**各章节知识点及内容（ma学长版）**

**第一章**

**第二章**

1. **WEB + HTTP**
2. **FTP**
3. **SMTP +POP3 + IMAP**
4. **DNS**

**第三章**

**1、分用和复用**

**2、UDP**

**3、可靠数据传输 rdt1.0、2.0、2.1、2.2、3.0**

**4、TCP**

**5、可靠数据传输的拥塞控制：GBN与SR**

**6、TCP拥塞控制**

**第四章**

**1、虚电路网络**

**2、路由器内部**

**3、IP段结构、IPv4地址、ICMP、IPv6、DHCP、NAT**

**4、路由算法（LS、DV、层次路由）**

**5、因特网中的路由（ROP、OSPF、BGP）**

**第五章**

**1、差错检错 CRC**

**2、多路访问协议 MAC**

1. **什么是协议？协议分层的好处是什么？详细描述TCP/IP协议栈5个层次的功能及相关协议**

**协议：**通信双发约定好发送发送数据包的格式、通信次序以及发送和接收数据所采取的动作

**协议分层好处：**

1. 相互通信的两个计算机系统必须高度协调工作，这种协调相当复杂，分层了将庞大复杂的问题转化为若干较小的局部问题，从而易于研究
2. 明确的结构有助于标志复杂系统构件的关系
3. 各层之间独立性好，灵活性好，各层的实现由其自身完成
4. 模块化，在结构上可分隔开，易于实验和维护
5. 能促进标准化工作

**TCP/IP协议栈五个功能及相关协议：**

|  |  |  |
| --- | --- | --- |
| 层次 | 功能 | 协议 |
| 应用层 | 允许应用访问网络资源 | HTTP、FTP、SMTP、POP3、 |
| 传输层 | 1. 为运行在不同主机上的应用进程提供逻辑通信 2. 提供可靠数据传输 | UDP、TCP |
| 网络层 | 将传输层递交下来的分组教导对方主机中去，实现主机间的逻辑通信 | IP、ICMP、RIP（选路信息协议）、  OSPF（开放最短路优先协议）  BGP（边界网关协议） |
| 数据链路层 | 实现数据在一段链路 两端节点的递交 | MAC（多路访问协议）、TDMA、FDMA、CDMA、随机访问协议、CSMA（载波监听多路访问协议）、ARP（地址戒心协议） |

**网络协议的组成要素：**

1. **语法**：数据和控制信息的结构或格式
2. **语义**：需要发出何种控制信息，完成何种动作，做出何种响应
3. **同步**：事件发生的的先后顺序
4. **访问因特网时为什么你的访问带宽远远低于实际物理带宽？请详细分析原因（分组交换网络中的时延有哪些，时延产生的原因是什么）**

**原因**：主要是因为分组的**时延**、丢失、流量控制、拥塞控制、多路访问协议限制和冲突

**时延**：

**① 队列时延**：分组在路由器缓存队列排队所经历的时间

**② 处理时延**：路由器为存储转发分组而进行的一些必要处理所花费的时间

**③ 传播时延**：分组在信道中传播花费的时间

**④ 传输时延**：数据块从节点进入到传输媒体所需要的时间

**丢失：**若选用TCP，进行分组重传需要时间

**流量控制：**发送方不能发送太多太快流量淹没缓冲区

**拥塞控制：**TCP拥塞控制防止发送方传输太多流量导致网络拥塞

**冲突：**数据链路层的多路访问协议会限制节点发送流量，出现冲突还要进行重传

1. **DNS服务的层次结构中各层的相互作用是什么？请描述手动查询本地DNS对[www.weihai2014.com](http://www.weihai2014.com)解析的过程，并详细描述如何获取层次结构的组成及各层次的功能**

**DNS各层的相互作用：**

提供下一层名称服务的的域名和对应关系

**各层次的功能：**

1. 根名称服务器：存放所有顶级域名称服务器的域名和对应关系
2. 顶级域名称服务器：存放具体负责某一部分的权威名称服务器的域名和对应关系
3. 权威名称服务器：负责最具体的内容，网站的域名和对应关系

**手动查询本地DNS的解析过程：**

1. 在本地DNS服务器上查找该域名，若本地名称服务器能找到该域名的对应信息，则返回给用户，否则，前往步骤2
2. 本地名称服务器向根名称服务器发起请求，获取能解析.com的顶级域名称服务器的域名；再向顶级域名臣服务器发起请求，获取能解析.weihai2014.com的权威名称服务器信息；再向权威名称服务器发出请求，获得[www.weihai2014.com](http://www.weihai2014.com)对应的域名；
3. 本地名称服务器将该信息返还给主机。
4. **详细描述TCP拥塞控制算法（三个主要部分的详细描述）？？？参见Google**
5. **加性增乘性减**：未出现丢包事件时，每RTT时间拥塞窗口值增加一最大段尺寸；出现丢包时间，若收到３个冗余的ACK，则将拥塞窗口值变为原１／２
6. **慢启动**：连接刚开始时，每RTT时间，拥塞窗口值翻倍，呈指数增长
7. **超时事件后的保守机制**：若出现超时时间，拥塞窗口值回落到一个最大段尺寸，进入慢启动阶段；出现3个冗余的ACK，拥塞窗口值变为原１／２
8. **详细描述主机H1发送数据到主机H3的转发过程，在描述转发过程中请考虑网络层及数据链路层的转发处理。注意本图为初始状态，主机及路由器中尚未形成ARP转发表**

① 首先，H1拿H1IP、H3IP分别与子网掩码与一下，发现H1与H3不在同一网段

② H1封装ARP广播包，src：H1IP，dest：R10IP，src MAC：MH1，dest MAC：全F。其余主机接收到广播包以后，其余主机在数据链路层接收包，把H1IP与MH1对应关系记录进ARP转发表；递交到网络层，发现不是自己的IP，将其丢弃

③ R10收到包以后，在自己的ARP广播表里面记录H1IP与MH1的对应关系；并发送报文响应；src：R10IP；dest：H1IP；src MAC：MR10；dest MAC：MH1；其余主机在数据链路层接收到分组，发现不是自己MAC地址，丢弃

④ H1收到R10的数据包，获得R10的MAC地址，并将R10IP与MR10的对应关系写入自己的ARP转发表；然后发送报文：src：H1IP；dest：H3IP；src MAC：MH1； dest MAC：MR10；

⑤ R10收到广播包之后，获取目的IP，按最长前缀匹配原则与表中的表项相匹配，决定从R11端口转发到R20；将src MAC改为MR11，dest MAC改为MR20；

⑥ R20收到广播包之后，查询路由表，将其移动到R21；

⑦ R21发送ARP广播包，经过与②、③相同的步骤，获取H3的MAC地址

⑧ R21将报文src MAC替换为MR21，dest MAC替换为 MH3；发送出去

⑨ H3接收到报文，发现dest MAC是MH3，递交到网络层，网络层发现dest是H3IP，递交到传输层。

⑩ 完成H1转发数据到H3

1. **请阐述虚电路网络和数据报网络的特点，电路交换网络与虚电路网络的异同**

**虚电路网络：**

① 发送数据之间需要先呼叫

② 每个分组携带虚电路标识，每经过一个路由器，VC被替换

③ 属于同一条虚电路网络的分组均按照同一路由进行转发，按序到达目的地

④ 可靠通信由网络保证

⑤ 由路由器建立虚电路表和路由表，维持连接状态

⑥ 当一个路由器节点损坏时，所有通过该节点的虚电路均不能正常公国

⑦ 网络核心复杂，网络边缘较为简单

**数据报网络：**

① 无连接服务，不需要建立连接

② 每个分组都是用源IP和目的IP

③ 分组经历的路径可能不同，可能乱序到达

④ 出现故障的路由器可能丢失分组，部分路由路径可能改变

⑤ 有用户主机保证可靠性通信

**数据包网络和虚电路网络的异同：**

① 同：都进行呼叫建立连接

② 异：虚电路网络共享信道，竞争成功使用满带宽；电路交换网络划分资源，独占信到

1. **TCP可靠数据传输的发送方和接收方各有什么特点？接收方收到错误或乱序的数据包如何处理**

**发送方：**

① 使用单一计时器，只为最早发出没有得到ACK响应的分组建立计时器

② 只重传引起计时器超时的分组，后面没有得到确认的分组不重传

③ 若得到对同一个分组的4次ACK，则进行快速重传

④ 具有多个发送窗口

**接收方：**

① 是否缓存乱序到达的分组由开发者决定

② 给出累计应答

③ 接收到一个分组，且是所期望的序号，等待500ms再给出应答

④ 接收到一个分组，若正处于上一个分组的延时应答时间内，立即给出累计应答

⑤ 接收到一个分组，若是期望的序号，而且能补全乱序到达的分组。立即给出累计应答

⑥ 接收到一个分组，乱序或分组错误，给出对上一个已确认分组的再次确认

**如何处理：**

① 否缓存乱序到达的分组由开发者决定，一般是缓存

收到乱序或错误的分组，给出对上次确认分组的再次确认

1. **以我校校园网为例，一个教育网的IP是A，三个外网的IP分别为BCD、解释如何利用DCHP和NAT协议的工作原理解决学生的上网问题**

// 参见Google

首先，主机通过以下方式获取IP

1. 主机使用UDP广播DHCP发现报文，源IP0.0.0.0，目的IP：255.255.255.255；源MAC：自己MAC；目的MAC：全F
2. DHCP服务器响应，发出DHCP提供报文，由于可能有多个DHCP服务器，仍然使用广播的形式发送，报文内容有分配的IP、使用时间、时间号等
3. 主机从DHCP主机中选择一个，发送DHCP请求报文，确认使用某一配置
4. 服务器回复确认

以上部分参见Google

然后，使用NAT上网：

1. 主机发送对外分组，路由器为其生成一个新的端口号，并将源IP替换为广域网一侧的IP，并在NAT转换表中增添一个表项
2. 当发往主机的分组到达路由器，路由器根据目的IP、目的端口号从NAT转化表中检索出主机的IP和端口号，改写后发送主机
3. **因特网为什么采用层次选路？AS是如何划分的？各包含什么常用的选路协议？协议的特点分别是什么？自治系统F收到其他自治系统的信息如下图，请阐述F依次通过什么策略确定其内部路由配置的？OSPF路由器的作用分别是什么**？**intra-AS与inter-AS有什么区别：**

**为什么采用层次选路**：

1. **规模**：因特网中主机数量巨大，路由器无法存储所有的路由信息表，且路由信息表的交换会阻塞通信链路
2. **管理自治**：每个管理员可能想要控制他自己网络中的选路

**AS如何划分：**

将某区域的路由器聚合为自治系统AS，相同的AS中的路由器运行相同的选路协议

**各包含什么常用的选路协议及其任务：**

I、**自治系统内部路由选择协议**

**1、RIP**（路由选择信息协议）：DV算法.

① 每30s在邻居节点之间交换相应报文，最长距离为15跳；

② 每个通告中包含最多25个目标子网的列表

③ UDP报文

若180s没有收到邻居节点的报文，就通知邻居节点通过该邻居节点的选路无效；如果其余邻居节点的距离向量表发生变化，就通知其他邻居节点，链路错误信息在网络中快速传播；使用毒性反转防止ping-pong回路（无限距离=16跳）

**2、OSPF**（开放最短路优先协议）：LS算法。

① 公开：开放可用；

② 使用LS算法：LS分组分发；每个节点都有一个拓扑图；使用Dijkstra算法

③ 洪泛发往AS中的每个路由节点

④ IS-IS算法：与OSPF几乎相同

⑤ 安全：相互传递信息的路由器必须相互认证；

⑥ 允许多条具有相同链路代价值的链路存在；

⑦ 可以完成广播和多播；

⑧ 可以有层次化的OSPF，在AS内部划分区域

⑨ 报文直接封装在IP报文中

**OSPF路由器的作用分别是什么**：

1. **边界路由器**：连接到其他自治系统，负责向本AS之外的目的地转发分组
2. **区域边界路由器**：负责向本区域之外的目的地转发分组
3. **骨干路由器**：为分组在区域间的转发提供路由选择
4. **普通路由器**：为分组在区域内的转发提供路由选择

II、**自治系统间路由选择协议**：

任务：

① 支持自治系统间的数据递交

② 知道自治系统间的可达信息，并将这些信息传给本自治系统的路由器

③ 有多个路径可以通过不同自治系统到达时，做出选择。

热土豆路由：把分组放到队列长度最短的地方排队

**BGP：边界网关协议 TCP**

**功能：**

① 从相邻的AS出获得子网可达信息

② 向本AS内部的所有的路由器传播这些可达信息

③ 基于可达性信息和AS策略，决定到达子网的好的路由

④ 允许一个子网向因特网其他部分公布它的位置

**会话：**

① 使用半永久性的TCP连接交换路由选择信息

② 每条TCP连接，两端路由器称BGP对等方；发送的BGP报文称BGP会话

③ eBGP：跨越两个AS的BGP会话

④ iBGP：在同一个AS中的两个路由器的会话

**选路方式**

① 管理员策略

② 最短路径

③ 热土豆路由

④ 其他路由

**如何确定其内部路由器配置**：

可以通过RIP、OSPF配置自治系统内部的路由器

**intra-AS与inter-AS有什么区别：**

① intra-AS：管理员需要控制选路方式，关注策略，策略大于性能

② inter-AS：只有一个管理员，关注性能，不需要策略

**如何把一个前缀-表项放入路由表：**

① 路由器知道前缀：

路由器转发表中的一个表项是前缀，分组到达路由器时，按照最长前缀匹配原则路由器找到对应的出口，假设该前缀属于“外部前缀“。要使该前缀进入路由器转发表表项，路由器首先要知道它，通过BGP路由公告，要么eBGP，要么iBGP

② 为前缀决定出口：

知道前缀加入路由表之前需要确定适当的出端口，若路由器接到多个有关该前缀的路由通告

使用BGP路由选择寻找最好的inter-AS路径。

使用OSPF寻找最好的intra-AS路径，从而获得最佳的intra-AS路径

路由器识别最佳路由的路由器端口

③ 把前缀-端口放入路由表

1. **链路状态算法求B节点到所有目的节点的最短路径（必须有节点的收集信息和扩散控制过程），LS算法与DV算法的异同，DV算法的缺点**
2. **收集节点信息**：

所有的节点要将链路状态信息，包括其与邻居节点的连通性和链路代价值传输给其他节点，使得每个节点都拥有整个网络的拓扑结构和链路代价值

① 发现邻居节点并学习它们的网络地址：通过发送hello包的形式

② 测量到达每个开销，发送要对方立即回应的echo包，开销为来回时间/2

③ 将所有学习到的内容封装成一个包，发往每个邻居节点

1. **扩散控制**

扩散过程中需要进行洪泛控制

① 为每个数据包设置TTL，每经过一个路由器TTL值减一，为0后路由器将将其丢弃

② 每个包包含一个序号，每发送新包时加一。分组到达时，若是新的序号，则转发，若重复，则丢弃，若比路由器记载的最大序号小，则认为过时，丢弃

1. **LS算法与DV算法比较**

① 消息复杂度：LS：O(nE)；DV：邻居之间的交换只是收敛时间不同

② 收敛速度：LS：O(n2)；DV：收敛时间变化可能有路由器循环计数到无穷大所致

③ 健壮性：LS：节点可以广播错误的链路开销，每一个节点只计算自己的路由表；DV：每个节点可以广播错误的链路开销，节点以来其他节点计算路由表，可能导致错误蔓延

1. **DV算法缺点**

① 选择路由时，没有考虑线路带宽

② 路由收敛速度慢

1. **解释以太网中CSMA/CD协议工作过程**

① 站点收到网络层递交的分组，封装成帧

② 站点开始监听信道，若信道空闲，则发送帧；若信道忙，则等待直到信道空闲，发送帧

③ 如果站点发送完帧没有检测到冲突，则发送成功

④ 若检测到冲突，停止发送，并发送冲突强化信号

⑤终止后，站点进入指数回退；第m次冲突后，站点随机从{0，1，2，…… 2m-1}中随机选择一个K值，等待K \* 512个比特时间并返回第二步

**多路访问协议：**

**冲突**：节点同时收到两个或更多信号

1. 信道划分
2. 随机访问：允许冲突，然后从冲突中恢复
3. 轮询方式
4. 有限争用协议

**（1）、信道划分方式：**

① TDMA：时分多路访问

将能完整传输一帧的时间划分成若干份，“循环访问信道”，每个站点在每个循环中获得固定长度

② FDMA：频分多路访问：

信道频率划分，为站点分配频率

③ CDMA decode/encode

**（2）随机访问协议：定义了如何检测冲突，从冲突中恢复**

**① 时隙ALOHAI**

I、节点获得新帧，则在下一个时隙进行传输

II、无冲突，节点能够在下一个时隙发送帧

III、有冲突，节点在每个后继时隙以概率P发送帧直到成功

**② 纯时隙ALOHA**

I、帧到达节点，立即传输

**③ I-坚持型CSMA**

I、站点有数据发送，就开始监听信道

II、信道空闲，就发送

III、信道忙，继续监听直到信道空闲

IV、产生冲突，等一随机时间开始发送

**④ 非坚持型CSMA**

I、站点接收到帧，监听信道

II、若信道空闲，就发送帧

III、若信道忙，就随机等待一段时间，再开始发送过程

IV、若产生冲突，就随机等待一段时间，再开始发送过程

**⑤ p-坚持型CSMA**

I、站点接收到数据，先监听信道

II、若信道空闲，则以概率p发送数据，以概率1-p延迟到下一时隙发送；若下一时隙仍空闲，重复此过程，直到数据被发送出去或者信道被占用

III、若信道忙，重新开始发送过程

IV、若有冲突，重新开始发送过程

（3）轮询方式

（4）有限争用协议

将站进行分组，每个竞争时间片只允许某个站的节点进行竞争

每组只有一个站：无冲突协议

所有站在一个组：争用协议

网络负载轻：每组站数多

网络负载重：每组站数少

1. **网络互联中常用哪些主要硬件设备？它们各有什么特点**

**路由器：**

1. 含有网络层、数据链路层、物理层
2. 用来互联网段，实现分组在不同网段之间的递交
3. 关键功能是转发和路由选择

**交换机：**

1. 是数据链路层设备，含有数据链路层、物理层
2. 存储并转发以太网帧
3. 可以隔离冲突
4. 透明，主机意识不到交换机的存在
5. 自主学习，自主生成，即插即用，不需要管理员干预
6. 主机有专属、直接的链路到交换机
7. **交换机ARP表的生成**
8. 初始交换表为空
9. 对于每个接口接收到的帧，交换机在表中存储源MAC地址、到达的接口、当 前时间
10. 一段时间之后，若交换机没有再次收到该地址作为源地址的帧，则从表中删除这个地址
11. **输入[www.google.com](http://www.google.com)，敲下回车发生了什么**

**1、笔记本通过DHCP获得IP地址等信息。**

①主机广播DHCP discover报文。源IP：0.0.0.0；目的IP：255.255.255.255；源IP：自己IP；目的MAC：全F，目的端口：67端口，递交到DHCP服务器相应进程

②DHCP服务器在数据链路层收到广播包，发现目的MAC全F，递交到网络层，网络层发现目的IP为255.255.255.255，递交到传输层67端口，运行DHCP服务，回复DHCP offer报文；源IP：服务器IP；目的IP：255.255.255.255；以广播的形式发送，报文中包含分配的IP、网关、首选DNS、子网掩码、事件号等信息

③笔记本收到DHCP offer广播包，从其中选择一个，发送DHCP request报文，src：0.0.0.0；dest：255.255.255.255，回显配置，确认使用某DHCP服务器使用的配置信息

④DHCP服务器收到DHCP offer广播包之后，回复DHCP ACK，源IP：服务器IP；目的IP：255.255.255.255；证实所要的参数

**2、笔记本获得了IP地址，要开始DNA解析**

① 笔记本配置了本地名称服务器，要发到本地名称服务器，笔记本拿自己的IP和本地名称服务器的IP与子网掩码与一下，发现不在同一网段，因此将信息发往网关

② 笔记本封装一个广播包：src：自己IP；dest：网关IP；src MAC：自己MAC；dest MAC：全F；在包传输过程中，其余主机记录笔记本MAC与IP的对应关系，生成ARP表。如果经过交换机，则交换机记录MAC地址、进来的端口号、时间，生成交换表。网关收到该信息后，回应笔记本；src：网关IP；dest：笔记本IP；src MAC：网关MAC；dest MAC: 笔记本MAC；笔记本由此获得网关MAC，封装查询包，使用UDP发送至网关，src：笔记本IP；dest：本地名称服务器IP；src MAC：笔记本MAC; dest MAC：网关MAC

第一级路由器接收到包以后，拿着目的IP去查询路由表，路由表由OSPF、BGP、管理员共同参与生成。获得下一跳地址，转发到相应出口，依次转发，直到发送到本地名称服务器；

若本地名称服务器中有该域名与IP的对应关系，则返回；若没有，前往负责该域名的权威名称服务器查询，权威名称服务器将域名对应的IP返给本地名称服务器，本地名称服务器再返还给笔记本，笔记本获得[www.google.com对应的IP](http://www.google.com对应的IP)

**3、然后笔记本通过HTTP协议，利用TCP去[www.google.com对应的IP](http://www.google.com对应的IP)去取地址**

① 三次握手过程。笔记本首先发送一个SYN置1的TCP报文信息，自定义序列号；服务器收到该信息后，回复SYN ACK信息，ack：对方报文序号+报文长度；笔记本接收到SYN ACK信号后，发送ACK报文，进行确认，同时发出HTTP GET请求，向服务器请求对象

② 传输过程中，服务器向笔记本通知缓冲区大小，进行流量控制，使笔记本未被确认的分组数据量不超过缓冲区大小

③ 拥塞控制：刚开始发送，TCP处于慢启动阶段，每RTT时间，cwnd=2\*cwnd；若出现超时事件，重新进入慢启动阶段，ssthresh设为出现拥塞时的1/2；出现3个冗余的ACK，执行快速重传，ssthresh=cwnd/2；到达ssthresh，进入拥塞控制阶段

在拥塞控制阶段，加性增乘性减，每RTT时间，拥塞窗口加一，出现３次ACK，ssthrest/=2，快速重传；出现超时现像，进入慢启动；

快速重传：对于引起TCP进入快速恢复的缺失报文段，对收到的每一个缺失报文的ACK，cwnd增加一个MSS，，然后进入拥塞避免阶段；出现超时事件，进入慢启动；出现3次冗余ACK，ssthresh /= 2；

1. 发送方与接收方死锁状态图
2. CRC校验核的生成和检测
3. IP无类别域间地址划分
4. LS