31 Days Before Your CCNA Exam (200-301)

A Day-By-Day Review Guide for the CCNA 200-301 Certification Exam

2nd Edition

ciscopress.com

Allan Johnson

FREE SAMPLE CHAPTER

31 Days Before Your CCNA Exam

A Day-by-Day Review Guide for the CCNA 200-301 Certification Exam

Second Edition

Allan Johnson

Cisco Press
Hoboken, NJ

31 Days Before Your CCNA Exam

Allan Johnson

Published by:
Cisco Press

$PrintCode

Library of Congress Control Number: 2024944817

ISBN-13: 978-0-13-821425-8

ISBN-10: 0-13-821425-5

Warning and Disclaimer

This book is designed to provide information about exam topics for the Cisco Certified Networking Associate (CCNA) certification. 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.

Please contact us with concerns about any potential bias at https://www.pearson.com/report-bias.html.

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.

Microsoft and/or its respective suppliers make no representations about the suitability of the information contained in the documents and related graphics published as part of the services for any purpose all such documents and related graphics are provided "as is" without warranty of any kind. Microsoft and/or its respective suppliers hereby disclaim all warranties and conditions with regard to this information, including all warranties and conditions of merchantability, whether express, implied or statutory, fitness for a particular purpose, title and non-infringement. In no event shall Microsoft and/or its respective suppliers be liable for any special, indirect or consequential damages or any damages whatsoever resulting from loss of use, data or profits, whether in an action of contract, negligence or other tortious action, arising out of or in connection with the use or performance of information available from the services.

The documents and related graphics contained herein could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Microsoft and/or its respective suppliers may make improvements and/or changes in the product(s) and/or the program(s) described herein at any time. Partial screen shots may be viewed in full within the software version specified.

Microsoft® Windows®, and Microsoft Office® are registered trademarks of the Microsoft Corporation in the U.S.A. and other countries. This book is not sponsored or endorsed by or affiliated with the Microsoft Corporation.

Special Sales

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

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.

Please contact us with concerns about any potential bias at https://www.pearson.com/report-bias.html.

GM K12, Early Career and Professional Learning	Soo Kang
Alliances Manager, Cisco Press	Caroline Antonio
Director, ITP Product Management	Brett Bartow
Executive Editor	James Manly
Managing Editor	Sandra Schroeder
Development Editor	Christopher Cleveland
Senior Project Editor	Mandie Frank
Copy Editor	Kitty Wilson
Editorial Assistant	Cindy Teeters
Designer	Chuti Prasertsith
Composition	codeMantra
Indexer	Timothy Wright
Proofreader	Donna E. Mulder

About the Author

Allan Johnson entered the academic world in 1999 after 10 years as a business owner/operator to dedicate his efforts to his passion for teaching. He holds both an MBA and an MEd in training and development. He taught CCNA courses at the high school level for 7 years and has taught both CCNA and CCNP courses at Del Mar College in Corpus Christi, Texas. In 2003, Allan began to commit much of his time and energy to the CCNA Instructional Support Team, providing services to Networking Academy instructors worldwide and creating training materials. He now splits his time between working as a Curriculum Lead for Cisco Networking Academy and as Account Lead for Unicon (unicon.net), supporting Cisco's educational efforts.

Dedications

For my wife, Becky. Thank you for all your support during this crazy whirlwind of a year. You are the stabilizing force that keeps me grounded.

Acknowledgments

As a technical author, I relied heavily on my technical editor. During the heavy revision of this book back in 2019, Steve Stiles had my back for this work. Steve Stiles did arduous review work necessary to make sure that you get a book that is both technically accurate and unambiguous.

Wendell Odom's *CCNA 200-301 Official Cert Guide, Volume 1* and *Volume 2* were two of my main sources. These two books have the breadth and depth needed to master the CCNA exam topics.

The Cisco Networking Academy authors for the online curriculum and series of Companion Guides take the reader deeper, past the CCNA exam topics, with the ultimate goal of preparing the student not only for CCNA certification but for more advanced college-level technology courses and degrees as well. Thank you especially to Rick Graziani, Bob Vachon, John Pickard, Dave Holzinger, Jane Gibbons, Martin Benson, Suk-Yi Pennock, Allan Reid, Jane Brooke, Anna Bolen, Telethia Willis, and the rest of the ACE team. Their excellent treatment of the material is reflected throughout this book.

James Manly, executive editor, daily juggles multiple projects simultaneously, steering each from beginning to end. James and I have completed many projects together. Thank you again, James, for shepherding this project for me.

Thank you to development editor Christopher Cleveland and project editor Mandie Frank for their professional and thorough review of this work. I've worked with the stellar Chris and Mandie on many previous projects. Their combined efforts ensure that what I authored is ready for publication.

And to the rest of the Pearson family who contributes in countless ways to bring a book to the reader, thank you for all your hard work.

Contents at a Glance

Reader Services

Register your copy of this book at www.ciscopress.com/title/9780138214258 for convenient access to downloads, updates, and corrections as they become available. To start the registration process, go to www.ciscopress.com/register and log in or create an account. (Be sure to check the box indicating that you would like to hear from us to receive exclusive discounts on future editions of this product.) Enter the product ISBN 9780138214258 and click Submit. When the process is complete, you will find any available bonus content under Registered Products.

Contents

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

If you're reading this introduction, you've probably already spent a considerable amount of time and energy pursuing your CCNA 200-301 certification. Regardless of how you got to this point in your travels through your CCNA studies, *31 Days Before Your CCNA Exam* most likely represents the last leg of your journey on your way to the destination: to become a Cisco Certified Network Associate. However, if you are like me, you might be reading this book at the *beginning* of your studies. If so, this book provides an excellent overview of the material you must now spend a great deal of time studying and practicing. But I must warn you: Unless you are extremely well versed in networking technologies and have considerable experience configuring and troubleshooting Cisco routers and switches, this book will *not* serve you well as the sole resource for your exam preparations. Therefore, let me spend some time discussing my recommendations for study resources.

Study Resources

Cisco Press and Pearson IT Certification offer an abundance of CCNA-related books to serve as your primary source for learning how to install, configure, operate, and troubleshoot small to medium-size routed and switched networks.

Primary Resources

First on the list of important resources is Wendell Odom's *CCNA 200-301 Official Cert Guide Library*, *Volume 1* and *Volume 2*, 2nd edition (ISBN: 9780138221393). If you do not buy any other books, buy these. Wendell's method of teaching, combined with his technical expertise and down-to-earth style, is unsurpassed in our industry. As you read through his books, you sense that he is sitting right there next to you, walking you through the material. With your purchase, you get access to practice exams and study materials and other online resources that are worth the price of the book. There is no better resource on the market for a CCNA candidate.

If you are a Cisco Networking Academy student, you are blessed with access to the online version of the CCNA version 7 curriculum and the wildly popular Packet Tracer network simulator. The Cisco Network Academy curriculum has three courses. To learn more about CCNAv7 courses and to find an Academy near you, visit http://www.netacad.com.

However, if you are not an Academy student but want to benefit from the extensive authoring done for these courses, you can buy any or all of CCNAv7 Companion Guides (CGs) and Labs & Study Guides (LSGs) of the Academy's popular online curriculum. Although with this option you will not have access to the Packet Tracer files, you will have access to the tireless work of an outstanding team of Cisco Academy instructors dedicated to providing students with comprehensive and engaging CCNA preparation course material. The titles and ISBNs for the CCNAv7 CGs and LSGs follow:

- *Introduction to Networks v7 Companion Guide* (ISBN: 9780136633662)
- *Introduction to Networks v7 Labs & Study Guide* (ISBN: 9780136634454)
- *Switching, Routing, and Wireless Essentials v7 Companion Guide* (ISBN: 9780136729358)
- *Switching, Routing, and Wireless Essentials v7 Labs & Study Guide* (ISBN: 9780136634386)

- *Enterprise Networking, Security, and Automation v7 Companion Guide* (ISBN: 9780136634324)
- *Enterprise Networking, Security, and Automation v7 Labs & Study Guide* (ISBN: 9780136634690)

You can find these books at http://www.ciscopress.com by clicking the Cisco Networking Academy link.

Supplemental Resources

In addition to the book you hold in your hands, I recommend three supplemental resources to augment your final 31 days of review and preparation.

First is Scott Empson's very popular *CCNA 200-301 Portable Command Guide* (ISBN: 9780135937822). This guide is much more than just a listing of commands and what they do. Yes, it summarizes all the CCNA certification-level IOS commands, keywords, command arguments, and associated prompts. It also provides you with tips and examples of how to apply the commands to real-world scenarios. Configuration examples throughout the book provide you with a better understanding of how these commands are used in simple network designs.

Second, Jason Gooley's *CCNA 200-301 Complete Video Course*, second edition (ISBN: 9780138213596), is a comprehensive training course that brings Cisco CCNA exam topics to life through the use of real-world demonstrations, animations, live instruction, and configurations, making learning these foundational networking topics easy and fun.

Third, Wendell Odom's *IP Subnetting LiveLessons* (ISBN: 9780135497777) and *IP Subnetting Practice Questions Kit* (ISBN: 9780135647288) will help you master this crucial skill. Subnetting is not only an IPv4 address design skill, it is also a crucial skill for troubleshooting situations where IPv4 addressing has been misconfigured. You are likely to have both types of questions on the CCNA exam.

The Cisco Learning Network

Finally, if you have not done so already, you should register with The Cisco Learning Network at https://learningnetwork.cisco.com/s/. The Cisco Learning Network, sponsored by Cisco, is a free social learning network where IT professionals can engage in the common pursuit of enhancing and advancing their IT careers. Here you can find many resources to help you prepare for your CCNA exam, in addition to a community of like-minded people ready to answer your questions, help you with your struggles, and share in your triumphs.

So which resources should you buy? The answer to that question depends largely on how deep your pockets are and how much you like books. If you're like me, you must have it all! I admit it; my bookcase is a testament to my Cisco "geekness." But if you are on a budget, choose one of the primary study resources and one of the supplemental resources (such as Wendell Odom's certification library and Scott Empson's command guide). Whatever you choose, you will be in good hands. Any or all of these authors will serve you well.

Goals and Methods

The main goal of this book is to provide you with a clear and succinct review of the CCNA objectives. Each day's exam topics are grouped into a common conceptual framework and use the following format:

- A title for the day that concisely states the overall topic
- A list of one or more CCNA 200-301 exam topics to be reviewed
- A "Key Topics" section that introduces the review material and quickly orients you to the day's focus
- An extensive review section consisting of short paragraphs, lists, tables, examples, and graphics
- A "Study Resources" section that gives you a quick reference for locating more in-depth treatment of the day's topics

The book counts down starting with Day 31, continues through exam day, and provides post-test information. This book also provides a calendar and a checklist that you can tear out and use during your exam preparation.

Use the calendar to enter each actual date beside the countdown day and the exact day, time, and location of your CCNA exam. The calendar provides a visual for the time you can dedicate to each CCNA exam topic.

The checklist highlights important tasks and deadlines leading up to your exam. Use it to help map out your studies.

Who Should Read This Book?

The audience for this book is anyone finishing preparation for taking the CCNA 200-301 exam. A secondary audience is anyone needing a refresher review of CCNA exam topics—possibly before attempting to recertify or sit for another certification for which the CCNA is a prerequisite.

Getting to Know the CCNA 200-301 Exam

For the current certification announced in August 2024, Cisco made minor revisions to the CCNA 200-301 exam. This book focuses on the entire list of topics published for the exam. It is a 120-minute exam associated with the CCNA certification. This exam tests a candidate's knowledge and skills related to network fundamentals, network access, IP connectivity, IP services, security fundamentals, and automation and programmability. Use the following steps to access a tutorial at home that demonstrates the exam environment before you go to take the exam:

Step 1. Visit **https://home.pearsonvue.com/cisco** and go through the signup process or log in.

Step 2. On the right side, click the **Certification Tutorial** link.

When you get to the testing center and check in, the proctor verifies your identity, gives you some general instructions, and takes you into a quiet room containing a PC. When you're at the PC, you have a few things to do before the timer starts on your exam. For instance, you can take the tutorial to get accustomed to the PC and the testing engine. Every time I sit for an exam, I go

through the tutorial even though I know how the test engine works. It helps me settle my nerves and get focused. Anyone who has user-level skills in getting around a PC should have no problem with the testing environment.

NOTE: You can also take the exam at home. For more information, visit https://home.pearsonvue.com/cisco/online.

When you start the exam, you are asked a series of questions. The questions are presented one at a time, and you must answer each one before you can move on to the next question. The exam engine does not let you go back and change any answers. Each exam question is in one of the following formats:

- Multiple choice
- Fill in the blank
- Drag and drop
- Testlet
- Simlet
- Simulation

The multiple-choice format simply requires that you point and click a circle or checkbox next to the correct answer(s). Cisco traditionally tells you how many answers you need to choose, and the testing software prevents you from choosing too many or too few.

Fill-in-the-blank questions usually require you only to type numbers. However, if words are requested, the case does not matter unless the answer is a command that is case sensitive (such as passwords and device names when you're configuring authentication).

Drag-and-drop questions require you to click and hold, move a button or an icon to another area, and release the mouse button to place the object somewhere else—usually in a list. For some questions, to get the question correct, you might need to put a list of five things in the proper order.

A testlet contains one general scenario and several multiple-choice questions about the scenario. Testlets are ideal if you are confident in your knowledge of the scenario's content because you can leverage your strength over multiple questions.

A simlet is similar to a testlet, in that you are given a scenario with several multiple-choice questions. However, a simlet uses a network simulator to allow you access to a simulation of the Cisco IOS Software command line. You can use **show** commands to examine a network's current behavior and answer the question.

A simulation also involves a network simulator, but you are given a task to accomplish, such as implementing a network solution or troubleshooting an existing network implementation. You do this by configuring one or more routers and switches. The exam grades the question based on the configuration you changed or added. A newer form of the simulation question is the GUI-based simulation, which simulates a graphical interface such as that found on a Linksys router or the Cisco Security Device Manager.

Registering for the CCNA 200-301 Exam

If you are starting this book 31 days before you take the CCNA 200-301 exam, register for the exam right now. In my testing experience, there is no better motivator than a scheduled test date staring me in the face. I'm willing to bet the same holds true for you. Don't worry about unforeseen circumstances. You can cancel your exam registration for a full refund up to 24 hours before the scheduled exam time. So if you're ready, gather the following information and register right now!

- Legal name
- Social Security or passport number
- Company name
- Valid email address
- Method of payment

You can schedule your exam at any time by visiting www.pearsonvue.com/cisco/. I recommend that you schedule it for 31 days from now. The process and available test times vary based on the local testing center you choose.

Remember: There is no better motivation for study than an actual test date. *Sign up today*.

Topics Covered on the CCNA Exam

Table I-1 summarizes the six domains of the CCNA 200-301 exam.

Table I-1 CCNA 200-301 Exam Domains and Weightings

Domain	Percentage of Exam
1.0 Network Fundamentals	20%
2.0 Network Access	20%
3.0 IP Connectivity	25%
4.0 IP Services	10%
5.0 Security Fundamentals	15%
6.0 Automation and Programmability	10%

Although Cisco outlines general exam topics, not all topics might appear on the CCNA exam; likewise, topics that are not specifically listed might appear on the exam. The exam topics that Cisco provides and that this book covers provide a general framework for exam preparation. Be sure to check Cisco's website for the latest exam topics.

Exam Topics Cross-reference

To give you a quick reference to help find which exam topics are covered on which days, I created two cross-reference tables. You can use Table I-2 to look up an exam topic and find the day or days on which it is covered. Use Table I-3 to find out which exam topics are covered on each day.

Table I-2 Days on Which Each Exam Topic Is Covered

Exam Topic	Day(s)
1.1 Explain the role and function of network components	31, 30, 22, 19
1.2 Describe characteristics of network topology architectures	31, 18, 7, 3
1.3 Compare physical interface and cabling types	31
1.4 Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed)	31, 29, 18
1.5 Compare TCP to UDP	31
1.6 Configure and verify IPv4 addressing and subnetting	29, 28, 18
1.7 Describe private IPv4 addressing	28
1.8 Configure and verify IPv6 addressing and prefix	27, 18
1.9 Describe IPv6 address types	27
1.10 Verify IP parameters for Client OS (Windows, Mac OS, Linux)	23
1.11 Describe wireless principles	22
1.12 Explain virtualization fundamentals (server virtualization, containers, and VRFs)	3
1.13 Describe switching concepts	30
2.1 Configure and verify VLANs (normal range) spanning multiple switches	26, 16
2.2 Configure and verify interswitch connectivity	26, 16
2.3 Configure and verify Layer 2 discovery protocols (Cisco Discovery Protocol and LLDP)	5
2.4 Configure and verify (Layer 2/Layer 3) EtherChannel (LACP)	24
2.5 Interpret basic operations of Rapid PVST+ Spanning Tree Protocol	25
2.6 Describe Cisco Wireless Architectures and AP modes	22
2.7 Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG)	22
2.8 Describe network device management access (Telnet, SSH, HTTP, HTTPS, console, TACACS+/RADIUS, and cloud managed)	29
2.9 Interpret the wireless LAN GUI configuration for client connectivity, such as WLAN creation, security settings, QoS profiles, and advanced settings	21
3.1 Interpret the components of routing table	17
3.2 Determine how a router makes a forwarding decision by default	19, 17
3.3 Configure and verify IPv4 and IPv6 static routing	15
3.4 Configure and verify single area OSPFv2	14, 13, 12
3.5 Describe the purpose, functions, and concepts of first hop redundancy protocols	24
4.1 Configure and verify inside source NAT using static and pools	8
4.2 Configure and verify NTP operating in a client and server mode	4
4.3 Explain the role of DHCP and DNS within the network	23
4.4 Explain the function of SNMP in network operations	4
4.5 Describe the use of syslog features, including facilities and severity levels	4
4.6 Configure and verify DHCP client and relay	23

Exam Topic	Day(s)
4.7 Explain the forwarding per-hop behavior (PHB) for QoS such as classification, marking, queuing, congestion, policing, and shaping	6
4.8 Configure network devices for remote access using SSH	20
4.9 Describe the capabilities and functions of TFTP/FTP in the network	4
5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)	11
5.2 Describe security program elements (user awareness, training, and physical access control)	11
5.3 Configure and verify device access control using local passwords	20
5.4 Describe security password policy elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)	11
5.5 Describe IPsec remote access and site-to-site VPNs	7
5.6 Configure and verify access control lists	10, 9
5.7 Configure and verify Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)	20
5.8 Compare authentication, authorization, and accounting concepts	20
5.9 Describe wireless security protocols (WPA, WPA2, and WPA3)	22
5.10 Configure and verify WLAN within the GUI using WPA2 PSK	21
6.1 Explain how automation impacts network management	2
6.2 Compare traditional networks with controller-based networking	3
6.3 Describe controller-based, software defined architecture (overlay, underlay, and fabric)	3, 2
6.4 Explain AI (generative and predictive) and machine learning in network operations	1
6.5 Describe characteristics of REST-based APIs (authentication types, CRUD, HTTP verbs, and data encoding)	1
6.6 Recognize the capabilities of configuration management mechanisms such as Ansible and Terraform	2
6.7 Recognize components of JSON-encoded data	1

Table I-3 Exam Topics Covered on Each Day

Day	Exam Topic(s)
31	1.1 Explain the role and function of network components
	1.2 Describe characteristics of network topology architectures
	1.3 Compare physical interface and cabling types
	1.4 Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed)
	1.5 Compare TCP to UDP
30	1.1 Explain the role and function of network components
	1.13 Describe switching concepts

Day	Exam Topic(s)
29	1.4 Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed)
	1.6 Configure and verify IPv4 addressing and subnetting
	2.8 Describe network device management access (Telnet, SSH, HTTP, HTTPS, console, TACACS+/RADIUS, and cloud managed)
28	1.6 Configure and verify IPv4 addressing and subnetting
	1.7 Describe private IPv4 addressing
27	1.8 Configure and verify IPv6 addressing and prefix
	1.9 Describe IPv6 address types
26	2.1 Configure and verify VLANs (normal range) spanning multiple switches
	2.2 Configure and verify interswitch connectivity
25	2.5 Interpret basic operations of Rapid PVST+ Spanning Tree Protocol
24	2.4 Configure and verify (Layer 2/Layer 3) EtherChannel (LACP)
	3.5 Describe the purpose, functions, and concepts of first hop redundancy protocols
23	1.10 Verify IP parameters for Client OS (Windows, Mac OS, Linux)
	4.3 Explain the role of DHCP and DNS within the network
	4.6 Configure and verify DHCP client and relay
22	1.1 Explain the role and function of network components
	1.11 Describe wireless principles
	2.6 Describe Cisco Wireless Architectures and AP modes
	2.7 Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, and LAG)
	5.9 Describe wireless security protocols (WPA, WPA2, and WPA3)
21	2.9 Interpret the wireless LAN GUI configuration for client connectivity, such as WLAN creation, security settings, QoS profiles, and advanced settings
	5.10 Configure and verify WLAN within the GUI using WPA2 PSK
20	4.8 Configure network devices for remote access using SSH
	5.3 Configure and verify device access control using local passwords
	5.7 Configure and verify Layer 2 security features (DHCP snooping, dynamic ARP inspection, and port security)
	5.8 Compare authentication, authorization, and accounting concepts
19	1.1 Explain the role and function of network components
	3.2 Determine how a router makes a forwarding decision by default
18	1.2 Describe characteristics of network topology architectures
	1.4 Identify interface and cable issues (collisions, errors, mismatch duplex, and/or speed)
	1.6 Configure and verify IPv4 addressing and subnetting
	1.8 Configure and verify IPv6 addressing and prefix

Day	Exam Topic(s)
17	3.1 Interpret the components of routing table
	3.2 Determine how a router makes a forwarding decision by default
16	2.1 Configure and verify VLANs (normal range) spanning multiple switches
	2.2 Configure and verify interswitch connectivity
15	3.3 Configure and verify IPv4 and IPv6 static routing
14	3.4 Configure and verify single area OSPFv2
13	3.4 Configure and verify single area OSPFv2
12	3.4 Configure and verify single area OSPFv2
11	5.1 Define key security concepts (threats, vulnerabilities, exploits, and mitigation techniques)
	5.2 Describe security program elements (user awareness, training, and physical access control)
	5.4 Describe security password policy elements, such as management, complexity, and password alternatives (multifactor authentication, certificates, and biometrics)
10	5.6 Configure and verify access control lists
9	5.6 Configure and verify access control lists
8	4.1 Configure and verify inside source NAT using static and pools
7	1.2 Describe characteristics of network topology architectures
	5.5 Describe IPsec remote access and site-to-site VPNs
6	4.7 Explain the forwarding per-hop behavior (PHB) for QoS such as classification, marking, queuing, congestion, policing, and shaping
5	2.3 Configure and verify Layer 2 discovery protocols (Cisco Discovery Protocol and LLDP)
4	4.2 Configure and verify NTP operating in a client and server mode
	4.4 Explain the function of SNMP in network operations
	4.5 Describe the use of syslog features, including facilities and severity levels
	4.9 Describe the capabilities and functions of TFTP/FTP in the network
3	1.2 Describe characteristics of network topology architectures
	1.12 Explain virtualization fundamentals (server virtualization, containers, and VRFs)
	6.2 Compare traditional networks with controller-based networking
	6.3 Describe controller-based, software defined architecture (overlay, underlay, and fabric)
2	6.1 Explain how automation impacts network management
	6.3 Describe controller-based, software defined architecture (overlay, underlay, and fabric)
	6.6 Recognize the capabilities of configuration management mechanisms such as Ansible and Terraform
1	6.4 Explain AI (generative and predictive) and machine learning in network operations
	6.5 Describe characteristics of REST-based APIs (authentication types, CRUD, HTTP verbs, and data encoding)
	6.7 Recognize components of JSON-encoded data

Credits

Figure 23.10 – Microsoft Corporation

Figure 23.11 – Apple Inc.

Figure 23.12 – Ubuntu

This page intentionally left blank

Day 22

Wireless Concepts

CCNA 200-301 Exam Topics

- 1.1 Explain the role and function of network components
- 1.11 Describe wireless principles
- 2.6 Describe Cisco Wireless Architectures and AP modes
- 2.7 Describe physical infrastructure connections of WLAN components (AP, WLC, access/trunk ports, LAG)
- 5.9 Describe wireless security protocols (WPA, WPA2, and WPA3)

Key Topics

Wireless specifications are detailed in the IEEE 802.11 family of standards, including wireless topologies, spectrum allocation, and wireless security. Today we review basic wireless network concepts.

Wireless Standards

The IEEE 802.11 WLAN standards define how radio frequencies (RFs) are used for wireless links. To avoid interference, different channels within an RF can be used.

RF Spectrum

The RF spectrum, shown in Figure 22-1, includes all types of radio communications, including the 2.4-GHz and 5-GHz frequencies used by wireless devices.

Channels

A frequency range is typically called a *band* of frequencies. For example, a wireless LAN device with a 2.4-GHz antenna can actually use any frequency from 2.4000 to 2.4835 GHz. The 5-GHz band lies between 5.150 and 5.825 GHz.

The bands are further subdivided into frequency channels. Channels become particularly important when the wireless devices in a specific area become saturated. Each channel is known by a channel number and is assigned to a specific frequency. As long as the channels are defined by a national or international standards body, they can be used consistently in all locations. Figure 22-2 and Figure 22-3 show the channel layouts for the 2.4- and 5-GHz bands, respectively.

Figure 22-1 RF Spectrum

Frequency (Hz)	Frequency Notation
10^{21}	
10^{20}	
10^{19}	
10^{18}	
10^{17}	
10^{16}	
10^{15}	
10^{14}	
10^{13}	
10^{12}	
10^{11}	100 GHz
10^{10}	10 GHz
10^{9}	1 GHz
10^{8}	100 MHz
10^{7}	10 MHz
10^{6}	1 MHz
10^{5}	100 kHz
10^{4}	10 kHz
10^{3}	1 kHz
10^{2}	100 Hz
10^{1}	10 Hz
0	0 Hz

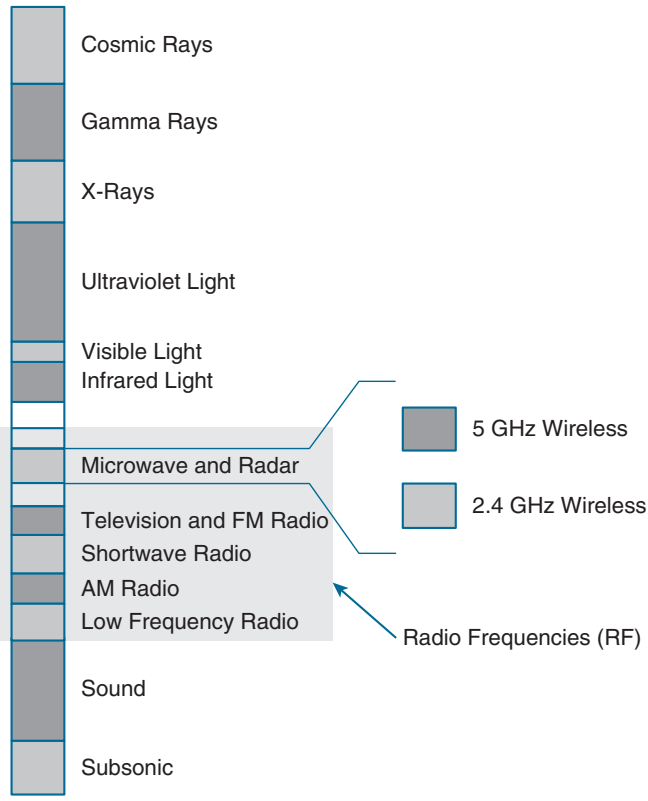
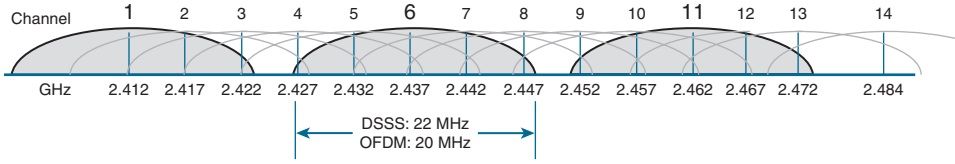
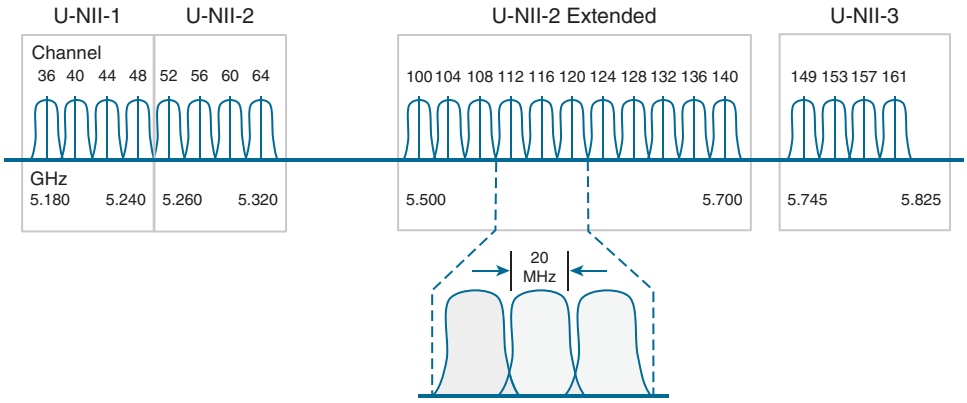


Figure 22-2 2.4-GHz Channels



Notice in Figure 22-3 that the 5-GHz band consists of nonoverlapping channels. Each channel is allocated a frequency range that does not encroach on or overlap the frequencies allocated for any other channel. The same is not true of the 2.4-GHz band in Figure 22-2. The only way to avoid any overlap between adjacent channels is to configure access points (APs) to use only channels 1, 6, and 11.

Figure 22-3 5-GHz Channels



802.11 Standards

Most of the standards specify that a wireless device must have one antenna to transmit and receive wireless signals on the specified radio frequency (2.4 GHz or 5 GHz). Some of the newer standards that transmit and receive at higher speeds require APs and wireless clients to have multiple antennas using the multiple input, multiple output (MIMO) technology. MIMO uses multiple antennas as both the transmitter and receiver to improve communication performance. Up to four antennas can be supported.

Various implementations of the IEEE 802.11 standard have been developed over the years. Table 22-1 highlights these standards.

Table 22-1 Summary of 802.11 Standards

IEEE WLAN Standard	2.4 GHz	5 GHz	6 GHz	Max Data Rate	Description
802.11-1997	Yes	No	No	2 Mbps	The original 802.11 standard, ratified in 1997
802.11a	No	Yes	No	54 Mbps	Introduced in 1999 Small coverage area Less effective at penetrating building structures Not interoperable with 802.11b and 802.11g
802.11b	Yes	No	No	11 Mbps	Introduced in 1999 Longer range than 802.11a Better able to penetrate building structures

IEEE WLAN Standard	2.4 GHz	5 GHz	6 GHz	Max Data Rate	Description
802.11g	Yes	No	No	54 Mbps	Introduced in 2003 Backward compatible with 802.11b with reduced bandwidth capacity
802.11n	Yes	Yes	No	600 Mbps	Introduced in 2009 Also known as High Throughput (HT) Distance range of up to 70 m (230 feet) APs and wireless clients require multiple antennas using MIMO technology Backward compatible with 802.11a/b/g devices with limited data rates
802.11ac	No	Yes	No	6.93 Gbps	Introduced in 2013 Also known as Very High Throughput (VHT) Uses MIMO technology Up to eight antennas can be supported Backward compatible with 802.11a/n devices with limited data rates
802.11ax	Yes	Yes	Yes	4x 802.11ac	Released in 2019 (latest standard) Also known as High-Efficiency Wireless (HEW) Higher data rates and increased capacity Handles many connected devices Improved power efficiency 1 GHz and 7 GHz capable when those frequencies become available

The Wi-Fi Alliance introduced a set of simplified names to identify each Wi-Fi generation, as listed in Table 22-2.

Table 22-2 Wi-Fi Alliance Generational Names

Wi-Fi Alliance Designation	Bands Supported	IEEE 802.11 Amendments Supported
Wi-Fi 0	2.4	802.11 (the original)
Wi-Fi 1	2.4	802.11b
Wi-Fi 2	5	802.11a
Wi-Fi 3	2.4	802.11g
Wi-Fi 4	2.4, 5	802.11n
Wi-Fi 5	5	802.11ac

Wi-Fi Alliance Designation	Bands Supported	IEEE 802.11 Amendments Supported
Wi-Fi 6	2.4, 5	802.11ax
Wi-Fi 6E	2.4, 5, 6	802.11ax
Wi-Fi 7	2.4, 5, 6	802.11be

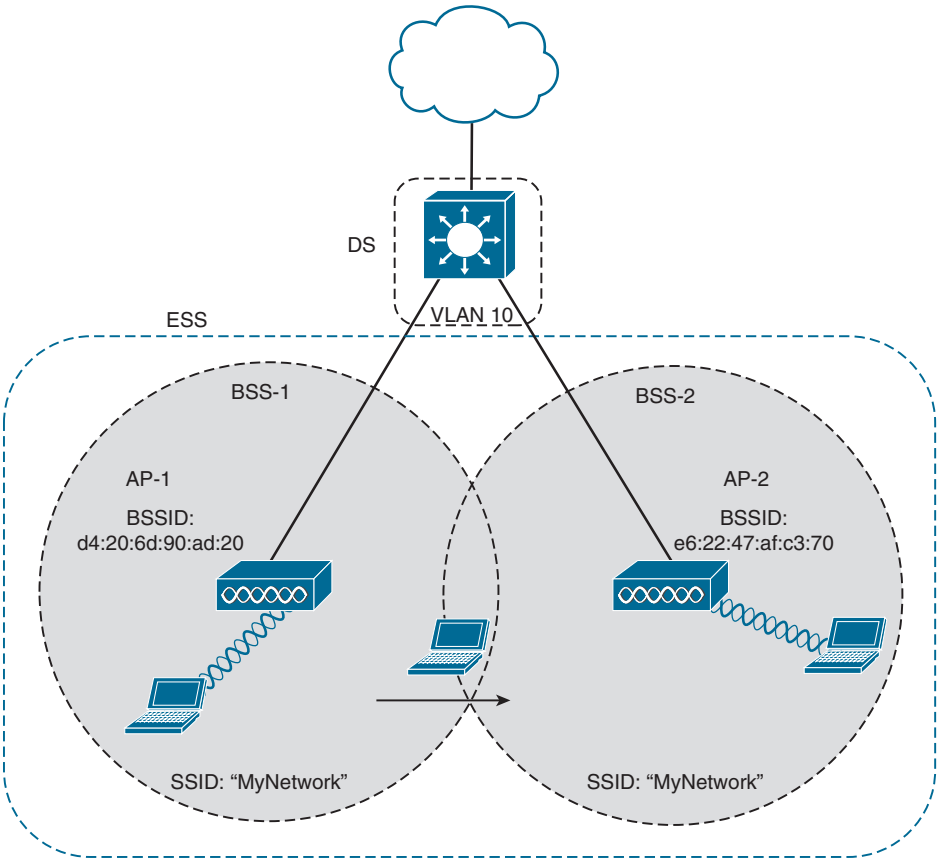
Wireless Topologies

The 802.11 standard identifies two main wireless topology modes: infrastructure mode and Independent Basic Service Set (IBSS). IBSS is also known as ad hoc mode. With the ubiquity of wireless networks, mesh topologies are now common.

Infrastructure Mode

With infrastructure mode, wireless clients interconnect via an AP. Figure 22-4 illustrates infrastructure mode terminology. Notice that the configuration of the APs to share the same SSID allows wireless clients to roam between BSAs.

Figure 22-4 Example of ESS Infrastructure Mode



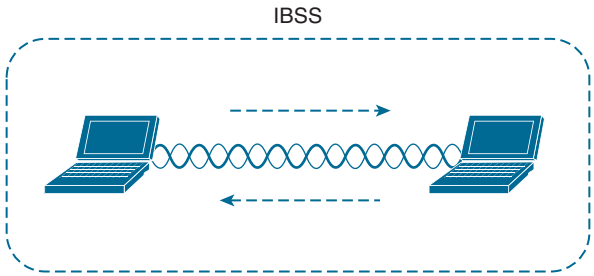
Infrastructure mode terminology includes the following:

- **Basic service set (BSS)**: This consists of a single AP interconnecting all associated wireless clients.
- **Basic service area (BSA)**: This is the area that is bound by the reach of the AP's signal. The BSA is also called a *cell* (the gray area in Figure 22-4).
- **Basic service set identifier (BSSID)**: This is the unique, machine-readable identifier for the AP that is in the format of a MAC address and is usually derived from the AP's wireless MAC address.
- **Service set identifier (SSID)**: This is a human-readable, non-unique identifier used by the AP to advertise its wireless service.
- **Distribution system (DS)**: APs connect to the network infrastructure using the wired DS, such as Ethernet. An AP with a wired connection to the DS is responsible for translating frames between 802.3 Ethernet and 802.11 wireless protocols.
- **Extended service set (ESS)**: When a single BSS provides insufficient coverage, two or more BSSs can be joined through a common DS into an ESS. An ESS is the union of two or more BSSs interconnected by a wired DS. Each ESS is identified by its SSID, and each BSS is identified by its BSSID.

IBSS, or Ad Hoc Mode

In the 802.11 standard, Independent Basic Service Set (IBSS) is defined as two devices connected wirelessly in a peer-to-peer (P2P) manner without the use of an AP. One device takes the role of advertising the wireless network to clients. The IBSS allows two devices to communicate directly without the need for any other wireless devices, as shown in Figure 22-5. IBSSs do not scale well beyond 8 to 10 devices.

Figure 22-5 802.11 Independent Basic Service Set

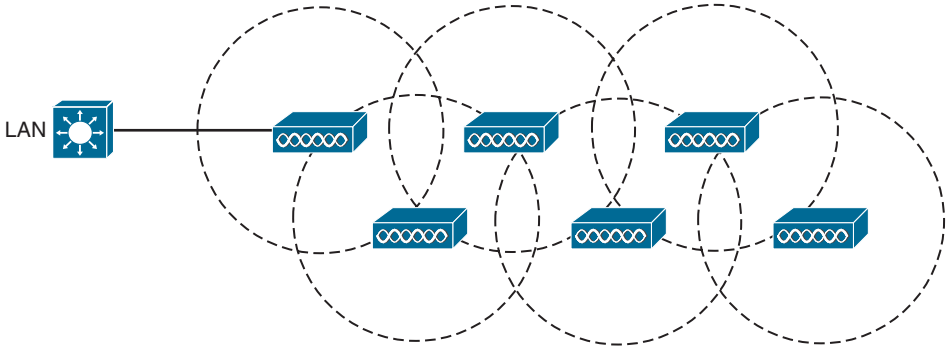


Mesh

Having a wired DS connecting all APs is not always practical or necessary. Instead, APs can be configured to connect in mesh mode. In this mode, APs bridge client traffic between each other, as shown in Figure 22-6.

Each AP in the mesh maintains a BSS on one channel used by wireless clients. Then the APs bridge between each other using other channels. The mesh network runs its own dynamic routing protocol to determine the best path to the wired network.

Figure 22-6 Example of a Wireless Mesh Network



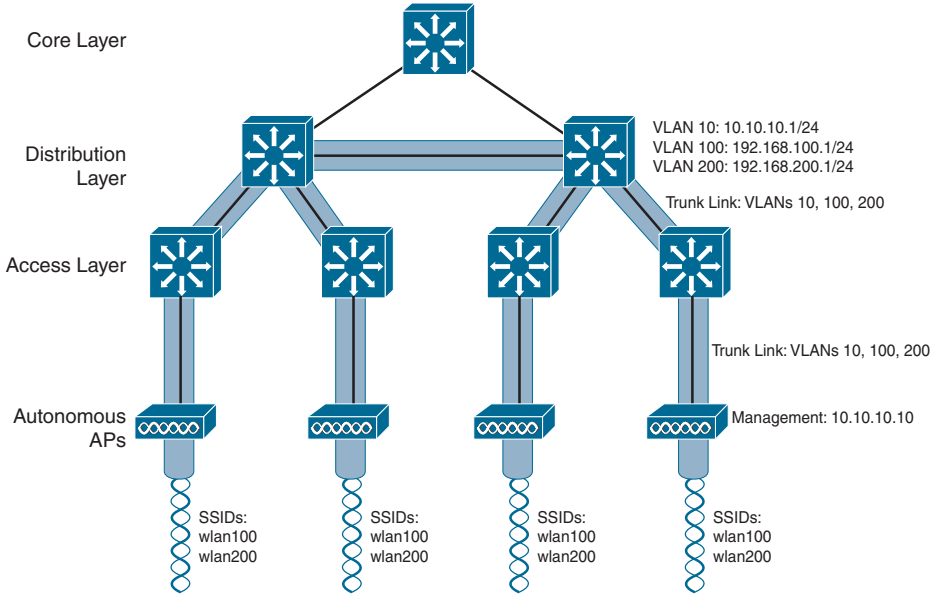
AP Architectures

APs can be networked together in a variety of architectures. The size and scalability of the network determine which architecture is most suited for a given implementation.

Autonomous AP Architecture

An autonomous AP is a self-contained device with both wired and wireless hardware so that it can bridge to the wired VLAN infrastructure wireless clients that belong to SSIDs, as shown in Figure 22-7. Each autonomous AP must be configured with a management IP address so that it can be remotely accessed using Telnet, SSH, or a web interface. Each AP must be individually managed and maintained unless you use a management platform such as Cisco DNA Center.

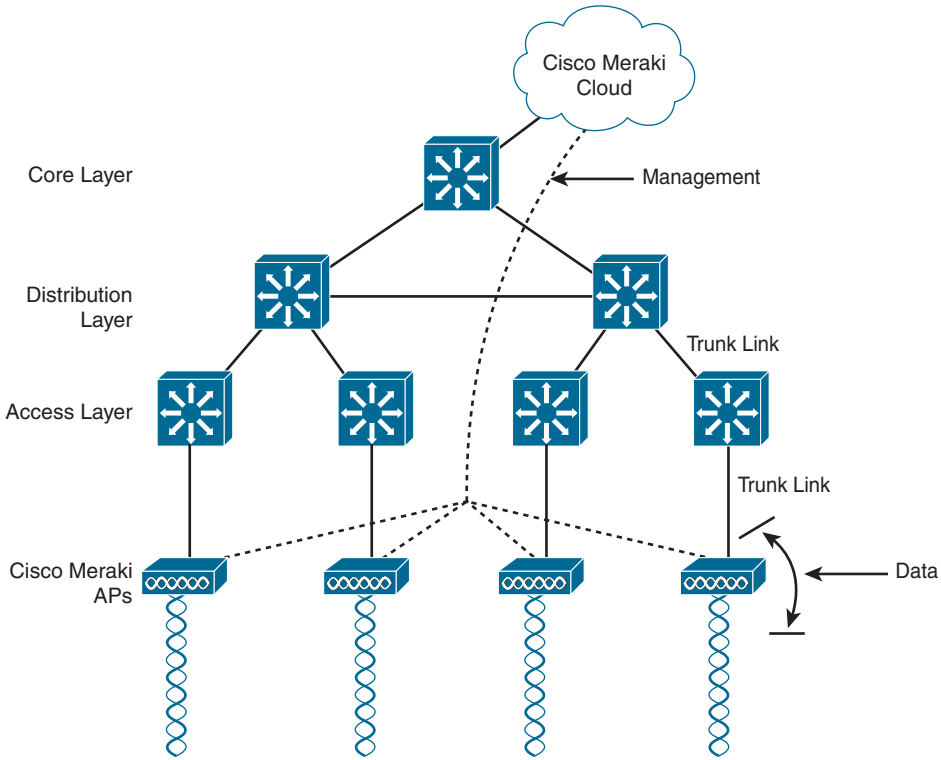
Figure 22-7 Autonomous APs



Cloud-Based AP Architecture

Cloud-based AP management is an alternative to purchasing a management platform. The AP management function is pushed into the Internet cloud. For example, Cisco Meraki is a cloud-based AP management service that allows you to automatically deploy Cisco Meraki APs. These APs can then be managed from the Meraki cloud web interface (dashboard). In Figure 22-8, the same APs shown in Figure 22-7 are now managed in the cloud.

Figure 22-8 Cisco Meraki Cloud-Based AP Management



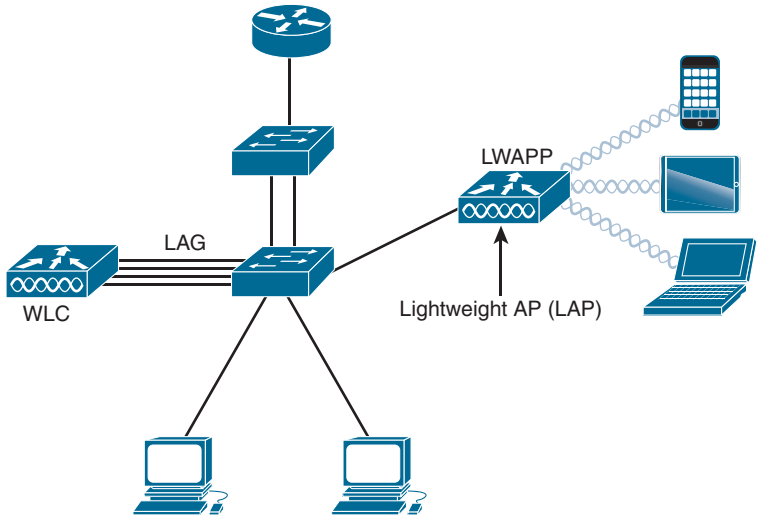
Notice that there are two distinct paths for data traffic and for management traffic, corresponding to the following two functions:

- **A control plane**: Traffic used to control, configure, manage, and monitor the AP itself
- **A data plane**: End-user traffic passing through the AP

Lightweight AP Architectures

Wireless LAN controllers (WLCs) use Lightweight Access Point Protocol (LWAPP) to communicate with lightweight APs (LAPs), as shown in Figure 22-9. LAPs are useful in situations where many APs are required in the network. They are "lightweight" because they only perform the 802.11 wireless operation for wireless clients. Each LAP is automatically configured and managed by the WLC.

Figure 22-9 Controller-Based AP Architecture



Notice in Figure 22-9 that the WLC has four ports connected to the switching infrastructure. These four ports are configured as a link aggregation group (LAG) so they can be bundled together. Much like EtherChannel, LAG provides redundancy and load balancing.

CAPWAP Operation

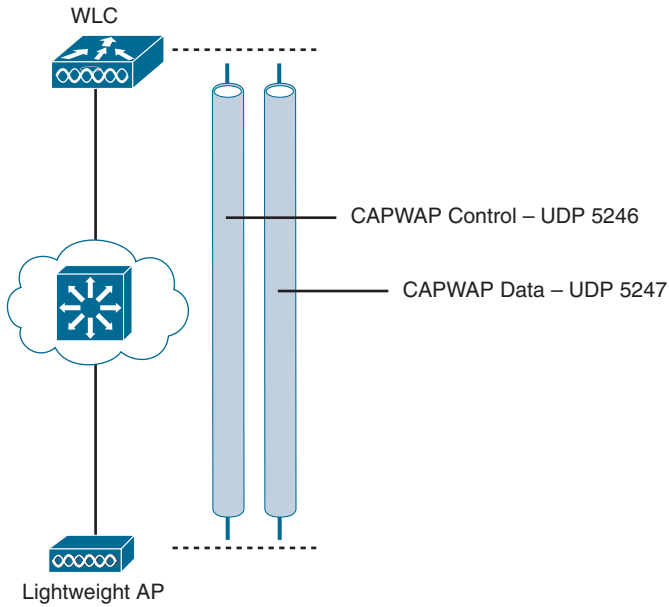
The division of labor between the WLC and LAPs is known as *split-MAC architecture*. The LAP must interact with wireless clients on some low level, known as the Media Access Control (MAC) layer. These functions must stay with the LAP hardware, closest to the clients. The management functions are not integral to handling frames but are things that should be centrally administered. Therefore, those functions can be moved to a centrally located platform away from the AP. Table 22-3 summarizes MAC functions of the LAP and WLC.

Table 22-3 Split-MAC Functions of the AP and WLC

AP MAC Functions	WLC MAC Functions
Beacons and probe responses	Authentication
Packet acknowledgments and retransmissions	Association and re-association of roaming clients
Frame queueing and packet prioritization	Frame translation to other protocols
MAC layer data encryption and decryption	Termination of 802.11 traffic on a wired interface

LWAPP has been replaced with the Control and Provisioning of Wireless Access Points (CAPWAP) tunneling protocol to implement these split-MAC functions. CAPWAP uses two tunnels—one for control and one for data—as shown in Figure 22-10 and described in the list that follows:

Figure 22-10 CAPWAP Control and Data Tunnels



- **CAPWAP control message tunnel**: Carries exchanges that are used to configure the LAP and manage its operation. The control messages are authenticated and encrypted, so the LAP is securely controlled by only the appropriate WLC and then transported over the control tunnel using UDP port 5246.
- **CAPWAP data tunnel**: Used for packets traveling to and from wireless clients that are associated with the AP. Data packets are transported over the data tunnel using UDP port 5247 but are not encrypted by default. When data encryption is enabled for a LAP, packets are protected with Datagram Transport Layer Security (DTLS).

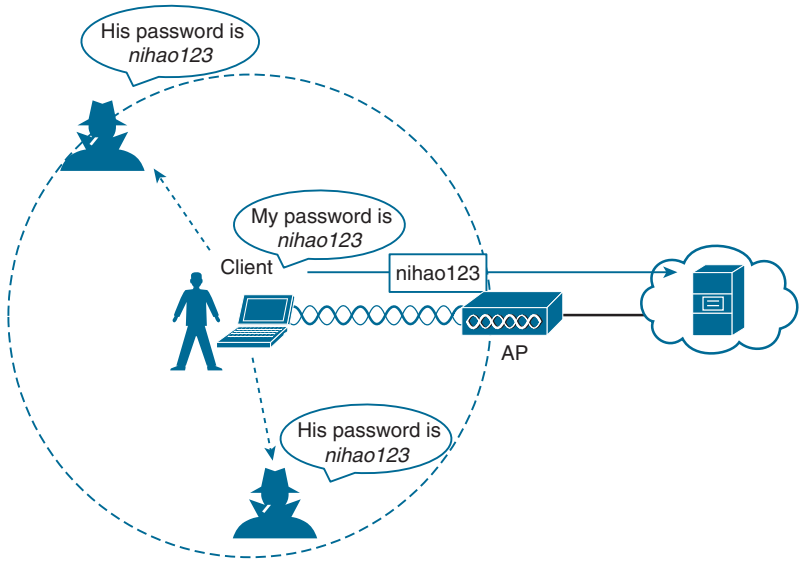
Wireless Security Protocols

Wireless traffic is inherently different from traffic traveling over a wired infrastructure. Any wireless device operating in the same frequency can hear the frames and potentially read them. Therefore, WLANs need to be secured to allow only authorized users and devices and to prevent eavesdropping and tampering of wireless traffic.

Wireless Authentication Methods

For wireless devices to communicate over a network, they must first associate with the AP. An important part of the 802.11 process is discovering a WLAN and subsequently connecting to it. During this process, transmitted frames can reach any device within range. If the wireless connection is not secured, then others can read the traffic, as shown in Figure 22-11.

Figure 22-11 Open Wireless Network



The best way to secure a wireless network is to use authentication and encryption systems.

Two types of authentication were introduced with the original 802.11 standard:

- **Open system authentication**: Should only be used in situations where security is of no concern. The wireless client is responsible for providing security such as by using a virtual private network (VPN) to connect securely.
- **Shared key authentication**: Provides mechanisms shown in Table 22-4 to authenticate and encrypt data between a wireless client and an AP. However, the password must be pre-shared between the parties to allow connection.

Table 22-4 Shared Key Authentication Methods

Authentication Method	Description
Wired Equivalent Privacy (WEP)	The original 802.11 specification designed to secure the data using the Rivest Cipher 4 (RC4) encryption method with a static key. However, the key never changes when exchanging packets. This makes WEP easy to hack. WEP is no longer recommended and should never be used.
Wi-Fi Protected Access (WPA)	A Wi-Fi Alliance standard that uses WEP but secures the data with the much stronger Temporal Key Integrity Protocol (TKIP) encryption algorithm. TKIP changes the key for each packet, making it much more difficult to hack.
WPA2	The current industry standard for securing wireless networks. It uses the Advanced Encryption Standard (AES) for encryption. AES is currently considered the strongest encryption protocol.
WPA3	The next generation of Wi-Fi security. All WPA3-enabled devices use the latest security methods, disallow outdated legacy protocols, and require the use of Protected Management Frames (PMF). However, devices with WPA3 are not yet readily available.

WPA and WPA2

Home routers typically have two choices for authentication: WPA and WPA2. WPA2 is the stronger of the two. WPA2 authentication methods included the following:

- **Personal**: Intended for home or small office networks, users authenticate using a pre-shared key (PSK). Wireless clients authenticate with the wireless router using a pre-shared password. No special authentication server is required.
- **Enterprise**: Intended for enterprise networks but requires a Remote Authentication Dial-In User Service (RADIUS) authentication server. Although more complicated to set up, it provides additional security. The device must be authenticated by the RADIUS server, and then users must authenticate using the 802.1X standard, which uses Extensible Authentication Protocol (EAP) for authentication.

802.1X/EAP

With open and WEP authentication, wireless clients are authenticated locally at the AP without further intervention. The scenario changes with 802.1X: The client uses open authentication to associate with the AP, and then the client authentication process occurs at a dedicated authentication server. Figure 22-11 shows the three-party 802.1X arrangement, which consists of the following entities:

- **Supplicant**: The client device that is requesting access.
- **Authenticator**: The network device that provides access to the network. In Figure 22-11, the AP forwards the supplicant's message to the WLC.
- **Authentication server (AS)**: The device that permits or denies network access based on a user database and policies (usually a RADIUS server).

WPA3

WPA3 includes four features:

- **WPA3-Personal**: In WPA2-Personal, threat actors can listen in on the "handshake" between a wireless client and the AP and use brute-force attacks to try to guess the PSK. WPA3-Personal thwarts such attacks by using Simultaneous Authentication of Equals (SAE), a feature specified in the IEEE 802.11-2016. The PSK is never exposed, making it impossible for the threat actor to guess.
- **WPA3-Enterprise**: WPA3-Enterprise still uses 802.1X/EAP authentication. However, it requires the use of a 192-bit cryptographic suite and eliminates the mixing of security protocols for previous 802.11 standards. WPA3-Enterprise adheres to the Commercial National Security Algorithm (CNSA) suite, which is commonly used in high-security Wi-Fi networks.
- **Open networks**: Open networks in WPA2 send user traffic in unauthenticated plaintext. In WPA3, open or public Wi-Fi networks still do not use any authentication. However, they do use Opportunistic Wireless Encryption (OWE) to encrypt all wireless traffic.

- **IoT onboarding**: Although WPA2 included Wi-Fi Protected Setup (WPS) to quickly onboard devices that were not previously configured, WPS is vulnerable to a variety of attacks and is not recommended. Furthermore, IoT devices are typically headless, meaning they have no built-in GUI for configuration and need an easy way to get connected to the wireless network. Device Provisioning Protocol (DPP) was designed to address this need. Each headless device has a hard-coded public key. The key is typically stamped on the outside of the device or its packaging as a Quick Response (QR) code. The network administrator can scan the QR code and quickly onboard the device. Although DPP is not strictly part of the WPA3 standard, it will replace WPS over time.

Wireless Encryption Methods

Encryption is used to protect data. An intruder may be able to capture encrypted data, but he or she would not be able to decipher it in any reasonable amount of time. The following encryption protocols are used with wireless authentication:

- **Temporal Key Integrity Protocol (TKIP)**: TKIP is the encryption method used by WPA. It provides support for legacy WLAN equipment and addresses the original flaws associated with the 802.11 WEP encryption method. It makes use of WEP but encrypts the Layer 2 payload using TKIP and carries out a message integrity check (MIC) in the encrypted packet to ensure that the message has not been altered.

- **Advanced Encryption Standard (AES)**: AES is the encryption method used by WPA2. It is the preferred method because it is a very strong method of encryption. It uses Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP), which allows destination hosts to recognize if the encrypted and nonencrypted bits have been altered.

- **Counter/CBC-MAC Protocol (CCMP)**: CCMP is the encryption protocol used by WPA2. It provides enhanced data confidentiality and integrity by using AES. CCMP operates using Counter Mode for encryption and Cipher Block Chaining Message Authentication Code (CBC-MAC) for message integrity, ensuring that both encrypted and non-encrypted parts of the packet have not been altered. This makes CCMP a highly secure and reliable protocol for protecting wireless communications.

- **The Galois/Counter Mode Protocol (GCMP)**: GCMP is the encryption protocol used by WPA3. It enhances security and efficiency compared to CCMP. GCMP combines the Galois Message Authentication Code (GMAC) for data integrity and authenticity with the Counter Mode for encryption. This dual approach ensures that encrypted data remains confidential, and any tampering with the data can be detected. GCMP provides robust protection against attacks and improves performance, making it suitable for modern wireless networks that require higher security standards.

Table 22-5 summarizes the basic differences between WPA, WPA2, and WPA3. Each successive version is meant to replace prior versions and offer better security features. You should avoid using WPA and use WPA2 instead—at least until WPA3 becomes widely available on wireless client devices, APs, and WLCs.

Table 22-5 Wireless Authentication and Encryption Comparison

Feature	WPA	WPA2	WPA3
Authentication with pre-shared keys?	Yes	Yes	Yes
Authentication with 802.1X?	Yes	Yes	Yes
Encryption and MIC with TKIP?	Yes	No	No
Encryption and MIC with AES and CCMP?	Yes	Yes	No
Encryption and MIC with AES and GCMP?	No	No	Yes

Study Resources

For today's exam topics, refer to the following resources for more study.

Resource	Module or Chapter
Cisco Network Academy: Switching, Routing, and Wireless Essentials v7	12
CCNA 200-301 Official Cert Guide, Volume 2, 2nd edition	1–3
Portable Command Guide	23

This page intentionally left blank

Index

Numerics

A

B

C

D

E

F

G

H

I

J-K-L

M

N

O

P

Q

R

S

T

U

V

W

X-Y-Z