**概念：**物联网是一个基于互联网、传统电信网等信息载体，让所有能被独立寻址的普通物理对象实现互联互通的网络。普通对象设备化，自治终端互联化和普适服务智能化是其三个重要特征。

**核心技术**：感知识别层、网络构建层、管理服务层、综合应用层

1.感知识别层：是物联网的核心技术之一，是联系物理世界和信息世界的纽带。既包括射频识别（RFID）、无线传感器等信息自动生成设备，也包括各种智能电子产品用来人工生成信息。

2.网络构建层：主要作用是把感知识别层的设备接入互联网，供上层服务使用。

3.管理服务层：在高性能计算和海量存储技术的支撑下，管理服务层将大规模数据高效可靠地组织起来，为上层行业应用提供智能的支撑平台。

4.综合应用层：实现人与物、物与物之间的互联。

**主要特点：**联网终端规模化；感知识别普适化；异构设备互联化；管理处理智能化；应用服务链条化。

**自动识别技术：**光符号识别技术；语音识别技术；生物计量识别技术（虹膜识别技术、指纹识别技术）；IC卡技术；条形码技术；射频识别技术

**射频识别技术**RFID：利用射频信号通过空间耦合实现无接触信息传递并通过所传递的信息达到自动识别的目的。优点：电子标签和阅读器无需接触便可完成识别；通过芯片提供存储在其中的巨大无形信息。

**RFID系统的组件：**传送器、接收器、微处理器（阅读器）；天线；标签。

**RFID标签的优点**：体积小且形状多样；环境适应性强；可重复使用；穿透性强；数据安全性。

**标签的分类：**被动式标签、主动式标签、半主动式标签

**传感器**：能够感受规定的被测量并按照一定的规律转换为可用输出信号的器件和装置。

**信息技术的三大支柱**：传感器、通信技术、计算机技术

**无线传感器节点的组成**：传感器部件、微型处理器、无线通信芯片、供能装置

**节点操作系统：**极其微型化

**ETX**的计算：ETX传输次数=1/d1+1/d2

**路由协议CTP**（收集树协议）：数据收集协议，将多个传感器节点上的数据收集到汇聚节点上；数据分发协议，将汇聚节点上的数据分发到网络中的每一个传感器节点

**定位系统：**卫星定位系统（GPS卫星定位系统、北斗卫星导航系统）；蜂窝基站定位系统；室内精确定位系统；WiFi基站定位系统

**GPS**（全球定位系统）**的组成**：宇宙空间部分；地面监控部分；用户设备部分

**蜂窝基站定位**：最简单的定位方法是COO定位，它是一种单基站定位方法；

ToA和TDoA测量法都至少需要三个基站才能进行定位；除此之外，还有利用信号强弱定位的方法（RSS定位）

ToA：基于距离的定位 TDoA：基于距离差的定位 RSS：基于信号特征的定位

**第二代通信技术**（2G）：目前仍在使用的2G网络是全球移动通信系统（GSM）和码分多址访问系统（CDMA）

我国采用的3G标准是TD-SCDMA（时分-同步码分多址）、W-CDMA（宽带码分多址）

DMA2000

**低功耗广域网**：远距离、低功耗、低带宽的协议；主要代表：远距离通信（LoRa）、窄带物联网（NB-loT）；区别：NB-loT技术可以和现有的移动通信基站相结合。

**无线网络的基本组成元素**：无线网络用户、无线连接（传输数据的通路）、基站

无线用户除了通过基站接入网络的中心结构模式外，还可以通过无中心模式形成自组织网络

**无线宽带网络的难点**：信号强度衰减、非视线传输（非视线环境下，由于阻挡物的存在，无线电信号可能会被吸收或者迅速衰减）、同频信号干扰、隐藏终端问题

隐藏终端：（画图）用户A-基站C-用户B 用户可以与基站访问 用户间不能相互访问

**IEEE 802.11协议：**使用带冲突避免的的载波监听多路访问（CSMA/CA）协议。CSMA是指用户在发送数据之前先监听信道，如果信道被占用则不发送数据。CSMA/CA是指即使侦听到信道为空，也为了避免冲突而等待一小段随机时间后再发送数据帧。

以太网使用带冲突检测的载波监听多路访问（CSMA/CD）协议。

**CSMA/CD协议的原理**：当用户监听到信道为空时立即发送数据。并且在发送数据的同时监听信道，如果此时它检测到和其他用户的数据传输信号发生了冲突，则立刻停止传输并随机等待一小段时间后重新传输。

**820.11协议采用CSMA/CA的原因：**冲突侦测需要全双工（发送数据的同时也可以接收数据）的信道。而对于无线传输信号来说往往发送信号的能量远高于接收到的信号的能量，建立能侦测的硬件代价是很高的。即使无线信道是全双工的，但是由于无线信号衰弱特性和隐藏终端问题，硬件还是不能侦听到全部可能的冲突。

**蓝牙：**蓝牙技术成为IEEE 802.15.1标准。蓝牙技术的物理层采用跳频扩频结合的调制技术，频段范围是2.402~2.480GHz（ZigBee和WiFi同在2.4附近），通信速率一般能达到1Mbps左右。在蓝牙通信中，蓝牙设备分为主设备和从设备两种可能角色。同一蓝牙设备可以在这两种角色之间转换。

ZigBee又称IEEE 802.15.4标准

**大数据：**大数据是指其大小超过了常规数据库工具获取、储存和分析能力的数据集。

从数据处理角度来看，大数据是只指用传统数据处理手段无法有效处理的数据集。

大数据的特征：大量、多样、高速、价值

**意义：**数据以意想不到的方式在收集；数据以极简的方式在分析处理；数据以真实又诡异的方式在讲故事（数据是真实的，数据却不会自己得出结论；不谨慎的分析解读会引向不正确的结论）；数据是一种重要的资源

**网络化存储体系结构：**存储（DAS）、网络附加存储（NAS）、存储区域网络（SAN）

**云计算：**为整个计算机行业提供了三个层次的基础服务

1.设施即服务：提供基础设施资源。包括虚拟化的计算资源、存储资源、网络资源和安全保障等。（亚马逊的EC2、阿里云）

2.平台即服务：服务应用的开发者。开发者通过这个平台开发、运行和管理应用程序时，无需处理诸如配置开发环境、测试环境等麻烦问题。（微软的Azure、App Servicr、谷歌的App Engine）

3.软件即服务：服务终端用户的应用程序。不操控硬件、网络、操作系统等基础资源，也不关心应用是如何开发调试的。（云盘、文档在线编辑<谷歌的Docs和Evernote>）

**虚拟化：**虚拟化是云计算的关键技术，它把刚性的物理硬件化成柔性的虚拟资源。

功能：把一台物理机拆分成多台虚拟机；把多台物理机组合成一台虚拟机；动态配置虚拟机的资源以及迁移虚拟机。

**网络信息安全的一般性指标**：

可靠性：系能够在规定的条件下和规定的时间内完成规定功能的特性

可用性：系统服务可以被授权实体访问并按需求使用的特性

保密性：信息只能被授权用户使用、不被泄露的特性

完整性：未经授权下不能改变信息的特性

不可抵赖性：信息交互过程中所有参与者都不可能否认或者抵赖曾经完成的操作和承诺的特性

可控性：对信息传播及内容控制的特性

**隐私权**：个人信息、身体、财产、自我决定等

**RFID的主要安全隐患：**窃听、中间人攻击、欺骗克隆重放、物理破解、篡改信息（数据篡改是一种非授权的修改或者是擦除RFID标签上的数据。攻击者可以让物品所附着的标签传达他们想要的信息）、拒绝服务攻击（通过发送不完整的交互请求来消耗系统资源）、RFID病毒、其他（电子破坏、屏蔽干扰、拆除）

**物理安全机制**：“灭活”法拉第网罩、主动干扰、阻止标签

灭活：杀死标签，使标签丧失功能，不能响应攻击者的扫描

法拉第网罩：屏蔽电磁波，阻止标签被扫描

主动干扰：用户主动广播无线信号阻止或破坏RFID阅读器的读取

阻止标签：通过特殊的标签碰撞算法阻止非授权阅读器读取那些阻止标签预定保护的标签

**位置隐私**：是用户对自己位置信息的掌控能力。自由决定是否发布自己的位置信息，将信息发布给谁，通过何种方式发布，以及发布的位置信息有多详细。

思考：位置信息与个人隐私是否矛盾

**保护隐私的手段**：制度约束，通过法律和规章制度规范物联网中对位置信息的使用；隐私方针，允许用户根据自己的需要来制定相应的位置隐私方针，以此指导移动设备和服务供应商之间的交互；身份匿名，将位置信息中的真实身份信息替换为一个匿名的代号，以此来避免攻击者将位置信息与用户的真实身份挂钩；数据混淆，对位置信息混淆，避免让攻击者得知用户的精确位置。（模糊范围、声东击西、含糊其辞）



**智能交通系统（ITS）：**物联网技术的发展为智能交通提供了更透彻的感知，道路基础设施中传感器和车载传感设备能够实时监控交通流量和车辆状态信息，监测数据通过泛在移动通信网络传至管理中心。物联网技术为智能交通提供了更深入的智能化。