1.一台分组交换机接收到一个分组并决定该分组应当转发的链路。当某分组到达时,另一个分组正在该出链路上被发送到一半,还有4个其他分组正在等待传输。这些分组以到达的次序传输。假定所有分组是1500bytes并且链路速率是2Mbps。该分组的排队时延时多少?

(1500*8*4.5)/(2*10^6)=27ms

2.假定有N个分组同时到达一条当前没有分组传输或排队的链路。每个分组长为L,链路传输速率为R。对于N个分组而言,其平均排队时延时多少?

(((N-1)*L)/R)/2

3.接上题,现在假定每隔LN/R秒就有N个分组同时达到链路。一个分组的平均排队时延时多少?

((N-1)*L)/R/2

4.考虑路由器缓存中的排队时延。忽略传播时延和处理时延。令I表示流量强度;I=La/R。假定排队时延的形势为 IL/R(1-I),其中 I<1。a.写出总时延公式 b.令a表示在一条链路上分组的到达率(分组/秒 为单位),令u表示一条链路上分组的传输率(分组/秒)。基于上述公式写出以a和u表示的总延时公式

a. IL/R(1-I) + L/R

b.1/u = L/R

IL/R(1-I) + L/R = L/(1-I)R =1/(1-I)u=1/(u-a)

#应用层练习

1. Http与Https的区别

1、https协议需要到ca申请证书，一般免费证书较少，因而需要一定费用。

2、http是超文本传输协议，信息是明文传输，https则是具有安全性的ssl加密传输协议。

3、http和https使用的是完全不同的连接方式，用的端口也不一样，前者是80，后者是443。

4、http的连接很简单，是无状态的；HTTPS协议是由SSL+HTTP协议构建的可进行加密传输、身份认证的网络协议，比http协议安全。

2. URI和URL的区别

URI包括URL和URN两个类别，URL是URI的子集，所以URL一定是URI，而URI不一定是URL

URI = Universal Resource Identifier 统一资源标志符，用来标识抽象或物理资源的一个紧凑字符串。

URL = Universal Resource Locator 统一资源定位符，一种定位资源的主要访问机制的字符串，一个标准的URL必须包括：protocol、host、port、path、parameter、anchor。

3. HTTPS工作原理

1.浏览器将自己支持的一套加密规则发送给网站。

2.网站从中选出一组加密算法与HASH算法，并将自己的身份信息以证书的形式发回给浏览器。证书里面包含了网站地址，加密公钥，以及证书的颁发机构等信息。

3.获得网站证书之后浏览器要做以下工作：

a) 验证证书的合法性（颁发证书的机构是否合法，证书中包含的网站地址是否与正在访问的地址一致等），如果证书受信任，则浏览器栏里面会显示一个小锁头，否则会给出证书不受信的提示。

b) 如果证书受信任，或者是用户接受了不受信的证书，浏览器会生成一串随机数的密码，并用证书中提供的公钥加密。

c) 使用约定好的HASH计算握手消息，并使用生成的随机数对消息进行加密，最后将之前生成的所有信息发送给网站。

4.网站接收浏览器发来的数据之后要做以下的操作：

a) 使用自己的私钥将信息解密取出密码，使用密码解密浏览器发来的握手消息，并验证HASH是否与浏览器发来的一致。

b) 使用密码加密一段握手消息，发送给浏览器。

5.浏览器解密并计算握手消息的HASH，如果与服务端发来的HASH一致，此时握手过程结束，之后所有的通信数据将由之前浏览器生成的随机密码并利用对称加密算法进行加密。

4. 一次完整的HTTP请求所经历的7个步骤

1：建立TCP连接

在HTTP工作开始之前，Web浏览器首先要通过网络与Web服务器建立连接，该连接是通过TCP来完成的，该协议与IP协议共同构建Internet， 即著名的TCP/IP协议族，因此Internet又被称作是TCP/IP网络。HTTP是比TCP更高层次的应用层协议，根据规则，只有低层协议建立之 后才能，才能进行更层协议的连接，因此，首先要建立TCP连接，一般TCP连接的端口号是80。

2：web浏览器向web服务器发送请求命令

一旦建立了TCP连接，Web浏览器就会向Web服务器发送请求命令。

3：web浏览器发送请求头信息

浏览器发送其请求命令之后，还要以头信息的形式向Web服务器发送一些别的信息，之后浏览器发送了一空白行来通知服务器，它已经结束了该头信息的发送。

4. Web服务器应答

客户机向服务器发出请求后，服务器会客户机回送应答， HTTP/1.1 200 OK ，应答的第一部分是协议的版本号和应答状态码。

5. Web服务器发送应答头信息

正如客户端会随同请求发送关于自身的信息一样，服务器也会随同应答向用户发送关于它自己的数据及被请求的文档。

6. Web服务器向浏览器发送数据

Web服务器向浏览器发送头信息后，它会发送一个空白行来表示头信息的发送到此为结束，接着，它就以Content-Type应答头信息所描述的格式发送用户所请求的实际数据。

7. Web服务器关闭TCP连接

一般情况下，一旦Web服务器向浏览器发送了请求数据，它就要关闭TCP连接，然后如果浏览器或者服务器在其头信息加入了这行代码：

Connection:keep-alive

TCP连接在发送后将仍然保持打开状态，于是，浏览器可以继续通过相同的连接发送请求。保持连接节省了为每个请求建立新连接所需的时间，还节约了网络带宽。

5. 常见的HTTP相应状态码

对网站管理工作者来说有个词不陌生，HTTP状态码，它是用以表示网页服务器HTTP响应状态的3位数字代码。状态码的第一个数字代表了响应的五种状态之一。

1XX系列：指定客户端应相应的某些动作，代表请求已被接受，需要继续处理。由于 HTTP/1.0 协议中没有定义任何 1xx 状态码，所以除非在某些试验条件下，服务器禁止向此类客户端发送 1xx 响应。

2XX系列：代表请求已成功被服务器接收、理解、并接受。这系列中最常见的有200、201状态码。

200状态码：表示请求已成功，请求所希望的响应头或数据体将随此响应返回

201状态码：表示请求成功并且服务器创建了新的资源，且其 URI 已经随Location 头信息返回。假如需要的资源无法及时建立的话，应当返回 '202 Accepted'

202状态码：服务器已接受请求，但尚未处理

3XX系列：代表需要客户端采取进一步的操作才能完成请求，这些状态码用来重定向，后续的请求地址（重定向目标）在本次响应的 Location 域中指明。这系列中最常见的有301、302状态码。

301状态码：被请求的资源已永久移动到新位置。服务器返回此响应（对 GET 或 HEAD 请求的响应）时，会自动将请求者转到新位置。

302状态码：请求的资源临时从不同的URI响应请求，但请求者应继续使用原有位置来进行以后的请求

304自从上次请求后，请求的网页未修改过。服务器返回此响应时，不会返回网页内容。 如果网页自请求者上次请求后再也没有更改过，您应将服务器配置为返回此响应(称为 If-Modified-Since HTTP 标头)。

4XX系列：表示请求错误。代表了客户端看起来可能发生了错误，妨碍了服务器的处理。常见有：401、404状态码。

401状态码：请求要求身份验证。 对于需要登录的网页，服务器可能返回此响应。

403状态码：服务器已经理解请求，但是拒绝执行它。与401响应不同的是，身份验证并不能提供任何帮助，而且这个请求也不应该被重复提交。

404状态码：请求失败，请求所希望得到的资源未被在服务器上发现。没有信息能够告诉用户这个状况到底是暂时的还是永久的。假如服务器知道情况的话，应当使用410状态码来告知旧资源因为某些内部的配置机制问题，已经永久的不可用，而且没有任何可以跳转的地址。404这个状态码被广泛应用于当服务器不想揭示到底为何请求被拒绝或

者没有其他适合的响应可用的情况下。

5xx系列：代表了服务器在处理请求的过程中有错误或者异常状态发生，也有可能是服务器意识到以当前的软硬件资源无法完成对请求的处理。常见有500、503状态码。

500状态码：服务器遇到了一个未曾预料的状况，导致了它无法完成对请求的处理。一般来说，这个问题都会在服务器的程序码出错时出现。

503状态码：由于临时的服务器维护或者过载，服务器当前无法处理请求。通常，这个是暂时状态，一段时间会恢复

6. TCP协议和UDP协议的区别是什么

tcp协议为传输控制协议

1）面向连接的可靠的传输控制协议,连接的建立需要三次握手，连接的释放需要进行四次握手才能保证连接的建立，数据的同步传输。

2）面向字节流，会把从上层传输下来的数据当作是无结构的字节流。

3）一对一的通信。

4）TCP在IP协议的基础之上添加了序号机制，确认机制，超时重传机制，数据校验，从而保证传输的可靠性，同时保证不出现丢失或者是乱序。

udp协议为用户数据报协议

1）无连接的数据包服务，一方向另一方发送数据不需要建立连接。相当于发短信，别人是否收到，短信信息是否丢失都不能知道。

2）面向报文的，从上层接收的数据如果报文不大于传输限制，则直接加上首部传输，如果报文过大，则进行IP分片后，再分别加入首部进行传输。

3）UDP协议可以一对一通信，同时可以一对多通信。

4）UDP仅仅是尽最大的努力进行交付，只是做比较初级的检查，比如端头检查，差错检测，往往在传输过程中会出现分组丢失、乱序、重复传输等问题。

7. TCP建立连接的过程采用三次握手，已知第三次握手报文的发送序列号为555，确认序列号为6666，请问第二次握手报文的发送序列号和确认序列号分别为?

发送序列号为6665，确认序列号为555

8. 简述tcp ip四层模型

1. 数据链路层

1.1 作用

(1) 实现网卡接口的网络驱动，以处理数据在以太网线等物理媒介上的传输

(2) 网络驱动程序隐藏了不同物理网络的不同电气特性，为上层协议提供一个统一的接口

1.2 协议应用

ARP和RARP(Reverse Address Resolve Protocol)即逆地址解析协议，该协议实现了IP地址和物理地址(MAC地址)之间的转换

2. 网络层

2.1 作用

网络有分局域网(LAN, Local Area Network)和广域网(WAN, Wide Area Network)。对于后者通常需要使用众多分级的路由器来连接分散的主机或者LAN，即通讯的两台主机一般不是直接连接，而是通过多个中间节点(路由器)连接的，从而形成网络拓扑连接。

(1) 网络层的任务之一就是选择这些中间节点，以确定两台主机间的通讯路径。

(2) 其次网络层对上层协议隐藏了网络拓扑连接的细节，在使得传输层看来通讯双方是直接连接的

2.2 协议应用

(1) IP协议: IP协议(Internet Protocol)是网络层最核心的协议，它根据数据包的目的IP地址来决定如何投递该数据包。若数据包不可直接发送给目标主机，那么IP协议就为它寻找一个合适的下一跳路由器，并将数据包交付给该路由器去转发，如此循环直至到达目标主机或者发送失败而丢弃该数据包。

(2) ICMP协议: ICMP协议(Internet Control Message Protocol，因特网控制报文协议)是IP协议的补充，用于检测网络的连接状态，如ping应用程序就是ICMP协议的使用。ICMP包发送是不可靠的，所以不能依靠接收ICMP包解决网络问题；ICMP与TCP/UDP不同，它们是传输层协议，虽然都具有类型域和代码域，但是前者和后者不同，ping用到的ICMP协议，不是端口。ICMP协议使用的是IP协议而非

使用下层协议提供的的服务，所以严格来讲它并非网络层协议，而是网络层程序。

3. 传输层

3.1 作用

传输层的作用是为应用程序提供端对端通讯的”错觉”，即为应用程序隐藏了数据包跳转的细节，负责数据包的收发、链路超时重连等。

3.2 协议应用

(1) TCP协议: TCP协议(Transmission Control Protocol, 传输控制协议)为应用程序提供可靠的、面向连接的、基于流的服务，具有超时重传、数据确认等方式来确保数据包被正确发送到目的端。因此TCP服务是可靠的，使用TCP协议通讯的双方必须先建立起TCP连接，并在系统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，多个定时器等。当通讯结束时双方必须关闭连接以释放这些内核数据。基于流发送意思是数据是没有长度限制，它可源源不断地从通讯的一段流入另一端。

(2) UDP协议: UDP协议(User Datagram Protocol, 用户数据报协议)与TCP协议相反，它为应用程序提供的是不可靠的、无连接的基于数据报的服务。

无连接: 通讯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方的地址；

基于数据报的服务: 这是相对于数据流而言的，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内容一次性读出，否则数据将被截断。

UDP不具有发送时是被重发功能，所以UDP协议在内核实现中无需为应用程序的数据保存副本，当UDP数据报被成功发送之后，UDP内核缓冲区中该数据报就被丢弃了。

(3) SCTP协议: SCTP(Stream Control Transmission Protocol, 流控制传输协议)是为了在因特网上传输电话信号而设计的。

4. 应用层

4.1 作用

前面所述的三层负责处理网络通讯的相关细节，这部分需要稳定高效，因此它们是在操作系统的内核空间中，而应用层是在用户空间实现的，负责处理众多业务逻辑，如文件传输、网络管理。

4.2 协议应用

应用层的协议很多，如：

(1) telne协议: 远程登录协议，它使我们能在本地完成远程任务

(2) OSPF协议: OSPF协议(Open Shorttest Path First, 开放最短路径优先)是一种动态路由更新协议，用于路由器之间的通讯，以告知对方自身的路由信息

(3) DNS协议: DNS协议(Domain Name Service, 域名服务)提供机器域名到IP地址的转换。如百度的机器域名是www.baidu.com，对应的IP地址是http://119.75.217.109/。

9. 简述 osi七层模型

OSI参考模型又称开放系统互联模型，它是美国国际标准化组织定义的网络参考迷行。OSI参考模型共分为七层，分别是：

1物理层：链路上比特流传输；

2数据链路层：网络内部帧的传输；

3网络层：网间两点间可达性；

4传输层：保证端到端的传输；

5会话层：会话的控制；

6表示层：数据的表达及数据格式的转换

7应用层：为用户具体应用服务。

10. dns是什么 dns是哪一层协议

dns是一个域名系统，是万维网上作为域名和IP地址相互映射的一个分布式数据库，能够使用户更方便的访问互联网，而不用去记住能够被机器直接读取的IP数串。

DNS协议运行在UDP协议之上，使用端口号53。

11. arp是哪一层协议

地址解析协议，即ARP（Address Resolution Protocol），是根据IP地址获取物理地址的一个TCP/IP协议。

12. wifi是哪一层协议

属于数据链路层和物理层

13. 简述cdn作用 #运输层网络层练习题

尽可能避开互联网上有可能影响数据传输速度和稳定性的瓶颈和环节，使内容传输的更快、更稳定。通过在网络各处放置节点服务器所构成的在现有的互联网基础之上的一层智能虚拟网络，CDN系统能够实时地根据网络流量和各节点的连接、负载状况以及到用户的距离和响应时间等综合信息将用户的请求重新导向离用户最近的服务节点上。

14. 服务器发生close wait是在什么时候

说明还没有发送fin给server

15. 简述syn洪攻击

SYN攻击利用的是TCP的三次握手机制，攻击端利用伪造的IP地址向被攻击端发出请求，而被攻击端发出的响应 报文将永远发送不到目的地，那么被攻击端在等待关闭这个连接的过程中消耗了资源，如果有成千上万的这种连接，主机资源将被耗尽，从而达到攻击的目的。

16. 156.123.32.13 是哪一类ip地址

B类地址

17. 主机ip地址为 193.32.5.22 掩码为 255.255.255.192 网络地址为多少,广播地址为多少

网络地址193.32.5.0 广播地址 193.32.5.255

18. icmp是哪一层协议

该协议是TCP/IP协议集中的一个子协议，属于网络层协议，主要用于在主机与路由器之间传递控制信息，包括报告错误、交换受限控制和状态信息等。当遇到IP数据无法访问目标、IP路由器无法按当前的传输速率转发数据包等情况时，会自动发送ICMP消息。我们可以通过Ping命令发送ICMP回应请求消息并记录收到ICMP回应回复消息，通过这些消息来对网络或主机的故障提供参考依据。

19. get方法和post方法的不同

最直接的区别，GET请求的参数是放在URL里的，POST请求参数是放在请求body里的；GET请求的URL传参有长度限制，而

POST请求没有长度限制；GET请求的参数只能是ASCII码，所以中文需要URL编码，而POST请求传参没有这个限制；

GET 向服务器获取指定资源

POST 向服务器提交数据，数据放在请求体里

20. 简述DOS攻击 和DDOS攻击

DoS是Denial of Service的简称，即拒绝服务，造成DoS的攻击行为被称为DoS攻击，其目的是使计算机或网络无法提供正常的服务。最常见的DoS攻击有计算机网络带宽攻击和连通性攻击。DoS攻击是指故意的攻击网络协议实现的缺陷或直接通过野蛮手段残忍地耗尽被攻击对象的资源，目的是让目标计算机或网络无法提供正常的服务或资源访问，使目标系统服务系统停止响应甚至崩溃，而在此攻击中并不包括侵入目标服务器或目标网络设备。这些服务资源包括网络带宽，文件系统空间容量，开放的进程或者允许的连接。这种攻击会导致资源的匮乏，无论计算机的处理速度多快、内存容量多大、网络带宽的速度多快都无法避免这种攻击带来的后果。

分布式拒绝服务(*DDoS:Distributed Denial of Service*)攻击指借助于客户/服务器技术，将多个计算机联合起来作为攻击平台，对一个或多个目标发动DDoS攻击，从而成倍地提高拒绝服务攻击的威力。通常，攻击者使用一个偷窃帐号将DDoS主控程序安装在一个计算机上，在一个设定的时间主控程序将与大量代理程序通讯，代理程序已经被安装在网络上的许多计算机上。代理程序收到指令时就发动攻击。利用客户/服务器技术，主控程序能在几秒钟内激活成百上千次代理程序的运行

21. tcp报文头中,首部长度的作用是什么?首部长度是多少位?首部的位数为二进制表现方式,那么首部表现成十进制的最大数字是多少?tcp首部最大长度是多少,他和首都长度段有什么联系?tcp首部可选数据字段是多长?

由于tcp首部包含一个长度可变的选项部分，所以需要一个值来指定这个tcp报文段到底有多长。首部长度是4位。15。60。长度段和4的乘积。40字节。

22. tcp最大端口号是多少?为什么?linux系统能开启多少个端口，为什么？linux操作系统端口号和进程号的关系是什么?

65535。端口号占用16bit，65535是16位二进制最大数。能开启很多个。可以通过进程号查看占用端口，先查看进程pid，ps -ef | grep 进程名，通过pid查看占用端口netstat -nap | grep 进程pid，也可以通过端口查看进程，netstat -nap | grep 端口号

23. tcp三次握手中 第三次握手首部中syn值是多少 为什么?

1。因为第二次握手发送了一个syn过来。

24. tcp协议中 ISN是什么意思?ISN的值一定是1吗?BSD使用的ISN值的方案是什么?不同的连接ISN一样吗,如果不一样如何确定?（参考RFC 793）

ISN是初始化序列号：Initial Sequence Number。不一定。OpenBSD-current的PRNG 输出为31-bit,也就是说，△seq[t]的值域范围可以是231 – 1，意味着,y,z值域也很大，这对使我们很难确定M集，经过我们的处理后，可以看到一个云状物(见上图)，它的R1半径很大，而且分布均匀，不呈现任何的空间结构化特性，很难对它进行分析。

25. tcp协议中 序列号是如何增长的,是每次加1还是随机增长还是其他方式增长?第三次握手时 ack序列号是否增加 为什么?第一次握手响应时ack序列号加多少 为什么?

加1。要增加，比第二次握手的seq序列号加1.加1，因为确认客户的syn，ack=seq+1这么设计的目的是确保建立连接的双方都是真实的对方，而不是被某个中间人冒充的。.

26. mss是什么?mss在什么时候确定?tcp报文最大长度理论上，多少 为什么?实际上面是多少 为什么?

mss是网络传输数据最大值。MSS=MTU-20字节TCP报头-20字节IP报头，那么在以太网环境下，MSS值一般就是1500-20-20=1460字节。TCP报文段的数据部分最多是65495。加上TCP首部20字节，加上IP首部20字节，正好就是IP数据报的最大长度了。

27. tcp最大长度是多少,为什么?

TCP：对于TCP来说，数据是流式传输的，传输数据可以接近无限大，单次传输的数据受限于网络层。

28. tcp窗口/mss大小如何确定,在什么时候,什么位置确定窗口/mss大小?

29. 如何理解tcp的半关闭(half-close)？什么是全双工?

30. 为什么握手需要三次?为什么关闭连接需要四次?

发送方以确定SYN标志，同时生成一个ISN（初始序列号），也就是消息序号来发送信息(消息字节数n)。接收方如果收到了信息，会以ACK标志和下次需要对方传递的序号值发送给对方，ack标志告诉对方我已经收到了信息，传递序号ISN+n告诉对方下次从这个序号的地方开始发送。两次消息的传递，意味着一次通信的完成。后面消息的序号都是基于ISN和传递消息的字节数逐渐累加计算得来。TCP协议的通信方式规定是这样的。同时，基于tcp协议的双方是双全工的，也就是说通信双方都可以向对方发送消息，也都可以独立关闭自己一方的通信通道。基于通信方式和双全工的特性，所以在tcp连接建立时，client需要将自己的ISN序号告知对方，同时需要对方的确定。server也需要将自己的ISN序号告知对方，同时也要对方的确定。

至于四次挥手，同样也是基于以上的原理。尤其是通信双方都可以独立关闭自己的通信通道，也就是半关闭。client先发送FIN告知对方我已经完成数据发送了，server回复ack来确定我知道了。这样一个流程，就关闭了client的发送信息通道。但是还可以接收来自server方的数据。server此时已经知道接收不到client的数据了，但是还可以给它发送数据。如果server也没有啥数据要发送给对方了，server也会以FIN标志位发送一个信息给client，client接到后，也会传递一个ack表示知道了。这样子，双方都完成了关闭。

31 GBN的定时器有几个 SR的定时器有几个

GBN：有发送方缓存，无接收方缓存，一个定时器（可认为最早的已发送但还未被确认的分组所使用的计时器），丢弃失序分组，采用累计确认

SR：有发送方缓存，有接收方缓存，每个分组都有定时器，缓存失序分组，不采用累计确认

32 为什么说tcp协议是面向连接的?

TCP连接是面向连接的，因为一个应用进程可以开始向另一个应用进程发送数据之前，这两个进程必须先相互“握手”。

33 GBN协议中,接收方窗口大小是多少
若从滑动窗口的观点来统一看待停等、后退n及选择重传三种协议，它们的差别仅在于各自窗口尺寸的大小不同而已。停等：发送窗口= 1，接收窗口=1； 后退n协议：发送窗口>1，接收窗口=1；选择重传协议：发送窗口>1,接受窗口>1;

34 GBN协议中,需要对大于当前期望收到的分组序号的序号做确认吗?SR中需要确认吗?
GBN累计确认 。 SR不需要确认

35 TCP/IP的中文解释是什么?
互联网协议套件（英语：Internet Protocol Suite，缩写IPS）是一个网络通信模型，以及一整个网络传输协议家族，为网际网络的基础通信架构。它常被通称为TCP/IP协议族（英语：TCP/IP Protocol Suite，或TCP/IP Protocols），简称TCP/IP。

36 假设链路层MTU为 1600 那么MSS最大为多少
1600-20-20=1560

37 MSS指的是什么的大小
报文

38 计算机的端口为什么最大是65535
在TCP、UDP协议的开头，会分别有16位来存储源端口号和目标端口号，所以端口个数是2^16-1=65535个。

39 a. 假定你有下列2个字节: 01011100和01100101。者两个字节之和的反码是什么?b.假定你有下列2个字节: 11011010和01100101这两个的反码和是多少?c. 1bit的差错将可能检测不出来吗?2bit呢?
01011100+01100101 = 92+101 = 193 =11000001
反码：11000001（正数反码为本身）
11011010+01100101 = 218+101 = 319 = 10011111

反码：10011111（本身）
负数的反码是在其原码的基础上, 符号位（第一位）不变，其余各个位取反.