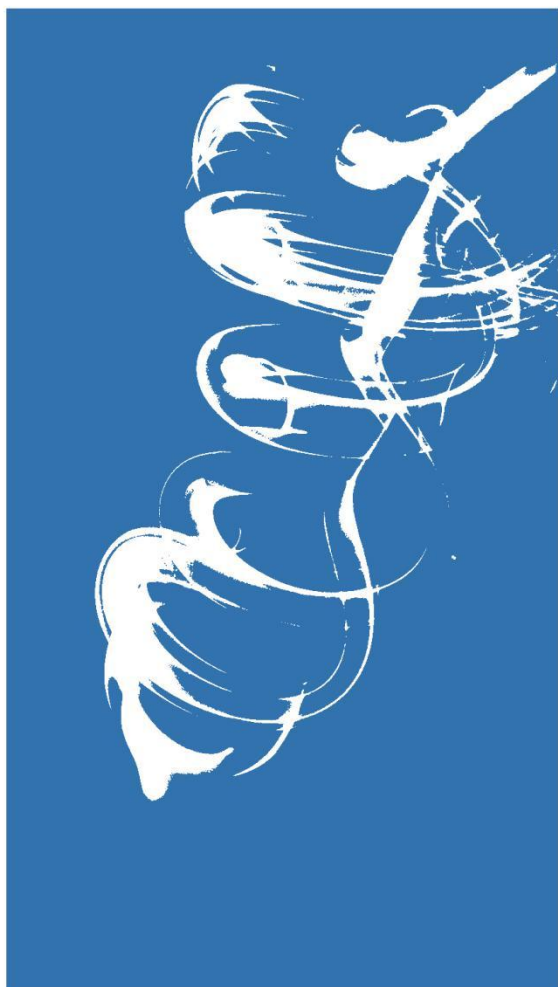


SUNLANDS MI XUN ZI LIAO



# 密训资料

计算机网络原理

SUNLANDS MI XUN ZI LIAO

微信扫码关注  
【尚德学术中心】



自考锦鲤学霸集训地  
尚德学术精英大本营



---

## 目录

|     |                 |   |
|-----|-----------------|---|
| 第一章 | 计算机网络概述 .....   | 1 |
| 第二章 | 网络应用 .....      | 2 |
| 第三章 | 传输层 .....       | 3 |
| 第四章 | 网络层 .....       | 4 |
| 第五章 | 数据链路层与局域网 ..... | 5 |
| 第六章 | 物理层 .....       | 6 |
| 第七章 | 无线与移动网络 .....   | 6 |
| 第八章 | 网络安全基础 .....    | 7 |

## 第一章 计算机网络概述

| 知识点名称               | 知识点内容  |   |
|---------------------|--|---|
| 协议的定义<br>★          | 协议是网络通信实体之间在数据交换过程中需要遵循的规则或约定，是计算机网络有序运行的重要保证。   |   |
| 协议的 3 个基本要素<br>★★★★ | 语法   | 定义实体之间交换信息的格式与结构。   |
|                     | 语义   | 定义实体之间交换的信息中需要发送哪些控制信息，这些信息的具体含义，以及针对不同含义的控制信息，接收信息端应如何响应。  |
|                     | 时序   | 也称为同步，定义实体之间交换信息的顺序以及如何匹配或适应彼此的速度。  |
| 计算机网络的功能<br>★★★★    | 硬件资源共享   | 如云计算、云存储。   |
|                     | 软件资源共享   | 如软件即服务（SaaS）。   |
|                     | 信息资源共享   | 如信息交换。  |
| 按拓扑结构分类<br>★★★★     | 星形拓扑结构   | 比较多见于局域网、个域网中   |
|                     | 总线型拓扑结构  | 在早期的局域网中比较多见。   |
|                     | 环形拓扑结构   | 多见于早期的局域网、园区网和城域网中。   |
|                     | 网状拓扑结构   | 比较多见于广域网、核心网络等。   |
|                     | 树形拓扑结构   | 目前，很多局域网采用这种拓扑结构。   |
|                     | 混合拓扑结构   | 绝大多数实际网络的拓扑都属于混合拓扑结构，比如 Internet。   |
| 数据交换技术<br>★★        | 电路交换   | 最早出现的一种交换方式。<br>优点：实时性高，时延和时延抖动都较小。<br>缺点：不适用于突发性数据传输，信道利用率低，且传输速率单一。   |
|                     | 报文交换   | 现在计算机网络没有采用。<br>优点：相对电路交换，报文交换线路利用率高。<br>缺点：不适用于实时通信，不得不丢弃报文。   |
|                     | 分组交换   | 目前计算机网络广泛采用的技术。<br>优点：（1）交换设备存储容量要求低（2）交换速度快（3）可靠传输效率高（4）更加公平。<br>分组长度的确定：分组长度与延迟时间：在其他条件相同的情况下，分组长度越长，延迟时间越长。分组长度与误码率：最佳分组长度 $L_{opt} = \sqrt{\frac{h}{P_e}}$ 。最高信道利用率可以表示为 $\eta_{max} = (1 - \sqrt{hP_e})^2$ |
| 计算机网络体系结构的含义★★      | 计算机网络所划分的层次以及各层协议的集合。  |   |
| OSI 参考模型★★          | <div style="display: flex; align-items: center;"> <div style="margin-right: 10px;"> <p>（信息处理服务）</p> <p>网络高层</p> <p>（数据交换和传输）</p> <p>网络低层</p> </div> <div style="display: flex; flex-direction: column; align-items: center;"> <div style="margin-bottom: 10px;"> <p>端对端层</p> <div style="border: 1px solid black; padding: 5px; margin: 5px;">7 应用层</div> <div style="border: 1px solid black; padding: 5px; margin: 5px;">6 表示层</div> <div style="border: 1px solid black; padding: 5px; margin: 5px;">5 会话层</div> <div style="border: 1px solid black; padding: 5px; margin: 5px;">4 传输层</div> </div> <div> <p>结点到结点点层</p> <div style="border: 1px solid black; padding: 5px; margin: 5px;">3 网络层</div> <div style="border: 1px solid black; padding: 5px; margin: 5px;">2 数据链路层</div> <div style="border: 1px solid black; padding: 5px; margin: 5px;">1 物理层</div> </div> </div> <div style="margin-left: 20px;"> <p>与提供给用户的网络服务相关。在 Internet 上常见的一些网络应用大多在这一层。例如：<b>www 服务：HTTP；文件传输：FTP；电子邮件：SMTP 和 POP3</b></p> <p>处理应用实体间交换数据的语法，解决格式和数据表示的差别，为应用层提供一致格式；还可实现文本压缩/解压缩、数据加密/解密、字符编码的转换等功能。</p> <p>会话层是指用户与用户的连接，通过在两台计算机间建立、管理和终止通信来完成对话。</p> <p>进程-进程层次。功能：复用/分解、端到端的可靠数据传输、连接控制、流量控制和拥塞控制机制等。<b>TCP：连接可靠传输协议。UDP：无连接不可靠传输协议。</b></p> <p>将分组通过交换网络传送到目的主机。功能：数据转发与路由。<b>整个 TCP/IP 参考模型的核心。核心协议：IP 协议。</b></p> <p>功能：实现相邻结点之间数据可靠而有效的传输。有：帧同步功能，流量控制、链路管理、寻址。</p> <p>功能：在传输介质上实现无结构比特流传输；规定数据终端设备（DTE）与数据通信设备（DCE）之间接口的相关特性，包括机械、电气、功能和规程。</p> </div> </div> |   |

|                           |                                   |             |        |           |
|---------------------------|-----------------------------------|-------------|--------|-----------|
| 3 种参考模型和 OSI 参考模型有关术语★★★★ |                                   |             |        |           |
|                           | OSI 参考模型                          | TCP/IP 参考模型 | 五层参考模型 | 各层 PDU 名称 |
| 计算机网络与因特网发展简史★            | ARPAnet 是第一个分组交换计算机网络，也是当今因特网的祖先。 |             |        |           |

## 第二章 网络应用

| 知识点名称        | 知识点内容   |   |  |
|--------------|---|---|--|
| 计算机网络应用体系结构★ | 客户/服务器 (C/S) 结构网络应用                                 | 最典型、最基本；通信只在客户与服务 器间进行。                                       |  |
|              | 纯 P2P 结构网络应用  | 所有通信都在对等的通行方之间直接 进行。  |  |
|              | 混合结构网络应用  | 存在客户与服务器之间传统 C/S 结构 的通信，也存在客户之间的通信。                           |  |
| 网络应用通信基本原理★  | 典型的网络应用编程接口是套接字，标识套接字的编号叫端口号，IP 地址用于唯一标识一个主机或路由器接口。 |   |  |
|              | TCP   | 面向连接、提供可靠数据流传输的传输控制协议。  |  |
|              | UDP   | 无连接不提供可靠数据传输的用户数据报协议。   |  |
| 层次化域名空间★★★   | “... 三级域名. 二级域名. 顶级域名”，各标号分别代表不同级别的域名。              |   |  |
| 域名服务器★★★★    | 根域名服务器  | 最重要的域名服务器，共 13 个，从 a 一直到 m。                                   |  |
|              | 顶级域名服务器   | 国家顶级域名  | cn(中国)，us(美国)，uk(英国)。  |
|              |   | 通用顶级域名  | com(公司和企业)，net(网络服务机构)，org(非盈利性组织)，edu(教育机构)，gov(政府部门)，mil(军事部门)，int(国际组织) |
|              |   | 基础结构域名  | arpa(用于反向域名解析)   |
|              | 权威域名服务器   | 负责一个区的域名服务器，保存该区中的所有主机的域名到 IP 地址的映射。                          |  |
|              | 中间域名服务器   | 既不是根域名服务器，也不是顶级域名服务器和权威域名服务器的域名服务器。                           |  |
| 域名解析过程★★★    | 递归解析  | 依次查询  | 若本地域名服务器没有被查询域名信息，都需要从根域名服务器查询。  |
|              | 迭代解析  | 直接响应结果  |  |
| 万维网应用结构★★★★  | 浏览器   | Web 应用的客户端软件  |  |
|              | Web 服务器   | Web 应用的服务器软件  |  |
|              | HTTP  | 客户与服务器之间的交互基于应用层协议。每个 Web 页面的寻址：URL 地址=主机域名（或 IP 地址）+ 对象的路径名。 |  |
| 电子邮件系统★★★★   | 邮件服务器   | 功能是发送和接收邮件，向发信人报告邮件传送情况，是电子邮件体系结构的核 心。                        |  |
|              | 简单邮件传输协议  | 特点  | 1、只能传送 7 位 ASCII 码文本内容。【多用途互联网邮件扩展 (MIME) 定义了将非 7 位 ASCII 码内容转换为           |

|                       |             |                              |  |
|-----------------------|-------------|------------------------------|--|
|                       | (SMTP)      |                              | 7 位 ASCII 码的编码规则。MIME 主要包括 3 个部分:(1) 5 个 MIME 邮件首部字段 (2) 定义了多种邮件内容的格式 (3) 定义了邮件传送编码。】<br>2、传送的邮件内容中不能包含“CRLF. CRLF”。<br>3、SMTP 是“推动”协议。<br>4、SMTP 使用 TCP 连接是持久的。 |
|                       |             | 发送过程                         | 握手阶段、邮件传输阶段、关闭阶段   |
|                       | 用户代理        |                              |  |
|                       | 邮件读取协议      | POP3                         | 使用传输层 TCP。POP3 协议交互过程可以分为 3 个阶段: 授权、事务处理和更新。   |
|                       |             | IMAP                         | IMAP 服务器维护了 IMAP 会话的用户状态信息, 允许用户代理只读邮件的部分内容。   |
|                       |             | HTTP                         | HTTP 是 Web 邮件系统的邮件读取协议。  |
| Socket 编程<br>基础<br>★★ | 分类          | 数据报类型套接字 SOCK_DGRAM (面向 UDP) |  |
|                       |             | 流式套接字 SOCK_STREAM (面向 TCP)   |  |
|                       |             | 原始套接字 SOCK_RAW               |  |
|                       | 常用 API 函数功能 | socket()                     | 创建套接字  |
|                       |             | close()                      | 关闭一个套接字  |
|                       |             | bind()                       | 绑定套接字的本地端点地址   |
|                       |             | connect()                    | 将客户套接字与服务器连接   |
|                       |             | listen()                     | 置服务器端的流(TCP)为监听状态  |
|                       |             | accept()                     | 从监听状态的流套接字的客户连接请求队列中, 取出排在最前的一个客户请求, 并且创建一个新的套接字来与客户套接字建立 TCP 连接。  |
|                       |             | send()                       | 发送数据   |
|                       |             | sendto()                     |  |
|                       |             | recv()                       | 接收数据   |
|                       |             | recvfrom()                   |  |
|                       |             | setsockopt()                 | 设置套接字选项  |
|                       |             | getsockopt()                 | 读取套接字选项  |

### 第三章 传输层

| 知识点名称                 | 知识点内容                         |              |                  |
|-----------------------|-------------------------------|--------------|------------------|
| 传输层功能<br>构★★          | 传输层的核心任务是为应用进程之间提供端到端的逻辑通信服务。 |              |                  |
| 端口号的分类★               | 服务端使用的端口号                     | 熟知端口号        | 0~1023           |
|                       |                               | 登记端口号        | 1024~49151       |
|                       | 客户端使用的端口号                     | 客户端端口号或暂时端口号 | 49152~65535      |
| 常用协议与端口号的对应关系<br>★★★★ | HTTP 超文本传输协议 (Web 服务器的默认端口号)  |              | 80               |
|                       | SMTP 简单邮件传输协议                 |              | 25               |
|                       | POP3 邮局协议版本 3                 |              | 110              |
|                       | FTP 文件传送协议                    |              | 21 控制连接 (默认)     |
|                       |                               |              | 20 数据连接          |
|                       | DNS 域服务器所开放的端口                |              | 53               |
|                       | DHCP 动态主机配置协议                 |              | DHCP 客户端 68      |
|                       |                               |              | DHCP 服务器端 67     |
|                       | Telnet 远程终端协议                 |              | 23               |
|                       | RIP 信息协议                      |              | 520              |
|                       | SNMP 简单网络管理协议                 |              | get UDP 161 (默认) |



|             |  |      |  |                               |
|-------------|--|------|--|-------------------------------|
|             |  |      |  | trap UDP 162                  |
| 传输层的复用与分解★  | 关键：IP 地址和端口号能够唯一标识一个套接字  | 无连接  | 提供协议   | UDP                           |
|             |  |      | 唯一标识   | <目的 IP 地址，目的端口号>              |
|             |  | 面向连接 | 提供协议   | TCP                           |
|             |  |      | 唯一标识   | <源 IP 地址，目的 IP 地址，源端口号，目的端口号> |
| 滑动窗口协议★★★   | 选择重传（SR）协议   |      | 发送窗口 $Ws>1$  | 接收窗口 $Wr>1$                   |
|             | 回退 N 步（GBN）协议  |      | 发送窗口 $Ws\geq1$   | 接收窗口 $Wr=1$                   |
| UDP 数据报结构★★ | <div><div><div>01631</div><div><div>源端口号</div><div>目的端口号</div><div>长度</div><div>校验和</div></div><div>应用数据</div></div><div>UDP 首部为 4 个字段，每个字段由 2 个字节组成</div></div> |      |  |                               |
| UDP 校验和★    | 计算内容包括   |      | UDP 伪首部、UDP 首部和应用层数据   |                               |
|             | 计算规则   |      | (1) 参与运算的内容按 16 位对齐求和。(2) 求和过程中遇到任何溢出（即进位）都被回卷（即进位与和的最低为再加），最后得到的和取反码。 |                               |

#### 第四章 网络层

| 知识点名称            | 知识点内容               |  |                  |
|------------------|---------------------|--|------------------|
| 网络层服务★★★         | 网络层的功能：转发、路由选择、连接建立 |  |                  |
|                  | 连接建立（分组交换网络）        | 仅在网络层提供连接服务：虚电路（VC）网络【通信之前，双方需要先建立虚电路（网络层逻辑连接），通信结束后再拆除虚电路。】 |                  |
|                  |                     | 仅在网络层提供无连接服务：数据报网络【按照目的主机地址进行路由选择的网络。】                       |                  |
| 数据报网络与虚电路网络的比较★★ | 项目                  | 虚电路交换  | 数据报交换            |
|                  | 端到端连接               | 需要先建立连接  | 不需要建立连接          |
|                  | 地址                  | 每个分组含有一个短的虚电路号   | 每个分组包含源和目的端地址    |
|                  | 分组顺序                | 按序发送，按序接收  | 按序发送，不一定按序接收     |
|                  | 路由选择                | 建立 VC 时需要路由选择，之后所有分组都沿此路由转发                                  | 对每个分组独立选择        |
|                  | 转发结点失效的影响           | 所有经过失效结点的 VC 终止  | 除了崩溃时丢失分组外，无其他影响 |
|                  | 差错控制                | 由通信网络负责  | 由端系统负责           |
|                  | 流量控制                | 由通信网络负责  | 由端系统负责           |
|                  | 拥塞控制                | 若有足够的缓冲区分配给已经建立的 VC，则容易控制                                    | 由端系统负责           |
|                  | 状态信息                | 建立的每条虚电路都要求占用经过的每个结点的表空间                                     | 网络不存储状态信息        |
|                  | 通信类型                | 传输质量要求高的通信   | 数据通信，非实时通信       |
|                  | 典型网络                | X.25、帧中继、ATM   | 因特网              |
| 异构网络互连★★★        | 网络层                 | 路由器  |                  |
|                  | 数据链路层               | 交换机和网桥（交换机就是多端口的网桥，是目前应用最广泛的数据链路层设备。）                        |                  |
|                  | 物理层                 | 集线器和中继器  |                  |
| 拥塞控制措施★★         | 流量感知路由              | 将网络流量引导到不同的链路上，均衡网络负载，从而避免拥塞发生。                              |                  |

|                    |  |   |                                     |         |
|--------------------|--|---|-------------------------------------|---------|
|                    | 准入控制   | 是一种广泛应用于虚电路网络的拥塞预防技术。<br>审核新建虚电路，如果新虚电路会导致网络拥塞，那么网络拒绝建立该新虚电路。                           |                                     |         |
|                    | 流量调节   | 在网络发生拥塞时，可以通过调整发送方向网络发送数据的速率来消除拥塞。抑制分组、背压   |                                     |         |
|                    | 负载脱落   | 通过有选择地主动丢弃一些数据报，来减轻网络负载，从而缓解或消除拥塞。  |                                     |         |
| 分类地址<br>★★★★       | 类  | 前缀长度  | 前缀                                  | 首字节     |
|                    | A  | 8 位   | 0xxxxxxx                            | 0~127   |
|                    | B  | 16 位  | 10xxxxxx xxxxxxxx                   | 128~191 |
|                    | C  | 24 位  | 110xxxxx xxxxxxxx xxxxxxxx          | 192~223 |
|                    | D  | 不可用   | 1110xxxx xxxxxxxx xxxxxxxx xxxxxxxx | 224~239 |
|                    | E  | 不可用   | 1111xxxx xxxxxxxx xxxxxxxx xxxxxxxx | 240~255 |
| ICMP<br>★★         | ICMP 包括 3 个字段  |   | 类型、代码和校验和。                          |         |
|                    | 差错报告报文   |   | 终点不可达、源点抑制、时间超时、参数问题、路由重定向。         |         |
|                    | 询问报文   |   | 回声（echo） 请求/应答、 时间戳请求/应答。           |         |
| IPv6 数据报格式<br>★★★★ | 地址长度为 128 位。IPv4 地址：地址长度为 32 位。<br>通常采用 8 组冒号分隔的十六进制数地址形式表示。对于连续的多组 “0000”，可以利用连续的两个 “:” （即 “::” ）代替，但在一个 IPv6 地址中只能用一次 “::” 。 |   |                                     |         |
| IPv6 地址<br>★★★★    | 单播地址   | 唯一标识网络中的一个主机或路由器网络接口。<br>可以作为 IPv6 数据报的源地址和目的地址。  |                                     |         |
|                    | 组播地址   | 标识网络中的一组主机。<br>只能用作 IPv6 数据报的目的地址。（向一个组播地址发送 IP 数据报，该组播地址标识的多播组每个成员都会收到一个该 IP 数据报的一个副本） |                                     |         |
|                    | 任播地址   | 标识网络中的一组主机。<br>只能用作 IPv6 数据报的目的地址。（但当向一个任播地址发送 IP 数据报时，只有该任播地址标识的任播组的某个成员收到该 IP 数据报。）   |                                     |         |

## 第五章 数据链路层与局域网

| 知识点名称                  | 知识点内容   |  |   |
|------------------------|---|--|---|
| 差错控制<br>★★★★           | 噪声分类  | 随机噪声   | 引起随机差错或独立差错。通常呈现为随机的比特差错。   |
|                        |   | 冲击噪声   | 指突然发生的噪声。引起的差错称为突发差错。差错通常集中发生在某段信息。突发错误发生的第一位错误与最后一位错误之间的长度称为 <b>突发长度</b> 。 |
| 差错编码的检错与纠错能力★          | 检错编码  | 如果编码集的汉明距离 $ds=r+1$ ，则该差错编码可以检测 $r$ 位的差错。                |   |
|                        | 纠错编码  | 如果编码集的汉明距离 $ds=2r+1$ ，则该差错编码可以检测 $r$ 位的差错。               |   |
| 信道划分<br>MAC 协议<br>★★★★ | 频分多路复用 (FDM)  |  | 频域划分制，优点分路方便，缺点串扰。  |
|                        | 时分多路复用 (TDM)  | 同步时分多路复用 (STDM)：按照固定顺序把时隙分配给各路信号。易造成信道资源浪费。              |   |
|                        |   | 异步时分多路复用 (ATDM)：也叫作统计时分多路复用 (STDM)，用户的数据并不是按照固定的时间间隔发送的。 |   |
|                        | 波分多路复用 (WDM)  |  | 广泛应用于 <b>光纤</b> 通信中。  |
| 分散式控制<br>★★★★          | 码分多路复用 (CDM)  |  |   |
|                        | 基于扩频技术，利用更长的相互正交的码组   |  |   |
| 分散式控制<br>★★★★          | 环网上最严重的两种错误： <b>令牌丢失</b> 和 <b>数据帧无法撤销</b> 。                                 |  |   |
| MAC 地址<br>★★           | MAC 地址长度为 6 字节，即 48 位。采用十六进制表示法 (用 A~F 表示 10~15)：每个字节表示一个十六进制数，“-”或“:”连接起来。 |  |   |



|                     |   |                                       |                |                |                          |
|---------------------|---|---------------------------------------|----------------|----------------|--------------------------|
| 以太网帧结构<br>★★★★      | <div> <div>6字节</div> <div>6字节</div> <div>2字节</div> <div>46~1500字节</div> <div>4字节</div> </div> |                                       |                |                |                          |
|                     | 目的地址  | 源地址                                   | 类型             | 数据             | CRC                      |
| 虚拟局域网<br>★★★★       | 划分虚拟局域网的方法：基于交换机端口划分、基于 MAC 地址划分、基于上层协议类型或地址划分。   |                                       |                |                |                          |
| 点对点链路协议<br>★★★<br>★ | PPP   | 字节填充技术（遇到 01111110 填充控制转义字节：01111101） |                |                |                          |
|                     |   | 1字节                                   | 1字节            | 1字节            | 1字节或2字节 可变长度 2字节或4字节 1字节 |
|                     |   | 标志<br>01111110                        | 地址<br>11111111 | 控制<br>00000011 | 协议 信息 校验和 标志<br>01111110 |
|                     | HDLCL   | 位填充技术（零比特填充）<br>3 种类型的帧：信息帧、管理帧、无序号帧。 |                |                |                          |

## 第六章 物理层

| 知识点名称         | 知识点内容    |   |
|---------------|----------|---|
| 物理介质<br>★     | 引导型传输介质  | 架空明线 2、双绞线 3、同轴电缆 4、光纤  |
|               | 非引导型传输介质 | 1、地波传输 2、天波传输 3、视线传输  |
| 信道传输特性★       | 恒参信道     | 1) 对信号幅值产生固定的衰减。2) 对信号输出产生固定的时延。  |
|               | 随参信道     | 信号的传输衰减随时间随机变化。2) 信号的传输时延随时间随机变化。3) 存在多径传播现象。   |
| 物理层接口特性<br>★★ | 机械特性     | 也叫物理特性，指明通信实体间硬件连接接口的机械特点。  |
|               | 电气特性     | 规定了在物理连接上，导线的电气连接及有关电路的特性   |
|               | 功能特性     | 指明物理接口各条信号线的用途，包括接口信号线功能的规定方法以及接口信号线的功能分类   |
|               | 规程特性     | 即通信协议，指明利用接口传输比特流的全过程，以及各项用于传输的事件发生的合法顺序，包括事件的执行顺序和数据传输方式，即在物理连接建立、维持和交换信息时，DTE、DCE 双方在各自电路上的动作序列等。 |


## 第七章 无线与移动网络

| 知识点名称                   |  | 知识点内容   |  |       |      |       |      |      |
|-------------------------|--|---|--|-------|------|-------|------|------|
| 无线网络基本结构<br>★★          |  | 1、无线网络主要包括：无线主机、无线链路、基站、网络基础设施。<br>2、自组织网络、或称为特定网络，也称为 Ad Hoc 网络：无线主机不通过基站(即没有基站)，直接与另一个无线主机直接通信的无线网络模式。<br>基础设施模式：无线主机与基站关联。 |  |       |      |       |      |      |
| 无线链路与无线网络特性★★           |  | 有线网络与无线网络的重要区别主要在：数据链路层和物理层。<br>无线链路有别于有线链路的主要表现：信号强度的衰减、干扰、多径传播。   |  |       |      |       |      |      |
| 移动结点的路由选择               |  | (1) 间接路由选择    (2) 直接路由选择  |  |       |      |       |      |      |
| IEEE 802. 11 帧★★★       |  | 3 种类型：控制帧、数据帧和管理帧。IEEE 802. 11 的 MAC 协议采用 CSMA/CA 协议。   |  |       |      |       |      |      |
|                         |  | 4 个地址<br>字段   | 去往 AP  | 来自 AP | 地址 1 | 地址 2  | 地址 3 | 地址 4 |
|                         |  |   | 0  | 1     | 目的地址 | AP 地址 | 源地址  | ——   |
| 移动通信<br>2G/3G/4G/5G 网络★ |  | 2G  | 代表性体制是 GSM 系统，采用的是 FDMA（频分多址）和 TDMA（时分多址）混合接入的方式。                    |       |      |       |      |      |
|                         |  | 3G  | 最关键的技术是无线传输技术。除了卫星接口技术外，被分为 CDMA（码分多址）和 TDMA（时分多址）两大类，其中 CDMA 占主导地位。 |       |      |       |      |      |
|                         |  | 4G  | LTE 系统。特征：高速率传输、智能化、业务多样化、无缝接入、后向兼容、                                 |       |      |       |      |      |

|                  |        |   |
|------------------|--------|---|
|                  |        | 经济。   |
|                  | 5G     | 有望共用一标准。  |
| 其他典型无线网络简介<br>★★ | WiMax  | 全球微波互联接入(WiMax)称为 IEEE 802.16 标准,目的是在更大范围内为用户提供可以媲美有线网络的无线通信解决方案。         |
|                  | 蓝牙     | IEEE 802.15.1 网络以小范围、低功率和低成本运行。   |
|                  | ZigBee | IEEE 第二个个人区域网络标准是 IEEE 802.15.4,称为 ZigBee。ZigBee 主要以低功率、低数据速率、低工作周期应用为目标。 |

## 第八章 网络安全基础

| 知识点名称                               | 知识点内容  |  |  |
|-------------------------------------|--|--|--|
| 数据加密<br>★★★★                        | 密码学  | 密码编码学  | 指将密码变化的客观规律应用于编制密码来保守通信秘密。   |
|                                     |  | 密码分析学  | 研究密码变化客观规律中的固有缺陷，并应用于破译密码以获取通信情报。  |
|                                     | 传统加密方式   |  | 替代密码   |
|                                     |  |  | 换位密码   |
|                                     | 对称密钥加密   |  | DES 加密算法   |
|                                     |  |  | 三重 DES   |
|                                     |  |  | AES 加密   |
| IDEA                                |  |  |  |
| 非对称/公开密钥加密<br>(解决了对称加密算法<br>密钥分发问题) |  | 比较典型的公开密钥加密算法有 Diffie-Hellman 算法和 RSA 算法。<br>公开密钥密码的一个重要特性：<br>$K_B^-(K_B^+(m)) = m = K_B^+(K_B^-(m))$ |  |
| 典型的散列函数<br>★★                       | MD5  | MD5 对报文散列后，得到 128 位的散列值。   |  |
|                                     | SHA-1  | SHA-1 可产生一个 160 位的散列值。SHA-1 是典型的用于创建数字签名的单向散列算法。   |  |
| 报文认证★                               | 对报文 m 应用散列函数 H，得到一个固定长度的散列码，称为报文摘要，记为 H(m)。报文摘要可以作为报文 m 的数字指纹。                         |  |  |
| 数字签名★                               | 数字签名就是用私钥进行加密，而认证就是利用公开密钥进行正确地解密，所以报文加密技术是数字签名的基础。当接收者和发送者之间有害害冲突时，此时须借助满足前述要求的数字签名技术。 |  |  |
| 密钥分发中心与证书认证机构                       | 秘 钥 分 发 中 心<br>(KDC)   |  | 对称密钥分发的典型解决方案是，通信各方建立一个大家都信赖的 KDC，并且每一方和 KDC 之间都保持一个长期的共享密钥。   |
|                                     | 证书认证机构 (CA)  |  | 将公钥与特定实体绑定。  |
| 防火墙分类<br>★★                         | 无状态分组过滤器（无状态分组过滤器是典型的部署在内部网络和网络边缘路由器上的防火墙。）、有状态分组过滤器和应用网关。                             |  |  |
| SSL 协议栈<br>★                        | SSL 更改密码规格协议   |  | 用于通信过程，通信双方修改密码组，标志着加密策略的改变。最后报文内容会封装到记录协议报文之中。  |
|                                     | SSL 警告协议   |  | 用于在握手过程或者数据加密等出错或者发生异常时，为对等实体传递 SSL 警告或者终止当前连接。<br>协议包含两个字节：警告级别和警告代码。   |
|                                     | SSL 握手协议   |  | 协商密码组和建立密钥，在协商确认后，才能进行派生密钥的导出等操作，协商结果是 SSL 记录协议的基础。<br>在 SSL3.0 版本中，握手过程用到 3 个协议：SSL 握手协议、SSL 更改密码规格协议、SSL 警告协议。 |
|                                     | SSL 记录协议   |  | 描述了 SSL 信息交换过程中的消息格式，前面的 3 个协  |

|   |                |  |
|---|----------------|--|
|   |                | 议都需要记录协议进行封装与传输。   |
| <b>IPSec 体系</b><br><b>简介</b><br> | 封装安全载荷协议 (ESP) | AH 和 ESP 是核心。与两种模式(传输模式、隧道模式)结合起来共有 4 种组合：传输模式 AH、隧道模式 AH、传输模式 ESP、隧道模式 ESP。 |
|   | 认证头 (AH) 协议    |  |
|   | 安全关联 (SA)      | 在发送数据之前，需要在发送实体和接收实体之间进行安全关联 SA。   |
|   | 密钥交换与管理 (IKE)  | 是 IPsec 唯一的密钥管理协议。   |