Computernetzwerktechnologie

Hier ist eine Liste von 100 Schlüsselpunkten, die den Umfang eines Kurses oder eines Selbststudiums zu „Computer Network Technology“abdecken, wobei grundlegende Konzepte, Protokolle und praktische Anwendungen behandelt werden.

1. Definition eines Computer-Netzwerks: Ein System von miteinander verbundenen Geräten, die Ressourcen und Daten teilen.
2. Hauptfunktionen von Netzwerken: Ressourcenteilung, Kommunikation, Datenübertragung und Zusammenarbeit.
3. Entwicklung von Netzwerken: Von ARPANET und frühen LANs bis zum globalen Internet, das wir heute haben.
4. Gängige Netzwerktypen: LAN (Local Area Network), MAN (Metropolitan Area Network), WAN (Wide Area Network).
5. Topologie-Strukturen: Bus, Stern, Ring, Masche und Hybrid.
6. Intranet vs. Extranet vs. Internet: Unterschiede im Umfang und typische Anwendungsfälle.
7. Standardisierungsorganisationen: IEEE, IETF, ISO—Definition und Pflege von Netzwerkstandards und -protokollen.
8. OSI-Referenzmodell: Ein siebenstufiges Konzeptmodell zur Verständnis von Netzwerkfunktionen.
9. TCP/IP-Modell: Ein vierstufiges (oder manchmal fünfstufiges) pragmatisches Modell, das das Internet untermauert.
10. Vergleich von OSI und TCP/IP: Ähnlichkeiten (schichtbasierter Ansatz) und Unterschiede (Anzahl der Schichten und Abstraktion).
11. Zweck der Bitübertragungsschicht: Beschäftigt sich mit der Übertragung roher Bits über ein physisches Medium.
12. Gängige Übertragungsmedien: Twisted-Pair-Kabel, Koaxialkabel, Glasfaser und drahtlos.
13. Bandbreite vs. Durchsatz: Theoretische maximale Rate vs. tatsächliche Datenübertragungsrate.
14. Signalcodierung: Methoden (z.B. Manchester-Codierung) zur Darstellung von Datenbits für die Übertragung.
15. Modulationstechniken: AM, FM, PM, die bei Analog-Digital- oder Digital-Analog-Umwandlungen verwendet werden.
16. Geräte der Bitübertragungsschicht: Hubs, Repeater—primär zur Signalwiederholung ohne Inspektion.
17. Zweck der Sicherungsschicht: Behandelt das Framing, Adressierung, Fehlererkennung/-korrektur und Flusskontrolle.

18. Framing: Einkapselung von Paketen in Sicherungsschicht-Header und -Trailer.
19. MAC (Media Access Control) Adresse: Ein eindeutiger Hardware-Identifikator für Netzwerkschnittstellenkarten.
20. Fehlererkennungsmechanismen: Paritätsprüfung, CRC (Cyclic Redundancy Check), Prüfsummen.
21. Ethernet-Grundlagen: Die gängigste LAN-Technologie; verwendet eine Frame-Struktur mit Quell-/Ziel-MAC.
22. Ethernet-Frame-Format: Präambel, Ziel-MAC, Quell-MAC, Typ/Länge, Nutzlast, CRC.
23. Switching: Weiterleitung von Frames unter Verwendung von MAC-Adressentabellen in einem LAN.
24. Lernprozess in Switches: Aufbau einer Tabelle von MAC-Adressen, während Geräte kommunizieren.
25. VLAN (Virtual LAN): Logische Segmentierung eines physischen LANs in mehrere virtuelle Netzwerke.
26. Zweck der Netzwerkschicht: Routing, logische Adressierung (IP) und Pfadbestimmung.
27. IPv4-Adressformat: 32-Bit-Adresse, typischerweise als Punktnotation dargestellt.
28. IPv4-Klassen (veraltet): Klasse A, B, C, D, E (historischer Kontext, ersetzt durch CIDR).
29. CIDR (Classless Inter-Domain Routing): Moderner Ansatz für eine flexiblere IP-Adresszuweisung.
30. IPv4 vs. IPv6: Wichtige Unterschiede (128-Bit-Adressierung, erweitertes Header-Format, Auto-Konfiguration).
31. Subnetting: Aufteilung eines großen Netzwerks in kleinere Subnetze für eine effiziente Adressnutzung.
32. NAT (Network Address Translation): Zuordnung privater IP-Adressen zu einer öffentlichen IP, um IPv4-Adressen zu sparen.
33. ARP (Address Resolution Protocol): Auflösung von IP-Adressen in MAC-Adressen innerhalb eines LANs.
34. ICMP (Internet Control Message Protocol): Diagnosetool—verwendet von ping, traceroute.
35. Routing vs. Switching: Routing erfolgt auf IP-Ebene (Schicht 3), während Switching auf MAC-Ebene (Schicht 2) erfolgt.
36. Statisches Routing: Manuelle Konfiguration von Routen in der Routing-Tabelle eines Routers.
37. Dynamische Routing-Protokolle: RIP (Routing Information Protocol), OSPF (Open Shortest Path First), BGP (Border Gateway Protocol).
38. Router-Grundlagen: Bestimmt den nächsten Netzwerk-Hop für ein Paket basierend auf IP-Adressen.
39. Zweck der Transportschicht: End-to-End-Datenübertragung, Zuverlässigkeit und Flusskontrolle.
40. TCP (Transmission Control Protocol): Verbindungsorientiertes Protokoll, das eine zuverlässige Datenübertragung bietet.

41. TCP-Segment-Struktur: Quellport, Zielport, Sequenznummer, Bestätigungsnummer usw.
42. TCP-Drei-Wege-Handshake: SYN, SYN-ACK, ACK-Prozess für den Verbindungsaufbau.
43. TCP-Vier-Wege-Abbau: FIN, FIN-ACK, ACK-Sequenz zum Schließen einer Verbindung.
44. TCP-Flusskontrolle: Mechanismen wie das gleitende Fenster zur Verwaltung der Datenübertragungsraten.
45. TCP-Verstopfungskontrolle: Algorithmen (langsamer Start, Verstopfungsvermeidung, schnelle Wiederherstellung, schnelles Neuübertragen).
46. UDP (User Datagram Protocol): Verbindungslos, minimaler Overhead, keine Garantie für die Zustellung.
47. UDP-Segment-Struktur: Quellport, Zielport, Länge, Prüfsumme, Daten.
48. Portnummern: Identifikatoren für Dienste (z.B. 80 für HTTP, 443 für HTTPS, 53 für DNS).
49. Socket: Kombination aus einer IP-Adresse und einem Port, die verwendet wird, um ein Endpunkt zu identifizieren.
50. Zweck der Anwendungsschicht: Bietet Netzwerkdienste für Benutzeranwendungen.
51. HTTP (Hypertext Transfer Protocol): Die Grundlage der Datenkommunikation im Web.
52. HTTP-Methoden: GET, POST, PUT, DELETE, HEAD usw.
53. HTTPS: Verschlüsseltes HTTP mit TLS/SSL für sichere Webkommunikation.
54. DNS (Domain Name System): Zuordnung von Domänennamen (z.B. example.com) zu IP-Adressen.
55. DNS-Auflösungsprozess: Rekursive und iterative Abfragen, Root-Server, TLD-Server, autoritative Server.
56. FTP (File Transfer Protocol): Legacy-Protokoll für Dateiübertragungen über TCP (Ports 20/21).
57. E-Mail-Protokolle: SMTP (Senden), POP3 und IMAP (Abrufen).
58. DHCP (Dynamic Host Configuration Protocol): Automatische Zuweisung von IP-Adressen an Geräte.
59. Telnet vs. SSH: Remote-Zugriffsprotokolle—SSH ist verschlüsselt, Telnet ist es nicht.
60. Client-Server-Modell: Eine gängige Architektur, bei der ein Client Dienste von einem Server anfordert.
61. P2P (Peer-to-Peer) Modell: Jeder Knoten kann sowohl Dienste anfordern als auch bereitstellen.
62. Web-Technologien: URLs, URIs, Cookies, Sitzungen, grundlegende Webanwendungsstruktur.
63. Netzwerksicherheitsprinzipien: Vertraulichkeit, Integrität, Verfügbarkeit (CIA-Triad).
64. Gängige Sicherheitsbedrohungen: Malware (Viren, Würmer, Trojaner), DDoS-Angriffe, Phishing, SQL-Injection.
65. Firewalls: Filtert den Verkehr basierend auf Regeln, platziert an Netzwerkgrenzen.

66. IDS/IPS (Intrusion Detection/Prevention Systems): Überwacht den Verkehr auf verdächtige Aktivitäten.
67. VPN (Virtual Private Network): Verschlüsselter Tunnel über ein öffentliches Netzwerk, der entfernte Verbindungen sichert.
68. TLS/SSL (Transport Layer Security / Secure Sockets Layer): Verschlüsselung für sichere Datenübertragung.
69. Grundlagen der Kryptographie: Symmetrische vs. asymmetrische Verschlüsselung, Schlüsselausausch, digitale Signaturen.
70. Digitale Zertifikate: Von CAs (Certificate Authorities) bereitgestellt, um die Identität zu validieren und HTTPS zu ermöglichen.
71. Netzwerksicherheitsrichtlinien: Richtlinien zur sicheren Netzwerknutzung, Zugriffskontrollen und Überwachung.
72. DMZ (Demilitarisierte Zone): Ein Subnetz, das nach außen gerichtete Dienste der Öffentlichkeit zugänglich macht.
73. WLAN-Sicherheit: Drahtlose Netzwerke (Wi-Fi) gesichert durch WPA2, WPA3 usw.
74. Physikalische Sicherheit: Sicherstellung, dass die Netzwerkinfrastruktur (Server, Kabel, Router) sicher untergebracht ist.
75. Social Engineering: Nicht-technische Eindringungstaktiken—Phishing, Vorwand, Köder.
76. OSI-Schicht-Angriffe: Verschiedene Bedrohungen/Abwehrmechanismen auf jeder Schicht (z.B. ARP-Spoofing auf der Sicherungsschicht).
77. Netzwerkverwaltungstools: ping, traceroute, netstat, nslookup, dig.
78. Paketsniffer: Tools wie Wireshark oder tcpdump zur Analyse des Verkehrs auf Paketebene.
79. Netzwerkverwaltungprotokolle: SNMP (Simple Network Management Protocol).
80. Protokollierung und Überwachung: Syslog, Ereignisprotokolle, SIEM-Lösungen für die Echtzeiterkennung.
81. Grundlegende LAN-Einrichtung: Bestimmung von IP-Bereichen, Subnetzmasken, Gateway, DNS-Server.
82. Kabelarten: CAT5, CAT5e, CAT6, Glasfaser, wann jede typischerweise verwendet wird.
83. Strukturierte Verkabelung: Standards für professionelle großflächige Netzwerkinstallationen.
84. Switch-Konfiguration: Erstellung von VLANs, Trunk-Ports und Spanning-Tree-Protokollen.
85. Router-Konfiguration: Einrichtung von Routen (statisch/dynamisch), NAT, ACL (Access Control Lists).
86. Grundlegende Firewall-Regeln: Alle eingehenden Verbindungen ablehnen, außer den erforderlichen, alle ausgehenden Verbindungen zulassen oder nach Bedarf einschränken.

87. Netzwerkadressierungspläne: Effiziente Zuweisung von IP-Adressen basierend auf Abteilung oder Subnetzen.
88. Redundanz und Failover: Verwendung von Backup-Verbindungen, Lastverteilung oder VRRP/HSRP für hohe Verfügbarkeit.
89. QoS (Quality of Service): Priorisierung bestimmter Verkehrsarten (z.B. VoIP), um die Leistung zu gewährleisten.
90. Grundlagen der Cloud-Netzwerke: Virtuelle Netzwerke, Sicherheitsgruppen, Lastverteiler in Cloud-Umgebungen.
91. SDN (Software-Defined Networking): Trennung der Steuerungsebene von der Datenebene für eine zentralisierte Verwaltung.
92. Virtualisierung: Verwendung von Hypervisoren (VMware, Hyper-V, KVM) zur Erstellung virtueller Server/Netzwerke.
93. Container und Microservices: Docker-Netzwerke, Kubernetes-Netzwerkkonzepte.
94. IPv6-Einführung: Dual Stack (IPv4/IPv6), IPv6 Auto-Konfiguration (SLAAC), IPv6-Tunnel.
95. DNS-Lastverteilung: Verteilung des Verkehrs über mehrere Server mittels DNS-Round-Robin.
96. Edge-Computing: Verarbeitung am Netzwerkrand, um die Latenz für IoT und Echtzeitdienste zu reduzieren.
97. 5G und drahtlose Evolution: Höhere Datenraten, geringere Latenz, Verwendung in IoT und mobiler Breitband.
98. Netzwerkfehlerbehebungsschritte: Problem identifizieren, isolieren, Hypothesen testen, beheben, überprüfen.
99. Dokumentation: Wichtigkeit der Pflege genauer Netzwerkdiagramme und Gerätekonfigurationen.
100. Kontinuierliches Lernen: Netzwerken entwickelt sich ständig weiter, was ein fortlaufendes Studium neuer Protokolle und Best Practices erfordert.

Diese 100 Punkte fassen die wesentlichen Themen in Computer-Netzwerken zusammen, die von der grundlegenden Theorie, Protokollen, Hardware, Adressierung, Sicherheit und modernen Trends reichen. Sie sollten Ihnen bei der Vorbereitung auf Prüfungen oder dem praktischen Verständnis von Computer-Netzwerken helfen.