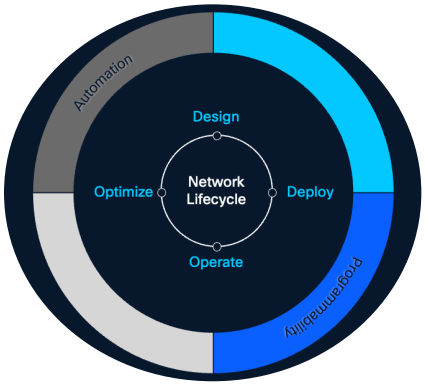
CCIE Wireless (v1.1) Exam Topics

Exam description: Cisco CCIE Wireless (v1.1) Practical Exam



The Cisco CCIE Wireless (v1.1) Practical Exam is an eight-hour, hands-on exam that requires a candidate to plan, design, deploy, operate, and optimize complex enterprise wireless networks.

Candidates are expected to program and automate the network as part of the exam, in alignment with the exam topics below. The exam is closed-book, and no outside reference materials are allowed.

The following topics serve as general guidelines for the content likely to be included in the exam. Your knowledge, skills, and abilities related to these topics will be tested throughout the entire network lifecycle, unless explicitly stated otherwise in this document.

The CCIE Wireless Blueprint covers:

- **Cisco Catalyst Wireless Portfolio**: For customers deploying on-premises/private cloud wireless solutions.
- **Cisco Meraki Portfolio**: For customers utilizing SaaS-based, cloud-managed solutions.

Unless explicitly specified, the topics in the blueprint apply to both solutions.

Additionally:

- **Cisco Spaces**, **OpenRoaming** and **Hotspot 2.0** topics are part of the Design module only.

1. Radio Frequency and Standards (15%)

- 1.1 IEEE 802.11 standards and protocols
- 1.2 Indoor and outdoor RF deployments
  - 1.2.a Coverage
  - 1.2.b High Density / Very High Density
  - 1.2.c Location
  - 1.2.d Throughput and Capacity
  - 1.2.e Voice
- 1.3 RF Design / Site survey
  - 1.3.a Define the tasks/goals for a preliminary site survey
  - 1.3.b Conduct a site survey
  - 1.3.c Determine AP quantity, antennas and placement
- 1.4 RF management and optimization
  - 1.4.a Channel use (Co-channel, radar, non-Wi-Fi interference, Dynamic Bandwidth Selection)
  - 1.4.b Catalyst CleanAir, CleanAir Pro and Event Driven Radio Resource Management (EDRRM)
  - 1.4.c Data rates
  - 1.4.d Power level
  - 1.4.e Radio Resource Management (manual, auto, AI-Enhanced RRM)
  - 1.4.f RF profiles
  - 1.4.g RX-SOP

2. Enterprise Wired Campus (10%)

- 2.1 AP power source options
- 2.2 Layer 2 technologies to support wireless deployments
  - 2.2.a CDP, LLDP
  - 2.2.b Dual uplink and mGig
  - 2.2.c EtherChannel
  - 2.2.d STP
  - 2.2.e VLANs
- 2.3 Data/Control plane technologies to support a SD-Access wireless deployment
  - 2.3.a VRFs
  - 2.3.b VXLAN and LISP
- 2.4 IPv4 and IPv6 connectivity
  - 2.4.a Static and inter-VLAN routing
  - 2.4.b Subnetting
- 2.5 Multicast on the switching infrastructure
  - 2.5.a Basic IGMP (including IGMP snooping)

- 2.5.b MLD
- 2.5.c PIM

2.6 QoS with Modular QoS Command-Line Interface (MQC)

2.7 Services to support a wireless deployment
- 2.7.a DHCPv4 / DHCPv6
- 2.7.b DNS
- 2.7.c NTP, SNTP
- 2.7.d SNMP
- 2.7.e SYSLOG

3. Enterprise Wireless Network (25%)

3.1 Access Points
- 3.1.a AP Auto Locate
- 3.1.b AP CLI troubleshooting
- 3.1.c Meraki Local Status Page (LSP) troubleshooting
- 3.1.d AP country and regulatory domain
- 3.1.e AP join profile
- 3.1.f AP level configuration settings
- 3.1.g AP logging
- 3.1.h AP modes
- 3.1.i Catalyst WGB on COS APs
- 3.1.j AP monitoring
- 3.1.k Dual-Mode and Global Use Access Points (GUAP)
- 3.1.l Power profiles, Power optimization
- 3.1.m VLAN tagging
- 3.1.n WLC discovery and AP join process

3.2 Wireless deployment models
- 3.2.a On-prem
- 3.2.b Cloud

3.3 Catalyst Wireless LAN Controller L2 & L3 functionality
- 3.3.a Interfaces and ports
- 3.3.b Routing and NAT

3.4 Wireless mobility
- 3.4.a L2/L3 roaming, including Meraki Distributed L3 Roaming (DL3R)
- 3.4.b Catalyst Mobility anchoring, encryption, group scaling, optimization
- 3.4.c Campus Gateway

3.5 Catalyst FlexConnect

3.6 Catalyst High availability, redundancy, and resiliency
- 3.6.a ISSU
- 3.6.b N+1, N+N

3.6.c Patching and rolling upgrades for IOS-XE
3.6.d SSO

3.7 URWB and Mesh

3.8 Catalyst wireless AP grouping through profiles and tags

3.9 Meraki data plane modes (bridge, mesh, repeater, tunnel)

4. Wireless Security and Identity Management (20%)

4.1 Access Point switchport authentication
- 4.1.a 802.1X
- 4.1.b IOS-XE interface templates
- 4.1.c IOS-XE port autoconfig
- 4.1.d MAB

4.2 Guest management
- 4.2.a Basic sponsor policy
- 4.2.b Captive portals
- 4.2.c Central web authentication
- 4.2.d Local web authentication

4.3 Identity management
- 4.3.a Basic PKI for dot1X and WebAuth
- 4.3.b Identity PSK
- 4.3.c Internal and external identity sources
- 4.3.d Wi-Fi Personal Network (UDN/WPN)

4.4 Intrusion detection and prevention features
- 4.4.a Client exclusion policies
- 4.4.b Rogue policies
- 4.4.c Standards and custom signatures

4.5 Secure management access, control plane and cloud dashboard
- 4.5.a AP authorization
- 4.5.b Catalyst control plane ACLs
- 4.5.c Device administration with TACACS+/RADIUS
- 4.5.d Management via wireless
- 4.5.e Password policies
- 4.5.f Deployments with a proxy server
- 4.5.g Meraki dashboard access and security

4.6 Cisco Group-Based Policy for wireless networks (Cisco TrustSec and Meraki Adaptive Policy)
- 4.6.a Classification
- 4.6.b Propagation

- 4.6.c Policy enforcement

4.7 Wireless security and network access policies
- 4.7.a ACLs
- 4.7.b Certificates / Trustpoint management
- 4.7.c Client authentication and authorization
- 4.7.d Client profiling and provisioning
- 4.7.e CoA
- 4.7.f Local policies
- 4.7.g L2/L3 security
- 4.7.h OpenRoaming and Hotspot 2.0
- 4.7.i RADIUS attributes
- 4.7.j Umbrella integration / Threat defense
- 4.7.k Meraki MR firewall
- 4.7.l Meraki pre-configured network policies

5. Wireless Services (20%)

5.1 AVC and Netflow

5.2 Client roaming optimization
- 5.2.a 802.11k/v
- 5.2.b 802.11r and Adaptive Fast Transition
- 5.2.c Band Select
- 5.2.d Load Balancing

5.3 mDNS
- 5.3.a mDNS gateway and proxy
- 5.3.b Service discovery
- 5.3.c Service filtering

5.4 QoS policies
- 5.4.a Admission control
- 5.4.b Bi-Directional Rate Limiting
- 5.4.c EDCA
- 5.4.d FastLane, FastLane+
- 5.4.e Catalyst QoS profiles and maps
- 5.4.f WMM
- 5.4.g Meraki QoS and traffic shaping

5.5 Wireless Multicast
- 5.5.a Multicast/Broadcast suppression and control
- 5.5.b Multicast direct
- 5.5.c Multicast modes in the Catalyst WLC
- 5.5.d Multicast snooping
- 5.5.e Catalyst Multicast VLAN

6. Automation, Analytics, and Assurance (10%)

- 6.1 Wireless Programmability
  - 6.1.a API calls
  - 6.1.b Data models
  - 6.1.c EEM scripts
  - 6.1.d Telemetry
- 6.2 Cisco Catalyst Center
  - 6.2.a API calls using python scripts
  - 6.2.b AI Analytics
    - 6.2.b i AI Enhanced RRM
    - 6.2.b ii AI Network analytics
    - 6.2.b iii AI Endpoint analytics
  - 6.2.c Assurance
    - 6.2.c i Analytics
    - 6.2.c ii Application experience
    - 6.2.c iii Client health and client 360
    - 6.2.c iv iCAP and on-demand captures
    - 6.2.c v Network health and WLC/AP 360
    - 6.2.c vi Network telemetry
    - 6.2.c vii Sensors
  - 6.2.d SD Access Wireless
    - 6.2.d i Fabric enabled wireless
    - 6.2.d ii SDA policy and segmentation
  - 6.2.e Wireless Automation
    - 6.2.e i Application policies
    - 6.2.e ii Day 0 – Provisioning
    - 6.2.e iii Operate Maps
    - 6.2.e iv Security policies
    - 6.2.e v SWIM
- 6.3 Cisco Spaces
  - 6.3.a API calls using python scripts
  - 6.3.b Management access
  - 6.3.c Network services
    - 6.3.c i Analytics & Metrics
    - 6.3.c ii Engage
    - 6.3.c iii Location
    - 6.3.c iv Profiles
  - 6.3.d Operational Insights
- 6.4 Cisco Meraki
  - 6.4.a Network assurance, service health
  - 6.4.b Intelligent capture