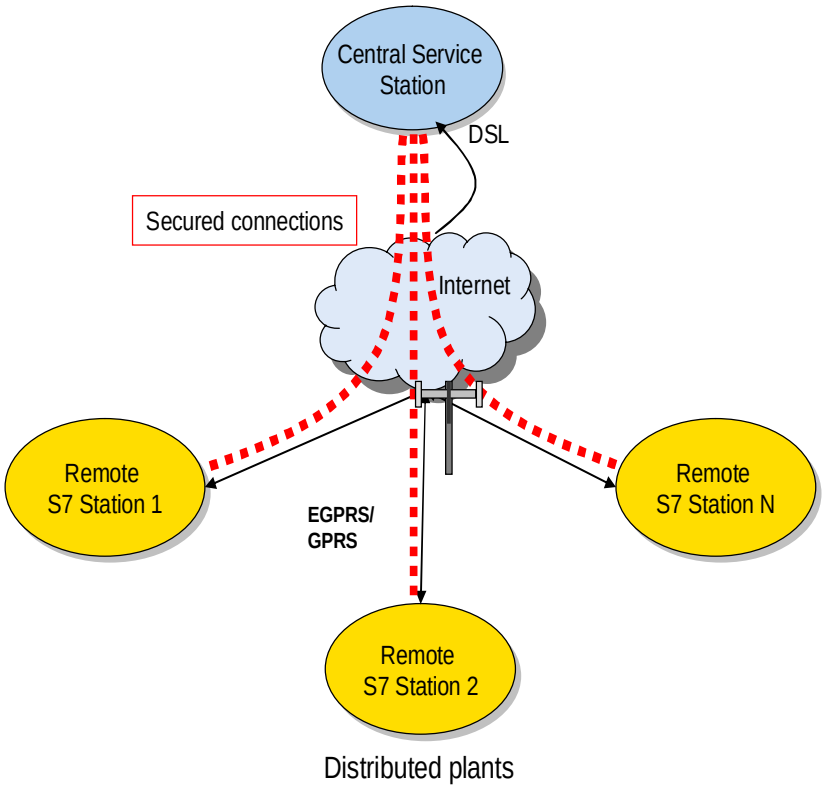
## 一、系统的概述

对生产设备的远程诊断和远程维护已经成为当前自动化技术中一部分。尤其是对于那些错误容易诊断且容易移除的情况，配一个服务工程师到现场解决，即增加工程师的工作负荷，由花费时间，而且相应的费用也增加。对于那些偏远的工厂或战争频发的的地区，利用当今的无线技术进行远程的维护，显然是一个即经济又有效的解决方案。

本文介绍的配置方案是通过安全的基于 EGPRS 或者基于 GPRS 的 internet 的连接对远程的分布的 S7 站进行访问。远程的 SIMATIC 站是通过 Ethernet 接口（S7-CPU, HMI 设备，以太网 CP 卡）通过无线的传输介质连接到中心服务站；中心服务站的 PG/PC 通过此连接可以执行基于有电缆连接的那些编程的功能（例如标准的诊断功能，上载和下载程序等）



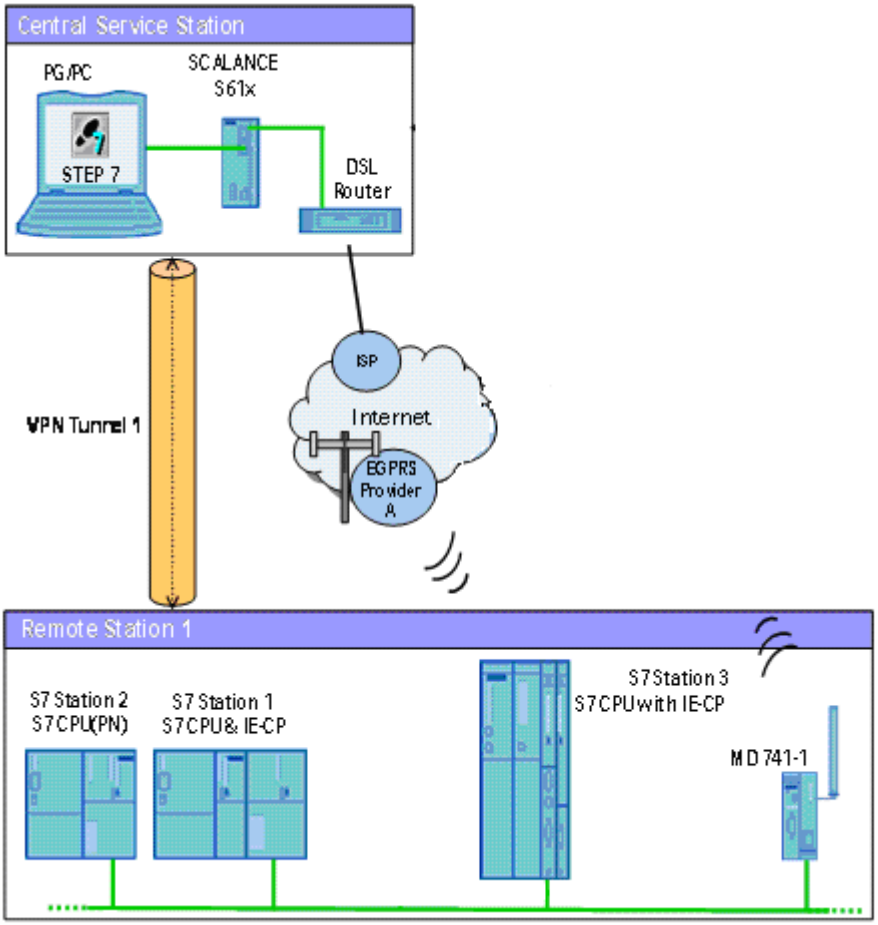

此方案的实现是由 SIMATIC 的主要部件 EGPRS 路由器 MD741-1 和中心站的安全模块 SCALANCE S612。

在这两个模块之间建立一个基于 IPSEC 的 VPN 隧道

中心站是通过 ADSL(宽带)连接到 internet

远程站是通过 EGPRS 或者 GPRS 连接到 internet

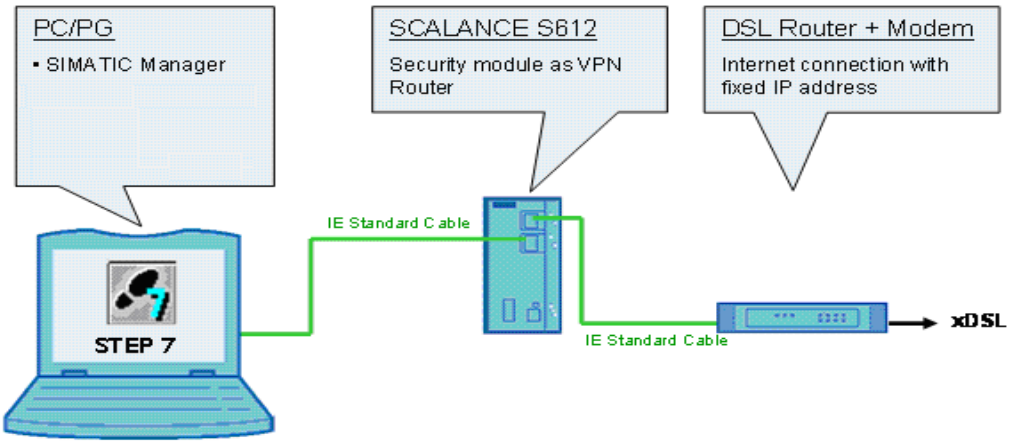
下图是实现此方案的配置的示意图：




## 二、安装

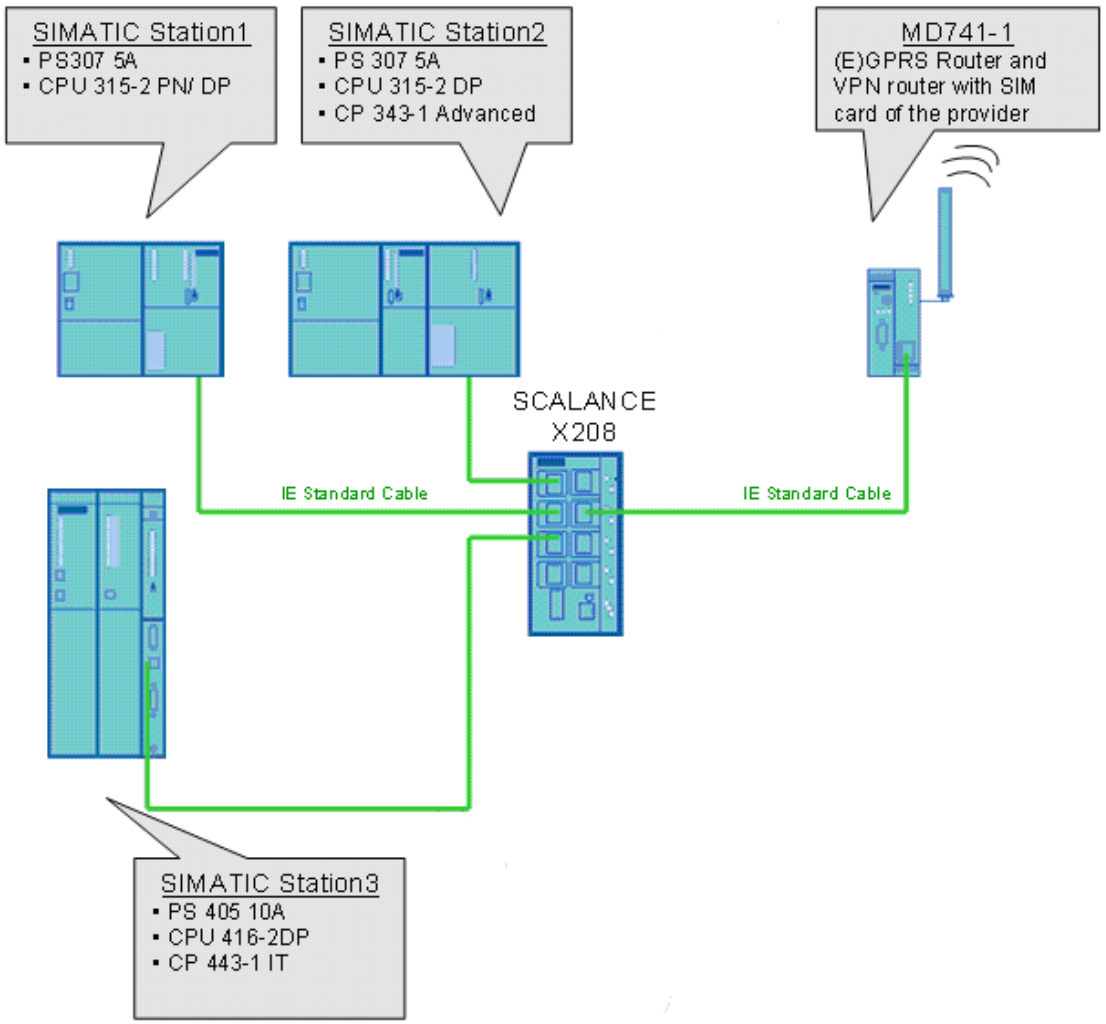
下面是各站的硬件安装示意图

**中心服务站**




中心站包含有标准的 PC/PG，通过 PC 的以太网接口连接到 SCALANCE S612 的内网口 port1,外网口连接路由器，路由器的 WAN 口连接 ADSL Modem。

**远程站**




远程包括了两个 SIMATIC S7-300 站、一个 SIMATIC S7-400 站、MD741-1EGPRS 路由器及以太网的连接部件 SCALANCE X208

## 三、需要的软件及硬件

### SIMATIC 部件

| Component | Qty. | MLFB / Order number | Note |
|---|---|---|---|
| CPU 315-2 DP | 2 | 6ES7315-2AG10-0AB0 | |
| CPU317-2 PN/DP | 1 | 6ES7317-2EJ10-0AB0 | |
| CP343-1 Advanced | 1 | 6GK7343-1GX21-0XE0 | |
| Power supply | 2 | 6ES7307-1EA00-0AA0 | |

| | | | |
|---|---|---|---|
| PS307 5A | | | |
| Micro Memory Card | 2 | 6ES7 953-8LF11-0AA0 | 至少 64 kB |
| PC | 1 | | |
| S7-400 UR2 Rack | 1 | 6ES7400-1JA00-0AA0 | |
| CPU 416-2DP | 1 | 6ES7416-2XK02-0AB0 | |
| CP 443-1 IT | 1 | 6GK7443-1GX11-0XE0 | 或者 CP 443-1 Advanced<br>6GK7 443-1GX20-0XE0 |
| Power supply<br>PS 405 10 A | 1 | 6ES7405-0KA00-0AA0 | |

安全部件及软件

| Component | No. | MLFB / Order number | Note |
|---|---|---|---|
| SCALANCE S612 **V2.1** | 1 | 6GK5612-0BA00-2AA3 | |
| Security Configuration Tool **V2.2** | 1 | - | SCT is delivered with SCALANCE S |
| EGPRS/GPRS router MD741-1 | 1 | 6NH9 741-1AA00 | |
| ANT 794-4MR | 1 | 6NH9860-1AA00 | |
| SIM card | 1 | | MD741-1 上 internet 需要 GSM SIM 卡并且激活了 EGPRS 功能 |

软件

| Component | Qty. | MLFB / Order number | Note |
|---|---|---|---|
| STEP 7 V5.4 SP1 | 1 | 6ES7810-4CC08-0YA5 | 或者更高 |

网络部件

| Component | Qty. | MLFB / Order number | Note |
|---|---|---|---|
| SCALANCE X208 | 1 | 6GK5208-0BA00-2AA3 | |
| RJ45 plug-in connector | 10 | 6GK1901-1BB10-2AA0 | 或者普通的以太网线 |

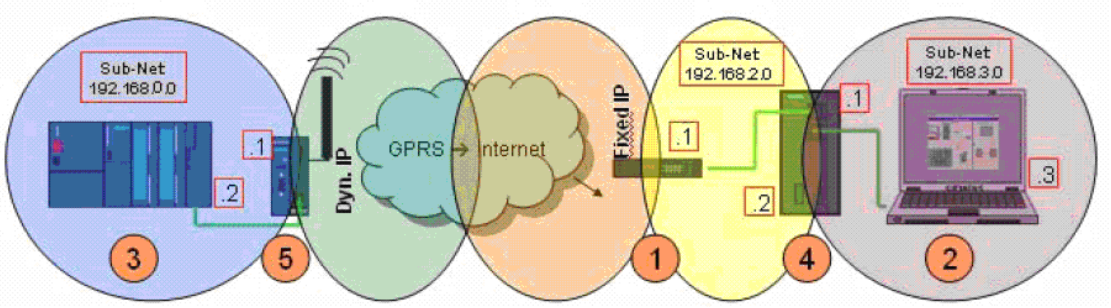
上 **internet** 所需部件

| Component | Qty. | MLFB / Order number | Note |
|---|---|---|---|
| ADSL Router + Modem<br>带有 VPN 穿越的功能(端口转发) | 1 | | 可选带有集成 Modem 的路由器或者独立的路由器和 Modem<br>例如：LINKSYS BEFSX41 |
| Internet 服务供应商 | 1 | | |

| | | | |
|---|---|---|---|
| 固定 IP 地址 | 1 | | 联系 Internet 服务供应商 |

## 四、VPN 的配置步骤

1、系统网络示意图，为了简化对于自动化单元这里只以一个 PLC 站为例介绍。其它 PLC 站的配置方法与此 PLC 站的配置类似。而且下图用标号来指示设置的步骤。




①、首先需要设置的是路由器：设定路由器上 Internet 获得公网的固定的 IP 地址，并设置路由器 VPN 的协议包可以通过，而且要设置路由器的端口转发机制，这样使的从外网发到路由器的 VPN 的数据包能够被转发到内网的 SCALANCE S612 的外网的端口上。

②、设置 PG/PC：在 PG/PC 上安装 STEP7 软件，并设置计算机的 IP 地址和 PLC 的 IP 地址在同一个网段上。

③、设置 PLC 站：用以太网线把 PG/PC 直接连接到 PLC 站，然后给 PLC 站分配 IP 地址，并对 PLC 站进行硬件组态，并下载程序。

④、配置 SCALANCE S612：首先需要把 PG/PC 上的以太网线插到 SCALANCE S612 的外网口，并把计算机的 IP 地址重新设置，地址应与 SCALANCE S612 在同一个网段上，然后用 SCALANCE S612 配置工具软件 Security Configuration Tool 对 SCALANCE S612 进行组态。

⑤、配置 MD741-1:设置 MD741-1 上 Internet 的所需的参数，并配置 VPN 的参数，使其能够与 SCALANCE S612 之间建立 VPN 的通讯。

详细的配置过程如下：

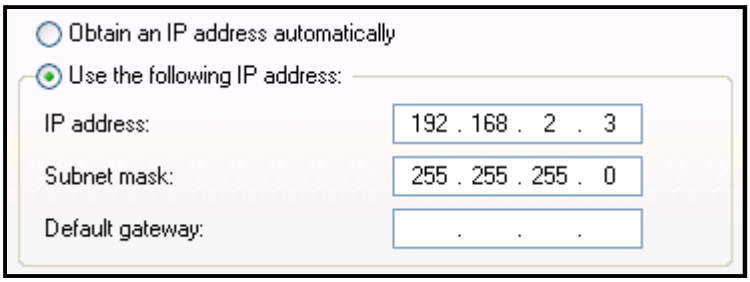
配置之前，先把 IP 的地址进行分配，如下表：

| | Module | IP address | |
|---|---|---|---|
| | | Internal | External |
| RMT 1 | CPU 317-2 PN/DP | 192.168.0.2 | |
| | MD741-1 | 192.168.0.1 | Dynamic from APN |

| | Module | IP address | |
|---|---|---|---|
| | | Internal | External |
| Central service station | ADSL Router | 192.168.2.1 | Fixed IP from provider |
| | SCALANCE S612 | 192.168.3.1 | 192.168.2.2 |
| | PC/ PG | 192.168.3.3 | |

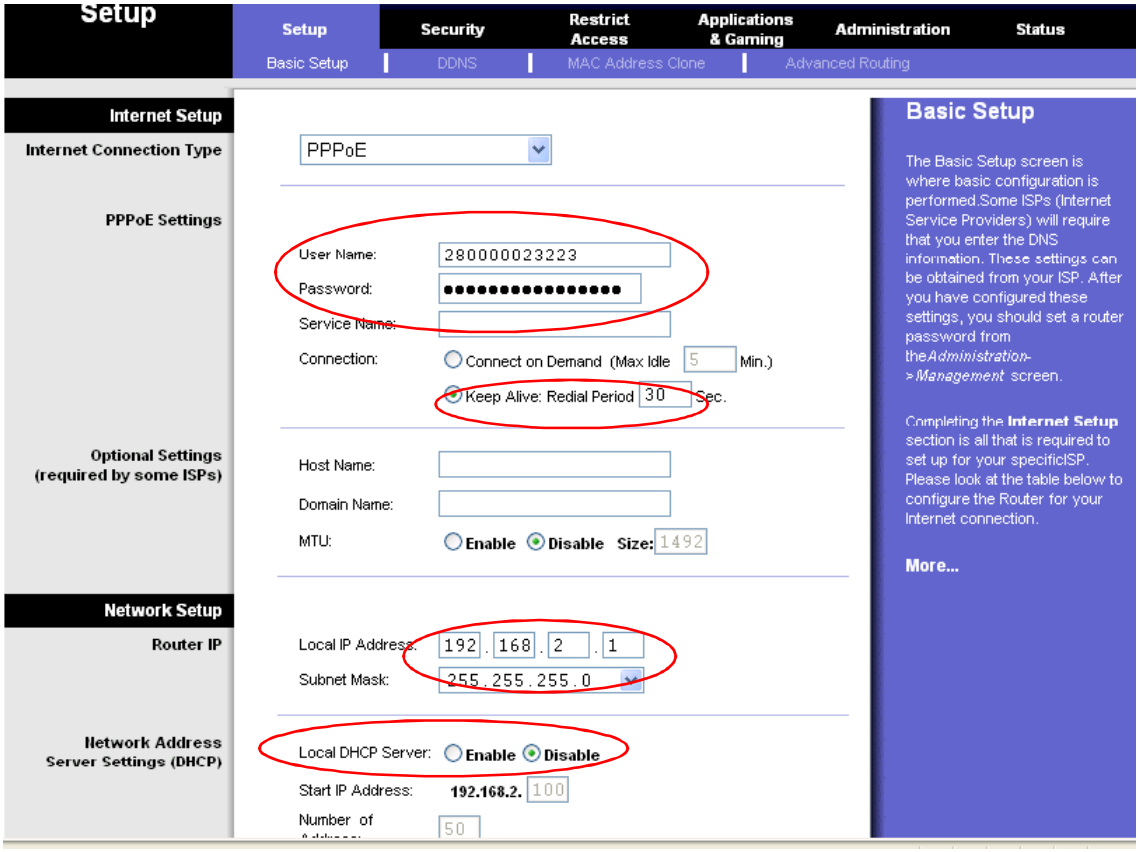
①、设置路由器：

在本文中我们选择了 Linksys 的一款型号为 BEFSX41 的路由器。为了配置路由器先设置计算机的 IP 地址为 192.168.2.3;子网掩码为 255.255.255.0。将网线连接至路由器的局域网口，在 IE 浏览器中输入路由器的的 IP 地址：192.168.2.1 ，键入用户名和密码（默认均为“admin”）即可进入路由器的配置界

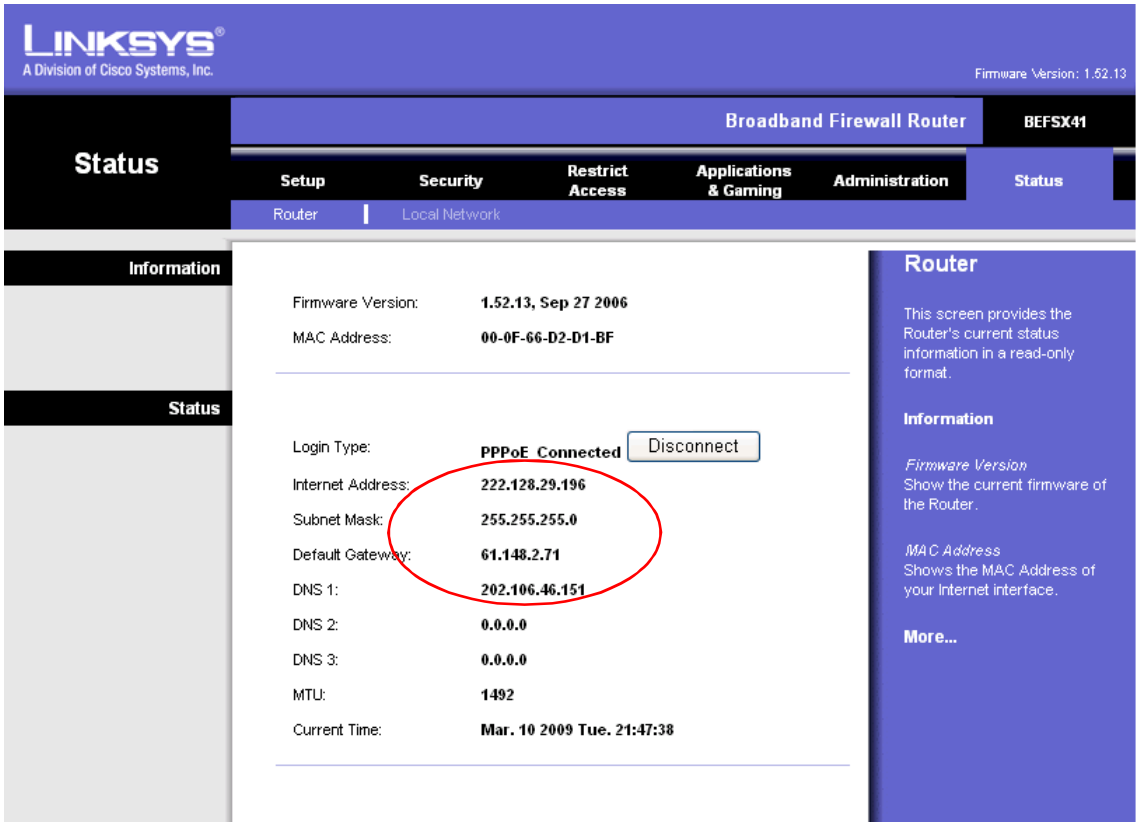




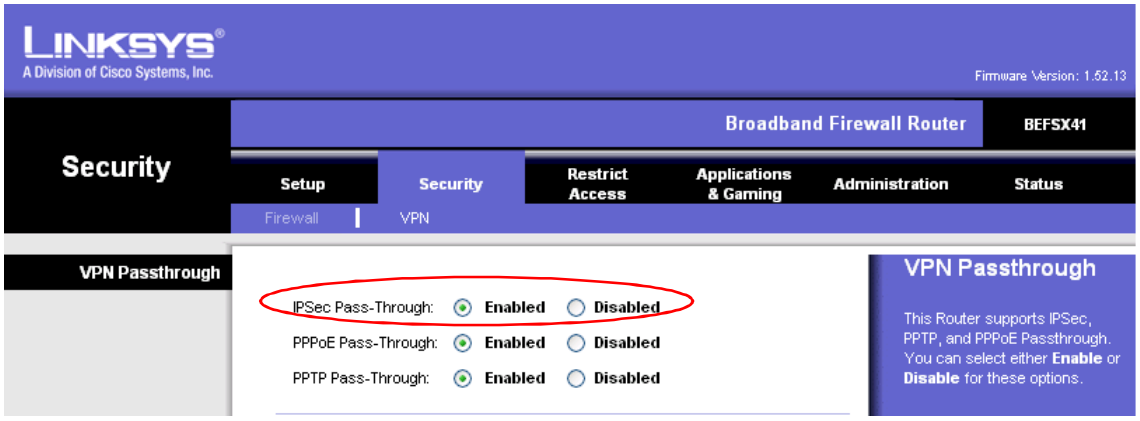
在“Setup→Basic Setup→Internet”下，选择以太网连接类型：PPPoE ，用户名和密码是用户所申请的 ADSL 的用户名和密码，并且选择“Keep Alive”选项。这样，路由器即可自动通过 ADSL 的账户登陆互联网。通过“Local IP Address”可更改路由器的 IP 地址，这里是 192.168.2.1 与我们分配的 IP 地址一致，所以不需要更改。而且在这里我们不使能“Local DHCP Server”。 设置完成后注意“Save Setting”如下图：



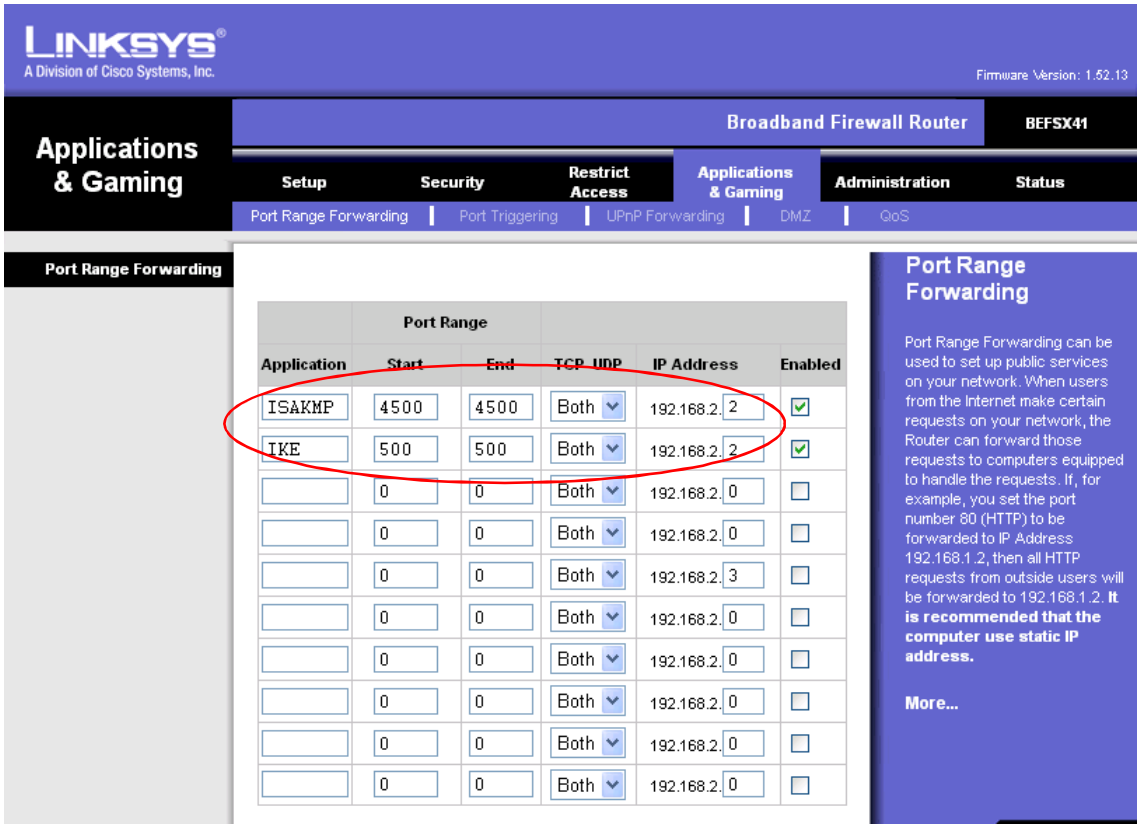

保存了上面的设置后，查看一下路由器是否正常登陆到 Internet，若登陆正常，就会从网络服务供应商那里获得一公网的 IP 地址（这里我们需要公网的固定 IP 地址，这个 IP 地址需要在 MD741-1 中设置，使 MD741-1 向此 IP 地址的设备发起 VPN 的连接请求，若是动态 IP 地址，那么当路由的地址发生了变化，就需要重新对 MD741-1 及 SCALANCE S612 组态）。查看此路由器是否正常登陆到 Internet 的步骤是点击路由器配置页面上的“Status”选项，若正常登陆，就会在此页面中看到它获得的公网 IP 地址、子网掩码、网关地址、域名服务器的地址。如下图：




路由器正常登陆公网后，接下来需要配置一下对 VPN 协议数据包的处理，首先需要使能 VPN PASS-Through 的功能（即让 VPN 的数据包能够通过此路由器进入到内网中），选择“Security”下的“VPN”选项，然后在 IPSec Pass-Through 后选择“Enabled”选项。参数设置如下图：




为了让从外网上发到路由器的数据能进入到内网的 SCALANCE S612 的端口上，所以需要设置一下端口的转发机制:选择“Application & Gaming”下的“Port Range Forwarding”标签卡，在里面把发到路由器上端口为 4500 及 500 应用数据转发到 SCALANCE S612 的外网 IP 地址。



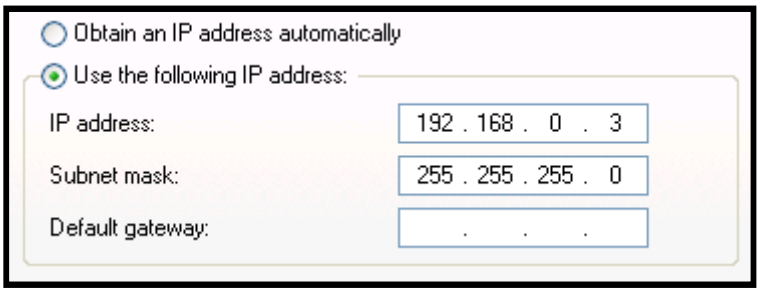

到此，我们就完成了对路由器的所有配置。

②、设置 PG/PC：

此步需要在计算机上安装 Step7 软件及 SCALANCE S612 的配置工具 Security Configuration Tool。具体的安装步骤我们在这里就不再作更详细的描述。

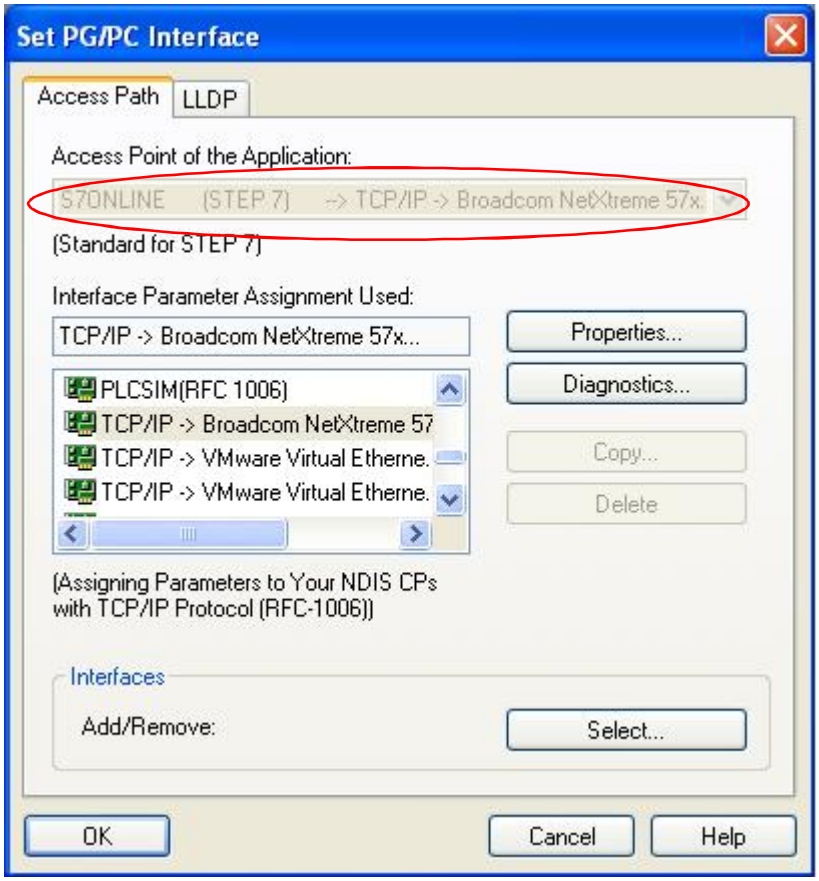
③、设置 PLC 站：

在配置 PLC 站前，首先需要把计算机的 IP 地址进行重新设置，这里我们给计算机分配的 IP 地址为 192.168.0.3,子网掩码为 255.255.255.0，与 IP 地址分配表中 PLC IP 地址 192.168.0.2 在同一个网段，如下图：

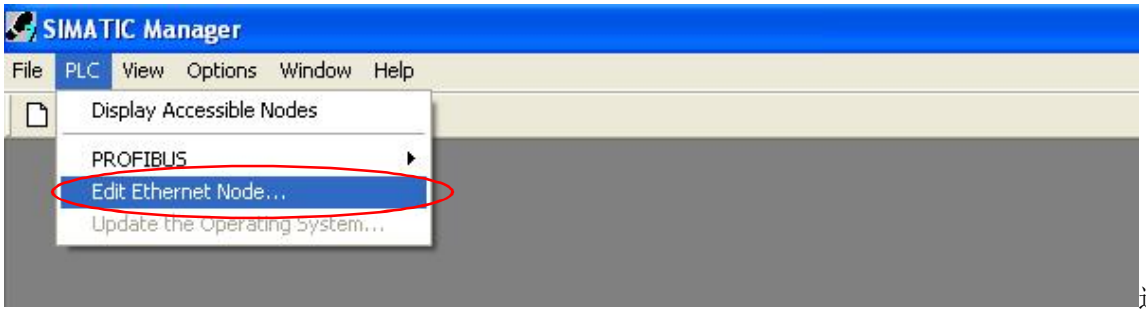



配置完计算机的 IP 地址后，就需要给 PLC 分配 IP 地址：

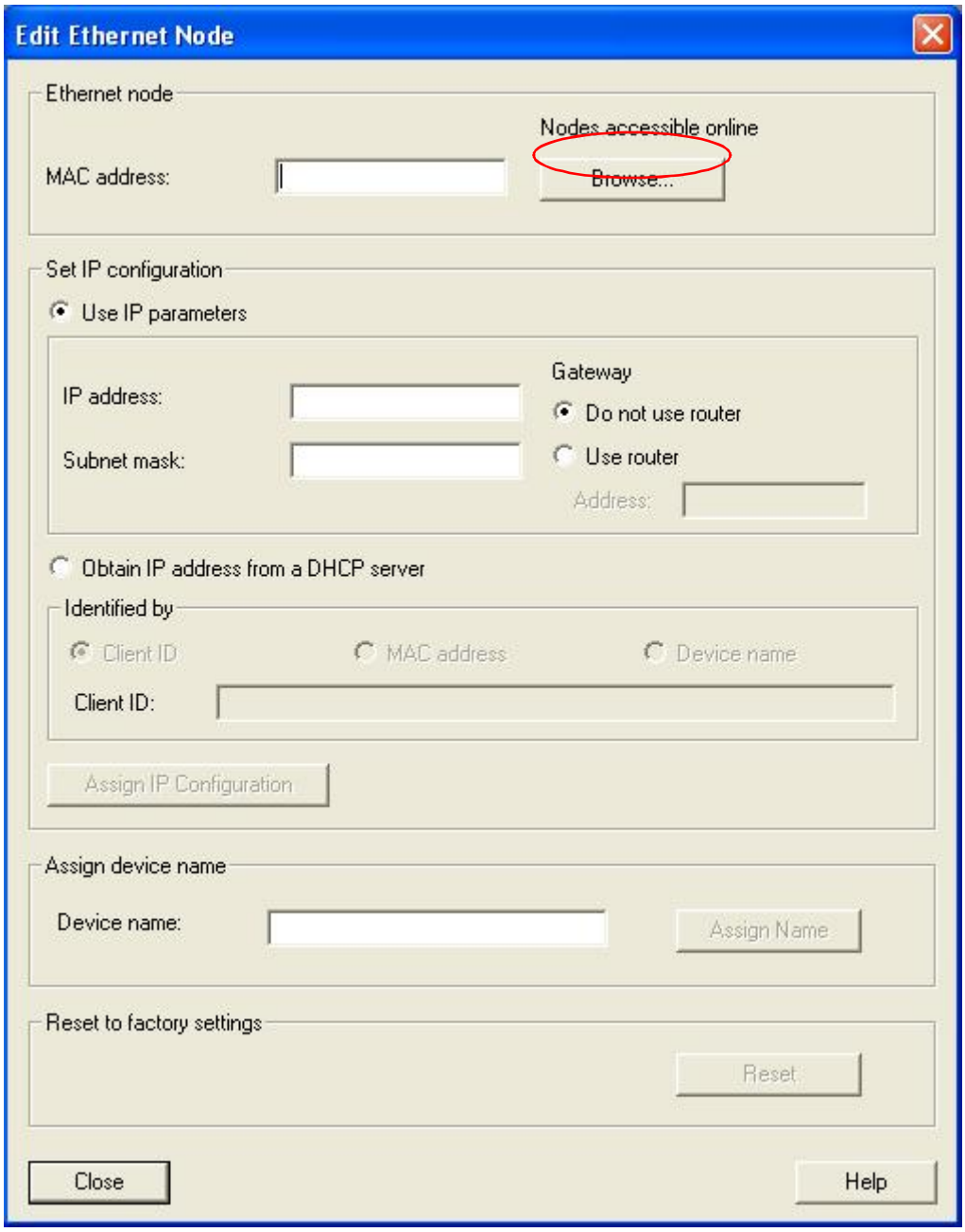
首先需要在控制面板的 SET PG/PC 里把编程接口修改为以太网的接口如下图



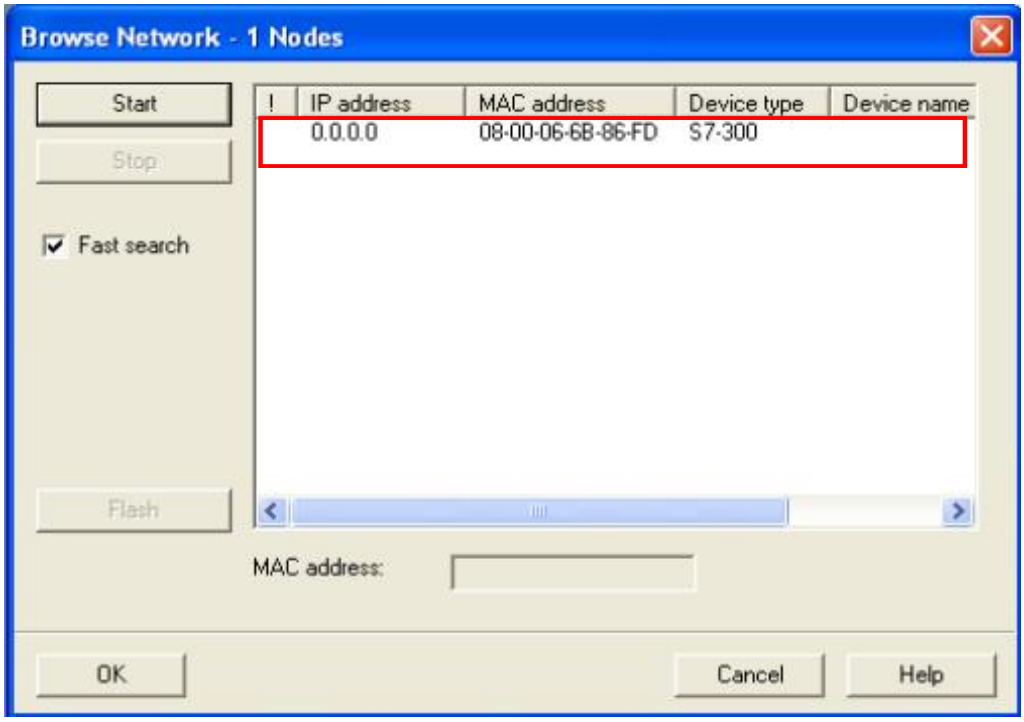

然后打开 SIMATIC Manager，在 **PLC** 的菜单下选择 **Edit Ethernet Node…**如下图：



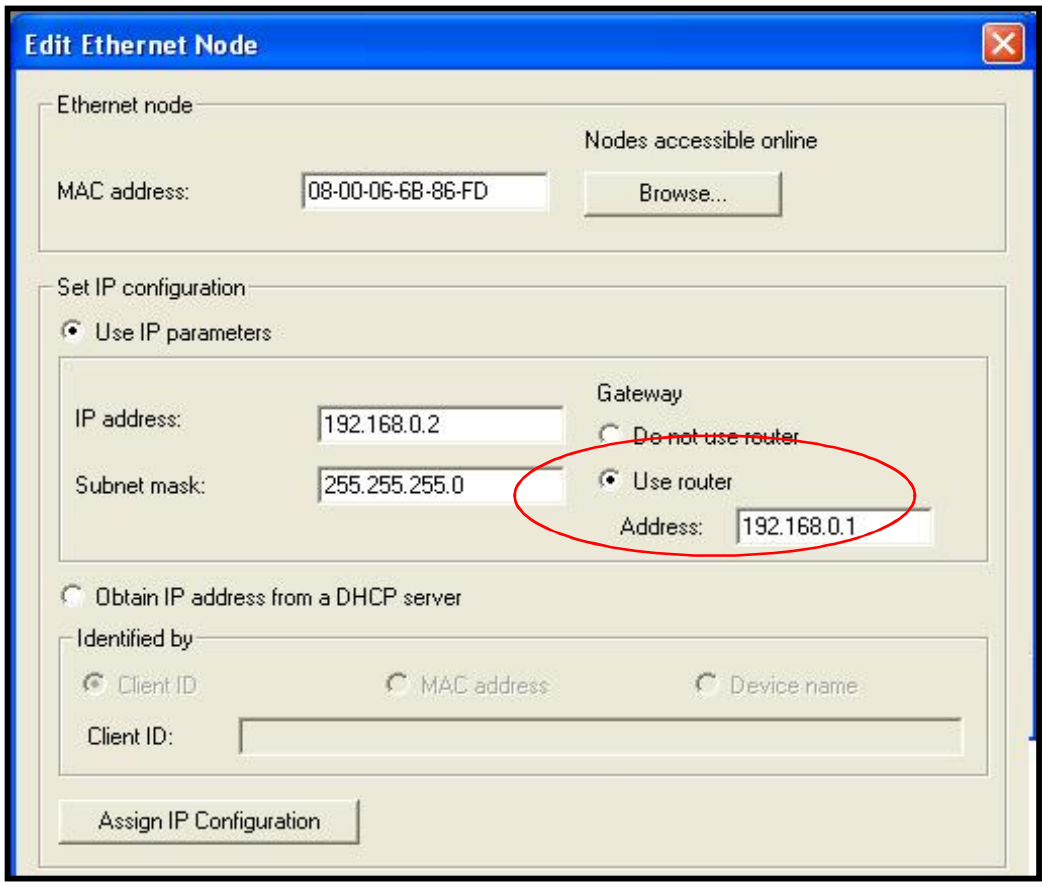
选择完 **Edit Ethernet Node…**后会弹出如下的窗口：



点击 **Browse..**进行对 PLC 的以太网接口的查找，如下图：




选择上面出现的以太网接口，点击 OK 按钮，设置 PLC 的 IP 地址如下，并且启用路由功能。



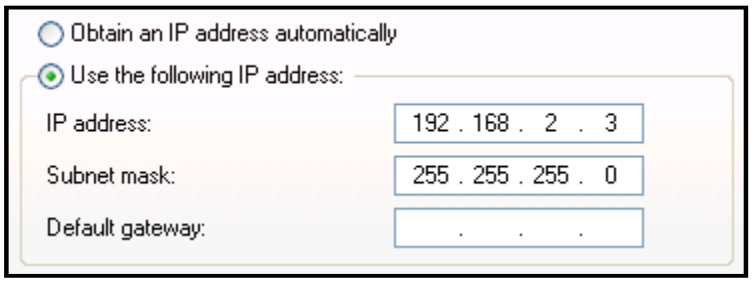

点击 **Assign IP Configuration** 按钮，这样完成了对 PLC IP 地址的设置。

然后在 **SIMATIC Manager** 里插入一个 300 站，在 300 站的硬件组态里插入机架及对应的型号的 300CPU，编译下载即可。

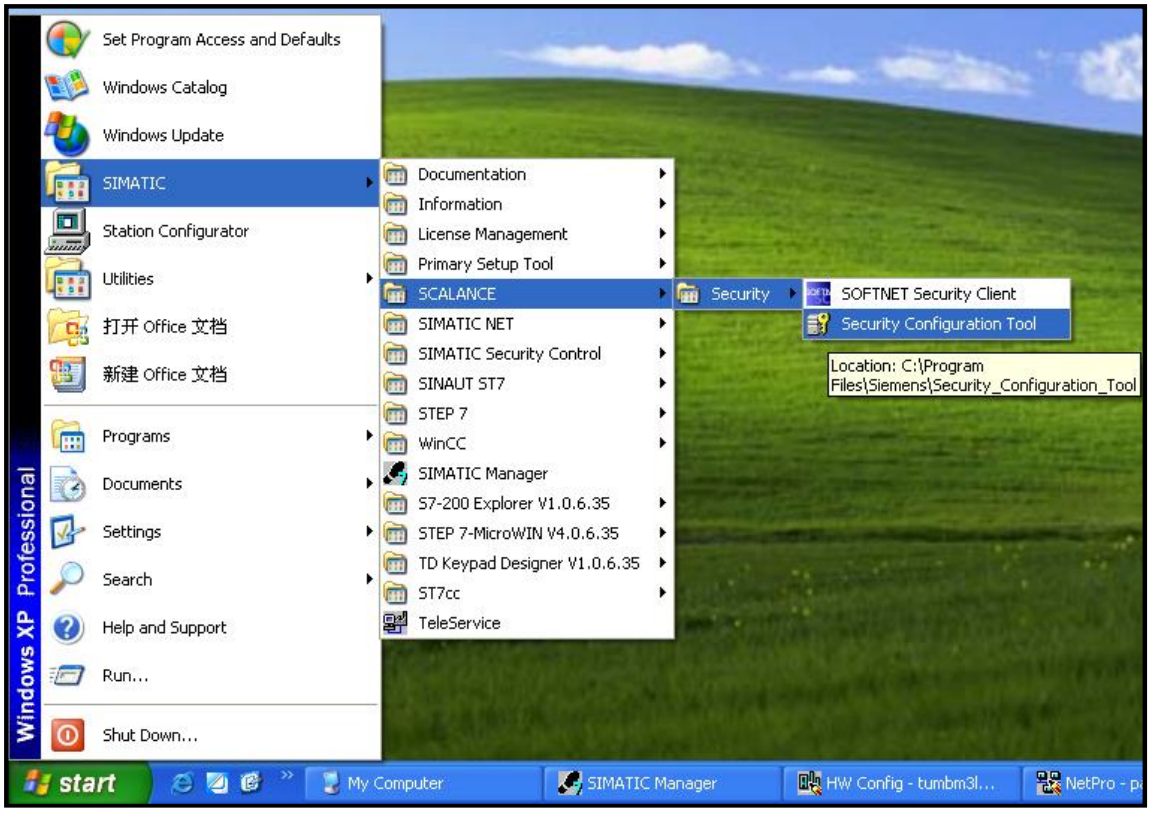
注意：在插入 CPU 后，需要把 CPU 的集成以太网接口的 IP 地址也设置成 192.168.0.2；子网掩码 255.255.255.0。并选择 **Use Router**，并设置路由器的 IP 地址为 192.168.0.1（因为 MD741-1 是 300PLC 的网关，所以此地址为 MD741-1 的内网 IP 地址）

④、配置 SCALANCE S612

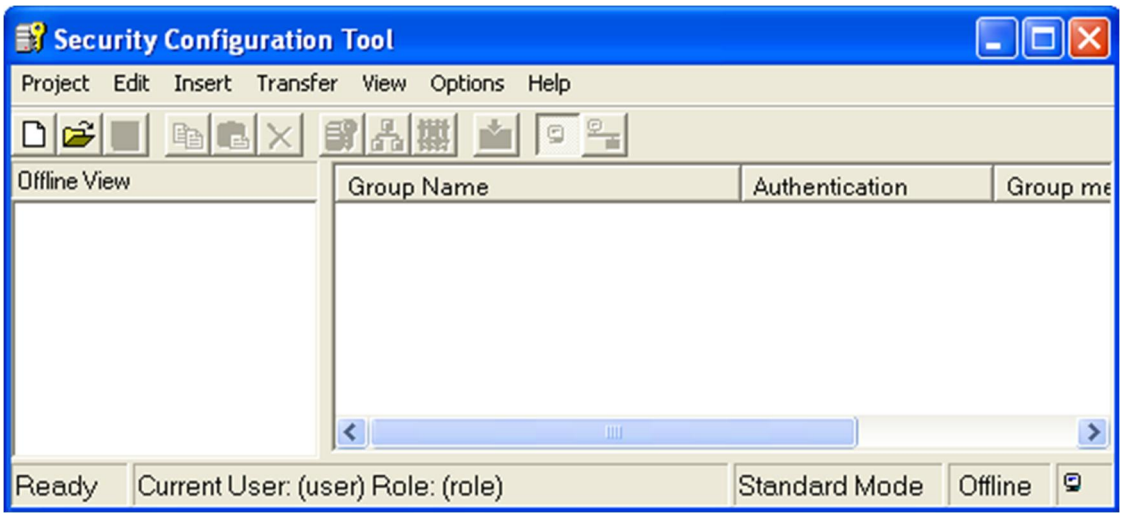
配置 SCALANCE S612 之前，需要连接计算机的以太网线到 SCALANCE S612 的外网口上，并把 SCALANCE S612 恢复出厂设置。修改计算机的 IP 地址如下图



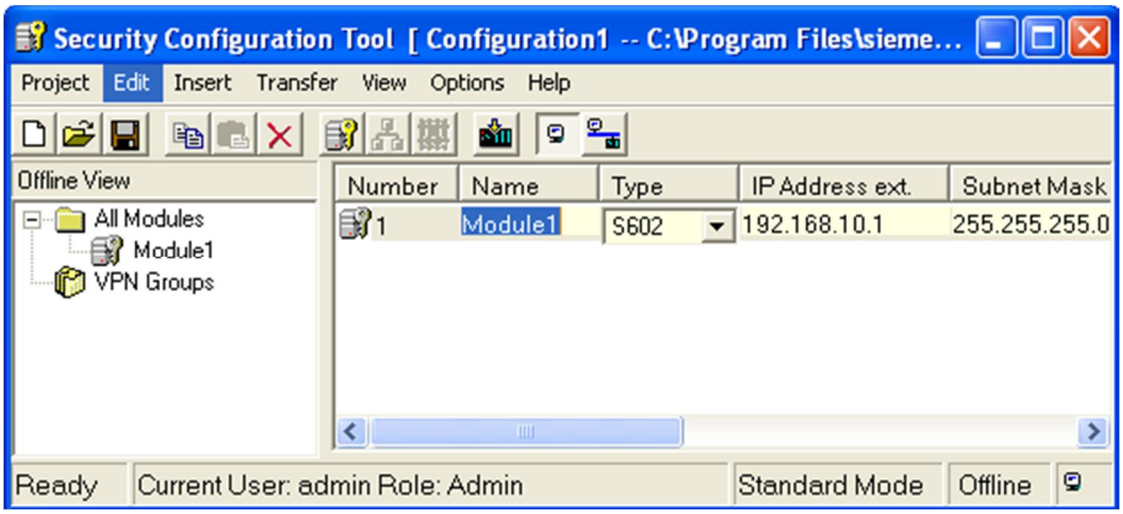

然后打开 SCALANCE S612 的配置工具如下图：




点击后出现 SCALANCE S612 配置界面：

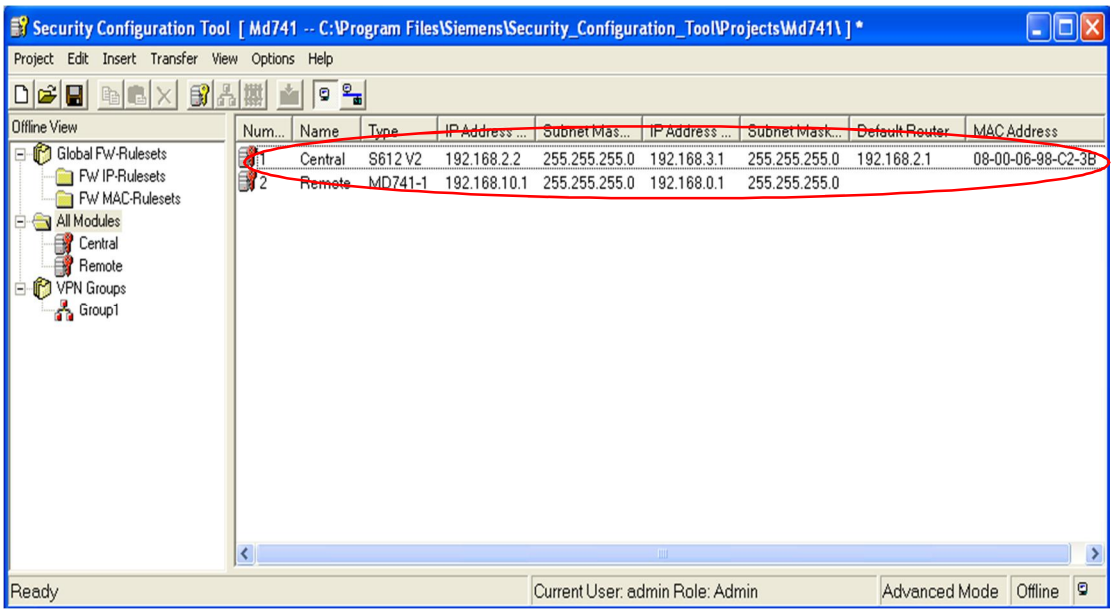



选择 **Project** 下的 **New**，新建一个项目，会弹出一个项目的用户名及密码设置的窗口，添加上用户名和密码都为 Admin 后会出现下面得窗口

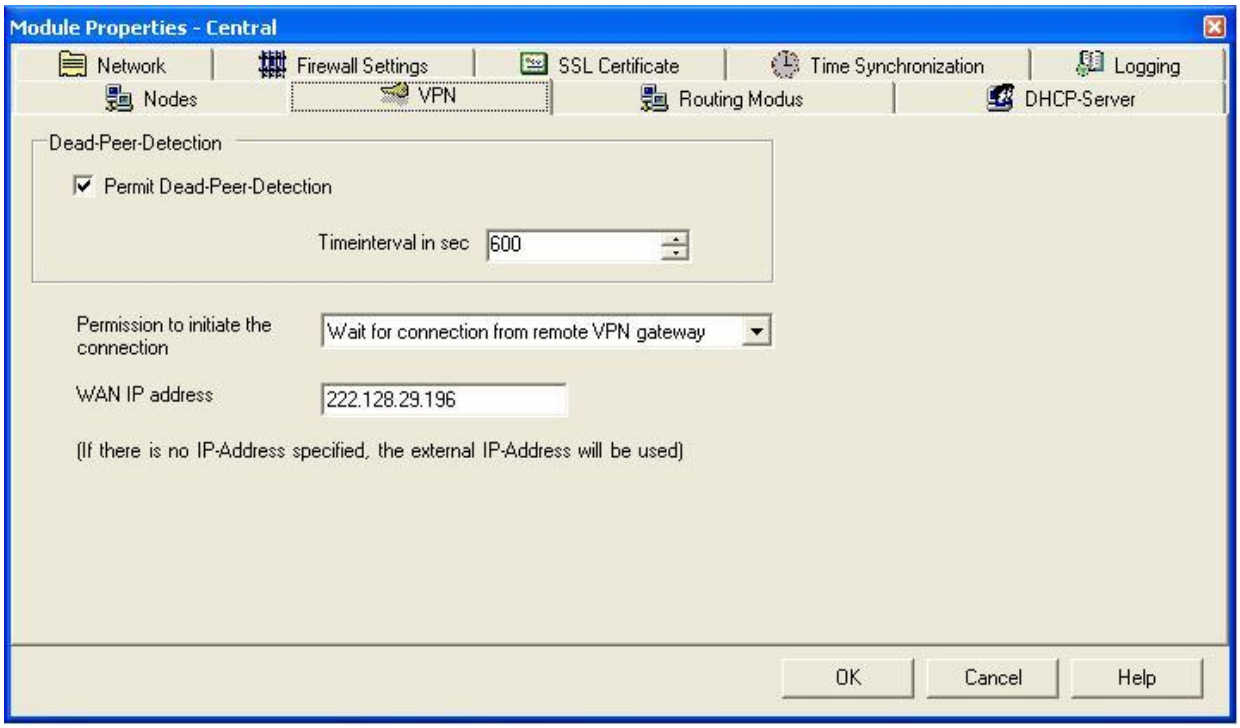



在弹出的上面得窗口。添加两个模块并进行 IP 地址的设置，且新建一个 VPN 的组，并把这两个模块添加到这个组里如下图：

注意：需要修改 SCALANCE S612 的 MAC 地址与实际的模块的 MAC 地址一致，否则无法对 SCALANCE S612 的配置文件下载成功。且需要把计算机的 IP 地址与 SCALANCE S612 的外网口的 IP 地址必须在同一个网段，否则也是无法下载成功的。




双击 SCALANCE S612 模块，配置 VPN 的参数如下

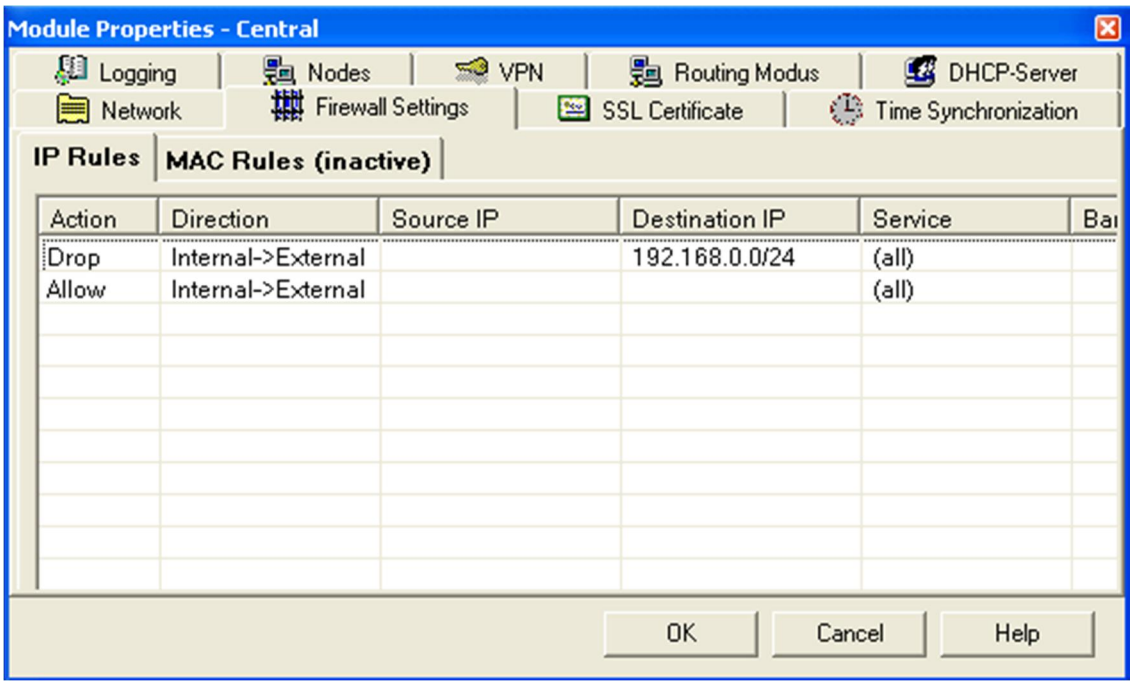



把 **Dead-Peer-Detection** 的时间修改为 600 秒；

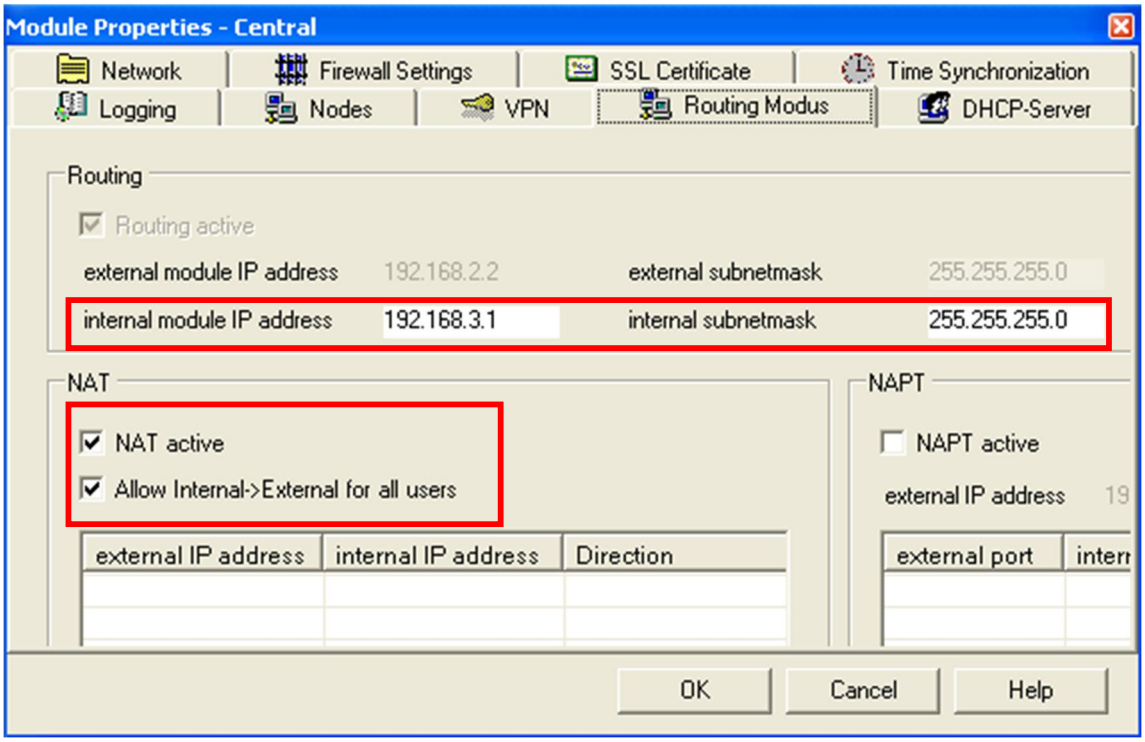
在 **Permission to initial the connection** 选择为 **Wait for connection from remote VPN gateway**；

**WAN IP address** 设置为路由器上获得的公网 IP 地址 **222.128.29.196**；

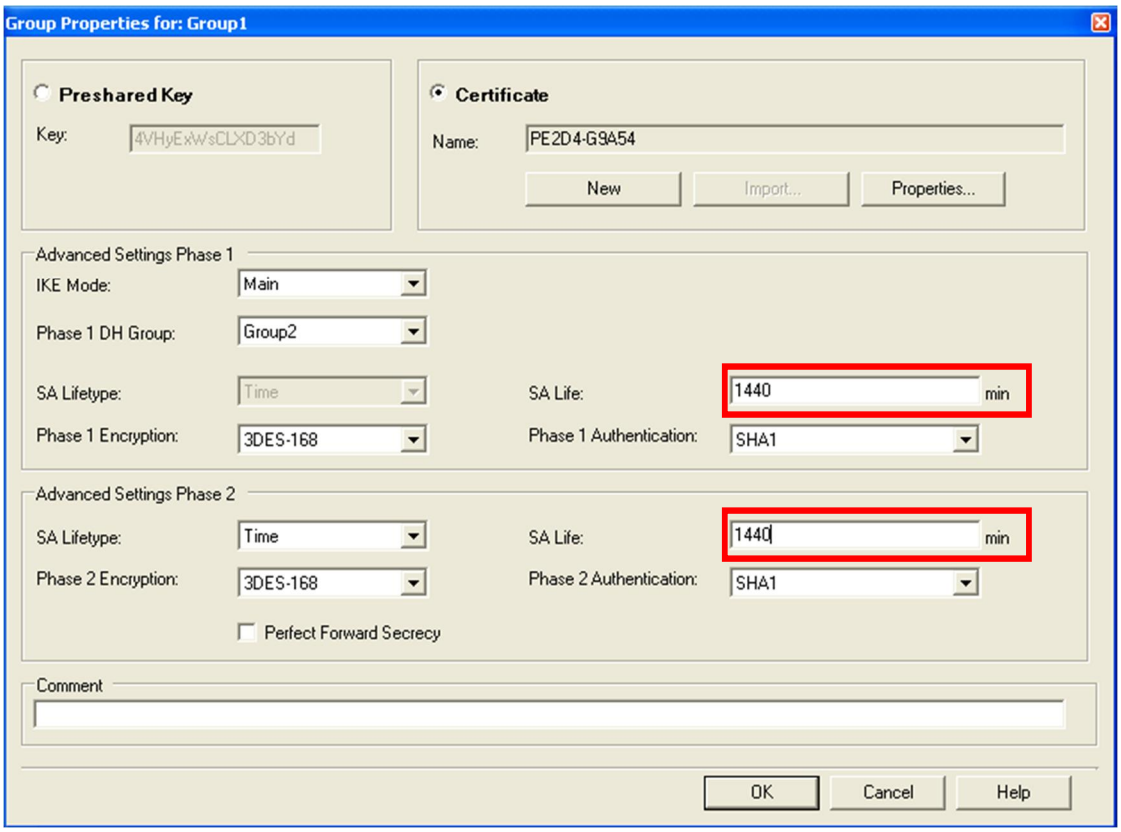
设置防火墙的规则如下：



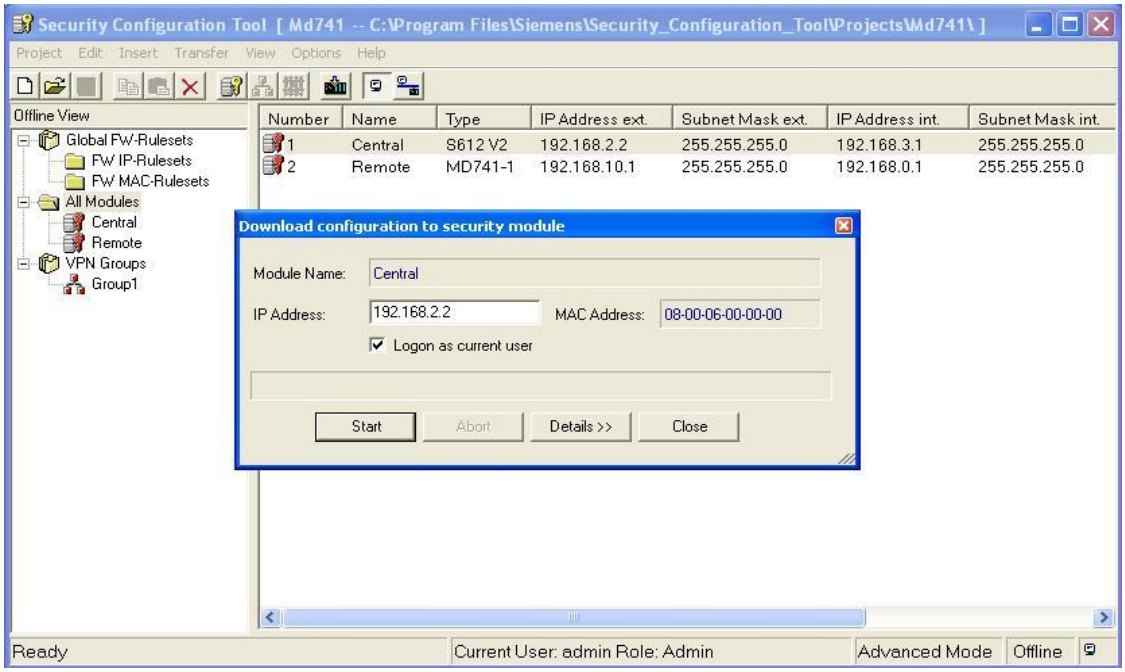

设置路由模式如下：



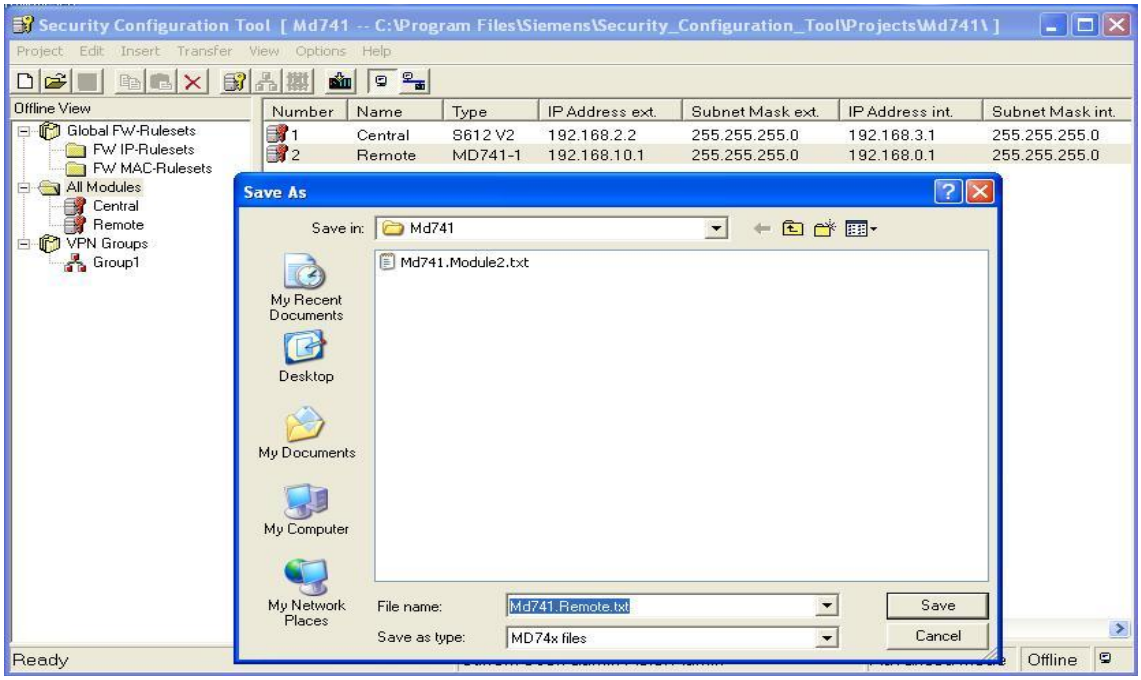

右击 VPN Groups 下的 Group1，在弹出的菜单中选择 Properties..，设置 VPN 的参数如下图：

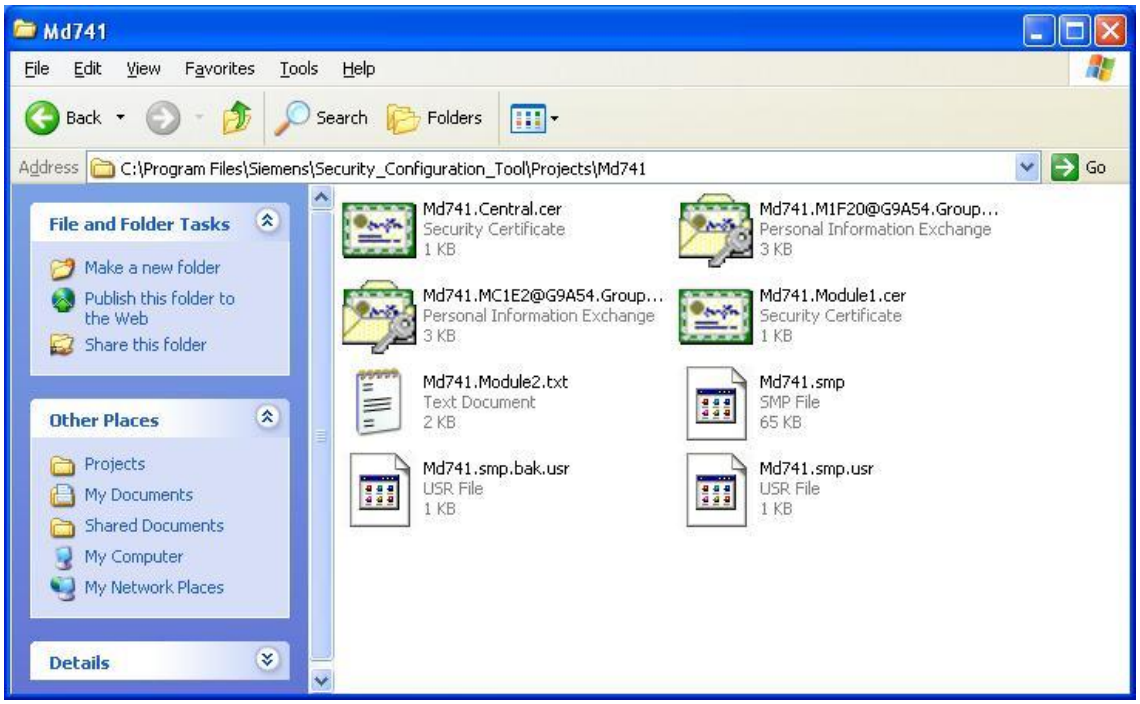



下载配置到 SCALANCE S612，如下图：




保存 MD741-1 需要的证书文件，如下图：



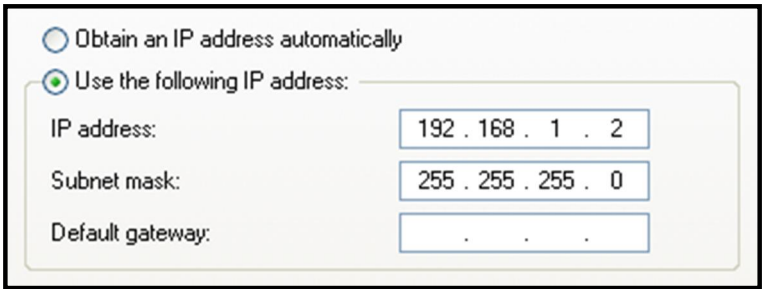




到此完成了对 SCALANCE S612 的配置及证书文件的生成。

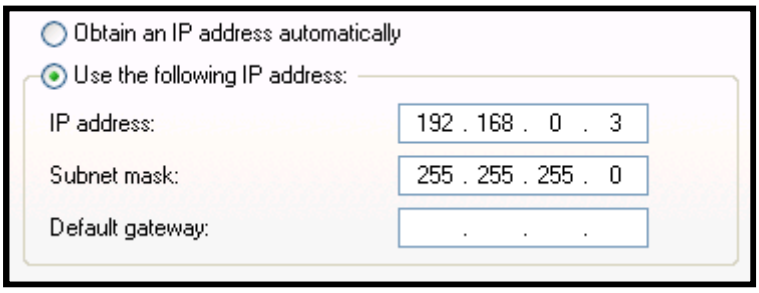
⑤、配置 MD741-1:

MD741-1 的出厂设置的 IP 地址为 192.168.1.1，所以为了能够满足我们的应用，必须修改其 IP 地址为 192.168.0.1。方法如下：

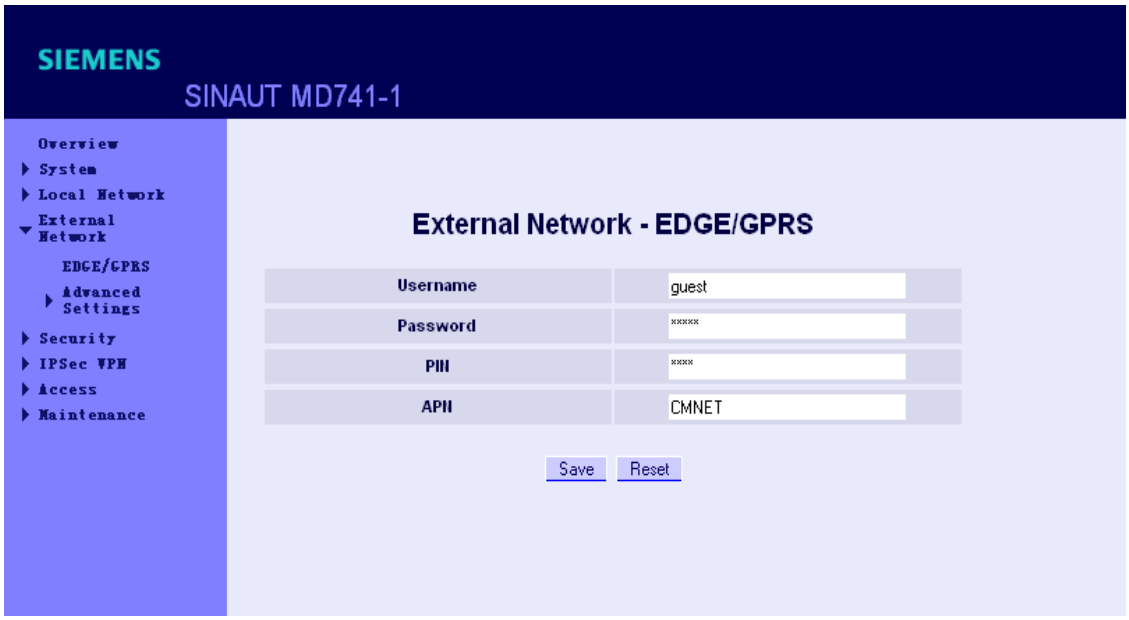
首先设置计算机的 IP 地址为 192.168.1.2；子网掩码为 255.255.255.0 如下图所示：



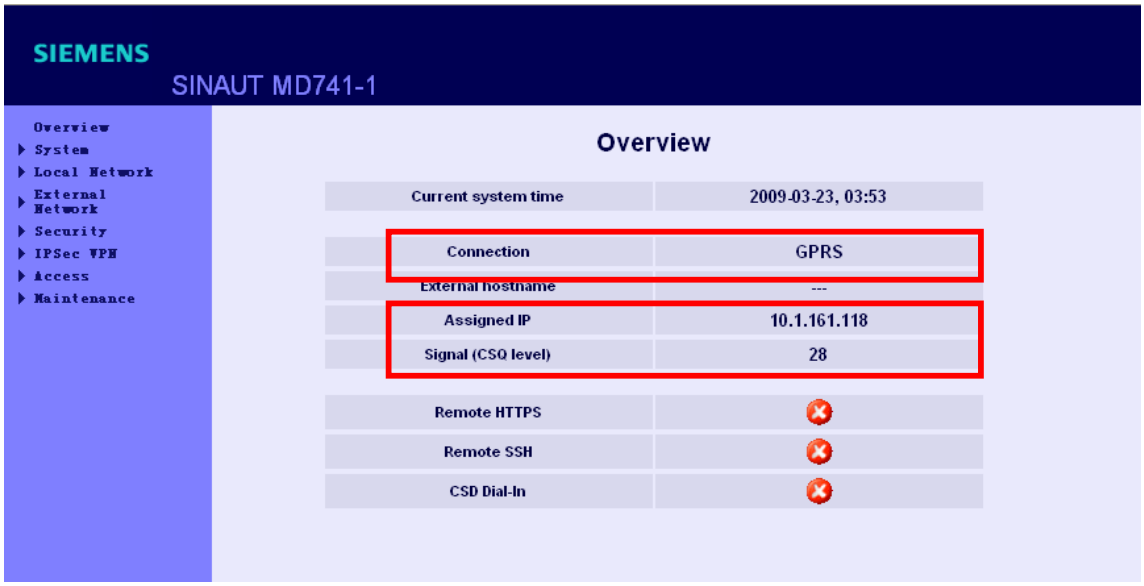

然后打开 IE 浏览器，在 IE 浏览器中输入 https://192.168.1.1，进入到 MD741-1 的配置界面，选择左面导航栏中 **Local Network**，修改 IP 地址为：192.168.0.1，点击 **Save** 按钮，后关闭 IE 浏览器。重新设置计算机的 IP 地址如下图：




设置后重新打开 IE 浏览器，在 IE 浏览器中输入 https://192.168.0.1,进入到 MD741-1 的配置界面,点击左面导航栏的 **External Network** 下的 **EDGE/GPRS**，配置接入 Internet 的参数如下图：

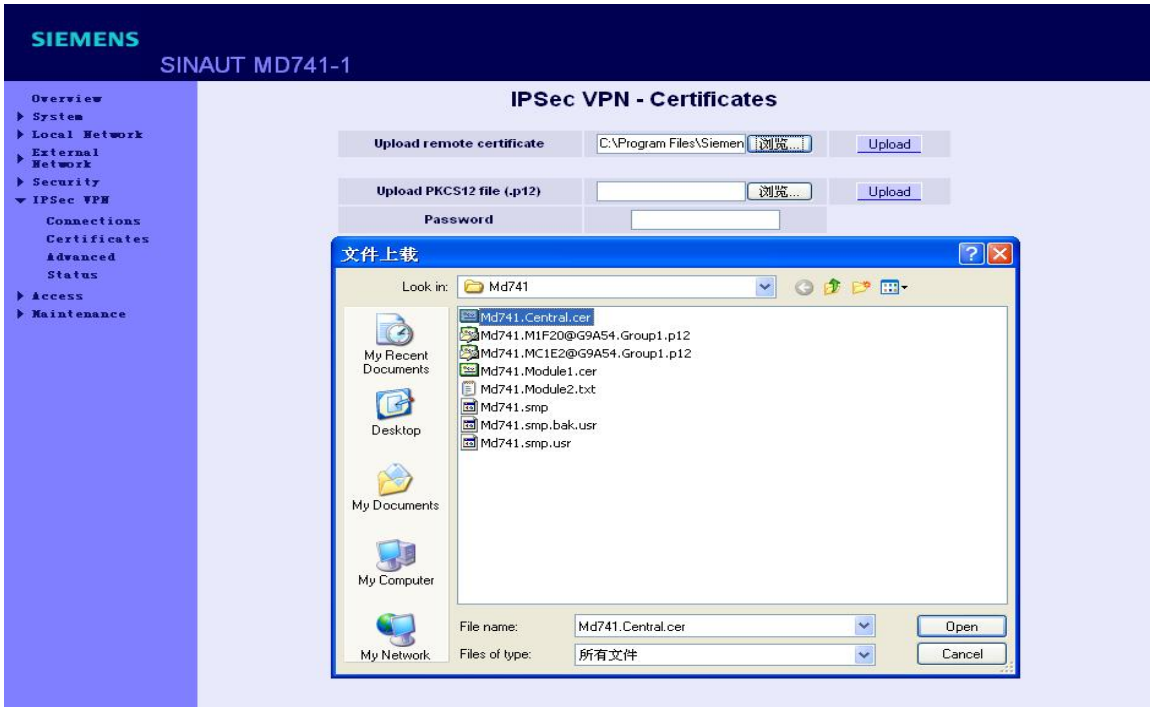



用户名和密码都为 **guest**； **APN** 为 **CMNET**,然后点击 **SAVE** 按钮保存设置。配置完后查看 MD741-1 是否接入到 Internet 上，若接入，则在左面得导航栏里的 **Overview** 显示如下图:

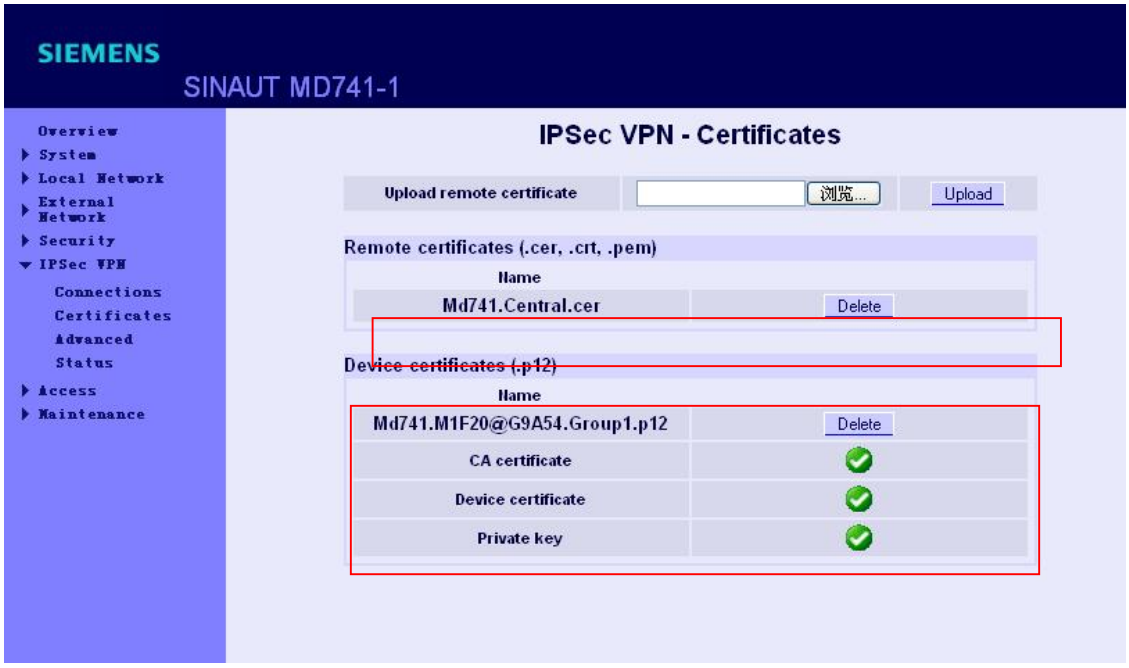



配置完公网接口后，需要配置 VPN 的参数，配置步骤如下：

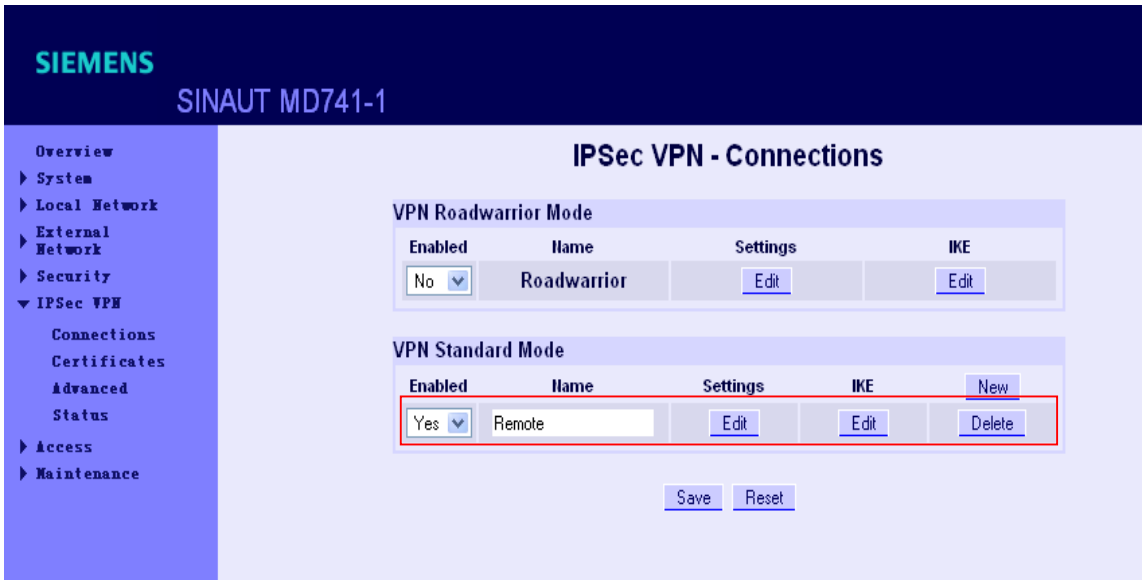
点击左面导航栏中的 **IPSec VPN** 下的 **Certificates**，在右面的窗口中加载证书文件（在第 4 步中生成的证书文件），如下图：



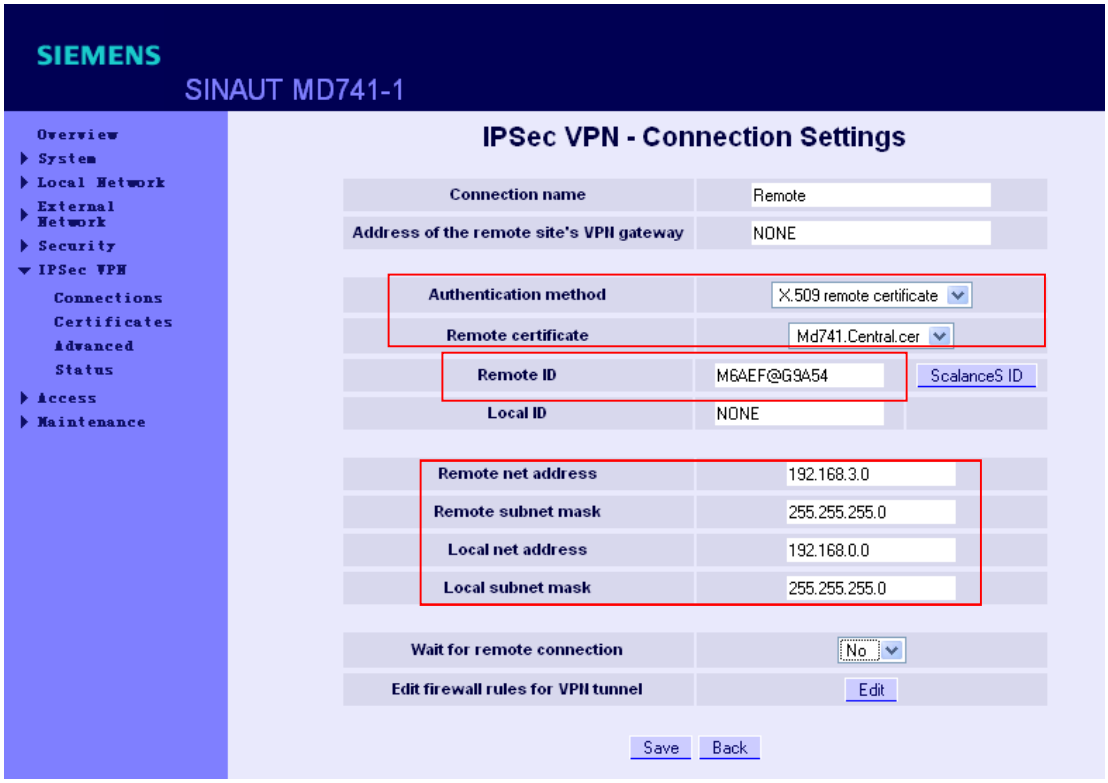

把所有的证书加载后，出现下面得画面后，表示已成功加载证书文件；




加载证书后，需要配置 VPN 的连接，点击点击左面导航栏中的 **IPSec VPN** 下的 **Connections**，在出现的右面的窗口中的 **VPN Standard Mode** 使能一个连接，如下图：

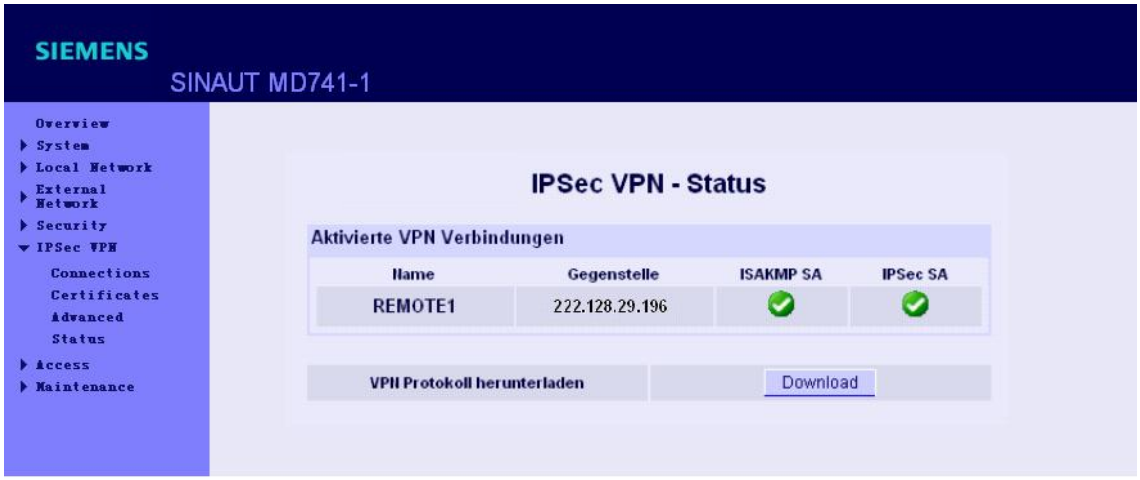



然后再点击 **Settings** 下的按钮，配置连接参数如下图：




配置完后点击 **Save** 保存设置的参数

到此就完成了所有的配置。然后就可以按照网络结构图把所有的设备连接好，并上电，当 VPN 正常连接后会出现下面的状态：




VPN 建立后就可以对 PLC 进行远程的程序下载。