Understanding the VPN Client
The VPN Client is a software program that runs on a Microsoft Windows-based PC. The VPN Client on a remote PC, communicating with a Cisco VPN device at an enterprise or service provider, creates a secure connection over the Internet that lets you access a private network as if you were an on-site user. That’s why it’s called a VPN: a Virtual Private Network.

As a remote user (low speed or high speed), you first connect to the Internet. Then you use the VPN Client to securely access the private enterprise network through a Cisco VPN device that supports the VPN Client.

The VPN Client comprises the following applications, which you select from the Program menu: In logical order of use, the applications are as follows:
- **Help** — displays an online manual with instructions on using the applications.
- **VPN Dialer** — lets you configure connections to a VPN device and lets you then start your connections.
- **Certificate Manager** — lets you enroll for certificates to authenticate your connections to VPN devices.
- **Log Viewer** — lets you display events from the.
- **Set MTU** — lets you change the MTU setting on your PC, used for troubleshooting.
- **Uninstall VPN Client** — lets you safely remove the VPN Client software from your system and retain your connection and certificate configurations.

How it works
The VPN Client works with a Cisco VPN device to create a secure connection, called a tunnel, between your computer and the private network. It uses Internet Key Exchange (IKE) and Internet Protocol Security (IPSec) tunneling protocols to make and manage the secure connection. Some of the steps include:
- Negotiating tunnel parameters: addresses, algorithms, lifetime, etc.
- Establishing tunnels according to the parameters.
- Authenticating users: making sure users are who they say they are, via usernames, group names and passwords, and X.509 digital certificates.
- Establishing user access rights: hours of access, connection time, allowed destinations, allowed protocols, etc.
- Managing security keys for encryption and decryption.
- Authenticating, encrypting, and decrypting data through the tunnel.

For example, to use a remote PC to read email at your organization, you connect to the Internet, then start the VPN Client and establish a secure connection through the Internet to your organization’s private network. When you open your email, the Cisco VPN device uses IPSec to encrypt the email message; and it transmits the message through the tunnel to your VPN Client, which decrypts the message so you can read it on your remote PC. If you reply to the email message, the VPN Client uses IPSec to process and return the message to the private network through the Cisco VPN device.

Connection technologies
The VPN Client lets you use any of the current technologies to connect to the Internet:
- **POTS (Plain Old Telephone Service)**: uses a dial-up modem to connect.
- **ISDN (Integrated Services Digital Network)**: may use a dial-up modem to connect.
- **Cable**: uses a cable modem; always connected.
- **DSL (Digital Subscriber Line)**: uses a DSL modem; always connected.

You can also use the VPN Client on a PC with a direct LAN connection.

Features
- **IPSec tunneling protocol.**
- **IKE key management protocol.**
- **IKE Keepalives** — monitoring the continued presence of a peer and reporting the VPN Client’s
continued presence to the peer, which prevents hung connections due to loss of connectivity.

- Data compression for modem users, which speeds transmission.
- Split tunneling — the ability to simultaneously direct packets over the Internet in clear text and encrypted through an IPSec tunnel.
- User authentication via VPN Concentrator:
  - Internal VPN Concentrator server database.
  - RADIUS (Remote Authentication Dial-In User Service).
    - NT Domain (Windows NT®).
  - RSA (formerly SDI) SecurID or SoftID.
- Automatic connection via Microsoft Dial-Up Networking.
- Automatic VPN Client configuration option.
- Log Viewer — an application that collects events for viewing and analysis.
- Set MTU size — the ability to control the size of packets sent through the network.
- Certificate Manager — an application that lets you manage your identity certificates.
- Complete browser-based context-sensitive HTML Help.
- Support for Cisco Secure PIX Firewall platforms that run Release 6.0 and above.
- Support for VPN Concentrator Series 3000 platforms.
- LZS data compression.
- Command line interface to the VPN Dialer.
- Start Before Logon — the ability to establish a VPN connection before logging on to a Windows NT or Windows 2000 system.
  - Application Launcher — the ability to launch an application from the logon desktop.