1.负责互联网协议开发、标准制定、地址分配的国际组织名称及其主要职责

(1) 地址支持组织（ASO）负责IP地址系统的管理。

(2) 域名支持组织（DNSO）负责互联网上的域名系统（DNS）的管理。

(3) 协议支持组织（PSO）负责涉及Internet协议的唯一参数的分配。此协议是允许计算机在因特网上相互交换信息，管理通讯的技术标准。

2.报文交换、分组交换和电路交换的特点

电路交换：整个报文的比特流连续地从源点直达终点，好像条物理的线路直接将源点和终点连接起来一样。

报文交换：整个报文先传送到相邻结点，全部存储下来后查找转发表，转发到下一个结点。

分组交换：单个分组 (这只是整个报文的部分)传送到相邻结点，存储下来后查找转发表，转发到下一个结点。注意，分组交换结点的输出接口和输入接口能够并行工作，当输出端口在发送一个分组时，其输入端口可以同时接收下一个分组。

3.在OSI、TCP/IP模型中，每个层次的名称、顺序、功能、服务类型、通信模式、寻址方式是什么？各层的网络互连设备、协议数据单元的名称，以及协议数据单元的最大最小值。网络节点和主机节点各实现了哪些层次。

物理层（Physical Layer）：

功能： 在物理媒体上传输比特流。

服务类型： 无。

通信模式： 单工、半双工、全双工。

寻址方式： 无。

网络互连设备： 中继器（Repeater）。

协议数据单元（PDU）： 比特。

最大最小值： 无。

数据链路层（Data Link Layer）：

功能： 提供可靠的点对点通信，错误检测和纠正。

服务类型： 帧传递。

通信模式： 点对点、点对多点。

寻址方式： 物理地址（MAC地址）。

网络互连设备： 网桥（Bridge）、交换机（Switch）。

PDU： 帧。

最大最小值： 最小单位为帧，最大受链路层协议的限制。

网络层（Network Layer）：

功能： 路由选择、逻辑寻址和路径选择。

服务类型： 分组交换。

通信模式： 多点到多点。

寻址方式： 逻辑地址（IP地址）。

网络互连设备： 路由器（Router）。

PDU： 分组（数据包）。

最大最小值： 取决于网络层协议。

传输层（Transport Layer）：

功能： 提供端到端的通信、流量控制和差错恢复。

服务类型： 端到端的连接服务。

通信模式： 点对点。

寻址方式： 端口号。

网络互连设备： 无。

PDU： 段（Segment）。

最大最小值： 取决于传输层协议。

会话层（Session Layer）：

功能： 管理会话、对话和同步。

服务类型： 会话。

通信模式： 多点到多点。

寻址方式： 无。

网络互连设备： 无。

PDU： 会话数据单元。

表示层（Presentation Layer）：

功能： 数据格式转换、加密和解密。

服务类型： 数据格式交换。

通信模式： 多点到多点。

寻址方式： 无。

网络互连设备： 无。

PDU： 表示数据单元。

应用层（Application Layer）：

功能： 提供网络服务和应用程序。

服务类型： 文件传输、电子邮件等。

通信模式： 多点到多点。

寻址方式： 无。

网络互连设备： 网关（Gateway）。

PDU： 应用数据单元。

4.IP地址、Socket、域名、邮件地址、URL的命名规则，及合法性判断。

IP地址：

命名规则： IPv4地址由四个十进制数字组成，每个数字范围从0到255，用点分隔。IPv6地址由八组四个十六进制数字组成，以冒号分隔。

合法性判断： IP地址必须符合规定的格式，每个部分的数字在合法范围内，并且没有额外的字符。例如，IPv4地址："192.168.1.1"，IPv6地址："2001:0db8:85a3:0000:0000:8a2e:0370:7334"。

Socket：

命名规则： 由IP地址和端口号组成，形如"IP地址:端口号"。

合法性判断： IP地址和端口号都需要符合各自的合法性规则，且中间用冒号分隔。例如，"192.168.1.1:8080"。

域名：

命名规则： 由一系列标签组成，标签之间用点号分隔。每个标签由字母、数字和连字符组成，总长度有限。

合法性判断： 域名不能以点号开头或结尾，标签之间不能有连续的点号，每个标签长度不超过63个字符。例如，"www.example.com"。

邮件地址：

命名规则： 由用户名和域名组成，中间用@符号分隔。

合法性判断： 邮件地址需要符合特定的格式，包括合法的用户名和域名。例如，"user@example.com"。

URL（统一资源定位符）：

命名规则： 由协议、主机名、路径和查询组成，形如"协议://主机名/路径?查询"。

合法性判断： 需要符合URL的标准格式，协议部分是必需的，主机名不能包含非法字符，路径和查询部分需要符合特定规则。例如，"https://www.example.com/path/to/page?query=value"。

5.IP地址的分类、掩码、前缀、子网、超网、路由聚合的概念，特殊的地址，IPv4-v6过渡策略

IP地址的分类：

IP地址根据其分配方式和范围可以分为不同的类别，主要有以下三类：

A类地址： 第一个字节范围为1-126，用于大型网络，其中第一位为0，后7位为网络号，后24位为主机号。

B类地址： 第一个字节范围为128-191，用于中型网络，其中前两位为10，后14位为网络号，后16位为主机号。

C类地址： 第一个字节范围为192-223，用于小型网络，其中前三位为110，后21位为网络号，后8位为主机号。

掩码、前缀、子网、超网：

掩码（Subnet Mask）： 用于指示IP地址中哪部分是网络号，哪部分是主机号。例如，255.255.255.0。

前缀（Prefix）： 在CIDR（Classless Inter-Domain Routing）中使用，表示IP地址中网络部分的长度。例如，/24表示网络地址的前24位用于网络号。

子网（Subnet）： 将一个大网络划分为若干个小网络，每个小网络称为子网，有自己的网络号。

超网（Supernet）： 将多个相邻的网络汇总为一个更大的网络，减少路由表的规模。

路由聚合：

路由聚合是将多个具体的路由信息合并成一个更广泛的路由表项，以减少路由表的大小，提高路由表的效率。这有助于优化网络资源的使用。

特殊的地址：

保留地址（Reserved Addresses）： 指定的地址范围，用于特殊目的，如0.0.0.0、127.0.0.1等。

广播地址（Broadcast Address）： 每个子网中的所有主机都能接收到的地址，如x.x.x.255。

回环地址（Loopback Address）： 用于本地主机测试，通常表示为127.0.0.1。

IPv4-v6过渡策略：

由于IPv4地址空间枯竭，IPv6被引入作为IPv4的继任者。过渡策略主要包括以下几种：

双栈（Dual Stack）： 在同一设备上同时支持IPv4和IPv6。

隧道（Tunneling）： 在IPv4网络上通过隧道技术传输IPv6数据。

NAT（Network Address Translation）： 在IPv4网络边界上进行地址转换，使得IPv6主机可以访问IPv4资源。

IPv6-over-IPv4 MPLS（6PE）： 在MPLS网络中通过IPv4网络传输IPv6数据。

6.TCP连接的确认方式，停等协议，累计确认，选择确认的过程。

TCP连接的确认方式：

在TCP连接的确认过程中，接收方通过发送ACK来确认已成功接收到发送方的数据。

确认方式分为累计确认和选择确认。

停等协议（Stop-and-Wait Protocol）：

停等协议是一种简单的数据传输协议，发送方发送一个数据包后必须等待接收方的确认才能发送下一个数据包。

该协议的特点是发送方每次只发送一个数据包，并等待接收方的确认。

累计确认（Cumulative Acknowledgment）：

在TCP中，接收方可以发送一个累计确认，指示它已成功接收到所有按序到达的数据。

如果接收方收到的数据包中有某个数据包失序，它会发送一个对最后按序到达的数据包的累计确认。

选择确认（Selective Acknowledgment）：

选择确认引入了更高级的确认机制，允许接收方指示已成功接收到的特定数据包范围。

接收方可以使用SACK选项（Selective Acknowledgment Option）来指定已成功接收的数据包的范围，而不仅仅是最后按序到达的数据包。

TCP连接的确认过程（简化描述）：

发送方发送数据包到接收方。

接收方收到数据包后，发送ACK确认给发送方。

累计确认：ACK中包含已成功接收的最后一个按序到达的数据包的序列号。

选择确认：如果启用了SACK选项，ACK中可以包含指示已成功接收的数据包范围的SACK块。

7.RIP、OSPF、BGP等路由算法的基本原理

RIP（Routing Information Protocol）：

基本原理：

RIP是一种距离向量路由协议，使用跳数（hop count）作为衡量路径的指标。

路由器通过周期性地交换路由更新来维护路由表，以了解到达目的地的最佳路径。

RIP使用Bellman-Ford算法，通过计算到达所有目的地的最小跳数路径来选择最佳路径。

特点：

简单易用，适用于小型网络。

收敛速度较慢，对大型网络不太适用。

OSPF（Open Shortest Path First）：

基本原理：

OSPF是一种链路状态路由协议，使用Dijkstra算法来计算最短路径。

路由器通过交换链路状态信息（LSA，Link State Advertisement）来构建网络拓扑图。

OSPF将网络划分为区域（Area），并在区域内计算最短路径。

支持VLSM（Variable Length Subnet Masking）和多种路由度量标准。

特点：

适用于中大型网络，支持分层设计，有更好的扩展性。

收敛速度相对较快，提供高度的灵活性和可定制性。

BGP（Border Gateway Protocol）：

基本原理：

BGP是一种路径矢量路由协议，用于在不同自治系统之间交换路由信息。

BGP使用路径矢量来描述路由，考虑多种属性如AS路径、权重等来选择最佳路径。

主要用于互联网核心路由器之间的路由选择。

BGP通过BGP路由器之间的TCP连接来交换路由信息。

特点：

用于互联网底层骨干路由器之间的路由选择。

考虑了各种策略性的因素，可实现灵活的路由策略。

收敛速度相对较慢，主要因为BGP的设计目标是稳定而非实时性。

8.各层常见的协议号和端口号的取值

网络层（IPv4、IPv6）：

IPv4 协议号：1（ICMP）、6（TCP）、17（UDP）等。

IPv6 协议号：58（ICMPv6）、6（TCP）、17（UDP）等。

传输层：

TCP 端口号范围：0 到 65535。

UDP 端口号范围：0 到 65535。

应用层（常见协议和端口号）：

HTTP：TCP端口号：80。

HTTPS：TCP端口号：443。

FTP：控制连接端口：21（TCP）。

数据连接端口范围：20到21（TCP）。

SMTP（简单邮件传输协议）：TCP端口号：25。

POP3（邮局协议第3版）：TCP端口号：110。

IMAP（互联网消息访问协议）：TCP端口号：143。

DNS（域名系统）：UDP端口号：53。

Telnet：TCP端口号：23。

SSH（安全外壳协议）：TCP端口号：22。

SNMP（简单网络管理协议）：UDP端口号：161（SNMP）和162（SNMP Trap）。

NTP（网络时间协议）：UDP端口号：123。

DHCP（动态主机配置协议）：UDP端口号：67（服务器）和68（客户端）。

9.IP、TCP、UDP协议的首部长度（固定、可变、总长度）、格式、字段的含义和内容解析

（1） IP协议：

首部长度： IP协议的首部长度是固定的20字节，但可能存在选项字段导致可变长度。

格式：

IP协议的首部包括版本号、首部长度、区分服务代码点、显式拥塞通知、总长度、标识、分片标志、分片偏移、生存时间、上层协议类型、首部校验和、源IP地址、目的IP地址等字段。

字段含义和内容解析：

版本号指示IP协议的版本，通常为4。

首部长度指示首部中32位字的个数，以4字节为单位。

区分服务代码点和显式拥塞通知用于指定数据包的服务等级和拥塞状态。

总长度表示整个IP数据包的长度，包括IP首部和数据部分。

标识是数据包的唯一标识，用于组装分片。

分片标志和分片偏移用于处理分片情况。

生存时间表示数据包在网络中的最大生存时间，每经过一个路由器值减1，为0时数据包被丢弃。

上层协议类型指示数据包的上层协议，例如TCP、UDP等。

首部校验和用于检测首部是否出错。

源IP地址和目的IP地址表示通信的源和目标地址。

（2）TCP协议：

首部长度： TCP协议的首部长度是可变的，最小20字节，最大60字节（包含选项字段）。

格式：

TCP协议的首部包括源端口号、目的端口号、序列号、确认号、首部长度、保留字段、标志、窗口大小、校验和、紧急指针等字段。

字段含义和内容解析：

源端口号和目的端口号标识通信的源和目标端口。

序列号和确认号用于保证数据的有序传输和确认。

首部长度表示首部中32位字的个数，以4字节为单位。

标志包括URG、ACK、PSH、RST、SYN、FIN等，用于控制TCP连接的建立、终止和数据的传输。

窗口大小表示允许发送方发送的未被确认的数据量。

校验和用于检测TCP首部和数据的传输错误。

紧急指针用于指示紧急数据的结束位置。

选项字段和填充字段长度可变，可包括TCP选项如时间戳、窗口缩放等。

（3）UDP协议：

首部长度： UDP协议的首部长度是固定的8字节。

格式：

UDP协议的首部包括源端口号、目的端口号、长度、校验和等字段。

字段含义和内容解析：

源端口号和目的端口号标识通信的源和目标端口。

长度表示UDP数据包的长度，包括首部和数据。

校验和用于检测UDP首部和数据的传输错误。

数据部分包含实际的应用层数据。

10.DNS的作用、查询过程、域名树，域名长度和命名规则

（1） DNS的作用：

DNS（Domain Name System）的作用：

DNS是一种分布式数据库系统，用于将人类可读的域名转换为计算机可理解的IP地址。其主要作用包括：

域名解析： 将域名映射到对应的IP地址。

IP地址解析： 根据IP地址查询对应的域名。

负载均衡： 提供多个IP地址对应同一域名，实现负载均衡和高可用性。

（2） DNS查询过程：

DNS查询过程：

本地域名解析器查询： 用户设备向本地域名解析器（通常是ISP提供的DNS服务器）发起域名解析请求。

本地域名解析器缓存查询： 如果本地解析器已经缓存了对应域名的IP地址，则直接返回给用户设备。

根域查询： 如果本地解析器缓存中没有记录，它将向根域名服务器发起查询请求。

顶级域查询： 根域名服务器返回指向顶级域名服务器（如.com、.org）的IP地址。

二级域查询： 顶级域名服务器返回指向下一级域名服务器的IP地址。

迭代查询： 逐级向下迭代，直到找到目标域名对应的IP地址，或者返回域名不存在的响应。

（3）域名树：

域名树：

域名系统的层次结构形成了一棵树状结构，称为域名树。

根域名位于树的顶部，之下是顶级域名（TLD），再下一级是二级域名，以此类推。

每个域名都唯一地标识了一个主机或域名服务器，并对应一个IP地址。

（4）域名长度和命名规则：

域名长度和命名规则：

域名长度最多为253个字符，每个标签（由点分隔的部分）最多为63个字符。

允许使用字母（大小写不敏感）、数字、连字符（减号），但不能以连字符开头或结尾。

顶级域名（TLD）可以是通用TLD（gTLD）如.com、.org，或国家代码TLD（ccTLD）如.us、.uk。

DNS是大小写不敏感的，但域名中通常使用小写字母以提高可读性。

11.网络协议三要素的名称和作用

语法（Syntax）：

作用： 定义了数据的结构和格式，确保数据的正确传输。

关键概念： 协议规定了消息的格式、字段的顺序、数据的编码方式等。

语义（Semantics）：

作用： 定义了数据的含义，确保通信双方理解数据的意义。

关键概念： 协议规定了数据的具体含义、各字段的解释、消息的目的等。

时序（Timing）：

作用： 确保通信双方在通信过程中的时间顺序和时机的协调。

关键概念： 协议规定了消息的发送和接收的时机、顺序、响应时间等。

12.TCP流量控制和拥塞控制的基本原理、窗口的概念、具体实现过程（阶段）、异同点

（1） TCP流量控制和拥塞控制的基本原理：

TCP流量控制：

目的： 防止发送方发送速率过快，导致接收方无法处理和存储所有接收到的数据。

原理： 通过使用滑动窗口机制来动态调整发送方可以发送的数据量，确保发送方和接收方的数据处理能力匹配。

TCP拥塞控制：

目的： 防止网络中出现拥塞，导致丢包和降低网络性能。

原理： 通过动态调整发送速率，以便在网络拥塞发生时减缓数据传输速率，防止过多数据堆积，从而减轻网络压力。

（2）窗口的概念：

TCP窗口：

定义： 窗口是TCP连接中的一个动态调整的缓冲区，用于控制发送方发送数据的速率。

滑动窗口： 窗口随着数据的传输而滑动，动态调整窗口的大小，以适应网络条件。

（3）TCP流量控制和拥塞控制的具体实现过程：

TCP流量控制实现过程：

接收方通告窗口大小： 接收方通过TCP头部中的窗口字段通告当前可接收的数据量。

发送方根据窗口大小发送数据： 发送方根据接收方通告的窗口大小，调整发送数据的量，确保不超过接收方的处理能力。

接收方动态调整窗口大小： 接收方根据自身处理能力的变化，通过更新窗口字段通告新的窗口大小。

TCP拥塞控制实现过程（阶段）：

慢启动（Slow Start）： 发送方从一个拥塞窗口大小为1的状态开始，每收到一个确认就将窗口大小翻倍，直到达到一个阈值。

拥塞避免（Congestion Avoidance）： 一旦窗口大小达到阈值，发送方切换到线性增加窗口的方式，即每收到一个确认就将窗口大小增加1。

快重传和快恢复： 在发生丢包时，接收方可以使用累积确认迅速通知发送方，发送方可以根据快重传和快恢复机制调整拥塞窗口大小。

超时重传： 当发送方检测到数据包丢失时，会触发超时重传，将拥塞窗口大小设置为1，重新开始慢启动阶段。

（4） 流量控制和拥塞控制的异同点：

异同点：

相同点： 二者都是为了确保数据在网络中可靠传输，防止过度发送导致数据丢失和网络拥塞。

不同点：

流量控制主要关注于发送方和接收方之间的数据传输速率匹配，通过调整窗口大小实现。

拥塞控制主要关注网络中的拥塞情况，通过动态调整发送速率来防止过多的数据在网络中积压。

13.以太网争用期的概念和计算方法

争用期的概念：

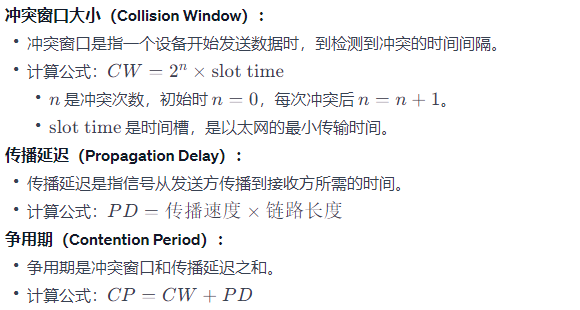
竞争访问： 多个设备都有权利争夺共享媒体的访问权。

侦听媒体： 设备在发送数据前会侦听媒体，确保没有其他设备在传输数据。

争用期： 如果多个设备同时侦听到媒体上没有其他设备在传输数据，它们会进入争用期，尝试发送数据。

争用期的计算方法：

在CSMA/CD协议中，设备进入争用期的时间是通过计算冲突窗口大小和传播延迟的方式确定的。争用期的计算方法如下：



14.常用传输介质的命名方式和特点

（1）双绞线（Twisted Pair）：

命名方式： 根据绞线的种类，分为不同的类别，如Cat 5e、Cat 6a等。

特点：

由多对绞线组成，每对绞线都包裹在绝缘层中，减少干扰。

常用于Ethernet网络，成本较低，易于安装和维护。

（2）同轴电缆（Coaxial Cable）：

命名方式： 通常按同轴电缆的厚度和性能进行分类，如RG-6、RG-58等。

特点：

由一对同心的导体构成，中间是绝缘层和屏蔽层。

常用于有线电视和计算机网络，信号传输较远，带宽相对较大。

（3）光纤（Optical Fiber）：

命名方式： 通常根据光纤的直径和性能进行分类，如单模光纤（Single-mode）和多模光纤（Multimode）。

特点：

由玻璃或塑料纤维构成，可以传输光信号。

具有高带宽、低损耗、抗电磁干扰等特点，适用于高速数据传输和长距离通信。

（4）无线传输介质：

命名方式： 通常根据使用的频段和协议进行分类，如Wi-Fi、Bluetooth等。

特点：

通过无线电波传输数据，不需要物理连接。

包括无线局域网（WLAN）、蓝牙、移动通信等，适用于移动设备和无线通信场景。

（5）卫星传输介质：

命名方式： 通常根据用途和频段进行分类，如通信卫星、气象卫星等。

特点：

通过卫星在空间中传输信号，适用于远距离通信和广播。

具有广覆盖区域的优势，但存在信号传播时延。

（6）电力线传输介质：

命名方式： 通常称为PLC（Power Line Communication）。

特点：

利用电力线进行数据传输，无需额外的数据线路。

适用于家庭电力线网络和智能电网通信。

15.VLAN的帧格式、长度

VLAN（虚拟局域网）是一种网络技术，用于在物理网络上创建逻辑上独立的网络，提高网络管理和隔离性。VLAN在以太网帧的格式上引入了802.1Q标签，以实现帧的归类和隔离。以下是VLAN帧的基本格式：

目的MAC地址（6字节）： 指定帧要传输到的目标设备的MAC地址，用于标识帧的目的地。

源MAC地址（6字节）： 指定帧的发送方的MAC地址，用于标识帧的来源。

802.1Q标签头（4字节）：

Tag Protocol Identifier (TPID)（2字节）： 固定为0x8100，表示这是一个带有802.1Q标签的帧。

Priority（3位）： 用于指定帧的优先级，支持QoS（Quality of Service）。

Canonical Format Indicator (CFI)（1位）： 表示MAC地址是否采用规范格式，0表示规范格式。

VLAN Identifier (VLAN ID)（12位）： 指定VLAN的ID，范围为1-4095，用于标识帧所属的VLAN。

EtherType（2字节）： 指定帧中实际数据的类型，例如IPv4或IPv6。

Payload： 实际数据，根据EtherType确定数据的类型和协议。

Frame Check Sequence（4字节）： 用于差错检测，确保帧在传输过程中的完整性。

16.CRC的计算方法

略

17.数据通信系统的组成部分、主要作用

1. 发送设备（Sender）：

作用： 生成并发送要传输的数据。

组成： 可以是计算机、传感器、摄像头等设备。

2. 发送数据（Data Transmission）：

作用： 将发送设备生成的数据转换成适合传输的形式，并在通信媒体上传输。

组成： 数据传输介质，如电缆、光纤、无线电波等。

3. 发送设备的接口（Interface）：

作用： 提供发送设备与数据传输媒体之间的连接。

组成： 网络接口卡、无线适配器等。

4. 传输媒体（Transmission Media）：

作用： 提供数据在发送设备和接收设备之间传输的物理路径。

组成： 双绞线、同轴电缆、光纤、无线信道等。

5. 接收设备的接口（Interface）：

作用： 提供接收设备与数据传输媒体之间的连接。

组成： 网络接口卡、无线适配器等。

6. 接收数据（Data Reception）：

作用： 接收传输媒体上的数据，并将其转换成接收设备可处理的形式。

组成： 解调器、无线接收器、网络接口卡等。

7. 接收设备（Receiver）：

作用： 接收并处理从发送设备传输过来的数据。

组成： 计算机、显示器、传感器控制器等设备。

8. 协议与控制（Protocols and Control）：

作用： 确保发送和接收设备之间的相互理解和协同工作。

组成： 通信协议、控制信号、错误检测和纠正机制等。

9. 传输控制器（Transmission Control）：

作用： 控制和管理数据的流动，确保数据在传输过程中的可靠性和有序性。

组成： 数据链路层和传输层的控制器。

10. 应用层（Application Layer）：

作用： 提供特定应用领域的服务和功能，如电子邮件、文件传输等。

组成： 应用软件和相关的通信协议。

主要作用：

数据传输： 实现数据在发送和接收设备之间的可靠传输。

通信协议： 确保发送和接收设备之间的正确交流，定义数据的格式和传输规则。

控制与管理： 确保数据的有序传输、错误检测和纠正，保障通信的可靠性。

应用服务： 提供特定应用领域的服务，如文件传输、远程登录等。

18.C/S、B/S和P2P模式的特点、区别和主要应用

C/S（Client/Server）、B/S（Browser/Server）和P2P（Peer-to-Peer）是常见的网络应用架构模式，它们在特点、区别和主要应用上有一些明显的差异。

1. C/S模式（Client/Server）：

特点：

分为客户端和服务器两部分，客户端负责用户界面和一部分逻辑，服务器负责数据存储、处理和业务逻辑。

客户端和服务器之间通过网络进行通信。

区别：

客户端和服务器的分工明确，通信较为集中。

客户端通常需要安装专用客户端软件。

主要应用：

企业管理系统、数据库应用等。

2. B/S模式（Browser/Server）：

特点：

用户通过浏览器访问应用，所有的应用逻辑和数据处理都在服务器端完成。

客户端主要负责展示和与用户交互，不处理业务逻辑。

区别：

客户端轻量，不需要安装专用客户端软件，通过浏览器即可访问应用。

服务器端负责处理逻辑和数据存储。

主要应用：

Web应用、电子商务网站、在线办公等。

3. P2P模式（Peer-to-Peer）：

特点：

所有节点（对等节点）都可以充当客户端和服务器，彼此对等，可以直接通信。

分布式网络结构，无中心服务器。

区别：

没有明确的客户端和服务器，节点之间可相互提供服务。

数据和逻辑可能分散在多个节点上。

主要应用：

文件共享、实时通信、区块链等。

主要区别和选择依据：

分工关系：

C/S： 明确的客户端和服务器分工。

B/S： 客户端主要负责界面，服务器负责逻辑和数据。

P2P： 对等节点，没有明确的客户端和服务器。

应用范围：

C/S： 适用于复杂的企业级应用。

B/S： 适用于Web应用和在线服务。

P2P： 适用于分布式应用、共享和通信场景。

部署和维护：

C/S： 需要在每个客户端安装专用客户端软件，维护相对独立。

B/S： 无需在客户端安装软件，维护更为方便。

P2P： 网络节点相对独立，但可能需要处理节点管理和协同的复杂性。

19.频分、时分、波分等多路复用技术的概念

1. 频分复用（FDM）：

概念： 频分复用是通过在频率域上将多个信号分配到不同的频率带宽上，使它们可以同时在同一传输介质上传输。

原理： 不同信号被调制到不同的频率上，通过频带分配，每个信号占据不同的频率范围。

特点：

需要足够的频谱宽度。

适用于模拟信号和数字信号。

应用： 无线电广播、有线电视等。

2. 时分复用（TDM）：

概念： 时分复用是通过在时间域上将多个信号按照时间顺序分配到同一个传输介质上，使得每个信号在不同的时间片传输。

原理： 时间被划分成若干个时隙，每个信号在各自的时隙内传输。

特点：

不需要额外的频谱宽度，仅需要时间分辨率。

适用于数字信号。

应用： 数字电话网络、数字通信系统等。

3. 波分复用（WDM）：

概念： 波分复用是通过在光纤通信中将多个光信号调制到不同的波长上，使它们能够同时传输。

原理： 不同信号被调制到不同的光波长上，通过波长分配，每个信号占据不同的波长。

特点：

适用于光纤通信系统。

提供更大的带宽。

应用： 光纤通信网络、光传输系统等。

20.应用层主要协议的作用

1. HTTP（Hypertext Transfer Protocol）：

作用： 用于在Web浏览器和Web服务器之间传输超文本文档，支持客户端向服务器请求Web页面，以及服务器向客户端返回Web页面。

2. HTTPS（Hypertext Transfer Protocol Secure）：

作用： 在HTTP的基础上增加了安全性，使用加密协议（如SSL/TLS）进行通信，用于保护用户在浏览器和服务器之间传输的数据的安全性。

3. FTP（File Transfer Protocol）：

作用： 用于在客户端和服务器之间传输文件，支持文件的上传和下载，以及文件夹的创建和删除。

4. SMTP（Simple Mail Transfer Protocol）：

作用： 用于在邮件客户端和邮件服务器之间传输电子邮件，负责发送电子邮件。

5. POP3（Post Office Protocol 3）：

作用： 用于在邮件客户端和邮件服务器之间下载电子邮件，负责将电子邮件从服务器传输到客户端。

6. IMAP（Internet Message Access Protocol）：

作用： 与POP3类似，也用于在邮件客户端和邮件服务器之间管理和获取电子邮件，但具有更多的功能，允许用户在邮件服务器上组织邮件。

7. DNS（Domain Name System）：

作用： 将域名解析为对应的IP地址，提供域名与IP地址之间的映射，使得用户能够使用容易记忆的域名访问互联网资源。

8. DHCP（Dynamic Host Configuration Protocol）：

作用： 用于自动分配IP地址和其他网络配置信息给计算机，使得计算机能够在网络中正确通信。

9. SNMP（Simple Network Management Protocol）：

作用： 用于网络管理和监控，允许管理员远程监测和管理网络设备的性能和状态。

10. SSH（Secure Shell）：

作用： 提供安全的远程登录和文件传输功能，通过加密方式保护网络通信的安全性。

21.Email系统的构成和主要协议

22.ARP协议的作用

23.端口的概要和作用

24.网络协议采用分层思想的原因

25.TCP建立连接和释放链接的过程

26.简述internet与Internet的区别

27.比较拥塞控制和流量控制的相同点与不同点

28.网络传输时延的主要构成，计算方法

29.IP分片、片偏移、标志位之间的关系

30.根据提示，补齐图中TCP连接双方的数据传递过程。

31.根据网络拓扑，完成路由器路由表

32.根据网络拓扑，完成IP地址分配方案的设计

33.比特填充法和字节填充法的具体实现过程