# ***Network***

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.

A computer network can be categorized by their size. A **computer network** is mainly of **four types**:



* LAN (Local Area Network)
* PAN (Personal Area Network)
* MAN (Metropolitan Area Network)
* WAN (Wide Area Network)

LAN (Local Area Network)

* Local Area Network is a group of computers connected to each other in a small area such as 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.



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.



**There are two types of Personal Area Network:**



* Wired Personal Area Network
* Wireless Personal Area Network

**Wireless Personal Area Network:** Wireless Personal Area Network is developed by simply using wireless technologies such as WIFI, Bluetooth. It is a low range network.

**Wired Personal Area Network:** Wired Personal Area Network is created by using the USB.

Examples Of Personal Area Network:

* **Body Area Network:** Body Area Network is a network that moves with a person. **For example**, a mobile network moves with a person. Suppose a person establishes a network connection and then creates a connection with another device to share the information.
* **Offline Network:** An offline network can be created inside the home, so it is also known as a **home network**. A home network is designed to integrate the devices such as printers, computer, television but they are not connected to the internet.
* **Small Home Office:** It is used to connect a variety of devices to the internet and to a corporate network using a VPN

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.
* The most widely used protocols in MAN are RS-232, Frame Relay, ATM, ISDN, OC-3, ADSL, etc.
* It has a higher range than Local Area Network (LAN).



Uses Of Metropolitan Area Network:

* MAN is used in communication between the banks in a city.
* It can be used in an Airline Reservation.
* It can be used in a college within a city.
* It can also be used for communication in the military.

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.



Examples Of Wide Area Network:

* **Mobile Broadband:** A 4G network is widely used across a region or country.
* **Last mile:** A telecom company is used to provide the internet services to the customers in hundreds of cities by connecting their home with fibre.
* **Private network:** A bank provides a private network that connects the 44 offices. This network is made by using the telephone leased line provided by the telecom company.

Advantages Of Wide Area Network:

Following are the advantages of the Wide Area Network:

* **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.
* **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 of Wide Area Network:

The following are the disadvantages of the Wide Area Network:

* **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**.
* The reference model used for internetworking is **Open System Interconnection (OSI)**.

Types Of Internetwork:

1. **Extranet:** An extranet is a communication network based on the internet protocol such as **Transmission Control protocol** and **internet protocol**. It is used for information sharing. The access to the extranet is restricted to only those users who have login credentials. An extranet is the lowest level of internetworking. It can be categorized as **MAN**, **WAN** or other computer networks. An extranet cannot have a single **LAN**, at least it must have one connection to the external network.

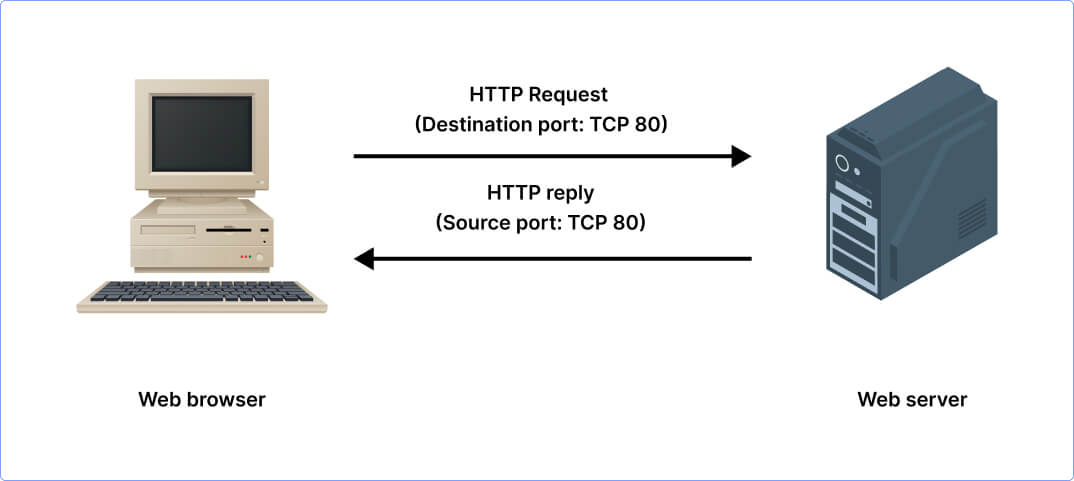
2. **Intranet:** An intranet is a private network based on the internet protocol such as **Transmission Control protocol** and **internet protocol**. An intranet belongs to an organization which is only accessible by the **organization's employee** or members. The main aim of the intranet is to share the information and resources among the organization employees. An intranet provides the facility to work in groups and for teleconferences.

Intranet advantages:

* **Communication:** It provides a cheap and easy communication. An employee of the organization can communicate with another employee through email, chat.
* **Time-saving:** Information on the intranet is shared in real time, so it is time-saving.
* **Collaboration:** Collaboration is one of the most important advantages of the intranet. The information is distributed among the employees of the organization and can only be accessed by the authorized user.
* **Platform independency:** It is a neutral architecture as the computer can be connected to another device with different architecture.
* **Cost effective:** People can see the data and documents by using the browser and distributes the duplicate copies over the intranet. This leads to a reduction in the cost.

**What is a Port Number in Networking?**

A port number is a 16-digit number that acts as a unique identifier for a connection endpoint or a service running on a host. Let’s consider an example for easy understanding.

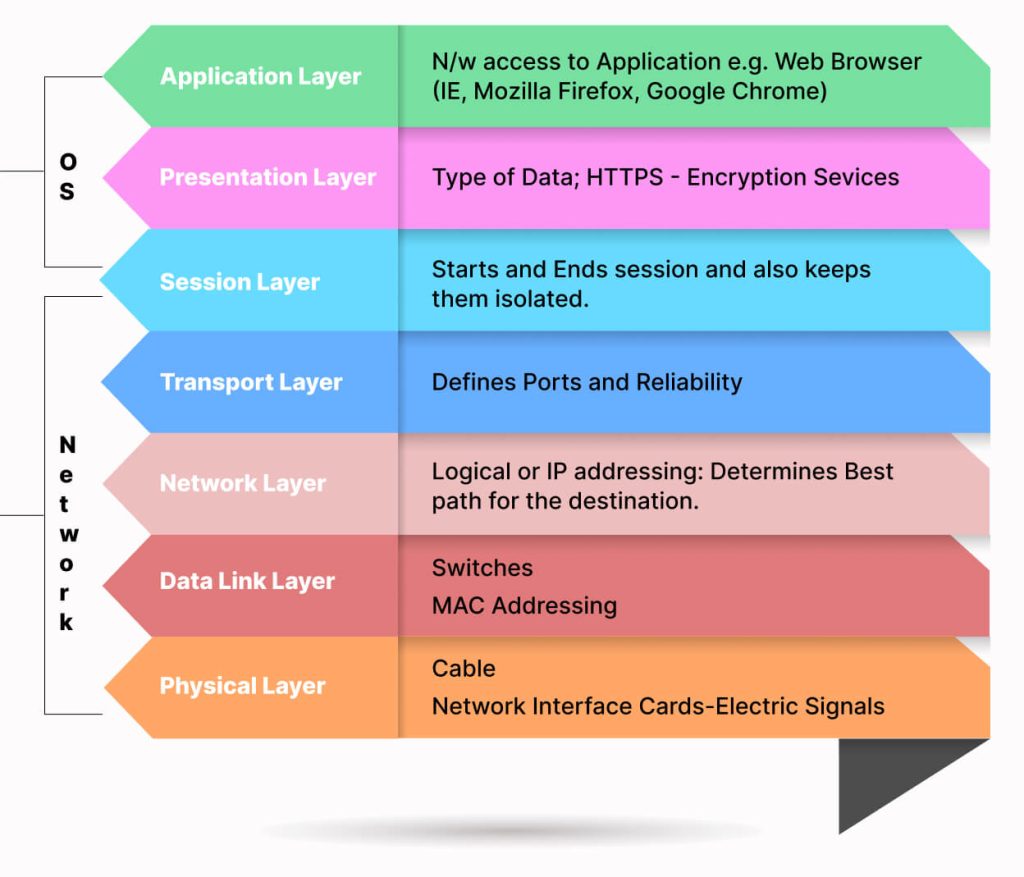


*Suppose you have different services running on your computer like your email, web browser, instant chat app, etc. Now each service you use has its own port number. When you browse a website by typing the web address and hitting enter, your web browser sends a request to get access to the website using port number 80. Likewise, when you open your email client to send an email, it uses port 25 to send your message and as you refresh to check for new emails, the client uses port 110. Further, as you open your instant chat app to talk with a friend in real time, the app communicates using port 6667.*

So, each service you use has its own specific port number. When your device i.e. your computer sends or receives data, it knows which door to use based on the service you’re accessing.

***Insight:****Port Numbers in networking are logical endpoints which is why they are often referred to as Logical Ports as well.*

Which Layer are Ports in the OSI Model?



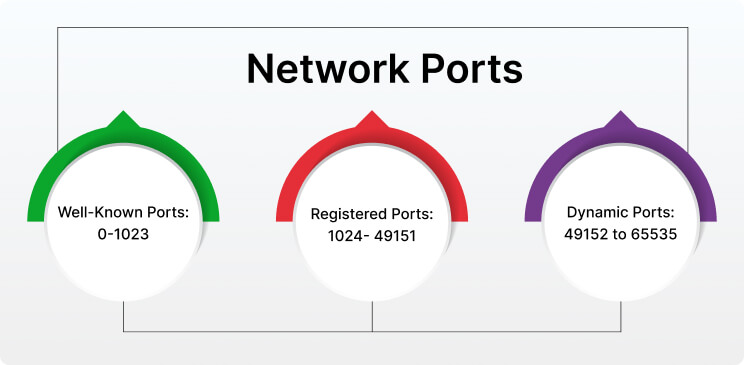
The OSI model is a conceptual model that represents how network communications work. This model has 7 layers shown in the above image. Ports are associated with the Transport Layer i.e. Layer 4 of the OSI model. The Transport Layer primarily makes use of 2 protocols – TCP and UDP. These protocols are needed to specify which port a packet should go to. In the header section of TCP and UDP, the information about port numbers is defined.

Difference Between IP Address and Port Number

In the context of networking, it is important to learn the difference between an IP address and a port number. It will help you understand how data is directed within a network. So let’s take a look:

An IP address identifies a machine in an IP network and is used to identify the destination address of a packet. On the other hand, a port number identifies a certain service or application on a system.

What are the Different Port Numbers?



Logical ports are categorized into 3 main types which are:

* Well Known Ports

These port numbers range from 0 to 1023. Well-known port numbers are specifically reserved for standard services. For example, Hyper Text Transfer Protocol i.e. HTTP uses port 80, FTP uses port 21, DNS uses port 53, etc.

* Registered Ports

The range for these ports is from 1024 to 49151. Registered ports are assigned by the Internet Assigned Number Authority (IANA) to specific services and applications that are not very common.

* Dynamic Ports

Dynamic Ports are also called Private Ports or Ephemeral Ports. The range for these ports is 49152 to 65535. These ports are used for short-lived or temporary connections. Also, these ports are not pre-assigned to any specific service.

Now, we have learned about the different types of ports and the port ranges assigned to them. In the next section, let’s catch a glimpse of why these ports hold significant value in networking.

What are some Popular Port Numbers?

There are a total of 65535 port numbers. So their range is from 0 to 65535. The list of port numbers is maintained by IANA and below are some commonly used port numbers along with their service and use. Have a look:

* **21:** It is used by FTP i.e. File Transfer Protocol which transfers files over a network.
* **22:** This port number is used by SSH i.e. Secure Shell which provides a secure remote command-line login.
* **23:** It is used by Telnet for remote terminal access (unencrypted).
* **25:** This port is used by SMTP i.e. Simple Mail Transfer Protocol which is responsible for email routing.
* **53:** It is used by DNS i.e. Domain Name System which resolves domain names to IP addressed.
* **80:** This port number is used by HTTP i.e. Hypertext Transfer Protocol which is used for unencrypted web traffic.
* **110:** It is used by POP3 (Post Office Protocol version 3) which retrieves emails from a server.
* **143:** This port number is used by IMAP i.e. Internet Message Access Protocol which manages and retrieves emails from a mail server.
* **443:** It is used by HTTPS (Hypertext Transfer Protocol Secure) which is used for secure web traffic with encryption.
* **465:** This port number is used by SMTPS (SMTP Secure) which is for secure email sending.
* **123:** It is used by NTP i.e. Network Time Protocol which synchronizes clocks on networked devices.
* **5060:** This port number is used by SIP i.e. Session Initiation Protocol for VoIP communication.
* **16384-32767:** This range of port numbers is used by RTP i.e. Real-time Transport Protocol for audio and video transmission.
* **2049:** It is used by the Network File System for file sharing.
* **3389:** This port is used by RDP i.e. Remote Desktop Protocol to enable users to connect to their desktop computers from another device remotely

***Protocol and Its Types***

In today’s technological world, we’re talking about millions of users communicating with different devices in different languages. That also includes various ways in which they transmit data along with the software they implement. Therefore, when discussing what is protocol and its types in networking, we need to point out that communicating worldwide would not be possible if there were no fixed ‘standards’ to govern the way users communicate for data as well as the way our devices treat that data.

## What Is Protocol and Its Types in Networking?

According to the [**Florida Centre for Instructional Technology**](https://fcit.usf.edu/network/chap2/chap2.htm), protocol is defined as **a set of rules that govern the communications between computers on a network**.

[**EDUCBA**](https://www.educba.com/types-of-networking-protocols/) adds that network protocols are formalized requirements and plans consisting of **rules**, **procedures**, and **types** that describe communication among a couple of devices across the network.

In networking, protocol can be described as an approach to rules that allows entities of a communication program to transfer information through any type of variety of physical medium. The protocol “identifies the **rules**, **syntax**, **semantics**, and **synchronization of communication** and **feasible error managing methods**”.

## Types of Networking Protocols

For two computers to communicate with each other, they must be speaking the same language. Different types of network protocols and standards are required to ensure that a computer (regardless of its OS, network card, or application used) can communicate with another one located in the next room or halfway around the world.

There are seven layers of networking protocols defined by the [**OSI (Open Systems Interconnection)**](https://heimdalsecurity.com/blog/osi-layers/) Reference Model. The complexity of these layers is beyond the scope of this article, nevertheless, they were simplified below into four layers to help identify some of the protocols you should be familiar with.

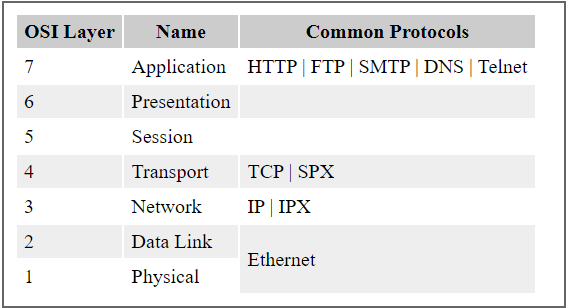


Image Source: [**Florida Centre for Instructional Technology**](https://fcit.usf.edu/network/chap2/chap2.htm)

Below, I will discuss the different types of networking protocols.

1. **Physical layer.** The [physical layer](https://www.techtarget.com/searchnetworking/definition/physical-layer) is the initial layer that physically connects two interoperable systems. It controls simplex or [duplex](https://www.techtarget.com/searchnetworking/definition/full-duplex) modem transmissions and transfers data in bits. Additionally, it oversees the hardware that connects the network interface card ([NIC](https://www.techtarget.com/searchnetworking/definition/network-interface-card)) to the network, including the wiring, cable terminators, topography and voltage levels.
2. **Data-link layer.** The [data-link layer](https://www.techtarget.com/searchnetworking/definition/Data-Link-layer) is responsible for the error-free delivery of data from one node to another over the physical layer. It's also the [firmware](https://www.techtarget.com/whatis/definition/firmware) layer of the NIC. It puts datagrams together into frames and gives each frame the start and stop flags. Additionally, it fixes issues brought on by broken, misplaced or duplicate frames.
3. **Network layer.** The [network layer](https://www.techtarget.com/searchnetworking/definition/Network-layer) is concerned with information flow regulation, switching and routing between workstations. Additionally, it divides up datagrams from the transport layer into error-free and smaller datagrams.
4. **Transport layer.** The [transport layer](https://www.techtarget.com/searchnetworking/definition/Transport-layer) transfers services from the network layer to the application layer and breaks down data into data frames for error checking at the network segment level. This also ensures that a fast host on a network doesn't overtake a slower one. Essentially, the transport layer ensures that the entire message is delivered from beginning to end. It also confirms a successful data transmission and retransmitting of the data if an error is discovered.
5. **Session layer.** The [session layer](https://www.techtarget.com/searchnetworking/definition/Session-layer) establishes a connection between two workstations that need to communicate. In addition to ensuring security, this layer oversees connection establishment, session maintenance and [authentication](https://www.techtarget.com/searchsecurity/definition/authentication).
6. **Presentation layer.** The [presentation layer](https://www.techtarget.com/searchnetworking/definition/presentation-layer) is also known as the *translation layer* because it retrieves the data from the application layer and formats it for transmission over the network. It addresses the proper representation of data, including the syntax and semantics of information. The presentation layer is also in charge of managing [file-level security](https://www.techtarget.com/searchcontentmanagement/tip/7-common-file-sharing-security-risks) and transforming data to network standards.
7. **Application layer.** The [application layer](https://www.techtarget.com/searchnetworking/definition/Application-layer), which is the top layer of the network, oversees relaying user application requests to lower levels. File transfer, email, remote login, data entry and other common applications take place at this layer.

## Network Communication Protocols

### 1. HTTP and HTTPS

Often referred to as the protocol of the Internet, HTTP/HTTPS stands for Hypertext Transfer Protocol and Hypertext Transfer Protocol (secure) respectively.

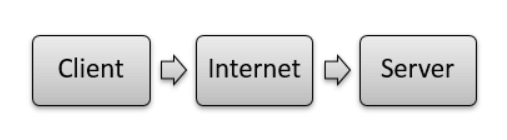


Image Source: [**EDUCBA**](https://www.educba.com/types-of-networking-protocols/)

The majority of application-layer protocols employ this model, using one device on the client’s network; the other device on the network is the server.

In the case of HTTP, Client-server principles 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.

While HTTP is used for transferring data between the client browser (request) and the web server (response) in the hypertext format, in the case of HTTPS the transferring of data is done in an encrypted format. Therefore, we can say that [**HTTPS**](https://heimdalsecurity.com/blog/https-security-101/) thwarts hackers from the interpretation or modification of data throughout the transfer of packets.

### 2. FTP (File Transfer Protocol)

FTP allows users to transfer files (program files, multimedia files, text files, documents, etc) from one machine to another.

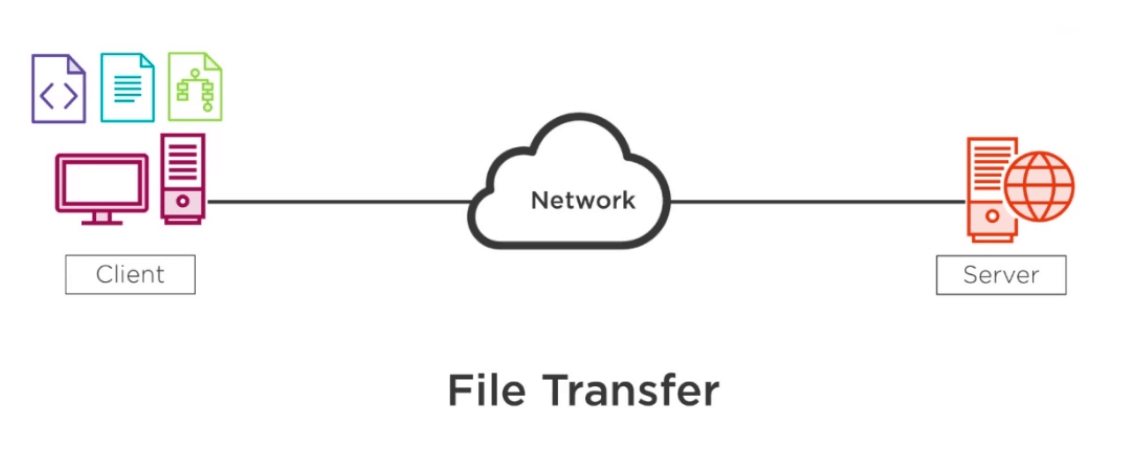


Image Source: [**EDUCBA**](https://www.educba.com/types-of-networking-protocols/)

### 3. TCP (Transmission Control Protocol)

[**TCP**](https://heimdalsecurity.com/blog/what-is-tcp/) is a popular communication protocol that separates data into packets that can be distributed across a network. Afterward, they can be sent by devices such as switches and routers to the designated targets.

### 4. UDP (User Datagram Protocol)

Although UDP works in a similar way to TCP, the main difference between the two is that TCP ensures a connection is made between the application and server, but UDP does not. User Datagram Protocol is mainly implemented for creating loss-tolerating and low-latency linking between various apps.

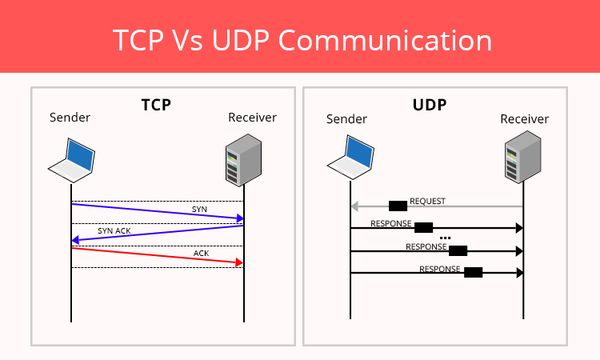


Image Source: [**CyberHoot**](https://cyberhoot.com/cybrary/transmission-control-protocol-tcp/)

### 5. IRC (Internet Relay Chat)

IRC is a text-based communication protocol that facilitates communication in the form of text. Although it supports private messages between two users, data transfer, and various server-side and client-side commands It is mainly used for group discussion in chat rooms called “channels”. This protocol works well on networks with numerous distributed machines.

## what is protocol and its types in networking IRC

Image Source: [**ResearchGate**](https://www.researchgate.net/figure/IRC-based-Botnet-Architecture-79_fig2_282477239)

## Network Management Protocols

### 1. SNMP (Simple Network Management Protocol)

[**SNMP**](https://heimdalsecurity.com/blog/what-is-snmp-in-computer-network-science/) is a standard protocol used to exchange network management information. It is part of the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite. SNMP provides a tool for network administrators to manage network performance, find and solve network issues, and plan for network growth.

### 2. ICMP (Internet Control Message Protocol)

ICMP is a network layer protocol mainly used to communicate with the source of a data packet about transmission issues. For example, if a datagram is not delivered, ICMP might report this back to the host with details to help discern where the transmission went wrong. It’s a protocol that believes in direct communication in the workplace.

## Network Security Protocols

### 1. SSL (Secure Socket Layer)

[**SSL**](https://heimdalsecurity.com/blog/what-is-ssl-vulnerability/) is a network security protocol used for data protection on the transport layer, and it’s located between the transport and application layer of the ISO/OSI reference model providing security services to any application-based protocols, like HTTP, FTP, LDAP, POP3. The SSL protocol is used in any client/server environment, being able to provide a series of features for the parties involved in the communication process. Data transferred with SSL is encrypted to prevent it from being readable.

### 2. SFTP (Secure File Transfer Protocol)

As its name suggests, this network security protocol is used to securely transfer files across a network. Data is encrypted and both the client and server are authenticated.

## Final Thoughts on What Is Protocol and Its Types in Networking

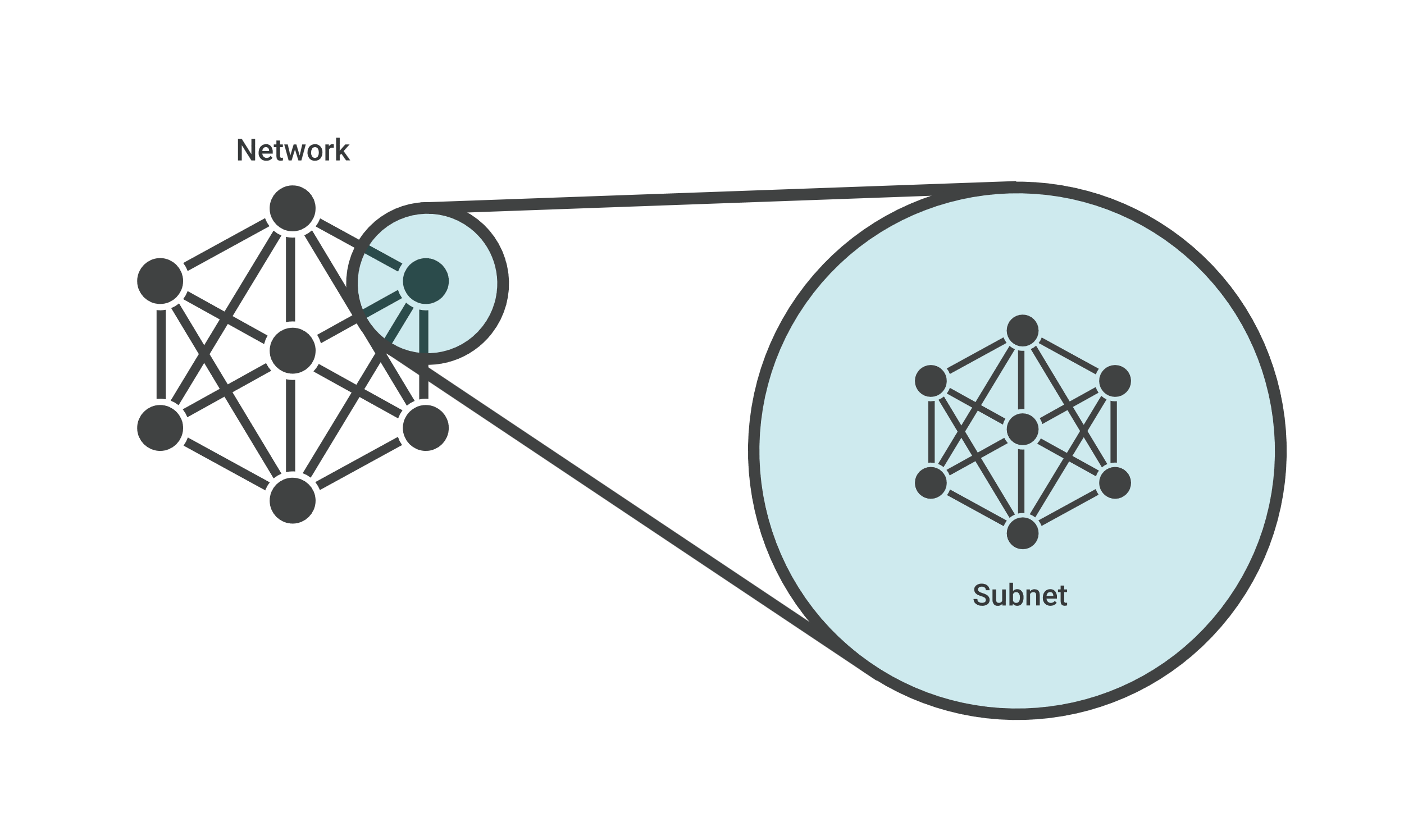
Every time we use the Internet, we leverage network protocols. Though you may not know how network protocols work or how frequently you encounter them, they are necessary for browsing the Internet or digital communications in any capacity.

Forging strongly into parts of existence that nobody had predicted, digital networking is additionally strengthening us for the future. New protocols and requirements will come out, new applications can be developed, and our lives will probably be further transformed and improved.

I hope this guide on what is protocol and its types in networking has been helpful. Drop a line below if you have any **comments**, **questions**, or **suggestions** related to the topic – I look forward to hearing your opinion!

**subnet**

A subnet, or subnetwork, is a [network](https://www.cloudflare.com/learning/network-layer/what-is-the-network-layer/) inside a network. Subnets make networks more efficient. Through subnetting, network traffic can travel a shorter distance without passing through unnecessary [routers](https://www.cloudflare.com/learning/network-layer/what-is-routing/) to reach its destination.



Imagine Alice puts a letter in the mail that is addressed to Bob, who lives in the town right next to hers. For the letter to reach Bob as quickly as possible, it should be delivered right from Alice's post office to the post office in Bob's town, and then to Bob. If the letter is first sent to a post office hundreds of miles away, Alice's letter could take a lot longer to reach Bob.

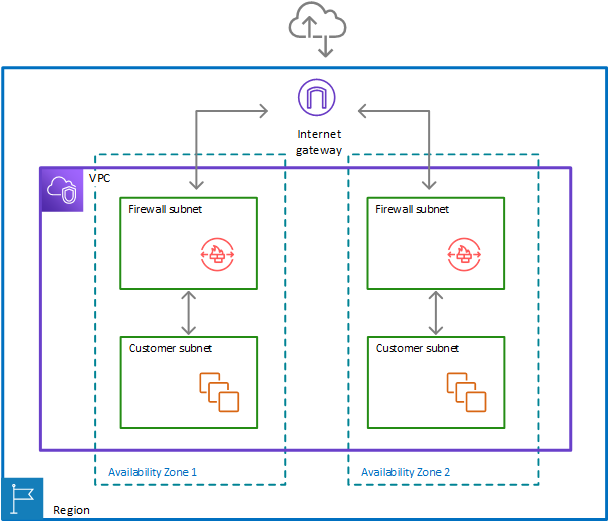
Like the postal service, networks are more efficient when messages travel as directly as possible. When a network receives data packets from another network, it will sort and route those packets by subnet so that the packets do not take an inefficient route to their destination.

**Public subnet vs Private subnet**

Public subnet – The subnet has a direct route to an internet gateway. Resources in a public subnet can access the public internet. Private subnet – The subnet does not have a direct route to an internet gateway. Resources in a private subnet require a NAT device to access the public internet

**Internet Gateway**

An Internet Gateway (IGW) is an AWS component that provides a path for network traffic to travel between a Virtual Private Cloud (VPC) and the public internet. It acts as a bridge between the two networks, enabling inbound and outbound connections from resources within the VPC



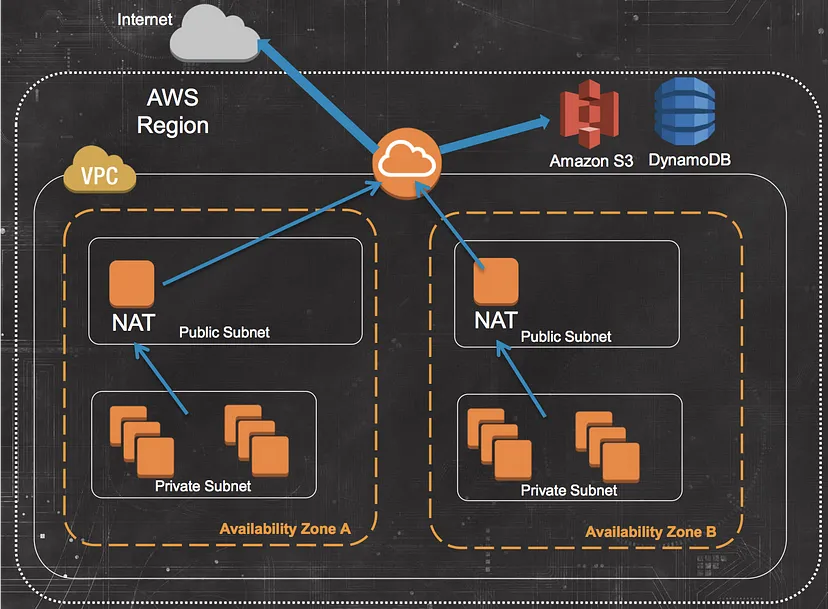
**Nat Gateway**

A NAT gateway is a Network Address Translation (NAT) service. You can use a NAT gateway so that instances in a private subnet can connect to services outside your VPC but external services cannot initiate a connection with those instances.

When you create a NAT gateway, you specify one of the following connectivity types:

* **Public** – (Default) Instances in private subnets can connect to the internet through a public NAT gateway, but cannot receive unsolicited inbound connections from the internet. You create a public NAT gateway in a public subnet and must associate an elastic IP address with the NAT gateway at creation. You route traffic from the NAT gateway to the internet gateway for the VPC. Alternatively, you can use a public NAT gateway to connect to other VPCs or your on-premises network. In this case, you route traffic from the NAT gateway through a transit gateway or a virtual private gateway.
* **Private** – Instances in private subnets can connect to other VPCs or your on-premises network through a private NAT gateway. You can route traffic from the NAT gateway through a transit gateway or a virtual private gateway. You cannot associate an elastic IP address with a private NAT gateway. You can attach an internet gateway to a VPC with a private NAT gateway, but if you route traffic from the private NAT gateway to the internet gateway, the internet gateway drops the traffic.

Both private and public NAT gateways map the source private IPv4 address of the instances to the private IPv4 address of the NAT gateway, but in the case of a public NAT gateway, the internet gateway then maps the private IPv4 address of the public NAT Gateway to the Elastic IP address associated with the NAT Gateway. When sending response traffic to the instances, whether it's a public or private NAT gateway, the NAT gateway translates the address back to the original source IP address



**Internet Gateway vs NAT Gateway**

Internet GW allows both inbound and outbound access to the internet whereas the NAT Gateway only allows outbound access. Thus, IgW allows instances with public IPs to access the internet whereas NAT Gateway allows instances with private IPs to access internet.

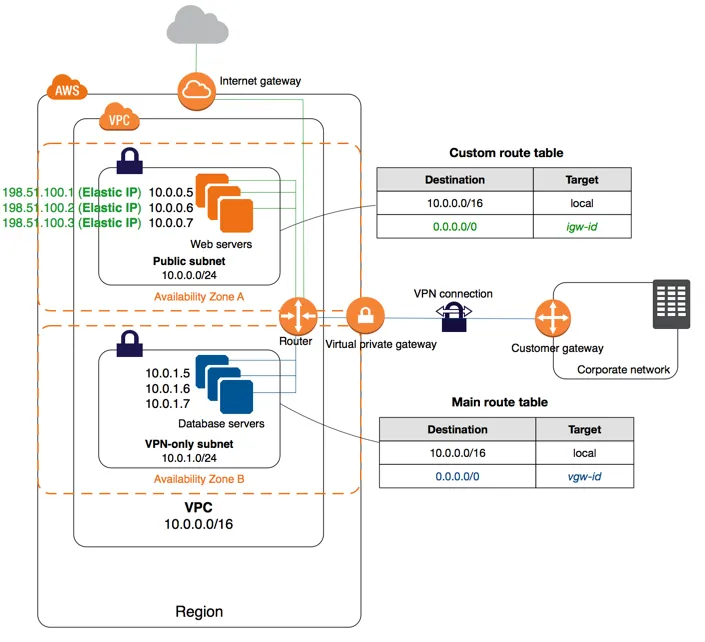
**Routing Tables**

A *route table* contains a set of rules, called *routes*, that determine where network traffic from your subnet or gateway is directed.

**Route table concepts**

The following are the key concepts for route tables.

* **Main route table**—The route table that automatically comes with your VPC. It controls the routing for all subnets that are not explicitly associated with any other route table.
* **Custom route table**—A route table that you create for your VPC.
* **Destination**—The range of IP addresses where you want traffic to go (destination CIDR). For example, an external corporate network with the CIDR 172.16.0.0/12.
* **Target**—The gateway, network interface, or connection through which to send the destination traffic; for example, an internet gateway.
* **Route table association**—The association between a route table and a subnet, internet gateway, or virtual private gateway.
* **Subnet route table**—A route table that's associated with a subnet.
* **Local route**—A default route for communication within the VPC.
* **Propagation**—If you've attached a virtual private gateway to your VPC and enable route propagation, we automatically add routes for your VPN connection to your subnet route tables. This means that you don't need to manually add or remove VPN routes. For more information, see [Site-to-Site VPN routing options](https://docs.aws.amazon.com/vpn/latest/s2svpn/VPNRoutingTypes.html) in the *Site-to-Site VPN User Guide*.
* **Gateway route table**—A route table that's associated with an internet gateway or virtual private gateway.
* **Edge association**—A route table that you use to route inbound VPC traffic to an appliance. You associate a route table with the internet gateway or virtual private gateway, and specify the network interface of your appliance as the target for VPC traffic.
* **Transit gateway route table**—A route table that's associated with a transit gateway. For more information, see [Transit gateway route tables](https://docs.aws.amazon.com/vpc/latest/tgw/tgw-route-tables.html) in *Amazon VPC Transit Gateways*.
* **Local gateway route table**—A route table that's associated with an Outposts local gateway. For more information, see [Local gateways](https://docs.aws.amazon.com/outposts/latest/userguide/outposts-local-gateways.html) in the *AWS Outposts User Guide*.



**VPC and VPN**

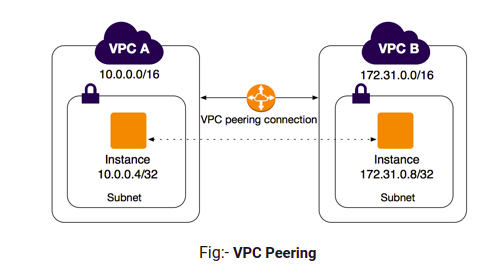
VPC and VPN are two essential components of cloud-based infrastructure that work together to provide secure and efficient access to resources.

**What Is a VPC?**

A virtual private cloud is a private cloud hosted in a public [cloud](https://controlplane.com/blog/post/what-is-cloud-deployment-complete-guide), where you can enjoy all the benefits and resources of the private network but with high scalability and isolation levels between the private and virtual environment of the cloud.

Thus, while the public cloud supports a series of clients accessing its resources, the VPC reserves part of these resources for the individual use of a client. With this, the customer can have more control over the environment without the need to be in the public cloud.

VPC provisions cloud servers according to current business demands, expanding the data centre without the need to invest in new equipment.



**What Is VPN?**

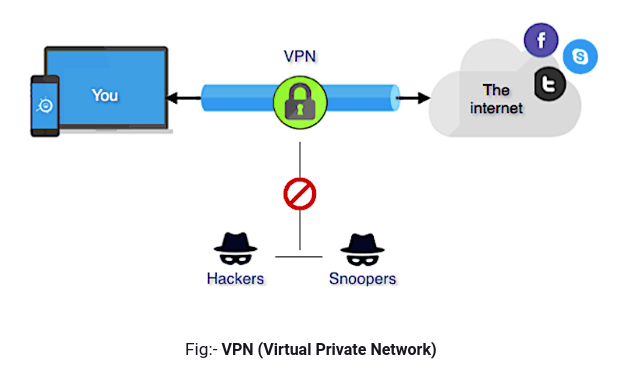
A virtual private network is a technology that allows users to establish a secure, encrypted connection to a network over the internet.

Companies commonly use VPNs to connect remote workers to their network, enabling access to resources that would otherwise be unavailable outside of the company’s physical location.

They’re also used to add an extra layer of security when accessing the internet from public WiFi networks, as VPNs encrypt all data transmitted between the user’s device and the network they’re connected to.

VPNs can be used to bypass geo-restrictions on content by allowing users to connect to servers in different locations around the world, making it appear as if they’re accessing the internet from a different country.

Overall, VPNs are an important tool for maintaining security and privacy when accessing the internet and connecting to networks remotely.



**VPC vs VPN**

VPN (Virtual Private Network) and VPC (Virtual Private Cloud) are related but distinct concepts used in networking and cloud computing.

A VPN is a technology that allows users to create a secure and private connection over a public network, such as the internet. It establishes an encrypted tunnel between the user’s device and a VPN server, ensuring that data transmitted between them remains confidential and protected from interception. VPNs are commonly used to enhance privacy, access restricted resources, bypass geographical restrictions, and provide secure remote access to corporate networks.

On the other hand, a VPC is a virtual network infrastructure provided by cloud computing platforms, such as Amazon Web Services (AWS) or Microsoft Azure. It enables users to create isolated and logically segmented networks within the cloud environment. A VPC allows you to define and control networking resources like subnets, IP addresses, routing tables, and security groups, much like you would do in a traditional on-premises network. VPCs provide the foundation for deploying and connecting cloud resources securely.

Although VPN and VPC are related in the sense that they both deal with private networks, they serve different purposes:

1. VPN operates at the network layer, providing secure communication between devices over public networks.
2. VPC operates at the infrastructure layer, allowing users to create and manage virtual network environments within a cloud computing platform.

In some cases, VPNs can be used to connect on-premises networks to a VPC, establishing a secure connection between the local network and the virtual network in the cloud. This enables secure and private communication between the two environments, extending the on-premises network to the cloud.