NETWORK PROTOCOLS AND SECURITY :

Computer or Nodes in a network follow some set of rules of communication. These set of rules is called Network Protocols.

"Network Protocols is a set of rules for communication which includes rules of how and when a device can send or receive the data and how it reaches its destination."

Some commonly used protocols are HTTP, TCP/IP, FTP and PPP etc. TCP/IP is a master protocol which comprises other protocols.

☑ **TCP/IPProtocol :**

The Transmission Control Protocol/ Internet Protocol Suite (TCP/IP) is most commonly used protocol to setup LAN, WAN, Internet and other similar networks.The TCP/IP Protocol Suite comprises 5 Layers including Physical media. Each layer is responsible for a well- defined task, and provides a well-defined service to the upper layers.

☑ **Hyper Text Transfer Protocol (HTTP) :**

HTTP is used to transfer web pages and data files from one computer to another on the World Wide Web (WWW). When you visit a web site on Web Browser program like Fire Fox, your computer becomes HTTP Client which receives web pages and data from web server. This communication is governed by the HTTP Protocol.

☑ **File Transfer Protocol(FTP) :**

FTP is used to transfer files from one computer to another on the Internet. Generally, it is used by Web Developer to upload web pages on the Web Hosting servers.

☑ **Point to Point Protocol(PPP) :**

It is a protocol used to establish a direct connection between two computers using Telephone lines. Before coming to ADSL Modems, most Internet Service Providers (ISPs) use PPP to provide dial-up access for the Internet to theircustomers.

MAC Address:

A Computer or node on a network needs a Network Interface Card (NIC) or LAN card. Each LAN card has unique 6-Byte Physical address assigned by the manufacturer, called **M**edia **A**ccess **C**ontrol (MAC) Address for its identification purpose. MAC address is a permanent physical address and does neverchange.

MAC addresses are 48-bit (6 Byte) hexadecimal numbers with each separated by colon and it looks like- MM : MM : MM : SS : SS : SS

The first half (MM) shows Manufacturer ID and second half (SS) shows unique serial number of the card. Example of MAC Address – 10:A0:C9:12:C5:32

IP Address:

Each machine in TCP/IP network needs to have a unique 32 bit (4 Byte) logical address called IP address.The IP address may be static or dynamic depending on the network type or network service provider. Generally all web servers and Gateways on Internet have static IP address.

In TCP/IP Network, an IP address of 32-bit number is known as Internet Protocol Version 4 (IPv4). This version theoretically ensures 232 possible unique addresses.

IP addresses are usually represented in dot-decimal notation (four numbers, each ranging from 0 to 255, separated by dots).

Example of IP address - 208.77.188.166

Domain Name:

In general, Domain name is a unique name assigned to a web server or web site. A domain name is also called Domain Name System (DNS). A Domain Name usually contains following parts-

(a) www

(b) Name of web server

(c) Top Level or Primary Domain and Sub-Domain name(s). For example :

"www.cbse.nic.in" Where **.in** is Primary domain and **NIC** is sub-domain of IN.

- Top level or Primary Domain are classified into **Generic Domains** like .com, .org, .edu, .net, .gov and **Country Domain** like .in, .ca, .jp, .nz, .us etc.
- The complete unique address of the page on a website is called **URL** (Uniform Resource Locator) e.g. http://www.cbse.nic.in/welcome.html

In general, we access any website through their domain name, because the domain name is much easier to memorise and recognize. Since computers on the network are identified by its IP addresses, so it is required to convert a Domain name or URL typed in the Browser into its corresponding IP address. The process of obtaining IP address from its domain name is called **Domain Name Resolution**. This resolution is done by the Designated Servers called DNS servers, provided by the Internet Service Providers (ISP) like BSNL or MTNL etc.

Wireless/MobileCommunication :

- **GSM :**

Global System for Mobile communications (GSM) is world's most widely used cell phone technology having 80% mobile phone users. It is a standard developed by the European Telecommunications Standards Institute (ETSI) to describe protocols for second generation (2G) digital cellular networks for mobile phones. GSM uses narrowband frequency ranges from 900 MHz to 1800 MHz based on Time Division Multiple Access (TDMA) technology. GSM users require Subscriber Identification Module (SIM)-a tiny chip that gives a cellular device its unique phone number.

- **CDMA :**

Code Division Multiple Access (CDMA) is an alternative cell phone technology to GSM. CDMA uses a "broad -spectrum" electromagnetic waves for signaling with wider bandwidth. This allows multiple people on multiple cell phones over the same channel to share a bandwidth of frequencies. In CDMAtechnology, data and voice packets are separated using codes and then transmitted using a wide frequencyrange.

- **3G :**

3G is the third generation of Wireless & Mobile technologies. It comes with enhancements over previous wireless technologies, like high-speed transmission, advanced multimedia access and global roaming. 3G is mostly used with mobile phones and handsets as a means to connect the phone to the Internet or other IP networks in order to make voice and video calls, to download and upload data and to surf thenet.

- **4G :**

4G is fourth-generation of wireless service, which refers to the next wave of high- speed mobile technologies that will be used to replace current 3G networks. The 4G wireless network is next step of 3G, available in limited countries and areas. The 4G is convergence of wired and wireless networks, wireless technologies including GSM, WLAN and Bluetooth as well as computers, communication devices and others. It is also called MAGIC, which stands for Mobile-Multimedia, Any-where, Global Mobility solutions over Integrated wireless and Customized services. It is Ip- based integrated system capable to provide 100Mbps speed offering IP telephony, Broadband Internet Access, HDTV streamed multimedia accessetc.

- **WLL (Wireless LocalLoop) :**

In traditional telephone networks, phone would be connected to the nearest exchange through a pair of copper wires. Wireless local loop (WLL) technology simply means that the subscriber is connected to the nearest telephone exchange through a radio link instead

of copper wires. WLL is more reliable and enhanced technology and offers high quality data transmission, signaling services and better bandwidth than traditional telephonesystem

- **Wi-Fi (WirelessFidelity) :**

Wi-Fi is a very common wireless technology that was developed in the 1990s. It is used to connect machines in a Local Area Network (LAN). So, Wi-Fi is like a wireless version of Ethernet. Wi-Fi allows 54 Mbps speed up to 300feet.

NETWORK SECURITY

In the modern age of networked information system, computers are not only capable of storing and processing data, but also delivering it on the globe. But, this increase connectivity of information system also brought some risk of privacy, theft and misuse of information.Information and Network security commonly refers the protection of data and network from various threats. It covers the following-

Confidentiality: Protection against unauthorized access. **Integrity:** Protected against unauthorized modification. **Authentication:** Identification of authorized user.

Security Threats :

☑ **Snooping :**

It refers to unauthorized access of someone else data, e-mail, computer activity or data communication. It may comprise monitoring of Keystrokes pressed, Capturing of passwords and login information and interception of e-mails and other private information.

☑ **Eavesdropping :**

It the act of secretly listening/ interpreting someone else's private communication or information while data is on its way on the network.

☑ **Spamming :**

Spamming refers to the sending of bulk-mail (junk-mail) by identified or unidentified sources.

☑ **Phishing :**

Phishing is a process of attempting to acquire sensitive information such as User name, passwords, Credit card number, bank account details etc. using a trap-mail in which user himself discloses their privatedetails.

☑ **Denial of Service (DoS)attack :**

DoS attack are those attacks that prevent the legitimate users from accessing or using the resources and information. These types of attack may eats up all the resources of the system and computer become to a halt state.

☑ **MaliciousProgram :**

Virus : Computer viruses are malicious and self-replicating codes/programs that cause damage to data and files on the computer system.

Worm : It is also a self-replicating program which eats entire disk space or memory. It copies itself until all the disk space or memory is filled.

Trojan horse : It is a program that appears harmless (like utility program) but actually performs malicious functions such as deleting damaging files.

Spyware : Spyware is a program designed to spy on your activities and report this data to people willing to pay it either legal or illegal purposes. It is getting installed in your system without your consent as a file or gets downloaded from Websites on Internet

☑ **Cookies :**

A cookie is message given to a web browser by a web server. The browser store these messages in a text file, which keeps track of users activity like user name, passwords, browsing history etc. and facilitates faster access of web page. Generally cookies do not act as malicious function, but are major

source of threat to privacy because by accessing cookies, the private and confidential information can be theft and misused.

☑ **Hackers &Crackers :**

A hacker is someone who seeks and exploits weaknesses in a computer system or computer network. Hackers may be motivated by various reasons such as profit, protest, or challenge. They are expert computer programmers who can break security to gain the computing resources and may exploit privacy.

Hacker, who breaks security for non-malicious reasons, perhaps to test any security system to make the security more effective, is called 'White Hat hacker'.The term "white hat" refers to an Ethical Hacker

Some Hackers can crack password or secure networks to destroy or theft data or make the network unusable for making money, are called Black Hat Hackers. Back |Hat Hackers are also called"crackers".

Network Security tools :

☑ **Authentication&Authorization(Login ID-Password) :**

A valid user is authenticated by a valid User-ID (Login Name) and correct passwordproves his/her Authorization to gain the systemresources. Generally, User name and Password in combination is used to provide better security.Generally, user name and password used to identify a legitimate user and grant permission (authorized) to access the system

☑ **Biometric Identification (PhysicalAuthentication)**

To provide more strong security, a system may have Biometric devices to identify a person by unique biological properties like Finger print , Retina Scan, Voice or Face Recognition etc., which cannot be transferred or stolen by others.

☑ **Anti-Virus for MaliciousProgram**

These Programs prevent the system from various malicious programs like Virus, Worms, Spywares and Trojan horses etc. The Anti-virus program monitors all running processes and activities, and notifies users in case of suspicious activites. The Anti-virus program must be updated regularly to provide better service.Some commonly used Anti- virus programs are- Quick Heal, Avast, Norton AV,Mcaffee etc.

☑ **CAPTCHA :**

CAPTCHA (Completely Automated Public Turing Test to tell Computers and Human Apart) is a program that displays distorted text/images as a challenge, which can read by human beings only. It ensures that website/program is being accessed by human being and not by malicious computer programs(bots).

☑ **Firewall**

☑ Firewall is a security system which acts like a gatekeeper or security wall to protect Computer or Network from unauthorized access. It monitors the network access as per rules defined by the Network Administrator. All requests entering or leaving theLAN

passed through the Firewall, which examines each requests and blocks those that do not meet the securitycriteria.

☑ **File AccessPermissions**

Files and folders which are stored and shared on the network may have limited access permissions like Read, Modify, Create and Execute rights as per need of the other users in the network.

☑ **Intrusion Detection System(IDS)**

It is system which identifies various types of Intrusions (Access attack) and monitors the user's activities and Network resources. It notifies to authorities in case of suspicious happenings. It is advanced system than Firewall, which provides a watch on internal and external user's suspicious activities and access for Network resources.

☑ **Digital Signature:**

Digital signature is a method for providing the authenticity of a message, document or attachment sent through e-mail. It is commonly used in Financial and Legal transactions where forgery and tempering of document is possible. It works like a valid signature of a person on a document which ensures recipient about authenticity of document.

☑ **Digital Certificate:**

Digital Certificate (Public Key Certificate) is an electronic document which uses digital signature and requires a public key or password to open or encode a document. It verifies and ensures that document belongs to an authorized individual ororganization.

Cyber Crime & Cyber Law :

Cyber crime refers to any crime wherein the computer is either a tool or a target or both. Some forms of Cyber Crime are-

- Creating and sending Spammails
- Posting offensive messages on Social NetworkingPortals.
- Hacking of Computer or Cracking Securitysystems.
- Unethical Financial transactions and Fraud throughInternet
- Harassment through e-mails and webmessages.
- Cyberterrorism.
- Creation & Propagation of Virus, Worms or Trojans etc.

Like traditional crime such as theft, fraud, forgery, defamation and mischief, Cyber Crime is also treated as criminal activities and is subject of punishment. The *Information Technology Act 2000 (IT Act)* in India provides legal support to the computer users against cyber crime. It also deals with Intellectual property rights on Internet