计算机网络预测

提示：本计算机网络预测由作者 Zenith 根据课堂以及往年题作出的知识点考察的猜想，不保证与最终考试内容一致，同时除了计算题有一定把握外，其他知识点考察方式不一定和标注的一样，可能出现在任何位置，最好的复习方式还是看书，刷王道，刷视频，做题，同时今年由覃老师出题，明确表明不会和前三年出现一样的题，所以前三年的题仅供参考，不建议画几十上百去买题，还不保真。

选择题10*2=20

- 什么是协议

> 协议是控制在对等实体之间进行通信的规则的集合，是水平的，是为了在网络中进行数据交换而建立的规则、标准、约定

- **各个中继设备属于什么层次**

> 集线器(Hub)和交换机(Switch)的确本质区别在于__3__
>
> (1) 集线器属于链路层设备、交换机属于应用层设备 （2）集线器属于链路层设备、交换机属于传输层设备 （3）集线器向所有端口转发帧、交换机仅向特定端口转发帧 （4）交换机向所有端口转发帧、集线器仅向特定端口转发帧
>
> 属于数据链路层设备是（ D ）。
>
> A. router B. hub C. repeater D. switch
>
> （B）属于第三层设备
>
> A.Hub B.Router C.Switch D.Bridge
>
> 在OSI 参考模型中,交换机、集线器、路由器实现的最高功能层分别是（B）
>
> A.2/2/3 B.2/1/3 C.3/1/2 D.3/2/2
>
> 局域网与广域网、广域网与广域网的互联是通过哪 种网络设备实现的?
>
> （ B ） A.集线器 B.路由器 C.交换机 D.传输介质

- **各个协议属于什么层次**

> RIP 路由发现协议属于 OSI 模型的__4__
>
> (1) 链路层 (2)网络层 (3)传输层 (4)应用层
>
> 下列哪个动态路由算法属于外部路由算法?
>
> （ C ）。 A. RIP B. OSPF C. BGP D.IGRP
>
> 在因特网的传输层提供可靠传输服务的协议是__3__
>
> (1) IP协议 （2）HTTP协议 （3）TCP协议（4）UDP协议
>
> 在下列几组协议中，哪一组是网络层协议？ （C ）
>
> A. IP, TCP, RIP B. ARP, IP, UDP C. ICMP, ARP, IP D. FTP, SMTP, BGP
>
> 以下协议或应用不基于UDP的是（A）
>
> A. SMTP B. RIP C. DHCP D.SNMP
>
> 在 Internet 上浏览网页时，浏览器和 WWW 服务器之间传输网页使用的应用层协议是 （B ）。

> A．SMTP B．HTTP C．FTP D. Telnet
>
> 传输层的主要功能是（ B ）。
>
> A.定义物理地址 B.建立端到端连接 C.在终端设备间传送比特流，定义了电压、接口、电缆标准和传输距离等 D.将数据从一个主机传送给另一个主机
>
> 在 TCP / IP 模型中，主机采用（ D ）标识，运行在主机上的进程采用（ ）标 识。
>
> A.端口号，主机地址 B.主机地址，IP 地址 C.IP 地址，主机地址 D.IP 地址，端口号
>
> 下列说法中错误的是（ B ）。
>
> A.IP层可以屏蔽各个物理网络的差异 B.IP层可以代替各个物理网络的数据链路层工作 C.IP层可以隐藏各个物理网络的实现细节 D.IP层可以为用户提供通用的服务
>
> 数据链路层的信息单位是（ B ）。
>
> A．位 B.帧 C.报文 D.分组
>
> 由于帧中继可以使用链路层来实现复用和转接，所 以帧中继网中间节点中只有（ A ）。
>
> A.物理层和链路层 B.链路层和网络层 C.物理层和网络层 D.网络层和运输层

- **应用层协议与端口号**

> 用户在利用客户端邮件应用程序从邮件服务器接收邮件时通常使用的协议是 （ B ）。
>
> A. FTP B. POP3 C. HTTP D. SMTP
>
> 在 Internet 域名体系中，域的下面可以划分子域，各级域名用圆点分开，按 照（A ）。
>
> A．从右到左越来越小的方式分多层排列 B．从右到左越来越小的方式分 4 层排列 C．从左到右越来越小的方式分多层排列 D．从左到右越来越小的方式分 4 层排列
>
> 若用户 1 与用户 2 之间发送和接收电子邮件的过程如下图所示，则图中①、 ②、③阶段分别使用的应用层协议可以是（ D ）
>
> A．SMTP、SMTP、SMTP B．POP3、SMTP、POP3 C．POP3、SMTP、SMTP D．SMTP、SMTP、POP3
>
> 下列不属于应用层协议的是（ B ）。
>
> A.FTP B.TCP C.TELNET D.SMTP

- **ABCD 地址分类**

> 以下哪个 IP 地址永远不会出现在网络上的 IP 分组中？__2__
>
> (1)192.222.1.10 (2)127.0.0.10 (3) 176.2.2.10 (4)224.0.0.10
>
> 188.118.66.88的子网掩码是（B）
>
> A.188.118.0.0 B.255.255.0.0 C.255.255.255.0 D.188.118.66.0
>
> 下列地址中,属于单播地址的是（B）
> A. 10.255.255.255 B. 172.31.128.255/17 C. 192.168.24.59/30 D. 224.105.5.221

- **路由器的主要功能：路由发现，分组转发**

> 路由器最主要的功能为__1__
>
> (1) 路由发现和分组转发 (2) 异种网络互联和网络协议转换 (3) 分组转发 (4) 分组过滤
>
> 路由器最主要的功能为（ A ）。
>
> A.路由发现和分组转发 B.异种网络互联和网络协 议转换 C.分组转发 D.分组过滤
>
> 在路由中的最短路径可以指（ D ）。

> A.最小延迟时间的路径 B.最短距离的路径 C.具有最少跳数的路径 D.以上任一或组合

- MTU IPv4 分片重组
- **动态路由**

  DV 距离矢量 Bellman-Ford RIP 路由信息协议 UDP

  LS 链路状态 Dijkstra OSPF 开放最短路径优先 IP

  BGP 边界网关协议 TCP

> 使用 Dijkstra 算法的路由算法是（ D ）。
>
> A. BGP B. DHCP C. RIP D. OSPF
>
> OSPF属于（A）路由算法
>
> A.Link state（链路状态） B.Distance Vector（距离矢量） C.Broadcost（广播） D.Multicast（组播）
>
> 下列哪个算法不是常用的路由算法（D）
>
> A OSPF B. BGP CRIP D. ARP
>
> 下面哪种路由发现机制采用Disjkstra算法求出最短 路由？ （ D ）
>
> A. AODV B. 选择性扩散 C.距离矢量路由 D.链路状态路由
>
> .某路由表中有转发接口相同的4条路由表项，其目 的网络地址分别为35.230.32.0/21、3.230.40.0/21、 35.230.48.0/21和35.230.56.0/21，将该4条路由聚合后 的目的网络地址为（ C ）。
>
> A.35.230.0.0/19 B.35.230.0.0/20 C.35.230.32.0/19 D.35.230.32.0/20

- **从 IPv4 地址的 IPv6 地址的过渡技术：双协议栈、隧道技术**
- 数据传播速率和传输速率

> 如果在通信信道上发送 100 比特信号所需的时间是 0.1us，那么信道的数据传输速率 为 （C ）。
>
> A. 1Mbps B. 10Mbps C. 1Gbps D. 100Mbps

- **递归和迭代搜索次数**

> 假设所有域名服务器均采用迭代查询方式进行域名解析。当 H4 访问规范域名为www.abc.xyz.com的网站时,域名服务器201.1.1.1在完成该域名解析过程中,可能发出 DNS 查询的最少和最多次数分别是（C）。
>
> A.0，3 B.1，3 C.0，4 D.1，4

- DNS的作用

> DNS的作用包括（D）
>
> A. 实现域名到IP的解析 B. 负载均衡 C. 主机别名 D. 以上都是

- **FTP 21/20 端口号 主动 被动**

> **FTP处理的协议数据单元是（D）**
>
> **A.Frame B.Datagram C.segment D.Message**
>
> > **物理层：处理比特流(Bits)**
> >
> > **数据链路层：处理帧(Frame) → A选项**

> > **网络层：处理数据报(Datagram) → B选项**
> >
> > **传输层：处理段(Segment) → C选项**
> >
> > **应用层：处理消息(Message) → D选项**
>
> FTP 客户和服务器间传递 FTP 命令时，使用的连接是（ A ）。
>
> A．建立在 TCP 之上的控制连接 B．建立在 TCP 之上的数据连接 C．建立在 UDP 之上的控制连接 D．建立在 UDP 之上的数据连接
>
> 下列关于 FTP 协议的叙述中，错误的是（ C ）。
>
> A. 数据连接在每次数据传输完毕后就关闭 B. 控制连接在整个会话期间保持打开状态 C. 服务器与客户端的 TCP20 端口建立数据连接 D. 客户端与服务器的 TCP 21 端口建立控制连接

- **Http 无状态 cookie**

> HTTP是一个无状态协议，然而 Web 站点经常希望能够识别用户，这时需要用到（B）
>
> A. Web 缓存 B. Cookie C. 条件 GET D. 持久连接
>
> HTTP 的会话有四个过程，不包括（ D ）。
>
> A.建立连接 B.发出请求信息 C.发出响应信息 D.传输数据
>
> > 第四个应该是关闭连接

- 分组交换和电路交换

> 因特网是典型的__2__
>
> （1）电路交换网络 (2)分组交换网络 (3)混合网络 (4)都不是
>
> Intnet使用了__3__交换技术
>
> （1）电路 (2)虚电路 (3)分组 (4)数据报

- IP 地址和 MAC 地址区别

> 以下关于MAC的描述中，正确的是（D）
>
> A.TDMA比FDMA吞吐量更高，延迟更小 B.ALOHA不能避免碰撞，CSMA/CD可以完全避免碰撞的发生 C.随机接入MAC协议在高负载下效率更高 D.都不对
>
> IPv4 地址、IPv6 地址、MAC 地址的长度分别为（B）比特
>
> A. 32、128、64 B. 32、128、48 C. 32、64、48 D. 32、64、128
>
> > IPv4 首部 20B
> >
> > IPv6 首部 40B
> >
> > MAC 首尾一共18B 故IP数据报最短为64-18=46B
> >
> > TCP 首部 20B
> >
> > UDP 首部 8B
>
> 下列IP地址中，只能作为IP分组的源IP地址但不能 作为目的IP地址的是（ A ）。
>
> A.0.0.0.0 B.127.0.0.1 C.20.10.10.3 D.255.255.255.255
>
> . 某主机的 IP 地址为 180.80.77.55 ，子网掩码为 255.255.252.0，如该主机向其所在子网发送广播分 组，则目的地可以是（ D）。
>
> A.180.80.76.0 B.180.80.76.255 C.180.80.77.255 D.180.80.79.255
>
> 当一台主机从一个网络移到另一个网络时，以下说 法正确的是（ B ）。

> A.必须改变它的IP 地址和MAC 地址 B.必须改变它的IP 地址，但不需改动MAC 地址 C.必须改变它的MAC 地址，但不需改动IP 地址 D.MAC 地址和IP 地址都不需改动

- **IPv6 零压缩**

> IPv6 地址的长度是__4__
>
> (1) 16 位 （2）32 位 （3）64 位 （4）128 位
>
> IPv6 地址的长度是__2__ 字节
>
> (1) 8 （2）16 （3）32 （4）128

- 最短帧长

> 以太网帧的最小和最大尺寸分别是（ D ）。
>
> A. 46，1500 B. 46，1518 C. 64，1500 D. 64，1518
>
> > A选项为IP数据报的最小最大尺寸，加上18B为以太网帧的最小最大尺寸

- TCP 三次握手和四次握手

> 若主机H1主动发起一个与主机H2的TCP 连接，H1、H2 选择的初始序列号分别为2018 和2022，则第三次握手 TCP 段的确认序列号是（D）
>
> A. 2018 B. 2019 C. 2022 D. 2023
>
> 如果在 TCP 连接中有一方发送了 FIN 分组，并且收到了回复，那么它将（ C ）。
>
> A.不可以发送数据，也不可以接收数据 B.可以发送数据，不可以接收数据 C.不可以发送数据，可以接收数据 D.连接马上断开

- **TCP && UDP**

> 某多媒体应用软件需要实质性地支持组播，该软件的编程基于以下哪个协议最合适？__4__
>
> (1) TCP (2) IP (3) HTTP (4) UDP
>
> 一个 C 程序要单向关闭 TCP 连接，应该使用哪个 API？__2__
>
> (1)close (2) shutdown (3) exit (4)write
>
> 一个 TCP socket 可以由（ D）组合唯一标识。
>
> A. IP 地址，端口号 B. 源 IP 地址，源端口号 C. 目的 IP 地址，目的端口号 D. 源 IP 地址，源端口号，目的 IP 地址，目的端口号
>
> UDP相对于TCP的优点不包括（B）
>
> A.不需要存储连接状态信息 B.可实现全双工传输 C.不对发包速率进行限制 D.较小的首部开销
>
> 接收端收到有差错的UDP用户数据时,传输层的处理方式是（A）
>
> A、丢弃 B、请求重传 C、差错校正 D、忽略差错
>
> 下列哪个应用层协议是用UDP传输的（D）
>
> A. HTTP B. SMTP C. FTP D. DNS
>
> 某多媒体应用软件需要实质性地支持组播，该软件的编程基于（ D ）协议最合 适?
>
> A.TCP B.IP C.HTTP D.UDP
>
> TCP 协议采用滑动窗口协议解决了（ A ）。
>
> A.端到端的流量控制 B.整个网络的拥塞控制 C.端到端的流量控制和网络的拥塞控制 D.整个网络的差错控制

- **CSMA/CD && CSMA/CA**

> 以下哪种介质访问控制机制不能完全避免冲突__4__
>
> (1) 令牌环 (2) TDMA (3) FDDI （4）CSMA/CD
>
> 以下哪种介质访问控制机制不能完全避免冲突？（C）
>
> A. 令牌环 B. TDMA C. ALOHA D.CSMA/CA
>
> 对于基带CSMA/CD而言，为了确保发送站点在传 输时能检测到可能存在的冲突，数据帧的传输时延至 少要等于信号传播时延的（B）。
>
> A.1倍 B.2倍 C.2.5倍 D.4倍

- CRC

> 下面没有使用 Internet Checksum 校验的是(D)
>
> A. TCP B. UDP C. IPv4 D. IPv6
>
> 3.在CRC码计算中，可以将一个二进制位串与一个只 含有0或1两个系数的一元多项式立对应关系。例如， 与位串101101对应的多项式为（B）。
>
> A. x6 +x4 +x3 +1 B. x5 +x3 +x2 +1 C. x5 +x3 +x2 +x D. x6 +x5 +x4 +1
>
> 发送方准备发送的信息位为1101011011，采用CRC 校验算法，生成多项式为，那么发出的校验位应该为 （D）。
>
> A.0110 B.1010 C.1001 D.1110

- C/S && P2P

> 下面有关P2P网络的描述中,不正确的是（C）
>
> A、充分利用网络边缘的资源 B、比C/S结构具有更好的可扩展性 C、仍旧具有单点故障问题 D、拓扑结构往往是动态变化的

- 拥塞控制 慢启动 拥塞避免 快重传 快恢复

> 有一条 TCP 连接，它的最大报文段长度是 2KB，TCP 拥塞窗口为 24KB，这 时候发生了超时事件，那么该拥塞窗口变成了（B）。
>
> A.1KB B.2KB C.5KB D.7KB
>
> 一个 TCP 连接的数据传输阶段，如果发送端的发送窗口值由 2000 变为 3000，意味着发送端可以（C）。
>
> A.在收到一个确认之前可以发送 3000个TCP 报文段 B.在收到一个确认之前可以发送 1000 字节 C.在收到一个确认之前可以发送 3000 字节 D.在收到一个确认之前可以发送 2000个TCP 报文段
>
> 流量控制是为防止（C）所需要的。
>
> A.位错误 B.发送方缓冲区溢出 C.接收方缓冲区溢出 D.接收方与发送方冲突

- SR && GRN

> 数据链路层采用选择重传协议（SR）传输数据，发送方已发送了0~3号数据 帧，已收到1号帧的确认，而0、2号帧依次超时，则此时需要重传的帧数是（B）。
>
> A.1 B.2 C.3 D.4
>
> 假设数据链路层采用后退N帧协议进行流量控制， 发送方已经发送了编号为0~6号的帧。当计时器超时 时，2号帧的确认还没有返回，则发送方需要重发的 帧数是（B）。

> A.1 B.5 C.6 D.7

名词术语辨析题4*5=20

所有回答仅供参考，全部都是由AI生成的，而且我看生成效果一般，如果我们要回答，第一是要将一组术语辨析的词翻译成中文，第二步是分别阐述二者的用途，记得多少写多少，包括但不限于基本实现方式，用于解决什么问题，工作在哪一层，典型特点有哪些，最后是阐述二者的区别与联系，这个看具体问题，有些重点在区别，有些重点在联系。

- 递归查询和迭代查询
- **CSMA/CD && CSMA/CA**

> **CSMA/CD（载波监听多路访问/冲突检测）**
>
> - 用于**有线以太网**（半双工）。
> - **检测冲突**（电压变化）后停止发送，退避重传。
>
> **CSMA/CA（载波监听多路访问/冲突避免）**
>
> - 用于**无线网络**（如 Wi-Fi）。
> - **避免冲突**（RTS/CTS 握手、随机退避），因无线环境难以检测冲突。
>
> **关键区别**：
>
> - **冲突处理**：CD 是“检测后补救”，CA 是“主动避免”。
> - **适用场景**：CD 用于有线，CA 用于无线。
> - **协议标准**：CD → IEEE 802.3（以太网），CA → IEEE 802.11（Wi-Fi）。
>
> **联系**：均基于“先监听再发送”的竞争信道访问机制。

- **Circuit Switching && Packet Switching**

> **电路交换（Circuit Switching）**：通信前需建立一条专用的物理通路，全程独占资源，传输时延低但资源利用率低。
>
> **分组交换（Packet Switching）**：数据被分割为分组，各分组独立传输，共享链路资源，动态分配带宽，资源利用率高但可能引入排队时延。
>
> **异同**：
>
> 1. **连接方式**：电路交换需预先建立连接；分组交换无连接（如IP）或逻辑连接（如TCP）。
> 2. **资源分配**：电路交换独占资源；分组交换统计复用，资源共享。
> 3. **适用场景**：电路交换适合实时性要求高的业务（如传统电话）；分组交换适合突发性数据（如互联网流量）。
> 4. **效率**：电路交换低效（空闲时资源浪费）；分组交换高效但可能拥塞。

- **ARP && NAT &&DNS**

> 1. **ARP（地址解析协议）**
> - **功能**：通过IP地址查询对应的MAC地址
> - **工作范围**：局域网(LAN)内
> - **特点**：二层协议，实现IP→MAC的转换
> 2. **NAT（网络地址转换）**
> - **功能**：将私有IP转换为公有IP
> - **工作范围**：路由器/网关

> - **特点**：解决IPv4短缺，实现多设备共享公网IP
> 3. **DNS（域名系统）**
> - **功能**：将域名解析为IP地址
> - **工作范围**：全球互联网
> - **特点**：分布式数据库，实现域名→IP的转换
>
> **关键区别**：
>
> - **转换类型**：
> - ARP：IP→MAC
> - NAT：私有IP→公有IP
> - DNS：域名→IP
> - **工作层次**：
> - ARP：网络层
> - NAT：网络层
> - DNS：应用层
>
> **联系**：三者共同完成网络通信中的地址转换，确保数据正确路由和传输

- **GBN && SR**

> Go-back-n && Selective Report
>
> 1. **回退N (GBN)**
> - 重传策略：丢失分组及其后所有分组全部重传
> - 接收方式：严格按序接收，丢弃乱序包
> - 特点：实现简单，但效率较低
> 2. **选择重传 (SR)**
> - 重传策略：仅选择性重传丢失分组
> - 接收方式：缓存乱序包，等待缺失包
> - 特点：实现复杂，但效率高
>
> **核心区别**：
>
> - 重传单位：GBN重传一组 vs SR重传单个
> - 接收处理：GBN丢弃乱序包 vs SR缓存乱序包
> - 效率：GBN带宽浪费多 vs SR带宽利用率高
>
> **联系**：
> 都是滑动窗口协议，用于可靠数据传输（ARQ）

- **Slotted ALOHA && Unslotted ALOHA**

> **时隙ALOHA（Slotted ALOHA）**：
> 将时间划分为固定时隙，节点只能在时隙起点发送数据。冲突仅发生在相同时隙内，信道利用率高（较纯ALOHA提升一倍）。
>
> **纯ALOHA（Unslotted ALOHA）**：
> 无时间同步，节点可随时发送数据。冲突窗口为2倍帧传输时间，信道利用率比时隙ALOHA低。
>
> **异同**：
>
> 1. **相同**：均基于随机接入、冲突重传机制；
> 2. **不同**：时隙ALOHA通过时间同步约束发送时机，降低冲突概率，效率更高。

- **CIDR && VLSM**

> **CIDR（无类别域间路由）**
>
> - **作用**：取消传统IP分类（A/B/C类），通过`IP/前缀长度`（如192.168.1.0/24）灵活划分网络，支持路由聚合（超网），减少路由表条目。
>
> **VLSM（可变长子网掩码）**
>
> - **作用**：允许同一网络中使用不同子网掩码，实现层次化子网划分，提高IP地址利用率。
>
> **关系与异同**
>
> - **相同点**：均突破传统IP分类限制，提升地址分配效率。
> - **不同点**：
> - **CIDR**：用于**网络间**的路由聚合（扩大网络范围）。
> - **VLSM**：用于**网络内**的子网划分（缩小主机范围）。

- **IPv4 IPv6 && MAC**

> 简述 IPv4 和 IPv6 的不同。
>
> 1. **IPv4**
>
> - 32位地址，点分十进制表示(如192.168.1.1)
> - 提供逻辑寻址，网络层使用
> - 面临地址耗尽问题
>
> 2. **IPv6**
>
> - 128位地址，冒号分隔十六进制表示(如2001:0db8::1)
> - 解决IPv4地址不足，增强安全性(QoS支持)
> - 与IPv4不兼容，需过渡技术
>
> 3. **MAC地址**
>
> - 48位物理地址，十六进制表示(如00-1A-2B-3C-4D)
> - 数据链路层使用，全球唯一
> - 用于局域网设备识别
>
> **关键区别**：
>
> - 功能：IPv4/IPv6用于网络层路由，MAC用于链路层传输
> - 地址空间：IPv6(128位) >> IPv4(32位)
> - 层次：IPv4/IPv6逻辑地址可变，MAC物理地址固化
>
> **联系**：
>
> - 共同完成数据包传输(IP负责端到端，MAC负责节点间)
> - ARP协议实现IPv4与MAC转换，NDP协议实现IPv6与MAC转换

- **SMTP && POP3**

> **SMTP（简单邮件传输协议）**：用于**发送**电子邮件的应用层协议，负责将邮件从客户端传输到服务器或服务器间转发。
>
> **POP3（邮局协议第3版）**：用于**接收**电子邮件的应用层协议，允许客户端从服务器下载邮件到本地，通常下载后删除服务器上的邮件（默认行为）。
>
> **关系/异同**：

> 1. **功能分工**：SMTP负责**发送**，POP3负责**接收**，二者常协同完成邮件收发。
> 2. **交互方向**：SMTP是“推送”协议（客户端→服务器），POP3是“拉取”协议（服务器→客户端）。
> 3. **存储机制**：POP3默认下载后删除服务器邮件（可配置保留），而SMTP仅中转，不长期存储邮件。
>
> （注：若题目强调对比，可补充与IMAP的区别，但本题仅要求POP3。）

- **SMTP && MIME**

> **SMTP（简单邮件传输协议）**：用于在邮件服务器之间或邮件客户端与服务器之间**发送电子邮件**的**文本协议**，仅支持ASCII编码，无法直接传输二进制数据。
>
> **MIME（多用途互联网邮件扩展）**：SMTP的**扩展协议**，通过添加头部字段将非ASCII数据（如图片、音频）编码为ASCII格式，使SMTP能传输多媒体内容。
>
> **关系**：MIME扩展了SMTP的功能，解决其仅支持ASCII的局限性，二者协同实现现代邮件系统的多样化数据传输。

- **POP3 && IMAP**

> **POP3（邮局协议第3版）** 和 **IMAP（互联网消息访问协议）** 都是用于电子邮件接收的应用层协议，但有以下区别：
>
> 1. **POP3**：
> - 从邮件服务器**下载邮件到本地**，默认删除服务器上的邮件（可配置保留）。
> - **离线访问**为主，仅支持单向同步（本地操作不影响服务器）。
> 2. **IMAP**：
> - 在服务器上**直接管理邮件**，操作（如删除、移动）会实时同步到服务器。
> - 支持**多设备同步访问**，适合需要随时在线处理的场景。
>
> **关键区别**：
>
> - POP3 侧重**本地存储**，IMAP 侧重**云端同步**；
> - IMAP 功能更丰富（如文件夹管理），但占用更多服务器资源。

- OSI && TCP/IP

> **OSI（开放系统互连模型）**：
> 国际标准化组织（ISO）提出的**七层**网络参考模型，理论性强，定义严格，但未实际广泛应用。
>
> **TCP/IP模型**：
> 实际应用的**四层**网络架构（含混合五层说法），源于互联网实践，兼容性强，是当今互联网的基础。
>
> **关系与异同**：
>
> 1. **分层差异**：OSI七层（物理层、数据链路层、网络层、传输层、会话层、表示层、应用层），TCP/IP四层（网络接口层、网际层、传输层、应用层）。
> 2. **用途**：OSI为理论标准；TCP/IP为实践标准，二者存在**层次映射**（如TCP/IP应用层对应OSI上三层）。
> 3. **协议支持**：TCP/IP模型直接绑定协议（如IP、TCP），OSI仅框架，不限定具体协议。
>
> **考试应答关键词**：七层理论模型、四层实践架构、层次映射、协议绑定。

- **C/S && P2P**

> **C/S（Client/Server，客户端/服务器模型）**：
>
> - 网络架构模式，由**客户端**（请求服务）和**服务器**（提供服务）组成，通信方式为集中式，服务器是核心。
> - 特点：服务器性能要求高，扩展性受限，典型应用如Web、FTP。
>
> **P2P（Peer-to-Peer，对等网络）**：
>
> - 网络架构模式，节点（Peer）兼具客户端和服务器功能，通信方式为分布式，无中心节点。
> - 特点：资源分散，扩展性强，典型应用如BitTorrent、区块链。
>
> **异同**：
>
> 1. **中心化 vs 去中心化**：C/S依赖中心服务器，P2P各节点平等。
> 2. **扩展性**：P2P动态加入节点更灵活，C/S受服务器瓶颈限制。
> 3. **可靠性**：P2P单点故障影响小，C/S服务器故障导致服务中断。
>
> （注：考试中若需进一步简化，可保留核心对比，如“C/S集中式，P2P分布式；C/S扩展性差，P2P弹性强”。）

- **Persistent HTTP && Nonpersistent HTTP**

> Persistnt HTTP && Non-persistent HTTP
>
> **Persistent HTTP（持久HTTP，引入流水线）** 和 **Non-persistent HTTP（非持久HTTP）** 是HTTP协议的两种连接方式，主要区别在于TCP连接的复用性：
>
> 1. **Non-persistent HTTP**
> - 每个请求/响应对需单独建立TCP连接，完成后立即关闭。
> - **缺点**：频繁握手（三次握手+四次挥手）导致高延迟和资源浪费。
> 2. **Persistent HTTP**
> - 单个TCP连接可传输多个请求/响应，默认保持连接（需服务器支持）。
> - **优点**：减少握手开销，提升性能（如HTTP/1.1默认持久化）。
>
> **异同**：
>
> - **相同**：均基于HTTP协议，用于客户端-服务器通信。
> - **不同**：持久HTTP复用连接，减少延迟；非持久HTTP每次新建连接，效率低。

- Broadcast && Multicast

> Broadcast && Multicast
>
> **Broadcast（广播）**：
> 向同一网络中的所有主机发送数据，无论其是否需要，接收方不可选择（如ARP协议）。
>
> **Multicast（组播）**：
> 向特定的一组主机（加入同一组播组）发送数据，接收方可选择性加入（如视频会议）。
>
> **异同**：
>
> 1. **范围**：广播针对全网，组播针对特定组。
> 2. **效率**：组播更高效，避免资源浪费；广播可能引发冗余流量。
> 3. **应用**：广播用于本地发现（如DHCP），组播用于多点通信（如IPTV）。

- **暴露终端 && 隐藏终端**

> **暴露终端（Exposed Terminal）**：指在无线网络中，某节点因听到其他节点的传输而避免发送，但实际上其发送不会造成冲突。导致信道资源未被充分利用。
>
> **隐藏终端（Hidden Terminal）**：指在无线网络中，两个互不可听的节点同时向同一接收节点发送数据，导致冲突发生，接收节点无法正确接收。
>
> **关系/异同**：
>
> 1. **相同点**：均因无线网络的信号覆盖范围有限引起，属于MAC层多址访问问题。
> 2. **不同点**：
> - **暴露终端**因“过度监听”而保守（发送被抑制）；**隐藏终端**因“无法监听”而冲突（发送未被抑制）。
> - 暴露终端导致**信道利用率降低**；隐藏终端导致**数据冲突增加**。
> 3. **解决协议**：通常通过RTS/CTS（如802.11）缓解两类问题。
>
> （注：考试作答时需严格简洁，以上内容可分点列出，控制每点在1行内。）

- Congestion Control && Flow Control

> Congestion Control 和 Flow Control
>
> **Congestion Control（拥塞控制）**：
> 防止网络因流量过载而出现性能下降（如丢包、延迟激增），通过全局调节发送速率确保网络稳定性，核心是避免*网络层*的拥塞。
>
> **Flow Control（流量控制）**：
> 解决*接收方处理能力不足*的问题，通过反馈机制（如窗口大小）确保发送速率不超过接收方的缓冲能力，作用于*传输层*的端到端通信。
>
> **异同**：
>
> 1. **目标**：拥塞控制维护网络整体健康；流量控制保护接收方。
> 2. **作用范围**：拥塞控制关注网络路径（多设备）；流量控制仅涉及收发两端。
> 3. **触发信号**：拥塞控制依据丢包/延迟；流量控制依赖接收方的窗口通告。
> 4. **协同性**：TCP等协议中二者共存，如TCP同时使用滑动窗口（流量控制）和拥塞窗口（拥塞控制）。

简答题&计算题5*6=30

- 各层设备

> 在局域网中使用集线器和交换机有什么本质的区 别，试述其工作原理。
>
> > 答案:局域网按介质访问控制方法分为共享介质局域网和交换介质局域网，使用集线器组建的星型结构局域网属于共享介质局域网，物理上是星型结构，逻辑上仍然是总线结构，在使用时，可以把集线器连接的网络看成一个共享式总线，在集线器的内部，各端口之间相互连在一起。所有连接到集线器的计算机设备属于一个冲突域，当连接在集线器中的一个结点发送数据时，它将用广播方式传送到集线器的每个端口。
> >
> > 用交换机组建的局域网属于交换式局域网，在交换式局域网中的核心设备是交换机，交换机有多个端口，每个端口可以连接一台计算机或一个网段，每个端口独占信道的带宽，且每一个端口属于一个冲突域，交换机端口支持半双工和全双工模式，同时交换机具有低交换延迟和支持VLAN服务等优点；交换机通过自学习建立“端口号/MAC地址映射表”，当一个结点向另一个结点发送数据时，交换机根据“端口号/MAC地址映射表”决定接收到的数据帧是否转发，交换机可以隔离本地信息，从而避免了网络上不必要的数据流动，这也是交换机与集线器重要的不同之处。

- **CIDR 和 VLSM 和 ABCD 类地址的选择，并计算利用率**

> 一个网段需要连接最多 6540 台计算机设备，若对其分配有类型的 IP 地址, 问 A、B、C 哪一类地址最合适？若采用可变长子网掩码(或称无类别域间编码)IP 地址，试求出最长子网掩码。在以上两种情况下，地址空间的利用率分别为多大？
>
> > 1. **分类IP地址**：最合适的是**B类地址。**
> > 2. **CIDR下的最长子网掩码**：**255.255.224.0**（或/19）。
> > 3. **地址空间利用率**：
> > - 分类IP（B类）：约9.98%。
> > - CIDR（/19）：约79.85%。
>
> ---
>
> （3）(10 分) 一个网段上需要连接最多 4130 台计算机设备，若对其分配 VLSM(可变长子网掩码)的IP 地址, 问子网掩码最长可达多少? 若分配有类型的 IP 地址, 问 A、B、C 哪一类地址最合适? 这两种方法的地址空间利用率分别有多大？（回答时请给出定量的理由）
>
> > 因 212-2 < 4130 < 213-2，因此子网掩码最长可达（32-13）=19.
> >
> > 使用 B 类地址比较合适。
> >
> > 使用 VLSM：利用率=4130/213-2≈.....
> >
> > 使用有类型方案，利用率=4130/216≈.....
>
> ---
>
> 如图有 A、B、C 三台主机，计算三台主机 A、B、C 所在网络的网络掩码和广播地址 。（6 分）
>
> ---
>
> 某单位分配到一个IP地址块200.108.0.0/16，有6个子网，每个有888台主机，求各个子网的最小和最大掩码长度分别为多少？
>
> > 19、22
>
> ---
>
> 某公司的一个部门有510 台计算机需要上网，并需要连到外网。假设IP地址段为172.16.20.22/20 用CIDR 进行地址配置，要求IP地址利用率最大。在这种情况下，网络掩码是什么，并求出 IP 地址利用率。(提示，接入路由器时也需要IP地址)
>
> > 共需 510+1=511 个，2^9 - 2 = 512 - 2 = 510 （不够），2^{10} - 2 = 1024 - 2 = 1022 （满足）
>
> ---
>
> 一个企业网有8个子网，每个子网上的主机数量相 同，各为1000台。若要求所有的IP地址都有形式 202.100.x.y, 试写出各个子网的IP地址(即NetID)、最 短子网掩码长度，并简要说明计算方法。
>
> > 答案：根据子网大小,每个子网至少需要10位主机号; 由于有8个子网, 因此需要至少3位扩展网络号部分, 因此每个子网掩码最短需要19位, 剩余13位（>10位）作为主机号。由此，8个子网的IP地址分别是：
> >
> > 202.100.0.0/19
> >
> > 202.100.32.0/19
> >
> > 202.100.64.0/19

> > 202.100.96.0/19
> > 202.100.128.0/19
> > 202.100.160.0/19
> > 202.100.192.0/19
> > 202.100.224.0/19
>
> ---
>
> 一个网络最多有709台计算机设备： （1）若对其分配VLSM(可变长子网掩码的)IP地址, 问子网掩码最长可达多少? （2）若分配有类型的IP地址, 问A、B、C哪一类最合 适? 简要说明理由。 （3）就对（1）和（2）给出的答案，分别计算地址 空间的使用效率，即实际使用的IP地址数量与可用IP 地址数量之比（%）。
>
> > 答案：
> > （1）设主机号部分长度为k位，由2k-1-2<709<2K-2得K=10，即子网掩码长度22位。
> > （2）B类地址空间最接近709，故B类地址最合适。
> > （3）使用22位子网掩码的效率=709/（210-2）=70%；
> > 使用B类地址的效率=709/（216-2）=1%。

- HTTP

> 简述 http 持久性（流水线/非流水线）和非持久性连接（串行/并行）的过 程，并简单计算他们的传输页面的总时间（假定该页面包含一个 HTML 基本文件 和 10 个 JPEG 图片）
>
> ---
>
> 描述 Web 缓存的作用和意义。
>
> > 1. **作用**：
> > （1）**减少访问延迟**：缓存就近提供资源，加快响应速度。
> > （2）**降低带宽消耗**：避免重复传输相同数据，节省网络流量。
> > （3）**减轻服务器压力**：减少对源服务器的请求，提高其处理能力。
> > 2. **意义**：
> > （1）**提升用户体验**：缩短网页加载时间，增强流畅性。
> > （2）**优化网络性能**：缓解网络拥塞，提高整体效率。
> > （3）**节约成本**：减少服务器负载和带宽使用，降低运营开销。
>
> **核心**：通过存储副本实现高效资源复用，提升系统性能。

- FTP

> 为什么说FTP是带外传送控制信息?
>
> > 答案：FTP 使用两个TCP 连接。控制连接在整个会话期间一直保持打开， FTP 客户发出的传送请求通过控制连接发送给服务器端的控制进程，但控制连接不用来传送文件。实际用于传输文件的是“数据连接”。服务器端的控制进程在接收到FTP 客户发送来的文件传输请求后就创建“数据传送进程”和“数据连接”，用来连接客户端和服务器端的数据传送进程。数据传送进程实际完成文件的传送，在传送完毕后关闭“数据传送连接”并结束运行。

- **MTU IPv4 分片重组**

> 阐述 IPv4 分段原因；并计算：一数据报（IP 层）数据部分为 3800 字节，要在 MTU 为 1500 字节的网络上传输，假设数据报中首部长度为 20 字节，问分几段？每段的数据部分长度为多少字节？

> 注意：偏移量（×8 字节），要是8的整数倍

IP数据报长3900字节，MTU1400字节（1）分片：几片？每片length长？offset？MF？（2）如不分片，路由器怎么处理

> IP首部20字节，1400-20=1380 取 1376，每片长1376+20=1396，offset是偏移量（×8 字节），MF=1 表示还有更多的分片
>
> 丢弃，向源主机汇报

某个路由器收到一个数据帧，帧中 UDP用户数据报的数据字段为8192B，下一跳要使用 以太网来传送。假定IP头中无可选项,DF字段为0。试问应当划分为几个IP 数据报片? 说明每个 IP 数据报片的数据字段长度和片段偏移字段的值。（提示：要考虑控制首部的长度）

> 注意：UDP首部8B，8+8192=8200作为IP数据报的数据部分

假定以太网的MTU=1500，分组（头+载荷）为 2500字节，网络层固定首部长度为20字节，问在网络 层需要分为几段？请写出每段的数据长度、及其 offset的值。

> 答案：需要分2段。
>
> 数据长度 offset
>
> 第一段 1480 0
>
> 第二段 1000 185

- **CRC 计算**

> x^4+x^2+1 接收到了 111011001，请问对不对
>
> ---
>
> IP数据报首部的检验和是否有对data检验，有什么优缺点？
>
> > IP：仅检验首部
> >
> > TCP：TCP伪首部+首部+数据
> >
> > UDP：UDP伪首部+首部+数据（可选）
>
> ---
>
> 在数据传输过程中,若接收方收到的二进制比特序列为10110011010,收发双方采用的生成多项式为$G(x)=x^4+x^3+1$，则该二进制比特序列在传输中是否出错？如果未出现差错，那么发送数据的比特序列和CRC 检验码的比特序列分别是什么？
>
> ---
>
> 要发送的数据为1101011011。采用CRC 的生成多 项式P(x)=x4 +x+1。试求应添加在数据后面的余数。 数据在传输过程中最后一个1变成了0，问接收端能否 发现？若数据在传输过程中最后两个1都变成了0，问 接收端能否发现？
>
> > 答案：添加的检验序列为1110（11010110110000除以10011）数据在传输过程中最后一个1变成了0,11010110101110除以10011，余数为011，不为0，接收端可以发现差错。数据在传输过程中最后两个1都变成0，11010110001110除以10011，余数为101，不为0，接收端可以发现差错。

- NAT 的功能、ARP的功能、DNS的功能

说明 ARP 协议的主要功能，并简述其工作过程.

> ARP 协议的主要功能是将 32 位 IP 地址转换为 48 位物理地址。 工作过程：首先每台主机都会在缓冲区建立一个 ARP 列表，以表示 IP 与 MAC 的 对应关系。当有数据包发送时，会先检查 ARP 列表中是否存在该 IP 对应的 MAC 地址， 如果有，则直接将包发送到这个 MAC 地址，如果没有，就向本地网段发起一个 ARP 请求的广播包，网络中所有主机收到这个 ARP 包后，会先检查自己的 IP 是否与包中的 IP 地址一致，如果不一致则忽略，如果一致，则将发送端的 MAC 地址和 IP 地址添加 到自己的 ARP 列表中（已存在的则覆盖），然后向发送端发送一个响应包，发送方收到 该响应包后将接收方的 IP 与 MAC 添加到自己的 ARP 列表中。然后开始数据的传输。

假设主机 A 使用的是固定 IP，没有任何缓存的情况下，访问 www.google.com。 描述该过程中， DNS、ARP、HTTP 这些网络协议分别是在哪一步使用的（要求排列出 使用的顺序），作用是什么（9 分）

> 在主机 A 访问 **www.google.com** 的过程中，网络协议的使用顺序及作用如下：首先，**DNS** 协议用于解析域名，将 **www.google.com** 转换为对应的 **IP 地址**（若本地无缓存，则递归查询根DNS、TLD DNS 和权威DNS）；接着，若目标 IP 不在同一子网，主机 A 使用 **ARP** 协议获取默认网关的 **MAC 地址**（若 ARP 缓存无记录，则广播 ARP 请求并等待响应）；然后，主机 A 通过 **HTTP** 协议（基于 TCP）与目标服务器建立 **TCP 连接**（三次握手），并发送 HTTP 请求获取网页内容。整个过程依次依赖 **DNS（域名→IP）→ ARP（IP→MAC）→ HTTP（获取数据）**，确保正确寻址和可靠传输。

解释 DHCP、NAT、IPv6 是如何解决 IPv4 地址枯竭问题的，IPv4 向IPv6过渡，一般采用哪两种技术?

> DHCP：动态主机配置协议，通过动态分配IP地址，提高IPv4地址的利用率。
>
> NAT：网络地址转换，允许多个设备共享一个公网IPv4地址，显著减少公网地址需求。
>
> IPv6：根本解决方案：提供128位地址空间（约3.4×10^{38}个地址），彻底解决地址枯竭问题。
>
> 双协议栈、隧道技术

域名系统的主要功能是什么？域名系统中的本地域名服务器、根域名服务器、 顶级域名服务器以及权限域名权服务器有何区别?

> 答案:域名系统的主要功能：将域名解析为主机能识别的IP 地址。
>
> 因特网上的域名服务器系统也是按照域名的层次来安排的。每一个域名服务器都只对域名体系中的一部分进行管辖。共有三种不同类型的域名服务器。即本地域名服务器、根域名服务器、授权域名服务器。当一个本地域名服务器不能立即回答某个主机的查询时，该本地域名服务器就以DNS 客户的身份向某一个根域名服务器查询。若根域名服务器有被查询主机的信息，就发送DNS 回答报文给本地域名服务器，然后本地域名服务器再回答发起查询的主机。但当根域名服务器没有被查询的主机的信息时，它一定知道某个保存有被查询的主机名字映射的授权域名服务器的IP 地址。通常根域名服务器用来管辖顶级域。根域名服务器并不直接对顶级域下面所属的所有的域名进行转换，但它一定能够找到下面的所有二级域名的域名服务器。每一个主机都必须在授权域名服务器处注册登记。通常，一个主机的授权域名服务器就是它的主机ISP 的一个域名服务器。授权域名服务器总是能够将其管辖的主机名转换为该主机的IP 地址。因特网允许各个单位根据本单位的具体情况将

> > 本域名划分为若干个域名服务器管辖区。一般就在各管辖区中设置相应的授权域名服务器。

- **拥塞控制 慢启动 拥塞避免 快重传 快恢复**

> 设TCP 的ssthresh的初始值为8(单位为报文段)。当拥塞窗口上升到12时网络 发生了超时，TCP 使用慢开始和拥塞避免。试分别求出第1 次到第15 次传输的 各拥塞窗口大小。
>
> > 答案：拥塞窗口大小分别为：1，2，4，8，9，10，11，12，1，2，4，6，7，8，9
>
> ---
>
> 有一个 TCP 连接，当它的拥塞窗口大小为 64个分组大小时超时，假设该线 路往返时间RTT是3s，不考虑其他开销，即分组不丢失，该TCP 连接在超时后 处于慢开始阶段的时间是多少秒？
>
> > 答案：当超时时，慢开始门限值 ssthresh 变为拥塞窗口大小的一半即 ssthresh = 64 / 2 = 32 个分组。此后，拥塞窗口重置为 1，重新启用慢开始算法。根据慢开始算法的指数增长规律，经过 5 个 RTT，拥塞窗口大小变为 25 = 32，达到 ssthresh。此后便改用拥塞避免算法。因此，该TCP 连接在超时后重新处于慢开始阶段的时间是 5RTT = 15s
>
> ---
>
> . 如下图所示为一个 TCP 主机中的拥塞窗口的变化过程，这里最大数据段长 度为 1024 字节，请回答如下问题： （1）该 TCP 协议的初始阀值是多少？为什么？ （2）本次传输是否有发生超时？如果有是在哪一次传输超时？ （3）在 14 次传输的时候阀值为多少？ （4）在本例中，采用了什么拥塞控制算法？
>
> > 答案：
> >
> > （1）该 TCP 协议的初始阀值为 16KB。可以看出来在拥塞窗口到达 16KB 之前指数增长，之后就呈线性增长了，说明初始阀值是 16KB。线性增长时拥塞窗口大小每次增加 1KB，同时说明最大数据段长度为 1KB。
> >
> > （2）可以看到拥塞窗口在第 13 次传输后变为 1KB，说明这次发送发生超时。
> >
> > （3）因为可以看到在之后的传输中，拥塞窗口到达 12KB 之后呈线性增长。说明在 14 次传输的时候拥塞窗口变为了 12KB。
> >
> > （4）因为可以看到在发送失败后拥塞窗口马上变为了 1KB，而且阀值也变为了之前的一半。在拥塞窗口未达到阈值且发送成功时，拥塞窗口将加倍，由此看出采用的是慢启动算法。

- TCP && UDP

> TCP 和 UDP 协议有哪些本质区别？
>
> > TCP 是面向连接的可靠的数据传输协议，进行拥塞控制和流量控制，不支持广播和组播。UDP 是无连接的，不可靠的数据传输协议，不支持流量控制和拥塞控制，支持广播 和组播。（典型用例：视频点播）
>
> ---
>
> 可靠数据传输机制有哪些，分别解决了什么问题？
>
> > 1. **确认应答（ACK）**
> >
> > **解决问题**：检测数据是否成功到达接收方。
> >
> > **方式**：接收方发送ACK确认，发送方超时未收到则重传。
> >
> > 2. **超时重传（Timeout & Retransmission）**

> **解决问题**：数据包丢失或ACK丢失。
>
> **方式**：发送方设定计时器，超时后重传未确认的数据。
>
> 3. **序号（Sequence Numbers）**
>
> **解决问题**：数据包乱序或重复。
>
> **方式**：为每个数据包编号，接收方按序号重组。
>
> 4. **滑动窗口（Sliding Window）**
>
> **解决问题**：提高传输效率（流量控制）和拥塞控制。
>
> **方式**：允许发送方连续发送多个未确认的数据包，窗口大小动态调整。
>
> 5. **选择重传（Selective Repeat, SR）**
>
> **解决问题**：单个数据包丢失导致全部重传（GBN的缺陷）。
>
> **方式**：仅重传丢失的包，接收方缓存乱序数据。
>
> 6. **否定确认（NAK）**
>
> **解决问题**：快速发现丢失的数据包（如TCP的快速重传）。
>
> **方式**：接收方显式通知发送方缺失的包序号。
>
> 7. **校验和（Checksum）**
>
> **解决问题**：检测数据在传输中的比特错误。
>
> **方式**：发送方计算校验和，接收方验证。

为什么 HTTP、FTP、SMTP、POP3 都运行在 TCP 而不是 UDP 之上?

> 答案：因为与这些协议相联系的应用都要求应用数据能够被无差错的有序的接收。TCP提供这种服务，而UDP不提供。TCP提供可靠的数据传输服务，而UDP提供的是不可靠数据传输。

对于 2.7 节所描述的运行在 TCP 之上的客户-服务器程序，服务器应用程序 为什么必须先于客户程序运行？ 对于运行在 UDP 之上的程序，客户程序是否可 以先于服务器程序运行？ 为什么?

> 在 TCP 协议中，服务器必须先运行以建立监听（`listen`）状态，等待客户端发起连接（`connect`），否则客户端会因为找不到目标而失败；而 UDP 是无连接的，客户端可以直接发送数据报，即使服务器未运行，数据也能发出（但可能丢失或无法被接收）。

TCP和UDP协议有哪些本质区别?

> 答案:TCP是面向连接的可靠的数据传输协议，进行拥塞控制和流量控制，不支持广播和组播。UDP是无连接的，不可靠的数据传输协议，不支持流量控制和拥塞控制，支持广播和组播。（典型用例：视频点播）

TCP 在进行流量控制时是以分组的丢失作为产生拥塞的标志。有没有不是因 拥塞而引起的分组丢失的情况？如有，请举出三种情况。

> 答案：当IP数据报在传输过程中需要分片，但其中的一个数据报未能及时到达终点，而终点组装IP 数据报已超时，因而只能丢失该数据报；IP 数据报已经到达终点，但终点的缓存没有足够的空间存放此数据报；数据报在转发过程中经过一个局域网的网桥，但网桥在转发该数据报的帧没有足够的差错空间而只好丢弃。

- **OSI TCP/IP 模型结构 对应关系、差异**

> 从下到上列举 OSI 7 层模型，并概要说明每层的主要功能。
>
> > 物理层：该层包括物理连网媒介，是计算机连网的基础。
> >
> > 数据链路层：点对点，在不可靠的物理线路上进行可靠的数据传递
> >
> > 网络层：实际完成主机到主机的通信服务。（IP、ARP、RARP、ICMP+各种选路协 议）
> >
> > 传输层：端到端，在终端用户之间提供透明的数据传输。（TCP、UDP）
> >
> > 会话层：负责在网络中的两节点之间建立和维持通信
> >
> > 表示层：为不同终端的上层用户提供数据和信息的格式化方法。（例如加密解密）
> >
> > 应用层：负责对软件提供接口以使程序能够使用网络服务（注意不是运行的那些应 用程序，而是提供的接口或者服务）
>
> ---
>
> 自上而下写出 TCP/IP 的 5 层参考模型,在上述过程中，各指出一个用到 TCP 和 UDP 的地方。（7 分）
>
> ---
>
> 自上而下写出 TCP/IP 的 5 层参考模型的名称和功能
>
> > 应用层：负责对软件提供接口以使程序能够使用网络服务（注意不是运行的那些应 用程序，而是提供的接口或者服务）
> >
> > 传输层：端到端，在终端用户之间提供透明的数据传输。（TCP、UDP）
> >
> > 网络层：实际完成主机到主机的通信服务。（IP、ARP、RARP、ICMP+各种选路协 议）
> >
> > 数据链路层：点对点，在不可靠的物理线路上进行可靠的数据传递
> >
> > 物理层：该层包括物理连网媒介，是计算机连网的基础。
>
> ---
>
> 从上到下写出 TCP/IP 协议栈，指出协议栈与7层参考模型的层次对应关系
>
> > 应用层：负责对软件提供接口以使程序能够使用网络服务（注意不是运行的那些应 用程序，而是提供的接口或者服务）-->会话层、表示层、应用层
> >
> > 传输层：端到端，在终端用户之间提供透明的数据传输。（TCP、UDP）--> 传输层
> >
> > 网络层：实际完成主机到主机的通信服务。（IP、ARP、RARP、ICMP+各种选路协 议）--> 网络层
> >
> > 数据链路层：点对点，在不可靠的物理线路上进行可靠的数据传递 --> 数据链路层
> >
> > 物理层：该层包括物理连网媒介，是计算机连网的基础。--> 物理层
>
> ---
>
> 从下到上列举OSI 7层模型和TCP/IP 5层模型， DHCP工作在哪一层?
>
> > 答案：
> >
> > 物理、数据链路、网络、传输、会话、表示、应用
> >
> > 物理、数据链路、网络、传输、应用

> > DHCP 属于应用层

- IP 地址和 MAC 地址区别

> .网页地址、MAC地址和IP地址有什么本质区别，分 别工作在哪一层?
>
> > 答案:
> >
> > 网页地址是URL，代表网站的地址，工作在应用层
> >
> > MAC地址代表局域网内网络设备的硬件地址，工作在数据链路层
> >
> > IP地址是Internet上一台主机的地址，工作在网络层

- **TCP 三次握手和四次握手**

> 画出在访问 www.google.com 时，TCP 连接建立的过程，假设双方的初始序列号都 为 2020，需要写出必要的序号、标志位等（6 分）
>
> ---
>
> 根据下表填写对应的序号和确认号

- **ABCD 地址分类**

> (1) (5 分) 共以下 IP 地址分别属 A、B、C、D 哪一类?
>
> > 110.210.45.3 A
> >
> > 112.0.3.23 A
> >
> > 204.30.71.34 C
> >
> > 224.9.8.29 D
> >
> > 172.10.0.9 B
>
> （2）(5 分)分别写出 5、10、14、18、23 位子网掩码的点分十进制形式。
>
> > 248.0.0.0
> >
> > 255.192.0.0
> >
> > 255.252.0.0
> >
> > 255.255.192.0
> >
> > 255.255.254.0
>
> （3）(10 分) 一个网段上需要连接最多 4130 台计算机设备，若对其分配 VLSM(可变长 子网掩码的)IP 地址, 问子网掩码最长可达多少? 若分配有类型的 IP 地址, 问 A、B、C 哪一类地址最合适? 这两种方法的地址空间利用率分别有多大? （回答时请给出定量的理由）
>
> > 因 212-2 < 4130 < 213-2，因此子网掩码最长可达（32-13）=19.
> >
> > 使用 B 类地址比较合适。
> >
> > 使用 VLSM：利用率=4130/213-2≈.....
> >
> > 使用有类型方案，利用率=4130/216≈.....
>
> ---
>
> 简述 A 类和 D 类 IP 地址的特点及作用，并解释 IP 地址 127.0.0.1
>
> > A 类：大规模网络。
> >
> > D 类：组播通信。

> > 127.0.0.1：本机回环测试。

- **最短帧长 CSMA/CD 协议的 2t 由来分析**

> 简述 CSMA/CD 工作过程，为什么会有最小帧长的限制，并描述如何计算。
>
> > 最小帧长的限制是为了确保站点能在帧发送完毕前检测到冲突
>
> ---
>
> 10BASE-T的以太网，信号传播速率是$2*10^8$m/s，两节点距离4km，求最短以太网帧。
>
> > 10BASE-T 的传输速率为 **10 Mbps**（10×10^6 bit/s）。最短帧长=2*距离/信号传播速率*传输速率=50 字节，以太网标准规定 **最小帧长为 64 字节**，因此需取两者中的较大值（即 64 字节）。
>
> ---
>
> 一个使用 CSMA/CD 介质访问协议的局域网，其带宽为1Gbps，最远两个站点的距离为8km，信号在电缆中的速度为200,000km/s，理论上数据帧的最小长度为多少？无线网络中的**隐藏站点**问题是什么，是用什么介质访问协议解决的。
>
> > 问题：可能会发生冲突同时还无法检测冲突，降低网络吞吐量，增加数据重传。介质访问协议：CSMA/CA 载波侦听多路访问/冲突避免
>
> ---
>
> 假定1km长的CSMA/CD网络的数据率为1Gbit/s。 设信号在网络上的传播速率为200000km/s。求能够使 用此协议的最短帧长。
>
> > 答案：对于1km电缆，单程端到端传播时延为：τ=1÷200000=5×10-6s=5μs，端到端往返时延为：2τ=10μs为了能按照CSMA/CD工作，最小帧的发送时延不能小于10μs，以1Gb/s速率工作，10μs可发送的比特数等于：10×10-6×1×109=10000bit=1250字节。
>
> 简述 CSMA/CD 工作过程，为什么会有最小帧长的限制，并描述如何计算。
>
> > 最小帧长的限制是为了确保站点能在帧发送完毕前检测到冲突
>
> ---
>
> 说明局域网的介质访问控制协议的主要目的，并概述 CSMA/CD 协议的工作过程。
>
> > 介质访问控制协议的目的是：提供寻址及媒体存取的控制方式，为了协同局域网上 的所有计算机发送帧的行为，有效避免帧冲突的发生，提高共享信道的利用率。 CSMA/CD（载波侦听多路访问/冲突检测）在发送帧的同时对信道进行侦听，以确 定是否发生冲突，若在发送数据过程中检测到了冲突，则发送阻塞信息，并立即停止发 送数据，然后等待随机时间再次发送

综合题2*15=30

- **TCP 建立连接和传输数据的过程**

> (1)(10分)以下是一个TCP建立连接和传输数据的过程, 假设每次接收方都全部接受所到达的数据, 请正确填写括号中的数字(不要求写计算过程)。
>
> > 注意SYN和FIN在等于一时都占有一位序号
>
> (2)（2 分）在时刻 TA 和 TB 之后，A 还能继续向 B 传输数据吗？为什么？B 还能继续向 A 传输数据吗？为什么？

> 答案：A可以向B传，但是B不能向A传，因为只有B单方面断开了连接而TCP连接时全双工的。

（3）（8 分）以下是 TCP 的成批传输实例，假设接收方每次接受全部到达的数据，请正确填写括号中的数字(不要求写计算过程)。

主机A与主机B基于一个TCP连接进行通信。主机B已经成功接收序列号(Seq)为800 的字节。假设主机 A以pipelining 的方式连续向主机B发送两个报文段(segments)。这两个报文段分别包含1420和1380个字节,默认发送方计时器为80秒。在第一个报文段 中,源端口号为3017,目的端口号为80。请画图完成如下步骤:

(1)对应的应用层协议是什么?

(2)如果第二个报文段丢失,此时发送方是否会重传该数据包,发送方计时器是否会发生 变化,请给出序列号:

(3)当服务器接收到第二个数据包后,进行确认同时传送1320字节的数据包，然后，决定关闭连接：给出序列号、确认号、相应的状态位:

(4)执行(3)后,发送方还有500字节数据要发送,此时还能发送吗？请说明原因。

.以下是一个TCP建立连接和传输数据的过程。 （1）假设每次接收方都全部接受所到达的数据,请正确填写括号中的数字(不要 求写计算过程)。

（2）在时刻TA和TB之后，A还能继续向B传输数据吗？为什么？B还能继续向A 传输数据吗？为什么？

> 答案：A可以向B传，但是B不能向A传，因为只有B单方面断开了连接而TCP连接时全双工的。

- **静态路由表的构建**

(1)(5 分)一个网络见下图, 其中 lan1, lan2 等是接口的名字, 请写出路由器 R2 的路由表。 注：对直接相连的网络,表项中的“下一跳 IP 地址”请用 C 标记； 不要求写默认路由项。

(2)(5 分)以下是某个路由器上的路由表:

一个目标地址是202.38.70.129的IP分组经此路由器转发后, 其下一站的IP地址是多少?请定量说明理由。

最长匹配原则

(3)(5 分)请根据第(2)小题的路由表，画出该路由器与其邻居路由器的连接关系, 并在图 上标出通过每个邻居路由器可到达的目标网络和 RIP 距离。

(4)(5 分)如果第(2)小题的路由表是:

一个目标地址是202.38.70.129的IP分组经此路由器转发后, 其下一站的IP地址是多少? 请定量说明理由；并请进一步回答：第(2)和第(4)小题中哪一个路由表是正确的？为什么？

> 要求路由表将掩码较长的排在前面，这样一旦找到匹配的记录则为最长匹配。

某个单位的网点由4个子网组成，结构如下图所示,其中主机 H1、H2、 H3 和H4的IP地址和子网掩码见下表。

（1）请写出路由器 R1到4个子网的路由表(假设用 RIP 生成)。直连情况下,下一跳IP 地址用C代替。(6分)

> RI的路由表: 目标IP地址 子网掩码 下一跳的IP地址 RIP-距离
>
> 注意RIP等于距离加一，也就是说直接连接的网络RIP=1

（2）试描述主机 H1 发送一个IP 数据报到主机 H2的两个过程：①物理地址解析过程: ②H1 发出、路由器转发、H2 收到的数据帧的 源、目的IP地址,源、目的 MAC地址。 (指出是哪个接口的MAC地址即可)。(9分)

一个网络见下图, 写出各路由器上的路由表。 注：lan1,lan2等是接口的名字；对直接相连的网络,表 项中的“下一跳IP地址”请用C标记；不要求写默认路 由项。

> 目标IP地址 子网掩码 下一跳的IP地址 RIP-距离 离出接口的名字

附

各个协议属于的层次

物理层：

数据链路层：ALOHA、CSMA

网络层：IP、NAT、ARP、ICMP、OSPF(IP)、IGMP

传输层：TCP、UDP、RDT

应用层：DHCP(UDP)、DNS(UDP/TCP)、FTP(TCP)、SMTP(TCP)、POP3(TCP)、MIME、IMAP(TCP)、HTTP(TCP/UDP)、RIP(UDP)、BGP(TCP)

AI修正后的协议分层：

物理层：

- 以太网物理层（如100BASE-T）

数据链路层：

- ALOHA
- CSMA/CD
- CSMA/CA
- PPP
- VLAN（IEEE 802.1Q）
- 802.11（Wi-Fi）

网络层：

- IP（IPv4/IPv6）
- NAT
- ARP（属于网络层，但工作在链路层和网络层之间）
- ICMP
- OSPF
- IGMP（Internet Group Management Protocol，互联网组管理协议，用于管理 IP 组播（Multicast） 的组成员关系）

传输层：

- TCP

- UDP
- RDT（可靠数据传输协议，通常是理论模型）

应用层：

- DHCP（基于UDP 67/68）
- DNS（基于UDP/TCP 53）
- FTP（基于TCP 20/21）
- HTTP（基于TCP 80，HTTP/3基于QUIC、UDP 443）
- HTTPS（HTTP over TLS，基于TCP 443）
- SMTP（基于TCP 25）
- POP3（基于TCP 110）
- IMAP（基于TCP 143）
- MIME（是SMTP的扩展，属于应用层格式）
- SNMP（Simple Network Management Protocol，简单网络管理协议，基于UDP 161/162）
- Telnet（基于TCP）
- RIP（基于UDP）
- BGP（基于TCP）