一、名词解释 协议
隧道技术 抖动 广播 抖动

1. 协议（Protocol）：在计算机领域中，协议是指计算机系统中规定的一系列通信标准或规则，用于在网络中进行数据传输和通信。协议包含了通信所需的各种规范和约定，如数据格式、传输速率、错误检测和纠正方法、数据传输控制、通信安全等等。
2. 隧道技术（Tunneling）：隧道技术是在计算机网络中用于将一种网络协议的数据包封装在另一种网络协议中进行传输的技术。隧道技术主要用于连接不同类型的网络或绕过网络屏障，如防火墙、代理服务器等。
3. 抖动（Jitter）：抖动是指在数据传输过程中，数据包到达接收方的时间不稳定，出现波动的现象。抖动通常由网络拥塞、网络延迟、网络故障等原因引起，会对音视频传输等实时应用产生影响。
4. 广播（Broadcast）：广播是指在计算机网络中，向同一网络中的所有计算机发送数据的操作。广播通常用于向所有计算机发送网络广告、路由信息等。广播虽然便于信息传输，但也会对网络带宽和安全性产生影响，因此在网络中应该谨慎使用。

计算机网络目的
哪个是广播共享信道
能够根据传输的流量确定收费，是选项中的哪种网络
给定一个IP和子网掩码，选项中哪一个IP属于同一个子网
哪个不是数据链路层设备
以太网帧地址长度

1. 计算机网络的主要目的是使不同的计算机和设备能够相互通信和交换信息。具体而言，计算机网络的目的包括资源共享、信息传递、数据存储和处理、协作工作等方面。
2. 广播是一种共享信道的方式，其中一个设备向所有其他设备发送数据。因此，广播是广播共享信道的一种。
3. 能够根据传输的流量确定收费的网络是计量网络。计量网络是一种按照实际使用量来计费的网络，通常用于互联网接入、云计算等场景。
4. 给定一个IP和子网掩码，如果两个IP地址的网络地址部分相同，那么它们属于同一个子网。
5. 打印机是数据链路层设备的一种。数据链路层设备包括网桥、交换机、网卡等。
6. 以太网帧地址长度是6个字节，其中前3个字节是目标MAC地址，后3个字节是源MAC地址。

1. 分组进入路由器后，如何根据路由表项进行转发。若有多个匹配，应该怎么处理，为 什么?

当分组进入路由器后，路由器会根据分组的目标IP地址查找路由表，以确定下一跳的转发路径。具体而言，路由器会将分组的目标IP地址与路由表中的每个表项进行匹配，以找到最匹配的路由表项，然后根据该路由表项中的出接口，将分组转发到下一跳。

如果有多个匹配的路由表项，通常会选择最长匹配的路由表项进行转发。最长匹配指的是，在路由表中找到与分组目标IP地址最长匹配的路由表项，其中匹配的位数最多的那个路由表项就是最长匹配路由表项。这种匹配方式的原因是，最长匹配能够保证分组被转发到正确的下一跳，并且能够减少不必要的路由器处理开销。

例如，假设有两个路由表项分别为：

10.0.0.0/8
10.1.0.0/16

当一个分组的目标IP地址为10.1.2.3时，路由器会选择第二个路由表项，因为它的匹配位数更多，匹配更精确。如果没有最长匹配规则，路由器可能会根据第一个路由表项转发分组，这将导致分组被错误地路由到了错误的网络。

17

2. 网桥流量过滤原理，以及查找表的建立过程

网桥是一种数据链路层设备，主要用于将多个局域网互联。网桥的流量过滤原理是基于MAC地址进行过滤。当网桥收到一个分组时，它会将分组的源MAC地址记录在一个MAC地址表中，然后查找MAC地址表，以确定分组的下一跳。

具体而言，网桥会根据分组的目标MAC地址查找MAC地址表，以确定下一跳的转发路径。如果目标MAC地址在MAC地址表中存在，则网桥会将分组转发到该目标MAC地址所对应的端口；否则，网桥会将分组转发到所有的端口（除了接收该分组的端口）。

建立MAC地址表的过程是通过学习实现的。当网桥收到一个分组时，它会将分组的源MAC地址记录在MAC地址表中，并与接收该分组的端口关联。如果该MAC地址已经存在于MAC地址表中，网桥会更新该MAC地址的关联端口信息。这样，随着时间的推移，网桥会逐渐学习到哪些MAC地址可以通过哪些端口访问，从而建立MAC地址表。

17

3.
简述CRC进行校验的过程

CRC（循环冗余校验）是一种在数据通信中广泛使用的校验方法，用于检测数据在传输过程中是否出现了错误。

CRC的校验过程基于除法运算。在发送端，数据帧的末尾附加一个CRC校验码，并将整个数据帧发送到接收端。接收端在收到数据帧后，对整个数据帧（包括CRC校验码）进行除法运算，得到余数。如果余数为0，则表明数据没有出现错误；否则，数据出现了错误。

具体而言，CRC的校验过程如下：

1. 选择一个固定的生成多项式，比如x^16 + x^12 + x^5 + 1，作为除数。
2. 将数据帧和一个固定的初值（通常为0）作为除数进行除法运算，得到余数。
3. 将余数附加在数据帧的末尾，得到带有CRC校验码的数据帧，并将其发送到接收端。
4. 在接收端，接收到带有CRC校验码的数据帧后，将整个数据帧作为除数进行除法运算，得到余数。
5. 检查余数是否为0。如果余数为0，则数据没有出现错误；否则，数据出现了错误。

需要注意的是，CRC算法的校验能力是有限的，即存在一定的错误检测概率。因此，在实际应用中，通常会采用更加复杂的纠错码来提高数据传输的可靠性。

17

4. 描述ARP原理

ARP（地址解析协议）是一种用于将IP地址映射到MAC地址的协议，主要用于局域网中的数据通信。当一台主机需要与另一台主机通信时，它首先需要知道目标主机的MAC地址，而ARP协议就是用来解决这个问题的。

ARP协议的工作原理如下：

1. 发送ARP请求
   当一台主机需要发送数据到另一台主机时，它首先检查自己的ARP缓存表中是否有目标主机的MAC地址。如果缓存中没有该地址，则主机会发送一个ARP请求广播帧，包含目标主机的IP地址。此时，所有连接到同一网络的主机都能收到该广播帧。
2. 接收ARP请求并响应
   当目标主机收到ARP请求后，它会检查请求中的IP地址是否与自己的IP地址匹配。如果匹配，则目标主机会向发送ARP请求的主机发送一个ARP响应广播帧，包含自己的MAC地址。此时，所有连接到同一网络的主机都能收到该广播帧。

3. 更新ARP缓存表
   发送ARP请求的主机在接收到ARP响应后，将目标主机的MAC地址存储在自己的ARP缓存表中。这样，下一次发送数据时就可以直接使用该MAC地址了。

需要注意的是，ARP协议只能在局域网中使用，因为它依赖于广播机制，而广播消息只能在同一局域网内传递。如果需要跨越不同的网络进行通信，就需要使用路由器来转发数据。

17

5. 电话系统是题目给出的背景 a) 本地回路的主要技术，实现方式 b) 交换局的主要技术，实现方式 c) 干线的主要技术，实现方式 d) 为什么不采用平面系统，而是采用分层系统

a) 本地回路的主要技术和实现方式：本地回路是电话系统中的一部分，用于连接用户的电话设备和电话交换机。它的主要技术是双绞线，这是一种由两根绝缘的铜线缠绕在一起而成的电缆。这种电缆的特点是成本低廉，安装方便，可以支持高速数据传输和双向通信。

b) 交换局的主要技术和实现方式：电话交换机是电话系统中的一个重要组成部分，它用于实现电话之间的连接和交换。交换局的主要技术是电子交换，它使用计算机控制和数字信号处理技术，将用户之间的通信连接起来。交换局中的核心设备是交换机，它能够根据拨号信号和用户号码将呼叫连接到正确的终端设备上。

c) 干线的主要技术和实现方式：干线是连接不同交换局之间的电话线路，它用于长距离电话通信。干线的主要技术是光纤通信，这是一种使用光纤传输数字信号的技术。光纤通信具有高速传输、大带宽、抗干扰等优点，因此被广泛应用于电话系统中的干线传输。

d) 为什么不采用平面系统而是采用分层系统：电话系统采用分层系统的主要原因是为了提高系统的可靠性和可维护性。分层系统将电话系统分为多个层次，每个层次之间的接口明确，各层之间相互独立，这样就能够降低系统的复杂度，便于维护和升级。同时，分层系统还能够提高系统的可靠性，因为每个层次都有独立的功能和任务，出现故障时能够更容易地定位和解决问题。相比之下，平面系统的结构比较简单，但是不利于扩展和升级，而且容易受到单点故障的影响，因此在大规模电话系统中不适合采用。

17

1. 数据链路层 a) 如何实现差错控制¡ b）如何实现流量控制

a) 差错控制是数据链路层中的重要功能，用于检测和纠正在数据传输过程中可能发生的差错。差错控制主要包括两个方面：奇偶校验和循环冗余校验（CRC）。

奇偶校验是一种简单的差错控制技术，它利用二进制位中1的个数的奇偶性来检测数据是否发生错误。在发送数据时，发送方将数据的二进制位按照一定的规则进行组合，使得组合后的数据中包含奇数个1或偶数个1。接收方在接收数据后，利用相同的规则对数据进行组合，并统计组合后的数据中1的个数。如果接收方统计出来的1的个数与发送方不同，则说明数据在传输过程中发生了差错。

循环冗余校验（CRC）是一种更为复杂的差错控制技术，它利用多项式除法的原理来检测数据是否发生错误。在发送数据时，发送方根据事先约定好的生成多项式，对数据进行除法运算，并将余数附加在数据帧的尾部。接收方在接收数据后，也利用相同的生成多项式对数据进行除法运算，并计算出余数。如果接收方计算出的余数不为零，则说明数据在传输过程中发生了差错。

b) 流量控制是数据链路层中的另一个重要功能，用于协调发送方和接收方之间的数据传输速度，避免数据的拥塞和丢失。数据链路层中实现流量控制的主要技术是停止等待协议和滑动窗口协议。

停止等待协议是一种简单的流量控制技术，它要求发送方每发送一帧数据就停止发送并等待接收方的确认帧。接收方在收到数据帧后，如果没有发生差错，就向发送方发送确认帧。发送方在收到确认帧后，才能继续发送下一帧数据。

滑动窗口协议是一种更为复杂的流量控制技术，它允许发送方连续发送多个数据帧，而不需要等待每个数据帧的确认帧。滑动窗口协议中，发送方和接收方各维护一个滑动窗口，用于协调数据的传输速度。发送方根据接收方的窗口大小来发送数据帧，接收方在收到数据帧后，如果没有发生差错，就向发送方发送确认帧，并将滑动窗口向前


17

2. 介质访问控制访问 a) 有线局域网介质控制的协议、原理 b) 无线局域网介质控制的协议、原理

a) 有线局域网介质访问控制协议和原理：
在有线局域网中，常见的介质访问控制协议包括CSMA/CD、令牌环和令牌总线。

CSMA/CD：即载波侦听多路访问/冲突检测。该协议通过在发送数据前先监听信道，确保信道上没有其他节点正在发送数据，避免数据碰撞。如果发现数据碰撞，就发送一个干扰信号来终止发送，然后采用退避算法，等待一段随机时间后再次尝试发送。
令牌环：在令牌环中，网络中的每个节点都按顺序连接成一个环状结构，通过传递一个特殊的令牌来控制数据的访问。当一个节点要发送数据时，需要等待令牌到达自己这里，然后将数据放入令牌中传递给下一个节点。如果一个节点没有数据要发送，就将令牌继续传递下去。这样，每个节点都可以控制自己的发送速率。
令牌总线：在令牌总线中，网络中的每个节点都连接到一个公共的总线上，通过发送一个特殊的令牌来控制数据的访问。当一个节点要发送数据时，需要等待令牌到达自己这里，然后将数据放入令牌中传递给下一个节点。如果一个节点没有数据要发送，就将令牌继续传递下去。这样，每个节点都可以控制自己的发送速率。

b) 无线局域网介质访问控制协议和原理：
在无线局域网中，常见的介质访问控制协议包括CSMA/CA和TDMA。

CSMA/CA：即载波侦听多路访问/冲突避免。该协议通过在发送数据前先监听信道，避免数据碰撞。如果信道上没有其他节点正在发送数据，那么就发送数据。如果信道上有其他节点正在发送数据，就采用一种称为“随机指数退避”的算法，等待一段随机时间后再次尝试发送。此外，为了进一步减少数据碰撞，CSMA/CA还采用了一种“请求-应答”的机制，即发送方在发送数据前会先发送一个请求帧，等待接收方的应答，以确保数据能够被正确接收。
TDMA：即时分多址。该协议将时间分成若干个时隙，每个时隙只允许一个节点发送数据。因此


17

3. 链路状态协议字段含义，根据图描述可靠的扩散过程

链路状态协议（Link State Protocol，简称LSP）是路由协议中的一种，用于构建链路状态数据库（Link State Database，简称LSDB）和计算最短路径树（Shortest Path Tree，简称SPT）。LSP是在网络中的每个路由器上生成的，并在整个网络中进行分发。

链路状态协议的数据包包括以下字段：

版本号：表示LSP的版本，用于兼容不同版本的LSP。
源ID：表示生成LSP的路由器的标识符，通常是路由器的接口IP地址。
序列号：表示LSP的序列号，用于防止重复LSP的产生。
TTL：表示LSP的生存时间，用于防止LSP在网络中循环。
类型：表示LSP的类型，如点到点LSP、多点到点LSP等。
链路状态：包含了LSP生成路由器知道的所有链路信息，包括链路的ID、代价、带宽、可用性等。

当一个路由器收到一个LSP时，它将更新自己的LSDB，并根据LSDB计算出最短路径树。具体的计算方法有Dijkstra算法和SPF算法等。

在一个网络中，LSP可以通过广播和单播两种方式进行传播。在广播方式下，LSP会被发送到网络中的所有路由器；在单播方式下，LSP只会被发送到需要更新的路由器。当一个路由器发送一个LSP时，它会把LSP发送到它的相邻路由器。如果一个路由器收到了一个序列号比自己的数据库中记录的序列号要小的LSP，它就会将自己的数据库更新，并把新的LSP发送给它的相邻路由器。

链路状态协议的可靠扩散过程如下：

1. 路由器生成一个LSP，包含了它知道的所有链路状态信息，并将LSP发送给它的相邻路由器。
2. 接收到LSP的路由器检查LSP的版本号和序列号是否正确，如果正确，则更新自己的LSDB，并将新的LSP发送给它的相邻路由器。

3. 如果接收到的LSP的版本号或序列号不正确，则丢弃该LSP。
4. 如果一个路由器在一定时间内没有接收到某个相邻路由器发送的LSP，就会认为该相邻路由器已经离线，将该相邻路由器连接的链路标记为不可用，并重新计算最短路径树。
5. 当一个链路状态发生变化时（如链路带宽变化、链路断开等），路由器会生成一个新的LSP，并把它发送给它的相邻路由器

17

4. TCP a) TCP建立连接过程，如何处理重复分组 b) TCP释放连接过程，如何尽最大努力避免数据丢失

a) TCP建立连接过程如下：

1. 客户端向服务器发送SYN包，SYN包包含了客户端的初始序列号。
2. 服务器收到SYN包后，向客户端发送SYN+ACK包，确认客户端的请求，并发送自己的初始序列号。
3. 客户端收到服务器的SYN+ACK包后，向服务器发送ACK包，确认连接已经建立。

如果在建立连接的过程中发生了重复的SYN包，TCP协议会忽略重复的SYN包，只认为第一次出现的SYN包是有效的，以避免重复建立连接。

b) TCP释放连接过程如下：

1. 当一方需要关闭连接时，向对方发送FIN包，表示该方已经没有数据需要发送了。
2. 接收到FIN包的另一方向发送方回复ACK包，表示收到了关闭请求。
3. 如果发送方还有数据需要发送，它可以在发送FIN包之前发送完数据。
4. 接收方在回复ACK包之前也可以继续接收数据。

TCP协议尽可能避免数据丢失的方法是在关闭连接时使用TCP的半关闭（half-close）功能。半关闭允许一方在发送完数据后关闭连接，而另一方可以继续接收数据。这样，数据就有更大的机会被完整地传输。

17

背景是TCP
报文、ipv4、以太网帧格式。
1. 接受窗口大小如何确定 2. 拥塞窗口大小如何确定 3. 发送速率如何确定 4.
IP 画图说明以太网帧 分组， 报文关系TCP IPv4
5.TCP需要分段，计算一个段的最大长度 6. 以太网帧何时填充位不为零

1. TCP接收窗口大小的确定：
   接收窗口大小是指接收方能够接收的未确认数据的最大字节数，它决定了发送方可以发送多少数据。接收窗口大小可以通过TCP的三次握手过程中互相传递窗口大小信息而获得。接收方在建立连接时将初始的窗口大小告知发送方，发送方在发送数据时会根据接收方返回的窗口大小来控制发送数据的速率。
2. TCP拥塞窗口大小的确定：
   拥塞窗口大小是指发送方在不断检测网络状况，动态调整发送速率的过程中，为防止网络拥塞而限制自己的最大发送速率而设定的窗口大小。TCP拥塞窗口大小是由拥塞控制算法动态调整的，其目标是在网络的拥塞程度适中的情况下，使得网络的带宽利用率达到最优。拥塞窗口大小的确定方式比较复杂，需要考虑诸如网络延迟、丢包率等多个因素。
3. TCP发送速率的确定：
   TCP发送速率是通过拥塞控制算法动态调整拥塞窗口大小来控制的。发送方根据接收方的接收窗口大小和拥塞窗口大小来控制发送数据的速率。如果接收窗口比较小，发送方就会降低发送速率，避免发送太多的数据导致接收方无法接收。如果网络拥塞程度较高，发送方也会根据拥塞窗口大小降低发送速率，以减少网络拥塞程度。
4. IP和以太网帧格式的关系：
   在TCP/IP协议栈中，TCP协议是运行在传输层，IPv4协议是运行在网络层，以太网帧是运行在数据链路层。在进行TCP通信时，数据会从应用层经过传输层和网络层后被封装成IP数据包，并在数据链路层封装成以太网帧进行传输。IP数据包的源IP地址和目标IP地址分别对应于以太网帧的源MAC地址和目标MAC地址，以太网帧中还包含有关帧的类型和长度等信息。
5. TCP段的最大长度：
   TCP协议会根据MSS（最大报文段长度）来分段。MSS是指TCP报文中的数据部分的最大长度，不包括TCP头部的长度。MSS的大小可以通过TCP的三次握手过程中互相传递信息来获得。发送方在发送数据时，需要根据MSS的大小