**一、简答题和综述题**

1、**什么是协议，五层协议栈分别是什么，写出其作用和相关协议**

2、**内网用NAT和DHCP访问外网的过程**以及（NAT穿越问题）

3、**为什么实际带宽会小于链路带宽？TCP拥塞控制的机制和过程**

4、LAN多路访问协议中的协议以及每个协议的特点

5、**一个网段向另一个网段发送数据的过程**（不知道对方mac地址，ARP原理）

6、描述一下死锁（给你一个rdt状态机让你描述）

7、**带冲突检测的载波监听多路的工作，及CMDSA/CD二进制指数回退算法**

8、TCP和UDP异同点

9、GBN和SR工作过程和发送窗口尺寸（异同点）

10、**描述DOS环境下DNS手动查询获取网站IP过程。DNS各层次间的关系**

11、TCP发送方接收方特点，接收方收到错误或乱序的数据包如何处理  
12、描述TCP连接创建和断开过程

13、**数据报网络和虚电路网络的异同点**

15、**为什么要包含层次选路AS的划分和各自的协议特点**（08简单第三题）

16、怎样保证路由表准确无误？

17、HTTP报文简述

18、描述电子邮件传输协议

19、距离向量算法（DV）和链路状态算法（LS）的区别

20、电路交换、分组交换、报文交换优缺点

21、**Google（25分必考）**

**二、计算题**

1、**Dijsktra算法**

2、**循环冗余码计算**

3、**划分IP**

4、DV算法

5、校验和（checksum）计算

6、TCP请求RTT时间计算

答案

**一、简答题和综述题**

**1、**

协议是因特网各个层次运行的标准

分层：应用层、传输层、网络层、数据链路层、物理层

好处：1.层次分明独立性好；2.灵活性好；3.易于管理

应用层：网络应用程序及其应用层协议存留的地方。涉及HTML、SMTP、FTP等

传输层：提供不同主机的用户进程间端到端的通信。TCP、UDP

网络层：完成网络中主机间的报文传输：IP等

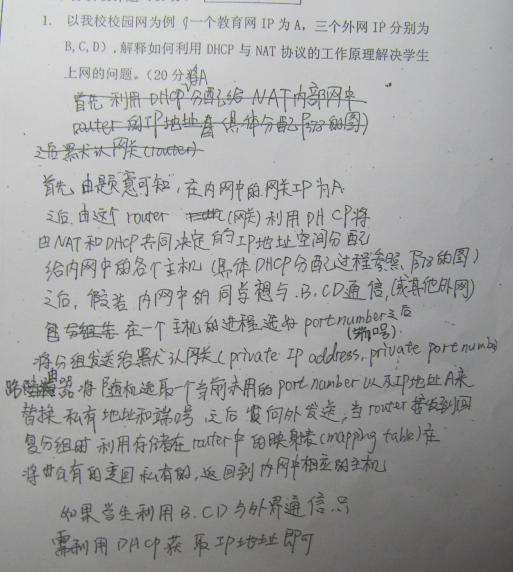
数据链路：提供给帧通过链路一端另一端的服务，将来自网络层来的数据可靠地传输到相邻节点的目标机网络层。：ARP等

物理层：将帧从物理信道上一个元素移动到另一个元素，确保原始的数据可在各种物理媒体上传输。RS-232 、RS-449、X.21、V.35、ISDN、以及FDDI、IEEE802.3、IEEE802.4、和IEEE802.5等

**2、**

这个题没有找到很好的答案，大家可以自己多从网上搜集一下资料

以下图片仅供参考



参考博客：https://blog.csdn.net/zhc\_24/article/details/82018678

**3、**

1.分组时延和丢失

传输时延：数据块长度与信道带宽的影响

传播时延：信道长度与信号传播速率

处理时延：交换结点（如路由器）为存储转发而进行了一些必要处理，比如差错检测；

排队时延：结点缓存队列中分组排队所经历的时延。与网络中通信量有关

2.拥塞控制和流量控制

传输层（TCP）会检测网络拥塞程度而抑制发送方的数据，使发送方发送分组的速度与接收方取分组的速度匹配

3.CSMA/CD协议等其他因素

注：TCP拥塞控制过程：

AIMD（加性增乘性减）：除慢启动阶段TCP大小每个周期增加1mss，如果出现拥塞则每次减半但不会小于1mss

慢启动：第一个周期发送1mss数据之后逐渐按指数级增加直到慢启动阈值（上一次loss事件的一半），结束慢启动阶段

超时处理：如果没有收到ack检测到超时事件表示严重拥塞则将tcp窗口大小改为1mss并重新开始慢启动，慢启动阈值变先前一半；若收到3个冗余ACK后：窗口减半再线性增加，慢启动阈值变先前一半。

**4、**

分类：1.信道划分协议：包括频分（信道频谱划分为若干频带，每个站点分配一个固定频带，无传输时相应频带空闲）、时分（周期性接入信道，每个站点在每个周期占用固定长度的时隙，未使用则时隙空闲）、波分、码分，分别简单描述

2.随机访问协议：当节点要发送数据时，利用信道全部速率发送分组，若多个节点同时传输则会产生冲突，典型的两种协议（时隙ALOHA和非时隙ALOHA协议还有CSMA、CSMA/CD（应用于以太网）、CSMA/CA（应用于802.11））。时隙ALOHA特点：所有帧大小相同，时间被划分为等长的时隙，结点只能在时隙开始时刻发送帧，如果冲突则以概率p重传；非时隙ALOTHA特点：有新的帧生成时立即发送，冲突可能性增大，但更加简单无需同步；CSMA特点：发送帧之前，监听信道，若空闲则发送，反之推迟发送（又分为1坚持、非坚持、p坚持），“边发边听，不发不听”；

3.轮转协议：分为轮询和令牌传递两大类；轮询：主节点轮流邀请从属节点发送数据；令牌传递：控制令牌依次从一个节点传递到下一个节点，拿到令牌才可以发送数据

**5、**

1.判断是否在同一子网：分别与子网掩码相与并比较是否一样——否，不在同一子网，封装arp广播包（目的mac为全F）获取网关1mac

2.网关1收到arp广播包返回自己的mac，主机将数据源ip和mac设为自己的，目的ip设为目的的，目的mac为网关1）封装发送数据帧到链路。

3.网关1收到，解析获得目的ip不是自己，查看路由表，路由表中有关于目标网段的下一跳，然后把源和目MAC地址重写 从相应的接口发出去，数据包沿途经过的路由器或网关设备都执行相同的动作，

4. 到达目标网段后，网关设备查看arp表，找目标IP的MAC地址（数据帧传输过程中源目IP不变，MAC地址在变化） 然后封装成帧进行发送（注意每次判断是否在同一网段都需要将子网掩码分别与自己的IP和目的IP与运算判别）

**6、**

此题简单，课本第三章第6题。附上那道题的答案：

如果 rdt2.1 发送方正处于“等待来自上层的调用0”，接收方处于“等待来自下层的0”，发送方发送序号为 0 的分组，而接收方正确接收并向发送方发送 ACK；此时发送方处于“等待 ACK 或 NAK 0”，接收方处于“等待下层的 1”，如果此 ACK 损坏，发送方重发序号0的分组，而接收方会发送 NAK，这将导致一个死循环；

其实此接收方并没有标注初始状态，如果发送方初始状态为“等待来自上层的 0”，接收方初始为“等待下层的 1”，也会导致上述死锁。

**7、**

话不多说，直接上图：



**8、**

UDP：①无连接；②尽最大努力交付；③面向报文；④无拥塞控制；⑤支持一对一、一对多、多对一和多对多的交互通讯；⑥首部开销少

TCP：①面向连接；②每一条TCP连接只能是点对点的（一对一）；③提供可靠的交互服务；④支持全双工通信；⑤面向字节流

**9、**

GBN：

1.分组头部包含序列号

2.窗口大小为N，最多允许N个分组未确认

3.ACK(n),则表示确认从开始到n（包含n）的序列号全部正确接收

4.为空中在传的分组设置一个Timer计时器，处理超时，如果收到了timeout(n)事件，那么会重传的是n以及n以后的所有分组（尽管后面的可能已经收到了，这就是回退，回退到n开始传，GBN）

5.接收方会有一个期望序列号，如果收到的不是期望的分组，直接丢弃

SR（选择重传）：

GBN有缺陷，累积确认机制导致回退到N，重复传了很多。为了解决这个问题

1.对每个分组分别确认，不再只接收期望的，接到不期望的，就先缓存（设置缓存机制），接到期望的才交付上层

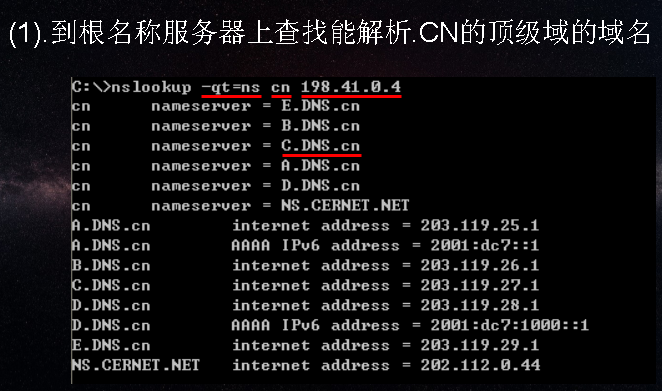
2.发送方只需要重传那些没收到ACK的分组了

3.产生了接收方窗口（GBN只有发送方窗口），用来缓存，现在有两窗口了

4.序列号的位数是K的话，那么得满足 接收方窗口大小N+发送方N<= 2的k次方，防止因为接收方ACK丢失导致发送重发k号分组，而此时接收方滑到了新窗口，新窗口有新的k号分组（不是原来的，共用序号产生的），导致出错

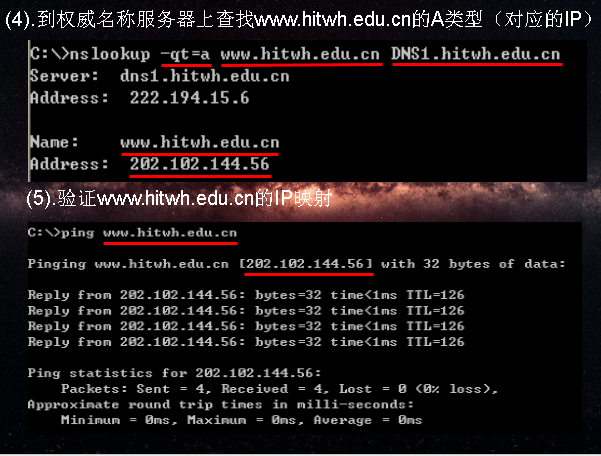
**10、**

直接上图了









答案一：

假定域名为m.xyz.com的主机想知道另一个主机y.abc.com的IP地址。下面是几个查询步骤：

1、主机m.abc.com先向本地服务器dns.xyz.com进行递归查询。

2、本地服务器采用迭代查询。它先向一个根域名服务器查询。

3、根域名服务器告诉本地服务器，下一次应查询的顶级域名服务器dns.com的IP地址。

4、本地域名服务器向顶级域名服务器dns.com进行查询。

5、顶级域名服务器dns.com告诉本地域名服务器，下一步应查询的权限服务器dns.abc.com的IP地址。

6、本地域名服务器向权限域名服务器dns.abc.com进行查询。

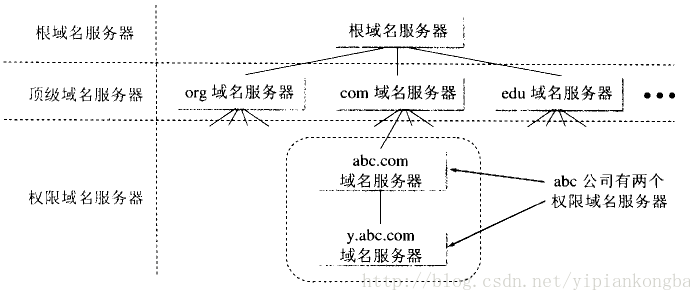
7、权限域名服务器dns.abc.com告诉本地域名服务器，所查询的主机的IP地址。

8、本地域名服务器最后把查询结果告诉m.xyz.com。

答案二：

以解析www.tsinghua.edu.cn为例，解析的过程如图 DNS解析过程。

　　1.客户端向DNS服务器发出查询www.tsinghua.edu.cn的请求，DNS服务器先在本机搜索是否有符合条件的域名。  
　　2.如果这台DNS服务器的本地区域文件和缓存中没有对应域名的资料，那么DNS服务器将向根域名服务器(root)发出查询请求。  
　　3.根域名服务器只知道它的下一级服务器地址，所以将.cn服务器的信息反馈给DNS服务器，以便查询。  
　　4.根据步骤3反馈的信息，向.cn域名服务器发出查询请求。  
　　5、将.edu.cn的域名服务器地址反馈给DNS服务器。  
　　6、7、8、9重复以上的步骤，直到找到www.tsinghua.edu.cn对应的IP地址。  
　　10、将最终结果反馈给客户端，并将这个结果存储在DNS的本地缓存中。



参考博客：https://blog.csdn.net/wyq\_tc25/article/details/51679520

**11、**

TCP发送接收特点：

发送方：采用应答机制，发送方发送的每个报文段都必须得到接收方的回答，才认为传输成功，为每个已经发送的数据段启动超时定时器，超时只重发引起超时的分组，若收到连续三个ACK则在计时器结束之前快速重传，有多个发送方窗口

接收方：多个接收方窗口，累计应答机制，收到TCP报文段后放入接收缓冲区。

遇到错误：对最近一次确认过的重新确认

遇到乱序：先缓存，根据序号重新排序在递交给应用层

**12、**

TCP建立的三次握手：

1、发送端发送一个SYN报文段（SYN位被置位1），SYN中包含TCP目的端口和发送端的初始序列号，同时携带着TCP选项数据。

2、接收端收到发送端连接请求后，接收端发送自己SYN报文段，同时对发送端的SYN进行确认，如前所述，接收端发送的ACK是发送的序列号+1。此时ACK位与SYN位都被置位。接收端发送SYN+ACK到发送端。

3、发送端接收到接收端的SYN+ACK数据后，进行确认，发送ACK=接收方发来的上一个seq+1的报文段给接收端，完成三次握手

TCP断开的四次握手：

1、TCP协议规定通过发送一个FIN段（FIN被置位1）来发起关闭操作，发送端发送FIN段给接收端，告知它数据已发送完毕，请求断开TCP连接。同时FIN报文段还包含着对最近收到的数据进行ACK。

2、接收端接收端FIN报文段后，对FIN进行确认，发送ACK=上一个seq+1给发送端。

3、接收端将连接关闭发送给上层应用程序，由应用程序发起连接关闭操作。此时接收端由被动关闭连接变成主动，并发送FIN报文段给发送端。

4、发送端接收到FIN后，发送回ACK给接收端后，TCP连接终止。如果FIN丢失，发送FIN的那端需要重新发送FIN，知道接收到ACK为止。

参考博客：https://blog.csdn.net/qq\_39010647/article/details/77531920

**13、**

虚电路网络/数据报网络特点：

1.发送数据前需要/不用先建立连接

2.每个分组含有虚电路标识/目的IP地址用于路由器转发

3.若路径中一个路由器损坏则所有分组都无法到达目的地/则可能都其他，剩余分组可选择其他路由器到达目的地

4.分组按序/乱序到达

另附一张图



**15、**

原因：1.规模：规模庞大时路由表无法存储和路由计算过程困难，交换量巨大，转发很难。

2.自制管理：管理者希望对自己范围内路由器进行管理，包括政策等方面诸多因素，减少路由也可以便于管理

每个AS由一组通常在相同管理控制下的路由器组成，同一AS内运行相同的路由协议分为自治系统内部和自制系统外部；

自制系统内部协议：RIP：采用DV（距离向量）算法，健壮性不好；

OSPF：采用洪泛链路状态信息的链路状态协议和dijkstra最低费用路径算法；

自治系统间路由选择协议：BGP协议：获得每个自治系统可达信息，分发路径信息承载了路径属性，并提供受控制的选路信息分布；

AS内通过什么策略确定：先通过AS间路由协议学习到目的子网是否可以通过多个网关到达，然后利用AS内路由协议获得路由信息确定到达每个网关的最小费用路径的费用。如果有多个网关可达，则采用用热土豆原则（将分组发给刚刚计算的最近的网关路由器）

内部路由器的用途：

边界（网关）路由器：为传递到自制系统外部的分组提供路由选择，安全保护

骨干路由器：为分组在区域间转发提供路由选择

区域边界路由器：为传递到区域外的分组提供路由选择

区域内路由器：为信息在区域内转发提供路由选择

**16、**

1.最大度量值：路由器设置一个最大度量值，当达到该值时，路由器就会认为这条路由已经失效，将他清除出路由表；

2.水平分割：从一个方向上学来的路由信息，不能再放入发回那个方向的路由更新包并且又发回那个方向；

3.路由中毒：网络出现故障时，通知邻居该网段不可用

4.毒性反转：当一条路径信息变为无效之后，[路由器](https://baike.baidu.com/item/%E8%B7%AF%E7%94%B1%E5%99%A8/108294" \t "_blank)并不立即将它从[路由表](https://baike.baidu.com/item/%E8%B7%AF%E7%94%B1%E8%A1%A8/2707408" \t "_blank)中删除，而是用16（表示不可到达），即不可达的[度量值](https://baike.baidu.com/item/%E5%BA%A6%E9%87%8F%E5%80%BC/8499637" \t "_blank)将它广播出去，它可以立即清除相邻路由器之间的任何环路，

5.保持时间：该网段的路由变成“down”状态时，还要在路由器中保留一段时间；

6.触发更新：当路由器发现某个网段出现故障时，立即发送路由更新包来通知邻居，而不用等到下一次发送路由更新包的时间

**17、**

最好了解一下。推荐博客：https://www.jianshu.com/p/74153d906e77

**18、**

1.运行在发送端邮件服务器主机上的SMTP客户，发起建立一个到运行在接收端邮件服务器主机上的SMTP服务器端口号25之间的TCP连接。

2.如果接收邮件服务器当前不在工作，SMTP客户就等待一段时间后再尝试建立该连接。这个连接建立之后，SMTP客户和服务器先执行一些应用层握手操作。就像人们在转手东西之前往往先自我介绍那样，SMTP客户和服务器也在传送信息之前先自我介绍一下。

3.在这个SMTP握手阶段，SMTP客户向服务器分别指出发信人和收信人的电子邮件地址。彼此自我介绍完毕之后，客户发出邮件消息。

4.SMTP可以依靠由 TCP提供的可靠数据传输服务把该消息无错地传送到服务器。如果客户还有其他邮件消息需发送到同一个服务器，它就在同一个TCP连接上重复上述过程;否则，它就指示TCP关闭该连接。

**19、**  
1.距离矢量:  
运行距离矢量路由协议的路由器,会将所有它知道的路由信息与邻居共享,但是只与直连邻居共享！  
链路状态:  
运行链路状态路由协议的路由器,只将它所直连的链路状态与邻居共享,这个邻居是指一个域内(domain),或一个区域内(area)的所有路由器！  
2. 所有距离矢量路由协议均使用Bellman-Ford(Ford-Fulkerson)算法，容易产生路由环路（loop）和无穷计数（counting to infinity）的问题。因此它们必须结合一些防环机制：split-horizon、route poisoning、poison reverse、hold-down timer、trigger updates  
同时由于每台路由器都必须在将从邻居学到的路由转发给其它路由器之前，运行路由算法，所以网络的规模越大，其收敛速度越慢。  
链路状态路由协议均使用了强健的SPF算法，如OSPF的dijkstra，不易产生路由环路，或是一些错误的路由信息。路由器在转发链路状态包时（描述链路状态、拓扑变化的包），没必要首先进行路由运算，再给邻居进行发送，从而加快了网络的收敛速度。  
3.距离矢量路由协议，更新的是“路由条目”！一条重要的链路如果发生变化，意味着需通告多条涉及到的路由条目！  
链路状态路由协议，更新的是“拓扑”！每台路由器上都有完全相同的拓扑，他们各自分别进行SPF算法，计算出路由条目！一条重要链路的变化，不必再发送所有被波及的路由条目，只需发送一条链路通告，告知其它路由器本链路发生故障即可。其它路由器会根据链路状态，改变自已的拓扑数据库，重新计算路由条目。  
4.距离矢量路由协议发送周期性更新、完整路由表更新（periodic & full）  
而链路状态路由协议更新是非周期性的（nonperiodic），部分的（partial）

**20、**

电路交换：

优点①　传输时延特别小②　双方物理链路一旦建立，随时通信，实时性强③　数据传输正确性强

缺点a. 电路交换平均建立时间对计算机通信来说长b. 物理通路被通信双方独占，信道利用率低c. 难以进行差错控制

报文交换

优点①　不存在连接建立时延，随时发送报文②　采用存储转发的传输方式，使路径多选择性，提高传输可靠性；便于不同类型，不同规格计算机之间进行通信；提供多目标服务；允许建立数据传输优先级③　提高了通信线路的利用率

缺点a. 转发时延大，实时性差b. 只适用于数字信号c. 需要网络结点有大的缓冲区储存整个报文，增加时延

分组交换

优点①　加速了传输速度，时延相比报文传输减小②　简化了存储管理③　减小了出错几率和重发数据量④　更适用于优先级策略

缺点a. 节点交换机需要有很强的处理能力b. 传送信息量增多，降低了通信效率，增加了处理时间c. 可能出现失序、丢失、重复的问题

**21、**

答案一：

1.通过DHCP获取主机地址，BOB笔记本电脑的操作系统生成一个DHCP请求报文，并将该报文放入到目的端口67，原端口68的UDP报文段，该udp报文段则被放置在一个具有广播ip目的地址（255.255.255.255）和源ip地址0.0.0.0的ip数据报中，该数据报被放置在以太网帧中，该帧到源mac地址为（自身mac地址）目的mac地址为（ff：ff：ff：ff：ff：ff）进行广播，路由器在它的具有mac地址xx的接口接收到该广播帧，分离出DHCP请求报文，然后给其分配ip，DHCP服务器会产生一个包含ip地址，d n s服务器ip，子网掩码，默认网关ip的DHCP ACK报文，将其报文封装并放入以太网帧中以目的mac为bob主机mac，源mac为路由器接口mac发送给bob，bob收到该报文后，将自己的ip地址，dns服务器ip记录下来，同时将默认网关的地址安装在ip转发表中

2.通过DNS查询谷歌的IP地址，将含有DNS查询报文的数据报放入以太网帧中，为了获取网关路由器的MAC地址，将生成一个目的ip为（默认网关）的ARP查询报文，将该报文放置在一个具有广播地址（FF:FF:FF:FF:FF:FF）的以太网帧中，发送该帧，网关路由器收到该帧后，将返回一个包含自身mac地址的ARP回答报文，将其放在一个以太网帧中返回bob主机，从中抽取网关路由器的mac地址，随后可以将包含dns查询报文的帧发送到网关路由器，路由器根据最大前缀匹配原则，利用他的转发表将其送到dns服务器上，dns服务器抽取出dns查询报文，然后在他的dns数据库中查找名字为[www.geogle.com](http://www.geogle.com)，假设它缓存在dns服务器中，则可以找到包含www.geogle.com的ip地址的dns源记录，dns服务器则形成一个包含主机名到ip地址映射的dns回答报文，将报文封装进以太网帧中，发送到bob主机，bob从dns回答报文中提取谷歌的ip地址

3.bob生成tcp套接字，随后开始进行tcp连接，首先生成一个具有目的端口80 的TCP SYN报文段，将该tcp报文段放置在具有目的ip地址（谷歌）的ip数据报中，将该数据报封装在mac地址（网关路由器）的帧中，利用路由器转发表将该数据报发送到www.geogle.com，从数据报中取出tcp syn报文并分解到与端口80想联系的欢迎套接字中，对于谷歌http服务器和bob主机之间的tcp连接生成一个连接套接字，产生一个tcp syn ack报文段，该报文段最终到达bob主机的以太网卡，将其分解到tcp套接字中， bob主机上的浏览器生成包含要获取的URL的http get报文，将该报文写入套接字中，get报文成为一个tcp报文段的载荷，将该报文段交付到www.geogle.com，www.geogle.com从tcp套接字中读取http get报文，生成一个包含请求的web页内容的响应报文，将该报文发送进tcp套接字中，包含http响应报文的数据报到达bob主机，bob主机上的web浏览器程序从套接字中读取http响应，从http响应体中抽取web页面的html，最后显示网页。

答案二

1.DHCP:客户机创建一个DHCP请求封装在UDP中（源IP全0，mac全f）全网广播，路由器接收到为其分配IP并将IP、子网掩码、网关IP及dns服务器IP封装到DHCP ACK数据包封装后发送给客户机，客户机记录自己的IP掩码dns并将网关IP记录到自己的转发表

2.客户机将自己和dns服务器的IP和子网掩码逐bit相与得到网络号，如果在同一网段则发全网arp广播包（目的mac为全F）；如果不同则发送arp广播包（目的mac为网关，IP为dns），路由器看到不是给自己的则持续上面这个过程发给上层其他路由直到到达dns服务器。dns服务器将mac发给客户机

3.获得dns的mac发送arp请求，再dns数据库中找到google域名，如果找到google的IP地址原始记录则形成一个dns回复报文（包含主机名到地址的映射）封装后发给客户及，如果没有则到根名称服务器中寻找其根名称的顶级域名称服务器IP，再在其中找其权威名称服务器的IP，最后在权威名称服务器中找主机名和IP地址，打包发给客户机。客户机从中提取谷歌的IP

4.客户机创建一个被用来发送http报文的tcp套接字进程，准备连接服务器。客户机创建tcp syn报文到http服务器后被封装发送给谷歌服务器，谷歌服务器接收到后将其分到80端口并形成一个tcp syn ack报文发给客户机之前创建的套接字中。客户机创建http get信息并将其套接字联同get信息一起成为tcp报文中有效荷载的一部分，封装后发给谷歌。谷歌从中提取get信息后形成tcp回复报文封装到http报文主体内然后发送套接字到客户机，客户机的web浏览器从套接字读取http回复报文，从http相应报文主体部分提取网页html内容，最后显示网页。

**二、计算题**

1、**Dijsktra算法**

解题步骤：先描述，再制表

描述过程：

1.所有结点需将链路状态信息传递到其他所有的节点，链路信息包括与邻居节点的连通性和每段链路的代价，从而每个结点都拥有整个网络的拓补结构和链路代价值。

2.在扩散过程中需要进行洪泛控制，主要方法包括①增加TTL值，没经过一个路由减一，减为0后丢弃②为每个分组标号，发送一个分组序号加一，路由器记录分组的最大序号，若到来的分组序号比这个序号小，则说明已经转发过，丢弃该分组，反之则进行转发

制表过程自己列

2、**循环冗余码计算（必考5分）**

简单题。参考博客：https://blog.csdn.net/u012965373/article/details/46785127?tdsourcetag=s\_pctim\_aiomsg

3、**划分IP**

重点掌握，不会的回去好好再看一遍

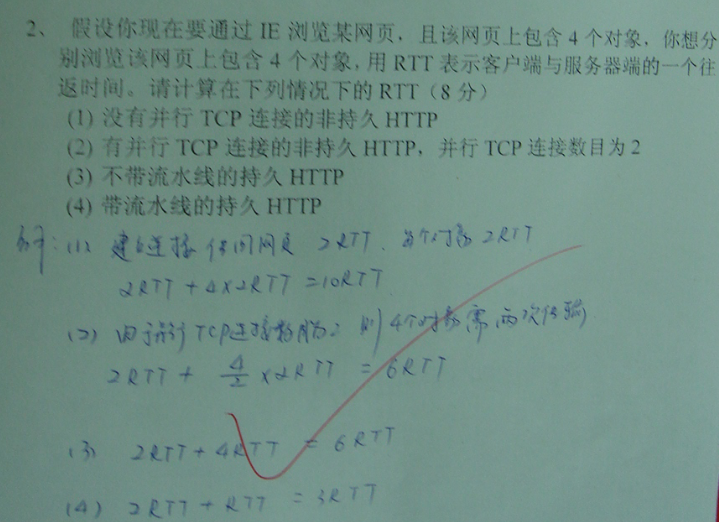
4、DV算法

会画图描述即可，有考的可能，参考课本283页P28

5、校验和计算（相加，若有进位继续加再取反）

6、TCP请求RTT时间计算

类似下图



附知识点：

实现网络互连的传输媒介（如光纤、双绞线、微波等）称为 链路；

协议三要素：语法 语义 时序；

UDP报文的头部8个字节，TCP一般20字节；

以太网帧范围：64-1518；其中数据字段 46-1500；

关于TCP、UDP数据包大小，参考博客：https://blog.csdn.net/caoshangpa/article/details/51530685

Rdt几个状态机最好能够记住画出来

rdt1.0：接收方无返回确认信息 rdt2.0：接收方进行检错，并发送ACK 或NAK反馈给发送方

rdt2.1：加入序列号0和1 rdt2.2：接收方不再发NAK而将ACK中加入序列号

rdt3.0：发送方引入定时器

祝大家计网都90+！