



# VPN

## Virtual Private Network

Best E-Book Free 100%

www.learntechanywhere.com



### Specific:-

- What is VPN?
- How VPN Works?
- Types of VPN?
- Types of VPN Protocols?
- Advantages of VPN?
- Disadvantages of VPN?



**Abstract** - Virtual Private Network (VPN) is rapidly growing technology which plays a great role in Wireless LAN (WLAN) by providing secure data transmission. The purpose of VPN is to provide safe and secure communication by creating virtual tunnels between pair of hosts, once tunnel is created data transfer can take place. This paper presents a comprehensive study of VPN- IPsec and SSL VPN, architecture and protocols used. The salient of this paper to present comparison analysis of both technologies IPsec and SSL VPN together with their advantages and disadvantages.

Keywords – Virtual Private Network, Authentication Header, Encapsulating Payload, Secure Socket Layer.

## 1. 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.

Two VPN technologies that are being used are:

**Site-to-site VPN** - A site-to-site VPN allows multiple offices in fixed locations to establish secure connections with each other over a public network such as the Internet. It also provides extensibility to resources by making them available to employees at other locations.

**Remote Access VPN** - A remote-access VPN allows individual users to establish secure connections with a remote computer network. These users can access the secure resources on that network as if they were directly plugged in to the network's servers.

### Features in VPN

- Provide extended connections across multiple geographic locations without using a leased line.
- Improved security mechanism for data by using encryption techniques.
- Provides flexibility for remote offices and employees to use the business intranet over an existing Internet connection as if they're directly connected to the network
- Saves time and expense for employees who commute from virtual workplaces
- VPN is preferred over leased line since leases are expensive, and as the distance between offices increases, the cost of leased line increase.
- IPsec VPN and SSL VPN are two solutions of VPN which are widely used in WLAN. We will discuss both of them together with their advantages and disadvantages.

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 travellers. 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.

## 2. METHODOLOGY:

This topic is chosen in order to become more familiar theoretically in the field of secure network connection using tunnel. To complete this research I have done the following things:

1. Various articles in the Internet were thoroughly examined and information was collected.
2. Several e-books and books from the library were used to find the content about the topics.
3. Consultation with friends was also done which helped in conduction the research in more depth.

4. For practical test, I have been through [www.vpnforuk.com](http://www.vpnforuk.com) for testing free VPN service.

### **3. ANALYSIS:**

VPN is growing very fast as the security is the major concern in the world. Modern technology has shown great changes the way we work few years ago. People started to work remotely and are seeking more security for their work. So, in upcoming days VPN would be the prime requirement for every organization and business people. Moreover, those who are sensitive towards their personal information VPN technology would be their first choice.

### **4. DISCUSSION:**

A virtual private network (VPN) is a network that uses a public telecommunication infrastructure, such as the Internet, to provide remote offices or individual users with secure access to their organization's network. A virtual private network can be contrasted with an expensive system of owned or leased lines that can only be used by one organization. The goal of a VPN is to provide the organization with the same capabilities, but at a much lower cost securely through public network.

A VPN works by using the shared public infrastructure while maintaining privacy through security procedures and tunneling protocols such as the Layer Two Tunneling Protocol (L2TP) along with IPSec (IPSec/L2TP). In effect, the protocols, by encrypting data at the sending end and decrypting it at the receiving end, send the data through a "tunnel" that cannot be "entered" by data that is not properly encrypted. An additional level of security involves encrypting not only the data, but also the originating and receiving network addresses.

## Why VPN?

As a business grows, it might expand to multiple shops or offices across the country and around the world. To keep things running efficiently, the people working in those locations need a fast, secure and reliable way to share information across computer networks. In addition, traveling employees like salespeople need an equally secure and reliable way to connect to their business's computer network from remote locations.

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 read it.

### 4.1 Types of VPN:

There are two types of VPN on the basis of deployment:

#### 4.1.1 Remote Access VPNs:

Remote Access VPN is also called virtual private dial-up networks (VPDNs). These are user-to-LAN connections used when employees of a company who are in remote locations need to connect to the company's private network. A company that wants to set up a remote-access VPN usually outsources to an ESP or enterprise service provider. The ESP sets up a NAS (network access server) and also provides remote users with the software they need for their computers. Then users simply dial the NAS using a toll-free number and access the network via their VPN client software. VPNs offer a good third-party service for encrypted, secure connections between remote users within a private network.

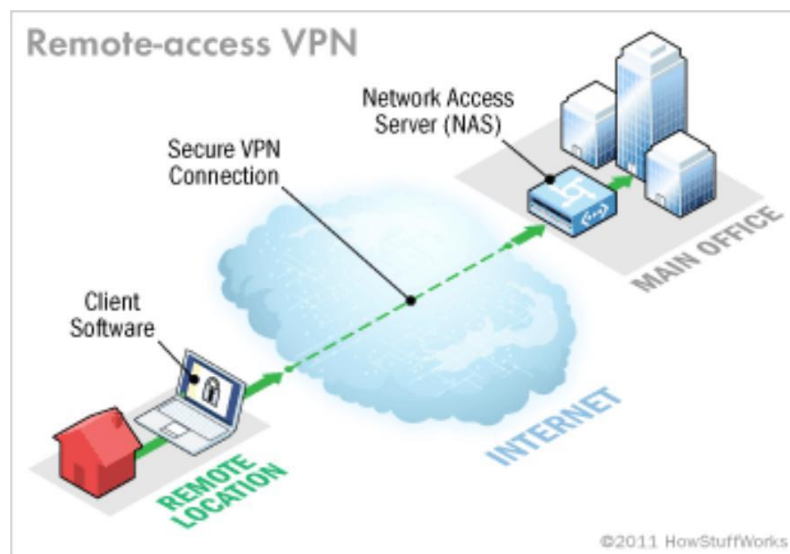


Fig 1. Remote Access VPNs

#### 4.1.2 Site to Site VPNs:

A site-to-site VPN allows offices in multiple fixed locations to establish secure connections with each other over a public network such as the Internet. Site-to-site VPN extends the company's network, making computer resources from one location available to employees at other locations. An example of a company that needs a site-to-site VPN is a growing corporation with dozens of branch offices around the world. There are two types of site-to-site VPNs:

**Intranet-based** -- If a company has one or more remote locations that they wish to join in a 2

single private network, they can create an intranet VPN to connect each separate LAN to a single WAN.

**Extranet-based** -- When a company has a close relationship with another company (such as a partner, supplier or customer), it can build an extranet VPN that connects those companies' LANs. This extranet VPN allows the companies to work together in a secure, shared network environment while preventing access to their separate intranets.

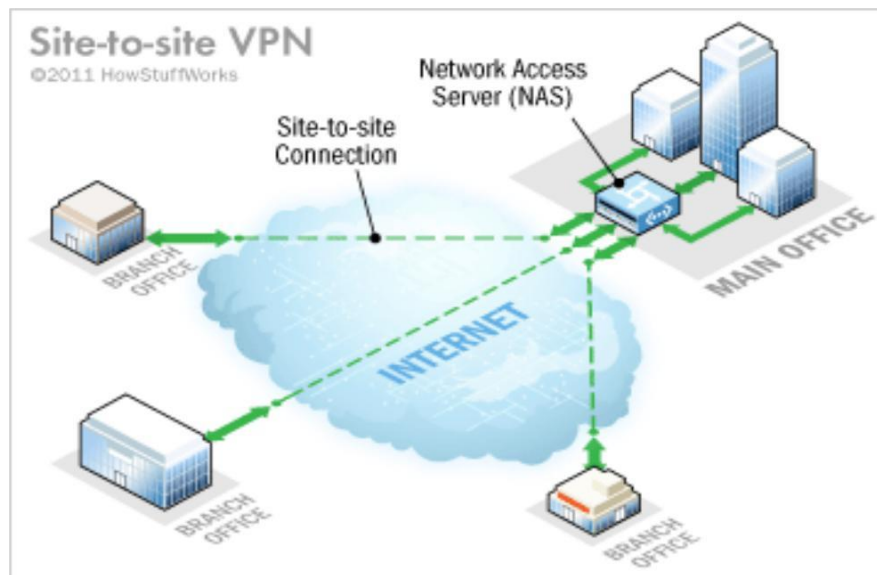


Fig 2. Site-to-Site VPN

#### 4.2 Components to Establish/Setup VPN:

1. Authentication
2. Tunneling
3. Encryption

##### 4.2.1 Authentication:

Tunnel endpoints must be authenticated before secure VPN tunnels can be established. User-created remote-access VPNs may use passwords, biometrics, two-factor authentication or other cryptographic methods. Network-to-network tunnels often use passwords or digital certificates. They permanently store the key to allow the tunnel to establish automatically, without intervention from the user.

##### 4.2.2 Tunneling:

Virtual private network technology is based on the idea of tunneling. VPN tunneling involves establishing and maintaining a logical network connection (that may contain intermediate hops). On this connection, packets constructed in a specific VPN protocol format are encapsulated within some other base or carrier protocol, then transmitted between VPN client and server, and finally de-encapsulated on the receiving side. VPN supports two types of tunneling - voluntary and compulsory. Both types of tunneling are commonly used.

#### VPN Tunneling Protocols

Several computer network protocols have been implemented specifically for use with VPN tunnels.

The three most popular VPN tunneling protocols listed below continue to compete with each other for acceptance in the industry. These protocols are generally incompatible with each other.

### **I. Point-to-Point Tunneling Protocol (PPTP)**

Several corporations worked together to create the PPTP specification. People generally associate PPTP with Microsoft because nearly all flavors of Windows include built-in client support for this protocol. The initial releases of PPTP for Windows by Microsoft contained security features that some experts claimed were too weak for serious use. Microsoft continues to improve its PPTP support, though. It uses TCP port 1723 to establish a connection.

### **II. Layer Two Tunneling Protocol (L2TP)**

The original competitor to PPTP for VPN tunneling was L2F, a protocol implemented primarily in Cisco products. In an attempt to improve on L2F, the best features of it and PPTP were combined to create a new standard called L2TP. Like PPTP, L2TP exists at the data link layer (Layer Two) in the OSI model -- thus the origin of its name.

### **III. Internet Protocol Security (IPsec)**

IPsec is actually a collection of multiple related protocols. It can be used as a complete VPN protocol solution or simply as the encryption scheme within L2TP or PPTP. IPsec exists at the network layer (Layer Three) of the OSI model.

#### **4.2.3 Encryption:**

You must use data encryption to provide data confidentiality for the data that is sent between the VPN client and the VPN server across a shared or public network, where there is always a risk of unauthorized interception. You can configure the VPN server to force encrypted communications. Users who connect to that server must encrypt their data or a connection is not allowed. For VPN connections, the Windows Server 2003 family uses Microsoft Point-to-Point Encryption (MPPE) with the Point-to-Point Tunneling Protocol (PPTP) and Internet Protocol security (IPSec) encryption with the Layer Two Tunneling Protocol (L2TP).

Because data encryption is performed between the VPN client and VPN server, data encryption is not necessary on the communication link between a dial-up client and its Internet service provider (ISP). For example, a mobile user uses a dial-up connection to dial in to a local ISP. Once the Internet connection is made, the user creates a VPN connection with the corporate VPN server. If the VPN connection is encrypted, encryption is not needed on the dial-up connection between the user and the ISP.

Note: VPN data encryption does not provide end-to-end data encryption. End-to-end encryption is data encryption between the client application and the server hosting the resource or service that is accessed by the client application. To get end-to-end data encryption, you can use IPSec to create a secure connection after the VPN connection is made.

## **4.3 Limitations of a VPN**

Despite their popularity, VPNs are not perfect and limitations exist as is true for any technology. Organizations should consider issues like the below when deploying and using virtual private networks in their operations:

















1. VPNs require detailed understanding of network security issues and careful installation / configuration to ensure sufficient protection on a public network like the Internet.
2. The reliability and performance of an Internet-based VPN is not under an organization's direct control. Instead, the solution relies on an ISP and their quality of service.



3. Historically, VPN products and solutions from different vendors have not always been compatible due to issues with VPN technology standards. Attempting to mix and match equipment may cause technical problems, and using equipment from one provider may not give as great a cost savings.

#### 4.4 Popular VPN service provider in 2014:

According to [whatismyipaddress.com](http://whatismyipaddress.com) specification of VPN providers are as follows:

Providers	Servers	Countries	Locations	Platforms	Monthly
 Hide my Ass	587	38	143		\$11.52
 vyprVPN	700	40	43		\$5.00
 pureVPN	300	47			\$6.95
 IPVANISH	113	74			\$10.00
 PROXIFY		19	1138		\$10.00
 STRONGVPN	446	7	44		\$15.00
 SUNVPN	9	18	9		\$9.99
 PROVPN	36	7	32		\$13.58
 VPN in Touch		32	9		\$4.99
 EarthVPN	204	12	114		\$3.99
 VPN.SH	21	5	21		\$3.31

#### 4.5 Connecting VPN

During research process, I have been through [vpnforuk.com](http://vpnforuk.com) which provides free VPN services. Here is sample for connection VPN in windows using PPTP protocol:

**Step 1:**  
Connect to a workspace

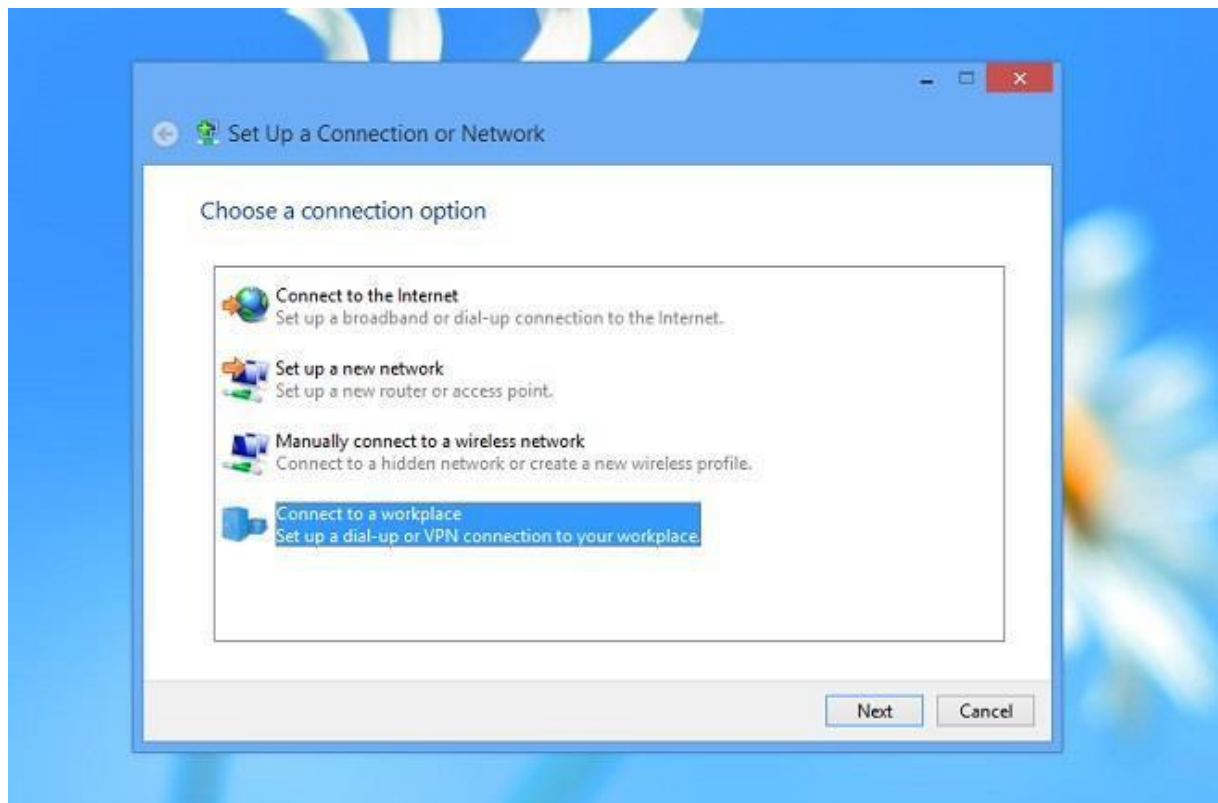


Fig 3: Connect to a workspace

**Step 2:**  
Use my internet connection (VPN)

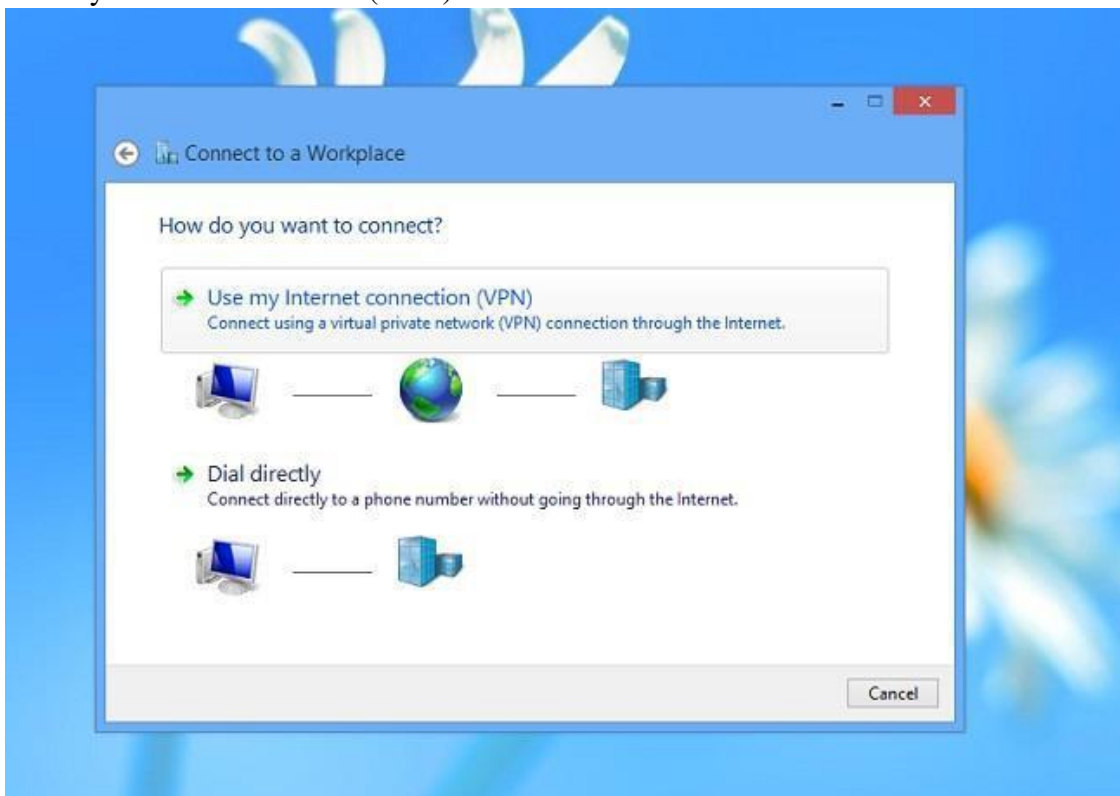


Fig 4: Use my internet connection(VPN)



**Step 3:**

Now Saugat\_VPN is ready to connect to the VPN.

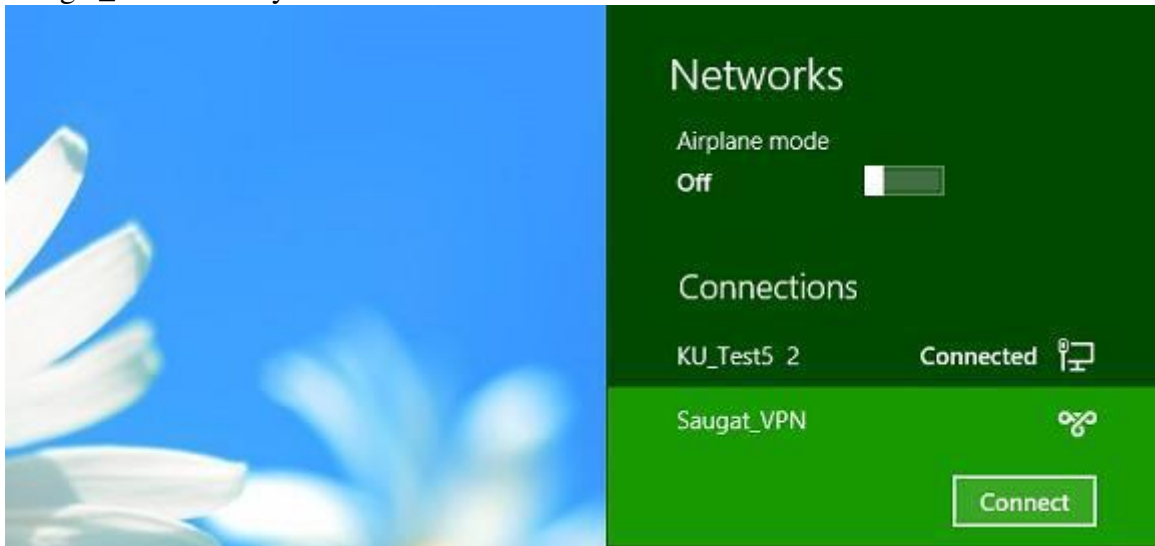


Fig 5: connect to Saugat\_VPN

**Step 4:**

Connecting to vpnforuk.com

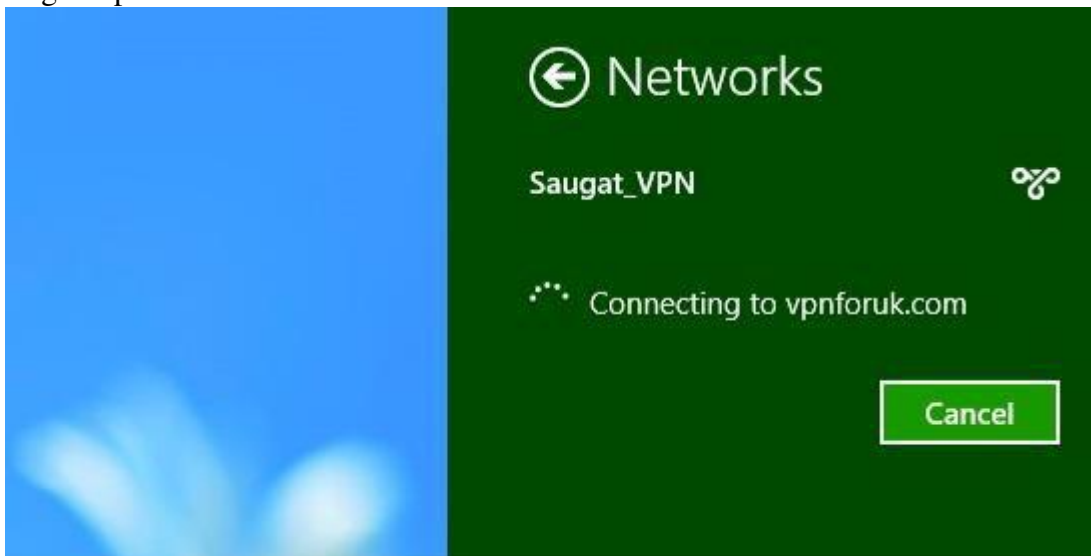


Fig 6: connecting to vpnforuk.com

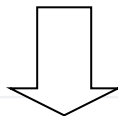
### Step 5:

Network Authentication to connect to VPN connection:



<b>IP</b>	2405:205:41ab:840b:6ce0:78f4:acab:bee4	<b>Hostname</b>	2405:205:41ab:840b:6ce0:78f4:acab:bee4	<b>ASN</b>	55836
<b>Country</b>	India (IN)	<b>Provider</b>	Reliance Jio Infocomm Limited	<b>Continent Code</b>	AS
<b>City</b>	Ludhiana	<b>Latitude</b>	30.8968	<b>Continent Name</b>	Asia
<b>Region</b>	Punjab (PB)	<b>Longitude</b>	75.8485	<b>TimeZone</b>	Asia/Kolkata
<b>Postal Code</b>	141008	<b>Metro Code</b>		<b>DateTime</b>	2019-03-26 21:50:10

<b>IP</b>	2405:205:41ab:840b:6ce0:78f4:acab:bee4	<b>Hostname</b>	2405:205:41ab:840b:6ce0:78f4:acab:bee4	<b>ASN</b>	55836
<b>Country</b>	India (IN)	<b>Provider</b>	Reliance Jio Infocomm Limited	<b>Continent Code</b>	AS
<b>City</b>	Ludhiana	<b>Latitude</b>	30.8968	<b>Continent Name</b>	Asia
<b>Region</b>	Punjab (PB)	<b>Longitude</b>	75.8485	<b>TimeZone</b>	Asia/Kolkata
<b>Postal Code</b>	141008	<b>Metro Code</b>		<b>DateTime</b>	2019-03-26 21:50:10



<b>IP</b>	178.128.31.231	<b>Hostname</b>	178.128.31.231	<b>ASN</b>	14061
<b>Country</b>	Singapore (SG)	<b>Provider</b>	DigitalOcean, LLC	<b>Continent Code</b>	AS
<b>City</b>	Singapore	<b>Latitude</b>	1.2929	<b>Continent Name</b>	Asia
<b>Region</b>	Central Singapore Community Development Council (01)	<b>Longitude</b>	103.8547	<b>TimeZone</b>	Asia/Singapore
<b>Postal Code</b>		<b>Metro Code</b>		<b>DateTime</b>	2019-03-27 00:21:36

Fig 8: IP address before and after connecting to VPN

## **5. 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.

**- Rohit  
Sharma**