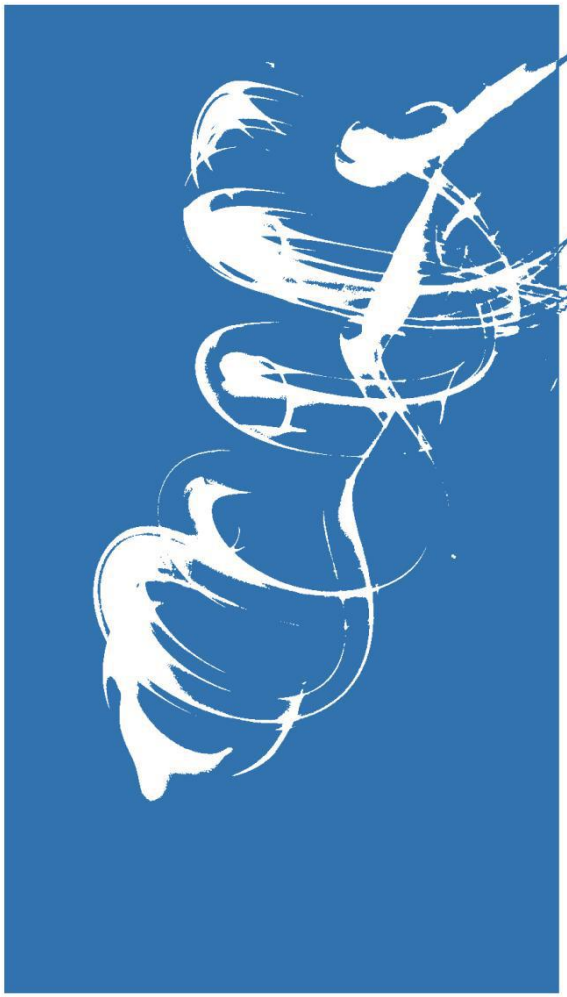
尚德机构™
SUNLANDS



密训资料

计算机网络原理

SUNLANDS MI XUN ZI LIAO

目录

第一章 计算机网络概述

知识点名称	知识点内容	
计算机网络的定义★	一个计算机网络是由**资源子网**和**通信子网**构成的。资源子网负责信息处理，通信子网负责全网中的信息传递。	
协议的定义★★★	1、定义：**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。 2、**3个基本要素**： **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**（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★★★	**1、核心**功能是：实现**资源共享** **2、**包括： **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★★★	**星形拓扑结构**	比较多见于局域网、个域网中。 **优点**：1)易于监控与管理；2)故障诊断与隔离容易。 **缺点**：中央结点是网络的瓶颈，一旦故障，全网瘫痪，网络规模**受限于中央结点的端口数**量。
	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。 **优点**：1)所需电缆长度短；2)可使用光纤；3)避免冲突；4)网络性能稳定（闭合回路） **缺点**：故障检测麻烦（任意结点出现故障都会造成网络瘫痪）
	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。
计算机网络结构★★	大规模现代计算机网络结构包括的部分：（1）网络边缘（2）接入网络（3）网络核心。比较典型的分组交换设备是**路由器和交换机**等。	
数据交换技术★★	**电路交换**：最早出现的一种交换方式。 **报文交换**：现在计算机网络没有采用。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。**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**。	
时延★★★	通常将连接两个结点的直接链路称为一个“**跳步**”，简称“**跳**”。 **传输时延**：当一个分组在输出链路发送时，从发送第一位开始，到发送完最后一位为止，所用的时间，称为传输时延，也称为发送时延，记为dt。设分组长度Lbit，链路带宽（即速率）Rbit/s，则dt=L/R。 **传播时延**：信号从发送端发送出来，经过一定距离的物理链路到达接收端所需要的时间，称为传播时延。设物理链路长度Dm，信号传播速度Vm/s，则dp=D/V。 **时延带宽积**：一段物理链路的传播时延dp与链路带宽R的乘积，记为G，G=dp*R，G的单位是位（bit）。物理意义在于：如果将物理链路看作一个传输数据的管道的话，时延带宽积表示一段链路可以容纳的数据位数，也称为以位为单位的链路长度。	
吞吐量★	对于分组交换网络，源主机到目的主机的吞吐量在理想情况下约等于瓶颈链路的带宽，即等于链路的带宽中的**最小值**。	
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★★	将整个计算机网络的通信功能分为 7 层，由低层至高层分别是：**物理层、数据链路层、网络层、传输层、会话层、表示层、应用层。**
3 种参考模型和 OSI 参考模型有关术语★★★	各层对应的 PDU 名称： **应用层：** 报文 **传输层：** 段(数据段或报文段) **网络层：** 分组或包 **数据链路层：** 帧 **物理层：** 位流或比特流
TCP/IP 参考模型★★★	由低层至高层分别是：**网络接口层、网络互联层**（IP 协议——核心）、**传输层**（TCP 协议与 UDP 协议）、**应用层。**
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

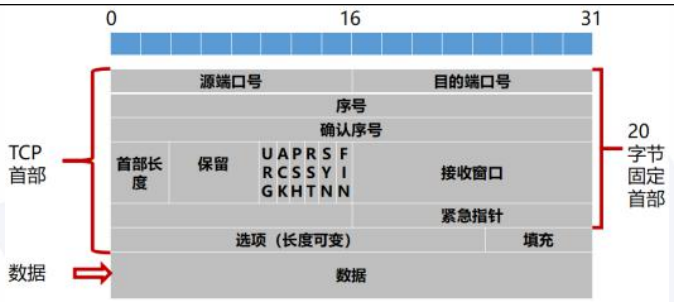
知识点名称	知识点内容		
计算机网络应用体系结构★	包括：**客户/服务器（C/S）结构网络应用**（最典型、最基本。如 www 应用、文件传输 FTP、电子邮件）、纯 P2P 结构网络应用、混合结构网络应用。		
网络应用通信基本原理★	典型的网络应用编程接口是套接字，标识套接字的编号叫端口号，IP 地址用于唯一标识一个主机或路由器接口。		
	TCP	面向连接、提供可靠数据流传输的传输控制协议。	
	UDP	无连接不提供可靠数据传输的用户数据报协议。	
域名服务器★★★	**根域名服务器**	**最重要**的域名服务器，**共 13 个**，从 a 一直到 m。若本地域名服务器没有被查询域名信息，都需要从**根域名服务器**查询。	
	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。【区：一个服务器负责管辖的范围】	
	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。	
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。**		
HTTP 报文★★★	组成	起始行、首部行、空白行、实体主体	
	分类	**请求报文**	**起始行<方法><URL><协议版本>** HTTP 典型的请求方法有： **GET（最常见）**、HEAD、POST、OPTION、PUT 。
		响应报文	**起始行**<协议版本>**<状态码>**<短语> 状态码：服务器向客户端通告响应情况，3 位十进制数构成： 100~199：信息提示； 200~299：成功； 300~399：重定向； 400~499 客户端错误； 500~599：服务器错误。
Cookie★★	Cookie 中文名称为小型文本文件，Cookie 是由服务器端生成。Cookie 是实现服务器对客户状态的跟踪的典型技术。		

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（SMTP）		**特点：**（1）只能传送 7 位 ASCII 码文本内容。（2）传送的邮件内容中不能包含“CRLF.CRLF”。（3）SMTP 是“推动”协议。（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 **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 7 位 ASCII 码的编码规则。
	用户代理		电子邮件应用的客户端软件，为用户提供使用电子邮件的接口。典型的电子邮件用户代理有：**微软的 Outlook，Apple Mail 和 Fox Mail 等**。
	邮件读取协议		POP3、IMAP、HTTP
Socket 编程基础 ★★	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_RAM
	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() sendto()	发送数据
		recv() recvfrom()	接收数据
		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。即其下层的网络层、数据链路层、物理层的设备中都无需实现传输层协议。		
传输层寻址与端口★	“IP 地址+端口号”可以唯一标识一个通信端点。 其中，IP 地址唯一标识进程运行在哪个主机上，同一主机上传输层协议端口号则可以唯一对应一个应用进程。		
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	客户端口号或暂时端口号	49152～65535
常用协议与端口号的对应关系 ★★★ （全书关于端口号的总结）	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
	RIP 信息协议		520
	SNMP 简单网络管理协议		get UDP 161（默认）

<table>
<tr><td></td><td colspan="4"></td><td>trap UDP 162</td></tr>
<tr><td rowspan="4">传输层的复用与分解★</td><td rowspan="4">关键：IP 地址和端口号能够唯一标识一个套接字</td><td rowspan="2">无连接</td><td>提供协议</td><td colspan="2">UDP</td></tr>
<tr><td>唯一标识</td><td colspan="2"><目的 IP 地址，目的端口号></td></tr>
<tr><td rowspan="2">面向连接</td><td>提供协议</td><td colspan="2">TCP</td></tr>
<tr><td>唯一标识</td><td colspan="2"><源 IP 地址，目的 IP 地址，源端口号，目的端口号></td></tr>
<tr><td>停-等协议★★</td><td colspan="5">最简单的自动重传请求（ARQ）协议。</td></tr>
<tr><td rowspan="3">滑动窗口协议★★★</td><td colspan="2">选择重传（SR）协议</td><td colspan="2">发送窗口 Ws>1</td><td>接收窗口 Wr>1</td></tr>
<tr><td colspan="2">回退 N 步（GBN）协议</td><td colspan="2">发送窗口 Ws>=1</td><td>接收窗口 Wr=1</td></tr>
<tr><td colspan="5">信道利用率与发送窗口的大小有关，当 Ws 足够大时，信道利用率为 100%。</td></tr>
<tr><td>UDP 数据报结构★★</td><td colspan="5"> 

UDP 首部为 4 个字段，每个字段由 2 个字节组成</td></tr>
<tr><td>TCP 报文段结构★★★</td><td colspan="5"> 

接收窗口字段用于实现 TCP 的流量控制。
TCP 连接的建立采用“三次握手”，释放采用“四次挥手”过程。</td></tr>
<tr><td>TCP 可靠数据传输★★</td><td colspan="5">实现机制包括差错编码、确认、序号、重传、计时器等。</td></tr>
</table>

第四章 网络层

<table>
<tr><th>知识点名称</th><th>知识点内容</th></tr>
<tr><td>网络层服务★★</td><td>网络层的功能：转发、路由选择、连接建立
虚电路网络是一种分组交换网络。（在网络的源节点和目的节点之间先建立逻辑通路的数据交换方式）</td></tr>
<tr><td>数据报网络与虚电路网络的比较★★</td><td>
<table>
<tr><th>项目</th><th>虚电路交换</th><th>数据报交换</th></tr>
<tr><td>端到端连接</td><td>需要先建立连接</td><td>不需要建立连接</td></tr>
<tr><td>地址</td><td>每个分组含有一个短的虚电路号</td><td>每个分组包含源和目的端地址</td></tr>
<tr><td>分组顺序</td><td>按序发送，按序接收</td><td>按序发送，不一定按序接收</td></tr>
<tr><td>路由选择</td><td>建立 VC 时需要路由选择，之后所有分组都沿此路由转发</td><td>对每个分组独立选择</td></tr>
<tr><td>转发结点失效的影响</td><td>所有经过失效结点的 VC 终止</td><td>除了崩溃时丢失分组外，无其他影响</td></tr>
<tr><td>差错控制</td><td>由通信网络负责</td><td>由端系统负责</td></tr>
<tr><td>流量控制</td><td>由通信网络负责</td><td>由端系统负责</td></tr>
<tr><td>拥塞控制</td><td>若有足够的缓冲区分配给已经建立的 VC，则容易控制</td><td>由端系统负责</td></tr>
<tr><td>状态信息</td><td>建立的每条虚电路都要求占用经过的每个结点的表空间</td><td>网络不存储状态信息</td></tr>
<tr><td>通信类型</td><td>传输质量要求高的通信</td><td>数据通信，非实时通信</td></tr>
</table>
</td></tr>
</table>

<table>
<tr><td></td><td colspan="3"><table><tr><td>典型网络</td><td>X.25、帧中继、ATM</td><td>因特网</td></tr></table></td></tr>
<tr><td>异构网络互连★★★</td><td colspan="3">1、同构网络互连：如两个异地以太网的互连，实现这类同构网络互连的典型技术是隧道技术。
2、各层设备：
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</td></tr>
<tr><td>交换结构★★</td><td colspan="3">包括：基于内存交换、基于总线交换、基于网络交换（性能最好）。</td></tr>
<tr><td rowspan="4">拥塞控制措施★★</td><td>流量感知路由</td><td colspan="2">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。</td></tr>
<tr><td>准入控制</td><td colspan="2">是一种广泛应用于虚电路网络的拥塞预防技术。
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。</td></tr>
<tr><td>流量调节</td><td colspan="2">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</td></tr>
<tr><td>负载脱落</td><td colspan="2">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。</td></tr>
<tr><td rowspan="4">IP 数据报格式★★</td><td rowspan="2">DF 标志位</td><td>DF=0</td><td>允许路由器将该 IP 数据分片</td></tr>
<tr><td>DF=1</td><td>禁止路由器将该 IP 数据分片</td></tr>
<tr><td rowspan="2">MF 标志位</td><td>MF=0</td><td>该数据报未被分片或是分片的最后一片</td></tr>
<tr><td>MF=1</td><td>该数据报一定是一个分片，且不是最后一个</td></tr>
<tr><td>IP 数据报分片★★</td><td colspan="3">一个数据链路层协议帧所能承载的最大数据量称为该链路的最大传输单元（MTU）。最大分片可封装的数据长度（字节）为 $d=\left\lfloor\frac{M-20}{8}\right\rfloor\times 8$；需要的 IP 分片总数为 $n=\left\lceil\frac{L-20}{d}\right\rceil$；每个 IP 分片的片偏移字段取值为 $Fi=\frac{d}{8}\times(i-1)$，$1\ll i\ll n$；每个 IP 分片的总长度字段为 $Li=\begin{cases}d+20, & 1\ll i<n\\ L-d\times(n-1), & i=n\end{cases}$ 每个 IP 分片的 MF 字段为 $MFi=\begin{cases}1, & 1\ll i<n\\ 0, & i=n\end{cases}$</td></tr>
<tr><td>分类地址★★★</td><td colspan="3"><table><tr><th>类</th><th>前缀长度</th><th>前缀</th><th>首字节</th></tr><tr><td>A</td><td>8 位</td><td>0xxxxxxx</td><td>0～127</td></tr><tr><td>B</td><td>16 位</td><td>10xxxxxx xxxxxxxx</td><td>128～191</td></tr><tr><td>C</td><td>24 位</td><td>110xxxxx xxxxxxxx xxxxxxxx</td><td>192～223</td></tr><tr><td>D</td><td>不可用</td><td>1110xxxx xxxxxxxx xxxxxxxx xxxxxxxx</td><td>224～239</td></tr><tr><td>E</td><td>不可用</td><td>1111xxxx xxxxxxxx xxxxxxxx xxxxxxxx</td><td>240～255</td></tr></table></td></tr>
<tr><td>ICMP★★</td><td colspan="3">功能：差错报告和网络探测。</td></tr>
</table>

IPv6 数据报格式 ★★★	地址长度为 128 位。IPv4 地址：地址长度为 32 位。 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 ★★★	**单播地址**	唯一标识网络中的一个主机或路由器网络接口。 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。 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。 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。）
路由算法与路由协议 ★★★	**全局式路由选择算法**：链路状态路由选择算法（**LS 算法**）——利用 Dijkstra 算法求最短路径的 **分布式路由选择算法**：距离向量路由选择算法（**DV 算法**）——距离向量路由选择算法的基础是 Bellman-Ford 方程（简称 B-F 方程）	
Internet 路由选择协议	自治系统内路由选择：内部网关协议（IGP）【路由信息协议（RIP）、开放最短路径优先协议（OSPF）】 自治系统间路由选择：外部网关协议（EGP）【边界网关协议（BGP）】	

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 ★★	噪声分类：**随机噪声**（引起随机差错或独立差错）**和冲击噪声**（引起的差错称为突发差错）。 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**突发长度**。	
差错控制的基本方式 ★★★	检错重发：是一种典型的差错控制方式，在计算机网络中应用广泛。 前向纠错：适用于单工链路或者对实时性要求比较高的应用。 反馈校验：优点：原理简单，易于实现，无须差错编码。 检错丢弃：只适用于实时性要求较高的系统。	
循环冗余码 ★★	CRC 编码的基本思想是：将二进制位串看成是系数为 0 或 1 的多项式的系数。一个 k 位二进制数据可以看作是一个 k-1 次多项式的系数列表，该多项式共有 k 项，从 x^(k-1)到 x^0。这样的多项式被认为是 k-1 阶多项式。故多项式 G(X) =X^4+X^2+X+1 对应的比特串为 10111，其阶为 4。	
信道划分 MAC 协议 ★★★	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**光纤**通信中。
	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
随机访问 MAC 协议 ★★	使用 CSMA/CD 协议实现多路访问控制时，通过共享信道通信的两个通信站之间相距的最远距离、信号传播速度、数据帧长度以及信道信 息传输速率之间要满足下列约束关系：$\frac{L_{min}}{R} \geqslant \frac{2D_{max}}{v}$，式中 Lmin 为数据帧最小长度；R 信息传输速率；Dmax 为两通信站之间的最远距离；v 为信号传播速度。	
分散式控制 ★★★	环网上最严重的两种错误：**令牌丢失**和**数据帧无法撤销**。	
局域网★	OSI/RM 中数据链路层功能在 IEEE802 参考模型中被分成**介质访问控制 MAC** 和**逻辑链路控制**两个子层。	
MAC 地址 ★★	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。	

<table>
<tr><td>地址解析协议★</td><td colspan="2">地址解析协议（ARP）：用于根据本网内目的主机或默认网关的 IP 地址获取其 MAC 地址。</td></tr>
<tr><td>以太网帧结构★★★</td><td colspan="2">以太网的最短帧长为 64 字节，即以太网帧中的数据字段最少要 46 字节（如果不足 46 字节，则需要填充）。</td></tr>
<tr><td>虚拟局域网★★★</td><td colspan="2">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。</td></tr>
<tr><td rowspan="2">点对点链路协议★★★</td><td>PPP</td><td>字节填充技术（遇到 01111110 填充控制转义字节：01111101）
<table>
<tr><td>1字节</td><td>1字节</td><td>1字节</td><td>1字节或2字节</td><td>可变长度</td><td>2字节或4字节</td><td>1字节</td></tr>
<tr><td>标志
01111110</td><td>地址
11111111</td><td>控制
00000011</td><td>协议</td><td>信息</td><td>校验和</td><td>标志
01111110</td></tr>
</table></td></tr>
<tr><td>HDLC</td><td>位填充技术（零比特填充）。
过程：发送端扫描整个数据字段，只要发现 5 个连续的 1，就立即插入一个 0，经过此过程处理后，数据字段不会出现连续的 6 个 1。
3 种类型的帧：信息帧、管理帧、无序号帧。</td></tr>
</table>

第六章 物理层

<table>
<tr><th>知识点名称</th><th colspan="2">知识点内容</th></tr>
<tr><td>连续信道容量★★★</td><td colspan="2">（1）奈奎斯特公式，给出了理想无噪声信道的信道容量：
$C = 2B\log_2 M$，式中，C 为信道容量，单位为 bit/s 或 bps；B 为信道带宽，单位为 Hz；M 为进制数，即信号状态数。
（2）香农公式给出连续信道的信道容量为：$C=B\log_2(1+\frac{S}{N})$；</td></tr>
<tr><td>数字基带传输编码★★</td><td colspan="2">差分码：差分码又称为相对码，差分码利用电平的变化与否来表示信息。
AMI 码：信息码中的 0 为 AMI 传输码中的 0；信号码中的 1 交替编码为 AMI 传输码中的+1 和−1。
双相码：双相码又称曼彻斯特码。正（高） 电平跳到负（低）电平表示 1，负电平跳到正电平表示 0。相当于信息码中 1 为双极非归零码的 10，信息码中 0 为双极非归零码的 01。
差分双相码，也称为差分曼彻斯特码。利用每位开始处是否存在电平跳变编码信息。其中，开始处有跳变表示 1，无跳变表示 0。</td></tr>
<tr><td>多进制数字调制★★</td><td colspan="2">数据传输速率R_b（bit/s）与码元传输速率R_B（Baud）以及进制数 M（通常为 2 的幂次）之间的关系为：$R_b = R_B \log_2 M$</td></tr>
<tr><td rowspan="4">物理层接口特性★★</td><td>机械特性</td><td>也叫物理特性，指明通信实体间硬件连接接口的机械特点。</td></tr>
<tr><td>电气特性</td><td>规定了在物理连接上，导线的电气连接及有关电路的特性</td></tr>
<tr><td>功能特性</td><td>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</td></tr>
<tr><td>规程特性</td><td>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。</td></tr>
</table>

第七章 无线与移动网络

<table>
<tr><th>知识点名称</th><th>知识点内容</th></tr>
<tr><td>无线链路与无线网络特性★★</td><td>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。
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。</td></tr>
<tr><td>IEEE802.11 标准小结★★★</td><td>
<table>
<tr><th>标准</th><th>数据率</th><th>频率范围 GHz</th><th>物理层</th></tr>
<tr><td>IEEE 802.11b</td><td>2.4</td><td>最高为 11 Mbit/s</td><td>扩频</td></tr>
<tr><td>IEEE 802.11a</td><td>5</td><td>最高为 54 Mbit/s</td><td>OFDM</td></tr>
<tr><td>IEEE 802.11g</td><td>2.4</td><td>最高为 54 Mbit/s</td><td>OFDM</td></tr>
<tr><td>IEEE 802.11n</td><td>2.4/5</td><td>最高为 600 Mbits</td><td>MIMO/OFDM</td></tr>
</table></td></tr>
<tr><td>IEEE 802.11</td><td>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。</td></tr>
</table>

<table>
<tr><td rowspan="3">帧★★★</td><td rowspan="3">4 个地址字段</td><td colspan="6"><table>
<tr><th>去往 AP</th><th>来自 AP</th><th>地址 1</th><th>地址 2</th><th>地址 3</th><th>地址 4</th></tr>
<tr><td>0</td><td>1</td><td>目的地址</td><td>AP 地址</td><td>源地址</td><td>——</td></tr>
<tr><td>1</td><td>0</td><td>AP 地址</td><td>源地址</td><td>目的地址</td><td>——</td></tr>
</table></td></tr>
<tr><td rowspan="3">其他典型无线网络简介
★★</td><td>WiMax</td><td colspan="6">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。</td></tr>
<tr><td>蓝牙</td><td colspan="6">IEEE 802.15.1。网络以小范围、低功率和低成本运行。</td></tr>
<tr><td>ZigBee</td><td colspan="6">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。</td></tr>
</table>

第八章 网络安全基础

<table>
<tr><th>知识点名称</th><th colspan="3">知识点内容</th></tr>
<tr><td rowspan="4">数据加密
★★★</td><td colspan="3">密码学包括：
（1）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。
（2）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。</td></tr>
<tr><td rowspan="2">传统加密方式</td><td colspan="2">替代密码（恺撒密码）：将明文字母表 M 中的每个字母用密文字母表 C 中的相应字母来代替，常见的加密模型有移位密码、乘数密码、仿射密码等。</td></tr>
<tr><td colspan="2">换位密码：又称置换密码，是根据一定的规则重新排列明文，以便打破明文的结构特性。可分为列置换密码和周期置换密码。</td></tr>
<tr><td>对称秘钥加密</td><td colspan="2">DES 加密算法、三重 DES、AES 加密、IDEA</td></tr>
<tr><td>非对称/公开秘钥加密</td><td colspan="2">典型：Diffie-Hellman 算法和 RSA 算法。
公开密钥密码的一个重要特性：$K_B^-\left(K_B^+(m)\right)=m=K_B^+\left(K_B^-(m)\right)$
解决了对称加密算法秘钥分发问题。</td></tr>
<tr><td rowspan="2">典型的散列函数
★★★</td><td>MD5</td><td colspan="2">MD5 对报文散列后，得到 128 位的散列值。</td></tr>
<tr><td>SHA-1</td><td colspan="2">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。</td></tr>
<tr><td rowspan="2">密匙分发中心与证书认证机构</td><td>秘钥分发中心（KDC）</td><td colspan="2">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。</td></tr>
<tr><td>证书认证机构(CA)</td><td colspan="2">将公钥与特定实体绑定。</td></tr>
<tr><td>防火墙分类
★★</td><td colspan="3">无状态分组过滤器（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。</td></tr>
<tr><td>入侵检测系统 IDS</td><td colspan="3">是当观察到潜在的恶意流量时，能够产生警告的设备或系统，IDS 不仅仅针对 TCP/IP 首部进行操作，而且会进行深度包检测， 并检测多数据之间的相关性。</td></tr>
<tr><td>SSL 协议栈</td><td colspan="3">SSL 更改密码规格协议、SSL 警告协议、SSL 握手协议、SSL 记录协议</td></tr>
<tr><td>安全电子邮件标准</td><td colspan="3">安全电子邮件标准——PGP</td></tr>
<tr><td rowspan="4">IPSec 体系简介
★</td><td>封装安全载荷协议（ESP）</td><td rowspan="2">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。</td></tr>
<tr><td>认证头（AH）协议</td></tr>
<tr><td>安全关联（SA）</td><td>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。</td></tr>
<tr><td>密钥交换与管理（IKE）</td><td>是 IPsec 唯一的密钥管理协议。</td></tr>
</table>