**局域网**：

节点之间网线的长度不超过100m ，覆盖范围小，带宽固定（10M，100M，1000M），自己安装维护

接入层交换机：直接与计算机相连的交换机；

汇聚层交换机：连接交换机的交换机，带宽要比接入层交换机大，防止拥塞。

**Internet**：由许多ISP组成（网络运营商）。

电信、移动运营商有自己的机房和网络，公司要建立服务器，要向运营商连接网线接口，获取IP地址。

**广域网**：距离远，花钱买服务，带宽不固定。

**网页访问的整个过程： mac地址指明下一站到哪，ip地址指明终点位置。**

计算机具有IP地址，计算机网卡由mac地址；路由器有IP地址也有mac地址。

（1）根据输入的网址，发送给DNS服务器，然后DNS将域名解析为IP地址传给本机，本机再访问这个地址。

（2）给目标地址发送的数据包需要包含（数据、源地址、目标地址）,但是还不够，还需要指明是发送给路由器还是另一台相连的主机，于是还要加上物理地址，构成了数据帧（数据，源地址，目标地址，源MAC地址，下一步的mac地址）。

（3）路由器接收到上一个节点发来的数据帧的时候，由于需要向下一个节点发送数据，所以会把接收的数据帧的mac地址改成现在的mac地址和下一个节点的mac地址。继续向后走。数据包没变，物理地址变了，数据帧变了。

（4）最终，你访问的那个服务器受到了数据帧，能够找到是那个ip访问了他，但是看不到源计算机的mac地址，只能追溯到上一级的mac地址。

（5）服务器受到数据请求后，对大的网页内容进行切割，方便传输。将网页切块编号，将待发的数据放在网卡的缓存里面，发出的时候缓存里面的数据还不能删除，当客户端受到数据之后返回一个成功的指令，才将缓存里面发送成功的数据帧删掉。客户接收的时候也是将其放在缓存里面，然后再慢慢读取显示。

**IP地址：**13.0.0.0，

子网掩码255.0.0.0.；子网掩码的255告诉我们对应的13是网络部分，后面.0.0.0是主机号。以此类推。

网关：出口地址，路由器地址，就是该网络出去之后给的地址就是网关。13.0.0.1.

**路由器：**不同网段之间转发数据，ip地址和mac地址都看，根据ip地址选择路径。

**交换机：**交换机看不懂ip地址，只看mac地址，根据mac地址转发数据。

网卡和路由器都有物理地址（mac地址）出厂就有，全球唯一。

**开放系统互联**：（OSI）体系结构：前三层必须有，中间交换机也有。

应用层：所有能产生网络流量的程序；

表示层：在传输之前是否进行加密或者压缩处理；发送端表示层加密和压缩，接收端表示层解压解密。

会话层：可以查看是否中了木马，只要和外界有联系就会建立会话，在命令输（cmd）入：netstat，能看到已经建立和释放了的会话。

传输层：可靠传输，流量控制，不可靠传输。没收到确认，重复发送（可靠传输）；接收端给传输端发送指令慢点，发送的传输层就会慢（流量控制），纠错处理

网络层：负责选择最佳路径，规划ip地址，路由器。

数据链路层：定义帧的开始和结束，实现透明传输（加入中间数据有些和结束数据相同，会在相同数据前加一些数据，数据链路层接收之后去掉加的东西），差错检验（不纠错）。交换机属于数据链路层。

物理层：接口标准，电气标准，如何在物理链路上传输更快的速度。

分层的优点：每层之间独立，一层的改变不会影响其它层的改变，下一层为上一层提供服务。每一层各司其职。先要解决网络层问题。网络出现了问题，要从底层开始查。

**OSI模型网络故障：**

物理层：查看链接状态，发送和接收的数据包。网线

数据链路层：mac地址冲突，同一个交换机上接的设备mac冲突；ADSL欠费；网速么法协商一致。计算机连接到错误的Vlan。

网络层：规划地址，选择路径。配置了错误的ip地址，子网掩码，网关等，路由器上没有到达目标的路由。

应用层：应用程序配置错误。

判断网络通不通，可以直接ping ip地址。

**OSI网络安全：**

物理层安全；

数据链路层安全：ADSL账号密码；VLAN 交换机端口绑定MAC地址；

网络层安全：在路由器上使用ACL 控制数据流量包，防火墙等

应用层安全：开发的应用程序没有漏洞。

**TCP/IP协议：**

应用层：最高的那前三层

传输层：数据分段

网络层：加地址

网络接口层：包括数据链路层和物理层。

应用层数据在传输层加上TCP的头（数据段）；在网络层加上IP层（数据包）；在数据链路层加上MAC地址和校验值（数据帧），物理层以比特流传输。

**速率：**每个信道（一个发送端与一个接收端）上的比特率**；** 10M的网速指的是比特率，10Mbit/s（每秒多少位）;但是**计算机中显示流量速度**的时候是每秒多少字节，就需要比特率/8，实际上除于10的样子。

**带宽**：数字信道所能传送数据最高的速率。

**吞吐量：**单位时间内通过某个网络的数据量。总的流量（加）。

**时延**：

发送时延：数据块的长度（比特）/信道的带宽（比特/秒）。

传播时延：

处理时延：

排队时延（排队超过路由器的缓存直接丢包）：

带宽改变的是发送时延，带宽越大发送时间越短，但是传播时间不会变，传播时间取决于介质。如果只提高发送带宽，则数据帧长度越短，接收端很难识别。光纤可以识别。光纤可以接受更快的发送速度，但是传播速度铜线比光纤快，但是铜线不支持高的带宽。

**时延带宽积**：传播时延X带宽。线路上存在的比特，提高了带宽，链路上的数据就增加了一倍。

**往返时间**：A发送数据，B返回接收到了数据的时间。Ping测试。

**信道利用率**：有数据通过的时间/（有+无）数据通过的时间。

**网络利用率**：信道利用率加权平均值。

**物理层：**在传输媒体上传输数据比特流，确定媒体的接口的特性。机械特性，电气特性，功能特性，过程特性。

**数据通信的基础**：

数字信号：0和1组成，是离散的；

模拟信号：信号连续变化；

计算机网卡发出的是数字信号；

数据：运送消息的实体；

信号：数据的电气或电磁的表现；

码元：用时间间隔相同的线条来表示二进制中的一位，这样的时间间隔内的信号称为二进制码元。一位数据波形的时间间隔称之为码元长度。1码元可以代替n bit的信息量（当电压被编码成很一个范围内，不是以高低区分，比如4v电压对应一个码元，4二进制是三位，此时一个码元携带了3bit信息量）。

信道：向一个方向传送信息的媒体。

单工（单向通信）：只能有一个方向的通信，没有反向的交互。收音机

半双工：双方都可以收发，但是不能同时。对讲机

全双工：双方可以同时收发。手机

基带信号：基本频带信号，信号源的信号，传输距离近可以采用此方式传输。

带通信号：基带信号经过载波**调制**后，将信号频率搬移到较高的频段以便在信道中传输。接收的时候也需要过滤。长距离传输。

调制方法：（1）调幅：高电平才有振幅，低电平没有振幅；（2）调频：高低电平的频率不一样；（3）调相：高低电平的相位不一样。

常用编码：

（1）单极性不归零码： 表示电压只有0-A之间变化，1对应A，0对应0，不归零持续到下一位。

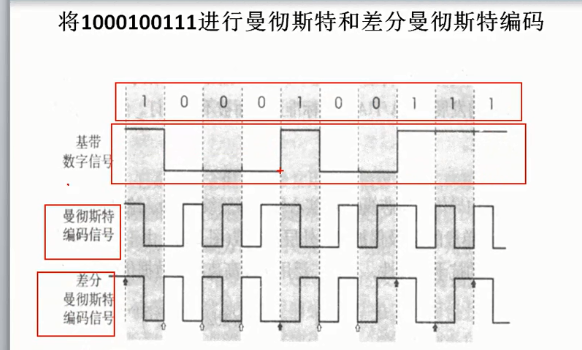
（2）双极性不归零码：电压在-A-A之间变化，1对应A，0对应-A。

（3）单极性归零：出现1的时候需要归零，就相当于原来一位的时间片分成了两部分，一部分用来表示1，一部分归零。

（4）双极性归零：同上。1的时候要归零，0的时候也归零。

（5）曼切斯特编码：高电平跳变为低电平代表1；低电平跳转为高电平代表0；其能够携带时钟信号，且可以表示是否有数据传输。跳转的时候是一个时钟的中间部分。

（6）差分曼切斯特编码：bit中间有信号跳变，bit与bit之间也有信号跳变。上一个bit与下一个bit之间有跳转，并且bit中间有跳转代表0；bit与bit之间没有跳转，bit中间有跳转代表1。



奈氏准则：信道极限容量：没有信噪干扰的情况下，发送速度不能太快，太快容易造成码元之间的干扰，码元的传输速率是有上限的。

香农公式：信噪比：传输速率与噪声之间的关系。总噪声越大，传输速率的极限越小。噪声越大，要不失真，就需要降低传输速度。无差错传输的公式。

奈氏准则适用于码元传输，香农定理可以适用于数字和模拟信号。

**传输媒体**：

（1）导向传输媒体：屏蔽双绞线（STP）；无屏蔽双绞线（UTP）；同轴电缆。双绞线有8根，有顺序的，100M和10M的网络只用了1,3，2,6四根线，但是千兆网络就用了8根。

直通线：主机与交换机或集线器连接，路由器到交换机或者集线器的连接；线的序号对应相连1-1；2-2；3-3 ；

交叉线：同类设备之间的通信，线的序号需要改变1-3；2-6。

2）光纤：多模光纤（可以传输多种入射角的信号）；单模光纤（带宽大，传播性能好，直接传，不用反射）。

（2）非导向传输：微波，地面卫星。

**物理层设备**：

（1）集线器：信号放大和重发的作用，扩大网络传输范围，不具备信号定向传输的能力，集线器在某段时间内，只能有两台设备进行通信，集线器的信号会给所有连接口发送数据，但是只是其他的设备因为mac地址不能构成通信。集线器类似于网线，是物理层设备。集线器是共享带宽，带宽平均到每台设备。集线器是一个大的冲突域。

**信道复用技术**：多个信道的数据在一根链路上传，还能拆分出来。

（1）频分复用FDM：所有用户占用不同的特定频率。不同的信源通过不同的频率调制叠加之后传，然后接收端先分开过滤，然后解调。

（2）时分复用TDM：在相同的时间段内每个信源都发送一定大小的数据块（一定的顺序）组成一个数据帧。可能造成线路的浪费，因为有的设备可能没有数据需要传输，但是还是会分配时间。

（3）统计时分复用STDM：每个信道传输数据的时候会加上标记，无规律传输，接收的时候通过标记分开。就不会出现时间的分配。

（4）波分复用WDM：光的频分复用。

**数字传输系统：**广域网的传输

脉码调制PCM：数据采样，数据保持，数据量化，数据编码；

**宽带接入技术**：

（1）ADSL（拨号上网）：通过电话线上网，0-4kHZ的低频段给电话使用，1MHZ以上的频率用于网络传输。DMT调制技术：频分复用。并行传输。上行信道（上传）和下行（下载）信道是非对称的。

（2）光纤同轴混合网HEC：

**数据链路层**：不关心信号的类型，只关心数据帧的开头和结尾，是否错误，以及数据链路层的封装。传输的数据是帧。对网络层的数据加上帧头，帧尾、校验。MAC地址。

**数据链路层的信道类型**：

（1）点到点通信：一对一通信；

（2）广播通信，一对多通信。

**链路**：一条点到点的物理线路段，中间没有任何节点

**数据链路**：除了物理线路之外，还有实现传输协议的硬件和软件。

**帧**：在IP层加上了ip地址，在数据链路加上了开头和结尾和校验。

数据链路层的工作：

（1）封装成帧：加上标记，如果数据中出现了开始和结束的标志数据，就在该数据前插入字节填充（转义字符ESC），受到之后会把ESC去掉。

（2）透明传输：去掉转义字符

（3）差错控制：数据的位发生了变化，传输错误的bit占bit总数的比率为**误码率**。有错误就把数据扔掉，不会纠错。

**差错检测措施**：帧检验序列

**CRC（循环冗余校验）**：得出的余数（FCS）为帧检验序列。（再学），不能确定是哪出错了，有可能出现错误检测不出来，如果除数位数多，检测精度越高。

**广域网**：点到点通信：中间一根线，没有其它设备，采用的协议是**PPP协议**，数据链路层协议。PPP协议的组成：用于异步串行或同步串行介质；使用LCP（链路控制协议）建立维护数据链路连接（身份验证，计费功能）；网络控制协议（NCP）允许点到点连接使用多种网络层协议。PPP帧的长度都是整数的字节。

**局域网**：广播信道通讯：局域网的拓扑：星型网；总线型（总线型需要两端接电阻，吸收信号，防止反射）；环型网；树形网。广播实现一对一通信，集线器和总线上所有的电脑都能收到数据，只是mac决定了那个电脑能够处理接收该数据。

**广播信道局域网协议**：**载波监听多点接入/碰撞检测 CSMA/CD协议**：多点接入：计算机以多点接入的方式连接在一根总线上；载波监听：在发送数据之前检测一下总线上是否有其他计算机正在发送数据，以免碰撞，利用电子技术检测。碰撞之后，本计算机会接收到幅值增大的信号，表示碰撞了。只能进行半双工通信。发送数据在2t时间之内都有可能发生碰撞，t是发送到接收端的时间。集线器理论上平摊了总的带宽，但是存在碰撞。2t就是争用期；

二进制指数类型退避算法：发生碰撞的站停止发送数据后，推迟一个随机时间才能再发送数据。一般取基本退避时间取争用期2t。当重传16次仍然不能成功就丢弃该帧，向高层报告。

**以太网**： DIX ENTHERNRT V2标准和IEEE 802.3标准；CSMA/CD的标准都称之为以太网。以太网提供的服务是不可靠交付，数据链路层，只提供无差错接收。

信道利用率：

**Mac层**：网卡的地址，48位二进制组成，确保全球唯一。前24位代表厂家，后24位代表地址。可以不使用网卡的mac地址，用一个自己改动的MAC地址。

目标MAC地址是全F的，表示广播。

**优化以太网**：

集线器级联，可以使得计算机数量增加，但是构成了巨大的冲突域，效率降低。

网桥：（用于分隔局域网）（网桥是接集线器的）工作在数据链路层，连接在不同集线器之间。会记住MAC地址，但是需要先学习，就是刚开始还是群发，记录发送数据的计算机的mac地址，然后接下来就不会群发，会根据记录的mac地址来决定发给那个HUB。

交换机：前身是网桥，交换机直接接的是计算机。学习了mac地址，就不会构成冲突，而且能够存储转发，先过来的先发，其他过来的可以排队等候。全双工通信。端口带宽独享，基于mac地址转发，能够学习mac地址，安全。

半双工使用CSMA/CD协议；全双工不使用该协议。

**网络层**：（四个协议）不管数据包是否正确，只是拼命的发和传，不负责丢包，和顺序的事情，只负责在不同网段之间转发数据包，不负责丢失重传，也不负责顺序，是随机的传送。可能一个数据被拆分成多个数据包，每个数据包都是单独发送的，可能走的路径不一样，网络层值负责传送他们，不管顺序和对错。

**路由器**工作在网络层，能看到网络层的内容。只要没有经过路由器，那就同属于一个局域网络的网络内。

子网掩码告诉计算机网络部分是哪几个部分。那部分是255，那部分就是网络部分。

一般：网关都是使用网段中的第一个地址，xx.xx.xx.01.接这些计算机路由器的进口地址。告诉计算机信息出口发给这个路由器。然后路由器出口的ip地址会自动路由。接收口是反过来。

路由器选择路径是根据路由表来选择的，需要管理员配置路由器，告诉路由器怎么才能到某个网段。就是路由器到底怎么走是有路由表来决定的。

**传输文件的准备工作**：

1、应用程序准备要传输的文件；

2、传输层将文件进行分段和编号；（数据段）

3、网络层给每个数据段加ip地址（目标IP和源IP）。（数据包）

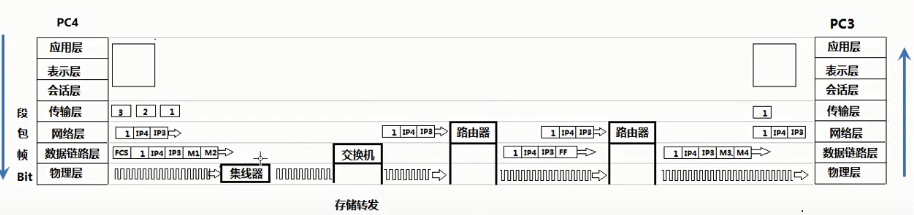
4、在数据链路层：使用自己的子网掩码判断自己在那个网段，使用自己的子网掩码判断目标在那个网段，如果是同一个网段（不通过路由器）直接使用ARP协议，直接广播询问计算机MAC地址；如果不是一个网段，ARP需要广播找到路由器的MAC地址。（数据帧）

5、物理层变成比特流。（比特流）

集线器：放大传输；物理层

交换机：存储转发；数据链路层，能看懂mac地址。

路由器：看不懂数据，但是能看懂mac地址和ip地址。去掉当前的mac地址，根据路由表选择路径，重新分配数据帧，重新写mac地址。点到点传输，目标mac地址就是FF。



**ARP协议**：数据通信前，先发送一个目标地址全F的广播，解析同一网段和网关的MAC地址。为IP协议提供服务。将IP地址在本网段中通过广播发出，目标地址为FF-FF-FF-FF-FF-FF，解析本网段目标IP地址的MAC地址。查看的时候，先ping以下目标地址，然后arp –a查看目标ip的MAC地址。**ARP欺骗**：就是在源计算机发送广播的时候，同一网段下的某台计算机黑客配置之后，可以在目标计算机发送了真是MAC地址之后，立即将本机的MAC地址也发送出去，能够覆盖目标的IP地址，这样就能使得源计算机将该计算机当做了目标的MAC地址。 Arp –a就能显示网关的物理地址。“”Arp –s ip 正确的MAC地址”给某个计算机绑定静态的MAC地址，就能避免arp欺骗。

**ICMP协议**：检测网络是否畅通。ping使用的是这个协议，局域网ping的延迟应该小于10ms，否则说明局域网太堵了。ping 中TTL是生存周期，每经过一个路由器就减1；防止其经过无限的路由器，占用带宽，当TTL==0的时候，就消失了。Linux 发出的TTL是64；windows的TTL 是128，UnixTTL是255，可以大概的判断对方系统。“ping ip -t”可以一直ping，crtl+c撤销。“ping ip –l 200”指定200大小的数据包来ping。“ping ip –i n”，n从1到n可以测试出沿途经过了哪些路由器（相当于设置TTL的值），显示出路由器的ip地址。“pathping”能够测试出来计算机到哪是不通的，还可以计算每一节的丢包情况。“tracert ip”能计算沿途的路由器。

**IGMP协议**：组播=多播：介于点到点和广播之间。以不同的多播的ip地址通信，不能快进类似于电视节目。点到点可以快进。多播节省带宽。IGMP配置在路由器上，扫描有多少计算机访问多播地址，如果有计算机访问多播地址，则向上一级请求获取多播数据。点播是可暂停继续的，需要建立会话。多播不可以暂停，快进；多播不建立会话。

**IP协议**：由首部和数据（来自于传输层）构成，首部的前一部分是固定长度20字节，是所有ip数据报必须具有的，在首部固定部分的后面是一些可选字段，其长度是可变的（一般没有）。开头半个字节是版本用来标识TCP/IP的版本V4或者V6；接下去半个字节是ip数据的首部长度；接下来一个字节是区分服务，建立优先级；接下来两个字节是总数据包的（不包括固定部分）长度，数据链路层的数据包最大支持是1500个字节，网络层数据包支持最大65535个字节，由此可见网络层传给数据链路层的包太大了，就需要分片了。接下来两个字节是标识，用于接收端受到分片数据能够根据标识组装成整个数据包，相同标识的数据包一起组装。接下来3位是标志，用于表示这是个分片数据包，可以用来确定该数据包是否最后一个数据包，010表示不分片，001表示允许分片，000表示允许分片同时是分片的最后一片，而且后面还有分片数据包。**接下来13位**是片偏移，偏移量就是每个数据片数据开头的第一个字节是整个完整数据包第多少个字节，也就是在整个数据包中的位置。接下来一个字节是生存时间就是TTL，每过一个路由器减1，减到0就消失，就会告诉计算机本数据不能前传了，防止进入死循环。接下来一个字节是协议，ICMP（协议号是1）,IGMP（协议号2）,TCP（6）,UDP（17）.接下来两个字节是首部检验和，用于检验首部是否错误，错误就丢掉，反码运算求和检验。接下来四个字节是源地址，接下来四个字节是目标地址。接下来四个字节是可变部分和填充。

网络畅通的条件是有去有回。有时候ping不通可能是有去但是没有回。

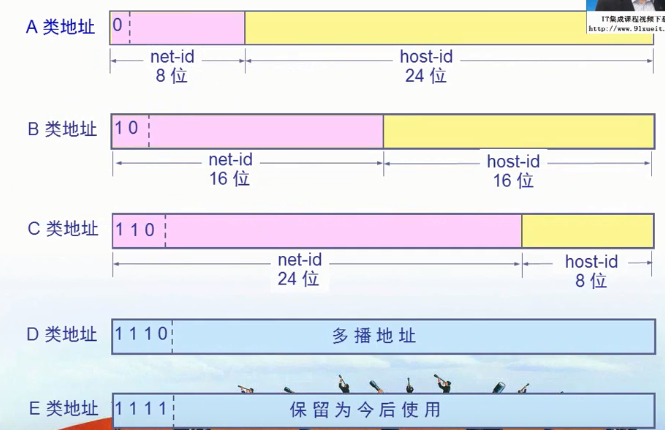
**IP协议**：静态路由（管理员设置路由的分配）；动态路由（路由器自己学习分配路由），（1）RIP；（2）OSPF；

**静态路由：**需要告诉路由器达到目标地址，该路由器下一步需要达到的路由器的地址。必须得配置到哪个ip地址的下一跳到哪，即使路由器能够访问到最远的ip，但是也可能ping不通中间路由器，因为目的地址是路由器的了，如果路由表中没有静态写入这个地址作为目的地址的路由表，则不通。没有直接连接的路由器，就需要将未直接连接的路由器和计算机设置为目的地址，并且配置路由表。需要告诉路由器没有直接连接的网络下一跳给谁。适合于小的网络，不能自动的适应网络的变化。

**动态路由**：路由器自己学习，RIP协议：经过的路由器越少，路径越优，给下一个路由器RIP广播，告诉路由器到达起点需要经过多少跳数（几个路由器），30s广播一次，更新网络状态。RIP周期性广播路由表，30s更新一次（目的是告诉下一个路由器自己还能工作），最大跳数是15跳，超过15跳认为不可达到。根据跳数选择最佳路径，所以不适用于大型的网络。

**TCP/IP专题**：IPV4是4个字节构成，分为网络号和主机号，网络号相当于区号，同一网段的计算机网络号一样，主机号不一样。

**IPv4分为ABCDE五类**：A类地址第一个字节为网络号，主机数为256\*256\*256台（主机部分不能全为1，也不能全为0）。B类地址前两字节为网络号，主机数为256\*256；C类地址前三个字节为网络号，主机数是256。D类地址用于组播，E类地址研究中。第一个字节判断：A类地址从1-127.，127.网段代表的本机的ip地址相当于自己。B类128.-191；C类192.-224；D类225-240； E类240-255。子网掩码255部分对应的就是网络部分，0的部分对应主机的部分。特殊的地址：“127.0.0.1”本地环回地址；“169.254.0.0”计算机没有获得ip地址，就会自动生成一个地址；“10.0.0.0”保留的A类地址；“172.16.0.0-172.31.0.0”16个B类保留地址；“192.168.0.0-192.168.255.0”C类保留地址；保留的地址都是私网地址，外面的网连不进去。



**子网掩码**：告诉计算机网络部分和主机部分，计算机将自己的ip地址与子网掩码进行与运算，然后子网掩码与目标地址进行与运算，两者结果相同，则在同一个网段，不经过路由器通信，否则计算机将数据给网关，就是路由器地址，一般使用网段第一个地址。

**子网划分**：每次划分就是将主机号部分对半分，先0-255的一半128，然后再半分。

**等分划分**：就是分成不同的子网段，用路由器通信。将主机号拆分出一部分来作为网络部分。主机号要避开全1和全0的情况，这个时候子网掩码不一定是255了，最后那个字节就算网络的那个数。比如将C类网络拆分成2个子网，就需要从主机号中拿出一位，这样主机号只有7位，然后避开全0和全1，主机就是1-126一个网段（127是全1的不行，全1是广播），129-254一个网段。然后子网掩码就是255.255.255.128（网络号全1，主机号全0）。如此类似可以继续分网段，但是主机数减少了。点到点网络子网掩码是255.255.255.252.划分子网就是将主机号的个数除于2，每划分一个子网，分界线就是除于2的地方；以上是等分的情况。

**变长子网划分**：可以不等分，就是有的网络号只占其中一位，有的只占两位，然后就是子网掩码不同，就可以划分出不同主机数的不同网段。每次划分都是除于2.

**超网合并**：将网络号的尾部的一部分给主机号，作为主机号，这样子网掩码就变了，就把之前不同的网段划分到一个网段了。小的那部分是偶数就可以合并。

**传输层**：只有两个协议TCP协议（传输控制协议）和UDP协议（用户数据报协议）。

**TCP协议**：需要将要传输的文件分段传输，需要建立会话，可靠传输，流量控制功能。

**UDP协议**：一个数据包就能完成数据通信，不分段，不建立会话，不需要流量控制，不可靠传输。域名解析的时候就是UDP协议；qq聊天是UDP；屏幕广播，或者多播。

**传输层协议与应用层协议的关系**：TCP（UDP）+端口=应用层协议；http=TCP+80（端口）；https=TCP+443;（远程桌面） RDP=TCP+3389; ftp=TCP+21; 共享文件夹=TCP+445；SMTP=TCP+25; telnet=TCP+23; POP3=TCP+110; SQL=TCP+1433; DNS=UDP+53. 利用端口侦听客户端请求。

**服务和应用层议之间关系**：服务使用TCP或者UDP端口侦听客户端请求，使用IP地址定位服务器，使用目标端口定位服务，可以在服务器网卡上设置必要的端口保证网络安全。根据传送过来的包的目标端口和协议，选择不同的协议和端口进行接待，进入相应的应用层协议，进入相应的服务。设置网卡只开放必要的端口，就能保证网络安全。

查看侦听端口：命令窗口输入netstat –an；netstat –n可以查看会话，看到是那个端口的服务。

**传输层功能**：为相互通信的应用程序提供逻辑通信。进行差错检验。