

- ◆ the direction of the exchanges
 - ◆ the transmission mode: the number of bits sent simultaneously
 - ◆ synchronization between the transmitter and receiver
- A. **Serial versus Parallel Transmission:** The transmission mode refers to the number of elementary units of information (bits) that can be simultaneously translated by the communications channel. There are two modes of transmitting digital data. These methods are Serial and Parallel Transmission.
- **Serial Transmission:** In serial transmission, the bits of each byte are sent along a single path one after another as illustrated in Fig 3.5.8. RS-232 is an example of serial port used for the mouse or MODEM.

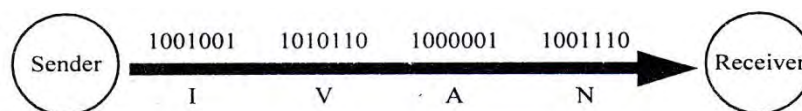


Fig. 3.7.3: Serial Transmission

- **Parallel Transmission:** In parallel transmission, there are separate, parallel paths corresponding to each bit of the byte so that all character bits are transmitted simultaneously as shown in Fig 3.5.9. Centronic port is the example of parallel port used for printer.

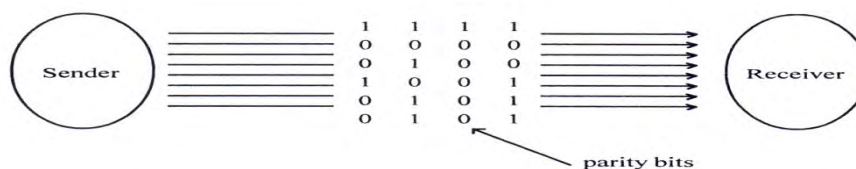


Fig. 3.7.4: Parallel Transmission

Table 3.7.1: Serial Transmission vs Parallel Transmission

S.No	SERIAL TRANSMISSION	PARALLEL TRANSMISSION
1	In this, the data bits are transmitted serially one after another.	In this, the data bits are transmitted simultaneously.
2	Data is transmitted over a single wire.	Data is transmitted over 8 different wires.
3	It is a cheaper mode of transferring data.	It is relatively expensive mode of transferring data.
4	It is useful for long distance data transmissions.	Not practical for long distance communications as it uses parallel paths, so cross talk may occur.
5	It is relatively slower	It is relatively faster.

B. **Synchronous versus Asynchronous Transmission:** As in serial connections, wherein a single wire transports the data, the problem is how to synchronize the transmitter and receiver, in other words, the receiver can not necessarily distinguish the characters (or more generally the bit sequences) because the bits are sent one after the other. When a computer sends the data bits and parity bit down the same communication channel, the data are grouped together in predetermined bit patterns for the receiving devices to recognize when each byte (character) has been transmitted. There are two basic ways of transmitting serial binary data that addresses the problem of sequencing and re-arranging of data at receiver end: synchronous and asynchronous. There are two types of transmission that address this problem:

- **Asynchronous Transmission:** In this, each character is sent at irregular intervals in time as in the case of characters entered at the keyboard in real time. So, for example, imagine that a single bit is transmitted during a long period of silence... the receiver will not be able to know if this is 00010000, 10000000 or 00000100.. To correct this problem, each character is preceded by some information indicating the start of character transmission by start-of-transmission information (called a START bit usually 0) and ends by sending end-of-transmission information (called STOP bit usually 1), as shown in Fig 3.7.5.

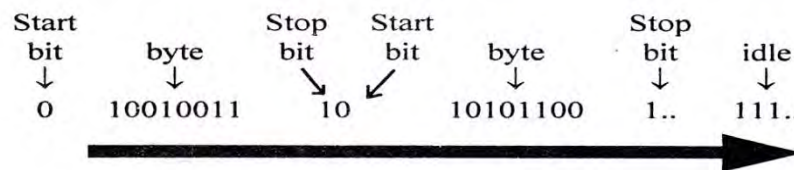


Fig. 3.7.5: Asynchronous Transmission

- **Synchronous Transmission:** In this, the transmitter and receiver are paced by the same clock. The receiver continuously receives (even when no bits are transmitted) the information at the same rate the transmitter sends it. This is why the transmitter and receiver are paced at the same speed. In addition, supplementary information is inserted to guarantee that there are no errors during transmission, as shown in Fig 3.7.6.

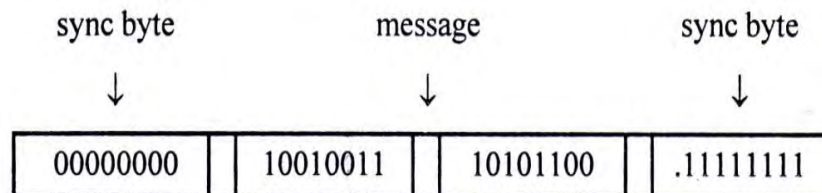


Fig. 3.7.6: Synchronous Transmission

A group of synchronization bits must be placed at the beginning and ending of each block to maintain synchronization.

Table 3.7.2 lists the differences between Asynchronous and Synchronous Transmission.

Table 3.7.2: Asynchronous vs Synchronous Transmission

S.No.	ASYNCHRONOUS TRANSMISSION	SYNCHRONOUS TRANSMISSION
1	Each data word is accompanied by start and stop bits.	Allows characters to be sent down the line without start-stop bits.
2	Extra Start and Stop bits slow down the transmission process relatively.	Transmission is faster as in absence of start and stop bits, many data words can be transmitted per second.
3	It is relatively cheaper.	The synchronous device is more expensive to build as it must be smart enough to differentiate between the actual data and the special synchronous characters.
4	More reliable as the start and stop bits ensure that the sender and the receiver remain in step with one another.	Chances of data loss are relatively higher.
5	It is less efficient.	It is more efficient.

C. Transmission Modes: There are three different transmission modes characterized according to the direction of the exchanges:

- **Simplex Connection:** A simplex connection is a connection in which the data flows in only one direction, from the transmitter to the receiver. This type of connection is useful if the data do not need to flow in both directions (for example, from your computer to the printer or from the mouse to your computer.).
- **Half-duplex Connection:** A half-duplex connection (sometimes called an *alternating connection* or *semi-duplex*) is a connection in which the data flows in one direction or the other, but not both at the same time. This type of connection makes it possible to have bidirectional communications using the full capacity of the line. For example: Walkie Talkie.
- **Full-Duplex Connection:** A Full-duplex connection is a connection in which the data flow in both directions simultaneously. Each end of the line can thus transmit and receive at the same time, which means that the bandwidth is divided in two for each direction of data transmission if the same transmission medium is used for both directions of transmission. For example, mobile phones.

- D. **Transmission Techniques:** A communication network consists of a collection of devices (or nodes) that wish to communicate and interconnect together. The primary objective in any communication network is simply moving information from one source to one or more destination nodes. Based on the techniques used to transfer data, communication networks can be categorized into Broadcast and Switched networks. In Broadcast networks, data transmitted by one node is received by many, sometimes all, of the other nodes.

In switched-communication networks, however, the data transferred from source to destination is routed through the switch nodes. The way in which the nodes switch data from one link to another as it is transmitted from source to destination node is referred to as a switching technique. Three common switching techniques are **Circuit Switching**, **Packet Switching**, and **Message Switching**.

- (i) **Circuit Switching:** A Circuit Switching network is one that establishes a fixed bandwidth circuit (or channel) between nodes and terminals before the users may communicate, as if the nodes were physically connected with an electrical circuit. The route is dedicated and exclusive, and released only when the communication session terminates. Circuit switching is what most of us encounter on our home phones. A single circuit is used for the entire duration of the call.
- (ii) **Packet Switching:** It is a sophisticated means of maximizing transmission capacity of networks. Packet switching refers to protocols in which messages are broken up into small transmission units called packets, before they are sent. Each packet is transmitted individually across the net. The packets may even follow different routes to the destination.
- (iii) **Message Switching:** In message switching, end-users communicate by sending each other a message, which contains the entire data being delivered from the source to destination node. As a message is routed from its source to its destination, each intermediate switch within the network stores the entire message, providing a very reliable service. The intermediary nodes (switches) have the responsibility of conveying the received message from one node to another in the network. Therefore, each intermediary node within the network must store all messages before retransmitting them one at a time as proper resources become available. This characteristic is often referred to as **Store-and-Forward**.

Electronic mail (e-mail) and voice mail are examples of message switching systems.

3.7.3 Network Architectures and Protocols

Network Architecture: Network architecture refers to the layout of the network, consisting of the hardware, software, connectivity, communication protocols and mode of transmission, such as wired or wireless. The diagram of the network architecture provides a full picture of the established network with detailed view of all the resources accessible.

In other words, network architecture includes hardware components used for communication, cabling and device types, network layout and topologies, physical and wireless connections, implemented areas and future plans. In addition, the software rules and protocols also constitute to the network architecture. This architecture is always designed by a network manager/administrator with coordination of network engineers and other design engineers.

The goal of network architectures is to promote an open, simple, flexible, and efficient telecommunications environment. This is accomplished by the use of:

- ◆ Standard protocols,
- ◆ Standard communications hardware and software interfaces, and
- ◆ Standard multilevel interface between end users and computer systems.

Protocols: A protocol is the formal set of rules for communicating, including rules for timing of message exchanges, the type of electrical connection used by the communications devices, error detection techniques, means of gaining access to communications channels, and so on. The goal of communications network architectures is to create more standardization and compatibility among communications protocols.

A. The OSI Model

The International Standards Organization (ISO) is working on the establishment of a standard protocol for data transmission. They have developed a seven-layer Open Systems Interconnection (OSI) model to serve as a standard model for network architectures. Dividing data communications functions into seven distinct layers promotes the development of modular network architectures, which assists the development, operation, and maintenance of complex telecommunications networks. Seven layers of OSI include:

- ◆ **Layer 7 or Application Layer:** The application layer of OSI layer architecture is closest to the end user, which means that both the OSI application layer and the user interact directly with the software application. This layer interacts with software applications and provides user services by file transfer, file sharing, etc. Database concurrency and deadlock situation controls are undertaken at this layer level. This is the layer at which communication partners are identified, quality of service is identified, user authentication and privacy are considered, and any constraints on data syntax are identified.
- ◆ **Layer 6 or Presentation Layer:** This layer at times referred as Syntax Layer also, is usually a part of an operating system, that converts incoming and outgoing data from one presentation format to another (for example, from a text stream into a popup window with the newly arrived text). The presentation service data units are then encapsulated into Session Protocol Data Units, and moved down the stack. It further controls on screen display of data, transforms data to a standard application interface. Encryption, data compression can also be undertaken at this layer level.
- ◆ **Layer 5 or Session Layer:** This layer sets up, coordinates, and terminates conversations, exchanges, and dialogs between the applications at each end. It deals

with session and connection coordination. It provides for full-duplex, half-duplex, or simplex operation, and establishes check pointing, adjournment, termination, and restart procedures. The OSI model made this layer responsible for "graceful close" of sessions also.

- ◆ **Layer 4 or Transport Layer:** This layer also ensures reliable and transparent transfer of data between user processes, assembles and disassembles message packets, and provides error recovery and flow control. Multiplexing and encryption are undertaken at this layer level. This means that the Transport Layer can keep track of the segments and retransmit those that fail.
- ◆ **Layer 3 or Network Layer:** The Network Layer provides the functional and procedural means of transferring variable length data sequences from a source to a destination via one or more networks, while maintaining the quality of service requested by the Transport Layer. The Network Layer makes a choice of the physical route of transmission, creates a virtual circuit for upper layers to make them independent of data transmission and switching, establishes, maintains, terminates connections between the nodes and ensure proper routing of data.
- ◆ **Layer 2 or Data Link Layer:** The Data Link Layer responds to service requests from the Network Layer and issues service requests to the Physical Layer. The Data Link Layer is the protocol layer which transfers data between adjacent network nodes in a wide area network or between nodes on the same local area network segment. This layer is also a hardware layer which specifies channel access control method and ensures reliable transfer of data through the transmission medium. It provides the functional and procedural means to transfer data between network entities and to detect and possibly correct errors that may occur in the Physical Layer.
- ◆ **Layer 1 or Physical Layer:** The Physical Layer is a hardware layer which specifies mechanical features as well as electromagnetic features of the connection between the devices and the transmission. In particular, it defines the relationship between a device and a physical medium. This includes the layout of pins, voltages, cable specifications, Hubs, repeaters, network adapters, Host Bus Adapters (HBAs used in Storage Area Networks) and more.

The major functions and services performed by the Physical Layer are:

- ◆ Establishment and termination of a connection to a communications medium.
- ◆ Participation in the process whereby the communication resources are effectively shared among multiple users. For example, contention resolution and flow control.
- ◆ Modulation or conversion between the representation of digital data in user equipment and the corresponding signals transmitted over a communications channel. These are signals operating over the physical cabling (such as copper and optical fiber) or over a radio link.

B. The Internet's TCP/IP

The Internet uses a system of telecommunications protocols that has become so widely used that it is equivalent to network architecture. The Internet's protocol suite is called Transmission Control Protocol/Internet Protocol and is known as TCP/IP. TCP/IP consists of five levels of protocols that can be related to the seven layers of the OSI architecture. TCP/IP is used by the Internet and by all Intranets and extranets. Many companies and other organizations are also converting their client/server networks to TCP/IP.

Five levels of TCP/IP include as shown in the Fig. 3.7.7 are as follows:

- ◆ Application or process layer
- ◆ Host-to-Host Transport layer
- ◆ Internet Protocol (IP)
- ◆ Network Interface
- ◆ Physical layer

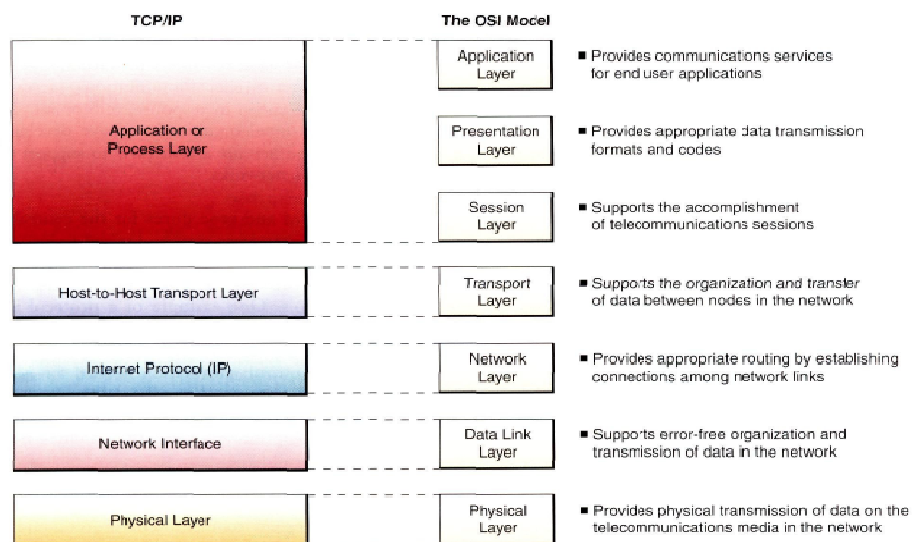


Fig. 3.7.7: Relationship between layers of TCP/IP and OSI Model

3.8 Network Risks, Controls and Security

The basic objective for providing network security is two-fold:

- (i) to safeguard assets, and
- (ii) to ensure and maintain the data integrity.

The boundary subsystem is an interface between the potential users of a system and the system itself. Controls in the boundary subsystem have the following purposes like

- (i) to establish the system resources that the users desire to employ and
- (ii) to restrict the actions undertaken by the users who obtain the system resource to an authorized set.

There are two types of systems security. A physical security is implemented to protect the physical systems assets of an organization like the personnel, hardware, facilities, supplies and documentation. A logical security is intended to control (i) malicious and non-malicious threats to physical security and (ii) malicious threats to logical security itself.

3.8.1 Threats and Vulnerabilities

Threat: A threat is anything that can disrupt the operation, functioning, integrity, or availability of a network or system. Network security threats can be categorized into four broad themes:

- ◆ **Unstructured Threats** - These originate mostly from inexperienced individuals using easily available hacking tools from the Internet. Many tools available to anyone on the Internet can be used to discover weaknesses in a company's network. These include port-scanning tools, address-sweeping tools, and many others. Most of these kinds of probes are done more out of curiosity than with a malicious intent in mind.

For example, if a company's external web site is hacked; the company's integrity is damaged. Even if the external web site is separate from the internal information that sits behind a protective firewall, the public does not know that. All they know is that if the company's web site is hacked, then it is an unsafe place to conduct business.

- ◆ **Structured Threats** - These originate from individuals who are highly motivated and technically competent and usually understand network systems design and the vulnerabilities of those systems. They can understand as well as create hacking scripts to penetrate those network systems. An individual who presents a structured threat typically targets a specific destination or group. Usually, these hackers are hired by industry competitors, or state-sponsored intelligence organizations.
- ◆ **External Threats** - These originate from individuals or organizations working outside an organization, which does not have authorized access to organization's computer systems or network. They usually work their way into a network from the Internet or dialup access servers.
- ◆ **Internal Threats** - Typically, these threats originate from individuals who have authorized access to the network. These users either have an account on a server or physical access to the network. An internal threat may come from a discontented former or current employee or contractor. It has been seen that majority of security incidents originate from internal threats.

Vulnerability: Vulnerability is an inherent weakness in the design, configuration, or implementation of a network or system that renders it susceptible to a threat.

The following facts are responsible for occurrence of vulnerabilities in the software:

- ◆ **Software Bugs** - Software bugs are so common that users have developed techniques to work around the consequences, and bugs that make saving work necessary every half an hour or crash the computer every so often are considered to be a normal part of computing. For example - buffer overflow, failure to handle exceptional conditions, access validation error, input validation errors are some of the common software flaws.
- ◆ **Timing Windows** - This problem may occur when a temporary file is exploited by an intruder to gain access to the file, overwrite important data, and use the file as a gateway for advancing further into the system.
- ◆ **Insecure default configurations** - Insecure default configurations occur when vendors use known default passwords to make it as easy as possible for consumers to set up new systems. Unfortunately, most intruders know these passwords and can access systems effortlessly.
- ◆ **Bad Protocols** - Some protocols, or the standards by which information is exchanged over the Internet, lack any security at all. For example, unsolicited commercial email, commonly referred to as "spam," is the irritating result of poor protocol programming.
- ◆ **Trusting Untrustworthy information** - This is usually a problem that affects routers, or those computers that connect one network to another. When routers are not programmed to verify that they are receiving information from a unique host, bogus routers can gain access to systems and do damage.
- ◆ **End users** - Generally, users of computer systems are not professionals and are not always security conscious. For example, when the number of passwords of an user increases, user may start writing them down, in the worst case to places from where they are easy to find. In addition to this kind of negligence towards security procedures users do human errors, for example save confidential files to places where they are not properly protected.

3.8.2 Level of Security

The task of a Security Administration in an organization is to conduct a security program which is a series of ongoing, regular and periodic review of controls exercised to ensure safeguarding of assets and maintenance of data integrity. Security programs involve the following eight steps –

- (i) **Preparing project plan for enforcing security:** The project plan components are at first outlining the objectives of the review followed by in sequence determining the scope of the review and tasks to be accomplished, assigning tasks to the project team after organizing it, preparing resources budget which will be determined by the volume and complexity of the review and fixing a target / schedule for task completion.
- (ii) **Asset identification:** Assets which need to be safeguarded can be identified and subdivided into Personnel, Hardware, Facilities, Documentation, Supplies, Data, Application Software and System Software.

(iii) **Asset valuation:** This step of valuation of assets can pose a difficulty. The process of valuation can differ depending on who is asked to render the valuation, the way in which the asset can be lost and the period for which it is lost and how old is the asset.

Valuation of physical assets cannot be considered apart from the valuation of the logical assets. For example, the replacement value of the contents in a micro computer's hard disk may be several times more than the replacement value of the disk itself.

(iv) **Threat identification:** The source of a threat can be external or internal and the nature of a threat can be accidental / non-deliberate or deliberate. The example of a non-deliberate external threat is an act of God, non-deliberate internal threat is pollution, deliberate external threat is hackers, and deliberate internal threat is employees.

(v) **Threats probability of occurrence assessment:** This step is an assessment of the probability of occurrence of threats over a given time period. This exercise is not so difficult if prior period statistical data is available. If however, prior period data is not available, it has to be elicited from the associated stakeholders like end users (furnishing the data aspect) and the management (furnishing the control aspect).

(vi) **Exposure analysis:** This step is the Exposures Analysis by first identifying the controls in the place, secondly assessing the reliability of the existing controls, thirdly evaluating the probability that a threat can be successful and lastly assessing the resulting loss if the threat is successful. For each asset and each threat the expected loss can be estimated as the product of the probability of threat occurrence, probability of control failure and the resulting loss if the threat is successful.

(vii) **Controls adjustment:** This involves the adjustment of controls which means whether over some time period any control can be designed, implemented and operated such that the cost of control is lower than the reduction in the expected losses. The reduction in the expected losses is the difference between expected losses with the (i) existing set of controls and (ii) improved set of controls.

(viii) **Report generation outlining the levels of security to be provided for individual systems, end user, etc.:** This is the last step that involves report generation documenting, the findings of the review and specially recommending new assets safeguarding techniques that should be implemented and existing assets safeguarding mechanisms that should be eliminated / rectified, and also recommending the assignment of the levels of security to be pervaded for individual end users and systems.

3.8.3 Network Security Protocols

Network Security Protocols are primarily designed to prevent any unauthorized user, application, service or device from accessing network data. This applies to virtually all data types regardless of the network medium used. Network security protocols generally implement cryptography and encryption techniques to secure the data so that it can only be decrypted with a special algorithm, logical key, mathematical formula and/or a combination of all of them.

Cryptography: Cryptography is the practice and study of techniques for secure communication in the presence of third parties (called Adversaries). More generally, it is about constructing and analyzing protocols that overcome the influence of adversaries and which are related to various aspects in information security such as data confidentiality, integrity, authentication, and non-repudiation.

Encryption: In Cryptography, encryption is the process of encoding messages (or information) in such a way that eavesdroppers or hackers cannot read it, but only authorized parties can.

- ◆ **Plaintext** - It is the message that is to be encrypted,. It is transformed by a function that is parameterized by a key.
- ◆ **CipherText** - It is the output of the encryption process that is transmitted often by a messenger or radio.
- ◆ **Encryption Model** - The intruder may hear and accurately copies down the complete ciphertext. However, unlike the intended recipient, he does not know what the decryption key is and so cannot decrypt the ciphertext easily. Sometimes the intruder can not only listen to the communication channel (passive intruder) but can also record messages and play them back later, inject his own messages, or modify legitimate messages before they get to the receiver (active intruder). The art of breaking ciphers, known as **Cryptanalysis**, and the art of devising them (cryptography) are collectively known as **Cryptology**.

There are two basic approaches to encryption:

- (i) Hardware encryption devices are available at a reasonable cost, and can support high-speed traffic. If the Internet is being used to exchange information among branch offices or development collaborators, for instance, use of such devices can ensure that all traffic between these offices is secure.
- (ii) Software encryption is typically employed in conjunction with specific applications. Certain electronic mail packages, for example, provide encryption and decryption for message security.

Some of the popular network security protocols include Secure Shell (SSH), Secure File Transfer Protocol (SFTP), Secure Hypertext Transfer Protocol (HTTPS) and Secure Socket Layer (SSL) etc..

- ◆ **SSH** - Secure Shell is a program to log into another computer over a network, to execute commands in a remote machine, and to move files from one machine to another. It provides strong authentication and secure communications over insecure channels. SSH protects a network from attacks such as IP spoofing, IP source routing, and DNS spoofing. An attacker cannot play back the traffic or hijack the connection when encryption is enabled. During ssh login, the entire login session, including transmission of password, is encrypted; therefore it is almost impossible for an outsider to collect passwords.

- ◆ SFTP – The SSH File Transfer Protocol (also known as Secure FTP and SFTP) is a computing network protocol for accessing and managing files on remote file systems. Unlike standard File Transfer Protocol (FTP), SFTP encrypts commands and data both, preventing passwords and sensitive information from being transmitted in the clear over a network.
- ◆ HTTPS – Hypertext Transfer Protocol Secure (HTTPS) is a communications protocol for secure communication over a computer network, with especially wide deployment on the Internet. The security of HTTPS uses long term public and secret keys to exchange a short term session key to encrypt the data flow between client and server.
- ◆ SSL – It is essentially a protocol that provides a secure channel between two machines operating over the Internet or an internal network. In today's Internet focused world, the SSL protocol is typically used when a web browser needs to securely connect to a web server over the inherently insecure Internet. In practice, SSL is used to secure online credit card transactions, system logins and any sensitive information exchanged online, to secure webmail and applications like Outlook Web Access, Exchange and Office Communications Server, to secure the connection between an email client such as Microsoft Outlook and an email server such as Microsoft Exchange, to secure intranet based traffic such as internal networks, file sharing, extranets, and database connections etc.

3.8.4 Network Security Techniques

As data is shared and organizations become connected to the outside world, the possibility of data exposure to vendors, service providers, and trading partners is significantly increased.

In spite of the varied concerns, corporations understand that the Internet is clearly the most promising infrastructure for “anywhere, anytime” electronic communication between businesses, customers, and suppliers; and progress is being made as companies further realize and respond to these concerns. Several tools are now available to protect information and systems against compromise, intrusion, or misuse:

1. **Firewall:** Firewall is a device that forms a barrier between a secure and an open environment when the latter environment is usually considered hostile, for example, the Internet. It acts as a system or combination of systems that enforces a boundary between more than one networks. Access controls are common form of controls encountered in the boundary subsystem by restricting the use of system resources to authorized users, limiting the actions authorized users can take with these resources and ensuring that the users obtain only authentic system resources.
2. **Message authentication** makes sure that a message is really from whom it purports to be and that it has not been tampered with. Regardless of a company's individual needs, clearly defined Internet security policies and procedures should always be part of any corporate Internet security strategy.

3. **Site Blocking** is a software-based approach that prohibits access to certain Web sites that are deemed inappropriate by management. For example, sites that contain explicit objectionable material can be blocked to prevent employee's from accessing these sites from company Internet servers. In addition to blocking sites, companies can also log activities and determine the amount of time spent on the Internet and identify the sites visited.
4. **IDS Technologies:** An **Intrusion Detection System (IDS)** is a device or software application that monitors network or system activities for malicious activities or policy violations and produces reports to a Management Station. The goal of intrusion detection is to monitor network assets to detect anomalous behavior and misuse. Primary IDS technologies are defined as follows:
 - **Network Intrusion Detection (NID):** Network Intrusion Detection System is placed on a network to analyze traffic in search of unwanted or malicious events on the wire between hosts. Typically referred to as "packet-sniffers", network intrusion detection devices intercept packets traveling along various communication mediums and protocols, usually TCP/IP.
 - **Host-based Intrusion Detection (HID):** Host-based Intrusion Detection systems are designed to monitor, detect, and respond to user and system activity and attacks on a given host. The difference between host-based and network-based intrusion detection is that NID deals with data transmitted from host to host while HID is concerned with what occurs on the hosts themselves.
 - Host-based intrusion detection is best suited to combat internal threats because of its ability to monitor and respond to specific user actions and file accesses on the host.
 - **Hybrid Intrusion Detection:** Hybrid Intrusion Detection systems offer management of and alert notification from both network and host-based intrusion detection devices. Hybrid solutions provide the logical complement to NID and HID - central intrusion detection management.
 - **Network-Node Intrusion Detection (NNID):** Network-Node Intrusion Detection was developed to work around the inherent flaws in traditional NID. Network-node pulls the packet-intercepting technology off the wire and puts it on the host. With NNID, the "packet-sniffer" is positioned in such a way that it captures packets after they reach their final target, the destination host. This scheme came from a HID-centric assumption that each critical host would already be taking advantage of host-based technology. Network node's major disadvantage is that it only evaluates packets addressed to the host on which it resides. The advantage of NNID is its ability to defend specific hosts against packet-based attacks in these complex environments where conventional NID is ineffective.

3.9 Network Administration and Management

In computer networks, network management refers to the activities, methods, procedures, and tools that pertain to the operation, administration, maintenance, and provisioning of networked systems. Network management is essential to command and control practices and is generally carried out of a network operations center.

- ◆ Operation deals with keeping the network (and the services that the network provides) up and running smoothly. It includes monitoring the network to spot problems as soon as possible, ideally before users are affected.
- ◆ Administration deals with keeping track of resources in the network and how they are assigned. It includes all the "housekeeping" that is necessary to keep the network under control.
- ◆ Maintenance is concerned with performing repairs and upgrades—for example, when equipment must be replaced, when a router needs a patch for an operating system image, when a new switch is added to a network. Maintenance also involves corrective and preventive measures to make the managed network run "better", such as adjusting device configuration parameters.
- ◆ Provisioning is concerned with configuring resources in the network to support a given service. For example, this might include setting up the network so that a new customer can receive voice service.

A common way of characterizing network management functions is FCAPS—Fault, Configuration, Accounting, Performance and Security.

Functions that are performed as part of network management accordingly include controlling, planning, allocating, deploying, coordinating, and monitoring the resources of a network, network planning, frequency allocation, predetermined traffic routing to support balancing, cryptographic distribution authorization, configuration management, fault management, security management, management, bandwidth management, Route analytics and accounting management.

3.10 The Internet Revolution

The Internet is the largest "network of networks" today, and the closest model we have to the information superhighway of tomorrow. Some distinguishing features of the Internet include:

- ◆ The Net does not have a central computer system or telecommunications center. Instead, each message sent on the Internet has a unique address code so any Internet server in the network can forward it to its destination.
- ◆ The Net does not have a headquarters or governing body.
- ◆ The Internet is growing rapidly.

Fig. 3.10.1 shows the strategic capabilities of Internet along with their business applications

Strategic Capabilities	e-Business Examples	Business Value
Overcome geographic barriers: Capture information about business transactions from remote locations	Use the Internet and extranets to transmit customer orders from traveling salespeople to a corporate data center for order processing and inventory control	Provides better customer service by reducing delay in filling orders and improves cash flow by speeding up the billing of customers
Overcome time barriers: Provide information to remote locations immediately after it is requested	Credit authorization at the point of sale using online POS networks	Credit inquiries can be made and answered in seconds
Overcome cost barriers: Reduce the cost of more traditional means of communication	Desktop videoconferencing between a company and its business partners using the Internet, intranets, and extranets	Reduces expensive business trips; allows customers, suppliers, and employees to collaborate, thus improving the quality of decisions reached
Overcome structural barriers: Support linkages for competitive advantage	Business-to-business electronic commerce websites for transactions with suppliers and customers using the Internet and extranets	Fast, convenient services lock in customers and suppliers

Fig. 3.10.1: Examples of the business value of e-Business Applications of Telecommunications Networks

3.10.1 Networks and the Internet

A computer network is two or more computers linked together to share information and/or resources. There are several types of computers networks, but the types most important to the topic of accounting information systems are local area network (LAN), the internet, extranet, and intranet.

The Internet is the global computer network, or “information super-high way”. The Internet developed from a variety of university and government-sponsored computer networks that have evolved and are not made up of millions and millions of computers and sub networks throughout the world. The Internet is the network that serves as the backbone for the World Wide Web (WWW).

An intranet is a company's private network accessible only to the employees of that company. The intranet uses the common standards and protocols of the Internet. The purpose of an intranet is to distribute data or information to employees, to make shared data or files available, and to manage projects within the company.

An extranet is similar to an intranet except that it offers access to selected outsiders, such as buyers to an intranet except, and wholesalers in the supply chain. Extranets allow business partners to exchange information. These business partners may be given limited access to company serves and access only to the data necessary to conduct supply chain exchanges with the company.

3.10.2 Internet Applications

Internet can be used as a very effective media for various applications such as:

- ◆ E-mail, browsing the sites on the World Wide Web, and participating in special interest newsgroups are the most popular Internet applications.
- ◆ Electronic commerce transactions between businesses and their suppliers and customers can also performed with online web applications.
- ◆ The Internet provides electronic discussion forums and bulletin board systems formed and managed by thousands of special-interest newsgroups.
- ◆ Other applications include downloading software and information files and accessing databases provided by thousands of businesses, governments, and other organizations.
- ◆ The Internet allows holding real-time conversations with other Internet users.
- ◆ The Internet allows gathering information through online services using web browsers and search engines.
- ◆ Internet browser software enables millions of users to surf the World Wide Web by clicking their way to the multimedia information resources stored on the hyperlinked pages of businesses, government, and other websites.

3.10.3 Business Use of the Internet

Business uses of the Internet include:

- ◆ Strategic business alliances
- ◆ Providing customer and vendor support
- ◆ Collaboration among business partners
- ◆ Buying and selling products and services
- ◆ Marketing, sales, and customer service applications
- ◆ Growth of cross-functional business applications
- ◆ Emergence of applications in engineering, manufacturing, human resources and accounting.
- ◆ Enterprise communications and collaboration
- ◆ Attracting new customers with innovative marketing and products.
- ◆ Retaining present customers with improved customer service and support.
- ◆ Developing new web-based markets and distribution channels for existing products.
- ◆ Developing new information-based products accessible on the Web.

- ◆ Generating revenue through electronic commerce applications is a growing source of business value.
- ◆ Electronic commerce

3.10.4 Intranet

An intranet is a network inside an organization that uses Internet technologies such as web browsers and servers, TCP/IP network protocols, HTML hypermedia document publishing and databases, and so on, to provide an Internet-like environment within the enterprise for information sharing, communications, collaboration, and the support of business processes.

An Intranet is protected by security measures such as passwords, encryption, and firewalls, and thus can be accessed by authorized users through the Internet. A Company's Intranet can also be accessed through the Intranets of customers, suppliers, and other business partners via extranet links. Refer to the Fig. 3.10.2.

- ◆ **The Business Value of Intranets:** Intranet applications support communications and collaboration, business operations and management, web publishing, and Intranet management. These applications can be integrated with existing IS resources and Applications, and extended to customers, suppliers, and business partners.
- ◆ **Communications and Collaboration:** Intranets can significantly improve communications and collaboration within an enterprise. Examples include:
 - Using an Intranet browser and workstation to send and receive e-mail, voicemail, paging, and fax to communicate with others within the organization, and externally through the Internet and extranets.
 - Using Intranet groupware features to improve team and project collaboration with services such as discussion groups, chat rooms, and audio and videoconferencing.
- ◆ **Web Publishing:** The advantages of developing and publishing hyperlinked multimedia documents to hypermedia databases accessible on World Wide Web servers has moved to corporate intranets. The comparative ease, attractiveness, and lower cost of publishing and accessing multimedia business information internally via intranet web sites have been one of the primary reasons for the explosive growth of the use of intranets in business. Examples include:
- ◆ **Business Operations and Management:** Intranets are being used as the platform for developing and deploying critical business applications to support business operations and managerial decision making across the internetworked enterprise. Examples include:
 - Many companies are developing customer applications like order processing, inventory control, sales management, and executive information systems that can be implemented on intranets, extranets, and the Internet.

- Many applications are designed to interface with, and access, existing company databases and legacy systems. The software for such business uses, is then installed on Intranet web servers.
- Employees within a company, or external business partners, can access and run applications using web browsers from anywhere on the network whenever needed.
- Company newsletters, technical drawings, and product catalogs can be published in a variety of ways including hypermedia and web pages, e-mail, net broadcasting, and as part of in-house business applications.
- Intranet software browsers, servers, and search engines can help to easily navigate and locate the business information.

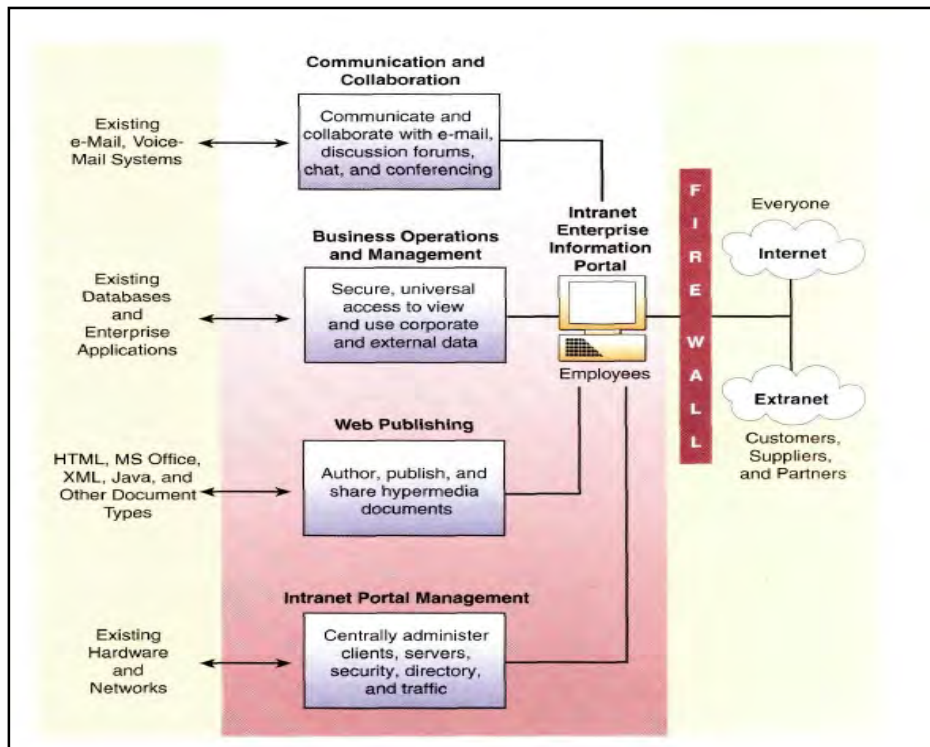


Fig. 3.10.2: Role of Intranet in any organization

3.10.5 Extranets

Extranets are network links that use Internet technologies to interconnect the intranet of a business with the intranets of its customers, suppliers, or other business partners. Companies can use extranets to perform following functions:

- ◆ Establish direct private network links between themselves, or create private secure Internet links between them called virtual private networks.

- ◆ Use the unsecured Internet as the extranet link between its intranet and consumers and others, but rely on encryption of sensitive data and its own firewall systems to provide adequate security.

Business Value of Extranets

The business value of extranets is derived from several factors:

- ◆ The web browser technology of extranets makes customer and supplier access of intranet resources a lot easier and faster than previous business methods.
- ◆ Extranets enable a company to offer new kinds of interactive Web-enabled services to their business partners. Thus, extranets are another way that a business can build and strengthen strategic relationships with its customers and suppliers.
- ◆ Extranets enable and improve collaboration by a business with its customers and other business partners.
- ◆ Extranets facilitate an online, interactive product development, marketing, and customer-focused process that can bring better designed products to market faster.

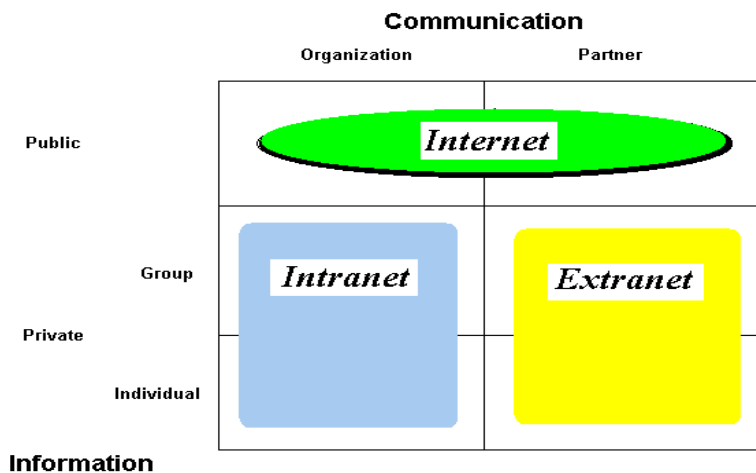


Fig. 3.10.3: Relationship between the Internet, Intranet and Extranet

An organization uses the Internet to communicate public information about itself to members of the organization and to others outside the organization. Referring to the Fig. 3.10.3, Intranets and Extranets are private versions of the Internet. An organization uses an intranet to share information between the members of the organization. Organizations use extranets to exchange information with and provide services to their business partners (customers, suppliers, etc.)

An extranet requires security and privacy that require firewall server management, the issuance and use of digital certificates or similar means of user authentication, encryption of messages, and the use of Virtual Private Networks (VPN) that tunnel through the public network.

Companies can use an extranet to do the following tasks:

- ◆ Share product catalogs exclusively with wholesalers or those "in the trade",
- ◆ Collaborate with other companies on joint development efforts,
- ◆ Jointly develop and use training programs with other companies,
- ◆ Provide or access services provided by one company to a group of other companies, and
- ◆ Share news of common interest exclusively with partner companies.

With competitive advantage as the ultimate prize, two fundamental drivers are propelling large enterprises to the extranet: market consolidation and service externalization. Markets are consolidating as the pace of merger, investment, and acquisition intensifies. Yet within companies, core services are also increasingly being externalized, delivered by a network of external parties that includes outsourcers, demand and supply chain partners, consultants, and contractors. This dynamic environment presents clear business needs, which can be summarized as the Five Rules of the Extranet which are as follows:

- ◆ **Be as flexible as the business:** An extranet must be driven by the demands of the market, not the limitations of technology. It must be extremely flexible and allow companies to immediately deploy extranet services that best fit the business need, be it intimate supply chain partners using a wide range of applications or mass e-commerce extranets driven by Web-based applications.
- ◆ **Deploy in "Internet time":** To deploy an extranet, companies shouldn't have to roll out a new infrastructure or go through a major re-architecting of their applications. To remain market-driven, enterprises must be able to deploy their extranet quickly, and leverage their existing infrastructure to do so.
- ◆ **Protect the interests of the data owner:** Extranet services need to be deployed in a fast and flexible way, but with the complete assurance that only the correct users can access the right services. An extranet must ensure that what's supposed to be private stays private.
- ◆ **Serve the partner as a customer:** An extranet presents a very important and delicate balance: providing customer service to key partners (who might also be customers) in a competitive environment with mission-critical resources at risk. The final solution must be an extranet without compromise. Partners should never be required to change their security policies, networks, applications, and firewalls for the "good" of the extranet community.
- ◆ **Drive information to the decision-maker:** An extranet must provide a central means to measure progress, performance, and popularity. Business units deploying applications need to understand which extranet content and applications are most successful.

3.11 Electronic Commerce

Electronic Commerce (e-Commerce) and its related technologies are unquestionably the current leading-edge business and finance delivery systems for the 21st Century. The explosion in the application of technologies and the delivery of these technologies into the hands of consumers has made the vision, the dream, the fantasy, of conducting business electronically, anywhere in the global community, a reality. Electronic Commerce (EC) is no longer just a concept; it is a market force to be reckoned with. As more and more organizations launch Internet/World Wide Web (WWW) home pages and intranets to disseminate company/product information, and expand their customer base, countless yet unnamed companies are just beginning to investigate this alternative. These companies are realizing that business via the Internet is inevitable that they will not be able to ignore. The lure of reaching additional customers, expanding market shares, providing value-added services, advancing technological presence, and increasing corporate profits is just too valuable to disregard, and will eventually attract companies to electronic commerce like moths to a flame.

Electronic commerce is the process of doing business electronically. It refers to the use of technology to enhance the processing of commercial transactions between a company, its customers and its business partners. It involves the automation of a variety of business-to-business and business-to-consumer transactions through reliable and secure connections.

E-Commerce is a sophisticated combination of technologies and consumer-based services integrated to form a new paradigm in business transaction processing. The future of e-Commerce is bright and viable—the application, however, has not yet reached full integration into the business mainstream. Several significant hurdles remain, which must be cleared before electronic commerce will become a mainstay business strategy.

3.11.1 Benefits of e-Commerce Application and Implementation

E-Commerce presents immense benefits to individual organizations, consumers, and society as a whole.

- ◆ Reduction in costs to buyers from increased competition in procurement as more suppliers are able to compete in an electronically open marketplace.
- ◆ Reduction in errors, time, and overhead costs in information processing by eliminating requirements for re-entering data.
- ◆ Reduction in costs to suppliers by electronically accessing on-line databases of bid opportunities, on-line abilities to submit bids, and on-line review of rewards.
- ◆ Reduction in time to complete business transactions, particularly from delivery to payment.
- ◆ Creation of new markets through the ability to easily and cheaply reach potential customers.

- ◆ Easier entry into new markets, especially geographically remote markets, for enterprises regardless of size and location.
- ◆ Better quality of goods as specifications are standardized and competition is increased and improved variety of goods through expanded markets and the ability to produce customized goods.
- ◆ Faster time to market as business processes are linked, thus enabling seamless processing and eliminating time delays.
- ◆ Optimization of resource selection as businesses form cooperative teams to increase the chances of economic successes, and to provide the customer products and capabilities more exactly meeting the requirements.
- ◆ Reduction in inventories and reduction of risk of obsolete inventories as the demand for goods and services is electronically linked through just-in-time inventory and integrated manufacturing techniques.
- ◆ Reduction in overhead costs through uniformity, automation, and large-scale integration of management processes.
- ◆ Reduction in use of ecologically damaging materials through electronic coordination of activities and the movement of information rather than physical objects).
- ◆ Reduction in advertising costs.

Clearly, the benefits of corporate-wide implementation of e-Commerce are many, and this list is by no means complete. With the benefits, however, also come the risks. An organization should be cautious not to leap blindly into e-Commerce, but rather first develop an e-Commerce strategy, and then organize a corporate-wide team to implement that strategy.

3.11.2 Risks involved in e-Commerce

The risks associated with e-Commerce are multi-faceted. Given below is a sample listing of risks of e-Commerce:

- ◆ **Problem of anonymity:** There is need to identify and authenticate users in the virtual global market where anyone can sell to or buy from anyone, anything from anywhere.
- ◆ **Repudiation of contract:** There is possibility that the electronic transaction in the form of contract, sale order or purchase by the trading partner or customer may be denied.
- ◆ **Lack of authenticity of transactions:** The electronic documents that are produced in the course of an e-Commerce transaction may not be authentic and reliable.
- ◆ **Data Loss or theft or duplication:** The data transmitted over the Internet may be lost, duplicated, tampered with or replayed.
- ◆ **Attack from hackers:** Web servers used for e-Commerce may be vulnerable to hackers.

- ◆ **Denial of Service:** Service to customers may be denied due to non-availability of system as it may be affected by viruses, e-mail bombs and floods.
- ◆ **Non-recognition of electronic transactions:** e-Commerce transactions, as electronic records and digital signatures may not be recognized as evidence in courts of law.
- ◆ **Lack of audit trails:** Audit trails in e-Commerce system may be lacking and the logs may be incomplete, too voluminous or easily tampered with
- ◆ **Problem of piracy:** Intellectual property may not be adequately protected when such property is transacted through e-Commerce

3.11.3 Types of e-Commerce

There are four general classes of e-Commerce applications:

- (a) Business-to-Business (B2B) e-Commerce
- (b) Business-to-Consumer (B2C) e-Commerce
- (c) Consumer-to-Business (C2B) e-Commerce
- (d) Consumer-to-Consumer (C2C) e-Commerce
- (e) Business-to-Government (B2G) e-Commerce
- (f) Business-to-Employee (B2E) e-Commerce

A. Business-to-Business (B2B) e-Commerce

B2B refers to the exchange of services, information and/or products from one business to another.

B2B electronic commerce typically takes the form of automated processes between trading partners and is performed in much higher volumes than Business-to-Consumer (B2C) applications. B2B can also encompass marketing activities between businesses, and not just the final transactions that result from marketing.

B. Business-to-Consumer (B2C) e-Commerce

It is defined as the exchange of services, information and/or products from a business to a consumer, as opposed to between one business and another. Typically, a B2C e-Commerce business has a virtual store front for consumers to purchase goods and services eliminating the need to physically view or pick up the merchandise.

The Business-to-Consumer (B2C) model can save time and money by doing business electronically but customers must be provided with safe and secure as well as easy-to-use and convenient options when it comes to paying for merchandise. This minimizes internal costs created by inefficient and ineffective supply chains and creates reduces end prices for the customers. This could be beneficial especially if we are in the business of commodity-like products where we must be innovative and accommodating to gain and retain customers.

Advantages of B2C E-Commerce include:

- (i) Shopping can be faster and more convenient.
- (ii) Offerings and prices can change instantaneously.
- (iii) Call centers can be integrated with the website.
- (iv) Broadband telecommunications will enhance the buying experience.

C. Consumer-to-Business (C2B) e-Commerce

In C2B e-Commerce model, consumers directly contact with business vendors by posting their project work online so that the needy companies review it and contact the consumer directly with bid. The consumer reviews all the bids and selects the company for further processing. Some examples are guru.com, rentacoder.com, getacoder.com, freelancer.com.

D. Consumer-to-Consumer (C2C) e-Commerce

C2C e-Commerce is an Internet-facilitated form of commerce that has existed for the span of history in the form of barter, flea markets, swap meets, yard sales and the like. C2C e-Commerce sites provide a virtual environment in which consumers can sell to one another through a third-party intermediary.

E. Business-to-Government (B2G) e-Commerce

B2G e-Commerce, also known as e-Government, refers to the use of information and communication technologies to build and strengthen relationships between government and employees, citizens, businesses, non-profit organizations, and other government agencies.

F. Business-to-Employee (B2E) e-Commerce

B2E e-Commerce, from an intra-organizational perspective, has provided the means for a business to offer online products and services to its employees.

3.11.4 Key aspects to be considered in implementing e-Commerce

Successful implementation of e-Commerce requires involvement of key stakeholders and should ideally include representatives from: accounting/ finance, internal audit, IT security, telecommunications, end users, system analysts, and legal. Further, key trading partners, external auditors, and representatives from other institutions such as banks, trading houses, brokers, and other third-party services should also be involved to obtain valuable insight into the design and deployment of the e-Commerce solution. Other key aspects to be considered are:

- ◆ Implementing appropriate policies, standards and guidelines
- ◆ Performing cost benefit analysis and risk assessment to ensure value delivery
- ◆ Implementing the right level of security across all layers and processes

- ◆ Establishing and implementing the right level of baseline (best practice) controls
- ◆ Integration of e-Commerce with the business process and the physical delivery channels
- ◆ Providing adequate user training
- ◆ Performing post implementation review to ensure controls are working as envisaged.

3.12 Mobile Commerce

Mobile Commerce or m-Commerce, is about the explosion of applications and services that are becoming accessible from Internet-enabled mobile devices. It involves new technologies, services and business models. It is quite different from traditional e-Commerce. Mobile phones or PDAs impose very different constraints than desktop computers. But they also open the door to a slew of new applications and services.

M-commerce (mobile commerce) is the buying and selling of goods and services through wireless handheld devices such as cellular telephone and personal digital assistants (PDAs). Known as next-generation e-commerce, m-commerce enables users to access the Internet without needing to find a place to plug in. The emerging technology behind m-commerce, which is based on the Wireless Application Protocol (WAP), has made strides in countries, where mobile devices equipped with Web-ready micro-browsers are much more common.

As content delivery over wireless devices becomes faster, more secure, and scalable, there is wide speculation that m-commerce will surpass wireline e-commerce as the method of choice for digital commerce transactions. The industries affected by m-commerce include:

- ◆ Financial services, which includes mobile banking (when customers use their handheld devices to access their accounts and pay their bills) as well as brokerage services, in which stock quotes can be displayed and trading conducted from the same handheld device.
- ◆ Telecommunications, in which service changes, bill payment and account reviews can all be conducted from the same handheld device.
- ◆ Service/retail, as consumers are given the ability to place and pay for orders on-the-fly.
- ◆ Information services, which include the delivery of financial news, sports figures and traffic updates to a single mobile device.

3.13 Electronic Fund Transfer

Electronic Funds Transfer (EFT) represents the way the business can receive direct deposit of all payments from the financial institution to the company bank account. Once the user signs up, money comes to him directly and sooner than ever before. EFT is Fast, Safe, and means that the money will be confirmed in user's bank account quicker than if he had to wait for the mail, deposit the cheque, and wait for the funds to become available.

The payment mechanism moves money between accounts in a fast, paperless way. These are some examples of EFT systems in operation:

- ◆ **Automated Teller Machines (ATMs):** Consumers can do their banking without the assistance of a teller, or to make deposits, pay bills, or transfer funds from one account to another electronically. These machines are used with a debit or EFT card and a code, which is often called a personal identification number or “PIN.”
- ◆ **Point-of-Sale (PoS) Transactions:** Some debit or EFT cards (sometimes referred to as check cards) can be used when shopping to allow the transfer of funds from the consumer's account to the merchant's. To pay for a purchase, the consumer presents an EFT card instead of a check or cash. Money is taken out of the consumer's account and put into the merchant's account electronically.
- ◆ **Preauthorized Transfers:** This is a method of automatically depositing to or withdrawing funds from an individual's account, when the account holder authorizes the bank or a third party (such as an employer) to do so. For example, consumers can authorize direct electronic deposit of wages, social security, or dividend payments to their accounts. Or they can authorize financial institutions to make regular, ongoing payments of insurance, mortgage, utility, or other bills.
- ◆ **Telephone Transfers:** Consumers can transfer funds from one account to another through telephone instructions rather than traditional written authorization or instrument. The accounts being debited can be checking or savings, for example—or can order payment of specific bills by phone.

3.14 Summary

Before wires and virtual networks transmitted communications, there were smoke signals, drums and carrier pigeons. Fortunately, technology has come a long way since then to the point where it's impossible to overemphasize the significance of telecommunications technology to any business, especially as it relates to growing the capacity of small businesses. From telephones, facsimile, television, Internet and the vast array of private networks, telecommunications technology has become firm's central nervous system. Without it, a small business couldn't compete or survive in the nation's information service-dependent economy, making it one of the most important investments we will make as we build our business.

Telecommunication is an important tool for businesses. It enables companies to communicate effectively with customers and deliver high standards of customer service. Telecommunication is also a key element in teamwork, allowing employees to collaborate easily from wherever they are located. Mobile telecommunication gives companies the opportunity to introduce more flexible working by allowing employees to work efficiently from home. The introduction of Internet gives employees new levels of productivity and capability on the move.