计算机网络原理理论作业

18342138 郑卓民 软工四班

1. 解释 ISO 的 7 层网络模型和互联网的 5 层网络模型，以及后者把前者的最顶三层合为一层的理由，并以课程所学协议为例，总结五层互联网模型的数据链路层、网络层和传输层的用途。

互联网 5 层网络模型：

1. 应用层：应用层是网络应用程序及它们的应用层协议存留的地方，互联网的应用层包括许多协议，例如 HTTP（它提供过了 Web 文档的请求和传送）、SMTP（它提供了电子邮件报文的传输）和 FTP（它提供了两个端系统之间的文件传送）。应用层协议分布在多个端系统上，而一个端系统中的应用程序使用协议与另一个端系统中的应用程序交换信息分组。应用层的信息分组称为报文（message）。
2. 运输层：互联网的运输层在应用程序端点之间传送应用层报文。在互联网中，有两种运输协议，即 TCP 和 UDP，利用其中的任一个都能运输应用层报文。TCP 向它的应用程序提供面向连接的服务，UDP 向它的应用程序提供无连接服务。运输层的分组称为报文段（segment）。
3. 网络层：互联网的网络层负责将称为数据报（datagram）的网络层分组从一台主机移动到另一台主机。互联网的网络层包括著名的网际协议 IP，该协议定义了在数据报中的各个字段以及端系统和路由器如何作用于这些字段。互联网的网络层也包括决定路由和路由选择协议，它根据该路由将数据报从源传输到目的地。
4. 链路层：为了将分组从一个节点（主机或路由器）移动到路径上的下一个节点，网络层必须依靠该链路层的服务。链路层提供的服务取决于应用于该链路的特定链路层协议，链路层的例子包括以太网、WIFI 和电缆接入网的 DOCSIS 协议。网络层将受到来自每个不同的链路层协议的不同服务。链路层分组称为帧（frame）。
5. 物理层：物理层的任务是将该帧中的一个个比特从一个节点移动到下一个节点。在这层中的协议仍然是链路相关的，并且进一步与该链路的实际传输媒体相关。例如，以太网具有许多物理层协议：一个是关于双绞铜线的，另一个是关于同轴电缆的。在每种场合中，跨越这些链路移动一个比特是以不同的方式进行的。

ISO 7 层网络模型：

1. 应用层：应用层也称为应用实体，一般是指应用程序，该层主要负责确定通信对象，并确保有足够的资源用于通信，常见的应用层协议有 FTP、HTTP、SNMP（简单网络管理协议）、FTP（文件传送协议）、Telenet（远程登录协议）、DNS（域名解析协议）、SMTP（邮件传送协议），POP3 协议（邮局协议）。（与互联网 5 层模型中对应层的功能相同。）
2. 表示层：表示层的作用是使通信的应用程序能够解释交换数据的含义，这些服务包括数据压缩和数据加密以及数据描述。表示层一般负责数据的编码以及转化，确保应用层的数据能够正常工作，该层是界面与二进制代码间互相转化的地方，同时该层负责进行数据额压缩、解压、加密、解密等，该层也可以根据不同应用目的将数据处理成不同的格式，表现出来就是各种各样的文件扩展名。
3. 会话层：会话层提供了数据交换的定界和同步功能，包括建立检查点和恢复方案的方法。会话层主要负责在网络中两个节点之间建立、维护、控制回话，区分不同的会话，以及提供单工、半双工、全双工三种通信模式服务，NFS（网络文件系统）、RPC（远程过程调用）和 X Window 等都工作在该层。
4. 运输层：与互联网 5 层模型中对应层的功能相同。
5. 网络层：与互联网 5 层模型中对应层的功能相同。

6. 链路层：与互联网 5 层模型中对应层的功能相同。
7. 物理层：与互联网 5 层模型中对应层的功能相同。

将应用层、表示层、会话层合并为一层的理由：
不同的应用程序对于表示层和会话层的服务需求程度不一样，将表示层和会话层的功能以可选的形式合并进应用层，可以简化设计，给开发者更多选择，将表示层和会话层的服务留给开发者处理，如果该服务对于开发的应用程序重要，应用开发者就可以在应用程序中构建该功能（服务）。

数据链路层用途：
运行链路层协议的任何设备均称为节点（node），沿着通信路径连接相邻节点的通信信道称为链路（link）。为了将一个数据报从源主机传输到目的主机，数据报必须通过沿端到端路径上的各段链路传输。在通过特定的链路时，传输节点将数据报封装在链路成帧中，并将该帧传送到链路中。
链路层协议能够提供的服务包括：
1. 成帧（framing）。
2. 链路接入。媒体访问控制协议（MAC）规定了帧在链路上传输的规则。
3. 可靠交付。
4. 差错检测和改正。
网络链路有两种类型：点对点链路和广播链路。
广播链路需要处理多路访问问题，此时需要多路访问协议，即通过这些协议来规范它们在共享的广播信道上的传输行为。多路访问协议分为三种类型：信道划分协议、随机接入协议和轮流协议。
此外还有地址解析协议（ARP），该协议提供了将 IP 地址转换为链路层地址的机制。每台主机和路由器有一个单一的 IP 地址和单一的 MAC 地址。

网络层用途：
网络层能够被分为两个相互作用的部分，即数据平面和控制平面。
数据平面：
即网络层中每台路由器的功能，该数据平面功能决定到达路由器输入链路之一的数据报（即网络层的分组）如何转发到该路由器的输出链路之一。
网络层的关键方面和著名的网际协议（IP）：
今天有两个版本的 IP 正在使用，IPv4 与 IPv6。
IPv4 数据报的格式：1. 版本号。2. 首部长度。3. 服务类型。4. 数据报长度。5. 标识、标志、片偏移。6. 寿命。7. 协议。8. 首部检验和。9. 源和目的 IP 地址。10. 选项。11. 数据（有效载荷）。
IPv6 数据报的格式：1. 版本号。2. 流量类型。3. 流标签。4. 有效载荷长度。5. 下一个首部。6. 跳限制。7. 源地址和目的地址。8. 数据。9. 分片/重新组装。 10. 首部检验和。11. 选项。
控制平面：
即网络范围的逻辑，该控制平面功能控制数据报沿着从源主机到目的主机的端到端路径中路由器之间的路由方式。
因特网控制报文协议（ICMP），该主机和路由器用来彼此沟通网络层的信息。ICMP 最典型的用途是差错报告。

传输层用途：

运输层协议为运行在不同主机上的应用进程之间提供了逻辑通信功能。应用进程使用运输层提供的逻辑通信功能彼此发送报文，而无须考虑承载这些报文的物理基础设施的细节。网络应用程序可以使用多种的运输层协议，例如因特网有两种协议，即 TCP 和 UDP。每种协议都能为调用的应用程序提供一组不同的运输层服务。

UDP（用户数据报协议），提供一种不可靠、无连接的服务。

TCP（传输控制协议），提供一种可靠、面向连接的服务。

UDP 和 TCP 最基本的责任是，将两个端系统间 IP 的交付服务扩展为运行在端系统上的两个进程之间的交付服务。将主机间交付扩展到进程间交付被称为运输层的多路复用与多路分解。另一方面，TCP 为应用程序提供了几种附加服务，可靠数据传输、拥塞控制。

2. 解释电路交换和数据包交换这两种技术的工作原理，并对其优缺点做对比分析。

电路交换：

是一种网络连接，连接过程中是网络中两端点的单路连接。普通语音电话服务就是一种电路交换。电话公司在通话期间为所呼叫号码预留一条实际的物理通路，其他人不能使用该通路。电路交换的基本过程可分为连接建立、信息传送和连接拆除三个阶段。

优点：数据传输可靠、迅速，数据不会丢失，且保持原来的序列。

缺点：线路的利用率较低，容易引起拥塞。电路空闲时的信道容量被浪费；另外，如数据传输阶段的持续时间不长，电路建立和拆除所用的时间就得不偿失。

数据包交换：

数据包交换，和虚拟电路交换技术都属于存储转发技术中的分组交换技术分类，他们都按照一定的路由算法选择通信路径。

数据报分组交换技术就是通信双方间至少要存在一条数据传输通路，这些通路可能要跨越多个中间节点，信源节点在通信以前将所要传输和交换的数据包准备好，并最终以分组的形式进行传输和交换。如果信源和信宿是相邻节点，则信源方可将数据直接投递给信宿。若信源信宿间通过中心节点连接，则信源通过合适的路由机制将分组传递给合适的中间节点，中间节点在经过数次的路由选择，选取合适的路径将分组数据传递到信宿处。

优点：同一报文的不同分组可以由不同的传输路径通过通信子网，正如两地间有多条交通线路一般，选取任何一条都能成功到达目的地。（如有故障可绕过故障点。）

缺点：同一报文的不同分组到达目的节点时可能会出现乱序、重复和丢失的现象。数据报分组方式传输延迟较大，适用于突发性的通信，不适用于长报文、会话式的通信。

3. 中山大学校园网的用户用浏览器访问一个网页：www.sina.com.cn，请详细论述访问过程涉及到的应用层协议操作，包括 DNS、HTTP 和 Proxy 等。

整个过程可以概括为几下几个部分：

1. 域名解析成 IP 地址；

   若 DNS 缓存中没有相关数据，则浏览器先向 DNS 服务器发出 DNS 请求，这一过程的目的是获取 www.sina.com.cn 这个域名所对应的 IP 地址。

2. 与目的主机进行 TCP 连接（三次握手）；

   浏览器向 www.sina.com.cn 发出 TCP 连接请求报文，该请求报文的传输过程为：

   TCP 请求报文(TCP)->IP（DNS）->MAC（ARP）->校园网关->www.sina.com.cn 主机 www.sina.com.cn 收到的数据帧->IP->TCP，TCP 协议单元会回应请求应答报文。

   同理，应答报文的传播过程也类似，并接着完成 TCP 的三次握手。

3. 发送与收取数据（浏览器与目的主机开始 HTTP 访问过程）；

浏览器向 www.sina.com.cn 发出 HTTP-GET 方法报文：

该 HTTP-GET 方法报文->TCP->IP->MAC->校园网关->www.sina.com.cn 主机

www.sina.com.cn 收到的数据帧->IP->TCP->HTTP

HTTP 协议单元会回应 HTTP 协议格式封装好的 HTML 超文本形式数据

HTTP-HTML 数据->TCP->IP->MAC->校园网关->请求主机

请求主机收到的数据帧->IP->TCP->HTTP->浏览器，浏览器会以网页形式显示 HTML 超文本，就是所看到的网页。

4. 与目的主机断开 TCP 连接（四次挥手）；

浏览器向 www.sina.com.cn 发出 TCP 连接结束请求报文，该请求报文的传输过程为：

TCP 结束请求报文(TCP)->IP（DNS）->MAC（ARP）->校园网关->www.sina.com.cn 主机

www.sina.com.cn 收到的数据帧->IP->TCP，TCP 协议单元会回应结束应答报文。

同理，应答报文的传播过程也类似，并接着完成 TCP 的四次挥手。

4. 简述电子邮件的三种协议 SMTP、IMAP 和 POP3 的用途，并以使用 Windows 上的 Outlook 软件发送和浏览邮件为例说明所涉及的协议操作。

SMTP：

SMTP 的全称是“Simple Mail Transfer Protocol”，即简单邮件传输协议（25 号端口）。它是一组用于从源地址到目的地址传输邮件的规范，通过它来控制邮件的中转方式。SMTP 协议属于 TCP/IP 协议簇，它帮助每台计算机在发送或中转信件时找到下一个目的地。

SMTP 是一个“推”的协议，它不允许根据需要从远程服务器上“拉”来消息。SMTP 服务器就是遵循 SMTP 协议的发送邮件服务器，SMTP 认证就是要求必须在提供了账户名和密码之后才可以登录 SMTP 服务器，这就使得那些垃圾邮件的散播者无可乘之机。

IMAP：

IMAP 全称是邮局协议的第 3 个版本，即交互式邮件访问协议，是一个应用层协议（端口是 143）。用来从本地邮件客户端（Outlook Express、Foxmail、Mozilla Thunderbird 等）访问远程服务器上的邮件。

POP3：

POP3 是 Post Office Protocol 3 的简称，即邮局协议的第 3 个版本，是 TCP/IP 协议族中的一员（默认端口是 110）。本协议主要用于支持使用客户端远程管理在服务器上的电子邮件。

邮件软件上的协议操作：

接受邮件使用 POP3 和 IMAP，此外，使用 IMAP 还可以同步客户端和服务器之间的操作。

发送邮件使用 SMTP。

5. 简述 TCP 的流控制、可靠数据传输和拥塞控制的方法原理和用途。

流控制：

TCP 协议里窗口机制有 2 种：一种是固定的窗口大小；一种是滑动的窗口。这个窗口大小就是我们一次传输几个数据。对所有数据帧按顺序赋予编号，发送方在发送过程中始终保持着一个发送窗口，只有落在发送窗口内的帧才允许被发送；同时接收方也维持着一个接收窗口，只有落在接收窗口内的帧才允许接收。这样通过调整发送方窗口和接收方窗口的大小可以实现流量控制。

可靠数据传输：

TCP 的可靠数据传输服务确保一个进程从其接受缓存中读出的数据流是无损坏、无间隙、非冗余和按序的数据流，即该字节流与连接的另一方端系统发送出的字节流是完全相同的。

与 TCP 可靠数据传输相关的技术有超时间隔加倍、快速重传、选择确认。TCP 的差错恢复机制也许最好被分类为 GBN 协议和 SR 协议的混合体。

拥塞控制：

TCP 拥塞控制的目标是最大化利用网络上瓶颈链路的带宽。只要网络中没有出现拥塞，拥塞窗口的值就可以再增大一些，以便把更多的数据包发送出去，但只要网络出现拥塞，拥塞窗口的值就应该减小一些，以减少注入到网络中的数据包数。常见的 TCP 拥塞控制算法：Reno（它将拥塞控制的过程分为四个阶段：慢启动、拥塞避免、快重传和快恢复）、BBR（BBR 算法不将出现丢包或时延增加作为拥塞的信号，而是认为当网络上的数据包总量大于瓶颈链路带宽和时延的乘积时才出现了拥塞，所以 BBR 也称为基于拥塞的拥塞控制算法）

目前有非常多的 TCP 的拥塞控制协议，例如：

基于丢包的拥塞控制：将丢包视为出现拥塞，采取缓慢探测的方式，逐渐增大拥塞窗口，当出现丢包时，将拥塞窗口减小，如 Reno、Cubic 等。

基于时延的拥塞控制：将时延增加视为出现拥塞，延时增加时增大拥塞窗口，延时减小时减小拥塞窗口，如 Vegas、FastTCP 等。

基于链路容量的拥塞控制：实时测量网络带宽和时延，认为网络上报文总量大于带宽时延乘积时出现了拥塞，如 BBR。

基于学习的拥塞控制：没有特定的拥塞信号，而是借助评价函数，基于训练数据，使用机器学习的方法形成一个控制策略，如 Remy。

6. TCP 拥塞控制中调整发送速率的方法有慢启动、加法提速和乘法降速，总结这些方法的设计原理，并举例说明其运作过程。

慢启动：慢启动阶段思路是不要一开始就发送大量的数据，先探测一下网络的拥塞程度，也就是说由小到大逐渐增加拥塞窗口的大小，在没有出现丢包时每收到一个 ACK 就将拥塞窗口大小加一（单位是 MSS，最大单个报文段长度），每轮次发送窗口增加一倍，呈指数增长，若出现丢包，则将拥塞窗口减半，进入拥塞避免阶段；

加法提速：当窗口达到慢启动阈值或出现丢包时，进入拥塞避免阶段，窗口每轮次加一，呈线性增长；当收到对一个报文的三个重复的 ACK 时，认为这个报文的下一个报文丢失了，进入快重传阶段，要求接收方在收到一个失序的报文段后就立即发出重复确认（为的是使发送方及早知道有报文段没有到达对方，可提高网络吞吐量约 20%）而不要等到自己发送数据时捎带确认；

乘法降速：快重传完成后进入快恢复阶段，将慢启动阈值修改为当前拥塞窗口值的一半，同时拥塞窗口值等于慢启动阈值，然后进入拥塞避免阶段，重复上述过程。

7. 对于可靠数据传输，滑动窗口协议相比停等协议有更好的效率，从两种协议的传输方法原理来对此进行分析。

停等协议：

发送方发送一帧，等待应答信号回应后，继续发出下一帧，接收方在接收到一帧后，发送回一个应答信号给发送方，发送方如果没有收到应答信号则必须等待，超出一定时间后启动重传机制。

滑动窗口协议：

允许发送方发送多个连续的帧，无需等待应答。接收方有一个窗口，窗口大小固定为 W 个帧大小，发送方可以发送连续的帧到接收方（最大发送帧数为 W 个帧），发送方在收到应答信号以前窗口位置不移动。接收方在收到一个帧后（表明没有后续的帧，已经接收完毕），发送应答信号，并将窗口移动到 W-i+1 位置，表明 i 之前的帧已经接收完毕，这种随传送数

据的过程而窗口发生移动，所以被叫做叫做滑动窗口协议。

滑动窗口协议比停等协议效率更高的原因：

停等协议导致线路利用率很低，信道延迟大的情况下，利用率就更低，时间都耗费在等待回应上面了。

8. ATM 和 IP 分属有连接和无连接的网络层协议，从数据包路由和转发的角度，简述两者的区别。

ATM(Asynchronous Transfer Mode)顾名思义就是异步传输模式。ATM 是一种传输模式，在这一模式中，信息被组织成信元，因包含来自某用户信息的各个信元不需要周期性出现，这种传输模式是异步的。

ATM 采用异步时分复方式(即统计复用),将来自不同信息源的信元汇集到一起,在缓冲器内排队,队列中的信元根据到达的先后按优先等级逐个输出到传输线路上,形成首尾相接的信元流。具有同样标志的信元在传输线上并不对应着某个固定的时隙,也不是按周期出现的。异步时分复用使 ATM 具有很大的灵活性,任何业务都按实际信息量来占用资源,使网络资源得到最大限度的利用。此外,不论业务源的性质有多么不同(如速率高低、突发性大小、质量和实时性要求如何),网络都按同样的模式来处理,真正做到完全的业务综合。

IP 协议(Transmission Control Protocol/Internet Protocol)叫做传输控制/网际协议，又叫网络通讯协议。IP 是面向无连接的。

正因为 ATM 是面向连接的，所以通信两端都要管理，比较复杂。ATM 融合了电路交换和分组交换的优点，是一个很好的技术，但就是太复杂。

IP 协议被成为“尽最大能力的协议”，因为它很简单，现在大量使用 IP 网络。

IP 协议是用于将多个包交换网络连接起来的，它在源地址和目的地址之前传送一种称之为数据报的东西,它还提供对数据大小的重新组装功能,以适应不同网络对包大小的要求。

IP 的责任就是把数据从源传送到目的地。它不负责保证传送可靠性，流控制，包顺序和其它对于主机到主机协议来说很普通的服务。

9. NAT 是当前缓解 IPv4 地址不足的主要技术，简述它的技术原理并分析优缺点。

技术原理：

NAT 的基本工作原理是，当私有网主机和公共网主机通信的 IP 包经过 NAT 网关时，将 IP 包中的源 IP 或目的 IP 在私有 IP 和 NAT 的公共 IP 之间进行转换。

我们一般使用私网 ip 作为局域网内部的主机标识，使用公网 ip 作为互联网上通信的标识。在整个 NAT 的转换中，最关键的流程有以下几点：

1. 网络被分为私网和公网两个部分，NAT 网关设置在私网到公网的路由出口位置，双向流量必须都要经过 NAT 网关。
2. 网络访问只能先由私网侧发起，公网无法主动访问私网主机。
3. NAT 网关在两个访问方向上完成两次地址的转换或翻译，出方向做源信息替换，入方向做目的信息替换。
4. NAT 网关的存在对通信双方是保持透明的。
5. NAT 网关为了实现双向翻译的功能，需要维护一张关联表，把会话的信息保存下来。

优点：

1. 节省合法的公有 ip 地址。
2. 地址重叠时，提供解决办法。
3. 网络发生变化时，避免重新编址。

缺点：

1. 无法进行端到端的 ip 跟踪（破坏了端对端通信的平等性）。

2. 很多应用层协议无法识别（比如 ftp 协议 ）。

10. 对 IPv4 和 IPv6 数据包结构进行对比分析，解释 IPv6 数据包结构简化的原因。

对比 IPv4 数据报头部格式可以看出，IPv6 去除了 IPv4 报头中的头部长度、标识、标志、段偏移、校验和、选项、填充这么多字段，却只增加了流标签这一个字段，因此 IPv6 报头处理和 IPv4 报头处理相比大大简化，提高了处理效率。另外，IPv6 为了更好地支持各种选项处理，提出了扩展头的概念，新增选项时不必修改现有的结构就能做到，理论上可以无限扩展，体现了优异的灵活性。

11. 在网络层和传输层都存在有连接服务，比如 ATM 和 TCP，从数据传输过程来分析它们的异同。

ATM 和 TCP 都是面向连接传送机制。先要建立连接然后才相互传送数据。

ATM 和 TCP 都是网络通信协议,但是 ATM 趋向于底层,而 TCP 则趋向于较高层。ATM 在 OSI 七层模式中相当于数据链路层,而 TCP 则是运输层。ATM 以信元为单位，TCP 以分组为单位。ATM 代表的是快速分组交换技术，异步时分复用技术，而 TCP 不属于交换技术。TCP 协议是可以应用在 ATM 网络上的。

12. 分片 ALOHA 的效率高于纯 ALOHA，解释原因。

纯 ALOHA 协议(Pure ALOHA)：

当传输点有数据需要传送的时候，它会立即向通讯频道传送。接收点在收到数据后，会 ACK 传输点。如果接收的数据有错误，接收点会向传输点发送 NACK。当网络上的两个传输点同时向频道传输数据的时候，会发生冲突，这种情况下，两个点都停止一段时间后，再次尝试传送。

分段（或时隙）ALOHA 协议(Slotted ALOHA)：

这是对纯 ALOHA 协议的一个改进，思想是用时钟来统一用户的数据发送。改进之处在于，它把频道在时间上分段，每个传输点只能在一个分段的开始处进行传送。用户每次必须等到下一个时间片才能开始发送数据,每次传送的数据必须少于或者等于一个频道的一个时间分段。**这样很大的减少了传输频道的冲突。从而避免了用户发送数据的随意性，减少了数据产生冲突的可能性，提高了信道的利用率。**

在实际应用当中，分段 ALOHA 协议主要应用在手机网络通信中。而纯 ALOHA 协议因为其较高的频道冲突很少被使用。但是 ALOHA 仍然是很多新的无线通信标准比如 Wi-Fi 的理论基础。

13. 简述 802.3 发生冲突后所用重发算法的工作原理。

CSMA/CD 的工作原理：

由 IEEE 802.3 标准确定的 CSMA/CD 检测冲突的方法如下：

（1）当一个站点想要发送数据的时候，它检测网络查看是否有其他站点正在传输，即监听信道是否空闲。

（2）如果信道忙，则等待，直到信道空闲；如果信道闲，站点就传输数据。

（3）在发送数据的同时，站点继续监听网络确信没有其他站点在同时传输数据。因为有可能两个或多个站点都同时检测到网络空闲然后几乎在同一时刻开始传输数据。如果两个或多个站点同时发送数据，就会产生冲突。

（4）当一个传输节点识别出一个冲突，它就发送一个拥塞信号，这个信号使得冲突的时间足够长，让其他的节点都能发现。

（5）其他节点收到拥塞信号后，都停止传输，等待一个随机产生的时间间隙（回退时间，Backoff Time）后重发。

14. 在 802.3 中，CD（冲突检测）可提高 CSMA 协议的效率，解释在 802.11 中用 CA（冲突避免）而非 CD 的原因。

CSMA/CD 协议已经成功地应用于使用有线连接的局域网，但在无线局域网的环境下，却不能简单地搬运 CSMA/CD 协议。

主要有两个原因：

（1）接受信号的强度往往会小于发送信号的强度，且在无线介质上信号强度动态变化范围很广。因此若要实现碰撞检测，在硬件上的花费就会过大；

（2）在无线通信中，并非所有的站点都能够听见对方。而“所有站点都能够听见对方”正是实现 CSMA/CD 协议必备的基础。

CSMA/CD 协议的特点是：先听再发，边听边发，冲突停发，随机重发；

CSMA/CA 协议的特点是：发送数据时先广播告知其他结点，让其他结点在某段时间内不要发送数据，以免发生碰撞；

15. 从协议层的角度，解释以下网络设备的用途：集线器，交换机，路由器。

集线器：位于物理层

集线器（HUB）属于数据通信系统中的基础设备，它和双绞线等传输介质一样，是一种不需任何软件支持或只需很少管理软件管理的硬件设备。它被广泛应用到各种场合。集线器工作在局域网(LAN)环境，像网卡一样，应用于 OSI 参考模型第一层，因此又被称为物理层设备。集线器内部采用了电器互联，当维护 LAN 的环境是逻辑总线或环型结构时，完全可以用集线器建立一个物理上的星型或树型网络结构。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。

交换机：位于数据链路层

交换机(Switch)是一种基于 MAC（网卡的硬件地址）识别，能完成封装转发数据包功能的网络设备。交换机也叫交换式集线器，它通过对信息进行重新生成，并经过内部处理后转发至指定端口，具备自动寻址能力和交换作用，由于交换机根据所传递信息包的目的地址，将每一信息包独立地从源端口送至目的端口，避免了和其他端口发生碰撞，因此，交换机可以同时互不影响的传送这些信息包，并防止传输碰撞，提高了网络的实际吞吐量。现在的交换机分为：二层交换机，三层交换机或是更高层的交换机。三层交换机同样可以有路由的功能，而且比低端路由器的转发速率更快。它的主要特点是：一次路由，多次转发。

路由器：位于网络层

路由器(Router)亦称选径器，是一种连接多个网络或网段的网络设备，它能将不同网络或网段之间的数据信息进行“翻译”，以使它们能够相互“读”懂对方的数据，从而构成一个更大的网络是在网络层实现互连的设备。所谓“路由”，是指把数据从一个地方传送到另一个地方的行为和动作，而路由器，正是执行这种行为动作的机器，是使用一种或者更多度量因素的网络层设备，它决定网络通信能够通过的最佳路径。路由器依据网络层信息将数据包从一个网络前向转发到另一个网络。它比网桥更加复杂，也具有更大的灵活性。路由器有更强的异种网互连能力，连接对象包括局域网和广域网。

路由器有两大典型功能，即数据通道功能和控制功能。数据通道功能包括转发决定、背板转发以及输出链路调度等，一般由特定的硬件来完成；控制功能一般用软件来实现，包括与相邻路由器之间的信息交换、系统配置、系统管理等。