

## 论文独创性声明

1. 论文作者（若与其他作者共同合作完成作品，则论文作者已获得其他所有合作作者的授权发表此声明）在此声明所呈交论文系其独立或集体完成的作品。文中依法引用他人成果，并均已做出明确标注并得到许可。论文内容未包含法律意义上已属于他人而未被他人授权使用的任何形式的研究和创作成果。
2. 论文作者对稿件内容的真实性及思想观点负责，论文由论文作者自负文责。
3. 作者保证论文不会侵犯第三人的任何权利和利益，包括但不限于他人的著作权、商业秘密。
4. 论文作者未曾将本论文提交于以往各届的西门子工业专家会议。
5. 论文提交至西门子工业专家会议会务组即表明论文作者同意上述声明。

# 西门子S7-200SMART PLC通过PPTP VPN远程通讯

孔祥东

(成都新宏基科技发展有限公司, 成都)

**摘要:** 本文主要介绍西门子S7-200SMART PLC如何通过VPN远程通讯。

**关键词:** S7-200SMART PLC VPN 远程通讯

**正文:**

## 一、项目简介

PLC 的通讯方式已经成为其发展的一个方向, 并受到越来越多的关注。西门子新一代 PLC 都主打以太网的通讯方式, 即便捷又快速, 结合目前的互联网技术, 通过 VPN 建立连接, 让我们不到现场就可以了解设备情况并进行程序修改, 甚至数据采集。用这种方法可以方便的让工程师不用到现场就可以掌握设备的运行状况, 并可以实现远程维护, 减少工程师的出差时间, 甚至可同时维护和监控多台设备。这种应用彻底改变了工程师的办公环境及工作效率, 以前必须到现场才能了解情况, 现在只需要通过远程通讯就可以做到, 并能合理分配公司资源——让最适合的人到现场去解决问题。

## 二、系统构成

VPN 已经是很成熟的技术了, 实现起来并不困难, 只需要建立一台 VPN 服务器就可以实现。图 1 是 VPN 服务器机柜, 图 2 是网络结构示意图。

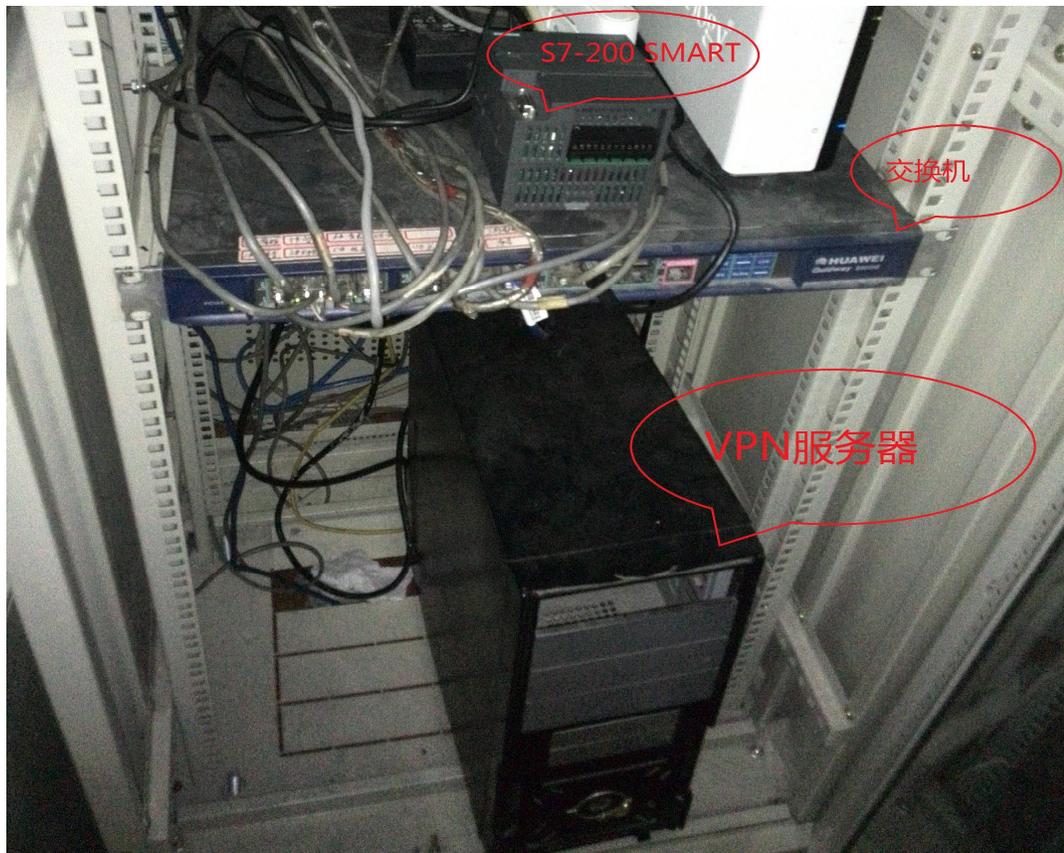


图 1

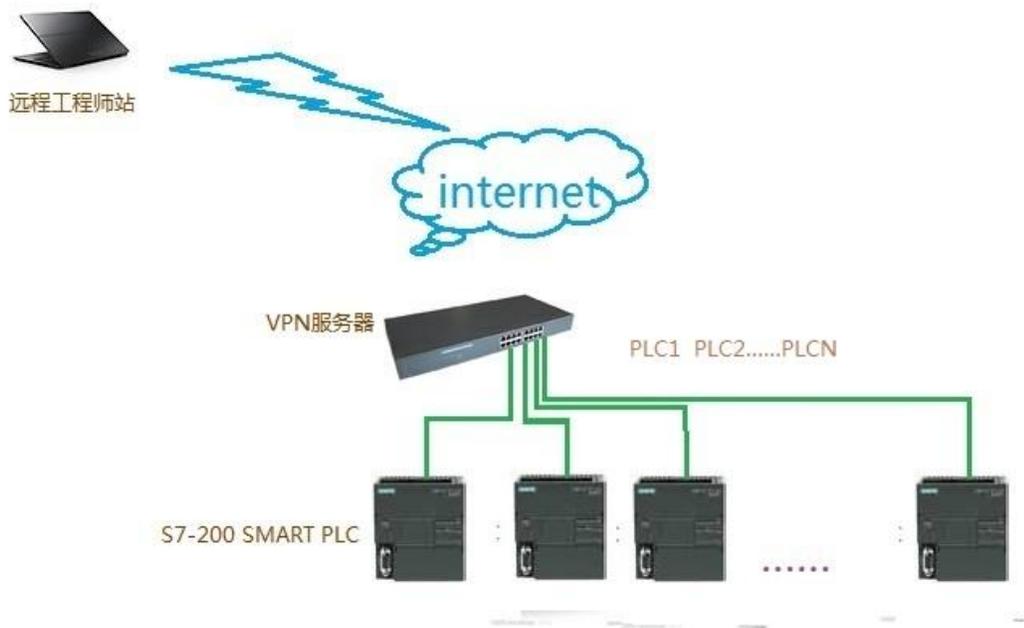


图 2

### 三、系统组成

VPN 服务器：图 1 采用的是一台淘汰的台式机安装海蜘蛛做虚拟路由器，也可以采用商用路由器代替，例如飞鱼星的 VE984W，已做过该路由器的测试，完全可以实现本文的功能，只是这个路由器如今放在客户那里做测试，所以本文以海蜘蛛路由器做介绍，选择路由器时必须选择具备 VPN 服务功能（不同于 VPN 客户端，有些路由器介绍的并不详细买回来可能只能做 VPN 客户端拨号用）和动态域名解析（除非服务器端有公网固定 IP，则不需要动态域名解析）的路由器。

动态域名解析：VPN 拨号时需要设置 VPN 服务器的主机名或在公网的 IP 地址，因此没有公网 IP 的用户可以在花生壳、金万维等 DDNS 服务商网站注册账号并申请域名（有免费和付费两种，我用的是免费的，使用一年多没有任何问题）。选择 DDNS 服务商时要注意：仅能选择 VPN 路由器动态域名解析中所能支持的服务商！海蜘蛛路由器选择范围非常广泛，VE984W 我用的是花生壳的。

VPN 客户端：可采用两种方式建立连接，一种是上位机（编程或数据采集）主动拨号到 PLC 所连接的 VPN 服务器，一种是 PLC 直接拨号到上位机所连接的 VPN 服务器。图 1 和图 2 的结构是前一种方式，后一种方式的结构是将“VPN 服务器”放到“远程工程师站”的本地，PLC 端通过一个具有 VPN 拨号功能的路由器实现和 VPN 服务器建立通讯，见图 3。

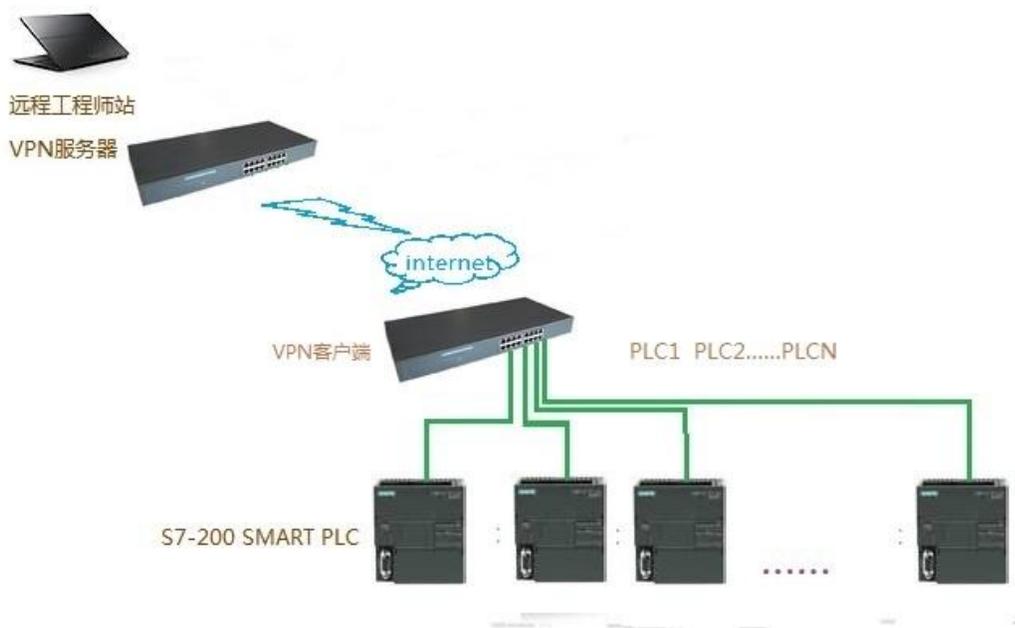


图 3

## 四、系统设置

## VPN 服务器设置

## 4.1、 动态域名解析设置，如图 4：



图 4

启用动态域名解析功能；选择 DDNS 服务商；用户名/密码是在网站注册的账号；DDNS 服务商下面一行填入所申请的域名，如有固定 IP 请忽略此内容。

## 4.2、VPNF 服务设置，如图 5



图 5

启用 PPTP VPN 服务；VPN 服务端 IP 可自定义但不要和本地 IP 设置在同一网段；VPN 客户端 IP 范围，必须和 VPN 服务器 IP 在一个网段；如拨入的所有 PLC 要进行数据交换，请勾选“运行 VPN 客户端之间互相访问”；支持的身份验证协议，后三项必须勾选。

#### 4.3、建立 VPN 账号如图 6

图 6

用户名 ID，在 VPN 客户端用来拨号的用户名；真实姓名，用来识别拨入的客户端；登陆密码，在 VPN 客户端用来拨号的密码；允许同时登陆的最大客户数，同时用改账号登陆的最大用户限制；其他可按默认设置。

至此 VPN 服务器已建立完毕。

#### VPN 客户端拨号

4.4、WINDOWS 直接创建连接，创建成功后跳过拨号，打开创建好的连接属性如图 7 进行设置



图 7

按红色框体内的设置勾选，完成后按 4.3 创建的账号拨号。

4.5、 路由器拨号如图 8

PPTP 拨号用户名:	<input type="text"/>
PPTP 拨号密码:	<input type="password"/>
最大传输单元(MTU):	1492 (默认为 1492)
最大接收单元(MRU):	1492 (默认为 1492)
发送 LCP(连接控制协议) 数据包间隔:	20 s (20~60)
多少个LCP请求未应答则断开连接:	3 (3~6)
启用代理 ARP:	<input type="checkbox"/> 是
开机自动启动:	<input checked="" type="checkbox"/> 是 (随系统启动, 一般选上)
负载权重:	1 <a href="#">?</a>
其他参数:	<input type="checkbox"/> 启用调试 <a href="#">?</a> <input type="checkbox"/> 不自动加入多线负载 <a href="#">?</a> <input type="checkbox"/> 禁止NAT <a href="#">?</a>
运营商:	中国电信 (用于多线策略及负载)
线路检测:	已禁用 [ <a href="#">检测日志</a>   <a href="#">清除</a> ]
身份验证 & 加密...	
身份验证协议:	<input checked="" type="checkbox"/> PAP <input checked="" type="checkbox"/> CHAP <input checked="" type="checkbox"/> MS-CHAP <input checked="" type="checkbox"/> MS-CHAP v2
启用数据加密 (MPPE):	<input type="checkbox"/> 是 (需要 MS-CHAP 或 MS-CHAP v2 协议支持)
启用软件压缩(MPPC):	<input type="checkbox"/> 是 (微软点对点压缩协议支持)
<input type="button" value="保存设置"/> <input type="button" value="重置"/> <input type="button" value="删除配置"/>	

图 8

填入 4.3 创建的账号，身份验证&加密与图 5 一致

## PLC 设置

只需要将 PLC 的 IP 设置成和本地路由器在一个网络段即可，为避免连接不上请给 PLC 设置网关。

至此，PLC 通过 PPTP VPN 远程通讯就建好了，只要 VPN 客户端拨号成功即可将远在异地的 PLC 当做本地设备进行管理。

## 五、应用体会

西门子 PLC 所具有的以太网通讯协议为我们实现这样的通讯方式提供了极大的便利，在此应用中，不仅 S7-200 SMART，甚至 S7-1200\S7-1500 及 S7-300PN 都可以这样应用。

在实际使用时，如对数据的实时性和可靠性有严格要求的，不建议这样使用，因为该应用主要依靠网络服务商，目前的网络服务商提供不了实时通讯。

在实际使用时建议使用图 3 的结构，优点是：所有 PLC 都通过路由器拨入到工程师站 VPN 服务器，只需要 VPN 服务器具有域名或公网 IP 即可，且经济方便，如 PLC 本地无法提供网络，可采用 3G 路由器为 PLC 建立单独的网络系

接入到互联网，而不需要通过客户的网络，减少不必要的麻烦；缺点是：需要管理好 PLC 的 IP 地址，所有拨入的 PLC 的 IP 地址不能重复，且一旦弄成 IP 地址可能造成危险，比如要操作 A 厂的 PLC，结果误连接到了 B 厂的 PLC 上，VPN 无法分辨这个错误。

这种应用的灵活性确实为我们带来了许多方便，虽然未曾在项目上应用，但每当客户遇到问题时只需要先给客户邮寄一台带 3G 网络的路由器即可为我们做出预先判断，或者很方便的对处在现场的工程师进行指导和技术支持。

## 六、参考文献

[1] STEP 7-Micro/WIN SMART Help

[2] 海蜘蛛路由器使用手册