

“All-in-One Is All You Need.”

ALL-IN-ONE

CCT[®]/CCNA[®]

Routing and Switching

EXAM GUIDE

EXAMS 100-490 & 200-301

Online content includes:

- Customizable exam engine with 290+ practice questions
- Video training from the author
- Glossary in PDF format
- Lab book and lab solutions PDFs

Complete coverage of all objectives for both exams

Ideal as both a study tool and an on-the-job reference

Filled with practice exam questions and in-depth explanations

Over 45 lab exercises and sample performance-based questions

**Mc
Graw
Hill**

GLEN E. CLARKE

CCT, CCNA, MCSE, MCS D, CEH™, CHFI™

RICHARD DEAL

CCNA, CCNP®, CCDA®, CCDP®

ABOUT THE AUTHORS

Glen E. Clarke, CCT, CCNA, MCITP, MCSE, MCSD, MCDBA, MCT, CEH, CHFI, CISSO, PenTest+, Security+, Network+, A+, is a technical trainer and owner of DC Advanced Technology Training (DCATT), an IT training company based out of Halifax, Nova Scotia. Glen spends most of his time delivering certified courses on Windows Server, Office 365, Hyper-V, SQL Server, Exchange Server, SharePoint, Visual Basic .NET, and ASP.NET. Glen also teaches a number of security-related courses covering topics such as ethical hacking and countermeasures, computer forensics and investigation, penetration testing, and information systems security officer. Glen also teaches a number of networking courses such as Cisco CCT, Cisco CCNA, and packet analysis.

Glen is an experienced author and technical editor whose published work was nominated for Referenceware Excellence Awards. Glen has authored numerous certification preparation guides, including the *CompTIA Network+ Certification Study Guide*, the *CompTIA Security+ Certification Study Guide*, the *CompTIA PenTest+ Certification for Dummies*, and the best-selling *CompTIA A+ Certification All-In-One for Dummies*.

When he's not working, Glen loves to spend quality time with his wife, Tanya, and their four children, Sara, Brendon, Ashlyn, and Rebecca. You can visit Glen online at www.dcatt.ca or contact him at glenclarke@dcatt.ca.

For almost 20 years, **Richard Deal** has operated his own company, The Deal Group, Inc., in Oviedo, Florida, east of Orlando. Richard has more than 25 years of experience in the computing and networking industry, including networking, training, systems administration, and programming. In addition to earning a B.S. in mathematics from Grove City College, he holds many certifications from Cisco and has taught many beginning and advanced Cisco classes. Richard is the author of *Cisco ASA Configuration*, an in-depth book on Cisco's ASA firewall appliances and their implementation, published by McGraw Hill. Richard is also the author of two books with Cisco Press: *The Complete Cisco VPN Configuration Guide* and *Cisco Router Firewall Security*; both books made it to Cisco's CCIE Security recommended reading list.

About the Technical Editor

Edward Tetz graduated in 1990 from Saint Lawrence College in Cornwall, Ontario, with a degree in business administration. Since that time, he has spent his career delivering certified technical training for a Microsoft Training Center and working as a service delivery professional in both Halifax, Nova Scotia, and Ottawa, Ontario. Over his career, Ed has supported Apple Macintosh, IBM OS/2, Linux, Novell NetWare, and all Microsoft operating systems from MS-DOS to Windows Server 2019, as well as hardware from most of the major manufactures. Ed currently works for Microsoft in Customer Success in Ottawa, supporting enterprise and government customers.

When not working with technology, Ed spends time with his wife, Sharon, and his two daughters, Emily and Mackenzie.

ALL ■ IN ■ ONE

CCT®/CCNA®

Routing and Switching

EXAM GUIDE

(Exams 100-490 & 200-301)

Glen E. Clarke
Richard Deal



New York Chicago San Francisco
Athens London Madrid Mexico City
Milan New Delhi Singapore Sydney Toronto

McGraw Hill is an independent entity from Cisco Systems®, Inc. and is not affiliated with Cisco Systems, Inc. in any manner. This study/training guide and/or material is not sponsored by, endorsed by, or affiliated with Cisco Systems, Inc. in any manner. This publication and accompanying media may be used in assisting students to prepare for the Cisco Certified Technician (CCT) and Cisco Certified Network Associate (CCNA) exams. Neither Cisco nor McGraw Hill warrants that use of this publication and accompanying media will ensure passing any exam.

McGraw Hill books are available at special quantity discounts to use as premiums and sales promotions, or for use in corporate training programs. To contact a representative, please visit the Contact Us pages at www.mhprofessional.com.

CCT®/CCNA® Routing and Switching All-in-One Exam Guide (Exams 100-490 & 200-301)

Copyright © 2021 by McGraw Hill. All rights reserved. Printed in the United States of America. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

Cisco®, Cisco Systems®, CCAR®, CCDA®, CCDE®, CCDP®, CCIE®, CCNA®, CCNP®, CCENT®, CCSI®, CCT®, the Cisco Systems logo and the CCIE logo are trademarks or registered trademarks of Cisco Systems, Inc. in the United States and certain other countries. All other trademarks are trademarks of their respective owners.

All trademarks or copyrights mentioned herein are the possession of their respective owners and McGraw Hill makes no claim of ownership by the mention of products that contain these marks.

1 2 3 4 5 6 7 8 9 LCR 24 23 22 21 20

Library of Congress Control Number: 2020947329

ISBN 978-1-260-46977-6

MHID 1-260-46977-8

Sponsoring Editor

Tim Green

Editorial Supervisor

Patty Mon

Project Manager

Revathi Viswanathan,
KnowledgeWorks Global Ltd.

Acquisitions Coordinator

Emily Walters

Technical Editor

Ed Tetz

Copy Editor

Lisa Theobald

Proofreader

Paul Tyler

Indexer

Ted Laux

Production Supervisor

Thomas Somers

Composition

KnowledgeWorks Global Ltd.

Illustration

KnowledgeWorks Global Ltd.

Art Director, Cover

Jeff Weeks

Information has been obtained by McGraw Hill from sources believed to be reliable. However, because of the possibility of human or mechanical error by our sources, McGraw Hill, or others, McGraw Hill does not guarantee the accuracy, adequacy, or completeness of any information and is not responsible for any errors or omissions or the results obtained from the use of such information.

Wireless Networking

In this chapter, you will

- Learn about wireless network concepts such as radio frequency, SSIDs, and channels
- Learn about wireless standards and protocols
- Understand wireless architectures, positioning of WLC, and AP modes
- Understand management access connections

Networks are no longer limited to using cabled, or wired, devices. Today's networks use a mix of wired systems along with wireless systems that use radio frequencies (RFs) to transmit data to a *wireless access point* (WAP). The WAP may have a connection to the wired network, which enables the wireless devices to communicate with the entire network.

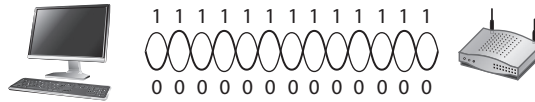
This chapter introduces you to the world of wireless networks! It's important that you understand the various aspects of wireless networks for your CCNA certification exam, so be sure to study this chapter well. This chapter introduces you to wireless basics, will discuss some security concerns around wireless, and will then show you how to set up a wireless network.

Introducing Wireless

In a wireless network, radio frequencies (RFs) transmit data from one device to another through the air. Wireless networks are especially useful in offices, where they enable workers to use laptops anywhere throughout the location to connect to the network instead of using only desktop computers hardwired to the network. Most laptops have wireless network cards installed to enable wireless.

As you know, computers work with data in the form of 1s and 0s. With wireless, the transceiver in the wireless network device is responsible for encoding that data into RF waves. If you could look at an RF wave, you'd see that the low frequency parts of the wave are 0s, while the high frequency parts of the wave are 1s (see Figure 15-1).

Figure 15-1
Radio waves
represent data
(1s and 0s) being
delivered.



When a system sends data on a wireless network, the transceiver built into the computer's wireless network card encodes the data (1s and 0s) into radio waves. The transceiver then passes the data to the wireless antenna on the device to send the radio waves through the air to the receiving device, where its antenna picks up the radio waves and passes them to the transceiver. Then the transceiver converts the radio waves to data (1s and 0s) for the receiving device to read.

Wireless Concepts

A number of network components are used to create a wireless network. In this section we look at the common components you need to be familiar with.

Wireless Access Point

The WAP device, commonly referred to as just *access point*, adds wireless capabilities to your network. It is responsible for sending and receiving radio waves to enable wireless devices to communicate with other devices on the local area network (LAN). A wireless device (such as a laptop) sends data to a device on the LAN (such as a printer), by first sending the data wirelessly to the wireless access point, which then passes the data on to the device that is connected to the wired network (the printer). Figure 15-2 displays a typical setup of a network that uses a WAP.

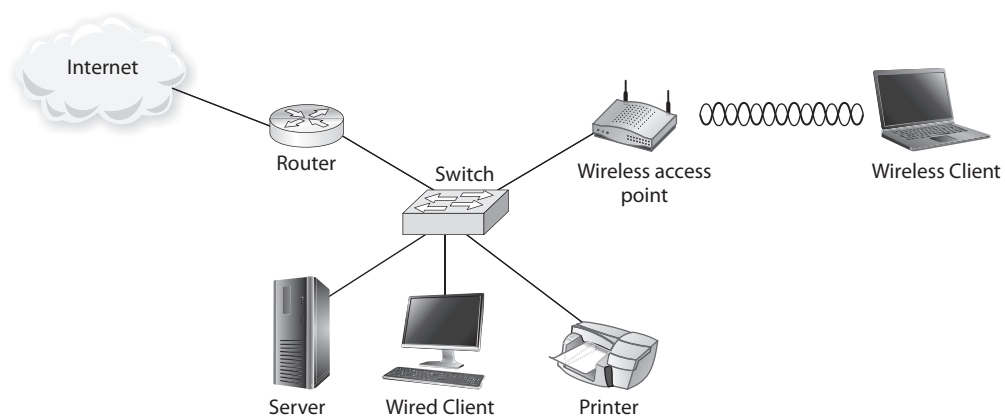


Figure 15-2 A WAP enables wireless devices to talk to the LAN.

Wireless Clients

A wireless client is any device that has a wireless network card installed and that communicates with an RF signal. Examples of wireless clients are laptops, smart phones, tablets, and any other device that has a wireless network card installed. The wireless client, also known as a wireless station, typically connects to the network via the WAP.

To connect your wireless clients to a wireless network, you need a WAP, which has antennas that send and receive the wireless signal between the wireless client and access point, but the access point also has a connection to the wired network so that wireless clients can access resources on the wired network. Most home users have a wireless router, which performs the function of an access point, but also includes other features such as Network Address Translation (NAT), a network firewall, and Dynamic Host Configuration Protocol (DHCP) services. Although most IT folks interchange the terms of wireless access point and wireless router, they are technically different devices. The wireless access point is focused on providing connectivity to wireless clients, while a wireless router does that, but also provides the additional services just mentioned.

Wireless LAN Controller

Enterprise networks that have a number of access points (APs) can have multiple APs configured from a central point by using a wireless LAN controller (WLC). The WLC can also provide centralized authentication for all your network's APs if you configure the WLC to use a central Remote Authentication Dial-In User Service (RADIUS) server.

The WLC connects to the network in the same way the AP does—they both connect to a network switch, which is a wired device on the network (that is, it's not connected wirelessly). Once all of the APs and the WLC are connected to the network, the WLC can be used to deploy configuration settings to the APs or to perform other administrative tasks such as software upgrades.

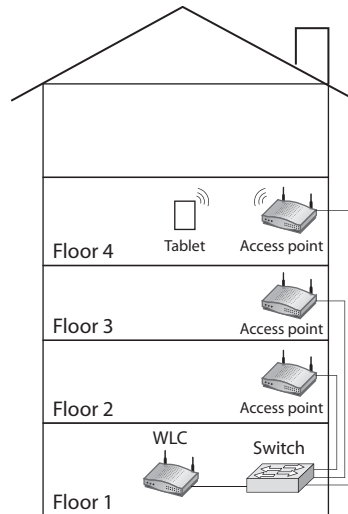
Figure 15-3 shows an example of how the WLC and the APs may be positioned on a network. Notice the APs on floors 2, 3, and 4 that provide wireless access to the devices on those floors. Also notice that each AP has a wired Ethernet connection to a switch; this switch is known as the *distribution system* (DS). The DS could be a dedicated switch for WAPs to connect to, or it could be a switch for your wired network that all other wired devices connect to. Note that the Cisco 9300 switch can have the WLC controller software installed on it, so that if you were using a 9300 switch in a branch office, you could then deploy a branch WLC without using any additional hardware.

Each of the APs will have its own management IP address, and you can remotely connect to that AP and change the configuration settings. Or you can add a WLC to the network that is used to centrally manage the configuration of all the APs. Notice in Figure 15-3 that the WLC is located on floor 1 and is connected to the switch, or distribution system, as well.

The port on the WLC that connects to the switch (the distribution system) is the *distribution port*. Because the WLC sends a lot of data through that port, including traffic destined for the APs in the CAPWAP (Control and Provisioning of Wireless Access Points) tunnel and traffic from the wireless clients, it is common for a WLC to have multiple distribution ports that connect the WLC to the distribution system (the switch).

Figure 15-3

Access points and a wireless LAN controller connect to the switch.



These distribution ports always operate as trunk ports (instead of access ports) because they need to carry traffic for all of the virtual LANs (VLANs). It is also common to combine the distribution ports together in a *link aggregation group* (LAG), which combines the bandwidth of all ports in the group. The LAG also provides load balancing on the ports so that no one port is over-utilized and fault tolerance on the link can handle the workload if one port fails the other ports in the group.

Putting It All Together

Let's take a look at a typical setup for a wireless network using an AP to provide network access to clients on the network that are part of different VLANs. In Figure 15-4, you can see a Cisco switch that contains two VLANs: VLAN 10 for the accounting department and VLAN 20 for the marketing department.

To give each department wireless access, we connect an access point to the switch, but notice in the figure that the access point is connected to a port that is outside the two VLANs. This is because we need the AP to deliver traffic for both VLANs. So we connect the AP to the switch, and then configure the port that the AP is connected to as a trunk port, so that it can carry traffic for VLAN 10 and VLAN 20.

To configure the AP, you connect to the AP, either through the CLI or the web GUI and configure two *Service Set Identifiers* (SSIDs). The SSID is the name of the wireless network that the clients will choose when they see a list of available networks; this is the wireless network that the clients will connect to. Each AP can provide multiple wireless networks or multiple SSIDs. In our example, we configure an SSID for accounting (ACCT_WLAN) and an SSID for marketing (MKT_WLAN) and then assign each SSID to the appropriate VLAN.

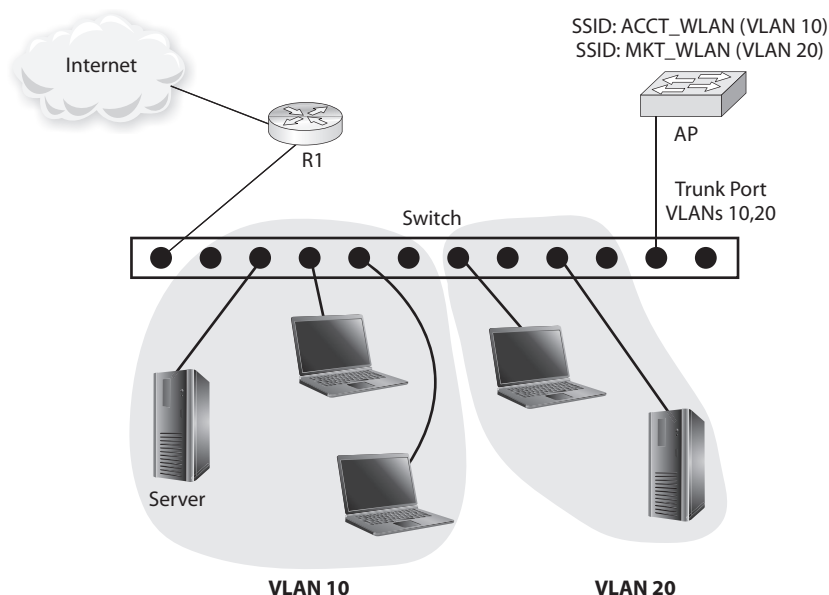


Figure 15-4 A single AP providing multiple wireless networks

Antenna Types

The typical wireless network environment involves using a WAP with connected antennas that transmit the radio signal through the air. The new CCNA exam expects you to understand these types of wireless antennas that are used by wireless technologies:

- **Omnidirectional** Sends the radio signals in all directions to cover a broad range or area.
- **Semi-directional** Sends radio signals in a single direction, but the signal has a wide range of coverage in that direction. You can compare this to a streetlight that shines downward but covers a wide area below. An example of a semi-directional antenna is a hallway wireless antenna in a facility.
- **Highly directional** Also known as *unidirectional*, this antenna sends radio signals in a single direction covering a very small area. Back to the light analogy—you can compare this to the way that a spotlight covers a small area when the light shines. A highly directional antenna could be used in a long hallway in a hospital or warehouse and would cover the long, narrow, confined space.

In addition, a few common practices can help cover the area needed by the wireless network and control connections to your wireless network. Several methods can help with area coverage and security with your wireless network by manipulating characteristics of the antenna.

For better performance and area coverage, try maintaining line of sight between antennas. Although this is not required, remember that the more objects the signal has to pass through, the weaker the signal will get. Also ensure that the antennas on the WAP are a reasonable distance from the wireless clients. If a client is too far away, it may not be able to connect. From a security point of view, you want to limit who is connecting to your wireless network by placing the WAP (and its antennas) in the center of the building. And remember that if you place the AP close to an outer wall of the building, it is possible that someone outside the building could connect to your wireless network.

You can also change the power levels on the AP to control how strong the signal is. If clients cannot connect to the AP because they are too far away, you may solve the problem by increasing the AP power level, which strengthens the signal so it can travel farther. From a security point of view, be aware that it's better to *lower* the power levels so that the range of the signal does not go beyond the building walls.

Wireless Network Types

You can create two major modes of wireless networks: ad hoc mode or infrastructure mode. Each of these is known as a wireless mode, and each has its advantages.

With *ad hoc mode*, the wireless device, such as a laptop, is connected to other wireless devices in a peer-to-peer environment without the need for a WAP. With *infrastructure mode*, the wireless clients are connected to a central device, which is a WAP. The wireless client sends data to the AP, which then sends the data on to the destination (as shown in Figure 15-5). As mentioned, the wireless client can access network

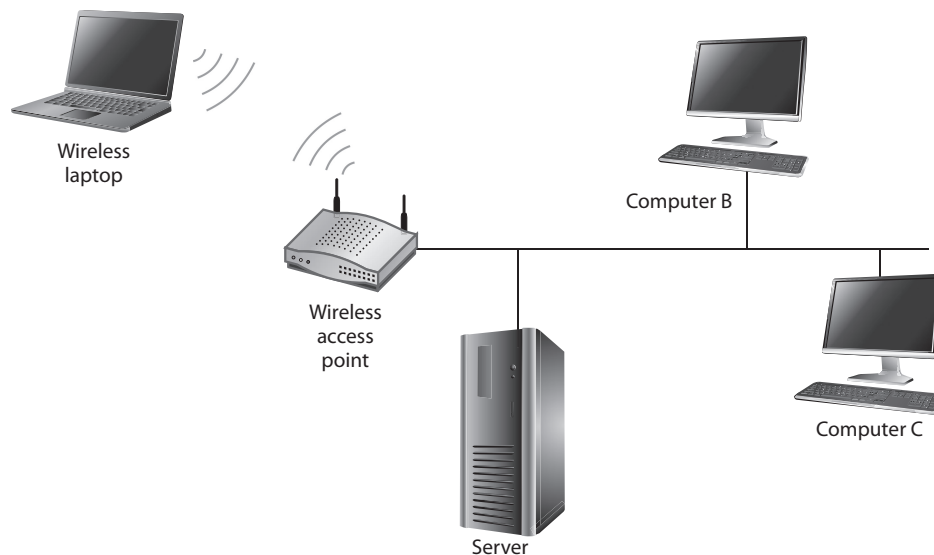


Figure 15-5 A typical wireless network running in infrastructure mode

resources on the wired network once connected to the AP because the AP is connected to the wired network.

The advantage of ad hoc mode is that you don't need to purchase the AP; the benefit of infrastructure mode is that when you use the WAP, you get to control who can connect to the wireless network, and many devices can connect to the AP at one time to share information.

Wireless Terminology

You need to be familiar with a number of other wireless terms and concepts for the Cisco CCNA exam. Some of these terms have already been mentioned in the chapter:

Basic Service Set (BSS) This refers to a wireless network that has a single AP. All wireless clients connect to the single AP to gain access to the network.

Basic Service Set Identifier (BSSID) This is the MAC address of the WAP. When you use wireless security tools to assess the security of a wireless network, you will notice that the tools identify the AP MAC with the label "BSSID." When you use many of the command line security tools, you usually specify the AP you are testing with the `--bssid` switch.

Service Set Identifier (SSID) This is the name of the wireless network. When configuring the AP, you will need to configure the name of the wireless network by setting the SSID setting.

Distribution System (DS) This is the network switch that connects the AP to the LAN.

Extended Service Set (ESS) In larger organizations with office environments that span large areas, such as multiple floors or multiple buildings, you'll probably not be able to have a single AP service (aka BSS) for all the wireless clients because they are physically spread out. In this case you need to set up an ESS, which comprises a number of access points, configured with the same SSID, that are positioned at different points throughout the building to service wireless clients within that area.

Creating an ESS requires the following:

- Each AP must be configured with the same SSID.
- Each AP must be configured with a different, non-overlapping, channel.
- The AP must cover areas that overlap by 10 percent, so that roaming wireless clients do not lose a connection.

Figure 15-6 compares a BSS with an ESS.



EXAM TIP Be sure to know the wireless terms discussed in this section for the CCNA exam.

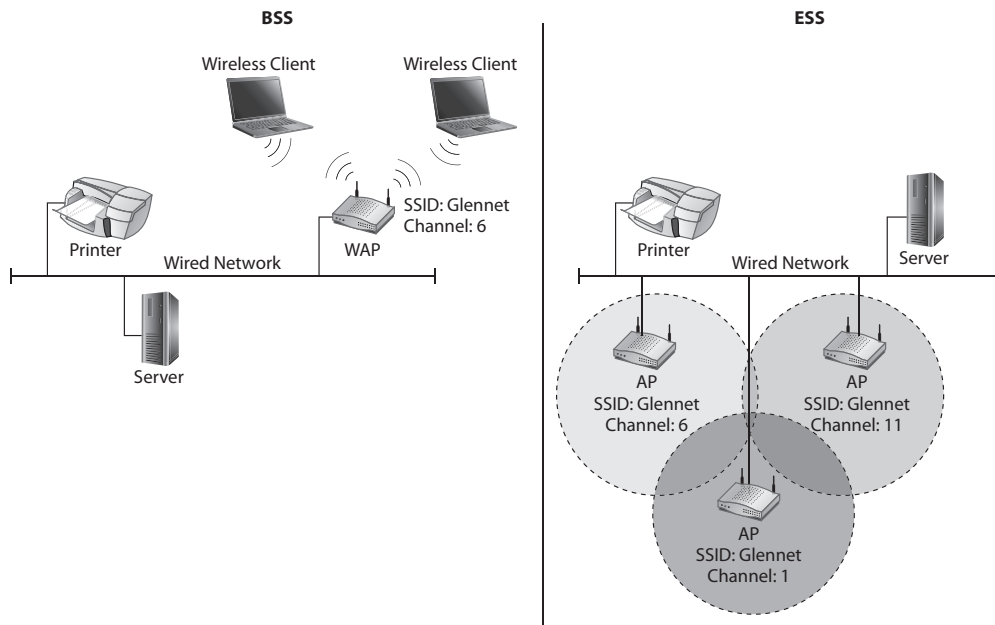


Figure 15-6 BSS versus ESS

Wireless Standards

The Institute of Electrical and Electronics Engineers (IEEE) committee has developed wireless standards in the 802 project models for wireless networking. Wireless and several standards are defined by the 802.11 project model.

802.11a

The 802.11a wireless standard is an older standard that runs at the 5 GHz frequency. 802.11a devices can transmit data at 54 Mbps and are incompatible with 802.11b and 802.11g devices.



EXAM TIP For the exam, remember that 802.11a was an early wireless standard that ran at a different frequency than 802.11b and 802.11g. This makes it incompatible with 802.11b/g. Remember that 802.11a defines wireless environments running at 54 Mbps while using a frequency of 5 GHz.

802.11b

The 802.11b wireless standard has a transfer rate of 11 Mbps while using a frequency of 2.4 GHz. These devices are compatible with 802.11g/n devices because they run at the same frequency and follow the Wi-Fi standard.



EXAM TIP Note that 802.11b runs at 11 Mbps, and 802.11g runs at 54 Mbps. The 802.11n standard is designed to reach up to 600 Mbps!

802.11g

The 802.11g wireless standard is a newer standard that was designed to be compatible with 802.11b, but it also increases the transfer rate. The transfer rate of 802.11g devices is 54 Mbps using a frequency of 2.4 GHz.

All 802.11g devices are compatible with 802.11b/n devices because they all follow the Wi-Fi standard and run at the same frequency of 2.4 GHz.

802.11n

The 802.11n wireless standard is a wireless standard that came out in late 2009. The goal of 802.11n is to increase the transfer rate beyond what current standards such as 802.11g support. 802.11n supports transfer rates up to 600 Mbps.

To help accomplish this, 802.11n introduced two new features: multiple input, multiple output (MIMO) and channel bonding. MIMO uses multiple antennas to achieve more throughput than can be accomplished with only a single antenna. Channel bonding enables 802.11n to transmit data over two non-overlapping channels to achieve more throughput. 802.11n is designed to be backward compatible with 802.11a, 802.11b, and 802.11g and can run at the 2.4 GHz or 5 GHz frequency.



EXAM TIP Wireless networks today are called *Wi-Fi*, which stands for *wireless fidelity*. 802.11b, 802.11g, and 802.11n are all part of the Wi-Fi standard and, as a result, are compatible with one another.

802.11ac

The 802.11ac wireless standard was approved in 2014 and is considered a high-throughput wireless standard that runs on the 5 GHz frequency range. The 802.11ac standard offers throughput of potentially 1 Gbps by increasing the channel width and offering similar features to the 802.11n standard, such as MIMO and multi-user MIMO (MU-MIMO), which involves enabling multiple transmitters to send separate signals and multiple receivers to receive separate signals at the same time.

Most 802.11ac wireless routers have a universal serial bus (USB) 3.0 port, where you can connect an external hard drive to the wireless router and stream high-definition video to clients.

It is important to note that 802.11a was an early implementation of wireless networking and is not compatible with early Wi-Fi networks such as 802.11b and 802.11g. As an example of the compatibility, my home wireless network has an AP that is an 802.11g device, but one of my old laptops has an 802.11b wireless network card. My old laptop can communicate on the network because the two standards are 100 percent compatible with one another. In this example, the laptop with the 802.11b card connects only at 11 Mbps, while my new laptop with the 802.11g card connects at 54 Mbps.

	802.11	802.11	802.11	802.11n	802.11ac
Frequency	5 GHz	2.4 GHz	2.4 GHz	5/2.4 GHz	5 GHz
Transfer Rate	54 Mbps	11 Mbps	54 Mbps	Up to 600 Mbps	1 Gbps
Range	150 feet	300 feet	300 feet	300 feet	300 feet, but more throughput
Compatibility	802.11	802.11g/n	802.11b/n	802.11a/b/g	802.11a/b/g/n

Table 15-1 Comparing the Different Wireless Standards

Key Points About Wireless Standards to Remember

Table 15-1 summarizes key points you need to be familiar with about the different wireless standards for the CCNA certification exam.



EXAM TIP Remember that wireless transmission speeds decrease as your distance from the WAP increases.

Channels

You’ve read that 802.11b/g/n/ac all run at the 2.4 GHz frequency, but you should also understand that 2.4 GHz is a frequency range. Each frequency in the range is known as a *channel*. This discussion focuses on the 2.4 GHz frequency, which also uses channels, but we’ll focus on the 2.4 GHz frequency first, because there are channels that overlap with one another. Using channels that overlap with one another could cause interference and instability with the wireless network.

Most wireless devices enable you to specify which channel you want to use. This is important because if you are having trouble with your wireless network failing a lot, it could be that the wireless devices are conflicting or interfering with other wireless devices in your area. A good example of this is cordless phones; they may run at the 2.4 GHz range and could cause issues with your wireless network. As a solution, you could change the channel on your WAP and clients, which changes the frequency—hopefully preventing any conflicts with other household items. Note that modern cordless phones follow the DECT 6 standard, which moves the communication to the 1.9 GHz band, solving the problem of interference from cordless phones.

Table 15-2 lists the different frequencies used by the different channels.

When looking at a diagram of overlapping channels in the 2.4 GHz frequency, you can see that you can use three main channels that do not overlap—channels 1, 6, and 11.

Looking at Figure 15-7, you can see that channels 1, 6 and 11 do not overlap with one another. So if you were to create multiple wireless networks within the 2.4 GHz frequency, you could start by placing one network on channel 1 and another on channel 6 or 11. Keep in mind that there are other wireless networks around you, so if you are getting interference on your wireless network, it could be because the other wireless

Table 15-2
Different Wi-Fi
Channels and
Their Operating
Frequency
Ranges

Channel	Frequency Range
1	2.3995 GHz–2.4245 GHz
2	2.4045 GHz–2.4295 GHz
3	2.4095 GHz–2.4345 GHz
4	2.4145 GHz–2.4395 GHz
5	2.4195 GHz–2.4445 GHz
6	2.4245 GHz–2.4495 GHz
7	2.4295 GHz–2.4545 GHz
8	2.4345 GHz–2.4595 GHz
9	2.4395 GHz–2.4645 GHz
10	2.4445 GHz–2.4695 GHz
11	2.4495 GHz–2.4745 GHz
12	2.4545 GHz–2.4795 GHz
13	2.4595 GHz–2.4845 GHz

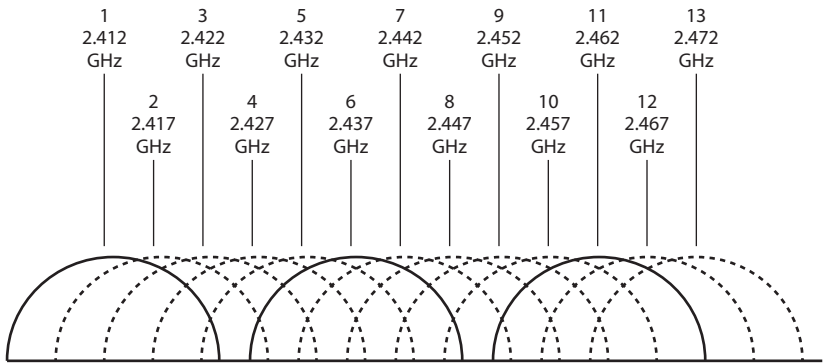
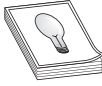


Figure 15-7 Channels 1, 6, and 11 do not overlap.

networks close to you are using the same channel. Experiment with changing the channel on your wireless network to increase the stability of the network.

Use Non-overlapping Channels

Remember when troubleshooting wireless networks that you could be getting interference from other wireless devices and household devices such as cordless phones or Bluetooth devices running on the same channel. To resolve this, experiment by changing the channel your wireless network uses to reduce the amount of interference received. As noted in Table 15-2, adjacent channels have overlapping frequencies and will interfere with one another, so changing from channel 2 to channel 1 will not solve interference problems, but changing from channel 2 to channel 6 might.



TIP To avoid interference on your wireless network from other household items, try to purchase items such as cordless phones that run on a different frequency than 2.4 GHz. If you are experiencing problems on the wireless network, you could try changing the channel on the wireless equipment and see if a different channel is more reliable. Also note that other non-wireless devices such as microwaves can cause interference by generating noise signals in the 2.4 GHz frequency range.

A channel has a specific “width” to it, and that width allows for a specific amount of data to pass through the channel (called *bandwidth*). The point to make here is that a wireless standard that has a larger channel bandwidth will be able to deliver more data and give better performance. For example, 802.11g has a channel bandwidth of 20 MHz, while 802.11n can have a channel bandwidth of 40 MHz (when running on 5 GHz frequency). Increasing the channel bandwidth is the way newer wireless standards are providing better transfer rates. The following lists the channel bandwidth per standard:

- 802.11a: 20 MHz
- 802.11b: 22 MHz
- 802.11g: 20 MHz
- 802.11n: 20 or 40 MHz
- 802.11ac: 20, 40, 80, or 160 MHz

Wireless Security Protocols

A number of wireless authentication and encryption protocols have been developed over the years to help secure your wireless network. You should consider them for implementation on your wireless network.

Wired Equivalent Privacy

Wired Equivalent Privacy (WEP) was designed to give the wireless world a level of security that could equate to that of the wired networking world. In the wired world, someone would have to be in your office to connect a cable to your network, but with wireless networking, this is, of course, not the case. Someone could sit outside your building in a parked car and connect to your wireless network.

To configure your wireless network with WEP, you simply specify a shared key, or passphrase, on the WAP. The theory is that if anyone wants to connect to your wireless network, they’d need to know the shared key and would need to configure their workstation with that key. When you configure the shared key on the AP and client, any data sent between the client and the AP is encrypted with WEP. This will prevent unauthorized individuals from capturing data in transit and reading it.

Note that there were huge flaws in how WEP implemented its encryption and key usage, and as a result, both 64-bit and 128-bit WEP are easily cracked. For security reasons, you should not use WEP unless you have older APs that do not support WPA or WPA2.

Wi-Fi Protected Access

Wi-Fi Protected Access (WPA) was designed to improve upon wireless security and fix some of the flaws in WEP. WPA uses a 128-bit key and the Temporal Key Integrity Protocol (TKIP), which is used to change the encryption keys for every packet that is sent. This will make it far more difficult for hackers to crack the key, which is very easy to do with WEP. WPA uses RC4 as the symmetric encryption algorithm, which is why WPA is sometimes referred to as TKIP-RC4, as in the CCNA objectives.

WPA has a number of other improvements over WEP; for example, it has improved integrity checking, and it supports authentication using the Extensible Authentication Protocol (EAP), a very secure authentication protocol that supports a number of authentication methods such as Kerberos, token cards, certificates, and smartcards.

EAP messages are encapsulated inside IEEE 802.1X packets for network access authentication with wired or wireless networks. When IEEE 802.1X is used to control access to the wireless network, the wireless client attempts to connect to a WAP; the AP asks the client for proof of identity and then forwards that to a RADIUS server for authentication.

Many variations of EAP have developed over time:

- **LEAP** Lightweight Extensible Authentication Protocol is Cisco's proprietary EAP solution created before the IEEE created 802.1X.
- **PEAP** Protected Extensible Authentication Protocol is used to encapsulate EAP messages over a secure tunnel that uses Transport Layer Security (TLS). Because EAP assumes the packets are sent over a secure network, with PEAP, TLS is used to create a secure tunnel between two points.
- **EAP-FAST** EAP-FAST is an authentication protocol designed by Cisco to replace LEAP. EAP-FAST is typically used to provide authentication services to wireless networks.
- **EAP-TLS** EAP-TLS is the EAP protocol that uses TLS security for secure authentication on wireless networks. The EAP-TLS solution typically involves the use of client certificates to perform the authentication.
- **EAP-TTLS** EAP-TTLS (EAP-Tunneled Transport Layer Security) builds on EAP-TLS by having the capabilities to authenticate both the client and the server, although the client does not need to use certificates for authentication. The server can authenticate the client after a secure channel is set up using the server's certificate.

When configuring WPA on the wireless network, note that WPA operates in three different modes—WPA Personal, WPA Enterprise, and Open:

- **WPA Personal** With WPA Personal, aka WPA-PSK (WPA preshared key), you can configure the AP with a starting key value, known as the preshared key, which is then used to encrypt the traffic. This mode is used most by home users and small businesses.

- **WPA Enterprise** WPA Enterprise, aka WPA-802.1X, is a WPA implementation that uses a central authentication server such as a RADIUS server for authentication and auditing features. WPA Enterprise is used by larger organizations so that they can use their existing authentication server to control who has access to the wireless network and to log network access.
- **Open** An open wireless network does not require any password to connect and does not use any form of encryption to keep the wireless data secret from prying eyes. Naturally, it is not recommend to leave your wireless network open (you should implement WPA2) or to connect your client system to an open network that you are not familiar with.



EXAM TIP The CCNA certification exam will test your knowledge of the different security protocols such as WPA, WPA2, WPA3, and open networks. Always be sure to implement the most secure method supported by your devices; this is usually WPA2.

WPA2

WPA2 improves upon the security of WPA and should be used instead of WPA if you have the choice. WPA2 uses Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP or CCM Mode Protocol) for data privacy, integrity, and authentication on a WPA2 wireless network. WPA2 uses CCMP with the Advanced Encryption Standard (AES) protocol (which is sometimes referred to as CCMP-AES) for the encryption of wireless traffic instead of TKIP and supports additional features, such as added protection for ad hoc networks and key caching. Because WPA2 uses AES as its encryption protocol, it supports 128-bit, 192-bit, and 256-bit encryption.

WPA2 also supports the TLS and the TTLS protocols through the use of the EAP. Known as EAP-TLS and EAP-TTLS, these protocols offer secure methods of performing authentication on a wireless network.

WPA3

WPA3 is the newest version of WPA, which was developed in 2018 and is slowly being adopted by manufacturers. Because WPA3 is fairly new, you may have it as an option only on newer wireless devices. WPA3 has improved security over WPA2 by introducing some new features:

- It improves the encryption by using 256-bit Galois/Counter Mode Protocol (GCMP-256) for data encryption.
- Simultaneous Authentication of Equals (SAE) is a feature of WPA3 that increases security by enabling the access point to authenticate the client, and the client to authenticate the access point. This stronger authentication method helps prevent eavesdropping and cracking of handshake traffic that was common with WPA2.
- The encryption process with WPA3 uses session keys, which are designed to protect a user from decrypting another user's traffic even if they both have used the same Wi-Fi key.



EXAM TIP Be sure to be familiar with the different wireless security protocols for the CCNA exam.

Wireless Security Practices

Authentication and Authorization

The CCNA exam expects you to be familiar with techniques used to control who gains access to a wireless network via *authentication* and *authorization*.

Shared or Open An open wireless network, also known as a shared network, does not implement any method to control who gains access to the network. It is the least secure of all the wireless network types.

Preshared Key You can control who gains access to the wireless network by configuring an encryption protocol such as WPA2 or WPA3 in personal mode, and then specify the encryption key, also known as the preshared key. This encryption key would need to be configured on any device that wants to connect to your wireless network.

MAC Filtering In addition to using a preshared key, you can configure MAC filtering, which authorizes who is allowed to access the network by their MAC address. Keep in mind that a number of tools can be used to monitor wireless traffic and view the MAC addresses of authorized clients connected to the access point. An attack could then spoof the MAC address to bypass the MAC filtering feature.

802.1X When using WPA2/WPA3 in enterprise mode, you must specify the IP address of the RADIUS or TACACS+ server in the configuration of the access point or WLC. This means that the access point/WLC will forward the client to the RADIUS server to be authenticated before being granted access to the network. The benefit of 802.1X is that you can authenticate users by more than just a preshared key—they can be authenticated using a username and password against a central authentication service.

Cisco Wireless Architectures

You can use different Cisco wireless architectures while designing your wireless network, as well as the different Cisco WAP modes. And you can connect to APs to perform remote management.

Wireless Architectures

You can set up your Cisco wireless network in different ways: each setup is known as a wireless architecture. Some wireless architectures are simple and involve only a WAP, while other architectures have WLC to help manage the wireless settings across multiple APs.

Autonomous Architecture

With the autonomous architecture model, your Cisco wireless network is made up of independent APs that you manage individually, typically with the GUI of the AP. Each AP could supply one or more SSIDs, with each SSID associated with a different VLAN.

With this model, each SSID is associated with a single VLAN, and the AP has a connection to a switch using a trunk port. The trunk port is configured to carry all traffic for each of the VLANs.

In this scenario, if you need to add a new wireless network (SSID) to all the APs, you must configure each AP individually, because they each operate independently.

Split-MAC Architecture

The split-MAC architecture offers a more centralized model in which a WLC is used to deploy the configuration to each of the APs. In this scenario, the APs are known as *lightweight access points* (LAPs) because they receive their configuration from the WLC and are not configured directly.

In this model the WLC is used to deploy configuration settings such as the radio frequency to use, quality of service (QoS) settings, any authentication, authorization, and accounting (AAA) settings that deal with configuration of a TACACS+/RADIUS server, and policy settings.

In the split-MAC architecture model, Control and Provisioning of Wireless Access Points (CAPWAP) is a secure private tunnel used to carry communication between the WLC and the LAP. All communication between the WLC and LAP travels through the CAPWAP. There are actually two tunnels: one for control communication and another for the data:

- The control channel carries the commands and is encrypted by default. The CAPWAP control channel uses UDP 5246.
- The data channel is not encrypted by default, but it can be encrypted. The CAPWAP data channel uses UDP 5247.

Cloud-based Architecture

In a cloud-based architecture, the WLC is not a device on your physical network, but is provided by a cloud provider and resides in the cloud. The cloud-based WLC provides the same functions as a WLC connected to your LAN, but you have the benefit of it being a cloud device that is managed by the cloud provider. Cloud-based architecture models include a Cisco Meraki license and a Cisco Catalyst 9800-CL, which provide WLC capabilities to a wireless network.

Positioning of WLC

You need to understand the role that the WLC plays on your network to understand where you should physically position the WLC. Types of architectures include centralized WLAN, Cisco FlexConnect mode, and converged WLAN.

Centralized WLAN Architecture

In a centralized WLAN architecture, you are using a WLC to manage your LAPs. All communication to the LAP must pass through the WLC to verify that the communication is authorized (remember that the WLC can provide AAA functionality). This means that communication between two wireless clients connected to the LAP must travel the network path to the WLC (and then back) when data goes from one wireless device to another. This could cause issues with delay or even outages if the WLC is physically distanced from the LAPs.

Placement of the WLC should be carefully considered. If you place the WLC on the opposite end of the network from the LAPs, then the CAPWAP tunnel that carries traffic between the LAP and the WLC must travel across the network, causing delays. Also, because the LAPs must be able to communicate with the WLC, if the WLC or the CAPWAP tunnel goes down in a centralized WLAN architecture, the wireless devices are dropped from the network (even if the LAP is functioning). You can solve this by either changing the mode on the AP (more on this in a bit) or by placing the WLC closer to the LAPs.

Cisco FlexConnect

The Cisco FlexConnect mode on the LAP enables the LAP to pass data to the LAN directly and is not required to pass the data through the WLC. Also, the LAPs can authenticate clients in order for the client to gain wireless access, whereas in the centralized model all authentication was done by the WLC. With the Cisco FlexConnect mode, if the CAPWAP tunnel fails, the LAPs still function because they have their configuration and are authorized to pass traffic on to the network and authenticate wireless clients. The Cisco FlexConnect mode is a popular choice when your WLC is located in the head office and you have LAPs in branch offices.

Converged WLAN Architecture

To ensure that communication between the WLC and the LAPs is efficient and reliable, the WLC and LAPs are connected to the same switch in a converged WLAN architecture. These could be access layer switches or distribution layer switches. This enables the LAPs to communicate with the WLC through the switch quickly, without needing the traffic to travel across the entire network. In the converged WLAN architecture, you would need multiple WLCs for different parts of the network. The benefit is the CAPWAP tunnel would be a shorter distance between the LAP and its WLC. This topology results in faster Wi-Fi access with less delays.

AP Modes

You just learned that you can change the AP mode to modify how it is being used and how it operates. For the CCNA exam, you need to be familiar with a number of different access point modes, listed here.

Local Mode This is the default mode for the LAPs and involves what we describe earlier: the LAP has a CAPWAP tunnel to the WLC in which all traffic must pass through the CAPWAP to the WLC. If the CAPWAP fails, all wireless clients are disconnected from that LAP.

Bridged Mode This mode is used when you want the AP to be used to connect two networks together, such as the networks of two buildings separated by a bit of distance. With this scenario, the AP acting as a bridge is authenticated to the remote wireless network, but the devices in the remote building are not.

FlexConnect Mode In this mode, the LAPs are in branch offices and the WLC is located in the head office. The LAPs can pass traffic directly between clients and to the LAN, while normally the traffic would need to be sent to the WLC. This is an important feature, because it reduces network delay that would have been caused by sending traffic over the WAN to reach the WLC. With FlexConnect mode, the LAP can be used to authenticate and authorize wireless clients as well. Remember that in FlexConnect mode, the LAPs still function even if the CAPWAP tunnel fails.

Mesh Mode This mode represents another special scenario mode in which a WAP connects to another WAP, essentially acting as an extender to the wireless network. When a wireless client connects and sends data to the LAN, it is possible that the data will travel through multiple mesh nodes before reaching the LAN. A mesh node (an AP in a mesh topology), also known as a mesh access point (MAP), uses the Adaptive Wireless Path Protocol (AWPP) to determine the best path to the root access point (RAP).

Monitor Mode This mode is used to monitor activity for rogue APs that are connected to the network. An AP running in monitor mode does not transmit wireless signals, but only receives wireless signals in order to detect the rogue AP.

Sniffer Mode To perform analysis of the wireless traffic, you can configure the AP in sniffer mode. Once sniffer mode is configured, the AP will capture wireless traffic and send the traffic to a remote computer for analysis.



EXAM TIP Be sure to know the AP modes for the Cisco CCNA certification exam.

Management Access Connections

When it comes to managing or configuring the WAP or the wireless LAN controller, you can use the CLI or a web interface.

Managing from the CLI

You can manage the AP or WLC through the CLI either by using the console port on the device for local administration or, if you have enabled remote management with telnet or Secure Shell (SSH), you can use those protocols. With many APs and wireless controllers, you can connect to a local console port to configure the device from the CLI. This, of

course, assumes that you have local access to the device. You can also enable telnet or SSH on the AP or wireless LAN controller to manage the device remotely from across the network. As you will learn in later chapters, you should use SSH over telnet, because SSH encrypts the communication.

Managing from a Web Interface

If you'd rather not use the CLI for configuration of the WAP or WLC, you can use the web interface by connecting to the management IP address of the device. Use HTTP (non-secure) or HTTPS (secure) to configure the AP or WLC, including configuring telnet or SSH, configuring RADIUS for central authentication, or creating wireless networks, to name just a few configuration settings.

TACACS+/RADIUS

You can configure your AP or WLC to use an authentication service such as TACACS+ or RADIUS. You will learn more about authentication services in the next few chapters, but for now, know that you can have the AP or WLC require someone that is connecting to be authenticated by an external authentication system (the TACACS+ or RADIUS server).

Configuring Wireless with a GUI

The new Cisco CCNA exam expects you to know the steps to create and configure a wireless LAN and settings such as security settings and QoS settings. In this section you will learn the steps to configure wireless networks on a WLC.

I should note that many WLCs have a *service port*, which is an out-of-band management port you can use to connect to the WLC and configure the device. There is also a management interface with an IP address assigned that you can also use to remotely manage the WLC device. The service port is a good backup method to manage the device should you not be able to connect to the management interface.

WLAN Creation

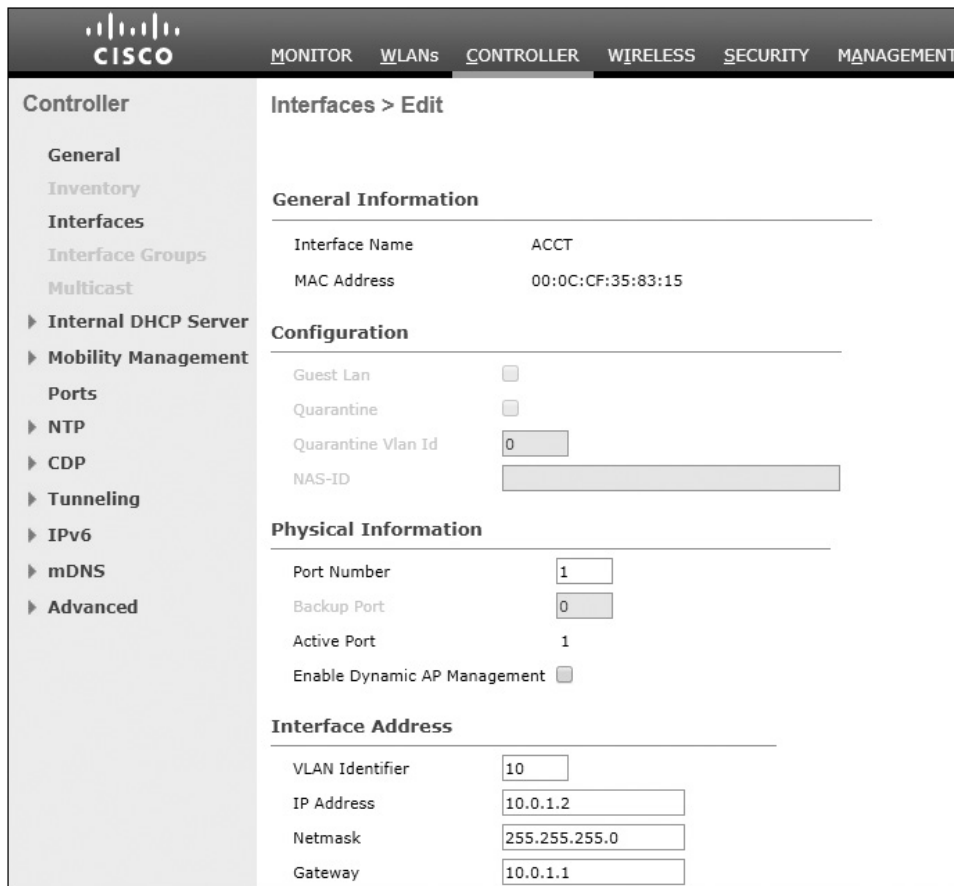
The first step to configuring a WLAN controller is to create the WLAN. You will need to connect the WLAN to the dynamic interface on the WLC that enables the WLAN to bind to the VLAN on the wired network.

Create a Dynamic Interface

Our first task is to create a dynamic interface, which is used to link the WLAN to a VLAN on the switch. Here are the steps:

1. Log into the WLC using the web interface.
2. Choose Controller at the top of the page.
3. Choose Interfaces from the left navigation pane.
4. Click the New button in the top-right corner to create a new interface.

5. Enter an interface name, such as ACCT.
6. Specify the VLAN ID you want to connect the interface to. For example, you can specify 10 (for VLAN ID 10).
7. Configure the interface for an IP address within the network range of the VLAN.



CISCO MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT

Controller

- General
- Inventory
- Interfaces**
- Interface Groups
- Multicast
- ▶ Internal DHCP Server
- ▶ Mobility Management
- Ports
- ▶ NTP
- ▶ CDP
- ▶ Tunneling
- ▶ IPv6
- ▶ mDNS
- ▶ Advanced

Interfaces > Edit

General Information

Interface Name	ACCT
MAC Address	00:0C:CF:35:83:15

Configuration

Guest Lan	<input type="checkbox"/>
Quarantine	<input type="checkbox"/>
Quarantine Vlan Id	0
NAS-ID	

Physical Information

Port Number	1
Backup Port	0
Active Port	1
Enable Dynamic AP Management	<input type="checkbox"/>

Interface Address

VLAN Identifier	10
IP Address	10.0.1.2
Netmask	255.255.255.0
Gateway	10.0.1.1

Create a WLAN

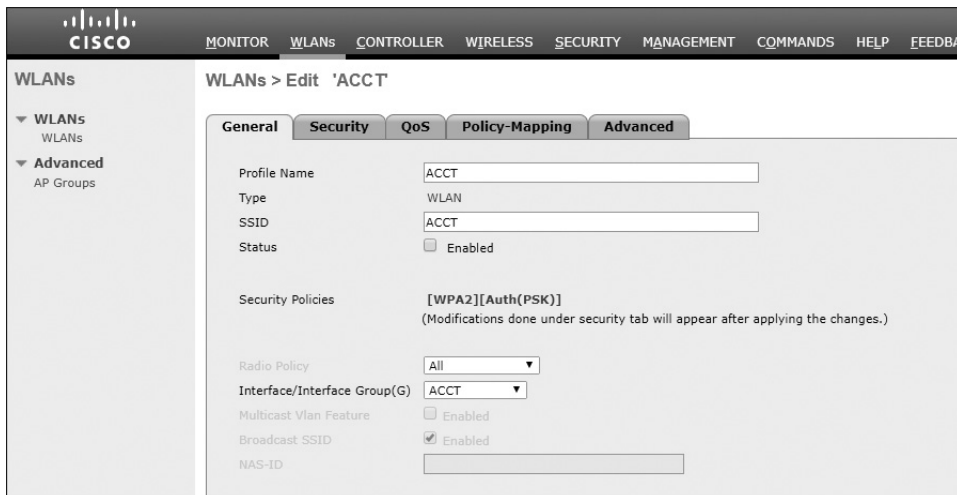
Your next task is to create the WLAN object within the WLC that will be bound to that interface. Follow these steps:

1. Click the WLANs link from the top navigation.
2. Choose Create New from the drop-down list at the upper-right and then click Go.



3. Enter the profile name for the WLAN, such as ACCT.
4. Enter the SSID for the wireless LAN, such as ACCT.
5. The WLAN is assigned a unique ID within the WLC. Click Apply.

After you click Apply, you'll see the configuration screen of the WLAN, where you can change common settings such as the SSID, the dynamic interface on the WLC the WLAN is assigned to, and whether or not you want to broadcast the SSID. Notice in the following illustration that I have assigned the ACCT wireless network to the dynamic interface, also called ACCT, that was created in the previous step.



Security Settings

You can change the security settings for the WLAN by choosing the Security tab while modifying the configuration of your WLAN.

1. Choose the Security tab at the top of the screen.
2. Choose WPA+WPA2 as the Layer 2 security protocol.

3. Choose WPA2 Policy in the WPA+WPA2 Parameters section.
4. You can then choose AES as the WPA2 Encryption type.
5. Choose PSK (preshared key) as the Authentication Key Management type.
6. Choose ASCII as the PSK Format.
7. Enter your desired preshared key (wireless password).

WLANs

- WLANs
- Advanced
 - AP Groups

WLANs > Edit 'ACCT'

General **Security** **QoS** **Policy-Mapping** **Advanced**

Layer 2 **Layer 3** **AAA Servers**

Layer 2 Security
 MAC Filtering ☐

Fast Transition
 Fast Transition ☐

Protected Management Frame
 PMF

WPA+WPA2 Parameters

WPA Policy ☐
 WPA2 Policy ☒
 WPA2 Encryption ☒ AES ☐ TKIP

Authentication Key Management

802.1X ☐ Enable
 CCKM ☐ Enable
 PSK ☒ Enable
 FT 802.1X ☐ Enable
 FT PSK ☐ Enable
 PSK Format

QoS Profiles

After configuring the wireless security settings, you can choose to configure the QoS settings for the wireless network. Choosing the QoS profile will specify how the WLC should handle and prioritize traffic from this wireless network. You can select one of the following QoS profiles:

- Platinum (used to ensure high quality of service for voice traffic)
- Gold (used to ensure high quality of service for video traffic)

- Silver (used for regular traffic—the default and considered a best effort profile)
- Bronze (used for background traffic as it is given the lowest bandwidth)

Choose the profile that best suits your needs. Remember for the certification exam that VoIP traffic should be using the Platinum QoS profile.

Advanced Wireless LAN Settings

After choosing the QoS profile, click the Advanced tab to set the advanced settings for the wireless network. Here you can specify settings such as the session timeout value, which is how frequent clients must reauthenticate to WLAN; configure features such as peer-to-peer (P2P) blocking, URL filtering to control URLs that are accessed by the clients, and the maximum number of clients that can connect.

1. Select the desired advanced settings.
2. Click Apply to complete the configuration.

Configuring RADIUS/TACACS+

If you would like to configure the wireless network to use a RADIUS server or TACACS+ server as an authentication service for clients who connect to your wireless network, you have a few steps to the configuration. First, you must add the RADIUS/TACACS+ server to the configuration, and then you can select the server when configuring your wireless LANs.

To add the RADIUS/TACACS+ server to the controller:

1. From the top navigation bar, choose the Security link.
2. Click the New button to add a new RADIUS server.
3. Type the IP address of the RADIUS server and fill in the Shared Secret/Confirm Shared Secret. The shared secret is the password needed to connect to the RADIUS server.

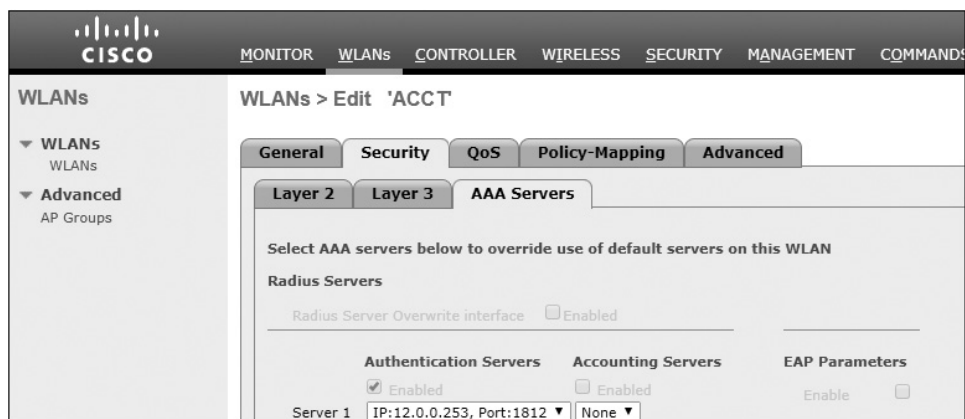
The screenshot shows the Cisco Wireless LAN Controller configuration interface. The top navigation bar includes links for MONITOR, WLANs, CONTROLLER, WIRELESS, SECURITY, MANAGEMENT, COMMANDS, HELP, and FEEDBACK. The left sidebar shows the Security menu expanded, with options for AAA, RADIUS, TACACS+, and various authentication methods. The main content area is titled 'RADIUS Authentication Servers > New' and contains the following fields:

- Server Index (Priority): 1
- Server IP Address(Ipv4/Ipv6): 12.0.0.253
- Shared Secret Format: ASCII
- Shared Secret: [Redacted]
- Confirm Shared Secret: [Redacted]
- Key Wrap: ☐ (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
- Port Number: 1812
- Server Status: Enabled

4. Choose Apply.

Now that you have added the RADIUS server, you can go back to your WLAN and configure the WLAN to use that RADIUS server. Follow these steps to configure your WLAN to use the RADIUS server:

1. Choose the WLANs link in the top navigation bar.
2. Click the link for the WLAN you wish to edit.
3. Choose the Security tab within the WLAN settings.
4. Choose the AAA Servers tab.
5. Select the RADIUS server's IP address from the Server 1 drop-down list.



6. Choose Apply in the top-right corner.

Chapter Review

In this chapter you learned about wireless networks and their components. You learned about how radio waves are used to deliver data and the components of a wireless network, such as wireless access points (WAPs) and wireless LAN controllers (WLCs).

You read about the difference between a Basic Service Set (BSS) and Extended Service Set (ESS) and the three core requirements for configuring an ESS: multiple access points with the same SSID, different channels, and overlapping areas of coverage of at least 10 percent. You also learned about the different wireless standards such as 802.11g, 802.11n, and 802.11ac.

You then read about the different wireless security protocols and how WPA2 or WPA3 (if possible) should be used on your wireless network to encrypt wireless communication. Finally, you learned about the Cisco wireless architectures such as an autonomous architecture, where each access point is configured individually, or a Split-MAC architecture that involves using a wireless LAN controller to configure all access points from a central point.

Quick Review

Introducing Wireless

- Wireless clients connect to the wireless access point (AP) to access the network. Wireless communication uses radio waves to transmit the data.
- In an enterprise environment, you can centrally manage multiple APs with a wireless LAN controller (WLC). The AP and WLC communicate using a private tunnel known as the CAPWAP.
- A BSS is a wireless network with a single AP, whereas an ESS is a wireless network that has multiple APs to cover a larger area. With an ESS, each AP uses the same SSID, but different channels.
- The 802.11b and 802.11g wireless standards run on the 2.4 GHz frequency. The 802.11b standard runs at 11 Mbps, while 802.11g runs at 54 Mbps. The 802.11n standard can run on the 2.4 GHz or 5 GHz frequencies, and 802.11ac runs on the 5 GHz frequency. The 802.11n standard provides a transfer rate of up to 600 Mbps and 802.11ac can provide 1 Gbps.
- The WEP security protocol uses RC4 as the encryption algorithm, WPA uses TKIP, and WPA2 uses AES. You can run the WPA/WPA2/WPA3 in enterprise mode, which means that you configure the AP to use an authentication service such as TACACS+ or RADIUS.

Cisco Wireless Architectures

- Autonomous architecture involves each AP being configured individually. Split-MAC architecture uses a WLC to configure all of the APs from a central location. With a cloud-based architecture, the WLC is located in the cloud.
- Configure the AP for FlexConnect mode to enable the LAPs to pass traffic directly between clients and to the LAN and to allow the AP to still function if the CAPWAP fails.
- The CAPWAP is a private tunnel that carries communication between the LAP and the WLC.
- There are two channels in the CAPWAP tunnel: the control channel and the data channel. The control channel transmits control information such as commands and uses UDP 5246. The data channel transmits all other information between the LAP and WLC and uses UDP 5247.