Networks and Security

Introduction

- The computers need to be interconnected to share information. Sharing of information leads to the collaboration of work and results in a collective environment. Such a congregation of computers is called a Network.
- A network is defined as the interconnection of computers for data and resource sharing.
- Two types of the most important types of networks are listed below:

1. Local Area Networt (LAN)
2. Wide Area Network (WAN)

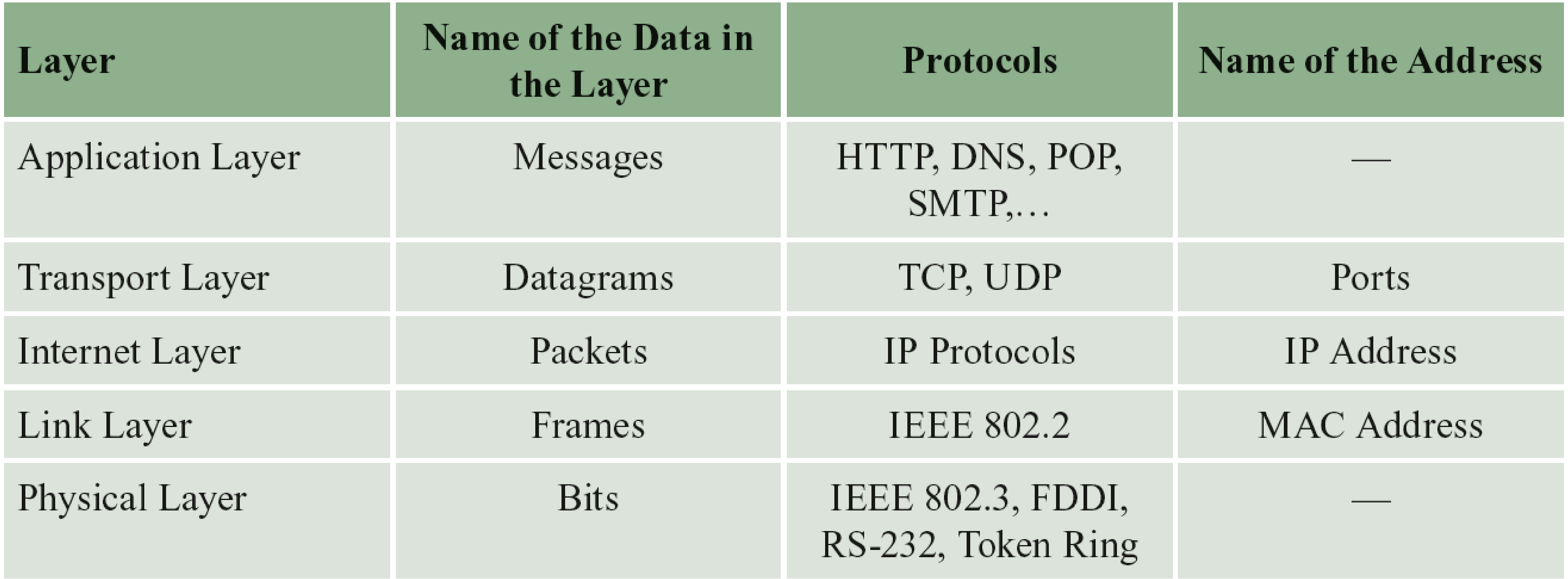
Open System Interconnect (OSI)

- The OSI is the standard for all types of connections and it contains seven layers. The seven layers in OSI Architecture are as follows:

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

Five Layer Architecture

- Layers along with the Protocols, Addresses, and Names of the Data in the Layer.



Layer	Name of the Data in the Layer	Protocols	Name of the Address
Application Layer	Messages	HTTP, DNS, POP, SMTP,…	—
Transport Layer	Datagrams	TCP, UDP	Ports
Internet Layer	Packets	IP Protocols	IP Address
Link Layer	Frames	IEEE 802.2	MAC Address
Physical Layer	Bits	IEEE 802.3, FDDI, RS-232, Token Ring	—

TCP/IP Architecture

- TCP is transport layer protocol and IP stands for Internet Protocol relating to the network layer.
- TCP/IP architecture is a four-layer architecture.

1. Application layer
2. Transport Layer
3. Internet Layer
4. Network Access Layer

Network Programming

- Network programming involves creating programs enabling the processes to communicate with each other over a network. For communicating with the process in other computers, communication establishing is important.
- The network devices handle the hardware components of the communications.
- To initiate communication, a software component should be created.

Client-Server Model: is a network model in which many clients requests and receive from a server. A client is a remote process that requests information for the process.

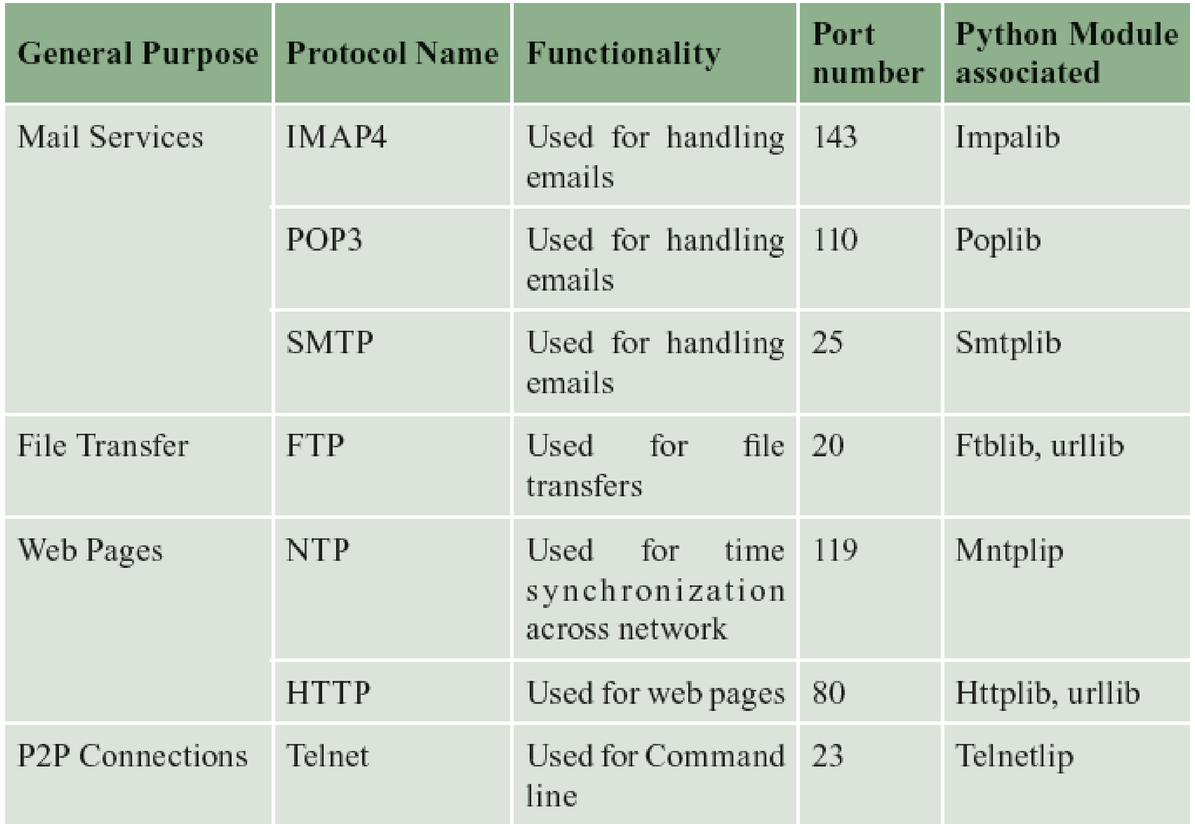
Socket Programming

- Socket Programming is the method of connecting two nodes on the network and communicating with each other.
- The socket package is available by default in Python Environment.
- The socket package is imported using the statement.
- The Processes performed with the socket are listed along with the syntax used in Python, discussed below,

1. Socket creation.
2. Binding the Socket (bind())
3. Listing to the socket (listen())
4. Connecting to the socket (connect())
5. Accepting the connection (accept())
6. Sending the data (send())
7. Receiving the data (recv())
8. Closing the socket (close())

Internet Modules in Python

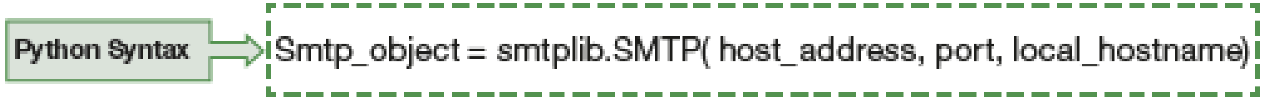
- Various packages and modules are used in Python for various purposes.



General Purpose	Protocol Name	Functionality	Port number	Python Module associated
Mail Services	IMAP4	Used for handling emails	143	Impalib
	POP3	Used for handling emails	110	Poplib
	SMTP	Used for handling emails	25	Smtplib
File Transfer	FTP	Used for file transfers	20	Ftblib, urllib
Web Pages	NTP	Used for time synchronization across network	119	Mntplip
	HTTP	Used for web pages	80	Httplib, urllib
P2P Connections	Telnet	Used for Command line	23	Telnetlip

Sending Emails

- In Python, it is possible to send emails without using the general web interface that the mail providers provide.
- The Email is governed by SMTP, POP, and IMAP protocols.
- The SMTP protocol handles the sending the mail between mail servers. In Python, the 'smtplib module' is used to utilize the SMTP protocol in which emails are sent from the interpreter to any mail server in the network that supports SMTP.
- The Gmail server and many email servers have deprecated third-party usages such as accessing from local machines for security reasons.
- An instance for the SMTP class from the smtplib module represents the SMTP link.
- The syntax for the instance created for the SMTP class is shown below.


Python Syntax

```
Smtp_object = smtplib.SMTP( host_address, port, local_hostname)
```

Web Scraping

- In this data era, the number of websites is increased; While doing various analyses, the data on the websites is needed. On many occasions, a large size of data are needed, and at many times, this is practically difficult. To solve this problem, web scrapping is used.
- Web scraping is the process of extracting data from websites automatically. The data extracted (scrapped) from the website could be structured or unstructured.
- The tools that are used for web scrapping in Python are as follows.

1) Beautifulsoup

2) Scrapy

3) Selenium

4) Urllib

5) LXML

6) Requests

Security

- Once the information is sent through the network in the form of packets, they are traceable by all the stakeholders involved in the network.
- The privacy of the information can not be assured in the an open network.
- Network security essentials are used to maintain privacy and to avoid malicious users.
- Cryptography is one of the major network security perspectives used today. Cryptography is securing information through the communication network using various algorithms and making the information understood only by the selected desired users.
- The concept of cryptography is divided
- into two major types, namely,
- 1) Classical Cryptography
- 2) Modern Cryptography

Classical Ciphers

- Classical cryptography algorithms are based on various complicated mathematical functions. These involve converting the input text to an encrypted text (called cipher text) on the sender side and converting the encrypted text to its original form on the receiver side.
- The process of converting the given input text to the intermediate form, which may convey a different meaning or meaningless combination of the text, is called encryption.
- After applying the process of encryption, the text is called encrypted text or cipher text.
- The reverse process of encryption is called decryption.
- Classical cryptography could be explained as the art of secret writing in which communication is kept secret unless the encrypting algorithm is a secret.
- There are several algorithms under classical cryptography.

Caeser Cipher

- Caesar cipher is one of the simplest cryptographic techniques. The mathematical model for the Ceaser Cipher is as follows. The value for the alphabet is assigned with values from 0 to 25, i.e., A = 0, B = 1, … , Z = 25. After converting the given string to a number, the encryption and decryption phase for the Ceaser Cipher is as follows.
- The encryption Phase of the Ceaser Cipher is given as,
- fE(x) = (x + n) mod 26
- In the encryption phase, the given alphabet is converted to the number and added with the value n.
- The added value is divided by 26, and the remainder is taken as the result. For the resulting value, the corresponding alphabet is substituted. The decryption Phase of the Ceaser Cipher is given as,

  fD(x) = (x – n) mod 26
- In the decryption phase, the given alphabet is converted to the number and subtracted with the value n; the remainder of the value (x-n) is divided by 26.

Asymmetric and Symmetric Algorithms

- Modern Cryptography algorithms are based on exchanging a key between the sender and receiver.
- The encrypting and decrypting of modern cryptographic algorithms involves one or more foreign keys to preserve secrecy.
- The keys are exchanged between the network nodes initially so that secrecy is prevented in the future.
- Symmetric key cryptographic algorithms use a single key for the both the process of encryption and decryption.
- Asymmetric key cryptographic algorithms use two keys, namely, public and private for encryption and decryption respectively.

RSA Algorithm

- RSA algorithm is an asymmetric key-based cryptographic algorithm, and it is based on the fact that factorizing a larger integer is a complex process.
- The public key consists of two numbers; one is the product of two prime numbers
- The Private key is also derived from the two prime numbers from where the public key is derived.
- RSA algorithm is implemented using RSA package.
- The private and public keys are created using the function newkeys()