

- [OSI 7层模型和TCP/IP 4层模型](#)
- [计算机网络中的七层模型](#)
- [TCP/IP四层模型](#)
- [TCP/IP（八）之总结TCP/IP四层模型](#)

# 计算机网络 7 层模型

---

七层模型，也称为 OSI(Open System Interconnection)参考模型，是国际标准化组织 ISO (Internationalization Standard Organization) 制定的一个用于计算机或通讯系统互联的标准体系。它是一个七层的，抽象的，包含了一系列抽象的术语和概念，也包括具体的协议。

## 7层模型的优点

---

主要目的：**解决异种网络连接时所遇到的兼容性问题。**

最大优点：将**服务，接口，协议**三个概念明确区分。

- **服务**说明某一层为上一层提供一些什么功能。
- **接口**说明上一层如何使用下一层的服务。
- **协议**则指定了如何实现本层的服务,采用什么样的协议是没有限制的，只要向上提供相同的服务并且不改变相邻的接口就可以。

## 7 层介绍

---

OSI 的上面 4 层（应用层，表示层，会话层，传输层）为高层，定义了程序的功能。

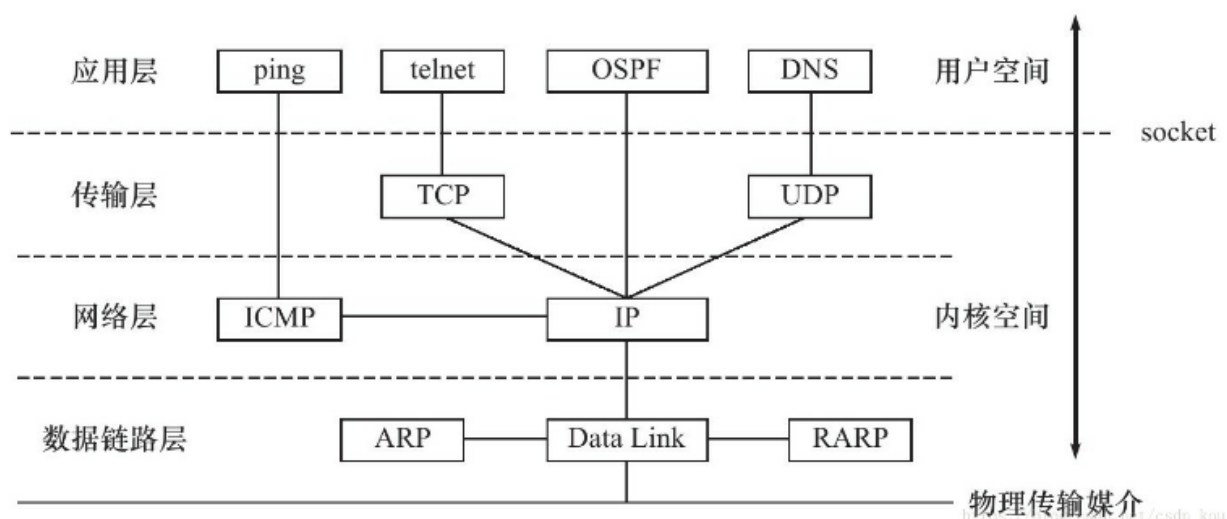
下面三层（网络层，数据链路层，物理层）为低层，主要处理面向网络的端到端数据流。

下面是一张网络图



## TCP/IP 四层协议

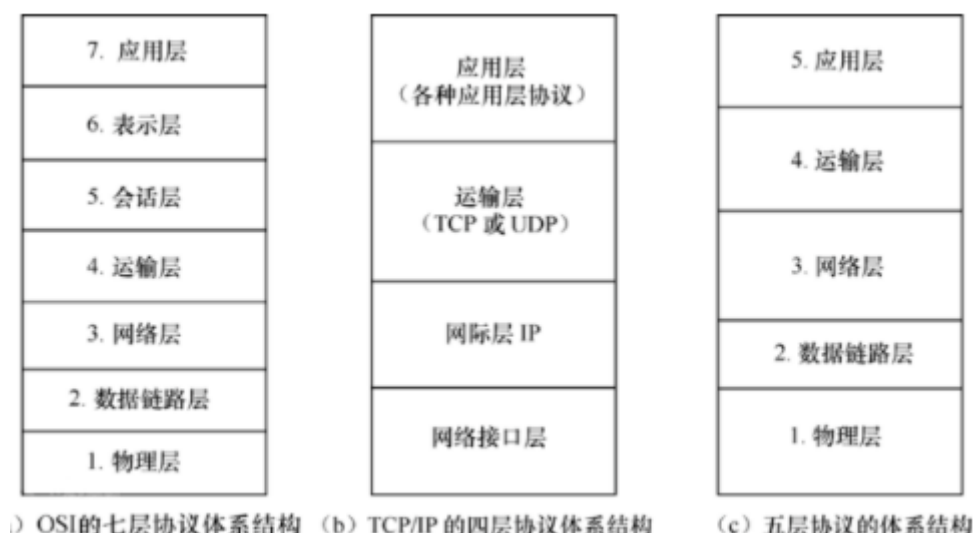
OSI 的七层协议体系结构的概念清楚，理论也比较完整，但它既复杂又不实用，TCP/IP体系结构则不同，它现在已经得到了非常广泛的应用，TCP/IP是一个四层的体系结构，自底向上分别是数据链路层，网络层，传输层和应用层。



它和 OSI 七层模型的对应关系如下图

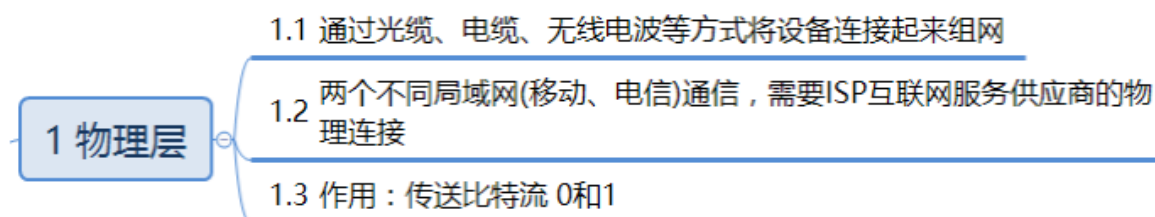
OSI七层网络模型	TCP/IP四层概念模型	对应网络协议
应用层 (Application)	应用层	HTTP、TFTP, FTP, NFS, WAIS、SMTP
表示层 (Presentation)		Telnet, Rlogin, SNMP, Gopher
会话层 (Session)		SMTP, DNS
传输层 (Transport)	传输层	TCP, UDP
网络层 (Network)	网络层	IP, ICMP, ARP, RARP, AKP, UUCP
数据链路层 (Data Link)	数据链路层	FDDI, Ethernet, Arpanet, PDN, SLIP, PPP
物理层 (Physical)		IEEE 802.1A, IEEE 802.2到IEEE 802.11

对于计算机网络来说，TCP/IP 四层协议中数据链路层没有什么新的具体内容，但是在学习计算机网络的时候通常采用了折中的办法，综合了 ISO 和 TCP/IP 的优点，采用了一种只有五层的体系结构

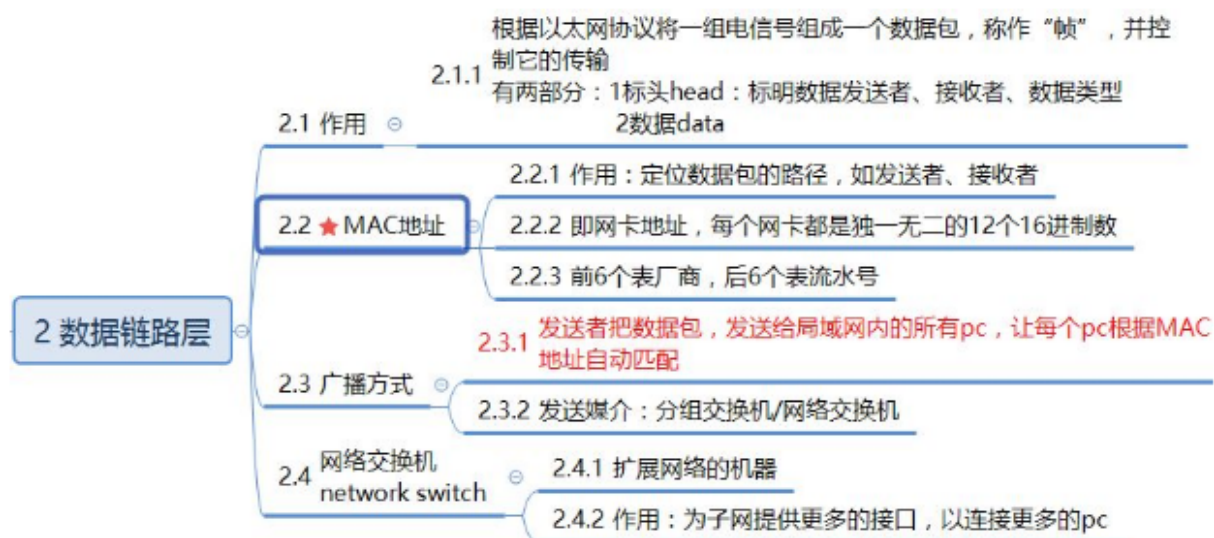


## 各层功能简介

### 物理层



## 数据链路层



**数据链路层实现了网卡接口的网络驱动程序，以处理数据在物理媒介（比如以太网、令牌环等）上的传输。**

数据链路层两个常用的协议是ARP协议（Address Resolve Protocol，地址解析协议）和RARP协议（ReverseAddress Resolve Protocol，逆地址解析协议）。它们实现了IP地址和机器物理地址（通常是MAC地址，以太网、令牌环和802.11无线网络都使用MAC地址）之间的相互转换。

网络层使用IP地址寻址一台机器，而数据链路层使用物理地址寻址一台机器，因此网络层必须先将目标机器的IP地址转化成其物理地址，才能使用数据链路层提供的服务，这就是ARP协议的用途。

RARP协议仅用于网络上的某些无盘工作站。因为缺乏存储设备，无盘工作站无法记住自己的IP地址，但它们可以利用网卡上的物理地址来向网络管理者（服务器或网络管理软件）查询自身的IP地址。运行RARP服务的网络管理者通常存有该网络上所有机器的物理地址到IP地址的映射。

## 网络层

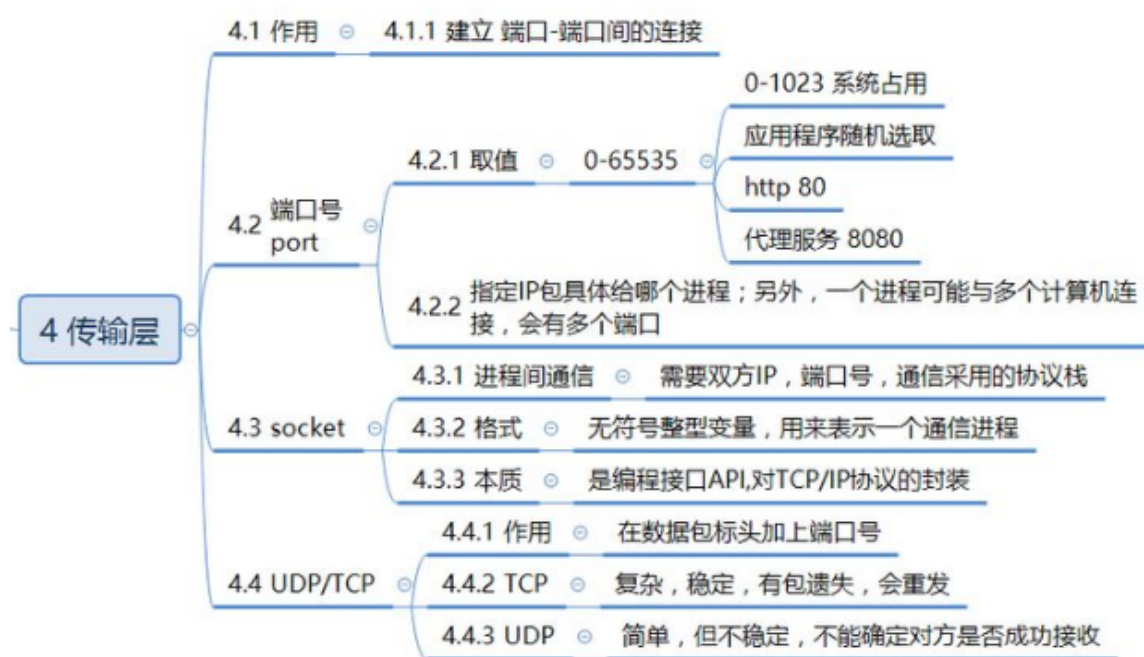




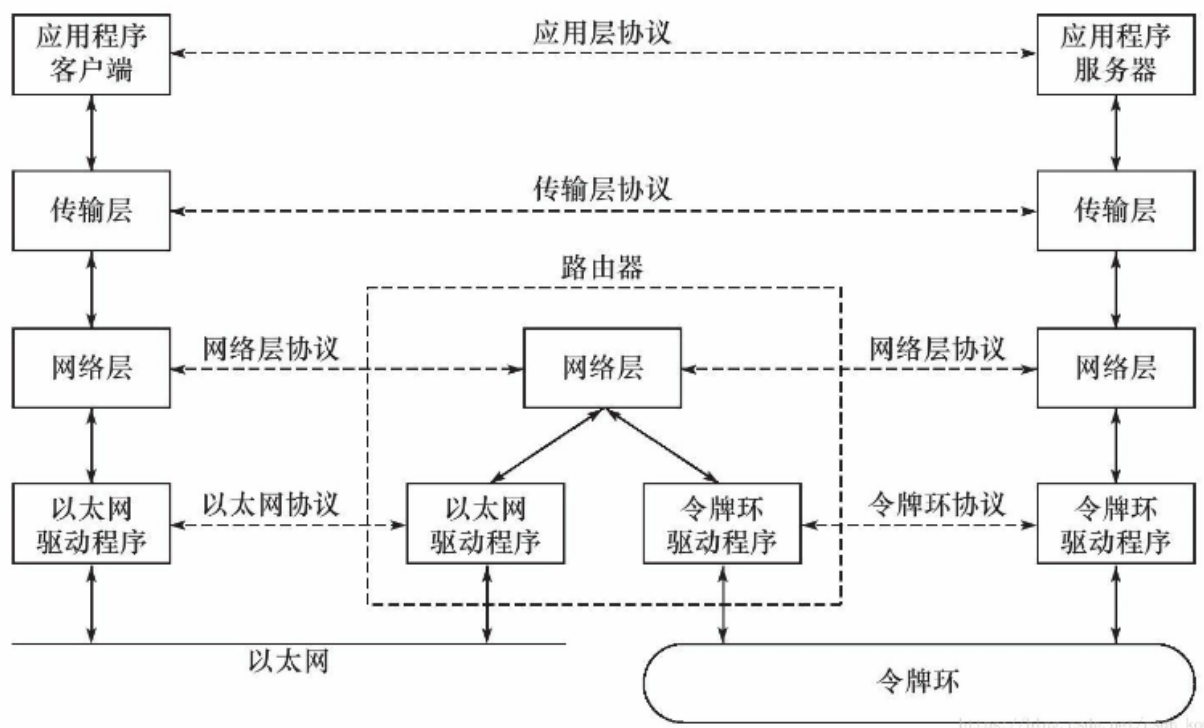
- 差错报文，这类报文主要用来回应网络错误，比如目标不可到达（类型值为3）和重定向（类型值为5）；
- 查询报文，这类报文用来查询网络信息，比如ping程序就是使用ICMP报文查看目标是否可到达（类型值为8）的。

有的ICMP报文还使用8位代码字段来进一步细分不同的条件。比如重定向报文使用代码值0表示对网络重定向，代码值1表示对主机重定向。ICMP报文使用16位校验和字段对整个报文（包括头部和内容部分）进行循环冗余校验（Cyclic Redundancy Check, CRC），以检验报文在传输过程中是否损坏。不同的ICMP报文类型具有不同的正文内容。

## 传输层



传输层为两台主机上的应用程序提供端到端（end to end）的通信。与网络层使用的逐跳通信方式不同，传输层只关心通信的起始端和目的端，而不在于数据包的中转过程。

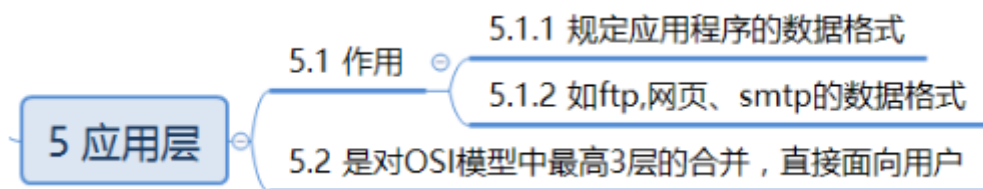


垂直的实线箭头表示TCP/IP协议族各层之间的实体通信（数据包确实是沿着这些线路传递的），而水平的虚线箭头表示逻辑通信线路。该图中还附带描述了不同物理网络的连接方法。可见，数据链路层（驱动程序）封装了物理网络的电气细节；网络层封装了网络连接的细节；传输层则为应用程序封装了一条端到端的逻辑通信链路，它负责数据的收发、链路的超时重连等。

传输层协议：TCP协议、UDP协议。

- TCP协议（Transmission Control Protocol，传输控制协议）为应用层提供可靠的、面向连接的和基于流（stream）的服务。TCP协议使用超时重传、数据确认等方式来确保数据包被正确地发送至目的端，因此TCP服务是可靠的。使用TCP协议通信的双方必须先建立TCP连接，并在内核中为该连接维持一些必要的数据结构，比如连接的状态、读写缓冲区，以及诸多定时器等。当通信结束时，双方必须关闭连接以释放这些内核数据。TCP服务是基于流的。基于流的数据没有边界（长度）限制，它源源不断地从通信的一端流入另一端。发送端可以逐个字节地向数据流中写入数据，接收端也可以逐个字节地将它们读出。
- UDP协议（User Datagram Protocol，用户数据报协议）则与TCP协议完全相反，它为应用层提供不可靠、无连接和基于数据报的服务。“不可靠”意味着UDP协议无法保证数据从发送端正确地传送到目的端。如果数据在中途丢失，或者目的端通过数据校验发现数据错误而将其丢弃，则UDP协议只是单地通知应用程序发送失败。因此，使用UDP协议的应用程序通常要自己处理数据确认、超时重传等逻辑。UDP协议是无连接的，即通信双方不保持一个长久的联系，因此应用程序每次发送数据都要明确指定接收端的地址（IP地址等信息）。基于数据报的服务，是相对基于流的服务而言的。每个UDP数据报都有一个长度，接收端必须以该长度为最小单位将其所有内容一次性读出，否则数据将被截断。

## 应用层



**应用层负责处理应用程序的逻辑。**

数据链路层、网络层和传输层负责处理网络通信细节，这部分必须既稳定又高效，因此它们都在内核空间中实现。而应用层则在用户空间实现，因为它负责处理众多逻辑，比如文件传输、名称查询和网络管理等。如果应用层也在内核中实现，则会使内核变得非常庞大。当然，也有少数服务器程序是在内核中实现的，这样代码就无须在用户空间和内核空间来回切换（主要是数据的复制），极大地提高了工作效率。不过这种代码实现起来较复杂，不够灵活，且不利于移植。

- ping是应用程序，而不是协议，前面说过它利用ICMP报文检测网络连接，是调试网络环境的必备工具。
- telnet协议是一种远程登录协议，它使我们能在本地完成远程任务。
- OSPF（Open Shortest Path First，开放最短路径优先）协议是一种动态路由更新协议，用于路由器之间的通信，以告知对方各自的路由信息。
- DNS（Domain Name Service，域名服务）协议提供机器域名到IP地址的转换。

应用层协议（或程序）可能跳过传输层直接使用网络层提供的服务，比如ping程序和OSPF协议。应用层协议（或程序）通常既可以使用TCP服务，又可以使用UDP服务，比如DNS协议。我们可以通过/etc/services文件查看所有知名的应用层协议，以及它们都能使用哪些传输层服务。

## 其他知识

一个设备工作在哪一层，关键看它工作时利用哪一层的数据头部信息。网桥工作时，是以MAC头部来决定转发端口的，因此显然它是数据链路层的设备。

具体说：

- 物理层：网卡，网线，集线器，中继器，调制解调器
- 数据链路层：网桥，交换机
- 网络层：路由器
- 网关工作在第四层传输层及其以上。

集线器是物理层设备，采用广播的形式来传输信息。交换机就是用来进行报文交换的机器。多为链路层设备（二层交换机），能够进行地址学习，采用存储转发的形式来交换报文。路由器的一个作用是连通不同的网络，另一个作用是选择信息传送的线路。选择通畅快捷的近路，能大大提高通信速度，减轻网络系统通信负荷，节约网络系统资源，提高网络系统畅通率。

### 交换机和路由器的区别

交换机拥有一条很高带宽的背部总线和内部交换矩阵。交换机的所有的端口都挂接在这条总线上，控制电路收到数据包以后，处理端口会查找内存中的地址对照表以确定目的MAC（网卡的硬件地址）的



NIC（网卡）挂接在哪个端口上，通过内部交换矩阵迅速将数据包传送到目的端口，目的MAC若不存在则广播到所有的端口，接收端口回应后交换机会“学习”新的地址，并把它添加入内部MAC地址表中。

使用交换机也可以把网络“分段”，通过对照MAC地址表，交换机只允许必要的网络流量通过交换机。通过交换机的过滤和转发，可以有效的隔离广播风暴，减少误包和错包的出现，避免共享冲突。

交换机在同一时刻可进行多个端口对之间的数据传输。每一端口都可视为独立的网段，连接在其上的网络设备独自享有全部的带宽，无须同其他设备竞争使用。当节点A向节点D发送数据时，节点B可同时向节点C发送数据，而且这两个传输都享有网络的全部带宽，都有着自己的虚拟连接。假使这里使用的是10Mbps的以太网交换机，那么该交换机这时的总流量就等于 $2 \times 10\text{Mbps} = 20\text{Mbps}$ ，而使用10Mbps的共享式HUB时，一个HUB的总流量也不会超出10Mbps。

总之，交换机是一种基于MAC地址识别，能完成封装转发数据包功能的网络设备。交换机可以“学习”MAC地址，并把其存放在内部地址表中，通过在数据帧的始发者和目标接收者之间建立临时的交换路径，使数据帧直接由源地址到达目的地。

从过滤网络流量的角度来看，路由器的作用与交换机和网桥非常相似。但是与工作在网络物理层，从物理上划分网段的交换机不同，路由器使用专门的软件协议从逻辑上对整个网络进行划分。例如，一台支持IP协议的路由器可以把网络划分成多个子网段，只有指向特殊IP地址的网络流量才可以通过路由器。对于每一个接收到的数据包，路由器都会重新计算其校验值，并写入新的物理地址。因此，使用路由器转发和过滤数据的速度往往要比只查看数据包物理地址的交换机慢。但是，对于那些结构复杂的网络，使用路由器可以提高网络的整体效率。路由器的另外一个明显优势就是可以自动过滤网络广播。

## 集线器与路由器在功能上有什么不同？

首先说HUB,也就是集线器。它的作用可以简单的理解为将一些机器连接起来组成一个局域网。而交换机（又名交换式集线器）作用与集线器大体相同。但是两者在性能上有区别：集线器采用的式共享带宽的工作方式，而交换机是独享带宽。这样在机器很多或数据量很大时，两者将会有比较明显的。而路由器与以上两者有明显区别，它的作用在于连接不同的网段并且找到网络中数据传输最合适的路径。路由器是产生于交换机之后，就像交换机产生于集线器之后，所以路由器与交换机也有一定联系，不是完全独立的两种设备。路由器主要克服了交换机不能路由转发数据包的不足。

总的来说，路由器与交换机的主要区别体现在以下几个方面：

（1）工作层次不同 最初的的交换机是工作在数据链路层，而路由器一开始就设计工作在网络层。由于交换机工作在数据链路层，所以它的工作原理比较简单，而路由器工作在网络层，可以得到更多的协议信息，路由器可以做出更加智能的转发决策。

（2）数据转发所依据的对象不同 交换机是利用物理地址或者说MAC地址来确定转发数据的目的地址。而路由器则是利用IP地址来确定数据转发的地址。IP地址是在软件中实现的，描述的是设备所在的网络。MAC地址通常是硬件自带的，由网卡生产商来分配的，而且已经固化到了网卡中去，一般来说是不可更改的。而IP地址则通常由网络管理员或系统自动分配。

（3）传统的交换机只能分割冲突域，不能分割广播域；而路由器可以分割广播域 由交换机连接的网段仍属于同一个广播域，广播数据包会在交换机连接的所有网段上传播，在某些情况下会导致通信拥挤和安全漏洞。连接到路由器上的网段会被分配成不同的广播域，广播数据不会穿过路由器。虽然第

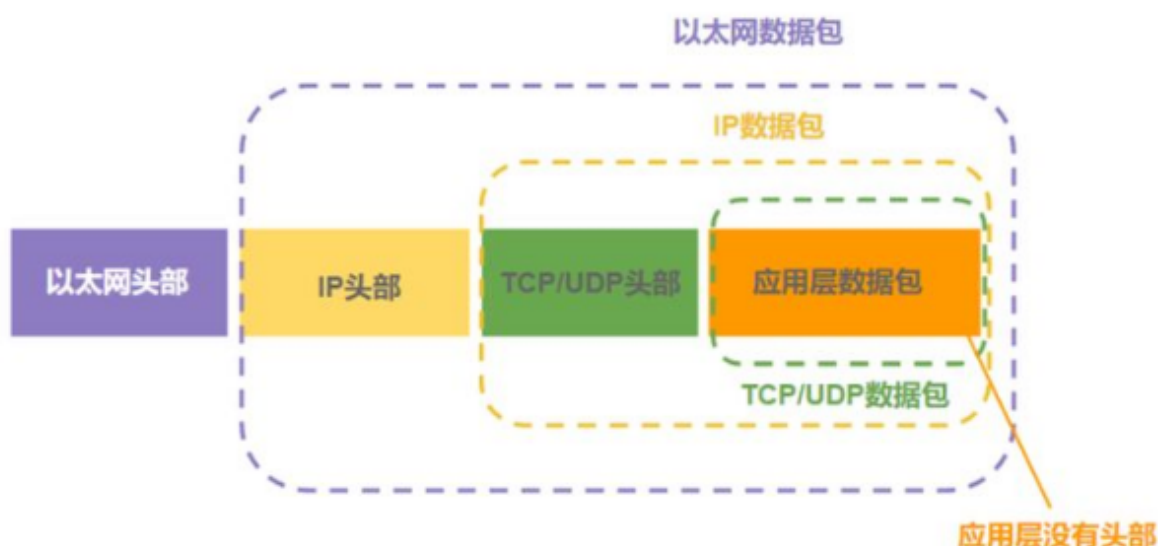
三层以上交换机具有VLAN功能，也可以分割广播域，但是各子广播域之间是不能通信交流的，它们之间的交流仍然需要路由器。

(4) 路由器提供了防火墙的服务 路由器仅仅转发特定地址的数据包，不传送不支持路由协议的数据包传送和未知目标网络数据包的传送，从而可以防止广播风暴。

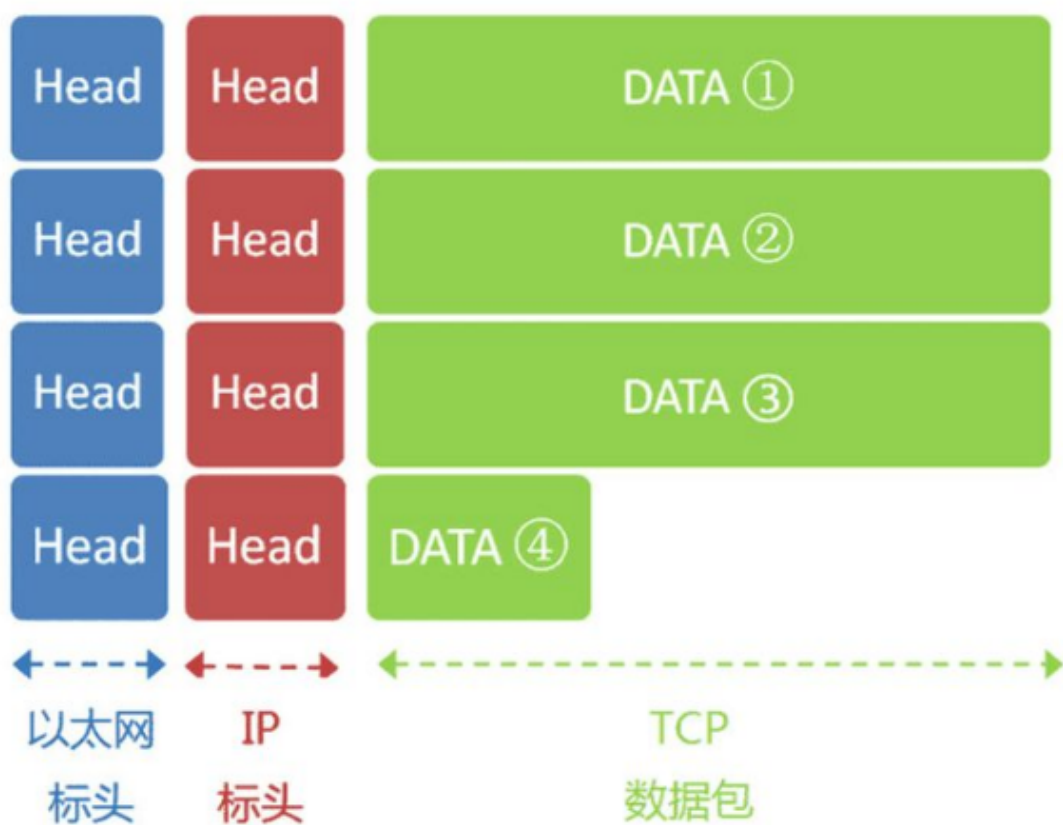
## PC 联网的设置



**数据链路层数据包（以太网数据包）格式，除了应用层没有头部，其他都有**



由于以太网数据包的数据部分，最大长度为1500字节，当IP包过大时，会分割下来，但是每个分割包的头部都一样



数据包在传送时的封装和解封装如下所示

