目录

[计算机网络概述 3](#_Toc129953549)

[了解计算机网络的发展历史； 3](#_Toc129953550)

[熟悉计算机网络的分类和应用； 3](#_Toc129953551)

[了解计算机网络发展的新技术； 4](#_Toc129953552)

[掌握计算机网络的定义和功能； 6](#_Toc129953553)

[掌握计算机网络的组成与拓扑结构。 6](#_Toc129953554)

[数据通信基础 8](#_Toc129953555)

[了解数据通信系统中的基本概念； 8](#_Toc129953556)

[掌握电路交换、报文交换和分组交换 3 种数据交换技术； 10](#_Toc129953557)

[掌握数据通信系统模型的基本组成； 12](#_Toc129953558)

[掌握奇偶校验码和循环冗余码两种差错控制技术； 12](#_Toc129953559)

[掌握并行传输与串行传输，单工、半双工和全双工的数据通信方式； 13](#_Toc129953560)

[掌握数据传输技术、数据传输同步方式和数据编码技术； 14](#_Toc129953561)

[熟悉信道复用技术。 17](#_Toc129953562)

[网络体系结构 19](#_Toc129953563)

[了解网络体系结构的定义及分类，熟悉网络体系结构相关的概念； 19](#_Toc129953564)

[掌握 OSI 参考模型结构、各个层次的功能以及报文封装格式； 20](#_Toc129953565)

[掌握 TCP/IP 参考模型结构、各个层次的功能以及报文封装格式。 25](#_Toc129953566)

[TCP/IP 协议 28](#_Toc129953567)

[了解 UDP 的特点、端口分配和数据报格式； 28](#_Toc129953568)

[掌握 TCP 的特点、端口分配和报文格式； 28](#_Toc129953569)

[了解地址解析协议和网际控制报文协议ICMP; 28](#_Toc129953570)

[掌握 TCP 传输连接的建立和释放过程； 28](#_Toc129953571)

[掌握 IPv4 地址的结构和分类； 28](#_Toc129953572)

[理解子网掩码的概念,掌握子网划分的方法； 28](#_Toc129953573)

[了解 IPv6地址的结构和特点。 28](#_Toc129953574)

[局域网技术 28](#_Toc129953575)

[了解局域网的特征、体系结构、802 标准和组网模式； 28](#_Toc129953576)

[掌握局域网的介质访问控制方法； 28](#_Toc129953577)

[掌握以太网技及快速以太网技术； 28](#_Toc129953578)

[掌握虚拟局域网； 28](#_Toc129953579)

[了解无线局域网技术。 28](#_Toc129953580)

[网络互联技术 29](#_Toc129953581)

[了解计算机网络互连的基本概念； 29](#_Toc129953582)

[了解常用网络互连介质的特性和用途； 29](#_Toc129953583)

[掌握双绞线的制作与测试方法； 29](#_Toc129953584)

[掌握各层次网络互连设备的作用、特点与用途； 29](#_Toc129953585)

[了解常用路由协议 RIP、OSPF、BGP的工作原理和应用。 29](#_Toc129953586)

[网络安全 29](#_Toc129953587)

[了解网络安全的概念、网络面临的威胁以网络安全的内容； 29](#_Toc129953588)

[了解数据加密技术、数字签名技术和身份认证技术； 29](#_Toc129953589)

[了解防火墙技术； 29](#_Toc129953590)

[了解计算机防病毒技术。 29](#_Toc129953591)

# 计算机网络概述

## 了解计算机网络的发展历史；

四个阶段：

面向终端的计算机网络

以通信子网为中心的计算机网络

标准化网络

以Interent为中心的新一代网络

## 熟悉计算机网络的分类和应用；

1. 根据网络覆盖范围的大小分类

局域网（LAN）、城域网（MAN）、广域网（WAN）

特点：局域网数据传输率快，传输时延低且误码率低，组网方便、使用灵活，是目前计算机网络中最活跃的分支。但局域网仅工作在有限的地理范围内，采用单一的传输介质。

城域网所采用的技术基本上与局域网相类似，只是规模上更大一些。城域网作用范围为一个城市，地理范围为5 km～10 km，传输速率在1 Mbps以上。城域网目前多采用光纤或微波作为通信介质。

广域网通常跨接很大的地理范围，可以是一个地区、一个省、一个国家甚至全球，地理范围一般在100 km以上，传输速率比局域网低得多。

1. 根据网络传输介质的不同分类

有线网和无线网

1. 根据网络传输技术的不同分类

广播式网络和点对点网络

## 了解计算机网络发展的新技术；

1. **物联网**

物联网是利用射频识别系统、传感器、全球定位系统（GPS）、激光扫描器等信息传感设备，按约定的协议，把任何物体与互联网相连接，进行信息交换和通信，以实现对物体的智能化识别、定位、跟踪、监控和管理的一种网络。

物联网体系结构：感知层、网络层和应用层3个层次；

感知层。感知层利用RFID、传感器、摄像头、全球定位系统等传感技术和设备，随时随地获取物体的属性信息并传输给网络层。

网络层。网络层通过各种网络，将物体的信息实时、准确地传递给应用层。

应用层。应用层有一个信息处理中心，用来处理从感知层得到的信息，以实现物体的智能化识别、定位、跟踪、监控和管理等实际应用。

物联网的3层结构体现了物联网的基本特征，即全面感知、可靠传递和智能处理；

物联网的分类：物联网可分为私有物联网、公有物联网、社区物联网和混合物联网4种；

物联网的应用领域：家居、医疗、物流、交通、金融、工业到农业；

**2.5G**

5G的优点

1.用户体验：具有更高速率、更大带宽的5G能够满足消费者对更高网络体验的需求。“快”是5G带给大众用户最直观的感受。

2.行业应用：5G具有更高的可靠性、更低的时延，能够满足智能制造、自动驾驶等行业应用的特定需求，拓宽融合产业的发展空间，支撑经济社会创新发展。

3.发展趋势：5G已于2019年在我国正式商用，且在持续高速发展，大有取代4G、占据行业主导地位之势。

5G的关键技术：大规模天线阵列、超密集组网、新型多址、全频谱接入和新型网络架构等关键技术。

5G的应用场景：智慧城市的建设、自动驾驶的实现，还是远程医疗、远程教育、远程办公的进一步发展，抑或是VR、AR、云游戏等娱乐方式的颠覆。

**3.三网融合**

实现有线电视网络、电信网络和计算机网络三者之间的融合；

三网融合的优点：

1. 信息服务将由单一业务转向文字、语音、数据、图像、视频等多媒体综合业务。
2. 三网融合可极大地减少基础建设投入，并简化网络管理，降低维护成本；
3. 三网融合将使网络从各自独立的专业网络向综合性网络转变，网络性能得以提升，资源利用水平进一步提高。
4. 三网融合是业务的整合，它不仅继承了原有的语音、数据和视频业务，而且通过网络的整合，衍生出了更加丰富的增值业务类型，如图文电视、VoIP、视频邮件和网络游戏等，极大地拓展了业务范围。
5. 三网融合打破了电信运营商和广电运营商在视频传输领域的恶性竞争状态，未来看电视、上网、打电话资费可能打包下调。

## 掌握计算机网络的定义和功能；

1. 数据通信
2. 资源共享

1.硬件资源

2.软件资源

3.信息资源

3. 提高系统可靠性

4. 均衡负荷与分布式处理

## 掌握计算机网络的组成与拓扑结构。

从逻辑功能上分为两个子网：资源子网和通信子网；

1. 资源子网负责全网的数据处理业务，为用户提供各种网络资源和网络服务，资源子网由主机、终端、各种软件资源与信息资源组成；
2. 通信子网承担全网的数据传输、转发、加工、转换等通信处理工作，一般由通信控制机、通信线路和其他通信设备组成；

常见的网络拓扑结构有总线型、星型、环型、树型和网状型；

**小结：**

计算机网络是现代通信技术与计算机技术紧密结合的产物，它的应用已经渗透到各个领域，对人类社会的进步做出了巨大贡献。数据通信和资源共享是计算机网络最基本的功能。

网络拓扑结构是一个很重要的基本概念，不同的拓扑结构具有不同的特点，对网络的系统设计、功能、可靠性等方面都有着重要的影响。

计算机网络分类的方法很多，通常按照网络覆盖范围的大小可分为局域网、城域网、广域网；按照网络的传输介质不同可分为有线网和无线网；按照网络的传输技术不同可分为广播式网络和点对点网络。

随着物联网、5G、三网融合等计算机网络新技术的不断发展，计算机网络的功能和提供的服务将会不断增加。

# 数据通信基础

## 了解数据通信系统中的基本概念；

信息：一个抽象的概念，可以理解为消息中所包含的有意义的内容

数据：对客观事物的性质状态以及相互关系等进行记载的符号及其组合；

信号：信息在传输通道中传播的合适的载体，称之为信号，通常以电磁或光的形式存在，并利用电压、电流、频率、相位等物理量的变化来表示信息；

一个完整的数据通信系统一般由信源、信号变换器、通信信道、信宿等构成

信源就是信息的产生和发送端，是发出待传送信息的人或设备。信宿就是信息的接收端，是接收所传送信息的人或设备。

通信信道是传送信号的一条通路，由传输线路和传输设备组成。同一个传输介质上可以同时存在多条信号通路；

信号变换器的作用是将信源发出的数据变换成适合在信道上传输的信号，或将信道上传来的信号变换成可供信宿接收的数据。

信号在传输过程中受到的干扰称为噪声。

描述数据通信系统数据传输速率的大小和传输质量的好坏，往往需要运用信道带宽、比特率、波特率、信道容量和误码率等技术指标；

信道带宽是指信道中传输的信号在不失真的情况下所占用的频率范围，即传输信号的最高频率与最低频率之差。例如，若某通信线路可以不失真地传送2 MHz～10 MHz的信号，则该通信线路的信道带宽为8 MHz。

波特率又称作波形速率或调制速率。它是指数据传输过程中，在线路上每秒钟传送的波形个数。其单位是波特，记作baud。

设一个波形的持续周期为T，则波特率B可按下式计算：

*B*=1/*T*（baud）

比特率又称数据传输速率，是指数字信号的传输速率，用每秒钟所传输的二进制代码的有效位数表示，单位为比特/秒（记作b/s或bps）。比特率S可按下式计算：

*S*=*B*log2*N*（bps）

式中*B*是波特率，*N*是一个波形代表的有效状态数。

信道容量一般是指物理信道能够传输信息的最大能力，它的大小由信道的带宽、可使用的时间、传输速率以及信道质量（即信号功率与干扰功率之比）等因素决定。

误码率，也称出错率，是衡量数据通信系统在正常工作情况下传输可靠性的重要指标。误码率等于传输出错的码元数占传输总码元数的比例。在计算机网络中一般要求数字信号误码率低于10-6。

信号在信道中的传输，从信源到信宿需要一定的时间，这个时间叫做传播延迟（也叫时延）。传播延迟与信源和信宿间的距离有关，也与具体的通信信道中的信号传播速度有关。

在信道中，信号功率与噪声功率的比值称为信噪比（Signal-to-Noise Ratio）。如果用S表示信号功率，用N表示噪声功率，则信噪比应被表示为S/N。

在实际传输中，更多地使用10 lg10（S/N）来表示信噪比，单位是分贝（dB）。对于S/N等于10的信道，则称其信噪比为10 dB；同样的道理，如果信道的S/N等于100，则称其信噪比为20 dB；以此类推。一般来说，信噪比越大，说明混在信号里的噪声越小，因此信噪比应该越高越好。

## 掌握电路交换、报文交换和分组交换 3 种数据交换技术；

在电话系统中，当用户进行拨号时，电话系统中的交换机（Telephone Switch）在呼叫者的电话与接收者的电话之间建立了一条实际的物理线路，通话便建立起来；此后两端的电话一直使用该专用线路，直到通话结束才能拆除该线路。电话系统中用到的这种交换方式叫做电路交换（Circuit Switching）技术。

电路交换技术的通信过程包括线路建立、数据传输和线路释放3个过程；传输延迟小；一旦线路建立，通信双方便独享该物理线路，不会与其他通信发生冲突。

报文交换（Message Switching）属于存储转发式交换，事先并不建立物理电路，当发送方有数据要发送时，它将要发送的数据当做一个整体交给中间交换设备，中间交换设备先将报文存储起来，然后选择一条合适的空闲输出线将数据转发给下一个交换设备，如此循环往复直至将数据发送到目的节点。采用这种技术的网络就是存储转发网络。不限制报文的大小，必须使用磁盘等外设来缓存较大的数据块报文交换，不适合交互式数据通信；

分组交换（Packet Switching）又称为包交换，是报文交换技术的改进，与报文交换同属于存储转发式交换。在分组交换中，用户的数据被划分成一个个大小相同的分组（packet），这些分组被称为“包”。这些“包”可以被缓存在交换设备的内存而不是磁盘中，通过不同的线路到达同一目的地。由于分组交换能够保证任何用户都不能长时间独占传输线路，因而它非常适合于交互式通信。

在分组交换中，根据传输控制协议和传输路径不同，可将其分为两种方式：数据报分组交换和虚电路分组交换。

**数据报分组交换：**每个数据分组又称为数据报。发送方将数据报按顺序发送，每个数据报在传输过程中按照不同的路径到达目的地，因此接收方接到的数据报的顺序与发送顺序是不同的，接收方还需要按照报文的分组顺序将这些数据报组合成完整的数据。

**虚电路分组交换**: 将数据报方式与电路交换方式结合起来，在发送数据分组之前，首先在发送方和接收方之间建立一条通路。通路建立后，数据分组将依次沿此路径进行传输。因此，接收方接到的数据分组的顺序与发送顺序是相同的。

但是与电路交换不同的是，虚电路方式建立的通路不是一条专用的物理线路，而只是一条路径，因此被称为“虚电路”。

分组交换除吞吐量较高外，还提供了一定程度的差错检测和代码转换能力。计算机网络常常使用分组交换技术，分组交换也存在许多问题拥塞、报文分片和重组；

电路交换和分组交换两种技术有许多不同之处，主要体现在以下3个方面：

信道带宽的分配方式不同；收发双方的传输要求不同；计费方法不同；

## 掌握数据通信系统模型的基本组成；

一个完整的数据通信系统一般由信源、信号变换器、通信信道、信宿等构成；

信源就是信息的产生和发送端，是发出待传送信息的人或设备。信宿就是信息的接收端，是接收所传送信息的人或设备。

通信信道是传送信号的一条通路，由传输线路和传输设备组成。同一个传输介质上可以同时存在多条信号通路，即一条传输线路上可以有多个通信信道。信道类型是由所传输的信号决定的，用来传输模拟信号的信道称为模拟信道，用来传输数字信号的信道称为数字信道；

信号变换器的作用是将信源发出的数据变换成适合在信道上传输的信号，或将信道上传来的信号变换成可供信宿接收的数据。发送端的信号变换器可以是编码器或调制器，接收端的信号变换器相对应的就是译码器或解调器。

信号在传输过程中受到的干扰称为噪声。

## 掌握奇偶校验码和循环冗余码两种差错控制技术；

奇偶校验码是最简单的校验码，其编码规则是：先将要传送的数据码元分组，并在每组数据后面附加一位冗余位，即校验位，使分组中包括冗余位在内的数据码元中“1”的个数保持为奇数（奇校验）或偶数（偶校验）。在接收端按照同样的规则进行检查，只有“1”的个数仍符合原定的规则才认为传输正确，否则认为传输出错。

循环冗余码（Cyclic Redundancy Code，CRC），又称为多项式码，是使用最广泛且检错能力很强的一种检错码。CRC的工作方法是在发送端产生一个冗余码，附加在信息位后面一起发送到接收端，接收端收到信息后按照与发送端形成循环冗余码同样的算法进行校验，如果发现错误，则通知发送端重发。

CRC将整个数据块当做一串连续的二进制数据，把各位看成是一个多项式的系数，则该数据块就和一个n次多项式M(X)相对应。例如，信息码1101表示为多项式为

*M*(*X*)=*X* 3+*X* 2+*X* 0。

## 掌握并行传输与串行传输，单工、半双工和全双工的数据通信方式；

串行传输：数据的若干位按顺序一位一位地传送，从发送端到接收端只要一条传输信道即可；可以节省传输线路和设备，利于远程传输

并行传输：字符的每一个数据位各占一条传输信道，通过多条并行的信道同时传输，速率高，但线路和设备增加若干倍，用于短距离要求快速传输的情况；

单工通信又称为单向通信。在单工通信中，数据信号固定地从发送端传送到接收端，即信息流仅沿一个方向流动；

半双工通信又称为双向交替通信。在半双工通信中，数据信号可双向传送，但不能在两个方向上同时进行。

全双工通信又称为双向同时通信。在全双工通信中，同一时刻双方能在两个方向上传输数据信息，它相当于把两个相反方向的单工通信方式组合起来；

## 掌握数据传输技术、数据传输同步方式和数据编码技术；

同步方式有两种：异步传输和同步传输。

异步传输又称为起止式传输。发送端可以在任何时刻向接收端发送数据，且将每个字符（5～8位）作为一个独立的整体进行发送，字符间的间隔时间可以任意变化。为了便于接收端识别这些字符，发送端需要在每个字符的前后分别加上一位或多位信息作为它的起始位和停止位；

同步传输要求数据的发送端和接收端始终保持时钟同步。根据同步通信规程，同步传输具体又分为面向字符的同步和面向位的同步；

面向字符的同步：发送端将字符分成组进行连续发送，并在每组字符前后各加一个同步字符（SYN）。当接收端接收到同步字符时开始接收数据，直到再次收到同步字符时停止接收，然后进入等待状态，准备下一次通信。

面向位的同步：发送端每次发送一个二进制位序列，并在发送过程的前后分别使用一个特殊的8位位串（01111110）作为同步字节来表示发送的开始和结束。

数字信号在信道中的传输技术分为基带传输和频带传输两类。

由计算机等直接发出的数字信号是一连串矩形电脉冲信号，包含直流、低频和高频等多种成分。在其频谱中，从零频开始到能量集中的一段频率范围称为基本频带，简称为基带。在线路上直接传输数字基带信号就称为基带传输。

基带传输是一种最简单的传输方式，它抗干扰能力强、成本低，通信信道利用率低基带传输信号衰减严重，传输的距离受到限制，因此常用于局域网；

**非归零编码：**用高电位表示“1”，低电位表示“0”。需要同时发送同步时钟信号来保证发送方和接收方同步**；**

曼彻斯特编码是一种“自含时钟”的编码方法，其编码规则是在每个时钟周期内产生一次跳变，由高电位向低电位跳变时，代表“0”；由低电位向高电位跳变时，代表“1”；收发双方可以根据自带的“时钟”信号来保持同步，无须专门传递同步信号的线路，因此这种编码方法通常用于局域网传输。

差分曼彻斯特编码规定当前比特位的取值由开始的边界是否存在跳变而定，开始边界有跳变表示“0”，无跳变表示“1”，

利用模拟信道实现数字信号传输的方法称为频带传输。

在频带传输中，由发送端将数字数据信号转换成模拟数据信号的过程称为调制，使用的调制设备称为调制器；在接收端把模拟数据信号还原为数字数据信号的过程称为解调，使用的设备称为解调器。同时具备调制和解调功能的设备称为“调制解调器”（Modem）。在实现全双工通信时，则要求收发两端都安装调制解调器；

模拟信号传输的基础是载波，载波信号可以表示为：



振幅A、角频率w 、相位 &是载波信号的三个可变参量，它们是正弦波的控制参数，也称为“调制参数”；

振幅键控（ASK）：ASK方式是指载波的幅度A随发送的数字信号而变化，以不同振幅表示二进制数字“1”和“0”，实现简单，但抗干扰能力差，调制效率低；

移频键控（FSK）：FSK方式是指用两个靠近载波频率的不同频率w1、w2，表示 1和 2分别表示二进制数字“1”和“0”，电路简单，抗干扰能力强，但频带的利用率低；

**移相键控（PSK）：PSK方式只是以载波的相位&变化来表示数据。在二相制情况下，二进制数字“0”和“1”分别用不同相位载波信号波形表示，实现较为复杂；**

模拟数据的数字编码是将连续的信号波形用有限个离散（不连续）的值近似代替的过程，其中最常用的方法就是脉冲编码调制（PCM）技术，简称脉码调制。PCM一般通过采样、量化和编码3个步骤实现；

（1）采样：将原信号波形的时间坐标按照固定的时间间隔离散化，以模拟数据的最大值（或平均值）作为样本，代替模拟数据在某一区间的值。

（2）量化：量化是指对采样得到的样本值按量化分级并取整。

（3）编码：将量化取整的样本值转换为相应的二进制编码。

## 熟悉信道复用技术。

在同一介质上，同时传输多个有限带宽信号的方法，被称为多路复用（Multiplexing）；

多路复用技术可以分为频分多路复用、时分多路复用、波分多路复用和码分多路复用等多种形式，最常用的是频分多路复用和时分多路复用；

频分多路复用（Frequency Division Multiplexing，FDM）：

利用频率变换或调制的方法，将若干路信号搬移到频谱的不同位置，相邻两路的频谱之间留有一定的频率间隔，以防相互干扰，这样排列起来的信号就形成了一个频分多路复用信号；

时分多路复用（Time Division Multiplexing，TDM）：

利用时间分隔方式来实现多路复用的，它将一个传送周期划分为多个时间间隔，让多路信号分别在不同的时间间隔内传送。

波分多路复用（Wave Division Multiplexing，WDM）：

指在一根光纤上能同时传送多个波长不同的光信号的复用技术，它实质上是利用了光具有不同波长的特征。是频率分割技术在光纤中的应用；

码分多路复用（Code Division Multiplexing，CDM）：

一种用于移动通信系统的技术，它的实现基础是微波扩频通信；

**小结：**

数据通信技术是计算机网络的基础，而数据通信是指在不同的计算机之间传送表示字符、数字、语音、图像的二进制代码的过程。数据通信是通过数据通信系统来实现的，一个完整的数据通信系统一般由信源、信号变换器、通信信道、信宿等构成。数据通信系统的主要技术指标包括信道带宽、波特率、比特率、误码率等。

数据通信可分为并行传输和串行传输；还可以按照信号传送方向与时间的关系分为3种：单工通信、半双工通信和全双工通信。在单工通信方式中，信号只能向一个方向传输；在半双工通信中，信号可以双向传送，但是同一时间只能向一个方向传送；在全双工方式中，信号可以同时双向传送。

数据通信中同步技术是解决通信的收发双方在时间基准上保持一致的问题。数据通信的同步方式主要包括异步传输和同步传输，同步传输又分为面向字符的同步和面向位的同步两种。

数字信号在信道中的传输技术分为基带传输和频带传输两种。在基带传输中，常采用非归零编码、曼彻斯特编码和差分曼彻斯特编码方式；在频带传输中，常采用振幅键控（ASK）、频移键控（FSK）、相移键控（PSK）来实现对数字信号的模拟化编码。

为了充分利用通信线路的带宽，提高通信介质利用率，可采用多路复用技术。最常用的多路复用技术是频分多路复用和时分多路复用。

数据交换技术是用来解决资源子网中的两台计算机如何通过通信子网实现数据交换问题的。通常使用的数据交换技术有3种：电路交换、报文交换和分组交换。计算机网络常常使用分组交换，偶尔才使用电路交换，一般不使用报文交换。

差错的控制方法是在发送的报文中附加校验码，接收端检测到有差错的报文后进行丢弃或纠错。常用的校验码有奇偶校验码和循环冗余码。

# 网络体系结构

## 了解网络体系结构的定义及分类，熟悉网络体系结构相关的概念；

网络体系结构：它将计算机互联的功能划分成有明确定义的层次，并规定同层次实体通信的协议及相邻层之间的接口服务，以给出网络通信的一般解决办法。简单来说，网络体系结构就是网络各层及其协议的集合。

分层设计：按照信息的流动过程将网络的整体功能分解为一个个的功能层，同一机器上的相邻功能层之间通过接口进行信息传递，不同机器上的同等功能层之间采用相同的协议。

网络体系结构是众多现有网络标准的抽象，也是制定新的网络标准与协议的准则。

网络协议：用于规定信息的格式以及如何发送和接收信息的规则称为网络协议（Network Protocol）或通信协议（Communication Protocol）。

网络协议主要由以下3个要素组成：

语法：规定用户数据与控制信息的结构与格式。

语义：规定通信双方需要发出何种控制信息、完成何种动作及做出何种响应等。

时序：又称“同步”，用于规定事件实现顺序的详细说明，即通信双方动作的时间、速度匹配和事件发生的顺序等。

## 掌握 OSI 参考模型结构、各个层次的功能以及报文封装格式；

OSI参考模型从下到上由物理层、数据链路层、网络层、传输层、会话层、表示层和应用层组成；

低层（物理层、数据链路层）执行的功能与物理通信相关，如构建帧、传输含有包的信号；中间层（网络层、传输层、会话层）协调结点间的网络通信，如确保通信会话无中断、无差错地持续进行；高层（表示层、应用层）的工作直接影响软件应用和数据表示，包括数据格式化、加密以及数据与文件传输管理。

物理层是OSI参考模型的最低层，主要为通信提供物理链路，并在两个网络设备之间透明地传输比特流。机械、电气、功能和规程特性；

数据服务单元是比特；

机械特性：规定了物理连接时所使用可接插连接器的形状和尺寸，连接器中引脚的数量与排列情况等。

电气特性：规定了在物理连接上传输二进制比特流时线路上信号电平高低、阻抗及阻抗匹配、传输速率与距离限制。早期的标准定义了物理连接边界点上的电气特性，而较新的标准定义了发送和接收器的电气特性，同时给出了互联电缆的有关规定。新的标准更有利于发送和接收电路的集成化工作。

功能特性：规定了物理接口上各条信号线的功能分配和确切定义。物理接口信号线一般分为数据线、控制线、定时线和地线。

规程特性：定义了信号线进行二进制比特流传输时的一组操作过程，包括各信号线的工作规则和时序。

数据链路层是OSI参考模型的第二层，其作用主要是负责将由物理层传来的数据封装成数据帧（Frame），并保证帧在计算机之间进行无差错地传输。分为MAC和LLC两个子层，MAC（介质访问控制）子层的功能包括数据帧的封装/拆封，帧的寻址和识别，帧的接收与发送，链路的管理，帧的差错控制等；LLC（逻辑链路层控制）子层负责为上层提供服务，如从上层接收包并发送到MAC层。主要功能包括链路管理、流量控制、差错处理、帧同步和寻址。

链路管理：当两个结点开始通信时，发送方必须确定接收方处在准备接收数据的状态。为此，双方必须交换一些必要的信息，然后建立数据链路连接；同时，在传输数据时要维持数据链路；当通信完毕时要释放数据链路。数据链路的建立、维持和释放就叫做链路管理。

流量控制：为防止传输数据的双方速度不匹配或接收方没有足够的接收缓存而导致数据拥塞或溢出，数据链路层必须采用流量控制技术来控制流量，使接收方来得及接收发送方发送的数据。

差错处理：数据链路层采用差错控制技术，把不可靠的物理连接变为可靠的数据链路，从而保证数据传输的正确性。数据链路层实体将对帧的传输过程进行检查，发现差错用重传方式解决。

帧同步：在数据链路层，数据以帧为单位进行传输。帧同步是指接收方应当能从来自物理层的比特流中准确地区分出一帧的开始和结束的位置。

寻址：在多点连接的情况下，寻址保证每一帧都能传送到正确的目的结点。同时，接收方也应当知道发送方是哪一个结点。

网络层能够读取包协议地址信息并将每一个包沿最佳路径转发直至到达目的结点。传输单位是分组或包（Packet）；网络层的关键问题是如何进行路由选择；

主要功能包括路由选择、流量控制和多用户数据传输。

网络层所提供的服务可分为两类：面向连接的网络服务和无连接网络服务。

面向连接的网络服务又称为虚电路（Virtual Circuit）服务，它具有网络连接建立、数据传输和网络连接释放三个阶段，是可靠的报文分组按顺序传输的方式，适用于确定型对象、长报文、会话型传输要求。特点是在数据传送以前必须在源结点和目的结点之间建立一条虚电路。

无连接网络服务有三种类型：数据报（datagram）、确认交付（confirmed delivery）与请求回答（request reply）。

虚电路方式与数据报方式之间的最大差别在于：虚电路方式为每一对节点之间的通信预先建立一条虚电路，后续的数据通信沿着建立好的虚电路进行，不必为每个数据包进行路由选择；而在数据报方式中，需为每一个进入的数据包进行一次路由选择，也就是说，每个数据包的路由选择都独立于其他数据包。

传输层位于OSI参考模型的第四层，它是网络中资源子网与通信子网的桥梁，主要负责确保数据可靠、顺序、无差错地从A点到传输到B点（A、B点可能位于相同或不同的网络）。如果没有传输层，数据将不能被接收端验证或解释。功能是在网络层提供服务的基础上建立的，其任务是向用户提供可靠的、透明的、端到端的数据传输，采用一些技术手段弥补用户对不同网络的要求以及网络可向用户提供的服务之间的差异，使得用户无需了解网络传输的细节，就能获得相对稳定的数据传输服务。采用的技术手段：分流/合流技术、复用/解复用技术、分段/合段技术、差错检测和恢复技术、流量控制技术；

会话层的功能是向会话的应用进程之间提供会话组织和同步服务，对数据的传送提供控制和管理，以协调会话过程，为表示层实体提供更好的服务。

具体实现技术包括以下4个方面。

（1）利用令牌（有时也成为“权标”）技术来保证数据交换、会话同步的有序性，拥有令牌的一方可以发送数据或执行其他动作。

（2）利用活动和同步技术来保证用户数据的完整性，并让用户知道整个交换的过程。

（3）利用分段和拼接技术来提高数据交换的效率，多块用户数据可以合并在一起进行传输。

（4）利用重新同步技术来实现用户会话的延续性，支持传输过程中的故障恢复。

会话层提供了丰富的服务来支持用户对数据交换的控制和管理。

进行了分类，组合成12个功能单元，分别为：核心功能单元（支持会话连接的建立和释放，以及常规数据的传输）、协商释放功能单元、半双工功能单元、全双工功能单元、加速数据功能单元、特权数据功能单元、能力数据功能单元、次同步功能单元、主同步功能单元、重新同步功能单元、异常功能单元、活动管理功能单元；

方便用户选择使用合适的功能单元，会话服务定义了三个子集：

基本组合子集（BCS）为用户提供会话连接建立、正常数据传送、令牌的处理及连接释放等基本服务。

基本同步子集（BSS）在BCS的基础上增加为用户通信过程同步的功能，能在出错时从指定的同步点处进行恢复，减少差错重传

基本活动子集（BAS）在BCS的基础上加入了活动管理。

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 功能单元 | BCS | BSS | BAS | 功能单元 | BCS | BSS | BAS |
| 核心 | √ | √ | √ | 次同步 |  | √ | √ |
| 半双工 | √ | √ | √ | 主同步 |  | √ |  |
| 双工 | √ | √ |  | 重新同步 |  | √ |  |
| 特权数据 |  | √ | √ | 加速数据 |  |  |  |
| 异常报告 |  |  | √ | 活动管理 |  |  | √ |
| 协商释放 |  | √ |  | 能力数据交换 |  |  | √ |

表示层的目的就是屏蔽不同计算机在信息表示方面的差异，其功能包括传送语法的协商，以及抽象语法和传送语法之间的转换。

应用层为网络用户和应用程序提供各种服务，也是最终用户应用程序访问网络服务的地方。

执行主机A的逆过程，这个过程可以理解为对数据的拆封或解封。

## 掌握 TCP/IP 参考模型结构、各个层次的功能以及报文封装格式。

流行的网络体系结构是TCP/IP参考模型，它已成为计算机网络体系结构事实上的标准，Internet就是基于TCP/IP参考模型建立的。

共包含4个功能层，由下往上依次为：网络接口层、网络互连层、传输层和应用层；

网络接口层是TCP/IP模型的最低层。作用是负责接收从网络层交来的IP数据包并将IP数据包通过低层物理网络发送出去；或者从低层物理网络上接收物理帧，然后抽出IP数据包交给网络层。

网际层与OSI参考模型中的网络层相当，是整个TCP/IP参考模型的关键部分。网际层的功能主要包括以下3个方面。

（1）处理来自传输层的分组发送请求：将分组装入IP数据包，填充报头，选择去往目的结点的路径，然后将数据报发往适当的网络接口。

（2）处理输入数据报：首先检查数据报的合法性，然后进行路由选择，假如该数据报已到达目的结点（本机），则去掉报头，将IP报文的数据部分交给相应的传输层协议；假如该数据包尚未到达目的结点，则转发该数据报。

（3）处理ICMP报文：即处理网络的路由选择、流量控制和拥塞控制等问题

网际层的主要协议有4个：网际协议（IP）、地址解析协议（ARP）、反向地址解析协议（RARP）和网际控制报文协议（ICMP），其中最核心的是IP协议。

传输层的作用在源结点和目的结点的两个进程实体之间提供可靠的端到端的数据传输。两个传输层协议：传输控制协议（TCP）和用户数据报协议（UDP）。

应用层位于TCP/IP模型的最高层主要为用户提供多种网络应用程序，如电子邮件、远程登录等。包含了所有高层协议，早期的高层协议有虚拟终端协议（Telnet）、文件传输协议（FTP）、电子邮件传输协议（SMTP）、域名服务（DNS），超文本传输协议（HTTP）；

OSI模型和TCP/IP模型区别：

两者层数不一样：OSI参考模型有7层，而TCP/IP参考模型只有4层。两者都有网络层、传输层和应用层。

两者服务类型不同：**OSI模型的网络层提供面向连接和无连接两种服务，而传输层只提供面向连接服务。TCP/IP模型在网络层只提供无连接服务，但在传输层却提供面向连接和无连接两种服务。**

概念区分不同; **在OSI参考模型中，明确区分了3个基本概念：服务、接口和协议。而TCP/IP模型并不十分清晰地区分服务、接口和协议这些概念。相比TCP/IP模型，OSI模型中的协议具有更好的隐蔽性，在发生变化时也更容易被替换。**

通用性不同: **OSI模型更具有通用性,** **协议实现方面存在某些不足**

**小结：**

**国**际标准化组织ISO建立了一个名为开放系统互联（OSI）的参考模型，允许各种不同的系统进行通信，其中物理层、数据链路层、网络层都是网络支持层，会话层、表示层、应用层都是用户支持层，传输层是连接网络支持层与用户支持层的。物理层用于在物理介质上透明地传输比特流；数据链路层负责点到点之间的无差错地传递数据单元；网络层负责将分组通过多条网络链路从源端传递到目的端；传输层负责整个报文从源端到目的端的传递；会话层负责通信设备之间建立、维护和同步会话；表示层通过将数据转换为通信双方互相认同的格式，确保通信设备之间的互操作性；应用层使用户能访问网络服务。

OSI参考模型虽然是国际标准，但是它层次多，结构复杂，在实际中完全遵从OSI参考模型的协议几乎没有。目前流行的网络体系结构是TCP/IP参考模型，它已成为计算机网络体系结构事实上的标准。TCP/IP参考模型共包含4个功能层，由下往上依次为：网络接口层、网络互连层、传输层和应用层，每一层负责不同的通信功能。

TCP/IP模型和OSI模型有许多相似之处，但是它们在层数、概念区分、服务类型和通用性等方面还存在许多不同之处。

# TCP/IP 协议

## 了解 UDP 的特点、端口分配和数据报格式；

UDP的主要特点包括：

（1）无连接的服务，即在传输数据之前不需事先建立连接。UDP无连接的特点使得数据传输时延比较小。

（2）不可靠性。UDP把应用层传给IP层的数据发送出去，使用尽最大努力交付，但是并不保证它们能够可靠交付。由于缺乏可靠性，UDP应用一般必须允许一定量的丢包、出错和复制。绝大多数UDP应用都不需要可靠机制，甚至可能因为引入可靠机制而降低性能。绝大多数UDP应用都不需要可靠机制，如流媒体、实时多媒体游戏和VoIP（voice over IP），甚至可能因为引入可靠机制而降低性能。

（3）缺乏拥塞避免和控制机制，使用UDP时，网络出现的拥塞不会使源主机的发送速率变低，因此需要基于网络的拥塞控制机制来减小因失控和高速UDP流量负荷而导致的拥塞崩溃效应。

使用包队列和丢弃技术的路由器等网络设备往往就成为降低UDP过大通信量的有效工具。此外，数据报拥塞控制协议（datagram congestion control protocol，DCCP）可以通过在诸如流媒体类型的高速率UDP流中增加主机拥塞控制来解决拥塞问题。

（4）支持多种交互通信。UDP支持一对一、一对多、多对一和多对多的交互通信。

常见UDP服务及端口号

|  |  |  |
| --- | --- | --- |
| UDP端口号 | 协议名称 | 说 明 |
| 53 | DOMAIN | 域名服务（DNS） |
| 69 | TFTP | 简单文件传输协议 |
| 161 | SNMP | 简单网络管理协议 |
| 520 | RIP | 路由信息协议 |

由于TCP和UDP是两个独立的模块，因此，它们的端口号也是相互独立的。也就是说，TCP和UDP可以使用相同的端口号，TCP端口号由TCP协议来查看，UDP端口号由UDP协议来查看。

UDP数据报有数据字段和首部字段两个字段。首部字段只有8个字节，由4个字段组成，每个字段长度都是两个字节，

## 掌握 TCP 的特点、端口分配和报文格式；

**TCP的特点**

（1）面向连接的服务。面向连接意味着两个使用TCP的应用程序（通常为一个客户和一个服务器）在彼此交换数据之前必须先建立一个TCP连接。TCP连接只存在于两个终端结点，网络当中的中间结点（如路由器和网桥）对这个连接毫不知情（只知道传输的数据而不是连接本身）。

（2）面向字节流的服务。流是无报文丢失、重复和失序的数据序列，两个应用程序通过TCP连接交换字节流。TCP协议从应用程序处收集数据后，封装成长度适中的一个数据报文段。在报文头中的序号域指出段中数据在发送端数据流中的位置。TCP协议为实现流传输服务付出了大量开销。

（3）可靠交付。TCP的传输过程由建立连接、传输数据和释放连接3个步骤组成。一个应用程序在发送数据时，首先要请求建立连接。通过TCP连接传送的数据，无差错、不丢失、不重复并且按序到达。

（4）全双工通信。TCP连接提供的是全双工的数据传输，采用点对点的方式，即在一个TCP连接中仅有两方进行通信，因此广播和多播方式不能用TCP。

（5）流量控制。TCP连接的双方都有固定大小的缓冲区，流量控制可以防止较快主机致使较慢主机的缓冲区溢出。通常把缓冲区中的空闲部分称为窗口。TCP采用可变滑动窗口协议，并且当交付的数据不够填满一个缓冲区时，流服务提供“PUSH”机制，应用程序可以用其进行强迫传送。

TCP端口号采用了动态和静态相结合的分配方法，、

常见TCP服务及端口号

|  |  |  |
| --- | --- | --- |
| TCP端口号 | 协议名称 | 说 明 |
| 21 | FTP | 文件传输协议-控制(File Transfer Protocol-Control) |
| 22 | SSH | SSH远程登陆协议（SSH Remote Login Control） |
| 23 | TELNET | 远程登录（Telnet） |
| 25 | SMTP | 简单邮件传输协议（Simple Mail Transfer Protocol） |
| 53 | DNS | 域名服务器（Domain Name Server） |
| 69 | TFTP | 简单文件传输协议（Trivial File Transfer Protocol） |
| 80 | WWW | Web服务（World Wide Web） |
| 119 | NNTP | 网络新闻传输协议（Network News Transfer Protocol） |

TCP虽然是面向字节流的，但TCP传送的数据单元是报文段。一个TCP报文段分为首部和数据两部分

（1）源端口号和目的端口号。源端口号和目的端口号用于表示发送端和接收端的端口号。这两个值加上IP首部中的源IP地址和目的IP地址可以确定一条唯一的TCP连接。

（2）序号。序号字段用于标识从TCP发送端向TCP接收端发送的数据字节流，它表示在这个报文段中的第一个数据字节的序号。例如，当前报文段的第一个数据字节的序号为201，数据长度为100字节，则当前报文段的序号字段的值为201，下一报文段的序号值为301。序号字段占4个字节，当序号到达232-1后又从0开始。

（3）确认序号。确认序号包含发送确认的一端所期望收到的下一个序号。既然每个传输的字节都被计数，确认序号应当是上次已成功收到数据字节序号加1。例如，接收端已成功接收发送端发送的序号为501，数据长度为200的报文段。那么，接收端期望收到的下一个数据序号是701，则该确认序号为701。

TCP为应用层提供全双工服务。这意味着数据能在两个方向上独立地进行传输。因此，TCP连接的每一端必须保持每个方向上的传输数据序号。

4）数据偏移。数据偏移字段指出TCP报文段的数据起始处距离TCP报文段的起始处有多远。需要这个字段是因为选项字段的长度是可变的。这个字段占4位，以4字节为单位，因此TCP数据偏移的最大值是60字节，也就是说TCP首部的最大长度为60字节。

（5）保留。保留字段占6位，保留为今后使用，目前设置为0。

（6）标志位。在TCP首部中有6个标志位，具体含义如下：

* URG（urgent）为紧急数据标志。当URG=1时，表示紧急指针字段的值有效。此时，该报文段中有紧急数据，应尽快传送，而不是按照原来的顺序传送。这时需要与首部中的紧急指针字段配合使用。
* ACK（acknowledgement）为确认标志位。当ACK=1时，表示报文段中的确认序号有效；当ACK=0时，确认序号无效。TCP规定：在连接建立后，所有传送的报文段的ACK字段必须置1。
* PSH（push）为推送标志位。当PSH=1时，表示发送端希望立即得到接收端的响应。此时，发送方的TCP协议软件马上发送该数据包，接收方收到后也应尽快把这个报文段交给应用层。
* RST（reset）为复位标志位，用来复位一条连接。如果TCP收到的数据不属于该主机上的任何一个连接，则将RST字段置1，向发送端发送一个复位数据包，释放当前连接。RST字段置1还可用来拒绝一个非法的报文段或拒绝打开一个连接。
* SYN（synchronous）为同步标志位，在建立连接时用来同步序号。如果SYN=1，而ACK=0，表示这是一个连接请求报文段；如果SYN=1，而ACK=1，则表示这是一个连接接受报文段。具体的连接过程将在4.2.4节中进行讲解。
* FIN（finish）为终止标志位，用来释放连接。当FIN=1时，表示发送端端完成发送任务，希望释放连接。

（7）窗口。窗口表明该报文段的发送端当前能够接收的从确认序号开始的最大数据长度，该值主要向对方声明本地接收缓冲区的使用情况。窗口大小是一个16位字段，因而窗口字段最大65 535字节。

8）校验和。校验和覆盖了整个TCP报文段：TCP首部和TCP数据。这是一个强制性的字段，一定是由发送端计算和存储，并由接收端进行验证。

（9）紧急指针。只有当URG=1时，该字段才有效。紧急指针是一个正的偏移量，指出本报文段中紧急数据的字节数。也就是说，紧急指针字段和序号字段中的值相加表示紧急数据最后一个字节的序号。值得注意的是，即使窗口字段为零，也可以发送紧急数据。

（10）选项。选项字段长度可变，最长可达40字节。TCP规定了最长报文大小，又称为MSS（Maximum Segment Size）。每个连接方通常都在通信的第一个报文段中指明这个选项，它指明本端所能接收的报文段的最大长度。

## 了解地址解析协议和网际控制报文协议ICMP;

地址解析协议ARP

ARP为IP地址到对应的物理地址提供动态的映射。之所以用“动态”这个词是因为这个过程是自动完成的，一般应用程序和系统管理员并不关心或干涉这个过程。

反向地址解析协议RARP

反向地址解析RARP一般用于无盘工作站和终端，解决已知物理地址获取IP地址的问题。RARP的基本思想是：网络中有一个RARP服务器，保存了本网中各个无盘工作站的地址绑定，并负责响应这些节点的地址请求；新启动的无盘工作站广播一个RARP请求分组，分组中给出自己的物理地址；RARP服务器查找地址绑定表，用单播方式发回RARP应答分组，给出所请求的IP地址。

RARP的缺点在于要求每个网络都要有一个RARP服务器，并且RARP响应中只包含很少的信息。它在概念上很简单，但是RARP服务器的实现却与系统相关。因此，并不是所有的TCP/IP实现都提供RARP服务器。使用RARP的常见协议是BOOTP（BOOTstrap Protocol，自举协议）和DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）。

网际控制报文协议

ICMP属于网络层协议，允许主机或路由器报告差错情况和提供有关异常情况的报告。当传送IP数据报发生错误，比如主机不可达，路由不可达等，ICMP将会把错误信息封包，然后传送回给主机，给主机一个处理错误的机会。

ICMP报文通常被网际层或更高层协议（TCP或UDP）所使用，但它并不是高层协议。通常将ICMP报文作为IP数据报的数据，并为其加上IP首部组成IP数据报，

ICMP报文大致分为两类：一种是查询报文，一种是差错报文。

* 查询报文：是成对出现的，它帮助主机或网络管理员从一个路由器或另一个主机得到特定的信息，主要有以下几种用途：Ping查询、子网掩码查询和时间戳查询。
* 差错报文：用于报告路由器或主机在处理一个IP数据报时可能遇到的一些问题。差错报文产生在数据传送发生错误的时候。
* **ICMP的应用举例**
* Ping是TCP/IP网络中一个最简单而又非常有用的ICMP应用程序，常用于验证两个主机之间的连通性。
* ICMP另一个非常有用的应用是tracert（Windows操作系统下的名字，在UNIX操作系统下称为traceroute）。

## 掌握 TCP 传输连接的建立和释放过程；

**连接：（1）第1次握手：客户发送连接请求。**

**（2）第2次握手：服务器同意连接确认。**

**（3）第3次握手：客户确认连接。**

**释放：（1）第1次握手：客户请求关闭连接。**

**（2）第2次握手：服务器确认客户请求。**

**（3）第3次握手：服务器请求关闭连接。**

**（4）第4次握手：客户确认服务器请求。**

## 掌握 IPv4 地址的结构和分类；

一个IP地址由4组8位的二进制数组成，一般采用十进制方式表达，每一段取值区间为[0,255]；

每个IP地址内部分成两部分，即网络号和主机号；

* 网络号：也叫做网络地址，用于标识大规模TCP/IP网际网络（即由网络组成的网络）内的单个网段。
* 主机号：也叫做主机地址，用于识别每个网络内部的TCP/IP节点，如工作站、服务器、路由器或其他TCP/IP设备。

为了方便网络的管理，IP地址分为A、B、C、D、E五类；

A、B、C类地址称之为单目传送地址，这些地址通常只能分配给唯一的主机；D类地址是组播地址；E类地址则是在IP地址设计之初保留作为科学研究用的。

IP地址类别详述

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| IP地址类型 | 二进制固定最高位 | 二进制网络位 | 二进制主机位 | 网络号地址范围 | 每个网络中最多可容纳主机数 |
| A类 | 0 | 8位 | 24位 | 1.0.0.0～126.0.0.0 | 224-2 |
| B类 | 10 | 16位 | 16位 | 128.0.0.0～191.255.0.0 | 216-2 |
| C类 | 110 | 24位 | 8位 | 192.0.0.0～223.255.255.0 | 28-2（254） |
| D类 | 1110 | 组播地址 | | 224.0.0.0~239.255.255.255 | —— |
| E类 | 11110 | 保留地址 | | 240.0.0.0~247.255.255.255 | —— |

在IP地址中，有一些特殊地址被赋予特殊的作用。

广播地址、组播地址、网络地址是127的IP地址称为环回地址或者回送地址，主要用于对本地回路测试及实现本地机进程间的通信；

**私有地址**

一般的IP地址是由网络信息中心（Network Information Center，NIC）统一管理并分配给提出注册申请的组织机构的，这类IP地址称为公有地址，通过它可以直接访问因特网。而私有地址属于非注册地址，专门为组织机构内部使用。

|  |  |
| --- | --- |
| 私有地址类别 | 范围 |
| A类 | 10.0.0.0～10.255.255.255 |
| B类 | 172.16.0.0～172.31.255.255 |
| C类 | 192.168.0.0～192.168.255.255 |

## 理解子网掩码的概念,掌握子网划分的方法；

子网掩码（或称子网屏蔽码）与IP地址相同，也是一个32位的二进制数。对于子网掩码的取值，通常是将对应于IP地址中网络地址（网络号和子网号）的所有位设置为“1”，对应于主机地址（主机号）的所有位都设置为“0”。

**按照子网的数量划分，首先要确定有多少个子网，然后确定子网所占的位数，可遵照如下公式进行：**

https://img-blog.csdnimg.cn/6b661c2a1d004251a45066185e3f3b98.png

**按照主机数量进行划分时，首先确定用多少个主机位能满足主机的数量，然后剩余的主机位为子网**

https://img-blog.csdnimg.cn/355c30e4818a482596121f7067cda9ea.png

## 了解 IPv6地址的结构和特点。

IPv6地址采用十六进制的表示方法，共128位，分8组表示，每组16位。因为一个十六进制数可以表示4位，所以每组由4个十六进制数组成，各组之间用“：”隔开。每组中前面的0可以省略，但每组必须有一个数，例如：1080:0:0:0:8:800:200C:417A；

128位的IPv6地址由64位网络地址和64位主机地址组成。其中，64位的网络地址又分为48位的全球网络标识符和16位的本地子网标识符；

特点：

（1）更大的地址空间。IPv6地址长度为128位（16字节），即有2128-1（3.4E+38）个地址，这一地址空间是IPv4地址空间的1E28倍。在IPv6的庞大地址空间中，目前全球连网设备已分配掉的地址仅占其中的极小一部分，有足够的余量可供未来的发展之用。

（2）简化的报头和灵活的扩展。IPv6对数据报头作了简化，将其基本报头长度固定为40字节，减少了处理器开销并节省了网络带宽。此外，IPv6定义了多种扩展报头，使得IPv6变得极其灵活，能提供对多种应用的强力支持，同时又为以后支持新的应用提供了可能。

（3）多样化的地址类型。IPv6定义了3种不同的地址类型：单点传送地址、多点传送地址和任意点传送地址。

（4）即插即用的连网方式。IPv6允许主机发现自身地址并自动完成地址更改，这种机制既不需要用户花精力进行地址设定，又可以大大减轻网络管理者的负担。IPv6有两种自动设定功能，一种是和IPv4自动设定功能相同的名为“全状态自动设定”功能，另一种是“无状态自动设定”功能。

（5）网络层的认证与加密。IP安全协议（IPSec）是IPv4的一个可选扩展协议，是IPv6的一个必须组成部分，主要功能是在网络层对数据分组提供加密和鉴别等安全服务。IPSec提供了认证和加密两种安全机制。

* 认证机制：使IP通信的数据接收方能够确认数据发送方的真实身份以及数据在传输过程中是否遭到改动。
* 加密机制：通过对数据进行编码来保证数据的机密性，以防数据在传输过程中被他人截获而失密。

（6）服务质量的满足。服务质量（Quality of Service，QoS）通常是指通信网络在承载业务时为业务提供的品质保证。基于IPv4的Internet在设计之初，只有一种简单的服务质量，即采用“尽最大努力（Best effort）”传输。但是随着IP网上多媒体业务增加（如IP电话、VoD、电视会议），对传输延时和延时抖动均有严格的要求，因此对服务质量的要求也就越来越高。

（7）对移动通信更好的支持。未来移动通信与互联网的结合将是网络发展的大趋势之一。移动互联网将成为我们日常生活的一部分，改变我们生活的方方面面。IPv6为用户提供可移动的IP数据服务，让用户可以在世界各地都使用同样的IPv6地址，非常适合未来的无线上网。

**小结：**

本章重点介绍了TCP/IP的几个核心协议：网络层的IP协议及由其衍生出来的ARP、RARP、ICMP，以及传输层的UDP和TCP协议。其中IP协议和TCP协议又是重点中的重点。IP是一个网络层协议，它包含寻址信息和控制信息，可使数据包在网络中路由。IP协议中的IP地址表示了因特网中的各个节点，网络中的节点又分处在各个子网当中，因此引入了子网掩码，使用子网划分方法实现了充分利用IP地址、易于管理等目标。

传输层有两大类协议：TCP和UDP。TCP提供可靠的面向连接的字节流服务，它是实际中大多数应用服务首选的传输层协议。UDP则是无连接的，它提供高效但低可靠性的服务。

# 局域网技术

## 了解局域网的特征、体系结构、802 标准和组网模式；

（1）网络所覆盖的地理范围比较小。通常不超过十公里，甚至只在一幢建筑或一个房间内，传输介质以光纤和双绞线为主。

（2）数据传输速率高，一般为10 Mbit/s～100 Mbit/s，目前已出现高达10 Gbit/s的局域网。

（3）误码率低，一般在10-12～10-8以下。这是因为局域网通常采用短距离基带传输，可以使用高质量的传输媒体，从而提高了数据传输质量。

（4）协议简单，结构灵活，组网成本低、周期短，便于管理和扩充。

（5）一般侧重共享信息的处理，通常没有中央主机系统，而是以PC为主体，包括终端及各种外设。

IEEE 802标准所描述的局域网参考模型只对应OSI参考模型的数据链路层与物理层，局域网参考模型将数据链路层划分为逻辑链路控制LLC（Logical Link Control）子层与介质访问控制MAC（Media Access Control）子层。

* IEEE 802.1标准：局域网概述、体系结构、网络管理和网络互联。
* IEEE 802.2标准：逻辑链路控制LLC，关于数据帧的错误控制及流控制。
* IEEE 802.3标准：以太网）准，包含CSMA/CD介质访问控制方法和物理层规范。
* IEEE 802.4标准：Token Bus局域网（令牌总线网）标准，包含令牌总线介质访问控制标准和物理层规范。
* IEEE 802.5标准：Token Ring局域网（令牌环网）标准，包含令牌环介质访问控制方法和物理层规范。
* IEEE 802.6标准：MAN（城域网）标准，包含城域网介质访问方法和物理层规范。
* IEEE 802.7标准：宽带技术标准，包括宽带网络介质、接口和其他设备。
* IEEE 802.8标准：光纤技术标准，包括光纤介质的使用以及不同网络类型技术的使用。
* IEEE 802.9标准：综合声音/数据服务的访问方法和物理层规范。
* IEEE 802.10标准：网络安全技术，包括网络访问控制、加密、验证或其他安全主题。
* IEEE 802.11标准：无线局域网介质访问控制方法和物理层技术规范，包括：IEEE 802.11a、IEEE 802.11b、 IEEE 802.11c 和IEEE 802.11q标准。
* IEEE 802.12标准：定义了100VGAnyLAN规范。
* IEEE 802.14标准：定义了电缆调制解调器标准。
* IEEE 802.15标准：定义了近距离个人无线网络标准。
* IEEE 802.16标准：定义了宽带无线局域网标准。
* IEEE 802.17标准：弹性分组环（RPR）工作组。
* IEEE 802.18标准：宽带无线局域网技术咨询组。
* IEEE 802.19标准：多重虚拟局域网共存技术咨询组。
* IEEE 802.20标准：移动宽带无线接入（MBWA）工作组。

**局域网的组网模式**

大多数局域网使用的拓扑结构主要有星型、环型和总线型3种。

局域网的基本组成包括网络硬件和网络软件两大部分。

网络硬件主要包括网络服务器、工作站和网络通信系统等。の

## 掌握局域网的介质访问控制方法；

介质访问控制方法有CSMA/CD介质访问控制、Token-Ring介质访问控制和Token Bus介质访问控制。

CSMA/CD的方式其实就是

所有节点都连接在同一作为传输介质的总线上，节点通过总线发送或接收数据

一个节点在总线上以广播形式发送数据时，其他的结点只能是收听的方式接收数据

总线是被多个结点所共享的，就有可能出现同一时间多个节点通过总线发送数据的情况，就会产生冲突，造成传输失败

节点需要通过“竞争”的方式获得发送权，每个节点能够得到总线发送权的时间是不确定的，所以CSMA/CD属于随机型介质访问控制方法

CSMA/CD协议的特点可以概括为4点：先听先发，边听边发，冲突停止，后退重传。

① Token ring中的节点通过网卡和点-点线路，逐个连接构成闭合的环状结构。环中的数据沿着一个方向绕环传输。

② 令牌是一种特殊的MAC控制帧。帧头中有一位标志令牌的忙/闲。

③当一个节点有数据帧要发送时，先等待空闲的令牌到来，将闲改为忙，然后传送数据帧，接收节点收到数据帧后，标志出发送数据已被正确接收的标记。发送节点重新接收到带有目的节点接收标志的数据帧后，将令牌由忙改为闲将空闲令牌向它的下一级传递。

④节点获取令牌发送数据的时间间隔是确定的，能够提供优先级服务。

**令牌环的维护：令牌丢失的差错、数据帧未撤销的差错；**

①Token Bus是在总线拓扑结构中，利用令牌作为控制节点访问公用总线的一种局域网。

②令牌是一种特殊结构的控制帧，任何节点只有在取得令牌后才能使用共享总线去发送数据。

③通过预先确定的结点获得令牌的顺序，连接在共享总线的多个结点在传输过程中形成逻辑的形状。

④一个节点两次获取令牌的时间T=N\*(YHT+Tr+Tc)。N为环中结点数，THT为令牌持有时间，Tr为令牌在两响铃节点传输时间，Tc为结点接收、处理帧与令牌的时间。由公式，只要控制接入网络的节点的数量，每一个结点利用环网传输数据的实时性是可以得到保证的。

**三种介质访问控制方法的共同点：**

①体系结构都遵循IEEE 802层次结构。

②传输介质主要采用同轴电缆、双绞线和光纤。

③采用共享介质的方式发送和接收数据帧。

④介质访问控制都采用了分布式控制方法，局域网中没有集中控制的主机

## 掌握以太网技术及快速以太网技术；

以太网的相关产品非常丰富，且大多发展成熟、性价比高、传输速率高、网络软件丰富、安装维护方便，且得到了业界几乎所有经销商的支持，逐渐成为当今国际最流行的局域网。

以太网在技术上具备以下基本特点：

（1）以太网不是一种具体的网络，而是一种技术规范，采用基带传输技术。

（2）以太网的标准是IEEE 802.3，使用CSMA/CD介质访问控制方法争用总线。

（3）以太网采用广播式传输技术，是一种广播式网络，具有广播式网络的全部特点。

（4）以太网采用曼彻斯特编码方案。

（5）传输速率高，最高甚至可达10 Gbps。

（6）以太网是可变长帧，长度为64字节～1 518字节。

（7）以太网可以采用多种连接介质，包括同轴电缆、双绞线和光纤等。

（8）以太网的拓扑结构主要有总线型和星型。

**LLC**



以太网体系结构与OSI参考模型的对应关系

**MAC**

**PLS**

**PMA**



IEEE 802.3以太网帧格式

<数据传输率（Mbps）> <信号方式> <最大段长度（百米）>

如10BASE5、10BASE2;

传统以太网的物理层规范

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 名称 | 介质 | 最大长度/段 | 工作站数目/段 | 特点 |
| 10Base5 | 粗同轴电缆 | 500 m | 100 | 适合主干网络 |
| 10Base2 | 细同轴电缆 | 185 m | 30 | 适合低廉的网络 |
| 10Base-T | 双绞线 | 100 m | 2 | 易于安装和维护 |
| 10Base-F | 光纤 | 2 000 m | 2 | 适合连接远程工作站 |

快速以太网标准支持3种不同的物理层标准，分别是100Base-TX、100Base-TX和100Base-FX，

快速以太网的3种物理层标准

|  |  |  |  |
| --- | --- | --- | --- |
| 物理层标准 | 100Base-TX | 100Base-T4 | 100Base-FX |
| 支持全双工 | 是 | 否 | 是 |
| 电缆对数 | 2对双绞线 | 4对双绞线 | 一对光纤 |
| 电缆类型 | 5类UDP/1类STP | UTP Cat 3 | 多模/单模光纤 |
| 最大距离 | 100 m | 100 m | 200 m，2 km |
| 接口类型 | RJ-45或DB9 | RJ-45 | MIC，ST，SC |

## 掌握虚拟局域网；

虚拟局域网（Virtual Local Area Network，VLAN）是指在交换式局域网的基础上，采用网络管理软件构建的可跨越不同网段、不同网络的端到端的逻辑网络。

**VLAN的优点**

1. **控制网络的广播域**
2. **提高组网的灵活性**
3. **提高网络的安全性**

**VLAN的实现方式**

基于端口、基于MAC地址、基于网络层、基于IP组播和基于策略5种；

## 了解无线局域网技术。

无线局域网（Wireless Local Area Network，WLAN）是一种以空气（或真空）为传输介质，以电磁波为载体的局域网，是有线局域网的一种延伸，能快速方便地解决有线方式不容易实现的网络连通问题。

WLAN使用的协议标准是IEEE 802.11（a,b,g,m）系列标准;

**无线局域网的产品和组件**

**无线网卡:** **常见的无线网卡有PCMCIA无线网卡、PCI接口无线网卡和USB接口无线网卡3类产品。**

**无线接入点**: 无线接入点（Access Point，AP）是有线局域网络与无线局域网络的桥梁，用于IEEE 802.11系列无线网络设备组网或接入有线局域网。AP主要分为普通路由AP和带路由AP两种。普通AP仅提供一个无线信号发射的功能；路由AP除了发射无线信号，还可以实现为ADSL等宽带上网方式提供自动拨号功能。

**无线路由器**:常见的无线路由器（见图5-20）包含了一个广域网（WAM）端口，可以用于ASDL接入、有线或无线网络连接等，允许企业、办公室或家庭中多台PC共享1条ADSL线路，通过一个公共的Internet ISP账户接入互联网。

在无线局域网组网时，一般有两种方式可供选择，分别为无中心分布对等方式无线局域网（Ad-hoc Wireless LAN）和有中心的集中控制方式无线局域网（Infrastructure Wireless LAN）

无线网络和有线网络存在很多重要的差异，具体包含以下几个方面：

1. **路径损耗。**
2. **信号的抗干扰性差。**
3. **多路径传播问题。**
4. **隐藏终端问题。**
5. **暴露终端问题。**

**小结：**

局域网是一种将较小地理范围内的各种数据通信设备互连在一起的通信网络。IEEE 802委员会制定了一系列局域网标准，称为IEEE 802标准。目前，大多数局域网使用的拓扑结构主要有星型、环型和总线型3种。从目前的发展情况来看，局域网可以分为共享式局域网和交换式局域网两大类。对于共享式局域网中，采用的介质访问控制方法有CSMA/CD介质访问控制、令牌环（Token Ring）介质访问控制和令牌总线（Token Bus）介质访问控制。

由于在局域网技术中，以太网的应用最为广泛，因此本章重点介绍了以太网技术，包括传统以太网，以及快速以太网、千兆以太网和万兆以太网等目前比较流行的高速局域网。其中，快速以太网已大量使用在桌面系统，而千兆以太网则被广泛用于校园网、园区网或企业网的主干网上，它们各有优缺点。

交换技术可以说是局域网技术的一场革命，它已成为网络的主导技术，因此本章对交换式局域网从本质上进行了分析并说明了它与共享式局域网的根本区别。交换式网络具有独享带宽、独占通信链路的特征，因此它能提供足够的带宽。交换式网络还支持先进的虚拟网络技术，通过软硬件的配置，能根据业务性质、网络应用或组织机构等自定的原则，灵活地划分子网。

本章还介绍了虚拟局域网（IEEE 802.1q）技术和无线局域网（IEEE 802.11）技术。虚拟局域网（VLAN）是指在交换式局域网的基础上，采用网络管理软件构建的可跨越不同网段、不同网络的端到端的逻辑网络。而无线局域网（WLAN）是采用无线传输介质的局域网，是有线局域网的延伸。

# 网络互联技术

## 了解计算机网络互连的基本概念；

**网络互连的主要原因：**

**（1）扩展网络覆盖范围的需要。**

**（2）扩大资源共享范围的需要**

**（3）网络分割的需要。**

**网络互连的类型：**

**（1）局域网（LAN）—局域网（LAN）互连。如：以太网与令牌网互连、以太网与ATM网互连。**

**（2）局域网（LAN）—广域网（WAN）互连。如：企业网、校园网通过电信接入Internet。**

**（3）局域网（LAN）—广域网（WAN）—局域网（LAN）互连。如：全球型企业的专用网。**

**（4）广域网（WAN）—广域网（WAN）互连。如：因特网是广域网互连的典型例子。**

**实现网络互连的基本要求:**

（1）在互连网络之间至少应当有一条在物理上连接的链路以及对这条链路的控制规程。

（2）在不同网络节点的应用程序间提供适当的路径来传递数据。

（3）协调各个网络的不同特性，不对参与互连的某个网络的硬件、软件、网络结构或协议做大的修改。

（4）不能为提高整个网络的传输性能而影响各子网的传输性能。

（5）向互连的网络提供不同层次的服务功能，包括协议的转换，分组的分段、组合和重定序以及差错检测等。

## 了解常用网络互连介质的特性和用途；

网络互连介质是连接各网络节点，承载网络中数据传输功能的物理实体。如果将网络中的计算机比作货站，数据比作汽车的话，那么网络互连介质就是不可缺少的公路。根据介质的物理特征，网络互连介质分为有线传输介质和无线传输介质两大类。目前常用的有线传输介质有双绞线、同轴电缆和光纤等，常用的无线传输介质有无线电波、微波和红外线等。

## 掌握双绞线的制作与测试方法；

剪断：利用压线钳的剪线刀口剪取适合布线长度的网线。

剥皮：用剥线刀口，划开双绞线的保护胶皮，长度3～5厘米，拔下胶皮。

排序：剥除外皮后再用力拔出4对双绞线，使双绞线外皮后退，首先按橙、蓝、绿、棕的颜色顺序从左到右排放（T568B标准），下来将4对双绞线解开、捋直，带白花的线在左，全色线在右，再将“蓝-白”线与“绿-白”线对换位置，最后将排序好的一排8根双线上下左右弯折、理顺，用指甲掐紧、挤进成扁平电缆带状。

剪齐：用压线钳剪线刀将理顺成扁平状的8根线剪齐，留在皮外长度2厘米左右。

插入：一手以拇指和中指捏住水晶头，使有塑料弹片的一侧向下，针脚一方朝向远离自己的方向，并用食指抵住，另一手捏住双绞线外面的胶皮，缓缓用力将8条导线同时沿RJ-45水晶头内的8个线槽插入到底；此时最好将外皮也能进入水晶头内部，这样压紧效果好。

压制：确认所有芯线都插到水晶头底部、线序无误后，可将水晶头直接放入压线钳的压线缺口中，用力压下，使金属片压下后刺破芯外层绝缘与线芯良好接触。可多压一次，增加可靠性。

检测：两端都做好的水晶头，可用网线测试仪进行测试，如果测试仪上8个指示灯按照派线顺序依次为绿色闪过，证明网线制作成功。如果出现任何一个灯不亮（或者为红灯、黄灯），都证明存在断路或者接触不良现象，此时最好先对两端水晶头再用网线钳压一次，再测，如果故障依旧，再检查一下两端芯线的排列顺序是否正确，如果不正确，则需要剪掉一端重新参照另一端芯线排列顺序制做水晶头。如果芯线顺序正确，但测试仪在重测后指示灯仍然不亮（或者显示红色灯、黄色灯），则表明其中肯定存在对应芯线接触不好，此时需要剪掉一端参照另一端芯线顺序重做一个水晶头了；再测，如果故障消失，则不必重做另一端水晶头，否则还得把原来的另一端水晶头也剪掉重做，直到测试全为绿色指示灯闪过为止。

## 掌握各层次网络互连设备的作用、特点与用途；



网络互连层次与互连设备示意图

**中继器**

中继器（Repeater）又称为转发器，是最简单的网络互连设备。中继器常用于在两个网络节点的物理层之间按比特位双向传递物理信号，完成信号的复制、调整和放大功能，以扩大数据的传输距离。安装简单，使用方便，价格相对低廉。广泛应用于局域网、广域网的互连及数据通信领域。

**集线器**

集线器（Hub）也称为集中器，是一种特殊的多端口中继器，用于连接多个设备和网段。集线器的主要功能是对接收到的信号进行再生、整形、放大，以扩大网络的传输距离，同时把所有节点集中在以它为中心的节点上。在局域网中得到了广泛的应用。

**网桥**

网桥（bridge）也叫桥接器，是连接两个或多个在数据链路层以上具有相同或兼容协议的局域网的一种存储转发设备；将网桥分为透明网桥和源路由网桥

特点：

（1）网桥能将一个较大的局域网分割为多个较小的局域网，进而分隔较小局域网之间的广播通信量，有利于提高互连网络的性能与安全性。

（2）网桥能将两个以上相距较远的局域网互连成一个大的逻辑局域网，使局域网上的所有用户都可以访问服务器，扩大网络的范围。

（3）网桥可以互连两个采用不同数据链路层协议、不同传输介质或不同传输速率的网络，但这两个网络在数据链路层以上应采用相同或相兼容的协议。

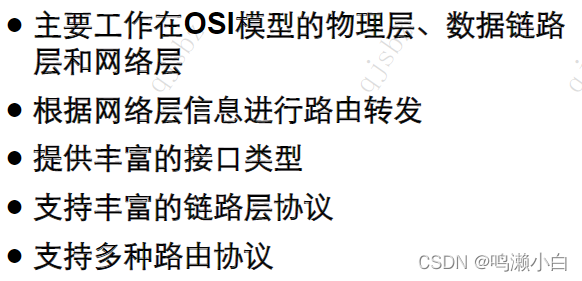
（4）网桥以“存储—转发”的方式实现互连网络之间的通信。

**二层交换机**

二层交换机工作在OSI参考模型的数据链路层，其本质是网桥。但网桥一般只有两个端口，而交换机通常有多个端口，如12口、24口、48口等，所以又可称二层交换机为多端口网桥。网桥在发送数据帧前，通常要对接收到的完整的数据帧执行帧检验（FCS），而交换机在一个数据帧接收结束前就可以发送该数据帧了。功能包括物理编址、构建网络拓扑结构、错误校验、传输数据帧序列以及流量控制。

**路由器**

路由器（Router）是一种连接多个相同或不同类型网络的网络互连设备，它具有按某种准则自动选择一条到达目的子网的最佳传输路线的能力，用来连接两个及以上复杂网络。把各个子网在逻辑上看作为多个独立的整体。路由器的作用就是完成这些子网之间的数据传送，它从一个子网接收输入的分组，然后向另一个子网转发。



**三层交换机**

三层交换机是一种在二层交换机的基础上增加了三层路由模块，能够检查数据包信息，并根据IP地址转发数据包，在网络层实现数据包高速转发，以及在多个局域网间完成数据传输的网络互连设备。三层交换机对数据包（或分组）的处理与传统路由器相似，它可以实现如路由信息的更新、路由表维护、路由计算、路由确定等功能。

1. 所有vlan都是独享一个物理接口速率，网络瓶颈不容易参数
2. 不存在单点故障
3. 配置简单
4. 传递效率高

广泛应用于校园网、城域教育网中

**网关**

网关（Gateway）又称网间连接器或协议转换器，按照网关的应用功能不同，网关可分为协议网关、应用网关和安全网关3种类型。

用于将两个或多个在OSI参考模型的传输层以上层次使用不同协议的网络连接在一起，并在多个网络间提供数据转换服务的软件和硬件一体化设备。

在互连的、不同结构的网络中的主机之间相互通信时，由网关完成这两种网络的数据报格式的相互转换，以实现不同网络协议的翻译和转换工作。例如，如果要将使用TCP/IP协议的微软系统与使用SNA系统的银行系统互连，则这两个网络系统之间需要用网关进行转换

## 了解常用路由协议 RIP、OSPF、BGP的工作原理和应用。

**RIP（路由信息协议）的工作原理：**

RIP使用跳数来衡量到达目的地的距离，即使用跳数作为路由度量值。跳数是指数据从源地址到达目的地址之间经过的路由器个数。从路由器到直接连接的网络的跳数定义为1，每经过一个路由器则数值加1。RIP允许的跳数最大为15跳，超过15跳的网络将无法到达，因此RIP一般适用于规模较小的同构网络。RIP共有3个版本：RIPv1、RIPv2和RIPng。RIPng应用于IPv6的网络环境中，而RIPv1和RIPv2则用于IPv4的网络环境中

**OSPF（开放最短路径优先）协议工作原理：**

OSPF需要每个路由器向其同一管理域的所有其他路由器发送链路状态广播信息。在OSPF的链路状态广播中包括所有接口信息、所有的量度和其他一些变量。使用OSPF的路由器首先必须收集有关的链路状态信息，并根据一定的算法计算出到达每个节点的最短路径。网络规模、网络拓扑、其他特殊要求路由自身要求；

**BGP（边界网关协议）工作原理：**

边界网关协议（Border Gateway Protocol，BGP）是为TCP/IP互联网设计的外部网关协议，用于多个自治系统之间。目前使用最多的版本是BGP-4，简写为BGP。BGP既不是基于纯粹的链路状态算法，也不是基于纯粹的距离向量算法。它的主要功能是与其他自治系统的BGP交换网络可达信息。各个自治系统可以运行不同的内部网关协议。

内部网关协议（IGP）的功能是完成数据在AS内部的路由选择，只作用于本地AS内部；而外部网关协议（BGP）是完成数据在AS之间的路由选择，只了解AS的整体结构，而不了解每个AS内部的拓扑结构。

**小结：**

本章主要内容是介绍如何将多个独立的局域网互连为一个规模更大、网络覆盖面积更广的互联网，以实现更大范围的资源共享和信息交流。文中讨论了网络互连的主要原因、互连形式、基本要求，常用的互连介质和互连设备，以及路由协议。

网络互连的核心是网络之间的硬件连接和网间互连协议。网络的物理连接是使用网络互连设备通过传输线路实现的，旨在为局域网之间提供一条用于传输数据的物理通道。网络互连设备极其重要，它直接影响着互联网的性能。所以本章着重介绍了工作在不同层次的网络互连设备的功能特性和应用场合，以及各种设备的差异。网络互连设备包括：工作在物理层的中继器和集线器；工作在数据链路层的网桥和第二层交换机；工作在网络层的路由器和三层交换机，以及工作在传输层以上的网关。

路由选择算法是用于判定数据到达目的地的最佳路径的方法，而路由协议则是实现路由算法的一系列规则和约定。常见的路由协议有内部网关协议（IGP）和边界网关协议（BGP）。其中，内部网关协议又分为路由信息协议（RIP）和开放式最短路径优先（OSPF）协议。

# 网络安全

## 了解网络安全的概念、网络面临的威胁以网络安全的内容；

网络安全是指网络系统的硬件、软件及数据受到保护，不遭受偶然的或者恶意的破坏、更改、泄露，系统能够连续、可靠、正常地运行，网络服务不中断。从本质上讲，网络安全问题主要就是网络信息的安全问题。凡是涉及网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论，都是网络安全的研究领域。

**网络面临的安全威胁**

1. **黑客的恶意攻击**
2. **计算机网络系统的漏洞与缺陷**
3. **网络信息安全保密问题**
4. **网络病毒**
5. **网络内部安全问题**

网络安全涉及的内容包括技术和管理等多个方面，需要相互补充、综合协同防范。其中，技术方面主要侧重于防范外部非法攻击，管理方面则侧重于内部人为因素的管理。从层次结构上，可将网络安全的内容概括为以下5个方面。

（1）实体安全

（2）系统安全

（3）运行安全

（4）应用安全

（5）管理安全

## 了解数据加密技术、数字签名技术和身份认证技术；

数据加密是通过某种函数进行变换，将正常的数据报文（称为明文）转变为密文（也称为密码）的方法。解密是加密的逆操作。用来将明文转换为密文或将密文转换为明文的算法中输入的参数称为密钥。

加密技术一般分为对称加密技术和非对称加密技术两类。对称加密技术是指加密和解密使用同一密钥。非对称加密技术是指加密和解密使用不同的密钥，分别称为“公钥”和“私钥”，两种密钥必须同时使用才能打开相应的加密文件。公钥可以完全公开，而私钥只有持有人持有。

数字签名是一种信息认证技术，它利用数据加密技术、数据变换技术，根据某种协议来产生一个反映被签署文件和签署人的特征，以保证文件的真实性和有效性，同时也可用来核实接收者是否存在伪造、篡改文件的行为。简单地说，数字签名就是只有信息的发送者才能产生的别人无法伪造的一段数字串，这段数字串同时也是对信息的发送者发送信息真实性的一个有效证明。

数字签名必须保证以下3点：

（1）接收者能够核实发送者对消息的签名。

（2）发送者事后不能抵赖对消息的签名。

（3）接收者不能伪造、篡改对消息的签名。

用户身份认证机制可划分为身份标识和身份认证两个组成部分

身份标识：为用户建立能够确认其身份状况的信息的过程

身份认证：系统确定用户合法身份的过程

## 了解防火墙技术；

防火墙（Firewall），是指位于两个或多个网络间，实施网络之间访问安全控制的一组组件的集合。防火墙有多种形式，有的以软件形式运行在普通计算机上，有的以硬件形式集成在路由器中。最常见的分类方式将防火墙分为两类，即包过滤型防火墙和应用级防火墙。

在应用级防火墙技术的发展过程中，经历了两个不同的版本。

**第一代应用网关型防火墙**

**第二代自适应代理型防火墙**

## 了解计算机防病毒技术。

计算机病毒具有以下几个明显的特征。

**（1）传染性。**

**（2）破坏性。**

**（3）隐蔽性。**

**（4）潜伏性。**

**（5）寄生性。**

**计算机病毒分类**

1. **按攻击的操作系统分类**

可分为DOS病毒、Windows病毒、Linux病毒、Unix病毒等，它们分别是发作于DOS、Windows、Linux、Unix操作系统平台上的病毒。

1. **按链接方式分类**

可分为源码型病毒、嵌入型病毒、外壳型病毒和操作系统型病毒4种。

（3）**按存在的媒体分类**

可分为引导型病毒、文件型病毒和混合型病毒3种。

为了将病毒拒之门外，用户要做好以下防范措施。

1. **建立良好的安全习惯**
2. **关闭或删除系统中不需要的服务**
3. **及时升级操作系统的安全补丁**
4. **为操作系统设置复杂的密码**
5. **安装专业的防病毒软件**
6. **定期进行数据备份**

**小结：**

网络安全是指网络系统的硬件、软件及数据受到保护，不遭受偶然的或者恶意的破坏、更改、泄露，系统能够连续、可靠、正常地运行，网络服务不中断。目前，网络面临着众多的安全威胁，使用数据加密技术、防火墙技术和防病毒技术有利于提高网络的安全性。

数据加密技术是实现数据机密性保护的主要方法。加密技术一般分为对称加密技术和非对称加密技术两类。数字签名是公开密钥加密技术和报文分解函数相结合的产物，只有信息的发送者才能产生的别人无法伪造的一段数字串，这段数字串同时也是对信息的发送者发送信息真实性的一个有效证明。

防火墙作为保护局域网的第一道屏障与实现网络安全的一个有效手段，在实际中得到了广泛地应用。最常见的分类方式将防火墙分为两类，即包过滤型防火墙和应用级防火墙。

病毒的广泛传播给网络带来了灾难性的影响。因此，每个用户都应遵守病毒防范的有关措施，不断学习、积累防病毒的知识和经验，培养良好的病毒防范意识。