9 Internet, the Web, Mobile Communications and IoTs

Opening Vignette -- IOT and WOT on the Move

Simply stated, IoT (Internet of Things) refers to any device that can be connected to the Internet. As more devices are developed with built-in sensors and wireless capabilities, the cost of IoT is dropping -- thus driving the applications of IoT at home, work or play. Web of Things (WoT) provide web interfaces to IoT devices. Thus more "things" on planet Earth are becoming digitally connected Internet devices and more appliances and gadgets are using web interfaces. Many interesting and far reaching applications are emerging. We mention only two broad areas of work – more later.

Web Enabled Robots: A wide range of Web enabled Robots are being used for a wide range of work functions. Thus we are finding more and more robots to perform medical operations, cut grass, examine dangerous areas, and serve as butlers. Robots are used for these tasks because, unlike humans, robots do not get tired, they do not get bored by repetition, they can endure physical conditions that are dangerous or uncomfortable, and they cannot be distracted from the task at hand. While robotics has been always used in the past, the AI capabilities, combined with IoT and WoT enablement, are triggering many new application scenarios.

One of the most interesting application of web enabled robots is to perform surgeries. For example, robots can make more precise movements and make a greater range of movement through a smaller incision, which minimizes the risk of infection and speed recovery. Specifically, a NeuroArm is used for surgery of the brain and the HeartLander can be used to conduct heart surgery without doctors having to cut open a patient’s chest. These and other surgical robots are supported by the following capabilities:

- Mobile apps on a smart phone contains an extensive checklist for scheduling of main procedures, equipment, personnel and medicine. For transportation of goods and personnel for major operations, a link to GPS could be used.
- Connections to a nearby pharmacy and other specialized providers, if needed.
- Cloud based Automated Medical Support System that links with regulatory bodies for possible liabilities for any damages that could result from malfunctions.

IoT4D (IoT for Development): IoTs offer a tremendous opportunity for the underserved populations to bridge the digital divide. Specifically, Cisco and the International Telecommunications Union (ITU), the United Nations specialized agency for ICTs, has published a report, “Harnessing the Internet of Things for Global Development”, that outlines how IoT can rapidly accelerate the rate of global development to achieve the UN Sustainable Development Goals (SDGs). The report describes 20 projects that are showing the following results:

- Affordable IoT devices in developing countries can significantly improve quality of life for the underserved populations.
- IoT devices are playing a key role in health, education, public safety, public welfare and

other vital sectors in the developing countries.

The report notes that the availability, affordability, and scalability of IoT is improving dramatically to make a quick and lasting impact on the day-to-day lives of the underserved populations.

Sources:

- ITU and Cisco Report: "Harnessing the Internet of Things for Global Development", (https://www.itu.int/en/action/broadband/Documents/Harnessing-IoT-Global-Development.pdf)
- Boudreaux, R., "The Web of Things: A web-connected world of smart devices", http://www.codeproject.com/Articles/483154/At-Your-Service-Application, accessed: May 26, 2016.

9.1 Introduction

IT infrastructure provides the technologies needed to *enable* the enterprise applications. Examples of such enabling technologies are the Web technologies (including Web 2.0 and Web Services) used in corporate intranets, computing platforms on which the applications reside, wireless and wired networks which connect all the computing platforms in an Intranet, "Extranets" which connect many businesses for B2B trade, and wireless sensor-enabled Internet of Things (IoT). Figure 9-1 shows a simplified technical architecture of a small healthcare provider that runs four types of applications on four types of computers that are interconnected over a wide range of wireless and wired networks. For example, the administrative applications such as patient admissions are run on corporate servers located in the cloud, the healthcare analytics and BI applications run on Windows/Unix servers, the patient care applications used by the physicians run on laptops, and patient monitoring applications in the emergency rooms and remote health facilities for aging populations run on handsets and IoT devices interconnected over wireless sensor networks. All these IT infrastructure components, explained in this chapter, collaborate with each other to provide highly valuable enterprise services.

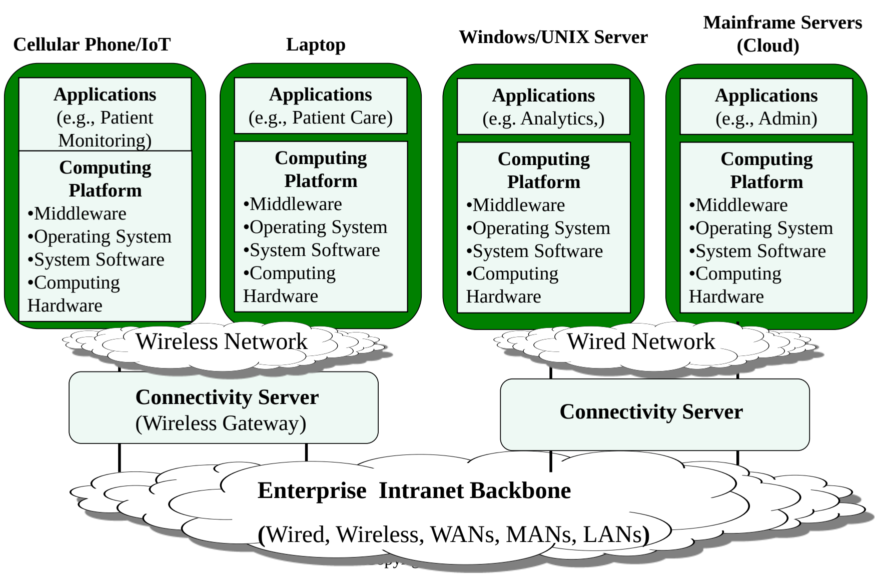


Figure 9-1: Sample IT Infrastructure for a Healthcare Provider

In this chapter, we will specifically concentrate on the following main IT building blocks and their role in enabling modern enterprises:

- Networks that provide the network transport between remote parties and are responsible for routing and flow/error control support. The networks may be the private value added networks (VANs), Public Internet, and/or Extranets that utilize the wired or wireless transmission media.

- Web technologies that serves as the middleware to interconnect remotely located users, databases and applications. The Web allows access to a multitude of information sources, applications and databases through Web browsers. XML, Semantic Web, Web 2.0 and Web Services are considerably extending the popularity of Web technologies.
- Mobile computing and wireless communications that are fundamentally changing the enterprise landscape. In particular, mobile computing applications are supporting m-Business, m-Health, and m-Government initiatives. These initiatives use Wireless Internet that operates over wide range of wireless networks such as WiFi, cellular networks, sensor networks, and satellites.
- IoT and WoT devices and applications that utilize a combination of all of the above (e.g., the Internet, the Web technologies, mobile communications, and wireless sensor networks).

Several examples and case studies illustrate the key points. After reading this chapter, you should be able to answer the following questions:

- What are the key network concepts
- What is a network architectures and what are its key components
- What is the Open System Interconnection (OSI) Reference Model and how does it help in network interconnectivity
- What are the key characteristics of broadband and wireless networks
- What is the Internet and how does it support modern enterprises
- What are Intranets and Extranets
- What is Next Generation Internet (NGI) and what is its role in the
- What is Web and what are the key Web technologies
- What is Web 2.0 and Social Networking
- What is Mobile Computing and what are its key components
- What are the examples of Mobile Computing Applications of value to modern enterprises
- What are the key aspects of Wireless Networks

9.2 Introduction to Communication Networks

9.2.1 The Basic Network Concepts

Communication networks play a central role in the global economy by connecting the consumers, businesses, suppliers, government agencies, doctors, hobbyists, students, farmers, social workers, and a variety of other players and communities of interest around the globe. In today's Internet driven world, the role and importance of networks is "intuitively obvious to even the most casual observers". A large number of examples of networks can be found in our daily lives (e.g., telephone networks, cable networks, and home networks for telecommuting), educational institutions (e.g., university and high school campus networks), healthcare systems (e.g., hospital networks), retail stores (e.g., the Staples network that ties several Staples sites together), financial networks (e.g., the networks used by banks and financial institutions to transfer funds), wireless sensor networks that support IoT, and many other wireless and broadband networks.

A ***communication network*** is a collection of equipment and physical media, viewed as one autonomous whole, that interconnects two or more stations. A ***station*** is an end-point (source/sink) in a communication network and can be a sensor, terminal, computer, telephone, or a TV. Communication networks, also referred to as networks in this book, provide the information exchange services in distributed systems. Specifically, they are responsible for three types of services: delivery, understanding and agreement. Delivery is the physical transport of data between stations.

Data, in this context, is anything that conveys meaning to a user (e.g., customer names, bank balances, voice and images). Delivery involves finding a path for the data and sending the data correctly over the selected paths. Understanding assures that the data sent is in a format which can be understood by the receiver. Data may need to be translated between senders and receivers. Agreement assures that the data is sent when the receiver is ready to receive it. This means that the rules of exchange ***(protocol)*** must be established between a sender and a receiver. At the lowest level, a communication network consists of the following components (see Figure 9-2):

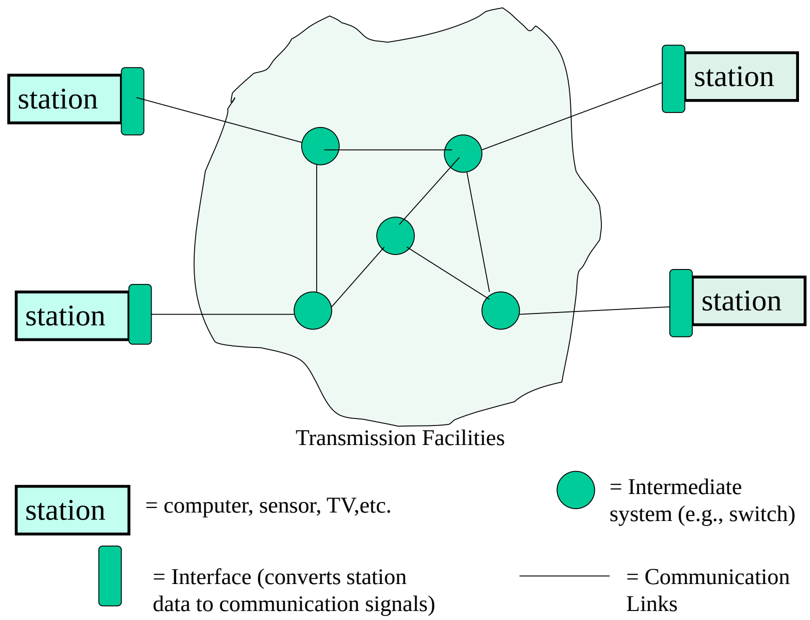


Figure 9-2: Conceptual View of Networks

- **Stations (data sources/sinks).** These entities generate and receive the data handled by the communication network. Examples of the data are voice, computer bits, sensor data, and TV patterns. A station is effectively an end-point (source/sink) in a communication network. Examples of stations are terminals (text and/or graphics), telephones, sensors (temperature, radiation levels), TVs, facsimiles, diskless workstations, personal computers, workstations, minicomputers, or mainframes.
- **Data/signal converters**. These devices convert the data to signals for transmission on one end and back to data at the other. Data is propagated from one point to another by means of signals which are electromagnetic representation of data. An example of a converter is a modem which converts data bits to continuous signals which are transmitted across a network. Converters basically translate different formats of data and signals (modems are digital to analog converters and codecs are analog to digital converters). In some networks, called baseband networks, the conversions are bypassed by "pressing" the data directly against the communication wire. In these cases, data and signals are the same.
- **Transmitting facilities**. These facilities deliver (transport) the signals across a network. This transport involves finding a path for the signals, sending the signals over the path, and dealing with signal attenuation and distortion over long transmission paths. The transmission facilities themselves consist of:
- **Links (communication links)** refer to the physical media that is used to interconnect stations in a communication network. Examples of links are telephone lines, coaxial cables, and fiber cables.

- **Intermediate systems**, also sometimes referred to as nodes, serve as intermediaries in a communication network. An example of a node is a router which is used to direct traffic from one point to another.

The transmission facilities consist of a wide range of hardware components and software modules. Network facilities are generally classified into three categories based on the geographical area covered (see Figure 9-3):

- **Local area networks (LANs)** which do not use common carrier facilities over short distances (around 100 meters) with data rates commonly in the range of 100 Mbps – some LANs are in the Gigabit range. LANs are usually used to interconnect computers within the same building (e.g., an office or home). A subclass of LANs is Personal Area Networks (PANs) that have shorter distances (around 10 meters) and lower data rates (around 10 Mbps). An example of PANs is wireless sensor networks that support IoT.
- **Wide area networks (WANs)** which use common carrier facilities over long distances commonly with data rates in the range of 1.5 to 100 Mbps. Fiber optic WANs easily operate in the Gigabit range. WANs are used to interconnect remotely located sites and equipment. A subclass of WANs is Global Area Networks (GANs) that utilize satellites for very long distances. Satellites, discussed later, interconnect continents and at present can go over a million mile (these are known as *deep space satellites*).
- **Metropolitan area networks (MANs)** are essentially large LANs which cover an entire metropolitan area (a city, a suburb, etc.). The evolving metropolitan area networks can be used to interconnect LANs within a metropolitan area. For example, Comcast is a well known company that provides MAN services in New Jersey and Pennsylvania.

Communication networks needed for the physical transmission and recognition of data between interconnected devices have transitioned to digital communication systems. These systems receive digital data which is regenerated over long distances by eliminating noise.

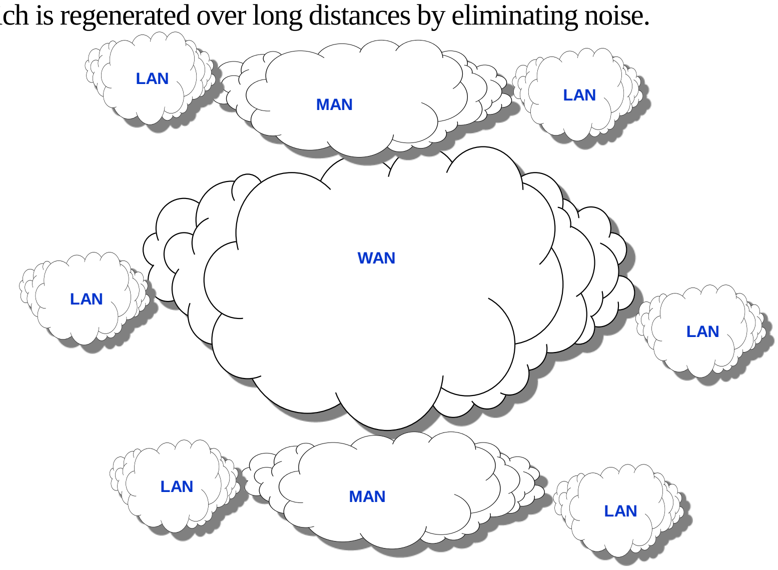


Figure 9-3: Network Configurations

9.2.2 Communication Media Characteristics

Communication media are used in networks to transmit data over short or long distances. Selection and design of communication media play an important role in the cost, reliability and performance of networks. Examples of the commonly used media are open wire pairs, twisted pair cables, coaxial cables, fiber optic systems, and wireless media.

Open Wire Pairs. This is the oldest, and at present almost obsolete, communication medium. Open wire pairs are low cost bare copper wires which were installed in the early part of this century for telephones and telegraphs. Some of these wires can still be found in some rural areas. Wire pairs are being replaced at present because they are susceptible to damage by weather and suffer from attenuation (signal loss) and crosstalk (interference) problems.

Twisted Pair Cables. These cables are used extensively in telephone circuits in buildings and trunks. Several wires are insulated and then enclosed in a cable. A twisted pair cable may include up to 3,000 wire pairs with a bandwidth up to 250 KHz. These cables do have better performance than open wires, but the signal/noise ratio is low due to crosstalk noise. Twisted pair cables are good for short distance communications.

Coaxial Cables. These cables have been around since the early 1940s and are used extensively in local area networks, long distance toll trunks, urban areas, and cable TV. The technology consists of a single central conductor, surrounded by a circular insulation layer, and a conductive shield. Coaxial cables have high bandwidth (up to 400 MHz) with much higher quality data transmission than the twisted pair cables. For example, a coaxial cable can support over 10,000 voice circuits by using the frequency division multiplexing technique mentioned previously. With different multiplexing techniques, coaxial cables can deliver high data speeds (above 10 Mbps) and support many data, voice, and video channels. This technology is limited due to signal loss at high frequencies.

Optical Fiber. This communication medium is showing more promise and potential for very high data transmission applications. The optical fiber uses light rays instead of electronic pulses for message transmission. A fiber optic cable is very thin, usually resembling a human hair, which uses special cladding so that the light rays cannot escape the cable and thus travel down the cable in a reflective path. The light source used in fiber optic is usually a laser or a light emitting diode (LED). Fiber optics show very high frequency ranges (higher than 20,000 MHz). Because of this high bandwidth, a single fiber optic cable can support over 30,000 telephone lines and can transmit data over 400 Mbps (remember the cable carrying all these telephone lines resembles a single human hair strand!!). Due to their very light weight and high bandwidths, fiber optic use is growing dramatically. Other reasons for the popularity of fiber optics are: a) resilience to fire and gaseous combustion (light waves do not generate electrical sparks), b) very low signal loss and error rates, c) high security characteristics due to the difficulties in tapping fiber optic cables, and d) decreasing costs of fiber optic devices. At the time of this writing, a fiber optic connector is more expensive than a copper cable tap. Thus the largest application of fiber optic cable is in enterprise "backbone networks" which interconnect many networks (see Figure 9-4).

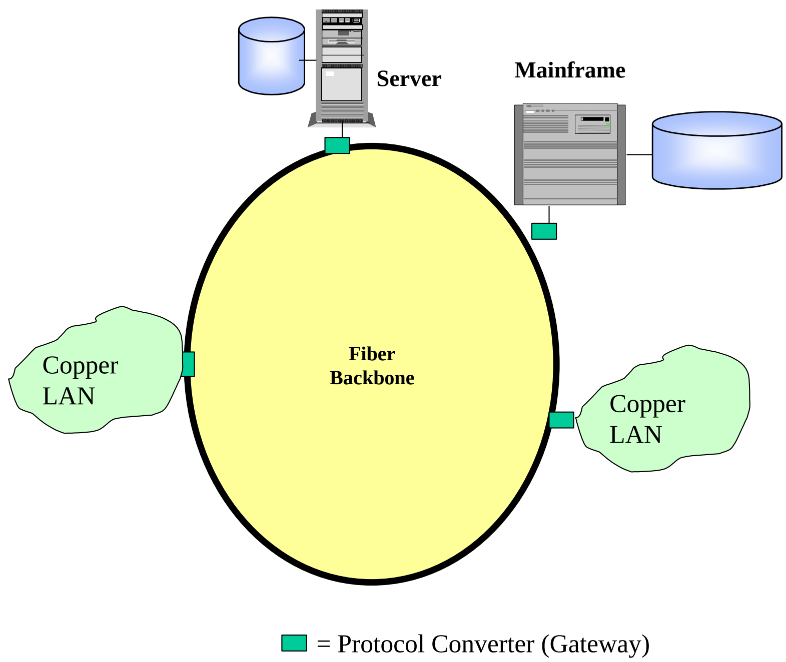


Figure 9-4: A Fiber Optic Network

Bandwidth and Data Rate of Communication Media

Communication media with high bandwidths and signal/noise ratios are desirable as evidenced by the following fundamental formula, derived by Claude Shannon, in 1948:

$$\text{Maximum data rate (bps)} = \text{carrier BW} \times \log_2 (1 + \text{signal/noise})$$

Thus increasing the bandwidth and/or the signal to noise ratio can improve the data rate. Consider, for example, a voice-graded line with signal to noise ratio of 1000 (a common line characteristic):

BW = 3000 Hz for a voice graded telephone line
$\log_2 (1 + 1000) = 10$ (approximately)
maximum data rate = 3000 x 10 = 30,000 bps

To improve the maximum data rate, the bandwidth and/or the signal to noise ratio needs to be improved. High bandwidth media are also desirable because they can support several users. For example, several telephone users can be supported on one high bandwidth cable. Different communication media with different bandwidths, signal/noise ratios, reliability and cost are currently being used in various networks. Examples of the commonly used media are open wire pairs, twisted pair cables, coaxial cables, fiber optic systems, and wireless media.

Satellites and Global Wireless Media. Communication through satellites is the foundation of global wireless systems and global networks in which users communicate with each other over long distances without a physical wire between them. A satellite is essentially a radio relay in the sky which receives signals from transmitting stations on earth and relays these signals back to the receiving stations on the earth (see Figure 9-5). The satellites are placed in the earth orbit at 22300 miles, called the Clark Belt after the famous science-fiction writer who first envisioned satellites in 1945. Once placed in the Clark Belt, the satellite rotates at the same speed as the earth's rotations so the satellite does not appear to move (called geo-synchronization). Thus the sending and receiving dishes can stay pointed to the satellite without any readjustments.

Satellites can provide high communications capacity and can support several thousand voice channels. However, each satellite message encounters a 0.25 second delay because of the distance a message has to travel between a sender and a receiver. In a satellite communication system, the transmission cost is independent of the distance between the sender and receiver (two stations 100 miles apart or 1000 miles apart still have to travel 22,300 miles to and from the satellite). Because of this, satellite communication systems are used to broadcast , i.e., send a message to several receivers simultaneously. Use of satellites, especially the broadcast services, presents serious security problems which require extensive encryption/decryption, such as scrambling and well protected keys. In addition to satellite systems, cellular telephones and residential cordless telephones (wireless systems) have been introduced in the mid 1980s. In cellular systems, the location of a sender/receiver is unknown prior to start of communication and can change during the conversation.

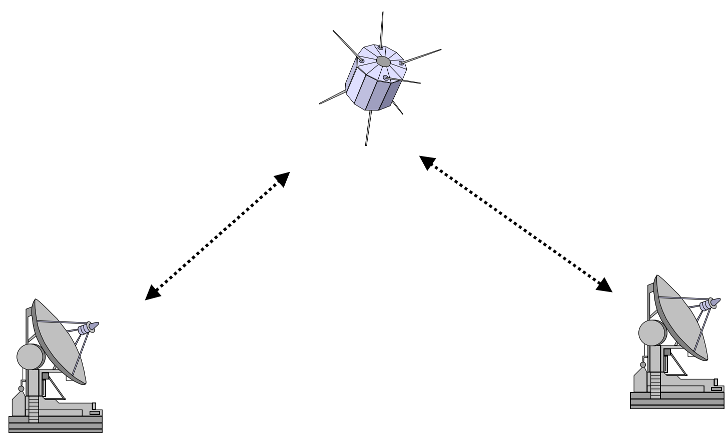


Figure 9-5: Satellite Transmission

9.2.3 Network Architectures

The architecture of any system describes the components (what are the pieces of a system?), the functions of components (what do they do?) and the interfaces/interactions between the components of a system (how do they interoperate with each other?). The following definition of computer architecture by Fred Brooks, author of "The Mythical Man-Month", distinguishes architecture from engineering:

"Computer architecture, like other architectures, is the art of determining the needs of the user of a structure and then designing to meet those needs as effectively as possible within economic and technological constraints. Architecture must include engineering considerations, so that the design will be economical and feasible; but the emphasis in architecture is upon the needs of the user, whereas in engineering the emphasis is upon the needs of the fabricator."

A ***network architecture*** defines the components, the functions and the interactions/interfaces (protocols/standards) between the components of a network. It encompasses hardware, software, standards, data link controls, topologies, and protocols. It defines the functions of, and the interfaces between, three types of components:

- Network hardware components such as cables, modems, communications controllers, adapter cards, etc.
- Communication software modules which establish and monitor sessions between remotely located processes and allow for exchange of data and control messages
- Application programs (user processes) which use the networks.

These components may be very simple or quite complex depending on the size of the network and the nature of devices supported (mainframes, minicomputers, microcomputers, terminals). Network architectures provide a systematic approach to describe the various categories of networks and define exactly what components will be supported and how. A ***protocol*** is a set of precisely defined rules of behavior between two parties. As we will see, protocols in network architectures define the formats and the rules of interaction between peers. Protocols play a key role in integration and interconnectivity in distributed systems.

Figure 9-6 presents a simple network architecture model. In this figure, several computers are connected to the network. One or more user applications (e.g., order processing) may run on each computer. Application Support Services "connect" the applications to the network. Network Services provide exchange of messages between the computers.
The functions performed by the application and network services vary widely between the size and complexity of networks and the stations. In the 1970s, these services were viewed as layers where each layer performed a specific function. Different researchers, vendors and standardizing bodies have proposed different layers. For example IBM's SNA (System Network Architecture) uses 7 layers; Department of Defense's Suite, commonly referred to as the TCP/IP Suite, uses 4 layers; and the OSI Reference Model uses 7 layers.

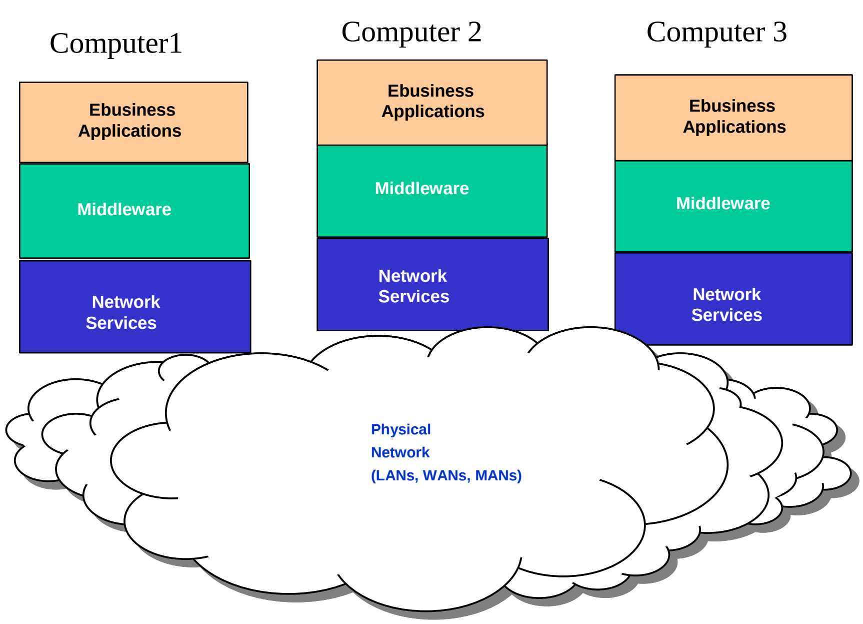


Figure 9-6: A Simple View of Network Architecture

Even though the number of layers differs between vendors, in all cases the lower layers provide low level (closer to the physical network) functions while the high level functions (application interfaces) are performed by the upper layers. For example, the first layer is physical link, the last is the application layer in most network architectures. In these layered systems, the data expands at the source as it goes through different layers (additional pieces of information are added as headers in each layer) and shrinks at the sink (headers are removed successively).

9.2.4 The Open System Interconnection (OSI) Reference Model

The Open System Interconnection (OSI) Reference Model, shown in Figure 9-7 specifies standards for networks from different vendors to exchange information with each other. The model describes network services in terms of 7 layers, but the lowest 4 layers are devoted to network services. These services are responsible for routing and transporting your messages in an error-free manner across a network. A common example of layered network protocols is the TCP/IP (Transmission Control Protocol/Internet Protocol) that is at the foundation of the Internet.

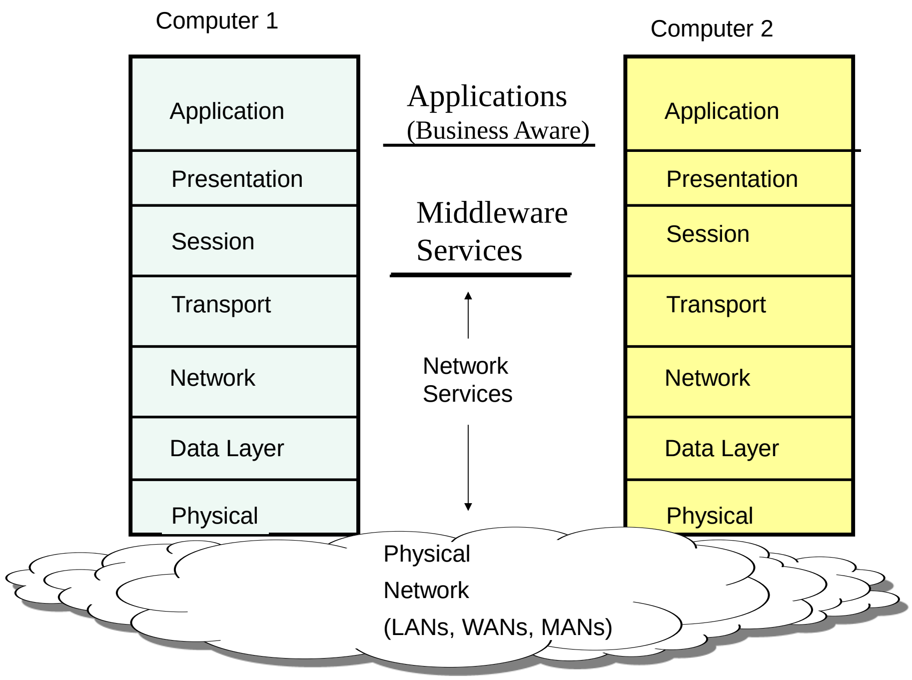


Figure 9-7: Conceptual View of OSI Network Model

9.2.5 Network Interconnectivity

Network interconnectivity is needed in large networks to provide interfaces and transport of messages between remotely located users, applications, databases, and devices. For example, if you access the Paris University Web site from Chicago, then many interconnectivity devices are used to get you from Chicago to Paris. The two principal network interconnectivity devices are:

- **Routers** find a path for a message in larger networks and then send the message over the selected path. Routers use very sophisticated routing algorithms and provide functionality such as "firewalls" for security checking.
- **Gateways** translate one type of protocol to another. In most large networks, protocols of some subnetworks need to be converted to protocols of other subnetworks for end to end communications. A gateway connects two dissimilar network architectures and is essentially a protocol converter. A gateway may be a special purpose computer, a workstation with associated

software (e.g., a PC with gateway software), or a software module which runs as a task in a mainframe. An example of gateways for network connectivity is the TCP/IP to Novell LANs.

Many routers and gateways are used commonly in enterprise networks and the general Public Internet. For example, if a salesman in Detroit needs to access a customer database in New York, then a series of routers and gateways would be needed to find the path between the two cities. Figure 9-8 shows a realistic enterprise network that uses TCP/IP very heavily, except the IBM SNA network (an old network technology) at the mainframe. The routers are used between all TCP/IP network segments and gateways are used to convert the TCP/IP messages to other protocols.

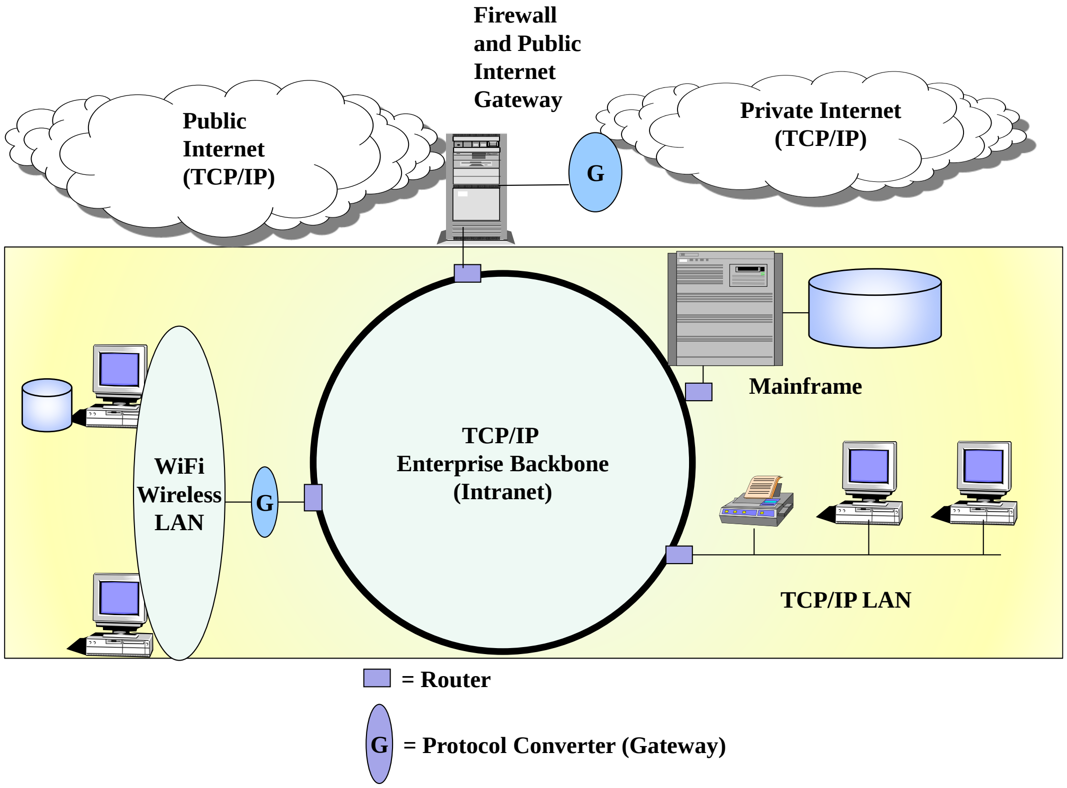


Figure 9-8: Network Interconnectivity in a Small Company

9.2.6 Broadband and Wireless Networks

The advancements in network transmission technologies have resulted in high data rate local and wide area transmissions, typically in the range of 100 million bits per second (Mbps) or higher (Gigabit networks). Examples of the evolving network communication technologies are Asynchronous Transfer Mode (ATM), Frame Relay, Fiber Distributed Data Interface (FDDI), and wireless networks. In general, networks are becoming faster, ubiquitous and more reliable. Another area of advancement is the integration of voice, data and video images for multimedia applications such as teleconferencing and group problem solving, among others. In particular, Next Generation Networks (NGNs) combine the voice and data networks into an integrated high speed network.

Wireless networks, as the name implies, interconnect devices without using wires -- instead they use the air as the main transmission medium. Wireless networks are enjoying widespread public approval with a rapidly increasing demand. The increase in the number of cellular phones, palm pilots, laptops, notebooks, and other handheld devices is phenomenal. To meet this demand, mobile communications technologies are emerging with digital speech transmission and the ability to integrate cordless systems into other networks. In the meantime, researchers are developing the next generation of technologies for several years to come.

The unique features of the wireless networks are:

- The bandwidths, and consequently data rates, of communication channels are restricted by government regulations. The government policies allow only a few frequency ranges for wireless communications.
- The communication channel between senders/receivers is often impaired by noise, interference and weather fluctuations.
- The senders and receivers of information are not physically connected to a network. Thus the location of a sender/receiver is unknown prior to start of communication and can change during the conversation.

A very large body of work on wireless networks exists with emphasis on different aspects such as radio transmission technologies, standards, protocols, systems engineering, and carriers. For our purpose, wireless networks can be broadly classified in terms of wireless local area networks, wide area networks and metropolitan area networks (see Figure 9-9).

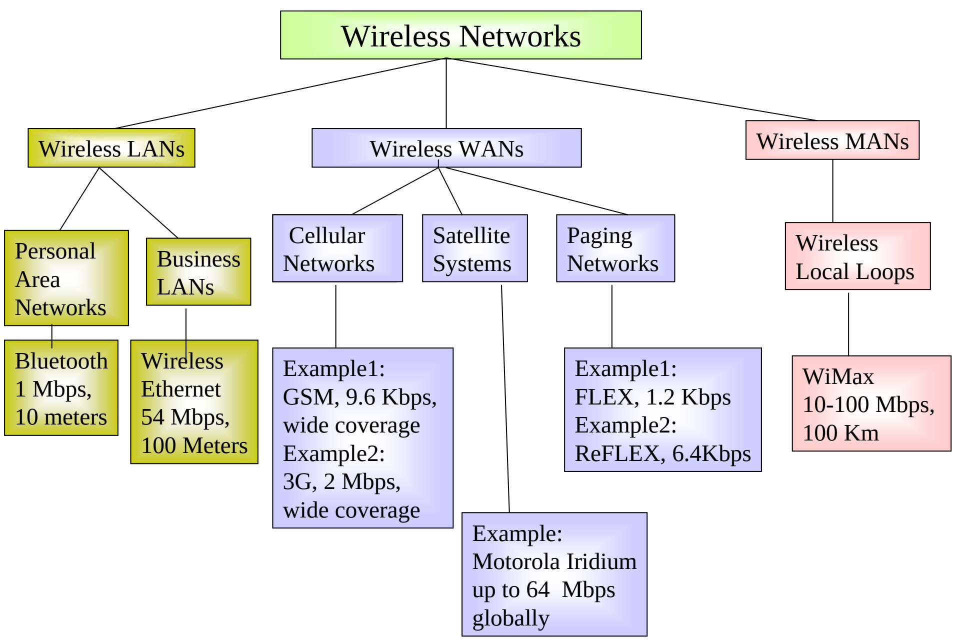


Figure 9-9: A View of Wireless Network Landscape

9.3 The Internet – A Network of Networks

9.3.1 The Internet at a Glance

Internet is of particular interest to e-business, since more than 80% of the e-business activities are expected to be conducted over the Internet. The origin of Internet is the ARPANET (Advanced Research Projects Agency Network) that was initiated in 1969 to support researchers on DOD (Department of Defense) projects. For many years, Internet was used mainly by scientists and programmers to transfer files and send/receive electronic mail. The users of Internet relied on text-based user interfaces and tedious commands to access remote computing resources. In 1989, this changed with the introduction of World Wide Web (WWW), commonly referred to as the Web. Technically speaking, Internet is a large collection of IP (Internet Protocol)-based networks that are interconnected through a wide range of interconnection devices. IP networks reside on a variety of physical network elements (e.g., fiber optics and wireless networks) to support Web technologies.

Figure 9-10 shows a conceptual view of the Internet. This "Big Person with Narrow Waist" model highlights the role of the IP (Internet Protocol) in supporting ever-growing web-based applications and real-time moving video operations on top of a very large number of physical communication devices that span wired and wireless networks. The IP (the narrow waist) basically serves as the glue that supports the large body of applications over an even larger family of network devices.

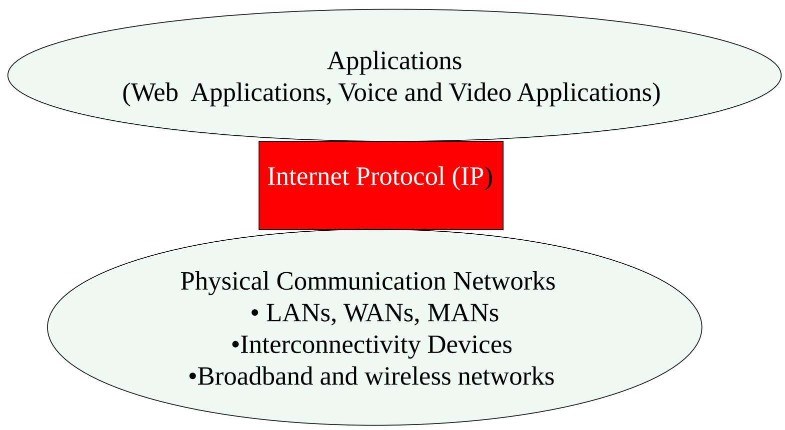


Figure 9-10: A Conceptual View of the Internet (The "Big Person with Narrow Waist" Model)

The Web has been a major contributor in turning the Internet, once an obscure tool, into a household word. The Web allows users to access, navigate and share information around the globe through GUI clients ("Web browsers") that are available on almost all computing platforms. The Web browsers allow users to access information that is linked through hypermedia links. Thus a user transparently browses around, or "surfs" around, different pieces of information that is located on different computers in different cities and even in different countries. In addition to Web, the IP-based networks are being used for a wide range of applications such as Internet Telephony, video conferencing, and corporate computing.

Technically speaking***, Internet*** is a network based on the TCP/IP protocol stack. At present, the term Internet is used to refer to a large collection of TCP/IP networks that are tied together through network interconnectivity devices such as routers and gateways . The TCP/IP (Transmission Control Protocol/Internet Protocol) was developed in the late 1960s and early 1970s by the Defense Advanced Research Projects Agency (DARPA). TCP/IP was developed for interconnecting many computers in the ARPANET (Advanced Research Projects Agency Network). ARPANET initially consisted of five protocols (indicated with * in the following list) that have been augmented with other key protocols (see Figure 9-11):

- *Internet Protocol (IP) for interconnecting and routing messages to a large number of physical networks
- *Transmission Control Protocol (TCP) for reliable information transfer
- User Datagram Program (UDP) for fast, but unreliable, information transfer
- *File Transfer Protocol (FTP) for file transfer
- *Simplified Mail Transfer Protocol (SMTP) for email

- *Terminal emulator (Telnet) for terminal emulation
- Domain Name Services (DNS) to translate an address such as www.mycorp.com to a physical IP address such as 192.28.200.32
- Hypertext Transfer Protocol (HTTP) for Web applications
- Real Time Protocol (RTP) for audio and video applications

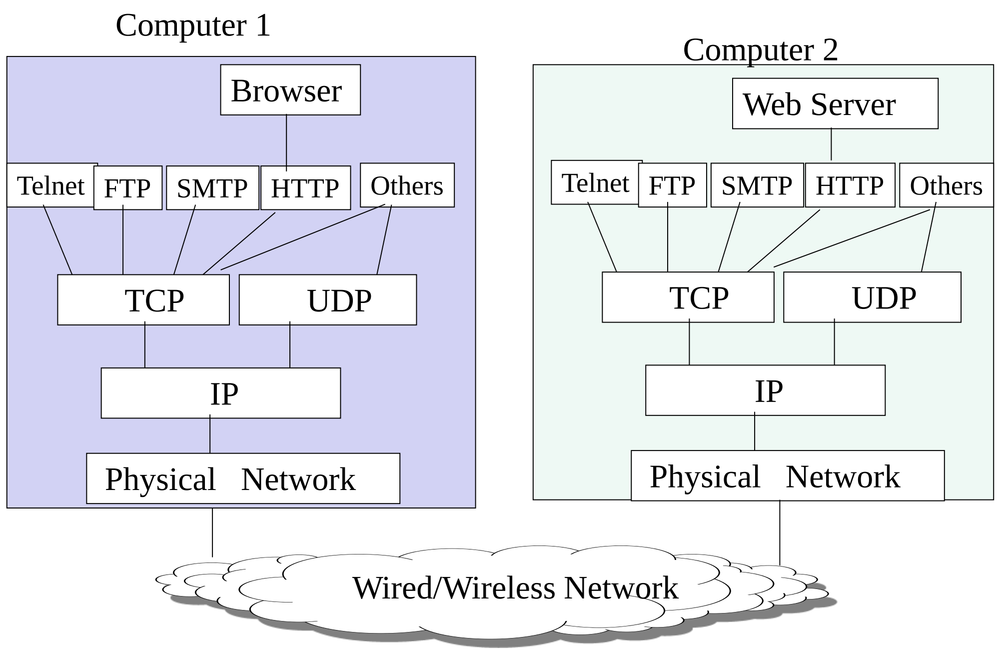


Figure 9-11: The IP Stack – Foundation of Internet

Although, the Internet at present uses TCP (i.e., higher level protocols and applications are based on TCP), this may not be true in the future since some future (especially real time) applications may be built directly on IP or newer alternatives to TCP. The main strength of IP is that it runs on top of a very diverse array of physical networks (wide area, local area, wireless) . In fact, IP supports almost all current physical network technologies and is expected to support most of the future high speed networks. We thus will use the following simple definition of the Internet:

Definition: Internet is a network of networks that is supported by the Internet Protocol (IP).

What does this mean? Basically it says that you need to have an IP network (or a gateway that translates to IP) to join the Internet. Once you have an IP network, then you can run almost any physical network under it and take advantage of voice, data, or video applications for your e-business that run on top of IP. At present, the term Internet is used to symbolize a Public Internet that is not owned by any single entity -- it consists of many independent IP networks that are tied together loosely.

9.3.2 Routing in the Internet

Initially, the public Internet was used to tie different university networks together. With time, several commercial and private networks have joined the public Internet. The computers on the public Internet have publicly known Internet Protocol (IP) addresses that are used to exchange information over the public Internet (we will discuss IP addresses later). The public Internet at present consists of millions of computers (PCs, Macs, Sun workstations, HP systems, IBM mainframes) that are interconnected through thousands of networks that use different underlying network technologies (ATMs, frame relays, Ethernet LANs, and wireless networks) in different parts of the world. All these computers and networks are tied together through a global IP network (see Figure 9-12).

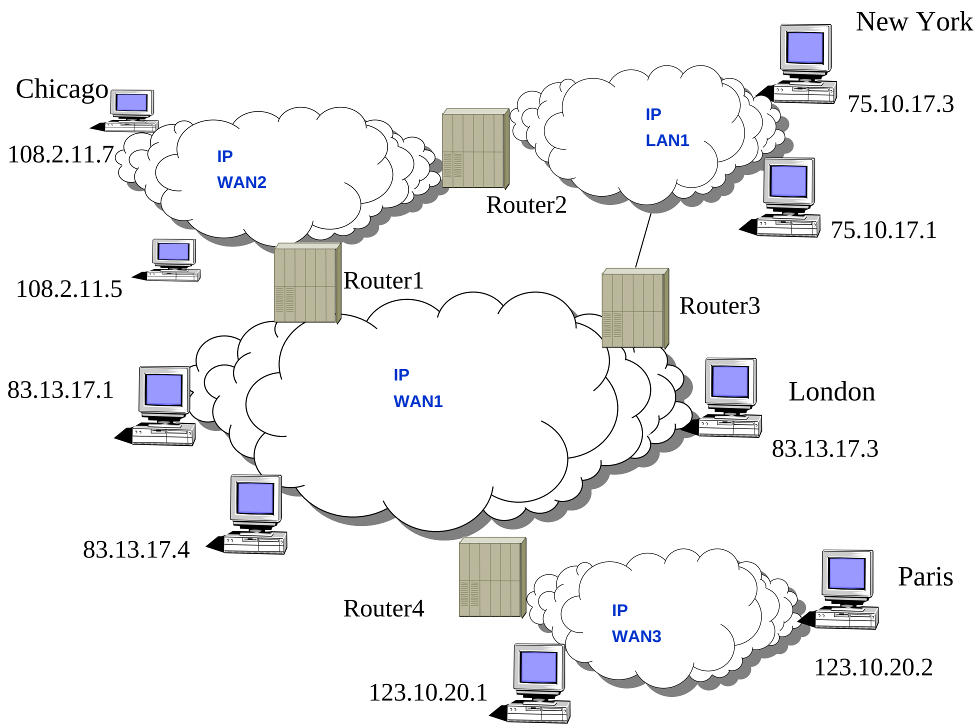


Figure 9-12: Public Internet – A Global IP Network

9.3.3 Private Value Added Networks (VANs)

E-commerce (EC) requires network services, of course, but also additional "value added" services such as purchasing and billing. Similarly, telephone network users also typically need value added services such as voice mail, call forwarding, and caller ID. Some networks, known as value added networks (VANs) bundle the value added services in addition to network transport services. Many VAN vendors such as GEIS, AT&T, and Harbinger support EC activities through very reliable, secure and well managed private data networks and proprietary technologies. In particular, these networks support purchasing and billing quite well (i.e., purchasing by sending purchase orders and billing by supporting invoices). The well known EDI standards X850 (for purchase orders) and X810 (for invoices) are examples of VAN services for EC. However, these networks were never designed for general public advertising and browsing. In addition, VANs for EC are too expensive and require too many proprietary interfaces and software modules to support advertising and browsing services for a large number of trading partners. In many cases, the traditional proprietary VANs for EC are finding it tough to compete with the Internet-based value added services. .

9.3.4 Extranets and Virtual Private Networks (VPNs)

"Extra-net" or "enterprise intra-nets" are semi-private IP networks which are used to communicate within a group of interdependent communities of enterprises or trading partners. Examples of such a group of interdependent community would be the automotive industry (including parts suppliers, manufacturers, retailers, and insurers), the health care industry (including physicians, pharmacists, hospitals, labs, and health insurers), or the real estate industry (including brokers, lending agencies, insurers, lawyers, and inspectors). To succeed, Extranets need to support high quality EC services (e.g., advertising, browsing/selection, purchasing, billing, and payments) coupled with security and management considerations.

An *Extranet* consists of a collection of Internet segments (intranets), each protected by firewalls, which are interconnected using secure leased lines across the remote locations. This solution provides security and guaranteed bandwidth, at the cost of leasing lines from telecomm providers. In contrast, *Virtual Private Networks* (VPNs) achieve a similar goal (that is, securely connecting remote locations, branch offices, field workers, telecommuters, vendors, customers, and suppliers) using the public Internet instead of leased lines. Specifically, VPNs encrypt the messages to provide security.

Internet Role Players

- Different individuals, groups and organizations play different roles in the Internet. To illustrate these roles, let us envision the Internet as an electronic shopping mall. Then we can discuss the following roles:
- Internet users are the people who visit the shopping mall (i.e., logon to the Internet). The Internet users are essentially the consumers of the services provided by the Internet.
- Content providers are the merchants (individuals, groups or organizations) that provide the products in the shopping mall (i.e., resources available on the Internet). You can think of these content providers as the merchants in the shopping mall.
- Internet access providers (IAPs) are the organizations that facilitate your access to the shopping mall (i.e., give you a communication line and an access port on the Internet). You can think of IAPs as the local authorities that provide you with roads and signs to get you to the shopping malls.
- **Internet** service **providers (ISPs)** are the individuals and organizations that help the content providers set up their shops in the shopping mall (i.e., help in building Web sites). Many small content providers seek the help of ISPs to set up Web servers with appropriate security and backup/recovery.

9.3.5 Next Generation Internet (NGI)

As we all know, the origin of Internet is the US Government funded ARPANET project. Buoyed by the enormous success of Internet and keeping up with the spirit, the US Government is now focussing on the future Internet. The NGI initiative is a US Federal research and development program, initiated in 1997, for developing advanced networking technologies and innovative applications that require 100 to 1,000 times faster end-to-end networks than today's Internet.

The goals of NGI, according to the NGI initiative (www.ngi.gov) are:

- Conduct R&D in advanced end-to-end networking technologies.
- Conduct R&D in revolutionary applications. This includes enabling middleware and a wide range of applications in basic and applied sciences.

Figure 9-13 shows a conceptual view of NGI. In essence it combines and extends the NGN and IPng to support future innovative applications. The NGI testbed will be built on a variety of networks such as NSF's very high performance Backbone Network Service (vBNS), NASA's Research and Education Network (NREN), DoD's Defense Research and Education Network (DREN), and the private sector's Abilene network

The NGI initiative is managed, at a high level, by the White House National Science and Technology Council. This work is providing funds to R&D organizations for open technology development and transfer. This strategy, which contributed to the success of the original Internet, promotes good ideas through funding and encourages deployment of new products and services. A quick overview of the initiative is given below. For more details, see the URL (www.ngi.gov).

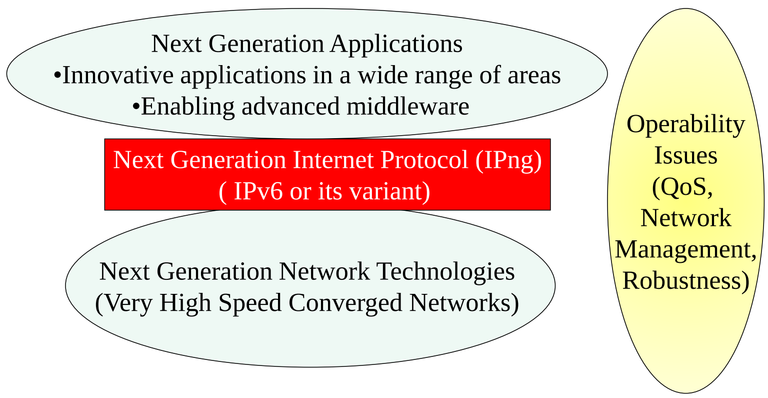


Figure 9-13: Next Generation Internet

9.3.5.1 Advanced Network Technologies

High speed networks that can move bits at 100 million bits per second (Mbps) to 1 billion bits per second (Gbps) are required for NGI. However, next generation Internet is not merely faster movement of bits. NGI involves faster networks with richer, more flexible, and affordable network service technologies needed by next generation applications such as high-quality team collaboration and videoconferencing. The main areas of network services and corresponding protocols of interest to NGI are: multicast, network management (including allocation and sharing of bandwidth), optical networking, quality of service / differentiation of service (including multicast and video), reliability, robustness, and security.

9.3.5.2 Revolutionary Applications

NGI involves R&D in revolutionary applications. These applications include: basic science, crisis management, education, the environment, health care, manufacturing, among others. The emphasis is on new and revolutionary applications instead of extensions of existing applications. These applications are expected to be highly interactive and collaborative. This will need enabling middleware technologies such as collaboration technologies, digital libraries, distributed computing, multi-megabit wireless, nomadic computing, privacy and security, remote operation and simulation.

9.3.5.3 Next Generation Internet Testbed

The networks developed under the NGI initiative will connect more than a hundred NGI sites at speeds 100 times faster than today's Internet. These sites (funded government agencies, universities, and industrial research labs) need to show end-to-end connectivity (to the workstation) at speeds from 100+ Mbps up to 1+ Gbps. This means end-to-end user connectivity at 100 to 1000 Mbps (although several backbone links at present operate at 1+ Gbps, the end user connectivity is typically at 10 Mbps because of network bottlenecks). The testbed will be a a wide-area demonstration network fabric that will function as a distributed laboratory, delivering greater than 100+ Mbps end-to-end to at least 100 interconnected NGI sites demonstrating highly important applications. Another area of research worth mentioning is Active Networks (see the sidebar "Active Networks").

Active Networks

Active networks allow routing elements to be programmed by the packets passing through them. This allows computations to be carried out within the network instead of the edges. Active networks is a research effort, funded by DARPA (http://www.darpa.mil/ito/research/anets/) with the goal of producing a new networking platform. The Active Network program is intended to produce a flexible network that can be extended at runtime to accommodate the future sophisticated defense applications.

Active networks are based on the notion of a "Smart Packet". The smart packet is an agent with the goal of delivering itself to its destination. The goal is expressed through a portion of the packet that describes its "method" -- a set of instructions that can be interpreted consistently by the Active Network nodes. Thus the packet can have a program that can sense the status of network and route itself as it fights through the network jungle. This is in contrast to the current "dumb" packets that just know their origin and destination addresses -- they are shuffled back and forth by the routers. The smart agents basically have a routing algorithm imbedded in them that can be modified as they go along. The smart packets can be engineered to allow security, reliability, availability and quality of service under a wide range of conditions.

Additional information about the active networks can be found at the DARPA site (http://www.darpa.mil/ito/research/anets. Pointers to research papers on this topic can be found at http://www.cis.upenn.edu/~switchware/.

Suggested Review Questions Before Proceeding

- What role do networks play in the modern enterprises. List three examples.
- What is the OSI model and how it is used to describe interconnectivity
- What are the tradeoffs between wireless and wired networks? How do broadband networks fit into this picture?
- What is the technical definition of the Internet and what are the key protocols used in the Internet?

9.4 Web at a Glance

9.4.1.1 Web Overview

Technically speaking, WWW is a collection of technologies that operates on top of the IP networks (i.e., the Internet). Figure 9-14 shows this layered view. The purpose of the WWW technologies is to support the growing number of users and applications ranging from entertainment to corporate information systems. Like many other (successful) Internet technologies, the first generation of WWW is based on a few simple concepts and technologies such as the following:

- Web servers

- Web browsers
- Uniform Resource Locator (URL)
- Hypertext Transfer Protocol (HTTP)
- Hypertext Markup Language (HTML)
- Web navigation and search tools
- Gateways to non-Web resources

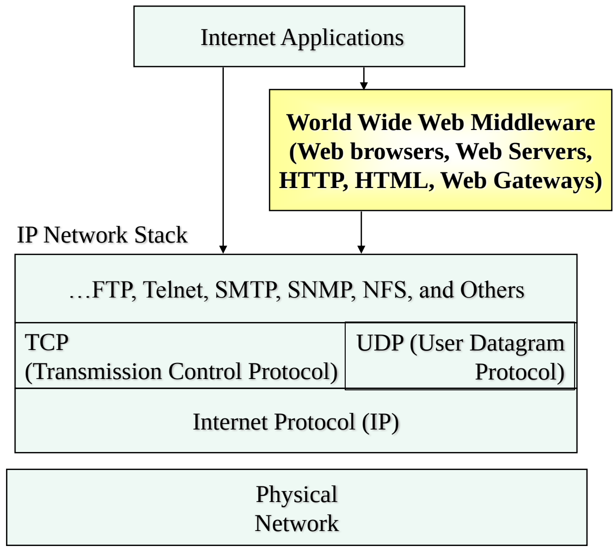


Figure 9-14: Technical View of World Wide Web

Let us briefly review these components and show how they tie in with each other through an example shown in Figure 9-15.

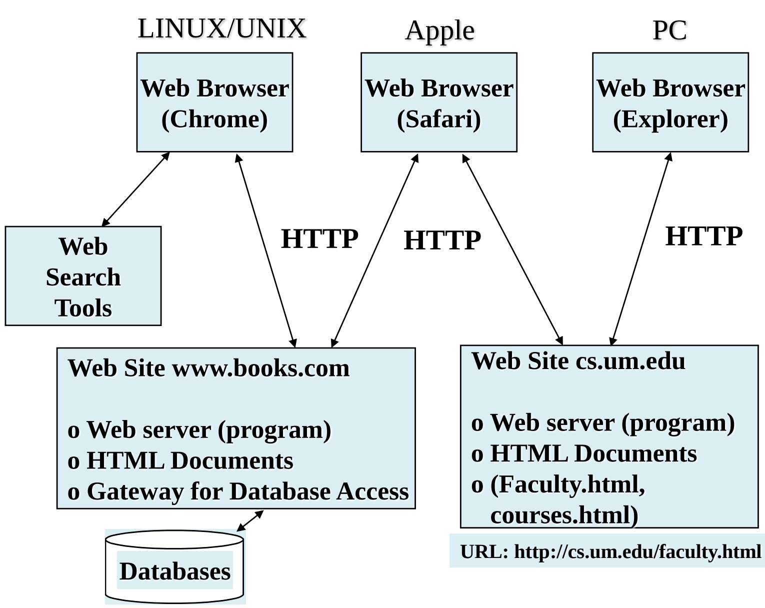


Figure 9-15: Conceptual View of World Wide Web

Web sites provide the content accessed by Web users. Web sites are populated and in many cases managed by the content providers. For example, Web sites provide the commercial presence for each of the content providers doing business over the Internet. Conceptually, a Web site is a catalog of information for each content provider over the Web. In reality, a Web site consists of three types of components: a Web server (a program), content files ("Web pages") and/or gateways (programs that access non-Web content). A Web server is a program (technically a server process) that receives calls from Web clients and retrieves Web pages and/or receives information from gateways (we will discuss gateways later). Once again, a Web user views a Web site as a collection of files on a computer, usually a UNIX, Linux or Windows machine. In many cases, a machine is dedicated/designated as a Web site on which Web accessible contents are stored. As a matter of convention, the entry point to a Web site is a "home page" which advertises a company business. Very much like storefront signs in a shopping mall, the home pages include a company logo, fancy artwork for attention, special deals, overviews, pointers to additional information, etc. The large number of Web sites containing a wide range of information tto be navigated and searched transparently by Web users is the main strength of WWW. Figure 9-15 shows two Web sites -- one for a book store (www.books.com) and the other for a computer science department for a university (cs.um.edu). Web sites and Web servers are explained later.

Web browsers are the clients that typically use graphical user interfaces to wander through the Web sites. The first GUI browser, Mosaic, was developed at the National Center for Supercomputer Applications at the University of Illinois. At present, Web browsers are commercially available from Microsoft, Google and many other software/freeware providers. These Web browsers provide an intuitive view of information where hyperlinks (links to other text information) appear as underlined items or highlighted text/images. If a user points and clicks on the highlighted text/images, then the Web browser uses HTTP to fetch the requested document from an appropriate Web site. Web browsers are designed to display information prepared in a markup language, known as HTML. We will discuss HTTP and HTML later. Three different browsers are shown in Figure 9-15. Even though these are different browsers residing on different machines, they all use the same protocol (HTTP) to communicate with the Web servers (HTTP compliance is a basic requirement for Web browsers).

Many browsers are relatively dumb (i.e., they just pass user requests to Web servers and display the results). However, this has changed because of Java, a programming language developed by Sun Microsystems. Java programs, known as Java applets, can run on Java compatible browsers. This has created many interesting possibilities where Java applets are downloaded to the Java enabled browsers where they run producing graphs/charts, invoking multimedia applications, and accessing remote databases. Several other capabilities such as Flash have been added to the browsers.

Uniform Resource Locator (URL) is the basis for locating resources in WWW. A URL consists of a string of characters that uniquely identifies a resource. A user can connect to resources by typing the URL in a browser window or by clicking on a hyperlink that implicitly invokes a URL. Perhaps the best way to explain URLs is through an example. Let us look at the URL "http://cs.um.edu/faculty.html" shown in Figure 9-15. The "http" in the URL tells the server that an HTTP request is being initiated (if you substitute http with ftp, then an FTP session is initiated). The "cs.um.edu" is the name of the machine running the Web server (this is actually the domain name used by the Internet to locate machines on the Internet). The "/faculty.html" is the name of a file on the machine cs.um.edu. The "html" suffix indicates that this is an HTML file. When this URL is clicked or typed, the browser initiates a connection to the "cs.um.edu" machine and initiates a "Get" request for the "faculty.html" file. Depending on the type of browser you are using, you can see these requests flying around in an appropriate window spot. Eventually, this document is fetched, transferred to the Web browser and displayed. You can access any information through the Web by issuing a URL (directly or indirectly). As we will see later, the Web search tools return a bunch of URLs in response to a search query. The general format of URL is:

protocol://host:port/path

where

protocol represents the protocol to retrieve or send information. Examples of valid protocols are HTTP, FTP, Telnet, Gopher, and NNTP (Network News Transfer Protocol).

host is the computer host on which the resource resides

port is an optional port number (this is not needed unless you want to override the HTTP default port, port 80)

path is an identification, typically a file name, on the computer host.

Hypertext Markup Language (HTML) is an easy-to-use language that tags the text files for display at Web browsers. HTML also helps in creation of hypertext links, usually called hyperlinks, which provide a path from one document to another. The hyperlinks contain URLs for the needed resources. The main purpose of HTML is to allow users to flip through Web documents in a manner similar to flipping through a book, magazine or a catalog. The Web site "cs.um.edu" shown in Figure 9-15 contains two HTML documents: "faculty.html" and "courses.html". HTML documents can imbed text, images, audio, and video. The current version of HTML (HTML5) heavily support s multimedia presentations. A sample of HTML is shown in the sidebar " **Example of HTML".**

Hypertext Transfer Protocol (HTTP) is an application-level protocol designed for Web users. It is intended for collaborative, distributed, hypermedia information systems. HTTP uses an extremely simple request/response model that establishes connection with the Web server specified in the URL, retrieves the needed document, and closes the connection. Once the document has been transferred to your Web browser, then the browser takes over. Keep in mind that every time you click on a hyperlink, you are initiating an HTTP session to transfer the needed information to your browser. The Web users shown in Figure 9-15 access the information stored in the two servers by using the HTTP protocol.

Web navigation and search services are used to search and surf the vast resources available over the "cyberspace". The term, cyberspace, as stated previously, was first introduced through a science fiction book by [Gibson 1984] but currently refers to the computer-mediated experiences for visualization, communication, and browser/decision support. The general search paradigm used is that each search service contains an index of information available on Web sites. This index is almost always created and updated by "spiders" that crawl around the Web sites chasing hyperlinks for different pieces of information. Search engines such as Google support keyword and/or subject-oriented browsing through the index.

Gateways to non-Web resources are used to bridge the gap between Web browsers and the corporate applications and databases. Web gateways are used for accessing information from heterogeneous data sources (e.g., relational databases, indexed files and legacy information sources) and can be used to handle almost anything that is not designed with an HTML interface. The basic issue is that the Web browsers can display HTML information. These gateways are used to access non-HTML information and convert it to HTML format for display at a Web browser. The gateway programs typically run on Web sites and are invoked by the Web servers. At present, Common Gateway Interface (CGI) is used frequently. We will discuss CGI gateways and other types of Web gateways later in this chapter. "Relational gateways" that provide access to relational databases from Web browsers are an area of active work.

Example of HTML

Web Browser View

Consulting Group1

Welcome to our consulting group. You can do the following:

- Read about our services
- Access home pages of the groups we work with (WWW)

Now choose the connections by clicking on the following

- Our services
- WWW Information

HTML

The following HTML statements can be used to design this home page (we have inserted appropriate URL's for the hot links):

```
<TITLE>Consulting Group1 </TITLE>
<H1>Consulting Group1 </H1>
<P> Welcome to our consulting group. You can do
    the following:
<UL>
<LI> Read about our services .
<LI> Access home pages of the groups we work with
    (WWW)
</UL>
<P> Now choose the connections by clicking on the
    following
<a href="http://www.myserver.com/services.html">
    Our services</a>
<a href="http://www.w3.org"> WWW
    Information</a>
```

9.4.1.2 A Simple Example

Figure 9-16 illustrates how the Web components can be used for purchasing from a department store, "Clothes.com". This store wants to advertise its products on the Web, (i.e., wants to be a Web content provider). The store first designates a machine, or buys services on a machine, called "clothes.com" as a Web site. It then creates an overview document, "overview.html", that tells the potential customers of the product highlights (think of this as the first few pages of a catalog). In addition, several HTML documents on the Web site for different types of clothes (men.html, women. html, kids.html) are created with pictures of clothes, size information etc. (once again think of this as a catalog). We can assume that the overview page has hyperlinks to the other documents (as a matter of fact, it could have hyperlinks to other branches of Clothes.com). In reality, design of the Web pages would require a richer, deeper tree structure design as well as sequential links for alphabetical and keyword searches needed to support the "flipping through" the catalog behavior.

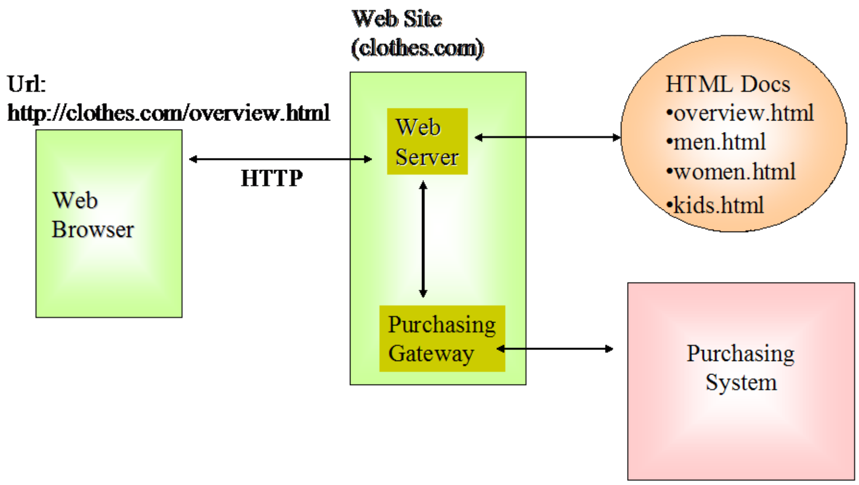


Figure 9-16: Conceptual View of an Internet-based Purchasing System

Once HTML documents have been created on the Web server, an Internet user can browse through them as if he/she is flipping through a catalog. The customers typically supply the URL, directly or indirectly, for the overview (http://clothes.com/overview.html) and then use the hyperlinks to look at different types of clothes. Experienced customers may go directly to the type of clothes needed (e.g., men may directly go to the "men.html" document). As shown in Figure 9-16, the URL consists of three components: the protocol (http), the Web server name (clothes.com), and the needed document (overview.html). HTTP provides the transfer of information between the Web users (the clients) and the Web Servers.

At first, clothes.com is only using Web to store an electronic catalog. After a customer has browsed through the catalog and has selected an item, he/she calls the store and places an order. Let us say that clothes.com also wants the customers to purchase the items over the Internet. In this case, a "Purchasing Gateway" software is developed and installed at the Web site. This gateway program gets into action when a user clicks on the "purchase" button on his screen. It prompts the user with a form (HTML supports forms) that the user fills out. The gateway program uses this form information to interact with a purchasing system that processes the purchase (see Figure 9-16). The purchasing system can be an existing system that is used for traditional purchasing. The role of the gateway is to provide a Web interface to the purchasing system. We will discuss gateways later in this chapter.

XML Overview

XML is a markup language, similar to HTML, for documents containing structured information. The main limitation of HTML is that it only concentrates on presentation (i.e., headers, highlights, etc) . If you need to specify, for example, the structure of information (i.e., represent customer name and address), then HTML cannot help. Before going into details, let us quickly show a very simple example of XML. The following statements represents an XML document that contains customer name and address:

```
<CUSTOMER>
        <NAME> Joe </NAME>
        <ADDRESS> NY </ADDRESS>
        <AGE> 33 </AGE>
```

</CUSTOMER>

You can see the striking resemblance between HTML and XML, at least at this simple level (i.e., tags in the format <tag> that are terminated by </tag>). As we will see, you can develop XML documents that represent customers, orders, bills, airline schedules, TV programs, bank statements, catalogs, etc. by just creating new tags. XML is very popular at present with applications ranging from e-commerce to music.

9.4.2 Web 2.0 and Social Networking

Web 2.0 has gained popularity since the mid 2000s. Although there are many definitions, Web 2.0 is commonly used to describe the trend in the use of Web technology to enhance collaboration among users, promote a democratic model where all users can create and share content, and encourage user creativity. Broadly speaking, the term Web 2.0 is used to represent the new and innovative way in which Web is being *used* . In addition, Web 2.0 also embodies a few new technologies that are *supporting* and fueling this new use. Web Services that combines components and Web technologies is a dominant technology in Web 2.0.

In Web 2.0, users can own the data on a site and exercise control over that data. In traditional websites, the users are limited to viewing the content that the site owner provides. Web 2.0 sites often feature a rich, user-friendly interface based on Ajax, Flex or similar rich media. The sites may also have social-networking aspects. Simply stated, a social network allows users to build online communities to share interests and to explore the interests and activities of others. Users can upload pictures, songs, videos and other artifiacts. Some social networks offer additional features, such as the ability to create groups for users with common interests or hold discussions in forums.. With increased features, social networking has grown dramatically and has become part of everyday life. The types of social networking services include dating clubs, friendships, and recommender systems. In addition, numerous social networking sites have sprung up catering to different countries, languages and cultures. Facebook is a good example of social networks (see the sidebar below).

Web Services directly support components that can be invoked over the Internet. The main idea of Web Services (WS) is quite simple – combine Web and components into a single framework where the user to component as well as component to component interactions are conducted by using standard Web technologies. In other words, a WS component defines a set of services that can be invoked from a browser or another WS component. XML is used for information exchange and messages are delivered by using HTTP. WS supports description, publication, discovery, selection, and binding of services over standard Web protocols. In essence, WS:

- provides discrete building-block applications (business components) based on XML that connect to each other and other larger applications over the Internet.
- supports a standard means to describe what services are provided by applications (business components) and to make the service available to others.
- is designed to be accessed directly by another service or software application (unlike Web sites, which are pictures of data designed to be viewed in a browser by a person).
- allows applications to share data, and invoke capabilities from other applications without regard to how those application were built, what platform they run on, and what devices are used to access them.

Example of Web 2.0 and Social Networking: Facebook

Facebook is a web-based social networking application used by millions of people every day. Utilizing the very latest web technologies, it has evolved into a comprehensive platform for online communication with friends, family, and co-workers. Facebook is one of the very first Web 2.0 companies, putting the users in control of content and syndicating that user-driven content through a variety of web services both internal and external to the web site. Facebook has utilized many of the latest web technologies to revolutionize the way people live and communicate on the internet.

At the core of Facebook is each individual person's page. In the early days of Facebook (the company was founded in 2004), this page contained little more than a basic profile very encyclopedic in nature. However, over time and with the help of several different web 2.0 features and applications, this basic profile evolved into a dynamic, content-rich page containing pictures, messages, and even mini-embedded applications.

In terms of specific technologies used, Facebook is a heavy implementer of AJAX (Asynchronous JavaScript and XML) which creates a desktop application-like look and feel and a very simple, intuitive user interface. AJAX also minimizes the number of page loads and reduces wait time for the end user. In 2006, Facebook adopted its own internal version of RSS feeds, called "news feeds," used to publish one user's recent activity out to all of their friends who subscribe.

In 2007, Facebook took another major step by launching the Facebook Platform, a framework for third-party developers to create applications that run directly on the Facebook website. Providing extensive API functionality, this platform fundamentally shifted Facebook away from the traditional website model and more to a service-oriented architecture where users can pick and choose the web services they want. This was an industry-shaping move that was mimicked by many other companies and products such as MySpace and Apple's iPhone.

Source: http://www.facebook.com

9.4.3 Transaction Processing Support for eCommerce

Business transactions are at the core of electronic commerce (EC). Examples of typical EC transactions are purchasing, claim processing, and billing/payment. For business to business activities in EC, the importance of supporting highly reliable and secure business transactions is quite obvious. Basic knowledge of transaction processing is essential for developing "serious" websites that handle billing, payment, credit card processing and other financial services.

Formally, a *transaction* is a collection of operations on a database which has the so-called ACID properties:

- **Atomicity**: All of the operations in the transaction must take place, or none must take place. In practice, if any of the elementary steps that are part of the transaction action fails, then all the steps must be undone;
- **Consistency**: The result of performing all the operations in the transaction is to take the database from one consistent state to another consistent state;

- **Isolation**: Other users of the database are isolated from any intermediate states of the transaction, i.e., they may see the state of the database before the transaction begins or after it completed, but not any state in the middle;
- **Durability:** Once all the actions in the collection have completed, the effects endure even in the event of system crashes.

EC is a mixture of decision support and transaction processing activities. Normally, only a portion of the core EC activities are transactional. Two main types of EC transactions are relevant:

- EC transactions between trusted business partners (e.g., suppliers and corporations that enter business agreements and contracts to buy and sell products). These transactions typically are large in volume (large amounts of money and goods), introduce medium traffic, and require rigorous security. These transactions are perfect candidates for Extranets.
- EC transactions between suppliers and the general public (e.g., Internet shopping malls)

Transactional support is implemented differently in different types of systems. For centralized mainframe systems, on-line transaction processing (OLTP), has been built for ACID transactions and has been a backbone of commercial data processing since the early 1970s. Mainframe-based transaction managers (TMs) such as CICS and IMS-DC/IMS-TM have matured over the years to provide high performance and reliable services The situation is dramatically different in distributed environments that characterize EC:

- TP-Less, i.e., do not use any transaction management facilities;
- TP-Lite, i.e., use database procedures to handle updates;
- TP-Heavy, i.e., use a distributed transaction manager to handle updates.

Which one of these approaches works depends on the type of EC activities being considered. It appears that each one of these approaches have certain pluses and minuses for EC. The following questions should be asked before deciding on the approach:

- In what format is the data stored (databases, flat files)? If the data is stored in multiple databases and flat files, then TP-Lite is not suitable (database procedures only work in RDBMS environments);
- How many SQL servers does the data reside on? If the application needs to update and commit data that is stored on multiple servers, then TP-Heavy should be used (database procedures cannot participate with other database procedures in a distributed transaction).
- What is the requirement for data synchronization? If the data synchronization interval is periodic, then a TP-Lite solution combined with a data replication server may be useful to handle updates against replicated data.
- What are the requirements for performance and load balancing?

TP-Less works well when you do not need any transaction processing capabilities. TP-Lite solutions with database procedures are much faster, on the surface, than the TP-Heavy solutions that require synchronization between sites. But TP-Heavy solutions provide many sophisticated procedures for dynamic load balancing, priority scheduling, process restarts, and pre-started servers that are especially useful for large scale production environment. These features are the main strength of TP-Heavy products because many of these products have been used over the years to handle thousands of transactions in production OLTP (on-line transaction processing) environments. Figure 9-17 shows a basic model of a distributed transaction processor that may use TP-Heavy in distributed environments. The protocol used in this case is two phase commit.

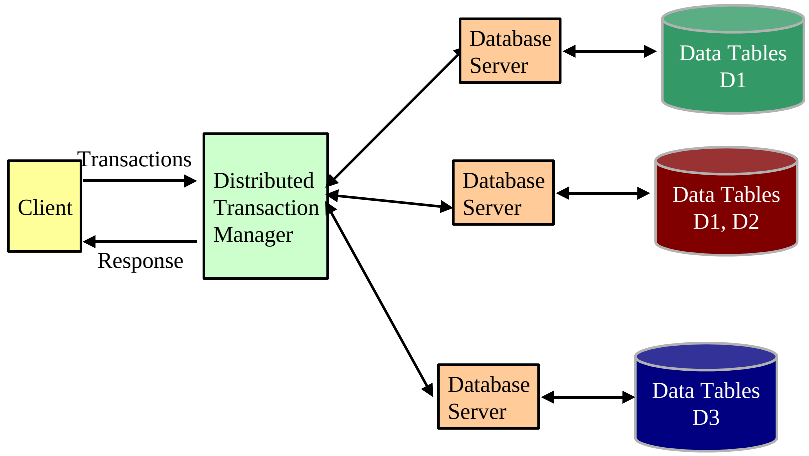


Figure 9-17: Models of Distributed Transactions

While the debate between the TP-Lite and TP-Heavy proponents continues, most EC projects are completely ignoring this whole issue by focusing primarily on EDI and in some sense re-inventing the wheel. EDI, at best, is a TP Less approach. Some EC applications are being deployed by using TP-Lite while large mission critical EC applications, if any, use TP-Heavy only at back-end mainframe systems. In the meantime, it seems that many small EC applications are quite happy with TP-Less.

9.5 Mobile Computing and Wireless Communications

9.5.1 Overview of Wireless

Guglielmo Marconi invented the wireless telegraph in 1896. By encoding alphanumeric characters in analog signals, he sent telegraphic signals across the Atlantic Ocean. This led to a great many developments in wireless communication networks that support radio, television, mobile telephone, and satellite systems that have changed our lives. The wireless networks themselves have improved tremendously with notable advances in cellular networks, satellite communications, and wireless local area networks. More recently, many mobile computing applications (computing applications that run partially or completely on mobile devices) have emerged that fully exploit the capabilities of wireless networks and mobile devices. The end result is numerous developments with far-reaching impact on business, education, entertainment, and daily lifestyles. Some of the examples were highlighted in the opening vignette, “Wireless in Action – A Few Snippets.”

Mobile computing and wireless communications have created several opportunities because of the appeal of wireless communications – typified by the overused slogan of “communications anytime and anywhere.” However, these developments have also raised several technical and business issues and have introduced a tremendous amount of jargon and new terms. Mobility involves several levels of issues that include wireless networks, computing platforms, middleware services, and applications. These issues are cast into a framework, shown in Figure 9-18, that will be used in this section to introduce the key building blocks of mobile systems.

- At the highest point in the chain are the initiatives such as mobile business, mobile government, and mobile life. These initiatives provide the main impetus for widespread use of mobile computing and wireless systems in the business, government, and personal life settings..

- The mobile computing applications that support m-business, m-government and mobile life. Several issues, such as personalization, are important at this level. Possible applications range from those currently available on the wired Internet (including banking, book purchasing, email, news, and travel) to new services designed specifically for mobile consumers (information about where to find the nearest store, for example, or the automatic notification to nearby employees). These applications use wireless technologies to support mobility of business activities, customers, suppliers, employees, managers, and other players in the corporate world. In addition, these applications support other activities in our life such as heath, entertainment, and social contacts.
- The mobile computing platforms provide the middleware and other software services needed to support mobile computing applications. Middleware services include general ecommerce middleware such as transaction support as well as wireless-specific services for various handsets such as iPhone and Android.
- At the bottom is the wireless network – the infrastructure that transports information between mobile devices, mobile users, data sources, and application providers. The wireless networks consist of wireless LANs, cellular networks, wireless local loops, and satellites. .

It should be noted, as shown in the figure, that higher levels drive lower developments and the lower levels enable the higher levels. This is true in most cases, but not always. In many cases, the developments in wireless network technologies are driving the development of new applications and business initiatives.

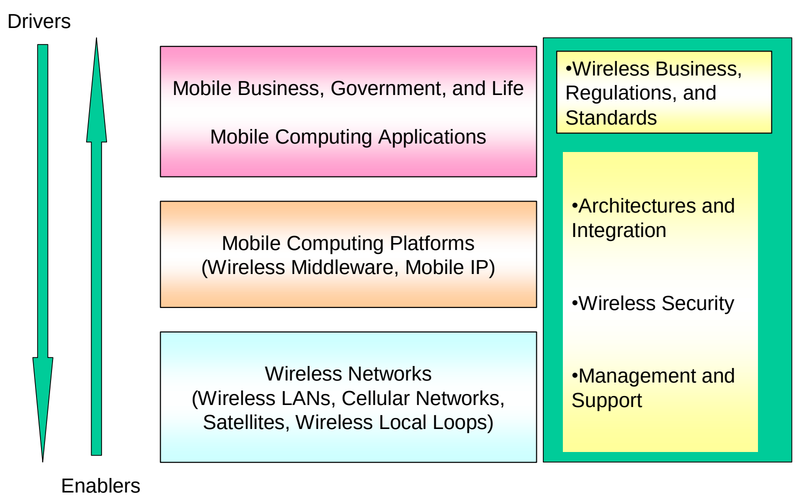


Figure 9-18: Framework for Discussion – Levels of Issues

Wireless in Action – A Few Snippets

We are surrounded by numerous examples of mobile computing and wireless communications in our personal and professional lives. This exposure is increasing steadily. Here are a few, almost random, snippets (some of these will be explained later):

- Mobile phone penetration is growing rapidly, particularly in underdeveloped countries. Globally, the number of mobile phones surpassed the number of fixed/wired phones way back in 2003. This is also the case in many individual nations, including numerous middle-income and low-income countries. Among these countries are Chad, Honduras, Indonesia, Jordan, Mexico, Mongolia, Nigeria, Philippines, Saudi Arabia, and South Africa.

- The US Federal Aviation Administration (FAA) has an email notification service that enables travelers with pagers, cell phones or Internet-enabled personal digital assistants to receive real-time airport status information via email. After the September 11 attack and the anthrax problems, each member of the House of Representatives was issued a BlackBerry device to facilitate communications between members.
- Doctors are increasingly using mobile devices in their practice. The physicians at the Children's Hospital of Wisconsin, for example, make their rounds accompanied by wireless carts that have wireless-enabled laptops for accessing drug suppliers and the Internet. This allows the physician to order new drugs quickly and also to use the Internet for instant research, if needed. These wireless carts have proved extremely helpful in recovery rooms where post-surgery patients need constant care and appropriate pain medications are needed immediately. The wireless carts have played a vital role in effective treatment of patients and helping the hospital to operate far more efficiently.
- The FCC has mandated that all cellular providers offer accurate location information for the users of E911 locations. The basic requirement is that the cellular providers should be able to locate the callers of the 911 emergency phone number with an accuracy of 100 to 300 meters. E911 support is one of the biggest drivers for location-based services (LBSs). LBS is an active area of work where you can, for example, locate a repair shop closest to where your car broke down, locate your children, and find the nearest bus stop. As another example, when driving by a grocery store, you could be reminded that you need to pick up eggs.
- Telecom carriers are increasingly using wireless technologies to address the "last mile" problem. This is especially popular in developing countries. For example, inhabitants of remote villages in India have been connected to the Internet through Wireless Local Loops (WLLs). The WLLs, based on fixed wireless technology, connect subscriber sites (homes, offices) to a local carrier office through microwaves. WiMax, a popular form of WLLs, is an attractive alternative to wired networks in the last mile, where the subscribers are far-flung and cannot be connected through wires due to terrain or hazardous situations.
- Deep space communications, involving satellite communications beyond the earth orbit (more than 11 million miles), is an active area of work for very long haul wireless networks. An example is the mission to Mars. A critical part of this mission is the communication system that allows the Mars rovers to receive commands from ground-based operators and to send its images and scientific data home by using wireless communications (it is somewhat difficult to connect Mars to the Earth through cables!).
- Wireless "Hotspots" are set up in hotel lounges, coffee lounges and airport waiting areas. Airline carriers are providing wireless LAN capabilities in their lounges and at the gates. For example, using the MobileStar service in several airports in the United States, American Airlines was one of the first companies to roll out wireless LAN service to gates and Admirals Club lounges. At present, many such wireless hotspots exist in airports and most hotels.
- Wireless homes are a major area of potential growth. We are already used to numerous wireless devices in home settings, such as remote controls for TVs that allow you to change TV channels and control the videocassettes remotely, garage door openers that open garage doors by using a short-distance wireless network, and remote controlled and interactive toys that use wireless networks to control the movements of toy cars and airplanes. Now a cell phone can connect to an alarm clock to wake you up at certain times based on certain situations. You can have conversations with your alarm clock: "Hello, alarm clock? Wake me up at 5:30 am unless there is a traffic problem on the way to the airport, then wake me up at 5 a.m."

- Automotive manufacturers are building "mobile offices" in cars, where a laptop is fitted in the backseat with a mobile phone, wireless Internet and fax support. Additional telematics services provide drivers with emergency services (such as automatic collision notification, emergency response, and roadside assistance). They also provide navigation and information services, such as routing assistance, traffic, weather, news, financial information, and sports information.
- Wireless content delivery systems that broadcast TV, radio, educational, military, and other content over satellites have proliferated dramatically. For example, even cable TV gets its content from the content providers over satellites. PBS (Public Broadcasting System), for example, was one of the first TV networks to broadcast its contents over an extensive satellite system, and BBC was one of the first companies to broadcast radio services around the globe through wireless communications. The situation has changed considerably.
- Some companies, such as Inner Wireless, provide "passive cell tower" technologies to the commercial real estate industry. Commercial real estate property owners can gain revenue by placing wireless technologies that boost cellular carriers' signals inside a building. Cellular signals just one foot inside a building are often 100 times less powerful than those just one foot outside the building, with a corresponding effect on the service quality provided to the end user. The technology has proven successful in office spaces, in the parking garages and elevators of said properties.

9.5.2 Mobile Business as an Integral Part of Modern Enterprises

M-Business is not a standalone activity – it is an integral part of modern enterprises that emphasize using up-to-date information, getting rid of delays, and using mobility and speed for competitive advantage. Specifically, getting the best information to and from mobile users is crucial to take advantage of the effect this group has on sales and revenues. For example, access to e-business applications can be enabled through mobile devices, and monitoring of business activities can be achieved through handheld devices. Office workers, sales-reps, and executives, as well as customers, have laptops, cellular phones and PDAs (Personal Digital Assistants) instead of desktop computers to do their work. American Express, for example, has created a mobile portal to give cardholders a real-time and comprehensive view of their finances – accessible through wireless devices. The financial information is aggregated from cardholder relationships with banks, brokerages, mutual fund companies, and others.

Similarly, self-serve systems allow mobile customers to receive services without interacting with the human representatives, who are typically stationary. Examples range from automated teller machines to e-tickets that the customers can use to get boarding passes on airlines without interacting with the representatives at specific locations. Self-serve customer systems do not eliminate the need for customer care but expand customer services at different sites without having to add new staff. Many of these services are also exploiting "positional knowledge" of the mobile users. For example, a salesman on a visit to Chicago is only given information about contacts and leads in Chicago. Speech recognition on mobile devices is another area of development. SpeechWorks International, for example, teamed with Quixi to develop a mobile customer relationship management (CRM) system. This CRM is a speech application that combines call center and voice recognition capabilities on mobile devices for enterprise sales staff. At present, many CRM systems fail because entering sales data is time-consuming and expensive. To attack this problem, speech recognition technology plays an important role in M-CRM.

M-Government, a subset of e-government, is the use of mobile computing and wireless communication technologies (ICTs) to improve the activities of public sector organizations. The goal of m-government is to make public information and government services available "anytime, anywhere" to citizens and officials. m-Government is not a fundamentally new idea because wireless technology has always been an important part of law enforcement. The difference is that today the law enforcement officers can use a laptop wirelessly connected to the Internet instead of the old two-way radios. For example, a Mobile Computing Project in Kentucky helps police officers use laptops to wirelessly connect to a database instead of talking to a dispatch operator. The database is linked with regional and national crime information, making the lookup much more comprehensive and accurate.

In addition, a large number of global initiatives such as M-Health, M-Agriculture and M-Life are breaking new ground by going beyond M-Business and M-Government and changing the way we live, stay healthy and survive. This is impacting developed as well as developing countries.

9.5.3 Mobile Computing Applications: Supporting m-Business and m-Government

Mobile computing applications support m-business, m-government, and mobile life initiatives. These applications have profound impact on the way corporations conduct their business and the way government agencies deal with the public by exploiting mobility. Specifically, these applications enable the C2B, B2B, B2E, C2G, B2G, G2G, and G2E operations between customers, business units, government agencies, and employees (see Figure 9-19).

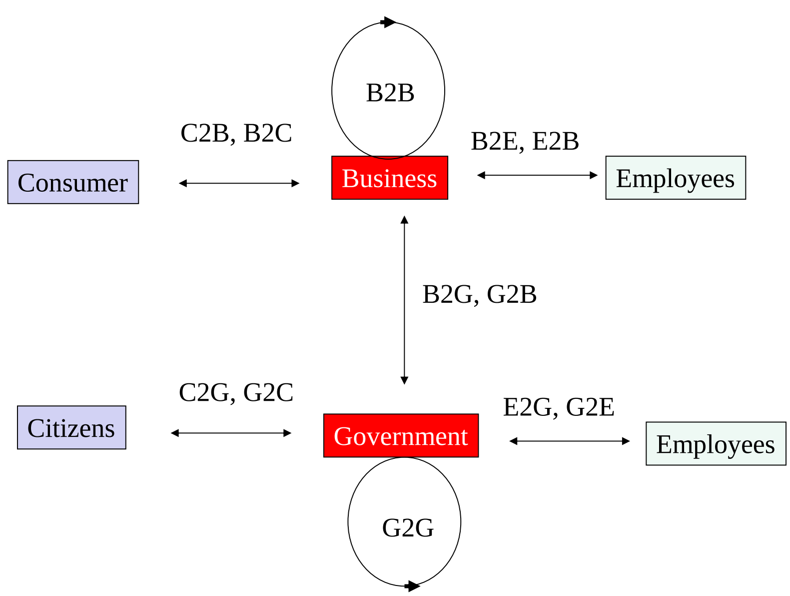


Figure 9-19: Interactions Between Consumers, Business Units, Government Agencies, Citizens, and Employees

A few observations are important before proceeding. First, most mobile computing applications are not fundamentally new applications. Instead, mobile device access over wireless networks is another aspect (dimension) of most existing arrays of applications. In fact, mobile access is being added to existing applications in a manner similar to the addition of Web access in the 1990s. Second, mobile access is not the only new feature of mobile computing applications – they also may include *positional* features that exploit location of the users, voice capabilities to support voice applications, and television features for interfacing with TV sets. These features, called MPTV (Mobile, Positional, Television, Voice) are shown in the sidebar "MPTV Applications". Finally, there are some core mobile computing applications that are being used, with minor and necessary modifications, for m-business and m-government initiatives. Examples of these applications are:

- Wireless messaging services
- Wireless Websites and mobile portals
- Mobile commerce and its variants
- Mobile customer relationship management systems (m-CRM)
- Mobile supply chain management systems (m-SCM)
- Specialized applications involving mobile agents and sensor networks

MPTV (Mobile, Positional, Television, Voice) Capabilities

Mobile capabilities enable mobile users, typically connected over wireless networks, to perform daily activities such as searching the Web, accessing remote applications, and invoking business transactions.

- ***Voice capabilities*** support voice communications over mobile devices. Voice support over cellular phones and voice commerce are examples.
- ***Positional capabilities*** support geographic position (location) for some applications. For example, positional commerce gives you information about deals in the Boston area when you are in Boston.
- ***V capabilities*** exploit the TV to do purchasing, Web surfing, and other operations typically available on mobile devices.

9.5.4 Mobile Computing Application Development and Support Issues

Applications for mobile users face many unique challenges because wireless networks pose unique problems that more commonly available fixed networks do not have. Wireless networks, although improving dramatically with time, are typically slower, get congested frequently, and are more error-prone and susceptible to outages than their wired counterparts. Thus mobile computing application designers should have some knowledge of the underlying communication network. For example, database queries over wireless networks should not attempt to send thousands of rows because the network may not be available that long. Besides wireless network weaknesses, the limitations of mobile devices also need to be considered. There is a potpourri of new mobile devices, such as cell phones, pagers, and personal digital assistants (PDAs). Developing applications for these devices is challenging because they have different form factors (e.g., varying numbers of display lines), different browsers and markup languages (HTML, WML, and cHTML[1]), and different device capabilities (some can display images, some cannot).

Special platforms, called ***mobile computing platforms***, are needed to provide the unique services needed by mobile computing applications. These platforms enable the operation and, in many cases,

[1] WML (wireless markup language) and cHTML (compact HTML)

development and deployment, of mobile computing applications. Figure 9-20, a refinement of the framework shown in Figure 9-18, depicts three types of services provided by these platforms:

- **Local platform services** that support the applications on the individual mobile devices. These services consist of operating systems (e.g., Symbian OS) needed to run the mobile devices, and also include local system software services such as database managers, transaction managers, and utilities for mobile devices. These services are designed specifically to handle the unique features of the devices.
- **Network transport services** that are responsible for shuffling the messages over, in this case, wireless networks. These services, mostly handled by the Internet technologies (TCP/IP, in particular), operate on top of physical wireless and wired networks to route the messages so that the mobile users can access their emails, websites, and corporate applications. Specialized protocols such as Mobile IP are needed for mobile devices. See Section 9.5.5.
- **Middleware services** that interconnect mobile users, databases and applications with each other. For example, wireless middleware provides remote access to a corporate database from a mobile phone and may also encrypt and compress the messages for security and performance. An interesting trend at present is to package a variety of middleware services into “wireless gateways” and “mobile application servers” that can support the current and future breed of mobile applications.

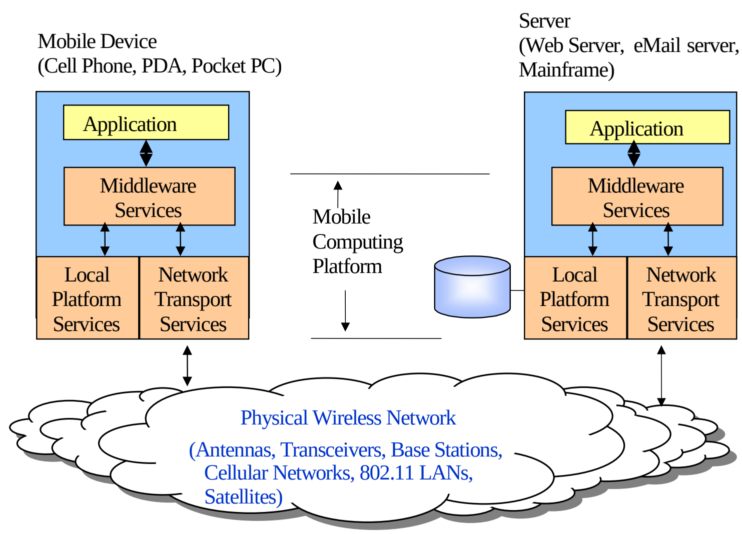


Figure 9-20: Platforms for Mobile Applications

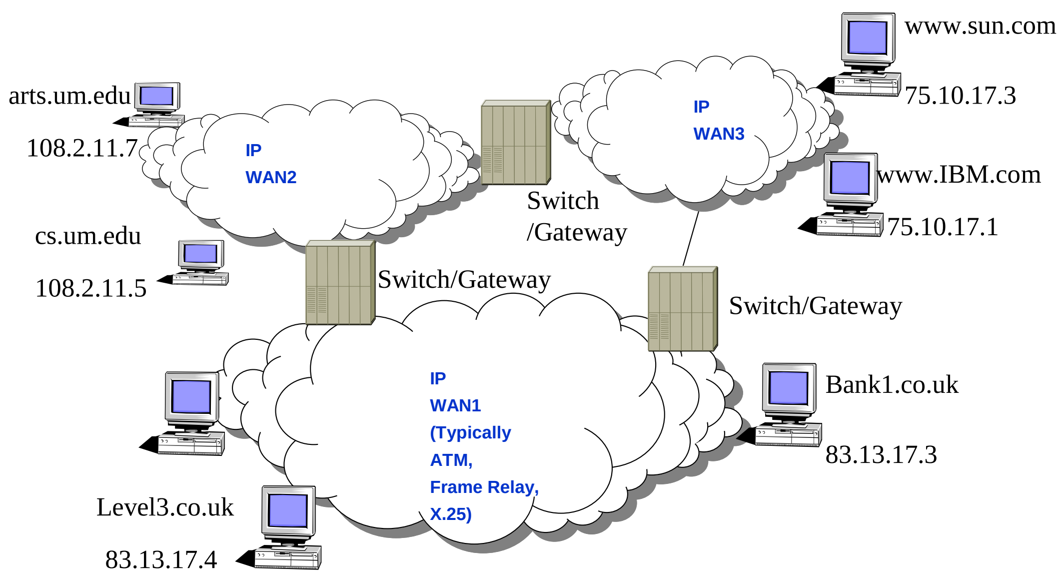
9.5.5 Wireless Internet, Mobile IP, and Wireless Web

Technically speaking, an Internet is a network based on the TCP/IP protocol stack. At present, the term *Internet* is used to refer to a large collection of TCP/IP networks that are tied together through network interconnectivity devices such as routers and gateways. At present, the term *Internet* is used to symbolize the following two situations:

- **Public Internet**, or just “the Internet,” that is not owned by any single entity – it consists of many independent TCP/IP networks that are tied together loosely.
- **Private Internets**, or intranets, are the TCP/IP networks that are used by corporations for their own business – they use the same technology as the public Internet but the underlying physical network is privately owned.

- **Extranets** are the TCP/IP networks that are jointly owned by corporations to conduct business.

Figure 9-21 shows a conceptual and partial view of the Internet. This Internet shows three networks (a university network with two computers, a commercial company network, and a network in UK). Each computer ("host") on this network has an IP address and has been assigned a domain name as well. The Internet is very heterogeneous (i.e., different computers, different physical networks). However, to the users of this network, it provides a set of uniform TCP/IP services (TCP/IP hides many details). Once a device (mobile device or a laptop) has an IP address, then it can send messages to any other device with another IP address. Thus a user at arts.um.edu can send email to someone at bank1.co.uk and browse the IBM website at www.ibm.com.



•DNS (Domain Name Services) translates cs.um.edu to 108.2.11.5
•Telnet cs.um.edu = Telnet 108.2.11.5
•FTP cs.um.edu = FTP 108.2.11.5

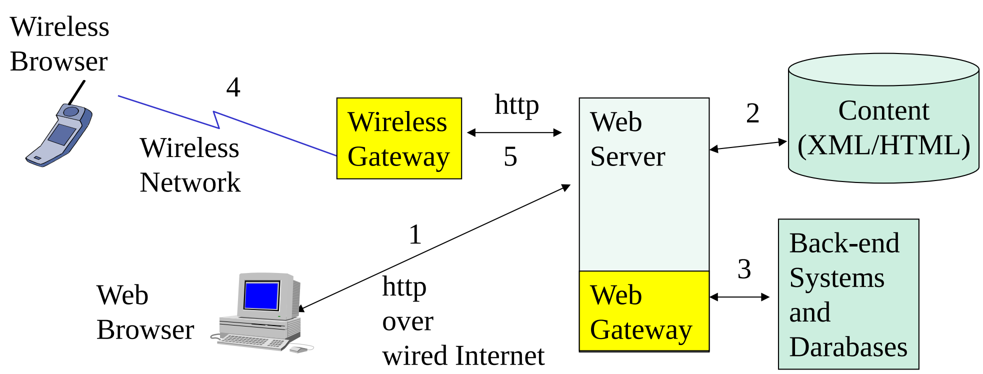
Figure 9-21: Partial View of Internet

To support highly mobile devices, a new protocol called Mobile IP has been introduced. Mobile IP allows mobile devices (PDAs, portable computers) to maintain Internet connectivity while moving from one Internet attachment point to another. This is done by using a concept similar to mail forwarding (the traffic is forwarded to the mobile device as it moves around).

How does wireless Web work? Web technologies reside on top of the Internet to support GUI operations. Figure 9-22 shows a conceptual view of how Web content is accessed from regular Web browsers (steps 1, 2, 3) as well as from cellular phones (steps 4, 5, 2, 3). The core building blocks of this view are:

- Web servers that are custodians of Web content and also provide access to non-Web content through Web gateways
- Web browsers that display the Web content (e.g., html pages) on PCs
- The Internet that carries the traffic between Web browsers and Web servers
- Wireless browsers that display the content on wireless handheld devices

- Wireless gateways that translate Internet protocols to wireless networks, if needed, and also convert ("render") the Web content to be displayed on handheld browsers
- Wireless networks that carry the data for handheld devices



1. Access from Web browser to Web Server over wired Internet
2. Access to Web contents from HTML/XML files
3. Access to non-Web content through a Web gateway
4. Access from cellular phone over a wireless network
5. Access from wireless gateway to Web Server over wired Internet

Figure 9-22: Conceptual View of Wireless Web

9.5.6 Overview of Wireless Networks

Wireless networks, as the name implies, interconnect devices without using wires – instead they use the air as the main transmission medium. Wireless networks are enjoying widespread public approval with a rapidly increasing demand. The unique features of the wireless networks are:

- The bandwidths, and consequently data rates, of communication channels are restricted by government regulations. The government policies allow only a few frequency ranges for wireless communications.
- The communication channel between senders/receivers is often impaired by noise, interference and weather fluctuations.

The senders and receivers of information are not physically connected to a network. Thus the location of a sender/receiver is unknown prior to start of communication and can change during the conversation.

A very large body of work on wireless networks exists, with emphasis on different aspects such as radio transmission technologies, standards, protocols, systems engineering, and carriers. See, for example, the Mobile Communications Series by Artech Publishing. For our purpose, wireless networks can be broadly classified in terms of distance covered: wireless local area networks, wide area networks and metropolitan area networks. Figure 9-23 displays an overall classification of wireless networks in terms of distance covered, from very short range (centimeters) to very long range (thousands of miles).

Wireless LANs (WLANs) allow workstations in a small area (typically less than 100 meters) to communicate with each other without using physical cables. The most popular example of Wireless LANs are the IEEE 802.11 LANs that deliver 54 Mbps or higher data rate. Another example is the Bluetooth LANs (for the data rates in the 1 Mbps range over 10 meters). Very short range LANs such as Bluetooth are also known as Wireless Personal Area Networks (WPANs) We will discuss wireless LANs and PANs in Section 9.5.7.

Wireless metropolitan area networks (WMANs) have been used in traditional packet radio systems often used for law-enforcement or utility applications. An interesting area of growth for wireless MANs is the wireless local loop (WLL) that is quite popular with long distance telephone companies. WLLs are ***fixed wireless networks*** where the devices being connected are stationary. WiMax is a very popular form of WLLs. See Section 9.5.9.

Wireless WANs (WWANs) provide wireless support over long distances. Traditional examples of wireless WANs are paging networks and satellite systems. However, a great deal of wireless WAN activity at present revolves around the cellular networks that provide support for cellular phones and other handheld devices such as PDAs and laptops.

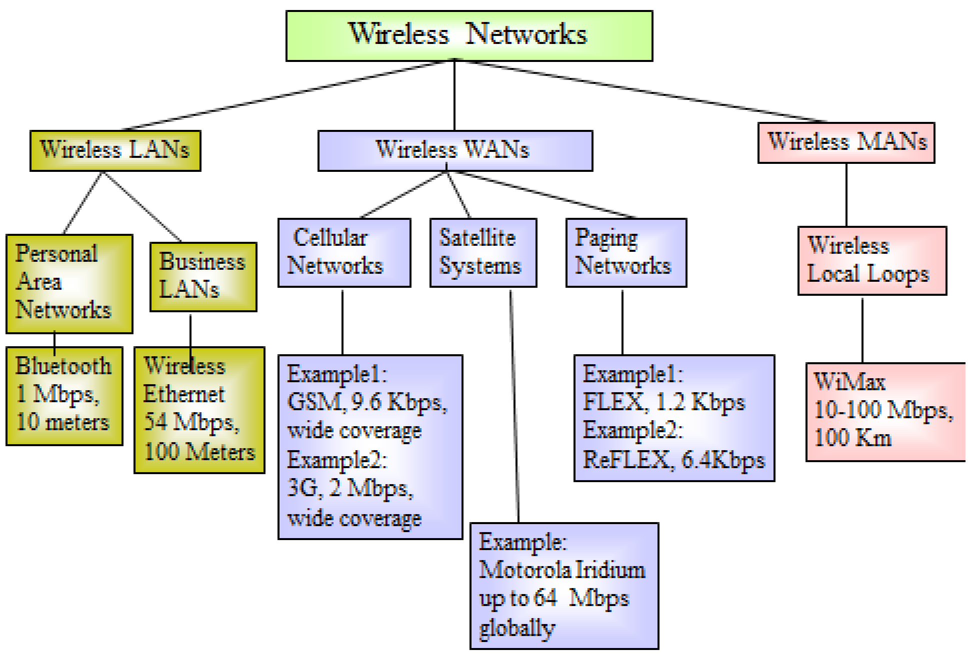


Figure 9-23: A View of Wireless Network Landscape

The wireless networks in the aforementioned categories are offering higher data rates than before. However, the wired networks are also offering higher data services.

Table 9-1 summarizes the typical data rates in the wireless versus the wired world. As you can see, the wireless technology is much slower than its wired counterpart but it offers greater flexibility to the users.

Table 9-1: Wireless Versus Wired Networks

	Local Area Networks (LANs)	Metropolitan Area Networks (MANs)	Wide Area Networks (WANs)
Wired	Wired LANs Ethernet (10-100 Mbps, 150 to 500 meters) Token Ring (4 -16 Mbps, 200 to 500 meters)	Wired MANs FDDI (100 Mbps, 50 Kilometers)	Wired WANs Dial-up (56 Kbps) DSL/cable modems (200 Kbps-1 Mbps) ATM (44 Mbps to 140 Mbps) Frame Relay (44 Mbps) Higher data rates (over 100 Mbps) available
Wireless	Wireless LANs Bluetooth (1 Mbps, 10 meters) IEEE 802.11 LANs (11-54 Mbps, 100 meters)	Wireless MANs Wireless local loops (10-50 Mbps, 10 Kilometers)	Wireless WANs Current GSM systems at 9.6 Kbps, future 3G systems at 2 Mbps Satellites at 64 to 100 Kbps

9.5.7 Wireless LANs: IEEE802.11 and Bluetooth

Wireless LANs allow workstations in a building to communicate with each other without having to be connected to physical cables. This is a major benefit because LAN wiring can be the most expensive component of a LAN. At the time of this writing, wireless LANs have several limitations such as short distances, lack of wireless adapter cards for PCs and workstations, limited connectivity to other LANs, and relatively low speeds. However, this technology is still in its infancy. Technologies such as Bluetooth (discussed in next section) are examples. Currently available wireless LANs use one of three signal types to transmit data:

- infrared
- spread spectrum
- narrowband microwave

Infrared signals behave like ordinary light (they cannot penetrate sold objects). Thus infrared wireless LANs are limited to data transmission to line of sight. Infrared technology is simple and well proven (it is used commonly in remote controls for VCRs and TVs). In addition, infrared signals are not regulated by the Federal Communications Commission (FCC). Spread spectrum is most widely used in wireless LANs. These LANs transmit in the industrial, scientific, and medical bands designated by the FCC. These bands are not licensed but are regulated by the FCC to prevent interference. This technology was developed for military and intelligence operations (the message is "spread" over a range of frequencies to make it jam-resistant). Wireless LANs based on narrowband microwave technology use the 18.82-to-18.87 GHz and 19.6-to-19.21 GHz frequency ranges. These frequency ranges are licensed by the FCC, which means that a vendor must be approved by the agency to use these frequency ranges. Many wireless LAN vendors consider this to be a restriction.

9.5.7.1 IEEE 802.11 Standard for Wireless LANs

The IEEE 802 standards committee formed the 802.11 Wireless Local Area Networks Standards Working Group in 1990. The Working Group defined the IEEE 802.11 standard protocol for two types of networks: ad hoc and client/server networks. The 802.11 LANs are most widely used. These networks operate at 54 Mbps and higher and can support distances between 100 feet and 500 feet. Detailed information about these LANs can be found at the Wireless LAN Association Website (www.WLANA.org).

Figure 9-24 shows a sample environment that supports wireless Ethernet LANs so that the students can access the school server as well as the public Internet. In this configuration, several wireless access points are connected to a wired LAN that is connected to the Internet and an internal server. Each access point supports mobile computers with wireless Ethernet cards in a wireless cell that spans around 100 meters.

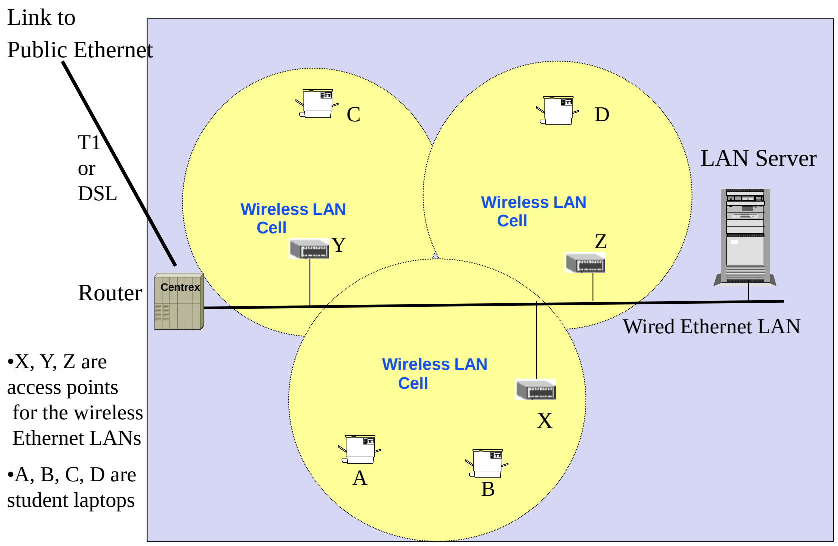


Figure 9-24: A Sample Configuration with Wireless Ethernet LANs

9.5.7.2 Wireless Personal Area Networks (WPANs), Bluetooth and UWB

Wireless Personal Area Networks (WPANs) are short-range (10 meter or less) radio networks for personal, home, and other special uses. Within the WPAN family, several specifications such as Bluetooth, wireless sensor networks, and UWB (Ultra Wideband) have emerged.

Bluetooth is a wireless cable replacement standard that provides a 1 Mbps data rate over 10 meters or less. It typically consists of a group of linked devices, such as a computer wirelessly connecting to a set of peripherals, known as a “piconet.” Multiple piconets can be formed to provide wider coverage. Due to its relatively low data rates and very short distances, Bluetooth is being used in home appliances, “Bluetooth-enabled” cars, and other such applications. Figure 9-25 shows a simple Bluetooth configuration. Bluetooth was designed to allow low-bandwidth wireless connections to become so simple to use that they seamlessly mesh into your daily life. A simple example of a Bluetooth application is updating your cellular phone directory. The main idea is that this could happen automatically as soon as the phone is within the range (10 meters) of a desktop computer where a directory resides.

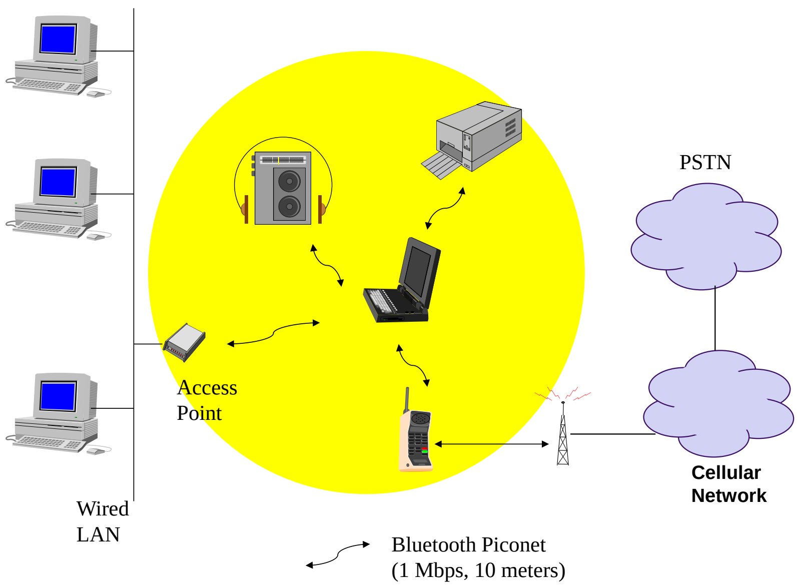


Figure 9-25: A Simple Bluetooth Configuration

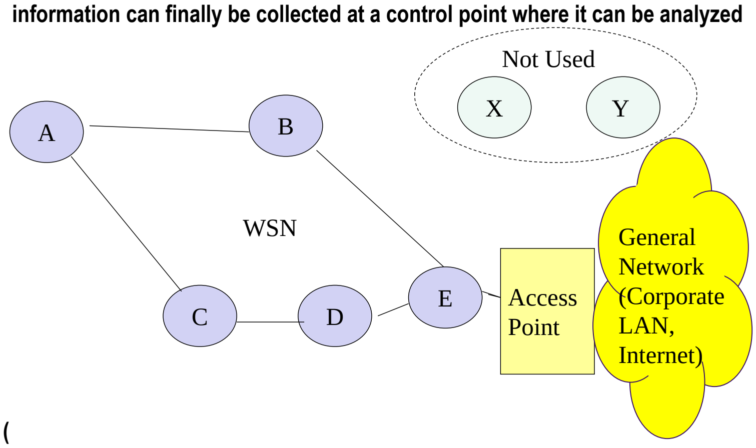
UWB (Ultra Wideband) is a relatively new[2] technology and is stronger than the other short-range wireless systems (such as Bluetooth) because of its simpler device designs, lower power consumption and higher data rates. Another player in the short-range radios is the **wireless sensor networks (WSNs)** that are formed between small, low-powered sensor devices mainly for monitoring and data collection purposes. Yet another player in short-range wireless, HomeRF, was primarily aimed at the needs of the small office and home office (SOHO) networks. HomeRF has been sidelined due to the popularity of other alternatives such as Bluetooth and UWB.

9.5.8 Wireless Sensor Network (WSN) and IoTs

Sensors are small devices that can be used to measure temperature, humidity, motion, color changes in a painting, or in a painting, or any other measurable thing. These sensors, also called motes, are installed in particular locations or particular locations or can be "sprayed" in a particular area to gather information. Sensors by themselves are not very themselves are not very powerful -- they just sit around and collect information. The real power of sensors come in the sensors come in the form of wireless sensor networks (WSNs) which are formed when these tiny sensors start sensors start communicating with each other through wireless. WSNs can shuffle the information collected through collected through thousands of sensors and transfer it to the public Internet or a corporate LAN. The information can

[2] As we will discuss in later chapters, UWB is not a new technology; it has been around for several years for military use, but has been "declassified in 2002 for commercial use.

information can finally be collected at a control point where it can be analyzed



(

Figure 9-26). Although most WSNs consist of very small processors communicating over slow wireless networks, WSNs can be used in several situations.

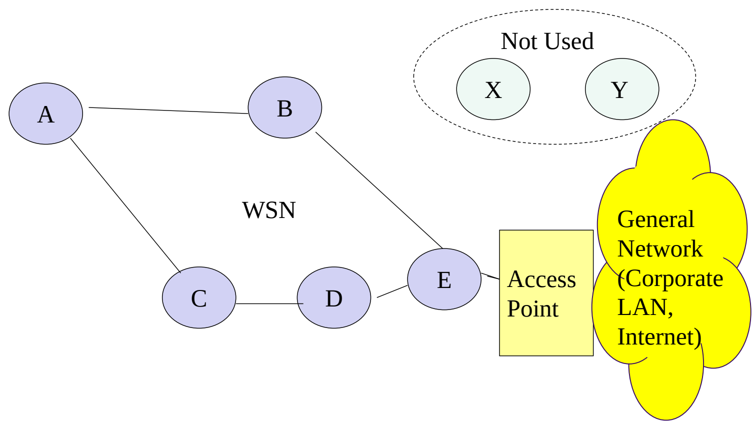


Figure 9-26: A Sample Wireless Sensor Network

Thousands of tiny low-power sensor devices are typically spread over large areas to form WSNs in many practical applications. The sensors of WSNs collaborate with each other to monitor the environment, guide vehicles, and detect faults in buildings and bridges. Some of the examples are:

- Internet of Things (IoT) heavily use wireless sensor networks in a wide range of sectors such as health, education, public safety, public welfare, agriculture and transportation. See Section 9.6.
- In many military situations, sensors are “sprayed” in a battlefield or an enemy area to detect and record certain activities and send information back to control centers for analysis and appropriate action.
- WSNs are being considered as an alternate to landmines where the sensors can detect enemy vehicles. This is much safer than landmines, which stay long after the conflict is over and are hazardous to the people living in that area. In contrast, sensors are harmless after conflict because they simply sit around collecting useless data until their batteries die.
- WSNs are also being used in medical situations for patient monitoring. For example, patient heart rate and blood oxygen levels are monitored by sensors. This information is gathered from different patients and sent to the PDA of an attending physician.

- WSNs are being used in supply chain management systems also. For example, Sears Canada has completed an experiment that uses WSNs to detect if an item is damaged on transit before the customer gets it.
- WSNs are also used to detect temperature fluctuations, earthquakes, automobile speeds, and cattle activities in fields. Many civilian applications of WSNs have been developed and deployed.

Example: RFID (Radio Frequency Identification) systems have been used in a variety of applications. An RFID system typically consists of the following components:

- A tag or label that is embedded with a single chip computer and an antenna. The antenna is so small that it can be printed on the tag with carbon-based inks. RFID tags (chip plus antenna) are also called “transponders.” The tag is somewhat similar to the commonly used bar code labels. However, an RFID tag has more intelligence. Tags are of two types. “Passive” tags, the type of tags commonly used in retail stores and supply chain systems, pick up enough energy from the radio to operate and to communicate back to the radio. “Active” tags have an embedded battery and offer the advantage of longer-range communications and can communicate with other tags. In this case, a WSN can be formed between the RFID tags.
- A short range radio (e.g., a wireless LAN such as Bluetooth) that communicates with the tag. The radio receiver is usually an RFID reader, or detector/interrogator., that gets the information from the RFID tag and then may send it to a back-end system for processing. An RFID system’s “read range” — the distance a tag must be from the detector/reader — varies from a few centimeters to tens of meters, depending on frequency used, whether a tag is active or passive, and the type of antenna used on the reader.

9.5.9 Wireless Metropolitan Area Networks (WMANs) – The Wireless Local Loop

Wireless metropolitan area networks (WMANs) are the wireless local loops (WLLs) that are gaining popularity with long distance telephone companies. WLLs allow long distance carriers to bypass the existing wired local loops owned by local phone carriers. Consider, for example, AT&T long distance services that need to connect a caller in Chicago to a caller in New York. AT&T has to pay the local carriers in Chicago and New York because these carriers own the wirings at the two end points. These charges can add up to $20 billion in the US alone. Figure 9-27 shows a sample configuration in which a local wired loop has been replaced with a wireless local loop.

WLLs are quick and cost-effective for quick setup of local phone services. Imagine laying millions of miles of copper cables to set up a local wired loop. Several technologies exist for WLLs. The best known is WiMax. WLLs are examples of wireless metropolitan area networks and offer broadband wireless data rates between 10 to 50 Mbps.

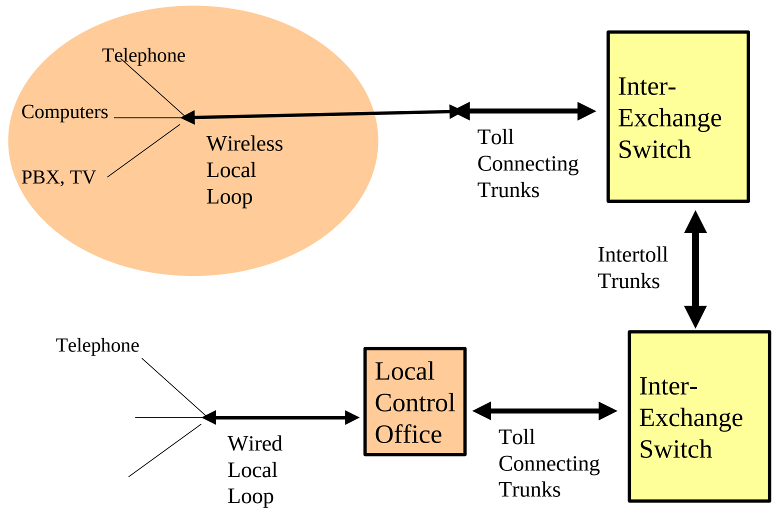


Figure 9-27: Wireless Local Loop

Another entrant in the WLL market is **Free Space Optics (FSO)**, which uses laser beams to deliver extremely high data rates (around 1 Gbps) over a few kilometers. FSO is gaining popularity because of its high security – it is difficult to intercept laser beams! In the last mile, wireless local loop technologies (LMDS, MMDS, and FSO) are providing strong competition to the wired local loops based on copper or fiber optic networks. Wireless solutions have the advantage that they can be installed quickly and less expensively.

9.5.10 The Wireless Wide Area Networks – Cellular Networks

Wireless wide area networks (wireless WANs) are used widely to support mobile users over long distances. These networks can be discussed in terms of paging networks, cordless networks, and cellular networks.

9.5.10.1 Cellular Network Landscape

Cellular telephones were introduced in the mid 1980s. These technologies are enjoying widespread public approval with a rapidly increasing demand. To meet this demand, mobile communications technologies are emerging with digital speech transmission and the ability to integrate cordless systems into other networks. In the meantime, researchers are developing the next generation of technologies for the next century.

Figure 9-28 shows a high-level view of a cellular communication network used in wide areas. The cellular network is comprised of many "cells" that typically cover 1 to 25 miles in area. The users communicate within a cell through wireless communications. A base transceiver station (BTS) is used by the mobile units in each cell by using wireless communication. One BTS is assigned to each cell. Regular cable communication channels are used to connect the BTSs to the mobile telephone switching office (MTSO). The MTSO determines the destination of the call received from a BTS and routes it to a proper destination, either by sending it to another BTS or to a regular telephone network. Keep in mind that the communications is wireless within a cell only. The bulk of cell-to-cell communication is carried through regular telephone lines.

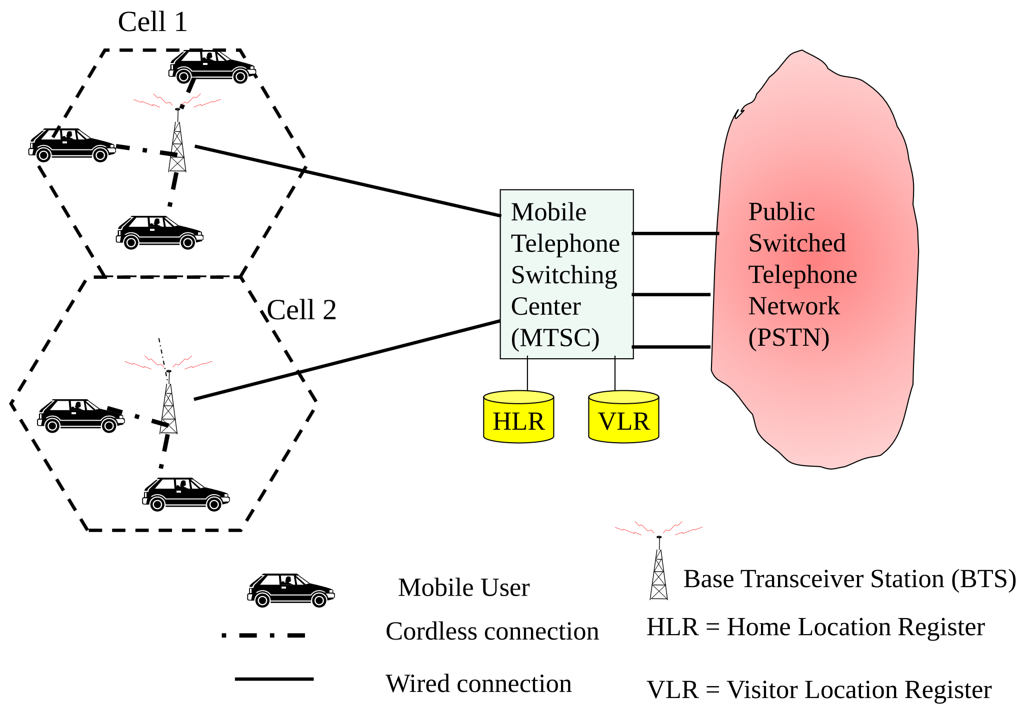


Figure 9-28: A Cellular Communication Network

Two issues are of fundamental importance in this conceptual model:

- **Cell sizes**. The sizes of the cells can be small or large. In some cases, such as cordless networks, the cell sizes are only a few feet. But in cellular networks, the cell sizes can be many miles (10 to 20 miles).
- **Location ("Roaming") support**. In some cases, the user is only covered for his "home cell"; in others, the user can roam between cells and still be covered adequately. For example, in a cordless phone, the user is only covered at the home cell, while roaming is typically supported in a wide coverage area where the user can travel through several cells.

It is good at this point to differentiate between cordless and cellular phones. In a cordless network, such as the cordless phone in your home, each telephone handset is the base station. You cannot go far from the handset (perhaps not more than 100 feet) if you are using the cordless phone. Cordless networks have smaller cell sizes and have no roaming support. ***Cordless communication*** basically operates on the same principle as the cellular systems; however, cordless systems operate at lower power (suitable for light telephone devices), so the cell sizes are smaller (usually within a building as compared to several miles). Basically, a cordless system has many more cells that can be accessed by weaker cellular devices and does not support roaming services. Due to their general use, we will concentrate more on the cellular networks.

The common features of the cellular and cordless PCS networks are:

- The senders and receivers of information are not physically connected to a network. Thus the location of a sender/receiver is unknown prior to start of communication and can change during the conversation.
- The communication channel between senders/receivers is often impaired by noise, interference and weather fluctuations.

The bandwidths, and consequently data rates, of communication channels are restricted by government regulations. The government policies allow only a few frequency ranges for wireless communications.

9.5.10.2 Evolution of Cellular Networks – The 3G Networks and LTE

The cellular networks are evolving through the following stages: (see Figure 9-29)

- **1G: First-generation wireless cellular:** These systems, introduced in the early 1980s, use analog transmission, and are primarily intended for speech. These networks are very slow (less than 1 kilobits per second).
- **2G: Second-generation wireless cellular**: Introduced in the late 1980s, these systems use digital transmission and are also intended primarily for speech. However, they do support low bit-rate data transmissions. The high-tier 2G systems use GSM and the low-tier systems are intended for low-cost, low-power, low-mobility PCS. These systems, most prevalent at present, operate at 9.6 Kbps.
- **2.5G Systems** are essentially 2G systems that have evolved to medium-rate (around 100 Kbps) data. As part of the 2.5G initiative, GSM is being extended by the General Packet Radio System (GPRS) to support data rates of 112 kilobits per second.
- **3G Systems** represent the broadband wireless networks that operate at 2 million bits per second for multimedia applications. 3G systems are based on evolution from 2G; they build on the success of GSM, and dual-mode terminals to ease migration from 2G to 3G are commercially available.
- **LTE (Long Term Evolution) and 4G+** are the family of wireless networks that go beyond 2 million bits per second data rates. These wireless networks are evolving rapidly to very high data rates for moving video sophisticated applications on cellular phones. An example of the LTE-4G applications is movies on the handsets from Netflix.

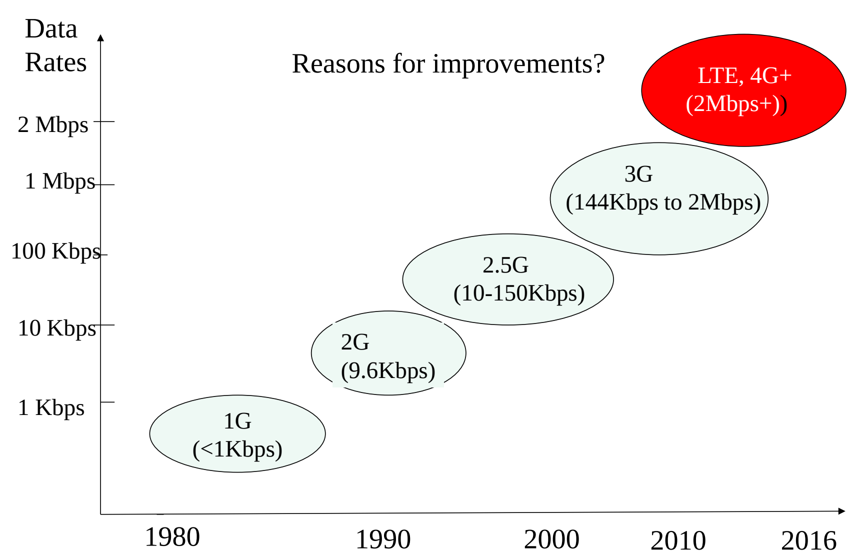


Figure 9-29: Evolution of Cellular Networks

9.5.11 Satellite Communication Systems

Satellites were first launched in 1962 and have ushered in the era of “celestial” and “global” communications. A satellite is essentially a microwave repeater in the sky which receives signals from transmitting stations on earth and relays these signals back to the receiving stations on the earth (see Figure 9-30). A satellite system consists of the following components:

- Earth Stations – antenna systems on or near the earth
- Uplink – transmission from an earth station to a satellite
- Downlink – transmission from a satellite to an earth station (different from uplink, typically faster, can be broad)
- Transponder – electronics in the satellite that convert/amplify uplink signals to downlink signals. There are typically 16 to 20 transponders per satellite, each with 36-50 MHz BW (bandwidth).

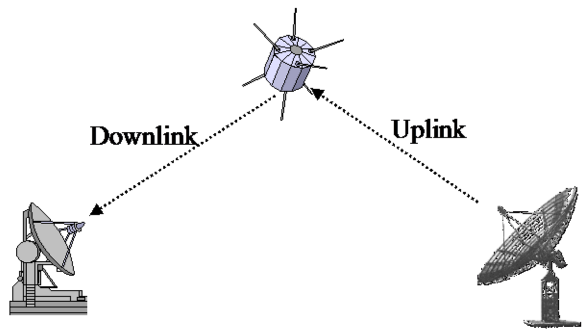


Figure 9-30: Satellite Transmission

A satellite covers a certain area – the higher the satellite, the more area it can cover. The coverage area of a satellite is called the satellite's footprint. Only receiving stations within this footprint can receive the satellite's signals.
The oldest example of satellites is the Geosynchronous (GEO) satellites that are in wide use providing international and long distance telephone services (to stationary users) and broadcasting services. GEO satellites are placed in the earth orbit at 22,300 miles – an area called the Clark Belt, after the famous science-fiction writer who first envisioned satellites in 1945. Once placed in the Clark Belt, the satellite rotates at the same speed as the earth's rotations so the satellite does not appear to move (this is called geo-synchronization). Thus the sending and receiving dishes can stay pointed to the satellite without any readjustments. GEO satellites can provide high communications capacity and can support several thousand voice channels. However, each satellite message encounters a 0.25-second delay because of the distance a message has to travel between a sender and a receiver. In a satellite communication system, the transmission cost is independent of the distance between the sender and receiver (two stations 100 miles apart or 1000 miles apart still have to travel thousands of miles to and from the satellite). Because of this, satellite communication systems are used to broadcast (i.e., send) a message to several receivers simultaneously.

An interesting area of satellite communications is "*Deep Space Satellites*" that communicate over hundreds of thousands of miles. In fact, NASA is working on an Interplanetary Internet that would form an Internet between the satellites in the sky.

.

A class of wireless wide area networks, not mentioned frequently in the popular press, is the paging networks that have been around for a long time. These networks are designed for short messages and are relatively slow.

9.6 Internet of Things (IoT) and Web of Things (WoT) – Examples and Case Studies

9.6.1 IoT and WoT: Combining Internet, Web, Mobile Communications and AI

As stated previously, the IoT (Internet of Things) refers to any device that can be connected to the Internet and Web of Things (WoT) provide web interfaces to IoTs. Thus more "things" on planet Earth are becoming digitally connected Internet devices and more appliances and gadgets are using web interfaces. IoT and WoT applications cleverly combine the following four mega trends for business, government and daily life:

- Internet, with its ability to connect almost any device over the IP network
- Web, with its ability to support users through browsers and business functionalities through apps
- Mobile communications, with its ability to wirelessly interconnect devices that are in motion from small sensors to large scale satellites
- Smart apps, with their AI (Artificial Intelligence) ability to detect different situations, adjust accordingly, and learn quickly to do better in the next round.

Due to these capabilities, ordinary devices such as alarm clocks and coffee machines (“things”) are becoming "smart" web connected devices that create, store, and share data (sometime referred to as “Micro Data”). These smart devices can be programmed to make decisions based on the data it has created and inputs from other sources such as humans. For IoT to reach its potential, a different design approach is needed that is based on how natural things such as plants, water and heat interact with each other. Here are some examples:

9.6.2 Some IoT Examples

Many examples of IoT are available over the Internet. The following is based on a few quick scans of the Internet:

- City-wide networks for machine to machine (M2M) communications and the Internet of Things. The network could be used for anything from monitoring car parking spaces to checking when rubbish bins need emptying, according to the partners.
- Microsoft and Rolls-Royce have announced a partnership centering on Rolls-Royce intelligent engines. Rolls-Royce will integrate Microsoft Azure IoT Suite and its Cortana Intelligence Suite.
- Manufacturing quality controls by using networked sensors, cameras, and lasers to analyze manufacturing processes to determine if a part is good or bad based on its physical characteristics; identify if it is the right component for the job and monitor trends, variations, and relationships in the system over time
- Combine farming sensor data from soil moisture levels, weather forecasts, and pesticide usage from farming sites into a consolidated web dashboard. Farmers can use this data with mapping information to identify crop issues and remotely monitor all of the farms assets and resource usage levels.
- Safety monitoring system that notifies authorities when a fire extinguisher is blocked, missing from its designated location or when its pressure falls below safe operating levels. Alerts can be sent directly through an instant email, phone call or pager notification to proper agencies and supervisors.

- Receive pollution warnings by using sensors installed in sewers that send alerts to local residents to help them avoid polluting local waterways.
- Light streets more effectively by intelligently providing the right level of lighting needed by time of day, season, and weather conditions.
- Recording, mapping, and sharing health and environmental data using smartphones that capture real-world measurements (sound levels, temperature, humidity, and carbon monoxide gas concentrations).
- Sensors installed inside equipment monitor if any parts have exceeded their designed thresholds and automatically send reports to owners and manufacturers if they have.
- Retailers can run use networked cameras and sensors to detect how customers are engaging with specific products and the store's layout.
- SmartPile technology uses wireless sensors embedded within concrete foundation piles to ensure the quality and integrity of a structure.
- An infant monitor that provides parents with real-time information about their baby's breathing, skin temperature, body position, and activity level on their smartphones. Similar monitors for aging family members utilize discrete wireless sensors placed around the home detect and monitor their activities.
- A Smartphone provides human activity monitoring by using a wide range of sensors (Accelerometer, Gyro, Video, Proximity, Compass, GPS, etc) and connectivity options (Cell, WiFi, Bluetooth, etc) to monitor movements, location, and workouts throughout the day.
- IoT pill detects when it comes in contact with your stomach fluid and communicates a signal that determines the timing of when you took your meds and the identity of the pill.
- A wearable sensor system that can remotely read a patient’s biometrics (ECG, heart rate, respiration rate and activity level), sending the data to the patient’s physician and allowing users to go about their daily lives.
- Remotely monitor and manage your home temperature controls, remotely turn on and off any plugged in device, and measure and record the power usage of any device.
- Detect and avoid disasters by detecting intruders in your home when you were away and detect power and utility failures.

9.6.3 Some WoT Examples

Since WoT is built on top of IoT, many examples of IoT mentioned previously can be also listed as WoTs especially if they use web browsers, web servers, and other web capabilities to search, extract, summarize and display the collected information.

Consider, for example, the following IoT example, mentioned previously, that combines farming sensor data from soil moisture levels, weather forecasts, and pesticide usage from farming sites into a consolidated *web* dashboard. Farmers can use this data with mapping information to identify crop issues and remotely monitor all of the farms assets and resource usage levels.

This can be definitely classified as an IoT plus WoT example, especially if it increases its reliance on web browsers, web servers and web services to extract data from multiple farming sites and stores it into a web-based farming portal.

The following examples of WoT, illustrate the key points in services such as web-based robots for surgical and domestic operations, remote patient monitoring, shopping mall mobile app, remote DVR (Digital Video Recording) scheduling, remote home security systems monitoring and administration, and remote home electricity grid usage monitoring. More examples are available at http://webofthings.org/ and other WoT resources available on the Internet.

- Web-based robots for surgical, domestic, manufacturing, and disaster recovery operations. These web-based robots can make more precise and wider range of surgical movements, serve as automated butlers who can perform repeated tasks without getting tired or bored, move items more quickly and precisely over the assembly lines, and detect plus rescue bodies more quickly from rubble. These and other examples of robots are supported by Internet connections, web browsers and servers, wireless communications, and AI capabilities.
- Real time patient monitoring capability using patient specialist mobile apps for smart phones that use web services for extracting and displaying patient information. This helps the physicians in keeping track of all the important parameters and help make important decisions quickly and suggest medication in time.
- Locate a specific product inside a shopping mall by entering its name on a mobile application and then using a combination of Internal Position System (IPS) and Internet of Things (IoT) to locate the needed products. This is a very web-based app that extracts information from multiple websites of various sellers in the shopping mall.
- DIRECTV's web interface that allows users to remotely set their DVR to record future programs using the DVR Scheduler via any PC or mobile phone is one example. To send a record request from directv.com requires a personal computer/mobile phone, Internet browser, an Internet connection, and valid ID-PW credentials.
- Remote home security allows remote device control over your home or business monitoring system. A user can remotely enable or disable security features, control energy sources, receive email or text notifications, and view current status or recent activity by using a web browser.
- Web-based remote access to smart utility meters at homes and businesses to review electricity usage for the current or past days, With proper credentials, a user can connect to a smart meter to monitor and adjust electrical usage from any PC or mobile phone with Internet access and a web browser.

9.6.4 Case Study: IoT4D (IoT for Developing Countries)

Many IoT applications in the well-to-do developed countries are making life more comfortable for people who are already living very comfortable lives. The focus of IoT4D is to use IoTs to support the basic necessities in health, education, public safety, and public welfare for the underserved populations. As noted in the opening vignette, Cisco and the International Telecommunications Union (ITU), the UN specialized agency for ICTs, has published a report, “Harnessing the Internet of Things for Global Development”. This report, published in January 2016, outlines how the IoT can rapidly accelerate the rate of global development to achieve the UN Sustainable Development Goals (SDGs) for the developing countries. The following quotes from the two major writers of this report are worth noting:

- From Dr. Robert Pepper, VP Global Technology Policy, CISCO: “The Internet of Things is one of the defining and transformative technologies of our time. The ability to impact millions, if not billions, of lives for the better in the developing world and prevent another digital divide is within our grasp and is an opportunity we can’t afford to miss. Let’s act now to prevent a two-tier world between the connected and the unconnected.”
- From Mr. Houlin Zhao, Secretary General, ITU: “The Internet of Things is one of the most exciting areas of our fast-evolving ICT industry, offering huge potential for disruption and transformation. In the context of global development challenges, this means we have the potential to surmount long-standing hurdles in basic services like health care, both quickly

and affordability. IoT could prove the long-awaited new approach that will help turn-around developing economies and greatly improve millions of people's day-to-day lives."

"Harnessing the Internet of Things for Global Development" report introduces over twenty IoT project implementations where low cost sensors and connectivity are improving lives, such as:

- In densely occupied informal urban settlements, networked smoke and fire sensors placed in homes are able to signal and warn residents, and neighbors, of potential fast moving fires, saving lives and property.
- In water delivery, sensors are monitor when village hand water pumps break and then alert local authorities, municipal utility providers and donor agencies, helping to reduce the downtime of water pumps providing critical water service.
- In healthcare, where cellular enabled thermometers are helping to protect the critical vaccine delivery to remote and rural areas via real-time monitoring of temperatures in cold storage units.

The report acknowledges that there are many obstacles to widespread deployment, from technical challenges (e.g. reliability, power, connectivity) to policy issues (e.g. interoperability, security, privacy). It is hoped that the report broadens the conversation on how the IoT, can play a positive role in development.

Source: ITU and Cisco Report: "Harnessing the Internet of Things for Global Development", (https://www.itu.int/en/action/broadband/Documents/Harnessing-IoT-Global-Development.pdf)

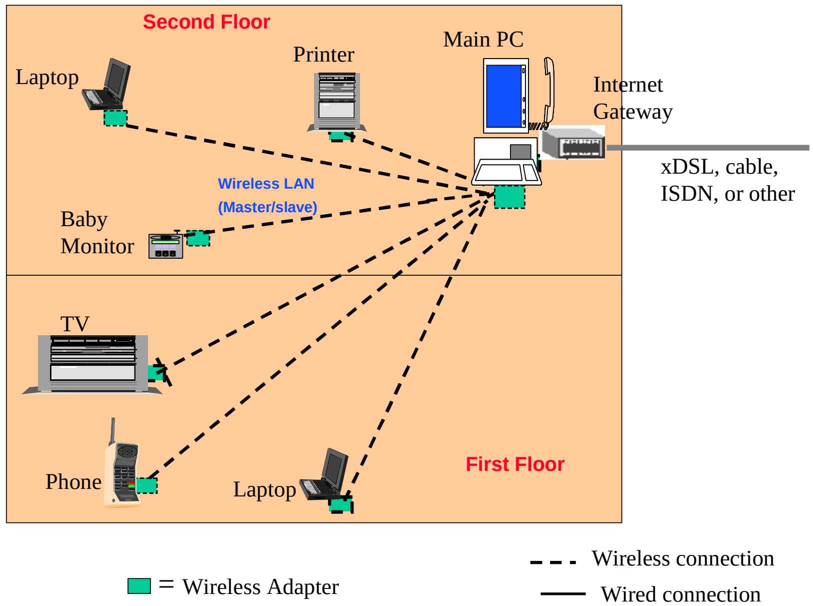
9.7 Short Examples of Sample IT Infrastructure Configurations

This section shows sample IT infrastructure configurations, from small LANs to large global networks. The configurations are highly simplified and can be used to represent many configurations encountered in technical architecture planning.

9.7.1 Home Networks (Small LANs)

Home networks are an area of explosive growth due to several laptops, desktops, and other computing devices in a typical home. Of course 802 based wired and wireless LANs can be used at home, but many different types of networks, especially wireless networks, are commonly available at home. The following diagram shows a conceptual view of a predominantly wireless home network that connects laptops, desktops, printers, phones and other devices though a wireless network. The main contenders for home networks are:

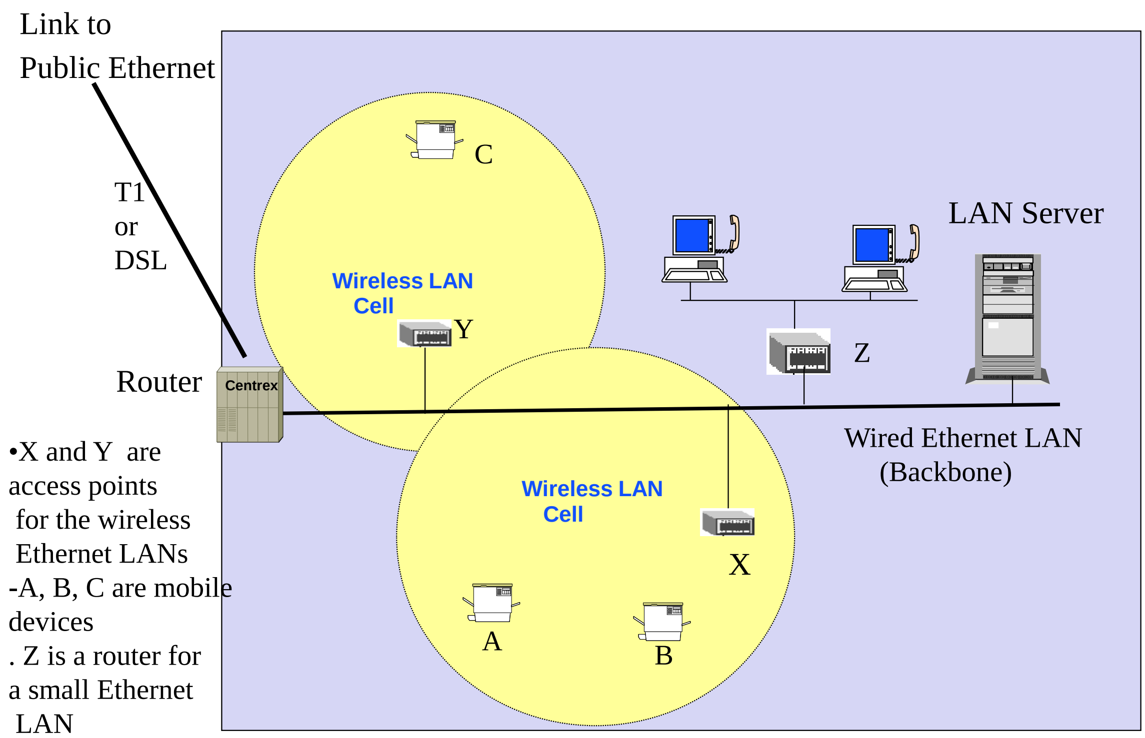
- Wireless and wired Ethernet (802) networks
- Bluetooth: 10 meters, 1 Mbps
- UWB (Ultra Wideband): very short-range (about a meter) but very high data rate (over 100 Mbps) applications such as connecting TV to VCR wirelessly.
- Wireless sensor networks (WSNs) for very small, low-powered sensor devices mainly for monitoring and data collection purposes (e.g., baby monitoring, etc).



9.7.2 Medium-sized (Single Floor) LANs

Almost all medium sized business LANs at present are based on the IEEE 802 standards committee that developed the very popular wired Ethernet (IEEE 802.3) and wireless Ethernet (IEEE802.11) Local Area Networks Standards. This includes the wired Ethernet LANs (10 Mbps over copper wires, 100 Mbps over fiber cables) and the wireless Ethernet LANs (11 Mbps 802.11b and 54 Mbps 802.11g). In most cases, a wired Ethernet LAN serves as a backbone to which several wired and wireless LANs are connected.

The following diagram shows a sample medium sized LAN. In this configuration, several wireless access points are connected to a wired LAN that is connected to the Internet and an internal server. Each access point supports mobile computers with wireless Ethernet cards in a wireless cell that spans around 100 meters.

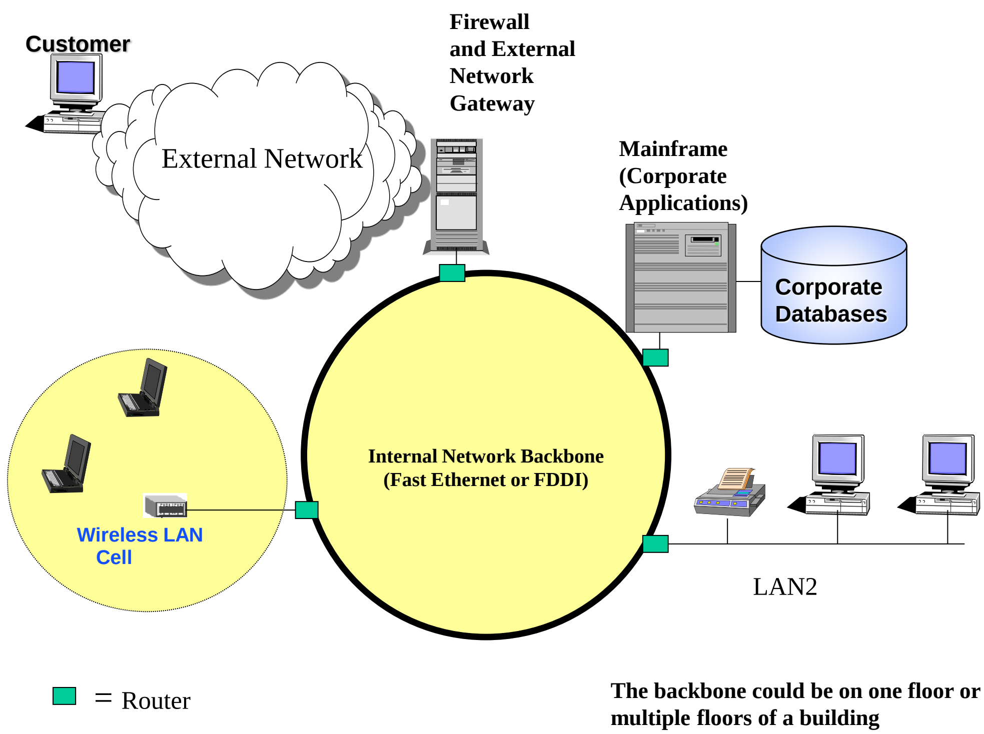


9.7.3 Large LANs (Large Building, Multiple Floors)

Large LANs that span multiple floors or multiple wings of a building typically use a a very strong backbone network that interconnects several individual LANs located in different parts of a building. Fiber is commonly used as a backbone because it has high bandwidth, is thin and lightweight, is not affected by electromagnetic interference from heavy machinery, and has excellent security due to difficulties in wiretapping. For these reasons, fiber optic is also very popular for metropolitan area networks.

Two types of technologies are used for large corporate backbones: Fast Ethernet (802.3U based on fiber) and FDDI (Fiber Distributed Data Interface). Although Fast Ethernet is popular, FDDI operate at 100 Mbps over distances up to 200 Km with 500 to 1000 stations connected with very low error rate (at most 1 error in 2500 million bits transmitted).

The following diagram shows a typical large LAN. The backbone of this network is a Fast Ethernet or FDDI LAN to which wireless as well as wired LANs plus mainframes and servers are connected through gateways (gateways are protocol converters that are used to interconnect different networks). It is common to also place the corporate firewall on the backbone for security reasons (single point of entry).

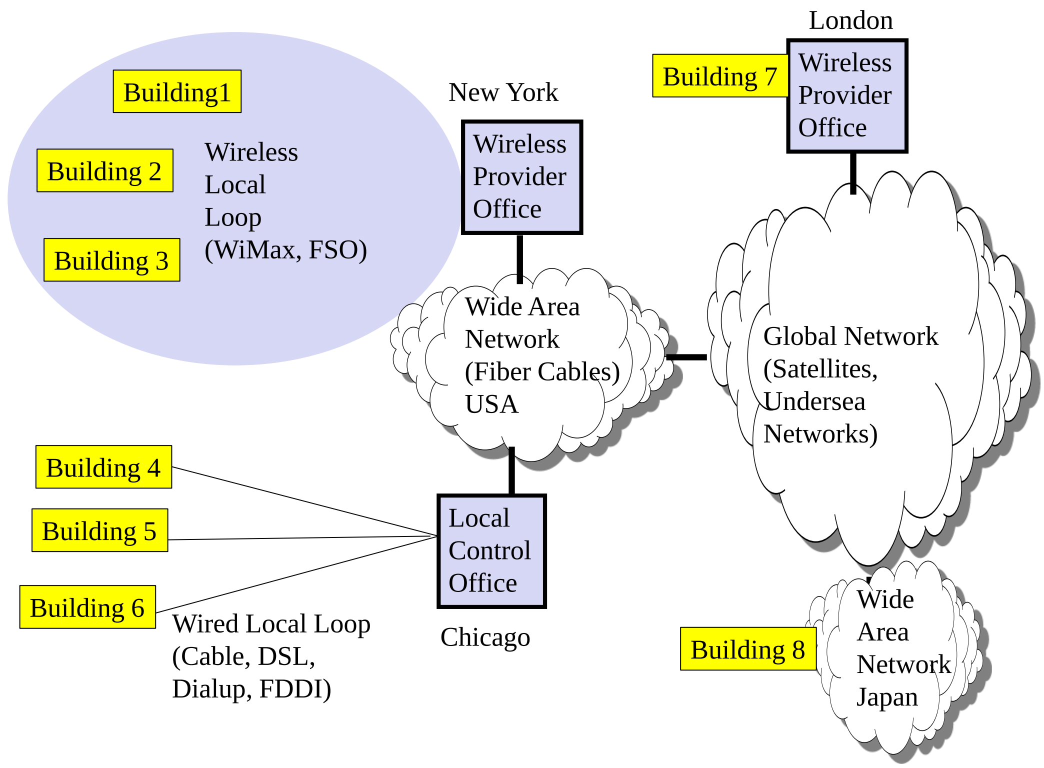


9.7.4 External Network in a Metropolitan Area

Metropolitan area network (MAN) technologies are commonly used for networks that may go upto 20 miles distance. These technologies are commonly used to support the local loops, also known as the last mile. MAN technologies include wireless as well as wired options:

- Wired options: FDDI (100 Mbps for upto 60 miles) or QDDB (150 Mbps for upto 15 miles)
- Wireless options: Wireless local loops such as Wimax (about 20-40 Mbps for 2-10 miles) or Free Space Optics (100 Mbps for upto 1 mile)

The following diagram shows a sample MAN configuration that consists of wired as well as wireless local loops. The local loops use MAN technologies. The local loops are connected to regional and global networks so that buildings located across continents can communicate with each other. For example, building1 communicates with building2 through a WLL. Building 1 (in New York) communicates with building 4 (in Chicago) through a WLL in New York, a regional wide area network between New York and Chicago, and a wired local loop in Chicago. A global network is used if Building1 wants to communicate with Building7 in London or Building8 in Tokyo.

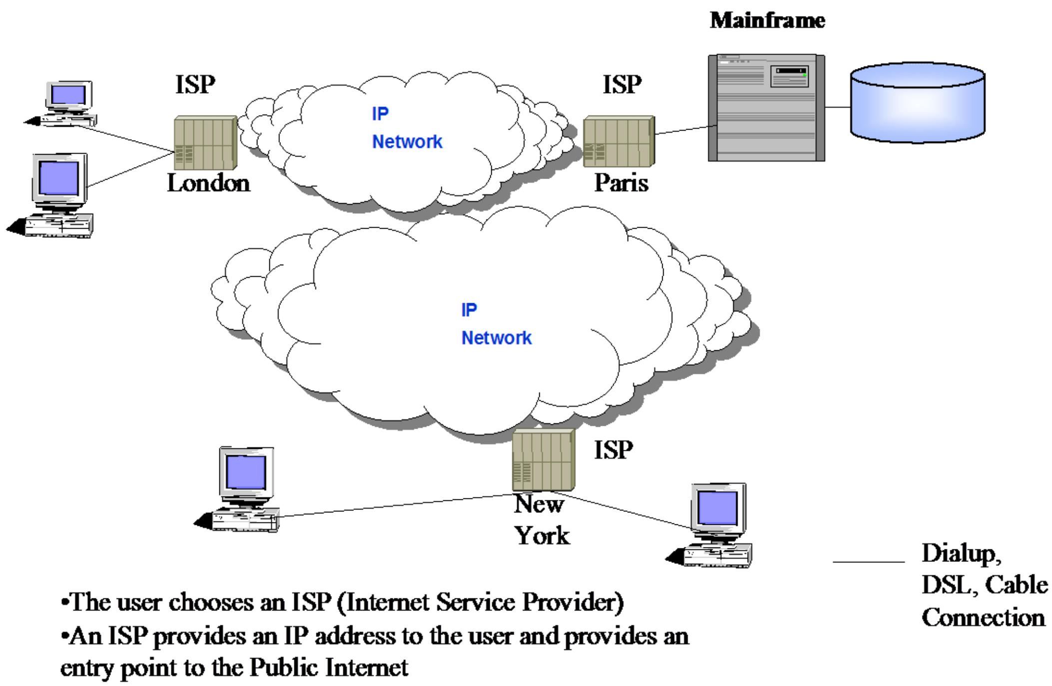


9.7.5 Regional Networks

Regional networks, commonly known as wide area networks (WANs), are commonly supported by using the Internet. Technically speaking, an Internet is a network of IP (Internet Protocol) networks. At present, the term *Internet* is used to refer to a large collection of IP networks that are tied together through network interconnectivity devices such as routers and gateways. *Internet* symbolizes the following situations:

- **Public Internet**, or just “the Internet,” that is not owned by any single entity – it consists of many independent IP networks that are tied together loosely.
- **Private Internets**, or intranets, are the IP networks that are used by corporations for their own business – they use the same technology as the public Internet but the underlying physical network is privately owned.
- **Extranets** are the IP networks that are jointly owned by corporations to conduct business.

The following diagram shows an end-user view of the Internet. This Internet shows two IP networks (in reality there are thousands of IP networks around the globe) The Internet is very heterogeneous (i.e., different computers, different physical networks). The entry point to the Internet is an ISP (Internet service Provider). An ISP basically provides an IP address to a user. Once a user has an IP address, then the user can send messages to any other device with another IP address. Thus an office in New York can send a message to a small provider in Malaysia or a partner in London, as long as they all have access to an ISP.

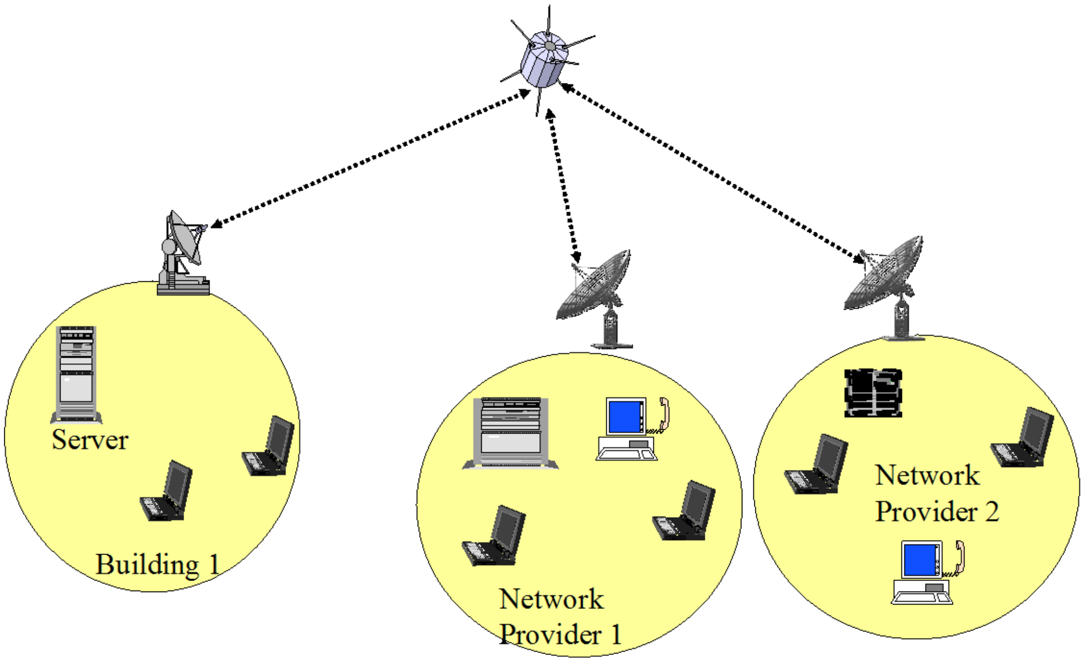


9.7.6 Global Networks

Global networks that span thousands of miles are typically supported through satellites. Although undersea networks between the US and England have been used in the past, most of the current and future global area networks are satellite-based. From an end-user point of view, satellites can deliver up to 50 Mbps over very wide (global) area networks to the subscribers. A satellite system consists of the following components:

- Earth Stations – antenna systems on or near earth.
- Uplink – transmission from an earth station to a satellite.
- Downlink – transmission from a satellite to an earth station (different from uplink, typically faster, can be broad).
- Transponder – electronics in the satellite that convert/amplify uplink signals to downlink signals. There are typically 16 to 20 transponders per satellite, each with 36-50 MHz BW (bandwidth).

The following diagram shows a typical global network based on satellites. The earth stations for the satellites can be an end-user building or a network provider that serves end-users.



A Sample Technology Pattern

As stated in chapter 2, patterns are a well-known format for capturing engineering knowledge. For the purpose of this book, a pattern *T* is a tuple *T(p, s, e)* where *p* is the problem to be solved, *s* is the solution (what works in practice), and *e* is an example. Additional information such as context, benefits, consequences, and limitations can also be added to a pattern to help the designer. In addition, each pattern is assigned a name. Pattern1 shows a pattern for small LANs.

Pattern1: Small (Single Room, SOHO) LANs

Problem:
How to design a small LAN for a single room or a SOHO (small office, home office).

Typical Solution:

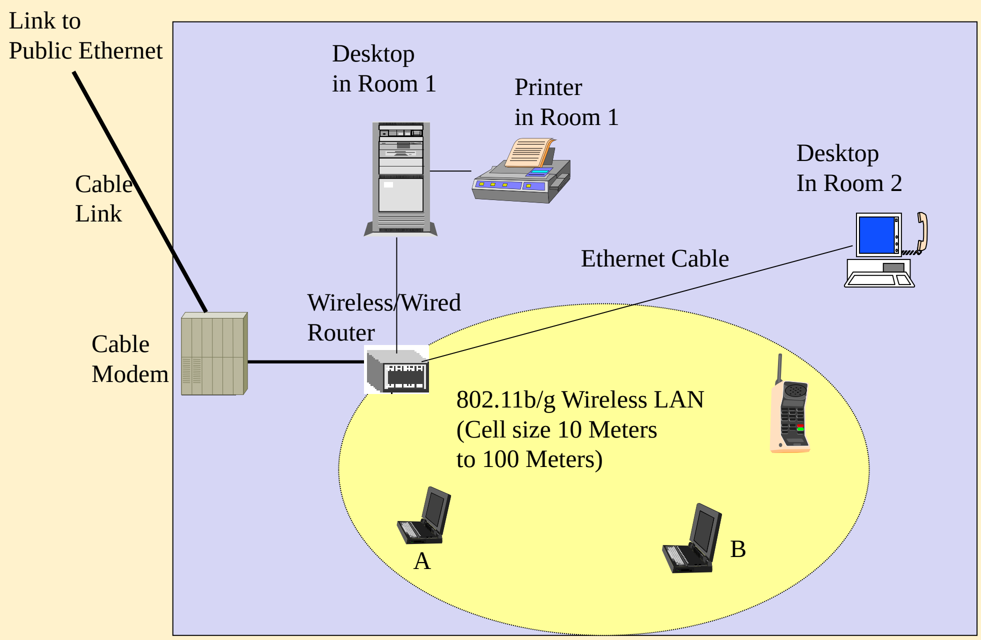
Most small LANs at present are based on the IEEE 802 standards committee that developed the very popular wired Ethernet (IEEE 802.3) and wireless Ethernet (IEEE802.11) Local Area Networks Standards. The older wired Ethernet LANs operate at 10 Million Bits Per Second (Mbps) over copper wires while the newer Ethernet (iEEE 802.11u) operate at 100 Mbps over fiber cables. Increasingly, wireless Ethernet (IEE 802.11) LANs are being used. These LANs operate at 11 Mbps (802.11b) and 54 Mbps (802.11g) and can support distances between 100 feet and 500 feet. Detailed information about these LANs can be found at the Wireless LAN Association Website (www.WLANA.org).

Although 802.11 LANs are very popular, Wireless Personal Area Networks (WPANs) for short-range (10 meter or less operating at 1 Mbps) personal, home, and other special uses are also popular.

Within the WPAN family, several specifications such as Bluetooth, wireless sensor networks, and UWB (Ultra Wideband) have emerged.

Example:

The following diagram shows a sample small LAN for a SOHO that uses wireless as well as wired Ethernet LANs. The workers can access the desktop in Room 1 (a server) plus access the public Internet through a cable modem. In this configuration, the wireless as well as wired devices are connected to a wireless/wired router. This router provides wireless access point as well as routing capabilities. The wireless LAN can be replaced with a Bluetooth LAN for small rooms.



9.7.7 Sample Application Architecture and Open Source

Let us quickly show how and where many of the technologies discussed so far fit into application architectures. Figure 9-31 shows the generic application architecture that was introduced previously. Many of the enabling technologies discussed in this chapter can be used at the front-end/back-end integration and business layers for enterprise applications. This diagram does not show the network infrastructure explicitly . However, the users, layers, and the back-end applications can reside on multiple computers that are interconnected through a network of LANs, WANs, and MANs over wired and wireless facilities.

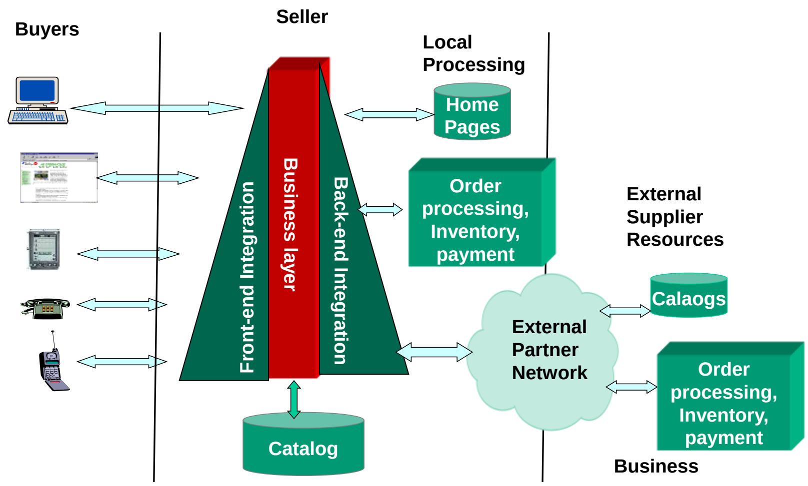


Figure 9-31: A Generic Application Architecture

Open source software is software for which source code is available so that it can be modified by software developers to fit their particular needs. This idea is gaining popularity as compared to the "closed source" systems in which the vendor keeps the source code as a proprietary internal asset. Open source software provides all computer users with free access to its source code so that they can modify the code to fix errors or to make improvements. The software itself is not owned by any company or individual and is free. Because it is free and can benefit from the expertise of numerous software developers, it has become popular during the past few years among sophisticated computer users and businesses. The best known examples of open source software are the Linux operating system, the Apache Web server, and the Kerberos security system. Here is an example of how a small company is using open source software.

A retail furniture dealer, Raymour & Flanagan (R&F) upgraded the network from dumb-terminals to 486-based personal computers with Linux as the operating system. To view inventory, the PCs use the Netscape web browser and Apache Web server, also an open source product, was used for web users. The routers are managed with NetSaint (http://www.netsaint.org/), an open-source code program. The network supports 50 stores in the northeastern part of the United States over T1 connections to an IP-and-frame relay WAN. Advantages of this type of system include:
Open source software for customizable applications

- Nominal, if any, licensing fees
- Nominal, if any, software update costs
- “Very” thin client configuration that consists of a Web browser residing on a customized kernel / OS on a low-end PC (Intel 40486 processor with 32 meg RAM or an Apple).

A disadvantage of this type of system may include the need to run a “dual shop” Linux and Windows for some applications because some applications are not available on Linux. Overall, this appears to be practical albeit slightly more labor-intensive alternatives to the typical Microsoft applications for network deployment. While potentially slightly more labor intensive, R&F indicated that overall performance is quite satisfactory and the cost savings appear to be fairly substantial.

9.8 Summary

IT infrastructure provides the technologies needed to *enable* the enterprise applications. In this chapter, we have concentrated on the following main IT building blocks and their role in enabling modern enterprises:

- Networks and the Internet
- Web technologies that reside on the Internet
- Mobile computing and wireless communications that provide mobile apps over wireless networks .
- IoT and WoT devices and applications that utilize a combination of all of the above

Several examples and case studies illustrate the key points. After reading this chapter, you should be able to answer the following questions:

- What are the key network concepts
- What is a network architectures and what are its key components
- What is the Open System Interconnection (OSI) Reference Model and how does it help in network interconnectivity
- What are the key characteristics of broadband and wireless networks
- What is the Internet and how does it support modern enterprises
- What are Intranets and Extranets
- What is Next Generation Internet (NGI) and what is its role in the
- What is Web and what are the key Web technologies
- What is Web 2.0 and Social Networking
- What is Mobile Computing and what are its key components
- What are the examples of Mobile Computing Applications of value to modern enterprises
- What are the key aspects of Wireless Networks

9.9 Major References

[1] Barrett, R., “Wireless Networks and Mobile Computing”, Wilford Press, 2016
[2] Beard, C. and Stallings, W. , "Wireless Communication Networks and Systems", Pearson, 2015
[3] Dietel, H., “Internet and World Wide Web: How To Program”, Pearson, 5th Edition, 2011
[4] Greengard, S., “The Internet of Things (The MIT Press Essential Knowledge series)”, MIT Press, 2015
[5] Sinha, K. and Ghosh, S., “Wireless Networks and Mobile Computing”, Chapman and Hall, 2015
[6] Stallings, W., "Data and Computer Communications", 10th Edition, Pearson, 2013
[7] Umar, A., “Mobile Computing And Wireless Communications: Applications, Networks, Platforms, Architectures and Security”, NGE Solutions, 2004
[8] Umar, A., “Enterprise Architecture and Integration”, Second Edition, Target: 2017, NGE Solutions, Inc.
[9] Umar, A., "Distributed Computing and Client/server Systems", Prentice Hall, revised edition, 1993.
[10] Wilbur, S. and Bacarisse, B., "Building Distributed Systems with Remote Procedure Calls", Software Engineering Journal, Sept. 1987, pp. 148 - 159.
[11] Whyte, W., and Whyte; B., "Enabling e-business - Integrating Technologies Architectures & Applications", John Wiley & Sons; 2001.
[12] Wooding, T., "Business Frameworks", Object Magazine, January 1997, pp. 50-53.
[13] Wu, J., "Distributed System Design", CRC Press; 1998.