

计算机网络概论

课程小结

2016年6月14日

一、计算机网络概述

- 网络定义：为共享资源（硬件、软件和信息等）而连接起来的、在协议控制下由一台或多台具有独立自治能力的计算机和传输设备等组成的系统。
- 网络分类：
- 覆盖范围：广域网、局域网、城域网、个人区域网、园区网；
- 拓扑结构：星型网、总线网、环型网、网状网、树状网；
- 管理性质：公用网、专用网、虚拟专用网（VPN）；
- 因特网、内联网、外联网、接入网；
- 交换方式：电路交换网、报文交换网、分组交换网；
- 功能特性：通信（子）网、资源（子）网。
- 计算机通信：协议控制下的进程之间的通信。

二、数据通信原理

- 信源/信宿和信道类型匹配：调制/解调和编码/解码；
 - 调制/解调：调幅/调频/调相/组合；
 - 编码/解码：取样-量化-编码；
- 信息在信道上的表示：通信编码
 - 单极性、双极性，RS232码、不归0交替码、曼码、4b/5b码；
- 信息在计算机内的显示：ASCII码等；
- 收发双方的同步：同步/异步传输
 - 只有实现位同步，才能完成块同步；

二、数据通信原理

- 差错处理—反馈重传法：
 - 停-等协议、滑动窗口（多块传输、统一确认）。
 - 常用的检错码：奇偶校验码、正反码、循环冗余码（CRC）；
 - 具有差错处理能力的传输控制规程：
 - 字符型传输控制规程（基于半双工的停-等协议）
 - 比特型传输控制规程（基于全双工的滑动窗口协议）；
 - 注意控制字符（或者控制序列）在数据字段中出现时的歧义解决方法（填充转义）
- 提高线路利用率的方法：
 - 多路复用(频分/时分/波分)和集中传输；
- 中间结点转发信息的方法：
 - 电路交换、报文交换、分组交换；
- 分组流传输管理方法：
 - 面向无连接的数据报、面向连接的虚电路。

三、计算机网络体系结构和协议

- 制定开放系统互连参考模型的目的；
- 开放系统互连实现的方法；
 - 系统设计方法：分解（模块化）和抽象；
 - 系统开放方法：定义公共模式，实现本地模式/公共模式映射；
- 开放系统互连参考模型的层次及功能；
 - 拟解决的问题及解决问题的方法；
- 开放系统互连参考模型中层间通信的区别；
 - 相邻层间、对等层间；
- 协议在层间通信中的作用。

三、计算机网络体系结构和协议

- 网络体系结构：网络标准的目的、**OSI/RM**的设计原则、**OSI**的术语和总体概况（包括层次划分、协议数据单元之间的关系、层间交换的方式）、物理层（设备和媒体的接口特性）、数据链路层（多链路规程）、网络层（**X25**协议）、运输层（解决用户需求和网络服务之间差异）；
- 网络体系结构：会话层（会话控制及完整性）、表示层（数据表示方法）、应用层（应用服务提供的基本模型）、其它体系结构简述。

四、局域网

- 局域网：局域网的基本结构和设计原理、相关标准、总线网（**CSMA/CD**及其实例——以太网、**TokingBus**）；重点为以太网，包括目前的现状和应用情况。
- 局域网：环形网（令牌环及其实例——**IBM**令牌环、时间片环及其实例——**TORnet**、光纤分布式数字接口**FDDI**）、**LLC**及其接口方式。

总线型局域网小结

特点：所有结点附接一根总线，通过总线收发帧；对应共享总线可能冲突，采用了各种总线访问方式。

竞争方式：

CSMA/CD—以太网；

特点：结点抢占总线；

发送前侦听，

发送时检测，

冲突退避；

结论：重载时性能不好，

难以确定帧的发送时间。

按序方式：

TokenBus—ARCnet；

特点：令牌传递总线访问权；

发送前等待令牌，

发送后传递令牌，

监控令牌唯一性；

结论：具有帧最小发送延迟，

可预测最大发送延迟。

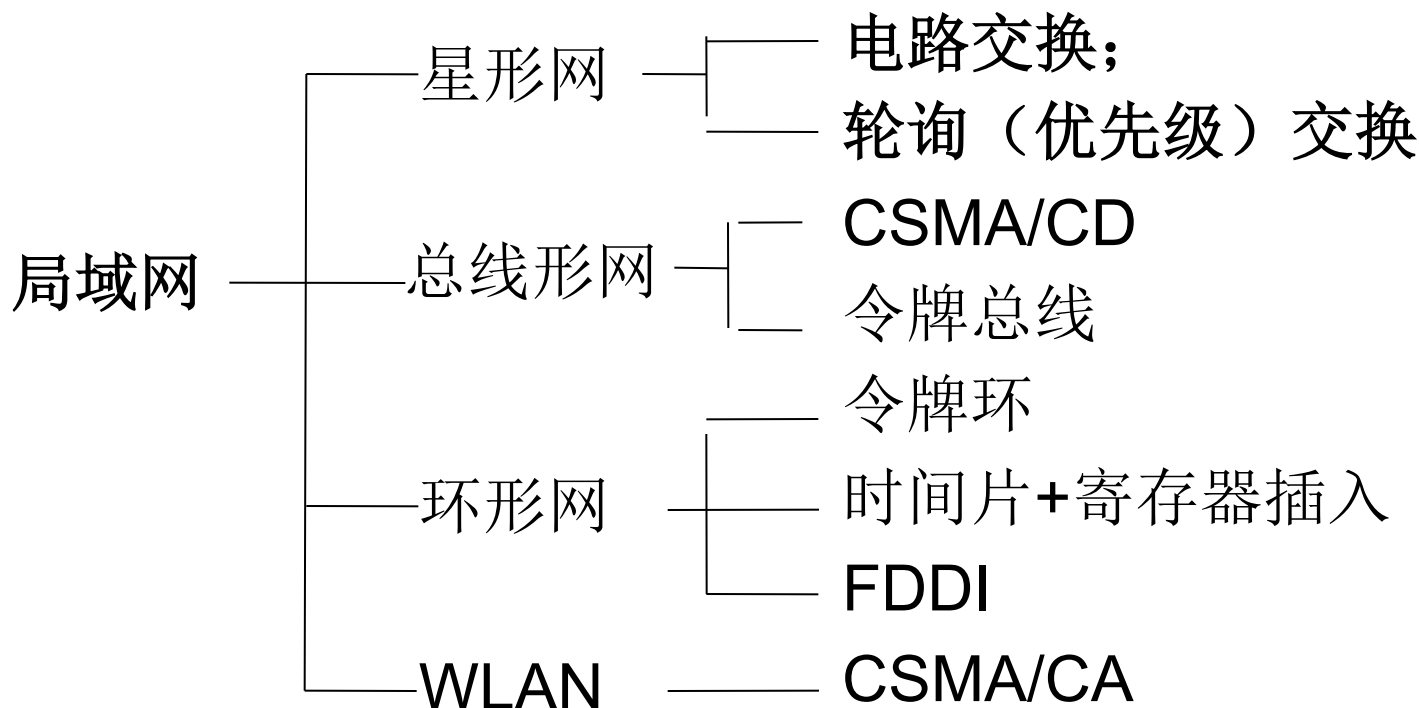
WLAN小结

- 结点采用无线信道作为传输媒体；
- 为了提供安全性，引入扩频技术（跳频扩频和直序扩频）；
- 为了共享无线信道，WLAN采用竞争信道的方式工作；
- CSMA/CA：发前侦听，闲时发送，预约信道，避免冲突；
- 预约信道：RTS / CTS；
- 预约冲突：指数退避。
- 结点漫游根据AP信号强度判断是否需要切换。

局域网的特点：范围小—传输媒体质量高—广播发送；

局域网的体系结构：数据链路层 = LLC子层 + MAC子层；

技术焦点：媒体访问控制（MAC）技术（包括传输和维护）；

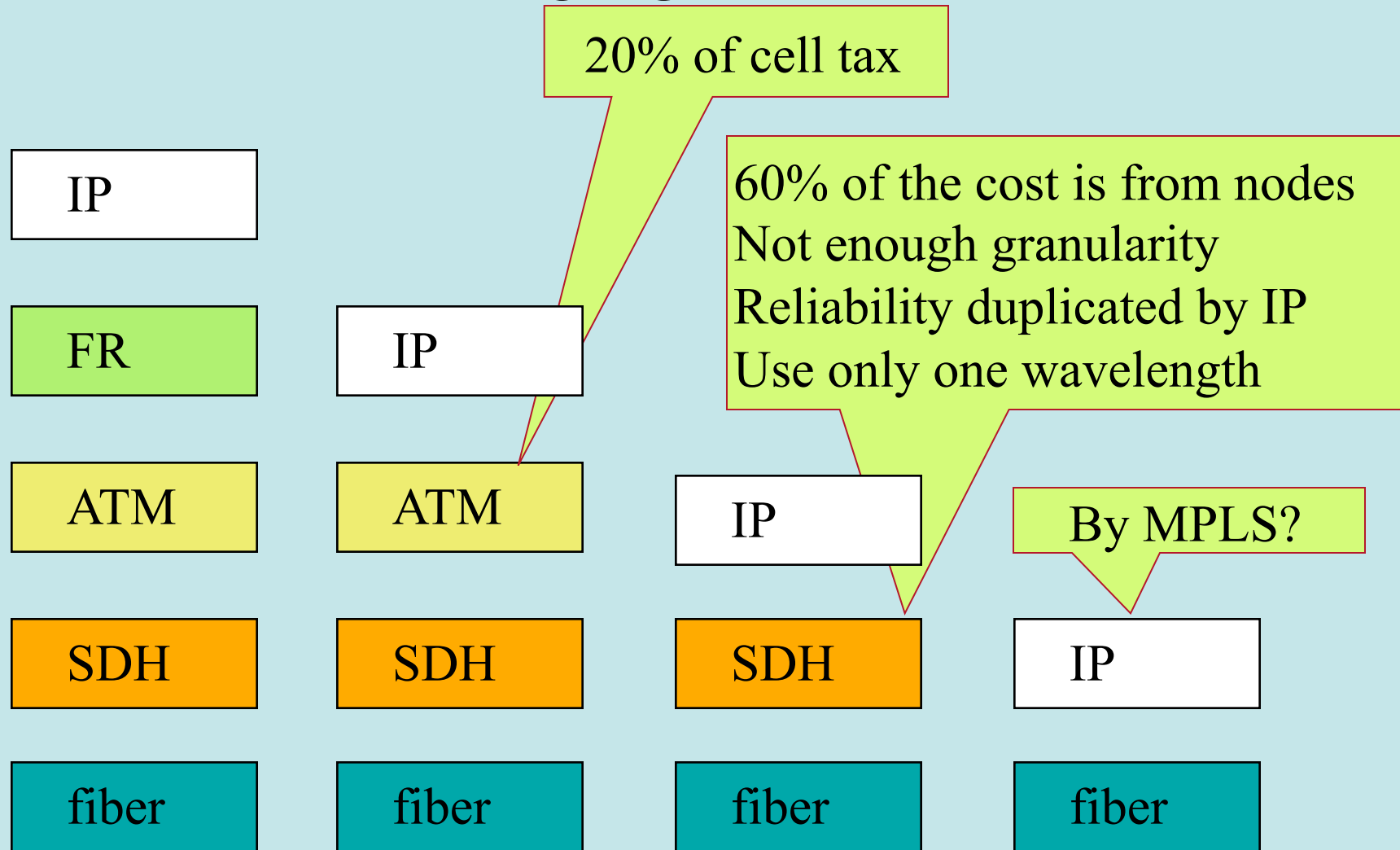


LLC屏蔽MAC子层差异，向上层提供统一的接口。

五、广域网

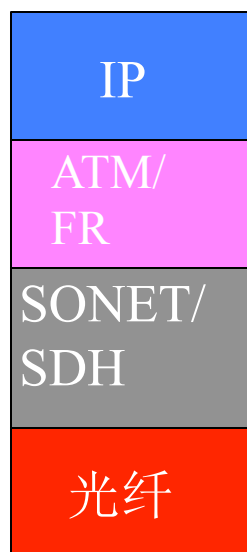
- 各类网络的原理及其使用方法
- PDH和SDH
- DDN
- 分组交换网
- 帧中继网
- ISDN
- ATM
- WDM

IP over ?



体系结构的简化趋势

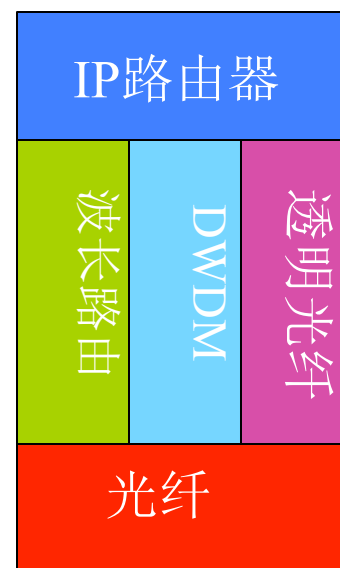
传统模型



- 降低设备成本
- 降低运营成本
- 简化体系结构
- 可扩展的网络容量



光纤互联网



IP服务

大容量光
纤管道

六、网络互连

- 互连的目的及其基本原则
- 网络互连设施的分类
- 转发器（集线器）、桥接器（交换器，冗余交换器及生成树协议）
- 虚拟局域网VLAN
- 路由器、网关。

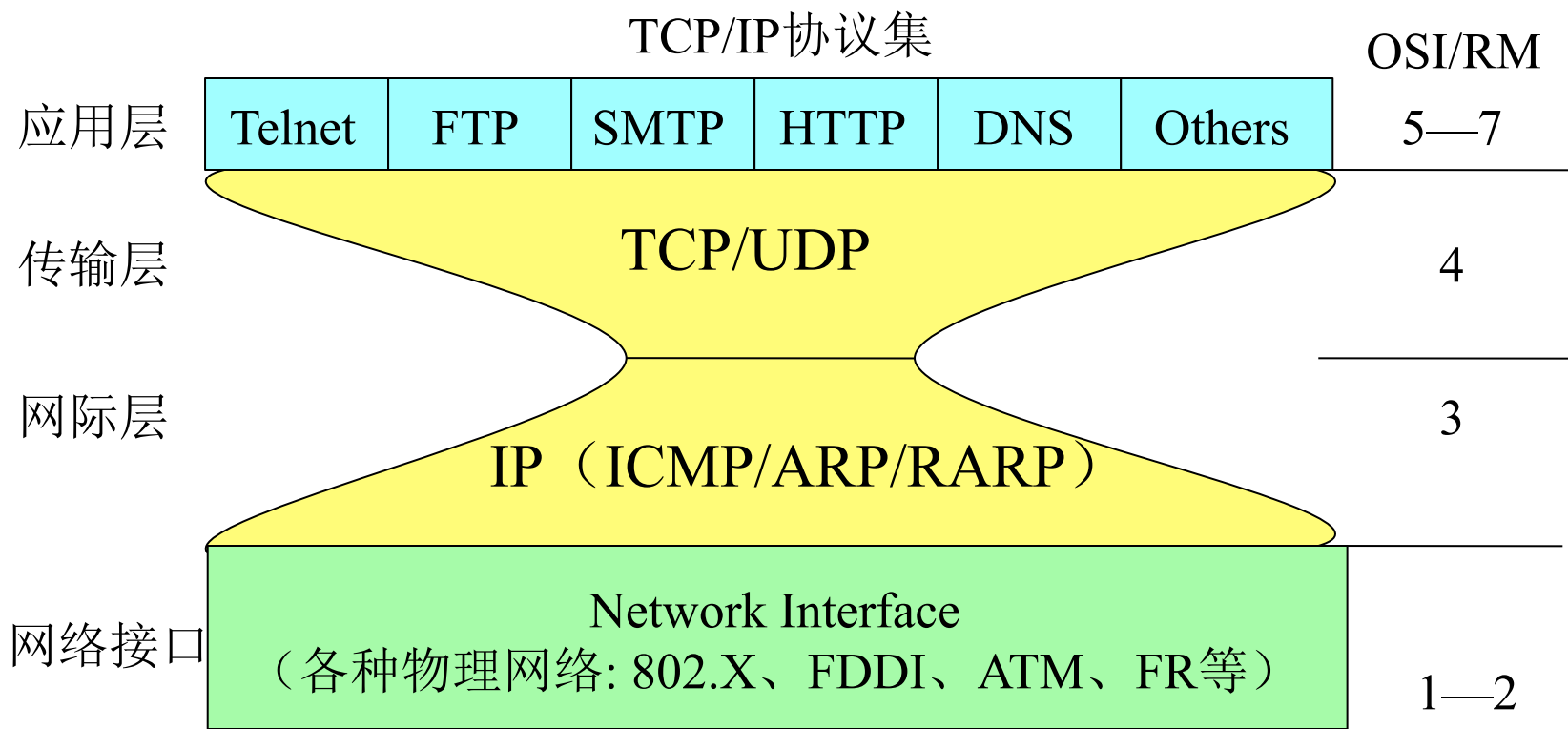
路由协议

- 路由的基本概念、分类
- Internal Routing
 - Routing Information Protocol
 - Open Shortest Path First
- External Routing
 - Autonomous Systems
 - Border Gateway Protocol
- 组播技术
- MPLS
- Mobile IP (v4、v6)

七、因特网

- 组成、层次结构等
- 因特网地址（网络地址、**IP**地址、域名地址、地址映射）
- 因特网协议集、**IP**协议、**TCP**协议（含**UDP**协议）、**Socket**编程
- 因特网服务（**SMTP**、**FTP**、**WWW**）、**IP**技术的推广应用（内联网、外联网、虚拟专用网）

因特网的体系结构—沙漏型结构:



因特网结构的包容性：上可支持各种应用，下可兼容/依托各种物理网络，简化中间结构；

IP的基本概念

设计原则

- 基于无连接传输服务的连接技术。
- 无论是否与其它网络互联，每一个网络都是唯一的和可自维持的，可自主运行；即网络是自治系统。
- 通信采用尽力而为的方式。
- 中继系统（路由器）不维护任何与特定数据流有关的状态。

IP地址分配

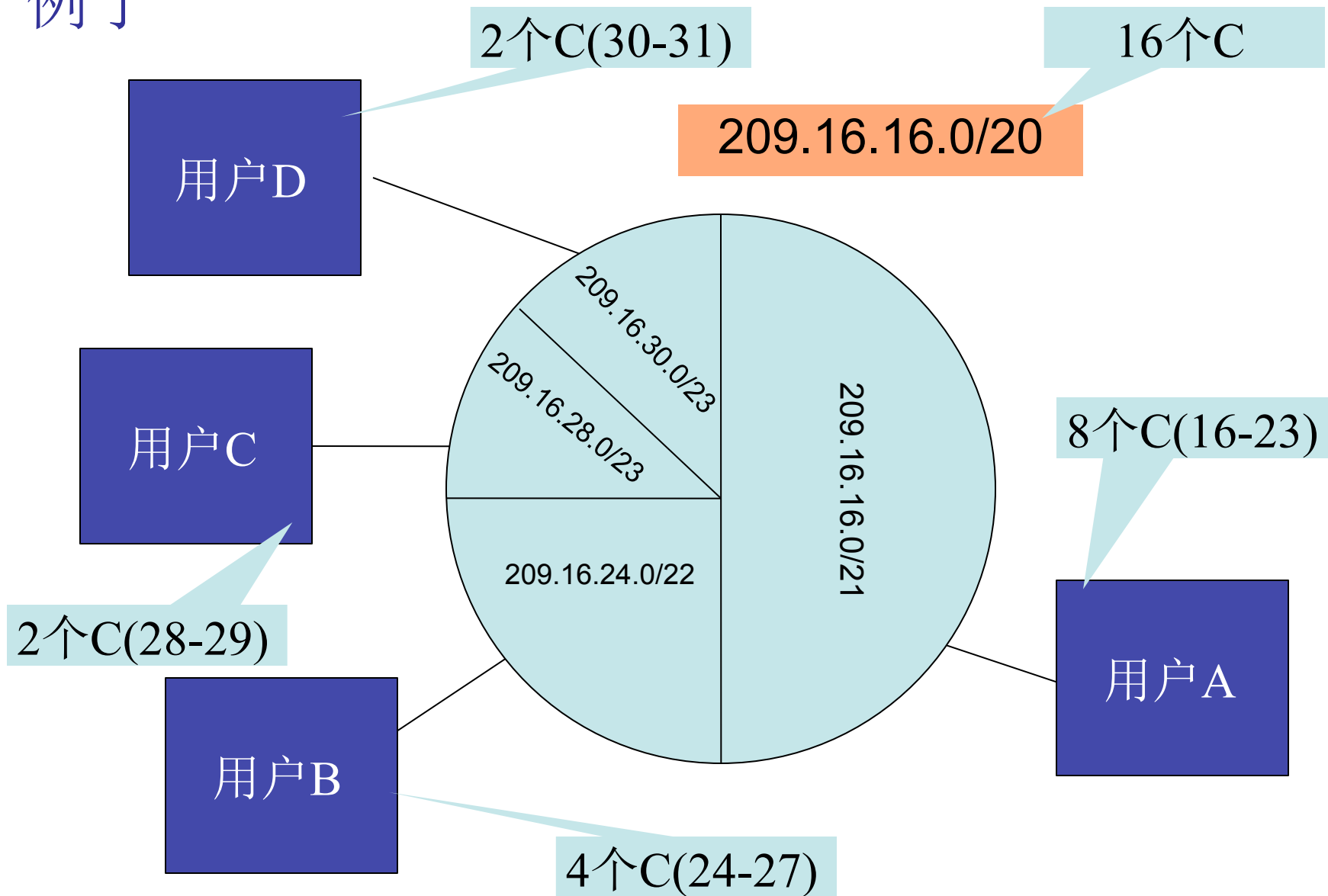
CIDR (Classless InterDomain Routing, RFC 1517-1520)

- 使用变长掩码来表示网络前缀的长度，可打破传统地址类别的边界。
 - 表达方式
 - 指出网络地址长度：aaa.bbb.ccc.ddd/xx
 - 给出网络地址的位数：255.255.255.xxx
- | | |
|------------------------------------|------------|
| Class A networks have a /8 prefix | 10/8 |
| Class B networks have a /16 prefix | 172.16/12 |
| Class C networks have a /24 prefix | 192.168/16 |
- 作用：实现子网划分与地址聚类，提高IP地址的使用效率。

Prefix Assignments

Number of Prefix	Dotted-Decimal Address	Number of Addresses	Number of Class
/13	255.248.0.0	512k	8 class B or 2048 class c
/14	255.252.0.0	256k	4 class B or 1024 class c
/15	255.254.0.0	128k	2 class B or 512 class c
/16	255.255.0.0	64k	1 class B or 256 class c
/17	255.255.128.0	32k	128 class C
/18	255.255.192.0	16k	64 class C
/19	255.255.224.0	8k	32 class C
/20	255.255.240.0	4k	16 class C
/21	255.255.248.0	2k	8 class C
/22	255.255.252.0	1k	4 class C
/23	255.255.254.0	512	2 class C
/24	255.255.255.0	256	1 class C
/25	255.255.255.128	128	1/2 class C
/26	255.255.255.192	64	1/4 class C
/27	255.255.255.224	32	1/8 class C

例子



➤子网掩码地址的扩展使用—无类域间选路（超网）

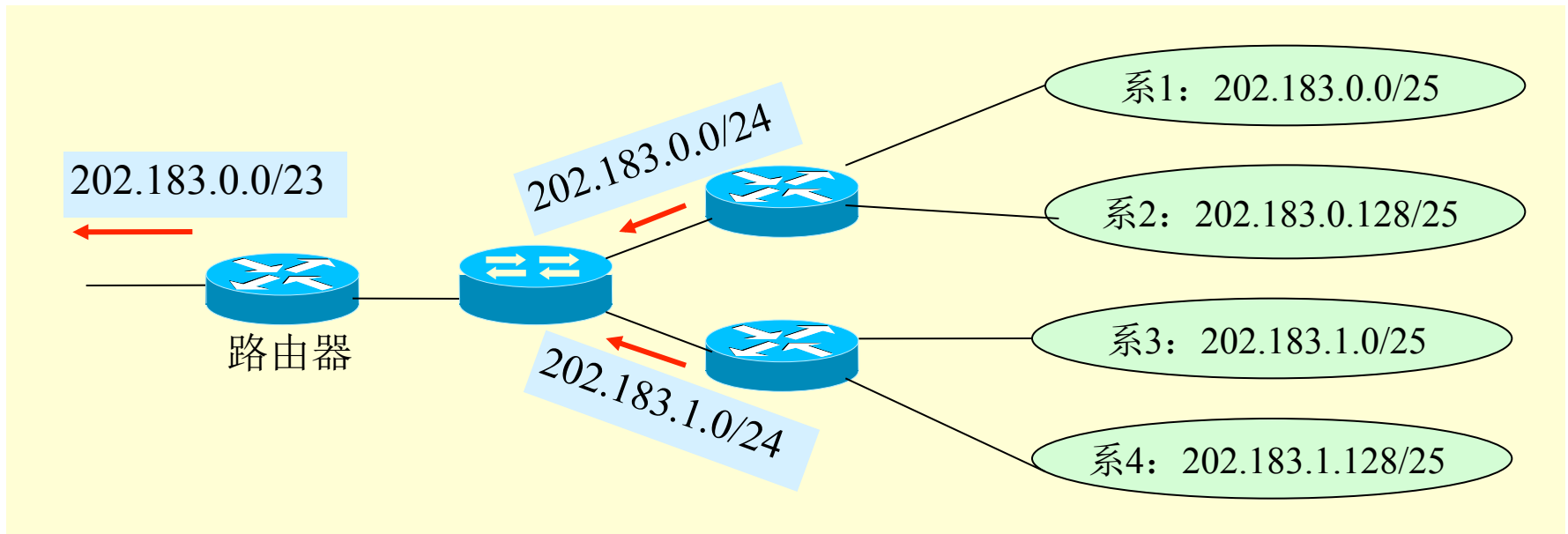
举例：某学院约有近400台计算机，申请2个C类地址，分配给4个系，90，100，110，120：

202.183.0.0—202.183.1.0；

掩码地址可定义为：255.255.252.0；

对外实际子网地址：202.183.0.0

表明这4个C类地址属于一个子网，可由一个路由器负责选路。



➤ 动态分配IP地址

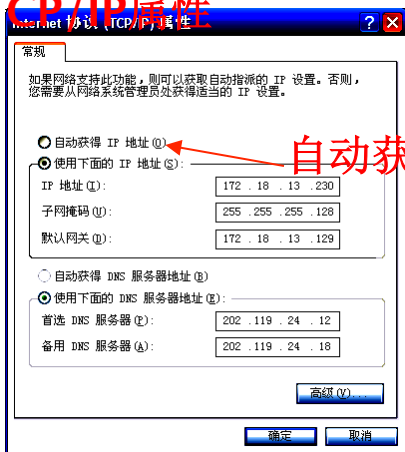
目的：动态调整，按需分配IP地址给希望上网的用户主机

原理：地址分配服务器维护IP地址池，希望上网的用户向其申请IP地址，使用后释放IP地址，提高地址利用率。

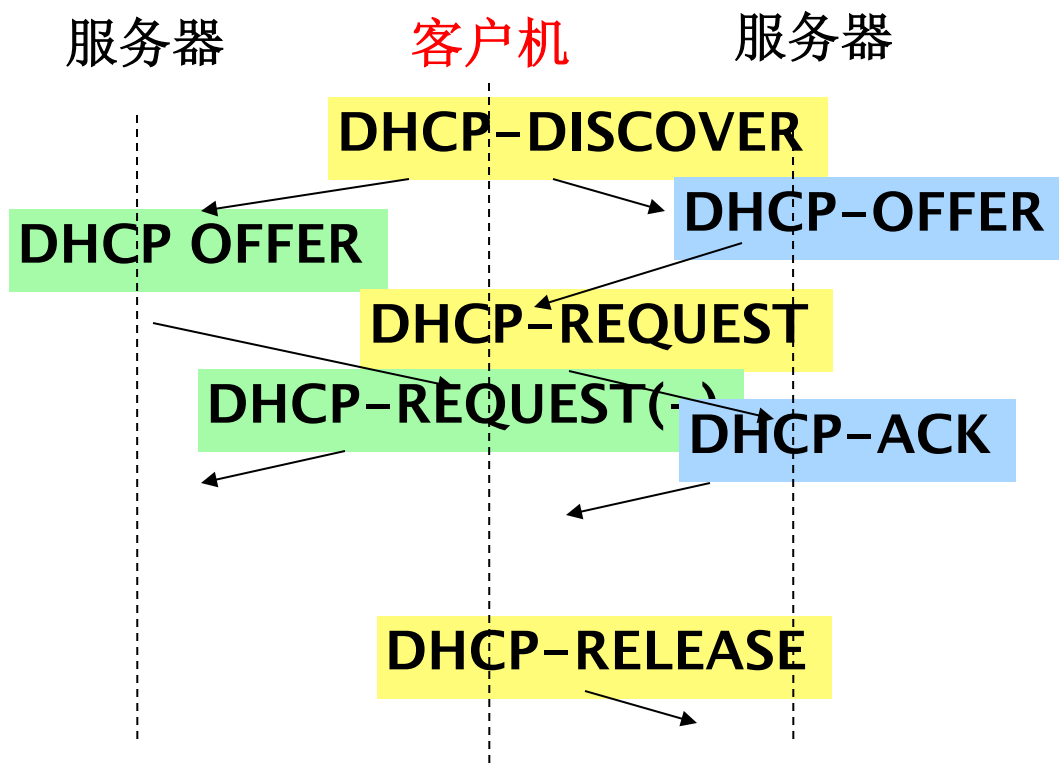
过程（RFC2131—动态主机配置协议DHCP）：广播寻找服务器，租用地址。

注：地址租用具有时间限制，续租或者回收。

TCP/IP属性



自动获取IP地址



因特网协议集

	TCP/IP协议集						OSI/RM
应用层	Telnet	FTP	SMTP	HTTP	DNS	Others	5—7
传输层	TCP / UDP						4
网际层	IP		ICMP	ARP RARP			3
接口层	Network Interface （各种物理网络: 802.X、FDDI、ATM、FR等）						1—2

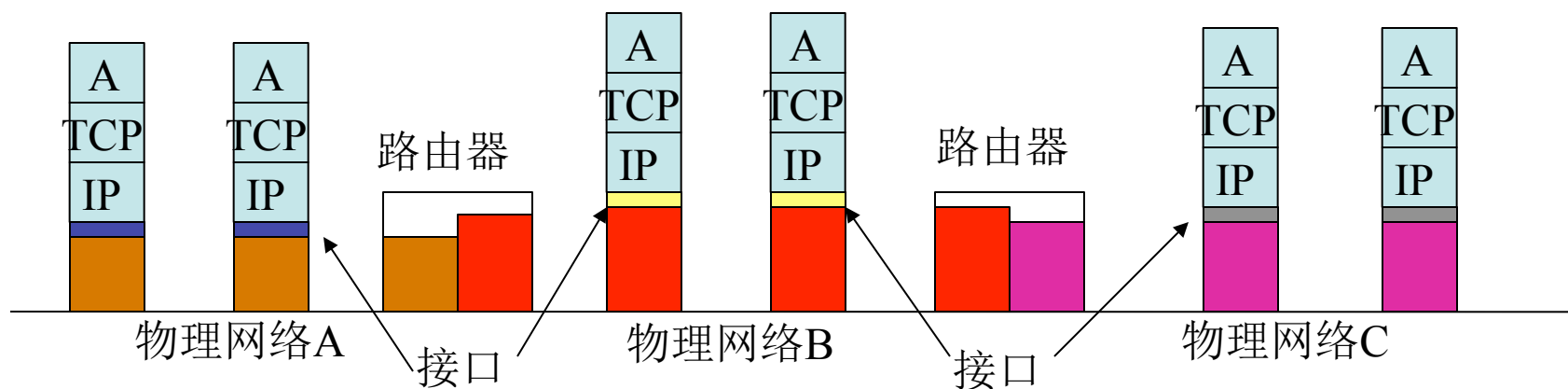
Telnet: 远程登录; FTP: 文件传输; SMTP: 电子邮件; DNS: 域名系统;
HTTP: 超文本传输; TCP: 传输控制协议; UDP: 用户数据报协议;
ICMP: 网际报文控制; IP: 网际协议; ARP: 地址解析; RARP: 反向地址解析。

特点: 利用网络接口屏蔽不同子网的差异, 定义相同的高层 (IP之上层) 协议, 提供多种应用服务。

IPv6

- IPv6概论
- IPv6地址
- IPv6的操作
- IPv4/IPv6并存技术

- ☆ 因特网的核心应是**IP技术**，通过定义接口，实现了基于不同物理网络的数据传输；
- ☆ 尽管IP本身仅提供无连接的、尽力而为的、不可靠的数据报传输，但**ICMP**的报错和**TCP**的恢复能力，使得基于因特网的应用可以获得可靠的数据传输保障。
- ☆ 对于不同的应用，可以选择**TCP**或者**UDP**来传输相应的信息；
- ☆ 因特网应用丰富，尤其是**E-mail**和**WWW**具有广泛的用户；
- ☆ 主机**接入因特网**的关键是执行TCP/IP协议集，可以获得合法的IP地址，以及某个合法的因特网设备愿意提供接入服务。



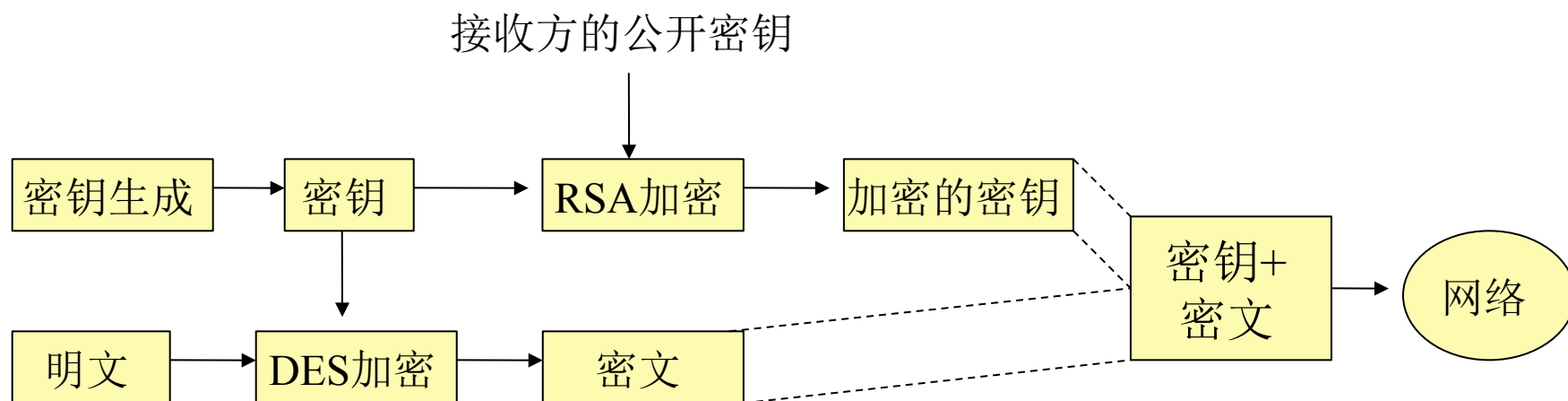
八、网络管理和网络安全

- 网管的功能：配置、故障、计费、性能和安全）、体系结构、基本模型、**MIB**。
- **SNMP**协议机制。
- 网络安全：网络攻击的类型、数据加密技术（对称/非对称密钥加密体系，相关加密算法）、摘录技术、防窃取技术（加密的应用）、防篡改/重播技术（完整性保护）。
- 防假冒/伪装技术（实体鉴别）、抗否认技术（数字签名）、防火墙技术（过滤、地址迁移）、权限和访问控制。

内容保密—防窃取

直接采用**加密技术**对数据进行加密；

为提高加密的效率，混合使用秘密密钥加密体系和公开密钥加密体系的算法。



特点： 对应每次通信，形成一个一次性密钥（随机数）；
只有指定的收方才可以获得密钥，解密密文；
使用DES算法和该密钥对明文加密，提高效率；
使用RSA算法对密钥加密，保护密钥的秘密性。

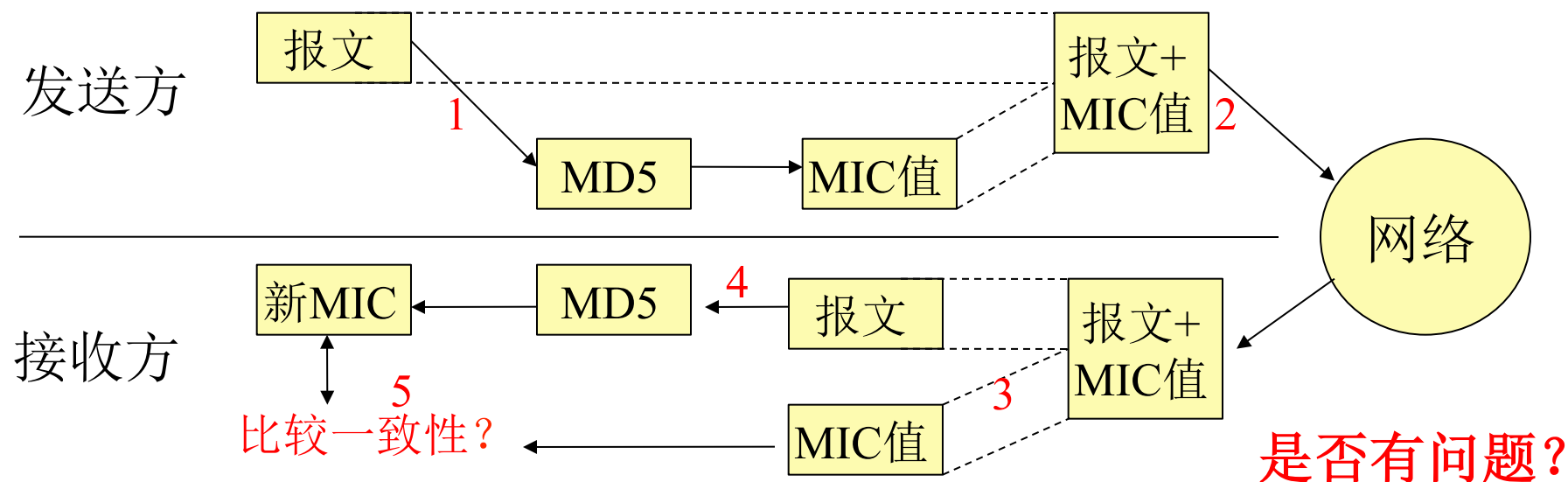
加密技术可用于提供网络安全中的内容保密服务。

内容完整性—防篡改

直接依赖**摘录技术**的特性（报文和摘录息息相关）。

工作过程：

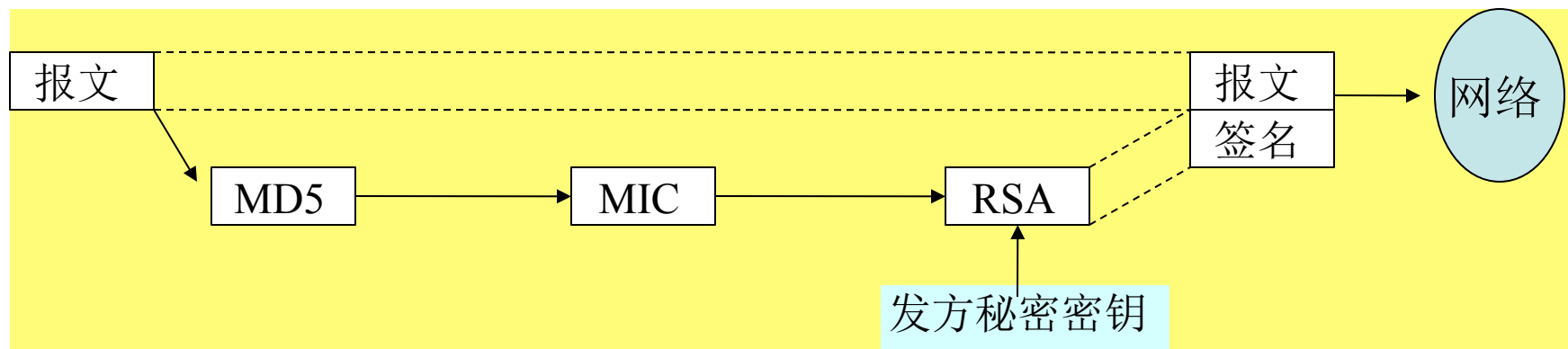
- 1 发送方利用摘录算法（如MD5）形成摘录值（报文完整性检查值—MIC值）；
- 2 报文连同MIC值一起传递给接收方；
- 3 接收方分隔报文和MIC值；
- 4 对报文执行相同的摘录算法，形成新的MIC值；
- 5 新MIC值和原MIC值比较，判断报文在传输过程中是否被修改。



实体鉴别：—防冒充（假冒）

★ 数据源鉴别—鉴别数据真实性，确实来自期望的发送方。

数字签名技术支持数据源的鉴别。



描述：形成的报文数字签名和报文内容及发方密钥密切相关；
收方利用发方的**公钥**处理签名，获得原始MIC值；
收方利用MD5对报文求MIC值；
如果新MIC值和原始MIC值一致，可认为报文确实来自期望的发送方，且在传输过程中内容未被篡改。

依据：只有发方才掌握发方的**私钥**。

展望

- 互联网面临的挑战
- 下一代互联网体系结构研究现状和发展趋势
- 两种技术路线
 - “演进性”路线，即在现有IPv4协议的互联网上不断“改良”和“完善”网络，最终平滑过渡到IPv6的互联网；
 - “革命性”路线，以美国FIND/GENI项目为代表，即重新设计新的互联网体系结构，满足未来互联网的发展需要。

考试安排

- 日期：2016年06月16日，星期四
- 时间：上午 9:00~11:00
- 地点：教六 – 402
- 形式：开卷

谢谢！