

Parvatibai Genba Moze College of Engineering, Wagholi,Pune.

**Department of Computer Engineering**

**Seminar Synopsis On topic**

**VPN(Virtual Private Network)**

Presented By

Amundkar Prathamesh Jitendra

**Roll no - 03**

**Class :** TE(Comp)

**Guide:** Prof. Shrikant Dhamdhere. **Sign:**

# Seminar Title:

“VPN(Virtual Private Network)”

# Seminar Area:

VPN(virtual Private Network)

# Seminar Guide:

Prof. Shrikant Dhamdhere.

# Technical Keywords:

Virtual private network(VPN),tunnel,Internet,public medium ,Encreption,decryption

# Problem Statement

One popular technology to accomplish these goals is a VPN (virtual private network). A VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together. The VPN uses "virtual" connections routed through the Internet from the business's private network to the remote site or employee. By using a VPN, businesses ensure security -- anyone intercepting the encrypted data can't readit.

# Abstract:

A Virtual Private Network (VPN) can be defined as a way to provide secure communication between members of a group through use of public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. There are many different VPN solutions out there, and just deciding which one to choose can be difficult since they all have advantages and disadvantages. VPNs can be categorized as Secure or Trusted VPNs, Client-based or Web-based VPNs, Customer Edge-based or Provider Edge-based VPNs, or Outsourced or In-house VPNs. These categories often overlap each other. In order to decide what VPN solutions to choose for different parts of the enterprise infrastructure, the chosen solution should be the one that best meets the requirements of the enterprise. The purpose of this paper is to serve as a basis when creating an enterprise WAN which connects sites and users together using VPN technology. The purpose of creating such a WAN is to allow the resources of a company to be remotely accessed.

# Goals and Objectives:

Secure [remote access](https://www.techtarget.com/searchsecurity/definition/remote-access) for users anywhere, anytime.

Easy setup, configuration, use and maintenance.

Affordability for widespread corporate use.

Ease of use: There should be no obvious [performance](https://www.newshosting.com/blog/vpn-speed-test/) problems, no major usage hoops to jump through, no "gotchas" or other downsides to regular frequent use.

# Scope

“Speaking about the future of [VPN](https://www.techradar.com/vpn/best-vpn)(opens in new tab), we should first think about the future of privacy. It is obvious that not much privacy left in today's world. We see many examples of Geo restricted countries.

The best example, is of course, The Great [China](https://www.techradar.com/news/best-vpn-for-china-our-5-top-choices)(opens in new tab) Firewall and Trump’s resolution to let ISPs share private data. Such innovations call other countries to go the same way. In the next 10 - 15 years VPN will become more of a platitude than today.

VPN will continue to advocate the right of privacy and people will use VPN hoping for salvation.

It will increase the number of VPN providers and competition on VPN market will continue to grow. In today's world, one of the main problems is that each device in one way or another collect data for different purposes.

Services for communication such as Skype, WhatsApp, Gmail, Facebook, also mean the transfer of data to a third party and of course people are not comfortable with that.

Our personal data is our intellectual property and we are interested in reducing all possible risks of leakage.

At the moment the truth is that most internet users are technically unsafe. VPN industry is trying to change it making use of VPN affordable and easy for everyone. In the future, there will be no need for users to setup VPN on their devices as it will be built in OS and automatized.

No doubts that the future of VPN looks promising and It will keep fighting for the internet with no restrictions and right for privacy.

There are actually two possible scenarios in the nearest future. The first one is the world where we completely forget about the word privacy. And the second one is continue standing up for our right of privacy and net neutrality. “

# Introduction:

# VPN stands for "Virtual Private Network" or "Virtual Private Networking." A VPN is a private network in the sense that it carries controlled information, protected by various security mechanisms, between known parties. VPNs are only "virtually" private, however, because this data actually travels over shared public networks instead of fully dedicated private connections. The main benefit of a VPN is the potential for significant cost savings compared to traditional leased lines or dial up networking. These savings come with a certain amount of risk, however, particularly when using the public Internet as the delivery mechanism for VPN data. The performance of a VPN will be more unpredictable and generally slower than dedicated lines due to public Net traffic. Likewise, many more points of failure can affect a Net-based VPN than in a closed private system. Utilizing any public network for communications naturally raises new security concerns not present when using more controlled environments like pointto-point leased lines. VPNs may save money in several different ways. Companies that lease private lines typically pay a very high monthly fee, and a VPN can replace these lines with much less expensive, shorter connections to a local ISP. VPNs can also support remote access connectivity for travelers. Instead of configuring remote access servers and paying for the long-distance charges to reach them, an organization can rely on an ISP to support local access on both ends of the vpn connection.

EVM is “networked” is the most important thing .EVM machines are extremely simple machines, like pocket calculators, with no connection to the internet, no operating system and no way of being altered without physical access to the machines.There were earlier claims regarding EVMs&#39; temper ability and security which have not been proved.

# Disadvantages of Current Voting system:

### **Slightly slower internet**

A VPN reroutes and encrypts your internet connection, which may slightly lessen your internet speed.

### **Illegal in some countries\***

Although the use of VPN is legal in India, in some countries, use of a VPN is banned or heavily regulated, so always check the legislation if you’re travelling to a different country.

### **Potentially difficult to set up**

Depending on the VPN you use, you may have some trouble setting it up. Be sure to choose a beginner-friendly VPN service to avoid this.

### **Lack of encryption knowledge**

Unless you’re an encryption expert, it’s hard to know the encryption quality of your VPN. However, selecting a reliable VPN service with positive reviews will more likely ensure a high quality encryption of your data.

# Advantages of Proposed system:

## **1. Hides your private information**

Websites and apps can continuously track your online activity, analyzing the data they collect. A VPN can prevent web browsers and others from accessing your connection, helping to keep the information you send and receive anonymous and secure. Some VPNs also offer military-grade 256-bit encryption of your data.

## **2. Escape data-throttling**

Data throttling occurs when you’ve used a certain amount of your data and, as a result, your internet service provider slows down your service. With a VPN, not only will your data be free from the prying eyes of ISPs and others, but you also won’t be subject to a data cap. ISPs can place caps on data to maximize internet speed for some of their customers.

## **3. Avoid bandwidth-throttling**

If you’ve suffered from slower internet speed on certain websites at times, you may have experienced bandwidth throttling. ISPs — or anyone with administrative controls over your network — might be responsible for the slowdown. A VPN can help. It can thwart the sluggishness by encrypting your device’s internet traffic. This prevents anyone on the same network from seeing your web traffic content and disguises its destination.

## **4. Access region-blocked services like PUBG Mobile\***

Some VPNs may be able to access geo-blocked apps and content such as PUBG Mobile (Banned in India in September 2020), Netflix, and other providers\*. How? A VPN can change your IP address to make a content provider think you’re browsing in another location or region that allows access. Note: Always check the Terms of Service agreements to determine what’s permitted by your local streaming service and follow those guidelines. Even though using VPN is perfectly legal in India, there are few cases where the government (police) has punished locals for using the service.2

## **5. Avoid censorship when travelling abroad\***

VPNs can help you bypass geographical restrictions. For instance, some countries restrict or forbid access to certain websites such as social media platforms or censor certain content. A VPN, however, may help grant you access by making your traffic look like it’s coming from a different location. Keep in mind that it is the user’s responsibility to identify whether their use of a VPN is legal or not and to check the country’s laws (where you’re travelling to)  before using a VPN.

## **6. Access regional sports coverage unavailable in your location\***

Some VPNs can help give you access to sports coverage that’s geographically restricted. For instance, a television network such as Sky Sports (available in the [**U.K and Ireland only**](https://en.wikipedia.org/wiki/Sky_Sports)) doesn’t have broadcast rights in India.3Nevertheless, a VPN will be capable of making viewing such a channel possible.

## **7. Offer cheaper leased-line alternatives**

A VPN can offer specific savings for businesses, in particular. For example, companies may bypass renting expensive network capacity lines that achieve connectivity between office locations through VPNs. Instead, they could connect via public infrastructure through cheaper local leased lines or broadband connections through a local ISP.

## **8. Offer cheaper long-distance telephone charges**

A VPN will be able to reduce long-distance phone charges. For example, instead of connecting via remote access servers and dial-up networks to access a company's intranet, you could connect to your local ISP access point by activating a VPN.

## **9. Provide network scalability**

As organizations grow, so do the costs of building a dedicated private network. Internet-based VPNs can allow businesses to tap into network lines and network capability already available, potentially giving remote and international locations, particularly, better reach and service quality.

## **10. Reduce support costs**

Using a VPN may help a business reduce the cost of maintaining servers because support can be outsourced to third-party service providers who can support a lower cost structure due to their many clients.

# Conclusion:

Network security is one of the trending topics in modern days. As world is more vulnerable, VPN importance has increased. Business organization nowadays is not limited to one place. So, they are in need of security in cheap price which can fulfill by using VPN and its modern tunneling protocol which has been impossible for anyone the go through it. It has been golden cake for those who work more in public cafe network than sitting in same place throughout the year. It is giving new name to the security and data transfer through the internet