.

After you choose a controller, you choose an AP model. Again, what you are trying to accomplish determines the type of AP to go with. If your idea is to build a small wireless network, you can do so with a 2000/2100 series WLC and a single AP. You then have to connect this into your existing network. If you have a large wired network, the same principle basically applies. You can purchase a 4404 and connect the gigports into your switch infrastructure. Then you can connect the APs throughout your network. Finally, there has to be IP connectivity between the APs and the WLC. After you configure the controller, your wireless network is up and running.

Controller Requirements

The controller GUI requires the following operating system and web browser:

- Windows XP SP1 or higher or Windows 2000 SP4 or higher
- Internet Explorer 6.0 SP1 or higher
- Mozilla Firefox 2.0.0.11 or later

Note Internet Explorer 6.0 SP1 or higher is the only browser supported for accessing the controller GUI and for using web authentication.

Software Requirements

The Cisco WiSM requires software release SWISMK9-32 or later. The Supervisor 720 12.2(18)SXF2 supports the Cisco WiSM software Release 3.2.78.4 or later, and the Supervisor 720 12.2(18)SXF5 (Cisco IOS Software Modularity) supports the Cisco WiSM software Release 4.0.155.5 (with Cisco IOS Software Modularity). If you want to use the Cisco WiSM in the Cisco 7609 and 7613 Series Routers, the routers must be running Cisco IOS Release 12.2(18)SXF5 or later.

The Cisco WLC Network Module is supported on Cisco 28/37/38xx Series Integrated Services Routers running Cisco IOS Release 12.4(11)T2, 12.4(11)T3, and 12.5.

If you want to use the controller in the Catalyst 3750G WLC Switch, the switch must be running Cisco IOS Release 12.2.25.FZ or 12.2(25)SEE.

The 2112 and 2125 controllers are supported for use only with Software Release 5.1.151.0 or later.

Lightweight AP Models

The lingo for the APs can be tricky, but overall it is simple. APs come in two types or groups. Simply put, one group requires a controller to operate, and the other group does not. The APs that do not require a controller to operate also utilize IOS as their operating system. The exception to this rule is Remote-Edge AP (REAP) and Hybrid Remote Edge Access Point (H-REAP), which are discussed in the 1030 Section of this chapter. Table 2-1 summarizes the differences between lightweight and autonomous APs.

Table 2-1 *Typical Naming Conventions Based on Wireless Technology*

Lightweight	Autonomous
Thin	Thick
LWAPP/CAPWAP	IOS
Controller Based	Standalone
Airespace	Aironet

Cisco Aironet APs

Cisco Aironet APs provide secure, manageable, and reliable wireless connectivity with exceptional range and performance. Wi-Fi certified for interoperability with a variety of client devices, these APs support robust 802.11a/b/g connectivity for indoor and outdoor environments.

These lightweight APs—APs that have been converted to run LWAPP—operate with Cisco WLCs to address the security, deployment, management, and control issues facing large-scale enterprise wireless LANs (WLANs).

As key elements of the Cisco Unified Wireless Network—an integrated, end-to-end wired and wireless network solution—Cisco Aironet APs offer comprehensive capabilities, including the following:

- Wireless voice over IP

- Guest access
- Wireless intrusion detection and intrusion prevention
- Scalable Layer 3 roaming
- Location services

Aironet 1250 Series

You can deploy existing wireless technologies with the confidence that your network investment will extend to support emerging and future wireless technologies. The Cisco Aironet 1250 Series AP is a modular platform designed to make field upgrades easy and to support various wireless capabilities.

The Aironet 1250 Series is the first enterprise-class AP to support the IEEE 802.11n draft 2.0 standard. These APs do the following:

- Offer combined data rates of up to 600 Mbps to provide users with mobile access to high-bandwidth data, voice, and video applications regardless of their location. Keep in mind that the 1250 AP really only provides optimum performance data rate at approximately 300 Mbps.
- Use multiple-input multiple-output (MIMO) technology to provide reliable and predictable WLAN coverage.
- Improve user experience for both existing 802.11a/b/g clients and new 802.11n clients.

The Aironet 1250 Series is part of the Cisco Unified Wireless Network, a comprehensive solution that unifies the wired and wireless network to accomplish these tasks:

- Deliver a common set of services and applications
- Provide a single experience for any mode of network connectivity
- Offer simplified operational management

Aironet 1240 Series

Cisco Aironet 1240AG Series IEEE 802.11a/b/g APs deliver the versatility, high capacity, security, and enterprise-class features that WLAN customers demand. Designed specifically for challenging RF environments such as factories, warehouses, and large retail establishments, it has the versatility associated with connected antennas, a rugged metal enclosure, and a broad operating temperature range.

The Aironet 1240AG Series is available in three versions:

- A lightweight version
- An autonomous version that can be field-upgraded to lightweight operation

- A single-band 802.11g version for use in regulatory domains that do not allow 802.11a/5 GHz operation

The product comes complete with all the mounting hardware necessary for a secure, rugged installation. The mounting bracket locks the AP as well as the Ethernet and console cables in place to prevent theft and tampering.

Aironet 1230 Series

The Cisco Aironet 1230AG Series delivers the versatility, high capacity, security, and enterprise-class features required in more challenging RF environments. It is designed for WLANs in rugged environments or installations that require specialized antennas, and it features dual-antenna connectors for extended range, coverage versatility, and more flexible installation options. The Cisco Aironet 1230AG Series combines antenna versatility with industry-leading transmit power, receives sensitivity, and delays spread for high multipath and indoor environments, providing reliable performance and throughput for the most demanding requirements.

Aironet 1200 Series

The Cisco Aironet 1200 Series AP is a single-band lightweight or autonomous AP with dual diversity antenna connectors for challenging RF environments. It offers the same versatility, high capacity, security, and enterprise-class features demanded by industrial WLAN customers in a single-band 802.11g solution. The modular device provides the flexibility to field-upgrade to a dual-band 802.11a/g network by adding a CardBus-based 802.11a upgrade module that can be easily installed into Cisco Aironet 1200 Series APs originally configured for 802.11g. The device is available in either a lightweight version or an autonomous version that can be field-upgraded to lightweight operation.

Aironet 1100 Series

Extend security, reliability, and scalability to the WLAN with an integrated wired and wireless framework. The Cisco Aironet 1100 Series offers customers an easy-to-install, single-band 802.11b/g AP that features enterprise-class management, security, and scalability. The device is available in an autonomous or lightweight version and is ideal for deployment in offices and similar environments.

Aironet 1130AG Series

The Cisco Aironet 1130AG Series packages high capacity, high security, and enterprise-class features delivering WLAN access for a low total cost of ownership. Designed for WLAN coverage in offices and similar RF environments, this unobtrusive AP features integrated antennas and dual IEEE 802.11a/g radios for robust and predictable coverage, delivering a combined capacity of 108 Mbps. The competitively priced Cisco Aironet 1130AG Series is ready to install and easy to manage, reducing the cost of deployment and ongoing maintenance.

Aironet 1140N Series

The Cisco Aironet 1140N is the next generation dual-band AP targeting indoor, carpeted area RF applications that are typically found in the ideal office space. The primary function of the 1140N series AP is that it is a dual-band AP with integrated 802.11n radios and integrated antennas.

Aironet 1300 Series

The Cisco Aironet 1300 Series Outdoor AP/Bridge is a flexible platform with the capability of AP, bridge, and workgroup bridge functionality. The Cisco Aironet 1300 Series provides high speed and cost-effective wireless connectivity between multiple fixed or mobile networks and clients. Building a metropolitan area wireless infrastructure with the Cisco Aironet 1300 Series offers deployment personnel a flexible, easy-to-use solution that meets the security requirements of wide area networking professionals. Typical applications for the Aironet 1300 Series are as follows:

- Network connections within a campus area
- Outdoor infrastructure for mobile networks and users
- Public access for outdoor areas
- Temporary networks for portable or military operations

The Cisco Aironet 1300 Series supports the 802.11b/g standard—providing 54 Mbps data rates with a proven, secure technology. Cisco makes the maintenance and installation of the 1300 Series easy by integrating it with your wired network. Based on the Cisco IOS operating system, the Cisco Aironet 1300 Series has advanced features such as Fast Secure Layer 2 Roaming, QoS, and VLANs. This series has the following key benefits:

- Configurable for AP, bridge, or workgroup bridge roles
- Support for both point-to-point or point-to-multipoint configurations
- Enhanced security mechanisms based on 802.1x standards
- Ruggedized enclosure optimized for harsh outdoor environments with extended operating temperature range
- Integrated or optional external antennas for deployment flexibility

Aironet 1400 Series

The Cisco Aironet 1400 Wireless Bridge creates a new benchmark for wireless bridging by providing a high-performance and feature-rich solution for connecting multiple LANs in a metropolitan area. Building a metropolitan area wireless infrastructure with the Cisco Aironet 1400 gives deployment personnel a flexible, easy-to-use solution that meets the security requirements of wide area networking professionals. Designed to be a cost-effective alternative to leased lines, it is engineered specifically for harsh outdoor environments.

The Cisco Aironet 1400 Wireless Bridge is the premier high-speed, high-performance outdoor bridging solution for line-of-sight applications, providing features such as these:

- Support for both point-to-point or point-to-multipoint configurations
- Industry-leading range and throughput, supporting data rates up to 54 Mbps
- Enhanced security mechanisms based on 802.11 standards
- Ruggedized enclosure optimized for harsh outdoor environments with extended operating temperature range
- Models with integrated antennas or models with connectors (must purchase an antenna, which is sold separately) for flexibility in deployment
- Designed specifically for ease-of-installation and operation

Aironet 1500 Series

Cisco Aironet 1500 Series lightweight outdoor mesh AP provides the security, manageability, reliability, and ease of deployment to create high-performance WLANs for outdoor wireless networks.

The Cisco Aironet 1500 Series operates with Cisco WLCs and Cisco Wireless Control System (WCS) Software, centralizing key functions of WLANs to provide scalable management, security, and mobility that is seamless between indoor and outdoor deployments. Designed to support zero-configuration deployments, the Cisco Aironet 1500 Series easily and securely joins the mesh network and is available to manage and monitor the network through the controller and WCS graphical or command-line interfaces (CLI). Compliant with Wi-Fi Protected Access 2 (WPA2) and employing hardware-based Advanced Encryption Standard (AES) encryption between wireless nodes, the Cisco Aironet 1500 Series provides end-to-end security.

Aironet 1520 Series

The Cisco Aironet 1520 Series wireless broadband platform is a high-performance outdoor wireless mesh product for a cost-effective, scalable, and secure deployment in outdoor environments such as municipalities, public safety environments, and oil and gas or other outdoor enterprises.

The Cisco Aironet 1520 Series delivers design innovation for radio versatility and provides flexibility for deploying wireless mesh networks in dynamic environments.

This platform has the following key features and benefits:

- **Versatile:** Provides a platform that enables mobility regardless of the frequency band required, with universal slots that allow for rapid development and integration of radio technology

- **Extensible:** Enables the broadband wireless infrastructure to easily and securely extend services to third-party devices such as IP cameras and automated meter readers in the harshest environmental conditions
- **Fortified:** Provides the highest standard of security with a secure rugged enclosure and the Cisco Self-Defending Network architecture

The 1520 Series wireless broadband platform operates with Cisco WLAN controllers and Cisco Wireless Control System (WCS) software, centralizing key functions of WLANs to provide scalable management, configuration, security, and transparent mobility between indoor and outdoor environments.

Airespace APs

This is the only portion of the book referring to Airespace and the 1000 series APs. Cisco acquired the company in early 2005 and consolidated the product line into the Aironet series. The premise behind the Aironet wireless network was that the APs would be in a standalone mode. Airespace took a different approach and developed a smaller and cheaper AP, often referred to as a thin or lightweight AP, which relied on a controller to function. The Airespace product line did not need as much hardware because it had a controller performing the majority of the functionality for the APs. For instance, the Aironet APs had faster processors and more memory because they had more tasks to perform and had to operate as a standalone unit.

Cisco found out it was able to develop the best AP by taking the benefits of both AP product lines and merging them. In addition, Cisco had already sold large numbers of the standalone AP models and needed a way for existing wireless customers to take advantage of this new technology. The solution here was to provide a conversion method for existing wireless customers. For these customers, Cisco developed code and a conversion utility so people had the option of converting their wireless network to a controller base network without purchasing all new equipment. As far as hardware, existing customers only needed to purchase a controller and convert their old IOS APs, and they had the new controller-based wireless technology. The new technology worked out for everyone in the long run, but it was even better for customers who had the original IOS-based APs. These units ended up being the core AP that Cisco would market and support. They also supported H-REAP, whereas the 1000 series could support only REAP.

The 1000 series APs are supported up to the 4.2.x software train. The older 1000 series APs are also labeled as AS1200. The AS letters referred to the Airespace company prior to Cisco acquiring the company. This model line, which is almost identical to the 1000 series, is last supported in the 4.0.x train. With that said, this chapter is going to briefly discuss the 1000 series; it will be the last reference to this series in the book. However, this does not mean to stop reading here if you do have a wireless network with the 1000 series APs. The functionality will still apply up to the versions mentioned earlier. You will still benefit greatly from this material, and much of it is still applicable to your current setup.

1010 Series APs

The 1010 offers two internal antennas and is the basic entry-level AP offered. This AP with the internal antennas was strictly for indoor applications.

1020 Series APs

The 1020 AP has two internal antennas and two connectors for the use of external antennas. This allows placement of antennas in environments that were not possible with the 1010 AP. The AP with external antennas allowed indoor and outdoor access.

1030 Series APs

The 1030 AP has two internal antennas and two connectors for the use of external antennas. This allows placement of antennas in environments that were not possible with the 1010 AP. The AP with external antennas allowed indoor and outdoor access. This device is also capable of performing a feature known as REAP. The idea behind a REAP is that it can be placed at branch offices to communicate with centrally located WLAN controllers. The REAP transverses the WAN to get to the centrally located controller. When the WAN connection breaks, the AP is still up and operational to provide wireless services. However, this service has limitations, which will be discussed in the AP 1000 Series Limitations Section.

AP 1000 Series Functionality Differences

The main difference between the 1010 and the 1020 is that the 1020 comes with external antenna adapters, whereas the 1010 does not. The 1010 has to use the internal dual omnidirectional antennas that are built into the AP. The 1030 AP is comparable to the 1020 AP because it also contains external antenna adapters. The main difference between the 1020 and the 1030 is that the 1030 has the ability to perform REAP. This allows APs in remote offices or locations to remain active if the link to the controller goes down. REAP does have limitations, however, which is why H-REAP was developed. This will be discussed in the AP1000 Series Limitations Section and also in Chapter 5.

AP 1000 Series Limitations

The main requirement for the 1000 series AP is that it must run on controller version 4.2 or earlier. The support as far as software ends with 4.2.

The 1030 AP has REAP, Remote Edge Capability; with this in mind, there are limitations as outlined in Table 2-2.

Table 2-2 shows the various REAP mode features.

Table 2-2 *REAP Mode Features*

		REAP (Normal Mode)	REAP (Standalone Mode)
Protocols	IPv4	Yes	Yes
	IPv6	Yes	Yes
	All other protocols	Yes (only if client is also IP enabled)	Yes (only if client is also IP enabled)
	IP Proxy ARP	No	No
WLAN	Number of SSIDs[1]	16	1 (the first one)
	Dynamic channel assignment	Yes	No
	Dynamic power control	Yes	No
	Dynamic load balancing	Yes	No
VLAN	Multiple interfaces	No	No
	802.1Q support	No	No
WLAN Security	Rogue AP detection	Yes	No
	Exclusion list	Yes	Yes (existing members only)
	Peer-to-peer blocking	No	No
	IDS[2]	Yes	No
Layer 2 Security	MAC authentication	Yes	No
	802.1X	Yes	No
	WEP (64/128/152bits)	Yes	Yes
	WPA-PSK	Yes	Yes
	WPA2-PSK	Yes	No
	WPA-EAP	Yes	No
	WPA2-EAP	Yes	No

[1] *SSID = Service Set Identifier*

[2] *IDS = Intrusion Detection System*

(Continues)

Table 2-2 *REAP Mode Features (Continued)*

		REAP (Normal Mode)	REAP (Standalone Mode)
Layer 3 Security	Web authentication	No	No
	IPsec	No	No
	L2TP	No	No
	VPN pass-through	No	No
	Access control lists	No	No
QoS	QoS profiles	Yes	Yes
	Downlink QoS (weighted round-robin queues)	Yes	Yes
	802.1p support	No	No
	Per-user bandwidth contracts	No	No
	WMM	No	No
	802.11e (future)	No	No
	AAA QoS profile override	Yes	No
Mobility	Intra-subnet	Yes	Yes
	Inter-subnet	No	No
DHCP	Internal DHCP server	No	No
	External DHCP server	Yes	Yes
Topology	Direct connect (2006)	No	No

Lightweight Compared to Traditional Autonomous APs

There are immense differences between lightweight and traditional autonomous APs. This chapter touches on some of the major functionality differences, but the complete explanations are discussed in remaining chapters. Although the autonomous AP is an effective solution, it does lack some of the benefits of the controller-based solution. In certain niches, autonomous systems thrive. However, as the controller-based solutions continue to develop, these niches are disappearing. The Home Office AP will eliminate many of the drawbacks because it will offer a VPN solution without the necessity of an onsite controller.

Scalability

As you will see, one of the strongest advantages of the controllers is all the levels of scalability they can offer. You can easily integrate them in virtually any type of network. This does not mean you have to console or Telnet into the device and configure the unit prior to connecting to your network. The scalability factor offers you the benefit of placing an AP straight out of the box onto your network. The controller itself then configures and provisions the unit. If you want to further manage the AP, you can do so straight from the controller or from a WCS application.

Note APs placed in different Layer 3 subnets of the controller require a discovery mechanism.

RRM

Radio Resource Management (RRM) allows the controller to dynamically control power and channel assignment of APs. Controllers can work together to ensure that your wireless network operates as smoothly as possible. RRM is quite comprehensive, so this book does not go into further detail until Chapter 12, “Radio Resource Management. RRM allows self-healing to take place if an AP fails. It also allows for the wireless network to adapt to RF interference or environmental issues.

Caution RRM is *not* a substitute for a site survey.

General Overview of RRM

Along with the marked increase in the adoption of WLAN technologies, deployment issues have similarly risen. The 802.11 specification was originally architected primarily with a home, single-cell use in mind. The contemplation of the channel and power settings for a single AP was a trivial exercise, but as pervasive WLAN coverage became one user expectation, determining the settings for each AP necessitated a thorough site survey. Thanks to the shared nature of the 802.11 bandwidth, the applications that are now run over the wireless segment are pushing customers to move to more capacity-oriented deployments. The addition of capacity to a WLAN is an issue unlike that of wired networks, where the common solution is to throw bandwidth at the problem. Additional APs are required to add capacity, but if they are configured incorrectly, they can actually lower system capacity because of interference and other factors. As large-scale, dense WLANs have become the norm, administrators have continuously been challenged with these RF configuration issues that can increase operating costs. If handled improperly, this can lead to WLAN instability and a poor end user experience.

With a finite spectrum (a limited number of nonoverlapping channels) to play with and the innate desire of RF to bleed through walls and floors, designing a WLAN of any size has historically proven to be a daunting task. Even given a flawless site survey, RF is ever-changing; what might be an optimal AP channel and power schema one moment might prove to be less than functional the next.

Enter the Cisco RRM. RRM allows the Cisco Unified WLAN Architecture to continuously analyze the existing RF environment, automatically adjusting the AP power levels and channel configurations to mitigate such things as cochannel interference and signal coverage problems. RRM reduces the need to perform exhaustive site surveys, increases system capacity, and provides automated self-healing functionality to compensate for RF dead zones and AP failures.

Self-Healing Mechanism

Another huge benefit of the WLC is the automation of the self-healing process. When an AP radio fails, the other APs power their radios up and adjust channel selection of neighbor APs to compensate for the lost wireless coverage. You will learn more about this feature and others related to the self-healing mechanism in Chapter 12, but this determination is made when neighbor APs no longer see RF neighbor messages from the suspected failed AP. Although this sounds like a good idea in theory, deployment plays a major role for this feature to work. The system must be designed to support self-healing capabilities. Specifically, APs must be placed so that the system has at least one power level available to move up if RF self-healing is activated. If the deployment were too dense, a failing AP might actually be a benefit. On the other hand, if the deployment were not dense enough and the APs were already at the highest power level, powering up or changing channels is not going to benefit anyone.

WLC Features

The controller-based solution offers a range of features. With each passing day, more and more functionality is added to make the life of a wireless administrator easier or to allow more flexibility with the current networks. For instance, following are some of the newest features currently available:

- **40-MHz channelization:** In controller software releases prior to 5.1.151.0, dynamic channel assignment (DCA) supports only those radios using 20-MHz channelization. In controller software Release 5.1.151.0, DCA is extended to support 802.11n 40-MHz channels in the 5-GHz band. 40-MHz channelization allows radios to achieve higher instantaneous data rates (potentially 2.25 times higher than 20-MHz channels).

Caution DCA does not support radios using 40-MHz channelization in the 2.4-GHz band.

You can override the globally configured DCA channel width setting by statically configuring the radio of an AP for 20- or 40-MHz mode on the 802.11a/n Cisco APs > Configure page. If you ever change the static RF channel assignment method to Global on the AP radio, the global DCA configuration overrides the channel width configuration that the AP was previously using.

Caution Cisco recommends that you do not configure 40-MHz channels in the 2.4-GHz radio band because severe cochannel interference can occur.

- **AP failover priority:** Each controller has a defined number of communication ports for APs. When multiple controllers with unused AP ports are deployed on the same network and one controller fails, the dropped APs automatically poll for unused controller ports and associate with them. Starting in controller software release 5.1.151.0, you can configure your wireless network so that the backup controller recognizes a join request from a higher-priority AP and if necessary disconnects a lower-priority AP as a means to provide an available port.

Caution Failover priority takes effect only if the number of association requests following a controller failure exceeds the number of available backup controller ports.

- **EAP-FAST/802.1X supplicant:** You can configure 802.1X authentication between a Cisco Aironet 1130, 1240, or 1250 series AP and a Cisco switch. The AP acts as an 802.1X supplicant and is authenticated by the switch using EAP-FAST with anonymous PAC provisioning.

  The following switches and minimum software releases are currently supported for use with this feature:

  Cisco Catalyst 3560 Series Switches with Cisco IOS Release 12.2(35)SE5

  Cisco Catalyst 3750 Series Switches with Cisco IOS Release 12.2(40)SE

  Cisco Catalyst 4500 Series Switches with Cisco IOS Release 12.2(40)SG

  Cisco Catalyst 6500 Series Switches with Supervisor Engine 32 running Cisco IOS Release 12.2(33)SXH

- **NAC out-of-band integration:** The Cisco NAC Appliance, also known as Cisco Clean Access (CCA), is a network admission control (NAC) product that identifies whether machines are compliant with security policies and repairs vulnerabilities before permitting access to the network. In controller software releases prior to 5.1.151.0, the controller integrates with the NAC appliance only in in-band mode, where the NAC appliance must remain in the data path. For in-band mode, a NAC appliance is required at each authentication location (such as at each branch or for each controller), and all traffic must traverse the NAC enforcement point. In controller software release 5.1.151.0, the controller can integrate with the NAC appliance in out-of-band mode, where the NAC appliance remains in the data path only until clients have been analyzed and cleaned. Out-of-band mode reduces the traffic load on the NAC appliance and enables centralized NAC processing.

- **WAN link latency:** You can configure link latency on the controller to monitor the round-trip time of the LWAPP heartbeat packets (echo request and response) from the AP to the controller and back. This time can vary based on network link speed and controller processing loads. You can use this feature with all APs joined to the controller, but it is especially useful for hybrid-REAP APs, for which the link might be a slow or unreliable WAN connection.

For a more complete list of features, please consult the Cisco Command reference guide or the controller configuration guide.

Central Management

The WLCs offer much easier and varied device management than the conventional standalone or autonomous AP. A WLC can offer to management anywhere from 6 to 150 APs from a single WLC or a single connection. Currently, you can access the WLC using the following methods:

- Telnet
- Secure Shell (SSH)
- HTTP
- HTTPS
- Console
- Service Port (if applicable)
- Management VIA Wireless

As you can imagine, if your task were to configure IP addresses and host names on 100 APs, you would need to manually access each device or use network management software such as WLSE. However, WLSE offers a different kind of management and is limited in what it can do. This configuration request and much more can be accomplished from a single WLC that the APs are registered to. If more than one controller is in use, the WCS can come into play, which is discussed in more detail in Chapter 6, "Understanding the Troubleshooting Tools."

Cisco WCS

Cisco WCS is an ideal software application that is used for WLAN planning, configuration, and management. Cisco WCS provides a powerful foundation that allows IT managers to design, control, and monitor enterprise wireless networks from a centralized location, simplifying operations and reducing the total cost of ownership.

The Cisco WCS is an optional network component that works in conjunction with Cisco Aironet Lightweight APs, Cisco WLCs, and the Cisco Wireless Location Appliance. With Cisco WCS, network administrators have a single solution for RF prediction, policy provisioning, network optimization, troubleshooting, user tracking, security monitoring, and WLAN systems management. Robust graphical interfaces make WLAN deployment and operations simple and cost-effective. Detailed trending and analysis reports make Cisco WCS vital to ongoing network operations.

Cisco WCS includes tools for WLAN planning and design; RF management; location tracking; IDS; and WLAN systems configuration, monitoring, and management.

Note WCS is *not* a necessary component for a wireless network. WCS has no effect on the controllers or APs. Certain actions you perform on WCS can affect service; nevertheless, the WLC (hardware) does not depend on WCS (software).

Cisco Wireless Location Appliance

The Cisco Wireless Location Appliance is the first location solution in the industry that simultaneously tracks thousands of devices from within the WLAN infrastructure, bringing the power of a cost-effective, high-resolution location solution to critical applications such as these:

- High-value asset tracking
- IT management
- Location-based security

This easy-to-deploy solution smoothly integrates with Cisco WLAN Controllers and Cisco lightweight APs to track the physical location of wireless devices to within a few meters. This appliance also records historical location information that can be used for location trending, rapid problem resolution, and RF capacity management.

The Cisco Wireless Location Appliance facilitates the deployment of new and important business applications by integrating tightly with a spectrum of technology and application partners through an open application programming interface (API). This integration helps enable the deployment of powerful location-based applications such as the following:

- Enhanced 911 (E911) services
- Asset management
- Workflow automation

Customers deploying this solution include government organizations and enterprises in the health care, finance, retail, and manufacturing industries.

Cisco WCS Navigator

The Cisco WCS Navigator delivers an aggregated platform for enhanced scalability, manageability, and visibility of large-scale implementations of the Cisco Unified Wireless Network. This powerful, software-based solution gives network administrators cost-effective, easy access to information from multiple, geographically diverse Cisco WCS management platforms.

The Cisco WCS Navigator supports partitioning of the unified wireless network at the management level. It supports up to 20 Cisco WCS management platforms with manageability of up to 30,000 Cisco Aironet lightweight APs from a single management console. It runs on a server platform with an embedded database.

The Cisco WCS Navigator centralizes the operational control and management of multiple Cisco WCS management platforms. This easy-to-use platform delivers the following cross-system capabilities:

- Network monitoring
- Aggregated alarm notifications
- Automated browser redirect
- Simplified setup and configuration
- Quick and advanced searches
- Location tracking of client, Wi-Fi, and rogue devices
- Inventory reports
- Secure administrative access

In summary, the WCS Navigator manages multiple installations of WCS. It is the same approach as WCS monitoring and managing multiple WLCs. To understand the place of Navigator in a network, refer to Figure 2-7.

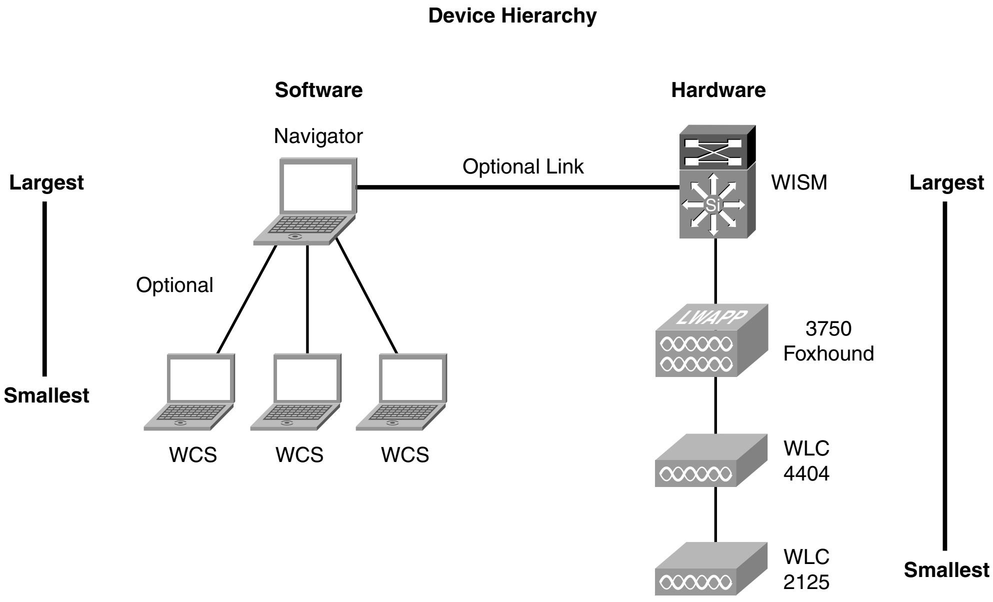


Figure 2-7 *Device Hierarchy*

Note Navigator is just like WCS in that it is neither necessary nor affects the uptime of your wireless network if it is not functional or present.

Summary

As far as industry trends are considered, wireless networks are certainly in high demand and growing at a phenomenal rate. The wireless technology is also expanding at an astounding rate. The standardization of 802.11n and Outdoor/Indoor Mesh adds yet another chapter to wireless technology. Mesh networks allows cities to deploy wireless networks citywide. Mesh networks were designed primarily for private city use, but this is changing. Some cities have already proposed providing free wireless networking to the public. As time goes on, you will see continual deployments of wireless networks and further developments of the technology. Wireless networks are here to stay.

The wireless transport has certainly changed within the past few years. The introduction of LWAPP and the standardization of CAPWAP have drastically changed wireless. Prior wireless deployments were deployed as "Autonomous" systems. The downside to Autonomous systems was that they were standalone devices requiring configuration on a per-unit basis. In a hospital environment, for example, configuring and deploying more than 300 APs could take some time. Technology such as WLSE, WLSM, and WDS made these deployments a little easier; however, it still required a great deal of labor to install and tweak (adjust to the RF in your environments) a wireless network. This is usually one of the greater challenges. Although controller-based solutions did not eliminate this step, they certainly made it easier. On the plus side for the autonomous system, if you are installing wireless in a small site that requires only one or two APs, the autonomous system is a much more cost-effective solution. Since the controller-based wireless solution started becoming popular, it developed technologies such as REAP and H-REAP to cover this limitation; this book will discuss these concepts in Chapter 5. Regardless of the wireless system, a site survey is always recommended.

This page intentionally left blank

Chapter 3

Introduction to LWAPP

Traditional wireless LAN (WLAN) deployments used X number of access points (AP) spread across the premises that needed wireless coverage. With standalone, each AP was an individual entity that needed configuration, monitoring, provisioning, and so on. If these tasks were required for only a few devices, they would be manageable; however, when you are talking about a full enterprise WLAN that might be offering advanced services such as Voice over Wireless, the management of each AP becomes daunting.

You can add additional complexities to an enterprise WLAN, such as radio frequency (RF) management (dynamically adapt to changes in the environment) and security, which is critical in wireless because of the broadcast nature of the medium.

Unless some kind of coordination is put in place, enterprise WLANs will hit scalability and practical limitations sooner or later. The Lightweight Access Point Protocol (LWAPP) was designed to overcome those limitations and expand the feature set and uses of WLANs without increasing the management burden or weakening the security standpoint of the enterprise.

LWAPP is not a "general" solution. In some scenarios, a traditional AP is best—for example with Point to Point bridging, where no coordination or RF monitoring is needed because of the characteristics of the controlled environment for this deployment.

Defining LWAPP

Given the explosion in growth for wireless networks and the ubiquity that these services have in the current enterprise, vendors have implemented multiple approaches to simplify the operation and deployment of wireless services.

Proposed as a potential way of simplifying the operation of wireless networks, LWAPP has been implemented across the Cisco Unified Wireless Networks set of products (Wireless LAN Controller [WLC], APs, and related devices) from their initial software release until version 5.1. New versions, in particular 5.2, are using Control and Provisioning of Wireless Access Points (CAPWAP) as the base protocol.

Formally speaking, LWAPP is described in several drafts of the Internet Engineering Task Force (IETF) CAPWAP working group, the latest of which (at press time) is Version 4 (draft-ohara-capwap-lwapp-04.txt). Cisco Systems, Inc. submitted this draft for standardization in 2004, and through a protocol evolution, CAPWAP is the end result. Chapter 4, "The CAPWAP Protocol," covers CAPWAP in greater detail. Even though LWAPP never became an RFC standard like CAPWAP (http://www.ietf.org/rfc/rfc5415.txt) has, LWAPP is still a relevant and widely used protocol.

The ideas behind LWAPP are as follows:

- Move the traffic forwarding, certain security functions such as authentication, and policy functions from the edge (AP) toward a centralized point.
- Simplify the AP, because higher-level functions are now done separately, which reduces AP complexity and cost.
- Provide an encapsulation and transport mechanism for wireless traffic.
- Centralize AP configuration and management.

LWAPP is a way for an AP to communicate directly with a management entity—the WLC. This new approach to the wireless networks was designed to have nodes or points of presence throughout a network. These node devices would not require configuration and would rely on a master device for their configurations and instructions. These nodes would exist to provide a point in the network to which a wireless user can connect. After a user connects, all traffic going to this node would be sent to the master device. The master device would then determine where in the network or on what virtual LAN (VLAN) the packet needed to go. This approach offers many advantages over the single device configuration setup but requires a protocol to provide constant connectivity and direction for these devices to operate. LWAPP provides the solution.

Although in official standard documents the APs are referred to as wireless termination points (WTP) and the WLCs as access controllers (AC), this book uses the more commonly known terms AP and WLC, or controller, to refer to the "wireless" and "aggregation" points respectively, to make it easier to follow the discussions throughout the book.

In Chapter 13, "H-REAP," we will discuss that the forwarding model of "all traffic" is sent from the AP to the WLC, is true only for a particular mode of operation of LWAPP, and has additional hybrid modes to solve several design needs.

Quick Protocol Overview

Briefly, LWAPP operation is as follows:

Step 1. AP tries to discover a list of valid WLCs with which to associate or *join*.

Step 2. When this discovery process is successful, the AP selects a WLC and then tries to join it.

Step 3. Upon join, the AP checks to see if the software version it is running matches that of the WLC. If it does not, the AP initiates an upgrade process (*image*).

Step 4. If an image process was done, the AP reloads and goes through the discovery/join process again. If the AP now has the correct software version, it receives the configuration from the WLC.

Step 5. Depending on the configuration received, the AP might need to do a reload (for example, the AP mode is changed) and pass through the discovery/join steps again.

Step 6. After newly joining and confirming that it now has the correct configuration and image, the AP transitions into *run* status and starts servicing clients.

Step 7. During this run status, the AP periodically sends RF and security monitoring information to the WLC for aggregation and processing.

LWAPP has two main traffic types, as seen in Figure 3-1:

- **Control:** Management traffic between AP and WLC. It is a control channel for configuration, session management, firmware management, and so on. Traffic is encrypted and authenticated.
- **Data:** Wireless traffic, encapsulated, sent between AP and WLC. You can make an analogy to a GRE-Tunnel.

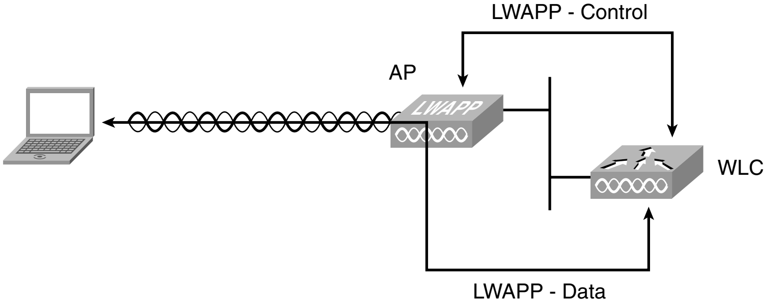


Figure 3-1 *LWAPP Traffic Types*

As Figure 3-2 and Figure 3-3 illustrate, LWAPP has two encapsulation types:

- **Layer 2:** All communication between the AP and WLC is done on top of native 802.3 Ethernet frames, with an Ethertype of 0xbbbb or 0x88bb, depending on the release.
- **Layer 3:** LWAPP is carried over IP/User Datagram Protocol (UDP), using port numbers 12222 and 12223 (data and control, respectively).