VPN setup for the XV100

Powering Business Worldwide

Table of Contents

1) Overview

1.1) Background Information

The business world has been transformed these last decades. The appearance of technology and especially the internet has changed the way of doing business. Instead of being a local or regional company, a lot of firms have now grown to be worldwide, having many facilities around the globe and a large part of their workforce mobile. This raises the question of how to communicate quickly, safely and reliably within the company.

Before the appearance of Virtual Private Networks (VPN), dependable communication outside of the nearby geographical area was achieved by using wide-area networks (WAN). This meant the use of leased lines ran by telecommunication providers. A very safe and reliable way of communicating, WANs have however two major weaknesses : extremely high cost who grow higher as the connecting networks are further from each other, and they are completely immobile.

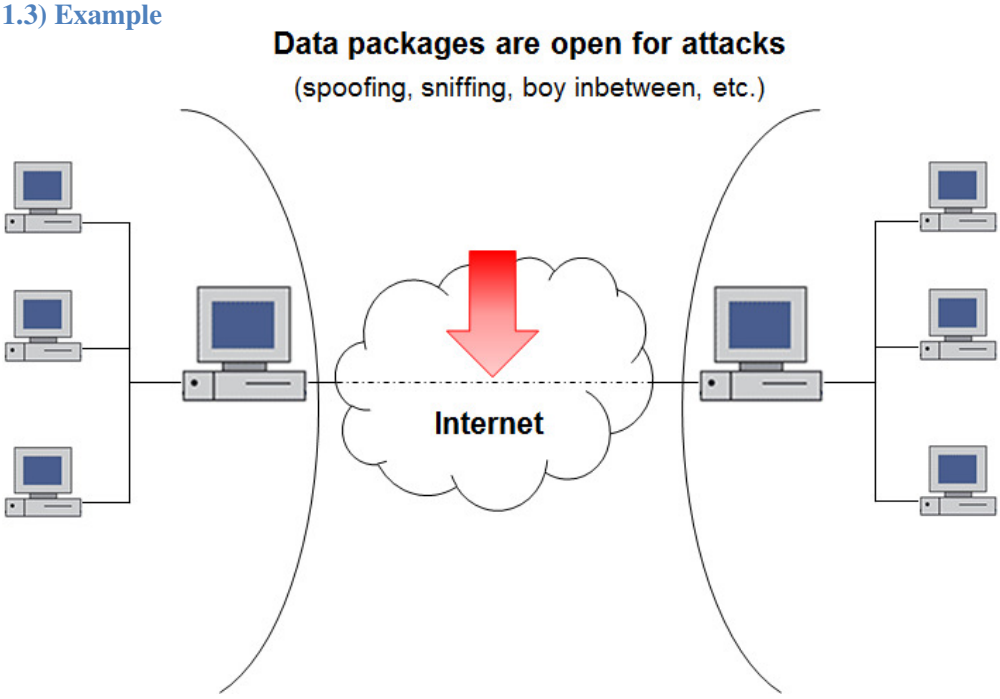
With the rise of the Internet, worldwide communication is much easier. Companies have turned to it, using it for its lower cost and mobility. The main problem with a network like the Internet is the fact that it is public. This means that your connection to another point of the Internet is open for attacks, perhaps compromising the confidentiality or the integrity of the exchanging data. This is why businesses use VPNs or even make their own, protecting their data from any attack.

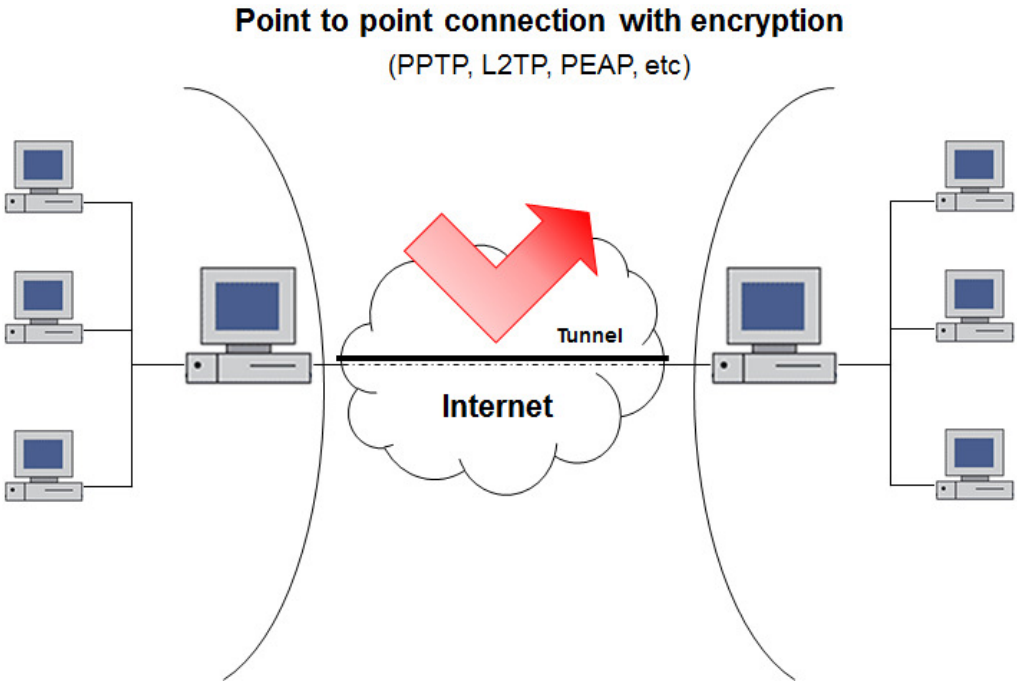
A typical VPN might have a main local-area network (LAN) at the corporate headquarters of a company, other LANs at remote offices or facilities, and individual users that connect from out in the field. A VPN is a private network that uses a public network (usually the Internet) to connect remote sites or users together. Instead of using a dedicated, real-world connection, such as leased line, a VPN uses "virtual" connections routed through the Internet from the company's private network to the remote site or employee.

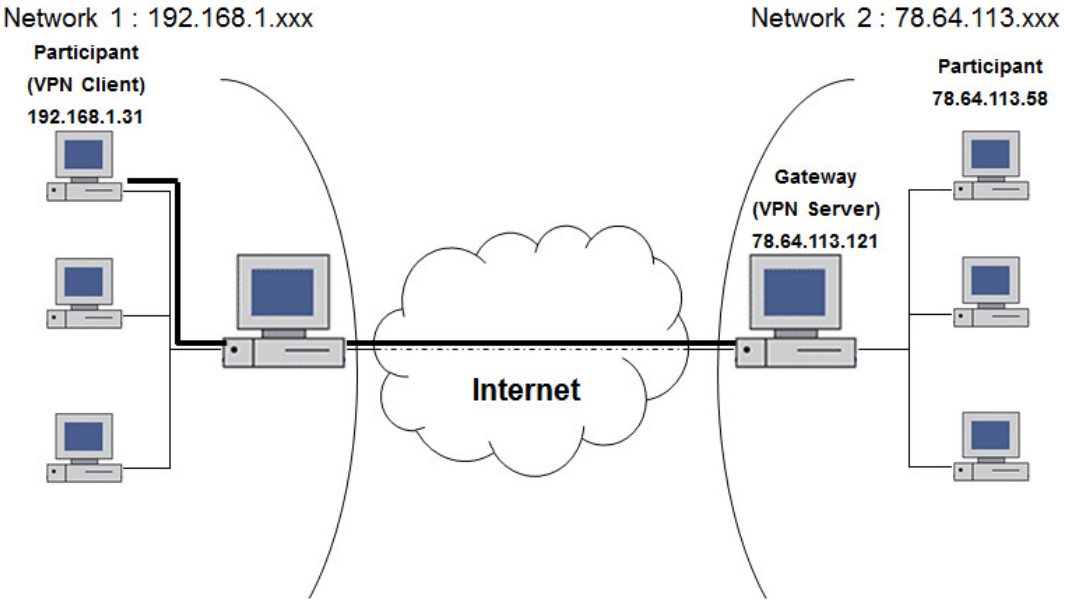
1.2) Short Definition

A VPN is a secure connection over the internet between two or multiple networks. It allows the parties to exchange data in a safe and rapid way. It does so by encrypting the data and/or tunneling it, and only the party with the encrypting key is able to decrypt the data. The two major part of a VPN are the client and the server. The client is the one that wants to access the private network, and the server is the one that allows him to connect, and assigns him a IP address.

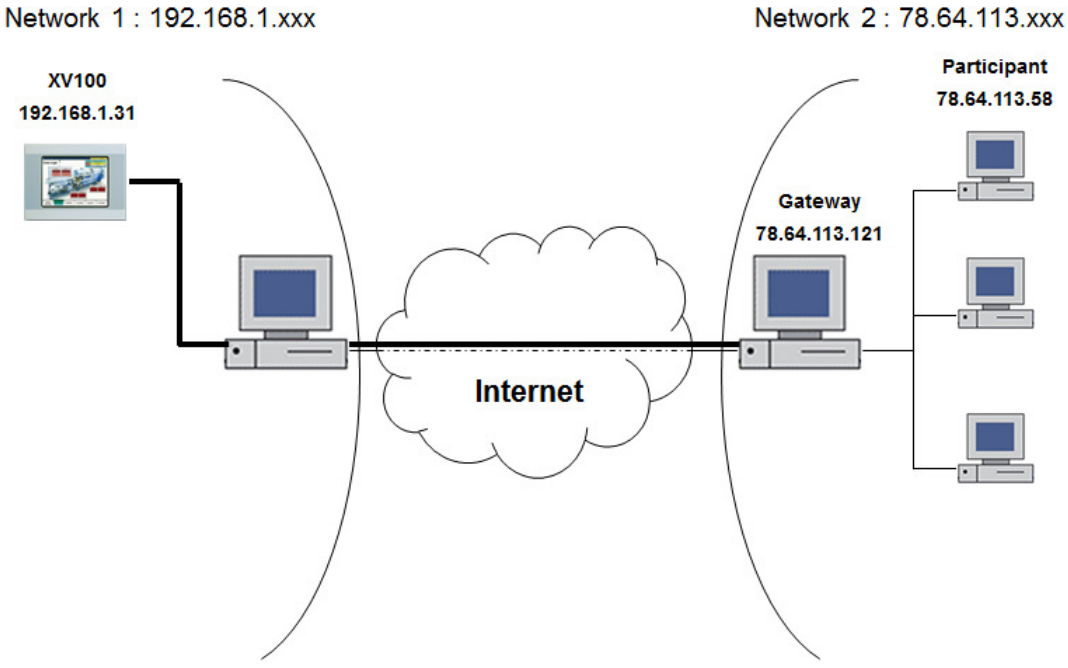
1.3) Example


Data packages are open for attacks
(spoofing, sniffing, boy inbetween, etc.)
Internet


Point to point connection with encryption
(PPTP, L2TP, PEAP, etc)
Tunnel
Internet



- A VPN client (192.168.1.31) connects to a VPN server (78.64.113.121).
- The VPN server assigns an IP address from the server subnet to the VPN client (78.64.113.92).
- The VPN client can send and receive data e.g. to 78.64.113.58 by sending first to the gateway which then rallies it further.
- Subnet participants can send data to the VPN client by using the address 78.64.113.92 as the gateway will package and send further.
- The connection as well as the internal data are encrypted and have security checks.



2) VPN Structure

2.1) Functionality

A VPN has one simple mission : to transfer data in a matter that is safe and fast from anywhere on the planet. This goal is accomplished with the use of diverse methods and technologies. It is based on a client-server model : the client sends a request to connect to the server, who accepts or rejects the demand of the client. If the connection is established, the two computers are now able to exchange data. VPNs work in a similar way, only it adds security layers to the connection.

The security in a VPN connection is provided by tunneling and encryption. Encryption is the fact of coding the data in a way that if any third party to the connection intercepts the data, it will not be able to understand it. The two connecting networks use encrypting keys to be able to decode the data. Tunneling on the other hand, does not encrypt the data, but rather hides the content and identity of data packets.

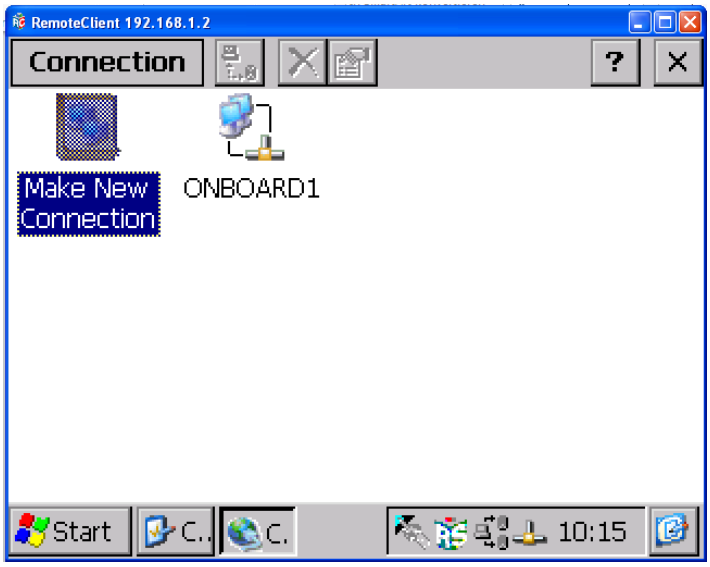
All of this is accomplished by the use of protocols, a list of rules used by the computers. Some of them include the Internet Protocol Security Protocol (IPsec), the Point-to-Point Tunneling Protocol (PPTP) and the Layer 2 Tunneling Protocol (L2TP). They are of course many more, but these are the most known ones. Most of them work in a combination with another protocol, guarantying the safety of the data. Tunneling keeping the data “invisible” and encryption making impossible to read for any other person than the receiver. No third party can see or read the data, protecting against any type of attacks. The confidentiality is important, but the most important is that the data stays completely intact, it should not be compromised or altered by a poor encryption that accidently modifies the content of the packet when decrypting it.

3) Requirements

The following is required from the XV100

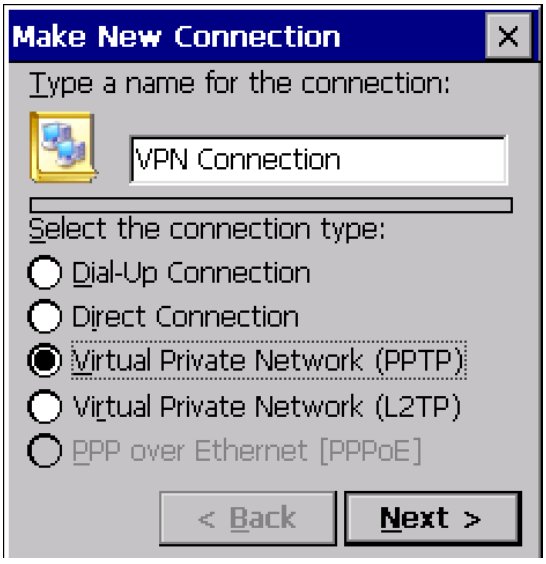
- Galileo 8.1.1
- Download operating system WindowsCE Image version 2.26.3 to the panel (in the documentation CE operating system image 2.26.3 in chapter 7.26 detailed information can be found)
- A connection to the local network. If needed, please refer to the Quick Start Guideline.

4) Setting up the VPN Client



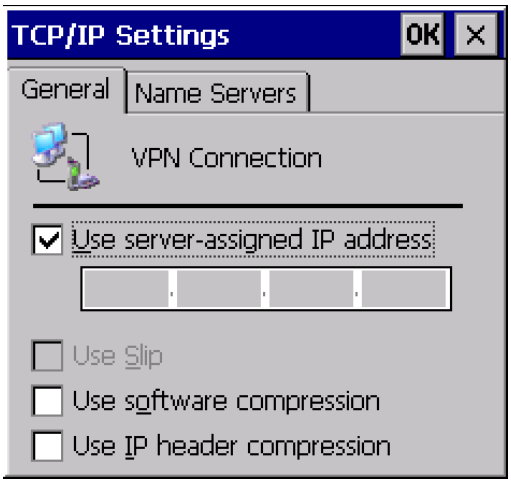
- Select "Start/Settings/Network and Dialup connections" in the operating system of the XV100.

- Double click "make new connection".



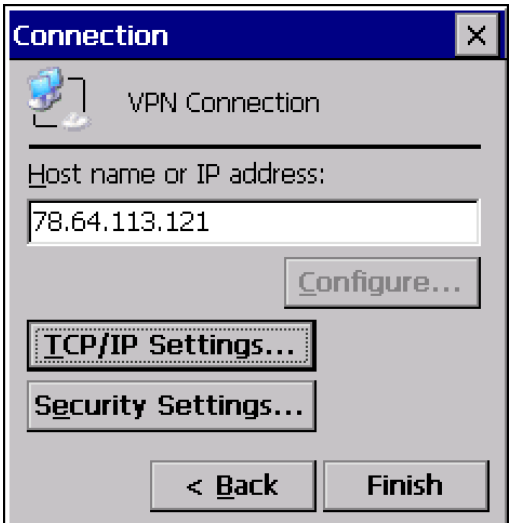
- Depending on the properties of the VPN server select the type of connection type.
(Typically PPTP –Point to Point Tunnel Protocol)

- Type in the IP address of the VPN server (or host name if using a DNS).

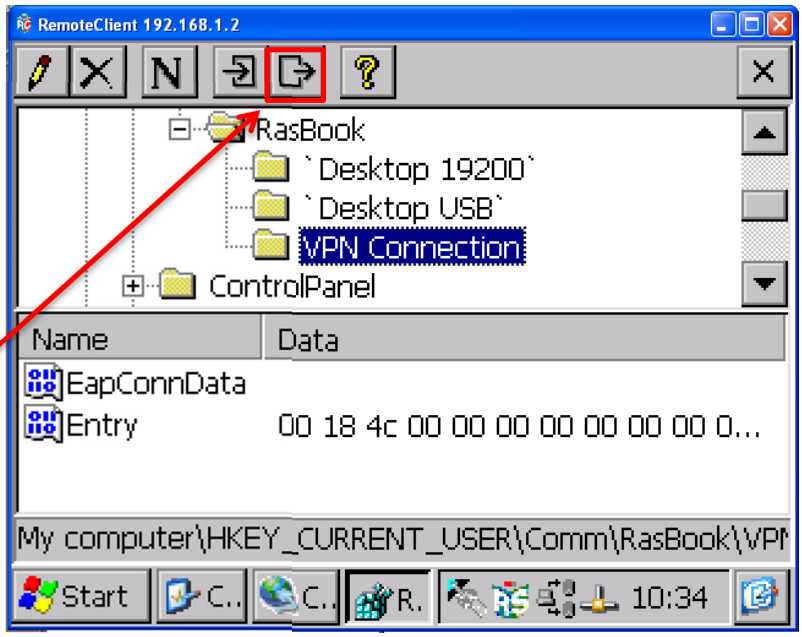


- Under TCP/IP settings check if the checkbox “use server-assigned IP address” (this should be the normal case).

- Here you can also select a fix address if the VPN server does not have DHCP capability.



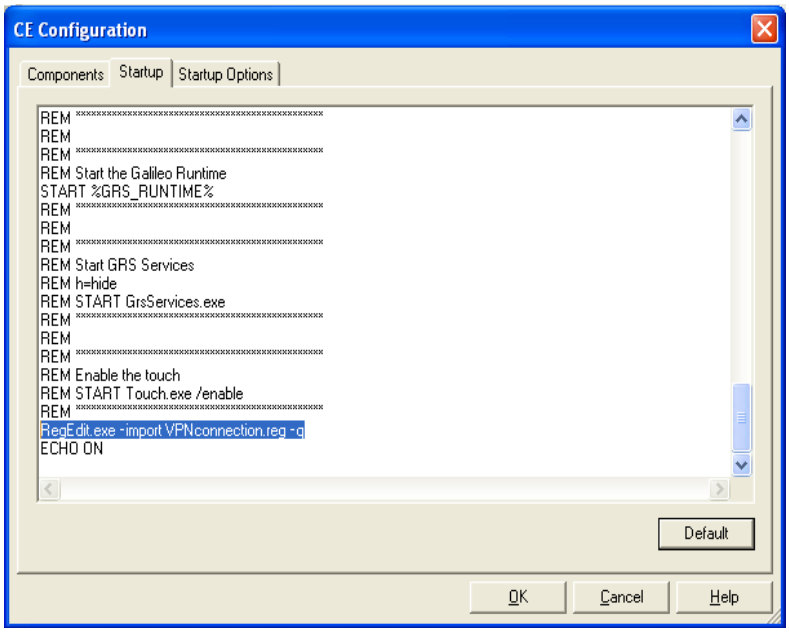
- Complete the connection with selecting “Finish”



- Open the registry editor through selecting “Start/Programs/System/Registry Editor”.

- Select in the registry editor the “HKEY_CURRENT_USER/Comm/RasBook/<Connection name>” In this example the connection name is “VPN connection”.

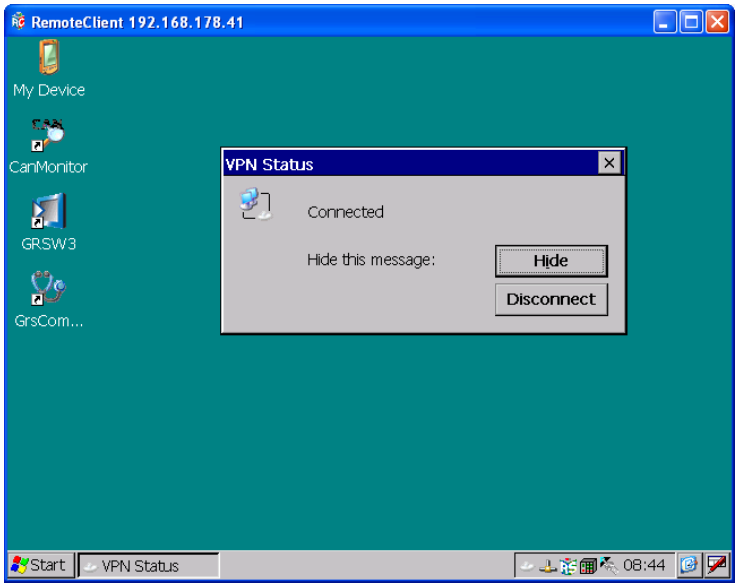
- Export the registry entry.



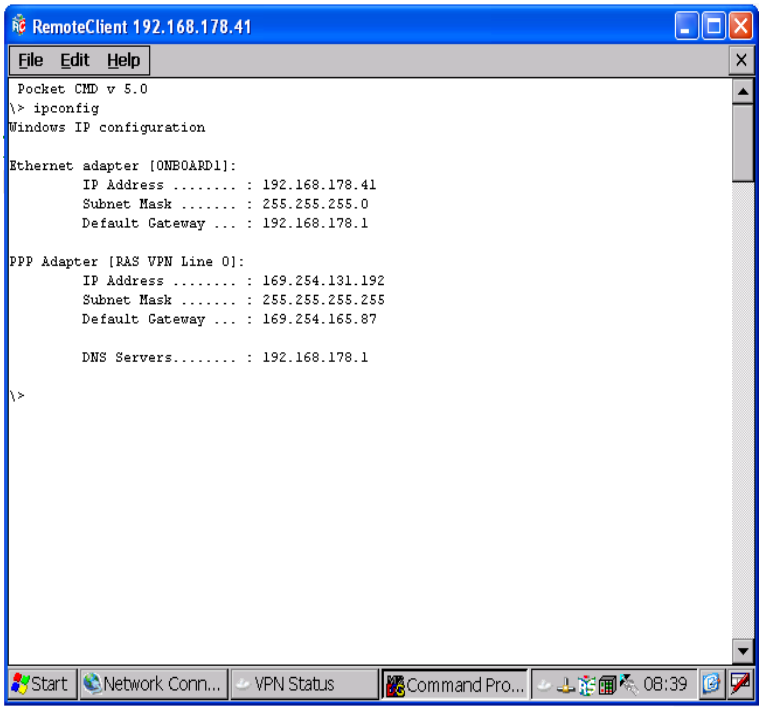
- In Galileo select “Config/CE Configuration”.

- Add in the autoexec.bat the call of the registry entry in this example “RegEdit.exe –import VPNconnection.reg –q”.

- Download with the Galileo project to the panel.



- VPN client connecting to the VPN server.



- The IP address of the unit is 192.168.178.41

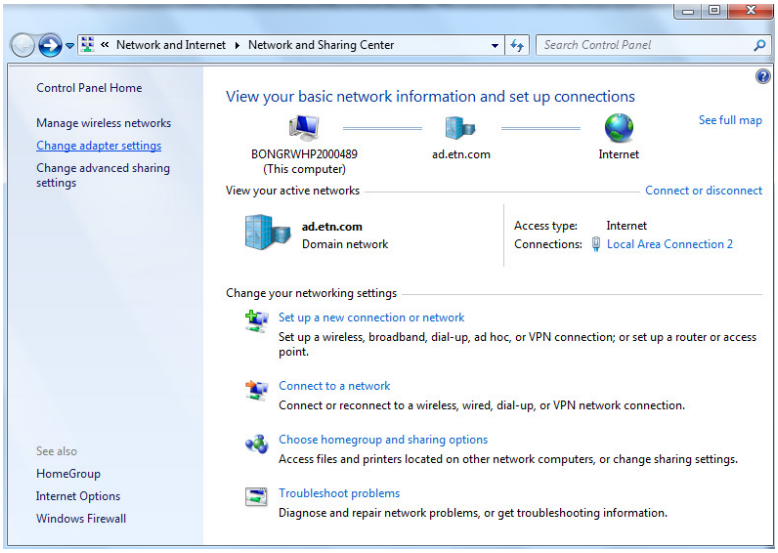
- The VPN address given by the VPN server is 169.254.131.192

5) Setting up the VPN server

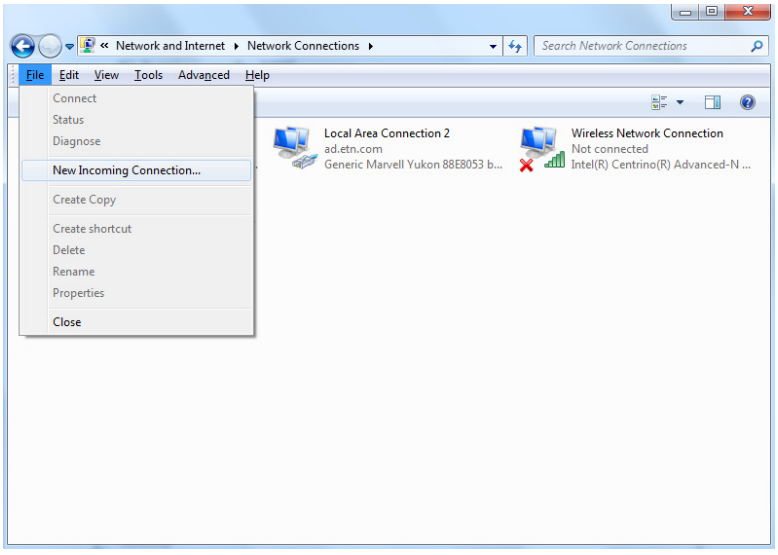
5.1) Info

The following tutorial is only for setting up a VPN server on your personal computer running on a Windows OS. For setting up a server with a different hardware and/or software, please refer to the product's manual.

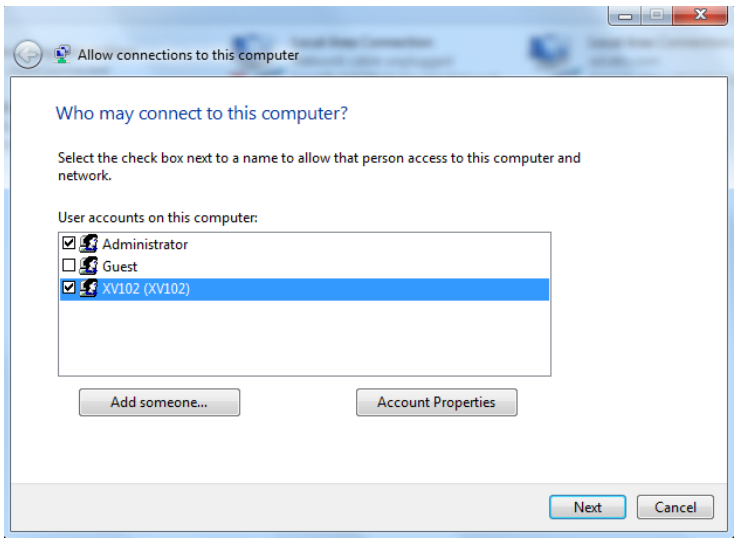
5.2) Setting up the server



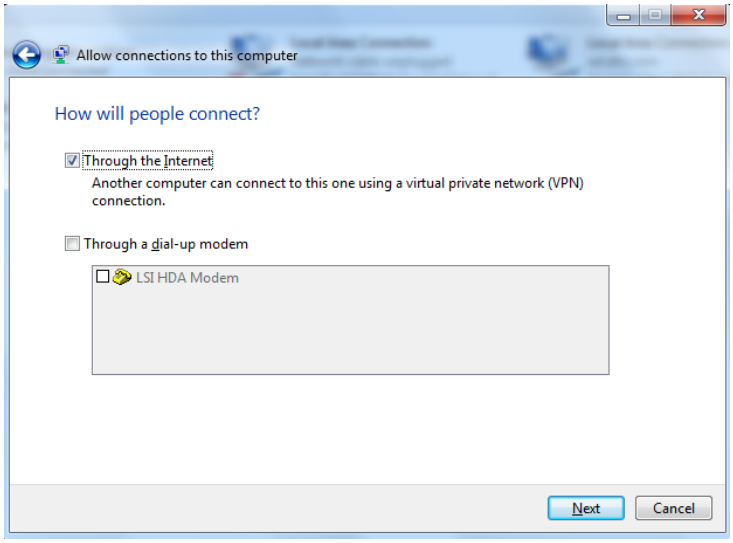
- Go to the start menu and write "Network and Sharing Center" and select it.
- Click on "Change adapter settings" (On the top left).



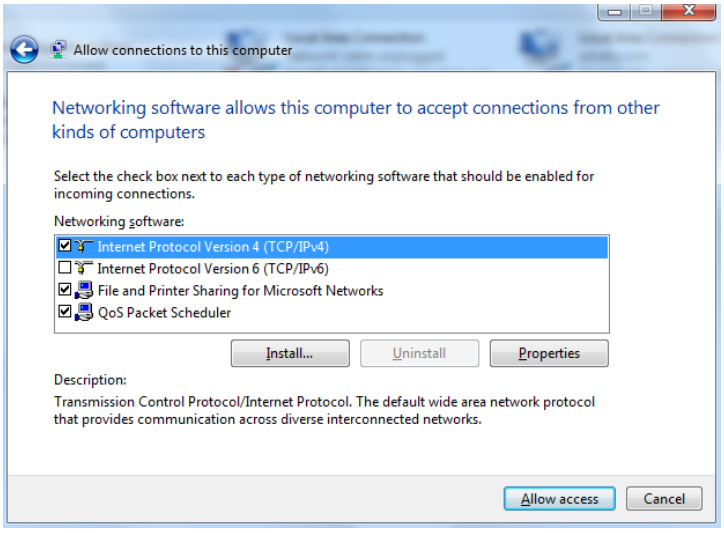
- On the top left, click on "File" then on "New Incoming Connection…" (If the top menu bar does not appear, press the "alt" key).



- Click on “Add someone” and put in the name of the device and a password, then click on “Ok” and then on “Next”.



- Check on the needed box/boxes (Usually “Through the Internet”).



- Check the needed option and then click on “Allow access”. (If unsure, check the box as seen in the picture).

6) Glossary

Client: A client is a piece of computer hardware or software that accesses a service made available by a server. The server is often on another computer system, in which case the client accesses the service by way of a network.

Dynamic Host Control Protocol (DHCP): A network server uses this protocol to dynamically assign IP addresses to networked computers. The DHCP server waits for a computer to connect to it, and then assigns it an IP address from a master list stored on the server. DHCP helps in setting up large networks, since IP addresses do not have to be manually assigned to each computer on the network. Because of the slick automation involved with DHCP, it is the most commonly used networking protocol.

Internet Protocol (IP): Provides a standard set of rules for sending and receiving data through the Internet.

IP Address: A code that identifies a particular computer on the Internet. Every computer requires an IP address to connect to the Internet. IP addresses consist of four sets of numbers from 0 to 255, separated by three dots. For example "66.72.98.236" or "216.239.115.148".

Local-Area Network (LAN): computer network that interconnects computers in a limited area such as a home, school, computer laboratory, or office building.

Server: A server is a system (software and suitable computer hardware) that responds to requests across a computer network to provide, or help to provide, a network service.

Wide-Area Network (WAN): a network that covers a broad area that links across metropolitan, regional, or national boundaries, using private or public network transports. Business and government entities utilize WANs to relay data among employees, clients, buyers, and suppliers from various geographical locations.

Application Summary

<Summary of the contents of the application. If there are companion sample programs list them here >

Products and Revisions

< List the products covered here along with the revisions of the products that are covered and the specific revision it was tested on.>

Vendor	Product	Applicable Revision	Tested Revision

Supporting Documentation

Manual Name	Reference Number

Important user information

< disclaimer requested from Legal. Example info only, copyright protected>

Application Details

< The body of the application note>

Additional Help

In the event additional help is needed:
In the US or Canada: please contact the Technical Resource Center at 1-877-ETN-CARE or 1-877-326-2273.

Location	Contact
United States	Technical Resource Center at 1-877-ETN-CARE or 1-877-326-2273.
Canada	
Europe	

All other supporting documentation is located on the Eaton web site at www.eaton.com

Eaton
1000 Eaton Boulevard
Cleveland, OH 44122 USA
Eaton.com

Powering Business Worldwide