

## **GREENTEL PLC Remote Maintenance and Diagnose**

### ***Case Study***

For R200 M2M Industrial Cellular VPN Router

## 1. Introduction

This document explains how to remote maintain and diagnose Siemens Simatic S7-1200 PLC through 3G HSPA networks.

We can also introduce the same solution to other similar applications, such as PLCs, Robotics, and Other Machines.



Picture: Siemens Simatic S7-1200 PLC

## 2. Service Benefits

- Deploy wherever there is wireless coverage and no Land Lines connectivity
- Reduced communication costs
- Quick and easy deployment with existing IP infrastructure
- Remote maintenance and diagnose at anytime, anyplace such as in office, at home and on business trip
- Enhanced security via IPsec VPN

## 3. Solution

Remote maintenance and diagnose become more and more important in automation networking field.

Remote maintenance and diagnose has low cost than traditional on site diagnose, engineer can diagnose the PLC remotely at any place and anytime via cellular networks.

### Application Diagram: Use R200 as primary link

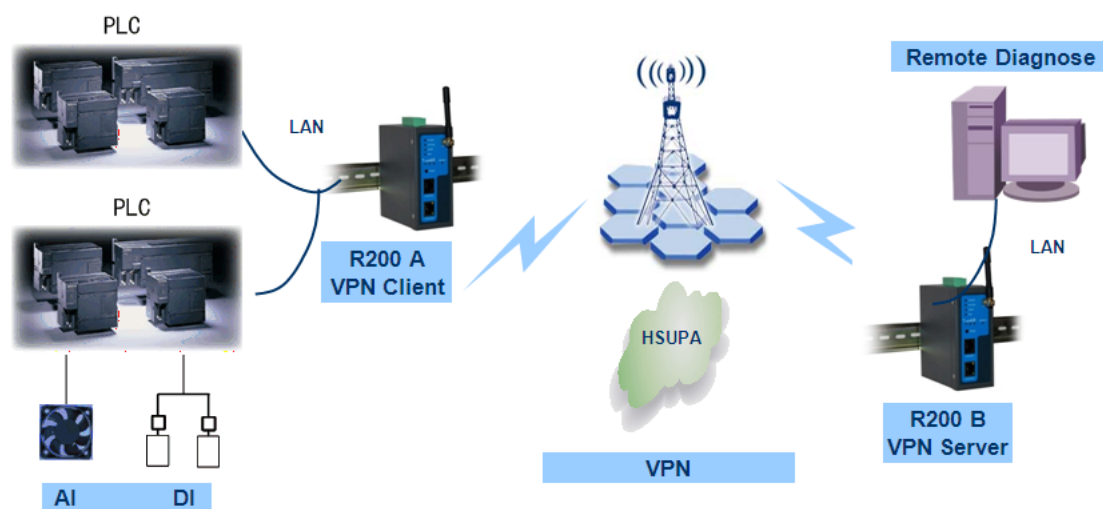


Diagram introduction:

1. R200 A connects to PLC via LAN port, work as VPN IPsec client
2. R200 B connects to PLC via LAN port, work as VPN IPsec server
3. R214 has 4 Ethernet ports, could connect to up to 4 PLCs and IP Camera
4. R200 work in 3G HSPA networks

Hardware requirement:

1. PC/PG programmer
2. Two units R200 routers
3. Two SIM cards
4. S7-1214C CPU (6ES7 214 -1BE30 -0XB0)

Software requirement:

1. Programming software: Step7 Basic V10.5 (6ES7 822-0AA0-0YA0)

## 4. R200 Series Benefits

1. Supports GSM/GPRS/EDGE/HSPA
2. Always online by built-in mechanisms to restore cellular connectivity: PPP LCP echo and ICMP keep alive for link inspection, watchdog
3. Front panel LED indicators, easy for diagnose
4. Supports IPSEC, PPTP, L2TP, OpenVPN VPN, VPN IPsec supports DES, 3DES, AES, MD5 and SHA-1 encryption, provides high security
5. R214 has 4 Ethernet ports, could connect to up to 4 PLCs and IP Camera
6. Wide range temperature from -25 to 70 degree centigrade
7. Certification: CE 0197, R&TTE, FCC



## 5. S7-1200 Configuration

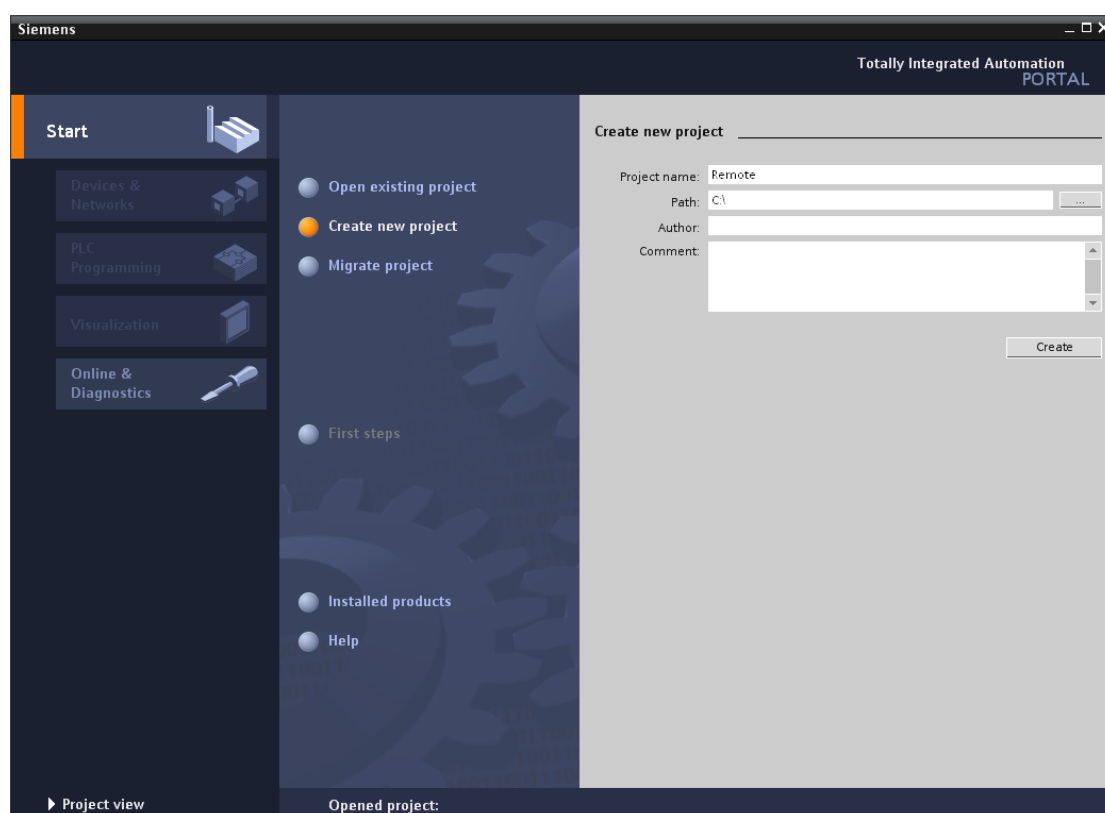
This paragraph explains how to remote maintenance and diagnose S7-1200 PLC.

Before remote maintenance and diagnose, engineer should operate as follow steps:

1. Read S7-1200's hardware component from configuration software.
2. Establish VPN IPSec tunnels between two R200 routers.
3. Remote read and configure S7-1200's settings via programming software.

### Create S7-200 Project

Click and open "Totally Integrated Automation Portal V10", you will see follow windows:

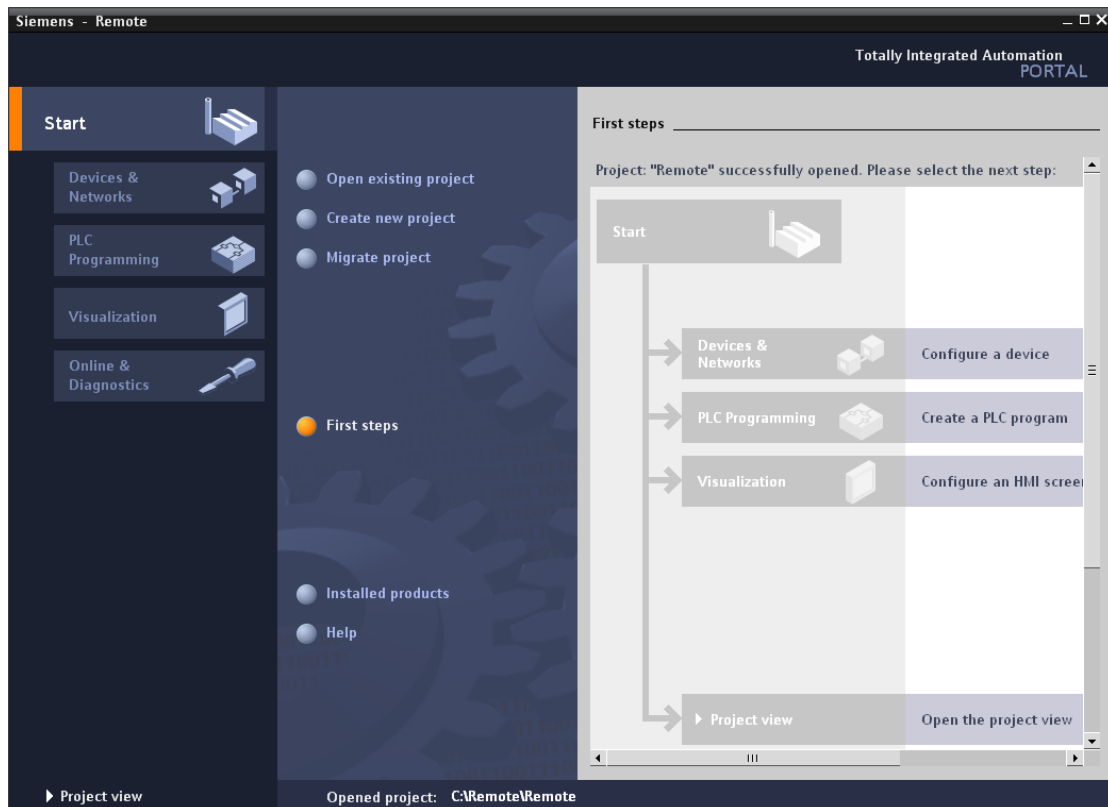


In "Portal View", select "Create new project", input "Remote" in "Project name:".

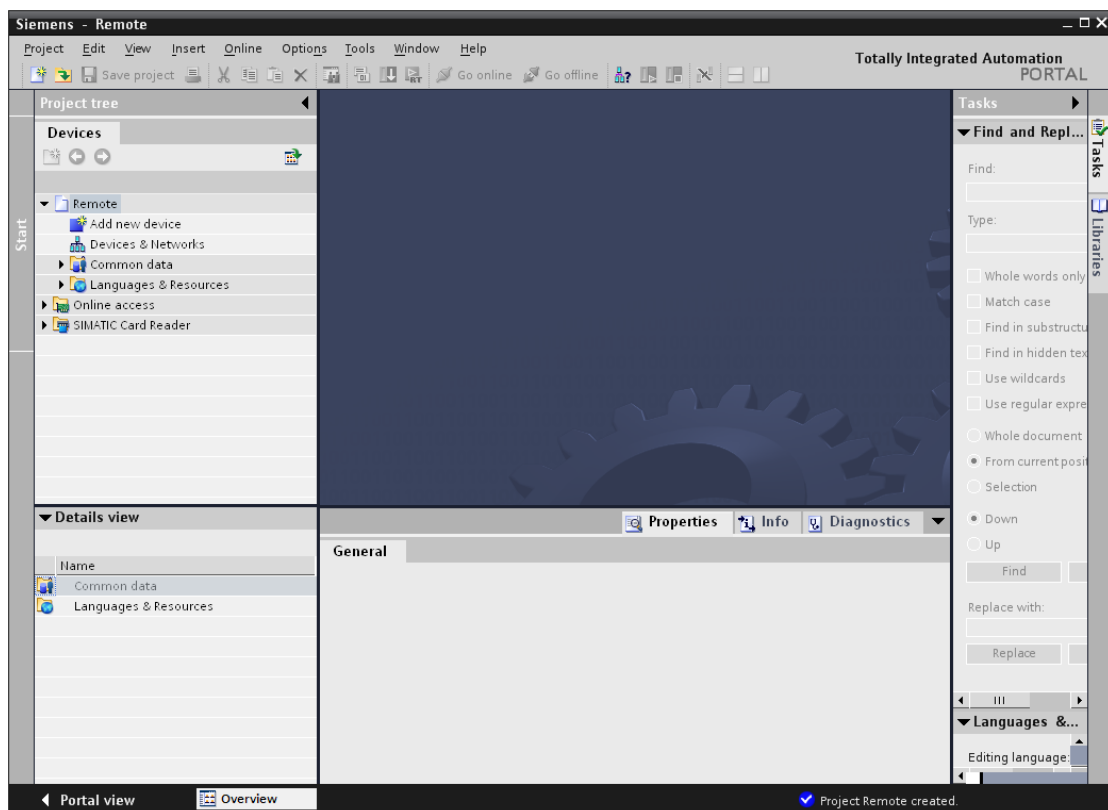
Input "C:\:" as "Path:", which is the path for saving project.

Click "Create", then a new project for remote maintenance has been done.

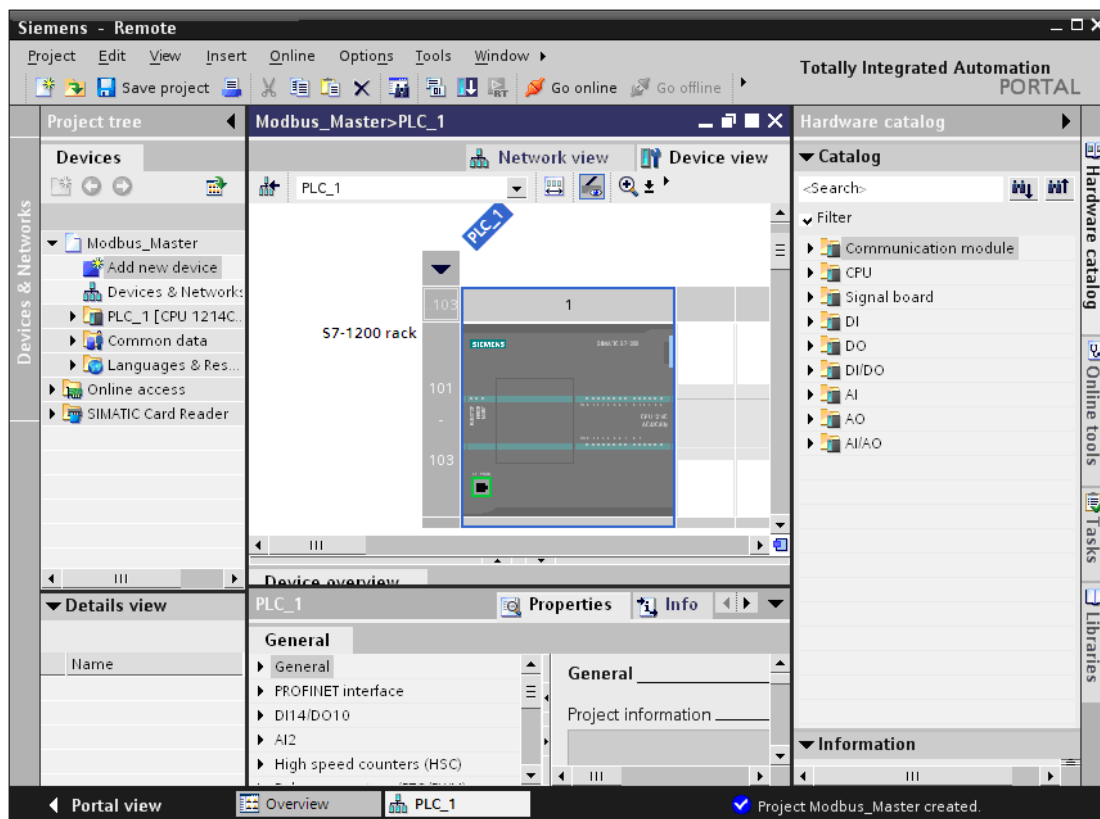
You will see follow windows after it:



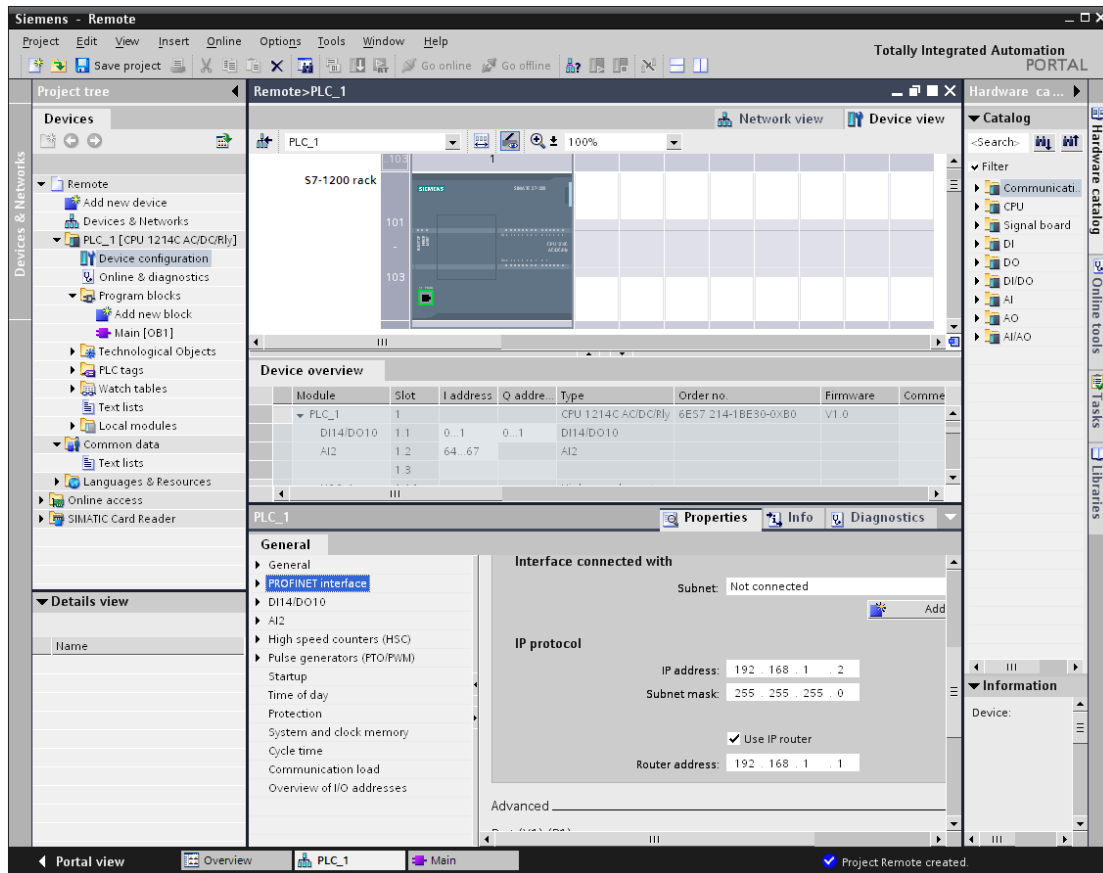
Click "Project view" in the "Portal view", you will see follow windows:



Click “Add new device” under “Devices”, input “PLC\_1” in popup menu, and select CPU type in “Devices”.

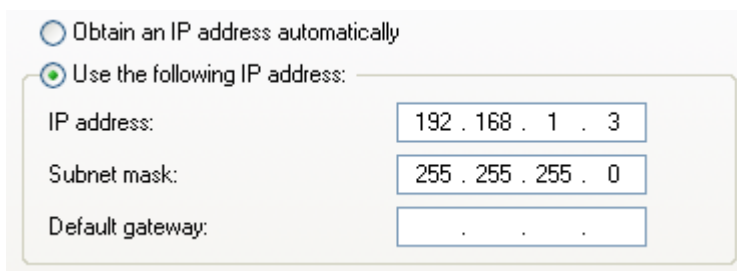


Select the “S7-1200” CPU, select “Profinet Interface” in “PLC\_1”.  
In “IP Protocol”, set “IP Address” as “192.168.1.2”, set “Subnet mask” as “255.255.255.0”.  
Select “Use IP router”, set “Router address” as 192.168.1.1.  
See follow windows:



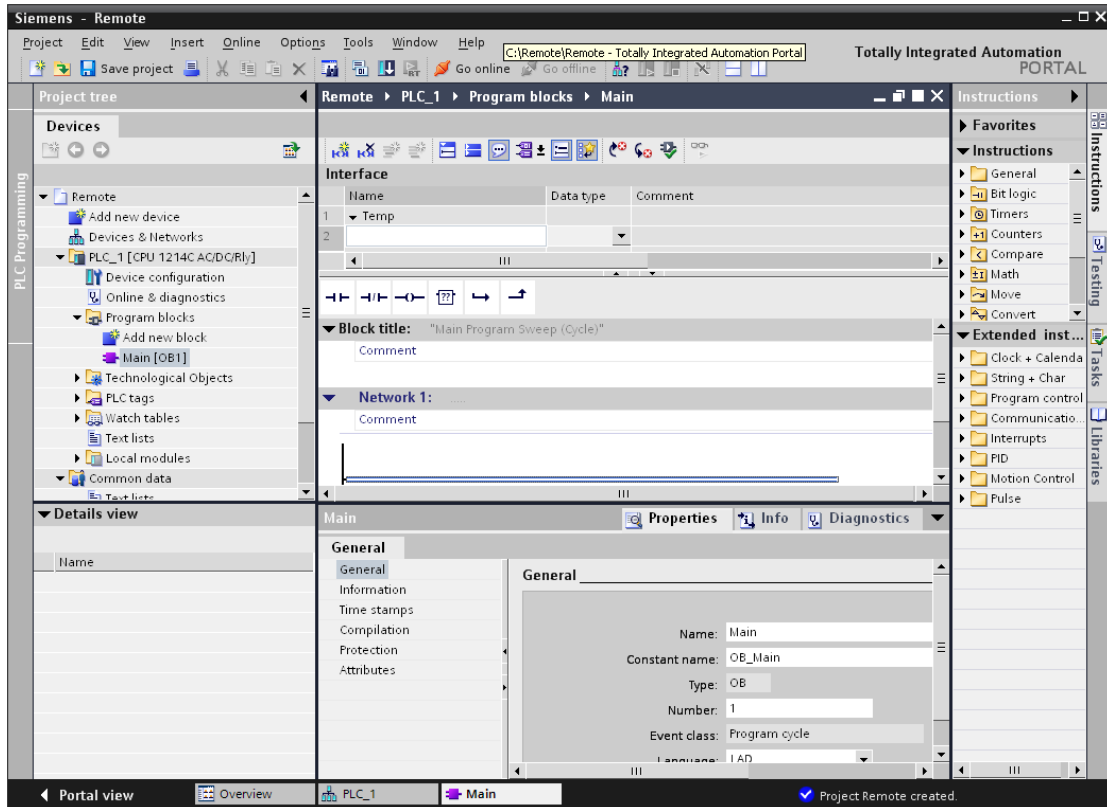
After configuration, connect S7-1200 to PC via LAN, set PC's IP as "192.168.1.3", subnet as "255.255.255.0".

See follow windows:

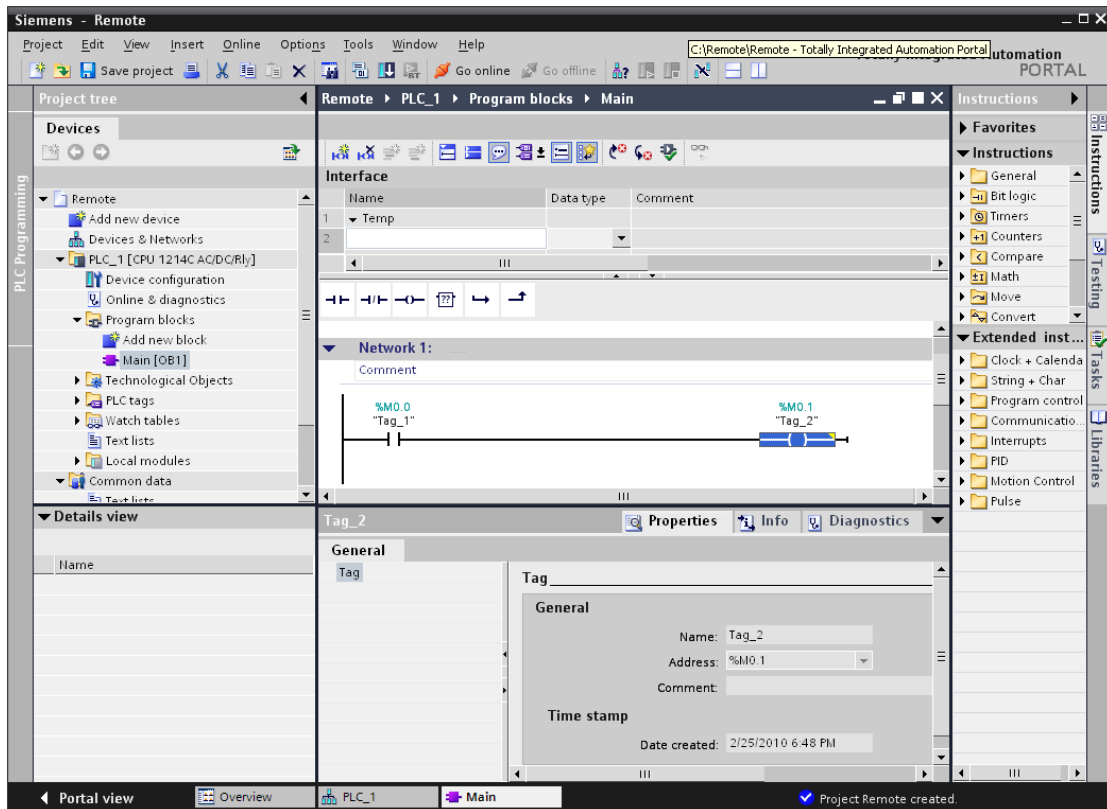


Program the PLC.

Click "Device-> Program block-> Main [OB1]" in "Project view", and engineer will see the popup windows as follow:

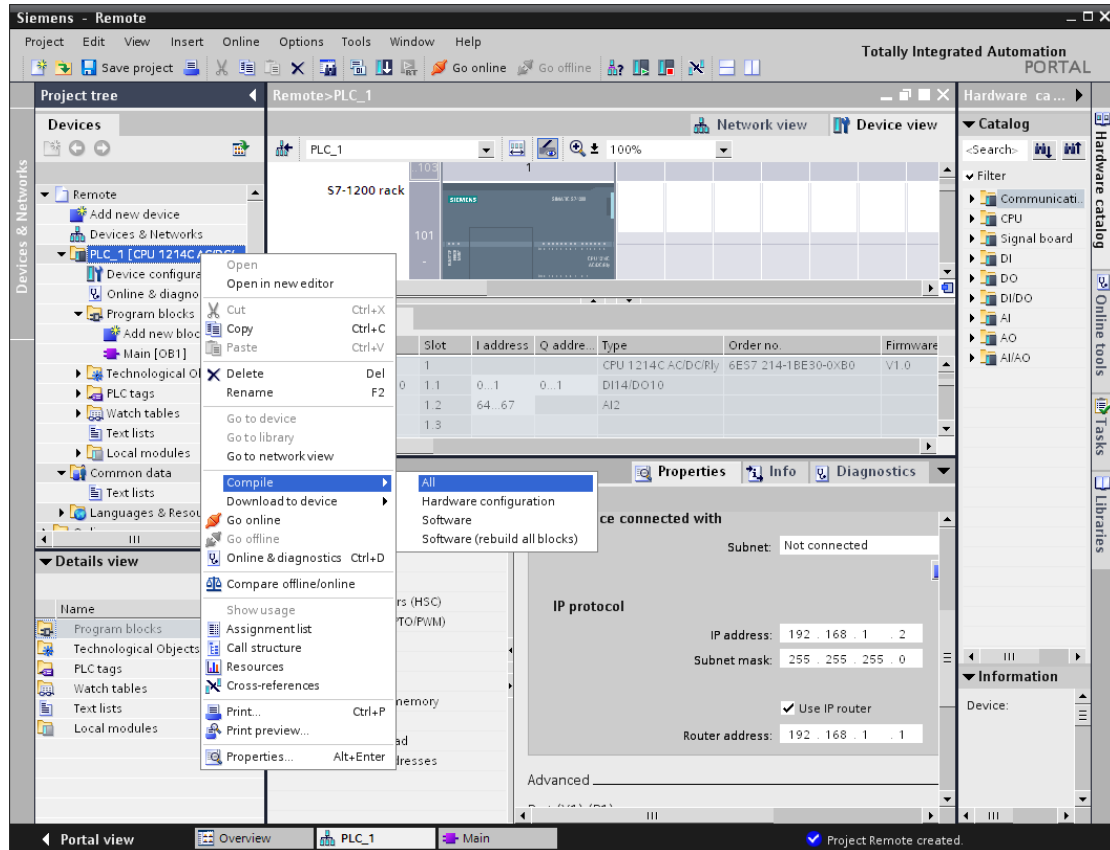


Add program in "Main-> NetWor1" as follow windows:



After finishing the programming, compile the program as follow:

Right click “PLC\_1”, select “Complies ALL” in popup windows to program both hardware and software. Engineer will see follow windows:



Download the program to the PLC if there is no error during compiling.

Right click “PLC\_1”, select “Download to Device” in popup windows.

After downloading, disconnect the LAN between S7-1200 and PC.

## 6. R200 Configuration

### R200 B VPN IPsec Server Configuration

#### LAN Configuration

Set PC's IP as "192.168.2.2", subnet as "255.255.255.0".

Connect PC to R200 B via LAN.

Click IE browser in PC, input R200 B's IP "192.168.2.1", username/password is "adm/123456".

Click "Network->LAN", you will see follow windows:

System	Network	Services	Firewall	QoS	VPN	Tools	Status
<b>LAN</b>							
MAC Address	<input type="text" value="00:04:25:00:9F:0A"/>		<input type="button" value="Default"/>				
IP Address	<input type="text" value="192.168.1.1"/>						
Netmask	<input type="text" value="255.255.255.0"/>						
MTU	Default <input type="text" value="1500"/>						
Detection host	<input type="text" value="0.0.0.0"/>						
LAN Mode	Auto Negotiation <input type="text"/>						
<b>Multi-IP Settings</b>							
IP Address	Netmask	Description					
<input type="text"/>	<input type="text"/>	<input type="text"/>					
							<input type="button" value="Add"/>
<input type="button" value="Apply"/>		<input type="button" value="Cancel"/>					

Set "IP Address" as "192.168.1.1" and click "Apply".

#### DDNS Configuration

Modify PC's IP as same network segment as R200 then login the R200 web page.

Select "Network->DDNS" as follow:

## DDNS

### Dynamic DNS ==> Dialup

Current Address

Service Type

URL

Username

Password

Hostname

Wildcard

MX

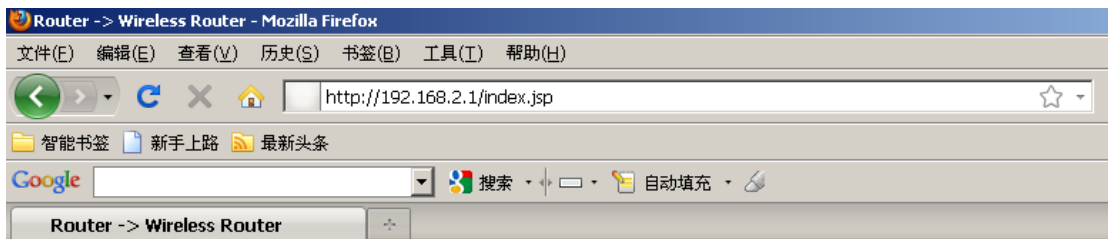
Backup MX

Force Update

Last Update -

Input your DDNS information.

### VPN IPSec Server Configuration (VPN->IPSec Tunnels->Add)



## Cellular Router

## IPSec Tunnels

### Edit IPSec tunnel

**Show Advanced Options**

**Basic Parameters**

Tunnel Name

Destination Address

Startup Modes

Restart WAN when failed

Negotiation Mode

IPSec Protocol

IPSec Mode

Tunnel Type

Local Subnet

Local Netmask

Remote Subnet	<input type="text" value="192.168.2.0"/>
Remote Netmask	<input type="text" value="255.255.255.0"/>
<b>Phase 1 Parameters</b>	
IKE Policy	<input type="text" value="3DES-MD5-DH2"/>
IKE Lifetime	<input type="text" value="86400"/> Seconds
Local ID Type	<input type="text" value="IP Address"/>
Remote ID Type	<input type="text" value="User FQDN"/>
Remote ID	<input type="text" value="client@siemens.com"/>
Authentication Type	<input type="text" value="Shared Key"/>
Key	<input type="text" value="*****"/>
<b>Phase 2 Parameters</b>	
IPSec Policy	<input type="text" value="3DES-MD5-96"/>
IPSec Lifetime	<input type="text" value="3600"/> Seconds
Perfect Forward Secrecy(PFS)	<input type="text" value="None"/>
<b>Link Detection Parameters</b>	
DPD Time Interval	<input type="text"/> Seconds (0: disable)
DPD Timeout	<input type="text"/> Seconds
ICMP Detection Server	<input type="text"/>
ICMP Detection Local IP	<input type="text"/>
ICMP Detection Interval	<input type="text" value="60"/> Seconds
ICMP Detection Timeout	<input type="text" value="5"/> Seconds
ICMP Detection Max Retries	<input type="text" value="10"/>
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

## R200 A VPN IPSec Client Configuration

### LAN Configuration

Click IE browser in PC, input R200 B's IP "192.168.2.1", username/password is "adm/123456".

Click "Network->LAN", you will see follow windows:

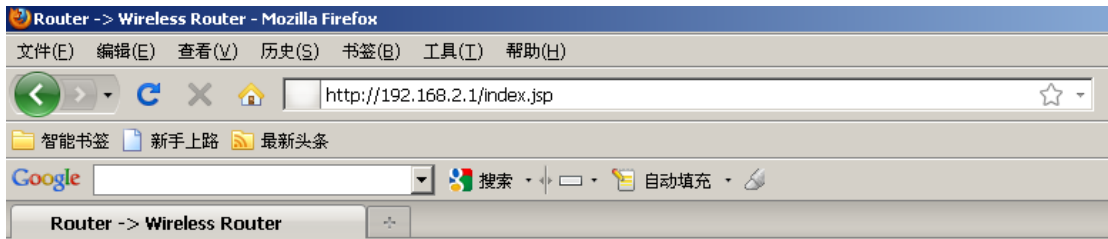
System	Network	Services	Firewall	QoS	VPN	Tools	Status
<b>LAN</b>							
MAC Address	<input type="text" value="00:04:25:00:7F:E8"/>	<input type="button" value="Default"/>					
IP Address	<input type="text" value="192.168.2.1"/>						
Netmask	<input type="text" value="255.255.255.0"/>						
MTU	<input type="text" value="Default"/> <input type="text" value="1500"/>						
Detection host	<input type="text" value="0.0.0.0"/>						

### Multi-IP Settings

IP Address	Netmask	Description
<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="button" value="Add"/>		

Set "IP Address" as "192.168.2.1" and click "Apply".

## VPN IPSec Client Configuration (VPN->IPSec Tunnels->Add)



## Cellular Router

System	Network	Services	Firewall	QoS	VPN	Tools	Status
<b>IPSec Tunnels</b>							
<b>Edit IPSec tunnel</b>							
<b>Show Advanced Options</b> <input checked="" type="checkbox"/>							
<b>Basic Parameters</b>							
Tunnel Name	IPSec_tunnel_1						
Destination Address	R200 A's DDNS						
Startup Modes	Auto Activated						
Restart WAN when failed	<input checked="" type="checkbox"/>						
Negotiation Mode	Aggressive Mode						
IPSec Protocol	ESP						
IPSec Mode	Tunnel Mode						
Tunnel Type	Subnet - Subnet						
Local Subnet	192.168.2.0						
Local Netmask	255.255.255.0						
Remote Subnet	192.168.1.0						
Remote Netmask	255.255.255.0						
<b>Phase 1 Parameters</b>							
IKE Policy	3DES-MD5-DH2						
IKE Lifetime	86400 Seconds						
Local ID Type	User FQDN						
Local ID	client@siemens.com						
Remote ID Type	IP Address						
Authentication Type	Shared Key						
Key	●●●●●●						
<b>Phase 2 Parameters</b>							
IPSec Policy	3DES-MD5-96						
IPSec Lifetime	3600 Seconds						

Perfect Forward Serecy(PFS)

**Link Detection Parameters**

DPD Time Interval  Seconds(0: disable)

DPD Timeout  Seconds

ICMP Detection Server

ICMP Detection Local IP

ICMP Detection Interval  Seconds

ICMP Detection Timeout  Seconds

ICMP Detection Max Retries

---

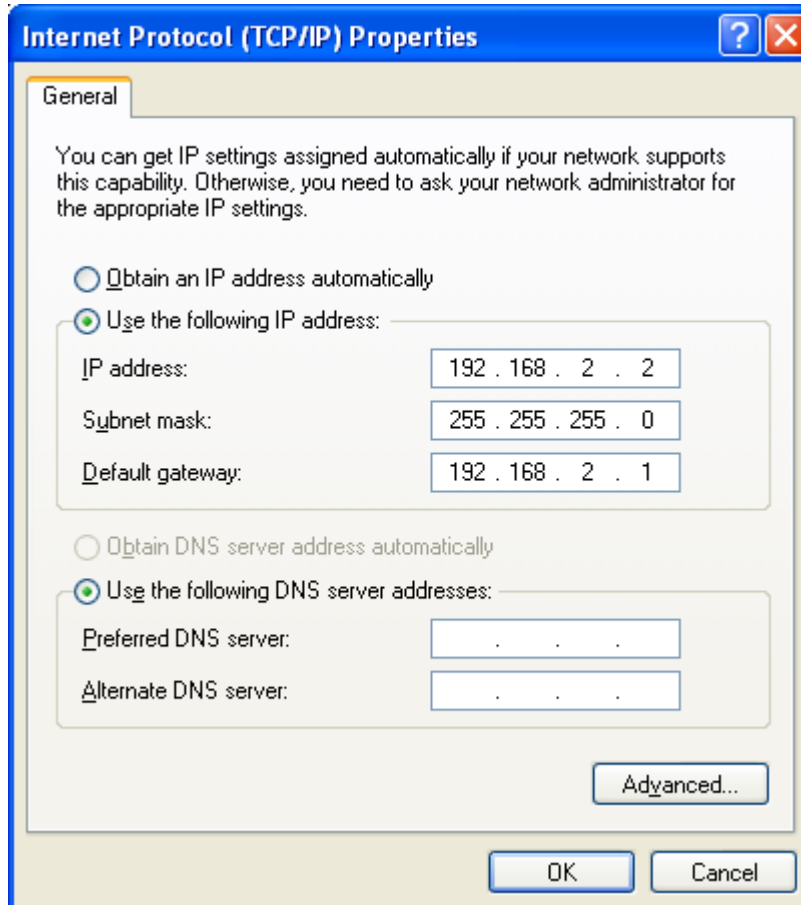
**Notice:**

Destination Address: input R200 B's IP Address or DDNS address, it is DDNS address in this case.

After configuring two R200 routers, restart the routers then they will establish a VPN IPSec tunnel automatically.

## 7. Remote Maintenance and Diagnose S7-1200

Connecting S7-1200 PLC to R200 B VPN IPsec Server, connecting remote diagnose PC to R200 A VPN IPsec Client, set PC's IP as "192.168.2.2", subnet as "255.255.255.0", gateway as "192.168.2.1". See follow windows:



Open "Remote" project which has been successful configured in "Totally Integrated Automation Portal V10". Then engineer could remote download and program the S7-1200.