

CCIE Routing & Switching Written Exam Topics v4.0 (Blueprint)

The comprehensive CCIE R&S Written Exam (#350-001) 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	Implement Layer 2 Technologies	√
1.10	Implement Spanning Tree Protocol (STP)	
	(a) 802.1d	
	(b) 802.1w	
	(c) 801.1s	
	(d) Loop guard	
	(e) Root guard	
	(f) Bridge protocol data unit (BPDU) guard	
	(g) Storm control	
	(h) Unicast flooding	
	(i) Port roles, failure propagation, and loop guard operation	
1.20	Implement VLAN and VLAN Trunking Protocol (VTP)	
1.30	Implement trunk and trunk protocols, EtherChannel, and load-balance	
1.40	Implement Ethernet technologies	
	(a) Speed and duplex	
	(b) Ethernet, Fast Ethernet, and Gigabit Ethernet	
	(c) PPP over Ethernet (PPPoE)	
1.50	Implement Switched Port Analyzer (SPAN), Remote Switched Port Analyzer (RSPAN), and flow control	
1.60	Implement Frame Relay	
	(a) Local Management Interface (LMI)	
	(b) Traffic shaping	
	(c) Full mesh	
	(d) Hub and spoke	
	(e) Discard eligible (DE)	
1.70	Implement High-Level Data Link Control (HDLC) and PPP	
2.00	Implement IPv4	
2.10	Implement IP version 4 (IPv4) addressing, subnetting, and variable-length subnet masking (VLSM)	
2.20	Implement IPv4 tunneling and Generic Routing Encapsulation (GRE)	
2.30	Implement IPv4 RIP version 2 (RIPv2)	
2.40	Implement IPv4 Open Shortest Path First (OSPF)	
	(a) Standard OSPF areas	
	(b) Stub area	
	(c) Totally stubby area	
	(d) Not-so-stubby-area (NSSA)	
	(e) Totally NSSA	
	(f) Link-state advertisement (LSA) types	
	(g) Adjacency on a point-to-point and on a multi-access network	
	(h) OSPF graceful restart	
2.50	Implement IPv4 Enhanced Interior Gateway Routing Protocol (EIGRP)	
	(a) Best path	
	(b) Loop-free paths	
	(c) EIGRP operations when alternate loop-free paths are available, and when they are not available	
	(d) EIGRP queries	
	(e) Manual summarization and autosummarization	
	(f) EIGRP stubs	

2.60	Implement IPv4 Border Gateway Protocol (BGP)	
	(a) Next hop	
	(b) Peering	
	(c) Internal Border Gateway Protocol (IBGP) and External Border Gateway Protocol (EBGP)	
2.70	Implement policy routing	
2.80	Implement Performance Routing (PfR) and Cisco Optimized Edge Routing (OER)	
2.90	Implement filtering, route redistribution, summarization, synchronization, attributes, and other advanced features	
3.00	Implement IPv6	
3.10	Implement IP version 6 (IPv6) addressing and different addressing types	
3.20	Implement IPv6 neighbor discovery	
3.30	Implement basic IPv6 functionality protocols	
3.40	Implement tunneling techniques	
3.50	Implement OSPF version 3 (OSPFv3)	
3.60	Implement EIGRP version 6 (EIGRPv6)	
3.70	Implement filtering and route redistribution	
4.00	Implement MPLS Layer 3 VPNs	
4.10	Implement Multiprotocol Label Switching (MPLS)	
4.20	Implement Layer 3 virtual private networks (VPNs) on provider edge (PE), provider (P), and customer edge (CE) routers	
4.30	Implement virtual routing and forwarding (VRF) and Multi-VRF Customer Edge (VRF-Lite)	
5.00	Implement IP Multicast	
5.10	Implement Protocol Independent Multicast (PIM) sparse mode	
5.20	Implement Multicast Source Discovery Protocol (MSDP)	
5.30	Implement interdomain multicast routing	
5.40	Implement PIM Auto-Rendezvous Point (Auto-RP), unicast rendezvous point (RP), and bootstrap router (BSR)	
5.50	Implement multicast tools, features, and source-specific multicast	
5.60	Implement IPv6 multicast, PIM, and related multicast protocols, such as Multicast Listener Discovery (MLD)	
6.00	Implement Network Security	
6.01	Implement access lists	
6.02	Implement Zone Based Firewall	
6.03	Implement Unicast Reverse Path Forwarding (uRPF)	
6.04	Implement IP Source Guard	
6.05	Implement authentication, authorization, and accounting (AAA) (configuring the AAA server is not required, only the client-side (IOS) is configured)	
6.06	Implement Control Plane Policing (CoPP)	
6.07	Implement Cisco IOS Firewall	
6.08	Implement Cisco IOS Intrusion Prevention System (IPS)	
6.09	Implement Secure Shell (SSH)	
6.10	Implement 802.1x	
6.11	Implement NAT	
6.12	Implement routing protocol authentication	
6.13	Implement device access control	
6.14	Implement security features	
7.00	Implement Network Services	
7.10	Implement Hot Standby Router Protocol (HSRP)	
7.20	Implement Gateway Load Balancing Protocol (GLBP)	
7.30	Implement Virtual Router Redundancy Protocol (VRRP)	
7.40	Implement Network Time Protocol (NTP)	
7.50	Implement DHCP	
7.60	Implement Web Cache Communication Protocol (WCCP)	

8.00	Implement Quality of Service (QoS)	
8.10	Implement Modular QoS CLI (MQC)	
	(a) Network-Based Application Recognition (NBAR)	
	(b) Class-based weighted fair queuing (CBWFQ), modified deficit round robin (MDRR), and low latency queuing (LLQ)	
	(c) Classification	
	(d) Policing	
	(e) Shaping	
	(f) Marking	
	(g) Weighted random early detection (WRED) and random early detection (RED)	
	(h) Compression	
8.20	Implement Layer 2 QoS: weighted round robin (WRR), shaped round robin (SRR), and policies	
8.30	Implement link fragmentation and interleaving (LFI) for Frame Relay	
8.40	Implement generic traffic shaping	
8.50	Implement Resource Reservation Protocol (RSVP)	
8.60	Implement Cisco AutoQoS	
9.00	Troubleshoot a Network	
9.10	Troubleshoot complex Layer 2 network issues	
9.20	Troubleshoot complex Layer 3 network issues	
9.30	Troubleshoot a network in response to application problems	
9.40	Troubleshoot network services	
9.50	Troubleshoot network security	
10.00	Optimize the Network	
10.01	Implement syslog and local logging	
10.02	Implement IP Service Level Agreement SLA	
10.03	Implement NetFlow	
10.04	Implement SPAN, RSPAN, and router IP traffic export (RITE)	
10.05	Implement Simple Network Management Protocol (SNMP)	
10.06	Implement Cisco IOS Embedded Event Manager (EEM)	
10.07	Implement Remote Monitoring (RMON)	
10.08	Implement FTP	
10.09	Implement TFTP	
10.10	Implement TFTP server on router	
10.11	Implement Secure Copy Protocol (SCP)	
10.12	Implement HTTP and HTTPS	
10.13	Implement Telnet	
11.00	Evaluate proposed changes to a Network	
11.01	Evaluate interoperability of proposed technologies against deployed technologies	
	(a) Changes to routing protocol parameters	
	(b) Migrate parts of a network to IPv6	
	(c) Routing Protocol migration	
	(d) Adding multicast support	
	(e) Migrate spanning tree protocol	
	(f) Evaluate impact of new traffic on existing QoS design	
11.02	Determine operational impact of proposed changes to an existing network	
	(a) Downtime of network or portions of network	
	(b) Performance degradation	
	(c) Introducing security breaches	
11.03	Suggest Alternative solutions when incompatible changes are proposed to an existing network	
	(a) Hardware/Software upgrades	
	(b) Topology shifts	
	(c) Reconfigurations	