2012~2013 年第一学期 Web 总结 by 10CISers

整理者：陈天赐，高源，黄佳丽，黄思颖，刘静洁，邱实，余韧哲

目录：

01. 概述
02. 传输与分组
03. 局域网及相关技术
04. 广域网及相关技术
05. 网络互联
06. IP 协议和传输层协议
07. 因特网路由技术
08. 网络安全
09. 空
10. 空
11. World wide Web 技术
12. Web 编程
13. Web 信息发现
14. web 信息获取和处理
15. web 信息整合与应用

01 概述

一、 计算机网络基本介绍

1、 定义：多台自主计算机组成的互联系统

2、 目的：资源共享（硬件、软件、信息）、信息交换

3、 应用：分布式系统（自主计算机互联，一个操作系统（管理硬件的软件）统一管理）

4、 分类

（1） 按介质：有线无线

（2） 按技术：广播式、点到点

（3） 按使用范围：专用、公用

（4） 按拓扑结构：

- 总线型：结构简单、成本低、组网易；传输距离有限、故障检测困难；
- 环型：成本低、增减易、可用光纤；信息流向固定、节点故障引起全网故障；
- 星型：结构简单、组网易、管理易、故障独立；
- 树状：扩展方便、故障独立；适合于上下级界限严格的军事单位；
- 网状：冗余性高、可靠灵活、传输量大、容错性能高；结构复杂、管理难、成本高；

（5）按规模：局域网、城域网、广域网（分组交换机）

二、网络互联和 Internet

1、 网络互连：多个分组交换技术互联为一个整体的技术

2、 TCP/IP 互联网协议族：一组标准。

成功原因：对异构性的容忍（使用虚拟化方法，定义与网络无关的 分组格式、识别方案）。

3、Internet：物理网络按层次关系连接的逻辑网络；

（组成：主机、路由器、子网）

三、 计算机网络参考模型

1、 ISO/OSI 七层：物理层、数据链路层(帧传输)、网络层、传输层（可靠）、会话层、表示层、应用层；

2、 TCP/IP（第 5 节 PPT 中 P33 有更详细分层示意图）

层	任务	实例
物理层	定义接口的一些特性，如机械特性、电气特性、功能特性以及规程特性	
网络接口层	发送、接收分组	
互联层	数据分组格式、转发方式	IP
传输层	应用程序之间建立会话和信息通信服务，处理关于可靠性、流量控制和重传等典型问题	TCP、UDP TCP 提供一个一对一的、数据无差错的可靠性传输服务 UDP 则提供一个一对一或一对多、无连接、不可靠的通信服务，主要用于容许传递差错的话

		音和视频业务
应用层（合并 ISO 原 3 层）	应用程序使用互联网的规程	HTTP、FTP、SMTP

3、 **分层的好处**

- ✓ 每一层实现一种相对独立的功能，这样可以简化问题
- ✓ 每一层的设计都是独立的，它不必关心其他层的实现，只需知道下一层为它提供什么服务，以及它需要为上一层提供什么服务
- ✓ 由于技术的变化而使某层的实现发生变化时，不会影响其他层

4、 备注

- ✓ 协议可以跨层使用

四、World Wide Web

1、 定义：分布式的多种信息组合的超媒体信息系统，以统一的格式在网络上发布各类数据（包括图像、动画、电影、录像、声音和文本等等），简称 Web

2、 目的：建立一个适用于各种不同数据类型的统一用户界面

3、 相关的概念

- ✓ 超级链接（Hyperlink）：文件中一些特殊的文字和图形，用鼠标单击这些文字和图形时，会按照链接地址从当前文本跳到到所指向文本。含有超级链接的文本称超文本（Hypertext）
- ✓ HTML:用于编写超文本文件的语言。用HTML 编写的超文本文件称为HTML 文件，以 .htm 或 .html 为文件扩展名
- ✓ 网页（page）：在 WWW 服务器上发布的 HTML 文件。网站的首页称“主页”（Home Page）
- ✓ URL 的格式：协议：// 服务器主机名. 域名 [：端口号] / 目录名 / … / html 文件名

- ✓ Web 信息浏览工作过程：浏览器发出 URL 请求→WWW 服务器返回 HTML 界面。

4、 Web 信息特点：

- （1）海量性
  - 众多信息源在同一时间产生的信息即为海量
- （2）异构性
  - 信息的组织方式和存储格式各不相同，同时，信息的展现形式和传播形式也各式各样
  - 自由与共享的矛盾——自由为主
- （3） 动态性
  - 信息的产生和消亡非常快，并且有越来越快之趋势
- （4）自组织性
  - 信息组织具有一定的结构和规律

5、 思考

Web 的生命力在于互联互通

但是今天的 Web 上几个超大型应用彼此互筑堡垒，人为地建立起沟通的障碍

请思考：

Google、Bing、Yahoo 的未来

Facebook、Twitter、LinkedIn 的未来

Baidu、人搜、360、搜狗的未来

GFW 的未来

五、未来的发展

下一代互联网：

- 目前而言，尚难预测下一代互联网的完整模型
- 几个发展特点

  智能化--在组织和应用方面不断走向深入

  信息载体多样化，更加方便

  与传统行业结合，互相提升

  对传统生活方式和理念造成冲击

02 传输与分组

一、传输介质

1、 分类

（1）有线/无线

（2）能量类型： 电气的、光、电磁波

2、 导线：网络采用三种基本连线类型

✓ 非屏蔽双绞线（性价比高、易被窃听）

✓ 屏蔽双绞线：价格相对高

✓ 同轴电缆抗干扰能力强

二、 局域异步通信(比特率，波特率，带宽，两个定理，传输方式)

1、异步通信：发送数据之前发送方和接收方无需时钟同步的通信；
异步传输系统：两次传输间可以空闲任意长时间

✓ 发送前加额外信息（前导位）→RS-232 制定相关标准（起始位、终止位、每个信号的传输时长、考虑实际硬件限制）

2、传输速率

✓ 波特率：每秒硬件产生的电信号变化次数；

✓ 比特率：每秒传送的二进制位数，也叫“位速率”；

✓ 比特率 = 波特率 * [log2 电平数]

✓ 有关传输速率上限的两个定理（注：带宽——频率范围）

Nyquist 定理： D(比特率) = 2 B(带宽) log2 K(电压种数)

Shannon 定理： C(比特率) = B log2 (1 + S(信号) / N(噪声))

3、传输方式

✓ 按信息交换的方向性：单工、半双工、全双工

✓ 按字符各位是否同时传输：串行（网络）、并行（计算机内部）

三、 远距离通信

1、信号形式：连续的振荡信号(载波)，经调制（实现：调制解调器）发送。

2、传输方式：多路复用 频分~(FDM)：不同信道信号，不同载波频率(扩展频谱)
- 波分~： ----------，不同波长的光
- 时分~(TDM)：----------，不同时间(网络，统计时分复用)
- 码分~(CDM)：----------，不同地址码（低时延，电话业务）

四、编码

1、 NRZ（Non-Return to Zero）Encoding

✓ 1—高信号，0—低信号

✓ 问题 1：一长串的 0 和 1 会引起基线漂移（baseline wander）。接收方需要保持一个它看到的信号的平均值，以此区分高、低信号。但太多的 0 或 1 会使这个平均值发生变化

✓ 问题 2：时钟漂移。无论何时，只要有信号从 1 到 0 或者相反的跳变，接收方就知道这是在时钟周期的边界上。若长时间没有跳变就会导致时钟漂移，使接收方和发送方不再同步

2、 NRZI （Non-Return to Zero Inverted） Encoding

- ✓ 保持当前信号
- ✓ 1—发送方以当前信号的一个跳变来编码 1
- ✓ 解决了连续 1 的问题，但未解决连续 0 的问题

3、 Manchester Encoding

- ✓ 通过传输 NRZ 编码数据与时钟的异或值使时钟与信号明显合并：0—由低到高的跳变，1—由高到低的跳变
- ✓ 由于 0 和 1 都导致信号的跳变，所以接收方能有效地恢复时钟，同时也不会发生基线漂移
- ✓ 问题：信号跳变速率加倍，比特率是波特率的一半，编码效率仅为 50%

4、 Differential Manchester Encoding

- ✓ 1 — 信号的前一半与前一比特信号的后一半信号相同
- ✓ 0 — 信号的前一半与前一比特信号的后一半信号相反
- ✓ 特性与曼彻斯特编码基本相同

5、 4B/5B Encoding

- ✓ 目标：如何在解决基线漂移和时钟漂移的同时，使编码效率尽量高一些
- ✓ 思想：在比特流中插入额外的比特而打破一连串的 0 或 1
- ✓ 方法：用 5 个比特来编码 4 个比特的数据，然后再传给接收方
- ✓ 5 比特代码由以下方式选定：每个代码最多有一个前导 0，并且末尾最多有 2 个 0
- ✓ 这样在连续传送时，在传输过程中任何一段 5 比特代码，连续的 0 最多有 3 个
- ✓ 最后使用 NRZI 编码进行传输，就解决了问题
- ✓ 4B/5B 编码的效率为 80%

五、 分组、帧与差错检测(数据充填，检错和纠错)

1、 分组交换

- ✓ 数据分成分组，统计时分复用，保证所有资源公平、迅速地接入网络；
- ✓ 实现方式：物理帧(特定的分组格式)；
  帧格式：为保证帧可以包含任意数据(起始位与终止位标记)，需要修改数据——数据充填（字节充填、比特充填）

2、 检错和纠错

- ✓ 思想：发送冗余数据，保证检测和纠正。
- ✓ 常见检错方法：
  （1）奇偶校验：每个字节上增加一个附加位，使其“1”个数为奇/偶；
    - ✓ 用于低速传输
    - ✓ 二位奇偶校验(见讲义)检错能力更强

  （2）校验和：数据当作二进制整数，求和，发送
  （3）循环冗余码（CRC）：
    - ✓ 应用最广

【附：CRC 码】相关资料

CRC 校验原理

利用 CRC 进行检错的过程可简单描述为：在发送端根据要传送的 k 位二进制码序列，以一定的规则产生一个校验用的 r 位监督码(CRC 码)，附在原始信息后边，构成一个新的二进制码序列数共 k+r 位，然后发送出去。在接收端，根据信息码和 CRC 码之间所遵循的规则进行检验，以确定传送中是否出错。这个规则，在差错控制理论中称为“生成多项式”。

代数学的一般性算法

在代数编码理论中，将一个码组表示为一个多项式，码组中各码元当作多项式的系数。例如 1100101 表示为

$1\cdot x^6+1\cdot x^5+0\cdot x^4+0\cdot x^3+1\cdot x^2+0\cdot x+1$，即 $x^6+x^5+x^2+1$。

设编码前的原始信息多项式为 P(x)，P(x)的最高幂次加1等于 k；生成多项式为 G(x)，G(x)的最高幂次等于 r；CRC 多项式为 R(x)；编码后的带 CRC 的信息多项式为 T(x)。

发送方编码方法：将 P(x)乘以 x^r(即对应的二进制码序列左移 r 位)，再除以 G(x)，所得余式即为 R(x)。用公式表示为

$T(x)=x^rP(x)+R(x)$

接收方解码方法：将 T(x)除以 G(x)，如果余数为0，则说明传输中无错误发生，否则说明传输有误。(G(x)是变量，可根据用户的需要自行设计，但好坏区别，一般位数与数据长度相等，首位和末位为1)

举例来说，设信息码为1100，生成多项式为1011，即 $P(x)=x^3+x^2$，$G(x)=x^3+x+1$，计算 CRC 的过程为

$x^rP(x)=x^3(x^3+x^2)=x^6+x^5$　　左移三位

$G(x)=x^3+x+1$ 即 $R(x)=x$。

注意到 G(x)最高幂次 r=3，得出 CRC 为010。

如果用竖式除法，计算过程为（用异或计算）以 G(x)为准，左移它的最高次位（r）再除以它本身求余可得可得一个的位的 CRC 码

1100000/1011 =111000/1011 =10100/1011=010（校验码）

因此，$T(x)=(x^6+x^5)+(x)=x^6+x^5+x$，即 1100000+010=1100010

如果传输无误，$T(x)$ x^6+x^5+x ------ = --------- = x^3+x^2+x, $G(x)$ x^3+x+1无余式。回头看一下上面的竖式除法，如果被除数是1100010，显然在商第三个1时，就能除尽。

上述推算过程，有助于我们理解 CRC 的概念。但直接编程来实现上面的算法，不仅繁琐，效率也不高。实际上在工程中不会直接这样去计算和验证 CRC。

下表中列出了一些见于标准的 CRC 资料：

名称	生成多项式	简记式*	应用举例
CRC-4	x^4+x+1	3	ITU G.704
CRC-12	$x^{12}+x^{11}+x^3+x+1$		
CRC-16	$x^{16}+x^{15}+x^2+1$	8005	IBM SDLC
CRC-ITU**	$x^{16}+x^{12}+x^5+1$	1021	ISO HDLC, ITU X.25, V.34/V.41/V.42, PPP-FCS

CRC-32	$x^{32}+x^{26}+x^{23}+...+x^2+x+1$	04C11DB7	ZIP, RAR, IEEE 802 LAN/FDDI, IEEE 1394, PPP-FCS
CRC-32c	$x^{32}+x^{28}+x^{27}+...+x^8+x^6+1$	1EDC6F41	SCTP

* 生成多项式的最高幂次项系数是固定的1，故在简记式中，将最高的1统一去掉了，如04C11DB7实际上是104C11DB7。 ** 前称 CRC-CCITT。ITU 的前身是 CCITT。

备注：（1）生成多项式是标准规定的

（2）CRC 校验码是基于将位串看作是系数为0或1的多项式，一个 k 位的数据流可以看作是关于 x 的从 k-1阶到0阶的 k-1次多项式的系数序列。采用此编码，发送方和接收方必须事先商定一个生成多项式 G(x)，其高位和低位必须是1。要计算 m 位的帧 M(x)的校验和，基本思想是将校验和加在帧的末尾，使这个带校验和的帧的多项式能被 G(x)除尽。当接收方收到加有校验和的帧时，用 G(x)去除它，如果有余数，则 CRC 校验错误，只有没有余数的校验才是正确的。

(3) 名称 生成多项式 简记式* 标准引用

CRC-4 x4+x+1 3 ITU G.704

CRC-8 x8+x5+x4+1 0x31

CRC-8 x8+x2+x1+1 0x07

CRC-8 x8+x6+x4+x3+x2+x1 0x5E

CRC-12 x12+x11+x3+x+1 80F

CRC-16 x16+x15+x2+1 8005 IBM SDLC

CRC16-CCITT x16+x12+x5+1 1021 ISO HDLC,ITU X.25,V.34/V.41/V.42, PPP-FCS

CRC-32 x32+x26+x23+...+x2+x+1 04C11DB7 ZIP, RAR, IEEE 802 LAN/FDDI, IEEE 1394, PPP-FCS

CRC-32c x32+x28+x27+...+x8+x6+1 1EDC6F41

CRC 总结：

看了大半天终于看懂了，看来看书得积极主动一点：

CRC 说了那么多实则是用一个规定的多项式（假设最高次是 r,当然包含 r+1位）把要发送的数据左移 r 位后，再去除那个多项式，当然会得到一个余数（设为 r(x),）那么这个余数是 r 位的二进制数。最后把它填充到数据移出的空位上去，这样变可以发送了，至于发送了几位接收了几位的细节问题自己考虑好了。

再说接收：举例：你有一个9 用它除2后当然余1了，那么给你一个9+1呢，余数又会是多少，0，则正确，

就像我要发送 9，现在有一个 2，发现它计算后余 1，那么发送时我把 1 加到要发送的数据上一块发送，当你收到一个数后，再让它除以 2 ，得 0 就正确了，关键就在“2”上

03.局域网及相关技术：

1、 局域网技术概论

a) 直接点对点通信

- 优点

  每个连接独立安装，可使用任何合适的硬件

  独占线路，可以自由决定如何传输数据

  易于增强安全性和保密性

- 缺点

  需要的连接数过多，尤其是接入计算机数比较多时

b) 局域网定义:允许多台计算机**共享通信介质的网络**被应用于局域通信。

这样每个局域网都有一个共享介质，多台计算机都连接在该介质上，并**按顺序轮流**使用该介质传输数据

c) 共享网络只被用于局域通信，**在于技术和经济上的双重原因**

- 计算机之间在地理上的远距离会带来较长的延迟时间，而长延迟的共享网络是不合适的，因为它们要花费更多时间来协调共享介质的使用
- 提供远距离高带宽的通信信道要比提供同样带宽的短距离通信信道昂贵得多

d) 局域网重要性：局域网所连接的计算机要比其他任何类型的网络所连接的都要多

- 局域网被大量安装使用的原因

  经济上，局域网比较便宜并具有广泛的可用性

  “访问的局部性”使得对局域网有很高的需求

- 访问的局部性原理：计算机通信遵循两种不同的模式

  第一，计算机与邻近的计算机通信的可能性比与远距离的计算机通信的可能性大

  第二，计算机很有可能与同一组计算机反复通信

e) 局域网的基本组成

i. 网络硬件:网络服务器，网络工作站，网络接口卡，网络设备，传输介质（主要讲了以下方面）

1. 网络服务器：为网络用户提供服务和共享资源的网络节点。可以使各种计算机，每台服务器上至少安装一块网卡。
2. 网络工作站：用户能够在网络环境中工作，访问网络共享资源的计算机系统。网卡+操作系统+网络软件（不在网上操作时，可以作为独立计算机）

ii. 网络软件：网络系统软件、网络应用软件

f) 局域网特点：

- 局域网中数据以帧为单位传输；
- 局域网内一般不需要中间交换，其拓扑结构有总线型、星型和环型，故路径选择功能可大大简化，通常不设单独的网络层
- 覆盖有限的地理范围，传输速率高误码率低
- 通常是单位自己建设和拥有，易于维护和管理

g) 局域网拓扑性能比较

性能	星型	总线型	环型
传输速率	高	较高	较高
网络维护	容易	较易	较难
扩展能力	高	较高	较弱

h) 局域网协议标准：IEEE 的 802 协议集是关于局域网的，这些协议只涉及 OSI 参考模型的最低两层

✓ 数据链路层：逻辑链路控制子层（LLC 子层）、介质控制子层（MAC 子层）

✓ 物理层

具体：

1、物理层

2、介质访问控制子层 MAC：规定了局域网的介质访问控制方式、帧的检验序列产生和检验等

MAC 地址：网卡上的**全球唯一的 48 位**编码序列

作用：局域网上的计算机利用 MAC 地址表示自己和其他机器的**身份区分**

MAC 地址通常存储在网络接口卡 NIC 中

MAC 地址位于 OSI 参考模型的数据链路层

3、逻辑链路控制子层 LLC

屏蔽了各种 MAC 的差别，向其上层提供统一的数据链路服务处理两个站点之间帧的交换

i) **【重点】**尽量避免“冲突”的发生，解决“冲突”的方法：对传输介质进行控制通常采用分散方式，网络中的所有节点都参与对共享介质的访问控制

i. CSMA（带冲突检测的载波监听多址访问，802.3）

争用型：载波监听多路访问 CSMA 的技术，对电缆上有无载波进行监听，以确定是否有别的站点在传输数据。如果电缆空闲，该站点便可传输数据；否则，该站点将避让一段时间后再做尝试。这就需要有一种退避算法来决定避让的时间，常用的退避算法有 1-坚持、非坚持、 P-坚持三种

• 1-坚持算法

算法规则：⑴如果电缆空闲的，则可以立即发送。

⑵如果电缆是忙的，则继续监听，直至检测到电缆是空闲，立即发送。

⑶如果有冲突(在一段时间内未收到肯定的回复)，则等待一随机量的时间，重复步骤⑴～⑵。

这种算法的优点是：只要电缆空闲，站点就立即可发送，避免了电缆利用率的损失；其缺点是：假若有两个或两个以上的站点有数据要发送，冲突就不可避免

• 非坚持算法

算法规则为：

⑴如果电缆是空闲的，则可以立即发送。

⑵如果电缆是忙的，则等待一个由概率分布决定的随机重发延迟后，再重复前一步骤。

采用随机的重发延迟时间可以减少冲突发生的可能性。非坚持算法的缺点是：即使有几个站点都有数据要发送，但由于大家都在延迟等待过程中，致使电缆仍可能处于空闲状态，使用率降低

• P-坚持算法

算法规则：

⑴监听总线，如果电缆是空闲的，则以 P 的概率发送，而以(1-P)的概率延迟一个时间单位。一个时间单位通常等于最大传播时延的 2 倍。

⑵延迟一个时间单位后，再重复步骤⑴。

⑶如果电缆是忙的，继续监听直至电缆空闲并重复步骤⑴。

P-坚持算法是一种既能像非坚持算法那样减少冲突，又能像 1-坚持算法那样减少电缆空闲时间的折中方案

改进的 CSMA：

一旦监听到总线空闲，发送站点立刻进行发送，但在传输过程中仍继续监听总线，以检测是否存在冲突；一旦检测到冲突，就立即停止发送，并向总线上发一串阻塞信号，用以通知总线上其它各有关站点。这样，通道容量就不致因白白传送已受损的帧而浪费，可以提高总线的利用率

CSMA/CD 是英文 carrier sense multiple access with collision detection 的缩写，即“载波侦听多址访问/冲突检测”，或“带冲突检测的载波侦听多址访问”

算法规则：（本质上是改进了的 1-坚持型的）

监听总线，等待空闲时发送数据

当发生冲突时，每个计算机选择一个小于最大延迟 x（x 是每台计算机确定的值）的随机延迟；这样选择到最小延迟的计算机将首先发送帧

如果一台计算机遇到连续的冲突，那么在随后的每次冲突后，它都把 x 加倍

注：冲突退避算法限制了每个主机的退避时间从 1 个时隙到最多 2^10=1024 个时隙。当达到 10 次冲突后，随机等待的最大时隙数固定在 1023；但适配器通常继续尝试，在 16 次冲突后不再重发，向上层报告出错。

CSMA/CD 特例：以太网：最早的局域网，是一种基于**总线**的局域网，指的就是那些**采用改进了的 1-坚持的 CSMA/CD 协议**的局域网

• 以太网三种传输介质:双绞线、同轴电缆和光纤

• 以太网的好处：以太网极易管理和维护；价格低廉：电缆便宜，其他成本就是网络适配器

• 以太网的使用经验：以太网在轻载情况下工作良好，超过 30%后，冲突将使网络能力大量浪费

即使以太网适配器没有实现链路层流量控制，主机通常会提供一种端到端的流量控制机制，很少出现一台主机连续不断地把帧送到网上的情况

注：冲突退避算法限制了每个主机的退避时间从 1 个时隙到最多 2^10=1024 个时隙，因此，由中继器连接的多段以太网中，主机数不超过 1024 个。主机发送 64 个字节需要 51.2 微秒（64*8*1/10M=51.2us），所以往返延迟不能大于这个数值，否则 CSMA/CD 无法正确判断是否发生冲突。

j) IEEE802.5 标准：令牌环局域网

i. 定义：环型网是由一段段点到点链路连接起来的闭合环路，信息沿环路单向逐点传送；每个节点都有地址识别能力，一旦发现有本站地址，便立即接收信息，否则继续向下一站传送

ii. 工作原理:

1. 大概过程：令牌环网由一组用传输媒体串联而成的多个工作站组成（不能用以太网卡）；通过设置令牌来控制冲突问题；；；；令牌（Token）：具有特殊性质的帧。平时不停地在环路上流动；若各站无数据发送时，称为空闲令牌
2. 具体过程：

（一）截获令牌与发送帧

空闲令牌传送到正准备发送数据的工作站时，该站将空闲令牌截获下来

将空闲令牌的标志转变成信息帧的标志，此时令牌变为忙令牌

将要传送的数据字段加上去，构成要发送的非令牌帧，然后送到环上

二）接收帧与转发帧

非令牌帧每经过一站，该站的转发器便将帧内的目的地址与本站地址相比较

三）撤消帧与重新发令牌

当非令牌帧返回发送站时，源站对返回的非令牌帧进行检查，判断是否发送成功：

3. 缺点：容易失效
   - ✓ 因为连接在环上的每台计算机必须向下一台计算机传输帧，所以一台机器的失效能使整个网络都失效；

k) IEEE802.4 标准：令牌总线网

i. 与其他比较

总线网：接入方便，可靠性较高；当网络负载增加时，冲突急剧增加，吞吐量下降；实时性差

令牌环网：不存在冲突，实时性好，负载能力强；管理相对复杂，可靠性差

令牌总线网（综合两者的优点）：物理上：总线网　逻辑上：环形网

ii. 令牌总线网的工作原理

1. 首先，令牌总线网在物理布线上是总线方式；
2. 其次，在物理总线上建立一个逻辑环；
3. 和令牌环一样，在令牌总线中的站点只有获得令牌才能发送信息，通过令牌来控制各站对总线的访问；
4. 令牌按逻辑顺序传递，从高地址站传递给较低地址的站，又从最低到最高；
5. 各站有公平的访问权

iii. 网络中令牌的传送是按逻辑环路进行的，而数据的传送却是在两站之间直接进行的，这样的网络称为逻辑环网

1. 物理上：总线网络拓扑
2. 逻辑上：各工作站按一定顺序形成一个逻辑环
3. 逻辑环网与物理环网对比

- ✓ 物理环网：传送数据必须按环路进行，延迟长
- ✓ 逻辑环网：传送数据有直接通路，所以这种总线式逻辑环网延迟时间短

4. 逻辑环网与竞争型总线网对比
   - ✓ 总线网冲突增加，效率迅速下降，而逻辑环网没有冲突问题，在重负载时具有较高的效率
   - ✓ 总线网各站平等，访问和响应都具有随机性，属于概率性网，不能满足实时性要求；逻辑网引入优先权策略实现数据的优先传送,访

问时间和响应时间都具有确定性，因而具有良好的实时性。工业控制中首选令牌总线网

4. 无线局域网距离受限，它不能采用 CSMA/CD，采用 CSMA/CA
   - ✓ 源计算机在传输一个帧之前先发送很短的控制消息
   - ✓ 目的计算机接收到控制消息后，发送另一个控制消息表明已经准备好接收数据
   - ✓ 当源计算机接收到响应的控制消息后，它就可以开始发送帧
   - ✓ 在 CSMA/CA 中，控制消息的传输可能会发生冲突，但能够很容易地处理。当这种冲突发生时，发送者可以随机等待一段时间，然后重发控制消息。因为控制消息比数据帧要短得多，所以发生第二次冲突的可能性也要比传统以太网要小很多

2、 硬件寻址与帧类型标识

a) 硬件寻址：在共享式局域网上传输数据时，发送计算机利用**硬件地址**来标识哪台或哪些计算机应该接收某个帧
b) 硬件地址，或物理地址，介质接入地址：局域网上的每个站点都分配了一个唯一的数值
c) 局域网如何用地址过滤帧：使用物理地址。网络接口硬件处理帧的发送与接收的所有细节，并比较每一个接收帧的目的地址与本站的物理地址，丢弃不匹配的帧
d) 编址形式
   - ✓ 静态编址方案:硬件厂商对每一个网络接口硬件分配一个全世界唯一的物理地址。
   - ✓ 动态编址方案：当站点第一次启动时，它能自动给站点分配一个物理地址。
   - ✓ 可配置编址方案：可由用户设置物理地址的机制。
e) 广播：当一个应用广播数据时，网络上所有计算机都可接收到一个副本，每台计算机分配一个特殊的地址，称为广播地址
f) 组播：在局域网上只发送数据给一部分计算机
g) 标识帧：
   - ✓ 显式帧类型（explicit frame type）。指明类型信息是怎样包含在帧里的，以及数值是怎样用来标识各种帧类型的。
   - ✓ 隐式帧类型（implicit frame type）。网络硬件不在每帧中包含类型域，帧只包含数据。
h) 网络分析器(network analyzer):是一种用来确定网络系统是否运行良好的设备。它可以用来计数或显示共享式网络上传输的帧

3、 有线局域网技术

a) 网络接口卡（NIC）能支持多种布线方案
b) 连接多路复用器连：允许多台计算机通过一个收发器连接到网络上。计算机**不必**知道它是连接到收发器上还是连接到多路复用器上
c) 以太网的细网布线方案使用柔软的同轴电缆直接连接每台计算机，而不使用单独的收发器。粗缆与细缆在物理上是不同的，但它们有相同的电气特性
d) 集线器技术：连接多路复用器概念的扩展。集线器中的电子部件模拟物理电缆的特性，使整个系统象一个传统以太网一样运行。连接在集线器上的计算机必须有一个**物理以太网地址**，使用 CSMA/CD 并采用标准**以太网的帧格式**，与传输介质无关。

e) 从物理上讲，双绞线以太网使用星型拓扑。逻辑上讲，双绞线以太网的功能像总线。一种特定的网络技术可以采用多种布线方案，这种技术决定了逻辑拓扑；而布线方案则决定了物理拓扑。物理拓扑与逻辑拓扑可能不同。

f) IBM 令牌环：采用集线器布线

物理上是星型拓扑；逻辑上环型拓扑（速率高高成本 FDDI 也采用）

4、 局域网扩展技术

a) 局域网的距离限制---公平访问机制

i. 两个最常用的访问机制是 CSMA/CD 和令牌传递，它们的响应时间都和网络的大小成正比。为了达到较小的网络延迟，局域网的连接距离就会受到限制

ii. 另一个限制因素是硬件发射固定能量的电磁波。电信号在导线中传输时逐渐变弱，信号不可能被传输到无限远

iii. 局域网硬件是为固定的最大电缆长度而设计的

b) 扩展局域网的方法：光纤扩展---计算机和收发器之间使用光纤和一对光纤调制解调器

✓ 主要优点：能连接远处的局域网，不必改变原来的局域网和计算机。由于光纤的延迟短，带宽高，它能在几公里的范围内正常地工作

c) 中继器：只是放大接收到的信号，并将放大后的信号进行转发[解决了电子信号在传输时会衰减

✓ 限制：一对工作站之间的中继器超过四个，网络便不能正常运行

✓ 缺点：不了解一个完整的帧。

d) 网桥：能处理一个完整的帧（因此是数据链路层设备）

✓ 工作过程：混杂模式：侦听每个网段上的信号，当它从一个网段接收到一个帧时，网桥会检查并确认该帧是否已完整地到达，然后根据需要就把该帧传输到其他网段。网桥能够隔离故障

✓ 桥接局域网上任何一对计算机都能互相通信，计算机**不知道**是否有网桥把它们隔开

✓ 帧过滤【最有用的功能】：在需要时网桥才转发帧
自适应的网桥检查所接收到的每个帧的帧头物理地址。网桥用源地址自动确定发出帧的计算机的位置，用目的地址来决定是否转发该帧

✓ 桥接网络的传播原则：稳定状态下，网桥对每个帧只在必要时转发

✓ 把交互频繁的计算机连在同一个网段上能提高桥接网的性能，网桥也能用来连接距离较远的计算机。

e) 远程桥接：租用串行线路（ leased serial line）来连接站点，或者租用卫星频道来连接【传输速度不同，有缓冲功能】

f) 网桥环和分布生成树
决定哪些网桥转发帧【DST 算法】

g) 交换：以太网交换机（或称第 2 层交换机）提供多个端口，可以转发帧而不仅仅是转发信号，可以看做是用网桥连接多个局域网网段
优点：提供最大的性能：交换机允许多对计算机间同时交换数据
应用：和集线器结合使用：把集线器连到交换机的每个端口上，然后把计算机连到集线器上，这样，每个集线器看上去就像一个局域网网段，而交换机看上去像连接所有网段的网桥

作业：

可能将以太网和 802.5 环桥接起来吗？为什么？

不能，IEEE 802.5 等属于以太网标准，而以太网不是一种具体的网络，是一种技术规范，定义了在局域网（LAN）中采用的电缆类型和信号处理方法。

CSMA/CD 为什么要使用一个随机延迟？

为了让多个计算机在发送信息时候不再冲突。

为什么在无线 LAN 中使用 CSMA/CA

无线 LAN 中计算机的距离跨度大于信号的传播范围

交换机和集线器哪个更好？

交换机具有交换功能，不会导致网络泛宏，而集线器会导致整个网络的数据包以广播的方式转发给集线器索连接的所有设备

网桥能够将 wifi 网络接入以太网么？交换机可以么？

不能。网桥或交换机作用于 MAC 子层，如果要连接不同传输介质的网络，那这些网络必须工作在相同高层协议下。

第四讲：广域网及相关技术

1、广域网技术基础

a) 概念：一个 WAN 可通过互连一系列站点构成，每个站点都有一定数量的计算机。

b) 广域分组交换系统的基本模式：存储/转发（store and forward）式交换，这个模式用分组交换机来进行

c) 基本构成：分组交换机，广域网由一些分组交换机互连而构成，然后将计算机连接在交换机上

- ✓ 分组交换机之间：较高速度　分组交换机与计算机之间：较低速度
- ✓ 增加广域网的的容量：加入计算机或者新的分组交换机
- ✓ 分组交换机构成：一台连接本地计算机的第 2 层（数据链路层）交换机，一个连接其他站点的路由器
- ✓ 工作原理：
  - i. 为完成存储/转发功能，分组交换机必须在存储器中对分组进行缓冲：当分组到达时，分组交换机的输入/输出硬件把一个分组副本放在存储器中并通知处理器，然后进行转发操作
  - ii. 处理器检查分组，决定应该送到哪个接口，并把分组输送到输出硬件
- ✓ 使用储存/转发的好处
  - i. 使分组以硬件所可容许的最快速度在网络中传送
  - ii. 如果有许多分组都必须送到同一个输出设备，分组交换机能将分组一直存储在存储器中排队，等待该输出设备准备好发送
  - iii. 分组不会在存储器中停留时间过长，但如果有很多计算机要同时发送分组时，就会增加延迟

d) 广域网的地址

i. 层次地址方案：第一部分表示分组交换机，第二部分表示连到该交换机上的计算机

ii. 下一站转发技术：仅包含关于分组到达目的地的下一站信息

- ■ 源地址独立性：仅依赖于分组的目的地址，使计算机网络中的转发机制更紧凑和更有效

iii. 路由

- ✓ 路由:转发一个分组到下一站的过程，分组交换机都必须有一张路由表
- ✓ 过程:首先检查分组目的地址中的第一部分(对应于分组交换机的那部分)；如果它与该交换机相一致，就利用第二部分地址把分组发送到计算机。否则，利用该地址在路由表中选择下一站
- ✓ 默认路由:广域网系统都允许路由表使用一个单项来代替那些具有相同下一站的项
- ✓ 路由表计算：
- ✓ 静态路由：分组交换机启动时由程序计算和设置路由，此后路由不再改变
- ✓ 动态路由：分组交换机启动时由程序建立初始路由，当网络变化时随时更新【大型网络】
- ✓ 路由选择算法的设计目标：最优化、简单性与低开销、强壮性和稳定性、快速收敛、灵活性

2、 **接入与互连技术**

a) 通信过程
- ✓ 远程通信：数据的远距离传输
- ✓ 最后一英里：本地用户线路

b) 数字线路：例如电话线路、**光载体线路、同步光网络**

c) 因特网接入技术（Internet access technology）：因特网用户和因特网服务提供商之间的数据通信技术【企业、**居民用户**】

1. **传统的“宽带”和“窄带”：分界是 128Kbit/s**
2. ADSL 好处：**现存的双绞线模拟信号电话线路上，实现了（相对）高速数据通信。它允许数据传输和传统电话同时使用【下行比上行快】**
3. 缺点：**缺少屏蔽使得导线对于干扰非常敏感**
4. 其他技术：CATV 调制解调器、光纤电缆混用、光纤到街道

3、 **网络所有权、服务模式和性能**

a) **私有网络[公司个人]和公用网络[运营商]**

i. **常见网络运用：**
- ✓ **大多数局域网：私有网络**
- ✓ **广域网：几乎所有公用网络 ，大单位也可拥有连接多个地点的计算机的私有广域网**
- ✓ 优缺点：
- ■ **私有网络**
  优点：拥有者具有对技术决策方面的完全控制权
  缺点：大型私有网络在安装和维护方面都很昂贵
- ■ **公用网络**
  优点：灵活性和采用最新联网技术的能力
  缺点：使用者无法完全控制

b) **VPN：虚拟私有网络。它允许具有多个站点的公司拥有一个假想的完全私有的网络，而使用公用网络作为其站点之间交流的传输线路**
- ✓ 使用：
  一套特殊的硬件和软件系统，该系统安放在公司的私有（即内部）网络和公用网络之间
  每个 VPN 系统必须配置好该公司的其他 VPN 系统的地址，使软件只在这些 VPN 系统之间交换分组
  为保护隐私， VPN 还在每个分组发送前进行加密

c) 网络分类：

i. **面向连接型服务**
- ✓ **两台计算机在传输任何数据之前必须通过网络建立一个连接**
- ✓ **一旦建立连接，两台计算机即可交互传输数据**
- ✓ **当通信完成后必须终止连接**
- ✓ **不会因网络出现拥塞而丢失，也不会乱序**

ii. **无连接型服务【在恶劣的环境下仍可工作】**
- ✓ 网络随时都可以接收主机发送的分组（数据报）
- ✓ 网络为每个分组独立地选择路由

- ✓ 网络只是尽最大努力地将分组交付给目的主机，但对源主机没有任何承诺
- ✓ 无连接型网络提供的服务是不可靠的，不能保证服务质量

iii. 比较：

- ✓ **面向连接型（虚电路）服务模式**

  主要优点：记帐方便而且在连接中断时能立即告诉通信的计算机（例如当硬件不能正常工作时）
- ✓ **无连接型（数据报）服务模式**

  主要优点是初始开销小—无连接网络允许计算机直接发送数据，而不必等待连接

  无连接系统中的故障可能不被发现—计算机在网络故障发生后仍继续发送分组

iv. 运用：

- ✓ 局域网的基本技术如以太网、令牌环网和 FDDI 都采用无连接服务模式。
- ✓ 在公用广域网中，面向连接及无连接服务模式都得到了应用

v. 网络性能特征：

- ✓ **延迟：计算机间传送一位所需的时间；有传播延迟、接入延迟、交换延迟和排队延迟等**
- ✓ **吞吐率：网络每秒可传送的位数；是对网络容量的度量**
- ✓ **延迟与吞吐率之间的关系：延迟与吞吐率并不独立—随着网络业务量的增加，延迟将随之增加；当吞吐量接近容量的 100%时，网络将会经受严重的延迟**
- ✓ **抖动是对延迟变化量的度量，它是数据网络中越来越重要的性能指标**

4、 X.25、帧中继和 ATM

a) **X.25 用途：指明数据终端设备和数据电路终结设备之间的接口规程，以便访问一个公共的或专用的分组网络**

- ✓ **X.25 对应了 OSI 体系结构的下三层**
- ✓ **LAPB 是 X.25 的数据链路层协议，其他协议的数据（如 IP、IPX 等）可以封装在分组中通过 X.25 传送**
- ✓ **X.25 支持纠错和诊错，因此对于那些处在恶劣的高噪声环境下而要求高可靠传输的应用来说十分理想**
- ✓ **从其展示的性能而言，X.25 代价算是非常昂贵，目前已经被其他 WAN 技术所取代**

b) 帧中继：**一种快速分组交换技术，是改进了的 X.25 协议【对应物理层和链路层核心层】【被 ATM 代替】**

i. 三种帧：信息帧、监视帧、无编号帧、

ii. 缺点：**在提供更高速访问链路上能力不足；缺乏对音视频等多媒体应用的支持，它仅限于传输数据（尤其适合来自 LAN 网段数据）**

c) **ＡＴＭ：【面向连接型】**

i. **ATM 作用：来同时满足话音、视频和数据传输三方面应用**

ii. **划分成很小的、固定长度的分组，叫做信元**

iii. **过程略：觉得好麻烦不会考这么细的嗯**

iv. **缺点：昂贵、连接建立延迟、有信元税、服务要求规范、缺乏有效的广播手段、QoS 的复杂性、缺乏与其他技术的可交换性**

作业和思考：

- ■ **论述：桥接局域网为什么不能被看作是广域网**

因为带宽限制决定了桥接网不能连接任意多个站点内的任意多台计算机。广域网可以连接任意多个站点内的任意多台计算机，桥接局域网不能连接任意多个站点内的任意多台计算机。所以桥接局域网不能被看作是广域网。

- **广域网与共享式局域网的区别？最本质的不同是什么？**

- **广域网与交换式局域网的区别？最本质的不同是什么？**

1、 补充：交换式局域网与共享式局域网的主要区别？

利用集线器连接的局域网叫共享式局域网，利用交换机连接的局域网叫交换式局域网。

2）交换式局域网与共享式局域网的区别

交换式局域网	共享式局域网
集线器连接	交换机连接
独享传输通道	共享传输通道
独享带宽	共享带宽
每个站点带宽固定	一个碰撞域的系统带宽固定
系统总带宽=B * N	每个站点平均带宽=系统带宽/N
同时允许多对站点通信	同时只能一对站点通信
交换机端口之间不受 CSMA/CD 约束	受 CSMA/CD 约束

广域网与局域网最本质区别在于：传输距离的远近

第五讲：网络互联

1. 协议与分层

※协议的目的：用网络软件（而非硬件）控制通信。

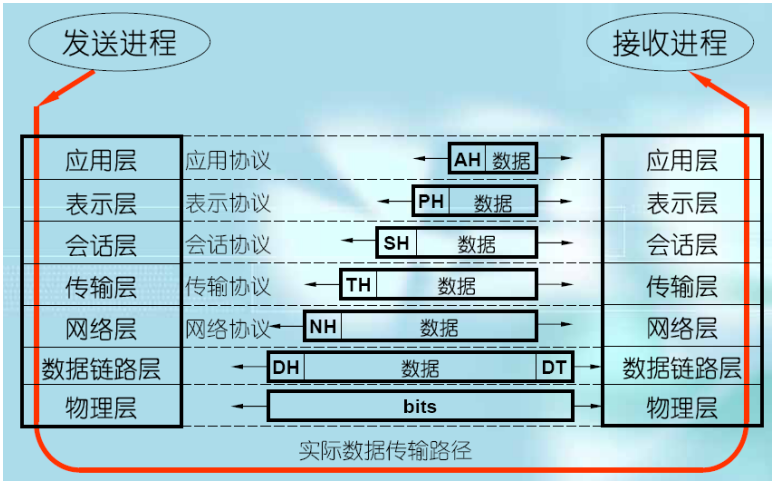
网络协议(计算机通信协议)：规定计算机信息交换中消息的**格式和含义**的协定。大多数应用程序和用户同协议软件打交道，而不是直接同网络硬件打交道。

协议系列(协议族)：为保证协议很好地协同工作，不能孤立地开发每个协议，而是要将协议设计和开发成**完整的、协同的集合**。

分层模型：帮助设计者控制协议软件复杂性的基本工具。通过分层可以把复杂的通信问题**划分成若干不同的部分**，然后设计者可以每次集中解决一个部分。

分层原理：在目的端的第 N 层上，要把源端第 N 层上进行过的变换，进行逆变换。这是分层设计的基础。

OSI 模型的数据传输：



栈：分层模型每一层对应于一个软件模块，**模块集总**称为栈（stack）。

理论上说，发送的数据在发送机上向下通过栈的每一层，在接收机上向上通过栈的每一层。不同栈的协议不能交互。

协议采用的通用技术：

使用排序来处理乱序和重复分组：无连接网络**不保证顺序**；硬件设备操作失误可能导致**重复的分组**

使用确认和重发来处理丢失分组

使用唯一的会话标识符来防止重传：避免前次会话对后次会话的干扰

使用停-等式协议或滑动窗口机制来控制流量（以下展开）

使用降低速率来处理网络拥塞（以下展开）

数据过载：当一台计算机通过网络发送数据的速度比目的计算机接收数据的速度快时，就出现了数据过载，从而导致数据丢失。

流量控制：解决数据过载问题的技术。

停-等模式

方式：每发出一个分组便等待接收方的回答；当接收方准备好接收下一个分组时，发送一个**控制报文**，通常就是某一种形式的确认。

特点：避免了过载；降低了网络带宽的利用率。

滑动窗口模式

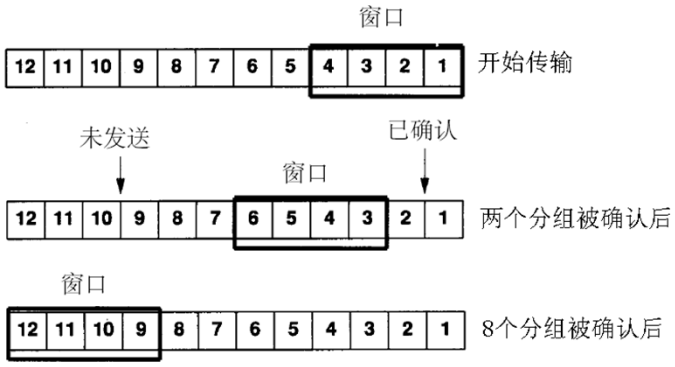
方式：程序设置发送方和接收方使用固定的**窗口尺寸**，这是在收到确认前可以发送的最大数据量；

发送方在开始发送数据时，提取数据填入第一个窗口，并发送每个分组的副本。如果有可靠性要求，发送方应保留一份副本，以备万一需要时重发；

接收方必须准备好缓冲区空间以接收整个窗口。当分组顺序到达时，接收方把分组传给应用程序，并返回一个确认给发送方；

当确认到达后，发送方丢弃已被确认的副本，并发送下一个分组。

特点：可以通过调节窗口大小充分利用可用的硬件带宽，获得**高吞吐率**。



滑过发送数据的一个4分组窗口

网络阻塞：

阻塞处理思路：让分组交换机通知**发送方**

①分组交换机发送一个特殊报文给分组的源发者

②分组交换机给每个由于拥塞而产生延迟的分组头部设置一个码位，接收该分组的计算机如果发现分组头部中置了该码位，就在确认报文中加入有关消息来通知源发者

阻塞估计：分组丢失(因为现代网络中大多数的分组丢失是由于拥塞而非硬件故障引起）

阻塞相应机制：降低分组传输速率

协议设计的注意事项：

①通盘考虑协议系列整体(因为协议机制之间相互作用，如流控机制和拥塞机制)

②仔细选择细节(如序列号域的大小)

2. 网络互联的概念

※网络互联的动机：**通用服务**概念，在**不同物理**网络间**任意通信**。

※限制：不同的**网络硬件、分组格式和物理编址**

网络互联：硬件（路由器）+软件=互联网

※因特网是最大的互联网

路由器：专门完成网络互联任务的**专用计算机**，可以将多个使用不同技术（包括不同的**介质、物理编址方案或帧格式**）的网络互联起来。

3. 互联网体系结构、地址

互联网基本结构：一组通过路由器连接起来的网络。

※很少使用单个路由器连接所有网络，原因：单个路由器的处理器不足以处理巨大通信

量；多个路由器的冗余能改善互联网的可靠性。

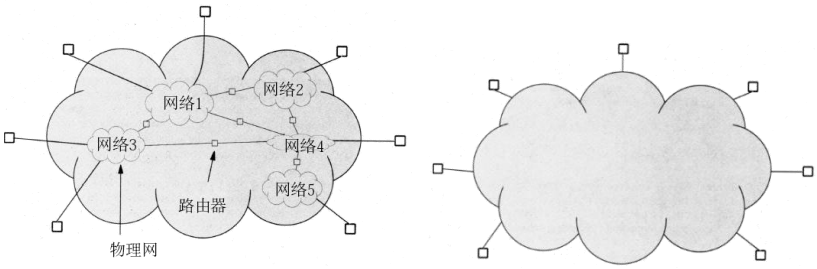
互联网基本要素：网络的数量和类型，用于互联的路由器数量，具体的互联拓扑结构。

※拓扑结构的具体细节依赖于物理网的带宽、预期的通信量、单位的可靠性要求，以及路由器硬件的费用和性能等。

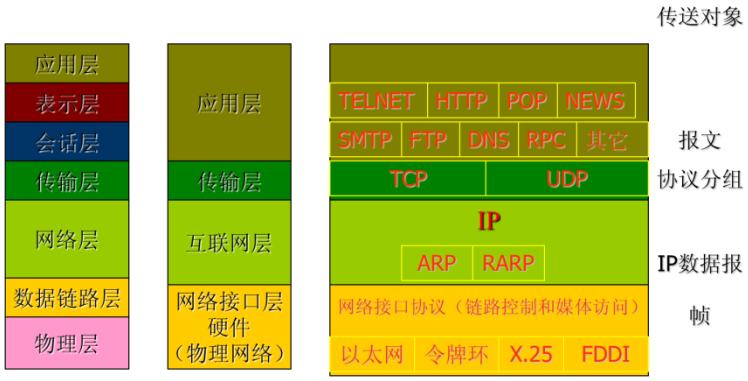
互联网协议：实现异构网络通用服务的协议，具体体现为**协议软件**。

※互联网中的每台计算机和路由器都必须运行协议软件，该软件能使应用程序交换分组。

作用：隐藏底层**物理连接**的细节，而着重于通过零个或多个路由器**将每个分组转送到目的地**，使互联网能够被看成一个**单一的、无缝的**通信系统。



TCP/IP 协议：Internet 的标准通信协议



① **网络接口层(网络访问层)【各种通信网络与 TCP/IP 之间的接口】**：包含 OSI 模型的数据链路层和物理层，负责在网络中**发送和接收 TCP/IP 数据分组**。TCP/IP 的设计不受网络访问方法、帧格式和媒体的限制，所以 TCP/IP 可用来连接不同的网络类型。

② **互联层【负责不同网络间的通信】**：对应于 OSI 参考模型的网络层，定义了互联网中**传输数据分组的格式**，以及从一个源点通过一个或多个路由器到达宿点的**数据分组转发机制**，包括寻址、封装和路由功能。核心协议是 IP，提供**相邻节点**之间的数据传送和为数据传送提供**正确的路径**，实现了主机之间相同格式数据的传输，但不能保证数据分组在传输中不会出现差错。

③ **传输层【提供应用程序间的通信】**：包含 OSI 传输层和部分会话层的功能，在两个主机之间**建立会话和信息通信服务**，处理关于**可靠性、流量控制和重传**等典型的问题。核心协议是传输控制协议 TCP 和用户数据报协议 UDP：TCP 功能包括分组重发技术、时序调整和拥塞控制机制等，提供一个**一对一的、数据无差错**的可靠性传输服务；UDP 则提供一个**一对一或一对多、无连接、不可靠**的通信服务，主要用于不要求数据报顺序到达的传输。

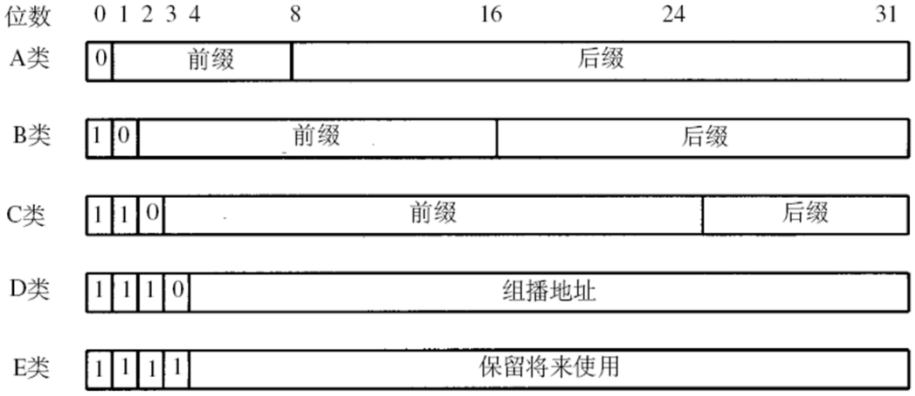
④ **应用层【包含所有的高层协议】**：定义了**应用程序**使用互联网的规程，内容包括处

理该层协议、有关表达、编码和对话控制等。常见协议有：TELNET、HTTP、FTP、SMTP、POP 等。

IP 编址：IP 协议规定的抽象编址方案，给每台主机分配一个唯一的地址。

IP 地址：32 位=前缀（网络号）+后缀（网络中的主机号）

① 有类地址：网络大小 A(8 位前缀)>B(16 位前缀)>C(24 位前缀)



点分十进制表示法：8 位一组，W.X.Y.Z，各类地址 W 值如下：

类	值范围
A	0~127
B	128~191
C	192~223
D	224~239
E	240~255

特殊 IP 地址：

本地地址	32 位全 0
网络地址	网络前缀+后缀全 0，表示网络本身，包含其中所有主机
直接广播	网络前缀+后缀全 1，对指定网络中的所有站点进行直接广播，即将信息送给该网络号下的每一台主机
有限广播	32 位全 1，在本地物理网内进行广播（不过路由器）
回送地址	W=127，,做循环测试，将信息回传给自己
D 类、E 类	D 类：多址通信(组播)；E 类：保留将来使用

② 子网编址和无类编址：直接利用前缀和后缀在地址的**任意码位**上进行分界。例如，给有 9 台主机的网络分配 28 位长的前缀，其余 4 位作为主机后缀（可容纳 14 台主机）。

CIDR 表示法：在一个地址的后面附加一个斜杠符和一个用十进制数表示的掩码大小值，来指定与此地址相关的掩码，如 **128.10.0.0/28** 表示 28 位网络前缀和 4 位主机后缀。

※地址掩码：32 位的**前后缀分界值**，1 表示前缀，0 表示后缀，把目的地址和地址掩码进行“**逻辑与**”操作，直接得到目的地址的网络前缀。

聚合分址：为多个网络分配连续的 IP 地址，使得一个 CIDR 记录就能表示这多个网络（最高若干位均相同）。

路由器与 IP 寻址原理：一个 IP 地址并不标识一台特定的计算机，而是标识一台计算机和一个网络之间的**一个连接**。一台连接多个网络的计算机（例如路由器）必须为**每个连接**分配一个 IP 地址。

地址解析：将计算机的**协议地址**(IP 地址)翻译成等效的**硬件地址**的过程。主机或路由器当需要向**同一物理网络内**的另一台计算机发送数据时，要进行地址解析。

必要性：在特定物理网络中传输帧时，必须使用**该硬件设备的帧格式**，帧中所有地址都用**硬件地址**。

※一台计算机只能解析连在**同一个物理网络**上的计算机的地址，路由器能解析其**连接的每个网络**上的计算机的地址。

解析方法：

① 查表法。地址绑定或映射信息被存储在内存中的一张表里，**表中的每一项是一个二元组（协议地址，物理地址）**，当软件要解析一个地址时，直接查找。

② 封闭式计算法（Closed-form computation）。认真为每台计算机挑选协议地址，使得这些计算机的硬件地址可通过**简单的布尔和算术运算**，由协议地址计算出来，如硬件地址=IP 地址&0xff

③ 报文交换法（Message exchange）。计算机通过网络交换报文来解析一个地址，包括 a)通过向**专门服务器**发送解析请求而后服务器发应答报文和 b)**向全网广播请求**而后目标机器应答 两种方式。

查表法是广域网中最常使用的方法；封闭式计算用于动态编址的网络；报文交换用于静态编址的局域网。

特点	解析方法
适用于任何硬件	T
地址变化影响所有主机	T
协议地址不依赖于硬件地址	T，D
硬件地址必须小于协议地址	C
协议地址由硬件地址决定	C
需要硬件广播	D
给网络增加了通信量	D
最小延迟产生解析结果	T，C
实现复杂	D

三类地址解析方法的对比

T:查表法,C:封闭式计算法,D:动态报文交换法

地址解析协议(ARP)：定义了计算机交换的 **ARP 报文格式和处理 ARP 报文的规则**，规定了一个 ARP 请求报文是**全网广播**的，但响应报文却是**直接发送**的，主要用于将一个 IP 地址解析成一个以太网地址。

具体内容：

① 封装 ARP：将 ARP 报文嵌入在一个**硬件帧**中进行传输，即把它当作数据来传输；

② 识别 ARP 帧：帧头中的**类型域**会指出帧中含有一个 ARP 报文，**操作域**会指出 ARP 报文是请求还是响应。发送方在传送前必须为类型域指定相应的值，接收方必须检测每个输入帧中的类型域，若有 ARP 报文，还须检测报文中的操作域。

③ 接收 ARP 报文

a. 接收方从取出发送方的地址绑定信息，检查 cache 中是否存在发送方的地址。若已有，则用从报文中取出的绑定信息以替代过去保存的绑定信息；

b. 接收方检查报文中的操作域以确认报文类型，若是响应报文，接收方以前一定发送过一个请求并在等待所需要的绑定信息；若是请求报文，接收方比较“目

标协议地址”域与自己的协议地址，若一样，则回发一个 ARP 响应。

动态主机配置协议 DHCP：为帮助新加入某网络的主机获得 IP 地址的协议。
具体内容：主机启动时，广播一个 DHCP 请求，服务器则发送一个 DHCP 应答。管理员一般将固定地址分配给服务器，而将动态地址分配给其他主机。按需分配的地址由 DHCP 产生一个租用期。当租期满时，主机可以释放地址，也可以与 DHCP 服务器重新协商延长租期，但服务器拥有绝对的控制权。
DHCP 优化：

① 分组丢失或重复：主机没有收到响应，重新发送请求报文；收到重复的响应，则忽略多余副本。
② 缓存服务器地址，提高租期续约过程的效率。
③ 避免阻塞：DHCP 协议要求每个主机在发送（或重发）请求之前要等待一个随机时间。

4. IPV6

改革动机：

① IPv4 定义的有限地址空间将被耗尽
② 设备增多，需要地址配置自动化、简单化
③ 因特网主干网路由器有维护大型路由表的能力，可支持平面路由机制
④ IP 层安全需求：IPSec 协议不普及
⑤ 更好的实时 QoS（服务质量）支持的需求

改革难点：IP 的依赖性以及 IP 带来的后续惰性导致改变 IP 就会改变整个因特网
IPv6 特性：

① 庞大的地址空间以及层次化实现：128 位地址，多级子网地址分配方式
② 简化的报头和灵活的扩展
③ 网络层的认证与加密：全面支持 IPSec，用户的数据加密和校验报文的自主权
④ QoS 的满足：路由器可以标识同一数据流的分组
⑤ 对移动性的更好支持：动态获得呼叫/会话时间内的 IP 地址
⑥ 高效的层次寻址及路由结构 ：聚合分址；分段仅由发送主机进行
⑦ 增强的组播与流量控制
⑧ 自动配置技术
⑨ 用于邻节点交互的新协议：邻居发现协议实现相邻节点（同一链路上的节点）的交互管理

IPv4 向 IPv6 的过渡：

① 双栈机制：在一台设备上同时运行 IPv4 和 IPv6 协议栈
② 隧道机制：在装有双协议栈的网关站点中，将 IPv6 数据包封装在 IPv4 数据包内，由 IPv4 网络传输，到达隧道端点后解封还原为 IPv6 包
③ 转换机制：转换网关在 IPv4 和 IPv6 网络之间转换 IP 报头的地址，同时根据协议不同对分组做相应的语义翻译

第六讲：IP 协议和传输层协议

分组在互联网上的传递过程：源主机创建分组→目的地址放入分组头部→将分组送往相邻的路由器→路由器收到分组→使用目的地址选择下一个路由器并转发→分组到达能将分组传递给最终目的地路由器

※这种**无连接**的互联网服务其实是分组交换的一种扩展——允许发送方通过互联网传输单独的分组，分组本身包含用以标识接收方的信息。

1. IP 数据报

必要性：为克服不同网络的异构性，互联网必须定义一种**与硬件无关的分组格式**。

IP 数据报：能无损地在底层硬件中传输的**通用的、虚拟的**分组。

结构：以一个头部开始，后跟数据区（与硬件帧相同）。数据报头部中源地址和目的地址都是 IP 地址，大小可变，取决于发送数据的应用。

传输过程：

① 由于路由表中的每个目的地对应于一个网络，所以路由表中的项数正比于互联网中的网络个数；

② 路由表中每项列出目的地、掩码和下一站；

③ 传输时，如果((掩码[i] & D)==目的地[i])，就转发到下一站[i]；

④ 路由器计算出下一站的 IP 地址之后，IP 软件使用地址绑定技术将 IP 地址翻译成等效的硬件地址，以便装帧传输。

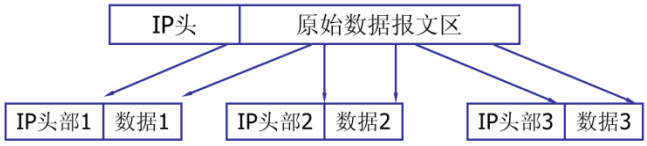
缺陷：IP 层会努力地尝试传递每个数据报（**“尽力传递”**），以满足操作各种类型的网络硬件，但可能出现延迟传送或乱序传送、数据报重复、数据的损坏、数据报的丢失。以上问题都需要高层协议软件处理。

数据报封装：（类比 ARP 报文封装）将整个数据报作为数据装入**帧的数据区**。帧中的目的地址是数据报下一站的地址（物理地址），由下一站的 IP 地址翻译得到。当封装在一个网络帧中的数据报到达时，接收方会将其从帧的数据区中取出来，同时**丢弃帧头部**。

数据报分片：当路由器收到一个数据报，其大小**超过所去网络的 MTU 时**，对数据报的分割操作。（MTU：最大传输单元，某种网络中一帧所能携带的最大数据量）

分片原则：

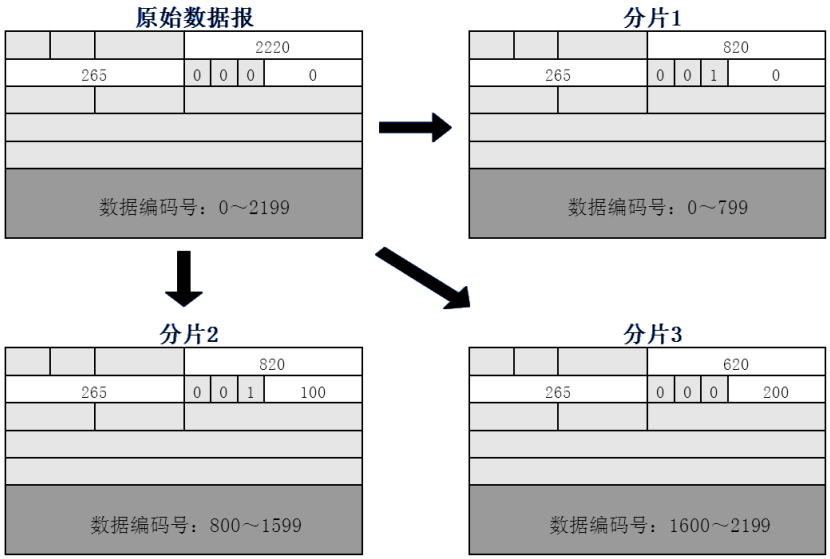
① 每一片都使用 IP 数据报格式，但只携带原数据报的一部分数据；



② 一个数据的所有片的**标识域**有相同的值(标识 ID 值)；

③ **标志域**有 3 bit，其中最低位 MF = 1，表示后面“还有分片”的数据报；MF = 0，表示这已是若干数据报片中的最后一片。中间一位 DF = 1，表示“不能分片”；DF = 0，允许分片。最高位无意义。

④ **片偏移域**表示该分片在整个数据报中的相对位置（8B 为一个单位）。



(第二行从左至右：标识域，标志域，片偏移域)

⑤ 进一步分片：如果某片遇到一个 MTU 值更小的网络时，其本身能够**再被分片**，且 IP 对原来的片与再分的子片并**不加以区分**，接收方亦不知情。（优点：接收方不需要先重装子片后才能重装原数据报，节省了 CPU 时间，减少了每一片头部所需的信息量）

数据报重装：在所有片的基础上重新产生原数据报的过程，在**目的主机**中进行。

※好处：减少路由器中的状态信息数量；允许动态改变路径

※片丢失问题：当数据报的某一片第一个到达时，接收方开始 IP 重组计数器，结果是全有/全无（all-or-nothing）：要么所有的片都到达了并且 IP 重组数据报，要么 IP 丢弃了整个数据报。

IPv6 数据报：基本头部+扩展头部(可选)+数据区，基本报头中所含信息比 IPv4 少。

※优点：经济性和可扩展性。类似数组（静态）和指针（动态）的区别。

基本头部	扩展头部1	.....	扩展头部N	数据区

IPv6 数据报组成：

① 不可分片部分：基本头部+控制路由的头部；

② 可分片部分。

包含分片信息的域放在一个单独的扩展头部中，该头部的存在就表示该数据报是一个片。

IPv4 和 IPv6 数据报的区别：在 IPv4 中，由路由器负责执行分片任务；但在 IPv6 中，由发送方主机负责分片，路由器不参与，如果需要分片，发送方主机将收到中间路由器发送的 ICMP 差错报文，从而不断减小分片长度，一直到分片能最终送达目的端为止（原因：IPv6 可能按需控制路由，使各片都按同一路径传输）。

2. ICMP 差错报告机制

ICMP：互联网控制报文协议，包含信息报文以及差错报文。当一个数据报出现问题时，路由器将发送一个 ICMP 差错报文给**源主机**。

※ICMP 利用 8 位长的**类型域**来识别每个报文，报文例如：

源抑制	路由器太多数据报以至于用完缓冲区，必须丢弃到来的数据报。每丢弃一个数据报，路由器向源主机发送源抑制报文。主机收到报文时，需要降低传送率。
超时	① 当一个路由器将一个数据报的生存时间（Time To Live）域减到零时，路由器丢弃这一数据报，并发送超时报文； ② 在一个数据报的所有片到达之前，IP 重组计时器到点，则主机发送超时报文.
目的不可达	路由器检测到数据报无法传递到最终目的地时，向源主机发送目的不可达报文，告知是特定的目的主机不可达，还是目的主机所连的网络不可达。
重定向	若路由器发现主机错误地将应发给另一路由器的数据报发给了自己，则通过重定向报文通知主机改变路由，指出是一台特定主机还是一个特定网络发生了变化（后者更为常见）
参数问题	指出数据报中的某一参数不正确

ICMP 报文传送机制：

每一个 ICMP 报文的产生对应于一个 IP 数据报。ICMP 报文整个封装在 **IP 数据报**的数据区中，IP 数据报封装在**物理帧**中进行传输。**数据报头部的源主机 IP 地址**作为 ICMP 报文的目的地址。

※若携带 ICMP 差错报文的数据报再次出错，不再发送差错报文，以避免网络拥塞。

ICMP 应用一：测试可达性

Ping→发送包含 ICMP 回应请求的报文→等待(短时)→若无应答则重传请求→若重传请求仍无应答或收到目的不可达报文，则声称该远程机器不可达

※前提：远端主机上的 ICMP 软件只要收到回应请求，则必须发送回应答复报文。

ICMP 应用二：跟踪路由

原理：Traceroute 程序利用 ICMP 差错报文及 IP 头部中的 **TTL 字段（生存周期）**发现给定路径上的中间路由器。TTL 是 8 bit 字段，由发送端初始设置段，**每个处理数据报的路由器都将 TTL 的值减 1**，当路由器收到 **TTL 字段为 1** 的数据报，则丢弃并发回超时报文。

关键：包含超时报文的 IP 报文的**信源地址**是该路由器的 **IP 地址**。

操作过程（理想）：

① 发送一份 TTL 字段为 1 的 IP 数据报给目的主机；

② 处理数据报的第一个路由器将 TTL 值减 1，丢弃该数据报，并发回超时报文；

③ 得到该路径中第一个路由器的地址。然后程序发送 TTL 值为 2 的数据报，从而得到第二个路由器的地址，依此类推。

局限：由于路由可能动态变化，路由跟踪程序更适合**相对稳定的互联网**。

ICMP 应用三：发现通路 MTU

通路 MTU：从源端到目的地路径上的**最小 MTU**

操作过程：

① 源端主机上的 IP 软件发送一系列探测报文，每一探测报文的数据报的头部的 DF 标志位都被置为 1 而**防止分片**；

② 若探测报文的数据报比路径上某个网络的 MTU 大，连在此网上的路由器丢弃数

据报，同时发回**要求分片的 ICMP 报文**给源主机；

③ 源主机收到差错报文后，发送另一个较小的探测报文。重复上述过程，直到某一探测报文成功到达目标主机。

ICMP 特点：

① ICMP 是**网络层**的协议，但报文不直接传给网络接口层（数据链路层），而是先**封装**在 IP 数据报中，然后再传给网络接口层（数据链路层）；

② 从协议体系上看，ICMP 的差错和控制信息传输只是要解决 IP 协议可能出现的**不可靠问题**，它不具有**独立于** IP 协议而单独存在的意义，因此将它看作是 IP 协议的一个部分，归于 IP 协议的体系；

③ ICMP 差错报告采用**路由器-源主机**模式，路由器发现数据报错误时，**只向源主机**报告差错原因；

④ ICMP **不纠正差错**，只报告差错。差错处理由高层协议完成。

3. UDP 协议

端到端协议：允许将单个**应用程序**作为通信端点的协议。TCP/IP 协议设置**单独的层次（传输层）**配置端到端协议。

UDP(User Datagram Protocol)：一个简单的面向数据报的传输层协议，允许**应用程序**发送和接收**单个报文**，UDP 报文**封装在 IP 数据报中**（类比 ICMP）。

UDP 特点：

① 端到端：提供协议端口，进行进程间的数据通信

② 无连接、不可靠：不提供确认、消息反馈控制（与 IP 数据报相同）

③ 面向报文：使用 UDP 的应用进程所发送和接收的数据是单个报文

④ 尽力而为：利用 IP 进行主机到主机的数据报传输，与 IP 相同

⑤ 任意交互：允许应用进程之间发送和接收的多对多

⑥ 操作系统无关性：标识应用程序的方法与本地 OS 无关

UDP 报文格式：

UDP 源端口(16 位)	UDP 目的端口(16 位)
UDP 报文长度	UDP 校验和
数据	
……	

① 源端和目的计算机的 IP 地址默认包含在携带该 UDP 报文的 **IP 数据报**中；

② **源端口、校验和**均**可选**，若无则全为零，但后者是 UDP 中唯一提供差错控制之处，故应使用；

③ 计算校验和时，考虑：**UDP 报文的头部和数据部分+伪报头**（源和目的 IP 地址、8 个 bit 的 0、协议号（17）、UDP 报文长度，共 12 字节）

④ **协议端口号**：标识符抽象集，独立于底层的 OS，通信时应用程序必须指定双方的 IP 地址和协议端口号。端口号可由授权组织统一指定或由软件动态绑定。

4. TCP 协议

TCP：传输控制协议，保证**可靠性**的传输协议。

端口：TCP 连接两端应用进程的端点，是一个 16 位的标识。TCP 连接利用端口提供多路

复用。

TCP 提供的服务：

① 面向连接：应用程序必须首先请求一个到目的地（远程应用程序）的连接，然后使用这一连接来传输数据；
② 点对点通信：每个 TCP 连接有两个端点；
③ 全双工通信：数据发送和接收可在连接的两个方向上同时进行；
④ 完全可靠性：TCP 确保通过一个连接发送的数据按发送时一样正确地送到，并且不会发生数据丢失或乱序；
⑤ 流接口：TCP 提供一个流接口，利用它应用进程可以通过连接发送连续的字节流；
⑥ 可靠的连接建立：TCP 要求当两个应用创建一个连接时，两端必须遵从新的连接。前一次连接所用的重复的分组不再有效，也不会影响新的连接；
⑦ 友好的连接关闭：TCP 确保在关闭连接之前传递的所有数据的可靠性。

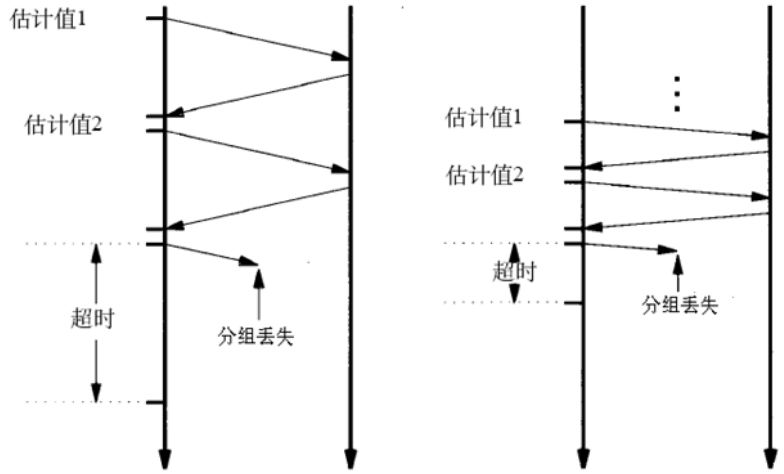
※由 TCP 提供的连接叫做虚拟连接，因为它们由软件实现。TCP 只把 IP 看作是一个连接起两个端点主机的分组通信系统，而 IP 只把每个 TCP 报文当作是要传输的数据。

TCP 解决的可靠性问题：

① 丢失数据的恢复问题

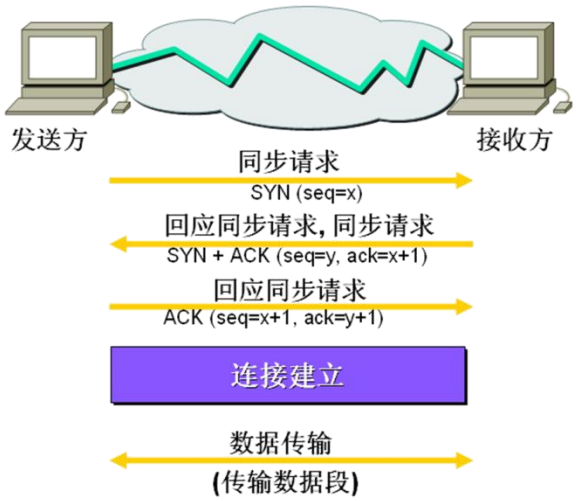
解决方案：自适应重发

a. 发送数据报文 N，设置重发定时器（等待时间比平均往返延迟稍大一点，从而刚好确定）
b. 等待对 N 的确认
c. 重发定时器报超时
d. 重发数据报文 N

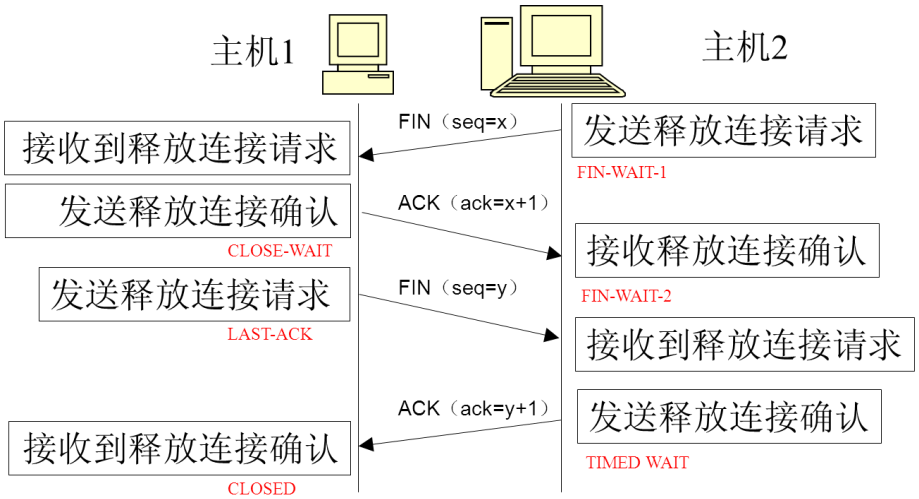


② 可靠建立与关闭连接问题

解决方案：三次握手



改进：四次握手（FIN 为终止段）



※主机 2 第二次发送 ACK 后进入 TIMED-WAIT 状态，等待**两个最长报文生命周期**才真正进入 CLOSED 状态，因为在这段等待时间里，如果最后的 ACK 丢失，主机 1 会超时并重发最后的 FIN，这样主机 2 的 TCP 可以再次发送 ACK 报文段（这也是它唯一可以发送的报文，并重置定时器）。

③ 流量控制问题

解决方案：窗口机制

窗口：（发送端或接收端）剩余缓冲区空间的数量。

接收端窗口 rwnd(通知窗口)：接收端根据其目前的接收缓存大小所许诺的最新的窗口值

拥塞窗口 cwnd：发送端根据自己估计的网络拥塞程度而设置的窗口值

※发送窗口的上限值＝**Min(rwnd，cwnd)**

※理想情况：全速传输 (cwnd 越大越好)，没有数据丢失

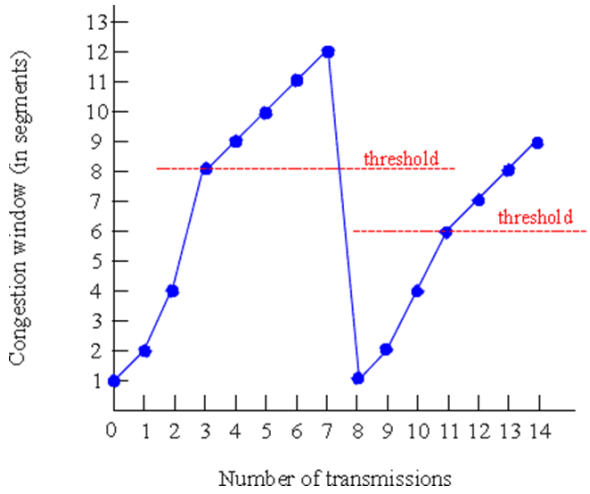
“刺探”带宽过程：

① 慢启动：从发送较少的信息量(如一个报文)开始，**双倍**增加 cwnd，直到其大于 threshold，或者出现数据丢失；

② 拥塞避免：当 cwnd 大于 threshold 时，**线性**增加 cwnd，重新进行刺探；

③ 当出现数据丢失时，**迅速回退**，开始慢启动，避免拥塞。

※threshold：定义慢启动的阈值



第七讲 因特网路由技术

一、网络地址转换（NAT）

1. 产生原因

IP 地址很快耗尽，引入子网和无类编址来节约 IP；希望能让多台计算机共享一个 IP

无类编址（CIDR）：传统编址方法将 IP 根据前几位分为 ABCDE 类，CIDR 不作此区分，可更有效地分配 IPv4 的地址空间

2. 目的

提供虚拟的寻址机制

3. 运行机制

a) 允许同站点内的多台计算机共用一个 IP，但为每台计算机分配一个本地唯一的地址。对外交换信息时，将本地私有地址转换为全球 IP 地址。

b) NAT 被连接在站点与因特网之间的通路上，对进入站点和送出到因特网的每个数据报头部域进行重写。

c) 只改变 IP 数据报中的地址域会造成校验和错误。因此，每当改变了源地址或目的地址时，NAT 必须重新计算 IP 校验和

4. 实现方式

a) 软件实现（便宜，用于低速网络）/ 硬件实现（线速，用于高速网络）

b) 一些路由器包括了 NAT 的软件实现

c) 各大 PC 操作系统中都有软件来实现家庭 NAT，如 Windows 上的 ICS

5. 更厉害的转换方式

a) 当站点中多台计算机要跟同一个目的地通信时，基本 NAT 不能满足要求。

b) 网络地址与端口转换（NAPT）利用 IP 与协议端口号的组合来满足要求。

c) NAPT 将每个数据报与 TCP 连接或某个“一对一”UDP 会话关系互相关联起来，是针对某一个传输连接而不是某台计算机进行操作。

二、静态路由与动态路由

1. IP 路由两大类别

静态路由

a) 系统启动时初始化路由表

b) 除非检测到错误，否则路由不变

c) 多数主机采用静态路由。适用于主机只有一个网络连接且只有一个路由器来连接 Internet 的情况。

d) 典型路由表只有两项：直接连接的网络-> direct delivery / 否则-> default

动态路由

a) 系统启动时初始化路由表，同时加载运行路由传播软件

b) 不同计算机上的路由软件交互作用，学习到通往每个站点的最佳路径，更新路由表

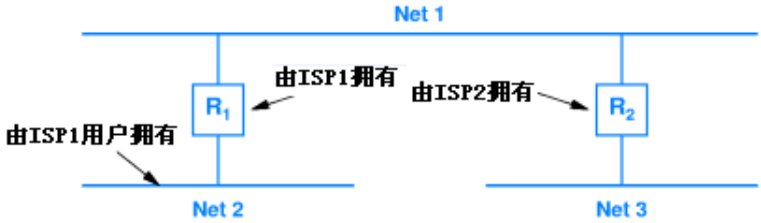
c) 可能持续改变

d) 大多数路由器采用动态路由，因为路径不断变化。

e) 为保证所有路由器能维持到达每个目的地的有关信息，每个路由器都运行采用路径传播协议的路由软件，以查询其他路由器可到达目的地的情况，并通知其他路由器其自己可到达目的地的情况。

f) 路由软件利用收到的信息来不断地更新本地的路由表。

g) 不错的图示哟：



如果 R2 崩溃了，R1 中的路由软件就会检测到 Net3 不再可达，并将 R1 路由表中的相关路径取消

2. 两级路由层次结构

a) 在全球因特网范围内，为防止过多的传播拖垮网络。

b) 将路由器和网络划分为群组（又称“自治系统”，AS），每个群组内由路由器交换信息，每组有至少一个路由器（组长……）负责收集综合信息并与其他群组交流。

c) 由因特网地址授权委员会（Internet Assigned Numbers Authority, IANA）分配。

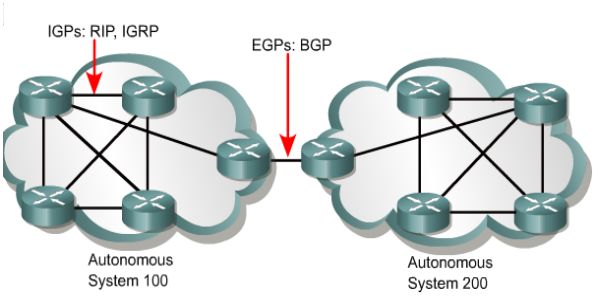
一般来说每个 ISP 都是单个自治系统，大型 ISP 本身还会被划分成多个自治系统。

三、因特网路由与路由协议

1. 两类因特网路由协议

内部网关协议 IGP 和 外部网关协议 EGP

不错的图示哟：



An autonomous system is a collection of networks under a common administrative domain. IGPs operate within an autonomous system. EGPs connect different autonomous system.

2. **路由度量**

路由软件选择路径时对所使用通路的测量。

典型因特网路由采用两种度量的组合：

管理成本：需要人工赋值，常用来控制对通信量合适的通路选择

跳计数：中间网络的个数

IGP 采用路由度量：每个自治系统自由选择路由度量，因为衡量标准可以一致。

EGP 无法采用路由度量：不同自治系统之间度量标准可能不一致。

3. 基本路由算法

距离矢量路由算法 DVR

基于少量路由信息交换。需要保存到所有可能目的地的路由表，表的每一项包含 本节点到目的地的距离 D 和 下一跳节点。通过与临节点交流更新路由表。

优点：无环路，具有快速收敛性；支持精确的度量值；支持通往同一目的站点的多重路径；能区分内部路由与外部路由。

链路状态路由算法 LSR

维护一张网络拓扑图。计算到每个其他路由器的最短路径。

4. **路由协议**

路由信息协议 RIP

a) 是 IGP。采用距离矢量算法：运行 RIP 的路由器对外通告所由它能够到达的目的地及距离，相邻的路由器接收被通告的信息，并用它来更新路由表。（类似 DVR 哟）

b) 特点：按跳数计算距离，无权值；使用 UDP 进行消息传输；使用广播/多播；支持默认路由传播，方便安装；允许主机被动听取和更新路由表。

c) 问题：路由器不知道整个网络的拓扑结构，在路径信息发生变化时容易引起环路；不适合大型组织对路由协议的需求；每个报文都包含目的地和距离的完整列表，报文很长；网络底层链路技术多种多样，带宽各不相同，而距离矢量算法对此则视而不见；网络庞大时收敛速度慢。

开放最短路径优先协议 OSPF

a) 是 IGP。采用链路状态算法：每个路由器周期性地探测相邻的路由器，广播一个“链路-状态”报文;所有路由器接收广播报文,利用报文中的信息更新本地的状态图;若状态改变就重新计算出最短路径。（类似 LSR 哟）允许管理员将一个 AS 中的路由器和网络再划分为子集，称为区域。

b) 特点：提供 CIDR 和 subnet 地址格式支持；提供认证的报文交换，安全性增强；无环路；收敛速度快。

c) 问题：开销较大，每台路由器都要维护整个网络的拓扑结构信息。

边界网关协议 BGP

a) 是 EGP。采用距离矢量算法，扩展性强但收敛速度慢。

b) 特点：提供自治系统级的路由信息；管理员可通过配置来限制 BGP 向外部发布的路由（有些内部信息不向外部发布！）；使用 TCP 通信，提供可靠传输；给出自治系统到其它每个目的地的路径。

5. **意义**

因特网的膨胀对路由技术提出更高要求：除找到路径外，还必须考虑路径的传输容量和服务质量；需要考虑全网负荷，平衡各通道流量；要求快速收敛性和高效的路由表查询。

未来热点：具有 QoS 和流量工程能力的路由算法 以及 相应规范。

6. **网关**

a) 在网络层以上的中继系统。

b) 可以和路由器部署在一起。但！路由器在网络层，网关在传输层/应用层。

c) 负责协议的转换，如无线网关、电子邮件网关等；经常与一些负责本网安全的应用功能结合起来，如防火墙、VPN 等。

四、组播路由技术

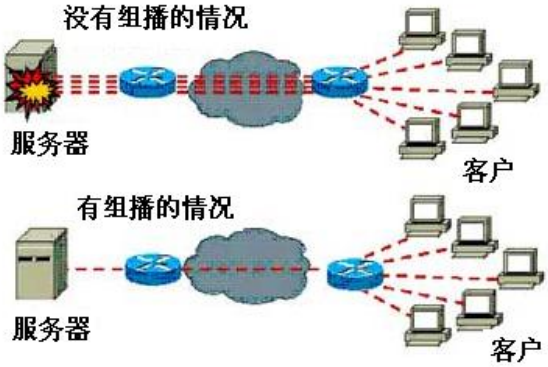
1. **IP 组播概念**

a) 组播：一个主机向特定的多个接收者发送报文的方法；组播群组的成员是动态的。

b) 特点：单点发送，多点接收。

c) 优点：比单播更适合支持流媒体、视频点播等。避免重复传输相同内容，节省资源。

不错的图示哟：



d) 组播报文：一个 IP 报文向一个“主机组”的传送。除目的地址部分，与普通报文没有区别。

e) 发展现状：已经有几个协议，但尚无整个因特网范围的组播技术

2. 地址分配与映射

a) 组播地址：主机组地址也称组播地址、D 组地址。其前缀是 1110。标识一组主机。

b) 性质：D 类地址是动态分配和恢复的瞬态地址。每一个组播组对应动态分配的一个 D 类地址；当组播组结束组播时，相对应的 D 类地址将被回收，用于以后的组播。

c) IP 组播地址与以太网硬件组播地址的映射：MAC 地址共有 48 位；把 IP 地址的最后 23 位拷贝到 MAC 地址的最后 23 位，然后把这 23 位前面的那一位置为 0。

3. 组播群组管理

a) 动态的组成员：主机可选择加入或者退出某个主机组；主机可以加入多个主机组；可以向自己没有加入的主机组发送数据;组播路由器定时向本地网络上的主机轮询。

b) 群组管理协议 IGMP

用于主机与路由器之间的网络，将计算机定义为群组成员。为其每个端口都维护一张主机组成员表，定期地探询表中的主机组的成员，以确定该主机组是否存活。(查户口……)

IGMP 报文被置于 IP 数据包中传送：主机求组播时，发送“主机成员报告”报文，告知想接收的组播地址；组播路由器将该主机加入指定的组，向所有支持组播的主机发送“主机成员询问”报文。

4. 数据包转发方式

a) 扩散与剪枝：适用于小群组，且成员都在邻近的局域网。

b) 配置与隧道：适用于群组成员地理位置分散时。

c) 基于核心的发现：适用于小型到大型之间的群组。类似星形拓扑。

五、域名解析与 DNS

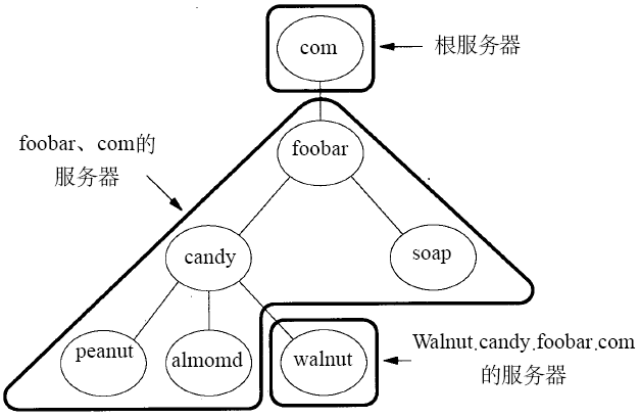
1. DNS

a) 域名系统（DNS）：提供计算机域名（如 www.sina.com）与 IP 地址之间的自动映射。

b) 工作方式：以大的分布式数据库的方式工作。每当应用需要将域名翻译为 IP 地址时,应用成为域名系统的一个客户。客户将待翻译的域名放在一个 DNS 请求信息中，并将这个请求发给 DNS 服务器。

c) 服务器层次结构：层次对应域名中的层次

不错的图示哟：



2. 域名解析

a) 域名解析:把域名翻译为等效的 IP 地址的过程。完成此过程的软件叫域名解析器。

b) 多重类型：数据库中每一项包含“域名 记录类型 值”，解析器必须指明类型。
例子：向一台计算机发送邮件的 DNS 请求类型与其他应用的请求类型不同。

c) 工作方式：客户机向本地 DNS 查询需要访问的主机的 IP→ 本地 DNS 向另一个 DNS 查询→ …直到解析出该主机的 IP

d) 三种查询模式：
递归查询：如果 DNS 服务器内没有用户要的数据，则代替客户机查询其他 DNS。
迭代查询：如果 DNS 服务器内没有用户要的数据，则让客户机自行查询其他 DNS。
反向查询：客户机利用 IP 地址查询其主机完整域名。
例子：向本地 DNS 查 mail.pku.edu.cn，本地 DNS 没有→ 本地 DNS 在根域名服务器处获得 cn 域名服务器的 IP→ 在 cn 域名服务器处获得 edu.cn 域名服务器的 IP→ 在 edu.cn 域名服务器处获得 pku.edu.cn 域名服务器的 IP→ 在 pku.edu.cn 域名服务器处获得 mail.pku.edu.cn 的 IP。

e) 可正向（域名→IP）和反向（IP→域名）查找

3. DNS 优化

复制：复制多个根服务器，地理上最近的服务器响应最好
缓存：每个服务器保留一个域名缓存

六、Internet 发展

1. 我国四大骨干网

ChinaNET 电信 ChinaGBN 联通 CerNET 教育网 CstNET 科技网

2. 下一代互联网

无争议的：

无线与移动通信是下一代网络的重要组成部分
固定网络与移动网络的融合是重要的发展方向
下一代互联网将达到 100Gbps
下一代网络将致力于信息共享与协同工作

有争议的：

分布式服务还是集中式服务？
骨干网做简单些还是做复杂些？
是客户/服务器结构还是对等结构?
从较长的时间来看，是重点发展全光网络还是光电混合网络？

第八讲 网络安全

一、概述

1. 安全威胁的根源

问题重视度不够；只有物理安全机制；TCP/IP 本身缺乏安全性；操作系统、安全产品配置的安全性不够；来自内部网用户的威胁；缺乏监视手段；电子邮件、web 恶意控件；应用服务漏洞……

2. 网络信息安全的含义

网络系统软硬件及其中信息受保护；保护传输、交换和存储的信息的机密性、完整性和真实性；对信息的传播及内容有控制能力；不因偶然的或者恶意的原因而遭到破坏、更改、泄露；系统连续可靠的运行；网络服务不中断。

用户角度：涉及个人隐私及商业利益的信息保持机密、完整、真实；避免窃听、篡改、冒充等；不受非法访问和破坏。

网络管理者角度：本地网络信息访问和读写受控制；避免后门、病毒、非法利用等；抵御黑客攻击。

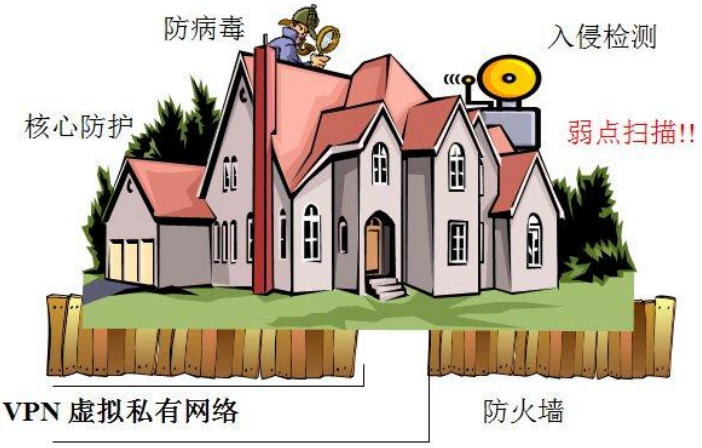
安全保密部门角度：对非法、有害或涉密的信息进行过滤和防堵；避免泄密。

3. 安全层次

安全的密码算法→安全协议→网络安全→系统安全→应用安全

4. 安全策略

不错的图示哟：



二、加密算法

1. DES 算法

a) 用 64 位密钥加密 64 位明文块：（初始变换）把块中 64 位打乱→对结果数据和密钥进行相同操作 16 次→对结果进行逆初始变换。

b) 安全性通过混淆和扩散实现。

c) 弱点：密钥容量小；可能有陷阱。

d) 改进版本：Double-DES；riple-DES；IDEA；AES。

2. RSA 算法

a) 设 X 为明文，Y 为密文，r 是两个素数 p、q 的乘积，PK 是公开密钥，SK 是秘密密钥；且 PK 满足(PK, (p-1)(q-1))=1，SK 满足 SK • PK=1 (mod r)

根据 p 和 q 选择合适的 PK，再根据 PK 计算 SK。

加密方程与解密方程是：$Y=X^{PK} \pmod r$；$X=Y^{SK} \pmod r$

b) 安全性在于 p 和 q 都很大……

所以可以用穷举法攻击

3. **MD5**

摘要计算过程：把摘要的值初始化为一个常量→将这个值与报文的前 512 个比特结合生成新的摘要值→使用同样的变换将这个新值与下一个 512 比特结合→依次类推→最终的摘要值

4. **性能评估**

用软件实现时，DES 和 MD5 比 RSA 快一些；用硬件实现时，DES 和 MD5 比 RSA 快好几条街。

RSA 只用来加密很少的数据。

安全协议会把三者配合，用 RSA 鉴别参与者的身份，用 DES 加密参与者交换的消息，用 MD5 保护消息的完整性。

三、安全机制

1. **安全性的内容**

保密性 完整性 真实性 可用性 隐秘性 ……

2. **完整性机制**

采用报文验证码对传输数据编码。典型方式是采用密码散列，如只有发送方和接收方才知道的密钥。

3. **数字签名**

签名时用私有密钥加密，验证时用对应的公开密钥解密。

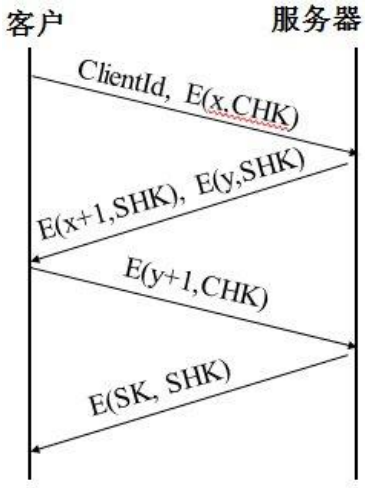
加密两次可同时保证可验证性和保密性。

4. **身份鉴别**

a) 两个参与者在通信前鉴别对方身份。

b) 三次握手方式：

E(x, CHK)表示用密钥 CHK 对随机数 x 进行加密。



c) 最初的 CHK 和 SHK 来自第三方，即鉴别服务器。

5. **证书**

证书的思想允许建立一条“信任链”：如果 X 证明某个公开密钥属于 Y，而 Y 继续证明另一公开密钥属于 Z，那么，尽管 X 与 Z 从未相遇，仍然存在一条从 X 到 Z 的证书链。

认证机构可以发行证书吊销表（CRL）。参与者接受到希望验证的证书时，首先查阅最新的 CRL，证书未吊销则有效。

四、系统实例

1. **网络层：IPSEC 协议**

2. **传输层**

TLS：位于 TCP 和应用层之间。握手协议（协商通信参数）+记录协议（实际数据传输）。

SSL：ppt 没讲……

HTTPS：并没有对 HTTP 协议做太多的改动，只是把数据转发到 TLS 层而不是 TCP 层，接收数据也是从 TLS 层而不是 TCP 层

3. **应用层**

PGP：为电子邮件提供加密和鉴别，保密性极好。

SSH：远程登录服务，提供客户/服务器鉴别。

五、防火墙

1. **概念**

指设置在不同网络（安全域）之间的一系列部件的组合。

是不同网络（安全域）之间的唯一出入口，能根据机构或企业的安全政策，控制出入网络的信息流，且本身具有很高的抗攻击能力。

是处理互不信任的单位之间建立网络连接时最重要的安全工具，能以较低的成本提供安全保障。

2. **防火墙设置**

机制：分组过滤，即检查每个分组头部中有关的参数域。

组成：一个分组过滤器用于限制从 Internet 到达的数据报；一个过滤器用于限制离开单位内部网的数据报；一个安全的计算机系统运行应用软件。

3. **防火墙特征**

保护脆弱和有缺陷的网络服务；集中化的安全管理；加强对网络系统的访问控制；加强隐私；对网络存取和访问进行监控审计。

4. **防火墙功能**

过滤进、出网络的数据；管理进、出网络的访问行为；封堵某些禁止的业务；记录通过防火墙的信息内容和活动；对网络攻击进行监测和报警。

5. **技术发展趋势**

把用户认证及其服务扩展到防火墙中；采用多级过滤策略并辅以鉴别手段；病毒防护功能；高速处理数据。

六、虚拟私有网络（VPN）

1. **核心**

利用公共网络建立虚拟的私有网络

2. **实现方式**

用软件实现。将路由器配置成只允许从机构的其他站点路由器发过来的分组通过，而且只允许从本站点路由器发给机构其他站点路由器的分组通过。分组数据在被传输出去之前，必须由 VPN 软件对它加密。

3. **IP-in-IP 隧道机制**

目的：机构各站点之间通过因特网传输数据报时，能保持信息的完全隐蔽性。

工作方式：发送方 VPN 软件对全部数据报进行加密→把它放置在另一个数据报中进行传输→接收方路由器的 VPN 软件从载荷中提取出原始数据报并进行解密→把它发给相应的计算机。

隧道协议：点到点 PPTP、第二层 L2TP（数据链路层）；IPSEC（网络层）；MPLS（第二层和第三层之间）

4. **用途**

对传输的数据加密。

防火墙保证内部网络安全，相当于门卫，VPN 保证网络上传输的数据不被窃取，相当于运钞车。（是镇远镖局吧……）

七、其他安全策略

1. 入侵检测系统：抓取网络上的所有报文，分析处理后报告异常和重要的数据模式和行为模式。使网络安全管理员清楚地了解网络上发生的事件，并能采取行动阻止可能的破坏。
2. 病毒防护策略
3. 风险评估：定期或按需寻找网络设备或主机上的漏洞，从而可以对这些漏洞进行及时弥补，以改善网络的安全性/

十一、World wide Web 技术

Web 网页与浏览

浏览器由一组客户、一组解释器和一个管理它们的控制器所组成。

HTTP 的变化

HTTP 是用来获取网页以及与网页相关的其他信息项（如图像/音频/视频）的标准应用协议

HTTP 使用端口 80。当浏览器要发送 HTTP 请求消息时，它建立到 URL 中指定服务器 80 端口的新 TCP 连接，然后通过该连接发送请求消息

在 HTTP 的早期版本（定义在 RFC 1945 中）中，浏览器正确接收到相关的响应消息之后，服务器就释放该连接。这种形式的 TCP 连接称为**非持久（nonpersistent）的连接**

每个请求/响应消息的传输都使用新 TCP 连接有很多缺点：

1.当访问包含多个实体（如图像）的网页时，在建立新连接传输每个实体时，会产生一个时间延迟

2.每次新传输启动过程缓慢，可能会导致额外延迟

为了减少延迟，当在网页中指定多个实体时，多个进程建立多个 TCP 连接，使每个实体能并发传输

这样能减少 Web 访问的整体时间延迟

但多个连接的使用会导致在客户端和服务器端的额外开销；这种开销对于繁忙的服务器来说影响很大

HTTPv1.1（定义在 RFC 2068 中）以上的版本中，除非特殊说明，服务器端在 Web 会话期间保留初始的 TCP 连接

这种 TCP 连接称为持久的（persistent）

一旦建立连接，浏览器就能发送多个请求而无需等待收到响应

通常当连接上不再有传输时，此次会话将由计时器超时结束

Java 技术

Java 的发展历史

1990 年，Sun 公司开始了一个 James Gosling（Java 创始人）项目，Gosling 用了一个新语言 Oak 来解决这个问题；

1994 年，他们完成了一个用 Oak 编写的早期 Web 查看器，称为 WebRunner，后被改名为 HotJava

1995 年，Oak 更名为 Java ，并在 SunWorld 95 中发布

组成；

程序设计语言　Java 包含一种新的程序设计语言，用它可以编写传统的计算机程序 或者 Java applet

运行环境。Java 系统定义了一个运行 Java 程序所必须的运行环境

Java 语言与运行系统被设计成独立于计算机硬件。

类库。

Java 的成功原因

1 体系结构中立　即 **Java 的平台无关性** （Java 源程序被 Java 编译器编译后生成的字节码，是一种与体系结构无关的代码格式；Java 解释器得到字节码后，负责进行翻译转换，然后在 Runtime 系统上执行；Java 在操作系统级得到统一支持）

2　**Java 的可移植性**（基本数据类型的大小和算法作统一规定；定义了可移植性接口；系统本身是可移植的；Java 系统可以放在任何环境中）

3　Java 的性能　其速度不会超过编译语言；Java 字节码的设计，使之具有较高的性能

4　Java 的多线程性 （Java 可以把一个程序分成多个任务，以便使任务易于完成和最大限度利用 CPU 资源；使应用程序能够并行执行；容易地实现网络上的实时交互行为）

个域网 PAN：　蓝牙，红外，ISM 无线

用于 Wi-Fi 的多路复用技术

DSSS：直接序列扩频。与 CDMA 类似，发送器把输出数据乘以一个序列从而形成多个频率，接收器乘以相同序列实现解码。DSSS 具**有良好的性能**

FHSS：跳频。发送器使用同一序列频率传输数据，接收器使用同样序列的频率提取数据。FHSS 使传输能更好地**抗噪声干扰**

OFDM：正交频分复用。传输波段被划分为多个载波，以使载波之间互不干扰。可提供**最大的灵活性**

无线 LAN 体系结构：特别建构性：无基站，无线主机间通信，很少用。

基础结构型 一台无线主机只与一个接入点通信，由接入点转发所有分组。目前的无线 LAN 大多是这种方式，从互连设备延伸到各个接入点的有线连接，常由双绞线以太网构成

3 个构件：互连设备：如用于连接“接入点”的交换机或路由器

接入点（AP）：“基站”

无线主机：也称为无线节点或无线站点

蜂窝通信系统

和 802.11 和 WiMAX 一样，蜂窝技术依赖对基站的使用

基站是有线网络的一部分，由一个基站天线负责的地理区域称为一个**蜂窝（cell）**

基站可以为 一个蜂窝服务，或利用多个方向上的天线为多个蜂窝服务

蜂窝没有明显的边界，可重叠。当在多个蜂窝重叠的区域通话时，对电话的控制由信号**最强**的基站负责

第二代蜂窝通信技术和 GSM

GSM　是 1992 年欧洲标准化委员会统一推出的标准，它采用数字通信技术、统一的网络标准，使通信质量得以保证，并可以开发出更多的新业务供用户使用。传输速度为 9.6Kbit/s

2.5G 蜂窝通信技术

GPRS　是一项高速数据处理的技术，其方法是以**“分组”**的形式传送数据。网络容量只在所需时候分配，不需要时就释放，亦即采用**统计时分复用**的方法。目前，GPRS 移动通信网的传输速度可达 115k/s，2.5G 技术

第三代蜂窝通信技术（3G）

能够处理图像、音乐、视频流等多种媒体形式，提供包括网页浏览、电话会议、电子商务等多种信息服务

目前的标准有 W-CDMA（宽频码分多路存取）、CDMA2000、TD-SCDMA 和 WiMAX 等

第四代蜂窝通信技术（4G）

始于 2008 年左右，专注于对实时多媒体业务的支持，

从技术标准的角度看，按照 ITU 的定义，静态传输速率达到 1Gbps，用户在高速移动状态下可以达到 100Mbps，就可以作为 4G 的技术之一

从营运商的角度看，除了与现有网络的可兼容性外，4G 要有更高的数据吞吐量、更低时延、更低的建设和运行维护成本、更高的鉴权能力和安全能力、同时支持多种 QoS 等级

从融和的角度看，4G 意味着更多的参与方，更多技术、行业、应用的融

无线应用协议 WAP

是移动通信与互联网结合的产物

十二、Web 编程

一 层次模型

1 计算机应用程序的一般特点：有三部分组成：（用户界面：表示层；应用逻辑部分：业务逻辑层；数据访问部分：数据访问层 ）

传统应用程序模型：主机系统：**主机/终端模式，单层结构。“胖客户端”**

2 Web 应用程序模型

传统的：三层分布式架构

多层计算模式的引入：从逻辑角度看，系统分成客户端、Web 服务器、应用服务器、数据库服务器四层；从物理角度看，应用服务器可以视用户并发数从 1 到 N 台进行扩充，以保证客户端用户的响应要求。

从 1 层到多层，得到的改进：

每一层可以被单独改变，而无需其它层的改变

降低了部署与维护的开销，提高了灵活性、可伸缩性

引入瘦客户端，计算被集中至服务器端，使性能提高成为可能

多层应用程序的三大优点

1 应用程序各部分之间松耦合，从而应用程序各部分的更新相互独立

2 业务逻辑集中放在服务器上由所有用户共享，使得系统的维护和更新变得简单，也更安全

3 数据库不再和每一个活动的用户保持一个连接，而是由应用程序组件负责与数据库打交道，降低数据库服务器的负担，提高了性能

二 中间件

定义：位于平台（硬件和操作系统）和应用之间的**通用服务**，这些服务具有标准的程序接口和协议。

一些特点：1 满足大量应用的需要 2 运行于多种硬件和 OS 平台

3 支持分布式计算，提供跨网络、硬件和 OS 平台的透明性应用或服务的交互

4 支持标准的协议 5 支持标准的接口

意义：由于标准接口对于可移植性和标准协议对于互操作性的重要性，中间件已成为许多标准化工作的主要部分

对于应用软件开发，中间件远比操作系统和硬件平台更为重要

分类：远程过程调用（RPC） 、消息中间件（MOM）、事务处理中间件（TP-Monitor）、集 成中间件……

消息中间件 MOM 指的是利用高效可靠的消息传递机制，进行平台无关的数据交流，并基于数据通信来进行分布式系统的集成

通过提供消息传递和消息排队模型，它可在分布环境下扩展进程间的通信，并支持多通讯协议、多语言、多硬件和软件平台。

事务处理中间件

功能：进程管理、事务管理（即保证在其监控下的事务处理的原子性、一致性、独立性和持久性）、通讯管理（为 client 和 server 之间提供了多种通讯机制，包括请求响应、会话、排队、订阅发布和广播等）、事务处理监控在操作系统之上提供一组服务，对 client 请求进行管理并为其分配相应的服务进程，使 server 在有限的系统资源下能够高效地为大规模的客户提供服务

几种新理念

1　面向服务体系架构 SOA　（服务提供者，服务使用者，服务注册中心：）

对其理解：

它支持将用户的业务作为链接服务或可重复业务任务进行集成，可在需要时通过网络访问，并且让用户感觉似乎这些服务就安装在本地桌面上一样

这些服务是自包含的，具有定义良好的接口，允许这些服务的消费者了解如何与其进行交互。所有交互都是基于“服务契约”进行的；服务契约用于定义服务提供者和消费者之间的交互

SOA 提供了这样一种框架：一个系统上的软件可以安全而且可靠地提出请求并获得其他系统上的计算资源，从根本上突破了客户/服务器交互模式

SOA 中的服务是整个 SOA 实现的核心

基本特征　服务的封装 、重用、互操作

服务是自治的（Autonomous）功能实体

服务之间的松耦合度

服务是位置透明的

明确定义的接口

意义 例如　Web 服务是众多实现 SOA 形式中的一个，但它正迅速成为用于支持 SOA 的事实标准

SaaS：软件即服务

理解：

SaaS 是随着互联网技术的发展和应用软件的成熟而开始兴起的一种完全创新的软件应用模式

SaaS 是一种通过 Internet 提供软件的模式

供应商将应用软件统一部署在自己的服务器上，用户根据自己的实际需求，通过互联网向供应商定购所需的应用软件服务，并按定购的服务多少和时间长短向供应商支付费用

SaaS 提供了更多的软件可用性

用户只需要运行带浏览器的设备以及相应的网络

这意味着用户不必提供、运行、管理以及支持自己的内部基础设施，对中小规模的用户非常有利

SaaS 系统使用特点

标准 SaaS 系统是多重租赁的（Multi-tenant），也就是一套软件和数据库平台，经过软件和数据库的隔离及保密技术，多个企业（用户）同时使用

SaaS 运营商普遍采用大型商用关系型数据库和集群技术；多重租赁软件针对数据库设计，

为节省成本，几乎所有公司都是共享一个数据库 license，

云计算

概念与原理

云计算通过数据中心（data centers）发布可靠的服务，这些数据中心建立在众多的互联网计算机上；云计算提供的服务在世界各地都能够访问，而“云”作为一个访问点出现，满足消费者的计算需要

特征

以服务的形式将计算技术提供给用户，**隐藏了技术的细节**

对服务的访问以 Web Service 或类似形式通过 Internet 提供，以达到**最后的位置无关性和兼容性**

服务提供商**以单位价格收取费**用

云计算的技术实现通常是网格技术的延伸，并**大量应用了虚拟化技术**

带来的改变

高性能低投入的云计算将带来工作方式和商业模式的根本性改变

商业机遇　尤其对于中小企业

对硬件的影响

新市场的拓展　云计算使开发新产品、拓展新市场的成本非常低：

网络应用发展趋势

1　服务器瓶颈问题　客户数量的增加——性能瓶颈

可扩展网络服务的需求

新途径与技术：

（1）　内容缓存加速　（使用**缓存区**对每个静态网页的副本进行保存

使用**分布式**缓存服务扩展缓存）

（2）　Web 负载均衡　（负载均衡器（load balancer）检查每个请求，

（3）　服务器虚拟化

（4）　P2P 通信　各节点之间平等，都是信息的 consumer 和 provider

（5）　分布式数据中心

2　社交网络

3　移动通信和无线联网

4　多媒体应用

5 IPv6 之发展　（这些前面或后面都有就不介绍了）

第十三讲：Web 信息发现

一．Web 信息的特点

1.海量性：众多信息源在同一时间产生的信息即为海量

2.动态性：信息的产生和消亡越来越快

Web 的几个演化特点：

Web page 实现方式：deep web 在快速发展，专业性内容在增多

Web page content：分类趋细，duplicate 内容增多

Link structure：有效连接减少，广告链接和 link spa 在增多

Surfing model：search dominant model

其他新特点：交互性，使用模式多样性，大众性与专业性

3.异构性：从 html 到 xml

4.自组织性：信息组织具有一定结构和规律

二．Web 信息整合（一）

整合模式：搜索引擎

系统所用方法：抓取 web 页面并存储

应用方式：主要是 keyword 查询

主要构成：crawler，indexer，searcher

三．Web 信息的整合（二）

整合模式：主题数据库（结构化或半结构化的），用户可以基于主题进行查询

整合方法：virtual，materialized

系统所用方法：在 web 上寻找相关信息（crawler）；基于 topic 进行整合

应用方式：基于内容进行查询

特点：针对性强，查询使用时定为准确；信息整合比较费时费力

四．PageRank – used to implement google

假设：A hyperlink from page A to page B is a recommendation of page B by the author of page A.

Main idea: a page has a high rank if the sum of the ranks of its in-links is high

A high PageRank page has many in-links or a few highl ranked in-links

The PageRank for a given document represents the probability that a random surfer(choosing a starting document randomly, following links randomly until they get bored, then stopping randomly) will hit that given document.

Naïve algorithm: 存在 dead ends 和 spider trap 的问题

$$R(p)=\sum_{(q,p)\in G}\frac{R(q)}{out\deg ree(q)}$$

Modification: damping factor d. *d* represents the probability that the random surfer will get bored and request another random page; (*1-d*) is the probability that the random surfer follows a link on current page

$$R(p)=d+(1-d)\cdot\sum_{(q,p)\in G}\frac{R(q)}{out\deg ree(q)}$$

五．HITS

假设：if page A and page B are connected by a hyperlink, they might be on the same topic.

Authorities: relevant pages of the highest quality on a broad topic --- highly important

pages

Hubs: Pages that link to a collection of authoritative pages on a broad topic

Main steps:

1. Constructing Subgraph
   - 1.1 Creating a root set: Given a query string on a broad topic; Collect the t highest-ranked pages for the query from a text-based search engine
   - 1.2 Expanding to a base set: Add the pages pointing to any page in root set; Add the pages pointed to by any page in root set
2. Computing Hubs and Authorities
   - 2.1 Associating weights: Initially set a uniform constant to all the values(authority weight, hub weight)
   - 2.2 Updating Authority Weight

$$x_p = \sum_{q \text{ such that } q \to p} y_q$$

Updating Hub Weight

$$y_p = \sum_{q \text{ such that } p \to q} x_q$$

六. PageRank V.S. HITS

PageRank: simulates a random walk across the web and computes the "score" of a page as the probability of reaching the page. Query independent page quality

computed for all web pages stored in the database prior to the query

computes authorities only

Trivial and fast to compute

HITS: focuses on broad topic queries that are likely to be answered with too many pages; the more a page is pointed to by other pages, the more popular is the page; popular pages are more likely to include relevant information than non-popular pages. Query dependent page quality

performed on the set of retrieved web pages for each query

computes authorities and hubs

easy to compute, but real-time execution is hard

七. 对连接的再认识

搜索引擎带来的影响

几点思考

这部分内容感觉不是很好总结，大家就看 ppt 吧，我觉得看一遍了解一下就行了，恩。

第十四讲 web 信息获取和处理

一．信息获取

1.概念：Download a set of web pages which consists typically of all pages reachable following links from a root set： Find new pages；Keep pages fresh；Select “good” or “important” pages

2.技术：Incremental Crawlers；Parallel Crawlers；Deep Web Crawlers；Focused Crawlers（没有具体讲）

2.1Periodic Crawler：Periodically visit the web and replace the entire old collection by a brand new collection

Incremental Crawler：Refresh existing pages； Replace “less-important” pages with new and “more-important” pages

2.2Parallel crawlers:

Advantages (compared with a single-process crawler)：Scalability；Network-load dispersion（分散）；Network-load reduction

Challenging and interesting points: Overlap；Quality；Communication bandwidth

Coordination modes:

a. Independent: each C-proc starts with its own set of seed URLs and follow links without consulting with other C-procs

优缺点：minimal coordination overhead and very scalable; too much overlap

b. Dynamic assignment: a central coordinator logically divides the Web into small partitions and dynamically assigns each partition to a C-proc

优缺点：less overlap; too complicated

c. Static assignment: the web is partitioned and assigned to each C-proc before they start to crawl. The crawler does not need a central coordinator

优缺点：Simplicity, scalability

2.3 Static assignment：Links from one partition to another (inter-partition links) can be handled either in:

a. Firewall mode: Each C-proc downloads only the pages within its partition and does not follow any inter-partition link

优缺点：the crawler has no overlap, also no communication overhead ；*Disadvantage*: may not download all pages that it has to download

b. Cross-over mode: a process follows also inter-partition links and discovers also more pages in its partition

优缺点：download all the pages; may clearly overlap

c. Exchange mode: Each C-proc downloads pages within its partition, however, it exchanges inter-partition links with other C-proc’s periodically and incrementally. This is the main method used in parallel crawlers!

优缺点：Can *download all the pages* and *avoid overlap*, however, need *more communications*

2.4 deep web: Consists largely of content-rich databases from universities, libraries, associations, businesses and government

二．信息处理框架

重复检测：Duplicate；Near-duplicate: fingerprint

正文提取：内容处理；噪声去除

文档解析：词素切分；停用词去除；词干提取；短语提取

链接分析：锚文本；排序；链接质量

Combating Web Spamming

分类和聚类

索引建立：需考虑的因素：相关性、倒排索引、压缩、索引构建、查询处理

三．Web spam

定义：any deliberate action solely in order to boost a web page's position in search engine results, incommensurate with page's real value

技术：

Boosting techniques：Techniques for achieving high relevance/importance for a web page

Term spamming：Manipulating the text of web pages in order to appear relevant to queries

类型：Body spamming; title spamming; anchor text spamming; url spamming

技术：repetition; dumping; weaving; phrase stitching

Link spamming：Creating link structures that boost page rank or hubs and authorities scores

类型：outgoing link spam; incoming link honey pot; crawling to post links(comment spamming); link farms; expired domain purchasing

Hiding techniques：Techniques to hide the use of boosting From humans and web crawlers

类型：Content hiding; Cloaking; Redirection

Combating web spam

方法：Statistical Detection；Comment Spam Detection；Detecting Cloaking and Redirection；Secrecy；Content Based Detection；Graph Based Detection

Trustrank idea

Selects good seed pages：inverse PageRank

Propagates scores to other good pages

Separates good from bad

第十五讲：web 信息整合与应用

一．Web 信息的集成

1.基于主题集成的具体任务：主题的确定，集成模式的确定，信息发现和获取，信息提取和转换，信息存储、索引和访问，信息应用，信息维护，系统演化与发展

2.集成方法

Lazy mediator：只有集成架构，并不存储信息

Eager mediator：由于需要存储信息，所以要处理好数据的时新性和一致性

3.信息提取与转换

是 wrapper 的任务，它从不同来源的数据中提取相关信息，并向预定的 webview 格式转化；提取方法为 manually 及 semi-automaticcally，希望能够提高自动化程度。

Wrapper：an extracting program to extract desired information from web pages and convert to a high-level schema.

信息提取方法：based on template/ ontology/ rules/ grammar.

二．Web 信息挖掘

1.Web page content mining: classification v.s. clustering

2.Web structure mining

3.Web usage mining

Navigation patterns

Association rules

Discovery of sequential patterns

Classification and clustering

三．社交网络

四．下一代互联网

对互联网的思考：是一个互联互通平台，无论如何发展，不要忘了其所应具有的最根本的特点，即互通性和互操作性；是一个商业操作平台，商业利益会促进其更快速的发展，但它只是一个平台，必须和其他行业相结合才有更强的生命力。