计算机网络技术

本文由 *ChatGPT* 撰写。

以下是上述 100 个要点的中文翻译，概括了“计算机网络技术”课程或自学大纲所涉及的核心内容，包括基础概念、协议与实践应用等方面。

---

1. 计算机网络的定义：由互联设备组成的系统，用于共享资源和数据。
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 和早期的局域网发展到如今的全球互联网。
4. 常见的网络类型：LAN（局域网）、MAN（城域网）、WAN（广域网）。
5. 拓扑结构：总线型、星型、环型、网状型及混合型。
6. Intranet 与 Extranet 与 Internet：范围及典型使用场景的差异。
7. 标准化组织：IEEE、IETF、ISO——负责制定并维护网络标准和协议。
8. OSI 参考模型：一个七层的概念框架，用于理解网络功能。
9. TCP/IP 模型：一个四层（或五层）的务实模型，支撑互联网的基础。
10. OSI 与 TCP/IP 对比：相似之处（分层思想）和不同点（层数、抽象方式）。
11. 物理层的目的：关注在物理介质上传输原始比特。
12. 常见传输介质：双绞线、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的区别。
14. 信号编码：将数据位表示为可传输信号的方法（如曼彻斯特编码）。
15. 调制技术：AM、FM、PM，在模拟与数字信号转换中的应用。
16. 物理层设备：集线器（Hub）、中继器（Repeater），主要是无差别转发信号。
17. 数据链路层的目的：处理成帧、寻址、错误检测/纠正和流量控制。
18. 成帧：将数据封装在数据链路层的头部和尾部中。
19. MAC（介质访问控制）地址：网卡的唯一硬件标识符。
20. 错误检测机制：奇偶校验、CRC（循环冗余校验）、校验和。
21. 以太网基础：最常见的局域网技术；使用帧结构包含源/目的 MAC。

22. 以太网帧格式：前导码、目的 MAC、源 MAC、类型/长度、数据载荷、CRC。

23. 交换技术：在局域网中使用 MAC 地址表转发帧。

24. 交换机的学习过程：设备通信时记录 MAC 地址表。

25. VLAN（虚拟局域网）：在一条物理 LAN 链路上，逻辑划分为多个虚拟网络。

26. 网络层的目的：路由、逻辑寻址（IP）和路径选择。

27. IPv4 地址格式：32 位地址，通常用点分十进制表示。

28. IPv4 地址分类（已过时）：A、B、C、D、E 类（历史用途，已被 CIDR 取代）。

29. CIDR（无类域间路由）：现代 IP 地址分配方式，提供更灵活的网络划分。

30. IPv4 与 IPv6 对比：关键差异（128 位地址、扩展首部、自配置等）。

31. 子网划分：将大型网络划分为多个较小子网，以提高地址效率。

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

33. ARP（地址解析协议）：在局域网内，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——被 ping、traceroute 等命令使用。

35. 路由与交换的区别：路由在 IP 层（第三层），交换在 MAC 层（第二层）。

36. 静态路由：手动在路由器的路由表中配置路由。

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 地址判断数据包的下一跳网络。

39. 传输层的目的：端到端数据传送、可靠性和流量控制。

40. TCP（传输控制协议）：面向连接，提供可靠数据传输的协议。

41. TCP 段结构：包括源端口、目的端口、序列号、确认号等。

42. TCP 三次握手：SYN、SYN-ACK、ACK 建立连接的过程。

43. TCP 四次挥手：FIN、FIN-ACK、ACK 依次关闭连接的过程。

44. TCP 流量控制：如滑动窗口等机制，用于控制数据传输速率。

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，开销小，但不保证数据可靠传输。

47. UDP 段结构：源端口、目的端口、长度、校验和、数据。

48. 端口号：标识服务类型（如 HTTP 的 80 端口、HTTPS 的 443 端口、DNS 的 53 端口）。

49. 套接字：由 IP 地址和端口号组合，用于标识网络通信的端点。

50. 应用层的目的：为用户应用提供网络服务。

51. HTTP（超文本传输协议）：构成 Web 数据通信的基础。

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

53. HTTPS：基于 TLS/SSL 加密的 HTTP，实现安全的 Web 通信。

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

55. DNS 解析流程：递归查询与迭代查询、根服务器、顶级域名服务器、权威服务器。

56. FTP（文件传输协议）：基于 TCP 的文件传输（使用 20/21 端口），较为传统。

57. 电子邮件协议：SMTP（发送），POP3 和 IMAP（接收）。

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：常见的网络架构，由客户端请求服务端提供服务。

61. P2P（对等）模型：每个节点既可以请求服务，也可以提供服务。

62. Web 技术：URL、URI、Cookie、Session 以及基础 Web 应用结构。

63. 网络安全原则：保密性、完整性、可用性（CIA 三元组）。

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

65. 防火墙：基于规则过滤流量，通常部署于网络边界。

66. IDS/IPS（入侵检测/防御系统）：监控流量，检测并阻止可疑活动。

67. VPN（虚拟专用网）：在公共网络上建立加密隧道，实现安全的远程连接。

68. TLS/SSL（传输层安全/安全套接字层）：为数据传输提供加密。

69. 密码学基础：对称加密与非对称加密，密钥交换，数字签名等。

70. 数字证书：由 CA（证书颁发机构）签发，用于验证身份并支持 HTTPS。

71. 网络安全策略：安全使用网络、访问控制和审计的指导方针。

72. DMZ（非军事区）：对外提供服务的子网，置于内网与外网之间。

73. WLAN 安全：无线网络（Wi-Fi）安全标准，如 WPA2、WPA3 等。

74. 物理安全：确保服务器、线缆和路由器等网络设施的安全防护。

75. 社会工程：利用非技术手段进行攻击，如钓鱼、电信欺诈等。

76. OSI 各层攻击：不同层级的攻击与防御措施（如数据链路层的 ARP 欺骗）。
77. 网络管理常用工具：ping、traceroute、netstat、nslookup、dig。
78. 数据包嗅探器：Wireshark、tcpdump 等，可在包级别分析流量。
79. 网络管理协议：SNMP（简单网络管理协议）。
80. 日志与监控：Syslog、事件日志、SIEM 系统，实现实时监控和审计。
81. 基础局域网配置：确定 IP 范围、子网掩码、网关、DNS 服务器等。
82. 布线类型：CAT5、CAT5e、CAT6、光纤等，及其典型应用场景。
83. 结构化布线：适用于大规模专业网络安装的规范和标准。
84. 交换机配置：创建 VLAN、配置干道端口、生成树协议等。
85. 路由器配置：设置静态/动态路由、NAT、ACL（访问控制列表）。
86. 基础防火墙规则：默认拒绝所有入站流量，仅允许必要流量；出站流量可全部放行或受限。
87. 网络地址规划：根据部门或子网需求高效分配 IP。
88. 冗余与故障切换：备份链路、负载均衡或 VRRP/HSRP 等高可用技术。
89. QoS（服务质量）：为特定业务（如 VoIP）设置优先级，确保性能。
90. 云网络基础：虚拟网络、安全组、云负载均衡器等。
91. SDN（软件定义网络）：将控制平面与数据平面分离，进行集中化管理。
92. 虚拟化：使用虚拟机管理程序（VMware、Hyper-V、KVM）实现服务器/网络虚拟化。
93. 容器和微服务：Docker 网络、Kubernetes 网络相关概念。
94. IPv6 部署：双栈（IPv4/IPv6），IPv6 自动配置（SLAAC），隧道技术。
95. DNS 负载均衡：通过 DNS 轮询将流量分散到多个服务器。
96. 边缘计算：在网络边缘处理数据，以降低物联网和实时应用的延迟。
97. 5G 与无线网络演进：更高数据速率、更低时延，在物联网和移动宽带中的应用。
98. 网络故障排除步骤：确认问题、定位故障、测试假设、修复并验证。
99. 文档管理：维护精准的网络拓扑图和设备配置。
100. 持续学习：网络技术不断发展，需要持续关注新协议和最佳实践。

这些要点从网络理论到协议、硬件、寻址、安全以及现代趋势，为“计算机网络”考试或实际工作提供了系统梳理与复习指南。结合实践操作、文档和工具使用，将有助于更好地掌握网络技术。