第二章 互联网核心技术

2.1 互联网技术演化历程

2.2 分组交换

2.3 TCP/IP模型

- 2.3.1 网络体系结构模型
- 2.3.2 网际互连协议
- 2.3.3 简单网络不简单
- 2.3.4 传输控制协议
- 2.3.5 TCP/IP改进措施

2.4 网络应用

- 2.4.1 应用层网络
- 2.4.2 万维网
- 2.4.3 网络社交

2.5 网络安全

2.1 互联网技术演化历程

分组交换

- 1964~1966年，分组交换技术产生；
- 1969年，根据美国ARPA提出的要求， ARPANET问世；
- 1972年，第一届国际计算机通信会议成立Internet工作组；
- 1973年，美国国防部开始研究不同计算机网互联；
- 1974年，IP和TCP问世，公开TCP/IP核心技术；

TCP/IP

- 1980年，美国人Vinton Cerf提出用TCP/IP联接所有计算机网络；
- 1983年，ARPANET分解APRPANET和MILNET；
- 1985～1986年，NSFNET成立，接管了ARPANET，后更名为Internet；
- 1987年，NSFNET升级、1990年，ARPANET关闭；
- 1989年，瑞士人Tim Berners-Lee发明World Wide Web；

WWW技术

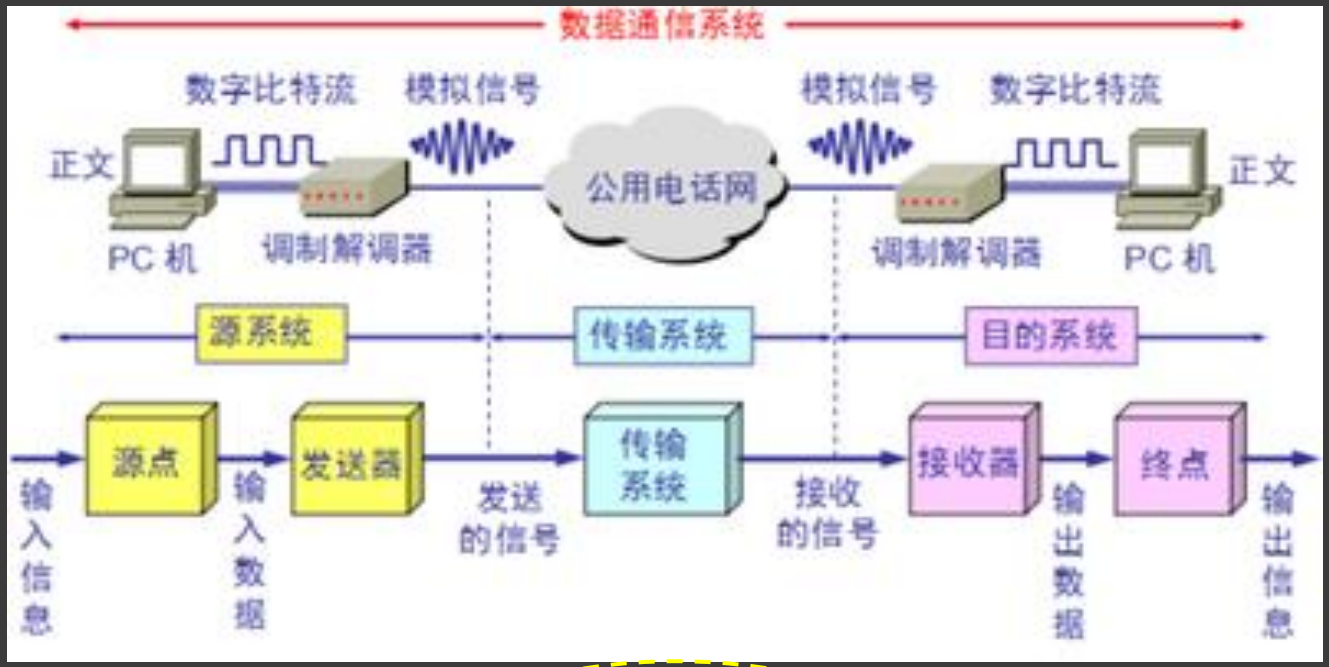
- 1991年，互联子网超过3000个，C/S模式开始应用推广；
- 1992年，国际Internet协会ISOC成立；
- 1996年，开始研究和实施下一代互联网计划——NGI；
- 2000~2010年，宽带IP网、移动互联网；

网络融合

- 2010- ，互联网技术泛在化、5G网络、…。

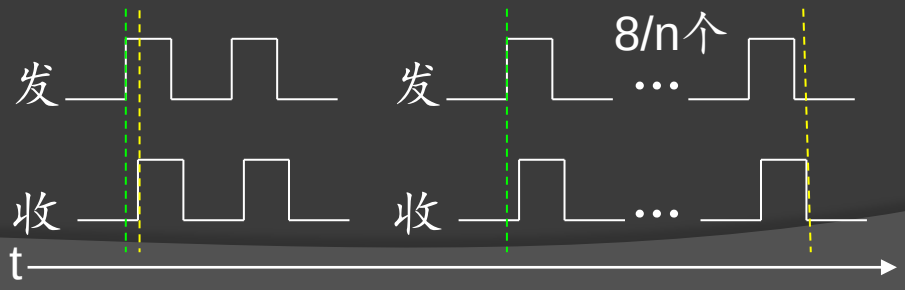
2.2 分组交换

点对点数据通信模型



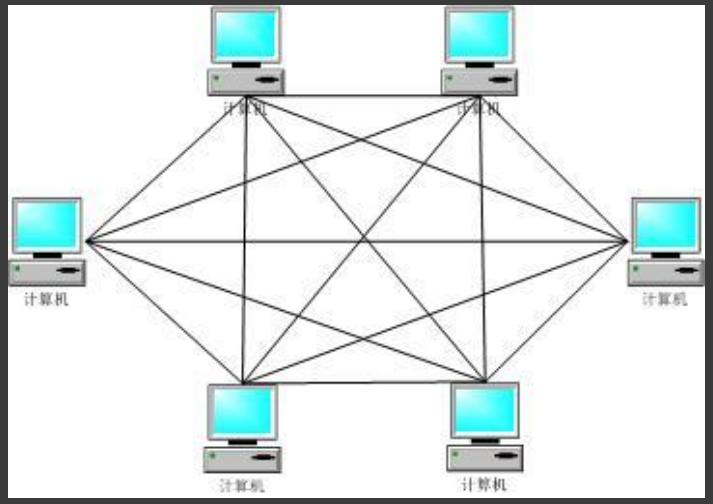
采样→编码→调制→发送 ⟶ 接收→解调→解码→还原

同步：位同步；字同步/码同步；帧同步；网同步。



网络通信

点对点网络



传输效率高；

利用率很低；

通信成本高昂。

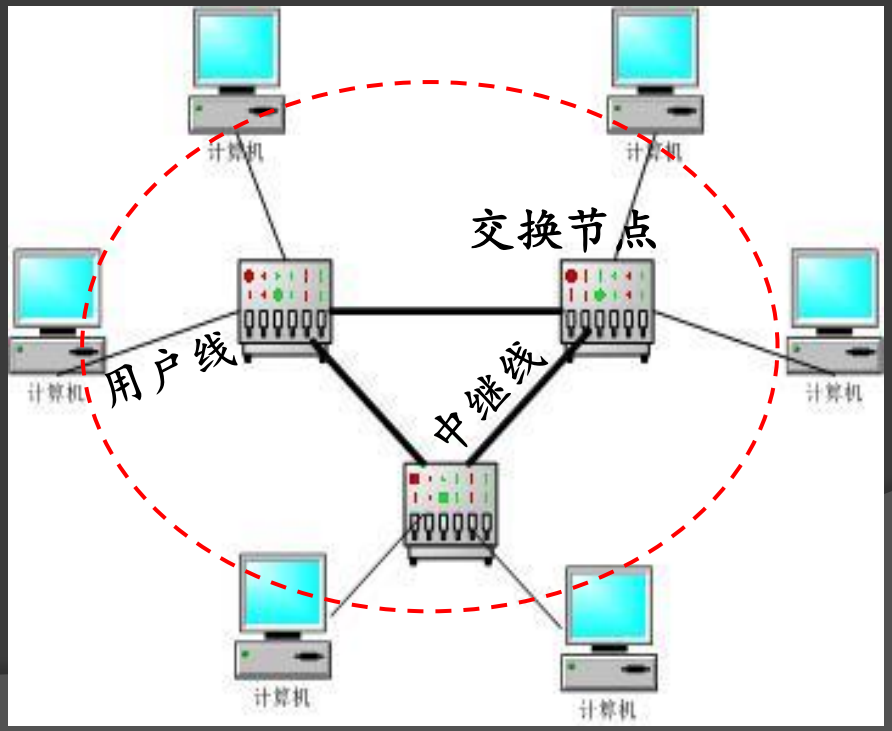
终端系统：

计算机、打印机、存储设备、传感设备、应用软件。

传输系统：

链路、交换设备、控制软件。

交换网络



利用率高；

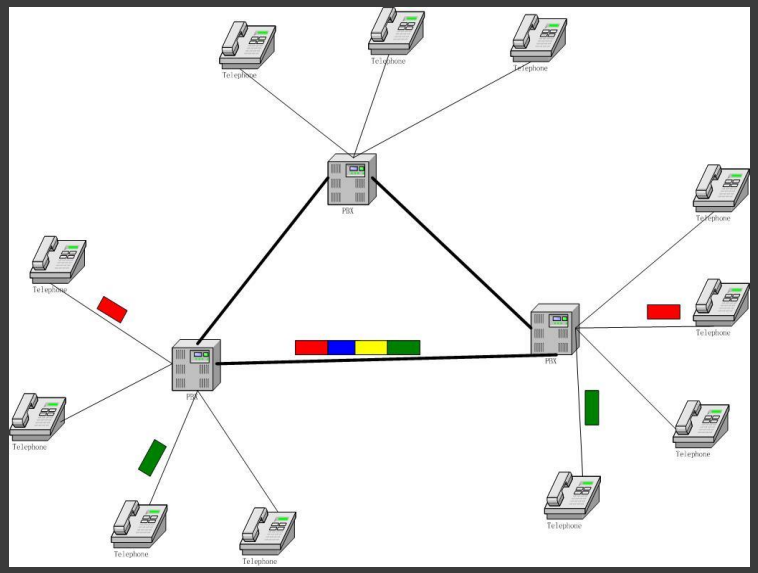
通信成本分担；

时延增大。

交换：中继和转发过程。

资源复用：一份资源被多个用户同时共同使用。

网络交换实现方式：电路交换和分组交换两类。



电路交换：

- ✓ 提供有连接传输服务；
- ✓ 网络传输时延有保证；
- ✓ 遇故障需重新建立连接；
- ✓ 按连接时间计费。

连接：通信双方为数据传输建立的一次临时性的联系过程。

面向连接的通信传输

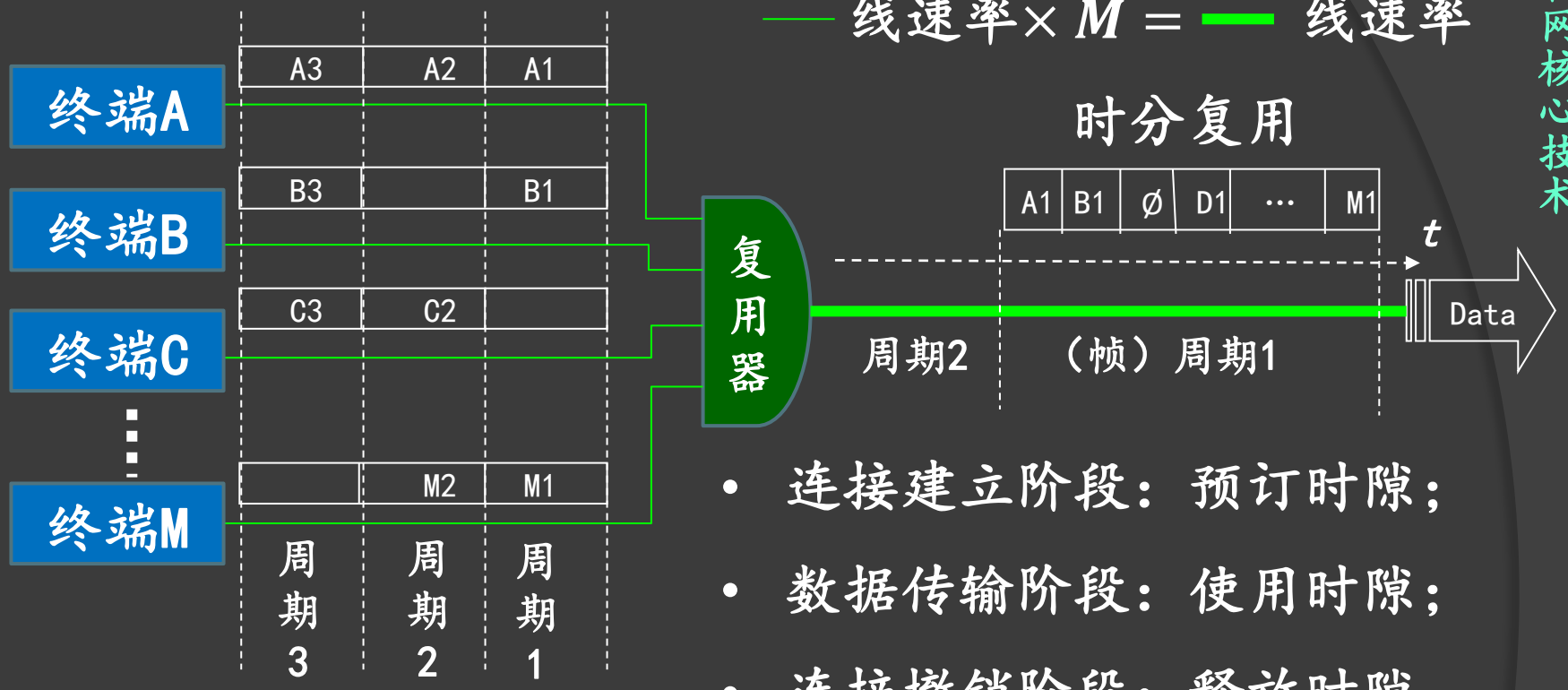
- 建立连接：预订路径、预留资源；
- 传输数据：交换数据、维护已建立的连接；
- 撤销连接：释放约定的路径和有关资源。

链路复用：

- ✓时分复用
- ✓波分复用
- ✓码分复用

基于连接的链路调用 ⟶ 基于时隙的链路复用

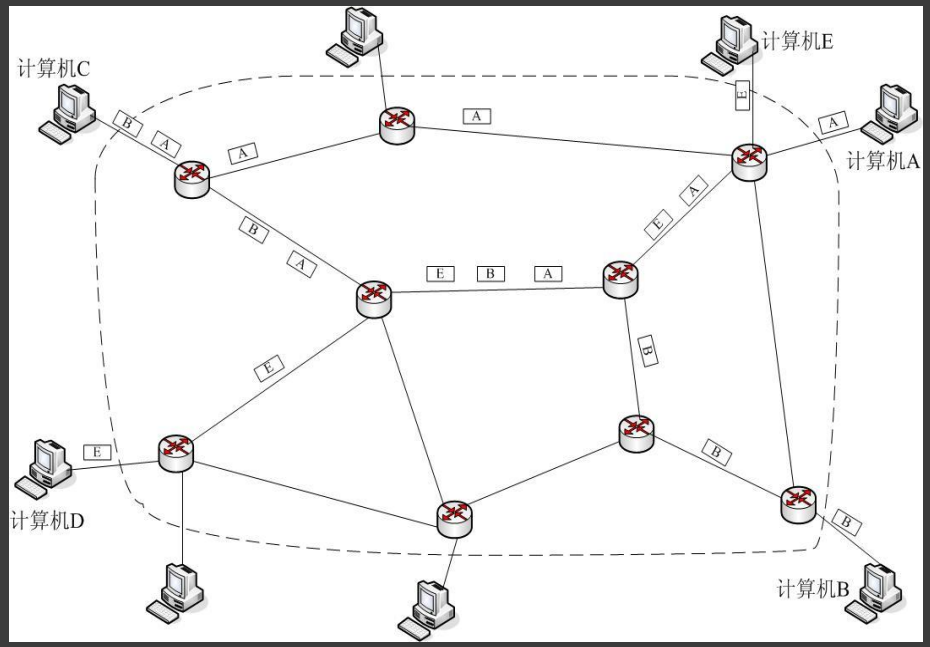
时分复用——TDM机制



- 连接建立阶段：预订时隙；
- 数据传输阶段：使用时隙；
- 连接撤销阶段：释放时隙。

“突发性”传输：传输发生的时间、传输持续的时间不确定。

问题：
- 随机性数据传输与周期性时隙调度不匹配。
- 固定时隙长度与变化数据长度不匹配。
- 当用户数量大于时隙数量时，会发生阻塞。



无连接的通信传输

- 传输前把数据分割为不超过限定长度的包，再与源和目的地址一起封装成分组。
- 然后将分组直接提交给传输系统中的交换节点即可。

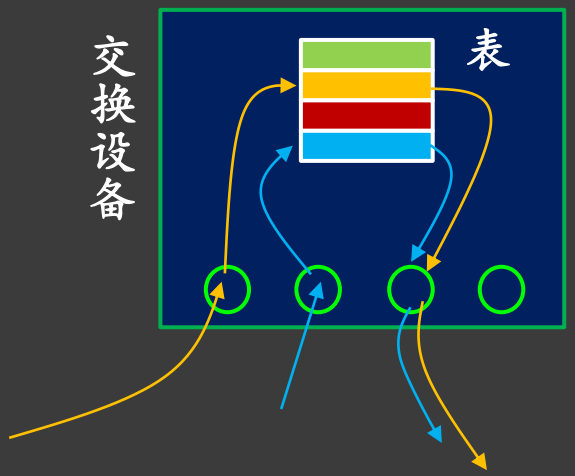
分组交换：

- ✓ 提供无连接传输服务；
- ✓ 链路利用率提高很大；
- ✓ 遇故障自动更换路径；
- ✓ 按传输流量计费。

主要技术特征：

- 存储转发方式中转分组；
- 基于分组的随机资源共享；
- 网络为到达的分组确定当前路径，提供无差错、无丢失、无失序、无重复的传输保障。

路由：选择合适的路径，并沿着路径交换数据的过程。



路由表A

目的	下一跳
A	A
B	D
C	D
D	D
E	B

路由表B

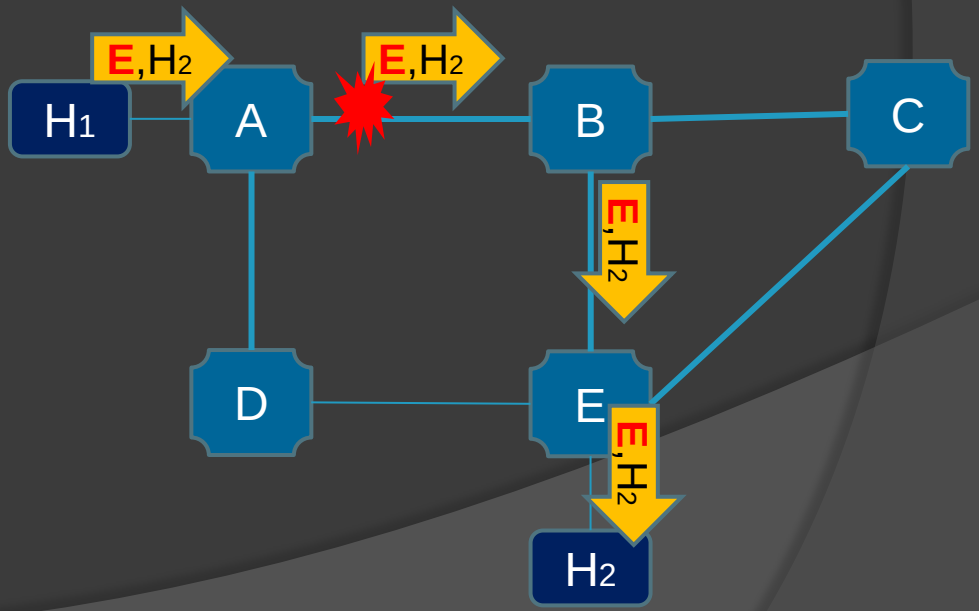
目的	下一跳
B	B
A	E
C	C
D	E
E	E

路由表生成：

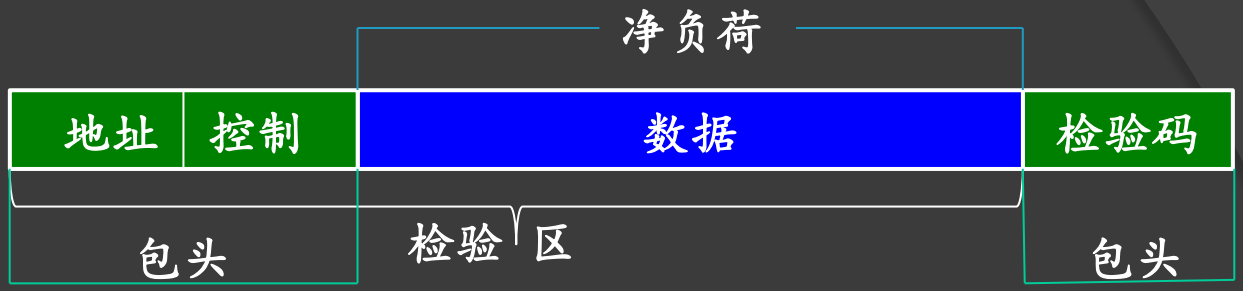
- 静态路由，人工配制。
- 动态路由，程序自动配置。

路由协议：

- 链路检测、信息交互。
- 最优路径计算算法。



分组封装



优点：

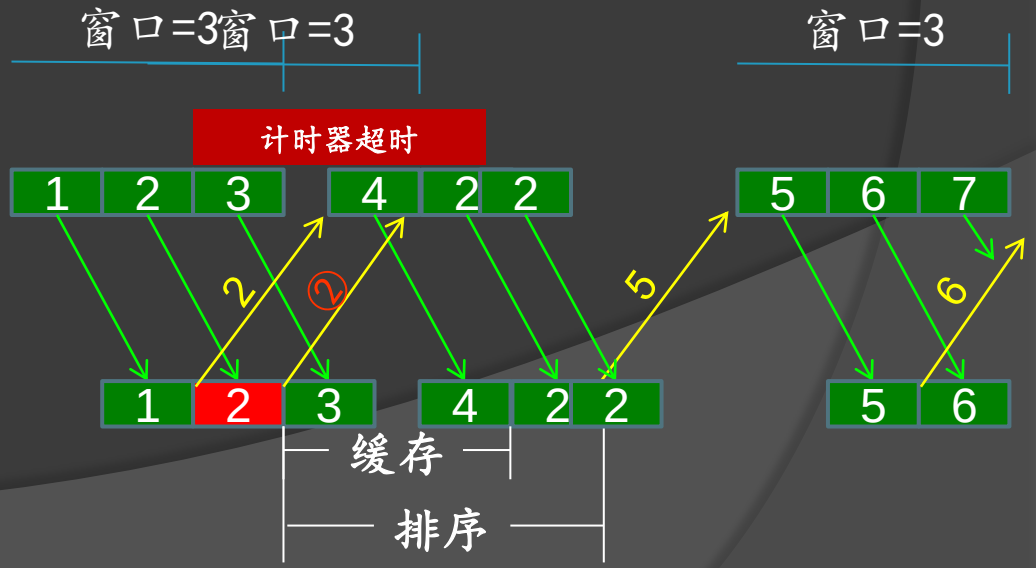
- 对突发性业务的保障好；
- 路由的自组织能力强；
- 容忍较大数量的超量使用；
- 上网成本大大降低。

缺点：

- 对周期性、实时性业务保障差；
- 网络拥塞不可避免；
- 网络流量调控难度大。

交换网络的差错与流量控制：

- 重传纠错；
- 接收方控制发送速率；
- 逐“跳”实施，提供全网络的传输保证。



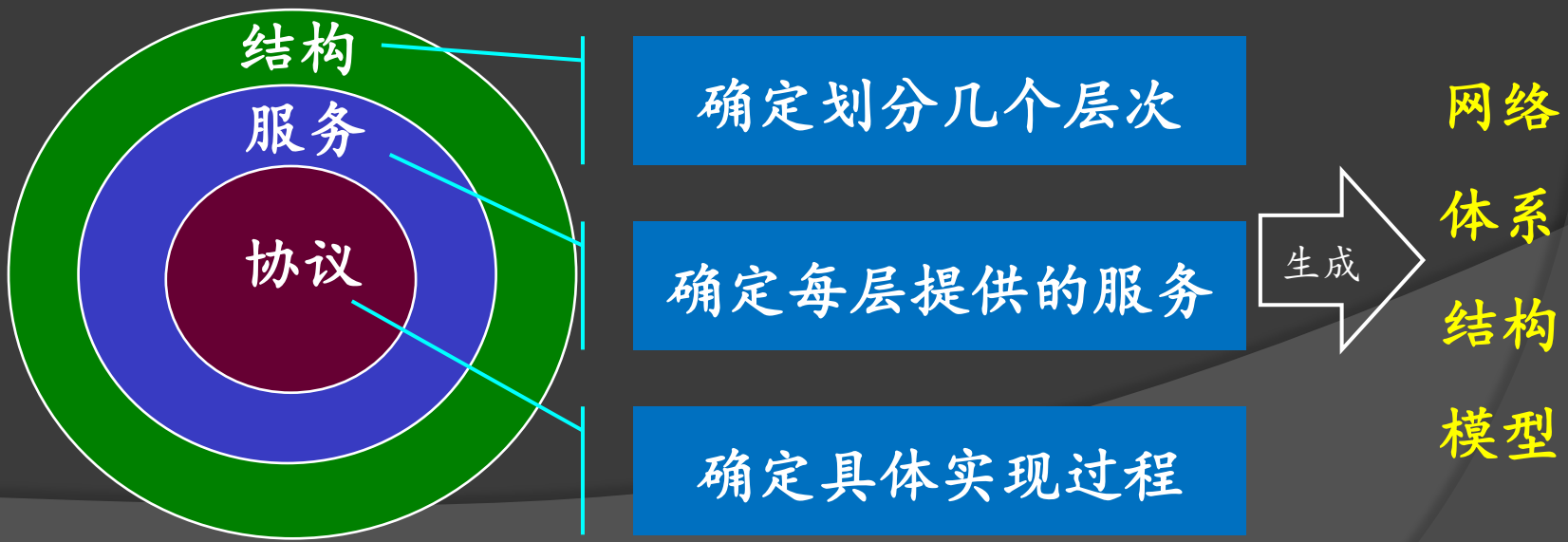
2.3 TCP/IP模型

2.3.1 网络体系结构模型

体系结构：对一个系统中基本元素、元素之间相互作用关系、实现方式等内容的描述和约定。

网络体系结构：指为实现网络通信，网络设备所实现通信功能的逻辑分布结构，以及必须遵守的相关通信协议。

网络体系结构设计：一般采用自顶向下，逐步求精的过程。



1、开放系统互连参考模型

(Open System Interconnect,OSI)

应用层：　应用调用接口。

表示层：　数据格式转换。

会话层：　通信双方交互。

（信息处理 → 终端功能）

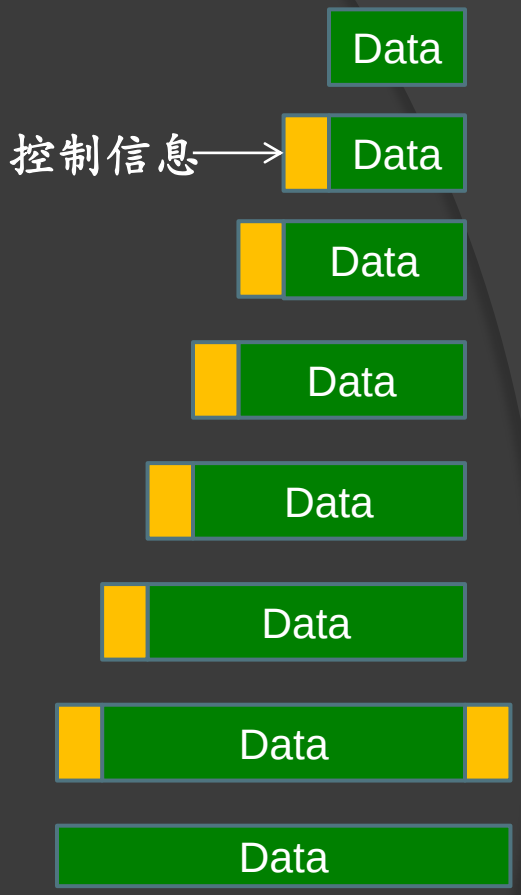
传输层：　端到端可靠传输。

网络层：　路由及拥塞控制。

数据链路层：点到点可靠传输。

物理层：　与物理介质连接。

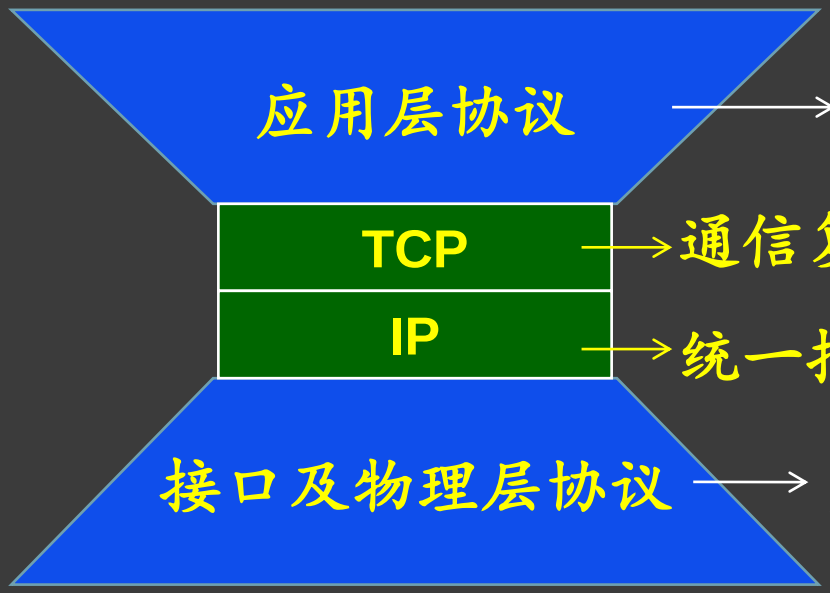
（通信传输 → 网络功能）



发送方从上往下层层封装；接收方从下往上层层拆封。

TCP/IP是实际的计算机网络模型，与OSI模型并不一一对应，采用简单网络/智能终端的设计思想以及开放式体系结构。

2、TCP/IP沙漏结构



开放性好；

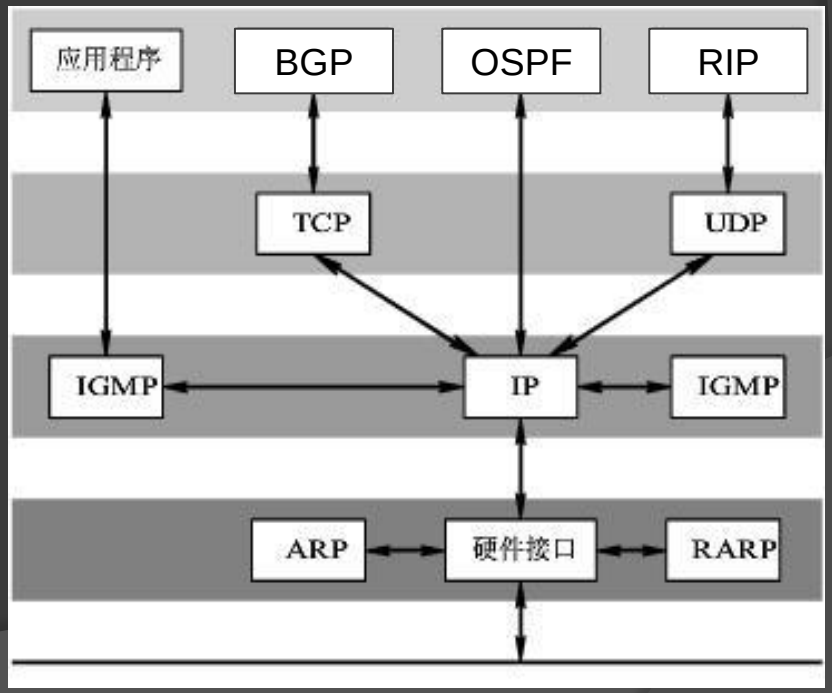
自组织能力强；

网络互联方便、灵活；

应用程序众多、发展迅速；

网络交换设备的控制能力弱，

后期完善任务艰巨。



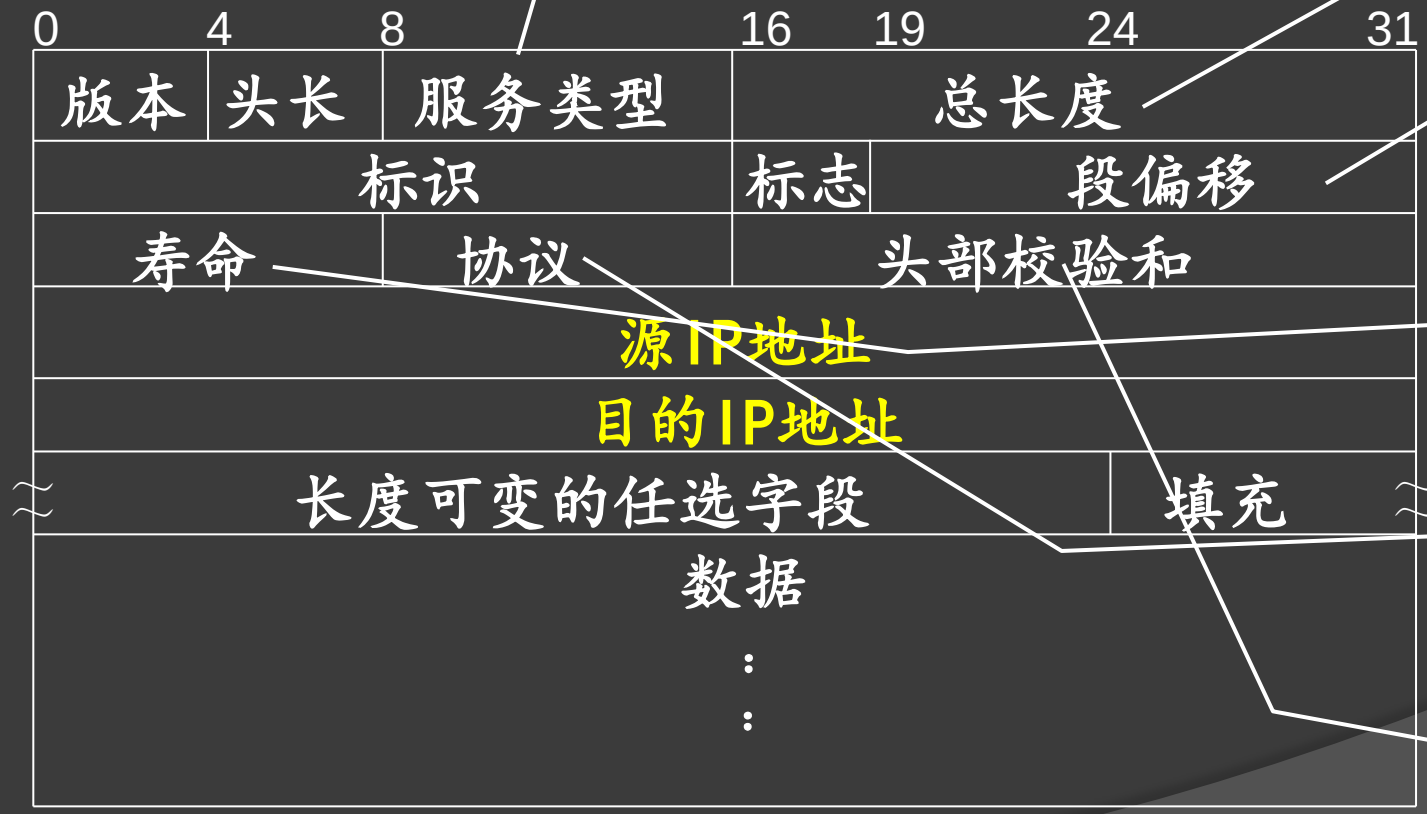
2.3.2 网际互连协议（Internet Protocol）

IP是提供“智能化”边缘（终端）设备之间通信的最小功能集，运行在所有Internet终端和交换设备之上。

1、限长报文格式

分组可划分为4个类8个等级

报文最大64Kbytes



用于报文的分片与重组

用于清除垃圾分组

指明分组归谁所有

保证头部信息正确

无差错控制；无流量控制；仅提供尽力而为的服务。

2、IP地址及寻址

层次化地址编码

网络号net_id + 主机号host_id

IP子网地址	设备地址
由IANA负责分配	由各运营单位自行分配

点十进制标记

11001010 . 01110010 . 01000000 . 00000010

202 . 114 . 64 . 2

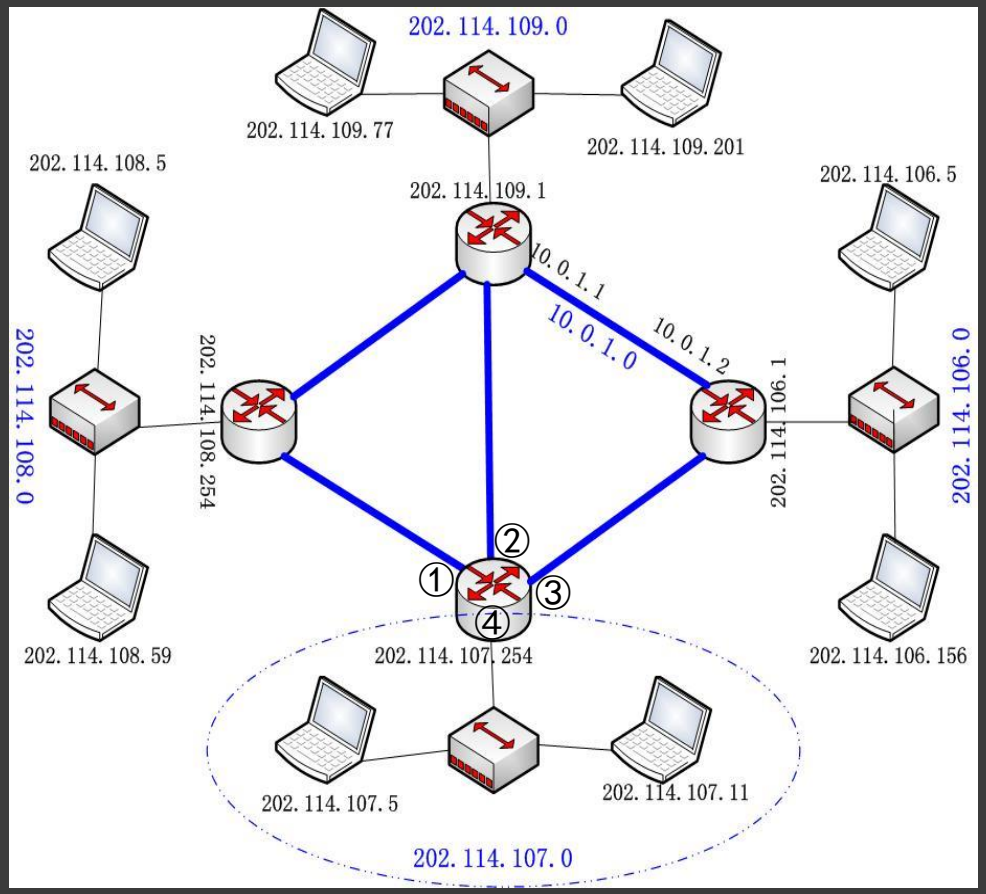
IP地址分类管理

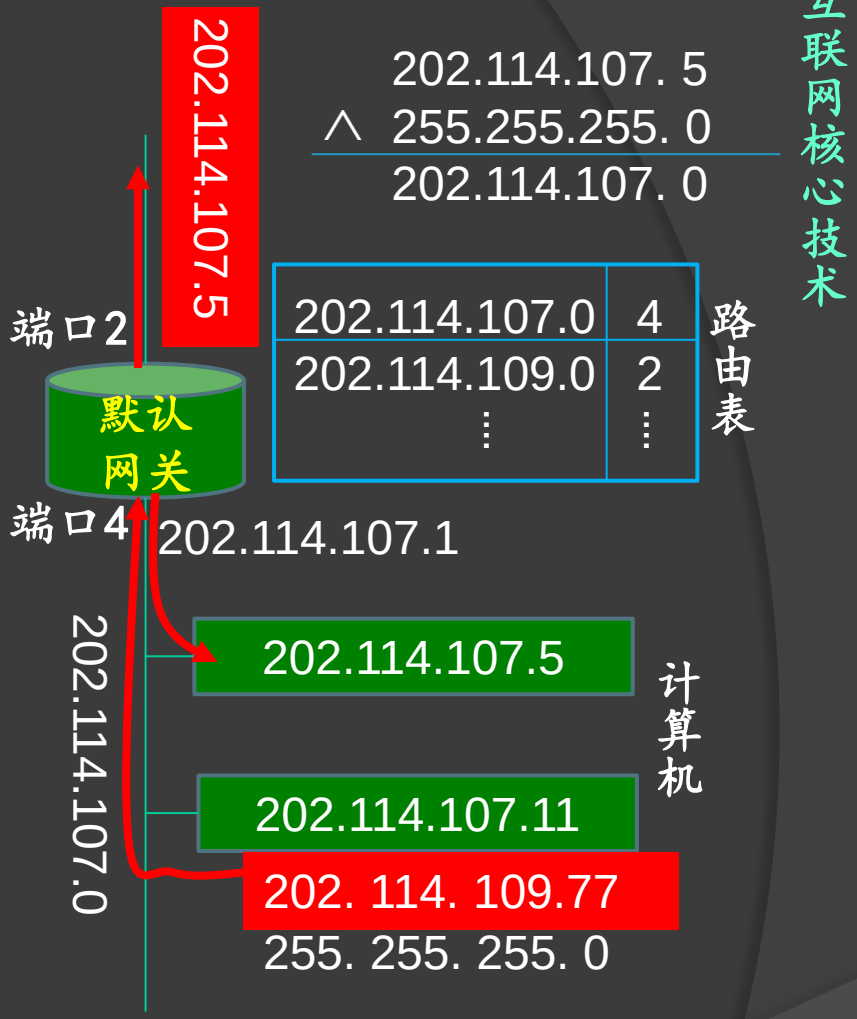
	31	24	16	8	0	
A类	0	net_id	host _id			0.0.0.0~127.255.255.255
B类	10	net_id	host_id			128.0.0.0~191.255.255.255
C类	110	net_id	host_id			192.0.0.0~223.255.255.255
D类	1110	group_id				224.0.0.0~239.255.255.255
E类	11110	实验用				240.0.0.0~255.255.255.255

主机号全0为子网地址；主机号全1为子网内全体设备接收。

10. 0. 0. 0~10. 255. 255. 255、100. 64. 0. 0~100. 127. 255. 255

172. 16. 0. 0~172. 31. 255. 255、192. 168. 0. 0~192. 168. 255. 255





IP寻址

子网内寻址：找到具体设备。　　子网掩码用于提取子网地址，

子网外寻址：找到网关中转端口。判断进行何种IP寻址转发。

A类：255.0.0.0 ；B类：255255.0.0；C类：255.255.255.0。

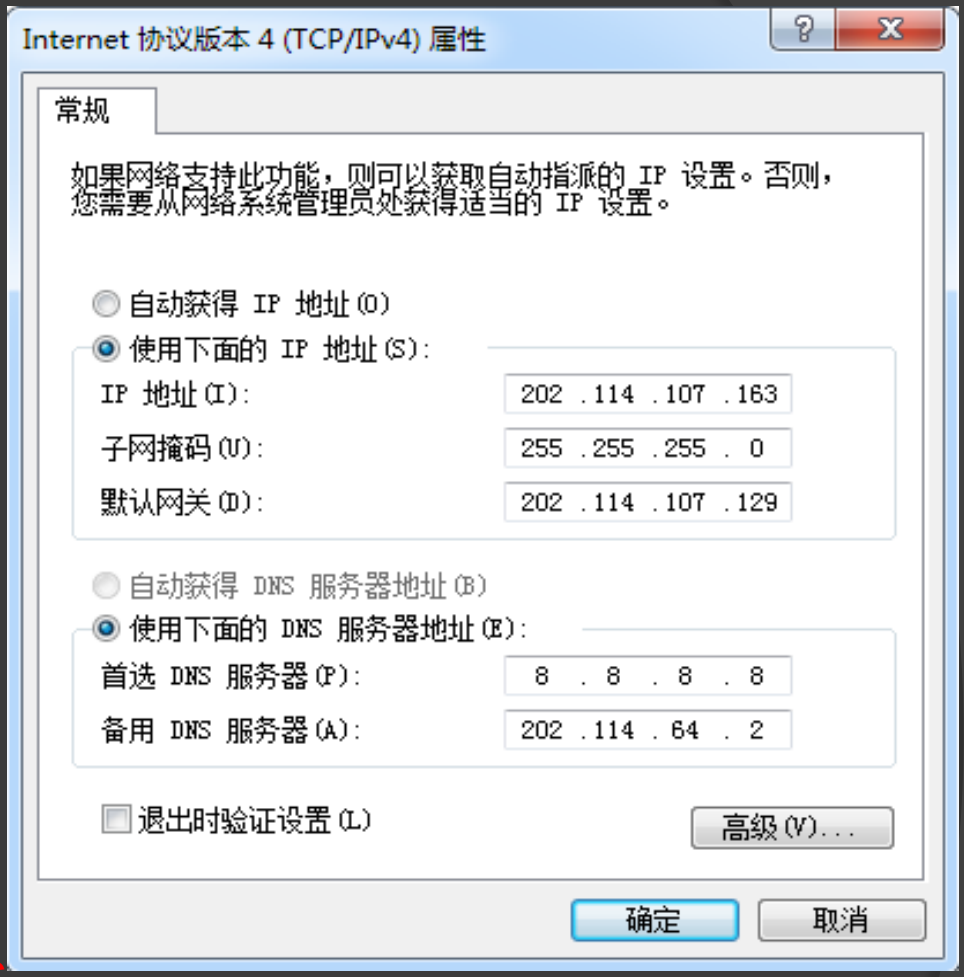
计算机将所有与自己IP子网地址不匹配的数据包都直接转交给**默认网关**。

域名解析系统——**DNS服务器**将互联网上某个设备的文字缩写地址解析为与之对应的IP地址。例如，

dns.whu.edu.cn

⇩

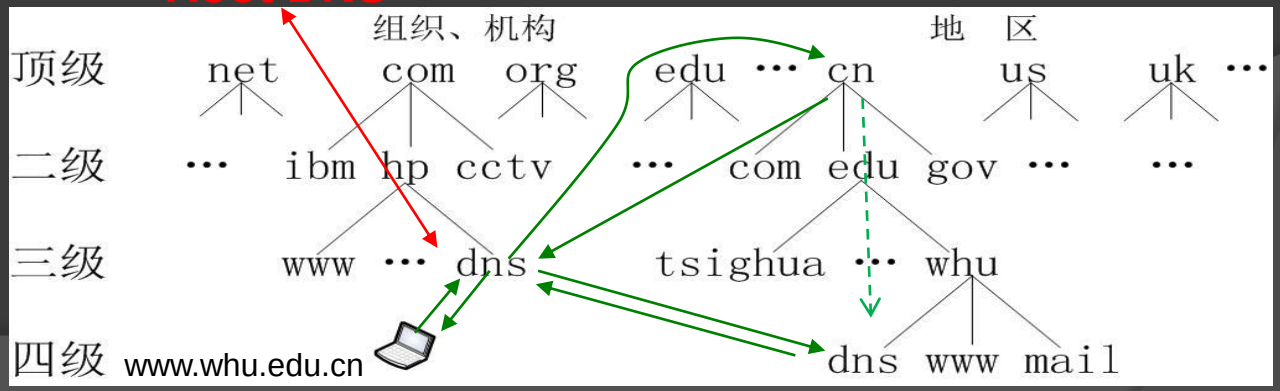
202.114.64.2



域名结构：

解析过程：

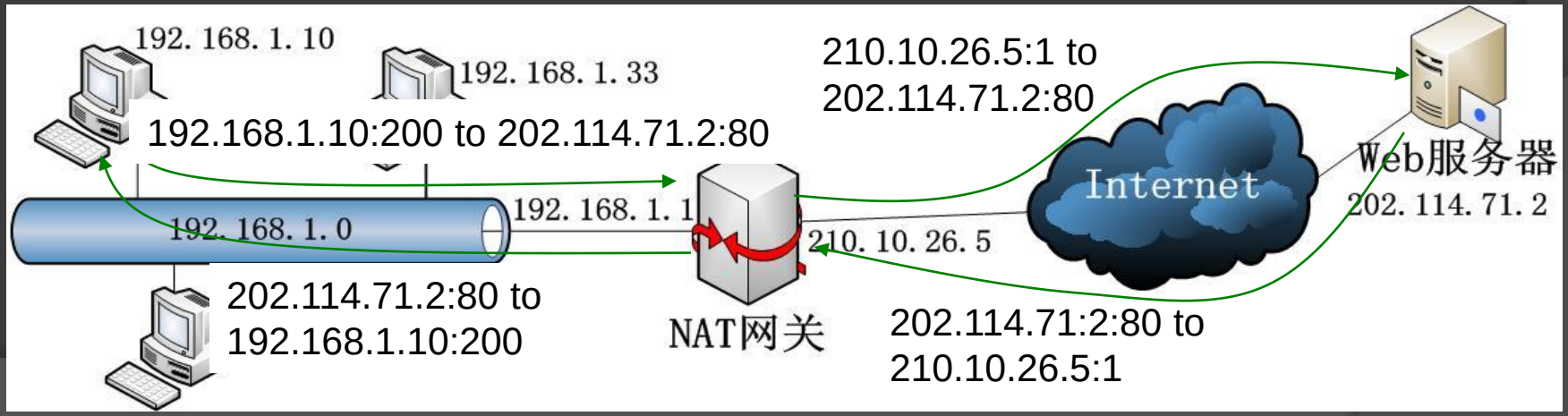
从根DNS开始逐层解析。



IP地址危机问题：IPv4地址总数约42亿多个，除去约定和保留的地址，实际可用的为25.68亿个，远小于需求数量。

动态主机配置协议——DHCP：基于该协议，DHCP服务器为子网内临时登录的主机分配IP地址、网关地址、DNS服务器地址。服务器监测到主机推出后，收回这些地址资源，再将资源提供给其他新登陆的主机使用。

网络地址转换——NAT网关：子网内部使用保留地址，子网外部使用一个联系地址，由NAT网关实现内外地址转换。



可变长子网掩码

	原网络地址		原主机地址
IP地址	net_id	subnet_id	host_id
子网掩码	1 1 1 … … … 1 1		0 0 … 0 0

示例，B类地址129.128.0.0 被12个临近的单位共用。

10000001 10000000 **** **** ********

net_id subnet_id host_id

子网号 主机号

0 0 0 0 0 0 0 0 0 0 0 0 0 0 0 1

1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 0

子网掩码 11111111 11111111 1 1 1 1 0 0 0 0 0 0 0 0 0 0 0 0

子网掩码 255 . 255 . 240 . 0

3、IPv6

基本首部	扩展首部1	---	扩展首部n	数据

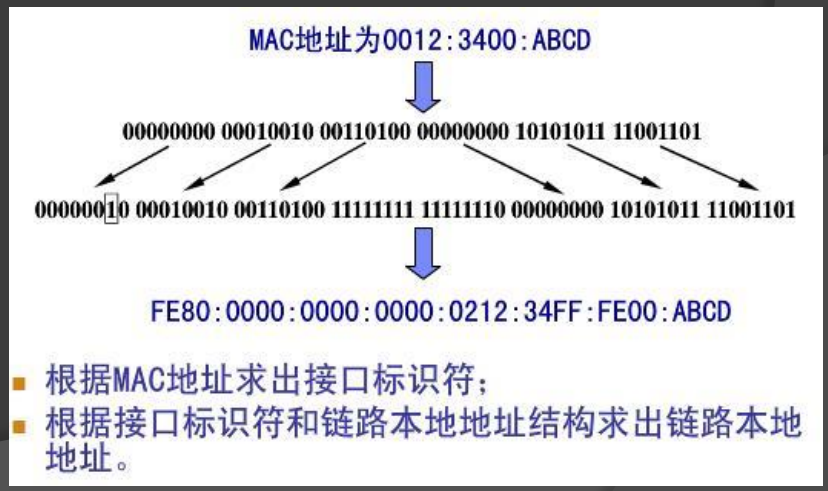
0	4	8	16	31
版本	优先级	流标号		
净负荷长度		下一个首部	跳数限制	
源站IP地址（16字节）				
目的站IP地址（16字节）				

单播地址
- 全局单播地址
- 本地链路地址
- 本地网点地址

组播地址

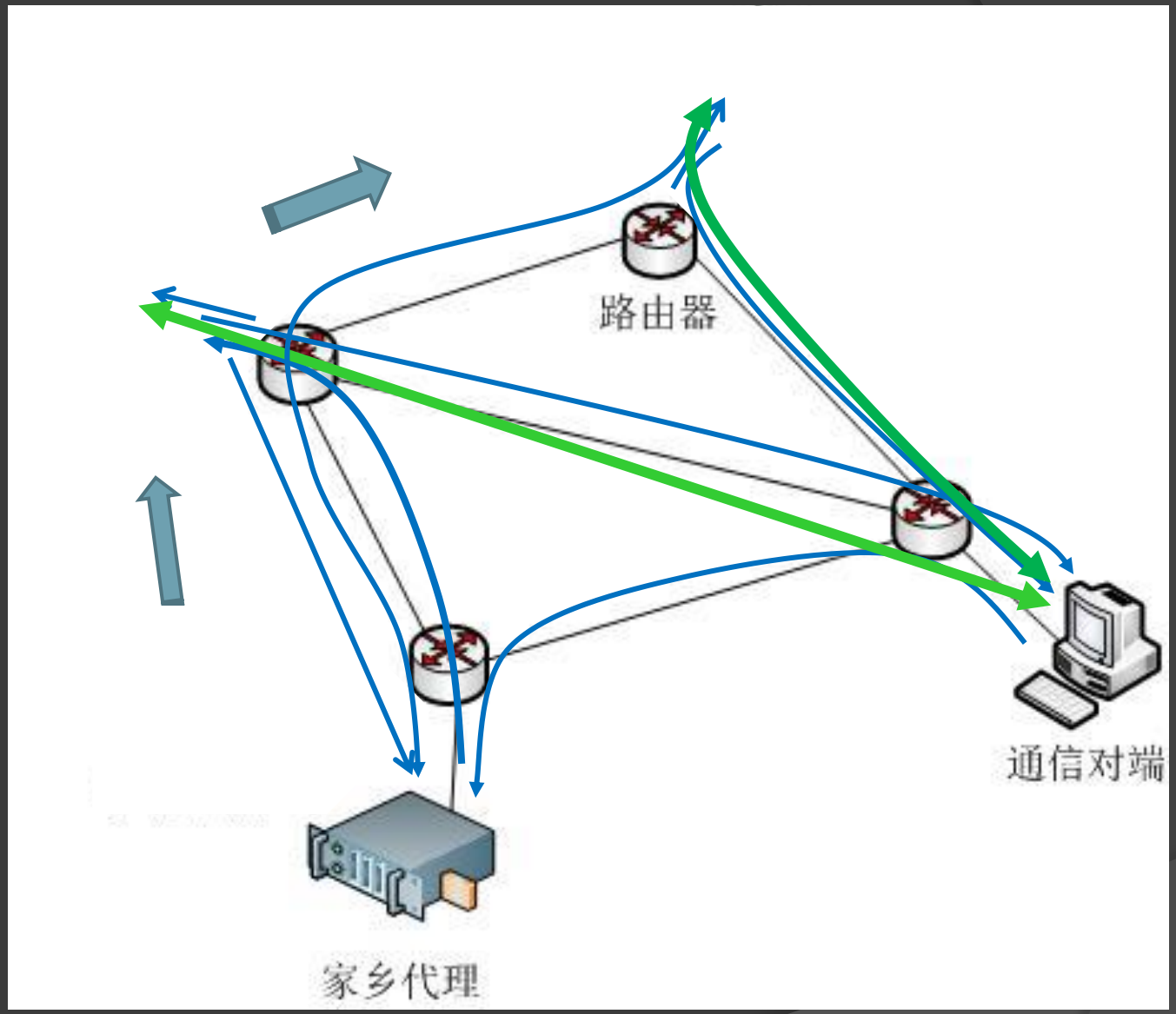
选播地址

IPv6自动实现与MAC地址的绑定。



移动IP

- ✓路由通告；
- ✓转交地址配置；
- ✓家乡注册；
- ✓家乡路由；
- ✓隧道转发；
- ✓对端注册；
- ✓直通路由。



移动节点到达新的网段时，通过注册获取自己的本地链路地址以及该网段默认网关、DNS的地址，从而保证自身在新的网段内的正常通信。

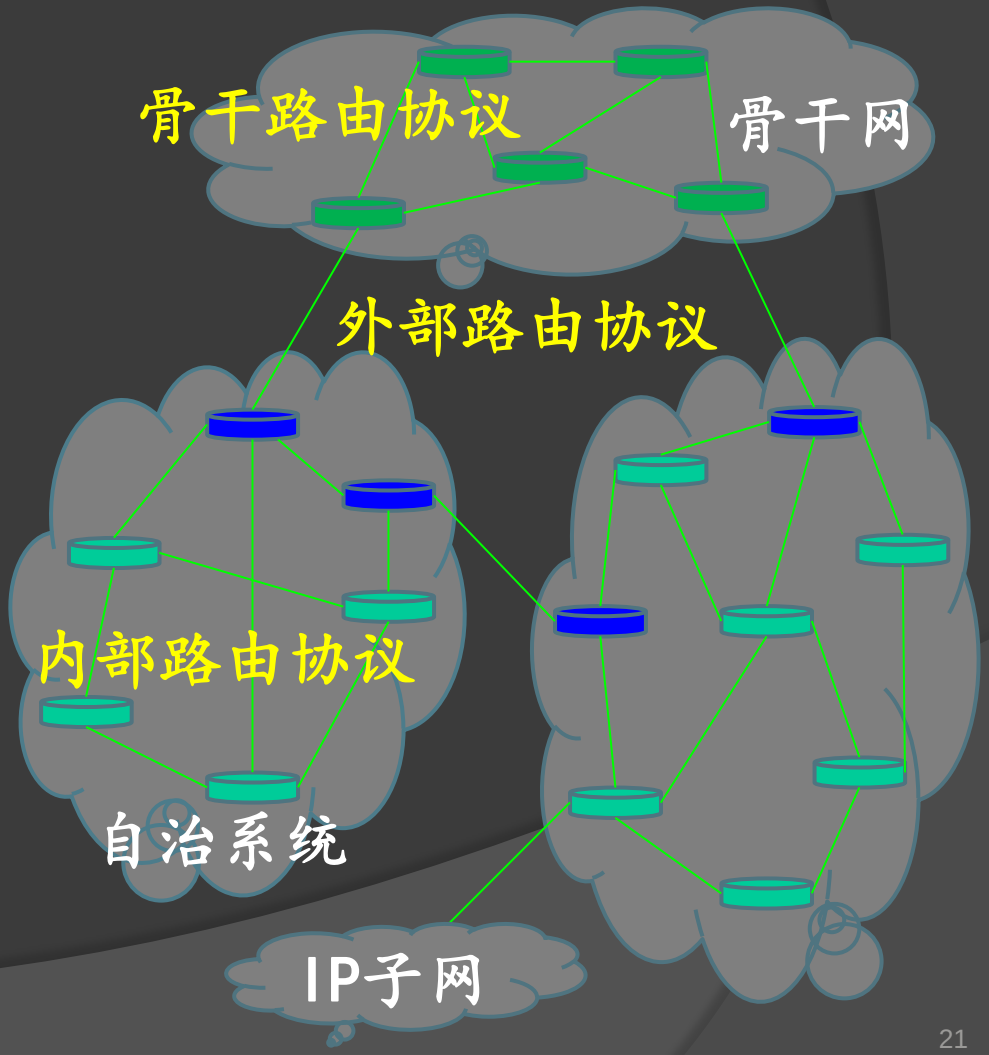
2.3.3 “简单”网络不简单

简单IP的连接性要求：只要存在任何可能的通路，数据分组就能在一段合理的时间内从源端传输到目的端。这也被称为Internet的**自组织特性**。

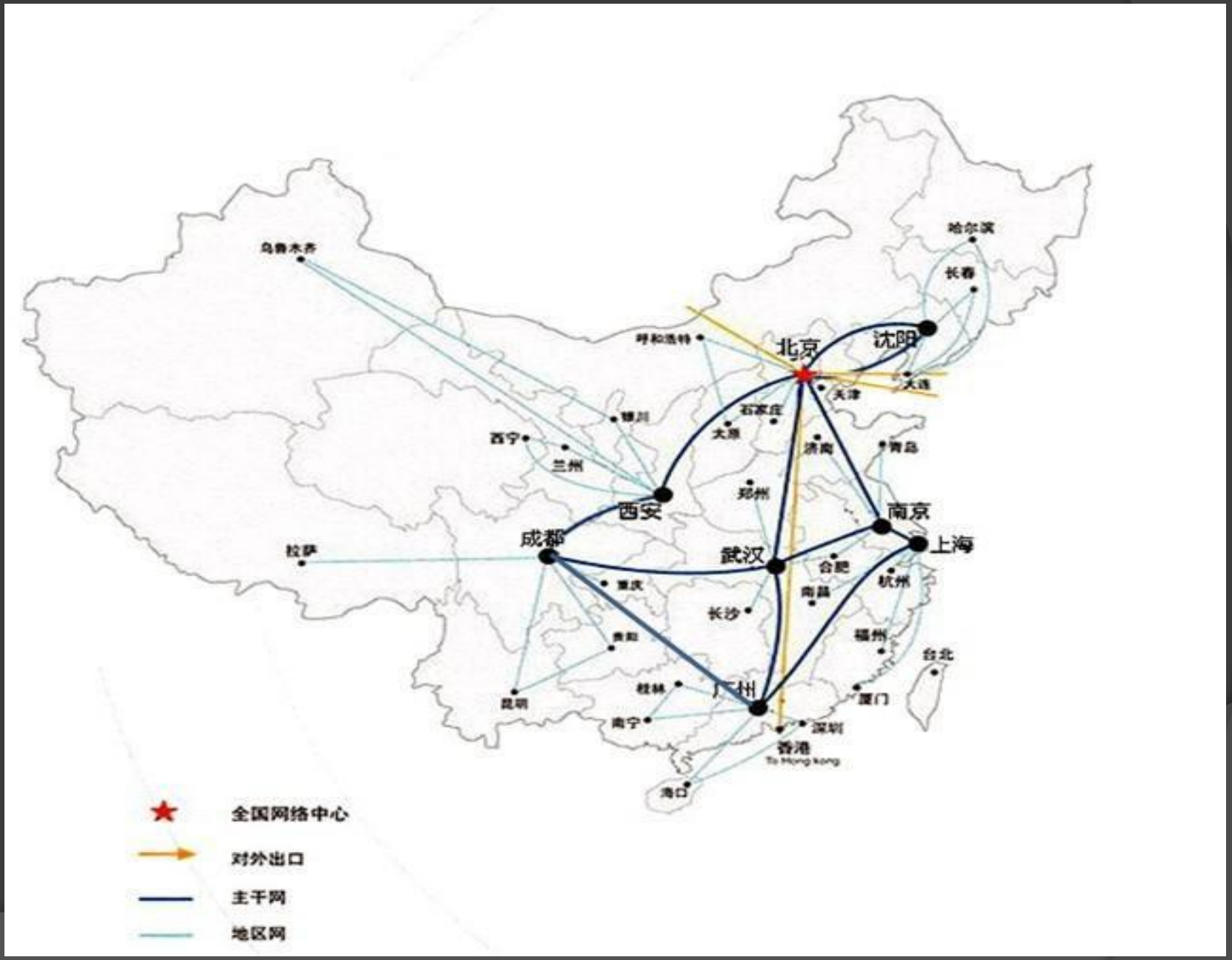
Internet采用平面“云图”结构，路由节点之间无等级之分，且可根据需要互联。

由于云太大，整个网络按照管理范围划分不同区域，并且运行不同的路由协议。

目前，Internet上路由器/网关超过十多万台。



中国电信的CHINANET



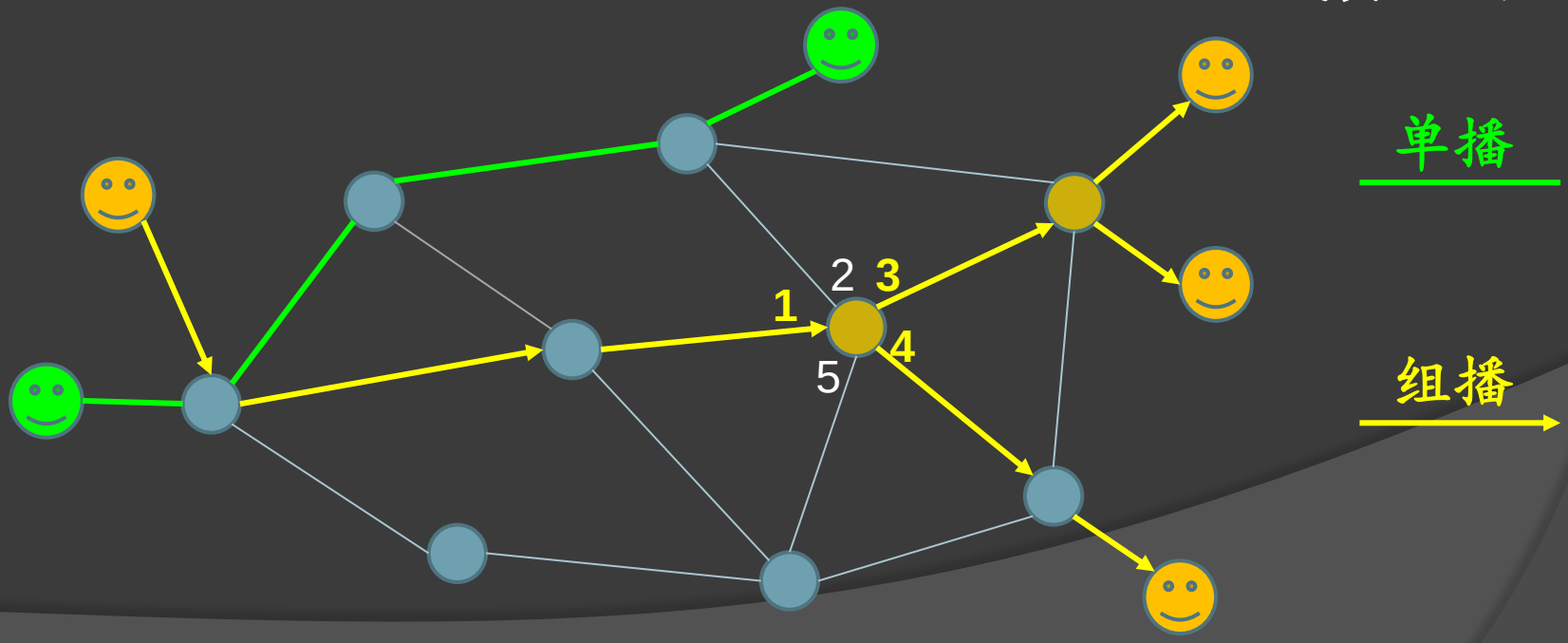
实现自组织功能的关键是IP路由协议，其主要任务：

- 发现网络中链路的连通状态；
- 计算源节点到目的节点的最佳路径；
- 自动更新和维护路由转发表。

单播路由：一对一传输的路径选择及转发。

组播路由：一对多传输的路径选择及转发。

组播路由表记录了连接组播源的端口和连接组成员的端口。

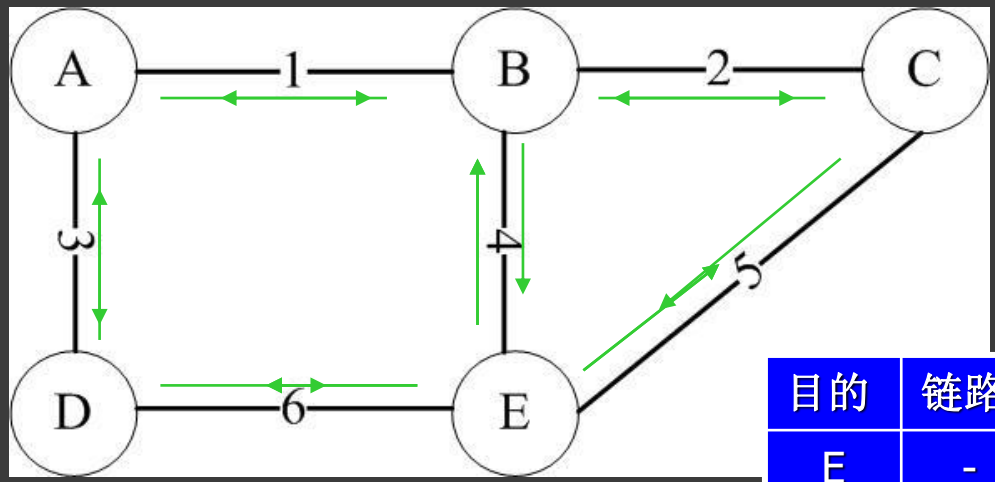


路由器周期性地与邻居路由器联络和交换路由表信息，实现网络路由功能的自组织特性。

目的	链路	跳数
A	-	0
B	1	1
C	1	2
D	3	1
E	3	2

目的	链路	跳数
B	-	0
A	1	1
C	2	1
E	4	1
D	4	2

目的	链路	跳数
C	-	0
B	2	1
A	2	2
E	5	1
D	5	2



目的	链路	跳数
D	-	0
A	3	1
E	6	1
B	6	2
C	6	2

目的	链路	跳数
E	-	0
C	5	1
B	4	1
A	4	2
D	6	1

2.3.4 传输控制协议(Transmission Control Protocol,TCP)

TCP层提供简单化和复杂化两类“衔接”服务，工作在所有互联网终端设备上。

- 用户数据报协议(User Datagram Protocol，UDP)，仅提供无连接服务的调用接口和无差错的端到端传输服务，适合报文短且可靠性要求低的通信传输。

- 传输控制协议TCP，提供有连接服务的调用接口和可靠的端到端传输服务，同时，支持网络拥塞控制管理。但是，不适合有实时性要求的通信传输。

➢ UDP和TCP都无法满足高实时性网络传输的通信要求。

TCP报文格式

源端口								目的端口
发送数据序号								
接收数据序号								
数据偏移	保留	URG	ACK	PSH	RST	SYN	FIN	通知窗口
检验和								紧急指针
选项和填充								
数据段								

IP地址指明计算机，端口号指明应用程序，提供通信复用。

熟知端口号：Web服务—80；电子邮件—25；FTP—21。

紧急标志与紧急指针配合使用，指明报文中携带有紧急数据以及紧急数据在报文中的起始位置。

指明报文为确认消息，通告：在同时双向的传输中，本方发送数据的起始编号；希望对方发来数据的起始编号；本方准备接收数据的数量。Ack也用于连接的建立和撤销过程。

TCP报文格式

源端口								目的端口
发送数据序号								
接收数据序号								
数据偏移	保留	URG	ACK	PSH	RST	SYN	FIN	通知窗口
检验和								紧急指针
选项和填充								
数据段								

Syn与Ack配合使用，采用“请求—应答—确认”的三次握手连接建立机制，确保发送程序和接收程序都做好准备。

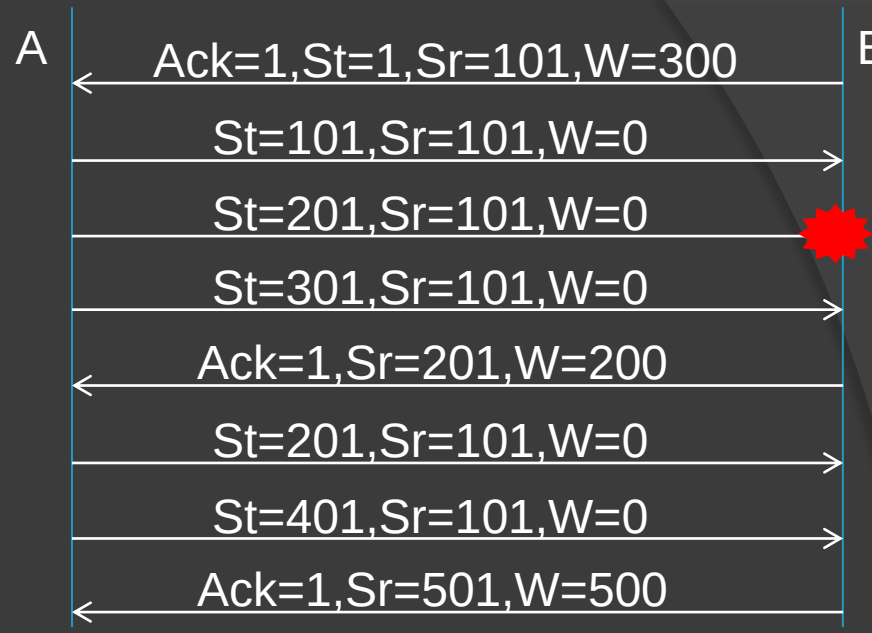
Fin与Ack配合使用，采用“通知—确认”的方式指明本方的数据发送结束。只有双方都数据发送结束后，才释放连接。

在连接建立时，用于双方协商每次传输报文的大小。

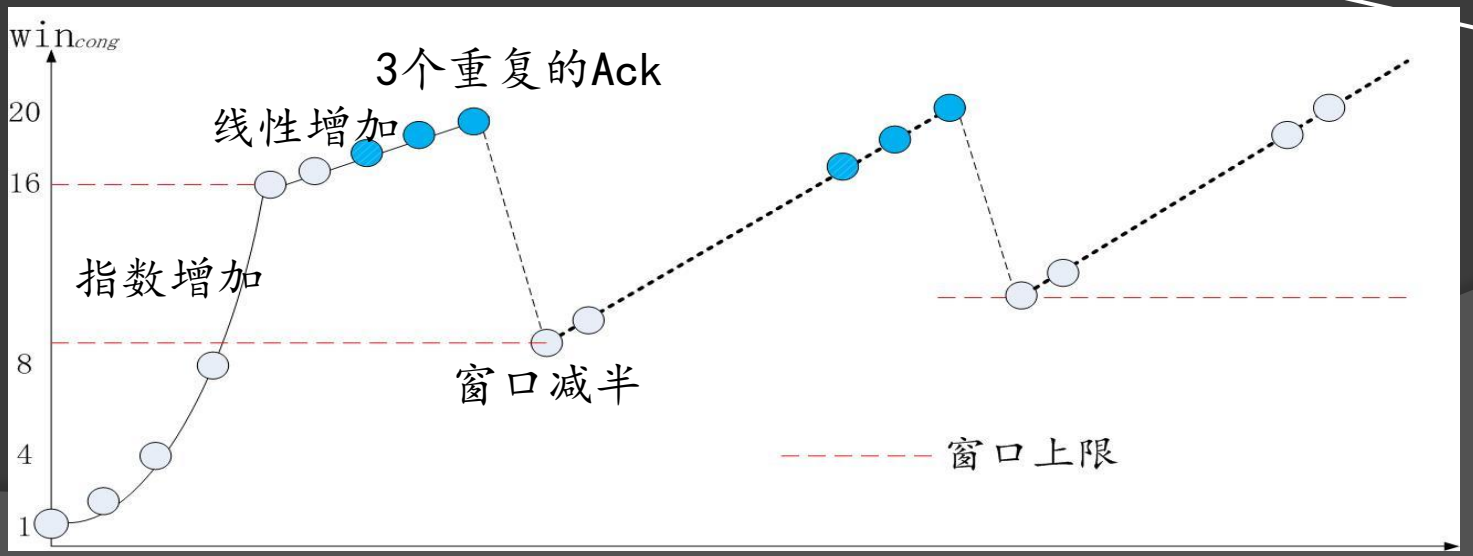
对所有报文数据进行错误检验。

端系统的差错与流量控制

- 采用自动重传请求机制，基于Ack，重传出错和丢失报文，调节发送速率。
- TCP测量平均往返时间，以此来评估是否发生网络拥塞。
- 发送窗口$win = min\{win_{cong}, win_{ack}\}$。



网络拥塞状态，由发送方调节。



接收缓存状态，由接收方调节。

2.3.5 TCP/IP改进措施

问题：1）网络流量波动大，链路利用率降低。

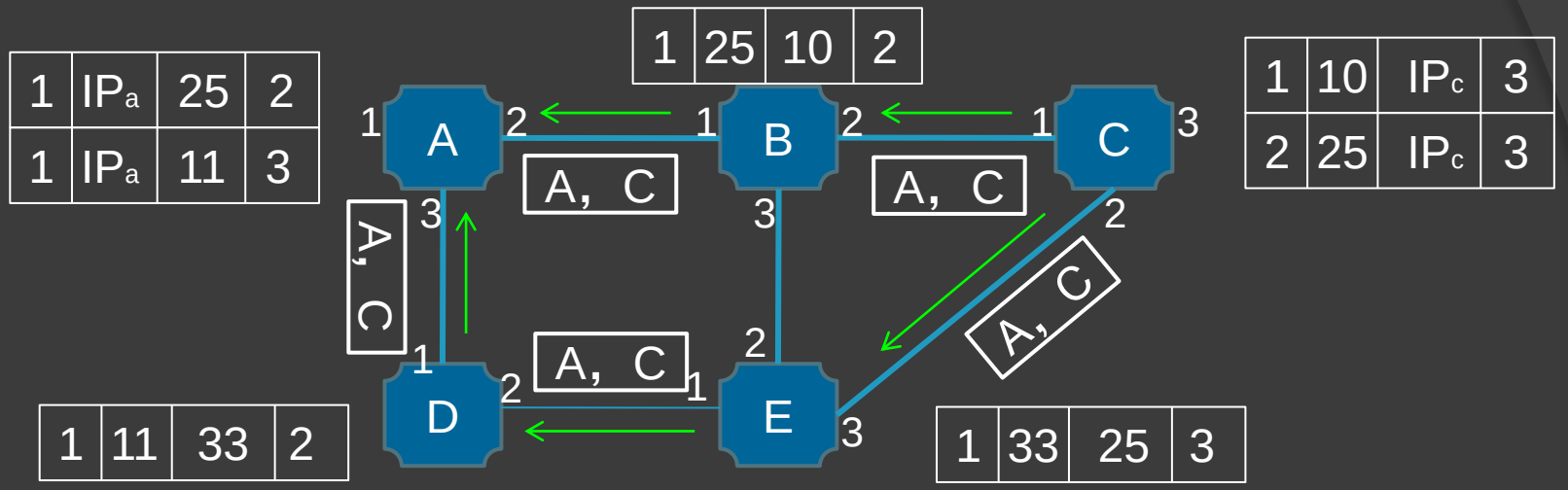
2）UDP报文会抢占TCP报文的资源。

3）简单的“先到先服务”策略反而造成不公平。

原因：网络中间结点的功能过于简单，仅依靠端系统的调控和保障，提供的服务能力十分有限。

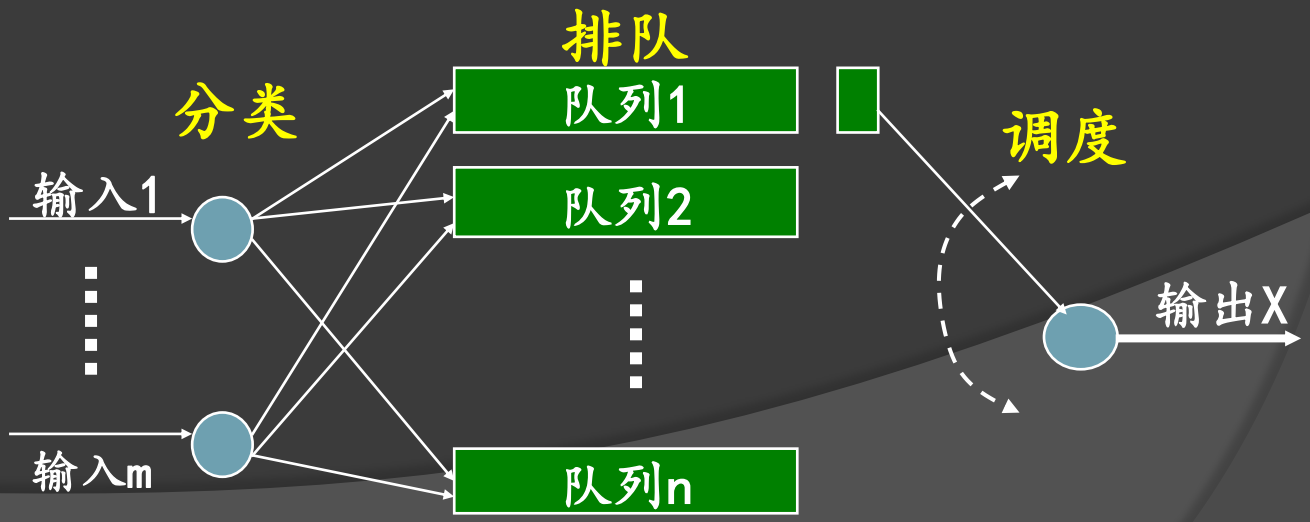
- ✓ 基于多路径路由和流量保护技术，开展流量工程，实现网络流量分布负载均衡，尽量避免拥塞发生，快速恢复故障以及缓解拥塞，最大限度地降低流量波动。
- ✓ 增加每一跳的分类、排队、调度控制，基于每一跳的服务质量保证(QoS)和QoS路由技术，实现端到端网络通信的传输路径的QoS保证。

✓ 面向连接的“虚电路”交换路径，可以提供端到端或边缘到边缘的路径保护、流量分流、QoS保证等服务。



✓ 每一跳的分类Classing、排队Queuing、调度Scheduling。

CQS结构：



2.4 网络应用

2.4.1 应用层技术

各种网络应用系统，在逻辑关系上将人和数据信息重新聚合成了基于物理网络设施的一个个新网络系统，也称网络社团。这些网络之上的网络，在组织方式、连接结构等方面与基础设施网络并无直接对应关系。

主要的应用系统

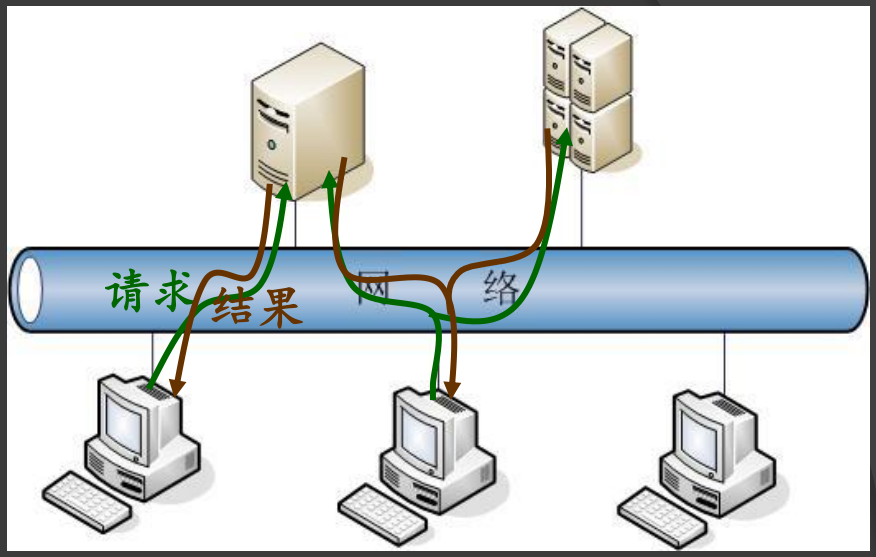
- 文件传输；
- 电子邮件；
- 万维网；
- 即时通信；
- 网络直播。

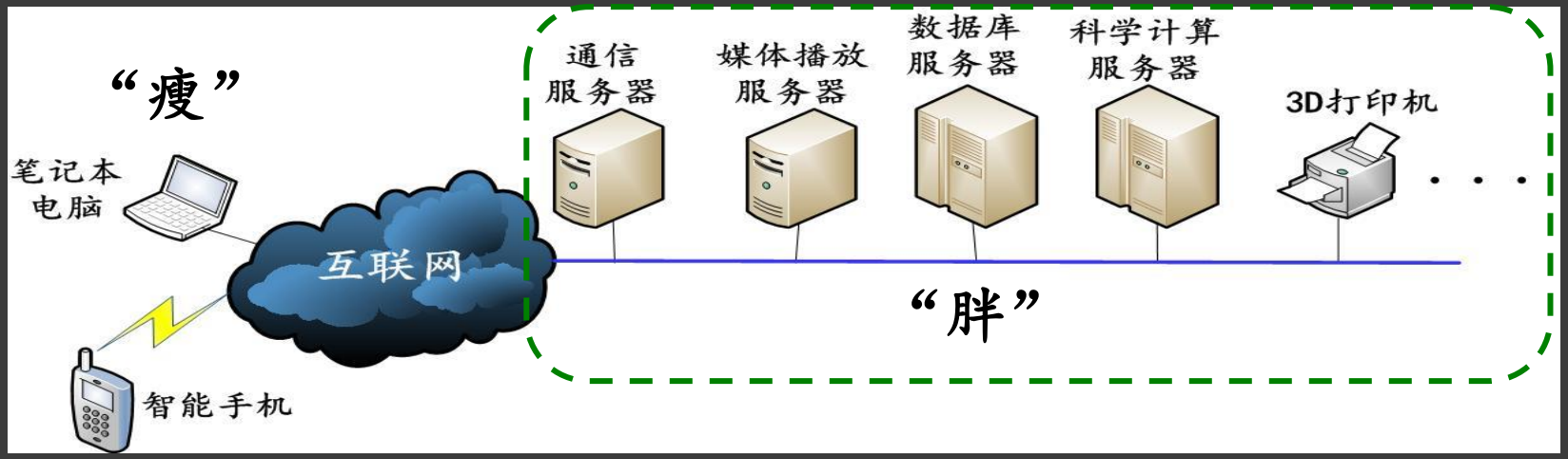
✓ 客户/服务器模式：软件功能划分为人机交互与网络计算两部分，分别运行在不同处理能力的计算机上。

✓ 点对点模式：人机交互与网络计算都运行在同一台计算机上，允许灵活地加入和撤出应用系统。

1、Client/Server

- 在网络中只传输“请求”和“响应”消息。
- 功能升级、更新需要在客户和服务器两端进行。





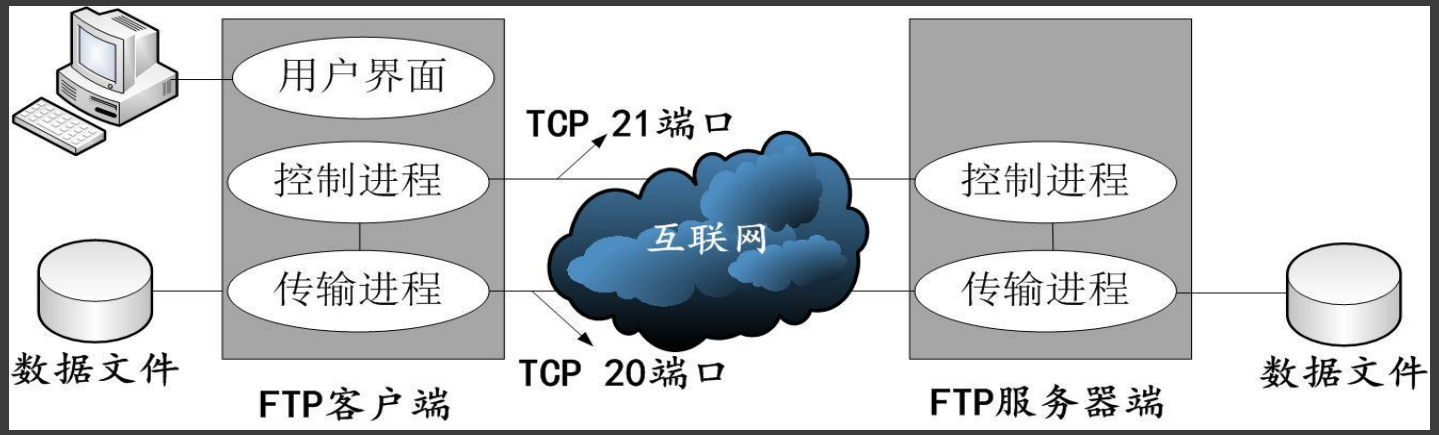
用户无需投资服务器端硬件与软件设施的建设。

✓ 基础设施租赁；
✓ 开发平台租赁；
✓ 应用系统租赁。

- 虚拟化技术；
- 分布式资源管理技术；
- 并行编程技术。

2、文件传输协议（File Transfer Protocol，FTP）

FTP屏蔽了计算机系统之间的差异，可以基于互联网在任意的两台计算机之间进行共享文件的“透明”存取。



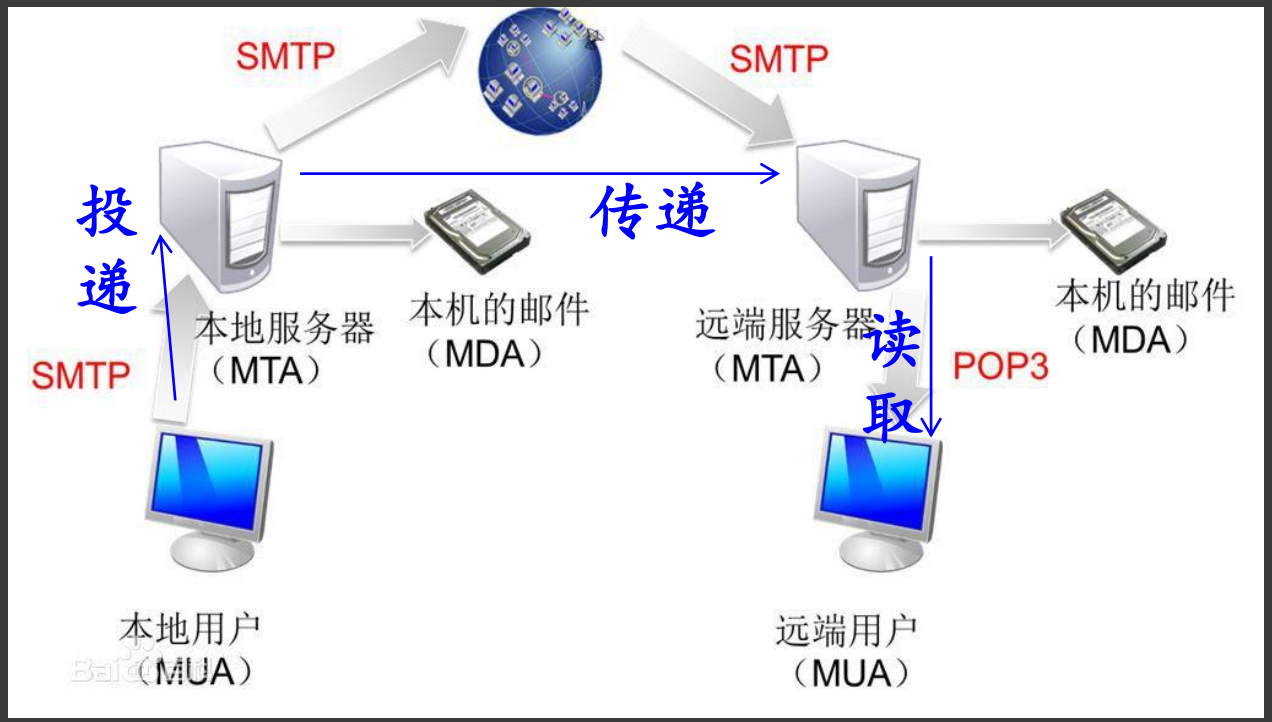
ftp://用户名:密码@FTP服务器IP或域名:FTP命令端口/路径/文件名

基于FTP的断点续传

下载：
1）告知已下载文件长度；
2）告知下载的文件名；
3）建立数据连接；
4）继续传输数据。

上载：
1）获取被中断的文件长度；
2）告知上载的文件名；
3）建立数据连接；
4）继续传输数据。

3、简单邮件传输协议/邮局协议——SMTP/POP3



SMTP负责投递邮件，以及在两个邮箱之间传递邮件。

POP3负责从邮箱读取邮件。

SMTP和POP3都采用C/S结构且基于TCP实现端到端的邮件传输。

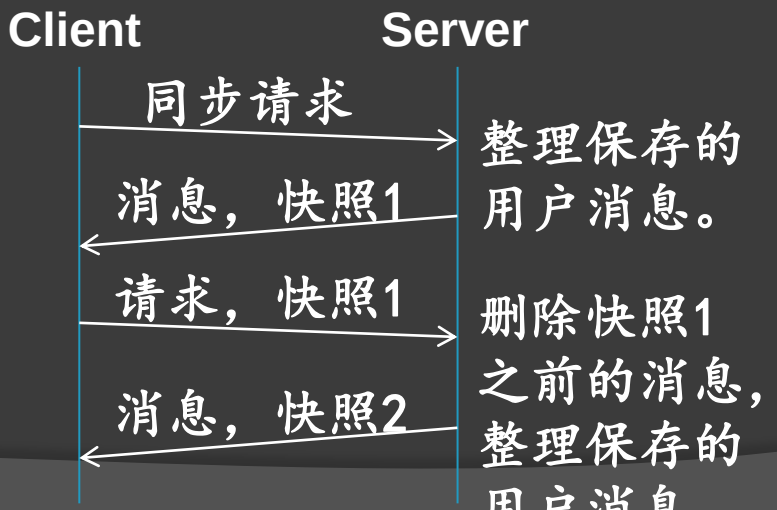
IMAP：用户通过浏览邮件头部后再决定是否收取或删除邮件，允许多个用户同时访问邮箱，支持访问消息中的MIME部分。

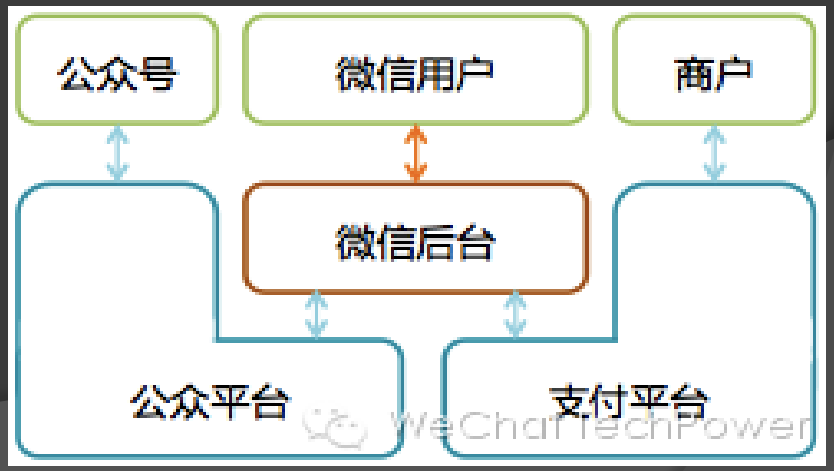
MIME：为文件设定某种扩展名，当该扩展名文件被访问的时候，浏览器会自动使用指定程序来打开文件的标准。

4、即时通信（Instant Messaging）

即时通信是基于C/S结构的消息传递工具，允许两人或多人通过网络即时地传递消息、文件、语音与视频交流。相比实时的电话交流，IM不需要联系人时刻在线；相比非实时的E-mail交流，IM消息传递更迅速，更接近电话交流。

类似E-Mail信息传递模型，但只有一个集中式管理的消息转发服务器。

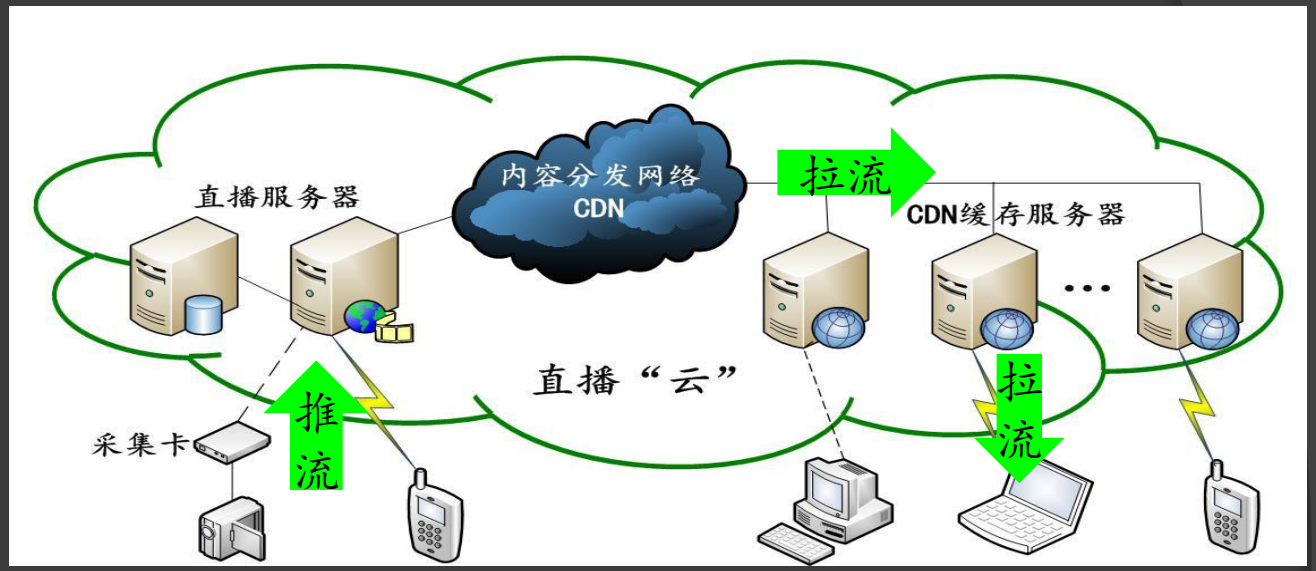


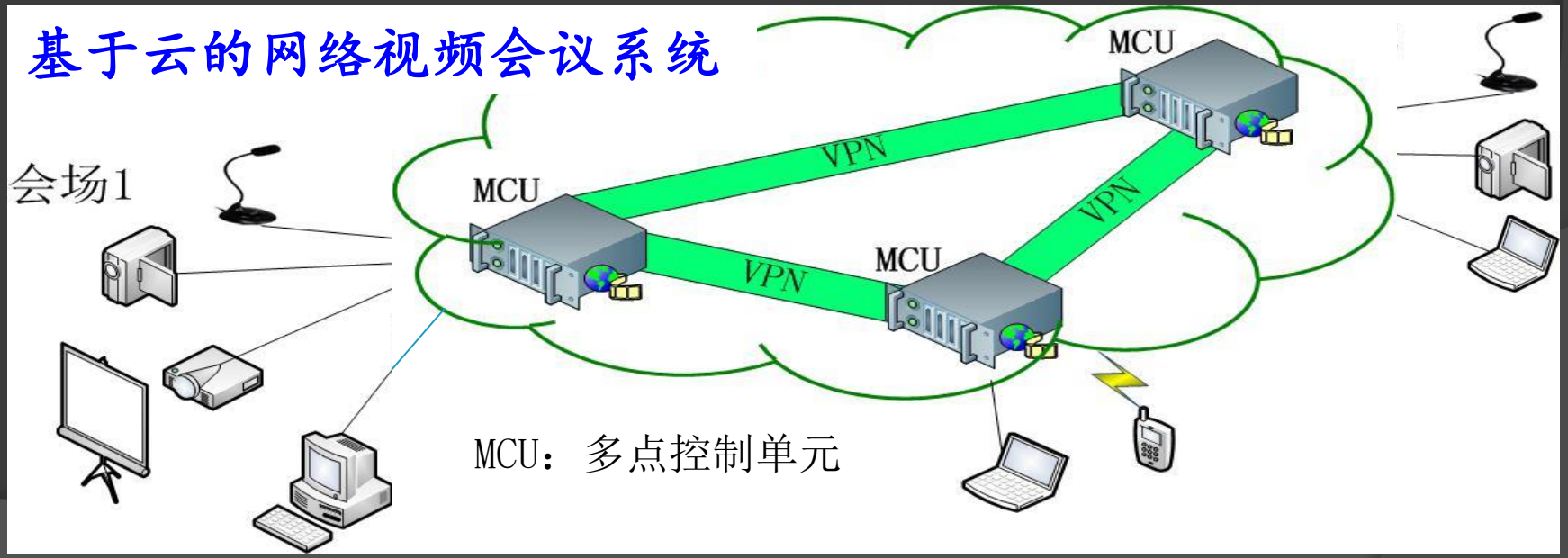


5、网络直播互动

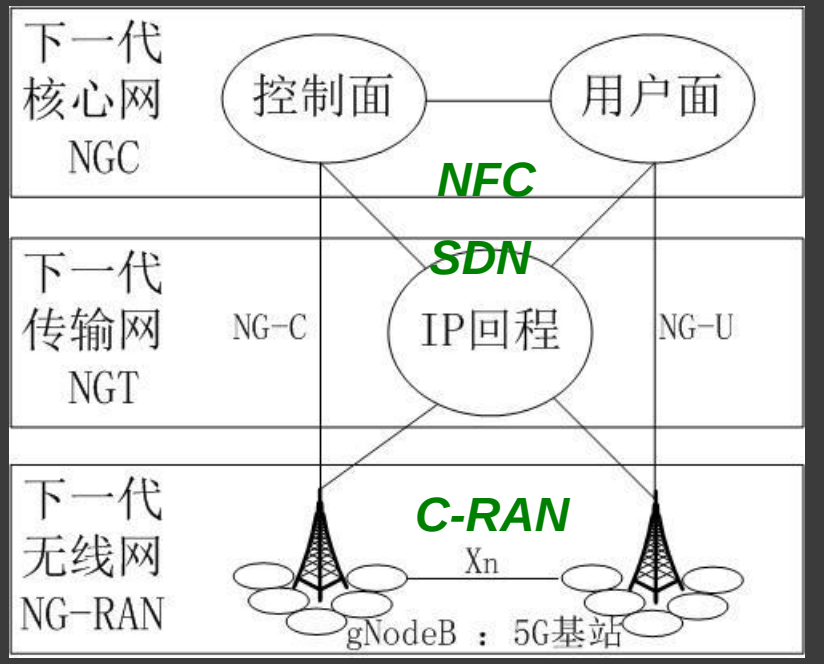
直播互动提供了实时视频的丰富信息和身临其境的参与感。

直播“云”用户只负责采集和接收，其余工作由“云”端负责。



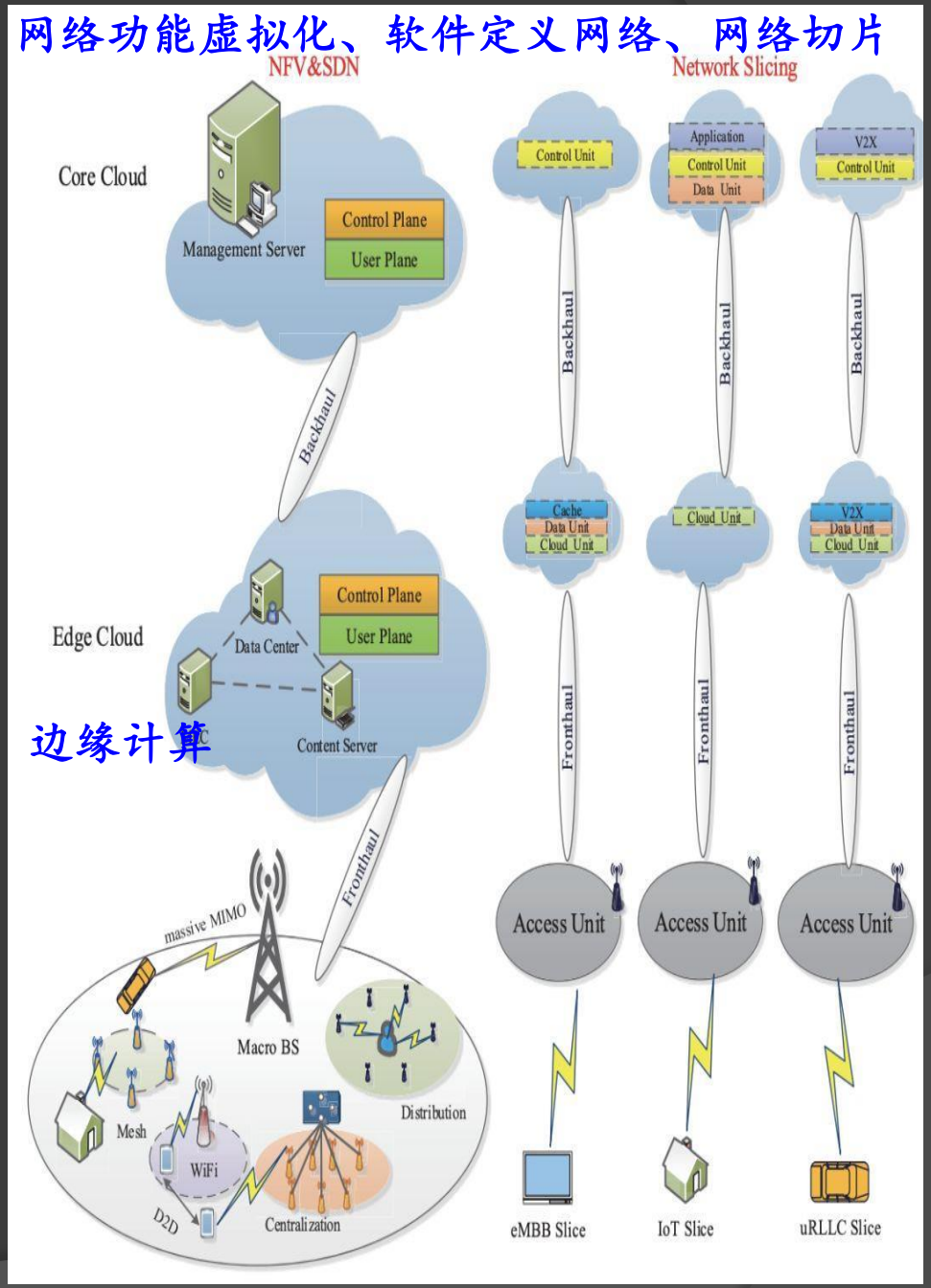


6、“5G网络”应用



- ✓ 增强移动带宽eMBB；
- ✓ 海量机器通信mMTC；
- ✓ 超可靠低时延通信URLLC。
- 毫米波、大规模MIMO；
- 编码、Cloud RAN；
- SDN、NFV、网络切片。

网络功能虚拟化、软件定义网络、网络切片



边缘计算

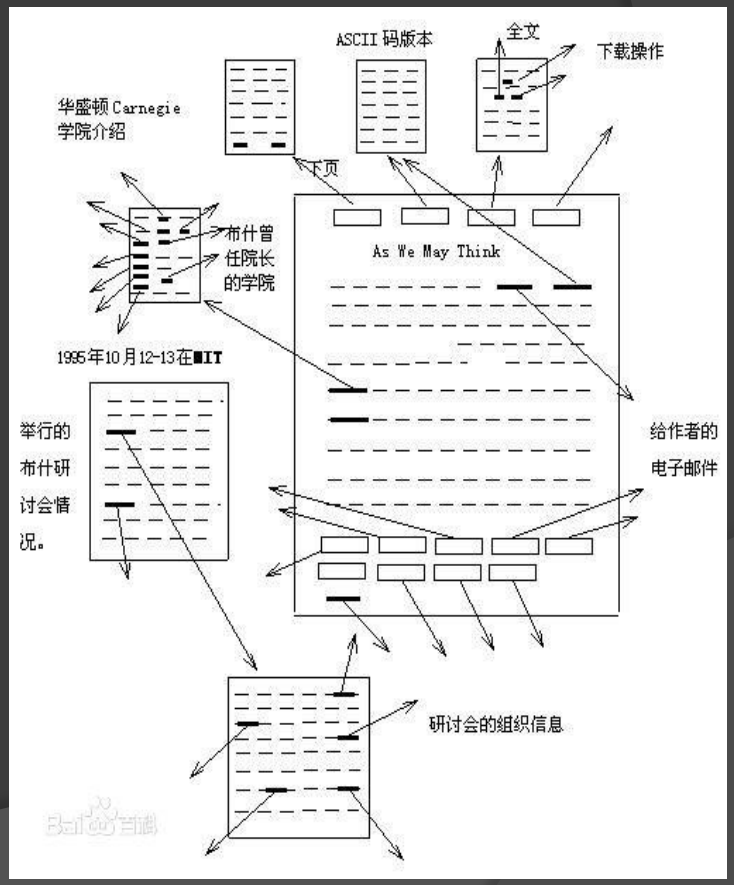
2.4.2 万维网(World Wide Web)

Web是全球性的、动态交互的、跨平台的分布式信息系统。

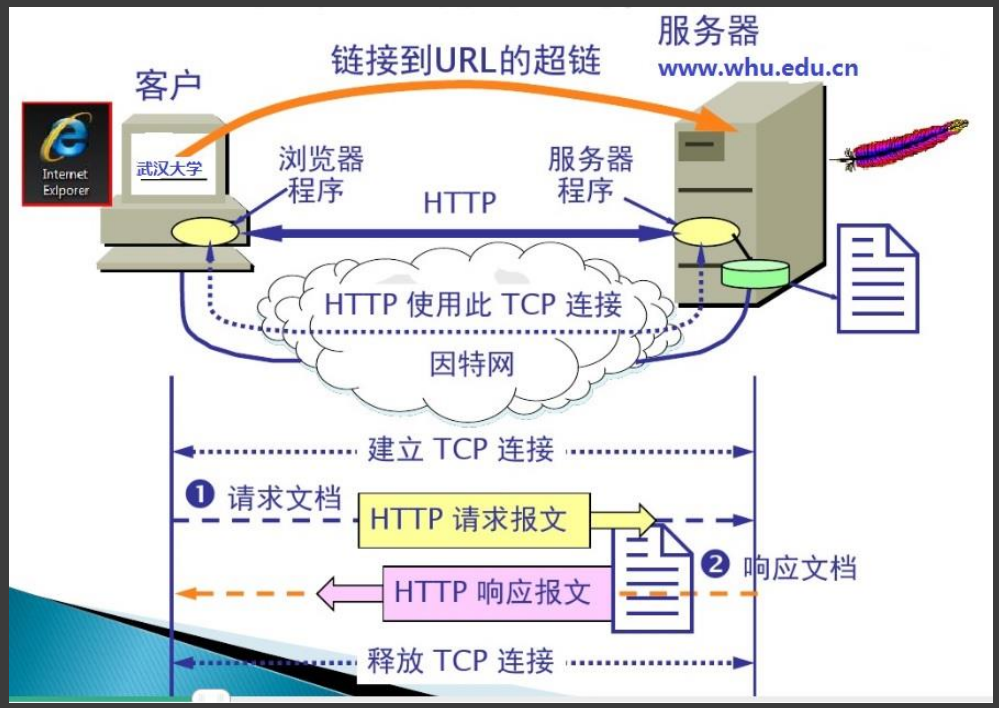
主要特性：
- 图形化的人机接口（点击鼠标即可上网）。
- 超文本（ HyperText，也称网络中的网络）。

超文本是被以超（特定）链接方式将不同位置空间的信息组织在一起的网状的信息文本集合。

超文本按照非线性关系组织、存储和显示信息，代表由众多信息节点和表示信息节点之间相关性的“链”所构成的一个具有逻辑关系和语义关系的非线性网络。



1、Web系统架构



系统构件：

- ✓ 浏览器端、服务器端程序；
- ✓ 统一资源定位符——URL；
- ✓ 超文本传输协议——HTTP；
- ✓ 超文本标记语言——HTML。

- 浏览器分析超链接指向页面的URL(http://www.whu.edu.cn/index.thml)；
- 浏览器向DNS请求解析www.whu.edu.cn的IP地址；
- DNS返回 202.114.71.2；
- 浏览器与服务器建立TCP连接；
- 浏览器发出读取网页文件命令：如 GET URL HTTP/1.1；
- 服务器将URL网页文件发给浏览器；
- TCP连接释放；
- 浏览器显示“武汉大学主页”上的所有信息。

URL（Uniform Resource Locator）：标识一个文档资源，同时指明资源的位置以及应怎样处理文档等内容。

格式：模式或协议、服务器名或IP地址、路径和文件名。

HTTP（HyperText Transfer Protocol）：采用请求/响应方式实现浏览器与服务器之间的Web文档传递。

- 利用TCP提供文档传输可靠性保证（点击链接后触发）。
- 支持一次TCP连接中请求多个文档，提高传输效率。
- 可通过Cookie机制维护客户的状态信息，简化操作。
- 设置代理缓存服务器提高已被访问文档的获取效率。

浏览器端缓存。
服务器端缓存。
中间结点缓存。

可大大减轻网络和服务器的工作负荷。

HTML（HyperText Markup Language）：一种制作Web页面的标准语言。其主要功能：1）告知浏览器如何显示信息；2）将分布的网页“链接”起来构成超文本。

- HTML定义了许多排版命令（即标签），将各种标签嵌入到需要显示的信息之间，就构成了HTML文档。
- 浏览器软件负责解释标签并显示标记的信息内容。
- Web网页可以包含文字、图片、音频、视频以及交互式内容的各类信息。
- HTML规定了链接的设置方法，指向同一网站的内链接需要指明路径；指向另一网站的外链接需要指明对方的URL，被点击后触发HTTP转入其他网站网页。
- 超链接关系无约束，由开发人员自行设计。

静态Web文档： 事先创建并存储在服务器中，通常不再改变。

动态Web文档： 接收到请求参数后才创建，再返回给用户。

服务器功能扩展
- 创建动态文档用的应用程序。
- 应用程序与Web服务器之间的通信机制。

活动Web文档： 在用户浏览过程中可实时更新内容的文档。

实现方式
- 服务器推送。
- 派遣小程序到客户端。

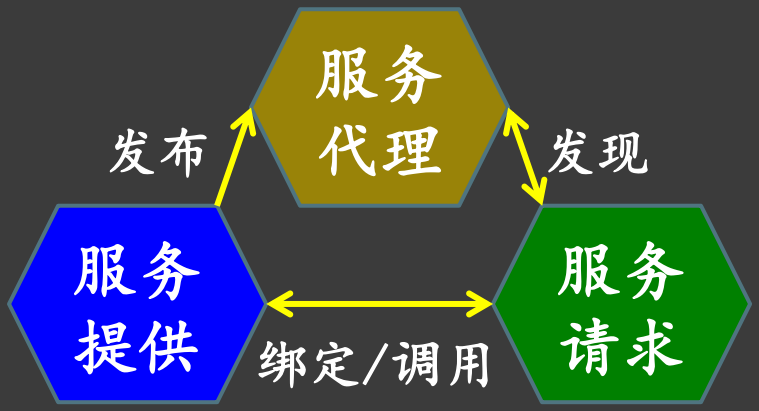
B/S结构

Internet Explorer、Chrome、360浏览器、…

Internet Information Services、Apache、…

Web Service

Web Service技术能使得运行在不同机器上的不同应用无须借助附加的、专门的第三方软件或硬件，就可相互交换数据或应用集成。



工作流程：

- 服务提供者将提供的服务功能发布到服务代理；
- 服务请求者到服务代理查询相关服务以及如何调用服务的信息；
- 服务请求者与服务提供者建立连接，调用所需的服务。

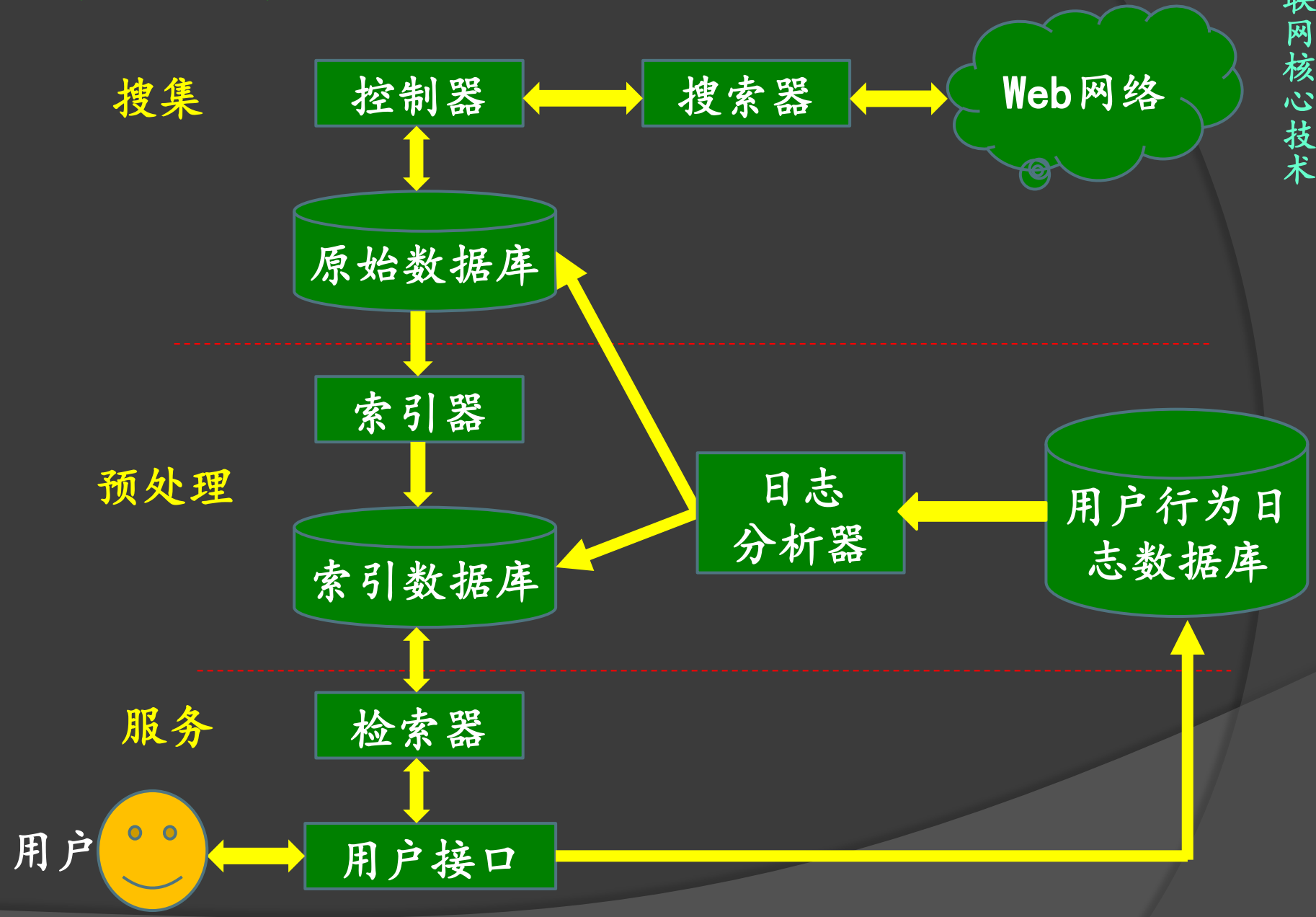
- WSDL：描述服务；
- UDDI：发布、查询服务；
- SOAP：执行服务；
- WSFL：将分散的、功能单一的服务组织成一个复杂的应用。

2、搜索引擎

搜索引擎是指根据一定的策略，运用程序从互联网上搜集和处理相关信息，为用户提供特定索引服务的系统。

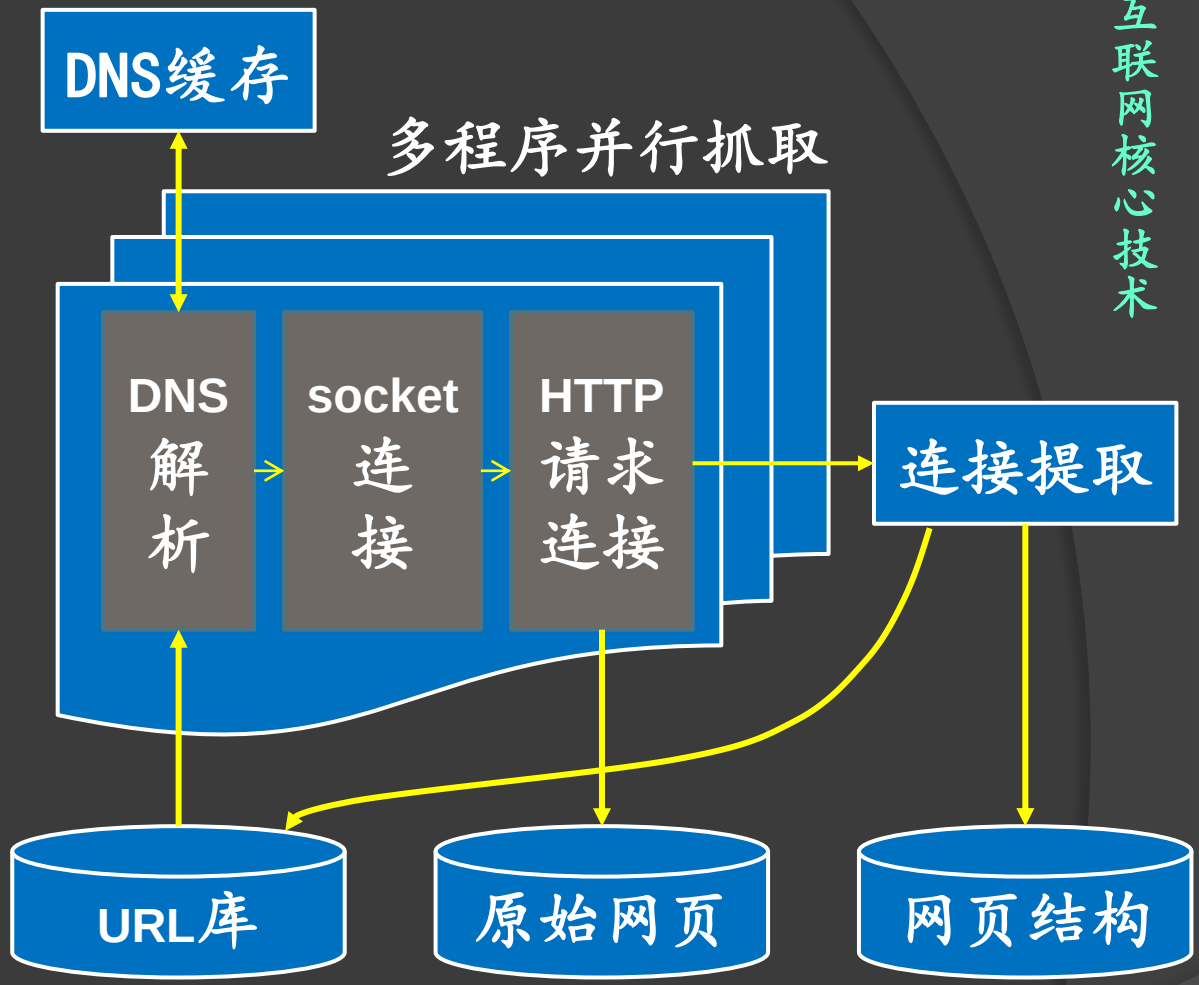
- 全文搜索：派出“spider”从网站提取信息，建立网页数据库。一种方式是定期搜索网站和更新数据库；另一种方式是网站主动提交新网址。
- 目录搜索：人工审核、编辑网站提交的关键词和站点描述信息，建立分类索引树。
- 元搜索：在多个搜索引擎查询与用户请求匹配的信息。
- 垂直索搜：针对特定需求去提取特定的相关信息。
- 集合式搜索，在用户提供的搜索引擎中查询相关信息。
- 搜索门户，查找专业经营搜索引擎业务的网站。

搜索引擎体系结构


搜集
控制器
搜索器
Web网络
原始数据库
索引器
预处理
日志
分析器
用户行为日
志数据库
索引数据库
服务
检索器
用户
用户接口

Web信息的搜集

从URL库获得输入；解析URL中的Web服务器地址；建立TCP连接；请求和接收网页；将获得的网页存入原始网页库；从网页中提取链接信息放入网页结构库；将新发现的URL加入到URL库；整个过程递归进行，直到URL库空为止。



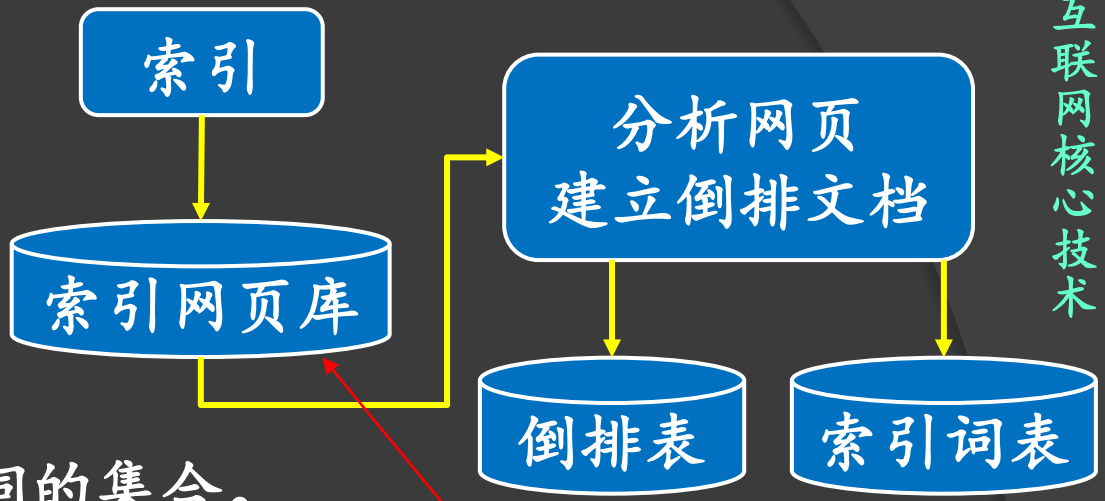
- 建立URL的“已访问表”和“访问表”，避免重复搜集。
- 需要专门处理域名与IP对应的问题。

搜集信息的预处理

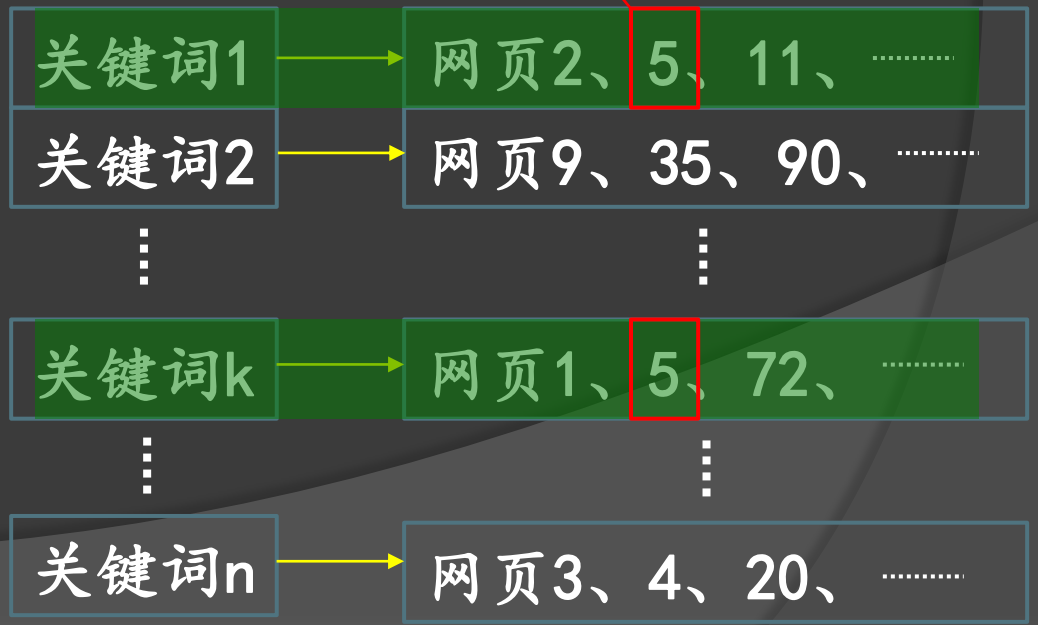
1）为原始网页建立索引，提供网页查询定位。

2）网页切分，将每一篇网页转化为一组关键词的集合。

3）将网页到索引词的映射转化为索引词到网页的映射，形成倒排文档，同时将非重复的索引词汇聚成索引词表。



搜索引擎面对的是海量数据，选择数据结构的时候需要考虑两个因素：紧凑的数据格式和高效的检索能力。

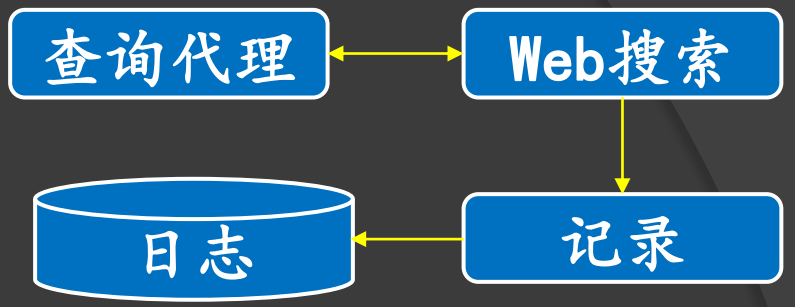


信息查询服务

查询代理接收用户输入的查询短语，切分后，从索引词表和倒排文档中检索获得包含查询短语的网页并返还给用户。

查询短语中可以包含多个关键词，关键词之间可以是逻辑“与”、“或”等运算关系，分别对应集合的交、并等运算。

针对查询的自然语言，对新提取的关键词需根据一些规则扩充进关键词库。



互联网核心技术

2.4.3 网络社交

平均130人左右 社交网络 —互联网→ 网络社交

联络人数指数性增长；非接触社交占80%以上。

- ✓ 一方面，互联网为社交提供了技术支撑；另一方面，网络社交成为推动互联网向现实世界无限靠近的关键力量。
- ✓ 即时通信提高交流的速度和并发；信息发布塑造“形象和性格”；两者结合就聚合了新的社团。

社交网络演进：

- 概念化；
- 结交陌生人；
- 娱乐化；
- 社交图；
- 云社交。

未成年人中：

- 74.8%认为网络不会暴露自己的身份；
- 70%认为网上聊天更轻松自在；
- 69%认为能找到志同道合的朋友。

2.5 网络安全

网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不因偶然的或者恶意的原因而遭受到破坏、更改、泄露，系统连续可靠地正常运行，网络服务不中断。

被动攻击：主要指从网络上截获他人信息。

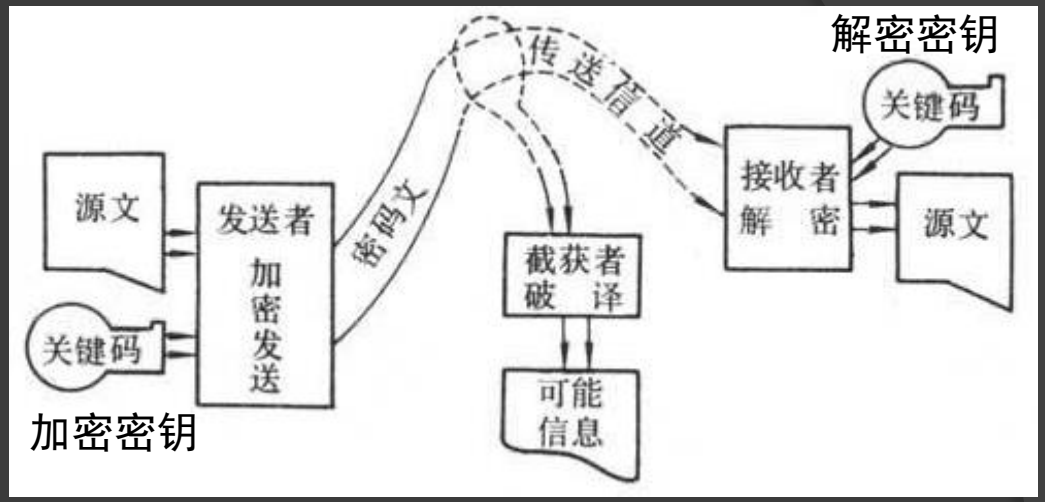
主动攻击：种类繁多，形式各异，五花八门。

- 篡改和假冒，修改他人的网络信息或者冒充他人身份去窃取信息。
- 恶意程序，通过派遣“小程序”实施干扰和破坏活动。计算机病毒、特洛伊木马、逻辑炸弹、拒绝服务、…

网络的社会特性决定了人类社会中所有欺诈手段和投机行为大都会在网络中体现，因此，安全防范需要全方位实施。

数据加密方法

传统加密方法有两种，替换和置换。单独使用这两种方法的任意一种都是不够安全的，但是，将这两种方法结合起来就能提供相当高的安全程度。安全性取决于通过相匹配的明文和密文破解密钥的难度。



对称密钥体制：加密与解密使用相同的密钥。典型代表IBM数据加密标准（Data Encryption Standard，DES）。

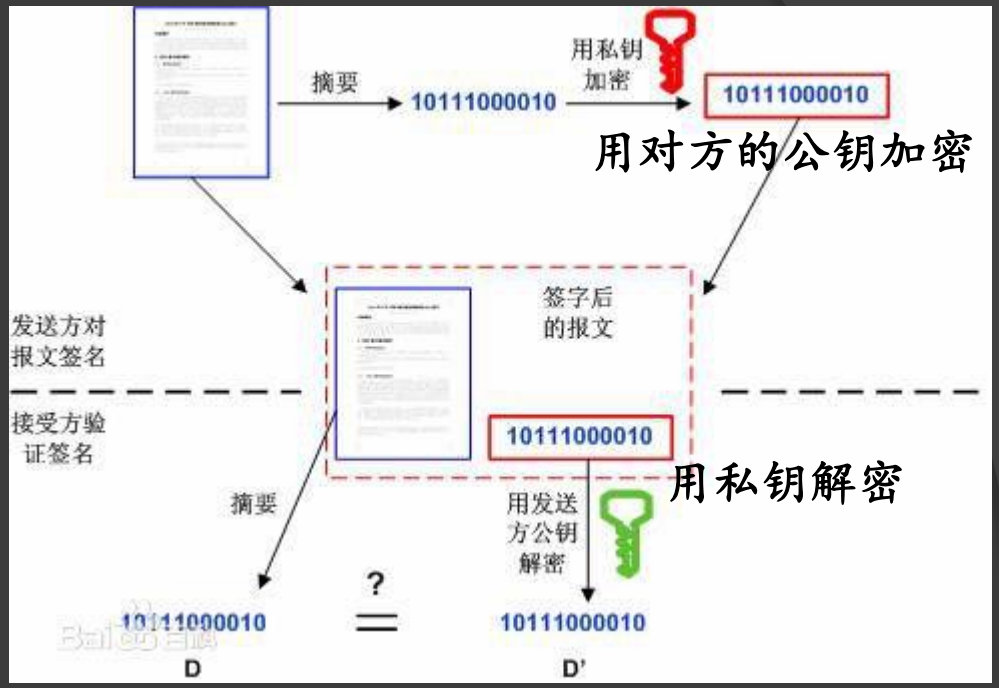
公开密钥体制：加密与解密使用不同的密钥。典型代表RSA方法，生成无法相互推导的公钥和私钥，用公钥加密，用私钥解密。其特点是加密者也无法解密密文。

数字鉴别机制

数字签名的功能：

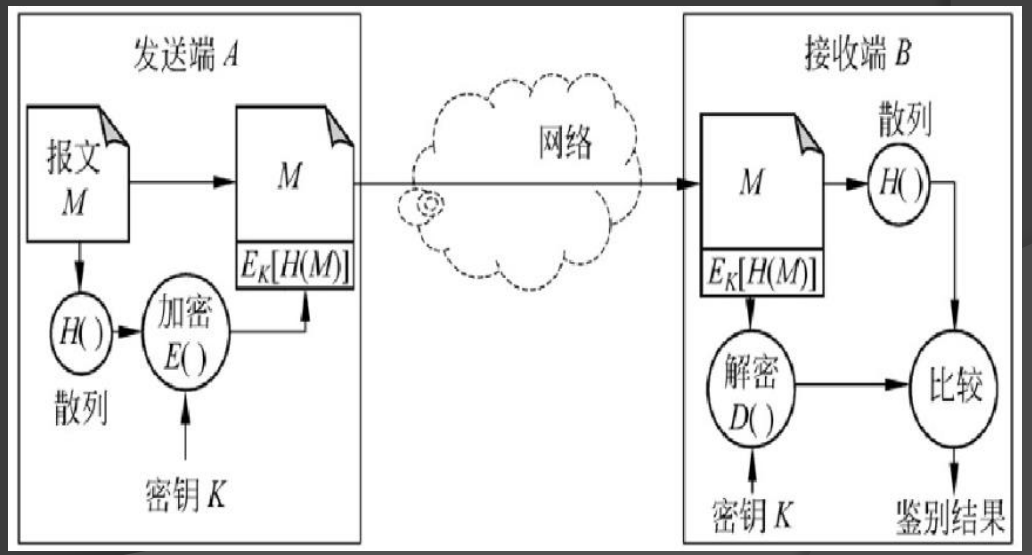
- ✓ 信息完整性；
- ✓ 不可伪造性；
- ✓ 不可否认性。

可采用公钥算法实现。



报文鉴别的功能：

证实收到的报文来自可信的源端，并且没有被篡改过。可采用散列码加密的报文摘要算法实现。



Internet安全协议

网络层：IPsec协议（AH协议和ESP协议）

- 首部鉴别协议AH提供数据完整性和身份认证服务。
- 载荷安全封装协议ESP进一步增加了报文加密服务。

安全关联在源端与目的端之间建立一条逻辑连接。

传输层：安全套接字层（Secure Socket Layer，SSL）

- 服务器鉴别服务。
- 客户鉴别服务。
- 会话加密与检测。

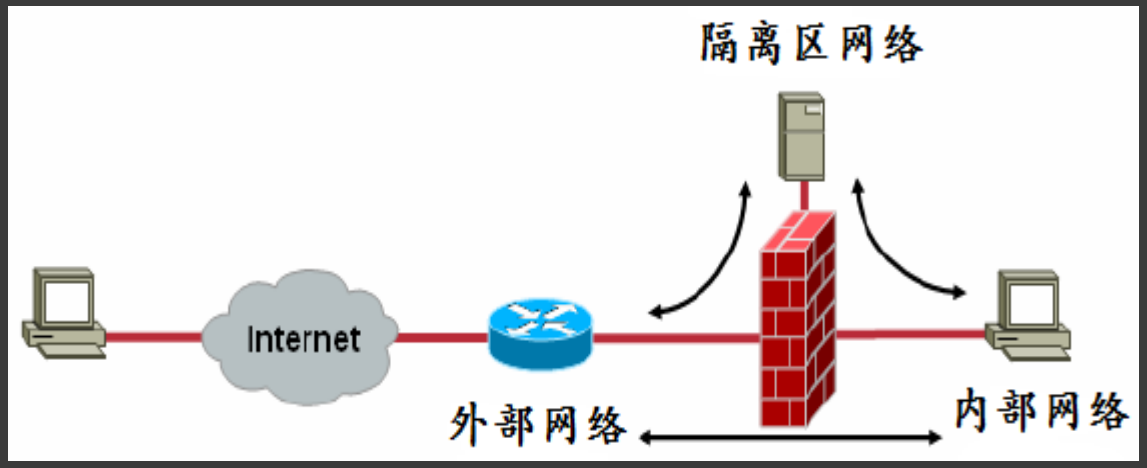
传输层安全（Transport Layer Security，TLS）协议

应用层：PGP(Pretty Good Privacy)，提供安全电子邮件服务。

⋮

安全网关——防火墙

防火墙是一种访问控制技术，通过严格地控制进出网关的分组，减少潜在入侵的发生，尽可能地降低安全风险。

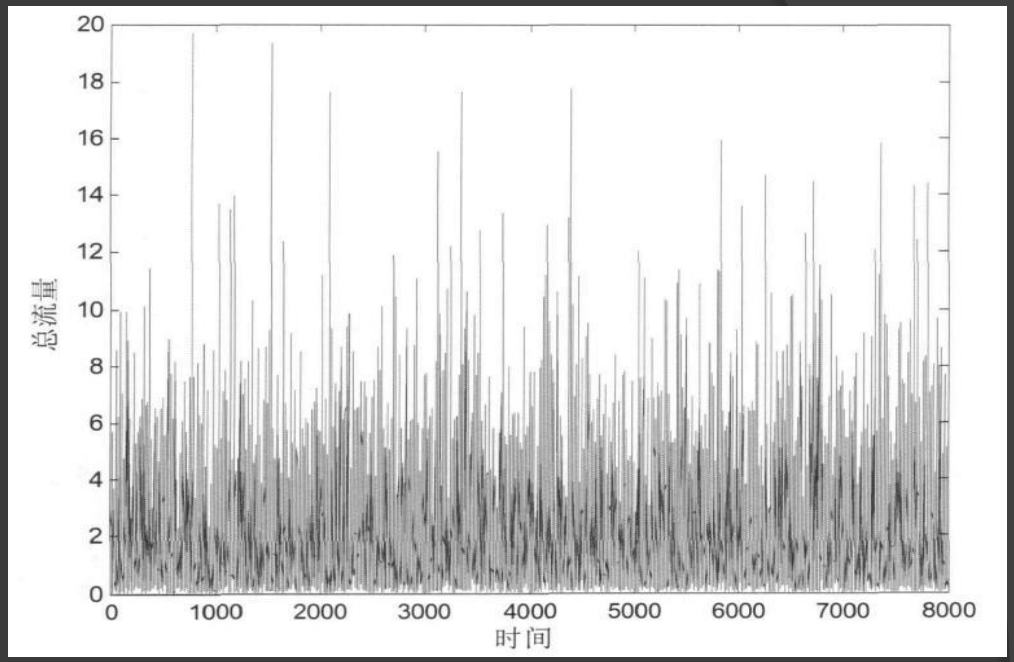


安全控制策略由使用者自行制定，以最适合本单位需求为目标。

- 认证功能，对一个实体所声称的身份进行确认。
- 完整性功能，防止传输的报文信息被篡改。
- 访问控制功能，决定是否允许分组通过防火墙。
- 审计功能，记录重要事件日志，监视事件的发生。
- 网关功能，对合法访问执行路由转发服务。

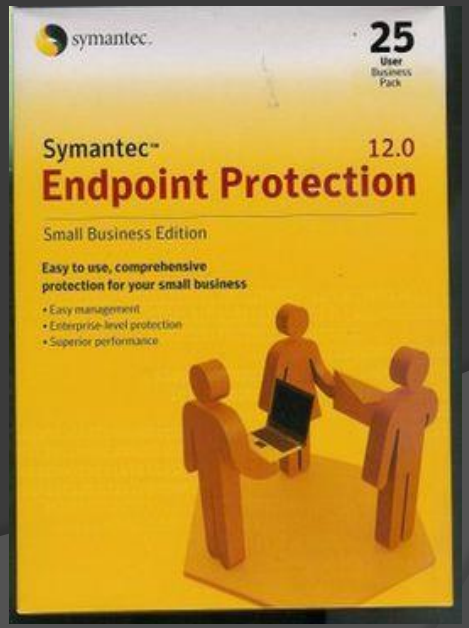
网络行为分析

网络行为分析是一种通过监测网络流量、分析和发现网上异常行为，从而提高专有网络安全性的手段。



病毒检测

- 将用户提交的程序与病毒库中定义的病毒特征码进行比较、甄别。
- 将用户提交的程序在开辟的虚拟执行系统内运行，根据其行为和结果作出判断。



防火墙 + 杀毒

作业：

4、电路交换与分组交换各自的主要优缺点是什么？

5、数据发送和接收中，封装和解封装的作用是什么？

6、简要说明IP层和TCP层完成的主要任务，以及该模型的开放性和兼容性。

7、写出你的计算机配置的IP地址、地址掩码、默认网关、DNS，并且，简要说明它们的用途。

8、为什么IPv4会出现地址危机问题？缓解这种地址危机的方法有哪些？

9、IPv6地址的长度是多少？接口标识符的用途是什么？

10、外部路由协议和内部路由协议有什么不同用途?

11、单播路由与组播路由有何相同与不同?

12、为什么说“TCP是可靠的，而UDP是不可靠的”?

13、解决TCP对网络流量调控能力不足的方法有哪些?

14、列举一些你经常使用的互联网应用程序。

15、为什么说Web网是“网络之上的网络”?

16、FTP、SMTP、HTTP等都采用TCP协议实现数据传输，这种做法的好处是什么？缺点是什么？

17、“云计算”采用的的网络应用模式是什么？其主要优点是什么？关键技术有哪些？

18、Web网页的地址信息如何标识？

19、搜索引擎的主要工作流程是什么（自己总结）？

20、Web服务系统的组件和相关协议有哪些？它们各自承担的主要任务是什么？

21、数据加密可以避免那些安全问题？

22、什么是对称密钥和非对称密钥？

23、在网上购物时，你需要进行那些身份认证操作？简要分析一下这样处理的好处是什么？

24、从网络组成布局看，在何处布设防火墙效果最好？