Solutions Security Strategies

RC:1270765

SEC-CONCEPTS NETWORKS®

It's Possible

Consultancy | Solutions | Security | Strategies

CISCO

CERTIFICATIONS

- ROUTING & SWITCHING
- SERVICE PROVIDER
- DATA CENTRE
- INDUSTRIAL
- CYBER OPs.
- SECURITY
- DESIGN

CCNA | CCNP | CCIE

PROGRAMME GUIDE

CISCO CERTIFICATIONS PROGRAMME GUIDE

CISCO CERTIFICATIONS

Cisco certifications validate your ability to use the best-in-class networking and business communications devices from Cisco Systems. The "Cisco Career Certification" program offers a diverse range of credentials that bring measurable rewards to network professionals and the companies that employ them. Cisco certifications improve your understanding of networking in more than just Cisco products; throughout the certification learning process, candidates will develop a complete understanding of IT networking and how different network topologies interact to form a secure and efficient network. This "big picture" knowledge is beneficial in any networking role, and it's one of the many reasons Cisco certifications are in consistent demand, even at companies with few Cisco products. The latest generation of Cisco certifications was designed to be more compatible with the day-to-day activities of computer networking professionals, thus Cisco certification candidates can quickly acquire the credentials that prove their job-specific expertise to hiring managers.

5 LEVELS OF CISCO CERTIFICATION

This newest generation of Cisco certifications features five levels of general IT certification; from lowest to highest the Cisco certification levels are: **Entry, Associate, Professional, Expert and Architect.**

8 PATHS OF CISCO CERTIFICATION

Within the five levels of Cisco certifications, the Cisco Career Certification program features various paths (a.k.a. tracks) so you can match your Cisco learning path to your specific job role or industry. The eight Paths of Cisco certifications are:

Routing and Switching : This is the Cisco Certification path for Network Professionals who Install and Support Cisco networks containing LAN and WAN Routers and Switches.

Design: The Design Cisco Certification path is aimed at Network Professionals who Design Cisco networks in which LAN and WAN routers and switches reside.

Network Security: This is the Cisco Certification path for Network Professionals who Design and Implement Cisco Secure Networks.

Service Provider: This Cisco Certification path is aimed at Network Professionals that work with Infrastructure or Access Solutions in a Cisco environment - primarily in the telecommunications arena.

Service Provider Operations: This is the Cisco Certification path for Network Professionals who Manage, Maintain, and Troubleshoot complex Service Provider Networks.

Storage Networking: This Cisco Certification path is for Network Professionals who Implement Storage Solutions over extended
networks utilizing multiple transport options.

Voice: The Voice Cisco Certification path is for Network Professionals who Install and Maintain Voice over IP (VoIP) Networks.

Wireless: The Wireless Cisco Certification path is aimed at Network Professionals who Configure, Implement, and Support Wireless Networks.

BENEFITS OF CISCO CERTIFICATION

· Cisco certified professionals are among the highest paid IT professionals in the world.
· Cisco certifications validate skills in networking, one of the fastest growing and most versatile IT domains.
· According to a Fairfield Research survey, CCNA certification gives on average of 16.7% salary increase.
· Industry data proves that each Cisco certification earned brings an increase in the IT professional's salary.
· Getting Cisco certified opens the door to exciting and lucrative IT careers in the government and military.
· Resumes with Cisco certifications grab the attention of information technology recruiters and employers.
· Cisco certified professionals gain access to a global community of like-minded network professionals.

CCNA ROUTING AND SWITCHING CERTIFICATIONS

OVERVIEW

Increasing Demand for Practical Network Skills As the network grows in complexity, so does the need for training for those who implement and manage network infrastructure and solutions. A skills gap emerges when technology outpaces professional skills development. To fill this talent gap, Cisco continues to develop training and certification products that help our customers be more successful using the network and the solutions that ride on top of the network—solutions like voice communications, video services and collaboration environments.

JOB-READY PRACTICAL SKILLS

The Cisco CCNA Routing and Switching, CCNP® Routing and Switching, and CCIE® Routing and Switching certification programs are practical, relevant, and job-ready certification curricula aligned closely with the specific tasks expected of these in demand professionals. Cisco realizes that the network professional increasingly must focus on design, configuration, and support responsibilities as the technical consultant, specialist or expert on a networking team. Therefore, the Cisco curriculum is specific to the best practices of network administrators, engineers, and experts using the latest Cisco network solutions.

BEST PRACTICES IN NETWORKING

Achieving CCNA (Cisco Certified Network Associate) Routing and Switching certification (formerly known as CCNA) is the first step in helping you prepare for a career in networking. Pursuing this certification will help improve your skill sets, and provide you with ability to manage and optimize network systems. CCNA Routing and Switching focuses on network infrastructure, mainly routing and switching, but it also includes wireless access, security, and connectivity to branch offices using WAN.

Cisco Certified Network Associate (CCNAv3)

The Cisco Certified Network Associate (CCNA) Routing and Switching composite **Exam (200-125)** is an assessment that is associated with the **CCNA Routing and Switching certification**. This exam tests a candidate's knowledge and skills related to network fundamentals, LAN switching technologies, IPv4 and IPv6 routing technologies, WAN technologies, infrastructure services, infrastructure security, and infrastructure management.

Prerequisites

Before taking the CCNAX course, learners should be familiar with:

- Basic computer literacy
- Basic PC operating system navigation skills
- Basic Internet usage skills
- Basic IP address knowledge
- Good understanding of network fundamentals

Course Content

This course consists of Interconnecting Cisco Networking Devices, Part 1 (ICND1) and Interconnecting Cisco Networking Devices, Part 2 (ICND2) content merged into a single course. Overlapping content between ICND1 and ICND2 is eliminated and content is rearranged for the purpose of the course flow. Students will learn how to install, operate, configure, and verify a basic IPv4 and IPv6 network, including configuring a LAN switch, configuring an IP router, connecting to a WAN, and identifying basic security threats. It also includes more in-depth topics that teach learners how to perform basic troubleshooting steps in enterprise branch office networks, preparing students for the Cisco CCNA certification.
Upon completing this course, you will have the skills and knowledge to: Install, operate, and troubleshoot a medium-sized network, including
connecting to a WAN and implementing network security.
Describe the effects of new technologies such as IoE, IoT, IWAN, and SDN on network
evolution.

CCNA R&Sv3 Course Outline

Module 1: Building a Simple Network
Module 2: Establishing Internet Connectivity
Module 3: Summary Challenge
Module 4: Implementing Scalable Medium Sized Network
Module 5: Introducing IPv6
Module 6: Troubleshooting Basic Connectivity
Module 7: Implementing Network Device Security
Module 8: Implementing an EIGRP-Based Solution
Module 9: Summary Challenge
Module 10: Implement a Scalable OSPF-Based Solution
Module 11: Implementing Wide-Area Networks
Module 12: Network Device Management
Module 13: Summary Challenge

Course Name:	CCNA: Routing and Switching
Batch Course Length:	15 days
Batch Course Availability:	1st & 15th of Every Month
Number of Exams:	1
Hours per day:	6hrs
Certifications:	CCNA: Routing and Switching
Training Locations:	Ilorin (Tanke & Geri-Alimi)
1-on-1 Course Length:	Students Determine
1-on-1 Training Location:	Ilorin (Unity) & Abuja (Maitama)

CISCO DESGN (CCDA) CERTIFICATIONS

Cisco DESGN v3 - Designing for Cisco Internetwork Solutions (CCDA) Certification

Enterprise environments require networks designed for performance, availability, and scalability with the flexibility to meet rapidly evolving demands. To meet these challenges head on, skilled IT professionals are needed with up-to-date, fundamental network design skills. For network design engineers, system engineers, and sales engineers and individuals looking to build and validate Cisco network design fundamental knowledge the Cisco CCDA certification program focuses on design methodologies and objectives, addressing and routing protocols, and network expansion considerations within basic campus, data center, security, voice, and wireless networks.

This course requires a foundation or apprentice knowledge of network design for Cisco enterprise network architectures. CCDA certified professionals can design routed and switched network infrastructures and services involving LAN/WAN technologies for SMB or basic enterprise campus and branch networks. In addition to general approaches and technologies for network design, this course promotes Cisco solutions in designing and implementing scalable internetworks. Among specific goals is the promotion of the modular approach to network design.

Prerequisites

It is recommended, but not required, that students have the following knowledge and skills:

• A Cisco CCNA certification and practical experience with deploying and operating networks based on Cisco network devices and Cisco IOS.
• BCMSN level knowledge of wireless and QoS topics.
• Complete the Building Cisco Multilayer Switched Networks (BCMSN) course.

Course Content

Upon completing this course, you will be able to meet these objectives:

• Describe and apply network design methodologies.
• Describe and apply network design concepts of modularity and hierarchy.
• Design a resilient and scalable Campus network.
• Design a resilient and scalable connectivity between parts of your Enterprise network.
• Design connectivity to the Internet and internal routing for your network.
• Integrate collaboration and wireless infrastructure into your core network.
• Create scalable IPv4 and IPv6 addressing.
• Describe what software defined networks are and describe example solutions.

Cisco DESGN v3 Course Outline

Module 1: Design Methodologies
Module 2: Network Design Objectives
Module 3: Campus Network
Module 4: Enterprise Network Design
Module 5: Design of Internal Routing and Connecting to the Internet
Module 6: Expanding the Existing Network
Module 7: IP Addressing Design

Course Name:	Cisco DESGN v3
Batch Course Length:	15 days
Batch Course Availability:	1st & 15th of Every Month
Number of Exams:	1
Hours per day:	6hrs
Certifications:	CCDA
Training Locations:	Ilorin (Tanke & Geri-Alimi)
1-on-1 Course Length:	Students Determine
1-on-1 Training Location:	Ilorin (Unity) & Abuja (Maitama)

CISCO DATA CENTER CERTIFICATIONS

Cisco Data Center Networking (DCICN) and Technologies (DCICT)
Agility is the hallmark of today's successful data center. Built for rapid application deployment and supported by a highly elastic infrastructure, the data center has become core to businesses competing in our digital era. CCNA Data Center certification provides the confidence and nimbleness you need to install, configure, and maintain data center technology. Gain grounding in data center infrastructure, data center networking concepts and technologies, storage networking, unified computing, network virtualization, data center automation and orchestration, and Cisco Application Centric Infrastructure (ACI).

Introducing Cisco Data Center Networking (DCICN) v6.1 is a fifteen-day instructor-led course is designed to help students prepare for the Cisco CCNA® Data Center certification and for associate-level data center roles. The course covers foundational knowledge, skills, and technologies including network protocols and host-to-host communication, data center networking concepts and technologies, data center storage networking, and Cisco Unified Computing System (UCS) architecture.

Introducing Cisco Data Center Technologies (DCICT) v6.1 is a fifteen-day instructor-led course that is designed to help students prepare for the Cisco CCNA Data Center certification and for associate-level data center roles. The course covers foundational knowledge, skills, and technologies including data center network virtualization, unified computing, data center automation and orchestration, and Cisco Application Centric Infrastructure (ACI). The hands-on lab exercises focus on configuring features on Cisco Nexus Operating System (NX-OS), Cisco Unified Computing System (UCS), and Cisco UCS Director.

Prerequisites
It is recommended that a learner has the following knowledge and skills before attending this course:
• Good understanding of networking protocols
• Good understanding of the VMware environment
• Basic computer literacy
• Basic knowledge of Microsoft Windows operating systems
• Basic Internet usage skills

Course Content
Upon completion of this course, you will be able to: • Describe and identify data center network protocols and host-to-host communication.
• Describe basic data center networking concepts and use the Cisco NX-OS command-line interface and implement VLANs, trunks, and port channels.
• Describe advanced data center networking concepts, implement multilayer switching, and perform basic configuration: protocols
(OSPF, EIGRP, HSRP); AAA on Cisco NX-OS devices and secure remote administration; and access control lists.
• Describe and compare basic data center storage connectivity options and configure VSANs.
• Describe advanced data center storage and configure zoning, NPV mode, and NPIV on Cisco Nexus and Cisco MDS switches.
• Identify the components of Cisco UCS architecture and use the Cisco UCS Manager GUI
• Describe and configure Cisco UCS
• Describe and configure Cisco data center virtualization
• Describe and configure Cisco data center networking
• Describe and configure Cisco automation and orchestration
• Describe and verify Cisco ACI

Cisco Data Center Course Outline
Module 1: Network Protocols and Host-to-Host Communication
Module 2: Basic Data Center Networking Concepts
Module 3: Advanced Data Center Networking Concepts
Module 4: Basic Data Center Storage
Module 5: Advanced Data Center Storage
Module 6: Cisco UCS Architecture
Module 7: Cisco Data Center Network Virtualization
Module 8: Cisco Data Center Network Technologies Configuration
Module 9: Cisco Unified Computing System
Module 10: Data Center Automation and Orchestration
Module 11: Cisco Application-Centric Infrastructure

Course Name:	Cisco Data Center
Batch Course Length:	15 days
Batch Course Availability:	1st & 15th of Every Month
Number of Exams:	2
Hours per day:	6hrs
Certifications:	**DCICN** & **DCICT**
Training Locations:	Ilorin (Tanke & Geri-Alimi)
1-on-1 Course Length:	Students Determine
1-on-1 Training Location:	Ilorin (Unity) & Abuja (Maitama)

CCNA SECURITY CERTIFICATIONS

Cisco Certified Network Associate Security (CCNA Security) Certification

Cisco Certified Network Associate Security (CCNA Security) validates associate-level knowledge and skills required to secure Cisco networks. With a CCNA Security certification, a network professional demonstrates the skills required to develop a security infrastructure, recognize threats and vulnerabilities to networks, and mitigate security threats. The CCNA Security curriculum emphasizes core security technologies, the installation, troubleshooting and monitoring of network devices to maintain integrity, confidentiality and availability of data and devices, and competency in the technologies that Cisco uses in its security structure.

Implementing Cisco Network Security (IINS) v3.0 is a 15-day instructor-led course presented by Cisco Learning Partners to end users and channel partner customers. The course focuses on security principles and technologies, using Cisco security products to provide hands-on examples. Using instructor-led discussions, extensive hands-on lab exercises, and supplemental materials, this course allows learners to understand common security concepts, and deploy basic security techniques utilizing a variety of popular security appliances within a "real-life" network infrastructure.

Prerequisites

• Skills and knowledge equivalent to those learned in Interconnecting Cisco Networking Devices Part 1 (ICND1).
• Working knowledge of the Windows operating system.
• Working knowledge of Cisco IOS networking and concepts.

Course Content

Upon completion of the course, students will have the knowledge and skills to:
• Describe common network security concepts.
• Secure routing and switching infrastructure.
• Deploy basic authentication, authorization and accounting services.
• Deploy basic firewalling services.
• Deploy basic site-to-site and remote access VPN services.
• Describe the use of more advanced security services such as intrusion protection, content security and identity management.

CCNA Security Course Outline

Module 1: Course Introduction
Module 2: Network Security Concepts
Module 3: Secure Network Devices
Module 4: Firewalls
Module 5: Virtual Private Networks
Module 6: Advanced Topics

Course Name:	IINS
Batch Course Length:	15 days
Batch Course Availability:	1st & 15th of Every Month
Number of Exams:	1
Hours per day:	6hrs
Certifications:	CCNA Security
Training Locations:	Ilorin (Tanke & Geri-Alimi)
1-on-1 Course Length:	Students Determine
1-on-1 Training Location:	Ilorin (Unity) & Abuja (Maitama)

CCNA SERVICE PROVIDER CERTIFICATIONS

Cisco Certified Network Associate Service Provider (CCNA SP: SPNGN1 and SPNGN2) Certification
Cisco Certified Network Associate Service Provider (CCNA SP) certification is for service provider network engineers, technicians and designers who focus on the latest in Service Provider industry core networking technologies and trends. With the ability to configure, implement, and troubleshoot baseline Cisco Service Provider Next-Generation networks, CCNA SP certified individuals deploy, maintain and improve carrier-grade network infrastructures.

The Building Cisco Service Provider Next-Generation Networks, Part 1 & Part 2 course is associated with the CCNA Service Provider certification. The course is a 15-day Instructor Lead Training course that provides network engineers and technicians with the basic knowledge and skills necessary to support a service provider network. The course provides knowledge of the major components of a network and helps learners to understand how service provider networks function. The course introduces IP Next-Generation Network (IP NGN) architecture that helps service providers to build modern, scalable and reliable networks.

Prerequisites
• Skills and knowledge equivalent to those learned in Interconnecting Cisco Networking Devices Part 1 (ICND1).
• Working knowledge of the Windows operating system.
• Working knowledge of Cisco IOS networking and concepts.
• **SPNGN1** for **SPNGN2.**

Course Content
• The course also includes classroom activities with remote labs that are useful to gain practical skills for deploying Cisco IOS / IOS XE and Cisco IOS XR software features to operate and support service provider networks.

CCNA SP Course Outline
Module 1: IP Fundamentals
Module 2: Basic LAN Switching
Module 3: Basic IP Routing
Module 4: Connectivity Technologies
Module 5: Network Management and Security
Module 6: Service Provider Network Architecture
Module 7: Advanced LAN Switching
Module 8: Internal Service Provider Traffic Forwarding
Module 9: External Service Provider Routing
Module 10: ACLs and IP Address Translation
Module 11: Cisco Service Provider Platforms

Course Name:	CCNA SP
Batch Course Length:	15 days
Batch Course Availability:	1st & 15th of Every Month
Number of Exams:	2
Hours per day:	6hrs
Certifications:	**SPNGN1** & **SPNGN2**
Training Locations:	Ilorin (Tanke & Geri-Alimi)
1-on-1 Course Length:	Students Determine
1-on-1 Training Location:	Ilorin (Unity) & Abuja (Maitama)

CCNA INDUSTRIAL CERTIFICATIONS

Cisco Certified Network Associate Industrial (CCNA Industrial) Certification

The Cisco Certified Network Associate Industrial (CCNA Industrial) certification is for plant administrators, control system engineers and traditional network engineers in the manufacturing, process control, and oil and gas industries, who will be involved with the convergence of IT and Industrial networks. This certification provides candidates the necessary skills to successfully implement and troubleshoot the most common industry standard protocols while leveraging best practices needed for todays connected networks. Combining theoretic knowledge with practical lab exercises, this curriculum provides the real-world skills that allow information technology (IT) and operational technology (OT) professionals to ensure that their current infrastructures are maximized while developing a converged platform for flexibility to support future business outcomes.

This course is a lab-based course which helps students with the foundational skills needed for the management and administration of networked industrial control systems. It helps plant administrators, control system engineers and traditional network engineers understand networking technologies that are needed in todays connected plants and enterprises. This course also helps prepare for the Cisco Industrial Networking Specialist Certification exam (200-401) and earn the Cisco Industrial Networking Specialist certification. This course is job-role specific and enables you to achieve competency and skills to configure, maintain, and troubleshoot industrial network systems while helping to ensure network availability, reliability, and Internet security throughout your company.

Prerequisites

It is recommended that a learner has the following knowledge and skills before attending this course:
- Describe network fundamentals and build simple LANs.
- Establish Internet connectivity.
- Manage network device security.
- Expand small- to medium-sized networks with WAN connectivity.
- Describe IP basics.
- Identify Cisco industrial networking solutions.
- Describe Cisco Industrial Ethernet switches, Rockwell Automation Stratix switches, and Cisco Connected Grid switches and routers.
- Interpret design and drawings.
- Recognize zone topologies.
- Install and deploy industrial network components.
- Perform basic maintenance tasks on the network.
- Troubleshoot network and control issues

Course Content

Upon completion of this course, you will be able to:
- Understand the functions of the OSI layers and TCP/IP model.
- Recognize the difference between enterprise and industrial networks.
- Troubleshoot the common issues that are found in Layers 1, 2, and 3 of the OSI model.
- Describe the functions and components of EtherNet/IP protocol.
- Configure and troubleshoot EtherNet/IP on Cisco and Stratix switches.
- Describe the functions and components of the PROFINET protocol.
- Configure and troubleshoot PROFINET protocol on Cisco Industrial Ethernet devices.
- Identify common network threats and resolutions, and configure basic security components (access lists and AAA features).
- Configure a wireless network within an industrial environment.

CCNA Industrial Course Outline

Module 1: Industrial Networking Concepts and Components
Module 2: General Troubleshooting Issues
Module 3: EtherNet/IP
Module 4: Troubleshooting EtherNet/IP
Module 5: PROFINET
Module 6: Configuring PROFINET
Module 7: Troubleshooting PROFINET
Module 8: Exploring Security Concerns
Module 9: 802.11 Industrial Ethernet Wireless Networking

Course Name:	CCNA Industrial
Batch Course Length:	15 days
Batch Course Availability:	1st & 15th of Every Month
Number of Exams:	1
Hours per day:	6hrs
Certifications:	Cisco Industrial Networking Specialist
Training Locations:	Ilorin (Tanke & Geri-Alimi)
1-on-1 Course Length:	Students Determine
1-on-1 Training Location:	Ilorin (Unity) & Abuja (Maitama)

CCNA CYBER OPs. CERTIFICATIONS

Cisco Certified Network Associate (CCNA) Cyber OPs Certification

Today's organizations are challenged with rapidly detecting cybersecurity breaches and effectively responding to security incidents. Teams of people in Security Operations Centers (SOC's) keep a vigilant eye on security systems, protecting their organizations by detecting and responding to cybersecurity threats. The CCNA Cyber Ops certification prepares candidates to begin a career working with associate-level cybersecurity analysts within security operations centers.

Implementing Cisco CyberSecurity Operations (SECOPS) 1.0

This course allows learners to understand how a Security Operations Center (SOC) functions and the introductory-level skills and knowledge needed in this environment. It focuses on the introductory-level skills needed for a SOC Analyst at the associate level. Specifically, understanding basic threat analysis, event correlation, identifying malicious activity, and how to use a playbook for incident response.

Understanding Cisco CyberSecurity Fundamentals (SECFND) 1.0

The course helps to prepare students for beginning and associate level roles in cybersecurity operations. The course focuses on security principles and technologies, using Cisco security products to provide hands-on examples. Using instructor-led discussions, extensive hands-on lab exercises, and supplemental materials, this course allows learners to understand common security concepts, and start to learn the basic security techniques used in a Security Operations Center (SOC) to find threats on a network using a variety of popular security tools within a real-life network infrastructure.

Prerequisites

It is recommended, but not required, that students have the following knowledge and skills:

- Skills and knowledge equivalent to those learned in Interconnecting Cisco Networking Devices Part 1 (ICND1).
- Working knowledge of the Windows operating system.
- Working knowledge of Cisco IOS networking and concepts.
- Working knowledge of the Windows operating system.
- Working knowledge of the Linux operating system.
- Basic IPv4 and IPv6 addressing knowledge

Course Content

- Define a SOC and the various job roles in a SOC.
- Understand SOC infrastructure tools and systems.
- Learn basic incident analysis for a threat centric SOC.
- Explore resources available to assist with an investigation.
- Explain basic event correlation and normalization.
- Describe common attack vectors.
- Learn how to identifying malicious activity.
- Understand the concept of a playbook.
- Describe and explain an incident respond handbook.
- Define types of SOC Metrics.
- Understand SOC Workflow Management system and automation.
- Describe, compare and identify various network concepts.
- Fundamentals of TCP/IP.
- Describe and compare fundamental security concepts.
- Describe network applications and the security challenges.
- Understand basic cryptography principles.
- Understand endpoint attacks, including interpreting log data to identify events in Windows and Linux.
- Develop knowledge in security monitoring, including identifying sources and types of data and events.

CCNA Cyber OPs. Course Outline

Module 1: SOC Overview
Module 2: Security Incident Investigations
Module 3: SOC Operations
Module 4: Network Concepts
Module 5: Security Concepts
Module 6: Cryptography /IP
Module 7: Host-Based Analysis
Module 8: Security Monitoring
Module 9: Attack Methods

Course Name:	CCNA Cyber OPs.
Batch Course Length:	15 days
Batch Course Availability:	1st & 15th of Every Month
Number of Exams:	2
Hours per day:	6hrs
Certifications:	**SECOPS** & **SECFND**
Training Locations:	Ilorin (Tanke & Geri-Alimi)
1-on-1 Course Length:	Students Determine
1-on-1 Training Location:	Ilorin (Unity) & Abuja (Maitama)

CCNP ROUTING & SWITCHING CERTIFICATIONS

Cisco Certified Network Professional (CCNP) Routing and Switching Certification

Cisco Certified Network Professional (CCNP) Routing and Switching certification validates the ability to plan, implement, verify and troubleshoot local and wide-area enterprise networks and work collaboratively with specialists on advanced security, voice, wireless and video solutions. The CCNP Routing and Switching certification is appropriate for those with at least one year of networking experience who are ready to advance their skills and work independently on complex network solutions. Those who achieve CCNP Routing and Switching have demonstrated the skills required in enterprise roles such as network engineer, support engineer, systems engineer or network technician. The routing and switching protocol knowledge from this certification will provide a lasting foundation as these skills are equally relevant in the physical networks of today and the virtualized network functions of tomorrow.

Required Exams (3):

- Implementing Cisco IP Routing (300-001 ROUTE). ROUTE v2.0 includes major updates and follows an updated blueprint. However, note that this course does not cover all items listed on the blueprint. Some older topics have been removed or simplified, while several new IPv6 routing topics have been added. Course content has been adapted to Cisco IOS Software Release 15 and technically updated. Course also introduces new type of labs, called discovery labs. Discovery labs are instructor guided lab through which student explores new topics in an interactive way. All labs are developed only as virtual labs. To get the full course experience, you should cover everything, including Introduction, Discovery labs, Summary, and Module Self-Check.

Prerequisites

The knowledge and skills that a learner must have before attending this Curriculum are as follows:

- Describing network fundamentals.
- Establishing Internet and WAN connectivity (IPv4 and IPv6).
- Managing network device security.
- Operating a medium-sized LAN with multiple switches, supporting VLANs, trunking, and spanning tree.
- Troubleshooting IP connectivity (IPv4 and IPv6).
- Configuring and troubleshooting EIGRP and OSPF (IPv4 and IPv6).
- Configuring devices for SNMP, Syslog, and NetFlow access.
- Managing Cisco device configurations, Cisco IOS images, and licenses.

It is highly recommended that this course be taken after the following Cisco courses:.

- Interconnecting Cisco Networking Devices v2.0, Part 1 (ICND1 v2.0) and Part 2 (ICND2 v2.0).
- Interconnecting Cisco Networking Devices: Accelerated version 2.0 (CCNAX v2.0)

Course Content

Upon completing this course, the learner will be able to meet these overall objectives:

• Describe routing protocols, different remote connectivity options and their impact on routing and implement RIPng.
• Configure EIGRP in IPv4 and IPv6 environment.
• Configure OSPF in IPv4 and IPv6 environment.
• Implement route redistribution using filtering mechanisms.
• Implement path control using policy based routing and IP SLA.
• Implement enterprise Internet connectivity.
• Secure Cisco routers according to best practices and configure authentication for routing protocols.

ROUTE Course Outline

Module 1: Basic Network and Routing Concepts.
Module 2: EIGRP Implementation.
Module 3: OSPF Implementation.
Module 4: Configuration of Redistribution.
Module 5: Path Control Implementation.
Module 6: Enterprise Internet Connectivity.
Module 7: Routers and Routing Protocol Hardening.

- Implementing Cisco IP Switched Networks (300-115 SWITCH). SWITCH v2.0, includes major updates and follows an updated blueprint. However, note that this course does not cover all items listed on the blueprint. Some older topics have been removed or simplified, while several new IPv6 routing topics have been added. Course content has been adapted to Cisco IOS Software Release 15 and technically updated. Course also introduces new type of labs, called discovery labs. Discovery labs are instructor guided lab through which student explores new topics in an interactive way. All labs are developed only as virtual labs. To get the full course experience, you should cover everything, including Introduction, Discovery labs, Summary, and Module Self-Check.

Prerequisites

The knowledge and skills that a learner must have before attending this Curriculum are as follows:

• Describing network fundamentals.
• Establishing Internet and WAN connectivity (IPv4 and IPv6).
• Managing network device security.
• Operating a medium-sized LAN with multiple switches, supporting VLANs, trunking, and spanning tree.
• Troubleshooting IP connectivity (IPv4 and IPv6).
• Configuring and troubleshooting EIGRP and OSPF (IPv4

and IPv6).
• Configuring devices for SNMP, Syslog, and NetFlow access.
• Managing Cisco device configurations, Cisco IOS images, and licenses.
It is highly recommended that this course be taken after the following Cisco courses:
• Interconnecting Cisco Networking Devices v2.0, Part 1 (ICND1 v2.0) and Part 2 (ICND2 v2.0).
• Interconnecting Cisco Networking Devices: Accelerated version 2.0 (CCNAX v2.0).

Course Content
Upon completing this course, the learner will be able to meet these overall objectives:
• Describe the hierarchical campus structure, basic switch operation, use of SDM templates, PoE, and LLDP.
• Implement VLANs, trunks, explain VTP, implement DHCP in IPv4 and IPv6 environment, and configure port aggregation.
• Implement and optimize STP mechanism that best suits your network - PVSTP+, RPVSTP+, or MSTP.
• Configure routing on a multilayer switch.
• Configure NTP, SNMP, IP SLA, port mirroring, and verify StackWise and VSS operation.
• Implement First Hop redundancy in IPv4 and IPv6 environments.
• Secure campus network according to recommended practices.

SWITCH Course Outline
Module 1: Basic Concepts and Network Design.
Module 2: Campus Network Architecture.
Module 3: Spanning Tree Implementation.
Module 4: Configuring Inter-VLAN Routing.
Module 5: Implementing High Availability Networks.
Module 6: First Hop Redundancy Implementation.
Module 7: Campus Network Security.

- Troubleshooting and Maintaining Cisco IP Networks (300-135 TSHOOT). TSHOOT v2.0, includes major updates and follows an updated blueprint. However, note that this course does not cover all items listed on the blueprint. Some older topics have been removed or simplified, while several new IPv6 routing topics have been added. Course content has been adapted to Cisco IOS Software Release 15 and technically updated. Course also introduces new type of labs, called discovery labs. Discovery labs are instructor guided lab through which student explores new topics in an interactive way. All labs are developed only as virtual labs. To get the full course experience, you should cover everything, including Introduction, Discovery labs, Summary, and Module Self-Check.

Prerequisites
Prior to attending this course students should have the knowledge of and experience with the implementation and verification of enterprise routing and switching technologies as offered by the Implementing Cisco Switched Networks (SWITCH) v2.0 and Implementing Cisco IP Routing (ROUTE) v2.0 courses or equivalent skills and knowledge. This includes knowledge and experience of the following technologies:
• Layer 2 switching VLANs, VLAN access control lists, port security Switch security issues.
• Link aggregation protocols.
• Spanning Tree Protocol (STP).
• Inter-VLAN routing solutions.
• First Hop Redundancy Protocols (FHRPs) - HSRP, VRRP, and GLBP.
• Branch office operations.
• Enhanced Interior Gateway Routing Protocol (EIGRP).
• Open Shortest Path First (OSPF).
• Layer 3 path control.
• Redistribution.
• Internal and External Border Gateway Protocol (BGP).
• IPv6 Networking.

Course Content
Upon completing this course, the learner will be able to meet these overall objectives:
• Describe the troubleshooting tools and methodologies that are used to identify and resolve issues in complex enterprise networks.
• Isolate and fix the network issues that your company, SECHNIK Networking Ltd., is facing.
• Isolate and fix the network issues that your customer, TINC Garbage Disposal Ltd., is facing.
• Isolate and fix the network issues that your customer, PILE Forensic Accounting Ltd., is facing.
• Isolate and fix the network issues that your customer, Bank of POLONA Ltd., is facing.
• Isolate and fix the network issues that your customer, RADULKO Transport Ltd., is facing.

TSHOOT Course Outline
Module 1: Tools and Methodologies of Troubleshooting.
Module 2: Troubleshooting at SECHNIK Networking Ltd.
Module 3: Troubleshooting at TINC Garbage Disposal Ltd.
Module 4: Troubleshooting at PILE Forensic Accounting Ltd.
Module 5: Troubleshooting at Bank of POLONA Ltd.
Module 6: Troubleshooting at RADULKO Transport Ltd.

Course Name:	CCNP R&S
Batch Course Length:	30 days
Batch Course Availability:	1st & 15th of Every Month
Number of Exams:	3
Hours per day:	6hrs
Certifications:	**ROUTE**, **SWITCH**, and **TSHOOT**
Training Locations:	Ilorin (Tanke & Geri-Alimi)
1-on-1 Course Length:	Students Determine
1-on-1 Training Location:	Ilorin (Unity) & Abuja (Maitama)

Call/WhatsApp: 08039134906
training@sec-conceptsnetworks.com
www.sec-conceptsnetworks.com

CCDP CERTIFICATIONS

Cisco Certified Design Professional (CCDP) Certification
Enterprise environments require networks designed for performance, availability and scalability to achieve outcomes. Seasoned IT professionals with progressive end-to-end network design expertise are crucial to ensure networks deliver to today's requirements while future proofing investments. For Senior Network Design Engineers, Principle System Engineer, Network/Solution Architects and CCDA professionals looking to build upon your fundamental Cisco network design expertise the Cisco CCDP certification program focuses on advanced addressing and routing protocols, WANs, services virtualization, and integration strategies for multi-layered Enterprise architectures.

Required Exams (3):
- Implementing Cisco IP Routing (300-001 ROUTE). ROUTE v2.0 *(See CCNP R&S)*
- Implementing Cisco IP Switched Networks (300-115 SWITCH). SWITCH v2.0 *(See CCNP R&S)*
- Designing Cisco Network Service Architectures (300-320 ARCH).
Designing Cisco Network Service Architectures (ARCH) v3.0 course enable students to perform the conceptual, intermediate, and detailed design of a network infrastructure that supports desired network solutions over intelligent network services, to achieve effective performance, scalability, and availability. ARCH enables learners, applying solid Cisco network solution models and recommended design practices, to provide viable, stable enterprise internetworking solutions. The course presents concepts and examples necessary to design converged enterprise networks. New in v3.0 is the addition of a content addressing software defined networks (SDN). Building on the Designing for Cisco Internetwork Solutions (DESGN) v3.0 course, in the ARCH course the students will learn additional aspects of modular campus design, advanced addressing and routing designs, WAN service designs, enterprise data center, and security designs.

Prerequisites
Before taking the ARCH course, learners should be familiar with:
• Internetworking technologies, Cisco products, and Cisco IOS features.
• Cisco Certified Network Associate (CCNA®) level-of-knowledge.
• Designing for Cisco Internetwork Solutions (DESGN) level-of-knowledge.
• Implementing Cisco IP Switched Networks (SWITCH) level-of-knowledge.
• Implementing Cisco IP Routing (ROUTE) level-of-knowledge

Course Content
Upon completing this course, you will be able to meet these objectives:
• Design internal routing for enterprise network.
• Design BGP routing for enterprise network.
• Design enterprise WAN connectivity.
• Design enterprise data center integration.
• Design security services in an enterprise network.
• Design QoS for optimized user experience.
• Design enterprise transition to IPv6.
• Design enterprise multicast network.

ARCH Course Outline
Module 1: Enterprise Connectivity and High-Availability
Module 2: BGP Design
Module 3: Wide Area Networks Design
Module 4: Enterprise Data Center Integration
Module 5: Design Security Services
Module 6: Design QoS for Optimized User Experience
Module 7: Transition to IPv6
Module 8: IP Multicast Design

Course Name:	CCDP
Batch Course Length:	30 days
Batch Course Availability:	1st & 15th of Every Month
Number of Exams:	3
Hours per day:	6hrs
Certifications:	**ROUTE, SWITCH,** and **ARCH**
Training Locations:	Ilorin (Tanke & Geri-Alimi)
1-on-1 Course Length:	Students Determine
1-on-1 Training Location:	Ilorin (Unity) & Abuja (Maitama)

CCNP DATA CENTER CERTIFICATIONS

CCNP Data Center Certification

The CCNP Data Center certification and training program offers comprehensive certification and Professional-level skills focused on the data center solutions, technologies and best practices to design, implement, and manage a modern data center infrastructure. IT practitioners who are Cisco trained and certified are uniquely qualified for key roles in complex data center environments, with expertise utilizing technologies including policy-driven infrastructure, virtualization, automation and orchestration, unified computing, data center security, and integration of cloud initiatives. CCNP Data Center certified professionals are highly qualified for senior roles chartered with enabling digital business transformation initiatives.

Required Exams (4):

- Implementing Cisco Data Center Unified Computing (300-175 DCUCI).

Designing Cisco Data Center Unified Computing Infrastructure (DCIDUC) v6.1 is a course that focuses on data center design based on Cisco unified computing solutions. The course includes theoretical content, as well as design-oriented case studies and exercises. The course is designed to help students prepare for Cisco Channel Partner Data Center Program requirements and for professional-level data center roles. The course includes information on designing data centers with Cisco components and technologies, including infrastructure design, compute connectivity design, and compute resource parameters design.

Prerequisites

It is recommended that a learner has the following knowledge and skills before attending this course:
• Understanding of server system design and architecture.
• Familiarity with Ethernet and TCP/IP networking.
• Familiarity with SANs.
• Familiarity with Fibre Channel protocol.
• Understanding of Cisco Enterprise Data Center Architecture.
• Familiarity with hypervisor technologies (such as VMware).

Course Content

Upon completion of this course, you will be able to:
• Install the UCS B-Series system out of the box and deploy service profiles using pooled identities and service profile templates.
• Configure the UCS B-Series system for deployments using iSCSI and configure B- and C-Series systems for deployments using Fibre Channel for regular data access and booting.
• Configure and implement security mechanisms such as RBAC with Organizations and Locales, LDAP integration, trusted points, and key rings.
• Configure and implement monitoring with syslog and Call Home.
• Manage UCS Manager domains with UCS Central, manage multiple C-Series servers with Cisco IMC Supervisor, and interact with the UCS Manager XML API

DCUCI Course Outline

Module 1: Cisco Unified Computing System Implementation.
Module 2: SAN Storage Implementation for Cisco Unified Computing System.
Module 3: Automation.
Module 4: Unified Computing Security.
Module 5: Cisco Unified Computing System Automation.

- Implementing Cisco Data Center Infrastructure (300-165 DCII).

The focus of this skills-building course is on deploying, securing, operating, and maintaining the Cisco Unified Computing System (UCS) and UCS C-Series Rack Servers for use in data centers. The extensively hands-on course covers configuring and managing Cisco UCS servers using unified I/O networking for LAN and SAN connectivity, virtualizing server hardware identifiers to enable rapid recovery of server operating system images, automating UCS deployments using UCS Central Software and Cisco Integrated Management Controller (IMC) Supervisor, configuring fault tolerance, implementing role-based access control (RBAC), backing up and restoring system configurations, and using the monitoring and troubleshooting tools in Cisco UCS Manager and Cisco IMC.

Prerequisites

It is highly recommended that this course be taken after the following Cisco courses:
• Data center networking concepts.
• Data center storage concepts.
• Data center virtualization.
• Cisco Unified Computing System.
• Data center automation and orchestration with the focus on Cisco ACI and UCS Director.
• Identify products in the Cisco Data Center Nexus and MDS families.
• Describe network fundamentals and build simple LANs, including switching and routing

Course Content

Upon completing this course, you will be able to describe and use design-oriented knowledge for unified computing topics, including:
• Hardware and device virtualization.
• FEX options.
• Virtual networking and appliances.
• Management and orchestration.

• Cisco UCS C-Series and B-Series servers and use cases.
• Fabric interconnect connectivity.
• Hyperconverged and integrated system.
• Management systems, including Cisco UCS, VMware vCenter, and Cisco CloudCenter.
• Hadoop, SAP HANA, and IoT on Cisco UCS.
• Systemwide parameters.
• RBAC.
• Pools and policies for service profiles.
• Network-specific adapters and policies.
• Templates in Cisco UCS Manager.

DCII Course Outline

Module 1: Data Center Protocols.
Module 2: Layer 3 Switching Features in the Data Center.
Module 3: Data Center Infrastructure Security.
Module 4: Data Center Infrastructure Storage Fabric.
Module 5: FCoE Unified Fabric.
Module 6: Data Center Infrastructure Storage Services.
Module 7: Data Center Infrastructure Maintenance, Management, and Operations.

- Implementing Cisco Data Center Virtualization and Automation (300-170 DCVAI). AND

The focus of this skills-building course is on the implementation and deployment automation of Cisco Application Centric Infrastructure (ACI) and Cisco Nexus switches.

Prerequisites

It is recommended that a learner has the following knowledge and skills before attending this course:
• Describe data center networking concepts.
• Describe data center storage concepts.
• Describe data center virtualization..

Course Content

Upon completion of this course, you will be able to:
• Implement infrastructure virtualization solutions, such as VDC, VRFs, Cisco Nexus 1000v, and Cisco AVS.
• Identify programmability methods and program Cisco Nexus switches using XML, Python, and NX-API.
• Implement a Cisco ACI solution that provides fabric connectivity to bare-metal hosts, virtual machines, and external Layer 2 and Layer 3 domains.
• Integrate Cisco ACI with virtual machine managers, such as VMware vCenter.
• Enforce application policies in intra- and intertenant scenarios.
• Deploy Cisco AVS and microsegmentation.
• Program Cisco ACI using Python, RESTful APIs, and Arya.
• Orchestrate Cisco ACI using the Cisco UCS Director.
• Insert L4-L7 services into the Cisco ACI fabric.
• Monitor Cisco ACI deployment using atomic counters and other monitoring tools.

DCVAI Course Outline

Module 1: Infrastructure Virtualization Implementation.
Module 2: NX-OS Configuration Automation.
Module 3: Application-Centric Infrastructure.
Module 4: ACI Constructs.
Module 5: Application-Centric Infrastructure Monitoring and Programmability.
Module 6: Cisco ACI Enhanced Features.
Module 7: Application-Centric Infrastructure Networking.

- DCID Designing Cisco Data Center Infrastructure (300-160 DCID). OR

The course includes information on designing data centers with Cisco components and technologies including: Device virtualization technologies, Storage and SAN design is covered, with explanation of Fibre Channel networks and Cisco Unified Fabric, Design practices for the Cisco Unified Computing System (UCS) solution based on Cisco UCS, B-Series and C-Series servers and Cisco UCS Manager are covered and Network management technologies.

Prerequisites

It is recommended that a learner has the following knowledge and skills before attending this course:
• Implement data center networking (LAN and SAN).
• Describe data center storage.
• Implement data center virtualization.
• Implement Cisco Unified Computing System.
• Implement data center automation and orchestration with the focus on ACI and UCS Director.
• Describe products in the Cisco Data Center Nexus and MDS families.

Course Content

Upon completion of this course, you will be able to:
• Describe Layer 2 switching and Layer 3 forwarding in a data center, including cabling and rack design for the access, aggregation, and core layers.
• Design vPC, Cisco FabricPath, OTV, and LISP in customer scenarios and describe management options in the LAN.
• Describe hardware virtualization and FEX technologies, discuss data center security threats and Cisco Virtual Application Container Services for IaaS, and describe management and automation options for the data center infrastructure.
• Describe storage and RAID options, describe the Fibre Channel concept and architecture, and design Fibre Channel and FCoE networks, along with management options.
• Describe the UCS C-Series, M-Series, and B-Series servers, with connectivity and adapter options. Compare the EHV and NPV network operations modes..
• Explain and distinguish among system integrated stack solutions and the management options for the UCS domains.

• Design the resource parameters for a UCS domain and design the resource pools and policies used in UCS service profiles and templates.

DCID Course Outline

Module 1: Data Center Network Connectivity Design.
Module 2: Data Center Infrastructure Design.
Module 3: Data Center Storage Network Design.
Module 4: Data Center Compute Connectivity Design.
Module 5:Data Center Compute Resource Parameters Design.

- Troubleshooting Cisco Data Center Infrastructure (300-180 DCIT).

The focus of this skills-building course is troubleshooting of LAN, SAN, Cisco Data Center Unified Fabric, Cisco Unified Computing System (UCS), and Cisco Application Centric Infrastructure (ACI). The course provides rich, hands-on experience in resolving problems on Cisco MDS switches, Cisco Nexus switches, Cisco fabric extenders (FEXs), Cisco UCS, and Cisco ACI.

Prerequisites

It is recommended that a learner should have attended the following classes or obtained an equivalent level of knowledge before attending this course:
• Introducing Cisco Data Center Networking (DCICN) v6.0 or higher.
• Introducing Cisco Data Center Technologies (DCICT) v6.0 or higher.
• Implementing Cisco Data Center Infrastructure (DCII) v6.0 or higher.
• Implementing Cisco Data Center Virtualization and Automation (DCVAI) v6.0 or higher.
• Implementing Cisco Data Center Unified Computing (DCUCI) v6.0 or higher.

Course Content

• Troubleshoot Layer 2 technologies, such as STP, port channels, vPC, Cisco FabricPath, and FEX.
• Troubleshoot first-hop redundancy, routing, and CFS in the data center.
• Troubleshoot virtualization solutions, such as OTV, VRF, and VXLAN.
• Troubleshoot storage area networks, including Fibre Channel, FCoE, zoning, NPV, and NPIV.
• Troubleshoot data center unified computing.

DCIT Course Outline

Module 1: Troubleshooting the Data Center LAN Network.
Module 2: Troubleshooting Data Center SAN.
Module 3: Troubleshooting Data Center Unified Computing.
Module 4: Troubleshooting Data Center ACI.

Course Name:	CCNP Data Center
Batch Course Length:	30 days
Batch Course Availability:	1st & 15th of Every Month
Number of Exams:	4
Hours per day:	6hrs
Certifications:	**DCUCI**, **DCII**, **DCVAI** or **DCID** or **DCIT**
Training Locations:	Ilorin (Tanke & Geri-Alimi)
1-on-1 Course Length:	Students Determine
1-on-1 Training Location:	Ilorin (Unity) & Abuja (Maitama)

CCNP SECURITY CERTIFICATIONS

Cisco Certified Network Professional Security (CCNP Security) Certification
Cisco Certified Network Professional Security (CCNP Security) certification program is aligned specifically to the job role of the Cisco Network Security Engineer responsible for Security in Routers, Switches, Networking devices and appliances, as well as choosing, deploying, supporting and troubleshooting Firewalls, VPNS, and IDS/IPS solutions for their networking environments.

Required Exams (4):
- Implementing Cisco Secure Access Solutions (300-208 SISAS).
Implementing Cisco Secure Access Solutions (SISAS) v1.0 is a newly created instructor-led training course that is part of the curriculum path leading to the Cisco Certified Network Professional Security (CCNP Security) certification. Additionally, it is designed to prepare security engineers with the knowledge and hands-on experience so that they can deploy Cisco's Identity Services Engine and 802.1X secure network access. The goal of the course is to provide students with foundational knowledge and the capabilities to implement and managed network access security by utilizing Cisco ISE appliance product solution. The student will gain hands-on experience with configuring various advance Cisco security solutions for mitigating outside threats and securing devices connecting to the network. At the end of the course, students will be able to reduce the risk to their IT infrastructures and applications using Cisco's ISE appliance feature and provide operational support identity and network access control.

Prerequisites
CCNA Security or valid CCSP. or any CCIE certification can act as a prerequisite

Course Content
Upon completing this course, the learner will be able to meet these overall objectives:
• Understand Cisco Identity Services Engine architecture and access control capabilities.
• Understand 802.1X architecture, implementation and operation.
• Understand commonly implemented Extensible Authentication Protocols (EAP).
• Implement Public-Key Infrastructure with ISE.
• Understand the implement Internal and External authentication databases.
• Implement MAC Authentication Bypass.
• Implement identity based authorization policies.
• Understand Cisco TrustSec features.
• Implement Web Authentication and Guest Access.
• Implement ISE Posture service.
• Implement ISE Profiling.
• Understand Bring Your Own Device (BYOD) with ISE.
• Troubleshoot ISE.

SISAS Course Outline
Module 1: Course Introduction.
Module 2: Lab Guide.
Module 3: Threat Mitigation through Identity Services.
Module 4: Cisco ISE Fundamentals.
Module 5: Advance Access Control.
Module 6: Web Authentication and Guest Access.
Module 7: Endpoint Access Control.
Module 8: Troubleshooting Network Access Control.

- Implementing Cisco Edge Network Security Solutions (300-206 SENSS).
Implementing Cisco Edge Network Security Solutions (SENSS) v1.0 is a newly created instructor-led training course that is part of the curriculum path leading to the Cisco Certified Network Professional Security (CCNP Security) certification. Additionally, it is designed to prepare security engineers with the knowledge and hands-on experience to prepare them to configure Cisco perimeter edge security solutions utilizing Cisco Switches, Cisco Routers, and Cisco Adaptive Security Appliance (ASA) Firewalls. The goal of the course is to provide students with foundational knowledge and the capabilities to implement and managed security on Cisco ASA firewalls, Cisco Routers with the firewall feature set, and Cisco Switches. The student will gain hands-on experience with configuring various perimeter security solutions for mitigating outside threats and securing network zones. At the end of the course, students will be able to reduce the risk to their IT infrastructures and applications using Cisco Switches, Cisco ASA, and Router security appliance feature and provide detailed operations support for these products.

Prerequisites
CCNA Security or valid CCSP. or any CCIE certification can act as a prerequisite

Course Content
Upon completing this course, you will be able to describe and use design-oriented knowledge for unified computing topics, including:
• Understanding and implementing Cisco modular Network Security Architectures such as SecureX and TrustSec.
• Deploy Cisco Infrastructure management and control plane security controls.
• Configuring Cisco layer 2 and layer 3 data plane security controls.
• Implement and maintain Cisco ASA Network Address Translations (NAT).
• Implement and maintain Cisco IOS Software Network Address Translations (NAT).
• Designing and deploying Cisco Threat Defense solutions

on a Cisco ASA utilizing access policy and application and identity based inspection.
• Implementing Botnet Traffic Filters.
• Deploying Cisco IOS Zone-Based Policy Firewalls (ZBFW).
• Configure and verify Cisco IOS ZBFW Application Inspection Policy.

SENSS Course Outline
Module 1: Course Introduction.
Module 2: Cisco Secure Design Principles.
Module 3: Deploying Cisco Network Infrastructure Protection Solutions.
Module 4: Deploying NAT on Cisco IOS and Cisco Adaptive Security Appliance (ASA) Firewalls.
Module 5: Deploying Threat Controls on Cisco ASA Firewalls.
Module 6: Deploying Threat Controls on Cisco IOS Software.
Module 7: Lab Guide.

- Implementing Cisco Secure Mobility Solutions (300-209 SIMOS).
Implementing Cisco Secure Mobility Solutions (SIMOS) v1.0 is a newly created instructor-led training (vILT) course that is part of the curriculum path leading to the Cisco Certified Network Professional Security (CCNP Security) certification. This course is designed to prepare network security engineers with the knowledge and skills they need to protect data traversing a public or shared infrastructure such as the Internet by implementing and maintaining Cisco VPN solutions. Students of this course will gain hands-on experience with configuring and troubleshooting remote access and site-to-site VPN solutions, using Cisco ASA adaptive security appliances and Cisco IOS routers.

Prerequisites
CCNA Security or valid CCSP. or any CCIE certification can act as a prerequisite.
Course Content
Upon completion of this course, you will be able to:
• Implement and maintain Cisco site-to-site VPN solutions.
• Implement and maintain Cisco FlexVPN in point-to-point, hub-and-spoke, and spoke-to-spoke IPsec VPNs.
• Implement and maintain Cisco clientless SSL VPNs.
• Implement and maintain Cisco AnyConnect SSL and IPsec VPNs.
• Implement and maintain endpoint security and dynamic access policies (DAP).

SIMOS Course Outline
Module 1: Course Introduction.
Module 2: Fundamentals of VPN Technologies and Cryptography.
Module 3: Deploying Secure Site-to-Site Connectivity Solutions.
Module 4: Deploying Cisco IOS Site-to-Site FlexVPN Solutions.
Module 5: Deploying Clientless SSL VPN -Deploying AnyConnect VPN for Remote Access.
Module 6: Deploying Endpoint Security and Dynamic Access Policies.
Module 7: Lab Guide.

- Implementing Cisco Threat Control Solutions (300-210 SITCS).
This course provides network professional with the knowledge to implement Cisco FirePOWER NGIPS (Next-Generation Intrusion Prevention System) and Cisco AMP (Advanced Malware Protection), as well as Web Security, Email Security and Cloud Web Security. You will gain hands-on experience configuring various advance Cisco security solutions for mitigating outside threats and securing traffic traversing the firewall.

Prerequisites
It is recommended that a learner has the following knowledge and skills before attending this course:
CCNA Security Certification any CCIE certification can act as a prerequisite.

Course Content
Upon completion of this course, you will be able to:
• Implement Cisco FirePOWER NGIPS (Next-Generation Intrusion Prevention System).
• Implement Cisco AMP (Advanced Malware Protection).
• Implement Web Security, Email Security and Cloud Web Security.
• Configuring various Advance Cisco security solutions for mitigating outside threats and securing traffic traversing the firewall.

SITCS Course Outline
Module 1: Network Security.
Module 2: Network Threat Defense.
Module 3: Cisco FirePOWER Next-Generation IPS (NGIPS).
Module 4: Security Architectures.
Module 5: Troubleshooting, Monitoring and Reporting Tools.

Course Name:	CCNP Security
Batch Course Length:	30 days
Batch Course Availability:	1st & 15th of Every Month
Number of Exams:	4
Hours per day:	6hrs
Certifications:	**SISAS , SENSS , SIMOS**, and **SITCS**
Training Locations:	Ilorin (Tanke & Geri-Alimi)
1-on-1 Course Length:	Students Determine
1-on-1 Training Location:	Ilorin (Unity) & Abuja (Maitama)