**Day 1 Assignment 1:** **Explain Network Terminology.**

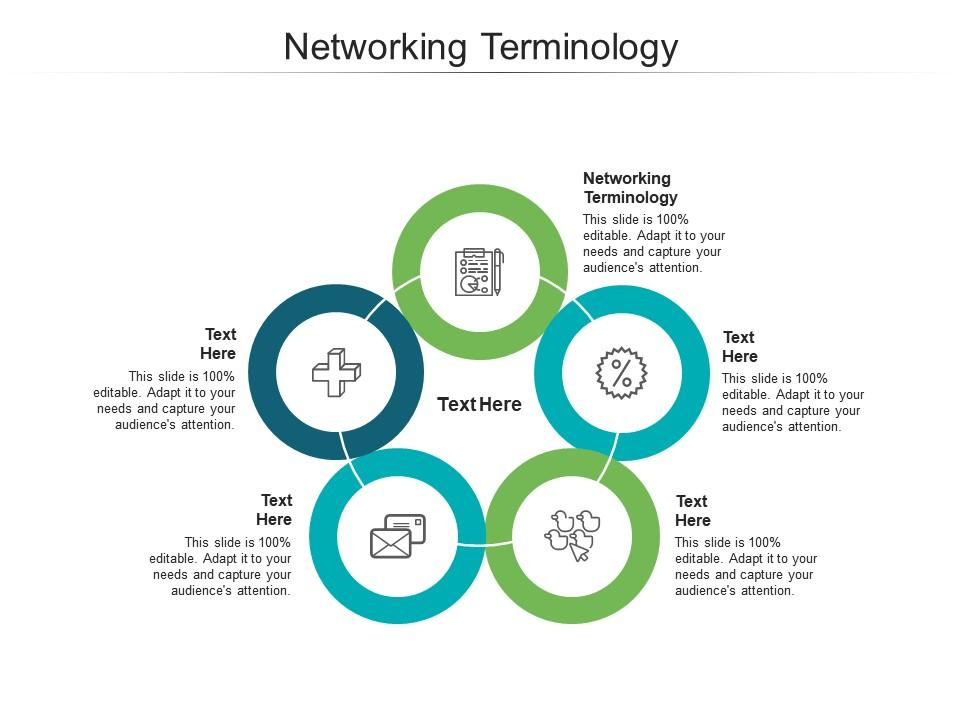
**Overview:**

A computer network is a set of connected devices. Devices are connected through a link. In the computer network, devices can transmit data and information using protocols.

The Internet is the biggest example of a network that connects devices globally and allows the transmission of data and information from anywhere in the world. The major terminology used in the network is protocol, ARP, Intranet, etc.

**Network Terminology:**

Notification sent by the receiver to the sender to acknowledge some data transmission. Acknowledgment is abbreviated as ACK and sent by the receiver to the sender as a receipt of data received. When the sender receives the acknowledgment sent by the receiver, then it will send the next packet to the receiver.



These terms will be expanded upon in the appropriate sections that follow:

**Connection:** In networking, a connection refers to pieces of related information that are transferred through a network. Generally speaking, a connection is established before data transfer (by following the procedures laid out in a protocol) and may be deconstructed at the end of the data transfer.

**Packet:** A packet is the smallest unit that is intentionally transferred over a network. When communicating over a network, packets are the envelopes that carry your data (in pieces) from one end point to the other.

**Network Interface:** A network interface can refer to any kind of software interface to networking hardware. For instance, if you have two network cards in your computer, you can control and configure each network interface associated with them individually.

**LAN**: LAN stands for “local area network”. It refers to a network or a portion of a network that is not publicly accessible to the greater internet. A home or office network is an example of a LAN.

**WAN:** WAN stands for “wide area network”. It means a network that is much more extensive than a LAN. While WAN is the relevant term to use to describe large, dispersed networks in general, it is usually meant to mean the internet, as a whole.

**Protocol:** A protocol is a set of rules and standards that define a language that devices can use to communicate. There are a great number of protocols in use extensively in networking, and they are often implemented in different layers.

**Port:** A port is an address on a single machine that can be tied to a specific piece of software. It is not a physical interface or location, but it allows your server to be able to communicate using more than one application.

**Firewall:** A firewall is a program that decides whether traffic coming or going from a server should be allowed. A firewall usually works by creating rules for which type of traffic is acceptable on which ports. Generally, firewalls block ports that are not used by a specific application on a server.

**NAT:** NAT stands for network address translation. It is a way to repackage and send incoming requests to a routing server to the relevant devices or servers on a LAN. This is usually implemented in physical LANs as a way to route requests through one IP address to the necessary backend servers.

**VPN:** VPN stands for virtual private network. It is a means of connecting separate LANs through the internet, while maintaining privacy. This is used to connect remote systems as if they were on a local network, often for security reasons.

**Network layers:**

While networking is often discussed in terms of topology in a horizontal way, between hosts, its implementation is layered in a vertical fashion within any given computer or network.

Each layer has the ability to add its own “wrapper” around the data that it receives from the adjacent layer, which will help the layers that come after decide what to do with the data when it is handed off.

**TCP/IP Model:**

**Application:** In this model, the application layer is responsible for creating and transmitting user data between applications. The applications can be on remote systems, and should appear to operate as if locally to the end user. This communication is said to take place between peers.

**Transport**: The transport layer is responsible for communication between processes. This level of networking utilizes ports to address different services.

**Internet:** The internet layer is used to transport data from node to node in a network. This layer is aware of the endpoints of the connections, but is not concerned with the actual connection needed to get from one place to another. IP addresses are defined in this layer as a way of reaching remote systems in an addressable manner.

**Link:** The link layer implements the actual topology of the local network that allows the internet layer to present an addressable interface. It establishes connections between neighbouring nodes to send data.

Some basic Protocols are:

* IP : Internet Protocol
* FTP : File Transfer Protocol
* SMTP : Simple Mail Transfer Protocol
* HTTP : Hyper Text Transfer Protocol

The Network reference models were developed to allow products from different manufacturers to interoperate on a network. A network reference model serves as a blueprint, detailing standards for how protocol communication should occur.

The most widely recognized reference models are the Open Systems Interconnect ( OSI ) Model and Department of Defense ( DoD, also known as TCP/IP) model.

* **LANs** (Local Area Networks)
* **MANs** (Metropolitan Area Networks)
* **WANs** (Wide Area Networks)

An Internwork is a general term describing multiple networks connected together. The Internet is the largest and most well-known internetwork.

SAN(Storage Area Network): A SAN provides systems with high-speed, lossless access to high-capacity storage devices.

VPN(Virtual Private Network): A VPN allows for information to be securely sent across a public or unsecured network, such as the Internet. Common uses of a VPN are to connect branch offices or remote users to the main office.

**DNS:**

DNS stands for domain name system. It is an application layer protocol used to provide a human-friendly naming mechanism for internet resources. It is what ties a domain name to an IP address and allows you to access sites by name in your browser.

**SSH:**

SSH stands for secure shell. It is an encrypted protocol implemented in the application layer that can be used to communicate with a remote server in a secure way. Many additional technologies are built around this protocol because of its end-to-end encryption and ubiquity.

There are many other protocols that we haven’t covered that are equally important. However, this should give you a good overview of some of the fundamental technologies that make the internet and networking possible.

**Conclusion:**

At this point, you should be familiar with some networking terminology and be able to understand how different components are able to communicate with each other. This should assist you in understanding other articles and the documentation of your system.