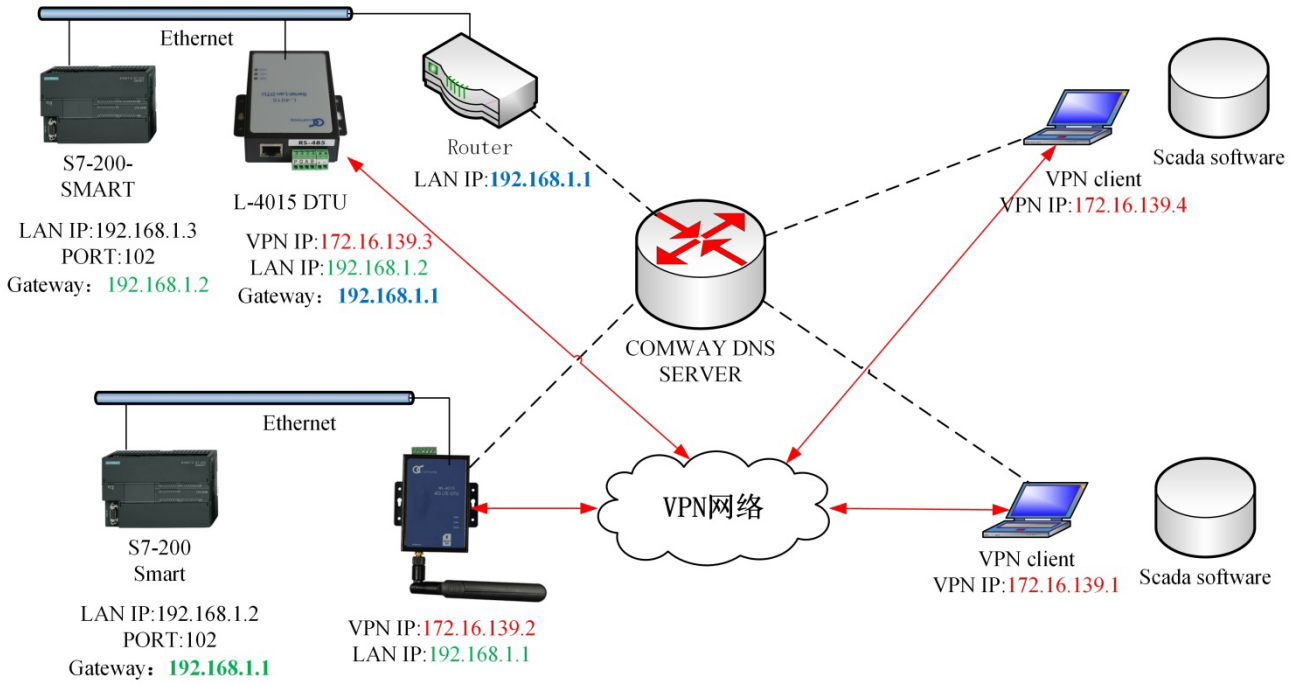
Implementation of VPN Communication for COMWAY 4G DTU and Ethernet DTU

Table of Contents

1. Overview

Comway 4G DTUs and RTUs are equipped with VPN communication functionality. They can achieve data communication via an Internet-based VPN network, and are suitable for connecting field devices with Ethernet ports, such as:

- Siemens S7-200 SMART, S7-1200, and S7-1500 PLCs: these can not only be used with configuration software to realize remote monitoring, but also with STEP 7 or TIA Portal programming software to enable PLC program downloading.
- PLCs with Ethernet ports from Mitsubishi, OMRON, and other manufacturers.
- HMI touch screens (MCGS) and other touch screen models.
- Campbell series data loggers.



2. Establishment of VPN Communication

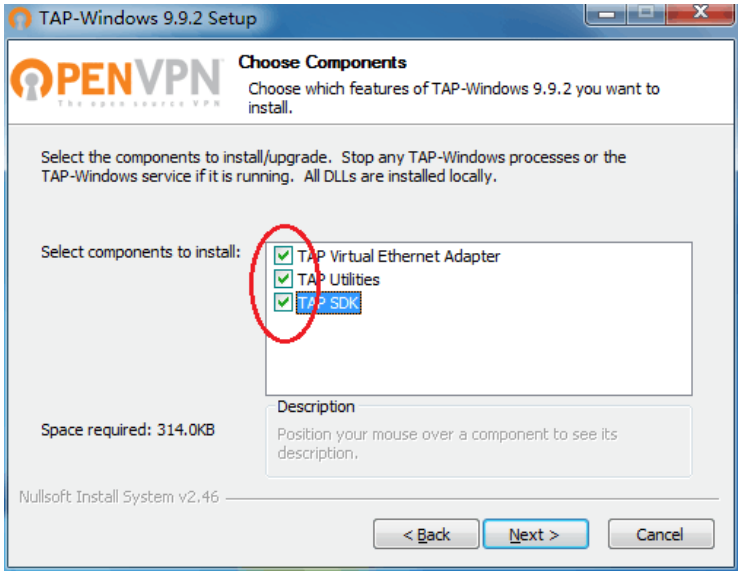
- Establish VPN communication via a Comway VPN Server.
- Apply for a public static IP address or a public dynamic IP address, then install the Comway VPN-HUB software to establish VPN communication.

3. Install DC-VPN Software on the Computer Side to Access the VPN

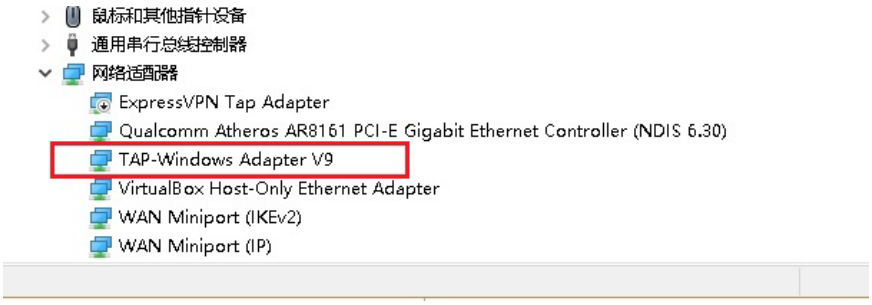
Any internet-accessible computer can install the VPN Client software (DC-VPN) to access the VPN network.

1) Install the virtual network adapter driver:

In the /tap-windows directory, double-click and run the tap-windows.exe program to install the virtual network adapter driver. In the interface shown in the figure below, make selections as indicated.

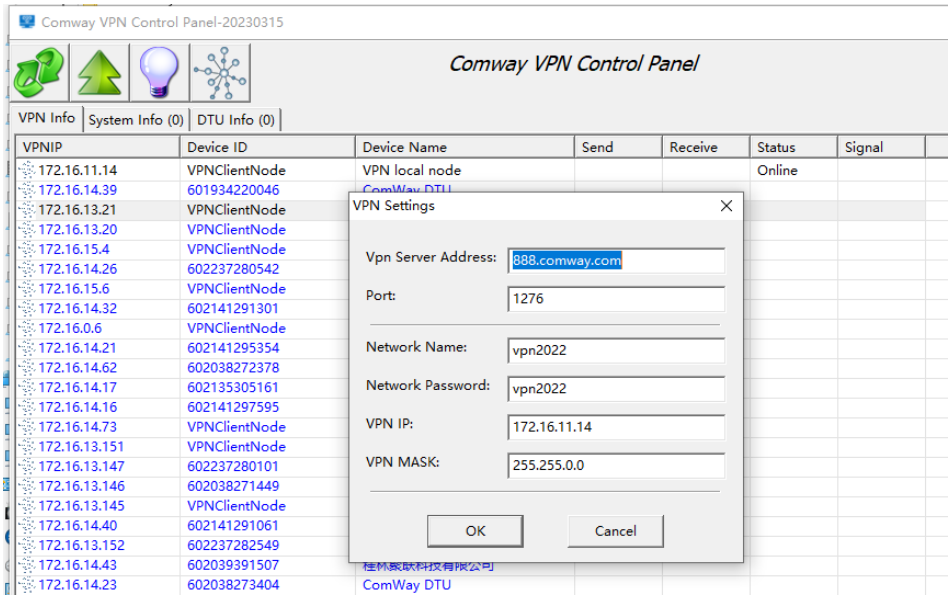


After the installation is completed, the content shown in the figure below will be displayed under **Network Adapters** in the **Device Manager** of the computer:



2) Install the DC-VPN software:

Unzip the COMWAY DC-VPN software, and grant administrator privileges to the bin\dc-vpn.exe executable file. The specific steps are as follows: right-click on the DC-VPN.exe file → select **Properties** → go to the **Compatibility** tab → check the box for **Run as administrator**. Then, launch the program, and the following interface will be displayed:



Right-click the mouse to display the function menu, then select **VPN Parameter Settings**; the interface shown in the figure will appear.

To communicate via the VPN SERVER provided by **Comway IOT.**, set the parameters as follows:

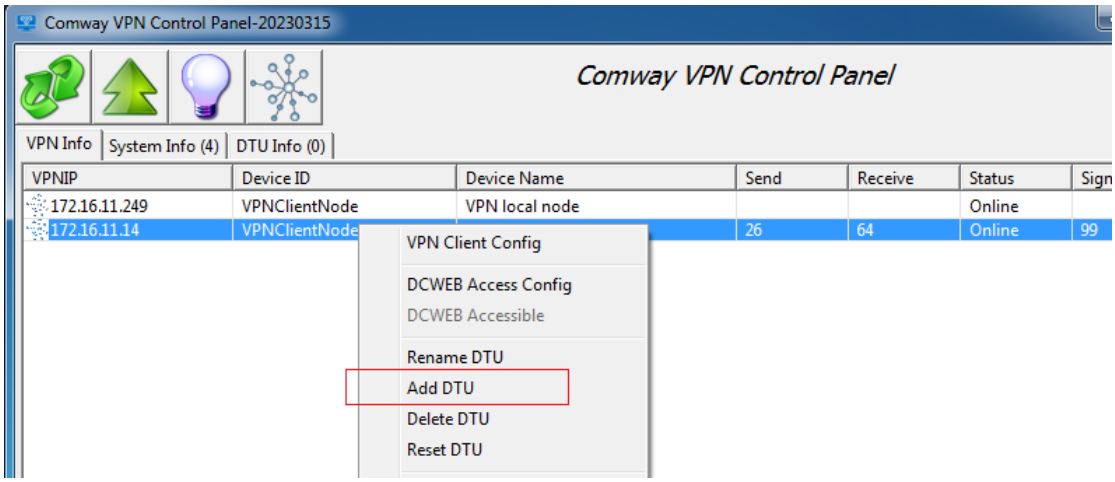
- **Server Address**: 888.comway.com
- **Port**: 1276

The **VPN name, password**, and **VPN IP address for the client side** are obtained in the following ways:

1. For connection to the VPN test server of Tontony Innovation Technology: Contact the company's technical support team to receive the assigned credentials and IP address.
2. For connection to a user-owned private VPN server: The VPN name and password must be consistent with those configured on the VPN-HUB side; the client's VPN IP address only needs to be in the same network segment as the one set on the VPN-HUB.

3) Add VPN Devices

To easily view the operating status of the VPN devices requiring communication establishment, you can right-click to display the function menu, then click **Add DTU** and enter the **VPN IP address** of the VPN device. When the device is online, its **device ID** and **signal strength value** will be automatically displayed, as shown in the figure below:



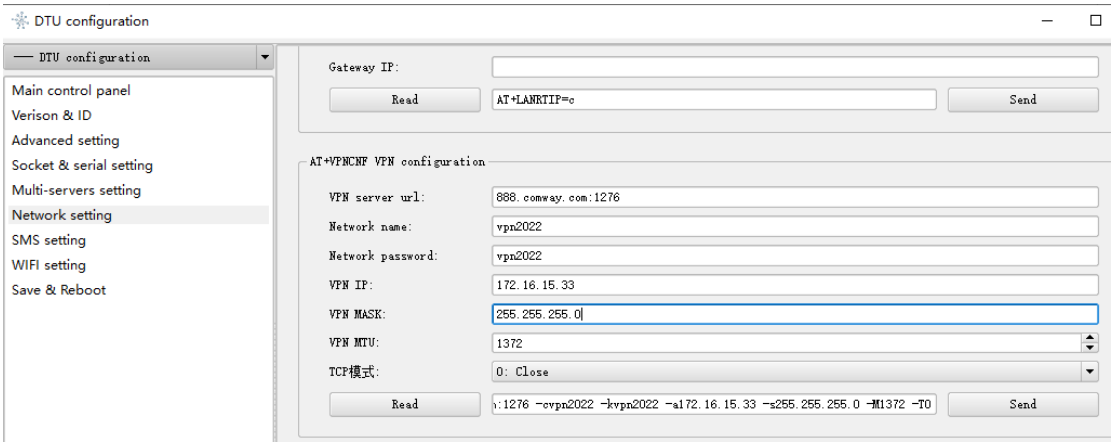
The DTU name is used for the user to easily identify the device.

After the VPN Client software runs normally, it should be able to **ping the VPN IP address of the VPN SERVER successfully**.

4. Set VPN parameters for 4G DTU

1) Configure the VPN Parameters of the 4G DTU

Use the 4G DTU configuration software, navigate to the Ethernet Communication Configuration interface, and set the VPN Network Configuration. Enter the corresponding parameters and click Send.



VPN Server URL: Enter the public network IP of the VPN SERVER, or the applied DNS domain name and port. Example: 888.comway.com:1276

Network IP: Enter the VPN IP assigned within the VPN network segment.

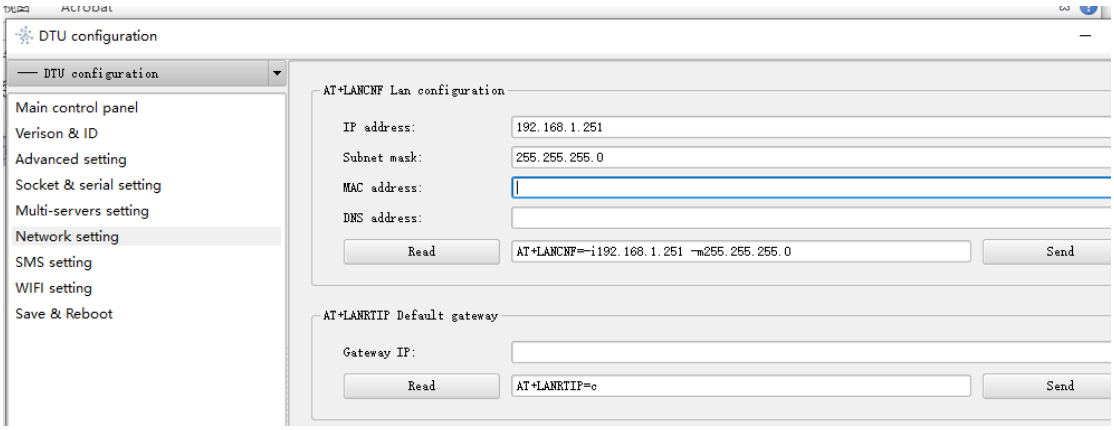
Network MASK: 255.255.255.0

Network Name and Network Password: Configure according to the relevant settings of the VPN-HUB software.

- If connecting to the COMWAY VPN SERVER, contact Tontony Innovation Technical Support to obtain these credentials.

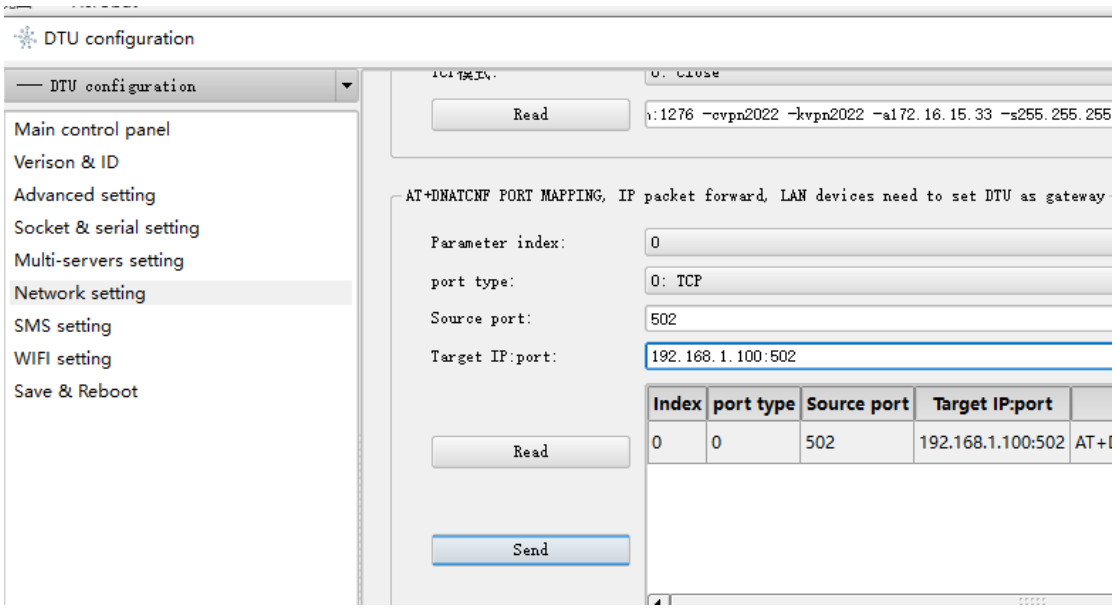
2) Set the LAN address of 4G DTU

Double click on "Network Port Communication Configuration" to set the IP address of the 4G DTU LAN to be in the same network segment as the IP address of the connected network port device, as shown below.



3) Set port mapping for 4G DTUs

As shown in the figure below, add a **port mapping** on the **Ethernet Communication Configuration** page of the DTU.



When accessing an internal network device from the external network via a DTU, **port mapping** must be configured. A maximum of 16 port mappings can be set.

- **Source Port Number**: Refers to the communication port accessible from the external network.
- **Destination IP Address**: The internal network IP address of the device connected to the DTU.
- **Destination Port**: The communication port of the internal network device.

In the **Configuration Software-2021**, parameters must be entered in the format of **[Destination IP Address]:[Destination Port Number]**.

Example: 192.168.1.55:102

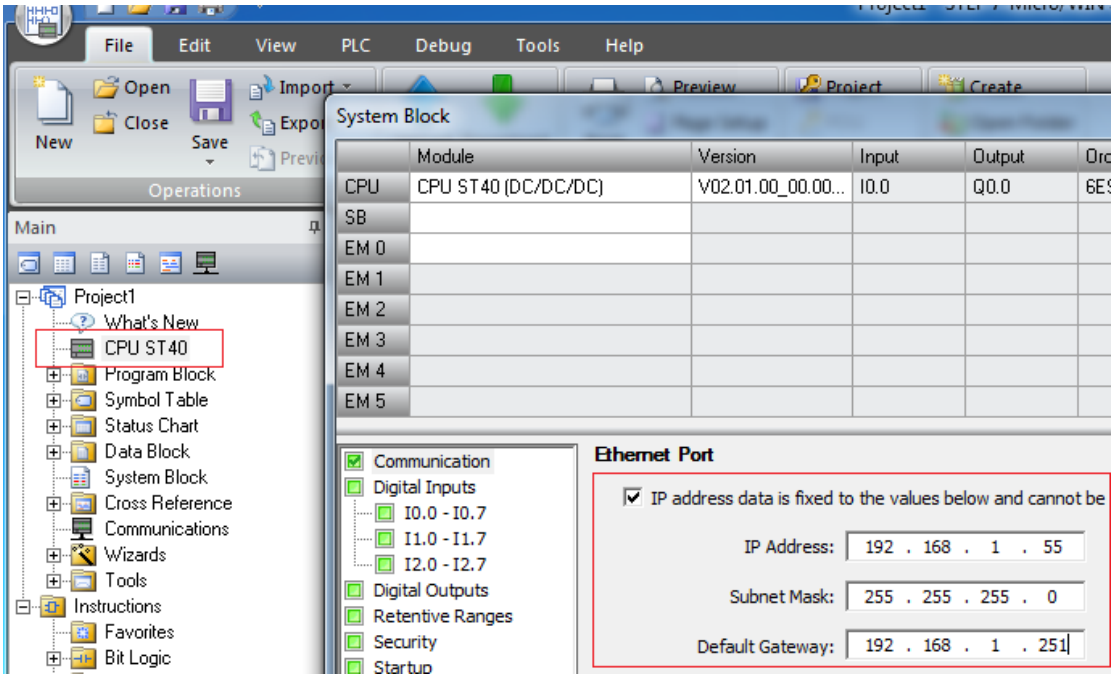
Example: The communication port of the S7-200 Smart PLC is 102. Therefore, as shown in the figure above, set the **Source Port Number** to 102, the **Destination IP Address** to the IP address of the PLC's LAN port, and the **Destination Port** to 102 as well. After completing the entries, click **Write** to save the parameters to the DTU. You can then access the S7-200 PLC in the internal network from the external network through the DTU.

5. Remote Download of PLC Programs

Taking the Siemens S7-200 SMART PLC as an example, first, install the VPN-HUB or DC-VPN software on the computer side to enable the computer to join the VPN network.

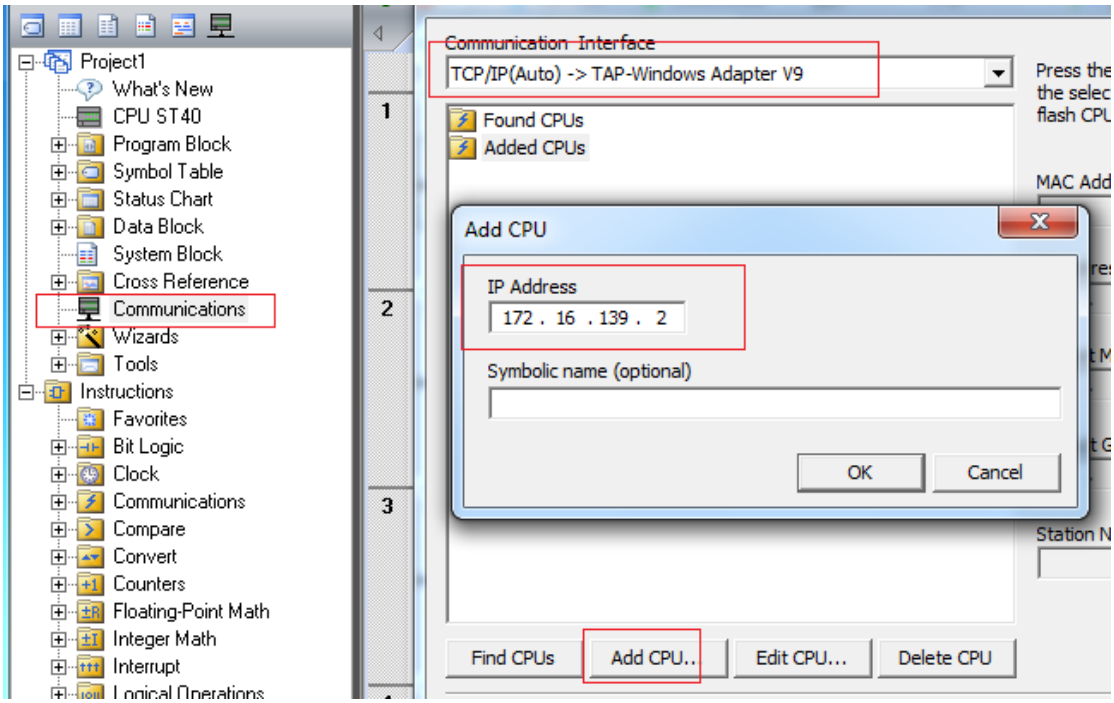
1) Configure the network parameters of the PLC

As shown in the figure below, configure the IP address of the PLC. This address must be in the same network segment as the DTU, and the IP address of the DTU's LAN port shall be used as the gateway address.

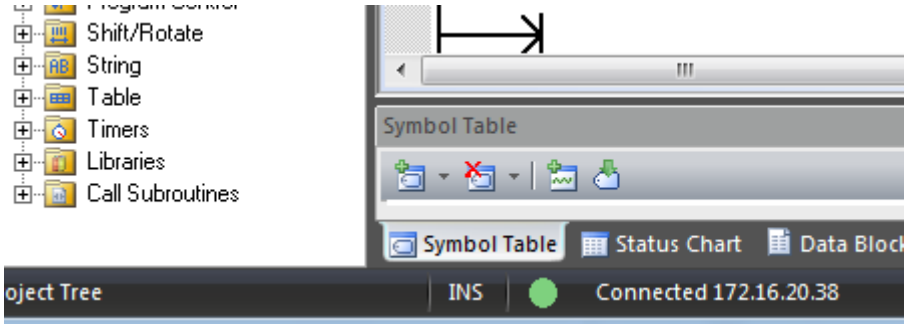


2) Add the CPU in the PLC Programming Software

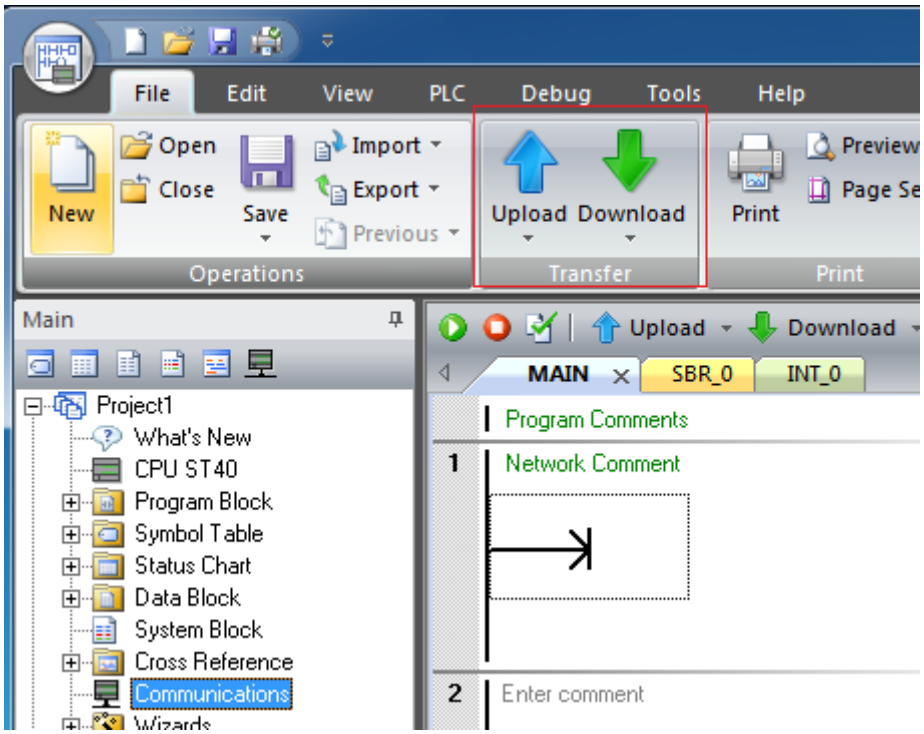
Launch the STEP 7 PLC programming software to add a PLC. As shown in the figure below, perform the following operations: click Communication → select the virtual network adapter (TAP-WINDOWS ADAPTER V9 TCPIP.1) → then complete the PLC addition either by searching for it or adding it manually.



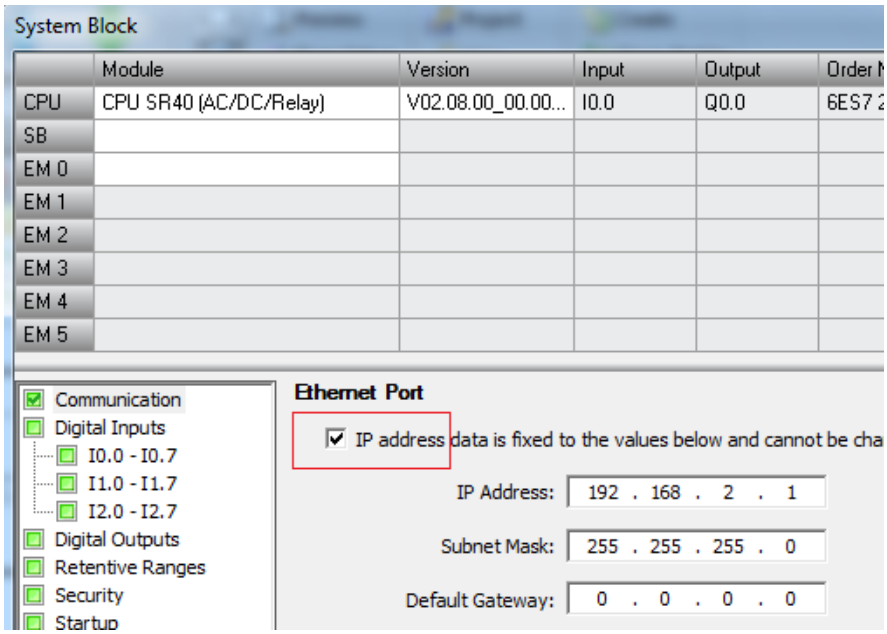
Once the VPN communication is established, the status bar of STEP 7 will display **Connected**.



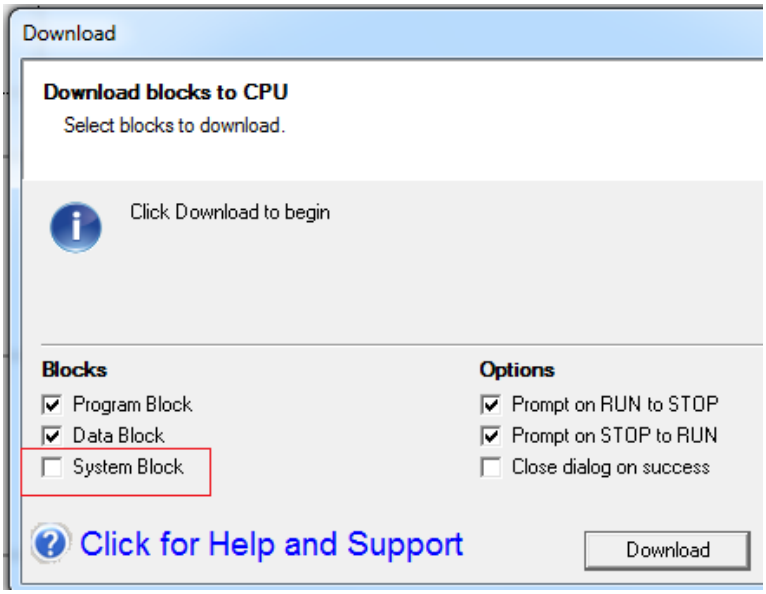
You can then click **Download** to implement the program download to the PLC.



It is particularly important to note that the following configuration **should not be checked** during the download process.



Alternatively, uncheck the System Block and then click Download.

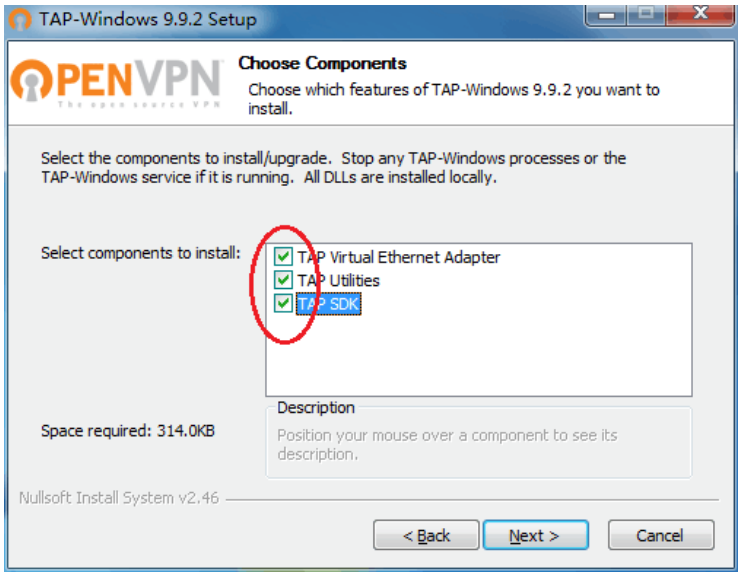


6. Establish a VPN Server

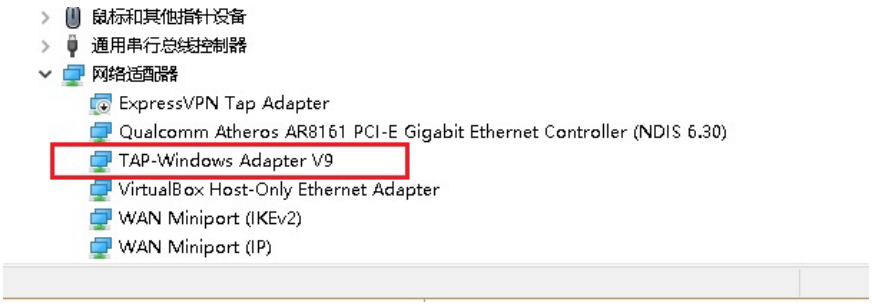
A VPN server is the core node of a VPN network. It must have either a fixed public IP address or a dynamic public IP address, and also be equipped with sufficient communication bandwidth (which depends on the specific communication requirements of the client; for example, real-time video streaming requires a relatively large bandwidth).

1) Install the virtual network adapter driver:

In the /tap-windows directory, double-click and run the tap-windows.exe program to install the virtual network adapter driver. In the interface shown in the figure below, make selections as indicated.



After the installation is completed, the content shown in the figure below will be displayed under **Network Adapters** in the **Device Manager** of the computer:



2) Configure port mapping on the cloud server or gateway router.

■ *Configure port mapping on the cloud server.*

A commonly used method is to rent a cloud server, such as Alibaba Cloud or Tencent Cloud. This solution can also be applied in the environment of an operator's APN private network.

The VPN server is mainly used for data relay, and has low requirements for CPU and storage resources. An Alibaba Cloud Elastic Compute Service (ECS) Lightweight Application Server is sufficient for normal operation.

On Alibaba Cloud: go to ECS Server > Security Group > Configure Rules > Manually Add Communication Ports. Note the port types: UDP and TCP.

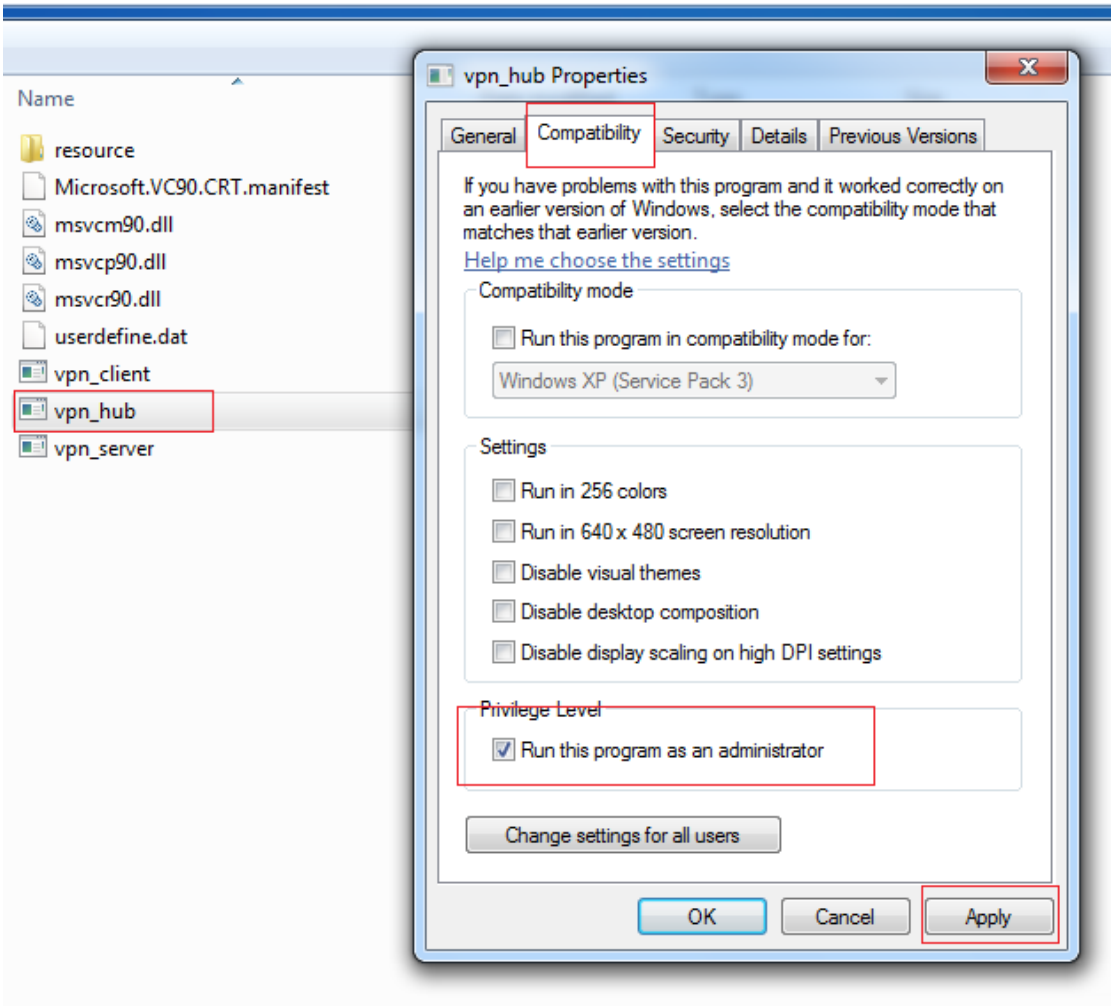
■ *Configure port mapping on the gateway router.*

If the user's router accesses the Internet via the operator's broadband connection and obtains a dynamic public IP address for its WAN port — as shown in the figure below (WAN port IP information of a China Unicom optical modem) — the user may apply for the DNS domain name provided by Comway Co., Ltd. to serve as the server address of the VPN-HUB.

The operation of port mapping is shown in the figure below: map the communication port to the **private IP address of the server (UDP protocol)**.

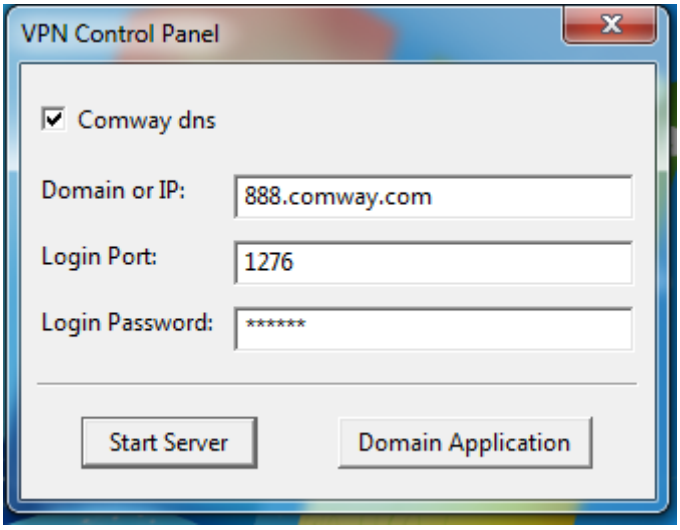
3) Configure the VPN-HUB software to run with administrator privileges.

As shown in the figure below, select the **vpn_hub.exe** file, then right-click it and navigate to **Properties > Compatibility > check the box for Run this program as an administrator**.



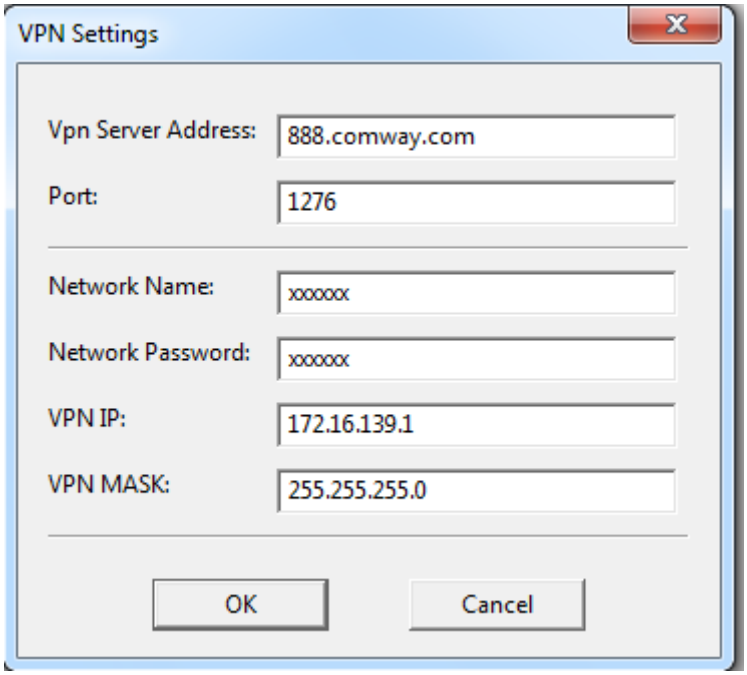
4) Run VPN_HUB

Running the **vpn_hub.exe** program will display the login interface as shown below. The figure below demonstrates the **DNS domain name mode**, where you need to enter the **DNS login password**. If you select the **fixed public IP mode**, directly enter the IP address and click **Start Server**.



5) Configure VPN parameters

Right-click on the blank area of the software to display the function menu. Click **"Configure VPN Parameters"** and the following menu will appear.



The **VPN network name and password** configured by the user on this page serve as the **security authentication method for accessing the VPN network**.

Set the **VPN IP address of the server**.

The VPN IP address must be a **private network IP address (to avoid conflicts with public network IP addresses)**. For example, it can be set to **172.16.139.1**.

The **VPN network segment must be completely different from the LAN network segment of the DTU**. For instance, if the LAN network segment is **192.168.1.x**, the VPN network segment can be **172.16.139.x**.

The setting of the **VPN subnet mask determines the maximum number of devices that can join this VPN network**. As shown in the figure, the maximum number of devices is **255**; if the subnet mask is set to **255.255.0.0**, then a maximum of **255 x 255 devices** can join this VPN network.

For the convenience of **automatic startup after booting**, you can check the boxes for **"Auto-Login on Startup"** and **"Start with System"** in the function menu.