Chapter 5 The Networks

The relationship of sections in this chapter is shown below (Figure 5-1).

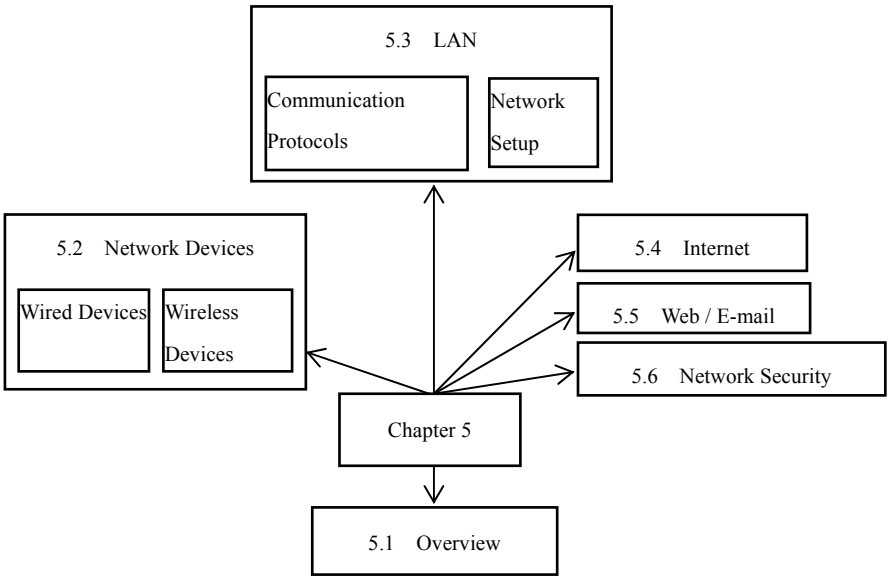


Figure 5-1 The relationship chart of Chapter Five

5.1 An Overview of the Networks

A **network** is a collection of computers and other devices that communicate to share data, hardware and software. In computer networks, networked computing devices pass data to each other along data connections. The connections (network links) between nodes are established using either cable media or wireless media. The best-known computer network is the Internet.

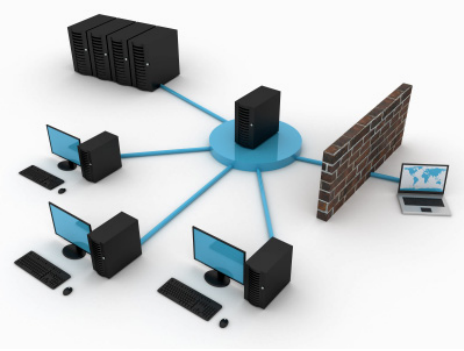


Figure 5-2 An example of Network

Network computer devices that originate, route and terminate the data are called network **nodes**. Nodes can include hosts such as personal computers,

phones, servers as well as networking hardware. Figure 5-2 shows a simple network.

5.2 Network Devices

Network devices (wired or wireless) are those components which used to connect computers or other electronic devices together so that they can share data or resources like printers or fax machines. The most common type of network devices is used to setup a Local Area Network (LAN). If you want to setup a LAN, a hub, router, cabling or radio technology, network cards are always needed.

One computer is designated as the **server**, and the others, **clients** in a network. The server and the clients are both connected to an external hub. The computers can use the hub to pass signals back and forth. The hub contains a device known as a router which is used to direct these signals. The router is the equivalent of an electronic traffic cop that handles data traffic between the nodes.

How to identity a node from one to another? The answer is that every node in the network must have a **network card** installed. These network devices each contain a unique address. In a network, data runs from network card to the hub. Figure 5-3 shows a typical network connected by network devices.

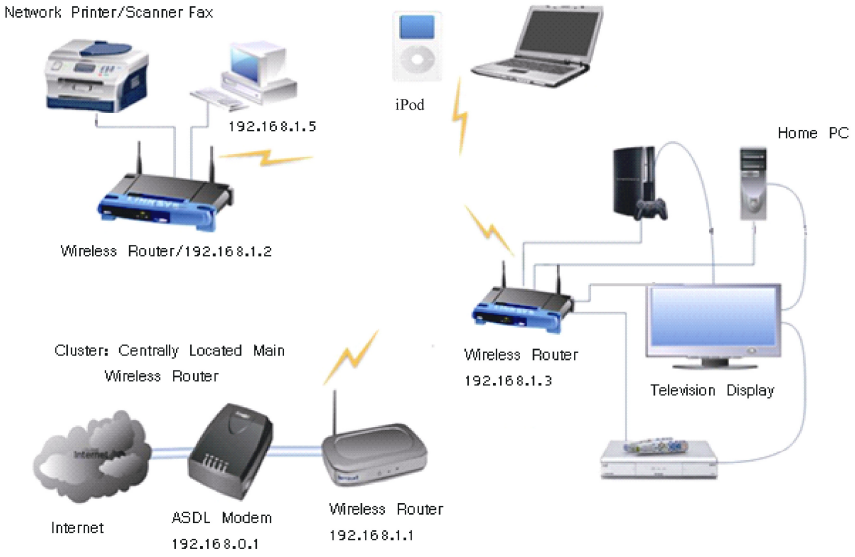


Figure 5-3 A typical Network Connected by Networks Devices

5.2.1 Wired Devices

Hub

A hub (shown in Figure 5-4) is a device for connecting multiple Ethernet devices together and

making them act as a single network segment. It has multiple input/output (I/O) ports, in which a signal introduced at the input of any port appears at the output of every port except the original incoming.

Router

A router device (shown in Figure 5-5) will forward packets from one network to another. Based on the destination network address in the incoming packet and an internal routing table, the router determines which port (line) to send the packet out (ports typically connect to Ethernet cables). Routers require packets to be formatted in a routable protocol, and the global standard routable protocol today is TCP/IP, or simply "IP".

Figure 5-4 Hub

Figure 5-5 Router

When a data packet comes in one of the lines, the router reads the address information in the packet to determine its ultimate destination. Then, using information in its routing table or routing policy, it directs the packet to the next network on its journey. Routers perform the "traffic directing" functions on the Internet. A data packet is typically forwarded from one router to another through the networks that constitute the internetwork until it reaches its destination node.

Network Cards

Figure 5-6 A Network Card

A Network interface card, **NIC**, or Network card is an electronic device that connects a computer to a computer network, usually a LAN. It is considered a piece of computer hardware shown in Figure 5-6. Today, most computers are equipped with network cards. Network cards enable a computer to exchange data with the network. To achieve the connection, network cards use a suitable protocol, for example CSMA/CD. Network cards usually implement the first two layers of the OSI model, that is the physical layer, and the data link layer. Today, most network cards use Ethernet.

Server

A network server is a system (software and suitable computer hardware) that responds to

requests across a computer network to provide, or help to provide, a network service. Servers can be run on a dedicated computer, which is also often referred to as “the server”, but many networked computers are capable of hosting servers. In many cases, a computer can provide several services and have several servers running.

Servers operate within a client-server architecture as shown in Figure 5-7. Servers are computer programs running to serve the requests of other programs, the clients. Thus, the server performs some tasks on behalf of clients. The clients typically connect to the server through the network but may run on the same computer. In the context of Internet Protocol (IP) networking, a server is a program that operates as a socket listener.

Servers often provide essential services across a network, either to private users inside a large organization or to public users via the Internet. Typical computing servers are database server, file server, mail server, print server, web server, gaming server, and application server.

Figure 5-7　Server and clients

Clients

A client is part of a client–server model, as shown in Figure 5-7, which is still used today. A client is a piece of computer hardware or software that accesses a service made available by a server. The server is often (but not always) on another computer system, in which case the client accesses the service by way of a network. The term applies to programs or devices that are part of a client–server model.

Clients and servers may be computer programs run on the same machine and connect via inter-process communication techniques. Combined with Internet sockets, programs may connect to a service operating on a possibly remote system through the Internet protocol suite. Servers wait for potential clients to initiate connections that they may accept.

5.2.2 Wireless Devices

Wireless devices are the networking devices do not require a physical wire for relaying information to another device. A networking device can pass files or resources to other wireless network gear without being physically connected.

Wireless Router

A wireless router is a device that performs the functions of a router but also includes the functions of a wireless access point. It is commonly used to provide access to the Internet or a computer network. It does not require a wired link, as the connection is made wirelessly, via radio waves. It can function in a wired LAN (local area network), in a wireless-only LAN (WLAN), or in a mixed wired/wireless network, depending on the manufacturer and model. Figure 5-8 shows a wireless router.

Wi-Fi adapters

Wireless adapters are one of those wireless network devices just like routers and come in different wireless standards. So make sure you choose an adapter that is going to perform channel bonding with your wireless router. In the last decade they have been selling mostly in the USB Wireless Adapter form factor. Figure 5-9 shows a Wi-Fi adapter.

Figure 5-8 Wireless Router

Figure 5-9 A Wi-Fi adapter

5.2.3 Transmission Media

A **transmission medium** is a material substance (solid, gas, etc) that can propagate signals to exchange data between network nodes. The transmission pattern can be wired by solid cables or wireless by air.

5.2.3.1 Cables

Networking cables are used to connect one network device to other network devices. The typical cables are twisted pairs, coaxial cables, and optical fibers.

Twisted pair wire

Twisted pair cabling is a type of wiring in which two conductors of a single circuit are twisted together for the purposes of canceling out electromagnetic interference (EMI) from external

sources; for instance, electromagnetic radiation from unshielded twisted pair (UTP) cables, and crosstalk between neighboring pairs.

Twisted pair wires are usually ended with RJ45 connector (shown in Figure 5-10) to plug into network interface card (NIC).

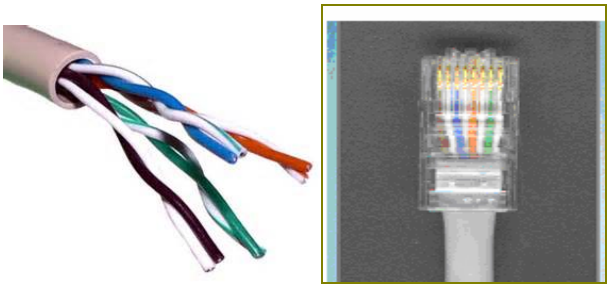


Figure 5-10 Twisted pair wire and RJ 45 connector

Coaxial cable

Coaxial cable (shown in Figure 5-11) is a type of cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield. The term coaxial comes from the inner conductor and the outer shield sharing a geometric axis. Coaxial cable differs from other shielded cable used for carrying lower-frequency signals, such as audio signals, in that the dimensions of the cable are controlled to give a precise, constant conductor spacing, which is needed for it to function efficiently as a radio frequency transmission line.

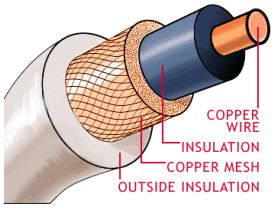


Figure 5-11 Coaxial cable

Optical Fiber

An optical fiber (or optical fiber) is a flexible, transparent fiber made of extruded glass (silica) or plastic, slightly thicker than a human hair. It can function as a waveguide, or "light pipe", to transmit light between the two ends of the fiber.

Optical fiber can be used as a medium for telecommunication and computer networking because it is flexible and can be bundled as cables. It is especially advantageous for long-distance communications, because light propagates through the fiber with little attenuation compared to electrical cables. This allows long distances to be spanned with few repeaters. Each fiber can carry many independent channels. For short distance application, fiber-optic cabling can save space in cable ducts. This is because a single fiber can carry much more data than electrical cables. Fiber is also immune to electrical interference; there is no cross-talk between signals in different cables, and no pickup of environmental noise. Non-armored fiber cables do not conduct electricity, which makes fiber a good solution for protecting communications equipment in high voltage environments, such as power generation facilities, or metal communication structures prone to lightning strikes. They can also be used in environments where explosive fumes are present, without danger of ignition. Figure 5-12 shows an optical

fiber.

5.2.3.2 Broadcast

Broadcast is used for the long distance network or the situation that cables are not practical. It uses microwaves as the communication tool.

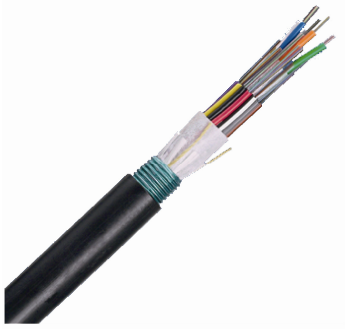


Figure 5-12 An optical fiber

Wireless

Wireless communication is the transfer of information between two or more points that are not connected by an electrical conductor.

Now almost in every public area there are Wi-Fi signals shown as Figure 5-13.The most common wireless technologies use radio. With radio waves distances can be short, such as a few meters for television or as far as thousands or even millions of kilometers for deep-space radio communications.

Microwave

Microwaves (as shown in Figure 5-14) are often used for point-to-point telecommunications. In general, setup with cell towers. 3G and 4G wireless connections are now common for smart phones but also laptops and tablets.

Figure 5-13 Wi-Fi signal logo

Figure 5-14 Microwave logo

Satellite

For fixed (point-to-point) services, communications satellites (shown in Figure 5-15) provide a microwave radio relay technology complementary to that of communication cables. They are also used for mobile applications such as communications to ships, vehicles, planes and hand-held terminals, and for TV and radio broadcasting.

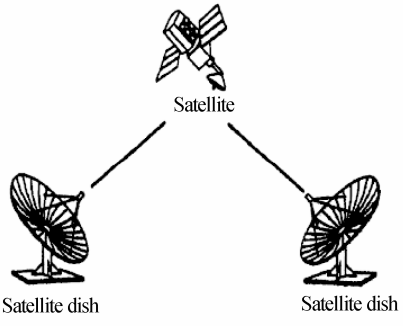


Figure 5-15 Satellite transmission

5.2.4 Network Topologies

Networks can be connected together in many ways. Device in the network, whether it's a

computer, printer, scanner, or whatever, is called a **node**. The configurations of network called network topologies usually are **star, bus** or **ring.**

Star

In the **star** pattern (shown in Figure 5-16), all devices are connected to a **host computer**, a **network switch,** or a **network hub**, which handles the network tasks. All data changing between computers go through the host/switch/hub. This configuration is used in home networks, often using a wireless hub instead of a host computer. Using a very large host computer, it is good for businesses that have large amounts of rapidly changing data, like banks and airline reservation offices.

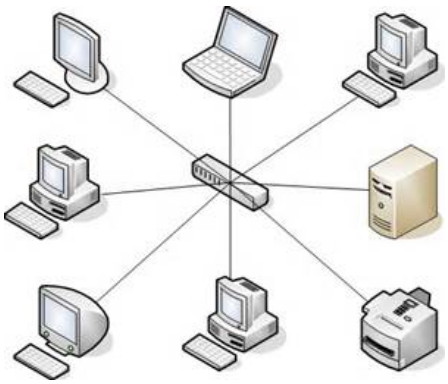


Figure 5-16 Star topology

Bus

A **bus** network is a network topology in which nodes are connected in a daisy chain by a linear sequence of buses shown in Figure 5-17. All the computers can communicate with each other directly. Using bus topology, it is easy to connect a computer or peripheral to a linear bus, requires less cable length than a star topology, and it works well for small networks.

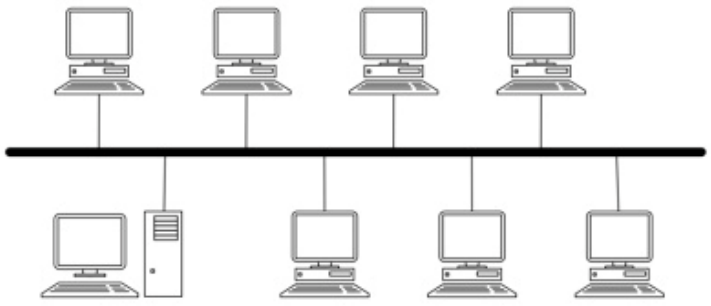


Figure 5-17 Bus topology

Ring

A **ring** network is a network topology in which each node connects to exactly two other nodes,

forming a single continuous pathway for signals through each node - a ring shown in Figure 5-18. Data travel from node to node, with each node along the way handling every packet.

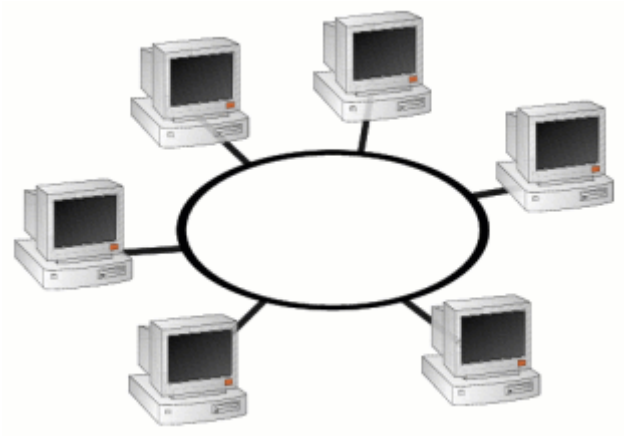


Figure 5-18 Ring topology

5.3 LAN

5.3.1 Communications Protocols

Communication protocols are formal descriptions of digital message formats and rules. They are required to exchange messages in or between computing systems and are required in telecommunications.

Communications protocols cover authentication, error detection and correction, and signaling. They can also describe the syntax, semantics, and synchronization of analog and digital communications. Communications protocols are implemented in hardware and software. There are thousands of communications protocols that are used everywhere in analog and digital communications. Computer networks cannot exist without them.

There are many properties of a transmission that a protocol can define. Common ones include: packet size, transmission speed, error correction types, handshaking and synchronization techniques, address mapping, acknowledgement processes, flow control, packet sequence controls, routing, address formatting.

What can communication protocol do

Protocols set standards for encoding and decoding data, guiding data to its destination, and mitigating the effects of interference.

- Packet switching.
- Binding address to packets.
- Initiating transmission.

- Controling the flow of data.
- Transmission errors check.
- Receipt of transmitted data acknowledgement.

How does data travel over a network

Shannon's model: data from a source is encoded and sent as signals over a communications channel to a destination. When data arrives at its destination, it is decoded. Figure 5-19 shows data travel over a network.

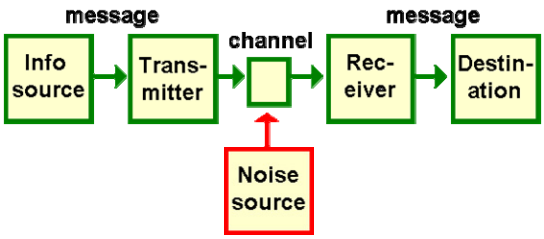


Figure 5-19 Data travel over a network

Basic conceptions of protocols

Messages are sent and received on communicating systems to establish communications. Protocols should therefore specify rules governing the transmission.

Data formats for data exchange

Digital message bit strings are exchanged. The bit strings are divided in fields and each field carries information relevant to the protocol. Conceptually the bit string is divided into two parts called the header area and the data area. The actual message is stored in the data area, so the header area contains the fields with more relevance to the protocol. Bit strings longer than the maximum transmission unit (MTU) are divided in pieces of appropriate size.

Address formats for data exchange

Addresses are used to identify both the sender and the intended receiver(s). The addresses are stored in the header area of the bit strings, allowing the receivers to determine whether the bit strings are intended for themselves and should be processed or should be ignored. A connection between a sender and a receiver can be identified using an address pair (sender address, receiver address). Usually some address values have special meanings. An all-1s address could be taken to mean an addressing of all stations on the network, so sending to this address would result in a broadcast on the local network. The rules describing the meanings of the address value are collectively called an addressing scheme.

Address mapping

Sometimes protocols need to map addresses of one scheme on addresses of another scheme. For instance, translate a logical IP address specified by the application to an Ethernet hardware

address. This is referred to as address mapping.

Routing

When systems are not directly connected, intermediary systems along the route to the intended receiver(s) need forward messages on behalf of the sender. On the Internet, the networks are connected using routers. This way of connecting networks is called internetworking.

Detection of transmission errors

Detection of transmission errors is necessary on networks which cannot guarantee error-free operation. In a common approach, CRCs of the data area are added to the end of packets, making it possible for the receiver to detect differences caused by errors. The receiver rejects the packets on CRC differences and arranges somehow for retransmission.

Connection-oriented communication

Acknowledgements of correct reception of packets are required for connection-oriented communication. Acknowledgements are sent from receivers back to their respective senders.

Loss of information - timeouts and retries

Packets may be lost on the network or suffer from long delays. To cope with this, under some protocols, a sender may expect an acknowledgement of correct reception from the receiver within a certain amount of time. On timeouts, the sender must assume the packet was not received and retransmit it. In case of a permanently broken link, the retransmission has no effect so the number of retransmissions is limited. Exceeding the retry limit is considered an error.

Media access control

Direction of information flow needs to be addressed if transmissions can only occur in one direction at a time as on half-duplex links. Arrangements have to be made to accommodate the case when two parties want to gain control at the same time.

Sequence control

We have seen that long bit strings are divided in pieces, and then sent on the network individually. The pieces may get lost or delayed or take different routes to their destination on some types of networks. As a result pieces may arrive out of sequence. Retransmissions can result in duplicate pieces. By marking the pieces with sequence information at the sender, the receiver can determine what was lost or duplicated, ask for necessary retransmissions and reassemble the original message.

Flow control

In data communications, flow control is the process of managing the rate of data transmission between two nodes to prevent a fast sender from overwhelming a slow receiver. It provides a mechanism for the receiver to control the transmission speed, so that the receiving node is not overwhelmed with data from transmitting node. Flow control should be distinguished from congestion control, which is used for controlling the flow of data when congestion has actually

occurred. Flow control mechanisms can be classified by whether or not the receiving node sends feedback to the sending node.

Electro-magnetic signals mostly

The signals of communication protocols is mostly electro-magnetic signals which looks like waves, as shown in Figure 5-20.

Figure 5-20 Electromagnetic waves

Waveform: wave pattern

Analog signal is a continuous signal which represents physical measurements (shown in Figure 5-21 (a)).

Digital signals are discrete time signals generated by digital modulation (shown in Figure 5-21 (b)).

Analog signals can be converted into digit signals which is called A/D converter.

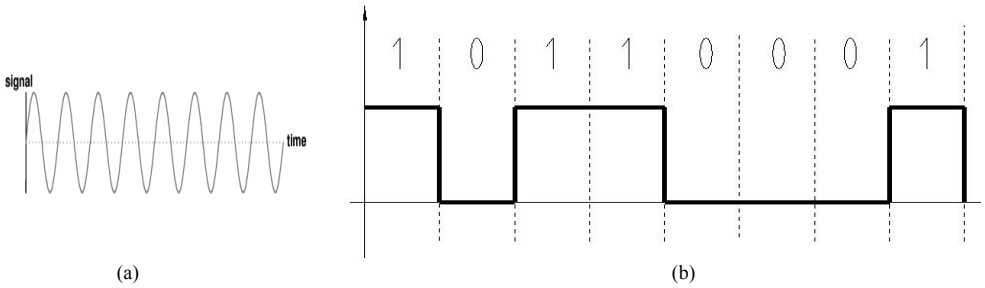


Figure 5-21 Electromagnetic wave pattern

Packet

A packet is one unit being routed through a computer network. It contains binary data including the address of its sender, the destination address, a sequence number, resource data in a packet. Figure 5-22 shows that a packet transferring in the network.

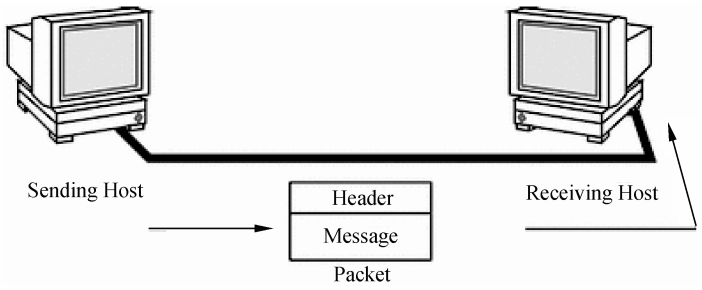


Figure 5-22 Packet in the link

Circuit switch and Packet switching technology

Circuit switched is a type of network in which a physical path is obtained for a single connection between two end-points. Ordinary voice phone service is circuit-switched. The telephone company reserves a specific physical path to the number you are calling for the duration of your call.

Packet switching technology can be concluded into 4 steps for packet switching:

- Divides a message into small unit called packet.
- Each packet in one message is addressed to the same destination, but one packet can travel a different route over the network than other packets.
- Transmit packets, gather packets, reassemble packets.
- Efficiently use available bandwidth.

Figure 5-23 shows packet switch technology and circuit switch. In circuit switching network dedicated channel has to be established before the call is made between users and the channel must be reserved between the users to make connection active. Packet switched networks are mainly used for data and voice applications not requiring real time scenarios.

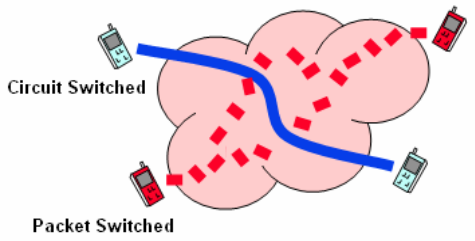


Figure 5-23 Packet switch and circuit switch

Address: MAC address and IP address

A **MAC address** (media access control address) is a unique identifier assigned to network interfaces for communications on the physical network segment. MAC addresses are used as a network address for most IEEE 802 network technologies, including Ethernet. Logically, MAC addresses are used in the media access control protocol sublayer of the OSI reference model.

MAC addresses are most often assigned by the manufacturer of a network interface controller (NIC) and are stored in its hardware, such as the card's read-only memory or some other firmware mechanism. If assigned by the manufacturer, a MAC address usually encodes the manufacturer's registered identification number and may be referred to as the burned-in address (BIA). It may also be known as an Ethernet hardware address (EHA), hardware address or physical address. This can be contrasted to a programmed address, where the host device issues commands to the NIC to use an arbitrary address.

MAC addresses are formed according to the rules of one of three numbering name spaces managed by the Institute of Electrical and Electronics Engineers (IEEE): MAC-48, EUI-48, and EUI-64. The IEEE claims trademarks on the names EUI-48 and EUI-64, in which EUI is an

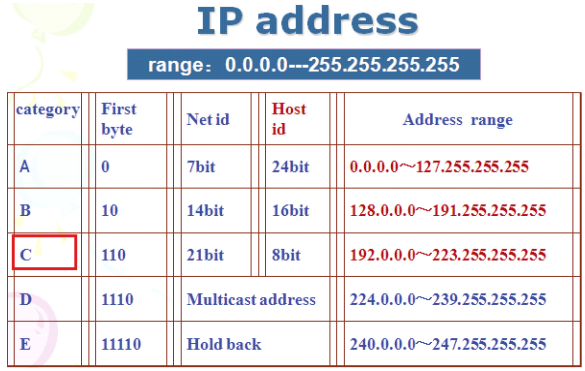
abbreviation for Extended Unique Identifier.

An Internet Protocol address (also known as an **IP address**) is a numerical label assigned to each network device participating in a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing. Its role has been characterized as follows: “A name indicates what we seek. An address indicates where it is. A route indicates how to get there”.

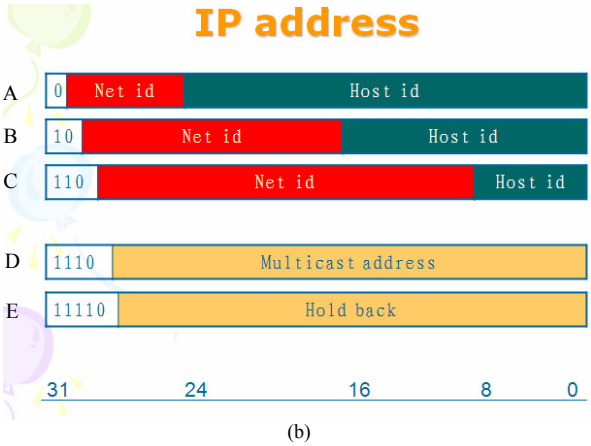
The designers of the Internet Protocol defined an IP address as a 32-bit number consisting of 4 octets and this system, known as Internet Protocol Version 4 (IPv4), is still in use today. However, due to the enormous growth of the Internet and the predicted depletion of available addresses, a new version of IP (IPv6), using 128 bits for the address, was developed in 1995. IPv6 was standardized as RFC 2460 in 1998, and its deployment has been ongoing since the mid-2000s.

IP addresses are binary numbers, but they are usually stored in text files and displayed in human-readable notations, such as 172.16.254.1 (for IPv4), and 2001:db8:0:1234:0:567:8:1 (for IPv6). An IP address consists of two parts, one identifying the network and anther identifying the node, or host.

IP address is divided into five classes ranging from 0.0.0.0 to 255.255.255.255 shown in Figure 5-24.



(a)



(b)

Figure 5-24　Category of IP address

CIDR

CIDR (Classless Inter-Domain Routing, sometimes known as supernetting) is a way to allocate and specify the Internet addresses used in inter-domain routing more flexibly than with the original system of Internet Protocol (IP) address classes. As a result, the number of available Internet addresses has been greatly increased. CIDR is now the routing system used by virtually all gateway hosts on the Internet's backbone network. The Internet's regulating authorities now expect every Internet service provider (ISP) to use it for routing.

Using CIDR, each IP address has a network prefix that identifies either an aggregation of network gateways or an individual gateway. The length of the network prefix is also specified as part of the IP address and varies depending on the number of bits that are needed (rather than any arbitrary class assignment structure). A destination IP address or route that describes many possible destinations has a shorter prefix and is said to be less specific. A longer prefix describes a destination gateway more specifically. Routers are required to use the most specific or longest network prefix in the routing table when forwarding packets.

A CIDR network address looks like this: a.b.c.d/x (shown in Figure 5-25), where x is # bits in subnet portion of address.

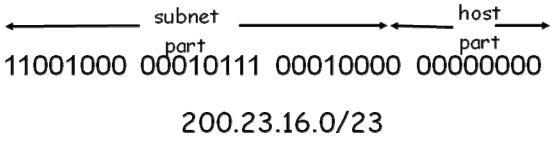


Figure 5-25 An example of CIDR IP address

Subnet

A subnetwork, or subnet, is a logically visible subdivision of an IP network. The practice of dividing a network into two or more networks is called subnetting.

All computers that belong to a subnet are addressed with a common, identical, most-significant bit-group in their IP address. This results in the logical division of an IP address into two fields, a network or routing prefix and the rest field or host identifier. The rest field is an identifier for a specific host or network interface.

The routing prefix is expressed in CIDR notation. It is written as the first address of a network, followed by a slash character (/), and ending with the bit-length of the prefix. For example, 192.168.1.0/24 is the prefix of the Internet Protocol Version 4 network starting at the given address, having 24 bits allocated for the network prefix, and the remaining 8 bits reserved for host addressing.

In IPv4 the routing prefix is also specified in the form of the subnet mask, which is expressed in quad-dotted decimal representation like an address. For example, 255.255.255.0 is the network mask for the 192.168.1.0/24 prefix. Traffic between subnetworks is exchanged or routed with special gateways called routers which constitute the logical or physical boundaries between the subnets. Valid subnet masks for Class A subnets are listed in Table 5-1.

Table 5-1 Valid subnet masks for Class A subnets

Subnet Mask	Networking Bits	Number of Subnets	Number of Hosts per Subnet
255.255.255.252	/30	4,194,304	2
255.255.255.248	/29	2,097,152	6
255.255.255.240	/28	1,048,576	14
255.255.255.224	/27	524,288	30
255.255.255.192	/26	262,144	62
255.255.255.128	/25	131,072	126
255.255.255.0	/24	65,536	254
255.255.254.0	/23	32,768	510
255.255.252.0	/22	16,384	1022
255.255.248.0	/21	8192	2046
255.255.240.0	/20	4096	4094
255.255.224.0	/19	2048	8190
255.255.192.0	/18	1024	16,382
255.255.128.0	/17	512	32,766
255.255.0.0	/16	256	65,534
255.254.0.0	/15	128	131,070
255.252.0.0	/14	64	262,142
255.248.0.0	/13	32	524,286
255.240.0.0	/12	16	1,048,574
255.224.0.0	/11	8	2,097,150
255.192.0.0	/10	4	4,194,302
255.128.0.0	/9	2	8,388,606
255.0.0.0	/8	1	16,777,216

DHCP

DHCP (also known as Dynamic Host Configuration Protocol) is a protocol that assigns unique IP addresses to devices, then releases and renews these addresses as devices leave and re-join the network.

Internet service providers usually use DHCP to help customers join their networks easily. And, home network equipment like broadband routers offers DHCP support for added convenience in joining home computers to LANs.

DHCP server should be set up with the appropriate configuration parameters for the given network. Key DHCP parameters include the range or “pool” of available IP addresses, the correct subnet masks, plus network gateway and name server addresses.

The common Operating systems make DHCP clients as a built-in component. Using System administrators do not need to configure these parameters individually for each client device.

5.3.2 Network Setup

Ethernet setup

A local area network (LAN) is an excellent way for a group of computers in a home or an office

to share resources and a common Internet connection. With the high speed of Ethernet technology and modern plug-and-play (PnP) networking, setting up an Ethernet LAN can be a quick and simple task.

Firstly, set up the router, hub or switch. plug the network device into an electrical outlet. If the device allows computers to access the Internet, connect an Ethernet cable between the network device's port and the broadband modem.

Connect an Ethernet cable between computers and the network device. Each end of an Ethernet cable has a plastic modular plug (known to technophiles as an RJ-45 plug shown in Figure 5-10).

Turn on the computer and allow them to fully boot up. If they were already on, acknowledge any networking messages that may have appeared on the screen.

Complete the network setup on the computer. Most modern computers use plug-and-play technology to automatically configure a network connection when an Ethernet connection is present. On a computer running Microsoft Windows, right click on the "My Network" desktop icon, select the TCP/IP adapter, click on "Properties," select "IP Address" click on "Obtain an IP address automatically" and click "OK." If you are using an Apple Macintosh computer, click the Apple logo, select "System Preferences," click on "Network," select the "Ethernet adapter" in the list on the left, click "Advanced" then "TCP/IP" and select "Using DHCP" from the drop list. After performing these steps on computers, the machine should be connected to the LAN via Ethernet to complete the LAN setup.

Wireless network setup

Want to get online without needing to plug in an Ethernet cable! Please setup A wireless network. A wireless router is needed before we get started building the network.

As follow steps:

Connect your modem to the wireless router using an Ethernet cable. This moves the internet connection from your modem to the wireless router. Then, plug your PC into the back of the router using the Ethernet jacks. We'll need this connection to configure the Wi-Fi network.

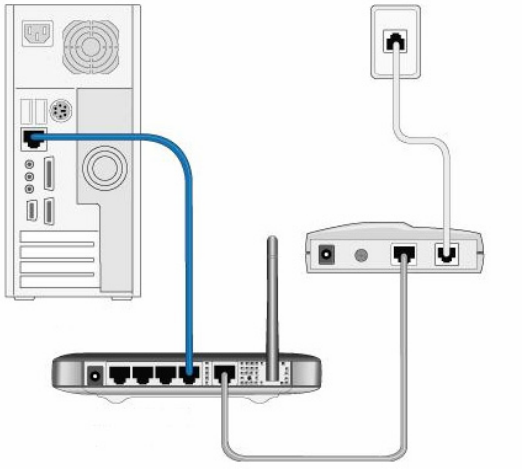


Figure 5-26 Wireless network setup

Turn on the modem, the wireless router and the computer. Read the documentation that came with your wireless router for the default IP address used by the device. Launch your computer's Web browser and head to IP address of the router.

You should see a login window requiring a username and password. The default values should be in your router's documentation.

Once you've logged in, you'll see your router's settings page. The first step is make sure you change the default admin password so other users won't be able to login to the settings page and reconfiguring the router. Check the product description of wireless router, and learn how to configure the SSID and encryption.

Once you're happy with your settings, disconnect your PC and then head to your network settings tool and you should see your new Wi-Fi network listed under available networks. Select your network and type in your password (if you're using one) to connect. Figure 5-26 shows the wireless network setup.

5.4 Internet

5.4.1 Internet Basics

What is the Internet

The Internet is a worldwide telecommunications system that provides connectivity for millions of other, smaller networks; therefore, the Internet is often referred to as a network of networks. It allows computer users to communicate with each other across distance and computer platforms.

The Internet began in 1969 as the U.S. Department of Defense's Advanced Research Project Agency (ARPA) to provide immediate communication within the Department in case of war. Computers were then installed at U.S. universities with defense related projects. As scholars began to go online, this network was changed from military use to scientific use. As ARPAnet grew, administration of the system became distributed to a number of organizations, including the National Science Foundation (NSF). This shift of responsibility began the transformation of the science oriented ARPAnet into the commercially minded and funded Internet used by millions today.

The Internet acts as a pipeline to transport electronic messages from one network to another network. At the heart of most networks is a server, a fast computer with large amounts of memory and storage space. The server controls the communication of information between the devices attached to a network, such as computers, printers, or other servers.

Network service provider

A network service provider (NSP) is a business entity that provides or sells services such as network access and bandwidth by allowing access into its backbone infrastructure or access to its network access points (NAP), which consequently also means access to the Internet. Network

service providers are very similar to or can even be considered the same as Internet service providers (ISPs), but in most cases they are the ones providing backbone services to the ISPs.

Network access points

A network access point (NAP) is a major point where internet service providers (ISPs) can connect with one another in peering arrangements. NAPs were central in the early days of the Internet when it was making the transition from a government-funded network to a commercial one.

Internet service provider

An ISP (Internet service provider) is a company that provides individuals and other companies access to the Internet and other related services such as Web site building and virtual hosting. An ISP has the equipment and the telecommunication line access required to have a point-of-presence on the Internet for the geographic area served. The larger ISPs have their own high-speed leased lines so that they are less dependent on the telecommunication providers and can provide better service to their customers. Figure 5-27 shows the service of Cisco Company in broadband.

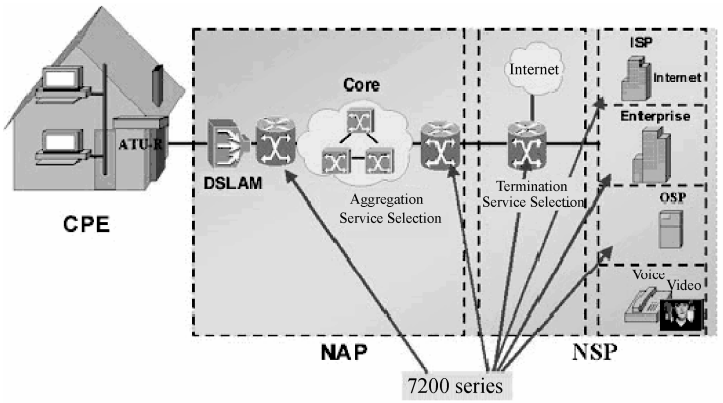


Figure 5-27 Internet service provider (Cisco Company)

Internet protocol

Internet protocols are a standard set of communication rules such as that shown in Table 5-2.

Table 5-2 A list of protocols

Protocol	Name	Function
TCP	Transmission Control Protocol	Creates connections and exchanges packets of data
IP	Internet Protocol	Provides devices with unique addresses
UDP	User Datagram Protocol	An alternative data transport to TCP used for DNS，Voice over IP，and file sharing
HTTP	Hypertext Transfer Protocol	Exchanges information over the Web
FTP	File Transfer Protocol	Transfers files between local and remote host computers

continued

Protocol	Name	Function
POP	Post Office Protocol	Transfers mail from an E-mail server to a client Inbox
SMTP	Simple Mail Transfer Protocol	Transfers E-mail messages from client computers to an E-mail server
VoIP	Voice over Internet Protocol	Transmits voice conversations over the Internet
IRC	Internet Relay Chat	Transmits text messages in real time between online users
BitTorrent	BitTorrent	Distributes files using scattered clients rather than a server

TCP/IP

TCP/IP (Transmission Control Protocol/Internet Protocol) is the basic communication language or protocol of the Internet. It can also be used as a communications protocol in a private network (either an intranet or an extranet). When you are set up with direct access to the Internet, your computer is provided with a copy of the TCP/IP program just as every other computer that you may send messages to or get information from also has a copy of TCP/IP.

TCP/IP is a two-layer program. The higher layer, Transmission Control Protocol, manages the assembling of a message or file into smaller packets that are transmitted over the Internet and received by a TCP layer that reassembles the packets into the original message. The lower layer, Internet Protocol, handles the address part of each packet so that it gets to the right destination. Each gateway computer on the network checks this address to see where to forward the message. Even though some packets from the same message are routed differently than others, they'll be reassembled at the destination.

TCP/IP uses the client/server model of communication in which a computer user (a client) requests and is provided a service (such as sending a Web page) by another computer (a server) in the network. TCP/IP communication is primarily point-to-point, meaning each communication is from one point (or host computer) in the network to another point or host computer. TCP/IP and the higher-level applications that use it are collectively said to be "stateless" because each client request is considered a new request unrelated to any previous one (unlike ordinary phone conversations that require a dedicated connection for the call duration). Being stateless frees network paths so that everyone can use them continuously. (Note that the TCP layer itself is not stateless as far as any one message is concerned. Its connection remains in place until all packets in a message have been received.)

UDP

The User Datagram Protocol (UDP) is one of the core members of the Internet protocol suite (the set of network protocols used for the Internet). With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network without prior communications to set up special transmission channels or data paths. The protocol was designed by David P. Reed in 1980 and formally defined in RFC 768.

UDP uses a simple transmission model with a minimum of protocol mechanism.[1] It has no handshaking dialogues, and thus exposes any unreliability of the underlying network protocol

to the user's program. As this is normally IP over unreliable media, there is no guarantee of delivery, ordering, or duplicate protection. UDP provides checksums for data integrity, and port numbers for addressing different functions at the source and destination of the datagram.

UDP is suitable for purposes where error checking and correction is either not necessary or performed in the application, avoiding the overhead of such processing at the network interface level. Time-sensitive applications often use UDP because dropping packets is preferable to waiting for delayed packets, which may not be an option in a real-time system.

HTTP

HTTP (Hypertext Transfer Protocol) is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. As soon as a Web user opens their Web browser, the user is indirectly making use of HTTP. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols (the foundation protocols for the Internet).

HTTP concepts include (as the Hypertext part of the name implies) the idea that files can contain references to other files whose selection will elicit additional transfer requests. Any Web server machine contains, in addition to the Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. Your Web browser is an HTTP client, sending requests to server machines. When the browser user enters file requests by either "opening" a Web file (typing in a Uniform Resource Locator or URL) or clicking on a hypertext link, the browser builds an HTTP request and sends it to the Internet Protocol address (IP address) indicated by the URL. The HTTP daemon in the destination server machine receives the request and sends back the requested file or files associated with the request. (A Web page often consists of more than one file.)

FTP

File Transfer Protocol (FTP) is a standard Internet protocol for transmitting files between computers on the Internet. Like the Hypertext Transfer Protocol (HTTP), which transfers displayable Web pages and related files, and the Simple Mail Transfer Protocol (SMTP), which transfers E-mail, FTP is an application protocol that uses the Internet's TCP/IP protocols. FTP is commonly used to transfer Web page files from their creator to the computer that acts as their server for everyone on the Internet. It's also commonly used to download programs and other files to your computer from other servers.

As a user, you can use FTP with a simple command line interface (for example, from the Windows MS-DOS Prompt window) or with a commercial program that offers a graphical user interface. Your Web browser can also make FTP requests to download programs you select from a Web page. Using FTP, you can also update (delete, rename, move, and copy) files at a server. You need to logon to an FTP server. However, publicly available files are easily accessed using anonymous FTP.

POP3

POP3 (Post Office Protocol 3) is the most recent version of a standard protocol for receiving E-mail. POP3 is a client/server protocol in which E-mail is received and held for you by your

Internet server. Periodically, you (or your client E-mail receiver) check your mail-box on the server and download any mail, probably using POP3. This standard protocol is built into most popular E-mail products, such as Eudora and Outlook Express. It's also built into the Netscape and Microsoft Internet Explorer browsers.

POP3 is designed to delete mail on the server as soon as the user has downloaded it. However, some implementations allow users or an administrator to specify that mail be saved for some period of time. POP can be thought of as a "store-and-forward" service.

SMTP

SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving E-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 or IMAP, that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending E-mail and either POP3 or IMAP for receiving E-mail. On Unix-based systems, sendmail is the most widely-used SMTP server for E-mail. A commercial package, Sendmail, includes a POP3 server. Microsoft Exchange includes an SMTP server and can also be set up to include POP3 support.

BitTorrent

BitTorrent is a protocol supporting the practice of peer-to-peer file sharing that is used to distribute large amounts of data over the Internet. BitTorrent is one of the most common protocols for transferring large files, and peer-to-peer networks have been estimated to collectively account for approximately 43% to 70% of all Internet traffic (depending on geographical location) as of February 2009. As of February 2013, BitTorrent was responsible for 3.35% of all worldwide bandwidth, more than half of the 6% of total bandwidth dedicated to file sharing.

Domain

Domain names are used in various networking contexts and application-specific naming and addressing purposes. In general, a domain name represents an Internet Protocol (IP) resource, such as a personal computer used to access the Internet, a server computer hosting a web site, or the web site itself or any other service communicated via the Internet. In 2010, the number of active domains reached 196 million. Figure 5-28 shows the domain name in Cisco Company.

DNS

The Domain Name System (DNS) is a hierarchical distributed naming system for computers, services, or any resource connected to the Internet or a private network. It associates information from domain names with each of the assigned entities. Most prominently, it translates easily memorized domain names to the numerical IP addresses needed for locating computer services and devices worldwide. The Domain Name System is an essential component of the functionality of the Internet. This article presents a functional description of the Domain Name

System. Broader usage and industry aspects are captured on the Domain name page.

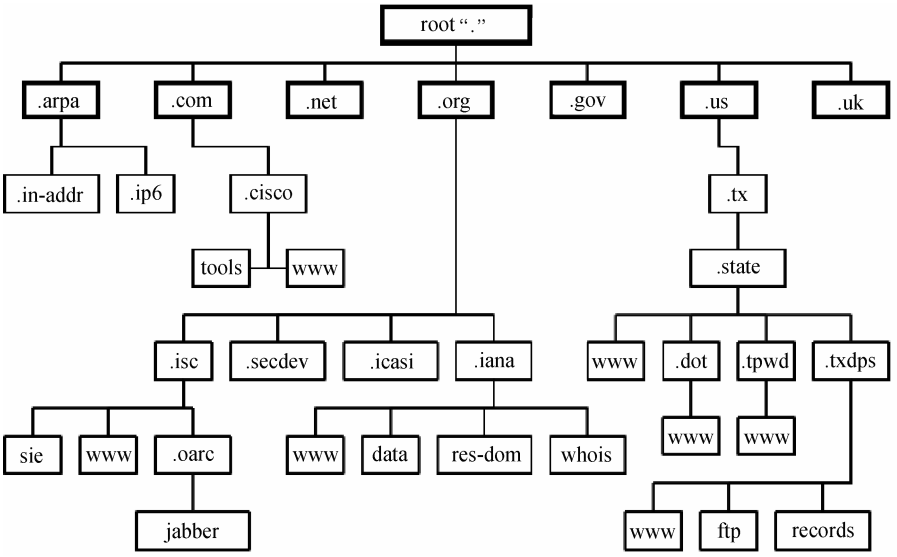


Figure 5-28 Domain name

The Domain Name System distributes the responsibility of assigning domain names and mapping those names to IP addresses by designating authoritative name servers for each domain. Authoritative name servers are assigned to be responsible for their supported domains, and may delegate authority over subdomains to other name servers. This mechanism provides distributed and fault tolerant service and was designed to avoid the need for a single central database.

The Domain Name System also specifies the technical functionality of this database service. It defines the DNS protocol, a detailed specification of the data structures and data communication exchanges used in DNS, as part of the Internet Protocol Suite. Here shows DNS in Figure 5-29.

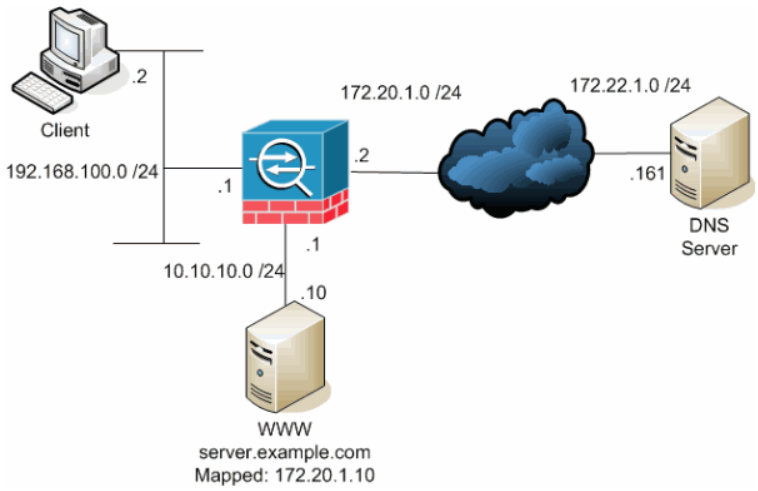


Figure 5-29 DNS

5.4.2 Internet Access

Internet access connects individual computer terminals, computers, mobile devices, and computer networks to the Internet, enabling users to access Internet services, such as email and the World Wide Web. Internet service providers (ISPs) offer Internet access through various technologies that offer a wide range of data signalling rates (speeds).

Dial-up Internet access

Dial-up Internet access is a form of Internet access that uses the facilities of the public switched telephone network (PSTN) to establish a dialed connection to an Internet service provider (ISP) via telephone lines. The user's computer or router uses an attached modem to encode and decode Internet Protocol packets and control information into and from analogue audio frequency signals, respectively. Dial-up internet is sometimes used where Broadband internet access is not available; primarily in rural or remote areas.

DSL, ISDN, and Dedicated Lines

Digital subscriber line (DSL, originally digital subscriber loop) is a family of technologies that provide Internet access by transmitting digital data over the wires of a local telephone network. In telecommunications marketing, the term DSL is widely understood to mean asymmetric digital subscriber line (ADSL), the most commonly installed DSL technology. DSL service is delivered simultaneously with wired telephone service on the same telephone line. This is possible because DSL uses higher frequency bands for data. On the customer premises, a DSL filter on each non-DSL outlet blocks any high frequency interference, to enable simultaneous use of the voice and DSL services.

The bit rate of consumer DSL services typically ranges from 256 Kbit/s to over 100 Mbit/s in the direction to the customer (downstream), depending on DSL technology, line conditions, and service-level implementation. Bit rates of 1 Gbit/s have been reached in trials. In ADSL, the data throughput in the upstream direction, (the direction to the service provider) is lower, hence the designation of asymmetric service. In symmetric digital subscriber line (SDSL) services, the downstream and upstream data rates are equal.

ISDN (Integrated Services Digital Network) is a set of CCITT/ITU standards for digital transmission over ordinary telephone copper wire as well as over other media. Home and business users who install an ISDN adapter (in place of a telephone modem) receive Web pages at up to 128 Kbps compared with the maximum 56 Kbps rate of a modem connection. ISDN requires adapters at both ends of the transmission so your access provider also needs an ISDN adapter. ISDN is generally available from your phone company in most urban areas in the United States and Europe. In many areas where DSL and cable modem service are now offered, ISDN is no longer as popular an option as it was formerly.

There are two levels of service: the Basic Rate Interface (BRI), intended for the home and small enterprise, and the Primary Rate Interface (PRI), for larger users. Both rates include a

number of B-channels and a D-channels. Each B-channel carries data, voice, and other services. Each D-channel carries control and signaling information.

The Basic Rate Interface consists of two 64 Kbps B-channels and one 16 Kbps D- channel. Thus, a Basic Rate user can have up to 128 Kbps service. The Primary Rate consists of 23 B-channels and one 64 Kbps D-channel in the United States or 30 B-channels and 1 D-channel in Europe.

ISDN in concept is the integration of both analog or voice data together with digital data over the same network. Although the ISDN you can install is integrating these on a medium designed for analog transmission, broadband ISDN (BISDN) is intended to extend the integration of both services throughout the rest of the end-to-end path using fiber optic and radio media. Broadband ISDN encompasses frame relay service for high-speed data that can be sent in large bursts, the Fiber Distributed-Data Interface (FDDI), and the Synchronous Optical Network (SONET). BISDN is intended to support transmission from 2 Mbps up to much higher, but as yet unspecified, rates.

In computer networks and telecommunications, a **dedicated line** is a communications cable or other facility dedicated to a specific application, in contrast with a shared resource such as the telephone network or the Internet.

In practice, such services may not be provided by a single, discrete, end-to-end cable, but they do provide guarantees of constant bandwidth availability and near-constant latency, properties that cannot be guaranteed for more public systems. Such properties add a considerable premium to the price charged.

Cable Internet service

In telecommunications, cable Internet access, shortened to cable Internet is a form of broadband Internet access that uses the cable television infrastructure. Like digital subscriber line and fiber to the premises services, cable Internet access provides network edge connectivity (last mile access) from the Internet service provider to an end user. It is integrated into the cable television infrastructure analogously to DSL which uses the existing telephone network. Cable TV networks and telecommunications networks are the two predominant forms of residential Internet access. Recently, both have seen increased competition from fiber deployments, wireless, and mobile networks.

Cable Modems

Similar in function with DSL modems, these electronic devices translate signals from your network servers to signals which your computer can understand. The main difference between a DSL modem and a Cable modem is what type of cable connects with them. For Cable Internet subscribers a coaxial cable similar to that for your cable TV subscription is connected directly to your modem.

Cable Internet connections are always on. This means that subscribers have a steady and available access to the internet. Upon visual inspection of cable modems, a series of lights are

noticed on the modem. These lights provide instant information regarding the status of your connection. Trouble shooting your cable connection is made simpler by information provided by these lights.

Cable

The quality of cables used plays a major role in determining the speed of your internet connection. High end cables which offer bigger bandwidths for signals are the most ideal to use. These are quite expensive and supplying them to every customer is too costly. Cable Internet providers utilize standard cables thus the true potential of Cable Internet speed is not reached.

Network Providers sometimes put a cap on how much bandwidth a customer gets. This is to provide equal surfing experience for all their customers. Signal loss through cable is also minimal, even allowing customers farthest from the company's central office to enjoy the same speeds to subscribers located near their offices.

DSL connection speeds are limited by customers distance from the central office. This however does not hold true for Cable Internet subscribers. Cable Internet subscribers are offered 1.5 Mbps as standard connection speeds. The main reason behind this is the limited bandwidths offered by network providers. Online experience through Cable Internet varies from time to time. The number of subscribers who are currently online eats a lot of the cables bandwidth thus speed is significantly decreased.

Cable Routers are electronic devices which you directly connect to your cable modem. These allow multiple computers to access the internet with just a single internet subscription. This is a very cost-effective option for subscribers who want to needs more than one computer connection.

Cable Internet or TV providers supplies signals through cables which run from their central office to your home. Like the different channels you see in your TV, internet signals are given a specific bandwidth. Cables containing these signals finally reach you home and the terminal end of the cable is attached to a cable modem. The cable modem separates the internet from TV signals. Cable modems also act as a modulator translating signals from the cable provider to those which your computer can understand. A standard way for your computer to communicate or connect with your modem is by the use of an Ethernet cable. This cable is inserted to the computers Ethernet port where the signal finally reaches your PC. Figure 5-30 shows a cable internet.

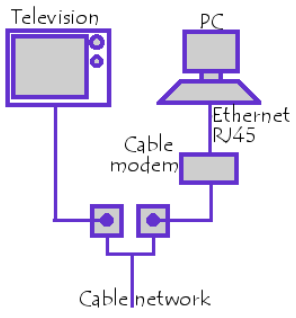


Figure 5-30　Cable Internet

Satellite Internet service

A satellite Internet connection is an arrangement in which the upstream (outgoing) and the downstream (incoming) data are sent from, and arrive at, a computer through a satellite. Each subscriber's hardware includes a satellite dish antenna and a transceiver (transmitter/receiver) that operates in the microwave portion of the radio spectrum.

In a two-way satellite Internet connection, the upstream data is usually sent at a slower speed than the downstream data arrives. Thus, the connection is asymmetric. A dish antenna, measuring about two feet high by three feet wide by three feet deep, transmits and receives signals. Uplink speeds are nominally 50 to 150 Kbps for a subscriber using a single computer. The downlink occurs at speeds ranging from about 150 Kbps to more than 1200 Kbps, depending on factors such as Internet traffic, the capacity of the server, and the sizes of downloaded files.

Satellite Internet systems are an excellent, although rather pricey, option for people in rural areas where Digital Subscriber Line (DSL) and cable modem connections are not available. A satellite installation can be used even where the most basic utilities are lacking, if there is a generator or battery power supply that can produce enough electricity to run a desktop computer system. The two-way satellite Internet option offers an always-on connection that bypasses the dial-up process. In this respect, the satellite system resembles a cable modem Internet connection. But this asset can also be a liability, unless a firewall is used to protect the computer against hack attempts.

The nature of the satellite connection is good for Web browsing and for downloading of files. Because of long latency compared with purely land-based systems, interactive applications such as online gaming are not compatible with satellite networks. In a two-way geostationary-satellite Internet connection, a transaction requires two round trips between the earth's surface and transponders orbiting 22,300 miles above the equator. This occurs in addition to land-based data transfer between the earthbound satellite system hub and the accessed Internet sites. The speed in such a connection is theoretically at least 0.48 second (the time it takes an electromagnetic signal to make two round trips at 186,000 miles per second to and from a geostationary satellite), and in practice is somewhat longer. Satellite systems are also prone to rain fade (degradation during heavy precipitation) and occasional brief periods of solar interference in mid-March and late September, when the sun lines up with the satellite for a few minutes each day. Rain fade and solar interference affect all satellite links from time to time, not just Internet systems. Figure 5-31 shows the satellite internet.

Fixed wireless service

Fixed wireless refers to the operation of wireless devices or systems in fixed locations such as homes and offices. Fixed wireless devices usually derive their electrical power from the utility mains, unlike mobile wireless or portable wireless which tend to be battery-powered. Although mobile and portable systems can be used in fixed locations, efficiency and bandwidth are

compromised compared with fixed systems. Mobile or portable, battery-powered wireless systems can serve as emergency backups for fixed systems in case of a power blackout or natural disaster.

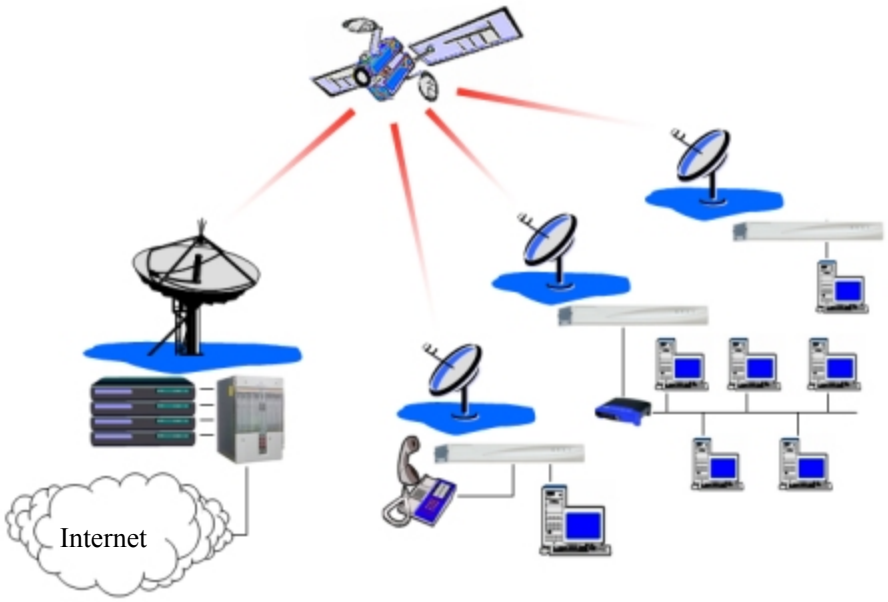


Figure 5-31　Satellite Internet service

The technology for wireless connection to the Internet is as old as the Net itself. Amateur radio operators began “patching” into telephone lines with fixed, mobile, and portable two-way voice radios in the middle of the 20th Century. A wireless modem works something like an amateur-radio “phone patch,” except faster. High-end fixed wireless employs broadband modems that bypass the telephone system and offer Internet access hundreds of times faster than twisted-pair hard-wired connections or cell-phone modems.

Portable and Mobile Internet Access

Portable internet access usually refers to the connection of a electronic device to a wireless network (usually Wi-Fi). This can be at a Wi-Fi hotspot (publically available Wi-Fi networks) or in a home Wi-Fi network. Many devices can connect to Wi-Fi. These include phones, laptops, portable gaming consoles and iPods.

A **hotspot** is a site that offers Internet access over a wireless local area network (WLAN) through the use of a router connected to a link to an Internet service provider. Hotspots typically use Wi-Fi technology.

The public can use a laptop or other suitable portable device to access the wireless connection (usually Wi-Fi) provided. Of the estimated 150 million laptops, 14 million PDAs, and other emerging Wi-Fi devices sold per year for the last few years, most include the Wi-Fi feature.

For venues that have broadband Internet access, offering wireless access is as simple as

configuring one access point (AP), in conjunction with a router and connecting the AP to the Internet connection. A single wireless router combining these functions may suffice. Figure 5-32 shows the portable and mobile internet access.

Figure 5-32 Portable and Mobile Internet Access

5.4.3 Internet Services

Real-Time Messaging

A real-time messaging system is a network-based product allows people to exchange short messages through Internet. Figure 5-33 shows some logos for real time messaging applications.

Figure 5-33 Real-Time Messaging

Voice over IP

VoIP is a technology that allows people to call each other over computer networks like the Internet. VoIP supports real-time, two-way transmission of conversations using Internet Protocol (IP).

A VoIP service provider and standard computer audio component can be used to make VoIP calls. Figure 5-34 shows a structure of VoIP.

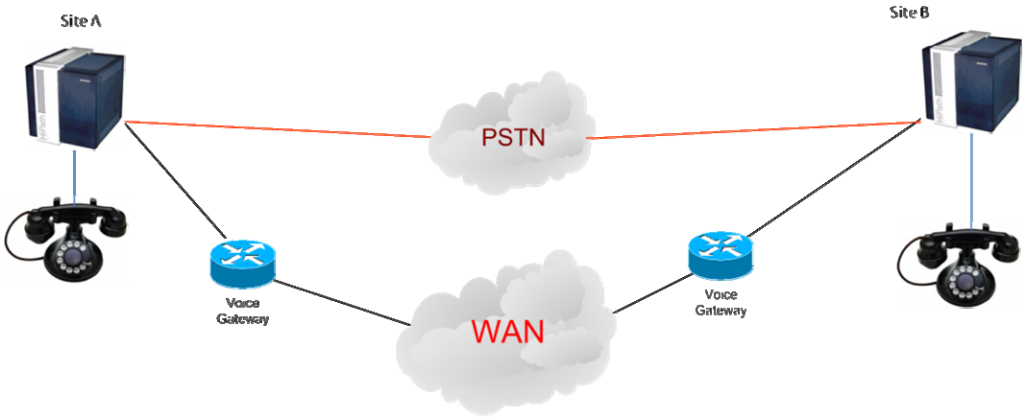


Figure 5-34　Structure of VoIP

Grid computing

Grid computing (or the use of a computational grid) is applying the resources of many computers in a network to a single problem at the same time—usually to a scientific or technical problem that requires a great number of computer processing cycles or access to large amounts of data.

Grid computing requires the use of software that can divide and farm out pieces of a program to as many as several thousand computers. Grid computing can be thought of as distributed and large-scale cluster computing and as a form of network-distributed parallel processing. It can be confined to the network of computer workstations within a corporation or it can be a public collaboration (in which case it is also sometimes known as a form of peer-to-peer computing).

A number of corporations, professional groups, university consortiums, and other groups have developed or are developing frameworks and software for managing grid computing projects. The European Community (EU) is sponsoring a project for a grid for high-energy physics, earth observation, and biology applications. In the United States, the National Technology Grid is prototyping a computational grid for infrastructure and an access grid for people. Sun Microsystems offers Grid Engine software. Described as a distributed resource management (DRM) tool, Grid Engine allows engineers at companies like Sony and Synopsys to pool the computer cycles on up to 80 workstations at a time. (At this scale, grid computing can be seen as a more extreme case of load balancing.)

Grid computing appears to be a promising trend for three reasons: (1) its ability to make more cost-effective use of a given amount of computer resources, (2) as a way to solve problems that can’t be approached without an enormous amount of computing power, and (3) because it suggests that the resources of many computers can be cooperatively and perhaps synergistically harnessed and managed as a collaboration toward a common objective. In some grid computing systems, the computers may collaborate rather than being directed by one managing computer. One likely area for the use of grid computing will be pervasive computing applications - those in

which computers pervade our environment without our necessary awareness.

For the segmentation of the grid computing market, two perspectives need to be considered: the provider side and the user side.

Cloud computing

Cloud computing is a general term for anything that involves delivering hosted services over the Internet. These services are broadly divided into three categories: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service (SaaS). The name cloud computing was inspired by the cloud symbol that's often used to represent the Internet in flowcharts and diagrams.

A cloud service has three distinct characteristics that differentiate it from traditional hosting. It is sold on demand, typically by the minute or the hour; it is elastic -- which means that a user can have as much or as little of a service as they want at any given time; and the service is fully managed by the provider (the consumer needs nothing but a personal computer and Internet access). Significant innovations in virtualization and distributed computing, as well as improved access to high-speed Internet and a weak economy, have accelerated interest in cloud computing.

A cloud can be private or public. A public cloud sells services to anyone on the Internet. (Currently, Amazon Web Services is the largest public cloud provider.) A private cloud is a proprietary network or a data center that supplies hosted services to a limited number of people. When a service provider uses public cloud resources to create their private cloud, the result is called a virtual private cloud. Private or public, the goal of cloud computing is to provide easy, scalable access to computing resources and IT services.

Infrastructure-as-a-Service like Amazon Web Services provides the customer with virtual server instances and storage, as well as application program interfaces (APIs) that allow the customer to start, stop, access and configure their virtual servers and storage. This model allows a company to pay for only as much capacity as is needed, and bring more online as soon as required. Because this pay-for-what-you-use model resembles the way electricity, fuel and water are consumed, it's sometimes referred to as utility computing.

Platform-as-a-service in the cloud is defined as a set of software development tools hosted on the provider's infrastructure. Developers create applications on the provider's platform over the Internet. PaaS providers may use APIs, website portals or gateway software installed on the customer's computer. Force.com, (an outgrowth of Salesforce.com) and Google Apps are examples of PaaS. Developers need to know that currently, there are not standards for interoperability or data portability in the cloud. Some providers will not allow software created by their customers to be moved off the provider's platform.

In the software-as-a-service cloud model, the vendor supplies the hardware infrastructure, the software product and interacts with the user through a front-end portal. SaaS is a very broad market. Services can be anything from Web-based E-mail to inventory control and database processing. Because the service provider hosts both the application and the data, the end user is

free to use the service from anywhere.

FTP

File Transfer Protocol (FTP) is a standard Internet protocol for transmitting files between computers on the Internet. Like the Hypertext Transfer Protocol (HTTP), which transfers displayable Web pages and related files, and the Simple Mail Transfer Protocol (SMTP), which transfers e-mail, FTP is an application protocol that uses the Internet's TCP/IP protocols. FTP is commonly used to transfer Web page files from their creator to the computer that acts as their server for everyone on the Internet. It's also commonly used to download programs and other files to your computer from other servers.

As a user, you can use FTP with a simple command line interface (for example, from the Windows MS-DOS Prompt window) or with a commercial program that offers a graphical user interface. Your Web browser can also make FTP requests to download programs you select from a Web page. Using FTP, you can also update (delete, rename, move, and copy) files at a server. You need to logon to an FTP server. However, publicly available files are easily accessed using anonymous FTP.

Basic FTP support is usually provided as part of a suite of programs that come with TCP/IP. However, any FTP client program with a graphical user interface usually must be downloaded from the company that makes it.

File sharing

File sharing is the practice of distributing or providing access to digitally stored information, such as computer programs, multimedia (audio, images and video), documents or electronic books. It may be implemented through a variety of ways. Common methods of storage, transmission and dispersion include manual sharing utilizing removable media, centralized servers on computer networks, World Wide Web-based hyperlinked documents, and the use of distributed peer-to-peer networking.

Users can use software that connects in to a peer-to-peer network to search for shared files on the computers of other users connected to the network. Files of interest can then be downloaded directly from other users on the network. Typically, large files are broken down into smaller chunks, which may be obtained from multiple peers and then reassembled by the downloader. This is done while the peer is simultaneously uploading the chunks it already has to other peers.

BitTorrent is a protocol supporting the practice of peer-to-peer file sharing that is used to distribute large amounts of data over the Internet. BitTorrent is one of the most common protocols for transferring large files.

Programmer Bram Cohen, a former University at Buffalo graduate student in Computer Science, designed the protocol in April 2001 and released the first available version on 2 July 2001, and the final version in 2008. BitTorrent clients are available for a variety of computing platforms and operating systems including an official client released by Bittorrent, Inc..

A **BitTorrent tracker** is a server that assists in the communication between peers using the BitTorrent protocol. In peer-to-peer file sharing a software client on an end-user PC requests a file, and portions of the requested file residing on peer machines are sent to the client, and then reassembled into a full copy of the requested file. The "tracker" server keeps track of where file copies reside on peer machines, which ones are available at time of the client request, and helps coordinate efficient transmission and reassembly of the copied file. The BitTorrent tracker is also, in the absence of extensions to the original protocol, the only major critical point, as clients are required to communicate with the tracker to initiate downloads. Clients that have already begun downloading a file communicate with the tracker periodically to negotiate faster file transfer with new peers, and provide network performance statistics; however, after the initial peer-to-peer file download is started, peer-to-peer communication can continue without the connection to a tracker.

5.5 The Web and E-mail

Web basics

On March 12, 1989, Tim Berners-Lee, a British computer scientist and former CERN employee, wrote a proposal for what would eventually become the World Wide Web. The 1989 proposal was meant for a more effective CERN communication system but Berners-Lee eventually realised the concept could be implemented throughout the world. Berners-Lee and Belgian computer scientist Robert Cailliau proposed in 1990 to use hypertext "to link and access information of various kinds as a web of nodes in which the user can browse at will", and Berners-Lee finished the first website in December of that year. The first test was completed around 20 December 1990 and Berners-Lee reported about the project on the newsgroup alt.hypertext on 7 August 1991.

Web site

A Web site is a related collection of World Wide Web (WWW) files that includes a beginning file called a home page. A company or an individual tells you how to get to their Web site by giving you the address of their home page. From the home page, you can get to all the other pages on their site. For example, the Web site for Baidu has the home page address of http://www.baidu.com.

Since site implies a geographic place, a Web site can be confused with a Web server. A server is a computer that holds the files for one or more sites. A very large Web site may be spread over a number of servers in different geographic locations.

You can have multiple Web sites that cross-link to files on each others' sites or even share the same files.

Web pages

A web page (or webpage) is a web document that is suitable for the World Wide Web and the web browser. A web browser displays a web page on a monitor or mobile device. The web page

is what displays, but the term also refers to a computer file, usually written in HTML or comparable markup language, whose main distinction is to provide hypertext that will navigate to other web pages via links. Web browsers coordinate web resources centered around the written web page, such as style sheets, scripts and images, to present the web page. Figure 5-35 shows a web page.

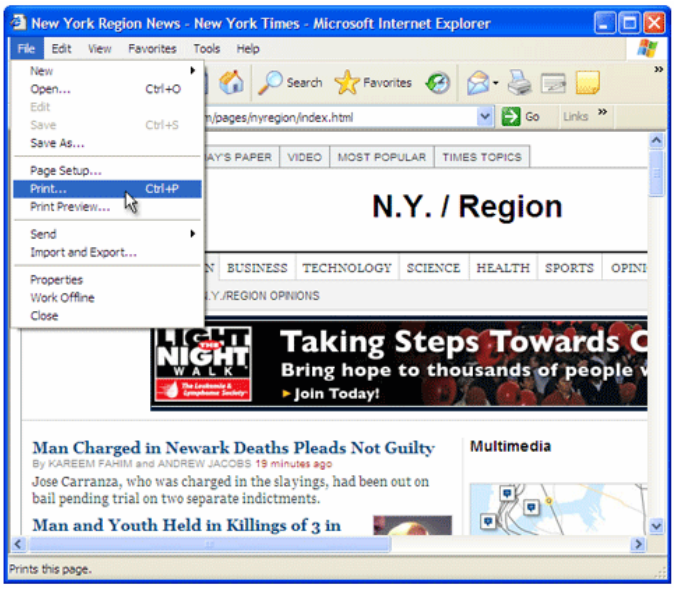


Figure 5-35 A HTML Web page

URL

A URL (Uniform Resource Locator, previously Universal Resource Locator) - usually pronounced by sounding out each letter but, in some quarters, pronounced “Earl” - is the unique address for a file that is accessible on the Internet. A common way to get to a Web site is to enter the URL of its home page file in your Web browser’s address line. However, any file within that Web site can also be specified with a URL. Such a file might be any Web (HTML) page other than the home page, an image file, or a program such as a common gateway interface application or Java applet. The URL contains the name of the protocol to be used to access the file resource, a domain name that identifies a specific computer on the Internet, and a pathname, a hierarchical description that specifies the location of a file in that computer.

On the Web (which uses the Hypertext Transfer Protocol, or HTTP), an example of a URL is: http://www.abcd.org/efg/hijk.txt. Which specifies the use of a HTTP (Web browser) application, a unique computer named www.ietf.org, and the location of a text file or page to be accessed on that computer whose pathname is /efg/hijk.txt.

HTML

HTML (Hypertext Markup Language) is the set of markup symbols or codes inserted in a file

intended for display on a World Wide Web browser page. The markup tells the Web browser how to display a Web page's words and images for the user. Each individual markup code is referred to as an element (but many people also refer to it as a tag). Some elements come in pairs that indicate when some display effect is to begin and when it is to end.

HTML is a formal Recommendation by the World Wide Web Consortium (W3C) and is generally adhered to by the major browsers, Microsoft's Internet Explorer and Netscape's Navigator, which also provide some additional non-standard codes. The current version of HTML is HTML 4.0. However, both Internet Explorer and Netscape implement some features differently and provide non-standard extensions. Web developers using the more advanced features of HTML 4 may have to design pages for both browsers and send out the appropriate version to a user. Significant features in HTML 4 are sometimes described in general as dynamic HTML. What is sometimes referred to as HTML 5 is an extensible form of HTML called Extensible Hypertext Markup Language (XHTML). Here is an example of a html file.

```
<form>
<table border=1>
<tr>
<td>Include descriptions?  
      <input type="radio" name="z" value="y">Yes  
      <input type="radio" name="z" checked value="n">No</td>
</tr>
<tr>
<td>What other options would you like?<br>
      <input type="checkbox" name="y" checked value="a">Location  
      <input type="checkbox" name="y" value="b">Update Info  
      <input type="checkbox" name="y" value="c">Language</td>
</tr>
<tr>
<td>Show resources for a particluar language:  
      <select name="x">
            <option value="A">Afrikaans
            <option value="B">French
            <option value="C">Gullah
            <option value="D">Malagasy
            <option value="E">Papiamento
            <option value="F">Welsh
      </select>
</td>
</tr>
<tr><td align="center"><input type="submit" value="Submit"></td></tr>
</table>
</form>
```

As the World Wide Web Consortium (W3C) describes it, **XHTML** (Extensible Hypertext Markup Language) is "a reformulation of HTML 4.0 as an application of the Extensible Markup Language (XML)." For readers unacquainted with either term, HTML is the set of codes (that's the "markup language") that a writer puts into a document to make it displayable on the World Wide Web. HTML 4 is the current version of it. XML is a structured set of rules for how one might define any kind of data to be shared on the Web. It's called an "extensible" markup

language because anyone can invent a particular set of markup for a particular purpose and as long as everyone uses it (the writer and an application program at the receiver's end), it can be adapted and used for many purposes - including, as it happens, describing the appearance of a Web page. That being the case, it seemed desirable to reframe HTML in terms of XML. The result is XHTML, a particular application of XML for "expressing" Web pages.

XHTML is, in fact, the follow-on version of HTML 4. You could think of it as HTML 5, except that it is called XHTML 1.0. In XHTML, all HTML 4 markup elements and attributes (the language of HTML) will continue to be supported. Unlike HTML, however, XHTML can be extended by anyone that uses it. New elements and attributes can be defined and added to those that already exist, making possible new ways to embed content and programming in a Web page. In appearance, an XHTML file looks like a somewhat more elaborate HTML file.

The W3C continues to develop a working draft for the XHTML 2.0 specification, releasing an eighth version in July of 2006.

To quote the W3C again, **the advantages of XHTML** are "extensibility and portability."

Extensibility means that as new ideas for Web communication and presentation emerge, they can be implemented without having to wait for the next major version of HTML and browser support. New tags or attributes can be defined to express the new possibilities and, assuming some program at the receiving end can understand and act on them, new things may happen on your Web page that never happened before. Specific sets of extensions for XHTML are planned for mathematical expressions, vector graphics, and multimedia applications.

If extensibility is likely to lead to more complicated pages and larger programs, the portability advantage means that Web pages can now be made simpler than they were before so that small devices can handle them. This is important for mobile devices and possibly household devices that contain microprocessors with embedded programming and smaller memories. XHTML defines several levels of possible markup complexity and each document states its level of complexity at the beginning. Programs in microdevices might expect XHTML-coded files that state the simplest level of complexity so that they could be handled by a small program and memory.

You can find out more by reading the specification and tutorials, but here are some **distinctive features** of XHTML and **differences** between HTML 4:

XHTML requires strict adherence to coding rules. Notably, it requires closing as well as opening elements (this is known as well-formed syntax) and that all elements be in lower case. HTML was much less rigorous about notation and browsers tended to be even more forgiving.

This means that XHTML files will tend to be "busier" than HTML. However, they won't necessarily be harder to read because rigor may force more order in coding. In addition, major editing and file creation tools can lay out pages for easier readability.

XHTML encourages a more structured and conceptual way of thinking about content and, combined with the style sheet, a more creative way of displaying it.

XHTML makes it easier for people to dream up and add new elements (and develop

browsers or other applications that support them).

HTTP

HTTP (Hypertext Transfer Protocol) is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. As soon as a Web user opens their Web browser, the user is indirectly making use of HTTP. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols.

HTTP defines methods (sometimes referred to as verbs) to indicate the desired action to be performed on the identified resource. What this resource represents, whether pre-existing data or data that is generated dynamically, depends on the implementation of the server. Often, the resource corresponds to a file or the output of an executable residing on the server. The HTTP/1.0 specification defined the GET, POST and HEAD methods and the HTTP/1.1 specification added 5 new methods: OPTIONS, PUT, DELETE, TRACE and CONNECT. By being specified in these documents their semantics are well known and can be depended upon. Any client can use any method and the server can be configured to support any combination of methods. If a method is unknown to an intermediate it will be treated as an unsafe and non-idempotent method. There is no limit to the number of methods that can be defined and this allows for future methods to be specified without breaking existing infrastructure. For example, WebDAV defined 7 new methods and RFC 5789 specified the PATCH method.

GET:

Requests a representation of the specified resource. Requests using GET should only retrieve data and should have no other effect. (This is also true of some other HTTP methods.)[1] The W3C has published guidance principles on this distinction, saying, "Web application design should be informed by the above principles, but also by the relevant limitations." See safe methods below.

HEAD:

Ask for the response identical to the one that would correspond to a GET request, but without the response body. This is useful for retrieving meta-information written in response headers, without having to transport the entire content.

POST:

Requests that the server accept the entity enclosed in the request as a new subordinate of the web resource identified by the URI. The data POSTed might be, as examples, an annotation for existing resources; a message for a bulletin board, newsgroup, mailing list, or comment thread; a block of data that is the result of submitting a web form to a data-handling process; or an item to add to a database.

PUT:

Request that the enclosed entity be stored under the supplied URI. If the URI refers to an already existing resource, it is modified; if the URI does not point to an existing resource, then the server can create the resource with that URI.

DELETE:

Delete the specified resource.

TRACE:

Echo back the received request so that a client can see what (if any) changes or additions have been made by intermediate servers.

OPTIONS:

Return the HTTP methods that the server supports for the specified URL. This can be used to check the functionality of a web server by requesting '*' instead of a specific resource.

CONNECT:

Converts the request connection to a transparent TCP/IP tunnel, usually to facilitate SSL-encrypted communication (HTTPS) through an unencrypted HTTP proxy.[15][16] See HTTP CONNECT Tunneling.

PATCH:

Is used to apply partial modifications to a resource.

HTTP servers are required to implement at least the GET and HEAD methods and, whenever possible, also the OPTIONS method.

Figure 5-36 demonstrates the messages that flow between your browser and a Web server to retrieve an HTML document.

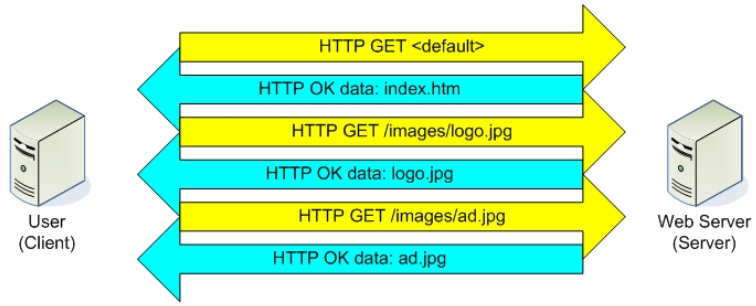


Figure 5-36 Retrieve HTML document between browser and Web server

Web Browsers

A web browser (commonly referred to as a browser) is a software application for retrieving, presenting and traversing information resources on the World Wide Web. An information resource is identified by a Uniform Resource Identifier (URI/URL) and may be a web page, image, video or other piece of content. Hyperlinks present in resources enable users easily to navigate their browsers to related resources.

Although browsers are primarily intended to use the World Wide Web, they can also be used to access information provided by web servers in private networks or files in file systems.

The major web browsers are Firefox, Internet Explorer, Google Chrome, Opera, and Safari as shown in Figure 3-37.

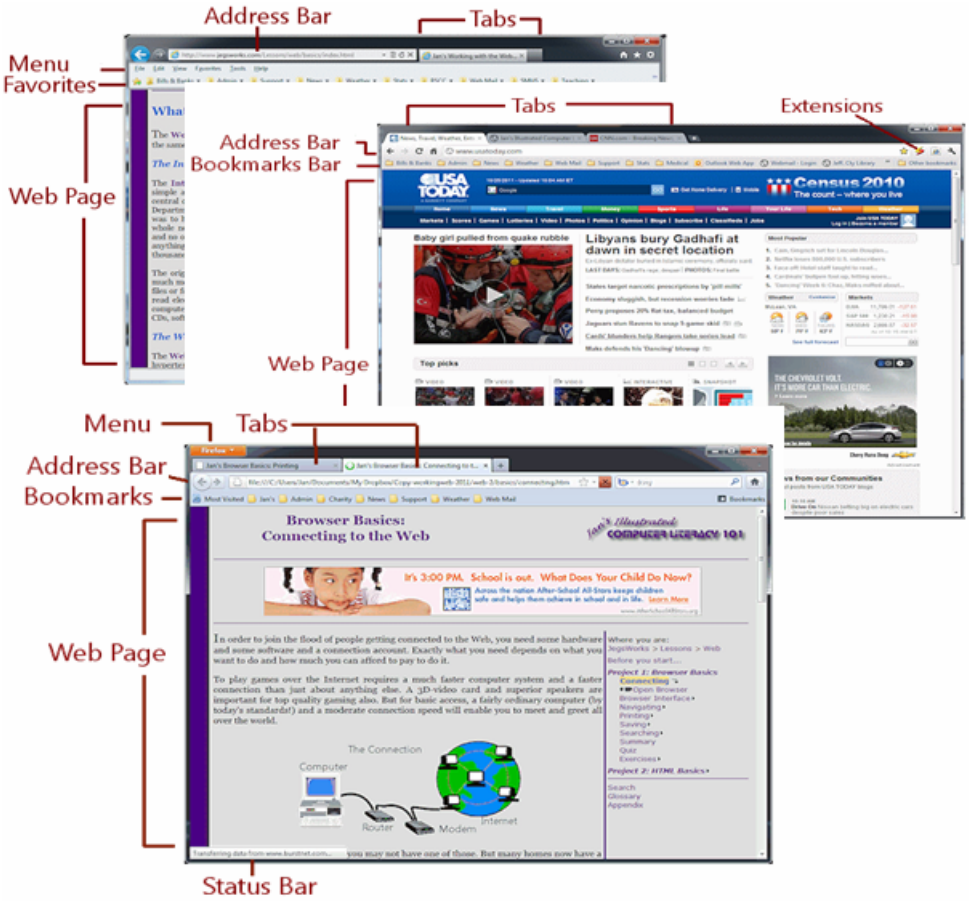


Figure 5-37 Interface of IE9, Chrome, Firefox

Cookies

A cookie, also known as an HTTP cookie, web cookie, or browser cookie, is a small piece of data sent from a website and stored in a user's web browser while the user is browsing that website. Every time the user loads the website, the browser sends the cookie back to the server to notify the website of the user's previous activity. Cookies were designed to be a reliable mechanism for websites to remember stateful information (such as items in a shopping cart) or to record the user's browsing activity (including clicking particular buttons, logging in, or recording which pages were visited by the user as far back as months or years ago).

Cookies can store passwords and form content a user has previously entered, such as a credit card number or an address. When a user accesses a website with a cookie function for the first time, a cookie is sent from server to the browser and stored with the browser in the local computer. Later when that user goes back to the same website, the website will recognize the user because of the stored cookie with the user's information.

Other kinds of cookies perform essential functions in the modern web. Perhaps most importantly, authentication cookies are the most common method used by web servers to know

whether the user is logged in or not, and which account they are logged in with. Without such a mechanism, the site would not know whether to send a page containing sensitive information, or require the user to authenticate themselves by logging in. The security of an authentication cookie generally depends on the security of the issuing website and the user's web browser, and on whether the cookie data is encrypted. Security vulnerabilities may allow a cookie's data to be read by a hacker, used to gain access to user data, or used to gain access (with the user's credentials) to the website to which the cookie belongs (see cross-site scripting and cross-site request forgery for examples).

ActiveX control

ActiveX is a software framework created by Microsoft which adapts its earlier Component Object Model (COM) and Object Linking and Embedding (OLE) technologies for content downloaded from a network, particularly in the context of the World Wide Web. It was introduced 1996 and is commonly used in its Windows operating system. In principle it is not dependent on Microsoft Windows, but in practice, most ActiveX controls require either Microsoft Windows or a Windows emulator. Most also require the client to be running on Intel x86 hardware, because they contain compiled code.

Many Microsoft Windows applications — including many of those from Microsoft itself, such as Internet Explorer, Microsoft Office, Microsoft Visual Studio, and Windows Media Player — use ActiveX controls to build their feature-set and also encapsulate their own functionality as ActiveX controls which can then be embedded into other applications. Internet Explorer also allows the embedding of ActiveX controls in web pages.

Search Engines

A web search engine is a software system that is designed to search for information on the World Wide Web. The search results are generally presented in a line of results often referred to as search engine results pages (SERPs). The information may be a mix of web pages, images, and other types of files. Some search engines also mine data available in databases or open directories. Unlike web directories, which are maintained only by human editors, search engines also maintain real-time information by running an algorithm on a web crawler. Figure 5-38 shows Google search engine.

On the Internet, a search engine is a coordinated set of programs that includes:

- A spider (also called a "crawler" or a "bot") that goes to every page or representative pages on every Web site that wants to be searchable and reads it, using hypertext links on each page to discover and read a site's other pages.
- A program that creates a huge index (sometimes called a "catalog") from the pages that have been read.
- A program that receives your search request, compares it to the entries in the index, and returns results to you.

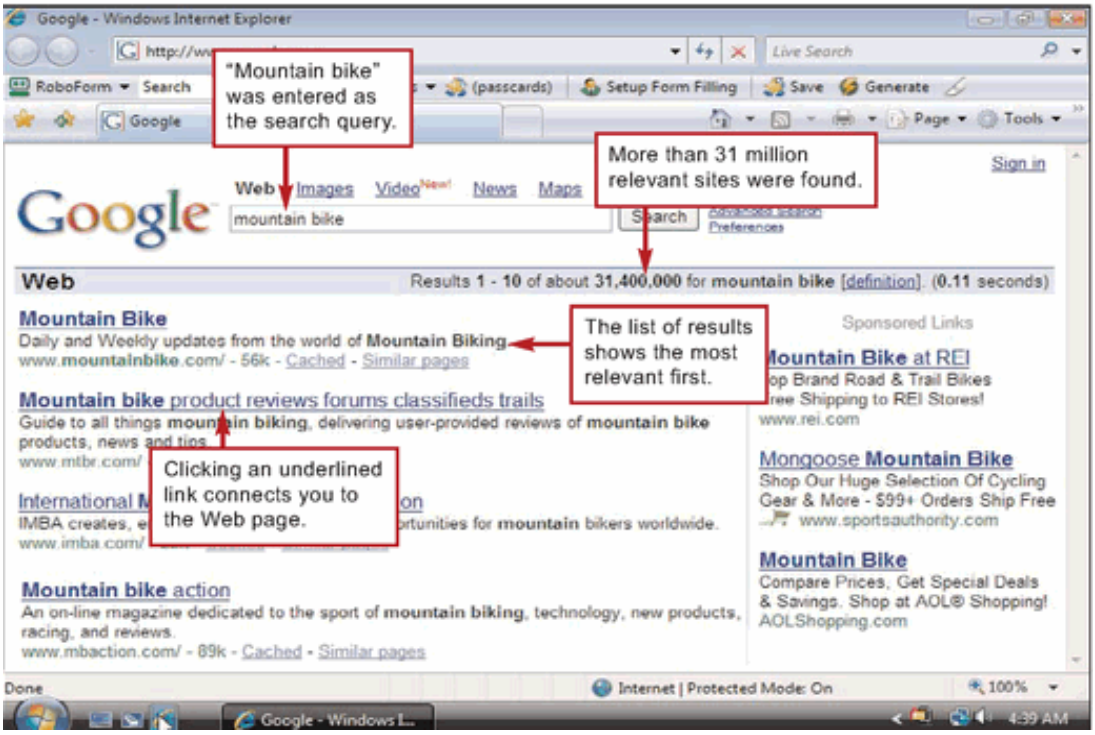


Figure 5-38 A query for "mountain bike" on Google

- An alternative to using a search engine is to explore a structured directory of topics. Yahoo, which also lets you use its search engine, is the most widely-used directory on the Web. A number of Web portal sites offer both the search engine and directory approaches to finding information.

Different Search Engine Approaches:

Major search engines such as Google, Yahoo (which uses Google), AltaVista, and Lycos index the content of a large portion of the Web and provide results that can run for pages - and consequently overwhelm the user.

Specialized content search engines are selective about what part of the Web is crawled and indexed. For example, TechTarget sites for products such as the AS/400 (http://www.search400.com) and CRM applications (http://www.searchCRM.com) selectively index only the best sites about these products and provide a shorter but more focused list of results.

Ask Jeeves (http://www.ask.com) provides a general search of the Web but allows you to enter a search request in natural language, such as "What's the weather in Seattle today?"

Special tools and some major Web sites such as Yahoo let you use a number of search engines at the same time and compile results for you in a single list.

Individual Web sites, especially larger corporate sites, may use a search engine to index and retrieve the content of just their own site. Some of the major search engine companies license or sell their search engines for use on individual sites.

E-commerce

Electronic commerce, commonly known as E-commerce or eCommerce, is trading in products or services conducted via computer networks such as the Internet. Electronic commerce draws on technologies such as mobile commerce, electronic funds transfer, supply chain management, Internet marketing, online transaction processing, electronic data interchange (EDI), inventory management systems, and automated data collection systems. Modern electronic commerce typically uses the World Wide Web at least at one point in the transaction's life-cycle, although it may encompass a wider range of technologies such as e-mail, mobile devices, social media, and telephones as well.

Electronic commerce is generally considered to be the sales aspect of e-business. It also consists of the exchange of data to facilitate the financing and payment aspects of business transactions. This is an effective and efficient way of communicating within an organization and one of the most effective and useful ways of conducting business. It is a Market entry strategy where the company may or may not have a physical presence.

E-commerce can be divided into 7 subsections:

- E-tailing or "virtual storefronts" on websites with online catalogs, sometimes gathered into a "virtual mall".
- Buying or selling on websites and/or online marketplaces.
- The gathering and use of demographic data through web contacts and social media.
- Electronic data interchange, the business-to-business exchange of data.
- E-mail and fax and their use as media for reaching prospective and established customers (for example, with newsletters).
- Business-to-business buying and selling.
- The security of business transactions.

Market research

In early 1999, it was widely recognized that because of the interactive nature of the Internet, companies could gather data about prospects and customers in unprecedented amounts -through site registration, questionnaires, and as part of taking orders. The issue of whether data was being collected with the knowledge and permission of market subjects had been raised. (Microsoft referred to its policy of data collection as "profiling" and a proposed standard has been developed that allows Internet users to decide who can have what personal information.)

E-mail

Email, or e-mail, is simply the shortened form of "electronic mail," a system for receiving, sending, and storing electronic messages. With the explosion growth of the Internet, e-mail has become nearly universal popularity around the world.

Emails can frequently include almost all kinds of files. Moreover, it is no longer necessary to send or receive an email just on a PC. A variety of mobile devices, such as portable devices,

make it possible manage correspondence on the go. Figure 5-39 shows an email.

There are some standardized protocols for users receiving and sending messages. Simple message transfer protocol (SMTP) enables the actual sending and receiving of messages. Other protocols, including Post Office Protocol (POP) and Internet Message Access Protocol (IMAP), allow users to retrieve and store messages over time. The process is shown in Figure 5-40.

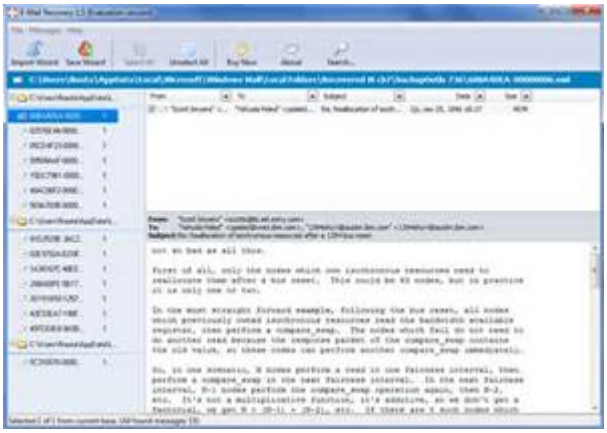


Figure 5-39 An E-mail

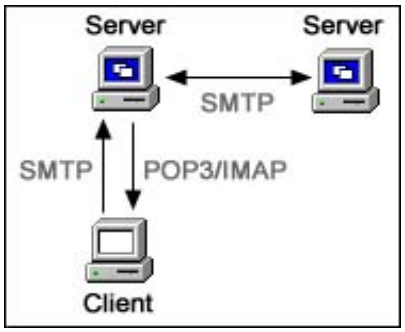


Figure 5-40 How the protocol can be used

5.6 The Network Security

Wi-Fi Security

Today, wireless threats come everywhere. But many wireless users have no idea what kinds of danger they face. Wireless communication is broadcast over radio waves, the messages they contained are easily picked by criminals. Because the range of a wireless LAN can extend far outside the physical boundaries of the office or building, so the attackers need not require specialized skills to break into a network.

(1) Use of Encryption

The most effective way to secure your wireless network from intruders is to encrypt, or scramble, communications over the network. Most wireless routers, access points, and base stations have a built-in encryption mechanism. If your wireless router doesn't have an encryption feature, consider getting one that does. Manufacturers often deliver wireless routers with the encryption feature turned off. You must turn it on. Figure 5-41 shows the use of encryption.

(2) Use anti-virus and anti-spyware software, and a firewall

Computers on a wireless network need the same protections as any computer connected to the Internet. Install anti-virus and anti-spyware software, and keep them up-to-date. If your firewall was shipped in the "off" mode, turn it on.

(3) Turn off identifier broadcasting

Most wireless routers have a mechanism called identifier broadcasting. It sends out a signal to any device in the vicinity announcing its presence. You don't need to broadcast this information if the person using the network already knows it is there. Hackers can use identifier broadcasting to home in on vulnerable wireless networks. Disable the identifier broadcasting mechanism if your wireless router allows it.

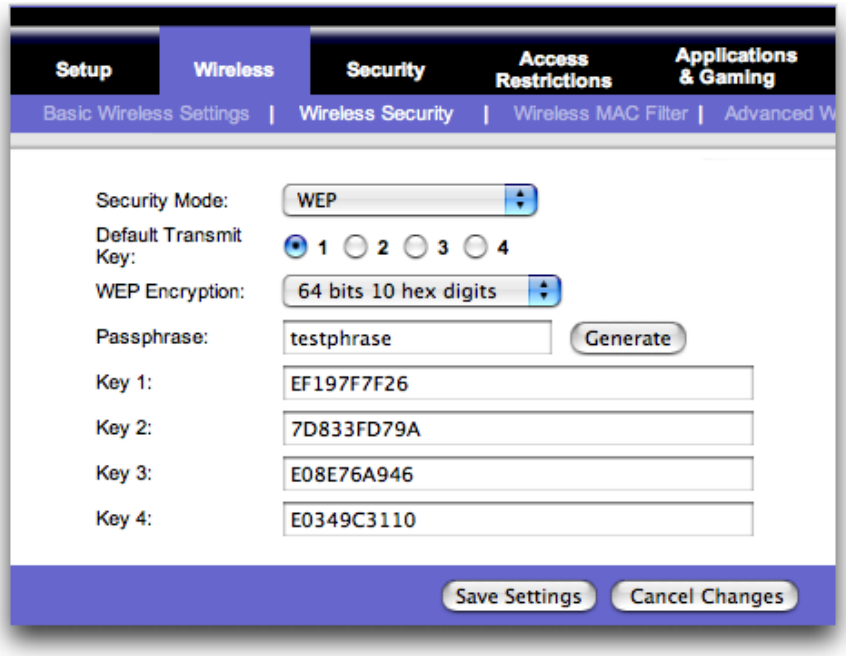


Figure 5-41 Using encryption

(4) Change the identifier on your router from the default

The identifier for your router is likely to be a standard, default ID assigned by the manufacturer to all hardware of that model. Even if your router is not broadcasting its identifier to the world, hackers know the default IDs and can use them to try to access your network. Change your identifier to something only you know, and remember to configure the same unique ID into your wireless router and your computer so they can communicate. Use a password that's at least 10 characters long: The longer your password, the harder it is for hackers to break.

(5) Change your router's pre-set password for administration

The manufacturer of your wireless router probably assigned it a standard default password that allows you to set up and operate the router. Hackers know these default passwords, so change it to something only you know. The longer the password, the tougher it is to crack.

(6) Allow only specific computers to access your wireless network

Every computer that is able to communicate with a network is assigned its own unique Media Access Control (MAC) address. Wireless routers usually have a mechanism to allow only

devices with particular MAC addresses access to the network. Some hackers have mimicked MAC addresses, so don't rely on this step alone.

(7) Turn off your wireless network when you know you won't use it

Hackers cannot access a wireless router when it is shut down. If you turn the router off when you're not using it, you limit the amount of time that it is susceptible to a hack.

(8) Don't assume that public "hot spots" are secure

Many cafés, hotels, airports, and other public establishments offer wireless networks for their customers' use. We can't assure they are secure.

Internet Security

Internet security is a tree branch of computer security specifically related to the Internet, often involving browser security but also network security on a more general level as it applies to other applications or operating systems on a whole. Its objective is to establish rules and measures to use against attacks over the Internet. The Internet represents an insecure channel for exchanging information leading to a high risk of intrusion or fraud, such as phishing. Different methods have been used to protect the transfer of data, including encryption.

Basically, a firewall, working closely with a router program, examines each network packet to determine whether to forward it toward its destination. A firewall also includes or works with a proxy server that makes network requests on behalf of workstation users. A firewall is often installed in a specially designated computer separate from the rest of the network so that no incoming request can get directly at private network resources.

There are a number of firewall screening methods. A simple one is to screen requests to make sure they come from acceptable (previously identified) domain name and Internet Protocol addresses. For mobile users, firewalls allow remote access in to the private network by the use of secure logon procedures and authentication certificates.

A number of companies make firewall products. Features include logging and reporting, automatic alarms at given thresholds of attack, and a graphical user interface for controlling the firewall (as shown in Figure 5-42).

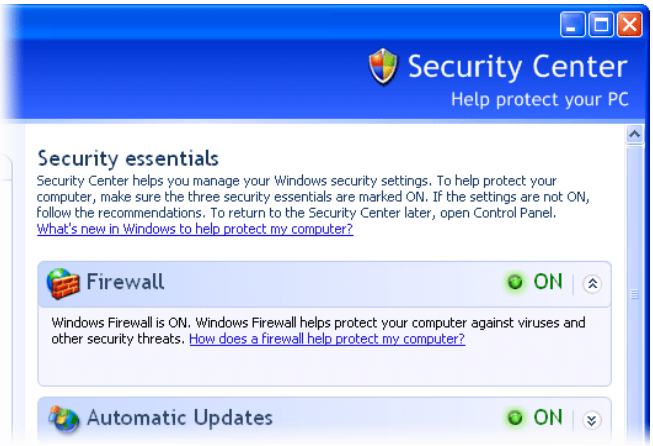


Figure 5-42 Internet Security

Web Security

The internet is a way to stay connected with friends and family. For many people, it's also a way to stay current on news, research information or shop online. The Internet has also become a popular method for banking, paying bills and completing and submitting applications and forms.

How does it work?

Many criminal activities online depend upon a lack of a user's security awareness. Criminals can send out hundreds upon thousands of hooks (called Phishing) in the form of spam emails hoping to catch a few users who will make their efforts worthwhile. Malicious links contained in phishing emails, scareware and other deceptions usually attempt to convince the user to click on a link or buy software through quite convincing claims or offers.

Protecting yourself online is a combination of using an up-to-date anti-virus program and internet browser whilst also having an awareness of the threats.

When submitting sensitive data such as logging into your E-mail, bank or social network you should ensure the connection to the website is secured by a digital certificate. Use of an identifying certificate by the website is indicated in the address bar of the Internet browser, it will always read https:// rather than http://, check for the "s" at the end before you log in.

There are more advanced options and features you can enable in your internet browser that can help identify potentially unsafe websites or search results. More information on browser security can be found in the useful links section.

What risk does it pose?

- The victim may have their identity stolen leading to financial damage.
- The files of the user's machine or device can be damaged or stolen.
- The user's machine may be used to send out Spam to other users.

How can I avoid it from happening?

- Install and maintain anti-virus software on your computer or device.
- Keep your internet browser up-to-date.
- Be alert to unusual computer activity or problems.
- Install and maintain a firewall on your computer.
- Use a modern browser with features such as a pop-up blocker.
- Avoid storing sensitive material indefinitely on your computer.
- Change your passwords often.
- Beware of links sent via instant messaging and e-mail attachments.

Top Tips

- Be suspicious of any emails or websites offering something too good to be true; it probably is.
- Use strong passwords containing numbers, uppercase and lowercase letters and symbols.
- Use up-to-date anti-virus software on your computer.

Note：

The contents of computer networks can be concluded into this KM chart of Figure 5-43.

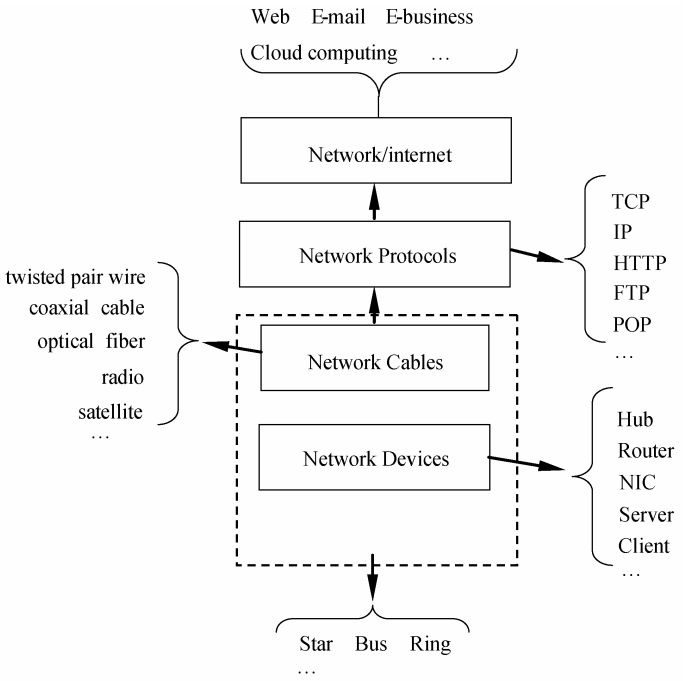


Figure 5-43 KM chart of computer networks

Exercises

For each question, choose the appropriate answer.

1. A computer which links several PCs together and answers the request in a network is called a _____.
   A. minicomputer B. server C. client D. main frame

2. Twisted wire, coaxial cable, and microwave are types of transmission _____.
   A. chains B. media C. data D. information

3. Fiber optics have the advantage of _____.
   A. being cheaper to install than twisted wire B. being easier to install than twisted wire
   C. having little interference D. using direct line-of-sight

4. A modem is used to _____.
   A. change incoming analog signals to digital signals and outgoing digital signals to analog signals
   B. connect two computers using a satellite uplink
   C. connect a computer to a shared printer
   D. None of above

5. A LAN is a _____ network.
   A. Long Array B. Local Area C. Land Access D. Line Area