**计算机网络复习提要**

客户程序、服务器程序的特点

**客户程序：客户程序是请求服务的一方，它向服务器程序发送请求并接收服务器的响应。客户程序 特点：**

**主动性：客户程序主动发送请求，请求服务器提供某种服务或资源。**

**请求-响应模式：客户程序发送请求后，等待服务器的响应，并根据响应进行相应的处理。**

**依赖性：客户程序通常依赖服务器程序的存在和运行，以获得所需的服务或资源。**

**服务器程序：服务器程序是提供服务的一方，它接收客户程序的请求并进行处理，然后向客户程序发送响应。服务器程序 特点：**

**被动性：服务器程序处于等待状态，接收来自客户程序的请求并作出相应。**

**处理能力：处理请求的能力，可根据客户程序的请求进行相应的计算、操作或数据传输等**

**高可用性：服务器程序通常需要保持运行状态，以便随时处理客户程序的请求。**

**多用户支持：服务器程序可以同时处理多个客户程序的请求，提供并发的服务。**

**客户程序和服务器程序通常通过网络进行通信。客户程序向服务器程序发送请求消息，服务器程序接收并处理这些请求，并返回响应消息给客户程序。**

协议分层的好处

1. **模块化设计：协议分层使得网络设计可以模块化进行，每个层次都专注于特定的功能。这样可以降低系统的复杂性，使得设计、实现和维护更加容易。**

2. **互操作性：协议分层的一个重要优势是促进了不同设备和软件的互操作性。由于每个层次都有明确定义的功能和接口，不同厂商可以独立地设计和实现每个层次的协议，只需遵循相应的接口规范，就能够相互通信和协作。**

3. **灵活性和可扩展性：协议分层允许网络设计者在需要时对特定层次进行修改和扩展，而无需对整个网络进行重大改动。这种灵活性使得网络可以根据需求进行调整和升级，同时保持底层的稳定性和兼容性。**

4. **故障隔离和故障恢复：由于协议分层，当一个层次出现故障时，只会影响该层次及其上下层次的功能，而不会影响整个网络。这种故障隔离的能力使得网络更加可靠，同时也更容易进行故障恢复和排除故障。**

5. **效率和优化：协议分层允许不同层次的协议进行优化，以提高网络的性能和效率。每个层次可以根据自身的需求和特点进行优化，而不会影响其他层次的功能。这样可以实现更高的网络吞吐量、更低的延迟和更好的资源利用。**

分组交换与电路交换的基本原理，优缺点

**分组交换是将数据分割成较小的数据包（分组），并通过网络独立地传输这些数据包。在发送端，数据被分成固定大小的分组，每个分组都附带有目标地址和其他必要的控制信息。然后，这些分组通过网络独立传输到目标地址。在接收端，分组按照其目标地址进行重新组装，最终得到完整的数据。在分组交换中，网络的资源（带宽、路由器等）是按需共享的，分组可以选择不同的路径进行传输。**

**分组交换 优点：**

**1. 高效利用网络资源：分组交换允许多个分组在网络中并行传输，可以更好地利用网络的带宽，提高网络的利用率。**

**2. 灵活性：由于分组可以选择不同的路径进行传输，因此分组交换对网络拓扑的变化有更好的适应性，具有更好的灵活性。**

**3. 容错性：在分组交换中，即使网络中的某个节点或链路出现故障，数据仍然可以通过其他路径传输，提高了网络的容错性。**

**分组交换 缺点：**

**1. 时延不确定性：由于分组可能选择不同的路径进行传输，不同的分组可能经历不同的时延，导致传输时延的不确定性。**

**2. 额外开销：每个分组都需要附带目标地址和其他控制信息，这增加了传输的额外开销。**

**3. 拥塞控制问题：在分组交换中，当网络中的流量超过网络的容量时，可能会发生拥塞，导致数据传输的延迟增加或丢包现象。**

**电路交换是在建立连接后，为发送方和接收方之间的通信提供一个专用的通信路径。在建立连接时，网络的资源被预留给该连接使用，连接期间的数据传输不需要附加的控制信息。**

**电路交换 优点：**

**1. 传输时延确定性：由于电路交换为发送方和接收方之间建立了一个专用的通信路径，传输时延是确定的，不会像分组交换那样存在时延的不确定性。**

**2. 无额外开销：在建立连接时，控制信息只需要传输一次，数据传输时不需要附加的控制信息，减少了传输的额外开销。**

**电路交换 缺点：**

**1. 资源浪费：在建立连接时，网络资源被该在建立连接时，网络资源被该连接独占使用，即使在连接期间没有实际数据传输也会占用资源，导致资源浪费。**

**2. 缺乏灵活性：由于电路交换需要在通信之前建立连接，因此对网络拓扑变化的适应性较差。如果网络中的节点或链路发生变化，可能需要重新建立连接。**

**3. 低容错性：在电路交换中，如果连接的某个节点或链路出现故障，可能会导致整个连接中断，无法进行数据传输。**

**分组交换适用于大规模网络、高并发传输和灵活性要求较高的场景，能够高效利用网络资源，但可能存在时延不确定性和拥塞控制问题。电路交换适用于对传输时延有严格要求、对资源利用较为节约的场景，但缺乏灵活性和容错性。**

计算机网络的性能指标

**1. 带宽：带宽指网络传输数据的能力，通常以每秒传输的比特数（bps）来衡量。较高的带宽表示网络可以更快地传输数据。**

**2. 时延：时延是指数据从发送端到接收端所需的时间。它包括以下几种类型：**

**- 传输时延：数据在传输介质上传播所需的时间。**

**- 传播时延：数据从发送端传播到接收端所需的时间，取决于物理距离和传播介质的速度。**

**- 处理时延：数据在网络设备上进行处理所需的时间。**

**- 排队时延：数据在网络设备的队列中等待处理的时间。**

**3. 往返时间（RTT）：RTT是指发送数据到接收确认的时间，然后再返回发送端的时间。它可以衡量网络的延迟和响应时间。**

**4. 丢包率：丢包率是指在传输过程中丢失的数据包的比例。较低的丢包率表示网络传输较可靠。**

**5. 吞吐量：吞吐量是指在单位时间内通过网络传输的数据量。较高的吞吐量表示网络可以更快地处理大量数据。**

**6. 网络可靠性：网络可靠性指网络正常运行的时间比例。较高的网络可靠性表示网络较少出现故障或中断。**

实体、协议、服务和服务访问点的含义、相互之间的关系

**实体：在计算机网络中，实体是指网络中的设备或节点，可以是计算机、路由器、交换机等。实体具有自己的唯一标识和地址，并能够进行通信和交换信息。**

**协议：协议是计算机网络中用于实体之间进行通信和交流的规则和约定。它定义了数据传输的格式、通信的过程、错误处理等细节。常见的网络协议有TCP/IP、HTTP、FTP等。**

**服务：服务是指计算机网络中提供给用户或其他实体的功能或特定的应用。它可以是文件传输、电子邮件、网页浏览等各种网络应用。**

**服务访问点：服务访问点是指通过网络访问和使用特定服务的位置或接口。它可以是一个网络地址、一个URL或其他标识符，用于唯一标识和定位服务。**

**实体、协议、服务和服务访问点之间的关系是：实体通过协议进行通信，使用特定的协议来访问和提供各种服务。实体通过服务访问点来访问和使用特定的服务，服务访问点标识了服务的位置和接口。实体之间通过协议进行交互，通过服务访问点来实现对特定服务的访问。**

协议与划分层次

**计算机网络中的协议是为了在不同计算机之间进行通信而制定的规则和约定。协议定义了数据的格式、传输方式、错误处理等内容，确保通信的可靠性和一致性。**

**划分层次是指将网络功能划分为不同的层级，每个层级负责不同的任务，并且层与层之间通过接口进行交互。常用的划分层次模型是OSI参考模型和TCP/IP模型。**

**OSI参考模型 七层，从下到上分别是物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。**

**TCP/IP模型 四层，从下到上分别是网络接口层、网络层、传输层和应用层。**

计算机网体系结构：7层、5层、4层

**7层模型是指ISO/OSI参考模型，它是国际标准化组织（ISO）制定的一种网络体系结构。这个模型将计算机网络的功能划分为七个层次，从下到上分别是物理层、数据链路层、网络层、传输层、会话层、表示层和应用层。每一层都有不同的功能和协议，它们一起工作以实现可靠的通信。**

**5层模型是指TCP/IP参考模型，它是互联网上最常用的网络体系结构。这个模型将计算机网络的功能划分为五个层次，从下到上分别是物理层、数据链路层、网络层、传输层和应用层。它是一种简化的模型，将ISO/OSI模型中的会话层和表示层合并到应用层中，使得整个体系结构更加紧凑。**

**4层模型是指传统的TCP/IP参考模型，它将计算机网络的功能划分为四个层次，从下到上分别是网络接口层、网络层、传输层和应用层。与5层模型相比，4层模型将数据链路层和物理层合并为网络接口层**

最基本的二元制调制方法

**振幅调制（AM） 频移键控调制（FSK）。**

**振幅调制（AM）：振幅调制是一种将二进制信号转换为模拟信号的调制方法。它通过改变载波的振幅来表示数字信号的不同状态。当二进制信号为1时，振幅较大；当二进制信号为0时，振幅较小。接收端可以通过检测振幅的变化来解调二进制信号。**

**频移键控调制（FSK）：频移键控调制是一种将二进制信号转换为数字信号的调制方法。它通过改变载波的频率来表示数字信号的不同状态。当二进制信号为1时，载波的频率较高；当二进制信号为0时，载波的频率较低。接收端可以通过检测频率的变化来解调二进制信号。**

信道的极限容量

**信道的极限容量是指在特定的传输环境下，信道所能传输的最高数据速率。根据香农定理，信道的极限容量由信噪比决定，即信号功率与噪声功率之比。**

**数学上，信道的极限容量可以用香农公式来计算：**

**C = B \* log2(1 + SNR)**

**其中，C表示信道的极限容量（单位为比特每秒），B表示信道的带宽（单位为赫兹），SNR表示信噪比。**

**香农公式表明，在给定的信道带宽下，信道的极限容量与信噪比成正比。当信噪比较高时，信道的极限容量也会相应增加。但是，当信噪比接近于零时，信道的极限容量趋近于零，即无法传输可靠的信息。**

**因此，为了提高信道的容量，可以采取多种方法，如增加信号功率、减小噪声功率、优化调制方案等。同时，还可以利用编码和调制技术、信道编码和纠错码等方法来提高信道的可靠性和容量。**

CDMA

**CDMA，即码分多址，是一种用于无线通信的多址技术。它允许多个用户同时在同一频率上进行通信，通过对每个用户的数据进行编码和解码来实现区分。以下是有关CDMA的一些重要信息：**

**1. 编码方式：CDMA使用一种称为扩频的编码技术。在发送数据之前，发送方将数据乘以一个特定的码（称为扩频码），使数据信号在频域上展宽。接收方通过与发送方使用相同的扩频码进行解码，从而恢复原始数据。**

**2. 多用户接入：CDMA允许多个用户同时在同一频率上进行通信，而不会产生明显的干扰。每个用户被分配一个唯一的扩频码，通过这种方式实现用户之间的区分。在接收端，使用与目标用户相关的扩频码进行解码，以提取该用户的数据。**

**3. 抗干扰能力：CDMA具有良好的抗干扰能力。由于每个用户使用不同的扩频码，即使在存在干扰的情况下，接收端仍然能够有效地解码目标用户的数据。**

**4. 频谱效率：CDMA的频谱效率相对较高。由于多个用户可以共享同一频率带宽，CDMA可以在有限的频谱资源下支持更多的用户。**

**5. 应用领域：CDMA广泛应用于无线通信系统中，如移动通信系统（例如CDMA2000和WCDMA）和卫星通信系统。它提供了一种可靠和高效的通信方式，适用于同时支持多个用户的场景。**

点对点信道的数据链路层在进行通信时的主要步骤

**1. 链路建立：两个通信节点首先需要建立一个物理链路，确保它们之间可以进行数据传输。这包括选择适当的物理介质（如电缆或光纤）和配置所需的硬件设备。**

**2. 帧封装：数据链路层将上层传递下来的数据分割成适当大小的数据块，称为帧。每个帧包含了控制信息（如起始位和结束位）、数据本身以及差错检测码（如循环冗余检验码）。**

**3. 帧传输：帧通过物理链路从发送方传输到接收方。这可能涉及到编码、调制和调制解调过程，以便将数字信号转换为适合传输的模拟信号。**

**4. 差错检测：接收方在接收到帧后，使用差错检测码检测是否存在传输过程中引入的错误。常见的差错检测码包括循环冗余检验码（CRC）和奇偶校验码。**

**5. 帧解封装：接收方将接收到的帧解封装，提取出原始的数据和控制信息。**

**6. 确认和重传：接收方向发送方发送确认信息，通知发送方已成功接收到帧。如果发送方在一定时间内未收到确认信息，或者接收方检测到错误，发送方将重新发送相应的帧。**

**7. 链路终止：当通信结束时，链路将被释放，以便其他通信可以使用该链路。**

PPP协议的三个组成部分

**1. 链路控制协议（LCP）：LCP用于建立、配置和测试数据链路连接。它负责在PPP连接的两端进行链路配置和维护，包括协商传输参数、错误检测和恢复机制等。**

**2. 网络控制协议（NCP）：NCP用于在PPP连接上协商和配置网络层协议。它负责选择和配置网络层协议，例如IP、IPX等，并确保它们在PPP连接上正常运行。**

**3. PPP数据链路协议：PPP数据链路协议封装和传输数据。它负责将网络层的数据封装成PPP帧，并在接收端将其解封装，以便在网络层进行处理。**

**这三个组成部分共同工作，使得PPP能够在点对点连接中有效地建立和管理数据传输。**

数据链路层的三个基本问题

**1. 封装成帧：数据链路层负责将从网络层接收到的数据划分为适当的帧（Frames），每个帧都包含了数据和控制信息。帧的划分通常通过在数据的开始和结束位置添加特殊的控制字符来完成。**

**2. 透明传输：数据链路层需要保证数据在传输过程中的透明性，即使在数据中存在与控制字符相同的字节时也能正确处理。这通常通过使用字节填充（Byte stuffing）或比特填充等技术来实现。**

**3. 差错检测与纠正：数据链路层需要提供可靠的数据传输，以确保数据在传输过程中的完整性。为了检测和纠正错误，常用的技术包括循环冗余检验（CRC）和海明码等。**

媒体共享信道技术的两大类，每一类又有哪几种

**媒体共享信道技术的两大类是时分多路复用（TDM）和频分多路复用（FDM）。**

**时分多路复用（TDM）的几种技术包括：**

**1. 统计时分多路复用：根据传输数据的实际需求，动态地分配时间片给不同的用户。**

**2. 固定时分多路复用：将时间划分为固定的时隙，每个时隙只分配给一个用户，不管其是否有数据传输需求。**

**频分多路复用（FDM）的几种技术包括：**

**1. 统计频分多路复用：根据传输数据的实际需求，动态地分配频率给不同的用户。**

**2. 固定频分多路复用：将频谱划分为固定的频带，每个频带只分配给一个用户，不管其是否有数据传输需求。**

为了通信的方便，以太网采用哪两种措施。

**1. CSMA/CD（载波侦听多路访问/碰撞检测）：CSMA/CD是一种用于以太网的介质访问控制（MAC）协议。在发送数据之前，网络设备会先监听信道上是否有其他设备正在发送数据。如果信道空闲，设备就可以发送数据；如果有其他设备同时发送数据导致碰撞，设备会停止发送并等待一段随机的时间后重新尝试发送，以减少碰撞的发生。**

**2. 媒体访问控制地址（MAC地址）：每个连接到以太网的设备都会有一个唯一的MAC地址，它由48位二进制数字表示。MAC地址用于标识网络中的设备，类似于设备的物理地址。以太网使用MAC地址来确定数据包的接收者和发送者，以便正确地路由和传递数据。这种方式使得以太网能够准确地将数据包发送到目标设备，实现通信的方便性。**

截断二进制指数退避算法

**截断二进制指数退避算法：在计算机网络中用于解决冲突问题的退避算法。当多个设备同时尝试在网络上发送数据时，可能会发生冲突，这时需要使用一种机制来避免继续发生冲突。**

**截断二进制指数退避算法的过程如下：**

**1. 当设备需要发送数据时，首先选择一个随机的退避窗口大小，通常使用指数函数进行计算，比如选择一个介于0和2^k之间的随机数，其中k是重传次数。**

**2. 设备在退避窗口时间内等待，如果在此期间没有检测到其他设备的活动，则设备可以发送数据。**

**3. 如果在退避窗口时间内检测到其他设备的活动（即冲突发生），则设备需要等待一段时间，并将退避窗口大小加倍。**

**4. 重复步骤2和步骤3，直到设备成功发送数据或达到最大重传次数。**

**下面是一个示例：**

**假设有两个设备A和B同时尝试在网络上发送数据。设备A选择了一个退避窗口大小为2的指数函数（即随机数为0或1），设备B选择了一个退避窗口大小为4的指数函数（即随机数为0、1、2或3）。**

**1. 设备A在退避窗口时间内等待，没有检测到冲突，可以发送数据。**

**2. 设备B在退避窗口时间内等待，没有检测到冲突，可以发送数据。**

**3. 如果两个设备在同一时间内发送数据，发生了冲突。设备A和设备B都需要等待一段时间，并将退避窗口大小加倍。**

**4. 设备A选择了一个退避窗口大小为4的指数函数（即随机数为0、1、2或3），设备B选择了一个退避窗口大小为8的指数函数（即随机数为0到7之间的数）。**

**5. 设备A在退避窗口时间内等待，没有检测到冲突，可以发送数据。**

**6. 设备B在退避窗口时间内等待，没有检测到冲突，可以发送数据。**

**通过不断调整退避窗口大小，并等待一段时间，截断二进制指数退避算法可以有效地减少冲突的发生，提高网络的传输效率。**

CSMA/CD协议的要点

**1. 载波侦听：在发送数据之前，节点首先检测信道上是否有其他节点正在发送数据。如果信道被占用，节点将等待一段时间，直到信道空闲，然后再发送数据。**

**2. 多点接入：多个节点共享同一个信道，任何节点都可以尝试发送数据。每个节点都有平等的访问权，可以根据需要发送数据。**

**3. 碰撞检测：如果两个或更多节点同时开始发送数据，它们的信号会在信道中发生碰撞。发送节点会检测到这个碰撞，并立即停止发送，然后等待一个随机的时间间隔，再次尝试发送。**

**4. 碰撞处理：当发生碰撞时，节点会使用一种指数退避算法，通过等待随机的时间间隔来避免再次发生碰撞。节点等待的时间间隔会逐渐增加，以减少再次发生碰撞的可能性。**

**5. 重传机制：如果节点成功发送了数据而没有发生碰撞，接收节点会返回一个确认帧。如果发送节点在一定时间内没有收到确认帧，它会假设数据丢失，并进行重传。**

以太网的自学习功能

**以太网的自学习功能是指网络交换机通过观察和分析网络数据帧的目的MAC地址来学习和建立转发表，从而实现数据的有效转发。当一个数据帧到达交换机时，交换机会检查该数据帧的源MAC地址，并将其与已学习到的MAC地址进行比对。如果该源MAC地址已存在于转发表中，交换机将根据表中的信息将数据帧发送到相应的端口。如果该源MAC地址尚未存在于转发表中，交换机将学习该地址，并将其与到达的接口关联起来，以便将来可以将数据帧正确地转发到该地址。**

**以太网的自学习功能使得网络交换机能够动态地学习和适应网络中设备的变化。当设备加入网络或者改变位置时，交换机能够及时学习到新的MAC地址，并更新转发表，确保数据可以准确地传送到目标设备。这种自学习的机制使得以太网网络更加智能和高效，提供了良好的数据转发能力。**

虚电路服务与数据报服务的对比

**1. 连接方式：**

**- 虚电路服务：在通信之前，虚电路服务需要建立一条预定的路径或连接。数据沿着这个路径传输，直到通信结束。连接建立后，数据包按照相同的路径传输，因此保证了数据包的顺序性。**

**- 数据报服务：数据报服务不需要提前建立连接。每个数据包都是独立传输的，它们可以通过不同的路径到达目的地。每个数据包都包含足够的信息，例如源地址和目的地址，用于路由和重新组装。**

**2. 传输可靠性：**

**- 虚电路服务：由于连接建立和数据包顺序的保证，虚电路服务通常更可靠。数据包可以按照预定路径传输，且在传输过程中不容易丢失或出错。**

**- 数据报服务：数据报服务相对不太可靠。由于数据包独立传输且可以经过不同的路径，数据包的丢失、重复或乱序可能会发生。为了增加可靠性，数据报服务通常使用一些额外的机制，如确认和重传。**

**3. 开销：**

**- 虚电路服务：虚电路服务需要在通信开始之前建立连接，这涉及到一些额外的开销，如建立连接的时间和资源消耗。但是，在连接建立后，传输的开销较小。**

**- 数据报服务：数据报服务不需要事先建立连接，因此避免了连接建立的开销。每个数据包都包含完整的地址和路由信息，这可能导致数据包的开销增加。**

**4. 适用场景：**

**- 虚电路服务：虚电路服务适用于对传输顺序和可靠性要求较高的应用，如实时音视频通话或流媒体传输。它提供了较好的数据包顺序保证和可靠性。**

**- 数据报服务：数据报服务适用于一些对实时性要求较低的应用，如电子邮件或网页浏览。它提供了更大的灵活性，允许数据包以并行和多路径的方式传输。**

计算机网络通信中，可靠交付应当由谁来负责的两种观点讨论，其原因是什么？

**第一种观点认为，可靠交付应由网络层来负责。网络层是计算机网络的一个层级，负责在源主机和目标主机之间提供端到端的数据传输服务。从这个观点出发，网络层应该负责确保数据在传输过程中的可靠性。网络层可以采用各种技术和协议，如错误检测、重传机制和流量控制等，以保证数据的完整性和正确性。这样的安排能够最大程度地减少数据传输过程中的丢包、错误和延迟等问题，确保数据能够按时、无损地到达目标主机。**

**第二种观点认为，可靠交付应由传输层来负责。传输层是计算机网络的另一个层级，主要负责为应用层提供端到端的数据传输服务。从这个观点来看，传输层应该负责确保数据在应用程序之间的可靠交付。传输层可以使用各种协议，如TCP（传输控制协议），该协议提供了可靠的数据传输机制，包括数据的分段、流量控制、拥塞控制和错误恢复等功能。通过在传输层实现可靠交付，可以减轻网络层的负担，并且使得应用程序更专注于数据的处理和业务逻辑。**

**这两种观点的原因是，不同的层级有不同的职责和功能。网络层更关注网络传输的可靠性和路由选择，而传输层更专注于应用程序之间的可靠数据传输。根据网络架构的设计和需求，决定可靠交付的责任分配到哪个层级是灵活的，并且可以根据具体情况进行调整和优化。**

IP地址具有的重要特点

**1. 唯一性：每个设备在网络中都必须具有唯一的IP地址，以便在网络上进行准确的寻址和通信。**

**2. 标识性：IP地址用于标识网络中的设备。它可以帮助数据包在网络中正确地路由和传输到目标设备。**

**3. 层次性：IP地址采用层次结构，以便实现有效的路由和子网划分。IP地址由网络部分和主机部分组成，其中网络部分用于标识设备所连接的网络，而主机部分用于标识特定网络中的设备。**

**4. 独立性：IP地址是与设备的物理位置无关的，它可以随着设备在网络中的移动而改变。这种独立性使得设备可以自由地切换网络而不需要更改IP地址。**

**5. 可变性：IP地址可以是静态的或动态的。静态IP地址是手动配置的，并且在设备重新启动后保持不变。而动态IP地址是通过动态主机配置协议（DHCP）自动分配的，它们可以在设备重新连接到网络时动态更改。**

从不同层次上看IP地址和MAC地址，可以得到的结论是？（P132的这里要强调指出以下几点）

**1. IP地址（Internet Protocol Address）是在网络层（网络协议的第三层）上使用的地址，用于标识网络中的主机或设备。IP地址是逻辑地址，它提供了一种在网络上唯一标识和寻址主机的方式。IP地址由32位或128位二进制数字组成，用于在互联网上进行路由和寻址。**

**2. MAC地址（Media Access Control Address）是在数据链路层（网络协议的第二层）上使用的地址，用于标识网络中的网络接口卡（NIC）或网卡。MAC地址是物理地址，是由网络接口卡的制造商分配的唯一地址。MAC地址由48位二进制数字组成，通常表示为十六进制数。**

使用ARP的四种典型情况

**1. 主机A与主机B在同一局域网内通信：当主机A需要与主机B通信时，它首先检查本地的ARP缓存，看是否已经知道主机B的MAC地址。如果缓存中没有记录，主机A将发送一个ARP请求广播消息，询问局域网内所有设备，"谁拥有IP地址为B的主机的MAC地址？" 主机B收到该请求后，会发送一个ARP响应消息，其中包含它的MAC地址。主机A接收到响应后，将更新本地的ARP缓存，并将通信数据发送到主机B的MAC地址。**

**2. 主机A与主机B在不同局域网内通信：当主机A需要与另一个网络中的主机B通信时，它首先检查本地ARP缓存，如果缓存中没有记录，主机A将发送ARP请求消息到默认网关（路由器）。默认网关收到该请求后，会根据目标IP地址转发请求到主机B所在的局域网。主机B接收到请求后，发送一个ARP响应消息给默认网关，其中包含它的MAC地址。默认网关将接收到的响应消息转发给主机A，主机A更新本地ARP缓存，并向主机B发送通信数据。**

**3. ARP缓存污染：ARP缓存污染是一种恶意攻击方法，攻击者发送虚假的ARP响应消息，将合法主机的IP地址与攻击者自己的MAC地址关联起来。当其他主机在发送数据时，数据将被发送到攻击者的MAC地址，攻击者可以截获或修改数据。**

**4. ARP欺骗：ARP欺骗是另一种恶意攻击方法，攻击者发送虚假的ARP响应消息，将合法主机的IP地址与攻击者控制的另一个主机的MAC地址关联起来。这导致网络流量被重定向到攻击者控制的主机上，攻击者可以进行监听、拦截或篡改通信数据。**

ARP的工作过程

**1. 主机A发送一个ARP请求广播包，其中包含目标主机B的IP地址。**

**2. 所有连接到网络的主机都会接收到这个ARP请求广播包，但只有IP地址与请求中的目标地址匹配的主机B会响应。**

**3. 主机B收到ARP请求后，会将自己的MAC地址包含在一个ARP响应包中，并发送回主机A。**

**4. 主机A收到ARP响应包后，会将主机B的IP地址和MAC地址存储在它的ARP缓存中，以便将来的通信中使用。**

**5. 之后，主机A就可以使用主机B的MAC地址直接发送数据包到主机B，而无需再进行地址解析过程。**

IP数据包的分片涉及到的字段

**1. 标识符：该字段用于标识原始IP数据包，并在分片过程中保持相同，以便接收端能够重新组装分片。**

**2. 标志位：标志位字段包含3个位，其中第一个位被设置为0，后两个位被用于控制分片。第二个位是“禁止分片（DF）”位，如果设置为1，表示该数据包不允许进行分片。第三个位是“更多分片（MF）”位，如果设置为1，表示还有更多的分片数据包。**

**3. 片偏移：片偏移字段表示当前分片在原始数据包中的位置，以8字节为单位。通过片偏移字段，接收端可以按照正确的顺序重新组装分片。**

**4. 生存时间：生存时间字段指定了IP数据包在网络上可以经过的最大路由器跳数。每经过一个路由器，TTL值就会减少1。如果TTL值为0，数据包将被丢弃。**

**5. 协议：协议字段指定了上层协议，例如TCP或UDP，该字段决定了数据包在到达目的地后应该由哪个协议进行处理。**

**6. 源IP地址和目的IP地址：这两个字段分别指定了数据包的源IP地址和目的IP地址，用于确定数据包的发送者和接收者。**

IP层转发分组的过程-基于终点的转发

**1. 分组接收：路由器收到一个IP数据分组。**

**2. 目的IP地址解析：路由器检查分组中的目的IP地址。**

**3. 查找路由表：路由器查询自己的路由表，以确定下一跳的目标路由器。**

**4. 下一跳确定：路由器根据路由表中与目的IP地址匹配的最长前缀，确定下一跳路由器的IP地址。**

**5. 下一跳地址解析：路由器将下一跳路由器的IP地址转换为对应的物理地址，如MAC地址。**

**6. 分组转发：路由器将分组通过适当的物理接口发送到下一跳路由器。**

**7. 重复过程：下一跳路由器重复上述步骤，直到分组到达最终目的地。**

IP层转发分组的过程-最长前缀匹配转发

**1. 当一个数据包到达路由器时，路由器会检查该数据包的目标IP地址。**

**2. 路由器会查找其路由表，该表包含了与不同网络相连的接口和相应的IP地址范围。**

**3. 路由器会将目标IP地址与路由表中的每个条目进行比较，使用最长前缀匹配的规则选择最佳匹配。**

**4. 最长前缀匹配规则是指路由器将选择具有最长公共前缀的IP地址范围。也就是说，路由器将选择与目标IP地址具有最长匹配前缀的路由表条目。**

**5. 路由器将根据匹配到的路由表条目确定转发接口，该接口将数据包发送到下一跳路由器或目标主机。**

**6. 如果找不到匹配的路由表条目，路由器将使用默认路由（default route）将数据包转发到一个预定义的接口，通常是连接到互联网的接口。**

理想路由算法的特点。

**1. 最优路径选择：理想路由算法能够选择最优的路径来传输数据。它会考虑网络中各个节点之间的拓扑结构、链路的带宽、延迟等因素，以确定最佳路径，从而实现高效的数据传输。**

**2. 负载均衡：理想路由算法会尽可能地平衡网络中各个路径的负载，确保数据在整个网络中分布均匀。通过合理的负载均衡，可以避免某些路径过载而造成的网络拥塞，提高整体网络的性能。**

**3. 容错性：理想路由算法具有较强的容错性能，能够在网络发生故障或链路出现问题时，及时调整路由，选择可用的备用路径来保证数据的传输。它可以自动检测和适应网络的变化，确保网络的可靠性和稳定性。**

**4. 可扩展性：理想路由算法可以适应不同规模和复杂度的网络环境。无论是小型局域网还是大规模互联网，理想路由算法都能够根据网络的规模和需求进行相应的扩展和优化，以满足不同网络环境下的路由需求。**

**5. 独立性：理想路由算法是独立于特定的网络技术和设备的。它可以应用于不同类型的网络，如IP网络、以太网等，而不受底层技术的限制。这种独立性使得理想路由算法具有广泛的适用性和灵活性。**

RIP协议的特点

**1. 分割的网络：RIP协议将网络分割成多个区域，每个区域内的路由器使用相同的RIP配置和参数进行通信。**

**2. 距离度量：RIP协议使用跳数作为路由的度量标准，即将到达目标网络所经过的路由器数量作为距离的衡量。**

**3. 最大跳数限制：RIP协议的最大跳数限制为15，意味着超过15个跳数的路由被认为是不可达的，这限制了RIP协议在大型网络中的应用。**

**4. 周期性更新：RIP协议通过周期性地广播路由更新信息，将整个网络中的路由信息进行交换和更新。默认情况下，更新时间间隔为30秒。**

**5. 路由表更新：RIP协议的路由表更新是基于距离向量的算法，每个路由器通过交换路由更新信息来更新本地的路由表，并根据最小跳数来选择最佳路径。**

**6. 无类别域间路由（CIDR）支持：RIP协议可以与CIDR协议结合使用，支持对网络地址的聚合和分割，提高了路由表的效率和灵活性。**

距离向量算法（RIP）。

**距离向量算法（RIP）是一种用于在计算机网络中确定路由表的动态路由协议。它通过使用距离向量（包含路由器与其他路由器之间的距离信息）来确定最佳的路由路径。**

**RIP使用基于跳数（即经过的路由器数量）的度量来确定路由的优先级。每个路由器通过广播其距离向量信息告知邻居路由器，并更新自己的路由表。当一个路由器接收到来自邻居路由器的距离向量信息时，它会检查是否存在更短的路径到目标网络，并根据需要更新自己的路由表。通过这种方式，RIP协议逐步收敛并确定整个网络的最佳路由路径。**

**以下是一个简单的示例，假设有三个路由器A、B和C，它们通过RIP协议进行路由表的交换：**

**- 初始状态下，每个路由器只知道直接相连的网络，并将距离设置为1。**

**- 路由器A广播自己的路由表给B和C，其中包含它直接相连的网络和距离。**

**- 路由器B和C收到A的路由表，并将自己的路由表更新为A的信息，将距离设置为A到目标网络的距离加1。**

**- 然后，路由器B和C分别广播自己更新后的路由表给A。**

**- 路由器A接收到B和C的路由表，检查是否存在更短的路径，如果有，则更新自己的路由表。**

**- 这个过程不断重复，直到网络中的所有路由器的路由表收敛并达到一致。**

**需要注意的是，RIP使用跳数作为度量，因此在大型网络中可能存在一些限制，例如最大跳数限制。此外，RIP需要一定的时间才能收敛，并且对网络的变化（如链路故障）响应较慢。因此，在复杂的网络环境中，可能需要使用其他更高级的动态路由协议来取代RIP。**

RIP协议的缺点

**1. 慢收敛：RIP使用距离向量算法来确定路由，其中每个路由器将自己的路由表信息传递给相邻路由器。当网络发生拓扑变化时，每个路由器需要将更新的路由信息发送给所有相邻路由器，并等待其他路由器的更新信息。这种逐跳传递和等待更新的过程导致了慢速的收敛，即网络在适应拓扑变化时需要花费较长时间。**

**2. 低效的网络利用率：RIP采用固定的跳数（最多15跳）作为路径选择的度量标准。这种度量标准不能反映出网络中实际链路的负载和拥塞情况，因此可能导致选择不是最优的路径。特别是在大型网络中，RIP的固定跳数限制可能导致路径选择不够灵活，无法有效地利用网络资源，从而降低网络的整体性能。**

**3. 支持有限的网络规模：RIP设计初衷是用于小型网络，因此其路由表的大小和网络规模有一定的限制。RIP使用存储路由表的方式，每个路由器需要维护和传递整个路由表信息，随着网络规模的增大，路由表的大小也会增加。当网络规模较大时，RIP的路由表可能会变得庞大，占用大量的存储和带宽资源。**

**4. 安全性弱：RIP协议在设计时没有考虑到安全性问题，缺乏对路由信息的验证和保护机制。这使得RIP容易受到路由欺骗、篡改和伪造等攻击，恶意用户可以通过发送虚假的路由更新信息来干扰网络的正常运行。**

OSPF的基本特点。

**1. 开放性：OSPF是一个开放的协议，它的协议规范公开发布，并且可以由不同厂商实现和支持。这使得不同厂商的路由器可以互相通信和交换路由信息。**

**2. 最短路径优先：OSPF使用最短路径优先算法（Dijkstra算法）来计算网络中的最佳路径。它通过评估链路的成本（通常是基于带宽）来确定最短路径，以便有效地转发数据包。**

**3. 分层设计：OSPF将网络划分为不同的区域（Area），每个区域内部有一个区域边界路由器，负责与其他区域交换路由信息。这种分层设计提高了网络的可扩展性和管理性。**

**4. 支持VLSM：OSPF可以支持可变长度子网掩码（VLSM），即允许在同一个网络中使用不同的子网掩码长度。这样可以更有效地利用IP地址空间，并支持网络的灵活划分。**

**5. 路由更新：OSPF使用链路状态数据库（Link State Database）来存储网络中的拓扑信息，每个路由器通过交换链路状态更新（LSA）来更新数据库。这种方式可以快速适应网络拓扑的变化，并减少路由收敛的时间。**

**6. 支持多种类型网络：OSPF可以应用于不同类型的网络，包括广域网（WAN）和局域网（LAN），支持多种链路层协议（如Ethernet、Frame Relay等），以及多种网络层协议（如IPv4和IPv6）。**

**7. 安全性：OSPF提供了一些安全机制，如认证和加密，以确保路由信息的可靠性和完整性。这有助于防止恶意攻击和未经授权的路由器加入网络。**

OSPF除了基本特点外，还具有的一些特点

**1. 分层设计：OSPF将网络划分为不同的区域（Area），每个区域内部使用自己的SPF（最短路径优先）算法进行路由计算，从而减少整个网络的复杂性和开销。**

**2. 路由选择：OSPF使用基于链路状态的路由选择算法，它考虑到链路的带宽、延迟、可靠性等因素，选择最优的路径作为数据包的传输路径。**

**3. 支持可扩展性：OSPF可以支持大型复杂网络，因为它允许将网络划分为多个区域，每个区域内部的路由信息相互独立，降低了网络中路由信息的传播范围，提高了网络的可扩展性。**

**4. 动态更新：OSPF可以动态地响应网络拓扑的变化，例如链路故障、带宽变化等，它通过交换链路状态信息（LSA）来实现路由表的更新和同步，从而保持网络的稳定性和可用性。**

**5. 支持多路径：OSPF可以支持在网络中存在多条等价路径，从而提高了网络的冗余性和容错能力。它可以在路由表中存储多个相同目的地的路由项，并将流量分配到不同的路径上。**

**6. 安全性：OSPF提供了一些安全机制来保护路由信息的机密性和完整性，例如使用认证密钥对路由器之间的交换进行身份验证，防止未经授权的路由器加入网络。**

BGP的路由选择

**1. 最短路径优先（SPF）：BGP使用最短路径算法来选择到达目标网络的最佳路径。这是基于每个路径的AS（自治系统）跳数来计算的，AS跳数越少，路径越优先。**

**2. 路径属性：BGP使用路径属性来描述网络路径的特性。其中，AS路径属性指定了数据包经过的AS序列，本地优先级属性可用于手动设置路径优先级，以及其他属性如自治系统内部的前缀长度、通告时间等。**

**3. 前缀长度：BGP将前缀长度作为路由选择的依据之一。较长的前缀（即前缀掩码较长）通常优先于较短的前缀。**

**4. 策略控制：BGP允许网络管理员根据特定需求和政策来控制路由选择。这些策略可以基于AS路径、前缀长度、自治系统关系等进行设置，以满足网络管理者的需求。**

**5. BGP属性的优先级：在BGP中，各种路径属性有不同的优先级。例如，LOCAL\_PREF属性用于在自治系统内部选择路由，优先级高的路径将被选择。**

多播路由协议为什么复杂？

**1. 地址管理：多播地址是一种特殊的IP地址，用于标识多播组。多播路由协议需要有效地管理和分配这些地址，以确保数据可以正确地传输到目标组。**

**2. 数据传输路径选择：在多播通信中，数据包需要通过网络中的多个路径传输到达目标组的所有成员。多播路由协议需要选择最佳的传输路径，以最小化延迟和网络拥塞，并确保数据包能够高效地传递到每个接收者。**

**3. 成员维护：多播组的成员可能会动态地加入或离开组。多播路由协议需要能够及时检测成员的变化，并相应地更新路由表和转发路径，以确保数据包能够正确地传输到有效的接收者。**

**4. 数据复制与转发：多播数据包需要被复制并在网络中的各个路径上转发，以达到所有接收者。这需要复杂的转发逻辑和控制机制，以确保数据的可靠传输和最小化网络资源的使用。**

**5. 协议兼容性：多播路由协议需要与现有的网络协议和设备兼容，以便在不同厂商和不同网络环境中运行。这需要协议设计考虑到各种网络设备和操作系统的差异，以确保协议的互操作性和可扩展性。**

反向路径广播和剪除

**反向路径广播用于确定数据包的最佳路径，而剪除技术用于提高数据包传输的效率。**

**反向路径广播是一种路由算法，用于在计算机网络中确定数据包传输的最佳路径。它主要用于无连接的分组交换网络中，例如因特网。**

**在反向路径广播中，当一个路由器收到一个数据包时，它会向所有的邻居路由器发送该数据包，除了它收到该数据包的接口所连接的路由器。这样做的目的是确保数据包能够传输到目的地，而不会陷入无限循环的情况。**

**具体而言，反向路径广播使用了路由表中的信息来确定最佳路径。当一个路由器收到一个数据包时，它会检查数据包的源地址，并查找与该地址相关联的路由表项。然后，它将数据包转发到与该路由表项中指定的下一跳路由器相连的接口。**

**剪除是一种数据包传输的技术，在计算机网络中用于提高传输效率。剪除技术允许数据包在到达目的地之前不必完全接收，并且可以在接收到数据包的一部分后立即开始转发。**

**在剪除技术中，当一个路由器收到一个数据包时，它会检查数据包的目的地地址，并查找与该地址相关联的路由表项。然后，它会立即开始将数据包转发到下一个路由器，而不必等待整个数据包完全接收。**

**剪除技术的优势在于它能够减少传输延迟，因为数据包不需要等待完全接收就可以开始转发。然而，剪除技术也带来了一些风险，因为如果在传输过程中发生错误，未完整接收的数据包可能会导致数据的丢失或损坏。**

IGMP工作的两个阶段

**1. 主机发现阶段：在这个阶段，主机（接收多播组的终端设备）会发送IGMP报文给本地路由器，以表明它对特定多播组的兴趣。主机发送的IGMP报文可以是成员查询报文或成员报告报文。成员查询报文由路由器发送，用于询问主机是否对某个多播组感兴趣。主机收到查询报文后，如果对该多播组感兴趣，则会发送成员报告报文进行回复，表示它想要加入该组。通过这种方式，主机可以将自己加入到所需的多播组中。**

**2. 组织管理阶段：在主机发现阶段完成后，路由器会根据接收到的成员报告报文来维护一个多播组成员表。这个表记录了哪些主机对哪些多播组感兴趣。路由器还会周期性地发送成员查询报文来确认主机是否仍然对某个多播组感兴趣。如果一段时间内没有收到主机的成员报告报文，路由器会假设该主机已经不再对该多播组感兴趣，并将其从多播组成员表中移除。**

为了避免多播控制信息给网络增加大量的开销，IGMP采用的具体措施有？

**1. 版本协商：IGMP协议通过版本字段来区分不同的IGMP版本。版本协商可以确保不同版本的设备之间能够正确地交互和理解IGMP消息，从而避免由于版本不一致而引发的问题。**

**2. 消息压缩：IGMP协议使用消息压缩技术来减少多播控制消息的数量和大小。通过合并相同的消息，删除冗余的信息，以及使用差异编码等技术，可以有效地减少传输的数据量，从而降低网络开销。**

**3. 查询延迟：IGMP协议引入了查询延迟机制，即在发送查询消息之后，等待一定的时间再接收主机的响应。这样可以避免在短时间内收到大量的重复响应，减轻网络负担。**

**4. 查询版本号：IGMP协议中的查询消息包含一个版本号字段，用于标识查询的类型和属性。通过查询版本号，可以使网络设备根据需要选择性地处理查询消息，避免对不必要的消息作出响应，从而减少网络开销。**

网络地址转换

**网络地址转换（简称NAT）将私有IP地址转换为公共IP地址的技术。**

**NAT的主要目的是解决IPv4地址不足的问题。在IPv4网络中，IP地址资源有限，而私有IP地址范围是可以被重复使用的。NAT允许多个设备共享同一个公共IP地址，通过转换私有IP地址和端口号，实现了局域网内部设备与公网之间的通信。**

**NAT的工作原理如下：当位于局域网内部的设备向公网发送数据包时，NAT设备会将源IP地址和端口号修改为公共IP地址和一个唯一的端口号。当公网返回响应数据时，NAT设备会根据端口号和转换表将数据包转发给对应的局域网设备。**

**NAT提供了一些重要的功能和优势，包括：**

**1. IP地址共享：多个设备可以使用同一个公共IP地址进行访问互联网，减少了对公共IP地址的需求。**

**2. 隐藏内部网络：通过将私有IP地址转换为公共IP地址，NAT可以隐藏内部网络的细节，增加了网络的安全性。**

**3. 灵活性：NAT可以根据网络管理员的配置进行灵活的地址映射和端口转换，满足不同网络需求。**

**4. 减少IP地址消耗：由于私有IP地址可以在多个网络中重复使用，NAT减少了对公共IP地址的需求，节省了IP地址资源。**

**总结来说，网络地址转换（NAT）是一种将私有IP地址转换为公共IP地址的技术，通过地址和端口的映射，实现了多个设备共享一个公共IP地址的功能，解决了IPv4地址不足的问题。它在网络中扮演着重要的角色，提供了地址共享、安全性增强、灵活性和节省IP地址资源等优势。**

MPLS的三个方面的特点

**1. 标签交换：MPLS使用标签来进行数据包的转发和路由。每个数据包都会附加一个标签，该标签根据网络中定义的转发表来确定下一跳路径。这种标签交换的方式可以提高数据包的转发速度和路由效率，因为它不需要每次都进行复杂的查找和解析IP地址。**

**2. 虚拟专用网络（VPN）支持：MPLS可以用于构建虚拟专用网络，即将不同的用户或组织的数据流隔离开来，就好像它们在物理上是分开的网络一样。MPLS使用标签来标识和区分不同的VPN流量，从而实现安全和可靠的数据隔离。**

**3. 服务质量（QoS）保证：MPLS提供了对不同类型流量的服务质量保证。通过为数据包附加特定的服务质量标签，网络可以根据这些标签对数据包进行分类和优先处理。这样可以确保实时流量（如语音或视频）获得较低的延迟和更高的带宽，从而提供更好的用户体验。**

MPLS基本工作过程的解释

**1. 标签分配：当数据包进入MPLS网络时，路由器会为该数据包分配一个唯一的标签。这个标签用于标识数据包的转发路径。**

**2. 标签交换：路由器根据数据包的目的地址和预先建立的路由表，将数据包的原始标签替换为下一跳路由器的标签。这样，数据包可以沿着预先定义的转发路径传输。**

**3. 标签转发：在数据包传输过程中，每个路由器都根据数据包的标签进行转发决策。它查找标签转发表，将数据包发送到正确的输出接口，使其沿着正确的路径到达目的地。**

**4. 标签删除：当数据包到达目的地时，最后一个路由器会删除数据包的标签，将其转换回普通的IP数据包，并将其交付给最终的目的地。**

UDP和TCP的特点

**UDP（用户数据报协议）的特点是：**

**1. 面向无连接：UDP不需要在发送数据之前建立连接，因此发送数据的开销较小。**

**2. 不可靠性：UDP不提供数据包的可靠传输，因此数据包可能会丢失、重复或者乱序到达。**

**3. 快速性：由于UDP不需要进行连接的建立和维护，所以传输速度相对较快。**

**4. 无拥塞控制：UDP不具备拥塞控制机制，因此在网络拥塞时，可能会导致丢包增加。**

**TCP（传输控制协议）的特点是：**

**1. 面向连接：在进行数据传输之前，TCP需要先建立连接，确保通信双方的可靠连接。**

**2. 可靠性：TCP提供可靠的数据传输，通过序号、确认和重传机制来确保数据包的可靠性。**

**3. 慢启动和拥塞控制：TCP具有慢启动和拥塞控制机制，可以根据网络的拥塞程度动态调整发送数据的速率，以避免网络拥塞。**

**4. 有序性：TCP能够确保数据包按照发送顺序到达接收端。**

可靠传输的工作原理：停止等待协议

**1. 发送方发送数据包：发送方将数据分割成较小的数据包，并逐个发送给接收方。每个数据包都带有一个唯一的序列号，以便接收方可以按顺序重新组装数据。**

**2. 等待确认：发送方在发送每个数据包后等待接收方发送确认信息。如果发送方在一定时间内未收到确认信息，它会认为该数据包已丢失或损坏，并重新发送该数据包。**

**3. 接收方确认：接收方在接收到每个数据包后发送确认信息给发送方。确认信息中包含接收到的数据包的序列号，表示已成功接收。**

**4. 丢失数据包的处理：如果发送方在等待确认期间未收到确认信息，它会假定该数据包已丢失，并重新发送该数据包。接收方在接收到重复的数据包时，会丢弃重复的数据包，并发送之前已接收到的最后一个数据包的确认信息，以便发送方知道数据包已经到达。**

**5. 顺序控制：接收方根据数据包的序列号将数据包按正确的顺序重新组装成完整的数据。**

连续ARQ协议

**连续ARQ协议是一种数据传输协议，用于在计算机网络中实现可靠的数据传输。它允许接收方确认接收到的数据，并在发生错误或数据丢失时请求发送方重新发送数据。**

**在连续ARQ协议中，发送方按顺序发送数据包，并等待接收方的确认。接收方收到数据后，会发送确认消息给发送方，指示成功接收到数据。如果发送方在一定时间内没有收到确认消息，或者接收方发送了一个否定确认消息（NACK），则发送方会认为数据包丢失或损坏，并重新发送该数据包。这个过程会一直重复，直到接收方正确接收到数据。**

**连续ARQ协议有两种常见的实现方式：停-等协议和选择重传协议。**

**停-等协议是最简单的连续ARQ协议。在停-等协议中，发送方发送一个数据包后会停止发送并等待确认消息，只有在接收到确认消息后才发送下一个数据包。这种方式效率较低，因为发送方需要等待确认消息才能发送下一个数据包。**

**选择重传协议提高了效率。在选择重传协议中，发送方可以连续发送多个数据包而不需要等待确认消息。接收方收到数据包后，会按顺序缓存这些数据包，并发送一个累积确认消息，指示成功接收到一系列连续的数据包。如果接收方发现有数据包丢失或损坏，它可以发送一个选择性确认消息，指示发送方重新发送特定的数据包。**

**连续ARQ协议通过不断重传数据包来确保可靠的数据传输，同时利用确认消息和选择性确认消息来优化传输效率。它在现代计算机网络中广泛应用，以确保数据的可靠性和完整性。**

控制TCP报文段发送时机的几种机制

**1. 慢启动：TCP连接开始时，发送方先以一个较小的拥塞窗口大小开始发送数据，然后根据网络的拥塞情况逐渐增加拥塞窗口的大小，以实现较快的数据传输。**

**2. 拥塞避免：一旦慢启动阶段结束，发送方会进入拥塞避免阶段。在这个阶段，发送方会逐渐增加拥塞窗口的大小，但增加的速度较慢，以避免过度拥塞网络。**

**3. 快速重传：当发送方收到接收方对于某个报文段的重复确认时，发送方会立即重传该报文段，而不必等待超时定时器的触发。这可以加快数据的传输速度。**

**4. 快速恢复：快速重传和快速恢复是一起使用的机制。当发送方接收到重复确认时，不仅会进行快速重传，还会将拥塞窗口的大小减半，而不是将其置为1（如慢启动阶段）。然后，发送方进入快速恢复状态，逐渐增加拥塞窗口的大小。**

TCP的发送缓存和接收缓存的作用

**发送缓存位于发送方的应用层和传输层之间，用于暂存待发送的数据。发送方应用程序通过将数据写入发送缓存，将数据传递给传输层的TCP协议。发送缓存允许发送方以适当的速率发送数据，并且可以对数据进行排序、分段和重组。此外，发送缓存还可以在网络拥塞或传输错误的情况下重新发送丢失的数据，确保数据的可靠传输。**

**接收缓存位于接收方的传输层和应用层之间，用于接收和存储接收到的数据。当接收方的TCP协议从网络中接收到数据时，它会将数据暂存到接收缓存中，然后通知接收方的应用程序来读取数据。接收缓存允许接收方以适当的速率接收数据，并且可以对数据进行排序和重组。此外，接收缓存还可以控制数据流量，防止接收方的应用程序被过多的数据压倒。**

**通过使用发送缓存和接收缓存，TCP协议能够提供可靠的数据传输服务。发送缓存和接收缓存的大小可以根据网络条件和应用程序需求进行配置，以平衡数据传输的效率和性能。**

超时重传时间的选择

**1. 网络延迟：网络延迟是指数据从发送方到接收方所需要的时间。如果网络延迟较高，那么超时重传时间应该相应增加，以允许足够的时间让数据在网络上传输完成。否则，过早触发重传机制可能会导致不必要的重传，影响网络性能。**

**2. 网络拥塞：网络拥塞是指网络中的流量过大，导致数据包丢失或延迟增加的情况。在拥塞的网络环境中，超时重传时间应该设置得较短，以尽快发现丢失的数据包并进行重传，从而减少网络拥塞的程度。**

**3. 数据重要性：不同的应用对数据的重要性有不同的要求。对于一些实时性要求较高的应用，如视频会议或实时游戏，超时重传时间应该设置得较短，以确保数据及时到达。而对于一些非实时性要求较高的应用，如电子邮件传输，超时重传时间可以设置得较长，以提高网络的吞吐量。**

**4. 重传机制的效率：超时重传时间的选择还应考虑重传机制的效率。如果超时时间设置得过长，可能会导致不必要的等待时间，降低网络的响应速度。相反，如果超时时间设置得过短，可能会导致频繁的重传，增加网络的负担。因此，需要综合考虑网络状况和重传机制的效率，选择一个合理的超时重传时间。**

Nagle算法

**Nagle算法是一种优化TCP（传输控制协议）数据传输的算法。它的目标是减少网络中的小型数据包数量，从而提高网络的效率和吞吐量。**

**Nagle算法的原理是，在发送TCP数据之前，先将较小的数据包缓存起来，直到一定条件满足时再发送。这个条件包括两个方面：第一，之前发送的数据包已经收到了对应的确认信息；第二，当前发送的数据量已经达到了一个阈值（通常为MSS，即最大报文段长度）。**

**通过将较小的数据包合并成较大的数据块发送，Nagle算法可以减少网络中的报文数量，从而降低了网络的拥塞程度和传输延迟。这对于某些应用场景，如通过网络进行实时音视频传输或远程控制操作，特别有益。**

**下面是一个示例来说明Nagle算法的工作原理：**

**假设有一个应用程序需要发送三个小型数据包（A、B和C），每个数据包的大小都比MSS小。在没有使用Nagle算法的情况下，应用程序会立即发送这三个数据包。**

**而使用Nagle算法时，应用程序会先发送数据包A，然后等待接收到对A的确认信息。接着，应用程序会发送数据包B，并等待对B的确认信息。最后，应用程序会发送数据包C，并等待对C的确认信息。这样就将三个小型数据包合并成了三个较大的数据块，减少了网络中的报文数量。**

**总结：Nagle算法通过缓存小型数据包并合并发送，以减少网络中的报文数量，提高网络效率和吞吐量。**

糊涂窗口综合症

**糊涂窗口综合症是指在计算机网络中，由于网络传输的不确定性和延迟导致的数据包到达顺序混乱的现象。**

**示例：**

**假设有两个主机A和B进行数据传输，A发送了三个数据包，编号为1、2、3，依次发送到B。由于网络传输的不确定性，这些数据包可能会以不同的顺序到达B。在正常情况下，B应该按照编号的顺序接收这些数据包，但由于糊涂窗口综合症的影响，数据包的接收顺序可能会变得混乱。**

**例如，B可能首先接收到数据包2，然后接收到数据包3，最后才接收到数据包1。这导致了数据包的顺序错乱，给后续的数据处理和应用程序造成了困扰。**

**糊涂窗口综合症的主要原因是网络中的拥塞、丢包和延迟等因素。这些因素会导致数据包在传输过程中发生乱序，使得接收方无法按照发送方的顺序正确地重组数据包。**

**为了解决糊涂窗口综合症，常用的方法是通过序列号、确认应答和重传机制来确保数据包的有序传输。TCP协议中的滑动窗口机制就是一种常见的解决方案，它可以跟踪和管理数据包的顺序，确保它们按照正确的顺序到达目标主机。**

**总结：糊涂窗口综合症是指在计算机网络中由于不确定性和延迟导致数据包到达顺序混乱的现象。为了解决这个问题，可以使用序列号、确认应答和重传机制等方法来确保数据包的有序传输。**

拥塞控制的算法：慢开始、拥塞避免、快重传、快恢复

**1. 慢开始算法：**

**慢开始算法是一种用于拥塞控制的算法，它用于确定发送方的起始发送速率。在开始发送数据时，发送方以指数级增加发送窗口的大小，以探测网络的拥塞程度。具体而言，发送方初始将发送窗口设置为一个较小的值，然后每经过一个往返时间（RTT），将发送窗口的大小加倍。这样逐渐增加的发送窗口可以有效地利用网络的带宽，并且在网络出现拥塞之前逐步增加发送速率。**

**2. 拥塞避免算法：**

**拥塞避免算法是用于在网络中避免拥塞的一种算法。一旦慢开始阶段结束，发送方将进入拥塞避免阶段。在拥塞避免阶段，发送方以线性增加的方式增加发送窗口的大小，而不是指数级增加。这样可以防止发送方在网络中发送过多的数据，从而避免引发拥塞。此算法通常使用拥塞窗口（cwnd）来控制发送方的发送速率。**

**3. 快重传算法：**

**快重传算法是一种用于快速恢复丢失数据的算法。当接收方发现一个数据包丢失时，通常会发送一个重复确认（duplicate ACK）给发送方。发送方在收到一定数量的重复确认后，就可以推断出某个数据包已经丢失，并立即进行重传，而不必等待超时定时器的触发。这样可以更快地恢复丢失的数据，提高网络的传输效率。**

**4. 快恢复算法：**

**快恢复算法是与快重传算法配合使用的一种拥塞控制算法。当发送方接收到一定数量的重复确认时，它会将拥塞窗口减半，并将拥塞窗口的大小设置为拥塞避免阈值的一半。然后，发送方进入快恢复阶段，每收到一个新的确认时，将拥塞窗口的大小增加一个数据包的大小。这样可以在网络中更快地进行重传，并逐渐增加发送速率，以恢复到正常的发送状态。**

绘制TCP连接和连接释放的过程图、并说明

**TCP连接建立的过程：**

**1. 主机A想要与主机B建立TCP连接，首先主机A发送一个带有SYN（同步）标志的TCP报文段给主机B。**

**2. 主机B接收到主机A发送的SYN报文段后，会向主机A发送一个带有SYN/ACK（同步/确认）标志的TCP报文段。**

**3. 主机A收到主机B发送的SYN/ACK报文段后，会再次向主机B发送一个带有ACK（确认）标志的TCP报文段，确认主机B的响应。**

**4. 主机B接收到主机A发送的ACK报文段后，TCP连接建立完成，主机A和主机B之间可以开始进行数据传输。=**

**TCP连接释放的过程：**

**1. 当主机A或主机B的应用程序需要关闭TCP连接时，会发送一个带有FIN（结束）标志的TCP报文段给对方。**

**2. 接收到FIN报文段的一方（例如主机B）会发送一个ACK报文段作为确认。**

**3. 在发送ACK报文段之后，接收到FIN和ACK报文段的一方会进入"半关闭"状态，仍然可以发送数据，但不再接收新的数据。**

**4. 如果另一方（例如主机A）也希望关闭连接，它会发送一个带有FIN标志的TCP报文段。**

**5. 接收到FIN报文段的一方会发送一个ACK报文段进行确认，并进入"时间等待"状态，等待一段时间以确保对方收到ACK报文段。**

**6. 在"时间等待"状态结束后，连接释放完成，TCP连接彻底关闭。**

**TCP连接建立过程中，双方通过交换带有SYN和ACK标志的TCP报文段来协商连接参数并确认对方的响应，从而建立连接。TCP连接释放过程中，双方通过交换带有FIN和ACK标志的TCP报文段来协商关闭连接，并确认对方的响应，最终关闭连接。**

DNS的域名解析过程

**1. 用户在浏览器中输入要访问的域名（例如www.example.com）。**

**2. 操作系统中的DNS解析器接收到该请求，首先检查本地缓存中是否有对应的IP地址。如果有，解析过程就结束了，直接返回缓存中的IP地址。**

**3. 如果本地缓存中没有对应的IP地址，DNS解析器将向本地配置的首选DNS服务器发送解析请求。**

**4. 首选DNS服务器收到解析请求后，首先查看自身的缓存，如果有对应的IP地址，则返回给解析器。**

**5. 如果首选DNS服务器的缓存中没有对应的IP地址，它将依次向根域名服务器、顶级域名服务器和权威域名服务器发送请求，直到找到负责该域名的权威域名服务器。**

**6. 权威域名服务器收到请求后，会返回该域名对应的IP地址给首选DNS服务器。**

**7. 首选DNS服务器将接收到的IP地址存储在本地缓存中，并将该IP地址返回给操作系统的DNS解析器。**

**8. 操作系统将获取到的IP地址返回给浏览器，浏览器使用该IP地址与目标服务器建立连接。**

**9. 一旦连接建立，浏览器就能够向目标服务器发送HTTP请求，并获取相应的网页内容。**

万维网必须解决的几个问题

**1. 信息过载：随着互联网的发展和普及，海量的信息在万维网上产生并不断增长。这导致用户在搜索和获取所需信息时面临信息过载的问题。因此，万维网需要提供有效的搜索引擎和信息过滤机制，帮助用户快速准确地找到所需信息。**

**2. 数据安全和隐私：万维网上的信息传输往往包含用户的个人数据和敏感信息。确保数据的安全性和用户隐私成为万维网必须解决的问题。这需要采取适当的加密和认证措施，确保信息在传输和存储过程中得到保护。**

**3. 网络速度和性能：万维网的用户数量庞大，网络流量巨大，因此网络速度和性能成为一个重要问题。为了提供良好的用户体验，万维网需要不断改进网络基础设施，提高网络带宽和响应速度，以满足用户对快速访问和加载内容的需求。**

**4. 跨平台和跨浏览器兼容性：万维网是一个开放的平台，用户使用不同的操作系统和浏览器来访问网页。为了确保用户在不同平台和浏览器上都能正常访问和浏览网页，万维网需要解决跨平台和跨浏览器的兼容性问题，使网页能够在各种环境下正确显示和运行。**

HTTP的代理服务器

**HTTP代理服务器是一种位于客户端和服务器之间的中间服务器，它充当客户端和服务器之间的中转角色。当客户端发送HTTP请求时，请求首先发送给代理服务器，然后代理服务器再将请求发送给目标服务器。类似地，当服务器返回响应时，响应首先发送给代理服务器，再由代理服务器转发给客户端。**

**HTTP代理服务器有以下几个主要功能：**

**1. 缓存：代理服务器可以缓存已请求的资源。当客户端再次请求相同的资源时，代理服务器可以直接返回缓存的副本，而无需再次向目标服务器发送请求，从而提高响应速度和减轻服务器负载。**

**2. 过滤和防火墙：代理服务器可以根据配置规则对HTTP请求和响应进行过滤，例如阻止某些特定的URL访问或屏蔽特定的内容。这有助于提高网络安全性和保护用户隐私。**

**3. 匿名化：通过使用代理服务器，客户端可以隐藏其真实的IP地址和身份，从而实现一定程度的匿名化。**

**4. 负载均衡：代理服务器可以作为负载均衡器，将客户端请求分发到多个服务器上，从而平衡服务器的负载，提高系统的性能和可靠性。**

**HTTP代理服务器在网络中起到了重要的作用，可以改善性能、提供安全性和保护隐私，并支持更高级的网络功能。**

点击 URL http://\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*后所发生的事件

**1. DNS 解析：计算机首先会将 URL 中的域名部分发送给 DNS 服务器，以获取对应的 IP 地址。这个步骤是为了将域名转换为可识别的 IP 地址。**

**2. 建立 TCP 连接：使用获取到的 IP 地址，计算机将与目标服务器建立 TCP 连接。这是为了确保可靠的数据传输，它涉及三次握手过程，即建立连接、确认连接、建立连接确认。**

**3. 发送 HTTP 请求：一旦建立了 TCP 连接，计算机会发送一个 HTTP 请求给目标服务器。这个请求中包含了用户需要获取的资源的信息，如请求类型（GET、POST 等）、请求头和请求体。**

**4. 服务器处理请求：目标服务器接收到请求后，会根据请求的内容进行处理。这可能涉及到查询数据库、执行应用程序等操作，以生成相应的数据。**

**5. 服务器发送 HTTP 响应：一旦服务器处理完请求，它会生成一个 HTTP 响应，其中包含了请求的结果或所需的资源。响应中还包括响应头和响应体等信息。**

**6. 接收 HTTP 响应：计算机接收到服务器发送的 HTTP 响应后，会解析响应头和响应体，以获取所需的数据。**

**7. 关闭 TCP 连接：在完成数据传输后，计算机会关闭与服务器之间的 TCP 连接，释放网络资源。**

三种万维网文档

**1. HTML（超文本标记语言）文档：HTML是一种用于创建网页的标记语言。它通过标签和元素描述了网页的结构和内容，包括标题、段落、链接、图像等。HTML文档是万维网的基础，由浏览器解析和呈现给用户。**

**2. CSS（层叠样式表）文档：CSS是一种用于定义网页样式和布局的标记语言。它通过选择器和属性来控制HTML文档中元素的外观和排版方式。CSS文档与HTML文档结合使用，可以改变文档的字体、颜色、大小、间距等外观特征，提供更丰富的用户界面设计。**

**3. JavaScript脚本：JavaScript是一种用于增强网页交互性和功能的编程语言。它可以嵌入到HTML文档中，通过处理用户的输入、操作文档对象模型（DOM）以及与服务器进行通信等方式，实现动态效果和实时更新。JavaScript脚本使得网页能够响应用户的操作，并实现复杂的交互功能。**

电子邮件的三个主要组成构建

**1. 邮件头部（Header）：邮件头部包含了诸如发件人、收件人、主题、日期和其他元数据等信息。这些信息提供了有关邮件的基本信息，帮助邮件系统进行正确的路由和处理。**

**2. 邮件正文（Body）：邮件正文是电子邮件的主要内容部分，其中包含了实际的文本信息。邮件正文可以包含文字、图片、链接和格式化的内容等。**

**3. 附件（Attachment）：附件是邮件中可以包含的其他文件，如文档、照片、音频或视频文件等。附件使得邮件可以携带和传输各种类型的文件，方便用户在邮件中分享和接收多媒体内容。**

用户代理的４个功能

**1. 发起请求（Requesting）：用户代理能够向服务器发送请求，请求获取特定的资源或执行某项操作。例如，在Web浏览器中，用户代理可以向Web服务器发送HTTP请求以获取网页内容。**

**2. 处理响应（Handling Responses）：用户代理接收并处理服务器返回的响应。这包括解析响应，提取所需的信息，并将其呈现给用户。在Web浏览器中，用户代理会解析服务器返回的HTML响应，并将其显示为网页。**

**3. 维护用户状态（Maintaining User State）：用户代理可以跟踪和维护与用户相关的状态信息。这些状态信息可以包括会话数据、cookie、缓存等。通过维护用户状态，用户代理可以提供个性化的服务，例如保存用户偏好设置、保持用户登录状态等。**

**4. 提供界面（Providing User Interface）：用户代理为用户提供了与网络交互的界面。这包括图形用户界面（GUI）、命令行界面（CLI）或其他形式的界面。用户代理通过这些界面使用户能够与网络进行交互，发送请求、查看响应和浏览资源。**

SMTP通信的三个阶段

**1. 连接建立阶段：在这个阶段，客户端应用程序（如电子邮件客户端）与邮件服务器建立TCP连接。客户端通过向服务器发送"HELO"命令来启动连接。服务器确认连接后，客户端可以开始发送邮件。**

**2. 邮件传输阶段：在这个阶段，客户端向服务器发送邮件内容。客户端通过使用"MAIL FROM"命令指定发件人地址，并使用"RCPT TO"命令指定收件人地址。然后，客户端发送实际邮件内容，包括主题、正文和附件。服务器接收并保存邮件内容。**

**3. 连接关闭阶段：在这个阶段，客户端发送"QUIT"命令来关闭与服务器的连接。服务器确认关闭连接，并断开与客户端的TCP连接。**

1-10、1-11、1-19、1-28、1-34、1-35、1-36

概述

2-9、2-16、

物理层

3-07、3-20，3-24、3-25、3-26、3-30、3-33

数据链路

4-15、4-18、4-19、4-20、4-22、4-24、4-25、4-26、4-28、4-29、4-31、4-33、4-37、4-38、4-39、4-47、4-48、4-63、4-66、4-67

网络

5-13、5-21、5-23、5-24、5-33、5-34、5-35、5-39、5-47、5-49、5-61

运输