1. 性能指标：

   速率（数据传输速率、比特率）

   带宽（最高数据传输率）

   时延（发送时延/传输时延、传播时延、处理时延---存储转发、排队时延）

   吞吐量（单位时间数据量）

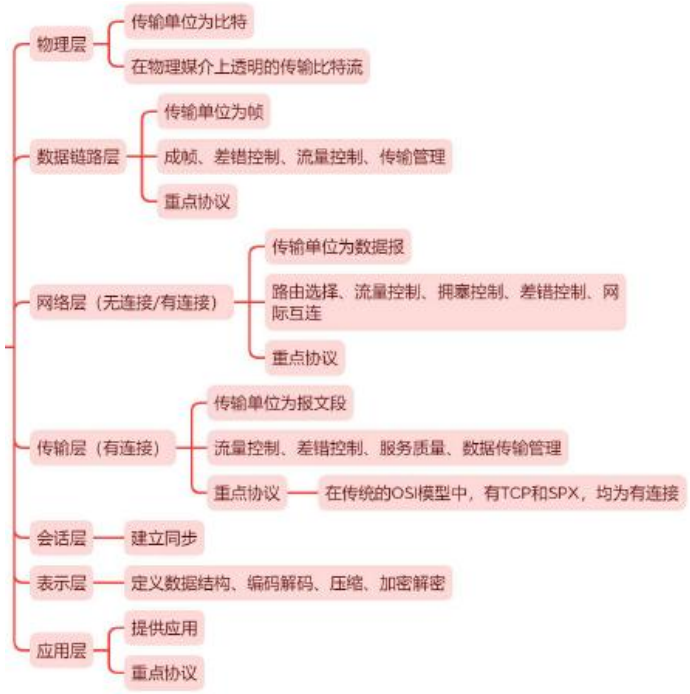
   信道利用率（并非越高越好，信道利用率增大会引起的时延也就迅速增加）

   时延带宽积（传播时延*信道带宽）

   往返时延 RTT

$$1Tb/s = 10^3Gb/s = 10^6Mb/s = 10^9Kb/s = 10^{12}b/s$$

2. 参考模型：协议 接口 服务
3. 服务分为：面向连接和无连接、可靠和不可靠、**有应答和无应答**
4. ISO/OSI：物理层、数据链路层、网络层、传输层、会话层、表示层、应用层



5. TCP/IP：**网络接口层**（物理层、数据链路层）、**网际层**、传输层、应用层
6. 计算机网络的组成

   （1）组成部分：硬件、软件、协议

   （2）工作方式：边缘部分、核心部分

   （3）功能组成：通信子网（传输介质、通信设备）、资源子网（资源共享的设备和软件）
7. 计算机网络的功能：数据通信、资源共享、分布式处理、提高可靠性、负载均衡

8. **报文交换** 方式（存储转发）用在早起电报网络、电子邮件通信，计算机网络采用 **分组交换** 方式（存储转发、流水线方式），而传统电话网络则采用 **电路交换** 方式（建立连接、通信、释放连接）。
9. 计算机网络分类
   （1）分布范围：广域网（WAN）、城域网（MAN）、局域网（LAN）、个人区域网（PAN）
   （2）传输技术：广播式网络、点对点网络
   （3）拓扑结构：总线型、星形、环形、网状
   （4）按使用者：公用网、专用网
   （5）传输介质：有线、无线
10. 协议的组成：语法 语义 同步
11. TCP/IP 协议栈

    TCP/IP协议栈
    - 应用层：HTTP、FTP、SMTP、POP3、DNS等
    - 传输层：TCP、UDP
    - 网络层：ARP、IP、ICMP、IGMP
    - 数据链路层和网络层：以太网、PPP、帧中继、X.25

12. OSI 7 层
    （1）物理层——解决用何种信号来表示比特 0 和 1 的问题
    （2）数据链路层——解决数据包在一个网络或一段链路上传输的问题
    （封装成帧、差错控制、流量控制、透明传输）
    （3）网络层——解决数据包在多个网络之间传输和路由问题
    （4）传输层（端到端）——解决进程之间基于网络的通信问题
    （5）会话层——允许不同主机上的各个进程之间进行会话
    （6）表示层——使不同表示方法的数据和信息之间能互相交流
    （7）应用层——通过应用进程的交互来实现特定网络应用的问题
13. ISO/OSI 参考模型在网络层支持无连接和面向连接的通信（CLNP、X.25 PLP），但在传输层仅支持面向连接的通信（TP0-TP4）；TCP/IP 模型在网络层仅支持无连接的通信（IP），但在传输层支持无连接和面向连接的通信（TCP、UDP）
14. 数据链路层将有差错的物理线路变成无差错的数据链路，实现相邻结点之间即**点到点**的数据传输

1. 信号分类

   （1）传输信号形式：模拟信道（传输模拟信号）、数字信道（传输数字信号）

   （2）传输介质：无线信道、有线信道

2. 通信的交互方式：**单向通信、半双工通信、全双工通信**

3. 奈奎斯特定理（无噪声）：极限传输速率 2W 波特，低通道极限传输速率= $2W\log_2 V$

   （W 为频率带宽-Hz，V 为码元离散电平数）

4. 香农定律（有噪声）：极限传输速率 = $W\log_2$（1+**S/N**），信噪比 = $10\log_{10}$（**S/N**）

   （W 为频率带宽-Hz，S/N 为信号和噪声平均功率之比）

5. 数据转换为模拟信号 **调制**

   数据转换为数字信号 **编码**

6. 带通调制：调频 AM、调幅 FM、调相 PM、正交振幅调制 QAM

7. 标准以太网：曼彻斯特编码（上升 0 下降 1）

   宽带高速网：差分曼彻斯特编码（跳变 0 不变 1）

8. 数据传输速率 $R = B\log_2$（N）（B 为波特率，N 为码元离散个数）

9. 码元速率 = 码元传输速率 = 调制速率

10. 传输介质：**导向传输介质**（铜线、光纤）、**非导向传输介质**（自由介质---水、空气）

11. 无线传输（电磁波在非导向介质）：无线电波、微波、红外线和激光

12. 传输介质接口性质：**机械特性**（接口）、**电气特性**（电压等）、

    功能特性（电平意义）、**过程特性**（功能的出现顺序）

13. 物理层设备：**中继器**（整形、放大、转发信号）、**集线器**

14. **基带**传输（不调制直接传输）、**频带**传输（调制后传输）、**宽带**传输 （调制后划分信道）

15. 一个码元可携带多个比特的信息量（4 进制码元：00 01 10 11）

16. 编码方式：不归零编码 NRZ（高 1 低 0）、归零编码、反向非归零编码、

    曼彻斯特编码、差分曼彻斯特编码

17. 标准编号

    （1）无线局域网 IEEE 802.11

    （2）以太网 IEEE 802.3

1. 数据链路层基本问题：封装成帧（封装 IP 数据包）、透明传输（边界转义）、差错检验
2. 数据链路层使用的主要信道：点对点信道（PPP 协议）

   广播信道（有线局域网：CSMA/CD、无线局域网：CSMA/CA）
3. 实现组帧：**字符计数法**（**帧首部**加字节计数字段，加自己）

   字节填充法（转义）

   零比特填充法（五个连续 1 后加 0）

   违规编码法（如曼彻斯特没采用的高-高电平界定）
4. 差错控制：自动请求重传 ARQ（重发）、向前纠错 FEC（发现差错并纠正）
5. 差错控制分为**检错编码**和**纠错编码**（海明码）
6. 常见的检错编码：奇偶检验码 循环冗余码
7. 三种 ARQ 协议：停止-等待协议（S-W）---**0，1 编号确认**，发送 1，接收 1

   后退 N 帧协议（GBN）---**累计确认**，发送<2^n-1，接收 1

   选择重传协议（SR）---**逐一确认**，发送+接收<=2^n（发送/接收<2^{n-1}）
8. （1）停止-等待信道利用率：$U=T_D/T_D+RTT+T_A$

   （1）连续 ARQ 信道利用率（n 为发送窗口大小）：$U=nT_D/T_D+RTT+T_A$
9. 介质访问控制方法：信道划分（静态）、随机访问、轮询访问（令牌传递协议）
10. 信道划分介质访问控制：频分复用 FDM（划分频带）、时分复用 TDM、

    波分复用 WDM（光的频分复用）、码分复用 CDM
11. 随机访问介质访问控制：ALOHA、CSMA、CSMA/CD、CSMA/CA
12. CSMA 协议：1-坚持、非坚持、p-坚持
13. CSMA/CD 协议

    （1）争用期：2t（2 倍端到端传播时延）

    （2）最短帧长=争用期*数据传输速率

    （3）以太网规定 51.2us 为争用期长度，计算出**以太网最小帧长 64B**

    （4）截断二进制指数退避算法：重传次数最大是 10*争用期，从[0 到 2^k-1]*争用期取

    （5）最长以太网数据帧：1518B
14. CSMA/CA 协议

    （1）IFS 帧间间隔：SIFS（分隔对话）、PIFS、DIFS（发送时要等待的时间）

    （2）虚拟载波监听机制：通知其他站占用时间

    （3）处理隐蔽站：RTS（预约）和 CTS（允许）

15. 以太网帧格式（18 字节）：

（1）头 6 目的地址+6 源地址+2 类型（协议）+ 4FCS

中间 46-1500 数据

尾部 4FCS

（交付物理层要插入 7 前同步码和 1 开始帧定界符）

（2）插入 VLAN 标签：802.1Q 帧（首部类型前+4 字节 VLAN 标签）

（3）以太网 MAC 协议无连接（逻辑）不可靠（无重传等）

16. 局域网 IEEE 802.11

（1）帧三种类型：数据帧 控制帧 管理帧

（2）帧首部 30 字节 尾部 4 字节 FCS

17. PPP 点对点协议

（1）异步传输（字符独立传输）用字节填充法，同步传输（连续比特流）用零比特填充法

(2) PPP 不是总线型，所以没有最短帧长度的限制，信息段可占 0-1500 而不是 46-1500

（3）PPP 提供有连接的不可靠服务（不用确认机制）

（4）PPP 协议三个组成：一个将 IP 数据报封装到串行链路的方法、链路控制协议 LCP、网络控制协议 NCP

(5) PPP 是面向字节的，所有 PPP 帧长度都是整数字节

18. 网桥和交换机在数据链路层，以太网交换机本质是多端口网桥

19. **数据链路**是除了**物理线路**，还必须有**通信协议**控制这些数据的传输，把实现这些协议的硬件和软件加到连路上，就构成了数据链路，现在最常用的方法是使用**适配器（网卡）**来实现这些协议的硬件和软件

20. 采用循环冗余校验只能做到**无比特差错**，并不是**无传输差错**（可靠传输），如果想要达到可靠传输必须加上**确认和重传机制**

21. 数据链路层的两个子层：逻辑链路控制 LLC子层、媒体接入控制 MAC子层

22. 以太网属于随机接入共享信道的方式

23. 数据链路层交换机、网桥隔离冲突域，网络层路由器隔离广播域

24. 交换机工作在全双工方式

25. 以太网交换机交换方式：存储转发方式、直通方式

26. 无线局域网：以太网、令牌网、DFFI

1. 网络层提供主机到主机的通信服务
2. 路由器的功能：**路由选择**和**分组转发**
3. 网络层提供的服务：面向连接的虚电路服务（顺序到达、虚电路号 VCID）

   无连接的数据包服务
4. IPv4 首部

   （1）IP 数据包首部长度 20B-60B（字段*4B），总长度最大 2^{16}-1B（字段*1B）

   （2）标志位 MF=1 后面有分片（More Fragment） DF=0 允许分片（Don't Fragment）

   （3）片偏移以 8B 为单位，说明除了最后一个分片外长度都是 **8B 整数倍**
5. 最大传输单元 MTU：以太网为 1500B
6. IP 地址由网络号和主机号两部分组成

   （1）主机号全 0 为网络本身，全 1 为网络广播地址

   （2）0.0.0.0 表示网络上本主机，255.255.255.255 表示整个网络广播地址

   （3）A 类地址网络号为 127 的是环回自检地址
7. A、B、C 类网络默认子网掩码为 255.0.0.0.0　255.255.0.0.0　255.255.255.0
8. 无分类编址 CIDR，路由聚合（超网），最长前缀匹配
9. 地址解析协议 ARP

   （1）IP 地址与 MAC 地址映射(从网络层使用的 IP 地址，解析出数据链路层使用的硬件地址)

   （2）每一个主机都有一个 ARP高速缓存，里面有所有**局域网**上的各主机和路由器的 IP 地址到硬件地址的映射表

   （3）没有缓存发送 ARP 请求分组（响应分组），路由器不转发 ARP 请求
10. NAT 路由器工作在传输层（要查看和更改端口号）
11. 网际控制报文协议 ICMP（Internet control）

    （1）两种报文：**ICMP 差错报告**报文 **ICMP 询问报文**

    （2）差错报告类型 终点不可达 源点抑制（拥塞）时间超时（TTL 为 0）

    参数问题 改变路由（重定向）

    （3）ICMP 询问报文：ping 命令（网络层）
12. 网际组管理协议 IGMP（Internet group）
13. IPv6 地址长度 128 位，IPv4 地址长度 32（8+8+8+8）位

    （地址是指源地址目的地址字段）

14. （1）IPv6 首部固定 40B

（2）IPv6 目的地址三种类型：单播、多播、任播（一组计算机中的最近一个）

（3）IPv4 向 IPv6 过渡策略：双协议栈、隧道技术（6 封装成 4）

15. 路由选择协议：内部网关协议 IGP（一个自治系统内，有 RIP 和 OSPF）

外部网关协议 EGP（不同自治系统，有 BGP-4）

16. 距离-向量路由算法最常见：RIP 算法（应用层协议，**用 UDP**）

（1）测试相邻节点->定期传播状态（向相邻路由器）

（2）最多包含 15 个路由器，16 不可达

17. 开放最短路径优先 OSPF 协议（网络层，**用 IP**）

（1）泛洪法（向自治系统内所有路由器发送）

（2）只有当链路状态发生变化时，路由器才用洪泛法向所有路由器发送这个信息

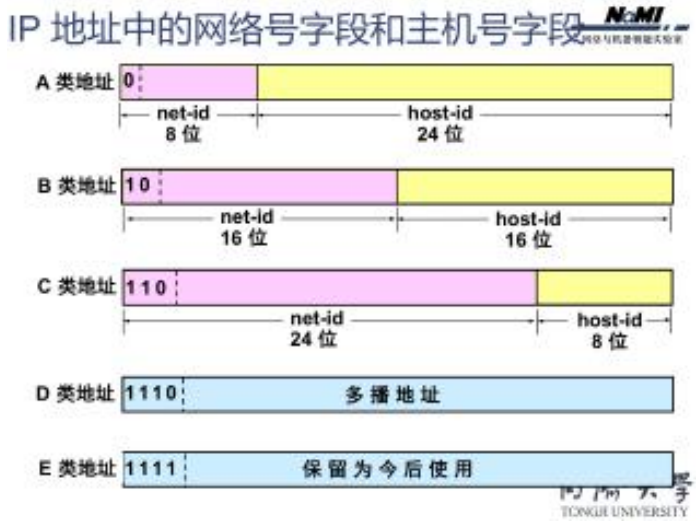
（3）使用了 Dijkstra 算法，采用了分布式的链路状态协议

18. 边界网关协议 BGP

（1）应用层，基于 TCP

（2）四种报文：打开、更新、保活、通知

19. IPv4 多播地址：224.0.0.0 ~ 239.255.255.255（1110-1111）



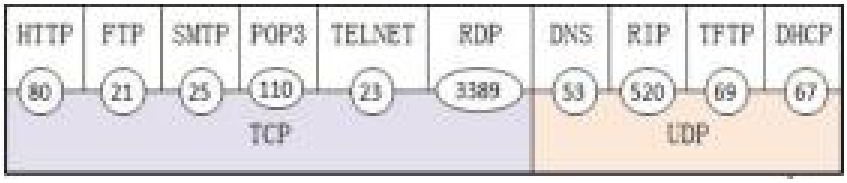
三类地址怎么区分，看前四个字节的十进制：

A类：1-126

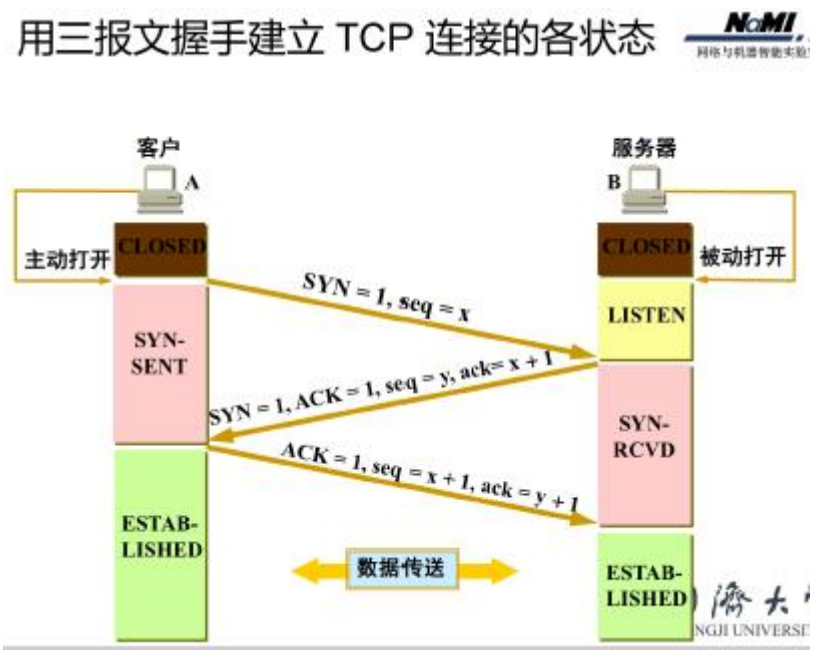
B类：128-191

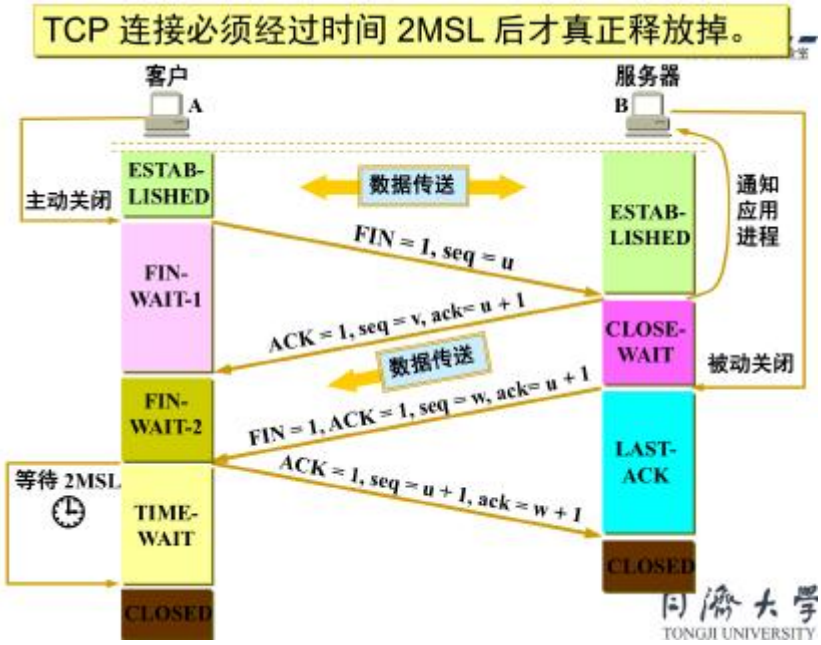
C类：192-223

1. 传输层提供端到端服务，功能之一：复用（发送方不同进程）和分用（接收方端口）
2. 检错：TCP 要求重发，UDP 直接丢弃
3. 端口号 16 位，熟知端口号（0-1023）、短暂端口号（**49152**-65535）2 的 16-14



4. 传输控制协议 UDP
   （1）首部 8B，每个字段 2B（源端口、目的端口、长度、检验和）
   （2）总长度最小 8B（只有首部）
   （3）UDP 无连接，不需要确认，面向报文
   （4）伪首部作用仅仅是为了计算检验和
5. 用户数据报协议 TCP
   （1）面向连接可靠
   （2）全双工，有发送和接受缓存
   （3）面向字节流
   （4）首部最短 20B，最长为 60B，总长度为 4B 倍
   （5）紧急位 URG，确认位 ACK，同步位 SYN，终止位 FIN
   （6）采用累计确认
6. 三次握手四次挥手





MSL：最长报文段寿命

客户机最短释放连接时间：1RTT+2MSL

服务器最短释放连接时间：1.5RTT

7. TCP **流量控制**和**拥塞控制**

（1）滑动窗口实现流量控制

（2）**拥塞控制**算法：**慢开始、拥塞避免、快重传、快恢复**

（3）发送窗口=min{接收窗口 rwnd，拥塞窗口 cwnd}

（4）慢开始门限 ssthresh，cwnd 增大到门限切换到拥塞避免算法

（5）快重传：发送方收到三个冗余 ACK（一共发送 4 个）后，立即重传

（6）快恢复：发生快重传后，ssthresh 和 cwnd 都调整为 cwnd 的一半，开始拥塞避免算法

8. 加权平均往返时间 RTTs

$$新的RTT_S = (1-\alpha) \times (旧的RTT_S) + \alpha \times (新的RTT样本)$$

$$RFC\ 2988推荐的\alpha值为\frac{1}{8}, 即0.125$$

超时重传时间 RTO

$$RTO应该略大于上面的RTT_S，\ RFC2988\ 建议使用下式计算RTO:$$

$$RTO = RTT_S + 4 \times RTT_D$$

1. DNS：域名——>IP 地址 ARP：IP 地址——>**48 位 MAC 地址**
2. C/S（客户/服务器）模型和 P2P 模型
3. （1）本地域名服务器向根域名服务器查询——迭代查询

   （2）主机向本地域名服务器查询——递归查询
4. 域名服务器类型:

   （1）**根域名**服务器：最高层次的域名服务器，管理顶级域，通常不会直接把域名解析成 IP 地址，而是告诉本地域名服务器下一步去哪一个顶级域名服务器查询，返回顶级域名服务器 IP 地址

   （2）**顶级域名**服务器：管理在该域名服务器注册的所有二级域名，当收到 DNS 请求使可以直接给出最后的结果， 也可以告诉下一步去哪查询

   （3）**权限域名**服务器：每台主机都必须在权限域名服务器上登记，可以直接将其管辖的主机名转换成为该主机的 IP 地址

   （4）**本地域名**服务器：当一个主机发出 DNS 查询请求时，该请求报文就要发送给本地域名服务器，本地域名服务器的 IP 地址需要直接配置在需要域名解析的主机中
5. HTTP

   （1）HTTP 本身也是无连接的，虽然它使用了面向连接的 TCP 向上提供的服务

   （2）HTTP1.0 协议是非持续连接的，HTTP/1.1 协议使用持续连接（分为流水和非流水）

   （3）HTTP 有两类报文：**请求报文**和**响应报文**

   （4）Cookie 识别码，首次访问产生，后续相应报文发送

   （5）HTTP 面向文本，报文字段都是 ASCLL 码
6. FTP

   （1）C/S 模式

   （2）建立**控制连接（21）**和**数据连接（20）**
7. SMTP 通信的三个阶段：连接建立、邮件传送、连接释放
8. （1）发送邮件的协议：SMTP（TCP 连接） Simple Mail trans Pro

   （2）读取邮件的协议：POP3（TCP 连接）和 IMAP

参考题目以及背诵

1. 无线局域网的标准编号是 **IEEE 802.11**，其架构有两种模式，它们分别是 **有固定基础设置的无线局域网** 和**无固定基础设施的移动自组织网**。

   有固定基础设置的无线局域网（基础结构模式，Infrastructure Mode）

   此模式依赖固定的基础网络设施构建无线环境。接入点（AP，Access Point ）是核心组件，它如同桥梁，一边连接有线网络，一边向周围发射无线信号 。无线终端（像手机、笔记本电脑等 ）需关联到 AP，借由 AP 接入有线网络，实现与其他终端或互联网的通信。比如在家庭中，无线路由器就是典型的 AP，手机连 WiFi 上网，就是通过无线路由器接入家庭有线网络，进而访问互联网，这种模式能提供稳定、大范围的无线覆盖，适合家庭、企业办公等场景 。

   无固定基础设施的移动自组织网（自组织模式，Ad - Hoc Mode）

   该模式无需预先部署固定接入点，由一组具备无线通信功能的终端设备自行组成网络。这些设备之间直接通信，相互作为对方的通信节点，构建临时的网络拓扑 。在野外作业、临时会议等无现成网络设施的场景中十分实用，比如几个携带无线网卡的笔记本电脑，可直接相互连接传输文件、共享资源，无需依赖 AP 或有线网络支持，不过其覆盖范围受终端设备无线信号传输距离限制，且网络性能会随终端移动、拓扑变化而受影响 。

2. IP 地址按目标节点数量多少可以分成 **单播** 地址、**组播** 地址和 **广播** 地址等三类，请各举三类地址实例 **192.168.1.1（单播）**、**224.0.0.1（组播）** 和 **192.168.1.255（广播）**
3. 传真机半双工
4. 非对称加密中，发送方用**接收方的公钥加密**数据，接收方用自己的**私钥解密**。
   数字签名中，发送方用**私钥加密**，接收方用**发送方的公钥解密**
5. 网桥隔离冲突域，两端网段的节点同时发送数据不会发生碰撞
6. 直接连接的设备必须使用相同的波特率（速率一致），否则无法正确解码信号
7.

   1. 调制解调器的传输机制（ACD）

   - **A. 可以接收数据**（正确）
   - **B. 不可以接收数据**（错误，调制解调器是双向通信设备）
   - **C. 可以发送数据**（正确）
   - **D. 使用载波作为传输信号**（正确，调制解调器通过载波调制解调数字信号）

4. 有效的以太网物理地址（AC）

- 以太网MAC地址格式：**6组十六进制数（48位）**，如 `XX:XX:XX:XX:XX:XX`
  - **A. 58:4e:3d:45:12:49**（正确）
  - **C. FF:FF:FF:FF:FF:FF**（广播地址，有效）
  - B. 34:4f:16:28:76（5组，错误）
  - D. 202.23.45.127（IP地址，错误）
  - E. 192.168.11.66（IP地址，错误）

7. 直接封装在物理帧中的协议（C）

- **C. ARP**（直接封装在以太网帧中）
- A. ICMP（封装在IP数据报中）
- B. IP（网络层协议，封装在帧中但不是直接）
- D. SNMP（应用层协议，封装在UDP/TCP）

11. IP路由器描述（AB）

- **A. 静态路由需要建立路由表**（正确）
- **B. 路由器能连接不同网络（如以太网和令牌网）**（正确）
- C. 动态路由也需要路由表（错误）

D 选项，路由器网卡一般工作在普通模式，交换机用于监听多端口数据时可能用混杂模式

12. 以太网机制（AB）

- **A. 帧头部需存放接收节点MAC地址**（正确）
- **B. 数据信号广播到所有节点**（正确，CSMA/CD机制）
- C. 网段距离有限制（如100米双绞线）
- D. 冲突时立即停止发送（CSMA/CD要求）

14. 广域网技术（AD）

- **A. ADSL**（广域网接入技术）
- **D. X.25**（早期广域网协议）
- B. 以太网（局域网技术）
- C. ARPANET（早期互联网，非技术标准）

（背诵）简述CSMA/CD的发送机制：（先听后发、边听边发、冲突停发、随机重发）

（1）适配其从网络层获得一个分组，封装成以太网帧，放入适配器的缓存，准备发送

（2）如果适配器侦听到信道空闲，那么它开始发送该帧。如果适配器侦听到信道忙，那么它持续侦听知道信道上没有信号能量，然后开始发送该帧

（3）在发送过程中，适配器持续检测信道。若一直未检测到碰撞，则顺利地把这个帧发送完毕。若检测到碰撞，则中止数据的发送，并发送一个拥塞信号，以让所有用户都知道

（4）在中止发送之后，适配器就执行指数退避算法，等待一段随机的时间后返回步骤2

（背诵）为什么无线局域网不适用CSMA/CD：

（1）接收信号的强度往往会远小于发送信号的强度，且在无线介质上信号强度的动态变化范围很大，因此若要实现碰撞检测，则在硬件上的花费会过大

（2）在无线通信中，并非所有的站点都能听见对方，即存在“隐蔽站”问题

无线局域网的发送机制是什么，请简要描述：

CSMA/CA（碰撞避免而不是碰撞检测）

（1）若站点最初有数据要发送时，且检测到信道空闲，在等到DIFS后，就发送整个数据帧.在发送数据帧之前，先广播一个短请求发送RTS控制帧，若信道空闲，则目标站广播一个允许发送CTS帧，为发送站预约了信道，一方面允许发送站发送数据，一方面指示其他站点不要在预约期间发送数据。

（2）否则，站点执行CSMA/CA退避算法，选取一个随机回退值，一旦检测到信道忙，退避计时器就保持不变，只要信道空闲，退避计时器就进行倒计时

（3）当退避计时器减到0时，这是信道一定是空闲的，站点就发送整个数据帧（同1）并等待确认

（4）发送站若收到确认，就指导已发送的数据帧被目的站正确接收，若要继续发送第二帧，则从（2）开始；若没有在规定时间内收到确认帧ACK(由重传计时器控制), 就必须重传该帧，再次使用CSMA/CA争用信道，直到收到确认为止，或者经过若干次失败后放弃发送

请分别描述TCP和UDP提供的通信服务类型

- **UDP（用户数据报协议）**
  - **无连接服务**：UDP 是一种无连接的协议，发送数据前不需要建立连接。
  - **不可靠传输**：UDP 不保证消息的可靠性，即不确认数据是否成功送达。
  - **快速、低延迟**：由于不需要建立连接且不进行重传和排序，UDP 传输速度快，适用于对速度要求高而对可靠性要求较低的场景，如视频流、在线游戏等。
  - **传输效率高**：由于无需维持连接状态，UDP 消耗的网络资源较少。
- **TCP（传输控制协议）**

- **面向连接服务**：TCP 在传输数据之前需要建立连接（三次握手），确保双方准备好进行通信。
- **可靠传输**：TCP 提供可靠的传输服务，确保数据包按序到达且无丢失，若发生丢包情况，TCP 会进行重传。
- **流量控制**：TCP 通过滑动窗口机制进行流量控制，确保发送方不会超出接收方的处理能力。
- **拥塞控制**：TCP 具有拥塞控制功能，避免因网络过载而导致的数据传输问题。
- **适用于可靠性要求高的应用**：如文件传输、电子邮件等。

按照 OSI 模型规范，UDP 传输服务能否担当任 OSI 模型中的传输层协议？为什么？

不能，因为OSI模型中的传输层仅提供面向连接的可靠传输

在 TCP 连接中，如何判断网络中发生的堵塞，请描述处理过程。（答案？）

- **拥塞的判断**：
  - **丢包检测**：TCP 通过超时重传和重复确认检测数据包丢失，这通常是网络拥塞的标志。
  - **RTT 增加**：通过监测往返时间（RTT）的增加来判断网络拥塞。
- **处理过程**：
  - 当 TCP 连接开始时，使用慢启动算法逐步指数式增加拥塞窗口的大小，当大小达到初始设置的慢开始门限（阈值）时，则进入拥塞避免阶段，拥塞窗口每次增加1.
  - 无论是在慢启动阶段还是拥塞避免阶段检测到拥塞，那么阈值变为当前拥塞窗口的一般，拥塞窗口则重新设置为1，重新进入慢启动阶段。
  - **若采用的是快速重传和快速恢复算法**：当收到三个重复确认时，TCP 立即重传丢失的数据包，同样将阈值变为发生拥塞时窗口的一半，并直接进入拥塞避免阶段，也就是拥塞窗口重新设置为阈值，并每个传输轮次加1。

1. 基于 Dijkstra 的最短路由算法步骤

输入：带权无向图 $G = (V, E)$，起点 s。
输出：起点到所有其他节点的最短路径及距离。

1. **初始化**：
   - 设置距离表 $dist$，其中 $dist[s] = 0$，其他节点 $dist[v] = \infty$。
   - 设置优先队列（最小堆）Q，包含所有节点，按 $dist$ 排序。
   - 设置前驱表 $prev$，记录路径。
2. **迭代更新**：
   - **While** Q 非空：
     - 从 Q 中取出 $dist$ 最小的节点 u。
     - **For each** 与 u 相邻的节点 v：
       - 计算新距离 $alt = dist[u] + w(u, v)$（w 为边权值）。
       - **If** $alt < dist[v]$：
         - 更新 $dist[v] = alt$，$prev[v] = u$。
         - 调整 Q 中 v 的优先级。
3. **生成路由表**：
   - 对每个目标节点 t，通过 $prev$ 回溯路径，记录下一跳节点。

1. 以太网两种常用介质是**双绞线**和**光纤**（早期还有同轴电缆）
2. 无线网络四种分类（按 IEEE 802.11 等标准，常见分类 ）是 WLAN（无线局域网 ）、WPAN（无线个人局域网 ）、WMAN（无线城域网 ）、WWAN（无线广域网 ） 。
3. 客户机/服务器通信：客户机：主动发起请求的一方，服务器：被动响应请求的一方
4. 通常发送者使用自己的**私钥**进行加密，接收者使用发送者的**公钥**进行解密

1. 发送方与接收方滑动窗口原理

核心目标：在不可靠网络上实现可靠、高效的数据传输（如TCP协议）。

（1）发送方滑动窗口

- **窗口定义**：发送方可连续发送的未确认数据段范围（由接收方窗口大小和网络拥塞情况决定）。
- **关键机制**：
  - **大数据量处理**：窗口内允许批量发送多个数据段（如窗口大小=4，可连续发送段1~4）。
  - **丢包重传**：若某段（如段2）超时未收到ACK，触发**选择性重传（SACK）**或**回退N步（GBN）**。
  - **乱序处理**：接收方缓存乱序到达的段（如先收到段3后收到段2），发送方仅重传缺失段。

（2）接收方滑动窗口

- **窗口定义**：接收方可接收的数据段范围（受缓冲区大小限制）。
- **关键机制**：
  - **累积确认**：返回最高连续正确接收的ACK（如收到段1、2、4，返回ACK=2）。
  - **乱序缓存**：暂存乱序段（如段4），待缺失段（段3）到达后一并提交给应用层。
  - **窗口通告**：通过ACK报文动态通知发送方可接收的窗口剩余大小（流量控制）。

2. 实例说明

场景：发送方窗口大小=4，发送段1~4，接收方窗口大小=4。

- **正常情况**：
  - 发送方发出段1~4 → 接收方全部收到，返回ACK=4 → 发送方窗口滑动到段5~8。
- **丢包与乱序**：
  - 发送段1~4，但段2丢失，段3、4先到达。
  - 接收方：
    - 缓存段3、4（乱序），返回ACK=1（因段2缺失）。
    - 发送方收到ACK=1，重传段2。
    - 接收方收到段2后，提交段2~4，返回ACK=4。
- **窗口动态调整**：
  - 若接收方缓冲区不足，通告窗口缩小为2 → 发送方仅发送段5~6。

HTTP请求发送流程（主机192.168.1.12首次访问 http://192.168.0.33/company/login.html）

---

1. 关键步骤时序

1. **DNS解析**（若域名非IP，需先解析，此处跳过）。
2. **ARP查询**：获取目标IP（192.168.0.33）的MAC地址。
3. **TCP三次握手**：建立HTTP连接的传输层通道。
4. **HTTP请求发送**：传输实际请求数据。

---

2. 数据包结构详解

（1）ARP请求（广播）

以太网帧头：

- **目标MAC**：`FF:FF:FF:FF:FF:FF`（广播）
- **源MAC**：192.168.1.12的MAC（如`00:1A:2B:3C:4D:5E`）
- **类型**：`0x0806`（ARP协议）

ARP报文：

- 操作码：`1`（请求）
- 发送方IP/MAC：192.168.1.12 / `00:1A:2B:3C:4D:5E`
- 目标方IP：192.168.0.33，目标MAC：`00:00:00:00:00:00`（未知）

（2）ARP响应（单播）

以太网帧头：

- **目标MAC**：`00:1A:2B:3C:4D:5E`（192.168.1.12）
- **源MAC**：192.168.0.33的MAC（如`00:6E:7F:8A:9B:0C`）
- **类型**：`0x0806`

ARP报文：

- 操作码：`2`（响应）
- 发送方IP/MAC：192.168.0.33 / `00:6E:7F:8A:9B:0C`

(3) TCP三次握手（SYN）

以太网帧头：

- 目标MAC：`00:6E:7F:8A:9B:0C`
- 源MAC：`00:1A:2B:3C:4D:5E`
- 类型：`0x0800`（IPv4）

IP头部：

- 版本：`4`，首部长度：`20字节`
- TTL：`64`，协议：`6`（TCP）
- 源IP：`192.168.1.12`，目标IP：`192.168.0.33`

TCP头部：

- 源端口：随机高位端口（如`54321`）
- 目标端口：`80`（HTTP）
- 标志位：`SYN=1`，序列号：随机值（如`1000`）

(4) HTTP请求（GET）

TCP数据段（在握手完成后）：

- 标志位：`ACK=1, PSH=1`（推送数据）
- 载荷：HTTP请求报文：

```http
GET /company/login.html HTTP/1.1
Host: 192.168.0.33
User-Agent: [客户端信息]
```

1. 每个 TCP 连接由四元组唯一标识：**(源 IP，源端口，目的 IP，目的端口)**
2. 在无线通信网络链路中，面临**隐蔽站**和**难以进行故障检测**两个基本问题，通过 RTS 和 CTS 机制来解决。
3. 计算机局域网拓扑结构主要分为：**星型**，环型和**总线型**等三类
4. 连接组网的网络设备主要有：接入设备（如网卡），**交换机**和**网桥**等

4. TCP/IP用于同一主机进程间通信

答案：正确

- **解析**：通过**回环地址（127.0.0.1）**和不同端口号，TCP/IP可实现本地进程间通信（如数据库客户端连接服务端）。

6. TCP初始序列号固定

答案：错误

- **解析**：初始序列号（ISN）是动态生成的（基于时钟和随机数），防止预测攻击。

用户进程主要使用 UDP 或 TCP 而不能直接使用 IP 数据包，原因如下：

1. **功能分层角度**：TCP/IP 体系结构中，IP 层主要负责网络间数据包的路由和转发，提供无连接、不可靠的网络层服务，缺乏对应用层进程的直接标识和通信管理能力；而 TCP 和 UDP 工作在传输层，TCP 提供可靠、面向连接服务，UDP 提供无连接、尽最大努力交付服务，能为应用层进程提供端口号标识，区分同一主机上不同应用进程，实现端到端通信。
2. **可靠性保障角度**：IP 数据包本身无法处理数据的可靠传输（如重传、流量控制、拥塞控制等），TCP 借助确认、重传机制等保障可靠性，UDP 虽不可靠但可由应用层按需实现部分可靠性逻辑；若直接用 IP，应用进程需自行处理这些复杂机制，增加开发难度和系统负担。
3. **进程通信角度**：网络通信最终是进程间的通信，IP 地址标识主机，端口号标识主机上的进程，TCP 和 UDP 通过端口号为应用进程提供通信端点，IP 数据包无端口号字段，无法直接关联到具体应用进程，所以用户进程需依托传输层的 TCP 或 UDP 来实现与其他进程的通信。

综上，用户进程需通过 TCP 或 UDP 间接使用 IP 数据包进行网络通信，不能直接使用。