计算机网络技术

以下是涵盖“计算机网络技术”课程或自学大纲的 100 个关键点，涉及基本概念、协议和实际应用。

1. 计算机网络的定义：一个共享资源和数据的互联设备系统。
2. 网络的主要功能：资源共享、通信、数据传输和协作。
3. 网络的演变：从 ARPANET 和早期的 LAN 到今天的全球互联网。
4. 常见网络类型：LAN（局域网）、MAN（城域网）、WAN（广域网）。
5. 网络拓扑结构：总线、星型、环形、网状和混合。
6. 内网、外网和互联网：范围差异和典型用例。
7. 标准组织：IEEE、IETF、ISO—定义和维护网络标准和协议。
8. OSI 参考模型：理解网络功能的七层概念框架。
9. TCP/IP 模型：支持互联网的四层（有时五层）实用模型。
10. OSI 和 TCP/IP 的比较：相似之处（分层方法）和不同之处（层数和抽象）。
11. 物理层的目的：关注通过物理介质传输原始比特。
12. 常见传输介质：双绞线电缆、同轴电缆、光纤和无线。
13. 带宽与吞吐量：理论最大速率与实际数据传输速率。
14. 信号编码：表示数据比特以进行传输的方法（例如，曼彻斯特编码）。
15. 调制技术：AM、FM、PM 用于模拟到数字或数字到模拟转换。
16. 物理层设备：集线器、中继器—主要重复信号而不检查。
17. 数据链路层的目的：处理帧、寻址、错误检测/纠正和流量控制。
18. 帧：在数据链路层头和尾封装数据包。
19. MAC（媒体访问控制）地址：网络接口卡的唯一硬件标识符。
20. 错误检测机制：奇偶校验、CRC（循环冗余检查）、校验和。
21. 以太网基础：最常见的 LAN 技术；使用具有源/目的 MAC 的帧结构。
22. 以太网帧格式：前导、目的 MAC、源 MAC、类型/长度、有效载荷、CRC。
23. 交换：使用 MAC 地址表在 LAN 中转发帧。
24. 交换机的学习过程：在设备通信时构建 MAC 地址表。
25. VLAN（虚拟局域网）：将一个物理 LAN 逻辑分段为多个虚拟网络。

26. 网络层的目的：路由、逻辑寻址（IP）和路径确定。

27. IPv4 地址格式：32 位地址，通常表示为点分十进制表示法。

28. IPv4 类（已废弃）：类 A、B、C、D、E（历史背景，已被 CIDR 取代）。

29. CIDR（无类别域间路由）：现代灵活 IP 地址分配方法。

30. IPv4 与 IPv6：关键差异（128 位寻址、扩展头格式、自动配置）。

31. 子网划分：将大网络划分为较小的子网以高效使用地址。

32. NAT（网络地址转换）：将私有 IP 地址映射到公共 IP 以节省 IPv4 地址。

33. ARP（地址解析协议）：在 LAN 中将 IP 地址解析为 MAC 地址。

34. ICMP（互联网控制消息协议）：诊断工具—用于 ping、traceroute。

35. 路由与交换：路由是 IP 级（第 3 层），而交换是 MAC 级（第 2 层）。

36. 静态路由：手动配置路由器的路由表中的路由。

37. 动态路由协议：RIP（路由信息协议）、OSPF（开放最短路径优先）、BGP（边界网关协议）。

38. 路由器基础：根据 IP 地址确定数据包的下一个网络跳转。

39. 传输层的目的：端到端数据传递、可靠性和流量控制。

40. TCP（传输控制协议）：提供可靠数据传输的面向连接协议。

41. TCP 段结构：源端口、目的端口、序列号、确认号等。

42. TCP 三次握手：SYN、SYN-ACK、ACK 过程用于连接设置。

43. TCP 四次挥手：FIN、FIN-ACK、ACK 序列以关闭连接。

44. TCP 流量控制：滑动窗口等机制管理数据传输速率。

45. TCP 拥塞控制：算法（慢启动、拥塞避免、快速恢复、快速重传）。

46. UDP（用户数据报协议）：无连接、最小开销、不保证交付。

47. UDP 段结构：源端口、目的端口、长度、校验和、数据。

48. 端口号：服务标识符（例如，80 用于 HTTP，443 用于 HTTPS，53 用于 DNS）。

49. 套接字：用于标识端点的 IP 地址和端口组合。

50. 应用层的目的：为用户应用程序提供网络服务。

51. HTTP（超文本传输协议）：网络数据通信的基础。

52. HTTP 方法：GET、POST、PUT、DELETE、HEAD 等。

53. HTTPS：使用 TLS/SSL 加密 HTTP 以进行安全的网络通信。

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

55. DNS 解析过程：递归和迭代查询、根服务器、TLD 服务器、权威服务器。

56. FTP（文件传输协议）：用于通过 TCP（端口 20/21）传输文件的传统协议。

57. 电子邮件协议：SMTP（发送）、POP3 和 IMAP（检索）。

58. DHCP（动态主机配置协议）：自动为设备分配 IP 地址。

59. Telnet 与 SSH：远程访问协议—SSH 加密，Telnet 不加密。

60. 客户端-服务器模型：客户端请求服务器服务的常见架构。

61. P2P（点对点）模型：每个节点都可以请求和提供服务。

62. 网络技术：URL、URI、cookie、会话、基本网络应用结构。

63. 网络安全原则：保密性、完整性、可用性（CIA 三要素）。

64. 常见安全威胁：恶意软件（病毒、蠕虫、特洛伊木马）、DDoS 攻击、钓鱼、SQL 注入。

65. 防火墙：根据规则过滤流量，放置在网络边界。

66. IDS/IPS（入侵检测/防护系统）：监控流量以发现可疑活动。

67. VPN（虚拟专用网络）：通过公共网络的加密隧道，保护远程连接。

68. TLS/SSL（传输层安全/安全套接字层）：用于安全数据传输的加密。

69. 加密基础：对称加密与非对称加密、密钥交换、数字签名。

70. 数字证书：由 CA（证书授权机构）提供，以验证身份并启用 HTTPS。

71. 网络安全策略：安全网络使用、访问控制和审计的指南。

72. DMZ（非军事区）：将外部面向服务公开给公众的子网。

73. WLAN 安全：Wi-Fi 等无线网络由 WPA2、WPA3 等保护。

74. 物理安全：确保网络基础设施（服务器、电缆、路由器）安全存放。

75. 社交工程：非技术入侵策略—钓鱼、假冒、诱饵。

76. OSI 层攻击：每层的不同威胁/防御（例如，ARP 欺骗在数据链路层）。

77. 网络管理工具：ping、traceroute、netstat、nslookup、dig。

78. 数据包嗅探器：Wireshark 或 tcpdump 等工具在数据包级别分析流量。

79. 网络管理协议：SNMP（简单网络管理协议）。

80. 日志记录和监控：Syslog、事件日志、SIEM 解决方案用于实时检测。

81. 基本 LAN 设置：确定 IP 范围、子网掩码、网关、DNS 服务器。

82. 电缆类型：CAT5、CAT5e、CAT6、光纤，每种电缆的典型用途。
83. 结构化布线：专业大规模网络安装的标准。
84. 交换机配置：创建 VLAN、干线端口和生成树协议。
85. 路由器配置：设置路由（静态/动态）、NAT、ACL（访问控制列表）。
86. 基本防火墙规则：拒绝所有入站除必要外，允许所有出站或根据需要限制。
87. 网络寻址计划：根据部门或子网高效分配 IP 地址。
88. 冗余和故障转移：使用备份链路、负载均衡或 VRRP/HSRP 以实现高可用性。
89. QoS（服务质量）：优先处理某些流量（例如，VoIP）以确保性能。
90. 云网络基础：云环境中的虚拟网络、安全组、负载均衡器。
91. SDN（软件定义网络）：将控制平面与数据平面分离以实现集中管理。
92. 虚拟化：使用虚拟机（VMware、Hyper-V、KVM）创建虚拟服务器/网络。
93. 容器和微服务：Docker 网络、Kubernetes 网络概念。
94. IPv6 部署：双栈（IPv4/IPv6）、IPv6 自动配置（SLAAC）、IPv6 隧道。
95. DNS 负载均衡：通过 DNS 轮询将流量分布到多个服务器。
96. 边缘计算：在网络边缘处理以减少 IoT 和实时服务的延迟。
97. 5G 和无线演变：更高的数据速率、更低的延迟、在 IoT 和移动宽带中的使用。
98. 网络故障排除步骤：识别问题、隔离、测试假设、修复、验证。
99. 文档：维护准确的网络图和设备配置的重要性。
100. 持续学习：网络技术不断发展，需要不断学习新协议和最佳实践。

这些 100 个点总结了计算机网络的基本主题，涵盖了基础理论、协议、硬件、寻址、安全和现代趋势。它们应该帮助您指导复习和学习考试或实际理解计算机网络。