1.

纯ALOHA：纯ALOHA当一帧首次到达，节点立刻将该帧完整地传输进广播通道，如果一个传输的帧发生了碰撞，这个节点该立刻以概率P重传该帧，否则该节点等待一个帧传输时间。纯ALOHA协议的信道利用率最大不超过18.4%（1/2e ）。

时隙ALOHA：每个帧分为多个时隙，节点只在时隙起点开始传输帧。重发策略与纯ALOHA相同 ，等待一段随机的时间，然后重发；如再次冲突，则再等待一段随机的时间，直到重发成功为止。将时间离散化，所以发生重叠的可能性很小，冲突危险区是纯ALOHA的一半，所以,与纯ALOHA协议相比，降低了产生冲突的概率，信道利用率最高为36.8%。

2.

令P是一个概率，当节点中有一个新帧要发生时，它等到下一个时隙开始并在该时传输整个帧，如果没有碰撞，则不用重传，如果有碰撞，该节点在时隙结束之前检测到这次碰撞，以概率P在后续每个时隙中重传这个帧，直到该帧被无碰撞地传输出去。

3.

802.11使用的是碰撞避免而非碰撞检测。CSMA/CA主要着眼点在冲突的避免，协议里也看到经常是等待一段时间再做动作，通过退避尽量去避免冲突，还有就是先发送一些特别小的信道侦测帧来测试信道是否有冲突。CSMA/CD主要着眼点在冲突的侦测，当侦测到冲突时，进行相应的处理，要求设备能一边侦测一边发送数据。在802.11适配器上，接受信号的强度远小于发送信号的强度，制造具有检测碰撞能力的硬件代价较大，适配器还会由于隐藏终端问题和衰减问题而无法检测到所有的碰撞。

4.

集线器：工作于物理层，作用于各个比特而不是作用于帧。

交换机：工作于链路层，它可以为接入交换机的任意两个网络节点提供独享的电信号通路，把传输的信息送到符合要求的相应路由上。交换机的过滤和转发借助于交换机表完成，记录了通向MAC地址的交换机接口，具有自学习功能.

路由器：工作于网络层，连接不同的网段，负责将局域网连接到广域网和互联网中。在路由器中记录着路由表，它会根据信道的情况自动选择和设定路由，以最佳路径，按顺序发送。

5.

10Mb/s = 10b/us，200000km/s = 200m/us

帧的最小长度(b) / 数据传输速率(b/us) = 2 \* 任意两结点间最大距离（m）/ 电磁波传播速率(m/us)

2 \* 2000 \* 10 / 200 = 200b

6.

数据链路层：负责建立和管理节点间的链路。通过信道划分协议或者随机接入协议，将有差错的物理信道变为无差错的、能可靠传输数据帧的数据链路。在物理层提供的比特流的基础上，通过差错控制、流量控制方法，使有差错的物理线路变为无差错的数据链路。

网络层：通过路由选择算法，为报文或分组通过通信子网选择最适当的路径。该层控制数据链路层与传输层之间的信息转发，建立、维持和终止网络的连接。数据链路层的数据在这一层被转换为数据包，然后通过路径选择、分段组合、顺序、进/出路由等控制，将信息从一个网络设备传送到另一个网络设备。常用的路由选择协议有：OSPF，BGP

传输层：向用户提供可靠的端到端的差错和流量控制，保证报文的正确传输。该层常见的协议：TCP/IP中的TCP协议。传输层提供会话层和网络层之间的传输服务，这种服务从会话层获得数据，并在必要时，对数据进行分割。然后，传输层将数据传递到网络层，并确保数据能正确无误地传送到网络层。

7.

对称加密算法：对称加密算法的加密和解密使用的密匙是相同的，也就是说如果通讯两方如果使用对称加密算法来加密通讯数据，那么通讯双方就需要都知道这个密匙，收到通讯数据后用这个密匙来解密数据。

非对称加密算法：非对称算法中用到的密匙有两个，分别是公匙和私匙，要求通讯双方都有自己的公匙和私匙，自己公匙加密的数据只有自己的私匙才能解开，自己私匙加密的数据也只有自己的公匙才能解开。公匙是可以公布在网络上的，可以被其他人获取到的。

电邮加密：

A先对自己的消息内容进行散列运算，得到H(m)，然后用A的私钥对H(m)加密。再用一个随机对称会话密钥Ks，对前面用私钥加密过的H(m)和原消息一起进行加密，再和用B的公钥对Ks进行加密后一起发送给B。B要求知道A的公钥。

在这个加密过程中，A B都要有自己的公钥和私钥，A还要有一个对称加密算法Ks。

数字签名：

A先对自己的消息内容进行散列运行，得到H(m)，然后用A的私钥对H(m)加密，最后把前面用私钥加密过的H(m)和原消息一起发送给B。

在这个加密过程中，A要用到B的私钥，B要用到B的公钥。

8.

IPSec适用于网对网的VPN连接，广泛应用于VPN路由器部署中。IPSec两端的软件需要供应商相同，不利于建立企业外网的应用。需要配置管理通讯的每个结点，且从特定设备接入，提高了配置和运行的成本。

SSL比较适用于移动用户的远程接入，广泛应用于网络安全交易和远程控制。SSL让企业实现多用户在不同地点接入，需要维护中心结点和网关设备，客户端免维护，对客户端设备要求低，降低了配置和运行成本。

IPSec是网络层保证IP通讯而提供的协议族，以网络层为中心。在UDP层进行协商，使用端口500，需保留重传计时器。允许多个用户使用两个端点间的同一隧道，可以减少因建立单个连接所需的开销。

SSL是套接字层保护HTTP通讯的协议，以应用层为中心。握手协议在TCP层进行协商，使用端口可以根据应用程序不同而有所改变。需要为每一个用户分配单独的通道及密钥，相互之间互不影响。

IPSec先对数据进行加密，然后为加密的数据生成消息鉴别码MAC。IPSec在进行任何解密过程之前，先验证MAC。

SSL先为明文创建MAC，然后再对数据进行加密。SSL先将数据包解密，然后再验证MAC。

IPSec支持一种身份验证方法，SSL支持多种不同的身份认证方法。

IPSec采用双向身份验证，SSL采用单向/双向身份验证。