**计算机网络，五层，每章都要考点内容（按黑皮书来讲，注：本复习重点最佳匹配于显平老师，如老师不同，侧重点和考法会有区别）**

**注：只讲重点，由于计网内容很多，会考一些小的、零碎的知识点，这个无法全部兼顾，**

**而且我说的不会考的地方是根据老师和我个人感觉的重点，如果真考了……轻点喷。**

**第一章：要会计算时延（各种时延），还有分组、报文、电路交换的概念（不会考默写），五层模型必背（不同老师要求不同）**

**第二章：对应应用层——**

**邮件解析过程（重点，我们考了一个简答，之后有例题，注：邮件传输不会考SMTP或者POP3），**

**网络应用模型P2P和CS（这个没说会考，但是这是最基本的知识点，必须清楚），**

**DNS的解析过程（我们没考，但是这是重点，递归和迭代）**

**FTP（大概率不考）**

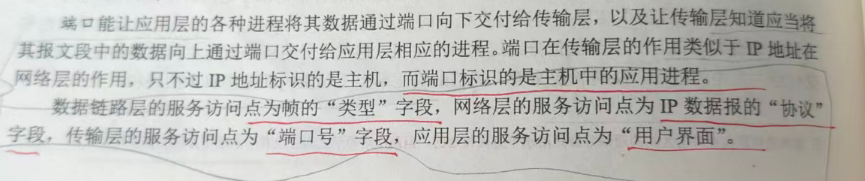
**套接字（可能考这个名词，但不考解释，就是考概念或者填空）和端口号的概念（端口号也就是考，比如FTP端口号是21等等比较重要的端口号，虽然说不考FTP，但是FTP端口号还是要知道点的）**

**HTTP（这个算重点，但是我们没考）**

**第三章：传输层——**

**（第三四章也就是传输层和网络层，我认为王道的计算机网络考研指导这本书讲的挺好的，我不喜欢大段大段的听网课，所以推荐大家去看书，网上买盗版或者电子版的应该也不贵，注：这是我根据个人感受觉得这两章更适合应试）**

**一个基本的知识如下：**



**要清楚哪些是使用UDP、哪些使用TCP、哪些使用IP（虽然IP不在传输层）**

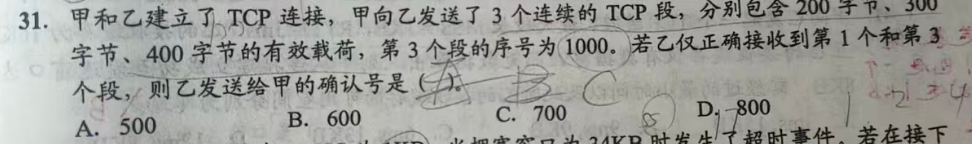
**UDP的内容（注：UDP的格式等，理论上来说不会考那么细，但是还是建议大家都去看一下，看完你能感觉出来哪些是重点、哪些不是，然后重点记忆，比如TCP有首部20B的开销，UDP有8B的开销，还有TCP有伪首部等等，这些在王道的书里都有的，传输层和网络层这两章要好好看，不只是为了期末考试，看完你绝对会对计网有更深的理解的）**

**UDP的校验和的计算（算重点，但我们没考，不代表后来人不会考）**

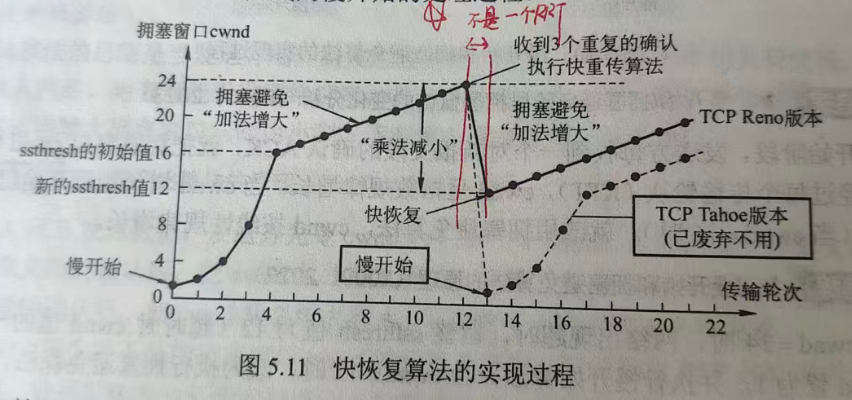
**TCP（重中之重，**

**1、和UDP一样，理解清楚格式**

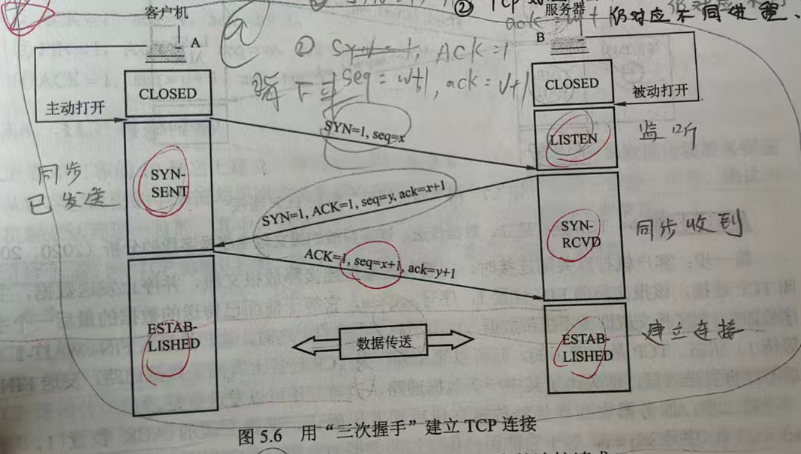
**2.TCP三次握手、四次挥手，毫无疑问，一定要背，一字不落！！！！（可考大题，可考小题，小题可以看王道后面的简答练习题，我们考了小题，如下）**



**3.慢开始、拥塞避免、快重传、快恢复（这个我们考了大题，就是下面这个图，当然你不能只背图，要理解））**



**注：有的同学可能会问王道上的题都要做吗？我的建议是做基础题，它分为基础和考研题，按于老师的话来说“考试希望大家去学知识，并不是以考倒大家为目的”，时间不够，跳着做**



**四次挥手我就不放了，大家自己去看书**

**第四章：网络层——分为路由选择和分组转发**

**SDN的内容看一下吧（我们考了SDN的优缺点，答至少三条，不过，显然，这种题目一般不会重复，但也说不定呢）**

**IPV4基本内容全看，大题或者小题考（比如什么是默认路由、第一个和最后一个对应的是网络本身和广播地址）**

**IP数据报的分片（必考，自己看）**

**IPv4:ABC类地址，必看，这是基本概念，可能不会明考，但是一定会以这个为基础去考**

**NAT原理要懂，我后面有简答题，大家最好理解着背一下（我们考了简答，注：什么是理解着背？计网这门课很难，所以很多老师为了让学生过就考一些文字描述类的简答题，尽量答到点上给分，但是这种题考的很灵活，我给的也就是个示例，你不理解这个原理我很容易让你背了也拿不到分或者拿不满分）**

**划分子网和路由聚合（可大可小，必考）**

**CIDR（可大可小，网络规划必考）划分子网、路由聚合、CIDR会做题就行，不会考原理**

**ARP地址解析协议（原理要懂，会考简答）**

**DHCP（原理要懂，可考简答可考选填）**

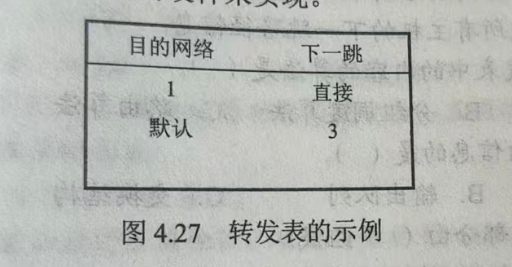
**ICMP（不用背协议内容，知道是什么就行，还有就是PING命令用的就是这个但是ping工作在应用层，而tracert工作在网络层）**

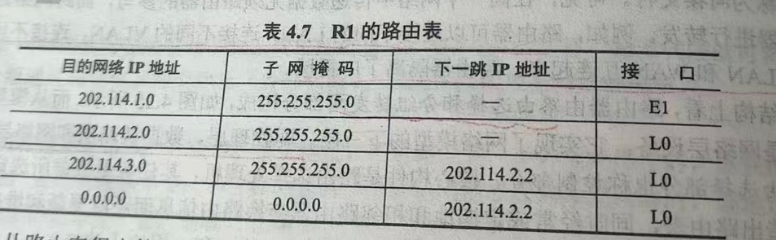
**IPV6大概看一下就行（我们考了简答还是选填：IPV6在哪些方面提高了路由转发效率，也就是IPV6相比IPv4的优点，背三条就行，不过感觉也不会再考这个了）**

**路由算法（RIP、OSPF、BGP，原理要懂，考试大概率会把OSPF作为最后一个压轴题，就是考应用和计算，我们是这样的，说白了就是迪杰斯特拉算法，嗯。。。还是要看是哪个专业哪个老师，计科中外我听说好像还考了伪代码，普通专业应该不会，于老师更不会，除非明说要考）**

**IGMP不考**

**有学生问路由表和转发表的格式，我觉得问的很好，因为我考试的时候最后一个OSPF要写路由表还是转发表，我不清楚格式是什么，估计有扣分，还有迪杰斯特拉算法要划哪个图，最好也看一下表格怎么划的，格式方面**





**格式可能会有区别：但是目的网络和下一跳一定要记住**

**数据链路层——最重要的概念就是帧**

**数据链路层的三个基本功能：封装成帧、流量控制、差错检验**

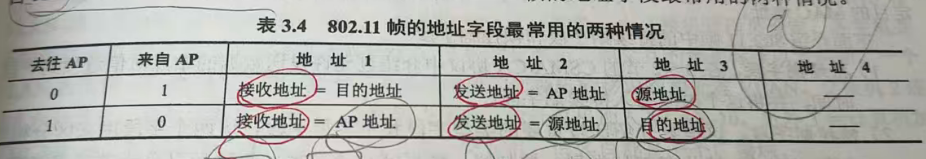
**检错编码（奇偶校验、循环冗余，是个重点，但是我们没考）**

**流量控制与滑动窗口机制，黑皮书应该在TCP那里讲的，但其实数据链路层也有应用，这些内容还是看一下吧，万一考呢，不过我们没考，比如：选择重传、后退N帧、停止等待**

**戒指控制访问，看一下就行了，不是重点，但是一定会考，就一个选择或者填空，我们考了一个名词（填空），我忘了是ALOHA还是CSMA/CD了，但就一个填空而已，不要就不要了，先看重点**

**二进制指数退避算法，我们考了一个很简单的选择，虽然当时我没看到，不过蒙对了**

**802.11数据帧的前三个地址的含义，这是一个重点，在选填里考，不过我那份题没考，应该是在补考的卷子里考了**



**Vlan要理解原理，可能会考配置命令，因为这是实验课的一个重点，我那套题没考，可能在补考里面了，一定要会，注意：我们实验用的是H3C的设备，别网上直接找一段华为的设备命令去背**

**一个琐碎的知识点（也算是重点）：数据帧的类型字段，比如vlan 0x8100,还有其他的重点类型字段，我忘记了，大家可以去查一下**

**以太网交换机自学习功能是指什么？要会**

**此外可能会考一种比较综合的简答题，具体后面看，就是发送一个帧要经历的过程**

**物理（只考概念题，就是物理层的作用，不考其他，如果考的话，当我没说，印象里物理层可以单独拿出来做一门课——数字通信原理，所以我认为不是重点也不会怎么考）**

**网络安全（一简答、一个填空，加密解密的流程，填空具体我忘了，简答就考一道，后面我会说的）**

**以上内容是我考完之后整理的，下面看一下我考前整理的内容，会提到到上面说的一些简答题。注意：还是那句话，文字描述类的简答题你要清楚整个原理，只背下我下面的内容没有任意意义，你有可能连题目问你什么都搞不清楚。**

**设计子网一定要考虑路由接口啊！！！！**

简答（6分）**WIFI链路层帧到路由器的转换过程（应该和ARP在一个题中）**

1.Wi-Fi链路层帧的发送

源设备将数据封装为 802.11帧，包含以下关键字段：

**MAC头部**：源MAC、目的MAC **帧类型：**数据帧。

**帧主体**：携带上层的数据。 **FCS**

2. 无线接入点的接收与转换

当无线信号到达路由器的Wi-Fi接口时，路由器作为接入点执行以下操作：

（1）解密与验证

如果Wi-Fi启用了加密，路由器首先解密802.11帧的载荷，并验证帧完整性。

（2）解封装802.11帧

路由器剥离802.11的MAC头部和尾部，提取出内部的IP数据包。

（3）MAC地址转换

如果目的IP不在本地网络，路由器会将目的MAC替换为下一跳的MAC。

源MAC替换为路由器有线接口的MAC。

（4）重新封装为以太网帧

路由器将IP数据包封装为以太网帧，通过有线接口转发。

简答（6分）

DNS还提供负载均衡的服务

**权威域名服务器的记录类型：**DNS，权威域名服务器，数据库记录类型 考自己在公司的数据库里加什么信息，第一个……第二个value，第三个……，

|  |  |  |  |
| --- | --- | --- | --- |
| 记录类型 | 名称（Name） | Value（值） | 作用 |
| A | www.example.com | 192.0.2.1 | 将域名解析为IPv4地址。 |
| CNAME | mail.example.com | server1.example.com | 别名记录，指向另一个域名。 |
| MX | example.com | 10 mail.example.com | 邮件服务器记录（优先级+域名）。 |
| NS | example.com | ns1.example-dns.com | 指定该域名的权威DNS服务器。 |

如果题目问“如何配置公司邮件服务器”，你需要填写：

记录类型：MX

名称（Name）：example.com（通常留空或写@表示根域名）

Value：10 mail.example.com 10是优先级；mail.example.com是邮件服务器域名

**邮件（MX记录）的解析过程：**写出来之后问发个邮件的解析过程是什么，先解析出邮件服务器的名字，再解析出.....

当用户发送邮件（如发送到user@example.com）时，DNS解析流程如下：

1. 解析邮件服务器的域名（MX 记录查询）

发送方通过“dig MX example.com”查询example.com的MX记录，得到example.com 的邮件服务器是 mail.example.com（优先级 10）。

2. 解析邮件服务器的 IP 地址

发送方通过“dig A mail.example.com”查询 mail.example.com 的 A 记录（IPv4），获取 mail.example.com 的 IP 地址，以便建立 SMTP 连接。

3. 建立 SMTP 连接并发送邮件

发送方与 192.0.2.1 建立 TCP 连接，使用 SMTP 协议传输邮件内容，将邮件传递到 example.com 的邮件服务器。

4. 反向验证

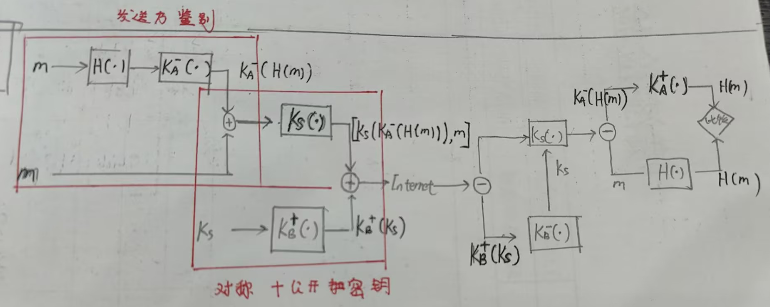
为防止伪造邮件，接收方可以选择检查以下记录“dig TXT example.com”

简答（6分） **安全技术方案**

数字签名：用于发送方鉴别

散列函数MD5：用于报文完整性

公开密钥（RSA）和对称密钥（AES）：用于机密性



发送方：

①A 对他要发送的报文m应用一个散列函数MD5 H（），从而得到一个报文摘要；

②采用公开密钥（RSA），用她的私钥*KA*−对散列函数的结果进行签名，从而得到一个数字签名；

③把初始报文和该数字签名级联起来生成一个包；

④选择AES随机对称会话密钥*KS*​加密级联生成的包；

⑤用B的公钥*KB*+​加密这个对称密钥；

⑥级联加密的包和加密的对称密钥再形成一个包；

⑦向 B 的电子邮件发送这个包。

**接收方**：

①使用其私钥*KB*−​得到对称密钥*KS*​；

②使用对称密钥*KS*​解密加密的包，得到*KA*−​(*H*(*m*))和报文 m；

③将 A 的公钥*KA*+​应用到被签名的报文摘要上；

④将③操作得到的H(m)与B对该报文的散列H进行比较，若两个结果相同，则B完全可以确信这个报文来自A且未被篡改 。

简答（6分） **TCP的五层协议（老师要求的是区分本质区别）**

**应用层：**直接面向用户或应用程序，提供特定服务，如电子邮件、文件传输、远程登录等（这三个都用的TCP）。

协议定义：规定应用数据的格式和交互规则（如HTTP请求）。

服务实现：支持具体功能（如DNS域名解析、SMTP邮件发送)

用户接口：为软件提供网络访问的API。

**传输层：**提供端到端（主机中的进程到主机中的进程）的可靠或不可靠数据传输，通过端口号区分不同应用。

可靠传输：TCP通过确认、重传、流量控制保证数据无差错、不丢失、按序到达。

不可靠传输：UDP提供低延迟、无连接的服务，适用于实时应用。

复用与分用：通过端口号区分同一主机上的不同应用。

拥塞控制：TCP通过慢启动、拥塞避免等算法适应网络状况。

**网络层：**实现主机到主机的通信，通过逻辑地址跨网络路由数据。

路由选择：决定数据包从源到目的的最佳路径（如OSPF、BGP）。

分组转发：将数据封装为IP数据报，处理分片与重组。

逻辑寻址：使用IP地址标识主机和网络。

拥塞控制：通过ICMP源抑制报文避免网络过载。

**数据链路层：**在直接相连的节点间提供可靠的数据传输，处理物理地址

成帧：将比特流组织为帧，添加头部（源/目的MAC地址）和尾部（校验和）。

差错控制：通过CRC校验检测物理层的传输错误。

流量控制：通过ARQ等协议协调发送方与接收方的速率。

介质访间控制：通过如：以太网的CSMA/CD等解决共享信道中的冲突。

**物理层：**唯一直接与物理媒介交互的层。

传输原始比特流

定义电气、机械、时序等物理特性

简答 **DHCP动态主机配置协议**

连接到互联网的计算机需要配置的项目包括：①IP 地址，②子网掩码，③默认路由器的IP地址（默认网关），④域名服务器的IP地址。

**交互过程四个阶段（背！！！）：**

DHCP发现：DHCP 客户广播 **“DHCP 发现”** 消息，试图找到网络中的 DHCP 服务器，以便从DHCP服务器获得一个IP地址。源地址为 0.0.0.0，目的地址为 255.255.255.255。

DHCP提供：DHCP 服务器收到 “DHCP 发现” 消息后，广播 “DHCP 提供” 消息，其中包括提供给 DHCP 客户机的 IP 地址。源地址为 DHCP 服务器地址，目的地址为 255.255.255.255。

DHCP请求：DHCP 客户收到 “DHCP 提供” 消息后，若接受该 IP 地址，则广播 “DHCP 请求” 消息向 DHCP 服务器请求提供IP地址。源地址为 0.0.0.0，目的地址为 255.255.255.255。

DHCP ACK：DHCP 服务器广播 “DHCP 确认” 消息，将 IP 地址分配给 DHCP 客户。源地址为 DHCP 服务器地址，目的地址为 255.255.255.255。

简答 **网络地址转换NA**T

私有IP地址需通过NAT访问公网。私有IP地址要记！！！

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| 类别 | 地址范围 | | | 子网掩码 | |
| A类 | 10.0.0.0/8 相当于1个A类网络  10.0.0.0 – 10.255.255.255 | | | 255.0.0.0 (/8) | |
| B类 | 172.16.0.0/12 相当于16个连续的B类网络  **172.16**.0.0–172.31.255.255 | | | 255.240.0.0 (/12) | |
| C类 | **192.168.0.**0/16相当于256个连续的C类网络  192.168.0.0 – 192.168.255.255 | | | 255.255.0.0 (/16) | |
| 网络类型 | | 网络号 | 最大可用网络 | | 最大可用主机 | |
| A（0+网络号） | | 1-126 | 27-2 | | 234-2 | |
| B（10+网络号） | | 128.0-191.255 | 214 | | 216-2 | |
| C（110+网络号） | | 192.0.0-233.255.255 | 221 | | 28-2 | |

则D类为（1110+网络号）

（1）主机号全为0表示本网络，主机号全为1表示本网络的广播地址，这两类地址一般不指派。（**很容易出网络号为给定位数，然后主机号全为1的ip地址迷惑**）

（2）127.×.×.× 保留作为环回地址的IP数据报发送到任何网络。不会将**目的地址为环回地址（127..）**的IP数据报发送到任何网络。

（3）路由器不会转发255.255.255.255、也不会转发目的地址是私有地址的数据报。

在互联网中，所有路由器对目的地址是私有的数据报一律不转发。

NAT的工作原理如下：要记！！！（更新与端口号和IP地址有关）

以某家庭办理10Mb/s电信宽带，获得全球IP地址（如138.76.29.7），家庭网络内3台主机使用私有地址（如10.0.0.0网段），家庭网关路由器开启NAT功能为例，NAT路由器工作原理如下：

**用户主机发起请求：**假设用户主机 10.0.0.1（随机端口3345）向 Web 服务器 128.119.40.186（端口 80 ）发送请求 。

**NAT 路由器处理outgoing分组：**

NAT 路由器收到IP分组后，为该IP分组生成一个新端口号 5001，将 IP 分组的源地址改为 138.76.29.7（NAT 路由器的全球IP地址），将源端口号改为5001。

NAT 路由器在 NAT 转换表中增加一个表项，可能包含 {LAN 端: 10.0.0.1:3345 ；WAN 端: 138.76.29.7:5001} 。

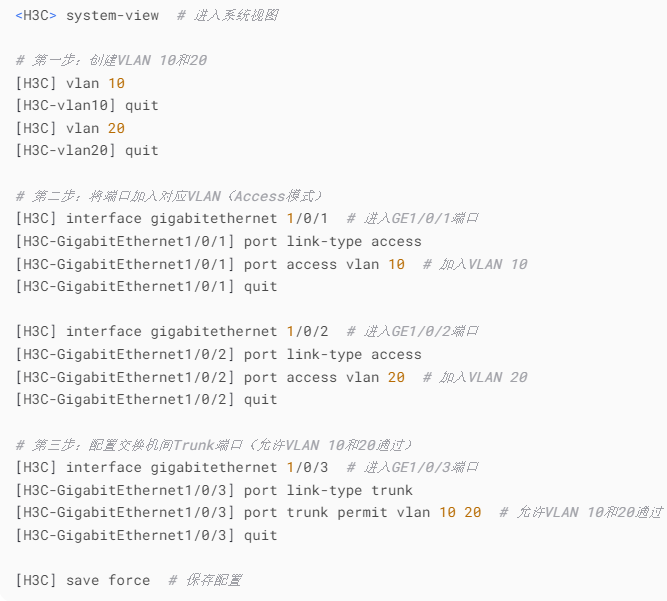
**Web 服务器响应：**Web 服务器响应的 IP 分组的目的地址是 NAT 路由器的全球 IP 地址 138.76.29.7，目的端口号是 5001 。

**NAT路由器处理incoming响应分组**：响应分组到达 NAT 路由器后，通过 NAT 转换表将 IP 分组的目的 IP 改为 10.0.0.1，将目的端口号改为 3345 ，再转发给内网中的用户主机。

这样，只需要一个全球 IP 地址，就可让多台主机同时访问互联网。

简答（6分） **vlan的配置 帧转发流程**





帧转发示例：PC1 给PC3发送帧.

**步骤 1：PC1 发送帧**

源：PC1（VLAN 10） 目的：PC3（VLAN 10）

帧内容：

源 MAC：PC1 的 MAC 目的 MAC：PC3 的 MAC 无 VLAN 标签（Untagged）。

**步骤 2：LSW1交换机接收帧（Access 端口处理）**

端口 GE 0/0/1 是 Access 端口，属于 VLAN 10。

交换机接收 Untagged 帧。根据端口配置，打上 VLAN 10 的标签。查询MAC地址表，确认目标 MAC（PC3）在哪个端口。

**步骤 3：LSW1 转发帧（Trunk 端口处理）**

如果 PC3 的 MAC 地址在 LSW1 的 MAC 表中，且对应端口是 GE 0/0/3（Trunk端口），则：检查 Trunk 端口允许的 VLAN（VLAN 10 和 20）。

VLAN 10 在允许列表中，保留 VLAN 标签（Tagged 帧）并通过 Trunk 端口转发。

**步骤 4：LSW2 接收帧（Trunk 端口处理）**

交换机读取 VLAN 标签（VLAN 10）。

查询 MAC 地址表，确认目标 MAC（PC3）在 GE 0/0/1（Access 端口，VLAN 10）。

**步骤 5：LSW2 转发帧（Access 端口处理）**

**端口 GE 0/0/1** 是 Access 端口，属于 VLAN 10。

移除 VLAN 标签（Untagged 帧）。将帧发送给 PC3。

简答6分 **一个网络里发一个IP数据报到另一个子网中给出原理过程（使用到ARP协议）**

**问题描述：在一个网络中，主机A（IP: 192.168.1.2）要向另一个子网中的主机B（IP: 192.168.2.3）发送一个IP数据报，说明传输过程（需包含ARP协议的作用）。**

**1. 判断目标是否在同一子网**

主机A通过 **子网掩码** 判断目标IP 192.168.2.3 是否在同一子网，若不在同一个子网，数据需通过网关转发。

**2. 主机A通过ARP获取网关MAC地址**

ARP请求：主机A**广播**询问 **网关**192.168.1.1 的MAC地址

ARP响应：网关**单播**回复其MAC地址。

**3. 封装IP数据报和以太网帧**

主机A构建：

IP层：源IP: 192.168.1.2，目的IP: 192.168.2.3

链路层：源MAC: A的MAC 目的MAC: 网关的MAC 00-11-22-33-44-55

**4. 网关（路由器）处理数据报**

**解封装**：网关收到帧后，发现目的MAC是自己，剥离以太网头部，检查目的IP 192.168.2.3。

**路由查询：**网关根据路由表，找到 192.168.2.0/24 的子网出口（接口IP 192.168.2.1）。

**转发准备：**

若网关无主机B的MAC，则通过ARP请求，广播询问获取192.168.2.3的MAC（过程同步骤2）。

**重新封装：**

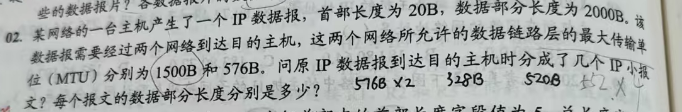
IP层：源/目的IP不变

链路层：源MAC: 网关的MAC地址。目的MAC: 主机B的MAC地址。

**5. 主机B接收数据报**

主机B检查帧的目的MAC是否匹配，匹配则接收并解封装，将IP数据报传递给上层协议。

简答中的一小问6分 **IP数据报的分片可难可简单，要注意两个网络的话要分别给出**

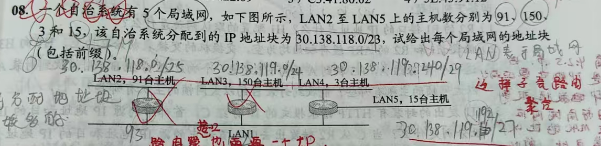




**网络聚合后，要看清楚尾号！！！**



**路由器也需要一个接口！！！**



综合10分 **OSPF**

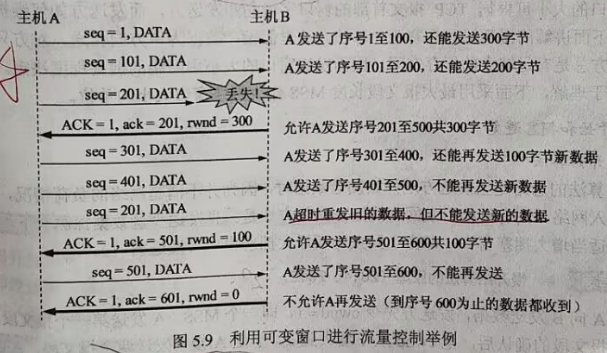
考迪杰斯特拉算法，这个看书上的内容。之后补上

简答（6分） **TCP的拥塞控制**

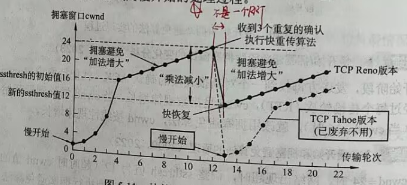
**拥塞控制**

TCP使用滑动窗口机制。接受方维护接收窗口rwnd，发送方拥塞窗口cwnd

**发送窗口的上限值= min[rwnd，cwnd]**



拥塞控制四种算法：**慢开始、拥塞避免、快重传和快恢复**。



**慢开始**2n，增大拥塞窗口，注意发送窗口的上限值= min[rwnd，cwnd]

若慢开始阶段2cwnd>ssthresh，则下一个RTT后的cwnd=ssthresh，而非2cwnd

**拥塞避免:**在cwnd达到ssthresh之后，线性增长，每经过一个RTT把cwnd增加1。

当出现拥塞的时候，则把ssthresh的值设定为cwnd/2.然后从1开始重新执行慢开始算法。

**快重传：**使发送方尽早进行重传，而不等超时计时器超时再重传。发送方一旦收到连续的3个冗余ACK，就立即重传相应报文段。

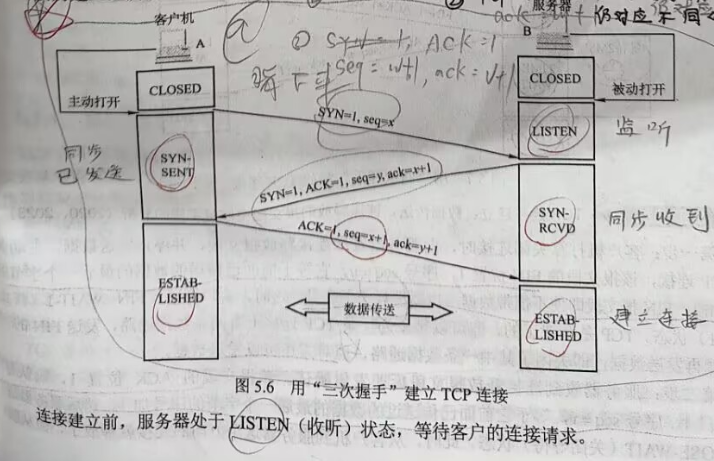
**快恢复：**当发送方收到3个冗余ACK后，把慢开始门限ssthresh调整为当前cwnd的一半，cwnd的值从更新后的ssthresh开始，启动拥塞避免算法线性增长。

总结：网络出现超时时，采用慢开始和拥塞避免算法（ssthresh=cwnd/2，cwnd=1）

收到3个冗余ACK时，采用快重传和快恢复（ssthresh=cwnd/2，cwnd=ssthresh）

注意：**当题目出现rwnd和cwnd，一定要记得，发送窗口的上限值= min[rwnd，cwnd]，选择较小那个。容易挖坑！！！**

**三次握手（c/s模型，必考！！！）：**

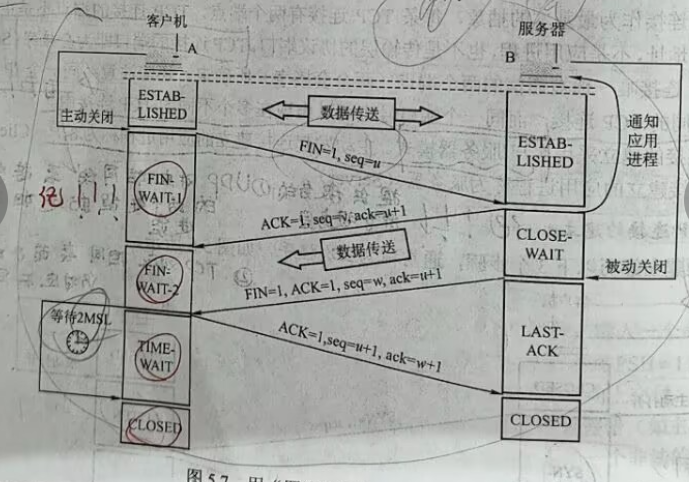


左边一列：SYN-SENT 右边一列：LISTEN SYN-RCVD

左边一列：FIN-WAIT1 FIN-WAIT2 TIME-WAIT 右边一列：CLOSE-WAIT LAST-ACK

三次握手，第一步和第二步不能携带数据，但要消耗一个序号。

四次挥手：



FIN=1，seq=u

ACK=1，seq=v，ack=u+1

FIN=1，ACK=1，seq=w，ack=u+1

ACK=1,seq=u+1,ack=w+1

第四步：ACK=1，ack=w+1，seq=u+1，经过时间等待计时器2MSL，

客户机释放的最短时间为；1RTT+2MSL，服务器释放的最短时间为1.5RTT。

**网络安全(填空1 简答1)**

填空可能：PGP（用于安全电子邮件）、TLS（用于使TCP）和IPsec（用于使网络层）

Rip 应用层 UDP OSPF 网络层 IP BGP 应用层 TCP

DHCP常用于给主机动态地分配 IP 地址，**应用层协议**，**基于UDP**，使用**cs**模型。

BGP**外部网关协议**（EGP），用于不同**自治系统**交换路由信息。**路径矢量协议、基于TCP**

ARP工作在**网络层**，NAT工作在**传输层**。重点就是MAC地址要一直随路由器变，请求是**多播**（因为ARP缓存中没有记录），响应是**单播**。（**背下简答题就可以了！！！**）

**ICMP的应用**，PING命令（应用层，测试两台主机间的连通性）和Traceroute（Tracert，工作在网络层，用来跟踪分组经过的路由）。Ping使用了ICMP回送请求和回答报文，Traceroute使用了ICMP时间超过报文。

**TCP应用：**FTP（文件传输协议）、HTTP（超文本传输协议，https使用TLS加密）、远程登录（TELENT）

**UDP应用：**DNS（域名解析）、DHCP（动态主机配置协议）、RIP（路由信息协议）、IGMP

选填**网络层和链路层协议靠什么区分上层  tcp，UDP靠端口号   IP好像靠type类型**

**传输层**靠**端口号**区分上层协议

**网络层靠协议号**，IPv4 头部中的 8位协议字段标识上层协议。6 → TCP 17 → UDP

1 → ICMP

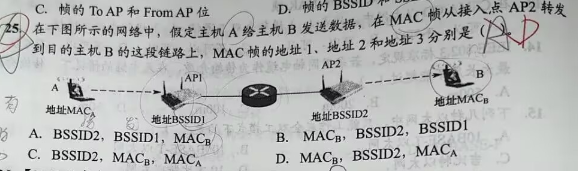
**链路层**（以太网/Wi-Fi）靠Type类型。

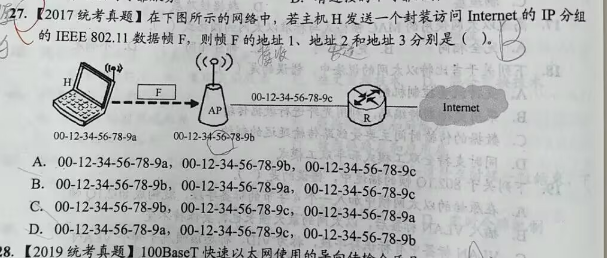
IPv4 0x0800 ARP 0x0806 IPv6 0x86DD IEEE 802.1Q VLAN标签 0x8100

**选择（2分）**一定要搞清楚传播时延、传输时延那些时延，要会区分

选择（2分） **IEEE802.11帧的三个地址字段怎么填**







接收地址 发送地址 （源或目的地址）， 源地址、接入点地址、目的地址（不可能出现两个路由器地址，一定有源主机和目的主机的地址）

填（1分） **存储交换对比电路交换，为什么存储交换更适合？**

存储交换（分组交换）能高效处理**突发性数据流量**，而电路交换固定占用资源，灵活性差。

填简（1分）**SDN对比传统技术的优点**

集中控制，全局统一管理，优化网络性能。

控制与转发分离，功能更灵活。

硬件与软件解耦，降低成本。

填(1分) **IPV6在哪些方面提高路由转发效率？**

取消了主校验和字段

流标签支持快速转发

IPv6 只有源主机才能分片，是端到端的

支持层次化编址

选填 **电话线上网（拨号接入）的核心特**征

电话线本身传输的是模拟信号，而非直接传输数字数据。

看到“电话线上网”模拟信号。若题目提到ADSL/光纤：则属于数字传输，。

选填2分**中间路由器（电路交换，分组交换）给两个计算机传信息，电话线接入，数字线接入的特征**

选填**为什么冲突了要等待一段时间发送，短帧间间隔CSMA/CA（填空）（1分）**

冲突后等待一段时间再发送是为了**让冲突的节点随机退避，避免再次同时发送**。

**短帧间间隔**的作用是为高优先级帧预留信道，确保有序传输。

选填（2分） **无线链路和网络特征的关键因素**

“无线链路和网络性能的关键影响因素是**信号衰减、多径效应和同频干扰**。无线链路的关键问题与**有线干扰无关**

**数据链路层和传输层地滑动窗口的区别：**（**容易跨考**）

数据链路层控制地流量是相邻节点，传输层是端到端。

数据链路层地控制手段是**接收方收不下就不返回确认**，传输层的控制手段是**接收方通过确认报文段中的窗口值来调整发送方的发送窗口**。

选填（2分） **BGP 与交换机自学习**

9.**交换机自我学习**是**记录帧的源MAC地址与该帧进入交换机的接口号（输入端口）**。

10.负载均衡（名词考）

选填（2分）TCP的拥塞控制常被称为“**加性增，乘性减**”

1.网络层提供的服务可以分为：**面向连接的虚电路服务**和**无连接的数据报服务**。

2.虚电路，采用**分组交换技术**

与电路交换类似，整个通信过程分为三个阶段：**虚电路建立、数据传输与虚电路释放**。

**分组的首部仅在连接建立时使用完整的目的地址**，之后每个分组的首部只需**携带这条虚电路的编号**即可。

虚电路提供了**可靠**通信，能保证每个分组正确且有序到达。还可对两个端点的**流量进行控制**。

**多站点同时发送不会冲突**。

数据报 采用**存储转发**技术，会有一定的时延。不一定按顺序到达，

3.SDN**集中式的控制平面**和**分布式的数据平面**

**5.IPv4（重点）**IP数据报首部长20B。

**首部长度（单位4B）总长度（单位1B）片偏移（单位8B）必考**

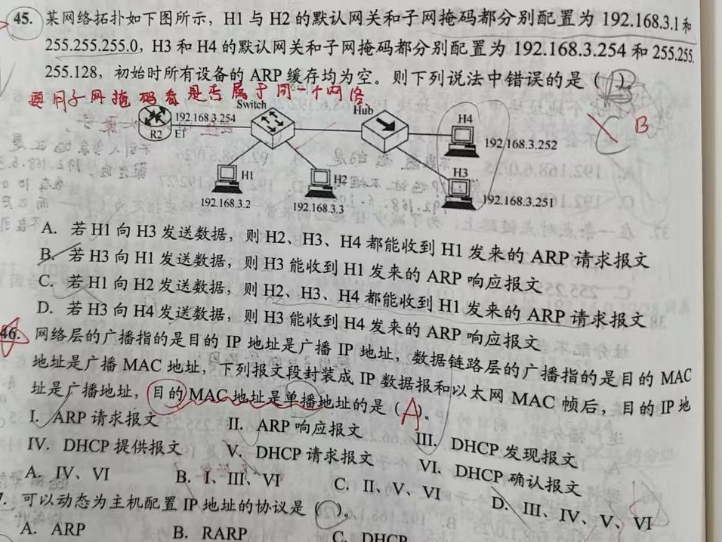
**首部检验和**，IP只检查数据报的首部，不检查数据部分。每个路由器都要重新计算首部检验和。TCP、UDP要检查全部，而且要添加**伪首部**，作用只为了进行校验和。

（3）CIDR**无分类编制**

CIDR网络前缀越短，地址块包含的地址数越多。路由聚合，最短匹配。查询转发表，最长前缀匹配。

默认路由。只要目的网络是其他网络(不在转发表中)，一律选择默认路由。

**ARP还有一个可能出的选择题**



路由器互联多个网络，不仅有多个IP地址，还有多个硬件地址。

**数据链路层和传输层地滑动窗口的区别：**（**容易跨考**）

数据链路层控制地流量是相邻节点，传输层是端到端。

数据链路层地控制手段是**接收方收不下就不返回确认**，传输层的控制手段是**接收方通过确认报文段中的窗口值来调整发送方的发送窗口**。

数据链路层的滑动窗口协议中，窗口大小是固定的，与传输层不同。

**9.ICMP网际控制报文协议**（**必考！！！**）

**ICMP**被封装在IP数据报中发送。**ICMP差错报告报文和ICMP询问报文**。

当终点在预先规定的时间内不能收到一个数据报的全部数据报片时，要把已经收到的都丢弃，并向源点发送时间超过报文。

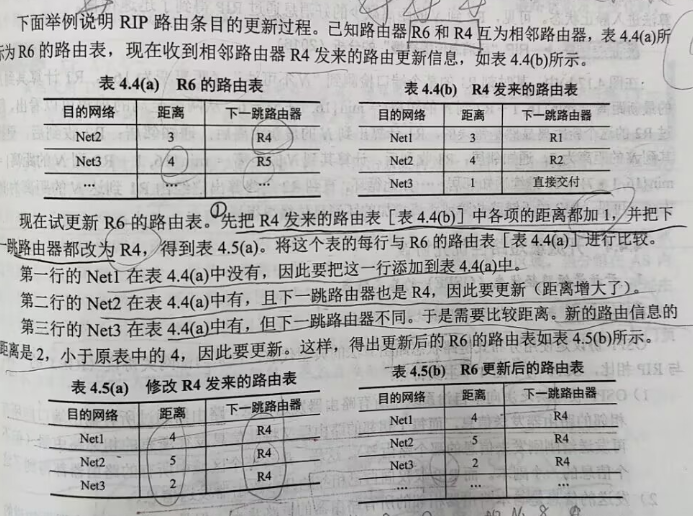
对ICMP差错报告报文、第一个分片的后面所有数据报片、具有多播地址的数据报、特殊地址（如：127.0.0.0或0.0.0.0）都不发送ICMP差错报告报文。

动态路由算法：距离-向量路由算法（ford算法，会操作，第x行y列不动，更新其余单元格）和链路状态路由算法（**迪杰斯特拉，考试必考**）

（注：OSPF只交换部分信息，BGP第一次交换路由表，后面交换部分信息）

**1.RIP（路由信息协议**使用跳数衡量到达目的网络的距离，目的使跳数最少。一条路径最多包含15个，因此距离为16时不可达，可能出现环路，所以规定最高跳数，减少网络拥塞。

**3.RIP收敛过程：**



（1）.先把R4发过来的路由表距离qu全部加1，并把路由表中的路由器改为R4.然后看目的网络：（注意：非常有可能出难题选择）

Net1在R6中不存在，所以要加上该信息。

Net2存在，且下一跳路由器相同，所以更新距离。（可能更新变大，也可能变小）

Net3存在，但下一跳路由器不同，新的距离比原来小，所以更新，若比原来大，则不更新。

**RIP的优缺点：**

优点：实现简单、开销小、收敛过程快。“**好消息传得快”**（路由器发现了更短的路由，更新信息就传播的快）

缺点：网络规模有限，交换信息表（随规模增加，开销变大），**坏消息传的慢**（网络出现故障，需要较长时间才能收敛）

OSPF使用**洪泛法**向AS中的**所有路由器**发送信息，每个相邻的路由器又将此信息发往所有相邻路由器中。RIP仅仅向自己相邻的路由器发送路由表。OSPF更新收敛快，不会出现RIP那种“坏消息传的慢”。

5.OSPF若到同一个目的网络有多条相同代价的路径，则可将通信量分配给这几条路径（**负载均衡，很有可能考填空！！！**）。

6.OSPF虽然使用了迪杰斯特拉算法，但路由表中不会存储完整路径，只存储“下一跳”。

7.OSPF划分AS的好处，把利用洪泛法交换信息局限在区域中，而不是整个AS，从而减少了整个网络的通信量。

8.**BGP**（BGP最后返回的也是一条路径，不是下一跳） **BGP不仅运行在AS之间，还运行在AS内部**

BGP只能是力求找到一条能够到达目的网络的且比较好的路由，并非最优路径。

BGP路由=<CIDR前缀，BGP属性> BGP最重要的两个属性是AS-PATH（自治系统路径）和NEXT-HOP（下一跳）

BGP路由选择 （1）本地偏好值最高的路由 （2）选择AS跳数最少的路由 （3）热土豆算法（选择最靠近NEXT-HOP路由器的路由，让分组经过最少的转发次数离开本AS）（4）选择BGP标识符数值最小的路由

BGP首次交换整个路由表，非首次交换有变化的部分。

**传输层（选填2 简答2）**

**2.标识**

**IP地址**标识的是**主机**，而**端口**标识的是主机中的**应用进程**。

**数据链路层**的服务访问点为帧的**“类型”**字段，**网络层**的服务访问点为IP数据报的**“协议”**字段，**传输层**的服务访问点为“**端口号**”字段，**应用层**的服务访问点为**“用户界面**”。

**3.套接字（名词很重要，很容易考）**

套接字（Socket）=（IP地址：端口号）

UDP相同套接字是同一进程，TCP相同套接字对应不通过进程。

**4.TCP和UDP的应用**（**肯定会有选择题**）

TCP全双工。UDP仅在IP层之上提供两个附加服务，**多路复用**和**对数据的错误检验**。

**5.IP数据报和UDP数据报的区别：**

IP数据报在网络层要经过路由器的存储转发；而UDP数据报封装成IP数据报在网络层传输时，UDP数据报的信息对路由器是不可见的。

**6.UDP**

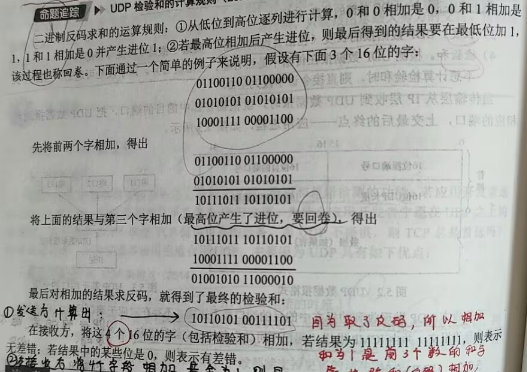
UDP首部8B，TCP有20B

**7.TCP**

UDP的报文长度由发送应用进程决定，TCP报文长度根据**接收方给出的窗口值**和**当前网络拥塞程度**决定。

检验和：

**二进制反码求和运算再取反。**



**8.TCP序号和确认号**（**必考选择**！！！）

TCP默认**累积确认**，只确认数据流中至第一个丢失字节为止的字节，从而减小开销。

TCP重传，两个原因：**超时**或**冗余ACK**（3个冗余ACK，**快速重传**）

多路访问链路和协议：PPP（点对点协议）和HDLC（高级数据链路控制）

信道划分协议：TDM（时分多路复用）、FDM（频分多路复用）、CDMA（码分多址）

有线普遍使用CSMA/CD协议，无线使用CSMA/CA协议。（有线是D，无线是A）

3.适配器的MAC地址具有**扁平**结构，与**层次**结构相反。

**停止等待协议：发送窗口WT=1，接收窗口WR=1**

**后退N帧协议：WT>1,WR=1**

**选择重传协议：WT>1,WR>1**

**可靠传输机制**：确认和超时重传，

ARQ协议包括：S-W协议、GBN协议、SR协议。

GBN允许**累积确认**，不一定发一个回一个，但只要回一个，前面的就都没问题。

SR不允许累积确认，逐一确认。一旦检测到数据出错，就立即发送一个**NAK否定帧**，要求**立即重传**。

连续ARQ（GBN、SR）采用**流水线传输**。

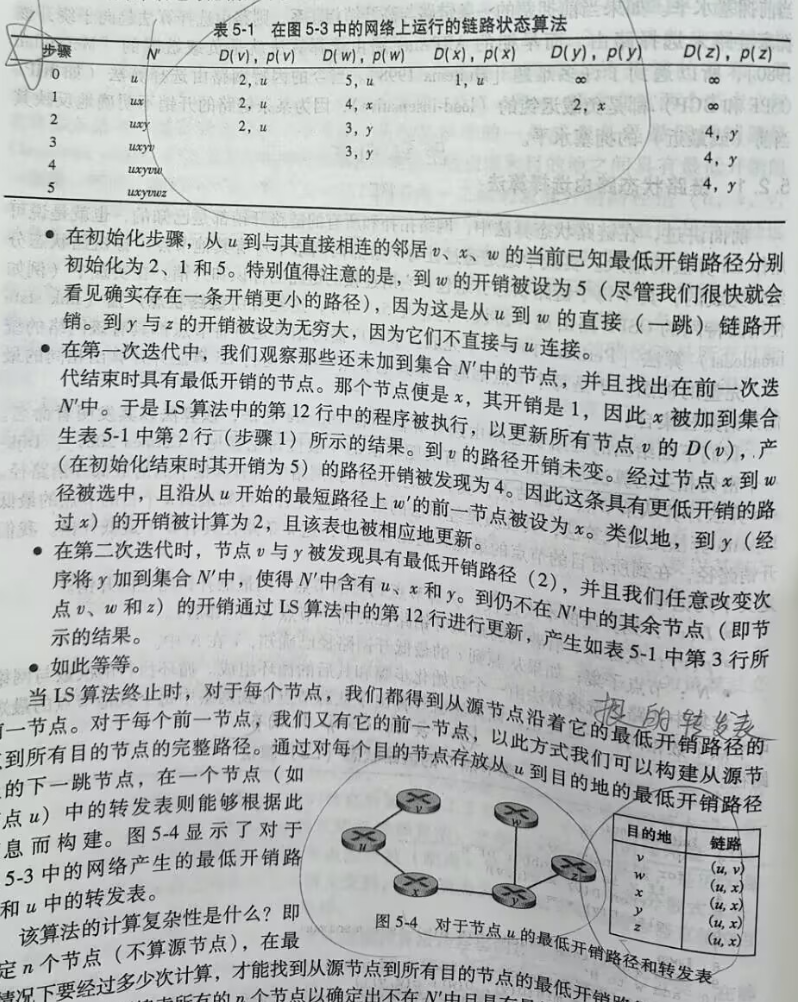
**14.以太网交换机（易考）**：

传统集线器的共享10Mb/s以太网，若共有N个用户，则每个用户平均带宽为总带宽的1/N。

而以太网交换机，每个接口到主机的带宽还是10Mb/s，但因为一个用户通信独占带宽，所以拥有N个接口的交换机总容量为N×10Mb/s，**这是交换机最大优点**。

802.11帧有三种类型：数据帧、控制帧和管理帧。

16.**vlan的三种划分方式**：基于接口、基于MAC地址、基于IP地址



9.电路、报文、分组

大量数据（传输时间远大于建立时间）用电路。从信道利用率来看，报文优于分组。但分组时延小，适用于突发性数据。

