Abstract: This paper discusses the algorithm for a backup virtual private network and its usage in banks for smooth and consistent functioning. It also discusses its functioning and implementation in banks.

Keywords: Virtual Private Network, topology, banking technology, internet service provider.

1. INTRODUCTION
While using internet through a network service provider, the compiler is given an address from the ISP. Banks do not allow users to access a particular service of the bank because their compiler is using an address from an external network. But still, we can connect to the banks VPN network through the internet. A VPN does not necessarily have explicit security features and properties, like authentication or data encryption. We can use Virtual Private Network to setup separate traffic for different communities of users over an underlying network having very high and strong security features.

2. VIRTUAL PRIVATE NETWORK IN BANKING
In order to have a secured connection between locations in an open internet, site to site VPN allows you to have it. Banks can save a great deal of money, as cheaper means can always be used - on connections like domestic broadband rather than high cost leased lines across sites with the help of site to site VPN.

3. REMOTE ACCESS VPN
Normally remote access VPN is also called VPDN (Virtual Private Dial up). It is used in banks that have a particular staff which works regularly in locations present outside the office. Dial up phone lines or isdn lines or over broadband can be used to connect into the office network from anywhere.
Advanced encryption and tunneling can be used by virtual private network banking to allow desktops or PC’s to establish a end to end , secure, private network connection over networks which are insecure i.e. internet and wireless networks. The network performance and overall computing is deeply affected by VPN services. Existence of VPNs is to protect high amounts of traffic on public data networks such as the internet. Other ISP dialup services too can be used to work with VPN services.

4. BACKUP VPN
4.1 Implementation
The head branch of the bank uses a dedicated LAN or VAN provided by network service provider (ISP) to connect to the different branches and their databases at different location. But the collisions in this kind of networks are high. So to reduce the collision, VPN is used as it can create its own network and separates traffic of different user communities over an underlying network with strong security features and so restricts the traffic unto a limited value and reduces the collisions.

4.2 Algorithm
Initially, when the bank uses VPN, the logic on link 1 is set to 1. If link 1 crashes, the logic on link 1 is then set to 0. As the backup VPN provider is connected by a NOT gate to link 1, the logic on link 2 becomes 1 and hence the backup VPN is created automatically. When traffic reduces to a certain level the bank gets connected to the other branches by the former VPN. So link 1 is created again and its logic becomes 1. Since link 2 is connected to the server through the NOT gate, link 2’s logic becomes 0 and it gets deactivated automatically.

4.2.1 Figures and Tables

![Figure 1 Virtual Private Network Layout for banks](image1)

![Figure 2 Overall Network Map](image2)
4.3 Advantages
There will be a reduction of packet collision due to separation of traffic communities which is a basic characteristic of a VPN server. The use of a backup VPN server will remove the disadvantage of VPN server i.e., its inconsistent behavior. Bank functionality can be improved by implementing site to site VPN server.

4.4 Disadvantages
Generally, VPNs are inconsistent. For example; the user who is making a transaction at one branch can transact money from/to other branches through this VPN. If many users are operating on the network and the crowd on this network reaches a threshold value of VPN, this VPN crashes and causes a link failure. And the users have to wait for getting the transaction done till the link is back. To solve this problem, Backup VPN provides another network, so that the user can complete its transaction till the link is back and no time gets wasted.

5. CONCLUSION
After observing the above advantages we can easily conclude that backup virtual private network can be implemented in banks as it provides a smooth functionality and does not affect the user transactions from crashed networks. It also provides a new network whenever the usual networking in banks fails to stand up to the load and rush of concurrent transactions by users. It recovers from a link failure as quickly as possible so that there is no effect on functioning of banks. It isolates the networking failures from the users/customers so that they can complete their transactions without any hint of network failure. It also reduces the amount of collisions in the network.

References