# Lecture – 13  (Dt. 15th April 2020)

## Electronic  Switching ( EC- 8th Sem)

## Virtual Private Network (VPN)

**References :**

1) S. Agrawal : Lecture Notes (VSSUT)

2) Telecommunication Switching Systems & Networks, Thiagrajan

3) Telecommunication System Engineering, R.L. Freeman

4) Telecommunication Switching and Networks, By, P. Gnanasivam

5) Internet sources

**The Writer is not responsible for any legal issue arising out of any copyright demands and/or reprint issues contained in this material. This is not meant for any commercial purpose. This is solely meant for personal reference of students during Covid-19 following the syllabus prescribed by the university.**

**Acknowledgment :**

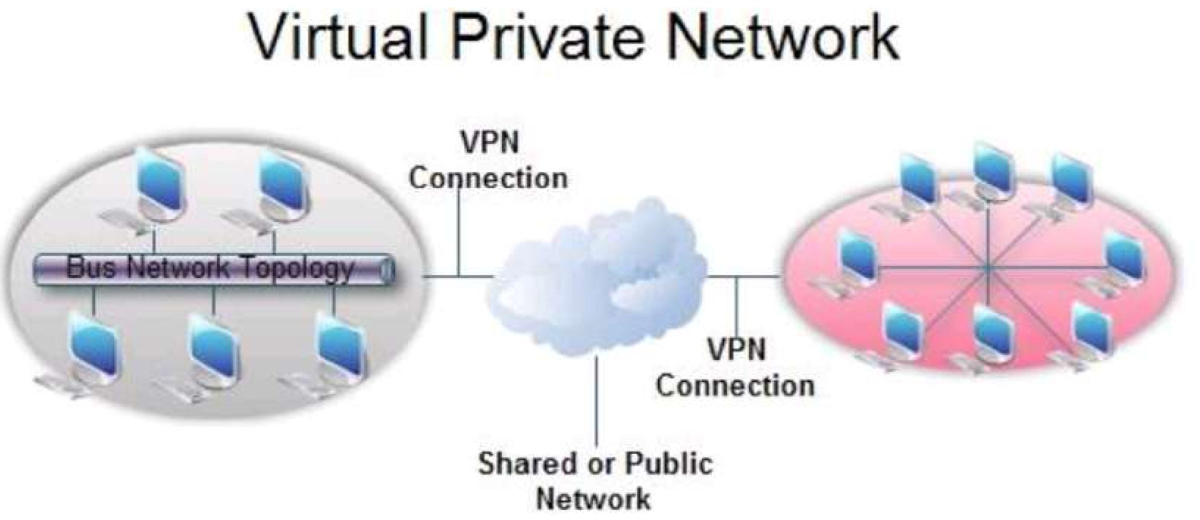
**Special thanks to Prof. S. Agrawal (VSSUT) for providing online lecture notes.**

*VPN* (*Virtual Private Network*) *Definition*: VPN meaning that it is a private point-to-point connection between two machines or networks over a shared or public network such as the internet. VPN (Virtual Private Network) technology, can be use in organization to extend its safe encrypted connection over less secure internet to connect remote users, branch offices, and partner private, internal network. VPN turn the Internet into a simulated private WAN.

A VPN client uses TCP/IP protocol, that is called tunnelling protocols, to make a virtual call to VPN server.

What is VPN

VPN allows users working at home or office to connect in a secure fashion to a remote corporate server using the routing infrastructure provided by a public inter-network (such as the Internet). From the user's perspective, the VPN is a point-to-point connection between the user's computer and a corporate server. The nature of the intermediate inter-network is irrelevant to the user because it appears as if the data is being sent over a dedicated private link.



Main Network Protocols

There are three network protocols are used within VPN tunnels. That are:

IPSec

IPsec (*Internet Protocol Security*) is a framework for uses cryptographic security services developed by the IETF to protect secure exchange communications over Internet Protocol (IP).It supported encryption modes are transport and tunnel.

PPTP

PPTP (*Point-to-Point Tunneling Protocol*) is a network protocol that extending the organization private networks over the public Internet via "tunnels.

L2TP

L2TP (*Layer Two Tunneling Protocol*) is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by Internet service providers (ISPs) to operate Virtual Private Networks (VPNs).

Privacy, Security and Encryption

Data sent across the public Internet is generally not protected from curious eyes, but you can make your Internet communications secure and extend your private network with a virtual private network (VPN) connection. VPN uses a technique known as tunneling to transfer data securely on the Internet to a remote access.

The Internet connection over the VPN is encrypted and secure. New authentication and encryption protocols are enforced by the remote access server. Sensitive data is hidden from the public, but it is securely accessible to appropriate users through a VPN.

## How to Setup a VPN

There are following two ways to create a VPN connection:

### By dialling an Internet service provider (ISP)

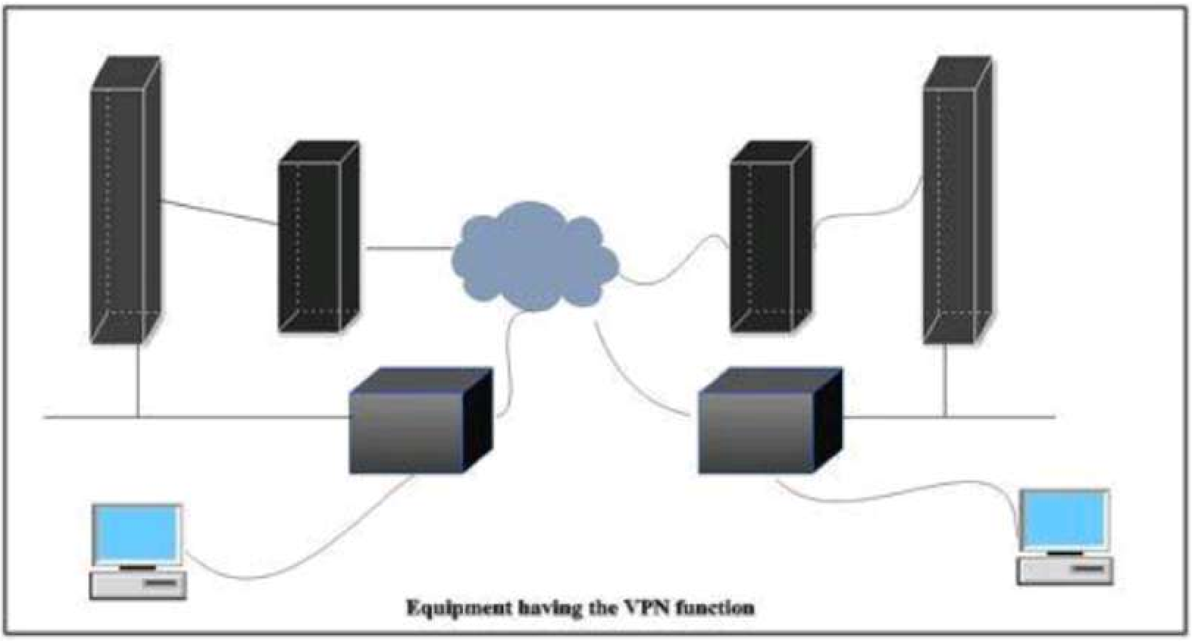
If you dial-in to an ISP, your ISP then makes another call to the private network's remote access server to establish the PPTP or L2TP tunnel after authentication, you can access the private network.

### By connecting directly to the Internet

If you are already connected to an Internet, on a local area network, a cable modem, or a digital subscriber line (DSL), you can make a tunnel through the Internet and connects directly to the remote access server. After authentication, you can access the corporate network.

## Equipment of VPN

Equipment having the VPN function includes routers and firewalls. Basically, communication is made via VPN equipment. Information is encrypted by the transmission VPN equipment before transmission and decoded by the receiving VPN equipment after receipt of information. The key for encrypt the data is set in VPN equipment in advance. The VPN equipment at receiving side decodes encrypted data before sending it to the receiving computer.



Equipment having the VPN function

The advantages of encryption by way of cryptography may be looked into other services, such as

1. Assuring integrity check: This ensures that undesirable person has not tampered data delivered to the destination during transmission.
2. Providing authentication: Authentication authorizes the sender identity.

## Features of a Typical VPN solution

When the remote offices connect each other to share vital resources and secret information, the VPN solution must ensure the privacy and integrity of the data as it traverses the Internet. Therefore, a VPN solution must provide at least all of the following:

Keep data confidential (encryption)

- Data carried on the public network must be rendered unreadable to unauthorized clients on the network.

Ensure the identities of two parties communicating (authentication)

- The solution must verify the user's identity and restrict VPN access to authorized users only. It must also provide audit and accounting records to show who accessed what information and when.
- Safeguard the identities of communicating parties (tunnelling)
- Guard against packets being sent over and over (replay prevention)
- Ensure data is accurate and in its original form (non-repudiation)

Address Management. The solution must assign a client's address on the private net and ensure that private addresses are kept private.

Key Management. The solution must generate and refresh encryption keys for the client and the server.

Multiprotocol Support. The solution must handle common protocols used in the public network. These include IP, Internet Packet Exchange (IPX), and so on.

An Internet VPN solution based on the Point-to-Point Tunneling Protocol (PPTP) or Layer 2 Tunneling Protocol (L2TP) meets all of these basic requirements and takes advantage of the broad availability of the Internet. Other solutions, including the new IP Security Protocol (IPSec), meet only some of these requirements, but remain useful for specific situations.

## Benefits of VPN

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 (in 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 point-to-point leased lines.