《计算机网络》知识点汇总

第一章 网络概述

1、计算机网络的组成：终端（客户机、服务器）、通信链路（光纤、双绞线、无线电、同轴电缆、电话线）和设备（路由器、二层交换机）。

2、（网络应用是）分布式应用程序仅运行在终端系统上，不运行在网络核心的分组交换机中，因此因特网是为应用程序提供服务的基础设施。

3、网络协议：定义了在两个或多个通信实体之间交换的报文格式和次序，以及报文发送（和/或）接收一条报文或其他事件所采取的动作。协议三要素：语法、语义、时序(同步)。

(1) 语法：即数据与控制信息的结构或格式（IP 头部、TCP 头部的字段含义）；

(2) 语义：即需要发出何种控制信息，完成何种动作以及做出何种响应；

(3) 时序（同步），即事件实现顺序的详细说明。

4、网络的接入形式：

（1）家庭接入：数字用户线技术接入（ADSL、电话双绞线、频分复用技术）、混合光纤同轴电缆技术接入（光电、同轴电缆、光纤、频分复用技术）、光纤到户技术接入（电信、光纤）、卫星链路接入（星链计划、无线电）

（2）企业（和家庭）接入：以太网（Ethernet，802.3）、无线以太网（WiFi，802.11）

（3）广域无线接入(移动接入)：3G（第三代移动通信系统）、4G、5G

5、网络的构建形式：分组交换网络和电路交换网络

（1）分组交换网络：主机将应用层消息(messages)分割为若干分组(packets)，每个分组沿着从源主机到目的主机的传输路径通过每个路由器（逐跳）转发，每个分组在每条链路传输时，以**链路的最大传输速率**传输。每个路由器采用**存储转发机制**，即将每个分组完整接收后，根据其 IP 头部包含的目的 IP 地址进行转发。

分组的传输时延、传播时延。分组出现丢包和排队的原因。路由和转发的区别。

（2）电路交换网络：数据的发送方和接收方之间需要建立一条物理的电路，发送方可以以恒定的速率向接收方发送数据，整条电路被临时占用，直到数据发送结束。

电路交换中的几种复用技术：频分复用（FDM）、时分复用（TDM）。

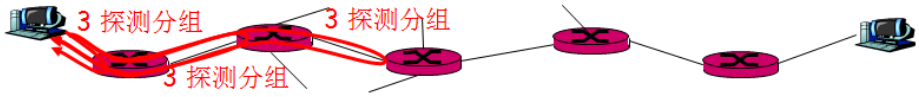
（3）电路交换和分组交换的区别。报文交换（存储转发，不预留资源，整个报文不分割为分组）。电路交换浪费资源（静默期）

掌握：一个文件在（分组交换、报文交换）方式下的传输时延。

6、分组交换网中的 4 种时延。

处理时延、排队时延、传输时延、传播时延。

7、traceroute 诊断程序：可追踪**源和目的之间经过的路由**




```
C:\Users\Administrator>tracert www.uestc.edu.cn

通过最多 30 个跃点跟踪
到 www.uestc.edu.cn [202.112.14.178] 的路由:

  1     3 ms     4 ms     1 ms  192.168.1.1
  2     4 ms     2 ms     1 ms  192.168.0.1
  3     8 ms     3 ms     2 ms  210.41.108.1
  4     3 ms     2 ms     2 ms  202.115.0.5
  5     *        *        *     请求超时。
  6     8 ms     7 ms    10 ms  202.112.14.178

跟踪完成。
```

8、协议层次及服务模型

TCP/IP 五层（四层）结构，每层的功能：

应用层:（网络应用）、各种网络应用（QQ、腾讯视频、FTP、Web、SMTP、DNS、DHCP）

运输层：实现（进程-进程）的数据传输，TCP、UDP

网络层：实现（主机-主机）的数据传输，IP、RIP、OSPF、BGP、ICMP、ARP（2.5 层）

数据链路层：实现单条链路的数据传输，802.11、802.1、802.3，

物理层；实现单条链路上比特流的编码和解码。

OSI 七层体系结构：

表示层：加解密、数据压缩、格式转换

会话层：对数据传输进行管理，包括数据交换的定界、同步，建立检查点等。

9、数据的封装和解封装：加（拿掉）头部

应用层：报文（message）

运输层：报文段（segment）

网络层：数据报（分组）packet（datagram）

数据链路层：数据帧（frame）

物理层：比特流（bit）

主机上：全部层次，路由器上运行物理层、数据链路层、网络层，交换机上运行物理层、数据链路层。

10、网络安全问题：

（1）恶意软件对主机的侵害：恶意代码(Malware)植入主机，包括病毒和蠕虫；也可以是间谍软件，记录你的键盘敲击、访问网站等信息，上传到指定网站；也可以将你的主机在僵尸网络中注册，参与分布式攻击等。

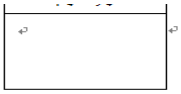
（2）恶意软件对网络基础设施的侵害：DoS 攻击和 DDoS 攻击，攻击路由器、服务器等，使其不能为正常用户服务。

（3）在网络上嗅探(sniffer)：在共享（广播）信道中，可以监听到别人的数据包；

（4）IP 哄骗：发送的数据包的 IP 地址等信息伪装成其他人的。

- 主动攻击：包含攻击者访问他所需信息的故意行为。比如远程登录到指定机器的端口 25 找出公司运行的邮件服务器的信息；伪造无效 IP 地址去连接服务器，使接受到错误 IP 地址的系统浪费时间去连接哪个非法地址。攻击者是在主动地做一些不利于你或你的公司系统的事情。正因为如此，如果要寻找他们是很容易发现的。主动攻击包括拒绝服务攻击、信息篡改、资源使用、欺骗等攻击方法。
- 被动攻击主要是收集信息而不是进行访问，数据的合法用户对这种活动一点也不会觉察到。被动攻击包括嗅探、信息收集等攻击方法。（不会影响受害人的设备）

本章练习题：



四、假设将从源主机向目的主机发送 40Mbit 的 Word 文档。在源和目的主机之间的路径中所有链路的传输速率都是 10Mbps。假设传播速率是 $2*10^8$ m/s，请回答以下问题：(16 分)

(1) 假设源和目的端之间单独使用一条距离是 10^7m 的物理链路连接，使用报文交换，该报文包括了完整的该 Word 文档，且忽略首部等封装用的字节的长度，忽略处理时延，分别计算传输时延、传播时延和端到端时延。(3 分)

(2) 假设源和目的端之间单独使用一条距离是 10^7m 的物理链路连接，使用 TDM 方式的电路交换，每帧划分为 10 个时隙，该 Word 文档使用其中一条电路进行发送，且发送时连接已经建立，分别计算传输时延、传播时延和端到端时延。(3 分)

(3) 假设源和目的端之间的路径是由一台路由器连接的 2 条链路所组成，每条链路长度为 $5X10^6$m，使用报文交换，该报文包括了完整的该 Word 文档，且忽略首部等封装用的字节的长度，忽略处理时延和排队时延，计算从发送方开始发送到接收方接受到完整的 Word 文档所花费的时间。(5 分)

(4) 假设源和目的端之间的路径是由一台路由器连接的 2 条链路所组成，每条链路长度为 $5X10^6$m，使用分组交换，该 Word 文档分为 4 个分组，每个分组长度为 10Mb，且忽略首部等封装用的字节的长度，忽略处理时延和排队时延，4 个分组连续发送，计算从发送方开始发送到接收方接受到完整的 Word 文档所花费的时间。(5 分)

- 在协议分层服务模型中，服务的定义为（ C ）。

A、各层向下提供的一组原语操作　B、各层间对等实体间通信的功能实现

C、各层通过其SAP向上层提供的一组功能　D、和协议的含义是一样的

- 当一台计算机从FTP服务器下载文件时，在该FTP服务器上对数据进行封装的五个转换步骤是(　)。

A、比特、帧、数据报、报文段、报文　B、报文、报文段、数据报、帧、比特

C、数据报、报文段、报文、比特、帧　D、报文段、数据报、帧、比特、报文

- 因特网协议栈分为几个层次？分别是哪几个层次(按自顶向下的顺序描述)？简单描述每个层次的主要功能。

第二章 应用层

1、网络应用程序的体系结构：C/S、P2P

C/S 架构下客户端和服务器的特点。

P2P 脚骨下客户端和服务器的特点。

2、TCP 可以提供的服务（数据的可靠传输、流量控制、拥塞控制），不能提供的服务（时间控制、最小吞吐量保证、安全性），是面向连接的方式（有连接的建立和拆除过程）

3、UDP 可以提供的服务（数据的不可靠传输），不能提供的服务（可靠性、流量控制、拥塞控制、时间保证、最小吞吐量保证、安全性），是无连接的方式（没有连接的建立和拆除过程）

思考：在什么应用场景下需要 UDP 协议（DNS、流媒体等）

4、Web 应用的应用层协议是 HTTP。（HTTP 采用 TCP 协议，80 端口）

（1）持续连接和非持续连接：非持续连接（TCP 连接最多发送一个对象，然后关闭 TCP 连接，下载多个对象需要建立多个 TCP 连接）；持续连接（多个对象可以基于一个 TCP 连接发送），浏览器默认使用持续连接。

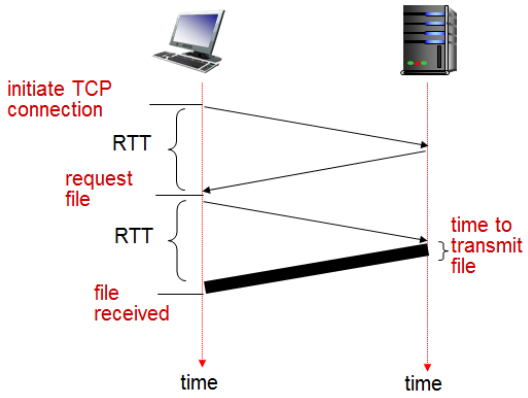
非持续连接的响应时间

RTT (definition): time for a small packet to travel from client to server and back

HTTP response time:

- 1个RTT用于建立TCP连接
- 1个RTT用于HTTP请求
- one RTT for HTTP请求和需要HTTP返回响应的前几个字节
- 文件传输时间
- 非持续HTTP

响应时间 = 2RTT+ file transmission time



（2）基本的 HTTP 报文格式，请求报文和响应报文，**前几个字段**。

（3）Cookie 的原理（4 个组件）及应用场景

authorization(认证)

shopping carts(购物车)

recommendations(推荐)

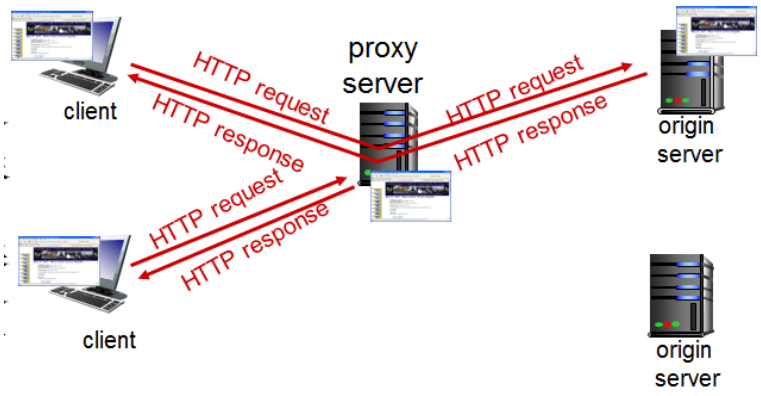
user session state (Web e-mail)(用户会话状态)

存在的问题：隐私泄露

（4）web 缓存

浏览器发送所有的 HTTP 请求给 cache(缓存服务器)

如果请求对象存在于缓存服务器：缓存服务器直接返回对象给客户；如果请求对象不在缓存服务器中，则缓存服务器向原始服务器请求，然后返回对象给客户



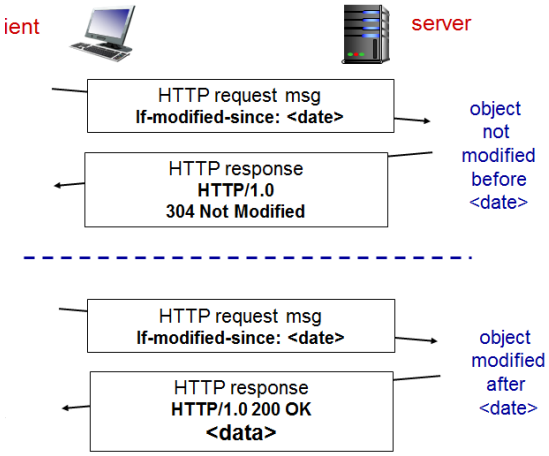
使用 web 缓存（cache）的优点：

- 减少对于客户端请求的响应时间
- 减少原始服务器接入链路的流量
- Internet dense with caches: enables “poor” content providers to effectively deliver content (so too does P2P file sharing)

（5）条件 Get：怎么确保缓存服务器上的 object 是最新的？

具体方法：

- 发送包含上次更新的时间
- 如果没有发生修改，则返回一个空数据的响应报文
- 如果发生了修改，则返回一个最新的数据



www上每一个网页都有一个独立的地址，这些地址统称为（ ）

A、IP地址　　B、域名地址

C、统一资源定位符　　D、www地址

Cookie主要包括哪几个部分？Cookie的作用是什么？会带来什么问题？（6分）

P114-P1

P114-P4，P5（下次课评讲）

描述引入Web缓存后浏览器访问网页的过程？

- 现有一个网页由8个对象文件组成，8个对象文件在一个web服务器上，使用**带流水线的持久HTTP连接**显示这个网页需要等待多少个RTT（A）

A. **3个RTT** B. 4个RTT C. 9个RTT D. 16个RTT

- 下列HTTP报文首部行正确的是（C）

A. GET HTTP/1.1 /somedir/index.htm B. HTTP/1.1 OK

C. **POST /somedir/index.htm HTTP/1.1** D.GET 200 OK

- 两个不同的Web页面（例如，www.uestc.edu.cn/index.html和mail.uestc.edu.cn/index.html）可以使用一个持久连接发送。(X)

- HTTP响应报文不会有空的报文体。（X）

5、文件传输应用的协议：FTP（TCP 协议，C/S，21 和 21 端口号）

有两个 TCP 连接：1 个用于控制连接（21，传输用户认证信息，浏览目录，文件请求命令），1 个数据连接（20，专门用于传输文件数据）

6、电子邮件应用的协议：SMTP（TCP，C/S，25）、POP3（TCP，C/S）

从客户端软件到发件人的邮件服务器：HTTP，SMTP

从发件人的邮件服务器到收件人的邮件服务器：SMTP

从收件人的邮件服务器获取邮件到本地：pop、IMAP，HTTP

注意：邮件内容使用 ASCII 码编码，对于非 ASCII 的内容，采用 MIME 格式。

- 一个FTP的用户，发送了LIST命令来获取服务器的文件列表，这时候服务器应该通过( )端口来传输该列表。

  A、21 B、20 C、22 D、19

- SMTP协议是面向ASCII编码的，那么它使用（D）支持非ASCII的数据传输。

  A、MAIL B、POP3 C、IMAP D、MIME

- FTP客户和服务器之间传递FTP命令时，使用的连接是(　　)。

A、建立在TCP之上的控制连接 B、建立在TCP之上的数据连接

C、建立在UDP之上的控制连接 D、建立在UDP之上的数据连接

A、D、A

- 电子邮件系统中，用户代理把邮件发往发送发邮件服务器、发送方邮件服务器把邮件发往接收方邮件服务器以及用户使用用户代理从接收方邮件服务器上读取邮件时，使用的协议可能是以下的哪种情形? (D)

A、IMAP 、SMTP、POP3 B、MIME、SMTP、POP3

C、SMTP、IMAP、POP3 D、SMTP、SMTP、IMAP

HOME WORK P115-R16

假定Alice使用一个基于web的电子邮件账户向Bob发送报文，而Bob使用POP3从他的邮件服务器访问自己的邮件。讨论是怎样从Alice主机到Bob主机得到该报文的。要列出在两台主机间移动该报文时所使用的各种应用层协议。

7、因特网域名查询 IP 地址的应用协议：DNS（UDP，C/S，53 端口）

（1）DNS 提供的服务：

- 主机名到 IP 地址的转换
- 主机别名查询 (host aliasing)：应用程序可以调用 DNS 来获得主机别名所对应的规范主机名以及主机的 IP 地址。
- 邮件服务器的别名：电子邮件应用程序可以调用 DNS，对提供的邮件服务器别名进行解析，以获得该主机的规范主机名及 IP 地址。
- 负载均衡 (load distribution)：一个域名对应多个 IP 地址及服务器，当一个 DNS 域名解析请求到达 DNS 服务器时，服务器依次使用 1 个 IP 地址作为响应，以实现负载均衡。

（2）DNS 应用采用的是一种分布式数据库系统，为什么不采用集中式数据库系统？

单一点失效、流量负担、远程的集中式数据库、维护开销大，不具有扩展性。

（3）DNS 是一个分布式、层次化的数据库

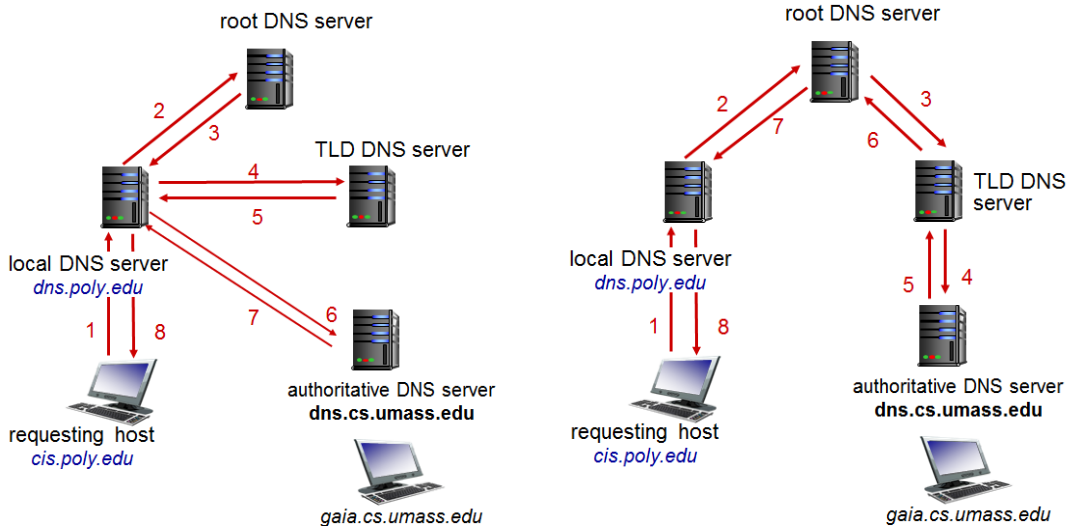
- 根服务器：在因特网上有 13（247：2011）个根服务器，主要维护的是顶级域名服务器的 IP 地址；
- 顶级域服务器（TLD）：维护顶级域名的 IP 地址

顶级域名：com、org、net、edu、gov、jp、ca、cn

- 权威 DNS 服务器：由组织机构维护的自己提供的服务器的域名到 IP 地址映射的 DNS 服务器。例如我们学校的 Web 服务器和电子邮件服务器的域名和 IP 地址的映射由我们学校自己的权威 DNS 服务器维护。

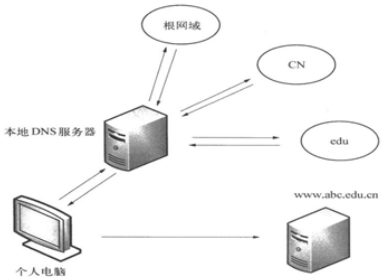
（不处于分级结构，本地的主机访问的 DNS 服务器）本地 DNS 服务器。

（4）基于 DNS 的域名解析过程：迭代查询和递归查询



课堂练习题：

一个主机申请了一个到www.abc.edu.cn的连接，为了获取服务器的IP地址，首先要进行DNS查询，下图为本次查询的过程，请回答如下问题：



- 由个人主机发送给本地DNS服务器的数据是采用什么运输层协议发送的？利用那个端口？
- 由个人主机到本地DNS服务器查询是采用了什么方式？
- 由本地DNS服务器到各个域名服务器的查询，采用了什么方式？
- 本地DNS服务器的查询顺序是什么？

8、P2P

（1）P2P 结构的特点

直接在对等方（peer）间传输：所有内容不经过第三方服务器;

高度的可扩展能力：利用众多对等方集合中的资源去分发内容;

使用客户机/服务器模式：请求的对等方是客户机，被选中的对等方是服务器。

服务器对等方使用文件传输协议向客户机对等方传送；通过传送“HTTP 请求”和“HTTP 响应”报文进行；所有的对等方必须既能运行文件传输协议的客户机端程序，又能运行服务器端程序；对等方既是一个客户机，又是一个瞬时 Web 服务器。

（2）在 P2P 中如何定位资源的位置：集中式目标、查询泛洪、层次化结构的维护

课堂练习：

- 以下关于P2P概念的描述中，错误的是（）。

A、P2P是网络结点之间采取对等的方式直接交换信息的工作模式。

B、P2P通信模式是指P2P网络中对等节点之间的直接通信能力。

C、P2P网路是指与互联网并行建设的，由对等结点组成的物理网络。

（应用层网络、逻辑网络（overlay network））

D、P2P实现技术是指为实现对等节点之间直接通信的功能所需要设计的协议、软件等。

9、视频流和内容分发网络（content delivery network, CDN）

DASH 主要针对视频流，CDN 可以提供文件存储服务

（1）DASH：流媒体服务器端可以将一个视频编码为不同的速率，每个速率的视频文件存为一个 URL，用户可以根据自己的网络状况选择一个适合自己的视频文件播放。

（2）CDN：对于提供大型（实时性、并发性）服务的公司，通常建立数据中心来为用户提供服务，但是集中式的数据中心存在 3 个问题。**问题 1**：客户可能与服务器距离遥远，需要经过若干链路和路由器，甚至是跨越多个 ISP，导致数据传输的端到端延时较大；**问题 2**：许多相同的视频数据可能在一条链路上重复传输，对于骨干链路的带宽资源是一种浪费，更好的方法是相同的视频数据在若干公共的骨干链路上只传输 1 次，在

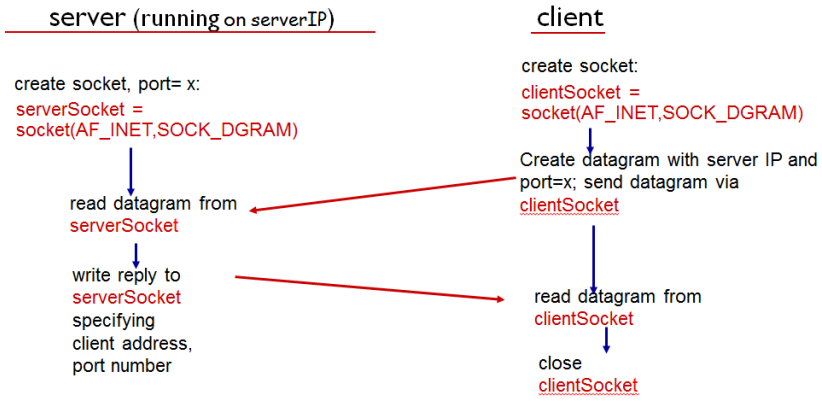
接近用户终端的接入点在复制为多份发送给不同的终端用户；**问题 3**：集中式数据中心是单点，如果单点失效，将不能提供服务，好的改进是将视频数据备份在不同地点的服务器上。这就对应提出了 CDN 的概念。在不同的 ISP 的接入点（或交换点）各个大型公司分别建立自己的 CDN 集群，以备份数据。当用户访问 YouTube 的网站时，实际访问的是距离用户最近的那个 CDN 集群的服务器。

10、套接字编程

（1）UDP 套接字编程，客户端程序和服务器程序包含的函数

客户端：socket\sendto\recvfrom\close

服务器：socket\bind\ sendto\ recvfrom



（2）TCP 套接字编程，客户端程序和服务器程序包含的函数

客户端：socket\connect\send\recv\close (connect 发起 TCP 连接请求)

服务器：socket\bind\listen\accept\recv\send\close

第三章 运输层

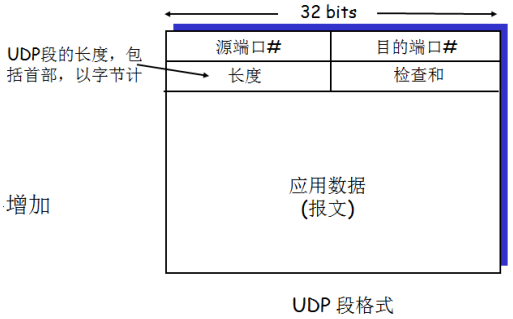
1、运输层提供的是（process-process）的数据传输服务。

TCP 提供可靠的、按序的数据交付服务：拥塞控制、流量控制、建立连接。

UDP 提供不可靠的、不按序的数据交付服务：不建立连接。

TCP 和 UDP 都不能提供数据传输的时延保证、最小带宽（吞吐量）保证。

2、TCP 和 UDP 的报文头部格式



UDP 段格式

3、UDP 协议

（1）使用 UDP 的应用层协议有哪些？DNS、SNMP

（2）UDP 的优势

（3）UDP 不提供数据可靠传输，因此如果应用程序需要保证数据可靠，需要在应用程序中实现数据可靠性。

（4）校验和（checksum）：每 16 比特一段，按位求和，最高位有进位，则回卷，按位求反。

课堂练习题

P3. UDP and TCP use 1s complement for their checksums. Suppose you have the following three 8-bit bytes: 01010011, 01100110, 01110100. What is the 1s complement of the sum of these 8-bit bytes? (Note that although UDP and TCP use 16-bit words in computing the checksum, for this problem you are being asked to consider 8-bit sums.) Show all work. Why is it that UDP takes the 1s complement of the sum; that is, why not just use the sum? With the 1s complement scheme, how does the receiver detect errors? Is it possible that a 1-bit error will go undetected? How about a 2-bit error?

4、TCP 协议

TCP 涉及到的可靠传输机制：定时器、重传、差错检测、正确确认、流水线

（1）流水线机制：GBN 和 SR。

（2）GBN 的原理：

发送方

- 维护一个窗口，不能发送超过窗口范围外序号的分组，分组首部需要 K 比特序号，2^k=N，允许 N 个连续的没有应答分组

  窗口内的分组分为已发送还未收到 ACK 确认的分组(黄色)，可发送还未发送的分组（蓝色）。send_base 指向已发送但未收到 ACK 确认的分组的最小序号。
- 收到发送方返回的 ACK(n)，表示接收方收到了所有比 n 小的序号的分组（累计确认机制）；可能会收到重复的 ACK 确认包
- 定时器，对最老已经发送还未收到确认 ACK 的分组（send_base）维护一个定时器；
- 定时器超时机制，timeout(n)，重传所有已经发送还没有收到 ACK 确认的分组。

接收方：

- 接收空间只有 1 个包的大小，如果是期望接收序号的包，就接收下来，向上层提交；

  如果不是期望接收序号的包，则丢弃，返回 ACK(期望的序号)；

注意：没有接收缓冲区。会发送一个重复的 ACK 确认。

练习题：

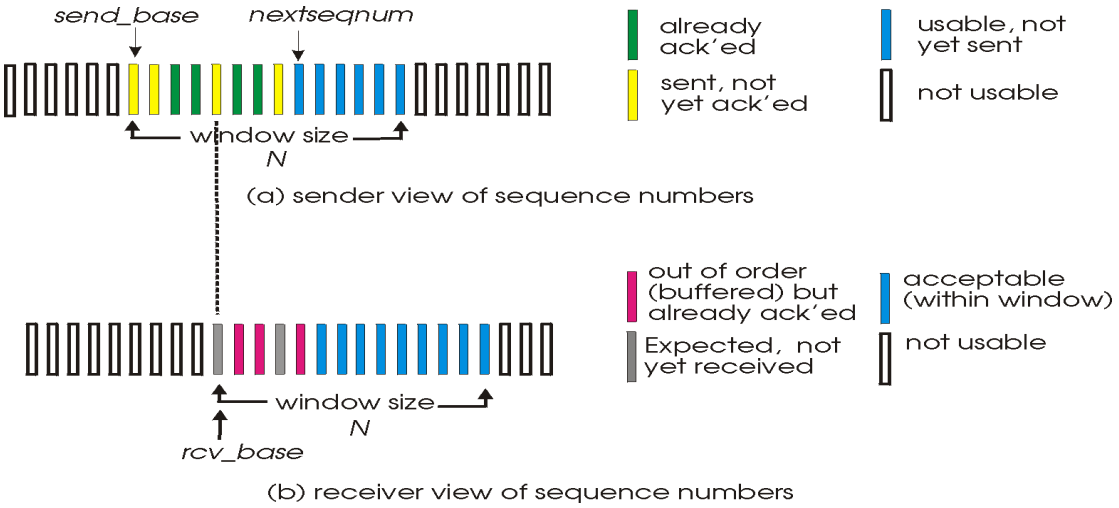
R12. Visit the Go-Back-N Java applet at the companion Web site.

a. Have the source send five packets, and then pause the animation before any of the five packets reach the destination. Then kill the first packet and resume the animation. Describe what happens.

b. Repeat the experiment, but now let the first packet reach the destination and kill the first acknowledgment. Describe again what happens.

c. Finally, try sending six packets. What happens?

（3）选择重传 SR 的原理



发送方：

- 维护发送缓冲区，有个滑动窗口，包括已发送未收到 ACK 确认的分组（黄色），已发送已收到 ACK 确认的分组（绿色），未发送分组（蓝色）；
- 收到 ACK(n)，在 SR 中，ACK 确认是针对单个分组的，收到对某个分组的 ACK 确认，说明这个分组被接收方收到。
- 定时器，对当前已发送未收到确认的所有分组各自维护一个定时器，多个定时器；
- 定时器超时，某个序号的分组的定时器超时，则只重传超时对应的这个分组。

接收方：

- 收到分组是期望序号的分组，则返回 ACK(n)给发送方；
- 对于收到的分组如果不是期望序号的分组，则缓存这个分组，发送按序到达的分组的确认 ACK 给发送方。

5、TCP 协议的可靠传输机制

（1）采用的机制：定时器/重传、ACK 确认（累计确认）、滑动窗口（发送方和接收方均采用滑动窗口，可缓存时序分组）、

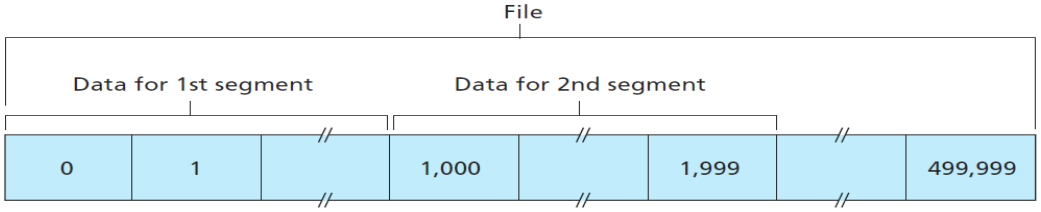


Figure 3.30 ♦ Dividing file data into TCP segments

序号：字节流中的位置

确认号：已收到序号的下一个序号

定时器（单个定时器）：只对发送窗口中最早的已发送未收到 ACK 确认的分组启动定时器，定时器超时，则只重传这个分组。如果收到这个最早已发送未确认分组的 ACK 确认，则停止定时器，继续对当前窗口中已发送未确认的分组重新启动定时器。

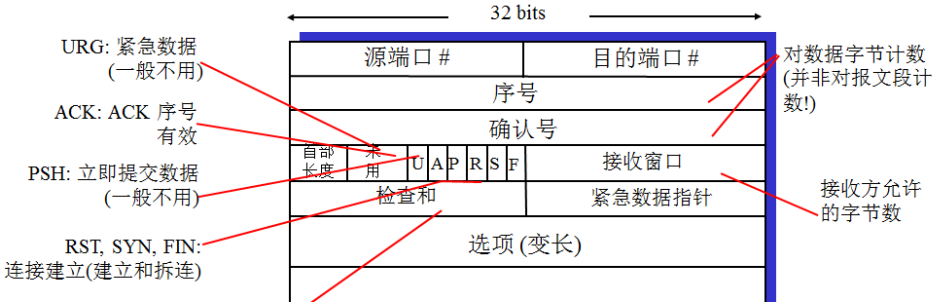
定时器设置多长时间？

TimeoutInterval = EstimatedRTT + 4*DevRTT

estimated RTT

"safety margin"

（2）TCP 头部字段（20 字节）



课堂练习题：

P27. Host A and B are communicating over a TCP connection, and Host B has already received from A all bytes up through byte 126. Suppose Host A then sends two segments to Host B back-to-back. The first and second segments contain 80 and 40 bytes of data, respectively. In the first segment, the sequence number is 127, the source port number is 302, and the destination port number is 80. Host B sends an acknowledgment whenever it receives a segment from Host A.

a. In the second segment sent from Host A to B, what are the sequence number, source port number, and destination port number?

b. If the first segment arrives before the second segment, in the acknowledgment of the first arriving segment, what is the acknowledgment number, the source port number, and the destination port number?

c. If the second segment arrives before the first segment, in the acknowledgment of the first arriving segment, what is the acknowledgment number?

d. Suppose the two segments sent by A arrive in order at B. The first acknowledgment is lost and the second acknowledgment arrives after the first timeout interval. Draw a timing diagram, showing these segments and all other segments and acknowledgments sent. (Assume there is no additional packet loss.) For each segment in your figure, provide the sequence number and the number of bytes of data; for each acknowledgment that you add, provide the acknowledgment number.

P31. Suppose that the five measured SampleRTT values (see Section 3.5.3) are 106 ms, 120 ms, 140 ms, 90 ms, and 115 ms. Compute the EstimatedRTT after each of these SampleRTT values is obtained, using a value of $\alpha = 0.125$ and assuming that the value of EstimatedRTT was 100 ms just before the first of these five samples were obtained. Compute also the DevRTT after each sample is obtained, assuming a value of $\beta = 0.25$ and assuming the value of DevRTT was 5 ms just before the first of these five samples was obtained. Last, compute the TCP TimeoutInterval after each of these samples is obtained.

6、TCP 协议的流量控制机制（原理）

7、TCP 的连接管理

（1）TCP 的建立：三次握手

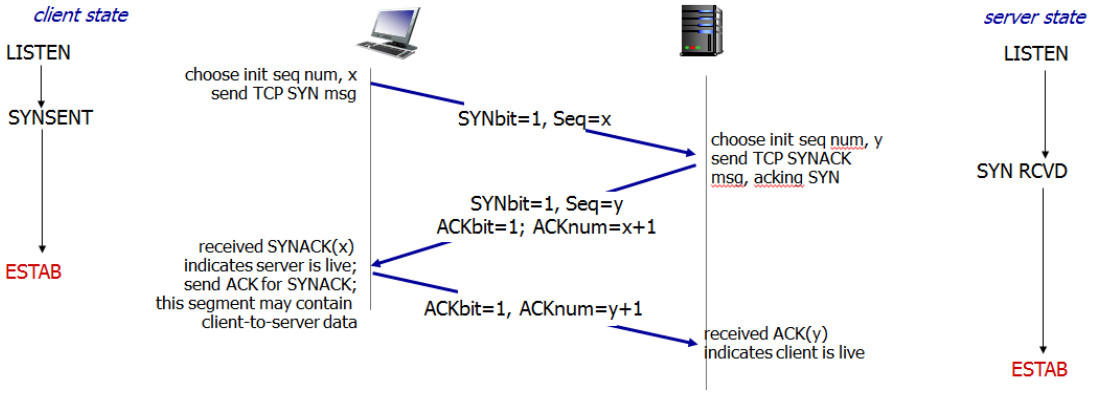
步骤 1：客户机向服务器发送 TCP SYN 报文段【表明准备好发送数据，不知服务器】

- 指定初始序号（随机产生）seq=x，
- 没有数据

步骤 2：服务器收到 SYN 报文段，用 SYNACK 报文段回复。【已知客户端准备好发送数据，表明自己准备好发送（接收）数据】

- 服务器为该连接分配缓冲区和变量
- 指定服务器初始序号（初始化自己的序号 seq=y）

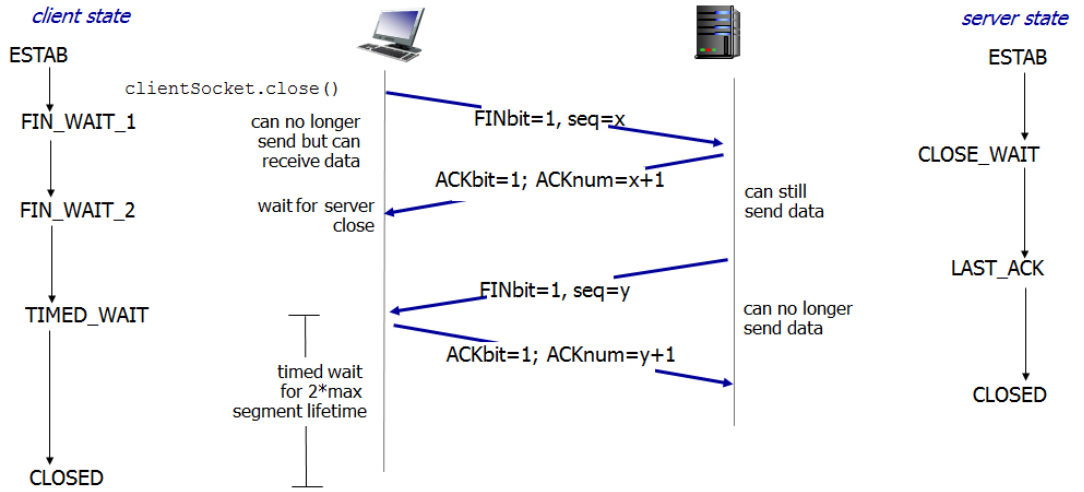
步骤 3：客户机接收到 SYNACK，用 ACK 报文段回复，可能包含数据【告诉服务器已经收到服务器确认（知道服务器准备好），发送数据】



为什么最后由客户端应答服务器确认消息的步骤不能缺少

我们说客户端和服务器在发送数据之前，需要完成的工作包括初始化序号，以及创建缓冲区，双方需要知道对方的序号，且确认序号是正确的（即客户端要知道服务器的序号，且确保服务器知道自己的正确序号【通过 SYBACK 可以确认】；服务器也需要知道客户端的序号，且确保客户端知道自己的正确序号【通过第三次握手的 ACK 消息告知服务器】）。因此不能省略第三次握手，否则服务器不能确保客户端知道自己正确的序号。

（2）TCP 的释放：四次挥手



步骤 1: 客户机向服务器发送 TCP FIN 控制报文段【告知服务器，客户端不再发送数据，但是可以接收来自服务器的数据】

步骤 2: 服务器收到 FIN，用 ACK 回答。关闭连接，发送 FIN，【告知客户端，服务器不再接收数据，但是仍然可以发送数据给客户端】

步骤 3: 客户机收到 FIN，用 ACK 回答，进入 “超时等待” – 将对接收到的 FIN 进行确认【收到服务器的结束消息，知道服务器不再发送数据，但仍然不会马上释放缓冲区，需要等待一个时间，因为服务器还可能有数据包正在网络中传输】

步骤 4: 服务器接收 ACK，连接关闭

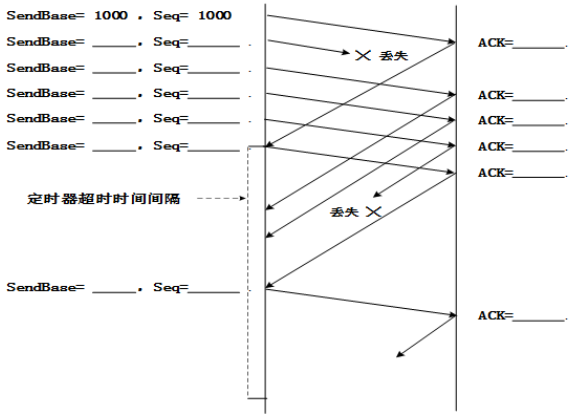
课堂练习题：

R15. 假设主机 A 通过一条 TCP 连接向主机 B 发送两个紧接着的 TCP 报文段。第一个报文段的序号为 90，第二个报文段序号为 110。

a. 第一个报文段中有多少数据?

b. 假设第一个报文段丢失而第二个报文段到达主机 B。那么在主机 B 发往主机 A 的确认报文中，确认号应该是多少?

假设主机A和主机B之间建立了TCP连接，并且主机A有大量的数据需要向B发送。发送发主机A支持快速重传，而接收方B会缓存正确接收但失序的报文段，每次发送的报文段的数据字段长度都为100字节。下面的描述中，Seq代表序号，ACK代表确认号，发送方窗口的基序号为SendBase，发送方窗口长度为500字节，请填写下图中各变量的值



8、TCP 协议的拥塞控制机制

结合 TCP 拥塞控制状态转移图

（1）早期的 Tahoe 机制：慢启动、拥塞避免

（2）目前的 Reno 机制：慢启动、拥塞避免、快速恢复（了解为什么引入快速恢复状态快速恢复状态的加入，为了能够更高效的利用网络的传输能力）

要能够结合图，掌握每种状态下，cwnd 的变化规则、因为什么事件会发生什么样的状态转移；

课堂练习

- 下列关于TCP拥塞控制机制描述错误的是_____。

A. 当TCP连接刚建立时，处于慢启动状态，此时，cwnd的值为1个MSS，每收到1个ACK确认，将cwnd的值增加1个MSS；

B. TCP使用的是端到端拥塞控制机制，而不是网络辅助的拥塞控制机制；

C. 当发送端连续收到3个重复的ACK确认，进入快速恢复状态。

D. 当cwnd的值大于慢启动阈值ssthresh时，进入拥塞避免状态，在该状态，每收到1个ACK确认，将cwnd的值增加1个MSS。

- 下列哪项不是TCP协议的特性_____。

A. 提供可靠服务　　B. 提供无连接服务

C. 提供端到端服务　　D. 提供全双工服务

第四章 网络层：数据平面

虚电路书上没有不要求

1、因特网的网络层提供的服务

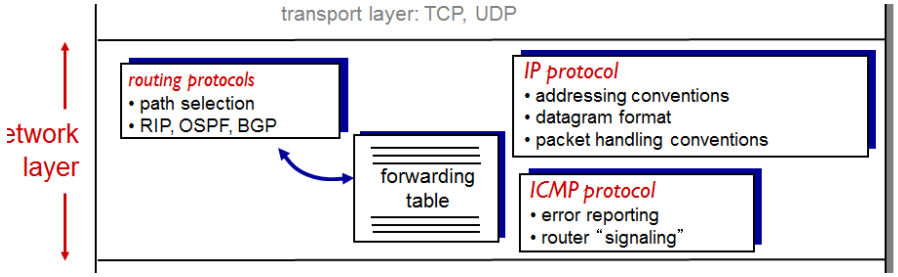
- 单一服务，即尽力而为服务(best-effort service) 。
- 分组间的定时不能被保证；
- 分组的接收顺序与发送顺序不一定相同；
- 传送的分组不能保证最终交付，即网络可能未向目的地交付分组。

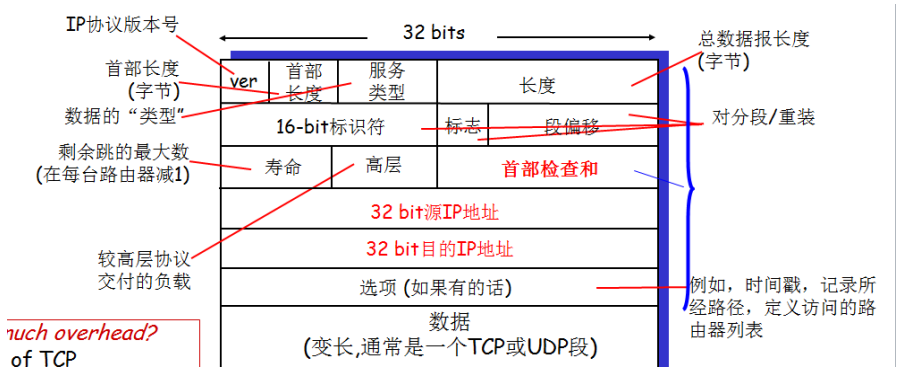
2、路由器的体系结构和组件的功能

输入端口、输出端口、交换结构（基于内存、基于总线、crossbar）、路由处理

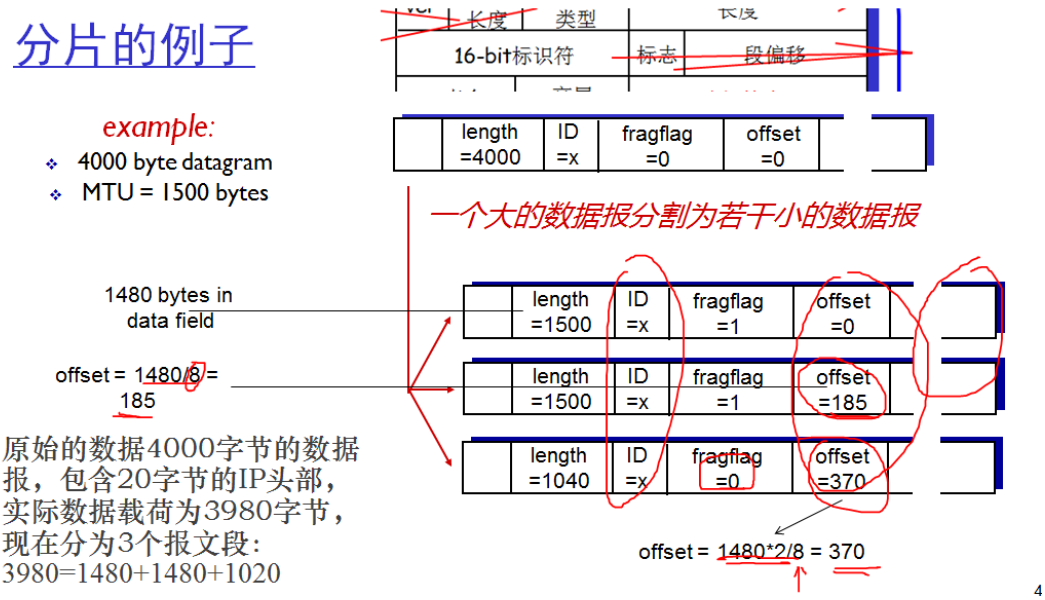
3、目的 IP 地址的转发规则：最长前缀匹配

4、网络层协议及网络层头部字段





5、IPv4 数据报分片和重组



4

6、IPv4 编址

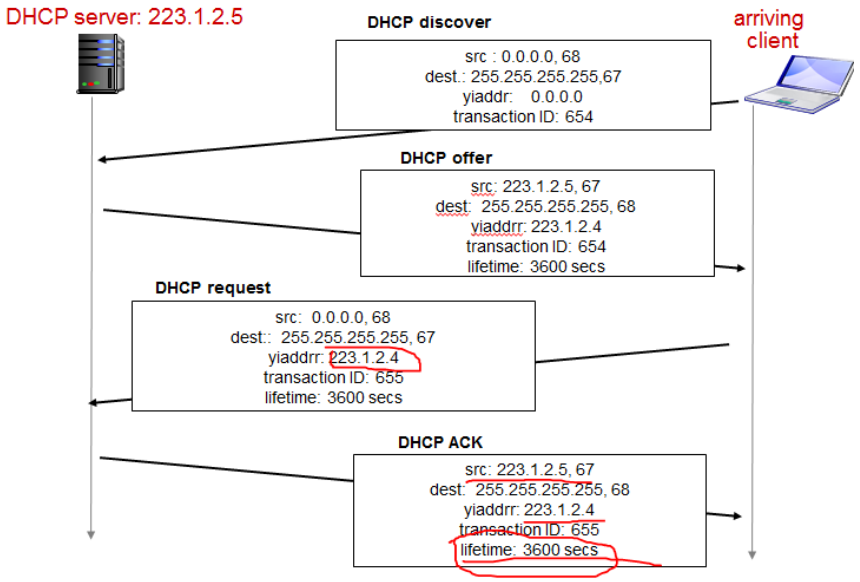
子网、子网掩码的概念，IPv4 寻址

7、子网划分

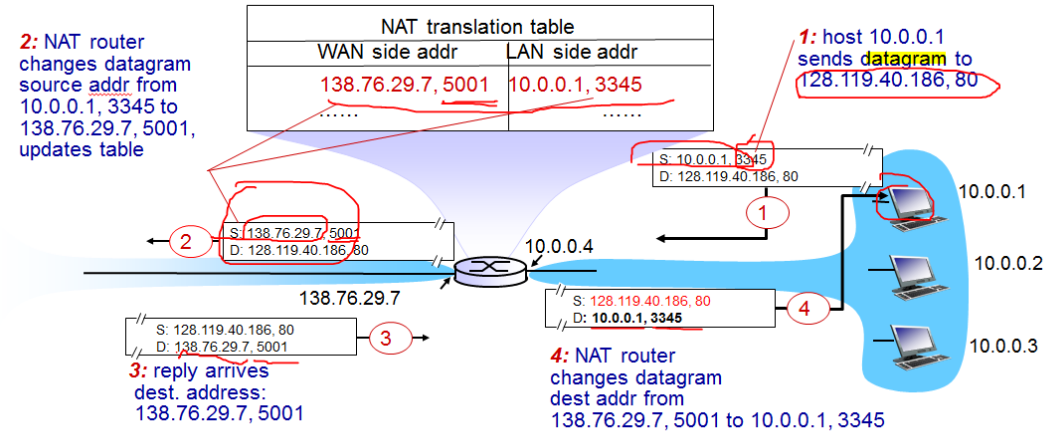
课堂练习题

P13. Consider a router that interconnects three subnets: Subnet 1, Subnet 2, and Subnet 3. Suppose all of the interfaces in each of these three subnets are required to have the prefix 223.1.17/24. Also suppose that Subnet 1 is required to support at least 60 interfaces, Subnet 2 is to support at least 90 interfaces, and Subnet 3 is to support at least 12 interfaces. Provide three network addresses (of the form a.b.c.d/x) that satisfy these constraints.

8、DHCP 动态地址配置（过程）

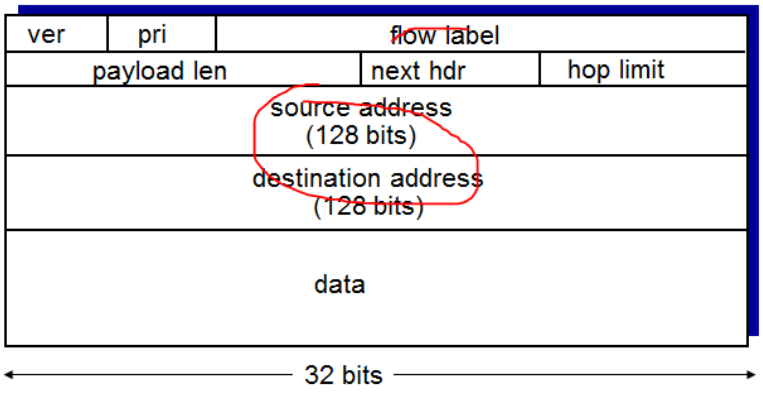


9、NAT 原理



* Check out the online interactive exercises for more examples: http://gaia.cs.umass.edu/kurose_ross/interactive/

10、IPv6 数据报格式



第五章 网络层：控制平面

1、路由算法：链路状态路由算法、距离向量算法

2、路由协议，简单的 OSPF(链路状态路由算法)、BGP（距离向量路由算法）、RIP（距离向量路由算法）

2、SDN 体系结构的关键特征：

（1）基于流的转发。（2）数据平面与控制平面分离。（3）网络控制功能：位于数据平面交换机外部。（4）可编程的网络。

3、OpenFlow 协议的作用。OpenFlow 协议运行在 SDN 控制器和（SDN 控制的）交换机或其他（实现 OpenFlow API 的）设备之间。

第六章 链路层

1、链路层是负责单条链路的数据传输，每条链路可以采用不同的链路层协议，例如一段链路是采用无线（802.11），另一段链路是有线的（以太网，802.3）。

2、链路层提供的功能：

（1）封装成帧，链路接入：封装数据报为数据帧，增加头部，尾部信息；如果是共享链路，接入链路；在数据帧头部中，用 MAC 地址来标识源和目的 MAC 地址，不同于 IP 地址；

（2）在相邻节点之间可靠传输数据帧（以太网是不提供的）；

（3）流量控制：用于控制发送节点向直接相连的接收节点发送数据帧的频率；

（4）差错检查：差错可能由信号衰减、噪声引入，接收方检测是否出现错误，通知发送方重传或丢弃数据帧；

（4）错误纠正：接收方标识和纠正比特错误，而不需要请求重传；

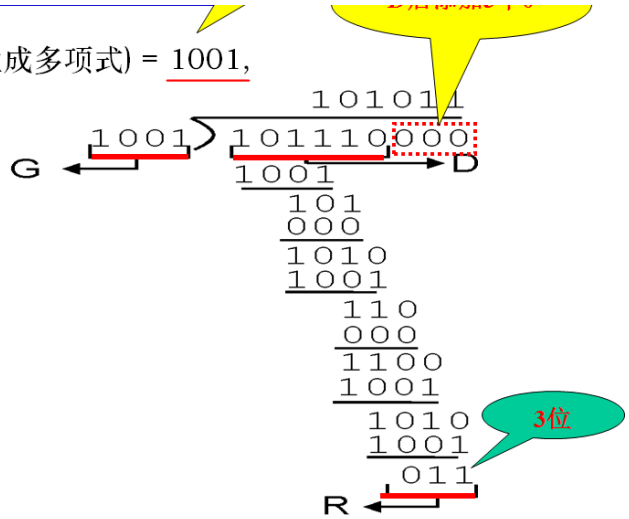
（5）半双工和全双工(half-duplex and full-duplex)：在半双工模式，链路的两个节点都可以发送数据，但是不能同时发送。

【注意区别以太网的数据链路层提供的服务，是有差异的】

3、三种主要差错检测技术：奇偶校验、校验和（UDP、TCP 校验和）、循环冗余检测（均要掌握）。

（1）循环冗余校验：已知发送的比特序列（能根据比特序列，写成多项式的形式），生成多项式（可以给比特序列或多项式的形式），请计算 CRC 校验码。【注意发送的序列是原始序列和 CRC 校验码的拼接】【CRC 检验码比生成多项式序列少 1 比特】

设 (数据) D = 101110,d = 6, G (生成多项式) = 1001,
r = 3



实际传输的数据形式是：
101110011

4、两种链路：点到点链路、共享链路（广播信道）

5、共享信道可能发生冲突，因此需要多路访问协议。三类多路访问协议如下：

（1）信道划分协议：TDMA、FDMA、CDMA

（2）随机访问（接入）协议：ALOHA（slot ALOHA、pure ALOHA）、CSMA【不带冲突检测】、CSMA\CD【带冲突检测的载波侦听】

CSMA/CD 的工作过程：

- 增加“载波侦听”和“冲突检测”两个规则。

  “先听后说”(listen before talk)

  “边说边听”(listen while talk)

- 基本原理：

传送前侦听，如果信道忙，则**延迟发送**；如果信道闲，则发送整个帧；

发送数据帧的同时进行冲突检测，一旦检测到冲突就立即停止传输， 尽快重发。

目的：缩短无效传送时间，提高信道的利用率。

（3）轮流协议：轮询协议（polling）、令牌传递协议（token passing）

6、以太网的 CSMA/CD 协议的运行原理：

（1）适配器从网络层获得一个数据报，封装成帧，准备发送；（2）如果适配器侦听到信道空闲，开始传输帧；如果检测到信道繁忙，将等待一段时间，直到侦听到信道空闲，开始传输帧；（3）在传输过程中，适配器会同时监听是否有其他适配器的信号能量；如果适配器在整个帧的传输过程中，没有监听到其他信号，则完成该帧的传输；如果监听到来自其他适配器的信号，则中止传输帧；（4）中止传输后，适配器会等待一个随机时间，重新执行步骤 2。关键是延迟的时间：

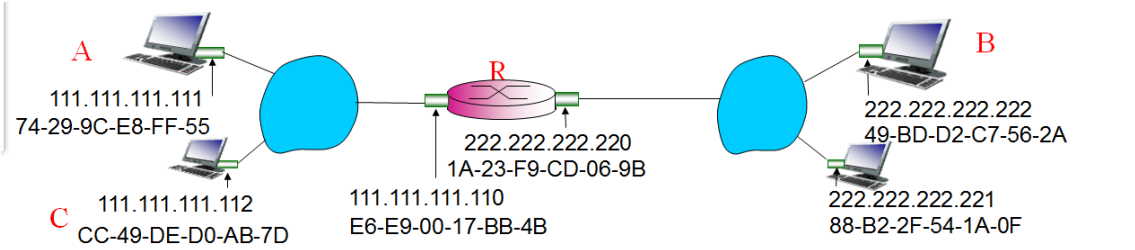
- 以太网的**二进制指数回退**
  - 当传输一个给定帧时，在该帧经历了一连串的n次碰撞后，结点随机地从{0,1,2….2^n-1}中选择一个K值， NIC waits K·512 bit times
  - 假设是100Mbps的以太网，那么发送512bit的时间是5.12*10-6秒
    - 第一次碰撞：{0, 1}
    - 第二次碰撞：{0, 1, 2, 3}
    - 第三次碰撞：{0, 1, 2, 3, 4, 5, 6, 7}
    - ……

K是等概率选择

7、链路层寻址

（1）MAC 地址：物理地址（48 比特），目的 MAC、源 MAC、广播帧目的 MAC 地址，在单条链路上发送和接收，依赖的是目的 MAC 地址。

（2）位于同一局域网的两台主机通信：

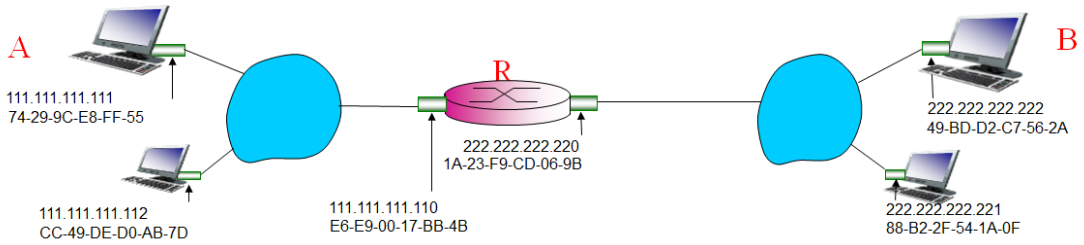


- 案例1：主机A发送数据报给主机C
  - 主机A的网络接口首先将数据报封装成数据帧

  目的MAC地址：CC-49-DE-D0-AB-7D，源MAC地址：74-29-9C-E8-FF-55
  - 如果A、C主机通过链路层交换机互联，则交换机收到数据帧后，会根据转发表确定数据帧的输出端口，如果目的MAC地址存在转发表，则转发到确定输出端口；如果转发表中没有对应MAC地址的转发表项，则将这个数据帧向所有端口转发(C/R的左侧端口)
  - 只有主机C的MAC地址与该数据帧的目的MAC地址匹配，因此接收。

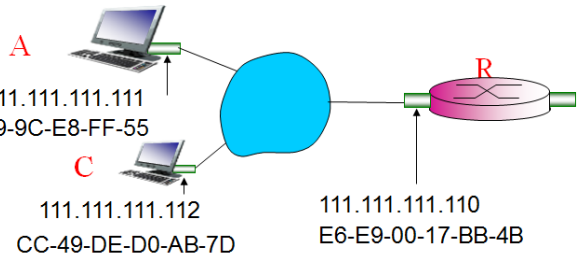
主机A怎么知道主机C的MAC地址?

（3）位于不同局域网的两台主机通信：



8、ARP 协议的工作过程

- 主机A希望发送数据报给主机C；
  - C的MAC地址不在A的ARP映射表中
- 主机A广播 ARP查询分组，其中包含C的IP地址
  - 目的MAC地址：FF-FF-FF-FF-FF-FF
  - 目的IP地址：111.111.111.112
  - 局域网中所有节点收到ARP查询分组
- 主机C收到ARP查询分组，返回响应分组给主机A，返回的数据帧包含有C的MAC地址（单播）
- 主机A在它的ARP表中缓存 **IP-to-MAC 地址对**，直到信息超时



ARP协议只能查找位于局域网内部的网络接口的IP地址对应的MAC地址！

9、以太帧的结构

10、以太网提供服务

以太网向网络层提供的服务。

- 无连接服务：通信时，发送方适配器不需要先和接收方适配器“握手”。
- 不可靠的服务：接收到的帧可能包含比特差错。
  - 收到正确帧，不发确认帧；
  - 收到出错帧，丢弃该帧，不发否定帧。
  - 发送适配器不会重发出错帧。
  - 丢弃数据的恢复是通过终端传输层的可靠数据传输机制来实现的
- 以太网的MAC协议：无时隙的CSMA/CD协议（二进制指数回退）

11、链路层交换机的工作原理（交换表的建立是通过自学习）

- 存储转发数据帧
- 检查达到的数据帧的 MAC 地址，有选择的转发数据帧到一个或多个输出链路，当数据帧被转发到一个共享网段时，使用 CSMA/CD 来访问共享链路

过滤和转发的原理

当交换机收到数据帧:

1. 记录到达链路和发送主机的MAC地址
2. 使用数据帧的目的MAC地址，在转发表中检索
3. 如果在转发表条目中找到对应的MAC地址
4. 执行{
   如果目的MAC地址对应的端口与数据帧的达到端口相同
   则 丢弃该数据帧
   否则 转发该数据帧到条目指定的端口
5. }
6. 否则，向除到达端口之外的所有端口转发(flood)

12、路由器、交换机、集线器的区别

- 集线器
  - 收到数据帧，会将其向自己的所有端口转发；
  - 不能隔离冲突域和广播域；
- 交换机
  - 收到广播帧，会将其向自己的所有端口转发；
  - 能够隔离冲突域，不能隔离广播域；
- 路由器
  - 收到广播帧，不会向其他端口转发；
  - 能隔离冲突域，能隔离广播域

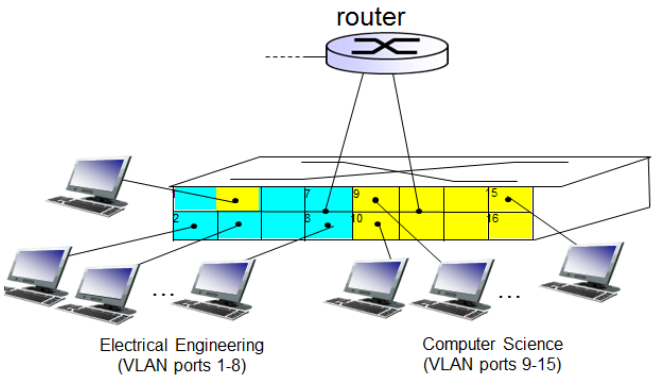
广播域（广播风暴）、冲突域

13、虚拟局域网

（1）VLAN 的划分方法：

- 按照端口号划分
- 按照 MAC 地址划分
- 按照网络层地址划分(IPv4)

（2）VLAN 的简单划分方式：



VLANs 可以跨越多个交换机