**Linux Installation**

In General, we can install Linux in 4 types.

1. Fresh boot into a PC/Laptop.
2. Parallel boot alongside with windows.
3. Installation via virtual machine.
4. Install as WSL (Windows Subsystem for LINUX).

For first 3 methods, Please refer - <https://www.guru99.com/install-linux.html>

You may download it from - <https://ubuntu.com/download/desktop#download>

To install using WSL, Please follow below steps –

1. Open PowerShell as Administrator
2. Enter command -> **wsl --install**
3. If you are facing any errors while installing please refer this link for Manual installation steps - <https://www.windowscentral.com/install-windows-subsystem-linux-windows-10>

**Connectivity:**

There are several ways to connect to LINUX machine from windows.

Few of them are..

**By using SSH :**

**SSH** – **S**ecure **Sh**ell or Secure Socket Shell – It’s a protocol which allows us to connect with remote computers or a server by using a text based interface.

* It is installed in all Linux machines by default.
* ssh <username>@<IPaddress>
* Then it will ask for password – Input your password to login.(to External servers)
* Tools supported – Putty, CMD, Linux terminal, Powershell

**Communication Protocols:**

There are various types of protocols that support a major and compassionate role in communicating with different devices across the network. These are:

1. **Transmission Control Protocol (TCP)**: TCP is a popular communication protocol which is used for communicating over a network. It divides any message into series of packets that are sent from source to destination and there it gets reassembled at the destination.
2. **Internet Protocol (IP)**: IP is designed explicitly as addressing protocol. It is mostly used with TCP. The IP addresses in packets help in routing them through different nodes in a network until it reaches the destination system. TCP/IP is the most popular protocol connecting the networks.
3. **User Datagram Protocol (UDP)**: UDP is a substitute communication protocol to Transmission Control Protocol implemented primarily for creating loss-tolerating and low-latency linking between different applications.
4. **Post office Protocol (POP)**: POP3 is designed for receiving incoming E-mails.
5. **Simple mail transport Protocol (SMTP):** SMTP is designed to send and distribute outgoing E-Mail.
6. **File Transfer Protocol (FTP):** FTP allows users to transfer files from one machine to another. Types of files may include program files, multimedia files, text files, and documents, etc.
7. **Hyper Text Transfer Protocol (HTTP):** HTTP is designed for transferring a hypertext among two or more systems. HTML tags are used for creating links. These links may be in any form like text or images. HTTP is designed on Client-server principles which allow a client system for establishing a connection with the server machine for making a request. The server acknowledges the request initiated by the client and responds accordingly.
8. **Hyper Text Transfer Protocol Secure (HTTPS):** HTTPS is abbreviated as Hyper Text Transfer Protocol Secure is a standard protocol to secure the communication among two computers one using the browser and other fetching data from web server. HTTP is used for transferring data between the client browser (request) and the web server (response) in the hypertext format, same in case of HTTPS except that the transferring of data is done in an encrypted format. So it can be said that https thwart hackers from interpretation or modification of data throughout the transfer of packets.
9. **Telnet:** Telnet is a set of rules designed for connecting one system with another. The connecting process here is termed as remote login. The system which requests for connection is the local computer, and the system which accepts the connection is the remote computer.
10. **Gopher:** Gopher is a collection of rules implemented for searching, retrieving as well as displaying documents from isolated sites. Gopher also works on the client/server principle.

**Some other protocols are.**.

* ARP (Address Resolution Protocol)
* DHCP (Dynamic Host Configuration Protocol)
* IMAP4 (Internet Message Access Protocol)
* SIP (Session Initiation Protocol)
* RTP (Real-Time Transport Protocol)
* RLP (Resource Location Protocol)
* RAP (Route Access Protocol)
* L2TP (Layer Two Tunneling Protocol)
* PPTP (Point To Point Tunneling Protocol)
* SNMP (Simple Network Management Protocol)
* TFTP (Trivial File Transfer Protocol)

**Some other terminologies mentioned below**,

**DNS (domain name system)**: A service that provides the naming policy and mechanisms for mapping domain and machine names to addresses outside of the enterprise, such as those on the Internet. DNS is the network information service used by the Internet.

**DMA (direct memory access):** Some devices can perform data transfers that involve main memory and other devices without the help of the CPU. This type of data transfer is known as direct memory access (DMA).

**Digital signature:** A digital code that is attached to an electronically transmitted message that uniquely identifies the sender.

**CA (certificate authority):** A trusted third-party organization or company that issues digital certificates. The digital certificates are used to create digital signatures and public-private key pairs. CA guarantees the identity of the individual who is granted the unique digital certificate.

**DES (Data Encryption Standard):** A symmetric-key 64-bit block data encryption method standardized by ANSI as ANSI X.3.92. DES uses a 56-bit key.

**AES (Advanced Encryption Standard):** A symmetric 128-bit block data encryption technique. AES is the U.S. government encryption standard.

**Node:** In a computer network, a node is a connection point or an end point for the transmission of the data.

**NFS (Network File System):** A file system protocol that is used to remotely access shared files across a network. Oracle Solaris supports NFSv2, NFSv3, NFSv4, and NFSv4.1 versions.

**SSL (secure sockets layer):** A form of secure low-level encryption that is used by protocols like HTTP and FTP. The SSL protocol includes provisions for server authentication, encryption of data in transit, and optional client authentication.

**Hostname:** The name assigned to a workstation or server in a network

**Port number:** A port is a number used to uniquely identify a transaction over a network by specifying both the host, and the service. They are necessary to differentiate between many different IP services, such as web service (HTTP), mail service (SMTP), and file transfer (FTP). Please find the default port numbers.

|  |  |  |
| --- | --- | --- |
| **Port** | **Service name** | **Transport protocol** |
| 20, 21 | File Transfer Protocol (FTP) | TCP |
| **22** | Secure Shell (SSH) | TCP and UDP |
| 23 | Telnet | TCP |
| 25 | Simple Mail Transfer Protocol (SMTP) | TCP |
| 50, 51 | IPSec |  |
| 53 | Domain Name System (DNS) | TCP and UDP |
| 67, 68 | Dynamic Host Configuration Protocol (DHCP) | UDP |
| 69 | Trivial File Transfer Protocol (TFTP) | UDP |
| **80** | HyperText Transfer Protocol (HTTP) | TCP |
| 110 | Post Office Protocol (POP3) | TCP |
| 119 | Network News Transport Protocol (NNTP) | TCP |
| 123 | Network Time Protocol (NTP) | UDP |
| 135-139 | NetBIOS | TCP and UDP |
| 143 | Internet Message Access Protocol (IMAP4) | TCP and UDP |
| 161, 162 | Simple Network Management Protocol (SNMP) | TCP and UDP |
| 389 | Lightweight Directory Access Protocol | TCP and UDP |
| **443** | HTTP with Secure Sockets Layer (SSL) | TCP and UDP |
| 989, 990 | FTP over SSL/TLS (implicit mode) | TCP |
| 3389 | Remote Desktop Protocol | TCP and UDP |