* Apple watch: In its development, features that required longer than 10 seconds to use were scrapped in favor of shorter, more concise interactions.
* Innovation Phase : the fundamental building blocks of the Internet—packet-switching hardware, a communications protocol called TCP/ IP, and client/server computing (all described more fully later in this section)—were conceptualized and then implemented in actual hardware and software. The Internet’s original purpose was to link large mainframe computers on different college campuses. This kind of one-to-one communication between campuses was previously possible only via the telephone system or private networks owned by the large computer manufacturers
* Institutionalization Phase, from 1975 to 1995, large institutions such as the U.S. Department of Defense (DoD) and the National Science Foundation (NSF) provided funding and legitimization for the fledging Internet. Once the concepts behind the Internet had been proven in several government-supported demonstra- tion projects, the DoD contributed $1 million to further develop them into a robust military communications system. This effort created what was then called ARPANET (Advanced Research Projects Agency Network). In 1986, the NSF assumed responsi- bility for the development of a civilian Internet (then called NSFNET) and began a 10-year-long $200 million expansion
* Commercialization Phase, from 1995 to the present, the U.S. government encouraged private corporations to take over and expand the Internet backbone as well as local service beyond military installations and college campuses to the rest of the population around the world
* three extremely important concepts that are the basis for understanding the Internet: packet switching, the TCP/IP communications protocol, and client/server computing
* **Packet switching** is a method of slicing digital messages into discrete units called **packets**, sending the packets along different communication paths as they become available, and then reassembling the packets once they arrive at their destination
* A **router** is a special- purpose computer that interconnects the different computer networks that make up the Internet and routes packets along to their ultimate destination as they travel. To ensure that packets take the best available path toward their destination, routers use a computer program called a **routing algorithm**.
* TCP/IP is divided into four separate layers, with each layer handling a different aspect of the communication problem (see Figure 3.4). The Network Interface Layer is responsible for placing packets on and receiving them from the network medium, which could be a LAN (Ethernet) or Token Ring network, or other network technology. TCP/IP is independent from any local network technology and can adapt to changes at the local level. The Internet Layer is responsible for addressing, packaging, and routing messages on the Internet. The Transport Layer is responsible for providing communication with other protocols (applications) within the TCP/IP protocol suite by acknowledging and sequencing the packets to and from the applications. The Applica- tion Layer includes a variety of protocols used to provide user services or exchange data. One of the most important is the Border Gateway Protocol (BGP), which enables the exchange of routing information among different autonomous systems on the Internet. BGP uses TCP as its transport protocol. Other important protocols included in the Application layer include HyperText Transfer Protocol (HTTP), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP)
* Most people cannot remember 32-bit numbers. An IP address can be represented by a natural language convention called a **domain name**.
* A **Uniform Resource Locator (URL)**, which is the address used by a web browser to identify the location of content on the Web, also uses a domain name as part of the URL
* Client/server computing is a model of computing in which client computers are connected in a network with one or more servers, which are computers that are dedicated to performing common functions that the client computers on the network need, such as file storage, software applications, printing, and Internet access
* The U.S. National Institute of Standards and Technology (NIST) defines cloud computing as having the following essential characteristics:
  + On-demand self-service: Consumers can obtain computing capabilities such as server time or network storage as needed automatically on their own. Ubiquitous network access: Cloud resources can be accessed using standard network and Internet devices, including mobile platforms. Location-independent resource pooling: Computing resources are pooled to serve multiple users, with different virtual resources dynamically assigned accord- ing to user demand. The user generally does not know where the computing resources are located.
  + Rapid elasticity: Computing resources can be rapidly provisioned, increased, or decreased to meet changing user demand.  
    Measured service: Charges for cloud resources are based on the amount of resources actually used.
* Cloud computing consists of three basic types of services:
  + Infrastructure as a service (IaaS): Customers use processing, storage, network- ing, and other computing resources from third-party providers called cloud service providers (CSPs) to run their information systems. For example, Amazon used the spare capacity of its information technology infrastructure to develop Amazon Web Services (AWS), which offers a cloud environment for a myriad of different IT infrastructure services. See Table 3.4 for a description of the range of services that AWS offers, such as its Simple Storage Service (S3) for storing customers’ data and
  + Software as a service (SaaS): Customers use software hosted by the vendor on the vendor’s cloud infrastructure and delivered as a service over a network. Leading SaaS examples are Google Apps, which provides common business applications online, and Salesforce.com, which provides customer relationship management and related software services over the Internet. Both charge users an annual subscrip- tion fee, although Google Apps also has a pared-down free version. Users access these applications from a web browser, and the data and software are maintained
  + on the providers’ remote servers.  
    • Platform as a service (PaaS): Customers use infrastructure and programming
  + tools supported by the CSP to develop their own applications. For example, IBM offers Bluemix for software development and testing on its cloud infrastructure. Another example is Salesforce.com’s Force.com, which allows developers to build applications that are hosted on its servers as a service.
* A **public cloud** is owned and main- tained by CSPs, such as Amazon Web Services, IBM, HP, and Dell, and made available
* A **private cloud** provides similar options as a public cloud but is operated solely for the benefit of a single tenant. It might be managed by the organization or a third party and hosted either internally or externally
* a **hybrid cloud** computing model, in which they use their own infrastructure for their most essential core activities and adopt public cloud computing for less-critical systems or for additional processing capacity during peak business periods
* **Telnet** is a network protocol that also runs in TCP/IP’s Application Layer and is used to allow remote login on another computer
* **Tracert** is one of several route-tracing utilities that allow you to follow the path of a message you send from your client to a remote computer on the Internet.
* **Packet InterNet Groper (Ping)** is a utility program that allows you to check the connection between a client computer and a TCP/IP network
* **Campus/corporate area networks (CANs)** are generally local area networks operat- ing within a single organization—such as New York University or Microsoft Corpora- tion
* An **intranet** is a TCP/IP network located within a single organization for purposes of communications and information processing. Internet technologies are generally far less expensive than proprietary networks, and there is a global source of new applications that can run on intranets.
* **LIMITATIONS OF THE CURRENT INTERNET** 
  + *Bandwidth limitations*
  + *Quality of service limitations*
  + *Network architecture elimitations*
  + Wired Internet
* **Internet2®** is an advanced networking consortium of more than 450 member institu- tions including universities, corporations, government research agencies, and not-for- profit networking organizations, all working in partnership to facilitate the development, deployment, and use of revolutionary Internet technologies
* **Differentiated quality of service** (**diffserv**) is a technology that assigns levels of priority to packets based on the type of data being transmitted. Video conference packets, for example, which need to reach their destination almost instantaneously, receive much higher priority than e-mail messages
* a web browser with a graphical user interface (GUI) called **Mosaic** that made it possible to view documents on the Web graphically—using colored backgrounds, images, and even primitive animations. Mosaic was a software program that could run on any graphically based interface such as Macintosh, Windows, or Unix
* **HyperText Markup Language (HTML)** is a GML that is relatively easy to use
* **eXtensible Markup Language (XML)** takes web document formatting a giant leap forward. XML is a markup language specification developed by the W3C that is similar to HTML, but has a very different purpose. Whereas the purpose of HTML is to control the “look and feel” and display of data on the web page, XML is designed to describe data and information
* **Really Simple Syndication (RSS)** is an XML format that allows users to have digital content, including text, articles, blogs, and podcast audio files, automatically sent to their computers over the Internet
* all web servers provide some additional basic capabilities such as the following:
  + *Security services*
  + FTP
  + Search Engine
  + Data Capture
* **IP telephony** is a general term for the technologies that use **Voice over Internet Protocol (VoIP)** and the Internet’s packet-switched network to transmit voice, fax, and other forms of audio communication over the Internet
* VoIP is a disruptive technology
* Six key dimensions to e-commerce security: integrity, nonrepudiation, authenticity, confidentiality, privacy, and availability.
* **Malicious code** (sometimes referred to as “malware”) includes a variety of threats such as viruses, worms, Trojan horses, ransomware, and bots
* Some malicious code, some- times referred to as an *exploit,* is designed to take advantage of software vulnerabilities in a computer’s operating system, web browser, applications, or other software compo- nents
* **Exploit kits** are collections of exploits bundled together and rented or sold as a commercial product, often with slick user interfaces and in-depth analytics functional- ity
* One of the latest inno- vations in malicious code distribution is to embed it in the online advertising chain (known as **maladvertising**)
* A **drive-by down- load** is malware that comes with a downloaded file that a user intentionally or unin- tentionally requests. Drive-by is now one of the most common methods of infecting computers
* A **backdoor** is a feature of viruses, worms, and Trojans that allows an attacker to remotely access a compromised computer. Downadup is an example of a worm with a backdoor, while Virut, a virus that infects various file types, also includes a backdoor that can be used to download and install additional threats.
* the e-commerce security environment is further chal- lenged by **potentially unwanted programs (PUPs)** such as adware, browser para- sites, spyware, and other applications that install themselves on a computer, such as rogue security software, toolbars, and PC diagnostic tools, typically without the user’s informed consent
* **Phishing** is any deceptive, online attempt by a third party to obtain confidential information for financial gain.
* Encryption can provide four of the six key dimensions of e-com- merce security: message integrity, nonrepudiation, authentication, and confidentiality.