第 3 章　计算机网络与云计算

计算机网络与云计算是现代信息技术的两大基石，它们相互依赖，共同推动了互联网和数字化服务的发展。计算机网络和云计算的结合，使得数据和计算能力可以跨越物理边界，实现全球范围内的资源共享和服务提供，这是现代互联网服务和数字化转型的基础。无论是大数据分析、人工智能模型训练等企业级应用，还是个人用户日常使用的云存储、在线教育和娱乐服务，都离不开计算机网络和云计算的支撑。

3.1　计算机网络

计算机网络是由多种通信手段相互连接起来的计算机复合系统，可实现数据通信和资源共享。Internet（因特网）是涵盖全球的计算机网络，通过 Internet 不仅可以获取分布在全球的多种信息资源，还能够获得方便、快捷的电子商务服务及方便的远程协作。

3.1.1　计算机网络的基本概念

1．网络的概念

计算机网络是指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、网络管理软件及网络通信协议的管理和协调下，实现资源共享和信息传递的计算机系统。

从宏观角度看，计算机网络一般由资源子网和通信子网两部分构成，如图3.1 所示。

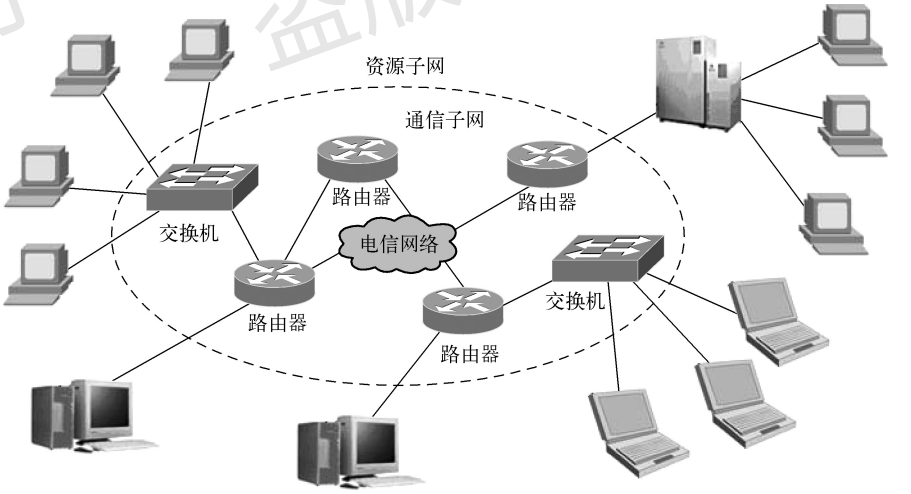


图 3.1　计算机网络的构成

（1）资源子网

资源子网主要由网络中所有的主计算机、I/O 设备和终端、各种网络协议、网络软件和数据库等组成，负责全网的信息处理，为网络用户提供网络服务和资源共享功能等。

（2）通信子网

通信子网主要由通信线路、网络连接设备（如网络接口设备、通信控制处理机、网桥、路

由器、交换机、网关、调制解调器和卫星地面接收站等）、网络通信协议和通信控制软件等组成，负责全网的数据通信，为网络用户提供数据传输、转接、加工和转换等通信处理工作。

2．基本特征

网络的定义从不同的方面描述了计算机网络的三个特征。

（1）联网的目的在于资源共享

可共享的资源包括硬件、软件和数据。

（2）互联的计算机应该是独立计算机

联网的计算机既可以联网工作也可以单机工作。如果一台计算机带多台终端和打印机，则这种系统通常被称为多用户系统，而不是计算机网络。由一台主控机和多台从控机构成的系统是主从式系统，也不是计算机网络。

（3）联网计算机遵守统一的协议

计算机网络由许多具有信息交换和处理能力的节点互联而成。若使整个网络有条不紊地工作，则要求每个节点必须遵守事先约定好的有关数据格式及时序等内容的规则。这些为实现网络数据交换而建立的规则、约定或标准就称为网络协议。

3.1.2 计算机网络的基本组成

根据网络的概念，计算机网络一般由三部分组成：计算机、通信线路、网络设备、网络软件。

1．计算机

联网计算机根据其作用和功能不同，可分为服务器和客户机两类。

服务器是整个网络系统的核心，它为网络用户提供服务并管理整个网络，在其上运行的操作系统是网络操作系统。随着局域网络功能的不断增强，根据服务器在网络中所承担的任务和所提供的功能不同，把服务器分为文件服务器、邮件服务器、打印服务器和通信服务器等。

客户机又称工作站，客户机与服务器不同，服务器为网络上许多用户提供服务和共享资源。客户机是用户和网络的接口设备，用户通过它可以与网络交换信息、共享网络资源。现在的客户机都由具有一定处理能力的个人计算机来承担。

2．通信线路

通信线路也称传输介质，是数据信息在通信系统中传输的物理载体，是影响通信系统性能的重要因素。传输介质通常分为有线介质和无线介质。有线介质包括双绞线、光纤等，而无线介质（包括卫星、红外线、激光、微波等）利用自由空间进行信号传播。衡量传输介质性能的重要概念包括带宽、衰减损耗、抗干扰性。带宽决定了信号在传输介质中的传输速率，衰减损耗决定了信号在传输介质中能够传输的最大距离，传输介质的抗干扰特性决定了传输系统的传输质量。

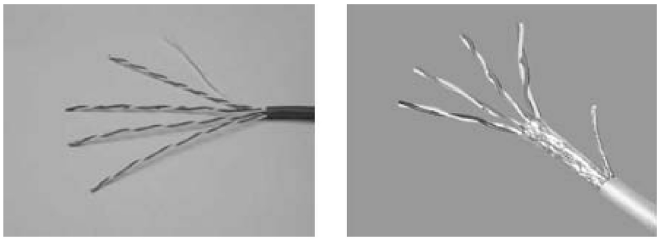
（1）有线传输

① 双绞线。

双绞线是最常用的传输介质，可以传输模拟信号或数字信号。双绞线是由两根相同的绝缘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，两根线缠绕的目的是减小相互之间的信号干扰。如果把多对双绞线放在一个导管中，则形成由多根双绞线组成的电缆。

局域网中的双绞线分为两类：屏蔽双绞线（Shielded Twisted Pair，STP）与非屏蔽双绞线（Unshielded Twisted Pair，UTP），如图 3.2 所示。屏蔽双绞线由外部保护层、屏蔽层与多对双

绞线组成；非屏蔽双绞线由外部保护层与多对双绞线组成。屏蔽双绞线对电磁干扰具有较强的抵抗能力，适用于网络流量较高的高速网络，而非屏蔽双绞线适用于网络流量较低的低速网络。



（a）非屏蔽双绞线　　（b）屏蔽双绞线

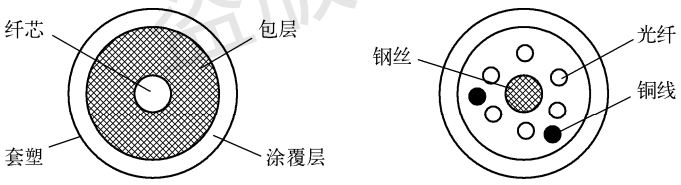
图 3.2　双绞线

双绞线的衰减损耗较高，因此不适合远距离的数据传输。普通双绞线传输距离限定在 100m 之内，一般速率为 100Mbps，高速可到 1Gbps。

② 光纤。

光纤是光导纤维的简称，是一种利用光在玻璃或塑料制成的纤维中按照全反射原理进行信号传递的光传导工具。光纤由纤芯、包层、涂覆层和套塑四部分组成，如图 3.3（a）所示。纤芯在中心，是由高折射率的高纯度二氧化硅材料组成的，主要用于传送光信号。包层由掺有杂质的二氧化硅组成，其光折射率比纤芯的折射率低，使光信号能在纤芯中产生全反射传输。涂覆层及套塑的主要作用是加强光纤的机械强度。

在实际工程应用中，光纤要制作成光缆，光缆一般由多根纤芯绞制而成，纤芯数量可根据实际工程要求而绞制，如图 3.3（b）所示。光缆要有足够的机械强度，所以在光缆中用多股钢丝来充当加固件。有时还在光缆中绞制一对或多对铜线，用于电信号传送或作为电源线。



（a）光纤　　（b）光缆

图 3.3　光纤与光缆

（2）无线传输

无线通信是利用电磁波信号可以在自由空间中传播的特性进行信息交换的一种通信方式，主要包括微波通信、卫星通信、无线通信等。

① 微波通信。

微波是指频率为 300MHz～300GHz 的电磁波，是无线电波中一个有限频带的简称，即波长为 1mm～1m（不含 1m）的电磁波，是分米波、厘米波、毫米波的统称。微波沿着直线传播，具有很强的方向性，只能进行视距离传播。因此，发射天线和接收天线必须精确地对准。由于微波长距离传送时会发生衰减，因此每隔一段距离就需要有一个中继站。

② 卫星通信。

为了增加微波的传输距离，应提高微波收发器或中继站的高度。当将微波中继站放在人造卫星上时，便形成了卫星通信系统。

卫星通信可以分为两种方式：一种是点对点方式，通过卫星将地面上的两个点连接起来；

另一种是多点对多点方式，即一颗卫星接收几个地面站发来的数据信号，然后以广播的方式将所收到的信号发送到多个地面站。多点对多点方式主要应用于电视广播系统、远距离电话及数据通信系统。

卫星通信的优点是：覆盖面积大、可靠性高、信道容量大、传输距离远、传输成本不随距离的增加而增大，主要适用于远距离广域网络的传输。其缺点是：卫星成本高、传播延迟时间长、受气候影响大、保密性较差。

③ 无线通信。

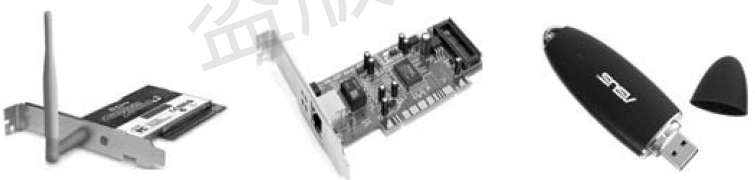
无线通信指多个通信设备之间以无线电波为介质遵照某种协议实现信息的交换，比较流行的有无线局域网、蓝牙技术、蜂窝移动通信技术等。无线局域网和蓝牙技术只能用于较小范围（10～100m）的数据通信。无线局域网主要采用 2.4GHz 频段，目前应用广泛的无线局域网是 IEEE802.11b、IEEE802.11g、IEEE802.11a 标准。蓝牙是无线数据和语音传输的开放式标准，也使用 2.4GHz 射频无线电，它将各种通信设备、计算机及其终端设备、各种数字数据系统及家用电器采用无线方式连接起来，从而实现各类设备之间随时随地进行通信，其传输范围为 10m 左右，最大数据速率可达 721Kbps。蓝牙技术的应用范围越来越广泛。

3．网络设备

网络设备包括用于网内连接的网卡（即网络适配器）、调制解调器、交换机、中继器、路由器、网桥、网关等。

（1）网卡

网卡用于实现联网计算机和网络电缆之间的物理连接，完成计算机信号格式和网络信号格式的转换。通常，网卡就是一块插件板，插在 PC 的扩展槽中并通过这条通道进行高速数据传输。在局域网中，每台联网计算机都需要安装一块或多块网卡，通过网卡将计算机接入网络电缆系统。常见的网卡如图 3.4 所示。



（a）无线网卡　　（b）普通网卡　　（c）USB无线网卡

图 3.4　网卡

（2）调制解调器

调制解调器使用广泛，尤其在智能手机和光纤通信中扮演着重要角色。调制解调器的主要功能是将模拟信号和数字信号进行转换，使得计算机或其他设备能够通过电话线或电缆等介质连接到互联网。尽管技术不断进步，但调制解调器的核心作用没有变，只是形式和性能上有所变化和提升。例如，在智能手机中，调制解调器与基带芯片集成在一起，负责处理手机通信和数据传输，从 3G、4G 到 5G 时代，其重要性一直在增加。

下面以手机通信为例介绍调制解调器的工作过程。

手机调制解调器在手机通信中扮演着不可或缺的角色。当打开手机并开始拨号时，调制解调器便开始工作。调制解调器将来自手机的数字信号转换成一种模拟信号，再通过天线发送出去。与此同时，调制解调器正在收听、处理从基站接收到的信号，并将接收到的信号解析成数字信号，传递给处理器完成进一步处理。因此，调制解调器可以说是手机通信的关键部件之一，在保证通信质量和高效率的基础上，提供了平稳和可靠的数据传输。

（3）交换机

交换机（Switch）是一种用于电信号转发的网络设备，如图 3.5 所示。它可以为接入交换机的任意两个网络节点提供独享的电信号通路。最常见的交换机是以太网交换机。在计算机网络系统中，交换概念的提出改进了共享工作模式。

图 3.5　交换机

交换机拥有一条带宽很高的背部总线和内部交换矩阵。交换机所有的端口都挂接在这条背部总线上，控制电路收到数据包以后，会查找地址映射表以确定目的计算机挂接在哪个端口上，通过内部交换矩阵迅速在数据帧的始发者和目标接收者之间建立临时的交换路径，使数据帧直接由源地址到达目的地址。

交换机的工作原理如图 3.6 所示，图中的交换机有 6 个端口，其中端口 1、4、5、6 分别连接节点 A、节点 B、节点 C 与节点 D。交换机的“端口号/MAC 地址映射表”可以根据以上端口号与节点 MAC 地址的对应关系建立起来。如果节点 A 与节点 D 同时要发送数据，那么它们可以分别在数据帧的目的地址字段（DA）中添上该帧的目的地址。例如，若节点 A 要向节点 C 发送帧，那么该帧的目的地址 DA=节点 C；若节点 D 要向节点 B 发送帧，那么该帧的目的地址 DA=节点 B。当节点 A，节点 D 同时通过交换机传送帧时，交换机的交换控制中心根据“端口号/MAC 地址映射表”的对应关系找出帧的目的地址的输出端口号，那么它就可以为节点 A 到节点 C 建立端口 1 到端口 5 的连接，同时为节点 D 到节点 B 建立端口 6 到端口 4 的连接。这种端口之间的连接可以根据需要同时建立多条，也就是说可以在多个端口之间建立多个并发连接。

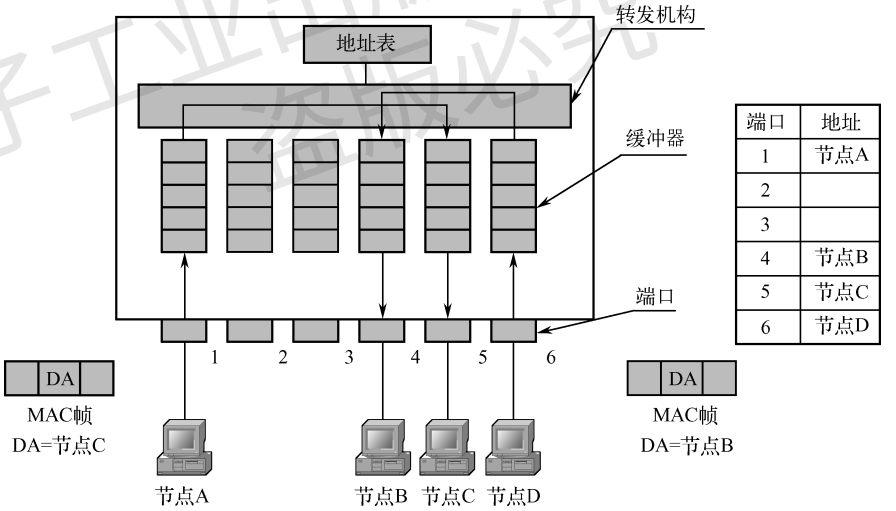


图 3.6　交换机的工作原理

目前，局域网交换机主要是针对以太网设计的。一般来说，局域网交换机主要有低交换传输延迟、高传输带宽、允许不同速率的端口共存、支持虚拟局域网服务等几个技术特点。交换机组网示意图如图 3.7 所示。

（4）中继器

中继器（Repeater）是网络物理层上面的连接设备，用于完全相同的两类网络的互联。受传输线路噪声的影响，承载信息的数字信号或模拟信号只能传输有限的距离，中继器的功能是对接收信号进行再生和发送，从而增加信号的传输距离。例如，以太网常常利用中继器扩展总线的电缆长度，标准细缆以太网的每段长度最大为 185m，最多可有 5 段。因此，通

过 4 个中继器将 5 段连接后，最大网络电缆长度则可增加到 925m。

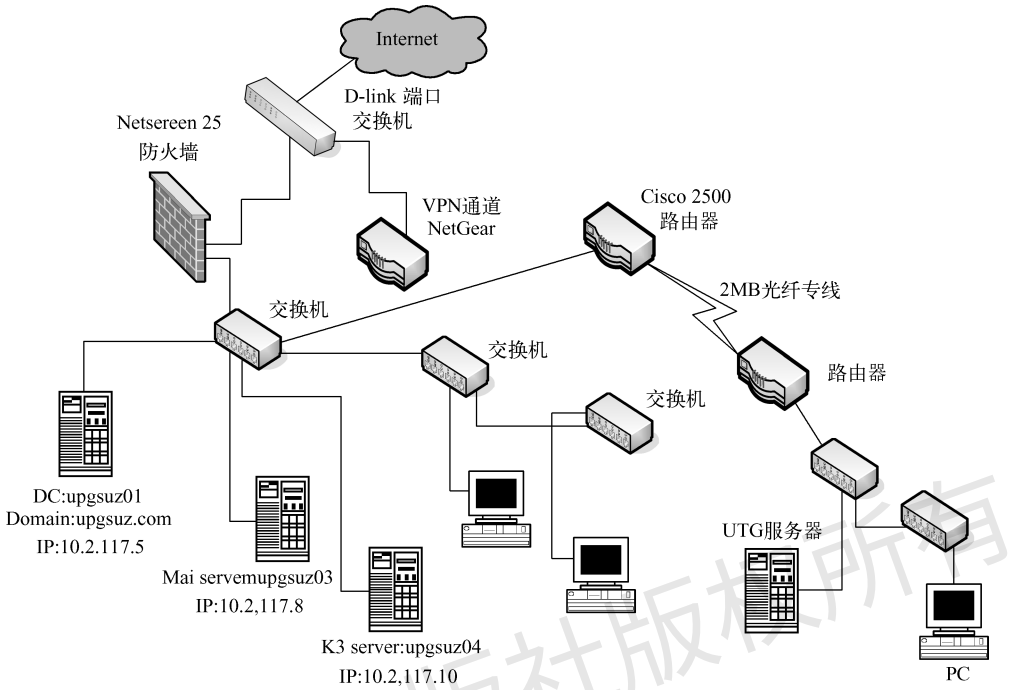


图 3.7　交换机组网示意图

（5）路由器

路由器（Router）是互联网的主要节点设备，作为不同网络之间互相连接的枢纽，路由器系统构成了基于 TCP/IP 的 Internet 的骨架。路由器联网示意图如图 3.8 所示。

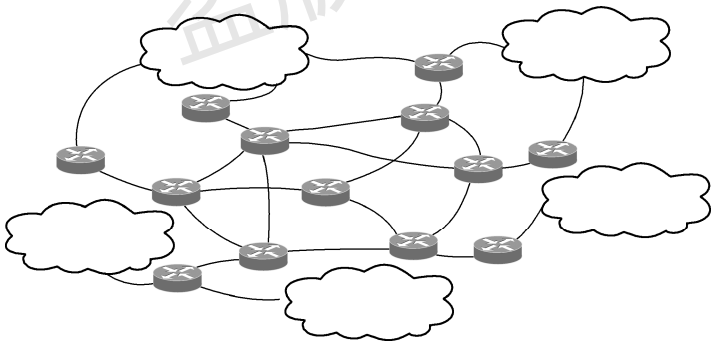


图 3.8　路由器联网示意图

路由器通过路由选择决定数据的转发，它的处理速度是网络通信的主要瓶颈之一，它的可靠性则直接影响着网络互联的质量。因此，在局域网乃至整个 Internet 研究领域中，路由器技术始终处于核心地位。

路由器的主要工作就是为经过路由器的每个数据报寻找一条最佳传输路径，并将该数据有效地传送到目的站点。选择最佳传输路径的策略是路由器的关键所在，为了完成这项工作，在路由器中保存着各种传输路径的相关数据（路由表）。路由表保存着子网的标志信息、网上路由器的个数和下一个路由器的名字等内容。路由表既可以由系统管理员固定设置（静态路由表），也可以由系统动态修改（动态路由表）。

（6）网桥

网桥工作于数据链路层，网桥不但能扩展网络的距离或范围，而且还可提高网络的性能、可靠性和安全性。通过网桥可以将多个局域网连接起来。网桥联网示意图如图 3.9 所示。

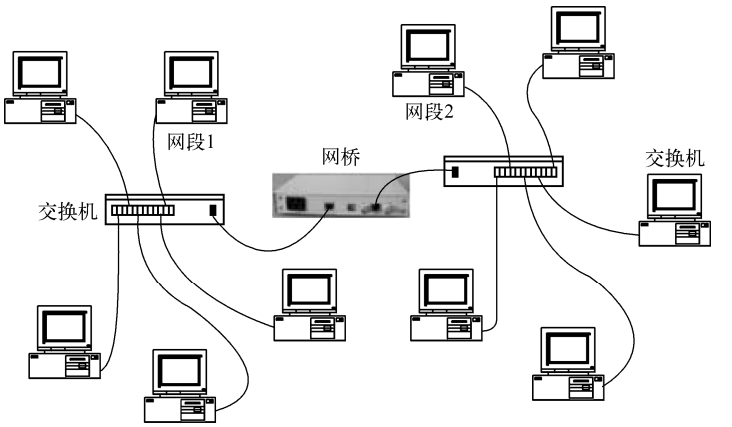


图 3.9　网桥联网示意图

当使用网桥连接两段局域网时，对于来自网段 1 的帧，网桥首先检查其终点地址，如果该帧是发往网段 1 上某站的，则网桥不将帧转发到网段 2，而将其滤除；如果该帧是发往网段 2 上某站的，网桥则将它转发到网段 2。这样可利用网桥隔离信息，将网络划分成多个网段，隔离出安全网段，防止其他网段内的用户非法访问。由于各个网段相对独立，所以一个网段出现故障不会影响到另一个网段。

（7）网关

网关（Gateway）又称网间连接器、协议转换器。网关在高层（传输层以上）实现网络互联，是最复杂的网络互联设备，用于两个高层协议不同的网络互联。网关既可以用于广域网互联，又可以用于局域网互联。在使用不同的通信协议、数据格式或语言，甚至体系结构完全不同的两种系统之间，网关是一个翻译器，网关对收到的信息要重新打包，以适应目的系统的需求。同时，网关也可以提供过滤和安全功能。大多数网关运行在应用层。

4．网络软件

网络软件在网络通信中扮演了极为重要的角色。网络软件可大致分为网络系统软件和网络应用软件。

（1）网络系统软件

网络系统软件控制和管理网络运行、提供网络通信和网络资源分配与共享功能，它为用户提供了访问网络和操作网络的友好界面。网络系统软件主要包括网络操作系统（NOS）和网络协议软件。

一个计算机网络拥有丰富的软、硬件资源和数据资源，为了能使网络用户共享网络资源、实现通信，需要对网络资源和用户通信过程进行有效管理，实现这一功能的软件系统称为网络操作系统。常见的网络操作系统有 Microsoft 公司的 Windows 7 和 Sun 公司的 UNIX 等。

网络中的计算机之间交换数据必须遵守一些事先约定好的规则。这些为网络数据交换而制定的关于信息顺序、信息格式和信息内容的规则、约定与标准被称为网络协议（Protocol）。目前常见的网络通信协议有：TCP/IP、SPX/IPX、OSI 和 IEEE802。其中，TCP/IP 是任何要连接到 Internet 上的计算机必须遵守的协议。

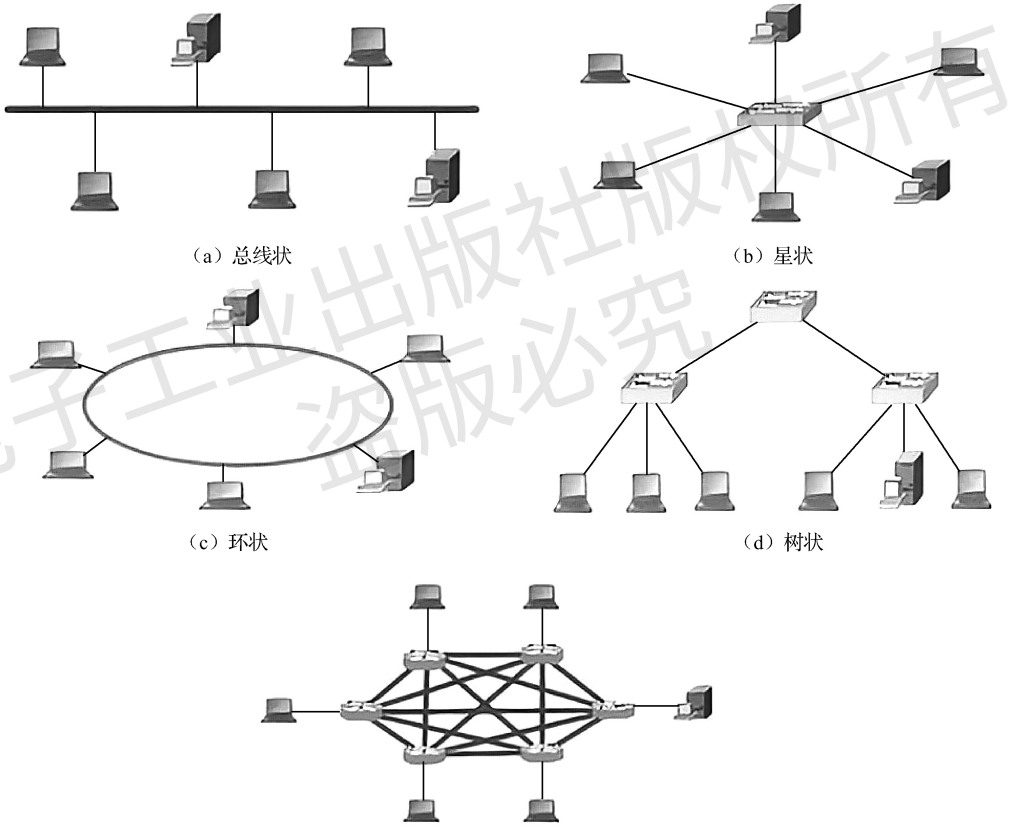
（2）网络应用软件

网络应用软件是指为某个应用目的而开发的网络软件。网络应用软件既可用于管理和维护网络本身，又可用于某个业务领域，如网络管理监控程序、网络安全软件、数字图书馆、Internet 信息服务、远程教学、远程医疗、视频点播等。网络应用的领域极为广泛，网络应用软件也极为丰富。

3.1.3 计算机网络的分类

1．拓扑结构

为了描述网络中节点之间的连接关系，将节点抽象为点，将线路抽象为线，进而得到一个几何图形，称为该网络的拓扑结构。不同的网络拓扑结构对网络性能、系统可靠性和通信费用的影响不同。计算机网络中常见的拓扑结构有总线状、星状、环状、树状、网状等，如图 3.10 所示。



（a）总线状　（b）星状　（c）环状　（d）树状　（e）网状

图 3.10　网络拓扑结构

其中，总线状、环状、星状拓扑结构常用于局域网，网状拓扑结构常用于广域网。

（1）总线状拓扑结构

总线状拓扑通过一根传输线路将网络中所有节点连接起来，这根线路称为总线。网络中各节点都通过总线进行通信，在同一时刻只能允许一对节点占用总线进行通信。随着技术进步，许多网络已经转向星状或网状拓扑结构，但总线状拓扑仍然在特定场合中发挥着重要作用。对于需要低成本且规模小的网络环境，总线状拓扑是一个经济有效的选择。然而，对于需要高可靠性和扩展性的网络，可能需要考虑其他更先进的拓扑结构。

特点：在总线状拓扑结构中，所有设备通过一条共享的电缆连接。每个节点通过分支接口连接到主电缆上。

优点：结构简单，安装方便，成本较低，各节点共用一条传输信道。

缺点：故障排查困难，信号随着传输距离的增加会衰减，一个节点的故障可能会影响整个网络。

（2）星状拓扑结构

星状拓扑中各节点都与中心节点连接，呈辐射状排列在中心节点周围。网络中任意两个节点的通信都要通过中心节点转接。单个节点的故障不会影响到网络的其他部分，但中心节点的故障会导致整个网络的瘫痪。

特点：在星状拓扑结构中，每个节点通过单独的电缆连接到中心节点，如集线器或交换机。

优点：易于管理和维护，单点故障不会影响整个网络，扩展性好。

缺点：中心节点出现故障会导致整个网络瘫痪，布线成本较高。

（3）环状拓扑结构

环状拓扑中各节点首尾相连形成一个闭合的环，环中的数据沿环单向逐站传输。环状拓扑中的任意一个节点或一条传输介质出现故障都将导致整个网络的故障。环状拓扑结构在网络设计中提供了一些独特的优势，尤其适用于某些特定应用。尽管其他拓扑结构如星状或网状拓扑在现代网络中更为常见，但环状拓扑依然在特定场景中发挥着重要作用

特点：环状拓扑结构中的每个节点连接两个相邻节点，形成一个闭合环路，数据在环中单向传输。

优点：适合实时控制，信号传输延时固定，无须复杂的路由选择。

缺点：可靠性低，一个节点或线路的故障会影响整个网络，维护和扩展比较困难。

（4）树状拓扑结构

树状拓扑由星状拓扑演变而来，其结构图看上去像一棵倒立的树。树状网络是分层结构，具有根节点和分支节点，适用于分级管理和控制系统。

特点：树状拓扑结构是分层的，根节点以下分出多个分支和子节点，形成层次式布局。

优点：路径选择简单，扩展容易，便于故障隔离，适合构建大型网络。

缺点：依赖根节点，数据传输效率受层级结构影响。

（5）网状结构

网状结构的每个节点都有多条路径与网络相连，如果一条线路出故障，通过路由选择可找到替换线路，网络仍然能正常工作。这种结构可靠性强，但网络控制和路由选择较复杂，广域网采用的是网状拓扑结构。

特点：网状拓扑结构中每个节点至少与其他两个节点相连，形成网状连接。

优点：可靠性高，多条路径可选，容错能力强，适合广域网。

缺点：成本高，布线复杂，维护难度大。

2．基本分类

虽然网络类型的划分标准各种各样，但根据地理范围划分是一种大家都认可的通用网络划分标准。按这种标准可以把网络类分为局域网、城域网和广域网三种。不过要说明的一点是，网络划分并没有严格意义上地理范围的区分，只是一个定性的概念。

（1）局域网（LAN）

局域网是最常见、应用最广的一种网络。局域网覆盖的地区范围较小，所涉及的地理距

离一般可以是几米至 10km 以内。这种网络的特点是：连接范围窄、用户数少、配置容易、连接速率高。目前，局域网的最快速率是 10Gbps。IEEE 的 802 标准委员会定义了多种主要的 LAN：以太网（Ethernet）、令牌环网（Token Ring）、光纤分布式接口网络（FDDI）、异步传输模式网（ATM）及最新的无线局域网（WLAN）。其中，使用最广泛的是以太网。

（2）城域网（MAN）

城域网是在一个城市范围内所建立的计算机通信网。这种网络的连接距离在几十千米左右，它采用的是 IEEE802.6 标准。城域网的一个重要用途是作为骨干网，城域网以 IP 技术和 ATM 技术为基础，以光纤作为传输媒介，将位于不同地点的主机、数据库及局域网等连接起来，实现集数据、语音、视频服务于一体多媒体数据通信；满足城市范围内政府机构、金融保险、大中小学校、公司企业等单位对高速率、高质量数据通信业务日益旺盛的需求。

（3）广域网（WAN）

广域网是一种跨越大范围区域、连接多个局域网的网络结构。它能够实现远距离通信和资源共享，其覆盖范围从几十公里到几千公里。在实际应用中，广域网常被用于连接跨国公司的分支机构、实现远程教育、提供云计算服务等。与局域网相比，广域网具有更广泛的覆盖范围和更高的传输容量，但同时也带来了更高的成本和更大的网络复杂性。

3．我国广域网服务商

我国广域网服务商主要有中国移动、中国电信、中国联通、阿里云、腾讯云等。这些服务商通过 SD-WAN 技术和其他网络服务，为企业提供高效、安全的广域网络连接解决方案。企业在选择服务商时，应综合考虑网络覆盖、运维能力、服务质量和成本等因素，以确保获得最佳网络连接和高效运维支持。

（1）中国移动

中国移动提供 SD-WAN 产品，支持全球组网、上云及安全融合服务。其基于全球云网融合底座的弹性扩展网络架构，能够平滑地支持 SASE（安全访问服务边缘），将 SD-WAN 网络功能和安全功能整合在一起。

（2）中国电信

中国电信结合全球分布的云平台，以 Overlay SD-WAN 的方式实现广域灵活组网，具有带宽按需弹性调度（BoD）、业务及时开通等优点。上海电信的“翼互联”SD-WAN 产品实现了 5G+多云+SASE 安全的企业融合组网需求。

（3）中国联通

中国联通正在向广域网的 SDN 化及产品服务化大规模演进，依托骨干网构建 SD-WAN 边缘接入网络，实现多网结合、多云互联。其智选专线产品为客户提供云+网+应用服务一体化的综合服务，并支持多种接入方式，满足不同业务需求。

（4）阿里云

阿里云通过其智能接入网关终端绑定到云连接网，再绑定到云企业网，实现线下接入矩阵和云上中心矩阵全连接。这种设置可以极大提高网络的快速收敛和跨网络通信的质量和安全性。

（5）腾讯云

腾讯云的“云联网”服务能够实现 VPC 间、VPC 与本地数据中心间的互联，通过智能调度和路由学习特性，构建极速、稳定、经济的全网互联。

3.2 局域网技术

局域网广泛应用于学校、企业、机关、商场等机构，为这些机构的信息技术应用和资源共享提供了良好的服务平台。局域网的典型拓扑结构有总线状、星状、环状。

3.2.1 交换式以太网

在传统以太网中，采用集线器作为中心节点，但集线器不能作为大规模局域网的选择方案。交换式以太网的核心设备是局域网交换机，交换机可以在多个端口之间建立多个并发连接，解决了共享介质的互斥访问问题。这种将主机直接与交换机端口连接的以太网称为交换式以太网，主机连接在以太网交换机的各个端口上，主机之间不再发生冲突，也不需要CSMA/CD来控制链路的争用。

交换式以太网是一种基于交换机的高速网络，它解决了共享式以太网中的许多问题，提高了网络传输效率和性能。

1．工作原理

（1）数据帧传输

当计算机发送一个数据帧到网络上时，交换机会读取该数据帧中的目标MAC地址，并将其与内部的MAC地址表进行比对，然后决定将数据帧转发到哪个接口。

（2）MAC地址表建立

交换机自动学习并记录每个设备的MAC地址，以及它们连接的接口。这样，在后续的数据传输过程中，交换机可以快速确定目标设备所在的接口，从而提高传输效率。

（3）广播和多播管理

当接收到广播或多播数据帧时，交换机会将其转发到所有其他接口，确保所有目标设备能够接收到这些数据。

2．技术优势

（1）避免网络拥塞

交换式以太网可以避免共享式以太网中常见的网络拥塞问题。在共享式以太网中，所有设备共享同一个信道，容易因数据包过多而产生冲突和拥塞，导致传输效率降低。交换式以太网则通过划分虚拟子网，为每个子网提供独立信道，从而有效避免了拥塞。

（2）全双工通信

交换式以太网支持全双工通信模式，这意味着数据可以同时双向传输，大大提高了网络的实际带宽。传统共享式以太网只能实现半双工通信，容易发生碰撞和延迟。

（3）高性能传输

由于交换机能够精确地将数据转发到目标端口，网络中的其他设备不受传输影响，因此可以实现更高的网络性能和较低的延迟。

（4）提高网络安全性

通过使用VLAN和其他安全设置，交换式以太网可以更好地保护数据安全，防止未经授权的网络访问

3.2.2 无线局域网

无线局域网（WLAN）是一种无线网络技术，用于实现计算机设备间的互联和通信，从而形成一个可以互相通信和实现资源共享的网络体系。它通过无线信道代替有线传输介质，

使得网络构建和终端移动更加灵活。

无线局域网的核心特点在于其不使用通信电缆，而是利用射频或电磁波在空中进行通信连接，从而避免了传统有线网络布线的复杂性和局限性。这种技术在办公楼、商场、家庭等多种场景中广泛应用，其便捷的部署和使用方式大大提高了网络的灵活性和扩展性。一个典型的无线局域网如图 3.11 所示。AP 是数据发送和接收设备，称为接入点。

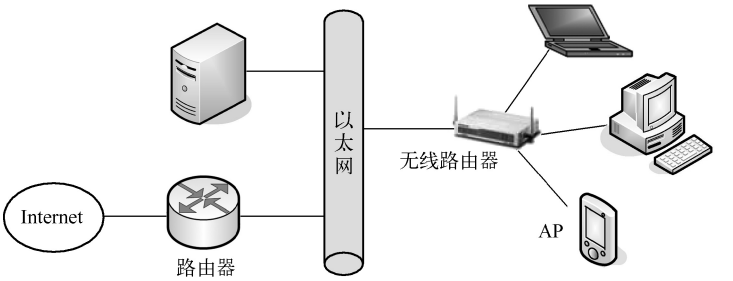


图 3.11　典型的无线局域网

1．基本原理

（1）组成元素

无线局域网的基本组件包括站（Station，STA），这些站可以是带有无线网卡的计算机或其他设备。

接入点（Access Point，AP），作为无线局域网的核心，负责与各个站的连接和管理。

分布式系统（Distribution System，DS），用于将多个 AP 连接在一起，扩展网络覆盖范围。

（2）拓扑结构

分布对等式拓扑（Peer to Peer）：适用于少数设备间的直接连接。

基础结构集中式拓扑（Infrastructure）：通常由一个或多个 AP 构成，为所有 STA 提供网络连接。

ESS 网络拓扑：由多个 BSS（Basic Service Set，基本服务集）通过 DS 互联形成 ESS（Extended Service Set，扩展服务集）。

2．通信标准

（1）早期标准

IEEE 802.11 标准于 1997 年发布，标志着无线局域网技术的规范化，初始速率为 1～2Mbps。

后续又发布了 IEEE 802.11a 和 802.11b 标准，它们分别工作在 5GHz 和 2.4GHz 频段，速率分别达到 54Mbps 和 11Mbps。

（2）现代标准

IEEE 802.11n 和 802.11ac 标准进一步提升了传输速率，它们分别工作在 2.4GHz 和 5GHz 频段，最高速率可达 600Mbps 和千兆级别。

最新的 Wi-Fi 6 标准（IEEE 802.11ax），在 2.4GHz、5GHz 及新增的 6GHz 频段上，进一步提高了每区域吞吐量和速率，适应了高密度网络环境。

3．应用场景

（1）家庭网络

家庭中的无线路由器可以为多台设备提供便捷的网络连接，实现共享上网、文件传输和媒体播放等功能。

家庭网络通常采用单一 AP 集中式部署，设置简单且易于扩展。

（2）企业网络

大中型园区常采用“AC+FIT AP”模式，通过无线控制器（AC）管理和控制多个瘦 AP（FIT AP），实现用户在不同 AP 间的无缝漫游。

小型企业则可以采用胖 AP（FAT AP），独立完成覆盖，但无法实现 AP 间的漫游功能。

4．优缺点

（1）优点

① 灵活性和移动性。

无线局域网用户可以在无线信号覆盖区域内任何位置接入网络，并保持同时移动和连接。

② 安装便捷。

免去或减少了复杂的网络布线，只需部署一个或多个 AP 即可建立广泛覆盖的网络。

③ 易于扩展。

无线局域网可以从小型局域网快速扩展至大型网络，并提供节点间的漫游特性。

（2）不足

① 性能受限。

无线电波易受建筑物、车辆等障碍物阻碍，影响网络性能。

② 速率较低。

相比有线网络，无线信道的传输速率较低，最大传输速率通常为 1Gbps。

③ 安全性问题。

开放的无线信道容易受到窃听和攻击，需要采取链路认证和数据加密等措施提高安全性。

3.3 Internet 技术

任何网络只有与其他网络相互连接，才能使不同网络上的用户相互通信，以实现更大范围的资源共享和信息交流。通过相关设备，将全世界范围内的计算机网络互联起来形成一个范围涵盖全球的大网，这就是 Internet。

3.3.1 基本概念

1．Internet 体系结构

Internet 的核心协议是 TCP/IP 协议，也是实现全球性网络互联的基础。TCP/IP 协议采用分层化的体系结构，共分为 5 个层次，分别是物理层、数据链路层、网络层、传输层、应用层，每层都有相应的数据传输单位和不同的协议。Internet 体系结构如图 3.12 所示。

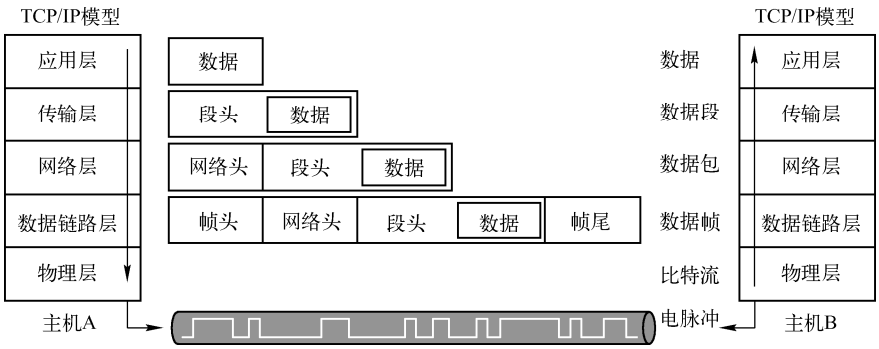


图 3.12　Internet 体系结构

TCP/IP 协议的名称的来源于 Internet 层次模型中的两个重要协议：工作于传输层的 TCP 协议（Transmission Control Protocol，传输控制协议）和工作于网络层的 IP 协议（Internet Protocol，Internet 协议）。网络层的功能是在不同网络之间以统一的数据分组格式（IP 数据报）传递数据信息和控制信息，从而实现网络互联。传输层的主要功能是对网络中传输的数据分组提供必要的传输质量保障。应用层可以实现多种网络应用，如 Web 服务、文件传输、电子邮件服务等。

（1）Internet 数据传输的基本过程

主机 A：应用层负责将要传递的信息转换成数据流，传输层将应用层提供的数据流分段，称为数据段（段头+数据），段头主要包含该数据由哪个应用程序发出、使用什么协议传输等控制信息。传输层将数据段传给网络层。网络层将传输层提供的数据段封装成数据包（网络头+数据段），网络头包含源 IP 地址、目标 IP、使用什么协议等控制信息，网络层将数据包传输给数据链路层。数据链路层将数据封装成数据帧（帧头+数据包+帧尾），帧头包含源 MAC 地址、目标 MAC 地址、使用什么协议封装等信息，数据链路层将数据帧传输给物理层形成比特流，并将比特流转换成电脉冲通过传输介质发送出去。

主机 B：物理层将电信号转变为比特流，提交给数据链路层，数据链路层读取该数据帧的帧头信息，如果是发给自己的，则去掉帧头，并交给网络层处理；如果不是发给自己的，则丢弃该数据帧。网络层读取网络头的信息，检查目标地址，如果是发给自己的，则去掉网络头交给传输层处理；如果不是，则丢弃该数据包。传输层根据段头中的端口号传输给应用层某个应用程序。应用层读取数据段的段头信息，决定是否进行数据转换、加密等，最后主机 B 获得了主机 A 发送的信息。

（2）网络层协议

网络层的主要协议是 IP 协议，它是建造大规模异构网络的关键协议，各种不同的物理网络（如各种局域网和广域网）通过 IP 协议能够互联起来。Internet 上的所有节点（主机和路由器）都必须运行 IP 协议。为了能够统一不同网络技术数据传输所用的数据分组格式，Internet 采用统一 IP 分组（称为 IP 数据报）在网络之间进行数据传输，通常情况下这些数据分组并不是直接从源节点传输到目的节点的，而是穿过由 Internet 路由器连接的不同的网络和链路。

IP 协议工作过程如图 3.13 所示。

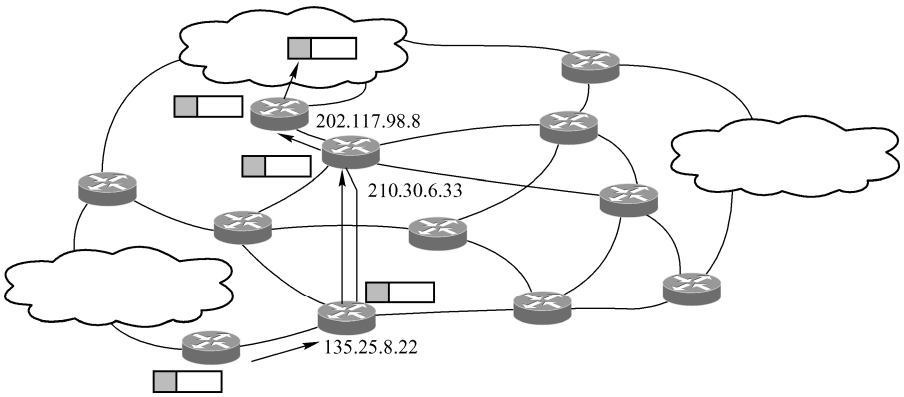


图 3.13　IP 协议工作过程

IP 协议以 IP 数据包的分组形式从发送端穿过不同的物理网络，经路由器选路和转发最终到达目的端。例如，源主机发送一个到达目的主机的 IP 数据包，IP 协议查路由表，找到下一个地址应该发往路由器 135.25.8.22（路由器 1），IP 协议将 IP 数据包转发到路由器 1，

路由器 1 收到 IP 数据包，提取 IP 数据包中的目的地址的网络号，在路由表中查找目的网络应该发往路由器 210.30.6.33（路由器 2），IP 协议将 IP 数据包转发到路由器 2，路由器 2 收到 IP 数据包，提取 IP 数据包中的目的地址的网络号，在路由表中查找目的网络应该发往路由器 202.117. 98.8（路由器 3），IP 协议将 IP 数据包转发到路由器 3，路由器 3 收到 IP 数据包后将数据包转发到目的主机。

（3）传输层协议

IP 数据包在传输过程中可能出现分组丢失、传输差错等错误。要保证网络中数据传输正确，应该设置另一种协议，这个协议应该准确地将从网络中接收的数据递交给不同的应用程序，并能够在必要时为网络应用提供可靠的数据传输服务质量，这就是工作于传输层的 TCP 协议和 UDP 协议（User Datagram Protocol，用户数据报协议）。

这两种协议的区别在于 TCP 协议对所接收的 IP 数据包通过差错校验、确认重传及流量控制等控制机制实现端系统之间可靠的数据传输；而 UDP 协议并不能为端系统提供这种可靠的数据传输服务，其唯一的功能就是在接收端将从网络中接收到的数据交付到不同的网络应用中，提供一种最基本的服务。

（4）应用层协议

应用层协议提供不同的服务，常见的有以下几个。

① DNS 协议。

DNS（Domain Name System，域名系统）协议运行在通信的端系统之间，通常使用 UDP 协议，通过端口 53 进行传输。DNS 协议的出现解决了直接记忆和输入复杂 IP 地址的问题，使得互联网的使用变得更加便捷。DNS 协议的基本功能是将人类可读的域名（如 www.example.com）转换为机器可理解的 IP 地址。除基本功能外，DNS 协议还提供主机别名、邮件服务器别名及负载分配等重要服务。

② SMTP 协议与 POP3 协议。

SMTP 协议（Simple Mail Transfer Protocal，简单邮件传输协议）是一种应用层协议，用于在互联网中高效、可靠地传输电子邮件。它通常工作在 TCP/IP 协议栈之上，通过端口 25 进行通信。SMTP 协议的目标是向用户提供高效、可靠的邮件传输服务，能够在不同网络之间接力传送邮件。

POP3 协议（Post Office Protocol Version 3，邮局协议版本 3）是一种广泛使用的电子邮件接收协议，它允许电子邮件客户端通过网络从远端服务器接收邮件。POP3 协议的工作原理主要包括连接建立与身份验证、电子邮件操作命令和会话结束与邮件删除。电子邮件客户端通过 TCP 协议连接到邮件服务器的 POP3 端口（默认为 110 端口，或者使用 SSL 加密的 995 端口）。连接建立后，客户端首先发送 USER 命令提供用户名，然后发送 PASS 命令提供密码以进行身份验证。

③ HTTP 协议。

HTTP 协议（Hypertext Transfer Protocol，超文本传输协议）是一种应用层协议，用于分布式、协作式和超媒体信息系统。HTTP 协议是基于 TCP/IP 协议之上的应用层协议，通常使用端口 80。HTTPS 协议是 HTTP 协议的安全版本，通过加入 SSL/TLS 协议提供数据加密、完整性校验和身份验证，通常使用端口 443。

④ Telnet 协议。

Telnet 协议是一种用于远程登录的 TCP/IP 协议，允许用户通过网络在本地计算机上操作远程主机，实现各种管理任务。Telnet 协议的基本概念包括网络虚拟终端（Network Virtual

Terminal，NVT），它是一种双向的虚拟设备，连接的双方都必须把它们各自的物理终端与NVT 进行相互转换。这种转换使得 Telnet 协议可以在任何主机或终端之间工作，而屏蔽具体的终端类型。

⑤ FTP 协议。

FTP 协议（File Transfer Protocol，文件传输协议）是一种在网络中进行文件传输的广泛应用的标准协议，它允许用户通过客户端软件与服务器交互，实现文件的上传、下载和其他文件操作。FTP 协议是基于客户-服务器模型设计的，使用 TCP 协议作为其传输协议，确保数据传输的可靠性和顺序性。它工作在 OSI 模型的应用层，通常使用 TCP 协议的 21 端口作为控制连接的默认端口。

2．IPv4 地址

Internet 中的主机之间要正确地传送信息，每个主机就必须有唯一的区分标志。IP 地址就是给每个连接在 Internet 上的主机分配的一个区分标志。按照 IPv4（Internet Protocol Version 4，Internet 协议版本 4）规定，每个 IP 地址用 32 位二进制数来表示。

（1）IP 地址

32 位的 IP 地址由网络号和主机号组成。IP 地址中网络号的位数、主机号的位数取决于 IP 地址的类别。为了便于书写，经常用点分十进制数表示 IP 地址，即每 8 位写成一个十进制数，中间用“.”作为分隔符，如 11001010 01110101 01100010 00001010 可以写成 202.117.98.10。

IP 地址分为 A、B、C、D、E 共 5 类，如图 3.14 所示。

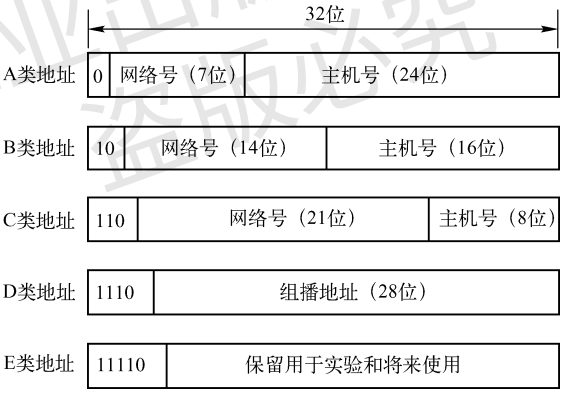


图 3.14　IP 地址的构成及类别

① A 类 IP 地址。

一个 A 类 IP 地址以 0 开头，后面跟 7 位网络号，最后是 24 位主机号。如果用点分十进制数表示，A 类 IP 地址就由 1 字节的网络地址和 3 字节主机地址组成。A 类网络地址适用于大规模网络，全世界 A 类网只有 126 个（全 0、全 1 不分），每个网络所能容纳的计算机数为 16 777 214 台（2^{24}–2 台，全 0、全 1 不分）。

② B 类 IP 地址。

一个 B 类 IP 地址以 10 开头，后面跟 14 位网络号，最后是 16 位主机号。如果用点分十进制数表示，B 类 IP 地址就由 2 字节的网络地址和 2 字节主机地址组成的。B 类网络地址适用于中规模的网络，每个网络所能容纳的计算机数为 65 534 台（2^{16}–2 台，全 0、全 1 不分）。

③ C 类 IP 地址。

一个 C 类 IP 地址以 110 开头，后面跟 21 位网络号，最后是 8 位主机号。如果用点分十

进制数表示，C 类 IP 地址就由 3 字节的网络地址和 1 字节主机地址组成的。C 类网络地址数量较多，适用于小规模的局域网络，每个网络最多只能包含 254 台计算机（2^8–2 台，全 0、全 1 不分）。

④ D 类 IP 地址。

D 类 IP 地址以 1110 开始，它是一个专门保留的地址。它并不指向特定的网络，目前这一类地址被用在多点广播中。多点广播地址用来一次寻址一组计算机，它标志共享同一协议的一组计算机。

⑤ E 类 IP 地址。

E 类 IP 地址以 11110 开始，保留用于实验和将来使用。

（2）子网掩码

子网掩码又叫网络掩码，子网掩码不能单独存在，它必须结合 IP 地址一起使用。子网掩码只有一个作用，就是表明一个 IP 地址中哪些位是网络号，哪些位是主机号。子网掩码的长度是 32 位，左边是网络位，用二进制数 1 表示，1 的数目等于网络位的长度；右边是主机位，用二进制数 0 表示，0 的数目等于主机位的长度。A 类地址的默认子网掩码为 255.0.0.0；B 类地址的默认子网掩码为 255.255.0.0；C 类地址的默认子网掩码为 255.255.255.0。

例如，某公司申请到一个 B 类网的 IP 地址分发权，网络号为 10001010 00001010，意味着该网拥有的主机数为 2^{16}–2=65 534 台，其主机号可以从 00000000 00000001 编到 11111111 11111110，这些主机都使用同一个网络号，这样的网络难以管理。Internet 采用将一个网络划分成若干子网的技术解决这个问题，基本思想是把具有这个网络号的 IP 地址划分成若干个子网，每个子网具有相同的网络号和不同的子网号。例如，可以将 65 534 个主机号按前 8 位是否相同分成 256 个子网，则每个子网中含有 254 个主机号。假定现在从子网号为 10100000 的子网中获得了一个主机号 00001010，则对应的 IP 地址为 10001010 00001010 10100000 00001010，用点分十进制数表示为 138.10.160.10，如果将该 IP 地址传给 IP 协议，IP 协议按默认方式理解，将认为该 IP 地址的主机号为 16 位，和实际不符，这时就需要告诉 IP 协议划分了子网，需要设置子网掩码 255.255.255.0。

例如，有一 IP 地址为 202.158.96.238，对应的子网掩码为 255.255.255.240。由子网掩码可知，网络号为 28 位，是 202.158.96.224；主机号为 4 位，是 14。

（3）特殊的 IP 地址

在总数约为 40 多亿个可用 IP 地址中，还有一些常见的有特殊意义的地址。

① 0.0.0.0 表示这样一个集合：所有不清楚的主机和目的网络。这里的“不清楚”是指在本机的路由表里没有特定条目指明如何到达。如果在网络设置中设置了默认网关，那么 Windows 系统会自动产生一个目的地址为 0.0.0.0 的默认路由。

② 255.255.255.255 是限制广播地址。对本机来说，这个地址指本网段内的所有主机。这个地址不能被路由器转发。

③ 127.0.0.1 是本机地址，主要用于测试。在 Windows 系统中，这个地址有一个别名是“Localhost”。

④ 224.0.0.1 是组播地址，从 224.0.0.0 到 239.255.255.255 都是这样的地址。224.0.0.1 特指所有主机，224.0.0.2 特指所有路由器。这样的地址多用于一些特定的程序及多媒体程序。如果主机开启了 IRDP（Internet 路由发现协议，使用组播功能）功能，那么主机路由表中应该有这样一条路由。

⑤ 10.x.x.x、172.16.x.x～172.31.x.x、192.168.x.x 是私有地址，这些地址被大量用于企业

内部网络中。一些宽带路由器经常使用 192.168.1.1 作为默认地址。使用私有地址的私有网络在接入 Internet 时，要使用地址翻译将私有地址翻译成公用合法地址。在 Internet 上，这类地址是不能出现的。

（4）IP 地址的申请与分配

所有的 IP 地址都由国际组织 NIC（Network Information Center，网络信息中心）负责统一分配，目前全世界共有三个这样的网络信息中心。ENIC 负责欧洲地区，APNIC 负责亚太地区，InterNIC 负责美国及其他地区。我国申请 IP 地址要经过 APNIC，APNIC 的总部设在澳大利亚布里斯班。申请时要先考虑申请哪一类 IP 地址，然后向国内的代理机构提出申请。

3．IPv6 地址

IPv6（Internet Protocol Version 6，Internet 协议版本 6）是一种互联网协议，是 IPv4 的升级版本，旨在解决网络地址耗尽的问题并提供更加安全、高效的网络通信能力。图 3.15 显示了某个手机的 IP 地址。

图 3.15　某个手机的 IP 地址

IPv6 是网络层协议的第二代标准协议，也称为 IPng。它解决了 IPv4 存在的诸多问题，其显著特点之一是将 IP 地址长度从 32 位增加到 128 位，极大地扩展了网络地址空间。这种扩展意味着在理论上可以有 2^{128} 个唯一地址，为未来可能接入互联网的设备提供了足够的标识空间。

（1）IPv6 在中国的现状

IPv6 在中国的整体发展势头强劲，用户数量和流量规模显著提升，正处于从网络基础设施到应用服务的全面升级阶段。

① 用户规模方面。

中国的 IPv6 活跃用户已达到 7.94 亿个，占全体网民的 72.7%。该数字从 2017 年初的 0.51%提高至如今的超过七成，显示出中国在推动 IPv6 用户规模方面的显著成效。

② 流量规模方面。

2024 年 7 月，第三届中国 IPv6 创新发展大会现场发布的《中国 IPv6 发展状况白皮书（2024）》（下称《白皮书》）显示，我国 IPv6 活跃用户达到 7.94 亿个，在全体网民总数中的比例由 2017 年初的 0.51%提高至 72.70%。IPv6 用户数是反映我国 IPv6 发展状况的核心指标，包括 IPv6 活跃用户数和已分配 IPv6 地址用户数。《白皮书》显示，2024 年 5 月，我国已分配 IPv6 地址终端数达到 17.65 亿个，其中移动网络已分配 IPv6 地址的终端为 13.50 亿个，固定宽带接入网络已分配 IPv6 地址的终端数为 4.15 亿个。

《白皮书》显示，截至 2024 年 5 月，我国城域网 IPv6 总流量占全网总流量的 21.21%。中国电信、中国移动、中国联通和教育网城域网 IPv6 流量分别占其全部流量的 20.33%、22.69%、20.75%和 36.51%。我国移动网 IPv6 总流量占全网移动网总流量的 64.56%。中国电信、中国移动和中国联通移动网 IPv6 的流量分别占其全网流量的 63.66%、65.50%和 63.11%。

③ 基础网络改造。

中国的 4G、5G 和固定宽带网络 IPv6 升级改造已全面完成。主要数据中心、CDN、云服务企业初步具备覆盖全国范围的 IPv6 服务能力。

④ 终端设备改造。

自 2018 年起，市场份额较大的移动终端厂商新发布的机型和系统均具备 IPv6 支持能力。三家基础电信企业已完成全部具备条件的存量家庭网关 IPv6 升级改造，并正在加快老旧家庭网关替换。

（2）IPv6 的地址表示方法

IPv6 地址是用于标识在互联网中设备接口的唯一编号，采用 128 位二进制数表示，以增强网络的扩展性和解决 IPv4 地址耗尽的问题。

① 基本表示。

IPv6 地址由 128 位二进制数构成，为了方便理解与使用，通常显示为 32 位十六进制字符串，并分为 8 组，每组由 4 个十六进制数组成，组间用冒号分隔。

② 前导零省略。

为了简化地址的书写，可以省略每组中的前导零，例如将“00A1”写作“A1”。

③ 连续零压缩。

在一个 IPv6 地址中，可以用双冒号“::”替代连续的零组，但这种压缩在地址中只能使用一次，以避免歧义。例如，“0000:0000:0000:0000:0000:0000:1234:5678”可以写作“::1234:5678”。

IPv6 地址作为网络技术的重要组成部分，不仅解决了 IPv4 地址资源有限的问题，还带来自动配置、安全性提升等许多新特性和优势。

4．域名系统

通过 TCP/IP 协议进行数据通信的主机或网络设备都要拥有一个 IP 地址，但 IP 地址不便于记忆。为了便于使用，常常赋予某些主机（特别是提供服务的服务器）能够体现其特征和含义的名称，即主机的域名。

（1）域名层次结构

域名系统（Domain Name System，DNS）提供一种分布式的层次结构，位于顶层的域名称为顶级域名，顶级域名有两种划分方法：按地理区域划分和按组织结构划分。域名层次结构如图 3.16 所示。

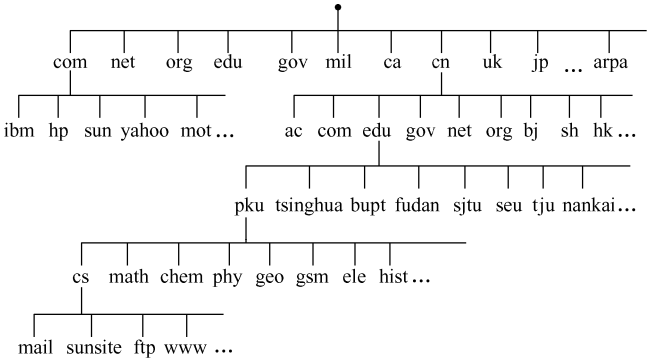


图 3.16　域名层次结构

地理区域是为国家或地区设置的，如中国是 cn，美国是 us，日本是 jp 等。机构类域定义了不同的机构分类，主要包括 com（商业组织）、edu（教育机构）、gov（政府机构）、ac

（学术机构）等。顶级域名下又定义了二级域名，如中国的顶级域名 cn 下又设立了 com、net、org、edu、gov 等组织结构类二级域名，以及按照各个行政区域划分的地理域名，如 bj（北京）、sh（上海）等。采用同样的思想可以继续定义三级或四级域名。域名的层次结构可以看成一个树状结构，在一个完整的域名中，由树叶到树根的路径点用“.”分割，如 www.nwu.edu.cn 就是一个完整的域名。

（2）域名解析

传送网络数据时需要用 IP 地址进行路由选择，域名无法识别，因此必须有一种翻译机制，能将用户要访问的服务器的域名翻译成对应的 IP 地址。为此 Internet 提供了域名系统（DNS），DNS 的主要任务是为客户提供域名解析服务。

域名服务系统将整个 Internet 的域名分成许多可以独立管理的子域，每个子域由自己的域名服务器负责管理。这就意味着域名服务器维护其管辖子域的所有主机域名与 IP 地址的映射信息，并且负责向整个 Internet 用户提供包含在该子域中的域名解析服务。基于这种思想，Internet DNS 有许多分布在全世界不同地理区域、由不同管理机构负责管理的域名服务器。全球共有十几台根域名服务器，其中大部分位于北美洲，这些根域名服务器的 IP 地址向所有 Internet 用户公开，是实现整个域名解析服务的基础。

例如，在如图 3.17 所示的 DNS 服务器的分层中，管辖所有顶级域名 com、edu、gov、cn、uk 等的域名服务器也称为顶级域名服务器；顶层域名服务器下面还可以连接多层域名服务器，如顶级 cn 域名服务器又可以提供在它的分支下面的“com.cn”“edu.cn”等域名服务器的地址。同样，在 com 顶级域名服务器下的“yahoo.com”域名服务器，也可以作为该公司的域名服务器，提供其公司内部的不同部门所使用的域名服务器。

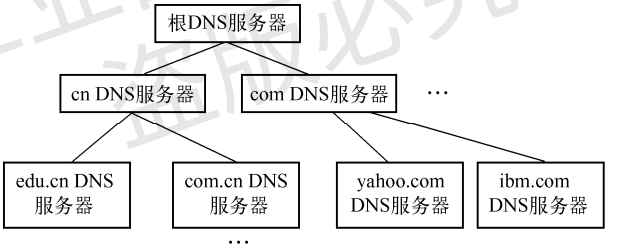


图 3.17　DNS 服务器的分层

域名解析的过程如图 3.18 所示，当客户以域名方式提出 Web 服务请求后，首先要向 DNS 请求域名解析服务，只有在得到所请求的 Web 服务器的 IP 地址之后，才能向该 Web 服务器提出 Web 请求。

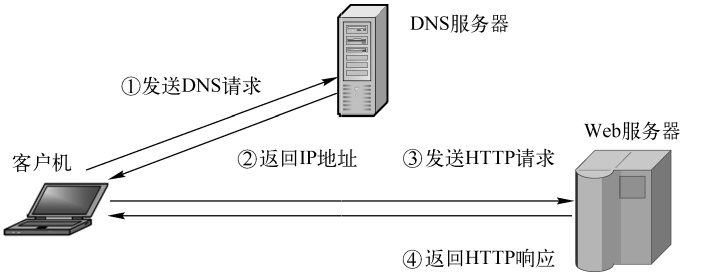


图 3.18　域名解析的过程

（3）域名的授权机制

顶级域名由 Internet 名字与编号分配机构直接管理和控制，负责注册和审批新的顶级域

名及委托并授权其下一级管理机构控制与管理顶级以下的域名。该组织还负责根和顶级域名服务器的日常维护工作。中国互联网信息中心（China Internet Network Information Center，CNNIC）作为中国的国家顶级域名 cn 的注册管理机构，负责 cn 域名根服务器和顶级服务器的日常维护和运行，以及管理并审批 cn 域下的域名使用权。Internet 始于美国，DNS 服务系统最早在美国国内开始向公共网络用户服务，当然也是美国的组织结构最早向互联网名称与数字地址分配机构 ICANN（The Internet Corporation for Assigned Names and Numbers）申请域名注册的，当 ICANN 意识到需要使用地域标记来扩展越来越多的域名需求时，许多美国的机构已经注册并使用了这些不需要地域标记的域名，因此，大部分美国的企业和组织所使用的域名并不需要加上代表美国的地域标记“us”。

（4）雪人计划

雪人计划（Yeti DNS Project）是一个基于全新技术架构的全球下一代互联网（IPv6）根服务器测试和运营实验项目，旨在打破现有的根服务器困局，为下一代互联网提供更多的根服务器解决方案。该项目由中国发起，并在全球范围内完成了 25 台 IPv6 根服务器的架设，其中中国部署了 4 台，包括 1 台主根服务器和 3 台辅根服务器。这一成就不仅打破了中国过去没有根服务器的困境，而且为建立多边、民主、透明的国际互联网治理体系打下了坚实基础。

雪人计划的成功不仅体现在技术架构的创新和全球范围内的部署上，还在于其对国际互联网治理体系的影响。通过增加根服务器的数量和分布，雪人计划有助于提升全球互联网的稳定性和安全性，减少对单一国家的依赖，从而促进互联网的公平和透明治理。此外，该项目还提升了中国在全球互联网治理中的话语权，有助于中国在国际互联网事务中发挥更加积极的作用。

尽管雪人计划的实施过程中可能面临技术同步和数据管理的挑战，但通过国际合作和共同努力，该项目已经取得了显著的进展，为中国及全球互联网的未来发展奠定了坚实的基础。

3.3.2 Internet 基本服务

Internet 采用客户机/服务器（Client /Server）模式，其工作过程如图 3.19 所示。通常情况下，一个客户机启动与某个服务器的对话。服务器通常是等待客户机请求的一个自动程序。客户机通常是作为某个用户请求或类似于用户的某个程序提出的请求而运行的。协议是客户机请求服务器和服务器如何应答请求的各种方法的定义。

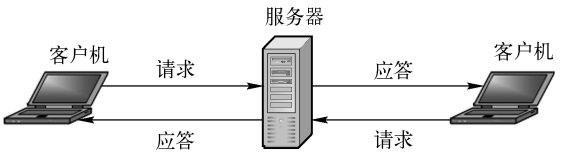


图 3.19　客户机/服务器模式

1．WWW 服务

WWW（World Wide Web，万维网）是一个以 Internet 为基础的庞大的信息网络，它将 Internet 上提供各种信息资源的万维网服务器（也称 Web 服务器）连接起来，使得所有连接在 Internet 上的计算机用户能够方便、快捷地访问自己喜好的内容。Web 服务的组成部分包括：提供 Web 信息服务的 Web 服务器、从 Web 服务器获取各种 Web 信息的浏览器、定义服务器和浏览器之间交换数据信息规范的 HTTP 协议及 Web 服务器所提供的网页文件。

（1）Web 服务器与浏览器

服务器指一个管理资源并为用户提供服务的程序，通常分为文件服务器、数据库服务器

和应用程序服务器等。运行以上程序的计算机或计算机系统也被称为服务器，相对于普通 PC 来说，服务器（计算机系统）在稳定性、安全性、性能等方面的要求更高。因此，其 CPU、芯片组、内存、磁盘系统、网络等硬件和普通 PC 有所不同。

这里所说的 Web 服务器是一个程序，运行在服务器计算机中，主要任务是管理和存储各种信息资源，并负责接收来自不同客户机端（简称客户端）的服务请求。针对客户端所提出各种信息服务请求，Web 服务器通过相应的处理返回信息，使得客户端通过浏览器能够看到相应的结果。

Web 客户端可以通过各种 Web 浏览器程序实现，浏览器是可以显示 Web 服务器或文件系统的 HTML（HyperText Markup Language，超文本标记语言）文件内容，并让用户与这些文件交互。浏览器的主要任务是接收用户计算机的 Web 请求，并将这个请求发送给相应的 Web 服务器，当接收到 Web 服务器返回的 Web 信息时，负责显示这些信息。大部分浏览器本身除支持 HTML 外，还支持 JPEG、PNG、GIF 等图像格式，并且能够扩展支持众多的插件。常用的 Web 浏览器有 Microsoft Internet Explorer、Netscape Navigator 和 Firefox 等。

（2）URL

浏览器中的服务请求通过在浏览器的地址栏定位一个 URL（Uniform Resource Locator，统一资源定位符）链接提出。URL 是用于完整地描述 Internet 上网页和其他资源的地址的一种标志方法。Internet 上的每个网页都具有一个唯一的名称标志，通常称为 URL 地址，简单地说，URL 就是 Web 地址，俗称网址。

URL 由三部分组成：协议类型、主机名和路径及文件名。其基本格式如下：

```
协议类型://主机名/路径及文件名
```

例如：http://www.n**.edu.cn/index.html。

协议指所使用的传输协议，最常用的是 HTTP 协议，它也是目前 WWW 中应用最广的协议，还可以指定的协议有 FTP、Gopher、Telnet、File 等。

主机名是指存放资源的服务器的域名或 IP 地址。有时，在主机名前可以包含连接到服务器所需的用户名和密码。

路径是由零个或多个“/”符号隔开的字符串，用来表示主机上的一个目录或文件地址。文件名则是所要访问的资源的名字。

（3）超文本传输协议（HTTP）

万维网的另一个重要组成部分是 HTTP 协议，它定义了 Web 服务器和浏览器之间信息交换的格式规范。运行在不同操作系统上的客户浏览器程序和 Web 服务器程序通过 HTTP 协议实现彼此之间的信息交流和理解。HTTP 协议是一种非常简单而直观的网络应用协议，主要定义了两种报文格式：一种是 HTTP 请求报文，定义了浏览器向 Web 服务器请求 Web 服务时所使用的报文格式；另一种是 HTTP 响应报文，定义了 Web 服务器将相应的信息文件返回给用户浏览器所使用的报文格式。

（4）Web 网页

网页是构成网站的基本元素，是承载各种网站应用的平台。Web 网页采用 HTML 格式书写，由多个对象，如 HTML 文件、JPG 图像、GIF 图像、Java 程序、语音片段等构成。不同网页之间通过超链接发生联系。网页有多种分类，通常可分为静态网页和动态网页。静态网页的文件扩展名多为.htm 或.html，动态网页的文件扩展名多为.php 或.asp。

静态网页由标准的 HTML 构成，不需要通过服务器或用户浏览器运算或处理生成。这就意味着用户对一个静态网页发出访问请求后，服务器只是简单地将该文件传输到客户端。所

以，静态网页多通过网站设计软件来进行设计和更改，相对比较滞后。动态网页是在用户请求 Web 服务的同时由两种方式及时产生：一种方式是由 Web 服务器解读来自用户的 Web 服务请求，并通过运行相应的处理程序，生成相应的 HTML 响应文档，并返回给用户；另一种方式是服务器将生成动态 HTML 网页的任务留给用户浏览器，在响应给用户的 HTML 文档中嵌入应用程序，由用户端浏览器解释并运行这部分程序以生成相应的动态网页。

静态网页是网站建设的基础，静态网页和动态网页之间并不矛盾，各有特点。网站是采用动态网页还是静态网页主要取决于网站的功能需求和网站内容的多少。如果网站功能比较简单，内容更新量不是很大，则采用纯静态网页的方式会更简单，反之则要采用动态网页技术来实现。在同一个网站上，动态网页内容和静态网页内容同时存在也是很常见的事情。

2．电子邮件服务

电子邮件（E-mail）也是 Internet 最常用的服务之一，利用 E-mail 可以传输各种格式的文本信息及图像、声音、视频等多种信息。

（1）E-mail 系统的构成

E-mail 服务采用客户机/服务器的工作模式，一个 E-mail 系统包含三部分：用户主机、邮件服务器和电子邮件协议。

用户主机运行用户代理 UA，通过它来撰写信件、处理来信（使用 SMTP 协议将用户的邮件传送到它的邮件服务器，用 POP 协议从邮件服务器读取邮件到用户的主机）、显示来信。

邮件服务器运行传送代理 MTA，邮件服务器设有邮件缓存和用户邮箱。其主要作用：一是接收本地用户发送的邮件，并存于邮件缓存中待发，由 MTA 定期扫描发送；二是接收发给本地用户的邮件，并将邮件存放在收信人的邮箱中。

（2）电子邮箱地址

很多站点提供免费的电子邮箱，只要能访问这些站点的免费电子邮箱服务网页，用户就可以免费建立并使用自己的电子邮箱。每个电子邮箱都有唯一的地址，电子邮箱的地址格式如下：收信人用户名@电子邮箱所在的主机域名。

例如，zhang8808@126.com 表示用户 zhang8808 在主机名为“126.com”的电子邮件服务器上申请了电子邮箱。

（3）电子邮件的收发

发送与接收电子邮件有两种方式：基于 Web 方式的电子邮件访问协议和客户端软件方式。基于 Web 方式的电子邮件访问协议（如 126）：用户使用超文本传输协议 HTTP 访问电子邮件服务器的电子邮箱，在该电子邮件系统网址上输入用户的用户名和密码，进入用户的电子邮箱，然后处理用户的电子邮件。这种方式使用方便，但速度比较慢。客户端软件方：用户通过一些安装在个人计算机上的支持电子邮件基本协议的软件使用和管理电子邮件。这些软件（如 Microsoft Outlook 和 Foxmail）往往融合了先进、全面的电子邮件功能，利用这些客户端软件可以进行远程电子邮件操作，还可以同时处理多个账号的电子邮件，而且速度比较快。

电子邮件的收发过程如图 3.20 所示。

① 发送方调用 UA 撰写电子邮件，并通过 SMTP 协议将客户的电子邮件交付发送电子邮件服务器，发送电子邮件服务器将其用户的电子邮件存储于电子邮件缓存，等待发送。

② 发送电子邮件服务器每隔一段时间对电子邮件缓存进行扫描，如果发现有待发电子邮件就通过 SMTP 协议发向接收电子邮件服务器。

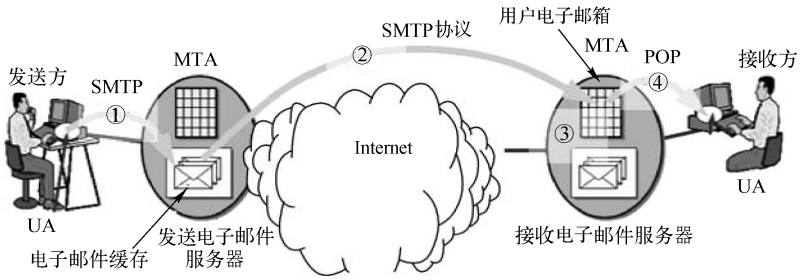


图 3.20　电子邮件的收发过程

③ 接收电子邮件服务器接收到电子邮件后，将它们放入收信人的电子邮箱中，等待收信被随时读取。

④ 接收方通过 POP 协议从接收电子邮件服务器上检索电子邮件，下载电子邮件后可以阅读、处理电子邮件。

3．文件传输服务

（1）FTP 工作模式

与大多数 Internet 服务一样，FTP 也是一个客户机/服务器系统。用户通过一个支持 FTP 协议的客户机程序连接到远程主机上的 FTP 服务器程序。用户通过客户机程序向服务器程序发出命令，服务器程序执行用户所发出的命令，并将执行的结果返回客户机。FTP 主要用于下载共享软件。在 FTP 的使用中，用户经常遇到两个概念：下载（Download）和上传（Upload）。下载文件就是从远程主机复制文件至自己的计算机上；上传文件就是将文件从自己的计算机中复制至远程主机上。

用户在访问 FTP 服务器之前必须先登录，登录时需要用户给出其在 FTP 服务器上的合法账号和口令。但很多用户没有获得合法账号和口令，这就限制了共享资源的使用。所以，许多 FTP 服务器支持匿名 FTP 服务，匿名 FTP 服务不再验证用户的合法性，为了安全，大多数匿名 FTP 服务器只准下载、不准上传。

（2）FTP 客户程序

需要进行远程文件传输的计算机必须安装和运行 FTP 客户程序。常见的 FTP 客户程序有三种类型：FTP 命令行、浏览器和下载软件。

① FTP 命令行

在安装 Windows 操作系统时，通常都安装了 TCP/IP 协议，其中就包含了 FTP 命令。但是，该程序是字符界面而不是图形界面，必须以命令提示符的方式进行操作。FTP 命令是 Internet 用户使用最频繁的命令之一，无论是在 DOS 还是在 UNIX 操作系统下使用 FTP 都会遇到大量的 FTP 内部命令。熟悉并灵活应用 FTP 内部命令，可以收到事半功倍之效。但其命令众多，格式复杂，对于普通用户来说，比较难掌握。所以，一般用户在下载文件时常通过浏览器或专门的下载软件来实现。

② 浏览器

启动 FTP 客户程序的另一途径是使用浏览器，用户只需在地址栏中输入如下格式的 URL 地址：

```
FTP:// [用户名:口令@]ftp 服务器域名:[端口号]
```

即可登录对应的 FTP 服务器。同样，在命令行下也可以用上述方法连接，通过 put 命令和 get 命令达到上传和下载的目的，通过 ls 命令列出目录。除上述方法外，还可以在命令行下输入 ftp 并回车，然后输入 open 来建立一个连接。

尽管可以使用通过浏览器启动 FTP 的方法，但是速度较慢，还会因将密码暴露在浏览器中而不安全。

③ 下载软件

为了实现高效文件传输，用户可以使用专门的文件传输程序，这些程序不但简单易用，而且支持断点续传。所谓断点续传，是指在下载或上传时，将下载或上传任务（一个文件或一个压缩包）划分为几个部分，每个部分采用一个线程进行上传或下载，如果碰到网络故障而终止，等到故障消除后可以继续上传或下载余下的部分，而没有必要从头开始，可以节省时间，提高速度。迅雷、快车、BitComet、优酷、百度视频、新浪视频、腾讯视频等都支持断点续传。

4．远程登录服务

远程登录是指用户使用 Telnet 命令，使自己的计算机暂时成为远程主机的一个仿真终端的过程。仿真终端只负责把用户输入的每个字符传递给远程主机，远程主机进行处理后，再将结果传回并显示在屏幕上。Telnet 是进行远程登录的标准协议和主要方式，它为用户提供了在本地计算机上完成远程主机工作的能力。

使用 Telnet 进行远程登录时需要满足以下条件：在本地计算机上必须装有包含 Telnet 协议的客户程序，必须知道远程主机的 IP 地址或域名，必须有合法的用户名和口令。

Telnet 远程登录服务分为以下 4 个阶段。

① 本地计算机和远程主机建立连接，该过程实际上是建立一个 TCP 连接。

② 将本地终端上输入的用户名和口令及以后输入的任何命令或字符以网络虚拟终端（NVT）格式传送到远程主机。

③ 将传回的 NVT 格式的数据转化为本地所接受的格式送回本地终端，包括输入命令回显和命令执行结果。

④ 最后，本地终端对远程主机撤销连接，该过程实际上是撤销一个 TCP 连接。

3.4 网络安全

网络安全涉及计算机科学技术、网络技术、通信技术、密码技术、信息安全技术等多个学科。从本质上讲，网络安全就是网络上的信息安全。

3.4.1 网络安全的概念与特征

随着计算机技术的迅速发展，系统的连接能力也在不断提高。与此同时，基于网络连接的安全问题也日益突出。

1．网络安全的概念

网络安全是指网络系统的硬件、软件及系统中的数据受到保护，不会出于偶然或恶意的原因而遭受到破坏、更改、泄露，系统可连续、可靠、正常地运行，网络服务不中断。从广义来说，凡是涉及网络上信息的保密性、完整性、可用性、可控性等的相关技术和理论都是网络安全的研究领域。

2．基本特征

网络安全的基本特征包括保密性、完整性、可用性、可控性和不可抵赖性。这些特征共同构成了网络安全的基础性要求，并在不同的层面上保护网络系统免受各种威胁和攻击。

（1）保密性

保密性是指信息不被未授权的用户、实体或进程获取或利用。在网络系统中，保密性要

求数据在存储和传输过程中保持加密状态，仅对有权限的用户透露内容。这种特性不仅适用于国家机密，还包括企业和社会团体的商业机密及个人信息。

（2）完整性

完整性是指信息在未经授权的情况下不被修改，确保信息在存储或传输过程中保持不被篡改、破坏或丢失。完整性要求维护数据的真实性和准确性，防止恶意篡改和意外更改，从而确保信息的可靠性和有效性。

（3）可用性

可用性要求信息和资源对授权用户始终保持可访问状态。这意味着在需要时，合法用户能够及时获得所需的信息和服务，不受拒绝服务（DoS）或其他形式攻击的影响。保证信息系统的高可用性是网络安全的重要目标之一。

（4）可控性

可控性是对信息的传播路径、范围及其内容进行有效控制的能力。这包括限制不良内容的传播，确保信息在合法用户的掌控之中，从而维护网络环境的秩序和安全。

（5）不可抵赖性

不可抵赖性也称为不可否认性，是指在信息交换过程中，所有参与者都不能否认已经完成的操作和承诺。通过数字签名和认证机制，不可抵赖性确保通信双方无法否认之前发生的行为，从而提高交易的安全性和可信度。

3.4.2 基本网络安全技术

网络安全技术致力于解决如何有效进行介入控制，以及如何保证数据传输的安全性，主要包括数据加密技术、认证技术、数字签名技术等。

1. 数据加密技术

数据加密是指对原始信息进行重新编码，将原始信息称为明文，经过加密的数据称为密文。密文即便在传输中被第三方获取，第三方也很难从得到的密文中破译出原始信息，接收端通过解密得到原始信息。加密技术不仅能保障数据信息在公共网络传输过程中的安全性，同时也是实现用户身份鉴别和数据完整性保障等安全机制的基础。

加密技术包括两个元素：算法和密钥。算法是将普通文本（或可以理解的信息）与一串数字（密钥）运算，产生不可理解的密文的步骤。在安全保密中，可通过适当的密钥加密技术和管理机制来保证网络的信息通信安全。加密技术的基本原理如图 3.21 所示。

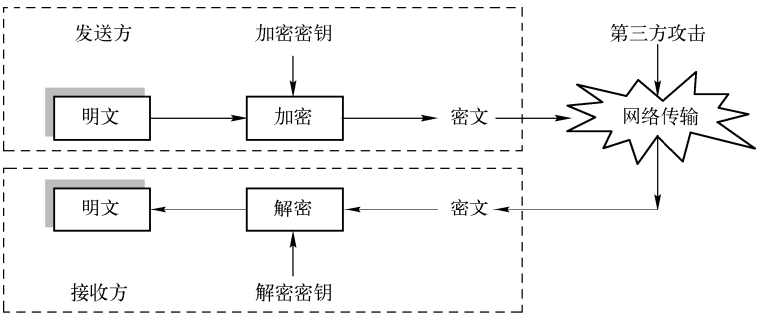


图 3.21　加密技术的基本原理

根据加密和解密的密钥是否相同，加密算法可分为对称密码和非对称密码。

（1）对称加密

对称加密采用对称密码编码技术，它的特点是文件加密和解密使用相同的密钥。除数据

加密标准（Data Encryption Standard，DES）外，另一个常见的对称密钥加密系统是国际数据加密算法（International Data Encryption Algorithm，IDEA），它比 DES 的加密性好，而且对计算机功能要求也不高。IDEA 由 PGP（Pretty Good Privacy，优良保密协议）系统使用。对称加密又称常规加密，其基本原理如图 3.22 所示。

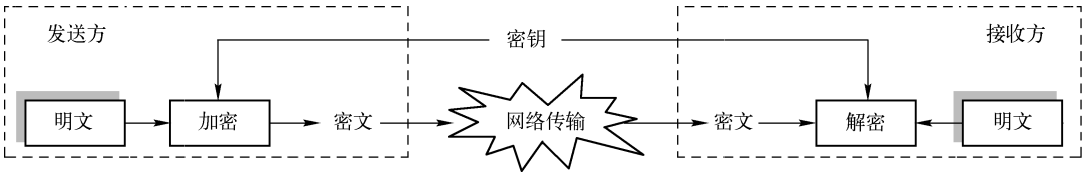


图 3.22　对称加密的基本原理

① 明文：作为算法输入的原始信息。

② 加密算法：加密算法可以对明文进行多种置换和转换。

③ 共享的密钥：共享的密钥也是算法的输入。算法实际进行的置换和转换由密钥决定。

④ 密文：作为输出的混合信息，由明文和密钥决定；对于给定的信息来讲，两种不同的密钥会产生两种不同的密文。

⑤ 解密算法：是加密算法的逆向算法。它以密文和同样的密钥作为输入，并生成原始明文。

对称加密的速度快，适合于大量数据的加密传输。但是，对称加密必须首先解决对称密钥的发送问题，而且对加密有以下两个安全要求。

① 需要强大的加密算法。

② 发送方和接收方必须使用安全的方式来获得密钥副本，必须保证密钥的安全。如果有人发现了密钥，并知道了算法，则使用此密钥的所有通信便都是可读取的。

（2）非对称加密

与对称加密算法不同，非对称加密算法需要两个密钥：公钥和私钥。这两个密钥成对出现，互不可推导。如果用公钥对数据进行加密，则只有用对应的私钥才能解密。如果用私钥对数据进行加密，那么只有用对应的公钥才能解密。因为加密和解密使用的是两个不同的密钥，所以这种算法叫非对称加密算法。

非对称密码体制有两种模型：一种是加密模型，如图 3.23 所示；另一种是认证模型，如图 3.24 所示。

图 3.23　非对称密码体制的加密模型

图 3.24　非对称密码体制的认证模型

在加密模型中，发送方在发送数据时，用接收方的公钥加密（双方都知道公钥），而信

息在接收方只能用接收方的私钥解密，由于解密用的密钥只有接收方自己知道，从而保证了信息的机密性。

认证主要完成网络通信过程中通信双方的身份认可。通过认证模型可以验证发送方的身份、保证发送方不可否认。在认证模型中，发送方必须用自己的私钥加密，而解密方则必须用发送方的公钥解密，也就是说，任何一个人，只要能用发送方的公钥解密，就能证明信息是谁发送的。

2．认证技术

所谓认证，是指证实被认证对象是否属实和是否有效的一个过程。其基本思想是通过验证被认证对象的属性来确认被认证对象是否真实有效。认证常常被用于通信双方相互确认身份，以保证通信的安全。认证一般可以分为两种：消息认证和身份认证，消息认证用于保证信息的完整性；身份认证用于鉴别用户身份。

（1）消息认证

消息认证是指接收方能够验证收到的消息是否真实的方法。消息认证又称为完整性校验，它在银行业称为消息认证，在 OSI 安全模式中称为封装。消息认证的主要内容如下。

① 证实消息的信源和信宿。

② 消息内容是否受到偶然或有意的篡改。

③ 消息的序号和时间性是否正确。

消息认证实际上是对消息本身产生一个冗余的消息认证码，它对于要保护的信息来说是唯一的，因此可以有效地保护消息的完整性，以及实现发送方消息的不可抵赖和不能伪造。消息认证技术可以防止数据的伪造和被篡改，以及证实消息来源的有效性。消息认证的工作机制如图 3.25 所示。

其中，安全单向散列函数具有以下基本特性。

① 一致性：相同的输入一定产生相同的输出。

② 单向性：只能由明文产生消息摘要，而不能由消息摘要推出明文。

③ 唯一性：不同的明文产生的消息摘要不同。

④ 易于实现高速计算。

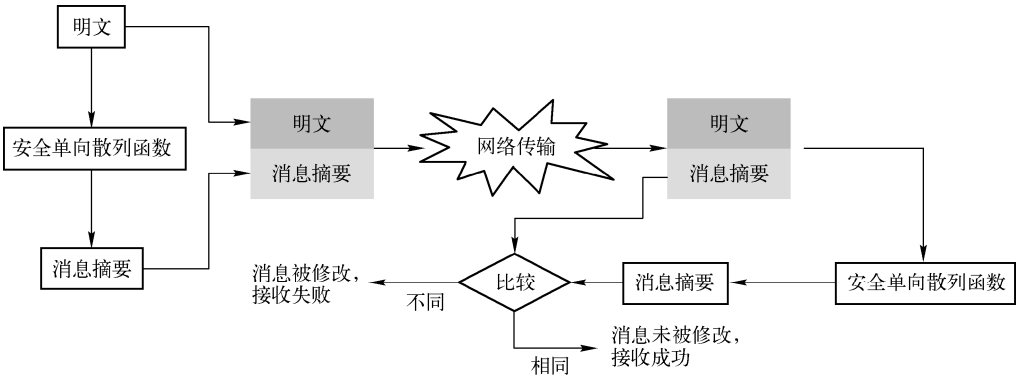


图 3.25　消息认证的工作机制

（2）身份认证

身份认证是指计算机及网络系统确认操作者身份的过程。身份认证技术的发展，经历了从软件认证到硬件认证、从静态认证到动态认证的过程。常见的身份认证技术包括以下几类。

① 口令认证。传统的认证技术主要采用基于口令的认证。当被认证对象要求访问提供

服务的系统时，认证方要求被认证对象提交口令，认证方收到口令后，将其与系统中存储的用户口令进行比较，以确认被认证对象是否为合法访问者。基于口令的认证实现简单，不需要额外的硬件设备，但易被猜测。

② 一次口令机制。一次口令机制采用动态口令技术，是一种让用户的密码按照时间或使用次数不断动态变化，且每个密码只使用一次的技术。它采用一种称为动态令牌的专用硬件来产生密码，因为只有合法用户才持有该硬件，所以只要密码验证通过就可以认为该用户的身份是可靠的。用户每次使用的密码都不相同，即使黑客截获了一次密码，也无法利用这个密码来仿冒。

③ 生物特征认证。生物特征认证是指采用每个人独一无二的生物特征来验证用户身份的技术，常见的有指纹识别、虹膜识别等。从理论上说，生物特征认证是最可靠的身份认证方式，因为它直接使用人的物理特征来表示每个人的数字身份。

3．数字签名技术

在网络通信中，希望能有效防止通信双方的欺骗和抵赖行为。简单的报文鉴别技术只能使通信免受来自第三方的攻击，但无法防止通信双方之间的互相攻击。例如，Y 伪造一个消息，声称是从 X 收到的；或者 X 向 Z 发了消息，但 X 否认发过该消息。为此，需要有一种新的技术来解决这种问题，数字签名技术为此提供了一种解决方案。

数字签名将消息发送者的身份与消息传送结合起来，可以保证消息在传输过程中的完整性，并提供消息发送者的身份认证，以防止消息发送者抵赖行为的发生。目前，利用非对称加密算法进行数字签名是最常用的方法。数字签名是对现实生活中笔迹签名的功能模拟，能够用来证实签名的作者和签名的时间。在对消息进行签名时，能够对消息的内容进行鉴别。同时，签名应具有法律效力，能被第三方证实，用以解决争端。

数字签名技术可分为两类：直接数字签名和基于仲裁的数字签名。其中，直接数字签名方案具有以下特点。

① 实现比较简单，在技术上仅涉及通信的源点 X 和终点 Y 双方。

② 终点 Y 需要了解源点 X 的公开密钥。

③ 源点 X 可以使用其私钥对整个消息进行加密来生成数字签名。

④ 更好的方法是，使用发送方私钥对消息的散列码进行加密来形成数字签名。

直接数字签名的基本过程是：数据源发送方通过散列函数对原文产生一个消息摘要，用自己的私钥对消息摘要进行加密处理，产生数字签名，数字签名与原文一起传送给接收方。发送方加密过程如图 3.26 所示。

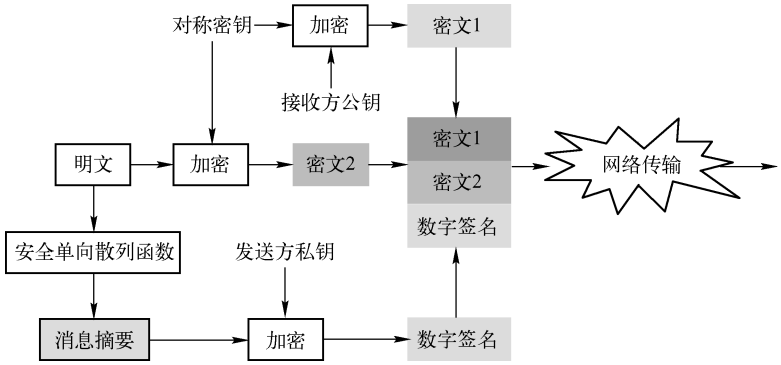


图 3.26　发送方加密过程

接收方使用发送方的公钥解密数字签名得到消息摘要，若能解密，则证明消息不是伪造的，实现了发送方认证。然后用散列函数对收到的原文产生一个消息摘要，与解密的消息摘要对比，如果相同，则说明收到的消息是完整的，在传输过程中没有被修改，否则说明消息被修改过，因此数字签名能够验证消息的完整性。接收方解密过程如图 3.27 所示。

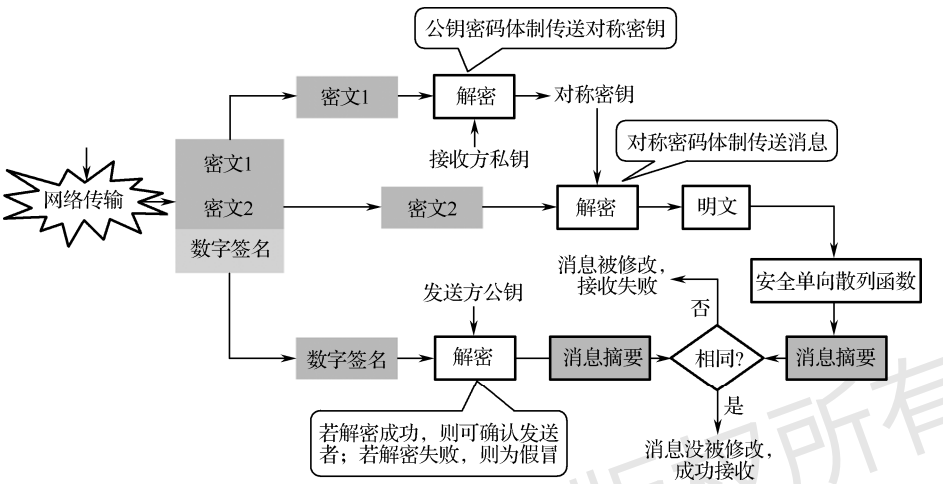


图 3.27　接收方解密过程

数字签名技术是网络中确认身份的重要技术，完全可以代替现实中的亲笔签字，在技术和法律上有保证。在数字签名应用中，发送方的公钥可以很方便地得到，但他的私钥则需要严格保密。利用数字签名技术可以实现数据的完整性，但由于文件内容太大，加密和解密速度慢，目前主要采用消息摘要技术，通过消息摘要技术可以将较大的报文生成较短的、长度固定的消息摘要，然后仅对消息摘要进行数字签名，而接收方对接收的报文进行处理产生消息摘要，与经过签名的消息摘要比较，便可以确定数据在传输中的完整性。

4．SSL 认证

SLL（Secure Socket Layer，安全套接层）由 Netscape 公司研发，用以保障在 Internet 上传输数据的安全，利用数据加密技术，确保数据在网络上传输过程中不会被截取及窃听。SSL 认证是指客户端到服务器端的认证，主要用来提供对用户和服务器的认证；对传送的数据进行加密；确保数据在传送中不被改变，即数据的完整性，现已成为该领域中全球化标准。

通过 SSL 认证后，可以实现数据信息在客户端和服务器之间的加密传输，可以防止数据信息的泄露，保证了双方传递信息的安全性，而且用户可以通过服务器证书验证它所访问的网站是否是真实可靠。对于金融机构、大型购物网站来说，高安全的加密技术及严格的身份验证机制可以确保部署 SSL 证书的网站安全可靠。

SSL 证书作为国际通用的产品，最为重要的便是产品兼容性，因为它解决了用户登录网站的信任问题，用户可以通过 SSL 证书轻松识别网站的真实身份，当用户访问某个网站时，如果该网站使用了 SSL 证书，则在浏览器地址栏的小锁头标志处单击，便可查看该网站的真实身份。

5．防火墙技术

防火墙是在网络之间执行安全控制策略的系统，用于保证本地网络资源的安全，通常是包含软件部分和硬件部分的一个系统或多个系统的组合。设置防火墙的目的是保护内部网络资源不被外部非授权用户使用，防止内部网络受到外部非法用户的攻击。

（1）防火墙的一般形式

防火墙通过检查所有进出内部网络数据包的合法性，判断是否会对网络安全构成威胁，为内部网络建立安全边界。一般而言，防火墙系统有两种基本形式：包过滤路由器和应用级网关。最简单的防火墙由一个包过滤路由器组成，而复杂的防火墙系统由包过滤路由器和应用级网关组合而成。在实际应用中，由于组合方式有多种，防火墙系统的结构也有多种形式。防火墙一般形式如图 3.28 所示。

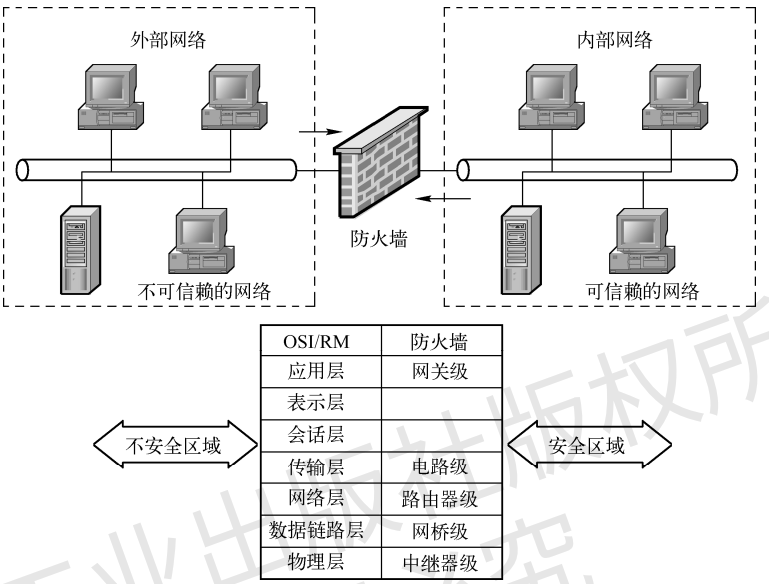


图 3.28　防火墙一般形式

（2）防火墙的作用

防火墙能增强机构内部网络的安全性。防火墙不仅是网络安全的设备的组合，更是安全策略的一个部分。

防火墙允许网络管理员定义一个中心“扼制点”来防止非法用户（如黑客、网络破坏者等）进入内部网络，禁止存在安全脆弱性的服务进出网络，并抗击来自各种路线的攻击。防火墙能够简化安全管理，网络的安全性在防火墙系统上得到了加固。

在防火墙上可以很方便地监视网络的安全性，并产生报警。防火墙是审计和记录 Internet 使用量的最佳设备。网络管理员可以在此向管理部门提供 Internet 连接的费用情况，查出潜在的带宽瓶颈的位置，并根据机构的核算模式提供部门级计费。

（3）防火墙的不足

对于防火墙而言，能通过监控所通过的数据包来及时发现并阻止外部对内部网络的攻击行为。但是，防火墙技术是一种静态防御技术，也有以下不足之处。

① 防火墙无法理解数据内容，不能提供数据安全性。

② 防火墙无法阻止来自内部的威胁。

③ 防火墙无法阻止绕过防火墙的攻击。

④ 防火墙无法防止病毒感染程序或文件的传输。

3.5　云计算

云计算是一种通过互联网提供计算资源和服务的模式，它允许用户访问和使用远程服务

器的计算能力、存储空间以及应用程序，而无须在本地设备上拥有这些资源。云计算的出现极大地改变了计算资源的使用方式，使得资源的获取更加灵活、成本效益更高，同时也促进了数据处理和存储能力的显著提升。

3.5.1 云计算与云

1．云计算的概念

云计算通过虚拟化技术将共享资源整合形成庞大的计算与存储网络，用户只需要一台接入网络的终端就能够以低廉的价格获得所需的资源和服务而无须考虑其来源。

云计算起源于 Amazon（亚马逊）产品和 Google-IBM 分布式计算项目。这两个项目直接使用了“Cloud computing”这个概念。从本质上讲，云计算是网格计算、分布式计算、并行计算、效用计算、网络存储、虚拟化、负载均衡等传统计算机技术和网络技术发展融合的产物。它旨在通过网络把多个成本相对较低的计算实体整合成一个具有强大计算能力的网络系统，并借助一些先进的商业模式把强大的计算能力分布到终端用户。云计算平台的拓扑结构，如图 3.29 所示。

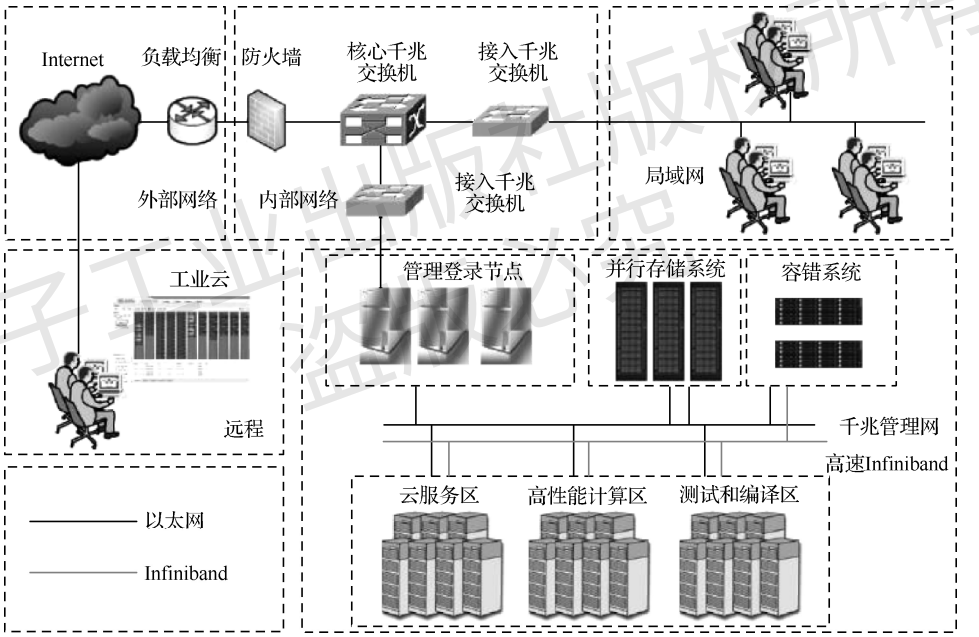


图 3.29　云计算平台的拓扑结构

云计算能将大量用网络连接的计算资源进行统一管理和调度，通过不断提高云的处理能力，减轻用户终端的处理负担，并为用户提供按需享受的计算处理能力。另外，云计算能通过千万台互联的计算机和服务器进行大量数据运算，为搜索引擎、金融行业建模、医药模拟等应用提供超级计算能力。

2．云的概念

所谓云是指以云计算、网络及虚拟化为核心技术，通过一系列的软件和硬件实现“按需服务”的计算机技术。

3．云计算与云的区别

云和云计算可从以下几个方面区分。

（1）任务不同

云是一些可以自我维护和管理的虚拟计算资源，通常是一些大型服务器集群，如计算服务器、存储服务器、宽带资源等，也包括应用端或网络终端的硬件及接入服务。

云计算侧重将所有的计算资源集中起来，并由软件实现自动管理，无须人为参与。应用提供者无须为烦琐的细节而烦恼，能够更加专注于自己的业务，有利于创新和降低成本。

（2）内涵不同

云是一种新型的 IT 技术，包括一系列的软件和硬件。

云计算是将大量用网络连接的计算资源进行统一管理和调度，构成一个计算资源池向用户提供按需服务的一种服务体系。

（3）目的不同

云的目的是更好地整合和利用网络资源，向高效节能方向发展。

云计算的目的是整合 IT 资源，更好地服务大众。

4．云计算产生的原因

云计算虽不是一个全新的概念，但它却是一项颠覆性的技术，是未来计算的发展方向。云计算产生的主要原因如下。

（1）满足硬件、基础设施的发展建设需求

高速发展的网络连接、芯片和磁盘驱动器产品性能的大幅提升，拥有成百上千台计算机的数据中心具备了快速为大量用户处理复杂问题的能力。同时，虚拟化技术日趋成熟为云计算的产生提供了基础。

（2）适应海量数据的处理需求

互联网上的信息量呈爆炸状态，各公司对数据处理能力的要求日益提高。效率、能耗、管理成本及人员、设备投入的矛盾日渐突出。另外，如何对互联网上的海量资源进行有效的计算、分配也成为一个重要的问题。

（3）网络发展的必然结果

Web 2.0 的兴起，让网络迎来了一个新的发展。MySpace、YouTube 等网站的访问量已经远远超过传统门户网站。用户数量多、参与程度高是这些网站的特点。因此，如何有效地为海量用户群体提供方便、快捷的服务，成为这些网站不得不解决的问题。

3.5.2　云计算的特点与不足

云计算是一种基于互联网的超级计算模式。它将计算任务分布在大量计算机构成的资源池上，各种应用系统能够根据需要获取计算能力、存储空间和软件服务。

1．云计算的特点

云计算的新颖之处在于它几乎可以提供无限的廉价存储和计算能力。从用户角度看，云计算有其独特的吸引力。

（1）广泛的网络接入

在任何时间、任何地点，不需要复杂的软硬件设施，通过简单的可接入网络设备，如手机就可接入云，使用已有资源或者购买所需的新服务。

（2）资源的共享

计算和存储资源集中在云端，再对用户进行分配。通过多租户模式服务多个消费者。在物理上，资源以分布式的共享方式存在，但最终在逻辑上以单一整体的形式呈现给用户，形成资源池，实现云上资源可重用。

（3）超大规模

云具有相当的规模，Google（谷歌）云计算已经拥有 100 多万台服务器，Amazon、IBM、Microsoft 等的云均拥有几十万台服务器。企业私有云一般拥有上千台服务器。云能赋予用户前所未有的计算能力。

（4）虚拟化

云计算支持用户在任意位置、使用各种终端获取应用服务。所请求的资源来自云，而不是固定的有形实体。应用在云中某处运行，但实际上用户无须了解且不用担心应用运行的具体位置。只需要一台笔记本或者一个手机，就可以通过网络服务实现需要的一切，甚至包括超级计算这样的任务。

（5）高可靠性

云使用数据多副本容错、计算节点同构可互换等措施来保障服务的高可靠性，使用云计算比使用本地计算机可靠。

（6）通用性

云计算不针对特定的应用，在云的支撑下可以构造出千变万化的应用，同一个云可以同时支撑不同的应用运行。

（7）高可扩展性

云的规模可以动态伸缩，满足应用和用户规模增长的需要。

（8）按需服务

云是一个庞大的资源池，用户按需购买。

（9）价格廉价

由于云的特殊容错机制，可以采用廉价的节点来构成云，云的自动化集中式管理使大量企业无须负担日益高昂的数据中心管理成本。云的通用性使资源的利用率较传统系统有大幅提升，因此用户可以充分享受云的低成本优势。

2．云计算的不足

（1）数据安全与隐私

云计算基础架构具有多租户的特性，厂商们通常无法保证 A 公司的数据与 B 公司的数据实现物理分隔。另外，考虑到大规模扩展性方面的要求，数据物理位置可能得不到保证。如果企业需要遵守业务交易及相关数据方面的国家或国际法规，则用户可能会觉得不放心。

（2）数据访问和存储模型

无论是 Amazon 的 S3 和 SimpleDB 服务，还是 Microsoft Azure 的数据服务，其提供的存储模型都需要适应不同的使用场景。因此，它们可能偏向采用基于二进制大对象的简单存储模型或简单的层次模型。这虽然带来了显著的灵活性，却给解释不同数据元素之间的关系增加了负担。许多依赖关系型数据库结构的事务型应用程序就不适合这种数据存储模型。

（3）缺乏标准

大多数厂商都定义了基于标准的机制来访问及使用其服务。不过，在云计算环境开发服务方面的标准才刚刚兴起，而且可移植性差。比如，使用 Google 的 AppEngine 开发应用程序的方式与在 Microsoft Azure 或 Force.com 上开发应用程序的方式截然不同。使用某厂商的编程模型开发的应用程序要移植到另一家厂商的平台上并非易事。

（4）故障处理

考虑到云计算应用程序具有大规模分布式的特性，当出现故障时，故障类型判定、故障位置确定是麻烦的事情。因此，开发应用程序时要把处理故障当作正常执行流程，而不是例外情况来处理。

（5）经济模型

按需付费的模型具有某些优势，但如果使用量一直很高，则这种模式的经济性就不再存在。特别是事务密集型应用如果要使用云计算，厂商就要考虑对付费实行最高限额。

（6）离线世界

云的实现以网络为基础，脱离了网络，云计算将变得无能为力。这也是云计算需要解决的问题。因此，对于云计算而言，端的作用方式仍需要研究。

3.6 云计算的基本类型

根据目前主流云计算服务商和服务商提供的服务，一般将云计算分为基础设施即服务（IaaS）、平台即服务（PaaS）和软件即服务（SaaS）三大类型，如图 3.30 所示。

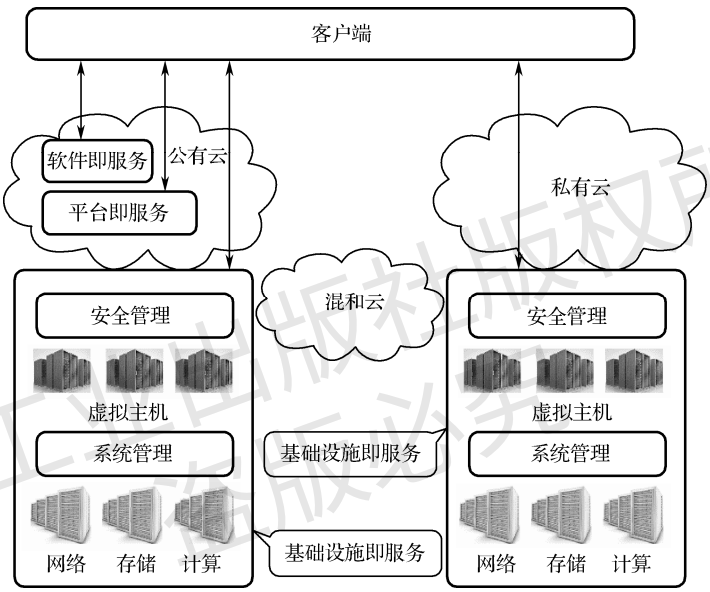


图 3.30 云计算的基本类型

3.6.1 基础设施即服务（IaaS）

基础设施即服务（Infrastructure as a Service，IaaS）指服务商通过 Internet 为用户提供计算机基础设施服务，如虚拟服务器、存储设备等。提供给用户的服务是对所有计算基础设施的利用，包括 CPU、内存、存储、网络和其他基本的计算资源，用户能够部署和运行任意软件，包括操作系统和应用程序。用户不管理或控制任何云计算基础设施，但能控制操作系统的选择、存储空间及部署应用，也有可能获得有限制的网络组件（如路由器、防火墙、负载均衡器等）控制。

IaaS 类型的云服务产品主要有 Amazon’s EC2、Go Grid’s Cloud Servers 和 Joyent。

1．IaaS 的技术特征

（1）拆分技术

拆分技术能将一台物理设备划分为多台独立的虚拟设备，各个虚拟设备之间可进行有效的资源隔离和数据隔离。由于多个虚拟设备共享一台物理设备的物理资源，所以能够充分复用物理设备的计算资源，提高资源利用率。

（2）合并技术

合并技术能将多个物理设备资源形成对用户透明的统一资源池，并能按照用户需求生成和分配不同性能配置的虚拟设备，提高资源分配的效率和精确性。

（3）弹性技术

IaaS 具有良好的可扩展性和可靠性，一方面能够弹性地进行扩容，另一方面能够为用户按需提供资源，并能够对资源配置进行适时修改和变更。

（4）智能技术

IaaS 能实现资源的自动监控和分配、业务的自动部署，能够将设备资源和用户需求更紧密地集合。

2．IaaS 的业务特征

（1）用户获得的是 IT 资源服务

用户能够租赁具有完整功能的计算机和存储设备，并获得相关的计算资源和存储资源服务。这是 IaaS 区别于平台即服务（PaaS）和软件即服务（SaaS）的特点。

IaaS 获取和使用服务都需要通过网络进行，网络成为连接云计算运营商和使用者的纽带。同时，在云服务广泛存在的情况下，IaaS 服务的运营商也会是服务的使用者，这不单是指支撑 IaaS 运营商服务的应用系统运行在云端，同时 IaaS 运营商还可能通过网络获取其他合作伙伴提供的各种云服务，以丰富自身的产品目录。

（2）用户通过网络获得服务

资源服务和用户之间的渠道是网络，当 IaaS 作为内部资源整合优化时，用户可以通过企业 Intranet 获得弹性资源。当 IaaS 作为一种对外业务时，用户可以通过互联网获得资源服务。

（3）用户能够自助服务

用户通过 Web 页面等网络访问方式，能够自助定制所需的资源类型和配置、资源使用的时间和访问方式，能够在线支付费用，能够实时查询资源使用情况和计费信息。

（4）按需计费

不论是公有云还是私有云，服务的使用者与运营商之间都会对服务的质量和内容有一个约定（SLA，Service Level Agreement，服务水平协议。为保证约定的达成，运营商需要对提供的服务进行度量和评价，以便对所提供的服务进行调度、改进与计费。所以，IaaS 服务应该是可计量的，所有资源的使用都能被监管和计量，并以此作为运营商的收费依据。IaaS 按照用户对资源的使用情况提供多种灵活的计费方式。

- 能够按照使用时长进行收费，如按月租和按小时收费。
- 能按照使用的资源类型和数量进行收费，如按照存储空间大小、CPU 处理能力进行收费。

3．IaaS 的资源层次

IaaS 的资源类型可分为 3 个层次。

（1）资源层

资源层是 IaaS 提供服务的物理基础，主要包括计算资源、存储资源和网络资源，以及必要的电力资源、IP 资源等。这一层主要通过规模采购和资源复用的模式来获得利润，利润不高。

（2）产品层

产品层是 IaaS 的核心，IaaS 运营商根据客户的各种不同需求，在资源层的基础上开发出各种各样的产品，如存储产品、消息产品、内容分发网络（Content Delivery Network，CDN）产品、监控产品。每一种产品又会根据场景和需求的不同，进行针对性的改造与优化，形成特定类型的产品。产品层是不同 IaaS 竞争力体现之处，也是 IaaS 利润的主要来源。像国内的阿里

云就提供了云主机和负载均衡、云监控等产品。Ucloud 提供了块设备存储的 UDisk、云数据库的 UDB 等产品。

（3）服务层

服务层在产品层之上，IaaS 运营商还会根据用户的需求提供更多的增值服务，如为用户提供数据快递服务、安全服务等。这部分从商业角度看利润不高，但却是用户使用 IaaS 的重要条件。

3.6.2 平台即服务（PaaS）

1．PaaS 的概念

平台即服务（Platform as a Service，PaaS）是指将研发的软件平台作为一种服务，平台通常包括操作系统、编程语言的运行环境、数据库和 Web 服务器。用户或者企业基于 PaaS 平台可以快速开发自己所需要的应用和产品。同时，PaaS 平台开发的应用能更好地搭建基于 SOA（Service-Oriented Architecture，面向服务架构）的企业应用。

PaaS 作为一个完整的开发服务，提供从开发工具、中间件到数据库软件等开发者构建应用程序所需开发平台的所有功能。用户不需且不能管理和控制底层的基础设施，只能控制自己部署的应用。

PaaS 类型的云服务产品主要有 Google’s App Engine、Microsoft’s Azure、Amazon Web Services 和 Force.com。

2．PaaS 的特点

PaaS 能将现有各种业务能力进行整合，向下根据业务能力需要测算基础服务能力，通过 IaaS 提供的 API 调用硬件资源，向上提供业务调度中心服务，实时监控平台的各种资源，并将这些资源通过 API 开放给 SaaS 用户。

PaaS 主要有两个特点。

（1）PaaS 提供的是一个基础平台，而不是某种应用

在传统的观念中，平台是向外提供服务的基础。一般来说，平台作为应用系统部署的基础，由应用服务提供商搭建和维护。而在 PaaS 模式中，由专门的平台服务提供商搭建和运营该平台，并将该平台以服务的方式提供给应用系统运营商。

（2）PaaS 运营商提供基础平台的技术支持服务

PaaS 运营商所需提供的服务，不仅是单纯的基础平台，而且包括针对该平台的技术支持服务，甚至包括针对该平台而进行的应用系统开发、优化等服务。因为 PaaS 运营商了解其运营的基础平台，所以由 PaaS 运营商提出的对应用系统进行优化和改进的建议非常重要。在应用系统的开发过程中，PaaS 运营商的技术咨询和支持团队的介入也是保证应用系统在以后运营中得以长期、稳定运行的重要因素。

3.6.3 软件即服务（SaaS）

软件即服务（Software as a Service，SaaS）是一种通过 Internet 提供软件的模式，用户无须购买软件，而是向提供商租用基于 Web 的软件来管理企业经营活动。云提供商在云端安装和运行应用软件，云用户通过云客户端使用软件。在 SaaS 模式中，云用户不能管理应用软件运行的基础设施和平台，只能进行有限的应用程序设置。

SaaS 类型的云服务产品有主要有 Yahoo 邮箱、Google Apps、Saleforce.com、WebEx 和 Microsoft Office Live。

SaaS 的服务模式类似于传统 ASP（Application Service Provider Model，应用服务提供商）模式，服务商提供软件，基础设施及工作人员为客户提供个性化的 IT 解决方案。两者的共同点都是为终端用户免去烦琐的安装过程，提供一站式的服务。不同的是，在 ASP 模式下，IT 基础设施和应用是专属于用户的。而在 SaaS 模式下，用户之间的应用和 IT 基础设施则是相互共享的。

1．SaaS 的两大类型

SaaS 企业管理软件分成两大阵营：平台型 SaaS 和傻瓜式 SaaS。平台型 SaaS 和傻瓜式 SaaS 的共同点是都能租赁使用。但是，无论是平台型 SaaS 还是傻瓜式 SaaS，SaaS 服务提供商都必须有自己的知识产权，所以企业在选择 SaaS 产品时应当了解服务商是否有自己的知识产权。

（1）平台型 SaaS

平台型 SaaS 是把传统企业管理软件的强大功能通过 SaaS 模式交付给客户，该类型的平台有强大的自定制功能。一般而言，因为平台型 SaaS 具有强大的自定制功能而更能满足企业的应用需求。当然，并非所有 SaaS 服务提供商的产品都具有自定制功能，所以企业在选择产品时要先考察清楚。

（2）傻瓜式 SaaS

傻瓜式 SaaS 提供固定功能和模块，简单易懂，但无法升级和不能自定制在线应用，用户也是按月付费。傻瓜式 SaaS 的功能是固定的，在某个阶段能适应企业的发展，一旦企业有了新的发展，只能“二次购买”所需服务。

2．SaaS 的优缺点

（1）优点

对企业来说，SaaS 的优点表现在以下几个方面。

① 技术方面。

SaaS 是简单的部署，不需要购买任何硬件，企业无须配备 IT 方面的专业技术人员，同时又能得到最新的技术应用，满足企业对信息管理的需求。

② 投资方面。

企业只以相对低廉的“月费”方式投资，不用一次性投资，不占用过多的运营资金，从而缓解企业资金不足的压力。同时，也不用考虑折旧问题，并能及时获得最新硬件平台及最佳解决方案。

③ 维护和管理方面。

由于企业采取租用的方式来进行业务管理，不需要专门的维护和管理人员，能缓解企业在人力、财力上的压力，使其能够集中资金有效地运营核心业务。

（2）缺点

① 安全性方面。

大型企业不愿使用 SaaS 是因为安全问题，他们要保护他们的核心数据，不希望这些核心数据由第三方来负责。

② 标准化方面。

SaaS 解决方案缺乏标准化。这个行业刚刚起步，没有明确的解决办法，每家公司都可以设计一个解决方案。

3.6.4 三种云计算类型的关系

1．云计算同传统 IT 服务模式的区别

云计算同传统 IT 服务模式的区别如表 3.1 所示。

表 3.1　云计算同传统 IT 服务模式的区别

云计算	服务内容	服务对象	使用模式	和传统 IT 的区别	典型系统
IaaS	IT 基础设施	需要硬件资源的用户	上传数据、程序和环境配置	相比于传统的服务器、存储设备： • 无限和按需获得资源； • 初始投资小； • 按需付费	• Amazon's EC2； • Go Grid's Cloud Servers； • Joyent
PaaS	提供应用程序开发环境	系统开发者	上传数据、程序	相比于传统的数据库、中间件、Web 服务器和其他软件： • 无限和按需获得资源； • 初始投资小； • 按需付费； • 兼容性； • 集成全生命周期开发环境	• Google's App Engine； • Microsoft's Azure； • Amazon Web Services； • Force.com
SaaS	提供基于互联网的应用服务	企业和个人用户	上传数据	相比于传统的 ASP 模式： • 无限和按需获得资源； • 初始投资小； • 按需付费； • 兼容性、灵活性； • 稳定可靠； • 共享的应用和基础设施	• Yahoo 邮箱； • Google Apps； • Saleforce.com； • WebEx； • Microsoft Office Live

2．三种模式的关系

虽然云计算具有三种服务模式，但在使用过程中并不需要严格地对其进行区分。底层的基础服务和高层的平台和软件服务之间的界限并不绝对。

随着技术的发展，三种模式的服务在使用过程中并不是相互独立的。

① 底层（IaaS）的云服务商提供最基本的 IT 架构服务，SaaS 层和 PaaS 层的用户既可以是 IaaS 云服务商的用户，也可以是最终端用户的云服务提供者。

② PaaS 层的用户同样也可能是 SaaS 层用户的云服务提供者。

从 IaaS 到 PaaS 再到 SaaS，不同层的用户之间互相支持，同时扮演多重角色。并且，企业根据不同的使用目的同时采用云计算三层服务的情况也很常见。

3.7　主流云计算技术介绍

3.7.1　常见的云解决方案

当前，各大云计算厂商采用各自的云计算方案，常见的有 Google 云计算技术、Amazon 的 AWS、Amazon 的 AWS、开源的 Hadoop、Microsoft 的 Windows Azure、基于应用虚拟化的云计算技术等。

1．Google 云计算技术

Google 采用由若干个相互独立又紧密结合在一起的系统组成云计算基础架构，主要包括 4 个系统：建立在集群之上的文件系统（Google File System）、针对 Google 应用程序特点提出的 Map/Reduce 分布式计算系统、分布式锁服务系统（Chubby）和大规模分布式数据库系统（BigTable）。

Google 的云可以看成利用虚拟化实现的云计算基础架构（硬件架构）加上基于云的文件系统和数据库及相应的开发应用环境，用户通过浏览器就可以使用分布在云上的 Google Docs

等应用，如图 3.31 所示。

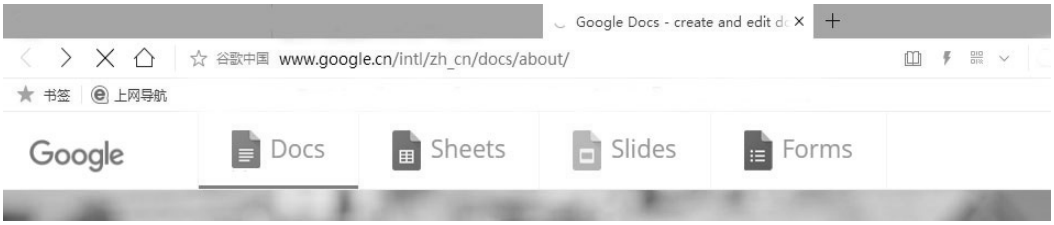


图 3.31　浏览器上的 Google 开发应用环境

2．Amazon 的 AWS

AWS（Amazon Web Service）基于云的基础架构如图 3.32 所示。AWS 提供基于 SOAP 的 Web Service 接口，在这之上建立基于云的 Web 2.0 服务，对最终用户来说，只需浏览器就可以使用。

图 3.32　AWS 基于云的基础架构

AWS 是一组服务，它们允许通过程序访问 Amazon 的计算基础设施。这些服务包括存储、计算、消息传递和数据集，具体见表 3.2。

表 3.2　AWS 的基本服务

基本服务	说明
存储：Amazon Simple Storage Service (S3)	所有应用程序都需要存储文件、文档，供用户下载或备份。可以把应用程序需要的任何东西存储在其中，从而实现可伸缩、可靠、高可用、低成本的存储
计算：Amazon Elastic Compute Cloud (EC2)	能够根据需要扩展或收缩计算资源，非常方便地提供新的服务器实例
消息传递：Amazon Simple Queue Service (SQS)	提供不受限制的可靠的消息传递，可以使用它消除应用程序组件之间的耦合
数据集：Amazon SimpleDB (SDB)	提供可伸缩、包含索引且无须维护的数据集存储，以及处理和查询功能

3．开源的 Hadoop

Hadoop 是 Apache 软件基金会研发的开放源码并行运算编程工具和分布式文件系统，与 Map/Reduce和 Google 文件系统类似，是用于在大型集群廉价硬件设备上运行应用程序的框架，提供高效、高容错性、稳定的分布式运行接口和存储。基于 Hadoop 的云计算环境能提供云计算能力和云存储能力的在线服务，最终用户可以通过浏览器使用这些服务。

图 3.33 描述了 Hadoop 项目的基础架构。其核心组件包括分布式文件系统 HDFS、分布式计算框架 MapReduce 等。

图 3.33　Hadoop 项目的基础架构

4．Microsoft 的 Windows Azure

Microsoft 的 Windows Azure 是构建在 Microsoft 数据中心基础上能够提供云计算的一个应用程序平台，包含云操作系统、基于 Web 的关系型数据库（SQL Azure）和基于.NET 的开发环境。开发环境与Visual Studio集成，开发人员能使用集成开发环境来开发与部署要挂载在 Azure 上的应用程序。Microsoft 倡导的云计算是“云+端计算”，终端是操作系统加上桌面软件的方式。

基于 Windows Azure 的云存储和 Web Service 接口建立的在线服务，对于最终用户来说是桌面软件的形态，使用的终端主要是 PC、笔记本，仍旧要依赖 Microsoft 的操作系统，软件的计算仍旧依赖终端的处理能力。

5．基于应用虚拟化的云计算技术

基于应用虚拟化的云计算技术，能按需提供服务，运行、存储都在云端，可以通过应用虚拟化实现 SaaS 云平台。2009 年，Amazon EC2（弹性计算云）已经与应用虚拟化产品的主要厂商 Citrix（思杰）合作推出商用云平台 Citrix C3 Lab。由于对终端的计算能力要求很低，用户甚至可以使用手机按使用传统软件的方式使用基于云的服务。

基于应用虚拟化的云计算通过应用虚拟化架构把表示层做成应用虚拟化引擎。该引擎可以放在计算系统的操作系统和应用层之间，隔绝重要应用，这是应用虚拟化技术的核心思想。应用虚拟化在后端服务与终端之间增加一个虚拟层，应用运行在虚拟层，而将应用运行的屏幕界面推送到终端上显示，即“应用交付”的概念。

通过应用虚拟化技术，用户可以远程访问程序，就好像它们在最终用户的本地计算机上运行一样。这些程序称为虚拟化程序。虚拟化程序与客户端的桌面集成在一起，而不是在服务器的桌面上向用户显示。虚拟化程序在自己的可调整大小的窗口中运行，可以在多个显示器之间拖动，并且在任务栏中有自己的条目。当用户在同一个服务器上运行多个虚拟化程序时，虚拟化程序将共享同一个远程会话。

3.7.2　基本云计算的技术对比

表 3.3 简明描述了常见云计算的技术比较。

表 3.3　常见云计算的技术比较

厂家	技术特性	核心技术	企业服务	开发语言	开源情况
Microsoft	整合其所用软件及数据服务	大型应用软件开发技术	Azure 平台	.NET	不开源

续表

厂家	技术特性	核心技术	企业服务	开发语言	开源情况
Google	存储及运算扩充能力	并行分散技术； • MapReduce 技术； • BigTable 技术； • GFS 技术	• Google App Engine； • 应用代管服务	Python、Java	不开源
IBM	整合其所有硬件及软件	• 网格技术； • 分布式存储	• 虚拟资源池提供； • 企业云计算整合		不开源
Oracle	软硬件弹性平台	• Oracle 的数据存储技术； • Sun 的开源技术	• EC2 上的数据库； • OracleVM； • SunxVM		部分开源
Amazon	弹性虚拟平台	虚拟化技术 Xen	• EC2； • S3； • SimpleDB； • SQS		开源
Saleforce	弹性可定制商务软件	平台整合技术	Force.com	Java、Apex	不开源
EMC	信息存储技术 及虚拟化技术	Vmware 的虚拟化技术	• Atoms 云存储系统； • 私有云解决方案		不开源
阿里巴巴	弹性可定制商务软件	平台整合技术	• 软件互联平台； • 云电子商务平台		不开源
中国移动	丰富宽带资源	• 底层集群部署技术； • 资源池虚拟技术	BigCloud		不开源

3.8 知识扩展

3.8.1 华为的星闪技术

华为的星闪技术也称为 NearLink，是华为在面临美国制裁后被迫退出蓝牙技术联盟时开始研发的一种先进的无线短距离通信技术，它综合了蓝牙和 Wi-Fi 的优势，并引入了 5G 技术的元素，旨在提供低时延、高速率、高可靠性及低功耗的通信解决方案。

华为的星闪技术在性能上的全面提升，使其在多种应用场景中展现出巨大的优势，尤其是在智能设备和物联网的快速发展背景下，具有重要应用价值。

1．技术架构

星闪技术采用了一种分层的系统架构，包括基础应用层、基础服务层和星闪接入层。其中，星闪接入层提供了 SLB（SparkLink Basic，基础接入）和 SLE（SparkLink Low Energy，低功率接入）两种通信接口，分别对标 Wi-Fi 和蓝牙，以满足不同场景下的通信需求。

2．技术性能

星闪技术在性能上有了显著提升。SLB 接口采用超短帧、多点同步等技术，拥有更快速度、更低时延（20μs），支持更快的数据传输速率，适用于低时延、高可靠性、精同步、高并发和高安全等传输需求的业务场景。而 SLE 接口则采用 Polar 信道编码等技术，支持更低的功耗，满足低功耗、高可靠性的场景需求。

据华为官方介绍，星闪技术的峰值传输速率可以达到 8Gbps，远超现有蓝牙的速率。这一技术特别适用于对数据传输速度有极高要求的场景，如高清视频传输、虚拟现实（VR）和增强现实（AR）应用，以及高速数据同步等。

蓝牙技术是一种广泛使用的无线通信标准，主要用于短距离设备之间的通信，如手机、

耳机、智能手表等。截至 2025 年 3 月，蓝牙技术的最新版本为蓝牙 5.4。蓝牙 5.4 的数据传输速度相较于之前的版本有所提升。尽管蓝牙 5.4 同样支持 2 Mbps 的数据传输速率，但由于采用了更高效的编码方式和更优化的数据传输协议，所以实际传输速度更快、延迟更低。这意味着在使用蓝牙 5.4 的设备时，用户可以感受到更短的等待时间，尤其是在传输大文件、玩游戏或观看高清视频时，体验会更加流畅。此外，蓝牙 5.4 还在连接稳定性、功耗控制以新特性上有所增强和优化。

3．应用场景

星闪技术被广泛应用于智能汽车、智能终端、智能家居、智能制造等快速发展的产业链上下游及新场景应用。例如，在智能汽车领域，星闪技术支持实时的 360°无线环视，优化有线线束的使用，减轻车重；在智能终端方面，星闪技术已应用于华为的 Mate 60 系列、Mate 70 系列直板手机，Mate X6 折叠屏手机，MatePad 系列平板电脑。

3.8.2 Google 的云计算技术构架分析

日常使用的 Google Search、Google Earth、Google Map、Google Gmail、Google Doc 等业务都是 Google 基于云计算平台提供的。从 Google 的整体的技术构架来看，Google 计算系统依然是边进行科学研究，边进行商业部署，依靠系统冗余和良好的软件构架实现庞大系统的低成本运作。Google 在应对互联网海量数据处理的压力下，充分借鉴大量开源代码及其他研究机构和专家的思路，构架自己的有创新性的计算平台。

1．Google 的整体技术构架

大型的并行计算、超大规模的 IDC（Internet Data Center，Internet 数据中心）快速部署、通过系统构架来使廉价 PC 服务器具有超过大型机的稳定性都已经成为互联网时代、IT 企业获得核心竞争力发展的基石。

Google 最大的优势在于它建造出能承受极高负载的高性价比的系统。因此，Google 认为自己与竞争对手，如亚马逊网站（Amazon）、电子港湾（eBay）、微软（Microsoft）和雅虎（Yahoo）等公司相比，具有更大的成本优势。其 IT 系统运营成本约为其他互联网公司的 60%左右。同时，Google 已经开发出了一整套专用于支持大规模并行系统编程的定制软件库，所以 Google 程序员的效率比其他 Web 公司的同行们高出 50%～100%。

Google 云计算技术架构如图 3.34 所示。从整体来看，Google 的计算平台包括如下几个方面。

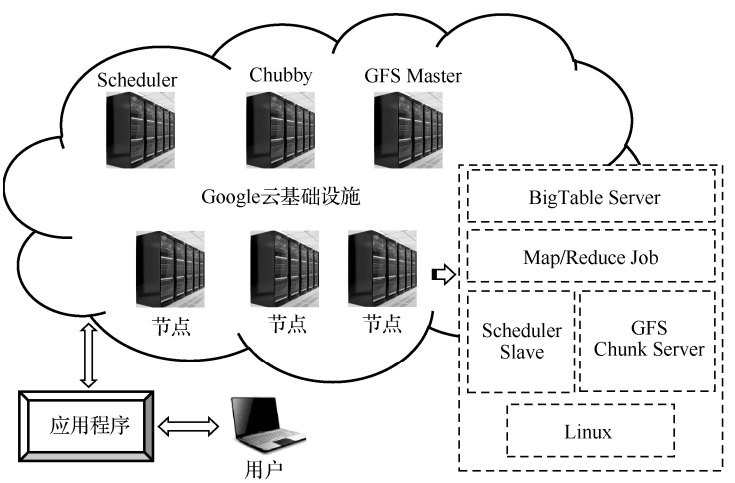


图 3.34　Google 云计算技术架构

（1）网络系统

网络系统包括外部网络（Exterior Network，简称外网）和内部网络（Interior Network，简称内网），这里的外部网络并不是指运营商自己的骨干网，而是指在 Google 计算服务器中心以外，由 Google 自己搭建的用于不同地区/国家、不同应用之间的负载平衡的数据交换网络。内部网络是指连接各个 Google 自建的数据中心之间的网络系统。

（2）硬件系统

硬件系统包括单个服务器，以及整合了多服务器机架和存放、连接各个服务器机架的数据中心（IDC）。

（3）软件系统

软件系统包括每个服务器上安装的 Red Hat Linux，以及 Google 计算底层软件系统（文件系统 GFS、并行计算处理算法 Map/Reduce、并行数据库 BigTable、并行锁服务 ChubbyLock、计算消息队列 GWQ）等。

（4）Google 内部使用的软件开发工具

这种工具包括 Python、Java、C++等。

（5）Google 自己开发的应用软件

这种软件包括 Google Search、Google Email、Google Earth 等。

2．Google 的外部网络系统

当一个互联网用户输入 www.google.com 的时候，这个 URL 请求就会被发到 Google 的 DNS 解析服务器。Google 的 DNS 解析服务器会根据用户的 IP 地址来判断用户请求是来自哪个国家、哪个地区的；根据不同用户的 IP 地址信息，解析到不同的 Google 的数据中心。

然后，用户请求进入第一级防火墙，这级防火墙主要任务是根据不同端口来判断应用，过滤相应的流量。如果仅接受浏览器应用的访问，一般只会开放 80 端口 HTTP 和 443 端口 HTTPS（通过 SSL 加密）。放弃来自互联网上的非 IPv4/IPv6 非 80/443 端口的请求，避免遭受互联网上大量的 DOS 攻击。

Google 使用 Citrix 的 NetScaler 应用交换机实现 Web 应用的优化。NetScaler 使用高级优化技术（如动态缓存时），可以大大提升 Web HTTP 性能，有效降低后端 Web 应用服务器的处理和连接压力。同时，Google 使用反向代理技术，屏蔽内部服务器差异。反向代理方式是指以代理服务器来接受 Internet 上的连接请求，然后将请求转发给内部网络上的服务器，并将从服务器得到的结果返回给 Internet 上请求连接的客户端，此时代理服务器对外就表现为一个服务器。

3．Google 的内部网络架构

Google 已经建设了跨国的光纤网络，连接跨地区、跨国家的高速光纤网络。内部网络采用 IPv6 协议。在每个服务器机架内部，服务器之间的连接网络是 100M 以太网，服务器机架之间的连接网络是 1000M 以太网。

在每个服务器机架内，通过 IP 虚拟服务器（IP Virtual Server，IPVS）的方式实现传输层负载平衡，这个就是所谓四层 LAN 交换。IPVS 使一个服务器机架中的众多服务成为基于 Linux 内核的虚拟服务器。这就像在若干服务器前安装一个负载均衡的服务器一样，当收到 TCP/UDP 的请求时，使某个服务器可以使用一个单一的 IP 地址来对外提供相关的服务支撑。

4．Google 的大规模 IDC 部署

海量信息的存储、处理需要大量的服务器，为了满足不断增长的计算需求，Google 很早就进行了全球的 IDC 部署。IDC 的选择面临电力供应、大量服务器运行后的降温排热、足够

的网络带宽支持等关键问题。因此，Google 在部署 IDC 的时候，是根据互联网骨干带宽和电力网的核心节点部署的。

目前，Google 已在全球部署了 38 个大型的 IDC、300 多个 GFSII 服务器集、80 多万台计算机。目前，Google 在中国的北京和香港建设了 IDC。Google 设计了创新的集装箱式服务器，IDC 以货柜为单位，标准的 Google 模块化集装箱装有 30 个机架、1160 台集装箱式服务器，每台服务器的功耗是 250kW。这种标准的集装箱式服务器部署和安装策略使 Google 能快速地部署一个超大型 IDC，从而大大降低对于机房基建的需求。

5．Google 的 PC 服务器刀片

Google 的核心技术之一是，Google 所拥有的 80 多万台服务器都是自己设计的，Google 的硬件设计人员直接和芯片厂商及主板厂商协作。从 2009 年开始，Google 开始大量使用 2U 的低成本解决方案，每个服务器刀片自带 12V 的电池来保证在短期没有外部电源的情况下可以保持服务器刀片正常运行，自带电池方式的效率比传统 UPS 方式的效率更高。

6．Google 服务器的操作系统

Google 服务器使用的操作系统是基于 Red Hat Linux 2.6 内核的修改版。它修改了 GNUC 函数库和远程过程调用（RPC），开发了自己的 IPvs；修改了文件系统，形成了自己的 GFSII；修改了 Linux 内核和相关的子系统，使其支持 IPv6；采用了 Python 作为主要的脚本语言。

7．Google 云计算的文件系统 GFS/GFSII

GFS（Google File System，Google 文件系统）是 Google 设计的由大量安装有 Linux 操作系统的普通 PC 构成的分布式文件系统。整个集群系统由一台 Master（通常有几台备份）和若干台 Chunk Server 构成。

在 GFS 中，文件备份成固定大小的 Chunk，分别存储在不同的 Chunk Server 上；每个 Chunk 有多份拷贝，也存储在不同的 Chunk Server 上。Master 负责维护 GFS 中的 Metadata（元数据），即文件名及其 Chunk 信息。客户端先从 Master 上得到文件的 Metadata，根据要读取的数据在文件中的位置与相应的 Chunk Server 通信，获取文件数据。GFS 为 Google 云计算提供海量存储，并且与 Chubby、Map/Reduce 及 BigTable 等技术紧密结合，处于所有核心技术的底层。

在实际中，GFS 块存储服务器上的存储空间以 64MB 为单位分成很多的存储块，由主服务器来进行存储内容的调度和分配。每份数据都是一式三份，将同样的数据分布存储在不同的服务器集中，以保证数据的安全性和吞吐率。当需要存储文件、数据的时候，应用程序将需求发给主服务器，主服务器根据所管理的块存储服务器的情况，将需要存储的内容进行分配（使用哪些块存储服务器和哪些地址空间）然后，由 GFS 接口将文件和数据直接存储到相应的块存储服务器中。

在块存储服务器中，数据经过压缩后存储，压缩采用 BMDiff 和 Zippy 算法。BMDiff 使用最长公共子序列进行压缩，压缩速度为 100MBps，解压缩速度约为 1000MBps。

8．Google 并行计算构架 Map/Reduce

Google 设计并实现了一套大规模数据处理的编程规范 Map/Reduce 系统。这样，非分布式专业的应用程序编写人员在不用顾虑集群可靠性、可扩展性等问题的基础上也能够为大规模集群编写应用程序。应用程序编写人员只需要将精力放在应用程序本身上，而关于集群的处理问题则交由平台来处理。

Map/Reduce 通过 Map（映射）和 Reduce（化简）这样两个简单的概念来参加运算，用户只需要提供自己的 Map 函数及 Reduce 函数就可以在集群上进行大规模的分布式数据处理。

Google 的文本索引方法（即搜索引擎的核心部分）已经通过 Map/Reduce 的方法进行了改写，获得了更加清晰的程序架构。

与传统的分布式程序设计相比，Map/Reduce 封装了并行处理、容错处理、本地化计算、负载均衡等细节；同时，还提供了一个简单而强大的接口，通过这个接口可以把计算自动地并发和分布执行，从而使编程变得非常容易。不仅如此，通过 Map/Reduce 还可以由普通 PC 构成巨大集群来达到极高的性能。另外，Map/Reduce 也具有较好的通用性，大量的不同问题都可以简单地通过 Map/Reduce 来解决。

（1）映射和化简

简单地说，一个映射函数就是对由一些独立元素组成的概念上的列表（例如一个测试成绩的列表）的每个元素进行指定的操作（比如，有人发现成绩列表中所有学生的成绩都被高估了一分，他可以定义一个“减一”的映射函数，用来修正这个错误）。事实上，每个元素都是被独立操作的，但原始列表没有被更改，因为这里创建了一个新的列表来保存新的答案。也就是说，Map 操作是可以高度并行的，这对高性能要求的应用及并行计算领域的需求非常有用。

化简操作是指对一个列表的元素进行适当的合并（例如，有人想知道班级的平均分，他可以定义一个化简函数，通过让列表中的元素与自己的相邻元素相加的方式把列表减半，如此递归运算直到列表只剩下一个元素，然后用这个元素除以人数，就得到了平均分）。虽然化简函数不如映射函数那么并行，但因为化简总是有一个简单的答案，大规模的运算相对独立，所以化简函数在高度并行环境下也很有用。

（2）分布和可靠性

Map/Reduce 通过把数据集分发给网络上的每个节点实现可靠性，每个节点会周期性地返回其所完成的工作和最新的状态。如果一个节点保持沉默超过一个预设的时间，主节点（类同 GFS 中的主服务器）则把这个节点标记为死亡状态，并把分配给这个节点的数据发到其他节点。

每个操作使用命名文件的原子操作以确保不会发生并行线程间的冲突。当文件被改名时，系统可能会把它们复制到任务名以外的另一个名字上去。由于化简操作的并行能力较差，主节点会尽量把化简操作调度在一个节点上，或者调度到离待操作数据尽可能近的节点上。

在 Google 中，Map/Reduce 应用非常广泛，包括分布 grep、分布排序、Web 连接图反转、每台机器的词矢量、Web 访问日志分析、反向索引构建、文档聚类、机器学习、基于统计的机器翻译等。值得注意的是，Map/Reduce 会生成大量的临时文件，为了提高效率，它利用 GFS 来管理和访问这些临时文件。

9．Google 并行计算数据库

BigTable 是 Google 开发的基于 GFS 和 Chubby 的分布式存储系统。Google 的很多数据，包括 Web 索引、卫星图像数据等在内的海量结构化和半结构化数据都存储在 BigTable 中。从实现上来看，BigTable 并没有什么全新的技术，但如何选择合适的技术并将这些技术高效地结合在一起恰恰是最大的难点。Google 的工程师通过研究及大量实践实现了相关技术的选择与融合。

BigTable 在很多方面和数据库类似，但它并不是真正意义上的数据库。BigTable 建立在 GFS、Scheduler、Lock Service 和 Map/Reduce 之上。每个 Table 都是一个多维的稀疏图（Sparse Map）。Table 由行和列组成，表中的数据通过一个行关键字（Row Key）、一个列关键字（Column Key）及一个时间戳（Time Stamp）进行索引。BigTable 对存储在其中的数据不做任何解析，

一律看成字符串，具体数据结构的实现需要用户自行处理。

在不同的时间对同一个存储单元 cell 有多份拷贝，这样就可以记录数据的变动情况。

BigTable 的存储逻辑可以表示为：（row：string，column：string，time：int64）→string。BigTable 数据的存储格式如图 3.35 所示。

为了管理大的 Table，把 Table 按行分割，这些分割后的数据统称为 Tablets。每个 Tablets 大概有 100～200MB，每个机器存储 100 个左右的 Tablets。底层的架构是 GFS。由于 GFS 是一种分布式文件系统，采用 Tablets 的机制后，可以获得很好的负载均衡。比如，可以把经常响应的表移动到其他空闲机器上，然后快速重建。Tablets 在系统中的存储方式是不可修改的 immutable 的 SSTables，一台机器一个日志文件。BigTable 中最重要的选择是将数据存储分为两部分：主体部分是不可变的，以 SSTable 的格式存储在 GFS 中；最近的更新则存储在内存（称为 memtable）中。读操作需要根据 SSTable 和 memtable 综合决定要读取的数据的值。

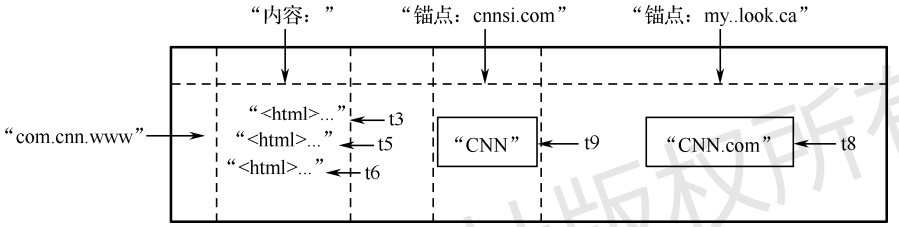


图 3.35　BigTable 数据的存储格式

Google 的 BigTable 不支持事务，只保证对单条记录的原子性。BigTable 的开发者通过调研后发现只要保证对单条记录更新的原子性就可以了。这样，为了支持事务所要考虑的串行化、事务的回滚、死锁检测（一般认为，分布式环境中的死锁检测是不可能的，一般都用超时解决）等复杂问题都可不予考虑，系统实现进一步简化。

10．Google 并行锁服务 Chubbylock

Chubby 是 Google 设计的提供粗粒度锁服务的一个文件系统，它基于松耦合分布式系统，解决了分布的一致性问题。通过使用 Chubby 的锁服务，用户可以确保数据操作过程中的一致性。需要注意的是，这种锁只是一种建议性锁（Advisory Lock），而不是强制性锁（Mandatory Lock），如此选择的目的是使系统具有更大的灵活性。

GFS 使用 Chubby 来选取一个 GFS 主服务器，BigTable 使用 Chubby 指定一个主服务器并发现、控制与其相关的子表服务器。除了最常用的锁服务，Chubby 还可以作为一个稳定的存储系统存储包括元数据在内的小数据。同时，Google 内部还使用 Chubby 进行名字服务（Name Server）。

Chubby 被划分成两个部分：客户端和服务器端，客户端和服务器端之间通过远程过程调用（RPC）来连接。在客户端，每个客户应用程序都有一个 Chubby 程序库（Chubby Library），客户端的所有应用都是通过调用这个库中的相关函数来完成。服务器一端称为 Chubby 单元，一般是由五个称为副本（Replica）的服务器组成，这五个副本在配置上完全一致，并且在系统刚开始时处于对等地位。这些副本通过 Quorum 机制选举产生一个主服务器（Master），并保证在一定的时间内有且仅有一个主服务器，这个时间就称为主服务器租约期（Master Lease）。如果某个服务器被连续推举为主服务器，则这个租约期就会不断地被更新。在租约期内，所有的客户请求都由主服务器来处理。客户端如果需要确定主服务器的位置，则可以向 DNS 发送一个主服务器定位请求，非主服务器的副本将对该请求做出回应，客户端通过这种方式能够快速、准确地对主服务器做出定位。Chubby 的基本架构如图 3.36 所示。

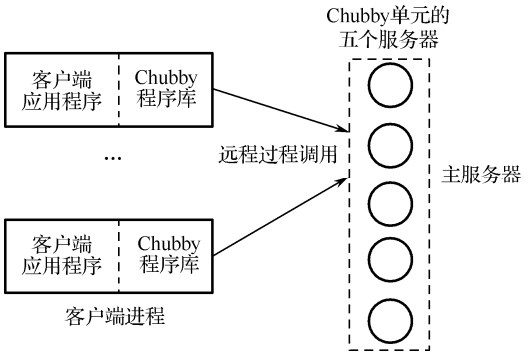


图 3.36　Chubby 的基本架构

11．Google 的工作队列（GWQ）系统

GWQ（Google Work Queue，Google 工作队列）系统负责将 Map/Reduce 的工作任务安排给各个计算单位。GWQ 系统可以同时管理数万台服务器。可以通过 API 接口和命令行调用 GWQ。

12．Google 的开发工具

除了传统的 C++和 Java，Google 开始大量使用 Python。在 Google 内部，很多项目使用 C++编写性能要求极高的部分，然后用 Python 调用相应的模块。

3.8.3　我国云服务的发展

随着全球数字化转型的加速，云计算作为重要的基础设施和服务模式，在中国经历了从萌芽到成熟的多个发展阶段，并持续推动着经济社会的数字化转型。

自 2006 年以来，中国云计算行业经历了形成期（2006—2010 年）、发展期（2010—2015 年）、应用期（2015—2020 年）和成熟期（2020—2025 年/2030 年）四个阶段。这一过程不仅展现了技术的不断进步，也反映了市场需求和政策支持的推动作用。

1．阿里云

阿里云隶属于阿里巴巴集团。自 2009 年成立以来，阿里云在技术创新、市场拓展和国际合作方面取得了显著成就，成为数字化转型的重要推动者。阿里云不仅在中国市场占有率高，还积极扩展国际市场，在全球多个国家和地区建立数据中心。例如，阿里云在印尼的数据中心是当地唯一的全球化公共云服务商。

（1）核心产品与服务

① 基础设施与服务。

阿里云提供广泛的云计算服务，包括基础设施即服务（IaaS）、平台即服务（PaaS）和软件即服务（SaaS）。其自主研发的飞天操作系统和分布式架构技术已达国际领先水平。

② 数据库与存储。

阿里云提供多种数据库和存储解决方案，如 PolarDB（云原生数据库）、OSS（Object Storage Service，对象存储服务）及分布式数据库服务等，帮助企业灵活管理数据。

③ 人工智能与大数据。

阿里云在人工智能与大数据领域也有深厚积累，推出多款人工智能产品和服务，如通义千问、机器学习平台 PAI 等。

（2）技术创新与成就

① 计算能力与效率。

阿里云在 Sort Benchmark 竞赛中多次打破世界纪录，利用自研的分布式计算平台 ODPS

高效完成数据排序任务。

② 防御能力。

2014 年，阿里云成功抵御了当时全球互联网史上最大的 DDoS 攻击，峰值流量达到 453.8Gbps。

③ 价格优势。

阿里云通过不断优化其服务和价格策略，在全球范围内降价，提高了市场竞争力。

（3）应用场景与合作伙伴

阿里云服务涵盖制造、金融、政务、交通、医疗等多个领域，为大型企业和互联网公司提供支持。例如，阿里云帮助中国一汽打造大模型应用，提升智能决策水平。

2．天翼云

天翼云是中国电信推出的云计算服务品牌，旨在为用户提供云网融合、安全可信的专属定制云服务。天翼云不断扩展其产品线和服务范围，从最初的基础设施即服务（IaaS）逐步发展到平台即服务（PaaS）和软件即服务（SaaS），形成了全面的云服务产品体系。

（1）核心产品与服务

① 基础设施与服务。

天翼云提供丰富的云计算服务，包括弹性云主机、云电脑、物理机、对象存储等，满足不同规模企业的上云需求。

② 数据库与存储。

天翼云提供关系型数据库 MySQL 版、分布式数据库、云硬盘备份等服务，帮助企业灵活管理数据并确保数据安全。

③ 人工智能与大数据。

天翼云在人工智能与大数据领域也积极布局，推出了天翼云诸葛 AI 平台，为企业提供数据分析、机器学习等智能服务。

（2）技术创新与成就

① 云网融合技术。

天翼云致力于实现云与网络的深度融合，通过全球分布的数据中心和高速网络连接，为用户提供低延时、高可用的云服务体验。

② 安全与信任。

天翼云通过了多项国内外安全认证，如 ISO 27001 信息安全管理体系认证、CSA STAR 云安全认证等，确保用户数据的安全和隐私。

（3）应用场景与合作伙伴

天翼云的服务已广泛应用于政府、金融、教育、医疗等多个行业，支持了无数企业和机构的数字化转型。天翼云积极构建开放的云生态，与众多技术合作伙伴和开发者共同开发创新应用，推动整个行业的技术进步。

3．华为云

华为云是华为公司提供的云计算服务，它提供了丰富的云产品和服务，帮助企业和个人进行数字化转型。

（1）云服务器

在云服务器方面，华为云提供的弹性云服务器 ECS，可以自动获取和弹性伸缩，适合各种计算需求。对于希望获得更高性能的用户，华为云的 Flexus 云服务器 X 实例能提供柔性算力和旗舰级体验。针对特定工作负载，如 GPU 加速云服务器 GACS 和 FPGA 加速云服务器

FACS，它们分别提供优秀的浮点计算能力和 FPGA 计算资源。

（2）存储服务

在存储服务上，华为云的对象存储服务 OBS 能够存储任意数量和形式的非结构化数据，而云硬盘 EVS 为计算服务提供持久性块存储的服务。对于需要备份数据的用户，云备份 CBR 可以为云服务器、云硬盘等提供备份服务。另外，数据快递服务 DES 支持将从 TB 到 PB 级的海量数据传输到华为云。

（3）网络产品

在网络产品方面，虚拟私有云 VPC 提供隔离的、私密的虚拟网络环境。全球加速 GA 提供 SLA 稳定的加速传输。CDN 与智能边缘服务则改善网络拥挤状况，提高用户访问速度。

（4）数据库服务

华为云的数据库服务也非常全面。关系型数据库服务包括云数据库 GaussDB for MySQL、RDS for MySQL 等，它们都兼容相应的数据库引擎，提供稳定可靠、安全运行和弹性伸缩的能力。非关系型数据库服务如文档数据库服务 DDS、云数据库 GeminiDB 等也提供不同的数据存储方案。

（5）人工智能服务

人工智能服务是华为云的另一大特色。盘古大模型打造行业大模型，重塑千行百业。AI 开发平台 ModelArts 面向 AI 开发者提供一站式开发平台。图像识别、文字识别 OCR、自然语言处理等基础 AI 服务以及智能问答机器人等预集成解决方案满足了不同用户的需求。

（6）安全与合规服务

安全与合规服务保护应用服务和云工作负载。DDoS 防护 AAD 防御大规模流量攻击，Web 应用防火墙 WAF 识别恶意请求特征并防御未知威胁。云防火墙 CFW 进行网络流量管控与入侵安全防护。数据库安全服务 DBSS、数据加密服务 DEW、云证书管理服务 CCM 等进一步保护用户的数据资产。

习题 3

一、填空题

1．计算机网络一般由三部分组成：组网计算机、（　　）、网络软件。

2．组网计算机根据其作用和功能不同，可分为（　　）和客户机两类。

3．（　　）是一种利用光在玻璃或塑料制成的纤维中的全反射原理而制成的光传导工具。

4．（　　）用于实现联网计算机和网络电缆之间的物理连接。

5．（　　）是互联网的主要节点设备，通过路由选择决定数据的转发。

6．计算机网络中常用的两种有线通信介质是（　　）和光纤。

7．（　　）从根本上改变了局域网共享介质的结构，大大提升了局域网的性能。

8．不同的网络拓扑结构对网络性能、（　　）和通信费用的影响不同。

9．WWW 上的每个网页都有一个独立的地址，这些地址称为（　　）。

10．网络层的主要协议是（　　），它是建造大规模异构网络的关键协议。

11．密码体制可分为（　　）和非对称密码体制两种类型。

12．在网络环境中，通常使用（　　）来模拟日常生活中的亲笔签名。

13．（　　）是指证实被认证对象是否属实和是否有效的一个过程。

14．云计算通过（　　）将共享资源整合形成庞大的计算与存储网络。

15．根据目前主流云计算服务商和服务商提供的服务，一般将云计算分为基础设施即服