Computer Network Technology

This post was written with ChatGPT.

Below is a list of 100 key points that broadly cover the scope of a "Computer Network Technology" course or self-study outline, touching on fundamental concepts, protocols, and practical applications.

1. Definition of a Computer Network: A system of interconnected devices that share resources and data.
2. Primary Functions of Networks: Resource sharing, communication, data transmission, and collaboration.
3. Evolution of Networks: From ARPANET and early LANs to the global Internet we have today.
4. Common Network Types: LAN (Local Area Network), MAN (Metropolitan Area Network), WAN (Wide Area Network).
5. Topology Structures: Bus, star, ring, mesh, and hybrid.
6. Intranet vs. Extranet vs. Internet: Scope differences and typical use cases.
7. Standard Organizations: IEEE, IETF, ISO—defining and maintaining network standards and protocols.
8. OSI Reference Model: A seven-layer conceptual framework for understanding network functions.
9. TCP/IP Model: A four-layer (or sometimes five-layer) pragmatic model that underpins the Internet.
10. Comparison of OSI and TCP/IP: Similarities (layered approach) and differences (number of layers and abstraction).
11. Physical Layer Purpose: Concerned with the transmission of raw bits over a physical medium.
12. Common Transmission Media: Twisted-pair cable, coaxial cable, optical fiber, and wireless.
13. Bandwidth vs. Throughput: Theoretical maximum rate vs. actual data transfer rate.
14. Signal Encoding: Methods (e.g., Manchester encoding) to represent data bits for transmission.
15. Modulation Techniques: AM, FM, PM used in analog-to-digital or digital-to-analog conversions.
16. Physical Layer Devices: Hubs, repeaters—primarily repeating signals without inspection.
17. Data Link Layer Purpose: Handles framing, addressing, error detection/correction, and flow control.
18. Framing: Encapsulating packets in data link layer headers and trailers.
19. MAC (Media Access Control) Address: A unique hardware identifier for network interface cards.

20. Error Detection Mechanisms: Parity check, CRC (Cyclic Redundancy Check), checksums.
21. Ethernet Basics: The most common LAN technology; uses a frame structure with source/destination MAC.
22. Ethernet Frame Format: Preamble, destination MAC, source MAC, type/length, payload, CRC.
23. Switching: Forwarding frames using MAC address tables in a LAN.
24. Learning Process in Switches: Building a table of MAC addresses as devices communicate.
25. VLAN (Virtual LAN): Logically segmenting one physical LAN into multiple virtual networks.
26. Network Layer Purpose: Routing, logical addressing (IP), and path determination.
27. IPv4 Address Format: 32-bit address, typically represented as dotted-decimal notation.
28. IPv4 Classes (Obsolete): Class A, B, C, D, E (historical context, replaced by CIDR).
29. CIDR (Classless Inter-Domain Routing): Modern approach to more flexible IP address allocation.
30. IPv4 vs. IPv6: Key differences (128-bit addressing, expanded header format, auto-configuration).
31. Subnetting: Dividing a large network into smaller subnetworks for efficient address use.
32. NAT (Network Address Translation): Mapping private IP addresses to a public IP to conserve IPv4 addresses.
33. ARP (Address Resolution Protocol): Resolving IP addresses to MAC addresses within a LAN.
34. ICMP (Internet Control Message Protocol): Diagnostics tool—used by ping, traceroute.
35. Routing vs. Switching: Routing is for IP-level (Layer 3), while switching is for MAC-level (Layer 2).
36. Static Routing: Manually configuring routes in a router' s routing table.
37. Dynamic Routing Protocols: RIP (Routing Information Protocol), OSPF (Open Shortest Path First), BGP (Border Gateway Protocol).
38. Router Basics: Determines the next network hop for a packet based on IP addresses.
39. Transport Layer Purpose: End-to-end data delivery, reliability, and flow control.
40. TCP (Transmission Control Protocol): Connection-oriented protocol providing reliable data transfer.
41. TCP Segment Structure: Source port, destination port, sequence number, acknowledgment number, etc.
42. TCP Three-Way Handshake: SYN, SYN-ACK, ACK process for connection setup.
43. TCP Four-Way Teardown: FIN, FIN-ACK, ACK sequence to close a connection.

44. TCP Flow Control: Mechanisms like sliding window to manage data transfer rates.
45. TCP Congestion Control: Algorithms (slow start, congestion avoidance, fast recovery, fast retransmit).
46. UDP (User Datagram Protocol): Connectionless, minimal overhead, no guarantee of delivery.
47. UDP Segment Structure: Source port, destination port, length, checksum, data.
48. Port Numbers: Identifiers for services (e.g., 80 for HTTP, 443 for HTTPS, 53 for DNS).
49. Socket: Combination of an IP address and port used to identify an endpoint.
50. Application Layer Purpose: Provides network services to user applications.
51. HTTP (Hypertext Transfer Protocol): The foundation of data communication on the web.
52. HTTP Methods: GET, POST, PUT, DELETE, HEAD, etc.
53. HTTPS: Encrypted HTTP using TLS/SSL for secure web communication.
54. DNS (Domain Name System): Maps domain names (e.g., example.com) to IP addresses.
55. DNS Resolution Process: Recursive and iterative queries, root servers, TLD servers, authoritative servers.
56. FTP (File Transfer Protocol): Legacy protocol for file transfers over TCP (ports 20/21).
57. Email Protocols: SMTP (Send), POP3 and IMAP (Retrieve).
58. DHCP (Dynamic Host Configuration Protocol): Automatically assigns IP addresses to devices.
59. Telnet vs. SSH: Remote access protocols—SSH is encrypted, Telnet is not.
60. Client-Server Model: A common architecture where a client requests services from a server.
61. P2P (Peer-to-Peer) Model: Each node can both request and provide services.
62. Web Technologies: URLs, URIs, cookies, sessions, basic web application structure.
63. Network Security Principles: Confidentiality, integrity, availability (CIA triad).
64. Common Security Threats: Malware (viruses, worms, trojans), DDoS attacks, phishing, SQL injection.
65. Firewalls: Filters traffic based on rules, placed at network boundaries.
66. IDS/IPS (Intrusion Detection/Prevention Systems): Monitors traffic for suspicious activities.
67. VPN (Virtual Private Network): Encrypted tunnel over a public network, securing remote connections.
68. TLS/SSL (Transport Layer Security / Secure Sockets Layer): Encryption for secure data transfer.
69. Cryptography Basics: Symmetric vs. asymmetric encryption, key exchange, digital signatures.

70. Digital Certificates: Provided by CAs (Certificate Authorities) to validate identity and enable HTTPS.
71. Network Security Policies: Guidelines governing safe network use, access controls, and auditing.
72. DMZ (Demilitarized Zone): A subnet that exposes external-facing services to the public.
73. WLAN Security: Wireless networks (Wi-Fi) secured by WPA2, WPA3, etc.
74. Physical Security: Ensuring network infrastructure (servers, cables, routers) is securely housed.
75. Social Engineering: Non-technical intrusion tactics—phishing, pretexting, baiting.
76. OSI Layer Attacks: Different threats/defenses at each layer (e.g., ARP spoofing at Data Link layer).
77. Network Administration Tools: ping, traceroute, netstat, nslookup, dig.
78. Packet Sniffers: Tools like Wireshark or tcpdump to analyze traffic at packet level.
79. Network Management Protocols: SNMP (Simple Network Management Protocol).
80. Logging and Monitoring: Syslog, event logs, SIEM solutions for real-time detection.
81. Basic LAN Setup: Determining IP ranges, subnet masks, gateway, DNS servers.
82. Cable Types: CAT5, CAT5e, CAT6, fiber optic, when each is typically used.
83. Structured Cabling: Standards for professional large-scale network installations.
84. Switch Configuration: Creating VLANs, trunk ports, and spanning tree protocols.
85. Router Configuration: Setting up routes (static/dynamic), NAT, ACL (Access Control Lists).
86. Basic Firewall Rules: Deny all inbound except required, allow all outbound or limit as necessary.
87. Network Addressing Plans: Efficiently assigning IP addresses based on department or subnets.
88. Redundancy and Failover: Using backup links, load balancing, or VRRP/HSRP for high availability.
89. QoS (Quality of Service): Prioritizing certain traffic (e.g., VoIP) to ensure performance.
90. Cloud Networking Basics: Virtual networks, security groups, load balancers in cloud environments.
91. SDN (Software-Defined Networking): Separating control plane from data plane for centralized management.
92. Virtualization: Using hypervisors (VMware, Hyper-V, KVM) to create virtual servers/networks.
93. Containers and Microservices: Docker networks, Kubernetes networking concepts.
94. IPv6 Deployment: Dual stack (IPv4/IPv6), IPv6 auto-configuration (SLAAC), IPv6 tunnels.
95. DNS Load Balancing: Distributing traffic across multiple servers via DNS round robin.

96. Edge Computing: Processing at the network edge to reduce latency for IoT and real-time services.
97. 5G and Wireless Evolution: Higher data rates, lower latency, use in IoT and mobile broadband.
98. Network Troubleshooting Steps: Identify the problem, isolate, test hypotheses, fix, verify.
99. Documentation: Importance of maintaining accurate network diagrams and device configurations.
100. Continuous Learning: Networking is ever-evolving, requiring ongoing study of new protocols and best practices.

These 100 points summarize the essential topics in computer networks, spanning foundational theory, protocols, hardware, addressing, security, and modern trends. They should help guide your review and study for exams or practical understanding of computer networking.