CCIE Wireless Written Exam Blueprint

The comprehensive CCIE Wireless written exam (#350-050) has 100 multiple-choice questions and is two hours in duration. The topic areas listed are general guidelines for the type of content that is likely to appear on the exam. Please note, however, that other relevant or related topic areas may also appear.

Exam Sections and Sub-task Objectives

1.00	**Plan WLAN installations**	√
1.01	Define standards-based WLAN (802.11x standards)	
1.02	Define WLAN organizations and regulations	
1.03	Identify customer requirements for the wireless LAN	
1.04	Translate customer requirements into services and design recommendations	
1.05	Determine WLAN security policies and constraints	
1.06	Identify ambiguity and/or information gaps	
1.07	Evaluate environmental characteristics	
1.08	Define the tasks/goals for a preliminary site survey	
1.09	Modify proposed solutions based on the applicable regulations	
1.10	Evaluate the existing L2/L3 network infrastructure	
1.11	Conduct the site survey	
2.00	**Design WLAN installations**	
2.01	Determine AP quantity and placement based upon the site survey and customer requirements, includes AP type and antenna type	
2.02	Recommend autonomous or unified deployment model and design	
2.03	Identify the wireless features needed to be implemented in the design, including AP groups, L2/L3 roaming, H-REAP, VoWLAN, AAA override, etc.	
2.04	Design the wireless topology including VLANs, DHCP, SSIDs, IP addressing, mobility groups, etc.	
2.05	Draft an RF operational model that includes:	
	(a) Radio resource management (Auto-RF, manual, hybrid, TPC and DCA)	
	(b) Channel use (Radar, other non-WiFi interference)	
	(c) Power level, overlap	
2.06	Draft WLAN Security policies:	
	(a) Traffic restrictions for L2 filters (802.11 association filters), L3/L4 filters (ACL)	
	(b) Per user, per interface, per SSID; Management access restrictions; peer-to-peer blocking	
	(c) Layer 2/3 security	
	(d) WPS, MFP, NAC	
2.07	Specify the server infrastructure needed to provide the required services	
2.08	Determine the feasibility of carrying LWAPP over WAN	
2.09	Determine hardware and software provisioning requirements for the supporting network infrastructure	
2.10	Determine client provisioning given client hardware and software requirements	
2.11	Use wireless network design tools	

2.12	Draft a design that includes deliverables such as: detailed or high level annotated topology diagram, internal estimates for each site, BOMs for a wireless LAN	
3.00	**Implement WLAN Installations**	
3.01	Implement the WLAN in stages including priming and system testing access points	
3.02	Set appropriate configuration parameters	
3.03	Configure the existing infrastructure applications to support the WLAN, including authentication services (Radius, TACACS+, CA), NTP, DHCP, DNS (LWAPP controller), clients	
3.04	Configure the existing network infrastructure to support the WLAN, including VLANS, Multicast, QoS, routing, switch port configurations, port access through Firewalls (guest access, anchor controllers), etc.	
3.05	For an autonomous wireless architecture deploy APs and antennas, Wireless Distribution Systems (WDS),	
3.06	Bridges (Point-to-Point, Point-to-Multi-Point), Work-group bridges	
3.07	For a unified wireless architecture deploy APs and antennas, WLC with(out) WCS, AP and WLC configurations (auto-provisioning), location (location server, WCS Maps, location calibration)	
3.08	Implement WLAN Security policies, including:	
	(a) Traffic restrictions:	
	(i) L2 filters (802.11 association filters)	
	(ii) L3/L4 filters (ACL) - per user, per interface, per SSID	
	(iii) Management access restrictions	
	(iv) Peer-to-peer blocking	
	(b) Layer 2/3 security	
	(c) WPS,MFP	
3.09	Implement support Voice over WLAN deployments, for both Unified and Autonomous	
3.10	Verify WLAN operation, Client, Location, Voice, Roaming, Post deployment site survey, Network High Availability, Auto-RF, etc	
4.00	**Operate WLAN installations**	
4.01	Determine key performance indicators (kpi) baseline WLAN operational characteristics	
4.02	Collect baseline WLAN operational characteristics using network analysis tools	
4.03	Establish fault management policy and procedures for indicators that should be routinely monitored including Establish Alert Profiles; Noise, Channel Utilization, Interference, Load, etc.	
4.04	Monitor for faults	
	(a) Actively monitor changes based on thresholds (proactive); SNMP polling	
	(b) Receive alarms and wait until notification. (reactive); SNMP traps, syslog messages, WCS notifications	
4.05	Monitor performance trends including Capacity planning; Error rates, Number of clients associated with an AP, AP loading, Threshold figures (1% packet loss for Voice), reference 802.11t; End-to-end traffic flows, etc.	
4.06	Monitor WLAN Security policies.	
	(a) Traffic restrictions:	
	(i) L2 filters (802.11 association filters)	

	(ii) L3/L4 filters (ACL) - per user, per interface, per SSID	
	(iii) Management access restrictions	
	(iv) Peer-to-peer blocking	
	(b) Layer 2/3 security	
	(c) WPS	
4.07	Monitor RF environments using Cisco Spectrum Expert; AP infrastructures	
4.08	Correlate events, alarms and alerts	
5.00	**Troubleshoot WLAN issues**	
5.01	Use the standard troubleshooting method to solve problems	
5.02	Check , validate and analyze:	
	(a) Client Devices	
	(i) Interpret and analyze client side logs.	
	(ii) Validate client connectivity/troubleshoot client via WCS.	
	(iii) Interpret and analyze wireless traces.	
	(iv) Client wireless drivers and supplicant software.	
	(a) Network infrastructure.	
	(i) Check and validate current channel/power settings	
	(ii) Validate security events with WCS	
	(iii) Validate location information in WCS	
	(iv) Validate trap generation, notifications in WCS	
	(v) Collect appropriate logs for analysis to isolate the problem.	
	(vi) Interpret and analyze sniffer traces	
5.03	Analyze the collected information on the RF environment using client-side information and AP-side information (through WLC or WCS) and spectrum analyzer (Cisco Spectrum Expert).	
5.04	Audit voice over WLAN deployment	
5.05	Verify baseline functionality has been restored upon implementing problem resolution	