1.先看试卷题型

2.从头看每一章 一共七章

对着提纲看教材

看完一章看那一章的习题

记录每一章主要考什么

3.看复习笔记

1. 试卷题型

16年试卷

1概念题：NAT multiplexing and demutiplexing DNS BGP Slow start Flow control

2问答题：1解释traceroute program的设计 2 packet switched network的延迟原因 四种，如何减轻这四种延迟

3计算题：1子网 网关 每个子网支持几个interfaces 算出地址a.b.c.d/x

2 4bit生成器，G=1101 想要D是111111101，则R的CRC值是多少

3 用Dj算法算出u到所有节点的最短路径

4 综合题：一个场景 输入<http://www.ucdavis.edu> 请说明应用层、运输层、网络层和链路层都做了说明操作，并列出每个层的主要协议

16年期中

1 概念题：IMAP persistent HTTP multiplexing and demultiplexing selective repeat network protocol

2 HTTP是无状态协议 请给出两个方法来跟踪用户在服务器都行为，？设计题

3 Domain Name System（DNS）的主要任务是什么，简述它是如何工作的

4 描述TCP连接重服务端和用户端都有哪些步骤，TCP服务器如何同时处理多个用户请求

5 UDP如何检测接受段的bit错误，请用一个例子描述这个机制

6 如何用一个非可靠网络层来实现一个可靠传输，描述具体细节

7 TCP如何实现高速传输（克服stop和wait短板），请描述这个机制并给出例子

15年期末

1 概念题：SYN and FIN NAT Slow Start DNS subnet difference of Datagram or VC network

2 计算题：7bit生成器，G=10011 想要D是1010101010和1001010101，则R的CRC值是多少

3 CSMA/CD protocol：Ethernet adapter waits K\*512bit time 如何确定k值

4 TCP＆UDP：传输协议的四大类服务 如何选择TCP和UDP

5 综合题：场景 输入[www.baidu.com](http://www.baidu.com) 从end-host角度，每一层执行什么样的操作

6 网络层：1Dj算法确定A到其他节点的最短距离，提出两个问题当使用链路状态和dj算法时，距离向量会遭受的问题

2子网 网关 每个子网支持几个interfaces 算出地址a.b.c.d/x

14年A卷：

1 简答题：1)丢包的两个原因 2)包延迟的四个因素，并说明在不同场景(LAN近距离，地球同步轨道卫星连接，不同城市网络连接)下哪个占主导

2 TCP机制：一堆看不懂的TCP stack on desktop 支持 timeout-driven重传 和快重传

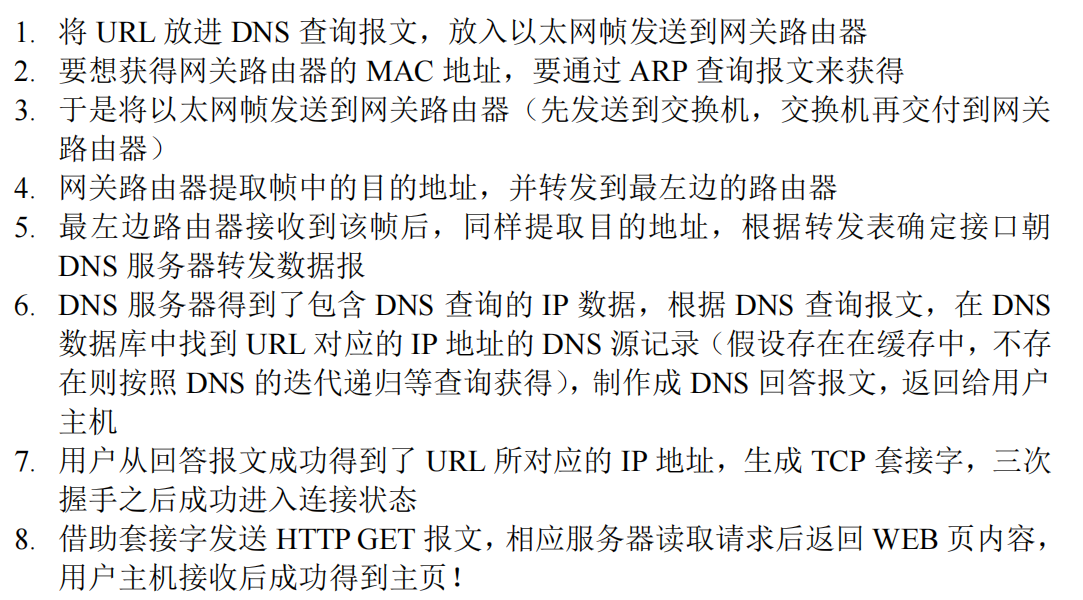
3 Dj算法 以及使用链路状态和dj算法中距离向量会遭遇什么问题

4 计算一些最大传输速率

5 错误检测 计算CRC（通过消息M和多项式P），说明校验和不能检测的错误

6 为什么Ethernet有最小的包大小 CSMA/CD 为什么不能用在无线环境

7 输入网址 各个层干了什么（DNS, TCP/UDP, IP, MAC）



14年B卷：

1 无状态的HTTP如何识别用户

2 TCP AIMD机制

3 给定拓扑结构 写出距离表 写出距离向量算法的最后一次迭代 比较链路状态和距离向量路由算法

4 NAT 填写数据包中缺失的源和目标IP地址和端口号。(

5 CAC 讨论校验和和CRCs之间的权衡。

6 CSMA/CA 是什么 如何工作

7 输入网址 各个层干了什么

1. 逐章复习

一些套话：减少响应时间，减少接入互联网通信量，降低web服务器流量

控制数据传输时间，无需连接、不用维护连接，首部行开销小

分散 开销 差错保护

丢包率、缺乏拥塞控制、引入时延

集中式：主节点瘫痪

一：概述

电路交换（频分复用FDM、时分复用TDM：问题：静默期空闲、效率低）

分组交换（四个时延：处理时延、排队时延、传输时延、传播时延）端到端时延

报文→报文段→数据报→以太网帧→比特

带宽-时延积：链路上正在传输的最大比特值

二：应用层

套接字：应用层和传输层的接口，网络应用程序的可编程接口

【TCP：面向连接 全双工 可靠 有序 拥塞控制 流量控制 公平共享带宽

UDP：最小的 必要的 运输层服务】

HTTP：超文本传输协议 在综合题描述场景（发送HTTP请求响应）

RTT：客户到服务到客户来回时间 和TLL区分

持久连接：所有请求和响应经过同一TCP连接，一段时间未使用则关闭（描述）

持久HTTP连接不能并行打开超过2个

非持久连接：每次请求和响应都要经过单独TCP连接来发送

HTTP无状态，使用cookie跟踪用户：用户首次请求访问到达web服务器将产生唯一识别码，作为索引存放在数据库中，服务器响应中包含了set-cookie的首部行，之后每次用户请求都包含cookie在首部行中，服务器就能根据cookie实现对不同用户的追踪

Web缓存 代理服务器 磁盘空间 TCP 缓存查找 作用

FTP文件传输 SMTP电子邮件 推协议 将所有对象放在一个报文中

IMAP是因特网邮件访问协议，提供了创建文件夹移动邮件的命令，提供了获取单独报文组件的命令，可以维护用户状态信息

DNS：域名系统，DNS服务器能够实现主机名到IP地址的转换，使用UDP协议，工作机理是从本地DNS服务器开始，返回下一个可查询的服务器，不断联系可能知道的服务器，知道得到主机名对应的IP地址。

功能是能够给主机起多个别名，实现负载配置。

TTL：信息缓存在本地存储器的时间

区分：计算DNS响应时间 2\*RTT0+RTT1+…+RTTN

非持续非并行的连接：k个对象 2\*k\*RTT0+2\*RTT0+RTT1+…+RTTN

非持续c个并行连接：2\*RTT0+RTT1+…+RTTN+(k/c上取整)\*2\* RTT0

持续连接（流水线）：k\*RTT0+2\*RTT0+RTT1+…+RTTN

服务器/客户机：最小分发时间 max{NF/Us, F/Dmin} 线性上升，且总大于P2P

P2P：最小分发时间max{F/Us, F/min(Di), NF/total(U)}

bitTorrent：方法特定文件的对等方集合：最稀罕优先 对换算法

三：运输层

多路复用：从源主机不同套接字收集数据块，并封装首部信息生成报文段，传递到网络层

多路分解：将传输层报文段数据正确交付到对应套接字

UDP：好处：控制数据传输时间，无需连接、不用维护连接，首部行开销小

坏处：丢包率、缺乏拥塞控制

校验和：16比特字的和取反码，溢出则回卷。 但是不提供差错恢复

可靠数据传输：画FSM

Rdt1.0：完全可靠信道上的可靠数据传输

Rdt2.0：具有比特差错信道上的可靠数据传输 停等协议 ACK NAK也可能受损

增加校验和比特：检测+恢复 重发冗余分组

Rdt2.1 引入数据分组编号：失序或受损则发NAK

Rdt2.2 无NAK 接收方发ACK+分组序号 发送方检测ACK的分组序号

Rdt3.0：具有比特差错的丢包信道上的可靠数据传输

发送方发送分组启动计时器，给定时间后中断重发

流水线可靠的数据传输：

GBN回退N步：发送方：检测窗口是否满 累计确认 超时重传

接收方：检查是否按序 只需要看下一个序号是否正确

问题：一个分组差错会导致全部重传

SR选择重传：发送方仅重传怀疑出错的分组

收到ACK在窗口内则标记为接收，移到至最小标记处，发送窗口内所有未发送分组

接收方范围：[rec\_base,rec\_base+N-1] [rec\_base-N,rec\_base-1]

窗口大小小于序号空间的1/2

TCP 点到点 可靠有序 字节流 缓存 全双工 连接“握手” 流量控制

MSS：最长报文段

连接：三次握手 ①发送连接请求SYN=1 ②服务器分配缓存和变量 SYN=1 ③客户机分配缓存和变量 确认请求 SYN=0

终止：四次握手 ①客户机发送终止请求 FIN=1 ②服务器发送确认最终报文段 ③服务器发送终止报文段 FIN=1 ④客户机确认终止

TCP拥塞控制：通过TCP发送方对发送流量的限制

未确认数量不超过congwin和recvwin最小值

加性增、乘性减：收到ACK确认congwin+MSS，丢包则congwin减半（不低于MSS）

（拥塞避免CA）

阈值：threshold，当conwin>threshold，则转SS为CA

慢启动SS：以慢速率开始发送，但是指数递增速率 因为线性增加太慢

超时反应：①收到三个冗余ACK则将threshold、congwin=congwin/2 (快速恢复)

②超时：congwin=1MSS进入慢启动

四：网络层

交换结构：选路处理器：交换技术：内存、一根共享总线、互联网络

影响丢包：排队：流量负载、交换结构相对速率、线路速率

子网：同一子网下的设备可通过不含路由器的网络相连，所有接口具有相同子网掩码。子网分开主机和路由器产生几个分离的网络岛

DHCP：动态主机配置协议，维护可用IP地址表，主机可自动获取IP地址和其他信息

1. 主机广播报文255.255 .。。DHCP服务器发现 ②提供ip地址和其他信息
2. 主机选择ip地址并发送请求 ④ DHCP确认ACK

NAT：网络地址转换，可用于具有专用地址的地域，NAT路由器对外界如同一个单一IP地址的单一设备，NAT路由器维护一张转换记录表

特点：不需要ISP分配连续地址，可自己修改内网地址，内网设备安全

争议：端口号属于编址进程 路由器处理多大三层 违反端到端介入ip地址

ICMP：主机和路由器之间交换网络层信息，差错报告 traceroute通过ICMP实现

MTU分片：减去首部行20 最大偏移量为255 标识为11110

SDD operflow 的流表向项：ingress port Ipsrc ip dst port forward

五：网络层

链路状态选路算法LS：dijkstra算法

问题：震荡

解决：确保不是所有路由器都运行dijkstra算法

距离向量算法DV：接收邻居节点信息，计算发回 d(y) c(x,v)

问题：选路环路和计算到无穷问题

解决：增加毒性反转，计算完邻居节点信息发回该更新信息不可达

其他方案：RIP设置最大距离 BGP协议每条路记录经过路由 水平分割

大问题：规模变大后，广播更新链路开销使得没有剩余带宽进行数据运输

自治系统：AS

AS内选路：RIP 距离向量协议 RIP限制了15跳（子网数量）

30s交换一次信息 180s没有监听到邻居则不再任务可达，修改路由表

OSPF dijkstra算法 洪泛链路信息

链路费用由管理员配置：1 链路容量的反比

AS间选路：BGP是边界网关协议，能够在跨越自治区域的源和目的地间确定路径

半永久TCP 有iBGP一个AS中路由器 eBGP：两个AS间路由器链路两种类型

六：链路层

差错检验：

奇偶校验 单位二位 不够健壮

互联网校验和 分组开销小 差错保护弱

循环冗余检验CRC 更高的误检率和更低的漏检率

使用生成多项式对数据进行计算

多路访问协议：

信道划分协议 时分复用TDM 频分复用FDM 码分复用CDMA

公平、消除碰撞 利用率低 同时使用不同编码

随机接入协议 时隙ALOHA协议 碰撞则以p概率重发

一个节点时可全速 高度分散 多个节点时会重复碰撞

CSMA协议：载波侦听 碰撞检测

轮流协议 轮询协议： 有一个主节点 消除碰撞和空时隙 效率高 轮询时延 主节点

令牌传递

MAC地址 配置

地址解析协议ARP：网络层和链路层

使用：每个节点存储一个ARP表，即插即用。查询节点表项：有则直接使用得到的MAC地址，无则广播ARP报文，匹配节点会发送响应ARP分组

请求访问的分组封装：IP地址源和目的IP地址 MAC地址同一子网下的源和目的MAC地址

以太网：CSMA/CD

1. 随时开始传输
2. 载波侦听：传输前侦听信号 碰撞检测传输时保持侦听
3. 重传等待随机时间 连续碰撞n次，取m={n,10} k=random{0,1,2,…2m-1} 等待K512比特时间

工作方式：①网络层数据包封装成以太网帧进入适配器缓冲区

1. 信道空闲则传输，否则等待至无信号能量传输
2. 传输中，侦听到碰撞则传输48bit阻塞信号（让其他适配器也察觉到碰撞），进入指数后退阶段

交换机：交换机表：转发和过滤 自学习 即插即用

消除碰撞，双工 最大聚合带宽低于所有接口速率之和 异质链路

对比：交换机 即插即用 过滤转发速度快（处理数据快） 无法处理广播风暴 链路限制在生成树上，且需要维护庞大的ARP表，流量大

路由器反过来

MPLS 标签交换路由器 跟着图写标签