

工业网络通讯实训系统

实验指导书

（进阶版）

北京德普罗尔科技有限公司

2019.9.25

目录

实验一 工业以太网电缆接头制作实验	5
1.1 技术背景	5
1.2 实验目的	5
1.3 实验准备	5
1.4 实验内容	6
1.5 实验步骤	6
1.6 课后作业	7
实验二 网络配置实验	8
2.1 实验目的	8
2.2 实验准备	8
2.3 实验内容	8
2.4 实验步骤	9
2.4.1 网络结构实施	9
2.4.2 配置上位机、SCALANCE XM408 和 S7 1200 的 IP 地址	9
2.4.3 通过浏览器配置交换机	12
2.5 实验结果核查	16
2.6 课后作业	16
实验三 单环冗余网络实验	17
3.1 技术背景	17
3.2 实验目的	17
3.3 实验准备	17
3.4 实验内容	17
3.5 实验步骤	18
3.5.1 配置上位机的 IP 地址和子网掩码	18
3.5.2 配置交换机 SCALANCE XM408-8C	19
3.5.3 配置 SCALANCE XB208(A)	22
3.5.4 配置 SCALANCE XB208(B)	23
3.5.5 在博途中配置 PLC S7 1200(A)（即网孔板上左侧的 S7 1200）	24
3.5.6 网络线缆连接	25
3.5.7 环形冗余通讯测试	25
3.6 课后作业	27
实验四 无线通信实验	28
4.1 技术背景	28
4.2 实验目的	28
4.3 实验准备	28
4.4 实验内容	29
4.5 实验步骤	29
4.5.1 网络结构实施	29
4.5.2 配交换机、无线模块和 PLC 配置 IP 地址	30
4.5.3 配置无线模块	31
4.5.4 在博途中配置 PLC	34
4.5.5 通讯测试	35

4.6 课后作业	36
实验五 实时通讯实验（通过 PROFINET IO 系统）	37
5.1 技术背景	37
5.2 实验目的	37
5.3 实验准备	38
5.4 实验内容	38
5.5 实验步骤	39
5.5.1 网络结构实施	39
5.5.2 配置上位机和交换机的 IP 地址	39
5.5.3 在 Portal 软件中配置 PROFINET IO 系统	39
5.5.4 通信测试	42
5.6 课后作业	44
实验六 光纤通讯实验	46
6.1 技术背景	46
6.2 实验目的	47
6.3 实验准备	47
6.4 实验内容	47
6.5 实验步骤	48
6.5.1 配置上位机、交换机的 IP 地址和子网掩码	48
6.5.2 在博途中配置 PLC	48
6.5.3 配置环网	49
6.5.4 网络结构实施	50
6.5.5 环形冗余通讯测试（以 S7 1200(A)为例）	51
6.6 课后作业	52
6.7 参考文献	52
实验七 无缝冗余实验	53
7.1 技术背景	53
7.2 实验目的	53
7.3 实验准备	53
7.4 实验内容	54
7.5 实验步骤	54
7.5.1 配置 SCALANCE X204 RNA（A）	54
7.5.2 配置 SCALANCE X204 RNA（B）	55
7.5.3 在 Portal 软件中将 S7 1200（A）配置为 IO 控制器	55
7.5.4 在 Portal 软件中将 S7 1200（B）配置为 IO 设备	57
7.5.5 网络结构实施	58
7.5.6 通信测试	59
7.6 课后作业	61
实验八 防火墙实验	62
8.1 技术背景	62
8.2 实验目的	62
8.3 实验准备	62
8.4 实验内容	63
8.5 实验步骤	64

8.5.1 在 S615 中划分 VLAN.....	64
8.5.2 在 S615 中进行子网设置	65
8.5.3 在 S615 中设置防火墙 IP 规则	66
8.5.4 网络实施	67
8.5.5 防火墙功能测试	67
8.6 课后作业	69

实验一 工业以太网电缆接头制作实验

1.1 技术背景

以太网电缆是从一个网络设备连接到另外一个网络设备传递信息的介质，是以太网网络的基本构件。

以太网有线传输介质主要包括：双绞线（也就是平时说的网线）、光纤和同轴电缆（较早产品，现在很少看到用了）。在这三者中，同轴电缆由于价格比较高、性能一般而逐渐被市场所淘汰；光纤的性能非常优良，但价格过高且安装起来也比较困难，一般只应用在各项指标都要求较高的网络环境中，家庭网络很少有此应用；双绞线由其低廉的价格，简单的安装方法，良好且稳定的性能在有线网络中广为使用。

双绞线电缆一般分为 8 类：1 类线主要用于语音传输；2 类线由于传输频率只有 1MHz，主要用于旧的令牌网；3 类线主要用于 10BASE-T 的网络；4 类线令牌网和 10BASE-T/100BASE-T 网络；5 类线传输率为 100MHz，用于 100BASE-T 和 10BASE-T 网络，它是最常用的以太网电缆；超 5 类线主要用于千兆位以太网（1000Mbps）；六类线的传输频率为 1MHz~250MHz，适用于传输速率高于 1Gbps 的网络；7 类线是最新的一种非屏蔽双绞线，传输频率至少可达 500 MHz，传输速率为 10 Gbps。

双绞线还分为非屏蔽和屏蔽 2 种。办公日常应用中最多的为 5 类非屏蔽双绞线，而屏蔽双绞线由于其增加了屏蔽层，所以比普通的非屏蔽双绞线更具可靠性和稳定性。

光纤光缆是新一代的传输介质，与铜质介质相比，光纤无论是在安全性、可靠性还是网络性能方面都有了很大的提高。除此之外，光纤传输的带宽大大超出铜质线缆，而且其支持的最大连接距离达两公里以上，是组建较大规模网络的必然选择。由于光纤光缆具有抗电磁干扰性好、保密性强、速度快、传输容量大等优点，所以它的价格也较为昂贵，在家用场合很少使用。

由于工业生产环境具有电磁干扰、腐蚀等特点，有时需要长距离传输，因此工业以太网中，通常使用的物理传输介质时屏蔽双绞线（TP——Twisted pair）、工业屏蔽双绞线（ITP——Industrial Twisted pair）以及光纤。工业以太网使用 8 芯和 4 芯双绞线，电缆连接方式也有两种：正线（标准 568B）和反线（标准 568A），其中正线也称为直通线，反线也称交叉线。。

1.2 实验目的

（1）以西门子四芯“快速连接”工业以太网线缆为例，掌握其做网线接头的方法。

1.3 实验准备

完成本实验所需准备的实验材料如下：

- 一根西门子四芯工业以太网线缆
- 两个“快接”工业以太网 RJ45 接头
- 一个做线工具



1.4 实验内容

- (1) 了解四芯工业以太网线缆的内部构造；
- (2) 按照实验步骤制作以太网线缆接头并进行测试。

1.5 实验步骤

- (1) 截取一根 500mm 长的工业以太网线



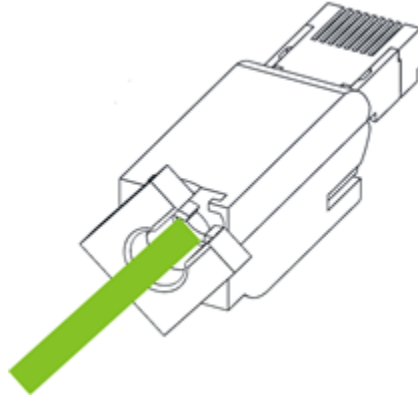
- (2) 线的两端剥去 25mm 长外皮，金属屏蔽网保留 5mm 长。



- (3) 打开金属接头，按照头内线颜色标识把对应线插入到底。



(4) 合拢金属接头，用螺丝刀插入金属圆环的孔内，顺时针旋转 90 度完成固定。



(5) 将制作完成的 ProfiNet 线接到线测试仪上进行测试，1、2、3、6 灯亮为正常。。

1.6 课后作业

- (1) 了解工业以太网四芯和八芯线的区别；
- (2) 了解光纤的种类及其在工业上的应用场合。

实验二 网络配置实验

2.1 实验目的

- (1) 了解网络配置的目的；
- (2) 掌握使用 PST（Primary Setup Tool）工具为交换机和 PLC 分配 IP 地址；
- (3) 掌握通过 WEB 界面配置交换机的方法（以 SCALANCE XM 408-8C L3 为例）。

2.2 实验准备

完成本实验所需准备的材料如下：

- 1 个交换机 SCALANCE XM 408-8C L3（下文简称 SCALANCE XM 408）；
- 1 个 PLC S7 1200；
- 1 个上位机（安装有 PST 软件）；
- 2 根工业以太网线。

2.3 实验内容

- (1) 网络拓扑结构实施，2-1 为网络结构逻辑拓扑图；
- (2) 通过 PST 软件为 SCALANCE XM408 和 S7 1200 分配 IP 地址；
- (3) 通过 WEB 界面，利用 IP 地址对 SCALANCE XM408 进行配置。

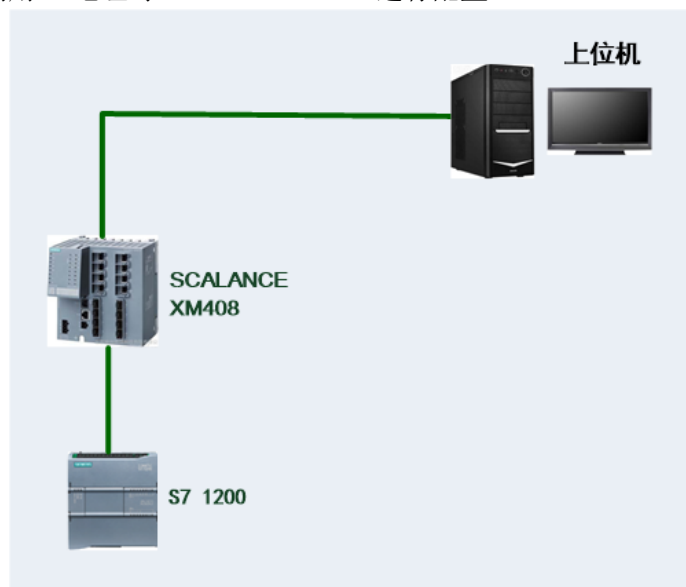


图 2-1 网络配置实验逻辑拓扑结构图

2.4 实验步骤

2.4.1 网络结构实施

- (1) 将 SCALANCE XM408 和 S7 1200 安装到导轨上;
- (2) 用工业以太网线缆将上位机与 SCALANCE XM408 的 P1 端口相连, 将 SCALANCE X408 的 P2 端口与 S7 1200 的以太网接口相连 (说明: 可以使用 SCALANCE XM408 的其他端口与上位机和 S7 1200 相连);
- (3) 接通电源。

2.4.2 配置上位机、SCALANCE XM408 和 S7 1200 的 IP 地址

- 1、为了能够让上位机与网络部件处在一个局域网内, 将上位机的有线网卡的 IP 地址设置为 192.168.0.100, 子网掩码为 255.255.255.0, 如图 2-2 所示。



图 2-2 配置上位机的 IP 地址和子网掩码

- 2、以管理员身份启动 Primary Setup Tool 软件 (以下简称 PST 软件), 界面如图 2-3 所示。

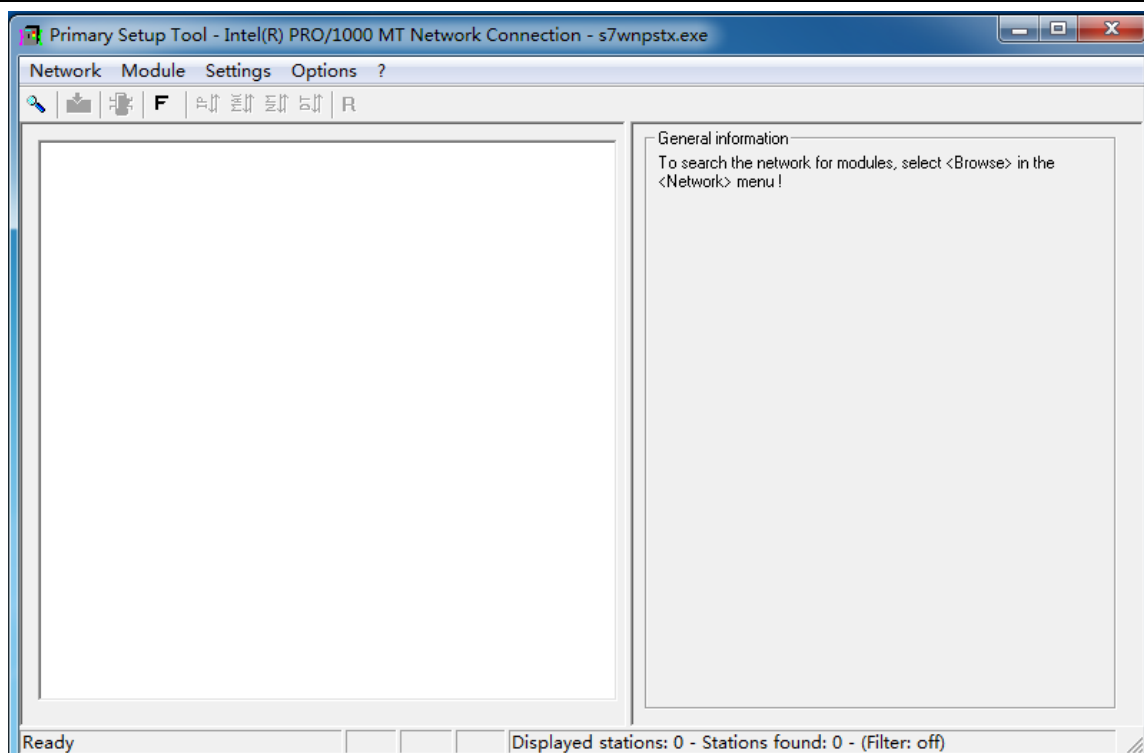


图 2-3 PST 软件主界面

点击 Network→Browse 菜单，PST 软件开始搜索设备，找到设备后如图 2-4 所示。

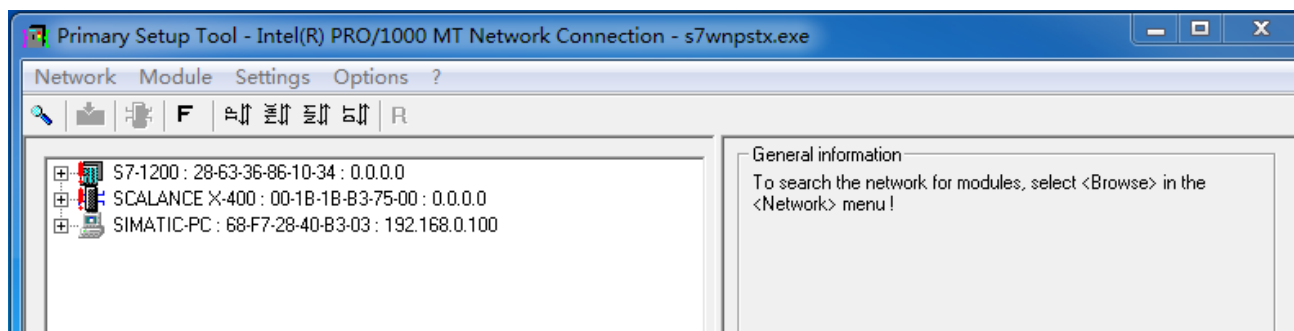



图 2-4 PST 软件搜索到设备后的界面

点击 SCALANCE XM408 前的 , 展开树状结构。选中 Ind. Ethernet interface, 在右侧界面中设置交换机 IP 地址为 192.168.0.11, 子网掩码设置为 255.255.255.0, 如图 2-5 所示。

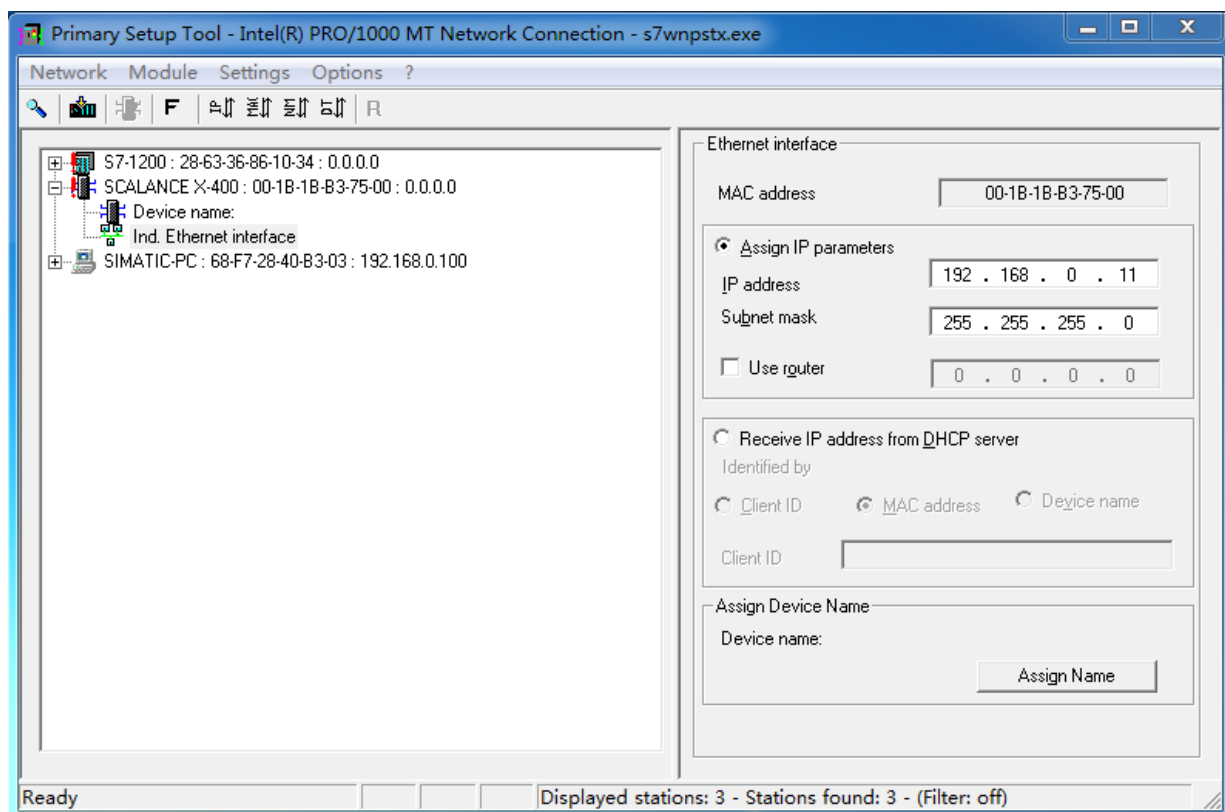


图 2-5 用 PST 软件配置交换机 IP 地址和子网掩码

同理，设置 S7 1200 的 IP 地址为 192.168.0.21，子网掩码设置为 255.255.255.0，如图 2-6 所示。

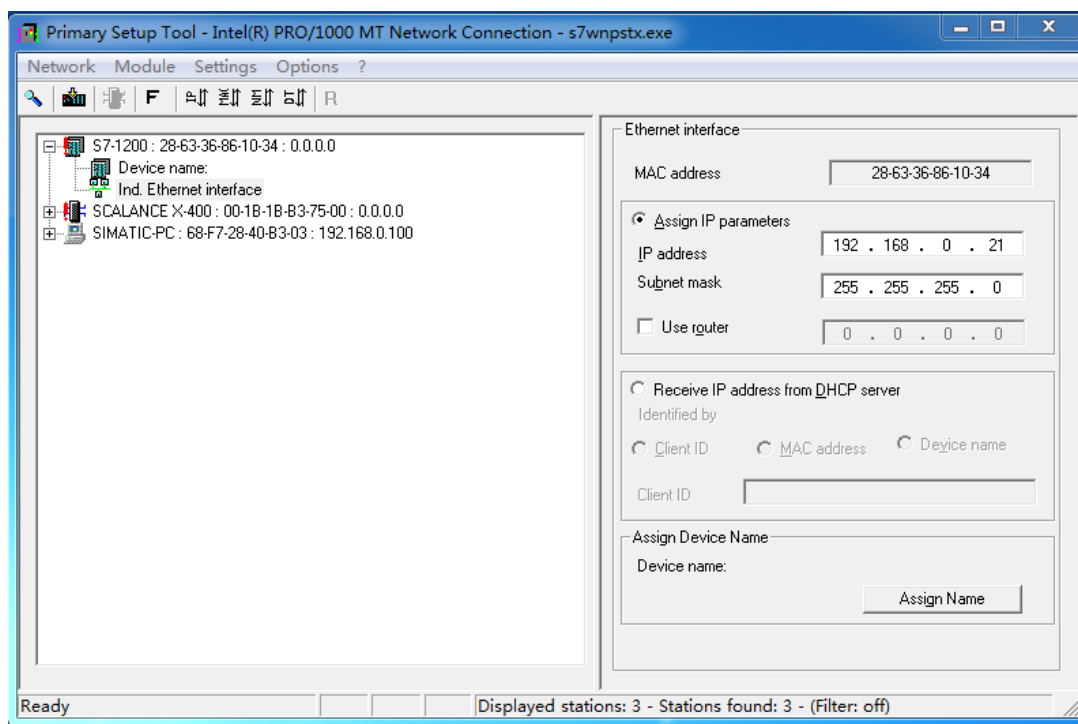




图 2-6 用 PST 软件配置 S7 1200 的 IP 地址和子网掩码

选中 S7 1200 条目，点击工具栏下载按钮 ，将配置下载到 S7 1200 中；选中 SCALANCE XM408 条目，点击工具栏下载按钮 ，将配置下载到 SCALANCE XM408 中。

2.4.3 通过浏览器配置交换机

本小节通过简单的配置示例展示交换机的配置方法。

1、打开浏览器，在地址栏中输入 192.168.0.11，进入 SCALANCE XM408 的网络配置登录界面。输入用户名 admin 和密码（默认都为 admin）后，弹出提示框，如图 2-7 所示。点击“OK”按钮后，进入密码修改界面，如图 2-8 所示，设置好新密码后，点击“Set Values”按钮，保存密码设置配置，此时网页自动进入 SCALANCE XM408 配置界面，如图 2-9 所示。SCALANCE XM408 配置界面包含 5 个部分，即“Information”、“System”、“Layer 2”、“Layer 3”和“Security”。点击这 5 个部分的任意一个子项，在配置界面的右上方会出现一个问号，点击问号，将弹出对该子项进行说明的帮助界面，如图 2-10 所示。

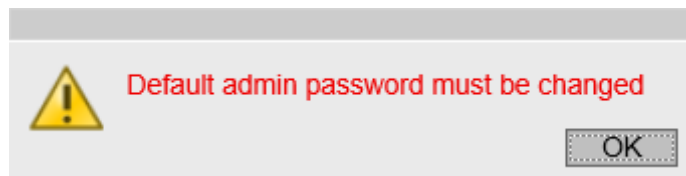


图 2-7 要求修改密码提示框

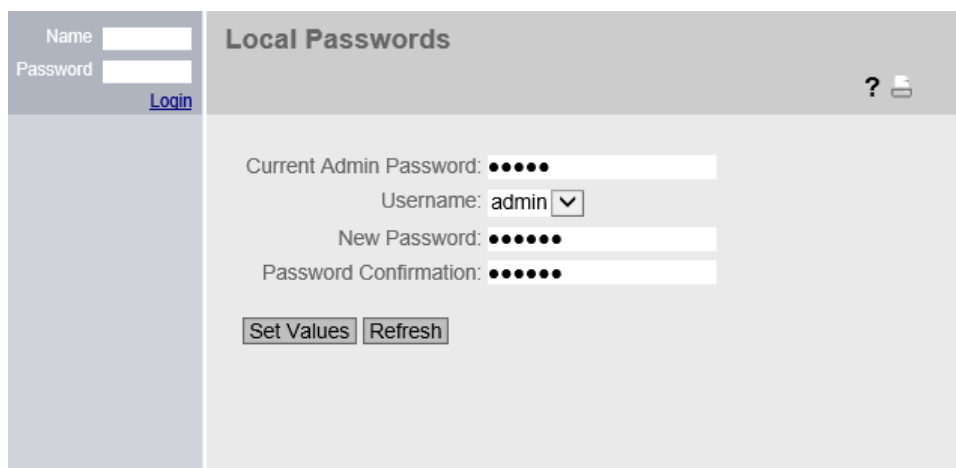
The "Local Passwords" configuration page. On the left, there is a sidebar with "Name" and "Password" input fields and a "Login" button. The main area contains fields for "Current Admin Password" (masked with dots), "Username" (set to "admin" with a dropdown arrow), "New Password" (masked with dots), and "Password Confirmation" (masked with dots). At the bottom are "Set Values" and "Refresh" buttons. A question mark icon is in the top right corner.

图 2-8 SCALANCE XM408 初始密码设置界面

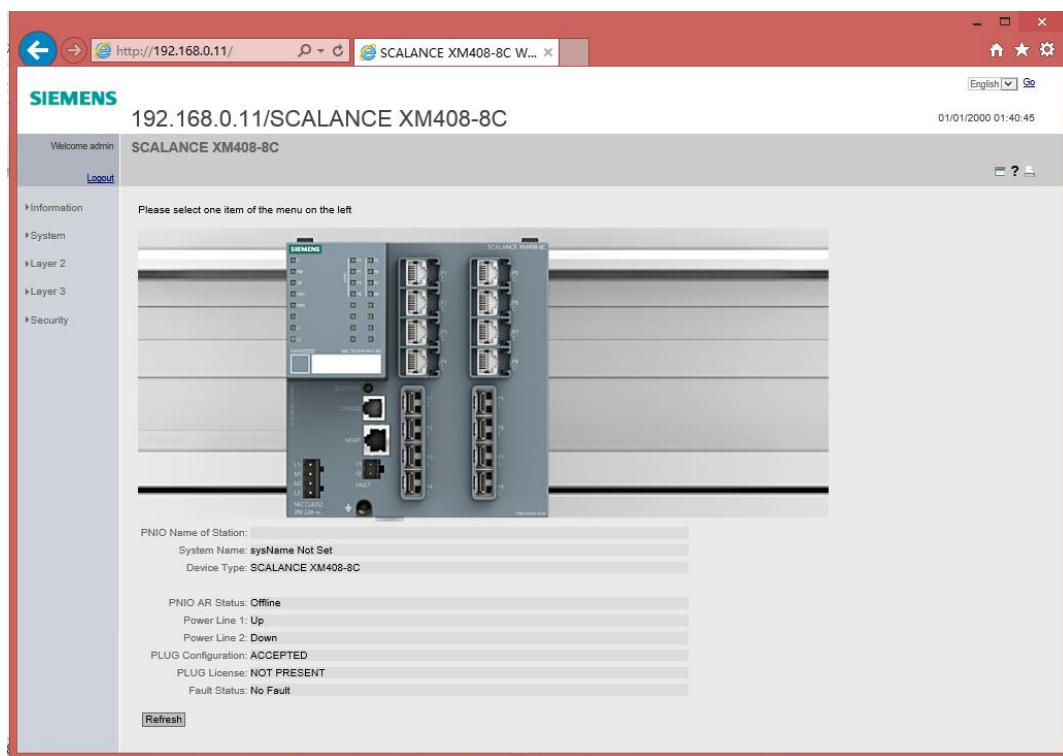


图 2-9 SCALANCE XM408 网络配置主界面

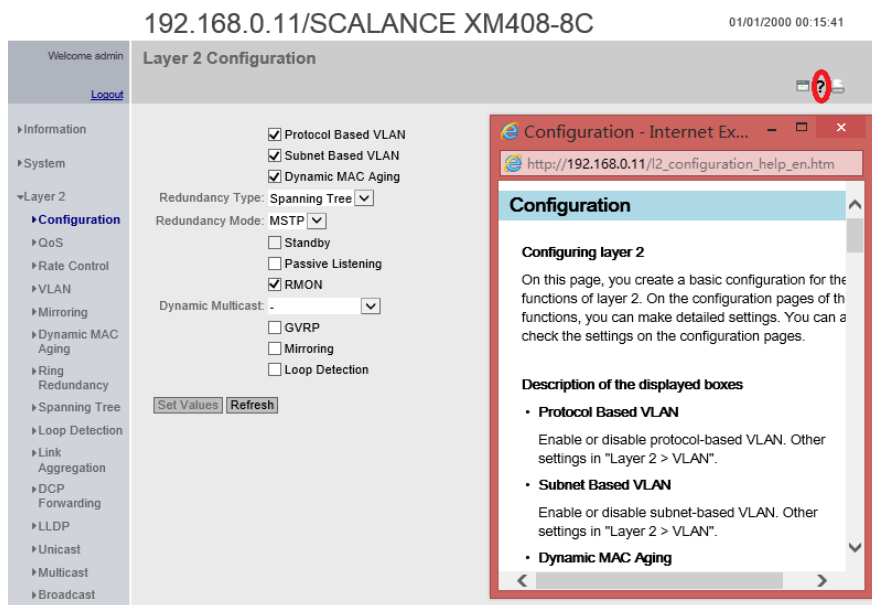



图 2-10 XM408 帮助界面

2、任何时候，点击 XM408 右上角的，将弹出 XM408 模块指示灯监视界面，如图 2-11 所示。

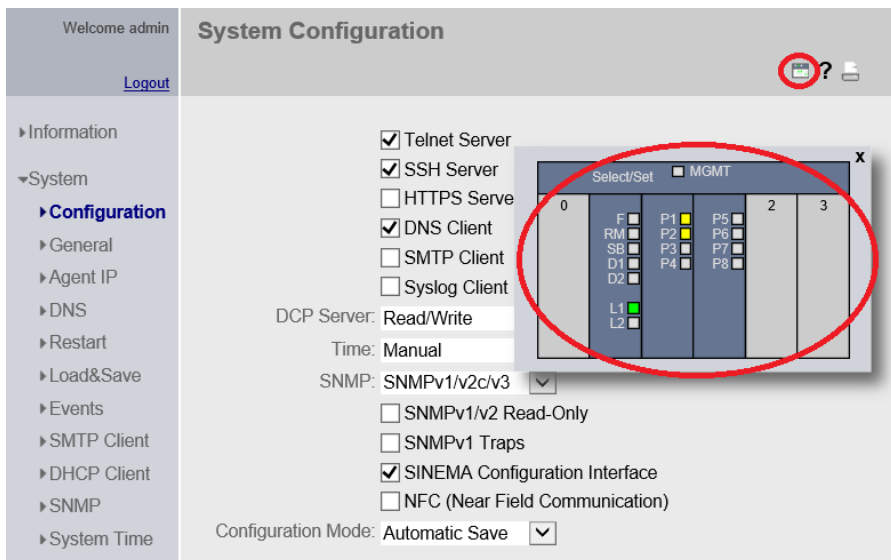


图 2-11 XM408 模块指示灯监视界面

3、在网络配置界面的左侧列表中，选中“Layer 2”下的“Ring Redundancy”。在“Ring Redundancy”界面中，将“Ring Redundancy”前的复选框勾上；在“Ring Redundancy Mode”的下拉列表中选择“HRP Manager”；然后配置在冗余环中使用的“Ring Ports”，如 P1.4 和 P1.8。如图 2-12 所示。

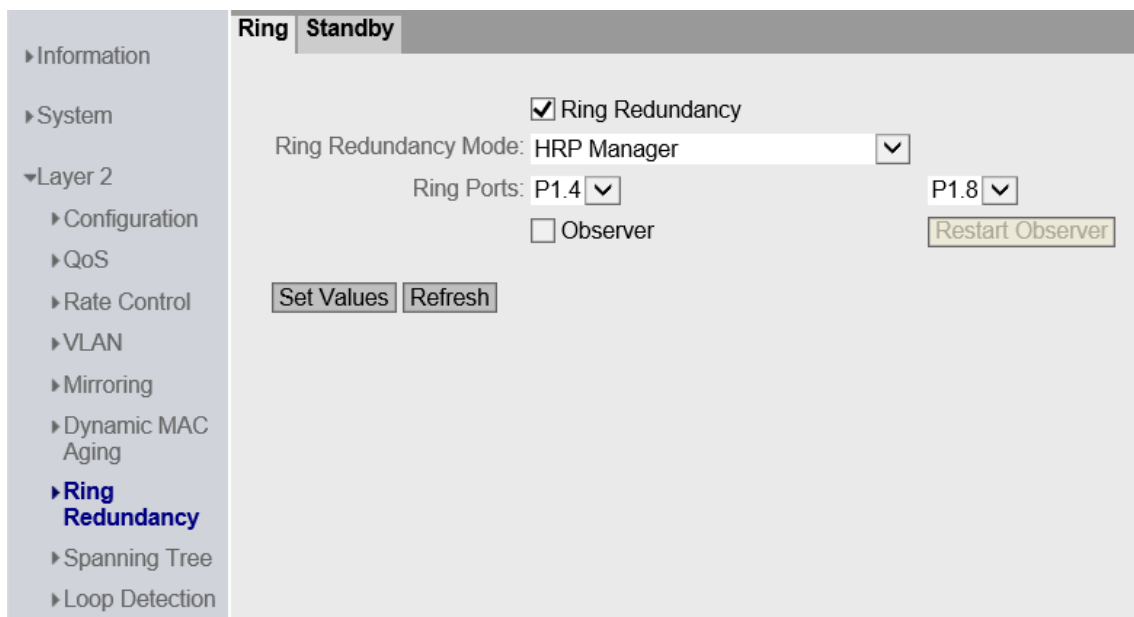


图 2-12 SCALANCE XM408 环形冗余配置界面

注意：第一次对该交换机进行配置时，在勾选“Ring Redundancy”前的复选按钮时，会弹出提示，如图 2-13 所示。这是因为交换机在出厂时默认将 Spanning Tree 选中。此时，需要进入 Layer2 下的 Spanning Tree 界面。在此界面将“Spanning Tree”前的复选框中的“v”勾掉，并点击“Set Values”按钮。如图 2-14 所示。

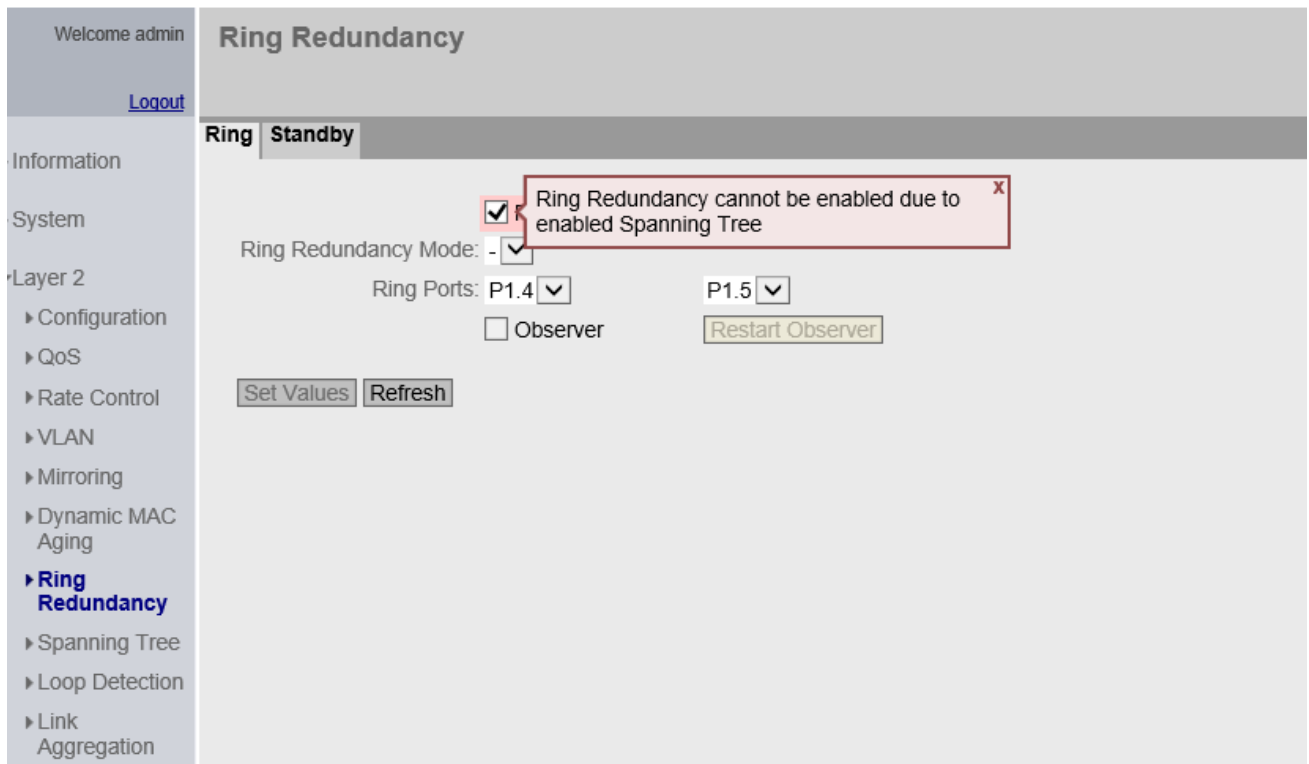


图 2-13 勾选“Ring Redundancy”前的复选按钮时可能弹出的提示

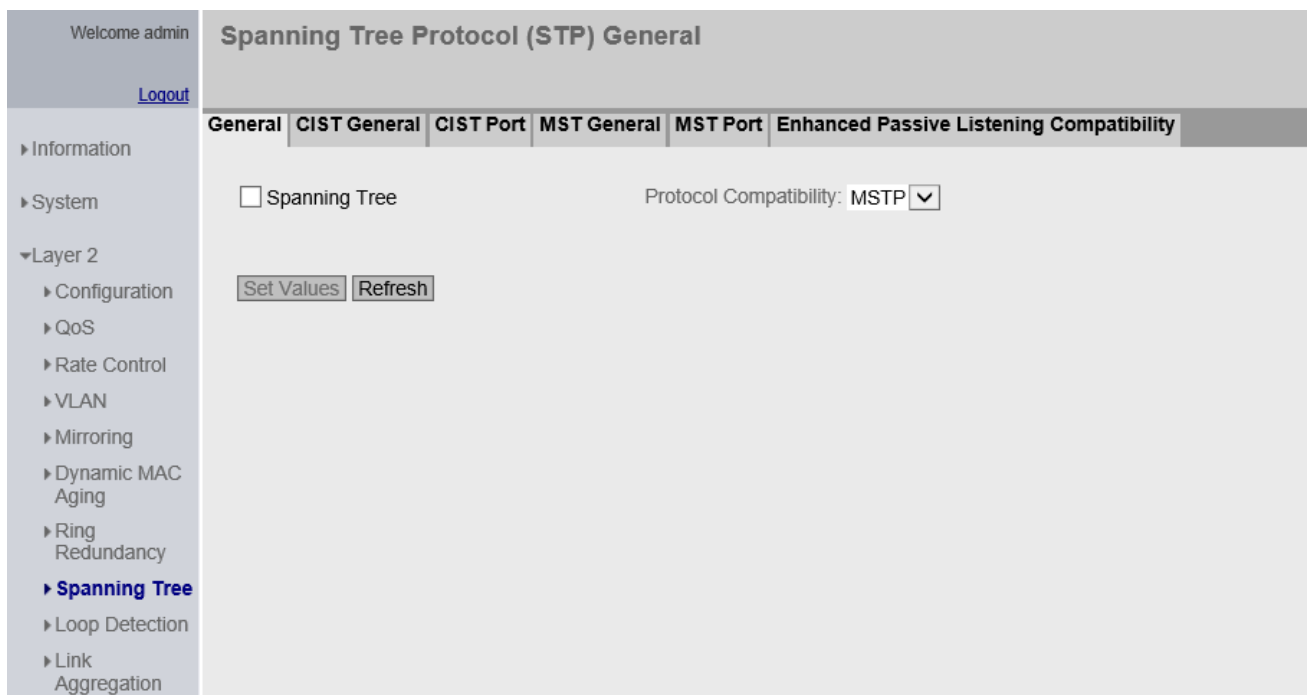



图 2-14 为了设置环形冗余功能勾选掉 Spanning Tree 前的复选框

4、配置好 XM408 的环形冗余参数后，点击“Set Values”按钮。此时，点击 XM408 右上角的，在弹出 XM408 模块指示灯监视界面中可以看到“RM”指示灯为绿色快闪状态，如图 2-15 所示，同时可以看到实际的 XM408 模块的 RM 指示灯也为绿色快闪状态，说明将 XM408 设置为环形冗余管理器的配置过程成功。

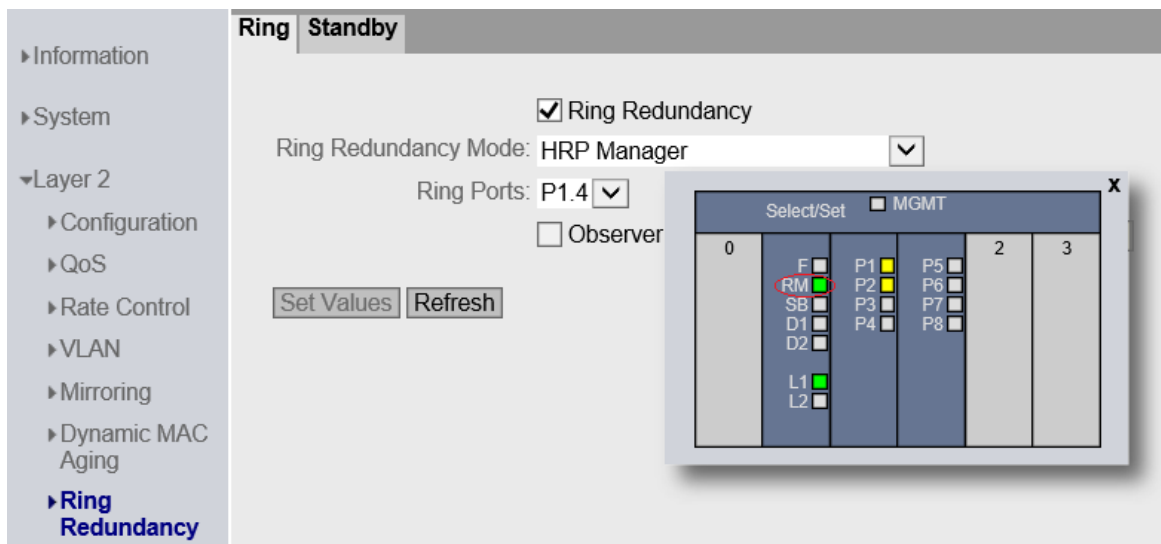


图 2-15 将 SCALANCE XM408 设置为环形冗余管理器后的监视界面

2.5 实验结果核查

- (1) 通过 PST 确认已经为 SCALANCE XM408 和 S7 1200 分配好了 IP 地址；
- (2) 将 SCALANCE XM408 设置完环形冗余管理器后，通过 WEB 监视界面和 SCALANCE XM408 确认“RM”指示灯为绿色快闪状态。

2.6 课后作业

- (1) 通过 WEB，了解 SCALANCE XM408 配置页面的每一项配置功能。

实验三 单环冗余网络实验

3.1 技术背景

网络冗余是工业网络的一项保障策略。作为快速反应备份系统，网络冗余的目的是减轻意外中断的风险，通过即时响应保证生产连续，从而降低关键数据流上任意一点失效所带来的影响。

工业网络对可用性要求较高，环网冗余是提高网络可用性的重要手段。

环形工业以太网技术是基于以太网发展起来的，继承了以太网速度快、成本低的优点，同时为网络上的数据传输提供了一条冗余链路，提高了网络的可用性。

将各台交换机通过冗余环口依次进行连接，即构成了环形网络结构。其中一个交换机作为冗余管理器 RM，管理冗余环网。在一个环网中，只能有一台交换机设置成冗余管理器。冗余管理器 RM 通过发送监测帧监控网络链路状态，在网络正常的情况下，RM 的其中的一个冗余环口会处于逻辑断开状态，这样整个网络在逻辑结构上保持一种线型结构，避免广播风暴（当网络中存在环路，就会造成每一帧都在网络中重复广播，引起广播风暴。）。冗余管理器监控网络状态，当网络上的连接线断开或交换机发生故障时，它会通过连通一个替代路径恢复成另外一种逻辑上的线型结构。如果故障被消除，网络逻辑结构会恢复原有的线型结构。环网可以是电气环网也可以是光纤环网，也可以是电气和光纤混合的环网。

3.2 实验目的

- （1）理解环网冗余的工作原理；
- （2）掌握单环冗余网络的配置及测试方法。

3.3 实验准备

完成本实验所需准备的实验材料如下：

- 1 个 SCALANCE XM408-8C；
- 2 个 SCALANCE XB208；
- 1 个 S7 1200；
- 5 根工业以太网线缆

3.4 实验内容

- （1）通过 WEB 界面配置交换机；
- （2）通过博途软件配置 PLC S7 1200（A），即硬件组态、配置 IP 地址和子网掩码、在变量表中设置；

(3) 网络结构实施，图 3-1 为网络结构拓扑图

①利用工业以太网线缆，将各个交换机通过配置的冗余接口相连，构成高速冗余环网 HSR

②利用工业以太网线缆，将上位机、PLC 与环网中的交换机相连

(4) 通讯测试：将环网中 SCALANCE XM408 的用于通讯的激活的端口的线缆拔掉，观察通讯网络能否重构通讯链路，并保证数据能够从 PLC 传输到上位机。

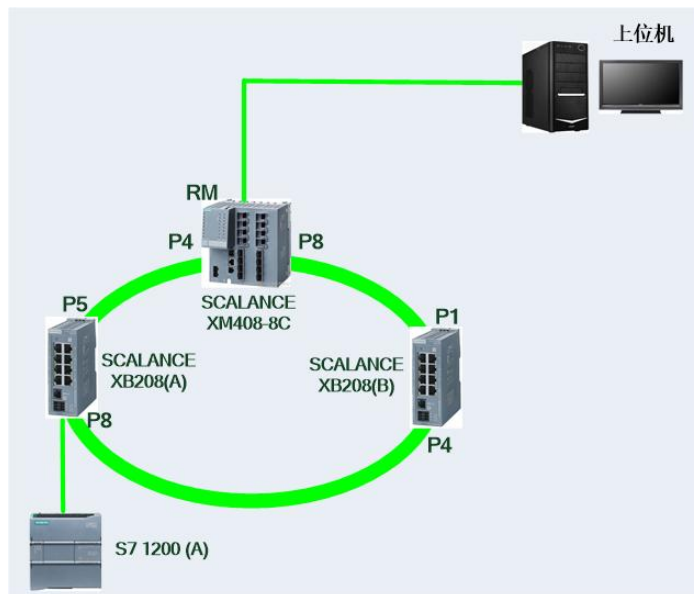


图 3-1 网络结构拓扑图

3.5 实验步骤

注意：在完成三个交换机配置前，不能将三个交换机连成环。

3.5.1 配置上位机的 IP 地址和子网掩码

1、将上位机的有线网卡的 IP 地址设置为 192.168.0.100，子网掩码为 255.255.255.0，如图 3-2 所示。

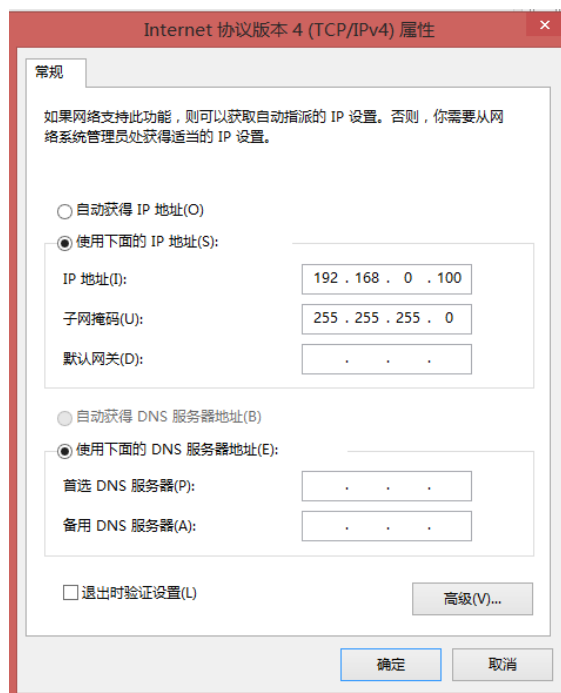


图 3-2 配置上位机的 IP 地址和子网掩码

3.5.2 配置交换机 SCALANCE XM408-8C

- 1、将上位机和 SCALANCE XM408-8C 用以太网线连接。
- 2、以管理员身份启动 Primary Setup Tool 软件（以下简称 PST 软件），界面如图 3-3 所示。

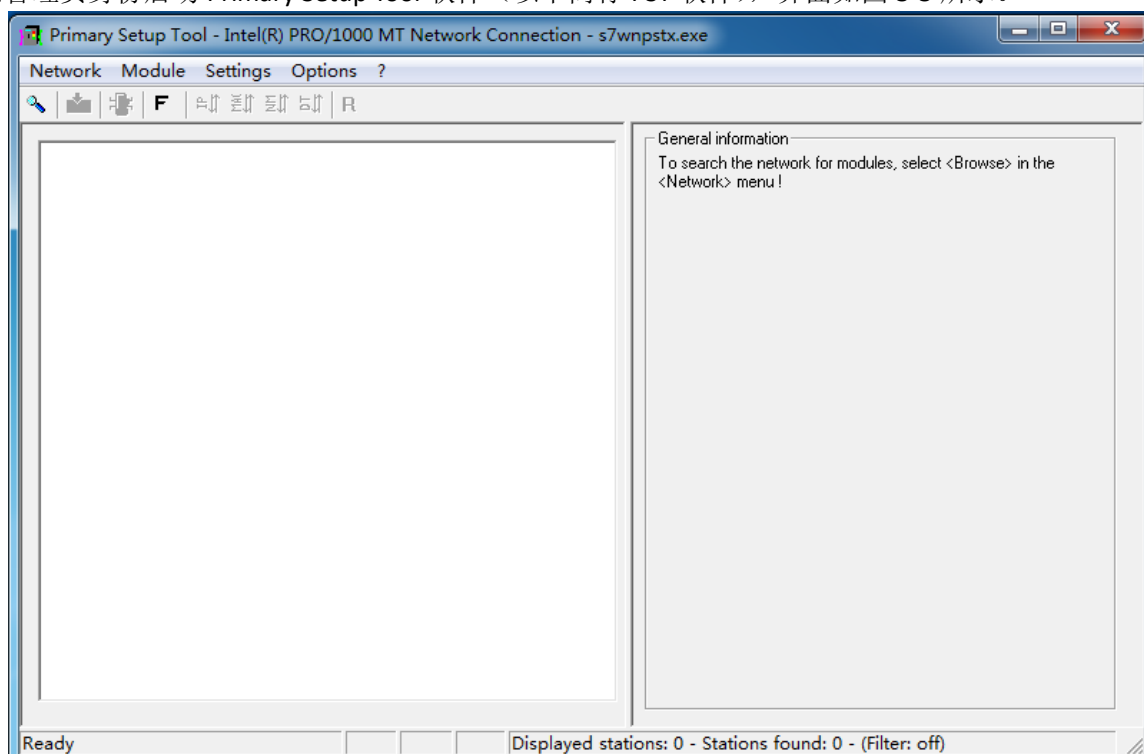


图 3-3 PST 软件主界面

点击 Network→Browse 菜单，PST 软件开始搜索设备，找到设备后如图 3-4 所示。

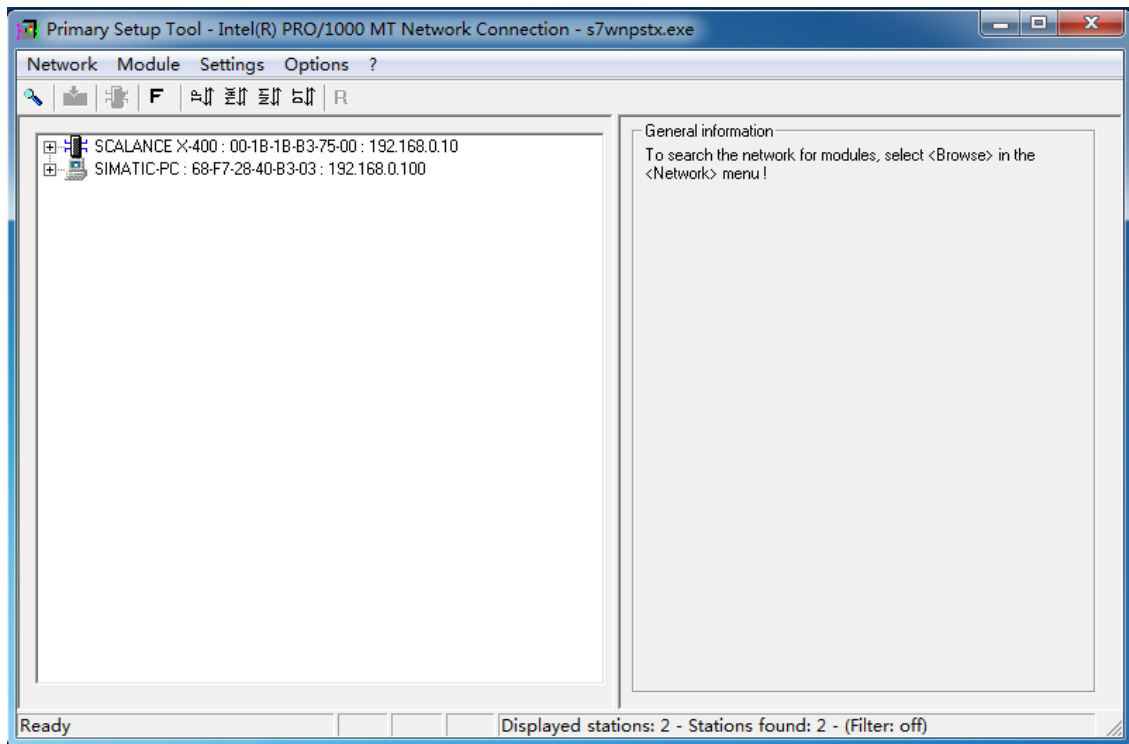



图 3-4 PST 软件搜索到设备后的界面

点击 SCALANCE X-400 前的 ，展开树状结构。选中 Ind. Ethernet interface，在右侧界面中设置交换机 IP 地址为 192.168.0.11，子网掩码设置为 255.255.255.0，如图 3-5 所示。

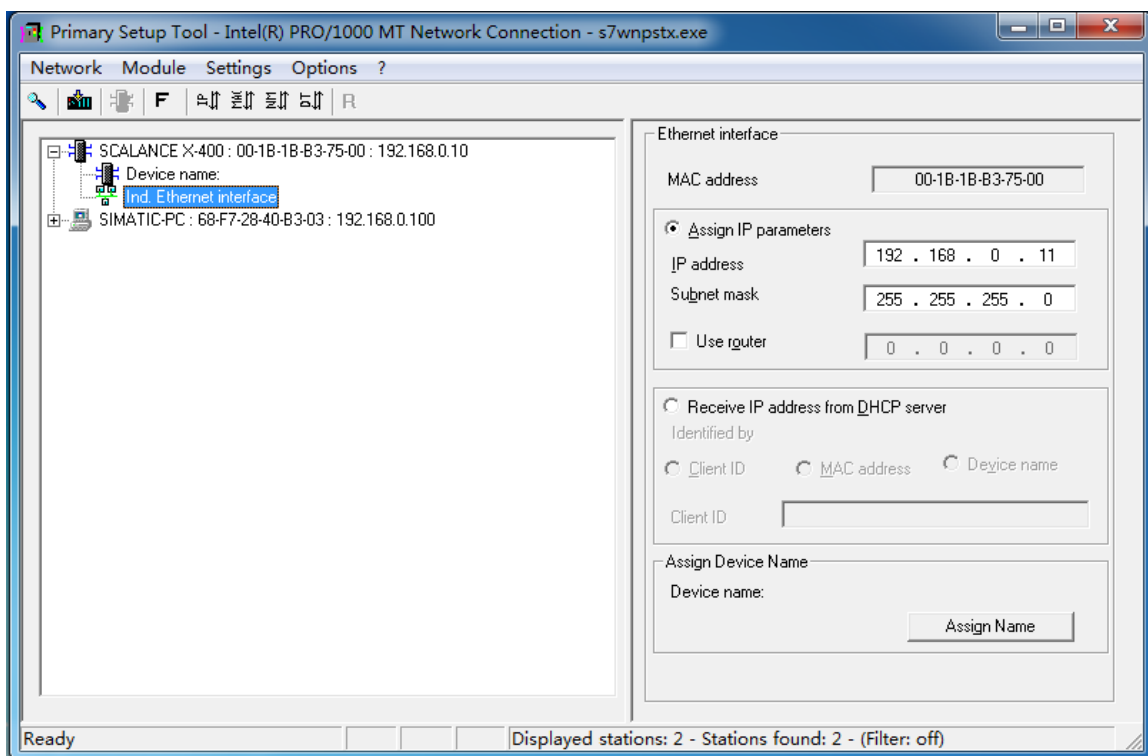



图 3-5 用 PST 软件配置交换机 IP 地址和子网掩码

点击工具栏下载按钮 ，将配置下载到交换机 SCALANCE XM408-8C 中。

3、打开浏览器，在地址栏中输入 192.168.0.11，进入 SCALANCE XM408-8C 的网络配置登录界面（首次进入

该页面需要修改密码)。输入用户名 **admin** 和密码后，进入 **SCALANCE XM408-8C** 配置界面，如图 3-6 所示。

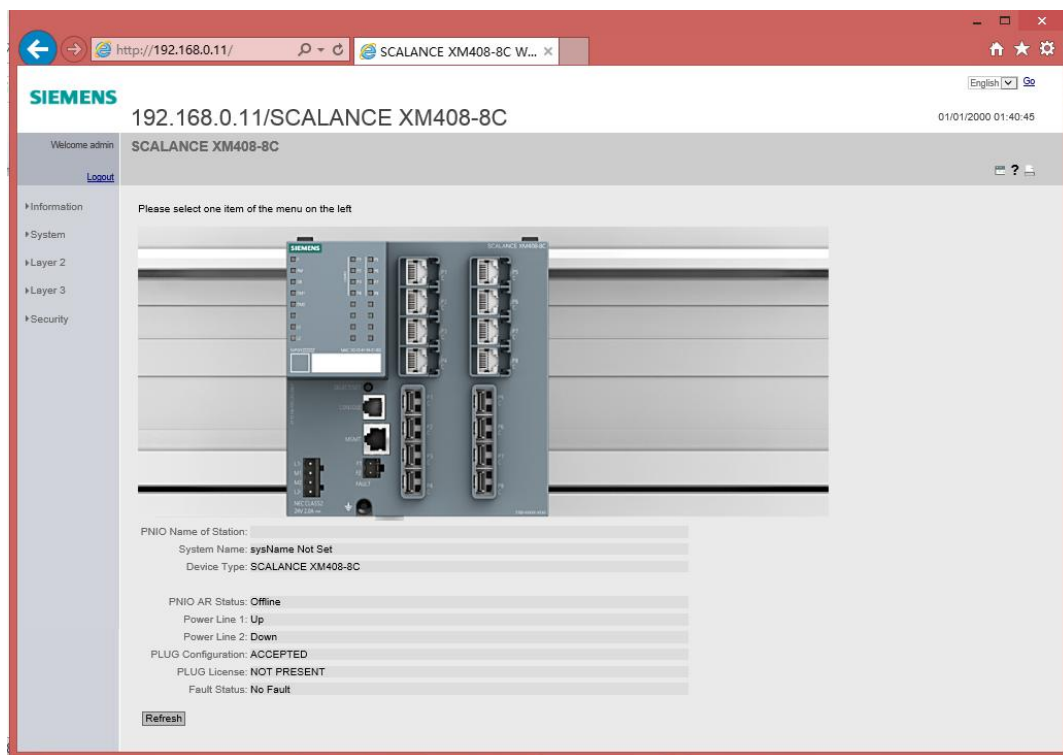


图 3-6 SCALANCE XM408-8C 网络配置主界面

4、在网络配置界面的左侧列表中，选中“Layer 2”下的“Ring Redundancy”。在“Ring Redundancy”界面中，将“Ring Redundancy”前的复选框勾上；在“Ring Redundancy Mode”的下拉列表中选择“HRP Manager”；然后配置在冗余环中使用的“Ring Ports”，P1.4 和 P1.8。如图 3-7 所示。

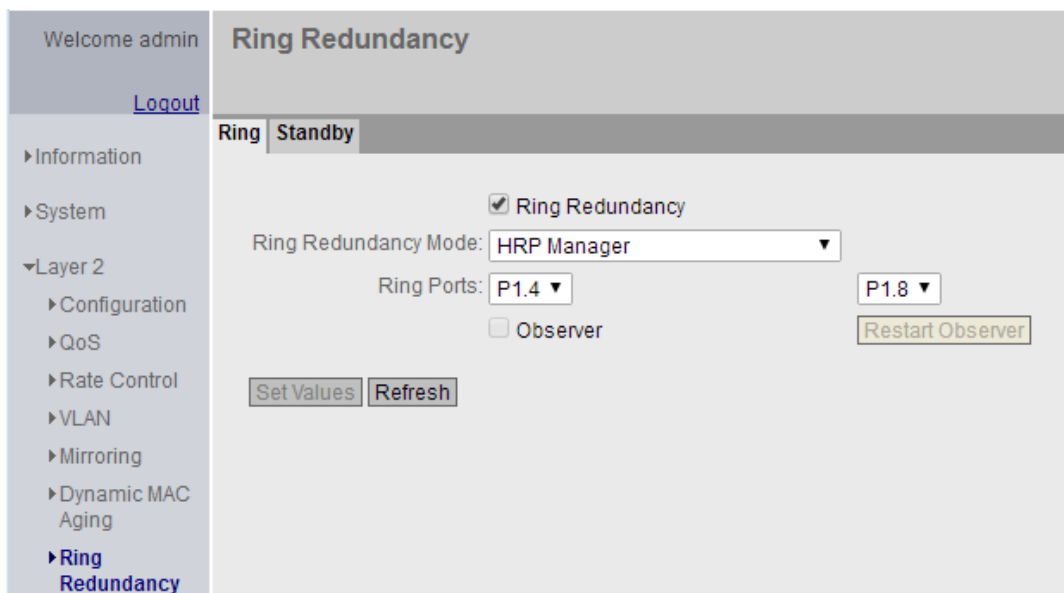


图 3-7 SCALANCE XM408-8C 环形冗余配置

注意：第一次对该交换机进行配置时，在勾选“Ring Redundancy”前的复选按钮时，会弹出提示，如图 3-8 所示。这是因为交换机在出厂时默认将 **Spanning Tree** 选中。此时，需要进入 **Layer2** 下的 **Spanning Tree** 界面。在此界面将“Spanning Tree”前的复选框中的“√”勾掉，并点击“Set Values”按钮。如图 3-9 所示。

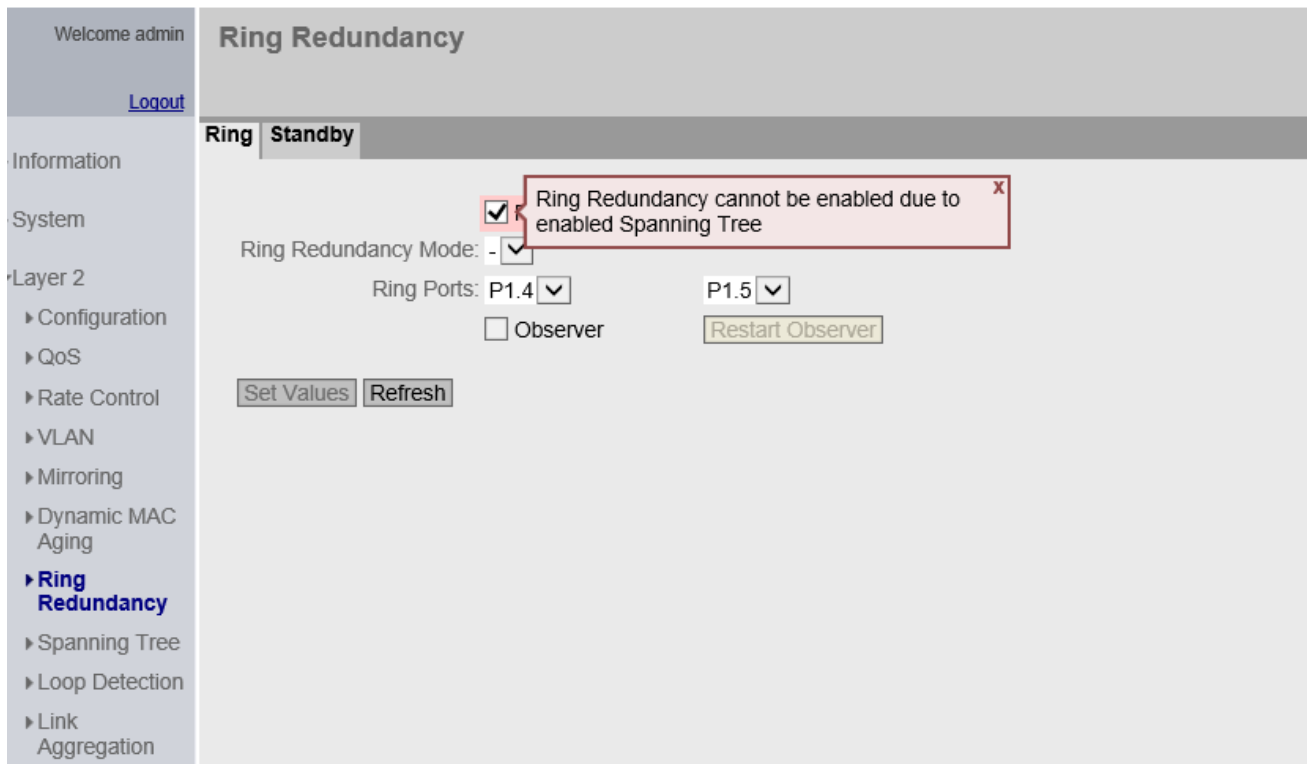


图 3-8 勾选“Ring Redundancy”前的复选按钮时可能弹出的提示

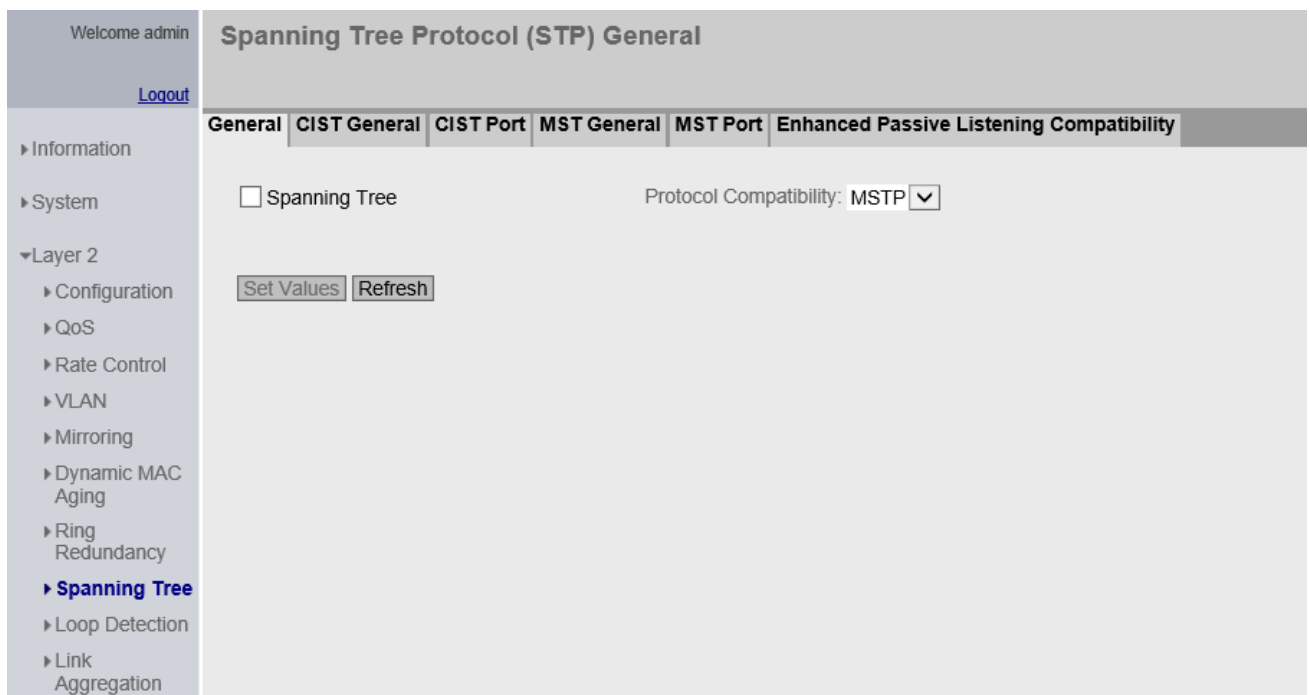



图 3-9 为了设置环形冗余功能勾选掉 Spanning Tree 前的复选框

3.5.3 配置 SCALANCE XB208(A)

1、使用 PST 软件，配置 SCALANCE XB208(A)的 IP 地址为 192.168.0.12，子网掩码设置为 255.255.255.0，点击

工具栏下载按钮 ，将配置下载到交换机 SCALANCE XB208(A)中。

2、打开浏览器，在地址栏中输入 192.168.0.12，进入 SCALANCE XB208 的网络配置登录界面。输入用户名 admin 和密码（默认为 admin）后，进入 SCALANCE XB208 配置界面，如图 3-10 所示。

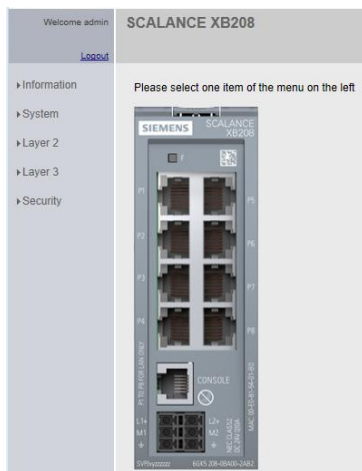


图 3-10 SCALANCE XB208 网络配置主界面

3、在网络配置界面的左侧列表中，选中“Layer 2”下的“Ring Redundancy”。在“Ring Redundancy”界面中，将“Ring Redundancy”前的复选框勾上；在“Ring Redundancy Mode”的下拉列表中选择“HRP Client”；然后配置在冗余环中使用的 Ring Ports，将“P0.5”（第 5 个端口）和“P0.8”（第 8 个端口）设置为冗余端口。如图 3-11 所示。

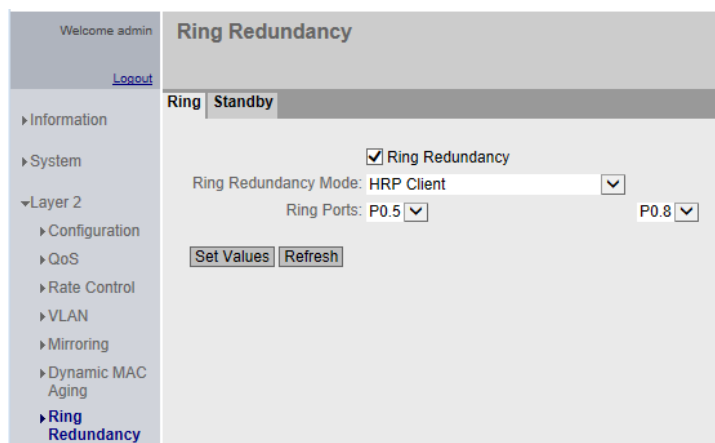



图 3-11 SCALANCE XB208(A)环形冗余配置

3.5.4 配置 SCALANCE XB208(B)

1、使用 PST 软件，配置 SCALANCE XB208(B)的 IP 地址为 192.168.0.13，子网掩码设置为 255.255.255.0，点击工具栏下载按钮 ，将配置下载到交换机 SCALANCE XB208(B)中。

2、打开浏览器，在地址栏中输入 192.168.0.13，进入 SCALANCE XB208(B)的配置界面。在配置界面的左侧列

表中，选中“Layer 2”下的“Ring Redundancy”。在“Ring Redundancy”界面中，将“Ring Redundancy”前的复选框勾上；在“Ring Redundancy Mode”的下拉列表中选择“HRP Client”；然后配置在冗余环中使用的 Ring Ports，将“P0.1”（第 1 个端口）和“P0.4”（第 4 个端口）设置为冗余端口。如图 3-12 所示。

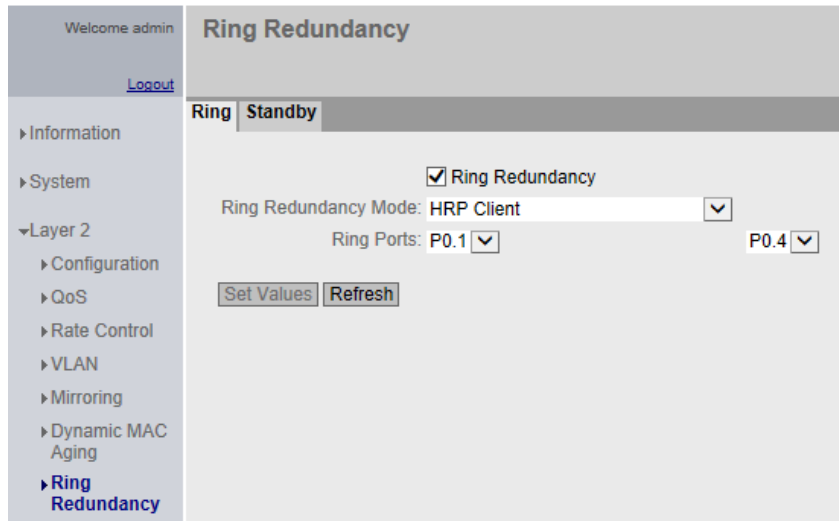


图 3-12 SCALANCE XB208(B)环形冗余配置

3.5.5 在博途中配置 PLC S7 1200(A)（即网孔板上左侧的 S7 1200）

在博途中配置 PLC 的目的是利用博途软件对 PLC 中的变量进行监视，同时测试 I/O 变量在通讯网络中的传输过程。

- 1、在博途软件中，在“硬件目录”中选择正确订货号的 S7 1200，添加到“设备视图”中；在“硬件目录”中选择正确订货号的信号板，拖拽到“设备视图”中 S7 1200 中信号板位置上；
- 2、在“设备视图”中选中 S7 1200 模块，在博途的“属性”界面中为其配置 IP 地址为 192.168.0.41 和子网掩码 255.255.255.0；
- 3、在博途软件“项目树”中，找到“CPU 1214C”并在其树状结构的子项中找到“PLC 变量”，在“PLC 变量”的子项中，双击打开“默认变量表”。在“默认变量表”中添加需要监视的 DI、DO、AI、AO 变量。本例添加了 4 个 DI 变量，如图 3-13 所示。（说明：这四个变量与操作面板中的“S7 1200(A)区域的四个钮子开关对应”）

默认变量表							
名称	数据类型	地址	保持	在 H...	可从 ...	注释	
1 DI_0	Bool	%I0.0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
2 DI_1	Bool	%I0.1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
3 DI_2	Bool	%I0.2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
4 DI_3	Bool	%I0.3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		
5 <添加>			<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		

图 3-13 在博途中配置需要监视的变量

5、编译程序

6、下载程序到 S7 1200 (A) 中。

3.5.6 网络线缆连接

1、将 3 个交换机连成环网

按照每个交换机环形冗余配置界面中配置的“Ring Port”号，将三个交换机连成环网。此时可以看到：

(1) SCALANCE XM408 的 RM 指示灯常亮，因为 CALANCE XM408 为 HRP Manager；(2) SCALANCE XM408 的两个 Ring Port 4 和 8 对应的指示灯一个快闪（如 P8），一个慢闪（如 P4），慢闪端口对应的通讯线路处于“热备”状态（即暂时不通）。

2、将 S7 1200 (A) 与 SCALANCE XB208(A)连接。

5、利用工业以太网线将 SCALANCE XM408 与安装有博途软件的上位机连接。

3.5.7 环形冗余通讯测试

1、正常通讯测试

正常情况下，从 S7 1200(A)到上位机的信息的传输路径如图 3-14 所示。

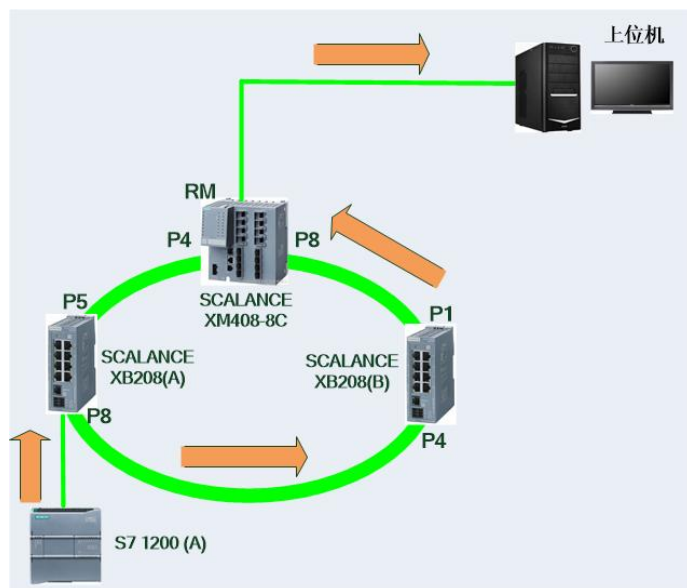


图 3-14 正常情况下从 S7 1200(A)出发到上位机的信息传输路径图

① 在博途软件“项目树”中，选中“CPU 1214C”项，点击工具栏中的“转到在线”按钮，然后在“PLC 变量”的子项中，双击打开“默认变量表”。在“默认变量表”中点击“全部监视”按钮。变量监视界面如图 3-15 所示。显示 DI_0 与 DI_2 对应变量值为 TRUE，DI_1 与 DI_3 对应变量值为 FALSE，与实际开关状态一致。说明此时的数据传输路径“S7 1200(A)→XB208(A)→XB208(B)→XM408→上位机”是通的，且数据传输正确。

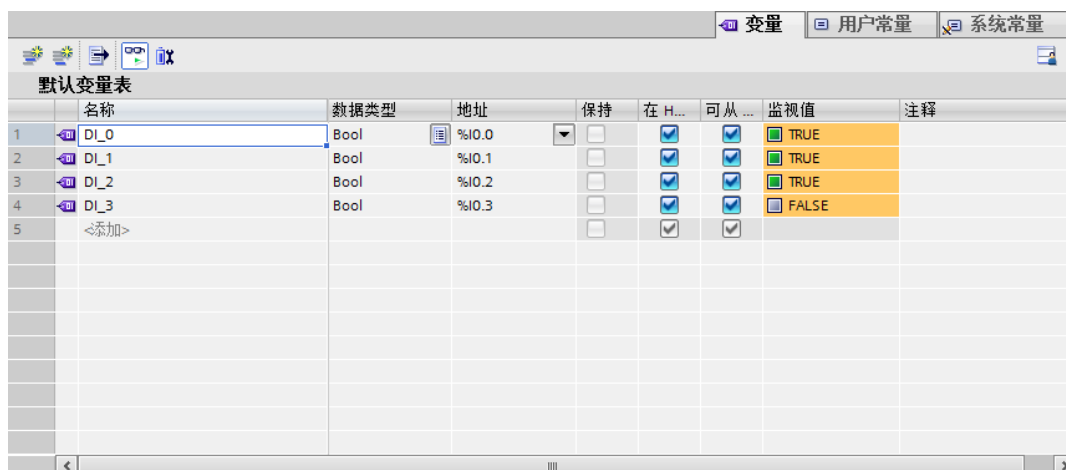


名称	数据类型	地址	保持	在 H...	可从 ...	监视值	注释
DI_0	Bool	%I0.0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	TRUE	
DI_1	Bool	%I0.1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	FALSE	
DI_2	Bool	%I0.2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	TRUE	
DI_3	Bool	%I0.3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	FALSE	
<添加>			<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		

图 3-15 正常通讯时的变量监视界面

2、环网通讯故障测试

将插入 SCALANCE XM408 的 P8 端口的网线拔掉，模拟环网中 XM408 与 XB208(B)交换机之间某一处通讯线路故障或损坏。此时 XM408-8C 的 4 端口立刻变为快闪状态，说明该端口已经“激活”，同时 RM 指示灯变为快闪，提示网络结构已经改变，网络中已经有地方出现故障。现在修改 S7 1200 (A) 的 DI 输入，即改变 IO 操作面板上 S7 1200(A)部分的钮子开关状态，此时博途变量监视界面中的变量值将相应改变，如图 3-16 所示。说明环网在网络故障情况下进行了重构，数据通过另一路径“S7 1200(A)→XB208(A)→XM408→上位机”进入到上位机，且数据传输正确。网络重构后从 S7 1200(A)到上位机的信息传递路径如图 3-17 所示。



名称	数据类型	地址	保持	在 H...	可从 ...	监视值	注释
DI_0	Bool	%I0.0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	TRUE	
DI_1	Bool	%I0.1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	TRUE	
DI_2	Bool	%I0.2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	TRUE	
DI_3	Bool	%I0.3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	FALSE	
<添加>			<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		

图 3-16 环网重构后变量监视界面

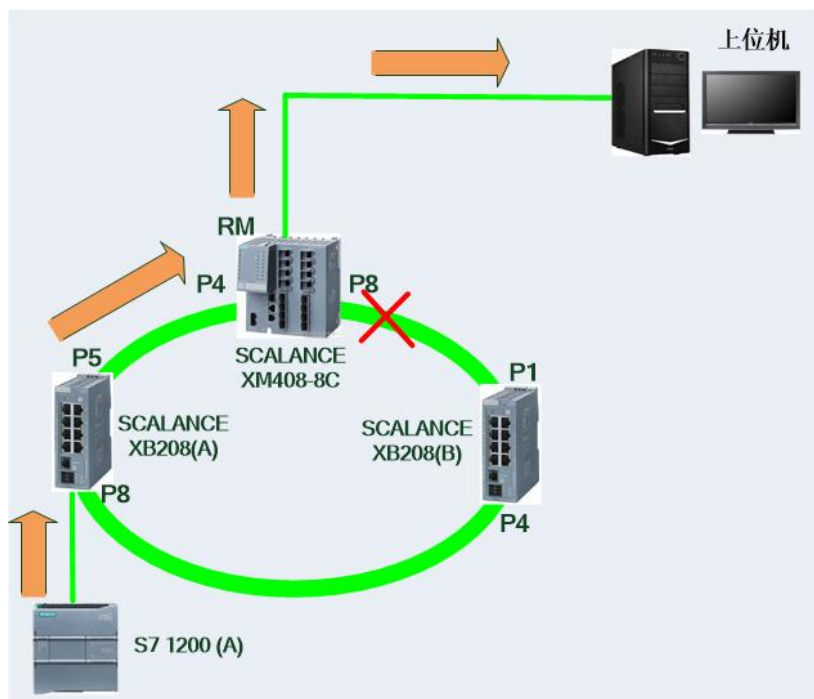


图 3-17 网络重构后从 S7 1200(A)到上位机的信息传递路径

3、环网通讯故障恢复测试

当从 XM408 的 P8 端口断开的线缆重新连接上时，XM408 的 P8 端口指示灯立刻恢复快闪状态，P4 端口立刻恢复为慢闪状态，同时 RM 指示灯变为常亮，说明冗余环网故障已经修复。此时 XM408 检测到网络故障已经恢复，重新将 P4 端口设置为逻辑断开状态。

3.6 课后作业

- 1、在工业通讯过程中为什么要采用环形冗余网络结构？
- 2、在实施环形冗余网络结构时应注意哪些问题？
- 3、环形冗余网络在哪些行业中广泛应用？

实验四 无线通信实验

4.1 技术背景

工业无线通信技术是 21 世纪初新兴的无线通信技术，它面向仪器仪表、设备与控制系统之间的信息交换，是对现有通信技术在工业应用方向上的功能扩展和提升。应用的行业包括石化、冶金、电力、煤炭、烟草、长距离管线、海上石油平台等各行各业。无线传送是指除了网关设备与监控系统之间以有线方式互联外，网关设备与多台无线变送器之间是以无线方式传送数字信号[1]。

工业无线通信技术是在现有智能数字仪表和现场总线技术基础上发展起来的最新技术，它不仅能传送现场设备（如各类变送器）的检测参数的测量值信号（如压力、温度的实时测量值），还可以同时传送多种类型信息，如设备状态和诊断报警、过程变量的测量单位、回路电流和百分比范围、生产商和设备标签等。

基于工业无线技术的测控系统，与传统的有线测控系统相比，具有以下一些优势[2]：

1）低成本。传统的有线测控系统需要布线，一般环境下布线的成本是每米¥300～¥1000，在一些恶劣环境下，可达到每米¥2000。测控系统运行期间需要不断检测系统状态，发现错误并更换电缆。使用工业无线技术将使测控系统的安装与维护成本降低90%，是实现低成本测控系统的关键。

2）高可靠、易维护。在有线系统中，绝大部分系统故障是由电缆或电缆的连接器件损坏而引发的，其维护复杂度大、维护费用高。使用无线技术将彻底杜绝此类故障的发生。工业无线设备可以采用电池供电，利用定时休眠等方法，可持续工作数年以上，维护成本极低。

3）高灵活、易使用。使用无线技术后，现场设备摆脱了电缆的束缚，从而增加了现场仪表与被控设备的可移动性、网络结构的灵活性以及工程应用的多样性，用户可以根据工业应用需求的变化快速、灵活、方便、低成本地重构测控系统。

利用基于工业无线技术的测控系统，人们可以以较低的投资和使用成本实现对工业全流程的“泛在感知”，获取传统由于成本原因无法在线监测的重要工业过程参数，并以此为基础实施优化控制，来达到提高产品质量和节能降耗的目标。

无线网络在工业现场主要应用在设备或环境实现物理连接困难以及技术上不允许或不希望用物理连接的场合，如移动或旋转设备、运动节点、远距离设备管理、障碍物阻隔环境、高危环境等，以弥补有线网络的不足[3]。由于有线和无线通讯都支持 TCP/IP 协议，因此这两种通讯方式能够有机地结合在一起，发挥各自优势。

4.2 实验目的

- （1）掌握工业无线通讯网络的组网方法；
- （2）掌握工业无线通讯网络的配置及测试方法。

4.3 实验准备

完成本实验所需准备的实验材料如下：

- 1 个 SCALANCE XM408-8C;
- 1 个 SCALANCE XB208;
- 1 个 SCALANCE W734 RJ45;
- 1 个 SCALANCE W774 RJ45;
- 1 个 S7 1200;
- 1 套 IO 操作面板;
- 4 根工业以太网线缆;

4.4 实验内容

(1) 网络结构实施

①利用工业以太网线缆，按照如图 4-1 所示的网络结构逻辑拓扑图将交换机与无线模块、交换机与上位机、交换机与 S7 1200 连接起来；

②将 IO 操作面板与 PLC 相连。

(2) 通过上位机中的博途软件配置需要监控的 S7 1200 中的变量

(3) 通讯测试：通过改变 IO 操作面板中的开关状态，查看开关状态数据是否通过 SCALANCE W774 和 SCALANCE 734 两个无线模块传输到上位机。

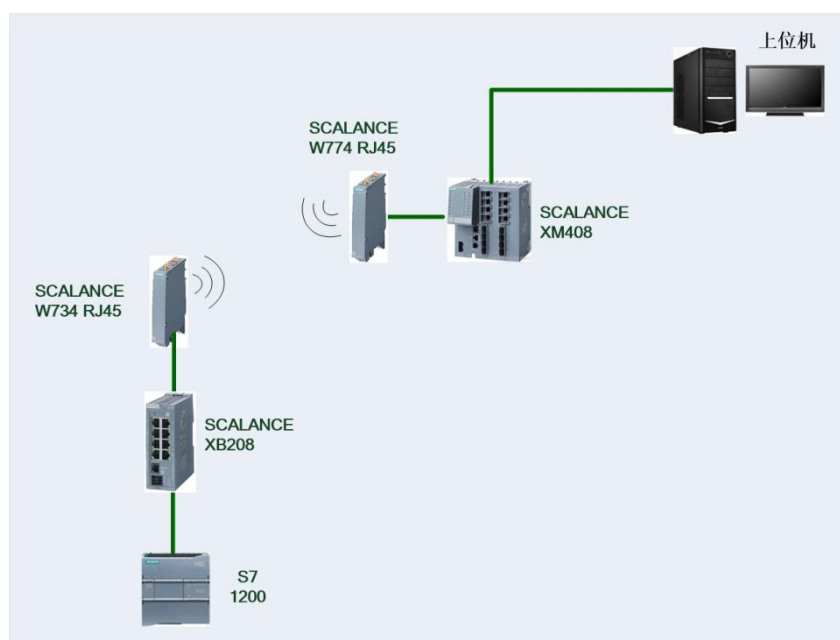


图 4-1 网络结构拓扑图

4.5 实验步骤

4.5.1 网络结构实施

- (1) 将 SCALANCE 408、SCALANCE XB208、SCALANCE W734、SCALANCE W774 和 S7 1200 安装到导轨上；

- (2) 利用工业以太网线缆,按照如图 6-1 所示的网络结构逻辑拓扑图将 SCALANCE 408 的 P3 端口与 SCALANCE W734 的以太网端口相连、SCALANCE W774 的以太网端口与 SCALANCE XB208 的 P5 端口相连、SCALANCE XB208 的 P1 端口与 S7 1200 的以太网端口相连(说明:也可以用交换机的其他端口与无线模块和 PLC 相连);
- (3) 接通电源

4.5.2 配交换机、无线模块和 PLC 配置 IP 地址

由图 6-1 可以看出两个无线模块将网络结构分为上下两个有线连接部分,由于此时上下两个部分没有物理连接且两个无线模块均未指定 IP 地址,因此将上位机与 SCALANCE 408 连接用 PST 设置设备 IP 地址时是无法发现下半部分网络结构中的模块的。所以需要分别为上下两个有线网络部分中的设备分配 IP 地址。

(1) 为上部网络中设备分配 IP 地址

利用工业以太网线缆将上位机与 SCALANCE X408 的空闲以太网口相连。参考“实验二网络配置实验”的 2.4.2 小节,利用 PST 工具将上位机的 IP 地址配置为 192.168.0.100,将 SCALANCE 408 的 IP 地址配置为 192.168.0.11,将 SCALANCE W734 的 IP 地址配置为 192.168.0.31。配置完的界面如图 4-2 所示。

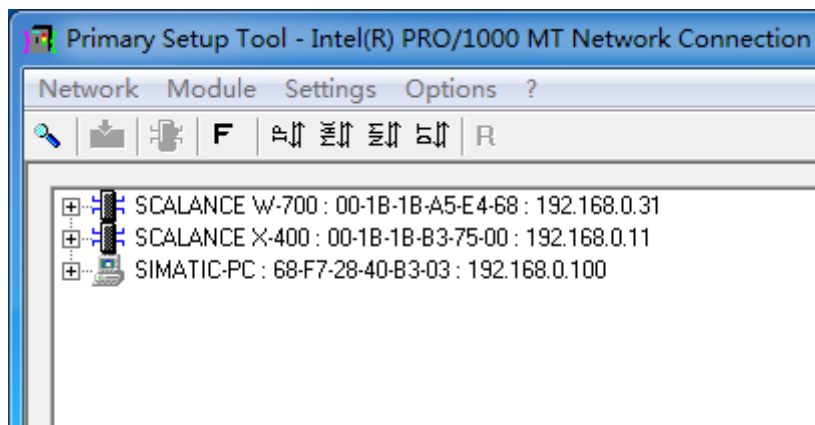


图 4-2 配置上部网络结构中设备的 IP 地址

(2) 为下部网络中设备分配 IP 地址

利用工业以太网线缆将上位机与 SCALANCE XB208 的空闲以太网口相连。参考“实验二网络配置实验”的 2.4.2 小节,利用 PST 工具将 SCALANCE XB208 的 IP 地址配置为 192.168.0.12,将 S7 1200 的 IP 地址配置为 192.168.0.21,将 SCALANCE W774 的 IP 地址配置为 192.168.0.32。配置完的界面如图 4-3 所示。

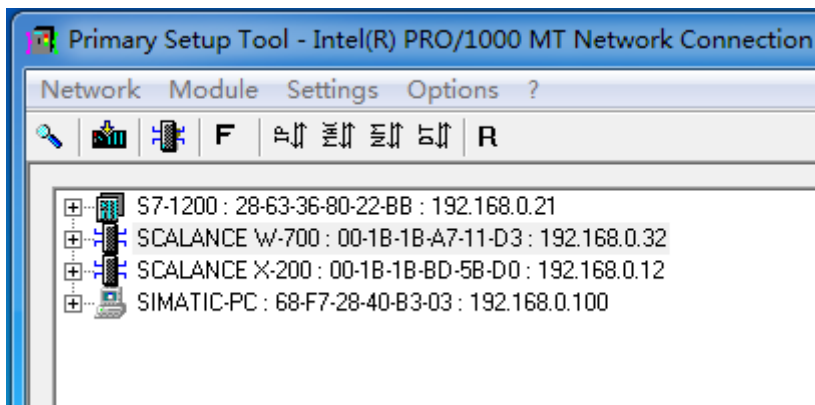


图 4-3 配置下部网络结构中设备的 IP 地址

4.5.3 配置无线模块

(1) 配置 SCALANCE W774

1) 利用工业以太网线缆将上位机与 SCALANCE X408 的空闲以太网口相连。

2) 在上位机的浏览器中输入 SCALANCE W774 的 IP 地址 192.168.0.31, 进入其登陆界面。SCALANCE W774 的默认用户名和密码均为 admin。首次登陆后, 会弹出界面要求修改登陆密码。修改密码后, 将进入 SCALANCE W774 的向导配置界面, 如图 4-4 所示。

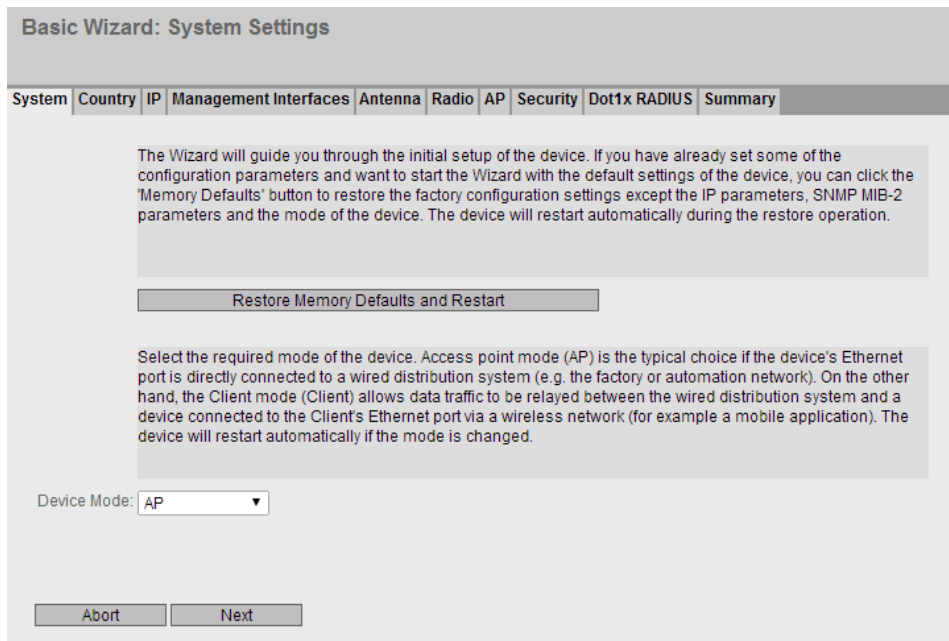


图 4-4 SCALANCE W774 的配置界面

点击配置界面右上角的, 将弹出 SCALANCE W774 模块指示灯监视界面, 如图 4-5 所示。由图 4-5 可以看出“RI”指示灯为白色, 说明该模块的无线功能还未开启。

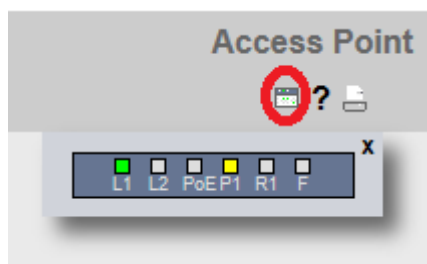


图 4-5 SCALANCE W774 模块指示灯监视界面

重新登陆 SCALANCE W774, 将进入完整的配置界面, 如图 4-6 所示。可以点击左侧“Basic Wizard”以向导的形式进行基本配置, 也可以分别点击左侧“Information”、“System”、“Interfaces”、“Layer2”和“Security”等各项, 进行有针对性的配置。

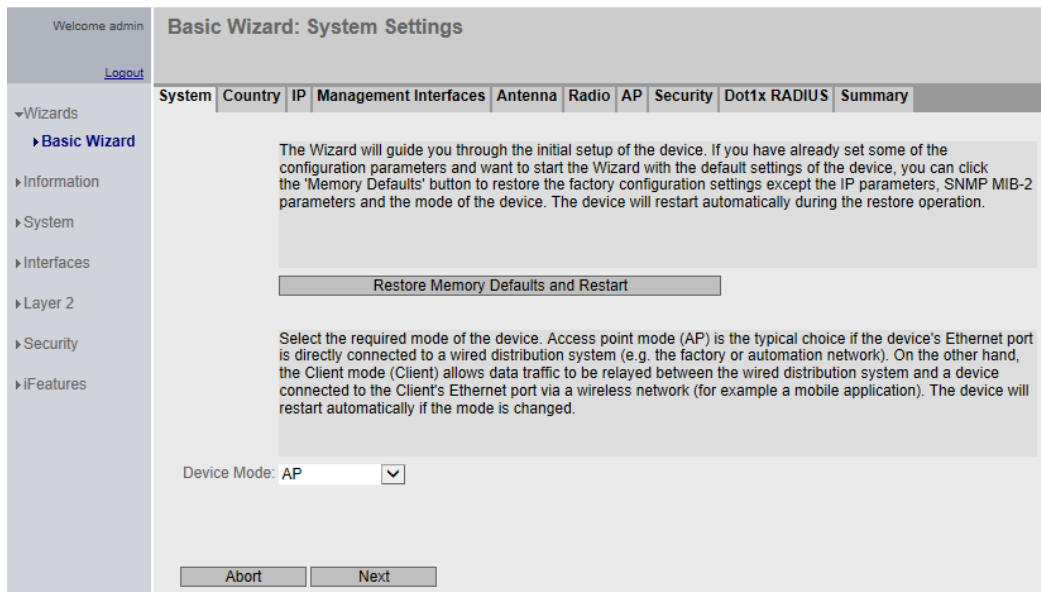



图 4-6 SCALANCE W774 完整配置界面

3) 点击配置界面左侧“Interfaces”的子项“WLAN”进行无线配置。

- 在“Antennas”标签页下，选择“Antenna Type”为“ANT795-4MA”，其他配置保持不变，如图 4-7 所示。最后点击“Set Values”按钮。
- 在“Basic”标签页下，选择“Country Code”为“China”，选中表格中“Enabled”标题栏下的复选框，将“max. Tx Power”值修选择为 17dBm，以便“Tx Power Check”显示为“Allowed”，其他配置保持不变，最后点击“Set Values”按钮。点击配置界面右上角的，在弹出的 SCALANCE W774 模块指示灯监视界面中可以看到“R1”指示灯开始闪烁（说明 SCALANCE W774 的无线功能已经启用），如图 4-8 所示。

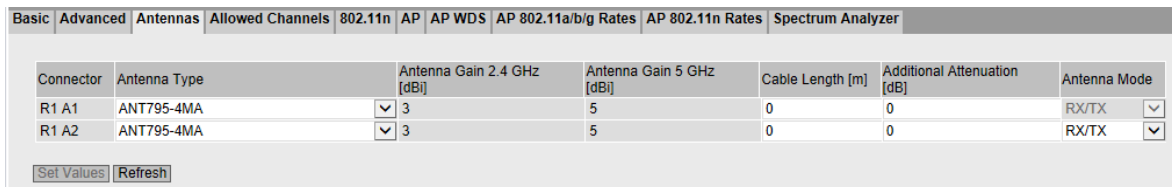


图 4-7 Antennas 配置界面

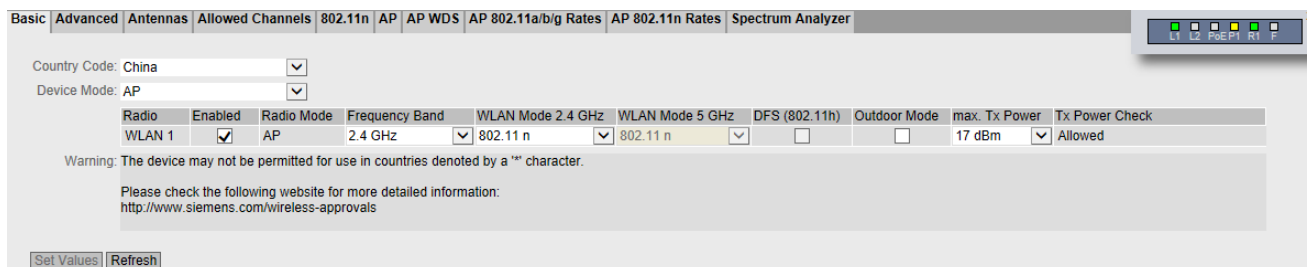


图 4-8 Basic 配置界面

- 在“Allowed Channels”页签，列出了选择频率带宽为 2.4G 或 5G 时可以选择的信道，可以保持默认设置，即所有信道都勾选（设备根据无线环境自适应选择信道），如图 4-9 所示；也可以勾选“Use Allowed Channels only”后，选择特定的信道。


图 4-9 无线信道配置界面

- 在“AP”页签下，可以修改 SSID 号，如 Siemens Wireless 1，要确保要使用的 SSID 号之前的“Enabled”为勾选状态，如图 4-10 所示。

图 4-10 AP 无线 SSID 设置

(2) 配置 SCALANCE W734

- 1) 利用工业以太网线缆将上位机与 SCALANCE XB208 的空闲以太网口相连。
- 2) 在上位机的浏览器中输入 SCALANCE W734 的 IP 地址 192.168.0.32，进入其登陆界面。SCALANCE W734 的默认用户名和密码均为 admin。首次登陆后，会弹出界面要求修改登陆密码。修改密码，重新登陆后，将进入 SCALANCE W734 的向导配置界面（与图 4-4 所示的 SCALANCE W774 的配置界面类似）。
- 3) 点击配置界面左侧“Interfaces”的子项“WLAN”进行无线配置（其配置过程与 SCALANCE W774 的类似）。

- 在“Antennas”标签页下，选择“Antenna Type”为“ANT795-4MA”，其他配置保持不变，最后点击“Set Values”按钮。
- 在“Basic”标签页下，选择“Country Code”为“China”，选择“Device Mode”为“Client”，选中表格中“Enabled”标题栏下的复选框，其他配置保持不变，最后点击“Set Values”按钮。点击配置界面右上角的，在弹出的 SCALANCE W734 模块指示灯监视界面中可以看到“R1”指示灯绿色常亮（说明 SCALANCE W734 的无线功能已经启用）。
- “Allowed Channels”页签页面内容保持不变；

- 在“Client”页签下，设置 SSID 名称为 Siemens Wireless 1，即要与 AP 设置的 SSID 名称一样，以便该客户端能够自动连接到 AP 上。如图 4-11 所示。

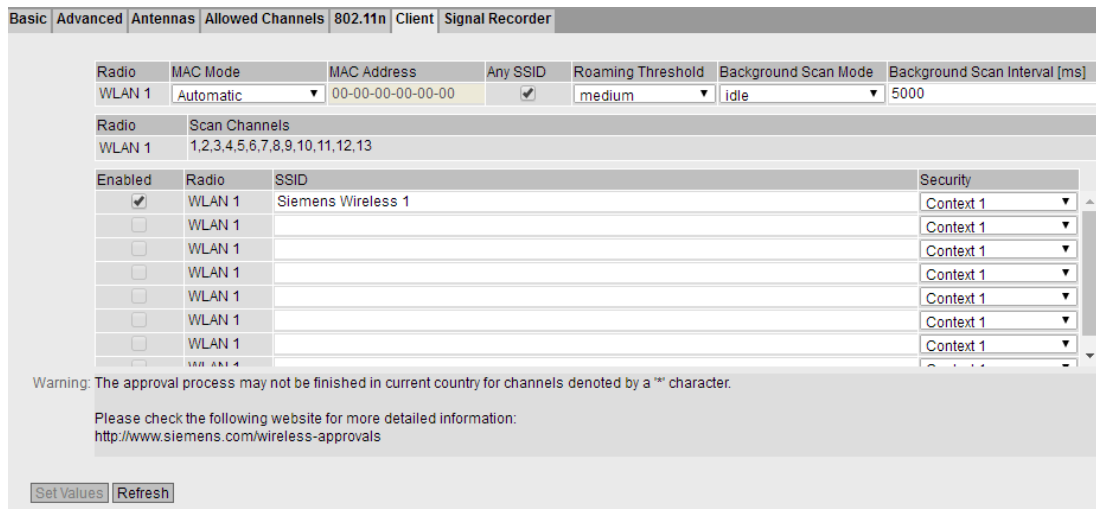


图 4-11 客户端 SSID 名称设置

4.5.4 在博途中配置 PLC

在博途中配置 PLC 的目的是利用博途软件对 PLC 中的变量进行监视，同时测试 I/O 变量在通讯网络中的传输过程。

- 在博途软件中，在“硬件目录”中选择正确订货号的 S7 1200，添加到“设备视图”中；在“硬件目录”中选择正确订货号的信号板，拖拽到“设备视图”中 S7 1200 中信号板位置上；
- 在“设备视图”中选中 S7 1200 模块，在博途的“属性”界面中为其配置 IP 地址和子网掩码（也可使用 PST 为其配置 IP 地址和子网掩码）；

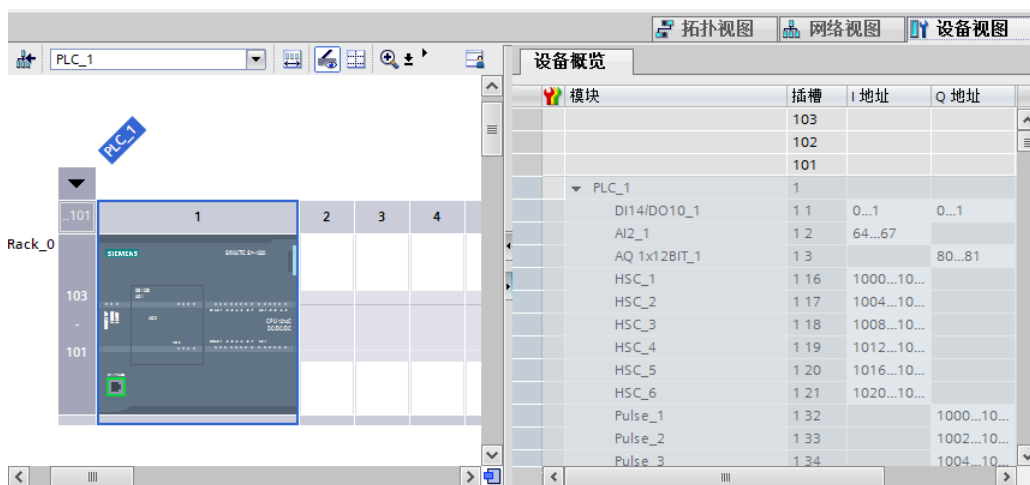


图 4-12 S7 1200 设备视图

- 在博途软件“项目树”中，找到“CPU 1214C”并在其树状结构的子项中找到“PLC 变量”，在“PLC 变量”的子项中，双击打开“默认变量表”。在“默认变量表”中添加需要监视的 DI、DO、AI、AO 变量。本例添加了 4 个 DI 变量，如图 4-13 所示。

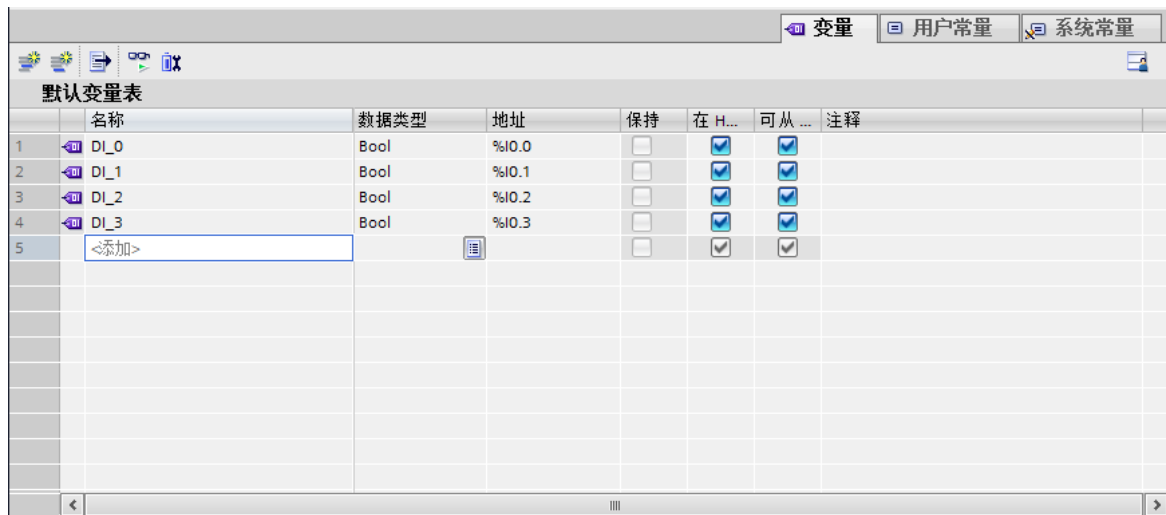


图 4-13 在博途中配置需要监视的变量

5、编译程序

6、下载程序到 IP 地址对应的 S7 1200 中。

4.5.5 通讯测试

在博途软件“项目树”中，选中“CPU 1214C”项，点击工具栏中的“转到在线”按钮，然后在“PLC 变量”的子项中，双击打开“默认变量表”。在“默认变量表”中点击“全部监视”按钮。变量监视界面如图 4-14 所示。4 个 DI 变量值均为 FALSE，与实际开关状态一致。说明此时的数据传输路径“S7 1200→XB208→SCALANCE W734→SCALANCE W774→SCALANCE XM408→上位机”是通的，且数据传输正确。



图 4-14 默认变量表初始监视界面

此时将开关 1 和开关 2 打开，可以看到默认变量表中对应变量 DI_0 与 DI_1 的值均为 TRUE，如图 4-15 所示。



图 4-15 改变开关状态后的变量监视界面

4.6 课后作业

- (1) 写出工业生产过程中使用无线通讯技术的必要性。
- (2) 了解工业无线通讯技术在各领域的具体应用形式。

参考文献：

- [1]方原柏.工业无线通信是推动自动化发展的关键技术[J]. 冶金自动化. 2014, 38 (5) .
- [2]曾鹏, 张华良, 徐皓冬. 工业无线技术在油气行业的应用[J]. 仪器仪表标准化与计量. 2008 (2) .
- [3]燕来荣. 无线网络通信技术将成为工业自动化中的一个新兴热点[J]. 电力电子. 2013 (1) .

实验五 实时通讯实验（通过 PROFINET IO 系统）

5.1 技术背景

对于 PROFINET 技术，已经在实验指导书的“前言”部分的“0.3 PROFINET 简述”部分进行的简述，本实验仅涉及 PROFINET 8 个主要功能模块之一，即 PROFINET 分布式现场设备（PROFINET IO）。

（1）实时通信与 PROFINET 通信[1]

实时是指系统在定义的时间内处理外部事件。确定性是指系统以可预测（确定的）方式进行响应。对于工业以太网，要求具备实时的确定性传输很重要。PROFINET 符合这些要求。因此，PROFINET 可以用作确定的实时通信系统，其功能如下：

- 在保证的时间间隔内传输对时间要求严格的数据。
- 为实现此目的，PROFINET 为实时通信提供优化的通信通道。
- 确保使用其它标准协议的通信可以在同一网络中无故障进行。

PROFINET 通信是通过工业以太网进行的。支持以下传输类型：

- 工程组态数据和诊断数据及中断的非循环传输
- 用户数据的循环传输

PROFINET 通信是以实时方式进行的。

（2）PROFINET IO

PROFINET IO 作为 PROFIBUS International 基于以太网的自动化标准，定义了跨厂商的通信、自动化系统和工程组态模式。作为 PROFINET 的一部分，PROFINET IO 是用于实现模块化、分布式应用的通信概念。PROFINET IO 是用于可编程控制器的 PROFINET 标准(IEC 61158-x-10) 来实现的。

PROFINET IO 具有 PROFIBUS DP 类似的组态、编程和诊断方法，而且有比 PROFIBUS 更高的实时性能。PROFINET IO 在 IO 控制器和 IO 设备之间进行过程数据数据交换。

- IO 控制器：用于对连接的 IO 设备进行寻址的设备。通常是运行自动化程序的控制器。
- IO 设备：分配给某个 IO 控制器的分布式现场设备，例如，分布式 IO、阀终端、变频器和具有集成的 PROFINET IO 功能的交换机。智能设备也可作为 IO 设备，如控制器。

PROFINET IO 是一个基于快速以太网第二层协议的可扩展实时通信系统。根据标准 IEEE802.1Q，PROFINET IO 消息帧优先于标准消息帧。这可以确保自动化技术中要求的确定性。数据通过优先的以太网消息帧来传输。使用 RT 功能，可实现起始值为 250μs 的更新时间。

具有实时通信（RT）功能的 PROFINET IO 是集成 I/O 系统的最优解决方案。该解决方案也可使用设备中的标准以太网以及市场上可购买到的工业交换机作为基础架构部件。不需要特殊的硬件支持。

如果希望使用全部的 PROFINET 功能，必须采用可根据标准 IEC 61158 支持 PROFINET 标准的交换机。在 PROFINET 设备的集成交换机和 PROFINET 交换机中（例如 SCALANCE 产品系列），可执行符合 PROFINET 标准的 PROFINET 功能，且无需对 PROFINET IO 系统中的集成进行限制即可使用该功能。

5.2 实验目的

- （1）掌握配置组态一个 PROFINET IO 系统的方法；

(2) 掌握 PROFINET IO 系统的通信测试方法。

5.3 实验准备

完成本实验所需准备的实验材料如下：

- 2 个 S7 1200;
- 1 个 SCALANCE XB208;
- 1 台工控机;
- 3 根工业以太网线缆。

5.4 实验内容

(1) 网络规划

本实验网络结构为一个星形结构，利用一个 SCALANCE XB208 将两个 S7 1200 和一个上位机互联。

- 作为 IO 控制器的 S7 1200 的 IP 地址为 192.168.0.21，通过 Portal 软件设置；
- 作为 IO 设备的 S7 1200 的 IP 地址为 192.168.0.22，通过 Portal 软件设置；
- SCALANCE XB208 的 IP 地址为 192.168.0.12，通过 PST 工具设置；
- 上位机的 IP 地址为 192.168.0.100，通过在上位机的“Internet 协议版本 4 (TCP/IPv4) 属性”对话框中设置。

(2) 网络结构实施

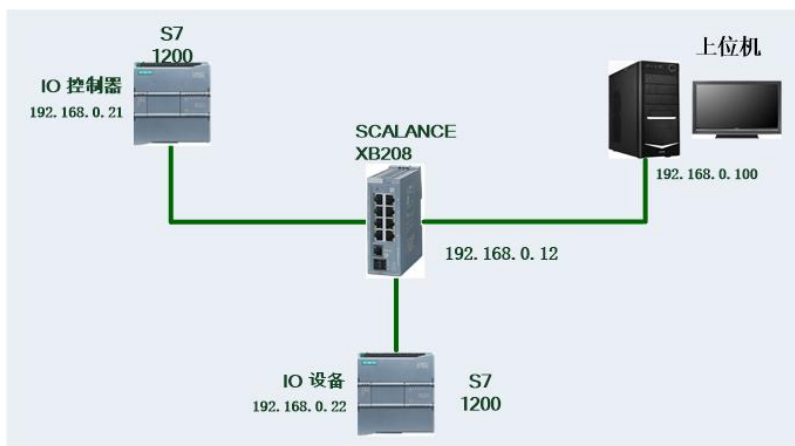


图 5-1 PROFINET IO 实验逻辑网络结构图

(3) 在 Portal 软件中配置 PROFINET IO 系统

(4) 通信测试

5.5 实验步骤

5.5.1 网络结构实施

(1) 利用工业以太网线缆，按照如图 5-1 所示的网络结构图，将作为 IO 控制器的 S7 1200 与 SCALANCE XB208 的 P2 端口连接，将作为智能 IO 设备的 S7 1200 与 SCALANCE XB208 的 P4 端口连接，将上位机与 SCALANCE XB208 的 P6 端口连接。

(2) 接通电源

5.5.2 配置上位机和交换机的 IP 地址

将上位机的 IP 地址配置为 192.168.0.100，子网掩码配置为 255.255.255.0，网关不需配置；参考“实验二网络配置实验”的 2.4.2 小节，利用 PST 工具，将 XB208 交换机的 IP 地址配置为 192.168.0.12。

5.5.3 在 Portal 软件中配置 PROFINET IO 系统

(1) 新建项目

配置 IO 控制器

(2) 在项目中通过“添加新设备”添加 S7 1200 PLC，添加成功后，在设备视图中选中 S7 1200，在属性→常规→项目信息页面中将名称修改为“IO-Controller”；

(3) 设置 IO-Controller 的子网、IP 地址和子网掩码。在设备视图中选中 S7 1200，在属性→常规→PROFINET 接口→以太网地址中设置子网、IP 地址和子网掩码，如图 5-2 所示。

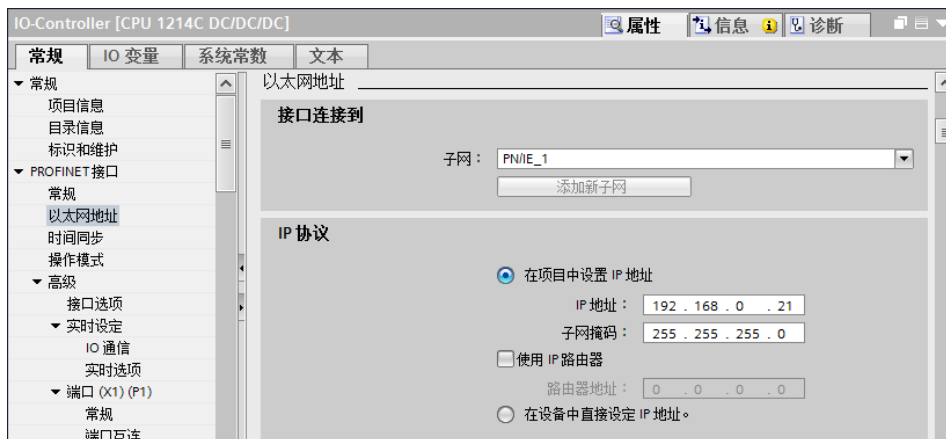


图 5-2 配置 IO 控制器的子网、IP 地址和子网掩码

(4) 属性→常规→PROFINET 接口→操作模式，使用默认配置，即将该 PLC 作为 IO 控制器，如图 5-3 所示。



图 5-3 IO 控制器设置界面

(5)为 IO 控制器添加数据类型为 Byte 的变量，变量名称分别为 Tag_1 和 Tag_2，地址分别为%QB2 和%IB2，如图 5-4 所示。



图 5-4 为 IO 控制器增加变量类型为 Byte 的变量

(6) 添加监控表。项目树→IO-Controller→监控与强制表下双击“添加新监控表”，在新建的“监控表_1”中，在“名称”列下分别选择 Tag_1 和 Tag_2 变量，将显示格式分别设置为二进制和字符，如图 5-5 所示。



图 5-5 在 IO 控制器的监控表中添加监控变量

配置 IO 设备

(7) 在项目中通过“添加新设备”添加 S7 1200 PLC，添加成功后，在设备视图中选中 S7 1200，在属性→常规→项目信息页面中将名称修改为“IO-Device”；

(8) 设置 IO-Device 的子网、IP 地址和子网掩码。在设备视图中选中 S7 1200，在属性→常规→PROFINET 接口→以太网地址中设置子网、IP 地址和子网掩码，如图 5-6 所示。

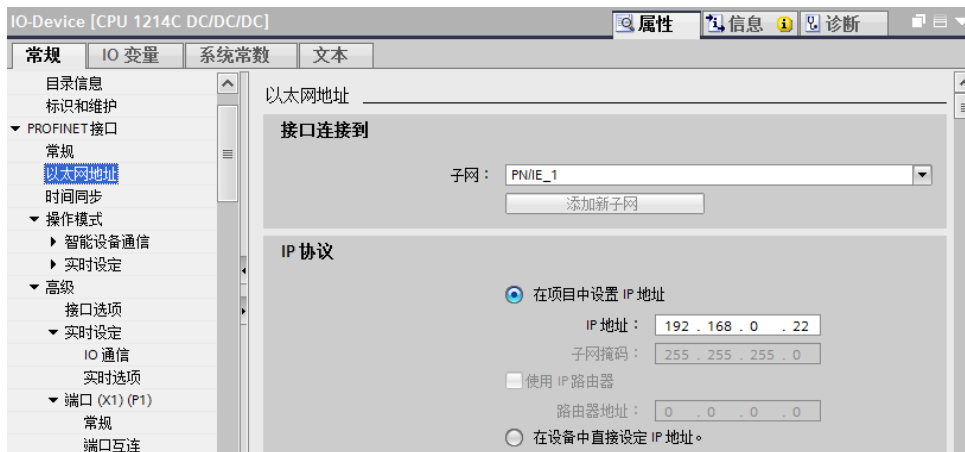


图 5-6 设置 IO 设备的子网、IP 地址和子网掩码

(9) 在设备视图中选中 S7 1200，属性→常规→PROFINET 接口→操作模式，勾选“IO 设备”前的复选框；在“已分配的 IO 控制器”下拉列表中选择 IO 控制器“IO-Controller.PROFINET 接口_1”，如图 5-7 所示。

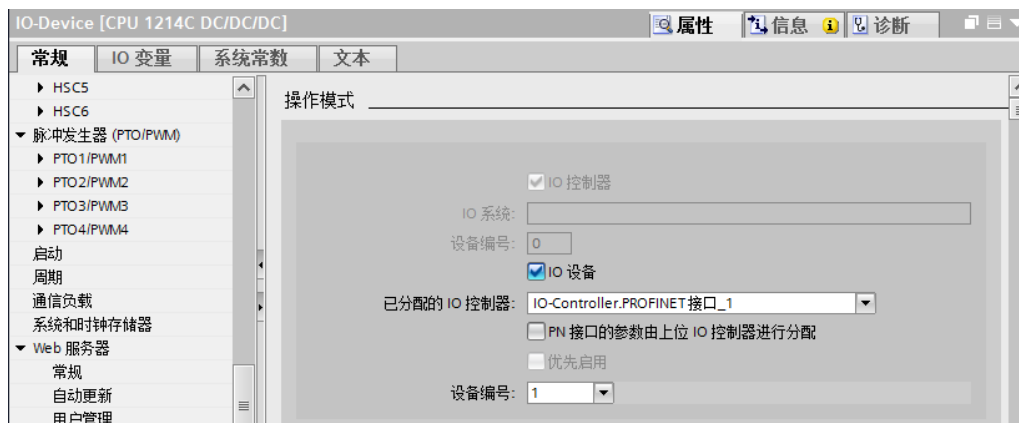


图 5-7 IO 设备配置界面

(10) 为 IO 设备添加数据类型为 Byte 的变量，变量名称分别为 Tag_3 和 Tag_4，地址分别为 %IB2 和 %QB3，如图 5-8 所示。



图 5-8 为 IO 设备添加变量类型为 Byte 的变量

(11) 添加监控表。项目树→IO-Device→监控与强制表下双击“添加新监控表”，在新建的“监控表_1”中，在“名称”列下分别选择 Tag_3 和 Tag_4 变量，将显示格式分别设置为二进制和字符，如图 5-9 所示。

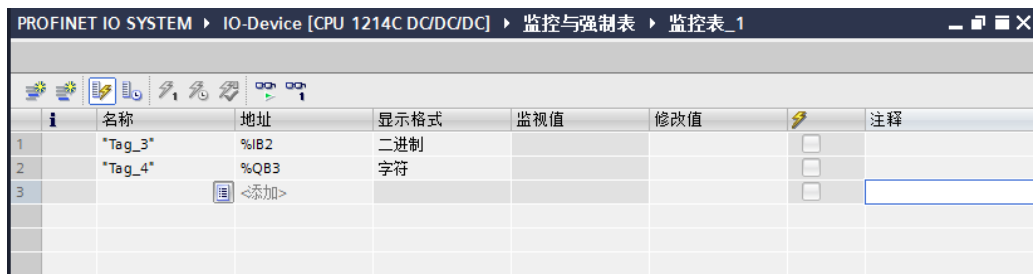


图 5-9 在 IO 设备监控表中添加监控变量

(12) 设置传输区。在设备视图中选中 S7 1200，属性→常规→PROFINET 接口→操作模式→智能设备通信，双击“新增”添加传输区。如图 5-10 所示，增加了两个传输区，第一个传输区表达的是将 IO 控制器中地址为 Q2 的变量的数据传输到智能设备中地址为 I2 的变量中，第二个传输区表达的是将智能设备中地址为 Q3 的变量的数据传输到 IO 控制器中地址为 I2 的变量中。单击箭头，可改变传输方向。



图 5-10 传输区设置

5.5.4 通信测试

将 IO-Controller 和 IO-Device 各自编译下载并运行。

在 IO 控制器的“监控表_1”和 IO 设备的“监控表_1”中，分别点击“全部监视”按钮。

IO 控制器中地址为 Q2 的变量值→智能设备中的地址为 I2 的变量值传输测试：

在 IO 控制器的“监控表_1”中，“在 Tag_1”行的修改值处右键，选择修改为 1，如图 5-11（1）所示，监视值将变为与修改值一样的数值，如图 5-11（2）。

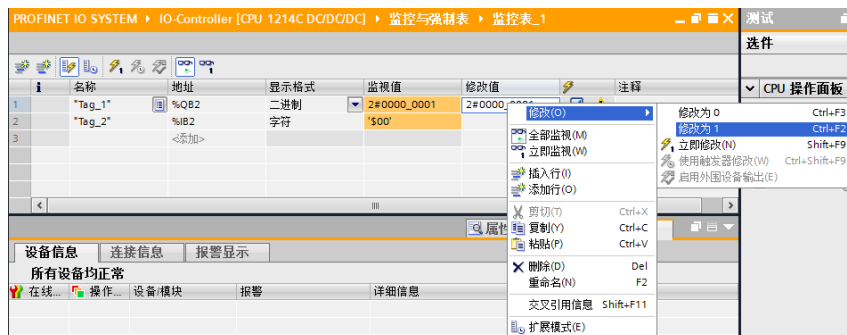


图 5-11（1）修改 IO 控制器中地址为 %QB2 的值



图 5-11（2）修改 IO 控制器中地址为 %QB2 的值

切换到 IO 设备的“监控表_1”，可以看到 IO 设备的 %IB2 地址已经收到来自 IO 控制器发送过来的数据，如图 5-12 所示。



图 5-12 IO 设备地址为 %IB2 的变量收到来自 IO 控制器 %QB2 的值

智能设备地址为 Q3 的变量值→IO 控制器地址 I2 的变量值传输测试：

在 IO 设备的“监控表_1”中，“在 Tag_4”行的修改值处将修改值设置为 ‘K’，右键，在弹出菜单中选择修改→立即修改，如图 5-13（1）所示，监视值将变为与修改值一样的数值，如图 5-13（2）。

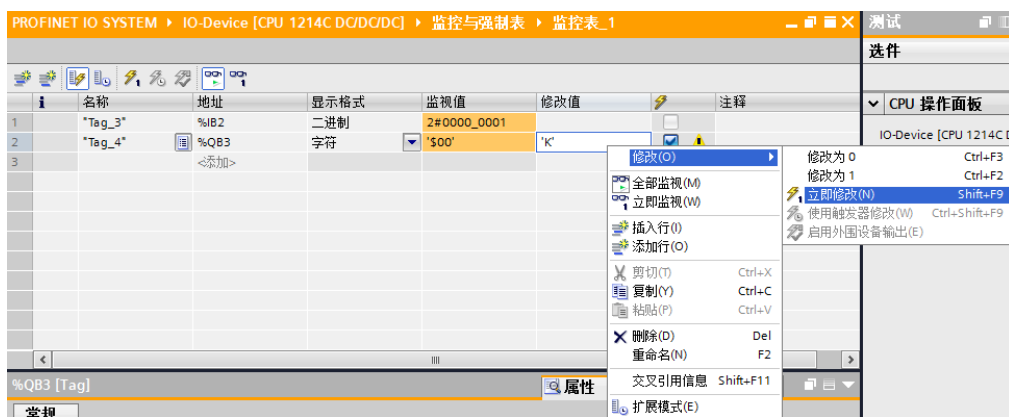


图 5-13 (1) 修改 IO 设备中地址为%QB3 的值



图 5-13 (2) 修改 IO 设备中地址为%QB3 的值

切换到 IO 控制器的“监控表_1”，可以看到 IO 控制器的%IB2 地址已经收到来自 IO 设备发送过来的数据，如图 5-14 所示。



图 5-14 IO 控制器地址为%IB2 的变量收到来自 IO 设备地址为%QB3 变量的值

5.6 课后作业

- (1) 列写出 PROFINET IO 通信的优点；
- (1) 在原有网络结构中增加一个 IO 设备，重新配置 IO 控制器和 IO 设备并进行测试。

参考文献:

[1] SIMATIC PROFINET 系统说明 系统手册 2012 年 3 月

实验六 光纤通讯实验

6.1 技术背景

网络冗余是工业网络的一项保障策略。作为快速反应备份系统，网络冗余的目的是减轻意外中断的风险，通过即时响应保证生产连续，从而降低关键数据流上任意一点失效所带来的影响。

工业网络对可用性要求较高，环网冗余是提高网络可用性的重要手段。

环形工业以太网技术是基于以太网发展起来的，继承了以太网速度快、成本低的优点，同时为网络上的数据传输提供了一条冗余链路，提高了网络的可用性。

将各台交换机通过冗余环口依次进行连接，即构成了环形网络结构。其中一个交换机作为冗余管理器 RM，管理冗余环网。在一个环网中，只能有一台交换机设置成冗余管理器。冗余管理器 RM 通过发送监测帧监控网络链路状态，在网络正常的情况下，RM 的其中的一个冗余环口会处于逻辑断开状态，这样整个网络在逻辑结构上保持一种线型结构，避免广播风暴（当网络中存在环路，就会造成每一帧都在网络中重复广播，引起广播风暴。）。冗余管理器监控网络状态，当网络上的连接线断开或交换机发生故障时，它会通过连通一个替代路径恢复成另外一种逻辑上的线型结构。如果故障被消除，网络逻辑结构会恢复原有的线型结构。环网可以是电气环网也可以是光纤环网，也可以是电气和光纤混合的环网。

在实际应用中往往利用光纤作为环网主干网络将各个工作站或车间连接，实现高速通讯。

现代光纤传输通信技术是将模拟电信号转化为光信号，以光波作为载波，以光纤介质作为载体承载光波信号，实现高速、稳定的信息传输[1]。从目前光纤通信技术的应用来看，利用光纤传输，有效解决了数据传输速度和传输质量问题，保证了数据能够以最快的速度进行传输，并保证数据传输的安全性和准确性[2]。光纤通信技术的主要特点如下[2]：

（1）通信信息传输容量大

由于光纤承载光信号的频带较宽、负载范围大，与传统电缆相比，其承载的通信容量较大。通过密集波分复用技术可以进一步提升光纤传输通信承载的信息量。

（2）数据信息传输损耗低

石英光纤介质是光纤管线的主要材料，与其他材质的信息传输载体相比，光纤损耗较低，而且重量较轻，降低了在搬运、安装、调试、使用过程中对光纤的损伤，在一定程度上减少了外部因素所带来的通信线路损耗。

（3）传输数据保密性强

光纤的特有结构很容易容纳光信号，包裹光纤传输线路的不透明包皮可以有效吸收在光纤信息传输中遗漏的射线，而且光纤传递采用的信号源多为光弧形式，避免了光波泄露导致的外部窃听所带来的安全风险。因此，光纤传输通信与传统的电波传输通信相比，具有更好的保密性。

（4）线路抗电磁干扰能力强

在工业网络领域，由其工作环境复杂，存在多种复合型干扰（设备高速运转、电机马达、电话通信等），传统的铜线电缆已无法解决信号的抗干扰问题，进而导致工业控制中加工精度受到严重影响，设备的稳定性大大下降，设备的寿命也明显缩短。因此，解决抗干扰问题成为实现可靠的工业网络通信的重要因素之一，特别是在远程控制模式下，信号在传输过程中的衰耗和干扰问题尤为突出。

由于石英材料是光纤的主要成分，因此光纤传输通信的绝缘性较高，可以有效降低外界电磁环境的干扰。

6.2 实验目的

- (1) 掌握光纤的接线方法；
- (2) 掌握利用光纤构成主干环网的方法。

6.3 实验准备

完成本实验所需准备的实验材料如下：

- 3 个 SCALANCE XM408-8C；
- 6 个千兆多模光模块 SFP992-1
- 3 对多模光纤
- 2 个 S7 1200；
- 3 根工业以太网线缆；
- 1 台上位机

6.4 实验内容

- (1) 配置上位机和交换机的 IP 地址和子网掩码；
- (2) 配置 S7 1200；
- (3) 将交换机配置成环网
- (4) 网络结构实施，图 6-1 为网络结构拓扑图
 - ①将多模光纤插入光模块中
 - ②将千兆多模光模块 SFP992-1 插入三个交换机设置为冗余端口的光口，构成高速冗余环网 HSR
 - ③利用工业以太网线缆，将上位机、PLC 和交换机相连。
- (5) 通讯测试：将环网中一个工业以太网接口从一个交换机端口拔出，通信网络能否在规定时间内重构通信链路，并保证数据能够从 PLC 传输到上位机。

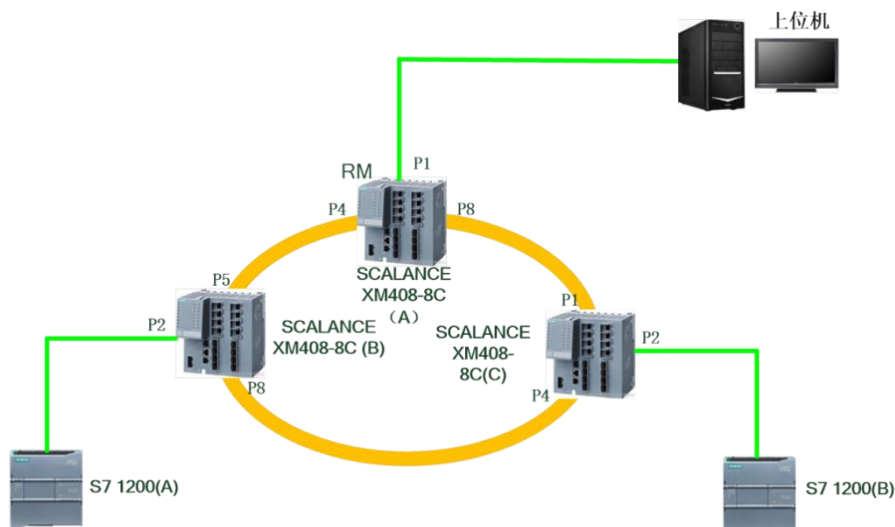


图 6-1 网络结构拓扑图

6.5 实验步骤

注意：在完成三个交换机配置前，不能将三个交换机连成环。

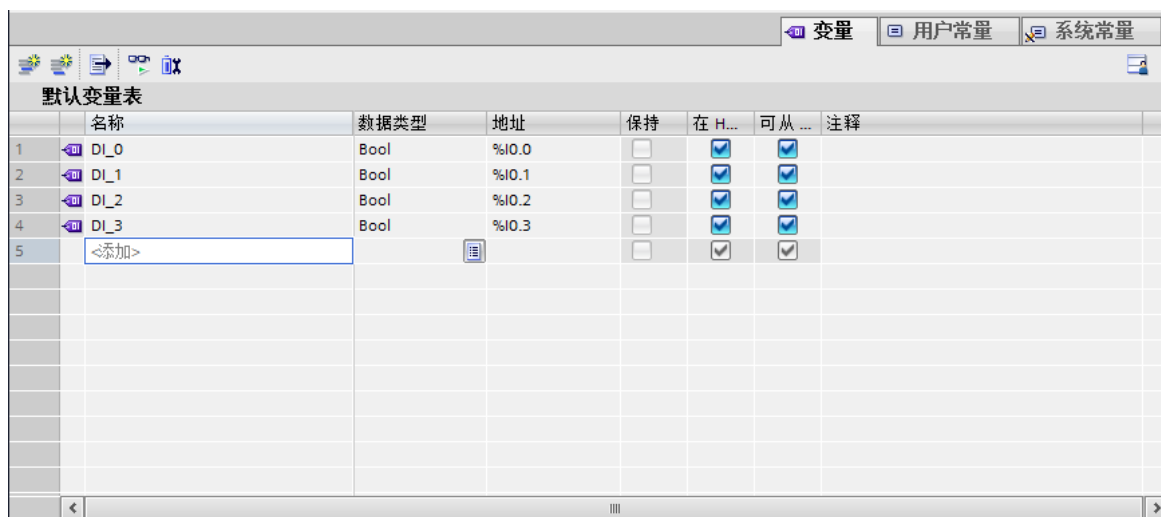
6.5.1 配置上位机、交换机的 IP 地址和子网掩码

将上位机的有线网卡的 IP 地址设置为 192.168.0.100，子网掩码为 255.255.255.0。配置交换机 SCALANCE XM408-8C（A）、SCALANCE XM408-8C（B）和 CALANCE XM408-8C（C）的 IP 地址分别为 192.168.0.11、192.168.0.12 和 192.168.0.13，子网掩码均为 255.255.255.0。

6.5.2 在博途中配置 PLC

在博途中配置 PLC 的目的是利用博途软件对 PLC 中的变量进行监视，同时测试 I/O 变量在通讯网络中的传输过程。

- 1、在博途软件中，在“硬件目录”中选择正确订货号的 S7 1200，添加到“设备视图”中；在“硬件目录”中选择正确订货号的信号板，拖拽到“设备视图”中 S7 1200 中信号板位置上；
- 2、在“设备视图”中选 S7 1200 模块，在博途的“属性”界面中为其配置 IP 地址和子网掩码。S7 1200（A）的 IP 地址为 192.168.0.31，S7 1200（B）的 IP 地址为 192.168.0.32，子网掩码均为 255.255.255.0。
- 3、在博途软件“项目树”中，找到“CPU 1214C”并在其树状结构的子项中找到“PLC 变量”，在“PLC 变量”的子项中，双击打开“默认变量表”。在“默认变量表”中添加需要监视的 DI、DO、AI、AO 变量。本例添加了 4 个 DI 变量，如图 6-2 所示。



默认变量表							
	名称	数据类型	地址	保持	在 H...	可从 ...	注释
1	DI_0	Bool	%I0.0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
2	DI_1	Bool	%I0.1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
3	DI_2	Bool	%I0.2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
4	DI_3	Bool	%I0.3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
5	<添加>			<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

图 6-2 在博途中配置需要监视的变量

- 5、编译程序
- 6、下载程序到 IP 地址对应的 S7 1200 中。

6.5.3 配置环网

打开浏览器，在地址栏中输入 192.168.0.11，进入 SCALANCE XM408-8C (A) 的网络配置登录界面（首次进入该页面需要修改密码）。输入用户名 admin 和密码后，进入 SCALANCE XM408-8C 配置界面，如图 6-3 所示。

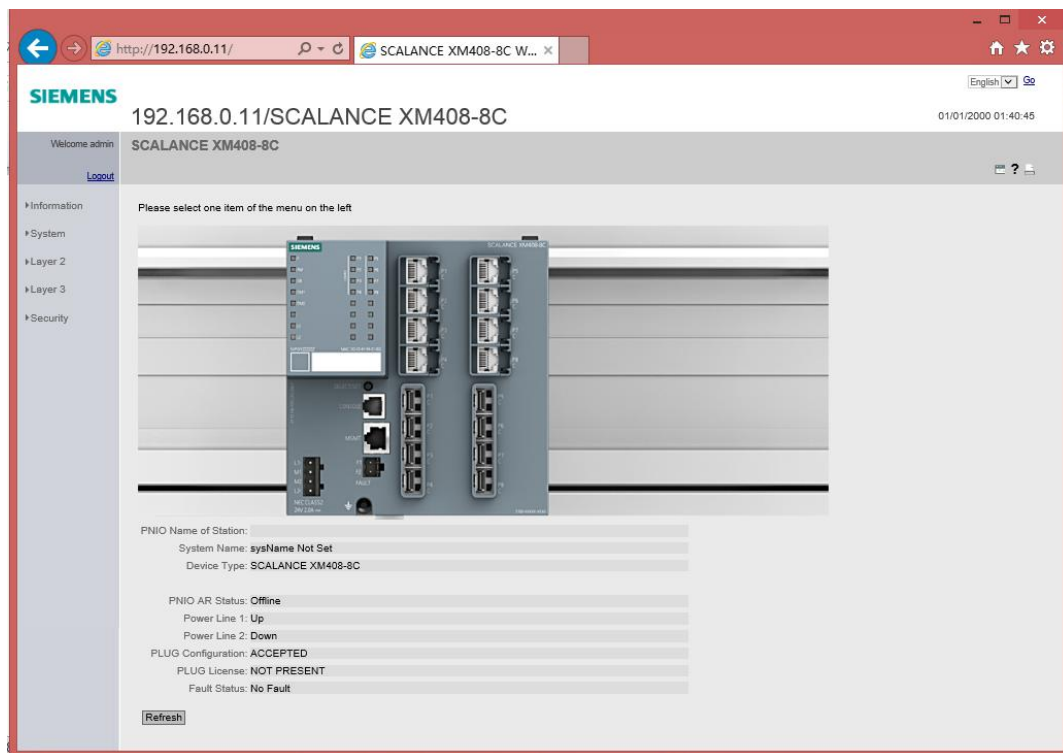


图 6-3 SCALANCE XM408-8C 网络配置主界面

在网络配置界面的左侧列表中，选中“Layer 2”下的“Ring Redundancy”。在“Ring Redundancy”界面中，将“Ring Redundancy”前的复选框勾上；在“Ring Redundancy Mode”的下拉列表中选择“HRP Manager”；然后配置在冗余环中使用的“Ring Ports”，如 P1.4 和 P1.8。如图 6-4 所示。

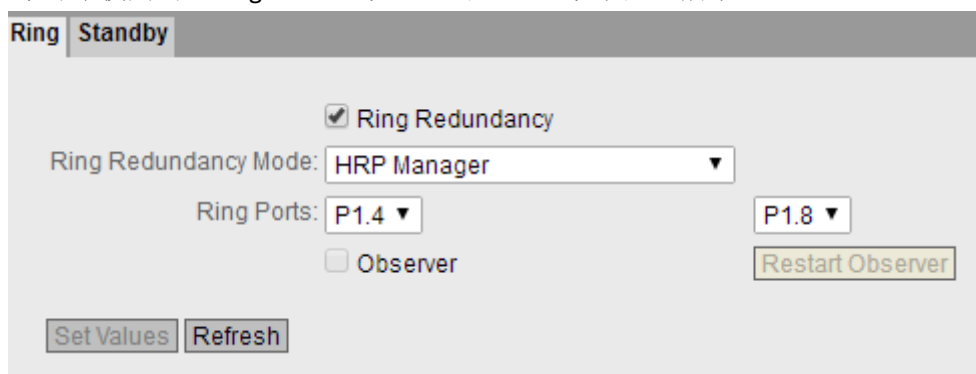


图 6-4 SCALANCE XM408-8C (A) 环形冗余配置

在地址栏中输入 192.168.0.12，进入 SCALANCE XM408-8C (B) 的网络配置登录界面。在网络配置界面的左侧列表中，选中“Layer 2”下的“Ring Redundancy”。在“Ring Redundancy”界面中，将“Ring Redundancy”前的复选框勾上；在“Ring Redundancy Mode”的下拉列表中选择“HRP Client”；然后配置在冗余环中使用的“Ring Ports”，如 P1.5 和 P1.8。如图 6-5 所示。CALANCE XM408-8C (C) 的环网冗余配置过程与 CALANCE

XM408-8C (B) 的类似，只是冗余端口设置为 P1.1 和 P1.4。

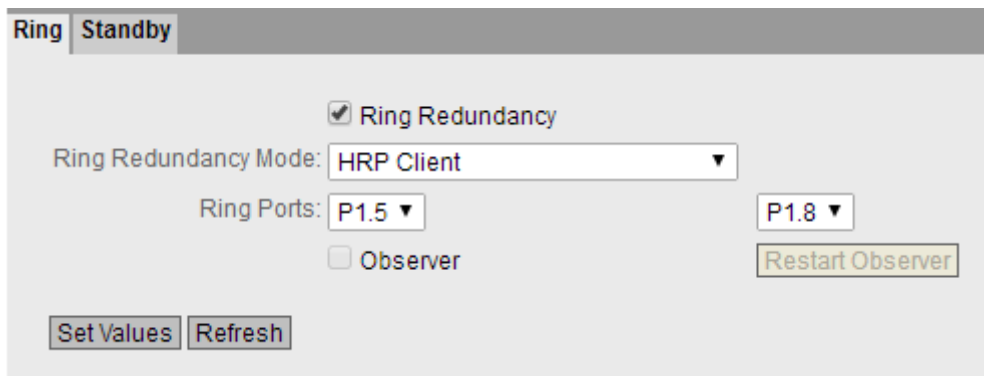


图 6-5 SCALANCE XM408-8C (B) 环形冗余配置

6.5.4 网络结构实施

千兆多模光模块 SFP992-1 如图 6-6 所示，将一对儿多模光纤插入两个光模块如图 6-7 所示（注意插入光纤的顺序，如果对于第一个光模块插入的顺序是左黄右白，那么第二个光模块插入的顺序是左白右黄）。



图 6-6 千兆多模光模块 SFP992-1



图 6-7 一对儿多模光纤

将装配好的光模块插入 SCALANCE XM408 的光口中，如图 6-8 所示。依据如图 6-1 所示端口编号，最终将三个交换机连接成环网。最后利用工业以太网线缆将上位机、PLC 与交换机连接，端口编号如图 6-1 所示。

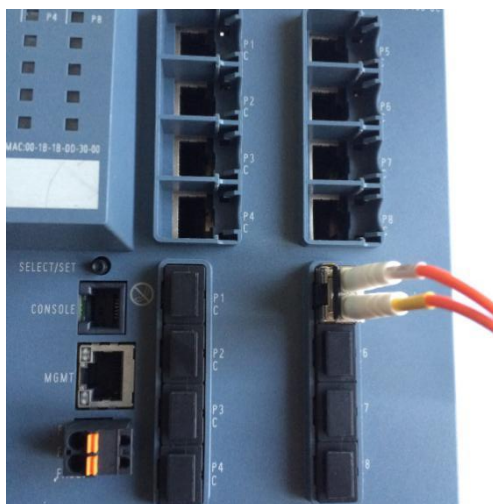


图 6-8 装配好的光模块插入 SCALANCE XM408 的光口中

6.5.5 环形冗余通讯测试（以 S7 1200(A)为例）

1、正常通讯测试

①在博途软件“项目树”中，选中“CPU 1214C”项，点击工具栏中的“转到在线”按钮，然后在“PLC 变量”的子项中，双击打开“默认变量表”。在“默认变量表”中点击“全部监视”按钮。变量监视界面如图 6-9 所示。显示 DI_0 与 DI_2 对应变量为 TRUE，DI_1 与 DI_3 对应变量为 FALSE，与实际开关状态一致。

默认变量表								
	名称	数据类型	地址	保持	在 H...	可从 ...	监视值	注释
1	DI_0	Bool	%I0.0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	TRUE	
2	DI_1	Bool	%I0.1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	FALSE	
3	DI_2	Bool	%I0.2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	TRUE	
4	DI_3	Bool	%I0.3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	FALSE	
5	<添加>			<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		

图 6-9 正常通讯时的变量监视界面

2、环网通讯故障测试

将插入 SCALANCE XM408(B)的 P5 光口的光模块拔掉，模拟环网中某一处通讯线路故障或损坏。此时 XM408-8C (A) 原来处于备用端口的指示灯立刻变为快闪状态，说明该端口已经“激活”。现在，修改与 XM408 (B) 连接的 S7 1200 的 DI 输入，即在 IO 操作面板上将 S7 1200 的第 1 路 DI 输入对应的开关打开，此时博途变量监视界面中 DI_1 对应变量为 TRUE，如图 6-10 所示。说明环网在网络故障情况下进行了重构，且数据传输正确。

默认变量表								
	名称	数据类型	地址	保持	在 H...	可从 ...	监视值	注释
1	DI_0	Bool	%I0.0	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	TRUE	
2	DI_1	Bool	%I0.1	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	TRUE	
3	DI_2	Bool	%I0.2	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	TRUE	
4	DI_3	Bool	%I0.3	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	FALSE	
5	<添加>			<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>		

图 6-10 环网重构后变量监视界面

6.6 课后作业

- 1、通过查阅资料列出单模光纤与多模光纤的区别？
- 2、思考实际生产过程中哪些情况下事宜使用光纤作为通讯介质？
- 3、在实施环形冗余网络结构时应注意哪些问题？

6.7 参考文献

- [1]陈宇,冯杰. 光纤通信技术的研究与分析[J]. 中国新通信,2013,09:77.
- [2]牛淑静,侯翔,王福峙. 现代光纤传输通信技术发展与应用[J]. 电信快报,2016,06:43-45.

实验七 无缝冗余实验

7.1 技术背景

环形网络冗余可以增加网络可靠性，当某一线路出现故障，可以自动重构恢复通讯。通常使用 HSP 冗余协议的收敛时间是 300ms，使用 MRP 冗余协议收敛时间是 200ms，但在一些特殊场合，需要使用无重构时间的网络。

目前，要实现无缝冗余涉及两个技术，即并行冗余协议(PRP)和高可靠性无缝冗余(HSR)。

PRP 使用标准网络组件组成的并行独立结构。通过通过无缝冗余模块，例如 SCALANCE X-204RNA，不具有 PRP 功能的节点或整个网段连接到 PRP 网络。当一个节点要发送的数据帧经过 SCALANCE X 204RNA 后，会被复制为两份，分别通过两个互相独立的局域网传输，到达对方的 SCALANCE X 204RNA 交换机时，它会将最先到达的数据帧转发给目的设备而丢弃后到达的数据帧。

HSR 通信的冗余则是通过环网式结构实现的。通过 SCALANCE X-204RNA，不具有 HSR 功能的节点或整个网段也可以连接到 HSR 网络。当一个节点要发送数据帧经过 SCALANCE X 204RNA 后，会被复制为两份，在环网中往两个方向传输，到达对方的 SCALANCE X 204RNA 交换机时，它会将最先到达的数据帧转发给目的设备而丢弃后到达的数据帧。

7.2 实验目的

- (1) 能够区分平行冗余网络与普通环网冗余的特点；
- (2) 掌握平行冗余网络的配置与调试方法。

7.3 实验准备

零秒切换环网冗余实验实验材料：

2 个 SCALANCE X204 RNA

2 个 S7 1200

1 台上位机

5 根工业以太网线缆

对比实验实验材料：

2 个 SCALANCE XM408-8C 交换机
2 个 S7 1200
1 台上位机
5 个工业以太网线缆

7.4 实验内容

- (1) 配置 SCALANCE X204 RNA
- (2) 将其中一台 S7 1200 配置成 PROFINET IO Controller，另一台 S7 1200 配置成 IO Device；
- (3) 网络结构实施，按照如图 7-1 所示的网络结构图连接各个设备
- (4) 零秒切换通讯测试
- (5) 普通环网冗余通讯对比实验

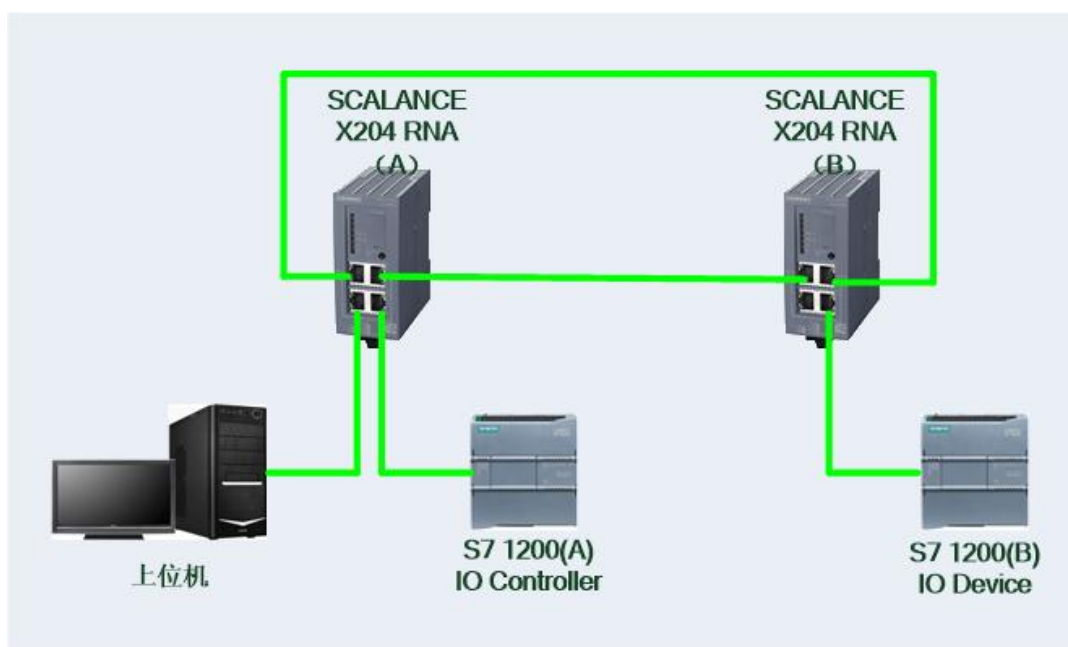


图 7-1 无缝冗余实验结构图

7.5 实验步骤

7.5.1 配置 SCALANCE X204 RNA（A）

将上位机通过 SCALANCE X204 RNA 的 **P1 或 P2** 口连接。

利用 PST 工具，将 SCALANCE X204 RNA（A）的 IP 地址配置为 192.168.0.41，子网掩码配置为 255.255.255.0。

打开浏览器，在地址栏中输入 192.168.0.41，登录后进入 SCALANCE X204 RNA（A）的网络配置界面。

在网络配置界面的左侧列表中，在目录树“X200”下选中“Coupling”。在“Coupling Mode”

下拉菜单中选择“HSR SAN mode”,如图 7-2 所示。

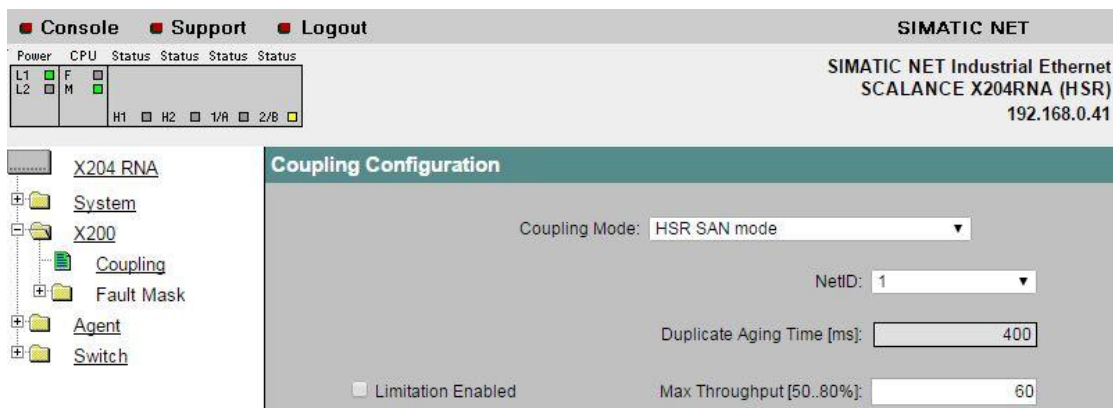


图 7-2 配置 SCALANCE X204 RNA

7.5.2 配置 SCALANCE X204 RNA (B)

将上位机通过 SCALANCE X204 RNA 的 **P1 或 P2** 口连接。

利用 PST 工具, 将 SCALANCE X204 RNA (B) 的 IP 地址配置为 192.168.0.42, 子网掩码配置为 255.255.255.0。

打开浏览器, 在地址栏中输入 192.168.0.42, 登录后进入 SCALANCE X204 RNA (B) 的网络配置界面。

对 SCALANCE X204 RNA (B) 进行与 SCALANCE X204 RNA (A) 相同的配置。

7.5.3 在 Portal 软件中将 S7 1200 (A) 配置为 IO 控制器

(1) 在项目中通过“添加新设备”添加 S7 1200 PLC, 添加成功后, 在设备视图中选中 S7 1200, 在属性→常规→项目信息页面中将名称修改为“IO-Controller”;

(2) 设置 IO-Controller 的子网、IP 地址和子网掩码。在设备视图中选中 S7 1200, 在属性→常规→PROFINET 接口→以太网地址中设置子网、IP 地址和子网掩码, 如图 7-3 所示。

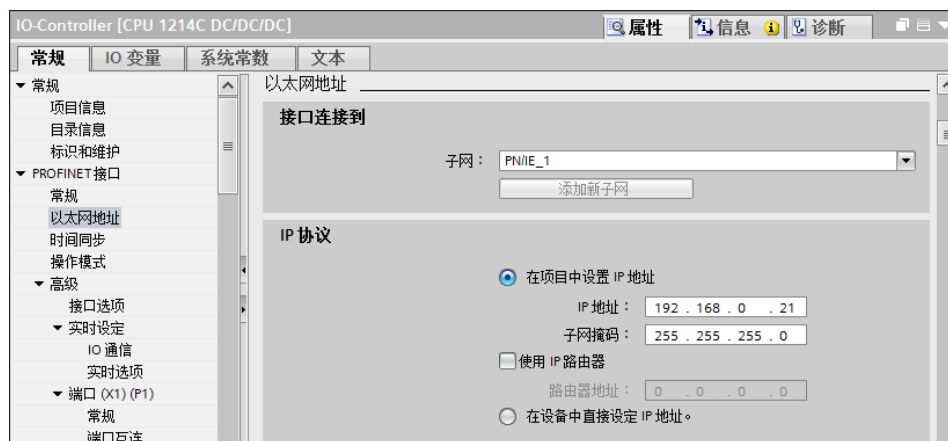


图 7-3 配置 IO 控制器的子网、IP 地址和子网掩码

(3) 属性→常规→PROFINET 接口→操作模式, 使用默认配置, 即将该 PLC 作为 IO 控制器, 如图 7-4 所示。



图 7-4 IO 控制器设置界面

(4) 为 IO 控制器添加数据类型为 Byte 的变量，变量名称分别为 Tag_1 和 Tag_2，地址分别为 %QB2 和 %IB2，如图 7-5 所示。

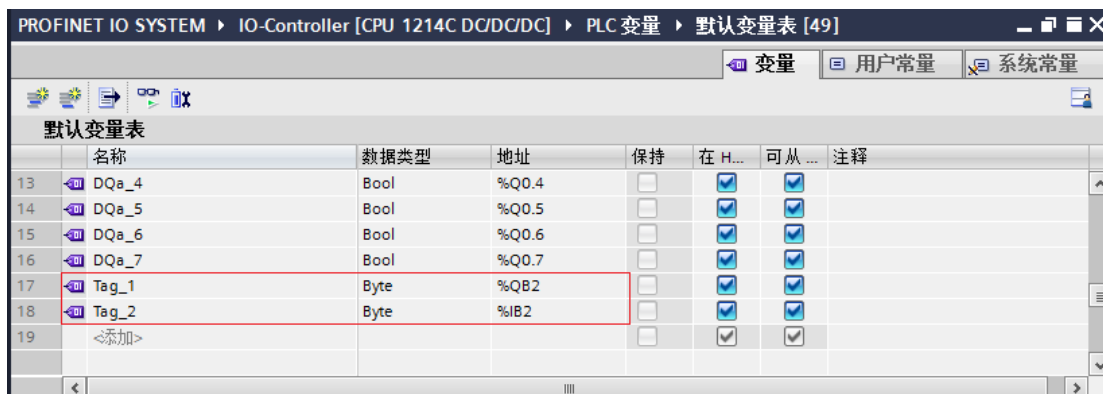


图 7-5 为 IO 控制器增加变量类型为 Byte 的变量

(5) 添加监控表。项目树→IO-Controller→监控与强制表下双击“添加新监控表”，在新建的“监控表_1”中，在“名称”列下分别选择 Tag_1 和 Tag_2 变量，将显示格式分别设置为二进制和字符，如图 7-6 所示。



图 7-6 在 IO 控制器的监控表中添加监控变量

7.5.4 在 Portal 软件中将 S7 1200（B）配置为 IO 设备

(1) 在项目中通过“添加新设备”添加 S7 1200 PLC，添加成功后，在设备视图中选中 S7 1200，在属性→常规→项目信息页面中将名称修改为“IO-Device”；

(2) 设置 IO-Device 的子网、IP 地址和子网掩码。在设备视图中选中 S7 1200，在属性→常规→PROFINET 接口→以太网地址中设置子网、IP 地址和子网掩码，如图 7-7 所示。

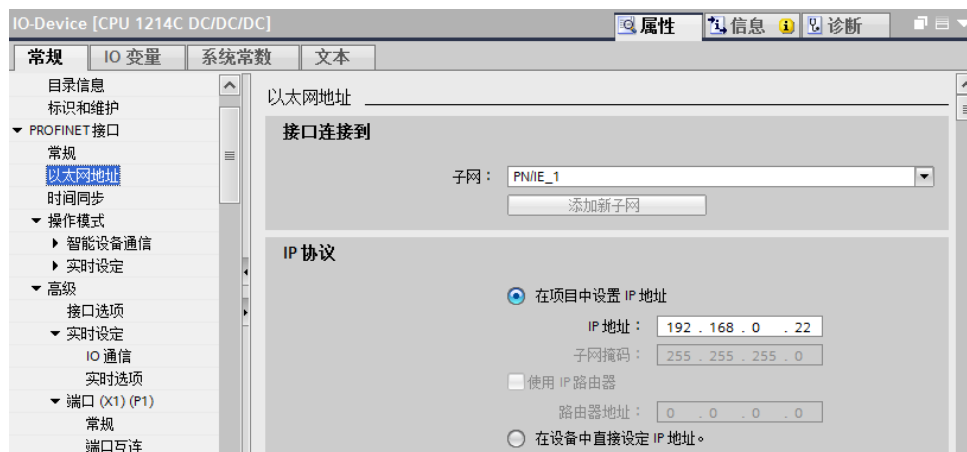


图 7-7 设置 IO 设备的子网、IP 地址和子网掩码

(3) 在设备视图中选中 S7 1200，属性→常规→PROFINET 接口→操作模式，勾选“IO 设备”前的复选框；在“已分配的 IO 控制器”下拉列表中选择 IO 控制器“IO-Controller.PROFINET 接口_1”，如图 7-8 所示。

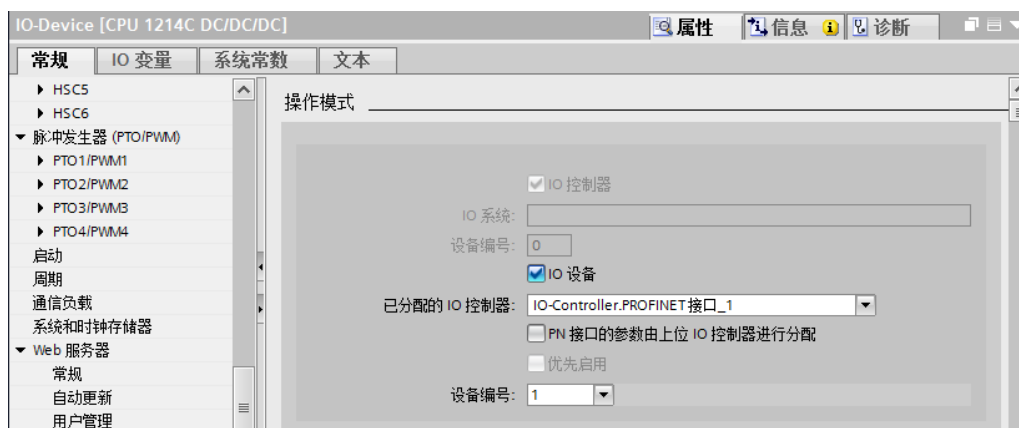


图 7-8 IO 设备配置界面

(4) 为 IO 设备添加数据类型为 Byte 的变量，变量名称分别为 Tag_3 和 Tag_4，地址分别为 %IB2 和 %QB3，如图 7-9 所示。



图 7-9 为 IO 设备添加变量类型为 Byte 的变量

(5) 添加监控表。项目树→IO-Device→监控与强制表下双击“添加新监控表”，在新建的“监控表_1”中，在“名称”列下分别选择 Tag_3 和 Tag_4 变量，将显示格式分别设置为二进制和字符，如图 7-10 所示。



图 7-10 在 IO 设备监控表中添加监控变量

(6) 设置传输区。在设备视图中选中 S7 1200，属性→常规→PROFINET 接口→操作模式→智能设备通信，双击“新增”添加传输区。如图 7-11 所示，增加了两个传输区，第一个传输区表达的是将 IO 控制器中地址为 Q2 的变量的数据传输到智能设备中地址为 I2 的变量中，第二个传输区表达的是将智能设备中地址为 Q3 的变量的数据传输到 IO 控制器中地址为 I2 的变量中。单击箭头，可改变传输方向。



图 7-11 传输区设置

7.5.5 网络结构实施

(1) 利用工业以太网线缆，按照如图 7-1 所示的网络拓扑图，将 SCALANCE X204 RNA (A) 的 HSR 1 端口与 SCALANCE X204 RNA(B) 的 HSR 2 端口连接，SCALANCE X204 RNA

(A) 的 HSR 2 端口与 SCALANCE X204 RNA (B) 的 HSR 1 端口连接。

(2) 将作为 IO 控制器的 S7 1200 与 SCALANCE X204 RNA (A) 的 P2 端口连接, 将作为智能 IO 设备的 S7 1200 与 SCALANCE X204 RNA (B) 的 P2 端口连接, 将上位机与 SCALANCE X204 RNA (A) 的 P1 端口连接。

(3) 接通电源。

7.5.6 通信测试

将 IO-Controller 和 IO-Device 各自编译下载并运行。

在 IO 控制器的“监控表_1”和 IO 设备的“监控表_1”中, 分别点击“全部监视”按钮。

IO 控制器中地址为 Q2 的变量值→智能设备中的地址为 I2 的变量值传输测试:

在 IO 控制器的“监控表_1”中, “在 Tag_1”行的修改值处右键, 选择修改为 1, 如图 7-12 (1) 所示, 监视值将变为与修改值一样的数值, 如图 7-12 (2)。

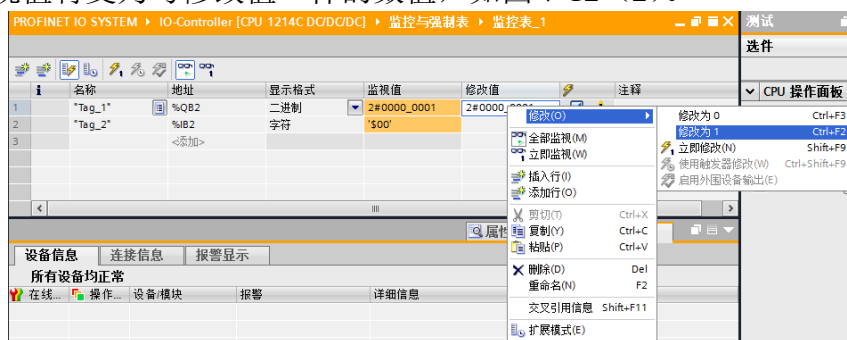


图 7-12 (1) 修改 IO 控制器中地址为 %QB2 的值



图 7-12 (2) 修改 IO 控制器中地址为 %QB2 的值

切换到 IO 设备的“监控表_1”, 可以看到 IO 设备的 %IB2 地址已经收到来自 IO 控制器发送过来的数据, 如图 7-13 所示。



图 7-13 IO 设备地址为 %IB2 的变量收到来自 IO 控制器 %QB2 的值

智能设备地址为 Q3 的变量值→IO 控制器地址 I2 的变量值传输测试:

在 IO 设备的“监控表_1”中, “在 Tag_4”行的修改值处将修改值设置为 'K', 右键, 在弹出

菜单中选择修改→立即修改，如图 7-14（1）所示，监视值将变为与修改值一样的数值，如图 7-14（2）。

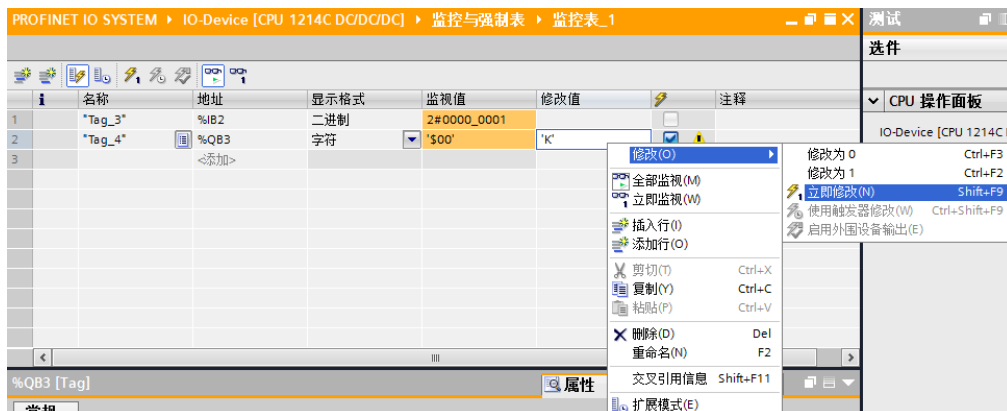


图 7-14（1）修改 IO 设备中地址为%QB3 的值



图 7-14（2）修改 IO 设备中地址为%QB3 的值

切换到 IO 控制器的“监控表_1”，可以看到 IO 控制器的%IB2 地址已经收到来自 IO 设备发送过来的数据，如图 7-15 所示。



图 7-15 IO 控制器地址为%IB2 的变量收到来自 IO 设备地址为%QB3 变量的值

上述通讯测试过程显示 IO Controller 和 IO device PLC 之间的 PROFINET 通讯是正常的（注意：两个 S7 1200 的 ERROR 灯没有报警）。在此基础上，下文将利用普通环网冗余与利用 SCALANCE X204 RNA 的 HSR 的平行冗余网络进行对比。

拔掉 SCALANCE X204 RNA(A) HSR1 或 HSR2 端口的工业以太网线来模拟线路故障，观察到 IO Controller 和 IO device PLC 的 Error 指示灯均未报警，即 IO Controller 和 IO device PLC 之间 PROFINET 通讯正常，未发生掉站情况。

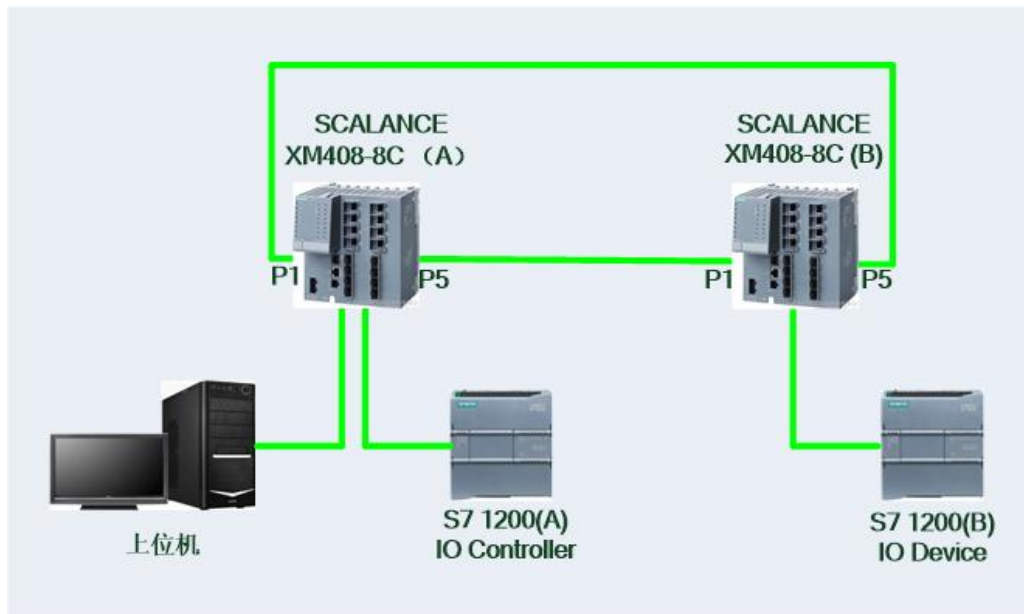


图 7-16 对比实验环网冗余网络结构图

利用 SCALANCE XM408-8C 构建如图 7-16 所示的环网（配置方法参考“实验三 单环冗余网络实验”），拔掉 SCALANCE XM408-8C 之间的当前用于通讯的工业以太网线缆（非备用线路）来模拟线路故障，观察到 PROFINET IO Controller 和 IO Device 之间通讯出现中断，即 IO Controller 和 IO device PLC 的 Error 指示灯报警，整个通讯恢复时间（包括环网重构时间和 IO Controller 和 IO device PLC 之间 PROFINET 通讯的恢复时间）大约 4s。

对比实验结论：由上述普通环网冗余与利用 SCALANCE X204 RNA 的 HSR 的平行冗余网络对比实验可以看出，利用 SCALANCE X204 RNA 组建的平行冗余网络在网络线路出现故障时能够做到零秒切换，即不需要环网重构时间，而利用普通环网整个网络的通讯恢复时间为约 4 秒。

7.6 课后作业

学习“IEC 62439-3-2012 工业通信网络 高可靠性自动控制网络 第 3 部分：并行冗余协议(PRP)和高可靠性无缝冗余(HSR)”内容，写出并行冗余协议(PRP)和高可靠性无缝冗余(HSR)在通讯机制上的详细区别。

实验八 防火墙实验

8.1 技术背景

所谓防火墙指的是一个由软件和硬件设备组合而成、在内部网和外部网之间、专用网与公共网之间的界面上构造的保护屏障。是一种获取安全性方法的形象说法，它是一种计算机硬件和软件的结合，使 Internet 与 Intranet 之间建立起一个安全网关（Security Gateway），从而保护内部网免受非法用户的侵入，防火墙主要由服务访问规则、验证工具、包过滤和应用网关 4 个部分组成。防火墙通常使用的安全控制手段主要有包过滤、状态检测、代理服务[1]。

防火墙能强化安全策略，有效地记录 Internet 上的活动。同时能限制暴露用户点，它隔开了网络中一个网段与另一个网段，这样能够防止影响一个网段的问题通过整个网络传播。防火墙是一个安全策略的检查站，所有进出的信息都必须通过防火墙，这样它便成为安全问题的检查点，使可疑的访问被拒绝于门外[1]。

随着工控信息安全越来越成为各方关注的焦点，越来越多的工业企业对工控信息安全产品投入了更多关注目光。现阶段工业防火墙仍是防护工控信息安全的的主流产品，作为扼守工业网络安全的重要设备，工业防火墙在运行稳定性、响应精准性以及安全防护能力上依然是工业用户普遍关注的重点[2]。未来的防火墙的发展趋势是向高速、多功能化、更安全的方向发展[3]。防火墙技术只有不断向主动型和智能型等方向发展，促进新一代防火墙技术产生，才能更好的满足人们对防火墙技术日益增长的需求，更好的促进我国经济的发展。

8.2 实验目的

- (1) 认识硬件防火墙设备；
- (2) 了解硬件防火墙工作原理；
- (3) 掌握防火墙的设置方法。

8.3 实验准备

完成本实验所需准备的实验材料如下：

- 1 个 SCALANCE S615；
- 1 个 SCALANCE XM408-8C；
- 2 个 SCALANCE XB208；
- 2 个 S7 1200 PLC
- 2 台计算机
- 7 根工业以太网线缆

8.4 实验内容

本实验设定的工厂网络环境与要求如下：

现有一个生产车间，包括两个工艺单元，每个工艺单元分别有一个 PLC S7 1200。两个工艺单元与车间“生产监控服务器”通过交换机 SCALANCE XM408 连接。防火墙模块 SCALANCE S615 将生产网络与外部管理网络隔离开。要求实现车间内部网络可以访问外部网络，外部网络不能访问车间内部网络，防止外部的恶意攻击。外部网络中，只有特定的用户可以访问内部网络。

网络拓扑结构图如图 8-1 所示。

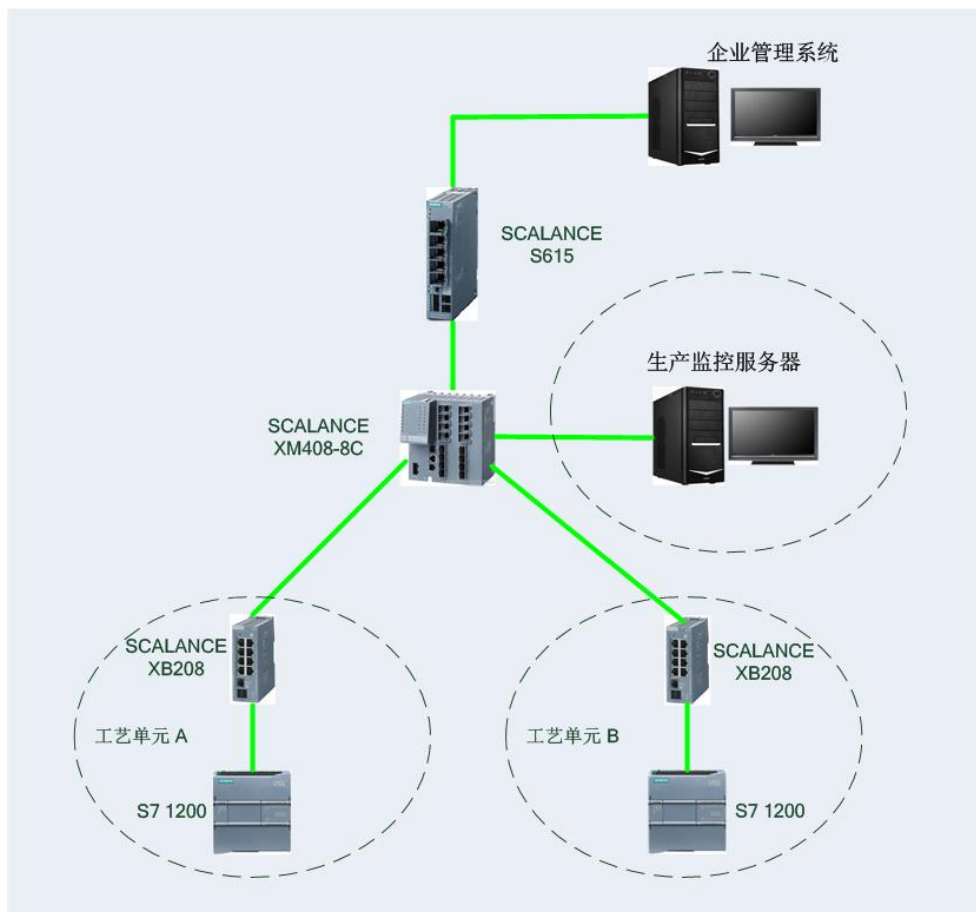


图 8-1 网络拓扑结构图

实验内容如下：

(1) IP 规划

防火墙 S615 将网络分为外部网络和内部网络，其中外网网关 IP 为 10.10.0.1，子网掩码为 255.255.255.0；内网网关为 192.168.2.1，子网掩码为 255.255.255.0。

运行企业管理系统的计算机：IP 地址 10.10.0.100，子网掩码 255.255.255.0，网关 10.10.0.1

生产监控服务器：IP 地址 192.168.2.100，子网掩码 255.255.255.0，网关 192.168.2.1

工艺单元 A 中 S7 1200：IP 地址 192.168.2.11，子网掩码 255.255.255.0，网关 192.168.2.1

工艺单元 B 中 S7 1200：IP 地址 192.168.2.12，子网掩码 255.255.255.0，网关 192.168.2.1

SCALANCE XM408 与两个 XB208 不需要特定的配置。

(2) 配置 SCALANCE S615

- (3) 网络结构实施
- (4) 通讯测试

8.5 实验步骤

8.5.1 在 S615 中划分 VLAN

在 Layer 2 下的 VLAN 界面中设置基于端口的 VLAN，如图 8-2 和 8-3 所示。其中，P1-P4 端口分配给 VLAN1，P5 端口分配给 VLAN2，VLAN1 的 Name 为 INT，VLAN2 的 Name 为 EXT。

Welcome admin [Logout](#)

Virtual Local Area Network (VLAN) General

General | **Port Based VLAN**

Base Bridge Mode: 802.1Q VLAN Bridge

VLAN ID:

Select	VLAN ID	Name	Status	P1	P2	P3	P4	P5
<input type="checkbox"/>	1	INT	Static	U	U	U	U	-
<input type="checkbox"/>	2	EXT	Static	-	-	-	-	U

2 entries.

[Create](#) [Delete](#) [Set Values](#) [Refresh](#)

图 8-2 VLAN 设置 1

Welcome admin [Logout](#)

Port Based Virtual Local Area Network (VLAN) Configuration

General | **Port Based VLAN**

	Priority	Port VID	Acceptable Frames	Ingress Filtering	Copy to Table
All ports	No Change	No Change	No Change	No Change	Copy to Table

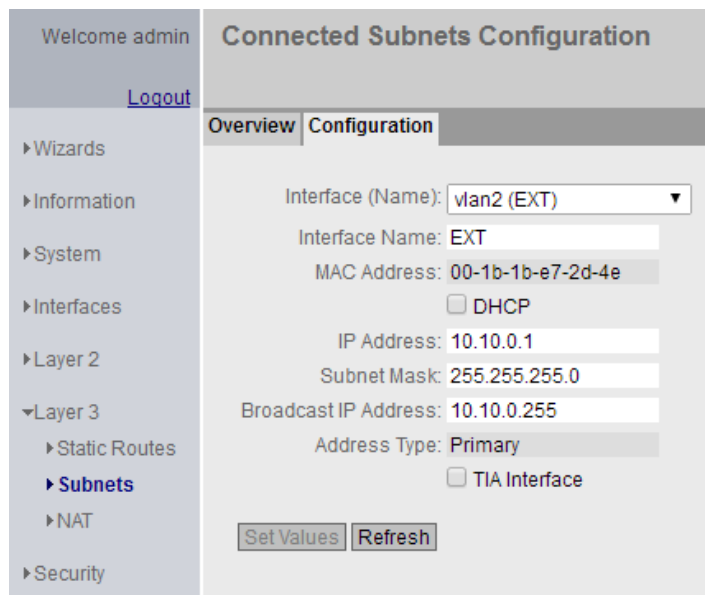
Port	Priority	Port VID	Acceptable Frames	Ingress Filtering
P1	0	VLAN1	All	<input checked="" type="checkbox"/>
P2	0	VLAN1	All	<input checked="" type="checkbox"/>
P3	0	VLAN1	All	<input checked="" type="checkbox"/>
P4	0	VLAN1	All	<input checked="" type="checkbox"/>
P5	0	VLAN2	All	<input checked="" type="checkbox"/>

[Set Values](#) [Refresh](#)

图 8-3 VLAN 设置 2

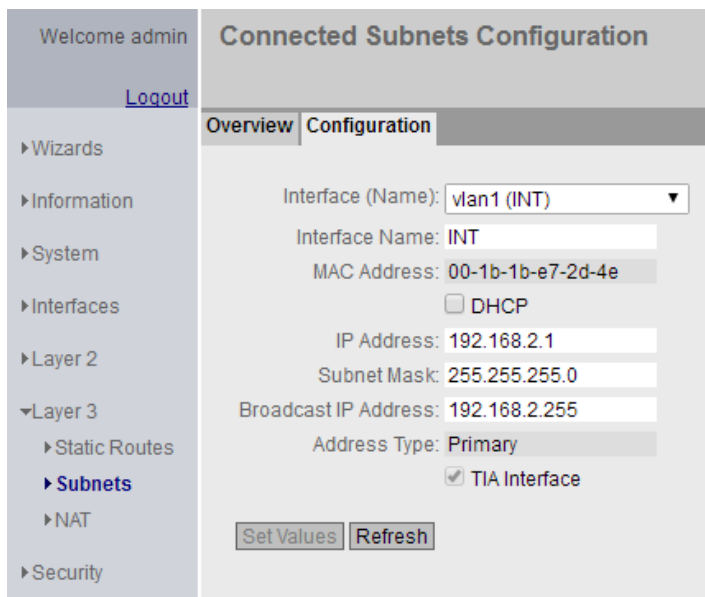
8.5.2 在 S615 中进行子网设置

在 Layer3 下的 Subnets 的 Configuration 页签下分别配置外网和内网网关，如图 8-4、8-5 所示。配置完成的结果如图 8-6 所示。



The screenshot shows the 'Connected Subnets Configuration' page for 'vlan2 (EXT)'. The left sidebar contains a navigation menu with 'Subnets' selected under 'Layer 3'. The main content area has two tabs: 'Overview' and 'Configuration'. The 'Configuration' tab is active, displaying the following fields: 'Interface (Name):' set to 'vlan2 (EXT)', 'Interface Name:' set to 'EXT', 'MAC Address:' set to '00-1b-1b-e7-2d-4e', 'DHCP' checkbox is unchecked, 'IP Address:' set to '10.10.0.1', 'Subnet Mask:' set to '255.255.255.0', 'Broadcast IP Address:' set to '10.10.0.255', 'Address Type:' set to 'Primary', and 'TIA Interface' checkbox is unchecked. At the bottom are 'Set Values' and 'Refresh' buttons.

图 8-4 外网网关设置



The screenshot shows the 'Connected Subnets Configuration' page for 'vlan1 (INT)'. The left sidebar contains a navigation menu with 'Subnets' selected under 'Layer 3'. The main content area has two tabs: 'Overview' and 'Configuration'. The 'Configuration' tab is active, displaying the following fields: 'Interface (Name):' set to 'vlan1 (INT)', 'Interface Name:' set to 'INT', 'MAC Address:' set to '00-1b-1b-e7-2d-4e', 'DHCP' checkbox is unchecked, 'IP Address:' set to '192.168.2.1', 'Subnet Mask:' set to '255.255.255.0', 'Broadcast IP Address:' set to '192.168.2.255', 'Address Type:' set to 'Primary', and 'TIA Interface' checkbox is checked. At the bottom are 'Set Values' and 'Refresh' buttons.

图 8-5 内网网关设置

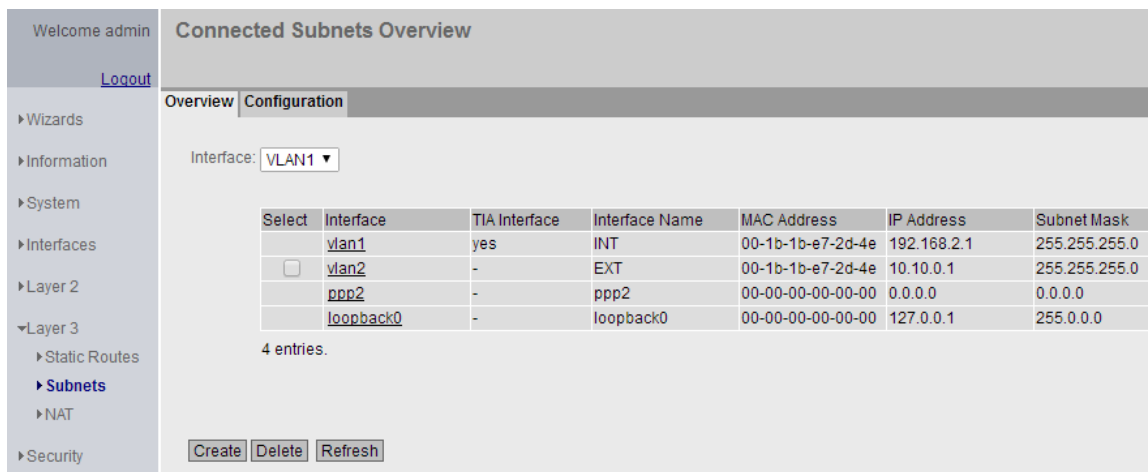


图 8-6 子网设置结果

8.5.3 在 S615 中设置防火墙 IP 规则

首先，激活防火墙功能，如图 8-7 所示。

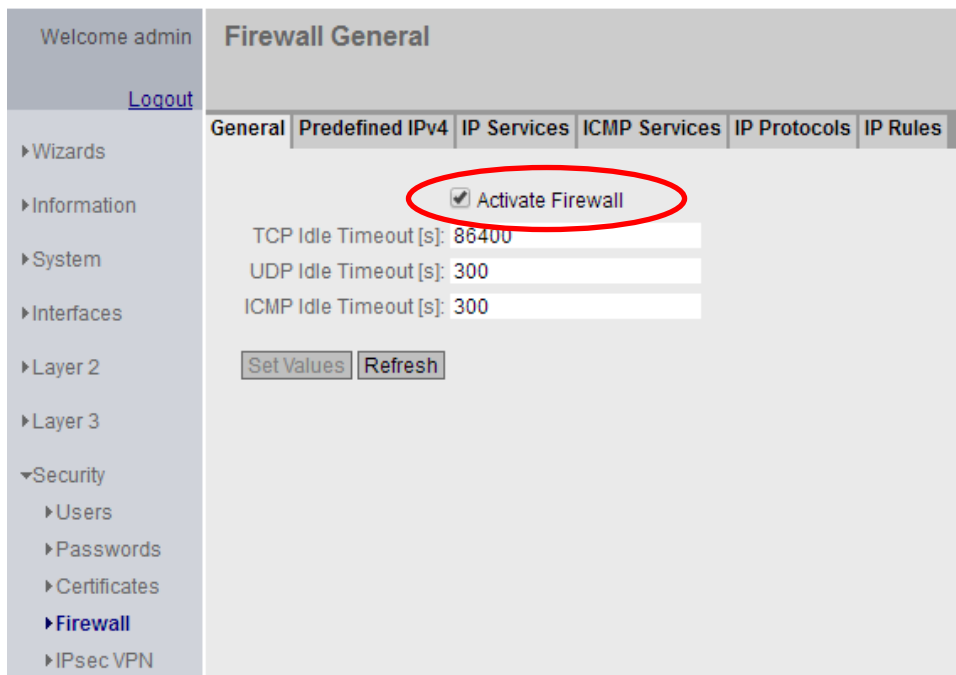


图 8-7 激活防火墙功能

然后，在“IP Rules”页签下添加 IP 过滤规则，如图 8-8 所示。其中第一条规则表示：内网中任一主机可以访问外网的任一主机。第二条规则表示：在外网访问内网方向，外网中只有 IP 地址为 10.10.0.100 的主机能够访问内网，且仅可以访问内网 IP 地址为 192.168.2.100 的主机。

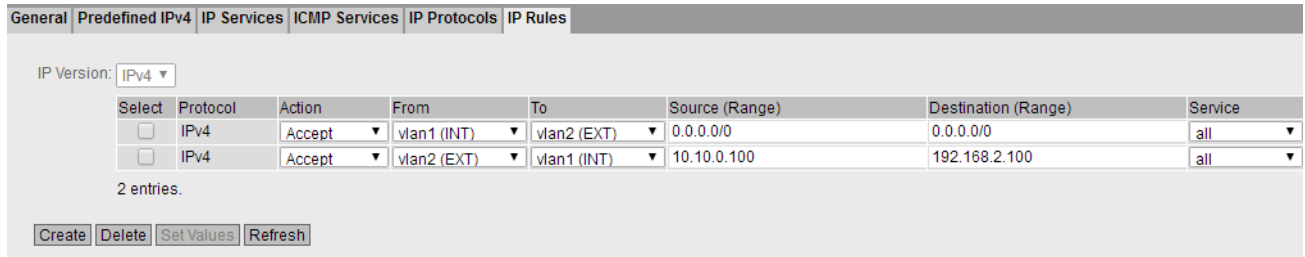


图 8-8 IP 规则

8.5.4 网络实施

根据如图8-1所示网络结构图，实施网络结构，其中将“企业管理系统”计算机与S615的P5端口连接，将XM408与S615的P1-P4的任一端口连接。XM408其他端口、XB208的端口任意选用。

8.5.5 防火墙功能测试

测试：内网中任一主机可以访问外网的任一主机

(1) 内网“生产监控服务器”主机IP地址为192.168.2.100，外网“企业管理系统”主机IP地址为10.10.0.100，前者ping后者的IP地址，是可以ping通的，如图8-9所示。

```
C:\Users\Administrator>ping 10.10.0.100

正在 Ping 10.10.0.100 具有 32 字节的数据:
来自 10.10.0.100 的回复: 字节=32 时间=1ms TTL=127
来自 10.10.0.100 的回复: 字节=32 时间=1ms TTL=127
来自 10.10.0.100 的回复: 字节=32 时间=1ms TTL=127
来自 10.10.0.100 的回复: 字节=32 时间=1ms TTL=127

10.10.0.100 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间<以毫秒为单位>:
        最短 = 1ms, 最长 = 1ms, 平均 = 1ms
```

图 8-9 内网主机 ping 外网主机 IP 地址测试 1

(2) 将内网“生产监控服务器”主机IP地址修改为192.168.2.101，仍然能够ping通，如图8-10所示。

```
C:\Users\Administrator>ping 10.10.0.100

正在 Ping 10.10.0.100 具有 32 字节的数据:
来自 10.10.0.100 的回复: 字节=32 时间=225ms TTL=127
来自 10.10.0.100 的回复: 字节=32 时间<1ms TTL=127
来自 10.10.0.100 的回复: 字节=32 时间<1ms TTL=127
来自 10.10.0.100 的回复: 字节=32 时间<1ms TTL=127

10.10.0.100 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间<以毫秒为单位>:
        最短 = 0ms, 最长 = 225ms, 平均 = 56ms
```

图 8-10 内网主机 ping 外网主机 IP 地址测试 2

(3) 将外网“企业管理系统”主机IP地址修改为10.10.0.101, 仍然能够ping通, 如图8-11所示。

```
C:\Users\Administrator>ping 10.10.0.101

正在 Ping 10.10.0.101 具有 32 字节的数据:
来自 10.10.0.101 的回复: 字节=32 时间<1ms TTL=127
来自 10.10.0.101 的回复: 字节=32 时间<1ms TTL=127
来自 10.10.0.101 的回复: 字节=32 时间<1ms TTL=127
来自 10.10.0.101 的回复: 字节=32 时间<1ms TTL=127

10.10.0.101 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间<以毫秒为单位>:
        最短 = 0ms, 最长 = 0ms, 平均 = 0ms
```

图 8-11 内网主机 ping 外网主机 IP 地址测试 3

测试: 在外网访问内网方向, 外网中只有IP地址为10.10.0.100的主机能够访问内网, 且仅可以访问内网IP地址为192.168.2.100的主机。

(1) 内网“生产监控服务器”主机IP地址为192.168.2.100, 外网“企业管理系统”主机IP地址为10.10.0.100, 后者ping前者的IP地址, 是可以ping通的, 如图8-12所示。

```
C:\Users\ZYL>ping 192.168.2.100

正在 Ping 192.168.2.100 具有 32 字节的数据:
来自 192.168.2.100 的回复: 字节=32 时间<1ms TTL=127
来自 192.168.2.100 的回复: 字节=32 时间<1ms TTL=127
来自 192.168.2.100 的回复: 字节=32 时间<1ms TTL=127
来自 192.168.2.100 的回复: 字节=32 时间<1ms TTL=127

192.168.2.100 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间<以毫秒为单位>:
        最短 = 0ms, 最长 = 0ms, 平均 = 0ms
```

图 8-12 外网主机 ping 内网主机 IP 地址测试 1

(2) 将外网“企业管理系统”主机IP地址修改为10.10.0.101, ping内网主机IP 192.168.2.100, ping不通。

```
C:\Users\ZYL>ping 192.168.2.100

正在 Ping 192.168.2.100 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

192.168.2.100 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),
```

图 8-13 外网主机 ping 内网主机 IP 地址测试 2

(3) 外网“企业管理系统”主机IP地址为10.10.0.100, 将内网“生产监控服务器”主机IP地址修改为192.168.2.101, 前者ping后者的IP地址, ping不通, 如图8-14所示。

```
C:\Users\ZYL>ping 192.168.2.101

正在 Ping 192.168.2.101 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

192.168.2.101 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),
```

图 8-14 外网主机 ping 内网主机 IP 地址测试 3

(4) 外网“企业管理系统”主机IP地址为10.10.0.100，ping内网中工艺单元A中S7 1200，ping不通，无法访问，如图8-15所示。这也符合信息安全要求，因为如果外网能够访问内网PLC是很容易遭受攻击的。

```
C:\Users\ZYL>ping 192.168.2.11

正在 Ping 192.168.2.11 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

192.168.2.11 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),
```

图 8-15 外网主机 ping 内网主机 IP 地址测试 4

(5) 外网“企业管理系统”主机IP地址为10.10.0.100，ping内网中工艺单元B中S7 1200，ping不通，无法访问，如图8-16所示。这也符合信息安全要求，因为如果外网能够访问内网PLC是很容易遭受攻击的。

```
C:\Users\ZYL>ping 192.168.2.12

正在 Ping 192.168.2.12 具有 32 字节的数据:
请求超时。
请求超时。
请求超时。
请求超时。

192.168.2.12 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 0, 丢失 = 4 (100% 丢失),
```

图 8-16 外网主机 ping 内网主机 IP 地址测试 5

8.6 课后作业

思考既然目前已经可以在交换机中集成信息安全控制功能为什么还需要特定的防火墙硬件模块。

参考文献:

- [1] 陈关胜.防火墙技术现状与发展趋势研究[A]. 中国优选法统筹法与经济数学研究会计算机模拟分会.信息化、工业化融合与服务创新——第十三届计算机模拟与信息技术学术会议论文集[C].中国优选法统筹法与经济数学研究会计算机模拟分会:,2011:6.
- [2] 工控信息安全防护——二零一四工业防火墙安稳准[J]. 信息安全与通信保密,2014,12:107.
- [3] 周启辉.防火墙的现状与发展趋势分析[J].涟钢科技与管理,2003(06):605-606.