大学生计算与信息化素养

—网络与信息安全

韩　慧

hanhuie@126.com

本次课程所讲内容

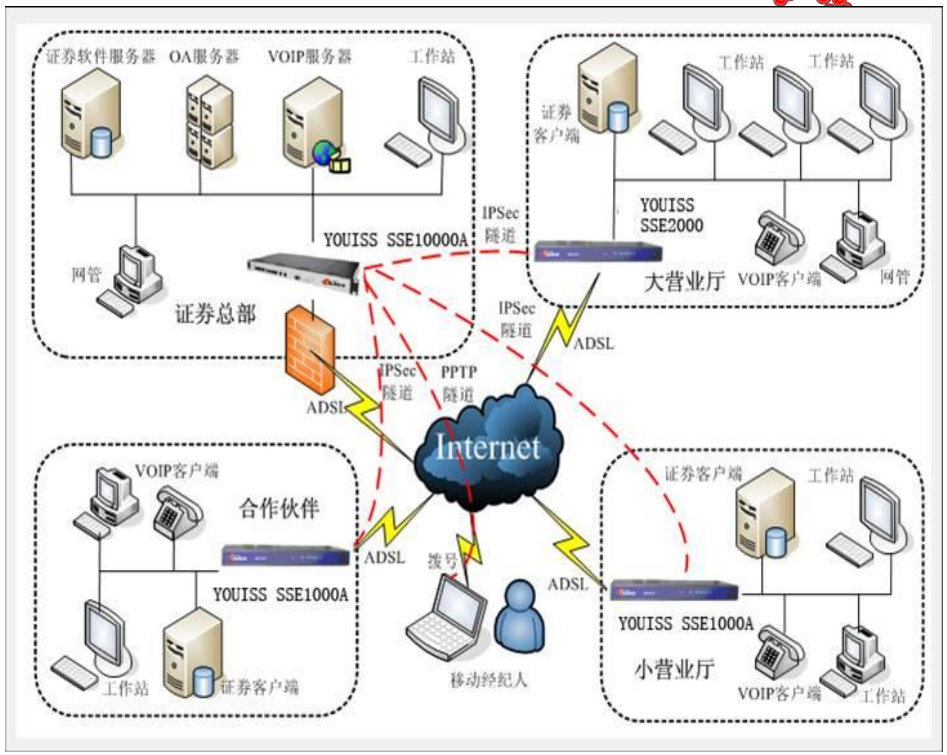
- 计算机网络概述
- 计算机网络的组成
- Internet基础
- 信息安全

本次课程所讲内容

- 计算机网络概述
- 计算机网络的组成
- Internet基础
- 信息安全

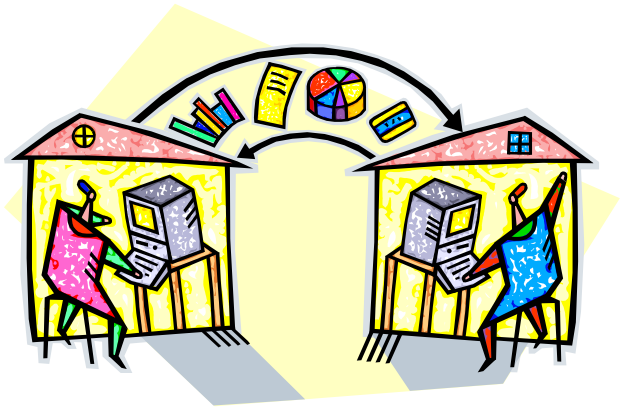
计算机网络的定义

计算机网络是指分布在**不同地理位置**的计算机系统，通过**通信线路**连接起来，在**网络操作系统**，**网络管理软件**及**网络通信协议**的支持下，实现数据传输和资源共享的系统。



计算机网络的功能与特点

- 资源共享
  - 硬件、软件、数据的共享
- 数据通信
  - 网络中计算机之间的数据传输和信息交换
- 分布式处理
  - 将一项复杂的任务划分为多个部分，由网络中的计算机分别来完成



计算机网络的性能指标

- 带宽
  - 表示数据传输速度的指标，单位是bps（bit per second）
- 误码率
  - 表示数据传输可靠性的指标
  - 误码率=接收端出现差错的比特数/总的发送的比特数

计算机网络的分类—按照覆盖范围分类

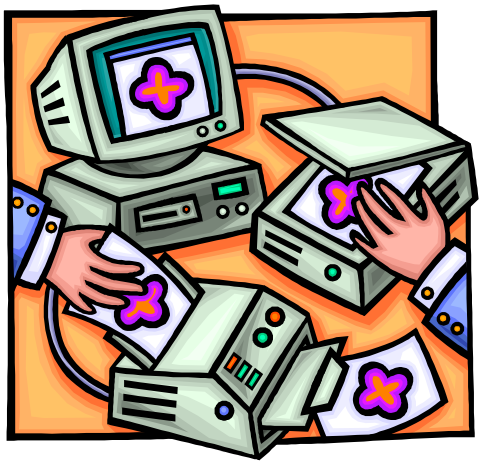
- 局域网（Local Area Network，LAN）
  - 覆盖范围为方圆几公里，通常用于一栋或几栋大楼，属于一个部门或者单位组建的专用网络，如公司或高校的内部网络
- 城域网（Metropolitan Area Network, MAN）
  - 城域网覆盖范围为几十~几百公里，一般来说是在一个城市
- 广域网（Wide Area Network，WAN）
  - 覆盖范围为几十~几千公里，网络跨越国界、洲界甚至全球范围，如Internet

计算机网络的分类—按照拓扑结构分类

- 安装或者建立网络时采用的布局形式叫拓朴结构，是网络中计算机之间的相互位置关系
- 网络的拓扑结构就是网络的形状

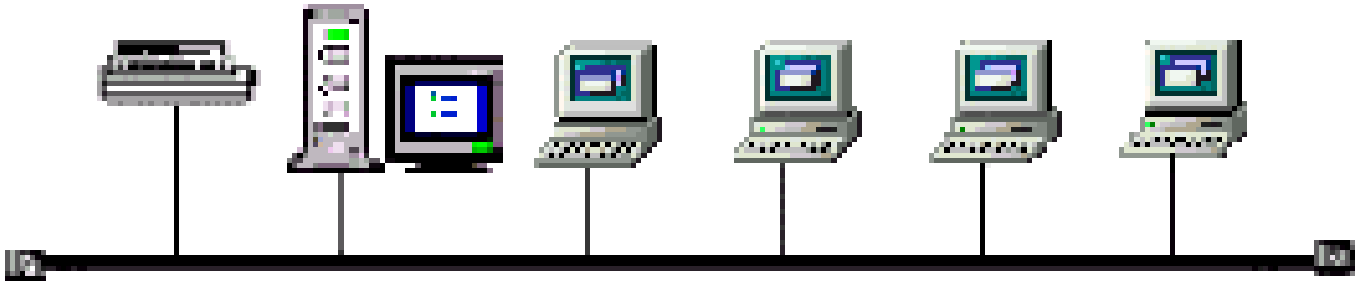
计算机网络的分类—按照拓扑结构分类

- 根据拓扑结构的不同，可以把计算机网络分为：
  - 总线型结构
  - 星型结构
  - 环型结构
  - 树型结构
  - 网状型结构



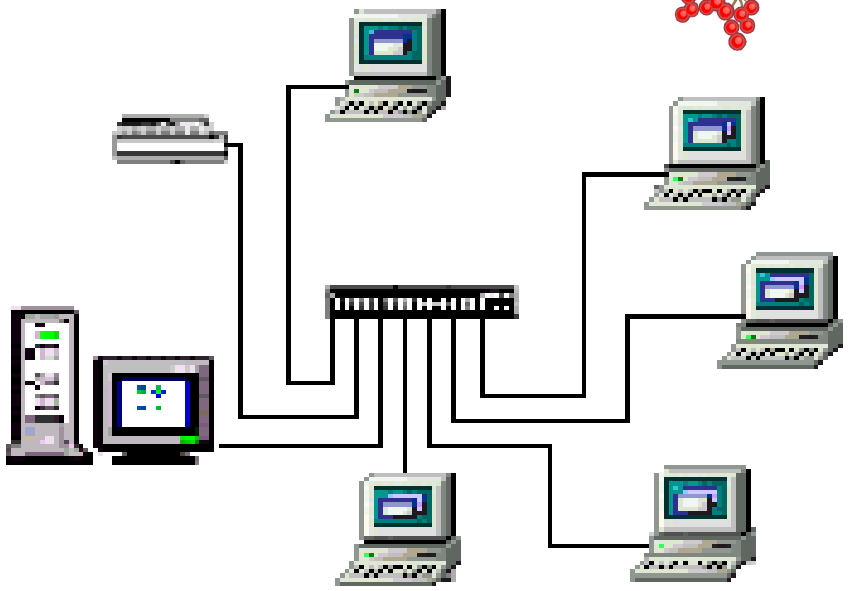
总线型结构

- 所有节点共享总线
- 安装简单方便，成本低，容易增删节点
- 总线任务重，易产生瓶颈问题



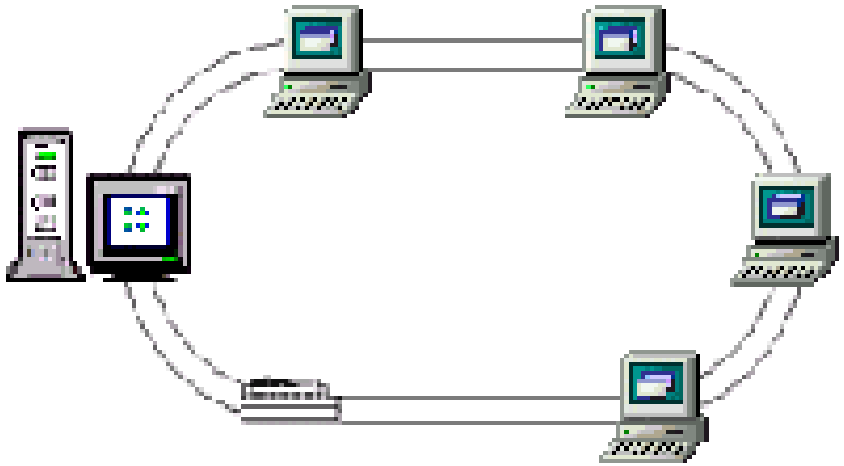
星型结构

- 中心站与各个节点组成
- 容易在网络中增删节点，容易实现网络监控
- 各节点间的信息交换必须由中心站中转，中心站超负荷或者发生故障时，整个网络停止工作



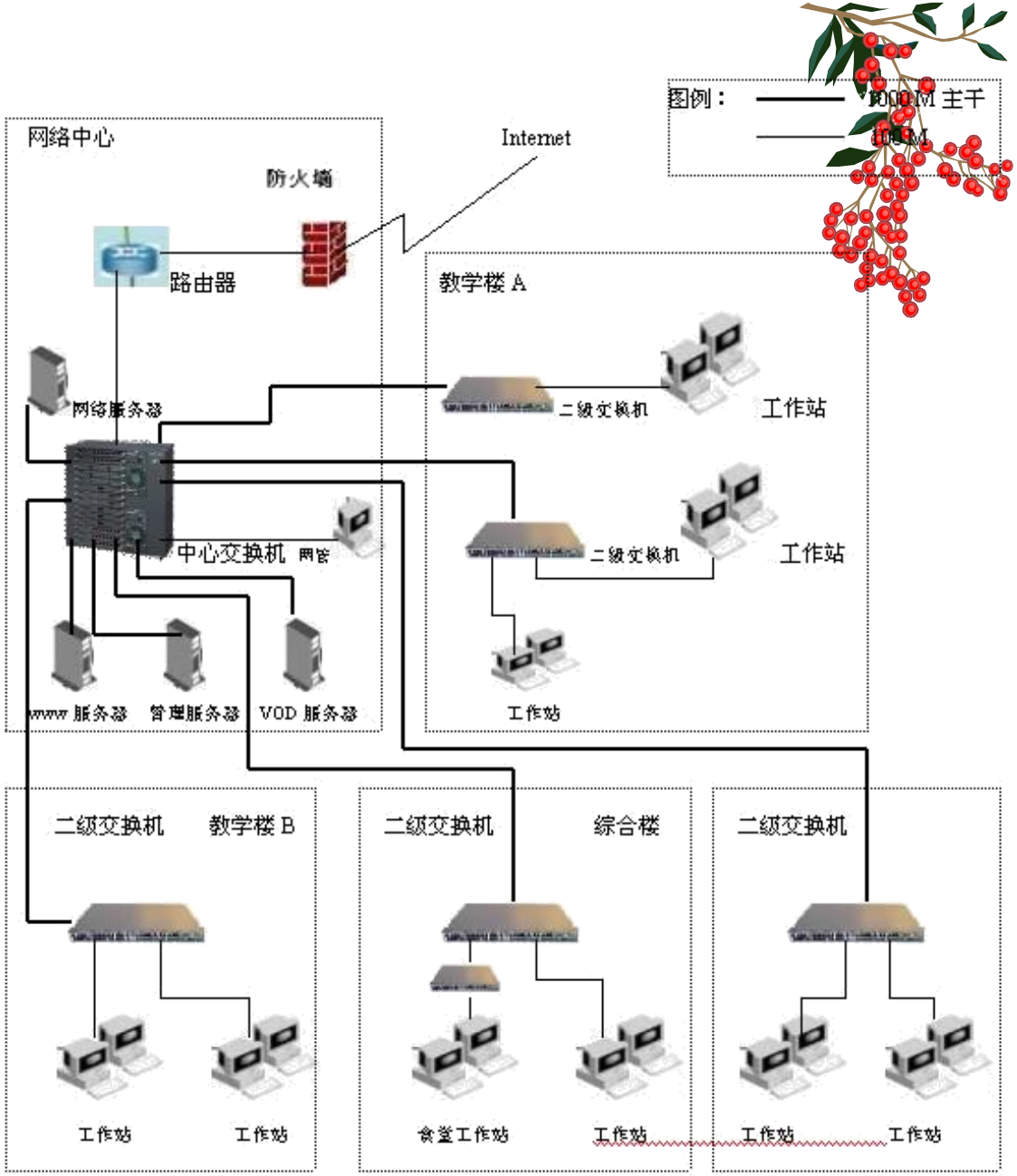
环型结构

- 各节点通过通信线路连成一个封闭的环形
- 网络建成后，难以增删节点
- 某一个节点发生故障，都可能导致整个网络停止工作



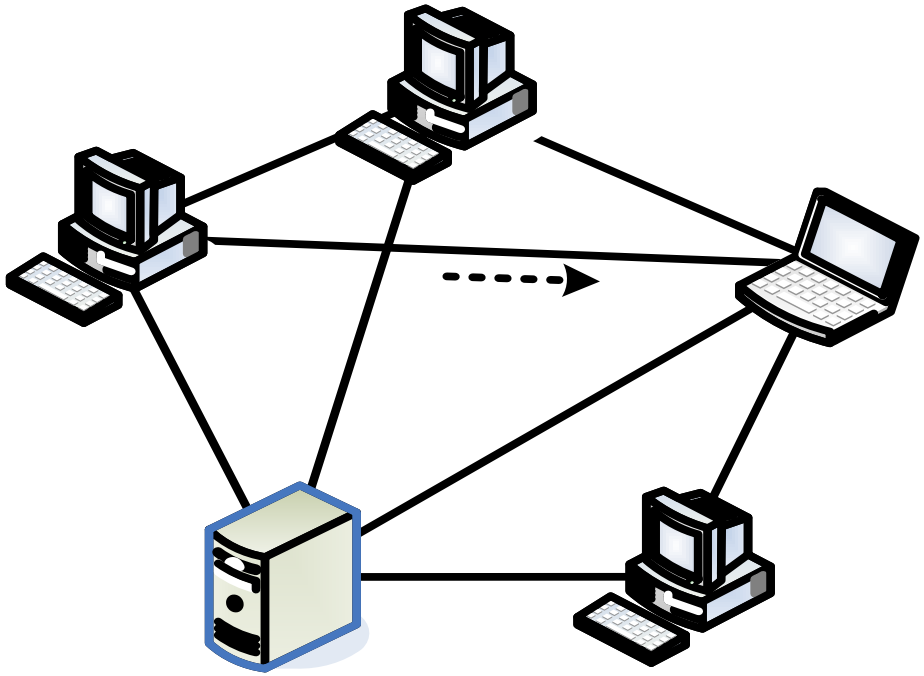
树型结构

- 树型结构是星型结构的扩展

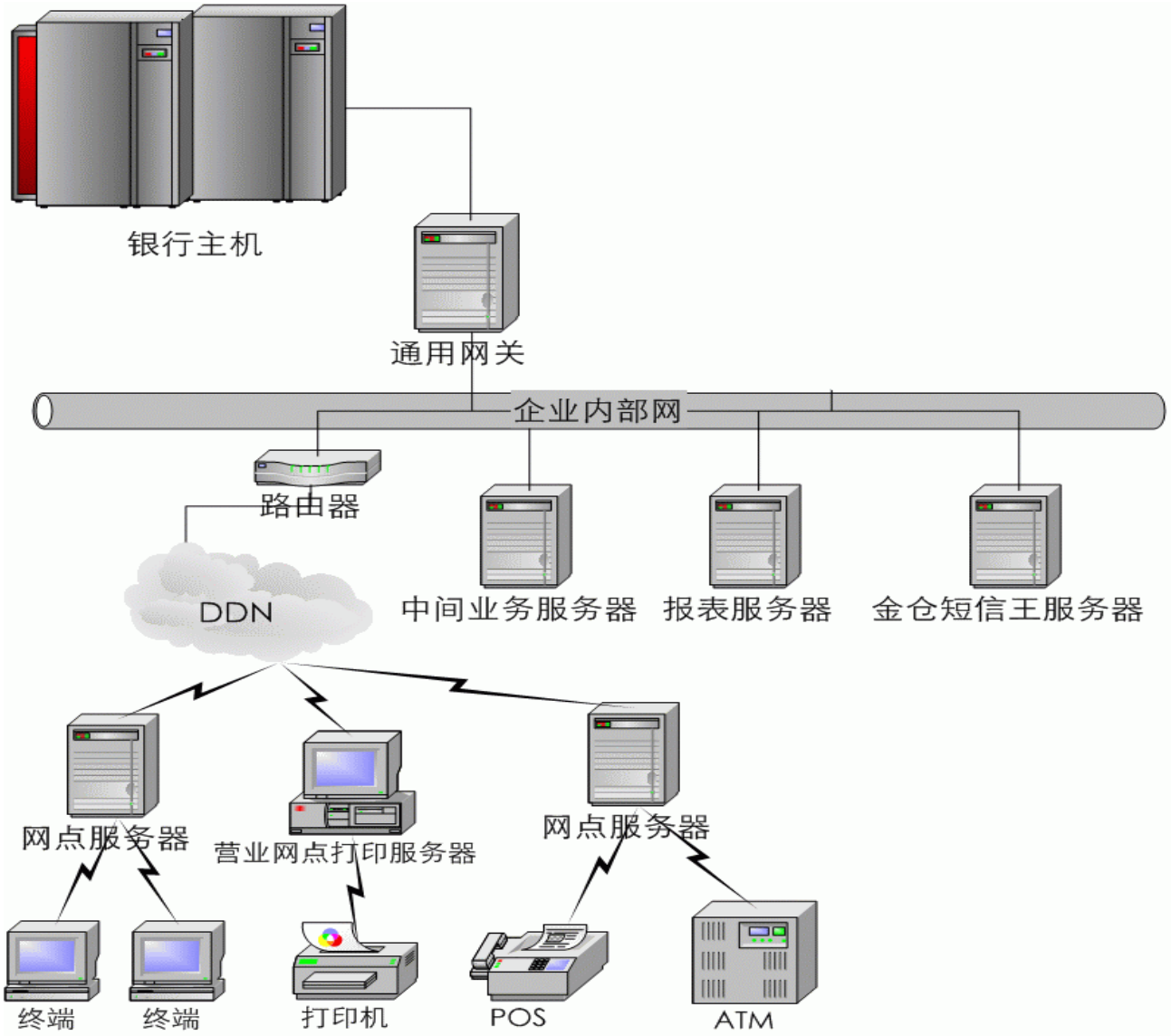


网状型拓扑结构

网状型结构的网络，其中任何一个结点都至少和其他两个结点相连，因而网络是非常可靠，但控制复杂，建网较难造价高。



实际的网络可能包含多种拓扑结构

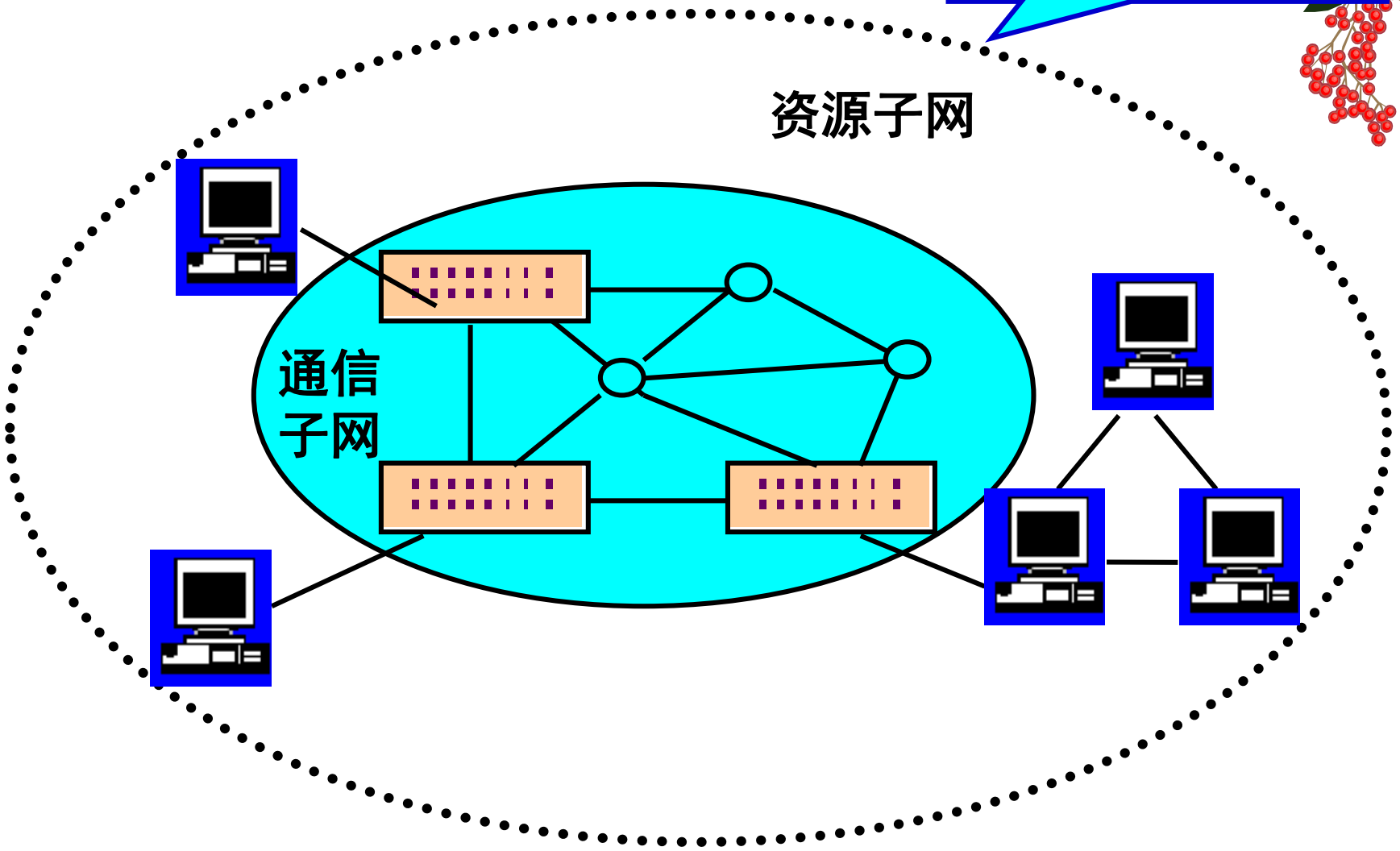


本次课程所讲内容

- 计算机网络概述
- 计算机网络的组成
  - 通信子网
  - 资源子网
  - 网络协议
- Internet基础
- 信息安全

计算机网络的组成

还要有网络协议



什么是通信子网？

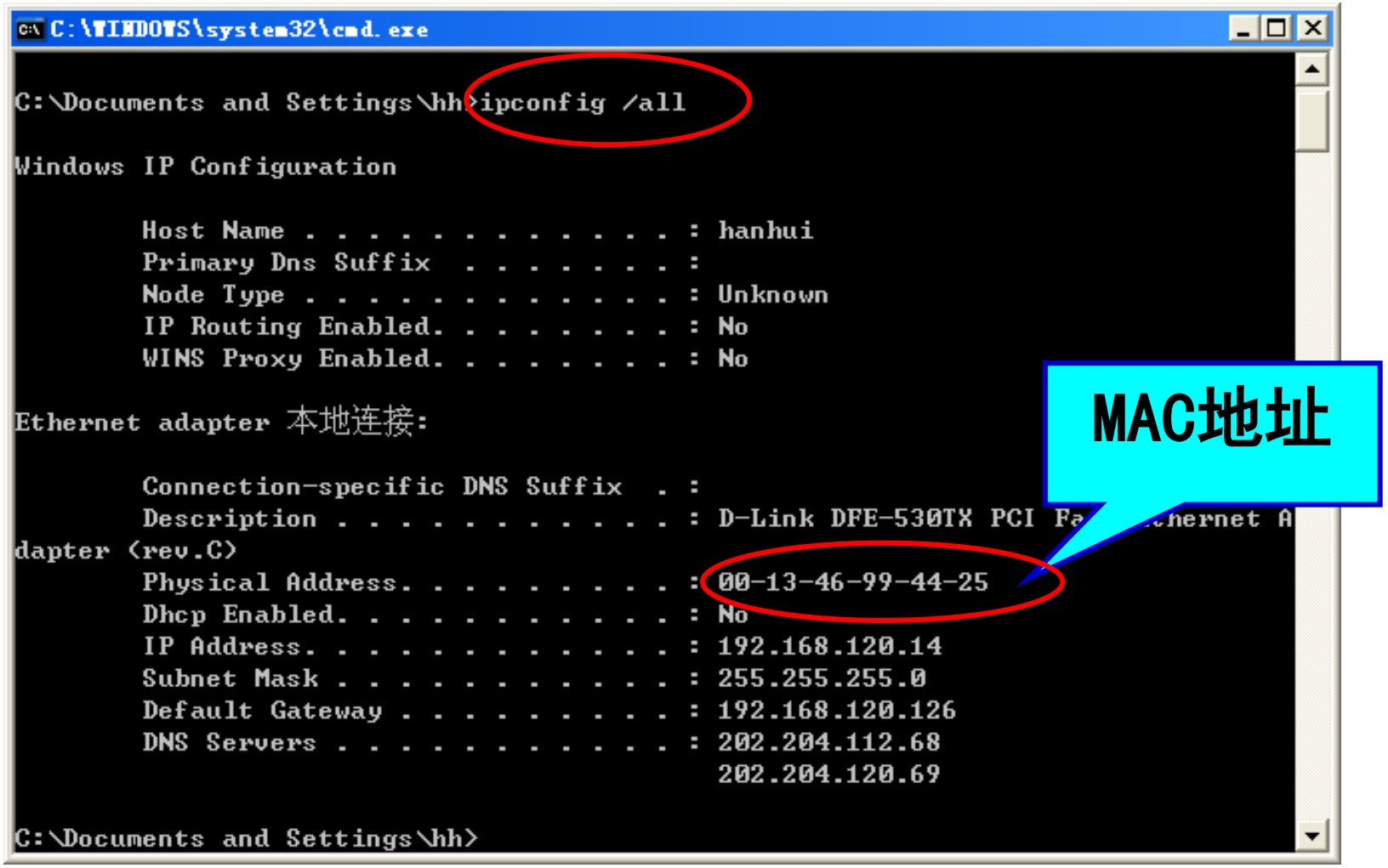
- 通信子网是指提供计算机之间互相传输信息的通路

通信子网的构成——网卡

- 连接计算机与网络的硬件设备
- 每块网卡都有一个唯一的物理地址(MAC地址)
- MAC地址是12位的十六进制数，前6位代表生产厂商，后6位是生产厂商分配给网卡的唯一号码

网卡的MAC地址

开始→运行→cmd



通信子网的构成——传输介质

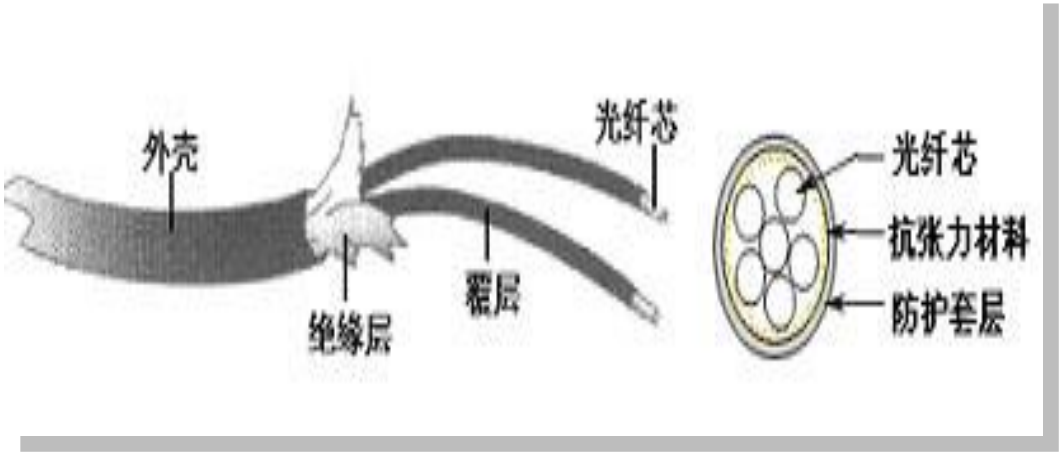
- 传输介质在网络中是连接收发双方的物理通路
  - 有线介质
    - 双绞线电缆、光纤
  - 无线介质
    - 无线电波、红外线等

双绞线（常用于局域网）

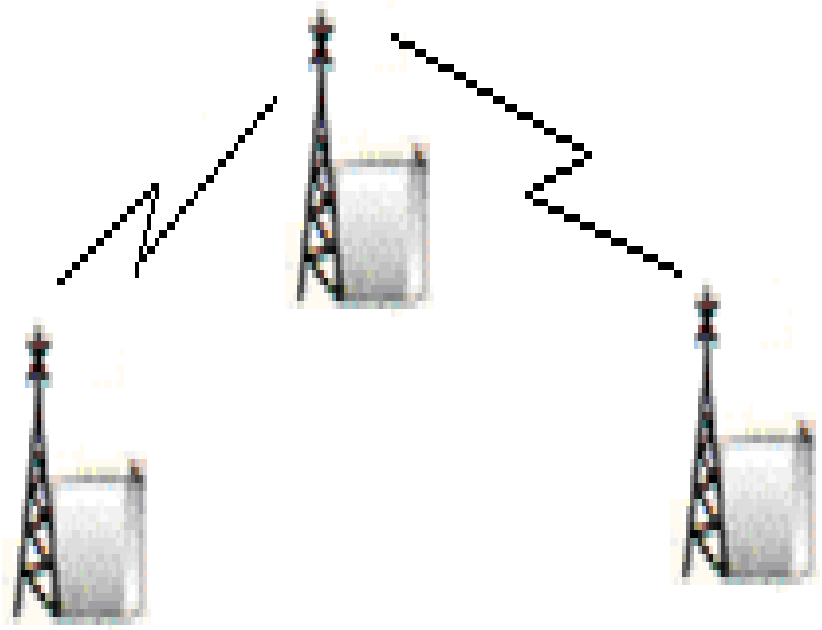
RJ45接头(水晶头)

光纤(常用于骨干网)

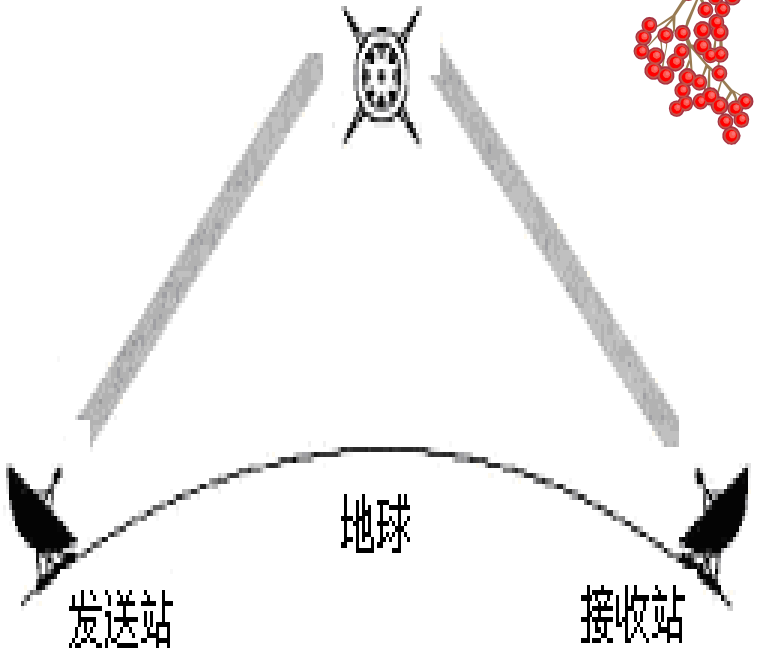
- 由一捆能传输激光光束的细微而柔韧的玻璃纤维组成
- 抗干扰能力强，传输距离远，传输容量大，但易折断



无线介质



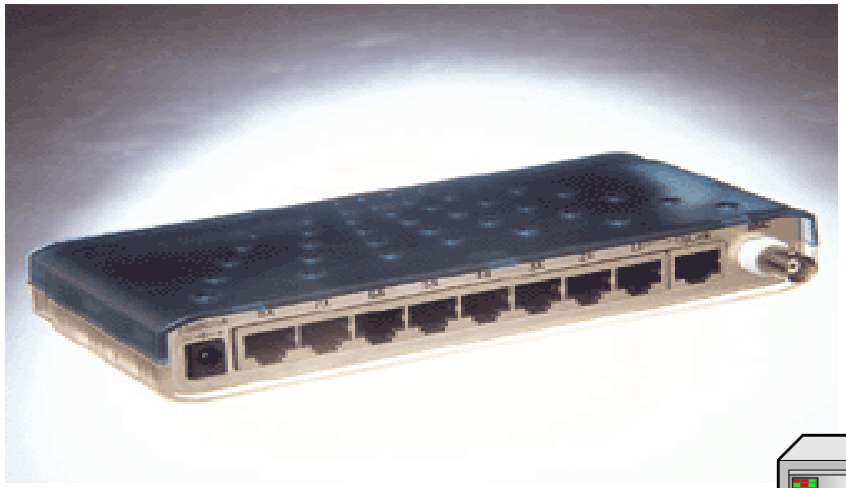
地面接收站

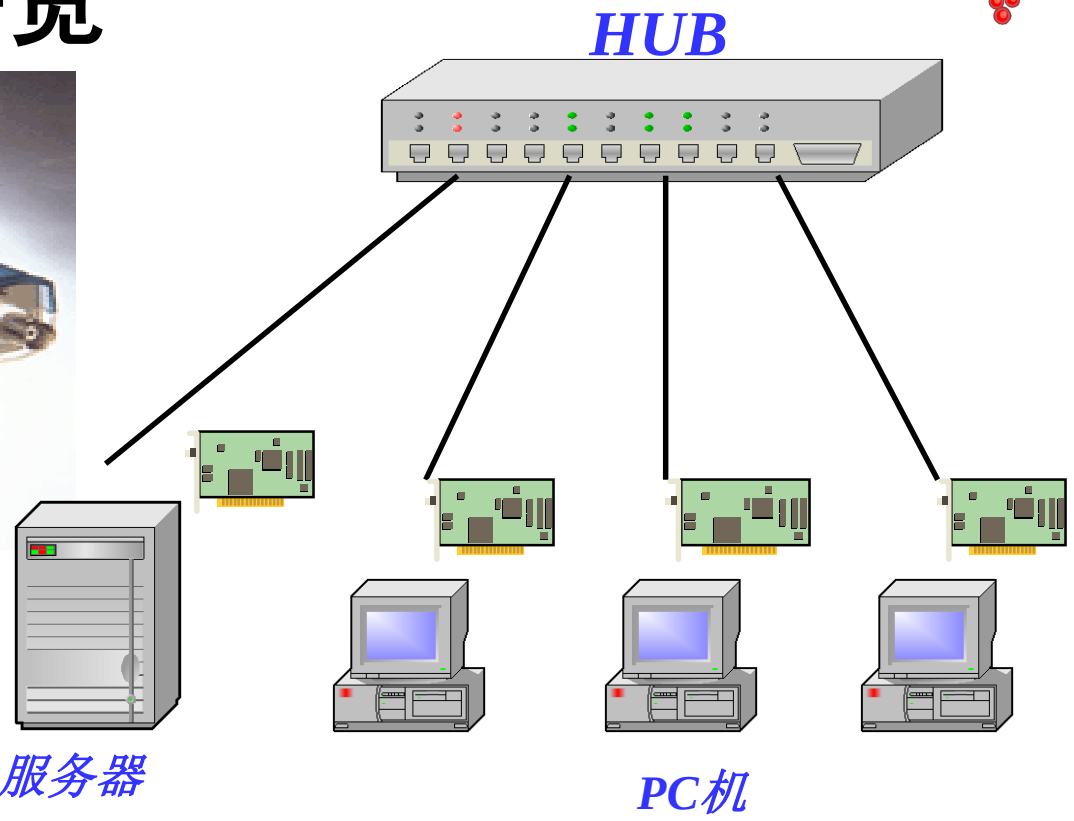


卫星

通信子网的构成——集线器(Hub)

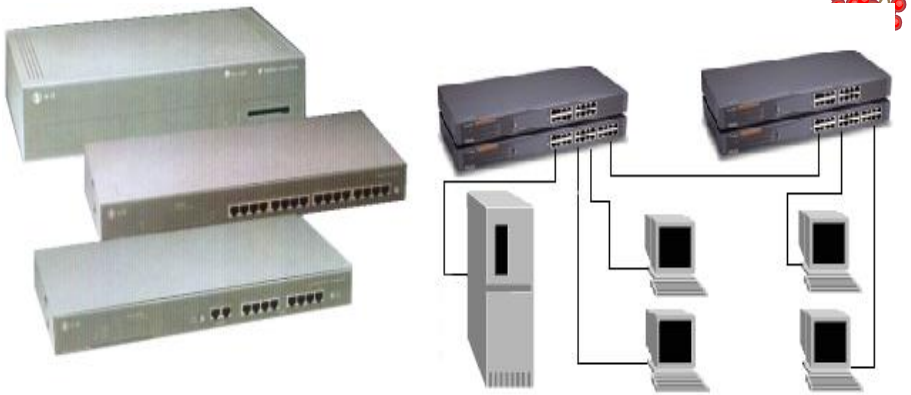
- 局域网内计算机之间的通信互联设备
- 所有主机共享带宽





通信子网的构成——交换机（switch）

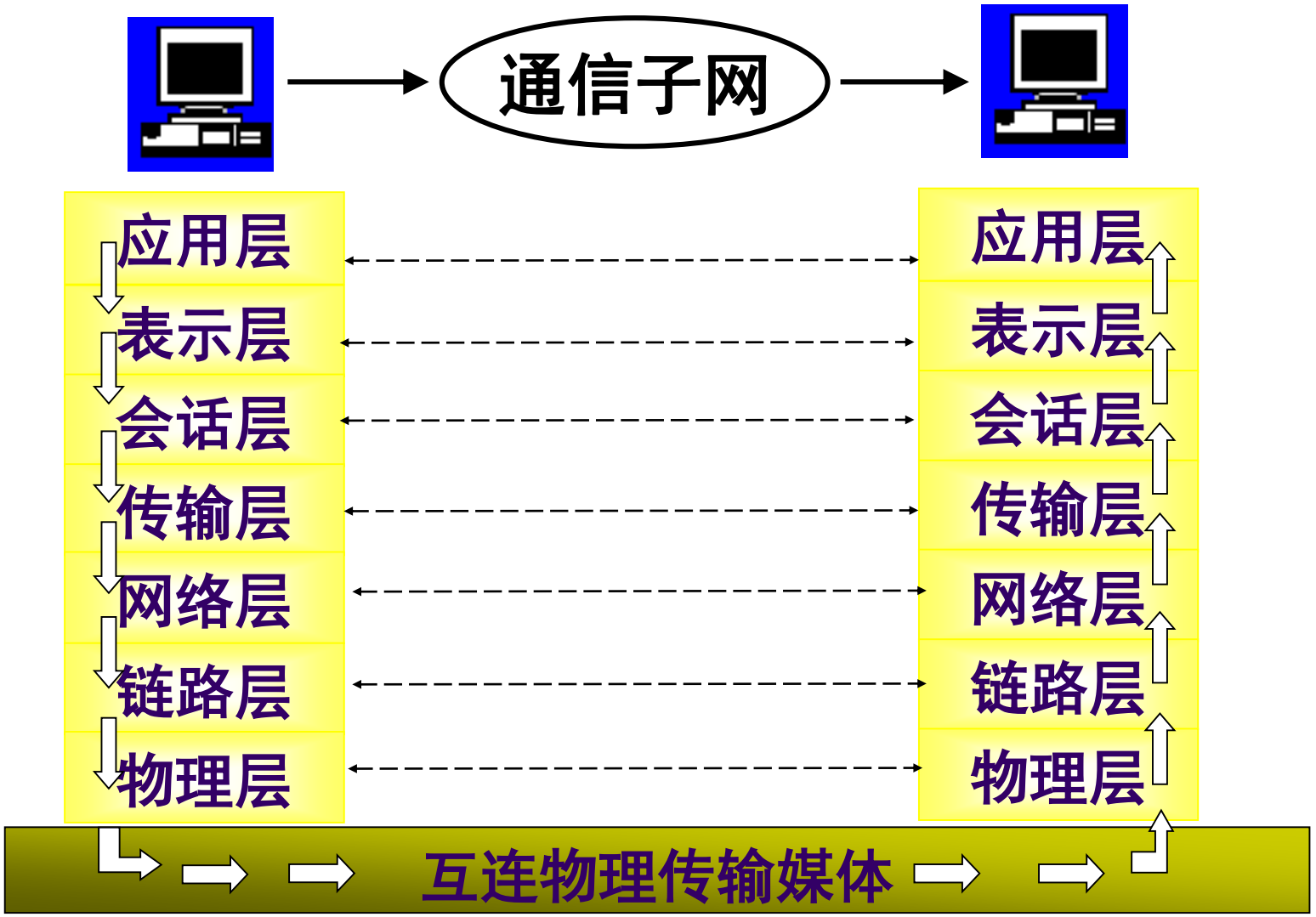
- 局域网内计算机之间的通信互联设备
- 最佳可达到每台主机独享带宽



什么是资源子网？

- 资源子网是指连接在通信子网上的计算机
- 一般用户使用的计算机称为**客户机**，提供各种服务的计算机称为**服务器**，有些计算机兼有两种功能

网络协议—开放系统互连参考模型OSI



网络协议—TCP/IP（因特网的核心技术）

<table>
<tr><th>OSI</th><th>TCP/IP</th></tr>
<tr><td>应用层</td><td rowspan="3">应用层 Telnet、SMTP、FTP</td></tr>
<tr><td>表示层</td></tr>
<tr><td>会话层</td></tr>
<tr><td>传输层</td><td>传输层 TCP、UDP协议</td></tr>
<tr><td>网络层</td><td>网间层 IP协议</td></tr>
<tr><td>数据链路层</td><td rowspan="2">网络接口层</td></tr>
<tr><td>物理层</td></tr>
</table>

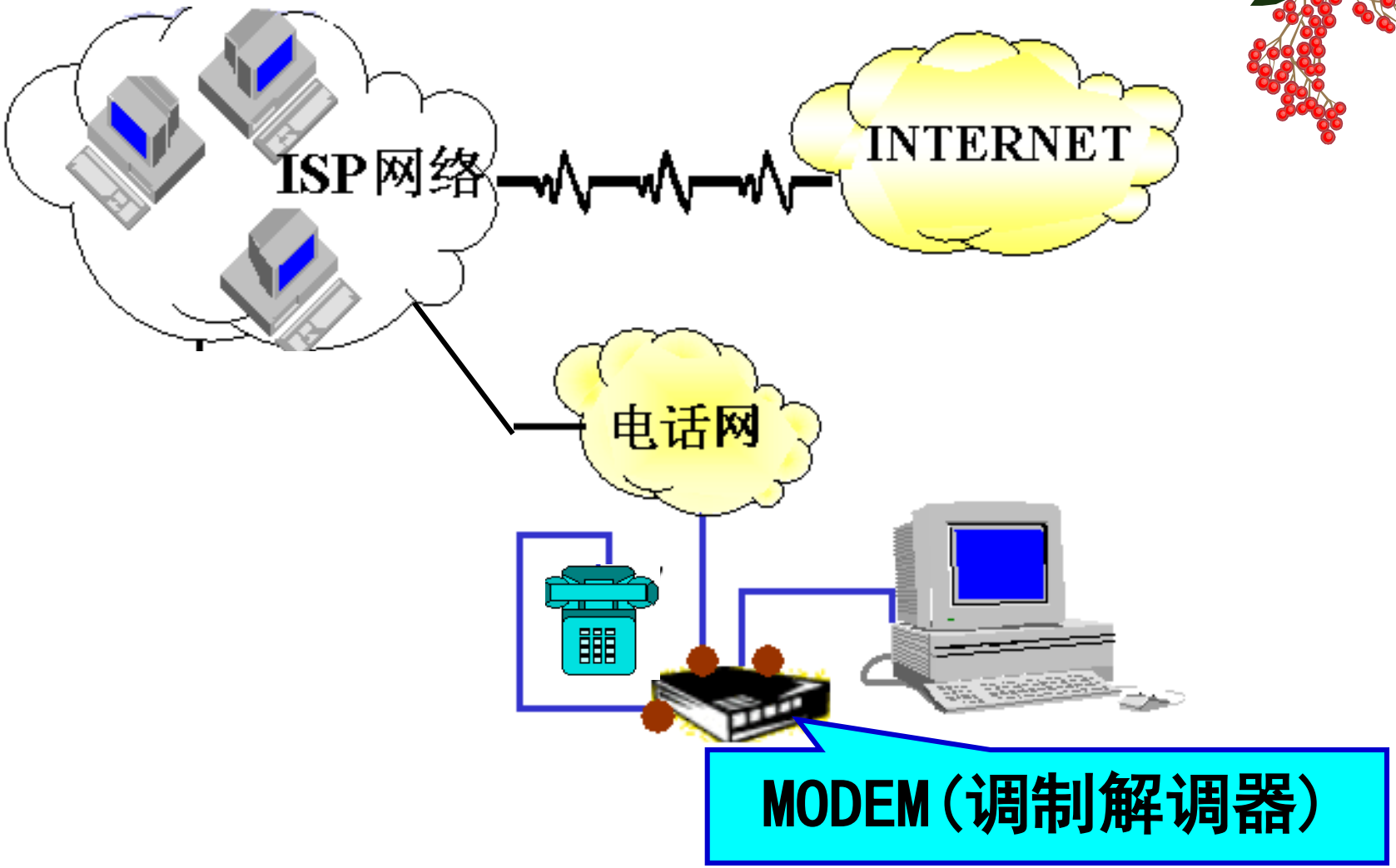
本次课程所讲内容

- 计算机网络概述
- 计算机网络的组成
- Internet基础
- 信息安全

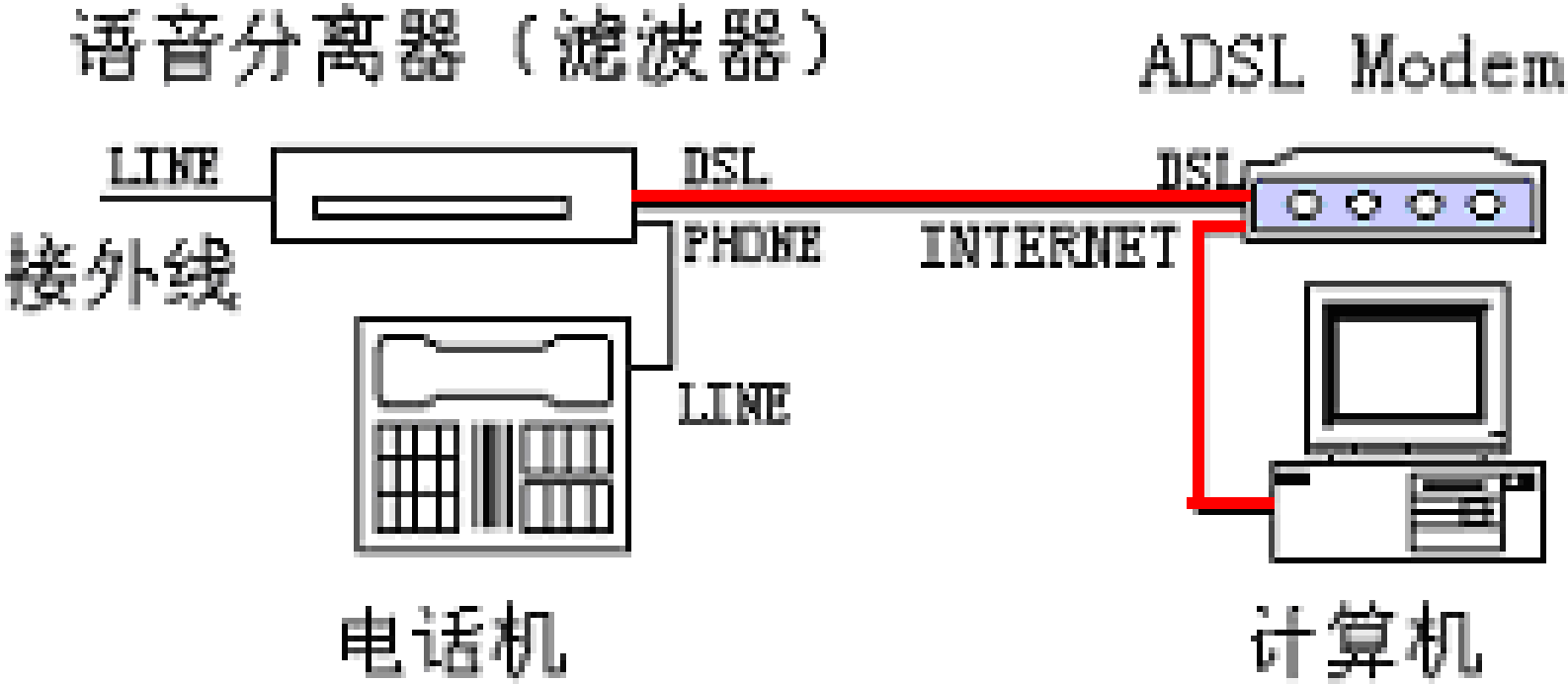
Internet接入技术

- 通过电话线拨号上网
- 通过ADSL技术上网
- 通过局域网上网
- 用户需要与因特网服务提供商(ISP)联系

通过电话线拨号上网



通过ADSL技术上网


语音分离器（滤波器）
ADSL Modem
LINE
DSL
DSL
接外线
PHONE
INTERNET
LINE
电话机
计算机

通过局域网上网

- 网卡
- 网线
- 交换机(如果网口数小于机器数)

IP地址

- TCP/IP规定Internet上的每台主机具有惟一的标识，即IP地址
- 目前使用的IPv4版本IP地址共占32位二进制数(4个字节)，每个字节用一个十进制数表示，字节之间用“.”间隔，如202.204.120.77

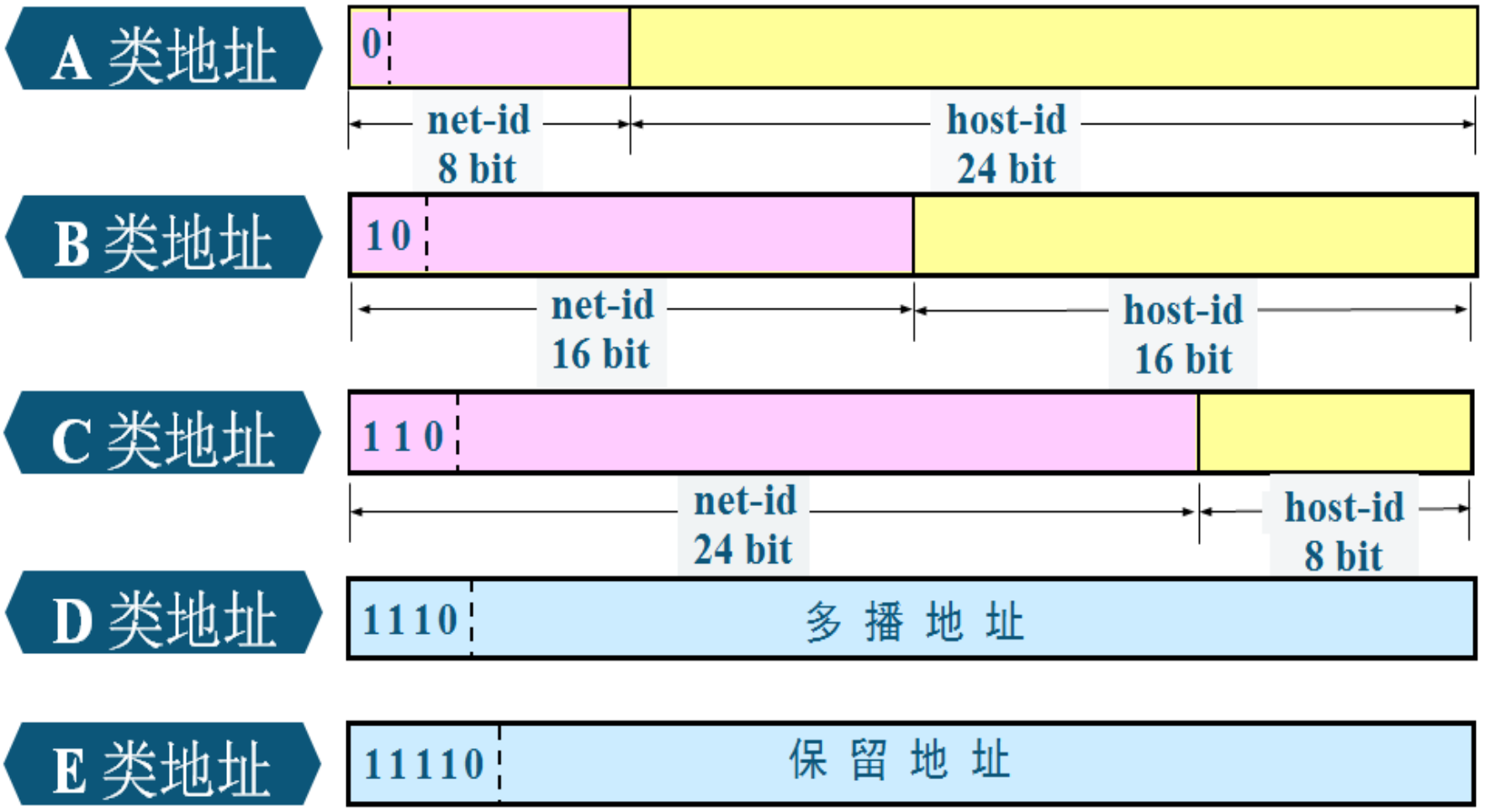
IP地址的规定

- IP地址的每一段数字的范围为0～255
- IP地址的第一段数字不能为127，127.0.0.1代表主机本身
- IP地址 ＝ 网络地址+主机地址

IP地址的分类

- A类网络的IP=网络地址(前8位)+主机地址(后24位)
  - 1.0.0.1~126.255.255.254
- B类网络的IP=网络地址(前16位)+主机地址(后16位)
  - 128.0.0.1~191.255.255.254
- C类网络的IP=网络地址(前24位)+主机地址(后8位)
  - 192.0.0.1~223.255.255.254
- 网络地址不能全为0或全为1
- 主机地址不能全为0或全为1

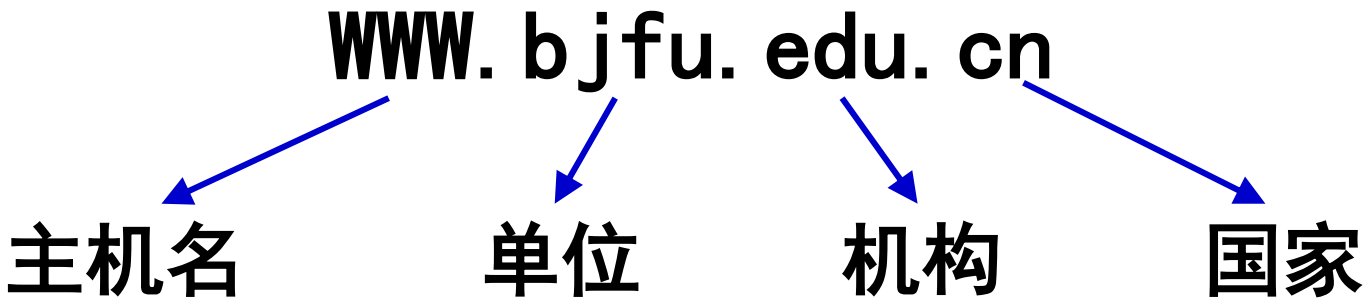
IP地址的分类


A 类地址
0
net-id
8 bit
host-id
24 bit
B 类地址
10
net-id
16 bit
host-id
16 bit
C 类地址
1 1 0
net-id
24 bit
host-id
8 bit
D 类地址
1110
多 播 地 址
E 类地址
11110
保 留 地 址

域名

- IP地址是一串数字，不便于识别和记忆，通常用具有一定含义的、容易记忆的一串字符来代替IP地址，这一字符串被称为域名。
- 域名的构成

域名服务器(DNS服务器)存放域名和IP地址的对照列表



国家或地区代码

代　码	国家或地区	代　码	国家或地区
cn	中国	dk	丹麦
fr	法国	kr	韩国
au	澳大利亚	ge	德国
ca	加拿大	it	意大利
jp	日本	hk	中国香港特别行政区
uk	英国	tw	中国台湾省

机构名称代码

机构代码	代表机构	机构代码	代表机构
com	商业机构	mil	军事机构
edu	教育科研机构	net	网络机构
gov	政府机构	org	民间组织

Internet基本服务——浏览网页

- WWW (World wide web)
  - 万维网Web，采用HTML语言进行信息发布和检索
- HTML语言
  - 超文本标记语言，包含HTML标记定义的页面元素
- Web浏览器和Web服务器
- HTTP
  - 超文本传输协议，是Web浏览器和Web服务器之间的通信协议

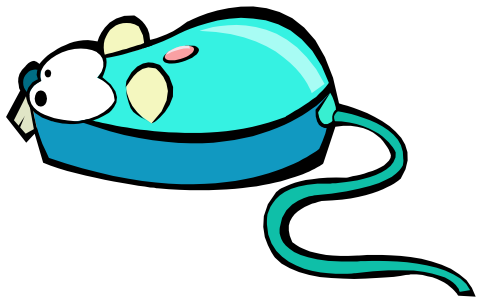
Internet基本服务——浏览网页

- URL
  - 统一资源定位器，俗称“网址”
  - URL的格式为

    协议类型://服务器(:端口号)/路径
  - http://www.163.com/public/index.htm
  - ftp://202.204.120.77/hanhui

Internet基本服务——其他应用

- 搜索引擎
- 网上购物
- 网上银行
- 网络视频
- 网络教育
- 电子邮件
- 网络游戏
- ……



本次课程所讲内容

- 计算机网络概述
- 计算机网络的组成
- Internet基础
- 信息安全

什么是信息安全？

信息安全强调信息的保密性（Confidentiality）、完整性（Integrity）和可用性（Availability）

保密性：确保机密信息不被窃听、不被泄漏，不被非授权的个人、组织和计算机程序使用。

完整性：确保数据的一致性，保证信息没有遭到篡改和破坏。

可用性：确保拥有授权的合法用户或程序可以及时、正常使用信息。

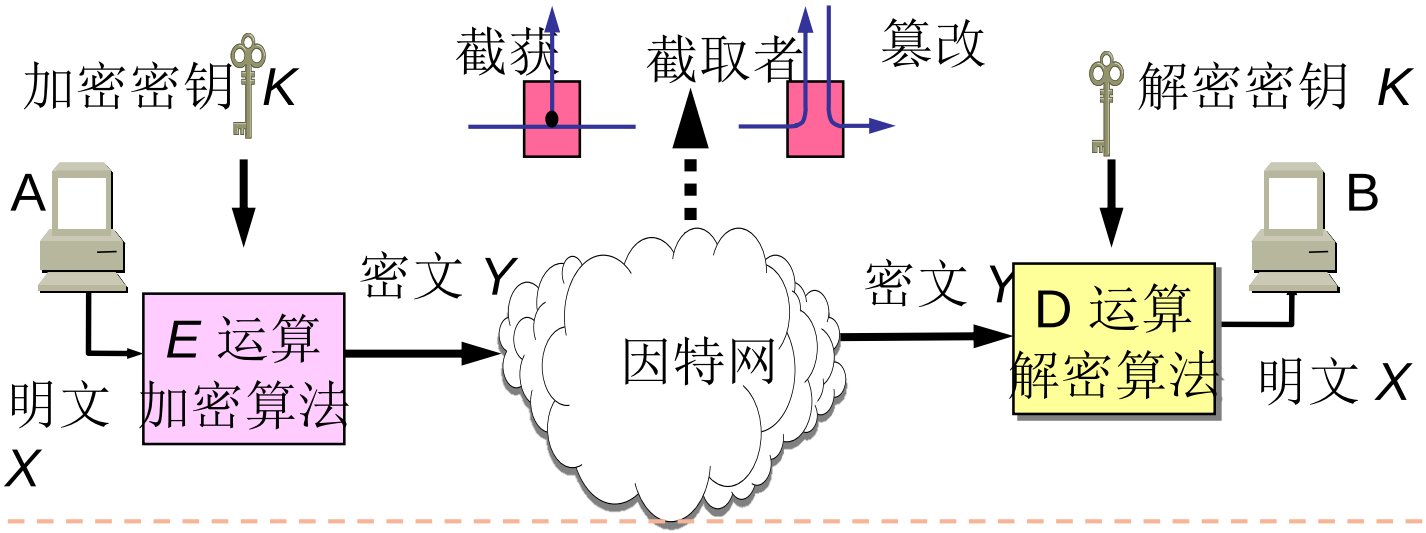
数据加密技术

数据加密技术是指将一个信息（或称明文）经过加密密钥及加密函数转换，变成没有任何规律的密文，而接收方则将此密文经过解密函数、解密密钥还原成明文。

加密技术是网络安全技术的基石，密码学是数据加密和解密的技术基础。

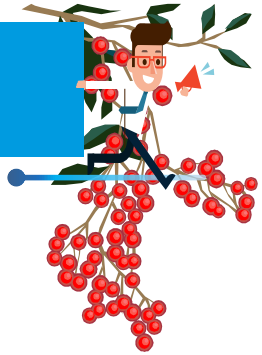
密码学分为**密码编码学**和**密码分析学**。密码编码学是对信息进行编码，实现隐蔽信息。密码分析学是是对密码进行研究分析和破译。

加密与解密过程



密码体制也叫密码系统，是指能完整地解决信息安全中的机密性、数据完整性、认证及身份识别、可控性及不可抵赖性等问题的。

密码体制



传统密码体制里所用的加密密钥和解密密钥相同，称为**对称密码**体制；

如果加密密钥和解密密钥不相同，则称为**非对称密码**体制。

替代密码

替代密码(substitution cipher)的原理可用一个例子来说明。（密钥是 3）

明文	abcdefghijklmnopqrstuvwxyz
密文	DEFGHIJKLMNOPQRSTUVWXYZABC

caesar cipher → FDHVDU FLSKHU

明文 c 变成了密文 F

置换密码

置换密码(transposition cipher)则是按照某一规则重新排列消息中的比特或字符顺序。

密钥	CIPHER
顺序	145326
明文	attack
	begins
	atfour

根据英文字母在26个字母中的先后顺序，我们可以得出密钥中的每一个字母的相对先后顺序。因为密钥中没有A和B，因此C为第1。同理，E为第2，H为第3，……，R为第6。于是得出密钥字母的相对先后顺序为145326。

密文的得出

密钥	CIPHER
顺序	145326
明文	attack
	begins
	atfour

先读顺序为 1 的明文列，即 aba

密文的得出

密钥	CIPHER
顺序	145326
明文	attack
	begins
	atfour

最后读顺序为 6 的明文列，即 ksr

因此密文就是：abacnuaiotettgfksr

接收端收到密文后按列写下

收到的密文：abacnuaiotettgfksr

密钥	CIPHER
顺序	145326
明文	a
	b
	a

先写下第 1 列密文 aba

接收端收到密文后按列写下

收到的密文：abacnuaiotettgfksr

密钥	CIPHER
顺序	145326
明文	attack
	begins
	atfour

最后写下第 6 列密文 ksr

接收端从密文解出明文

收到的密文：abacnuaiotettgfksr

密钥	CIPHER
顺序	145326
明文	attack
	begins
	atfour

最后按行读出明文

Thanks!