Sharing Resource & Internet connection

committed information rate (CIR)

- In frame relay networks, a committed information rate (CIR) is a bandwidth (expressed in bits per second) associated with a logical connection in a permanent virtual circuit (PVC).
- Frame relay networks are digital networks in which different logical connections share the same physical path and some logical connections are given higher bandwidths than others. For example, a connection conveying a high proportion of video signals (which require a high bandwidth) could be set up for certain workstations in a company (or on a larger network) and other connections requiring less bandwidth could be set up for all other workstations.

- Under a CIR, a customer is guaranteed a certain bandwidth under a service level agreement.
- Frame relay connections are also usually burstable with an excess information rate (EIR) or peak information rate (PIR).
- The bandwidth is guaranteed by the provider even if other customers are sharing the same physical connection over frame relay.
- The bandwidth is expressed in kilobits per second.

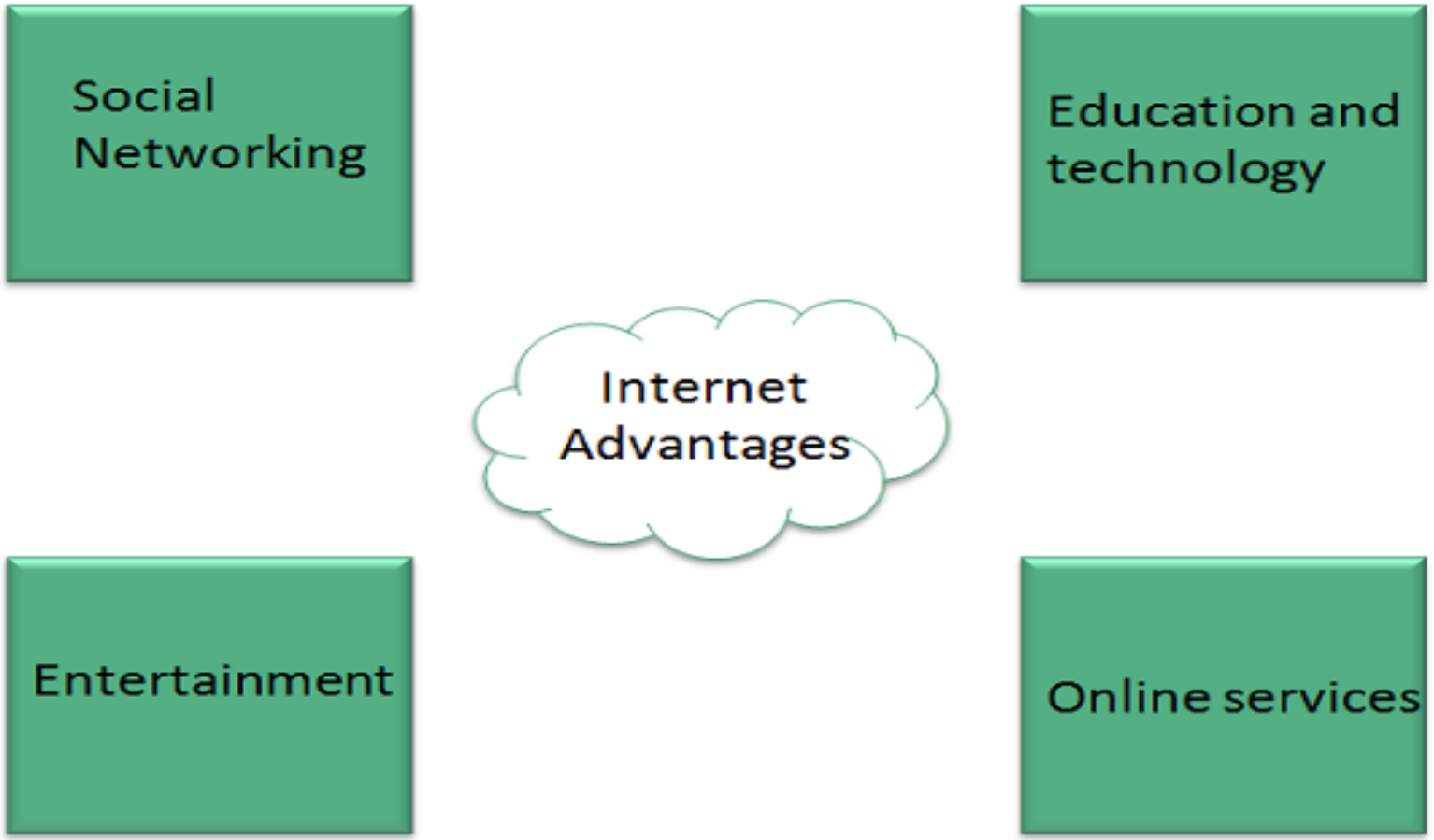
Concept of Internet

- Internet is defined as an Information super Highway, to access information over the web. However, It can be defined in many ways as follows:
- Internet is a world-wide global system of interconnected computer networks.
- Internet uses the standard Internet Protocol (TCP/IP).
- Every computer in internet is identified by a unique IP address.
- IP Address is a unique set of numbers (such as 110.22.33.114) which identifies a computer location.
- A special computer DNS (Domain Name Server) is used to give name to the IP Address so that user can locate a computer by a name.
- For example, a DNS server will resolve a name http://www.tutorialspoint.com to a particular IP address to uniquely identify the computer on which this website is hosted.
- Internet is accessible to every user all over the world.

Evolution

- The concept of Internet was originated in 1969 and has undergone several technological & Infrastructural changes as discussed below:
- The origin of Internet devised from the concept of Advanced Research Project Agency Network (ARPANET).
- ARPANET was developed by United States Department of Defence.
- Basic purpose of ARPANET was to provide communication among the various bodies of government.
- Initially, there were only four nodes, formally called Hosts.
- In 1972, the ARPANET spread over the globe with 23 nodes located at different countries and thus became known as Internet.
- By the time, with invention of new technologies such as TCP/IP protocols, DNS, WWW, browsers, scripting languages etc., Internet provided a medium to publish and access information over the web.

Advantages of Internet



Hypertext Documents

- The WWW makes extensive use of hypertext documents which contain
- Multimedia data such as text, images, sounds, video clips etc.
- Links to other documents (situated anywhere on the web).

HTTP

- The client/server protocol used to exchange hypertext documents is called HTTP (Hyper Text Transport Protocol). The main thing you need to know is that HTTP is a language spoken between your web browser (client software) and a web server (server software) so that they can communicate with each other and exchange files.
- HTTP is a "request-response" type protocol that specifies that a client will open a connection to a server then send a request using a very specific format. The server will then respond and close the connection.

HTML

- Hypertext documents are represented using a specialised markup language called HTML (Hyper Text Markup Language).

The Domain Name System (DNS)

- The Domain Name System (DNS) is a distributed directory that resolves human-readable hostnames, such as www.dyn.com, into machine-readable IP addresses like 50.16.85.103

Why is DNS important?

- DNS is like a phone book for the internet. If you know a person's name but don't know their telephone number, you can simply look it up in a phone book. DNS provides this same service to the internet.

What Is a DNS Server?

- A DNS server is a computer server that contains a database of public IP addresses and their associated hostnames, and in most cases serves to resolve, or translate, those names to IP addresses as requested.
- DNS servers run special software and communicate with each other using special protocols.

The Purpose of DNS Servers

- It's easier to remember a domain or hostname like lifewire.com than it is to remember the site's IP address numbers 151.101.2.114. So when you access a website, like Lifewire, all you have to type is the URL https://www.lifewire.com.

- However, computers and network devices don't work well with domain names when trying to locate each other on the internet. It's far more efficient and precise to use an IP address, which is the numerical representation of what server in the network (internet) the website resides on.

Computer Concepts - Internet Access Techniques

- Dial-up Connections
- In dial-up connection, computer uses its modem to dial a telephone number given to the user by an Internet Service Provider. This launches a connection between personal computer and ISP server. The process begins when the ISP server answers, and ceases when your computer or the server "hangs up". This is similar to a traditional telephone call. Most ISP servers disconnect automatically after a certain period of inactivity. Once a connection is configured on the user’s computer, he/she can use the connection. It is secure and de-allocates unused memory automatically.

Internet Access Techniques

- Dial-up Connections
- In dial-up connection, computer uses its modem to dial a telephone number given to the user by an Internet Service Provider. This launches a connection between personal computer and ISP server. The process begins when the ISP server answers, and ceases when your computer or the server "hangs up". This is similar to a traditional telephone call. Most ISP servers disconnect automatically after a certain period of inactivity. Once a connection is configured on the user’s computer, he/she can use the connection. It is secure and de-allocates unused memory automatically.

Broadband Connection

- Broadband connections are considered as high speed connections, as they use modes that can handle several signals at once, such as fiber optics, twisted pair cables, coaxial cable and other technologies. Even with hundreds of users on the network, these connections allow large files and complex web pages to download quickly.
- To be considered as a broadband, the connection must be able to transmit data at a rate faster than is possible with the fastest dial-up connection. Downloading and uploading content will be fast.

Digital Subscriber Line (DSL)

- Digital Subscriber Line is similar to that of ISDN in using telephone network, but it uses more advanced digital signal processing and algorithms to squeeze maximum number of signals through telephone lines. DSL also requires changes in components of telephone network before it can be offered in any area. Like, DSL provides simultaneous data, voice and fax transmission on the same line. Several versions of DSL services are available for home and business use; each version provides 24/7 full-time connection at different levels of service, speed, bandwidth and distance.

Wireless LAN (WLAN) Connections

- Wireless LAN connections are very common these days, which are based on the technology that is often cited as Wi-Fi (Wireless Fidelity).
- The distance covered by WLAN is usually measured in meters rather than miles. Therefore, this is not a technology that connects directly to an ISP but can be used to connect to another LAN or device through which internet access is achieved.

Process

- To connect to internet, the wireless access point is connected to a wired LAN like any other devices, and then computers with wireless NICs can access the wired LAN. "Wireless access point" is a device that acts as a hub or switch.

- "NIC" refers to a Network Interface Card which helps to identify a computer on a network.

Satellite Services

- Satellite services provide a mutual (two-way) communication between user and the internet.
- This provides a full-time connection which is used in armed forces, business, etc. It includes two parts −
- Transceiver − A satellite dish that is placed outdoors in direct line of sight to one of the several satellites in geostationary orbit.
- Modem-like device − It is connected to a dish, placed indoors and connected to a LAN or computer.

What Is Social Networking?

- Social networking is the use of Internet-based social media sites to stay connected with friends, family, colleagues, customers, or clients. Social networking can have a social purpose, a business purpose, or both, through sites such as Facebook, Twitter, LinkedIn, and Instagram, among others. Social networking has become a significant base for marketers seeking to engage customers.

KEY TAKEAWAYS

- Social networking is the use of Internet-based social media platforms to stay connected with friends, family, or peers.
- While always changing, the most popular social networking sites are include Facebook, Instagram, and Twitter.
- Marketers use social networking for increasing brand recognition and encouraging brand loyalty.

Internet Service Provider (ISP)

- An Internet Service Provider (ISP) is the industry term for the company that is able to provide you with access to the Internet, typically from a computer. If you hear someone talking about the Internet and they mention their "provider," they're usually talking about their ISP.
- Your ISP makes the Internet a possibility. In other words, you can have shiny computer with a built-in modem and could have a router for networking, but without a subscription with an ISP, you won't have a connection to the Internet.

Indian ISPs are Jio, BSNL, Vodafone etc.

Virus and virus protection

- Virus protection software is designed to prevent viruses, worms and Trojan horses from getting onto a computer as well as remove any malicious software code that has already infected a computer.
- Most virus protection utilities now bundle anti-spyware and anti-malware capabilities to go along with anti-virus protection. Internet security suites go a step further by including additional capabilities like anti-spam, anti-phishing, firewall, file protection and PC optimization.
- A computer virus is a malicious program that self-replicates by copying itself to another program.
- In other words, the computer virus spreads by itself into other executable code or documents. The purpose of creating a computer virus is to infect vulnerable systems, gain admin control and steal user sensitive data. Hackers design computer viruses with malicious intent and prey on online users by tricking them.

What is Unified Threat Management (UTM)?

- Unified threat management (UTM) is an approach to information security where a single hardware or software installation provides multiple security functions.
- This contrasts with the traditional method of having point solutions for each security function.
- UTM simplifies information-security management by providing a single management and reporting point for the security administrator rather than managing multiple products from different vendors.

- UTM appliances have been gaining popularity since 2009, partly because the all-in-one approach simplifies installation, configuration and maintenance.
- Such a setup saves time, money and people when compared to the management of multiple security systems. Instead of having several single-function appliances, all needing individual familiarity, attention and support, network administrators can centrally administer their security defenses from one computer.
- Some of the prominent UTM brands are Fortinet, Sophos, WiJungle, SonicWall and Check Point

Service set identifier (SSID)

- A service set identifier (SSID) is a sequence of characters that uniquely names a wireless local area network (WLAN).
- An SSID is sometimes referred to as a "network name." This name allows stations to connect to the desired network when multiple independent networks operate in the same physical area.
- Each set of wireless devices communicating directly with each other is called a basic service set (BSS). Several BSSs can be joined together to form one logical WLAN segment, referred to as an extended service set (ESS).

- For example, a departmental WLAN (ESS) may consist of several access points (APs) and dozens of stations, all using the same SSID.
- Another organization in the same building may operate its own departmental WLAN, composed of APs and stations using a different SSID.
- The purpose of SSID is to help stations in department A find and connect to APs in department A, ignoring APs belonging to department B.

SD-WAN (Software-Defined Wide-Area Network)

- SD-WAN stands for software-defined wide area network (or networking). A WAN is a connection between local area networks (LANs) separated by a substantial distance—anything from a few miles to thousands of miles.
- The term software-defined implies the WAN is programmatically configured and managed.
- So, it can be easily adapted quickly to meet changing needs.

How Does SD-WAN Work?

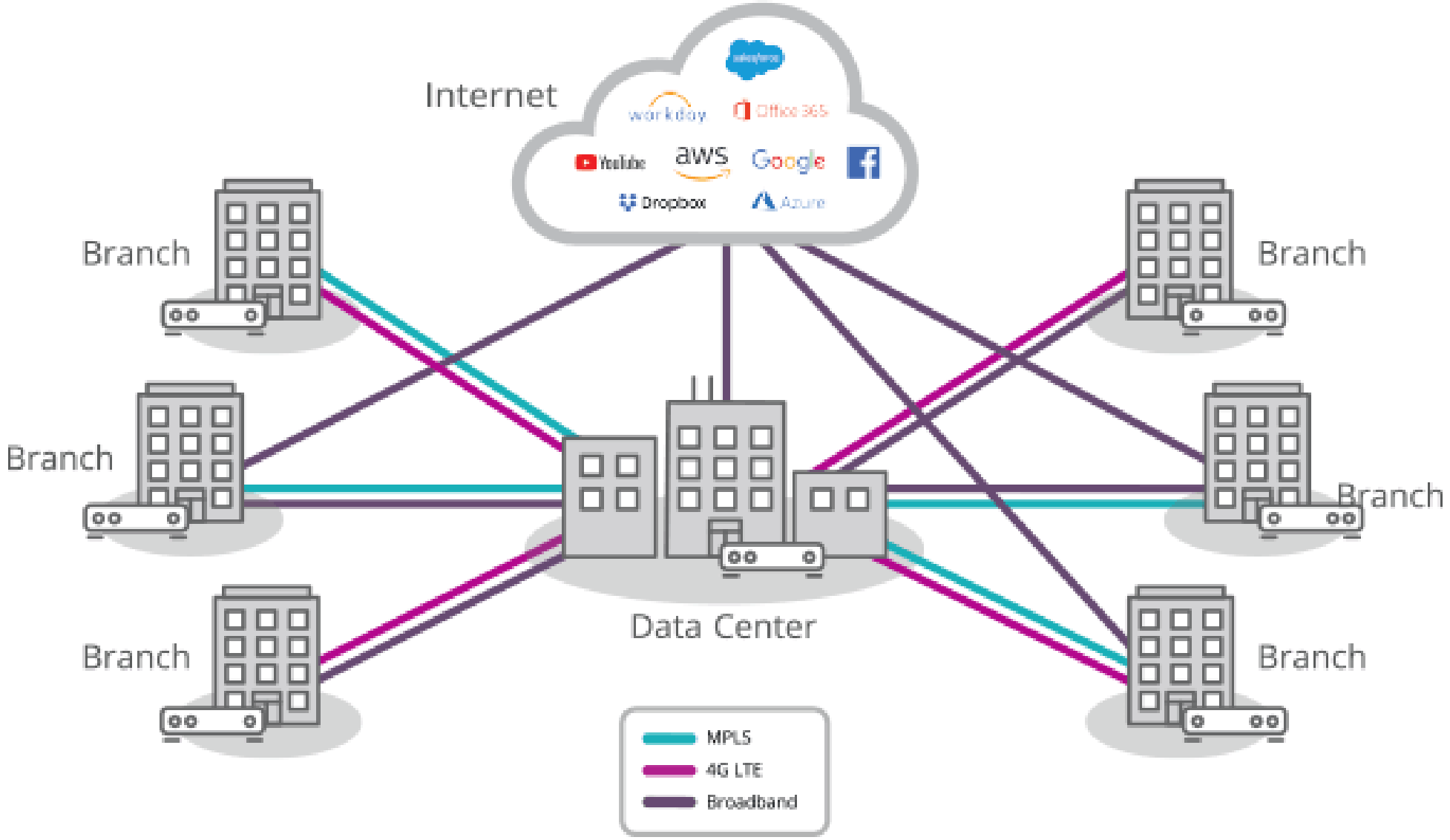
Centralized control

- The primary means of control in an SD-WAN is centralized. It often resides in a SaaS application(**Software** as a service) running on a public cloud. Control is decoupled from the hardware to simplify network management and improve the delivery of services. SD-WAN appliances (and virtual appliances) follow operational rules passed down from the central SD-WAN controller. This greatly reduces or eliminates the need to manage gateways and routers on an individual basis.

Multi-connection, multi-transport

- SD-WAN gateways support hybrid WAN, which implies that each gateway can have multiple connections using different transport, broadband, Multiprotocol Label Switching (**MPLS**) , Internet, LTE, etc. A virtual private network (VPN) is typically set up across each WAN connection for security. Consequently, the SD-WAN can be an overlay spanning a diverse communications infrastructure.

SD-WAN Architecture

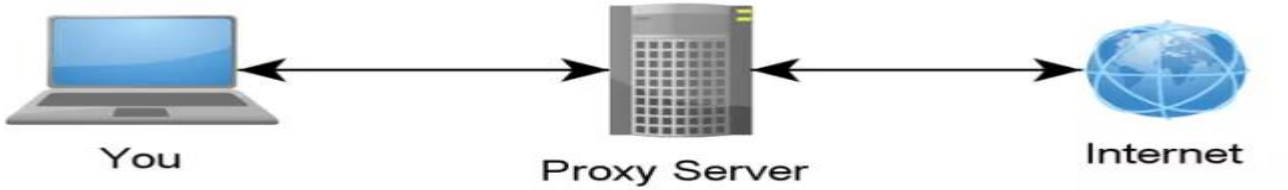


Shared resource

- In computing, a shared resource, or network share, is a computer resource made available from one host to other hosts on a computer network. It is a device or piece of information on a computer that can be remotely accessed from another computer, typically via a local area network or an enterprise intranet, transparently as if it were a resource in the local machine. Network sharing is made possible by inter-process communication over the network
- Some examples of shareable resources are computer programs, data, storage devices, and printers. E.g. shared file access (also known as disk sharing and folder sharing), shared printer access, shared scanner access, etc. The shared resource is called a shared disk, shared folder or shared document

Working principle of Proxy Server.

- A proxy server acts as a gateway between you and the internet. It’s an intermediary server separating end users from the websites they browse.



- Proxy servers provide varying levels of functionality, security, and privacy depending on your use case, needs, or company policy.

- Modern proxy servers do much more than forwarding web requests, all in the name of data security and network performance.
- Proxy servers act as a firewall and web filter, provide shared network connections, and cache data to speed up common requests.
- A good proxy server keeps users and the internal network protected from the bad stuff that lives out in the wild internet.
- Lastly, proxy servers can provide a high level of privacy.
- A proxy server is basically a computer on the internet with its own IP address that your computer knows. When you send a web request, your request goes to the proxy server first. The proxy server then makes your web request on your behalf, collects the response from the web server, and forwards you the web page data so you can see the page in your browser.

Why Should You Use a Proxy Server?

- **To control internet usage of employees and children:**

Organizations and parents set up proxy servers to control and monitor how their employees or kids use the internet.

Most organizations don’t want you looking at specific websites on company time, and they can configure the proxy server to deny access to specific sites, instead redirecting you with a nice note asking you to refrain from looking at said sites on the company network.

- **Bandwidth savings and improved speeds:**

Organizations can also get better overall network performance with a good proxy server.

Proxy servers can cache (save a copy of the website locally) popular websites – so when you ask for www.varonis.com, the proxy server will check to see if it has the most recent copy of the site, and then send you the saved copy.

What this means is that when hundreds of people hit www.varonis.com at the same time from the same proxy server, the proxy server only sends one request to varonis.com.

This saves bandwidth for the company and improves the network performance.

- **Privacy benefits:**

Individuals and organizations alike use proxy servers to browse the internet more privately. Some proxy servers will change the IP address and other identifying information the web request contains.

- **Improved security:**

Proxy servers provide security benefits on top of the privacy benefits.

You can configure your proxy server to encrypt your web requests to keep prying eyes from reading your transactions.

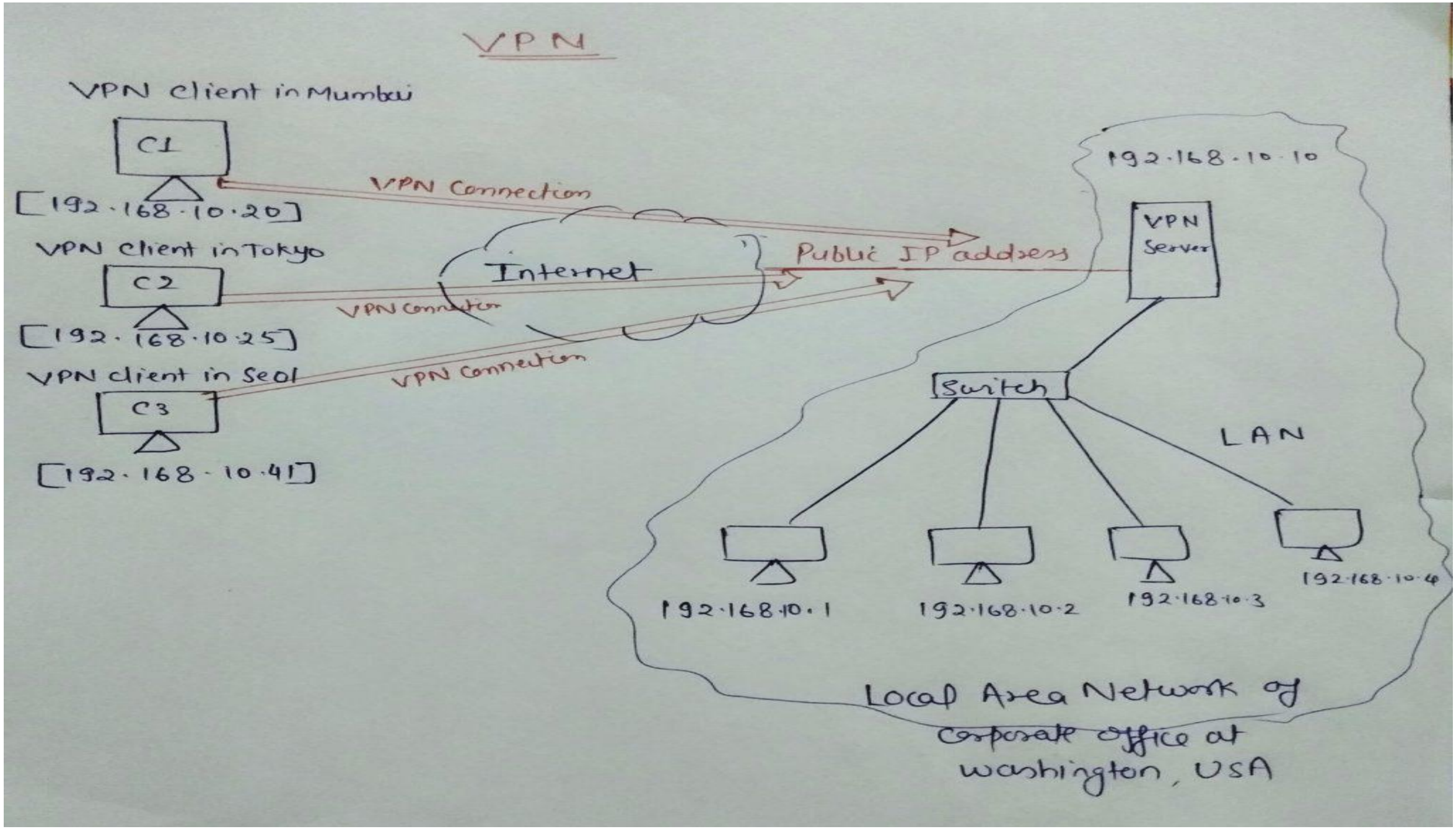
You can also prevent known malware sites from any access through the proxy server. Additionally, organizations can couple their proxy server with a Virtual Private Network (VPN), so remote users always access the internet through the company proxy.,

VPN – virtual private network

- VPN stands for virtual private network. A virtual private network (VPN) is a technology that creates a safe and encrypted connection over a less secure network, such as the internet. Virtual Private network is a way to extend a private network using a public network such as internet. The name only suggests that it is Virtual “private network” i.e. user can be the part of local network sitting at a remote location. It makes use of tunneling protocols to establish a secure connection.
- ***Tunnelling Protocol***
- *In computer networks, a tunneling protocol is a communications protocol that allows for the movement of data from one network to another. It involves allowing private network communications to be sent across a public network through a process called encapsulation.*

Lets understand VPN by an example:

- Think of a situation where corporate office of a bank is situated in Washington, USA.
- This office has a local network consisting of say 100 computers. Suppose another branches of bank are in Mumbai, India and Tokyo, Japan.
- The traditional method of establishing a secure connection between head office and branch was to have a leased line between the branches and head office which was very costly as well as troublesome job.
- VPN let us overcome this issue in an effective manner.


VPN
VPN client in Mumbai
C1
[192.168.10.20]
VPN Connection
VPN client in Tokyo
C2
[192.168.10.25]
VPN client in Seol
C3
[192.168.10.41]
Internet
Public IP address
192.168.10.10
VPN Server
Switch
LAN
192.168.10.1
192.168.10.2
192.168.10.3
192.168.10.4
Local Area Network of
Corporate office at
washington, USA