1. 能介绍一下OSI七层模型各层之间的功能与对应的协议吗?

答：OSI七层模型自底向上依次是：物理层、数据链路层、网络层、运输层、会话层、表示层、应用层。各层的功能与相应的协议有：

① 物理层：屏蔽传输媒体以及通信手段的差异，只关注如何在物理介质上传输二进制数据，主要协议有IEEE 802等；

② 数据链路层：为网络层提供服务，将二进制数据封装成帧、进行透明传输与差错检测，无论比特流是什么样的组合，都可以无差别的在物理介质上传输，并且有特定的传输地址，主要的协议有PPP、CSMA/CD协议等；

③ 网络层：网络层向上提供简单的、无连接的、尽最大努力的交付，利用IP地址以及路由选择将各种异构的网络相连接。主要的协议有：IP、ICMP、IGMP、RIP、OSPF协议等；

④ 运输层：提供从一个进程到另一个进程之间的逻辑通信，实现可靠传输、流量控制、拥塞控制以及连接控制等功能。主要的协议有：TCP、UDP协议等。

⑤ 会话层：建立或解除与其他节点的联系；

⑥ 表示层：数据格式化、数据加密；

⑦ 应用层：为应用程序提供服务。主要的协议有：FTP、SMTP、HTTP（建立在TCP上），DNS、SNMP（建立在UDP上）。

2. 计算机网络为什么要分层？分层的优点是什么?

答：由于计算机网络　是一个复杂而且大的系统，分层主要是利用分而治之的思想，将大的问题分解为若干个更小的子问题，从而将复杂问题简单化。分层的主要优点有：

① 各层之间相互独立：每层只需要用合适的技术解决独立的问题，并不关心相邻层之间的实现，只是接受下层提供的服务，并为上层提供服务，降低问题复杂度；

② 灵活性好：当任何一层发生变化时，只要保持各层接口不变，则对某一层的修改将不影响相邻层间的功能实现；

③ 结构上可分割：每层都可以采用最合适的技术来实现该层的功能；

④ 易于实现和维护；

⑤ 促进标准化工作：每层之间有明确的功能与服务。

3. 协议的三要素是什么?

答：① 语法：规定传输数据的格式；

② 语义：规定所要完成的功能；

③ 同步：规定各种操作的顺序。

4. 计算机常见的性能指标有什么?

答：常见的性能指标有：

① 速率：表示单位时间内发送比特的数量；

② 带宽：带宽是物理链路的上限，它决定了物理设备单位时间内最多可以向链路发送多少比特的数据；

③ 吞吐量：单位时间内通过某个网络的数据量，受限于物理设备；
（区分：速率好比一个衡量指标，即一辆汽车的行驶速度km/h；带宽则是不同道路的限速，有的限速100km/h，有的60km/h；吞吐量则是某段道路中汽车实际行走速度）
④ 时延：包括排队时延、发送时延、传输时延和处理时延；
⑤ 时延带宽积：时延 × 带宽，是一种衡量指标，用于某段链路当前有多少比特量；
⑥ 往返时间RTT：从发送方发送数据开始，到发送方接受到接收方的确认所经过的时间；
⑦ 利用率：包括信道利用率和网络利用率。

5. 什么是码元?

答：码元指的是一段固定时间内信号的波形，即代表不同离散数值的波形。一个码元可能携带不同大小的数据量，例如以低电平与高电平两种不同波形的码元只能携带1bit的数据量，分别用低电平和高电平表示0和1。通常用波特率来表示码元传输速率，即每秒传输多少个码元。

6. 奈氏准则是什么?

答：如果码元的传输速率过快，则会出现码间串扰的现象，即由于失去了码元之间的清晰界限从而导致接收方无法正确识别码元的波形的现象。奈氏准则规定了在理想条件下，为了避免码间串扰，极限码元传输速率应该是2W，W是信道带宽。同时也可以推出，理想信道下的极限数据传输率是2Wlog2V，其中V是码元的离散电平数（几种变化）。
计算题：带宽3KHz，采用4个相位，每个相位4钟振幅的QAM调制技术，最大?

7. 香农公式是什么?

答：通常在带宽受限并且有噪声的信道中，为了不产生误差，信息的传输速率有上限，这就是香农定律，而香农公式则是用于计算该极限数据传输速率的，其计算方式为Wlog2（1+S/N）（单位b/s），其中S/N是信噪比。信噪比还有另外一种等价的方式，单位为分贝，计算方式为10log10（S/N）。前提：信道是高斯白噪声信道。
计算题：给出信噪比的dB数值，反推出S/N，再代入公式计算。

8. 你了解的数据链路层组帧方法有什么?

答：① 字符填充法：为了区分不同帧的开始与结束，防止帧中出现与首部或者尾部相同的字符组合，在数据中在出现与首部或者尾部相同的字符之前插入转义字符；② 零比特填充法：在发送端，扫描整个信息段，只要发现连续5个1，就插入一个0，在接收端，发现连续五个1后，就把紧接着的0进行删除。

9. 简述一下CSMA/CD协议。

答：CSMA协议是指载波监听多路访问协议，分为以下三种：
① 非持续式：监听到介质空闲则开始发送，否则等待一个随机时间再发送；
② 1-持续式：监听到介质空闲则开始发送，否则持续监听，一旦空闲立刻发送（容易冲突）；
③ p-持续式：监听到介质空闲则，则以p概率发送，（1-p）概率等待随机时间再发送；若忙则持续监听，一旦介质空闲，重复上述操作。

CSMA/CD协议的执行流程如下：

（1）在发送数据前，网络适配器监听信道。如果信道忙，则持续等待；如果信道空闲，则在等待一段细微时间后将开始传输数据；

（2）在传输数据的过程中，一边传输一边监听信道是否发生碰撞。如果在争用期之内没有检测到碰撞，则说明已经独占信道，可以持续至完成发送；若在争用期内发生碰撞，则将停止数据发送，并发送一个拥塞信号；

（3）检测到发生碰撞后，适配器将执行二进制退避算法随机等待一段时间后，在进行数据发送。

10. 简述一下与自治系统AS相关的内部网关协议和外部网关协议?

答：内部网关协议是指自治系统内部所使用的路由选择协议，一般有路由信息协议RIP和开放最短路径优先协议OSPF。

RIP：RIP协议是一种分布式的，基于距离向量的路由选择协议，它要求每一个路由器都维护一个从它自己到其他每一个网络的距离记录。一条RIP路径最多包含15个路由器，当距离为16时表示不可达。该协议中路由器只和相邻路由器进行信息交换，交换的信息是路由表；

OSPF：OSPF协议中路由器发送的信息是相邻路由器的链路状态，并且使用洪泛法进行发送。最终，每个路由器都将建立一个链路状态数据库，即整个网路的拓扑结构。

外部网关协议是指在不同自治系统之间交换可达性信息的协议，通常每个自治系统需要选择一个路由器作为BGP发言人，并且建立TCP连接，利用BGP会话交换路由信息。

11. 简述TCP和UDP的异同点?

答：相同点：TCP和UDP都是传输层协议，都是保证网络层的传输，双方的通信都需要开放端口；

不同点：① TCP是可靠传输，UDP是不可靠传输；② TCP是面向连接的，UDP是面向无连接的；③ TCP使用套接字或者端口建立通信，负载与开销较大，UDP由于不需要事先建立连接，开销较小；④ TCP首部与UDP首部结构不同；⑤ TCP提供流量控制，拥塞控制，超时重传等功能，UDP不提供可靠性；⑥ TCP是面向字节流的，而UDP是面向报文的；⑦ TCP只提供点对点的全双工通信，而UDP支持一对多，多对多和多对一通信。

12. 简述TCP的三次握手和四次挥手过程？为什么不能采用二次握手?

答：三次握手：在建立TCP连接时，A首先向B发送一个请求建立连接报文段，同步位SYN设置为1，ACK为0，序列设置为x；B收到后，将会向A发送一个确认报文，SYN为1，ACK为1，设置序列为y，确认号是x+1；A收到B的确认后，会发送对B的确认的确认，SYN为0，ACK为1，序列为x+1，确认号是y+1，并且此时可以携带发送数据；

四次挥手：释放TCP连接时，A向B发送请求释放连接报文段，FIN设置为1；B收到后，向A发送确认帧，ACK为1，此时进入半关闭状态，A不再发送数据，而B会继续发送未发送的数据；B发送完数据之后，会向A发送一个请求释放报文，FIN为1；A收到后也会返回一个确认报文，ACK为1，并且等待2MSL后关闭；B收到来自A的ACK后关闭。

为什么不能二次握手：先假如出现了一种异常情况，即A发出的第一个连接请求报文段因为在某些网络节点上滞留了。由于超时重传，于是A又向B发起请求并成功建立了连接，在传输完数据之后，AB同之间释放了连接。而在A和B已经释放连接之后，那个在网络上滞留的报文段又达到了B。这时候，B接收到报文以为是A发起的新的一次建立连接的请求，于是就向A发出确认建立连接报文段。而A此时并没有发起建立连接的请求，于是不予理睬。但是B以为新的连接已经建立，一直等待A发送数据，于是B的许多资源就浪费了。

为什么挥手需要等待2MSL之后才关闭：第一，为了保证A发送的最后一个ACK报文段能够到达B。因为这个ACK报文段有可能丢失，这样B就无法接收到而进入CLOSED状态。于是B会重传请求释放连接的报文段，A在这段等待时间接收到了，重传ACK报文段，这样B还是会顺利接收到确认报文段，进入CLOSED状态。如果此时A已经关闭了，那么就无法收到B的请求报文段，也不会发送ACK报文段，这样B就无法进入CLOSED状态了。第二，在这2MSL的等待时间内，本次连接的所有报文都已经从网络中消失，从而不会出现失效的报文出现在下次连接中。

13. 介绍一下TCP和UDP的头部结构?

答：UDP首部有8个字节，由4个字段构成，每个字段都是两个字节，包括：源端口号，目的端口号，长度（UDP数据报的总长度），校验和（检测UDP数据报在传输过程中是否出错）；

TCP首部的最小长度是20个字节，其中包括源端口，目的端口，序号（本报文段发送数据的第一个字节序号），确认号（期望收到发送方下一个报文段的第一个字节序号），数据偏移（TCP报文的起始点到数据起始部分的偏移量），控制位（URG，ACK，PSH，RST，SYN，FIN），窗口（发送本报文段一方允许对方发送的数据量大小，即发送方的接收窗口大小），紧急指针（本报文段中的紧急数据的字节数）。

14. 在TCP拥塞控制中，什么是慢开始，拥塞避免，快重传和快恢复算法?

答：慢开始和拥塞避免：发送方会维持一个拥塞窗口，刚开始拥塞窗口和发送窗口大小相同，初值为1。每次收到一个确认，就让拥塞窗口大小变为原来的两倍，并以此类推，形成指数增大。而当窗口值等于慢开始门限值时，就会执行拥塞避免，窗口值每次加1，形成加法增大。若此时出现网络拥塞，则将拥塞窗口值重新设置为1，并且修改门限值为发生网络拥塞时的拥塞窗口值的一半；

快重传和快恢复：当发送方收到三个连续确认时，发送方执行乘法减小策略，将拥塞窗口设置为当前的一半，同时对接收方请求的帧执行快重传算法立刻进行重传而不是等待超时，并且直接执行快恢复算法，即进入拥塞避免状态，采取加法增大每次将拥塞窗口大小+1。

15. 流量控制和拥塞控制的关系是什么?

答：流量控制解决的是发送方和接收方速率不匹配的问题，是一个端到端的问题；拥塞控制解决的是避免网络资源被耗尽的问题，是一个全局性问题。

流量控制是通过滑动窗口来实现的，而拥塞控制是通过拥塞窗口来实现的。

流量控制是作用于接受者的，它是控制发送者的发送速度从而使接受者来得及接收；拥塞控制是作用于网络的，它是防止过多的数据注入到网络中，避免出现网络负载过大的情况。

16. 两个服务器间已经联通却收不到彼此的UDP报文原因有什么？丢包的主要原因?

答：例如设置了ACL（访问控制列表），禁用了某些端口，发生网络拥塞，丢包等。

丢包的主要原因有：① 接收端处理时间过长导致丢包；② 发送的包巨大而丢包；③ 发送的包超过接受者缓存导致丢包；④ 发送包的的频率太快；⑤ 局域网内不丢包，但是在公网内发生了丢包。

17. 什么是地址解析协议?

答：ARP即地址解析协议，其主要作用是将IP地址转化为MAC地址。主要的工作流程是：ARP中从IP到MAC的映射主要依靠APR高速缓存，以IP地址为key查询高速缓存，获取对应的value即为MAC地址。若高速缓存中没有对应的记录，则此时适配器将在局域网中进行APR广播，对该MAC地址进行询问。若此时局域网内

存在目的地址的主机，其会想发送方发送一个APR响应，其中包含了该网卡的MAC地址，发送方便将其写入APR告诉缓存；若此时局域网内没有目的地址的主机，则将通过路由器对APR请求进行转发，并且在其他网络中进行广播查询。

18. 网卡的作用有什么?

答：① 进行数据并行到串行的转换，计算机内部的数据传输通常是并行方式，而在计算机网络间数据的传输方式通常是串行；② 对数据进行缓存，用于消除不同设备之间的传输速率差异；③ 实现以太网协议，例如APR协议等，是电脑与上网的接口。

19. 简述DNS域名解析的过程?

答：① 当客户机提出请求查询时，首先在本地计算机缓存中查找；

② 若本地缓存没有相关信息，则将查询请求转发给本地DNS服务器，本地DNS服务接受到查询请求后，在其所管理的区域的记录中查找并解析。若没有区域信息可以满足查询要求，则服务器在本地缓存中查找；

③ 若缓存没有，则本地DNS服务器（取决于是迭代方式还是递归方式）将查询请求转发到根应服务器，根域名服务器负责解析根域部分，并将下一级域名信息的DNS服务器地址返回给本地DNS服务器；

④ 采用递归的方式，按照上述方法逐级查询接近查询目标，最后获得响应的IP地址信息；同时也可以采用迭代的方式，由根域名服务器直接转发给下级域名服务器。

20. TCP建立连接的过程中如何保证可靠传输?

答：TCP协议保证数据传输可靠性的方式主要有：校验和、序列号、确认应答、超时重传、连接管理、流量控制、拥塞控制。

① 校验和：将需要发送的数据都当做一个16位的整数，将这些整数加起来并且将进位补在后面，最后取反得到校验和。接收方接收到数据后进行相同的计算并且与发送方的校验和进行比较；

② 确认应答与序列号：TCP传输时对每个字节数据进行编号，并且每次接收方在收到数据之后都会对传输放进行确认应答，即发送ACK报文。ACK报文中携带对应的确认序列号，用于告诉发送方什么数据已经接收到，期望收到的下一个数据是什么；

③ 超时重传：发送方完成数据发送之后迟迟未接收到接收方的响应ACK，则在等待一定的时间之后会对刚才发送的数据进行重新发送；

④ 连接管理：连接管理即TCP的三次握手与四次挥手的过程；

⑤ 流量控制：用于控制发送方与接收方直接的速度差异，使得接收方来得及接收发送方的数据。这通过滑动窗口协议进行实现，发送方维持一个发送窗口，接收方维持一个接收窗口，接收方动态地对窗口值进行调整；

⑥ 拥塞控制：通过在网络中引入拥塞窗口，并且引入慢开始、拥塞控制、快重传、快恢复协议对网络的拥塞情况进行全局的控制。

21. IP地址和MAC地址的区别和用途?

答：IP地址在网络层及以上层进行使用，它为互联网上每一个网络的每一台主机都分配一个全网唯一的逻辑地址，作用于广域网中，是网络层上的协议用于屏蔽不同网络的差异从而进行全网连通；

MAC地址则是物理地址，用于确认网上设备的位置与地址，通常一个网卡有一个唯一的MAC地址。MAC地址作用于局域网，是数据链路层上的协议。

22. DHCP的作用是什么?

答：DHCP即动态主机配置协议，是一个局域网的网络协议，使用UDP协议工作。其主要有两个用途：用于内部网络或网络服务供应商自动分配IP地址；给用户用于内部网管理员作为对所有计算机做中央管理。主要功能如下：

① 保证任何IP地址在同一时刻只能由一台DHCP客户机所使用；

② DHCP应当可以给用户分配永久固定的IP地址；

③ DHCP应当可以与同用其他方法获得IP地址的主机共存（例如手工配置IP）；

23. HTTP状态码和对应的含义？HTTP和HTTPS的区别?

答：① 1XX：表示临时相应并需要请求者继续执行操作；

② 2XX：表示成功处理请求；

③ 3XX：表示重定向；

④ 4XX：表示请求出错；

⑤ 5XX：表示服务器在处理请求时发生了内部错误。

HTTP与HTTPS的区别：HTTP协议传输的数据都是未加密的，即以明文进行传递，因此HTTP协议传输隐私信息非常不安全。为了保证隐私数据，通过SSL协议对HTTP协议传输的数据进行加密从而产生了HTTPS。HTTP的端口号是80，而HTTPS的端口号是443。

24. 在浏览器里输入一个网址，会发生什么?

答：① 对输入的网址进行域名解析；

② 通过三次握手的方式建立TCP连接；

③ 建立TCP链接之后发起HTTP请求；

④ 服务器接收并且响应HTTP请求；

⑤ 浏览器解析HTML代码，并且请求HTML代码中的其他资源；

⑥ 通过四次挥手断开TCP连接；

⑦ 浏览器对页面进行渲染并且呈现给用户。

25. 简述一下Session和Cookie的区别?

答：① 数据库位置不同，cookie存放于客户浏览器，session存放于服务器；

② 安全程度不同：session的安全性高于cookie；

③ 性能使用程度不同：session在一定时间内保存在服务器上，访问增多时将占用服务器的性能；

④ 数据存储能力不同，cookie保存的数据较小，而session则与服务器端有关；

⑤ 会话机制不同，session利用类似于哈希表的结构来保存信息，cookie则是存储在本地计算机上的小块文本。

26. 什么是Socket?

答：socket即套接字，由IP地址+端口号组成，是计算机之间的进程进行逻辑通信的一种方式。Socket提供了一个针对TCP或者UDP变成的接口，即socket是一种特殊的文件，一些socket函数就是对其进行的操作。

27. 为什么有MAC地址还需要IP地址?

答：① 各式各样的网络使用不同的硬件地址，IP地址的作用是屏蔽异构网路的差异，使得不同网络之间的设备可以进行信息交互。② IP地址的本质是终点地址，它在跳过路由器的时候不会改变，而MAC地址则是下一跳的地址，每一次经过一个路由器都会改变。③ 分别用MAC地址和IP地址表示物理地址和逻辑地址方便网络分层，使得网络层和数据链路层的协议可以更灵活地替换。

28. Ipv6出现的动机是什么？报文首部的哪些字段发生了变化?

答：最初动机是32位的Ipv4地址空间已经分配殆尽，而其他的动机也包括改进首部的格式、快速处理/转发数据报、支持QoS。
首部发生变化的字段有：移除了校验和，同时将选项从首部移除，定义多个选项首部，并且通过“下一个首部”字段进行知识，同时新增了ICMPv6。

29. 什么叫做http无状态，为什么要无状态，如何让它有状态?

答：许多常见的七层协议是有状态的，通信的双方必须要时刻记住当前连接的状态，因为在不同的状态下能够接受的命令是不同的。之前的命令传输的某些数据也必须要记住，其可能会对后面的命令产生影响。这种协议就是有状态的协议。
而HTTP是无状态的，因为它每个请求都是完成独立的，每个请求包含了处理这个请求所需要的完整的数据，发送请求不涉及到状态变更。HTTP是无状态的是因为其最初只是用来浏览静态文件的，无协议已经足够。而随着Web的发展，HTTP需要变得有状态，但是因为我们经常长时间逗留在某一网页，然后才进入到另外一个网页，如果在这两个页面之间维持状态，代价很高。因此我们引入了其他机制来实现这种状态的连接，而不改变HTTP的无状态性。这些机制包括：Cookie，用于记录客户端的信息；Session，将信息存放于服务端，保证安全性；token：解决session占用内存问题；JWT：以json形式存放token。