计网复习大纲

导论（第一章）

1.1 网络协议（network protocols）

1.2 网络边缘

网络边缘：主机 服务器

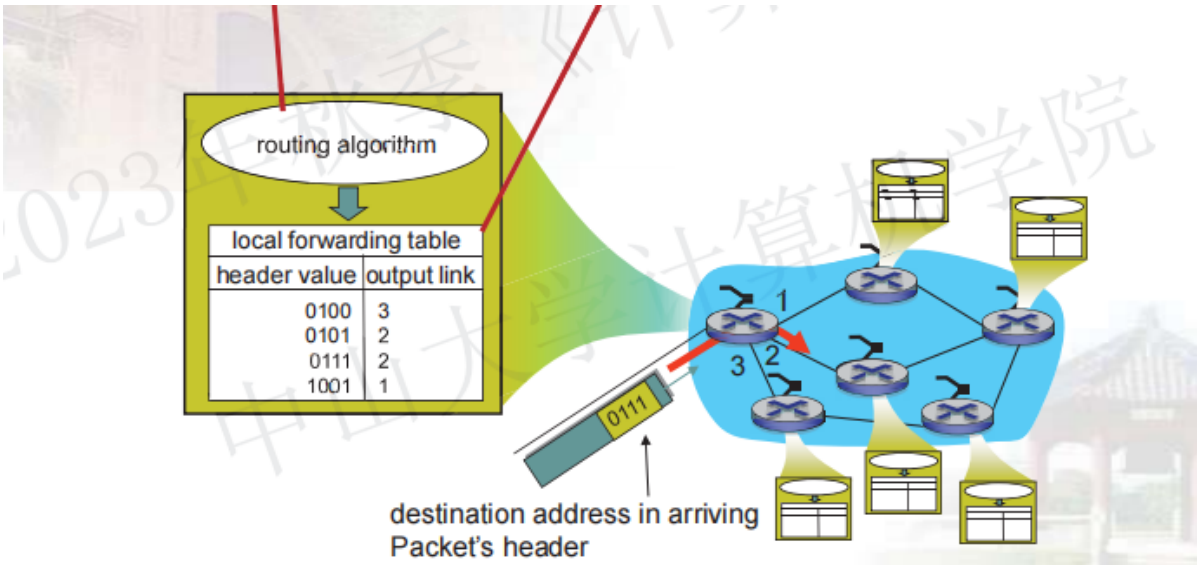
接入网：DSL

网络核心：交换机和链路构成的网络

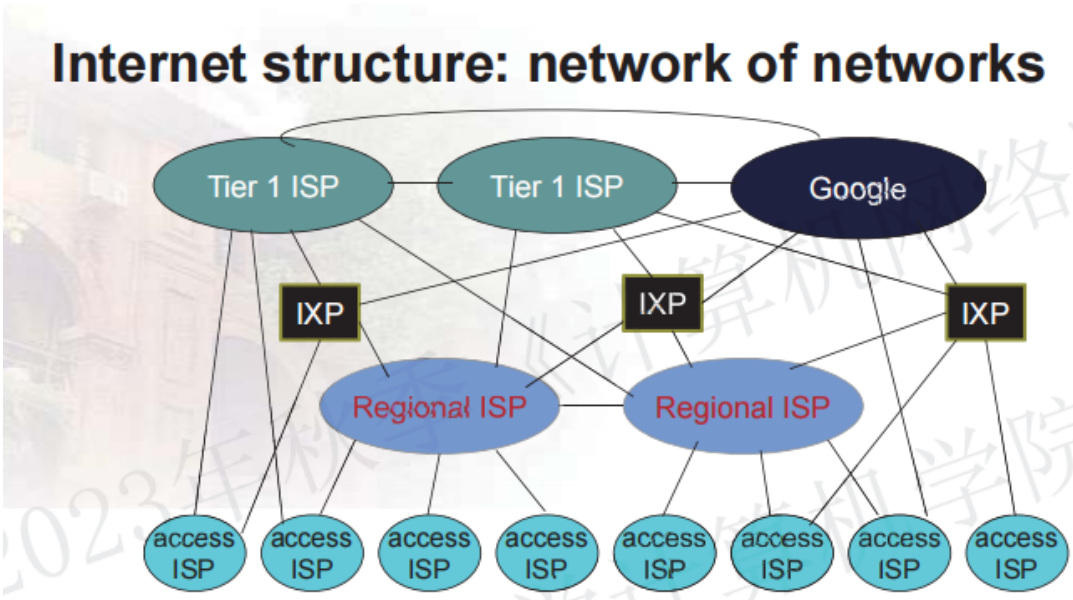
1.3 网络核心

分组交换与电路交换（可能出计算题）

转发表的格式：



网络结构：



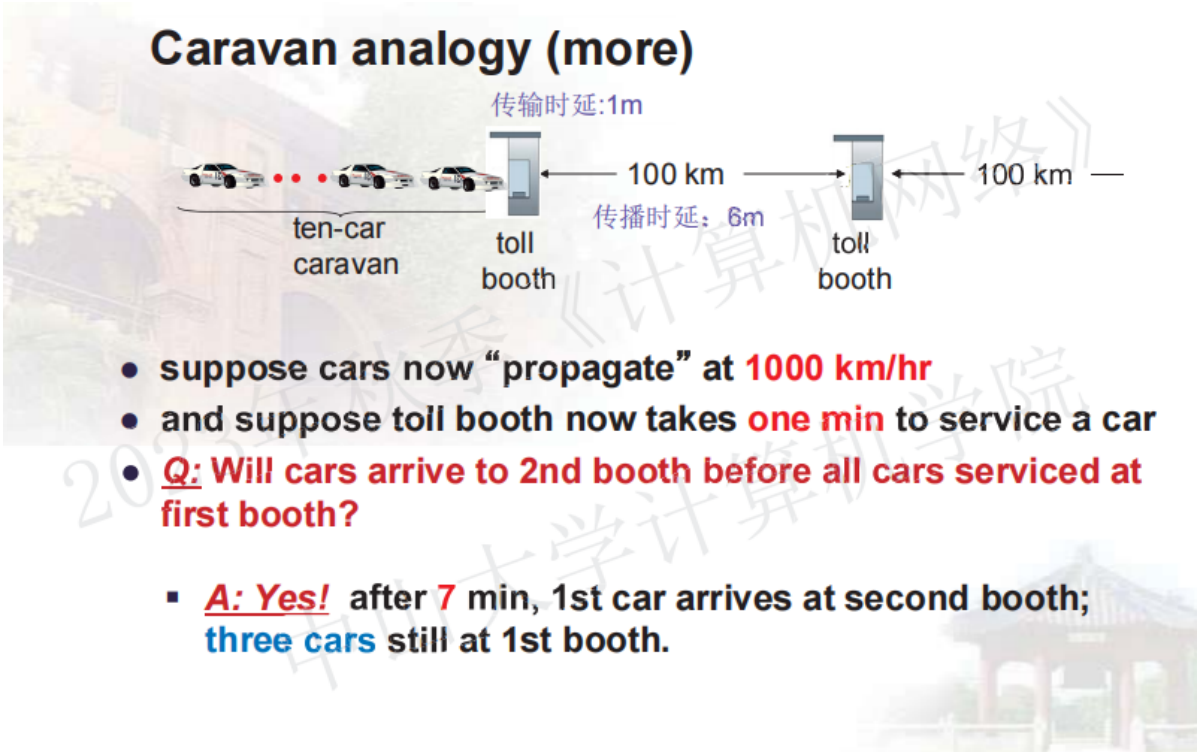
1.4 延迟与损失

四种延迟：处理延迟，排队延迟，传输延迟，传播延迟

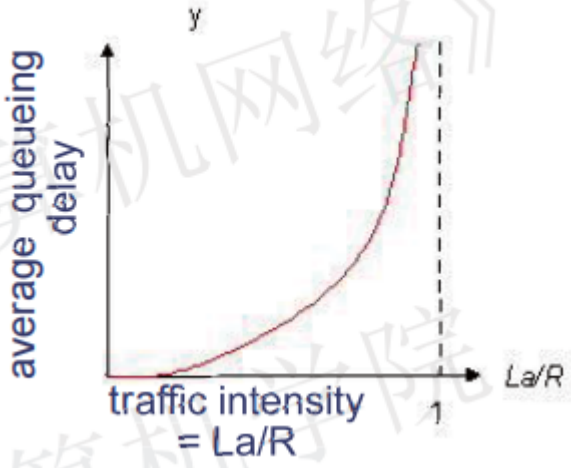
处理延迟：对数据检查，决定输出哪条链路

传输延迟：所有分组比特推向链路所需要的时间

传播延迟：在物理链路上传播的时间

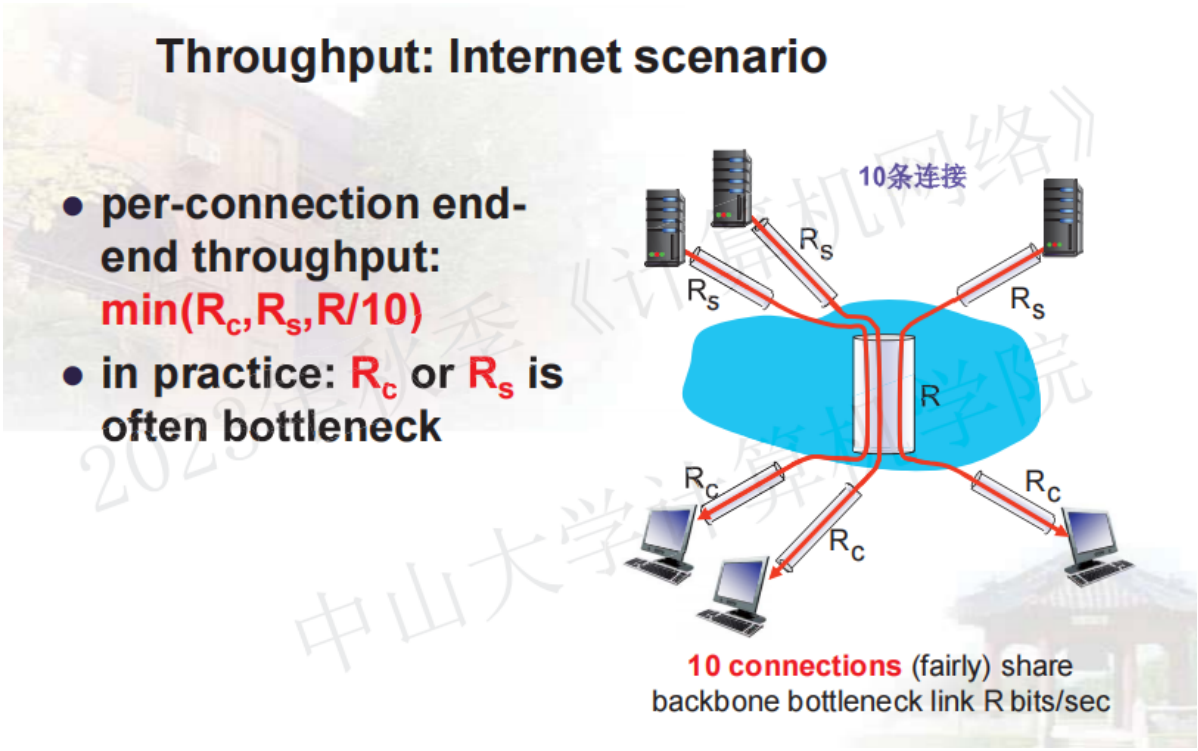


排队延迟：流量强度：La/R



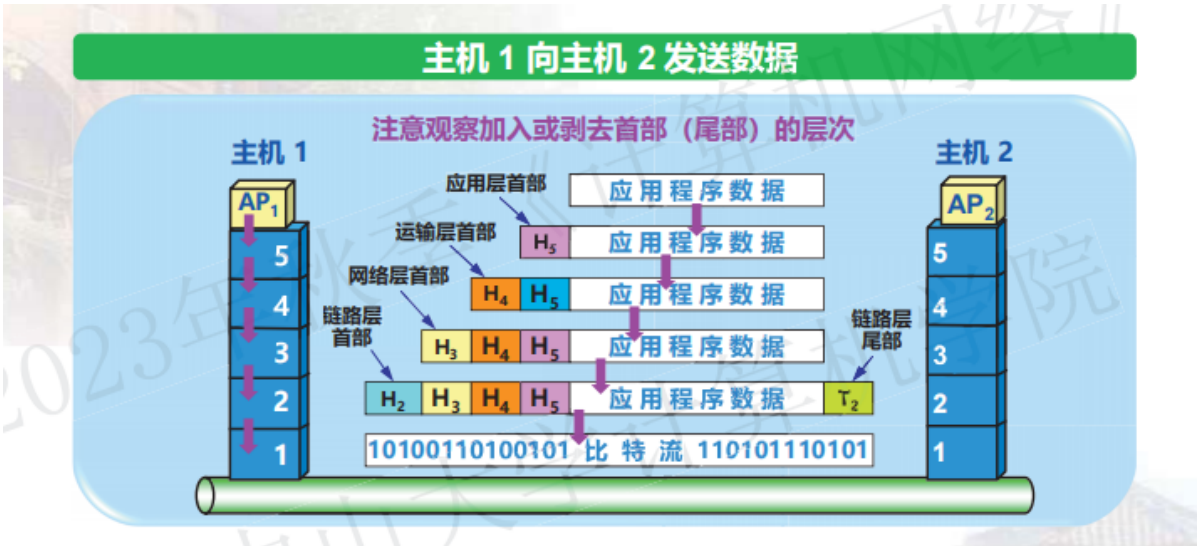
tarcert结果的解读

吞吐量：



协议分层：

- 应用层：为软件应用程序提供了网络服务接口，比如网页浏览器、电子邮件客户端和其他端到端的通信软件。主要协议有HTTP、FTP、SMTP，这里的信息分组称作报文
- 传输层：负责端到端通信和数据流的控制，确保数据有效和可靠地从源传输到目的地，常见的协议有TCP和UDP，这里的信息分组称作报文段
- 网络层：负责不同网络进行数据包的传输，处理如何在复杂的网络中路由数据包，包括数据包的寻址和路径选择。常见的协议有IP，这里的信息分组称为数据报
- 数据链路层：在物理网络设备间（如路由器、交换机和终端设备）提供了数据传输。这一层包括了协议如以太网（Ethernet）和Wi-Fi，这里的分组称为帧
- 物理层



应用层（第二章）

C-S模型

服务器：总是打开、固定周知的IP地址、有一个主机群

客户机：不总是打开、向服务器发出请求、IP地址不固定

P2P模型

自拓展性

DNS服务器

进行主机名到 IP 地址的转换。

DNS 协议运行在 UDP 之上，使用 53 号端口。

DNS服务器的类型：

- 根DNS服务器
- 顶级域DNS服务器
- 权威DNS服务器

递归查询：被联系的服务器不断递归查询下一可能知道的服务器直至得到答案。（被联系的服务器帮你去得到结果）

迭代查询：服务器返回下一个可查询的服务器名。（让本地DNS去查询其他的DNS服务器）

实际:采用递归+迭代相结合的方法

DNS 将能将信息缓存在本地存储器，**在一段时间后丢弃缓存的信息。**

本地DNS服务器

- DNS 报文：
  1) 前 12 个字节是首部区域；
  2) 问题区域：正在进行的查询信息。
     - 名字字段：指出正在被查询的主机名字；
     - 类型字段：住处正在询问的问题类型。
  3) 回答区域：对最初请求的名字的资源记录。
  4) 权威区域：其他权威 DNS 服务器的记录；
  5) 附加区域。

FTP服务器

用户通过一台主机，向一台远程主机上传文件或从远程主机下载文件。

FTP 用**两个并行的 TCP**连接传输文件，采用CS的工作方式，工作端口是21（控制连接）和20（数据连接）。

这两个端口都是服务器的。

FTP 的**控制信息**是**带外（out-of-band）传输**：使用一个分离的控制连接。

控制连接：两个主机之间传输控制信息（例如连接请求，传送请求），在整个会话期间一直保持打开状态。

数据连接：在客户端发送"传输请求"后建立，传送完毕后关闭。

电子邮件

电子邮件3个最主要的构建：用户代理、邮件服务器和电子邮件的协议（SMTP）

SMTP：使用**TCP** 可靠数据传输服务，从发送方的邮件服务器向接收方的邮件服务器发送邮件。

SMTP使用25号端口建立TCP连接。

具体操作：

SMTP有3个阶段：

- 连接建立（简单握手）：指明发送方和接收方邮件地址
- 发送报文：利用TCP，将数据可靠传输到接收服务器
- 关闭连接

1) Alice 调用她的邮件代理程序并提供 Bob 的邮件地址，撰写邮件，通过用户代理发送该邮件；
2) Alice 的用户代理将报文发送给 Alice 的邮件服务器，在那里报文被放在报文发送队列中；
3) 运行在 Alice 邮件服务器上的 SMTP 客户机端发现报文队列中的报文，创建一个到运行在 Bob 邮件服务器上的 SMTP 服务器的 TCP 连接；

ly 13

4) 握手后，SMTP 客户机通过该 TCP 连接发送 Alice 的报文；
5) Bob 的邮件服务器上的服务器端接收该报文，Bob 的邮件服务器将该报文放入 Bob 的邮箱中；
6) Bob 方便的时候，调用用户代理阅读该报文。

SMTP只支持传输7bits的ASCII码内容。

邮件格式：RFC 822规定了邮件的首部，最重要的是To（表明收件人的地址）和Subject（表明主题），以及from

首部和内容间隔一个空行。

POP：采用CS工作方式，使用TCP，端口号为110，可以获取右键

POP3采用明文登录

基于 Web 的电子邮件：用户代理是普通的浏览器，用户和其远程邮箱之间的通信通过 HTTP 进行。只有在不同邮箱服务器之间传输才会使用到SMTP。

http协议

web页面由对象组成，对象即文件，包括

- HTML
- URL：用于寻址文件

HTTL：

- 采用CS工作方式
- 采用TCP作为运输层协议
- 是无状态的（不保存任何信息，但是现在有cookie）
- 端口是80

非持久连接：每个请求及相应的响应对经一个单独的 TCP 连接发送。每次请求需要2RTT

持久连接：发送响应后依然保持连接（这样就不用再次来一次3次握手之类的了）

- 非流水线：用户收到前一个响应才能发出下一个请求
- 流水线：用户遇到一个对象引用就发一起请求。

HTTP的报文格式：

请求报文：get\head\post\put\delete

响应报文：状态码:

- 200 OK：请求成功，信息包含在返回的响应报文中；
- 301 Moved Permanently：请求的对象被永久转移，新的 URL 定义在响应报文的 Location：首部行；

- 400 Bad Request：请求不能被服务器理解；
- 404 Not Found：被请求的文档不再服务器上；
- 505 HTTP Version Not Supported：服务器不支持请求报文使用的 HTTP 协议版本。

web缓存器

P2P运用

运输层（第三章）

运输层提供**逻辑通信**，在端系统（PC）而非在网络路由器上实现

UDP

无连接：发送方和接收方没有握手

UDP 中缺乏拥塞控制机制

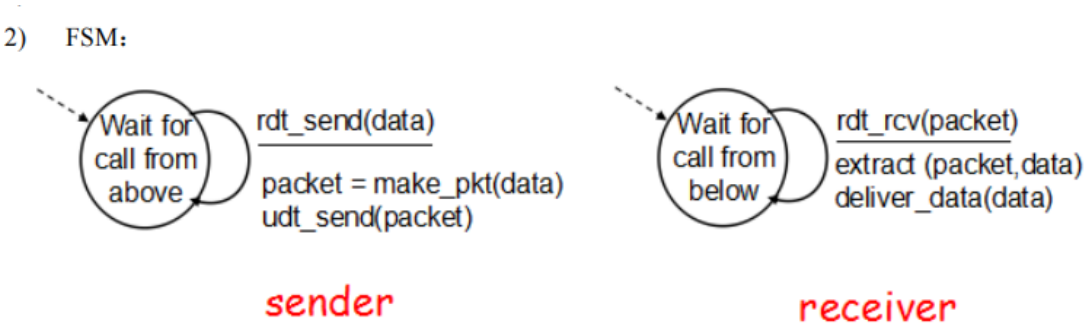
UDP首部仅有**8B**

UDP数据报：

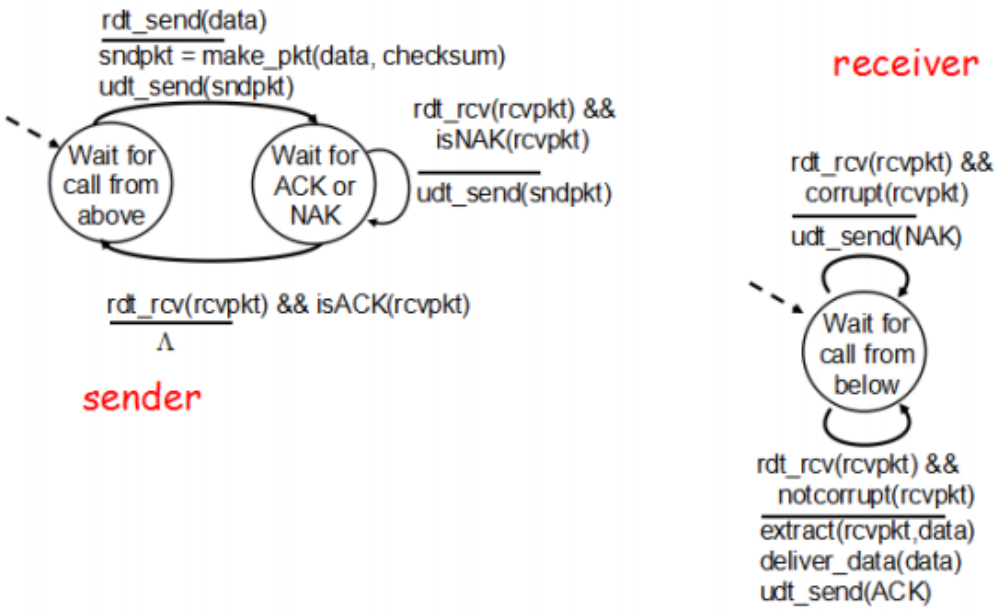
- 源端口号
- 目的端口号
- 长度：包括首部在内的 UDP 报文段长度。
- 校验和（该字段可选，如果主机不想计算则全部为0）
    - 计算：进行反码运算（得到结果后取反，需要注意的是如果有溢出则需要回卷）

可靠数据传输

rdt1.0：底层信道是完全可靠的



rdt2.0：可能存在比特差错，如果有差错则返回NAK，接收到NAK后重发一次



rdt2.1：引入数据编号（1，0），如果接收方接收到一样的数字，说明漏发，则返回NAK，收到NAK后发送方重发包

rdt2.2：不用NAK改用ACK

rdt3.0：加入超时

流水线操作：

GBN：允许发送方发送多个分组而不需等待确认，每收到一个分组的ACK，就把窗口右移一位，如果超时，则从第i个分组重新发送

SR：如果分组序号在窗口内，则确认已经被接收，但只有窗口的全部分组接收到了ACK才会继续移动，否则只会移动到最小未获确认的分组中。

TCP

TCP是面向连接的传输层协议

TCP是点对点的协议，即发送方和接收方都只能是单个的。

TCP采用**全双工服务**：应用数据可以从进程 B 流向进程 A 的同时，从进程 A 流向进程 B；

TCP报文段结构：20B

- 源端口号、目的端口号
- 序号字段
- 确认号字段
- 接收窗口字段
- 首部长度字段
- 选项字段

三次握手过程：

1.客户机发送请求报文段，SYN=1,seq=x,ack=y

2.服务器发送确认报文段，SYN=1,seq=y，ack=x+1

3.客户机返回确认：SYN=0,seq=x+1,ack=y+1

连接终止：

TCP流量控制

流量窗口：类似缓存机制

发送窗口的上限值：min[rwnd,cwnd]

TCP拥塞控制

cwnd小于阈值：采用慢开始算法

cwnd大于阈值：采用拥塞避免算法（每次+1）

发生丢包：阈值被设为当前cwnd的一半，同时阈值变为1

改进方法：快重传和快恢复

快恢复：由 3 个冗余 ACK 检测到的丢包事件（快重传），则阈值/2，cwnd=阈值，进行拥塞避免算法

网络层（第四、五章）

链路层（第六章）

信道类型：

- 广播信道
- 点对点传输

差错检验

循环冗余检测（CRC）

G*2^r/p，余数得到R，教程帧检验序列

每个 CRC 标准可都能检测到任何奇数个比特差错。

多路访问协议

信道划分协议

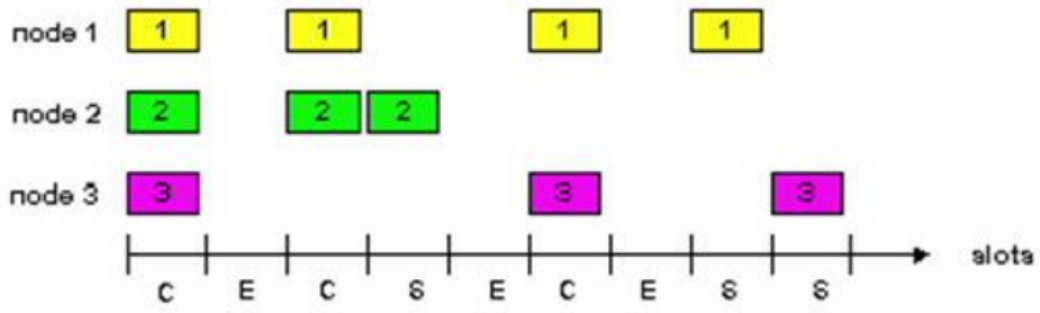
- 频分多路复用：划分为不同频段，每个频段具有R/N贷款，每个节点都可以得到一个
- 时分多路复用：将时间划分为时间帧，每个时间帧有N个时隙。

多路复用的优点：消除碰撞且公平

缺点：节点被限制于R/N的速率，必须等待在传输序列中的轮次。

随机接入协议：一个传输节点总是以信道的全部速率（即 R bps）进行发送。当有碰撞时，设计碰撞的每个节点反复重发它的帧，直到无碰撞的通过为止。

2) 时隙 ALOHA 协议的操作：
   - 节点由新帧发送时，等到下一个时隙开始并在该时隙传输整个帧；
   - 没有碰撞，则无需考虑重发；
   - 有碰撞，则在时隙结束前检测，然后节点以概率 p 在后续的每个时隙中重新传输该帧，直至其被无碰撞的传输出去。



优点：简单，某节点唯一活跃时可以全速传输，每个节点决定何时重传，是高度分散的

缺点：多个活跃节点存在时一部分会被浪费掉，时隙的另一部分将是空闲的（因为可能大家都是（1-p）的概率

最大效率：37%，有37%的时隙是空闲的，36%的时隙有碰撞产生

CSMA：

- 载波侦听：节点在传输前先听信道
- 碰撞检测：一个传输节点在传输时一直侦听信道

为什么CSMA还会有碰撞？传播延迟，AB都想发数据，此时大家都听到信道空闲，A先发出，此时B听到的还是空闲，所以B也发送数据，导致冲突

CSMA/CD：

适配器在任意时刻开始传输，没有时隙的概念

重传前适配器等待一个随机事件

轮询访问协议：

主节点以循环的方式轮询每个节点

令牌传递协议：

一个令牌的特殊帧在节点之间进行交换，一个节点收到令牌时则进行传输，如果没有传输则将这个令牌传给其他节点。

链路层编址

MAC地址：端口具有的地址

ARP：将IP转换为MAC地址