**计算机网络**

**一、网络技术基础**

1.网络分类：

（1）宽带城域网（MAN）：双环光纤传输；FDDI；（2）无线局域网（WLAN）；（3）无线自组网（Ad hoc）（自组织；对等；无线网络）；（4）无线传感网（WSN）：Ad hoc与传感器技术结合；（5）无线网状网（WMN）：用于扩大范围；对Wimax和WLAN的补充

2.操作系统

（1）Unix操作系统：小型机、C语言（第一版本由汇编语言编译）、部分开源；集中式、多用户，多任务，分时操作系统；贝尔公司开发；

I**BM—AIX SUN公司—Solaris HP—HP-UN**

（2）Linux操作系统：继承了Unix以网络为核心的设计，核心部分：内核；开源操作系统；版本很多；由不同组织管理维护；**不是Unix操作系统的变种**。

**Red Hat**

（3）Windows NT是微软公司开发的闭源系统；采用32位操作系统，可以提供全面的网络服务功能；**基于不对等结构**，分Windows NT Sever和Windows NT Workstation。

3.拓扑结构

（1）环型拓扑：传输延时确定；

（2）网状拓扑：广域网普遍使用；

4.数据报方式和虚拟电路方式

（1）数据报方式（分组存储转发）：**同一报文不同分组可以通过不同的传输路径；不同分组可能会出现乱序、重复和丢弃现象；分组均携带源地址和目的地址；延迟大，不适宜报文会话式；**

（2）虚电路方式：**传输之前在源节点和目的节点之间建立逻辑连接；每个结点可以与任意结点建立多条虚电路连接，不需要路由选择；一次通信所有分组通过虚电路顺序传输，分组不需要携带目的地址和源地址等信息；结点只进行纠错。**

5.网络体系结构

（1）ISO建立的OSI（开放系统互联）模型：

A.物理层（透明传输比特流）、数据链路层（MAC&LLC）、**网络层（选择路由IPSec）**、传输层（端到端服务）、会话层、表示层（加密/解密）、应用层（提供应用进程交换和远程操作）；

（2）TCP/IP模型：IETF制定的

A.主机-网络层、**互联层（IP/ARP/ICMP）、传输层（TCP\UDP）、**

**应用层**（FTP\HTTP\RIP\NFS\SMTP\Telnet\**SNMP\CIMP**\**PGP\S/MIME**\）

B.**开放式网络协议标准；与网络硬件无关；每一层服务上一层**

6.计算机网络：以能够相互**共享资源**方式互联起来的**自治**计算机系统集合。

7.**ARPANET**：Internet的始祖，是世界范围内的广域网，是世界上开发的第一个运营的封包交换网络（分组交换网络技术），是**美国国防部高级研究计划局**研究的网络。

**二、局域网技术**

1.局域网三要素：

（1）网络拓扑：**总线型、环型、星型；**

（2）传输介质：**双绞线、同轴电缆（最早）、光纤和无线信道；**

（3）介质访问：按照介质访问控制方式分为**共享介质**和**交换局域网**。其中：

共享介质（总线型局域网：利用CSMA/CD避免冲突；环型局域网：利用令牌环控制冲突）

2. IEEE 802

（1）对象：OSI的**物理层和数据链路层**。专门从事**局域网**的标准化工作。（不同局域网中，MAC和物理层可以不同，**LLC（介质访问控制层）必须相同**）

（2）分类：

802.3：定义CSMA/CD**总线型**介质访问MAC和物理层标准（**以太网标准**）；

802.4：定义令牌环网的协议标准；

802.11：无线局域网标准；

**802.15：无线个人区域网介质访问MAC和物理层标准；**

**802.16：宽带无线局域网。**

3.共享以太网

（1）概念：核心是集线器；ALOHA网络是基础；总线型局域网；核心技术：CSMA/CD；

（2）帧结构：

**间导码7B 帧前定界符1B|目的地址6B源地址6B类型2B|数据46-1500B校验位4B（CRC）**

（接收同步，不计帧头） （帧头；类型：网络层协议） （帧长64-1518B）

（3）以太网物理地址：长度48位，十六进制，两两一组，共6组；**前三组生产公司，后三组生产商分配流水号**，可分配地址2^47，第一位1则为组/广播；为0才可以分配给生产商。

4.高速局域网标准（MAC层与原标准兼容，仅定义物理层标准）

（1）802.3u：Fast Ethernet，百兆以太网；

（2）**802.3z**：Gigabit Ethernet，千兆以太网，定义多模光纤或屏蔽双绞线；

802.3ab：Gigabit Ethernet，千兆以太网，定义**单模光纤或非屏蔽双绞线**；

采用GMII分隔物理层和MAC层；与传统以太网的帧格式一致；

（3）802.3ae:10Gigabit Ethernet，万兆以太网，使用光纤传输，**只有全双工模式，不存在介质访问控制，传输距离不受冲突检测的限制。**

（4）802.3ba：40/100Gigabit Ethernet（40Gbps网络使用**波分复用技术**，100GPS物理接口类型）

5.**交换式局域网**

（1）概念：典型的是交换式以太网，**核心设备：以太网交换机**（专用/共享端口）；**可以在多个端口之间建立多个并发连接，实现多结点之间的并发连接，**

（2）帧转发方式：**直接交换**；**存储转发**；**改进直接交换**（接收一帧前64B，检测由主机进行）；

（3）**虚拟局域网（VLAN）**组网方式：**用交换机端口定义；MAC地址定义；基于网络层地址（IP）定义；基于广播组定义。**

6.无线局域网

（1）按物理层传输方式分类：**红外、直接序列扩频、跳频广播、微波**；

（2）红外无线局域网IR、跳频扩频FHSS（将频带划分为多个信道，使用2.5GHZ的ISM频段）、直接序列扩频DSSS（所有接受结果使用相同频段通信）、窄带微波无线局域网。

（3）802.11定义的两种访问方式：**无争用服务、争用服务**；MAC层采用CSMA/CA避免冲突；支持AP访问模式和漫游访问模式；802.11管理帧为**探测帧和认证帧**；采用层次结构模型；**MAC层主要功能是对无线环境的访问控制；物理层定义了红外、调频扩频与直接序列扩频的数据传输标准。**

（4）802.11协议族：

802.11a: 5HZ 54M

802.11b: 2.4HZ **11M**（跳频）

**802.11g: 2.4HZ 54M**

802.11n: 5G 100M

（5）网络结构为：端站（有无线网卡的用户结点）、接入点（AP）、接入控制器（AC在WLAN与外部网络之间充当网关作用）、AAA服务器（计费、认证、授权；**802.11认证有三种：基于IEEE 802.1x的认证、基于PPoE的认证和基于Web的认证**）

6. 1000BASE-SX:多模光纤 1000BASE-CX:屏蔽双绞线

1000BASE-LX:单模光纤 1000BASE-T:非屏蔽双绞线

100BASE-FX:单/多模光纤

7.不能够通信的原因：**不在一个虚拟子网中；不在一个子网中**。

8.总线局域网的特点：所有结点都通过网卡连接到作为公共介质的总线上，通常采用双绞线或同轴电缆作为传输介质；所有的结点都可以发送或接收数据，但在一段时间内只允许一个结点通过总线发送数据（即半双工形式）；当一个结点通过总线以“广播”方式数据时，其他结点只能以“收听”方式接收数据；由于总线作为公共传输介质被多结点共享，因此会出现冲突现象。

**三、Internet基础**

1.互联网构成：通信线路（基础设备）、**路由器**（主要设备，**主要功能：维护路由表信息；转发IP数据报；选择最佳路径**）、**主机**（信息资源和服务的载体）和**信息资源。IP协议是Internet中的主要协议。**

2.**Internet的接入方式**：

（1）电话线接入；

（2）ADSL接入：使用**电话线路，完成非对称数据用户线路**，ADSL调制解调器：具备网桥、路由器和调制解调的功能；

（3）HFC接入：有线电视网接入（混合光纤/同轴电缆），**非对称**数字用户线路；

（4）数据通信线路接入：（成本高）

3.IP协议

（1）定义：**IP数据报格式、对数据寻址和路由、数据报分片和重组、差错控制和处理**等。

（2）IP服务特点：**不可靠服务；面向无连接；尽最大努力投递；（一般不随意丢弃报文）**

（3）IP网络特点：**隐藏底层物理网络细节；不制定拓扑结构，不要求网络之间全部互联；在物理网络之间转发数据，信息可以跨网传输；公平对待互联网中每一个网络；使用同一的地址描述法。**

4.IP地址（A\B\C\D\E类地址）

（1）特殊IP地址：网络地址；广播地址（直接广播/有限广播：255.255.255.255）；**回送地址（127.0.0.0）**；本地地址（A:10.0.0.0/8;B:172.16.0.0/12;C:192.168.0.0/16）

（2）若要发送广播：源地址是本机，目的地址：网络号不变，主机号全为1.

5.地址解析协议ARP

（1）工作在**互联层**，能够实现IP到MAC的解析；

（2）工作原理：**以广播形式发送请求报文（ARP请求），单播响应**；

（3）通过**高速缓存技术避免大量请求报文出现，提高有效性**；拥有计时器的目的是**保证主机ARP表的正确性。**

6.**IP数据报格式**

（1）组成：报头区和数据区；

（2）数据报各字段及其功能：版本和协议类型；长度；服务类型；生存周期；头部校验和域（保证报头完整性，没有数据区校验字）；

（3）报头长度：32bit双字节为单位；总长度以8bit字节为单位。包含与分片和重组有关：**标识（原数据是谁）、标志（是否是最后一片）**和片偏移（顺序重组）

7.IP封装、**分片**（MTU:最大传输单元，一帧携带最多能携带的数据量。）**和重组**。

8. **IP数据报选项**

（1）目的：控制和测试；

（2）选项数据：

A.源路由：严格路由（严格按照路径转发）；松散路由（规定主要路由）；

B.记录路由：记录经过的所有路由IP；

C.时间戳

9.**差错与控制**

一个ICMP报文对应一个数据报

（1）**ICMP差错控制报文**：拥塞控制（源抑制报文）、路由控制（重定向报文）；

（2）**请求/应答对：回应请求与应答（用于测试目的主机或路由器的可达性）、时间戳请求与应答（同步时间）、掩码请求与应答；**

（3）ICMP特点：**不享受优先权和不享受特别的可靠性；报告伴随丢弃；报文包含IP数据报头和数据前64比特数据**。

（4）当路由器收到IP数据报，对IP数据报进行检测，当对其首部进行校验后发现数据报存在错误时，将抛弃该数据报。

10.**路由器与选择**

（1）特殊路由：默认路由、待定主机路由（制定到达的主机）

（2）**RIP协议**（路由器信息协议）：采用**V-D算法**（距离-矢量算法），简单、中小型网络、多路径、动态IP互联网环境；距离按跳数计算；慢收敛（解决：限制路径最大距离；水平分割对策；保持策略；带触发刷新的毒性逆转对策）

（3）**OSPF协议：**采用**L-S算法**（链路-状态算法），大型网络、多路径、动态IP互联网环境；每个路由都有一个LSA，最终获得一个LSDB（链路状态数据图），收敛比V-D算法快。

11.IP组播技术：

（1）特点：使用组地址（D类地址）；动态组播地址，成员也是动态；不仅通过IP层，还与要底层硬件支持功能。

（2）相关协议：**组播管理协议（IGMP,CGMP）、组播路由协议**。

IGMP：Internet制定的，一方面主机通过本地路由器主动加入；一方面ICMP协议路由器会周期查询。组播路由由：**源地址、组地址、入接口和出接口组成**（前三个进行匹配）。

12. IPv6

（1）地址：128位（IPv4:32位）**；送回地址（0:0:0:0:0:0:0:1）；**

（2）数据报格式：一个基本头（固定40B）、多个扩展头和一个高层协议数据单元组成。

（3）扩展头种类：**逐跳选项报头**；目的选项报头；**路由报头**（强制数据报经过指定路由）；分片头；

13.TCP与UDP：

（1）TCP**:面向对象，可靠，全双工。**（使用窗口机制进行流量控制；RTT算法进行数据丢失与重发；**连接端口用12位二进制表示**）

（2）UDP:**非面向连接，不可靠，高效率。（应用程序提供可靠性保障**）

14.NAT：内外网地址翻译。分类：静态NAT、动态NAT、网络地址端口转换**NAPT**（多个内网主机共享一个全局IP地址，同时访问外部网络）

15.MTU：1500字节；一般IP首部为20字节，UDP首部为8字节，数据的净荷部分预留是1472字节；**如果超出1472字节，就会出现分片现象。**

**四、Internet基本服务**

1.应用进程响应并发请求分类：

（1）**重复服务器**：“先进先出”原则；

（2）**并发服务器**：每来一条请求，创建一个子进程。

2.对等计算机模型（P2P）基本结构：

（1）**集中式**（Napster，服务器通常**只存储目录**和**索引信息**）；（2）**分布式非结构化**（无中心节点；**随机图**；支持复杂查询；模糊查询；**利用TTL机制控制泛洪；Gnutella**）；（3）**分布式结构化**（无中心节点；采用分布式散列表**DHT**；支持精确关键字匹配查询；可扩展；维护复杂；**pastry; tapestry; chord; CAN**）；（4）**混合式结构**（**索引结点**维护**搜索结点**在**搜索用户**结点；skype; BT; pplive）

3.域名解析方式：

（1）分类：**递归解析**（一次完成）、**反复解析**（分层多次解析）；

（2）每一个域名服务器至少知道根服务器的**IP地址**及其父节点服务器的**IP服务地址**，才能解析。（**本地域名服务器IP地址**）

（3）提高域名解析的效率：**解析从本地域名服务器开始；在域名服务器使用高速缓存技术；在主机上采用高速缓冲技术。**

4.域名对象类型：

A—主机；MX—邮件交换；PTR—指针；CNAME—别名；SOA—授权开始；

**HINFO—描述主机信息**

5.远程登录中，网络虚拟终端利用**NVT格式**将不同的用户本地终端统一起来。

6.FTP服务

（1）C/S模型，利用TCP建立双向连接（一个控制连接/一个数据连接）；

（2）建立联系方式：**主动模式**（服务器主动，使用**PORT**命令将端口发送给服务器）；**被动模式**（服务器被动，向服务器发送**PASV**命令）

（3）FTP文件格式传输方式：文本文件传输（ASCII）；二进制文件传输（BINARY，不对文件格式进行任何变化，按照原始文件相同的位序以连续比特流方式进行传输）；

（4）FTP口令描述：delete—删除远程主机上的文件命令；**pwd—显示远程主机的当前工作目录；**

7.电子邮件系统

（1）**SMTP**：服务器之间的传递；主要目的是实现**发送邮件**的。

（2）POP3/IMAP：向邮件服务器进行读取（**认证阶段、事务处理、更新阶段Quit**）；

（3）电子邮件报文格式：RFC822、MIME.

（4）命令：**PASS—用户邮件口令（认证）；STAT—查询报文总数和长度； REST—复位，删除标记，中止当前操作；NOOP—无操作（事务处理）**

8.Web服务

（1）HTML：页面规范，**解释单元**，能够对请求和返回进行页面翻译，显示内容；

（2）HTTP：客户机和服务器之间的传输协议，建立在TCP连接上，面向对象协议，精确定义了请求/相应报文；

（3）URL：页面地址，统一资源定位器；

（4）安全性：**SSL协议**（工作在传输层协议；位于TCP/IP协议与各类应用层协议之间）（浏览器安全性）（防止第三方偷看内容；防止第三方篡改）；CA证书（Web服务器）（证明自己）

（5）浏览器组成：**控制单元**（解释键盘/鼠标输入命令）、**客户单元、解释单元**组成。Web服务器不但需要保存大量的Web页面，而且需要接受和处理浏览器的请求，实现HTTP服务器功能。**Web服务器不具备编辑Web页面的功能。**

9.安全性：

（1）如何保护自己的计算机：浏览器将Internet世界划分成几个区域；

（2）如何验证站点真实性：利用Web站点传来的证书；

（3）如何避免他人假冒自己：用户可以在CA安全认证中心申请自己的证书，放在浏览器中；

（4）在与Web交互敏感信息时如何避免第三方篡改或偷看：使用安全套接层技术SSL技术；

（5）保证传输机密性：将Web站点放入可信站点区可保证信息传输的机密性；

（6）防止病毒传播：使用SSL技术。

9.网络蠕虫：独立、通过漏洞传播、早期利用电子邮件传播、自我复制和主动传播；**木马是没有复制能力的。**

**五、新型网络应用**

1.即时通信（IM）

（1）由IMPP工作组提出；IETF批准成为正式RFC文件；**有RFC2778文件描述功能**；该文件未提出即使通信系统必须使用同一标准。

（2）模式：客户机/服务器；客户机/客户机

2. QQ

（1）客户机的两种聊天方式：**UDP主/TCP辅；服务器中转（无法直接通信）；**

（2）采用自己私有的即时通信协议；

（3）每次登陆时客户机会获得一个来自服务器的会话密钥。

3.即时通信协议（基于SIP的SIMPLE；基于JABBER的XMPP）

（1）**SIP：工作在应用层**；**IEFT提出**；可在TCP/UDP上传输；支持多种信息类型（文件、视频、图像）；用于创建、修改和释放一个或多个用户会话；**分类**（用户代理、代理服务器、重定服务器（用于规划SIP路径服务器，可与其他服务器共存一个设备中）、注册服务器）；**SIP消息组成**（起始行、消息头、一个标志消息头的空行、消息体）；SIP定义的**6种请求消息**（INVITE：邀请用户/服务器参加一个会话；ACK；OPTIONS:获取服务器相关能力；BYE:终止一次会话；CANCLE:取消挂起呼叫；REGISTER）；**SIP消息通常可分为2类**，**从客户机到服务器的请求消息**和**从服务器到客户机的响应消息**。

（2）SIMPLE：以SIP为基础，不需建立会话，支持多媒体会话；IEFT的SIMPEL工作组制定；IM消息以message命令为载体传输，**每条IM由单独message命令传输，彼此独立**。

（3）**XMPP：工作在应用层;基于JABBER协议**；由IEFT制定；**由4个RFC文档组成；设计上延续E-mail系统**；包含用户客户端、XMPP服务器、XMPP协议网管；**XML是其核心**，统一选址方案，**实体地址叫做JID**。

（4）基本服务：**呈现服务和即时消息服务。**

4.网络文件共享

（1）NFS（网络文件系统）：Linux\Windows上均可使用；与主机操作系统无关；**采用C/S结构**；若想远程计算B的某一个文件系统：”mount:B:/usr/lib(远程主机目录)/usr/lib(本机目录)”

（2）NFS服务器共享出来的文件或目录都记录在/etc/exports文件中。

5.Windows LAN文件共享：**Windows2000以前的系统使用NetBIOS协议；以后使用CIFS协议**

6.P2P文件共享

（1）P2P:起源于Napster；BT（中心服务器tracker存放用户信息；种子文件：**.torrent**，包含存储用户信息和共享文件的信息）；**源于MIT开源系统**；加入DHT以实现无tracker服务器的文本传输；**基于“六度分隔理论”、“世界最小理论假设”、“瓦斯特领导理论”。**

（2）Maze：支持即时通信；参考Kerberos机制；在线资源搜索和文件目录视图；支持多点下载和断点续传；基于积点的资源交易体系；有种子机制；分布式认证机制（类似于信用卡机制）；类似URL表示文件位置；混合型P2P系统；**包括集中式的用户管理服务器（注册、登录）、目录收集服务器、检索服务器、心跳服务器和种子服务器。**

（3）**P2P不支持种子机制**；BT系统不支持积点机制；P2P可以实现用户之间直接传输；BT后期系统能够实现无Tracker服务器的文件传输；**P2P与BT相互不兼容。**

5.IPTV

（1）业务种类：近式点播（NVOD，多个视频流依次间隔发送同样的内容）、真实点播电视（TVOD）和交互式点播（IVOD）;

（2）**媒体内容分发（MCDN）技术组成：**

A.内容发布：借助相关技术，将内容发布或投递到距离用户最近的远程服务点；

B.内容路由：网络负载均衡技术，重定向路由器以请求最近内容源响应；

C.内容交换：根据内容可用性、服务器可用性等，利用应用层交换技术，智能平衡负载流量；

D.性能管理：保证网络处于最佳状态，测量内容发布的端到端性能。

6.VOIP（基于IP网络的语音传输技术）：

（1）组成：终端设备、**网关（号码查询、建立通信、信号调制、压缩和解压缩、路由寻址）、多点控制单元（多终端）**、**网守（**中央控制实体，负责用户注册和管理；消息控制中心；确定网关地址；计费管理；留存呼叫详细记录）

（2）Skype：**利用VOIP和P2P技术；混合式网络结构；AES算法作为密钥，密钥长度256bit；加密保存好友列表；支持免费多方通信；采用iLBS和iSAC编码技术；系统中SN是动态生成的；可以进行NAT穿越。**

7.搜索引擎组成：**搜索器、检索器、索引器、用户接口。**

8**.ICQ、AOL采用OSCAR通信协议。**

9.网管模型：（一般采用网络管理者-网管代理模型，管理者实际是运行在计算机操作系统上的一组应用程序，代理位于被管理的设备内部，一个管理者可以和多个代理之间进行信息交换）

（1）**组织模型描述网管系统的组成部分；**

（2）**信息模型描述网管系统的对象命名；**

（3）**通信模型描述网管系统的管理协议；**

**六、网络管理与网络安全**

1.网络管理

（1）管理对象：物理介质、计算机设备和网络互连设备（硬件资源）；操作系统、应用软件和通信软件（软件资源）；

（2）目标：用户及运营商对网络的有效性、可靠性、开放性、综合性、安全性和经济性。（3）模型：**集中式管理和分布式管理（时效好）**

2.网络管理功能

（1）**配置管理**：包含两阶段：网络初次运行的初始配置管理阶段和网络正常运行的工作配置管理阶段；负责网络建设、业务展开和配置维护，达到网络性能最优；包括：设置系统中有关路由操作的参数、被管理对象的名字管理、初始化或关闭被管对象、根据要求收集系统当前状态的有关信息、获取系统重要变化信息、更改系统配置、**生成网络拓扑**。

（2）故障管理：**发现和排除故障；维护和监测错误日志；接收错误响应；跟踪辨别错误**；

（3）**性能管理**：计算机网络性能；**收集统计信息**；监控网络使用状况；维护网络使用状况；

（4）计费管理

（5）安全管理：对授权机制、访问控制、加密和解密关键字的管理。

3.网络管理协议：

（1）CMIS和**CMIP：**由**IOS**制定；**所用功能都要映射到应用层**；采用报告机制（**委托管理制）**；实施复杂且花费高；

（2）**SNMP**：**工作在应用层；IETF制定**；遵循ISO的管理模型，可以应用于**TCP/IP环境下**；**收集数据的方式有轮询**（不断收集，按顺序存储在**MIB**中，时效低）**和基于中断**（时效高，需要转发大量信息，消耗管理设备资源时间，改进：trap）两种；SNMP第一版安全性差；第二版提供验证、加密和时间同步机制，在安全性和更有效的传递管理信息方面加以改进；

4.信息安全等级

（1）美国制定（DOD5200.28-STD）：

**非安全保护类：**D（客户机系统）；**自主保护类：**C1、C2（存取控制，以用户为单位）

**强制性安全保护类：B1（标记安全保护）B2（结构化安全保护）B3（安全域机制保护）**A1

（2）中国制定：自主保护级、指导保护级、监督保护级、强制保护级、专控保护级

5.OSI安全框架（X.800）中安全攻击类型

（1）被动攻击：不更改信息，**窃听检测，内容泄漏，流量分析**（重在预防）；

（2）主动攻击：更改信息，**消息篡改，DOS攻击，消息重放，拒绝，伪装**（重在检测）；

（3）服务攻击：针对特定服务攻击；**邮件炸弹；端口攻击；分布式拒绝服务攻击**；

（4）非服务攻击：基于网络层或底层协议漏洞攻击；**源路由攻击，地址欺骗，NetXray攻击**。

6.对称密码

（1）DES：**分组长度64位，分组置换，密钥长度56位；美国NIST采纳；**

（2）三重DES：多个密钥对DES进行三次加密；

（3）高级加密（AES）：**分组长度128，分组置换，密钥长度128,192或256位，性能不低三重DES；**

（4）Blowfish算法：**可变长度密钥，分组长度64；**

（5）**RC5：分组长度和密钥长度均变。**

7.非对称密钥（公钥密码）

（1）RSA算法：发明者姓名命名；分组密码；**加密强度取决于密钥长度（概率加密方法）；质数值越大，破解越难；**

（2）ElGamal算法：公钥密码体制和椭圆曲线加密体系；基于离散对数；常用于数字签名；**密文是明文的两倍。**

（3）背包加密算法：目前一次背包不安全；

8.密钥的验证：认证中心（CA），验证实体身份；产生证书，将公钥和身份绑定；证书由CA进行数字签名；**认证后公钥的发布不受限制；保管用户的公钥**；

9.认证技术

（1）消息认证的方法：**认证消息来源；认证信息的完整性；认证信息的序号和时间。**

（2）认证模式：单向和双向；

（3）认证函数：信息加密函数；信息认证码；散列函数（Hush，消息通过散列函数生成摘要。MD5同步处理可得到128位摘要）

（4）数字签名：防止抵赖

（5）身份认证：口令认证、持证认证和生物识别；协议有Kerberos（对称密钥；TCP/IP环境下；美国麻省理工）、X.509（公钥体制；CCITT制定）

10.安全电子邮件（**应用层**）

（1）PGP：数字签名采用DSS/SHA或RSA/SHA；压缩：ZIP；兼容：64-BASE

（2）**S/MIME：支持数据加密和数字签名；**

11.**IPSEC：网络层**安全协议；将互联层改造为逻辑连接的层；主要有**身份认证头（AH）**协议（对于发送方提供源身份认证和数据完整性，没有提供秘密性）和**封装安全负载（ESP）**协议（**提供源身份认证和数据完整性，提供了秘密性**）；源主机与网络主机进行握手并建立网络逻辑连接，该逻辑通道成为安全协议（SA）；**SA定义的逻辑连接是单工的，三元组**。

12.防火墙分类：

（1）包过滤路由器：根据IP数据包进行处理，决定转发或丢弃；

（2）应用级网关：代理服务器；

（3）**电路级网关：不允许端到端直接TCP连接；**

（4）堡垒主机。

13.公钥加密和数字签名技术建立的安全基础设施为：PKI

14.密钥分发中心（KDI）：**是一个独立的可信的服务器；对称密钥；知道每个用户的密文，可一次性方法密钥，与客户通过密文传输。**

15.安全电子交易协议SET是一种应用于Internet环境下，以信用卡为基础的安全电子交付协议，它给出了一套电子交易的过程规范。通过SET协议可以实现电子商务交易中的加密、认证、密钥管理机制等，保证了在Internet上使用信用卡进行电子购物的安全。主要目的是解决信用卡电子付款的安全保障性问题，这包括：保证信息的机密性、保证信息安全传输、不被窃听，只有收件人才能得到和解密信息。（**常用于电子商务应用中；防止交易数据被篡改；需要认证中心的支持；验证交易双方的身份）**