INTRODUCTION TO E-BUSINESS

Dr P.V. Praveen Sundar
Assistant Professor,
Department of Computer Science
Adhiparasakthi College of Arts & Science,
Kalavai.

03-08-2020

III BBA

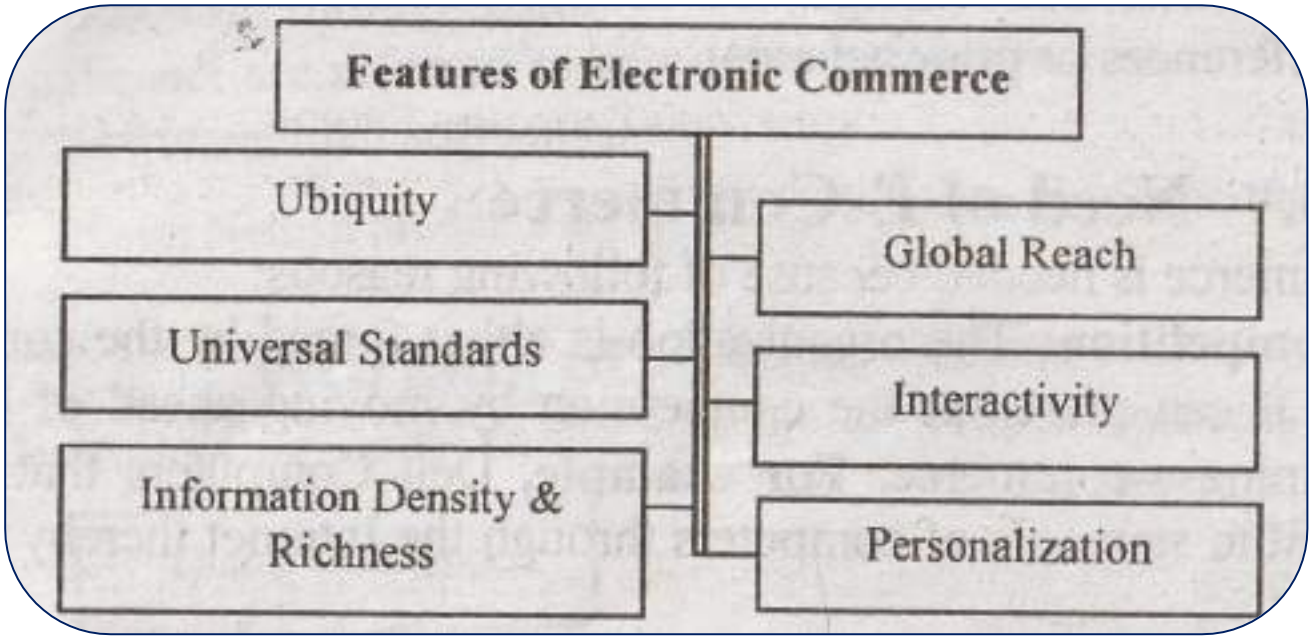
Introduction

- **E-commerce, also known as Electronic commerce or internet commerce refers to the buying and selling of goods or services using the internet, and the transfer of money and data to execute these transactions.**
- Some examples of real-world application of e-commerce are online banking, online shopping, online ticket booking, etc.
- The basic requirement of e-commerce is a website. The marketing, advertising, selling, and conducting transactions are done with the help of the internet. Any monetary transaction, which is done with the help of electronic media in e-commerce.

- According to Kalakota and Whinston, "Electronic Commerce can be defined from following four perspectives:
  - **Communications Perspective:** Electronic commerce is the delivery of information, products/services, or payments via telephone lines, computer networks, or any other means.
  - **Business Process Perspective:** Electronic commerce is the application of technology toward the automation of business transactions and workflows.
  - **Service Perspective**: Electronic commerce is a tool that addresses the desire of firms, consumers, and management to cut service costs while improving the quality of goods and increasing the speed of service delivery.
  - **Online Perspective:** Electronic commerce provides the capability of buying and selling products and information on the Internet and other online services."

- Electronic Commerce can also define from some other perspectives:
  - **Commercial (Trading):** From a commercial perspective, EC provides the capability of buying and selling products, services, and information over the Internet and via other online services.
  - **Learning:** From a learning perspective, EC is an enabler of online training and education in schools, s universities, and other organizations, including businesses.
  - **Collaborative:** From a collaborative perspective, EC is the framework for inter- and intra-organizational collaboration.
  - **Community:** From a community perspective, EC provides a gathering place for community members to learn, transact, and collaborate.

Features of Electronic Commerce



- **Ubiquity:** E-commerce is ubiquitous, meaning that it is available just about everywhere at all times. It liberates the market from being restricted to a physical space and makes it possible to shop from your desktop. The result is called a market space.
- From a consumer point of view, ubiquity reduces transaction costs - the cost of participating in a market. To transact, it is no longer necessary that you spend time and money traveling to a market. At a broader level, the ubiquity of e-commerce lowers the cognitive energy required to complete a task.

- **Global Reach:** E-commerce technology permits commercial transactions to cross-cultural and national boundaries far more conveniently and effectively as compared to traditional commerce. As a result, the potential market size for e-commerce merchants is roughly equal to the size of the world's online population.
- **Universal Standards:** One strikingly unusual feature of e-commerce technologies is that the technical standards of the Internet and therefore the technical standards for conducting e-commerce are universal standards i.e. they are shared by all the nations around the world.

- **Interactivity:** Unlike any of the commercial technologies of the twentieth century, with the possible exception of the telephone, e-commerce technologies are interactive, meaning they allow for two-way communication between merchants and consumers.
- **Information Density and Richness:** The Internet vastly increases information density. It is the total amount and quality of information available to all market participants, consumers, and merchants. E-commerce technologies reduce information collection, storage, communication, and processing costs. At the same time, these technologies increase greatly the accuracy and timeliness of information, making information more useful and important than ever.

- As a result, information becomes plentiful, cheaper, and of higher quality. Information richness refers to the complexity and content of a message.
- **Personalization:** E-commerce technologies permit personalization. Merchants can target their marketing messages to specific individuals by adjusting the message to a person's name, interests, and past purchases. The technology also permits customization. Merchants can change the product or service based on the user's preferences or prior behavior.

Need of E-Commerce

E-commerce is needed because of the following reasons:

- **Competition:** The organization is either forced by the competition or it can preempt the competition by moving ahead of others in joining e-commerce. For example, Dell Computers was the first to start the sale of computers through the Internet thereby reducing cost.
- It also provided a facility to the customers to assemble the computer choosing different hardware components such as Memory, Hard Disk, CD Drive, Monitor, etc. IBM, Compaq, and other manufacturers had to change their marketing strategy to find ways to reduce operational costs by adopting the e-business model of sale through the Internet.

- **Global Reach:** The Internet has crashed the geographical boundaries and the entire world has shrunk to a global village. This permits the customers to make purchases from any part of the world without actually visiting the place. This widens the reach of the companies to the entire globe. This further translates into 24 hours, 7 days a week, and 365 days in a year business for the company. For example, books can be purchased from amazon.com from any part of the world, AT&T allows the customer to receive the bill and authorize payment electronically from any part of the world.

- **Customer Service:** Personalized and Customized services through the Internet are one of the greatest advantages e-commerce offers. The customers can customize the product according to their own taste such as online newspapers. The customers can be updated on the status of orders placed by them when it goes through various stages of processing such as packing, shipping, etc. Pre-sale and Post-sale support is an important ingredient of the e-commerce package.

- **Value Addition:** A product has to go through various stages of value addition from manufacturers to the consumers and at each stage, the cost is added-up making the product expensive for the consumer. This business chain can be shortened through the adoption of e-commerce thereby making the product cheaply available to the consumers.
- **Nettish Products:** The products which are more suitable for purchase through the Internet as their delivery takes place through the net are referred to as Nettish products, e.g., e-mail, e-greetings, software, chat software, etc. Note: Nettish products are 'by the net, for the net and to the net'.

Working of E-Commerce

1.2.4. Working of E-Commerce

The following model shows how the e-commerce process works

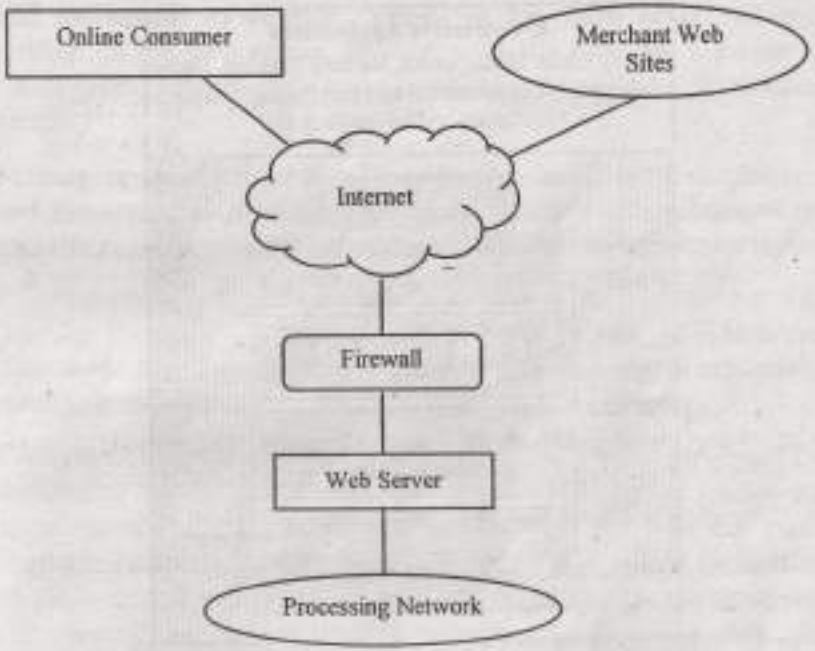


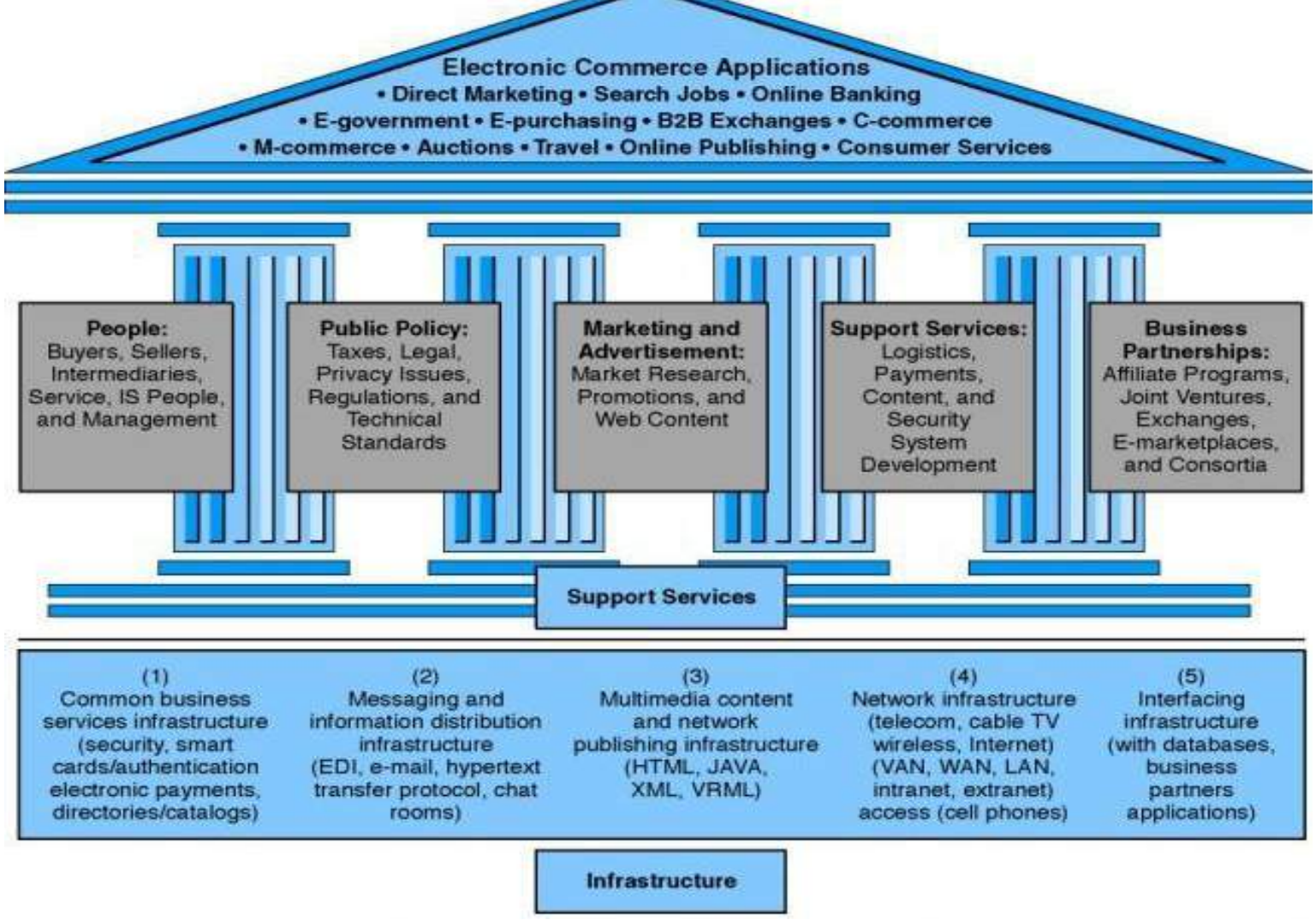
Figure 1.1

- The following model shows how the e-commerce process works
- Steps of E-Commerce Process
  - The consumer logs into the Internet using a web browser to connect to the company's website.
  - Firewall protects the company's computers from an unauthorized user who tries to access the site.
  - Consumer browses the products available on the site and selects items to purchase and place the items in the electronic equivalent of a shopping cart. After that consumer provides a bill-to and shipping address for purchase and delivery.

- Web server handles the customer request, calculates the cost of the order, takes care of taxes, and displays the details to the customer.
- Consumer provides the payment information, such as credit card no places the order.
- After validating the credit card no by the company, the consumer receives the details from the company about products and order confirmation. The commerce server site then forwards the order to a processing network for payment processing.

E-Commerce Framework

- The term E-Commerce framework is related to software frameworks for e-commerce applications. They offer an environment for building e-commerce applications quickly.
- E-Commerce frameworks are flexible enough to adapt them to your specific requirements. As result, they are suitable for building virtually all kinds of online shops and e-commerce related (web) applications.
- According to Choi, Stahl, & Whinston (1997) identified e-commerce framework infrastructure as
  - Common Business Services Infrastructure
  - The Messaging and Information distribution Infrastructure.
  - Content and Network Publishing Infrastructure.
  - The Information Superhighway Infrastructure(The Internet).
  - Interfacing infrastructure.


Electronic Commerce Applications
• Direct Marketing • Search Jobs • Online Banking
• E-government • E-purchasing • B2B Exchanges • C-commerce
• M-commerce • Auctions • Travel • Online Publishing • Consumer Services
People: Buyers, Sellers, Intermediaries, Service, IS People, and Management
Public Policy: Taxes, Legal, Privacy Issues, Regulations, and Technical Standards
Marketing and Advertisement: Market Research, Promotions, and Web Content
Support Services: Logistics, Payments, Content, and Security System Development
Business Partnerships: Affiliate Programs, Joint Ventures, Exchanges, E-marketplaces, and Consortia
Support Services
(1) Common business services infrastructure (security, smart cards/authentication electronic payments, directories/catalogs)
(2) Messaging and information distribution infrastructure (EDI, e-mail, hypertext transfer protocol, chat rooms)
(3) Multimedia content and network publishing infrastructure (HTML, JAVA, XML, VRML)
(4) Network infrastructure (telecom, cable TV wireless, Internet) (VAN, WAN, LAN, intranet, extranet) access (cell phones)
(5) Interfacing infrastructure (with databases, business partners applications)
Infrastructure

Elements of E-Commerce Framework

- **Information Super Highway (I-Way):** The information superhighway is the transportation foundation that enables the transmission of content.
- The Information Superhighway facilitates the convergence of content and distribution channels, which brings corporations together, indicating huge commercial and cultural developments from the Internet.
- Telephone Wires, Cables, Wireless, Internet, Intranet, Extranet, Satellites, VAN, MAN, LAN, and Cell Phones.
- Any successful e-commerce application will require the I-Way infrastructure in the same way that regular commerce needs the interstate highway network to carry goods from point to point A myriad of computers, communications networks, and communication software form the emerging Information Superhighway (I-Way).

- **Multimedia Content and Network Publishing:** The electronic system through which content is transmitted is an analogous to the non electronic world in which different type of products are stored in distribution centers before they are loaded onto various vehicles for transport. currently the most prevalent architecture that enables network publishing is the WWW. The web allows small businesses and individuals to develop content in the form of HTML and publish on the web server. In short web site provides a means to create product information and a means to publish it in a distribution center.
- Standards for multimedia file types and data communication circuits over which the information travels respectively. Digital Video/Audio, Electronic Books, World Wide Web, Digital Games, HTML, Java, XML,VRML.

- **Messaging and Information Distribution:** Information distribution and messaging technologies provide a transparent mechanism for transferring information content over a network infrastructure layer. It is accomplished through software systems that implement File Transfer Protocol (FTP), Hypertext Transfer Protocol, and Simple Message Transfer Protocol (SMTP) for exchanging multimedia contents consisting of text, graphics, video, audio data.
- **Interfacing Infrastructure:-** Database, Business partner Applications.

- **Common Business Services:** Common business services, for facilitating the buying and selling process. Electronic commerce applications require that the information sources to be made available online to geographically dispersed clients and facilitation of the transactional environment. Addressed by deploying strong site security measures that constantly monitor the site for authenticated and authorized activities, virus detection and elimination systems, and intrusion detection systems and firewalls.
- Common Business Services includes Security, Authentication, Electronic payment, Directories and Catalogs.

- Securing the transaction, carried out over the network, requires addressing several security and confidentiality related issues. The confidentiality or privacy of the transaction data can be addressed by using various encryption techniques. The shared key as well as the public/ private key pair based encryption techniques can be used for the purpose.
- Electronic payment is fundamental to the acceptance of electronic commerce as a viable alternative to traditional commerce. mechanism that facilitates an online financial exchange between concerned parties. Several scalable and flexible electronic payment mechanisms- cash cheques and credit cards have emerged, essentially imitating traditional payment mechanisms.

- The second part is **"Supporting Services"** to support e-commerce. According to Choi, Stahl, & Whinston (1997), support service involving people, public policy or government regulation on e-commerce-based business, marketing and advertisement on the Internet, support service, and business partnership.
- In general it can be concluded that the support service within its framework Choi, Stahl, & Whinston (1997) defines that a site or e-commerce portal will engage the services of businesses and third parties or business partnership, depending on the type of business model used.

- The third part of the framework is the **Application of e-commerce** itself. In this case, the application of e-commerce is highly dependent on the business model that is run by a service provider of e-commerce. For example, companies that provide or carry out online job applications (eg www.jobsdb.com) will have a different business model of the Bank is running the application for the purposes of e-Banking.

Applications of E-Commerce

- Supply Chain Management
- Procurement & Purchasing
- Audio and Video on Demand
- Entertainment and Gaming
- E- Marketing
- E-Advertising
- E-Shopping
- Online Financial Transaction
- E-banking
- Mobile Commerce
- E-learning
- Online Training.

Advantages of E-Commerce

The advantages of e-commerce can be enumerated in following categories:

- 1) **Advantages to Customers**
  - **Reduced Prices:** Costs of products are reduced since stages along the value chain are decreased. For example, intermediaries can be eliminated by the company directly selling to the consumer instead of distributing through a retail store.
  - **Global Marketplace:** Consumers can shop anywhere in the world. Currently, according to the World Trade Organization (WTO) there are no custom duties put on products bought and traded globally electronically. This also provides wide selection of products and services to consumers.
  - **24-Hour Access:** Online businesses never sleep as opposed to brick and mortar businesses. E-commerce allows people to carry out businesses without the barriers of time or distance. One can log on to the Internet at any point of time, be it day or night and purchase or sell anything one desires at a single click of the mouse.

- **More Choices:** Provides consumers with more choices. For example, before making any purchase, customer can study about all the major brands and features of any item. It also provides consumers with less expensive products and services by allowing them to shop in many ,places and conduct quick comparisons.
- **Quicker Delivery:** Allows quick delivery of products and services (in some cases) especially with digitized products.
- **Information:** Consumers can receive relevant and detailed information in seconds, rather than in days or weeks. Comparison of products and prices can be made easier.

2) Advantages to Businesses

- **Increased Potential Market Share:** The Internet enables businesses to have access to international markets thereby increasing their market share. Companies can also achieve greater economies of scale.
- **Low-cost Advertising:** Advertising on the Internet costs less than advertising on print or television depending on the intricacies and extent of the advertisement. A company can still spend a lot on advertising on the Internet if the company hires an external party to create their advertisements but advertising on the Internet itself is less costly since there is less cost associated with it in terms of printing and limited television spots.
- **Low Barriers to Entries:** 'Anyone can start up a company on the Internet. Start-up costs are a lot lower for companies since there is less need for money for capital.
- **Global Reach:** Business organizations are able to send messages world-wide, explore new market and reach globally at lower cost. E-commerce helps to attract customers and business clients from anywhere in the world due to global reach.

- **Strategic Benefit:** The strategic benefit of making a business `e-commerce enabled' is that it helps reduce the delivery time, labor cost and the cost incurred in the following areas:
  - Document preparation
  - Error detection and correction
  - Reconciliation
  - Mail preparation
  - Telephone calling
  - Data entry
  - Overtime
  - Supervision expenses
  - Anytime business

Disadvantages

The disadvantages of e-commerce can be enumerated in following categories

- **Technical Limitations**
  - **Lack of Security:** There is a lack of system security, reliability, standards, and some communication protocols.
  - **Low Bandwidth:** There is insufficient telecommunication bandwidth.
  - **Needed More Applications Tools:** It is difficult to integrate the Internet and electronic commerce software with some existing applications and databases. Vendors may need special Web servers and other infrastructures, in addition to the network servers.
  - **Incompatibility:** Some electronic commerce software might not fit with some hardware, or may be incompatible with some operating systems or other components.

Non-Technical Limitations

- **Cost and Justification:** The cost of developing electronic commerce in-house can be very high, and mistakes due to lack of experience may result in delays. There are many opportunities for outsourcing, but where and how to do it is not a simple issue. Furthermore, to justify the system one must deal with some intangible benefits (such as improved customer services and the value of advertisement), which are difficult to quantify.
- **Security and Privacy:** These issues are especially important in the B2C area, especially security issues that are perceived to be more serious than they really are when appropriate encryption is used. Privacy measures are constantly improved. Yet, the customers perceive these issues as very important, and, the electronic commerce industry has a very long and difficult task of convincing customers that online transactions and privacy are, in fact, very secure.

- **Lack of Trust and User Resistance:** Customers do not trust an unknown faceless seller (sometimes they do not trust even known ones), paperless transactions, and electronic money. So switching from physical to virtual stores may be difficult.
- **Other Limiting Factors:** Lack of touch and feel online. Some customers like to touch items such as clothes and like to know exactly what they are buying.
- **Customers Relations Problems:** Not many businesses realize that even an e-business cannot survive over the long term without loyal customers.
- **Corporate Vulnerability:** The availability of product information, database catalogs and other about a business through its web site makes it vulnerable to access by the competition. The idea of extracting business intelligence from the competitor's web pages is called Web farming.

- Legal Issues: Legal problems encountered in the e-commerce environment include:
  - Software and Copyright Infringements
  - Credit Card Fraud and Stolen Identities
  - Business Fraud

E-Business

- **Electronic business (e-business) refers to the use of the Internet, intranets, or some combination thereof to conduct business. It includes not only buying and selling of goods and services, but also, servicing customers, collaborating with business partners and suppliers, conducting electronic transactions within an organization.**
- E-Business is comprised of e-marketing, e-commerce and e-operations:
  - E-Business: The application of internet technology to streamline all aspects of business processes.
  - E-Marketing: Building an online presence, showcasing a company providing detailed information.
  - E-Commerce: Selling products and services online, conducting payment, handling transaction details and supporting automated customer inquires.
  - E-Operations: Streamlining of business process and steps to enhance business efficiencies between functional departments of a company.
  - E-Business= E-Marketing + E-Commerce +E-Operations.

- E-business includes a much wider range of business processes, such as Supply Chain Management (SCM), Electronic order processing, and Customer Relationship Management (CRM).
- eBusiness or Electronic Business is the administration of conducting business via the Internet. This would include the buying and selling of goods and services, along with providing technical or customer support through the Internet.
- Electronic business can take place between a very large number of market participants; it can be between business and consumer, private individuals, public administrations or any other organizations such as NGOs.
- These various market participants can be divided into three main groups:
  1) Business (B)
  2) Consumer (C)
  3) Administration (A)
- All of them can be either buyer or service provider within the market.

History of E-Business

- Michael Aldrich is considered as the developer of the predecessor to online shopping. In 1979, the entrepreneur connected a television set to a transaction processing computer with a telephone line and called it "teleshopping".
- One the earliest consumer shopping experiences was Book Stacks Unlimited, an online bookstore created by Charles M. Stack in 1992.
- In 1994, IBM, with its agency Ogilvy & Mather, began to use its foundation in IT solutions and expertise to market itself as a leader of conducting business on the Internet through the term "e-business."
- Amazon was founded by Jeff Bezos in 1995, started as an online bookstore and grew to become nowadays the largest online retailer worldwide, selling food, toys, electronics, apparel and more.
- India's e-commerce market was worth about $3.9 billion in 2009.


Estimated U.S. Retail Ecommerce Sales as a Percent of Total Retail Sales (1999 - 2007)
4
3.5
3
2.5
2
1.5
1
0.5
0
1999
2000
2001
2002
2003
2004
2005
2006
2007

- The Indian e-commerce market is estimated at ₹28,500 Crore ($6.3 billion) for the year 2011.
- The market went up to $12.6 billion in 2013. In 2013, the e-retail segment was worth US$2.3 billion. About 79% of India's e-commerce market was travel related in 2013.
- According to Google India, there were 35 million online shoppers in India in 2014.
- Overall e-commerce market had reached ₹1,07,800 crores (US$24 billion) by the year 2015 with both online travel and e-tailing contributing equally.
- Another big segment in e-commerce is mobile/DTH recharge with nearly 1 million transactions daily by operator websites.
- The ecommerce market grew to $38.5 billion in 2018.

Traditional vs E-Business Applications

Basis	Traditional Business	E-Business
Formation	Difficult	Simple and Easy
Physical presence	Necessary	Not Required
Cost of Setting up	High cost	Low as no requirement of physical facilities.
Opportunity for inter touch	More	Less
Global Reach	Less	More as Cyberspace is without boundaries
Transaction risk	Less	High due to distance and anonymity of the parties

E-Commerce vs E-Business

Basis for Comparison	E-commerce	E-business
Meaning	Trading of merchandise, over the internet is known as E-commerce.	Running business using the internet is known as E-business.
What is it?	Subset	Superset
Is it limited to monetary transactions?	Yes	No
What they carry out?	Commercial transactions	Business transactions
Requires	Website	Website, CRM, ERP, etc.
Which network is used?	Internet	Internet, Intranet and Extranet.

Traditional Commerce vs E-Commerce

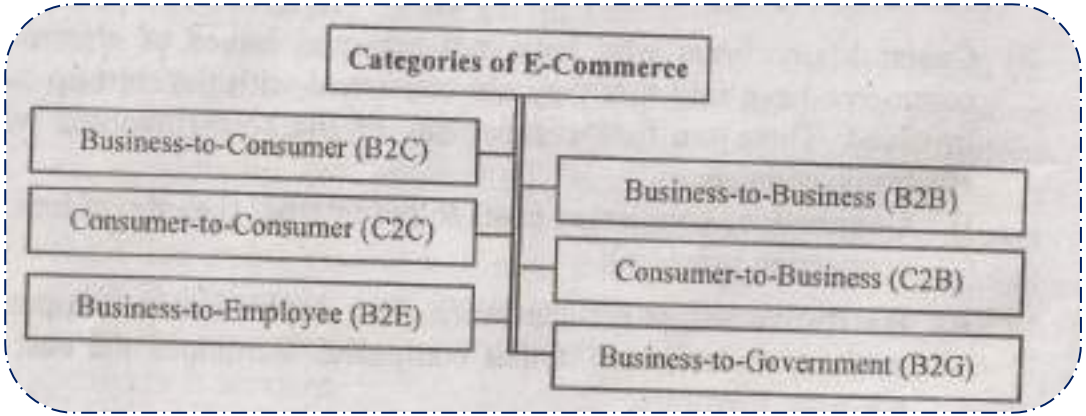
TRADITIONAL COMMERCE	E-COMMERCE
Traditional commerce refers to the commercial transactions or exchange of information, buying or selling product/services from person to person without use of internet.	E-commerce refers to the commercial transactions or exchange of information, buying or selling product/services electronically with the help of internet.
In traditional commerce it is difficult to establish and maintain standard practices.	In traditional commerce it is easy to establish and maintain standard practices.
In traditional commerce direct interaction through seller and buyer is present.	In traditional commerce indirect interaction through seller and buyer occurs using electronic medium and internet.
Traditional commerce is carried out by face to face, telephone lines or mail systems.	E-commerce is carried out by internet or other network communication technology.

TRADITIONAL COMMERCE	E-COMMERCE
In traditional commerce processing of transaction is manual.	In e-commerce processing of transaction is automatic.
For customer support, information exchange there is no such uniform platform.	For customer support, information exchange there is exists uniform platform.
In traditional commerce delivery of goods is instant.	In e-commerce delivery of goods takes time.
Its accessibility is for limited time in a day.	Its accessibility is 24×7×365 means round the clock.

TRADITIONAL COMMERCE	E-COMMERCE
Traditional commerce is done where digital network is not reachable.	E-commerce is used to save valuable time and money.
Traditional commerce is a older method of business style which comes under traditional business.	E-commerce is a newer concept of business style which comes under e-business.
Its resource focuses on supply side.	Its resource focuses on demand side.
In traditional commerce customers can inspect products physically before purchase.	In e-commerce customers can not inspect products physically before purchase.
Its business scope of business is a limited physical area.	Its business scope is worldwide as it is done through digital medium.

Categories of E-Commerce

- The several types of e-commerce models in use today are classified based on the nature of the interaction with players are:



Business-to-Consumer(B2C)

- In B2C, businesses sell directly a diverse group of products and services to customers. In these cases, e-commerce supplements the traditional commerce by offering products and services through electronic channels. Wal-Mart Stores and the Gap are examples of companies that are very active in B2C e-commerce. Some of the advantages of these e-commerce sites and companies include availability of physical space customers can physically visit the store, availability of returns (customers can return a purchased item to the physical store and availability of customer service in these physical stores.
- For example, the Amazon.com is B2C ecommerce site. This e-tailor acts predominantly as a goods marketer in e-space. Amazon.com also sells digital goods such as e-books and offers a platform for other retailers.

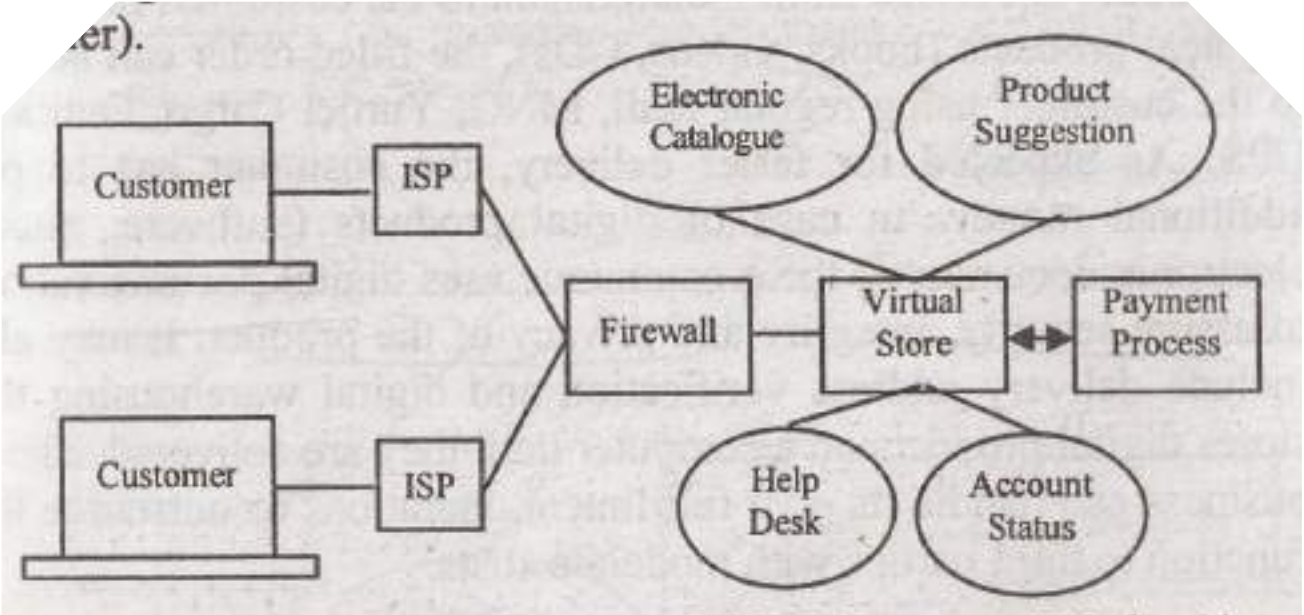


Figure 1.7: Business-to-Consumer (B2C) E-Commerce Relationship

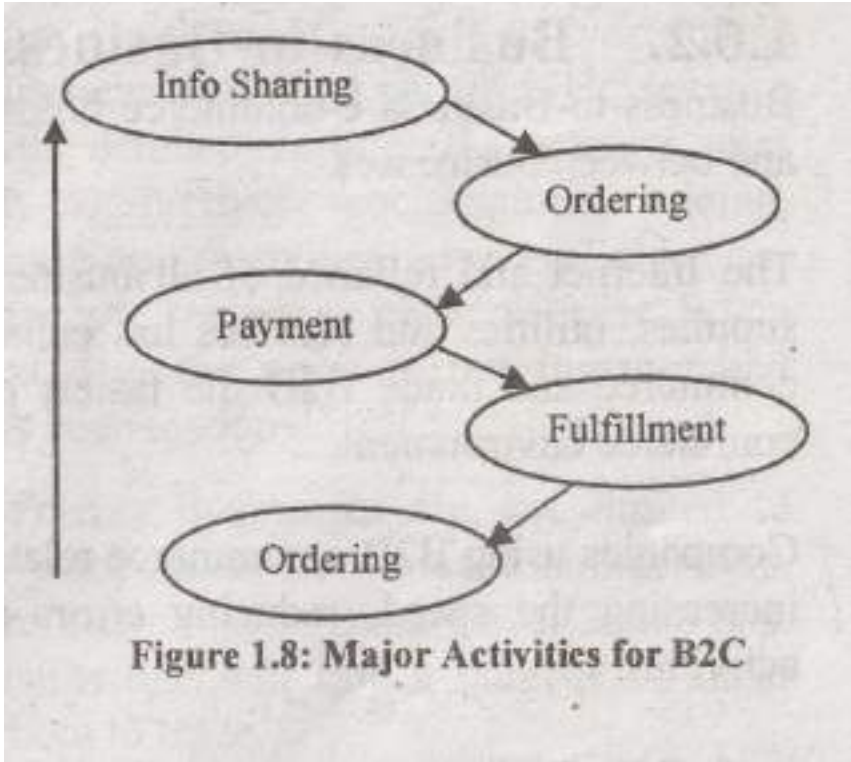


Figure 1.8: Major Activities for B2C

There are five major activities involved in conducting B2C e-commerce.

- **Information Sharing:** A B2C e-commerce may use some or all of the following applications and technologies toshare information with customers: online advertisements, e-mail, newsgroups/ discussion groups, company website, online catalogs, message board systems, -bulletin board systems, multiparty conferencing.
- **Ordering:** A customer may use electronic e-mai1 or forms available on the company's website to order a product from a B2C site. A mouse click sends the essential information relating to the requested piece(s) to the B2C site.
- **Payment:** Credit cards, electronic checks and digital cash are among the popular options that the customer has options for paying for the goods or services.

- **Fulfillment:** Fulfillment that is responsible for physically delivering the product or service from the merchant to the customer. In case of physical products (books, videos, CDs), the filled order can be sent to the customer using regular mail, MNG, Yurtic, Cargo, FedEx or UPS. As expected for faster delivery, the customer has to pay additional money. In case of digital products (software, music, electronic documents), the e-commerce uses digital documentations to assure security, integrity and privacy of the product. It-may also include delivery address verification and digital warehousing that stores digital products on a computer until they are delivered. The e-business can handle its own fulfillment operations or outsource this function to third parties with moderate costs.

- **Service and Support:** It is much cheaper to maintain current customers than to attract new customers. For this reason, e-commerce should do whatever that they can in order to provide timely, high-quality service and support to their customers. As e-commerce companies lack a traditional physical presence and need other ways to maintain current customers, service and support are even more important in e-commerce than traditional commerce.

Business 2 Business (B2B)

- Business-to-Business e-commerce holds electronic transactions among and between businesses.
- The Internet and reliance of all businesses upon other companies for supplies, utilities and services has enhanced the popularity of B2B e-commerce and made B2B the fastest growing segment within the e-commerce environment.
- Companies using B2B e-commerce relationship observe cost savings by increasing the speed, reducing errors and eliminating many manual activities.

- In a B2B environment, purchase orders, invoices, inventory status, shipping logistics and business contracts handled directly through the network result in increased speed, reduced errors and cost savings.
- B2B e-commerce reduces cycle time, inventory and prices and enables business partners to share relevant, accurate and timely information. The end result is improved supply-chain management among business partners.
- The figure 1.9 illustrates a generic B2B relationship.

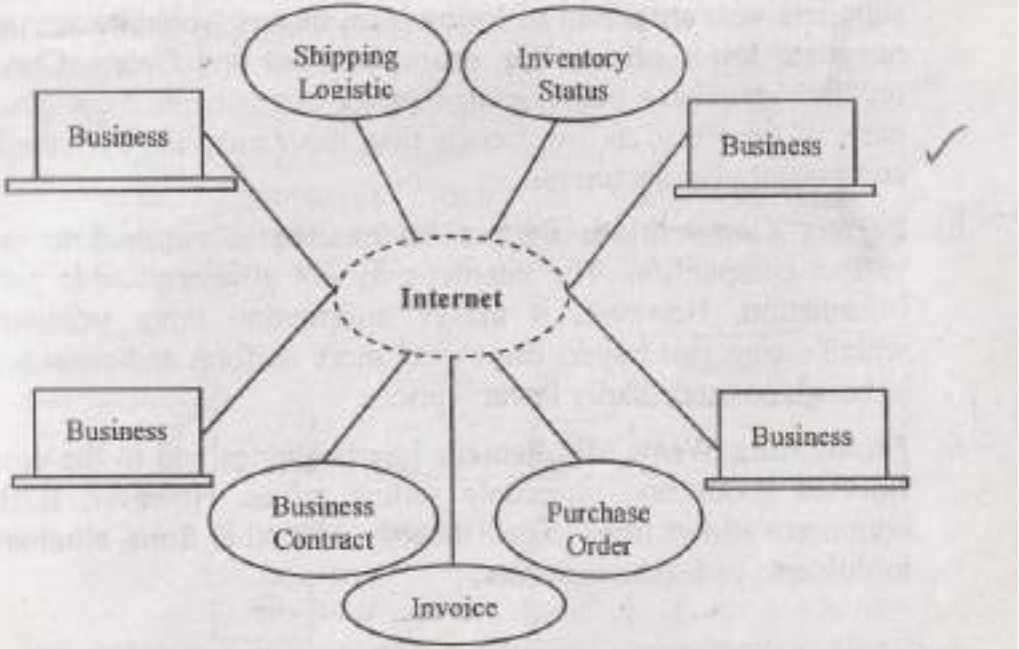


Figure 1.9: Business-to-Business (B2B) Relationship

Advantages of B2B E-Commerce

- **24/7/365:** Businesses are no longer bound by closing hours. The business is open 24 hours, 7 days a week, 365 days a year. Organizations in different time zones find it difficult to synchronize their business times with international trading partners. However, a comprehensive website with detailed information ensures that business information, such as product specifications, pricing, delivery charges and minimum quantities, is available for prospective and existing partners to see and to place an order. When the business opens the next day, the order is put together and dispatched after payment has been tendered.

- **Breaking Geographic Barriers:** Businesses are not limited to purchasing raw materials or components from local manufacturers. A Google search for 'sugar refineries' will generate over 20000 hits. By sifting through these results one will find a number of sugar refineries worldwide with whom to trade.
- **Online Tenders:** Indiamart.com is a tender portal where one can tender to sell products to states in India. One of the large manufacturers of sweets and chocolates put a tender online and, within days, was able to purchase sugar from Brazil at a fraction of the cost of local sugar.

- **Lower Costs:** With the ability to access foreign suppliers of raw materials and components, businesses can keep their costs low, because they have access to more suppliers. Furthermore, local suppliers who are afraid of losing local buyers would be willing to negotiate lower prices. For example, Ford and DaimlerChrysler regularly purchase manufactured motor components from obscure parts of the world at lower costs than those supplied by American component manufacturers.
- **Perfect Competition:** Perfect information is required to reach perfect competition. The internet may not always provide perfect information. However, it makes information more transparent, which means that buyers can expect more uniform and consistent —although not necessarily lower — prices.

- **Eliminating Weak Middlemen:** Intermediaries add to the cost of finished goods and ultimately selling prices. However, B2B e-commerce allows firms to deal directly with other firms, eliminating middlemen and reducing costs.

Consumer-to-Consumer (C2C)

- Using C2C e-commerce, consumers sell directly to other consumers using the Internet and web technologies.
- Individuals sell a wide variety of services/products on the Web or through auction sites such as eBay.com and gittigidiyor.com through classified ads or by advertising. Examples are OLX, Quickr etc.
- Figure 1.10 illustrates a general C2C e-commerce relationship. Consumers are also able to advertise their products and services in organizational intranets and sell them to other employees.

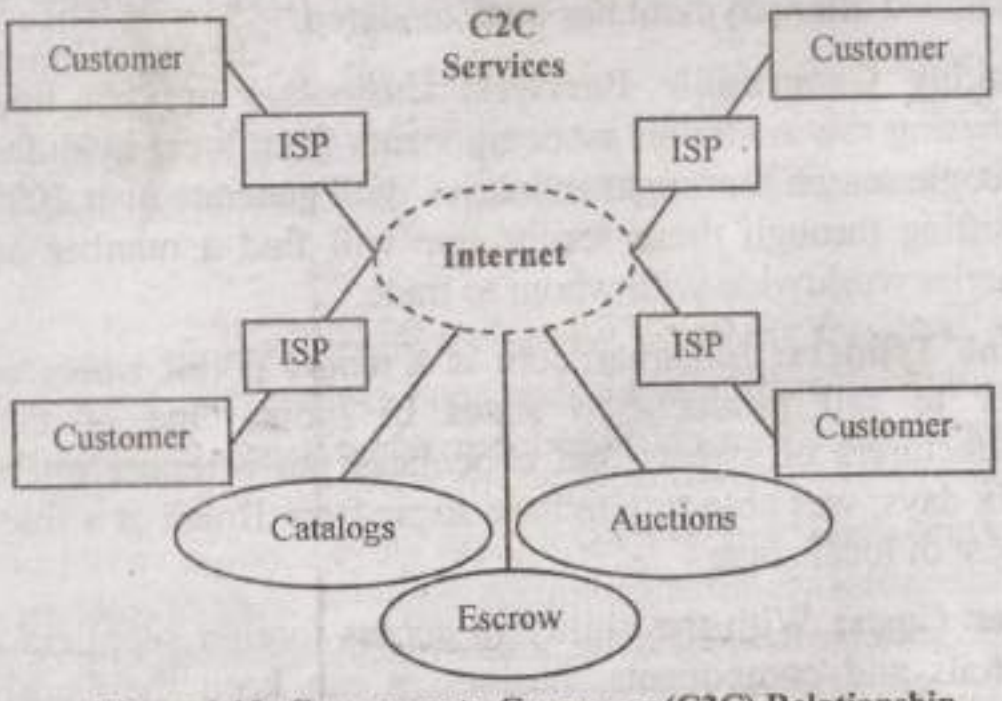


Figure 1.10: Consumer-to-Consumer (C2C) Relationship

Consumer-to-Business(C2B)

- Consumer-to-Business(C2B) e-commerce that involves individuals selling to businesses may include a service/product that a consumer is willing to sell, Individuals offer certain prices for specific products/service and the companies pay the consumers.
- Companies such as pazaryerim.com , mobshop.com, eBay, blogs or internet forums, Elance are examples of C2B.
- Figure 1.11 shows a C2B e-commerce relationship.

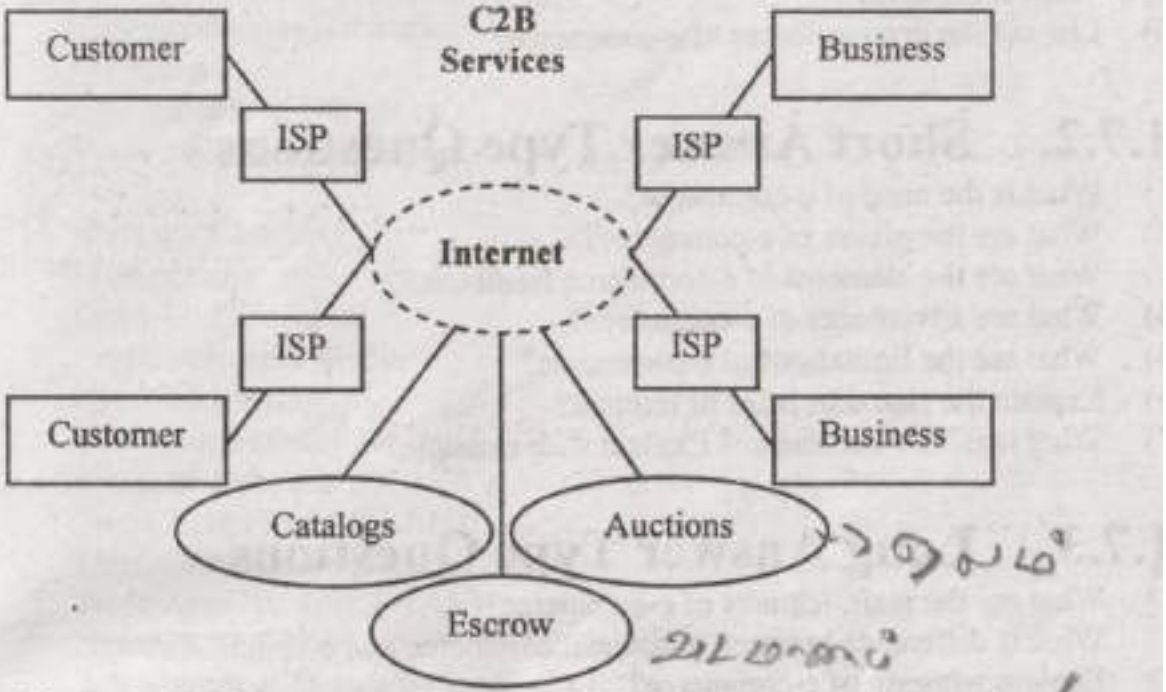


Figure 1.11: Consumer-to-Business (C2B) E-Business Relationship

Business-to-Employee (B2E)

- The transactions between the business and the employee is called business-to-employee services. Searching for a particular type of information from the vast information base of the company may be time consuming for an employee. To overcome this, B2E application provides employees a self-service capability. The intranet-based business-to-employee applications are sometimes used for implementing improved employee relationship management initiatives.

Business-to-Government (B2G)

- The transactions between the business and government over electronic network are termed as B2G. B2G e-commerce involves the use of internet for public procurement, licensing procedures, government-related formalities and filing of tax returns.
- For example, when Classic Shoes Ltd., submits the tax returns to the income tax department through internet, then it is B2G e-commerce.

Advantages of E-Business

- Easy to set up:
- Flexible Business Hours:
- Cheaper than Traditional Business:
- No Geographical Boundaries:
- Government Subsidies:
- New market entry:
- Lower levels of inventory:
- Lower costs of marketing and sales:

Disadvantages of E-Business

- Lack of Personal Touch:
- Delivery Time:
- Security Issues:

E-business Applications

- E-advertisement.
  - Display Ads
  - Email Ads.
  - Search Ads.
- E-marketing.
  - Search Engine Optimization (SEO)
  - Local Search Engine Optimization (LSEO)
  - Social Media Marketing.
  - Referral marketing
  - Content marketing
  - Search Engine Marketing (Pay per click, Cost per impression)

- E-Auction.
  - eCrater
  - Listia
  - Ubid
  - Bonanza
  - OnlineAuction.com
  - Atomic Mall
- E-Banking
- E-Directories
- E-Engineering.

- E-mail.
- E-marketing.
- E-Commerce.
- E-Learning.
- E-Franchising
- E-Gambling
- E-Trading (Stocks, Foreign Currency, Exchange Trading).

Internet as Infrastructure

- Internet is a network of network that connect computers all over the world.
- Network is an interconnection of systems to share data and information.
- Internet is a collection of government, academic, commercial, individual and other sites.

History of Internet

- In 1969,Department of Defense (DoD) USA created a small network of four computers called ARPANET (**A**dvanced **R**esearch **P**rojects **A**gency **Net**work).
- This Network was setup for the military purpose.
- The Primary goal of ARPANET was to allow multiple users to send and receive information simultaneously over the communication path.
- The Network operated with a technique called packet switching using TCP.

- The ARPANET was successful, and many universities joined the network.
- This ARPANET was divided into two parts MILNET and ARPANET.
- MILNET was used for military related sites and ARPANET for non-military related sites.
- These two networks were connected together by Internet Protocol (IP).
- The combined set of protocol is called TCP/IP.

- During the 1970's networks like BITNET and USENET came into being.
- Around 1980's NSFNET (National Science Foundation Network) was created.
- In 1984, NSF designed a high-speed successor to the ARPANET for all university research groups.

Overview of Internet Applications

- **E-mail:** This service has been available since the early days of the ARPANET and its enormous popular.
- **News:** Newsgroups are specialized forums in which users with common interest can exchange messages.
- **Remote login:** Users on the internet can log into any other machine on the internet on which they have account.
- **File Transfer:** Users can copy files from one machine on the internet to another.

Internet Terminologies

- **Client:** A client is any computer on the network that requests services from another computer on the network. To be able to request services and access the resources present on some other computer on the network, the client should have adequate access permissions.
- **Server:** A server is a computer that receives requests from client computers, process these requests and send the output to the respective client computers that had placed requests. The range of services that a server can offer a client is based on the permissions possessed by the client. The server computer defines these permissions.

Client-Server Network

- Client-Server Network is one of the most basic architecture that is used for computer connectivity.
- In this type of network, several client computers are connected to the server and also to each other.
- Client computers request services from the server computer, and the server accepts/rejects these requests.
- The server computer is also responsible for storing relevant information that is frequently used by the client.

Web Server.

- A Web Server is a computer that is dedicated to provide web services to clients on the internet.
- A Web server is a dedicated computer that uses HTTP (Hypertext Transfer Protocol) and other protocols to respond to client requests made over the World Wide Web.
- The main job of a web server is to display website content through storing, processing and delivering webpages to users.
- Basically **web server** is used to host the **web** sites but there exists other **web servers** also such as gaming, storage, FTP, email etc.

Web - Server Types

- **Apache HTTP Server:** This is the most popular web server in the world developed by the Apache Software Foundation.
- Apache web server is an open source software and can be installed on almost all operating systems including Linux, Unix, Windows, FreeBSD, Mac OS X and more.
- About 60% of the web server machines run the Apache Web Server.

Internet Information Services:

- The Internet Information Server (IIS) is a high-performance Web Server from Microsoft.
- This web server runs on Windows NT/2000 and 2003 platforms (and may be on upcoming new Windows version also).
- IIS comes bundled with Windows NT/2000 and 2003; Because IIS is tightly integrated with the operating system, so it is relatively easy to administer it.

Lighttpd:

- lighttpd: pronounced lighty is also a free web server that is distributed with the FreeBSD operating system.
- This open source web server is fast, secure and consumes much less CPU power.
- Lighttpd can also run on Windows, Mac OS X, Linux and Solaris operating systems.

Sun Java System Web Server:

- This web server from Sun Microsystems is suited for medium and large websites.
- Though the server is free it is not open source.
- However, it runs on Windows, Linux and Unix platforms.
- The Sun Java System web server supports various languages, scripts and technologies required for Web 2.0 such as JSP, Java Servlets, PHP, Perl, Python, Ruby on Rails, ASP and Coldfusion etc.

Jigsaw Server:

- Jigsaw (W3C's Server) comes from the World Wide Web Consortium.
- It is open source and free and can run on various platforms like Linux, Unix, Windows, Mac OS X Free BSD etc.
- Jigsaw has been written in Java and can run CGI scripts and PHP programs.

Internet Service Provider (ISP)

- Internet services typically provided by ISPs can include Internet access, Internet transit, domain name registration, webhosting, Usenet service, and colocation.
- ISP's are companies that help users connect to the internet for a monthly fee. In return, they provide a username and password and a telephone number.
- The username and password are used to authenticate the user on the internet.
- Some of the ISP are Hathway, Railwire, JIO, Airtel, Vodafone, BSNL, etc.,

Modem

- To access the internet, a user requires a hardware device called a Modem.
- The word Modem originated from the word's ***modulator*** and ***demodulator***.
- A modem transmits data over telephonic lines as anolog signals and then converts them to digital signals that can be interpreted by a computer.
- The sending **modem** modulates the data into a signal that is compatible with the phone line, and the receiving **modem** demodulates the signal back into digital data.

Web Page

- Any page that is hosted on the internet is called as web page.
- A **web page** is a **simple** document displayable by a browser. Such documents are written in the HTML language.
- A Web page may be Static or Dynamic.
- Collection of web pages is called as website.

Web Development

- Web development is the work involved in developing a Web site for the Internet or an intranet.
- Web development can range from developing a simple single static page of plain text to complex Web-based Internet applications, electronic businesses, and social network services.

- **The Domain Name System (DNS)** is the phonebook of the Internet. DNS translates domain names to IP addresses so browsers can load Internet resources.
- **Uniform Resource Locator (URL)** is used to specify addresses on the World Wide Web. A URL is the fundamental network identification for any resource connected to the web (e.g., hypertext pages, images, and sound files). URLs have the following format: protocol://hostname/other_information.
- **Browser:** Contains the basic software that can retrieve, view and send information over the internet.
- **Download:** To copy data from a remote computer to the local computer.

- **Upload:** To send data from local computer to remote computer.
- **E-mail:** Electronic Mail is the exchange of computer stored messages by Tele communication. Email can be distributed to lists of people as well as individuals.
- **HTML:** HTML is the standard markup language for creating Web pages. HTML describes the structure of a Web page. HTML consists of a series of elements. HTML elements tell the browser how to display the content.

Hypertext

- Hypertext is text which contains links to other texts.
- Hypertext is text displayed on a computer display or other electronic devices with references to other text that the reader can immediately access.
- Hypertext documents are interconnected by hyperlinks, which are typically activated by a mouse click, keypress set or by touching the screen.

Hypermedia

- Hypermedia is an extension of the term hypertext.
- Hypermedia is a nonlinear medium of information that includes graphics, audio, video, plain text and hyperlinks.
- The term was first used in a 1965 article written by Ted Nelson.
- The World Wide Web is a classic example of hypermedia.
- The most common type of hypermedia is an image link. Photos or graphics on the Web are often linked to other pages.

Managing E-business Infrastructure

- The **Internet** is the global system of interconnected computer networks that uses the Internet protocol suite (TCP/IP) to communicate between networks and devices
- An **Intranet** is a computer network for sharing information, collaboration tools, operational systems, and other computing services within an organization, usually to the exclusion of access by outsiders.
- An **Extranet** is a controlled private network that allows access to partners, vendors and suppliers or an authorized set of customers – normally to a subset of the information accessible from an organization's intranet

- **Collaborative commerce** (C-commerce) is the use of digital technologies by different business parties for sourcing products, making transactions or completing similar interactive business processes. It is a subcategory of e-commerce.
- Collaborative commerce is a business-to-business (B2B) transaction involving a trading community or a segment of an industry. To allow collaboration between the business parties, the buyers and sellers use compatible software tools in their distribution and supply chain. Hence, C-commerce is sometimes viewed as an aspect of supply chain management.

- **Mobile commerce**, also known as m-commerce, is the use of wireless handheld devices like cellphones and tablets to conduct commercial transactions online, including the purchase and sale of products, online banking, and paying bills.

Advantages of Internet

- **Ease of Access and Global Reach:** The World Wide Web (WWW) is an ideal mechanism for providing relevant information to the public globally. It allows organizations an opportunity for publicizing their products and services at mini* cost. The WWW holds the potential to increase thd market share and helps expand into new markets by virtue of its global reach. Additionally, easy access to information through the Internet gives the opportunity to compare the costs and characteristics of products & services.

- **Online Communication:** The Internet offers online facility that is a two-way communication interactive for e-commerce purchasing and selling of products.
- **Low-Cost Advertising Medium:** There is no doubt that Internet has become an inexpensive advertising medium for organizations and is being effectively used by some firms for commerce.
- **Low Barriers to Entry:** Small and large firms alike have the opportunity to be on the www and conduct business on the Internet. The barriers to entry to the Internet are very small.
- **Perceived Image Enhancer:** Several executives mentioned that they have to have presence on the Internet as their competitors are already on the Internet. Without it their reputation can be tarnished and they will be perceived as laggards in employing state-of-the-art technologies.

Disadvantages of Internet

Based on the research conducted by many experts, several problems are identified and they are summarized below:

- **Security:** A security threat is defined as "a circumstance, condition or event with the potential to cause economic hardship to data or network resources in the form of destruction, disclosure, modification of data, denial of service and/or fraud, waste and abuse". When an organization uses the Internet to engage in electronic commerce, it exposes itself to security risk.
  - According to Kalakota and Whinston, "when an organization establishes an Internet connection, that connection effectively breaches the physical security perimeter of the corporate network and opens itself to access from other networks comprising the public Internet". These risks fall into three general categories: Client/ Server risk, data transfer and transaction risk and virus risk.

- **Costs:** Many firms who have not explored issues of electronic commerce have said that they are concerned with the start-up cost involved.
- There are four components of the costs involved with electronic commerce:
  - **Connection:** connection costs to the Internet (i.e., direct link or connection provider);
  - **Hardware/Software:** hardware (i.e., sophisticated computer, modem, routers, etc.). Other companies mentioned the cost of adequate hardware;
  - **Set-up:** employee work hours involved in the processes of setting up the systems;
  - **Maintenance:** employee training and maintenance (of web pages);

- **Legal Issues:** Many executives mentioned the legal issues as a significant impediment to conducting EC on the Internet. It is uncertain what the possible legal issues are that will start to pop up as business on the Internet progresses.
- **Training and Maintenance:** A qualified staff whose job would be to initiate, update, and maintain their Internet facilities is needed. Some of the issues involved with training and maintenance can be handled by outsourcing certain functions and services.

- **Lack of Skilled Personnel:** Several executives mentioned that they had some difficulty in finding skilled www developers, content providers, and knowledgeable professionals to manage and maintain customer hot-line.
- **Uncertainty and Lack of Information:** Most of the companies interviewed, see the Internet as a marketing tool and as a media for advertisement. For a company that has never used any electronic means of communication with its customers, the Internet is an unknown model. Measures of how effective it is like the conduct of commerce are undermined and sometimes uncertain.

Architectural Framework for E-Commerce

- Architectural Framework of E-commerce means the synthesizing of various existing resources like DBMS, data repository, Computer languages, software agent –based transactions, monitors or communication protocols to facilitate the integration of data and software for better applications.
- Architecture Framework for E-Commerce contains six layers of functionality or services.
  - Application Services.
  - Brokerage Services, Data or Transaction Management.
  - Interface and support layers.
  - Secure messaging, security and EDI.
  - Middleware and structured document interchange
  - Network Infrastructure and Basic communication services.

Application Services Layer

- Application Services layer decides what type of e-commerce application is going to be implemented.
- It may be business-to-business, consumer-to-business or Intra organizational transactions.
- Consumer-to-Business: also called as Enterprise Marketplace Transaction. In marketplace transaction customer learn about the product differently through Electronic publishing then pay for them differently using Electronic cash and secure payment and have them developed differently.

- Business to Business: This is called as market link transaction. Here business, govt and other organizations depend on computer to computer communication as a fast, economical dependable way to conduct business transactions. They include the use of EDI and E-mail for Purchasing goods and services, buying information and consulting services, submitting requests for proposals and receiving proposals.
- Intra Organizational transactions: This is called market driven transaction. A company becomes market driven by dispersing throughout the firm information about his customers and competitors by spreading strategic and tactical decision making so that all units can participate and by continuously monitoring their customer commitment.

- Information Brokerage and Management Layer is dealing with voluminous amounts of information on the networks.
- This layer works as an intermediary who provides service integration between customers and information providers, give some constraint such as low price, fast services or profit maximation. Eg: Flight Booking.
- Brokerage Layer also supports data management and traditional transaction services.

- Brokerages may provide tools to accomplish more sophisticated, time-delayed updates or future-compensating transactions.
- The third layer of the architectural framework is Interface layer. This layer provides interface for e-commerce applications.
- Interactive catalogs and directory support services are the examples of this layer.
- Interactive catalogs are the customized interface to customer applications such as home shopping. Interactive catalogs are very similar to the paper-based catalog.

- The only difference between the interactive catalog and paper-based catalog is that the first one has the additional features such as use of graphics and video to make the advertising more attractive.
- **Directory services** have the functions necessary for information search and access. The directories attempt to organize the enormous amount of information and transactions generated to facilitate e-commerce.
- The main difference between the interactive catalogs and directory services is that the interactive catalogs deal with people while directory support services interact directly with software applications.

Secure Messaging Layer

- In any business, electronic messaging is an important issue. The commonly used messaging systems like phone, fax and courier services.
- The electronic messaging has changed the way the business operates. The major advantage of the electronic messaging is the ability to access the right information at the right time across diverse work groups.
- The main constraints of the electronic messaging are security, privacy, and confidentiality through data encryption and authentication techniques.

Middleware services

- The enormous growth of networks, client server technology and all other forms of communicating between/among unlike platforms is the reason for the invention of middleware services.
- Middleware is computer software that provides services to software applications beyond those available from the operating system.
- Middleware makes it easier for software developers to implement communication and input/output, so they can focus on the specific purpose of their application
- The middleware services are used to integrate the diversified software programs and make them talk to one another.

Transparency

- Middleware services focus on three elements.
  - Transparency
  - Transaction security management
  - Distributed object management services.
- Transparency implies that users should be unaware that they are accessing multiple systems.
- Transparency is essential for dealing with higher-level issues than physical media and interconnection that the underlying network infrastructure is in charge of.

- The ideal picture is "Virtual" Network is collection of work group, departmental, enterprise, and inter-enterprise LAN that appears to the end user or client application to be a seamless and easily accessed whole.
- Transparency is accomplished using middleware that facilitates a distributed computing environment. This gives users and applications transparent access to data, computation, and other resources across collections of multi-vendor and heterogenous systems.
- Users need not spend their time trying to understand where something is.
- Application developers have to code into their applications the exact locations of resources over the network.
- The goal is for the applications to send a request to the middleware layer, which then satisfies the request any way using remote information

Transaction Security and Management

- Transaction processing(TP) is fundamental to success in the electronic commerce market.
- Security and management are essential to all layers in the electronic commerce model.
- At the transaction security level, two broad general security services are Authentication and Authorization.

- Transaction integrity must be a given for businesses that cannot afford any loss or inconsistency in data.
- middleware provides the qualities expected in standard TP system called ACID properties(Atomic, Consistency, Isolation and durability).
  - Atomic - all changes are made (commit), or none (rollback).
  - Consistent- transaction won't violate declared system integrity constraints
  - Isolated - results independent of concurrent transactions.
  - Durable - committed changes survive various classes of hardware failure.

Distributed Object Management

- It is hard to write a network based application without either extensive developer retaining or technology that adopts the difficulties of the network.
- Objects are defined as combination of data and instructions acting on the data.
- A natural instance of an object in E-commerce is a document. A document carries data and instruction about the action to be performed on the data.
- Middleware acts an integrator for various stand protocols such as TCP, IP and OLE.

Network Infrastructure

- We know that the effective and efficient linkage between the customer and the supplier is a precondition for e-commerce. For this a network infrastructure is required.
- The early models for networked computers were the local and long-distance telephone companies.
- The telephone company lines were used for the connection among the computers. As soon as the computer connection was established, the data traveled along that single path.

- Telephone company switching equipment (both mechanical and computerized) selected specific telephone lines, or circuits, that were connected to create the single path between the caller and the receiver.
- This centrally-controlled, single-connection model is known as Circuit Switching.


Thank you

COMMUNICATION MEDIA

Dr P.V. Praveen Sundar
Assistant Professor,
Department of Computer Science
Adhiparasakthi College of Arts & Science,
Kalavai.

19-08-2020

III BBA

COMMUNICATION NETWORK OVERVIEW

Dr P.V. Praveen Sundar
Assistant Professor,
Department of Computer Science
Adhiparasakthi College of Arts & Science,
Kalavai.

17-08-2020

III BBA

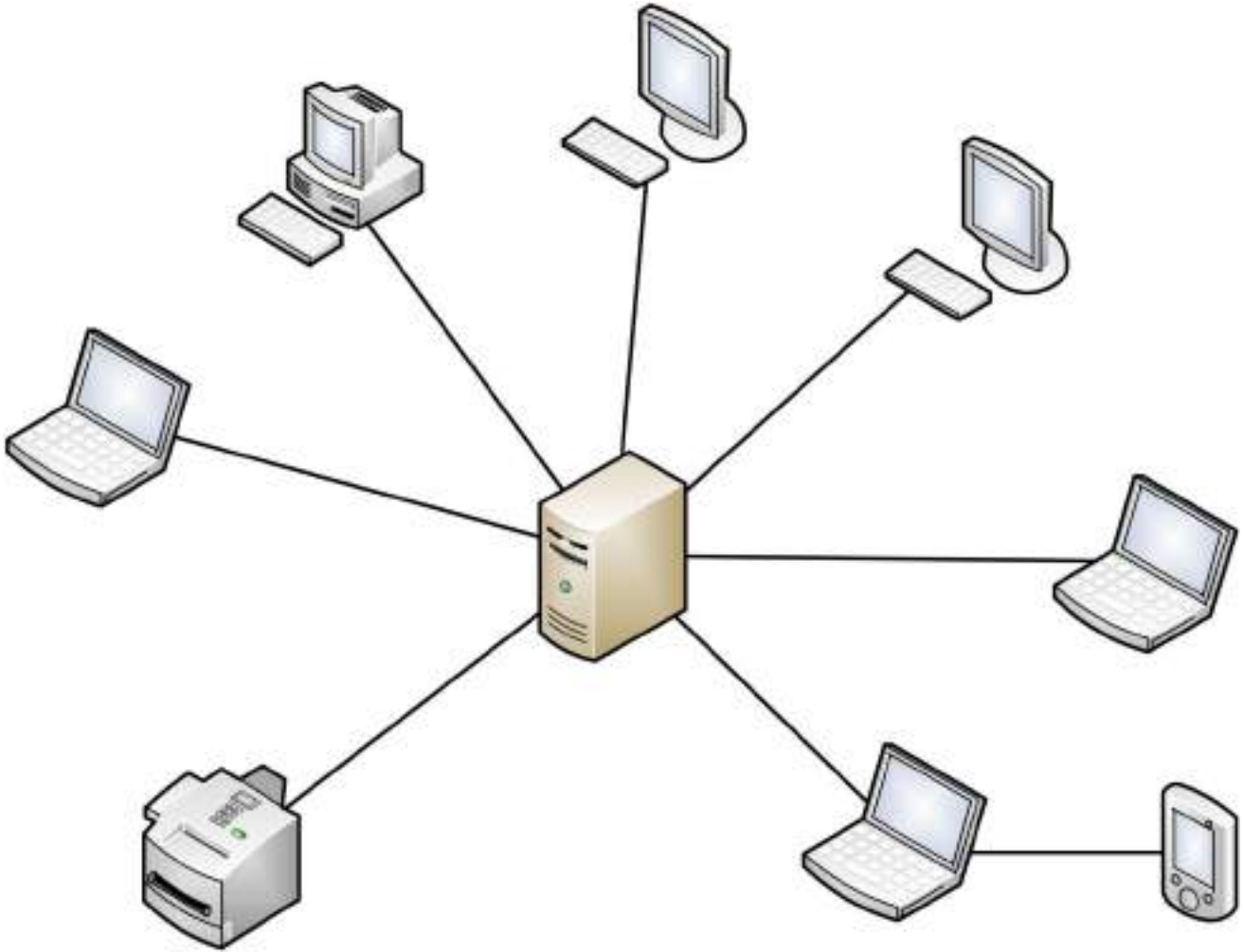
Communication Network

- A computer network is a group of computers that use a set of common communication protocols over digital interconnections for the purpose of sharing resources located on or provided by the network nodes.
- A **network** consists of two or more computers that are linked in order to share resources (such as printers and CDs), exchange files, or allow electronic communications.
- The computers on a network may be linked through cables, telephone lines, radio waves, satellites, or infrared light beams.

Components of Computer Network

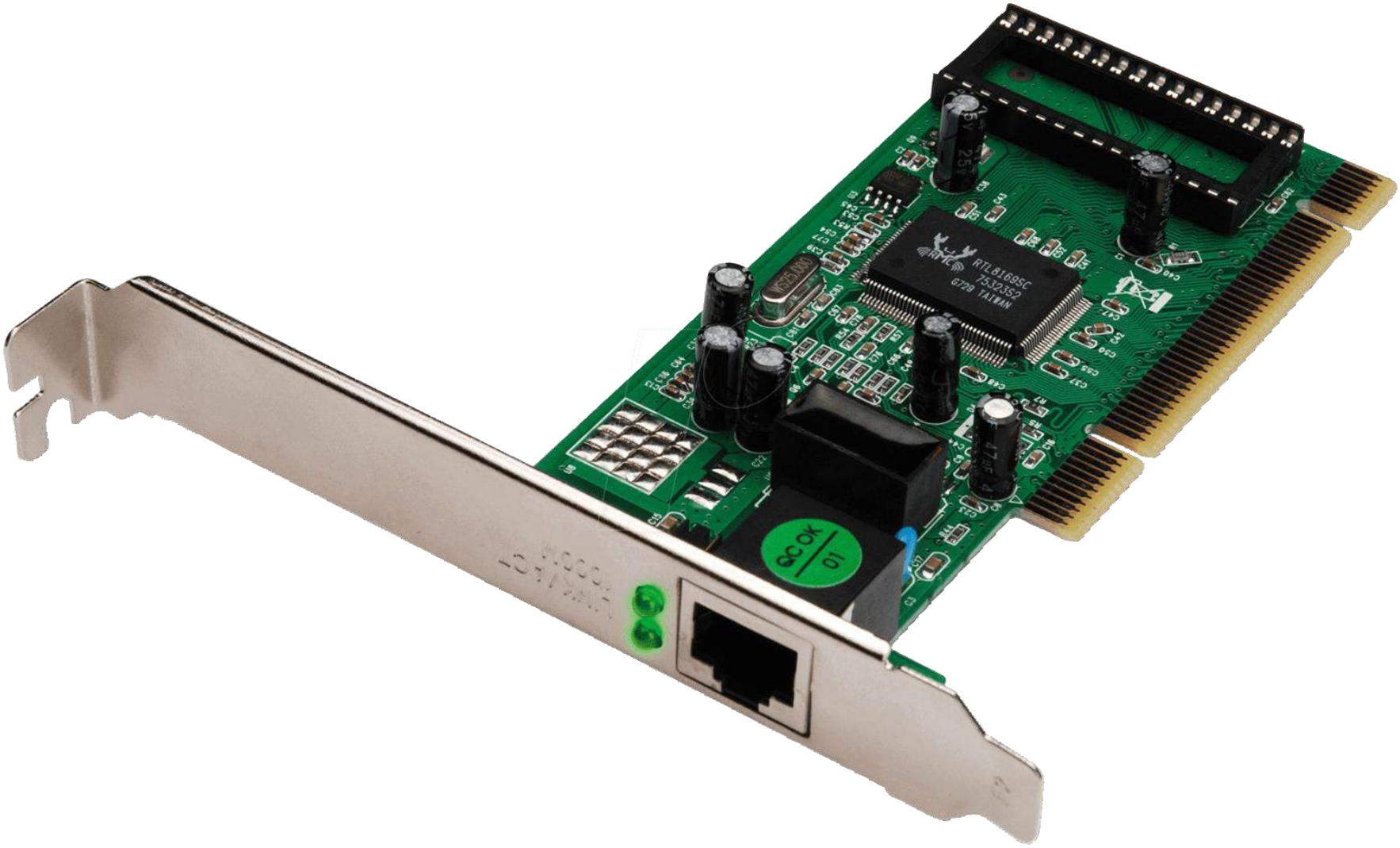
- **Servers** - Servers are computers that hold shared files, programs, and the network operating system.
- Servers provide access to network resources to all the users of the network.
- There are many kinds of servers, and one server can provide several functions.
- Sometimes it is also called host computer, servers are powerful computer that store data or application and connect to resources that are shared by the user of a network.

- For example, there are file servers, print servers, mail servers, communication servers, database servers, fax servers and web servers, to name a few.
- **Clients** - Clients are computers that access and use the network and shared network resources.
- Client computers are basically the customers(users) of the network, as they request and receive services from the servers.



- **Transmission Media** - Transmission media are the facilities used to interconnect computers in a network, such as twisted-pair wire, coaxial cable, and optical fiber cable. Transmission media are sometimes called transmission medium channels, links or lines.
- **Shared data** - Shared data are data that file servers provide to clients such as data files, printer access programs and e-mail.
- **Shared printers and other peripherals** - Shared printers and peripherals are hardware resources provided to the users of the network by servers. Resources provided include data files, printers, software, or any other items used by clients on the network.

- **Network Interface Card** - Each computer in a network has a special extension card called a network interface card (NIC).
- The NIC prepares(formats) and sends data, receives data, and controls data flow between the computer and the network.
- On the transmit side, the NIC passes frames of data on to the physical layer, which transmits the data to the physical link. On the receiver's side, the NIC processes bits received from the physical layer and processes the message based on its contents.


RTL8168SC
7532352
0729 TAIWAN
QC OK
01

- **Local Operating System** - A local operating system allows personal computers to access files, print to a local printer, and have and use one or more disk and CD drives that are located on the computer.
- Examples are MS-DOS, Unix, Linux, Windows 2000, Windows 98, Windows XP etc.
- The network operating system is the software of the network.
- It serves a similar purpose that the OS serves in a stand-alone computer

- **Hub** - Hub is a device that splits a network connection into multiple computers.
- It is like a distribution center. When a computer requests information from a network or a specific computer, it sends the request to the hub through a cable.
- The hub will receive the request and transmit it to the entire network.
- Each computer in the network should then figure out whether the broadcast data is for them or not. If not, the request will be dropped.

Switch

- **Switch** - A switch is a hardware device that connects multiple devices on a computer network.
- A Switch contains more advanced features than Hub.
- The Switch contains the updated table that decides where the data is transmitted or not.
- Switch delivers the message to the correct destination based on the physical address present in the incoming message.
- A Switch does not broadcast the message to the entire network like the Hub.

- It determines the device to whom the message is to be transmitted.
- In other words, switch connects the source and destination directly which increases the speed of the network.

Network switches

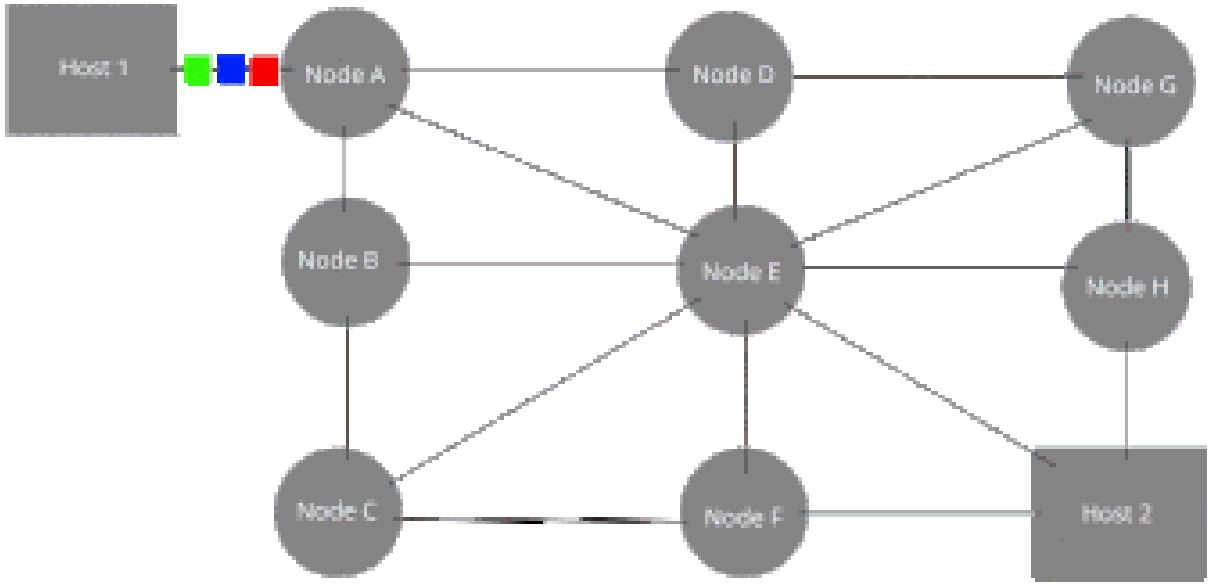
- **Router** - A router is a hardware device which is used to connect a LAN with an internet connection.
- It is used to receive, analyze and forward the incoming packets to another network.
- A router forwards the packet based on the information available in the routing table.
- It determines the best path from the available paths for the transmission of the packet.
- **LAN Cable** A local area Network cable is also known as data cable or Ethernet cable which is a wired cable used to connect a device to the internet or to other devices like computer, printers, etc.


LINKSYS
EA7500

Packet Switching

- A **packet** is a small amount of data sent over a network, such as a LAN or the Internet.
- Each **packet** includes a source and destination as well as the content (or data) being transferred.
- Packets are composed of a header and payload. Information in the header is used by networking hardware to direct the packet to its destination where the payload is extracted and used by application software
- Packet switching increases network efficiency and robustness and enables technological convergence of many applications operating on the same network.

The original message is Green, Blue, Red.



Public Switched Telephone Network

- PSTN stands for Public Switched Telephone Network, or the traditional circuit-switched telephone network that are operated by national, regional, or local telephony operators, providing infrastructure and services for public telecommunication.
- This system has been in general use since the late 1800s.
- The phones themselves are known by several names, such as PSTN, landlines, Plain Old Telephone Service (POTS), or fixed-line telephones.

The PSTN consists of telephone lines, fiber optic cables, microwave transmission links, cellular networks, communications satellites, and undersea telephone cables, all interconnected by switching centers, thus allowing most telephones to communicate with each other.

Originally a network of fixed-line analog telephone systems, the PSTN is now almost entirely digital in its core network and includes mobile.

The Switches nowadays are digital and the traffic between switches is digitally multiplexed voice signals.

The Subscribers can send/receive either analog or digital voice to/from telephone exchange.

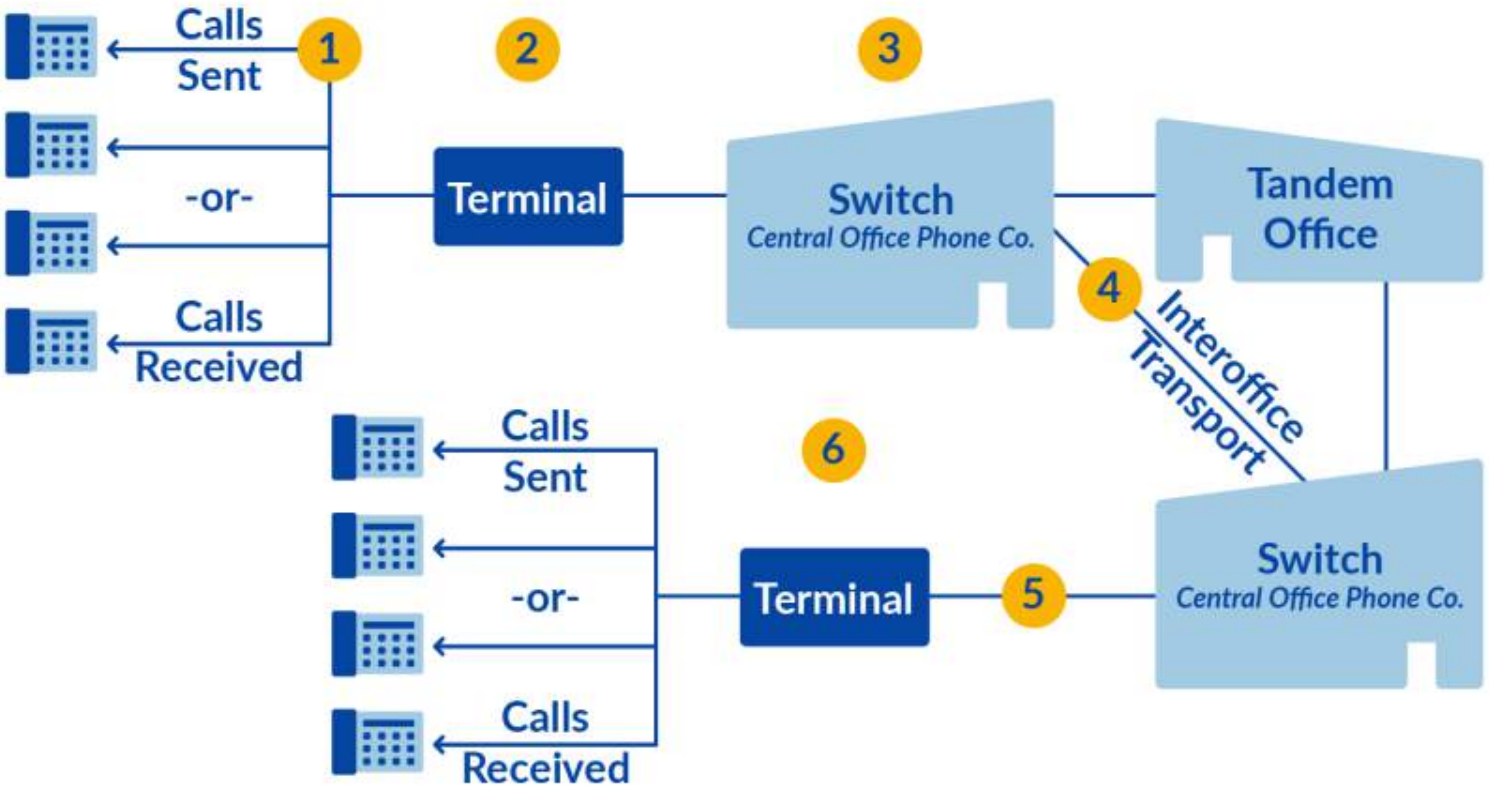
If the user has an analog instrument the voice signals are converted to the digital form at telephone exchange.

For the digital user, the analog to digital conversion of voice is done at the user's telephone instrument called digital telephone.

The Telephone network can carry data as well as facsimile traffic using suitable modems at user ends.

With advances in technology the circuit switches may be replaced by packet switches using Internet Protocol (IP) leading to the emerging voice over IP (VoIP) technique in telephonic networks.

Plain Old Telephone Service (POTS) Networking



Computer/Data Networks

- Computer Networks includes the internet carries digital data from source and destination.
- Here the nodes are packet switches and use store and forward mechanism.
- A packet switch information in the form of packets, stores them and forwards the packets to a free outgoing link.
- Packet switches transmits the packets onward identifying the address of the packet.

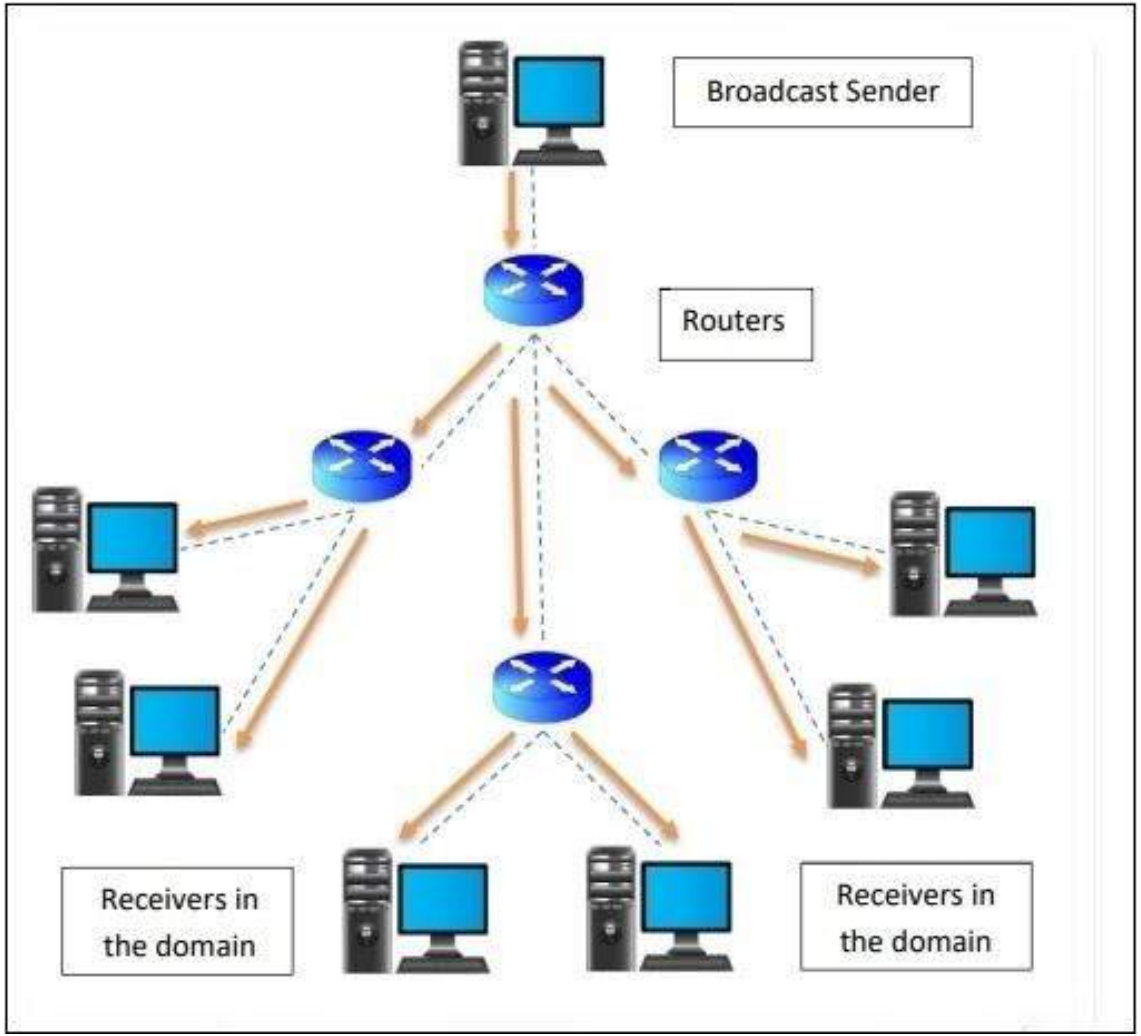
- The branches are the similar to the ones used in telephone networks.
- The data networks carry data traffic varying from low bit rates to extremely high bit rates such as Giga/Tera/Peta bits per second.
- The internet is a network of networks which interconnects multiple of networks and primarily designed to carry text messages.
- Nowadays, internet can support multimedia traffic as well.
- Telephone, music and video traffic are supported by internet.

Broadcast Network

- Broadcasting in computer network is a group communication, where a sender sends data to receivers simultaneously. This is an all – to – all communication model where each sending device transmits data to all other devices in the network domain.
- A typical example is a TV network where the same TV channel is delivered to all devices attached to the network.
- Earlier the broadcast network was supporting only the audio signal but today we have TV broadcast networks. This is basically a receive-only network.

- Because of the TV transmission the bandwidth is very high compared to the conventional telecommunication networks.
- The advances in technology will make this networks interactive where the user will be able to send some messages also.
- The broadcasting can be wireless as in radio and TV Networks.

- It can be using satellites as well. With the help of satellites broadcast can be over much larger areas.
- Cable TV and Optic fiber cables are also used for distribution of information/message.
- This mode has become very popular because it provides a large number of channels to the users.


Broadcast Sender
Routers
Receivers in the domain
Receivers in the domain

Mobile Communication Networks

- The requirement of the users to communicate even when they are on the move and the advances in the wireless/radio communication technology has propelled the emergence of the mobile telephone network, called the Cellular Mobile Telephone Network.
- Initially intended primarily for telephone communication, the mobile network now provides data as well as multimedia services to the mobile users on a global basis.
- A given geographical are is subdivided into small cells each with a fixed base station which in turn is connected to a switching centre by wired or wireless media.

- Switching centre (known as the mobile switching centre) connects the mobile user with rest of the telecommunication infra-structure and vice-versa.
- The mobile user is connected to the respective base station on a duplex radio link. Thus communication between a mobile and a fixed user is via the base station and the switching centre.
- The radio link between the mobile user and the base station allows the mobile user to move.

- It supports data in addition to voice communication.
- Adjacent cells are given different frequencies, but the far-off cells can be assigned the same frequencies for the radio links.
- This way the frequencies can be reused relaxing the constraint on limited spectrum.
- Mobile communication has evolved from the original first generation (analog) to the second generation (digital) like the GSM (Global System for Mobile Communications) and the CDMA (Code-Division Multiple Access).

- The third generation of mobile communication known as the IMT-2000 and the UMTS are rolling out.
- They can support data up to 2Mbps and have many advanced features.
- Wireless local area networks (WLAN) provide access to the Internet at speeds of 54 Mbps. Advances in cellular mobile telecommunications, WLAN's and mobile computing are paving the way for the ubiquitous global broadband mobile communications.

Communication Processors

- Communication processors resemble computer CPUs in that they have similar circuitry, have memories, and can be programmed, but their purpose is limited to enhance data communication between two points.
- Communication processors include the following.
  - Modems
  - Multiplexers
  - Message Switches
  - Concentrators and Controllers and
  - Front end Processors.

Modem

- A Modem is a peripheral device that allows a computer to connect and communicate with other computers.
- Modem stands for Modulator Demodulator.
- It is a hardware, which converts digital data into analog signals that can sent over an analog telephone line and Convert the analog signals back into digital data.

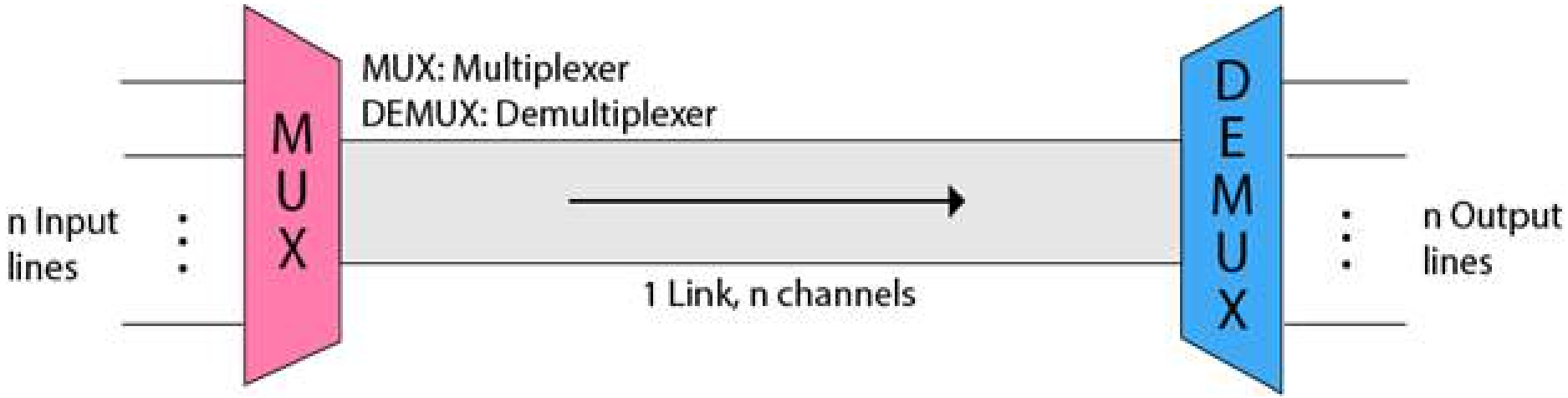
- The digital data from sender side computer is converted into analog data by the modem and it is transmitted over the telephone line. This is called Modulation.
- On the receiver side the analog data is converted into digital data by the modem and is given to the receiver computer. This is called as Demodulation.

Multiplexers

- Multiplexing is a technique used to combine and send the multiple data streams over a single medium.
- The process of combining the data streams is known as multiplexing and hardware used for multiplexing is known as a multiplexer.
- Multiplexer (MUX) combines n input lines to generate a single output line.

- Multiplexing follows many-to-one, i.e., n input lines and one output line.
- Demultiplexing is achieved by using a device called Demultiplexer (DEMUX) available at the receiving end. DEMUX separates a signal into its component signals (one input and n outputs).
- Therefore, we can say that demultiplexing follows the one-to-many approach.

- The transmission medium is used to send the signal from sender to receiver. The medium can only have one signal at a time.
- If there are multiple signals to share one medium, then the medium must be divided in such a way that each signal is given some portion of the available bandwidth. For example: If there are 10 signals and bandwidth of medium is100 units, then the 10 unit is shared by each signal.
- When multiple signals share the common medium, there is a possibility of collision. Multiplexing concept is used to avoid such collision.
- Transmission services are very expensive.


MUX: Multiplexer
DEMUX: Demultiplexer
MUX
DEMUX
n Input lines
n Output lines
1 Link, n channels

Concentrators

- A concentrator is a device that acts as an efficient forwarder of data transmission signals.
- A type of multiplexor that combines multiple channels onto a single transmission medium in such a way that all the individual channels can be simultaneously active.
- For example, ISPs use concentrators to combine their dial-up modem connections onto faster T-1 lines that connect to the Internet.

- A concentrator may be able to handle up to 100 dial-up modem calls, support a certain number of ISDN connections, and support leased line and frame relay traffic while also functioning as a router.
- The main function of this device is to make a kind of load balancing between two or more servers connected, data distribution is done according to the server processing rate.

Controllers

- Controllers will link group of terminals or other devices to the communications channel.
- The controller polls the status of each terminals and transfers data from terminal to the host computer when necessary.

Message switchers

- A message switcher is a processor that receives data messages from terminals, determines their designation, and routes them one at a time to the CPU.
- It distributes the messages coming from the CPU to the appropriate terminal.

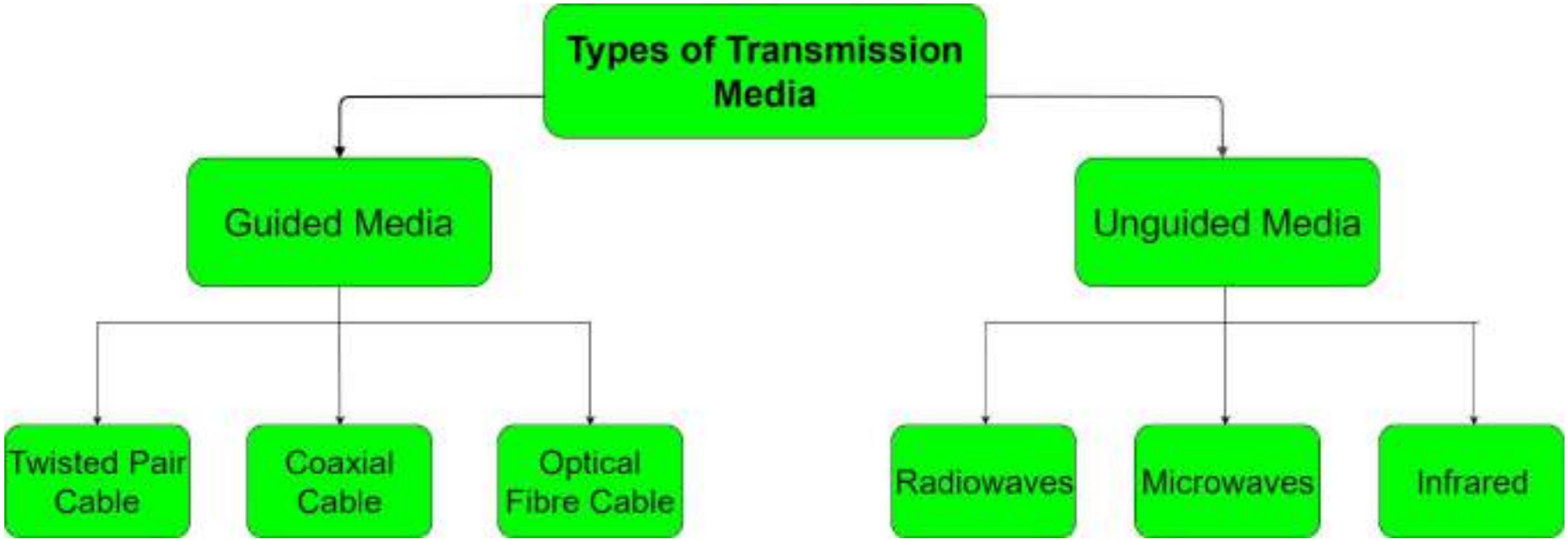
Front end Processor

- A front-end processor (FEP) is a processing device usually connected to the host computer at one end and communications channels at the other.
- The FEP is closer to the input source than is the main processor. It performs some task such as telemetry control, data collection, reduction of raw sensor data, analysis of keyboard input,
- FEP directs the transmitting and receiving of messages, detects and corrects transmission errors, assembles and disassembles messages, and performs other processing functions so that the main computer receives pure information.


Thank you

Communication Media

- Communication Media can be defined as physical path between transmitter and receiver in a data transmission system.
- In the communication process, a medium is a channel or system of communication by which information (the message) is transmitted between the sender and the receiver. The plural form is media, and the term is also known as a channel.
- The speed of data transmission or data rate depends upon the type of medium being used in the network. There are basically two types of networks:
  - Wired Network
  - Wireless Network


Types of Transmission Media
Guided Media
Unguided Media
Twisted Pair Cable
Coaxial Cable
Optical Fibre Cable
Radiowaves
Microwaves
Infrared

Guided Transmission Media

- In a Guided Transmission Media or wired network, data is transmitted over a physical medium. There are three types of physical cables used in a wired network.
  - Twisted Pair
  - Coaxial Cable
  - Fiber Optical

Twisted Pair

- One of the earliest guided transmission media is twisted pair cables.
- A twisted pair cable comprises of two separate insulated copper wires, which are twisted together and run in parallel.
- The copper wires are typically 1mm in diameter.
- One of the wires is used to transmit data and the other is the ground reference.

- All transmissions are prone to noise, interferences, and crosstalk's.
- When the wires are twisted, some part of the noise signals is in the direction of data signals while the other parts are in the opposite directions.
- Thus the external waves cancel out due to the different twists.
- The receiver calculates the difference in the voltages of the two wires for retrieving data. Thus a much better immunity against noise is obtained.
- Four wires are used to transmit the data- Orange and white is for sending data, Green is for receiver , brown and blue is for bandwidth signaling.

- **Applications of Twisted-Pair Cables**
  - In telephone lines
  - In DSL lines
  - In LANs
- **Types of Twisted–Pair Cables**

There are two types of twisted pair cables −

- Unshielded Twisted Pair (UTP):
- Shielded Twisted Pair (STP):

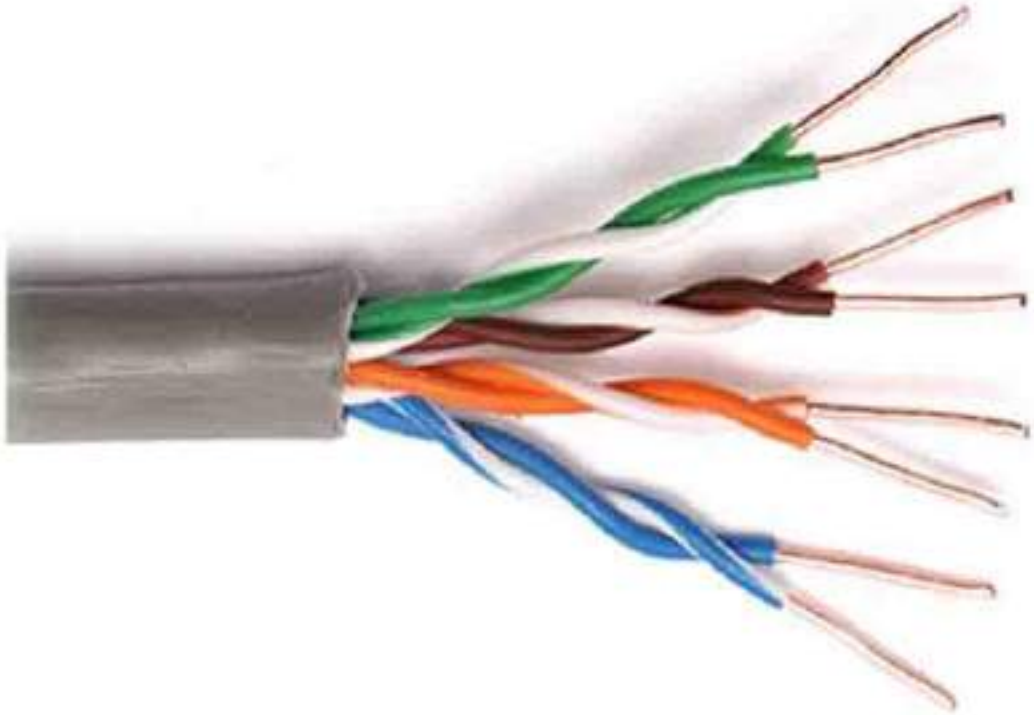
Categories of Twisted–Pair Cables

The Electronic Industries Alliance (EIA) has classified twisted pair cables into seven categories −

- **Category 1** – Defines a traditional UTP cable. It is designed to carry only voice and not data. This type of cable is not recommended for networking purposes and is used in telephony services.
- **Category 2** – Defines a cable that can carry data up to 4 Mbps. It consists of 4 pairs of wires.
- **Category 3** – Defines a cable that can carry data up to 10 Mbps. It consists of 4 pairs of wires. It is 1000 feet in length with marks of length at every 2 feet. The frequency of this cable is 16 MHz and It is used for the 10BaseT network.

- **Category 4 –** Defines a cable that can carry data up to 16 Mbps. It cable consists of 4 pairs of wires. The signaling frequency of this cable is up to 20 MHz.
- **Category 5 –** Defines a cable that can carry data up to 100 Mbps. The signaling frequency of this cable is up to 100 MHz. This type of cable is primarily used in today's networking environment. The cable is used in 100BaseX Ethernet architecture and **Asynchronous Transfer Mode (ATM)** architectures.
- **Category 5e –** Defines a cable that can carry data up to 1000 Mbps with a signaling frequency of 100 MHz It is used to connect computers, **hubs, switches** and print servers.

- **Category 6** – Defines a 4-pair cable that provides an improved performance as compared to Cat 5e. It can carry data up to 1000 Mbps with a signaling frequency of 250 MHz.
- **Category 7** – Defines a fully shielded twisted pair cable that operates at the signal frequency of 600 MHz Fully shielded means all the four pairs of a cable have an additional shield over them.



UTP

UNSHIELDED TWISTED PAIR CABLE

Unshielded Twisted Pair

- **UTP** is the copper media inherited from telephony, which is being used for increasing high data rates
- **UTP** cables are widely **used** in the computer and telecommunications industry as Ethernet cables and telephone wires.
- UTP is a very flexible, low cost media and can be used for either voice or data communications.

Characteristics of UTP Cable

Characteristics	Description
Maximum cable length	100 meters
Bandwidth	100 Mbps
Connector type	RJ-45
Cost	Cheapest form of cable
Interference protection	Very poor protection from EMI and RFI
Bend radius	360 degrees / feet
Signal transmission mode	Baseband
Resistance	50 ohms

- Advantages:
  - Cheapest form of cable available for networking purpose.
  - Easy to handle and install.
  - Can be used for high speed LAN
- Disadvantages:
  - Limited Bandwidth
  - High prone to crosstalk's.
  - Unable to provide secured transmission of data.

STP

SHIELDED TWISTED PAIR CABLE

Shielded Twisted Pair (STP)

- **STP Cable** or **Shielded Twisted Pair Cable** is a pair of wires wound around each other and each pair is placed inside a protective foil wrap to protect it from **crosstalk.**
- It is cheaper than fiber optic cables but more expensive than **UTP**.
- Shielded Twisted Pair Cable provides better protection from crosstalk and other interference as compared to **Unshielded Twisted Pair Cable.**
- The STP Cable price is approx Rs 50/meter.

- It is used in fast-data-rate Ethernet and in voice and data channels of telephone lines.
- The extra covering in **shielded twisted pair** wiring protects the transmission line from electromagnetic interference leaking into or out of the **cable.**
- STP cabling often is **used in** Ethernet networks, especially fast data rate Ethernets.

Characteristics of STP Cable

Characteristics	Description
Maximum cable length	100 meters
bandwidth	100 Mbps
Connector type	RJ-48c
Cost	Costlier than UTP but cheaper than fiber optic cable
Interference protection	Better protection from crosstalk and external interference
Signal transmission mode	Baseband
Resistance	50 ohms

Advantages of STP Cable

- Better protection from crosstalk.
- Better protection from external interference.
- Secured data transmission.

Disadvantages of STP Cable

- Costlier than UTP
- Difficult to install as compared to UTP.

Coaxial cable

- Coaxial cables are copper cables with metal shielding designed to provide immunity against noise and greater bandwidth.
- Coax can transmit signals over larger distances at a higher speed as compared to twisted pair cables.
- Coaxial cable transmits information in two modes: Baseband mode(dedicated cable bandwidth) and Broadband mode(cable bandwidth is split into separate ranges).
- Cable TVs and analog television networks widely use Coaxial cables.

BNC Connector

- Commonly used coaxial connector is BNC Connector("Bayonet Neill–Concelman").
- This **connector** has a center pin connected to the outer cable shield. A rotating ring outside the tube locks the cable to any female **connector**.
- They can also be used to split a **CCTV** or video signal for distribution to multiple devices or locations.
- Advantages
  - Bandwidth high
  - Transmits signals at high rate
- Disadvantages
  - Fault in the cable causes failure in the entire network.

- **Broadband** system use modulation techniques to reduce the effect of noise in the environment. Broadband transmission employs multiple channel unidirectional transmission using combination of phase and amplitude modulation.
- **Baseband** is a digital signal is transmitted on the medium using one of the signal codes like Non Return to Zero(NRZ), Return to Zero(RZ) Manchester biphase-M code etc. is called baseband transmission.

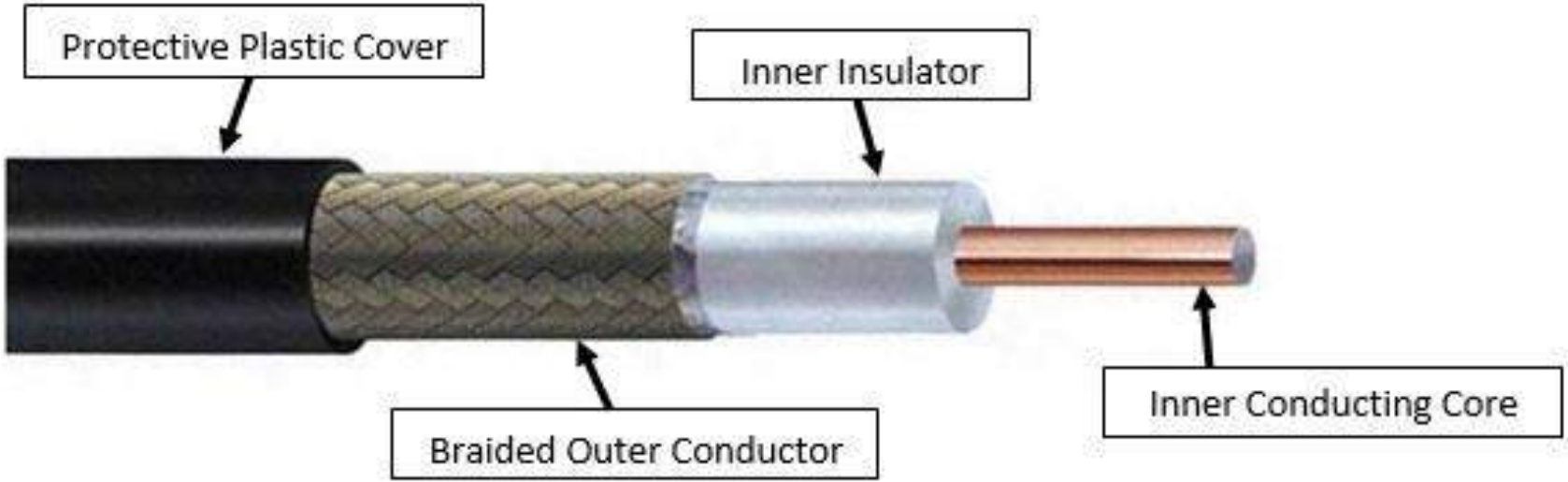
Baseband transmission –

1. Digital signaling.
2. Frequency division multiplexing is not possible.
3. Baseband is bi-directional transmission.
4. Short distance signal travelling.
5. Entire bandwidth is for single signal transmission.
6. Example: Ethernet is using Basebands for LAN.

Broadband transmission –

1. Analog signaling.
2. Transmission of data is unidirectional.
3. Signal travelling distance is long.
4. Frequency division multiplexing possible.
5. Simultaneous transmission of multiple signals over different frequencies.
6. Example : Used to transmit cable TV to premises.

- Coax has a central core of stiff copper conductor for transmitting signals.
- This is covered by an insulating material. The insulator is encased by a closely woven braided metal outer conductor that acts as a shield against noise.
- The outer conductor is again enclosed by a plastic insulating cover.


Protective Plastic Cover
Inner Insulator
Braided Outer Conductor
Inner Conducting Core

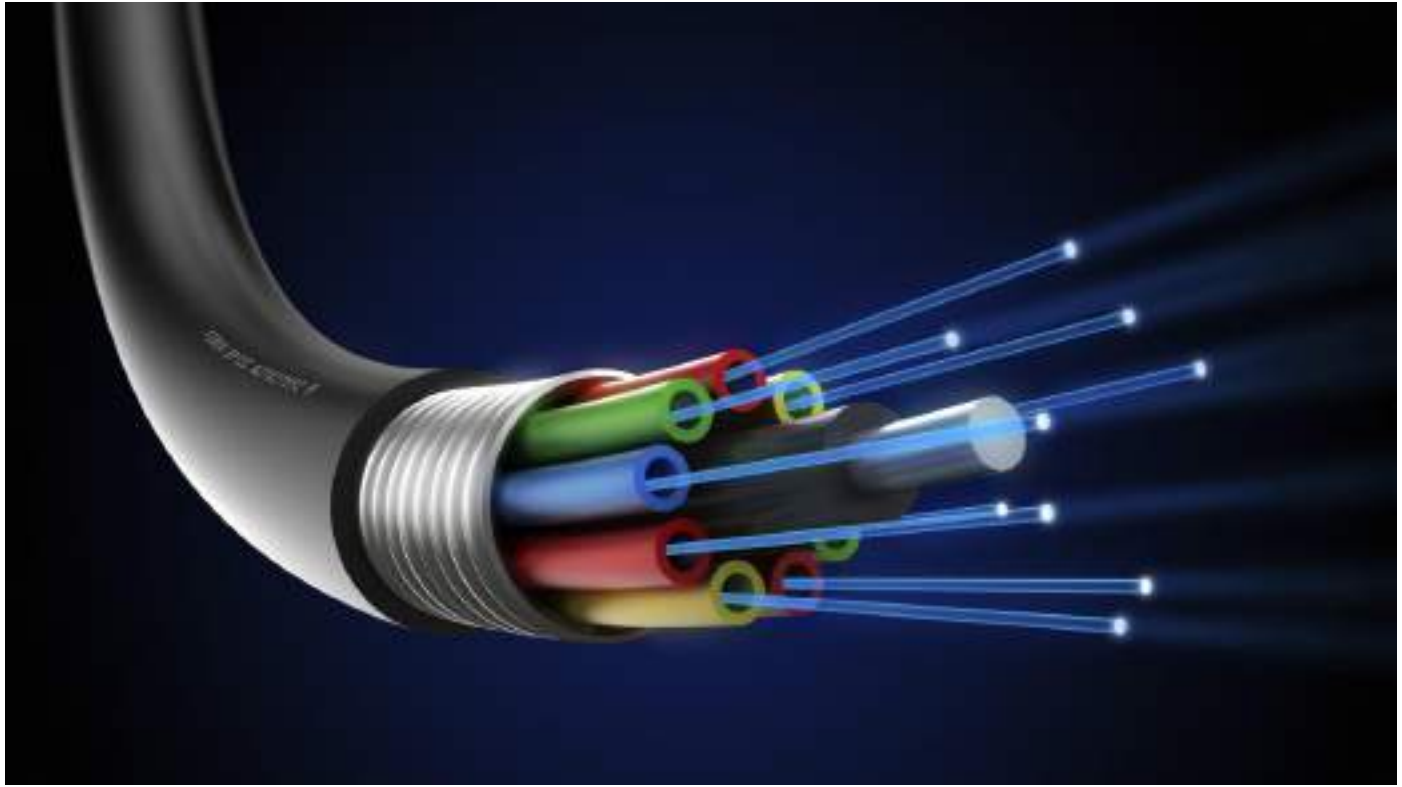
Advantages:

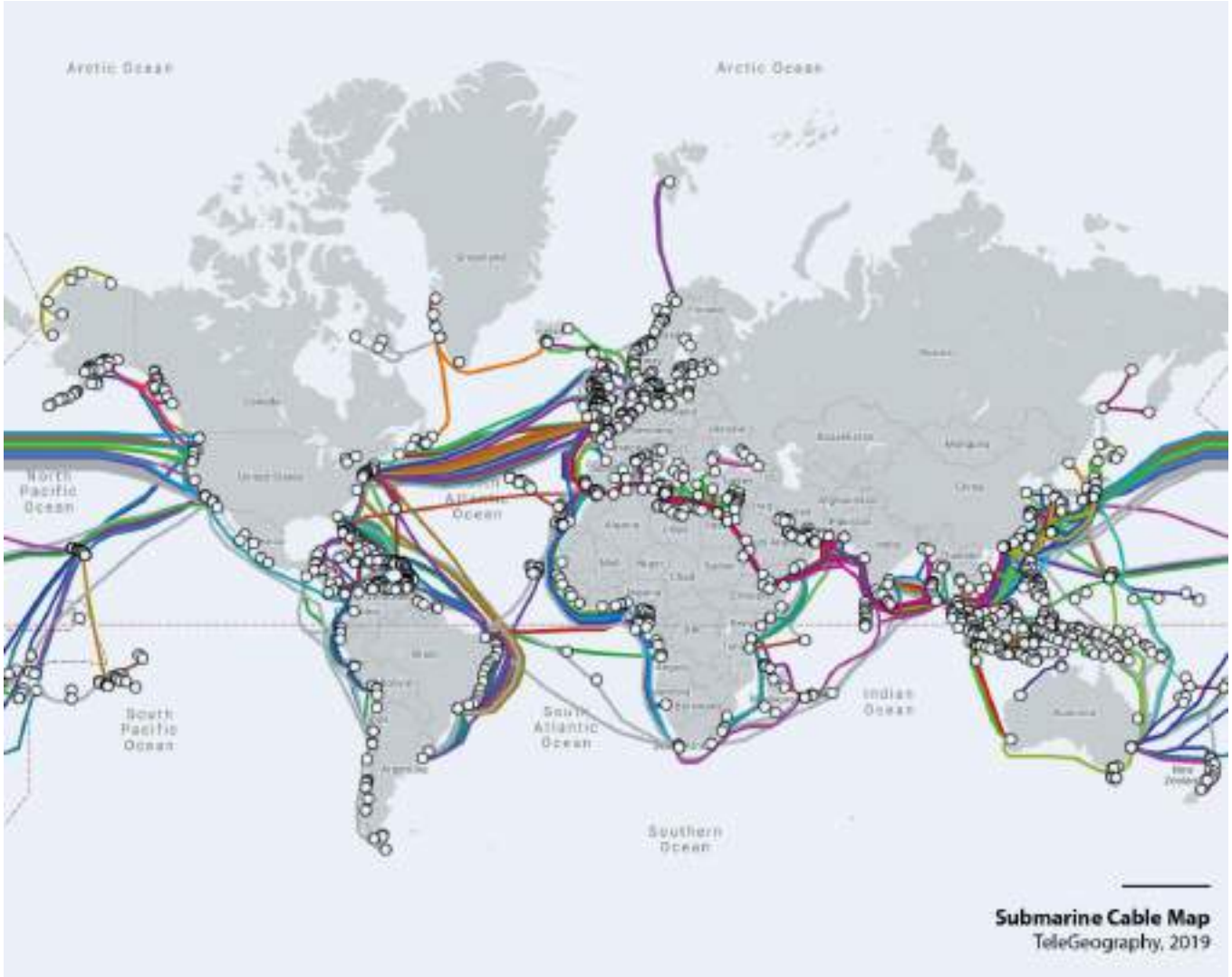
- High Bandwidth
- Better noise Immunity
- Easy to install and expand
- Inexpensive

Disadvantages

- Number of node connected is limited.
- Distance is limited

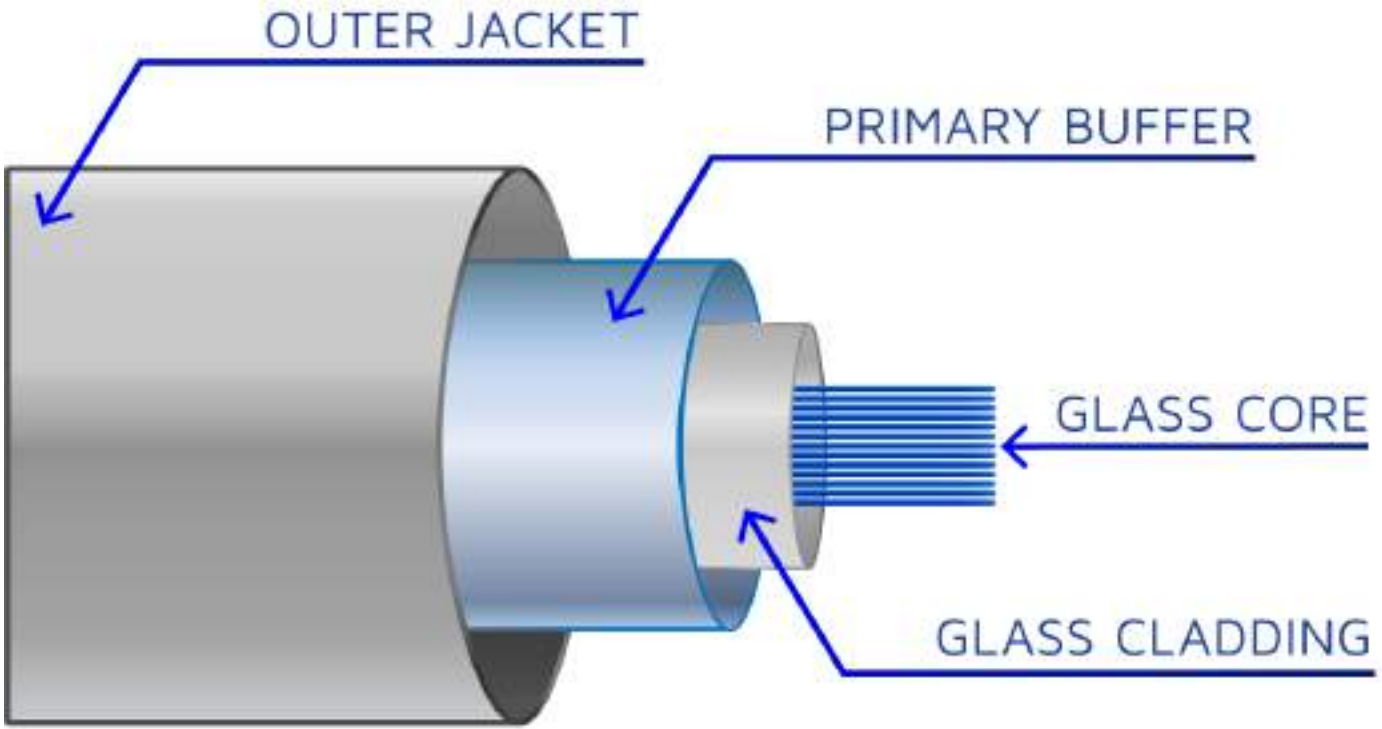
Fiber Optic Cable

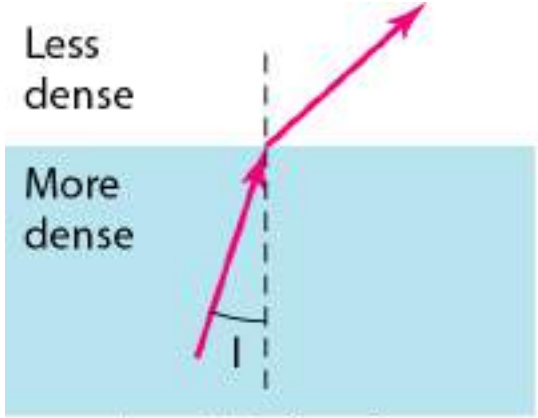



Arctic Ocean
Arctic Ocean
North Pacific Ocean
Atlantic Ocean
South Pacific Ocean
South Atlantic Ocean
Indian Ocean
Southern Ocean
Submarine Cable Map
TeleGeography, 2019

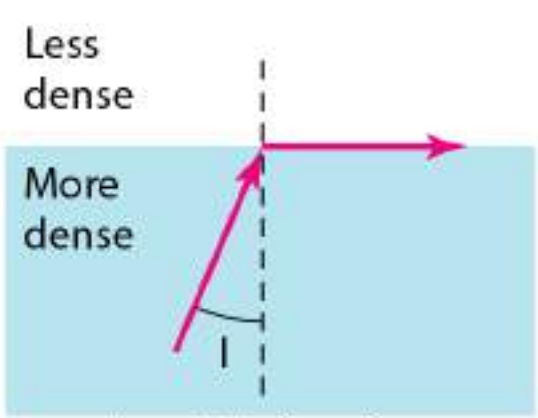
Fiber Optic Cable

- Optical fiber consists of thin glass fibers that can carry information at frequencies in the visible light spectrum and beyond.
- Typical fiber consists of a very narrow stand of glass called core.
- Around the core is a concentric layer of glass called cladding.
- A typical core diameter is 62.5 microns. Typical cladding has a diameter of 125 microns.
- Coating the cladding is a protective coating of plastic, it is called as jacket.
- Critical angle is referred as the angle of incidence beyond which total internal reflection occurs

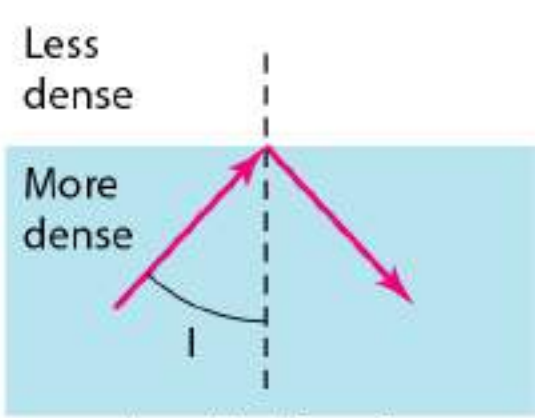

OUTER JACKET
PRIMARY BUFFER
GLASS CORE
GLASS CLADDING



I < critical angle,
refraction



I = critical angle,
refraction



I > critical angle,
reflection

- An important characteristics of fiber optics is refraction.
- Refraction is the characteristics of a material to either pass or reflect light.
- When light pass through a medium, it “bends” as it passes from one medium to the other.
- An example of this is when we look into a pond of water if the angle of incidence is small, the light rays are reflected and do not pass into the water.
- If the angle of incidence is great, light passes through the media, but it is bent of refracted.

- Optical fibers work on the principle that the core refracts the light and the cladding reflects the light.
- The core refracts the light and guides the light along the path.
- The cladding reflects any light back into core and stops light from escaping through it- it bounds the medium.

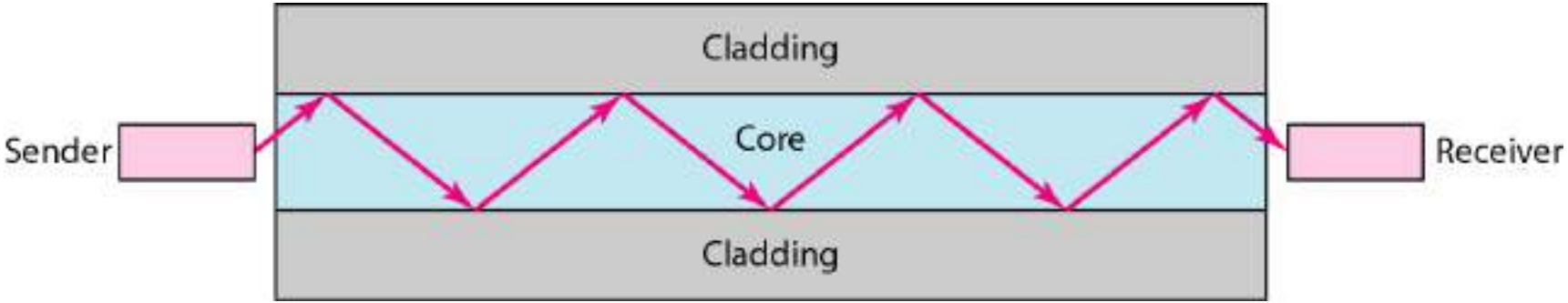
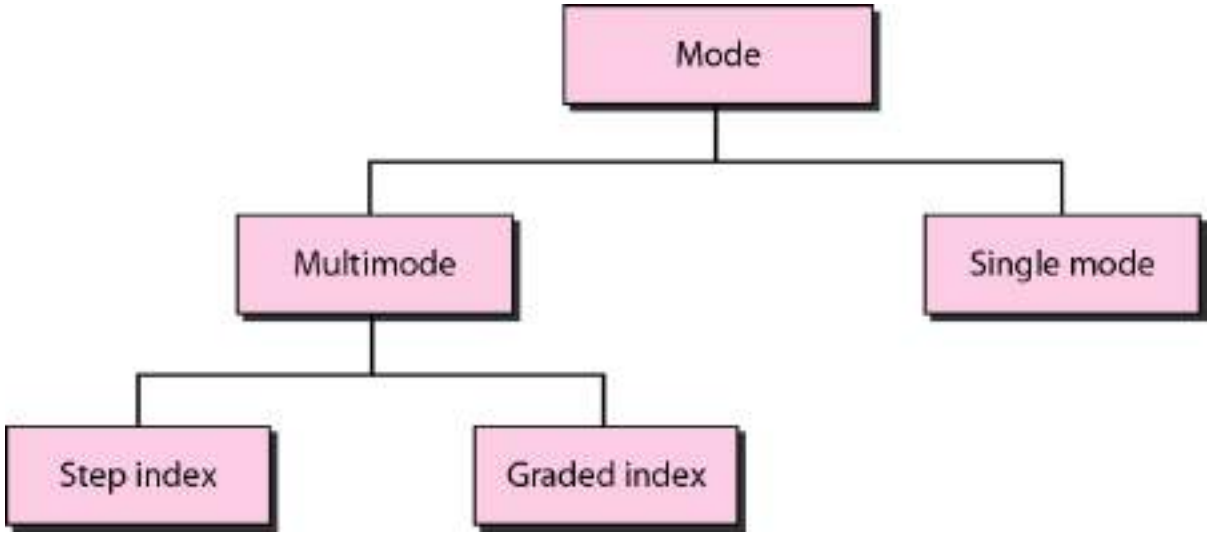

Cladding
Core
Cladding
Sender
Receiver

Figure 7.12 *Propagation modes*

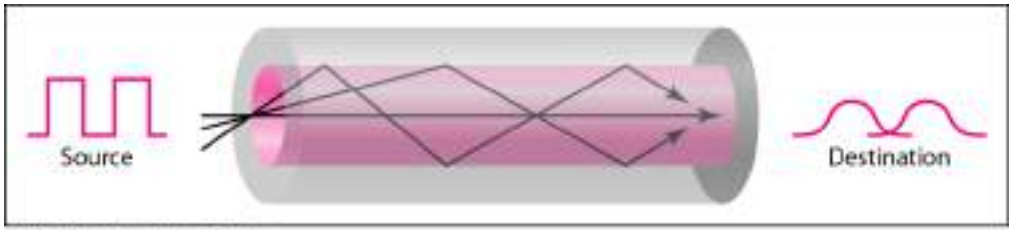


- Single-mode fiber optic cable excels at long-distance communication.
- Single-mode cable is designed to carry a single signal source with low transmission loss over great distances. (uniform entirely)
- It is frequently used for communication systems due to the clarity it provides.
- This type of fiber optic cable has the smallest core and the thickest sheathing.

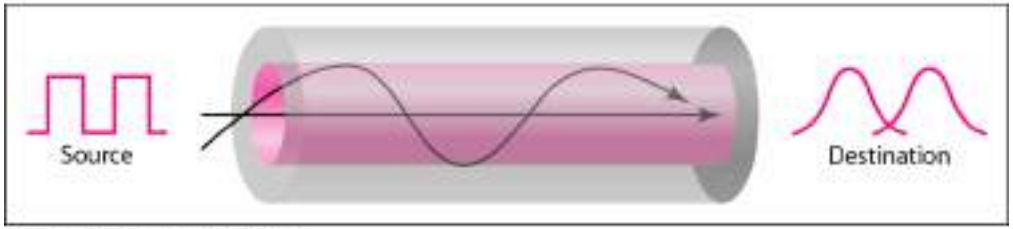
- Multimode cables are designed to carry multiple signals; however, this capacity comes with a loss of range. Multimode cables come in two primary varieties. They are Step index or Graded index cables.
- *Step index multimode cables* have a thick core through which signals are fed. They work well over moderate distances and can offer longer range communication potential with the use of amplifiers. The various light signals enter at different angles, transmitting at different rates through the cable.

- *Graded index multimode cables* have a core arranged in concentric circles, like the cross section of a tree.
- As light enters, it is transmitted through the rings with the outer rings travelling faster than transmissions in the central core. (Helical)
- This type of cable can handle many wavelengths of light at once, making it perfect for clear communication and data transfer requiring up to 100Gb transfer rate, as you would find at a large data center.

Figure 7.13 *Modes*

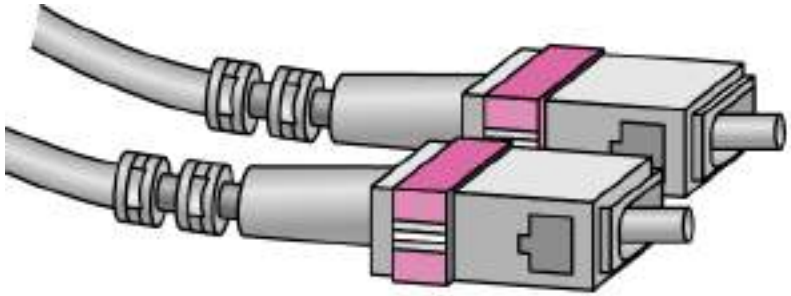


a. Multimode, step index

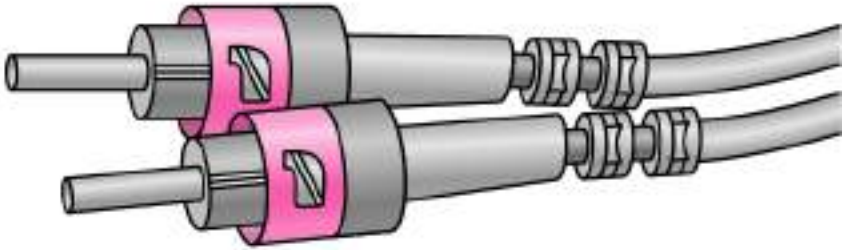


b. Multimode, graded index

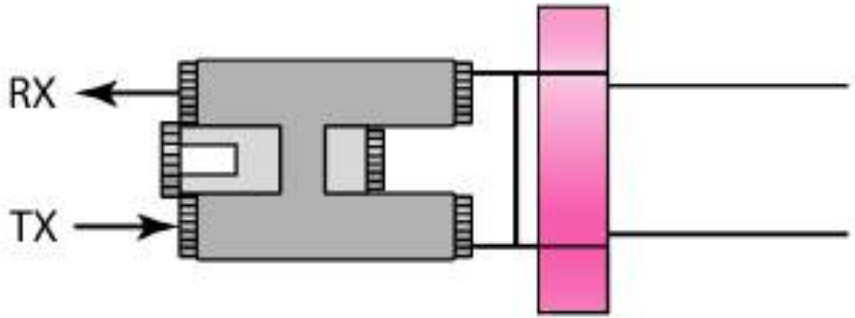
c. Single mode



SC connector



ST connector



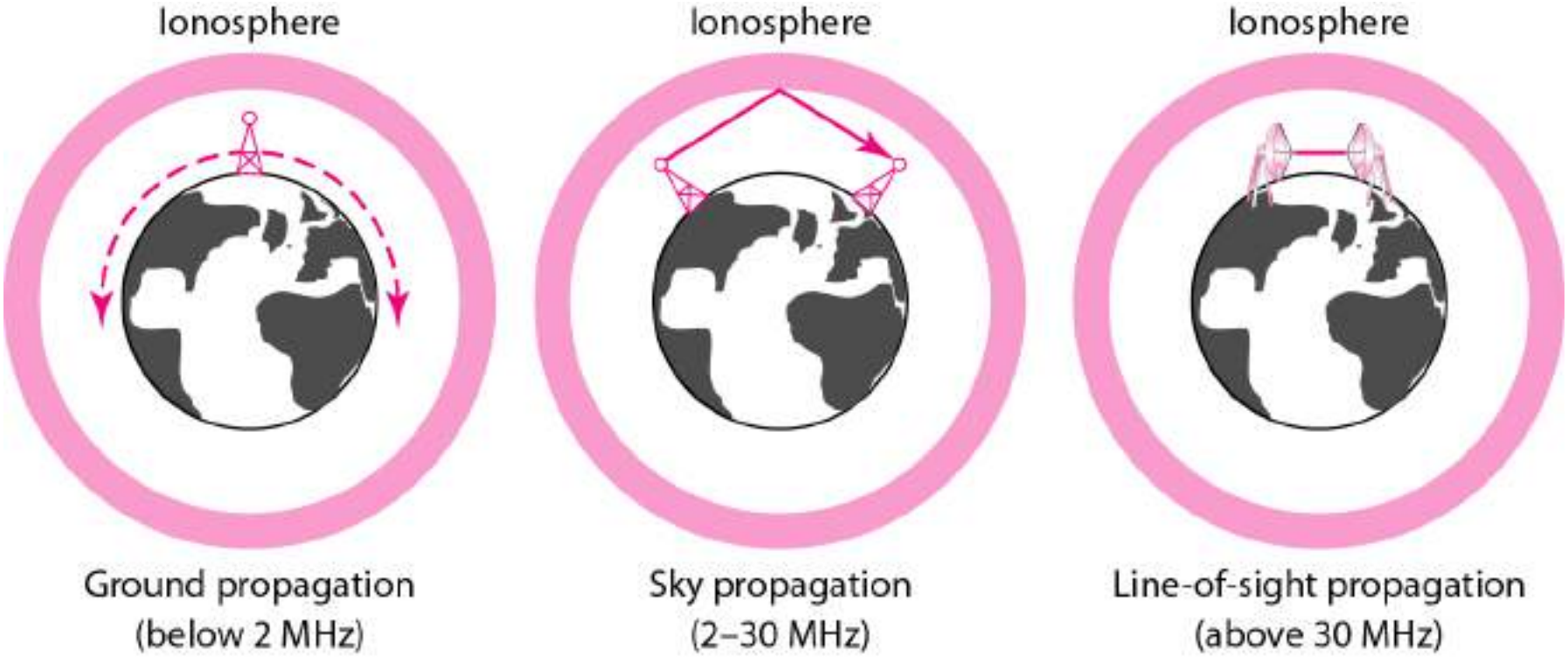
MT-RJ connector

- Advantages
  - Very high data rate, low error rate.
  - Less signal weakening.
  - Higher bandwidth
  - Fiber optic cables are much lighter than copper cables.
  - Electro magnetic noise cannot affect fiber optic cables.
- Disadvantages
  - High Initial cost
  - Maintenance and repairing cost.

Characteristics	UTP	STP	Coaxial Cables	Fiber Optic Cables
Bandwidth	10 Mbps - 100 Mbps	10 Mbps - 100 Mbps	10 Mbps	100 Mbps -1 Gbps
Maximum cable segment	100 meters	100 meters	200 - 500 meters	2 k.m. - 100 k.m.
Interference rating	Poor	Better than UTP	Better than Twisted Pair Cable	Very good as compared to any other cable
Installation cost	Cheap	Costly than UTP	Costlier than twisted pair wires	Costliest to install
Bend radius	360 degrees / feet	360 degrees / feet	360 degrees / feet or 30 degrees / feet	30 degrees / feet
Security	Low	Low	Low	High

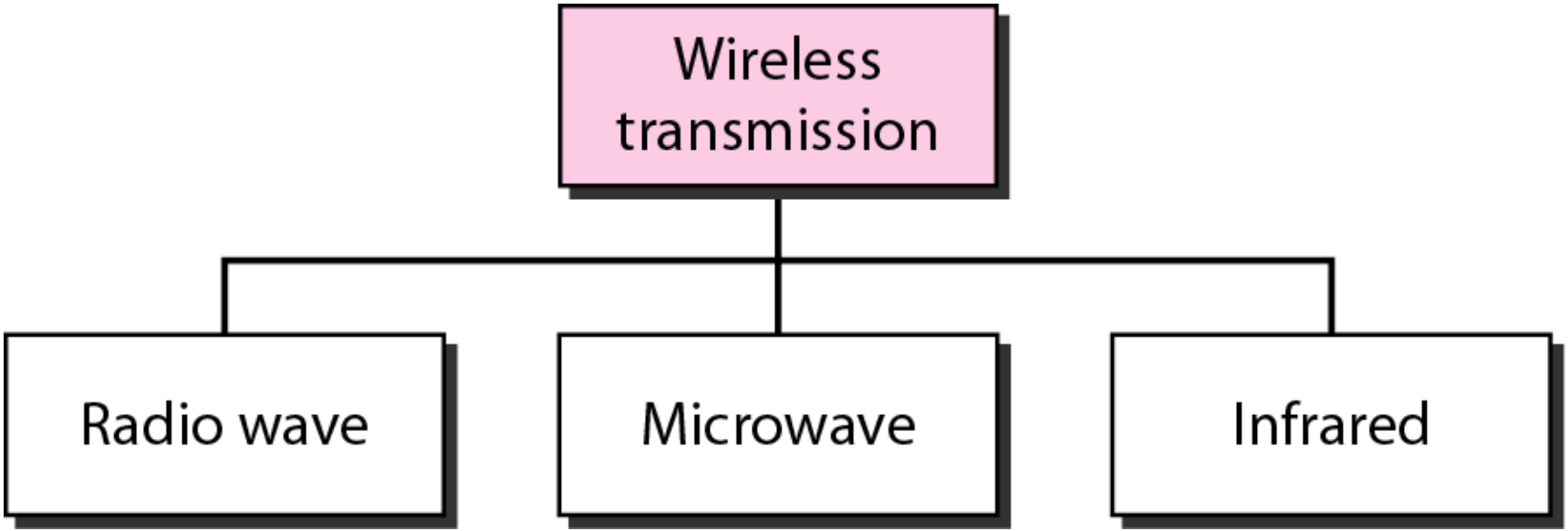
Wireless Transmission Media

- Wireless transmission is a form of unguided media.
- Wireless communication involves no physical link established between two or more devices, communicating wirelessly.
- Wireless Communication, signals can be propagation in three modes
  - Ground Propagation (below 2 MHz)
  - Sky propagation (2 MHz to 30 MHz)
  - Line of sight propagation (30 MHz)


Ionosphere
Ionosphere
Ionosphere
Ground propagation
(below 2 MHz)
Sky propagation
(2–30 MHz)
Line-of-sight propagation
(above 30 MHz)

- Wireless signals are spread over in the air and are received and interpreted by appropriate antennas.
- When an antenna is attached to electrical circuit of a computer or wireless device, it converts the digital data into wireless signals and spread all over within its frequency range.
- The receptor on the other end receives these signals and converts them back to digital data.

Band	*Range*	*Propagation*	*Application*
VLF (very low frequency)	3–30 kHz	Ground	Long-range radio navigation
LF (low frequency)	30–300 kHz	Ground	Radio beacons and navigational locators
MF (middle frequency)	300 kHz–3 MHz	Sky	AM radio
HF (high frequency)	3–30 MHz	Sky	Citizens band (CB), ship/aircraft communication
VHF (very high frequency)	30–300 MHz	Sky and line-of-sight	VHF TV, FM radio
UHF (ultrahigh frequency)	300 MHz–3 GHz	Line-of-sight	UHF TV, cellular phones, paging, satellite
SHF (superhigh frequency)	3–30 GHz	Line-of-sight	Satellite communication
EHF (extremely high frequency)	30–300 GHz	Line-of-sight	Radar, satellite


Wireless transmission
Radio wave
Microwave
Infrared

Radio Waves

- Radio waves are used for multicast communications, such as radio and television, and paging systems.
- They can penetrate through walls.
- Highly regulated.
- Use omni directional antennas
- Frequency range: 10kHz to 1 GHz.

Omnidirectional antenna

- Radio frequency is easier to generate and because of its large wavelength it can penetrate through walls and structures alike.
- Radio waves can have wavelength from 1 mm – 100,000 km.
- Radio waves at lower frequencies can travel through walls whereas higher RF can travel in straight line and bounce back.
- The power of low frequency waves decreases sharply as they cover long distance.
- High frequency radio waves have more power.
- Lower frequencies such as VLF, LF, MF bands can travel on the ground up to 1000 kilometers, over the earth's surface.

- Radio waves of high frequencies are prone to be absorbed by rain and other obstacles. They use Ionosphere of earth atmosphere. High frequency radio waves such as HF and VHF bands are spread upwards. When they reach Ionosphere, they are refracted back to the earth.

Characteristics

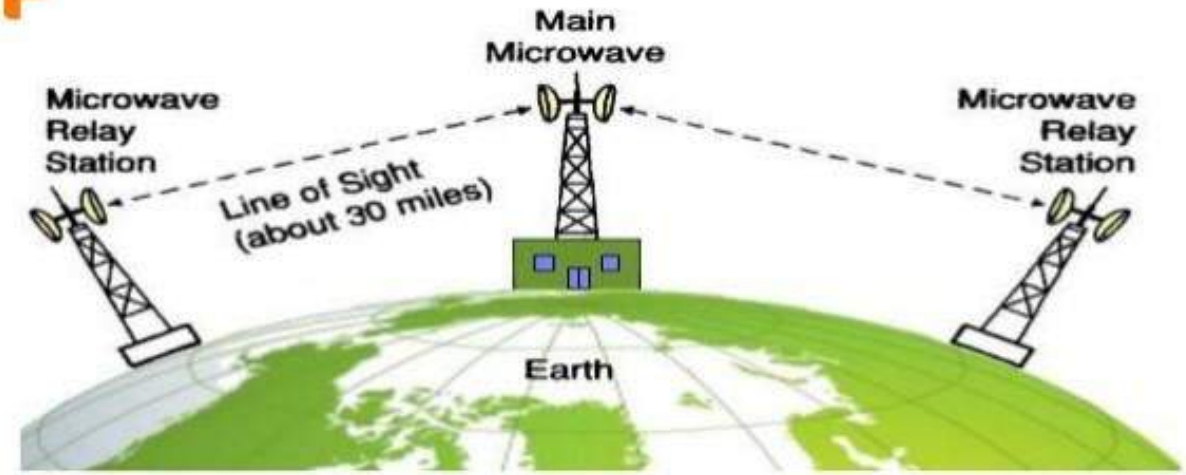
- Radio waves are easy to generate.
- They can travel long distances.
- Low frequency and medium frequency range cannot be used for data transfer because of their small band width.
- Radio waves are directional (they travel in all directions from source), so that the transmitter and receiver do not have be carefully aligned physically.

Microwave Transmission

- In the electromagnetic spectrum, waves within the frequencies 1GHz to 300GHz are called **microwaves**.
- Microwave signals propagate in one direction at a time, which means that two frequencies are necessary for two communication such as telephone conversation.
- One frequency is reserved for microware transmission in one direction and the other for transmission in the other direction.
- Each frequency requires its own transmitter and receiver.
- Nowadays, both pieces of equipment usually are combined in a single piece of equipment called a **Transceiver**, which allows a single antenna to serve both frequencies and functions.

- Microwave antennas use line of sight transmission, which means that to receive and transmit a signal, each antenna must be in sight of the next antenna.
- To increase the distance served by microwave, a system of repeaters can be installed with each antenna.
- A signal received by one antenna can be converted back into transmittable form and relayed to the next antenna.
- The Microwave band is relatively wide, almost 299 GHz. Therefore wider sub-bands can be assigned, and a high data rate is possible.
- Use of certain portions of the bands requires permission from authorities.
- Very high-frequency microwave cannot penetrate walls.

MICROWAVES TRANSMISSION



Microwave Relay Stations

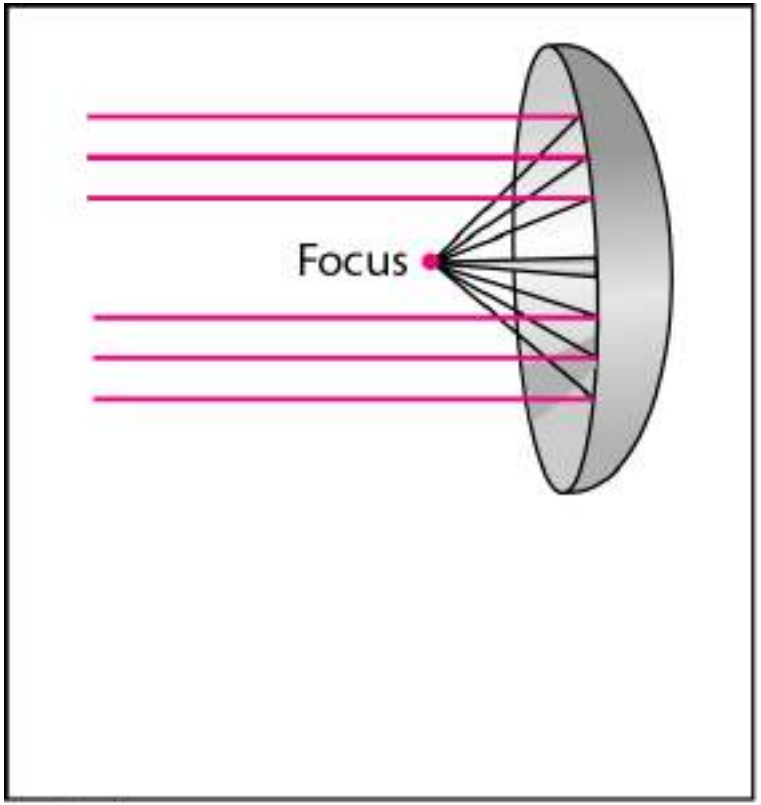
- Height of 40-50ft
- Spaced at least 20-30miles apart

Features of Microwaves

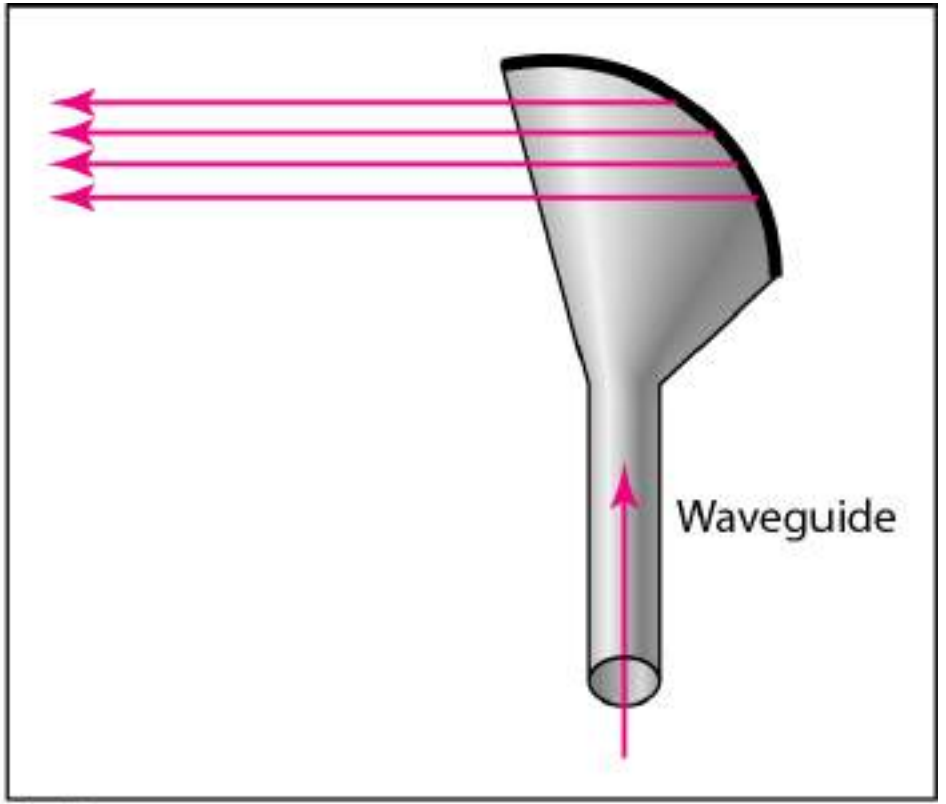
- Microwaves travel in straight lines, and so the transmitter and receiver stations should be accurately aligned to each other.
- Microwave propagation is line – of – sight propagation. So, towers hoisting the stations should be placed so that the curvature of the earth or any other obstacle does not interfere with the communication.
- Since it is unidirectional, it allows multiple receivers in a row to receive the signals without interference.
- Microwaves do not pass through buildings. So, indoor receivers cannot be used effectively.

- Microwaves are often refracted by the atmospheric layers. The refracted rays take longer time to reach the destination than the direct rays. This causes out of phase transmission, called multipath fading.
- Microwaves need unidirectional antennas to send out signals. Two types of antennas are needed −
  - **Parabolic Dish Antenna** − It is used by the receiving station. It is parabolic in shape, which concentrates all energy to a small beam thus achieving a strong signal with high SNR.
  - **Horn Antenna** − It has a stem with a curved head. In sending stations, outgoing waves from the stem are broadcast by the curved head as a series of parallel beams. In the receiving station, the rays are collected by the curved head and deflected in the stem.

- Microwave systems have the capacity to carry large quantities of data at high rates of speed.
- The data transmission rate is about 16 gbps (Gigabits per second). Also, microwave systems can carry 250,000 voice channels at the same time. They are used for the transmission of Radio, TV and telephone signals.



a. Dish antenna



b. Horn antenna

Standard gain horn antenna

Frequency Range :1.13GHz ~110GHz

Gain Type : 15dB ~ 30dB

Applications

- Long distance telephone communication
- Cellular phones
- Television networks
- Satellites
- Wireless LANs
- One to one communication.

Disadvantage

- Very costly
- Electromagnet waves cannot bend or pass through obstacles like mountains etc.
- Requires repeaters for long-distance transmission.
- Microwave signals are vulnerable to electromagnetic interference. Microwave systems are also affected by atmospheric conditions.
- This communication offers limited bandwidth.

Infrared Transmission

- Infrared waves are those between the frequencies 300GHz and 400THz in the electromagnetic spectrum.
- Their wavelengths are shorter than microwaves but longer than visible light.
- Infrared propagation is line of sight.
- They cannot penetrate walls and sun's infrared rays interfere with these rays. So cannot be used for long – range communication.
- As their usage is confined within closed space, they do not need any government permissions for their applications.

- The remote control used in TV, VCR, and stereos uses infrared communication.
- They are relatively directional, cheap and easy to build.
- Due to its short-range communication system, the use of an infrared communication system in one room will not be affected using another system in the next room.
- This is why using an infrared TV remote control in our home will not interfere with the use of our neighbor's infrared TV remote control.

Applications of Infrared Waves in Communications

- Remote controls for television, stereos and other home appliances.
- Wireless LANs
- Wireless modem, keyboard, mouse, printer etc
- Fire detectors
- Night vision systems
- Intrusion detection systems
- Motion detectors

Disadvantages

- Infrared signals cannot be used for long distance communication.
- In addition, we cannot use infrared waves outside a building because sun's rays contain infrared waves that can interfere with communication.
- Line of Sight:
- Blocked by common Materials
- Short Range.
- Light, weather sensitive.
- Speed.


Thank you

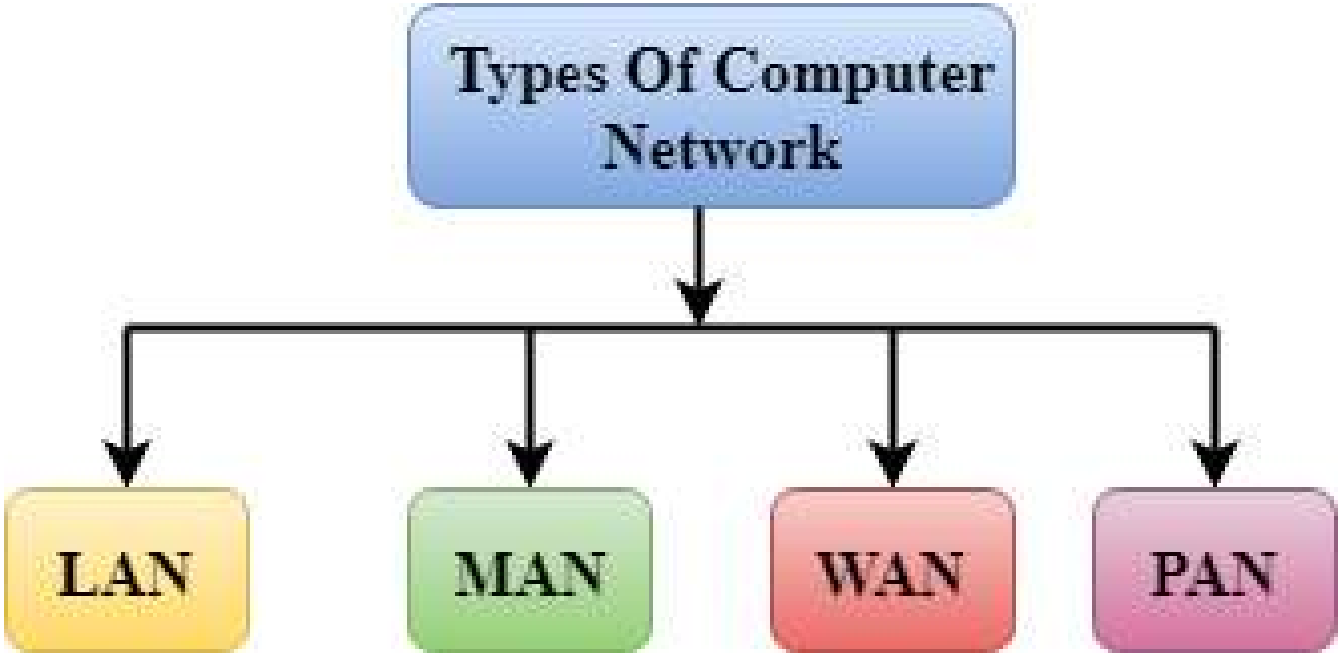
COMPUTER NETWORKS

Dr P.V. Praveen Sundar
Assistant Professor,
Department of Computer Science
Adhiparasakthi College of Arts & Science,
Kalavai.

Computer Networks

- A **Computer network** is a group of computers linked to each other that enables the computer to communicate with another computer and share their resources, data, and applications.
- **Communication Media:** is a physical path by which a message transfers from sender to receiver.
- **Access Devices:** A device that can accept transmitted data in network and can places data on the network.
- **Repeater:** A repeater is a device that accepts transmitted signals, amplifies them and put them back on network.

- **Protocol:** A protocol is a set of rules that control data communication.
- **Device driver:** A device driver is a hardware level program that controls a specific device.
- **Communication Software:** Communication software makes the available network bandwidth actually usable.


Types Of Computer Network
LAN
MAN
WAN
PAN

- A computer network can be categorized by their size. A computer network is mainly of four types:
  - PAN(Personal Area Network)
  - LAN(Local Area Network)
  - MAN(Metropolitan Area Network)
  - WAN(Wide Area Network)

PAN(Personal Area Network)

- Personal Area Network is a network arranged within an individual person, typically within a range of 10 meters.
- Personal Area Network is used for connecting the computer devices of personal use is known as Personal Area Network.
- **Thomas Zimmerman** was the first research scientist to bring the idea of the Personal Area Network.
- Personal Area Network covers an area of **30 feet**.
- Personal computer devices that are used to develop the personal area network are the laptop, mobile phones, media player and play stations.

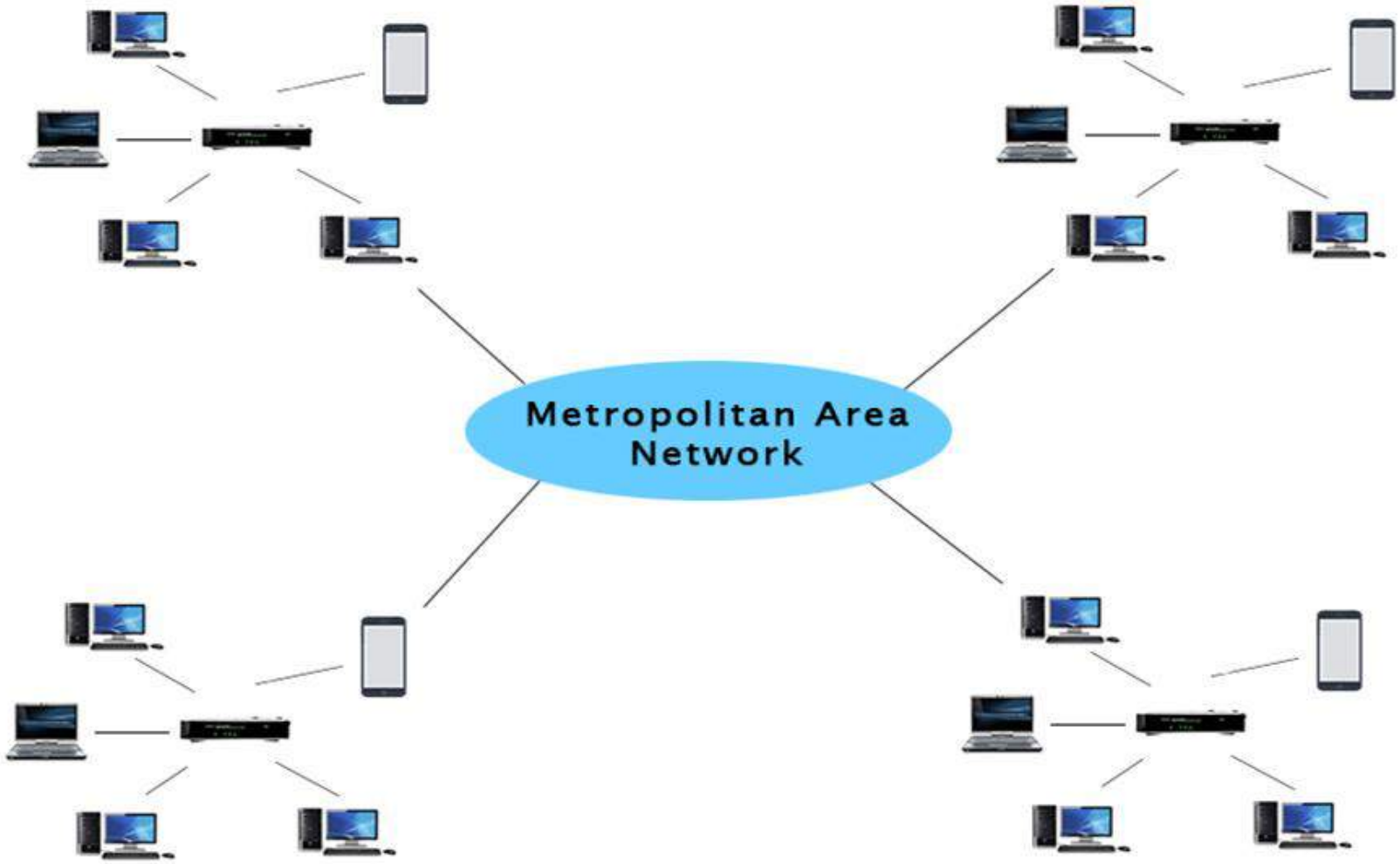
LAN(Local Area Network)

- Local Area Network is a group of computers connected to each other in a small area such as Home,building, office.
- LAN is used for connecting two or more personal computers through a communication medium such as twisted pair, coaxial cable, etc.
- It is less costly as it is built with inexpensive hardware such as hubs, network adapters, and ethernet cables.
- The data is transferred at an extremely faster rate in Local Area Network.
- Local Area Network provides higher security.


LAN

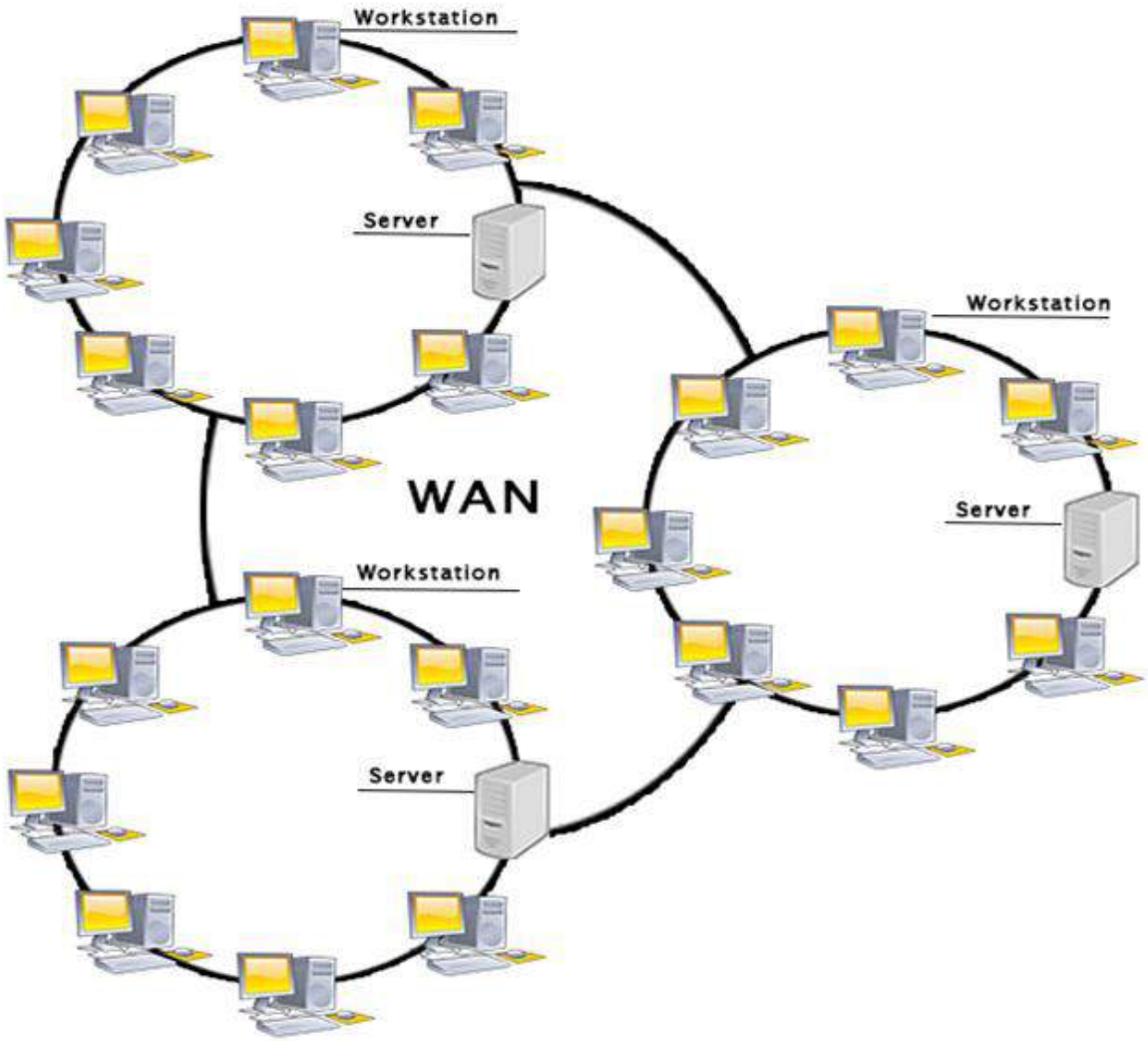
MAN(Metropolitan Area Network)

- A metropolitan area network is a network that covers a larger geographic area by interconnecting a different LAN to form a larger network.
- Government agencies use MAN to connect to the citizens and private industries.
- In MAN, various LANs are connected to each other through a telephone exchange line.
- It has a higher range than Local Area Network(LAN).
- Cable Television network is the best example for MAN.


Metropolitan Area
Network

WAN(Wide Area Network)

- A Wide Area Network is a network that extends over a large geographical area such as states or countries.
- A Wide Area Network is quite bigger network than the LAN.
- A Wide Area Network is not limited to a single location, but it spans over a large geographical area through a telephone line, fibre optic cable or satellite links.
- The internet is one of the biggest WAN in the world.
- A Wide Area Network is widely used in the field of Business, government, and education.


Workstation
Server
WAN
Workstation
Server
Workstation
Server

Advantages of WAN

- **Geographical area:** A Wide Area Network provides a large geographical area. Suppose if the branch of our office is in a different city then we can connect with them through WAN. The internet provides a leased line through which we can connect with another branch.
- **Centralized data:** In case of WAN network, data is centralized. Therefore, we do not need to buy the emails, files or back up servers.
- **Get updated files:** Software companies work on the live server. Therefore, the programmers get the updated files within seconds.

Advantages

- ✓ **Exchange messages:** In a WAN network, messages are transmitted fast. The web application like Facebook, Whatsapp, Skype allows you to communicate with friends.
- ✓ **Sharing of software and resources:** In WAN network, we can share the software and other resources like a hard drive, RAM.
- ✓ **Global business:** We can do the business over the internet globally.
- ✓ **High bandwidth:** If we use the leased lines for our company then this gives the high bandwidth. The high bandwidth increases the data transfer rate which in turn increases the productivity of our company.

Disadvantages

- **Security issue:** A WAN network has more security issues as compared to LAN and MAN network as all the technologies are combined together that creates the security problem.
- **Needs Firewall & antivirus software:** The data is transferred on the internet which can be changed or hacked by the hackers, so the firewall needs to be used. Some people can inject the virus in our system so antivirus is needed to protect from such a virus.
- **High Setup cost:** An installation cost of the WAN network is high as it involves the purchasing of routers, switches.
- **Troubleshooting problems:** It covers a large area so fixing the problem is difficult.

Internetwork

- An internetwork is defined as two or more computer network LANs or WAN or computer network segments are connected using devices, and they are configured by a local addressing scheme. This process is known as internetworking.
- An interconnection between public, private, commercial, industrial, or government computer networks can also be defined as internetworking.
- An internetworking uses the internet protocol.

LAN	MAN	WAN
Local Area Network is a group of computers connected to each other in a small area.	Metropolitan Area Network is a larger network of computers and other network devices which are connected together usually spans several buildings.	A Wide Area Network is a network that extends over a large geographical area such as states or countries.
LAN has very high speed	Slow compared to LAN	Various based on geographical location of the servers
Speeds can be 10mbps to 1000 mbps	Speed can be 10 or 100 Mbps	Speed can be 10 or 100 Mbps
Uses Guided Media	Uses Guided or Unguided Media	Uses Guided or Unguided Media

COMMUNICATION SATELLITES

Dr P.V. Praveen Sundar
Assistant Professor,
Department of Computer Science
Adhiparasakthi College of Arts & Science,
Kalavai.

19-08-2020

III BBA

Satellite Transmission

- A **Satellite** is a smaller object that revolves around a larger object in space. For example, moon is a natural satellite of earth.
- **Communication** refers to the exchange (sharing) of information between two or more entities, through any medium or channel.
- If the communication takes place between any two earth stations through a satellite, then it is called as **satellite communication**.
- In this communication, electromagnetic waves are used as carrier signals. These signals carry the information such as voice, audio, video or any other data between ground and space and vice-versa.

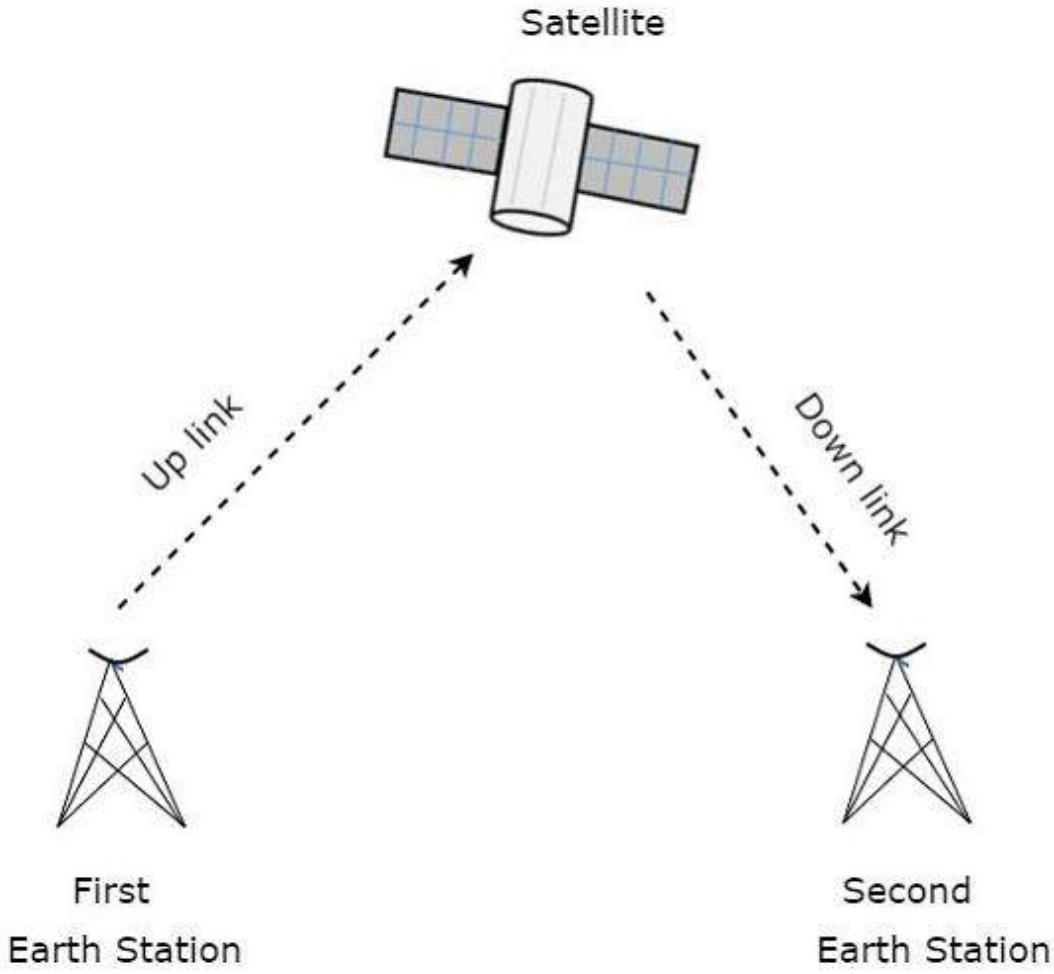
- Satellite Transmission is used to transmit and receive signals from ground station.
- The purpose of satellite communication is to use it for video transmission and sharing.
- Satellite is a device which revolves the earth either for collecting useful information or helping transfer of information.

Need of Satellite Communication

- The following two kinds of propagation are used earlier for communication up to some distance.
  - **Ground wave propagation** – Ground wave propagation is suitable for frequencies up to 30MHz. This method of communication makes use of the troposphere conditions of the earth.
  - **Sky wave propagation** – The suitable bandwidth for this type of communication is broadly between 30–40 MHz and it makes use of the ionosphere properties of the earth.
- The maximum hop or the station distance is limited to 1500KM only in both ground wave propagation and sky wave propagation.
- Satellite communication overcomes this limitation. In this method, satellites provide **communication for long distances,** which is well beyond the line of sight.

Satellite Works

- A **satellite** is a body that moves around another body in a particular path. A communication satellite is nothing but a microwave repeater station in space. It is helpful in telecommunications, radio and television along with internet applications.
- A **repeater** is a circuit, which increases the strength of the received signal and then transmits it. But, this repeater works as a **transponder**. That means, it changes the frequency band of the transmitted signal from the received one.
- The frequency with which, the signal is sent into the space is called as **Uplink frequency**. Similarly, the frequency with which, the signal is sent by the transponder is called as **Downlink frequency**.


Satellite
Up link
Down link
First
Earth Station
Second
Earth Station

Advantages

- Area of coverage is more than that of terrestrial systems
- Each and every corner of the earth can be covered
- Transmission cost is independent of coverage area
- More bandwidth and broadcasting possibilities

Disadvantages

- Launching of satellites into orbits is a costly process.
- Propagation delay of satellite systems is more than that of conventional terrestrial systems.
- Difficult to provide repairing activities if any problem occurs in a satellite system.
- Free space loss is more
- There can be congestion of frequencies.

Applications of Satellite Communication

Satellite communication plays a vital role in our daily life. Following are the applications of satellite communication −

- Radio broadcasting and voice communications
- TV broadcasting such as Direct To Home (DTH)
- Internet applications such as providing Internet connection for data transfer, GPS applications, Internet surfing, etc.
- Military applications and navigations
- Remote sensing applications
- Weather condition monitoring & Forecasting

- An orbit is the curved path that an object in space (such as a star, planet, moon, asteroid or spacecraft) takes around another object due to gravity.
- The orbits, which are assigned to satellites with respect to earth are called as **Earth Orbits**. The satellites present in those orbits are called as **Earth Orbit Satellites**.
- We should choose an orbit properly for a satellite based on the requirement. For example, if the satellite is placed in **lower orbit**, then it takes less time to travel around the earth.
- Similarly, if the satellite is placed in **higher orbit**, then it takes more time to travel around the earth and it covers more earth's surface at one time.

Types of Satellites (Based on Orbits)

- Geo-synchronous Earth Orbit (GEO): These Satellites are in orbit 35,863 Km above the earth's surface.
- Objects in geostationary orbit revolve around the earth at the same speed as the earth rotates.
- GEO satellites remain in the same position relative to the surface of earth.
- GEO Satellites are **used to** provide visible and infrared images of Earth's surface and atmosphere for weather observation, oceanography, and atmospheric tracking.

- The **advantage** of Geostationary orbit is that no need to track the antennas in order to find the position of satellites.
- Geostationary Earth Orbit Satellites are used for weather forecasting, satellite TV, satellite radio and other types of global communications.
- Satellites in GEO cover a large range of Earth so as few as three equally-spaced satellites can provide near global coverage.

Low Earth Orbit (LEO):

- LEO **satellites orbit** between 1500 and 200 kilometers above the **earth.**
- LEO **satellites** are commonly **used** for communications, military reconnaissance, spying and other imaging applications.
- LEO satellites do not always have to follow a particular path around Earth in the same way.
- It is also the orbit used for the International Space Station (ISS).

- Satellites in this orbit travel at a speed of around 7.8 km per second; at this speed, a satellite takes approximately 90 minutes to circle Earth, meaning the ISS travels around Earth about 16 times a day.

Medium Earth orbit (MEO)

- Medium Earth orbit comprises a wide range of orbits anywhere between LEO and GEO.
- It is similar to LEO in that it also does not need to take specific paths around Earth, and it is used by a variety of satellites with many different applications.
- Orbit period: 2 to 8 hours
- Orbit height from Earth: 5000 to 12000 Km
- Life of satellite in the orbit: Long
- Propagation loss in the orbit: High
- Number of satellites to cover entire regions on Earth: 8 to 20

Comparison of LEO,GEO and MEO

Parameter	LEO	MEO	GEO
Satellite Height	500-1500 Km	5000-12000 Km	35,800 KM
Orbital Period	10-40 minutes	2-8 Hours	24 Hours
Number of Satellites	40-80	8-20	3
Satellite Life	Short	Long	Long
Gateway Cost	Very Expensive	Expensive	Cheap
Propagation Loss	Least	High	Highest

WIRELESS NETWORKS

Dr P.V. Praveen Sundar
Assistant Professor,
Department of Computer Science
Adhiparasakthi College of Arts & Science,
Kalavai.

Wireless Networks

- Wireless is a term used to describe telecommunications in which electromagnetic waves carry the signal over part of all the communication path.
- Wireless network refers to two or more computers communicating using standard network rules or protocols, without use of cabling to connect the computers together.
- They use wireless radio signals to send information from one to the other.

- A wireless local area network consists of two key components: An Access Point (base station) and a wireless card.
- Information can be transmitted between these two components as long as the are fairly close together. (up to 100 meters indoors or 350 meters outdoors).
- Wireless Networks can be divided into following categories.
  - System interconnection.
  - Wireless LAN's
  - Wireless WAN's

System Interconnection

- System Interconnection is all about interconnecting the components of a computer using short range radio.
- Almost every computer has monitor, keyboard, mouse and printer connected to the main unit by cables.
- Some companies uses wireless Bluetooth to allows digital cameras, headsets, scanners and printers within a range.

Wireless LAN

- A Wireless Local Area Network (WLAN's) links two or more devices using wireless distribution methods and providing a connection through an access point to the wider internet.
- This gives users the mobility to move around within a local coverage area and still be connected to the network.
- Wireless have become popular in the home due to the ease of installation and increasing popularity of laptop computers.
- Public business such as coffee shops and malls offer wireless access to their customers for free.

WPAN's

- Wireless Personal Area Networks: The two current technologies for wireless personal area networks are Infrared (IR) and Bluetooth (IEEE 802.15).
- These will allow the connectivity of personal devices with an area of about 30 feet.
- However, IR requires a direct line of site and the range is less.

WWAN's

- Wireless Wide Area Networks: These types of networks can be maintained over large areas, such as cites or countries.
- Wireless WAN's are created through the use of mobile phone signals typically maintained by specific mobile phone(cellular) service providers.
- WWAN's can provide a way to stay connected even when away from other forms of network access.

Advantages

- It is easier to add or move workstations.
- It is easier to provide connectivity in areas where it is difficult to lay cable.
- Installation can be fast and easy and can eliminate the need to pull cable through walls and ceilings.
- Access to the network can be from anywhere within range of an access point.
- Portable or semi permanent buildings can be connected using wireless LAN.

Disadvantages

- As the number of computers using the network increases, the data transfer rate to each computer will decrease accordingly.
- As standards change, it maybe necessary to replace wireless cards or access points.
- Lower wireless bandwidth means some applications such as video streaming will be more effective on a wired LAN.
- Security is more difficult to guarantee, and requires configuration.
- Devices will only operate at a limited distance from an access point. With the distance determined by the standard used buildings and other obstacles between the access point and the user.

Wireless Internet Access

- Wireless internet access requires attaching a special radio modem to the laptop.
- The main types of internet connectivity as follows;
  - Dialup Connection
  - ISDN Connection
  - Broadband Connection
  - WiFi

Dialup Connection

- Dial up modem connections also called as intermittent connections.
- These connections are the most common type of internet connection.
- Dialup modems are popular among individuals and small to mid sized organizations because they are inexpensive and easy to install and maintain.
- Dialup connection requires the use of a modem and a phone line to dial into an Internet Service Provider (ISP)node.

- The data transmission rate is usually 56 kbps or less.
- Dialup internet access was very popular in the past but now it is replaced by Broad band internet services.

Advantages

- Dialup connection is available with everyone with computer and modem.
- Only choice for rural and remote areas where broadband connection is not available.
- Low cost (Rs 500 Month)
- Easy setup.

Disadvantages

- While using internet, if call is receiving means then internet connection is disconnected.
- Additional cost
- Data transmission rate is rather low. With the rate of 56 Kbps or less.

ISDN Connection

- ISDN Stands for Integrated Service Digital Network.
- ISDN connection is one of the widely used internet options in the global market.
- ISDN is a circuit-switched telephone network system, which also provides access to packet switched networks, designed to allow digital transmission of voice and data over ordinary telephone copper wires, resulting in potentially better voice quality than an analog phone can provide.

- It offers circuit-switched connections (for either voice or data), and packet-switched connections (for data), in increments of 64 kilobit/s.
- In ISDN Connection, the information which is sent from computer to internet is digital.
- ISDN Lines requires power from outside. when there is a shutdown, ISDN lines will not work.
- The main feature of ISDN is that it can integrate speech and data on the same lines, which were not available in the classic telephone system.

- The ISDN standards define several kinds of access interfaces, such as Basic Rate Interface (BRI), Primary Rate Interface (PRI.
- BRI is the lower tier of service. It only provides basic needs at a lower cost.
- PRI is the main service. It provides a better connection, more reliable service, and faster speeds.

Basic Rate Interface (BRI)

- There are two data-bearing channels ('B' channels) and one signaling channel ('D' channel) in BRI to initiate connections.
- The B channels operate at a maximum of 64 Kbps while the D channel operates at a maximum of 16 Kbps.
- The two channels are independent of each other. For example, one channel is used as a TCP/IP connection to a location while the other channel is used to send a fax to a remote location.

- The BRI configuration provides 2 data (bearer) channels (B channels) at 64 kilo bit/s each and 1 control (delta) channel (D channel) at 16 kilo bit/s.
- The B channels are used for voice or user data, and the D channel is used for any combination of data, control/signaling, and X.25 packet networking.
- The 2 B channels can be aggregated by channel bonding providing a total data rate of 128 kilo bit/s.
- The BRI ISDN service is commonly installed for residential or small business service in many countries.

Primary Rate Interface (PRI)

- PRI is the standard for providing telecommunication services to enterprises and offices.
- It is based on T-carrier (T1) transmission in the US, Canada, and Japan, while the E-carrier (E1) is common in Europe and Australia.
- The T1 line consists of 23 bearer (B) channels and one data (D) channel for control purposes, for a total bandwidth of 24x64-kbit/s or 1.544 Mbit/s.
- The E1 carrier provides 30 B- and one D-channel for a bandwidth of 2.048 Mbit/s.

- Larger connections are possible using PRI pairing.
- A dual T1-PRI could have 24 + 23 = 47 B-channels and 1 D-channel (often called "47B + D"), but more commonly has 46 B-channels and 2 D-channels thus providing a backup signaling channel.

- Both PRI and BRI ISDN use B channels for sending data and D channels for other forms of communication. The difference lies in the number of channels they use to accomplish this.
- For instance, BRI uses only two B channels and one D channel. It has a maximum speed of **128 kbps.**
- PRI varies in the number of channels it uses given its location. It can be adjusted for speeds up to 2.94 Mbps.

- Bharat Sanchar Nigam Limited, Reliance Communications and Bharti Airtel are the largest communication service providers and offer both ISDN BRI and PRI services across the country.
- Reliance Communications and Bharti Airtel uses the Digital Loop Carrier technology for providing these services.
- With the introduction of broadband technology, ISDN continues to be an important backup network for point-to-point leased line customers such as banks, E-seva Centers, Life Insurance Corporation of India, and SBI ATMs.

Narrowband ISDN

- The Narrowband Integrated Services Digital Network is called the N-ISDN.
- This can be understood as a telecommunication that carries voice information in a narrow band of frequencies.
- This is an attempt to digitize the analog voice information. This uses 64kbps circuit switching.
- The narrowband ISDN is implemented to carry voice data, which uses lesser bandwidth, on a limited number of frequencies.

Advantages and Disadvantages of ISDN

ISDN is a telephone network-based infrastructure, which enables the transmission of both voice and data simultaneously. There are many advantages of ISDN such as −

- ✓ As the services are digital, there is less chance for errors.
- ✓ The connection is faster.
- ✓ The bandwidth is higher.
- ✓ Voice, data and video − all of these can be sent over a single ISDN line.

The disadvantage of ISDN is that it requires specialized digital services and is costlier.

ISDN Services

- ISDN supports a variety of services. A few of them are listed below −
  - Facsimile
  - Electronic Mail
  - Electronic Fund transfer
  - Image and graphics exchange
  - Document storage and transfer
  - Audio and Video Conferencing

Broadband

- Broadband Internet (High-speed Internet) is an internet connection offering high data transmission rate of 256 kbps or more.
- Broadband communication can handle voice, data and video information's.
- Data transmission rates of broadband internet access varies greatly from 256 kbps to 24 Mbps depending on the internet service providers and their service plans.
- The actual transmission rate is also affected by other factors such as number of subscribers sharing the bandwidth and the distance from service station.

- The broadband communication is usually made using the fiber optic cables.
- As the speed is greater than 1.544 Mbps, the communications based on this are called Broadband Communications.
- The broadband services provide a continuous flow of information, which is distributed from a central source to an unlimited number of authorized receivers connected to the network.

- The most popular broadband technologies for home users are DSL and cable internet.
- Digital Subscriber Line (DSL) is a wireline transmission technology that transmits data faster over traditional copper telephone lines already installed to homes and businesses.
- DSL-based broadband provides transmission speeds ranging from several hundred Kbps to millions of bits per second (Mbps).
- The availability and speed of your DSL service may depend on the distance from your home or business to the closest telephone company facility.

The following are types of DSL transmission technologies:

- **Asymmetrical Digital Subscriber Line (ADSL) –** Used primarily by residential customers, such as Internet surfers.
- ADSL typically provides faster speed in the downstream direction than the upstream direction.
- ADSL allows faster downstream data transmission over the same line used to provide voice service, without disrupting regular telephone calls on that line.
- **Symmetrical Digital Subscriber Line (SDSL) –** Used typically by businesses for services such as video conferencing, which need significant bandwidth both upstream and downstream.

Cable Connections

- Cable internet refers to the delivery of internet service over cable network.
- A cable modem is used to transfer data signal using unused bandwidth on a cable television network.
- Cable internet is capable of providing higher connection speed than DSL internet service.
- The Download speed can reach up to 30 mbps and the upload speed upto 2 mbps.
- Subscribers can access their cable modem service by simply turning on their computers, without dialing-up an ISP.
- We can still watch cable TV while using it. Transmission speeds vary depending on the type of cable modem, cable network, and traffic load. Speeds are comparable to DSL

Fiber optic

- Fiber optic technology converts electrical signals carrying data to light and sends the light through transparent glass fibers about the diameter of a human hair.
- Fiber transmits data at speeds far exceeding current DSL or cable modem speeds, typically by tens or even hundreds of Mbps.
- The actual speed you experience will vary depending on a variety of factors, such as how close to your computer the service provider brings the fiber and how the service provider configures the service, including the amount of bandwidth used.

- The same fiber providing your broadband can also simultaneously deliver voice (VoIP) and video services, including video-on-demand.
- Telecommunications providers sometimes offer fiber broadband in limited areas and have announced plans to expand their fiber networks and offer bundled voice, Internet access, and video services.
- Variations of the technology run the fiber all the way to the customer's home or business, to the curb outside, or to a location somewhere between the provider's facilities and the customer.

Advantages of Broadband

- Connection speed is up to 100 times faster than dialup connection.
- It does not affect phone line.
- It is convenient because the internet connection is always on.
- Don't need to dial an access number and risk getting busy signal.
- Broadband offers unlimited access and wont charged extra.
- Broadband not only gives high speed internet also provide cheap phone services via VoIP technology.

Disadvantages

- Highly monthly fee compared to dialup access
- High security risk than dialup connection. A personal firewall needed to protect our computer.
- Not all phone wires are equipped to DSL service. May not be available in rural or remote areas.
- Not all cable tv networks are equipped to cable internet access. May not be available in rural or remote areas.

Wireless

- Wireless broadband connects a home or business to the Internet using a radio link between the customer's location and the service provider's facility.
- Wireless broadband can be mobile or fixed.
- Wireless technologies using longer-range directional equipment provide broadband service in remote or sparsely populated areas where DSL or cable modem service would be costly to provide.
- Speeds are generally comparable to DSL and cable modem.

- An external antenna is usually required.
- WiFi is the leading wireless technology based on the IEEE 802.11specifications.
- It allows a person with WiFi device, such as laptop or Personal Digital Assistant (PDA) to connect to the internet via access points (AP).
- The region covered by one or several access points are called as Hotspots.

- WiFi is useful for business travellers who need to get access to the internet in Café, hotels and airports.
- For Home users, a wireless routers can connect group of WiFi enabled devices to an adjacent wired network to establish home networking.
- Wireless internet service providers offer hotspot network in many locations.

- The users can get online with a broadband speed up to 100 times faster than dialup.
- Free WiFi networks are also available in restaurants, coffee shops, hotels, airports, convention centers, and city parks, but these open access points may pose great security risks to novice users.

Advantages

- A network can be setup without cabling or wiring.
- Economical networking solution
- Provide access to the internet in outdoor areas.
- Roaming is supported. A user can move from one access point to another.
- A large number of hotspots are available worldwide.

Disadvantages

- High power consumption rate for laptop computers.
- Wireless encryption standard is easy to break.
- WiFi network has limited range.
- Overlapping access points can interface signal transmissions.
- Subject to security risks, if wireless encryption is not enabled.
- Internet connection speed of wireless network is lower than the wired network.


Thank you

OSI MODELS

Dr P.V. Praveen Sundar
Assistant Professor,
Department of Computer Science
Adhiparasakthi College of Arts & Science,
Kalavai.

OSI Models

- OSI stands for Open System Interconnection is a reference model that describes how information from a software application in one computer moves through a physical medium to the software application in another computer.
- It has been developed by ISO – 'International Organization of Standardization', in the year 1984.
- OSI model divides the whole task into seven smaller and manageable tasks. Each layer is assigned a particular task.
- Each layer is self-contained, so that task assigned to each layer can be performed independently.

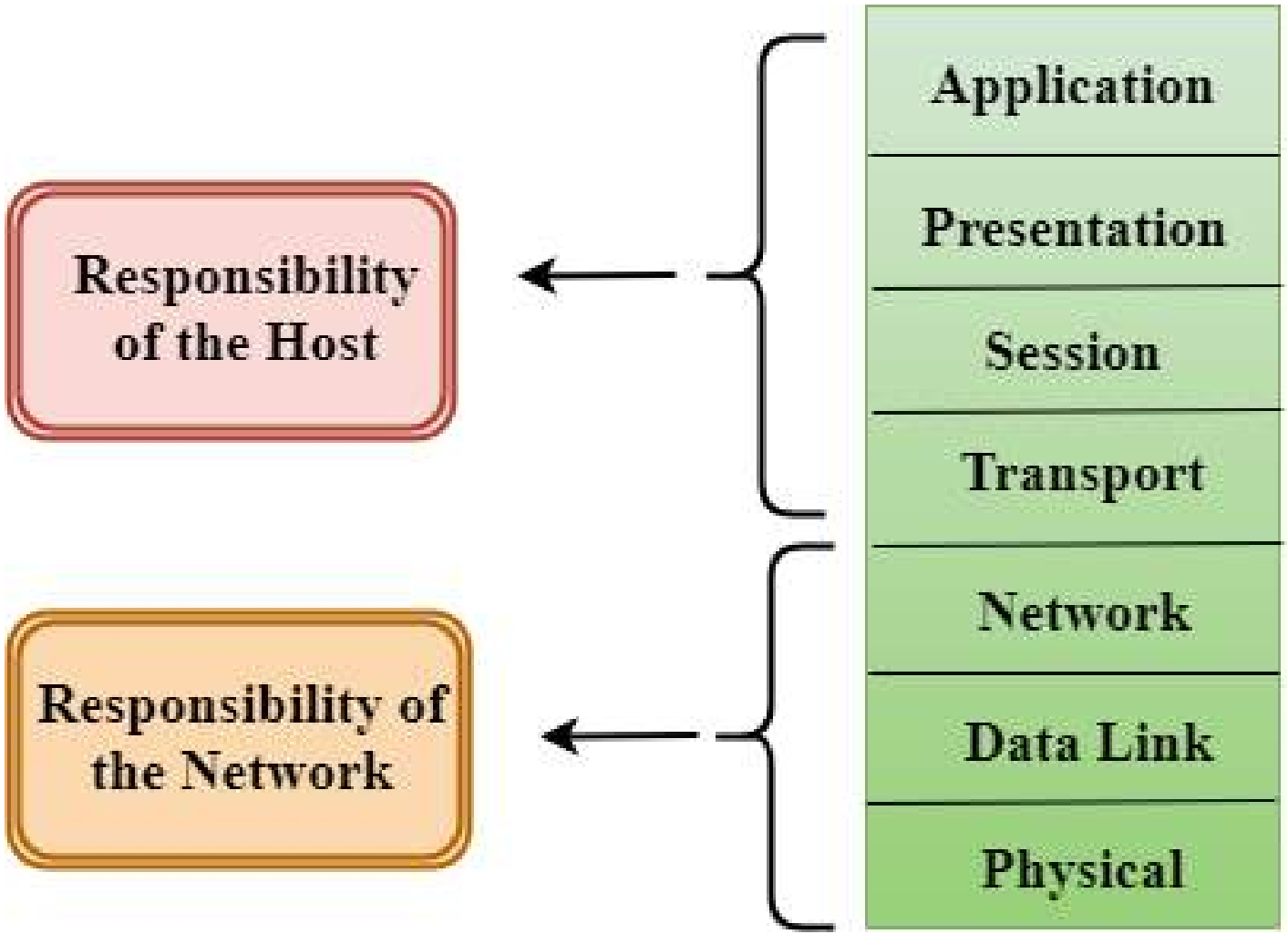
Seven Layers of OSI Model

1. Application Layer
2. Presentation Layer
3. Session Layer
4. Transport Layer
5. Network Layer
6. Data-Link Layer
7. Physical Layer

Characteristics of OSI Model:

- The OSI model is divided into two layers: upper layers and lower layers.
- The upper layer of the OSI model mainly deals with the application related issues, and they are implemented only in the software.
- The application layer is closest to the end user.
- Both the end user and the application layer interact with the software applications.

- The lower layer of the OSI model deals with the data transport issues.
- The data link layer and the physical layer are implemented in hardware and software.
- The physical layer is the lowest layer of the OSI model and is closest to the physical medium.
- The physical layer is mainly responsible for placing the information on the physical medium.


Application
Presentation
Session
Transport
Network
Data Link
Physical
Responsibility of the Host
Responsibility of the Network

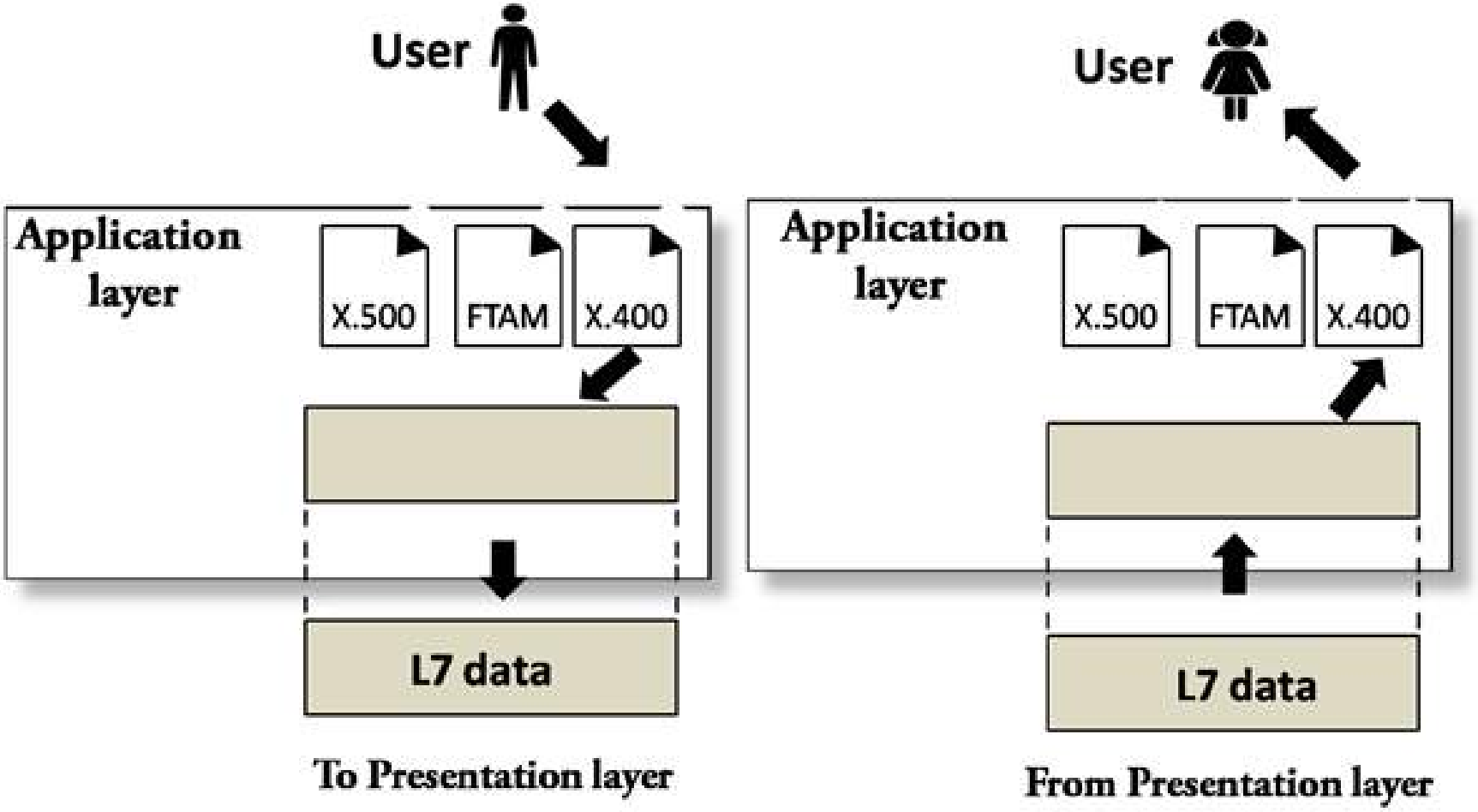
FUNCTIONS OF OSI LAYER

Application Layer

- An application layer serves as a window for users and application processes to access network services.
- It handles issues such as network transparency, resource allocation, etc.
- Network transparency is the situation in which an operating system or other service allows a user to access a resource (such as an application program or data) without the user needing to know, and usually not being aware of, whether the resource is located on the local machine.
- An application layer is not an application, but it performs the application layer functions. This layer provides the network services to the end-users.
- Ex: Application – Mails, Browsers, Skype Messenger etc.
- Protocols – HTTP, FTP, SMTP, SNMP, DNS etc.,

Functions of Application layer:

- **File Transfer, Access, and Management (FTAM):** An application layer allows a user to access the files in a remote computer, to retrieve the files from a computer and to manage the files in a remote computer.
- **Mail services:** An application layer provides the facility for email forwarding and storage.
- **Directory services:** An application provides the distributed database sources and is used to provide that global information about various objects.


User
Application layer
X.500
FTAM
X.400
L7 data
To Presentation layer
User
Application layer
X.500
FTAM
X.400
L7 data
From Presentation layer

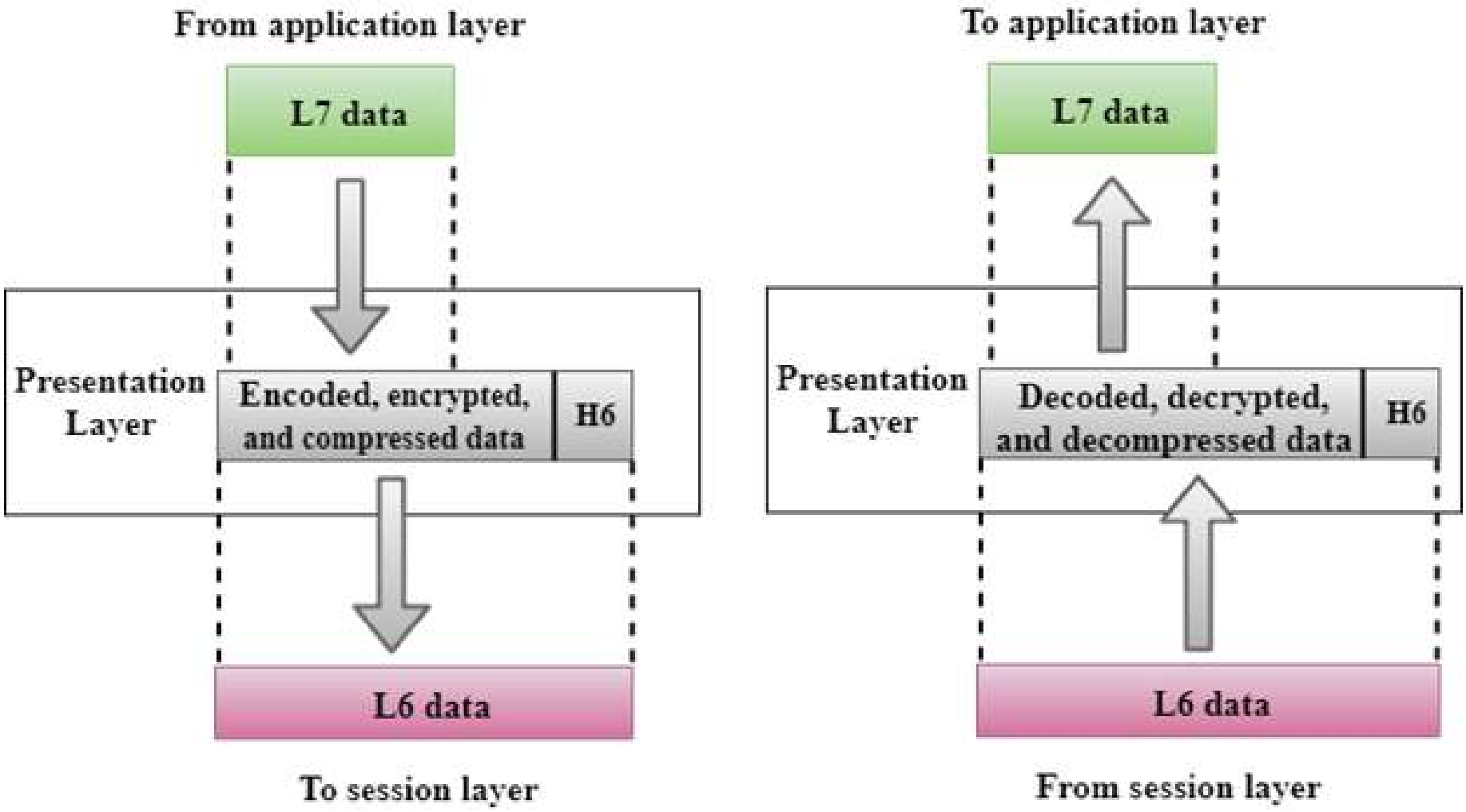
Presentation Layer

- A Presentation layer is mainly concerned with the syntax and semantics of the information exchanged between the two systems.
- It acts as a data translator for a network.
- This layer is a part of the operating system that converts the data from one presentation format to another format.
- The Presentation layer is also known as the syntax layer.

Functions

- **Translation:** The processes in two systems exchange the information in the form of character strings, numbers and so on.
- Different computers use different encoding methods, the presentation layer handles the interoperability between the different encoding methods.
- It converts the data from sender-dependent format into a common format and changes the common format into receiver-dependent format at the receiving end.

- **Encryption:** Encryption is needed to maintain privacy. Encryption is a process of converting the sender-transmitted information into another form and sends the resulting message over the network.
- **Compression:** Data compression is a process of compressing the data, i.e., it reduces the number of bits to be transmitted. Data compression is very important in multimedia such as text, audio, video.


From application layer
L7 data
Presentation Layer
Encoded, encrypted, and compressed data
H6
L6 data
To session layer
To application layer
L7 data
Presentation Layer
Decoded, decrypted, and decompressed data
H6
L6 data
From session layer

Session Layer

- This layer is responsible for establishment of connection, maintenance of sessions, authentication and ensures security.
- It can support message mode data transfer.
- It deals with session and connection coordination.

Functions

- **Session Management:** Divide the sessions into sub sessions by inserting checkpoints.
- **Synchronization:** Session layer adds some checkpoints when transmitting the data in a sequence. If some error occurs in the middle of the transmission of data, then the transmission will take place again from the checkpoint. This process is known as Synchronization and recovery.

- **Dialog control:** Session layer acts as a dialog controller that creates a dialog between two processes, or we can say that it allows the communication between two processes which can be either half-duplex or full-duplex.
- **Closing the session:** Ensures that the data transfer is completed before the session closes.

Transport Layer

- The Transport layer is a ensures that messages are transmitted in the order in which they are sent and there is no duplication of data.
- The main responsibility of the transport layer is to transfer the data completely.
- It receives the data from the upper layer and converts them into smaller units known as segments.
- This layer can be termed as an end-to-end layer as it provides a point-to-point connection between source and destination to deliver the data reliably.

Protocols used in this layer are:

Transmission Control Protocol

- ✓ It is a standard protocol that allows the systems to communicate over the internet.
- ✓ It establishes and maintains a connection between hosts.
- ✓ When data is sent over the TCP connection, then the TCP protocol divides the data into smaller units known as segments.
- ✓ Each segment travels over the internet using multiple routes, and they arrive in different orders at the destination. The transmission control protocol reorders the packets in the correct order at the receiving end.

User Datagram Protocol

- User Datagram Protocol is a transport layer protocol.
- It is an unreliable transport protocol as in this case receiver does not send any acknowledgment when the packet is received, the sender does not wait for any acknowledgment. Therefore, this makes a protocol unreliable.

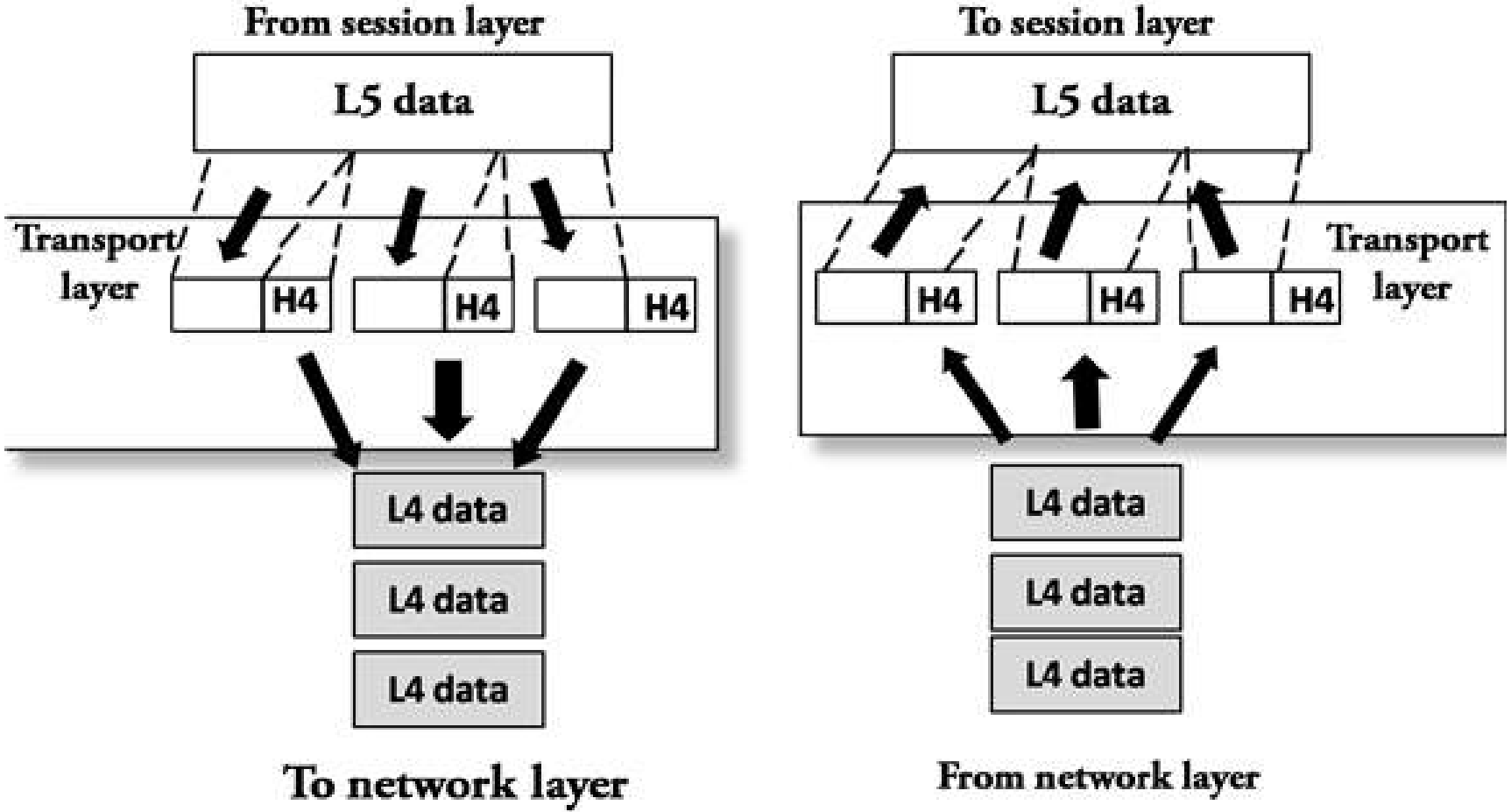
Functions

- **Service-point addressing:** Computers run several programs simultaneously due to this reason, the transmission of data from source to the destination not only from one computer to another computer but also from one process to another process.
- The transport layer adds the header that contains the address known as a service-point address or port address.
- The responsibility of the network layer is to transmit the data from one computer to another computer and the responsibility of the transport layer is to transmit the message to the correct process.

- **Segmentation and reassembly:** When the transport layer receives the message from the upper layer, it divides the message into multiple segments.
- Each segment is assigned with a sequence number that uniquely identifies each segment.
- When the message has arrived at the destination, then the transport layer reassembles the message based on their sequence numbers.

- **Connection control:** Transport layer provides two services Connection-oriented service and connectionless service.
- A connectionless service treats each segment as an individual packet, and they all travel in different routes to reach the destination.
- A connection-oriented service makes a connection with the transport layer at the destination machine before delivering the packets.
- In connection-oriented service, all the packets travel in the single route.

- **Error control:** The transport layer is also responsible for Error control.
- Error control is performed end-to-end rather than across the single link.
- The sender transport layer ensures that message reach at the destination without any error.


From session layer
L5 data
Transport layer
H4
H4
H4
L4 data
L4 data
L4 data
To network layer
To session layer
L5 data
Transport layer
H4
H4
H4
L4 data
L4 data
L4 data
From network layer

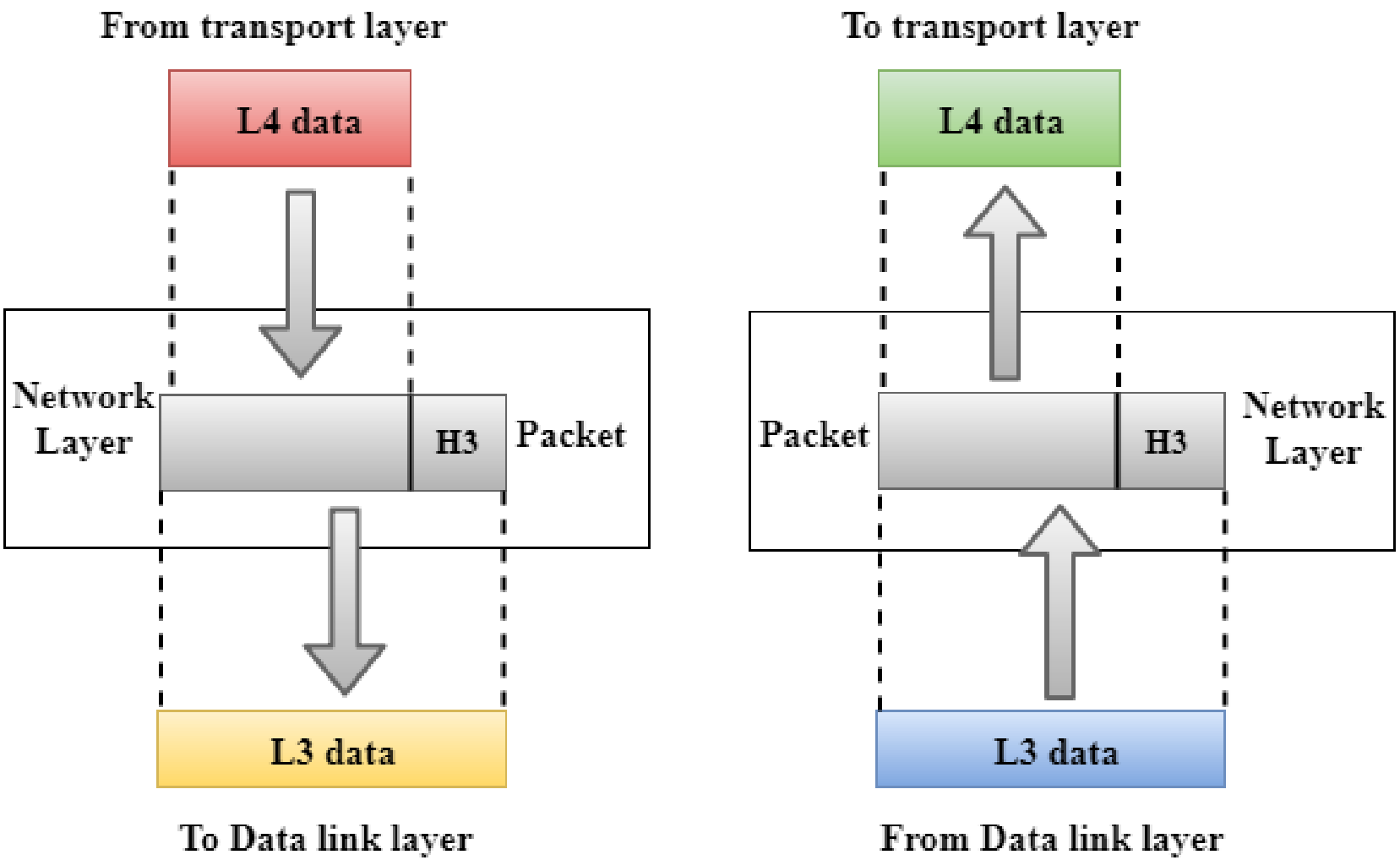
Network Layer

- Network layer manages device addressing, tracks the location of devices on the network.
- It determines the best path to move data from source to the destination based on the network conditions, the priority of service, and other factors.
- The Data link layer is responsible for routing and forwarding the packets.
- Routers specified in this layer and used to provide the routing services within an internetwork.
- The protocols used to route the network traffic are known as Network layer protocols. Examples of protocols are IP and Ipv6.

Functions

- **Internetworking:** An internetworking is the main responsibility of the network layer. It provides a logical connection between different devices.
- **Addressing:** A Network layer adds the source and destination address to the header of the frame. Addressing is used to identify the device on the internet.

- **Routing:** Routing is the major component of the network layer, and it determines the best optimal path out of the multiple paths from source to the destination.
- **Packetizing:** A Network Layer receives the packets from the upper layer and converts them into packets. This process is known as Packetizing. It is achieved by internet protocol (IP).


From transport layer
L4 data
Network Layer
H3
Packet
L3 data
To Data link layer
To transport layer
L4 data
Packet
H3
Network Layer
L3 data
From Data link layer

Data-Link Layer

- This layer is responsible for the error-free transfer of data frames.
- It defines the format of the data on the network.
- It provides a reliable and efficient communication between two or more devices.
- It is mainly responsible for the unique identification of each device that resides on a local network.
- Packet in Data Link layer is referred as Frame.
- Data Link layer is handled by the NIC (Network Interface Card) and device drivers of host machines.

- Switch & Bridge are Data Link Layer devices.

It contains two sub-layers:

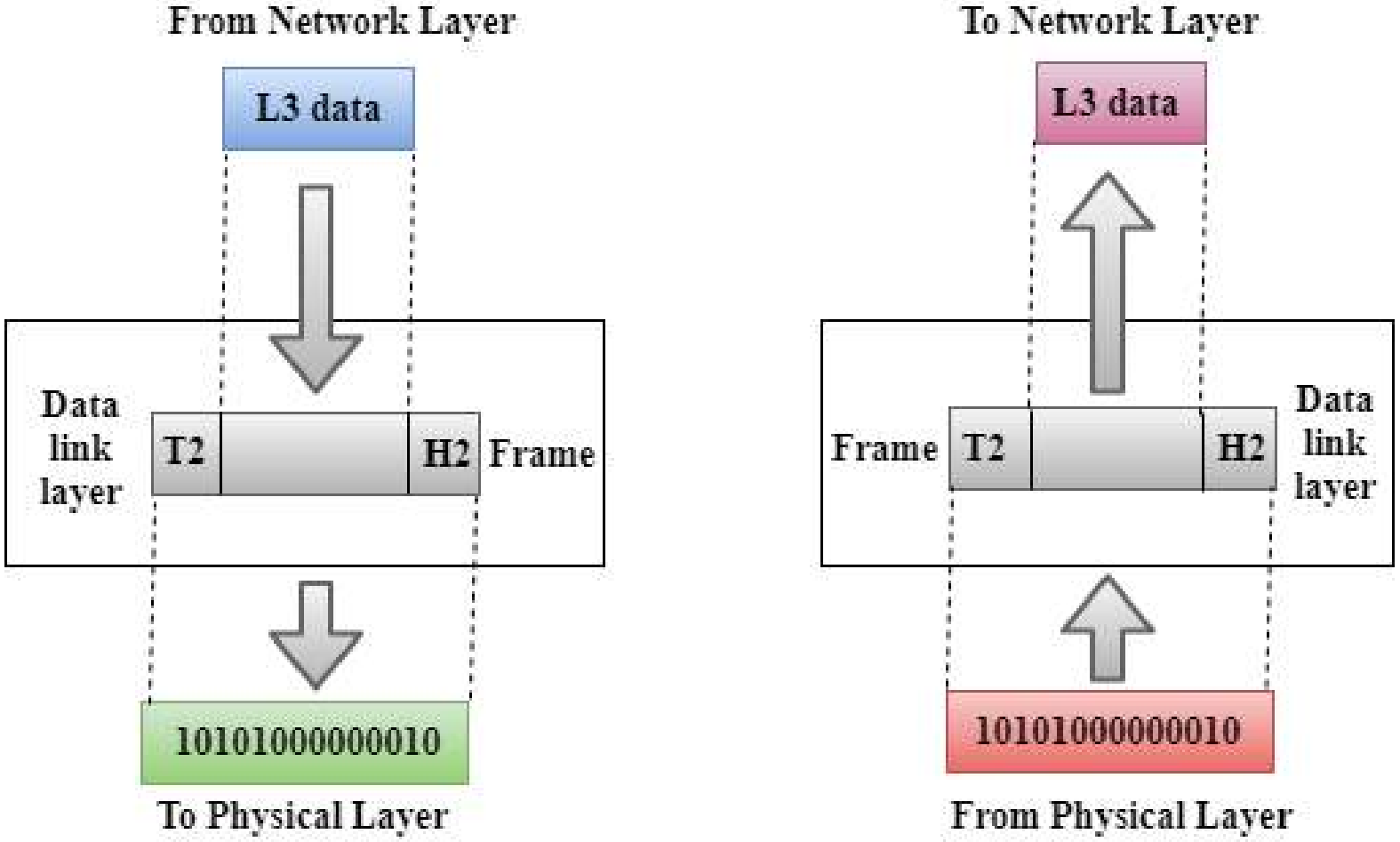
- **Logical Link Control Layer**
  - It is responsible for transferring the packets to the Network layer of the receiver that is receiving.
  - It identifies the address of the network layer protocol from the header.
  - It also provides flow control.
- **Media Access Control Layer**
  - A Media access control layer is a link between the Logical Link Control layer and the network's physical layer.
  - It is used for transferring the packets over the network.

Functions

- **Framing:** The data link layer translates the physical's raw bit stream into packets known as Frames. The Data link layer adds the header and trailer to the frame. The header which is added to the frame contains the hardware destination and source address.
- **Physical Addressing:** The Data link layer adds a header to the frame that contains a destination address. The frame is transmitted to the destination address mentioned in the header.

- **Flow Control:** Flow control is the main functionality of the Data-link layer. It is the technique through which the constant data rate is maintained on both the sides so that no data get corrupted. It ensures that the transmitting station such as a server with higher processing speed does not exceed the receiving station, with lower processing speed.

- **Error Control:** Error control is achieved by adding a calculated value CRC (Cyclic Redundancy Check) that is placed to the Data link layer's trailer which is added to the message frame before it is sent to the physical layer. If any error seems to occur, then the receiver sends the acknowledgment for the retransmission of the corrupted frames.
- **Access Control:** When two or more devices are connected to the same communication channel, then the data link layer protocols are used to determine which device has control over the link at a given time.

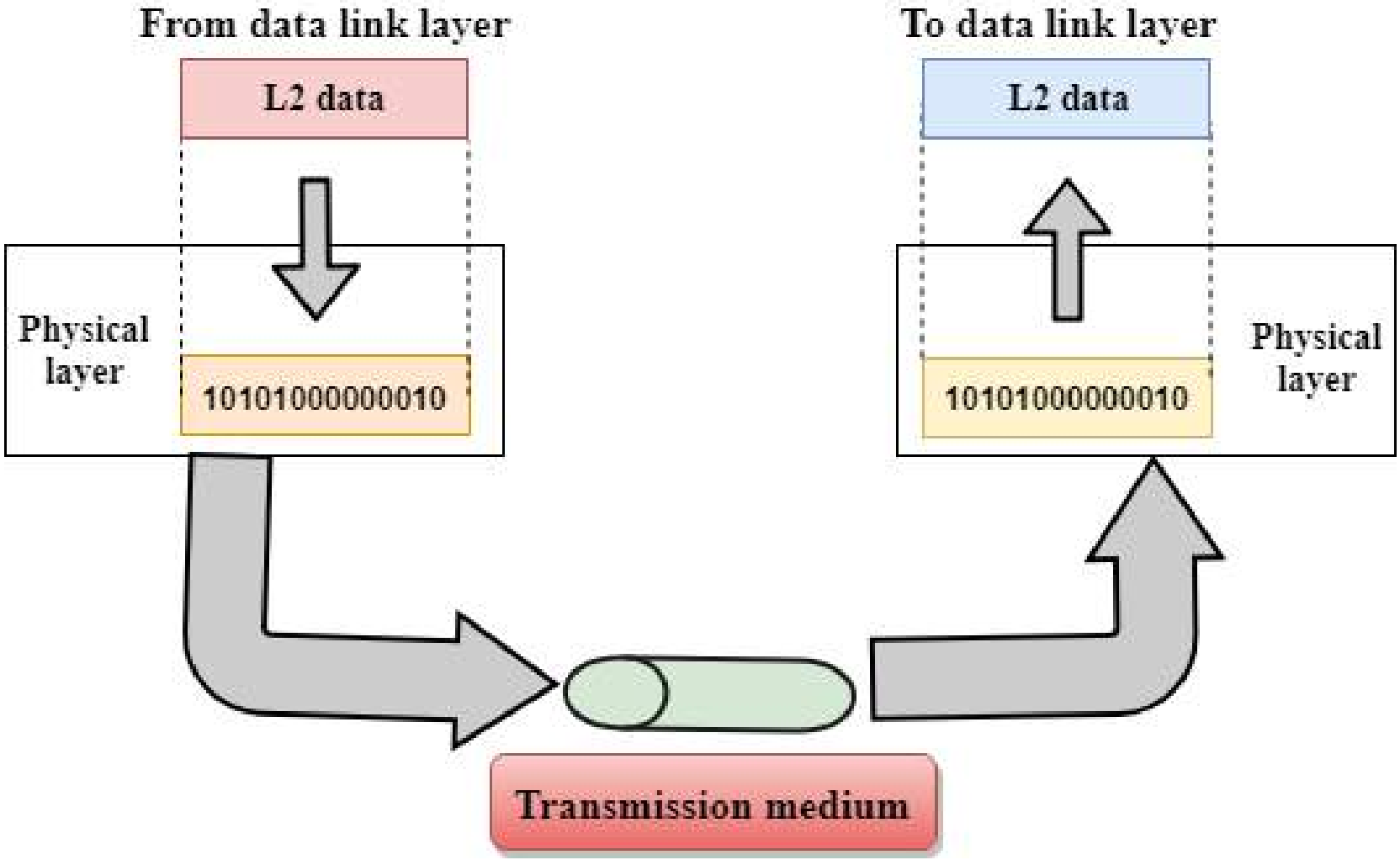

From Network Layer
L3 data
Data link layer
T2
H2
Frame
10101000000010
To Physical Layer
To Network Layer
L3 data
Frame
T2
H2
Data link layer
10101000000010
From Physical Layer

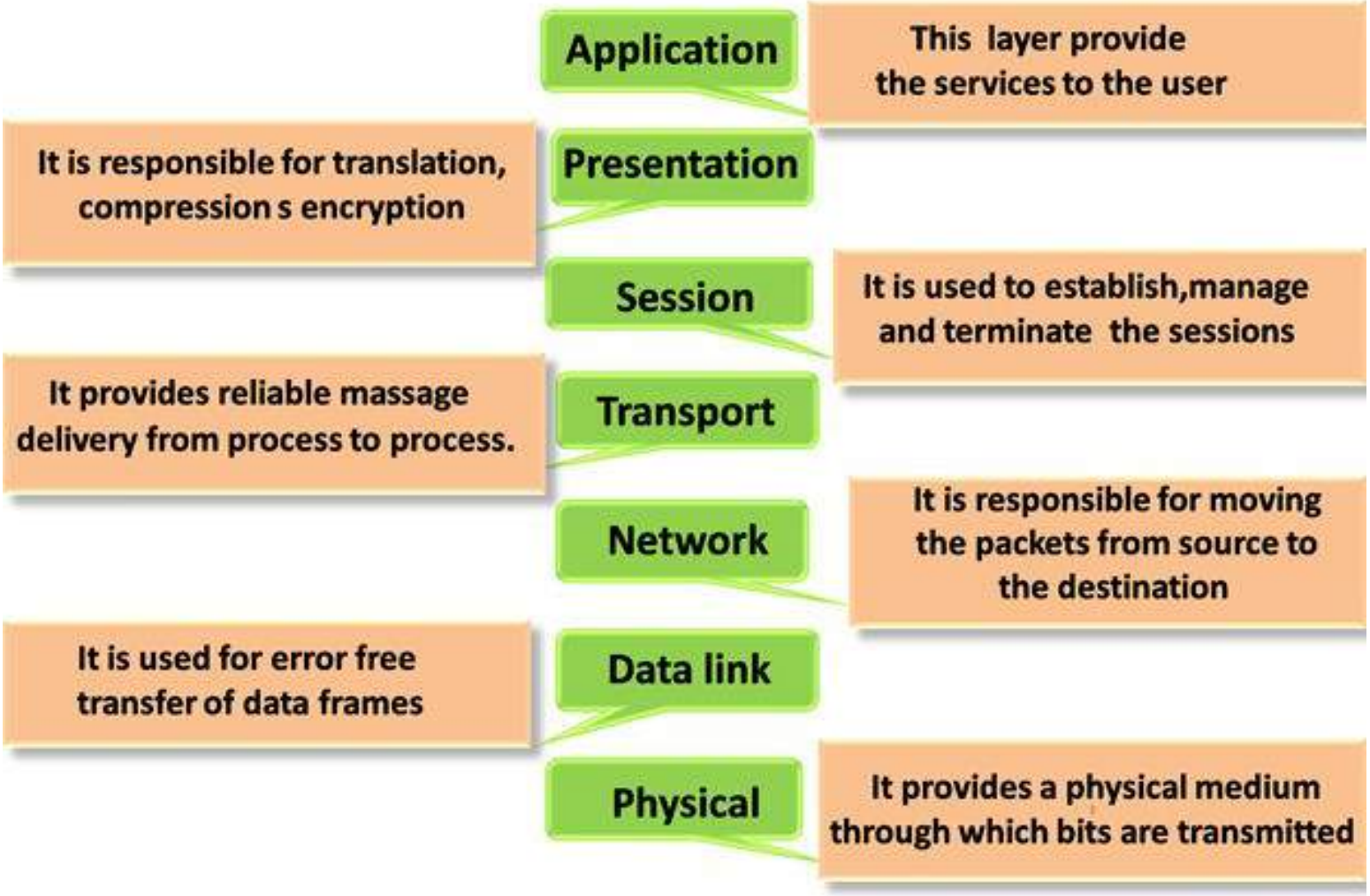
Physical Layer

- The lowest layer of the OSI reference model is the Physical layer.
- It is responsible for the actual physical connection between the devices.
- The physical layer contains information in the form of **bits.**
- It is responsible for transmitting individual bits from one node to the next.
- When receiving data, this layer will get the signal received and convert it into 0s and 1s and send them to the Data Link layer, which will put the frame back together.
- Hub, Repeater, Modem, Cables are Physical Layer devices.

Functions

- **Line Configuration:** It defines the way how two or more devices can be connected physically.
- **Data Transmission:** It defines the transmission mode whether it is simplex, half-duplex or full-duplex mode between the two devices on the network.
- **Topology:** It defines the way how network devices are arranged.
- **Signals:** It determines the type of the signal used for transmitting the information.


From data link layer
L2 data
Physical layer
10101000000010
To data link layer
L2 data
Physical layer
10101000000010
Transmission medium


Application
This layer provide the services to the user
It is responsible for translation, compression s encryption
Presentation
Session
It is used to establish,manage and terminate the sessions
It provides reliable massage delivery from process to process.
Transport
Network
It is responsible for moving the packets from source to the destination
It is used for error free transfer of data frames
Data link
Physical
It provides a physical medium through which bits are transmitted

Network Security

- Security means protecting information and information systems from unauthorized access, disclosure, disruption, modification and destruction.
- Security refers to the policies, procedures and technical measures used to prevent unauthorized access, alteration, theft or physical damage to information systems.
- Network security is the process of strategizing a defensive approach to secure your data and resources over the computer network infrastructure against any potential threat or unauthorized access.

- It uses software as well as hardware technologies to achieve the optimal solution for network defense.
- Network security involves all activities that organizations, enterprises and institutions undertake to protect the value and ongoing usability of assets and continuity of operations.
- The effective network security strategy requires identifying threats and then choosing the most effective set of tools to combat them.

- The goal of network security is to allow authorized users access to information and services while preventing unauthorized users from gaining access to, and possibly corrupting, the network.
- A basic tool used in network security is the firewall, which protects a Local Area Network (LAN) from intruders outside the network.

Model for Network Security

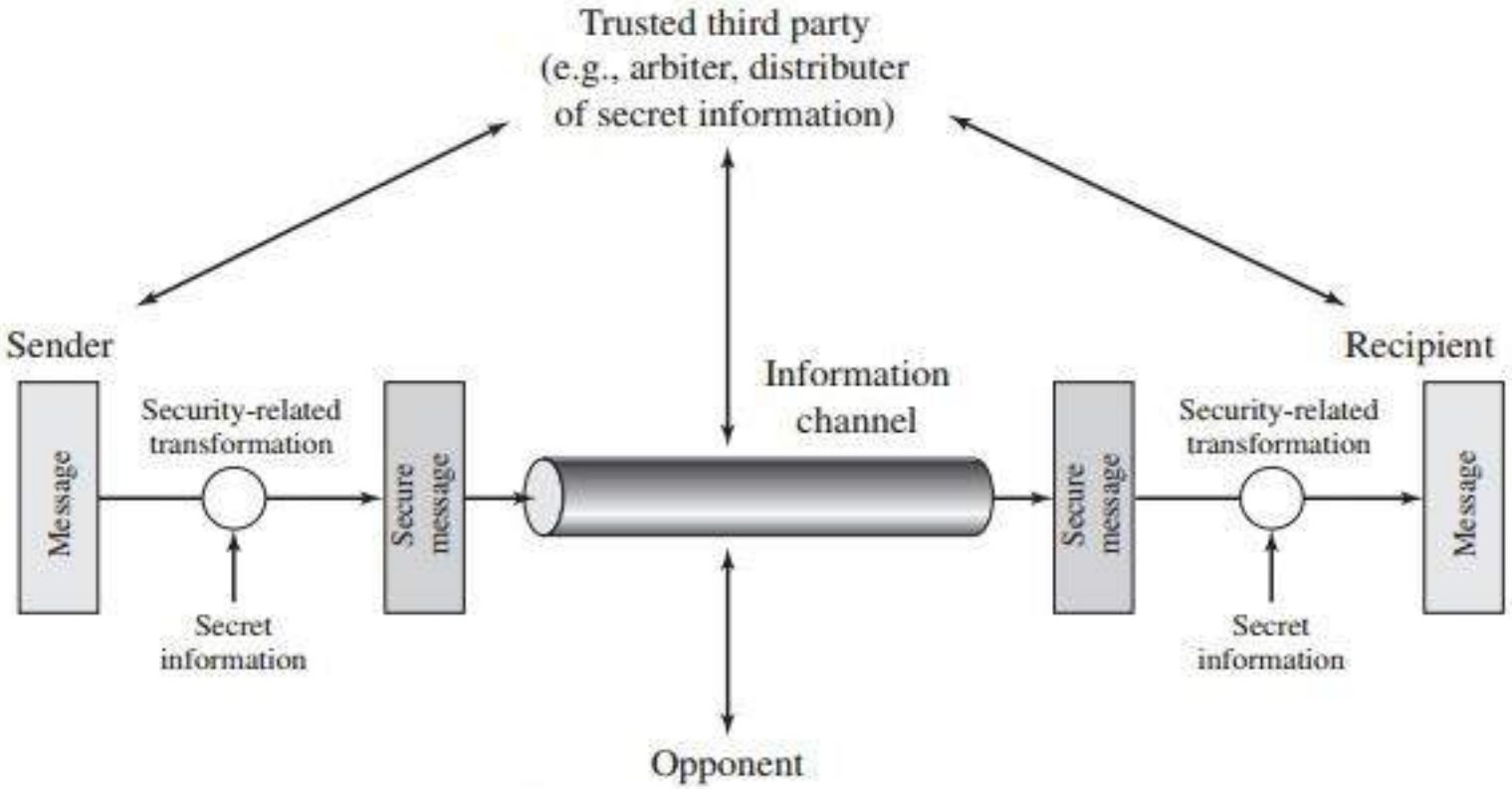
- A message is to be transferred from one source side to destination side, we must use some transfer method like the internet or any other communication channel by which we are able to send our message.
- The two parties, who are the principals in this transaction, must cooperate for the exchange to take place.
- When the transfer of data happened from one source to another source some logical information channel is established between them by defining a route through the internet from source to destination and by the cooperative use of communication protocols (e.g., TCP/IP) by the two principals.

- Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, and so on.
- All the techniques for providing security have two components:
- They are security related transformation and secret information.

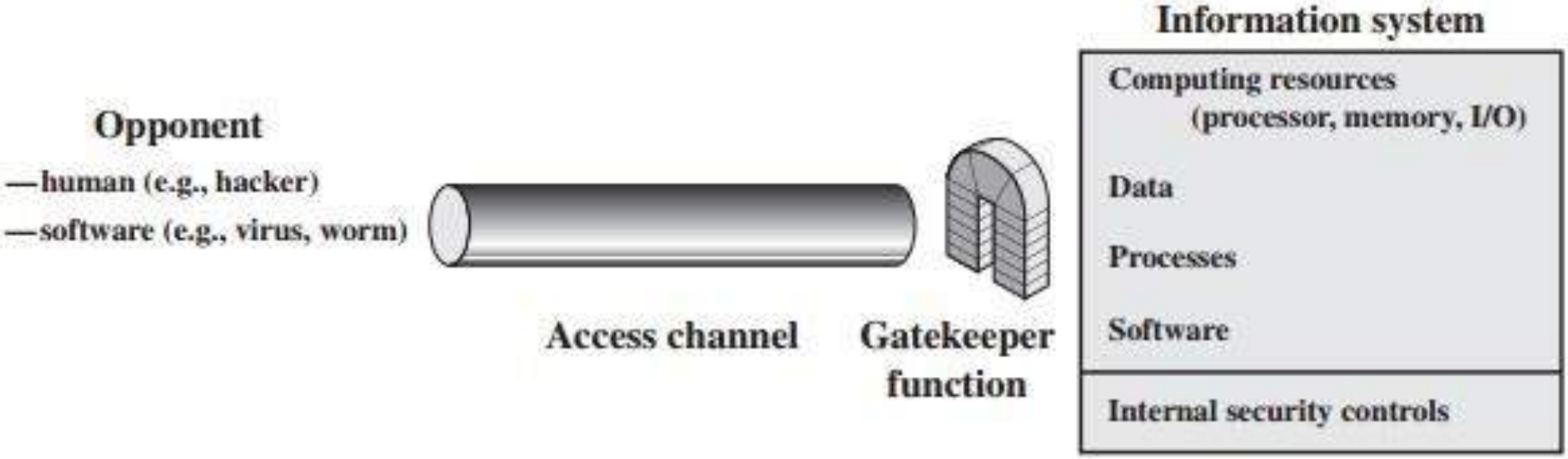
- A Security related transformation on the information to be sent.
- Examples include the encryption of the message, which scrambles the message so that it is unreadable by the opponent, and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.
- Some secret information shared by the two principals and, it is hoped, unknown to the opponent.

- An example is an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception.
- A trusted third party may be needed to achieve secure transmission.
- For example, a third party may be responsible for distributing the secret information to the two principals while keeping it from any opponent. Or a third party may be needed to arbitrate disputes between the two principals concerning the authenticity of a message transmission.

- According to this model, there are four basic tasks in designing a particular security service:
  1. Design an algorithm for performing the security-related transformation.
  2. Generate the secret information to be used with the algorithm.
  3. Develop methods for the distribution and sharing of secret information.
  4. Specify a protocol to be used by the two principals that make use of the security algorithm and the secret information to achieve a particular security service.



Model for Network Security



Network Access Security Model

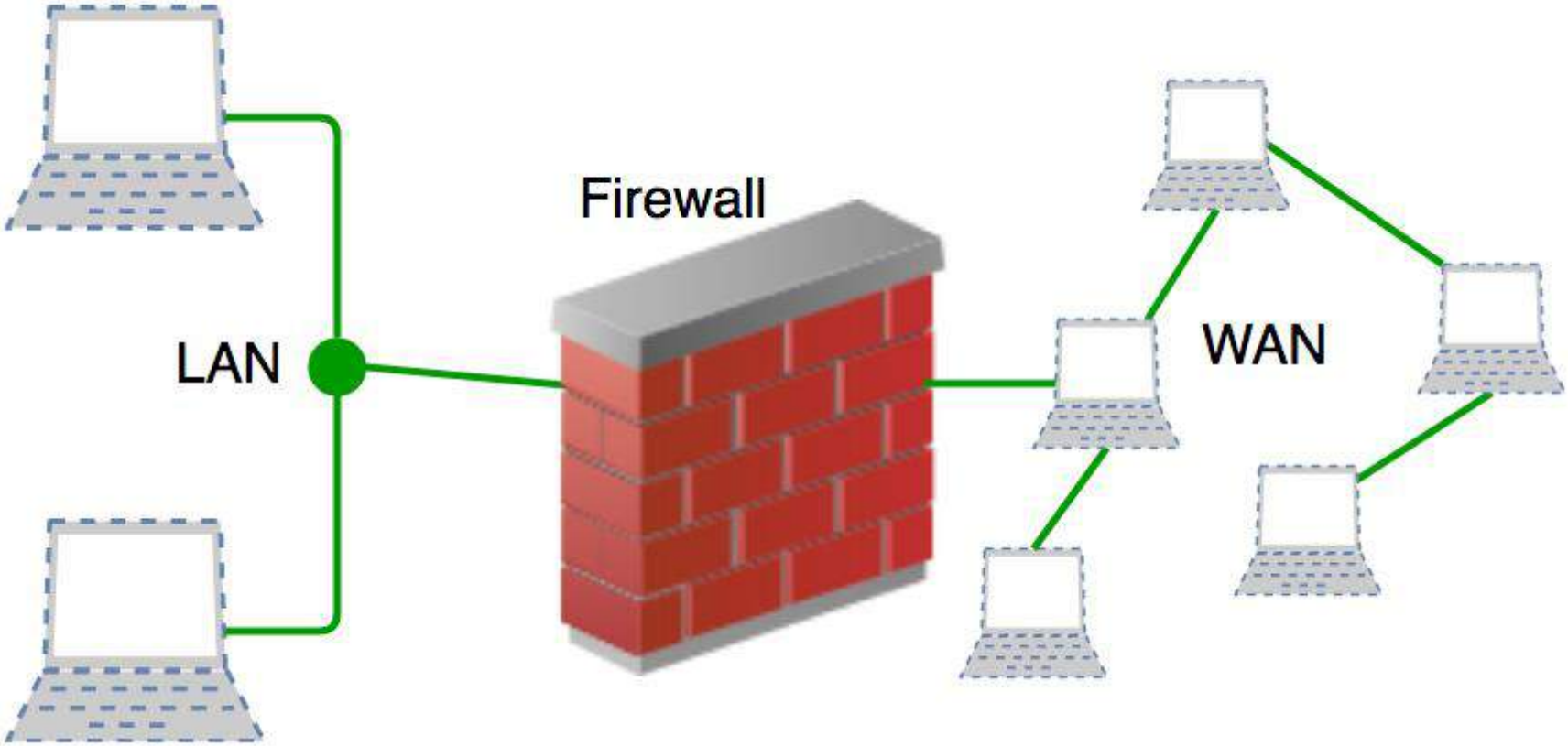
- A general model is illustrated by the above Figure, which reflects a concern for protecting an information system from unwanted access.
- Most readers are familiar with the concerns caused by the existence of hackers, who attempt to penetrate systems that can be accessed over a network.
- The hacker can be someone who, with no malign intent, simply gets satisfaction from breaking and entering a computer system.
- The intruder can be a disgruntled employee who wishes to do damage, or a criminal who seeks to exploit computer assets for financial gain.

- The security mechanisms needed to cope with unwanted access fall into two broad categories.
- The first category might be termed a gatekeeper function. It includes password-based login procedures that are designed to deny access to all but authorized users and screening logic that is designed to detect and reject worms, viruses, and other similar attacks.
- Once either an unwanted user or unwanted software gains access, the second line of defense consists of a variety of internal controls that monitor activity and analyze stored information to detect the presence of unwanted intruders.

Firewall

- A Firewall is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules.
- Firewalls have been a first line of defense in network security for over 25 years. They establish a barrier between secured and controlled internal networks that can be trusted and untrusted outside networks, such as the Internet.
- A firewall can be hardware, software, or both.

- Before Firewalls, network security was performed by Access Control Lists (ACLs) residing on routers.
- ACLs are rules that determine whether network access should be granted or denied to specific IP address.
- But ACLs cannot determine the nature of the packet it is blocking. Also, ACL alone does not have the capacity to keep threats out of the network. Hence, the Firewall was introduced.


Firewall
LAN
WAN

How Firewall Works

- Firewall match the network traffic against the rule set defined in its table. Once the rule is matched, associate action is applied to the network traffic.
- For example, Rules are defined as any employee from HR department cannot access the data from code server and at the same time another rule is defined like system administrator can access the data from both HR and technical department. Rules can be defined on the firewall based on the necessity and security policies of the organization.

- From the perspective of a server, network traffic can be either outgoing or incoming.
- Firewall maintains a distinct set of rules for both the cases. Mostly the outgoing traffic, originated from the server itself, allowed to pass. Still, setting a rule on outgoing traffic is always better in order to achieve more security and prevent unwanted communication.

- Incoming traffic is treated differently. Most traffic which reaches on the firewall is one of these three major Transport Layer protocols- TCP, UDP or ICMP.
- All these types have a source address and destination address.
- Also, TCP and UDP have port numbers.
- ICMP uses *type code* instead of port number which identifies purpose of that packet

- Default policy: It is very difficult to explicitly cover every possible rule on the firewall. For this reason, the firewall must always have a default policy. Default policy only consists of action (accept, reject or drop).
  - Accept : allow the traffic.
  - Reject : block the traffic but reply with an “unreachable error”.
  - Drop : block the traffic with no reply.
- Suppose no rule is defined about SSH connection to the server on the firewall. So, it will follow the default policy. If default policy on the firewall is set to accept, then any computer outside of your office can establish an SSH connection to the server. Therefore, setting default policy as drop (or reject) is always a good practice.

Packet Filters

- It is a first generation firewall and is a basic component of most firewalls. It operates at the IP or TCP/UDP layers of the TCP/IP suite of protocols.
- It is a basic border firewall that can be a single host or commercial router interconnecting an organization's internal network and some untrusted network.
- In this configuration, this single host or router provides all firewall functions.

- Packet filters filter IP packets during the routing process.
- The packet filtering firewall examines each IP packet coming into the equipment, looking at basic IP header information available in that pocket (e.g., source address, destination address, protocol, port).
- It compares that information with rules that the enterprise has setup. These are Firewall policies.

- If the source address, destination address and port are in trusted list then it is forwarded else the pocket is dropped.
- Packet firewalls treat each packet in isolation. They have no ability to tell whether a packet is part of an existing stream of traffic. Only It can allow or deny the packets based on unique packet headers.
- Packet filtering firewall maintains a filtering table which decides whether the packet will be forwarded or discarded. From the given filtering table, the packets will be Filtered according to following rules:

	Source IP	Dest. IP	Source Port	Dest. Port	Action
1	192.168.21.0	--	--	--	deny
2	--	--	--	23	deny
3	--	192.168.21.3	--	--	deny
4	--	192.168.21.0	--	>1023	Allow

Sample Packet Filter Firewall Rule

1. Incoming packets from network 192.168.21.0 are blocked.
2. Incoming packets destined for internal TELNET server (port 23) are blocked.
3. Incoming packets destined for host 192.168.21.3 are blocked.
4. All well-known services to the network 192.168.21.0 are allowed.

Circuit-Level Gateways

- Circuit-level gateways work at the session layer of the OSI model between the application layer and the transport layer of the TCP/IP stack.
- A Stateful inspection firewall allows or blocks traffic based on state, port, and protocol.
- They monitor TCP handshaking between packets to determine whether a requested session is legitimate.
- These firewall type is meant to quickly and easily approve or deny traffic by verifying the transmission control protocol (TCP) handshake.

- While extremely resource-efficient, these firewalls do not check the packet itself. So, if a packet held malware, but had the right TCP handshake, it would pass right through. This is why circuit-level gateways are not enough to protect your business by themselves.
- Filtering decisions are made based on both administrator-defined rules as well as context, which refers to using information from previous connections and packets belonging to the same connection.

Application Level Firewall

- An application-level proxy gateway, examines and filters individual packets, rather than simply copying them and blindly forwarding them across the gateway.
- Application-specific proxies check each packet that passes through the gateway, verifying the contents of the packet up through the application layer. These proxies can filter kinds of commands or information in the application protocols.

- Application gateways can restrict specific actions from being performed. For example, the gateway could be configured to prevent users from performing the 'FTP put' command. This can prevent modification of the information stored on the server by an attacker.
- Drawback to proxy firewalls, it's that they can create significant slowdown because of the extra steps in the data packet transferal process.

Limitations of Firewall

- Firewall cannot protect against attacks that bypass the firewall .
- Firewall does not protect against internal threats such as disgruntled employee or an employee who unwittingly cooperates with an external attacker.
- Firewall cannot protect against the transfer of virus infected programs or files .
- Firewall can be *"fooled"* by source routing or address spooling.

Protocols

- Network protocols are formal standards and policies made up of rules, procedures and formats that determine how two computers communicate with one another over a network.
- Those rules indicates the formatting, ordering, and error checking data sent across a network.
- Protocol determine how the sending device indicates that it has finished sending a message and how the receiving device will indicate that it has received (or not received) the message.

Contd.,

- They incorporate all the processes requirement and constraints of initiating and accomplishing communication between computers, routers, servers and other network enabled devices.
- Network protocols must be confirmed and installed by the sender and receiver to ensure network\data communication.
- It also applies software and hardware nodes that communicate on a network.
- Some protocols also support message acknowledgement and data compression designed for reliable and high performance network communication.

Elements of Protocol

- The key elements of protocols are as follows:
- **Syntax:** Syntax concerns the format of the data blocks. It refers to the structure or format of the data that is the order in which they are represented.
- Example: A Simple protocol may expect the first 8 bits of data to be the address of the sender, the second 8 bits to be the address of the receiver, and the rest of the stream to be the message itself.

Contd.,

- **Semantics:** it refers to the meaning of each section of bits. How is a specified pattern to be interpreted; and what action is to be taken based on that interpretation.
- For e.g. Does an address identify the route to be taken or the final destination of the message.
- **Timing:** Timing refers to two characteristics:
  - When the data should be sent.
  - How fast they can be sent.
- For E.g.: if a sender produces data at 100 Mbps but the receiver can process data at only 1 Mbps, the transmission will overload the receiver and will be largely lost.

TCP/IP

- The Internet Protocol (IP) is the most important communications protocol in the Internet protocol suite for relaying data across network boundaries.
- It essentially establishes the Internet.
- In the past, IP did not provide the connectivity; It only specified how packets are supposed to be created.
- The Transmission Control Protocol (TCP) allowed this functionality. Since one could not perform its task without the other, they earned the name TCP/IP to show how they depend on each other.

TCP/IP

- Think of IP as something like the postal system. It allows you to address a package and drop it into the system, but there is no actual direct link between you and the recipient.
- Instead, there is a "web" of links interconnecting with each other. This is where IP and TCP come in.
- IP tells packets what their destination is and how to get there; TCP ensures a reliable connection, checking packets for errors, requesting a "re-transmission" if it detects one.

- The Internet Protocol gets information from a source computer to a destination computer. It sends this information in the form of packets.
- IP packets or datagram has two parts. The first part is the header, which is like a label on an envelope. The second part is the payload, which is like the letter inside an envelope.
- The header contains the source and destination IP addresses, and some extra information. This information is called metadata, and is about the packet itself. Putting data in a packet with a header is encapsulation.

File Transfer Protocol

- FTP, also known as File Transfer Protocol, is a communication protocol for the rapid, simple transmission of computer files across a network supporting the TCP/IP.
- FTP uses the Client-Server architecture, meaning that there is a server, that holds the files, and does the authentication, and a client, or the end-user, who is accessing the files.
- The server listens on the network for connection requests from other computers.

- The client can make a connection to the FTP server by using FTP client software.
- Once connected and authenticated (via rsh or SFTP) the client can do things such as uploading files to the server, downloading files (taking the server's files and putting them on his own computer) from the server, and renaming, deleting files on the server, changing file permissions, etc.
- By using FTP the internet becomes a huge disk drive attached to your computer.

- FTP sites contain book, journals, software's, games, images, sound, multimedia courseware, databases and other information available for you to transfer.
- FTP uses Archie server. An agent who uses normal FTP commands to get directory listing of all the files on hundrends of anonymous sites around the world.

Hypertext Transfer Protocol (HTTP)

- Hypertext Transfer Protocol(HTTP) is an internet communication protocol used to send and receive webpages and files on the internet.
- HTTP defines how messages are formatted and transmitted, and what action web browsers should take in response to various commands.
- for e.g., when the user enters a URL in a browser, the browser sends and HTTP command to the web server directing it to fetch and transmit the requested web page.

- HTTP is a connectionless text-based protocol. Clients (web browsers) send requests to web servers for web elements such as web pages and images.
- After the request is serviced by a server, the connection between client and server across the Internet is disconnected.
- A new connection must be made for each request.

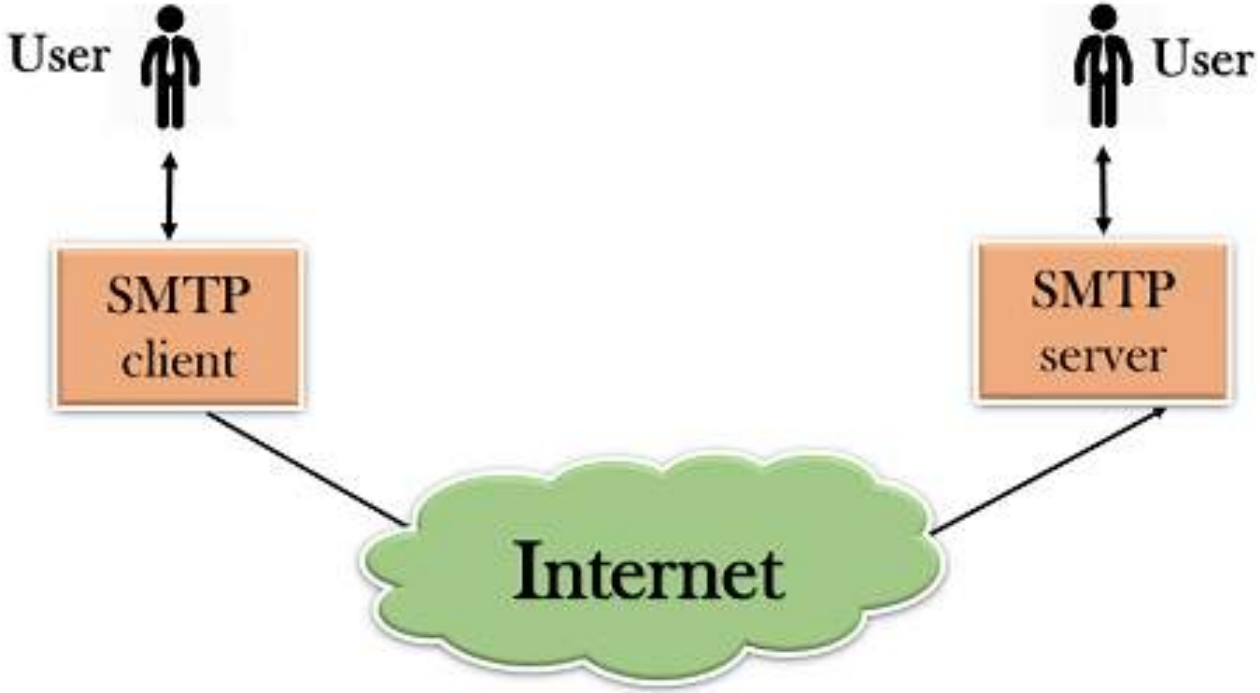
- The server must be located using a URL or URI. This always contains http:// at the start.
- It normally connects to port 80 on a computer.
- A more secure version of HTTP is called HTTPS (Hypertext Transfer Protocol Secure).
- This contains https:// at the beginning of the URL. It encrypts all the information that is sent and received.

- This can stop malicious users such as hackers from stealing the information and is often used on payment websites.
- HTTPS uses port 443 for communication instead of port 80.

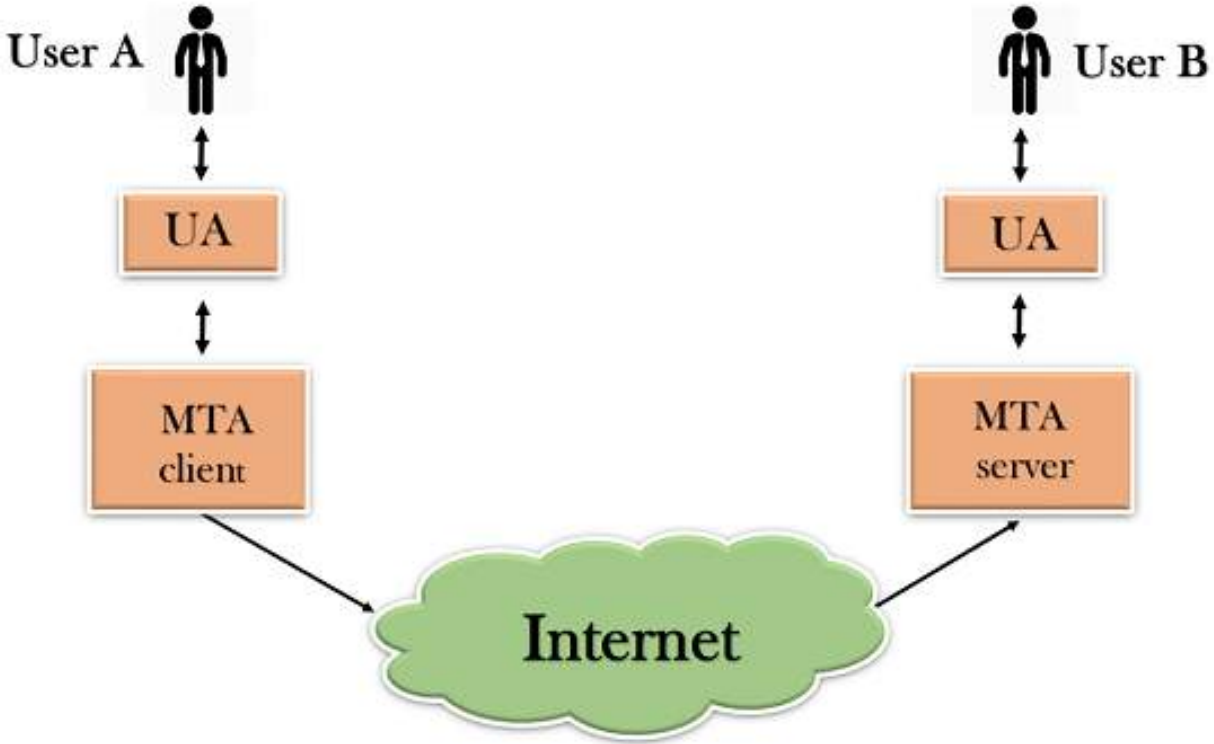
Simple Mail Transfer Protocol (SMTP)

- Simple Mail Transfer Protocol is a TCP/IP used in sending and receiving e-mail.
- It provides a mail exchange between users on the same or different computers, and it also supports:
  - It can send a single message to one or more recipients.
  - Sending message can include text, voice, video or graphics.
  - It can also send the messages on networks outside the internet.

- The main purpose of SMTP is used to set up communication rules between servers.
- The servers also handles the errors such as incorrect email address.
- For example, if the recipient address is wrong, then receiving server reply with an error message of some kind.


User
User
SMTP
client
SMTP
server
Internet

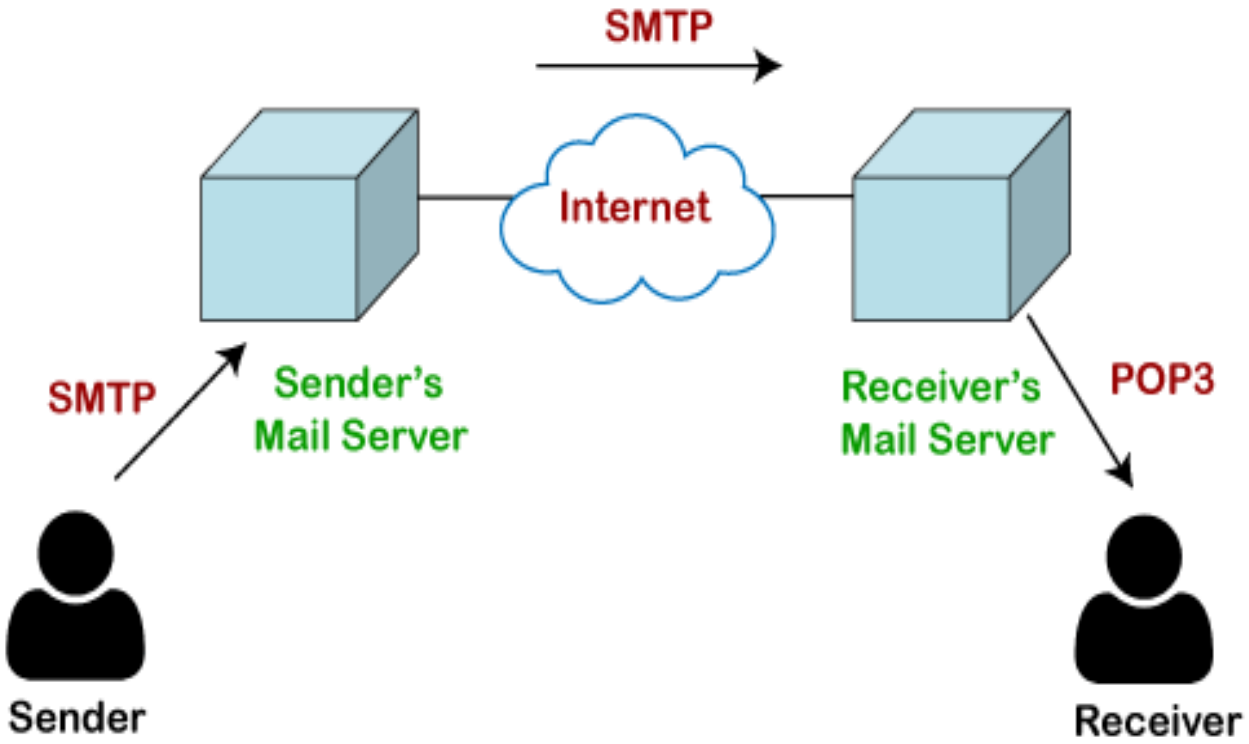
- The SMTP client and server into two components such as User Agent (UA) and Mail Transfer Agent (MTA).
- The User Agent (UA) prepares the message, creates the envelope and then puts the message in the envelope.
- The Mail Transfer Agent (MTA) transfers this mail across the internet.


User A
User B
UA
UA
MTA
client
MTA
server
Internet

Post Office Protocol

- The POP protocol stands for Post Office Protocol.
- Usually, SMTP is used as a message transfer agent. When the message is sent, then SMPT is used to deliver the message from the client to the server and then to the recipient server. But the message is sent from the recipient server to the actual server with the help of the Message Access Agent.
- The Message Access Agent contains two types of protocols, i.e., POP3 and IMAP.

- The transmission of mail from the sender to the sender's mail server and then to the receiver's mail server is done with the help of the SMTP protocol.
- At the receiver's mail server, the POP or IMAP protocol takes the data and transmits to the actual user.
- Since SMTP is a push protocol so it pushes the message from the client to the server.
- The next stage of email communication requires a pull protocol, and POP is a pull protocol. When the mail is transmitted from the recipient mail server to the client which means that the client is pulling the mail from the server.


SMTP
Internet
SMTP
Sender's
Mail Server
Receiver's
Mail Server
POP3
Sender
Receiver

User Datagram Protocol

- User Datagram Protocol is a standard protocol over the internet.
- The UDP protocol allows the computer applications to send the messages in the form of datagrams from one machine to another machine over the Internet Protocol (IP) network.
- The UDP is an alternative communication protocol to the TCP protocol (transmission control protocol).
- UDP provides a set of rules that governs how the data should be exchanged over the internet.

- The UDP works by encapsulating the data into the packet and providing its own header information to the packet. Then, this UDP packet is encapsulated to the IP packet and sent off to its destination.
- Both the TCP and UDP protocols send the data over the internet protocol network, There are many differences between these two protocols.
- UDP enables the process to process communication, whereas the TCP provides host to host communication.

- Since UDP sends the messages in the form of datagrams, TCP sends the individual packets, so it is a reliable transport medium.
- Another difference is that the TCP is a connection-oriented protocol whereas, the UDP is a connectionless protocol as it does not require any virtual circuit to transfer the data.

- Network security on the Internet is a major concern for commercial organizations, especially top management.
- Recently, the Internet has raised many new security concerns. By connecting to the Internet, a local network organization may be exposing itself to the entire population on the Internet.
- As figure below illustrates, an Internet connection opens itself to access from other networks comprising the public Internet

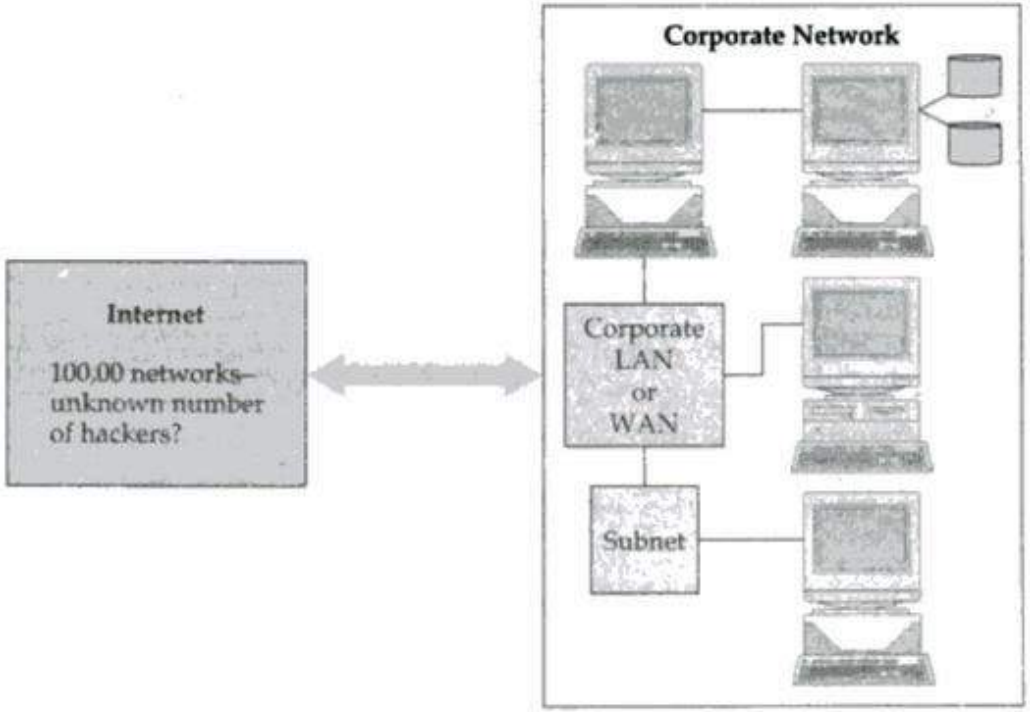


Figure 5.1 Unprotected Internet connection

- That being the case, the manager of even the most relaxed organization must pay some attention to security.
- For many commercial operations, security will simply be a matter of making sure that existing system features, such as passwords and privileges, are configured properly.
- They need to audit all access to the network.
- A system that records all log-on attempts—particularly the unsuccessful ones—can alert managers to the need for stronger measures.
- However, where secrets are at stake or where important corporate assets must be made available to remote users, additional measures must be taken.

- Hackers can use password guessing, password trapping, security holes in programs, or common network access procedures to impersonate users and thus pose a threat to the server.
- Security concerns in e-commerce can be divided into two broad types
  - Client Server Network Security
  - Data and Message Security

Client Server Network Security

- It uses various authorization methods to make sure that only the valid users and programs have access to information resources.
- Access control mechanisms must be setup to ensure that properly authenticated users are allowed access only to those resources that they are entitled to use. Such mechanisms include biometrics, encrypted smartcards, words protection and firewalls.

Data and Message Security

- It ensures the privacy and confidentiality in electric messages and data packets, including authentication of remote users in network transactions for activities such as online payments.
- The goal is to defeat any attempt to assume another identity while involved with email or other forms of data communication.
- Preventive measures include data encryption using various cryptographic methods.

Security issues in CSNS

Client–server network security problems manifest themselves in three ways:

- **Physical security holes** result when individuals gain unauthorized physical access to a computer.
- A good example would be a public workstation room, where it would be easy for a wandering hacker to reboot a machine into single-user mode and tamper with the files, if precautions are not taken. On the network, this is also a common problem, as hackers gain access to network systems by guessing passwords of various users.

Software Security holes

- **Software security holes** result when badly written programs or "privileged" software are "compromised" into doing things they shouldn't.
- The most famous example of this category is the "sendmail" hole, which brought the Internet to its knees in 1988.
- A more recent problem was the "rlogin" hole in the IBM RS-6000 workstations, which enabled a cracker (a malicious hacker) to create a "root" shell or superuser access mode. This is the highest level of access possible and could be used to delete the entire file system, or create a new account or password file.

Inconsistent usage holes

- **Inconsistent usage holes** result when a system administrator assembles a combination of hardware and software such that the system is seriously flawed from a security point of view.
- The incompatibility of attempting two unconnected but useful things creates the security hole.
- Problems like this are difficult to isolate once a system is set up and running, so it is better to carefully build the system with them in mind. This type of problem is becoming common as software becomes more complex.

Protection Methods

- To reduce these security threats, various protection methods are used.
- At the file level, operating systems typically offer mechanisms such as access control lists that specify the resources various users and groups are entitled to access.
- Protection also called authorization or access control-grants privileges to the system or resource by checking user-specific information such as passwords.
- The problem in the case of e-commerce is very simple:

- If consumers connect a computer to the Internet, they can easily log into it from anywhere that the network reaches. That's the good news.
- The bad news is that without proper access control, anyone else can too. Over the years, several protection methods have been developed, including trust-based security, security through obscurity, password schemes, and biometric systems.

Trust based Security

- Quite simply, trust-based security means to trust everyone and do nothing extra for protection.
- It is possible not to provide access restrictions of any kind and to assume that all users are trustworthy and competent in their use of the shared network.
- This approach assumes that no one ever makes an expensive breach such as getting root access and deleting all files (a common hacker trick).
- This approach worked in the past, when the system administrator had to worry about a limited threat. Today, this is no longer the case.

Security through Obscurity (STO)

- The Security through obscurity (STO) Philosophy is of the notion that any network can be secure as long as nobody outside its management group is allowed to find out anything about its operational details and users are provided information on a need to know basis.
- Hiding account passwords in binary files or scripts with the presumption that nobody will ever find them is a prime case of STO.

Password Schemes

- A password schemes erects a first level barrier to accidental intrusion.
- In actuality, password schemes do little about deliberate attack, especially when common words or proper names are entered as passwords.
- For instance, network administrators at a Texas air force base discovered that they could crack about 70 percent of the passwords on their UNIX network with tools resembling those used by hackers.
- Simplest method used by most hackers is dictionary comparison.

- Dictionary comparison consists of comparing a list of encrypted user passwords against a dictionary of encrypted common words.
- This scheme often works because users tend to choose relatively simple or familiar words as passwords.
- To beat the dictionary comparison method, experts often recommend using a minimum of eight-character length mixed-case passwords containing at least one non-alphanumeric character and changing passwords every 60 to 90 days.

- Since passwords in a remote log-in session usually pass over the network in unencrypted form, any eavesdropper on the network (which means anyone with any control at all of his or her hardware) can simply record the password any time it is used. Having distinct passwords for dis-tinct devices is sometimes a problem, because people will write them down (making them easy for others to find), share them (with people on the same project), or include them in automatic scripts (eliminating the inconvenience of typing them and also eliminating the protection from accidental access).
- To counter these threats, various approaches have been suggested for creating one-time passwords, including smart cards, randomized tokens, and challenge-response schemes.

Biometric Systems

- Biometric systems, the most secure level of authorization, involve some unique aspect of a person's body.
- Past biometric authentication was based on comparisons of fingerprints, palm prints, retinal patterns, or on signature verification or voice recognition.
- Biometric systems are very expensive to implement: At a cost of several thousand dollars per reader station, they may be better suited for controlling physical access—where one biometric unit can serve for many workers—than for network or workstation access. Many biometric devices also carry a high price in terms of inconvenience;

Client Server Threats

- Another security threat that is emerging in the electronic commerce world is mobile code (software agent), which in many ways resembles a more traditional virus threat.
- Mobile code is an executable program that has the ability to move from machine to machine and also to invoke itself without external influence.
- To circumvent this threat, organizations are installing firewalls that filter incoming data packets.

- These threats can be divided into two major categories:
  - Threats to local computing environment that include viruses, Worms, trojan horses and logic bombs.
  - Access control and threats to servers that include impersonation, eaves-dropping, denial of service, packet replay, and packet modification.

Threats to Local Computing Environment

- The major threat to security from running client software results because of the nature of the Internet:
- Client programs interpret data downloaded from arbitrary servers on the Internet.
- In the absence of checks on imported data, the potential exists for this data to subvert programs running on the systems.
- The security threat arises when the downloaded data passes through local interpreters (such as PostScript) on the client system without the user's knowledge.

- A similar problem existed in the UNIX mail system, whereby a remote user, through various escape sequences, could invoke the shell program (csh or sh) on the recipient's machine. This potential security breach has been plugged in most of the new mail systems.
- In short, client threats mostly arise from malicious data or code.
- Malicious code refers to viruses, worms, Trojan horses, logic bombs, and other deviant software programs.

- **Virus:** Virus is a computer program or software that connect itself to another software or computer program to harm computer system. When the computer program runs attached with virus it perform some action such as deleting a file from the computer system.
- **Trojan Horse:** Trojan Horse does not replicate itself like virus and worms. It is a hidden piece of code which steal the important information of user. For example, Trojan horse software observe the e-mail ID and password while entering in web browser for logging.
- **Worm.** Worms is also a computer program like virus but it does not modify the program. It replicate itself more and more to cause slow down the computer system.

Virus	Worm	Trojan Horse
Virus is a software or computer program that connect itself to another software or computer program to harm computer system.	Worms replicate itself to cause slow down the computer system.	Trojan Horse rather than replicate capture some important information about a computer system or a computer network.
Virus replicates itself.	Worms are also replicates itself.	But Trojan horse does not replicate itself.
Virus can't be controlled by remote.	Worms can be controlled by remote.	Like worms, Trojan horse can also be controlled by remote.
Spreading rate of viruses are moderate.	While spreading rate of worms are faster than virus and Trojan horse.	And spreading rate of Trojan horse is slow in comparison of both virus and worms.
The main objective of virus to modify the information.	The main objective of worms to eat the system resources.	The main objective of Trojan horse to steal the information.
Viruses are executed via executable files.	Worms are executed via weaknesses in system.	Trojan horse executes through a program and interprets as utility

- Malicious code is sometimes mistakenly associated only with stand-alone PCs but can also attack computer networks easily.
- In the latter case, actual costs attributed to the presence of malicious code have resulted primarily from system outages and staff time to repair the systems. Nonetheless, these costs can be significant.
- Clients must scan for malicious data and executable program fragments (such as MIME mail messages and PostScript files) that are transferred from the server to the client.

Threats to Servers

- Threats to servers consist of unauthorized modification of server data, unauthorized eavesdropping or modification of incoming data packets, and compromise of a server system by exploiting bugs in the server software.
- Compared to stand-alone systems, network servers are much more susceptible to attacks where legitimate users are impersonated.
- **Security Holes:** Hackers have potential access to a large number of systems. As a result, computers that are not properly configured and/or are running programs with security holes are particularly vulnerable

- **Password Guessing:** Hackers can use popular UNIX programs like Finger, rah, or ruser to discover account names and then try to guess simple passwords using a dictionary or more sophisticated password guessing methods (e.g., a hacker could use a password guessing program in which multiple computer systems are used simultaneously for comparison purposes).
- **Eavesdropping:** Hackers can use electronic eavesdropping to trap user names and unencrypted passwords sent over the network. They can monitor the activity on a system continuously and impersonate a user when the impersonation attack is less likely to be detected.

- Hackers can spoof, or configure, a system to cover-up as another system, thus gaining unauthorized access to resources or information on sys-tents that "trust" the system being mimicked.
- Hackers can eavesdrop using software that monitors packets sent over the network Many network programs, such as Telnet and ftp, are vulnerable to eavesdroppers who obtain passwords, which are often sent across the network unencrypted.
- Eavesdropping often allows a hacker to make a complete transcript of network activity and thus obtain sensitive information, such as passwords, data, and procedures for performing functions.

- A cracker can also eavesdrop using wiretapping, radio, or auxiliary ports on computers, which are used by network programs.
- In most cases, it is difficult to detect that someone is eavesdropping.
- Network programs that involve remote file transfer are especially susceptible to eavesdroppers gaining access to the contents of files.
- Encryption can prevent eavesdroppers from obtaining data traveling over unsecured networks.

- **Denial of Service Attack (DoS Attack):** Servers can also be attacked with threats such as denial of service, where a user can render the system unusable for legitimate users by "hogging" a resource or by damaging or destroying resources so that they cannot be used.
- The two most common forms of denial-of-service attacks are Service Overloading and Message Flooding.
- Servers are especially vulnerable to service overloading. For instance, one can easily overload a WWW server by writing a small loop that sends requests continually for a particular file, for example, a home page. The server tries to respond to the request in good faith as it assumes that all requests are legitimate. Hence, denial-of-service attacks may be caused intentionally or unintentionally by "runaway' software programs such as those caught in an infinite loop.

- Message Flooding occurs when someone sends a very large Me to a message box every few minutes.
- The message box rapidly grows in size and begins to occupy all the space on the disk and increases the number of receiving processes on the recipient's machine, tying it up even more and often causing a disk crash.
- The best way to avoid message overloading is to provide separate areas for different programs and to make provisions for graceful failure.

FIREWALLS AND NETWORK SECURITY

Dr P.V. Praveen Sundar
Assistant Professor,
Department of Computer Science
Adhiparasakthi College of Arts & Science,
Kalavai.

Proxy Application Gateways

- A proxy application gateway is a special server that typically runs on a firewall machine.
- Its primary use is access to applications such as the World Wide Web from within a secure perimeter.
- Instead of accessing directly to external WWW servers, each request from the client would be routed to a proxy on the firewall that is defined by the user.
- The proxy knows how to get through the firewall.
- An application-level proxy makes a firewall safely permeable for users in an organization, without creating a potential security hole through which hackers can get into corporate networks.

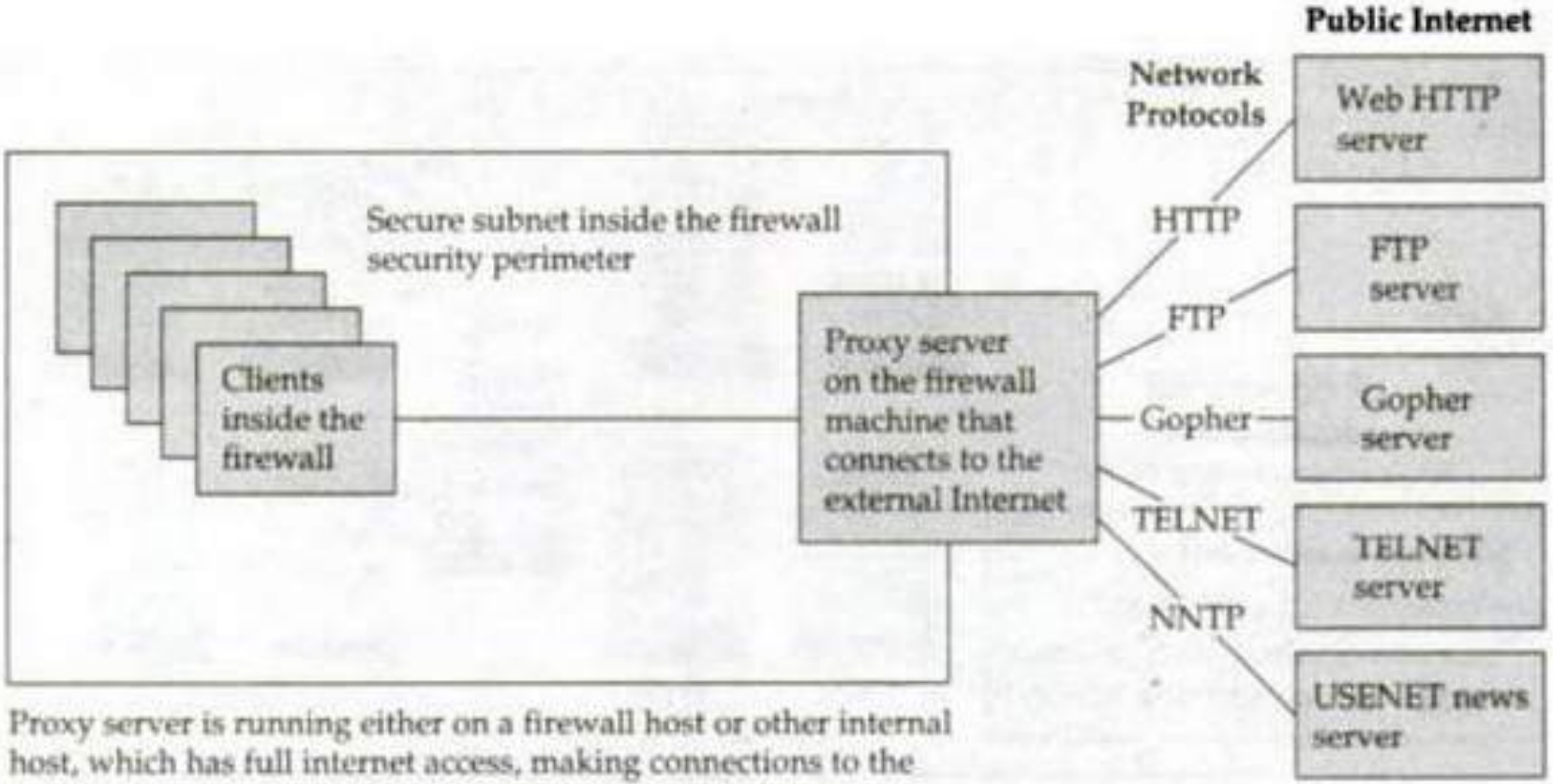


Figure 5.4 Proxy servers on the World Wide Web

- The proxy waits for a request from inside the firewall, forwards the request to the remote server outside the firewall, reads the response, and then returns it to the client.
- In the usual case, all clients within a given subnet use the same proxy.
- This makes it possible for the proxy to execute efficient caching of documents that are requested by a number of clients.

- Proxy gateways have several advantages. They allow browser programmers to ignore the complex networking code necessary to support every firewall protocol and concentrate on important client issues.
- For instance, by using HTTP between the client and proxy, no protocol functionality is lost, since FTP, Gopher, and other Web protocols map well into HTTP methods.
- Proxies can manage network functions. Proxying allows for creating audit trails of client transactions, including client IP address, date and time, byte count, and success code.

- Proxy mediation helps moderate security concerns by
  (1) Limiting dangerous subsets of the HTTP protocol (a site's security policy may prohibit the use of some of HTTP's methods);
  (2) Enforcing client and/or server access to designated hosts (an organization should have the capability to specify acceptable web sites);
  (3) Implementing access control for network services that is lost when the proxy is installed (to restore the security policy enforced by the firewall); and
  (4) Checking various protocols for well-formed commands.
- A bug existed in a previous version of the Mosaic browser that permitted servers to download a "Trojan horse" URL to the client that would cause the client to run an arbitrary program. The proxy must be in a position to filter dangerous URLs and malformed commands.

Hardened Firewall Hosts

- A hardened firewall host is a stripped-down machine that has been configured for increased security.
- This type of firewall requires inside or outside users to connect to the trusted applications on the firewall machine before connecting further.
- Generally, these firewalls are configured to protect against unauthenticated interactive logins from the external world.
- This helps prevent unauthorized users from logging into machines on the network.

Creating a hardened host requires several steps, among them:

- Removing all user accounts except those necessary for operation of the firewall, the logic being that, if users cannot log in to the firewall host, they cannot subvert the security measures.
- Removing all noncrucial files and executables, especially network server programs and client programs like FTP and Telnet.
- Extending traffic logging and monitoring to check remote access.
- Disabling IP forwarding to prevent the firewall from forwarding unauthorized packets between the Internet and the enterprise network.

- The hardened firewall host method can provide a greater level of audit and security, in return for increased configuration cost and decreased level of service.
- Hardened firewall hosts also offer specific advantages,
  - **Concentration of security:** All modified software and logging is located on the firewall system as opposed to being distributed on many hosts.
  - **Information hiding:** A firewall can "hide" names of internal systems or e-mail addresses, thereby revealing less information to outside hosts.
  - **Centralized and simplified network services management:** Services such as FTP, e-mail, Gopher, and other similar services are located on the firewall system(s) as opposed to being maintained on many systems.

Hardened Firewalls with Proxy Application Gateway

- Any one from inside or outside an organization give their user id, password, service required to the firewall machine which acts as one's proxy.
- Proxy firewall is now server to the requestor's desktop PC and also a client to some other requested service acting on requestor's behalf.
- Firewall needs proxy agent for each service requested such as FTP, HTTP, TELNET etc. Now proxy firewall is the initiator of all sessions and thus knows every activity thus ensuring security.
- Firewall with a proxy function replaces the source address of transaction requestor with its own IP address.

Security policies in Firewall Management

- The Firewall method of protection spans a continuum between ease of use and paranoid security.
- Before putting a firewall in place, the administrator who has the responsibility of designing, specifying, and implementing or overseeing the installation of a firewall must address a number of management issues.

- The first issue reflects the security policy of the organization: Is the firewall in place explicitly to deny all services except those integral to the mission of connecting to the Internet, or is the firewall in place to provide a metered and audited method of regulating access in a non threatening manner?
- The second issue is: What is the level of monitoring, redundancy, and control? Having established the acceptable risk level by resolving the first issue, a checklist is made of what should be monitored, permitted, and denied.

- For instance, the firewall computer can control access based on time of day, organizations might allow employees to run e-mail or FTP at any time, but to read USENET news groups only between 7 P.M. and 8 A.M.
- Finally, firewall policies must be realistic reflections of the level of security in the entire network. For example, a site with top secret or classified data should not be hooking up to the Internet in the first place; or the systems with the really secret data should be isolated from the rest of the corporate network.
- Firewalls are poor protection against threats such as viruses. The ways of encoding binary files for transfer over networks are too numerous, and the formats and viruses too varied to monitor them all.

Data and Message Security

- **Data Security:** Data Security refers to the technological safeguards and management procedure which can be applied to the computer hardware and software and data to ensure that organizational assets and individual privacy are protected.
- Data security means protecting information and information systems from unauthorized access, use, disclosures, disruption, modification or destruction/
- It is important when people are considering banking and financial transaction by PC.
- Major threat of data security is Packet Sniffing (unauthorized network monitoring), Sniffers use the network traffic, Example: Telnet, FTP and re login sessions through it gains the information like username and password

Message Security

- Message Security is a program that provides protection for companies messaging infrastructure. It protects all the personal messages of the company which are related to company vision and mission.
- Message Security: Threats to message security fall into three categories,
- **Message Confidentiality:** Confidentiality is the property of preventing disclosure of information to unauthorized individuals or systems.
  - For e.g.: A credit card transaction on the internet requires the credit card number to be transmitted from the buyer to the merchant and from the merchant to a transaction processing network. The system attempts to enforce confidentiality by encrypting the card number the transmission, by limiting the places where it might appear (in database, log files, backups, printed receipts and so on.) and by restricting access to the places where it is stored.

- If an unauthorized party obtains the card number in any way, a breach of confidentiality has occurred.
- **Message and system integrity:** Integrity means that data cannot be modified without authorization.
- Integrity is violated when an employee accidentally or with malicious intent deletes important data files, when a computer virus infects a computer, when an employee is able to modify his own salary in a payroll database, when an authorized user vandalizes a website.
- There are many ways in which integrity could be violated without malicious intent.

- On a larger scale, if an automated process is not written and tested correctly, bulk database to a database could alter data in a incorrect way, leaving the integrity of the data compromised.
- Information security professionals are tasked with finding ways to implement controls that prevent errors of integrity.
- **Message sender authentication or identification:** Identification is the process whereby a network element recognizes a valid user's identity. Authentication is the process of verifying the claimed identity of the user based on Password, Personal identification Number (PIN), smart card, biometrics, token , exchange of keys, etc.

- It verifies the identity of an user using certain encrypted information transferred from sender to receiver.
- Authentication information should be kept confidential.
- Authentication can be established by requiring a single login to access information on the network.
- This is the common method of gaining access to resources, computers and data on corporate systems.

ENCRYPTION & DECRYPTION

Dr P.V. Praveen Sundar
Assistant Professor,
Department of Computer Science
Adhiparasakthi College of Arts & Science,
Kalavai.

- **Cryptography** is the discipline dedicated to addressing secure data protection and transmission issue. Its approach is to convert the message into a form in which it is meaning is hidden and then transmitting it.
- **Encryption** is a process of transforming information (plain text) using an algorithm (called cipher) to make it unreadable to anyone except those processing special knowledge, usually referred as key. The result of the process is encrypted information (cipher text).
- Message is encrypted at the sender's side using various encryption algorithms and decrypted at the receiver's end with the help of the decryption algorithms.
- The conversion of encrypted data into its original form is called **Decryption**.

Types of Encryption

1. **Symmetric Encryption–** Data is encrypted using a key and the decryption is also done using the same key.
2. **Asymmetric Encryption**-Asymmetric Cryptography is also known as public key cryptography.
   - It uses public and private keys to encrypt and decrypt data.
   - One key in the pair which can be shared with everyone is called the public key.
   - The other key in the pair which is kept secret and is only known by the owner is called the private key.
   - Either of the keys can be used to encrypt a message; the opposite key from the one used to encrypt the message is used for decryption.

Secret key/Symmetric Encryption

- In Symmetric algorithms, the encryption key and the decryption keys are the same.
- These algorithms require that the sender and receiver agree on a key before they can communicate securely.
- Components of Symmetric cipher model.
  - Plain text: Original text that is readable and understandable.
  - Encryption Algorithm: an algorithm used to encrypt the message is called encryption algorithm.
  - Secret Key: it is the key that it is input to encryption algorithm.
  - Cipher Text: an encrypted message is known as cipher text.
  - Decryption algorithm: the process of turning cipher text back into plain text is called decryption. An algorithm used to encrypt the message is called decryption algorithm.

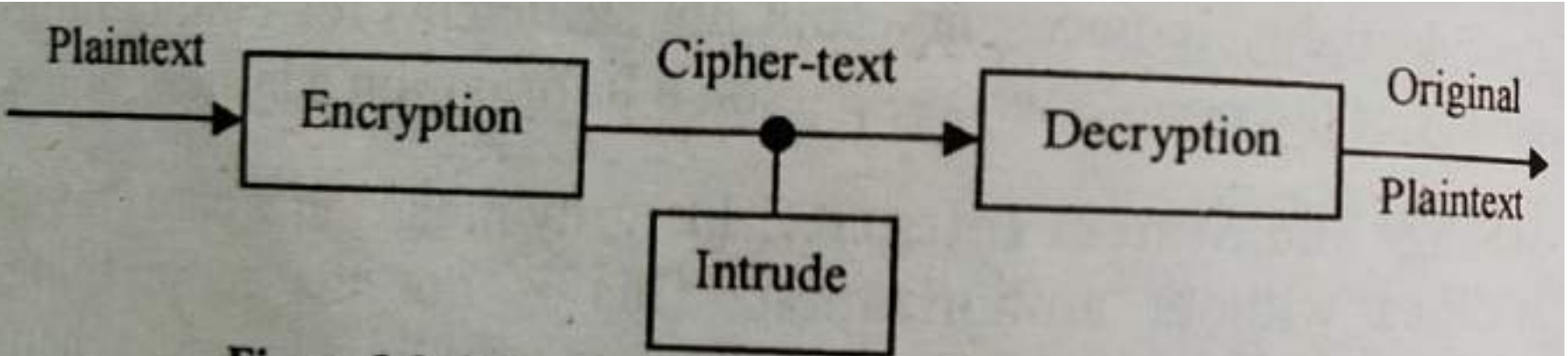
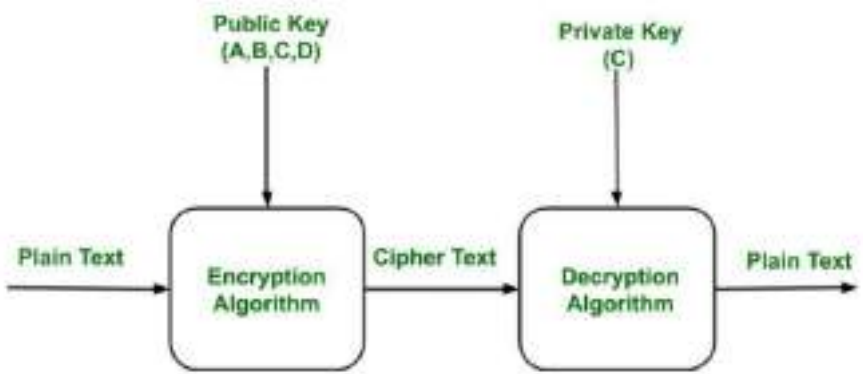


Figure 3.9: Process of Encryption and Decryption

Public key/Asymmetric Encryption

- Asymmetric is a form of Cryptosystem in which encryption and decryption are performed using different keys-Public key (known to everyone) and Private key (Secret key). This is known as **Public Key Encryption**.
- The need for the sender and receiver to share secret information is eliminated; all communications involve only public keys, and no private key is ever transmitted or shared.
- All of the security in these algorithms is based in the key; none is based in the details of algorithm. This means that the algorithm can be published and analyzed.

- Public keys of every user are present in the Public key Register. If B wants to send a confidential message to C, then B encrypt the message using C Public key. When C receives the message from B then C can decrypt it using its own Private key. No other recipient other than C can decrypt the message because only C know C's private key.



- **Plain Text:** This is the message which is readable or understandable. This message is given to the Encryption algorithm as an input.
- **Cipher Text:** The cipher text is produced as an output of Encryption algorithm. We cannot simply understand this message.
- **Encryption Algorithm:** The encryption algorithm is used to convert plain text into cipher text.
- **Decryption Algorithm:** It accepts the cipher text as input and the matching key (Private Key or Public key) and produces the original plain text
- **Public and Private Key:** One key either Private key (Secret key) or Public Key (known to everyone) is used for encryption and other is used for decryption

Data Encryption Standard (DES)

- The Data Encryption Standard is a block cipher operating on 64-bit data blocks.
- DES was designed by IBM and adopted by the U.S. government as the standard encryption method for nonmilitary and non classified use.
- DES has two transposition blocks (P-boxes) and 16 complex round ciphers (they are repeated).
- Although the 16 iteration round ciphers are conceptually the same, each uses a different key derived from the original key.

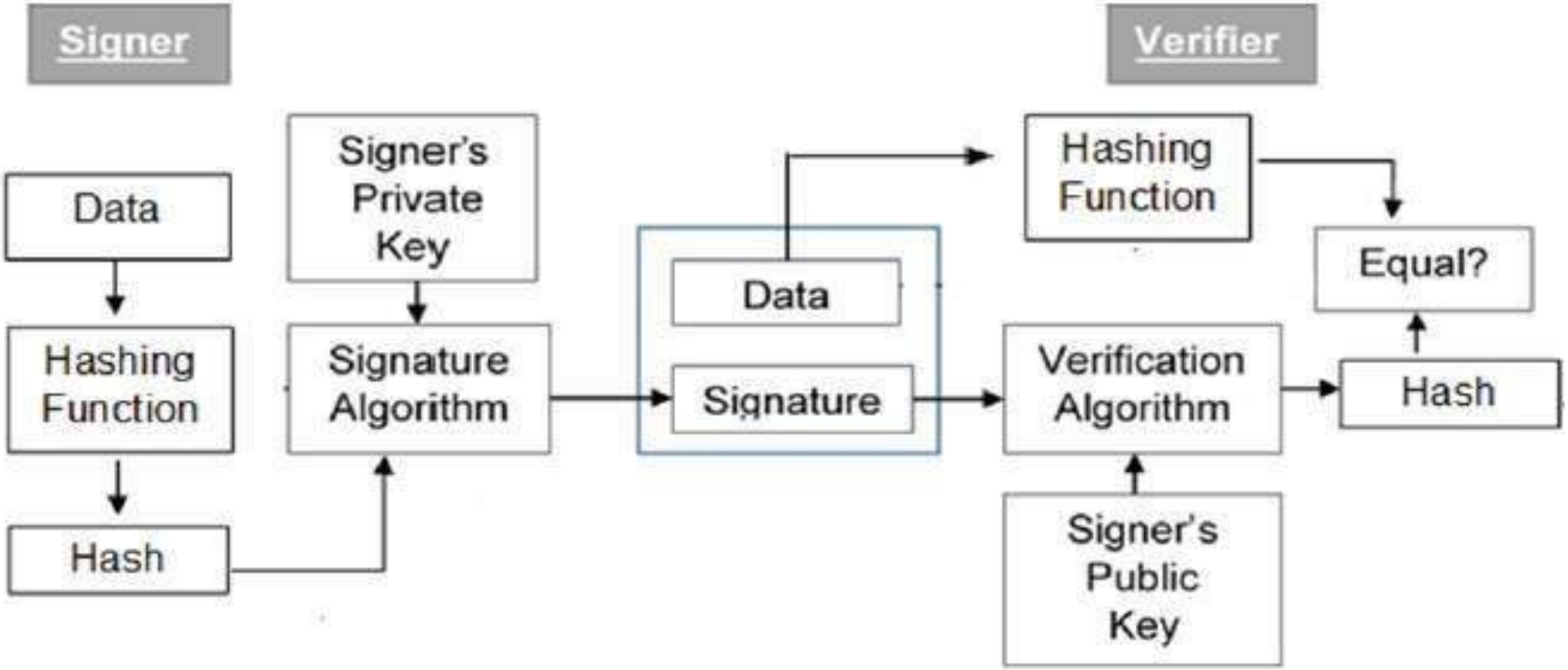
- The initial. and final permutations are keyless straight permutations that are the inverse of each other.
- The permutation takes 64-bit input and permutes them according to predefined values.
- Each round of DES is a complex round cipher and structure of the encryption round ciphers is different from that of the decryption one.
- DEA can also be used for single user encryption, such as to store files on a hard disk in encrypted form.
- In a multi user environment, secure key distribution maybe difficult.

Digital Signature

- Digital signature is an electronic signature that can be used to authenticate the identity of sender of a message or the signer of a document, and to ensure that the original content of message or document that has been sent is unchanged.
- *A digital signature is an electronic, encrypted stamp of authentication on digital data. The signature confirms that the information originated from the signer and has not been altered.*
- Digital signatures are easily transportable, cannot be imitated by someone else, and can be automatically time stamped.
- A digital certificate contains the digital signature of the certificate issuing authority so that anyone can verify that the certificate is real.

How Digital signature works?

- The sender creates an original message.
- The sender applies a hash function, producing a 128 bit hash result.
- The sender encrypts the message and the hash result using recipient's public key.
- The result of this result, again using private key.
- The result of this double encryption is sent over the internet.
- The receiver uses the sender's public key to authenticate the message.
- The receiver uses private key to decrypt the hash function and the original message. The receiver checks to ensure the original message and the hash function results confirm to one another.


Signer
Verifier
Data
Hashing Function
Hash
Signer's Private Key
Signature Algorithm
Data
Signature
Hashing Function
Equal?
Verification Algorithm
Hash
Signer's Public Key

Functions of Digital Signature

- **The authentication function:** The term digital signature is relevant to the practice of adding a string of characters to an electronic message that serves to identify the sender or the originator of a message.
- **The seal function:** Some digital signature techniques also serve to provide a check against any alteration of the text of the message after the digital signature was appended.
- **The integrity function:** This function is of great interest in cases where legal documents are created using such digital signatures.
- **The privacy function:** Privacy and confidentiality are of significant concerns in many instances where the sender wishes to keep the contents of the message private from all but the intended recipient.

Properties of Digital Signature

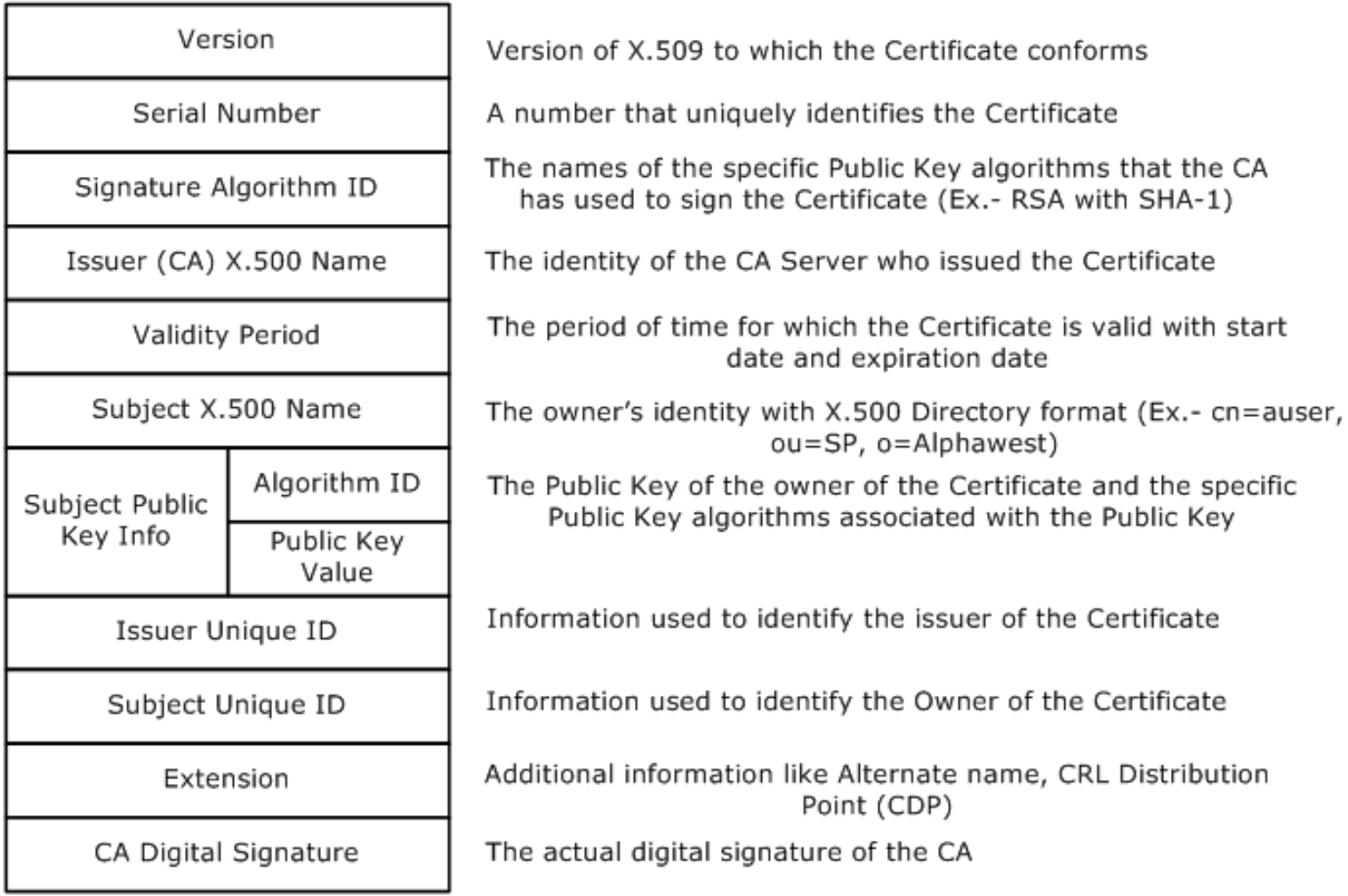
Digital signatures require properties:

- **Authenticity:** a valid signature implies that the signer deliberately signed the associated message.
- **Unforgeability:** only the signer can give a valid signature for the associated message.
- **Non-reusability:** the signature of a document cannot be used on another document.
- **Non-repudiation:** the signer cannot deny having signed a document that has valid signature.
- **Integrity:** ensure the contents have not been modified.

Digital Certificates

- A digital certificate is an electronic document that ties each person's or organization's identity to a public key. It contains digitally signed information including the identification of the person to be certified, the public key, the purpose and scope of the usage of the key and name of the certificate authority.
- A digital certificate is an electronic "credit card" that establishes credentials when doing business or other transactions on the web.
- A digital certificate is issued by a Certification Authority (CA). It contains name, a serial number, expiration dates, a copy of the certificate holder's public key(used for encrypting messages and digital signature). So that a recipient can verify that the certificate is real.
- Examples of trusted CA across the world are Verisign, Entrust, etc.
- The CA guarantees the validity of the information in the certificate.

- **Public Key Infrastructure (PKI)** consists of protocols, standards and services, that allows users to authenticate each other using digital certificates that are issued by CA.
- For a digital certificate to be useful, it has to be structured in a standard way so that information within the certificate can be retrieved and understood regardless of who issued the certificate.
- The ***X.509***, ***PKI X.509*** and ***Public Key Cryptography Standards (PKCS)*** are the building blocks a PKI system that defines the standard formats for certificates and their use.


Version
Version of X.509 to which the Certificate conforms
Serial Number
A number that uniquely identifies the Certificate
Signature Algorithm ID
The names of the specific Public Key algorithms that the CA has used to sign the Certificate (Ex.- RSA with SHA-1)
Issuer (CA) X.500 Name
The identity of the CA Server who issued the Certificate
Validity Period
The period of time for which the Certificate is valid with start date and expiration date
Subject X.500 Name
The owner's identity with X.500 Directory format (Ex.- cn=auser, ou=SP, o=Alphawest)
Subject Public Key Info
Algorithm ID
Public Key Value
The Public Key of the owner of the Certificate and the specific Public Key algorithms associated with the Public Key
Issuer Unique ID
Information used to identify the issuer of the Certificate
Subject Unique ID
Information used to identify the Owner of the Certificate
Extension
Additional information like Alternate name, CRL Distribution Point (CDP)
CA Digital Signature
The actual digital signature of the CA

1. Generate Key-pair

2. User-A requests CA Certificate

3. CA responds with its CA Certificate including its Public Key

4. Gather information

5. Request the Certificate which has User-A's identity and Public Key

6. CA verifies the identity of User-A

7. Issue the Certificate for User-A

The Process of Obtaining a Digital Certificate

1.**Generate Key-pair:** User-A generates a Public and Private key-pair or is assigned a key-pair by some authority in their organization.

2.**Request CA Certificate:** User-A first requests the certificate of the CA Server.

3.**CA Certificate Issued:** The CA responds with its Certificate. This includes its Public Key and its Digital Signature signed using its Private Key.

4.**Gather Information:** User-A gathers all information required by the CA Server to obtain its certificate. This information could include User-A email address, fingerprints, etc. that the CA needs to be certain that User-A claims to be who she is.

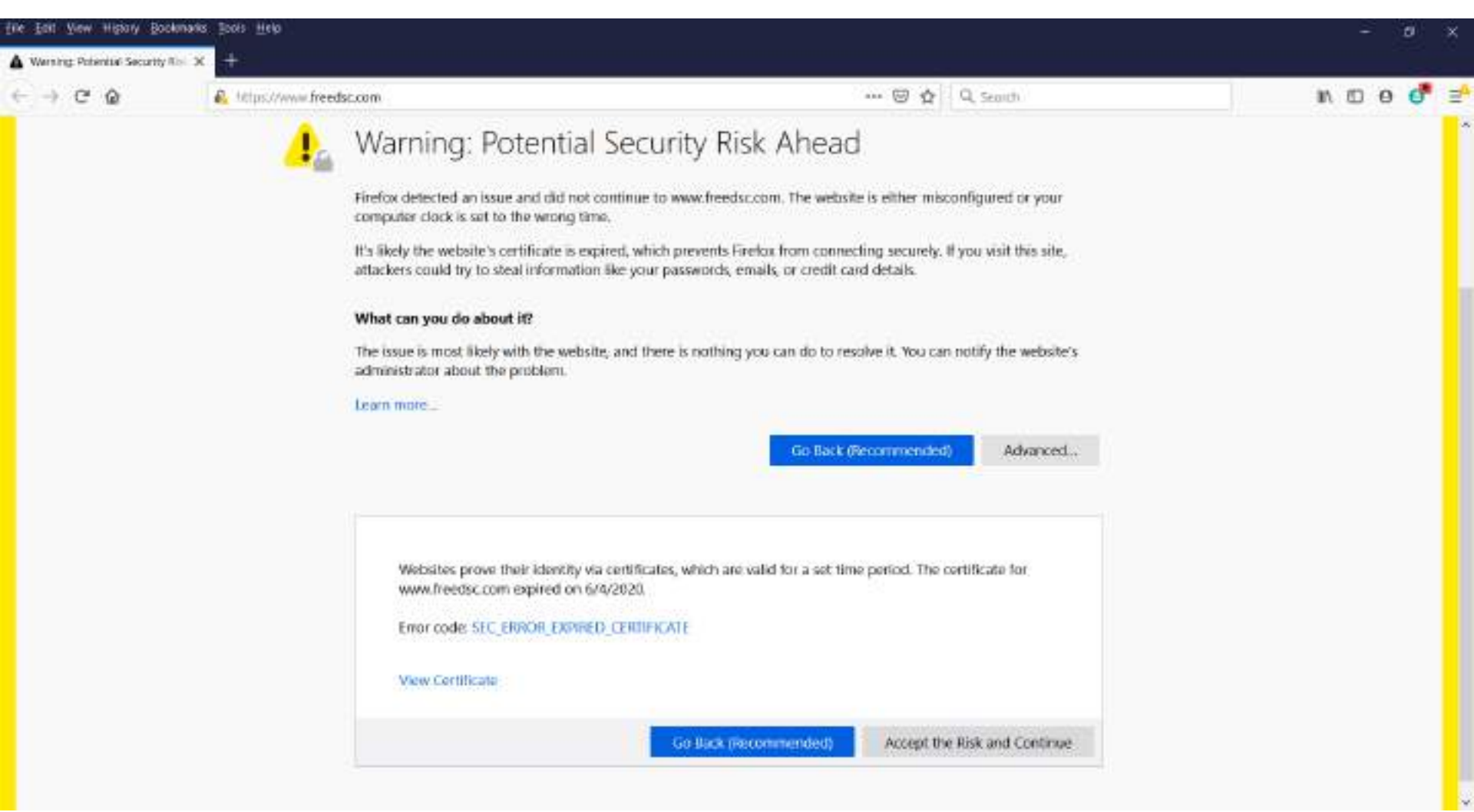
5. **Send Certificate Request:** User-A sends a certificate request to the CA consisting of her Public Key and additional information. The certificate request is signed by CA's Public Key.

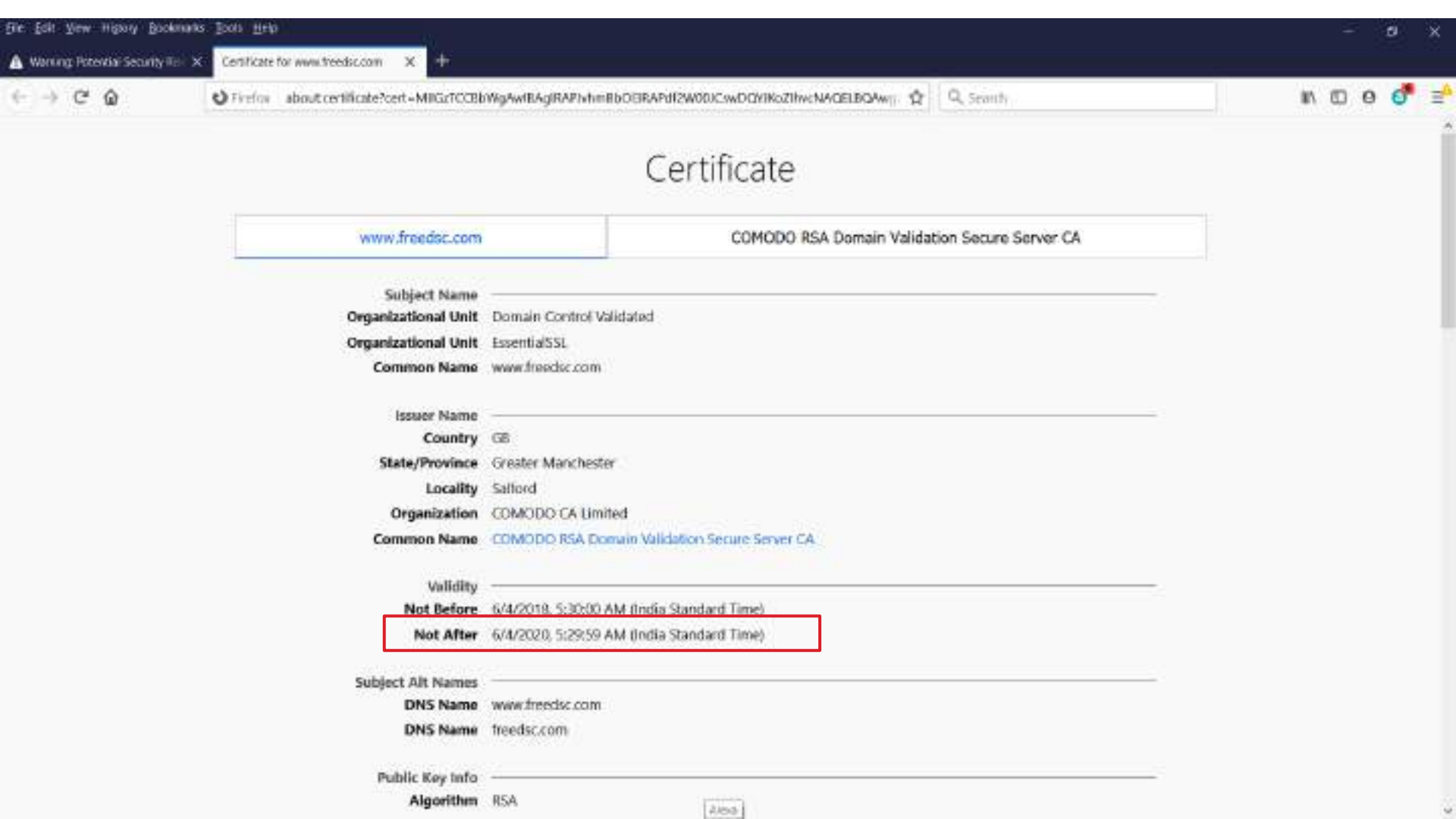
6. **CA verifies User-A:** The CA gets the certificate request, verifies User-A's identity and generates a certificate for User-A, binding her identity and her Public Key. The signature of CA verifies the authenticity of the Certificate.

7. **CA issues the Certificate:** The CA issues the certificate to User-A.

Benefits of Digital Certificates

- Send Signed Email Messages: This ensures the recipients that the message came from you and not pretending to be you. This is particularly important when sending out official university messages, such as from the president office.
- Encrypt the contents of email messages and attachments, protecting them from being read by online intruders, Only your intended recipient can decrypt them.
- Encrypt files and/or folders on your computer. "This is helpful for lost or stolen mobile devices and laptops because thieves would need to know your password to access any of the encrypted files or folders.
- Streamline business processes by allowing people to use digital certificates to electronically sign documents or approve something at a given stage of the process.


File Edit View History Bookmarks Tools Help
Warning: Potential Security Risk
https://www.freedsc.com
Search
Warning: Potential Security Risk Ahead
Firefox detected an issue and did not continue to www.freedsc.com. The website is either misconfigured or your computer clock is set to the wrong time.
It's likely the website's certificate is expired, which prevents Firefox from connecting securely. If you visit this site, attackers could try to steal information like your passwords, emails, or credit card details.
What can you do about it?
The issue is most likely with the website, and there is nothing you can do to resolve it. You can notify the website's administrator about the problem.
Learn more...
Go Back (Recommended)
Advanced...
Websites prove their identity via certificates, which are valid for a set time period. The certificate for www.freedsc.com expired on 6/4/2020.
Error code: SEC_ERROR_EXPIRED_CERTIFICATE
View Certificate
Go Back (Recommended)
Accept the Risk and Continue



Certificate

www.freedsc.com	COMODO RSA Domain Validation Secure Server CA

Subject Name

Organizational Unit	Domain Control Validated
Organizational Unit	EssentialSSL
Common Name	www.freedsc.com

Issuer Name

Country	GB
State/Province	Greater Manchester
Locality	Salford
Organization	COMODO CA Limited
Common Name	COMODO RSA Domain Validation Secure Server CA

Validity

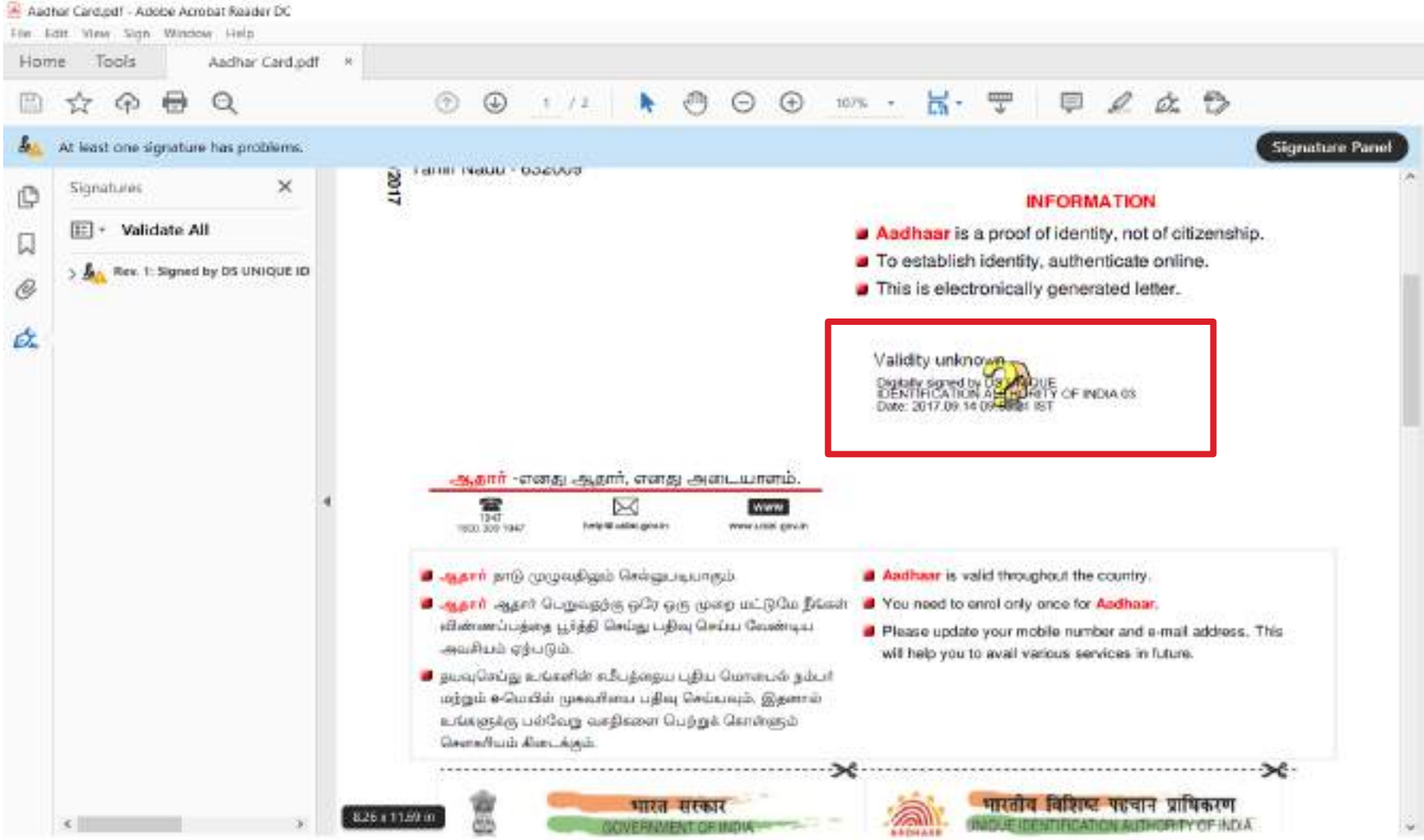
Not Before	6/4/2019, 5:30:00 AM (India Standard Time)
Not After	6/4/2020, 5:29:59 AM (India Standard Time)

Subject Alt Names

DNS Name	www.freedsc.com
DNS Name	freedsc.com

Public Key Info

Algorithm	RSA


Aadhar Card.pdf - Adobe Acrobat Reader DC
File Edit View Sign Window Help
Home Tools
Aadhar Card.pdf
At least one signature has problems.
Signature Panel
Signatures
Validate All
Rev. 1: Signed by DS UNIQUE ID
INFORMATION
Aadhaar is a proof of identity, not of citizenship.
To establish identity, authenticate online.
This is electronically generated letter.
Validity unknown
Digitally signed by DS UNIQUE IDENTIFICATION AUTHORITY OF INDIA 03
Date: 2017.09.14 09:
IST
ஆதார் -எனது ஆதார், எனது அடையாளம்.
1947
www
ஆதார் நாடு முழுவதிலும் செல்லுபடியாகும்.
ஆதார் ஆதார் பெறுவதற்கு ஒரே ஒரு முறை மட்டுமே நீங்கள் விண்ணப்பத்தை பூர்த்தி செய்து பதிவு செய்ய வேண்டிய அவசியம் ஏற்படும்.
தயவுசெய்து உங்களின் சமீபத்திய கைபேசி எண் மற்றும் இ-மெயில் முகவரியை பதிவு செய்யவும். இதனால் உங்களுக்கு பல்வேறு சேவைகள் பெற்றுக் கொள்ளும் வசதியும் கிடைக்கும்.
Aadhaar is valid throughout the country.
You need to enrol only once for Aadhaar.
Please update your mobile number and e-mail address. This will help you to avail various services in future.
826 x 1169 in
भारत सरकार
GOVERNMENT OF INDIA
भारतीय विशिष्ट पहचान प्राधिकरण
UNIQUE IDENTIFICATION AUTHORITY OF INDIA

Feature	Digital Signature	Digital Certificate
Basics / Definition	Digital signature is like a fingerprint or an attachment to a digital document that ensures its authenticity and integrity.	Digital certificate is a file that ensures holder's identity and provides security.
Process / Steps	Hashed value of original message is encrypted with sender's secret key to generate the digital signature.	It is generated by CA (Certifying Authority) that involves four steps: Key Generation, Registration, Verification, Creation.
Security Services	**Authenticity** of Sender, **integrity** of the document and **non-repudiation**.	It provides security and **authenticity** of certificate holder.
Standard	It follows Digital Signature Standard (DSS).	It follows X.509 Standard Format

Digital Envelopes

- A digital envelope is the electronic equivalent of putting your message into a sealed envelope to provide privacy and resistance to tampering. A digital signature is the electronic equivalent of a signet ring and sealing wax: You seal the message so that the receiver has a high degree of confidence that the message really came from the purported sender and that no one has altered it.
- A digital envelope is a secure electronic data container that is used to protect a message through encryption and data authentication. A digital envelope allows users to encrypt data with the speed of secret key encryption and the convenience and security of public key encryption.
- A digital envelope is also known as a digital wrapper.

A digital envelope uses two layers for encryption:

1. Secret (symmetric) key . Secret key encryption is used for message encoding and decoding.
2. Public key encryption is used to send a secret key to a receiving party over a network. This technique does not require plain text communication.

- A digital envelope may be decrypted by using a receiver's private key to decrypt a secret key, or by using a secret key to decrypt encrypted data.
- An example of a digital envelope is Pretty Good Privacy (PGP) - a popular data cryptography software that also provides cryptographic privacy and data communication authentication.

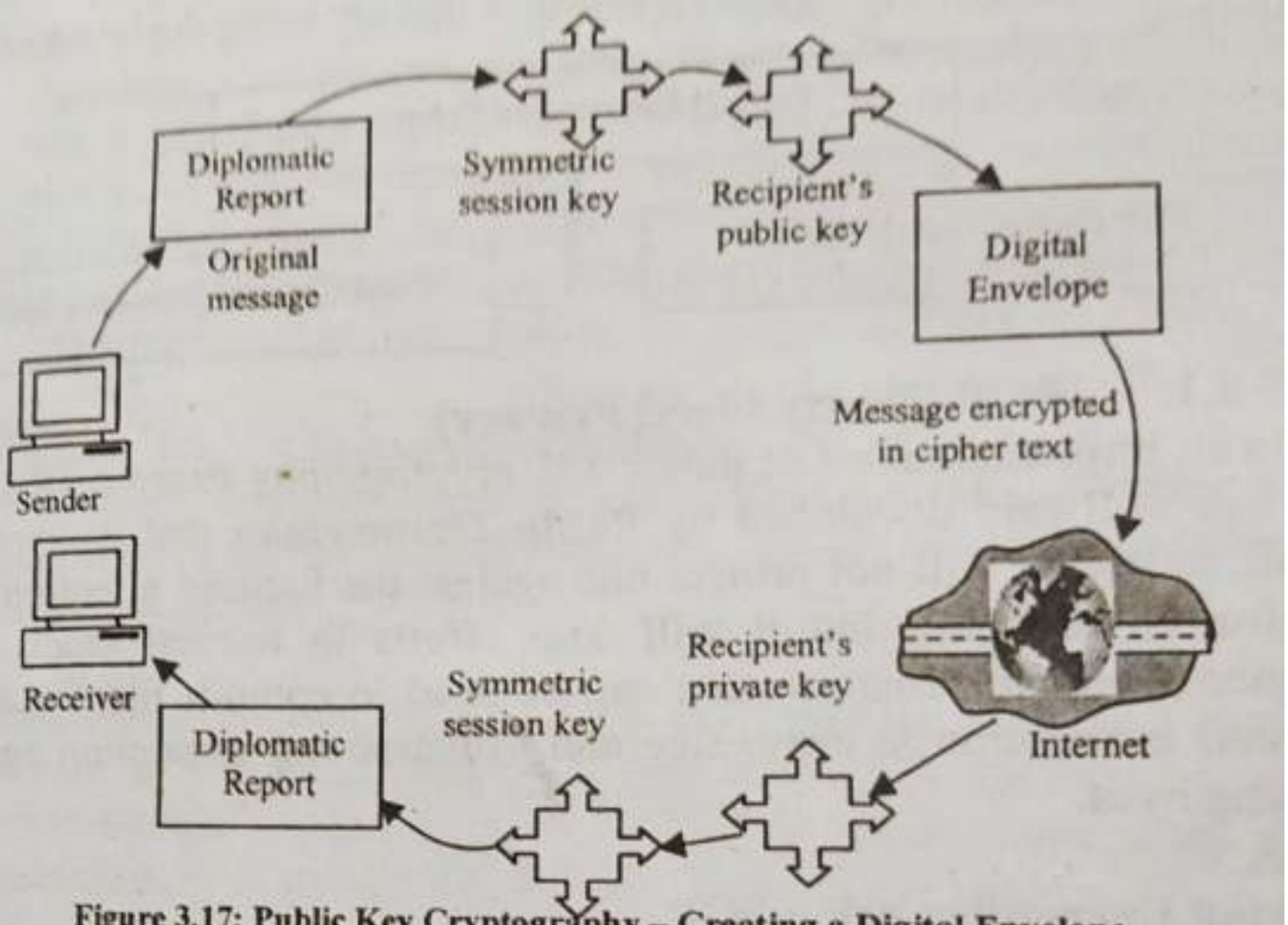


Figure 3.17: Public Key Cryptography – Creating a Digital Envelope

Working of Digital Envelope

- In figure 3.17, a diplomatic document is encrypted using a symmetric key.
- The symmetric key — which the recipient will require to decrypt the document - is itself encrypted, using the recipient's public key. So one has a "key within a key" (a digital envelope).
- The encrypted report and the digital envelope are sent across the web.
- The recipient first uses his/her private key to decrypt the symmetric key, and then the recipient uses the symmetric key to decrypt the report. This method saves time because both encryption and decryption are faster with symmetric keys.
- A digital envelope can be created to transmit a symmetric key that will permit the recipient to decrypt the message and be assured the message as not intercepted in transit.

Encrypted Documents

- Most email messages you send travel vast distances over many networks, secure and insecure, monitored and unmonitored, passing through and making copies of themselves on servers all over the Internet. In short, pretty much anyone with access to any of those servers - or sniffing packets anywhere along the way - can read your email messages sent in plain text.
- E-mail software is increasingly incorporating specific options that simplify encryption and decryption. Examination of encrypted information is non-trivial; each file must be decrypted even before it can be examined. If the file itself proves to contain embedded, compressed, encrypted files, those too must be expanded and decrypted. This process may need repeating several times before the innermost files' contents are discernible.

Privacy Enhanced Mail Standard(PEM)

- PEM is the Internet Privacy Enhanced Mail standard, designed, proposed, but not yet officially adopted, by the Internet Activities Board to provide secure electronic mail over the Internet.
- Designed to work with current Internet e-mail formats, PEM includes encryption, authentication, and key management, and allows use of both public-key and secret-key cryptosystems.
- The system supports multiple cryptographic tools: for each mail message, the specific encryption algorithm, digital signature algorithm, hash function, and so on are specified in the header.

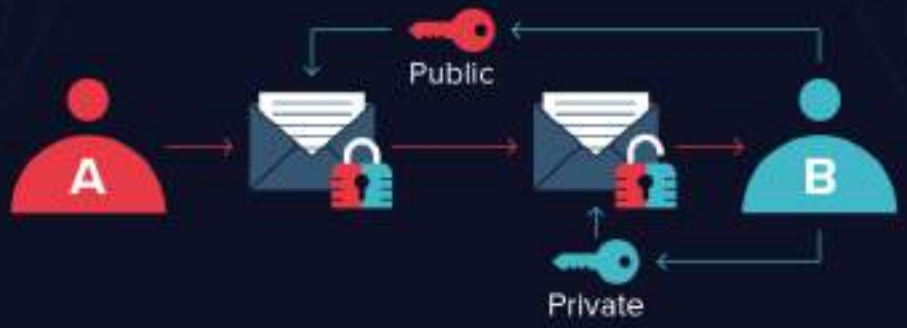
- PEM explicitly supports only a few cryptographic algorithms; others may be added later. It uses the DES algorithm for encryption and the RSA algorithm for sender authentication and key management.
- PEM also provides support for nonrepudiation, which allows the third-party recipient of a forwarded message to verify the identity of the message originator (not just the message forwarder) and to verify whether any of the original text has been altered.

- Although PEM is not yet widespread, a number of vendors are offering versions of it in conjunction with or integrated into their commercial e-mail applications.
- Trusted Information Systems, Inc. has developed a free non-commercial implementation of PEM, and other implementations should soon be available as well.
- RIPEM, a program developed by Mark Riordan, enables secure Internet e-mail; it provides both encryption and digital signatures, using RSA and DES routines from RSAREF (a set of routines provided by RSA).
- RIPEM is not fully PEM-compatible; for example, it does not currently support certificates. However, future versions will include certificates and will be fully compliant with the PEM standard

Pretty Good Privacy (PGP)

- Pretty Good Privacy (PGP) is an implementation of public-key cryptography based on RSA.
- It is a free software package developed by Phillip Zimmerman that encrypts e-mail. Since being published in the United States as freeware in June 1991,
- PGP has spread rapidly and has since become the de facto worldwide standard for encryption of e-mail.
- It is freely available for DOS, Macintosh, UNIX, Amiga, VMS, Atari, and OS/2 systems.
- PGP provides secure encryption of documents and data files that even advanced supercomputers are hard pressed to "crack."
- When plaintext is encrypted with PGP, it first compresses the plaintext. Data compression saves transmission time, disk space, and reinforces cryptographic security.

HOW PGP ENCRYPTION WORKS



1. User A wants to send User B a private email
2. User B generates a public and private key
3. User B keeps the private key and sends back the public key
4. User A encrypts their message using the public key
5. User A sends the private encrypted message
6. User B decrypts the message with the private key

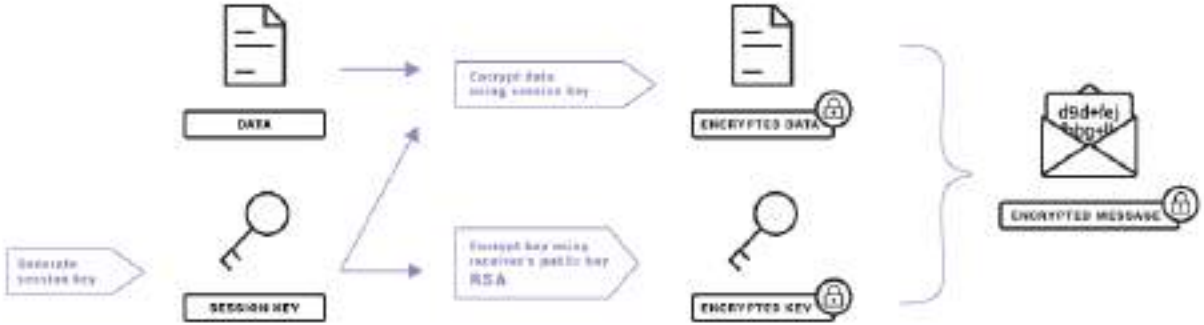
- The process is simple enough that anyone with a PC can do it with almost no effort.
- For authentication, PGP employs the RSA public-key encryption scheme and the MD5 (Message Digest version 5) developed by Rivest, a one-way hash function to form a digital signature that assures the receiver that an incoming message is authentic (that it comes from the alleged sender and that it has not been altered).
- The transaction sequence begins when the sender types an e-mail and MD5 is used to generate a digital signature of the e-mail.

- The digital signature is then encrypted with RSA using the sender's private key, and the result is prepended to the e-mail. The receiver uses RSA with the sender's public key to decrypt and recover the digital signature.
- The receiver then generates a new digital signature for the recovered e-mail and compares it with the decrypted digital signature.
- If the two match, the message is accepted as authentic. All this is done automatically by the program.
- The combination of MD5 and RSA provides an effective digital-signature scheme.

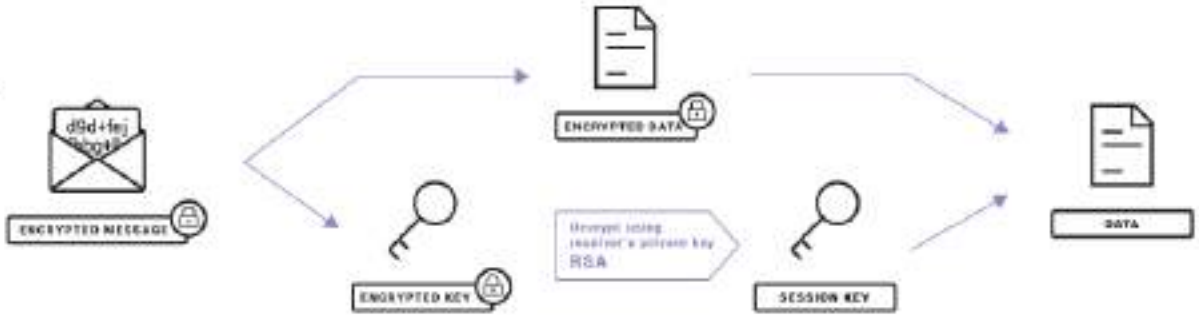
- RSA's strength assures the receiver that only the possessor of the private key can generate the signature, and MD5's strength assures the receiver that no one else can generate a message that matches the content of the original message.
- PGP provides confidentiality by encrypting messages to be transmitted or to be stored locally as files.
- In both cases, the conventional encryption algorithm known as IDEA (international data encryption algorithm) is used.
- Relatively new, IDEA is considered to be much stronger than the widely used DES and is not subject to government-imposed cryptographic controls.

- Any secret-key encryption system must address the problem of key distribution; in PGP, each key is used only once. That is, a new key is generated as a random number for each message. This key is bound to the message and transmitted with it.
- Let's examine the process. When the sender generates a message, the system generates a random 128-bit number as a session key for that message only.
- The message is encrypted, using IDEA with the session key. The session key is encrypted with RSA, using the receiver's public key, and is prepended to the message.
- The receiver uses RSA with private key to decrypt and recover the session key. The session key then decrypts the message.
- IDEA is much faster than RSA and reduces message encryption time as only the key is encrypted using RSA.

ENCRYPT



DECRYPT



PROS	CONS
• Extremely secure	• Not user-friendly
• OpenPGP is free to use	• Requires software
• Improves cloud security	• No anonymity


Thank you

E-COMMERCE AND WORLD WIDE WEB

Dr P.V. Praveen Sundar
Assistant Professor,
Department of Computer Science
Adhiparasakthi College of Arts & Science,
Kalavai.

World Wide Web

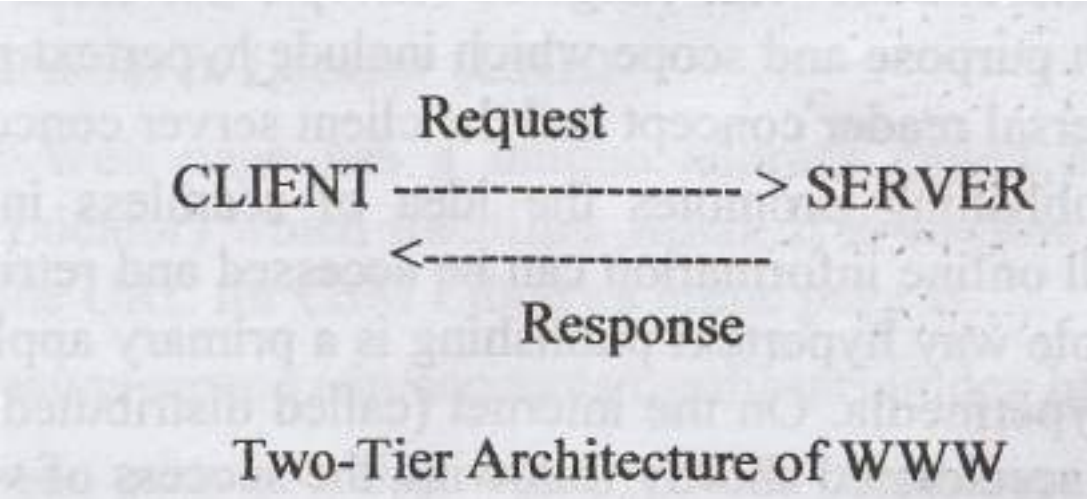
- WWW is the part of the internet that supports multimedia and contains of a collection of linked documents.
- Web is a system of interlinked hypertext documents accessed via the internet.
- Web is an application that uses the internet for communications with TCP/IP as the underlying transport mechanism.
- A web is a huge collection of pages of information linked to each other around the globe.

- Web uses the HTTP to transmit the data.
- Web pages are stored on web server and send them to a client computer as and when it requests for them.
- Internally, a web page is a computer file stored on the disk of the server. The file contains tags written in the codified form. These tags decide how the file would look when displayed on the screen. The website address is called as Uniform Resource Locator (URL).
- A website is a collection of web pages. These pages on a website are stored digitally on a web server.

World Wide Web as Architecture

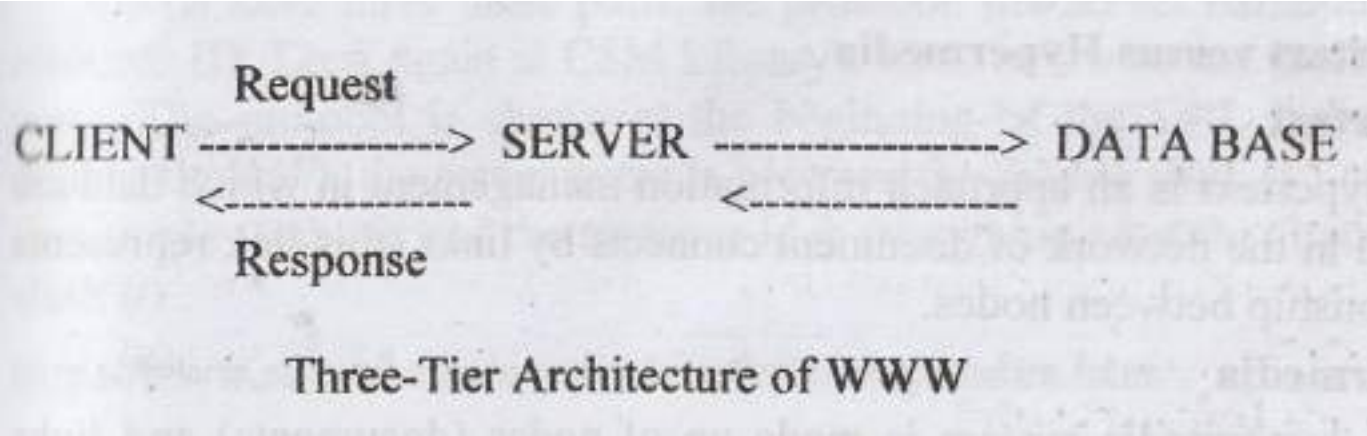
- WWW is a hypertext-based system that provides a uniform and a user-friendly interface for accessing the resources on the Internet.
- It is an information space in which the items of interest, referred to as resources, are identified by global identifiers called Uniform Resource Identifiers (URI).
- The architecture of WWW is two tiered. It consists of the client and the server. The client (web browser) requests for a web page. This page is retrieved from the server. The architecture depends on three key standards:
  - HTML for encoding document content,
  - Uniform Resource Locator (URL) for naming remote information objects in a global namespace, and
  - HTTP for staging the transfer.

- The following figure shows the two tired architecture of WWW.



Two-Tier Architecture of WWW

- If the web pages are interacting with the database, then the architecture becomes three tiered, as shown in the following figure.



Three-Tier Architecture of WWW

Working of the WWW

- The WWW works on a Client-server approach. Whenever the user wants to retrieve a webpage, the www works as follows:
  - A user enters the URL of the webpage in the address bar of the web browser.
  - The web browser requests the Domain Name Server for the IP address corresponding to www.google.com.
  - After receiving the IP address, the browser sends the request for the webpage to the Internet using HTTP protocol which specific the way the browser and Web Server communicates.

- The Internet Routers send the request to the intended web server.
- Then the web server receives the request using HTTP protocol. It then examines the hard disk or memory and if the requested file is found it returns it back to the web browser and closes the Http connection.
- The Web browser then interprets the file and displays contents of the webpage in the browser window.

Web background: Hypertext publishing

- Hypertext publishing promotes the idea of seamless information world in which all online information can be accessed and retrieved.
- Hypertext is an approach to information management where the data is stored in network of documents and these documents are connected by links.
- Here the documents are taken as nodes and links represent the relationship between the documents and nodes.
- The nodes or documents may contain text, graphic, animation, audio video, images or programs.

- The nodes, and in some systems network itself, are meant to be viewed through an interactive browsers and are manipulated, through a structure editor.
- Nodes are connected to other nodes by links. The node from which the link gets started is known as reference or anchor and the node at which it ends is called referent.
- The movement between nodes is made possible by activating links which connect related concepts or nodes.
- Links can be of bi-directional providing backward traversals, referential, hierarchical.
- In some browsers hypertext is a very simple context lies in its ability to produce large, complex, richly connected and cross referenced bodies of information.

Hypermedia

- A hypermedia system is made of nodes(documents) and links (pointers).
- Hypermedia is an extension of the term hypertext.
- Hypermedia is a nonlinear medium of information that includes graphics, audio, video, plain text and hyperlinks.
- The term was first used in a 1965 article written by Ted Nelson.
- The World Wide Web is a classic example of hypermedia.
- The most common type of hypermedia is an image link. Photos or graphics on the Web are often linked to other pages.

Benefits of Hypermedia

- Hypermedia documents are much more flexible than conventional documents.
- Hypermedia documents offer video sequences animation and even compute programs.
- Its power and appeal increases when it is implemented in computing environments that include network, micro computers, work stations, high resolution displays and large online storage.
- It provides dynamic organization.
- Hypermedia systems provide non-linear innovative way accessing and restricting network documents.

Uniform Resource Locator (URL)

- Every Web page has a unique address called a URL (Uniform Resource Locator) which identifies where it is located on the Web.
- For example, the URL for APCAS home page is: http://www.apcas.in/home/
- The basic parts of a URL often provide "clues" to where a web page originates and who might be responsible for the information at that page or site.
- URLs have three basic parts: the protocol, the server name and the resource ID.

- Look again at APCAS's URL below to see these three parts.
- The protocol is shown at the beginning of the URL before the double slash (//); the server name is between the double slash (//) and the first single slash (/); and the resource id is everything after the first single slash(/).

  http://www.apcas.in/home/

  protocol |Server Name |resource id

- Let's examine each part of this URL:

First part: protocol (http://)

- The protocol identifies the method (set of rules) by which the resource is transmitted. All Web pages use Hypertext Transfer Protocol (HTTP). Thus, all web URL's begin with http://.

- **Second Part: Server Name**
- The server name identifies the computer on which the resource is found.
- This part of the URL commonly identifies which company, agency or organization may be either directly responsible for the information, or is simply providing the computer space where the information is stored.
- Web server names often begin with the letters www, but not always.
- The server name always ends with a dot and a three-letter or two-letter extension called the domain name.

- The domain is important because it usually identifies the type of organization that created or sponsored the resource. Sometimes it indicates the country where the server is located.
- The most common domain names are:
  - .com which identifies company or commercial sites
  - .org for non-profit organization sites
  - .edu for educational sites
  - .gov for government sites
  - .net for Internet service providers or other types of networks.

- If the domain name is two letters, it identifies a country, e.g. .us for the United States,
  - .uk for the United Kingdom,
  - .au for Australia,
  - .mx for Mexico or
  - .ca for Canada.
- The server name for our college website is: www.apcas.in. The server name may also be the name of a website.
- Websites can be either all of the pages on one server(computer) or all of the pages under a specific sub directory on a server.

- **Third part: resource ID (home/)**
- The resource ID is the name of the file for the page and any directories or subdirectories under which it is stored on the specified computer.
- The resource ID for our College's homepage is: /home.htm. (A "homepage" is the opening or main page for any web site that provides links to all of the other pages on the site.)
- The part of the resource ID after the last slash (/) is the file name for the specific page or other resource.
- The file name ends with a three or four letter designation that specifies the file type (e.g., .htm or .html for A standard Web page, .jpg or .gif for common graphic files.)

HTTP

- Hypertext Transfer Protocol(HTTP) is an internet standard or set of rules that allows the exchange of information on the World Wide Web.
- HTTP defines how messages are formatted and transmitted and what actions Web servers and browsers should take in response to various commands.
- For example, when anyone enter a URL, in browser, this actually sends an HTTP command to the Web server directing it to fetch and transmit the requested Web page. Sending and receiving messages can be done through HTTP.

CGI (Common Gateway Interface)

- The Common Gateway Interface (CGI) provides the middleware between WWW servers and external databases and information sources.
- The Common Gateway Interface (CGI) is a standard way for a Web server to pass a Web user's request to an application program and to receive data back to forward to the user.
- When the user requests a Web page (for example, by clicking on a highlighted word or entering a Web site address), the server sends back the requested page.

- However, when a user fills out a form on a Web page and sends it in, it usually needs to be processed by an application program.
- Web server typically passes the form information to a small application program that processes the data and may send back a confirmation message. This method or convention for passing data back and forth between the server and the application is called the Common Gateway Interface (CGI).
- It is part of the Web's Hypertext Transfer Protocol (HTTP).

HTTPD Servers (Hypertext Transfer Protocol Domain)

- The servers that are used to publish information via WWW servers are called HTTPD servers.
- While choosing a web server flexibility, ease of administrator, security features, familiarity and performance are considered.
- It is important to evaluate the tasks for which the web server is used.
- A server used for Internet based marketing & technical support task will need more powerful server than the web server used internally within a firewall for distributing memos and bulletins.
- HTTPD servers are ideal for companies that want to provide multitude of services ranging from product information to technical support.

Hyper Text Markup Language (HTML)

- HTML stands for Hyper Text Markup Language,.
- HTML is used to create document on the World Wide Web.
- It is simply a collection of certain key words called 'Tags' that are helpful in writing the document to be displayed using a browser on Internet.
- It is a platform independent language that can be used on any platform such as Windows, Linux, Macintosh, and so on.
- To display a document in web it is essential to mark-up the different elements (headings, paragraphs, tables, and so on) of the document with the HTML, tags.

- A browser understands and interprets the HTML tag, identifies the structure of the document and makes decision about presentation of the document.
- HTML also provides tags to make the document look attractive using graphics, font size and colors.
- User can make a link to the other document or different section of the same document by creating Hypertext Links.
- Using this language we can create web pages in the internet.
- Using any web browser we can execute the HTML files. The result of the execution will appear as a web page.

E-PAYMENTS (INTRODUCTION)

Dr P.V. Praveen Sundar
Assistant Professor,
Department of Computer Science
Adhiparasakthi College of Arts & Science,
Kalavai.

Electronic Payment Systems

- An Electronic Payment System (EPS) is a system of financial exchange between buyers and sellers in the online environment that is facilitated by a digital financial instrument (such as encrypted credit card numbers, electronic cheques or digital cash) that is backed by a bank or an intermediary, or by a legal tender.
- Electronic Payment always involves a payer and payee who exchange money for goods or services.
- Methods of electronic payments include credit cards, debit cards and the ACH (Automated Clearing House) network.
- The ACH system comprises direct deposit, direct debit and electronic checks (e-checks).

- Issues of trust and acceptance play a more significant role in the e-commerce world than in traditional businesses as far as payment systems are concerned.
- Traditionally, a customer sees a product, examines it, and then pays for it by cash, cheque, or credit card (Figure 4.5a)
- In the e-commerce world, in most cases the customer does not actually see the concrete product at the time of transaction, and the method of payment is performed electronically.

- EPSs enable a customer to pay for the goods and services online by timing integrated hardware and software systems.
- The main objectives of EPS are to increase efficiency, improve security, and enhance customer convenience and ease of use.
- Although these systems are in their Immaturity, some significant development has been made.
- There are several methods and tools that can be used to enable EPS Implementation (figure 4.6):

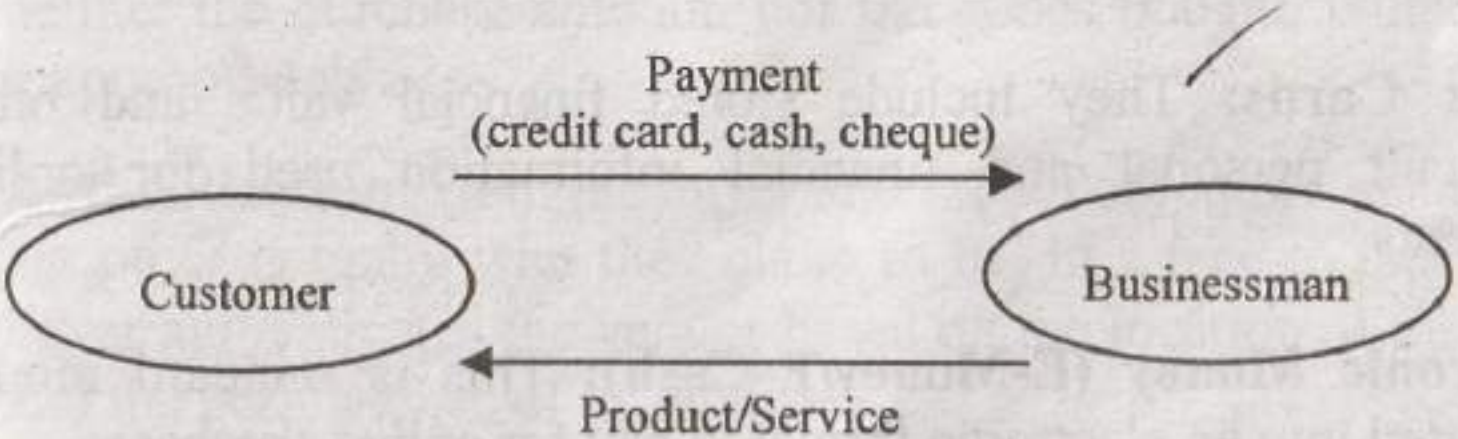


Figure 4.5: Traditional Payment Scheme

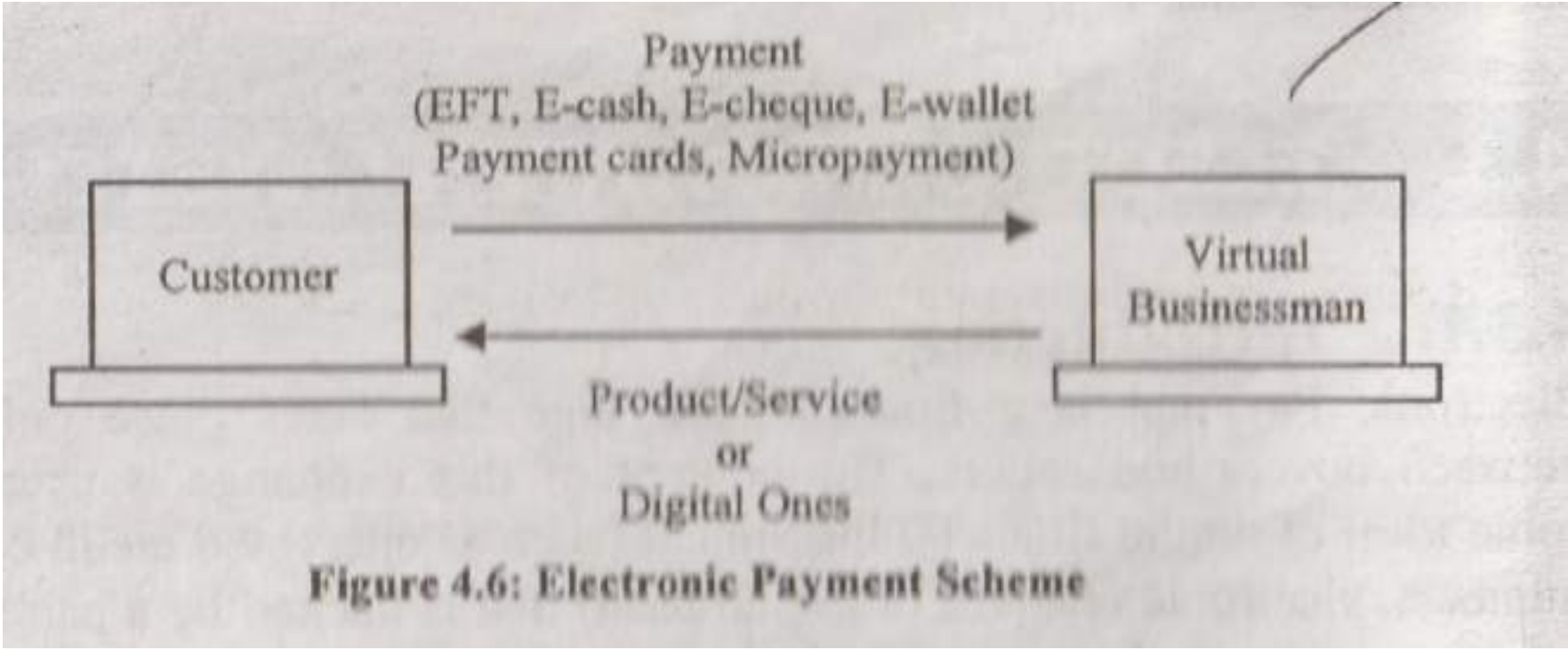


Figure 4.6: Electronic Payment Scheme

- While customers pay for goods/services by cash, cheque, or credit cards in conventional businesses, online buyers may use one of the following EPSs to pay for products/services purchased online:
  - **Electronic Funds Transfer (EFT):** It involve electronic transfer of money by financial institutions.
  - **Payment Cards:** They contain stored financial value that can be transferred from the customer's computer to the businessman's computer.
  - **Credit Cards:** They are the most popular method used in EPSs and are used by charging against the customer credit.
  - **Smart Cards:** They include stored financial value and other important personal and financial information used for online payments.

- **Electronic Money (E-Money/E-Cash):** This is standard money converted into an electronic format to pay for online purchases.
- **Online Payment:** This can be used for monthly payment for internet, phone bills, etc.
- **Electronic Wallets (E-Wallets):** They are similar to smart cards as they include stored financial value for online payments.
- **Micropayment Systems:** They are similar to e- wallets in that they include stored financial value for online payments; on the other hand, they are used for small payments.
- **Electronic Gifts:** They are one way of sending electronic currency or gift certificates from one individual to another. The receiver can spend these gifts in their favourite online stores provided they accept this type of currency.

Need of Electronic Payment Systems

- Three factors are stimulating the development of electronic payment systems:
  - Reduced operational and payments processing costs,
  - Growing online commerce, and
  - Decreasing the costs of technology.
- The central impact for e-commerce and e-business is to provide a more efficient service, primarily in terms of costs.

Requirements of Electronic Payment Systems

The general requirements of payment systems are:

- **Confidentiality:** The user expects a secure system of payment. The system must have a set of special characteristics that the customer can depend on. For example, when the user gives the credit card number to a merchant, the former expects confidentiality that the number will only be disclosed to those who have a legitimate need to know it. It could for instance be disclosed to the bank issuing the payment.
- **Integrity:** The payment system requires integrity to ensure that neither the purchase amount, nor the goods bought, will be altered inappropriately.

- **Authentication:** Both the buyer and the seller require assurance that the other is really who they claim to be.
- In a face-to-face deal, the buyer authenticates the vendor based on the location of the business and the permanence of its facilities.
- On the part of the vendor, if the customer is not paying by cash, the vendor usually asks for the customer's driver's license and compares the signatures on the charge slip and that on the license. In this manner the seller authenticates the customer.

- **Authorization:** Authorization allows the merchant to determine if the buyer actually has funds to pay for the purchase.
- The merchant verifies that the customer's bank account has sufficient balance to honor the cheque amount.
- In case of a credit card transaction, the merchant obtains the approval from the credit card clearing house for the amount of the credit card purchase.

- **Safety:** Customers want to be sure that it is safe to provide credit/debit card number on Internet. They also want protection against fraud by sellers or by criminals posing as sellers.
- **Nonrepudiation:** Merchants need protection against the customer's unjustified denial of placing an order. On the other hand, customers need protection against merchants unjustified denial of payments made. (such denials, of both types are called as repudiation.)

- **Assurance:** The customer on his part might want to be sure that the merchant is competent and worthy of his trust. This might involve some kind of business license, endorsements from other customers or even surety bonds for more complex transactions.
- **Privacy:** Many customers want their identity to be secured. They want to make sure others do not know what they buy. Some prefer complete anonymity, as it is possible with cash payments. For example, a business conducting research might not want its competitors to know the details of its purchases.

Advantages of Electronic Payment Systems

Convenience: Electronic payment is very convenient for the consumer.

- In most cases, the user need to enter their account information - such as your credit card number and shipping address once.
- The information is then stored in a database on the retailer's Web server. When the user come back to the Web site and just log in with his username and password. Then continue the shopping.
- Completing a transaction is as simple as clicking through mouse: the only thing the user has to do is confirm their purchase.

- **Low Cost:** Electronic payment lowers costs for businesses.
- The more payments they can process electronically.
- The less they spend on paper and postage.
- Offering electronic payment can also help businesses improve customer retention.
- A customer is more likely to return to the same e-commerce site where his or her information has already been entered and stored.

Increased Speed and Convenience:

- E-payment is very convenient compared to traditional payment methods such as cash or check.
- Since users can pay for goods or services online at any time of day or night, from any part of the world, customers don't have to spend time in a line, waiting for their turn to transact.
- Also they don't have to wait for a check to clear the bank so they can access the funds they need to shop.
- E-payment also eliminates the security risks that come with handling cash money.

- **Increased Sales:** As internet banking and shopping become widespread, the number of people making cash payments is decreasing.
- e-payment enables businesses to make sales to the customers who choose to pay electronically and gain a competitive advantage over those that only accept traditional methods.

- **Staying in control:** e-payment systems helps you to stay in control of transactions. The account shows all transaction details, including the date, amount and the name of the retailer. It's therefore easy to see where your money is going, and you can check transaction details without waiting for a monthly statement.

Disadvantages

- **Security:** Although security measures such as symmetric encryption are in place to make e-payment safe and secure, it is still vulnerable to hacking.
- Fraudsters use phishing attacks to trick unsuspecting users into providing the log-in details of their e-wallets, which they capture and use to access the victims' personal and financial information.
- Malware and other hacking attempts can track keystrokes in order to copy account passwords and access payment information.
- Inadequate authentication also troubles e-payment systems. Without superior identity verification measures like biometrics and facial recognition, anyone can use another person's cards and e-wallets and get away without being caught.

- **Payment System Collision:** Because online payment systems are new and global in their perspective, problems can occur when it comes to applying them to all e-commerce businesses.
- Some types of payment that customers are used to depending on may not be available in other countries, even when purchasing online from those countries is an option.
- E-payments can also struggle to match up the values of different currencies or different types of bank account. Usually, the user have to pay a transaction fee.
- Internet connection failure can leave companies unable to make or accept payments.

Difference between Conventional and Electronic Payment Systems

Aspect	Conventional System	Electronic Payment System
Transfer Time needed	Days or week	Instantaneous
Delivery mode	Physical	Electronic
Mistakes	Difficult in tracing	Easy to trace
Speed	Slower	Faster
Transaction cost	Higher due to physical handling and human involvement	Lower due to electronic handling without much human involvement
Fraud	Yes, possibilities present	Cyber thefts due to cyber criminals

Electronic Funds Transfer

- Electronic funds transfer (EFT) is the electronic transfer of money from one bank account to another, either within a single financial institution or across multiple institutions, via computer-based systems, without the direct intervention of bank staff.
- According to the United States Electronic Fund Transfer Act of 1978, **EFT is defined as "any transfer of funds initiated through an electronic terminal, telephone, computer (including on-line banking) or magnetic tape for the purpose of ordering, instructing, or authorizing a financial institution to debit or credit a consumer's account".**

- EFT utilizes computer and telecommunication components both to supply and to transfer money or financial assets.
- Transfer is information-based and intangible.
- Thus EFT stands in marked contrast to conventional money and payment modes that rely on physical delivery of cash or checks (or other paper orders to pay) by truck, train, or airplane.
- Work on EFT can be segmented into three broad categories:
  - Banking and financial payments.
  - Retailing payments.
  - On-line electronic commerce payments.

- Banking and financial payments
  - Large-scale or wholesale payments (Example : Bank-to-Bank transfer).
  - Small-scale or retail payments (Example: ATM and cash dispensers).
  - Home banking (Example: bill payment).
- Retailing payments
  - Credit cards (e.g., VISA, MasterCard, Maestro, Rupay)
  - Private label credit/debit cards.

- On-line electronic commerce payments
  - Token-based payment systems
    - Electronic cash (e.g., DigiCash)
    - Electronic checks (e.g.', NetCheque)
    - Smart cards or debit cards.
  - Credit card-based payment systems
    - Encrypted credit cards (e.g., World Wide Web form-based encryption)
    - Third-party authorization numbers (e.g., First Virtual)

Advantages of EFT

- Reduces cheque bouncing.
- Clerical work reduced in organization.
- A customer can access his account in hand held devices.
- Large financial transaction can be performed at a very fast rate.
- Less paper work
- Less human intervention.
- Security, Reliability and Integrity.

List of Banks Participating in Electronic Fund Transfer – (EFT)

1. State Bank of India (SBI)
2. State Bank of Bikaner & Jaipur (SBJ)
3. State Bank of Hyderabad (SBH)
4. State Bank of Indore (SBN)
5. State Bank of Mysore (SBM)
6. State Bank of Patiala (SBP)
7. State Bank of Saurashtra (SBS)
8. State Bank of Travancore (SBT)
9. Allahabad Bank (ALB)
10. Andhra Bank (ANB)
11. Standard Chartered Grindlays Bank
12. Bank of America NT & SA (BOA)
13. Bank of Baroda (BOB)
14. Bank of India (BOI)
15. Bank of Maharashtra (BOM)
16. The Bank of Rajasthan Ltd. (BOR)
17. Banque Nationale De Paris (BNP)
18. The Bassein Catholic Co op Bank Ltd. (BCH)
19. Canara Bank (CAB)
20. Central Bank of India (CBI)
21. CITI Bank N.A.(CIT)
22. The Citizen Co op Bank Ltd. (CCB)
23. Corporation Bank (COB)
24. The Cosmos Co op Bank Ltd. (CSM)
25. Credit Agricole Indosuez (CAI)
26. Dena Bank (DEB)
27. Deutsche Bank Ltd (DTB)
28. Development Credit Bank Ltd. (DCB)
29. The Federal Bank Ltd. (FBL)
30. The Global Trust Bank Ltd.
31. The Greater Bombay Co op Bank Ltd. (GBC)
32. The ICICI Bank Ltd.(Bank of Madura Merged with ICICI w.e.f. 12/03/2001)
33. Indian Bank (INB)

34. Indian Overseas Bank (IOB)
35. The Janata Sahakari Bank Ltd. Pune (JSB)
36. The Karnataka Bank Ltd. (KBL)
37. The Karur Vysya Bank Ltd. (KVB)
38. The Lakshmi Vilas Bank Ltd. (LVB)
39. Lord Krishna Ltd. (LKR)
40. The North Kanara Gaud Saraswat Brahmin Co op Bank Ltd. (NKC)
41. Oriental Bank of Commerce (OBC)
42. Punjab & Sind Bank (PSB)
43. Punjab Natrional Bank (PNB)
44. The Ratnakar Bank Ltd. (RTN)
45. The Saraswat Co op Bank Ltd. (SRC)
46. The South Indian Bank Ltd. (SIB)
47. ABN Amro Bank N.V.
48. Syndicate Bank (SYB)
49. UCO bank (UCO)
50. Union Bank of India (UBI)
51. United Bank of India (UNI)
52. The United Western Bank Ltd (UWB)
53. The UTI Bank Ltd (UTI)
54. Vijaya Bank (VJB)
55. The Vysya Bank Ltd. (VBL)
56. Hongkong & Shanghai Banking Corporation (HON)
57. The Punjab & Maharashtra Co op Bank Ltd. (PMB)
58. Indusind Bank Ltd. (IDS)
59. Sangali Bank Ltd. (SAN)
60. The Shamrao Vithal Co op Bank Ltd. (SVC)
61. The Kalupur Commercial Co op Bank Ltd. (KCC)
62. Oman International Bank S.A.O.G. (OIB)
63. The Maharashtra State Co op Bank Ltd. (MSCB)
64. HDFC Bank Ltd.
65. IDBI Bank Ltd.
66. Mumbai GPO (GPO)
67. The Dhanalakshmi Bank Ltd.
68. The Bank of Punjab Ltd.
69. City Union Bank Ltd.

70. Mandvi Co op Bank Ltd.
71. The A.P. State Co op Bank Ltd.
72. The Bank of Nova Scotia (Scotiabank)
73. The Janakalyan Sahakari Bank Ltd.
74. Ahmedabad Disrict Co op Bank Ltd.
75. The Catholic Syrian Bank Ltd.
76. The Bank of Tokyo Mitsubisi Ltd.
77. The SBI Commercial & International Bank Ltd.

Electronic Data Interchange (EDI)

- Electronic Data Interchange (EDI) is the computer-to-computer exchange of business documents in a standard electronic format between business partners.
- According to International Data Exchange Association (IDEA), EDI is defined as " **The transfer of structured data, by agreed message standards, from one computer system to another, by electronic means.** " This definition of EDI has four elements, all of which are essential to an EDI system:

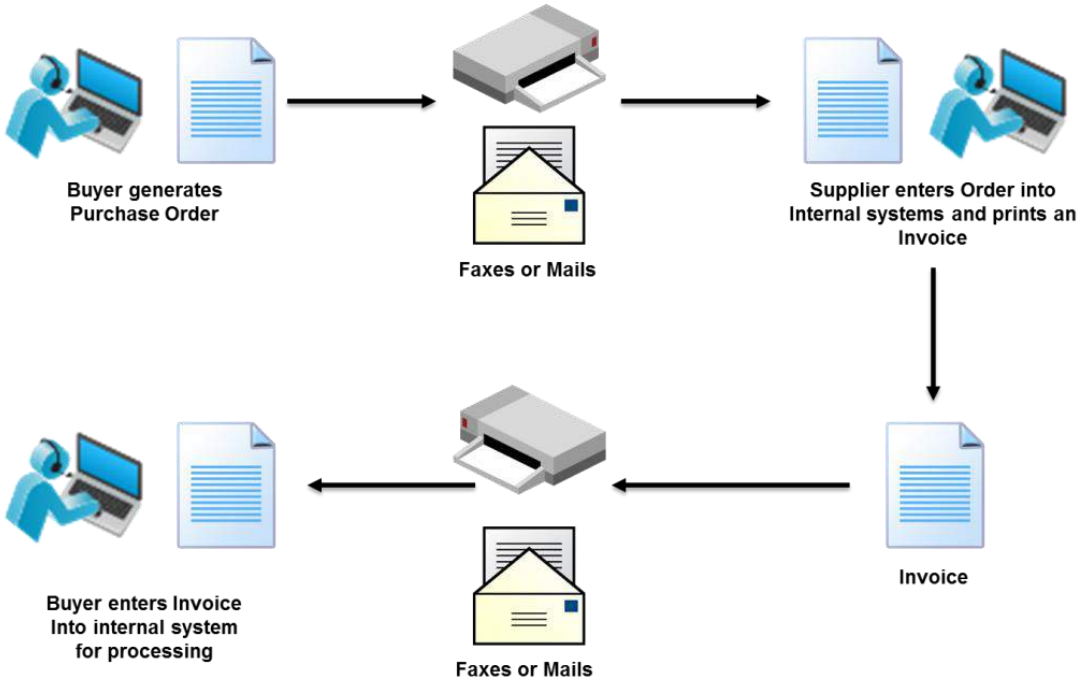
- **Computer-to-computer–**
- EDI replaces postal mail, fax and email. While email is also an electronic approach, the documents exchanged via email must still be handled by people rather than computers.
- Having people involved slows down the processing of the documents and also introduces errors.
- Instead, EDI documents can flow straight through to the appropriate application on the receiver's computer and processing can begin immediately. A typical manual process looks like this, with lots of paper and people involvement:

- **Business documents** – These are any of the documents that are typically exchanged between businesses.
- The most common documents exchanged via EDI are purchase orders, invoices and advance ship notices.
- But there are many, many others such as bill of lading, customs documents, inventory documents, shipping status documents and payment documents.

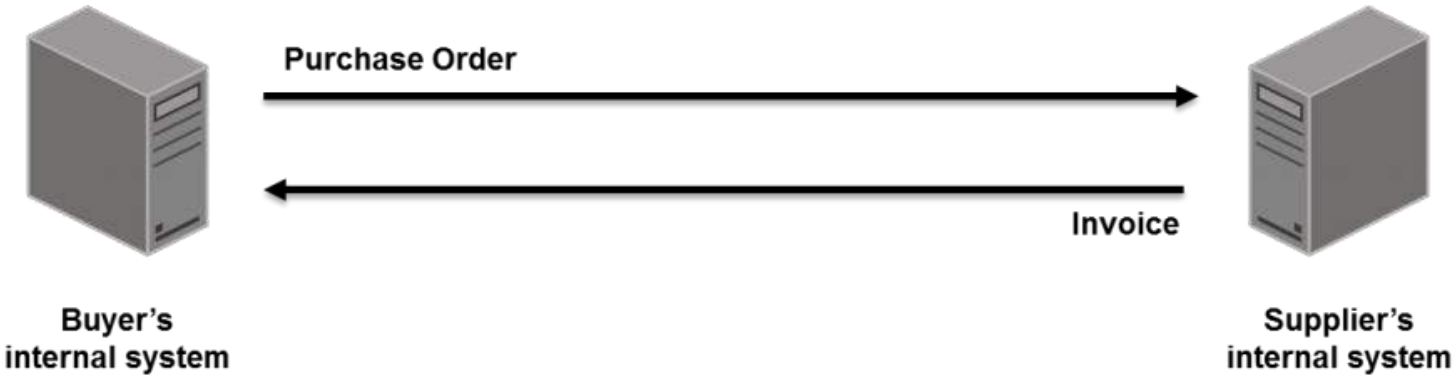
- **Standard format–** Because EDI documents must be processed by computers rather than humans, a standard format must be used so that the computer will be able to read and understand the documents.
- A standard format describes what each piece of information is and in what format (e.g., integer, decimal, mmddyy).
- Without a standard format, each company would send documents using its company-specific format and, much as an English-speaking person probably doesn't understand Japanese, the receiver's computer system doesn't understand the company-specific format of the sender's format.

- **Business partners –** The exchange of EDI documents is typically between two different companies, referred to as business partners or trading partners.
- For example, Company A may buy goods from Company B. Company A sends orders to Company B. Company A and Company B are business partners.

Manual Document Exchange



EDI


Purchase Order
Invoice
Buyer's internal system
Supplier's internal system

- **Structured Data:-** EDI transactions are composed of codes, values, short pieces of text. Each element has a strictly defined purpose. For example, an order has codes for the customer, product, quantity ordered etc.
- **Agreed Message Standards:** The EDI transaction has to have a standard format. The standard is a not just agreed between the trading partners but is a general standard agreed at a national or international level.
- **From one Computer System To Another:** The EDI message sent is between two computer applications. There is no requirement for people to read the message or re-key it into a computer system.
- **By Electronic Means:** The EDI message is sent electronically i.e. by using networks specifically designed for EDI.

Use of EDI

- The data from one computer is normally not in a form suitable to be entered directly into another computer.
- The data may have to be arranged differently before it can be entered into another computer or some items of data may not be needed at all.
- With EDI, all the data is converted into an agreed standard format before it is sent over the networks.
- The computer that receives the data can then extract the information it requires.

- Using EDI implies three things:
  - Information is transferred electronically rather than on paper.
  - Information is transferred between trading partners who have negotiated trading agreements and have formalized their data transfer system.
  - Information that is transferred complies with agreed standards for the format of the content and the transmission control mechanisms.

How EDI Works?

- The Basic Steps of EDI are as follows:
- **Preparation of Electronic Documents:** The first step in any sequence of Electronic Data Interchange is the collection and organization of data. Rather than printing out purchase orders, their system builds an electronic file of purchase orders.
- **Outbound Translation:** The next step is to translate this electronic file into a standard format. The resulting data file will contain a series of structured transactions related to the purchase orders. EDI translation software will produce a separate file for each manufacturer.

- **Communication:** The computer automatically makes a connection with the Value Added Network, and transmits all the files that have been prepared. The VAN will process each file, routing it to the appropriate electronic mailbox for each manufacturer.
- **Inbound Translation:** The manufacturers retrieve the files from their electronic mailboxes at their convenience, and reverse the process that went through, translating the file from the standard format into the specific format required by the manufacturer's application software.
- **Processing Electronic Documents:** Each manufacturer will process the PO's received in their internal application systems.

Basics of EDI

- There are three major components of EDI.
  - Trading Partners
  - Translation software
  - Communications

Trading Partners

- Business organizations that agree to exchange business information, data and documents via EDI.

Translation Software

- It is a dual purpose software. It converts file to or from an EDI format is called a document. Document contains EDI messages.

Communications

- The transmission and reception of a document between trading partners using compatible hardware and software.

Layered Architecture of EDI

- EDI architecture provides a framework that enables you to standardize the information which can be easily exchanged between and within business organizations and government entities using electronic channels.
- EDI architecture specifies 4 layers:-
  1. Semantic (application layer)
  2. Standard translation layer
  3. Packing (transport) layer
  4. Physical n/w infrastructure layer.

EDI Semantic Layer	Application Level Services	
EDI Standard Layer	TRADACOMS, EDIFACT, ANSI X12	
EDI Transport Layer	Electronic Mail	X.435, MIME
	Point to Point	FTP,TELNET
	World Wide Web	HTTP
Physical Layer	Dialup lines, Internet, I-way.	

- **Semantic Layer:** It describes the business application that is driving EDI.
- For a procurement application, this translates into requests for quotes, price quotes, acknowledgements & purchase orders involves.
- The information seen at this layer must be translated from a company specific from to a more generic form so that it can be send to various trading partners, who could be using a variety of software applications at this end.

- When a trading partner sends a document, the EDI translation software converts the proprietary format into a standard mutually agreed on by the processing system.
- When a company receivers the document, their EDI translation software automatically changes the standard format into proprietary format of their document processing software so that company can manipulate the information in whatever way it chooses to.
- **Physical Network Infrastructure Layer:** It describes the physical devices which involved in transaction. They use various devices like dialup systems, internet, I-way.

- **Standards Translation Layer:-** It specify business form structure and it also influence the content at application layer.
- The most two important standards are:-
  - EDIFACT
  - ANSI X12
- **Packing (Transport layer):-** it corresponds closely with the non-electronic activity of sending a business form from one company A to company B.
- The business form could be sent via regular postal service, registered mail, certified mail or private carrier such as United Parcel Service (UPS) or simply faxed between the companies.
- Generally EDI transport layer chooses email as a carrier services.

EDI Model/Building Blocks of EDI

- EDI model required for sending or receiving EDI messages are shown in figure.
- The three components of EDI Models are:
  - EDI Standards
  - EDI Software
  - Third Party Networks

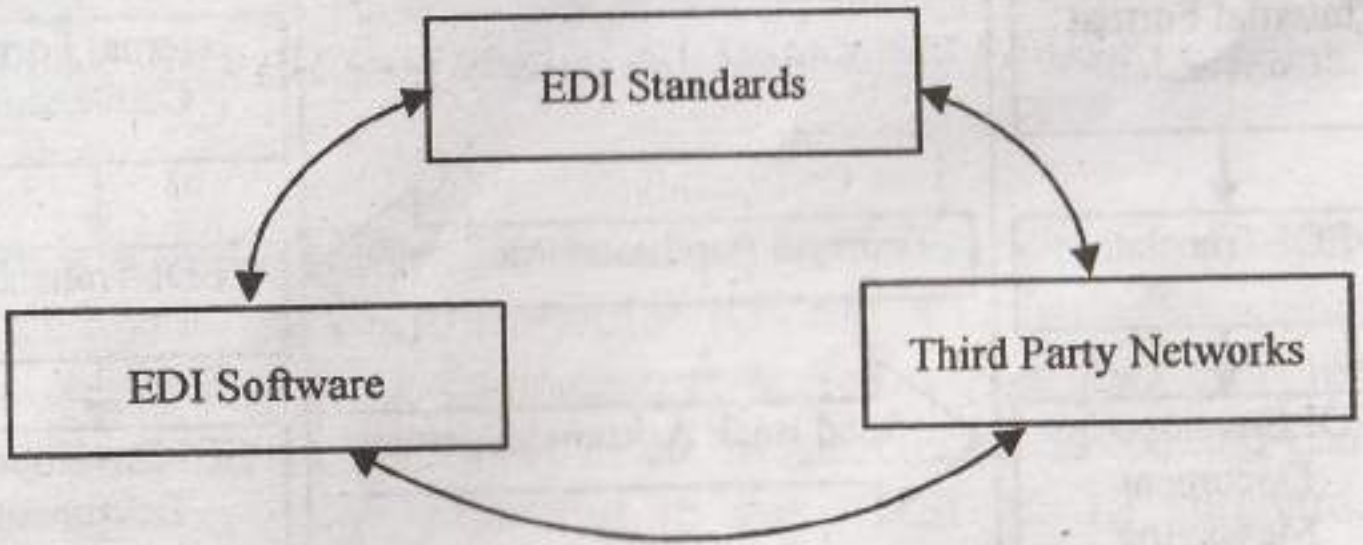


Figure 4.8: EDI Model

EDI Standards

- Using EDI, a business application on the computer of one organization can communicate directly with the business application on the computer of another organization.
- To ensure that this exchange of information is independent of hardware, software or the nature of implementation at either of these two organizations, it is necessary to extract data from the business application and to transform it into a standard format, which is widely acceptable.
- This data when received at the destination is interpreted and automatically delivered to the recipient application in an acceptable form.

- The exchange of business documents in a commonly agreed structured format necessitated the development of EDI standards. EDI standards are basically data standards in the sense that they lay down the syntax and semantics of the data being exchanged.
- EDI standard provides or attempts to provide, a standard for data interchange that is:
  1. Ready formulated and available for use;
  2. Comprehensive in its coverage of the data requirements for any given transaction;
  3. Independent of hardware and software; and
  4. Independent of the special interest of any party in the trading network.
- EDI Standards provide a common language for the interchange of standard transactions.

Categories of EDI Standards

- Over a period of time two major EDI standards have evolved:
- **ANSI X12:** ANSI X12 was developed for the American National Standards Institute (ANSI) by the Accredited Standards Committee (ASC) in 1979.
- The aim was to develop uniform standards for inter-industry electronic exchange of business transactions.
- The X12 standard defines a set of documents, referred to as transaction sets, for a wide range of business transaction forms.

- Each transaction set is given a numeric code and each transaction set is used and for defining the transfer of a single document (purchase order, manifest, etc.) between the computers of two trading partners.
- The data embedded in a transaction set conveys the same information that is contained in the printed version of the document; usually, it is a subset of the whole information on the printed version.

- The printed version of the document can be thought of as containing three distinct types of information:
  - **Header:** It contains the information that is common to the whole document such as date; from address; to address; terms and conditions, etc.
  - **Detail:** It refers to line items that describe the actual business transaction. In case of a purchase order, it may contain item number, description, quantity ordered, and price information.
  - **Summary:** It refers to the control information and other components that refer to the complete transaction. In case of a purchase order, it may refer to order value.

- **EDIFACT:** EDIFACT stands for Electronic Data Interchange For Administration, Commerce and Transport.
- EDIFACT is accepted as the international EDI standard that has been adopted by organizations wishing to trade in a global context.
- A standard set of syntax rules have been ratified by the United Nations.
- The EDIFACT standards cover transaction sets (the business documents that to transmit), data element directories and syntax rules which cover delimiter characters etc.

- An EDIFACT electronic transmission consists of one or more Interchanges.
- Each Interchange may consist of one or more Messages. These Messages contain segments of data relating to the business transaction.
- At each level, a series of enveloping data pairs keep track of the exchange structure.
- For trade purposes the documents include order, dispatch advice, invoice, payment order, and remittance advice.

- **TRADACOMS** is a UK-based standard, designed for domestic trade. TRADACOMS is the first standard was released in 1982, a number of years before EDIFACT appeared.
- The TRADACOMS standard encompasses 26 messages and each message is set out in a hierarchical structure.
- Unlike EDIFACT, TRADACOMS does not use a single message format, but instead uses multiple messages which constitute a transmission.
- A single order message would typically comprise an Order Header Message (ORDHDR), multiple Order Messages (ORDERS) and an Order Trailer Message (ORD TLR).
- Multiple individual order messages can repeat between the ORDHDR and the ORDTLR

EDI Software

- EDI software consists of computer instructions that translate the information from unstructured, company-specific format to the structured EDI format, and then communicate the EDI message from the sender to the recipient.
- EDI software also receives the message and translates from standard format to company-specific format, Thus the major functions of the EDI software are data conversion, data formatting and message communication.
- EDI software is available for mainframes, minicomputers and microcomputers.
- The requirements of EDI are:
  1. A computer
  2. A communication interface and
  3. Appropriate software

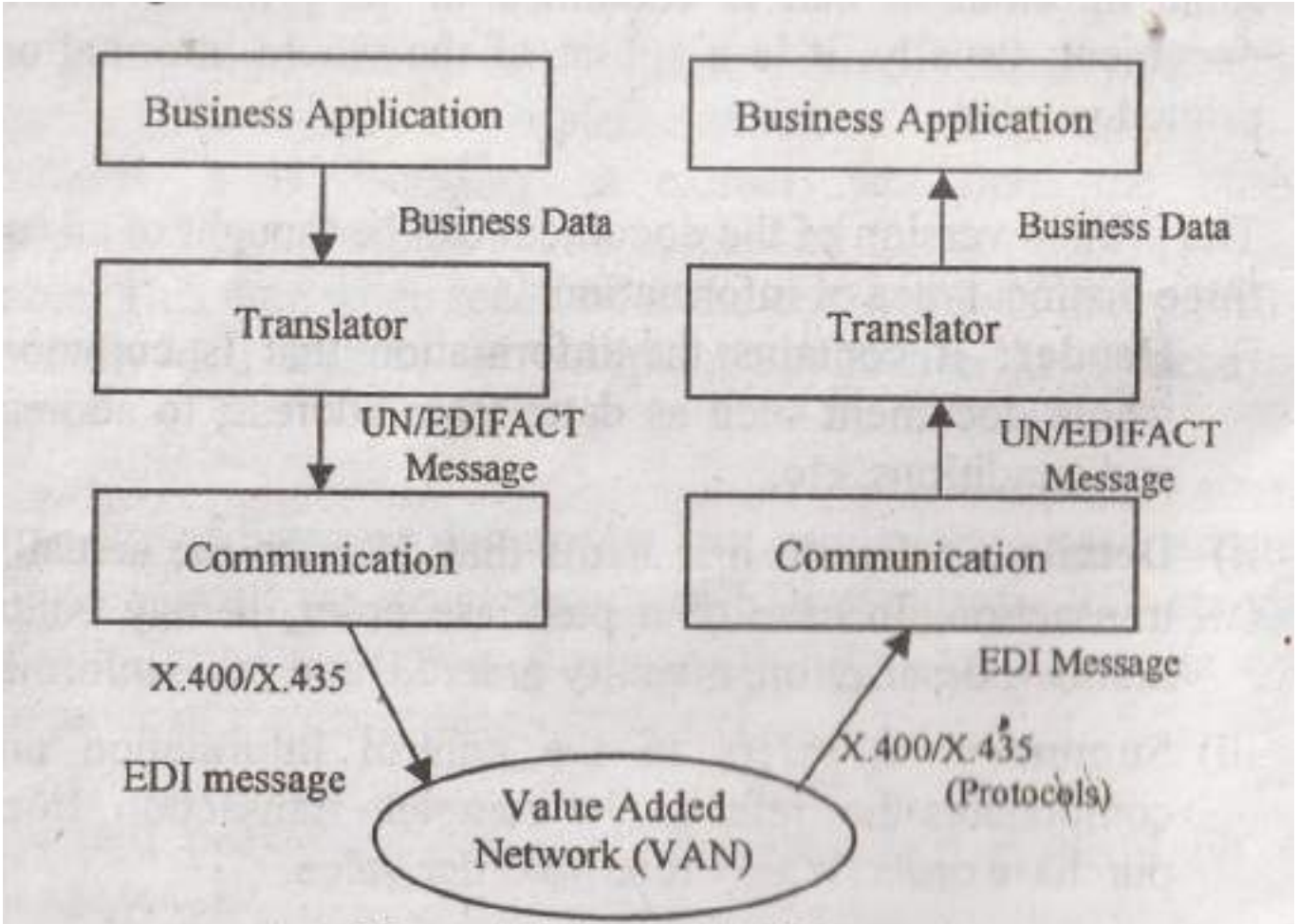


Figure 4.9: Layers in EDI

Layers in EDI Software

- There are the different layers in EDI software. These layers package the information and send it over the Value Added Network to the target business. The target business then reverses the process to obtain the original information.
- **EDI Business Application Layer:** The first step in the EDI process is to create a document in a software application. This software application then sends the document to an EDI translator, which automatically reformats the document into the agreed-on EDI standard.

- If these two pieces of software are from different vendors, it is important that the document preparation application integrates with the EDI translation software.
- If both the EDI translator and the business application are on the same type of computer, the data will move faster and more easily form one computer to another.
- The translator creates and wraps the document in an electronic envelope that has a mailbox id for the company's trading partner.
- The EDI wrapper software can be a module to the translator, a programming tool to write to different communications protocols or a separate application.

- **EDI Translation Layer:** Translation is an integral part of the overall EDI solution.
- The Translator describes the relationship between the data elements in the business application and the EDI standards.
- The Translator ensures that the data is converted into a format that the trading partner can use.
- **EDI Communication Layer**: The communications portion (which could be part of the translation software or a separate application), dials the phone number of the value-added network service provider or employs any other type of access method.

- The three different types of EDI access methods available are:
- **Direct Dial or Modem to Modem Connection:** Direct dial systems are the simplest and most common. The user has direct access to the partner's modem and communicates by using the modem to dial the modem of the other party.
- **Limited Third-Party Value-Added Network (VAN) Services:** A VAN (Value Added Network) is a communications network that typically exchanges EDI messages among trading partners.
- They offered store-and-forward mailboxes and were deployed to help trading and supply chain partners automate many business-to-business communications and thereby reduce the number of paper transfers needed.
- VANs often provide only the very basic technical services such as protocol conversion and data error detection and correction, directing and delivering EDI traffic to buyers and sellers.

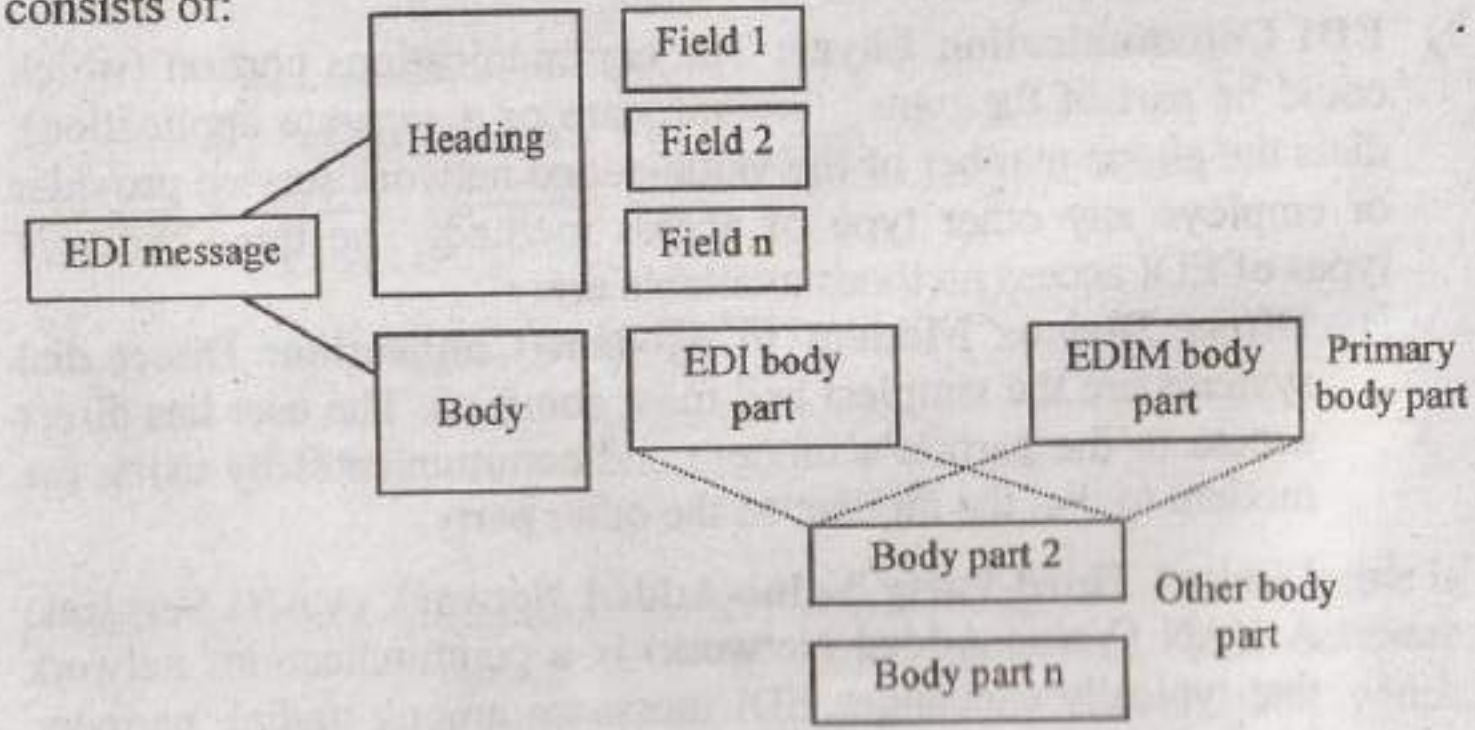
- **Full-Service Third Party VANs:** Full third-party services provide more that just communication between two or more parties.
- Electronic mailboxes and associated extra features are the heart of these third party services.
- Extra features include access control for security and document tracking, which allows users to track their own documents as they pass through the system.

Third Party Networks for Communications

- EDI documents are electronically exchanged over communication networks, which connect trading partners to one another.
- These documents are stored in user mailboxes on the network's EDI server from where they can be downloaded/ uploaded at the user's convenience.
- Value Added Networks (VANs) are third party communication networks established for exchanging EDI traffic amongst partners.

Communication of EDI Message

EDIM stands for EDI message. An EDIM is shown in **figure below**. It consists of:



- Heading: A set of heading fields each one of them is an information item giving a characteristic to the EDI message.
- Body: A sequence of one or more body parts of the message.
- The primary body part contains the EDI interchange itself or a forwarded EDI message,
- The other body parts that can be included in the EDIM are related to the primary body part and can be used to carry data such as voice, text or a drawing related to the interchanged.
- The EDI heading contains information required to provide services such as selective retrieval that fully satisfies EDI requirements.

Applications of EDI

- In a production department, EDI is used to share its computer design like CAD/CAM documents between its divisions located at various regions.
- In-a Manufacturing department, EDI is generally integrated with, its Supply Chain Management (SCM) - to connect the departments with its various suppliers.
- EDI is also used in standalone applications like tender tracking system, railway rolling, stock monitoring system etc.
- EDI is used in hospital industry and healthcare data interchange. system.
- Trade facilitation centers use EDI for uniting producers and consumers at Internet

Tangible Benefits of EDI

- Cost & time savings, Speed, Accuracy, Security, System Integration, Just-In-Time Support.
- Reduced paper-based systems, i.e. record maintenance, space paper, postage costs.
- Improved problem resolution & customer service.
- Expanded customer/supplier base or suppliers with no EDI program lose business.

Advantages of EDI

- **Reduction in data entry errors.** − Chances of errors are much less while using a computer for data entry.
- **Shorter processing life cycle** − Orders can be processed as soon as they are entered into the system. It reduces the processing time of the transfer documents.
- **Electronic form of data** − It is quite easy to transfer or share the data, as it is present in electronic format.
- **Reduction in paperwork** − As a lot of paper documents are replaced with electronic documents, there is a huge reduction in paperwork.
- **Cost Effective** − As time is saved and orders are processed very effectively, EDI proves to be highly cost effective.
- **Standard Means of communication** − EDI enforces standards on the content of data and its format which leads to clearer communication.

Limitations of EDI

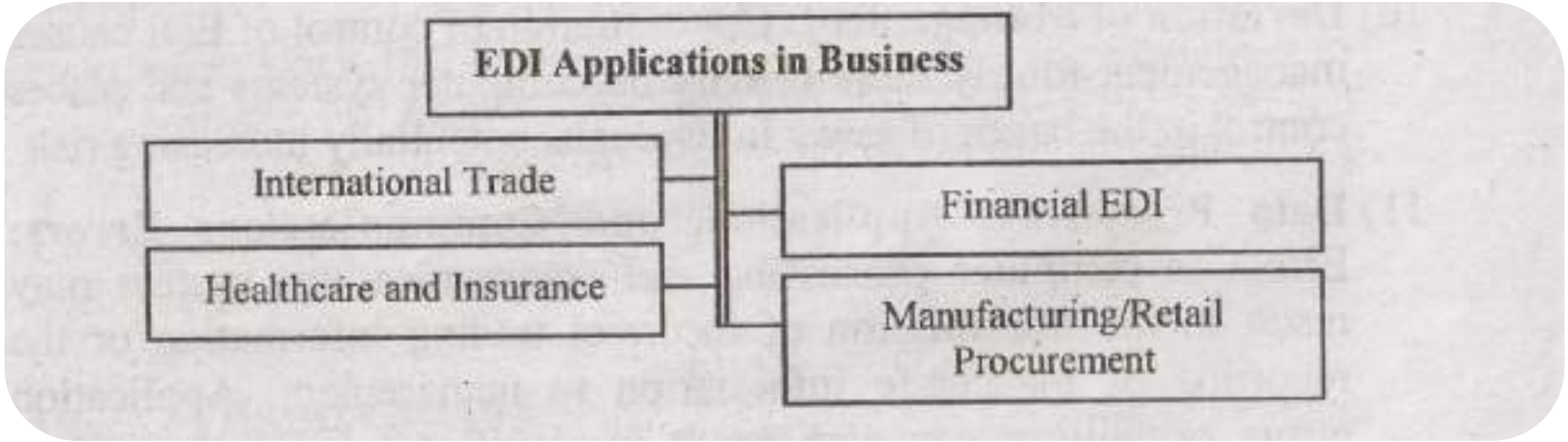
- Both buyers and sellers involved in an EDI use a standard, mutually agreed format for data interchange, which is practically impossible in many cases.
- The setup and initial training cost of EDI is very high. Small and/ medium size organization cannot afford to it.
- Less Transparent than paper based systems.
- Even though there are widely accepted and widely used standards, there are no ways to force trading partners to accept these standards.

Table 9.1 EDI Versus e-mail

Electronic Data Interchange (EDI)	*Electronic Mail*
There is typically no human involvement in the processing of the information, as the interface has software-to-software orientation. The data are structured in a software-understandable way.	The data are not necessarily structured to be software-understandable. A human-to-software interface is involved at a minimum of one end of the interchange.
The interchange is composed by one software for interpretation by another software. If a reply is involved, it is composed by a software to be interpreted by another software.	The message is composed by a human and/or interpreted by a human and/or a reply is composed by a human and/or interpreted by a human.

EDI Application in Business

- Although EDI was developed to improve transportation and trade, it has spread everywhere.
- In short, EDI has grown from its original use as expediter of the transfer of trade goods to facilitator of standard format data between any two computer systems.
- An examination of EDI usage in various industries provides insight into the business problems that EDI is attempting to solve.
- Four very different scenarios in industries that use EDI extensively:
  1. International or cross-border trade,
  2. Financial EDI or electronic funds transfer (EFT),
  3. Health care EDI for insurance claims processing, and
  4. Manufacturing and retail procurement.


EDI Applications in Business
International Trade
Healthcare and Insurance
Financial EDI
Manufacturing/Retail Procurement

International or Cross-border trade

- EDI has always been very closely linked with international trade as broader and less costly transactions, is a necessity.
- Trade efficiency can be accomplished only by using EDI as a primary global transactions medium.
- EDI attempts to facilitate the smooth flow of information. It allows faster, simpler, broader & less costly transactions.
- Physical aspects of international trade are — the movement of goods, containers, vehicles, ships, and aircraft.
- EDI replaces paper, which has been the main stay for carrying trade-related information. Vast amounts of time and resources are often spent transferring and checking the information from one paper document to another.

- EDI Benefits for International Trade
  1. Reduced transaction expenditures;
  2. Quicker movement of imported and exported goods;
  3. Improved customer service through "track and trace" programs that quickly identify to the many participants in a trade deal — companies, customs, banks, insurers, transport agents, and so on — where things are located or being handled; and
  4. Faster customs clearance and reduced opportunities for corruption, a huge problem in trade.

Financial EDI:

- Financial EDI (FEDI) is the computer-to-computer exchange of payment and payment-related information between companies using a standard format.
- Unlike other forms of EDI, such as exchange of price quotes or purchase orders, financial EDI always involves a bank because a financial transaction (a payment) is being effected.
- Although Internet EDI is growing and offering new, flexible information interchange solutions for many trading partners, some elements of EDI remain difficult to transfer to the internet.
- **The EDI transaction sets that provide instructions to a trading partner's bank are called Financial EDI (FEDI).**
- Financial EDI comprises the electronic transactions of payments and remittance information between a payer, payee, and their respective banks.

Benefits of Financial EDI

- No deposit delays
- Prompt availability of funds
- Better cash management
- Opportunity to automate updating of accounts receivable.
- Remittance information and email notification of impending EDI deposit one day prior to date of deposit.
- No lost or stolen checks
- Fully traceable payments
- More cost effective than handling paper checks.

Types of Financial EDI

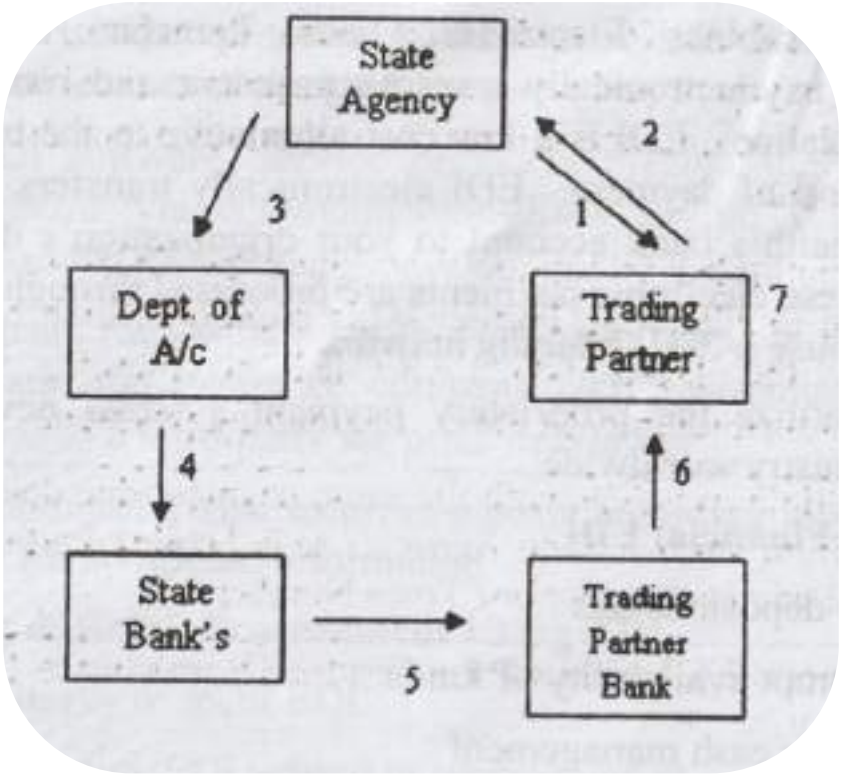
- Traditionally, wholesale or business-to-business payment is accomplished using cheques, EFT, and Automated Clearing Houses (ACH) for domestic and international funds transfer.

These terms can be described as:

- **Bank Cheques:**
  - These are instruments for debit transfers where payees collect funds from payers.
  - Funds made available by banks to depositors of cheques are provisional and may be reversed if the payer does not have sufficient funds in its account to pay the cheque when it is received by the payer's bank.

How Financial EDI works

- The Following figure explains how Financial EDI works for a vendor (Remittance Data Passing through the banking system.
- This procedure is based on Bank system.



1. STATE AGENCIES procure goods/services from a TRADING PARTNER (vendor).
2. The TRADING PARTNER provides goods/services to one or more State Agencies and submits a bill or invoice to each STATE AGENCY.
3. STATE AGENCIES certify payments to the Trading Partner by inputting payment requests with payment remittance information controlled by the DEPARTMENT OF ACCOUNTS.
4. The DEPARTMENT OF ACCOUNTS processes the STATE AGENCY payment requests and transmits the payment and the remittance information to the STATE's BANK.
5. The STATE's BANK passes the payment and remittance information to the TRADING PARTNER's BANK via the Automated Clearing House (ACH).

6. The TRADING PARTNER's BANK credits the payment to the Trading Partner's Account by the opening of business on the payment due date that is supplied by the State Agency. As prearranged by the Trading Partner, the TRADING PARTNER's BANK then notifies the TRADING PARTNER of the deposit and provides the remittance information to the TRADING PARTNER. Your bank may be able to provide an electronic file that can be translated for automated payment application of funds to your internal accounts receivable system.

7. The TRADING PARTNER posts its accounts receivable from the payment and remittance information received from the bank.

- A trace number is uniquely assigned by DOA to each electronic transmission to a Trading Partner. This number, which begins with "T", is used by the TRADING PARTNER to identify and match the remittance information with the corresponding payment.
- NOTE: Multiple payments with the same payment due date from one State, Agency or from various State Agencies to a Trading Partner are combined into one EDI payment; under one Trace Number:

- The Following figure explains how Financial EDI works for a vendor (Remittance Data by way of Internet.
- This procedure is based on Bank system.

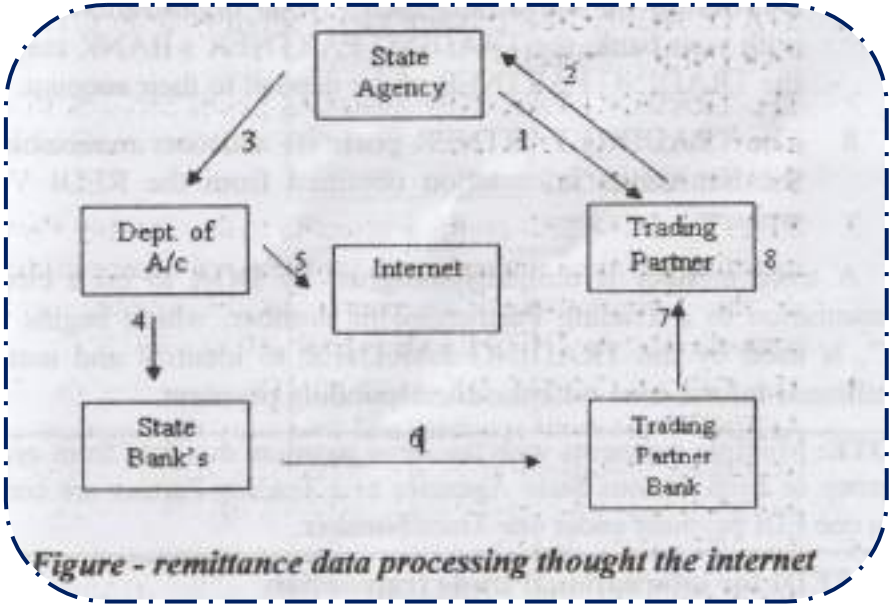


Figure - remittance data processing thought the internet

1. STATE AGENCIES procure goods/services from a TRADING PARTNER (vendor).
2. The TRADING PARTNER provides goods/services to one or more State Agencies and submits a bill or invoice to each STATE AGENCY.
3. STATE AGENCIES certify payments to the Trading Partner by inputting payment requests with payment remittance information which is controlled by the DEPARTMENT OF ACCOUNTS.
4. The DEPARTMENT OF ACCOUNTS processes the State Agency payment requests and transmits the payment without the remittance information, to the STATE's BANK.

5. While the payment information is transmitted to the State's Bank, the remittance information is transmitted to the Department of Accounts. Remittance information is usually available one business day prior to the payment being deposited in the TRADING PARTNER's bank account.
6. The STATE's BANK passes the payment to the TRADING PARTNER's BANK via the Automated Clearing House (ACH) banking network.
7. The TRADING PARTNER's BANK credits the payment to the Trading Partner's account by the opening of business on this payment due date that is supplied by the State Agency, Depending on the arrangements your organization has made with your bank, the TRADING PARTNER's BANK may notify the TRADING PARTNER of the deposit to their account.

8. The TRADING PARTNER posts its accounts receivable from the remittance information.

- A trace number is uniquely assigned by DOA to each electronic transmission to a Trading Partner. This number, which begins with a "T", is used by the TRADING PARTNER to identify and match the remittance information with the corresponding payment.
- NOTE: Multiple payments with the same payment due date from one State Agency or from various State Agencies to a Trading Partner are combined into one EDI payment under one Trace Number.

FEDI for International trade transaction

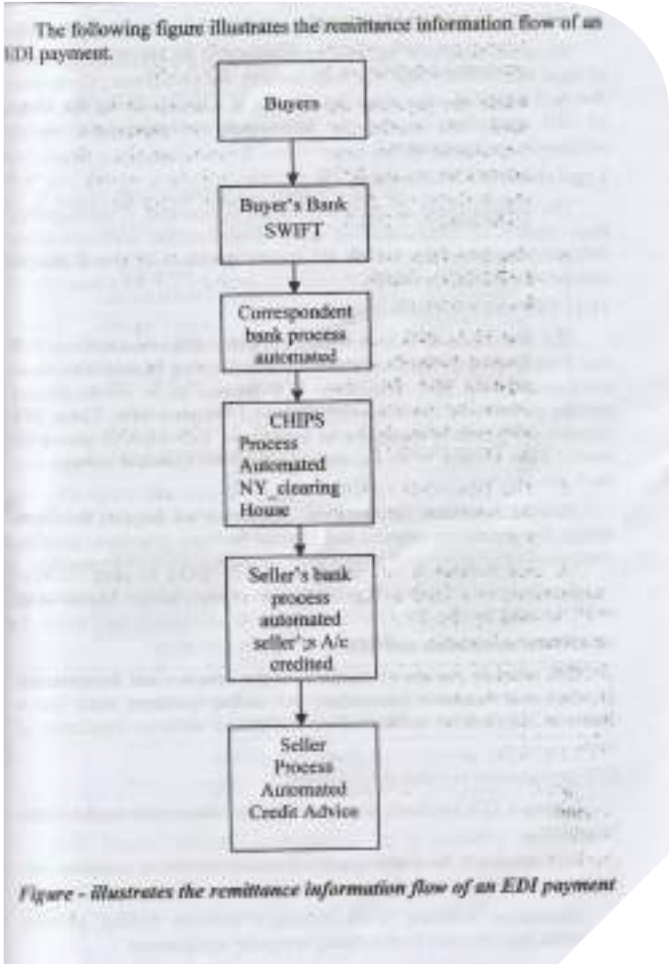


Figure - illustrates the remittance information flow of an EDI payment

- Swift is used by a buyer's bank in Delhi to move funds from its account maintained in a bank in New York called correspondent bank.
- The sellers account is credited immediately on receipt of instructions in SWIFT format by the correspondent bank.

Interbank Electronic Funds Transfer (EFT):

- Electronic Funds Transfer (EFT) is credit transfers between banks where funds flow directly from the payer's bank to the payee's bank.
- EDI utilizes computer and telecommunication components both to supply and transfer money and financial assets.
- They are same day, almost instantaneous payments.
- EFT is one of the earliest examples of payment systems that use online transactions although these transactions are carried-out on private networks.

- **Automated Clearing House (ACH) Transfers:** In contrast to the EFT process, ACH transfers are used to process high volumes of relatively small-dollar payments for settlement in one or two business days.
- An ACH provides the following services
  - Preauthorized Credits, such as the direct deposit of payrolls;
  - Preauthorized Debits, such as repetitive bill payments; and
  - Consumer Initiated Payments (called GIRO in banking circles).
- This is primarily a high-volume/low-dollar, consumer-oriented product.

Healthcare and Insurance EDI:

- EDI is rapidly becoming a permanent fixture in both insurance and healthcare industries as medical providers, patients, and payers increasingly process claims via electronic networks.
- Electronic claim processing is quick and reduces the administrative costs of healthcare.
- In most cases, claims can be sent to payers within 24 hours.
- Fewer errors translate to decreased turnaround time.

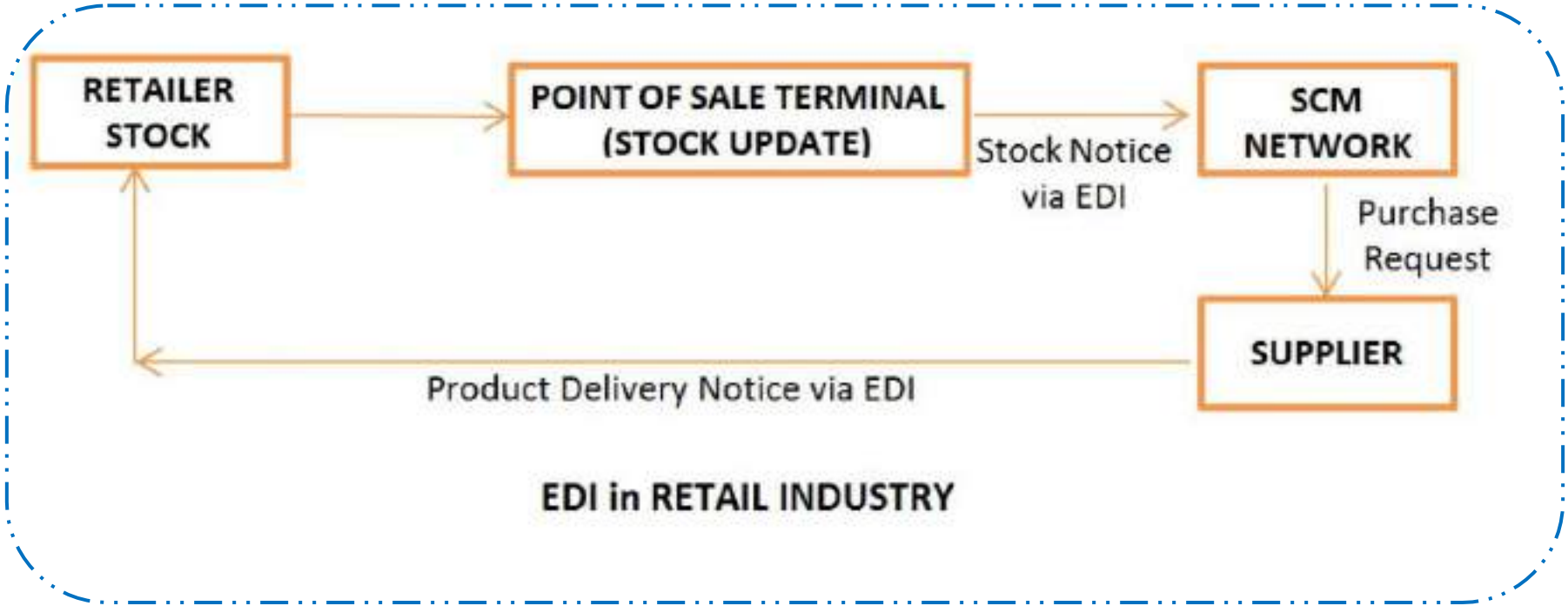
- In addition to processing claims for billing purposes, EDI enables doctors to communicate with other physicians, laboratories, hospitals, and other healthcare settings. In short, it leads to better managed care.
- Other transactions targeted for electronic transmission include claims submission or billing, payment, and payment posting, eligibility verification, and primary care member enrollment.
- EDI could reduce labor, intensive activities of providers and /payers involved with submitting, adjudicating, processing, and paying claims.

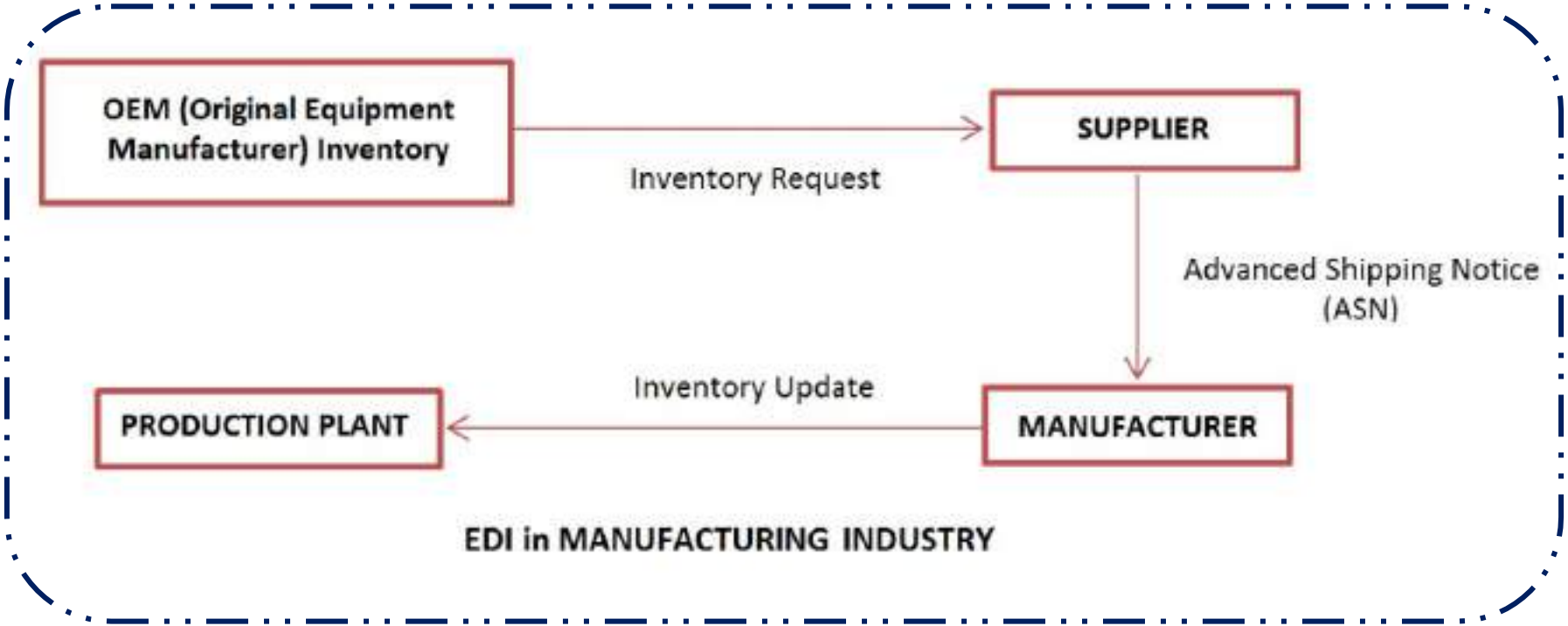
Manufacturing/Retail Procurement using EDI:

- Both manufacturing and retail procurement are already heavy users of EDI. In manufacturing, EDI is used to support just-in-time. In retailing, EDI is used to support quick response.
- **Just-in-Time and EDI:** Companies using JIT and EDI no longer stock thousands of large parts in advance of their use.
- Instead, they calculate how many parts are needed each day based on the production schedule and electronically transmit orders and schedules to suppliers every day or its some cases every 30 minutes.
- Parts are delivered to the plant "just in time" for production activity.

- **Quick Response and EDI:** Manufacturers have gained from just-in-time manufacturing techniques, retailers are redefining practices through the entire supply chain using Quick Response (QR) systems.
- For the customer, QR means better service and availability of a wider range of products.
- For the retailer and suppliers, QR may mean survival in a competitive marketplace.

- Much of the focus of QR is in reduction of lead times using event-driven EDI.
- Occurrences such as inventories falling below a specified level immediately trigger a chain of events including automatic ordering from one company's application directly into the other's application.
- In QR, EDI documents include purchase orders, shipping notices, invoices, inventory position, catalogs, and order status.


RETAILER STOCK
POINT OF SALE TERMINAL (STOCK UPDATE)
Stock Notice via EDI
SCM NETWORK
Purchase Request
SUPPLIER
Product Delivery Notice via EDI
EDI in RETAIL INDUSTRY


OEM (Original Equipment Manufacturer) Inventory
Inventory Request
SUPPLIER
Advanced Shipping Notice (ASN)
MANUFACTURER
Inventory Update
PRODUCTION PLANT
EDI in MANUFACTURING INDUSTRY

- **Automobile Sector –** In automobile sector EDI is used to keep customers updated with the current product and pricing information during the purchase cycle.
- An advance shipping notice is transmitted through EDI to the customers to prepare a loading schedule and to ensure proper receipt of the product.
- The customer may also make payment on receipt of goods via EDI to speed up the payment process.

Intranet Applications in Business

- **Intranet is a private computer network based on the Internet that can be accessed by the employees of an organization.**
- An Intranet provides easy access to internal files and documents to the various employees of the organization, from their individual workstations.
- Sharing of data, made possible through the Intranet, not only helps in saving time of employees, but also allows employees from various levels to access data. It also contributes to a paperless office.
- Today's most modern businesses are adopting intranet technology due its competitive advantages in dealing with the corporate information essential for any business.

- **Communication :** Intranet is extremely beneficial for communication and collaboration between the employees for successful functioning of any business organization.
- Intranet provides this to businesses in the form of tools like discussion groups, Intranet forms, and bulletin boards that helps in communication between different departments of an organization.
- Intranet tools help in conveying and distributing necessary information or documents among the employees of an organization.
- This results in easy communication and sound relationship between the employees and top-level management.

- **Time Saving :** Every business knows the importance and value of time. Intranet technology allows to distribute valuable information among the employees in a quick and efficient manner. Intranet saves time by interactivity, i.e employees can access information at a relevant time that suit them, rather than sending and waiting for email and email replies.
- **Productivity:** Intranet technology provides fast information to employees and helps to perform their various tasks with responsibility. An employee can access any data from any database of the organization without wastage of time. Employees working on projects can collaborate easily, ensuring better and faster results.

- **Reduce Costs:** An important benefit of Intranet is that it is cost-affective. This can be attributed to the fact that it is paperless.
- As Intranet supports online publishing, it definitely cuts down the printing and distribution costs as well.
- All the documents of the company can be published through the Intranet using web pages, as compared to spending Policy on printing documents.
- The information can be accessed from the respective workstations of the employees. Intranet results in reduced costs for administrative and operational purposes.

- **Rich in Format:** Intranet allows employees to view documents in Various rich format applications as well as video and audio. Multimedia programs can be used with intranet as well, allows better communication and information to be shared quickly.
- **Incorporated and Distributed Computing Environment:** Intranet supports an active distribution of stored information through different types of operating systems and computer types, from which the employees can access information. Intranet results in distributing information at a low cost due to the web architecture feature of intranet.

- **Increases Collaboration:** As intranet allows all employees to access data, this helps build team work activities within the organization. also certain contents of intranet like declaration section help desk. FAQ, handbook of employee, etc., aids in collaboration among the employees.
- **Training:** Intranet technology is well suited for presenting different types of e-learning content in various formats to the employees. Also Intranet allows to conduct induction programmes.
- **Increased Security:** Since Intranet is a private network, the information is shared among employees through firewalls. Hence Intranet provides increased internal security.

- Apart from all these benefits, Intranet also promotes equal corporate culture in information viewing.
- Intranet helps in maintaining good communication between different departments and also facilitates an immediate updation of operations.
- It provides teleconferencing software for interactive communication within the organization.
- Implementing Intranet in a business organization helps save significant time and money in the long run.
- Truly a boon to all business organizations, the benefits of Intranet to business has made it a necessity rather than a luxury, for most organizations.


Thank you

E-PAYMENTS

Dr P.V. Praveen Sundar
Assistant Professor,
Department of Computer Science
Adhiparasakthi College of Arts & Science,
Kalavai.

Electronic Payments

- Electronic Payment system is a financial exchange that takes place online between buyers and sellers. The content of this exchange is usually some form of digital financial instrument (such as encrypted credit card numbers, electronic cheques or digital cash) that is backed by a bank or an intermediary, or by a legal tender.
- The various factors that have leaded the financial institutions to make use of electronic payments are:
  - Decreased technology cost
  - Reduced operational and processing cost
  - Increasing online commerce

- Online payment is when the customer or buyer makes his payment transactions for the goods or services purchased with the use of the Internet.
- This type of payment lowers the costs for businesses as the more payments made electronically (online or offline) the less they spend for paper and postage.
- Also, it helps on improving customer retention as he is more likely to return to the same e-commerce site where his or her information has already been entered and stored.
- With online payment, it is not necessary for the payer to be in a long queue as payment is made in just a click of a mouse. Almost all the banks have an online bill payment service when it is offered free of charge and is available all days of the week or 24/7.

Basic Steps of an Online Payment

- The basic steps of an online payment transaction include the following:
  - The customer places an order online by selecting items from the merchant's Website and sending the merchant a list.
  - The merchant often replies with an order summary of the items, their price, n total, and an order number.
  - The customer places an order along with their credit/debit card information and sends it to the business.
  - The payment information is usually encrypted by an SSL pipeline set up between the customer's web browser and the merchant's web server SSL certificate.

- The merchant confirms the order and supplies the goods or services, to the customer.
- The business sends the consumer an invoice, their certificate and their bank's certificate.
- The business then generates an authorization request for customer's credit card and sends it to their bank.
- The business's bank then sends the authorization request to the acquirer.
- The acquirer sends an acknowledgement back to the business's bank after receiving an acknowledgement from the customer's Bank.
- Once the consumer's bank authorizes payment, the business's bank sends an acknowledgement back to the business with an authorization number.

Prepaid and Post Paid Payment Systems

- Electronic payment systems are broadly classified in to prepaid and post paid payment systems:
- **Prepaid Payment Systems:** It provides a service that is paid prior to usage. Here the customer is allowed to spend only up to the amounts that have pre-determined into the account.
- This type of payment system is highly useful to those customers who would like to control overspending. E.g. Prepaid debit cards.

- Prepaid payment system is taken by the customer by depositing money with the credit given company.
- It can be deposited in the savings account or the current account.
- Once the money is deposited, the card is used as a regular debit card.
- It is very effective card as it doesn't put in to debt.
- Once the money is exhausted the account, the debit card cannot be used.
- There is no interest Charges related to this card.

Benefits of the Pre-Paid Payment System

- It is accepted at the entire merchant establishment worldwide according to the affiliation of the Bank
- It can be used to withdraw cash from the ATMs.
- Reloadable anytime anywhere.
- It can be used to withdraw cash in any international currency.
- It is usually backed up by personal accident insurance cover.
- Customer has the facility to get online and track spending , check balance, change pin.

Post Paid Payment System

- This system is like a credit card used to make incremental purchases through the web site.
- As purchases are made, the accumulated debt on the post paid credit instrument increase until a credit limit is reached, or until an arrangement has made to settle the debt such as monthly payment.
- Normally all credit cards are post paid cards.
- The customer gets the eligibility of spending through the income statement and credit history produced before the credit card company.
- The customer gets a credit limit and a credit period by which the customer is supposed to pay back the money to the credit card company.

Features of Post Paid Payment System

- **Global acceptance** — accepted by all the merchant establishments according to the network set by the credit card company.
- **Balance transfer option** — It is possible to transfer outstanding funds from one card to other cards with low interest rates.
- **Revolver facility** — Customer can pay only a small amount of the total outstanding and revolve the rest for the payment of the next month.

- **Cash advance facility** — Customer can withdraw around 30% of the credit limit at any ATM connected to the credit card company.
- **Tele draft** — These facilities are available at the door steps of the customer.
- **Other services** — Credit card can be used for railway tickets and airline ticket purchase.
- **Convenience** — as the customer is not required to carry cash for any purchase.
- **Easy availability** — holder can load prepaid credit cards ay anytime they need.

Types of Electronic Payment Systems

- The various types of electronic payment systems are as follows:
- **Electronic Cash or E-Cash**
- E-Cash or Electronic Cash is a new concept to execute cash payment using computers connected with network.
- E-cash is an electronic medium for making payments.
- The primary function of e-cash is to facilitate transactions on the Internet.
- Many of these transactions may be small in size and would not be cost efficient through other payment medium such its credit cards.

- Electronic money [also known as e-currency, e-money, electronic cash, electronic currency, digital money, digital cash or digital currency] refers to money or scrip which is exchanged only electronically. Typically, this involves the use of computer networks, the internet and digital stored value systems.
- Electronic Fund Transfer and direct Deposit are all examples of electronic money.
- E-cash is a system of purchasing cash credits in relatively small amounts, storing the credits in our computer, and then spending them when making electronic purchases over the Internet.

- The e-cash is the creation of electronic money or tokens, usually by a bank, which buyers and sellers trade for goods and services.
- It consists of a token, which may be authenticated independently of the issuer. This is commonly achieved through the use of self-authenticating tokens.
- It includes credit cards, smart cards, debit cards, electronic fund transfer etc.

- An e-cash system must have the following properties: -
  - Digital cash must have a monetary value. It must be backed by cash.
  - Digital cash must be exchangeable.
  - It should be storable and retrievable.
  - It should not be easy to copy or tamper with while it is being exchanged.
- E-cash can be used for making or receiving payments between buyer and seller. The bank's server computer sends a secure e-cash packet to the customer effect the network currency server of the bank is issuing a hunk note with a serial number for a specified amount. The bank uses its private key to digitally sign such a bank note.

Electronic Cheques

- The electronic cheques (E-cheques) are modeled on paper checks. except that they are initiated electronically.
- They use digital signatures for signing and endorsing and require the use of digital certificates to authenticate the payer, the payer's bank and bank account.
- They are delivered either by direct transmission using telephone lines or by public networks such as the Internet.
- Integration of the banking and the information technology industry has benefitted the consumers in many aspects with respect to time, cost and operational efficiency.

- The advantages of Electronic cheques are:
  - The online merchants could receive payments instantly.
  - Similar to traditional cheques and eliminates need for customer education.
  - Much faster.
  - Less chance for cheque bouncing.
  - Cost — effective manner.

Electronic Wallets

- An e-wallet is a software component that a user downloads to their desktop and in which the user stores credit card numbers and other personal information.
- When a user shops at a merchant who accepts e-wallet, the user click the e-wallet and the forms are automatically filled in with all the necessary information in just one click.
- Credit card companies such as Visa and MasterCard also offer this e-wallet.
- Electronic wallets (E-Wallets) being very useful for frequent online shoppers are commercially available for pocket, palm-sized, handheld, and desktop PCs.

- They offer a secure, convenient, and, portable tool for online shopping.
- They store personal and financial information such as credit cards, passwords, PINs, and much more.
- To facilitate the credit-card order process, many companies are introducing electronic wallet services.
- E-wallets allow you to keep track of your billing and shipping information so that it can be entered with one click at participating merchants' sites.

- E-wallets can also store e-checks, e-cash and your credit-card information for multiple cards.
- A popular example of an e-wallet on the market is Microsoft Wallet.
- To obtain Microsoft Wallet, one needs to set up a Microsoft Passport. After establishing a Passport, a Microsoft e-wallet can be established.
- Then, e-wallets can be used for micro-payments.
- They also eliminate reentering personal information on the forms, resulting in higher speed and efficiency for online shoppers.

- Microsoft Passport consists of several services including the following:
- A single sign-in, wallet and kids passport services.
- A single sign-in service allows the customer to use a "single name and password at a growing number of participating e-commerce sites.
- The shopper can use to make fast online purchases with a wallet service.
- Kids' passport service helps to protect and control children's online privacy.

Features of E-Wallet

- Firewall encrypted security logic.
- Compatible with many supporting hardware.
- No separate card reader is required to access our card.
- Reusability of our card is unlimited.
- Multiple card features are incorporated in the same card.
- External complexities are less.
- Refillable
- Current balance can be stored and read.
- User authentication is provided.
- Universal access
- Maximum possible cash

Advantages of E-Wallet

- Withdraw or deposit value by telephone.
- No signature required.
- In the future, access points may include mobile phones.
- Accessibility and convenience.
- Cash machines and telephones give more access points to funds in bank account. Available 24 hours / 365 days.
- Cash machines and telephones cannot run out of electronic cash.
- Flexibility

- Transfer value by telephone.
- Pay person to person.
- Multi-currency capability.
- No age limit, so suitable for all the family.
- Safety and control
- Read your balance. Load value at home.
- Lock your card or wallet.
- Keep track of what you have spent and where Customer will traceable if a lost card is found.

Credit cards

- A credit card system is a type of retail transaction settlement and credit system, named after the small plastic card issued to users of the system.
- A credit card is different from a debit card in that it does not remove money from the user's account after every transaction. In the case of credit cards, the issuer lends money to the consumer (or the user) to be paid to the merchant.
- It is also different from a charge card (though this name is sometimes used by the public to describe credit cards), which requires the balance to be paid in full each month.
- Most credit cards are the same shape and size, as specified by the ISO 7810 standard.

- Credit card is small plastic card with a unique number attached with an account.
- It has also a magnetic strip embedded in it which is used to read credit card via card readers.
- When a customer purchases a product via credit card, credit card issuer bank pays on behalf of the customer and customer has a certain time period after which he/she can pay the credit card bill. It is usually credit card monthly payment cycle.
- Following are the actors in the credit card system.
  - The card holder – Customer
  - The merchant – Seller of product who can accept credit card payments.
  - The card issuer bank – Card holder's bank
  - The acquirer bank – The merchant's bank
  - The card brand – for example , Visa or Mastercard.

Step	Description
Step 1	Bank issues and activates a credit card to the customer on his/her request.
Step 2	The customer presents the credit card information to the merchant site or to the merchant from whom he/she wants to purchase a product/service.
Step 3	Merchant validates the customer's identity by asking for approval from the card brand company.
Step 4	Card brand company authenticates the credit card and pays the transaction by credit. Merchant keeps the sales slip.
Step 5	Merchant submits the sales slip to acquirer banks and gets the service charges paid to him/her.
Step 6	Acquirer bank requests the card brand company to clear the credit amount and gets the payment.
Step 7	Now the card brand company asks to clear the amount from the issuer bank and the amount gets transferred to the card brand company.

- They are the convenient method of making online payment.
- Credit cards work around the globe regardless of the location of country of the issuing bank.
- They also handle multiple currencies through a series of clearing houses.
- The credit card holders can purchase goods and services either offline or online without making immediate payment.
- Payment to the merchant's will be made by the customer's Bank.
- The credit card is a financial instrument which can be used more than once to borrow money or buy products and services on credit.

- To accept a credit card for payment, we have to open a merchant account with our bank.
- A merchant account allows sellers to accept and process credit card transactions. In these transactions, the card number and transaction details are processed with no identification of the buyer.
- To implement the payments over the internet, the web merchant needs some form of secure and encrypted line using the Secure sockets Layer [SSL] that is standard on Netscape and Microsoft browsers, The merchant server needs an encryption key for the purpose.

Types of Credit Cards Payments

- **Payments Using Plain Credit Card Details:**
- The easiest method of credit card payment is the exchange of unencrypted credit cards over a public network such as telephone lines or the Internet.
- The low level of security inherent in the design of the Internet makes this method problematic (any hacker can read a credit card number, and there are programs the scan the Internet traffic for credit card numbers and send the numbers to their programmers).
- Authentication is also a significant problem, and the vendor is usually responsible for ensuring that the person using the credit card is its owner.

Steps of Payments Using Plain Credit Card

- A plain electronic credit card transaction processes the following steps:
  1. The customer accesses a vendor's server and receives a display of the goods/services being offered by the vendor.
  2. The customer selects the desired goods/services and offers a credit card payment to the vendor by typing in the credit card number in a HTML form provided by the vendor's server.
  3. The vendor server accesses the acquirer for credit authorisation of the consumer's credit card number and the amount of purchase.
  4. The acquirer forwards the request to the customer's credit card issuer.
  5. The customer's issuer informs the acquirer of the authenticity of the credit card number and the credit status of the customer.

6. The acquirer informs the vendor whether to proceed with the sale or not.
7. The vendor informs the customer whether the transaction has been completed.
8. Later the vendor accesses the acquirer's server and sends the details of the various electronic credits helms given.
9. The acquirer accesses the respective credit card issuer and obtains the money on behalf of the vendor.
10. The issuer charges the customer for the credit amount within the specified credit days. For this, the customer may receive his account updates from the issuer.

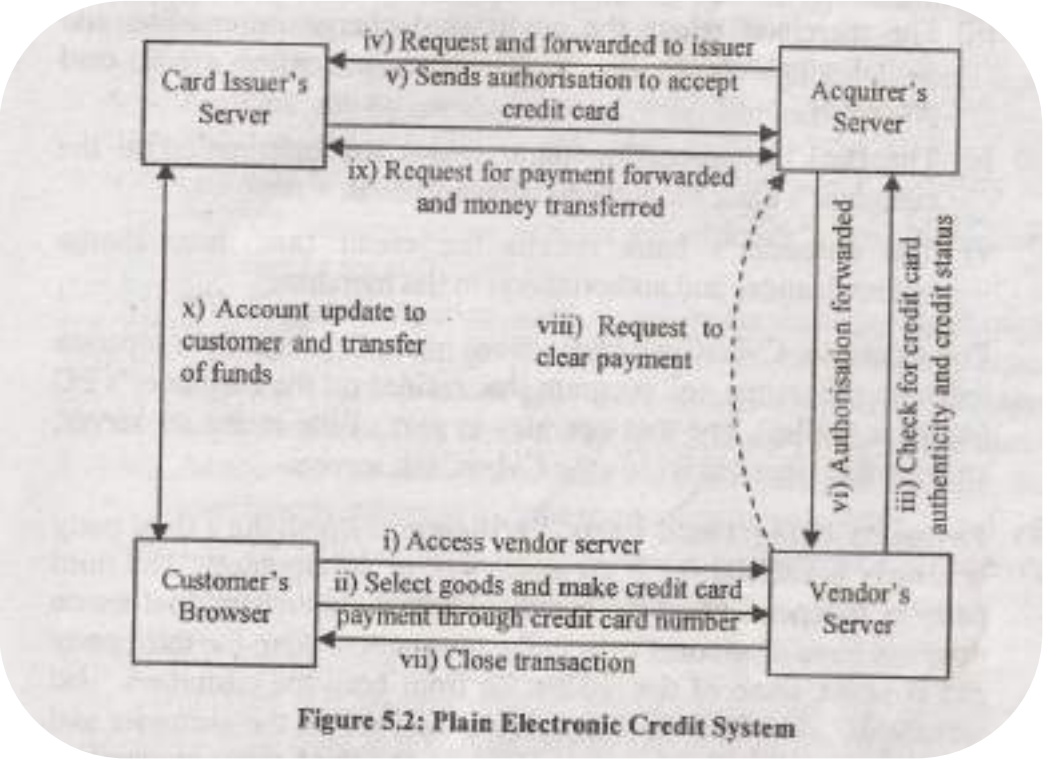


Figure 5.2: Plain Electronic Credit System

Payments Using Encrypted Credit Card Details:

- Encryption is initiated when credit card information is entered into a browser or other electronic commerce device and sent securely over the network from buyer to seller as an encrypted message.
- To make a credit card transaction truly secure and non-refutable, the following sequence of steps must occur before actual goods, services, or funds flow:
  1. A customer presents his or her credit card information (along with an authentic signature or other information such as mother's maiden name) securely to the merchant.
  2. The merchant validates the customer's identity as the owner of the credit card account.

3. The merchant relays the credit card charge information and digital signature to his or her bank or online credit card processor.
4. The bank or processing party relays the information to the customer's bank for authorization approval.
5. The customer's bank returns the credit card data, charge authentication, and authorization to the merchant.

- For example, CyberCash transactions move between three separate software programs: one program that resides on the consumer's PC (called a wallet), one that operates as part of the merchant server, and one that operates within the CyberCash servers.

Payments Using Third-Party Verification:

- Involving a third party is always beneficial, be it an agreement or an argument. The third party is independent of the customer and the merchant, and hence does not have a personal gain in the transaction.
- Also the third party can conduct some of the processing from both the customers 'and merchants' side.
- This further reduces the load on the customer and merchant involved in the transaction.
- In the third party processing, consumes register with a third party on the internet to verify their transactions.
- The various steps involved in an online credit card transaction using third party verification is explained below and is diagrammatically represented in figure 5.3.

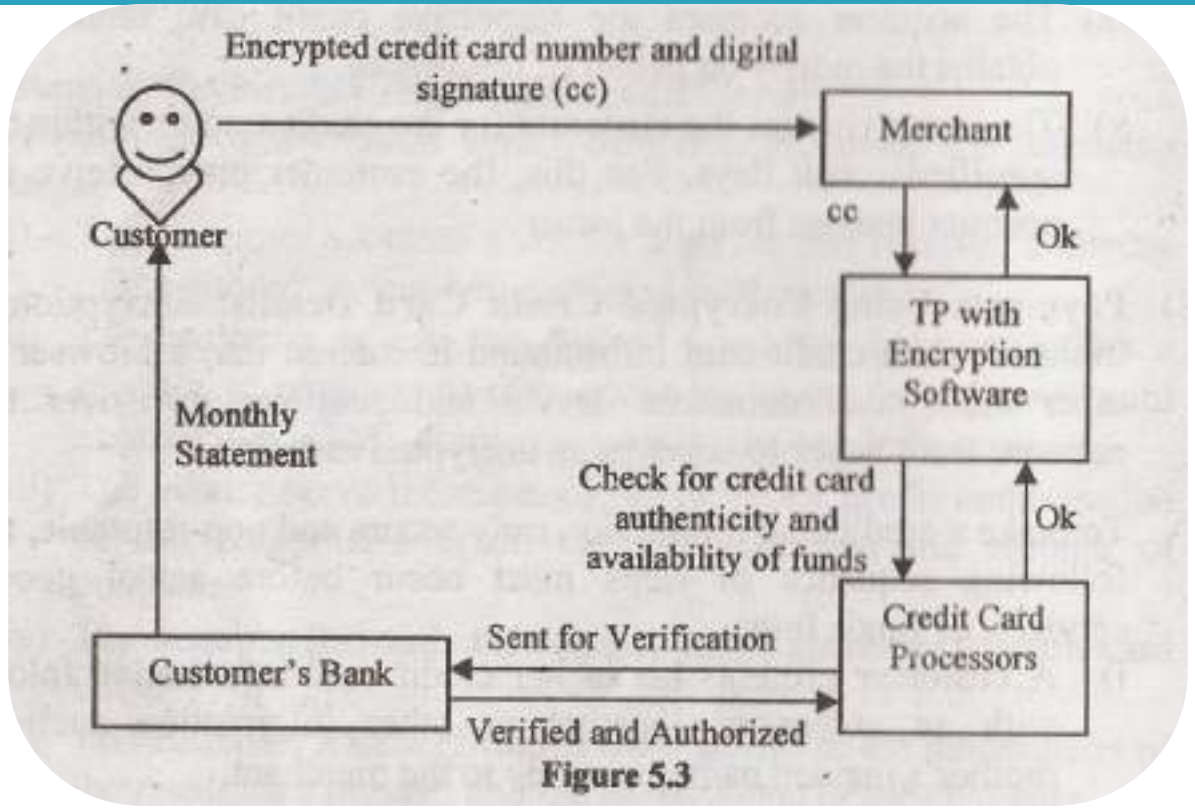

Encrypted credit card number and digital signature (cc)
Merchant
Customer
cc
Ok
TP with Encryption Software
Monthly Statement
Check for credit card authenticity and availability of funds
Ok
Credit Card Processors
Sent for Verification
Customer's Bank
Verified and Authorized

Figure 5.3

1. The customer acquires a TP (Third Party) account that provides a complete customer profile and is backed by with the credit card of the customer.
2. To purchase goods on-line, the customer requests the item from the merchant by quoting his/her TP account number.
3. The merchant contacts the TP payment server with the customer's account number.
4. The TP payment server verifies the customer's account number and checks for sufficient funds.

5. The TP payment server sends e-mail to the customer confirming the purchase of the goods and the buyer responds back either agreeing to pay or denying it. This step ensures that the customer has indeed placed an order for the goods and services in question.
6. As soon as the customer signals the authenticity of the deal, the merchant is informed and the transaction is completed.
7. The TP will not debit the customer's account until it receives confirmation of the purchase completion.

Credit Card Security Overview

- Credit card security is based on privacy of the actual credit card number. This means that whenever a person other than the card owner reads the number, security is potentially compromised. Since this happens most of the time when a transaction is made, security is low. However, a user with access to just the number can only make certain types of transactions.
- Merchants will often accept credit card numbers without extra verification for mail order, but then the delivery address will be recorded, so the thief must make sure he can have the goods delivered to an anonymous address (i.e. not his own) and collect them without being detected.

- Some merchants will accept a credit card number for in-store purchases, where upon access to the number allows easy fraud, but many require the card itself to be present, and require a signature. Thus, a stolen card can be cancelled, and if this is done quickly, no fraud can take place in this way.
- For internet purchases, there is sometimes the same level of security as for mail order (number only) hence requiring only that the fraudster take care about collecting the goods, but often there are additional measures. The main one is to require a security PIN with the card, which requires that the thief have access to the card.

Credit card numbering

- The numbers found on credit cards have a certain amount of internal structure, and share a common numbering scheme.
- The card number's prefix, called the Bank Identification Number, is the sequence of digits at the beginning of the number that determine the bank to which a credit card number belongs.
- This is the first six digits for MasterCard and Visa cards.
- The next nine digits are the individual account number, and the final digit is a validity check code.
- In addition to the main credit card number, credit cards also carry issue and expiration dates (given to the nearest month), as well as extra codes such as issue numbers and security codes.
- Not all credit cards have the same sets of extra codes nor do they use the same number of digits.

Credit cards in ATMs

- Many credit cards can also be used in an ATM to withdraw money against the credit limit extended to the card but many card issuers charge interest on cash advances before they do so on purchases.
- The interest on cash advances is commonly charged from the date the withdrawal is made, rather than the monthly billing date.
- Many card issuers levy a commission for cash withdrawals, even if the ATM belongs to the same bank as the card issuer.
- Merchants do not offer cash back on credit card transactions because they would pay a percentage commission of the additional cash amount to their bank or merchant services provider, thereby making it uneconomical.

Advantages of Credit Cards

- The advantages and acceptability of credit cards from the customer's view point vary from that of a banker or member establishments. Some of them are as below:
- **To Card Holder:** The small and attractive plastic credit cards are very easy to carry and they have very much substituted currency notes. The credit cards have enabled the holder to go shopping, without the burden of carrying wards of currency notes with its inherent risks, inconveniences and dangers. Numbers of fringe benefits are available to the credit card holder. It has increased the purchasing power and has also become a status symbol to the holder. In short, it can be said that the cardholder has at his disposal 'instant credit' up to a fixed limit whenever he needs it.

- **To Issuer:** The credit cards enable the issuer to provide a fuller service to their customers. They are also useful marketing tools, as they open up relationship with merchants, retailers and consumers who are not previous customers to the issuer and thus credit cards potentially attract new business. As the cards enable the holders to exercise an enormous clout in purchases, it means increase in the business and thus an increase in the income to the issuer in the nature of commission and interest. In the case of issuing banks the credit cards have made it easy to handle small personal loan and installment loans for durable goods. The issuer gets publicity by the display of credit card acceptance by the member establishments.

Disadvantages of Credit Cards

- Credit cards have many drawbacks for the user, issuer, and the merchant establishments alike.
- Some of these are:
  - **Waste of Money:** It would be a waste of money to subscribe to a credit card if the card was not utilized.
  - **Thoughtless Buying:** Credit cards invariably encourage impulsive purchases. Since the user need not pay instantly, it may tempt the purchase of products/services that are not genuinely required.
  - **Financial Problem:** Use of credit cards may drag the user into financial problems including overdraft. This happens where repayment on the credit card account is not done promptly.
  - **Mental Agony:** The pressure tactics used by recovery agents appointed by some card issuers to collect outstanding dues may cause mental agony to the user.
  - **Costly:** The user invariably ends up paying more than the actual price of the product/service obtained from the merchant establishments. This is, because, often the price charged to card-customers is relatively higher than the charge to cash-customers.

Debit Cards

- Debit Card is a prepaid card with some stored value.
- Banks issue debit cards to their customers who have maintained an account in the balance with sufficient credit balance.
- Each time the customer makes a purchase, an exact amount of the purchase is debited in his account.
- An individual has to open an account with the issuing bank which gives debit card with a Personal Identification Number (PIN).
- When he makes a purchase, he enters his PIN on shops PIN pad.

- When the card is slurped through the electronic terminal, it dials the acquiring bank system — either Master Card or VISA that validates the PIN and finds out from the issuing bank whether to accept or decline the transactions.
- The customer can never overspend because the system rejects any transaction which exceeds the balance in his account.
- The bank never faces a default because the amount spent is debited immediately from the customers account.

Components of a Debit card

- A debit card has the following details:
- **The Card Number:** this is a 16- digit number. The card number is unique and is not the same as the bank account number.
- **The Issue And Expiration Date:** The issue date is also printed in the MM/YY format. The expiry date is also printed in the same MM/YY format.
- **The Logo:** The card has the logo of the bank that has issued it. It also has the logo which determines the type of debit card it is: Visa, Mastercard , Maestro or RuPay logo.
- **Customer Service Number:** The toll-free number is printed on the back of the card. You can call this number in case of any questions or to report the loss or theft of your card.

- **The Signature Bar:** A signature bar is provided on the back of the card. It is important that you sign the bar as soon as you receive the card. This can help you to prevent fraudulent transactions. Some merchant retail outlets do not swipe the card unless the signature is verified.
- **CVV number:** Also known as the card verification value number, the CCV number is unique to every debit. This number needs to be provided at the time of making online payments. It provides an additional layer of security to the card.

Advantages of Debit Cards

- **Debit card can be easily obtained:** Most banks issue a free debit card. Once we open a savings or current account.
- **Very convenient to use:** One of the advantages of a debit card is that it can be swiped for transactions as well as withdrawal of cash from ATMs.
- **No more debts:** When you have a credit card, you are more likely to make impulsive purchases. But a debit card keeps you in check as it is linked to your bank account. You are only able to spend the amount that is in your account.
- **Easily accepted:** Debit cards are accepted widely all over India and at international destinations. Make sure to authorise international transactions by simply calling your bank. These debit cards can be used for cash withdrawal at international ATMs too.
- **Earn rewards:** Several online and retail outlets offer cashback offers for every purchase made on the debit card. The points can be redeemed at any time to either purchase products from an online catalogue of the bank or to earn shopping vouchers from various brands.

Disadvantages

- **No credit allowed:** A debit card is linked to your bank account. There is no possibility of making any transaction on credit. All transactions and withdrawals are limited to the balance available in your account.
- **Difficult to dispute fraudulent use:** It is easier to fraudulently use your debit card. In case someone steals the details of your card, especially the PIN and CVV, the chances of a fraudulent transaction are very high. It is difficult to dispute such transactions with the bank.
- **Additional fees on ATM withdrawals:** Every bank offers you a limited number of free ATM transactions and other non-financial transactions per month at the branches of other banks. Once you exceed the limit of free withdrawals/ non-financial transactions, fees are levied.

Parameters	Debit Card	Credit Card
Definition	Deducts money directly from your saving's bank account or your current account.	Allows you to borrow funds to pay for goods and services.
Source of funds	Your savings bank account or current account.	Credit extended to you by your card issuer. It gives you access to money you otherwise do not have (like a very short-term loan).
Spending advantage	You can only spend how much you have.	Can spend more than what you have.
Who pays for the purchase	You pay for your purchase.	The credit card company pays the vendor for your purchase. You pay the credit card company.
Bill	There is no bill or statement	You get a bill or statement each month with details of the transactions you have made.

Parameters	Debit Card	Credit Card
Payment	There is no payment that needs to be made since you are using your own money.	A bill needs to be paid each month since it is being borrowed.
Fees and charges	Annual fees and PIN regeneration fees are applicable.	Credit cards have multiple fees applicable. These include joining fees, annual fees, late payment fees, and bounced cheque fees among others.
Interest	There is no interest that is charged.	Interest is charged on the outstanding amount if it hasn't been paid by the due date.
Limit to funds that can be accessed	You can access any amount up to what is currently available in your savings bank or current account.	You can use the card only up to the pre-set credit limit on your card.

Parameters	Debit Card	Credit Card
Rewards	Typically, the rewards you get are minimal	Get to enjoy cashback, air miles, and reward points which can be redeemed.
Privileges	Doesn't come with many privileges.	Come with numerous dining, retail, entertainment, and travel privileges (depending on the type of card you have).
Lost card liability	Protection from theft or loss of the card is minimal.	Most cards offer 100% lost liability protection. So, you are not liable for any unauthorized transactions made.

Smart Card

- Smart cards, also called stored value cards, which use magnetic stripe technology or integrated circuit chips to store customer-specific information, including electronic money.
- The cards can be used to purchase goods or services, store information, control access to accounts, and perform many other functions.
- Smart cards offer clear benefits to both merchants and consumers. They reduce cash-handling expenses and losses caused by fraud, expedite customer transactions at the checkout counter, and enhance consumer convenience and safety.
- In addition, many state and federal governments are considering stored value cards as an efficient option for dispersing government entitlements.
- Other private sector institutions market stored value products to transit riders, university students, telephone customers, vending customers, and retail customers.

- One successful use of stored value cards is by Bangalore Metro Rail Corporation Limited. (https://english.bmrc.co.in/Ticket)
- Smart cards have been in existence since the early 1980s and hold promise for secure transactions using existing infrastructure.
- Smart cards are credit and debit cards and other card products enhanced with microprocessors capable of holding more information than the traditional magnetic stripe.
- The chip, at its current state of development, can store significantly greater amounts of data, estimated to be 80 times more than a magnetic stripe.
- Industry observers have predicted that, by the year 2000,one-half of all payment cards issued in the world will have embedded microprocessors rather than the simple magnetic stripe.

- The possible applications of smart cards are the following:
  - **Banking & Retail -** Smart banking cards can be used as credit, direct debit or stored value cards, offering a counterfeit- and tamper-proof device.
  - **Electronic Purse -** A smart card can be used to store a monetary value for small purchases. Card readers retrieve the amount currently stored, and subtract the amount for the goods or services being purchased.
  - **Health Care -** Smart cards allow the information for a patient's history to be reliably and safely stored. Health care professionals can instantaneously access such information when needed, and update the content.
  - **Mobile Communications** — Smart cards are used as identification device for GSM digital mobile phones. The card stores all the necessary information in order to properly identify and bill the user, so that any user can use any phone terminal.

Micropayment

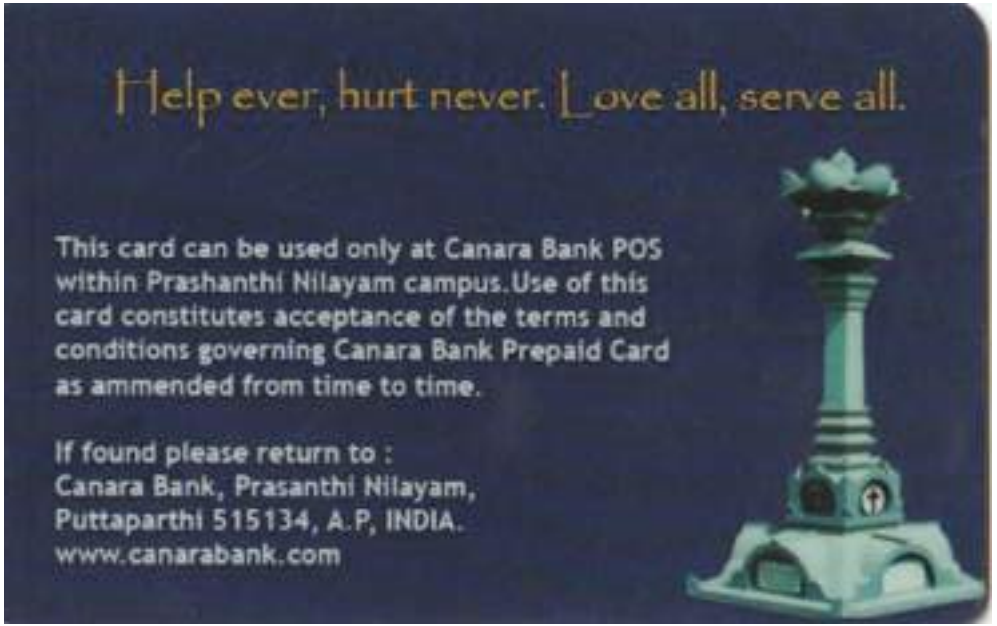
- A micropayment is a small transaction, often carried out online, that can be as small as a fraction of a cent. Depending on the payments system, a "micropayment" may be defined as any transaction size less than $1.00, $5.00, or more.
- Micropayment platforms built for handling small transactions work in a number of ways.
- Here's one scheme for micropayment: The user and seller each establish an account with a third-party service provider who monitors, collects and distributes micropayments.
- When the user initiates a transaction, payment goes through an Internet wallet account managed by the service provider.
- Micropayments accumulate until they are collected as single, larger payments. Such a system is helpful when a user wants to make one-time micropayments to multiple sellers.
- Seller-based accounts are more common for repeat business with an individual enterprise.

Stored Value Cards

- Store value cards are better known as gift cards. it functions like debit cards specific to a certain retailer or set of retailers.
- A Stored Value Card (SVC) is a plastic card with an integrated circuit embedded in it. This embedded circuit allows the card to store information and perform certain transactions when inserted into special devices designed to read and process the cards.
- They coexist with credit and debit technology and principally target the low value transactions.
- Transaction security can range from low to high, depending on the per-determined application of the card.
- Stored-value cards have a specific dollar value programmed into them.

- Banks provide these cards as a service for customers who cannot open checking or other deposit accounts.
- Stored value cards works similarly to debit cards, but the funds are not withdrawn from the user's bank account. The funds are taken from a pre-paid monetary value.
- Stored-value cards can be divided into two categories.
  - **Closed system cards** also known as merchant gift cards. “Closed system” means that the cards are only accepted at a single merchant. These cards are also referred to as “closed loop” or “single-purpose” cards. Purchasers buy a card for a fixed amount and can only use the card at the merchant that issues the card. The cards have often an expiration date or a service fee. In addition most closed system cards cannot be repaid in cash
  - **Open-loop cards,** on the other hand, can be reloaded with cash and used again.

Open loop Card



Terms & Conditions for Debit Card

- This is not a credit card and is not transferable.
- The terms and conditions, rules & regulations & bye laws of Fun Republic in force govern the card holder from time to time.
- The card is valid only at Fun Food Court Coimbatore. The balance would be refunded on return of this card.
- Please produce this card during all transactions.
- This card is property of E-City Real Estate Pvt Ltd and must be returned on request.
- Conditions apply.
- This card is valid for 365 days after the date of issue.

0130084432

If found please return to the customer service centre at :
Fun Republic Mall, Avinashi Road, Coimbatore - 641 004.

Closed Loop Cards


Gift Card
Flipkart
issued by wikcilver

Charge Card

- A Charge Card is a specific kind of a credit card.
- The balance on a huge card account is payable in full when the statement is received and cannot be rolled over from one billing to the next. Because you cannot carry a balance, a charge card does not have a periodic or annual percentage rate.

Net Banking

- Online banking is also known as "Internet banking" or "Web Banking."
- It is the process of conducting banking transactions over the Internet.
- Viewing bank statements and the status of a bank account online also comes under the definition of net banking.
- The bank updates accounts and records of transactions almost instantly on the Internet. This form of banking comes with both benefits and scams.
- Banks need to use enhanced security measures to ensure the safety and privacy of Internet transactions.

- Online banks cannot provide direct ATM access, but they make provisions for consumers to use ATMs at other banks and retail stores, and they may reimburse consumers for any associated fees.
- Because of the reduced overhead costs associated with not having physical branches, online banks tend to offer consumers significant savings and pay higher Interest rates.
- Online banks handle customer service tasks by phone, mail or online chat.

Advantages of Net Banking

- **Convenience** — Banks that offer internet banking are open for business transactions anywhere a client might be as long as there is internet connection.
- Apart from periods of website maintenance, services are available 24 hours a day and 365 days round the year. In a scenario where internet connection is unavailable, customer services are provided round the clock via telephone.
- At the touch of a button, actual time account balances and information are availed. This accelerates the banking processes hence increasing their efficiency and effectiveness.
- Online banking allows for easier updating and maintaining of direct accounts. The time for changing mailing address is greatly reduced, ordering of additional checks is availed and provision of actual time interest rates.

- **Specialized services:** Many banks offer specialized and convenient tools to enable easier financial management. Services such as investment analysis tools, money monitoring tools, Sweep-in facility, loan calculators, online bill payments etc. are available. Furthermore, banks also provide online tax forms and tax preparation services.
- **Transfer services** — Online banking allows automatic funding of accounts from long established bank accounts via electronic funds transfers.
- **Ease of monitoring** — A client can monitor his/her spending-via a virtual wallet through certain banks and applications and enable payments.
- **Ease of transaction** — the speed of transaction is faster relative to use of ATM's or customary banking.

- **High interest rates:** Internet banking provides low interest rate on mortgage loans than banks. The operational cost is also low which helps to saving amount that is beneficial for the customers. There are various other facilities such as no minimum balance account which helps to maintain account with zero balance. It increases total disposable income of the consumers without even worry about maintaining minimum balance.

- **Low cost banking service:** Internet banking reduce enable to reduce operational costs with better quality of services. It provides convenience with high customer service at lower rate. The Bank charges minimal amount for operations which reflect that the e-banking services are reasonable and efficient.
- **High liquidity:** You can transfer money and utilize anytime which is the greatest advantage to access internet banking. You don't need to visit banks for transferring money which can be done from anywhere without visiting to the banks physically.

Disadvantages

E-banking has various advantages which improves the banking system but there are disadvantages of using internet banking. These are as follows:

- **Security issues:** Internet banking is completely insecure as there are many problems related to the website and data can be hacked by the hackers. It can leads to financial loss to the users. The financial information can also be stolen that can also create financial loss. Direct banks are governed by laws and regulations similar to those of customary banks. Accounts are protected by Reserve Bank of India.
- **Lack of direct contact between customer and banking officer:** Online banking requires effective customer service for handling issues faced by the user. But lack of customer support creates disappointment among the customers. There are some online payments which may not be reflected in the system due to technical issues. It also creates insecurity among the customers. Thus the lack of support from customer service executive is a barrier in online banking.

Mobile Banking

- Mobile banking is a wireless Internet-based service that allows you to do your banking safely and conveniently while you are out and about using a mobile device.
- Mobile Banking provides access to the most popular Internet Banking features and services including:
  - Viewing your account balances,
  - Looking up transactions,
  - Paying your bills,
  - Transferring funds and checking rates.

- Mobile banking is one step closer to creating a completely digitalized environment. It lessens paperwork and shrinks waiting time which is otherwise wasted in long queues.
- Banks provide mobile banking services to their clients in the different ways listed here:
  - Mobile Banking over mobile applications (for smartphones; e.g. SBI Yono and iMobile by ICICI Bank, etc.)
  - Mobile Banking over SMS (also known as SMS Banking)
  - Mobile Banking over Unstructured Supplementary Service Data (USSD)

Benefits of Mobile Banking

- Mobile banking is useful to customers in the following ways:
- **Access to Account Information:** Information is power. And thus, knowing your exact bank balance is important. This helps you in better management of your funds. And thus, this is the primary mobile banking service provided by any bank. You can check the following:
  - View account balance (balance enquiry)
  - Transaction history
  - e-statement of account
  - Loan statements
  - Card statements
  - e-Passbooks

- **Transactions:** Making payments and transferring money from one account to another is the most basic banking activity. Therefore it only makes sense that these are the most used and in-demand mobile banking services. You can transfer funds to anyone by adding them as beneficiaries.
  - Bank to bank transfers
  - Transfer of funds to self
  - Payments to third parties (rent payments, bill payment, etc.)
  - Giving standing instructions for periodic payments
  - Payments via National Electronic Fund Transfer (NEFT)/ Immediate Payment Service (IMPS)/Real-time gross settlement(RTEG)/ Unified Payments Interface (UPI)/ Mobile Money Identifier (MMID).

- Investments
  - Opening fixed deposit/recurring deposits
  - Mutual fund investments
  - Portfolio management services (e.g. SBI Capital Securities)
- Other Services: Apart from the account summary, bill payments, fund transfers and investments, there are other services that a customer requires for smooth banking experience. These services include:
  - ATM locators
  - Branch locators
  - Lodging complaint/ tracking applications
  - Ordering new cheque book
  - Cancelling/stopping an issued cheque

Mobile Banking over SMS

- Along with mobile apps, most banks offer mobile banking services over SMS. This service is useful for those who do not have smartphones and/or internet connection. Customers need to register their mobile number with their bank in order to avail SMS banking.
- Services Offered by SMS Banking
  - Balance Enquiry
  - Get mini-statement
  - Transfer of funds to/from self-accounts (e.g. savings A/c to current A/c)
  - Block ATM card or a credit card
  - Enquiry for forex rates
  - Enquiring about current interest rates (e.g. FD rates and savings rates)

- These services are carried out by push/pull messages. Push messages mean when the bank initiates a communication, often reminding about payment or notification about a withdrawal. OTP or One-Time Password is also a type of push message that falls within the periphery of mobile banking.
- Pull messages are those messages that are initiated by the customer. These can be for account balance enquiry and for cancelling an issued cheque, etc.
- For instance, to check the available balance in their account, they may have to send an SMS in the format: AVAIL BAL XXXX where XXXX is the last 4 digits of the account number. The bank replies with an SMS with the current available balance in the account.

Mobile Banking over USSD

- USSD Mobile Banking is a type of communication via which one can exercise basic banking services. There is no need for a smartphone or an internet connection for this service. It allows services like balance enquiry and transfer of funds.
- *99# – a USSD based mobile banking service, has been launched by NPCI which is supported in 51 leading banks in India. The following services are offered by *99# USSD payment option:
  - Balance enquiry
  - Mini statement
  - Transfer of funds via
    - A/c no
    - Aadhaar
    - MMID
  - Change MPIN
  - Generate OTP


Thank you

WWW PROCESS

Dr P.V. Praveen Sundar
Assistant Professor,
Department of Computer Science
Adhiparasakthi College of Arts & Science,
Kalavai.

III BBA

World Wide Web

- The World Wide web consists of information organized into web pages containing text and graphic images.
- It contains hypertext links or highlighted keywords and images that lead to related information.
- A collection of linked web pages that has a common theme or focus is called website. The main page that all of the pages on a particular website are organized around and link back to is called Home Page.
- A web is a huge collection of pages of information linked to each other around the globe.
- A web page is created using HTML. It consists of standardized tags that are used to define the structure of information on a web page. These codes enable web pages to have many features including bold text, italic text, headings, paragraph break and numbered or bulleted lists.

Web Hosting Server

- Web hosting is a service that allows organizations and individuals to post a website or web page on to the Internet.
- A web host, or web hosting service provider, is a business that provides the technologies and services needed for the website or webpage to be viewed in the Internet.
- Websites hosted, or stored, on special computers called servers.

- When Internet users want to view your website, all they need to do is type your website address into their browser. Their computer will then connect to your server and your web pages will be delivered to them through the browser.
- Most hosting companies require that you own your domain name in order to host with them.
- If you do not have a domain name, the hosting companies will help you purchase one.

- There are various types of web hosting services available to host your website.
- Before signing up for web hosting services, it is important to understand what kind of service your website needs, the kind of server you or your business needs, your budget, and what type of services the web host offers.
- Hosting options available are:
  - Free Hosting
  - Shared Hosting
  - Dedicated Hosting
  - Collocated Hosting

Free Hosting

- Free web hosting can be a good choice when you just want to build a non-critical website for fun.
- Very often in a free hosting environment, connection speed is slow, website can be down frequently, and advertising banners is automatically added to your website.
- Some companies require you to purchase your domain name to receive free hosting services from them, while others offer you a free sub domain under them, such as [yourname.webhost.com].
- Be careful as you will be able to transfer these free sub domains.

Shared Hosting

- In a shared hosting environment, your and other website owners shared one server.
- This includes sharing the physical server and the software applications within the server.
- Shared hosting services are affordable because the cost to operate the server is shared between you and these other owners. There are, however, a number of down sides such as being slower.

Dedicated Hosting

- In a dedicated hosting environment, you have the entire web server to yourself.
- This allows for faster performance, as you have all the server's resources entirely, without sharing with other website owner However, this also means that you will be responsible for the cost of server operation entirely.
- This is a good choice for websites that requital a lot of system resources, or need a higher level of security.

Collocated Hosting

- In this type of hosting, you will purchase your own server and have it housed at a web host's facilities.
- We will be responsible for the server itself.
- An advantage of this type of hosting service is you have full control of the web server.
- We can install any scripts or applications you need.

Registering a Domain Name

- Choosing a select registrar is as important as choosing the right Web host.
- Selecting a domain name is an important marketing and branding consideration for any business. The domain name will be the business's online address and it provides an opportunity to create an identity for the business.
- A domain name is a name-based address that identifies an internet connected server.
- The domain name should be an easy-to-remember: name, (e.g., apcas.in) that the Domain Name System (DNS) maps to a corresponding IP (Internet Protocol) address, (e.g.,198.143.132.50).
- Each domain name starts with a Top-Level Domain (TLD) at the far right. This is either a general top-level domain or it is a country-code Top-Level Domain (ccTLD).

- Domain name assignment is under the authority of the Internet Corporation for Assigned Names and Numbers (ICANN).
- ICANN has delegated responsibility for domain name registration procedures and database administration in the general TLDs to top-level domain administrators such as Afilias (for .info), Public Interest Registry (for .org), and VeriSign Global Registry Services (for .com and .net). Similarly, regional internet registries administer the ccTLDs, (e.g., Nominet for the .uk domain, Japan Registry Service for .jp).
- Actual registration of domain names is carried-out by hundreds of ICANN—accredited registrars. These are located in various countries, but most are in the United States.
- A list of these registrars is available at

  www.icann.org/registrars/accredited-list.html

- A domain name registrar is a business that assists prospective website owners with finding and registering a domain name of their choice.
- The first step for a prospective web site owner is to visit a domain name registrar such as AllDomains (www.alldomains.hosting), or directNIC (www.directnic.com).
- Typically the owner will use the domain name look-up service at the registrars' website to determine if the desired domain name is available.

- If it is, the visitor is invited to register it through the registrar for a small fee. The registrar submits the domain name and the owner's details to the appropriate domain name database, and the name then becomes unavailable to anyone else.
- If the domain name is not available, most registrars automatically offer a list of available alternatives.
- If the desired domain name has already been taken, it sometimes can be purchased from the current owner.

- The BetterWhois database of registered domain names (www.betterwhois.com) contains the name, postal address, e-mail address, and telephone number of the domain name owner.
- A business with an established website will be reluctant to give-up a domain name, but if the domain name is reserved but not in use, the owner may be willing to sell it for a reasonable price.

- Once the name is registered with a registrar, it can be held by the registrar until the hosting service is in place. Then management of the domain name can be transferred from the registrar or previous owner to the host for establishment of the website.
- A useful resource for learning more about domain names and the registration process is About Domains (aboutdomains.com), which offers "guides and resources for successful internet presence", including a domain name glossary, a registration FAQ file, and "horror stories" from domain name owners who have had bad experiences with registrars.

Web Server.

- A Web Server is a computer that is dedicated to provide web services to clients on the internet.
- Web services are often provided through Web sites that are hosted on a Web server that is accessed by a client. However, before the clients can access the site, it is preferable to register the domain name at a Domain Name Service.
- Web servers also perform the following functions:
  - Provide access control, determining who can access particular directories or files on the Web server.
  - Run scripts and external programs to either add functionality to the Web documents or provide real time access to database and other dynamic data.
- This is done through various application programming interfaces, such as PHP or ASP.NET.

Web - Server Types

- **Apache HTTP Server:** This is the most popular web server in the world developed by the Apache Software Foundation.
- Apache web server is an open source software and can be installed on almost all operating systems including Linux, Unix, Windows, FreeBSD, Mac OS X and more.
- About 60% of the web server machines run the Apache Web Server.

Internet Information Services:

- The Internet Information Server (IIS) is a high-performance Web Server from Microsoft.
- This web server runs on Windows NT/2000 and 2003 platforms (and may be on upcoming new Windows version also).
- IIS comes bundled with Windows NT/2000 and 2003; Because IIS is tightly integrated with the operating system, so it is relatively easy to administer it.

Lighttpd:

- lighttpd: pronounced lighty is also a free web server that is distributed with the FreeBSD operating system.
- This open source web server is fast, secure and consumes much less CPU power.
- Lighttpd can also run on Windows, Mac OS X, Linux and Solaris operating systems.

Sun Java System Web Server:

- This web server from Sun Microsystems is suited for medium and large websites.
- Though the server is free it is not open source.
- However, it runs on Windows, Linux and Unix platforms.
- The Sun Java System web server supports various languages, scripts and technologies required for Web 2.0 such as JSP, Java Servlets, PHP, Perl, Python, Ruby on Rails, ASP and Coldfusion etc.

Jigsaw Server:

- Jigsaw (W3C's Server) comes from the World Wide Web Consortium.
- It is open source and free and can run on various platforms like Linux, Unix, Windows, Mac OS X Free BSD etc.
- Jigsaw has been written in Java and can run CGI scripts and PHP programs.

Domain Naming Systems (DNS)

- A domain name is a unique name associated with a specific IP address by a program that runs on an Internet host computer.
- This program, which coordinates the IP addresses and domain names for all computers attached to it, is called DNS (Domain Name System).
- Domain names are case insensitive so com and COM mean the same thing.

Types of Domain Naming System

- DNS is divided into two categories:
  - Generic Top Level Domain(gTLD)
  - Country code Top Level Domain(ccTLD)

Generic Top Level Domain (gTLD)

- There are seven domains within the generic top-level domal (gTLD).
- They .com, .org, .net, .gov, .mil, . edu, .int.
- The .com, .org, of .net are open domains and anyone can register their names within the domains.
- .edu is restricted to individuals register
- . gov is restricted to u by government agencies and its employees
- and mil is restricted to u military.

.biz	Business of all sizes
.com	commercial organizations, businesses and companies
.org	organisation site (non-profits, etc.)
.net	Network providers or commercial companies
.edu	educational site (universities, schools, etc.)
.gov	government organizations
.info	Business organizations of individuals providing general information's.
int	organizations established by international treaty
.mil	military site
.pro	Certified professionals such as doctors, lawyers and accountants.

Country code top- level domains (ccTLD)

- Country code top- level domains (ccTLD) are two letter designations assigned to individual countries.
- Each country linked to the Web has a two letter top-level domain, for example .fr is France, .ie is Ireland, in is India etc.
- Presently there are close to 250 such ccTLDs one for each country in the world.
- The registration process for sites with the ccTLDs slightly different from that using the gTLDs.
- The registration can be assigned through one of the several registrars accredited with The Internet Corporation for Assigned Names and Numbers(ICANN).
- ICANN currently accredits domain-name registrars for the following country code top level domain (ccTLD).

Domain	Country	Domain	Country
.af	Afghanistan	.it	Italy
.aq	Antarctica	.is	Island
.at	Austria	jP	Japan
.bd	Bangladesh	.kw	Kuwait
.bm	Bermuda	.lk	Sri Lanka
.br	Brazil	.ly	Libya
.bt	Bhutan	.ma	Morocco
.ca	Canada	.mn	Magnolia
.ch	Switzerland	.mx	Maxico
.cn	China	.ng	Nigeria
.co	Colombia	.n1	Netherland
.cu	Cuba	.nz	New Zealand
.de	Germany	.om	Oman
.dk	Denmark	.pk	Pakistan
.eg	Egypt	.qa	Qatar
.fr	France	.sa	Saudi Arabia
.hu	Hungary	.sd	Sudan
.in	India	.se	Sweden
.th	Thailand	.sg	Singapore
.tw	Taiwan		

Working of Domain Name System (DNS)

- DNS is a name resolution service that resolves host names to IP addresses. A DNS server resolves host names to IP addresses for DNS queries sent by the DNS clients. These queries can be in the form of name resolution query or a resource record.
- The resolver sends a User Datagram Protocol (UDP) packet to the local DNS server.
- The DNS server searches its table and returns the IP address, which matches the domain name.
- DNS has a hierarchical and distributed database that contains mappings of host names with the corresponding IP addresses.

- Resource records are stored in a specific portion of the DNS database called the DNS zone.
- A DNS zone contains resource records along with the owner names.
- For example, an application program calls a procedure with its domain name as parameter. The procedure sends an UDP packet to the local DNS server. The DNS server searches its table and returns the IP Address which matches the Domain name.
- The program can now establish a TCP connection or send UDP packets.

Accredited Registrar

- To purchase a domain name, one must find an accredited registrar.
- An accredited registrar, also called an accredited certification body (CB), is an organization accredited by a recognized accrediting body for its competence to audit and issue certification confirming that an organization meets the requirements of a standard (e.g. ISO 9001 or ISO 14001).
- Accreditation means that certification and inspection bodies have been assessed against recognized standards to demonstrate their competence, impartiality and capability.

Internet Cooperation for Assigned Names and Numbers (ICANN)

- To reach another person on the Internet, the user needs to type an address in his computer - a name or a number. That address has to be unique so computers know where to find each other.
- ICANN coordinates these unique identifiers across the world. Without that coordination we wouldn't have one global Internet.
- ICANN was formed in 1998. It is a not-for-profit partnership of people from all over the world dedicated to keeping the Internet secure, stable and interoperable.
- It promotes competition and develops policy on the Internet's unique identifiers.
- ICANN doesn't control content on the Internet. It cannot stop spam and it doesn't deal with access to the Internet. But through its coordination role of the Internet's naming system, it does have an important impact on the expansion and evolution of the Internet.

- ICANN plays a similar administrative role with the IP addresses used by computers as it does with the domain names used by humans.
- In the same way that you cannot have two domain names the same (otherwise you never know where you would end up), for the same reason it is also not possible for there to be two IP addresses the same.
- ICANN help co-ordinate how IP addresses are supplied to avoid repetition or clashes.
- ICANN is also the central repository for IP addresses, from which ranges are supplied to regional registries who in turn distribute them to network providers.

- ICANN has taken various measures to oversee the domain-name registration system's transition from government hands to private hands and to coordinate its decentralization and the integration into a global community.
- In more technical terms, the Internet Corporation for Assigned Names and Numbers (ICANN) coordinates the Domain Name System (DNS), Internet Protocol (IP) addresses, space allocation, protocol identifier assignment, generic (gTLD) and country code (ccTLD) Top-Level Domain name system management, and root server system management functions. These services were originally performed under U.S. Government contract by the Internet Assigned Numbers Authority (IANA) and other entities. ICANN now performs the IANA function.

Below are the lists of fastest growing ICANN registrars worldwide:

Registrars	Total Domains
GO DADDY	28,041,724
ENOM	6,965,073
TUCOWS	5,892,672
NETWORK SOLUTIONS	5,366,456
MELBOURNE IT	2,782,884
WILD WEST DOMAINS	2,439,543
REGISTER.COM	1,804,145
RESELLERCLUB.COM	1,567,875
FASTDOMAIN.COM	1,195,093

POP3

- Post Office Protocol version 3 (POP3) is a standard mail protocol used to receive emails from a remote server to a local email client.
- POP3 allows you to download email messages on your local computer and read them even when you are offline.
- When we use POP3 to connect to email account, messages are downloaded locally and removed from the email server. This means that accessing an account from multiple locations, that may not be the best option.
- On the other hand, while using POP3, the messages are stored on local computer, which reduces the space email account.
- By default, the POP3 protocol works on two ports:
  - Port 110 – this is the default POP3 non-encrypted port;
  - Port 995 – this is the port you need to use if you want to connect using POP3 securely.

IMAP

- The Internet Message Access Protocol (IMAP) is a mail protocol used for accessing email on a remote web server from a local client. IMAP and POP3 are the two most commonly used Internet mail protocols for retrieving emails. Both protocols are supported by all modern email clients and web servers.
- While the POP3 protocol assumes that your email is being accessed only from one application, IMAP allows simultaneous access by multiple clients. This is why IMAP is more suitable to access email from different locations or messages are managed by multiple users.
- By default, the IMAP protocol works on two ports:
  - Port 143 – this is the default IMAP non-encrypted port;
  - Port 993 – this is the port you need to use if you want to connect using IMAP securely.

Post Office Protocol (POP3)	Internet Message Access Protocol (IMAP)
POP is a simple protocol that only allows downloading messages from your Inbox to your local computer.	IMAP is much more advanced and allows you the user to see all the folders on the mail server.
The POP server listens on port 110, and the POP with SSL secure(POP3DS) server listens on port 995	he IMAP server listens on port 143, and the IMAP with SSL secure(IMAPDS) server listens on port 993.
In POP3 the mail can only be accessed from a single device at a time.	Messages can be accessed across multiple devices
To read the mail it has to be downloaded on the local system.	The mail content can be read partially before downloading.
The user can not organize mails in the mailbox of the mail server.	The user can organize the emails directly on the mail server.
The user can not create, delete or rename email on the mail server.	The user can create, delete or rename email on the mail server.
It has two modes : delete mode and keep mode. In delete mode , the mail is deleted from mail box after retrieval. In keep mode , the mail remains in the mail box after retrieval.	Multiple redundant copies of the message are kept at the mail server, in case of loss of message of a local server, the mail can still be retrieved
Changes in the mail can be done using local email software.	Changes made web interface or email software stay in sync with the server.
All the message are downloaded at once.	Message header can be viewed prior to downloading.

Internet Regulatory Organisations

- While there is no central internet governing body or a king of the World Wide Web, there are internet regulation bodies that work behind the scenes to keep everything running semi-smoothly.
- Here are the main internet regulation entities:
  1. **Internet Society:** It provides leadership in addressing issues that confront the future of the internet, and is the organization home for the groups responsible for internet infrastructure standards. (https://www.internetsociety.org/)
  2. **Internet Architecture Board:** Its responsibilities include internet standards and oversight. (https://www.iab.org/)
  3. **Internet Engineering Task Force:** A large open international community of network designers, operators, vendors, and researchers concerned with the evolution of the Internet architecture and the smooth operation of the internet. It is open to any interested individual. (https://www.ietf.org/)

4. **InterNIC:** It provides public information regarding internet domain name registration services. (https://www.internic.net/)
5. **PFIR — People for Internet Responsibility:** A group of people concerned about the present and future operations, development, management, and regulation of the internet. (https://www.pfir.org/)

Some other internet regulatory organizations are as follows:

- **ICANN:** Abbreviation for Internet Corporation for Assigned Names and Numbers. It is a private, California-based, non-profit corporation managing internet domain names and Internet Protocol (IP) addresses: It administers as dispute resolution system for resolving domain name disputes.

- **UDRP:** Abbreviation for Uniform Dispute Resolution Policy. This policy establishes a procedure for the online resolution of disputes that concern domain names.
  - This policy has been established by ICANN.
  - The UDRP is a non-national authority for the resolution of domain name disputes.
  - Its purpose is to avoid the competition and conflicts that arise from a variety of national courts and rules.
  - The UDRP is intended to be applied only to very flagrant types of cybersquatting.
  - The four institutions designated by ICANN to resolve domain name disputes are — WIPO, eResolution, the National Arbitration Forum, and the CPR Institute for Dispute Resolution.

- **The Internet Governance Forum (IGF)** is a multi stakeholder governance group for policy dialogue on issues of Internet governance.
- It brings together all stakeholders in the Internet governance debate, whether they represent governments, the private sector or civil society, including the technical and academic community, on an equal basis and through an open and inclusive process

- **The World Wide Web Consortium (W3C)** is the main international standards organization for the World Wide Web. Founded in 1994 and currently led by Tim Berners-Lee, the consortium is made up of member organizations that maintain full-time staff working together in the development of standards for the World Wide Web. W3C also engages in education and outreach, develops software and serves as an open forum for discussion about the Web.


Thank you