POČÍTAČOVÉ SIETE / BEZPEČNOSŤ POČÍTAČOVÝCH SIETÍ

Okruhy na skúšku

CCNA 1 - CCNAv7: Introduction to Networks

Okruh č. 1 - Základy sietí a modely (Moduly 1–3)

1. Vymenujte základné sieťové komponenty (koncové zariadenia, sieťové zariadenia, médiá).
2. Vysvetlite rozdiel medzi fyzickou a logickou topológiou.
3. Vysvetlite rozdiely medzi typmi počítačových sietí: PAN, LAN, MAN a WAN.
4. Čo sa rozumie pod pojmom konvergovaná sieť?
5. Vysvetlite pojmy: škálovateľnosť, bezpečnosť, kvalita služieb (QoS) a odolnosť voči chybám.
6. Porovnajte modely prístupu: Konzola, SSH a Telnet – vlastnosti a využitie.
7. Uveďte Cisco IOS módy a ich základnú charakteristiku.
8. Vysvetlite rozdiel medzi metódami doručovania správ: unicast, multicast, broadcast.
9. Vymenujte a charakterizujte vrstvy OSI modelu (PDU, zariadenia, adresovanie, funkcia každej vrstvy).
10. Vysvetlite pojem enkapsulacia a dekapsulacia.
11. Ako sa menia MAC/IP adresy pri komunikácii v rámci tej istej LAN a medzi rôznymi LAN sieťami?

Okruh č. 2 - IP adresácia (Moduly 11–13)

12. Charakterizujte IPv4 adresu – sieťová a hostovská časť, sieťová maska.
13. Aký je účel a význam predvolenej brány (default gateway)?
14. Na čo slúži prefix a čo hovorí dĺžka prefixu?
15. Popíšte typy komunikácie v IPv4 (unicast, multicast, broadcast) a IPv6 (unicast, multicast, anycast).
16. Aký je rozdiel medzi súkromnými a verejnými adresami? Uveďte rozsahy súkromných adries podľa RFC 1918.
17. Čo sú loopback a link-local adresy (IPv4 aj IPv6)? Aké majú rozsahy?
18. Aký je rozdiel medzi triednym adresovaním (Class A/B/C/D/E) a beztriednym adresovaním (CIDR)?
19. Charakterizujte IPv6 adresu – dĺžka, formát, skracovanie, typy.
20. Na čo slúži podsieťovanie? Základný princíp a zmysel.
21. Základná charakteristika protokolu ICMP a príklady využitia (ping, traceroute).

Okruh č. 3 - Fyzická, linková vrstva a prepínanie (Moduly 4–10)

22. Charakterizujte fyzickú vrstvu – médiá: metalické, optické, bezdrôtové.
23. Rozdiel medzi šírkou pásma (bandwidth), priepustnosťou (throughput) a oneskorením (latency).
24. Definujte typy káblov: koaxiálny, UTP, STP.
25. Rozdiel medzi priamym, kríženým a konzolovým káblom. Čo je Auto-MDIX?
26. Základné vlastnosti optických káblov.

27. Základná charakteristika bezdrôtového prenosu.
28. Charakterizujte linkovú vrstvu – LLC a MAC podvrstvy.
29. Rozdiel v kontrole prístupu medzi CSMA/CD (Ethernet) a CSMA/CA (Wi-Fi).
30. Charakterizujte duplex (full/half).
31. L2 adresovanie – MAC adresy (unicast, multicast, broadcast).
32. Základná charakteristika prepínača – budovanie CAM tabuľky a flooding.
33. Prístupy k posielaniu rámcov: store-and-forward, cut-through, fragment-free.
34. Protokol ARP – funkcia, priebeh, ARP cache.
35. Sieťová vrstva – protokol IP (vlastnosti: nespojový, nezávislý na médiu, ...).
36. Smerovanie – rozdiel medzi lokálnymi a vzdialenými sieťami.
37. Funkcia a využitie smerovacej tabuľky pri smerovaní dát.

Okruh č. 4 - Transportná a aplikačná vrstva (Moduly 14–17)

38. Základná charakteristika transportnej vrstvy – segmentácia, čísla portov, multiplexovanie.
39. Vlastnosti TCP (spojový, spoľahlivý, riadenie toku) a UDP (bezspojový, nízka latencia) – kedy sa ktorý používa.
40. Čísla portov – well-known (napr. HTTP=80, HTTPS=443, DNS=53, FTP=21, SMTP=25).
41. Ako sa nadväzuje TCP spojenie – three-way handshake (SYN → SYN-ACK → ACK).
42. TCP mechanizmy: usporiadanie segmentov, veľkosť okna (window size), potvrdenia (ACK), retransmisia, zabránenie zahlteniu.
43. Aplikačná, prezentačná a relačná vrstva – základná charakteristika.
44. Protokoly aplikačnej vrstvy: FTP, TFTP, HTTP, HTTPS – vlastnosti a rozdiely.
45. Emailová komunikácia – protokoly SMTP (odosielanie), POP3 a IMAP (prijímanie, rozdiely).
46. Protokol DNS – úloha, priebeh prekladu doménového mena na IP adresu.

Okruh č. 5 - Bezpečnosť sietí (Moduly 16–17)

47. Typy bezpečnostných hrozieb a ich základná charakteristika.
48. Typy útokov: škodlivý kód (vírus, červ, trójsky kôň, ransomware, spyware), prieskumnícky útok (port scanning, ping sweep), útok na prístup (spoofing, MitM, phishing, sociálne inžinierstvo), DoS/DDoS útok.
49. Funkcia a účel bezpečnostných mechanizmov: VPN (remote-access vs. site-to-site), firewall (packet filtering, stateful inspection), AAA (Authentication, Authorization, Accounting).

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

Okruh č. 6 - Konfigurácia prepínača a smerovača (Moduly 1–2, 11)

50. Postup bootovania prepínača (POST, bootstrap, IOS, startup-config).
51. Typy pamätí: RAM (running-config), NVRAM (startup-config), Flash (IOS obraz), ROM (bootloader).
52. Logické rozhranie SVI – funkcia, konfigurácia pre vzdialenú správu.
53. Základná konfigurácia smerovača: heslá (enable secret, service password-encryption), banner, Telnet, SSH (ip domain-name, crypto key generate rsa, hostname).
54. Rozdiel medzi kolíznou doménou a broadcastovou doménou.
55. Princíp prepínania paketov: budovanie CAM tabuľky, flooding neznámej MAC adresy.
56. Port Security – módy narušenia (shutdown, restrict, protect), sticky MAC, predvolené nastavenie.
57. Stav rozhrania Error-Disabled – príčina a obnova (shutdown / no shutdown).

Okruh č. 7 - VLAN a segmentácia siete (Moduly 3–4)

58. Definícia VLAN, jej účel, typy VLAN (data, management, native, voice, default VLAN 1).
59. Prístupové (access) a trunkové (trunk) rozhranie – rozdiel, konfigurácia.
60. Natívna VLAN – funkcia, bezpečnostné riziká (native VLAN mismatch), odporúčaná konfigurácia.
61. Protokol 802.1Q – tagovanie rámcov na trunku.
62. Protokol DTP – funkcia, módy (trunk, access, dynamic desirable, dynamic auto) a ich kombinácie.
63. Spôsoby smerovania dát medzi VLAN: tradičné (legacy), Router-on-a-Stick (subinterface + dot1Q), smerovanie pomocou L3 prepínača (ip routing + SVI).
64. Router-on-a-Stick – čo treba konfigurovať na prepínači (trunk) aj na smerovači (subinterface, encapsulation dot1Q, IP adresa).

Okruh č. 8 - DHCP a redundancia brány – FHRP (Moduly 7–9)

65. Protokol DHCP – fungovanie (DORA: Discover, Offer, Request, ACK), typy správ.
66. Obsah DHCP poolu: rozsah adries, default gateway, DNS server, lease time.
67. DHCP relay (ip helper-address) – prečo a ako sa používa.
68. DHCPv6 – SLAAC, bezstavové DHCPv6, stavové DHCPv6 – rozdiely a príznaky O/M v RA správe.
69. Protokoly typu FHRP – princíp redundancie brány.
70. Protokol HSRP – active/standby router, virtuálna IP a MAC adresa, priorita, preempcia, Hello správy.
71. VRRP (otvorený štandard RFC 5798) a GLBP – základná charakteristika.

Okruh č. 9 - Smerovanie (Moduly 14–16)

72. Základná funkcia smerovača.
73. Spôsoby tvorby smerovacej tabuľky: priamo pripojené siete (C), statické záznamy (S), dynamicky naučené cesty.
74. Rozhodovací proces pri smerovaní – princíp longest prefix match.
75. Štruktúra záznamu v smerovacej tabuľke: kód zdroja, sieťová adresa/prefix, administratívna vzdialenosť, metrika, next-hop, rozhranie.

1. Administratívna vzdialenosť (AD) – čo vyjadruje, hodnoty: Connected=0, Static=1, OSPF=110, RIP=120.
2. Rozdiel medzi metrikou a administratívnou vzdialenosťou.
3. Výhody a nevýhody statického vs. dynamického smerovania.
4. Dynamické smerovacie protokoly: OSPF (link-state, cost = ref BW / BW), EIGRP (kompozitná metrika), RIP (počet hopov, max. 15).
5. Typy statických ciest: štandardná, predvolená (0.0.0.0/0), floating static route (vyššia AD = záložná cesta).

Okruh č. 10 - Bezdrôtové siete WLAN (Modul 12)

6. Typy bezdrôtových technológií a WLAN štandardy: 802.11b/g/n/ac/ax – frekvenčné pásma, rýchlosti.
7. Bezdrôtové topológie: Ad-hoc (IBSS – bez AP), Infrastructure (BSS – jeden AP), Extended Service Set (ESS – viac AP).
8. Atribúty pre asociáciu klienta s AP: SSID, bezpečnostný mód a heslo, frekvenčné pásmo/kanál.
9. Hrozby pri používaní WLAN: rogue AP, evil twin, WEP cracking, MitM, deauthentication útok, odpočúvanie.
10. Zabezpečenie WLAN: skrytie SSID, filtrovanie MAC adries, WPA2/WPA3.
11. Rozdiel medzi Personal (PSK – zdieľané heslo) a Enterprise (RADIUS server, individuálne prihlasovacie údaje) autentifikáciou.
12. Šifrovacie protokoly: TKIP (WPA), AES-CCMP (WPA2/WPA3), WPA3-SAE (odolnosť voči slovníkovým útokom).
13. Neprekrývajúce sa kanály v pásme 2,4 GHz – prečo sú dôležité (interferencia).