<<<DP读书>>>

> 第八章 跨机器通讯

- 在第六章之中，介绍了一个计算机系统内线程间进程间的通信机制，对于小白（至少我）来说想要完全理解计算机中非常中重要的概念——进程，并不容易
- 啃了很久的，编译原理、处理器内核、Rt-Thread 甚至Kunpeng、openEuler社区的各种文档，才稍许有些理解

基于openEuler的TCP与UDP

- 在计算机系统领域，多机的网络互联成为越来越重要的也逐渐不容忽视的话题，很多的解决方案围绕其不断产生，对我来说值得学习。
- 开始更新了，再不更，催更都99+了。

计算机网络

本节从计算机网络的历史、分层模型、TCP/IP五层分层模型的功能特点出发，开啃！

简介

计算机网络发展形态，在历史初期分层模型用于解决计算机系统网络之间的兼容弊端。
20世纪80年代，国际化标准组织（International Standards Organization，ISO）制定了计算机网络体系结构标准及国际标准化协议，并发布了“开发系统互联参考模型”，简称OSI模型。OSI将网络协议栈分为七层的OSI模型

OSI定义了各层的功能，使计算机网络变得拓展性强、兼容性好

但是，由于OSI模型的复杂性，另一种由DARPA（Defence Advanced Research Projects Agency）创建的TCP/IP四层模型，由于更为简单，成为了主导模型

随着计算机网络的不断发展，OSI与TCP/IP 模型相融合，形成了TCP/IP五层模型，该模型沿用至今，成为计算机网络的典型模型。

图1 网络分层模型

TCP/IP协议栈

A. 物理层

- 直连两个信号间如何用信道（channel）传递信号
- TCP/IP协议栈中的物理层是负责在通信链路中传输原始比特流，包括物理媒体（如电缆、光纤等）以及连接这些媒体的物理电子设备（如调制解调器、集线器等）。在这一层，目标是确保比特流的可靠传输，以及提供数据链路层的物理接口。
- 物理层的核心功能：在直连通信中，信道通常指的是物理媒体本身，如双绞线、同轴电缆、光纤等。这些信道通过使用不同的信号编码和传输技术，能够将发送端的信号（即比特流）准确地传输到接收端。

物理层涉及一些关键概念和技术，如数据速率、传输延迟、误码率等，这些都是评估信道性能的重要参数。此外，物理层还需要处理诸如同步、信号调制和解调等问题，以确保数据能够有效地在信道上传

输。

> 数据速率是指在单位时间内传输的数据量，通常以比特率（bit rate）表示，即每秒传输的比特数。数据速率的确定取决于物理层的传输能力和信道的质量。在高速传输中，数据速率可能会受到信道带宽和信号质量的限制。

> 传输延迟是指数据从一个节点传输到另一个节点所需要的时间。它包括发送延迟、传播延迟、处理延迟和排队延迟等组成部分。在计算机网络中，传输延迟是一个重要的性能指标，它影响网络的整体性能和用户体验。

> 误码率是指数据传输过程中发生错误的比特数与总传输比特数之比。由于各种原因，如信道噪声、干扰和信号衰减等，数据在传输过程中可能会出现错误。误码率是衡量数据传输质量的一个重要指标，低误码率意味着数据传输的准确性高，而高误码率则可能导致数据传输失败或数据损坏。

在TCP/IP协议栈的物理层中，这些参数是非常重要的，因为它们直接影响着数据在网络中的传输质量和效率。通过优化物理层的设计和参数，可以降低传输延迟和误码率，提高数据传输的效率和质量。

1.信号及信道传递

信号和信道是数据传输中两个相互关联的重要概念。信号是数据在通信链路中传输的具体形式，它可以表示为随时间变化的电压或电流。在物理层中，信号的传输依赖于信道，信道是用于传输信号的物理介质。

信道可以是导线的电缆、光纤、无线电波等。根据信道类型的不同，信号的传输方式也会有所不同。例如，在双绞线或同轴电缆中，信号通常以电压的形式传输；而在光纤中，信号则通过光脉冲进行传输。

在信号的传输过程中，信道的质量和特性对信号的传输效果产生重要影响。信道的带宽、阻抗、传播延迟等参数都会影响信号的传输速率和质量。如果信道质量较差，信号可能会出现失真、噪声、衰减等现象，导致信号无法准确传输到目的地。

因此，在TCP/IP协议栈的物理层中，为了确保数据的可靠传输，需要对信道进行适当的配置和管理。这包括选择适当的传输介质、调整信号的调制方式、进行差错控制和信道均衡等措施。通过这些措施，可以有效地降低信道对信号传输的影响，提高数据传输的可靠性和效率。

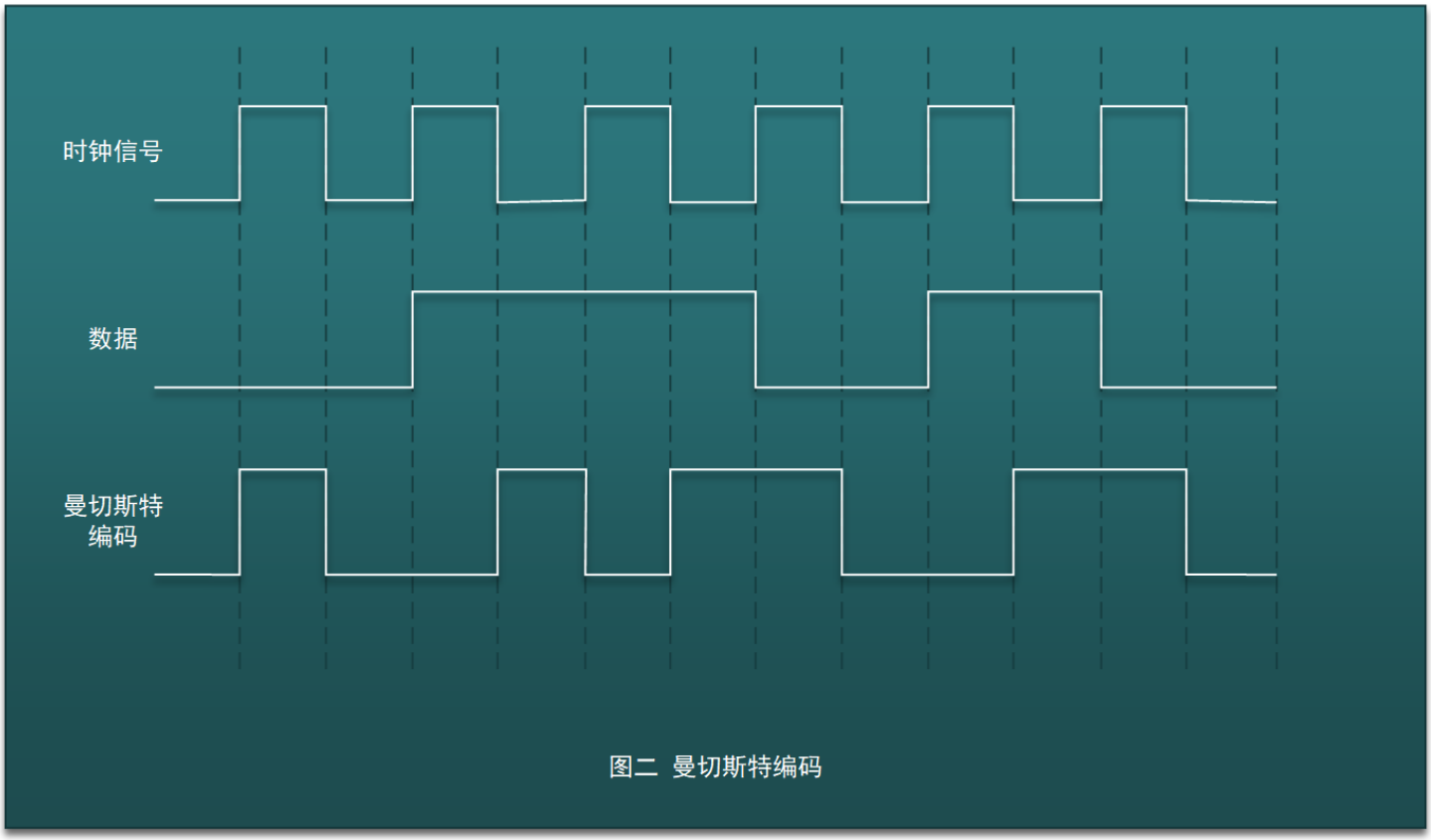
2.信号调制与调解

Line coding按照使用到的电压等级（level）不同可以分成

- 单极性码（Uni-polar Encoding）
- 极性码（Polar Encoding）

- 双极性码（Bipolar Encoding）
- 曼彻斯特编码（Manchester Encoding）
- 差分曼彻斯特编码（Differential Manchester Encoding）

常见的编码为曼切斯特编码如下：

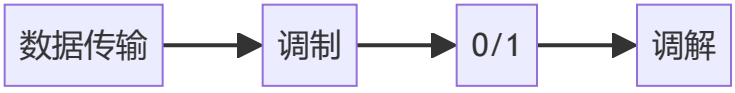


图二 曼切斯特编码

信号的调制和调解是数据传输中的重要过程。调制是将低频信号转换为高频载波信号的过程，以便在信道中传输。常见的调制方式包括调幅（AM）、调频（FM）和调相（PM）。在曼切斯特编码中，也使用了相位的调制。

而调解则是与调制相反的过程，是将高频载波信号还原为原始的低频信号。在接收端，调解器将接收到的信号解调为原始信号，以便进行处理和使用。

曼切斯特编码是一种常见的编码方式，它使用相位的跳变来表示数据。在曼切斯特编码中，每位编码的中心点都有一个跳变，可以是上升沿或下降沿，分别表示二进制数据的“1”和“0”。这种编码方式的特点是每一位的中间都有一个跳变，可以作为同步时钟信号，使得接收端能够准确地判断数据的起始和结束。



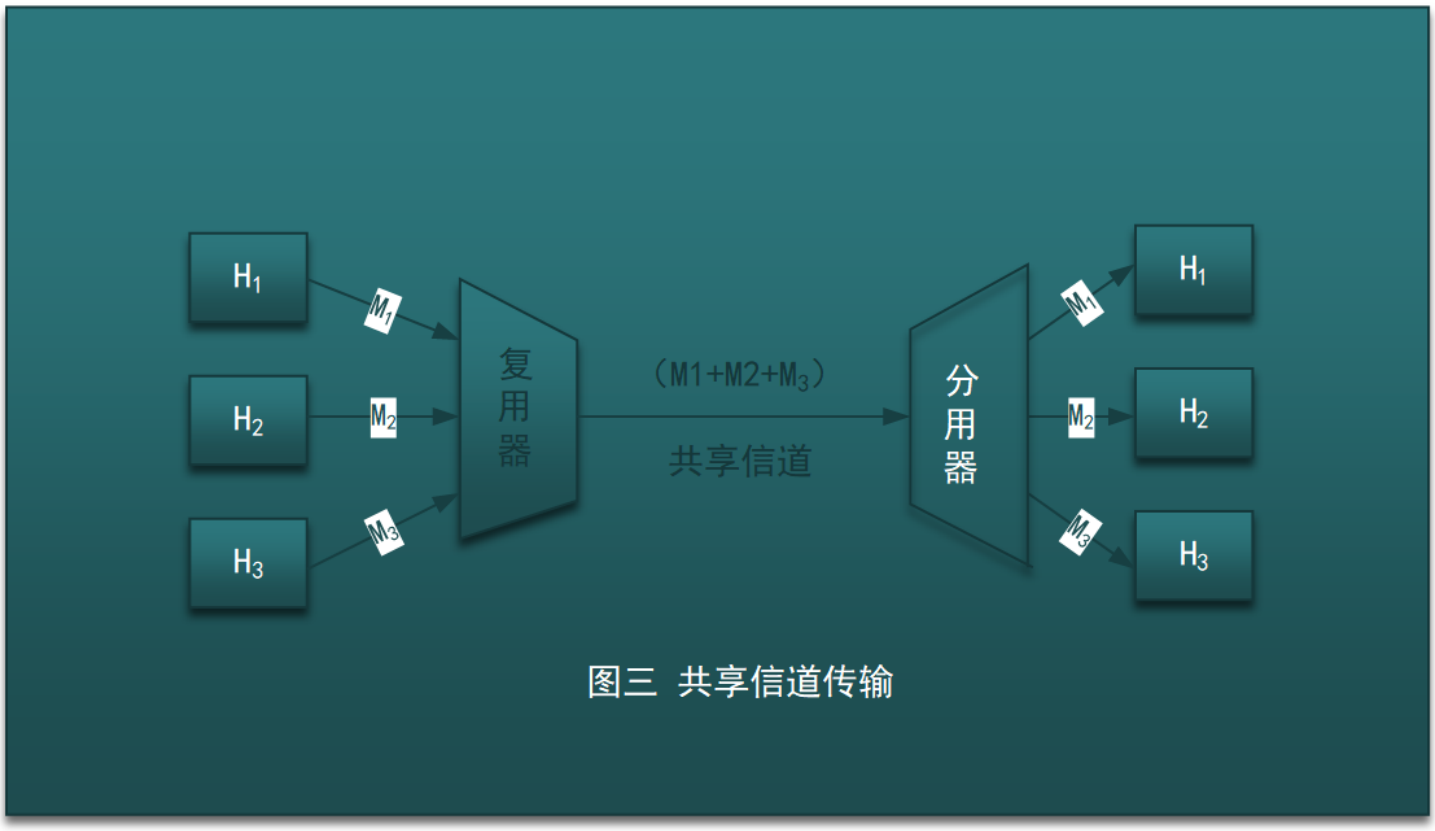
信号的调制和调解是数据传输中的关键技术，它们能够实现数据的可靠传输和正确解译。而曼切斯特编码是一种常见的编码方式，它通过使用相位的跳变来表示数据，具有较好的抗干扰性能和自同步能力。

3.信道的复用

信道复用是一种将若干个彼此独立的信号，合并为一个可在同一信道上同时传输的复合信号的方法。信道复用技术主要有频分复用、时分复用、统计时分复用、波分复用、码分复用等。

频分复用是将用于传输信道的总带宽划分成若干个子频带，每个子频带传输一路信号，这样就可以在同一个信道上传输多路信号。时分复用是将时间划分为一段段等长的时分复用帧，每个时分复用的用户在每个时分复用帧中占用固定序号的时隙，这样就可以在同一个信道上传输多路信号。统计时分复用是一种改进的时分复用，它通过动态分配时隙来提高信道的利用率。波分复用是利用不同波长的光信号在光纤中传输时的不同频带宽度，将多个信号调制在不同的波长上，然后通过一根光纤进行传输。码分复用是一种利用不同的码字进行信号调制的方法，不同用户的信号在同一信道上传输时，可以通过不同的码字进行区分。

信道复用技术可以显著提高信道的利用率和传输效率，是现代通信系统中的重要技术之一。



图三 共享信道传输

B. 数据链路层

1.封装成帧

在数据链路层，封装成帧是一个重要的概念。它指的是将数据按照特定的格式进行封装，以便在物理层上传输。封装成帧的目的是在发送方和接收方之间建立一个可靠的通信链路。

数据链路层使用帧作为数据传输的基本单位。帧的结构通常包括帧头、帧尾以及帧的数据部分。帧头包含了一些控制信息，如目的地址和源地址，用于标识帧的发送方和接收方。帧尾包含了校验码，用于检

测传输过程中可能发生的错误。帧的数据部分则是实际要传输的数据。

封装成帧的过程通常包括以下几个步骤：

1. **添加帧头和帧尾**：在发送数据之前，需要在数据的开头和结尾分别添加帧头和帧尾。帧头和帧尾包含了必要的控制信息，用于标识帧的发送方和接收方，以及用于错误检测的校验码。
2. **数据打包**：在添加了帧头和帧尾之后，将数据按照特定的格式进行打包，以便在物理层上进行传输。打包的过程可能会对数据进行一些处理，例如进行位填充等。
3. **发送数据**：将打包后的数据发送到物理层，由物理层负责数据的实际传输。
4. **接收数据**：在接收端，数据链路层接收到物理层传输的数据后，进行相应的解包和处理，提取出实际的数据内容。

通过 **封装成帧** 的过程，数据链路层能够确保数据的可靠传输，并在发送方和接收方之间建立一个可靠的通信链路。

2.透明传输

由于我无法直接生成带有颜色的关系图，以下是一个文字描述的关系图，描述了透明传输在串行通信中的作用和SerialNet模式的相关参数。

- **透明传输**：
  - 定义：一种数据传输方式，使数据在传输过程中保持原始状态，不改变数据的任何内容。
  - 作用：在网络上实现数据的双向透明传输，使设备不需要做任何改变。

透明传输是一种数据传输方式，其特点是无论所传数据是什么样的比特组合，都应当能够在链路上传送。当所传数据中的比特组合恰巧与某一个控制信息完全一样时，就必须采取适当的措施，使接收方不会将这样的数据误认为是某种控制信息。这样才能保证数据链路层的传输是透明的。

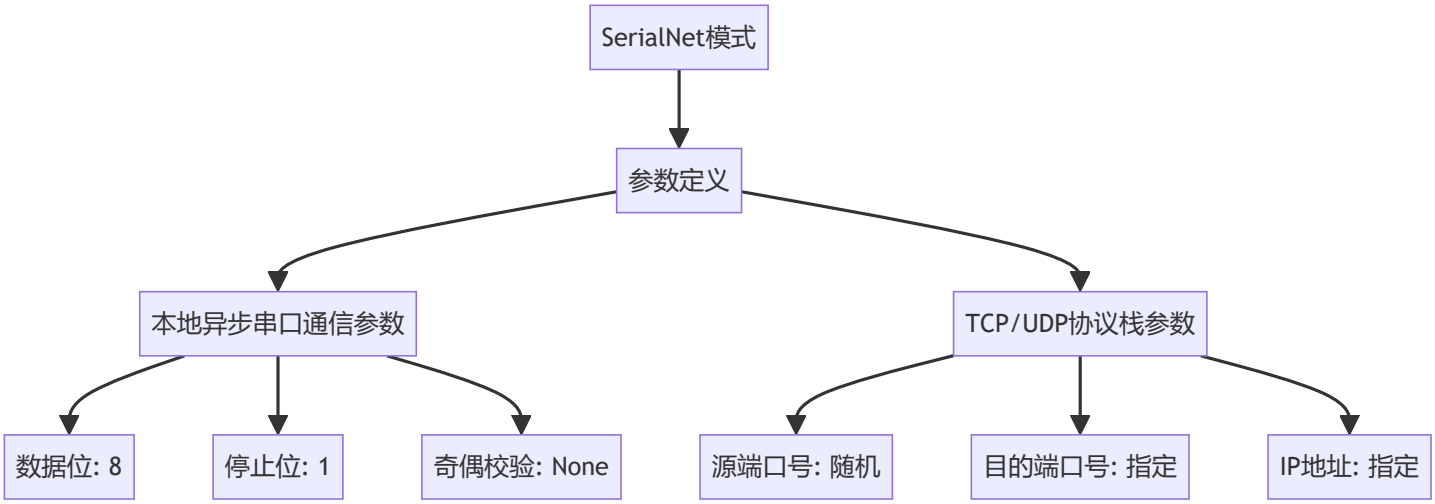
在串行通信中，透明传输通过实现在网络上的通信，使设备不需要做任何改变。为此，SerialNet模式定义了一系列相关的操作参数，这些参数的定义实现了网络连接所需要的属性。工作在SerialNet模式下的设备将自动完成串口到网络通信的转换，所有数据可透明的在两设备之间双向传输。

- **SerialNet模式**：
  - 定义：一种串行通信模式，通过定义相关参数来实现网络连接的属性。
  - 参数定义：包括数据位、停止位、奇偶校验等本地异步串口通信参数和源端口号、目的端口号、IP地址等TCP/UDP协议栈参数。
  - 作用：使设备自动完成串口到网络通信的转换，所有数据可透明的在两设备之间双向传输。

SerialNet模式需要定义以下参数：

1. 本地异步串口通信的参数，包括数据位、停止位、奇偶校验等。
2. TCP/UDP协议栈的相关参数，包括源端口号、目的端口号、IP地址等。

通过这些参数，SerialNet模式可以实现本地异步串口通信与基于TCP/UDP协议的网络通信之间的转换，使得设备无需进行任何修改即可在网络上进行通信。



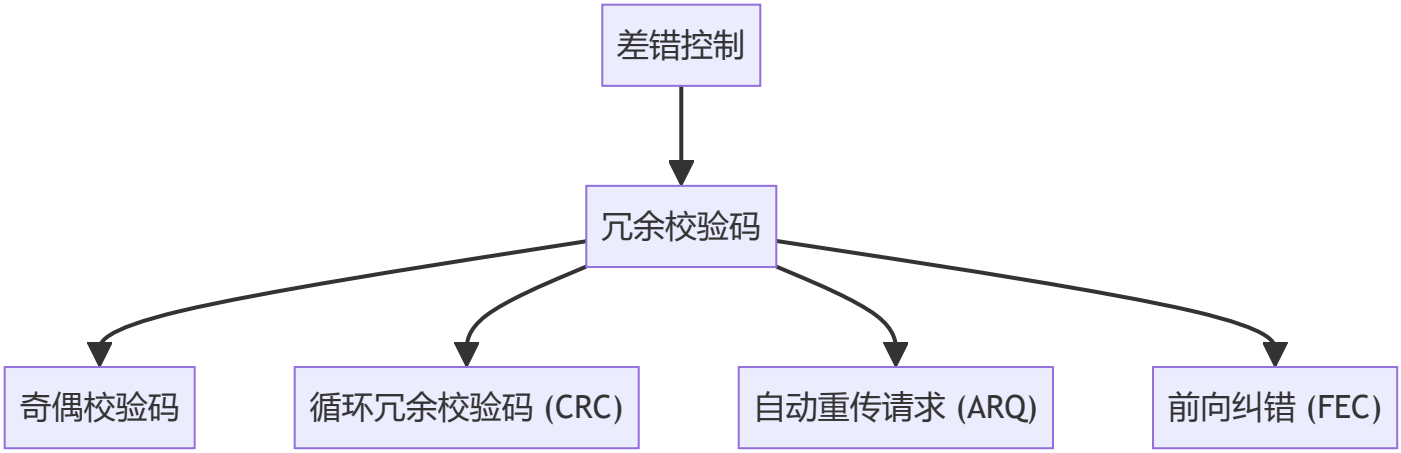
3.差错控制

差错控制是指在数据传输过程中，对传输的数据进行检查、发现错误并进行纠正的过程。差错控制的主要目的是确保数据在传输过程中的准确性和完整性。

- 差错控制可以通过不同的方式实现，其中最常见的是使用冗余校验码。冗余校验码是一种附加的数据，它被添加到原始数据中，以便在接收端进行错误检测和纠正。常见的冗余校验码包括奇偶校验码和循环冗余校验码（CRC）。

- - 奇偶校验码通过添加一个额外的位来确保数据中的1的个数是偶数（偶校验）或奇数（奇校验）。如果数据中的1的个数与校验位不匹配，则可以检测到错误。
- - 循环冗余校验码（CRC）是一种更复杂的校验码，它使用模2除法运算来检测数据中的错误。在发送端，发送方将数据作为被除数，使用特定的生成多项式作为除数，进行模2除法运算。将得到的余数附加到数据的末尾，作为冗余校验码发送。在接收端，接收方使用相同的生成多项式对数据进行模2除法运算，并将得到的余数与接收到的余数进行比较。如果两者相等，则数据没有错误；否则，数据被标记为错误并采取相应的措施进行纠正。

除了冗余校验码外，还有其他的差错控制方法，如自动重传请求（ARQ）和前向纠错（FEC）。自动重传请求是一种方法，它要求发送方重新发送出错的数据包，直到接收方成功接收为止。前向纠错是一种方法，它通过在数据中添加额外的信息来允许接收方纠正错误，而不需要重新发送数据。



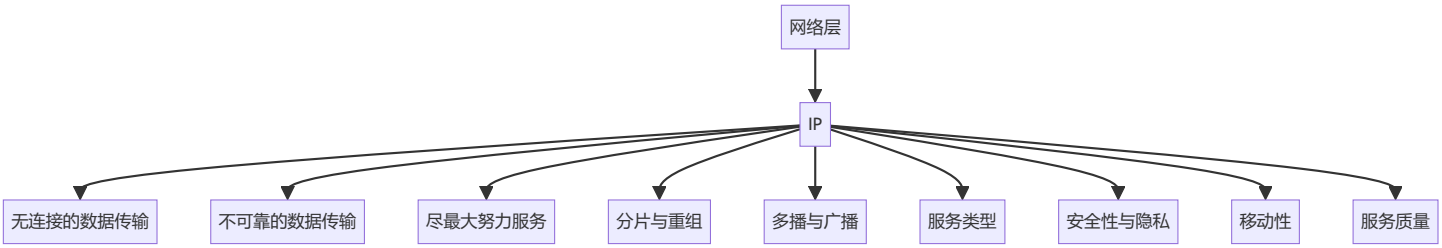
C. 网络层

1.IP

网络层是OSI参考模型中的第三层，负责处理网络中数据的传输。在这一层中，数据被打包成数据包，以便能够在网络上进行路由。**IP（Internet Protocol）** 是网络层的核心协议，用于将数据包从一个网络节点传输到另一个网络节点。

IP的主要功能如下：

1. **无连接的数据传输**：IP不建立连接，而是直接发送数据包。每个数据包都独立发送，并独立路由。
2. **不可靠的数据传输**：IP不保证数据包的可靠传输。如果数据包在传输过程中丢失或损坏，IP协议不会重新发送。
3. **尽最大努力服务**：IP提供的是“尽最大努力”的数据传输服务。这意味着IP不会保证数据包一定会到达目的地，但会尽量做到。
4. **分片与重组**：如果一个数据包的大小超过网络的MTU（最大传输单元），IP会将数据包分片，并在接收端重新组合。
5. **多播与广播**：IP支持多播和广播通信，允许一个发送方同时与多个接收方或特定网络段的所有接收方通信。
6. **服务类型**：IP可以根据需要提供多种服务类型，如实时流媒体、电子邮件等。
7. **安全与隐私**：随着IP协议的发展，它已经集成了许多安全和隐私保护功能，如IPsec和GRE。
8. **移动性**：随着移动设备和WiFi的普及，IP还提供了支持移动设备的能力，使得设备可以在不同的网络间无缝切换。
9. **服务质量**：为了满足某些业务需求，IP提供了一系列机制来控制和服务质量（QoS），如DiffServ和IntServ。



2.ARP

网络层的 **APR（Address Resolution Protocol，地址解析协议）** 是一个用于将IP地址解析为MAC地址（或称物理地址）的协议。ARP的主要作用是在局域网中，当主机或其它网络设备有数据要发送给另一个主机或设备时，它必须知道对方的网络层地址（即IP地址）。但是仅仅有IP地址是不够的，因为IP数据报文必须封装成帧才能通过物理网络发送，因此发送站还必须有接收站的物理地址，所以需要一个从IP地址到物理地址的映射。ARP就是实现这个功能的协议。

ARP通过广播或单播报文来解析IP地址与MAC地址之间的映射关系。当主机发送信息时，它将包含目标IP地址的ARP请求广播到网络上的所有主机。收到ARP请求的主机将检查其中的目标IP地址，如果与自己的IP地址匹配，则它将返回一个ARP应答，其中包含自己的MAC地址。这样，发送主机就可以通过ARP协议获取到目标主机的MAC地址，从而将数据发送给目标主机。

ARP协议是建立在网络中各个主机互相信任的基础上的，网络上的主机可以自主发送ARP应答消息，其他主机收到应答报文时不会检测该报文的真实性就会将其记入本机ARP缓存；由此攻击者就可以向某一主机发送伪ARP应答报文，使其发送的信息无法到达预期的主机或到达错误的主机，这就构成了一个ARP欺骗。

- 除了ARP协议，网络层还有许多其他的协议。其中一些重要的协议包括IP协议、ICMP协议、IGMP协议等。
- IP协议（Internet Protocol）是网络层的核心协议，用于在互联网中传输数据。IP协议通过路由和转发机制，将数据从一个网络节点传输到另一个网络节点，直到到达目的地。
- ICMP协议（Internet Control Message Protocol）是用于在IP主机和路由器之间传递控制消息的协议。这些控制消息主要用于诊断和控制目的，例如ping命令就是基于ICMP实现的。
- IGMP协议（Internet Group Management Protocol）是用于IPv4网络中的多播组成员资格报告的协议。它允许主机向本地多播路由器报告其感兴趣的多播组，以便多播路由器能够将多播数据发送给该主机。

此外，还有一些其他的网络层协议，如ARP协议、BOOTP协议、RARP协议等。这些协议在网络层中发挥着重要的作用，以确保数据能够可靠地传输到目标地址。

3.路由选择协议

路由选择协议是用于自动发现和选择最佳路径的协议，以便将数据从一个网络节点传输到另一个网络节点。路由选择协议在网络层中扮演着重要的角色，以确保数据能够高效、可靠地传输到目的地。

- 路由选择协议可以分为内部网关协议（IGP）和外部网关协议（EGP）两类。IGP是在一个自治系统内部使用的协议，如RIP和OSPF等。EGP是在自治系统之间使用的协议，如BGP等。
- 常见的路由选择协议包括RIP、OSPF、BGP等。这些协议通过不同的算法和策略来选择最佳路径，并维护路由表以记录到达各个目标网络的最佳路径。当网络发生变化时，路由选择协议能够自动更新路由表，以确保数据能够继续沿着最佳路径传输。

路由选择协议是网络层中不可或缺的一部分，它能够自动发现和选择最佳路径，确保数据能够可靠地传输到目的地。

D. 传输层

1.端口号

传输层使用端口号来标识通信的应用进程，从而实现端到端的通信。端口号由一个16位的数字组成，范围从0到65535。其中，端口号0到1023是预留给系统级服务的，称为知名端口。端口号1024到49151是动态分配的，而端口号49152到65535是保留给临时端口使用的。

端口号的作用是标识发送和接收数据的进程，从而在网络层的基础上实现更高层次的数据传输和控制。在TCP/IP协议中，传输层有两个主要的协议：TCP和UDP，它们都使用端口号来标识通信的进程。

TCP协议使用端口号来标识发送和接收数据的进程，从而建立可靠的连接并进行有序的数据传输。TCP协议的端口号范围是1到65535，其中一些端口号被预留给特定的服务，如HTTP使用80端口，HTTPS使用443端口等。

UDP协议同样使用端口号来标识发送和接收数据的进程，但它是无连接的协议，不保证数据的可靠传输。UDP协议的端口号范围也是1到65535，一些常见的UDP服务包括DNS使用53端口，SNMP使用161端口等。

端口号是传输层中用于标识通信进程的一种机制，它使得数据可以在网络中进行有序、可靠的传输。

2.

TCP（Transmission Control Protocol，传输控制协议）是一种面向连接的、可靠的、基于字节流的传输层协议。它是TCP/IP协议族中的核心协议之一，与IP协议一起共同构成了互联网的基础。

TCP的主要特点如下：

1. 面向连接：TCP协议是一种面向连接的协议，需要在传输数据之前先建立连接。通过三次握手（3-way handshake）过程，双方协商并建立传输参数，如端口号、数据传输速率等。
2. 可靠传输：TCP协议通过一系列机制确保数据的可靠传输。它采用确认机制（ACK）、重传机制（Retransmission）、流量控制（Flow Control）和拥塞控制（Congestion Control）等机制，确保数据按照发送的顺序、完整无误地到达目的地。
3. 字节流：TCP协议将数据看作字节流，不区分数据的大小和边界，按照发送的顺序连续传输。接收端按照接收到的字节流重新组成完整的数据。
4. 端到端通信：TCP协议采用端到端的通信模式，通信双方建立连接后，直接进行数据传输。数据的传输路径由IP协议确定，而TCP协议主要负责端到端的通信控制。
5. 全双工通信：TCP协议支持全双工通信模式，即通信双方都可以同时发送和接收数据。TCP连接建立后，双方都可以在任何时刻发送数据，并且能够实时地接收对方的回应。
6. 流量控制和拥塞控制：TCP协议采用流量控制和拥塞控制机制来避免网络拥塞和丢包现象。流量控制通过滑动窗口机制控制发送速率，而拥塞控制通过慢启动、拥塞避免、快速重传和快速恢复等算法来应对网络拥塞问题。

TCP协议通过这些机制提供了可靠、有序和高效的数据传输服务，广泛应用于互联网和各种应用程序中。

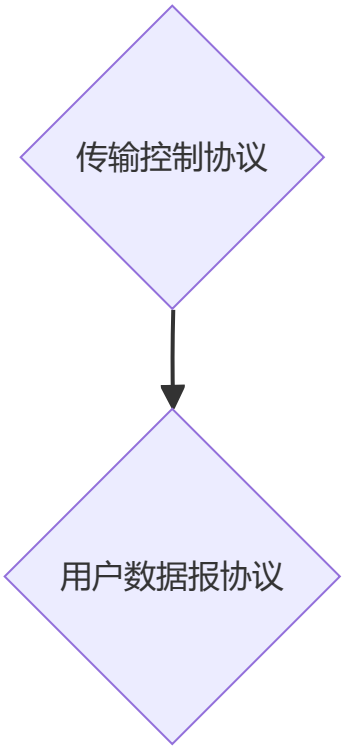
3.UDP

UDP（User Datagram Protocol，用户数据报协议）是另一种传输层协议，与TCP协议不同，它是一种无连接的协议。

UDP的主要特点如下：

1. 无连接：UDP协议在进行数据传输之前不需要建立连接，发送端可以直接发送数据报文到目标地址，不需要事先与接收端进行通信协商。
2. 尽最大努力交付：UDP提供了一种尽最大努力交付的不可靠通信方式，它不保证数据报文的顺序和完整性，可能会出现丢包、乱序或重复接收的情况。
3. 面向报文：UDP将数据拆分成大小不一的数据报文进行传输，每个数据报文称为一个报文段。UDP对数据报文的边界保持不变，接收端按照接收到的报文段重新组成完整的数据。
4. 简单性：相对于TCP协议，UDP协议相对简单，它没有TCP的确认机制、流量控制和拥塞控制等复杂的通信机制。因此，UDP协议的处理速度较快，适用于对实时性要求较高的应用，如视频通话、在线游戏等。
5. 快速传输：由于UDP协议没有TCP的确认机制和重传机制，所以它可以快速地发送数据。在某些情况下，UDP的传输速度比TCP更快。
6. 错误检测：虽然UDP协议本身不保证数据的可靠传输，但许多应用程序在应用层实现错误检测和恢复机制，例如校验和、重传和重排等。

UDP协议适用于一些对实时性要求较高、错误检测和恢复机制在应用层实现的应用场景，如在线视频、语音通话、在线游戏等。



- 一个简单的有向图，其中TCP和UDP是两个节点