電腦網絡技術

以下是一個涵蓋「電腦網絡技術」課程或自學大綱的 100 個關鍵要點，涉及基本概念、協議和實際應用。

1. 電腦網絡的定義：一個互連設備的系統，共享資源和數據。
2. 網絡的主要功能：資源共享、通信、數據傳輸和協作。
3. 網絡的演變：從 ARPANET 和早期的 LAN 到今天的全球互聯網。
4. 常見的網絡類型：LAN（局域網）、MAN（都市區域網）、WAN（廣域網）。
5. 拓撲結構：總線、星型、環形、網狀和混合。
6. 內網、外網和互聯網：範圍差異和典型用例。
7. 標準組織：IEEE、IETF、ISO—定義和維護網絡標準和協議。
8. OSI 參考模型：一個七層概念框架，用於理解網絡功能。
9. TCP/IP 模型：一個四層（或五層）實用模型，構成互聯網的基礎。
10. OSI 和 TCP/IP 的比較：相似之處（分層方法）和不同之處（層數和抽象）。
11. 物理層的目的：關注通過物理介質傳輸原始位元。
12. 常見的傳輸介質：雙絞線電纜、同軸電纜、光纖和無線。
13. 帶寬與吞吐量：理論最大速率與實際數據傳輸速率。
14. 信號編碼：表示數據位元以進行傳輸的方法（例如，曼徹斯特編碼）。
15. 调制技術：AM、FM、PM 用於模擬到數位或數位到模擬轉換。
16. 物理層設備：集線器、重複器—主要重複信號而不檢查。
17. 數據鏈路層的目的：處理封框、地址、錯誤檢測/校正和流量控制。
18. 封框：在數據鏈路層標頭和尾部封裝數據包。
19. MAC（媒體訪問控制）地址：網絡介面卡的唯一硬件標識符。
20. 錯誤檢測機制：奇偶校驗、CRC（循環冗餘檢查）、校驗和。
21. 以太網基礎：最常見的 LAN 技術；使用具有源/目的 MAC 的框架結構。
22. 以太網框格式：前導碼、目的 MAC、源 MAC、類型/長度、負載、CRC。
23. 交換：使用 MAC 地址表在 LAN 中轉發框。
24. 交換機的學習過程：在設備通信時建立 MAC 地址表。
25. VLAN（虛擬局域網）：將一個物理 LAN 邏輯分段為多個虛擬網絡。

26. 網絡層的目的：路由、邏輯地址（IP）和路徑確定。
27. IPv4 地址格式：32 位地址，通常表示為點分十進制表示法。
28. IPv4 類別（已過時）：類 A、B、C、D、E（歷史背景，已被 CIDR 取代）。
29. CIDR（無類別域間路由）：現代靈活 IP 地址分配的方法。
30. IPv4 與 IPv6：關鍵差異（128 位地址、擴展標頭格式、自動配置）。
31. 子網：將大網絡分為較小的子網以有效使用地址。
32. NAT（網絡地址轉換）：將私有 IP 地址映射到公共 IP 以節省 IPv4 地址。
33. ARP（地址解析協議）：在 LAN 中將 IP 地址解析為 MAC 地址。
34. ICMP（互聯網控制訊息協議）：診斷工具—用於 ping、traceroute。
35. 路由與交換：路由是 IP 層（層 3），而交換是 MAC 層（層 2）。
36. 靜態路由：手動配置路由器的路由表中的路由。
37. 動態路由協議：RIP（路由信息協議）、OSPF（開放最短路徑優先）、BGP（邊界網關協議）。
38. 路由器基礎：根據 IP 地址確定數據包的下一個網絡跳轉。
39. 傳輸層的目的：端到端數據傳輸、可靠性和流量控制。
40. TCP（傳輸控制協議）：面向連接的協議，提供可靠數據傳輸。
41. TCP 段結構：源端口、目的端口、序列號、確認號等。
42. TCP 三次握手：SYN、SYN-ACK、ACK 過程設置連接。
43. TCP 四次握手：FIN、FIN-ACK、ACK 序列關閉連接。
44. TCP 流量控制：滑動窗口等機制管理數據傳輸速率。
45. TCP 擁塞控制：算法（慢啟動、擁塞避免、快速恢復、快速重傳）。
46. UDP（用戶數據報協議）：無連接、最小開銷、不保證交付。
47. UDP 段結構：源端口、目的端口、長度、校驗和、數據。
48. 端口號：服務的標識符（例如，80 用於 HTTP、443 用於 HTTPS、53 用於 DNS）。
49. 套接字：IP 地址和端口的組合，用於識別端點。
50. 應用層的目的：為用戶應用程序提供網絡服務。
51. HTTP（超文本傳輸協議）：網絡數據通信的基礎。
52. HTTP 方法：GET、POST、PUT、DELETE、HEAD 等。
53. HTTPS：使用 TLS/SSL 加密 HTTP 以進行安全的網絡通信。

54. DNS（域名系統）：將域名（例如，example.com）映射到 IP 地址。

55. DNS 解析過程：遞歸和迭代查詢、根服務器、TLD 服務器、權威服務器。

56. FTP（文件傳輸協議）：用於通過 TCP（端口 20/21）傳輸文件的傳統協議。

57. 電子郵件協議：SMTP（發送）、POP3 和 IMAP（檢索）。

58. DHCP（動態主機配置協議）：自動為設備分配 IP 地址。

59. Telnet 與 SSH：遠程訪問協議—SSH 是加密的，Telnet 不是。

60. 客戶端-伺服器模型：一種常見架構，客戶端從伺服器請求服務。

61. P2P（點對點）模型：每個節點都可以請求和提供服務。

62. 網絡技術：URL、URI、cookie、會話、基本網絡應用程序結構。

63. 網絡安全原則：機密性、完整性、可用性（CIA 三元組）。

64. 常見安全威脅：惡意軟件（病毒、蠕蟲、特洛伊木馬）、DDoS 攻擊、釣魚、SQL 注入。

65. 防火牆：根據規則過濾流量，放置在網絡邊界。

66. IDS/IPS（入侵檢測/防止系統）：監控流量以檢測可疑活動。

67. VPN（虛擬私人網絡）：通過公共網絡的加密隧道，保護遠程連接。

68. TLS/SSL（傳輸層安全/安全套接字層）：用於安全數據傳輸的加密。

69. 加密學基礎：對稱加密與非對稱加密、密鑰交換、數位簽名。

70. 數位證書：由 CA（證書授權機構）提供，以驗證身份並啟用 HTTPS。

71. 網絡安全政策：規範安全網絡使用、訪問控制和審計的指南。

72. DMZ（非軍事區）：一個子網，將面向外部的服務暴露給公眾。

73. WLAN 安全：無線網絡（Wi-Fi）由 WPA2、WPA3 等保護。

74. 物理安全：確保網絡基礎設施（伺服器、電纜、路由器）安全存放。

75. 社會工程學：非技術入侵策略—釣魚、預文本、誘餌。

76. OSI 層攻擊：每層的不同威脅/防禦（例如，ARP 欺騙在數據鏈路層）。

77. 網絡管理工具：ping、traceroute、netstat、nslookup、dig。

78. 數據包嗅探器：Wireshark 或 tcpdump 等工具在數據包級別分析流量。

79. 網絡管理協議：SNMP（簡單網絡管理協議）。

80. 日誌和監控：Syslog、事件日誌、SIEM 解決方案進行實時檢測。

81. 基本 LAN 設置：確定 IP 範圍、子網掩碼、網關、DNS 伺服器。

82. 電纜類型：CAT5、CAT5e、CAT6、光纖，何時使用每種。
83. 結構化電纜：專業大規模網絡安裝的標準。
84. 交換機配置：創建 VLAN、幹線端口和生成樹協議。
85. 路由器配置：設置路由（靜態/動態）、NAT、ACL（訪問控制列表）。
86. 基本防火牆規則：拒絕所有入站除必要外，允許所有出站或根據需要限制。
87. 網絡地址計劃：根據部門或子網有效分配 IP 地址。
88. 冗餘和故障轉移：使用備用鏈路、負載平衡或 VRRP/HSRP 以實現高可用性。
89. QoS（服務質量）：優先處理某些流量（例如，VoIP）以確保性能。
90. 雲網絡基礎：雲環境中的虛擬網絡、安全組、負載均衡器。
91. SDN（軟體定義網絡）：將控制平面與數據平面分離以進行集中管理。
92. 虛擬化：使用虛擬機（VMware、Hyper-V、KVM）創建虛擬伺服器/網絡。
93. 容器和微服務：Docker 網絡、Kubernetes 網絡概念。
94. IPv6 部署：雙重堆疊（IPv4/IPv6）、IPv6 自動配置（SLAAC）、IPv6 隧道。
95. DNS 負載均衡：通過 DNS 輪詢將流量分佈到多個伺服器。
96. 邊緣計算：在網絡邊緣處理以減少 IoT 和即時服務的延遲。
97. 5G 和無線演變：更高的數據速率、更低的延遲、在 IoT 和移動廣帶中的使用。
98. 網絡故障排除步驟：識別問題、隔離、測試假設、修復、驗證。
99. 文檔：維護準確的網絡圖和設備配置的重要性。
100. 持續學習：網絡技術不斷演變，需要不斷學習新協議和最佳實踐。