Abstract
A VPN, as its name suggests, is just a virtual version of a secure, physical network—a web of computers linked together to share files and other resources. But VPNs connect to the outside world over the Internet, and they can serve to secure general Internet traffic in addition to corporate assets. In fact, the lion's share of modern VPNs are encrypted, so computers, devices, and other networks that connect to them do so via encrypted.

VPN Security and Design
VPN Pros and Cons
Pro – Virtual private networks offer a much higher level of secure communication when compared to other remote methods of communication.  
Con – The design and security implementation for a virtual private network can be complex. This means that it requires a professional with a high level of understanding for the best type of VPN configuration and some of the security issues that can occur when using a VPN.

VPN Cost
Pro – When it comes to operating a virtual private network within an organization the costs are significantly lower than other types of configurations.  
Con – Reliability can become a factor depending upon the service provider that you choose. If the VPN utilizes the Internet it is important to work with a provider that can guarantee minimal downtime.

Conclusion:
During our project we learned and used real time installation of server and client software, Active directory, DNS, DHCP, VPN and Group policy using in Windows environment.