CCIE Wireless Unified Exam Topics v3.1

The Cisco CCIE® Wireless version 3.1 unifies written and lab exam topics documents into a unique curriculum, while explicitly disclosing which domains pertain to which exam, and relative weight of each domain.

The Cisco CCIE® Wireless written exam version 3.1 (400-351) is a two-hour test with 90–110 questions that assesses and validates wireless expertise at the highest level. Candidates who pass the CCIE Wireless written exam demonstrate broad theoretical knowledge of wireless networking at enterprise level, including a solid understanding of wireless local area networking (WLAN) technologies, and the ability to design, implement, and troubleshoot complex wireless solutions. The exam is closed book and no outside reference materials are allowed.

An Evolving Technologies section is included in the written exam only. It will enable candidates to bridge their core technology expertise with knowledge of the evolving technologies that are being adopted at an accelerated pace, such as Cloud, Network Programmability, and IoT.

The Cisco CCIE® Wireless lab exam is an eight-hour, hands-on exam which requires candidates to configure, diagnose, and troubleshoot a series of complex network scenarios. The candidate will need to understand how the network and service components interoperate, and how the functional requirements translate into specific device configurations. Knowledge of troubleshooting is an important skill and candidates are expected to diagnose and solve issues as part of the CCIE lab exam. The candidate will not configure all end-user systems; however, the candidate will be responsible for all devices residing in the network.

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. In order to better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

*NOTE: This CCIE Wireless unified exam topics version 3.1 includes Evolving Technologies version 1.1 domain and should be referenced for written exams scheduled **on** August 30, 2018 and beyond.*

Domain Number	Domain	Written Exam Percentage (%)	Lab Exam Percentage (%)
1	Plan and Design WLAN Technologies	16	N/A
2	Configure and Troubleshoot the Network Infrastructure	12	15
3	Configure and Troubleshoot an Autonomous Deployment Model	8	12
4	Configure and Troubleshoot AireOS appliance, virtual, and Mobility Express controllers	18	27
5	Configure and Troubleshoot Wireless Security & Identity Management with ISE	13	17
6	Configure and Troubleshoot Prime Infrastructure and MSE/CMX	12	15
7	Configure and Troubleshoot WLAN media and application services	11	14

8	Evolving Technologies	10	N/A
	Total	100	100

1.0 Plan and Design WLAN Technologies

- 1.1. Describe WLAN organizations and regulations
- 1.2. Describe IEEE 802.11 standards and protocols
- 1.3. Plan & design wireless solutions requirements
  - 1.3.a. Translate customer requirements into services and design recommendations
  - 1.3.b. Identify ambiguity and/or information gaps
  - 1.3.c. Evaluate interoperability of proposed technologies against deployed IP network infrastructure & technologies
  - 1.3.d. Select an appropriate deployment model
  - 1.3.e. Regulatory domains and country codes
- 1.4. RF planning, designing and validation
  - 1.4.a. RF Design / Site survey
    - 1.4.a (i) Define the tasks/goals for a preliminary site survey
    - 1.4.a (ii) Conduct the site survey
    - 1.4.a (iii) Determine AP quantity, placement and antenna type
  - 1.4.b Architect indoor and outdoor RF deployments
    - 1.4.b (i) Coverage
    - 1.4.b (ii) Throughput
    - 1.4.b (iii) Voice
    - 1.4.b (iv) Location
    - 1.4.b (v) High Density / Very High Density
  - 1.4.c Construct an RF operational model that includes:
    - 1.4.c (i) Radio resource management (Auto-RF, manual, hybrid, Flexible Radio Assignment, TPC and DCA)
    - 1.4.c (ii) Channel use (radar, non-WiFi interference, Dynamic Bandwidth Selection)
    - 1.4.c (iii) Power level, overlap
    - 1.4.c (iv) RF profiles
  - 1.4.d Validate implemented RF deployment

2.0 Configure and Troubleshoot the Network Infrastructure

- 2.1 Configure and troubleshoot wired infrastructure to support WLANs
  - 2.1.a VLANs
  - 2.1.b VTP
  - 2.1.c STP
  - 2.1.d Etherchannel
- 2.2 Plan network infrastructure capacity
- 2.3 Configure and troubleshoot network connectivity for:
  - 2.3.a WLAN clients
  - 2.3.b WLCs (appliance, virtual, and Mobility Express)
  - 2.3.c Lightweight APs
  - 2.3.d Autonomous APs
- 2.4 Configure and troubleshoot PoE for APs
- 2.5 Configure and troubleshoot QoS on the switching infrastructure
  - 2.5.a MQC
  - 2.5.b MLS QoS
- 2.6 Configure and troubleshoot multicast on the switching infrastructure

- 2.6.a PIM
- 2.6.b Basic IGMP (including IGMP snooping)
- 2.6.c MLD

2.7 Configure and troubleshoot IPv4 connectivity
- 2.7.a Subnetting
- 2.7.b Static and inter-VLAN routing

2.8 Configure and troubleshoot basic IPv6 connectivity
- 2.8.a Subnetting
- 2.8.b Static and inter-VLAN routing

2.9 Configure and troubleshoot wired security for APs
- 2.9.a MAB
- 2.9.b dot1X for APs

2.10 Configure and troubleshoot the following to support wireless services
- 2.10.a DNS
- 2.10.b DHCPv4 / DHCPv6
- 2.10.c NTP, SNTP
- 2.10.d SYSLOG
- 2.10.e SNMP
- 2.10.f CDP, LLDP
- 2.10.g mDNS (including SDG)

3.0 Configure and Troubleshoot an Autonomous Deployment Model

3.1 Configure and troubleshoot different modes and roles
- 3.1.a WGB
- 3.1.b Point to point & Point to multi-point bridge

3.2 Configure and troubleshoot SSID/MBSSID

3.3 Configure and troubleshoot security
- 3.3.a L2 security policies
- 3.3.b Association filters
- 3.3.c Local radius
- 3.3.d dot1X profiles

3.4 Configure and troubleshoot radio settings

3.5 Configure and troubleshoot multicast

3.6 Configure and troubleshoot QoS

4.0 Configure and Troubleshoot AireOS appliance, virtual, and Mobility Express controllers

4.1 Configure and troubleshoot secure management access and control plane
- 4.1.a AAA
- 4.1.b CPU ACLs
- 4.1.c Management via wireless interface
- 4.1.d Management via dynamic interface

4.2 Configure and troubleshoot interfaces

4.3 Configure and troubleshoot lightweight APs
- 4.3.a dot1x
- 4.3.b AP modes
- 4.3.c AP authentication / AP authorization
- 4.3.d Logging
- 4.3.e Local AP CLI configuration
- 4.3.f WLC based AP configuration

- 4.4 Configure and troubleshoot high availability and redundancy
  - 4.4.a SSO
  - 4.4.b N+1, N+N
- 4.5 Configure and troubleshoot wireless segmentation
  - 4.5.a RF profiles
  - 4.5.b AP groups
  - 4.5.c FlexConnect
- 4.6 Configure and troubleshoot wireless security policies
  - 4.6.a WLANs
  - 4.6.b L2/L3 security
  - 4.6.c Rogue policies
  - 4.6.d Local EAP
  - 4.6.e Local profiling
  - 4.6.f ACLs
  - 4.6.g Certificates
- 4.7 Configure and troubleshoot FlexConnect and Office Extend
- 4.8 Configure and troubleshoot Mesh
- 4.9 Implement RF management
  - 4.9.a Static RF management
  - 4.9.b Automatic RF management
  - 4.9.c CleanAir
  - 4.9.d Data rates
  - 4.9.e RX-SOP
  - 4.9.f Air Time Fairness (ATF)
  - 4.9.g Flexible Radio Assignment (FRA)
- 4.10 Configure and troubleshoot mobility
  - 4.10.a L2/L3 roaming
  - 4.10.b Multicast optimization
  - 4.10.c Mobility group scaling
  - 4.10.d Inter-release controller mobility
  - 4.10.e Mobility anchoring
- 4.11 Configure and troubleshoot multicast
- 4.12 Configure and troubleshoot client roaming optimization
  - 4.12.a CCKM
  - 4.12.b Optimized Roaming
  - 4.12.c Band Select
  - 4.12.d Load Balancing
  - 4.12.e 802.11r/k/v

5.0 Configure and Troubleshoot Wireless Security & Identity Management with ISE

- 5.1 Configure and troubleshoot identity management
  - 5.1.a Basic PKI for dot1x and WebAuth
  - 5.1.b External identity sources (AD)
- 5.2 Configure and troubleshoot AAA policies
  - 5.2.a Client authentication and authorization
  - 5.2.b Management authentication and authorization
  - 5.2.c Client profiling and provisioning
  - 5.2.d RADIUS attributes
  - 5.2.e CoA

- 5.3 Configure and troubleshoot wireless guest management
  - 5.3.a Local web authentication
  - 5.3.b Central web authentication
  - 5.3.c Basic sponsor policy

6.0 Configure and Troubleshoot Prime Infrastructure and MSE/CMX

- 6.1 Configure and troubleshoot management access
  - 6.1.a AAA
  - 6.1.b Virtual domain
- 6.2 Perform basic operations
  - 6.2.a Create and deploy templates
  - 6.2.b Operate maps
  - 6.2.c Import infrastructure devices
  - 6.2.d High availability
  - 6.2.e Audits
  - 6.2.f Client troubleshooting
  - 6.2.g Notification receivers
  - 6.2.h Reports
  - 6.2.i Monitoring policies
- 6.3 Configure and troubleshoot Prime Infrastructure jobs
- 6.4 Operate Security management
  - 6.4.a Configure rogue management
  - 6.4.b Manage alarms and events
- 6.5 Implement and troubleshoot MSE/CMX
  - 6.5.a Management access
  - 6.5.b Network services
    - 6.5.b (i) Location
    - 6.5.b (ii) Analytics
    - 6.5.b (iii) Connect and Engage
    - 6.5.b (iv) CleanAir
    - 6.5.b (v) wIPS
    - 6.5.b (vi) NMSP
- 6.6 Integrate ISE with Prime Infrastructure and MSE/CMX

7.0 Configure and Troubleshoot WLAN media and application services

- 7.1 Configure and troubleshoot voice over wireless
  - 7.1.a QoS profiles
  - 7.1.b EDCA
  - 7.1.c WMM
  - 7.1.d BDRL
  - 7.1.e Admission control
  - 7.1.f MQC/MLS
- 7.2 Configure and troubleshoot video and media
  - 7.2.a Media Stream
  - 7.2.b Admission control
- 7.3 Configure and troubleshoot mDNS
  - 7.3.a mDNS proxy
  - 7.3.b Service discovery
  - 7.3.c Service filtering

7.4 Configure and troubleshoot AVC and netflow
7.5 Configure and troubleshoot FastLane and Adaptive Fast Transition (802.11r)

8.0 Evolving Technologies v1.1

8.1. Cloud
- 8.1.a Compare and contrast public, private, hybrid, and multicloud design considerations
  - 8.1.a (i) Infrastructure, platform, and software as a service (XaaS)
  - 8.1.a (ii) Performance, scalability, and high availability
  - 8.1.a (iii) Security implications, compliance, and policy
  - 8.1.a (iv) Workload migration
- 8.1.b Describe cloud infrastructure and operations
  - 8.1.b (i) Compute virtualization (containers and virtual machines)
  - 8.1.b (ii) Connectivity (virtual switches, SD-WAN and SD-Access)
  - 8.1.b (iii) Virtualization functions (NFVi, VNF, and L4/L8)
  - 8.1.b (iv) Automation and orchestration tools (CloudCenter, DNA-center, and Kubernetes)

8.2 Network programmability (SDN)
- 8.2.a Describe architectural and operational considerations for a programmable network
  - 8.2.a (i) Data models and structures (YANG, JSON and XML)
  - 8.2.a (ii) Device programmability (gRPC, NETCONF and RESTCONF)
  - 8.2.a (iii) Controller based network design (policy driven configuration and northbound/ southbound APIs)
  - 8.2.a (iv) Configuration management tools (agent and agentless) and version control systems (Git and SVN)

8.3 Internet of things (IoT)
- 8.3.a Describe architectural framework and deployment considerations for IoT
  - 8.3.a (i) IoT technology stack (IoT Network Hierarchy, data acquisition and flow)
  - 8.3.a (ii) IoT standards and protocols (characteristics within IT and OT environment)
  - 8.3.a (iii) IoT security (network segmentation, device profiling, and secure remote access)
  - 8.3.a (iv) IoT edge and fog computing (data aggregation and edge intelligence)

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.