计算机网络与信息安全

第3章
CHAPTER 3

3.1 任务导入

小强大学即将毕业，经过重重选拔，他如愿进入了自己心仪的企业实习，实习第1天部门就给小强分配了一台新的台式计算机，小强激动地领到了自己的新计算机。根据自己所学的知识，小强快速地完成了电源、显示器、鼠标、键盘、网线等硬件设备的安装，开机发现新计算机里已经安装了很多常用软件，但打开QQ、微信都不能登录，网页也无法正常打开，原来是这台计算机的网络没有正常连接。平时小强都是使用笔记本电脑或者手机连接无线网络，但这台台式机却没有安装无线网卡，找不到连接无线网的地方。此时小强不能接收企业导师发送的学习资料，也不能进入公司的资源库获取企业的内部资料，一时间小强有点不知所措。

另外，小强实习的这家公司高度重视企业信息安全，除了要求员工的计算机必须按要求安装杀毒软件和配置防火墙之外，公司的重要资料文件也仅限内部流通，对于刚进入职场的小强来讲，如何在工作中高效地完成工作并遵守公司的信息安全要求呢？

本章旨在向小强普及计算机网络和信息安全的相关知识，包括计算机网络的组成、网络结构、网络安全知识和计算机病毒、木马和数据安全防护等，培养信息安全意识，让小强根据企业和自己的工作学习需求配置工作计算机的IP地址、网关等网络信息，配置防火墙并使用杀毒软件进行检测，并学会简单的互联网日常办公应用，例如通过网络搜索和本地搜索获取所需的资源，有效发送电子邮件，使用FTP上传和下载资源等。

3.2 知识学习

3.2.1 计算机网络的概念

21世纪是信息化、数字化、智能化高速发展和广泛应用的时代，但无论是智能化、数字化还是信息化都离不开一个最基本的网络化，没有网络化它们都不可能实现。谈到网络化，

类似蜘蛛网一样的网状结构必然在脑海中浮现,大家熟悉的高速公路网、高铁交通网、地铁交通网都是网络,都是通过不同的线路连接各个地点,运送人员或者物资。

与交通网络类似,计算机网络则是将地理位置不同的具有独立功能的多台计算机及其外部设备,通过通信线路连接起来,在网络操作系统、网络管理软件和网络通信协议的管理和协调下,实现资源共享和信息传递为目标的计算机系统。

计算机通信与计算机网络有着密切的联系,又有各自的特点。计算机通信主要是计算机与计算机之间的数据传输和数据处理,不一定形成一个网络,而计算机网络则是强调在网络范围内计算机资源的共享和传递,但计算机网络必定需要以计算机通信为基础才能实现其功能,是计算机系统发展和通信系统发展相结合的产物,是一个非常复杂的结构。

3.2.2 计算机网络的发展史

1. 第 1 代计算机网络

第 1 代计算机网络是以单个主机为中心面向终端的联机网络。在 20 世纪 60 年代早期,基本采用的是一台计算机主机,通过线缆连接多台终端。此时的终端只有键盘和显示器,没有运算器和存储器,不能单独进行数据处理,也没有任何数据可共享。该系统中只有主机拥有数据的处理能力和存储能力,用户通过终端进行数据输入和显示。当时的通信网络也只有固定电话网络,主机和终端也可以通过调制解调器接入公共固定电话网络,实现与异地终端的数据传输和分享。第 1 代计算机网络主机是网络的中心和控制者,只提供终端和主机之间的通信,子网之间无法通信。典型的代表是 1954 年美国军方建立的半自动地面防空系统。第 1 代计算机网络的组成如图 3-1 所示。

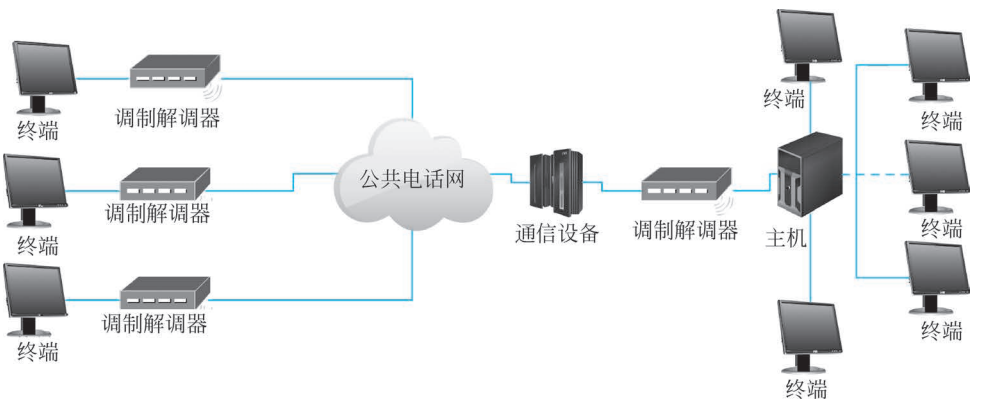


图 3-1 第 1 代远程终端联机系统

2. 第 2 代计算机网络

20 世纪 60 年代中后期,随着通信交换技术的发展,第 2 代计算机网络迎来了突破性的发展,在第 1 代计算机网络的基础上,不再仅使用功能简单的终端,而是实现了多个主机通过通信线路互联,通过实现主机互联资源共享,并以分组交换为主,可以实现负载均衡,从而大大提高了单机的响应速度。典型代表是美国国防部高级研究计划局协助开发的

ARPANET。第 2 代计算机网络的组成如图 3-2 所示。

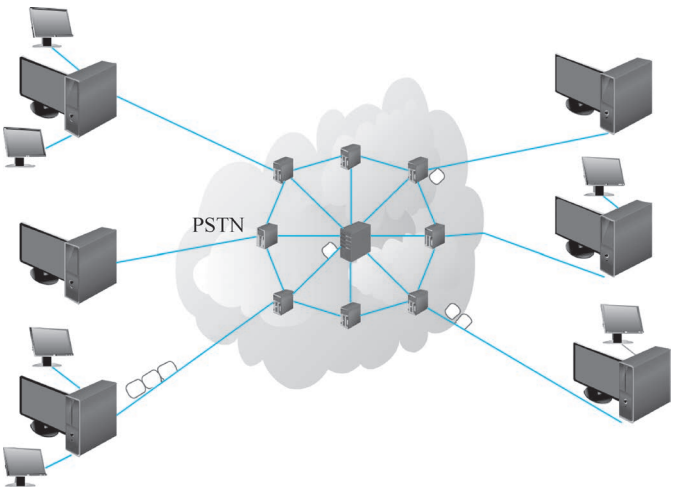


图 3-2　第 2 代计算机网络系统

3. 第 3 代计算机网络

第 2 代计算机网络存在不同硬件和软件厂家的网络之间，不能实现互联互通，世界标准化组织成立并制定了全球统一的网络体系结构，这就是 20 世纪 80 年代早期出现的开放系统互连参考模型（Open Systems Interconnection，OSI）参考模型。因为第 3 代计算机网络基于 OSI 模型，实现了不同厂家生产的计算机之间的互联互通，可以说第 3 代计算机网络进入了计算机网络的成熟阶段。第 3 代计算机网络主要具有以下几个特点：

（1）网络体系结构的形成和网络协议的标准化。

（2）建立了全网统一的通信规则。

（3）使计算机网络对用户提供透明的服务。

4. 第 4 代计算机网络

随着计算机处理数据能力的增强和多媒体数据量的增多，对网络传输和数据处理能力也有了更高的要求，公共电话网已经不能满足网络发展的需求。1993 年，美国提出了建设信息高速公路的概念，加快信息基础设施的建设。1995 年，多国签署了共同建设国际互联网的协议，将世界各地分散的网络连接起来，实现更大范围内的资源共享和信息交换。除了快速以太网、光纤分布式数字接口（FDDI）、快速分组交换技术（包括帧中继、ATM）、千兆以太网、B-ISDN 等一系列新型网络技术相继出现之外，计算机网络进入了高速和综合化发展阶段。互联网是第 4 代计算机网络的典型代表，目前已经成为人类最重要的、最大的知识宝库。

3.2.3　计算机网络的特点

计算机网络主要具有资源共享、高效数据交换、扩展性、分布式处理、高可靠性等特点。

（1）资源共享：资源共享是计算机网络最突出的特点。在计算机网络中，用户可以共

享网络中的主机、外设硬件和软件等资源，实现资源的无地域共享。用户之间可以分工合作，共同完成任务，这有利于提高系统资源的利用率，减少重复资源的投资，并节约成本。

(2) 高效数据交换：计算机网络的数据通信功能可以满足计算机与终端之间或计算机与计算机之间各种信息的快速传送。计算机网络的数据通信功能拉近了用户之间的距离，克服了地域限制。日常生活中，人们可以利用计算机网络实现相互之间的远距离联系，交换语音、视频信息和文件，发送和接收邮件，甚至可以远距离完成协同作业。改变了传统的通信手段，如电报、电话、传真和写信，为人们的生活带来了极大的便利。

(3) 扩展性：通过网络连接，可以快速扩展网络。新的网络只要接入互联网，即刻成为互联网的一部分，从而参与网络的互联互通和信息资源的交换共享。

(4) 分布式处理：当网络中的某台计算机的任务负荷过重时，可以通过网络和应用程序进行控制和管理，将任务分散到网络中的其他计算机上运行，或者由网络中比较空闲的计算机分担负荷，这样可以大大地提高工作效率并降低成本。

(5) 高可靠性：在一些用于计算机实时控制和要求高可靠性的场景中，通过计算机网络实现备份技术可以提高计算机系统的可靠性。网络中的每台计算机都可相互成为后备机，一旦某台计算机出现故障，它的任务就可由备份计算机代为完成，可以避免在单机情况下，一台计算机发生故障而引起整个系统瘫痪，提高系统的可靠性。

3.2.4 计算机网络的分类

计算机网络的类型划分标准有很多种，例如可以按照网络的覆盖范围划分、按照网络的通信介质划分、按照网络的通信方式划分、按照网络的拓扑结构划分等，其中最常见的是根据网络的覆盖范围划分，计算机网络可分为局域网、城域网、广域网和互联网。

(1) 局域网(Local Area Network，LAN)是最常见、应用最广的一种计算机网络。局域网是指在局部范围内的网络，其覆盖的地区范围较小。随着计算机网络技术的发展和提高，局域网得到了充分应用和普及，大部分单位和家庭拥有自己的局域网。局域网的规模可以从只有两台计算机到几百台不等，其配置上没有太多的限制。局域网的覆盖范围可以从几米到 10 千米以内。局域网只能在内部互相通信，信息共享度较低，但实现了物理隔离，因此信息安全性较高。

(2) 城域网(Metropolitan Area Network，MAN)是指在一座城市范围内的计算机网络，属于宽带局域网。城域网采用具有有源交换元器件的局域网技术，具有较低的传输时延，其传输媒介主要采用光缆，传输速率在 100 兆比特/秒以上。城域网的一个重要用途是作为骨干网，将位于同一城市内不同地点的主机、数据库及局域网等相互连接起来。城域网相对比较安全，可以进行适度共享。

(3) 广域网(Wide Area Network，WAN)，又称为外网、公网，通常跨越很大的物理范围，覆盖的范围从几十千米到几千千米不等。它能连接多个地区、城市和国家，甚至可以横跨几个洲，并提供远距离通信，形成国际性的远程网络。广域网是连接不同地区的局域网或城域网的远程网络，但广域网并不等同于互联网。例如某企业在众多城市拥有分公司，甚至

有海外分公司，可以通过广域网以专线的方式将这些分公司连接起来，这就被称为“广域网”。因为广域网采用专线，所以价格比较昂贵，但安全性较高。

（4）互联网（Internet），又称为国际互联网络，指的是将多个网络相互连接而形成的庞大网络。这些网络以一组通用的 TCP/IP 协议相连，形成逻辑上的单一巨大国际网络。互联网实现了全球信息的高度共享，但也存在着很大的安全隐患。

另外，计算机网络按照网络拓扑结构分类也是比较常见的。根据不同的网络拓扑结构，可以将计算机网络分为星状、树状、总线型、环状和网状等。

3.2.5　数据在计算机网络中的传输

数据本来存储在计算机网络中的一个设备的硬盘或者存储设备中。那么数据是如何从这个网络设备的存储设备中传输或共享给另外的网络设备的呢？

例如在日常生活中，用户通过 QQ、WeChat 等即时聊天工具，手指轻轻单击一下，文字、图片、语音或者视频等数据就发送到另外一用户端了，给人感觉是一种极其简单的操作，但事实上，数据传输过程是非常复杂的过程。应用数据需要加上 TCP 头、IP 头、MAC 地址等层层包裹后，通过传输介质发送到交换机。交换机根据 MAC 地址表匹配 MAC 地址与接口的对应关系，确定发送的接口将数据发送给路由器，路由器通过路由表查询到 IP 对应的下一跳地址，将数据发送到对应的目标设备上。

如果要想真正理解这个复杂而专业的过程，则必须充分理解计算机网络的组成和工作原理。下面将从计算机网络的组成、拓扑结构等方面进行介绍。

3.2.6　计算机网络组成

计算机网络由硬件系统和软件系统组成。

1. 计算机网络的硬件系统

计算机网络的硬件系统具体包括计算机终端设备、网络设备和传输介质。

1）计算机终端设备

计算机网络中的计算机终端设备可能是 PC、笔记本、智能手机，还可能是摄像头、电冰箱、智能电视等，可以是存在于网络节点中的物理主机，也可以是虚拟主机或云主机。根据终端设备的功能还可以分为服务器端和客户端，服务器端是整个网络的核心，为网络用户提供服务并管理整个网络，客户端是用户与网络进行信息交换和资源共享的接口设备。常见的计算机终端设备如图 3-3 所示。

2）网络设备

网络设备是计算机网络的骨架，是搭建计算机网络系统的拓扑结构所用到的设备，常见的网络设备有网卡、交换机、路由器、硬件防火墙等。

（1）网卡：网卡又称为网络适配器或者网络接口卡，是计算机连接到网络通信介质上进行数据传输的硬件设备。每张网卡都有处理器和存储器，每张网卡都有一个独一无二的 MAC 地址作为标识，两张网卡不可能拥有相同的 MAC 地址。

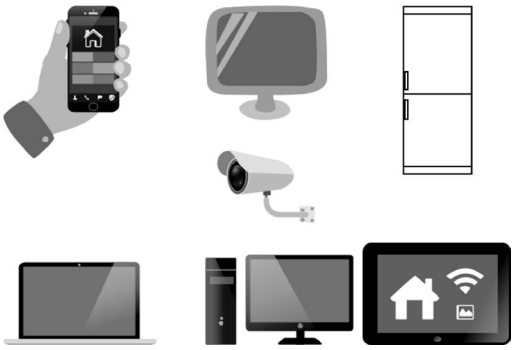


图 3-3　常见计算机终端设备

(2) 交换机：交换机又叫交换式集线器，是电/光信号转发的网络设备。交换机主要用于连接局域网中的设备，通过交换机连接的每台设备都有自己的 IP 地址。交换机除了能够连接相同类型的网络之外，还可以连接不同类型的网络，例如连接以太网和快速以太网。

交换机的主要功能包括物理编址、网络拓扑结构、错误校验、帧序列和流控等。随着交换机的发展，新一代交换机还具备支持虚拟局域网、支持链路汇聚功能，有些甚至还具有防火墙功能。

交换机从传输介质和传输速度上可分为以太网交换机、快速以太网交换机、千兆以太网交换机、FDDI 交换机、ATM 交换机和令牌环交换机等。目前为止，普及率最高的短距离二层计算机网络是以太网，而以太网的核心部件就是以太网交换机。

普通的交换机是工作在 OSI 参考模型的第 2 层数据链路层的，这类交换机又叫层二交换机，层二交换机不具备路由转发功能。随着交换机的发展，出现了具备路由转发功能的三层交换机，三层交换机工作在 OSI 的网络层。2010 年之前全球交换机市场占比最高的是思科公司出品的交换机，但目前几乎已经被我国的华为公司出品的交换机替代。交换机如图 3-4 所示。

图 3-4　交换机

(3) 路由器：路由器是连接两个或多个网络的硬件设备，是互联网的主要节点网关设备，是专用智能的网络设备，路由器系统构成了基于 TCP/IP 的国际互联网络 Internet 的骨架。路由器能够理解不同的协议，是不同网络之间进行连接的枢纽，起到网关的作用，读取每个数据包中的地址，然后决定如何传送。

路由器工作在 OSI 模型的第 3 层，即网络层，它的功能就是在 OSI 模型中完成网络层的中继任务，对不同的网络之间的数据包进行存储、分组转发。

路由器作为网关设备，可以用来划分公网和局域网，也可以通过局域网端口将局域网划

分为多个子网。公网端口是单独的网卡，具有公网 IP 和 MAC 地址，局域网子网每个端口也有单独的网卡，也有该子网网段的 IP 和 MAC 地址。

无线路由器是供小范围或者家庭使用的路由器，带有无线覆盖功能，可看作一个网络信号转发器。目前市场上常用的无线路由器一般支持多种接入方式，还具备一些网络管理功能，如 DHCP 服务、NAT 防火墙、MAC 地址过滤、动态域名管理等功能。常见路由器如图 3-5 所示。

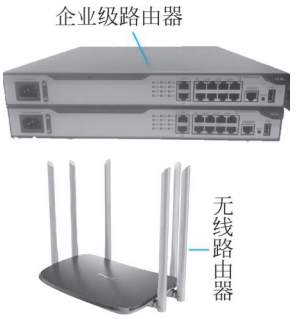


图 3-5　常见路由器

（4）硬件防火墙：硬件防火墙是一种物理网络设备，类似于计算机流量的过滤服务器。将网线连接到防火墙，将防火墙定位在上行链路和计算机之间。防火墙采用强大的网络软硬件组件，使用可配置的规则集强制检查所有通过该设备的流量，相应地授予或拒绝访问。

硬件防火墙是一种物理网络设备，类似于计算机流量的过滤服务器。将网线连接到防火墙，将防火墙定位在上行链路和计算机之间。防火墙采用强大的网络软硬件组件，使用可配置的规则集强制检查所有通过该设备的流量，相应地授予或拒绝访问。

硬件防火墙充当了计算机网络和互联网之间的过滤器。它监视数据包并确定在传输过程中是否阻止或传输它们。硬件防火墙用于保护整个网络及传入和传出流量，使网络管理员能够控制网络的使用方式，无须在每台设备上单独安装，节省了大量时间和资源。常见硬件防火墙如图 3-6 所示。

图 3-6　硬件防火墙

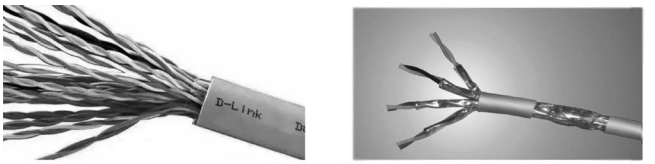
3）传输介质

传输介质也就是通信线路，是数据信息在网络通信中的路径，传输介质可以是有线的，也可以是无线的。常见的有线介质有双绞线、铜轴电缆、光纤等。

（1）双绞线：双绞线是常用的传输介质，可以传输模拟或者数字信号，一般可以传输几千米到十几千米的距离。双绞线是由两根相同的绝缘铜导线相互缠绕而形成的一对信号线，其中一根是信号线，另一根是地线，两条线缠绕可以减少相互之间的信号干扰。

根据有无屏蔽层，双绞线可以分为屏蔽式双绞线和非屏蔽式双绞线。非屏蔽式双绞线由 4 对不同颜色的传输线所组成，被广泛地用于以太网和电话线中。屏蔽式双绞线在双绞线与外层绝缘封套之间有一层金属屏蔽层，屏蔽层可减少辐射，防止信息被窃听，也可阻止外部电磁干扰的进入，使屏蔽式双绞线比同类的非屏蔽式双绞线具有更高的传输速率，然而，在实际施工时，很难完美地接地，屏蔽层本身成为最大的干扰源，导致性能远不如同类非屏蔽式双绞线，因此，除非有特殊需要，在综合布线系统中通常采用非屏蔽式双绞线。双绞

线如图 3-7 所示。



非屏蔽式双绞线　　屏蔽式双绞线

图 3-7　双绞线

双绞线按照频率和信噪比还可以分为一类线(CAT1)、二类线(CAT2)、三类线(CAT3)、四类线(CAT4)、五类线(CAT5)、超五类线(CAT5e)、六类线(CAT6)、超六类或6A 线(CAT6A)和七类线(CAT7),而最常见的是三类线、五类线、超五类线和六类线。

(2) 同轴电缆:同轴电缆一般由 5 层组成:最内层铜芯导体是一根导电铜线,铜线的外面有一层绝缘体塑料,绝缘塑料外又有一层薄的铝箔,再外层是铜或合金的网状导电体,导电体外面是最外层的绝缘外皮。同轴电缆及其组成如图 3-8 所示。

图 3-8　同轴电缆及其组成

同轴电缆可用于模拟信号和数字信号的传输,适用于有线电视传播、长途电话传输、计算机系统之间的短距离连接及局域网传输等。在过去固网的时代,同轴电缆曾是长途电话网的重要组成部分,但如今大多被光纤、微波和卫星替代。

(3) 光纤:光纤是光导纤维的简写,是一种由玻璃、塑料或者硅制成的直径为 50～100μm 的纤维,是一种根据“光的全反射”原理能传播光波的介质。光纤主要由纤芯和包层构成双层同心圆柱体,纤芯由玻璃、塑料或者硅拉丝而成,它是光波的通道,是光纤的核心。光纤如图 3-9 所示。

光纤　　纤芯

图 3-9　光纤

光纤按传输点的模数可以分为单模光纤和多模光纤，当光纤的直径非常小且小到只有一个光的波长时，可以使光一直向前沿着一条路径传播，不会产生多次反射，这样的光纤称为单模光纤，而光纤直径相对较大，在一条光纤中光波会有多条路径传播，称为多模光纤。多模光纤适用于距离比较短的传输，一般不超过 500m，目前市场上基本不再使用多模光纤，而单模光纤的传输距离非常远，现在大量网络铺设的是单模光纤。单模光纤和多模光纤的传输如图 3-10 所示。

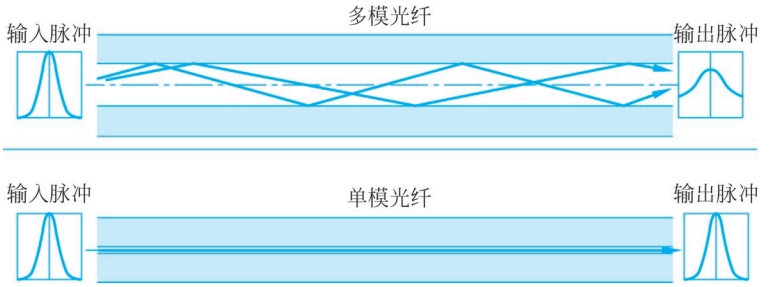


图 3-10　单模光纤和多模光纤的传输

光纤以光脉冲进行通信，传输带宽远超其他介质，以光速进行数据传输，传输速度非常快，并且光纤传输损耗小，中继距离长，抗雷电和电磁干扰性能也很好，体积小，质量轻，价格也便宜，因此目前光纤在通信网络中被广泛地应用，几乎替代了同轴电缆。不过光纤质地非常脆弱，机械强度差，容易受损，并且具有怕水等缺点。光纤作为国家的通信基础设施，各个单位和个人在施工和作业的过程中都需要注意光纤标识，保护好它们。

（4）无线传输介质：常见的无线传输介质包括无线通信、微波通信，是一种无形的、看不见的传输介质。

无线通信即无线短波通信，通过基站或者路由器进行信号的转发，例如目前大部分家庭有 WiFi，人手必备的手机采用的是无线通信。无线通信的特点是覆盖范围广，不受地理环境影响，成本低，使用非常方便，但是也有传输速度慢、抗干扰能力和安全性差的缺点。

微波通信包括地面微波和卫星通信两类，地面微波接力靠的是直线可见的微波站进行中继接力，每隔 50 千米左右就需要设置一个中继站。微波接力如图 3-11 所示。

卫星通信靠同步卫星作为中继，实现微波信号的远距离通信，例如使用 3 颗卫星就可以实现全球覆盖，容量大，通信质量较好，但是延时较长。例如中国北斗卫星导航系统、美国全球 GPS 定位系统都是非常成功的卫星通信案例。卫星通信如图 3-12 所示。

2. 计算机网络的软件系统

计算机网络除了必备的硬件外，还离不开软件的配合，计算机网络的软件系统包含网络操作系统、网络协议和网络设备软件。

1）网络操作系统

网络操作系统指的是能使网络上各个计算机方便有效地共享网络资源，为用户提供所需的各种服务的操作系统，是网络的心脏和灵魂。网络操作系统不仅具备普通操作系统的

功能,还必须提供网络安全性管理和服务功能,如远程管理、文件传输、数据库服务、电子邮件、远程打印等网络服务功能。网络操作系统负责管理和控制计算机的软硬件资源,是网络用户和计算机网络的接口。

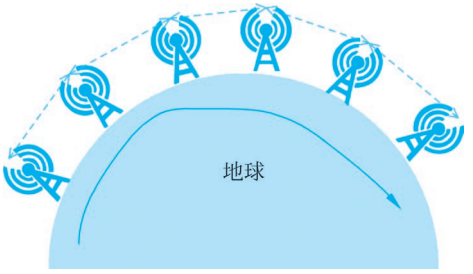


图 3-11 微波中继

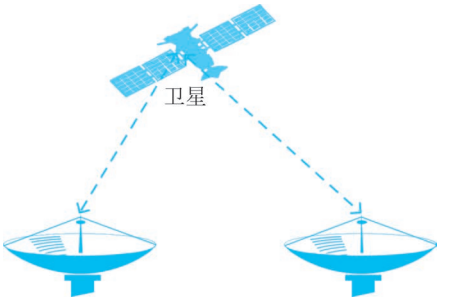


图 3-12 卫星通信

常见的网络操作系统有 UNIX、Linux、NetWare、HarmonyOS 和 Windows 等,用户可以根据实际需求选择合适的网络操作系统。

UNIX 网络操作系统由 AT&T 和 SCO 公司推出,常用的版本主要有 UNIX System V Release 4.0、HP-UX 11.0、SUN 的 Solaris 8.0 等。UNIX 网络操作系统支持网络文件系统服务,提供数据等应用,功能强大,稳定性和安全性能非常好,但多以命令方式进行操作,初级用户不容易掌握,一般用于大型的网站或大型的企事业的网络中。

Linux 网络操作系统跟 UNIX 一样在安全性和稳定性方面都很好,Linux 最大的特点就是代码开源,中文版本的 Linux 像红帽、红旗等,在国内市场得到了用户充分的肯定。目前绝大部分中、高端服务器使用的是 Linux 网络操作系统。

NetWare 操作系统兼容 DOS 命令,是最早使用的网络操作系统,曾经雄霸一方,目前市场应用已经不多,NetWare 服务器对无盘站和游戏的支持较好,在教学网和游戏厅偶尔还有一些应用。

HarmonyOS 鸿蒙操作系统是我国华为公司自主研发的操作系统,该系统可以用于网络操作系统的服务器端和客户端,是万物互联的全场景分布式操作系统,提供应用开发、设备开发的一站式服务平台,目前已经有较广泛的应用。

Windows 也有网络操作系统,但由于 Windows 对服务器的硬件要求较高,并且稳定性不是很高,一般用在中低档服务器中。常用的 Windows 网络操作系统版本主要有 Windows NT、Windows Server、Windows ME/XP 等。Windows 网络操作系统因为继承了 Windows 家族统一的界面,用户学习、使用起来更加容易,功能基本上也能满足中、小型企业的各项网络需求,所以在市场上仍占有一定的份额。

2) 网络协议

类似汽车载货物或者人在高速公路上行驶需要遵守交通规则一样,数据在计算机网络中发送、传输、转发、接收等也都需要按照一定的规则,这个规则就是网络协议。网络协议是一种特殊的软件系统,是实现计算机网络功能的基本组成部分之一,随着互联的发展,网络

协议也在不断发展和更新。

计算机网络协议中的 OSI 参考模型和 TCP/IP 协议是大家最熟悉的基本协议模型，基于 OSI 和 TCP/IP 协议模型，各层又有负责各层功能的协议，网络协议遍布协议模型的各个层次。例如 HTTP、FTP、TCP、UDP、以太网等。

3）网络设备软件

网络设备软件主要包括网络管理软件和网络应用软件等，用于对网络资源进行管理和维护，是一种为网络用户提供服务的软件。

通过网络管理软件对网络进行管理和维护，例如性能管理、配置管理、故障管理、计费管理、安全管理、网络运行状态监视与统计等。网络应用软件最重要的特点是它研究的重点不是网络中各个独立的计算机本身的功能，而是如何实现网络特有的功能，为网络用户提供服务。

3.2.7　计算机网络拓扑结构

计算机网络拓扑是指组成计算机网络的设备的分布情况及连接状态，它反映的是网络中各实体间的结构关系。拓扑设计对网络性能、系统可靠性与通信费用都有重大影响，一般主要是指通信子网的拓扑结构。常见的计算机网络拓扑结构有总线型、树状、星状、网状及环状等。计算机网络拓扑结构如图 3-13 所示。

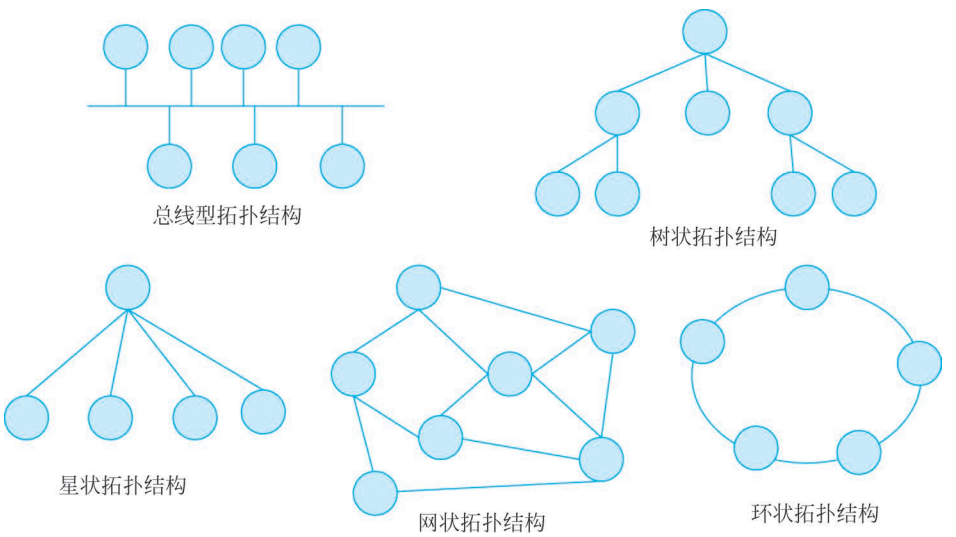


图 3-13　计算机网络拓扑结构

1）总线型拓扑结构

总线型拓扑将网络中的各个节点设备用一根总线挂接起来，实现计算机网络功能。总线型结构简单灵活，成本较低，易于扩展，传输速度快，但是节点个数有限。

2）树状拓扑结构

树状拓扑可以看作总线型拓扑结构或星状拓扑结构的扩展，可以包含分支，每个分支又可以包含多个节点，是一种分层的结构，适用于分级管理和控制系统，非常适用于网络主干

的构建。

3）星状拓扑结构

星状拓扑采用集中式通信控制策略，所有的通信均由中央节点控制，中央节点必须建立和维持许多并行数据通路。星状结构结构简单，是最古老的一种连接方式，部署与维护相对比较容易，目前是在局域网中应用得最为普遍的一种结构，在企业网络中大部分采用这一方式，但是网络资源共享能力较差且中央节点负荷较重。

4）网状拓扑结构

网状拓扑指各个节点通过传输线路互相连接起来，并且每个节点都至少与其他两个节点相连接。这种网络可靠性较高，但是结构复杂，成本高，并且不易维护和管理。

5）环状拓扑结构

环状拓扑是使用公共电缆组成一个封闭的环，各节点直接连接到环上，信息沿着环按一定方向从一个节点传送到另一个节点。环路是封闭的，不利于扩展，并且信息传输要通过环路上的每个节点，某个节点发生故障将会导致全网故障。

在实际应用中应根据实际需求选择合适的拓扑结构组网，更多时候也会采取两种或两种以上的网络拓扑结构混合的方式进行组网，集合多种网络拓扑结构的优点。

3.2.8 计算机网络体系结构

计算机网络体系结构是计算机网络通信系统的整体设计，它为网络硬件、软件、协议、存取控制和拓扑提供标准，实际上指的是计算机网络的层次结构模型，它包括各层的协议及层次之间的接口。计算机网络体系结构广泛采用的是 OSI 参考模型，互联网的 TCP/IP 模型也是基于 OSI 参考模型的理念。

1. OSI 参考模型

在网络开始发展的 20 世纪 60、70 年代，各个厂家都自己生产自己的设备，生产的网络设备相互不兼容，为了解决这个问题，国际标准化组织成立，并制定了一个公共的标准，即 OSI 参考模型。各厂家都遵循这个标准生产网络设备，这样各家的设备和系统就都能够相互通信。

OSI 参考模型采取了分层的思想，将复杂的过程简化，让专业的人做专业的事情。OSI 参考模型划分了 7 个层级：物理层、数据链路层、网络层、传输层、会话层、表示层、应用层，每个层级既相互独立又相互关联。OSI 参考模型如图 3-14 所示。

（1）物理层：位于 OSI 模型的最底层，利用传输介质为数据链路层提供物理连接，所传送数据的单位是位。物理层包括网口、传输介质、集线器或者中继器、电压、电流等。

（2）数据链路层：位于物理层之上，为网络层提供服务，解决两个相邻节点之间的通信问题，进行硬件物理地址寻址，也就是 MAC 地址寻址、差错校验、流量控制和重发等，传送的协议数据单元是数据帧。

（3）网络层：网络层是为传输层提供服务的，该层的主要作用是进行逻辑地址寻址，也就是 IP 地址寻址，进行路由和交换节点选择，使数据包通过各节点传送到目的地，网络层传

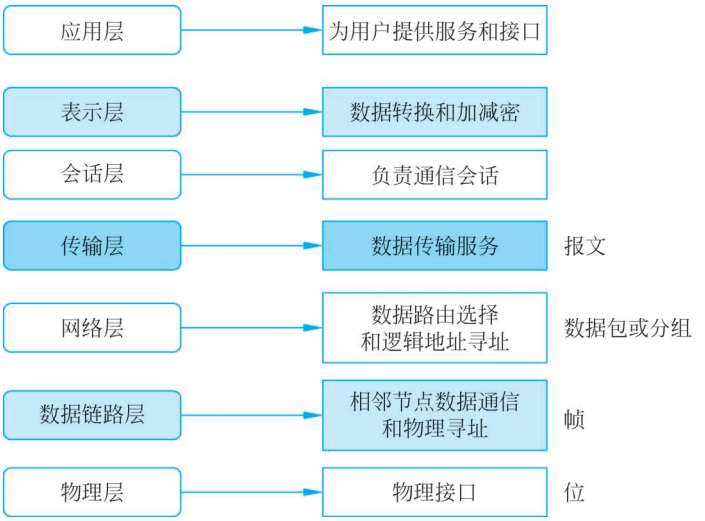


图 3-14　OSI 参考模型

送的协议数据单元是数据包或分组。

（4）传输层：为上层协议提供端到端的可靠、透明的数据传输服务，即分割与重组数据、按端口号寻址、连接管理、差错控制和流量控制。传输层传送的协议数据单位是报文，当报文较长时将其分割成若干分组，然后交给网络层进行传输。传输层是高低层之间衔接的接口层，该层以上各层将不再管理数据传输问题。

（5）会话层：该层负责会话连接的管理、对话管理、同步管理、活动管理。

（6）表示层：该层的主要任务是把所传送的数据的抽象语法转换为传送语法，即转换成网络通信中的标准表示形式。还负责对传送的数据进行加密或解密、数据的压缩和解压缩等。

（7）应用层：该层是 OSI 中的最高层，直接面向客户，主要任务是为用户提供应用的接口，即提供不同计算机间的文件传输、访问与管理，电子邮件的内容处理，不同计算机通过网络交互访问的虚拟终端功能等。

2. TCP/IP 模型

OSI 模型的提出是网络突破性发展的基础，但由于 OSI 协议发展较慢，而且 OSI 模型层次过多，设计冗余而复杂，编程实现困难。随着国际互联网的快速发展，TCP/IP 协议模型随之出现，并很快被各个互联网厂商广泛采用，TCP/IP 是目前 Internet 使用最广泛的协议模型。

TCP/IP 模型不是单个协议，而是很多个互联网协议的集合，如 IP、ICMP、TCP 及 HTTP、FTP、POP3 等协议，以 TCP 和 IP 为主，因此被称为 TCP/IP 协议。TCP/IP 基于 OSI 模型的分层思想，将 OSI 模型的几个相似功能层划分到同一层，减少了冗余。该协议实际上划分为 4 个或 5 个层次，区别在于四层协议将物理层与数据链路层划分在同一层。在实际应用中，较多采用 4 个层次的 TCP/IP 模型。TCP/IP 和 OSI 模型的层次对应关系如图 3-15 所示。

（1）应用层：对应 OSI 模型的应用层、表示层和会话层。该层包含所有的高层协议，例

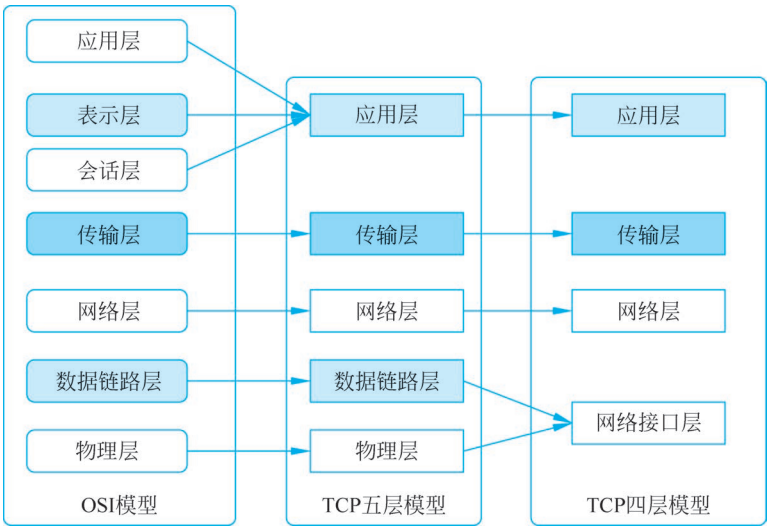


图 3-15 TCP/IP 和 OSI 模型的层次对应关系

如常用的远程登录协议 Telnet、文件传输协议 FTP、邮件传输协议 SMTP、域名服务 DNS、网络新闻传输协议 NNTP 和超文本传输协议 HTTP 等。

(2) 传输层：位于应用层之下，这层有著名的 TCP 和 UDP 协议。TCP 是面向连接的协议，提供可靠的报文传输和对上层应用的连接服务。TCP 还具备可靠性保证、流量控制、多路复用、优先权和安全性控制等功能。UDP 是面向无连接的不可靠传输协议，主要用于不需要排序和流量控制等功能的应用程序使用。

(3) 网络层：位于传输层的下一层，是 TCP/IP 体系结构的关键部分，使主机把数据报或者分组发送到任何网络，独立地传输到目标，网络层使用的协议主要是 IP 协议。

(4) 网络接口层：位于模型最底层的网络接口层，是整个体系结构的基础部分，是主机与网络的实际连接接口。负责接收网络层的 IP 数据报，通过网络向外发送，或接收从网络上传来的物理帧，提取 IP 数据报后发送给网络层。该层主要对应的协议就是著名的以太网协议等。

计算机网络系统结构有协议模型，模型的各层也有相应的协议规范。各层使用的协议如图 3-16 所示。

3.2.9 数据在计算机网络中的处理

学习了计算机网络的组成和体系结构后，大家清楚了数据经过分层处理后，通过传输介质发送到交换机和路由器，经过交换机或者路由器进行路径选择和寻址后，正确地传输到目标设备用户，但是数据在计算机网络的每层又是如何逐层封装的呢？交换机和路由器又是如何进行路径选择和寻址的呢？带着这些问题，我们进一步学习计算机网络的工作原理。

1. 计算机网络基础知识

在学习计算机网络的工作原理之前，先来了解一下计算机网络的几个基础知识和概念。

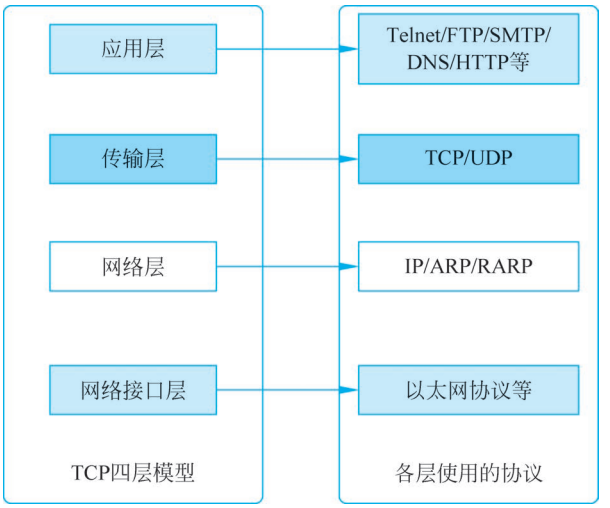


图 3-16　TCP/IP 各层协议

在计算机网络中通信时，网际协议地址（Internet Protocol Address，IP 地址）描述的是数据传输的起点和终点，即从源主机到目的主机，所以必须知道对方的 IP 地址。实际上，数据包中已经附带了 IP 地址，将数据包发送给路由器后，路由器会根据 IP 地址找到对方的地理位置，完成一次数据的传递。路由器具有高效和智能的算法，能够快速地找到目标计算机。那么，IP 地址是由什么组成的呢？

1）IP 地址

在计算机网络中用 IP 地址来标识网络中唯一的一台主机，也就是每台计算机可以使用一个独立的 IP 地址。IP 地址的资源是非常有限的，在实际应用中通常是一个局域网才拥有一个 IP 地址。

IP 地址是一个 32 位的二进制数，通常用点分十进制来表示，即用 a. b. c. d 的形式表示（a、b、c、d 为 0～255 的数）。那么它是如何定位一台主机的呢？

IP 地址 ＝ 网络号 ＋ 主机号。

网络号：用来标识网段，保证相互连接的两个网段具有不同标识。

主机号：用来标识主机，包括网络上的工作站、服务器和路由器等，同一网段内不同的主机可以有相同的网络号，但是主机号必须不同。

Internet 委员会将 IP 地址分为 A～E 类五大类，适用于不同容量的网络，其中 A、B、C 三类由 Internet 委员会在全球范围内统一分配，D、E 类为特殊地址。IP 地址的分类如图 3-17 所示。

A、B、C 三类 IP 地址的具体范围和容量见表 3-1。

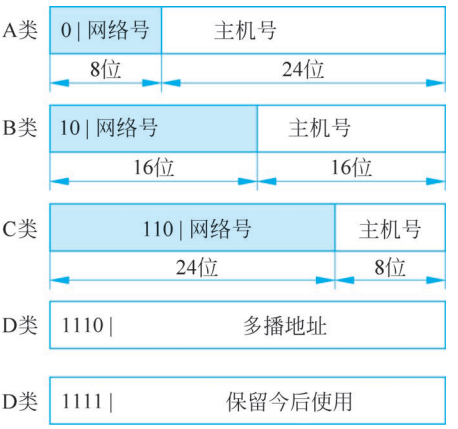


图 3-17　IP 地址的分类

表 3-1 A、B、C 三类 IP 地址详情

类别	最大网络数	IP 地址范围	单个网段最大主机数	私有 IP 地址范围
A	126(2^{7-2})	1.0.0.1～127.255.255.254	16 777 214	10.0.0.0～10.255.255.255
B	16 384(2^{14})	128.0.0.1～191.255.255.254	65 534	172.16.0.0～172.31.255.255
C	2 097 152(2^{21})	192.0.0.1～223.255.255.254	254	192.168.0.0～192.168.255.255

注意：A 类中最大主机连接数减去 2，是因为减去了全为 0 和全为 1 的两个特殊的 IP 地址。

IP 地址全为 0：网络号，代表这个局域网；

IP 地址全为 1：广播地址，用于给同一个链路中相互连接的所有主机发送数据报。

另外 127.0.0.1 一般用于本机环回测试，用于本机到本机的网络通信。

2）MAC 地址

在网络数据传输中，实际上是网络硬件设备将数据发送到网卡上，以网卡来接收数据，那么数据如何能正确地发送到目标网卡上呢？网卡具有唯一的硬件标识，即 MAC 地址。MAC 地址描述的是网络路径中每个节点的起点和终点，即每跳的起点和终点。

MAC 地址(Media Access Control Address)是用于标识网络硬件设备的物理地址，主机具有一个或多个网卡，交换机或路由器具有两个或多个网卡，每个网卡都有唯一的 MAC 地址。网卡出厂时，MAC 地址就已经固定了，不能修改，并且是全球唯一的。

MAC 地址的格式：长度为 48 位的串行号，写在网卡的存储器 ROM 中，一般用十六进制数字加冒号的形式表示，如 07:00:27:03:FC:1E。

注意：FF:FF:FF:FF:FF:FF 为特殊的 MAC 地址，表示对同网段所有主机发送数据报。

数据在网络中传输的过程中，数据包中除了会附带对方的 IP 地址，还会附带对方的 MAC 地址。当数据包达到局域网后，交换机会根据数据包中的 MAC 地址找到对应的计算机，直到将数据包转交给目标计算机，这样就完成了数据的传递。

3）端口

有了 IP 地址和 MAC 地址，虽然可以找到目标计算机，但仍然不能进行通信。因为一台计算机可以同时提供多种网络服务，如 Web 服务、FTP 文件传输服务、SMTP 邮箱服务等，仅有 IP 地址和 MAC 地址，计算机虽然可以正确地接收到数据包，但是要将数据包交给哪个网络程序来处理依然是个问题。

为了区分不同的网络程序，计算机为每个网络程序分配一个唯一的端口号(Port Number)，端口是一个虚拟的、逻辑上的概念。可以理解为一扇门，数据经过这扇门流入或流出，每扇门用不同的端口号标识，端口号是一个整数，是可以进行修改的，但通常为了在互

联网上统一地进行数据交换，对常用的一些网络程序的端口号进行了约定。例如常用的Web 服务的端口号是 80，FTP 服务的端口号是 21，SMTP 服务的端口号是 25。

4）域名系统

就像很难记住每个人的身份证号码或护照号码一样，要记住要访问的主机的 IP 地址也非常困难，因此，将 IP 地址和域名关联起来，只需记住域名就可以了，但是计算机只能识别 IP 地址并通过 IP 地址定位，所以需要进行域名解析，对域名和 IP 地址进行相互转换。

域名系统（Domain Name System，DNS）是 TCP/IP 网络中负责域名解析的系统。简单来讲，当在浏览器网址栏中输入某个 Web 服务器的域名时，用户主机会向网络中的某台 DNS 服务器查询。DNS 服务器中有域名和 IP 地址的映射关系数据库。当 DNS 服务器收到 DNS 查询报文后，在其数据库中进行查询，然后将查询结果发送给用户主机。

5）地址解析协议

地址解析协议（Address Resolution Protocol，ARP）是在计算机网络中根据 IP 地址获取 MAC 地址的协议。主机和路由器中都保存了一张 ARP 缓存表，通过 IP 地址可以找到 MAC 地址。如果找不到 MAC 地址，则广播发送 ARP 数据报，询问下一跳设备 IP 地址对应的 MAC 地址。如果跨越局域网，则还需要路由器的帮助。ARP 寻址过程如图 3-18 所示。

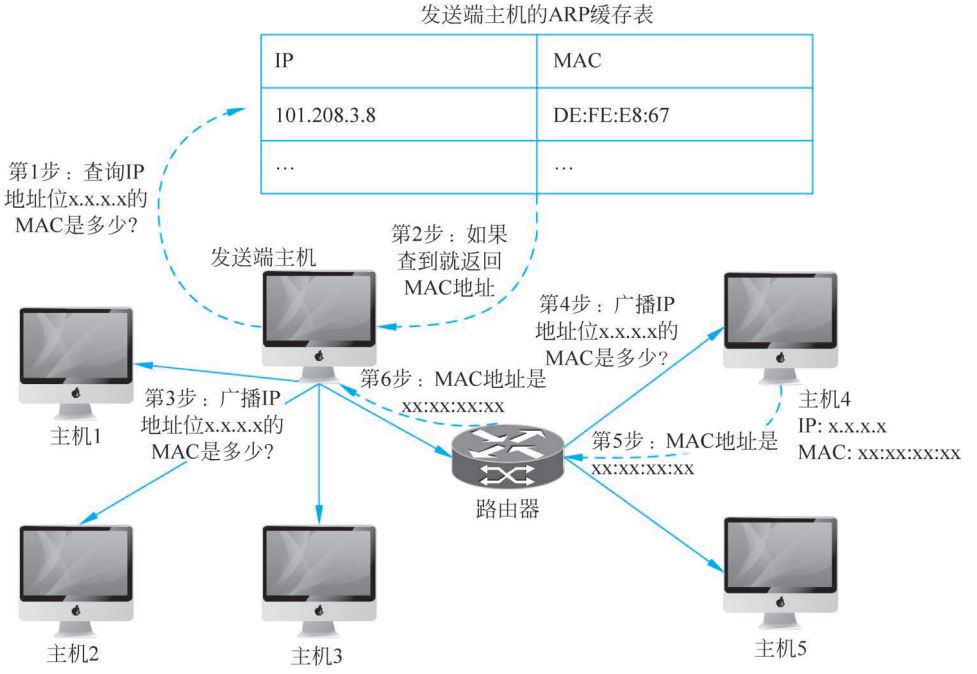


图 3-18　ARP 寻址过程

2. 数据在计算机网络的处理流程

在学习了计算机网络的组成和体系结构后，再来看数据在网络中是如何处理和传输的

就比较容易理解了。在日常生活中,用户打开浏览器,输入网址 www. taobao. com,按 Enter 键后就能访问网页。那么在这个过程中,数据又是如何处理和传输的呢?

这里以在浏览器网址栏输入 www. taobao. com 后,数据在 Internet 网络中的处理和传输流程为例,主要分成以下步骤介绍,以便大家更好地理解。

1) 域名解析获得 IP 地址

将域名 www. taobao. com 转换为 IP 地址。在实际过程中,首先用户主机会在自己的高速缓存中查找是否有该域名对应的 IP 地址。如果之前访问过且仍保存在缓存中,就可以直接查询到域名对应的 IP 地址,否则用户主机会向网络中的某台 DNS 服务器查询。DNS 服务器在其数据库中查询之后,将查询结果发送给用户主机,从而得到 www. taobao. com 域名对应的 Web 服务器的 IP 地址,如图 3-19 所示。

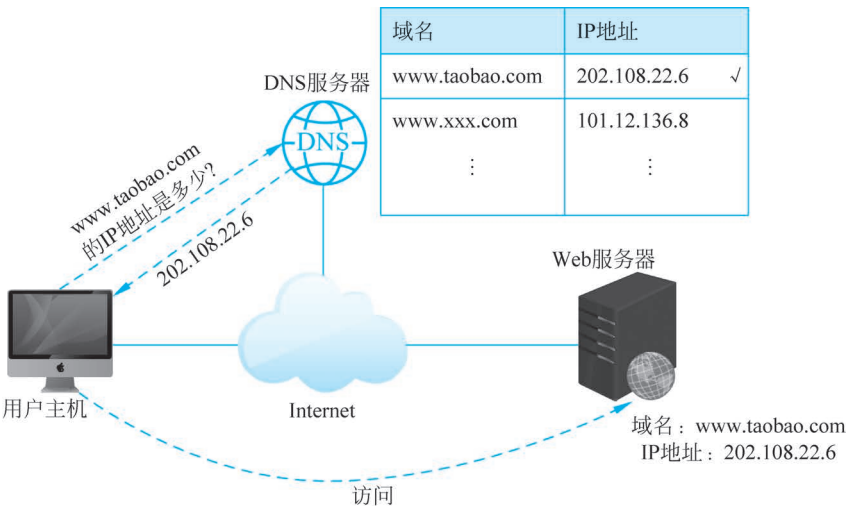


图 3-19 DNS 域名解析过程

2) 主机进行数据封装

用户主机根据 TCP/IP 模型分层对数据从上到下逐层进行封装,数据封装过程如图 3-20 所示。

在访问 Web 服务器上的网页时,应用层采用的协议是超文本传输协议 HTTP 或者加密的 HTTPS,浏览器将网址等信息组成 HTTP 数据,并将数据传送给传输层。

传输层在应用层传送来的数据前面加上 TCP 或者 UDP 头,并标记上源端口和目的端口,这两个端口为 Web 服务器的默认端口 80,形成 TCP 或者 UDP 报文段,然后将这个报文段传给网络层。

网络层收到传输层的数据段后会继续在数据段前面加上自己机器的 IP 地址和目的 IP 地址,形成 IP 数据报,然后将 IP 数据报传给数据链路层。

数据链路层收到 IP 数据报后,先在 IP 数据报的前面加上自己机器的 MAC 地址及目

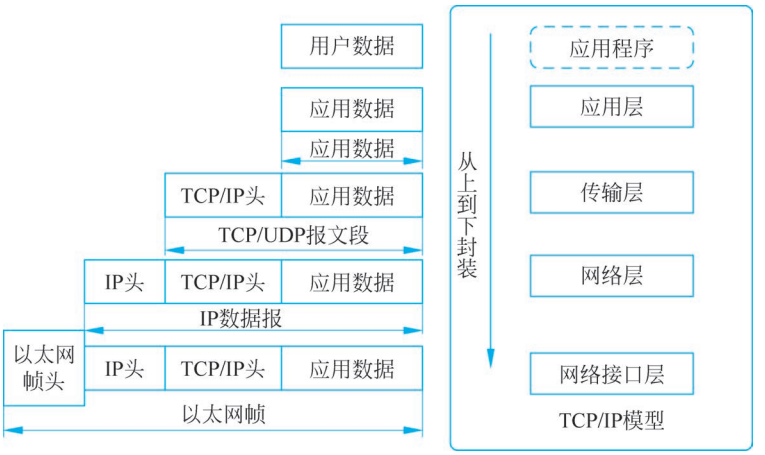


图 3-20　主机进行数据封装过程

的 MAC 地址，形成数据帧，然后通过物理网卡把数据帧以比特流的方式发送到网络上。

3）判断下一跳设备

首先通过子网掩码计算源主机和目的主机是否在同一个网段，如果在同一个网段，直接通过 ARP 寻址就可以找到局域网内的任意一台主机，下一跳设备就是目的主机，否则发送端主机无法知道目的主机的 MAC 地址，必须设置下一跳网关设备，即路由器。

4）交换机接收和转发数据

如果网络中存在交换机，则交换机接收到数据后会根据内部维护的 MAC 地址转发表找到目的 MAC 地址对应的端口，如果在转发表中找到目的 MAC 地址对应端口，就将数据转发到对应端口，否则交换机就发送广播数据帧，等待目的主机响应后记录并转发到目的 MAC 地址对应端口。交换机接收和转发数据的过程如图 3-21 所示。

MAC	端口
MAC-PC1	E1/0/1
MAC-PC2	E1/0/2
MAC-PC3	E1/0/3
MAC-PC4	E1/0/4

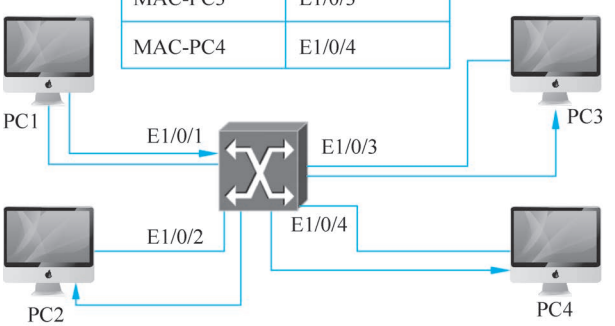


图 3-21　交换机接收和转发数据的过程

5）路由器接收和转发数据

当局域网内的主机将数据发送到公网主机时，数据会被发送给路由器。路由器接收到数据后会根据协议模型的分层结构从下层到上层进行处理。路由器会基于路由选择获取下一跳设备的 IP 地址，并通过 ARP 协议寻址找到 IP 地址对应的 MAC 地址，然后路由器会自上而下封装数据，并将其发送到下一个设备。路由寻址的流程如图 3-22 所示。

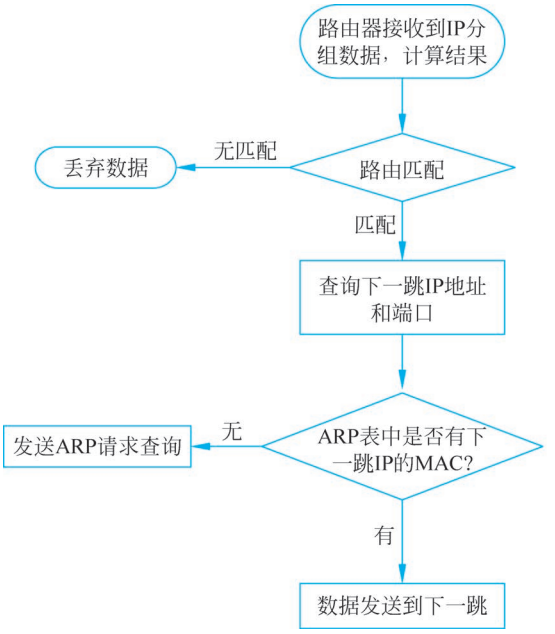


图 3-22 ARP 寻址的流程

6）目的主机接收和处理数据

目标主机接收到网络中发送来的访问 www.taobao.com 网页的数据，也是根据协议分层模型从下到上进行处理的，并向源主机返回响应数据，即网页的内容。当响应数据返回后，用户就能看到网页。响应数据返回的流程与发送数据的流程相同，只是源 IP 地址与目标 IP 地址互换及源端口与目标端口互换的区别。这里就不再重复说明了。

3.2.10 数据在计算机网络中传输的安全性

随着互联网的发展，如今在每个人的生活、工作和学习中都离不开互联网了，每天有各种数据在网络中传输。数据在计算机网络这个如此复杂的结构体系中传输，可能经过成千上万台设备，经过不可估量的超远距离传输，数据是否存在安全问题呢？答案是肯定的。不仅发送和接收的数据在网络传输过程中可能存在网络安全问题，在互联网的使用过程中也存在着各种信息安全问题，需要大家注意并引起重视。

3.2.11 信息安全

信息安全是指信息系统（包括硬件、软件、数据、人、物理环境及其基础设施等）受到保

护，不因为偶然的或者恶意的原因而遭到破坏、更改、泄露，系统可以连续可靠地正常运行，信息服务不中断，最终实现业务连续性。

信息安全问题体现出的显著特点有广泛性、灾难性、高智能性、隐蔽性、机动性、来源的多样性和防范对象的不确定性等。

随着全球互联和全球数字化的发展，在全民网络的时代，信息安全问题日益突出，各种网络攻击、敲诈勒索、数据窃取等全球范围内的信息安全重大事件频发。信息安全越来越受到各国政府的重视，近年来我国也非常重视信息安全工作。

1. 信息安全的目标

信息安全的目标是要保护信息系统的安全，保证信息的保密性、完整性、可用性，要从这些方面来管理、防范及降低安全风险。

（1）保密性：是要防范信息泄漏给非授权用户的特性，强调有用信息只被授权个人或组织之间共享使用的特征。可以通过身份认证、信息加密、访问控制、安全通信协议等技术实现，其中信息加密是防范信息泄露的最基本手段。

（2）完整性：是指信息在传输、交换、存储和处理的过程中保持信息真实、完整（不被破坏或篡改）、不丢失和信息未经授权不能改变的特性，是最基本的安全特征。

（3）可用性：指信息资源可被授权人或组织按要求访问、正常使用，在异常情况下能恢复使用的特性。是网络信息系统面向用户的一种安全性能，保障系统为用户提供正常服务。

2. 信息安全分类

根据信息安全涉及的内容通常将信息安全分为物理安全、网络安全、系统安全、应用安全、管理安全等 5 个方面。

1）物理安全

物理安全是指保护计算机设备、设施（网络及通信线路）免遭地震、水灾、火灾等自然灾害和环境事故（如电磁污染等），以及人为操作失误及计算机犯罪行为导致的破坏。保证计算机信息系统各种设备的物理安全，是整个计算机信息系统安全的前提。物理安全主要包括以下 3 个方面。

（1）环境安全：对系统所有环境的安全保护，如区域保护（电子监控）和灾难保护（灾难的预警、应急处理、恢复等）。

（2）设备安全：主要包括设备的防盗、防毁（接地保护）、防电磁信息辐射泄漏、防止线路截获、抗电磁干扰及电源保护等。

（3）媒体安全：包括媒体数据的安全及媒体本身的安全。

物理安全是非常容易被忽视的，尤其是在一些小的单位和家庭中。一旦被黑客入侵，短短几分钟就会受到安全的威胁。

2）网络安全

网络安全指网络上信息的安全，即网络中传输和保存的数据等信息的安全，保障网络安全使用的典型技术包括密码技术、设置防火墙、入侵检测技术、访问控制技术、认证技术、备份、虚拟专用网络技术等。

在局域网与公网之间,可以设置防火墙来实现内外网的隔离和访问控制,是保护内部网安全的主要措施之一,也是最有效、最经济的措施之一。

网络安全检测工具通常是一个网络安全性的评估分析软件或硬件,使用此类工具可以检测出系统的漏洞或潜在的威胁,增强网络安全性。

备份是为了尽可能快速地全面恢复运行计算机系统所需的数据和信息。备份可以在网络系统硬件出现故障或人为操作失误时起到保护作用,也可以在入侵者非授权访问或对网络进行攻击并破坏数据完整性时起到保护作用,同时也是系统灾难恢复的前提之一。

3) 系统安全

系统安全包含操作系统安全和数据系统安全,数据库的安全往往被忽视,其实数据库系统也是一种非常重要的系统软件,与其他软件一样需要保护。系统安全可以通过操作系统加固、数据库加固、系统安全检测、审计分析等手段来保障。

4) 应用安全

应用安全建立在系统平台之上,是应用程序在使用过程中的安全,是应用层的安全,包括 Web 安全、电子邮件安全等。

5) 管理安全

安全是一个整体,完整的安全解决方案不仅包括物理安全、网络安全、系统安全和应用安全等技术手段,还需要以人为核心的策略和管理支持。信息安全至关重要的往往不是技术手段,而是对人的管理。无论采用了多么先进的技术设备,只要安全管理上有漏洞,那么这个系统的安全就没有保障。专家们一致认为"30%的技术,70%的管理",而且信息安全是一个动态的过程,必须通过一个动态的管理来保证安全。

3. 计算机病毒

计算机病毒会严重地破坏计算机信息系统,是信息安全重点防范对象之一。计算机病毒是指编制者在计算机程序中插入的能够自我复制的一组计算机指令或程序代码,用于破坏计算机功能或者破坏数据,从而影响计算机正常使用。

计算机病毒具有传染性、隐蔽性、感染性、潜伏性、可激发性、表现性和破坏性等典型的特点。

4. 常见的计算机病毒

随着计算机和互联网的快速发展,计算机病毒不断地推陈出新,变形速度和破坏力不断提高,呈现新的发展趋势。目前常见的计算机病毒主要有系统病毒、蠕虫病毒、木马病毒、脚本病毒、宏病毒等。

1) 系统病毒

系统病毒的前缀为 Win32、PE、Win95、W32、W95 等,这些病毒一般可以感染 Windows 操作系统的 *.exe 和 *.dll 文件,并通过这些文件进行传播,例如 CIH 病毒。

2) 蠕虫病毒

蠕虫病毒的前缀是 Worm,这种病毒是通过网络或系统漏洞进行传播,很大部分的蠕虫病毒有向外发送带毒邮件、阻塞网络的特性。例如感染型的蠕虫病毒有熊猫烧香、小邮差(发带毒邮件)等。

3）木马病毒

木马病毒的前缀是 Trojan，黑客病毒的前缀名一般为 Hack。木马病毒是通过网络或系统漏洞进入用户的系统并隐藏，然后向外界泄露用户的信息，而黑客病毒则有一个可视的界面，能对用户的计算机进行远程控制。木马、黑客病毒往往是成对出现的，即木马病毒负责侵入用户的计算机，而黑客病毒则会通过该木马病毒来进行控制。现在这两种类型的病毒越来越趋向于整合了。

4）脚本病毒

脚本病毒的前缀是 Script、VBS 和 JS 等，脚本病毒是使用脚本语言编写的并通过网页进行传播的病毒，例如红色代码（Script. Redlof）、欢乐时光（VBS. Happytime）、十四日（Js . Fortnight. c. s）等。

5）宏病毒

宏病毒的前缀是 Macro，第二前缀是 Word、Word97、Excel、Excel97 中的一个。该类病毒的共同特点是能感染 Office 系列文档，然后通过 Office 通用模板进行传播，例如著名的美丽莎（Macro. Melissa）、Macro. Word97。

6）后门病毒

后门病毒的前缀是 Backdoor，是通过网络传播的，给系统开后门，给用户的计算机带来安全隐患。例如 IRC 后门 Backdoor. IRCBot。

7）病毒植入程序

病毒植入程序是在运行时会从内部向系统目录释放出一个或多个新的病毒，由释放出来的新病毒造成破坏。例如冰河播种者（Dropper. BingHe2. 2C）、MSN 射手（Dropper . Worm. Smibag）等。

8）破坏性程序病毒

破坏性程序病毒的前缀是 Harm，本身具有诱人单击的图标来引诱用户单击，当用户单击这类病毒时，病毒就会直接对用户计算机造成破坏。例如格式化 C 盘（Harm. formatC. f）、杀手令（Harm. Command. Killer）等。

9）玩笑病毒

玩笑病毒的前缀是 Joke，也称为恶作剧病毒。这类病毒本身具有诱人单击的图标来引诱用户单击，当用户单击这类病毒时，病毒会做出各种破坏操作来吓唬用户，但实际上病毒并没有对用户计算机进行任何破坏。例如女鬼（Joke. Girlghost）病毒。

10）捆绑机病毒

捆绑机病毒的前缀是 Binder。这类病毒的作者会使用特定的捆绑程序将病毒与一些应用程序（如 QQ、IE）捆绑起来，表面上看是一个正常的文件，当用户运行这些捆绑病毒时会正常运行这些应用程序，然后隐藏运行捆绑在一起的病毒，从而给用户造成危害。例如捆绑 QQ（Binder. QQPass. QQBin）、系统杀手（Binder. killsys）等。

5. 常用防范计算机病毒的技术

计算机病毒无时无刻不在关注并时刻准备攻击，但计算机病毒也不是完全不可控的，通

常用户可以从安装杀毒软件、提升信息安全意识、培养良好的上网习惯等方面防范。

(1) 安装最新的杀毒软件：及时升级杀毒软件病毒库，定期扫描查杀病毒，上网时开启杀毒软件的监控，不要执行未经杀毒处理的软件，另外打开 Windows 更新功能，以及时打全系统补丁。

(2) 提升信息安全意识：不贪图小便宜，使用移动存储设备时，尽可能不要共享设备，防止移动存储设备成为病毒传播的途径和攻击的目标，在对信息安全要求较高的场所和设备，不经授权不能随意使用 USB 接口、使用相机拍摄或安装即时通信工具，尽量专机专用。

(3) 培养良好的上网习惯：不访问来源不明或可能带有病毒的网站，对不明邮件及附件慎重打开，不接收可疑红包陷阱等，密码设置不要太常用和简单，猜测简单密码是许多网络病毒攻击系统的一种新方式。

(4) 另外一旦发现异常或计算机受到病毒侵害，应该及时中断网络，将异常计算机隔离，以免病毒在网络中传播。

对于专业研发人员，在产品研发过程中，可以通过加密技术、身份认证、数字证书技术、配置防火墙等方面来对产品进行完善，增强产品的安全性能，防范和减少病毒带来的破坏。

(1) 加密：加密技术是利用一定的加密算法，将明文转换成无意义的密文，阻止非法用户获取和理解原始明文数据，确保数据的安全性，是一种主动的信息安全防护措施。目标用户收到后再通过解密还原原始数据。密码技术的工作原理如图 3-23 所示。

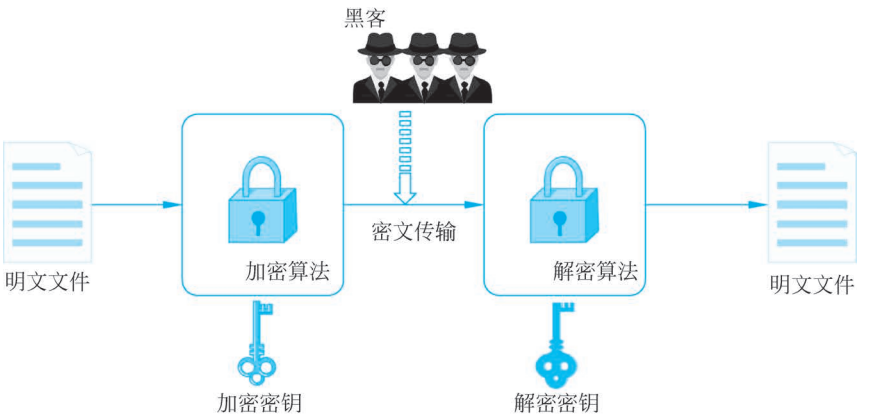


图 3-23　密码技术工作原理

常见的加密方式有 MD5、SHA1、AES、DES、RSA、ECC 加密等，其中 MD5、SHA1 采用的是哈希算法进行加密，一般是不可逆的，加密简单，速度很快。通常不用于加密，而是被应用在检查文件完整性和数字签名等场景。AES、DES 是典型的对称加密算法，RSA、ECC 加密则是非对称加密算法，对称加密算法的优点是速度快，但同时安全性较低，而非对称加密算法则非常安全，但速度相对较慢。用户需要根据实际应用场景选择合适的加密方式，在实际网络应用中一般混合使用。

(2) 身份认证：是证实实体对象的数字身份与物理身份是否一致的过程，身份认证具

有唯一性、非描述性、权威签发等几个特性，身份认证的凭证一般有账户口令、令牌或者生物特征等，其中基于口令的身份认证是应用最广泛的一种，也就是常用的用户名和密码的方式，口令设置一定要遵循易记、难猜、抗分析的原则。令牌指常用的 U 盾、智能卡等，而生物特征就是常用的指纹、虹膜、签名、语音等认证方式。

（3）数字证书：是标识网络用户身份信息的一系列数据，用于在网络通信中识别通信各方的身份。数字证书是由权威认证机构数字签名的数字文件，一般包含用户的身份信息、用户的密钥信息、身份验证机构及数字签名等数据。数字证书主要在网上银行、电子商务的交易、在线支付及电子病历管理中广泛应用。

（4）防火墙：借鉴了古时候用于防火的防火墙的喻义，防火墙是隔离企业内部网络与互联网之间或与其他外部网络之间的一道防御系统，是由硬件和软件组成的系统，可以通过限制网络互访来保护内部网络。防火墙根据工作方式的不同分为个人防火墙和网络防火墙。目前防火墙的应用非常广泛，无论是个人计算机还是企业网络都配置了防火墙。网络防火墙架构如图 3-24 所示。

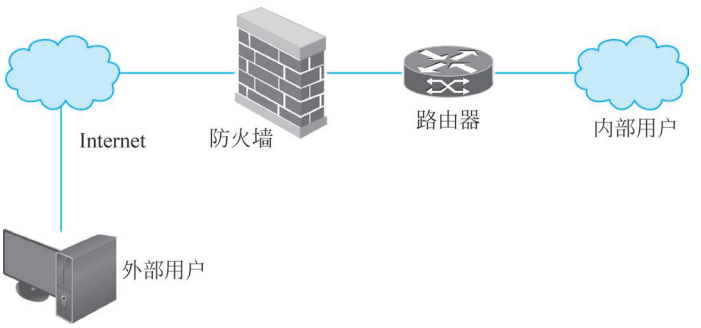


图 3-24　网络防火墙的架构

3.3　任务实施

通过普及知识，小强对计算机网络的软硬件组成、计算机网络体系结构及计算机网络的工作原理都有了清楚的认识，也认识到信息安全的重要性和基本的安全防范意识，开始配置计算机网络接入公司的企业网络，并安装更新杀毒软件，配置个人防火墙，开始日常的工作。

3.3.1　配置计算机网络

小强从公司 IT 管理员那里获得了自己计算机的指定专用 IP 地址为 192.168.3.132，公司局域网的网关地址为 192.168.3.1，DNS 服务器地址为 101.198.128.68。接下来开始操作，配置的步骤如下。

1. 配置网络

（1）按快捷键 Win+R，在“运行”对话框中输入 control，按 Enter 键，打开控制面板，选择“网络和 Internet”→“网络和共享中心”→“更改适配器设置”，进入网络连接，如图 3-25 所示。

图 3-25　网络连接窗口

(2) 找到连接网线的以太网，右击“属性”，在“以太网属性”对话框中找到“Internet 协议版本 4(TCP/IPv4)”，双击进入“Internet 协议版本 4(TCP/IPv4)”对话框，如图 3-26 所示。

图 3-26　Internet 协议版本 4(TCP/IPv4)属性对话框

(3) 根据 IT 管理员给的网络信息进行设置，IP 地址设置如图 3-27 所示。

平常通过无线网络 WiFi 进行网络连接的时候，一般选择自动获得 IP 地址，无须自己设置具体的 IP 地址等信息，但这里是通过网线接入公司的企业网络，就需要选择使用下面的 IP 地址。

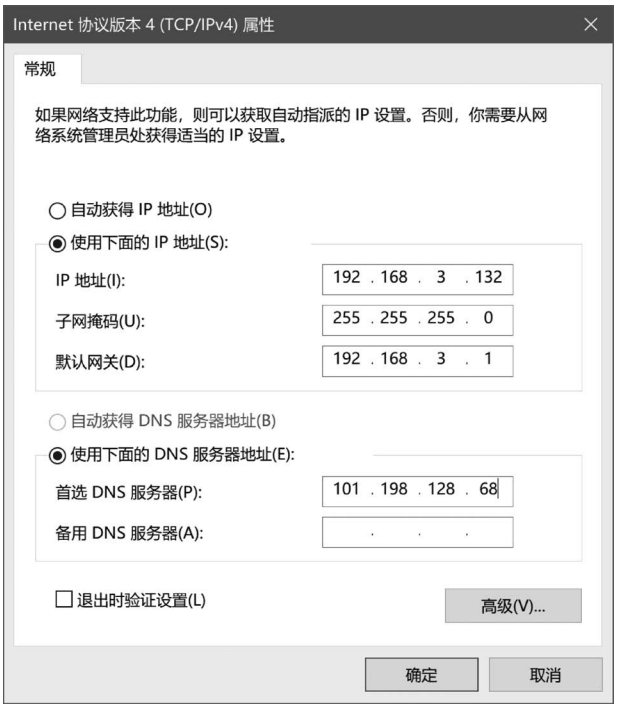


图 3-27　IP 地址设置

设置自己专用的 IP 地址在“IP 地址”一栏，这里需要注意，很多企业的网络 IT 管理员在路由器中设置了 IP 地址与计算机 MAC 地址绑定，也就是说计算机只有使用分配的专用 IP 地址才能正常接入。

在子网掩码一栏中，将子网掩码设置为 255.255.255.0，表示在同一子网中可以有 254 台机器，一般是够用的，IT 管理员在设置子网时也会考虑同一网段的用户数问题。

默认网关一栏，填入 IT 管理员给的公司局域网的网关地址，只有通过此地址才能正常接入公司网络并通过此网关与外网进行通信。

因为需要手动设置 DNS 服务器地址，所以选择使用下面的 DNS 服务器地址，并在首选 DNS 服务器栏中设置 IT 管理员给的 DNS 服务器地址即可，如果某些大型企业的网络有多个 DNS 服务器地址，则可以填上备用 DNS 服务器地址，一般只填一个。

设置完成之后，单击“确定”按钮关闭弹窗，网络就设置好了。

2. 测试网络连接

设置好的网络是否可以正常使用呢？下面来测试一下。

如果公司网络允许连接 Internet，则可直接打开浏览器，进入 www.baidu.com 或其他可用的外网地址，如果公司网络已经解除对 Internet 的限制，则浏览器连接公司的内部网站访问即可验证。通常也可以使用命令 ping 要访问的 IP 地址，查看是否有响应。命令行的使用方式如下：

(1) 按快捷键 Win+R,在“运行”对话框中输入 cmd,按 Enter 键,打开命令行窗口。

(2) 在“命令行”中输入 ping 命令,连接要连接的网站 IP 地址或者网关地址,如果有响应,则表示网络设置成功,否则需要再次检查网络信息设置是否正确。使用 ping 命令测试网络如图 3-28 所示。

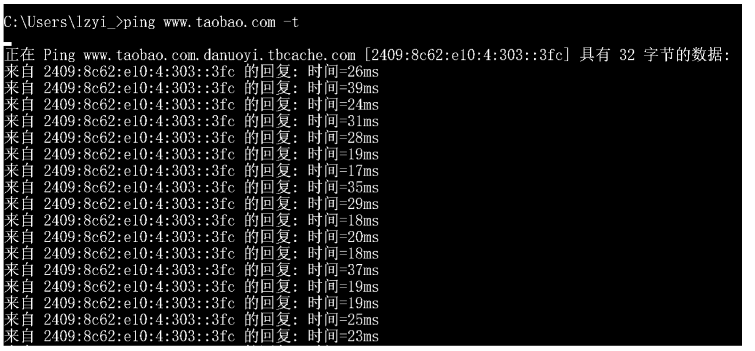


图 3-28 测试网络

3.3.2 配置个人防火墙

网络配置好后,按照公司的规定,接下来小强需要对计算机防火墙进行配置,配置的操作步骤如下:

(1) 按快捷键 Win+R,在“运行”对话框中输入 control,按 Enter 键,打开控制面板,选择“系统和安全”→“Windows Defender 防火墙”,进入 Windows Defender 防火墙对话框,左侧是设置防火墙的“功能列表”,右侧是计算机的 Windows Defender 防火墙状态、传入连接、活动的公用网络和通知状态等防火墙的“设置状态”,如图 3-29 所示。

图 3-29 Windows Defender 防火墙对话框

（2）在“Windows Defender 防火墙”对话框，单击“允许应用或功能通过 Windows Defender 防火墙”，对允许的应用和功能进行选择设置。在需要应用的应用或者功能后面勾选“专用”或“公用”，不同的应用可以选择不同的方式，选择好了以后，单击“确定”按钮即可，注意仅选择专用的应用和功能，将不能与公用外网连接。配置允许的应用和功能如图 3-30 所示。

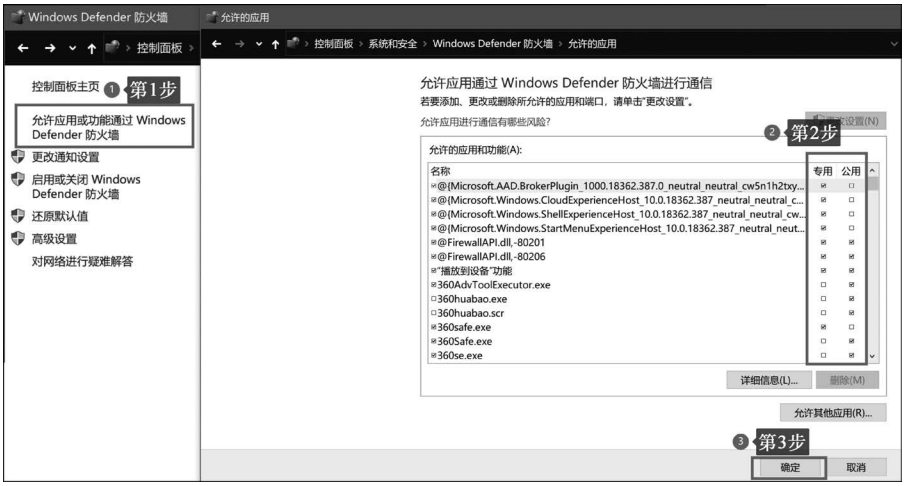


图 3-30　配置允许的应用和功能

（3）在“Windows Defender 防火墙”面板的功能列表中，单击“启用或关闭 Windows Defender 防火墙”，可以自定义设置专用网络和公用网络中是否启用 Windows Defender 防火墙的设置，如果设置“启用 Windows Defender 防火墙”，则计算机在接入专用网络或者公用网络时将使用防火墙的配置。设置好以后，单击“确定”按钮。如果设置错误或者希望回到计算机防火墙的默认设置，则可以单击面板功能列表中的“还原默认值”，如图 3-31 所示。

图 3-31　设置启用 Windows Defender 防火墙

(4) 对于普通的用户,防火墙设置到这里就可以了,但对安全有更高要求的用户,可以单击防火墙面板的功能列表中的“高级设置”,进入“高级安全 Windows Defender 防火墙”面板,进一步设置防火墙。高级安全 Windows Defender 防火墙提供基于主机的双向网络流量筛选,阻止流入或流出本地设备的未经授权的网络流量。还可以使用 Internet 协议安全性(IPsec)保护在网络间传送的流量的连接安全规则,如图 3-32 所示。

图 3-32 高级安全 Windows Defender 防火墙设置面板

3.3.3 安装或者更新杀毒软件

防火墙安装好了,小强继续检查计算机上杀毒软件的情况,并定期对计算机进行安全扫描和检测,操作步骤如下:

1. 安装或者更新杀毒软件

(1) 在“开始”中查看是否已经安装杀毒软件,目前 Windows 10 系统的新计算机一般安装了内置的杀毒软件,单击“开始”菜单→“Windows 系统”,展开后能看到 Windows Defender,这就是 Windows 10 自带的杀毒软件,但也有一些系统没有内置杀毒软件。

(2) 计算机自带的杀毒软件功能更加纯净,但是查杀力度不够,第三方的杀毒软件扫描更加全面,杀毒更加强力,但大部分带有广告和各种其他插件。一般用户计算机可以继续安装计算机管家、360 安全卫士、360 杀毒来全方位地保护计算机的安全,安装时最好在产品的官方网站进行下载,防止下载到木马或者被植入广告的安装包,例如 360 安全卫士的官网下载如图 3-33 所示。

(3) 下载完成后,双击下载的 exe 安装包就可进行安装,可以选择“下一步”默认安装,直到完成,在 360 安全卫士中,除了可以查杀病毒木马外,还有系统修复、软件管家等功能,

图 3-33　360 安全卫士官方下载

安装完成后 360 安全卫士的界面如图 3-34 所示。

图 3-34　360 安全卫士主界面

2. 开启 360 安全卫士防护

(1) 打开 360 安全卫士软件，单击主页面顶部的“功能大全”→“全部工具”→“计算机安全”→“系统安全防护”，进行系统安全防护安装，如果之前已经安装过，再单击就是进行

修补。系统安全防护安装如图 3-35 所示。

图 3-35　系统安全防护安装

（2）系统安全防护安装完成后，再次单击“系统安全防护”，打开 360 系统安全防护弹窗面板，在面板中将“开启 360 系统防黑安全防护服务”右边的开关打开，使其变成绿色，360 安全卫士的防护功能就开启了。360 安全卫士的系统防护功能开启如图 3-36 所示。

图 3-36　开启 360 安全卫士的系统防护功能

3. 扫描和病毒检测

360 安全卫士的系统防护功能开启后，就可以正常对系统进行防护和安全检测了，接下来扫描和检测一下计算机的安全情况。

单击 360 系统安全防护页面底部的“立即检测”按钮，开始进行扫描，扫描完成后，如果检测到漏洞和问题，则可单击右上角的“立即处理”按钮，完成处理，最后单击“确定”按钮完成扫描和检测，这个安全检测过程后期需要定期做。360 系统安全防护检测过程如图 3-37 所示。

图 3-37　360 系统安全防护检测过程

3.3.4　使用加密工具对文件进行加密和完整性校验

小强完成了防火墙和杀毒软件等安全设置后，开始了正常有序的工作，有一天他又遇到了新问题。小强的同事在外地出差，他需要小强将一个与工作相关的技术文件发给他，小强在请示了领导之后，需要对该文件先进行加密，再通过邮件发送给同事，操作步骤如下。

1. 对技术文件进行加密

(1) 对文件进行加密，小强首先要找一款合适的文件加密工具，目前市场上有非常多的文件和文件夹加密工具，如打开 360 软件管家，在搜索框输入加密，就能找到很多的加密工具，小强选择了一款公司很多同事在使用的小巧方便的加密工具 Encrypto。

Encrypto 是一个免费的、极简的、跨平台的文件和文件夹加密工具，不仅支持 Windows 系统，还支持 Mac 系统。Encrypto 应用程序使用 AES-256 加密，使用该工具可以轻松地对文件和文件夹进行加密，生成一个加密后的文件，对方获取加密文件后，使用对应的加密密码即可对文件进行解密，查看原文件的内容。

(2) 下载 Encrypto 加密工具,在百度搜索框中输入 Encrypto,进入官网进行下载,如图 3-38 所示。

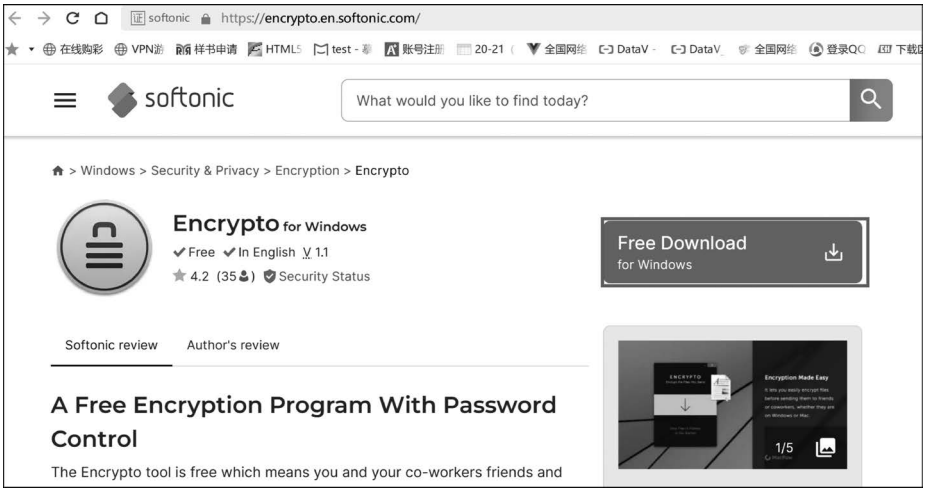


图 3-38 Encrypto 下载

下载完成后,双击刚下载的 exe 程序包开始安装 Encrypto,程序比较小,可以快速完成安装,注意在安装过程中如果计算机开启了安全防护,则可能会提示是否允许修改注册表,选择允许即可。加密工具安装完成后会在计算机桌面默认生成快捷方式,双击即可启动加密工具,Encrypto 启动面板如图 3-39 所示。

(3) Encrypto 工具的使用很简单,将需要加密的文件或者文件夹直接拖入,或者通过程序的 Add Files 或者 Add Folders 选择要加密的文件或者文件夹就可以了,Encrypto 可以加密任何类型的文件,Encrypto 加密完成后,生成的文件可以保存到计算机的任意位置。Encrypto 加密生成的文件如图 3-40 所示。

图 3-39 Encrypto 启动页面

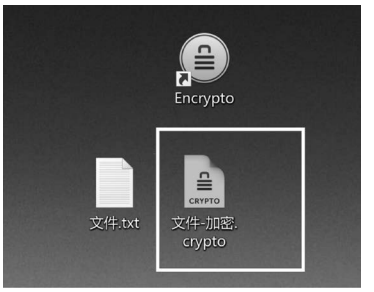


图 3-40 Encrypto 加密生成的文件

2. 规范编写电子邮件并发送

电子邮件是一种用电子手段提供信息交换的通信方式，是互联网应用最广泛的服务之一。通过电子邮件系统，用户可以以非常低廉的价格、非常快速的方式与世界上任何一个角落的网络用户进行联系。电子邮件可以是文字、图像、声音等多种形式，极大地方便了人与人之间的沟通与交流，促进了社会的发展。编写电子邮件并发送包括以下步骤：

（1）启动浏览器，在网址栏中输入 QQ 邮箱的登录网址，进入登录界面，通过自己的邮箱账户和密码登录邮箱。

（2）登录邮箱后，单击“写信”按钮，进入编辑新邮件页面，如图 3-41 所示。

图 3-41　编辑新邮件页面

（3）“收件人”为对方的邮箱地址，“抄送”为与此事相关需要知晓的人的邮箱地址，一般领导和其他需要知晓此事的人都在抄送人之列。“主题”为简明扼要描述邮件的主要内容和目的，让人一目了然，看主题就知道邮件的内容。“正文”一般以纸质信件的格式进行编写，有称谓、主要内容和落款等信息，需要注意在编写邮件的主要内容时，可以通过字体、颜色和格式等突出重点信息。

（4）单击“添加附件”，将已经加密的文件以附件的形式上传到邮件中，跟随邮件一起发送，编辑完成后，单击“发送”按钮进行发送，如图 3-42 所示。

3. 对文件进行完整性检查

加密文件跟随电子邮件在计算机网络中其实有被截获或者破坏的可能，根据信息安全

图 3-42 邮件编辑和发送

的要求,一般要将加密文件和加密密码、完整性校验码分开发送,防止被截获和破解。

图 3-43 Encrypto 解密过程

(1) 这里的 Encrypto 加密密码就是进行文件加密时输入的密码,对方收到邮件后,单击“下载”按钮,获得小强发送的加密文件,打开 Encrypto 应用程序,输入 Encrypto 加密密码进行解密,得到原始的文件资料。文件解密过程如图 3-43 所示。

(2) 事实上收到文件后一般还需要进行完整性校验,以验证收到的文件跟小强发送的文件是否是同一个文件,确保文件没有在传输过程中被截获和修改,以及被嵌入木马或者文件不完整等。

在实际应用中,通常使用 MD5 工具来进行完整性校验,可以使用 MD5 工具查看已经加密的文件信息和 MD5 值。MD5 工具有很多,可以在 360 软件管家直接安装,如图 3-44 所示。

(3) 这里下载的 MD5 工具是一个免安装的,下载解压后,双击可执行文件便可进入 MD5 工具使用面板,“计算类型”选择 MD5,单击“计算文件哈希值”,选择之前加密的文件,在“哈希值”和“字符串”栏中显示该加密文件的 MD5 哈希值和文件的详细信息。MD5 校验过程如图 3-45 所示。

(4) 小强的同事收到文件后会使用跟上一步完全一样的操作过程,验证他收到的这个加密文件的 MD5 哈希值,对比小强给的 MD5 哈希值,如果是一样的,则表明文件是完整且与发送的文件一致,否则就是存在安全问题的文件,需要丢弃处理。

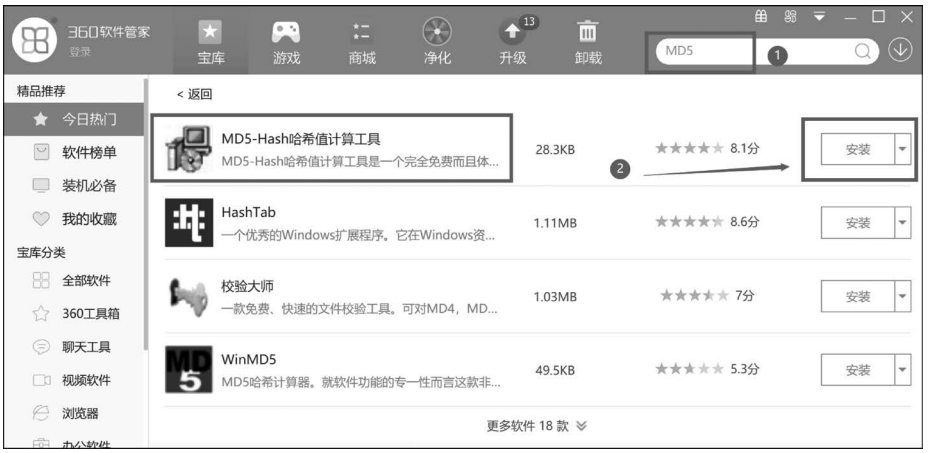


图 3-44　360 软件管家安装 MD5 工具

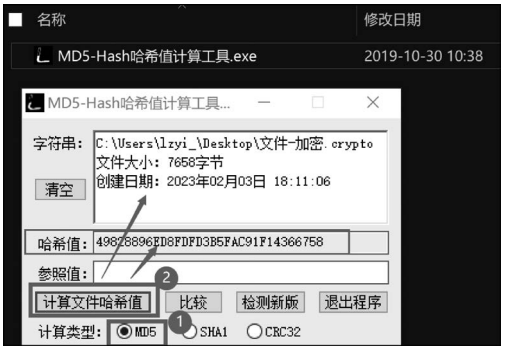


图 3-45　MD5 校验过程

人物介绍

蒂姆·伯纳斯·李

蒂姆·伯纳斯·李(Tim Berners-Lee),1955 年 6 月 8 日生于英格兰伦敦西南部,英国计算机科学家,1973 年,他中学毕业,进入牛津大学王后学院深造,最后以一级荣誉获得物理学士学位。2017 年,他因“发明万维网、第 1 个浏览器和使万维网得以扩展的基本协议和算法”而获得 2016 年度的图灵奖。历来也荣获 20 世纪最重要的 100 个人物,BBC 最伟大的 100 名英国人等诸多荣誉,也是公认的世界“互联网之父”。

1973 年,伯纳斯·李中学毕业,进入牛津大学王后学院深造。伯纳斯·李打小就是一个“不安分”的孩子,大学时代他用

电烙铁、晶体管-晶体管逻辑门、一块摩托罗拉 6800 微处理器和一台旧电视机制作了一台计算机,还因与一个朋友私自闯入其他计算机系统而被禁止使用大学的计算机。

大学毕业后,伯纳斯·李在欧洲粒子物理研究所担任软件工程顾问。在此期间,他一直构想可以采用超文本技术把研究所内部的各个实验室连接起来。试验成功后,他又不断修改立项书,规划在系统建成后,可以扩展到全世界。经过不断地修改和完善,1989 年仲夏之夜,伯纳斯·李成功地开发出世界上第 1 个网络服务器和第 1 个客户机,用户可以通过超文本传输协议从一台网络服务器转到另一台网络服务器上检索信息。同年 12 月,欧洲粒子物理研究所首次启动了万维网并成立了全球第 1 个网站,第二年万维网开始得到广泛应用。

在此之后,伯纳斯·李又相继制定了互联网的 URIs、HTTP、HTML 等技术规范,并在美国麻省理工学院成立了非营利性互联网组织——万维网联盟。

1960 年互联网开始出现,但是到了 1989 年之后才爆炸式地繁荣起来,业内普遍认为,伯纳斯·李发明的万维网起了决定性的作用,1989 年是互联网史上划时代的分水岭。

可能最初构成万维网的各个组成部分都很简单,伯纳斯·李的功绩在于将它们有效地组合在一起,使它们发挥出最大的效用。不过,他并未为“WWW”申请专利或者限制人们使用,从这个方面来讲,他最大的贡献是无偿地将他的主意提供出来供人们使用。

2012 年伦敦奥运会开幕式上有一个“感谢蒂姆”环节,伯纳斯·李坐在他熟悉的“计算机”前,打出了“This is for Everyone”字样,意为把互联网献给所有人。他是英国人的骄傲,并在那一刻接收到了来自全世界的感谢。

伯纳斯·李并没有靠万维网谋得财富。《时代》周刊将伯纳斯·李评为世纪最杰出的 100 位科学家之一,并称万维网只属于伯纳斯·李一个人,“与所有推动人类进程的发明不同,这是一件纯粹个人的劳动成果。他的发明在信息全球化的发展中的意义,可以比肩古印刷术。”

习题

1. 选择题

(1) 第 1 代计算机网络的特点是(　　)。

A. 没有主机　　B. 没有终端

C. 只有主机有运算和存储能力　　D. 具备分组交换能力

(2) 以下属于物理层的设备是(　　)。

A. 网卡　　B. 路由器　　C. 交换机　　D. 以上都是

(3) TCP 和 UDP 的相同点是(　　)。

A. 都是面向连接的协议　　B. 都是传输层协议

C. 都是面向非连接的协议　　D. 以上都不是

(4) DNS 是(　　)。

A. 域名解析服务器　　B. 地址解析协议

C. 一个网络中 DNS 只能有一个　　D. 以上描述都正确

(5) 光纤的纤芯是(　　)。

A. 塑料　　B. 铜　　C. 玻璃　　D. 合金

(6) 传输速度最快的是(　　)。

A. 双绞线　　B. 同轴电缆　　C. 网线　　D. 光纤

(7) IP 地址中全 1 的 IP 地址用于(　　)。

A. 广播　　B. 本机地址　　C. 网络号　　D. 主机号

(8) 信息安全的目标是要保证信息的保密性、完整性和(　　)。

A. 安全性　　B. 可用性　　C. 广泛性　　D. 灾难性

(9) 安全性最好的加密方式是(　　)。

A. MD5　　B. SHA1　　C. AES　　D. RSA

(10) 以下不是 MAC 地址的特点是(　　)。

A. 48 位串行号

B. 出厂就确定了,不能修改

C. 可以给每台计算机设置一个 MAC 地址

D. 每个网卡有一个唯一的 MAC 地址

2. 填空题

(1) 计算机网络中是根据_____来区分不同的设备的。

(2) 计算机网络中_____又叫地址解析协议,是可以根据 IP 地址获取 MAC 地址的协议。

(3) 第 1 代计算机网络的典型代表是_____。

(4) TCP/IP 协议模型四层结构分为应用层、_____、_____、网络接口层。

(5) 计算机网络主要有_____、高效数据交换、_____、分布式处理、高可靠性等的特点。

(6) 计算机网络按覆盖范围划分,可分为 _____、城域网、广域网和_____。

(7) 路由器的功能是在 OSI 模型中,完成_____及第 3 层中继任务。

(8) 计算机网络操作系统按工作的模式可以分为集中模式、_____和对等模式几种。

(9) 在计算机网络中著名的 TCP 和 UDP 协议在 TCP/IP 模型的_____层。

(10) 在信息安全中,常用的安全技术身份认证是证实实体对象的数字身份与物理身份是否一致的过程,身份认证具有_____、非描述性、_____几个特性。

3. 简答题

(1) 请描述计算机网络 TCP/IP 四层模型与 OSI 模型,以及两个模型的对应关系。

(2) 简述信息安全定义及如何防范信息安全。