

操作指南 • 11/2015

如何在西门子 PLC 诊断以太网 连接状态

Ethernet, SIMATIC PLC, SNMP

目录

1	在西门子 PLC 诊断以太网连接状态	3
1.1	问题描述	3
1.2	解决方案	3
1.3	配置	4
1.3.1	CPU 的配置	4
1.3.2	通讯对象的配置	6
1.3.3	测试	7

1 在西门子 PLC 诊断以太网连接状态

1.1 问题描述

随着工业以太网技术发展，工业以太网现场网络的节点数和设备类型日益庞杂，因此越来越多的客户希望 PLC 能够有能力对网络的节点状态作出诊断（例如：网络断线等）。

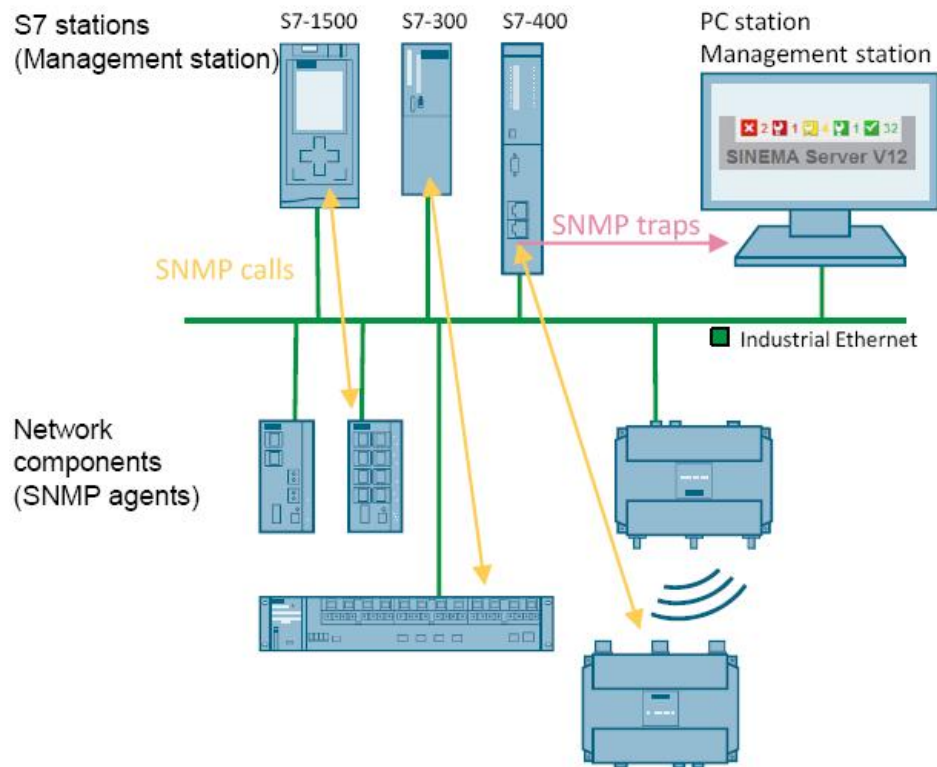
通过 PROFINET 的扩展诊断功能，可以对网络节点的状态作出快速的判断，
参考链接：<https://support.industry.siemens.com/cs/cn/zh/view/87668286>，
<https://support.industry.siemens.com/cs/cn/zh/view/109477206>。但是不足之处是对于网络节点是第三方设备或者不支持 PROFINET 扩展诊断无效。

S7-300/400 以太网模块程序块可以使用“Ping”命令判断目标的连接状态，
参考链接：<https://support.industry.siemens.com/cs/cn/zh/view/88484028>，但是“Ping”指令会受到一些防火墙软件及设备的限制，而且，在庞大的网络里频繁的“Ping”操作也会增大网络的负荷，并且对于支持该功能的模块也会有版本的限制。

1.2 解决方案

SNMP，简单网络管理协议，是开放的以太网协议，通过访问标准的 MIB 数据库就可以获得网络设备的具体状态信息。

西门子为 S7 自带以太网接口的 CPU 提供了标准的库，可以支持 SNMP 协议。这样 S7 CPU 通过指令可以作为 SNMP 的管理者获得网络节点的信息。如图 1-1。



<图 1-1 SNMP>

因为 SNMP 是开放的网络管理协议，绝大多数网络设备都支持，所以功能上具备良好的兼容性；又因为，SNMP 规定了公开的 MIB 数据库，因此可以提供丰富多彩的信息给 S7 CPU。

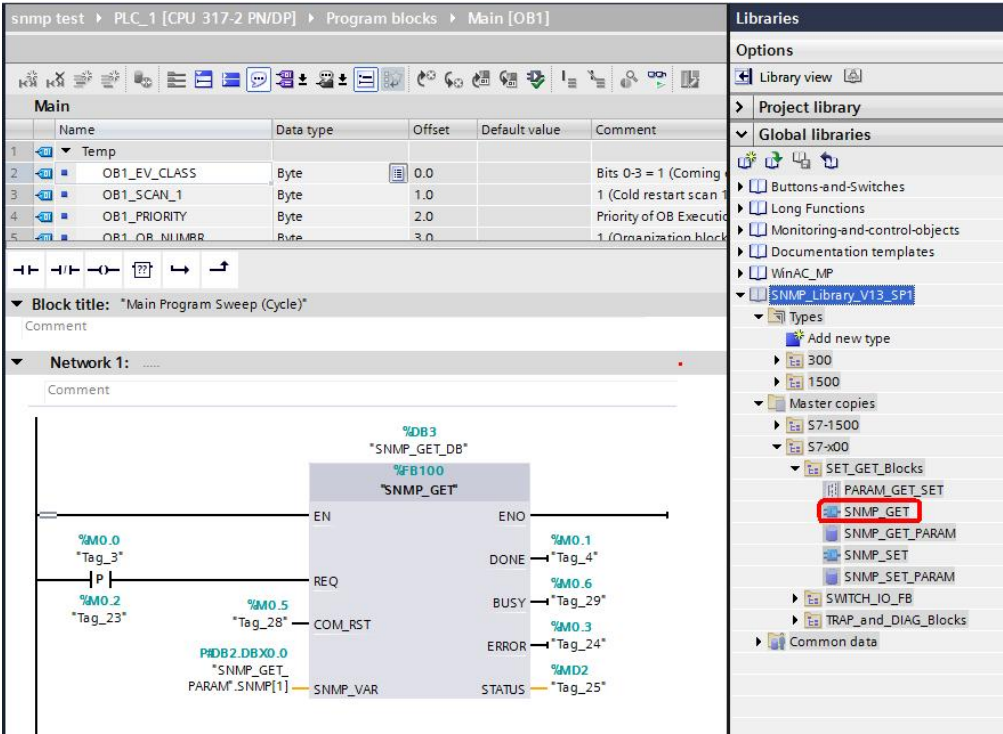
S7 CPU SNMP 库的下载和具体使用可以参考以下链接：

<https://support.industry.siemens.com/cs/cn/en/view/57249109>

1.3 配置

1.3.1 CPU 的配置

安装 SNMP 库后，可以在博途软件中调用 SNMP 程序块，本例中使用 V13 SP1、“SNMP_GET”指令读取网络设备的端口状态，如图 1-2。



<图 1-2 “ SNMP_GET ” >

“ SNMP_GET ” 指令 “ SNMP_VAR ” 管脚定义通讯对象的信息，如图 1-3，部分重要参数含义如下：

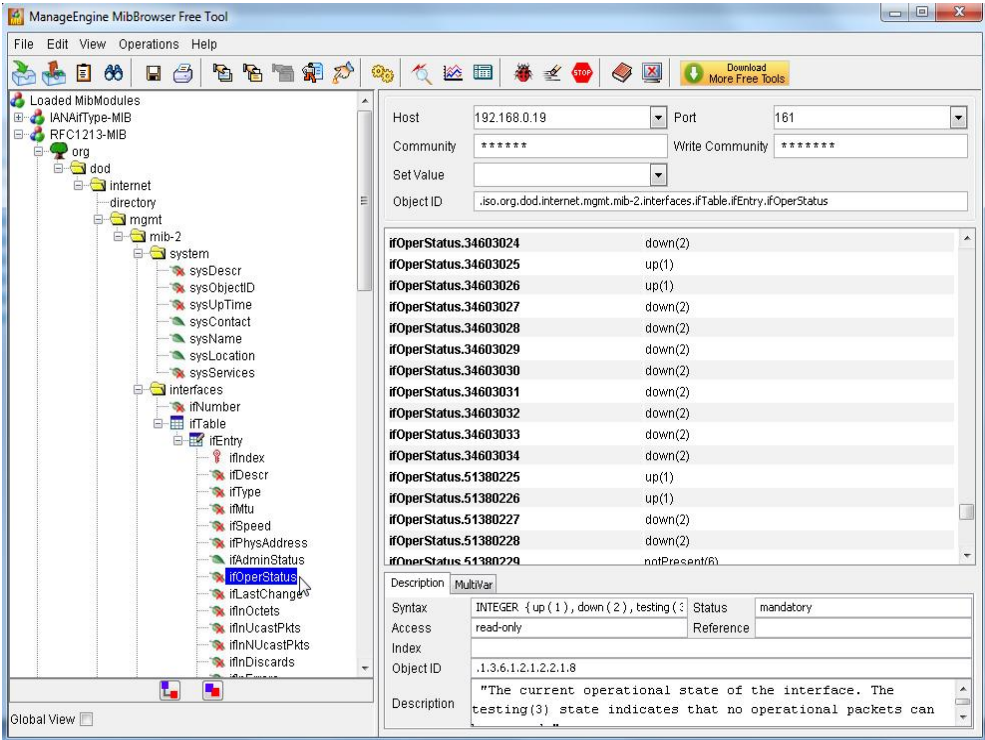
- ❖ “ IP_ADR ” ： 通讯对象的 IP 地址（十六进制表示）
- ❖ “ DEVICE_ID ” ： S7-300 固定为 2
- ❖ “ CON_ID ” ： UDP 连接的 ID（默认）
- ❖ “ LOCAL_P ” ： 本地端口号
- ❖ “ OID ” ： MIB 数据库中每一个变量的地址
- ❖ “ Community ” ： “ public ” -只读，“ private ” -读/写

Name	Data type	Offset	Start value	Monitor value
Static				
SNMP	Array[1..4] of "PAR...	0.0		
SNMP[1]	"PARAM_GET_SET"	0.0		
IP_ADR	DWord	0.0	16#C0A8001f	16#C0A8_001F
DEVICE_ID	Byte	4.0	2	16#02
CON_ID	Word	6.0	W#16#0063	16#0063
LOCAL_P	Word	8.0	W#16#7D0	16#07D0
OID	String[254]	10.0	'1.3.6.1.2.1.2.2.1.8.4'	'1.3.6.1.2.1.2.2.1.8.4'
Community	String[20]	266.0	'public'	'public'
VALUE_TYPE	Byte	288.0	16#0	16#02
VALUE_LEN	Byte	289.0	16#0	16#01
VALUE	Array[1..255] of Byte	290.0		
VALUE[1]	Byte	0.0	16#0	16#01
VALUE[2]	Byte	1.0	16#0	16#00

<图 1-3 “ SNMP_VAR ” >

1.3.2 通讯对象的配置

对于通讯对象，我们首先要确保激活其 SNMP 的功能，并且在设置“Community”参数时和 CPU 侧的一致，这样才能确保操作的权限可靠。然后我们需要知道通讯对象支持的 MIB 的类型，一般第三方的手册都会有介绍，当前比较通用的标准是 MIB2 RFC1213。OID 如果不好确认，也可以使用第三方 SNMP 的管理软件，如图 1-4。



<图 1-4 SNMP 软件>

如果希望读取网络设备端口的连接状态，可以通过路径“iso.org.dod.internet.mgmt.mib-2.interfaces.ifTable.ifEntry.ifOperStatus”访问，“ifOperStatus”表示设备的端口状态，具体到端口表示“ifOperStatus.x”，其中“x”表示具体的端口索引。

以罗杰康 RS900 交换机为例，如图 1-5。其 8 个 RJ45 以太网接口对应的端口索引 ID：1-8。所以端口 1、2 连接状态的 OID 分别为“1.3.6.1.2.1.2.2.1.8.1”、“1.3.6.1.2.1.2.2.1.8.2”



<图 1-5 罗杰康 RS900>

1.3.3 测试

可以调用多次“SNMP_GET”指令，触发激活之后，在“SNMP_VAR”定义的结构里“VALUE”得到结果，通常情况下“1”代表端口连接；“2”代表端口无连接（具体含义要参考通讯对象的手册说明！）。

如图 1-6、1-7，此时罗杰康 RS900 交换机的 1 口无连接，2 口连接正常。

	Name	Data type	Offset	Start value	Monitor value
1	Static				
2	SNMP	Array[1..4] of ...	0.0		
3	SNMP[1]	*PARAM_GET_SET	0.0		
4	IP_ADR	DWord	0.0	16#C0A80019	16#C0A8_0019
5	DEVICE_ID	Byte	4.0	2	16#02
6	CON_ID	Word	6.0	W#16#0063	16#0063
7	LOCAL_P	Word	8.0	W#16#7D0	16#07D0
8	OID	String[254]	10.0	'1.3.6.1.2.1.2.2....'	'1.3.6.1.2.1.2.2.1.8.1'
9	Community	String[20]	266.0	'public'	'public'
10	VALUE_TYPE	Byte	288.0	16#0	16#02
11	VALUE_LEN	Byte	289.0	16#0	16#01
12	VALUE	Array[1..255] of Byte	290.0		
13	VALUE[1]	Byte	0.0	16#0	16#02
14	VALUE[2]	Byte	1.0	16#0	16#00

<图 1-6 罗杰康 RS900，端口 1>

4	SNMP[2]	*PARAM_GET_SET	546.0		
5	IP_ADR	DWord	0.0	16#C0A80019	16#C0A8_0019
6	DEVICE_ID	Byte	4.0	2	16#02
7	CON_ID	Word	6.0	W#16#0064	16#0064
8	LOCAL_P	Word	8.0	W#16#7D1	16#07D1
9	OID	String[254]	10.0	'1.3.6.1.2.1.2.2....'	'1.3.6.1.2.1.2.2.1.8.2'
10	Community	String[20]	266.0	'public'	'public'
11	VALUE_TYPE	Byte	288.0	16#0	16#02
12	VALUE_LEN	Byte	289.0	16#0	16#01
13	VALUE	Array[1..255] of ...	290.0		
14	VALUE[1]	Byte	0.0	16#0	16#01
15	VALUE[2]	Byte	1.0	16#0	16#00

<图 1-7 罗杰康 RS900，端口 2>