COMPUTER NETWORKS

Exam Topics

CCNA 1 - CCNAv7: Introduction to Networks

Topic 1 - Network Fundamentals and Models (Modules 1–3)

1. List the basic network components (end devices, network devices, media).
2. Explain the difference between physical and logical topology.
3. Explain the differences between network types: PAN, LAN, MAN and WAN.
4. What is meant by the term converged network?
5. Explain the following concepts: scalability, security, quality of service (QoS) and fault tolerance.
6. Compare access models: Console, SSH and Telnet – characteristics and use cases.
7. List Cisco IOS modes and their basic characteristics.
8. Explain the difference between message delivery methods: unicast, multicast, broadcast.
9. List and characterize the OSI model layers (PDU name, devices, addressing method, and function of each layer).
10. Explain the concepts of encapsulation and decapsulation.
11. How do MAC/IP addresses change when communicating within the same LAN vs. between different LANs?

Topic 2 - IP Addressing (Modules 11–13)

12. Characterize an IPv4 address – network and host portions, subnet mask.
13. What is the purpose and significance of the default gateway?
14. What is a prefix and what does the prefix length indicate?
15. Describe communication types in IPv4 (unicast, multicast, broadcast) and IPv6 (unicast, multicast, anycast).
16. What is the difference between private and public addresses? List the private address ranges per RFC 1918.
17. What are loopback and link-local addresses (IPv4 and IPv6)? What are their ranges?
18. What is the difference between classful addressing (Class A/B/C/D/E) and classless addressing (CIDR)?
19. Characterize an IPv6 address – length, format, abbreviation rules, types.
20. What is subnetting used for? Explain the basic principle and purpose.
21. Basic characteristics of the ICMP protocol and examples of its use (ping, traceroute).

Topic 3 - Physical Layer, Data Link Layer and Switching (Modules 4–10)

22. Characterize the physical layer – media types: copper, optical fibre, wireless.
23. Difference between bandwidth, throughput and latency.
24. Define cable types: coaxial, UTP, STP.
25. Difference between straight-through, crossover and console cables. What is Auto-MDIX?
26. Basic characteristics of optical fiber cables.
27. Basic characteristics of wireless transmission.
28. Characterize the data link layer – LLC and MAC sublayers.
29. Difference in media access control between CSMA/CD (Ethernet) and CSMA/CA (Wi-Fi).

30. Characterize duplex modes (full/half).
31. L2 addressing – MAC addresses (unicast, multicast, broadcast).
32. Basic characteristics of a switch – building the CAM table and flooding.
33. Frame forwarding methods: store-and-forward, cut-through, fragment-free.
34. ARP protocol – function, operation, ARP cache.
35. Network layer – IP protocol characteristics (connectionless, media-independent, ...).
36. Routing – difference between local and remote networks.
37. Function and use of the routing table in packet forwarding.

Topic 4 - Transport Layer and Application Layer (Modules 14–17)

38. Basic characteristics of the transport layer – segmentation, port numbers, multiplexing.
39. Characteristics of TCP (connection-oriented, reliable, flow control) and UDP (connectionless, low latency) – when to use each.
40. Port numbers – well-known ports (e.g. HTTP=80, HTTPS=443, DNS=53, FTP=21, SMTP=25).
41. How is a TCP connection established – three-way handshake (SYN → SYN-ACK → ACK).
42. TCP mechanisms: segment ordering, window size, acknowledgements (ACK), retransmission, congestion avoidance.
43. Application, presentation and session layers – basic characteristics.
44. Application layer protocols: FTP, TFTP, HTTP, HTTPS – characteristics and differences.
45. Email communication – protocols SMTP (sending), POP3 and IMAP (receiving, differences).
46. DNS protocol – role and process of resolving a domain name to an IP address.

Topic 5 - Network Security (Modules 16–17)

47. Types of security threats and their basic characteristics.
48. Types of attacks: malicious code (virus, worm, Trojan horse, ransomware, spyware), reconnaissance attacks (port scanning, ping sweep), access attacks (spoofing, MitM, phishing, social engineering), DoS/DDoS attacks.
49. Function and purpose of security mechanisms: VPN (remote-access vs. site-to-site), firewall (packet filtering, stateful inspection), AAA (Authentication, Authorization, Accounting).

CCNA 2 - CCNAv7: Switching, Routing, and Wireless Essentials

Topic 6 - Switch and Router Configuration (Modules 1–2, 11)

50. Switch boot process (POST, bootstrap, IOS, startup-config).
51. Memory types: RAM (running-config), NVRAM (startup-config), Flash (IOS image), ROM (bootloader).
52. SVI (Switch Virtual Interface) – function and configuration for remote management.
53. Basic router configuration: passwords (enable secret, service password-encryption), banner, Telnet, SSH (ip domain-name, crypto key generate rsa, hostname).
54. Difference between a collision domain and a broadcast domain.
55. Packet switching principle: building the CAM table, flooding for unknown MAC addresses.
56. Port Security – violation modes (shutdown, restrict, protect), sticky MAC, default settings.
57. Error-Disabled interface state – cause and recovery (shutdown / no shutdown).

Topic 7 - VLANs and Network Segmentation (Modules 3–4)

58. Definition of VLAN, its purpose, types (data, management, native, voice, default VLAN 1).
59. Access and trunk ports – differences and configuration.
60. Native VLAN – function, security risks (native VLAN mismatch), recommended configuration.
61. 802.1Q protocol – frame tagging on trunk links.
62. DTP protocol – function, modes (trunk, access, dynamic desirable, dynamic auto) and their combinations.
63. Inter-VLAN routing methods: legacy (one physical port per VLAN), Router-on-a-Stick (subinterface + dot1Q), Layer 3 switch routing (ip routing + SVI).
64. Router-on-a-Stick – what must be configured on the switch (trunk) and on the router (subinterface, encapsulation dot1Q, IP address).

Topic 8 - DHCP and Gateway Redundancy – FHRP (Modules 7–9)

65. DHCP protocol – operation (DORA: Discover, Offer, Request, ACK), message types.
66. DHCP pool contents: address range, default gateway, DNS server, lease time.
67. DHCP relay (ip helper-address) – why and how it is used.
68. DHCPv6 – SLAAC, stateless DHCPv6, stateful DHCPv6 – differences and O/M flags in RA messages.
69. FHRP protocols – principle of gateway redundancy.
70. HSRP protocol – active/standby router, virtual IP and MAC address, priority, preemption, Hello messages.
71. VRRP (open standard, RFC 5798) and GLBP – basic characteristics.

Topic 9 - Routing (Modules 14–16)

72. Basic function of a router.
73. How a router builds its routing table: directly connected networks (C), static routes (S), dynamically learned routes.
74. Packet forwarding decision process – longest prefix match principle.
75. Routing table entry structure: source code, network address/prefix, administrative distance, metric, next-hop, outgoing interface.

76. Administrative distance (AD) – what it represents, values: Connected=0, Static=1, OSPF=110, RIP=120.
77. Difference between metric and administrative distance.
78. Advantages and disadvantages of static vs. dynamic routing.
79. Dynamic routing protocols: OSPF (link-state, cost = ref BW / BW), EIGRP (composite metric), RIP (hop count, max. 15).
80. Types of static routes: standard, default (0.0.0.0/0), floating static route (higher AD = backup route).

Topic 10 - Wireless Networks – WLAN (Module 12)

81. Wireless technology types and WLAN standards: 802.11b/g/n/ac/ax – frequency bands, speeds.
82. Wireless topologies: Ad-hoc (IBSS – no AP), Infrastructure (BSS – single AP), Extended Service Set (ESS – multiple APs).
83. Attributes required for a client to associate with an AP: SSID, security mode and passphrase, frequency band/channel.
84. WLAN threats: rogue AP, evil twin, WEP cracking, MitM, deauthentication attack, eavesdropping.
85. WLAN security options: SSID hiding, MAC address filtering, WPA2/WPA3.
86. Difference between Personal (PSK – shared passphrase) and Enterprise (RADIUS server, individual credentials) authentication.
87. Encryption protocols: TKIP (WPA), AES-CCMP (WPA2/WPA3), WPA3-SAE (resistance to offline dictionary attacks).
88. Non-overlapping channels in the 2.4 GHz band – why they matter (interference avoidance).