时延：是数据（一个报文或分组，甚至比特）从网络或链路的一段传送到另一端所需要的时间。
发送时延：是从发送数据帧的第一个比特算起，到该帧的最后一个比特发送完毕所需的时间。
发送时延=数据帧长度(b) /信道带宽(b/s) [信道带宽就是数据率]
传播时延：电磁波在信道中需要传播一定的距离而花费的时间。
传播时延=信道长度(m)/电磁波在信道上的传播速率(m/s)
处理时延：主机或路由器处理所收到的分组的时间。
排队时延：分组在输入队列中排队等待处理，在输出队列中等待转发，就形成了排队时延。
总时延=发送时延+传播时延+处理时延+排队时延

#延时 吞吐量托练习题

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?

前面等待了4.5个分组，也就是4.5 * 1500 = 6750Bytes，然后1Byte = 8bit，所以 6750Bytes = 54000bit，所以排队时延为54000/(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)n/2 * l/r

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?

由于LN/R比(N - 1) * L / 2R大，所以在下一次N个分组来之前，上一次N个分组已经处理完了，没有额外排队时延，所以平均排队时延依然是(N - 1) * L / 2R

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
5.

#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。而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包括了URL和URN，URN和URL有交集。
1.统一资源标志符URI：就是在某一规则下能把一个资源独一无二地标识出来。（标识出这是一个人）
URI一般由三部组成：
①访问资源的命名机制
②存放资源的主机名
③资源自身的名称，由路径表示，着重强调于资源。

2.统一资源定位符URL：描述资源的详情地址。（标识出张三家的地址，）
URL一般由三部组成：
①协议(或称为服务方式)
②存有该资源的主机IP地址(有时也包括端口号)
③主机资源的具体地址。如目录和文件名等
3.统一资源名URN：描述资源的名称。（标识出这个人叫张三）

3. HTTPS工作原理

数据完整性和隐私性由TLS Record Protocol保证，身份认证由TLS Handshaking Protocols实现。
—>1. 客户端发起HTTPS请求
—>2.服务端将证书（公钥）发给客服端
—>3.客服端解析证书（1.验证，2.生成随机对称密钥（即加密，解密；客服端和服务端一人一份），3.用验证的证书对生成的对称密钥加密）
—>4.发送证书加密的对称密钥给服务端
—>5.服务端通过证书（私钥）解密，获得一份对称密钥
—>6.现在客服端和服务端就人手一份对称密钥，最后就通过这一份对称密钥加密通信信息进行通信。

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进行更高层协议的连接，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。例如：GET/sample/hello.jsp HTTP/1.1。

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

请求收到，继续处理：

100	客户端必须继续发出请求
101	客户端要求服务器根据请求转换HTTP协议版本

操作成功/收到/分析/接受：

200	交易成功
201	提示知道新文件的URL
202	接受和处理、但处理未完成

203 返回信息不确定或不完整

204 请求收到，但返回信息为空

205 服务器完成了请求，用户代理必须复位当前已经浏览过的文件

206 服务器已经完成了部分用户的GET请求

重定向：

300 请求的资源可在多处得到

301 永久重定向，在Location响应首部的值仍为当前URL(隐式重定向)

302 临时重定向，在Location响应首部的值仍为新的URL(显示重定向)

303 建议客户端访问其他URL或访问方式

304 Not Modified 请求的资源没有改变 可以继续使用缓存

305 请求的资源必须从服务器指定的地址得到

306 前一版本HTTP中使用的代码，现行版本中不再使用

307 声明请求的资源临时性删除

客户端错误：

400 错误请求。由于语法错误，该请求无法完成

401 未经授权。服务器拒绝响应

HTTP 401.1 未授权，登录失败

HTTP 401.2 未授权，服务器配置问题导致登录失败

HTTP 401.3 ACL 禁止访问资源

HTTP 401.4 未授权 授权被筛选器拒绝

HTTP 401.5 未授权 ISAPI或CGI授权失败

402 保留有效ChargeTo头响应

403 禁止访问，服务器拒绝响应

HTTP 403.1 禁止访问 禁止可执行访问

HTTP 403.2 禁止访问 禁止读访问

HTTP 403.3 禁止访问 禁止写访问

HTTP 403.4 禁止访问 要求SSL

HTTP 403.5 禁止访问 要求SSL 128

HTTP 403.6 禁止访问 IP地址被拒绝

HTTP 403.7 禁止访问 要求客户端证书

HTTP 403.8 禁止访问 禁止站点访问

HTTP 403.9 禁止访问 连接的用户过多

HTTP 403.10 禁止访问 配置无效

HTTP 403.11 禁止访问 密码更改

HTTP 403.12 禁止访问 映射器拒绝访问

HTTP 403.13 禁止访问 客户端证书已被吊销

HTTP 403.15 禁止访问 客户端访问许可过多

HTTP 403.16　禁止访问　客户端证书不可信或者无效

HTTP 403.17　禁止访问　客户端证书已经到期或者尚未生效

404　未找到。无法找到请求的位置。

405　方法不被允许。用户在Request-Line字段定义的方法不允许

406　不可接受。服务器只生成客户端不接受的响应。根据用户发送的Accept，请求资源不可访问

407　类似401，需要代理身份验证。客户端必须先使用代理对自身进行身份验证

408　超时。等待请求的服务器超时。客户端没有在用户指定的时间内完成请求

409　冲突。由于请求中的冲突，无法完成该请求。对当前资源状态，请求不能完成

410　过期。请求页不再可用。服务器上不再有此资源且无进一步的参考地址

411　服务器拒绝用户定义的Content-Length属性请求

412　一个或多个请求头字段在当前请求中错误

413　请求的body大于服务器允许的大小

414　请求的URL长于服务器允许的长度

415　不支持的媒体类型。服务器不会接受该请求，因为媒体类型不受支持。

416　请求中包含Range请求头字段，在当前请求资源范围内没有range指示值，请求也不包含If-Range请求头字段

417　服务器不满足请求Expect头字段指定的期望值，如果是代理服务器，可能是下一级服务器不能满足请求长

服务器端错误：

500 – 内部服务器错误

HTTP 500.100 – 内部服务器错误

HTTP 500-11 服务器关闭

HTTP 500-12 应用程序重新启动

HTTP 500-13 – 服务器太忙

HTTP 500-14 – 应用程序无效

HTTP 500-15 – 不允许请求

501 – 未实现。服务器不识别该请求方法，或者服务器没有能力完成请求。

502 – 网关错误

503 – 服务不可用。服务器当前不可用(过载或故障)。

504 – 网关超时

6. TCP协议和UDP协议的区别是什么

1.基于连接与无连接；

2.对系统资源的要求（TCP较多，UDP少）；
3.UDP程序结构较简单；
4.流模式与数据报模式；
5.TCP保证数据正确性，UDP可能丢包，TCP保证数据顺序，UDP不保证。

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?

8. 简述tcp ip四层模型

1.应用层：传输文件
2.传输层：对接端口
3.网络层：选择路由
4.链路层：线路光纤

9. 简述 osi七层模型

1.应用层： 文件传输，电子邮件
2.表示层： 数据格式化
3.会话层： 接触或建立与别的借口
4.传输层： 提供端口对接
5.网络层： 为数据选择路由
6.数据链路层： 传输有地址的帧 以及错误检测功能
7.物理层： 以二进制数据形式在物理媒体上传数据

10. dns是什么 dns是哪一层协议

DNS是计算机域名(Domain Name System)的缩写，它是由解析器和域名服务器组成的。域名服务器是指保存有该网络中所有主机的域名和对应IP地址，并具有将域名转换为IP地址功能的服务器。其中域名必须对应一个IP地址，一个IP地址可以同时对应多个域名，但IP地址不一定有

域名。
DNS是应用层协议，TCP/IP协议族的一员

11. arp是哪一层协议

ARP和RARP都是网络层的协议,但是它所工作的内容是链路层的。
ARP具体说来就是将网络层（IP层，也就是相当于OSI的第三层）地址解析为数据连接层（MAC层，也就是相当于OSI的第二层）的MAC地址。

12. wifi是哪一层协议

wifi 数据链路层

13. 简述cdn作用

简述cdn作用,即内容分发网络,在现有的Internet中增加一层新的网络架构，将内容发布到最接近用户的网络"边缘"，使用户可以就近取得所需的内容，解决Internet网络拥挤的状况，提高用户访问网站的响应速度。

14. 服务器发生close wait是在什么时候

发生在第二次挥手和第三次挥手之间

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。
对于SYN泛洪攻击的防范，优化主机系统设置是常用的手段。如降低SYN timeout时间，使得主机尽快释放半连接的占用;又比如采用SYN cookie设置，如果短时间内连续收到某个IP的重复SYN请求，则认为受到了该IP的攻击，丢弃来自该IP的后续请求报文。此外合理地采用防火墙等外部网络安全设施也可缓解SYN泛洪攻击。

16. 156.123.32.13 是哪一类ip地址

B类

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　　广播地址为：193.32.5.63

18. icmp是哪一层协议

icmp是网络层协议：它是TCP/IP协议族的一个子协议，用于在IP主机、路由器之间传递控制消息。控制消息是指网络通不通、主机是否可达、路由是否可用等网络本身的消息。这些控制消息虽然并不传输用户数据，但是对于用户数据的传递起着重要的作用。

19. get方法和post方法的不同

GET ： 从指定的资源请求数据。

POST ： 向指定的资源提交要被处理的数据

20. 简述DOS攻击 和DDOS攻击

DoS：是Denial of Service的简称，即拒绝服务

最常见的DoS攻击有计算机网络带宽攻击和连通性攻击。

DDOS：分布式拒绝服务

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。

事实上DOS的攻击方式有很多种，比如下面的常见的：

1、SYN FLOOD

利用服务器的连接缓冲区（Backlog Queue），利用特殊的程序，设置TCP的Header，向服务器端不断地成倍发送只有SYN标志的TCP连接请求。当服务器接收的时候，都认为是没有建立起来的连接请求，于是为这些请求建立会话，排到缓冲区队列中。

如果你的SYN请求超过了服务器能容纳的限度，缓冲区队列满，那么服务器就不再接收新的请求了。其他合法用户的连接都被拒绝掉。可以持续你的SYN请求发送，直到缓冲区中都是你的只有SYN标记的请求。

2、IP欺骗DOS攻击

这种攻击利用RST位来实现。假设现在有一个合法用户(1.1.1.1)已经同服务器建立了正常的连接，攻击者构造攻击的TCP数据，伪装自己的IP为1.1.1.1，并向服务器发送一个带有RST位的TCP数据段。服务器接收到这样的数据后，认为从1.1.1.1发送的连接有错误，就会清空缓冲区中建立好的连接。这时，如果合法用户1.1.1.1再发送合法数据，服务器就已经没有这样的连接了，该用户就必须从新开始建立连接。

攻击时，伪造大量的IP地址，向目标发送RST数据，使服务器不对合法用户服务。

3、带宽DOS攻击

如果你的连接带宽足够大而服务器又不是很大，你可以发送请求，来消耗服务器的缓冲区消耗服务器的带宽。这种攻击就是人多力量大了，配合上SYN一起实施DOS，威力巨大。不过是初级DOS攻击。

4、自身消耗的DOS攻击

这是一种老式的攻击手法。说老式，是因为老式的系统有这样的自身BUG。比如Win95 (winsock v1), Cisco IOS v.10.x, 和其他过时的系统。

这种DOS攻击就是把请求客户端IP和端口弄成主机的IP端口相同，发送给主机。使得主机给自己发送TCP请求和连接。这种主机的漏洞会很快把资源消耗光。直接导致当机。这中伪装对一些身份认证系统还是威胁巨大的。

上面这些实施DOS攻击的手段最主要的就是构造需要的TCP数据，充分利用TCP协议。这些攻击方法都是建立在TCP基础上的。还有其他的DOS攻击手段。

5、塞满服务器的硬盘

通常，如果服务器可以没有限制地执行写操作，那么都能成为塞满硬盘造成DOS攻击的途径，比如：

发送垃圾邮件。一般公司的服务器可能把邮件服务器和WEB服务器都放在一起。破坏者可以发送大量的垃圾邮件，这些邮件可能都塞在一个邮件队列中或者就是坏邮件队列中，直到邮箱被撑破或者把硬盘塞满。

让日志记录满。入侵者可以构造大量的错误信息发送出来，服务器记录这些错误，可能就造成日志文件非常庞大，甚至会塞满硬盘。同时会让管理员痛苦地面对大量的日志，甚至就不能发现入侵者真正的入侵途径。

向匿名FTP塞垃圾文件。这样也可以塞满硬盘空间。

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?

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　　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。

28232

23. tcp三次握手中 第三次握手首部中syn值是多少 为什么?

1）第一次握手：建立连接时，客户端A发送SYN包（SYN=j）到服务器B，并进入SYN_SEND状态，等待服务器B确认。

（2）第二次握手：服务器B收到SYN包，必须确认客户A的

SYN（ACK=j+1），同时自己也发送一个SYN包（SYN=k），即SYN+ACK包，此时服务器B进入SYN_RECV状态。

（3）第三次握手：客户端A收到服务器B的SYN＋ACK包，向服务器B发送确认包ACK（ACK=k+1），此包发送完毕，客户端A和服务器B进入ESTABLISHED状态，完成三次握手。

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: 初始的序列号，Sequeue Number，TCP 协议栈为每一个封包都会分配一个sequence number，主要用来保证顺序的问题

ISN是一个随时间变化的值

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?

每次加1

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

MSS:最大报文长度，发送的报文不要超过这个值，一般情况下MTU-IP Header - TCP Header

TCP协议在实现的时候往往用MTU值代替（需要减去IP数据包包头的大小20Bytes和TCP数据段的包头20Bytes）所以往往MSS为1460

理论1500 实际1460

27. tcp最大长度是多少,为什么?

对于TCP协议来说，整个包的最大长度是由最大传输大小（MSS，Maxitum Segment Size）决定，MSS就是TCP数据包每次能够传 输的最大数据分段。

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?

发送窗口的大小因素有2部分： 拥塞、和接收方的接受窗口。
发送和接收数据的时候
接收端决定窗口大小

29. 如何理解tcp的半关闭(half-close)? 什么是全双工?

全双工指可以同时（瞬时）进行信号的双向传输（A→B且B→A）。指A→B的同时B→A，是瞬时同步的。

30. 为什么握手需要三次?为什么关闭连接需要四次?

三次握手：为了防止已失效的连接请求报文段突然又传送到了服务端，因而产生错误
四次挥手：在建立连接的时候,Server把响应客户端的请求和请求客户端的确认放在一起发送给客户端了,即第二次握手时有SYN+ACK
而断开连接的时候,一个方向的断开,只是说明该方向数据已传输完毕,而另一个方向或许还有数据,所以得等到另一个方向数据也全部传输完成后,才能执行第三次挥手

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.