

密训·资料

计算机网络原理（全国）

1904

MI XUN ZI LIAO

编前语

试卷说明：本科目考试题型为单选、填空、简答、综合题。各题型分值分布情况如下表所示：

| 题型 | 分值 |
|-----|-----------------------------------|
| 单选题 | 25 分 (25 道×1 分) |
| 填空 | 10 分 (10 道×1 分) |
| 简答题 | 30 分 (6 道×5 分) |
| 综合题 | 35 分 (3 道 , 10 分 , 12 分 , 13 分) |

资料说明：本资料提供的都是考试重点，但是在重点中，按照知识点的重要程度，对知识点进行了标星。如下表：

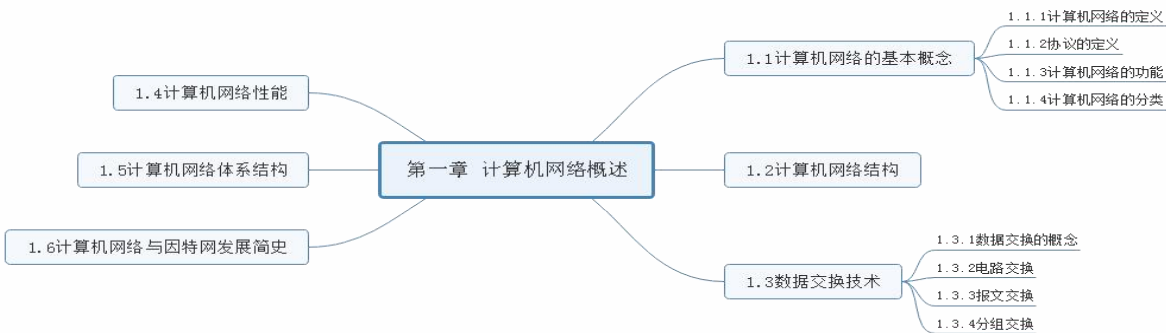
| 星级 | 说明 |
|-------|-----------------------|
| 1-2 星 | 易考单选、填空，2 星相对 1 星更重要。 |
| 3-4 星 | 易考简答，4 星相对 3 星更重要。 |
| 5 星 | 易考综合题 |

星标数目越多，表示知识点越重要，越可能考到。但要注意的是，资料提供的是知识重点，并不是押题。文中加粗的是需要重点了解的地方。这份资料是为了指导学员考前最后的复习，帮助学员理清知识点间的逻辑，加速记忆。学员在拿到资料后，可根据星标数、资料里的逻辑整理和标识，了解哪些知识点是重点，然后重点复习。

| | |
|-------------------------------|----|
| 第一章 计算机网络概述..... | 4 |
| 第一节 计算机网络的基本概念..... | 4 |
| 第二节 计算机网络结构☆☆..... | 5 |
| 第三节 数据交换技术☆☆..... | 5 |
| 第四节 计算机网络性能☆☆..... | 6 |
| 第五节 计算机网络体系结构☆☆..... | 7 |
| 第六节 计算机网络与因特网发展简史☆☆..... | 8 |
| 第二章 网络应用..... | 8 |
| 第一节 计算机网络应用体系结构☆☆..... | 9 |
| 第二节 网络应用通信基本原理☆☆..... | 9 |
| 第三节 域名系统 (DNS) ☆☆..... | 9 |
| 第四节 万维网应用☆☆..... | 9 |
| 第五节 Internet 电子邮件☆☆..... | 10 |
| 第六节 FTP☆☆..... | 11 |
| 第七节 P2P 应用☆..... | 11 |
| 第八节 Socket 编程基础☆☆..... | 11 |
| 第三章 传输层..... | 12 |
| 第一节 传输层的基本服务..... | 12 |
| 第二节 传输层的复用与分解☆..... | 12 |
| 第三节 停-等协议与滑动窗口协议..... | 13 |
| 第四节 用户数据报协议 (UDP) ☆..... | 13 |
| 第五节 传输控制协议 (TCP) ☆☆☆☆☆..... | 13 |
| 第四章 网络层..... | 15 |
| 第一节 网络层服务☆☆..... | 16 |
| 第二节 数据报网络与虚电路网络☆☆..... | 16 |
| 第三节 网络互连与网络互连设备..... | 16 |
| 第四节 网络层拥塞控制☆☆☆..... | 17 |
| 第五节 Internet 网络层☆☆☆☆☆..... | 17 |
| 第六节 路由算法与路由协议☆☆..... | 19 |
| 第五章 数据链路层与局域网..... | 20 |
| 第一节 数据链路层服务☆☆☆..... | 20 |
| 第二节 差错控制..... | 20 |
| 第三节 多路访问控制协议..... | 21 |
| 第四节 局域网..... | 22 |
| 第五节 点对点链路协议☆☆..... | 23 |
| 第六章 物理层..... | 24 |
| 第一节 数据通信基础☆☆☆..... | 24 |

| | |
|--------------------------|----|
| 第二节 物理介质☆ | 24 |
| 第三节 信道与信道容量 | 25 |
| 第四节 基带传输☆☆☆☆ | 25 |
| 第五节、频带传输☆☆☆ | 26 |
| 第六节 物理层接口规程☆ | 26 |
| 第七章 无线与移动网络 | 27 |
| 第一节 无线网络☆ | 28 |
| 第二节 移动网络☆ | 28 |
| 第三节 无线局域网 IEEE802.11☆☆☆☆ | 28 |
| 第四节 蜂窝网络☆☆ | 29 |
| 第五节 移动 IP 网络☆ | 29 |
| 第六节 其他典型无线网络简介☆ | 29 |
| 第八章 网络安全基础 | 30 |
| 第一节 网络安全概述☆☆☆ | 30 |
| 第二节 数据加密☆☆ | 30 |
| 第三节 消息完整性与数字签名☆☆ | 31 |
| 第四节 身份认证☆ | 31 |
| 第五节 秘钥分发中心与证书认证机构☆ | 31 |
| 第六节 防火墙与入侵检测系统☆☆ | 31 |
| 第七节 网络安全协议☆☆ | 32 |

第一章 计算机网络概述



第一节 计算机网络的基本概念

一、计算机网络的定义☆☆

计算机网络是互连的、自治的计算机的集合

二、协议的定义☆☆

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。

协议的 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：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。

三、计算机网络的功能☆☆

（1）硬件资源共享，如云计算、云存储。（2）软件资源共享，如 SaaS。（3）信息资源共享，如信息交换。

四、计算机网络的分类☆☆

| 按覆盖范围分类 | 个域网（PAN）、局域网（LAN）、城域网（MAN）、广域网（WAN） | |
|---------|-------------------------------------|--|
| 按拓扑结构分类 | 星形拓扑结构 | 星形拓扑结构网络的主要优点是易于监控与管理，故障诊断与隔离容易；主要缺点是中央结点是网络的瓶颈，一旦故障，全网瘫痪。 |
| | 总线型拓扑结构 | 主要优点是结构简单，所需电缆数量少，易于扩展；主要缺点是通信范围受限，故障诊断与隔离较困难，容易产生冲突。 |
| | 环形拓扑结构 | 主要优点是所需电缆长度短，可以使用光纤，易于避免冲突；主要缺点是某结点的故障容易引起全网瘫痪，新结点的加入或撤出过程比较麻烦，存在等待时间问题。 |
| | 网状拓扑结构 | 主要优点是网络可靠性高，一条或多条链路故障时，网络仍然可联通；主要缺点是网络结构复杂，造价成本高，选路协议复杂。 |

| | | |
|-----------|--------|---|
| | 树形拓扑结构 | 主要优点是易于扩展，故障隔离容易；主要缺点是对根结点的可靠性要求高，一旦根结点故障，则可能导致网络大范围无法通信。 |
| | 混合拓扑结构 | 主要优点是易于扩展，可以构建不同规模网络，并可根据需要优选网络结构；主要缺点是网络结构复杂，管理与维护复杂。 |
| 按交换方式分类 | 电路交换网络 | 优点是实时性高，时延和时延抖动都较小；缺点是对于突发性数据传输，信道利用率低，且传输速率单一。 |
| | 报文交换网络 | 优点是报文交换线路利用率高，缺点是报文经过网络的延迟时间长且不固定。 |
| | 分组交换网络 | 优点是交换设备存储容量要求低、交换速度快、可靠传输效率高、更加公平。 |
| 按网络用户属性分类 | 公用网 | 公用网是指由国家或企业出资建设，面向公众提供收费或免费服务的网络。 |
| | 私有网 | 私有网是指由某个组织（如政府部门或企业等）出资建设，专门面向该组织内部业务提供网络传输服务，不向公众开放的网络。 |

第二节 计算机网络结构☆

| | | |
|---------|------|---|
| 计算机网络结构 | 网络边缘 | 连接到网络上的计算机、服务器、智能手机、智能传感器、智能家电等称为主机或端系统。连接到网络上的所有端系统构成了网络边缘。 |
| | 接入网络 | 常见的接入网络技术包括：电话拨号技术、非对称数字用户线路 ADSL、混合光纤同轴电缆 HFC 接入网络、局域网、移动接入网络。 |
| | 网络核心 | 网络核心是由通信链路互连的分组交换设备构成的网络，作用是实现网络边缘中主机之间的数据中继与转发。比较典型的分组交换设备是路由器和交换机等。 |

第三节 数据交换技术☆☆

一、数据交换的概念

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电路交换、报文交换和分组交换。

二、电路交换

电路交换是最早出现的一种交换方式，电话网络则是最早、最大的电路交换网络。

利用电路交换进行通信包括建立电路、传输数据和拆除电路 3 个阶段。

三、报文交换

报文交换也称为消息交换，其工作过程为：发送方把要发送的信息附加上发送/接收主机的地址及其他控制消息，构成一个完整地报文。然后以报文为单位在交换网络的各结点之间以存储-转发的方式传送，直至送达目的主机。

四、分组交换

分组交换是目前计算机网络广泛采用的技术。分组交换需要将待传输数据（即报文）分割成较小的数据块，每个数据块附加上地址、序号等控制信息构成数据分组，每个分组独立传输到目的地，目的地将收到的分组重新组装，还原为报文。

分组交换优点：（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。

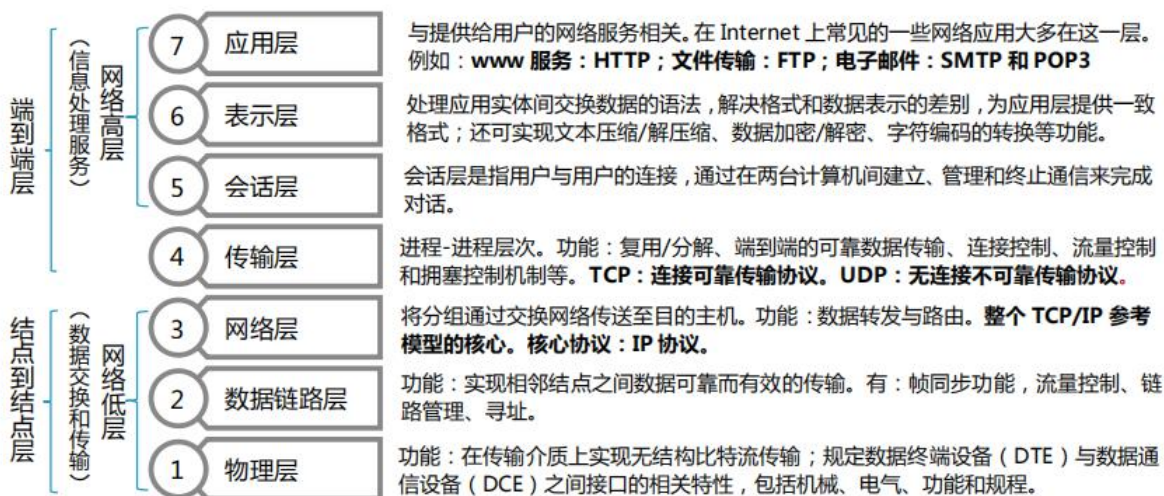
分组长度的确定：分组长度与延迟时间：在其他条件相同的情况下，分组长度越长，延迟时间越长。分组长度与误码率：最佳分组长度 $L_{opt} = \sqrt{\frac{h}{P_e}}$ 。最高信道利用率可以表示为 $\eta_{max} = (1 - \sqrt{hP_e})^2$

第四节 计算机网络性能☆☆

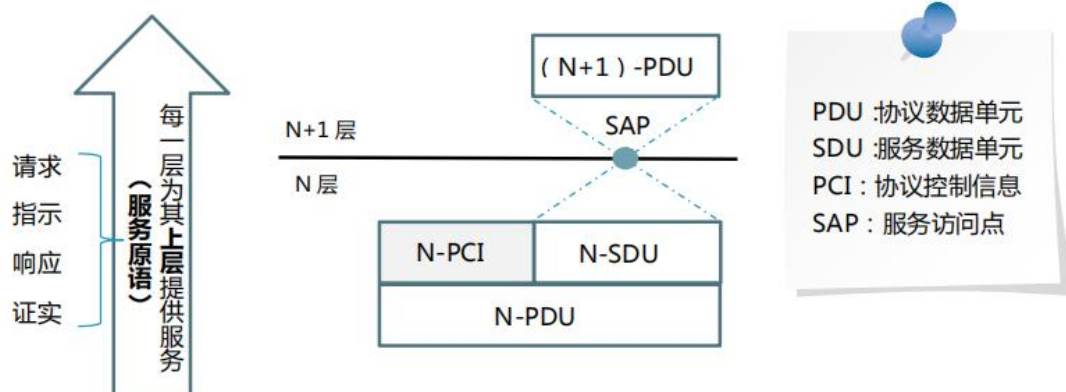
| | | |
|-------|---|--|
| 速率和带宽 | 速率 | 指网络单位时间内传送的数据量，用以描述网络传输数据的快慢。速率的基本单位是 bit/s。 |
| | 带宽 | “带宽”表示链路或信道的最高数据速率，单位也是 bit/s。 |
| 时延☆☆ | 结点处理时延 | 每个分组到达交换结点时进行的检错、检索转发表等时间总和，常忽略。记为 d_c |
| | 排队时延 | 分组在缓存中排队等待的时间。大小不确定。记为 d_q |
| | 传输时延 | 当一个分组在输出链路发送时，从发送第一位开始，到发送完最后一位为止，所用的时间，称为传输时延，也称为发送时延，记为 d_t 。设分组长度 L bit，链路带宽（即速率） R bit/s，则 $d_t = L/R$ 。 |
| | 传播时延 | 设物理链路长度 D m，信号传播速度 V m/s，则 $d_p = D/V$ 。 |
| 时延带宽积 | 一段物理链路的传播时延与链路带宽的乘积，称为时延带宽积，记为 G ，于是 $G = d_p \times R$ | |
| 丢包率 | 丢包率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。丢包率可以定义为 $\eta = \frac{N_1}{N_s} = \frac{N_s - N_r}{N_s}$ | |
| 吞吐量 | 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），记为 Thr 。吞吐量经常用于度量网络的实际数据传送（通过）能力。 | |

第五节 计算机网络体系结构☆☆

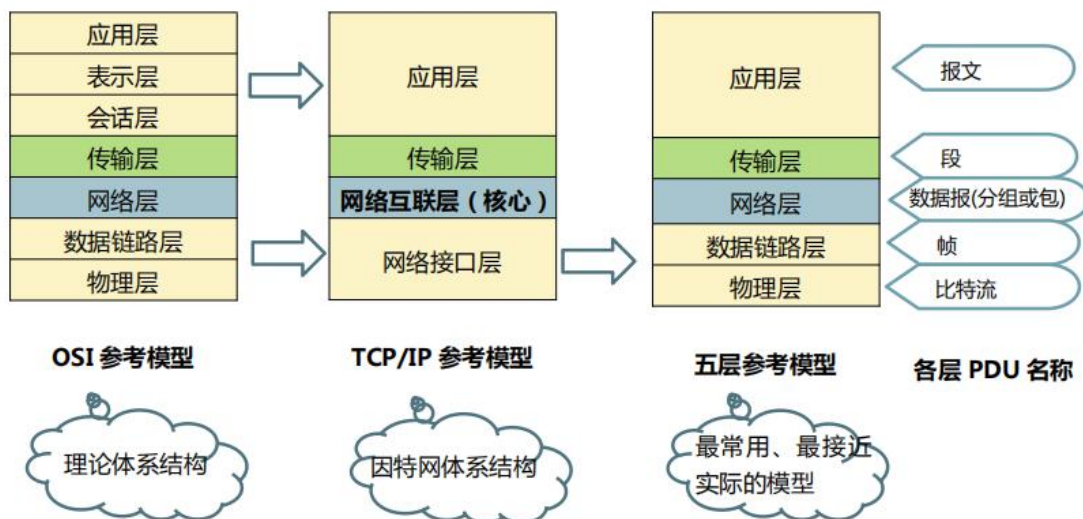
一、OSI 参考模型☆☆



2、OSI 参考模型有关术语☆☆



二、TCP/IP 参考模型、五层参考模型☆☆



第六节 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。

密训押题

1、网络协议中涉及用于协调与差错处理的控制信息的要素是 ()

A:语义 B:语法 C:定时 D:编码

答案：A

解析：语义就是定义实体之间交换的信息中需要发送（或包含）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。另外，有的协议还需要进行差错检测，这类协议通常会在协议信息中附加差错编码等控制信息。语义还需要定义彼此采用何种差错编码，以及采取何种差错处理机制。

2、下列网络协议中提供传输层服务的协议是 ()

A:TCP 与 IP B:FTP 与 TCP C:IP 与 DNS D:TCP 与 UDP

答案：D

解析：传输层的协议为运行在不同主机上的进程提供了一种逻辑通信机制。TCP/IP 参考模型的传输层主要包括面向连接、提供可靠数据流传输的传输控制协议 TCP 和无连接不提供可靠数据传输的用户数据报协议 UDP。

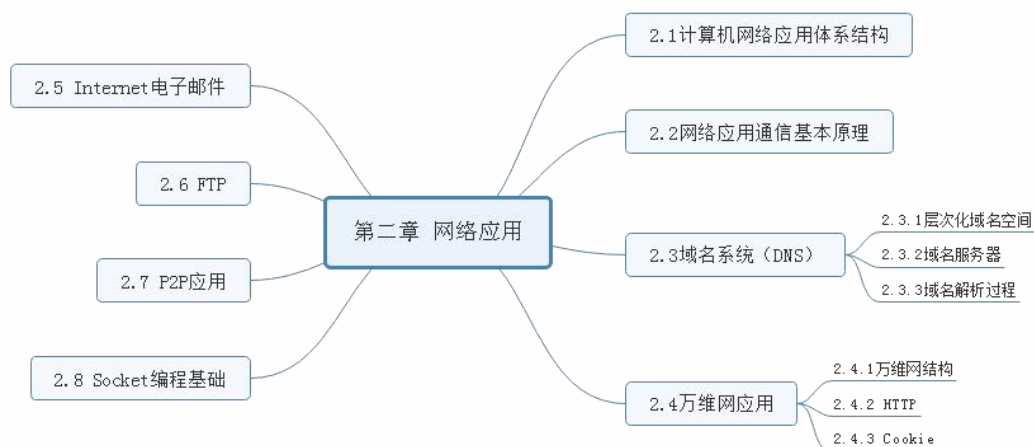
3、以下网络拓扑构型中不采用点-点线路的通信子网的拓扑是 ()

A:星形 B:网状形 C:树形 D:总线形

答案：D

解析：总线型拓扑结构网络采用一条广播信道作为公共传输介质，称为总线，所有结点均与总线连接，结点间的通信均通过共享的总线进行。

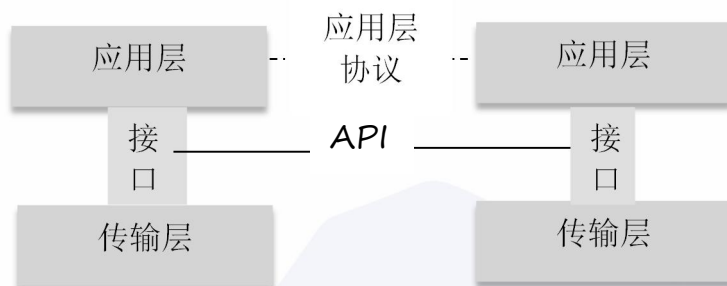
第二章 网络应用



第一节 计算机网络应用体系结构☆☆

| | 特点 | 实用案例 |
|-------------------------|--------------------------------------|------------------------------|
| 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。 | www 应用 、文件传输 FTP、电子邮件 |
| 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。 | Gnutella、BitTorrent |
| 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。 | IPTV |

第二节 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。

Internet 传输层能提供的服务只有两类：面向连接的可靠字节流传输服务 TCP 和无连接的不可靠数据报传输服务 UDP。

第三节 域名系统 (DNS) ☆☆

一、层次化域名空间☆☆

(1) 国家顶级域名：cn，us，uk。(2) 通用顶级域名：com，net，org，edu，gov，mil，int。(3) 基础结构域名：arpa。

二、域名服务器☆☆

(1) 根域名服务器（最重要的域名服务器，知道所有的顶级域名服务器的域名和 IP。在因特网上共有 13 个不同 IP 地址的根域名服务器，它们的名字是用一个英文字母命名，从 a 一直到 m（前 13 个字母），如 a.rootservers.net。）

(2) 顶级域名服务器 (3) 权威域名服务器 (4) 中间域名服务器。

三、域名解析过程

(1) 递归解析：依次查询 (2) 迭代解析：直接响应结果

第四节 万维网应用☆☆

一、万维网结构

Web 应用主要包括 Web 服务器、浏览器与超文本传输协议 (HTTP) 等部分。

HTML 基本 Web 页也是通过 URL 地址引用页面中的其他对象。每个 **URL 地址主要由两部分组成**：存放对象的服务器主机域名（或 IP 地址）和对象的路径名。

二、HTTP

| | | | |
|---------|--|--|--|
| HTTP 概述 | Web 应用的应用层协议。定义浏览器如何向 Web 服务器发送请求以及 Web 服务器如何向浏览器进行响应。 | | |
| HTTP 连接 | 非持久连接：每次请求一个对象都需要新建一个 TCP 连接。 | | |
| | 并行连接：建立多条并行 TCP 连接，并行发送 HTTP 请求和并行接收 HTTP 响应。 | | |
| | 持久连接 | 非流水方式持久连接：收到前对象响应后再发出下一个请求报文 流水方式持久连接：收到前一个响应前，依次发送后续对象请求 | |
| 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 等。 |
| | | 响应报文 | 起始行<协议版本><状态码><短语> 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。 |

三、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。

主要包括 4 部分：HTTP 响应报文中的 Cookie 头行，用户浏览器在本地存储、维护和管理 Cookie 文件，HTTP 请求报文中的 Cookie 头行，网站在后台数据库中存储、维护 Cookie 信息。

第五节 Internet 电子邮件☆☆

| | | | |
|--------|----------------|---------------------------------------|---|
| 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。【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。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。】 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 |
| | 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。 |

第六节 FTP☆

| | | |
|-----|----|---|
| FTP | 定义 | 在互联网的两个主机间实现文件互传的网络应用，其应用层协议也称为 FTP。FTP 使用的默认端口号是 21。 |
| | 特点 | FTP 应用使用两个“并行”的 TCP 连接：控制连接和数据连接。 |
| | | FTP 服务器必须在整个会话期间保留用户的状态，即 FTP 是有状态的。 |
| | | FTP 会话形式是客户向服务器发送命令，服务器发送状态码和短语作为应答。 |

第七节 P2P 应用☆

P2P 体系结构对服务器的依赖很小，对于纯 P2P 来说，整个应用几乎不依赖某个集中服务器。

P2P 体系结构实现文件分发的最快时间为： $D_{P2P} = \{F/u_s, F/d_{\min}, \frac{nF}{u_s + \sum_{i=1}^n u_i}\}$

第八节 Socket 编程基础☆☆

利用 Socket 编程技术可以开发客户/服务器网络应用程序。

网络应用进程可以创建 3 种类型的 Socket 数据报类型套接字 SOCK_DGRAM(面向 UDP)、流式套接字 SOCK_STREAM (面向 TCP) 和原始套接字 SOCK_RAW。

典型的 SocketAPI 函数：

int **socket()** 创建套接字
int **close()** 关闭套接字
int **bind()** 绑定套接字的本地端点地址 (一般用于服务器端)
int **listen()** 监听状态 (只用于服务器端，仅用于 TCP 服务器套接字)
int **connect()** 将客户套接字与服务器连接 (只用于客户端)
int **accept()** 创建新的套接字来与客户套接字建立 TCP 连接 (只用于服务器端)

Ssize_t **send()** 发送数据
Ssize_t **sendto()** 发送数据(只用于 UDP)
Ssize_t **recv()** 接收数据
Ssize_t **recvfrom()** 接收数据 (只用于 UDP)
Int **setsockopt()** 设置套接字选项
Int **getsockopt()** 读取套接字选项

密训押题

1、文件传输协议 FTP 使用的默认端口号是 ()

A: 21 B:23 C:25 D:80

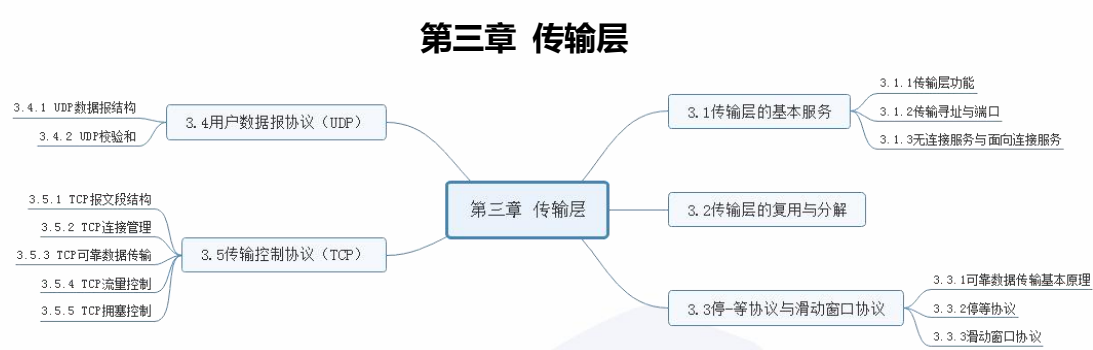
答案：A

解析：用户在使用 FTP 服务时，首先客户进程需要请求与 FTP 服务器的 21 号端口建立一条 TCP 连接，称为控制连接，然后开始 FTP 会话。所以文件传输协议 FTP 使用的默认端口号是 21。

2、WWW 采用的是____的工作模式。

答案:客户/服务器

解析：客户/服务器结构的网络应用是最典型的、最基本的网络应用。人们平时使用的许多网络应用都属于这类应用，比如 WWW 应用、文件传输 FTP、电子邮件等



第一节 传输层的基本服务

一、传输层功能☆☆

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。

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。

二、传输寻址与端口☆

| | | | |
|--------|-----------|-------------|--------------|
| 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 | |

三、无连接服务与面向连接服务☆☆☆

Internet 网络提供无连接服务的传输层协议是 UDP，提供面向连接服务的传输层协议是 TCP。

第二节 传输层的复用与分解☆

| | | | |
|-----------|----------------|--|-----------------------------|
| 传输层的复用与分解 | 定义 | 支持众多应用进程共用同一个传输层协议，并能够将接收到的数据准确交付给不同的应用进程。 | |
| | 实现复用与分解的关键 | 传输层协议能够唯一标识一个套接字 | |
| | 无连接的多路复用与多路分解 | 提供协议 | UDP |
| | | 唯一标识 | <目的 IP 地址，目的端口号> |
| | 面向连接的多路复用与多路分解 | 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 |

第三节 停-等协议与滑动窗口协议

一、可靠数据传输基本原理☆☆☆

- 1、不可靠传输信道在数据传输中可能发生：(1) 比特差错 (2) 乱序 (3) 数据丢失
- 2、实现可靠数据传输措施：(1) 差错检测 (2) 确认：ACK (肯定确认)；NAK (否定确认) (3) 重传 (4) 序号 (5) 计时器。

二、停等协议☆☆☆

停-等协议的基本工作过程是：1、发送方发送经过差错编码和编号的报文段，等待接收方的确认；2、接收方如果正确接收报文段，即差错检测无误且序号正确，则接收报文段，并向发送方发送 ACK；3、否则丢弃报文段，并向发送方发送 NAK；4、发送方如果收到 ACK，则继续发送后续报文段，否则重发刚刚发送的报文段。

停等协议信道利用率：
$$U_{\text{Sender}} = \frac{t_{\text{Seg}}}{t_{\text{Seg}} + \text{RTT} + t_{\text{ACK}}}$$

三、滑动窗口协议☆☆

滑动窗口协议实质上就是将可靠数据传输的工作过程，抽象到分组序号空间，即发送方确保分组按序发送，接收方确保分组按序提交。

两种最具代表性的滑动窗口协议是：**GBN 协议（发送窗口 ≥ 1 ，接收窗口 $= 1$ ）**和**SR 协议（发送窗口和接收窗口都大于 1）**

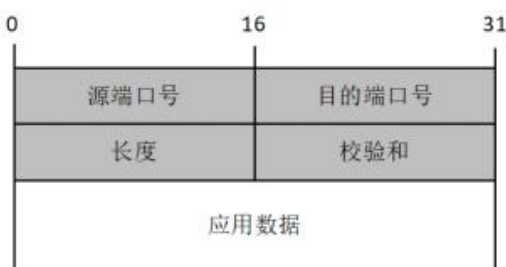
滑动窗口协议信道利用率：
$$U_{\text{Sender}} = \frac{W_s \times t_{\text{Seg}}}{t_{\text{Seg}} + \text{RTT} + t_{\text{ACK}}}$$

第四节 用户数据报协议（UDP）☆

用户数据报协议 UDP 是 Internet 传输层协议，提供无连接、不可靠、数据报尽力传输服务。

UDP 与 TCP 相比，优点有：(1) 应用进程更容易控制发送什么数据以及何时发送。(2) 无需建立连接。(3) 无连接状态。4) 首部开销小。

一、UDP 数据报结构



二、UDP 校验和

- 1、提供了差错检测功能
- 2、计算内容包括：UDP 伪首部、UDP 首部和应用层数据
- 3、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。

第五节 传输控制协议（TCP）☆☆☆☆☆

TCP 协议特点：1、应用进程要先建立连接。2、每一条 TCP 连接只有两个端点。3、可靠交付。无差错，不丢失，不重复且按序到达。4、全双工通信。5、面向字节流。

一、TCP 报文段结构☆☆



二、TCP 连接管理☆☆☆☆☆

| | | | | |
|-----------------|----------|----------|-------|----------------------------------|
| TCP 连接 管理 | 建立 连接 | 三次 握手 | 第一次握手 | 主机 A 向主机 B 收送连接请求段。 |
| | | | 第二次握手 | 主机 B 收到 TCP 连接请求段后，如同意，则发回确认报文段。 |
| | | | 第三次握手 | (可携带数据)主机 A 对主机 B 的同意连接报文段进行确认。 |
| | 拆除 连接 | 四次 挥手 | 第一次挥手 | 主机 A 向主机 B 发送释放连接报文段 |
| | | | 第二次挥手 | 主机 B 向主机 A 发送确认段 |
| | | | 第三次挥手 | 主机 B 向主机 A 发送释放连接报文段 |
| | | | 第四次挥手 | 主机 A 向主机 B 发送确认段 |
| | | | | |

TCP 的序号是对每个应用层数据的每个字节进行编号。确认序号是期望从对方接收数据的字节序号，将已连续接收到的应用层数据的最后一个字节的序号加 1，作为确认序号。

三、TCP 可靠数据传输☆☆☆

TCP 的可靠数据传输实现机制包括差错编码、确认、序号、重传、计时器等。

TCP 可靠数据传输的工作机制：1、数据分割 2、启动计时器 3、校验和检测数据差错 4、重新排序 5、丢弃重复报文段 6、提供流量控制。

发送方的 3 个与发送和重传有关的主要事件：从上层应用程序接收数据、定时器超时、收到 ACK。

四、TCP 流量控制☆☆☆

流量控制 (flow control) 的目的是协调协议发送方与接收方的数据发送与接收速度，避免因发送方发送数据太快，超出接收方的数据接收和处理能力，导致接收方被数据“淹没”，即数据到达速度超出接收方的接收、缓存或处理能力，致使数据在接收方被丢弃。

五、TCP 拥塞控制☆☆☆☆☆

拥塞控制就是通过合理调度、规范、调整向网络中发送数据的主机数量、发送速率或数据量，以避免拥塞或尽快消除已发生的拥塞。TCP 的拥塞控制算法包括了慢启动、拥塞避免、快速重传和快速恢复。(CongWin 初值为 1，Threshold 的初值为 16MSS。)

慢启动：收到一个确认，CongWin 值就加倍，即指数增长的时间段。

拥塞避免：每经过一个 RTT，拥塞窗口 CongWin 的值增加 1MSS，即线性增长的时间段。

快速重传：基本思想是接收端收到 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：是配合快速重传使用的算法，不再重新从慢启动阶段开始，而是从新的阈值开始，直接进入拥塞避免阶段。具体做法是：当发送端连续收到 3 次重复确认时，将阈值 Threshold 减半，并且将拥塞窗口 CongWin 的值置为减半后的 Threshold，然后开始执行拥塞避免算法，使 CongWin 缓慢地加性增长。

密训押题

1、从滑动窗口的观点来看“选择重传”协议，其窗口尺寸的大小为（ ）

- A:发送窗口>1，接收窗口>1 B:发送窗口>1，接收窗口=1
C:发送窗口=1，接收窗口>1 D:发送窗口=1，接收窗口=1

答案：A

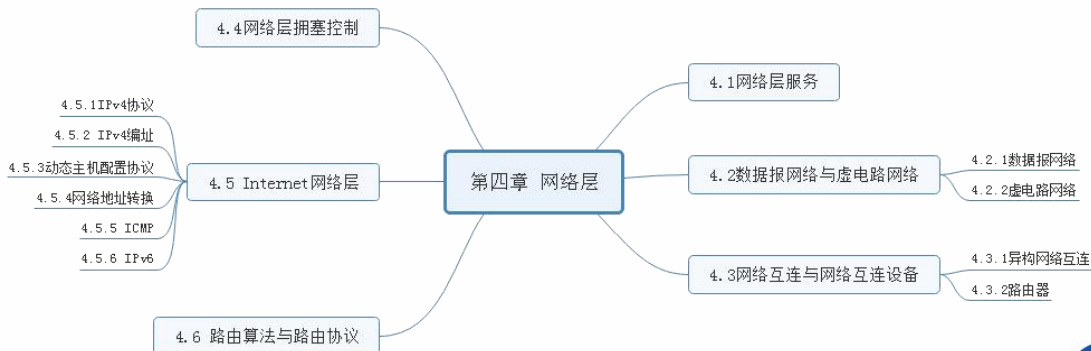
解析：选择重传（SR）协议是通过让发送方仅重传那些未被接收方确认的分组，而避免了不必要的重传。为此，SR 协议的接收方是对每个正确接收的分组进行逐个确认。SR 协议的发送窗口和接收窗口都大于 1，虽然理论上发送窗口和接收窗口大小可以不相等，但很多 SR 协议设计取相同的发送窗口和接收窗口大小。

2、简述传输层提供的两种传输服务及其概念。

答案：传输层提供的服务可以分为无连接服务和面向连接服务两大类。无连接服务是指数据传输之前无需与对端进行任何信息交换（即“握手”），直接构造传输层报文段并向接收端发送；面向连接服务是指在数据传输之前，需要双方交换一些控制信息，建立逻辑连接，然后再传输数据，数据传输结束后还需要再拆除连接。

解析：传输层提供的服务可以分为无连接服务和面向连接服务两大类。无连接服务是指数据传输之前无需与对端进行任何信息交换（即“握手”），直接构造传输层报文段并向接收端发送；面向连接服务是指在数据传输之前，需要双方交换一些控制信息，建立逻辑连接，然后再传输数据，数据传输结束后还需要再拆除连接。

第四章 网络层



第一节 网络层服务☆☆

| | | |
|-------------------|------------------|---|
| 网 络 层 的 功 能 | 转发 | 当通过一条输入链路接收到一个分组后，路由器需要决策通过哪条输出链路将分组发送出去，并将分组从输入接口转移到输出接口。 |
| | 路由 | 当分组从源主机流向目的主机时，必须通过某种方式决定分组经过的路由或路径，计算分组所经过的路径的算法被称为路由选择算法，或称为路由算法。 |
| | 连接建立 (分组交换网络) | 仅在网络层提供连接的 虚电路网络 。 仅在网络层提供无连接服务的 数据报网络 。 |

第二节 数据报网络与虚电路网络☆☆

一、数据报网络

按照目的主机地址进行路由选择的网络称为数据报网络。

二、虚电路网络

1、虚电路网络在网络层提供面向连接的**分组交换服务**。虚电路是在源主机到目的主机的一条路径上建立的一条网络层逻辑连接，称之为虚电路。

2、一条虚电路由 3 个要素构成：1) 从源主机到目的主机之间的一条路径 2) 该路径上的每条链路各有一个虚电路标识 3) 该路径上每台分组交换机的转发表中记录虚电路标识的接续关系

3、虚电路分组交换有永久型和交换型两种。

4、虚电路交换与数据报交换主要差别表现为：是将顺序控制、差错控制和流量控制等功能交给网络来完成（虚电路），还是由端系统来完成（数据报）。

第三节 网络互连与网络互连设备

一、异构网络互连☆☆

异构网络主要是指两个网络的通信技术和运行协议的不同。实现异构网络互连基本策略主要包括协议转换和构建虚拟互联网络。

在网络层实现网络互连的设备是**路由器**。**集线器**和**中继器**都是物理层设备。**交换机**和**网桥**是数据链路层设备，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。

二、路由器☆☆☆☆

路由器是最典型的网络层设备。

| | | |
|-------------|-----------|----------------------------------|
| 路 由 器 | 输入端口 | 线路端接 → 数据链路处理（协议、拆封）→ 查找、转发、排队 → |
| | 交换结构 | 基于内存交换、基于总线交换、基于网络交换 |
| | 输出端口 | → 排队、缓存管理 → 数据链路处理（协议、拆封）→ 线路端接 |
| | 路由处理 器 | 转发与路由选择是路由器两项最重要的基本功能。 |

第四节 网络层拥塞控制☆☆☆

| | | | |
|------|----|--|--------------------------------------|
| 拥塞 | 概念 | 拥塞是一种持续的过载的网络状态，即用户对网络资源的总需求超过了网络固有容量。 | |
| | 原因 | 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 4) 网络中某些部分发生了故障 | |
| 拥塞控制 | 概念 | 端系统或结点，采取某些措施来避免拥塞的发生，或者尽快消除已发生的拥塞。 | |
| | 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，从避免拥塞发生。 |
| | | 准入控制 | 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 | 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。 |

第五节 Internet 网络层☆☆☆☆☆

一、IPv4 协议

1、IP 数据报格式☆☆

| | | | | | | | | | | | |
|--------------|--|--|--|-----------|--|-------------|--|-------------|--|--|--|
| 版本（4 位） | | | | 首部长度（4 位） | | 区分服务（8 位） | | 数据报长度（16 位） | | | |
| 标识（16 位） | | | | | | 标志（3 位） | | 片偏移量（13 位） | | | |
| 生存时间（8 位） | | | | 上层协议（8 位） | | 首部校验和（16 位） | | | | | |
| 源 IP 地址（32） | | | | | | | | | | | |
| 目的 IP 地址（32） | | | | | | | | | | | |
| 选项（可选，长度可变） | | | | | | | | | | | |
| 数据 | | | | | | | | | | | |

2、IP 数据报分片☆☆☆☆☆

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 $F_i = \frac{d}{8} \times (i-1)$ ， $1 \leq i \leq n$ ；每个 IP 分片的总长度字段为

$$L_i = \begin{cases} d + 20, & 1 \leq i < n \\ L - d \times (n - 1), & i = n \end{cases} \quad \text{每个 IP 分片的 MF 字段为 } MF_i = \begin{cases} 1, & 1 \leq i < n \\ 0, & i = n \end{cases}$$

二、IPv4 编址☆☆☆☆☆

1、IPv4 地址有 3 种常用的标记法：二进制标记法、点分十进制标记法、十六进制标记法。

2、IP 地址划分为两部分：前缀 (网络部分) 和后缀 (主机部分)。定长前缀为分类地址，无类地址中网络地址前缀长度可变。

| 分类地址划分 | | | |
|--------|------|-------------------------------------|-----------|
| 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 |

| 特殊地址 | 私有 IP 地址 | 无类地址 |
|------------------------------|-----------------------|---------------------------------|
| 本地主机地址 0.0.0.0/32 | A 类 10.0.0.0/8 | 前缀变成 0 ~ 32 位的任意值。形式为 a.b.c.d/x |
| 有限广播地址 255.255.255.255/32 | B 类 172.16.0.0/12 | |
| 回送地址 127.0.0.0/8 | C 类 192.168.0.0、16 | |

3、子网划分：子网化就是指将一个较大的子网划分为多个较小子网的过程。超网化是指将具有较长前缀的相对较小的子网合并为一个具有稍短前缀的相对较大的子网。超网化是子网化的逆过程。子网掩码用来定义一个子网的网络前缀长度，是一个 32 位数，取值规则是：对应网络前缀，全部为 1，其余全部为 0。准确描述一个子网有两种形式：CIDR 和子网地址加子网掩码。

4、路由聚合：路由聚合是为了提高路由效率，减少路由表项数，尽可能将能够聚合在一起的子网聚合成一个大的子网。“下一跳地址”和“接口”相同，才能聚合。

三、动态主机配置协议☆

动态主机配置协议 DHCP 工作过程是：1、DHCP 服务器发现 2、DHCP 服务器提供 3、DHCP 请求 4、DHCP 确认

四、网络地址转换☆

NAT 工作原理：对于从内网出去，进入公共互联网的 IP 数据报，将其源 IP 地址替换为 NAT 服务器拥有的合法的公共 IP 地址，同时替换源端口号，并将替换关系记录到 NAT 转换表中；对于从公共互联网返回的 IP 数据报，依据其目的 IP 地址与目的端口号检索 NAT 转换表，并利用检索到的内部私有 IP 地址与对应的端口号替换目的 IP 地址和目的端口号，然后将 IP 数据报转发到内部网络。

五、ICMP☆

ICMP 包括 3 个字段：类型、代码和校验和。ICMP 差错报告报文有 5 种：终点不可达、源点抑制、时间超时、参数问题、路由重定向。ICMP 询问报文：回声（echo）请求/应答、时间戳请求/应答。

六、IPv6☆☆

1、数据报格式：（1）版本字段（4位）；（2）流量类型字段（8位）；（3）流标签字段（20位）；（4）下一个首部字段（8位）；（5）跳数限制字段（8位）；（6）源IP地址（128位）和目的IP地址字段（128位）；（7）数据。

2、IPv6地址：地址长度为128位。

IPv6地址包括：（1）**单播地址**（可以作为IPv6数据报的源地址和目的地址）。（2）**组播地址**（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**（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）。

第六节 路由算法与路由协议☆☆

| 类别 | 代表性算法 | 基础 |
|-----------|----------------------------|---|
| 全局式路由选择算法 | 链路状态路由选择算法（动态）☆☆☆☆☆ | 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（动态） | 距离向量路由选择算法的基础是 Bellman-Ford 方程（简称 B-F 方程） |

层次化路由选择：实现大规模网络路由选择最有效的、最可行的解决方案。每个自治系统都存在网关路由器。层次化路由选择将大规模互联网的路由划分为两层：自治系统内路由选择和自治系统间路由选择。

| | | |
|--------------------------|-----------|-----------------|
| Internet 路由选择协议（层次化路由选择） | 自治系统内路由选择 | RIP☆☆☆☆☆ |
| | | OSPF |
| | 自治系统间路由选择 | BGP |

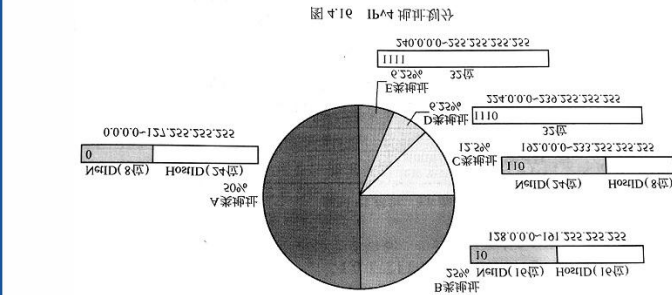
密训押题

1、下列IP地址中正确的B类IP地址是（ ）

A:182.16.0.18 B:202.96.209.5 C:255.255.0.0 D:59.117.25.22

答案：A

解析：

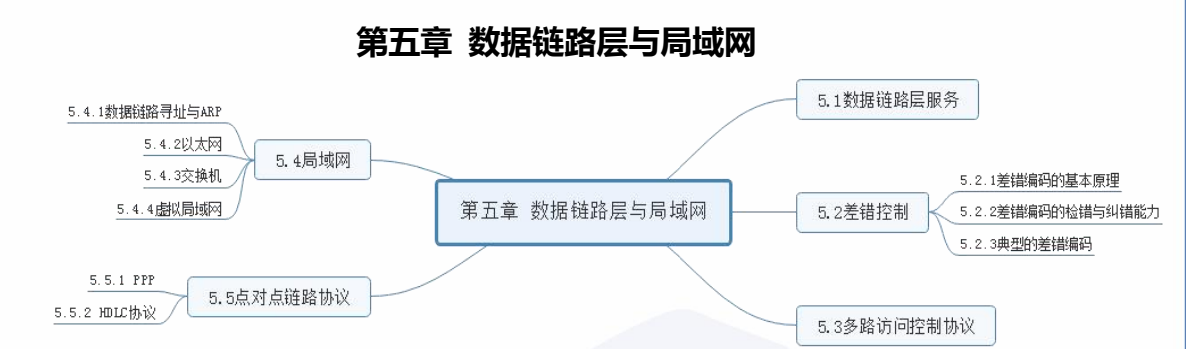


A选项的首字节是182，在128~191之间，故属于B类。

2、路由选择的核心是_____。

答案:路由选择算法

解析 :路由选择的关键 ,就是从源主机的默认路由器到目的主机的默认路由器之间的路径优选。于是 ,路由选择问题就可以简化为在路由器之间选择最佳路径问题。路由选择算法的目的 ,就是在给定一组网络中的路由器以及路由器之间的连接链路的情况下 ,寻找一条从源路由器到目的路由器的最优路径。所以路由选择的核心是路由选择算法。



第一节 数据链路层服务☆☆☆

数据链路层提供的服务：组帧、链路接入、可靠交付、差错控制。

第二节 差错控制

差错控制：就是通过差错编码技术，实现对信息传输差错的检测，并基于某种机制进行差错纠正和处理，是计算机网络中实现可靠传输的重要技术手段，并在许多数据链路层协议中应用。☆☆☆☆

| | | |
|------------------|-----------------------|--|
| 噪声(导致差错) ☆☆ | 随机噪声 | 引起 随机差错 或 独立差错 。 |
| | 冲击噪声 | 指突然发生的噪声。冲击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 突发长度 。 |
| 差错控制基本方 式☆☆☆☆ | 检错重发 | |
| | 前向纠错 (接收端进行、利用纠错编码) | |
| | 反馈校验 | |
| | 检错丢弃 | |

一、差错编码的基本原理☆☆☆

在待传输 (或待保护) 数据信息的基础上，附加一定的冗余信息，该冗余信息建立起数据信息的某种关联关系，将数据信息以及附加的冗余信息一同发送到接受端，接受端可以检测冗余信息表征的数据信息的关联关系是否存在，如果存在则没有错误，否则就是有错误。

二、差错编码的检错与纠错能力☆

- 1、对于检错编码，如果编码集的汉明距离 $d_s=r+1$ ，则该差错编码可以检测 r 位的差错。
- 2、对于纠错编码，如果编码集的汉明距离 $d_s=2r+1$ ，则该差错编码可以检测 r 位的差错。

三、典型的差错编码☆☆☆☆☆

| | | |
|----------------|---|---------------------------------------|
| 奇偶校验码 ☆☆☆☆☆ | 奇 校 验码 | 1 位冗余位的取值为“0”或“1”，使得编码后的码字中“1”的个数为奇数。 |
| | 偶 校 验码 | 1 位冗余位的取值为“0”或“1”，使得编码后的码字中“1”的个数为偶数。 |
| 汉明码 | 若一个信息为 $k=n-1$ 位的比特流 $a_{n-1}a_{n-2}\dots a_1$ 加上偶校验位 a_0 ，构成一个 n 位的码字 $a_{n-1}a_{n-2}\dots a_1a_0$ 。在接收方校验时，可按关系式 $S=a_{n-1}\oplus a_{n-2}\oplus\dots a_1\oplus a_0$ 计算，若 $S=0$ ，则无错，若 $S=1$ ，则有错。 | |
| 循环冗余码 ☆☆☆☆☆ | <p>(1) 在帧的低位端加上 r 个 0 位，使该帧扩展为 $m+r$ 位(相当于左移 r 位)，对应的多项式为 $x^rM(x)$。</p> <p>(2) 用 $G(x)$ 系数对应的位串，去除(模 2 除法)$x^rM(x)$ 系数对应的位串，求得 r 位余数 R。</p> <p>(3) 用 $x^rM(x)$ 系数对应的位串，减(模 2 减法)去余数 R，结果就是完成 CRC 编码的帧。</p> | |

第三节 多路访问控制协议

| | | |
|------------------------|----------|---|
| 信道划分 MAC 协议 ☆☆ | 频分多路复用 | 频域划分制，优点分路方便，缺点串扰。 |
| | 时分多路复用 | 时域划分，可分为同步时分多路复用和异步时分多路复用。 |
| | 波分多路复用 | 广泛应用于 光纤通信 中。 |
| | 码分多路复用 | |
| 随机访问 MAC 协议 ☆☆☆☆ | ALOHA 协议 | <p>(1) 纯 ALOHA：任何一个站点有数据要发送时就可以直接发送至信道。</p> <p>(2) 时隙 ALOHA：把信道时间分成离散的时隙，每个时隙为发送一帧所需的发送时间，每个通信站只能在每个时隙开始时刻发送帧，如果在一个时隙内发送帧出现冲突，下一个时隙以概率 P 重发该帧，以概率 $(1-P)$ 不发该帧(等待下一个时隙)，直到帧发送成功。</p> |
| | CSMA | <p>(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，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；若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。</p> <p>(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。</p> <p>(3) P-坚持 CSMA：适用于时隙信道(即同步划分时隙)。基本原理：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。</p> |

| | | |
|--------------|---|---|
| | CSMA/CD ☆☆☆☆☆ | 3 种状态：传输状态、竞争状态、空闲状态。约束关系： $\frac{L_{\min}}{R} \gg \frac{2D_{\max}}{v}$ |
| 受控接入 | 集中式控制：主要方法是轮询技术，又分为：轮叫轮询和传递轮询。 | |
| MAC 协议 ☆☆ | 分散式控制：最重要的就是对令牌的维护。令牌丢失和数据帧无法撤销，是环网上最严重的两种错误。 | |

第四节 局域网

一、数据链路层寻址与 ARP

1、MAC 地址（物理地址、局域网地址）☆☆

(1) 两块网络适配器具有不同的 MAC 地址，用来标识局域网的结点或网络接口。MAC 地址具有唯一性，每个接口对应一个 MAC 地址。

(2) 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。如：00-2A-E1-76-8C-39 或者 00:2A:E1:76:8C:39。

链路层的交换机（第二层交换机）的接口没有相关联的链路层地址。

2、地址解析协议（ARP）☆☆☆☆

(1) 作用：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。

(2) 基本思想：在每一台主机中设置专用内存区域，称为 ARP 高速缓存（也称为 ARP 表），存储该主机所在局域网中其他主机和路由器的 IP 地址与 MAC 地址的映射关系，并且这个映射表要经常更新。ARP 通过广播 ARP 查询报文，来询问某目的 IP 地址对应的 MAC 地址，即知道本网内某主机的 IP 地址，可以查询得到其 MAC 地址。

(3) 注意：ARP 查询分组是通过一个广播帧发送的，而 ARP 响应分组是通过一个标准的单播帧发送的。

二、以太网☆☆

1、以太网帧结构

| 目的地址 (6 字节) | 源地址 (6 字节) | 类型 (2 字节) | 数据 (46 ~ 1500 字节) | CRC (4 字节) |
|----------------|---------------|--------------|----------------------|---------------|
|----------------|---------------|--------------|----------------------|---------------|

注意：以太网的最短帧长为 64 字节，即以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）。

2、以太网技术：(1) 10Base-T 以太网 (2) 快速以太网 (3) 千兆位以太网 (4) 万兆位以太网

三、交换机☆

交换机就是多端口网桥，是目前应用最广泛的数据链路层设备。

交换机的优点是：消除冲突、支持异质链路、网络管理。

四、虚拟局域网☆☆

虚拟局域网是一个基于交换机的逻辑分割广播域的局域网应用形式。

划分虚拟局域网的方法主要有三种：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。

第五节 点对点链路协议☆☆

一、PPP

- 1、PPP 提供的功能：成帧、链路控制协议、网络控制协议。
- 2、PPP 数据帧结构：标志（01111110），地址（11111111），控制（00000011），协议，信息，校验和，标志（01111110）

二、HDLC 协议☆☆

- 1、帧格式：01111110，地址，控制，校验和，01111110。
- 2、HDLC 有 **3 种类型的帧**：信息帧（控制字段是 0 Seq T/F Next）、管理帧（控制字段是 10 Type T/F Next）、无序号帧（控制字段是 11 Type T/F Next）。
- 3、零比特填充过程：发送时，发现 5 个连续的 1，即插入一个 0，收到后，当发现 5 个连续的 1，就删除其后的 0，还原信息。

密训押题

- 1、在光纤信道上可以采用的多路复用技术是（ ）

A:波分多路复用 B:异步时分多路复用 C:统计多路复用 D:同步时分多路复用

答案：A

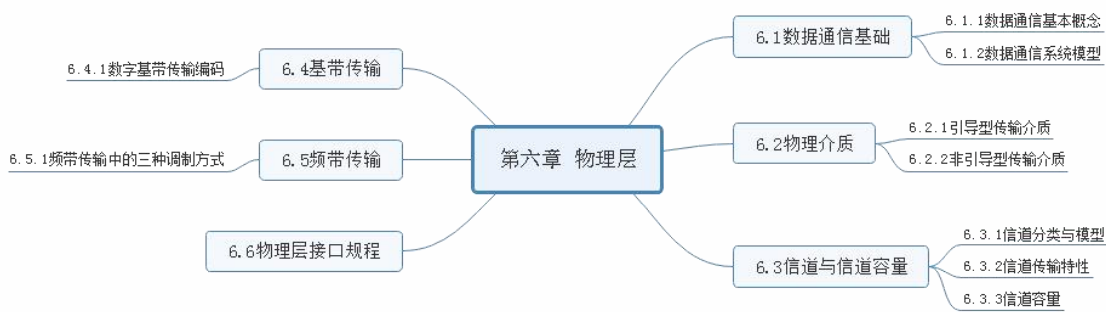
解析：波分多路复用（WDM）简称波分复用，广泛应用于光纤通信中，其实质是一种频分多路复用，只是由于在光纤通信中，光载波频率很高，通常用光的波长来代替频率来讨论，所以称为波分多路复用。

- 2、利用 HDLC 规程在信源传出的数据是 11111010111110，则信宿收到的数据是_____。

答案:11111011111

解析：HDLC 协议是面向位的协议，为确保数据的透明传输，HDLC 使用位填充。首先，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。接收端接收一个帧后，先找到标志字段 01111110 确定帧的边界，接着利用硬件扫描整个比特流，当发现 5 个连续的 1，就删除其后的 0，以还原原来的信息。利用 HDLC 规程在信源传出的数据是 11111010111110，发现 5 个连续的 1，所以要删除后面的 0，所以接收端收到的信息为 11111011111。

第六章 物理层



第一节 数据通信基础☆☆☆

一、数据通信基本概念

1、消息与信息：信息是消息中包含的有意义的内容，消息是信息的载体。2、通信：能够实现通信功能的各种技术、设备和方法的总体。3、信号：信息在传输通道中传播的载体。4、数据：对客观事物的性质状态以及相互关系等进行记载的符号及其组合。5、信道：信号传输的介质。

二、数据通信系统模型

1、数据通信系统的构成：信源、发送设备、信道、信宿、噪声。

2、模拟通信和数字通信

模拟信号是指信号的因变量完全随连续消息的变化而变化的信号。模拟信号的因变量一定是连续的；数字信号是指表示消息的因变量是离散的，自变量时间的取值也是离散的信号，数字信号的因变量的状态是有限的。

3、数据通信方式

| | | |
|-----------|-------------|---|
| 按传输方向分类 | 单向通信(单工) | 任何时间都只能有一个方向的通信，而没有反方向的交互。 |
| | 双向交替通信(半双工) | 通信的双方都可以发送信息，但不能双方同时发送(或同时接收)对讲机。 |
| | 双向同时通信(全双工) | 通信双方可以同时发送和接收信息。 |
| 二进制传输时空顺序 | 并行通信 | 为一个字节的每一位(bit)都设置一个传输通道，全部位(bit)同时进行传送。 |
| | 串行通信 | 只为信息传输设置一条通道。(适用于长距离传输) |
| 按发送和接收步调 | 异步通信 | 以字符为单位单独发送 |
| | 同步通信 | 以数据库为单位进行发送 |

第二节 物理介质☆

一、引导型传输介质

1、架空明线 2、双绞线 3、同轴电缆 4、光纤

二、非引导型传输介质

1、地波传输 2、天波传输 3、视线传输

第三节 信道与信道容量

一、信道分类与模型☆

- 1、调制信道：调制信道是指信号从调制器的输出端传输到解调器的输入端经过的部分。
- 2、编码信道：编码信道是指数字信号由编码器输出端传输到译码器输入端经过的部分，包括其中的所有变换装置与传输介质。

二、信道传输特性☆

| 信道类别 | 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 | 1) 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。 |

三、信道容量☆☆☆☆☆

(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： $C = B \log_2 \left(1 + \frac{S}{N} \right)$ ；

(3) 离散信道容量：每个符号能传输的最大平均信息量和单位时间内能够传输的最大平均信息量。

第四节 基带传输☆☆☆☆☆

一、数字基带传输编码

| | | |
|---------|--------|--|
| 数字基带信号码 | 单极不归零码 | 脉冲幅值要么是正电平、要么是零电平，只有一个极性，在整个脉冲持续时间内，电平保持不变，且脉冲持续期结束时也不要求必须回归 0 电平。 |
| | 双极不归零码 | 脉冲幅值要么是正电平、要么是负电平，在整个脉冲持续时间内，电平保持不变，且脉冲持续期结束时也不要求必须回归 0 电平。 |
| | 单极归零码 | 与单极不归零码不同的是，在每个正脉冲持续期的中间时刻，电平要回到零电平。 |
| | 双极归零码 | 与双不归零码不同的是，在每个正、负脉冲持续期的中间时刻，电平要回到零电平。 |
| | 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。 |

| | | |
|---------|--------|---|
| 数字基带传输码 | 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。 双相码的另一种码型是差分双相码，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。 |
| | 米勒码 | （1）信息码中的 1 编码为双极非归零码的 01 或者 10； （2）信息码连 1 时，后面的 1 要交替编码； （3）信息码中的 0 编码为双极非归零码的 00 或者 11； （4）信息码单个 0 时，其前沿、中间时刻、后沿均不跳变； （5）信息码连 0 时，两个 0 码元的间隔跳变，即前一个 0 的后沿跳变。 |
| | CMI 码 | 信息码的 0 编码为双极不归零码的 01；信息码的 1 交替编码为双极不归零码的 11 和 00。 |
| | nBmB 码 | 将 n 位码映射为 m 位， $m > n$ ，从 2^m 个码中选出 2^n 个有效码，获得良好的编码性能。 |

第五节、频带传输☆☆☆☆

一、频带传输中的三种调制方式

| | | |
|---------|---|--|
| 二进制数字调制 | 二进制幅移键控 | 根据二进制基带信号电平的高低，控制载波信号选择两种不同的幅值。 |
| | 二进制频移键控 | 根据二进制基带数字信号控制或选择输出一段(与码元持续时间相同)频率为 f_1 或 f_2 载波信号。 |
| | 二进制相移键控 | 根据二进制基带信号电平的高低，控制载波信号选择两种不同的相位。 |
| | 二进制差分相移键控 | 利用相邻两个码元载波间的相对相位变化表示数字基带信号的数字信息 |
| 多进制数字调制 | 多进制数字调制是二进制数字调制的扩展，是利用多进制数字基带信号去调制载波信号的特征参数 | |
| 正交幅值调制 | QAM 是“二维”调制技术，对载波信号的幅值和相位同时进行调制的联合调制技术。 | |

第六节 物理层接口规程☆

物理层接口特性：

- （1）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。
- （2）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。
- （3）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。

(4) 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。

密训押题

1、简述模拟信号、数字信号和信道的概念。

答案：模拟信号是指信号的因变量完全随连续消息的变化而变化的信号。模拟信号的自变量可以是连续的，也可以是离散的；但其因变量一定是连续的。

数字信号是指表示消息的因变量是离散的，自变量时间的取值也是离散的信号，数字信号的因变量的状态是有限的。

信道是信号传输的介质。

解析：模拟信号是指信号的因变量完全随连续消息的变化而变化的信号。模拟信号的自变量可以是连续的，也可以是离散的；但其因变量一定是连续的。传统的电视图像信号、电话语音信号、各种传感器的输出信号以及许多遥感遥测信号都是模拟信号。

数字信号是指表示消息的因变量是离散的，自变量时间的取值也是离散的信号，数字信号的因变量的状态是有限的。

信道是信号传输的介质，或信道是以传输介质为基础的信号通道。

2、设数据传输速率为 3600bps，若采用 8 相调制方式，则码元速率应为（ ）

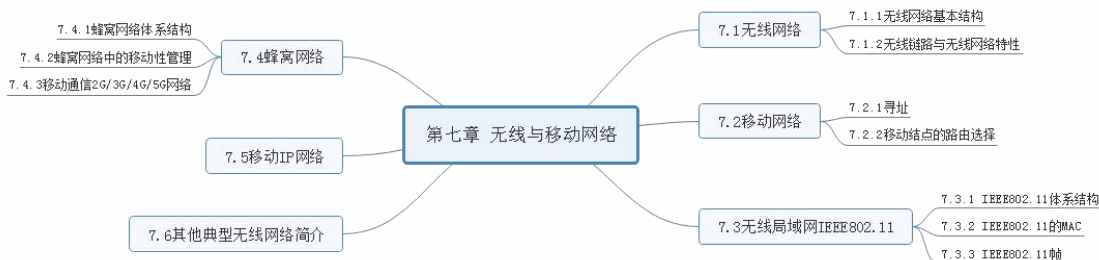
A:1200Baud B:1800Baud C:7200Baud D:9600Baud

答案：A

解析：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： $R_b = R \log M$ ；

根据题意代入公式得： $3600 = R \log 8$ ，又 $2^3 = 8$ ， $\log 8$ 为 3，最终求得码元速率 R 为：1200Baud。

第七章 无线与移动网络



第一节 无线网络☆

一、无线网络基本结构

- 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。
- 2、无线主机不通过基站（即没有基站），Ad Hoc 网络中的每个节点都兼有路由器和主机两种功能。

二、无线链路与无线网络特性。

无线链路有别于有线链路的主要表现在以下方面：信号强度的衰减、干扰、多径传播。

第二节 移动网络☆

无线网络不一定是移动网络、但移动网络一定是无线网络。移动网络中的移动结点是随时间改变其与网络连接位置的结点，并且移动采用无线通信技术。

一、寻址

- 1、外部网络可以通过向所有其他网络发通告，告诉它们该移动结点正在它的网络中。
- 2、将移动网络功能从网络核心搬到网络边缘，由该移动结点的归属网络来实现。

二、移动结点的路由选择

- 1、间接路由选择
- 2、直接路由选择。

第三节 无线局域网 IEEE802.11☆☆☆☆

| 标准 | 频率范围/GHz | 数据率 | 物理层 | 特点 |
|--------------|----------|----------------|-----------|-----------------------------|
| IEEE 802.11b | 2.4 | 最高为 11 Mbit/s | 扩频 | 信号传播距离最远，且穿透能力较好 |
| IEEE 802.11a | 5 | 最高为 54 Mbit/s | OFDM | 支持更多用户同时上网，传输距离较短 |
| IEEE 802.11g | 2.4 | 最高为 54 Mbit/s | OFDM | 支持更多用户同时上网，信号传播距离最远，且穿透能力较好 |
| IEEE 802.11n | 2.4/5 | 最高为 600 Mbit/s | MIMO/OFDM | 数据速率高 |

IEEE802.11 标准的共同特征：

- （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。

一、IEEE802.11 体系结构☆

基站和基本服务集。

二、IEEE 802.11 的 MAC☆

IEEE 802.11 的 MAC 协议采用 CSMA/CA 协议。IEEE 802.11 使用链路层确认/重传(ARQ) 方案。

三、IEEE 802.11 帧☆☆

IEEE 802.11 帧共有 3 种类型：控制帧、数据帧和管理帧。IEEE 802.11 数据帧结构：MAC 首部（30 字节）、帧主体、尾部（FCS）。

第四节 蜂窝网络☆☆

一、蜂窝网络体系结构

第二代蜂窝移动通信（2G）的代表性体制是 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。

第三代蜂窝移动通信（3G）系统中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。

二、蜂窝网络中的移动性管理

GSM 标准采用了一种间接路由选择方法管理移动性。GSM 的归属网络维护一个称作归属位置寄存器(Home Location Register, HLR)的数据库，GSM 的被访网络维护一个称作访问者位置寄存器(Visitor Location Register, VLR)的数据库。

三、移动通信 2G/3G/4G/5G 网络

| 类别 | 技术 | 特征 |
|----|-----------|--|
| 2G | FDMA/TDMA | 移动电话系统的开端，分为承载业务、电信业务、附加业务。 |
| 3G | CDMA/TDMA | 全球统一频谱、标准，无缝覆盖，更高频谱效率和系统容量，服务质量优、保密强，适应多种环境。 |
| 4G | LTE 系统 | 高速率传输、智能化、业务多样化、无缝接入、后向兼容、经济。 |
| 5G | 在研究中 | 有望共用一标准。 |

第五节 移动 IP 网络☆

移动 IP 标准由 3 部分组成：代理发现、向归属代理注册以及数据报的间接路由选择。

第六节 其他典型无线网络简介☆

| | |
|--------|---|
| 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。 |

密训押题

1、移动 Ad Hoc 网络中的每个节点都兼有路由器和_____两种功能。

答案:主机

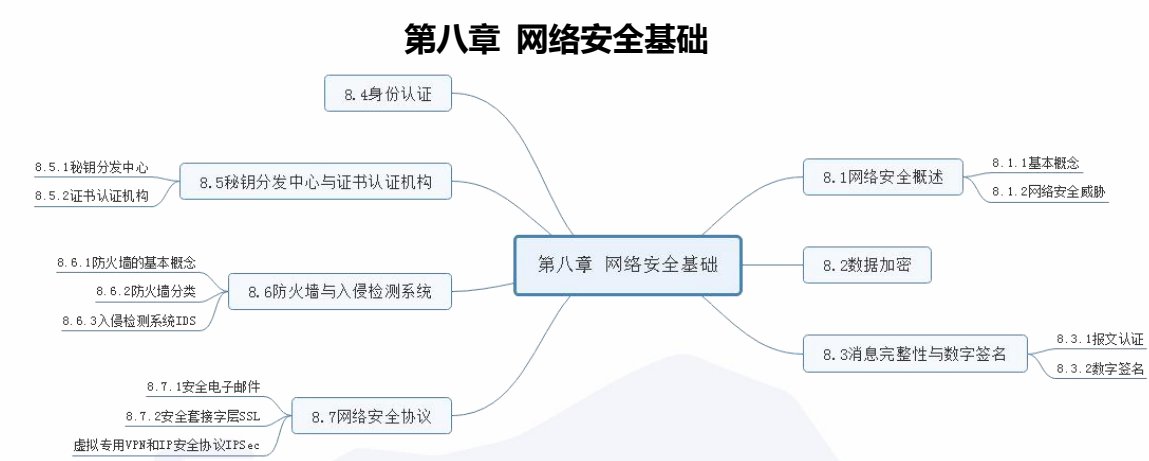
解析：无线主机不通过基站（即没有基站），直接与另一个无线主机直接通信的无线网络模式称为自组织网络，或称为特定网络，也称为 Ad Hoc 网络。自组织网络没有基站，无线主机也不与网络基础设施相连，因此，主机本身必须提供诸如路由选择、地址分配等服务。故 Ad Hoc 网络中的每个节点都兼有路由器和主机两种功能。

2、蜂窝移动通信系统中的多址接入方法有频分多址接入、时分多址接入和_____接入。

答案:码分多址

解析：第二代蜂窝移动通信（2G）的代表性体制是 GSM，采用的是 FDMA（频分多址）和 TDMA（时分多址）混合接入的方式。

第三代蜂窝移动通信（3G）系统中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。综合上，蜂窝移动通信系统用了频分多址接入、时分多址接入和码分多址接入



第一节 网络安全概述☆☆☆

一、基本概念

网络安全所需要的基本属性：机密性、消息完整性、可访问与可用性、身份认证。

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

二、网络安全威胁

网络主要面临安全威胁有：首先，从报文传输方面，主要包括窃听、插入、假冒、劫持等安全威胁。比较常见的网络攻击还包括拒绝服务 DoS 以及分布式拒绝服务 DDoS 等。其次还包括映射、分组“嗅探”和 IP 欺骗等。

第二节 数据加密☆☆

| | | |
|--------|---------------|---|
| 传统加密方式 | 替代密码 ☆☆☆☆☆ | 替代密码是将明文字母表 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。 |
| | 换位密码 ☆☆☆☆☆ | 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。 |
| 对称密钥加密 | DES 加密算法 | 典型分组密码，使用 56 位的密钥，明文为 64 位分组序列，共进行 16 轮的加密，每轮都进行复杂的替代和置换操作，并且每轮加密都会使用一个由 56 位密钥导出的 48 位子密钥，最终输出与明文等长的 64 位密文。 |

| | | |
|------------|---|--|
| | 三重 DES | 该方法使用两个密钥,执行三次 DES 算法。加密的过程是加密-解密-加密,解密的过程是解密-加密-解密。 |
| | AES 加密 | AES 加密过程涉及 4 种操作:字节替代、行移位、列混淆和轮密钥加。 |
| | IDEA | 一个分组长度为 64 位的分组密码算法,密钥长度为 128 位,同一个算法即可用于加密;也可用于解密。 |
| 非对称/公开密钥加密 | 比较典型的公开密钥加密算法有 Diffie-Hellman 算法和 RSA 算法。 | |

第三节 消息完整性与数字签名☆☆

一、报文认证

消息完整性检测的一个重要目的就是要完成报文认证的任务。对报文应用散列函数,得到一个固定长度的散列码,称为报文摘要。报文认证的目的有两个: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。

二、数字签名

报文完整性认证的过程中,数字签名是有效地技术手段。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。数字签名包括简单数字签名和签名报文摘要。

第四节 身份认证☆

身份认证又称身份鉴别,是一个实体经过计算机网络向另一个实体证明其身份的过程。

第五节 密钥分发中心与证书认证机构☆

一、密钥分发中心

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密钥分发中心 (Key Distribution Center, KDC),并且每一方和 KDC 之间都保持一个长期的共享密钥。

二、证书认证机构

将公钥与特定实体绑定,通常是由认证中心 (Certification Authority, CA) 完成的。CA 具有以下作用。

1) CA 可以证实一个实体的真实身份。2) 一旦 CA 验证了某个实体的身份,CA 会生成一个把其身份和实体的公钥绑定起来的证书,其中包含该实体的公钥及其全局唯一的身份识别信息等,并由 CA 对证书进行数字签名。

第六节 防火墙与入侵检测系统☆☆

一、防火墙的基本概念

防火墙是能够隔离组织内部网络与公共互联网,允许某些分组通过,而阻止其他分组进入或离开内部网络的软件、硬件或者软件硬件结合的一种设施。

二、防火墙分类

防火墙大致可以分为三类: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。

三、入侵检测系统 IDS

入侵检测系统(Intrusion Detection System, IDS)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。

第七节 网络安全协议☆☆

一、安全电子邮件

电子邮件对网络安全的需求:机密性、完整性、身份认证性、抗抵赖性。

安全电子邮件标准是 PGP 标准。

二、安全套接字层 SSL

1、安全套接字层 SSL 是由 NetScape 最先实现,并广泛部署的安全协议,几乎所有的浏览器和 Web 服务器都支持。

2、简化的 SSL 主要包含 4 个部分。

1) 发送方和接收方利用各自证书、私钥认证、鉴别彼此,交换共享密钥。2) 密钥派生或密钥导出。3) 数据传输。4) 连接关闭。

3、SSL 协议栈

| | | |
|----------|------------|----------|
| SSL 握手协议 | SSL 更改密码协议 | SSL 警告协议 |
| SSL 记录协议 | | |
| TCP | | |
| IP | | |

注意:SSL 使用的加密算法:公开密钥加密算法、对称密钥加密算法、MAC 算法。

三、虚拟专网 VPN 和 IP 安全协议 IPSec

1、VPN 简介

VPN 关键技术: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。

隧道协议包括:乘客协议、封装协议、承载协议。

2、IPSec 体系简介

(1) IPSec 两种典型的传输模式:传输模式和隧道模式。

(2) 主要包括封装安全载荷协议(ESP)、认证头(AH)协议、安全关联(SA)、密钥交换与管理(IKE)。

①**安全关联(SA)**:在 SA 建立时需要维护很多参数,主要有以下几个:安全参数索引,序列号,抗重放窗口,生存周期,运行模式,IPSec 隧道源和目的地址。

②**AH 协议和 ESP**:AH、ESP 两种不同协议和两种模式(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。

③IPsec 密钥交换 IKE:

IPSec 进行自动协商建立安全关联和交换密钥的方式就是互联网密钥交换协议 IKE。

IKE 自动管理 SA 的建立、协商、修改和删除,是 IPsec 唯一的密钥管理协议。IKE 包括 3 个主要部分。

1) 互联网安全关联与密钥管理协议。2) 密钥交换协议 OAKLEY。3) 共享和密钥更新技术 SKEME,提供了 IKE 交换密钥的算法。

密训押题

1、数字签名时报文的发送方从报文中生成的 128 位散列值被称为_____。

答案:报文摘要

解析：消息完整性检测的一个重要目的就是要完成报文认证的任务。对报文应用散列函数，得到一个固定长度的散列码，称为报文摘要。

2、简述网络安全的概念及网络安全攻击的常见形式。

答案：网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。

网络主要面临安全威胁有：首先，从报文传输方面，主要包括窃听、插入、假冒、劫持等安全威胁。比较常见的网络攻击还包括拒绝服务 DoS 以及分布式拒绝服务 DDoS 等。其次还包括映射、分组“嗅探”和 IP 欺骗等。

