全国高等教育自学考试

考前30天

自考密训资料

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 ★★	1.**分组交换设备**可以实现数据分组的接收与转发，是构成 Internet 的重要基础，存在多种形式，最典型的是**路由器**和**交换机**。 2.目前**最大的、应用最广泛**的计算机网络就是 Internet 或称**因特网**。	
协议的定义 ★★★★	3.定义：计算机网络中的实体在进行数据交换的过程中必须遵循一些规则或约定，这些规则或约定就是**网络协议**。 4.**3 个基本要素**： (1) **语法**：定义实体之间交换信息的**格式与结构**。 (2) **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。 (3) **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 ★★★	5.**计算机网络的功能：**在不同主机之间实现快速的信息交换。**核心**功能是：实现**资源共享。** 6.包括：【助记：软硬心】 (1) **硬件资源共享：**如云计算、云存储。 (2) **软件资源共享：**如软件即服务（SaaS）。 (3) **信息资源共享：**如信息交换。	
按拓扑结构分类 ★★★★	**网络拓扑**是指网络中的主机、网络设备间的物理**连接关系与布局**。	
	7.**星形拓扑结构**	(1) 比较多见于**局域网、个域网**中。 (2) **优点**：1)易于监控与管理；2)故障诊断与隔离容易。 (3) **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**。
	8.**总线型拓扑结构**	在**早期的局域网**中比较多见。
	9.**环形拓扑结构**	(1) 多见于**早期的局域网、园区网和城域网**中。 (2) **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） (3) **缺点**：故障检测麻烦（任意结点出现故障都会造成网络瘫痪）
	10.**网状拓扑结构**	比较多见于**广域网、核心网络**等。
	11.**树形拓扑结构**	目前，**很多局域网**采用这种拓扑结构。
	12.**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 ★★★	13.大规模现代计算机网络结构包括的部分： （1）**网络边缘**：连接到网络上的所有**端系统**构成了网络边缘。 （2）**接入网络**： 1）**电话拨号接入**是利用电话网络接入网络。 2）**HFC 接入网络**是利用有线电视网络实现网络接入的技术。 3）ADSL 是利用现有的电话网络的用户线路实现的接入网络。 4）**局域网接入**：企业、学校等机构会在组织范围内建设局域网，连接所有需要接入外部网络（如	

	Internet）的主机，然后通过企业网络或校园网的边缘路由器连接网络核心。 5）**移动接入网络**主要利用移动通信网络，如 3G/4G/5G 网络，实现智能手机、移动终端等设备的网络接入。 （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 ★★★★	14.数据交换是实现在大规模网络核心上进行数据传输的技术基础。常见的数据交换技术包括： (1) **电路交换：最早**出现的一种交换方式。主要适用于**语音和视频**这类实时性强的业务。包括 **3 个阶段：建立电路、传输数据和拆除电路**。 (2) **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。 (3) **分组交换（包交换）：**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 ★★★★★	15.时延是评价计算机网络性能的一个重要的性能指标，也称为延迟。 16.通常将连接两个结点的直接链路称为**一个“跳步”**，简称**“跳”**。 17.**时延分类**： **（1）结点处理时延**：每个分组到达交换结点时进行的**检错、检索转发表**等时间总和，**常忽略**。记 dc。 **（2）排队时延**：分组在**缓存中排队等待**的时间。大小不确定。记为 dq。 **（3）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。 **（4）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 ★★★★	18.一段物理链路的**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）**。 19.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。
丢包率 ★★	20.常被用于评价和衡量网络性能的指标，在很大程度上可以反映网络的**拥塞程度。**因为**引发网络丢包的主要因素**是**网络拥塞**。
吞吐量 ★★	21.**吞吐量**表示在单位时间内源主机通过网络向目的主机实际送达的数据量，单位为 bit/s 或 B/s （字节每秒）。 22.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★★	23.**计算机网络体系结构**：计算机网络所划分的**层次**以及**各层协议**的集合。 24.体系结构应当具有足够的信息，以便软件设计人员为每层编写实现该层协议的有关程序，即协议软件。需要注意的是，这种分层体系结构通常是**按功能划分的**，并不是按实现方式划分的。
OSI 参考模型 ★★★★	25.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： （1）物理层：物理层的主要功能是在传输介质上实现无结构比特流传输。 （2）数据链路层：数据链路层的主要功能是实现**相邻结点之间**数据可靠而有效的传输。在 OSI 参考模型中，数据链路的建立、维持和释放过程称为链路管理。 （3）网络层：网络层解决的核心问题是如何将分组通过交换网络传送至目的主机。 （4）传输层：传输层的功能主要包括复用/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。 （5）会话层：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。 （6）表示层：表示层主要用于处理应用实体间交换数据的语法。 （7）应用层：应用层与提供给用户的网络服务相关，这些服务非常丰富，包括文件传送、电子邮件、P2P 应用等。
3 种参考模型和 OSI 参考模型有关术语 ★★★★	26.各层对应的 PDU 名称： （1）应用层：报文　　（2）传输层：段(数据段或报文段) （3）网络层：分组或包　　（4）数据链路层：帧 （5）物理层：位流或比特流 27.OSI 参考模型中，相邻层间的服务是通过其接口面上的服务访问点(SAP)进行的，N 层 SAP 就是(N+1)层可以访问 N 层的地方。
TCP/IP 参考模型 ★★★★	28.由低层至高层分别是： (1) 网络接口层：未定义，具体实现方法随网络类型的不同而不同。 (2) 网络互联层（核心）：IP 协议（核心协议）无连接不可靠网络协议。网络互联层还包括互联网控制报文协议 ICMP、互联网多播组管理协议 IGMP 以及路由协议，如 BGP、OSPF 和 RIP 等。 (3) 传输层：TCP 面向连接的协议；UDP 无连接不提供可靠数据传输的协议。 (4) 应用层：按照协议定义的格式进行封装，以便达到对应控制功能。如 WWW 服务的应用层协议：HTTP。
计算机网络与因特网发展简史★	29.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 ★★	30.包括： （1）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）：最主要的特征是通信只在客户与服务器之间进行，客户与客户之间不进行直接通信。 （2）纯 P2P 结构网络应用。 （3）混合结构网络应用。
网络应用通信基本原理 ★★★	31.典型的网络应用编程接口是套接字（Socket），套接字是每个应用进程与其他应用进程进行网络通信时，真正收发报文的通道。 32.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。 33.传输层的协议有： (1) TCP：面向连接、提供可靠数据流传输的传输控制协议。 (2) UDP：无连接不提供可靠数据传输的用户数据报协议。
域名系统（DNS）★	34.实现将域名映射为 IP 地址的过程，称为域名解析。

层次化域名空间 ★★★★	35.因特网采用了层次树状结构的命名方法。域名的结构由标号序列组成，各标号之间用点隔开，如“….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。 36.顶级域名包括： (1) **国家顶级域名**：cn(中国)，us(美国)，uk(英国)。 (2) **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)。 (3) **基础结构域名**：arpa(用于反向域名解析)。
域名服务器 ★★★★	37.任何一台主机在网络地址配置时，都会配置一个域名服务器作为**默认域名服务器**，称为**本地域名服务器**。这样这台主机任何时候需要进行域名解析，都会将域名查询请求发送给该服务器。 38.**域名服务器的分类：** (1) **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。 (2) **顶级域名服务器：**国家顶级域名、通用顶级域名、基础结构域名。 (3) **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。任何一个拥有域名的主机，其域名与 IP 地址的映射关系等信息都存储在所在网络的**权威域名服务器**上。【区：一个服务器负责管辖的范围】 (4) **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 ★★★★	39.Web 应用主要包括 3 部分：【助记：客服协议】 (1) **浏览器**——Web 应用的**客户端**软件。 (2) **Web 服务器**——Web 应用的**服务器**软件。 (3) **HTTP**——客户与服务器之间的交互基于**应用层协议**。 40.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 连接 ★★★★★	41.**非持久连接**：指 HTTP 客户与 HTTP 服务器**建立 TCP 连接后**，通过该连接发送 HTTP **请求报文，接收** HTTP **响应报文**，**然后断开连接**。典型优化技术包括以下两种： (1) **并行连接**，通过**建立多条并行的 TCP 连接**，并行发送 HTTP 请求和并行接收 HTTP 响应。 (2) **持久连接**，重用已建立的 TCP 连接发送新的 HTTP 请求和接收 HTTP 响应，从而消除新建 TCP 连接的时间开销。 42.**持久连接**：不断开已连接的 TCP 连接。分为两种工作方式： (1) **非流水方式持久连接**：也称为非管道方式持久连接，客户端在通过持久连接**收到前一个响应报文后**，才能发出对下一个对象的请求报文。 (2) **流水方式持久连接**：也称为管道方式持久连接，客户端在通过持久连接**收到前一个对象的响应报文之前，连续依次发送对后续对象的请求报文**，再通过该连接依次接收服务器发回的响应报文。
HTTP 报文 ★★★★	43.**组成**：起始行、首部行、空白行、实体主体（**起始行和空白行不可缺少**，首部行可以是零行或多行，实体主体则根据报文类型、功能等可有可无。） 44.**分类**： (1) **请求报文**的起始行（请求行）：<方法><URL><协议版本> (2) **响应报文**的起始行（状态行）：<协议版本><状态码><短语> 45.HTTP 典型的请求方法有：

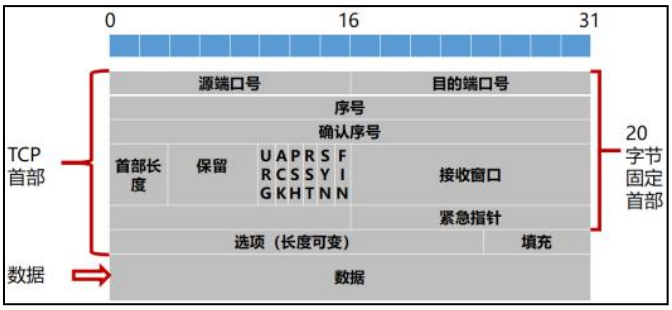
	（1）GET：请求读取由 URL 所标识的信息，是**最常见**的方法。 （2）HEAD：请求读取由 URL 所标识的信息的首部，即无须在响应报文中包含对象。 （3）POST：给服务器添加信息。 （4）OPTION：请求一些选项的信息。 （5）PUT：在指明的 URL 下存储一个文档。 46.**状态码**：服务器向客户端通告响应情况，3 位十进制数构成： （1）100~199：信息提示；　（2）200~299：成功；　（3）300~399：重定向； （4）400~499：客户端错误；　（5）500~599：服务器错误。	
Cookie ★★★★	47.作用：由于 HTTP 是一种无状态的协议，Web 应用引入了 Cookie 机制，用于**用户跟踪**。 48.定义：Cookie 中文名称为**小型文本文件**，指某些网站为了辨别用户身份、进行会话跟踪而储存在用户本地终端上的数据。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。 49.Cookie 的常见用途： (1) 网站可以利用 Cookie 的 ID 来准确统计网站的实际**访问人数**、新访问者和重复访问者的人数对比、访问者的访问频率等数据。 (2) 网站可以利用 Cookie **限制**某些特定用户的**访问**。 (3) 网站可以存储用户访问过程中的操作**习惯和偏好**。 (4) 记录用户登录网站使用的**用户名、密码**等信息。 (5) 电子商务网站利用 Cookie 可以实现**“购物车”**功能。	
电子邮件系统 ★★★★	50.**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**。
	51.**简单邮件传输协议（SMTP）**	(1) 邮件服务器间发送邮件的**应用层协议**。SMTP 使用**传输层 TCP 实现可靠数据传输**，从发送方（客户端）向接收方（服务器端）发送邮件。 (2) 特点：1）只能传送 **7 位 ASC II** 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**。 (3) **发送过程**：握手阶段、邮件传输阶段、关闭阶段。 (4) **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。
	52.**用户代理**	(1) 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。 (2) 典型的电子邮件用户代理有：**微软的 Outlook，Apple Mail 和 Fox Mail 等**。
	53.**邮件读取协议**	**(1) 邮件读取协议分类如下所示：** 1) 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、更新**。 2) 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**。 3) HTTP：HTTP 是 **Web 邮件系统**的邮件读取协议。 **(2) POP3 协议交互过程可以分为 3 个阶段：**

		1) **授权阶段**，用户代理需要向邮件服务器发送**用户名和口令**，服务器鉴别用户身份，授权用户访问邮箱。 2) **事务处理阶段**，用户代理向邮件服务器发送 **POP3 命令**，实现邮件读取、为邮件做删除标记、取消邮件删除标记以及获取邮件的统计信息等操作。 3) **更新阶段**，客户发出了 **quit 命令**，结束 POP3 会话，服务器删除那些被标记为**删除的邮件**。	
Socket 编程基础 ★★★★★	54.**分类**	(1) **数据报**类型套接字 SOCK_DGRAM（面向 **UDP**） (2) **流式**套接字 SOCK_STREAM（面向 **TCP**） (3) **原始**套接字 SOCK_RAM	
	55.**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 ★★★	56.**传输层主要实现的功能**：传输层**寻址**；对应用层报文进行**分段和重组**；对报文进行**差错检测**；实现进程间的端到端可靠数据**传输控制**；面向应用层实现**复用与分解**；实现端到端的**流量控制**；**拥塞控制**等。 57.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 ★★	58.**“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。 59.**端口号的分类** (1) **服务器**使用的端口号：**熟知端口号**（0～1023）、**登记端口号**（1024～49151） (2) **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	60.HTTP 超文本传输协议（Web 服务器的默认端口号）：80
	61.SMTP 简单邮件传输协议：25

<table>
<tr><td rowspan="5">对应关系
★★★★
（全书关于端口号的总结）</td><td colspan="4">62.POP3 邮局协议版本 3：110</td></tr>
<tr><td colspan="4">63.FTP 文件传送协议：控制连接 21、数据连接 20</td></tr>
<tr><td colspan="4">64.DNS 域服务器所开放的端口：53</td></tr>
<tr><td colspan="4">65.DHCP 动态主机配置协议：客户端 68、服务器 67</td></tr>
<tr><td colspan="4">66.RIP 信息协议：520</td></tr>
<tr><td></td><td colspan="4">67.SNMP 简单网络管理协议
get UDP 161（默认）
trap UDP 162</td></tr>
<tr><td rowspan="4">传输层的复用与分解
★★★</td><td rowspan="4">68.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（自动创建，或调用 bind()函数）</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>可靠数据传输基本原理
★★★★</td><td colspan="5">69.不可靠传输信道的不可靠性主要表现在：
（1）比特差错：交付给信道传输的数据可能出现比特跳变，即 0 错成 1 或 1 错成 0 的现象。
（2）出现乱序：先发的数据包后到达，后发的数据包先到达。
（3）数据丢失：部分数据会在中途丢失，不能到达目的地。
70.实现可靠数据传输的措施主要包括：
(1) 差错检测：利用差错编码实现数据包传输过程中的比特差错检测。
(2) 确认：接收方向发送方反馈接收状态。
(3) 重传：发送方重新发送接收方没有正确接收的数据。
(4) 序号：确保数据按序提交。
(5) 计时器：解决数据丢失问题
71.可靠数据传输协议：
(1) 自动重传请求（ARQ）协议（最简单：停-等协议。）
(2) 流水线协议或管道协议（典型：滑动窗口协议）</td></tr>
<tr><td>滑动窗口协议
★★★★</td><td colspan="5">72.最具有代表性的滑动窗口协议：
(1) 选择重传（SR）协议：GBN 协议的发送端缓存能力较高，可以在未得到确认前连续发送多个分组，因此，GBN 协议的发送窗口 Ws≥1。GBN 接收端缓存能力很低，只能接收 1 个按序到达的分组，不能缓存未按序到达的分组，通常称 GBN 协议的接收端无缓存能力。因此，GBN 协议的接收窗口 Wr=1。
(2) 回退 N 步（GBN）协议：发送窗口 Ws>1；接收窗口 Wr>1
73.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>用户数据报协议（UDP）★</td><td colspan="5">74.UDP 是无连接的，因此在支持两个进程间通信时，没有握手过程。
75.使用 UDP 的优点：
（1）应用进程更容易控制发送什么数据以及何时发送；</td></tr>
</table>

	（2）无需建立连接；（3）无连接状态；（4）首部开销小。
UDP 数据报结构★★	76.UDP 数据报首部包括的字段：**源端口号、目的端口号、长度、校验和**。 77.UDP 首部为 4 个字段，每个字段由 2 个字节组成。
TCP 报文段结构★★★	 78.在 TCP 报文段中，首部长度字段占 4 位，TCP 段的首部长度，以 **4 字节为计算单位**。 79.接收窗口字段用于实现 TCP 的流量控制。 80.TCP 连接的建立采用“三次握手”，释放采用“四次挥手”过程。
TCP 可靠数据传输★★★★	81.传输层实现**可靠数据传输的主要措施** (1) **查错检测**（利用差错编码实现检测） (2) **确认**（确认是否接收数据） (3) **重传**（重新发送没有接收的数据） (4) **序号**（确保按序提交给接收方） (5) **计时器**（解决丢失问题） 82.**快速重传算法的基本思想**是：接收端每收到一个失序的报文段后就立即发出重复确认，以便更早地通知发送端有丢包情况发生。发送端会在收到三次重复确认段后立即重传丢失的报文段，而不需要等待计时器超时。
TCP 拥塞控制★★★★★	83.TCP 拥塞控制算法包括： 慢启动：收到一个确认，CongWin 值就**加倍**。 拥塞避免：每经过一个 RTT，拥塞窗口 CongWin 的**增加 1MSS**。 快速重传：接收端收到 **3 次重复确认**时，则推断被重复确认的报文段已经丢失，于是立即发送被重复确认的报文段。 快速恢复：配合快速重传，当发送端连续**收到 3 次重复确认**，将**阈值减半**，并将 CongWin 的值设为减半后的阈值。然后开始执行拥塞避免的算法。 84.传输层的拥塞控制，如 TCP 的拥塞控制，通过**是否发生报文段的超时**来推断网络是否发生拥塞。TCP 的拥塞控制采用的是窗口机制的基本策略：网络未发生拥塞时，逐渐**“加性”增大窗口大小**，当网络拥塞时**“乘性”快速减小窗口大小**，即 AIMD。

第四章 网络层

知识点名称	知识点内容
网络层服务★★	85.网络层的功能：**转发、路由选择**、连接建立 86.虚电路网络是一种**分组交换网络**。（在源节点和目的节点之间先建立逻辑通路的数据交换方式）
数据报网络与虚电路	项目 | 虚电路交换 | 数据报交换

网络的比较 ★★★

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 ★★★

87.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。实现异构网络互连的基本策略主要包括协议转换和构建虚拟互联网络。

88.各层设备：

(1) 网络层：**路由器**。

(2) 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。）

(3) 物理层：**集线器**和**中继器**。

路由器 ★★★

89.路由器组成：

(1) **输入端口**：负责从物理接口接收信号，还原数据链路层帧，提取 IP 数据报，根据 IP 数据报的目的 IP 地址检索路由表，决策需要将该 IP 数据报交换到哪个输出端口。

(2) **交换结构**：将输入端口的 IP 数据报交换到指定的输出端口。主要包括**基于内存交换（性能最低，最便宜）**、**基于总线交换（独占性）**和**基于网络交换（性能最好，最贵）**的 3 种交换结构。

(3) **输出端口**：首先提供一个缓存排队功能，排队交换到该端口的待发送分组，并从队列中不断取出分组进行数据链路层数据帧的封装，通过物理线路端接发送出去。

(4) **路由处理器**：路由器的 CPU。转发与路由选择是路由器两项最重要的基本功能。路由器在收到 IP 数据报时，会利用 IP 数据报的目的 IP 地址检索匹配路由表，如果除默认路由外，有多条路由项匹配成功，则选择网络前缀匹配成功位数最长的路由项，通过该路由项指定的接口转发该 IP 数据报，这就是路由转发过程的**“最长前缀匹配优先原则”**。

网络拥塞 ★★★★

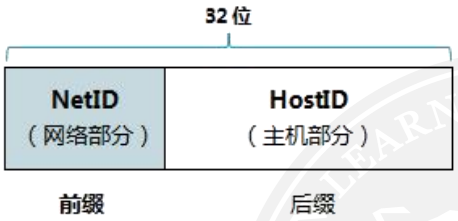
90.OSI 模型的**网络层中产生拥塞的主要原因**：【口诀：带宽容量处理故障。】

（1）缓冲区**容量**有限。

（2）传输线路的**带宽**有限。

（3）网络结点的**处理**能力有限。

<table>
<tr><td></td><td>（4）网络中某些部分发生了故障。
91.拥塞控制主要考虑端系统之间的网络环境，目的是使网络负载不超过网络的传送能力；而流量控制主要考虑接收端的数据接收与处理能力，目的是使发送端的发送速率不超过接收端的接收能力。另外，拥塞控制的任务是确保网络能够承载所达到的流量；而流量控制只与特定的发送方和特定的接收方之间的点到点流量有关。</td></tr>
<tr><td>拥塞控制措施
★★</td><td>92.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。
93.准入控制：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。
94.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。
95.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。</td></tr>
<tr><td>IP 数据报格式
★★</td><td>32位
<table><tr><td>版本（4位）</td><td>首部长度（4位）</td><td>区分服务（8位）</td><td colspan="2">数据报长度（16位）</td></tr><tr><td colspan="3">标识（16位）</td><td>标志（3位）</td><td>片偏移量（13位）</td></tr><tr><td colspan="2">生存时间（8位）</td><td>上层协议（8位）</td><td colspan="2">首部校验和（16位）</td></tr><tr><td colspan="5">源IP地址（32）</td></tr><tr><td colspan="5">目的IP地址（32）</td></tr><tr><td colspan="5">选项（可选，长度可变）</td></tr><tr><td colspan="5">数据</td></tr></table>96.首部长度字段：占 4 位，给出的是 IP 数据报的首部长度，以 4 字节为单位。</td></tr>
<tr><td>IP 数据报分片
★★★★</td><td>97.标志位：
(1) DF 标志位：DF=0：允许路由器将该 IP 数据分片。DF=1：禁止路由器将该 IP 数据分片。
(2) MF 标志位：MF=0：该数据报未被分片或是分片的最后一片。MF=1：该数据报一定是一个分片，且不是最后一个。
98.一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）。
99.最大分片可封装的数据长度（字节）为 d=$\lfloor\frac{M-20}{8}\rfloor\times 8$；需要的 IP 分片总数为 n=$\lceil\frac{L-20}{d}\rceil$；每个 IP 分片的片偏移字段取值为 Fi=$\frac{d}{8}\times$（i-1），$1\leqslant i\leqslant n$；每个 IP 分片的总长度字段为 Li=$Li=\begin{cases} d+20, & 1\leq i<n \\ L-d\times(n-1), & i=n \end{cases}$ 每个 IP 分片的 MF 字段为 $MFi=\begin{cases} 1, 1\leq i<n \\ 0, & i=n \end{cases}$
100.目的主机重组 IP 数据报分片的过程：（1）首部的标识字段→判断是否属于同一个 IP 数据报；
（2）分片首部的标志字段（MF）→判断是否是最后一个分片；
（3）片偏移字段→判断各 IP 分片的先后顺序，判断是否缺少 IP 分片。</td></tr>
<tr><td>IPv4 编址分类地址
★</td><td>101.分类地址
<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>
</table>

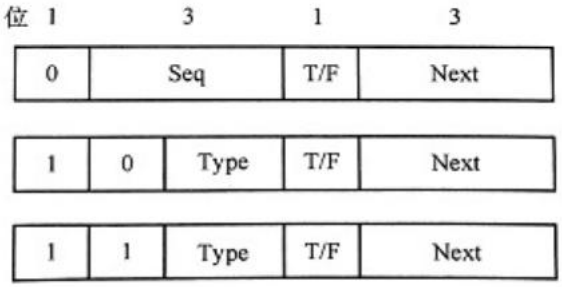
IPv4 编址 特殊地址 ★	102.**网络中一些常见的特殊地址**如下 (1) 本地主机地址：0.0.0.0/32 (2) 有限广播地址：255.255.255.255/32 (3) 回送地址：127.0.0.0/8 103.**私有 IP 地址**类别与范围对应如下： (1) A 类：10.0.0.0～10.255.255.255(或 10.0.0.0/8) (2) B 类：172.16.0.0～172.31.255.255(或 172.16.0.0/12) (3) C 类：192.168.0.0～192.168.255.255(或 192.168.0.0/16)
子网划分 ★★★★★	104.IP 地址结构：  前缀表示**网络规模**，后缀表示该网络中的**主机数**。 105.只有给出子网地址中的某主机的 IP 地址和**子网掩码或网络前缀**，才能准确描述一个子网的规模。通过将该地址与子网掩码做**按位与运算**，就可以得到**该子网的子网地址**。子网掩码的反码与该地址做**按位或运算**，就可以得到该子网的**直接广播地址**。
ICMP★★	106.功能：**差错报告**和**网络探测**。
IPv6 数据报格式 ★★	107.**IPv4 地址**：地址长度为 32 位。**IPv6 地址**长度为 128 位。IPv6 地址数量也扩展到了 2^128。 108.IPv6 数据报基本**首部长度**为**固定的** 40 字节。
IPv6 地址 ★★★	109.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“::”。 110.IPv6 地址包括： (1) **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。 (2) **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） (3) **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 ★★★★★	111.**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 112.**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） 113.在 Dijkstra 算法中，需要记录的信息： (1) D(v)：到本次迭代为止，源结点(计算结点)到目的结点 v 的当前路径距离。初始化时，如果结点 v 和源结点直接相连，那么 D(v)就是其链路上的权值，否则就是∞。 (2) P(v)：到本次迭代为止，在源结点到目的结点 v 的当前路径上，结点 v 的前序结点。 (3) C(x, y)：结点 x 与结点 y 之间直接链路的费用，如果 x 和 y 之间没有之间链路相连，则 c(x, y)=

	∞。 (4) S：结点的集合，用于存储从源结点到该结点的最短路径已求出的结点集合，初始值只有源点本身。
Internet 路由选择协议 ★★	114.**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）】** 115.**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
数据链路层服务★★	116.数据链路层提供的主要服务：**（1）组帧（2）链路接入（3）可靠交付（4）差错控制**
差错控制 ★★★	117.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）。 118.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 ★★★★	119.**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。**停-等协议和滑动窗口协议实现的都是这类差错控制方式。** 120.**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。 121.**反馈校验**：优点：原理简单，易于实现，无须差错编码。 122.**检错丢弃**：只适用于实时性要求较高的系统。
循环冗余码 ★★	123.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。
信道划分 MAC 协议 ★★★	124.**频分多路复用（FDM）：**频域划分制，优点分路方便，缺点串扰。 125.**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。 126.**波分多路复用（WDM）：**广泛应用于光纤通信中。 127.**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 ★★★★	128.CSMA 可以细分为 3 种不同类型的 CSMA 协议： （1）**非坚持 CSMA**：若通信站有数据发送，先侦听信道；若发现信道空闲，则立即发送数据；若发现信道忙或发送数据时产生冲突，则等待一个随机时间，然后重新开始侦听信道，尝试发送数据。 （2）**1-坚持 CSMA**：若通信站有数据发送，先侦听信道；若发现信道空闲，则立即发送数据；若发现信道忙，则继续侦听信道直至发现信道空闲，然后立即发送数据。若产生冲突，发现冲突后通信站会等待一个随机时间，然后重新开始发送过程。 （3）**P-坚持 CSMA**：若通信站有数据发送，先侦听信道；若发现信道空闲，则以概率 P 在最近时隙开始时刻发送数据，以概率 Q=1-P 延迟至下一个时隙发送。若下一个时隙仍空闲，重复此过程，直至数据发出或时隙被其他通信站占用；若信道忙，则等待下一个时隙，重新开始发送过程；若发送数据时发生冲突，则等待一个随机时间，然后重新开始发送过程。 129.CSMA/CD 存在冲突的**主要原因**是信号传播时延的原因。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

<table>
<tr><td></td><td>息传输速率之间要满足下列约束关系：$\frac{L_{min}}{R} \geq \frac{2D_{max}}{v}$，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。</td></tr>
<tr><td>分散式控制
★★★</td><td>130.环网上最严重的两种错误：令牌丢失和数据帧无法撤销。</td></tr>
<tr><td>局域网
★</td><td>131.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。</td></tr>
<tr><td>MAC 地址
★★</td><td>132.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。</td></tr>
<tr><td>地址解析协议★★</td><td>133.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
★★★</td><td>134.以太网采用的 MAC 协议是 CSMA/CD 协议。
135.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>交换机
★★★★</td><td>136.以太网交换机的基本工作方式是存储一转发，因此交换机可以具有多种速率的端口。
137.交换机的决策依据：以帧的目的 MAC 地址为主键，查询其内部的交换表，如果交换表中有帧的目的 MAC 地址对应的交换表项，且对应的端口与接收到该帧的端口相同，则丢弃该帧（即无须转发），否则向表项中的端口转发帧（选择性转发）；如果交换表中没有帧的目的 MAC 地址对应的交换表项，则向除接收到该帧的端口外的所有其他端口转发该帧（即泛洪）。
138.交换机的自学习
以太网交换机有 4 个端口（1234），各连接一台计算机，其 MAC 地址分别是 ABCD。开始，以太网交换机里面的转发表是空白的。（1-A、2-B、3-C、4-D）
（1）A 向 B 发送一个帧，从端口 1 进入交换机。交换机把这个帧的源 MAC 地址 A 和端口 1 写入交换表，完成第一次学习。
（2）交换机查询转发表，没找到往哪里转发该帧。交换机向除端口 1 以外所有端口泛洪(广播)这个帧。
（3）C 和 D 丢弃该帧，因为目的 MAC 地址与自己的不匹配。B 收下该帧。
（4）B 向 A 发送一个回复帧，交换机收到该帧后，现在交换表中新增表项(B,2)，完成第二次学习。
（5）交换机查询转发表，发现表中有 MAC 地址为 A 的项，则交换机就把这个帧从端口 1 转发出去。</td></tr>
<tr><td>虚拟局域网
★★★★</td><td>139.虚拟局域网是一种基于交换机（必须支持 VLAN 功能）的逻辑分割（或限制）广播域的局域网应用形式。
140.划分 VLAN 的方法：基于交换机端口划分、基于 MAC 地址划分和基于上层协议类型或地址划分。</td></tr>
<tr><td>点对点链路协议
★★★★</td><td>141.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>
</table>

	142.HDLC	(1) **位填充技术（零比特填充）**。 (2) 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) 3 种类型的帧：**信息帧（I 格式）、管理帧（S 格式）、无序号帧（U 格式）**。3 种帧的 8 位控制字段为： 

第六章 物理层

知识点名称	知识点内容
连续信道容量 ★★★	143.**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。 144.**香农公式**给出连续信道的信道容量为：$C=B\log_2(1+\frac{S}{N})$；
数字基带传输编码 ★★★★	145.**差分码**：又称为**相对码**，利用电平的跳变与否来表示信息。 （1）数字 0：相邻电平无跳变。 （2）数字 1：相邻电平有跳变。 146.信号交替反转码（AMI 码）：用 3 种电平(正电平、负电平、零电平)进行编码 （1）数字 0：零电平表示。 （2）数字 1：交替用正电平和负电平表示，且在脉冲持续的中间时刻回归零电平。 147.**双相码**：又称**曼彻斯特码**。只有正负电平，脉冲持续时间的中间时刻都要进行电平跳变。 （1）数字 0：一个脉冲时间内，从负电平跳到正电平（0：负正） （2）数字 1：一个脉冲时间内，从正电平跳到负电平（1：正负） 148.**差分双相码**，也称**差分曼彻斯特码**。 （1）数字 0：相邻电平无跳变表示 （2）数字 1：相邻电平有跳变表示 149.**米勒码**的编码规则（数字相同交替，数字不同延续） （1）数字 1：正负或负正，脉冲中间时刻跳变。 （2）数字 11：交替编码。 （3）数字 1 后的 0：延续前面 1 的电平，正或负。脉冲中间时刻不跳变。 （4）数字 00：交替编码。 （5）数字 0 后的 1：延续 0 的电平，正负或负正。 150.传号反转码（CMI 码）： （1）数字 1：正、负电平交替编码。脉冲中间时刻不跳变。 （2）数字 0：一个脉冲时间内从负电平到正电平。

频带传输中的三种调制方式 ★★	151.**二进制数字调制**包括 3 种基本调制：二进制**幅移**键控(2ASK)、二进制**频移**键控 (2FSK)和二进制**相移**键控(2PSK)，还有二进制**差分相移**键控（2DPSK） 152.二进制幅移键控（2ASK）:利用二进制基带信号控制载波信号的幅值变化。 （1）基带编码 编码信息为 0 时：调制后为一段幅值为 0 的载波信号。 （2）基带编码 编码信息为 1 时：调制后为一段幅值为 A 的载波信号。 153.二进制频移键控（2FSK）：利用二进制基带信号控制载波信号的频率变化。 （1）基带编码 编码信息为 0 时：调制后为一段频率为 f_1的载波信号。 （2）基带编码 编码信息为 1 时：调制后为一段频率为 f_2的载波信号。 154.二进制相移键控（2PSK）：利用二进制基带信号控制载波信号的相位变化。 （1）基带编码 编码信息为 0 时：调制后为一段相位为 ϕ_1的载波信号。 （2）基带编码 编码信息为 1 时：调制后为一段相位为 ϕ2 的载波信号。 155.二进制差分相移键控（2DPSK）：利用相邻两个码元载波间的相对相位变化。 （1）基带编码 编码信息为 0 时：调制后为相位相对于相邻载波相位无变化。 （2）基带编码 编码信息为 1 时：调制后为相位相对于相邻载波相位有变化。 156.二进制数字调制性能比较：在恒参信道中，2ASK、2PSK 及 2DPSK 均可获得较高的频带利用率，而 2FSK 的频带利用率最低；**2PSK 与 2DPSK 均可获得较好的抗噪声性能(低误码率)，2ASK 抗噪声性能最差。**对于随参信道，2FSK 与 2PSK 的适应性更好，2ASK 最差。目前在实际通信系统中应用比较多的是 2DPSK 和 2FSK，前者主要用于高速数据传输，后者主要用于的中、低速数据传输。 157.**多进制数字调制**：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：$R_b=R_B\log_2 M$ 158.**正交幅值调制（QAM）:**也称幅值相位联合键控（APK），对载波信号的幅值和相位同时进行调制的联合调制技术。**优点**：频带利用率高、抗噪声能力强、调制解调系统简单。
物理层接口特性 ★★	159.**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。 160.**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。 161.**功能特性：**指明物理接口各条信号线的用途，接口信号线功能的规定方法和分类。 162.**规程特性：**即通信协议，利用接口传输比特流的**全过程**，各项用于传输的事件发生的**合法顺序**。

第七章 无线与移动网络

知识点名称	知识点内容
无线链路与无线网络特性 ★★	163.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**。 164.**无线网络**与有线网络最主要的区别是**使用了无线链路**，而无线链路的独有特性，在很大程度上决定了无线网络的特性。 165.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。 166.**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。Ad Hoc 网络中的每个节点都兼有**路由器和主机**两种功能。 167.**基础设施模式**：无线主机与基站关联，并通过基站实现通信中继的无线网络。

无线局域网 IEEE 802.11 ★★★★

168.IEEE802.11 中 4 个主要协议具有的共同特征：

（1）都使用相同的介质访问控制协议 CSMA/CA。

（2）链路层帧使用相同的帧格式。

（3）都具有降低传输速率以传输更远距离的能力。

（4）都支持“基础设施模式”和“自组织模式”两种模式。

169.IEEE802.11 标准小结

标准	数据率	频率范围 GHz	物理层
IEEE 802.11b	2.4	最高为 11 Mbit/s	扩频
IEEE 802.11a	5	最高为 54 Mbit/s	OFDM
IEEE 802.11g	2.4	最高为 54 Mbit/s	OFDM
IEEE 802.11n	2.4/5	最高为 600 Mbits	MIMO/OFDM

170.带碰撞避免的载波监听多路访问协议（CSMA/CA 协议）的工作步骤：

（1）源站发送数据：先监听，若空闲，等待一个分布式帧间间隔的时间后，发送一个很短的请求发送(RTS)控制帧。RTS 控制帧：源地址，目的地址，本次通信所需的持续时间。

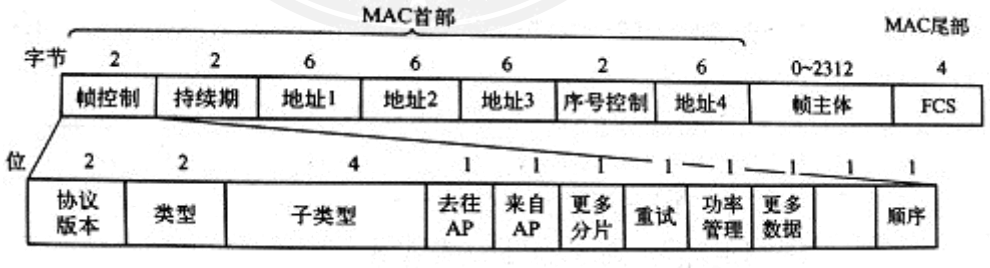
（2）目的站正确收到源站发来的 RTS 帧：物理介质空闲，等待一个短帧间间隔的时间后，发送一个很短的允许发送(CTS)控制帧作为响应。CTS 控制帧：本次通信持续时间等。

（3）其他站点：监听到两者要通信，其他站点在其持续通信时间内不会发送帧。其他站根据监听到的 RTS 或 CTS 帧中的持续时间来确定数据帧传输的时间。

（4）源站收到 CTS 帧：等待一段时间后，发送数据帧，若目的站正确收到了数据帧，在等待时间后，就向源站发送确认帧(ACK)。

IEEE 802.11 帧 ★★★

171.802.11 数据帧结构：



（1）MAC 首部共 30B；

（2）帧主体，帧的数据部分，**不超过 2312B**，不过 IEEE 802.11 帧的长度通常都是小于 1500B；

（3）尾部是帧检验序列 FCS，**共 4 字节**。

172.**3 种类型**：控制帧、数据帧和管理帧。【口诀：空灌输（控管数）】

173.**4 个地址字段**

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	——
1	0	AP 地址	源地址	目的地址	——

蜂窝网络体系结构

174.**小区(Cell)**：蜂窝网覆盖的区域分成的六边形的区域。

175.**收发基站（BTS）**：负责向小区内的移动站点发送或接收信号。

★	176.**基站控制器（BSC）**：服务于几十个收发基站，为移动用户分配 BTS 无线信道。BSC 及其控制的 BTS 共同构成了 GSM 基站系统（BSS）。 177.**移动交换中心（MSC）**：在用户鉴别和账户管理以及呼叫建立和切换中起决定性作用。单个 MSC 通常包含多达 5 个 BSC。一个蜂窝服务提供商的网络将由若干个 MSC 构成，并使用称为网关 MSC 的特殊 MSC 将提供商的蜂窝网络与更大的公共电话网相连。 178.**蜂窝网络中的移动性管理：** （1）通信者拨打移动用户的电话号码。 （2）归属移动交换中心收到该呼叫，查询归属位置注册器来确定移动用户的位置。确定移动用户的漫游号码。 （3）漫游号码确定后，归属移动交换中心通过网络呼叫被访网络的移动交换中心，被访网络的移动交换中心呼叫移动用户.
移动 IP 网络★	179.代理发现：当移动 IP 站点到达一个新网络时，移动站点都必须知道相应的外部代理或归属代理的身份。 （1）代理通告：代理周期性的广播一个 ICMP 报文。 （2）代理请求：移动结点广播一个 ICMP 报文。 180.外部代理向移动结点的归属代理注册或注销 COA 的步骤： （1）移动结点向外部代理发送一个移动 IP 注册报文。 （2）外部代理收到注册报文并记录移动结点的永久 IP 地址，分配一个 COA。 （3）外部代理把注册请求发送给归属代理，归属代理检查真实性和正确性。 （4）外部代理接收注册应答。
其他典型无线网络简介 ★★★	181.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。 182.**蓝牙**：IEEE 802.15.1。网络以**小范围、低功率和低成本**运行。 183.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
网络安全威胁 ★★★★	184.比较常见的网络攻击包括**拒绝服务 DoS** 以及**分布式拒绝服务 DDoS** 等。 （1）**拒绝服务（DoS）**是指阻止服务器为其他用户提供服务。 （2）**分布式拒绝服务 DDoS** 指利用多个源主机协同淹没接收方。 185.网络在报文传输方面所面临的安全威胁： （1）**窃听**指的是报文传输过程中窃听信息，获取报文信息。 （2）**插入**威胁指的是攻击者主动在连接中插入信息，混淆信息，让接收信息者收到虚假信息。 （3）**假冒**指的是可以伪造分组中的源地址（或者分组的任意其他字段）。 （4）**劫持**指的是通过移除/取代发送方或者接收方“接管”连接。
数据加密 ★★★★★	186.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。

	187.**传统加密方式** （1）**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。 （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。 188.列置换密码加密过程： （1）首先，将明文 P 按密钥 K 的长度 n 进行分组，并且每组一行按行排列，即每行有 n 个字符。 （2）若明文长度不是 n 的整数倍，则不足部分用双方约定的方式填充，如双方约定用字母“x”替代空缺处字符。 （3）设最后得到的字符矩阵为 M_{mn},m 为明文划分的行数。然后，按照密钥规定的次序将 M_{mn}对应的列输出，便可得到密文序列 C。 188.**对称秘钥加密：** （1）**DES 加密算法：**明文分为 64 位分组，使用 56 位的密钥，进行 16 轮加密。 （2）**三重 DES：**使用两个密钥，执行三次 DES 算法，密钥长度达到 112 位。 （3）**AES 加密：**密钥长度：128/192/256 位 （4）**IDEA：**密钥长度：128 位。 189.**非对称/公开秘钥加密** （1）典型：**Diffie-Hellman 算法**和 **RSA 算法**。 （2）公开密钥密码的一个重要特性：$K_B^-\left(K_B^+(m)\right)=m=K_B^+\left(K_B^-(m)\right)$
典型的散列函数 ★★★	190.**MD5：**MD5 对报文散列后，得到 128 位的散列值。 191.**SHA-1：**SHA-1 可产生一个 160 位的散列值。**典型的用于创建数字签名的单向散列算法。** 192.密码散列函数的主要特征： （1）一般的散列函数具有算法**公开**。 （2）能够**快速计算**。 （3）对任意长度报文进行多对一映射均能产生**定长输出**。 （4）对于任意报文**无法预知**其散列值。 （5）不同报文**不能产生相同的散列值**。 （6）**单向性、抗弱碰撞性、抗强碰撞性**。
报文认证 ★	193.**报文认证**是使消息的接受者能够检验收到的消息是否是真实的认证方法。 194.报文认证的**目的**：一个是消息源的认证，即验证消息的来源是真实的；另一个是消息的认证，即验证消息在传送过程中未被篡改。 195.**简单报文验证：不足：无法达到对消息源认证。** （1）发送方对报文 m 应用散列函数，得到固定长度的散列码，获得报文摘要 h 将扩展报文(m,h)发送给接收方。 （2）接收方收到扩展报文后，提取出报文 m 和报文摘要 h，同样对报文 m 应用散列函数 H 获得新的报文摘要 H(m)，将 H(m)和 h 比较。 （3）若相同，报文认证成功。否则报文认证失败。 196.**报文认证码 MAC：不足：无法保证消息在接收方没有被篡改。**

	（1）发送方和接收方共享一个认证密钥 s，发送方对报文 m 和认证密钥 s 应用散列函数 H 得到报文认证码 h，将扩展报文(m,h)发送给接收方。 （2）接收方收到扩展报文后，提取出报文 m 和报文认证码 h，对报文 m 和认证密钥 s 应用散列函数 H 获得新的报文认证码 H(m+s)，将 H(m+s)与 h 比较。 （3）若相等，则报文认证成功。否则失败。。
数字签名 ★★	197.数字签名应满足的要求： （1）接收方能够确认或证实发送方的签名，但不能伪造。 （2）发送方发出签名的消息给接收方后，就不能再否认他所签发的消息。 （3）接收方对已收到的签名消息不能否认，即有收报认证。 （4）第三者可以确认收发双方之间的消息传送，但不能伪造这一过程。 【助记：对于**接收方**——不能伪造、不能否认。对于**发送方**——不能否认。**第三方**——不能伪造】 198.**简单数字签名** （1）Bob 利用自己的私钥对报文 m 加密，创建签名报文。将扩展报文(报文，签名报文)发送给 Alice。 （2）Alice 收到扩展报文。利用 Bob 的公钥解密签名报文，并检验解密后的签名报文和报文 m 是否一致。 （3）若一致，则签名 m 的一定是 Bob 的私钥。 199.**签名报文摘要** （1）Bob 对报文 m 应用散列函数 H 生成报文摘要 H(m)，然后 Bob 通过其私钥对报文摘要进行加密生成加密的报文摘要，将扩展报文(报文，加密的报文摘要)发送给 Alice。 （2）Alice 收到报文 m 以及加密的报文摘要。Alice 利用 Bob 的公钥解密加密的报文摘要，并对 m 应用散列函数生成新的报文摘要。 （3）如果两者一致，则签名报文 m 的一定是 Bob 的私钥。
身份认证 ★	200.为了预防重放攻击，比较有效的解决方式是引入**一次性随机数（Nonce）**，该随机数在一个生命期内只使用一次。
密匙分发中心与证书认证机构★	201.**秘钥分发中心（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。 202.**证书认证机构（CA）**：将公钥与特定实体绑定。
防火墙分类 ★★★	**203.分类：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、应用网关** 204.**无状态分组过滤器**：典型部署在内部网络和网络边缘路由器上的防火墙。 路由器逐个检查数据报，根据访问控制表(Access Control Lists ,ACL)实现防火墙规则。 205.**有状态分组过滤器**：跟踪每个 TCP 连接建立、拆除，根据状态确定是否允许分组通过。 206.**应用网关**：应用网关实现授权用户通过网关访问外部网络的服务。
入侵检测系统 IDS★★	207.IDS 指当观察到潜在的**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。
安全套接字层 SSL★	208.HTTP 协议使用 SSL 进行安全通信时，称为安全 HTTP，简记为 **HTTPS**。 209.SSL 协议栈：**SSL 更改密码规格协议、SSL 警告协议、SSL 握手协议、SSL 记录协议**

安全电子邮件 ★	210.电子邮件对网络安全的**需求**： （1）机密性：阅读方（非第三方、真正的接收方）。 （2）完整性：不被篡改，篡改完整性验证。 （3）身份认证性：发送方（不能被假冒），接收方（确认发送方的身份）。 （4）抗抵赖性：发送方（无法抵赖），接收方（预防抵赖）。 211.**安全电子邮件标准——PGP**	
VPN 简介 ★★	212.许多机构组织会使用 IPSec 创建运行在公共网络之上的**虚拟专用网络（VPN）**。 213.VPN 通过**隧道技术、数据加密、身份认证、密钥管理、访问控制和网络管理**等，实现与专用网类似的功能，可以达到 PN 安全性的目的，同时成本相对而言要低很多。 214.VPN 的实现技术：**IPSec（最安全、使用最广）**；利用 **SSL 协议**（SSL 具有高层安全协议的优势，使用常见的浏览器就可以部署）；	
IPSec 体系简介 ★	215.**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。
	216.**认证头（AH）协议**	
	217.**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。
	218.**密钥交换与管理（IKE）**	是 IPsec 唯一的密钥管理协议。
	219.隧道模式 ESP：最广泛和最重要的 IPSec 形式。	