

CCNA

**A COMPREHENSIVE GUIDE TO THE LATEST CCNA (CISCO
CERTIFIED NETWORK ASSOCIATE) CERTIFICATION,
INCLUDING ADVICE AND TIPS ON TAKING THE EXAM**



WALKER SCHMIDT

CCNA

*A Comprehensive Guide to the Latest
CCNA (Cisco Certified Network
Associate) Certification, Including
Advice and Tips on Taking the Exam*

© Copyright 2020 by Walker Schmidt - All rights reserved.

The content contained within this book may not be reproduced, duplicated or transmitted without direct written permission from the author or the publisher.

Under no circumstances will any blame or legal responsibility be held against the publisher, or author, for any damages, reparation, or monetary loss due to the information contained within this book, either directly or indirectly.

Legal Notice:

This book is copyright protected. It is only for personal use. You cannot amend, distribute, sell, use, quote or paraphrase any part, or the content within this book, without the consent of the author or publisher.

Disclaimer Notice:

Please note the information contained within this document is for educational and entertainment purposes only. All effort has been executed to present accurate, up to date, reliable, complete information. No warranties of any kind are declared or implied. Readers acknowledge that the author is not engaged in the rendering of legal, financial, medical or professional advice. The content within this book has been derived from various sources. Please consult a licensed professional before attempting any techniques outlined in this book.

By reading this document, the reader agrees that under no circumstances is the author responsible for any losses, direct or indirect, that are incurred as a result of the use of the information contained within this document, including, but not limited to, errors, omissions, or inaccuracies.

Table of Contents

[Introduction](#)

[Chapter 1: Cisco](#)

[A Brief History of Routers and Networking](#)

[Cisco Facts](#)

[Chapter 2: Cisco Certifications](#)

[Changes to the Cisco Certification Path for 2020](#)

[Entry Level](#)

[Associate Level](#)

[Professional Level](#)

[Expert Level](#)

[Architect Level](#)

[Chapter 3: The New CCNA Certification](#)

[Why CCNA?](#)

[Topics Included in the New CCNA Certification](#)

[The Course Specifics](#)

[CCNA Candidates](#)

[New CCNA Certification Prerequisites](#)

[Chapter 4: The New Cisco Certified Network Associate \(CCNA\) Course](#)

[The Course Outline](#)

[Instructor-Led Course Outline](#)

[Self-Study Course Outline](#)

[Lab Course Outline](#)

[Course Objectives](#)

[Chapter 5: 200-301 Cisco Certified Network Associate \(CCNA\) Exam](#)

[Basic Exam Information](#)

[Booking the CCNA Exam](#)

[Cisco Exam Policies](#)

[Retaking the CCNA Exam](#)

[What the Exam Covers](#)

[Chapter 6: 200-301 CCNA - Exam Preparation](#)

[What to Expect at the Exam Testing Center](#)

[The Testing Center](#)

[The Exam Room](#)

[The Exam Format](#)

[Preparing for the Exams](#)

[Network Simulators for the CCNA](#)

[Cisco Learning Network](#)

[Pearson Test Prep](#)

[Exam Study Schedule](#)

[Chapter 7: Understanding Networks](#)

[What is a Network?](#)

[Understanding Network Architecture](#)

[Types of Computer Networks](#)

[Network Topology](#)

[Standards](#)

[Protocols](#)

[Network Layers](#)

[Interfaces](#)

[Important Network Terms to Remember](#)

[Basic Network Fundamentals](#)

[Access Points](#)

[Routers](#)

[Switches](#)

[Wireless Networking](#)

[Chapter 8: Study Material — Network Fundamentals](#)

[Foundation Topic](#)

[Network Components](#)

[Network Topology Architecture](#)

[Cabling Types and Physical Interfaces](#)

[Chapter 9: Study Material — Network Access](#)

[Chapter 10: Study Material — IP Connectivity](#)

[Chapter 11: Study Material — IP Services](#)

[Chapter 12: Study Material — Security Fundamentals](#)

[Network Security](#)

[VPN](#)

[Layer 2 Security](#)

[Wireless Security](#)

[Chapter 13: Study Material — Automation and Programmability](#)

[Chapter 14: CCNA Interview Questions](#)

[Interview Questions for CCNA Position](#)

[Top Jobs for CCNA Certified Professionals](#)

[Conclusion](#)

[Quick Recap Tips For Passing Your CCNA Exam](#)

References

Introduction

Cisco devices are one of the most popular networking device brands on the market today. Their systems are found in thousands of large data centers and corporations all over the world. Every IT engineer knows the Cisco brand name and chances are, they have probably at some stage or other come across one or more of their switches, routers, and even their telephony systems.

With their huge market presence and continuous introduction of new products as well as updating some of their older more popular ones, they are going to be around well into the future. In order to help information technology engineers better understand, manage, and operate their devices, Cisco has a certification program that starts off with entry-level certificates to the highest architect level. There are six different certification levels and each level has its own set of certifications.

These certifications have been designed to help network engineers use the Cisco products with confidence and ease. The courses are aimed at different divisions of the IT networking environment, for instance, the new CCNA course is the networking foundation course that covers a broad spectrum of IT topics and systems. Prior to the new CCNA course, the student chooses from one of the IT topics such as the CCNA Cloud or the CCNA Wireless certifications. This means that if the student wanted to do both they would have to purchase the two courses and sit two separate exams.

With the new CCNA certification, all the older courses except for the CCNA Cyber Ops all the other Associate level CCNA certifications have been retired or are going to be retired on 22 February 2020. But fear not, because the new CCNA covers a lot of what those certifications did, only the information has all been revamped and brought up to date with current technologies. The good news is now there is only the one CCNA course and exam to take.

DevOps has taken off and the world of IT is scrambling towards implementing DevOps solutions. Cisco has adopted DevOps into the Cisco environment and added some new specialist certifications to its new revamped list. One of these specialist certifications is at the Associate level and that is the DevNet Associate certifications. Now with only one super

CCNA course, a student can opt to do either the Associate level certifications to become more specialized in the Cisco field. Cisco also offers various forums and help centers that are available through the Cisco Learning Network and Cisco Community.

The material in this book has been written with both the beginner and the more advanced network engineer that is thinking of taking the CCNA exam in mind. As there are no prerequisites for the CCNA exam, anyone who has an interest in becoming a certified network engineer can take the course and exam. Although, Cisco does recommend a person has some network experience or understanding that is only for taking the exam.

When you arrive at your training all eager to get started, it is then assumed that you do have the necessary experience and basic knowledge. As once having been a newbie myself to the world of networking, I know how daunting and confusing it can be to find yourself neck-deep in confusing terminology, especially that of the networking world.

IT people tend to forget that there are people in the world that speak English and not tech. So even when they do cover the basics of networking, it sounds like some language from Star Trek. This book has been written in order to give everyone a chance to understand what is expected from the learner for the new CCNA exam.

At some points, it may seem pretty basic to those who have been working as network engineers. But trust me, you will be surprised at how rusty your memory may be when it comes to some of the very basics you take for granted every day or do not really use much. Although during the course, the information may be skimmed over, it is still important, and as is stressed throughout the book, examiners love to throw a spanner in the works with a question about the basics of basics.

Note: *The following information has been gathered to help you with your study preparation for the 200-301 CCNA certification and is not meant to replace the actual 200-301 CCNA course information. Together with your course materials, they will provide a good base for you to start planning your study schedule.*

Chapter 1: Cisco

Cisco is one of the largest corporations in the United States, with its products primarily targeted at the business sector. Cisco is the leading innovator and provider of networking and communications technologies worldwide. The principal office is based in Silicon Valley, San Jose, California. The company has offices across the United States as well as various sales and service centers located in seventy-five countries worldwide.

A Brief History of Routers and Networking

The history of routers goes back quite a few decades and has its roots in devices called Interface Message Processors. This was a gateway computer that was used in ARPANET in 1967 and functioned the same as the more modern router does.

The idea of networking computers together came about mainly because organizations like ARPANET needed to identify a more effective way to exchange data between their core sites. They had these ‘new’ computers but transferring data between them was quite a task in itself.

The first gateway machines were limited in the scope of inter-networking which gave rise to a group of researchers that were called the International Network Working Group. This informal group was put together in the early 1970s with the primary purpose of being a think tank for resolving internetworking issues.

Ginny Strazisar developed the first true IP router in 1976 as part of a DARPA initiation project. Ginny worked for BBN, as a research and development company, at the time.

In 1981 two staff researchers from independent universities in the United States developed the first two multiprotocol routers. William Yeager developed the system for Stanford University, while Noel Chiappa developed the router for MIT. These routers were primarily based on the PDP-11s protocol. PDP-11s were widely used to link multiprotocol computers throughout the 1970s into the 1980s before the use of TCP/IP became the

standard.

Cisco was founded in 1984 by Sandra Lerner and Leonard Bosack. Sandra and Leonard both graduated from and worked in different computer departments at Stanford University.

Using base technology devised in the 1970s by past Stanford University employees, Leonard Bosack devised a method to connect various campus department networks together.

Cisco Facts



As of 1 November 2019, Cisco Systems market cap was over \$190 billion United States dollars, therefore making Cisco the largest communications and networking technologies company. It has been a global industry leader in networking and information technology throughout the globe. It is a very recognized brand name that most people, not just those in IT, recognize.

Cisco's main product lines are that of various networking systems such as routers, switches, IoT and various networking security products. Not only does Cisco have a presence in organizations for IT solutions, but also telephone systems. Cisco prides itself on its network integrating telephony models which include a range of teleconferencing systems.

Cisco has been around for almost four decades, and each year continues to hold its position in the IT industry. Here are some facts about Cisco Systems that every aspiring CCNA or CCNP should know about the organization.

Cisco's Name

The company's name derives from the town where the co-founders established the business back in 1984. Cisco is short for San Francisco and is the reason why the Cisco logo is a representation of the Golden Gate Bridge.

Cisco vs Stanford University

In 1984 when the co-founders, who were married at the time, founded Cisco, they were both employed at different IT departments by Stanford. Kirk Lougheed, another co-founder of Cisco, was also employed at Stanford at the time he and Bosack developed Cisco's first router. The "new" router turned out to be the same as the current "Blue Box" router which was already in use at Stanford University. The router also ran an unlicensed copy of the Blue Boxes multiprotocol software they had re-designed and became the base for the Cisco IOS.

Lougheed and Bosack were made to resign their positions at Stanford University in 1986 with the threat of Stanford looking to file charges against Cisco for the use of their router and software design. However, in 1987, Stanford and Cisco were able to come to an agreement and the university agreed to let Cisco license their software.

A World-Wide Global Giant

On the 10th December 19200-301 CCNA84, Cisco was officially incorporated and it went public on 16th February 1990. Today, Cisco employs, globally, over 70,00 employees. It is one of the top IT companies in the world and it became the world's most valuable company in March of 2000 with a \$500 billion market cap. This was at the height of the dot-com surge, and as might have been expected, when the dot-com era came to a halt Cisco took the plunge with it.

Cisco has never been able to regain its title as the world's most valuable company after the dot-com era halted abruptly. That title went to Apple which, as of June 2019, was knocked into the second position after Amazon took over the title. Even now Cisco remains a giant and innovative leader in the world of networking and communications infrastructure technology.

Cisco and Cybersecurity

One of the fastest growing IT industries is cybersecurity, which has been growing aggressively over the past few years. Cisco has been growing their cybersecurity over the recent years and bundles some of its security products with their software and hardware. This provides them with an edge over the smaller IT security companies.

Cisco Networking Academy

Cisco's Networking Academy started in October of 1997 and was launched in seven states. There were sixty-four institutes whereby Cisco provided students with free training.

NetAcad has since spread to over 150 countries and has trained over 1 million students. They have over 10,000 Cisco Networking Academies that are integrated into high schools, colleges, technical schools, and universities.

Chapter 2: Cisco Certifications



Cisco has introduced its new Cisco certification path which goes live on 24 February 2020.

Anyone who is already on the Cisco Certified Design Architect (CCDA) or the Cisco Certified Network Associate (CCNA) certification path, is encouraged to keep working towards their certification. However, you will have to write the exam(s) before 23 February 2020. Upon completion of the Cisco Certified Design Architect (CCDA) or Cisco Certified Network Associate (CCNA), the candidate will be awarded the new Certified Cisco Network Associate (CCNA) certification. The certification will be accompanied by the corresponding area of technology recognition badge.

Holders of the Cisco Certified Entry Networking Technician (CCENT) certification are encouraged to upgrade their certification to a Cisco Certified Network Associate (CCNA) before 23 February 2020.

As of February 24, you will need to take the new exam to complete CCNA certification. The new exams do not only affect the Cisco entry-level or the associate levels, as Cisco has revamped nearly all their certifications for 2020.

For active CCIE certificate holders if their suspended year was May 10,

2020, this will be made active and for a period of one year. For instance, the certification for May 10, 2020 will then become inactive on May 10, 2021.

Changes to the Cisco Certification Path for 2020

While a few of the certifications may remain, they have been revamped to keep up with modern technology trends. Cisco has brought their training program in line with the latest technological trends to ensure that their Cisco Professionals are keeping up with the latest innovations.

It should also be noted that some of the recertification policies will be changing. From the 23 February 2020, any individuals who are doing or about to do one of the Cisco certification paths should check the policies.

The new Cisco Certification path as from 23 February 2020 is as follows:

Entry Level

The entry-level is the basic foundation courses that introduce the individual to networking solutions. The certifications that are available in this section teach the students the basic fundamentals of networking and start them on the correct path to becoming a Cisco networking engineer.

CCENT — Cisco Certified Entry Network Technician

This was the basic entry-level exam and the recommended prerequisite to climbing to the next level and to get the CCNA. In this course students were introduced to the basic networking fundamentals. This course teaches about routing technologies, infrastructure maintenance and services, and LAN switching.

This certification will no longer be available as of 23 February 2020. All those that are currently taking this certification or currently hold this certification should complete their exams before the 23 February and take the CCNA certifications.

CCT — Cisco Certified Technician

This certificate is another entry-level certificate from Cisco. Upon the

successful completion of the course, Cisco Certified Technicians are able to confidently diagnose networking problems. They are able to repair, replace, and restore various critical networking systems.

CCT's have the option of following multiple solution tracks to obtain their CCT certifications. These certifications are designed to further advance their careers as a CCT by giving them the added advantage of expanding their skill set.

This course and certification will still be available with the new structure of the Cisco certification path. The new CCT certification will be available from the 23 February 2020.

The other two certifications tracks available under this section are:

CCT Data Centers

Upon the successful completion of the CCT Data Center certification, the candidate will have acquired the skill set to competently be able to maintain and support 'Cisco Unified Computing Systems' as well as servers. It focuses on the skills required for onsite support and maintenance of Cisco Unified Computing Systems and servers.

There is only one exam requirement that must be passed to obtain the CCT Data Centers certification.

This course and certification will still be available with the new structure of the Cisco certification path. The new CCT Data Centers certification will be available from the 23 February 2020.

CCT Switching & Routing

Upon successful completion of the CCT Routing and Switching course, the individual will have the skill set to offer support of Cisco networking systems including that of routers, operating environments, and switches.

There is only one exam requirement that must be passed to obtain the CCT Switching and Routing certification.

The certification is valid for three years before recertification is required.

This course and certification will still be available with the new structure of the Cisco certification path. The new CCT Switching and Routing certification will be available from the 23 February 2020.

Associate Level

The Associate level of the Cisco certification path is the foundation certificate for the next step up to the professional level. In the new February 2020 course structure, a lot of changes have been made to the courses and exams at this level.

As the various networking infrastructure has rapidly evolved in the past years, IT engineers need to keep themselves updated with all the latest technology trends. As IT is an ever-changing landscape, keeping your career moving forward means keeping your knowledge fresh and moving with the times. As the systems become more advanced, so does the need for programmability, security, automation, and stability in mission-critical systems.

New CCNA — Cisco Certified Network Associate

As the job market is really competitive, keeping your Cisco certifications up to date gives you the edge over your competition. Cisco has revamped its Cisco Certified Network Associate (CCNA) certification to make sure its Certificate carrying engineers are fully trained in today's latest technologies.

The new CCNA certification path has replaced the following certifications that will be retired come 23 February 2020:

- CCDA — Cisco Certified Design Architect
- CCNA Cloud
- CCNA Collaboration
- CCNA Data Center
- CCNA Industrial
- CCNA Routing & Switching
- CCNA Security
- CCNA Service Provider
- CCNA Wireless

The above certifications will now be covered within the new CCNA course which will cover a broader spectrum of IT fundamentals in one course. This means that after the successful completion of the new CCNA exam, the individual will have a breadth of networking knowledge that would previously have taken at least three to four exams to acquire.

There is only one exam requirement that must be passed to obtain the new CCNA certification.

The certification is valid for three years before recertification is required.

The new CCNA certification will be available from the 23 February 2020.

CCNA Cyber Ops

Cybersecurity has become one of the fastest growing IT industries and is set to keep growing over the next decade or so. Cisco Cyber Ops course is one of the most recognized cybersecurity courses and it was approved by the DOD in July of 2018.

There are two exam requirements that must be passed to obtain the CCNA Cyber Ops certification.

The certification is valid for three years before recertification is required.

The CCNA Cyber Ops course will be part of the new revamped 2020 course structure, but requirements for recertification of the course may be changing. The new CCNA Cyber Ops certification will be available from the 23 February 2020.

Cisco Certified DevNet Associate

The Cisco Certified DevNet Associate is a new course that has been added to the Associate certification level. This new certification is for software professionals including developers, automation specialists, and DevOps engineers.

There is only one exam requirement that must be passed to obtain the new Cisco Certified DevOps certification.

The certification is valid for three years before recertification is required.

This certification will be launched on the 23 February 2020.

Professional Level

The Professional level of Cisco certification is a level that validates the individual's advanced networking skills. This level of the Cisco certification path has also had quite a revamp with various certifications falling away as they are incorporated into one single course.

CCNP Enterprise

The new CCNP Enterprise certificate has been designed to include programmability and automation for network scaling. This replaces the following Professional Level certifications:

- CCDP — Cisco Certified Design Professional
- CCNP Wireless
- CCNP Routing and Switching

There are two exam requirements that must be passed to obtain the CCNP Enterprise certification.

The certification is valid for three years before recertification is required.

The new CCNP Enterprise certification will be available as of the 23 February 2020.

CCNP Collaboration

The CCNP collaboration course is for anyone who is interested in pursuing a career in collaboration infrastructure. Although there are no prerequisites except for a basic understanding of the exam topic, most of the individuals who do the CCNP Collaboration course have at least three to five years of data center experience.

There are two exam requirements that must be passed to obtain the new CCNP Collaboration certification. There are the core exam and an elective concentration exam which you can choose between four collaboration paths:

- CLICA — Implementing Cisco Collaboration Applications
- CLACCM — Implementing Cisco Advanced Call Control and Mobility Services
- CLCEI — Implementing Cisco Collaboration Cloud and Edge Solutions
- CLAUI — Implementing Cisco Automation for Cisco Collaboration Solutions

The certification is valid for three years before recertification is required.

This course will still be an available option in the February 2020 course restructuring. However, the current course and exams will be replaced by newer versions. The new CCNP Collaboration certification will be available

from the 23 February 2020.

CCNP Data Center

The CCNP Data Center is another of the Professional certifications that have been updated. This certification is for anyone interested in a career in Datacenter solutions.

There are two exam requirements that must be passed to obtain the new CCNP Data Center certification.

The certification is valid for three years before recertification is required.

This course will still be an available option in the February 2020 course restructuring. However, the current course and exams will be replaced by newer versions. The new CCNP Data Center certification will be available from the 23 February 2020.

CCNP Security

The CCNP Security course has been updated to include programmability and automation. It is a specialist certification that is highly valued by organizations as systems security is of great concern in today's world.

There are two exam requirements that must be passed to obtain the new CCNP Security certification. To obtain the CCNP Security certification the core exam has to be passed followed by one elective exam chosen from the following six exams:

- SSNGFW — Securing Network with Cisco Firepower Next-Generation Firewall and the SSFIPS — Securing Networks with Cisco Firepower Next-Generation IPS
- SISE — Implementing and Configuring Cisco Identity Services Engine
- SESA — Securing Email with Cisco Email Security Appliance
- SWSA — Securing the Web with Cisco Web Security Appliance
- SVPN — Implementing Secure Solutions with Virtual Private Networks
- SAUI — Implementing Automation for Cisco Security Solutions

The certification is valid for three years before recertification is required.

This course will still be an available option in the February 2020 course

restructuring. However, the current course and exams will be replaced by newer versions. The new CCNP Security Center certification will be available from the 23 February 2020.

CCNP Service Provider

The CCNP Service Provider course is for anyone who is currently involved with working with service provider technologies or who is interested in pursuing a career along this path. The CCNP Service Provider certification has been updated to include programmability and automation which help in providing scalable infrastructures.

There are two exam requirements that must be passed to obtain the new CCNP Service Provider certification. To obtain the CCNP Security certification the core exam has to be passed followed by one elective exam chosen from the following three exams:

- SPRI — Implementing Cisco Service Provider Advanced Routing Solutions
- SVPI — Implementing Cisco Service Provider VPN Services
- SPAUI — Implementing Automation for Cisco Service Provider Solutions

The certification is valid for three years before recertification is required.

This course will still be an available option in the February 2020 course restructuring. However, the current course and exams will be replaced by newer versions. The new CCNP Service Provider certification will be available from 23 February 2020.

DevNet Professional

The DevNet Professional certification is a specialist certification designed to provide the professional with the skills required to develop an application on a Cisco platform. They will also acquire the skills needed to maintain those applications and upgrade them through continuous improvement.

There are two exam requirements that must be passed to obtain the new DevNet Professional certification. To obtain the DevNet Professional certification the core exam has to be passed followed by one elective exam chosen from the following six exams:

- CLAUI — Implementing Cisco Automation for Cisco

Collaboration Solutions

- DCAUI — Implementing Cisco Data Center Solutions
- SPAUI — Implementing Automation for Cisco Service Provider Solutions
- SAUI — Implementing Automation for Cisco Security Solutions
- DEVOPS — Implementing DevOps Solutions and Practices using Cisco Platforms
- DEVIOT — Developing Solutions using Cisco IoT and Edge Platforms
- DEVWBX — Developing Applications for Cisco Webex and Webex Devices

The certification is valid for three years before recertification is required.

The new DevOps Professional certification will be available from the 23 February 2020.

Expert Level

The Cisco expert-level certifications can be very demanding and most of them will have a written exam and then a practical lab exam that needs to be passed in order to become certified.

CCDE — Cisco Certified Design Expert

This certification is for network professionals wanting to expand their career to network design or for those already working in networking design that wants to validate their skills.

There are two exam requirements that must be passed to obtain the new CCDE certification. To obtain the CCDE certification the individual will have to pass the core written exam first before they can take the 8-hour CCDE Practical exam.

The certification is valid for two years before recertification is required.

The new CCDE certification will be available from the 23 February 2020.

CCIE Enterprise Infrastructure

This certification is for network professionals wanting to expand their networking skills by learning about the more complex enterprise

infrastructure environments. It is also for those that may already be working with enterprise infrastructure that would like to validate their skills with a CCIE certification. This certificate is the next level up for individuals that have taken the CCNP Enterprise Infrastructure certification.

There are two exam requirements that must be passed to obtain the new CCIE Enterprise Infrastructure certification. To obtain this certification the individual will have to pass the core written exam to qualify for the 8-hour lab exam.

The certification is valid for two years before recertification is required.

The new CCIE Enterprise Infrastructure certification will be available from the 23 February 2020.

CCIE Wireless Certification Program

This certification is for network professionals wanting to expand their networking skills by learning about the more complex enterprise wireless environments. It is also for those that may already be working with enterprise wireless that would like to validate their skills with a CCIE certification.

There are two exam requirements that must be passed to obtain the new CCIE Enterprise Wireless certification. To obtain this certification the individual will have to pass the core written exam to qualify for the 8-hour lab exam.

The certification is valid for two years before recertification is required.

The new CCIE Enterprise Wireless certification will be available from the 23 February 2020.

CCIE Collaboration Certificate

This certification is for network professionals wanting to expand their networking skills by learning about the more complex collaboration technologies. It is also for those that may already be working with collaboration technologies that would like to validate their skills with a CCIE certification. This certification is also the next level for those that hold the CCNP Collaboration certificate.

There are two exam requirements that must be passed to obtain the new CCIE Collaboration certification. To obtain this certification the individual will have to pass the core written exam to qualify for the 8-hour lab exam.

The certification is valid for two years before recertification is required.

The new CCIE Collaboration certification will be available from the 23 February 2020.

CCIE Data Center Certificate

This certification is for network professionals wanting to expand their networking skills by learning about the more complex data center solutions. This is the next level certificate for the holders of the CCNP Data certificate.

There are two exam requirements that must be passed to obtain the new CCIE Data Center certification. To obtain this certification the individual will have to pass the core written exam to qualify for the 8-hour lab exam.

The certification is valid for two years before recertification is required.

The new CCIE Data Center certification will be available from the 23 February 2020.

CCIE Security Certificate

This certification is for network professionals interested in systems security or those wanting to validate their system's security skills by earning a CCIE certification. This is also the next level certification path for current holders of the CCNP Security certificate.

There are two exam requirements that must be passed to obtain the new CCIE Security certification. To obtain this certification the individual will have to pass the core written exam to qualify for the 8-hour lab exam.

The certification is valid for two years before recertification is required.

The new CCIE Security certification will be available from the 23 February 2020.

CCIE Service Provider

This certification is for network professionals interested in learning about complex solutions designed around service providers. It is also for those that may already be working with service providers that would like to validate their skills with a CCIE certification. It is the next logical step in the certification path for current holders of the CCNP Service Provider certification

There are two exam requirements that must be passed to obtain the new CCIE Service Provider certification. To obtain this certification the individual will have to pass the core written exam to qualify for the 8-hour lab exam.

The certification is valid for two years before recertification is required.

The new CCIE Service Provider certification will be available from the 23 February 2020.

Architect Level

This is the highest level of certification in the Cisco certification path. Professionals who hold an Architect level of certification have had years of experience as an IT professional and would have had to pass rigorous testing in order to prove their skills.

CCAr — Cisco Certified Architect

This is the highest level of Cisco certifications and is designed for the more senior networking infrastructure architect with years of experience designing complex network structures. At this level, the professional learns how to translate the business needs into a successful networking infrastructure that adds value to an organization.

The CCAr exam is a board exam whereby candidates have to submit their credentials, which have to include their working experience and various qualifications they have. The applicant will then be interviewed by the ‘Cisco-designated Architecture Board’ team members. There are very strict rules and regulations as to what a candidate may and may not submit within their experience and qualifications applications. For instance, they will not be permitted to submit any information about any classified projects they may have worked on.

When the applicant has been vetted and approved by the ‘Cisco-designated Architecture Board’, they will be assigned a project in the form of an architectural challenge. At the final stage, they will once again meet with the board and answer questions about their assigned challenge.

The certification is valid for five years before recertification is required.

The new CCAr certification will be available from the 23 February 2020.

Chapter 3: The New CCNA Certification

The CCNA certification opens up new doors for IT professionals interested in a career in IT technologies. By earning the CCNA Certification, it validates your skills and shows a commitment to your chosen career path. It is also the first step towards climbing higher up the Cisco certification ladder. As the foundation certificate, it introduces the individual to the different certification paths available from Cisco.

Cisco has recently redesigned its Associated level course structure to give IT professionals a broader spectrum based on all the latest networking technologies, IT job roles, and software development. The certification has been revamped to include a broader range of IT Fundamentals in one course instead of having to take a few courses. This also means only one exam is required to achieve the CCNA certifications.

The new CCNA certification now includes automation, programmability, and security at the Associate level, giving the candidate all the tools they need to succeed in a Cisco associate level role.

Why CCNA?

The CCNA not only validates the networking professionals' skills, but it also gives them the confidence to install, configure, manage, and maintain a network of average size. The new CCNA certification covers a broader scope of networking fundamentals including that of networking security, automation, and network programmability.

Benefits of the CCNA Certification

- Successful completion of the CCNA certification shows prospective or current employees that the individual is serious about their career and future.
- The course covers networking, automation, and security technology areas which is the basis for every entry-level to mid-level networking professional.
- CCNA certification is a globally accepted certification.
- CCNA certified professionals demand higher-paying jobs than those

without a CCNA in the same position.

- CCNA is a highly sought after job around the world and the demand for certified professionals is growing all the time.
- A CCNA certification increases a person's chance at promotion or salary increase for those currently employed in a networking position.
- The CCNA certification gets you set along the path to higher Cisco certification a lot easier.
- The CCNA certification is accredited by one of the largest globally recognized corporations.

Topics Included in the New CCNA Certification

The new CCNA certification course and exam includes the following topics:

Automation and Programmability

Cisco's "intent-based networking" gives IT professionals a faster and more efficient way to manage and deploy networking devices with the use of Applications Programming Interfaces (API). APIs enable the collection of valuable data as well as the power to automate various networking operations. The new CCNA certification introduces the fundamentals of software-defined networking, automation, and network programmability. This section will cover REST APIs, Puppet, Chef, JSON, and SDN.

Network Fundamentals

Network fundamentals include the following topics:

- Network topologies
- Network infrastructure
- Cabling
- OSI
- TCP/IP and TCP/UDP
- Firewalls
- Access Points
- Routers
- Cloud resources

Network Access

Install, configure, and manage switches, routers, and wireless LAN devices at

an associate level. There is also a section that covers VLAN, trunking, and EtherChannel.

IP Connectivity and Services

IP connectivity covers the basics of how to operate, verify, configure, and install IPv4 and IPv6. IP routing and OSPFv2.

Security Fundamentals

This will cover VPNs, port security, and wireless security.

The Course Specifics

The new CCNA course has three training options available to it:

Classroom Instructor-Led Plus Self-Study

With this option the individual will spend five days in an instructor-led classroom environment and will have three days of self-study to complete the course.

Virtual Classroom Instructor-Led Plus Self-Study

With this option the individual will have five days studying in a virtual classroom environment which is instructor-led. After five days, the individual will have to complete the course with three days of self-study.

E-Learning

The individual that opts for the E-learning course is responsible for their own learning which will be equivalent to 8 days of the instructor-led course.

CCNA Candidates

The new CCNA certification has been designed for individuals who are interested in pursuing a career in networking technology. It is beneficial to those already working in a network environment, specifically one that uses Cisco equipment.

The course would benefit the following individuals:

- Network engineers at the entry-level of their careers

- Help desk administrators
- Network administrators
- Network support engineers
- Individuals with a basic knowledge of networking

New CCNA Certification Prerequisites

Although the CCNA certification has no formal prerequisites, the learner should have a basic understanding of the topics that are included in the CCNA certification course.

Most learners that take the CCNA certification will also have:

- At least one year's experience in a Cisco networking environment as an administrator or support engineer.
- The candidate should also have a basic knowledge and understanding of IP addressing
- They should be knowledgeable about and have a good understanding of the basic networking fundamentals and protocols.

Chapter 4: The New Cisco Certified Network

Associate (CCNA) Course

The new CCNA certification recommended study material is *Implementing and Administering Cisco Solutions (CCNA) v1.0*. This is the course material that will be given to any candidates that enroll for the CCNA certification after the 23 February 2020.

The course is a combination of lectures, self-study, and a bit of hands-on experience in a lab environment. The candidates will learn about basic networking devices such as switches, routers, wireless LAN's and how they work.

Candidates will learn how to configure, install, troubleshoot, and manage these devices as well as touch on the basics of identifying various security threats. With the revamp on the CCNA course, Cisco has included a section that covers software-defined networking, network programmability, and automation.

The Course Outline

As previously stated, this course has some instructor-led classroom study as well as self-study sections.

Instructor-Led Course Outline

Instructor-led classrooms will either be:

- Classroom-based courses will have an instructor per class
- For virtual classrooms, the study is a live instructor-led real-time class that takes place in a video conferencing format.
- E-learning students will receive their lectures as pre-recorded videos.

Lectures Include the Following Topics:

- How to implement VLANs and trunks.

- The routing between VLANs.
- An introduction to the Open Shortest Path First (OSPF) routing protocol.
- How to use EtherChannel to improve upon redundant switched topologies.
- Introduction to Access Control Lists (ACL).
- Internet connectivity enabling.
- Introduction to the evolution of intelligent networks.
- Introduction to systems monitoring.
- How to manage Cisco devices.
- How to secure the administrative access to Cisco devices.
- How to implement device hardening.

Self-Study Course Outline

For the self-study portion of the course, candidates will be required to do their own reading and study of the topics marked for self-study purposes.

Self-study

- Course material provided with the CCNA certification course.
- Pre-recorded videos.

Self-study Includes the Following Topics:

- How to build redundant switched topologies.
- Learn about layer 3 redundancy.
- Learn about the fundamentals of WAN technologies.
- Learn about Quality of Service (QoS).
- Learn about the fundamentals of Wireless technology.
- Learn the basics of networking architecture and virtualization.
- Overview of the security threat landscapes.
- Learn how to implement a threat defense environment.

Lab Course Outline

This is the section of the course where the learner gets to have hands-on experience and interact with the various devices they are learning about.

Lab Environment:

- In a classroom-based course, the learner will be given access to the device they are working on.
- For virtual classroom study, the learner will be expected to have access to a device in order to partake in the lecture.
- E-learning students will be expected to have access to a device in order to get the hands-on experience they will need to further their course studies.

Lab Environment Will Cover the Following:

- Learn to use the Cisco Command-Line Interface (CLI).
- Learn how a switch works (observation).
- Learn how to do a basic switch configuration and implement the initial configuration.
- Learn how to inspect TCP/IP applications.
- Learn how to configure a Cisco router interface.
- Learn about layer 2 discovery protocols as well as how to identify and configure them.
- Learn how to configure and implement an initial router configuration.
- Learn how to configure a system gateway.
- Learn about packet forwarding by observations.
- Learn to identify and deal with various port issues and switch media problems (troubleshooting exercise).
- Learn to identify and deal with port duplex problems (troubleshooting exercise).
- Learn how to configure IPv6 connectivity.
- Learn about the static routes of IPv4 as well as how to configure and verify them.
- Learn about the static routes of IPv6 and how to configure them.
- Learn how to implement static routing for IPv4.
- Learn how to implement static routing for IPv6.
- Learn the basic configuration for VLANs and Trunks.
- Learn how to troubleshoot Trunks and VLANs.
- Learn about configuring a router on a stick.
- The learner will get to implement multiple VLANs.
- The learner will get to implement basic routing between the VLANs they implement.

- Learn how to configure a single-area OSPF and verify it.
- Learn how to configure an EtherChannel and verify it.
- Learn how to use EtherChannel to improve redundant switched topologies.
- Learn how to configure IPv4 ACLs and verify them.
- Learn how to implement named IPv4 ACLs.
- Learn how to implement numbered IPv4 ACLs.
- Learn how to successfully configure an IPv4 address that is provider-assigned.
- Learn how to successfully configure static Network Address Translation (NAT).
- Learn how to successfully configure dynamic NAT.
- Learn how to successfully configure Port Address Translation (PAT).
- Learn how to successfully implement PAT.
- Learn how to access and login to the Wireless LAN Controller (WLC).
- Learn how to monitor WLC.
- Learn how to successfully configure a Dynamic Interface (VLAN).
- Learn how to successfully configure a Dynamic Host Configuration Protocol (DHCP) Scope.
- Learn how to successfully configure a WLAN.
- Learn about and how to define a Remote Access Dial-In User Service (RADIUS) Server.
- The learner will get an introduction to the management options and get the chance to explore them.
- The learner will get an introduction to the Cisco Digital Network Architecture (DNA) Center.
- The learner will learn about the Network Time Protocol (NTP) as well as how to configure and verify it.
- The learner will learn about the System Message Logging system and how to configure it.
- The learner will be taught about and how to create a Cisco IOS Image Backup.
- The learner will learn how to upgrade the Cisco IOS Image.
- The learner will learn how to use Wi-Fi Protected Access 2 (WPA2) Pre-Shared Key (PSK) to configure a WLAN using the graphical user interface (GUI).
- Learn about Secure Console.

- Learn about Remote Access.
- Learn about and how to enable as well as limit remote access connectivity to a network.
- Learn about secure device administrative access
- Learn about and how to configure port security and verify it.
- Learn about and how to implement device hardening.

Course Objectives

Upon completion of the course, whether a candidate has done a classroom-based, virtual classroom-based, or E-learning CCNA, the candidate should be ready to write the CCNA exam.

Once the candidate has completed the course they should be able to:

- The student will be able to recognize computer network components.
- The student will be able to describe the basic characteristics of those network components.
- The student will have an understanding of a host-to-host communication model.
- The student will be able to confidently list the functions and features of the Cisco Internetwork Operating System (IOS) software.
- The student will be confident in their ability to discuss what a LAN is.
- The student knows what function switches within a LAN.
- The student will be able to discuss what the purpose of a switch is.
- The student will be able to discuss TCP/IP and ethernet as the protocols network access layer.
- The student will be able to install a switch and perform the initial configuration
- The student will be able to discuss the TCP/IP Internet layer protocol.
- The student will be able to discuss the IPv4 as well as its addressing scheme.
- The student will be able to discuss subnetting.
- The student will be able to discuss the TCP/IP Application layer.
- The student will be able to discuss the TCP/IP Transport layer.
- The student will comfortably be able to navigate various routing functions.

- The student will be able to commission a basic Cisco router configuration.
- The student will be able to describe host-to-host communications across routers and switches.
- The student will be able to troubleshoot common errors that occur with switched networks and be able to resolve them.
- The student will be able to troubleshoot and resolve common problems related to IPv4 addressing.
- The student will be able to confidently discuss what the main IPv6 features are.
- The student will be able to discuss IPv6 addresses.
- The student will be able to configure basic IPv6 connectivity and verify it.
- The student will have an understanding of static routing.
- The student will be able to discuss what the benefits, limitations, and operations of static routing are.
- The student will have an understanding of Virtual Local Area Networks (VLANs).
- The student will be able to commission a Virtual Local Area Networks (VLANs) and trunks as well as verify them.
- The student will be able to discuss inter-VLAN routing as well as the application and configuration thereof.
- The student will be able to describe the basics of dynamic routing protocols.
- The student will be able to identify the terms and components of Open Shortest Path First (OSPF).
- The student will be able to describe how Spanning Tree Protocol (STP) works.
- The student will be able to explain how the Rapid Spanning Tree Protocol (RSTP) works.
- Using EtherChannel the student will know how to configure link aggregation.
- The student will be able to explain what the purpose of Layer 3 redundancy protocols are.
- The student will be able to explain basic WAN concepts.
- The student will be able to explain basic VPN concepts.
- The student will be able to explain what the operation of Access

Control Lists (ACLs) are.

- The student will be able to explain what ACLs applications in the network are.
- The student will be able to use Dynamic Host Configuration Protocol (DHCP) clients to configure Network Address Translation (NAT) and Internet access on Cisco routers.
- The student will be able to explain what Quality of Service (QoS) is and the basic concepts thereof.
- The student will be able to explain the concepts of wireless networks.
- The student will be able to explain the types of wireless networks that can be built.
- The student will be able to explain how to correctly use Wireless LAN Controllers (WLCs).
- The student will be able to explain network architecture, device architectures, and what virtualization is.
- The student will have an understanding of the network programmability concept as well as what Software-Defined Networking (SDN) is.
- The student will be able to explain what smart network management solutions are. They will be able to demonstrate their basic knowledge by being able to discuss the Software-Defined Access (SD-Access), Cisco DNA Center, and Software-Defined Wide Area Network (SD-WAN).
- The student will be able to do a basic configuration of the IOS system monitoring tools.
- The student will be able to demonstrate their knowledge of the management of Cisco devices.
- The student will be able to explain the current security threat landscape.
- The student will be able to explain what threat defense technologies are.
- The student will have an understanding of the device management plan and be able to deliver a basic security configuration of it.
- The student will understand the concept of systems hardening and be able to take the basic steps to harden network devices.

If a student is confident that they have achieved all the course objectives, they are ready to take the CCNA certification exam.

Chapter 5: 200-301 Cisco Certified Network

Associate (CCNA) Exam

From 23 February 2020, the new CCNA exam will be the 200-301 CCNA certification exam.

Basic Exam Information

The duration of the 200-301 CCNA exam is 120 minutes.

The 200-301 CCNA exam consists of 120 questions.

There are different exam-type questions that make up the 120 questions. These are broken down into the following exam test question categories:

- Multiple-choice single answer questions
- Multiple-choice multiple answer questions
- Drag and Drop answer questions
- Fill-in-the-Blank question tasks
- Testlet questions
- Simulation questions
- Simlet questions

Booking the CCNA Exam

The tests must be done at an authorized Cisco testing center and are hosted by Pearson VUE. Pearson VUE is the test delivery partner for Cisco worldwide.

Once you are ready to book your exam you can go to the Pearson VUE website. The website will help you find a testing center near you.

If there is an available space you can book an exam on the day you would like to take it or you can book your exam in advance.

The Cisco exam must be taken within a year after completing the course.

Cisco Exam Policies

There are a few exam policy requirements that must be met before a person can take any Cisco exams. These can be found on the Cisco website under the “Certification Exam Policies” section.

There are policies about age restriction, candidate identification, the candidate’s rights and responsibilities, the standard confidentiality agreements, privacy statement, and an embargoed country policy statement.

Make sure you have read through these and understand them before booking your exam.

Retaking the CCNA Exam

Should an individual not pass their CCNA exam the first time, they can retake the exam but will have to wait for five calendar days before they can retake the test. The days must be counted from the day after the test was taken.

What the Exam Covers

The exam will test the candidate's knowledge and skill set in the following technological areas:

Network Fundamentals — 20% of the Exam

The exam requires the student to be able to explain the role and function of network components including that of:

- Access points
- Controllers — both Cisco DNA Center and WLC
- Endpoints
- L2 and L3 switches
- Next-generation firewalls and IPS
- Routers
- Servers

Students should also be able to identify the characteristics of network

topology architectures:

- On-premises and cloud
- Small office/home office (SOHO)
- Spine-leaf
- WAN
- 2 tier
- 3 tier

The exam also requires the student be able to compare various cabling types and physical interfaces:

- Concepts of PoE
- Connections (Ethernet shared media and point-to-point)
- Single-mode fiber, multimode fiber, copper

In addition, students should be able to troubleshoot cable and interface issues such as errors, mismatch duplex, collisions, and speed. They should also understand and compare UDP to TCP, configure and verify IPv4 addressing and subnetting, and be able to explain why private IPv4 addressing is needed.

The exam requires the student to be able to configure IPv6 addressing, verify them, and prefix:

- Anycast
- Compare IPv6 address types
- Global unicast
- Link local
- Modified EUI 64
- Multicast
- Unique local

Students should be able to easily verify the IP parameters for a Client OS such as Mac OS, Windows, and Linux.

The exam requires the student be able to explain the concept of wireless principles:

- Encryption
- Nonoverlapping Wi-Fi channels
- RF
- SSID

Learners must be able to discuss the fundamentals of virtualization and virtual machines.

Identify and explain various switching concepts:

- Frame flooding
- Frame switching
- MAC address table
- MAC learning and aging

Network Access — 20% of the Exam

Configure VLANs in the normal range, spanning multiple switches and verify.

- Access ports (data and voice)
- Connectivity
- Default VLAN

Configure interswitch connectivity and verify.

- 802.1Q
- Native VLAN
- Trunk ports

Explain, verify, and configure layer 2 discovery protocols such as LLDP and Cisco Discovery Protocol.

Successfully configure EtherChannel (LACP) (layer 2/layer 3) and verify.

Students must be able to explain what Rapid PVST+ Spanning Tree Protocol, identify basic operations, and what the need for it is.

- PortFast benefits
- Port states (forwarding/blocking)
- Root bridge — primary/secondary, root port, and other port names

Understand the basics of access points (AP) and wireless lan controllers (WLC) to comfortably compare AP Modes and Cisco Wireless.

Learners must be able to confidently explain the physical infrastructure connections of WLAN components such as AP, access/trunk, WLC, and LAG.

Explain AP and WLC management access connections including console,

HTTP, SSH, Telnet, HTTPS, and TACACS+/RADIUS.

The exam requires the student use a GUI such as WLAN creation, advanced WLAN settings, security settings, and QoS profiles to configure the components of a wireless LAN access to enable client connectivity.

IP Connectivity — 25% of the Exam

The learner must know IP well enough to be able to explain routing tables components.

- Administrative distance
- Gateway of last resort
- Metric
- Network mask
- Next hop
- Prefix
- Routing protocol code

Explain the default forwarding decision a router makes.

- Administrative distance
- Longest match
- Routing protocol metric

Learners must be able to verify and configure static routing for IPv4 and IPv6.

- Default route
- Floating static
- Host route
- Network route

Understand Open Shortest Path First version 2 (OSPFv2) in order to confidently work with single area OSPFv2 by configuring and verify the protocol

- Broadcast — DR/BDR selection
- Neighbor adjacency
- Point-to-point
- Router ID

Understand the concept of hops and be able to explain what the purpose of

first hop redundancy protocol is.

IP Services — 10% of the Exam

Using static and pool, the student must be able to configure and verify inside source NAT.

Operating in a client and server node, the student must be able to configure and verify NTP.

The student must be able to explain what the role of DNS and DHCP is within the network.

The student must be able to explain what the function of SNMP in network operations is.

The student must be able to explain what the use of syslog features, including facilities and levels, is.

The student must be able to verify and implement DHCP client and relay.

For QoS, the student must be able to explain the forwarding per-hop behavior (PHB) such as classification, congestion, marking, policing, queuing, and shaping.

Using SSH, the student must be able to configure network devices for remote access.

The student must be able to explain the function as well as the capabilities TFTP/FTP is in the network.

Security Fundamentals — 15% of the Exam

The student must be able to explain what the key security concepts are, for instance, exploits, mitigation techniques, threats, and vulnerabilities.

The student must be able to explain what the elements of a security program are. For instance, physical access control, ness, training, and user awareness.

Using local passwords the student must be able to configure device access control.

The student must be able to explain security password policies. These elements should include password complexity, management, and password alternatives such as biometrics, certifications, and multifactor authentication.

The student must be able to describe site-to-site VPNs and remote access.

The student must know how to verify and configure access control lists (ACLs).

The student will need to know how to configure Layer 2 security features such as dynamic ARP inspection, DHCP snooping, and port security.

The student must be able to differentiate accounting, authorization, and authentication concepts.

The student must be able to explain the various wireless security protocols such as WPA, WPA2, and WPA3.

Using the GUI the student must be able to configure a WLAN using WPA2 PSK.

Automation and Programmability — 10% of the Exam

The student must be able to discuss the impact of automation on network management.

The student must be able to identify traditional networks with controller-based networking.

The student must be able to explain controller-based and software-defined architectures such as fabric, overlay, and underlay.

- North-bound and south-bound APIs
- Separation of control plane and data plane

The student must know the characteristics of REST-based APIs such as CRUD, data encoding and HTTP verbs.

The student must be able to determine the capabilities of configuration management mechanisms Ansible, Chef, and Puppet.

The student must be able to translate JSON encoded data

Chapter 6: 200-301 CCNA - Exam Preparation

For those who have never taken a Cisco exam, you may not know what to expect. It can be quite daunting, especially since an aspiring CCNA is already under pressure knowing how high Cisco sets their bar for passing exams.

If you are doing an instructor-led course, the instructor may not teach the course section by section or chapter by chapter. They will teach what they feel is relevant for that lesson. For e-learning students, you will probably learn on a chapter-by-chapter basis and how the pre-recorded course video instruction guides you.

For the stake of this book, we are going to go chapter-by-chapter learning for the Cisco exam — **200-301 CCNA**.

What to Expect at the Exam Testing Center

The first thing to learn is how the exam is actually given. You won't be sitting in a classroom and given an exam paper. No, this is completely different. You will have to register with a Pearson VUE test, or authorized test center in order to book and write the exam. If you were not paying attention earlier, Pearson VUE is the Cisco partner for their certification exams.

You can find their information from the Cisco CCNA Certification and Training Program Webpage or do an Internet search for Pearson VUE. Both of these website's URLs can be found in the reference section of this book to make your search a little easier.

The Testing Center

Before we continue, it must be noted that this is a general overview of what to expect. Each test center may be a bit different from the other. But the general rules to how the test is given, biometrics, and so on are the same if not similar.

When you are ready to book your exam you will need to find an authorized,

registered testing center near you. This, as stated before, can be done through the Cisco and Pearson VUE websites.

The tests can be booked in advance, or pending availability, on the day you want to write the test. If you are not a native English speaker you need to let the institute know on the day you book the exam as, depending on the exam policy, they usually allow extra exam time when taking it in English. Please check with the institute you book with for the most updated information and policies on this.

Make sure you arrive on time, but if for some reason you cannot make the exam, make sure you cancel it on time. Always check the cancellation and rebooking policies. If you cannot find the information on the website, call and ask. You are paying for the exam, after all, and you are entitled to know all the details.

Upon arrival at the test center, you will be asked to sign in and have your picture taken. You will have to sign an exam form, as well as drop off all your personal belongings such as phones, wallets, bags, keys, and so on. These will be put into a secured lockbox for your retrieval once the exam has been completed.

The Exam Room

Unless otherwise arranged for whatever reason, no food or drinks are allowed in the exam room. You may have water outside before you enter the room.

The exam is what they call ‘proctored’ which basically means that you are being watched while writing the exams on a CCTV camera that is positioned in the room.

The rooms usually consist of a desk, chair, and PC which will have been pre-loaded with your exam as well as all your personal details. So, it is important to ensure that these are correct when you book the exam and it is best to check again when you are at the test center to make sure.

You will be given 2 to 3 pieces of paper and a pen before you enter the room or it may already be set up in there for you. The paper may be laminated and the pen may also be a non-permanent marker. This is great because you can clear it as you go and don’t run out of paper halfway through the exam.

When you start the exam simulator the first ten to fifteen minutes (more or less) is an introduction to how the test works. Pay attention if you did not go onto the Cisco website to find out how the questions work. If you already know how they work, spend the time jotting down information you want to keep fresh in your mind for quick reference.

At the end of the exams, you will have to sign out, collect your things, and you will be given a print out of your test score. You find out if you passed or not as soon as you have finished and the exam simulator has tallied up your marks.

The pass mark for the CCNA exam is 85%. If you did not pass it you can write the test again five days after the day you failed. The print out you will receive with your exam scores on it will show you all the answers you got wrong or right. If you do need to re-write the test, take those five days to study and ensure you go over the points you did not get right.

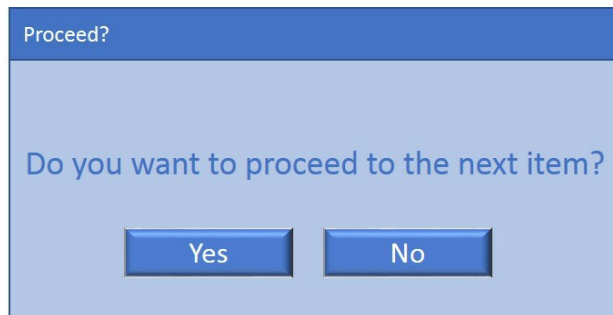
The Exam Format

The exam is 120 minutes and there are 120 questions. Each question must be answered before the simulation will allow you to continue on to the next one. Make sure you read the question carefully and have understood it.

The time remaining for the exam is usually located on the top right-hand side of the computer screen. The next button will be located on the bottom left-hand side of the computer screen with the questions in their relative format in the middle of the screen.

Move the mouse to position and click where you want to either select a radio button, checkbox or click on an empty box to start typing. The mouse works in the same way as it normally does for drag and drop; position the mouse over the item to be selected, click and hold to move it into position, and let go.

Once you click on the “Next” button you cannot go back to a previous question. But before you can move on the “Proceed” box will appear for you to confirm that you are happy with your answer. If you click “Yes” at this point you will continue onto the next question, and if you click “No” you will return to the questions.



Should you run into any technical difficulties, feel ill, or need assistance for whatever reason, **jot down where you are on the screen and take the time remaining.** Exit the room and seek someone who can help you. The testing center may even have a panic button in the room for emergencies. Always ask before you go into the testing room what the procedure is for emergencies or technical difficulties.

The test consists of the following question types:

Multiple-choice single answer questions

What color is the sky on a clear day?

- ☐ Green
- ☒ Blue
- ☐ Yellow
- ☐ Orange

For multiple-choice single answer questions there is only one answer. Choose the answer that is the best match for the question. Move the cursor over the radio button and click the mouse to select it. A dot will appear next to the selected answer.

To deselect the answer simply click on another answer and it will move the dot to that answer.

Click the next button to move onto the next question when you are sure you have answered to the best of your knowledge.

Multiple-choice multiple answer questions

What color do clouds appear to be?

- ☒ White
- ☐ Pink
- ☒ Grey
- ☐ Yellow

Multiple-choice multiple answer questions have more than one correct answer. Choose the answers that best match the question. Move the cursor over the checkboxes and click the mouse to select it. A checkmark will appear next to the selected answer.

To deselect the answer simply click on the checkmark and it will be removed.

Click the next button to move onto the next question when you are sure you have answered all the questions to the best of your knowledge.

Drag and Drop answer questions

Drag each item listed on the left to its proper category on the right.
Not all items will fit the categories.

Drag each item listed on the left to its proper category on the right.
Not all items will fit the categories.

Drag the correct answers and drop them on correct box.

Drag each item listed on the left to its proper category on the right.
Not all items will fit the categories.

Drag and drop answer questions have more than one correct answer. Choose the answer that best matches the question by choosing one answer at a time. Point to the answer on the left and then drag to the correct corresponding box on the right.

Not all the answers are going to fit into the boxes; there may be one or two

leftovers.

To remove or move an answer simply pick it up and either move it to the left or into the next box.

Click the next button to move onto the next question when you are sure you have answered all the questions to the best of your knowledge.

Fill-in-the-Blank question tasks

What color is the sky during the night and during the day?

Day

Night

Cursor positioned to type

Type the answer into the correct box.

What color is the sky during the night and during the day?

Day	Blue
Night	Black

Fill-in-the-box answer questions have more than one correct answer. They are not multiple-choice questions and require you to type in the correct answer into the corresponding boxes. Click in the box and when you see the flashing cursor, you can start to type.

To delete the answer simply click back in the box and either backspace or delete what is typed in there.

Click the next button to move onto the next question when you are sure you have answered all the questions to the best of your knowledge.

Testlet questions

Time Remaining 1:00:04

This is a "Testlet" – it contains 4 questions that relate to the scenario below

Scenario

An employee is having problems connection to the company network. The helpdesk is called to help solve the problem. After a series of questions the helpdesk has the employee ping the gateway which is 192.168.0.1. The following is reported:
Pinging 192.168.0.1 with 32 bytes of data: Request timed out.

Of the choices below, what is the only certain conclusion that can be drawn

Question #1

☐ There is a cable problem
☐ The network card is faulty
☐ There is a configuration problem
☐ The TCP/IP Stack is installed on the laptop

1

2

3

4

Next (N)

Testlet questions can be a little bit confusing as they are scenario-based questions that have more than one question linked to the scenario. The screen is split into two sections; the top is the scenario and the bottom half is the question as well as answer selection screen.

Scenario — this is the description of the scenario. Read it carefully and make sure you understand it. On the right-hand side of the scenario pane is a scroll bar. Be sure to scroll down as there may be a bit more to the scenario. The scenario screen will stay the same and does not change when you flip through the questions on the bottom.

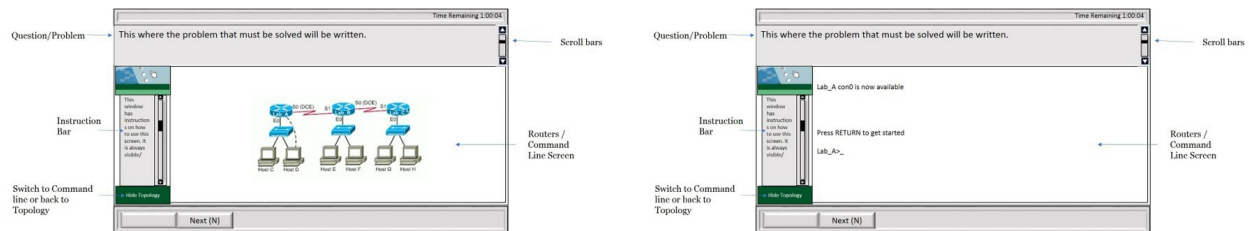
Question — The top section of the question screen will contain the question to be answered. On the right of the question screen you will see numbers down the right-hand side of the screen. These are the number of questions that must be answered for this scenario. Make sure you answer all the questions or you will not be able to move on to the next questions.

Answers — the answers are below the questions and they are in the form of either multiple-choice single answers or multiple-choice multiple answers. The way to answer these questions works the same was as they do as per the above information regarding multiple-choice single or multiple answers.

Click the next button to move onto the next question when you are sure you have answered all the questions to the best of your knowledge.

<https://t.me/learningnets>

Simulation questions



The simulation questions are questions on the function of routers. It must be noted that the functions on these simulations may not match those of an actual router environment. All the commands that are available for each task can be used to complete the task. The commands are available from privileged mode.

Problem/Questions — this can be found in the top pane of the simulation questions. Make sure you use the scroll bar on the right-hand side of the screen to ensure you have read the entire problem/questions.

Instruction Box — this can be found on the right-hand side of the screen below the question/problem box and it will always be visible. It too has a scroll bar, so make sure you have scrolled through the entire box of instructions as this will tell you how to perform or answer each problem/question.

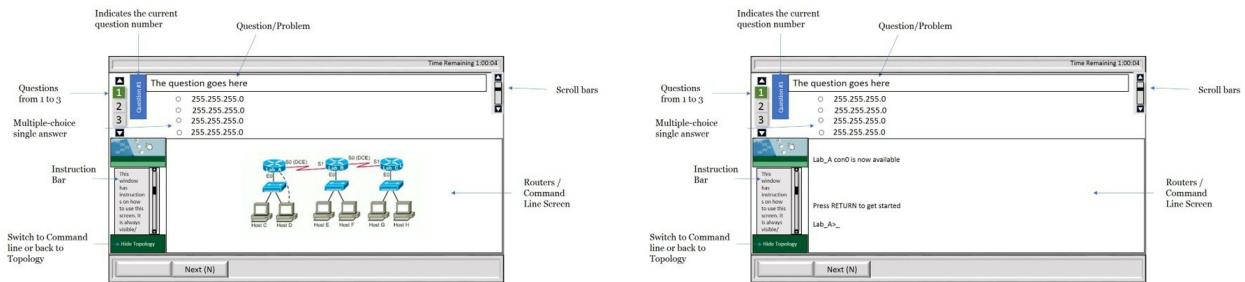
Router Topology/Command line — this button is located beneath the help box and switches you between the topology and command-line screen.

Console — this is the screen in the middle that has a graphical representation of the router topology on it. This screen will also switch to a command-line screen in order to carry out the task you have been assigned to do.

The router that will need to be worked on will show a dotted line to it which indicates a workstation with a console cable attached to it. To start configuring the router you will need to click on the computer with the dotted line running to it.

Click the next button to move onto the next question when you are sure you have answered to the best of your knowledge.

Simlet questions



The simlet questions are questions on the function of routers. Once again, as per the simulation type questions, it must be noted that the functions on these simlets may not match those of an actual router environment. As per the simulation question, all the commands that are available for each task can be used to complete the task; the commands are available from privileged mode.

The simlet is a mishmash of the multiple-choice single question questions, the Testlet questions, and the simulations questions. All the screens and functions in each section work the same way as they do for those question types mentioned above.

Problem/Questions — this can be found in the top pane of the simulation questions. Make sure you use the scroll bar on the right-hand side of the screen to ensure you have read the entire problem/questions.

There are one to three different problems/questions. You will need to scroll through the question bar and the left-hand side of the question box. Either use button 1, 2, or 3 or you can also scroll between the questions using the up and down arrows above and below the numbered question box.

Instruction Box — this can be found on the right-hand side of the screen below the numbered question box and it will always be visible. It too has a scroll bar, so make sure you have scrolled through the entire box of instructions as this will tell you how to perform or answer each problem/question.

Router Topology/Command line — this button is located beneath the help box and switches you between the topology and command-line screen.

Console — this is the screen in the middle that has a graphical representation of the router topology on it. It functions in the same way as the simulation questions console screen does.

Click the next button to move onto the next question when you are sure you have answered to the best of your knowledge.

Preparing for the Exams

It may sound a bit like eating dessert before the main meal, but the first step you should take once you have received your course material is to start exam preparations. Set yourself a learning schedule, starting with going over what you have learned in your classroom, virtual classroom, or e-learning schedule that day. Even if you go over your notes or apply what you have learned in a simulated environment, it will help you when you start to study for the exam.

Network Simulators for the CCNA

While you are doing a Cisco certification you will be training in a lab-type environment. In fact, some of the higher-level certifications actually have an 8-hour lab exam the student has to complete.

The CCNA does not have a lab exam as such, but as you have seen in the section above it does have lab type simulated questions. You will also do some of your training for the CCNA in a lab-type environment where you have to configure, troubleshoot, and so on various devices.

It stands to reason that you are going to need a lab-type environment to work on when you are studying or going over your day's training. No one expects you to have your own Cisco set up and you are not really going to want to practice on systems at your work. But what you can do is get a network simulator.

A network simulator is a piece of software that simulates a network environment. These are great for you to practice on. There are also a number of great simulators out there for you to choose from. Some of them you will have to pay for, but Cisco Packet Tracer is free with enrollment.

- Cisco Packet Tracer
- Cisco Virtual Internet Routing Lab
- Boson NetSim 12 Networking Simulator
- GN3 Networking Simulator
- Pearson VUE also has simulators that can you purchase once you have registered on their website.

Cisco Learning Network

It is very beneficial to join the Cisco Learning Network. Here you will join forums that can help you with your studies and the CCNA in general. There is a lot of handy advice, podcasts, certification training, and various webinars to join.

It is free to join and is a great resource to help you pass your exams as it also has a lot of discussions and interesting blogs all designed to help you with your CCNA certification.

Pearson Test Prep

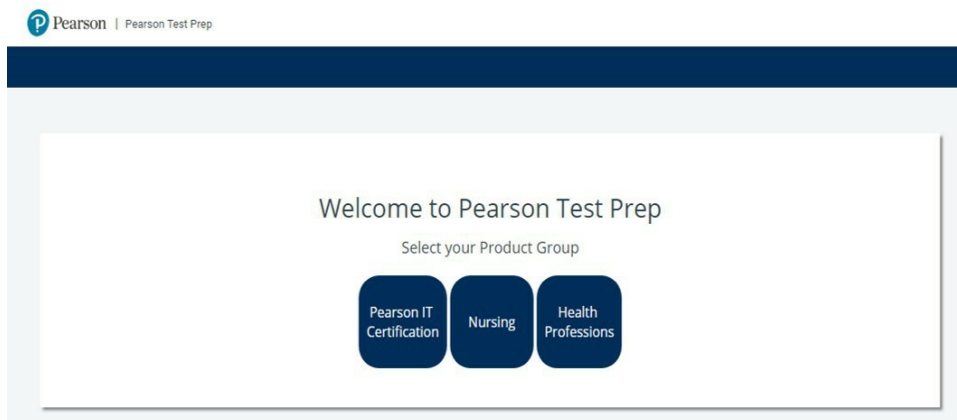
Pearson VUE is a website where you can book your exams, and it also offers test preparation. This includes simulators and exam questions that can be bought when you register for your exams or separately. They are a little cheaper if you buy them with your exam booking though.

Every product you buy on the Pearson Test Prep (PTP) website gives you access to exam questions for that product and these are extremely helpful while you are studying. Usually, when you buy Cisco course materials you get access to some exam questions or simulations that are designed around the actual CCNA exam which help test your knowledge and prepare you for the type of questions you will come across in the actual exam.

As soon as you have your Cisco course material you should register with PTP as you may receive discounts or test questions with the course materials. The nice thing about PTP is that you can opt to use the exam database in either practice exam mode or study mode. The PTP also enables you to go over the DIKTA questions each night to help you with your daily course review in study mode.

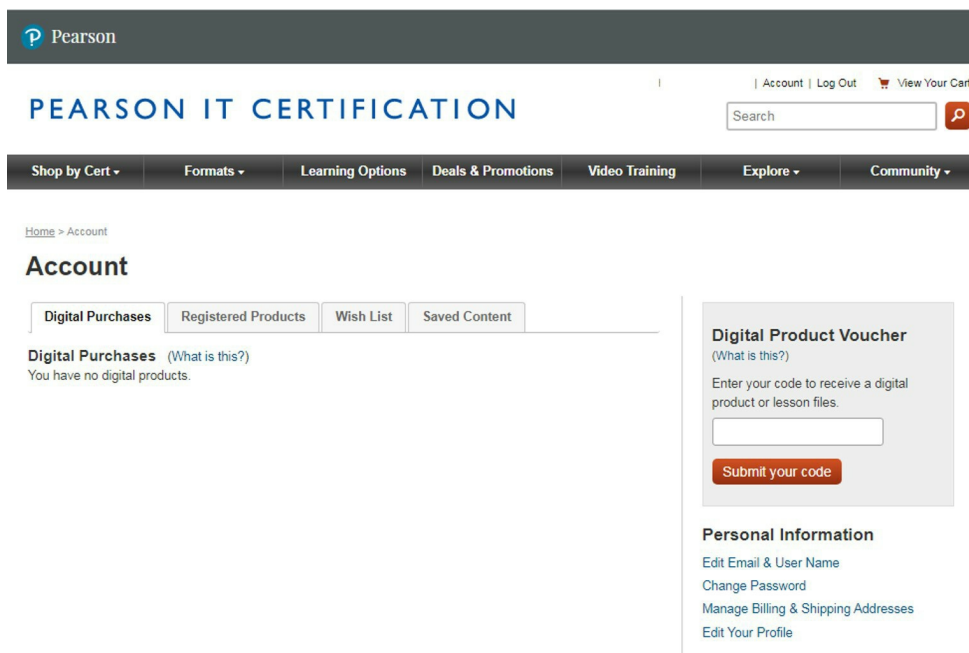
Take a bit of time to find your way around the PTP site and understand how it works, as it is a very valuable tool to help you with your study for the 200-301 CCNA exam.

The Pearson Test Prep Website (you can find the link in the references page) is where you will find a host of CCNA test questions and simulated exams to help you test your knowledge.



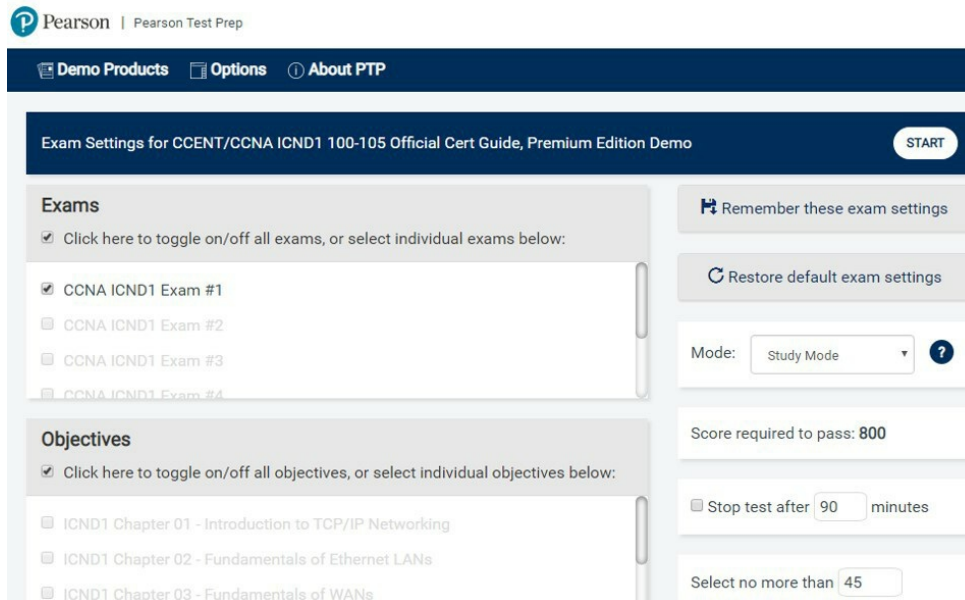
All you have to do is register on their site and get logged in. It is quick, simple, and free.

Once you are logged in you will be able to choose the course you are studying for and you will get a list of the available study materials, simulations, and test questions.



In the search bar, either type in the course number or just CCNA. This will bring up a list of what they have to offer for the chosen Cisco course. It should also be noted that when you log in again once you have chosen your course, the screen will be different. In the menu bar, you will see My Products, Options, Tools, and Help. The screen will default to My Products where there will be a list of the products you have used or bought. The Options menu is where you can set your screen preferences to make your test

prep easier for you. The Tools menu has some handy resources to activate any product you may have bought, reset your exam data, or learn about more exam resources. When you click on the resource you will be able to review any of the test exams you have done, you will get a PDF booklet of course questions, and a test simulator to practice tests on. Read all the instructions on how to use your test questions and simulators in the very helpful help files.



Pearson's Test Prep has a list of very good networking simulators to help you practice your lab work.

Simulators

Cisco & CompTIA

Gain hands-on experience without having to invest heavily in hardware or software

The state-of-the-art, interactive Simulator Series from Pearson IT Certification—a leader in IT Certification learning—are the most effective simulators for hands-on skills enhancement for the exam and workplace. These simulators are the perfect learning product to help you prepare for performance-based questions, which require exam candidates to perform a task or solve a problem within a simulated IT environment, demonstrating specific knowledge or skills.

Watch Sample Videos

CCNA Routing and Switching 200-125 Network Simulator
By Sean Wilkins, Wendell Odom
DVD \$119.99

CCNA Routing and Switching 200-125 Network Simulator, Download Version
By Sean Wilkins, Wendell Odom
Software Download \$119.99

CCENT ICND1 100-105 Network Simulator
By Sean Wilkins, Wendell Odom
DVD \$79.99

CCNA Routing and Switching ICND2 200-105 Network Simulator, Download Version
By Sean Wilkins, Wendell Odom
Software Download \$79.99

CCNA Routing and Switching 200-125 Network Simulator, Pearson uCertify Academic Edition Student Access Card
By Sean Wilkins, Wendell Odom
Book \$136.00

CCNA Routing and Switching ICND2 200-105 Network Simulator, Pearson uCertify Academic Edition Student Access Card
By Sean Wilkins, Wendell Odom
Book \$95.00

Exam Study Schedule

During your tour around various test prep sites and simulations, you may come across the term DIKTA. This stands for, “Do I know this already?” These are questions that will help you determine the amount of time you will need to spend on each chapter.

When setting out your exam schedule for the day, mark the sections that you do know. These are the sections that you can leave until the end of the study period to review. Concentrate on the study material that needs your attention.

Going over what you already know must be done, but it should not be a priority when there is so much else to learn. Before the start of each study session, you sort out what you know and what you need to work on.

The Cisco CCNA exam will be very challenging, as you have to learn a lot of concepts and know how to put most if not all of those concepts into practice. You will have to also learn a lot of Cisco device commands that are unique to Cisco. The challenge of the exam comes from many angles.

In order to get through the exams, you will need to have an in-depth understanding of how these concepts and elements work. You will have to be able to successfully predict an outcome and be able to analyze it. There is the lab or simulation part of the exam that will require you to know how to configure various devices in order to get them working correctly on a network.

The most challenging parts of the exam questions are the simulations that only supply a student with part of the answer, and you are expected to figure out the rest. That is why it is so important to have a networking simulation software to practice on.

Your studying should be broken into reading material and network simulation training so you can put into practice what you are learning. Being able to visualize what you are learning also helps you to better understand the information and remember it. Download one and customize it to best suit your needs. It may be best to start off with the Cisco Packet Tracer, as it is free. As you will need to become a member of the Cisco Networking Academy, you will find another great resource that is filled with information to help you with your CCNA certification.

Study Table

CCNA 200-301 Exam Study Table

Course Material	Study Task	DIKTA?	Target Study Date	First Date of Study	Practice Test Results	Need to Work on	Second Date of Study	Practice Test Results 2
Chapter 1	Topic	No	12/06/20	05/06/20	50%	Topic(s)		
Chapter 1	Review Chap.	No	12/06/20	07/06/20				

Make yourself an exam study table and fill it in with a pencil or make one on your computer using Excel or your preferred method. There are even a few exam time table apps you can download on your smart device or for your PC/Laptop.

Whichever method you prefer, set up your exam study table and make sure you make yourself obtainable study goals. If you manage to finish studying before time, don't slack off or take a break. Move your study table up. This way you will have extra study time before you write your exam. Extra study time means more time to review and ensure you know all the key topics.

If you miss a study date, don't get discouraged and instead move your study time around. Always take into account your social activities, home-life commitments, work commitments, and so on. If you can, move some of those commitments that are not too important as you are going to want to prioritize your studying over a big night out. Remember that you can do a big night out anytime, but you want to try your best to pass your CCNA exam the first time around.

The exams cost every time you take them and you are aiming to be able to move up the career ladder with your new certification. So prioritize your life around family, important commitments, and your studies.

Daily Course Review

Each night after your course you should at least review the chapters you have covered and use the "Chapter Review" exercises at the end of each chapter or section. These questions are designed to test how much of the chapter you

have learned and it is a good indication of what you need to prioritize in your studies. These chapter review questions are also good questions to work through while you are studying.

Practice what you have learned on your network simulator even if it is looking up IP addresses. It shows that you have understood the day's topics and are able to use what you have learned. After all, besides wanting to pass the exam, you want to be able to practice what you are learning.

Join the Cisco CCNA Study Group

There are online forums that are listed on the Cisco Learning Network Website, such as the CCNA Study Group. This group will enable you to ask questions and clarify the information you need clarified about the exam and the course material. You get to connect with others doing the CCNA, so you can share your ideas, and maybe even get to help one of your peers.

Keep Updated with the Cisco Certification Podcast

One of the certifications program managers hosts a podcast full of all the latest news about the CCNA exam, the course, and holds various discussions about the exam.

Make Use of the Training Videos and Webinars

The Cisco Learning Network has a whole host of training videos and webinars to help its students through their courses and exams. There are loads of training materials, advice on how to schedule your study for the exams, and what you can expect in the exams.

Chapter 7: Understanding Networks

To take the CCNA you should have a basic understanding of what a network is, the basic concepts, and how it works. Not everyone who takes the CCNA course works in a networking environment so this chapter will go over a few network basics.

Whether you are a seasoned networking pro or a beginner, it never hurts to refresh your memory and get back to the basics. You may be amazed at just how much you have forgotten, and the thing about these exams is that you never know when they are going to sneak in a random question about the very basics.

What is a Network?

Most people who have worked in an office environment, on a PC in the school lab, or even used a mobile device understands the most basic level of what a network is. It is a whole lot of devices that are connected by a common source to gain access to and share various resources.

There are different networking types such as cellular or mobile networks which are communications networks, wireless networks, local area networks, wide area networks, virtual private networks, and many more.

A network is two or more devices that do not need to be of the same device type that is connected together by a common source and can share resources. These computers, depending on rights assignments, can see each other's files, share a printer that is connected to one of the devices, or an access point.

A device can connect to a network through an access point such as a wall port or a wireless access point. They can be connected with radio waves, infrared, cables, satellites, and telephone lines.

There are many different types of devices that can be attached to the network such as computers, printers, mobile devices, and faxes. Other devices include telephones, visualization systems, CCTV cameras, shop floor manufacturing equipment, RF barcode scanners, point of sale systems (POS), and more.

As the world becomes more dependent on technology, most devices these days have a way in which to connect to the network. Being able to connect various machinery to a network helps a company to gather important data from the machinery. This data is free from human error as it is analyzed and processed by the system. This also gives systems more visibility as they have better traceability and more accurate systems audit trails.

For the most part, the CCNA will cover data networks, both physical and cloud-based solutions. It is important to note that all types of networks come in all shapes and sizes according to the needs of the individual or organization. They may all be very different in the way they are set up or what they are used for. No matter their size or differences at their core, networks are defined by their topology, protocol, and architecture.

Understanding Network Architecture

The Network Architecture is the complete plan of how a network is connected. It is depicted by a network diagram that shows the entire organization's networked system is done by location, office, or site. The network diagram will show everything for that particular office or location from the server room, with all its devices, to every single device that connects back to the network devices.

The diagram will go into detail and list datacenters, their access points, what is in the datacenter, and where it connects to. Each office or floor will have a graphical representation of floor/wall ports, computers, printers, machinery, cameras, and so on that are connected to the network.

This is an important document which usually has a few layers to it. The first being the overall picture as stated above, and then another that shows the server room or datacenter in detail. The detail will normally get broken down with a table on one side listing the devices attached to certain patch panel ports, routers, switches, wi-fi devices, etc. It will include components such as cabling, cabinets, UPS devices, backup devices, communication devices, protocol, and it will list the network topologies. The diagram also needs to show how the wireless, remote, and physical connections to the network are made. It will also show the systems software rules, which are also included as part of network architecture.

The network architecture is designed by an experienced systems engineer or infrastructure architect. The network architecture shows all the network layers in their logical and detailed form. It is a complex document that details the entire networking infrastructure and it takes planning, as well as a complete understanding of the organization's needs, to plan a new network infrastructure.

Documenting an existing network architecture is just as complex and needs the collaboration of all those involved in the day to day operations. The network architect would work closely with the team to ensure each part of the diagram is accurate and to scale. This document is not only for system audits but to ensure that any upgrades are done correctly and it can be invaluable as a troubleshooting tool if designed correctly.

Types of Computer Networks

There are around ten or more types of networks, especially if you are going to include telecommunication networks, satellite networks, and so on. But for the sake of this book, we think of networks in terms of data networks. This section gives a brief overview of ten different network types that are in use today.

Local Area Network (LAN)

We will start off with local area networks as they are the type of network that is the most popular and best known of all the network types. They are used by businesses to connect low-voltage devices and computers together in order for the users of the equipment to be able to share information and resources.

LANs can also be connected to wide area networks by means of a router which will also connect them to the Internet. Routers ensure that devices can quickly, efficiently, and safely connect to the wide-area network.

LANs are maintained by in-house IT network engineers or if they are part of a larger corporation they may be managed by a central team located at the organization's data center, or they can have outsourced network management.

Campus Area Network (CAN)

These are networks that are spread across a university campus, K-12 schools, a business park or industrial areas. They are not classed as a local area

network as the network typically spans a few corporate buildings, factories, or classrooms which are located in the same area or not too far apart as to be classed as a WAN. They are designed so the people in these buildings can share information, software, and other resources, much like users of LANs do.

Each building has its own LAN which are networked together through the use of routers and switches to create one campus area network. On university campuses, a CAN is sometimes referred to as ResNet which is short for the residential network. These networks can only be accessed by student housing and campus building or offices.

Campus area networks are usually managed by a single IT Department that would be housed on the campus. This means all network devices, policies, software, and access are managed locally.

The sharing of large data files is a lot faster over a CAN as one of these network types' biggest advantage is the speed.

Personal Area Network (PAN)

This is one of the least complex as well as the smallest of networks. It is usually made up of one router, with Wi-Fi being the most popular device, and a few devices such as PC, laptop, smart devices, and a printer.

At the most, there will be a wireless network access point in order to boost the Wi-Fi router's signal. They are found in most homes, small one or two office businesses that do not need a lot of devices, and small nursery schools.

The devices can be managed by the person who owns the device or their ISP.

Wide Area Network (WAN)

A wide area network is a group of local area networks located in different geographical locations that are connected together by routers. A WAN allows users located in different cities, countries, and even continents to share data and resources.

Because of the sheer scope of a WAN, they are usually managed and supported by more than one IT team positioned anywhere in the world the company has representation. The best example of a WAN that everyone has access to is the Internet, which as everyone basically knows spans the globe. It offers access to various resources that are used by millions of people

worldwide. Facebook would be an example of a shared resource. Now there is cloud-based computing which offers resources like cloud storage solutions. Companies can even host their networking environment through the cloud.

Metropolitan Area Network (MAN)

These are large networks that will span a metropolitan area like a town, city, or campus that may have parts of its campus located in different areas of a city. They are not as big as a WAN but are designed using components and concepts of both LANs and WANs.

These networks are usually managed and maintained by the IT department(s) town that owns them.

Wireless Local Area Network (WLAN)

These networks work similarly to the way a LAN does, only they are used for wireless connectivity to the LAN. Using a Wi-Fi device and wireless access points, a company can offer its employees the convenience of a cable-free connection to the LAN. Most devices today support Wi-Fi access and those that do not can be made to do so with USB modems.

Virtual Private Network (VPN)

A virtual private network is a device that sits between two networks and creates a secure tunnel between them that is encrypted. Devices such as a computer can access the network through the VPN. That device then connects to the network through the tunnel to ensure a safe private connection.

Enterprise Private Network (EPN)

Enterprise private networks are networks that are largely owned by corporations that allow for secure end to end connections to their offices that are located in different geographical areas.

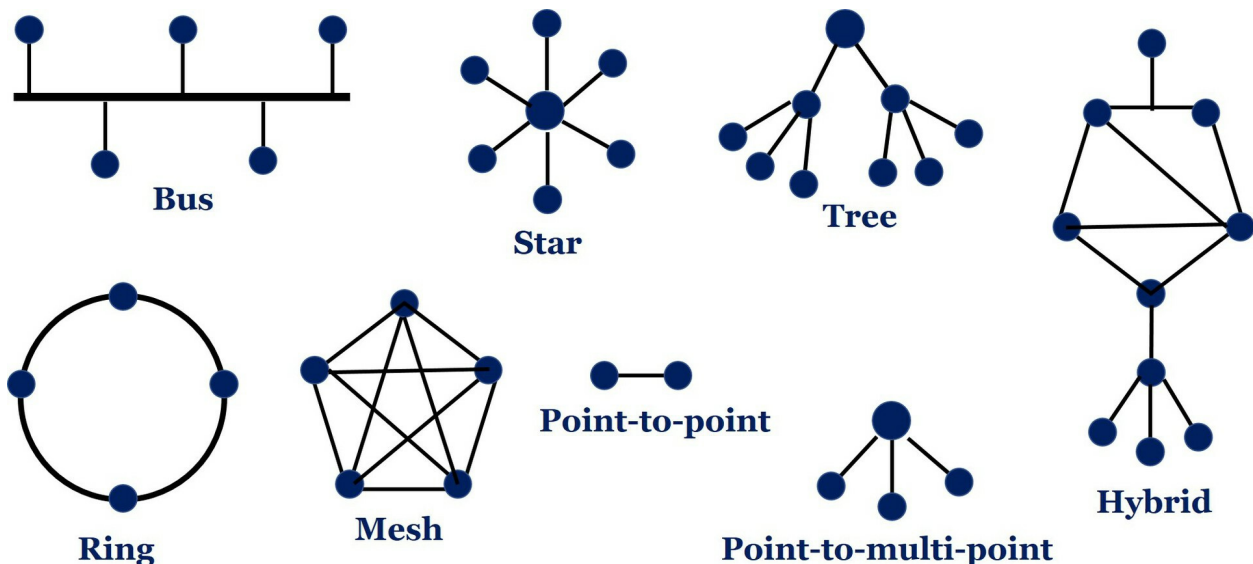
Storage-Area Network (SAN)

There are two types of SANs, so it is important not to get them confused. A storage-area network is a network that connects storage devices such as backup drives to one or more servers. These types of storage devices do not operate across the LAN as they take data from networked devices such as servers to store them on their own network of related storage media. Storage-

Area Networks are like having a series of high-speed external drives to servers in order to backup or archive company data.

The System-Area Network is the second type of SAN network that is used in a cluster environment and is used for server-to-server connectivity at high speeds. They are used to connect storage-area networks as well as processor-to-processor reliant software.

Network Topology



Network topology is the pattern of how network elements are interconnected on a network. A topology may include the physical way a network is connected, how the hardware configuration is mapped, or it could be the route the data takes to travel through the network.

There are numerous types of topologies and some of them can be combined to accommodate a network's unique infrastructure. However, they are not interchangeable as each topology has its own set of standards or rules as they use different hardware methods.

Any device that is connected to a network is known as a node. Nodes can be connected to the network either wirelessly or with a network cable.

Network topology is further broken down into physical and logical topology.

- The physical is the way in which the actual devices, which include computers, cables, and various other peripherals on a network are

connected.

- Logical topology refers to the method by which data or information is passed between the physical devices on the network.

There are eight common types of topologies:

Bus Topology

With the bus topology, all the devices are connected to a single cable or line which is called the backbone. The backbone will have a terminator at each end of the cable or line which dampens the signal and stops it from traveling any further down the line.

When data is sent from computer A to computer D, the information will be transmitted to all the devices along the route but on the device it is intended for it will accept the information. Think of the backbone cable as a bus route and each of the devices attached to it as the bus stops. The data will then be the bus passenger who gets on the bus at the bus stop A. The passenger wants to go to bus stop D so they will travel down the line, stopping at all the stops along the way but only get off at bus stop D, which is the intended destination.

There are linear or distributed bus topologies.

- A linear bus topology means that there is only one line with two termination points.
- A distributed bus topology means that there are two or more linear bus topology patterns on the same network.

The advantages of bus topology are that its simplicity of design makes it easy to install and it is a relatively inexpensive setup.

The disadvantages of bus topology are that there is a single point of failure which means a central line break could bring down the entire network. It is also harder to troubleshoot than most other topologies. There is always the chance of single loss, and it has slower transmission speeds.

Bus topology is not used in today's network environments but it used to be one of the most used and the first option network engineers would choose. When the thicker coaxial cable was used for the backbone a hole would be drilled into the coax cable in order to install a vampire tap to connect devices over a 10BASE-T LAN. A BNC (T) connector would be the port to which a

device would attach to the network. LAN cards would come with a BNC plug on them. When twisted pair started to become popular LAN cards for devices would have both 10BASE-T and RJ45 connectivity capabilities.

Star Topology

Star topology is one of the most popular or common of the network topologies, and most modern-day networks have some variant of the star topology. With the star topology, each device is connected directly to a central device which is either a switch or a hub. Depending on the type of network, the device connects to the central device by means of a twisted pair (UTP) cable with an RJ-45 jack on either side of it. Wireless networks also use star topology to connect to a wireless network.

It is called star topology as it is visually represented with the central gateway device in the middle and the devices that attach to it branching out around the center point. It can also be referred to as a star network.

The advantage of star topology is that it is easy to install as it has a relatively simple design. It is easy to troubleshoot because each device connects to the network through a separate dedicated cable. When one goes down, it will not affect the other devices. Moving devices around the office is a lot easier to do than with most other topologies.

The disadvantage of star topology is that if the central device goes down, the entire network or network node supported by that device goes down with it. There is a need for more cabling and the cabling it uses is prone to cable breaks. Star topology can be quite expensive to set up and maintain.

Star topologies are found in all different sizes and types of organizations. They are found in many government departments, wireless networks, and even home networks, especially the wireless home networks.

Ring topology

On October 15, 1985, IBM released its own topology which was then known as Token Ring. The ring topology allowed for the attachment of devices such as mainframes, IBM PCs, and midrange computers which were physically wired in a star topology. The devices attached to the network using shielded twisted-pair cables (STP) at 4 Megabits per second.

IBM developed the ring or token ring topology in order to overcome the

limitations of bus topology. With the ring topology, all the devices connect in a circular design with each device having a direct connection to two other devices in the circle. When data is transmitted from one device it moves around the circle by being passed from one device to the other. Each device that receives the signal will regenerate it and pass it on until it reaches its desired destination.

As the signal moves from one computer to another there is less chance of packet loss. As it is regenerated at each device it is delivered to, the quality of the signal is not degraded as it passes around the ring.

If you think of the ring as an athletics track, the data will be the baton that needs to be passed. The runner starts the race at a specific point and takes it to the next runner, who, without dropping it, accepts the baton and continues on until the next person is reached. This continues until the race is finished. Much like the data, it does not continue any further than its destination device. The runner will be how the data is transported, and each device will be where the next runner is stationed waiting for the baton.

The advantage of ring topology is that it does not use terminators so the signal is not dampened and can continue on its path. There are no packet collisions on the network as data only flows in one direction and it is an easy topology to troubleshoot.

The disadvantage of ring topology is that this type of topology requires a lot more cables which makes it a costly network to implement. If there is a break in the cable it will bring the entire network to a halt.

Like the bus topology, the ring topology is no longer used in modern-day networking architecture.

Tree Topology

Tree topology stems from one root node with a level of devices that connect directly to it, and in turn each device on the second level has other devices connecting back to it. It is also called a hierarchical topology and must have at least three levels of devices branching out.

The tree topology only allows for one connection between the nodes that are connected together. This creates a perfect parent/child hierarchical structure for the tree topology.

The advantages of a tree topology are that it is not too hard to expand on nodes. It is easy to troubleshoot, install, and maintain. It is a good topology to use for wide area networks.

Disadvantages of a tree topology are that it is a very cable heavy topology; it can be expensive to install and maintain. If the central connection fails the entire network goes down.

Mesh Topology

Mesh topology is a topology that connects nodes on the network with multiple paths. This topology is divided into two types: there is the fully meshed and then there is the partial mesh topology.

Full Mesh topology is when each device on the network has a direct path to each of the other devices connected to the network.

Partial Mesh topology is when there are multiple paths existing between the nodes.

To find out if a network is partial or full mesh, you can use the following formula. This formula can also be used to determine the number of connections that would be required to make a full mesh.

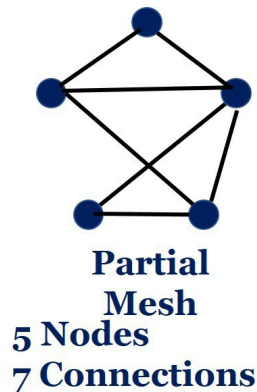
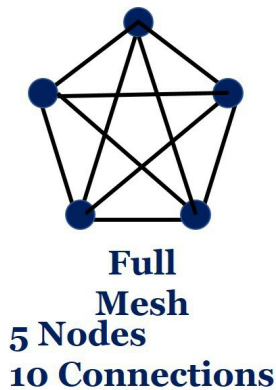
Required connections / no. connections = $\text{nodes} * (\text{nodes}-1)/2$

An example of how to use the formula is:

5 nodes on the network would need = $5 * (5-1)/2 = 10$ connections are required

A partial mesh topology will have less actual connections than nodes, while a full mesh topology will have more connections than nodes.

Mesh topology networks can be expensive networks to implement and are generally used where the network stability, security, and reliability are of the utmost importance. This topology type may be used by city networks for continuous monitoring of their various components such as street lights, traffic lights, sewage works, and more. Some military branches may use mesh technology in order to ensure constantly there is no communications breakdown. Emergency services, research facilities, electricity companies, gas companies, and so on are all organizations that would benefit from a mesh topology network.



The advantage of mesh topology is that it is very robust and each connection is capable of carrying its own data load. It can be a very private network that makes it secure and it is easy to troubleshoot.

The disadvantage of mesh topology is that it can be extremely cable heavy which makes installation quite tricky to downright difficult. It can be a very cable bulky, expensive networking topology to configure and install.

Hybrid Topology

A hybrid topology is a mix of two or more topologies. When you connect two different topologies together to form one network it creates a hybrid topology. This happens, for example, when a company amalgamated with another company. They will most likely have different networking technologies and changing networking topologies is expensive, so joining the two to form a hybrid topology is more cost-effective.

It could also be the way a company is geographically located, or how the office is structured, cable limitations, etc. which requires the need for hybrid topology infrastructure.

The advantages of hybrid topology are that it is not restricted to just one topology. Resilience can be built in quite easily and in some cases, it is the most cost-effective way of joining a network.

The disadvantages are that it can be quite difficult to troubleshoot and can get costly.

Point-to-Point Topology

Point-to-point topologies are very simple topologies and are networks where two devices are connected together. This is used in a home network for

sharing resources and data or small offices where there are only two staff members that need to share data and printers.

It can also be a point-to-point between two routers that can branch out into another networking topology or a connection between two LAN segments.

Point-to-Multiple-Point Topology

Point-to-multipoint topology is where one end device will connect to two or more other end devices on a network and is mainly used for WAN networks.

Network Topology Considerations

There are some standard things an engineer should consider when choosing a network topology:

- Cable length
- Cable Type
- Room for growth or expansion
- Cost

Standards

Standards are what make it possible for the interoperability of components that are not vendor-specific. In other words, because of industry standards, you can mix and match components from different vendors. If you have ever taken a PC apart you would see that not all the parts in that PC are made by the manufacturer of the machine. Instead, you may see memory from one vendor and a hard drive from another. That is because the parts in that machine conform to the industry standards that have been set.

This works the same for industry standards set out for networking technology which is a set of rules that define how different devices over the network can communicate effectively and efficiently. A standard ensures that all components are able to work together on a network, for example, all networking cards conform to a set of standards, making them able to connect a device to a network.

Standards are set by organizations with five of the top organizations being:

American National Standards Institute (ANSI)

The ANSI is the United States of America's official standards organization.

Institute of Electrical and Electronics Engineers (IEEE)

The IEEE is well known for the standards for Ethernet networks which is the IEEE 802.3. They are an international standards organization that is involved with a lot of networking standards.

Internet Engineering Task Force (IETF)

The IETF is the organization that takes care of the standards to ensure that the Internet keeps operating as it does.

International Organization for Standardization (ISO)

The ISO is a federation that incorporates more than 100 standards organizations from all over the globe.

World Wide Web Consortium (W3C)

W3C is an international organization that develops standards for the World Wide Web globally.

Tips for the Exams

When it comes to networking exams, they like to slip in questions about the different standards. When you are going through your course, highlight the various standards you come across, or better yet make a note of them in the back of your notebook. Make sure you revise these and they could just be the points you need to get your mark up a bit more.

Some standards to look out for will include but are not limited to the following standards:

- All the IEEE standards that will include the standards for:
 - general internetworking standards
 - MAC-bridging as well as SpanningTree protocol
 - VLANs
 - Data-Link layer including MAC and LLC
 - All ethernet standards from 10 Mbts through to 10 GB
 - Port Aggregation
 - All Wireless LAN (WLAN) standards
 - Wireless Personal Area Networks (WPANs)
- All the ISO standards that are listed in the CCNA.

Protocols

A network has different devices attached to it. Each device has a specific function along with various rules and conventions they have which enables them to effectively communicate with each other. A network needs a way to be able to identify what the device is to get it connected, how the device handles data, and if it supports message acknowledgment and data compression.

If you think of devices as houses, office blocks, factories, shops, and schools for example, the network system would be the postal service that takes messages, packages, and parcels from each place to deliver them to their destination. The houses, office blocks, schools, shops, and factories are all different. They are not only different types of buildings but they serve different purposes, will have different volumes of packages or messages to send, and have different postal needs. Just like all the different devices that attach to an actual network do.

The one thing all these buildings have in common is the postal service. As it would be absolute chaos to just accept mail, packages, or parcels in any form these entities deem fit, they are governed by standards. These standards would be what envelopes are allowed to be used, box sizes, weights, etc. These standards would be likened to networking standards as discussed above. These standards will be different depending on the needs of each entity, but if these are not adhered to, the postal service will not accept what is being sent. This is true too for networking standards.

But the postal service has its own limitations, rules, and conventions which would be what type of building the post is from and the way a package is packed. It will include what can and cannot be included in a package, size limitations of certain packages, priority service, and if it needs to be signed for. These are the postal service's protocols which are a set of rules and conventions that govern each entity or in the case of a network, the type of device connected to it.

Just like the postal service, data received on the network will have what the package contains, an indicator of where it originated from, and where it must go to. These are basically a set of rules and conventions that allow for effective communications between various devices or nodes on a network.

The network has limitations, certain rules, and conventions each device or node must follow or adhere to. If the device does not conform to these rules or conventions it is not compatible with the network, therefore, it will be refused connection to it.

A lot of computer networks in the modern-day use a technique called packet switching to send and receive information across the network. The switch will be discussed at the end of this section on protocols.

All operating systems in use today will be designed with built-in functions and services. These functions and services are there to enable the support of various network protocols. For example, a smartphone operating system will contain software libraries that support the protocols necessary for the phone to be able to attach to a wireless network. Protocols are also implemented into actual hardware or hardware components in order to work correctly on the network.

Packets that are sent and received over a network will have been modified by the respective protocols required to handle the packet. Each protocol may add a header and footer to the packet which will contain information relating to the sender and the receiver.

A protocol family is a group of network protocols that are designed to work together at both higher and lower layer levels. In the next section, you will learn or have a refresher of the OSI model vs the TCP/IP models. We will discuss how networking protocols are stacked one on top of each other to allow for data to be sent through the networking utilizing multiple protocols each encapsulated within the other.

Some examples of protocol families are:

- **Internet Protocols**
- **Wireless Network Protocols**
- **Network Routing Protocols**

Media Access Control Protocol

Media access control, or more commonly known as MAC, is the protocol that is used to identify the type of device that is attached to the network. It is a communications protocol that sits at the first layer (lower levels) of both the OSI and TCP/IP models. This protocol is what defines what the device is and what the device's MAC address is. No two MAC addresses should ever be

the same, as this is what makes each networking interface unique. This is pretty much the same as street addresses; no two should ever be the same, and if they have similarities there is always something that makes that specific physical address unique like the city postcode or the country code, etc.

A MAC address allows a device to be uniquely identified by a unique number.

IP Protocol

IP stands for Internet Protocol and is, as the name suggests, one of the basic protocols that allow Internet connectivity for devices attached to a network. Each device that attaches to the network will be issued with an IP address from the network IP address pool. Each number should be unique to the network they have attached to. The IP protocols are also what allow devices on a network to communicate with other devices on the network.

The IP protocol sits at the network layer of the OSI model and the Internet layer of the TCP/IP model. IPv4 and IPv6 are the most common implementations of the IP protocol. IPv4 addresses are becoming quite scarce and as such IPv6 is growing has started to take off.

The first version of IP was **IPv4**. This was deployed by ARPANET in 1983. It is a 32-bit address scheme and has over 4 billion IP addresses. It is still the most widely used IP address scheme and is responsible for 94% of all traffic across the Internet. However, IPv4 address pools have been exhausted and as such new technologies have been introduced over the past few decades. These include **network address translation (NAT)**, **IPv6**, and **Classless Inter-Domain Routing (CIDR)**.

IPv6 was introduced in 1994 and was created to resolve the issues and limitations of IPv4 as well as fulfill the need for more IP addresses that rapidly became exhausted with IPv4. It also has a 128-bit address space which allows for a lot more IP addresses than IPv4. Where IPv4 uses the numeric address, IPv6 uses the alphanumeric address scheme.

ICMP Protocol

The ICMP protocol is for the sending of messages between devices on a network in order to ascertain the availability of the device. ICMP means Internet control message protocol and is the protocol that produces packets

for various diagnostic tools, such as traceroute and ping. ICMP packets are used to determine whether there is a problem with a device and sits at the Internet layer.

TCP Protocol

The TCP protocol sits in the transport layer of the TCP/IP model and stands for transmission control protocol. It is the protocol that is used to establish and keep a reliable connection open so applications can communicate and exchange information with each other across a network.

Without the TCP protocol, we would not have the Internet as it is the protocol that is mostly used for the Internet, especially for email which just about everyone relies on these days.

UDP Protocol

The user datagram protocol (UDP) also sits on the transport layer and is used for the transferring of data across the network. However, UDP does not need to wait for a connection nor does it need to verify if the data was received or not. This makes it a lot faster for data transfer and it is a very useful protocol when it comes to being able to query network resources.

Because UDP does not need to maintain a state, it makes it the ideal protocol for sending data from one node to many nodes in real-time. It is the best protocol for handling games, time-sensitive applications, and VoIP environments.

HTTP Protocol

The hypertext transfer protocol (HTTP), is a protocol that sits at the application layer and is the protocol that communicates with the World Wide Web. It is the protocol that helps interpret what a person wants to do over the Internet such as get a web page, post a blog, and so on. It is the protocol that takes your point and click or search request to translate it for the Internet to understand and execute it.

FTP Protocol

The file transfer protocol is an application layer protocol that transfers full files from one node to another node on a network. It is not the most secure protocol for use across the Internet and should be used with caution.

DNS Protocol

The domain name system (DNS) is an application layer protocol that is used to provide basic naming conventions that can be understood by the end-user, such as turning an IP address into a domain name so when an end-user is looking for a website all they have to do is type in the actual name or something close to the name for the web page to pop-up. DNS is what translates the IP address into a domain name.

SSH Protocol

The secure shell (SSH) protocol is a protocol that sits at the application layer and is used to create a secure connection to a remote server.

Packet Switching

Packet switching is a technique used by various system network protocols to transfer information across a LAN or WAN. Packet switching techniques include IP, Frame Relay, and X.25 for example.

Packet switching works by breaking the data being transmitted into a number of parts. These parts are packaged into units that are specially or specifically formatted. These units are called packets. These packets are then sent from the source across the network by switches or routers to its destination. When the packet is received by the destination device it will be unpackaged to be restored to its original form.

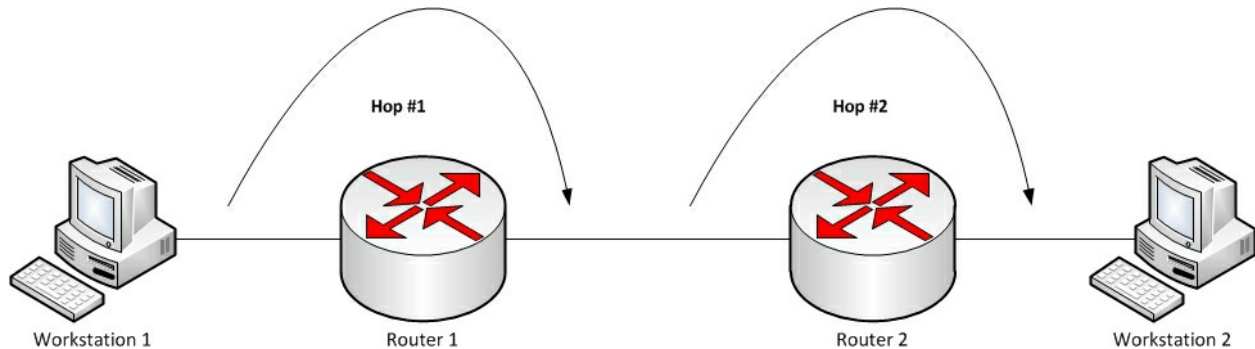
Once again, if you liken this to the postal scenario, the content to be sent via the postal service will be put into the packaging material most suited to it. It does not always fit in one envelope or box, so the contents may need to be broken up and distributed into a number of packages. When they arrive at the destination these packages or envelopes have to be opened in order to see what is inside.

Each packet that is sent across the network will contain information that is specific to both the sender and receiver. This is information such as the sending device address and the intended recipient address. Once again this works in much the same way as sending conventional packages through the postal service. There is a pickup address and a recipient address for the item to be delivered.

Network devices such as switches and routers will use these addresses to

figure out how to transfer the packet to get it to its destination. The device(s) figures this out by calculating the fastest route with the least amount of stops, called hops, along the route to the destination.

Hop



If you look at the diagram above you will see that workstation one is on the first portion of the network, while workstation two would be on the second portion of the network. A hop is the number of networking devices the information must travel over on its path to reach the destination device.

For example, in the diagram above if the workstation one needed to send information (data packet) to workstation two, it would take two hops to get there. The network represents one portion of the full path between the source and the destination. When communicating over the Internet, for example, data passes through a number of intermediate devices, including routers and switches, rather than flowing directly over a single wire. Each device causes data to hop between one point-to-point network connection and another.

The goal is to send the data packet through the route with the least amount of hops because the more hops data packets must traverse along the path to the destination, the greater the packet or transmission deliver delay will be. You can think about hops in the form of traffic lights; they can slow you down on the way to your destination. In order to get where you are going traveling at the speed limit, you would choose the route with fewer traffic lights.

If you want to determine the hop count to a specific device or destination, a common utility such as ping, which can be run from a command line, can be used.

The ping command sends packets that will include a reserved field to include the hop count to the destination device being tested. When that packet sent from ping arrives at the first device it must traverse, the device will receive

the packets and then update it by increasing the hop count by an increment of one. When ping is used to determine hop count the command used requires you to set a predetermined limit of hops. When each device receives the packet and has updated it to reflect its hop number, it will compare the hop count with the predetermined hop number. If the hop count is lower or the same as that number it will send the packet on to the next device. If the hop count exceeds the predetermined hop count number the packet will be discarded. This stops the packet from being sent on an endless journey through the network which could very well happen if there are routing errors.

Packet Analyzer

Instead of just using ping to determine hop counts and networking traffic, there are applications called Packet Analyzers that can help with that. As with all applications available on the Internet these days, you get the free versions and those you have to pay for.

Some of the better packet analyzer on the market today are:

- SolarWinds
- Wireshark
- Windump
- Network Miner

Network Layers

<u>OSI Model</u>	<u>Protocols Per Layer</u>	<u>TCP/IP Model</u>
Application Layer [7]	HTTP, FTP, DHCP, PING, NTP, POP3, SMTP	Application Layer [4]
Presentation Layer [6]	MME	
Session Layer [5]	SSL, NetBIOS	
Transport Layer [4]	TCP, UDP	Transport Layer [3]
Network Layer [3]	IP, ICMP, ARP, IGMP	Internet Layer [2]
Data Link Layer [2]	PPP, HDLC	Network Access or Link Layer [1]
Physical Layer [1]	Ethernet	

A network consists of multiple technologies as well as protocols that are designed one on top of the other to create cross-functionality and communication between these devices. The way they sit on top of each other is called networking layers and it is designed this way to allow for the leveraging of lowering levels without too much effort in that new protocols do not have to be designed to handle all the different types of traffic that flow through a network.

The OSI was one of the first network layer models, and today there are a few more. One model in particular that has gained a lot of interest as of late is the TCP/IP model. The TCP/IP model closely relates to the OSI one but where the OSI has seven layers, the TCP/IP model only has four.

Although these models may be significantly different in their layout or designs, the data path will remain the same no matter the model. A data signal that is sent from a machine will start at the top of the OSI or TCP/IP model and flow downwards towards the lower layers. Each layer in the stack is capable of adding its own wrapper to encapsulate the data before it moves down to the next one. When the data reaches the bottom layer it is then transmitted to the destination machine where it will start at the bottom of the layer stack and work its way back up to the application layer.

OSI Model

The OSI was developed by Hubert Zimmermann in 1978 then polished and published in 1984 by the ISO. OSI stands for Open Systems Interconnection model and it consists of seven layers.

The seven layers of the OSI model, from the bottom up, are:

Layer 1 — Physical Layer

Layer 1 is the lowest level. It is the physical layer that is responsible for sending and receiving raw data streams. These raw data streams are transmitted over a physical medium such as network cables, network interface cards, and level one networking devices. This is the layer that handles the devices that physically connect to the network including both hardware and the software for the device.

Protocols at this layer include ethernet and MAC, while the components and devices at this layer include network interface cards, repeaters, hubs, wireless, and cables.

Layer 2 — Data Link Layer

The data link layer is responsible for defining network data. It is the layer that uses existing physical links to make connections and maintain a stable link between devices on the network.

Protocols at this layer include PPP and HDLC, while data link layer components and devices include layer 2 switches, modems, and network interface cards.

Layer 3 — Network Layer

This is the layer that is responsible for routing information between nodes on the network and uses addresses to determine the destination of the data. At this layer, larger packages may get broken down into smaller pieces. These smaller pieces will be reassembled when they arrive at their destination.

Protocols at this layer include IP, ICMP, ARP, IGMP, while network layer components and devices include layer 3 switches, routers, and bridges.

Layer 4 — Transport Layer

The transport layer is responsible for the error, flow, and congestion control as it is the layer that ensures data packets are efficiently delivered. This is that layer the checks for duplication and unsent or timed out delivery so it can resend unsent packets.

Protocols at this layer include TCP for the sending of packets that require a reliable connection and UDP for the sending of connectionless data.

Layer 5 — Session Layer

The session layer coordinates communications between servers on the network by managing the sessions between these devices. This is the level that is responsible for authenticating communication between servers and applications.

Protocols at this layer include SSL, RPC, SDP, PPTP, SCP, and NetBIOS.

Layer 6 — Presentation Layer

The presentation layer is responsible for the translation of networking data from lower levels into a format that is understood and accepted by applications in the application layer.

Protocols at this layer include MME.

Layer 7 — Application Layer

The application layer is the layer that the users work on and where applications can be found. It is responsible for available resources and data synchronization.

Protocols at this layer include HTTP, FTP, DHCP, PIN, NTP, POP3, AND SMTP.

TCP/IP Model

The Internet protocol suite is a lot simpler than the OSI model and has started to become more popular out of the two models. It only specifies four layers that overlap with that of the OSI model.

The four layers of the TCP/IP model are:

Layer 1 — Network Access or Link Layer

This layer represents the networking topology for the LAN and is the layer that creates the connection between two network nodes to allow them to communicate.

Layer 2 — Internet Layer

The Internet layer is the layer that takes the data from the source to the destination and is where the IP addresses are defined.

Layer 3 — Transport Layer

The transport layer uses ports as a way to address various services on the network and is the layer that is responsible for the interaction between processes.

Layer 4 — Application Layer

This is the layer where user data is created and sent between applications both locally and remotely to the device.

Interfaces

An interface is a point of communication or connection between the network and a device attached to the network. An interface can be both a physical or

virtual networking device. A server has one interface per network card for either wireless or ethernet connections.

Interface cards are usually configured to be able to access a private network, the Internet, or another device interface on the network.

Important Network Terms to Remember

The following are a few networking terms to remember.

Connection

In networking terms, a connection means establishing a link to another device on the network before data is transferred to it through the network. Once the connection between two network nodes has been established the data will be sent between them.

Firewall

A firewall is a program with rules about what traffic is allowed through different ports on the network. It is the device that stops harmful or unauthorized traffic trying to access the network. It can also be used to block certain ports on a server that may not be in use.

LAN

A local area network (LAN) is a network or portion of a network that may only be accessed through authorized devices that are local to the main network. A LAN can be found in both office and home environments.

Network Interface

A network interface is a special software that interfaces with the device driver (also software) of network-specific hardware such as network cards. A server can have more than one network card in it and each one of these cards can be configured individually.

There are both physical and virtual network interfaces that both work in the same way.

Packet

Packets are the simplest of units that can be sent across a network. Data is packaged into packets before it is sent across the network to its destination.

device. Packets are like the envelopes or packing boxes that are needed to send the data across the network. The packet will contain information about the sender's and receiver's addresses. They are much like envelopes and packing boxes that get sent through the actual mail or a transport company.

Data packets contain information such as the source, destination, timestamp, hops, and so on which is contained in the header portion of the packet. The body of the packet is where the data that is being sent is.

Port

A port is another type of address that can be found on a device. Ports are usually allocated to a specific piece of software and are not a physical interface. Ports are what allow a single networked device to use multiple services to communicate with. For instance, messaging services with TCP use port 25, while transferring a file with FTP may use port 21, and another service running on the machine may use port 18.

Protocol

Protocols are a standard set of rules that network components and devices use to interconnect and work together on a network. There are many protocols in use today that work on different layers with some of the most common being IP, UDP ICMP, and TCP which are lower-level protocols. Application level protocol that is built on these lower protocols includes TLS/SSL, FTP, and HTTP which is the protocol used for accessing web pages on the Internet.

VPN

A virtual private network or VPN is a secure connection tunnel that allows for a safe and secure connection through the Internet from one LAN to another LAN. The VPN provides a stable and secure environment that is private and can be used to safely and seamlessly connect remote systems to make them seem as if they were part of a LAN. Corporations and organizations use VPN to ensure the security of their network while affording remote users the ability to connect to the system.

WAN

A wide area network is a network that extends passed a LAN and is a term that is generally used to describe a corporate network that spans more than one region, country, or continent. A WAN can also mean that a network may

be reachable through the Internet.

Basic Network Fundamentals

In the previous section, it discusses what a network is, the various components, terms, rules, and information that is involved in the make-up of a network. This section covers a few basic network foundation devices that are at the core of a network no matter what the size of the network is. These are the basic devices that are required for a network to make it possible for other devices on your network to communicate with each other. Some of these devices allow one network to communicate with another network, and as long as certain criteria are met, it does not matter what the geographical location of the other network is. Network foundation devices are the devices that allow network access to the Internet and make it possible for different types of devices to connect to the network, or interconnect, like telephones, conference devices, smart devices and so on.

Devices such as wireless access points, switches, and routers are the basic foundation of a network, each of which has a specific function to perform on a network

Access Points

An access point is what is used to connect a device to a network. There are access points that require a physical cable to connect the device to the network or there are wireless access points that make connecting to a network possible without cables.

Floor or Wall Ports

A wall or floor port is a physical network point for use with a network cable that would run from the network access point to the LAN card in the PC, laptop, server, printer, or other devices.

Patch Panel

If a network has wall or floor ports there will be a patch panel in a central server room or data center room. The floor port is connected to a patch panel

with a Cat 5, Cat 6, or Cat 7 type cable that will be connected (crimped) into the ethernet port which is visible to the end-user.

The side of the cable that goes into the patch panel is also connected (crimped) into one of the many ports of the patch panel. There are different sized patch panels, and they typically come as 12, 18, or 24 port patch panels.

It is the patch panel that will connect to the network switch, making it possible for the device connected to the wall or floor port to access the network.

Wireless Access Point

A Wireless Access Point extends the range of a Wi-Fi router's reach. In other words, it amplifies the Wi-Fi. This allows devices that are further away from the router to connect with a decent signal enabling the Wi-Fi to support more systems.

A Wireless Access Point can also relay information about each device connecting through it back to the Wi-Fi router and may also be used for a bit of extra security.

Routers

Routers are devices that connect networks together and what connects systems to the Internet. It only needs one Internet connection for multiple devices; this saves a lot of money for a company.

Routers do not only connect devices; they also analyze the data that flows through. It also decides which is the best route to send the data to its destination. They can be set to prioritize certain devices on the network, and they can protect the company's information from security threats.

Some routers have features such as an Internet Protocol (IP), a firewall, or a virtual private network (VPN). Routers operate at Network layer 3 as they do not communicate through a physical MAC address but rather an IP address.

Switches

A switch is a network controller that connects the different network devices

such as computers, printers, servers, backup devices, and so on to a particular network that may reside in an office block, lab, campus, etc.

Switches are the devices that allow all the other devices to communicate with each other as well as communicate with other networks in order to create an environment of shared resources.

Cloud-managed switches offer a simple and easy to manage switch that can be instantly monitored and configured over the web without the need for a physical connection. The switch can be configured remotely, power over ethernet (PoE) can be controlled, and more. All updates are managed and done through the cloud.

Managed on-premises switch is a switch that is managed in-house and on the premises where the switch is located. In order to manage the switch, IT personnel would need to access it through a device directly attached to the switch or through a console cable. All updates to maintain the integrity of the switch needs to be done locally.

Wireless Networking

There are three wireless networking deployment methods and these are:

Centralized Deployment

Wireless centralized deployment has a wireless controller installed on-premise in a centralized location that facilitates easy access to it. This deployment is found where offices or buildings are in close proximity to each other.

Cloud-based Deployment

Cisco devices such as Cisco Meraki cloud-managed devices are used for these types of deployment. These devices allow for cloud-based management of wireless network devices attached to the system.

Converged Deployment

This type of wireless deployment uses one network device such as an access switch which converges both wireless and wired network devices through it. This type of deployment is ideal for smaller offices, campuses, or schools that require consistency for their wired and wireless device connections.

Chapter 8: Study Material — Network

Fundamentals

This section accounts for 20% of the 200-301 CCNA exam. The following is a quick overview of what the student is required to know for each topic.

***Note:** There are must know questions — these are key points that the student is required to know for the exam. They will start with RK for Required to Know, while AH stands for answer hints that the student taking the course is required to know for the examination.*

Foundation Topic

The first part of the course will cover the foundation topics which are about networking, what a network is, network layer models (OSI, TCP/IP), and the protocols that work at each layer.

You will cover the basics and history of some key networking fundamentals of which this book gave you an overall preview of in the previous chapters, only you will go a little more in-depth with history. It may all seem trivial and a little boring but PAY ATTENTION, Cisco loves to throw in the odd question here and there about something that was highlighted in these chapters.

Don't skip any test exam questions regarding these chapters as well, especially the DIKTA questions.

This section requires the student to be able to compare the OSI and TCP/IP models. It will go into particular detail about the most prevalent model which is the TCP/IP model.

TCP/IP Model

In the previous chapters, we covered both the OSI and TCP/IP models. Don't discount either of these models, even though they may go more into depth about the TCP/IP model.

The protocols they pay close attention to for the TCP/IP model (including the

packets for each protocol) are:

- Application Layer — HTTP
- Transport Layer — TCP and UDP
- Network Layer — IP (IP Addressing basics and IP Routing basics)
- Link Layer — NIC basics and Ethernet

At each layer, you should be able to identify the packets and how they are passed from layer to layer. In particular, you will need to know how data is packaged. You will need to know how the data is encapsulated starting at the source per layer and how it would be decapsulated at the destination per layer.

Data Encapsulation

As data is passed from the application layer down towards the link layer, before it is sent from the application level it is packaged and that layer's header put onto it. Just like mailing a letter, you put the letter into an envelope, address it and then put your return address on it. When data is packaged it is placed into a packet and the details of the source and destination addresses are added to it as a header. But it also adds the details of the protocol, as its own header, on it as it goes down through the layers. So by the time it reaches the link layer, it would have three headers.

The path of the data from the source is as follows:

- Application layer packet has an HTTP header that encapsulates the data being transmitted.
- Transport layer packet has a TCP header that encapsulates the entire HTTP packet.
- Network layer packet has an IP header that encapsulates the entire TCP packet.
- Link layer packet will encapsulate the entire IP packet containing the TCP, HTTP headers and data. At this layer, the packet will be encapsulated with both a header and a trailer before being sent on to the destination.

The path of the data at the receiving host will work the opposite way with the packet being de-encapsulated header per header through the layers until it reaches the application layer in a form recognizable to the application.

Exercise: As an exercise, you may be asked to create a packet from the

application layer through to the link layer with a message as the data. For example HTTP|Hello World. The exercise will be in the form of steps and each step you will be asked to encapsulate the data with a protocol header.

Keep in mind that the questions may not always go in the exact order that the layers do,. They may ask you to encapsulate layer 1 (which is the Link layer — not the application layer).

Pay attention to detail of the question as per the above example; know the layers by name and number.

Network Components

The student must be able to identify and explain the role as well as what the function of the following network components is.

Routers

RK: What role does a router have and what is the device's functions on the network?

AH: There is a reason why network engineers need to know about the TCP/IP model and packet addressing. It is so they can understand not only what a router is or why the device is needed on the network, but how it works as well.

One of the primary functions of a CCNA is to be able to install, configure, maintain, and troubleshoot routers. Routers are the devices that join TCP/IP networks together by routing IP packets through the network and ensuring they are received by the correct device.

L2 and L3 Switches

RK: What role do switches have and what are the device's functions on the network?

AH: A switch, also known as a MAC bridge, switching hub, and bridging hub is a hardware device that enables the devices to connect to the network to send and receive data.

Learn the differences between hubs and switches as well as how both devices work to better understand the differences between the two.

- L2 Switches — a data link layer switch that segments a LAN using a device connected to the LAN to segment the network.
- L3 Switches — are used to forward frames that are based on layer 2 addresses as well as packets that are based on layer 3 addresses. Layer 3 switches may be able to perform the functions of both switches and routers. Cisco's layer 3 switches carry out packet forwarding using the Cisco Express Forwarding (CEF) service.

Next-generation firewalls and IPS

RK: What role do firewalls and IPS have and what are the devices' functions on the network?

AH: A firewall is a device/software that can be programmed with a set of rules to permit or block traffic from entering the network/device, while the intrusion prevention system (IPS) works with a firewall (or on its own) to prevent malicious software from entering the system or within the system. It can be used in conjunction with a firewall to ensure the information the firewall permits is legitimate information.

Learn the differences between the two and to configure both of them as separate entities and working together.

- Next-generation firewalls (NGFW) — learn about Cisco's next generation firewall which is a network security device with capabilities that go beyond that of a traditional stateful firewall.

Controllers

RK: What role do controllers have and what are the device's functions on the network?

AH: For the exam, students will need to know why controllers are important for a network, what they are, and what their function is. They will also be required to know about the Cisco DNA center as well as the Cisco WLC, how to use these management tools, what their role is on a network and why a network engineer would use them.

- Cisco DNA Center — DNA stands for Digital Network Architecture, which is an “open, extensible, and software-driven architecture” which allows for the preparation and configuration of network devices. It is a network management command center designed to aid in leaner and

less risky configuration of networking devices.

- Cisco WLC — WLC stands for Wireless LAN Controller which is used to centrally manage as well as configure all available access points for a LAN installation.

Endpoints

RK: What role do endpoints have and what are the device's functions on the network?

AH: An endpoint is another name for remote devices connected to and which have an open communication path to and from a network. These devices include laptops, desktops, smartphones, servers, and tablets. They are also one of the major points of vulnerability when it comes to network security. But they are the key element to a network that are attached so that they can share resources and get the benefit from the network services. Learn about the different endpoints, what each of their functions is, how they connect to the network and what vulnerabilities they cause to the network.

Servers

RK: What role do servers have and what are the device's functions on the network?

AH: Servers are the devices that store information/data, run applications, and are used to send and retrieve files from. Servers are computers with a lot more storage, processing power, and memory than client computers that attach to them via a network.

Network Topology Architecture

The student must be able to describe the characteristics of each of the network topology architectures covered in the course.

On-premises and cloud

RK: Explain the characteristics of on-premises topology architectures

AH: On-premise means that software is installed onto a local physical device and can be accessed from the system. On-premise hardware means that the entire system or LAN is physically based on the site.

RK: Explain the characteristics of cloud topology architectures

AH: Cloud-based software is provided by the cloud-services provider and can be accessed through a web browser. Cloud-based infrastructure means that the company's network is cloud-based and runs in a virtual cloud-based environment on the supplier's systems.

Small office/home office (SOHO)

RK: Explain the characteristics of SOHO architectures

AH: The SOHO network model is one where the office consists of between 2 to 50 users and the most popular network is 10/100 Base Ethernet due to cost reasons. It is also fast becoming one of the most popular networking segments arising, as thanks to online marketing media and being able to do business online, small businesses are springing up fast. The student should learn about the SOHO culture and what the characteristics of a SOHO network are.

Spine-leaf

RK: Explain the characteristics of spine-leaf topology architectures

AH: Learn about the spine-leaf topology architecture, who uses this kind of topology, and what the benefits of this topology are. The topology consists of a core router with spine switches attached to it to which leaf switches attach to the spine switches.

WAN

RK: Explain the characteristics of WAN topology architectures

AH: A WAN is a wide area network that makes it possible for a local area network (LAN) to attach to other networks located anywhere in the world. Usually WAN also refers to being able to access the network across the Internet. WANs were covered in the previous chapters but the learner should also learn more about WAN topology through the Cisco learning network on top of the course curriculum.

Cabling Types and Physical Interfaces

The student must be able to compare various cabling types and physical

interfaces in order to pass the CCNA exam.

Concepts of PoE

RK: Explain the concepts of PoE

AH: PoE exists over a wired LAN environment and it allows networked devices to be powered by the LAN cable instead of a power cable. PoE is a popular cabling technique for IP phones, switches, and so on. Learners should learn about Cisco PoE devices, what the importance of PoE is, and why it is advantageous to use in a networking environment.

RK: Cabling and connections.

AH: Learners should learn about the various Ethernet cables used on a network to connect a networked device from a floor port, connect PC to PC, switch to switch, switch to a router and so on. Learn about the different cable types.

RK: Single-mode fiber, multimode fiber, copper

AH: Learners need to learn about the different fiber and copper cables that are used to connect networks. Learn the strengths, limitations, vulnerabilities, what applications they are best for, when a company would use each, and what the expensive for each is.

Exercise: Learn how to troubleshoot cable and interface issues such as errors, mismatch duplex, collisions, and speed. Learn what utilities to use to troubleshoot these errors.

Exercise: The exam requires the student to be able to understand and compare UDP to TCP. Learn the differences between TCP and UDP as well as what layer they work on. TCP is a protocol that relies on a verified connection, while UDP is a connectionless protocol that sends data regardless of whether it can make a connection with the intended receiver or not.

Exercise: Learn how to configure and verify IPv4 addressing and subnetting. Subnetting is when an address and IP network are broken down into a logical subdivision of the main IP addressing pool.

Exercise: The exam requires the student to be able to explain why private IPv4 addressing is needed. Learn about IPv4, the addressing formats, and procedures.

Exercise: Learn how to successfully configure IPv6 addressing, verify them, and prefix:

- Anycast — network routing methodology that allows a single destination many different routing paths.
- Compare IPv6 address types — learn about IPv6 IP addresses
- Global unicast — is an address that is publically routable
- Link local — an address that is only useable on a specified network segment
- Modified EUI 64 — automatically configure IPv6 using the MAC address of the interface.

Exercise: Learn how to verify the IP parameters for a Client OS such as Mac OS, Windows, and Linux. There are a few ways to do this; the easiest is through the command prompt on the computer. For Windows, it would: `ipconfig /all`

Exercise: Learn the concept of wireless principles and be able to confidently explain the following:

- Encryption — used to secure the wireless network connection with an authentication protocol.
- Nonoverlapping Wi-Fi channels — learn about what the different Wi-Fi channels are as well as their limitations.
- RF — RF means radio frequency; learn about the different frequencies and spectrums RF operates in.
- SSID — is short for Service Set Identifier and it is the identifying name for a Wireless LAN.

Exercise: Learn about the fundamentals of virtualization and virtual machines. Learn what types of environments you would use virtual machines on and what Cisco's preferred program for managing virtual machines is.

Exercise: Learn about and be able to explain the different switching concepts such as:

- Frame flooding — a switch receives a unicast frame
- Frame switching — frame switching is used to increase the speed of a network
- MAC address table — it is a table of all the reachable devices on a network

- MAC learning and aging — MAC aging is the time before a MAC address is forgotten from the network and MAC learning is the process of gathering all the reachable MAC addresses on a network.

Chapter 9: Study Material — Network Access

This section accounts for 20% of the 200-301 CCNA exam. The following is a quick overview of what the student is required to know for each topic.

Note: *There are must know questions — these are key points that the student is required to know for the exam. They will start with RK for Required to Know, while AH stands for answer hints that the student taking the course is required to know for the examination.*

Exercise: The student must be able to configure and verify VLANs in a normal range spanning multiple switches. Reference Access ports (data and voice), connectivity, and default VLAN. Learn VLANs and trunking, as well as, the fundamentals of virtual local area networks.

Exercise: Learn how to configure and verify interswitch connectivity with 802.1Q, native VLAN, and trunk ports. Learn about the IEEE 802.1Q standard or Dot1q, how it supports VLANs on an IEEE 802.3 Ethernet network, and what VLAN tagging for Ethernet frames is. The learner is also required to know what devices can support these frames.

Exercise: Learn how to configure and verify layer 2 discovery protocols such as Link Layer Discovery Protocol (LLDP) and Cisco Discovery Protocol (CDP). Learn why a network needs to advertise its identity, and capabilities.

Exercise: Learn how to configure EtherChannel (LACP) (layer 2/layer 3) and verify it. Learn why EtherChannel is used and what the benefit of port link aggregation technology is. Why you would group ports into one logical link and the benefits of LACP.

Exercise: Explain Rapid PVST+ Spanning Tree Protocol, identify basic operations, and what the need for it is. Learn about PortFast benefits, Port states, (forwarding/blocking), and Root bridge — primary/secondary, root port, and other port names. Learn what they are used for and why they are important, as well as where they are used.

Exercise: The student must learn how to compare AP Modes and Cisco Wireless. Learn about AP mode that stands for Access Point mode and is the mode that encapsulates all data from wireless clients over a WAN using CAPWAP tunnel. Learn the different functions of AP modes and about Cisco

Wireless technology. AP mode is also capable of switching VLAN and SSID if WLC or CAPWAP is unreachable.

Exercise: Learn about the physical infrastructure connections of WLAN components such as Access Point (AP), access/trunk, Wireless LAN Controller (WLC), and Link Aggregation Groups (LAG). Learn about what the components are for, what the limitations are, and where they are used in what capacity.

Exercise: Explain Access Point (AP) and Wireless LAN Controller (WLC) management access connections including console, HTTP, SSH, Telnet, HTTPS, and TACACS+/RADIUS. Learn about the different connections as well as the differences, what their purpose is and where they would be used.

Learn what management access to an AP or WLC is and how to access them with a console cable.

TACAS+ stands for Terminal Access Controller Access Control Service Plus. RADIUS stands for Remote Access Dial-In User Service. These services are used for administrative control over services such as accounting, authorization, and authentication processes. Learn how it can be used to gain management access to an AP or WLC.

HTTP stands for HyperText Transfer Protocol and is the protocol that is used by the World Wide Web to determine how messages are sent and what actions to take in response to a request. Learn how it can be used to gain management access to an AP or WLC.

HTTPS stands for HyperText Transfer Protocol Secure. It is an extension of the HTTP protocol. HTTPS is used to have a more secure connection over which to communicate across a digital network such as the Internet. Learn how it can be used to gain management access to an AP or WLC.

SSH stands for Secure Shell and is a protocol that is necessary for using networking service securely over an unsecured network environment. Learn how it can be used to gain management access to an AP or WLC.

Telnet is an application software that is used to gain access to a command-line interface on a remote host. Learn how it can be used to gain management access to an AP or WLC.

Exercise: This exercise requires the learner to use a GUI such as WLAN

creation, advanced WLAN settings, security settings, and QoS profiles to configure the components of a wireless LAN access to enable client connectivity.

Chapter 10: Study Material — IP Connectivity

This section accounts for 25% of the 200-301 CCNA exam. The following is a quick overview of what the student is required to know for each topic.

Note: *There are must know questions — these are key points that the student is required to know for the exam. They will start with RK for Required to Know, while AH stands for answer hints that the student taking the course is required to know for the examination.*

Exercise: The student must learn to interpret the components of a routing table including Administrative distance, Gateway of last resort, routing protocol code, and so on. This is covered under the topic of IP Routing and the learner should learn how it works and why routing tables are important.

Exercise: Learn how routers determine how to forward information by default by utilizing:

- The administrative distance which is the feature a router will use to select the best path when there is more than one to choose from.
- The longest match is when a router must pick the route with the longest prefix out of the routes in a routing table. This prefix will also match the prefix for the destination address.
- The routing protocol metric is the cost that is assigned to a particular routing route.

Exercise: The student will need to be able to configure static routing for IPv4 and IPv6. They will need to know what default routes, floating statics, host routes, and network routers are. This is covered in “Fundamentals of Static routing” which can be found on the Cisco Learning network. This video is a great supplemental learning resource to help with understanding IP routing.

Exercise: Working with single area OSPFv2 and learning to configure and verify the protocol. The student will have to learn what the following are:

- Broadcast — DR/BDR selection is the designated routers and backup designated router on a multi-access network.
- Neighbor adjacency in OSPF is when two routers will start to share their LSDBs if their parameters are a match and if they do they are said to be neighbors adjacent.

Exercise: Learn about the first-hop redundancy protocol (FHRP) and what the purpose of the protocol is. FHRP is a networking protocol that allows one of the neighboring routers on a network to provide backup support for the default gateway. If the gateway fails one of the active routers will step in and take over the gateway address to ensure the network is operational.

Chapter 11: Study Material — IP Services

This section accounts for 10% of the 200-301 CCNA exam. The following is a quick overview of what the student is required to know for each topic.

Note: *There are must know questions — these are key points that the student is required to know for the exam. They will start with RK for Required to Know, while AH stands for answer hints that the student taking the course is required to know for the examination.*

Exercise: Learn the fundamentals of Network Address Translation (NAT). The student has to be able to confidently configure inside source NAT and verify. This has to be done using static and pools which is covered in the “Fundamentals of Network Address Translation (NAT)”. The IP Addressing NAT configuration guide can be found under study materials on the Cisco Learning Network, which is an excellent source to get this information from. The network source also has how to verify NAT Operations and explains how to do basic NAT troubleshooting.

Exercise: Learn how to configure the Network Time Protocol (NTP) and the best practices thereof. This is important as the learner will need to be able to configure and verify NTP while operating in a client and server node. Learn the importance of NTP.

Exercise: The student must be able to explain what the role of DNS and DHCP is within the network.

RK: Explain what SNMP stands for and what the function of SNMP in network operations is.

AH: Simple Network Management Protocol is a set of protocols that is used to monitor and manage network devices such as routers, bridges, switches, servers, workstations, printers, and hubs. It is important to learn what the function of this protocol is, how it works, and why it is important.

RK: Explain how Syslog features are used.

AH: The student must be able to explain the use of Syslog features, including facilities and levels. These are part of some of the popular services that log server events. The learner must be able to identify the Syslog data log, the Syslog facility and what it is (it is the machine that creates the Syslog) and

know what the severity level of the Syslog is.

Exercise: Learn about DHCP as the student must be able to implement DHCP client and relay. They will have to be able to understand IP addressing and automated IP address system which includes static IP addresses, IP address lease, IP address pools and so on.

Exercise: Understand Quality of Service (QoS) as the student will be required to explain the forwarding per-hop behavior (PHB) such as classification, congestion, marking, policing, queuing, and shaping.

Chapter 12: Study Material — Security

Fundamentals

This section accounts for 15% of the 200-301 CCNA exam. The following is a quick overview of what the student is required to know for each topic.

***Note:** There are must know questions — these are key points that the student is required to know for the exam. They will start with RK for Required to Know, while AH stands for answer hints that the student taking the course is required to know for the examination.*

Network Security

RK: Explain: what are the key security concepts?

AH: The student will need to have an understanding of what the key security concepts are, in particular:

- Security exploits
- Security mitigation techniques
- Security threats
- Security vulnerabilities.

The student should learn Network Security Threatscape from introduction through to learning what the best tools are and what types of security attacks there are as well as how they are handled.

RK: What are the elements of a security program?

AH: The student needs to know about the Network Security Baseline and the elements of a security program including physical access control and user awareness.

RK: Explain security policies and how they are managed.

AH: Learn about security password policies, best practices for password policies, password complexity, management, and password alternatives. It is important to learn about password alternatives such as biometrics, certifications, and multifactor authentication.

Exercise: Configure access control for a device. The student must learn how to configure access control for a device using a local password. They must be able to confidently use passwords and privileges commands.

Exercise: Configure device access control lists and verify them. The student must be able to confidently navigate access control lists, configure them, and verify them. Learn about classifying network traffic with access lists.

VPN

RK: Explain site-to-site VPNs and remote access

AH: Virtual Private Networks make secure connections for remote device access to a LAN. A VPN can make the remote access device seem like it is directly connected to the LAN. Learn how VPNs connect for site-to-site VPN access as well as remote access, what the differences are, and the pros and cons of each VPN connection method.

Layer 2 Security

Exercise: Configure Layer 2 security features such as dynamic ARP inspection, DHCP snooping, and port security. Learn about Layer 2 security and the Layer 2 landscape attacks as well as why it is important to implement Layer 2 security in that lower levels affect higher levels with layer 2 being a possible weak link in networking security.

It is important to know how to prevent and defend against Layer 2 security attacks.

Exercise: Understand the basic concepts of Accounting, Authorization, and Authentications mechanism (AAA Mechanism). Students are required to know the basic concepts of the AAA mechanisms and be able to describe them as well as differentiate between them.

Wireless Security

RK: Explain the wireless security protocols; WPA, WPA2, and WPA3. When would you use either of them?

AH: Students should know what each of the above wireless security protocols is and how to configure them.

Exercise: Configure a WLAN using WPA2 PSK. The student needs to be able to successfully configure the WPA2 PSK security protocol using a GUI. It is a good idea to learn about WEP, WPA, WPA2, TKIP, AES, CCMP, and EAP. The course will cover all of these protocols, but you should know what each of them is for and how to configure them.

Chapter 13: Study Material — Automation and Programmability

This section accounts for 10% of the 200-301 CCNA exam. The following is a quick overview of what the student is required to know for each topic.

***Note:** There are must know questions — these are key points that the student is required to know for the exam. They will start with RK for Required to Know, while AH stands for answer hints that the student taking the course is required to know for the examination.*

Automation and Programmability — 10% of the Exam

For the programmability sections, the student must learn about the impact of automation on network management. Why it is important and how it cuts down on the risk of human error, especially when it comes to configuring hundreds of switches and routers across WAN networks. How coding can save time for network administrators.

The student must be able to identify traditional networks with controller-based networking such as Cisco DNA and Cisco WLC.

RK: Explain controller-based and software-defined architectures such as fabric, overlay, and underlay.

- North-bound and south-bound APIs
- Separation of control plane and data plane

AH: Cisco software-defined access will have to be learned to discuss the importance of understanding how the Cisco DNA SD-Access architecture layers work. As with the TCP/IP layer, the Cisco DNA SD-Access architecture can be defined in four layers:

- Physical layer — layer 1 which is where the physical devices sit. It is also the lowest level layer.
- Network layer — layer 2 which is where the Fabric Overlay (LISP, VOLAN, CTS) sits on top of the Network Underlay (Settings and protocol) within the same layer.
- Controller layer — layer 3 which is where the Network Control

Platform (NCP), Network Data Platform (NDP), and Identity Services Engine (ISE) sits.

- Management layer — layer 4 and the top layer are where the Cisco DNA center User Interface sits.

The Cisco website has some very in-depth helpful documents to help you better understand Software-Defined Access.

RK: Learn about the characteristics of REST-based APIs.

AH: The student must know the characteristics of REST-based APIs. The student will need to know and understand model-driven programmability and RESTCONF. You will learn how RESTCONF uses HTTPS for transport and the data models it is coupled with and learn to CRUD using GET, POST, and Delete with RESTCONF.

Exercise: Learn about the different applications for configuration management with some of the top apps that will be covered being Ansible, Chef, and Puppet. With the implementation of DevOps taking off configuration management and automation has become an important part of every corporation. Knowing how to use these applications and what they are for is something every aspiring network engineer needs to learn in order to keep up with technology trends.

Exercise: Learn how to interpret JSON encoded data

Chapter 14: CCNA Interview Questions

When you are going for a job in IT you are going to get some interview questions that have usually been designed by an HR firm if the job is with a large company. As the job market is rather competitive, being prepared is a good foot in the door.

Some of the more common questions have been covered in the previous chapters of this book. Why not test yourself and write down your best answers? These are questions like:

- What is a network?
- What is a switch?
- Why would you use a switch?
- What are routers?
- Why would you use a router?
- What are the differences between a switch and a router?
- What is a hub?
- How is a hub different from a switch and a router?
- Is there a difference between a MAN, LAN, and WAN? Please explain.
- What is PING used for?
- Explain Topology and define 8 different topologies
- What is a WLAN?
- What is an AP?

Interview Questions for CCNA Position

Here are some top interview questions you may be asked if you are going for a CCNA position.

Question: Do you know the different ranges and classes of IP Addresses?

Answer: Class A — ranges 1 - 126

Class B — ranges 127 - 191

Class C — ranges 192 - 223

Class D — ranges 224 - 239

Class E — ranges 240 - 254

Question: Can you explain what Private and Public IP are?

Answer: Public IP is an IP address that is used over the Internet, while a Private IP address is an address that is used on a LAN.

Question: What is a MAC address?

Answer: A MAC address is defined at the Link Layer of the TCP/IP model and the Physical Layer of the OSI model. MAC stands for Media Access Control and it is a unique number assigned to a network interface that is used to identify a device. No two MAC addresses should even be the same.

Question: Can you list the different types of cabling that are associated with routing?

Answer: Crossover cable which is used between a switch to a switch and a computer to a computer.

Rollover or console cable that is used from a switch to a computer.

A straight cable that is used between a switch and router.

Question: Can you explain what a protocol is?

Answer: A protocol is what enables devices on a network to communicate with each other.

Question: Can you explain DHCP?

Answer: DHCP stands for Dynamic Host Configuration Protocol and is the protocol that is used to automatically assign IP addresses to a client from an IP address pool.

Question: Can you explain the Domain Name System (DNS)?

Answer: DNS is the service that translates domain names into IP addresses over the Internet for any device that connects to the Internet.

Question: Can you explain network congestion?

Answer: Network congestion refers to the instance when a network will slow down and in some severe cases may even come to a standstill due to too many devices trying to use the network bandwidth.

Question: Can you explain BootP?

Answer: BootP is used on diskless workstations that are connected to a network and is the protocol that is used to boot them. BootP stands for Boot Program.

Question: Can you explain the difference between half-duplex and full-duplex?

Answer: With half-duplex a device cannot receive and transmit at the same time, while the full-duplex device can transmit and receive simultaneously.

Question: Can you explain what latency is?

Answer: Latency is the time delay between the time a device receives a packet to the time it sends out a response.

Question: Explain what MTU is.

Answer: It is the maximum size a packet can get before the data will need to be fragmented. MTU stands for maximum transmission unit.

Question: Explain what a node is.

Answer: A node is a network connection point to which any device that can access the network attaches.

Question: Can you name the layers of the OSI model from the bottom to the top?

Answer: Physical layer, data link layer, network layer, transport layer, session layer, presentation layer, and the application layer.

Question: Explain what a Window is in relation to a network.

Answer: A window is the time between the sent information before a response is received.

Top Jobs for CCNA Certified Professionals

Before the new CCNA certification 200-301, there were different certification paths for the CCNA. Thus, to get the job you really wanted, you would most likely have had to have two or three of the CCNA certifications. With the new CCNA certification, it incorporates nearly all of the single CCNA certifications into one, which means one certificate can open up a whole lot more job paths.

Network Administrator

Network administrators are responsible for the day to day administration of the network.

Network Analyst

Network analysts analyze as well as maintain computer systems and data communications networks.

Systems Administrator

Systems administrators are responsible for the maintenance, configuration, upgrading, and daily management of the network and networking devices.

Network Design Engineer

A network design engineer is responsible for the network topology design of the network and is able to design workable networks.

Infrastructure Engineer

An infrastructure engineer is responsible for maintaining the network infrastructure which includes ensuring the network is always up to date with the latest technology. They are responsible for ordering the system's hardware. They can also design, plan, and install networks.

Cloud Engineer

A cloud engineer is responsible for systems that run in the cloud environment. They are responsible for the security of the network and ensuring the cloud network is agile as well as operates efficiently.

Cloud Architect

A cloud architect is responsible for the cloud computing architectures and design strategy of an organization's cloud network.

Collaboration Engineer

A collaboration engineer is responsible for the convergence of applications such as data, mobile apps, video, and voice.

VoIP Engineer

A VoIP engineer is responsible for designing, implementing, maintaining, troubleshooting and managing Cisco's voice as well as unified

communications.

Data Center Manager

A data center manager is responsible for the managing of all the systems and components of an organization's data center. This will include troubleshooting of the network systems, cable maintenance, system upgrades, updating the data center records and keeping the data center's schematics up to date.

Data Center Network Engineer

A data center engineer is responsible for keeping the systems in the data center running at their optimum and ensuring all the systems work together as they should.

Data Center Technician

A data center technician is responsible for the day to day care and support of the data center. They oversee the maintenance of the systems and put preventative measures in place to ensure the systems are reliable and stable.

Industrial Network Specialist

An industrial network specialist is responsible for the systems in a manufacturing or operations environment and offers support on industrial products such as various robotic systems stress testing machines. Engineering machines that design parts and manufacturing electronic jigs.

Network Security Engineer

A network security engineer is responsible for all day to day system security devices and risk management. They have to keep abreast of potential network and device threats, and they need to make sure they have both preventative measures and ways to deal with any system attacks.

Cyber Security Engineer

A cybersecurity engineer has to analyze various computer networks to make sure that all security measures are in place to prevent cybersecurity attacks. They have to be proactive in ensuring the system is robust enough to handle malicious and natural disasters.

Upgrading Your Certification

As you go higher up the Cisco Certification level, there are a few different areas that a network engineer can branch out into. The more qualified you are, the bigger and better job opportunities and promotions will become available to you. The higher up the levels you go with the Cisco certification, the harder the exams get. Most of the higher-level certifications have the added bonus of having to do not only a practical exam but an 8 hour lab exam too.

But at the end of the day, when you are Cisco certified, all your hard work and focus will pay off with a lucrative career. With the IT world evolving as it is, your career will only grow from strength to strength in a very exciting and fast paced industry.

Cisco certified professionals are highly sought after all over the world and get very well paid, too.

Conclusion

During the duration of the course, you should spend at least an hour going over the materials you covered in the course for that day. Do any self-study that has been suggested for the day and if you are able to, go through the course materials for the next day. Ask questions when you do not understand something or feel it is not clear. You want to go away from the course each day confident that you understood the day's work.

Practice exams and exam questions are the best way to test your knowledge of the CCNA course material. Don't rush yourself but at the same time do not procrastinate and put the exam off because you want to do it while all the information from the course is still fresh in your mind.

It is a tough exam and not everyone passes it the first time around, so do not feel bad if you do not pass on your first try. Take note of the sections you did not do well on, as they will be listed on the test scores you will receive once the exam has finished. When you re-study for the exam make sure you pay special attention to the areas you did not do well on. Find similar test questions and go over them until you feel confident about your knowledge of the material.

Join all the study groups that are offered on the Cisco Learning Network and join the interactive forums. You will never be short of study buddies or help from trained, experienced Cisco professionals. Joining in will not only help you with your current Cisco certification but also set you up for help with your job once you are working as a networking engineer. You never know when you will need not only study help but professional help as well, and what better way to get help than in a Cisco environment?

Quick Recap Tips For Passing Your CCNA Exam

Create a Study Plan

The best way to create a study plan is on the PC and keep an updated printout that you can stick on your whiteboard or refrigerator. Keep it updated and remember to make it flexible, but not too flexible; you do not want to procrastinate.

Cisco Command Line Interface

Get to know the Cisco command-line interface as it is the basis for most networking engineer's work. There are a lot of great network simulators including a free one on the Cisco website to use. These network simulators help you simulate a networking environment to practice lab work and get hands-on experience.

Practice, Practice, Practice

Take practice exam tests every day. Go over all the exam questions you can get your hands on and remember to always do the DIKTA questions first. As soon as you have your course materials, sign up with Pearson Test Prep.

Prepare for Exam Day

Get yourself ready for your exam day so when it arrives, you are not as anxious. Pearson VUE website has all the information you need to get your exam kit ready.

Make sure you are well rested for at least two nights before the exam. You will need a clear head and to be alert.

Get some exercise before the test and stretch out in order to calm yourself. Nerves can make you make snap judgments and misread questions so make sure you are calm — breathe!

Keep a Clear Head

On the exam day, remember to do calming exercises and stretch, breath, and keep a clear mind.

Watch instructional videos on how to write the exam and jot down some key points while you are waiting for the instructions to finish.

During the exam, remember to read each question carefully and make sure you have answered every question before moving on to the next one, as you cannot go back to a previous question.

Keep an eye on the timer on the top right-hand corner of the screen during your test, but do not panic if you see the time running out. Panic is going to cause you to make silly mistakes.

If there is a technical problem or you need to leave the test for an emergency of any kind, remember to let it be known to the individual at the testing

center right away.

Good luck, stay confident, study hard, and pay attention to detail.

References

- 2nd International Semantic Web conference (ISWC2003). (n.d.). Retrieved from <http://www.w3c.org/>
- American National Standards Institute. (n.d.). Retrieved from <https://www.ansi.org/>
- CCNA Certification and Training Program. (2020). Retrieved from <https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/associate/ccna.html>
- Cisco Digital Network Architecture [PDF File]. (n.d.). Retrieved from <https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/digital-network-architecture/q-and-a-c67-736803.pdf>
- CCNA Exam v1.0 (200-301) [PDF File]. (n.d.). Retrieved from https://www.cisco.com/c/dam/en_us/training-events/le31/le46/cln/marketing/exam-topics/200-301-CCNA.pdf
- Cisco. (2020). File: Cisco logo blue 2016.SVG - Wikimedia Commons [Photograph]. Retrieved from https://commons.wikimedia.org/wiki/File:Cisco_logo_blue_2016.svg
- Cisco Certification. (n.d.). Retrieved from <https://home.pearsonvue.com/cisco.aspx>
- Cisco Learning Network. (n.d.). Retrieved from <https://learningnetwork.cisco.com/welcome#certrain>
- Cisco Next Level Certifications. (2020). Retrieved from <https://www.cisco.com/c/en/us/training-events/training-certifications/next-level-certifications.html>
- Cisco Packet Tracer. (n.d.). Retrieved from <https://www.netacad.com/courses/packet-tracer>
- Cisco Training and Certification Frequently Asked Questions [PDF File]. (2020, January 02). Retrieved from https://www.cisco.com/c/dam/en_us/training-events/training-certification-faqs.pdf

Cisco Virtual Internet Routing Lab. (n.d.). Retrieved from <http://virl.cisco.com/>

GNS3 The Software That Empowers Network Professionals. (n.d.). Retrieved from <https://www.gns3.com/>

IEEE Advanced Technology for Humanity. (n.d.). Retrieved from <https://www.ieee.org/>

IETF. (n.d.). Retrieved from <https://www.ietf.org/>

Implementing and Administering Cisco Solutions (CCNA) v1.0. (n.d.). Retrieved from <https://www.cisco.com/c/en/us/training-events/training-certifications/training/training-services/courses/implementing-and-administering-cisco-solutions-ccna.html>

ISO. (n.d.). Retrieved from <https://www.iso.org/home.html>

NetSim 12 Network Simulator. (n.d.). Retrieved from <https://www.boson.com/netsim-cisco-network-simulator>

Networking Standards. (n.d.). Retrieved from https://www.webopedia.com/Networks/Networking_Standards

Pearson Test Prep. (n.d.). Retrieved from <https://www.pearsontestprep.com/#/login>

Pearsons VUE Cisco Certifications. (n.d.). Retrieved from <https://home.pearsonvue.com/cisco>

Software-Defined Access 1.0 [PDF File]. (n.d.). Retrieved from <https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/software-defined-access/white-paper-c11-740585.pdf>

Stagira. (2011). File:Hop-count-trans.png - Wikimedia Commons [Photograph]. Retrieved from <https://commons.wikimedia.org/wiki/File:Hop-count-trans.png>