

SIEMENS

SIMATIC NET

工业以太网交换机 SCALANCE XB-200/XC-200/XP- 200 Web Based Management




配置手册

简介	1
说明	2
IP 地址分配	3
技术基础	4
使用“基于 Web 的管理”进行组态	5
故障排除/FAQ	6

法律资讯

警告提示系统

为了您的人身安全以及避免财产损失，必须注意本手册中的提示。人身安全的提示用一个警告三角表示，仅与财产损失有关的提示不带警告三角。警告提示根据危险等级由高到低如下表示。

 危险
表示如果不采取相应的小心措施， 将会 导致死亡或者严重的人身伤害。
 警告
表示如果不采取相应的小心措施， 可能 导致死亡或者严重的人身伤害。
 小心
表示如果不采取相应的小心措施，可能导致轻微的人身伤害。
注意
表示如果不采取相应的小心措施，可能导致财产损失。

当出现多个危险等级的情况下，每次总是使用最高等级的警告提示。如果在某个警告提示中带有警告可能导致人身伤害的警告三角，则可能在该警告提示中另外还附带有可能导致财产损失的警告。


合格的专业人员

本文件所属的产品/系统只允许由符合各项工作要求的**合格人员**进行操作。其操作必须遵照各自附带的文件说明，特别是其中的安全及警告提示。

由于具备相关培训及经验，合格人员可以察觉本产品/系统的风险，并避免可能的危险。

按规定使用Siemens 产品

请注意下列说明：

 警告
Siemens 产品只允许用于目录和相关技术文件中规定的使用情况。如果要使用其他公司的产品和组件，必须得到 Siemens 推荐和允许。正确的运输、储存、组装、装配、安装、调试、操作和维护是产品安全、正常运行的前提。必须保证允许的环境条件。必须注意相关文件中的提示。

商标

所有带有标记符号®的都是西门子股份有限公司的注册商标。本印刷品中的其他符号可能是一些其他商标。若第三方出于自身目的使用这些商标，将侵害其所有者的权利。

责任免除

我们已对印刷品中所述内容与硬件和软件的一致性作过检查。然而不排除存在偏差的可能性，因此我们不保证印刷品中所述内容与硬件和软件完全一致。印刷品中的数据都按规定经过检测，必要的修正值包含在下一版本中。

目录

1	简介	9
2	说明	13
2.1	系统功能硬件设备	13
2.2	产品特征	17
2.3	安装和操作的要求	18
3	IP 地址分配	19
3.1	IP 地址的结构	19
3.2	IP 地址的初始分配	20
3.3	用 DHCP 进行地址分配	22
4	技术基础	23
4.1	组态限制	23
4.2	PROFINET	25
4.3	EtherNet/IP	25
4.4	冗余机制	26
4.4.1	生成树	26
4.4.1.1	RSTP、MSTP、CIST	27
4.4.2	HRP	28
4.4.3	MRP	29
4.4.3.1	MRP - 介质冗余协议	29
4.4.3.2	在 WBM 中组态	32
4.4.3.3	在 STEP 7 中组态	33
4.4.4	备用	37
4.4.5	并行冗余协议	39
4.5	VLAN	39
4.6	VLAN 标记	40
4.7	SNMP	43
4.8	服务质量	45
5	使用“基于 Web 的管理”进行组态	47
5.1	基于 Web 的管理	47
5.2	登录	49
5.3	“Information”菜单	52

5.3.1	起始页面.....	52
5.3.2	版本.....	58
5.3.3	I&M.....	59
5.3.4	ARP 表.....	61
5.3.5	日志表.....	62
5.3.6	故障.....	64
5.3.7	冗余.....	65
5.3.7.1	生成树.....	65
5.3.7.2	环网冗余.....	69
5.3.7.3	备用.....	71
5.3.8	以太网统计信息.....	74
5.3.8.1	Interface Statistics.....	74
5.3.8.2	Packet Size.....	75
5.3.8.3	Packet Type.....	77
5.3.8.4	Packet Error.....	78
5.3.8.5	历史.....	79
5.3.9	单播.....	81
5.3.10	组播.....	83
5.3.11	LLDP.....	84
5.3.12	光纤监视协议.....	86
5.3.13	DHCP 服务器 (DHCP Server).....	88
5.3.14	诊断 (Diagnostics).....	90
5.3.15	SNMP.....	91
5.3.16	Security.....	92
5.4	“System”菜单.....	95
5.4.1	组态 (Configuration).....	95
5.4.2	常规 (General).....	99
5.4.2.1	设备 (Device).....	99
5.4.2.2	坐标 (Coordinates).....	100
5.4.3	代理 IP (Agent IP).....	102
5.4.4	重启 (Restart).....	104
5.4.5	加载和保存.....	107
5.4.5.1	HTTP.....	108
5.4.5.2	TFTP.....	111
5.4.5.3	密码 (Passwords).....	115
5.4.6	事件.....	117
5.4.6.1	组态.....	117
5.4.6.2	严重程度过滤器 (Severity Filters).....	121
5.4.7	SMTP 客户端.....	122
5.4.8	DHCP.....	124
5.4.8.1	DHCP 客户端.....	124
5.4.8.2	DHCP 服务器.....	126
5.4.8.3	端口范围 (Port Range).....	129
5.4.8.4	DHCP 选项.....	130

5.4.8.5	中继代理信息	133
5.4.8.6	静态租用	135
5.4.9	SNMP	137
5.4.9.1	常规	137
5.4.9.2	陷阱	139
5.4.9.3	组	141
5.4.9.4	用户 (Users)	143
5.4.10	系统时间 (System Time)	146
5.4.10.1	手动设置 (Manual Setting)	146
5.4.10.2	DST 概述	148
5.4.10.3	DST 组态 (DST Configuration)	150
5.4.10.4	SNTP 客户端 (SNTP Client)	154
5.4.10.5	NTP 客户端 (NTP Client)	157
5.4.10.6	SIMATIC Time Client	160
5.4.11	自动注销	161
5.4.12	按钮	162
5.4.13	Syslog 客户端	163
5.4.14	端口	165
5.4.14.1	概述	165
5.4.14.2	组态	167
5.4.15	故障监视	171
5.4.15.1	电源	171
5.4.15.2	链路变化	172
5.4.15.3	冗余	174
5.4.16	PROFINET	174
5.4.17	EtherNet/IP	176
5.4.18	PLUG	178
5.4.18.1	组态	178
5.4.19	Ping	181
5.4.20	Power over Ethernet (PoE)	182
5.4.20.1	常规	182
5.4.20.2	端口	183
5.4.21	端口诊断	186
5.4.21.1	电缆测试器	186
5.4.21.2	SFP 诊断	188
5.5	“第 2 层”菜单	190
5.5.1	组态	190
5.5.2	Quality of Service (QoS)	194
5.5.2.1	常规	194
5.5.2.2	CoS 映射 (CoS Map)	195
5.5.2.3	DSCP 映射 (DSCP Map)	196
5.5.2.4	QoS 信任 (QoS Trust)	197
5.5.2.5	CoS 端口重映射	200
5.5.3	速率控制	202

5.5.4	VLAN.....	204
5.5.4.1	常规.....	204
5.5.4.2	GVRP.....	208
5.5.4.3	基于端口的 VLAN	209
5.5.5	镜像.....	212
5.5.5.1	常规.....	212
5.5.5.2	端口.....	214
5.5.6	动态 MAC 老化.....	216
5.5.7	环网冗余.....	217
5.5.7.1	环网.....	217
5.5.7.2	备用.....	220
5.5.8	生成树	222
5.5.8.1	常规.....	222
5.5.8.2	CIST 概述.....	223
5.5.8.3	CIST 端口.....	226
5.5.8.4	MST General.....	230
5.5.8.5	MST 端口	232
5.5.8.6	增强的被动侦听兼容性.....	235
5.5.9	回路检测.....	235
5.5.10	链路汇聚.....	238
5.5.11	DCP 转发	241
5.5.12	LLDP.....	243
5.5.13	光纤监视协议	244
5.5.14	单播.....	247
5.5.14.1	过滤.....	247
5.5.14.2	锁定端口 (Locked Ports).....	249
5.5.14.3	学习.....	251
5.5.14.4	未知单播阻止	252
5.5.15	组播.....	254
5.5.15.1	组.....	254
5.5.15.2	IGMP.....	257
5.5.15.3	GMRP	259
5.5.15.4	组播阻止.....	261
5.5.16	广播.....	262
5.5.17	RMON	264
5.5.17.1	Statistics.....	264
5.5.17.2	历史.....	266
5.6	“第 3 层”(Layer 3) 菜单.....	269
5.6.1	DHCP 中继代理	269
5.6.1.1	常规.....	269
5.6.1.2	选项.....	270
5.7	“Security”菜单	274
5.7.1	用户管理.....	274

5.7.2	用户	276
5.7.2.1	本地用户	276
5.7.3	密码	279
5.7.3.1	密码	279
5.7.3.2	选项	281
5.7.4	AAA	282
5.7.4.1	常规	282
5.7.4.2	RADIUS 客户端	283
5.7.4.3	802.1x 验证器	287
5.7.5	管理 ACL	292
6	故障排除/FAQ	297
6.1	使用 TFTP 下载新固件（无需 WBM 和 CLI）	297
6.2	消息：尚未接受 SINEMA 组态	299
	索引	301

简介

本组态手册的有效性

本组态手册涵盖了以下产品：

- SCALANCE XB-200
- SCALANCE XC-200
- SCALANCE XP-200

在下文中，这些产品还被称为工业以太网交换机、设备或网络组件。

一些设备有两种变型，分别使用不同的部件编号。这两种变型仅在出厂设置上有所不同。所有其它属性都完全相同。

本组态手册适用于以下软件版本：

- 自固件版本 2.0 起的 SCALANCE XB-200
- 自固件版本 2.1 起的 SCALANCE XC-200
- 自固件版本 2.0 起的 SCALANCE XP-200

出厂设置

PROFINET 型号

- 工业以太网协议：PROFINET
- 基础网桥模式：802.1D 透明网桥
- 冗余机制：环网冗余
- 信任模式：信任 COS

EtherNet/IP 型号

- 工业以太网协议：EtherNet/IP
- 基础网桥模式：802.1Q VLAN 网桥
- 冗余机制：RSTP
- 信任模式：信任 COS-DSCP

本组态手册的用途

本组态手册旨在为用户提供安装、调试和运行工业以太网交换机所需的信息。其中包含了组态工业以太网交换机所需的信息。

文档说明

除了您当前阅读的组态手册外，产品还包含下列文档：

- 组态手册“SCALANCE XB-200/XC-200/XP-200 Command Line Interface”
本文档包含工业以太网交换机支持的 CLI 命令。
- 操作说明“SCALANCE XB-200”、“SCALANCE XC-200”和“SCALANCE XP-200”
这些文档包含产品安装、连接和认证的相关信息。

可从以下位置找到文档：

- 一些产品随附的数据介质中：
 - 产品 CD/产品 DVD
 - SIMATIC NET 手册集
- Siemens 工业在线支持的 Internet 页面。
 - SCALANCE XB-200
(<https://support.industry.siemens.com/cs/ww/zh/ps/15291/man>)
 - SCALANCE XC-200
(<https://support.industry.siemens.com/cs/ww/zh/ps/24185/man>)
 - SCALANCE XP-200
(<https://support.industry.siemens.com/cs/ww/zh/ps/21869/man>)

更多文档

在系统手册《工业以太网/PROFINET 工业以太网》和《工业以太网/PROFINET 无源网络组件》中，可以找到有关可在工业以太网网络中与该产品系列的设备一起使用的其它 SIMATIC NET 产品的信息。

其中还包含安装所需的通信伙伴的光学性能数据。

系统手册可在以下位置找到：

- 一些产品随附的数据介质中：
 - 产品 CD/产品 DVD
 - SIMATIC NET 手册集
- Siemens 工业在线支持的 Internet 页面中的以下条目 ID：
 - 27069465 (<http://support.automation.siemens.com/WW/view/en/27069465>)
《工业以太网/PROFINET 工业以太网》系统手册
 - 84922825 (<http://support.automation.siemens.com/WW/view/en/84922825>)
《工业以太网/PROFINET - 无源网络组件》系统手册

SIMATIC NET 手册

用户可在以下位置找到 SIMATIC NET 手册：

- 一些产品随附的数据介质中：
 - 产品 CD/产品 DVD
 - SIMATIC NET 手册集
- Siemens 工业在线支持 (<http://support.automation.siemens.com/WW/view/zh>)的 Internet 页面。

SIMATIC NET 词汇表

对于本文档中所用的许多专业术语，SIMATIC NET 词汇表部分都给了解释。

用户可在以下位置找到 SIMATIC NET 词汇表：

- SIMATIC NET 手册集或产品 DVD
该 DVD 随一些 SIMATIC NET 产品一起提供。
- 请参见 Internet 上的以下条目 ID：
50305045 (<http://support.automation.siemens.com/WW/view/zh/50305045>)

安全提示:

Siemens

为其产品及解决方案提供了工业安全功能，以支持工厂、系统、机器和网络的安全运行。

为了防止工厂、系统、机器和网络受到网络攻击，需要实施并持续维护先进且全面的工业安全保护机制。Siemens 的产品和解决方案仅构成此类概念的其中一个要素。

客户负责防止其工厂、系统、机器和网络受到未经授权的访问。只有在必要时并采取适当安全措施（例如，使用防火墙和网络分段）的情况下，才能将系统、机器和组件连接到企业网络或 Internet。

此外，应考虑遵循 Siemens

有关相应安全措施的指南。更多有关工业安全的信息，请访问

<http://www.siemens.com/industrialsecurity> (<http://www.siemens.com/industrialsecurity>)。

Siemens 不断对产品和解决方案进行开发和完善以提高安全性。Siemens

强烈建议您及时更新产品并始终使用最新产品版本。如果使用的产品版本不再受支持，或者未能应用最新的更新程序，客户遭受网络攻击的风险会增加。

要及时了解有关产品更新的信息，请订阅 Siemens 工业安全 RSS 源，网址为

<https://support.industry.siemens.com/cs/ww/en/ps/15247/pm>

(<https://support.industry.siemens.com/cs/ww/zh/ps/15247/pm>)。

许可证条款

说明

开源软件

在使用本产品之前，请仔细阅读开源软件的许可证条款。

可以在 WBM 中的“系统 > 加载和保存 > Copyright”(System > Load&Save > Copyright) 页面上下载许可证条款。

商标

下文的一些名称以及可能的其它名称不带注册商标符号®，它们均为 Siemens AG 的注册商标：

SIMATIC NET, SCALANCE, C-PLUG, OLM

固件

固件已签名且加密。这可确保只能将 Siemens 创建的固件下载到设备。

说明

2.1 系统功能硬件设备

系统功能的可用性

下表列出了工业以太网交换机上系统功能的可用性：请注意，本组态手册和在线帮助中介绍了所有功能。根据您的工业以太网交换机，某些功能不可用。

我们保留进行技术更改的权利。

		SCALANCE XB-200	SCALANCE XC-200	SCALANCE XP-200
信息	ARP 表	✓	✓	✓
	日志表	✓	✓	✓
	以太网统计信息	✓	✓	✓
	诊断（温度）	-	✓	✓
系统	SMTP 客户端	✓	✓	✓
	DHCP 客户端	✓	✓	✓
	DHCP 服务器	✓（受限）	✓	✓
	SNMP	✓	✓	✓
	手动设置时间	✓	✓	✓
	DST	-	✓	✓
	SNTP	✓	✓	✓
	NTP	✓	✓	✓
	SIMATIC 时间客户端	✓	✓	✓
	NFC	-	✓	-
	自动注销	✓	✓	✓
	Syslog 客户端	✓	✓	✓
	故障监视	✓	✓	✓
	PROFINET	✓	✓	✓
EtherNet/IP	✓	✓	✓	

2.1 系统功能硬件设备

		SCALANCE XB-200	SCALANCE XC-200	SCALANCE XP-200
	以太网供电	-	-	√（设备名称中有标识符“PoE”）
	电缆测试器	√	√	√
	SFP 诊断	-	√	-
	光纤监视	-	√	-
第 2 层	发送优先级	-	√	√
	CoS 分配	√	√	√
	DSCP 分配	√	√	√
	QoS 优先级	√	√	√
	CoS 端口重新分配	-	√	√
	Load control	√	√	√
	GVRP	-	√	√
	基于端口的 VLAN	√	√	√
	交换机端口 VLAN 主干	-	√	√
	基于端口的镜像	√	√	√
	动态 MAC 老化	√	√	√
	环网冗余	√	√	√
	备用	√	√	√
	观察器	-	√	√
	生成树	√	√	√
	RSTP	√	√	√
	MSTP	-	√	√
	增强的被动侦听兼容性	√	√	√
	回路检测	√	√	√
	链路汇聚	-	√	√
	DCP 转发	√	√	√
LLDP	√	√	√	
单播过滤器	√	√	√	
锁定端口	√	√	√	

		SCALANCE XB-200	SCALANCE XC-200	SCALANCE XP-200
	单播学习	✓	✓	✓
	单播阻止	✓	✓	✓
	组播组	✓	✓	✓
	IGMP	✓	✓	✓
	GMRP	-	✓	✓
	组播阻止	✓	✓	✓
	广播阻止	✓	✓	✓
	RMON	✓	✓	✓
	RMON 历史	-	✓	✓
第 3 层	DHCP 中继代理	✓	✓	✓
Security	密码	✓	✓	✓
	RADIUS 验证	✓	✓	✓
	MAC 验证	-	✓	✓
	访客 VLAN	-	✓	✓
	802.1X 验证	✓	✓	✓
	管理 ACL	✓	✓	✓

2.1 系统功能硬件设备

硬件的可用性

下表列出了工业以太网交换机的硬件。

我们保留进行技术更改的权利。

	SCALANCE XB-200	SCALANCE XC-200	SCALANCE XP-200
C-PLUG 支持	-	✓	✓
SELECT/SET 按钮	-	✓ 1) 2) 3)	✓ 2) 3)
RESET 按钮	✓ 1)	-	✓ 1)
信号触点	-	✓	✓
串口	✓	✓	✓
显示模式	-	✓	✓
可插拔收发器插槽	-	✓	-

按钮的功能：

- 1) 复位为出厂设置
- 2) 通过冗余管理器切换
- 3) 设置故障掩码

2.2 产品特征

工业以太网交换机具有以下属性：

- 以太网接口支持以下模式：
 - 全双工和半双工 10 Mbps 和 100 Mbps
 - 1000 Mbps 全双工（带适当可插拔收发器的 XC206-2SFP 和 SCALANCE XP216）
 - 自动协商
 - 自动跨接
 - 自动极性变换

- EtherNet/IP

EtherNet/IP（以太网/工业协议）是基于 TCP/IP 和 UDP/IP 的工业实时以太网开放式工业标准。

- PROFINET

PROFINET（过程现场网络）是基于 TCP/IP 和 IT 标准的工业实时以太网开放式工业标准。可通过 PROFINET 将分布式 IO 设备连接到控制器。

- 冗余方法生成树协议。

生成树冗余机制定义了网络中各节点之间的多个连接路径，其中只有一个路径处于激活状态。这可抑制回路并优化路径。

- 虚拟网络 (Virtual networks, VLAN)

要想构建节点数快速增加的工业以太网，可以将一个物理网络分成若干个虚拟子网。

- 可限制使用组播和广播协议时（例如，视频传输）的负载

工业以太网交换机通过学习组播源和目标（IGMP 监听、IGMP 查询器），可以对组播数据通信进行过滤并减少网络中的负载。可以对组播和广播数据通信加以限制。

- 时钟同步

日志表条目、电子邮件等诊断消息具有时间戳。通过与 SICLOCK 时间发送器或 SNTP/NTP

服务器进行同步，本地时间在整个网络中保持一致，这使得识别多个设备的诊断消息更为轻松。

2.3 安装和操作的要求

- 用于对网络流量进行分类的服务质量符合 CoS (Class of Service, 服务等级 - IEEE 802.11Q) 和 DSCP (Differentiated Services Code Point, 区分服务代码点 - RFC 2474)
- 端口镜像
镜像功能允许将一个端口的数据流镜像到另一个端口 (监视端口)。然后可在该监视端口对数据流进行分析, 而不影响数据通信。
- 符合 IEEE 802.1x 标准的网络访问保护
根据 IEEE 802.1x, 可以为支持验证的终端设备组态端口。通过 RADIUS 服务器进行验证, 且必须能通过网络访问到该服务器。
- 日志表
日志表记录操作期间发生的事件。用户可以指定将生成表中条目的事件。
- 使用链路汇聚 (IEEE 802.1AX) 捆绑端口 (SCALANCE XC-200/SCALANCE XP-200)

2.3 安装和操作的要求

工业以太网交换机的安装和操作要求

必须具有能够联网的 PG/PC, 才能对工业以太网交换机进行组态。
必须为工业以太网交换机分配一个在网络中可用的 IP 地址, 另请参见“IP 地址的初始分配 (页 20)”。

IP 地址分配

3.1 IP 地址的结构

地址类别

IP 地址范围	最大网络数	最大主机/网络数	类别	CIDR
1.x.x.x 至 126.x.x.x	126	16777214	A	/8
128.0.x.x.x 至 191.255.x.x.x	16383	65534	B	/16
192.0.0.x 至 223.255.255.x	2097151	254	C	/24
224.0.0.0 - 239.255.255.255	组播应用		D	
240.0.0.0 - 255.255.255.255	为将来的应用保留		E	

一个 IP 地址由 4 个字节组成。每个字节由一个十进制数表示，并且用点与前一个字节隔开。结果得到如下结构，其中的 XXX 代表一个介于 0 到 255 之间的数字：

XXX.XXX.XXX.XXX

IP 地址由网络 ID 和主机 ID 这两部分组成，因此可以创建不同的子网。根据用作网络 ID 与主机 ID 的 IP 地址字节，可以将 IP 地址归到特定的地址类别中。

子网掩码

可用主机 ID 的位创建子网。起始位代表子网地址，其余位代表子网中的主机地址。

子网由子网掩码定义。子网掩码的结构与 IP 地址的结构一致。如果子网掩码中的一位为“1”，则该位属于子网地址的 IP 地址中的相应位置，否则属于计算机地址。

B 类网络示例：

B 类网络的标准子网地址是 255.255.0.0；也就是说，可用最后两个字节来定义子网。如果必须定义 16 个子网，则必须将子网地址的第 3 个字节设为 11110000（二进制表示）。在这种情况下，子网掩码为 255.255.240.0。

3.2 IP 地址的初始分配

要查明两个 IP 地址是否属于同一个子网，将拿这两个 IP 地址与子网掩码按位进行逻辑与运算。如果两个逻辑运算的结果相同，则说明两个 IP 地址属于同一子网，例如 141.120.246.210 和 141.120.252.108。

在局域网之外，网络 ID 和主机 ID 之间的区别并不重要，在这种情况下，将根据完整的 IP 地址传送数据包。

说明

在子网掩码的位表示中，必须按左对齐方式设置“1”，也就是说，“1”之间不能有“0”。

3.2 IP 地址的初始分配

组态选项

不能使用基于 Web 的管理 (Web Based Management, WBM)

为工业以太网交换机分配初始 IP 地址，因为这个组态工具只能在事先已经具有 IP 地址的情况下使用。

可通过以下方法将 IP 地址分配给未组态的设备：

- **DHCP**（出厂设置）
- **Primary Setup Tool (PST)**
 - 要使用 PST 将 IP 地址分配给工业以太网交换机，必须能通过以太网访问工业以太网交换机。
 - 可以在 Siemens 工业在线支持 Internet 页面的条目 ID 19440762 (<http://support.automation.siemens.com/WW/view/zh/19440762>) 下找到 PST。
 - 有关使用 PST 分配 IP 地址的详细信息，请参见文档“Primary Setup Tool (PST)”。

- **STEP 7**

在 STEP 7 中，可以组态拓扑、设备名称和 IP 地址。如果将未组态的工业以太网交换机连接至控制器，控制器会自动为工业以太网交换机分配已组态的设备名称和 IP 地址。

- **STEP 7**

- SCALANCE XB-200: V5.5.4 及更高版本

- SCALANCE XC-200: V5.5.4 HF11 及更高版本

- SCALANCE XP-200: V5.5.4 HF9 及更高版本

- 有关使用 STEP 7 分配 IP 地址的详细信息，请参见文档“组态硬件和通信连接 STEP 7”的“PROFINET IO 系统组态步骤”部分。

- **STEP 7 Basic 或 Professional**

- SCALANCE XB-200: V13 SP1 及更高版本

- SCALANCE XC-200: V14 及更高版本

- SCALANCE XP-200: V14 及更高版本

- 有关使用 STEP 7 分配 IP 地址的详细信息，请参见在线帮助“信息系统”的“寻址 PROFINET 设备”部分。

- 使用 **CLI** 通过串行接口分配

- 有关使用 CLI 分配 IP 地址的详细信息，请参见“SCALANCE XB-200/XC-200/XP-200 Command Line Interface”文档。

- **NCM PC**

- 有关使用 NCM PC 分配 IP 地址的详细信息，请参见文档“调试 PC 站 - 手册及快速入门”的“创建 PROFINET IO 系统”部分。

说明

产品出厂时以及在“恢复出厂默认设置并重启”后，DHCP 都处于启用状态。如果局域网中有 DHCP 服务器，且能回应工业以太网交换机的 DHCP 请求，则在设备初次启动时会自动分配 IP 地址、子网掩码和网关。

3.3 用 DHCP 进行地址分配

DHCP 属性

DHCP (Dynamic Host Configuration Protocol, 动态主机配置协议) 是一种自动分配 IP 地址的方法。它具有下列特性:

- 启动设备时和设备运行期间均可使用 DHCP。
- 分配的 IP 地址仅在有限时间 (称为租用时间) 内有效。当有效时间段过半后, DHCP 客户端可延长所分配 IPv4 地址的有效时间。当整个时间段过期后, DHCP 客户端需要请求新的 IPv4 地址。
- 如果设备在租用时间到期之前没有将新请求发送到 DHCP 服务器, 则继续使用已分配的 IP 地址、子网掩码和网关。

因此, 即使没有 DHCP 服务器, 通过上次分配的 IP 地址仍然可访问设备。这不是办公设备的标准行为, 但对无故障运行的工厂来说却是必要的。

- 通常不会分配固定的地址; 即, 当客户端再次请求 IP 地址时, 它通常会接收到一个与之前不同的地址。可以对 DHCP 服务器进行组态, 使得 DHCP 客户端发出请求后, 总是接收到同一个固定地址。用来将 DHCP 客户端标识为固定地址分配的参数在 DHCP 客户端和服务器上设置。可以通过 MAC 地址、DHCP 客户端 ID、PROFINET 或系统名称分配地址。在“系统 > DHCP > DHCP 客户端”(System > DHCP > DHCP Client) 中组态参数。

技术基础

4.1 组态限制

设备的组态限制

下表列出了设备基于 Web 的管理和命令行接口的组态限制。

根据您的工业以太网交换机，某些功能不可用。

	可组态的功能	最大数量		
		SCALANCE XB-200	SCALANCE XC-200	SCALANCE XP-200
系统	最大帧大小（传入）	1632 字节		
	Syslog 服务器	3		
	电子邮件服务器	3		
	DHCP 池	16 ¹⁾	24	
	每个 DHCP 池的 IPv4 地址	1	24	
	DHCP 服务器管理的 IPv4 地址（动态 + 静态）	16 ¹⁾	575	
	每个 DHCP 池的 DHCP 静态分配	-	24	
	SNMP 陷阱接收方	10		
	SNTP 服务器 (SNTP server)	1		
	NTP 服务器	1		
	代理/TIA 接口 ²⁾	1		
第 2 层	虚拟 LAN（基于端口，包括 VLAN 1）	17	257	
	镜像会话	1		
	多重生成树实例	-	4	
	链路汇聚或以太信道（每个汇聚最多 8 个端口）	-	8	
	一个链路汇聚中的端口数	-	8	
	单播过滤	128		

4.1 组态限制

	可组态的功能	最大数量		
		SCALANCE XB-200	SCALANCE XC-200	SCALANCE XP-200
	无活动 GMRP 的组播地址	256	512	
	有活动 GMRP 的组播地址	-	50	
	FDB（转发数据库）中的静态 MAC 地址	128		
第 3 层	DHCP 中继代理接口	1		
	DHCP 中继代理服务器	4		
安全性	RADIUS 服务器的 IP 地址	4		
	管理 ACL（管理性访问规则）	10		

- 1) 使用 SCALANCE XB-200 时，DHCP 池的数量和可管理 IPv4 地址的数量取决于端口的数量。端口的数量对应于 DHCP 池和可管理 IPv4 地址的最大数量。
- 2) 这是 IP 接口。

4.2 PROFINET

PROFINET

PROFINET 是基于工业以太网的工业自动化开放式标准 (IEC 61158/61784)。PROFINET 使用现有 IT 标准，支持现场级到管理级以及工厂范围的工程系统的端到端通信。PROFINET 还具有下列特性：

- 使用 TCP/IP 协议
- 满足实时要求的自动化应用
 - 实时 (RT) 通信
 - 等时实时 (IRT) 通信
- 无缝集成现场总线系统

在“系统 > PROFINET”(System > PROFINET) (页 174) 中组态 PROFINET。

PROFINET IO

在 PROFINET 的框架内，PROFINET IO 是实现模块化、分布式应用的通信机制。PROFINET IO 由可编程控制器的 PROFINET 标准 (IEC 61158-x-10) 实现。

4.3 EtherNet/IP

EtherNet/IP

EtherNet/IP (以太网/工业协议) 是基于 TCP/IP 和 UDP/IP 的工业实时以太网开放式工业标准。通过 EtherNet/IP，应用层中的通用工业协议 (Common Industrial Protocol, CIP) 可扩展以太网。在 EtherNet/IP 中，OSI 参考模型的低层由以太网通过物理网络和传输功能采用。

在“系统 > EtherNet/IP (页 176)”(System > EtherNet/IP) 中组态 EtherNet/IP。

通用工业协议

通用工业协议 (CIP) 是一种自动化应用协议，支持工业以太网和 IP 网络中现场总线的转换。现场总线/工业网络（如 DeviceNet、ControlNet 和 EtherNet/IP）将此工业协议用作应用层中的接口以连接确定性现场总线领域和自动化应用（控制器、I/O、HMI、OPC ...）。CIP 位于传输层上方，通过自动化工程的通信服务来扩展纯传输服务。其中包括周期性、时间要求严格和事件控制的数据通信服务。CIP 区分时间要求严格的 I/O 消息（隐式消息）和用于组态与数据采集的各个查询/响应帧（显式消息）。CIP 面向对象；所有从外部“可见”的数据都可通过对象的形式进行访问。CIP 具有通用组态基础：EDS（电子数据表）。

电子数据表

电子数据表（Electronic Data Sheet, EDS）是描述设备的电子数据表。可在“系统 > 加载和保存 (页 107)”(System > Load&Save) 中找到 EtherNet/IP 操作所需的 EDS。

4.4 冗余机制

4.4.1 生成树

避免在冗余连接中形成环路

生成树算法允许创建在两个工业以太网交换机/网桥之间有多个连接的网络结构。生成树通过仅允许一条路径并禁用其它（冗余）端口的数据通信，防止在网络中形成环路。如果路径中断，可以通过备用路径发送数据。生成树算法的功能基于组态和拓扑变更帧之间的交换。

使用组态帧定义网络拓扑

设备彼此交换的组态帧被称为 BPDU（Bridge Protocol Data Unit, 桥接协议数据单元），用于计算拓扑。通过这些帧选择根网桥并创建网络拓扑。BPDU 还可引起根端口的状态变化。

根网桥是控制所有相关组件的生成树算法的网桥。

一旦指定根网桥，每台设备就会设置一个根端口。根端口是对于根网桥路径开销最低的端口。

对网络拓扑变化的响应

无论在网络中添加节点还是删除节点，都会影响对最佳数据包路径的选择。为了能够响应这种变化，根网桥会以规定的时间间隔发送组态消息。可以用“呼叫时间”(Hello Time)参数设置两个组态消息之间的时间间隔。

使组态信息保持最新

可以用“最大使用期限”(Max Age)参数来设置组态信息的最长有效期。如果网桥具有比“最大使用期限”(Max Age)中设置的时间更早的信息，则它会放弃该消息并重新计算路径。

网桥不会立即使用新的组态数据，而是在经过“转发延迟”(Forward Delay)参数中指定的时间之后才使用。这样可确保只有在所有网桥均获得所需信息之后才以新拓扑运行。

4.4.1.1 RSTP、MSTP、CIST

快速生成树协议 (RSTP)

STP

的一个缺点是如果出现中断或设备故障，网络需要对自身进行重新组态：仅当出现中断时设备才会开始协商新路径。这最多需要 30 秒钟的时间。为此，STP 得到了扩展以创建“快速生成树协议”（RSTP，IEEE 802.1w）。设备在正常运行期间已经收集到有关备选路径的信息，不需要在发生中断后再收集此信息，这点与 STP 有本质区别。这意味着，由 RSTP 控制的网络的重新组态时间可以缩短至几秒钟。

通过使用以下功能可以实现这一点：

- 边缘端口（终端节点端口）
边缘端口是指连接到终端设备的端口。
定义为边缘端口的端口会在建立连接后立即激活。如果在边缘端口接收到生成树 BPDUs，该端口将失去其作为边缘端口的角色，并重新参与 (R)STP。如果经过特定的时间（3 倍呼叫时间）后没有再接收到任何 BPDUs，则该端口返回到边缘端口状态。
- 点对点（两个邻近设备之间直接通信）
通过直接连接两个设备，可以无延迟地进行状态变化（重新组态端口）

4.4 冗余机制

- 备用端口（根端口的替代端口）
组态根端口的替代端口。如果失去与根网桥的连接，设备可以通过备用端口建立连接，不存在由重新组态导致的延迟。
- 对事件的反应
快速生成树可无延迟地对事件（例如连接中止）做出反应。不用像在生成树中一样等待计时器。
- 最大网桥跳跃计数器
数据包自动变为无效之前所允许的网桥跳跃数。

因此，原则上，在快速生成树中，已预先组态多个参数的备选项，并且会考虑网络结构的某些属性，以减少重新组态时间。

多重生成树协议 (MSTP)

多重生成树协议 (MSTP) 是对快速生成树协议的进一步发展。此外，它还允许在不同的 VLAN 或 VLAN 组中操作多个 RSTP 实例，例如，使各个 VLAN 中的路径可用，而单个快速生成树协议则会导致全局阻塞。

公共内部生成树 (CIST)

CIST 可识别交换机使用的在原理上与 RSTP 内部实例类似的内部实例。

4.4.2 HRP

HRP - 高速冗余协议

HRP

是适用于环型拓扑网络的一种冗余方法的名称。交换机通过环网端口互连。其中一台交换机组态为冗余管理器 (RM, Redundancy Manager)。其它交换机为冗余客户端。冗余管理器通过测试帧检查环网以确保其没有中断。冗余管理器通过环网端口发送测试帧并检查其它环网端口是否接收到这些测试帧。冗余客户端转发测试帧。

如果由于网络中断导致 RM 发送的测试帧无法到达其它环网端口，则 RM 将在自身的两个环网端口之间切换并立即将切换情况通知给冗余客户端。环中断后的重新组态时间最长为 300 ms。

备用冗余

借助备用冗余方法可以将分别通过高速冗余实现保护的环网以冗余方式连接起来。在环网中，将组态主/从设备对，并且设备对通过自身的环网端口彼此监视对方。如果发生故障，数据通信从一个以太网连接（主设备或备用服务器的备用端口）重定向到其它以太网连接（从设备的备用端口）。

要求

- 在具有最多 50 个设备的环型拓扑中支持 HRP。
超过此设备数可能导致通信数据丢失。
- 只有支持 HRP 功能的设备才能在环网中使用。
- 不支持 HRP 的设备必须通过具有 HRP 功能的特殊设备连接到环网中。到达环网之前的连接不是冗余的。
- 所有设备必须通过其环网端口互连。在两台工业以太网交换机之间可实现最长 3 km 的多模连接和最长 26 km 的单模连接。在更远的距离，指定的重新组态时间可能更长。
- 必须将环中一个设备组态为冗余管理器，通过选择“HRP 管理器”(HRP Manager) 设置来执行。在环中所有其它设备上，必须激活“HRP 客户机”(HRP Client) 或“自动冗余检测”(Automatic Redundancy Detection) 模式。
- 您可在基于 Web 的管理、命令行接口中或通过 SNMP 组态 HRP。

4.4.3 MRP

4.4.3.1 MRP - 介质冗余协议

“MRP”方法符合以下标准中规定的“介质冗余协议”(MRP, Media Redundancy Protocol):
IEC 62439-2 版本 1.0 (2010-02) Industrial communication networks - High availability automation networks Part 2: Media Redundancy Protocol (MRP)

环中断后的重新组态时间最长为 200 ms。

拓扑

下图显示了使用 MRP 的环中设备的可能拓扑。

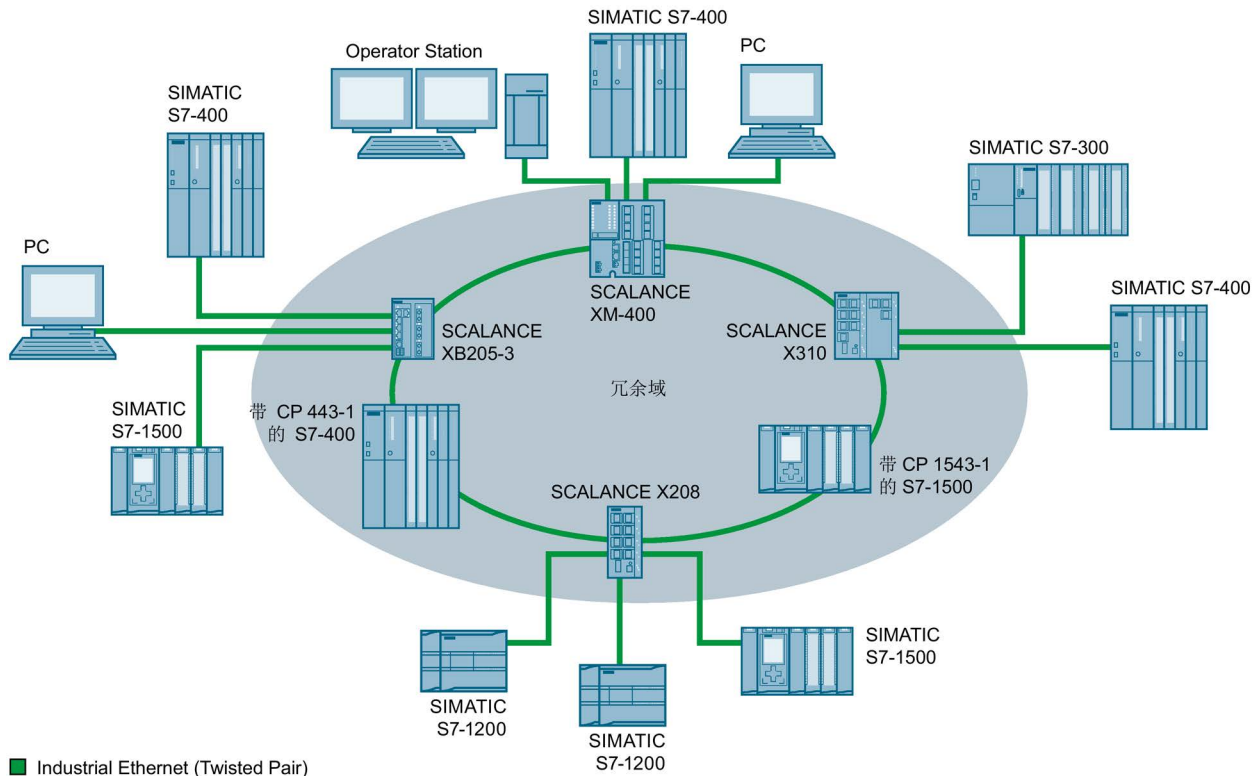


图 4-1 支持 MRP 介质冗余协议的环型拓扑示例

以下规则适用于使用 MRP 的具有介质冗余的环型拓扑：

- 在环型拓扑中连接的所有设备属于同一个冗余域的成员。
- 环中的一个设备用作冗余管理器。
- 环中的所有其它设备是冗余客户端。

非 MRP 兼容的设备可通过 SCALANCE X 交换机或带具有 MRP 功能的 CP 的 PC 连接到环中。

要求

使用 MRP 介质冗余协议进行无故障操作的要求如下：

- 在具有最多 50 个设备的环型拓扑中支持 MRP。
超过此设备数可能导致通信数据丢失。
- 要在其中使用 MRP 的环只能包括支持此功能的设备。
这些设备包括某些工业以太网 SCALANCE X 交换机、某些适用于 SIMATIC S7 和 PG/PC 的通信处理器 (CP) 或支持此功能的非 Siemens 设备等。
- 所有设备必须通过其环网端口互连。
在两台 SCALANCE X 工业以太网交换机之间可实现最长 3 km 的多模连接和最长 26 km 的单模连接。在更远的距离，指定的重新组态时间可能更长。
- 必须在环中的所有设备上激活“MRP”（请参见“在 STEP 7 中组态 (页 33)”部分）。
- 所有环网端口的连接设置（传送介质/双工）必须设置为全双工和至少 100 Mbps。否则，可能丢失通信数据。
 - STEP 7: 在属性对话框的“选项”(Options) 选项卡中将环中涉及的所有端口设置为“自动设置”(Automatic settings)。
 - WBM: 如果通过基于 Web 的管理进行组态，环网端口会自动设置为自动协商。

4.4.3.2 在 WBM 中组态

角色

请根据以下使用案例来选择角色：

- 想要在仅有西门子设备的环型拓扑中使用 MRP：
 - 针对环网中的至少一台设备，选择“自动冗余检测”或“MRP 自动管理器”。
 - 针对环网中的所有其它设备，选择“MRP 客户端”或“自动冗余检测”。
- 想要在同时包含非西门子设备的环型拓扑中使用 MRP：
 - 针对环网中的一台设备，选择“MRP 自动管理器”角色。
 - 针对环型拓扑中的所有其它设备，选择“MRP 客户端”角色。

说明

使用非西门子设备时，无法使用“自动冗余检测”。

- MRP 环型拓扑中的部分设备使用 WBM 组态，部分使用 STEP 7 组态：
 - 针对使用 WBM 组态的所有设备，选择“MRP 客户端”。
 - 针对使用 STEP 7 组态的设备，选择一个设备作为“Manager”或“Manager (Auto)”；针对所有其它设备，选择“MRP 客户端”。

说明

如果使用 STEP 7

为某个设备分配了“Manager”角色，则必须为环网中的所有其它设备分配“MRP 客户端”角色。如果环网中同时存在充当“Manager”角色和充当“Manager (Auto)”或“MRP Auto-Manager”角色的设备，则会引起帧循环传送，从而导致网络故障。

组态

在 WBM 中，您可以按照以下页面组态 MRP：

- 组态 (页 190)
- 环网 (页 217)

4.4.3.3 在 STEP 7 中组态

STEP 7 中的组态

要在 STEP 7 中创建组态，请在 PROFINET 接口上选择参数组“介质冗余”(Media redundancy)。

为设备的 MRP 组态设置以下参数：

- 域
- 角色
- 环网端口 (Ring port)
- 诊断中断

下文介绍了这些设置。

说明

有效的 MRP 组态

在 STEP 7 的 MRP 组态中，关闭环网之前，请确保环网中的所有设备都具有有效的 MRP 组态。否则，可能出现导致网络故障的循环帧。

环网中的一个设备需要组态为“冗余管理器”，环网中的其它设备则组态为“客户端”。

说明

注意出厂设置

对于下列全新工业以太网交换机以及复位为出厂设置的设备，禁用 MRP 并启用生成树：

- SCALANCE XB-200 (Ethernet/IP 型号)
- SCALANCE XP-200 (Ethernet/IP 型号)
- SCALANCE XM-400
- SCALANCE XR-500

要将 PROFINET 组态加载到其中一个指定的设备中，首先禁用设备上的生成树。

说明

更改角色

如果要更改 MRP 角色，首先打开环网。

说明

启动和重启

设备重启或电源故障和热启动后，MRP 设置仍然有效。

说明

优先级启动

如果在环中组态 MRP，则无法在所涉及设备上的 PROFINET 应用中使用“优先级启动”功能。

如果想要使用“优先级启动”功能，则在组态中禁用 MRP。

在 STEP 7 组态中，将相关设备的角色设置为“不是环中的节点”(Not a node in the ring)。

域

单 MRP 环网

如果要组态单 MRP 环网，请在“域”(Domain) 下拉列表中保留出厂设置“mrpdomain 1”。

环网中组态有 MRP

的所有设备都必须属于同一个冗余域。一台设备不能属于一个以上的冗余域。

如果将“域”设置留作工厂设置“mrpdomain-1”，则“角色”和“环端口”的缺省设置也将保持激活。

MRP 多环网

如果组态多 MRP 环网，将使用“域”(Domain) 参数将环网的节点分配给各个端口。

为环网内的所有设备设置相同的域。为不同的环网设置不同的域。不属于同一环网的设备必须具有不同的域。

角色

请根据以下使用案例来选择角色。

- 希望在仅包含 Siemens 设备的**单环网**拓扑中使用 MRP 且不监视诊断中断：
 - 将所有设备分配到“mrpdomain-1”域和角色“Manager (Auto)”。
 - 真正起冗余管理器作用的设备由 Siemens 设备自动进行协商。
- 希望在仅包含 Siemens 设备的**多环网**拓扑中使用 MRP 且不监视诊断中断（MRP 多环网）：
 - 为连接到环网的设备分配“Manager”角色。
 - 对于环型拓扑中的其它设备，选择“客户端”(Client) 角色。

- 希望在还包含非 Siemens 设备的环型拓扑中使用 MRP，或希望从设备接收与 MRP 状态相关的诊断中断（参见“诊断中断”）：
 - 只为环中的一台设备分配“Manager (Auto)”角色。
 - 对于环型拓扑中的其它设备，选择“客户端”(Client) 角色。
- 想要禁用 MRP：

如果不想使用 MRP 来运行环型拓扑中的设备，请选择“不是环中的节点”(Not node in the ring) 选项。

说明

复位为出厂设置后的角色

对于全新的 Siemens 设备以及复位为出厂设置的设备，设置以下 MRP 角色：

- “Manager (Auto)”
 - CP
- “Automatic Redundancy Detection”
 - SCALANCE X-200
 - SCALANCE XC-200
 - SCALANCE XB-200（PROFINET 型号）
 - SCALANCE XP-200（PROFINET 型号）
 - SCALANCE X-300
 - SCALANCE X-400

如果在环网中将非 Siemens 设备用作冗余管理器运行，可能导致通信数据丢失。

对于下列全新工业以太网交换机以及复位为出厂设置的设备，禁用 MRP 并启用生成树：

- SCALANCE XB-200（Ethernet/IP 型号）
 - SCALANCE XP-200（Ethernet/IP 型号）
 - SCALANCE XM-400
 - SCALANCE XR-500
-

环网端口 1/环网端口 2

请在此处将要组态的端口选作环网端口 1 和环网端口 2。

对于 8 个以上端口的设备，并不是所有端口都可以选作环网端口。

下拉列表中显示了每种设备类型可能的端口选项。如果在出厂设置中指定了端口，这些框会以灰色突出显示。

注意
复位为出厂设置后的环网端口
如果复位为出厂设置，也会复位环网端口设置。
如果复位前已将其它端口用作环网端口，则在特定的连接情况下，之前已正确组态的设备可能会引起数据帧循环传送，从而导致数据通信故障。

诊断中断

如果希望输出本地 CPU 上与 MRP 状态相关的诊断中断，请启用“诊断中断”(Diagnostic interrupts) 选项。

可能生成以下诊断中断：

- 接线或端口错误
 - 如果环网端口出现以下错误，就会生成诊断中断：
 - 环网端口上的连接中止
 - 环网端口的邻居不支持 MRP。
 - 环网端口连接到非环网端口。
 - 环网端口连接到其它 MRP 域的环网端口。
- 主动/被动状态更改（仅限冗余管理器）

如果环网的状态发生更改（主动/被动），则生成诊断中断。

不通过 STEP 7 设置冗余参数分配（冗余替代）

该选项仅会影响 SCALANCE X 交换机。如果想要使用 WBM、CLI 或 SNMP 等其它方式设置介质冗余的属性，则选择该选项。

如果启用该选项，则保留 WBM、CLI 或 SNMP 的现有冗余设置，且不会覆盖这些设置。之后，“MRP 组态”(MRP configuration) 框中的参数会复位并呈灰色显示。表示这些条目没有任何意义。

4.4.4 备用

常规

SCALANCE X

交换机不但支持环网内的环冗余，还支持在环网之间或开放网段（线性总线）之间采用冗余连接。在冗余链路中，环网通过以太网连接相连在一起。

实现的方法是在一个环网中组态一个主/从设备对，使设备对的设备能彼此监视对方，并且能在发生故障时将数据通信从常用的主以太网连接重定向到替代（从）以太网连接。

备用冗余

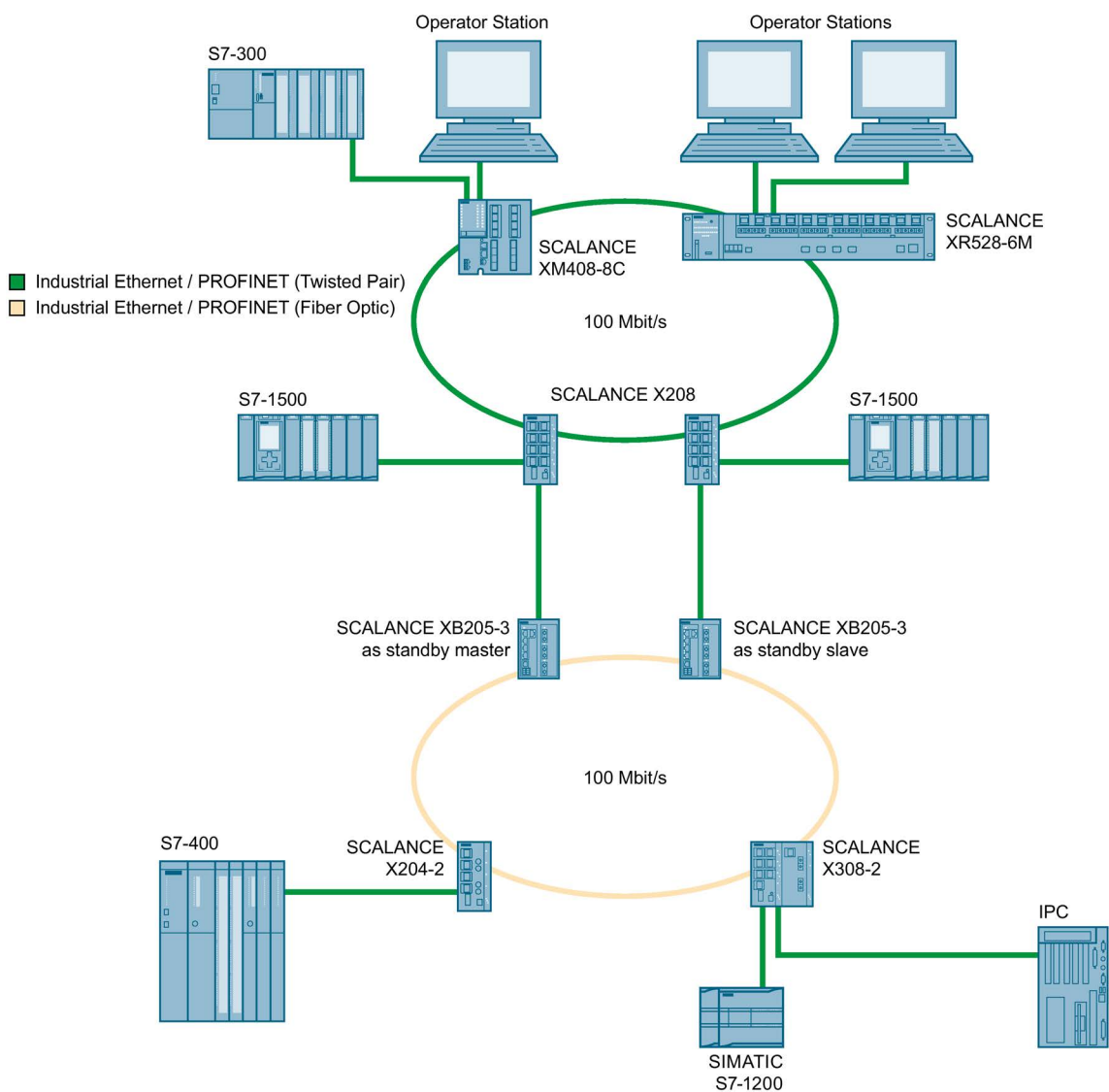


图 4-2 环网间的冗余链路示例

对于图示的冗余连接，必须将一个网段中的两台设备组态为备用冗余交换机。在本例中，网段是具有一个冗余管理器的环网。除环网外，网段也可能是线性的。

在组态中连接的两个备用冗余交换机彼此交换数据帧，以同步其工作状态（一个设备为主站，另一个为从站）。如果没发生问题，仅激活从主设备到另一网段的连接。如果此连接失败（例如，由于连接断开或设备故障），只要问题仍然存在，从设备就会激活其连接。

4.4.5 并行冗余协议

并行冗余协议

“并行冗余协议”(PRP) 是用于以太网网络的冗余协议。它是在 IEC 62439 标准的第 3 部分中定义的。如果网络中存在中断，该冗余方法有助于继续保持数据通信，而不会产生中断/重新组态时间。

例如，SCALANCE X-200RNA 产品系列设备支持 PRP 方法。

超长帧

发送 PRP 帧时，工业以太网交换机会通过 PRP 帧尾扩展帧。对于最大长度的帧，附加 PRP 帧尾会导致生成超过帧最大允许长度的超长帧（根据 IEEE 802.3 标准）。

要防止超长帧中的数据丢失，PRP 网络中的所有网络组件必须支持长度至少为 1528 个字节的帧。

本手册中介绍的设备可在 PRP 网络中使用，另请参见“组态限制 (页 23)”部分。

4.5 VLAN

与节点的空间位置无关的网络定义

VLAN（虚拟局域网）将物理网络划分成若干个相互屏蔽的逻辑网络。此时，设备组合在一起形成逻辑组。只有相同 VLAN 上的节点才能彼此寻址。因为仅在特定的 VLAN 中转发组播和广播帧，所以它们也称为广播域。

VLAN 的独特优势是可减少其它 VLAN 的节点和网段的网络负载。

要确定数据包属于哪个 VLAN，需要将帧扩展 4 个字节（VLAN 标记 (页 40)）。这种扩展不仅包括 VLAN ID，还包括优先级信息。

VLAN 分配选项

为设备的每个端口分配一个 VLAN ID（基于端口的 VLAN）。可在“第 2 层 > VLAN > 基于端口的 VLAN”(Layer 2 > VLAN > Port-based VLAN) (页 209) 中组态基于端口的 VLAN。

标记控制信息 (TCI)

两个字节的标记控制信息 (TCI) 包含以下信息：

QoS 信任

标记帧有 3 个位用于优先级，又称为服务类别 (Class of Service, CoS)，另请参见 IEEE 802.1Q。

CoS 位	优先级	数据通信的类型
000	0 (最低)	Background
001	1	Best Effort
010	2	Excellent Effort
011	3	Critical Applications
100	4	Video, < 100 ms 延时 (延迟和抖动)
101	5	Voice (语言), < 10 ms 延时 (延迟和抖动)
110	6	Internetwork Control
111	7 (最高)	Network Control

仅当组件中存在队列（可在其中缓冲优先级较低的数据包）时，方可实现数据包的优先级。

设备具有多个并行队列，可在其中处理各种优先级的帧。默认情况下，首先会处理具有最高优先级的帧。此方法可确保即使在数据通信繁忙时，具有最高优先级的帧仍能得到发送。

规范格式标识符 (CFI)

CFI 用于表示以太网与令牌环之间的兼容性。

其值的含义如下：

值	含义
0	MAC 地址格式符合规范。以规范形式表示 MAC 地址时，先传送最低有效位。以太网交换机的标准设置。
1	MAC 地址格式不符合规范。

4.6 VLAN 标记

VLAN ID

在 12 位数据字段中，最多可构成 4096 个 VLAN ID。存在以下惯例：

VLAN ID	含义
0	帧中仅包含优先级信息（标记有优先级的帧），不包含任何有效的 VLAN 标识符。
1- 4094	有效 VLAN 标识符，该帧被分配给某 VLAN 并且也可以包含优先级信息。
4095	预留

设备提供了同时引导入站或出站数据流经过其它接口以进行分析或监视的选项。这对受监视的数据流没有影响。此过程称为镜像。在此菜单部分，可启用或禁用镜像并设置参数。

镜像端口

镜像端口是指将工业以太网交换机的某个端口（镜像端口）上的数据通信复制到另一个端口（监视端口）。可以将一个或多个端口镜像到监视端口。

如果协议分析器与监视端口相连接，则可在不中断连接的情况下记录镜像端口的数据通信。这意味着可在不影响数据通信的情况下对数据通信进行研究。只有设备有空闲端口可用作监视端口时，才能实现此功能。

4.7 SNMP

简介

借助 (Simple Network Management Protocol , SNMP)，可以监视和控制中央站中的网络元件，例如路由器或交换机。SNMP 控制被监视设备与监视站之间的通信。

SNMP 的任务：

- 监视网络组件
- 远程控制网络组件，以及远程为网络组件分配参数
- 错误检测和错误通知

版本 v1 和 v2c 的 SNMP

没有安全机制。网络中的所有用户都可以访问数据，还可使用适当的软件来更改参数分配。

如果只需对访问权限进行简单控制而无需考虑安全性，则可使用团体字符串。

团体字符串与查询一起传送。如果团体字符串正确，SNMP 代理将做出响应并发送所请求的数据。如果团体字符串不正确，SNMP 代理将放弃查询。可以为读取和写入权限定义不同的团体字符串。团体字符串以明文形式传送。

团体字符串的标准值：

- **public**
具有只读权限
- **private**
具有读写权限

说明

由于 SNMP

团体字符串用于访问保护，请勿使用标准值“public”或“private”。请在初始调试之后更改这些值。

设备级的更多简单保护机制：

- **Allowed Host**
被监视系统知道监视系统的 IP 地址。
- **Read Only**
如果为被监视设备指定“Read Only”，则监视站只能读取数据，但无法更改。

SNMP 数据包未加密，其他用户可轻松读取。

中央站也称为管理站。SNMP 代理安装在与管理站交换数据的被监视设备上。

管理站发送以下类型的数据包：

- GET
向 SNMP 代理请求数据记录
- GETNEXT
调用下一条数据记录。
- GETBULK（自 SNMPv2c 起可用）
每次请求多条数据记录，例如，表中的多行。
- SET
包含相关设备的参数分配数据。

SNMP 代理发送以下类型的数据包：

- RESPONSE
SNMP 代理返回管理器请求的数据。
- TRAP
如果发生特定事件，SNMP 代理将发送陷阱。

SNMPv1/v2c/v3 使用 UDP（User Datagram Protocol，用户数据包协议）并使用 UDP 端口 161 和 162。管理信息库 (Management Information Base, MIB) 对该数据进行了介绍。

SNMPv3

与先前版本 SNMPv1 和 SNMPv2c 比较，SNMPv3 引入了广义的安全概念。

SNMPv3 支持：

- 完全加密的用户验证
- 对全部数据通信进行加密
- 在用户/组级别对 MIB 对象进行访问控制

4.8 服务质量

Quality of Service (QoS) 是一种有助于高效利用网络中现有带宽的方法。

QoS 通过排定数据传输的优先级来实现。传入帧根据特定优先级分类到 Queue 中，然后进行进一步处理。这为帧分配了特定的优先级。

各种不同的 QoS 方法相互影响，并按下列顺序加以考虑：

1. 交换机首先检查传入帧是广播帧还是代理帧。

→ 第一个条件满足时，交换机将考虑“常规 (页 194)”页上设置的优先级。

交换机将根据“CoS 映射 (CoS Map) (页 195)”页面上的分配将帧分类到队列中。

2. 如果第一个条件不满足，交换机将检查帧是否包含 VLAN 标记。

→ 如果第二个条件满足，交换机将检查“常规 (页 194)”页面上的优先级设置。交换机将检查是否为优先级设置了“非强制”(Do not force) 以外的值。

如果设置了优先级，交换机将根据“CoS 映射 (CoS Map) (页 195)”页面上的分配将帧分类到队列中。

3. 如果第二个条件也不满足，则将根据信任模式对帧进行进一步处理。信任模式在“QoS 信任 (QoS Trust) (页 197)”页面上组态。

参见

常规 (页 204)

使用“基于 Web 的管理”进行组态

5.1 基于 Web 的管理

工作原理

设备集成有 HTTP 服务器，可供“基于 Web 的管理”(WBM) 使用。如果通过 Internet 浏览器对设备进行寻址，则它会根据用户输入向客户端 PC 返回 HTML 页面。

用户在设备发送的 HTML

页面中输入组态数据。设备评估该信息，并动态生成响应页面。

这种方法的优势在于只需要在客户端上安装 Internet 浏览器。

说明

安全连接

WBM 也可用来通过 HTTPS 建立安全连接。

可使用 HTTPS 保护数据传输。如果希望只通过安全连接访问 WBM，则请激活“System > Configuration”下的“HTTPS Server only”选项。

要求

WBM 显示

- 设备具有 IP 地址。
- 设备与客户端 PC 之间存在连接。可以通过 ping 命令检查是否可以访问设备。
- 已启用通过 HTTPS 进行的访问。
- 在 Internet 浏览器中激活 JavaScript。

- 不可将 Internet

浏览器设置成每次从服务器访问页面时，浏览器都会重载页面。页面动态内容的更新是通过其它机制来确保的。在 Internet Explorer 中，可以在“选项 > Internet 选项 > 常规”(Options > Internet Options > General) 菜单的“浏览历史记录”(Browsing history) 部分，用“设置”(Settings)

按钮进行适当的设置。在“检查所存网页的较新版本：”(Check for newer versions of stored pages:) 下，选择“自动”(Automatically)。

5.1 基于 Web 的管理

- 如果使用了防火墙，则必须打开相关端口。
 - 若使用 HTTP 进行访问：TCP 端口 80
 - 若使用 HTTPS 进行访问：TCP 端口 443

WBM 的显示情况已使用如下桌面 Internet 浏览器测试过：

- Microsoft Internet Explorer 11
- Mozilla Firefox 38 ESR
- Google Chrome V50

说明

兼容性视图

为确保显示正确和使用 WBM 组态顺利，请在 Microsoft Internet Explorer 中禁用兼容性视图。

在移动设备上显示 WBM

对于移动设备，必须满足以下最低要求：

分辨率	操作系统
960 x 640 像素	Android（自版本 4.2.1 起） iOS（自版本 6.0.2 起）

已在移动设备上使用以下 Internet 浏览器执行过测试：

- 基于 iOS（自版本 V8.1.3 起）的 Apple Safari（自版本 8 起）（iPad Mini 型号 A1432）
- 基于 Android（自版本 5.0.2 起）的 Google Chrome（自版本 40 起）(Nexus 7C Asus)
- 基于 Android（自版本 5.0.2 起）的 Mozilla Firefox（自版本 35 起）(Nexus 7C Asus)

说明

在移动设备上使用 WBM 及其显示

在移动设备上显示 WBM

页面以及对页面的操作方式与桌面设备相比可能有所不同。一些页面的显示还针对移动设备进行过优化。

5.2 登录

建立与设备的连接

使用 Internet 浏览器按照以下步骤与设备建立连接：

1. 设备与客户端 PC 之间存在连接。可以通过 ping 命令检查是否可以访问设备。
2. 在 Internet 浏览器的地址框中，输入设备的 IP 地址或 URL。如果设备存在连接，就会显示基于 Web 的管理 (Web Based Management, WBM) 的登录页面。

使用 Internet 浏览器登录

选择 WBM 的语言

1. 从右上方的下拉列表中，选择 WBM 页面的语言版本。
2. 单击“Go”按钮更改为所选语言。

说明

可用语言

在此型号中，提供德语和英语。

The screenshot shows the Siemens WBM login interface. At the top left is the Siemens logo. At the top right, there is a language dropdown menu currently set to 'English' and a 'Go' button. On the left side, there is a sidebar with 'Name' and 'Password' input fields and a 'Login' button. The main content area has a large 'LOGIN' heading, followed by 'Name:' and 'Password:' labels with corresponding input fields, and a 'Login' button. Below the input fields, there is a link 'Switch to secure HTTP' and a note: 'For information about browser compatibility please refer to the manual'.

5.2 登录

使用 HTTP 登录

可以采用两种方法通过 HTTP

进行登录。可以使用浏览器窗口中央的登录选项进行登录，也可以使用其左上方区域的登录选项进行登录。

无论选择以上哪一种方法登录，都可以按照以下步骤进行操作：

1. “名称”(Name) 输入框：

- 如果是首次登录或是在“恢复出厂默认设置并重启”(Restore Factory Defaults and Restart) 后登录，则输入出厂时预设的用户“admin”。

使用这种用户帐户时，可以更改设备的设置（对组态数据进行读写访问）。

说明

出厂时设置的默认用户“user”

自固件版本 V2.1 起，出厂时设置的默认用户“user”在产品交付后不再可用。

如果将设备固件版本更新到

V2.1，用户“user”起初仍然可用。如果将设备复位为出厂设置（“恢复出厂默认设置并重启”(Restore Factory Defaults and Restart)），则用户“user”将被删除。

可以使用“user”角色创建用户。

- 输入已创建用户帐户的用户名。可在“安全 > 用户”(Security > Users) 中组态本地用户帐户。

2. “密码”(Password) 输入框：

- 如果是首次登录或是在“恢复出厂默认设置并重启”后登录，则输入出厂时预设的默认用户“admin”的密码“admin”。
- 输入相关用户帐户的密码。

3. 单击“登录”(Login) 按钮或按“Enter”键确认输入内容。

如果是以前用户“admin”的身份首次登录，或是在“恢复出厂默认设置并重启”之后登录，系统会提示您更改密码。

新密码必须符合以下密码策略：

- 密码长度：至少 8 个字符，最多 128 个字符。
- 至少 1 个大写字母
- 至少 1 个特殊字符
- 至少 1 个数字

您需要重新输入密码进行确认。密码输入必须匹配。

单击“设置值”(Set Values) 按钮，完成操作并激活新密码。

成功登录后，将显示起始页面。

使用 HTTPS 登录

“基于 Web 的管理”还允许通过 HTTPS 协议的安全连接与设备相连。请按下列步骤操作：

1. 单击登录页面上的链接“切换到安全的 HTTP”(Switch to secure HTTP)，或在 Internet 浏览器地址框中输入“https://”和设备的 IP 地址。
2. 检查显示的证书警告并在适用时进行确认。
将显示“基于 Web 的管理”登录页面。
3. “名称”(Name) 输入框：
 - 如果是首次登录或是在“恢复出厂默认设置并重启”(Restore Factory Defaults and Restart) 后登录，则输入出厂时预设的用户“admin”。

使用这种用户帐户时，可以更改设备的设置（对组态数据进行读写访问）。

说明

出厂时设置的默认用户“user”

自固件版本 V2.1 起，出厂时设置的默认用户“user”在产品交付后不再可用。

如果将设备固件版本更新到

V2.1，用户“user”起初仍然可用。如果将设备复位为出厂设置（“恢复出厂默认设置并重启”(Restore Factory Defaults and Restart)），则用户“user”将被删除。

可以使用“user”角色创建用户。

- 输入已创建用户帐户的用户名。可在“安全 > 用户”(Security > Users) 中组态本地用户帐户。

5.3 “Information”菜单

4. “密码”(Password) 输入框:

- 如果是首次登录或是在“恢复出厂默认设置并重启”后登录，则输入出厂时预设的默认用户“admin”的密码“admin”。
- 输入相关用户帐户的密码。

5. 单击“登录”(Login) 按钮或按“Enter”键确认输入内容。

如果是以前设用户“admin”的身份首次登录，或是在“恢复出厂默认设置并重启”之后登录，系统会提示您更改密码。

新密码必须符合以下密码策略:

- 密码长度: 至少 8 个字符，最多 128 个字符。
- 至少 1 个大写字母
- 至少 1 个特殊字符
- 至少 1 个数字

您需要重新输入密码进行确认。密码输入必须匹配。

单击“设置值”(Set Values) 按钮，完成操作并激活新密码。

成功登录后，将显示起始页面。

5.3 “Information”菜单

5.3.1 起始页面

起始页面视图

输入设备的 IP

地址并成功登录后，将显示起始页面。无法对该页面上的任何内容进行组态。

WBM 页面的常规布局

每个 WBM 页面通常都会有以下几个区域:

- 选择区 (1): 上方区域
- 显示区 (2): 上方区域

- 浏览区 (3): 左侧区域
- 内容区 (4): 中间区域

① SIEMENS English Go

192.168.16.202/SCALANCE XP216PoE EEC 01/01/2000 00:14:34

Welcome admin SCALANCE XP216PoE EEC

Logout

③

- Information
- System
- Layer 2
- Layer 3
- Security

Please select one item of the menu on the left

④

SCALANCE XP216PoE EEC

PROFINET Name of Station:

Diagnostics Mode: **PROFINET**

System Name: **sysName Not Set**

Device Type: **SCALANCE XP216PoE EEC**

PROFINET AR Status: **Offline**

Power Line 1: **Down**

Power Line 2: **Up**

PLUG Configuration: **ACCEPTED**

Fault Status: **No Fault**

Refresh

选择区 (1)

选择区中有以下内容：

- **Siemens AG 徽标**

当您点击徽标时，您将访问 Siemens 工业在线支持中相应基本设备的 Internet 页面。

- **显示：“系统位置/系统名称”(System Location / System Name)**

- “系统位置”(System Location) 包含设备的位置。
如果使用设备出厂时的设置，则会显示设备的 IP 地址。
- “系统名称”(System name) 是设备名称。
如果使用设备出厂时的设置，则会显示设备类型。

可以通过“System > General > Device”更改该显示画面的内容。

- 用于选择语言的下拉列表
- 系统日期和时间

可以通过“System > System Time”更改该显示画面的内容。

显示区 (2)

在显示区的上半部分，您可以看到当前登录用户的名称和当前所选菜单项的完整标题。

显示区的下半部分包含以下项目：

- **注销**

可以单击“注销”(Logout) 链接从任何 WBM 页面注销。



- **LED 模拟** 

每个设备都具有一个或多个

LED，用于提供有关设备工作状态的信息。根据其安装位置，可能不是总能直接访问设备。因此“基于 Web 的管理”显示的是仿真 LED。未使用的连接器会显示为灰显 LED。各种 LED 显示的含义在操作说明中进行了说明。

单击该按钮后，可以打开 LED

仿真窗口。可以在切换菜单过程中显示该窗口，并根据需要进行移动。要关闭 LED 仿真，请单击 LED 仿真窗口中的关闭按钮。

- **帮助** 单击此按钮时，将在新的浏览器窗口中打开当前所选菜单项的帮助页面。
帮助页面包含内容区的说明。在某些情况下，还会对设备上不可用的选项进行说明。
- **打印** 如果单击此按钮，将打开一个弹出窗口。此弹出窗口包含针对打印机优化过的页面内容视图。

说明

打印较大的表格

如果要打印较大的表格，请使用 Internet 浏览器的“打印预览”功能。

浏览区 (3)

在导航区中，可以使用各种菜单。单击各菜单可显示其子菜单。子菜单包含提供了信息的页面或可用来创建组态的页面。这些页面始终在内容区显示。

内容区 (4)

内容区显示设备图形。该图形始终显示 WBM 已被调用的设备。

设备图形下面会显示以下项目：

- **站的 PROFINET 名称 (PROFINET Name of Station)**
显示 PROFINET 设备名称。
- **诊断模式 (Diagnostics Mode)**
显示启用 EtherNet/IP 还是 PROFINET IO。
- **系统名称 (System Name)**
显示设备名称。
- **设备型号 (Device Type)**
显示设备的型号标识。

5.3 “Information”菜单

- **PROFINET AR 状态 (PROFINET AR Status)**

显示 PROFINET 应用关系状态。

 - 在线 (Online)

存在与 PROFINET 控制器的连接。PROFINET 控制器已将其组态数据下载到设备。设备可以将状态数据发送到 PROFINET 控制器。

在这种状态下，无法在设备上组态 PROFINET 控制器所设置的参数。
 - 离线 (Offline)

不存在与 PROFINET 控制器的连接。
- **电源 1 (Power Supply 1)/电源 2 (Power Supply 2)**
 - “接通”(Up)

电源 1 或 2 已接通
 - “无效”(Down):

电源 1 或 2 未接通或电压低于允许值。
- **PLUG 配置 (PLUG Configuration)**

显示 PLUG 上组态数据的状态，请参见“系统 > PLUG > 组态”(System > PLUG > Configuration) 部分。
- **“故障状态”(Fault Status)**

显示设备的故障状态。

常用按钮

WBM 页面中包含下列标准按钮：

- **使用“刷新”(Refresh) 按钮刷新显示画面**

在显示当前参数的“基于 Web 的管理”页面底部有一个“刷新”(Refresh) 按钮。单击该按钮可为当前页面请求设备的最新信息。

说明

如果在使用“设置值”(Set Values) 按钮将组态更改传送到设备之前单击“刷新”(Refresh) 按钮，则会删除更改，并会从设备加载之前的组态并在此进行显示。

- **使用“设置值”(Set Values) 保存条目**
在进行组态设置的页面底部有一个“设置值”(Set Values) 按钮。仅当至少更改了页面上的一个值时，该按钮才会激活。单击该按钮，可保存在设备上输入的组态数据。保存之后，该按钮会再次变为未激活状态。

说明

只有“admin”用户才能更改组态数据。

- **使用“创建”(Create) 按钮创建条目**
在可以创建新条目的页面底部有一个“创建”(Create) 按钮。单击该按钮可创建新条目。创建一个条目后，页面将进行更新。
- **使用“删除”(Delete) 按钮删除条目**
在可以删除条目的页面底部有一个“删除”(Delete) 按钮。单击该按钮可将之前选择的条目从设备内存中删除。删除一个条目后，页面将进行更新。
- **使用“下一页”(Next) 按钮向下翻页**
在含有许多数据记录的页面中，页面上能够显示的数据记录数受到限制。单击“下一页”(Next) 按钮，可向下翻页查看数据记录。
- **使用“上一页”(Prev) 按钮向上翻页**
在含有许多数据记录的页面中，页面上能够显示的数据记录数受到限制。单击“上一页”(Prev) 按钮，可向上翻页查看数据记录。

消息

如果您已启用“自动保存”(Automatic Save)

模式并且更改了一个参数，则显示区域中将出现如下消息“所做更改将在 x 秒内自动保存。按下‘写启动组态’(Write Startup Config) 可立即保存更改”(Changes will be saved automatically in x seconds.Press 'Write Startup Config' to save the changes immediately.)

说明

中断保存

只有消息中的定时器到期后，才会启动保存。此时将显示如下消息：“正在保存组态数据。请勿关闭设备”(Saving configuration data in progress. Please do not switch off the device)。保存所需的时间取决于设备。

- 不要在定时器到期后立即关闭设备。
-

5.3.2 版本

硬件和软件的版本

该页面会显示设备的硬件和软件版本。无法对该页面上的任何内容进行组态。

Version Information			
Hardware	Name	Revision	Order ID
Basic Device	SCALANCE XB208	1	6GK5 208-0BA00-2AB2
Software	Description	Version	Date
Firmware	SCALANCE XB200 Firmware	V02.00.00	06/10/2014 19:35:41
Bootloader	SCALANCE XB200 Bootloader	V02.00.00	06/04/2014 19:30:00
Firmware_Running	Current running Firmware	V02.00.00	06/10/2014 19:35:41

显示值说明

表 1 包含以下列：

- **硬件 (Hardware)** - 基本设备
显示基本设备。
- **名称 (Name)**
显示设备或模块的名称。
- **修订版 (Revision)**
显示设备的硬件版本。
- **订货 ID (Order ID)**
显示设备或所述模块的部件编号。

表 2 包含以下列：

- **Software**
 - 固件 (Firmware)
显示当前固件版本。如果下载了新的固件文件，并且尚未重启设备，则在此处显示已下载固件文件的固件版本。下次重启后会激活并使用下载的固件。
 - 引导加载程序 (Bootloader)
显示存储在设备上的引导软件的版本。
 - Firmware_Running
显示设备上当前使用的固件版本。
- **说明 (Description)**
显示软件的简要说明。
- **版本 (Version)**
显示软件版本的版本号。
- **日期 (Date)**
显示软件版本的创建日期。

5.3.3 I&M

标识和维护数据

该页面包含具体设备的供应商信息以及维护数据（如订单编号、序列号、版本号等）。无法对该页面上的任何内容进行组态。

Identification & Maintenance	
Manufacturer ID:	42
Order ID:	6GK5 208-0BA00-2AB2
Serial Number:	VPBN59912
Hardware Revision:	1
Software Revision:	V01.00.00
Revision Counter:	0
Revision Date:	01/04/2000 22:11:45
Function Tag:	Documentation Device
Location Tag:	Desktop
Date:	2014-12-05 15:13
Descriptor:	SCALANCE XB208 for Documentation
<input type="button" value="Refresh"/>	

显示值说明

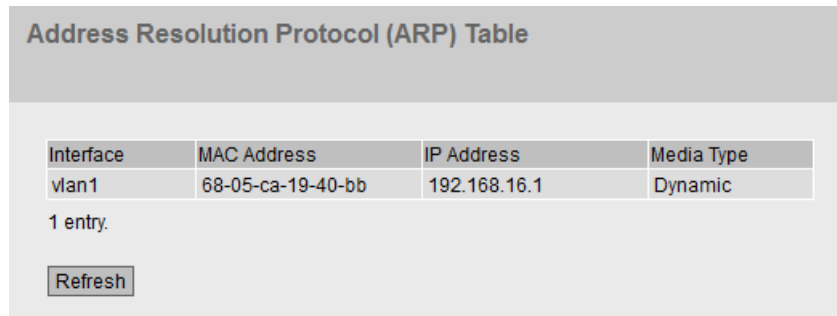
该表格包括以下行：

- **“制造商 ID”(Manufacturer ID)**
显示制造商 ID。
- **“订货号”(Order ID)**
显示订货号。
- **“序列号”(Serial Number)**
显示序列号。
- **“硬件版本”(Hardware Revision)**
显示硬件版本。
- **软件版本 (Software version)**
显示软件版本。
- **修订计数器 (Revision Counter)**
无论何种版本，此框始终显示值“0”。
- **修订日期 (Revision Date)**
显示上次修订的日期和时间。
- **功能标签 (Function Tag)**
显示设备的功能标签（工厂标识）。工厂标识 (HID) 是通过 STEP 7 的 HW Config 在设备组态过程中创建的。
- **位置标签 (Location tag)**
显示设备的位置标签。位置标识符 (LID) 是通过 STEP 7 的 HW Config 在设备组态过程中创建的。
- **“日期”(Date)**
显示通过 STEP 7 的 HW Config 组态设备时创建的日期。
- **说明 (Description)**
显示通过 STEP 7 的 HW Config 组态设备时创建的说明。

5.3.4 ARP 表

MAC 地址和 IPv4 地址的分配

使用地址解析协议 (Address Resolution Protocol, ARP) 时，MAC 地址到 IPv4 地址的分配具有唯一性。该分配情况由各网络节点记录在自己的 ARP 表中。此 WBM 页面显示设备的这个 ARP 表。



Interface	MAC Address	IP Address	Media Type
vlan1	68-05-ca-19-40-bb	192.168.16.1	Dynamic

1 entry.

Refresh

显示值说明

该表格包括以下列：

- **“接口”(Interface)**
显示获取行条目所用的接口。
- **MAC Address**
显示目标设备或源设备的 MAC 地址。
- **IP 地址 (IP Address)**
显示目标设备的 IPv4 地址。
- **“介质类型”(Media Type)**
显示连接的类型。
 - “动态”(Dynamic)
设备自动识别到地址数据。
 - “静态”(Static)
地址作为静态地址输入。

5.3.5 日志表

记录事件

设备允许用户记录正在发生的事件，有些事件可以在“系统 > 事件”(System > Events) 菜单的页面上指定。这样（举例来说）便可记录身份验证尝试失败的时间或某端口连接状态发生变化的时间。

即使在设备关闭后，事件日志表的内容仍可保留。

Log Table

Severity Filters

Info

Warning

Critical

Restart	System Up Time	System Time	Severity	Log Message
41	08:25:24	Date/time not set	6 - Info	Spanning Tree: topology change detected.
41	08:24:48	Date/time not set	6 - Info	Link up on P0.15.
41	08:24:18	Date/time not set	6 - Info	Link down on P0.15.
41	07:29:01	Date/time not set	6 - Info	IP communication is possible. Remote logging activated.

1 - 10 of 517 entries [Show all](#) 1 [Next](#)

显示值说明

Severity Filters

可以根据严重程度过滤表中的条目。选中表格上方所需的复选框。

- **Info**

如果启用该参数，则会显示“Info”类别的所有条目。

- **Warning**

如果启用该参数，则会显示“Warning”类别的所有条目。

- **Critical**

如果启用该参数，则会显示“Critical”类别的所有条目。

要显示所有条目，可选中所有复选框，或将它们留空。

该表格包括以下列：

- **重启 (Restart)**
统计自上次复位为出厂设置以来的重启次数，并显示与发生的事件对应的设备重启。
- **“系统运行时间”(System Up Time)**
显示在所描述的事件发生时设备自上次重启以来已持续运行的时间。
- **系统时间 (System Time)**
如果已设定系统时间，则还会显示事件发生的日期和时间。
- **“严重程度”(Severity)**
将条目分为以上类别。
- **“日志消息”(Log Message)**
显示已发生事件的简要说明。

按钮和输入框说明

“Clear”按钮

单击此按钮可删除事件日志文件的内容。无论在“Severity Filters”中作出了何种选择，均会删除所有条目。

还会清空显示画面。仅当将设备恢复为出厂设置并重启设备后，才会复位重启计数器。

说明

该表中的条目数量限制为 1200 条。该表中每个严重程度可包含 400 个条目。达到这一数字后，会丢弃相关严重程度的最早的条目。该表会永久保存在内存中。

“全部显示”(Show all) 按钮

单击该按钮可在 WBM 页面上显示所有条目。请注意，显示所有消息可能会花费一些时间。

“Next”按钮

单击该按钮可转至下一页。

“Prev”按钮

单击该按钮可转至上一页。

用于更改页面的下拉列表

从该下拉列表中选择要转至的页面。

“Update”按钮

刷新表中各值的显示画面。

5.3.6 故障

错误状态

如果出现错误，则会显示在此页面。在设备上，通过红色故障 LED 点亮来指示错误。

将指示设备的内部错误以及在下列页面上组态的错误：

- 系统 > 事件 (System > Events)
- 系统 > 故障监视 (System > Fault Monitoring)

确认后，将删除“冷/暖启动”(Cold/Warm Start) 事件的错误。

始终从上次系统启动后开始计算错误时间。

如果没有错误，则故障 LED 将熄灭。

The screenshot displays the 'Faults' section of the management interface. At the top, it shows 'No. of Signaled Faults: 1' with a 'Reset Counters' button below it. A table lists two fault events:

Fault Time	Fault Description	Clear Fault State
16s	Link down on P0.1.	Clear Fault State
17s	Warm start performed.	Clear Fault State

At the bottom of the table area, there is a 'Refresh' button.

显示值说明

- **No. of Signaled Faults**

自上次启动后显示的错误数。

- **复位计数器 (Reset Counters)**

单击“复位计数器”(Reset counter) 可复位所有计数器。重启后，计数器将复位。

该表包含以下列：

- **故障时间 (Fault Time)**
显示自系统上一次因发生所描述的错误/故障而导致重启以来已持续运行的时间。
- **故障说明 (Fault Description)**
显示已发生故障/错误的简要说明。
- 如果启用了“Clear Fault State”按钮，则可删除故障。

5.3.7 冗余

5.3.7.1 生成树

简介

该页面显示有关生成树和根网桥设置的最新信息。

Spanning Tree

Spanning Tree	Ring Redundancy	Standby																								
Spanning Tree Mode: MSTP Instance ID: 0 Bridge Priority: 32768 Bridge Address: 08-00-06-70-56-00 Root Priority: 32768 Root Address: 00-1b-1b-cd-3b-00 Root Cost: 220000 Regional Root Priority: 32768 Regional Root Address: 08-00-06-70-56-00 Regional Root Cost: 0																										
<table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th>Port</th> <th>Role</th> <th>State</th> <th>Oper. Version</th> <th>Priority</th> <th>Path Cost</th> <th>Edge Type</th> <th>Pt.P. Type</th> </tr> </thead> <tbody> <tr> <td>P0.1</td> <td>Root</td> <td>Forwarding</td> <td>MSTP</td> <td>128</td> <td>200000</td> <td>No Edge Port</td> <td>Pt.P</td> </tr> <tr> <td>P0.15</td> <td>Designated</td> <td>Forwarding</td> <td>MSTP</td> <td>128</td> <td>200000</td> <td>Edge Port</td> <td>Pt.P</td> </tr> </tbody> </table>			Port	Role	State	Oper. Version	Priority	Path Cost	Edge Type	Pt.P. Type	P0.1	Root	Forwarding	MSTP	128	200000	No Edge Port	Pt.P	P0.15	Designated	Forwarding	MSTP	128	200000	Edge Port	Pt.P
Port	Role	State	Oper. Version	Priority	Path Cost	Edge Type	Pt.P. Type																			
P0.1	Root	Forwarding	MSTP	128	200000	No Edge Port	Pt.P																			
P0.15	Designated	Forwarding	MSTP	128	200000	Edge Port	Pt.P																			
<input type="button" value="Refresh"/>																										

显示值说明

该页面显示以下字段：

- **“生成树模式”(Spanning Tree Mode)**
显示设置的模式。在“第 2 层 > 组态”(Layer 2 > Configuration) 和“第 2 层 > 生成树 >

5.3 “Information”菜单

常规”(Layer 2 > Spanning Tree > General) 中指定模式。

可以使用以下值：

- ' '
- STP
- RSTP
- MSTP

- **实例 ID (Instance ID)**

显示实例编号。该参数取决于组态的模式。

- **Bridge Priority / Root Priority**

哪个设备成为根网桥由网桥优先级决定。优先级最高的网桥（换句话说，此参数的值最小）将成为根网桥。如果网络中有多个设备具有相同优先级，则 MAC 地址数值最小的设备将成为根网桥。网桥优先级和 MAC 地址这两个参数一起构成网桥标识符。由于根网桥管理所有路径的变更，出于帧延迟的考虑，根网桥应该尽可能处在中心位置。网桥优先级的值是 4096 的整数倍数，值范围从 0 到 32768。

- **网桥地址/根地址 (Bridge address/root address)**

网桥地址显示设备的 MAC 地址，根地址显示根交换机的 MAC 地址。

- **根开销 (Root Cost)**

显示从设备到根网桥的路径开销。

- **“网桥状态”(Bridge Status)**

显示网桥的状态，例如，设备是否为根网桥。

- **区域根优先级 (Regional root priority)**（仅适用于 MSTP）

有关描述，请参见“网桥优先级”(Bridge Priority)/“根优先级”(Root Priority)。

- **区域根地址 (Regional root address)**（仅适用于 MSTP）

显示设备的 MAC 地址。

- **区域根开销 (Regional Root Cost)**（仅适用于 MSTP）

显示从区域根网桥到根网桥的路径开销。

该表格包括以下列：

- **Port**
显示设备通信所用的端口。端口由模块号和端口号组成，例如，端口 0.1 表示模块 0，端口 1。
- **Role**
显示端口状态。可能的值包括：
 - **Disabled**
已从生成树中手动移除端口，生成树将不再考虑该端口。
 - **Designated**
端口从根网桥中转移数据。
 - **备用 (Alternate)**
端口具有指向网段的备用路径
 - **Backup**
如果交换机具有多个指向同一网段的端口，则“较差”端口将变为备用端口。
 - **Root**
端口提供指向根网桥的最佳路径。
 - **Master**
此端口指向 MST 区域外部的根网桥。
- **状态 (Status)**
显示端口的当前状态。仅显示这些值。具体参数取决于组态的协议。可能的值包括：
 - **Discarding**
端口接收 BPDU 帧。其它进入或离开的帧会被丢弃。
 - **Listening**
端口接收和发送 BPDU 帧。端口包括在生成树算法中。其它进入或离开的帧会被丢弃。
 - **Learning**
端口主动学习拓扑，即学习节点地址。其它进入或离开的帧会被丢弃。
 - **Forwarding**
经过重新组态时间后，端口在网络中激活。该端口接收和发送数据帧。
- **运行版本 (Oper. Version)**
显示端口所使用生成树的兼容模式。

- **优先级 (Priority)**

如果由生成树计算出的路径可能经过设备的多个端口，则选择优先级最高的端口（也就是此参数值最小的端口）。可输入的优先级数值介于 0 和 240 之间，步长为 16。如果输入的值不能被 16 整除，则会自动调整该值。默认值为 128。

- **路径开销 (Path Cost)**

此参数用于计算将要选择的路径。选择具有最小值的路径。如果设备的多个端口具有相同的值，则选择端口号最小的端口。

如果“开销计算”(Cost Calc.)

框中的值为“0”，则显示自动计算出的值。否则会显示“开销计算”(Cost Calc.) 框的值。

主要根据传输速度来计算路径开销。可达到的传输速度越高，路径成本的值就越低。

快速生成树的典型路径成本值如下：

- 10,000 Mbps = 2,000
- 1000 Mbps = 20,000
- 100 Mbps = 200,000
- 10 Mbps = 2,000,000

组态“成本计算”(Cost Calc.)，具体可在“第 2 层 > 生成树 > CIST 端口”(Layer 2 > Spanning Tree > CIST Port) 和“第 2 层 > 生成树 > MST 端口”(Layer 2 > Spanning Tree > MST Port) 页面上组态。

- **Edge Type**

显示连接类型。可能的值包括：

- Edge Port
此端口上有终端设备。
- 无边缘端口 (No Edge Port)
此端口上有生成树设备。

- **P.t.P 类型 (P.t.P Type)**

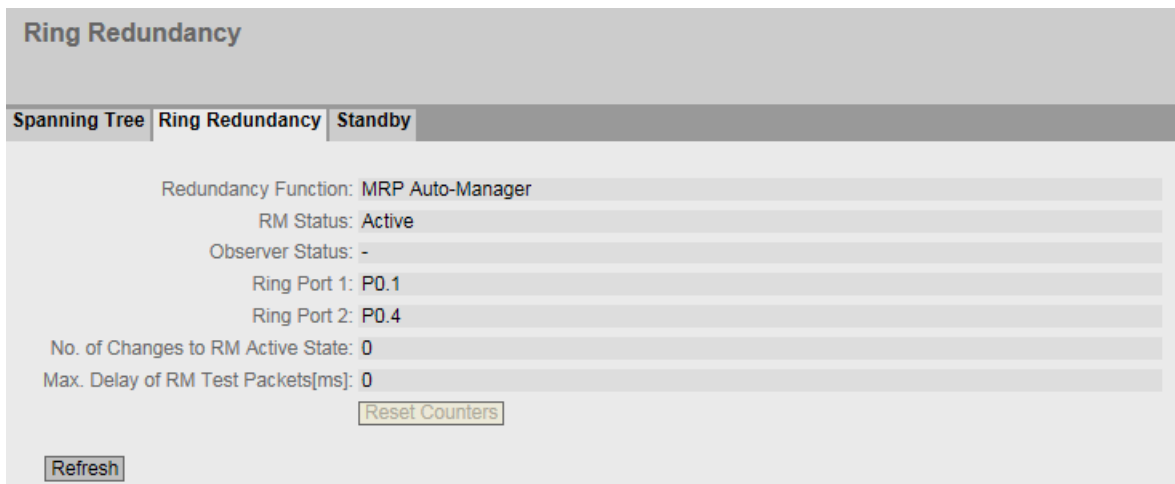
显示点对点链路类型。可能的值包括：

- P.t.P.
对于半双工，认为是点对点链路。
- “共享介质”(Shared Media)
对于全双工连接，不认为是点对点链路。

5.3.7.2 环网冗余

有关环网冗余的信息

在该选项卡中，您将获得有关环网冗余的设备状态信息。此页面中的文本框均为只读模式。



显示值说明

显示以下对话框：

- **冗余功能 (Redundancy Function)**

“冗余功能”(Redundancy Function) 列显示设备在环网内的角色：

- 无环网冗余 (no Ring Redundancy)
工业以太网交换机正在无冗余功能的情况下运行。
- HRP 客户端 (HRP Client)
工业以太网交换机充当 HRP 客户端。
- HRP 管理器 (HRP Manager)
工业以太网交换机充当 HRP 管理器。
- MRP 客户端 (MRP Client)
工业以太网交换机充当 MRP 客户端。
- MRP 管理器 (MRP Manager)
工业以太网交换机充当 MRP 管理器。使用 STEP 7 时，为设备设置“管理器”角色。

5.3 “Information”菜单

- MRP 自动管理器 (MRP Auto-Manager)

工业以太网交换机充当 MRP 管理器。使用 WBM 或 CLI 时，设置“MRP 自动管理器”(MRP Auto-Manager) 角色，在使用 STEP 7 时，设置“管理器（自动）”角色。

- **RM 状态 (RM Status)**

“RM 状态”(RM Status)

列显示工业以太网交换机是否充当冗余管理器，以及此角色是断开环网还是闭合环网。

- 被动 (Passive)

工业以太网交换机充当冗余管理器，并已打开环网；即：与环网端口相连的交换机线路处于无故障运行状态。在工业以太网交换机并未充当冗余管理器时（冗余管理器禁用），也将显示“被动”(Passive) 状态。

- 主动 (Active)

工业以太网交换机充当冗余管理器，并已关闭环网；即：与环网端口相连的交换机线路已中断（故障）。冗余管理器将接通其环网端口并恢复未中断的线性拓扑。

- “-”

禁用冗余功能。

- **观察器状态 (Observer Status)**

显示观察器的当前状态。

- **环网端口 1/环网端口 2 (Ring Port 1/Ring Port 2)**

“环网端口 1”(Ring Port 1) 和“环网端口 2”(Ring Port 2)

两列显示当前用作环网端口的端口。如果完全禁用环型拓扑中的介质冗余，则会显示最后组态的环网端口。

- **变为 RM 激活状态的次数 (No. of Changes to RM Active State)**

显示充当冗余管理器的设备切换至激活状态（即闭合环网）的频率。

如果冗余功能已禁用或设备为“HRP/MRP 客户端”(HRP/MRP client)，则将显示文本“冗余管理器已禁用”(Redundancy manager disabled)。

- **RM 测试帧的最大延迟 [ms] (Max. Delay of the RM Test Packets [ms])**

显示冗余管理器测试帧的最大延迟时间。

如果冗余功能已禁用或设备为“HRP/MRP 客户端”(HRP/MRP client)，则将显示文本“冗余管理器已禁用”(Redundancy manager disabled)。

按钮描述

复位计数器 (Reset Counters)按钮

单击“复位计数器”(Reset Counters) 可复位所有计数器。将通过重启复位计数器。

5.3.7.3 备用

有关备用冗余的信息

在该选项卡中，您将获得有关备用冗余的设备状态信息。此页面中的文本框均为只读模式。

说明

MAC 地址较高的设备成为主设备

以冗余方式连接 HRP 环网时，总是将两个设备组态为主/从设备对。这同样适用于中断的 HRP 环网（线性总线）。在工作正常情况下，MAC 地址较高的设备将承担主设备的角色。

这种类型的分配很重要，尤其是在更换设备时。根据 MAC 地址，前一台具有从站功能的设备可接管备用主站角色。

“备用”(Standby) 选项卡显示备用功能的状态：

The screenshot shows a web management interface for the Standby configuration. At the top, there is a header "Standby". Below it, there are three tabs: "Spanning Tree", "Ring Redundancy", and "Standby", with "Standby" being the active tab. The main content area displays the following information:

- Standby Ports: (empty field)
- Standby Name: no-name
- Standby Function: Disabled
- Standby Status: -
- No. of Changes to Standby Active State: Standby Disabled

At the bottom of the main content area, there is a "Reset Counters" button. At the very bottom of the page, there is a "Refresh" button.

显示值说明

显示以下对话框：

- **备用端口 (Standby Ports)**

显示备用端口。

- **备用名称 (Standby Name)**

备用连接名称

- **备用功能 (Standby Function)**

- **Master**

该设备与伙伴设备相连并充当主设备。正常运行时，此设备的备用端口处于激活状态。

- **Slave**

该设备与伙伴设备相连并充当从设备。正常运行时，此设备的备用端口处于未激活状态。

- **禁用 (Disabled)**

备用链接已禁用。该设备既不充当主设备也不充当从设备。组态为备用端口的端口将用作不具有备用功能的常规端口。

- **等待连接 (Waiting for Connection)**

尚未与伙伴设备建立连接。备用端口处于未激活状态。在这种情况下，或是伙伴设备中的组态不一致（例如，连接名错误、备用链路被禁用），或是存在实际故障（例如，设备故障、链路中断）。

- **连接丢失 (Connection lost)**

与伙伴设备的现有连接已丢失。在这种情况下，或者是伙伴设备中的组态已被修改（例如，不同的连接名称、备用链路已禁用），或者是存在实际故障（例如，设备故障、链路中断）。

- **备用状态 (Standby Status)**

“备用状态”(Standby Status) 显示框中显示备用端口的状态:

- **激活 (Active)**

该设备的备用端口处于激活状态; 即, 备用端口已启用, 可以进行帧通信。

- **未激活 (Passive)**

该设备的备用端口处于未激活状态; 即, 备用端口已封锁, 无法进行帧通信。

- **“-”:**

备用功能已禁用。

- **变为备用激活状态的次数 (No. of Changes to Standby Activate State)**

显示工业以太网交换机的备用状态从“未激活”(Passive) 变为“激活”(Active)

的频率。如果备用主站上的备用端口连接失败, 工业以太网交换机变为“激活”(Active) 状态。

如果备用功能已禁用, 该框中显示文本“备用已禁止”(Standby Disabled)。

按钮描述

复位计数器 (Reset Counters) 按钮

单击“复位计数器”(Reset Counters) 可复位所有计数器。重启后, 计数器将复位。

5.3.8 以太网统计信息

5.3.8.1 Interface Statistics

接口统计信息

此页面显示管理信息库 (MIB) 的接口表中的统计信息。

	In Octet	Out Octet	In Unicast	In Non-Unicast	Out Unicast	Out Non-Unicast	In Errors
P0.1	1278372	1117817	3218	974	1732	109	0
P0.2	0	0	0	0	0	0	0
P0.3	0	0	0	0	0	0	0
P0.4	0	0	0	0	0	0	0

显示值说明

该表格包括以下列：

- **输入八位位组 (In Octet)**
显示接收到的字节数。
- **输出八位位组 (Out Octet)**
显示发送的字节数。
- **输入单播 (In Unicast)**
显示已接收的单播帧数。
- **In Non Unicast**
显示接收到的非单播类型帧的数目。
- **输出单播 (Out Unicast)**
显示已发送的单播帧数。

- **Out Non Unicast**

显示发送的非单播类型帧的数目。

- **In Errors**

显示所有可能的 RX 错误数，请参见“Packet Error”选项卡。

按钮描述

复位计数器 (Reset Counters) 按钮

单击“复位计数器”(Reset Counters) 可复位所有计数器。重启后计数器复位。

5.3.8.2 Packet Size

按长度分类的帧

该页面会显示每个端口发送并接收了多少个包含长度的帧。无法对该页面上的任何内容进行组态。

显示的值由 RMON 传送。

在“Layer 2 > RMON > Statistics”页面中，可以设置要显示哪个端口的值。

Ethernet Statistics: Packet Size						
Interface Statistics	Packet Size	Packet Type	Packet Error	History		
Port	64	65-127	128-255	256-511	512-1023	1024-max
P0.1	0	0	0	0	0	0
P0.2	0	0	0	0	0	0
P0.3	0	0	0	0	0	0
P0.4	0	0	0	0	0	0

Reset Counter

Refresh

显示值说明

该表格包括以下列：

- **端口 (Port)**

显示可用端口和链路汇聚。端口由模块号和端口号组成，例如，端口 0.1 表示模块 0，端口 1。

说明

帧统计信息显示

在与帧长度相关的统计信息中，需要注意的是，会同时对到达帧和离开帧进行计数。

- **帧长度 (Frame lengths)**

端口号后面的其它各列包含按照帧长度分类的帧的绝对数量。

帧长度分为以下几类：

- 64 字节
 - 65 - 127 字节
 - 128 - 255 字节
 - 256 - 511 字节
 - 512 - 1023 字节
 - 1024 - 最大值
-

说明

封锁端口上的数据通信

由于技术原因，可根据需要显示封锁端口上的数据包信息。

按钮描述

“Reset Counters”按钮

单击“Reset Counters”可复位所有计数器。将通过重启复位计数器。

5.3.8.3 Packet Type

按帧类型分类的已接收帧

此页面显示各个端口接收到的类型为“单播”、“组播”和“广播”的帧的数目。无法对该页面上的任何内容进行组态。

显示的值由 RMON 传送。

在“Layer 2 > RMON > Statistics”页面中，可以设置要显示哪个端口的值。

Ethernet Statistics: Packet Type			
Interface Statistics Packet Size Packet Type Packet Error History			
Port	Unicast	Multicast	Broadcast
P0.1	0	0	0
P0.2	0	0	0
P0.3	0	0	0
P0.4	0	0	0

Reset Counter

Refresh

显示值说明

该表格包括以下列：

- 端口 (Port)**
 显示可用端口和链路汇聚。端口由模块号和端口号组成，例如，端口 0.1 表示模块 0，端口 1。
- Unicast/Multicast/Broadcast (单播/组播/广播)**
 端口号之后的其它各列包括按照其帧类型“Unicast”(单播)、“Multicast”(组播)和“Broadcast”(广播) 分类的到达帧的绝对数量。

按钮描述

“Reset Counters”按钮

单击“Reset Counters”可复位所有计数器。将通过重启复位计数器。

5.3.8.4 Packet Error

接收到的坏帧

该页面显示每个端口接收到多少坏帧。无法对该页面上的任何内容进行组态。

显示的值由 RMON 传送。

在“Layer 2 > RMON > Statistics”页面中，可以设置要显示哪个端口的值。

Ethernet Statistics: Packet Error						
Interface Statistics	Packet Size	Packet Type	Packet Error	History		
Port	CRC	Undersize	Oversize	Fragments	Jabbers	Collisions
P0.1	0	0	0	0	0	0
P0.2	0	0	0	0	0	0
P0.3	0	0	0	0	0	0
P0.4	0	0	0	0	0	0

Reset Counter

Refresh

显示值说明

该表格包括以下列：

- **端口 (Port)**
显示可用端口和链路汇聚。端口由模块号和端口号组成，例如，端口 0.1 表示模块 0，端口 1。
- **错误类型 (Error types)**
端口号之后的其它各列包括按照其错误类型分类的到达帧的绝对数量。

在该表的各列中，将根据以下错误类型进行区分：

- **CRC**
内容与 CRC 校验和不符合的数据包。
- **Undersize**
长度小于 64 字节的数据包。
- **Oversize**
由于长度过长而被丢弃的数据包。

- Fragments
长度小于 64 字节并且 CRC 校验和错误的数据包。
- Jabber
包含错误 CRC 校验和且由于长度过长而被丢弃的带 VLAN 标记的数据包。
- Collisions
检测到的冲突。

按钮描述

“Reset Counters”按钮

单击“Reset Counters”可复位所有计数器。将通过重启复位计数器。

5.3.8.5 历史

统计信息的样本

此页面显示每个端口的 RMON 统计信息的样本。

在“第 2 层 > RMON > 历史”(Layer 2 > RMON > History) 页面中，可以设置要对其进行采样的端口。

Ethernet History												
Interface Statistics	Packet Size	Packet Type	Packet Error	History								
Port: P0.1 <input type="text"/>												
Buckets: 24												
Interval[s]: 3600												
Sample	Sample Time	Unicast	Multicast	Broadcast	CRC	Undersize	Oversize	Fragments	Jabbers	Collisions	Utilization[%]	
67	2d 18h 14m 13s	0	0	0	0	0	0	0	0	0	0	
68	2d 19h 14m 25s	0	0	0	0	0	0	0	0	0	0	
69	2d 20h 14m 37s	0	0	0	0	0	0	0	0	0	0	
70	2d 21h 14m 49s	0	0	0	0	0	0	0	0	0	0	
71	2d 22h 15m 1s	0	0	0	0	0	0	0	0	0	0	
Refresh												

图 5-1 历史

设置

- **端口**
选择要为其显示历史记录端口。

显示值说明

- **Entries**
可同时保存的最大样本数目。
- **Interval [s]**
将统计信息的当前状态保存为样本的间隔。

该表格包括以下列：

- **样本 (Sample)**
样本的编号
- **采样时间 (Sample Time)**
获取样本时的系统运行时间。
- **单播**
已接收的单播帧数。
- **组播**
已接收的组播帧数。
- **广播 (Broadcast)**
已接收的广播帧数。
- **CRC**
CRC 校验和错误的帧的数目。
- **Undersize**
长度小于 64 字节的帧的数目。
- **Oversize**
由于长度过长而被丢弃的帧的数目。
- **Fragments**
长度小于 64 字节并且 CRC 校验和错误的帧的数目。

- **Jabbers**
带有 CRC 校验和错误的 VLAN 标记，并由于长度过长而被丢弃的帧的数目。
- **Collisions**
接收到的帧的冲突数目。
- **Utilization [%]**
端口在获取样本期间的利用率。

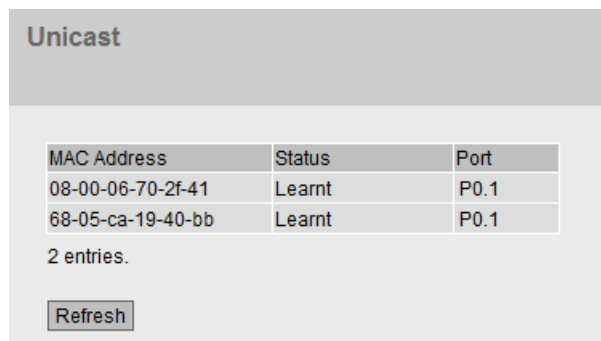
5.3.9 单播

单播过滤表的状态

此页面显示单播过滤表的当前内容。该表列出了单播地址帧的源地址。条目可以在节点向端口发送帧时动态生成，也可以通过用户设置参数静态生成。

“基础网桥模式”(Base bridge mode) 的相关性

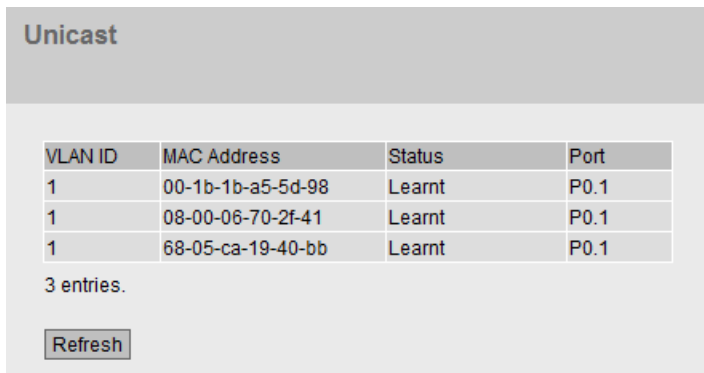
显示的列取决于所设置的“基础网桥模式”(Base bridge mode)。如果更改“基础网桥模式”(Base bridge mode)，现有条目将丢失。



MAC Address	Status	Port
08-00-06-70-2f-41	Learnt	P0.1
68-05-ca-19-40-bb	Learnt	P0.1

2 entries.

图 5-2 基础网桥模式：802.1D 透明网桥



VLAN ID	MAC Address	Status	Port
1	00-1b-1b-a5-5d-98	Learnt	P0.1
1	08-00-06-70-2f-41	Learnt	P0.1
1	68-05-ca-19-40-bb	Learnt	P0.1

3 entries.

图 5-3 基础网桥模式：802.1Q VLAN 网桥

说明

该表包含以下列：

- **VLAN ID**

显示分配给此 MAC 地址的 VLAN ID。

- **MAC 地址 (MAC Address)**

显示设备已学习或用户已组态的节点 MAC 地址。

- **状态 (Status)**

显示每个地址条目的状态：

- **Learnt**

通过从节点接收帧，学习相应的地址；如果从此节点再没接收到数据包，则在老化时间结束时删除该地址。

说明

如有链路中断，则已学习的 MAC 条目将被删除。

- **Static**

由用户组态。静态地址会永久存储；也就是说，当老化时间结束或交换机重启时，静态地址不会被删除。

- **端口 (Port)**

显示访问指定地址的节点时所使用的端口。设备接收到的目标地址与此地址相匹配的帧将被转发到此端口。

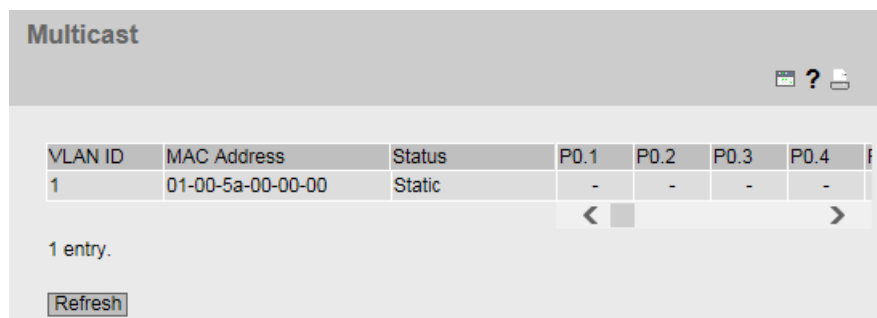
5.3.10 组播

组播过滤表的状态

该表显示的是组播过滤表中当前输入的组播帧及其目标端口。这些条目可以是动态的（设备已学习），也可以是静态的（由用户设置）。

“基础网桥模式”(Base bridge mode) 的相关性

如果更改“基础网桥模式”(Base bridge mode)，现有条目将丢失。



VLAN ID	MAC Address	Status	P0.1	P0.2	P0.3	P0.4
1	01-00-5a-00-00-00	Static	-	-	-	-

1 entry.

说明

该表包含以下列：

- **VLAN ID**
显示要向其分配 MAC 组播地址的 VLAN 的 VLAN ID。
- **MAC 地址 (MAC Address)**
显示设备已学习或用户已组态的 MAC 组播地址。
- **状态 (Status)**
显示每个地址条目的状态。可能的信息如下：
 - **静态 (Static)**
此地址是由用户以静态方式输入的。静态地址会永久存储；也就是说，当老化时间结束或设备重启时，静态地址不会被删除。这些地址可由用户删除。
 - **IGMP**
此地址的目标端口通过 IGMP 获得。
 - **GMRP**
此地址的目标端口由收到的 GMRP 帧注册。

5.3 “Information”菜单

- **端口列表 (Port List)**

每个插槽都有一列对应。在每一列内，端口所属的组播组显示如下：

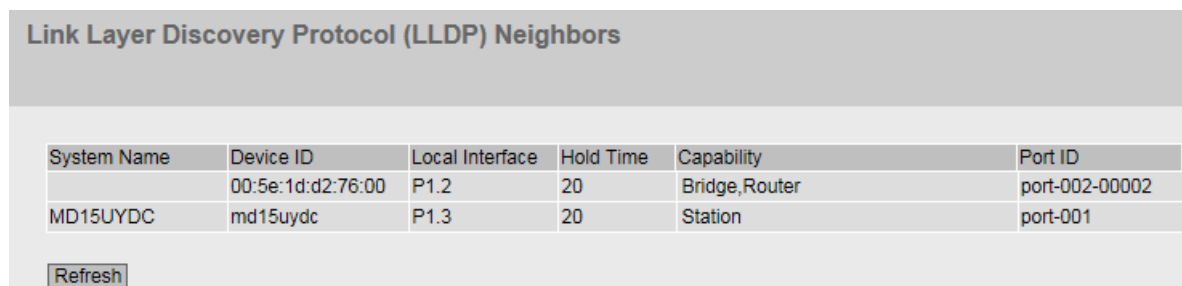
- M
(成员) 通过此端口发送组播帧。
- R
(已注册) 组播组的成员，由 GMRP 帧注册。
- I
(IGMP) 组播组的成员，由 IGMP 帧注册。
- -
不是组播组的成员。不通过此端口发送包含所定义组播 MAC 地址的组播帧。
- F
(已禁止) 不是组播组的成员。此外，在此端口上不能使用 IGMP 动态学习。

5.3.11 LLDP

邻居表状态

此页面显示邻居表的当前内容。该表存储 LLDP 代理从所连接设备接收到的信息。

在以下部分设置 LLDP 代理接收或发送信息所使用的接口：“第 2 层 > LLDP”(Layer 2 > LLDP)。



System Name	Device ID	Local Interface	Hold Time	Capability	Port ID
	00:5e:1d:d2:76:00	P1.2	20	Bridge,Router	port-002-00002
MD15UYDC	md15uydc	P1.3	20	Station	port-001

Refresh

图 5-4 信息 LLDP

显示值说明

该表包含以下各列：

- **System Name**

所连接设备的系统名称。

- **Device ID**

所连设备的设备 ID。设备 ID 与通过 PST (STEP 7) 分配的设备名称相对应。如果未分配设备名称，则显示设备的 MAC 地址。

- **Local Interface**

工业以太网交换机接收信息的端口。

- **Hold Time**

此处指定的时间是条目持续存储在设备中的时间。在这段时间内，如果工业以太网交换机未从所连设备接收到任何新信息，则将删除该条目。

- **Capability**

显示所连设备的属性：

- 路由器
- 网桥
- 电话
- DOCSIS 电缆设备
- WLAN 接入点
- 中继器
- 站
- 其它

- **Port ID**

连接工业以太网交换机的设备端口。

5.3.12 光纤监视协议

监视光链接

通过光纤监视可以监视光链接。该表显示了端口的当前状态。

可以在以下页面设置要监视的值：“第 2 层 > FMP”(Layer 2 > FMP)。

Fiber Monitoring Protocol (FMP) Diagnosis				
Port	Rx Power State	Rx Power[dBm]	Power Loss State	Power Loss[dB]
P0.1	link down	-	idle	-
P0.2	ok	-21.1	ok	-5.9
P0.4	link down	-	idle	-

显示值说明

端口 (Port)

显示支持光纤监视的光纤端口。它与收发器有关。

接收功率状态 (Rx Power State)

- **disabled**

已禁用光纤监视。

- **ok**

光纤链路的接收功率值在设定的限值范围内。

- **maint. req.**

检查链接。

发出了报警信号。

- **maint. dem.**

需要检查链接。

已发出报警信号，故障 LED 亮起。

- **link down**

与通信伙伴的连接已中断。未检测到连接。

接收功率 [dBm] (Rx Power [dBm])

显示接收功率的当前值。该值可以有 ± 3 dB 的容差。

如果不存在连接（连接中断）或光纤监视功能已禁用，则会显示“-”。如果伙伴端口上的光纤监视功能未启用，则会显示值 0.0。

功率损耗状态 (Power loss State)

为了监视连接的功率损耗，连接伙伴的光纤端口的光纤监视功能必须启用。

- **disabled**

已禁用光纤监视。

- **ok**

光纤链路的功率损耗值在定义的范围內。

- **maint. req.**

检查链接。

发出了报警信号。

- **maint. dem.**

需要检查链接。

已发出报警信号，故障 LED 亮起。

- **idle**

端口未与另一个启用了光纤监视功能的端口相连。

如果持续 5

个周期均未从连接伙伴的光纤端口处接收到诊断信息，则认为光纤监视连接已中断。

一个周期持续 5 秒。

功率损耗 [dB] (Power Loss [dB])

显示功率损耗的当前值。该值可以有 ± 3 dB 的容差。

如果不存在连接（连接中断）、光纤监视功能已禁用或者伙伴端口不支持光纤监视功能，则会显示“-”。

5.3.13 DHCP 服务器 (DHCP Server)

此页面显示通过 DHCP 服务器分配给设备的 IPv4 地址。

DHCP Server Bindings									
IP Address	Pool ID	Identification Method	Identification Value	Remote ID	Circuit ID	Allocation Method	Binding State	Expire Time	
192.168.16.90	1	Client ID	OS-EC74BA03FED2			dynamic	assigned	01/01/2000 05:21:03	
1 entry.									
<input type="button" value="Refresh"/>									

说明

- IP 地址 (IP Address)**
 显示分配给 DHCP 客户端的 IPv4 地址。
- 池 ID (Pool ID)**
 显示 IPv4 地址段编号。
- 标识方法 (Identification method)**
 显示标识 DHCP 客户端的方法。
- 标识值 (Identification value)**
 显示 DHCP 客户端的 MAC 地址和客户端 ID。
- 远程 ID (Remote ID)**
 显示 DHCP 客户端的远程 ID。
- 电路 ID (Circuit ID)**
 显示 DHCP 客户端的电路 ID。
- 分配方法 (Allocation Method)**
 显示 IPv4 地址是以静态方式分配还是以动态方式分配。可在“系统 > DHCP > 静态租用”(System > DHCP > Static Leases) 中组态静态条目。

- **绑定状态 (Binding State)**

显示分配的状态。

- **已分配 (Assigned)**

已使用分配。

- **未使用 (Not used)**

未使用分配。

- **检查 (Probing)**

正在检查分配。

- **未知 (Unknown)**

分配状态未知。

- **超期时间 (Expire Time)**

显示所分配的 IPv4 地址保持有效的时长。超过该时间后，DHCP 客户端必须请求新的 IPv4 地址，或延长现有 IPv4 地址的租用时间。

按钮和输入框说明

“全部显示”(Show all) 按钮

单击该按钮可在 WBM

页面上显示所有条目。请注意，显示所有消息可能会花费一些时间。

“下一页”(Next) 按钮

单击该按钮可转至下一页。

“上一页”(Prev)按钮

单击该按钮可转至上一页。

用于更改页面的下拉列表

从该下拉列表中选择要转至的页面。

“刷新”(Refresh) 按钮

刷新表中各值的显示画面。

5.3.14 诊断 (Diagnostics)

此页用于显示设备内部和外部模块的温度值。只有当模块提供温度信息时，才会进行显示。如果添加或删除某个模块，显示画面将自动调整。

如果温度值降至所显示阈值以下或超出所显示阈值，则状态将相应地发生变化。

在“系统 > 事件 > 组态”(System > Events > Configuration) 中，可指定设备指示状态变化的方式。

Diagnostics						
Temperature Table						
Name	Status	Temperature [°C]	Low Critical Threshold [°C]	Low Warning Threshold [°C]	High Warning Threshold [°C]	High Critical Threshold [°C]
Enclosure	OK	33	-80	-60	105	120

Aktualisieren

说明

- **名称 (Name)**

显示模块名称。

“Enclosure”或“Chassis”行中的信息指的是外壳的内部温度。

- **状态 (Status)**

基于阈值与当前温度之间的关系，以优先级升序显示以下状态值。

- OK

温度值处于预设的阈值范围内。

- WARNING

已超出“Warning”严重级别对应的上限或下限阈值。

- CRITICAL

已超出“Critical”严重级别对应的上限或下限阈值。

- INVALID

值无法读取或无效。在“温度 [°C]”(Temperature [°C]) 框中，将显示“-”。

- INITIAL

尚未读取任何数据。所有框中都显示“-”。

- **温度 [°C] (Temperature [°C])**
显示温度的当前值。显示画面会定期更新。
该值可以有 +/- 3 °C 的容差。
- **下限阈值 [°C] (严重) (Lower Threshold [°C] (Critical))**
如果值降至该值以下，则状态将切换为“CRITICAL”。您可组态为发生此事件时通过消息进行通知。
- **下限阈值 [°C] (警告) (Lower Threshold [°C] (Warning))**
如果值降至该值以下，则状态将切换为“WARNING”。您可组态为发生此事件时通过消息进行通知。
- **上限阈值 [°C] (警告) (Upper Threshold [°C] (Warning))**
如果值超出该值，则状态将切换为“WARNING”。您可组态为发生此事件时通过消息进行通知。
- **上限阈值 [°C] (严重) (Upper Threshold [°C] (Critical))**
如果值超出该值，则状态将切换为“CRITICAL”。您可组态为发生此事件时通过消息进行通知。

5.3.15 SNMP

该页面显示所创建的 SNMPv3 组。在“系统 > SNMP”(System > SNMP) 中组态 SNMPv3 组。

Simple Network Management Protocol v3 (SNMPv3) Groups Overview	
Group Name	User Name
service	Miller
maintenance	Peterson

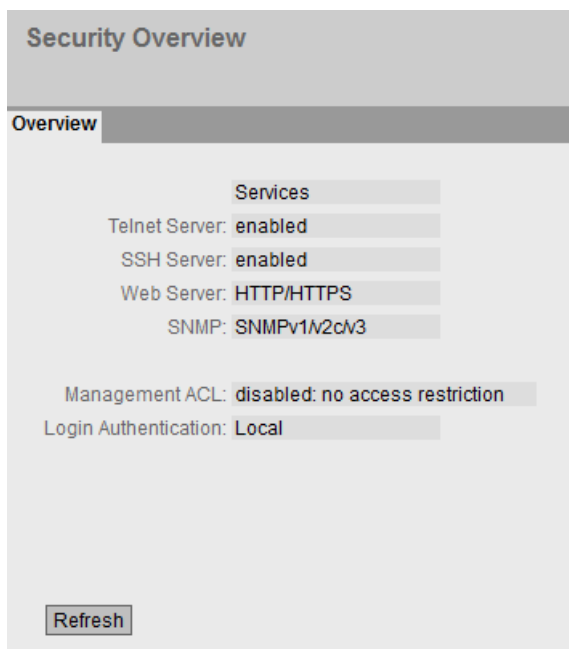
说明

该表格包括以下列：

- **组名称 (Group Name)**
显示组名称。
- **用户名 (User Name)**
显示分配到该组的用户。

5.3.16 Security

该页面显示安全设置和本地用户帐户。



说明

“服务”(Services) 列表显示了安全设置。

- **Telnet 服务器 (Telnet Server)**

在“系统 > 组态”(System > Configuration) 中组态设置。

- 启用 (Enabled): 对 CLI 进行不加密形式的访问。
- 禁用 (Disabled): 无法对 CLI 进行不加密形式的访问。

- **SSH 服务器 (SSH Server)**

在“系统 > 组态”(System > Configuration) 中组态设置。

- 启用 (Enabled): 对 CLI 进行加密形式的访问。
- 禁用 (Disabled): 无法对 CLI 进行加密形式的访问。

- **Web 服务器 (Web Server)**

在“系统 > 组态”(System > Configuration) 中组态设置。

- HTTP/HTTPS: 可以通过 HTTP 和 HTTPS 访问 WBM。
- HTTPS: 只能通过 HTTPS 访问 WBM。

- **SNMP**

可以在“系统 > SNMP > 常规”(System > SNMP > General) 中组态设置。

- “-” (SNMP 已禁用)
不能通过 SNMP 访问设备参数。
- SNMPv1/v2c/v3
可以通过 SNMP 版本 1、2c 或 3 访问设备参数。
- SNMPv3
只可通过 SNMP 版本 3 访问设备参数。

5.3 “Information”菜单

- **管理 ACL (Management ACL)**

在“安全 > 管理 ACL”(Security > ManagementACL) 中组态设置。

- 禁用：无访问限制 (Disabled: no access restriction)

禁用访问控制。

- 启用：无访问限制 (Disabled: no access restriction)

已启用访问控制，但尚未定义任何访问规则。

- 启用：仅受限访问 (Enabled: restricted access only)

已启用访问控制，且已定义访问规则。

- **登录验证 (Login Authentication)**

在“安全 > AAA > 常规”(Security > AAA > General) 中组态设置。

- 本地 (Local)

必须在设备上进行本地验证。

- RADIUS

必须通过 RADIUS 服务器处理验证。

- 本地和 RADIUS (Local and RADIUS)

使用设备上的用户（用户名和密码）以及通过 RADIUS 服务器都可以进行验证。

首先在本地数据库中搜索用户。如果本地数据库中不存在该用户，将发送 RADIUS 查询。

- RADIUS 和备用本地 (RADIUS and fallback local)

必须通过 RADIUS 服务器处理验证。

只有无法在网络中访问 RADIUS 服务器时，才执行本地验证。

5.4 “System”菜单

5.4.1 组态 (Configuration)

系统组态

该 WBM 页面包含设备访问选项的组态概览。

指定用于访问设备的服务。对于某些服务提供了更多组态页面，可在其中进行更加具体的设置。

System Configuration

Telnet Server
 SSH Server
 HTTPS Server only
 SMTP Client
 Syslog Client

DCP Server: Read/Write

Time: Manual

SNMP: SNMPv1v2cV3

SNMPv1v2 Read-Only
 DHCP Client
 SNMPv1 Traps
 SINEMA Configuration Interface

Configuration Mode: Trial

Write Startup Config

Set Values Refresh

显示框说明

该页面包含以下框：

- **Telnet 服务器 (Telnet server)**
启用或禁用“Telnet 服务器”(Telnet server) 服务，以对 CLI 进行未加密的访问。
- **SSH 服务器 (SSH Server)**
启用或禁用“SSH 服务器”(SSH Server) 服务，以便对 CLI 进行加密访问。

5.4 “System”菜单

- **仅 HTTPS 服务器 (HTTPS Server only)**
如果启用此功能，则只能通过 HTTPS 访问 WBM。
- **SMTP 客户端 (SMTP Client)**
启用或禁用 SMTP 客户端。可以在“系统 > SMTP 客户端”(System > SMTP Client) 中组态其它设置。
- **Syslog 客户端 (Syslog Client)**
启用或禁用 Syslog 客户端。可以在“系统 > Syslog 客户端”(System > Syslog Client) 中组态其它设置。
- **DCP 服务器 (DCP Server)**
指定是否可用 DCP（发现和组态协议，Discovery and Configuration Protocol）访问设备：
 - “-”（已禁用）
DCP 已禁用。既不能读取也不能修改设备参数。
 - 读/写 (Read/Write)
借助 DCP，既可以读取设备参数又可以对其进行修改。
 - 只读 (Read Only)
借助 DCP，可以读取设备参数，但不能对其进行修改。
- **时间 (Time)**
从下拉列表中选择设置。可能的设置如下：
 - 手动 (Manual)
手动设置系统时间。可以在“系统 > 系统时间 > 手动设置”(System > System Time > Manual Setting) 中组态其它设置。
 - SIMATIC Time
通过 SIMATIC 时间发送器设置系统时间。可以在“系统 > 系统时间 > SIMATIC 时间客户端”(System > System Time > SIMATIC Time Client) 中组态其它设置。
 - SNTP 客户端 (SNTP client)
通过 SNTP 服务器对系统时间进行设置。可以在“系统 > 系统时间 > SNTP 客户端”(System > System Time > SNTP Client) 中组态其它设置。
 - NTP 客户端 (NTP client)
通过 NTP 服务器对系统时间进行设置。可以在“系统 > 系统时间 > NTP 客户端”(System > System Time > NTP Client) 中组态其它设置。

- **SNMP**

从下拉列表中选择协议。可能的设置如下：

- “-” (SNMP 已禁用)

不能通过 SNMP 访问设备参数。

- **SNMPv1/v2c/v3**

可以通过 SNMP 版本 1、2c 或 3 访问设备参数。可以在“系统 > SNMP > 常规”(System > SNMP > General) 中组态其它设置。

- **SNMPv3**

只可通过 SNMP 版本 3 访问设备参数。可以在“系统 > SNMP > 常规”(System > SNMP > General) 中组态其它设置。

- **SNMPv1/v2 只读 (SNMPv1/v2 Read Only)**

启用或禁用通过 SNMPv1/v2c 对 SNMP 变量进行写访问。

- **DHCP 客户端 (DHCP Client)**

启用或禁用 DHCP 客户端。可以在“System > DHCP 客户端”(System > DHCP Client) 中组态其它设置。

- **SNMPv1 陷阱 (SNMPv1 Traps)**

启用或禁用发送 SNMPv1 陷阱（报警帧）。可以在“系统 > SNMP > 陷阱”(System > SNMP > Traps) 中组态其它设置。

- **SINEMA 组态接口 (SINEMA configuration interface)**

如果启用了 SINEMA 组态接口，则可通过 STEP 7 Basic/Professional 将组态下载到工业以太网交换机中。

5.4 “System”菜单

- **NFC**

激活或取消激活“NFC”（近场通信）功能。

有关 NFC 的更多信息，请参见操作说明。

- **组态模式 (Configuration Mode)**

从下拉列表中选择模式。可能的模式如下：

- **自动保存 (Automatic Save)**

自动备份模式。在最后修改参数的约 1 分钟后或重启设备前，自动保存组态。

此外，显示区域中将出现如下消息“将在 x 秒内自动保存更改。按下‘写入启动组态’可立即保存更改。”(Changes will be saved automatically in x seconds.Press 'Write Startup Config' to save the changes immediately.)

说明

中断保存

只有消息中的定时器到期后，才会启动保存。保存所需的时间取决于设备。

- 不要在定时器到期后立即关闭设备。
-

- **Trial**

试用模式。在试用模式下，虽然会采用更改，但不会将更改保存在组态文件中（启动组态）。

要将更改保存在组态文件中，请使用“写入启动组态”(Write startup config) 按钮。只要存在未保存的更改内容，显示区仍会显示消息“试用模式已激活 - 单击‘写入启动组态’按钮保存设置”(Trial mode active - Press "Write Startup Config" button to make your settings persistent)。可以在每个 WBM 页面上看到这条消息，直至所做的更改已保存或设备已重启。

组态步骤

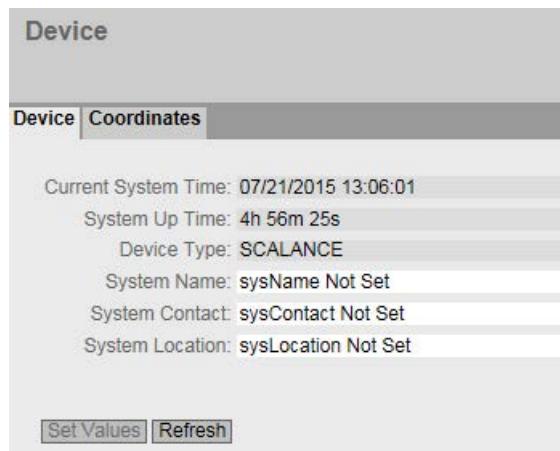
1. 要使用所需功能，请选中相应的复选框。
2. 从下拉列表中选择所需选项。
3. 单击“设置值”(Set Values) 按钮。

5.4.2 常规 (General)

5.4.2.1 设备 (Device)

常规设备信息

该页面包含常规设备信息。



The screenshot shows a web interface for device configuration. At the top, there is a header 'Device' with a sub-header 'Coordinates'. Below this, there are several rows of information:

Current System Time:	07/21/2015 13:06:01
System Up Time:	4h 56m 25s
Device Type:	SCALANCE
System Name:	sysName Not Set
System Contact:	sysContact Not Set
System Location:	sysLocation Not Set

At the bottom of the form, there are two buttons: 'Set Values' and 'Refresh'.

无法更改“当前系统时间”(Current System Time)、“系统运行时间”(System Up Time)和“设备类型”(Device Type) 框。

说明

该页面包含以下框：

- **Current System Time**
显示当前系统时间。系统时间由用户或时钟帧设置：即 SINEC H1 时钟帧、NTP 或 SNTP。（只读）
- **System Up Time**
显示设备自上次重启以来的运行时间。（只读）
- **Device Type**
显示设备的型号标识。（只读）
- **System Name**
可以输入设备的名称。输入的名称显示在选择区域中。最多支持 255 个字符。系统名称还显示在 CLI 输入提示中。CLI 输入提示中的字符数是有限的。系统名称前 16 个字符后面的部分将被截断。

5.4 “System”菜单

- **System Contact**

可输入设备管理责任人的名字。最多支持 255 个字符。

- **System Location**

可输入设备的安装位置。输入的安装位置显示在选择区域中。最多支持 255 个字符。

说明

输入框中使用 ASCII 码 0x20 至 0x7e。

在“System name”、“System Contact”和“System Location”框的开头和结尾，不允许使用“<”、“>”和“空格”字符。

步骤

1. 在“System Contact”输入框中输入设备管理责任人。
2. 在“System Location”输入框中输入设备安装位置的标识符。
3. 在“System Name”输入框中输入设备的名称。
4. 单击“Set Values”按钮。

5.4.2.2 坐标 (Coordinates)

有关地理坐标的信息

在“地理坐标”(Geographic Coordinates)

窗口中，可以输入地理坐标的相关信息。可以在“地理坐标”(Geographic Coordinates)窗口的输入框中直接输入地理坐标的参数（符合 WGS84 的椭球面纬度、经度和高度）。

获取坐标

使用适当的地图来获取设备的地理坐标。

还可以通过 GPS

接收器获取地理坐标。设备的地理坐标通常会直接显示，并且只需要在该页面的输入框中输入即可。

Device	Coordinates
	Latitude: e.g. DD°MM'SS"
	Longitude: e.g. DDD°MM'SS"
	Height: e.g. dddd m

说明

该页面包含以下框。这些是最多可包含 32 个字符的纯信息框。

- **“Latitude”输入框**
地理纬度：在此输入设备位置的北纬值或南纬值。
例如，值 $+49^{\circ} 1'31.67''$ 表示设备位于北纬 49 度、1 弧分和 31.67 弧秒。
通过在前面加上负号显示南纬度。
还可以在数字信息后面附加字母 **N**（北纬）或 **S**（南纬），如 $49^{\circ} 1'31.67'' \text{ N}$ 。
- **“Longitude”输入框**
地理经度：在此输入设备位置的东经或西经值。
 $+8^{\circ} 20'58.73''$ 表示设备位于东经 8 度、20 分和 58.73 秒。
通过在经度前面加上负号表示西经。
还可以在数字信息前面加上字母 **E**（东经）或 **W**（西经），如 $8^{\circ} 20'58.73'' \text{ E}$ 。
- **输入框：“Height”**
在此输入地理海拔高度的米数值。
例如，**158 m** 表示设备位于海平面上 158 m 高的位置。
对于低于海平面的高度（例如死海），可在前面添加负号来进行表示。

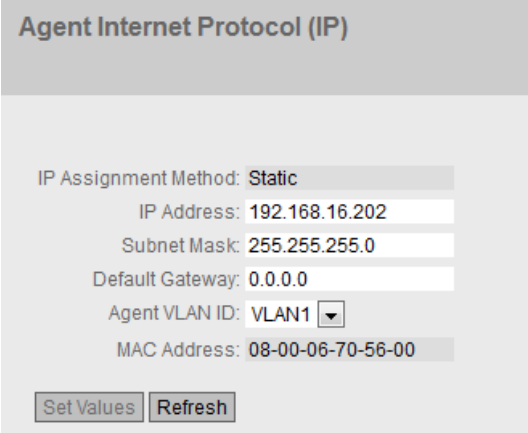
步骤

1. 在“Latitude”输入框中输入计算得出的纬度。
2. 在“Longitude”输入框中输入计算得出的经度。
3. 在“Height”输入框中输入海拔高度。
4. 单击“Set Values”按钮。

5.4.3 代理 IP (Agent IP)

IP 地址组态

在此 WBM 页面中组态设备的 IP 地址。



Agent Internet Protocol (IP)

IP Assignment Method: **Static**

IP Address: 192.168.16.202

Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

Agent VLAN ID: VLAN1

MAC Address: 08-00-06-70-56-00

Set Values Refresh

说明

该页面包含以下框：

- **IP 分配方法 (IP Assignment Method)**

显示如何分配 IP 地址。

- 静态 (Static)

IP 地址是静态的。在“IP 地址”(IP Address) 和“子网掩码”(Subnet Mask) 中输入 IP 设置。

- 动态 (DHCP) (Dynamic (DHCP))

设备从 DHCP 服务器获得动态 IP 地址。

- **IP 地址 (IP Address)**

输入设备的 IP 地址。

单击“设置值”(Set Values) 按钮后，此 IP 地址也将显示在 Internet 浏览器的地址栏中。如果未自动显示，则需要手动在 Internet 浏览器的地址栏中输入该 IP 地址。

- **子网掩码 (Subnet Mask)**

输入设备的子网掩码。

- **默认网关 (Default gateway)**

输入默认网关的 IP

地址，以便可以与其它子网内的设备（如诊断站、电子邮件服务器）进行通信。

- **代理 VLAN ID (Agent VLAN ID)**

从下拉列表中选择 VLAN ID。只可以选择已组态的 VLAN。

在“802.1D 透明网桥”模式下，此下拉列表呈灰显，另请参见“第 2 层 > VLAN > 常规”(Layer 2 > VLAN > General)。

说明

更改“代理 VLAN ID”(agent VLAN ID)

如果组态 PC 通过以太网与设备直接相连，并且您更改了“代理 VLAN ID”(agent VLAN ID)，则更改后无法再通过以太网访问该设备。

- **“MAC 地址”(MAC Address)**

显示设备的 MAC 地址。MAC 地址链接到了硬件，无法修改。

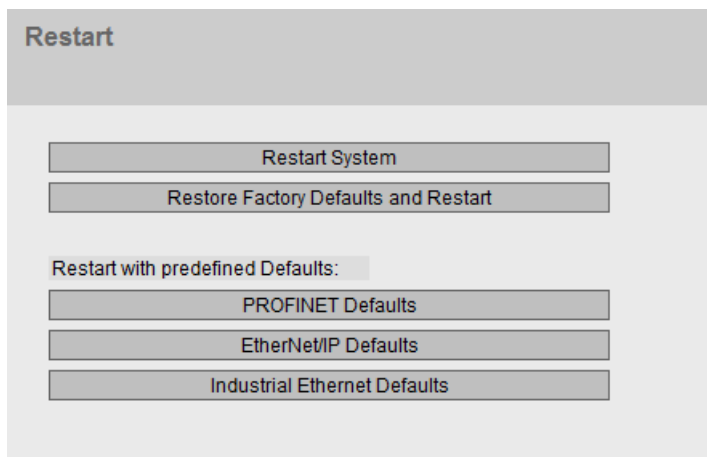
步骤

1. 在输入框中输入 IP 地址、子网掩码和默认网关。
2. 从“代理 VLAN ID”(Agent VLAN ID) 下拉列表中选择分配的 VLAN ID。
3. 单击“设置值”(Set Values) 按钮。

5.4.4 重启 (Restart)

复位为默认设置

在此菜单中，有一个可用来重新启动设备的按钮，以及用于复位为出厂设置或复位不同配置文件的默认设置的选项。



重启 (Restart)

对于重启设备，请注意以下几点：

- 仅在拥有管理员权限时才能重启设备。
- 设备只可以通过该菜单的按钮或适当的 CLI 命令来重启，而不能通过设备的循环上电来重启。
- 如果设备处于“Trial”模式，则必须在重启之前手动保存对组态所做的修改。所作的任何修改仅在单击相关 WBM 页面上的“设置值”(Set values) 按钮后才会设备上生效。
- 如果设备在“自动保存”(Automatic Save) 模式下，会在设备重启之前自动保存最后的更改。

复位为出厂默认设置

将所有设置复位为出厂设置时，IP 地址和密码均会丢失。之后，只能利用 Primary Setup Tool 或 DHCP 通过串行接口访问设备。

注意

在特定连接情况下，之前已正确组态的设备复位后可能会引起数据帧循环传送，从而导致数据通信故障。
--

复位为默认值（配置文件）

配置文件针对设备的不同用途提供预组态。

当您以配置文件的默认设置启动设备时，设置将复位为出厂设置，某些参数将针对特定用途进行设置。与复位为出厂设置不同，用户和密码在重启后保持不变。组态的 IP 地址丢失，因此之后只能利用 Primary Setup Tool 或 DHCP 通过串行接口访问设备。

注意

在特定连接情况下，之前已正确组态的设备复位后可能会引起数据帧循环传送，从而导致数据通信故障。
--

重启前，将显示针对配置文件专门进行的设置。

配置文件可独立于设备的出厂设置单独使用。

显示框说明

说明

请注意上述部分提到的各个功能的影响。

5.4 “System”菜单

为重启设备，该页面上的按钮提供了以下选项：

- **重启 (Restart)**

单击该按钮可重启系统。必须在对话框中确认重启操作。重启期间，将重新初始化设备，重新加载内部固件，并且设备会执行自检。启动组态的设置保持不变，例如设备的 IP

地址。此外会删除地址表中已学习到的条目。在设备重启期间，可以不关闭浏览器窗口。重启后，您将需要再次登录。

- **恢复出厂默认设置并重启 (Restore Factory Defaults and Restart)**

单击该按钮可恢复设备的出厂默认设置并重启设备。必须在对话框中确认重启操作。

出厂默认设置取决于设备。

为重启带预定义配置文件的设备，该页面上的按钮提供了以下选项：

- **PROFINET 默认设置 (PROFINET Defaults)**

单击该按钮可恢复 PROFINET

配置文件的默认设置并重启设备。必须在对话框中确认重启操作。对话框将显示专门针对使用 PROFINET 协议的操作进行的设置。

- **EtherNet/IP 默认设置 (EtherNet/IP Defaults)**

单击该按钮可恢复 EtherNet/IP

配置文件的默认设置并重启设备。必须在对话框中确认重启操作。对话框将显示专门针对使用 EtherNet/IP 协议的操作进行的设置。

- **工业以太网默认设置 (Industrial Ethernet Defaults)**

单击该按钮可恢复工业以太网配置文件的默认设置并重启设备。必须在对话框中确认重启操作。对话框将显示专门针对工业以太网环境中的操作进行的设置。

5.4.5 加载和保存

文件类型概述

文件类型	说明
Config	此文件包含启动组态。 此外，该设备还包含用户的定义。密码存储在“用户”(Users)文件中。
ConfigPack	详细组态信息。例如，启动组态、用户、证书包含组态、用户和 LSYS 文件的 ZIP 文件。
版权	OSS 许可证
Debug	此文件包含有关 Siemens 支持的信息。 它已被加密，可通过电子邮件发送给 Siemens 支持且不会带来安全风险。
EDS	电子数据表 (EDS) 电子数据表用于描述 EtherNet/IP 模式下的设备
固件	固件已签名且加密。这可确保只能将 Siemens 创建的固件下载到设备。
GSDML	有关设备属性的 PROFINET 信息
HTTPSCert	包含密钥的默认 HTTPS 证书 预设及自动创建的 HTTPS 证书均为自签署证书。 强烈建议您创建自己的 HTTPS 证书并使其可用。建议您使用由可靠外部或内部认证机构签署的 HTTPS 证书。HTTPS 证书会检查设备的身份并控制加密数据交换。 不能复制不同格式的证书。
LogFile	带有事件日志表中条目的文件
MIB	专有 MSPS MIB 文件
RunningCLI	包含 CLI 命令的文本文件 此文件包含 CLI 命令形式的当前组态概览。可下载此文本文件。如果此文件未更改，则不会再次上传。

5.4 “System”菜单

文件类型	说明
Script	包含 CLI 命令的文本文件 可以在设备中上传脚本文件。会相应地执行其中包含的 CLI 命令。
StartupInfo	启动日志文件 该文件包含上次启动时已在日志中输入的消息。
用户	该文件包含分配给相应密码的用户名。

5.4.5.1 HTTP

通过 HTTP 加载和保存数据

WBM 使您可以将设备数据存储于客户端 PC 上的外部文件中，或将此数据从客户端 PC 的外部文件加载到设备中。这意味着，您也可以通过位于客户端 PC 上的文件加载新固件等。

说明

此 WBM 页面在通过 HTTP 或 HTTPS 建立连接时均可用。

固件

固件已签名且加密。这可确保只能将 Siemens 创建的固件下载到设备。

说明

插入/未插入 PLUG 时与先前固件版本的不兼容性

在安装先前版本的过程中，组态数据可能丢失。在这种情况下，安装固件后，设备会使用出厂设置启动。

如果此时设备中插入 PLUG，由于 PLUG 仍保持之前最新固件的组态数据，因此重启后状态为“不接受”。这样，您便可以返回之前的最新固件而不丢失任何组态数据。如果不再需要 PLUG 上的原始组态，则可使用 WBM 页面“系统 > PLUG”(System > PLUG) 手动删除或重写 PLUG。

组态文件

说明

组态文件和 Trial 模式/自动保存

在“自动保存”模式下，数据会在传输组态文件（ConfigPack 和 Config）前自动保存。在 Trial 模式下，虽然会采用更改，但不会将更改保存在组态文件（ConfigPack 和 Config）中。在“系统 > 组态”(System > Configuration) WBM 页面中使用“写入启动组态”(Write Startup Config) 按钮将更改保存在组态文件中。

CLI 脚本文件

可下载现有 CLI 组态 (RunningCLI) 并上传您自己的 CLI 脚本 (Script)。

说明

如果可下载的 CLI 脚本未更改，则不会再次上传。

Load and Save via HTTP

HTTP |
 TFTP |
 Passwords

Type	Description	Load	Save	Delete
Config	Startup Configuration	<input type="button" value="Load"/>	<input type="button" value="Save"/>	
ConfigPack	Startup Config, Users and Certificates	<input type="button" value="Load"/>	<input type="button" value="Save"/>	
Copyright	Copyright		<input type="button" value="Save"/>	
Debug	Debug Information for Siemens Support		<input type="button" value="Save"/>	<input type="button" value="Delete"/>
EDS	EDS		<input type="button" value="Save"/>	
Firmware	Firmware Update	<input type="button" value="Load"/>	<input type="button" value="Save"/>	
GSDML	GSDML Device Description		<input type="button" value="Save"/>	
HTTPSCert	HTTPS Certificate	<input type="button" value="Load"/>	<input type="button" value="Save"/>	<input type="button" value="Delete"/>
LogFile	Event Log (ASCII)		<input type="button" value="Save"/>	
MIB	SCALANCE XB200 MSPS MIB		<input type="button" value="Save"/>	
RunningCLI	'show running-config all' CLI settings		<input type="button" value="Save"/>	
Script	Script	<input type="button" value="Load"/>		
StartupInfo	Startup Information		<input type="button" value="Save"/>	
Users	Users and Passwords	<input type="button" value="Load"/>	<input type="button" value="Save"/>	

5.4 “System”菜单

显示框说明

该表格包括以下列：

- **类型 (Type)**
显示文件类型。
- **说明 (Description)**
显示文件类型的简要说明。
- **加载 (Load)**
可以使用此按钮将文件上传到设备。如果文件类型支持该功能，将启用该按钮。
- **保存 (Save)**
可使用此按钮从设备下载文件。仅当文件类型支持该功能且文件存在于设备上时，才会启用该按钮。
- **Delete**
可以使用此按钮删除设备中的文件。仅当文件类型支持该功能且文件存在于设备上时，才会启用该按钮。

说明

更新固件之后，请删除 Internet 浏览器的缓存。

组态步骤

使用 HTTP 上传文件

1. 单击“加载”(Load) 按钮之一即可启动上传功能。
将打开用于上传文件的对话框。
2. 选择所需文件并确认上传。
上传文件。
3. 如果需要重启，将输出相应消息。单击“确定”(OK) 按钮，之后将重启。如果单击“中止”(Abort) 按钮，设备将不会重启。所做的更改只在重启后生效。

使用 HTTP 上传文件

1. 单击“保存”(Save) 按钮之一即可启动下载操作。
2. 选择存储位置并输入文件名。
3. 保存文件。

随即会下载并保存文件。

使用 HTTP 删除文件

1. 单击“Delete”按钮之一启动删除功能。

随即会删除文件。

复用组态数据

如果多台相同的设备将接收相同的组态，且已通过 DHCP 分配 IP 地址，则可通过保存并读入组态数据来简化重新组态过程。

要复用组态数据，请按以下步骤操作：

1. 将已组态设备的组态数据保存在 PC 上。
2. 按这种方式将该组态文件加载到要组态的所有其它设备中。
3. 如果有必要对特定设备进行单独设置，则必须在相关设备上在线进行设置。

说明

组态数据具有校验和。如果修改这些数据，将无法再将其上传到工业以太网交换机。

5.4.5.2 TFTP

通过 TFTP 服务器加载和保存数据

在该页面上，可以组态 TFTP 服务器和文件名。WBM 使您可以将设备数据存储在 TFTP 服务器上的外部文件中，或将此数据从 TFTP 服务器上的外部文件加载到设备中。这意味着，您也可以通过位于 TFTP 服务器上的文件加载新固件等。

5.4 “System”菜单

固件

固件已签名且加密。这可确保只能将 **Siemens** 创建的固件下载到设备。

说明

插入/未插入 **PLUG** 时与先前固件版本的不兼容性

在安装先前版本的过程中，组态数据可能丢失。在这种情况下，安装固件后，设备会使用出厂设置启动。

如果此时设备中插入 **PLUG**，由于 **PLUG** 仍保持之前最新固件的组态数据，因此重启后状态为“不接受”。这样，您便可以返回之前的最新固件而不丢失任何组态数据。如果不再需要 **PLUG** 上的原始组态，则可使用 **WBM** 页面“系统 > **PLUG**”(System > **PLUG**) 手动删除或重写 **PLUG**。

组态文件

说明

组态文件和 **Trial** 模式/自动保存

在“自动保存”模式下，数据会在传输组态文件 (**ConfigPack** 和 **Config**) 前自动保存。在 **Trial** 模式下，虽然会采用更改，但不会将更改保存在组态文件 (**ConfigPack** 和 **Config**) 中。在“系统 > 组态”(System > Configuration) **WBM** 页面中使用“写入启动组态”(Write Startup Config) 按钮将更改保存在组态文件中。

CLI 脚本文件

可下载现有 **CLI** 组态 (**RunningCLI**) 并上传您自己的 **CLI** 脚本 (**Script**)。

说明

如果可下载的 **CLI** 脚本未更改，则不会再次上传。

Load and Save via TFTP

HTTP
TFTP
Passwords

TFTP Server Address:

TFTP Server Port:

Type	Description	Filename	Actions
Config	Startup Configuration	config_SCALANCE_XB200.conf	Select action <input type="button" value="v"/>
ConfigPack	Startup Config, Users and Certificates	configpack_SCALANCE_XB200.zip	Select action <input type="button" value="v"/>
Copyright	Copyright	ReadMe_OSS_SCALANCE_XB200.zip	Select action <input type="button" value="v"/>
Debug	Debug Information for Siemens Support	debug_SCALANCE_XB200.bin	Select action <input type="button" value="v"/>
EDS	EDS	EDS_SCALANCE_XB208.zip	Select action <input type="button" value="v"/>
Firmware	Firmware Update	firmware_SCALANCE_XB200.sfw	Select action <input type="button" value="v"/>
GSDML	GSDML Device Description	gsdml_SCALANCE_XB200.zip	Select action <input type="button" value="v"/>
HTTPSCert	HTTPS Certificate	https_cert	Select action <input type="button" value="v"/>
LogFile	Event Log (ASCII)	logfile_SCALANCE_XB200.csv	Select action <input type="button" value="v"/>
MIB	SCALANCE XB200 MSPS MIB	scalance_x_xb200_msps.mib	Select action <input type="button" value="v"/>
RunningCLI	'show running-config all' CLI settings	RunningCLI.txt	Select action <input type="button" value="v"/>
Script	Script	Script.txt	Select action <input type="button" value="v"/>
StartupInfo	Startup Information	startup_SCALANCE_XB200.log	Select action <input type="button" value="v"/>
Users	Users and Passwords	users.enc	Select action <input type="button" value="v"/>

显示框说明

该页面包含以下框：

- **TFTP 服务器地址 (TFTP Server Address)**
在此输入用于交换数据的 TFTP 服务器的 IP 地址。
- **TFTP 服务器端口 (TFTP Server Port)**
在此输入处理数据交换的 TFTP 服务器的端口。如有必要，可以将默认值 69 更改为适合您需要的值。

该表格包括以下列：

- **类型 (Type)**
显示文件类型。
- **说明 (Description)**
显示文件类型的简要说明。

- **文件名 (Filename)**

在此为每种文件类型预设一个文件名。

说明

更改文件名

可以更改此列中预设的文件名。单击“设置值”(Set Values)

按钮后，更改后的文件名会保存在设备上，并且还可用于命令行接口。

- **操作 (Actions)**

从下拉列表中选择操作。可供选择的选项取决于所选文件类型，例如，只能保存日志文件。

可能的操作包括：

- **保存文件 (Save file)**

通过该选项将文件保存到 TFTP 服务器上。

- **加载文件 (Load file)**

通过该选项加载 TFTP 服务器中的文件。

组态步骤

通过 TFTP 加载或保存数据

1. 在“TFTP 服务器地址”(TFTP Server Address) 输入框中输入 TFTP 服务器的 IP 地址。
2. 在“TFTP 服务器端口”(TFTP Server Port) 输入框中输入要使用的 TFTP 服务器的服务器端口。
3. 如果适用，在“文件名”(File name) 输入框中输入要保存数据或从中获取数据的文件的名称。
4. 从“操作”(Actions) 下拉列表中选择要执行的操作。
5. 单击“设置值”(Set Values) 按钮启动所选操作。
6. 如果需要重启，将输出相应消息。单击“确定”(OK) 按钮，之后将重启。如果单击“中止”(Abort) 按钮，设备将不会重启。所做的更改只在重启后生效。

复用组态数据

如果多台相同的设备将接收相同的组态，且已通过 DHCP 分配 IP 地址，则可通过保存并读入组态数据来简化重新组态过程。

要复用组态数据，请按以下步骤操作：

1. 将已组态设备的组态数据保存在 PC 上。
2. 按这种方式将该组态文件加载到要组态的所有其它设备中。
3. 如果有必要对特定设备进行单独设置，则必须在相关设备上在线进行设置。

说明

组态数据具有校验和。如果修改这些数据，将无法再将其上传到工业以太网交换机。

5.4.5.3 密码 (Passwords)

有些文件的访问受密码保护。例如，为了能够使用 HTTPS 证书，需要在 WBM 页面上指定相应的密码。

Passwords					
HTTP	TFTP	Passwords			
Type	Description	Enabled	Password	Password Confirmation	Status
HTTPSert	HTTPS Certificate	<input checked="" type="checkbox"/>	••••••	••••••	-

Set Values Refresh

说明

该表格包括以下列：

- **Type**
显示文件类型。
- **Description**
显示文件类型的简要说明。
- **Enabled**
选中后，将使用文件。只有在组态了密码的情况下才能启用。
- **Password**
输入文件的密码。

5.4 “System”菜单

- **Password Confirmation**
确认密码。
- **Status**
显示文件的当前设置是否与设备相匹配。
 - 有效 (Valid)
“启用”(Enabled) 复选框已选中且密码与文件匹配。
 - 无效 (Invalid)
“启用”(Enabled) 复选框已选中，但密码与文件不匹配或者尚未加载文件。
 - ' '
无法评估密码或者尚未使用密码。未选中“启用”(Enabled) 复选框。

步骤

1. 在“Password”中输入密码。
2. 要确认密码，在“Password Confirmation”中再次输入密码。
3. 选择“Enabled”选项。
4. 单击“Set Values”按钮。

5.4.6 事件

5.4.6.1 组态

选择系统事件

在此页面中指定设备对系统事件的响应方式。要启用或禁用选项，请单击各列的相关复选框。

Event Configuration

Configuration
Severity Filters

Signaling Contact Method: conventional

Signaling Contact Status: open

	E-mail	Trap	Log Table	Syslog	Fault	Copy To Table
All Events	No Change	No Change	No Change	No Change	No Change	Copy To Table

Event	E-mail	Trap	Log Table	Syslog	Fault
Cold/Warm Start	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Link Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Authentication Failure	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
RMON Alarm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Power Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
RM State Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Spanning Tree Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Fault State Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Standby State Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Loop Detection	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Pnac Port Authentication State Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
PoE State Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Temperature Alarms	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Set Values
Refresh

显示框说明

该页面包含以下框：

- **信号触点方法 (Signaling Contact Method)**

从下拉列表中选择信号触点反应。可能的响应包括：

- 传统 (conventional)

默认的信号触点设置。由故障 LED

指示错误/故障，并且信号触点断开。错误/故障状态不再存在时，故障 LED 熄灭，并且信号触点闭合。

- 用户自定义 (User Defined)

信号触点的工作方式不取决于已发生的错误/故障。可以根据用户操作的要求断开或闭合信号触点。

- **信号触点状态 (Signaling Contact Status)**

要改变信号触点的状态，从“信号触点的状态”(Signaling Contact Method)

下拉列表中选择“用户自定义”(User defined)。

从下拉列表中选择信号触点的状态。可能的状态如下：

- 闭合 (Closed)

信号触点闭合。

- 断开 (Open)

信号触点断开。

利用表 1，可以一次启用或禁用表 2 中某个列的所有复选框。表 1 包含以下列：

- **所有事件 (All Events)**

说明设置对于表 2 的所有事件都有效。

- **电子邮件 (E-mail)/陷阱 (Trap)/日志表 (Log Table)/Syslog/故障 (Faults)**

启用或禁用所有事件的所需通知类型。如果选中“无变化”(No Change)，则表 2 中相应列的条目保持不变。

- **复制到表 (Copy to Table)**

如果单击此按钮，则为表 2 的所有事件应用此设置。

表 2 包含以下列：

- **事件 (Event)**

此列包含以下值：

- **冷/热启动 (Cold/Warm Start)**
用户打开或重启设备。在设备的故障存储器中，生成新条目，且具有所执行的重启的类型。
- **“链路变化”(Link Change)**
仅当对接口状态进行监视和更改时才会发生该事件，请参阅“系统 > 故障监视 > 链路变化”(System > Fault Monitoring > Link Change)。
- **验证失败 (Authentication Failure)**
当试图用错误的密码访问时会发生该事件。
- **“RMON 报警”(RMON Alarm)**
发生了与系统远程监视相关的报警或事件。
- **电源变化 (Power Change)**
仅当对电源线路 1 和 2 进行监视时才会发生该事件。这表示线路 1 或线路 2 发生了变化。请参见“系统 > 故障监视 > 电源”(System > Fault Monitoring > Power Supply)。
- **RM 状态变化 (RM State Change)**
冗余管理器已识别到环网出现中断或恢复的情况，并已相应地切换线路。
- **生成树变化 (Spanning Tree Change)**
生成树拓扑发生变化。
- **故障状态变化 (Fault State Change)**
故障状态已发生变化。故障状态可能涉及已激活的端口监视、信号触点的响应或电源监视。
- **备用状态变化 (Standby State Change)**
已建立备用连接的设备（主设备或从设备）激活或禁用了与其它环网之间的链路（备用端口）。数据通信从一个以太网连接（主设备的备用端口）重定向到其它以太网连接（从设备的备用端口）。
- **回路检测 (Loop detection)**
在网段中检测到回路。
- **802.1X 端口验证状态变化 (802.1X Port Authentication State Change)**
此事件在 802.1X 身份验证时发生。

5.4 “System”菜单

- PoE 状态变化(State Change)
PoE 状态已发生变化。
- 温度报警 (Temperature Alarm)
温度已降至特定限值以下或超出特定限值。
- **电子邮件 (E-mail)**
设备发送电子邮件。仅当已设置 SMTP 服务器并已启用“SMTP 客户端”(SMTP client) 功能时，该功能才可用。
- **“陷阱”(Trap)**
设备发送 SNMP 陷阱。仅当已在“System > Configuration”中启用 SNMPv1 Traps 时，该功能才可用。
- **“日志表”(Log Table)**
设备在事件日志表中写入一个条目，请参阅“信息 > 日志表”(Information > Log Table)
- **Syslog**
设备将一个条目写入系统日志服务器。仅当已设置系统日志服务器并已启用“Syslog 客户端”(Syslog client) 功能时，该功能才可用。
- **故障 (Faults)**
设备触发一个故障。错误 LED 亮起

组态步骤

1. 选中所需事件行的复选框。在以下操作下的列中选择事件：
 - 电子邮件 (E-mail)
 - 陷阱 (Trap)
 - 日志表 (Log table)
 - Syslog
 - 故障 (Faults)
2. 单击“设置值”(Set Values) 按钮。

5.4.6.2 严重程度过滤器 (Severity Filters)

设置 Severity Filters

在此页面上，设置发送系统事件通知的阈值级别。

Client Type	Severity
E-mail	Info
Log Table	Info
Syslog	Info

表格首列显示了要进行设置的客户端类型：

- **E-mail**
通过电子邮件发送系统事件消息
- **Log Table**
在日志表中输入系统事件
- **Syslog**
将系统事件消息发送至 Syslog 服务器。

从表格第二列的下拉列表中选择所需等级。

您可以从以下值中选择：

- **Critical**
处理严重程度不低于“Critical”级别的系统事件。
- **Warning**
处理严重程度不低于“Warning”级别的系统事件。
- **Info**
处理严重程度不低于“Info”级别的系统事件。

5.4 “System”菜单

步骤

按以下步骤组态所需级别：

1. 组态客户端类型后，从表格第二列的下拉列表中选择所需值。
2. 单击“Set Values”按钮。

5.4.7 SMTP 客户端

通过电子邮件进行网络监视

设备提供了在发生报警事件时自动发送电子邮件的选项（例如发送给网络管理员）。该电子邮件包含发送设备的标识、报警原因的简单说明以及时间戳。这样便可基于电子邮件系统使用很少的节点为网络建立集中式网络监视。当接收到电子邮件事件消息时，可通过 Internet 浏览器启动 WBM 来利用发送方的标识读出更多诊断信息。

在此页可组态最多三个 SMTP 服务器和相应的电子邮件地址。

Simple Mail Transfer Protocol (SMTP) Client

SMTP Client

Sender Email Address: device@scalance

SMTP Port: 25

SMTP Server Address:

Select	SMTP Server Address	Receiver Email Address
<input type="checkbox"/>	192.168.16.20	service@scalance

1 entry.

说明

该页面包含以下框：

- **SMTP 客户端 (SMTP Client)**
启用或禁用 SMTP 客户端。
- **发送方电子邮件地址 (Sender Email Address)**
输入电子邮件中的发送方名称，如设备名称。
此设置适用于所有已组态的 SMTP 服务器。
- **发送测试电子邮件 (Send Test Mail)**
发送一封测试电子邮件检查组态。
- **SMTP 端口 (SMTP Port)**
输入可用来访问 SMTP 服务器的端口。
出厂设置：25
此设置适用于所有已组态的 SMTP 服务器。
- **SMTP 服务器地址 (SMTP Server Address)**
输入 SMTP 服务器的 IP 地址。

该表包含以下各列：

- **选择 (Select)**
启用要删除的行中的复选框。
- **SMTP 服务器地址 (SMTP Server Address)**
显示 SMTP 服务器的 IP 地址。
- **接收方电子邮件地址 (Receiver Email Address)**
输入电子邮件地址，发生故障时，设备会将电子邮件发送到该地址。

步骤

1. 启用“SMTP 客户端”(SMTP Client) 选项。
2. 在“发送方电子邮件地址”(Sender Email Address) 输入框中输入相关的电子邮件地址。
3. 如有必要发送一封测试电子邮件。
4. 在“SMTP 服务器地址”(SMTP Server Address) 输入框中输入 SMTP 服务器的 IP 地址。
5. 单击“创建”(Create) 按钮。会在表中生成一个新条目。

5.4 “System”菜单

6. 在“接收方电子邮件地址”(Receiver Email Address) 输入框中，输入电子邮件地址，发生故障时，设备会将电子邮件发送到该地址。
7. 单击“设置值”(Set Values) 按钮。

5.4.8 DHCP

5.4.8.1 DHCP 客户端

DHCP 模式设置

如果设备组态为 DHCP 客户端，则它将启动 DHCP 查询。作为对查询的回复，设备将从 DHCP 服务器接收 IPv4 地址。服务器管理一个地址范围，并且分配该范围内的 IPv4 地址。还可以对服务器进行组态，使得客户端发出请求后，总是接收到同一个 IPv4 地址。

The screenshot shows the 'Dynamic Host Configuration Protocol (DHCP) Client' configuration page. It features a navigation bar with tabs for 'DHCP Client', 'DHCP Server', 'Port Range', 'DHCP Options', 'Relay Agent Information', and 'Static Leases'. The 'DHCP Client' tab is active. The main content area includes a checked checkbox for 'DHCP Client Configuration Request (Opt.66, 67)', a 'DHCP Mode' dropdown menu set to 'via MAC Address', and a table with columns 'Interface' and 'DHCP'. The table lists 'vlan1' with an unchecked checkbox. At the bottom, there are 'Set Values' and 'Refresh' buttons.

Interface	DHCP
vlan1	<input type="checkbox"/>

说明

该页面包含以下框：

- **DHCP 客户端组态请求（66、67 选项）(DHCP client configuration request (opt. 66, 67))**
如果想要 DHCP 客户机使用选项 66 和 67 下载并随后启用某个组态文件，则选择此选项。

- **DHCP Mode**

从下拉列表中选择 DHCP 模式。可能的模式如下：

- **via MAC Address**
基于 MAC 地址识别设备。
- **via DHCP Client ID**
基于自由定义的 DHCP 客户端 ID 识别设备。
- **via System Name**
基于系统名称识别设备。如果系统名称的长度为 255 个字符，则最后一个字符不用于识别设备。
- **通过站的 PROFINET 名称 (via PROFINET Name of Station)**
使用 PROFINET 设备名称识别。

该表格包括以下列：

- **Interface**

与设置相关的接口。

- **DHCP**

为相关接口启用或禁用 DHCP 客户端。

步骤

1. 从“DHCP 模式”(DHCP Mode) 下拉列表中选择所需模式。如果选择 DHCP 模式“通过 DHCP 客户端 ID”(via DHCP Client ID)，则将出现输入框。
 - 在启用的“DHCP 客户端 ID”(DHCP client ID) 输入框中，输入用于识别设备的字符串。DHCP 服务器随即会评估该字符串。
2. 选择“DHCP 客户端组态请求（选项 66 和 67）”(DHCP Client Configuration Request (Opt. 66, 67))，如果想要 DHCP 客户机使用选项 66 和 67 下载并随后启用某个组态文件，则选择此选项。
3. 在表中启用“DHCP”选项。
4. 单击“Set Values”按钮。

说明

如果下载组态文件，这会触发系统重启。如果当前运行的组态和所已下载的配置文件中配置不同，则系统将重启。

确保不再设置选项“DHCP 客户端组态请求（选项 66 和 67）”(DHCP Client Configuration Request (Opt. 66, 67))。

5.4.8.2 DHCP 服务器

可将设备用作 DHCP 服务器。从而可自动为相连的设备分配 IP 地址。既可以通过指定的地址段（池）动态分布 IP 地址，也可以将一个特定的 IP 地址分配给一个特定设备。

在此页面上指定地址段，所连设备接收该地址段的任一 IP 地址。在“静态租用”(Static Leases) 中组态 IP 地址的静态分配。

Select	Pool ID	Interface	Enable	Subnet	Lower IP Address	Upper IP Address	Lease Time [sec]
<input type="checkbox"/>	1	vlan1	<input type="checkbox"/>	0.0.0.0/0	0.0.0.0	0.0.0.0	3600

要求

将所连设备组态成从 DHCP 服务器中获取 IP 地址。

说明

该页面包含以下框：

- **DHCP 服务器 (DHCP Server)**

启用或禁用设备上的 DHCP 服务器。

说明

为避免 IPv4 地址发生冲突，在网络中只能将一个设备组态为 DHCP 服务器。

- **提供服务前通过 ICMP 回送检查地址 (Probe address with ICMP echo before offer)**

选中后，DHCP 服务器会检查是否已经分配 IP 地址。为此，DHCP 服务器会向此 IPv4 地址发送 ICMP 回送消息 (ping)。如果未收到应答，则会分配 IPv4 地址。

说明

如果网络中存在回送服务默认被禁用的设备，则可能发生 IPv4 地址冲突。为避免这种情况发生，请使用 DHCP 服务器为这样的设备分配 IPv4 地址段以外的 IPv4 地址。

该表格包括以下列：

- **选择 (Select)**

选中要删除的行中的复选框。

- **池 ID (Pool ID)**

显示 IPv4 地址段编号。如果单击“创建”(Create) 按钮，会创建一个具有唯一编号的新行（池 ID）。

- **接口 (Interface)**

选择 VLAN IP 接口。IPv4 地址通过此接口动态分配。

分配要求接口的 IPv4 地址处于 IPv4 地址段子网范围内。若非如此，接口不会分配任何 IPv4 地址。

- **启用 (Enable)**

指定是否会使用此 IPv4 地址段。

说明

如果启用 IPv4 地址段，在此 DHCP 选项卡和其它 DHCP 选项卡中的设置将呈灰显状态，不能进行编辑。

- **子网 (Subnet)**

输入要分配给设备的网络地址范围。使用 CIDR 表示法。

- **低位 IP 地址 (Lower IP address)**

输入用于指定动态 IPv4 地址段起始的 IPv4 地址。此 IPv4 地址必须处于为“子网”(Subnet) 组态的网络地址范围内。

5.4 “System”菜单

- **高位 IP 地址 (Upper IP address)**

输入用于指定动态 IPv4 地址段结束的 IPv4 地址。此 IPv4 地址必须处于为“子网”(Subnet) 组态的网络地址范围内。

- **租用时间 (秒) (Lease Time (sec))**

指定分配的 IPv4 地址保持有效的秒数。当有效时间段一半过后，DHCP 客户端可延长所分配 IPv4 地址的有效时间。当整个时间段过期后，DHCP 客户端需要请求新的 IPv4 地址。

步骤

全局启用 DHCP 服务器

1. 选择“DHCP 服务器”(DHCP Server) 复选框。
2. 单击“设置值”(Set Values) 按钮。

创建 DHCP 池

1. 单击“创建”(Create) 按钮。
2. 选择 VLAN IP 接口。
3. 输入子网、低位和高位 IPv4 地址。
4. 输入租用时间。
5. 单击“设置值”(Set Values) 按钮。

在“端口范围”(Port Range) 选项卡中，将启用当前属于所选 VLAN 的所有端口。

池的标准选项在“DHCP 选项”(DHCP Options) 选项卡中创建。

6. 在 DHCP 选项卡中，完成池所需的设置。
7. 选中此选项卡上的“启用”(Enable) 复选框。

删除 DHCP 池

说明

只能删除未启用的条目。

1. 启用要删除的行中的“选中”(Select) 复选框。

对所有要删除的条目重复此步骤。

2. 单击“删除”(Delete) 按钮。

删除了相关条目。

5.4.8.3 端口范围 (Port Range)

在此页面上，定义用来分配地址段内 IPv4 地址的端口。

在“DHCP 服务器”(DHCP Server) 选项卡中创建 IPv4 地址段后，此选项卡中将创建一个新行，并且会选择当前位于相应 VLAN 中的所有端口。如果您稍后向 VLAN 添加端口，则在此选项卡中不会自动启用这些端口。

Pool ID	Interface	All ports	P0.1	P0.2	P0.3	P0.4
1	vlan1	No Change	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

说明

该表包含以下各列：

- **池 ID (Pool ID)**
显示 IPv4 地址段编号。为每个地址段创建一行。
- **接口 (Interface)**
显示分配的 VLAN IP 接口。
- **所有端口 (All ports)**
从下拉列表中选择设置。可选择以下设置选项：
 - 启用 (Enabled)
为相关 VLAN 的所有端口启用该复选框。
 - 禁用 (Disabled)
为相关 VLAN 的所有端口禁用该复选框。
 - 无变化 (No Change)
表保持不变。

5.4 “System”菜单

- P.x.y

指定将用于分配地址段的 IPv4 地址的端口。

只能选择位于相应 VLAN 内的端口。

步骤

组态各个端口

1. 启用或禁用所需端口的复选框。
2. 单击“设置值”(Set Values) 按钮。

组态所有端口

1. 在“所有端口”(All ports) 下拉列表中选择所需条目。
2. 单击“设置值”(Set Values) 按钮。

5.4.8.4 DHCP 选项

在此页面上指定 DHCP 服务器支持的 DHCP 选项。RFC 2132 中定义了各种 DHCP 选项。

创建 IPv4 地址段后，会自动创建 DHCP 选项 1、3、6、66 和 67。除了 DHCP 选项 1 以外，其它选项均可被删除。在使用 DHCP 选项 1 时，将自动设置您针对“DHCP 服务器”(DHCP Server) 中的地址段输入的子网掩码。在使用 DHCP 选项 3 时，可使用复选框将设备的内部 IPv4 地址设置为 DHCP 参数。

Dynamic Host Configuration Protocol (DHCP) Options

DHCP Client	DHCP Server	Port Range	DHCP Options	Relay Agent Information	Static Leases
Pool ID: 1 ▾					
Option Code: <input style="width: 150px;" type="text"/>					
Select	Pool ID	Option Code	Description	Use Interface IP	Value
<input type="checkbox"/>	1	1	Subnet Mask		255.255.255.0
<input type="checkbox"/>	1	3	Router	<input type="checkbox"/>	0.0.0.0
<input type="checkbox"/>	1	6	Domain Name Server		0.0.0.0
<input type="checkbox"/>	1	66	TFTP Server Name		
<input type="checkbox"/>	1	67	Bootfile Name		.
5 entries.					
<input type="button" value="Create"/> <input type="button" value="Delete"/> <input type="button" value="Set Values"/> <input type="button" value="Refresh"/>					

说明

该页面包含以下框：

- **池 ID (Pool ID)**

选择所需的 IPv4 地址段。

- **选项代码 (Option Code)**

输入所需 DHCP 选项的编号。RFC 2132 中定义了各种 DHCP 选项。下段列出了所支持的 DHCP 选项。

该表格包括以下列：

- **选择 (Select)**

选中要删除的行中的复选框。

- **池 ID (Pool ID)**

显示 IPv4 地址段编号。

- **选项代码 (Option Code)**

显示 DHCP 选项的编号。

- **说明 (Description)**

显示 DHCP 选项的说明。

- **使用接口 IP (Use interface IP)**

如果启用该复选框，则会将 IPv4 地址用作分配给 VLAN IP 地址的默认网关。如果禁用该复选框，则可以输入 IPv4 地址。

5.4 “System”菜单

- **值 (Value)**

输入要传输至 DHCP 客户端的 DHCP 参数。内容取决于 DHCP 选项。

- DHCP 选项 3（默认网关）：

输入一个 DHCP 参数作为 IPv4 地址，例如 192.168.100.2。

- DHCP 选项 6 (DNS):

输入一个 DHCP 参数作为 IPv4 地址，例如 192.168.100.2。可指定最多三个 IPv4 地址，地址之间以逗号分隔。

- DHCP 选项 12（主机名称）

以字符串格式输入主机名称。

- DHCP 选项 66（TFTP 服务器）：

输入一个 DHCP 参数作为 IPv4 地址，例如 192.168.100.2。

- DHCP 选项 67（引导文件名称）

以字符串格式输入引导文件的名称。

支持的 DHCP 选项

支持以下 DHCP 选项：

- 选项 1
- 选项 3
- 选项 6
- 选项 12
- 选项 66
- 选项 67

步骤

创建 DHCP 选项

1. 选择一个池 ID
2. 输入选项代码。
3. 单击“创建”(Create) 按钮。
4. 输入一个值。

5. 如果适用于选项 3，则启用“使用接口 IP”(Use Interface IP) 复选框。
6. 单击“设置值”(Set Values) 按钮。

删除 DHCP 选项

1. 启用要删除的行中的“选中”(Select) 复选框。

对所有要删除的条目重复此步骤。

2. 单击“删除”(Delete) 按钮。

删除了相关条目。

5.4.8.5 中继代理信息

在此页面上定义,为具有某远程 ID 和电路 ID 的设备分配来自特定地址段的 IPv4 地址。

如果您为某个地址段创建此类条目，则相应地址段的端口仅通过 DHCP 中继代理（选项 82）响应 DHCP 查询。可为相同的 VLAN IP 接口创建更多地址段，以使端口响应不同请求。

说明

扩展或释放通过中继代理分配的 IPv4 地址。

服务器将忽略通过中继代理“Renew”和“Release”消息（直接从 DHCP 客户端发送到 DHCP 服务器）实现的地址分配。

- 使用由客户端以广播形式自动发送的“Rebinding”消息，可延长通过中继代理分配的 IPv4 地址的有效时间段。
- 要加快通过中继代理分配的 IPv4 地址的释放速度，可组态较短的有效周期。

Relay Agent Information

DHCP Client	DHCP Server	Port Range	DHCP Options	Relay Agent Information	Static Leases
-------------	-------------	------------	--------------	-------------------------	---------------

Pool ID:

Remote ID:

Circuit ID:

Select	Pool ID	Remote ID	Circuit ID
<input type="checkbox"/>	1	Switch	7

1 entry.

5.4 “System”菜单

说明

该页面包含以下框：

- **池 ID (Pool ID)**

选择所需的 IPv4 地址段。

- **远程 ID (Remote ID)**

输入远程 ID。

- **电路 ID (Circuit ID)**

输入电路 ID。

该表格包括以下列：

- **选择 (Select)**

选中要删除的行中的复选框。

- **池 ID (Pool ID)**

显示 IPv4 地址段编号。

- **远程 ID (Remote ID)**

显示远程 ID。

- **电路 ID (Circuit ID)**

显示电路 ID。

步骤

创建条目

1. 选择一个池 ID。
2. 输入远程 ID。
3. 输入电路 ID。
4. 单击“创建”(Create) 按钮。

删除一个条目

1. 启用要删除的行中的“选中”(Select) 复选框。

对所有要删除的条目重复此步骤。

2. 单击“删除”(Delete) 按钮。

删除了相关条目。

5.4.8.6 静态租用

在此页面上定义，根据 DHCP 客户端的客户端 ID 或 MAC 地址为其分配一个预设的 IPv4 地址。

Static Leases

DHCP Client
DHCP Server
Port Range
DHCP Options
Relay Agent Information
Static Leases

Pool ID:

Client Identification Method:

Value:

Select	Pool ID	Identification Method	Value	IP Address
<input type="checkbox"/>	2	Client ID	65756767	0.0.0.0

1 entry.

说明

该页面包含以下框：

- **池 ID (Pool ID)**
选择所需的 IPv4 地址段。
- **客户端标识方法 (Client identification method)**
选择用于标识客户端的方法。
 - Ethernet MAC
客户端按照其 MAC 地址进行标识。
 - 客户端 ID (Client ID)
客户端按照自由定义的 DHCP 客户端 ID 进行标识。

5.4 “System”菜单

- **值 (Value)**

输入客户端的 MAC 地址 (Ethernet MAC) 或客户端 ID。

该表格包括以下列：

- **选择 (Select)**

选中要删除的行中的复选框。

- **池 ID (Pool ID)**

显示 IPv4 地址段编号。

- **标识方法 (Identification method)**

显示客户端是根据其 MAC 地址还是客户端 ID 进行标识。

- **值 (Value)**

显示客户端的 MAC 地址或客户端 ID。

- **IP 地址 (IP Address)**

指定将分配给客户端的 IPv4 地址。IPv4 地址必须在 IPv4 地址段范围内。

步骤

创建静态租用

1. 选择一个池 ID。
2. 选择客户端标识方法。
3. 输入值。
4. 单击“创建”(Create) 按钮。
5. 指定将分配给客户端的 IPv4 地址。
6. 单击“设置值”(Set Values) 按钮。

删除静态租用

1. 启用要删除的行中的“选中”(Select) 复选框。
对所有要删除的条目重复此步骤。
2. 单击“删除”(Delete) 按钮。
删除了相关条目。

5.4.9 SNMP

也可参见“技术基础”章节的“SNMP (页 43)”部分。

5.4.9.1 常规

SNMP 组态

在该页面对 SNMP 进行基本设置。根据希望应用的功能启用相应的复选框。

Simple Network Management Protocol (SNMP) General

General Traps v3 Groups v3 Users

SNMP: SNMPv1/v2c/v3

SNMPv1/v2c Read Only

SNMPv1/v2c Read Community String: public

SNMPv1/v2c Read/Write Community String: private

SNMPv1 Traps

SNMPv1/v2c Trap Community String: public

SNMPv3 User Migration

SNMP Engine ID: 80.00.10.e9.05.00.1b.1b.40.91.23

Set Values Refresh

说明

该页面包含以下框：

- **SNMP**

从下拉列表中选择 SNMP 协议。可能的设置如下：

- “-”（禁用）
禁用 SNMP。
- SNMPv1/v2c/v3
支持 SNMPv1/v2c/v3。

说明

注意版本 1 和 2c 的 SNMP 不包含任何安全机制。

- SNMPv3
仅支持 SNMPv3。

- **SNMPv1/v2c Read-Only**

如果启用此选项，则 SNMPv1/v2c 仅可读取 SNMP 变量。

说明

团体字符串

由于安全考虑，请勿使用标准值“public”或“private”。请在初始安装之后更改团体字符串。

- **SNMPv1/v2c Read Community String**

输入框输入 SNMP 协议的读访问团体字符串。

- **SNMPv1/v2c Read/Write Community String**

输入 SNMP 协议的读写访问团体字符串。

- **SNMPv1 陷阱 (SNMPv1 Traps)**

启用或禁用发送 SNMPv1 陷阱（报警帧）。在“陷阱”(Trap) 选项卡上，指定 SNMPv1 陷阱将发送到的设备的 IP 地址。

- **SNMPv1/v2c Trap Community String**

输入用于发送 SNMPv1/v2c 消息的团体字符串。

- **SNMPv3 用户移植 (SNMPv3 User Migration)**

- 已启用

如果启用该功能，会生成一个可移植的 SNMP 引擎 ID。可以将已组态的 SNMPv3 用户传送至不同的设备。

如果启用该功能并将设备的组态加载到另一个设备，将保留组态的 SNMPv3 用户。

- 已禁用

如果禁用该功能，会生成一个设备特定的 SNMP 引擎 ID。要生成此 ID，需要使用设备的代理 MAC 地址。不得将此 SNMP 用户组态传送至其他设备。

如果将设备的组态加载到另一个设备，将删除所有组态的 SNMPv3 用户。

- **SNMP 引擎 ID (SNMP Engine ID)**

显示 SNMP 引擎 ID。

步骤

1. 从“SNMP”下拉列表中选择所需选项：
 - “-”（禁用）
 - SNMPv1/v2c/v3
 - SNMPv3
2. 只有希望使用 SNMPv1/v2c 对 SNMP 变量进行读访问时才启用“SNMPv1/v2c 只读”(SNMPv1/v2c Read Only) 复选框。
3. 在“SNMPv1/v2c Read Community String”输入框中输入所需字符串。
4. 在“SNMPv1/v2c Read/Write Community String”输入框中输入所需字符串。
5. 如有必要，可以启用“SNMPv3 用户移植”(SNMPv3 User Migration)。
6. 单击“Set Values”按钮。

5.4.9.2 陷阱

报警事件的 SNMP 陷阱

如果发生报警事件，设备最多可同时向十个不同的管理站发送 SNMP 陷阱（报警帧）。仅当“系统 > 事件”(System > Events) 菜单中指定的事件发生时，才会发送陷阱。

说明

只有已启用“常规”(General) 选项卡或“系统 > 组态”(System > Configuration) 中的选项“SNMPv1 陷阱”(SNMPv1 Traps) 时，才会发送陷阱。

说明

- **陷阱接收方地址 (Trap Receiver Address)**
输入设备发送 SNMP 陷阱的目标站 IP 地址。最多可指定十个不同的接收方服务器。

该表格包括以下列：

- **选择 (Select)**
选择要删除的行。
- **陷阱接收方地址 (Trap Receiver Address)**
如有必要，请更改站的 IP 地址。
- **陷阱 (Trap)**
启用或禁止发送陷阱。已输入但未激活的工作站不会接收 SNMP 陷阱。

步骤

创建陷阱条目

1. 在“陷阱接收方地址”(Trap Receiver Address) 中，输入设备发送陷阱的目标站的 IP 地址。
2. 单击“创建”(Create) 按钮创建新的陷阱条目。
3. 选中所需行中的“陷阱”(Trap)。
4. 单击“设置值”(Set Values) 按钮。

删除陷阱条目

1. 启用要删除的行中的“选择”(Select)。
2. 单击“删除”(Delete) 按钮。删除了相关条目。

5.4.9.3 组

安全设置和权限分配

SNMP 版本 3

允许在协议级分配权限，以及身份验证和加密。安全等级和读/写权限按照组来分配。这些设置会自动应用到组内的每个成员。

Simple Network Management Protocol (SNMP) v3 Groups

General
Traps
v3 Groups
v3 Users

Group Name:

Security Level: no Auth/no Priv ▼

Select	Group Name	Security Level	Read	Write	Persistence
<input type="checkbox"/>	maintenance	no Auth/no Priv	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	no
<input type="checkbox"/>	service	Auth/no Priv	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	no

2 entries.

Create
Delete
Set Values
Refresh

说明

该页面包含以下框：

- **Group Name**
输入组名称。最大长度为 32 个字符。
- **安全等级 (Security Level)**
选择对所选组有效的安全等级（验证、加密）。可选择以下安全等级：
 - no Auth/no Priv
启用验证/未启用加密。
 - Auth/no Priv
启用验证/未启用加密。
 - Auth/Priv
已启用验证/已启用加密。

该表格包括以下列：

- **Select**
选择要删除的行。
- **Group Name**
显示定义的组名称。

5.4 “System”菜单

- **Security Level**
显示组态的安全等级。
 - **Read**
启用或禁用所需组的读访问。
 - **Write**
启用或禁用所需组的写访问。
-

说明

要实现写访问，还需启用读访问。

- **Persistence**
显示组是否已分配至 **SNMPv3** 用户。如果组未分配至 **SNMPv3** 用户，则不会触发自动保存，并且在重启设备之后会删除该组态的组。
 - 是 (Yes)
组已分配至 **SNMPV3** 用户。
 - 否 (No)
组未分配至 **SNMPV3** 用户。

步骤

创建新组

1. 在“Group Name”中输入所需的组名称。
2. 从“Security Level”下拉列表中选择所需安全等级。
3. 单击“Create”按钮以创建新条目。
4. 在“Read”中为组指定所需的读权限。
5. 在“Write”中为组指定所需的写权限。
6. 单击“Set Values”按钮。

修改组

1. 在“Read”中为组指定所需的读权限。
2. 在“Write”中为组指定所需的写权限。
3. 单击“Set Values”按钮。

说明

指定了组名称和安全等级之后，在组创建之后再无法对其进行修改。如果要更改组名称或安全等级，将必须删除该组并重新创建，然后重新指定新名称。

删除组

1. 启用要删除的行中的“Select”。
对所有要删除的组重复此步骤。
2. 单击“Delete”按钮。将删除相关条目。

5.4.9.4 用户 (Users)

用户特定的安全设置

在 WBM 页上，可以创建新的 SNMPv3

用户以及修改或删除现有用户。基于用户的安全模型采用用户名概念；换言之，所有帧中都会加入用户 ID。发送方和接收方均会检查此用户名和适用的安全设置。

Simple Network Management Protocol (SNMP) v3 Users

General Traps v3 Groups v3 Users

User Name:

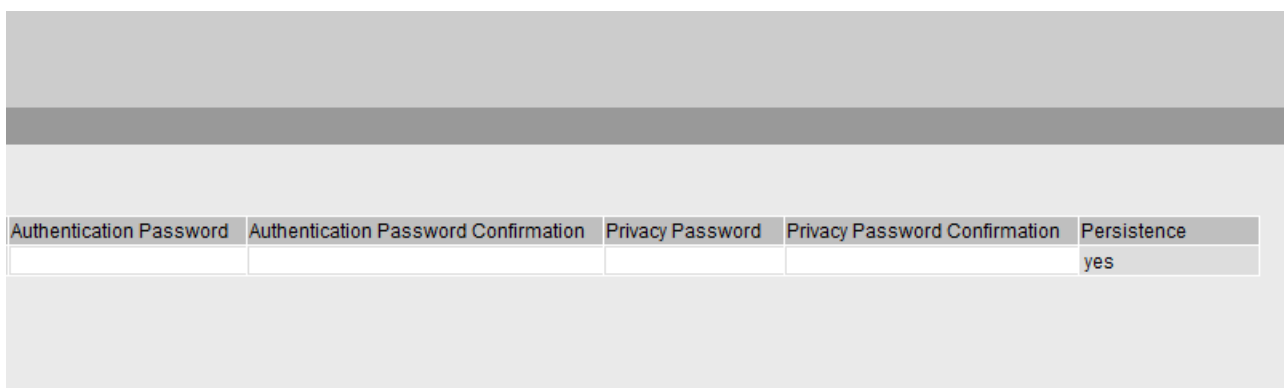
Select	User Name	Group Name	Authentication Protocol	Privacy Protocol
<input type="checkbox"/>	Miller	Service	MD5	DES

1 entry.

Create Delete Set Values Refresh

图 5-5 SNMPv3 用户 - 表的第一部分

5.4 “System”菜单



Authentication Password	Authentication Password Confirmation	Privacy Password	Privacy Password Confirmation	Persistence
				yes

图 5-6 802.1X 用户 - 表的第二部分

说明

该页面包含以下框：

- **User Name**

输入可自由选择的用户名。输入相关数据之后，不可以再修改该名称。

该表格包括以下列：

- **Select**

选择要删除的行。

- **User Name**

显示已创建的用户。

- **Group Name**

选择待分配用户的组。

- **验证协议 (Authentication Protocol)**

指定验证协议以为其存储密码。

可使用以下设置：

- None
- MD5
- SHA

- **加密协议 (Encryption Protocol)**

指定是否应为使用 DES 算法的加密存储密码。仅在已选择验证协议后方可启用。

- **Authentication Password**

在第一个输入框中输入身份验证密码。该密码必须至少 6 个字符，最多 32 个字符。

- **Authentication Password Confirmation**
重复输入以确认密码。
- **Privacy Password**
输入加密密码。该密码必须至少 6 个字符，最多 32 个字符。
- **Privacy Password Confirmation**
再次输入加密密码以进行确认。
- **Persistence**
显示用户是否已分配至 SNMPv3 组。如果用户未分配至 SNMPv3 组，则不会触发自动保存，并且在重启设备之后会删除该组态的用户。
 - Yes
用户已分配至 SNMpv3 组。
 - No
用户未分配至 SNMpv3 组。

步骤

创建新用户

1. 在“User Name”输入框中输入新用户的名称。
2. 单击“Create”按钮。会在表中生成一个新条目。
3. 在“Group Name”中，选择新用户将所属的组。
如果尚未创建组，则切换至“v3 Groups”页面并对该组进行设置。
4. 如果有必要对所选的组进行身份验证，请从“Authentication Protocol”中选择身份验证算法。
在相关输入框中，输入身份验证密码并确认。
5. 如果已为该组指定了加密，请从“Privacy Protocol”中选择算法。在相应的输入框中，输入加密密码和确认密码。
6. 单击“Set Values”按钮。

删除用户

1. 启用要删除的行中的“Select”。
对所有要删除的用户重复此步骤。
2. 单击“Delete”按钮。删除了相关条目。

5.4.10 系统时间 (System Time)

可以采用不同的方法来设置设备的系统时间。每次只能采用一种方法。
激活一种方法后，将自动禁止之前激活的方法。

5.4.10.1 手动设置 (Manual Setting)

手动设置系统时间

在此页面上设置系统本身的日期和时间。要使用此设置，请启用“手动设置时间”(Time Manually)。

The screenshot shows the 'Manual System Time Setting' web page. At the top, there is a navigation bar with tabs: 'Manual Setting' (selected), 'DST Overview', 'DST Configuration', 'SNTP Client', 'NTP Client', and 'SIMATIC Time Client'. Below the navigation bar, the 'Time Manually' checkbox is checked. The 'System Time' field displays '01/01/2000 00:39:58'. There is a 'Use PC Time' button. Below this, the 'Last Synchronization Time' is 'Date/time not set', the 'Last Synchronization Mechanism' is 'Not set', and the 'Daylight Saving Time' is 'inactive (offset + 0h)'. At the bottom, there are 'Set Values' and 'Refresh' buttons.

说明

该页面包含以下框：

- **手动设置时间 (Time Manually)**
启用或禁用手动时间设置。如果启用该选项，则可以编辑“System Time”输入框。
- **系统时间 (System Time)**
按“MM/DD/YYYY HH:MM:SS”格式输入日期和时间。
重启之后，时钟从 01/01/2000 00:00:00 开始。
- **使用 PC 时间 (Use PC Time)**
单击该按钮以使用 PC 的时间设置。
- **上次同步时间 (Last Synchronization Time)**
显示上一次发生时钟同步的时间。如果无法进行时钟同步，该框会显示“Date/time not set”。

- **上次同步机制 (Last Synchronization Mechanism)**
显示上次时钟同步的执行方式。
 - 未设置 (Not set)
未设置时间。
 - 手动 (Manual)
手动设置时间
 - SNTP
使用 SNTP 自动进行时钟同步
 - NTP
使用 NTP 自动进行时钟同步
 - SIMATIC
使用 SIMATIC 时钟帧自动进行时钟同步
- **夏令时 (DST) (Daylight Saving Time (DST))**
显示夏令时切换是否已激活。
 - active (offset +1 h)

系统时间已更改为夏令时；即增加了一小时。您可在 WBM 选择区域的顶部看到当前系统时间。

设置的时间继续在“系统时间”(System Time) 框中显示。
 - inactive (offset +0 h)
不会更改当前系统时间。

步骤

1. 启用“手动设置时间”(Time Manually) 选项。
2. 在“系统时间”(System Time) 输入框中，按“MM/DD/YYYY HH:MM:SS”格式输入日期和时间。
3. 单击“设置值”(Set Values) 按钮。
将采用该日期和时间，并在“上次同步机制”(Last Synchronization Mechanism) 框中输入“手动”(Manual)。

5.4 “System”菜单

5.4.10.2 DST 概述

在此页面中，您可以创建新的夏令时切换条目。

该表显示了现有条目的概览。

设置

Daylight Saving Time (DST) Overview								
Manual Setting DST Overview DST Configuration SNTP Client NTP Client SIMATIC Time Client								
Select	DST No.▲	Name	Year	Start Date	End Date	Recurring Date	State	Type
<input type="checkbox"/>	1	CEST	-	03/26 02:00	10/29 03:00	Last Sunday March 02 Last Sunday October 03	enabled	Recurring
<input type="checkbox"/>	2	DST 2017	2017	03/30 02:00	11/15 03:00	-	enabled	Date

2 entries.

- **选择 (Select)**

选择要删除的行。

- **DST 编号 (DST No.)**

显示条目编号。

如果创建新的条目，会创建一个带有唯一编号的新行。

- **名称 (Name)**

显示条目名称。

- **年 (Year)**

显示条目的创建年份。

- **起始日期 (Start Date)**

显示夏令时的起始月、日和时间。

- **结束日期 (End Date)**

显示夏令时的结束月、日和时间。

- **重复日期 (Recurring Date)**

对于“规则”(Recurring)

类型的条目，将显示夏令时激活的时间段，其中包括周、日、月和时钟。

对于“日期”(Date) 类型的条目，将显示“-”。

- **状态 (State)**

显示条目的状态:

- 启用 (Enabled)

条目已正确创建。

- 无效 (Invalid)

新建条目，但起始和结束日期完全相同。

- **类型 (Type)**

显示如何进行夏令时切换:

- 日期 (Date)

输入固定日期作为夏令时切换的时间。

- 规则 (Recurring)

定义夏令时切换的规则。

步骤

创建条目

1. 单击“创建”(Create) 按钮。

随即会在表中创建一个新条目。

2. 单击“DST 编号”(DST No) 列中所需的条目。

切换到“DST 组态”(DST Configuration) 页面。

3. 从“类型”(Type) 下拉列表中选择所需的类型。

根据选择的类型，将提供各种设置。

4. 在“名称”(Name) 框中输入一个名称。

5. 如果已选择类型“日期”(Date)，则填写以下框。

- 年

- 日（对于起始日期和结束日期）

- 小时（对于起始日期和结束日期）

- 月（对于起始日期和结束日期）

5.4 “System”菜单

6. 如果已选择类型“规则”(Rule)，则填写以下框。

- 小时（对于起始日期和结束日期）
- 月（对于起始日期和结束日期）
- 周（对于起始日期和结束日期）
- 日（对于起始日期和结束日期）

7. 单击“设置值”(Set Values) 按钮。

删除条目

1. 启用要删除的行中的“选择”(Select)。
2. 单击“删除”(Delete) 按钮。删除了相关条目。

5.4.10.3 DST 组态 (DST Configuration)

在此页面中，您可以组态夏令时切换条目。切换到夏令时或标准时间后，可以按当地时区正确设置系统时间。

可定义夏令时切换规则，也可指定固定日期。

设置

说明

此页面包含的内容取决于您在“类型”(Type) 框中做出的选择。

始终都会显示“DST 编号”(DST No.)、“类型”(Type) 和“名称”(Name) 框。

- **DST 编号 (DST No.)**

选择条目的类型。

- **类型 (Type)**

选择夏令时切换方式：

- **日期 (Date)**

您可以设置固定日期作为夏令时切换的时间。

此设置适用于没有夏令时切换管理规则的地区。

- **规则 (Rule)**

可以定义夏令时切换的规则。

此设置适用于夏令时起始和结束日期始终为特定工作日的地区。

- **名称 (Name)**

输入条目名称。

名称最长为 16 个字符。

选择“日期”(Date) 时的设置

DST Configuration

Manual Setting | DST Overview | DST Configuration | SNTP Client | NTP Client | SIMATIC Time Client

DST No: 2

Type: Date

Name: DST 2017

Year: 2017

Start Date

Day: 30

Hour: 02:00

Month: March

End Date

Day: 15

Hour: 03:00

Month: November

Set Values Refresh

可设置夏令时开始和结束的固定日期。

- **年 (Year)**

输入夏令时切换的年份。

- **起始日期 (Start Date)**

输入以下值作为夏令时的起点：

- **日 (Day)**

指定日期。

- **时 (Hour)**

指定小时。

- **月 (Month)**

指定月份。

5.4 “System”菜单

- **结束日期 (End Date)**

输入以下值作为夏令时的终点：

- 日 (Day)
指定日期。
- 时 (Hour)
指定小时。
- 月 (Month)
指定月份。

选择“角色”(Recurring) 时的设置

DST Configuration

Manual Setting | DST Overview | DST Configuration | SNTP Client | NTP Client | SIMATIC Time Client

DST No: 1

Type: Recurring

Name: DST 2016

Start Date End Date

Hour: 00:00 Hour: 00:00

Month: September Month: September

Week: Third Week: Fourth

Day: Monday Day: Tuesday

Set Values Refresh

可以创建夏令时切换规则。

- **起始日期 (Start Date)**

输入以下值作为夏令时的起点：

- 时 (Hour)
指定小时。
- 月 (Month)
指定月份。

- 周 (Week)

指定周。

可以选择月中的第 1 周到第 4 周或最后一周。

- 日 (Day)

指定工作日。

- **结束日期 (End Date)**

输入以下值作为夏令时的终点：

- 时 (Hour)

指定小时。

- 月 (Month)

指定月份。

- 周 (Week)

指定周。

可以选择月中的第 1 周到第 4 周或最后一周。

- 日 (Day)

指定工作日。

5.4.10.4 SNTP 客户端 (SNTP Client)

网络中的时间同步

SNTP (Simple Network Time Protocol) 用于在网络中同步时间。SNTP 服务器在网络中发送适当的帧。

说明

为避免时间跳跃，需确保网络中只有一台时间服务器。

Simple Network Time Protocol (SNTP) Client

Manual Setting | DST Overview | DST Configuration | **SNTP Client** | NTP Client | SIMATIC Time Client

SNTP Client

Current System Time: 01/01/2000 00:47:41

Last Synchronization Time: Date/time not set

Last Synchronization Mechanism: Not set

Time Zone: +00:00

Daylight Saving Time: inactive (offset + 0h)

SNTP Mode: Listen ▼

Set Values Refresh

说明

该页面包含以下框：

- **SNTP 客户端 (SNTP Client)**
启用或禁用使用 SNTP 自动进行时钟同步。
- **当前系统时间 (Current System Time)**
显示从服务器接收的当前日期和当前标准时间。如果指定了时区，则会相应调整时间信息。
- **上次同步时间 (Last Synchronization Time)**
显示上一次时钟同步发生的时间。

- **上次同步机制 (Last Synchronization Mechanism)**

显示上次时钟同步的执行方式。可能的方法如下：

- 未设置 (Not set)
未设置时间。
- 手动 (Manual)
手动设置时间
- SNTP
使用 SNTP 自动进行时钟同步
- NTP
使用 NTP 自动进行时钟同步
- SIMATIC
使用 SIMATIC 时钟帧自动进行时钟同步

- **时区 (Time Zone)**

在此框中，以“+/- HH:MM”的格式输入所使用的时区。时区与 UTC 标准世界时间相关。

相应调整“当前系统时间”(Current System Time) 框中的时间。

- **夏令时 (DST) (Daylight Saving Time (DST))**

显示夏令时切换是否已激活。

- active (offset +1 h)
系统时间已更改为夏令时；即增加了一小时。您可在 WBM 选择区域的顶部看到当前系统时间。
“当前系统时间”(Current System Time) 框将继续显示包括时区在内的标准时间。
- inactive (offset +0 h)
不会更改当前系统时间。

- **SNTP 模式 (SNTP Mode)**

从下拉列表中选择同步模式。可以使用下列同步类型：

- Listen
在该模式下，设备处于被动状态，且会接收传递时钟的 SNTP 帧。
- Poll
如果选择该模式，则会显示输入框“SNTP 服务器地址”(SNTP Server Address)、“SNTP 服务器端口”(SNTP Server Port) 和“轮询间隔[s]”(Poll Interval[s])，以便进一步进行组态。若使用该同步类型，设备会激活，并向 SNTP 服务器发送时间查询。

5.4 “System”菜单

- **SNTP 服务器地址 (SNTP Server Address)**
输入 SNTP 服务器的 IP 地址。
- **SNTP 服务器端口 (SNTP Server Port)**
输入 SNTP 服务器的端口。
可用的端口如下：
 - 123 (标准端口)
 - 1025 到 36564
- **轮询间隔[s] (Poll Interval[s])**
在此输入两次时间查询间的时间间隔。在此框中输入查询间隔的秒数值。可能的值介于 16 到 16284 秒之间。

步骤

1. 单击“SNTP 客户端”(SNTP Client) 复选框以启用自动时间设置。
2. 在“时区”(Time Zone) 输入框中输入当地时间与世界时间 (UTC) 的时差。由于 SNTP 服务器始终发送 UTC 时间，因此输入格式为“+/-HH:MM”（例如，对于 CEST 是 +02:00）。该时间随后会被重新计算并根据指定的时区显示为当地时间。在设备本身不会将夏令时转换为标准时间。在“时区”(Time Zone) 输入框输入时，还需要考虑到这一点。
3. 从“SNTP 模式”(SNTP Mode) 下拉列表中选择下列选项之一：
 - Listen
对于该模式，需要组态以下内容：
 - 与服务器发送的时间之间的时差（第 2 步）
 - 通过第 7 步完成组态。
 - Poll
单击“设置值”(Set Values) 按钮。将显示有关 SNTP 模式“Poll”的更多选择框。
对于该模式，需要组态以下内容：
 - 与服务器发送的时间之间的时差（第 2 步）
 - 时间服务器（第 4 步）
 - 端口（第 5 步）
 - 查询间隔（第 6 步）
 - 通过第 7 步完成组态。
4. 在“SNTP 服务器地址”(SNTP Server Address) 输入框中，输入 SNTP 服务器的 IPv4 地址，该服务器的帧将用于同步时钟。

5. 在“SNTP 服务器端口”(SNTP Server Port) 输入框中，输入可用来使用 SNTP 服务器的端口。仅当输入 SNTP 服务器的 IPv4 地址之后，才可以修改该端口。
6. 在“轮询间隔[s]”(Poll Interval[s]) 输入框中，输入以秒表示的时间值，经过这段时间后，会向时间服务器发送新的时间查询。
7. 单击“设置值”(Set Values) 按钮将更改传输到设备。

5.4.10.5 NTP 客户端 (NTP Client)

使用 NTP 自动设置时钟

如果需要使用 NTP 进行时钟同步，可以在此做相关设置。

说明

为避免时间跳跃，需确保网络中只有一台时间服务器。

Network Time Protocol (NTP) Client

Manual Setting | DST Overview | DST Configuration | SNTP Client | **NTP Client** | SIMATIC Time Client

NTP Client

Current System Time: 01/01/2000 00:51:53

Last Synchronization Time: Date/time not set

Last Synchronization Mechanism: Not set

Time Zone: +00:00

Daylight Saving Time: inactive (offset + 0h)

NTP Server Address: 0.0.0.0

NTP Server Port: 123

Poll Interval[s]: 64

Set Values Refresh

说明

该页面包含以下框：

- **NTP 客户端 (NTP Client)**

选中此复选框可启用使用 NTP 自动进行时钟同步。

- **当前系统时间 (Current System Time)**

显示由工业以太网交换机接收的当前日期和当前标准时间。如果指定了时区，则会相应调整时间信息。

- **上次同步时间 (Last Synchronization Time)**

显示上一次发生时钟同步的时间。

- **上次同步机制 (Last Synchronization Mechanism)**

显示上次时钟同步的执行方式。可能的方法如下：

- 未设置 (Not set)

未设置时间。

- 手动 (Manual)

手动设置时间

- SNTP

使用 SNTP 自动进行时钟同步

- NTP

使用 NTP 自动进行时钟同步

- SIMATIC

使用 SIMATIC 时钟帧自动进行时钟同步

- **时区 (Time Zone)**

在此框中，以“+/- HH:MM”的格式输入所使用的时区。时区与 UTC 标准世界时间相关。

相应调整“当前系统时间”(Current System Time) 框中的时间。

- **夏令时 (DST) (Daylight Saving Time (DST))**

显示夏令时切换是否已激活。

 - active (offset +1 h)

系统时间已更改为夏令时；即增加了一小时。您可在 WBM 选择区域的顶部看到当前系统时间。

“当前系统时间”(Current System Time) 框将继续显示包括时区在内的标准时间。
 - inactive (offset +0 h)

不会更改当前系统时间。
- **NTP 服务器地址 (NTP Server Address)**

输入 NTP 服务器的 IPv4 地址。
- **NTP 服务器端口 (NTP Server Port)**

输入 NTP 服务器的端口。

可能的端口包括：

 - 123 (标准端口)
 - 1025 到 36564
- **轮询间隔[s] (Poll Interval[s])**

在此输入两次时间查询之间的时间间隔。在此框中输入查询间隔的秒数值。可能的值介于 64 到 1024 秒之间。

步骤

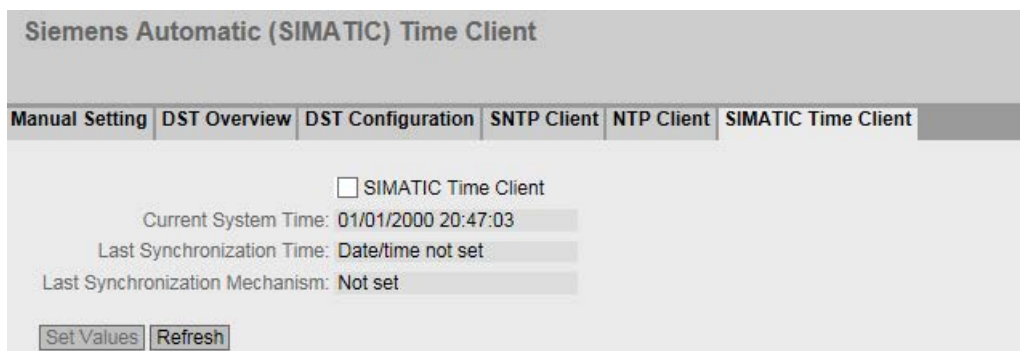
1. 单击“NTP 客户端”(NTP Client) 复选框，启用使用 NTP 自动进行时间设置。
2. 在以下框中输入需要的值：
 - 时区
 - NTP 服务器的 IPv4 地址
 - NTP 服务器端口
 - 查询间隔
3. 单击“设置值”(Set Values) 按钮。

5.4.10.6 SIMATIC Time Client

通过 SIMATIC 时间客户端设置时间

说明

为避免时间跳跃，需确保网络中只有一台时间服务器。



说明

该页面包含以下框：

- **SIMATIC Time Client**
选中此复选框可启用设备作为 SIMATIC 时间客户端。
- **当前系统时间 (Current System Time)**
显示当前系统时间。
- **上次同步时间 (Last Synchronization Time)**
显示上一次时钟同步发生的时间。
- **上次同步机制 (Last Synchronization Mechanism)**
显示上次时钟同步的执行方式。可能的方法如下：
 - 未设置 (Not set)
未设置时间。
 - 手动 (Manual)
手动设置时间
 - SNTP
使用 SNTP 自动进行时钟同步

- NTP
使用 NTP 自动进行时钟同步
- SIMATIC
使用 SIMATIC 时钟帧自动进行时钟同步

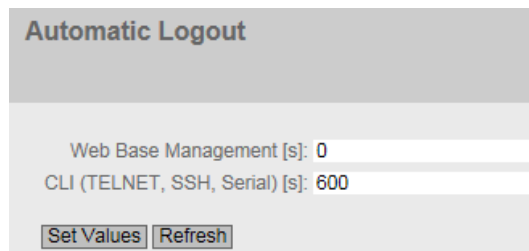
步骤

1. 单击“SIMATIC Time Client”复选框可启用 SIMATIC Time Client。
2. 单击“设置值”(Set Values) 按钮。

5.4.11 自动注销

设置自动注销

在该页面，设置从用户不活动后自动从 WBM 或 CLI 注销所需经过的时间间隔。
如果您已经自动注销，则需要再次登录。



Automatic Logout

Web Base Management [s]: 0

CLI (TELNET, SSH, Serial) [s]: 600

Set Values Refresh

组态

1. 在“基于 Web 的管理 [s]”(Web Based Management [s]) 输入框中输入一个 60 到 3600 秒之间的值。如果输入值 0，则禁用自动注销。
2. 在“CLI (TELNET, SSH, Serial) [s]”输入框中输入一个 60 到 600 秒之间的值。如果输入值 0，则禁用自动注销。
3. 单击“设置值”(Set Values) 按钮。

5.4 “System”菜单

5.4.12 按钮

按钮的可用性

根据您的工业以太网交换机，将提供不同的按钮和功能，请参见“系统功能硬件设备 (页 13)”。

按钮的功能

有关按钮功能的详细说明，请参见设备操作说明。

可在以下页面中启用或禁用该按钮的功能。




显示框说明

支持以下功能：

- **恢复出厂默认设置 (Restore Factory Defaults)**

如果选中该复选框，则可通过按钮执行功能“恢复出厂默认设置”(Restore Factory Defaults)。

 小心
<p>启动期间，按钮功能“恢复出厂默认设置”处于激活状态</p> <p>如果在组态中禁用此功能，则仅将在运行期间禁用。重启（例如断电后重启）时，在组态加载前此功能将处于激活状态，因而设备可能无意间被复位为出厂设置。这可能导致网络运行意外中断，因为设备需要进行重新组态。另外，插入的 PLUG 也会被删除并恢复至出厂时的状态。</p>

- **冗余管理器 (Redundancy Manager)**

如果选中该复选框，则可通过按钮激活或取消激活“冗余管理器”(Redundancy Manager) 功能。

- **设置故障屏蔽 (Set Fault Mask)**

如果选中该复选框，则可通过按钮定义故障屏蔽。

组态步骤

1. 要使用所需功能，请选中相应的复选框。
2. 单击“设置值”(Set Values) 按钮。

5.4.13 Syslog 客户端

按照 RFC 3164，Syslog 用于在 IP 网络中通过 UDP 传送简短的未加密文本消息。这需要一个 Syslog 服务器。

发送日志条目的要求

- 已在设备上启用 Syslog 功能。
- 已为相关事件启用 Syslog 功能。
- 网络中存在可接收日志条目的 Syslog 服务器。由于这是一个 UDP 连接，因此不会向发送方发送确认。
- 在设备中已输入 Syslog 服务器的 IP 地址。

System Logging (Syslog) Client

Syslog Client

Syslog Server Address:

Select	Syslog Server Address	Server Port
0 entries.		

5.4 “System”菜单

说明

该页面包含以下框：

- **Syslog 客户端 (Syslog Client)**
启用或禁用 Syslog 功能。
- **Syslog 服务器地址 (Syslog Server Address)**
输入 Syslog 服务器的 IP 地址。

该表包含以下各列

- **选择 (Select)**
选择要删除的行。
- **Syslog 服务器地址 (Syslog Server Address)**
显示 Syslog 服务器的 IP 地址。
- **服务器端口 (Server Port)**
输入要使用的 Syslog 服务器端口。

步骤

启用功能

1. 选择“Syslog 客户端”(Syslog Client) 复选框。
2. 单击“设置值”(Set Values) 按钮。

创建新条目

1. 在“Syslog 服务器地址”(Syslog Server Address) 输入框中，输入将保存日志条目的 Syslog 服务器的 IP 地址。
2. 单击“创建”(Create) 按钮。将在表中插入一个新行。
3. 在“服务器端口”(Server Port) 输入框中，输入服务器 UDP 端口的端口号。
4. 单击“设置值”(Set Values) 按钮。

说明

服务器端口的默认设置是 514。

更改条目

1. 删除条目。
2. 创建新条目。

删除条目

1. 选中要删除的行中的复选框。
2. 单击“删除”(Delete) 按钮。会删除所有选中的条目并刷新显示。

5.4.14 端口

5.4.14.1 概述

端口组态概述

此页面显示设备所有端口的数据传送组态。无法对该页面上的任何内容进行组态。

Ports Overview										
Overview Configuration										
Port	Port Name	Port Type	Status	OperState	Link	Mode	Negotiation	Flow Ctrl. Type	Flow Ctrl.	MAC Address
P0.1		Switch-Port VLAN Hybrid	enabled	up	up	100M FD	enabled	<input type="checkbox"/>	disabled	00-1b-1b-40-91-24
P0.2		Switch-Port VLAN Hybrid	enabled	up	up	100M FD	enabled	<input type="checkbox"/>	disabled	00-1b-1b-40-91-25
P0.3		Switch-Port VLAN Hybrid	enabled	down	down	100M FD	enabled	<input type="checkbox"/>	disabled	00-1b-1b-40-91-26
P0.4		Switch-Port VLAN Hybrid	enabled	down	down	100M FD	enabled	<input type="checkbox"/>	disabled	00-1b-1b-40-91-27

Refresh

显示框说明

该表格包括以下列：

- **端口 (Port)**
显示可用端口。如果单击该端口，相应组态页便会打开。端口由模块号和端口号组成，例如，端口 0.1 表示模块 0，端口 1。
- **端口名称 (Port Name)**
显示端口名称。

5.4 “System”菜单

- **端口类型 (Port Type)**

显示端口类型。可能的类型如下：

 - 交换机端口 VLAN 混合 (Switch Port VLAN Hybrid)
 - 交换机端口 VLAN 主干 (Switch Port VLAN Trunk)
- **状态 (Status)**

显示端口是开启还是关闭状态。数据通信只能通过已启用的端口。
- **OperState**

显示当前运行状态。运行状态取决于已组态的“状态”(Status)和“链接”(Link)。可用选项如下：

 - 接通 (up)

已将端口的状态组态为“启用”(enabled)，且端口与网络之间存在有效的连接。
 - 中断 (down)

已将端口的状态组态为“禁用”(disabled) 或“链路中断”(Link down)，或者端口不存在连接。
 - 不存在 (not present)

对于模块设备，例如，当没有插入任何媒介模块时，将显示此状态。
- **链路 (Link)**

显示网络连接状态。有以下连接状态：

 - 接通 (up)

端口与网络之间存在有效链路，正在接收链路完整性信号。
 - 中断 (down)

链路中断，例如因为连接的设备被关闭而中断。
- **模式 (Mode)**

显示端口的传输参数。
- **协商 (Negotiation)**

显示自动组态是启用还是禁用状态。
- **流控制类型 (Flow Ctrl.Type)**

显示此端口的流控制是启用还是禁用状态。
- **流控制 (Flow Ctrl.)**

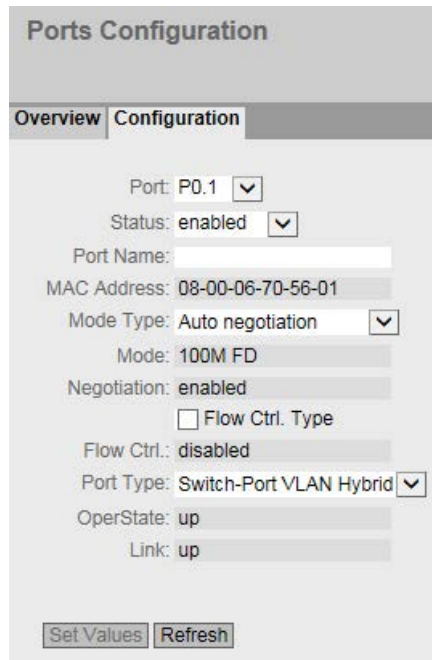
显示此端口上的流量控制是否正常工作。
- **MAC 地址 (MAC Address)**

显示端口的 MAC 地址。

5.4.14.2 组态

组态端口

在此页面上可组态设备的所有端口。



The screenshot displays the 'Ports Configuration' web interface. It features two tabs: 'Overview' and 'Configuration', with 'Configuration' being the active tab. The configuration area includes several fields and controls:

- Port: P0.1 (dropdown menu)
- Status: enabled (dropdown menu)
- Port Name: (text input field)
- MAC Address: 08-00-06-70-56-01 (text input field)
- Mode Type: Auto negotiation (dropdown menu)
- Mode: 100M FD (text input field)
- Negotiation: enabled (text input field)
- Flow Ctrl. Type (checkbox)
- Flow Ctrl.: disabled (text input field)
- Port Type: Switch-Port VLAN Hybrid (dropdown menu)
- OperState: up (text input field)
- Link: up (text input field)

At the bottom of the configuration area, there are two buttons: 'Set Values' and 'Refresh'.

显示框说明

该表格包括以下行：

- **“端口”(Port)**
从下拉列表中选择要组态的端口。端口由模块号和端口号组成，例如，端口 0.1 表示模块 0，端口 1。

5.4 “System”菜单

- **“状态”(Status)**

指定端口是启用还是禁用状态。

- 启用 (enabled)

启用端口。数据通信只能通过已启用的端口。

- 禁用 (disabled)

禁用端口但保持连接。

- 链路中断 (link down)

禁用端口并且中断到伙伴设备的连接。

说明

减小电流消耗

对于每个设置为“链路中断”的光学端口，设备的电流消耗可减少 30 mA。

- **端口名称 (Port Name)**

输入端口的名称。

- **MAC 地址 (MAC Address)**

显示端口的 MAC 地址。

- **模式类型 (Mode Type)**

在此下拉列表中，选择端口的传输速度和传输模式。

如果将模式设置为“自动协商”(Auto negotiation)，会自动与连接的伙伴端口协商这些参数。

在某个端口与伙伴端口互相通讯之前，两端必须具有匹配的设置。

说明

“自动协商”模式

- 如果将端口永久设置为全双工模式，则必须将连接的伙伴端口也设置为全双工模式。
 - 如果将以“自动协商”模式运行的端口连接到不是以“自动协商”模式运行的伙伴端口，则必须修改伙伴端口的设置。
 - 不支持“自动协商”的设备必须永久设置为 100 Mbps 半双工或 10 Mbps 半双工。
-

说明

“自动协商”和自动跨接

- SCALANCE XB-200/SCALANCE XC-200: 如果禁用了“自动协商”功能, 则“MDI/MDI-X”自动跨接功能也会关闭。使用跨接电缆。
 - SCALANCE XP-200: 如果禁用了“自动协商”功能, 则“MDI/MDI-X”自动跨接功能保持激活状态。
-

- **模式 (Mode)**

显示端口的传输速度和传输模式。传输速度可以是 10 Mbps、100 Mbps 或 1000 Mbps。对于传输模式, 可以组态为全双工 (FD) 或半双工 (HD)。

- **“协商”(Negotiation)**

显示对伙伴端口连接的自动组态是处于已启用状态还是处于已禁用状态。

- **流控制类型 (Flow Ctrl.Type)**

启用或禁用端口的流控制。

- **流控制 (Flow Ctrl.)**

显示此端口上的流量控制是否正常工作。

说明

自动协商与开启/关闭流控制

只有关闭“自动协商”功能, 才可启用或禁用流控制。之后, 可再次启用“自动协商”。

- **端口类型 (Port Type)**

从下拉列表中选择端口类型。

- 交换机端口 VLAN 混合 (Switch Port VLAN Hybrid)

端口发送有标记和无标记的帧。它不会自动成为 VLAN 的成员。

- 交换机端口 VLAN 主干 (Switch Port VLAN Trunk)

端口仅发送有标记的帧, 并且自动成为所有 VLAN 的成员。

5.4 “System”菜单

- **OperState**

显示当前运行状态。运行状态取决于已组态的“状态”(Status)和“链接”(Link)。可用选项如下：

- 接通 (up)
已将端口的状态组态为“启用”(enabled)，且端口与网络之间存在有效的连接。
- 中断 (down)
已将端口的状态组态为“禁用”(disabled) 或“链路中断”(Link down)，或者端口不存在连接。
- 不存在 (not present)
对于模块设备，例如，当没有插入任何媒介模块时，将显示此状态。

- **链路 (Link)**

显示网络连接状态。可用选项如下：

- 接通 (up)
端口与网络之间存在有效链路，正在接收链路完整性信号。
- 中断 (down)
链路中断，例如因为连接的设备被关闭而中断。

更改端口组态

单击相应的框可更改组态。

说明

光学端口只能以最大传输速率工作在全双工模式下。因此，不能对光学端口进行以下设置：

- 自动组态
 - 传输速度
 - 传输技术
-

说明

利用各个自动功能，设备可以在某个端口过载时，防止或降低对其它端口和优先级 (Class of Service) 的影响。这意味着即使启用流量控制，帧也可能被丢弃。

当设备接收的帧多于它可以发送的帧时（例如由于不同的传输速度），会发生端口过载。

组态步骤

1. 根据组态更改设置。
2. 单击“设置值”(Set Values) 按钮。

5.4.15 故障监视

5.4.15.1 电源

监视电源的设置

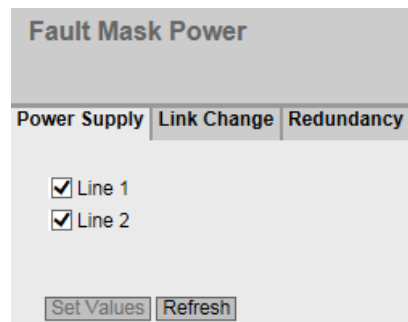
组态是否通过消息系统监视电源。根据硬件型号，会有一个或两个电源连接器（电源 1/电源 2）。带冗余电源时，应对每个单独的进线线路分别组态监视。

当所监视的电源线路（线路 1 或线路 2）未通电或所施加的电压过低时，消息系统将发出故障信号。

说明

设备的操作说明中包含允许的工作电压限值。

故障将触发信号触点，使设备上的故障 LED 亮起，而且根据组态，可触发陷阱、电子邮件或事件日志表中的条目。



步骤

1. 单击要监视的线路名称前的复选框，启用或禁用监视功能。
2. 单击“设置值”(Set Values) 按钮。

5.4.15.2 链路变化

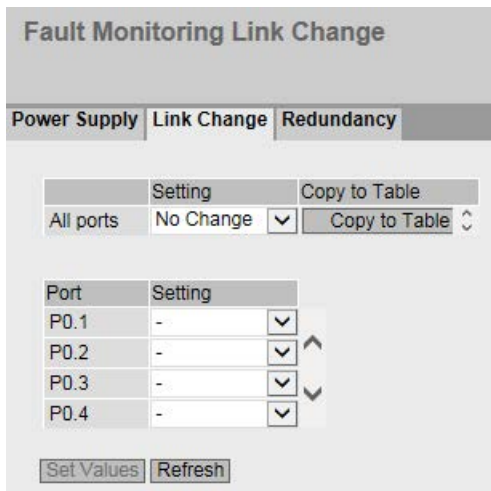
连接状态变化的故障监视组态

在此页面上组态出现网络连接状态变化时是否触发错误信息。

如果启用连接监视，在以下情况下将发出错误信号：

- 当端口上应当有链路但缺失时。
- 或者当端口上不应有链路却检测到链路时。

故障将触发信号触点，使设备上的故障 LED 亮起，而且根据组态，可触发陷阱、电子邮件或事件日志表中的条目。



显示框说明

表 1 包含以下列：

- **第 1 列**
显示设置对于所有端口有效。
- **设置 (Setting)**
从下拉列表中选择设置。可选择以下设置选项：
 - “-”（禁用）
 - Up
 - Down
 - 无变化 (No Change): 表 2 中的设置保持不变。

- **复制到表中 (Copy to Table)**

如果单击此按钮，则为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **“端口”(Port)**

显示可用端口。端口由模块号和端口号组成，例如，端口 0.1 表示模块 0，端口 1。

- **设置 (Setting)**

从下拉列表中选择设置。可做以下选择：

- 有效 (Up)

当端口变为激活状态时触发错误处理。

(从“链路中断”(Link down) 到“链路接通”(Link up))

- 无效 (Down)

当端口变为未激活状态时触发错误处理。

(从“链路接通”(Link up) 到“链路中断”(Link down))

- “-” (禁用)

不触发错误处理。

组态步骤

为端口组态错误监视

1. 从相应的下拉列表中，选择要监视连接状态的插槽/端口对应的选项。
2. 单击“设置值”(Set Values) 按钮。

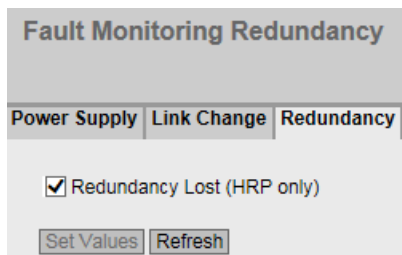
为所有端口组态错误监视

1. 从“设置”(Setting) 列的下拉列表中选择所需设置。
2. 单击“复制到表中”(Copy to table) 按钮。会为表 2 的所有端口应用此设置。
3. 单击“设置值”(Set Values) 按钮。

5.4 “System”菜单

5.4.15.3 冗余

在此页面上组态出现冗余连接状态变化时是否触发错误信息。



设置

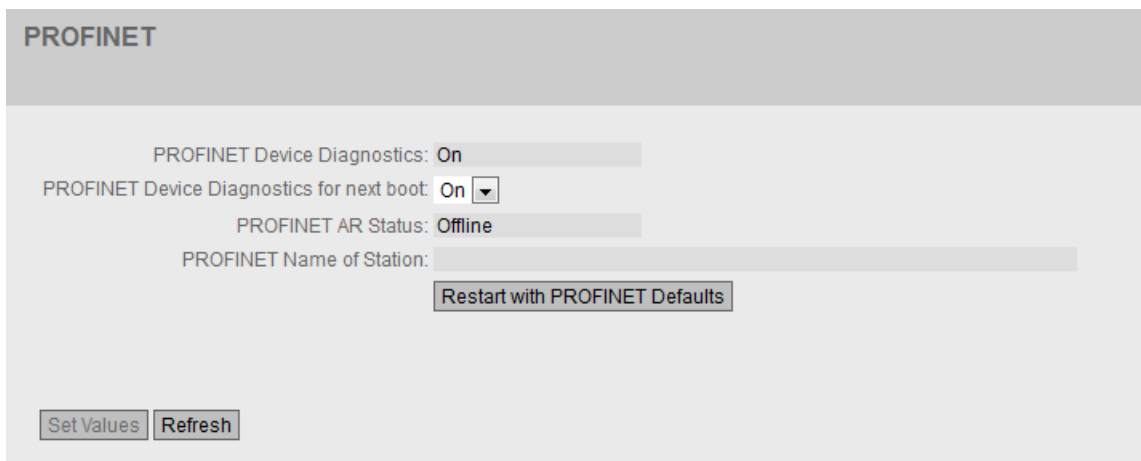
- **Redundancy loss (HRP only)**

启用或禁用连接监视。若失去连接冗余，则指示出错。

5.4.16 PROFINET

PROFINET 的设置

在此页面上组态 PROFINET 的模式。



显示框说明

该页面包含以下框：

- **PROFINET 设备诊断 (PROFINET Device Diagnostics)**
显示启用 (“On”) 还是禁用 (“Off”) PROFINET。
- **下一次启动的 PROFINET 设备诊断 (PROFINET Device Diagnostics for next boot)**
设置下次设备重启后是启用 (“On”) 还是禁用 (“Off”) PROFINET。

说明

PROFINET 和 EtherNet/IP

开启 PROFINET 时，EtherNet/IP 将关闭。PROFINET 和 EtherNet/IP 的切换对 DCP 无影响。

说明

PROFINET AR 状态

如果已建立 PROFINET 连接，即 PROFINET AR 状态为“Online”，则无法禁用 PROFINET。

- **PROFINET AR 状态 (PROFINET AR Status)**
此框显示 PROFINET 连接的状态；也就是说，设备与 PROFINET 控制器连接“Online”(在线) 还是“Offline”(离线)。
在此处，“Online”表示存在到 PROFINET 控制器的连接，即它的组态数据已经下载到设备并且设备可以向 PROFINET 控制器发送状态数据。在这种称为“正在进行数据交换”的状态下，无法对 PROFINET 控制器的参数集进行组态。
- **PROFINET 站名称 (PROFINET Name of Station)**
此框根据 STEP 7 HW Config 中的组态显示 PROFINET 设备名称。

5.4 “System”菜单

- **以 PROFINET 默认设置重启 (Restart with PROFINET Defaults)**

单击该按钮可恢复 PROFINET

配置文件的默认设置并重启设备。必须在对话框中确认重启操作。对话框将显示专门针对使用 PROFINET 协议的操作进行的设置。

注意

将全部设置复位为配置文件的默认设置后，IP 地址也会丢失。之后，只能利用 Primary Setup Tool 或 DHCP 通过串行接口访问设备。

在特定连接情况下，之前已正确组态的设备复位后可能会引起数据帧循环传送，从而导致数据通信故障。

5.4.17 EtherNet/IP

EtherNet 工业协议 (EtherNet/IP)

在此页面上组态 EtherNet/IP 的模式。

EtherNet Industrial Protocol (EtherNet/IP)

EtherNet/IP Device Diagnostics: Off

EtherNet/IP Device Diagnostics for next boot: Off ▾

Restart with EtherNet/IP Defaults

Set Values Refresh

说明

该页面包含以下框：

- **EtherNet/IP 设备诊断 (EtherNet/IP Device Diagnostics)**

显示启用 (“On”) 还是禁用 (“Off”) EtherNet/IP。

- 下一次启动的 **EtherNet/IP 设备诊断 (Ethernet/IP Device Diagnostics for next boot)**

设置下次设备重启后是启用 (“On”) 还是禁用 (“Off”) EtherNet/IP。

说明

EtherNet/IP 和 PROFINET

开启 EtherNet/IP 时，PROFINET 将关闭。EtherNet/IP 和 PROFINET 的切换对 DCP 无影响。

说明

PROFINET AR 状态

如果已建立 PROFINET 连接，即 PROFINET AR 状态为“Online”，则无法启用 EtherNet/IP。

- 以 **EtherNet/IP 默认设置重启 (Restart with Ethernet/IP Defaults)**

单击该按钮可恢复 EtherNet/IP

配置文件的默认设置并重启设备。必须在对话框中确认重启操作。对话框将显示专门针对使用 EtherNet/IP 协议的操作进行的设置。

注意

将全部设置复位为配置文件的默认设置后，IP 地址也会丢失。之后，只能利用 Primary Setup Tool 或 DHCP 通过串行接口访问设备。
--

在特定连接情况下，之前已正确组态的设备复位后可能会引起数据帧循环传送，从而导致数据通信故障。
--

5.4 “System”菜单

5.4.18 PLUG

5.4.18.1 组态

注意
切勿在运行期间插拔 C-PLUG 只有在设备关闭情况下才可以插拔 PLUG。 设备以 1 秒的间隔检查 PLUG 是否存在。如果检测到 PLUG 被卸下，则会重启。

C-PLUG 组态的相关信息

此页面提供了有关 C-PLUG 上存储的组态的详细信息。还可以将 PLUG 复位为“出厂默认设置”或向其中加载新内容。

说明

只有在单击“Set Values”按钮后，才会执行此操作。

此操作无法撤销。

如果进行选择之后您决定不执行此功能，则单击“Refresh”按钮。随后将再次从设备中读取此页面数据，并会取消选择。

说明

插入的 PLUG 组态与旧固件版本不兼容

在安装旧固件版本的过程中，组态数据可能丢失。在这种情况下，安装固件后，设备会使用出厂设置启动。如果此时设备中插入了 PLUG，则重启后，由于 PLUG 仍具有之前最新固件的组态数据，因此状态为“NOT

ACCEPTED”。这样，您便可以返回之前的最新固件而不丢失任何组态数据。

如果不再需要 PLUG 上的原始组态，则可使用“系统 > PLUG”(System > PLUG) 手动删除或重写 PLUG。

PLUG Configuration (C-PLUG)

Configuration

State: ACCEPTED

Device Group: SCALANCE XP200

Device Type: SCALANCE XP216PoE EEC

Configuration Revision: 1

File System: UBIFS

File System Size: 2749824

File System Usage: 17609

Info String: 6GK5 216-0UA00-5ES6
SCALANCE XP216PoE EEC
HW: 1
SW: V02.00.00

Modify PLUG: Select action

Set Values Refresh

显示框说明

该表格包括以下行：

- **State**

显示 PLUG 的状态。可能的状态包括：

 - ACCEPTED
设备中存在具有有效且适当组态的 PLUG。
 - NOT ACCEPTED
插入的 PLUG 上的组态无效或不兼容。
 - NOT PRESENT
设备中未插入 C-PLUG。
 - FACTORY
PLUG 已插入，但不包含组态。如果在操作过程中对 PLUG 进行了格式化，则也会显示此状态。
- **设备组 (Device Group)**

显示先前使用该 C-PLUG 的 SIMATIC NET 产品系列。

5.4 “System”菜单

- **设备类型 (Device Type)**
显示先前使用该 C-PLUG 的产品系列的设备类型。
- **Configuration Revision**
组态结构的版本。此信息与设备支持的组态选项相关，而与具体的硬件配置无关。因此，在添加或移除附加组件（模块或扩展器）时，此版本信息不会改变，但是如果更新固件，则该信息可能会发生改变。
- **File System**
显示 PLUG 上的文件系统类型。
- **File System Size [bytes]**
显示 C-PLUG 上文件系统的最大存储能力。
- **File System Usage [bytes]**
显示 C-PLUG 文件系统中已使用的存储空间。
- **Info String**
显示有关之前使用该 PLUG 的设备的所有附加信息，例如：订货号、型号标识以及硬件与软件的版本。显示的软件版本与上次更改了组态的版本相对应。状态为“NOT ACCEPTED”时，将显示有关问题原因的更多信息。
- **修改 PLUG (Modify PLUG)**
从下拉列表中选择设置。用户可使用以下选项更改 C-PLUG 上的组态：
 - **Write current Configuration to the PLUG**
仅当 PLUG 的状态为“NOT ACCEPTED”或“FACTORY”时，此选项才可用。
会将设备内部闪存中的组态复制到 PLUG。
 - **Erase PLUG to factory default**
删除 C-PLUG 中的所有数据并触发低级格式化功能。

组态步骤

1. 仅当以“管理员”身份登录时，才能对此框进行设置。在此处，您可决定更改 PLUG 内容的方式。
2. 从“Modify PLUG”下拉列表中选择所需选项。
3. 单击“设置值”(Set Values) 按钮。

5.4.19 Ping

IPv4 网络中地址的可访问性

通过 ping 功能，可检查某一 IPv4 地址在网络中是否可访问。



The screenshot shows a web-based interface for a ping utility. At the top, there is a header bar with the text "Ping". Below this, there are two input fields: "Destination Address:" followed by a text box, and "Repeat 3" followed by a text box. To the right of the "Repeat 3" field is a button labeled "Ping". Below these fields is a large, empty text area labeled "Ping Output". At the bottom left of this text area is a button labeled "Clear".

说明

该表格包括以下列：

- **目标地址 (Destination Address)**
输入设备的 IPv4 地址。
- **Repeat**
输入 ping 请求的数量。
- **Ping**
单击该按钮可启动 ping 功能。
- **Ping Output**
该框会显示 ping 功能的输出。
- **Clear**
单击该按钮可清空“Ping Output”框。

5.4.20 Power over Ethernet (PoE)

5.4.20.1 常规

以太网供电 (PoE) 的设置

在此页面，您会看到由工业以太网交换机使用 PoE 供电的相关信息。

SCALANCE XP-200 的 PoE 型号是 PSE（供电设备）。

PSE	Maximum Power[W]	Allocated Power[W]	Power In Use[W]	Usage Threshold[%]
1	90	0	0	80
2	90	0	0	80

显示框说明

- **PSE（只读）**
显示 PSE 编号。
- **Maximum Power [W]（只读）**
PSE 为 PoE 设备提供的最大功率。
- **Allocated Power [W]（只读）**
PoE 设备根据“分类”保留的功率总和。
- **Power in Use [W]（只读）**
终端设备使用的功率总和。
- **Usage Threshold [%]**
只要终端设备使用的功率超过此处显示的百分比，就会触发事件。

5.4.20.2 端口

端口的设置

对于每个 PoE 端口，都可以指定是否通过以太网供电。还可以为各个连接的受电设备 (PD) 设置优先级。优先级高的设备优先于其它受电设备。

在此页面上，可以查看各个 PoE 端口的详细信息。

Power over Ethernet (PoE) Port

General | **Port**

Port	Setting	Priority	Type	Use Custom Maximum Power	Custom Maximum Power[W]	Copy to Table
All ports	No Change ▾	No Change ▾	No Change	No Change	No Change	Copy to Table

Port	Setting	Priority	Type	Use Custom Maximum Power	Custom Maximum Power[W]	Classification	Status	Power[mW]	Voltage[V]	Current[mA]
P0.5	<input checked="" type="checkbox"/>	low ▾		<input type="checkbox"/>	0	-	searching	0	0	0
P0.6	<input checked="" type="checkbox"/>	low ▾		<input type="checkbox"/>	0	-	searching	0	0	0
P0.7	<input checked="" type="checkbox"/>	low ▾		<input type="checkbox"/>	0	-	searching	0	0	0
P0.8	<input checked="" type="checkbox"/>	low ▾		<input type="checkbox"/>	0	-	searching	0	0	0

Set Values Refresh

显示框说明

该页面包含两个表。在表 1 中，可进行设置，并同时将这些设置分配到所有端口。在表 2 中，可以对各端口进行不同的设置。

表 1 包含以下列：

- Port**
 显示设置对于所有端口有效。
- Setting**
 选择所需设置。
 如果选择“无变化”(No Change)，则表 2 中的条目保持不变。
- Priority**
 选择所需优先级。
 如果选择“无变化”(No Change)，则表 2 中的条目保持不变。
- Type**
 在此处可输入字符串，更详细地描述所连接的设备。最大长度为 255 个字符。

5.4 “System”菜单

- **使用自定义最大功率 (Use Custom Maximum Power)**

选择是否使用自定义最大功率。

如果选择“无变化”(No Change)，则表 2 中的条目保持不变。

- **自定义最大功率 [W] (Custom Maximum Power [W])**

输入端口为所连设备所能提供的最大功率。

仅当选中“使用自定义最大功率”(Use Custom Maximum Power)复选框时，才考虑该值。

如果输入“无变化”(No Change)，则表 2 中的条目保持不变

- **Copy to Table**

如果单击此按钮，则为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **Port**

显示可组态的 PoE 端口。

端口由模块号和端口号组成，例如，端口 0.1 表示模块 0，端口 1。

- **Setting**

启用对此端口的 PoE 供电或中断供电。

- **Priority**

从下拉列表中选择此端口的供电优先级。

可进行以下设置（按相关性以升序排列）：

- 低 (Low)

低优先级

- 高 (High)

中优先级

- 关键 (Critical)

高优先级

如果所连电源不足以为连接的所有设备供电，则优先为优先级较高的设备供电。

如果为两个端口设置相同的优先级，则必要时优先选择编号较低的端口。

- **Type**

在此处可输入字符串，更详细地描述所连接的设备。最大长度为 255 个字符。

- **Use Custom Maximum Power**

如果为某个端口选中了该复选框，则会使用用户定义的最大功率。

- **自定义最大功率 [W] (Custom Maximum Power [W])**

确保端口所能实现的最大功率可用于为连接的设备供电。

选中“Use Custom Maximum Power”复选框时，会将该值考虑在内。

用户定义的电源与所连设备指示的类别的值范围进行比较。

- 如果用户定义的电源处于所连设备的类别内，则使用用户定义的值。
- 如果用户定义的电源高于所连设备的类别，则使用该类别的最大值。
- 如果用户定义的电源低于所连设备的类别，则使用该类别的最小值。

如果所连设备的功耗超过指定的或所用的最大功率，则所连设备被关闭。

- **Classification (只读)**

分类指定设备的类别。

- **Status (只读)**

显示端口的当前状态。

可能的状态有：

- **disabled**

禁止对此端口进行 PoE 供电。

- **delivering**

激活对此端口的 PoE 供电并连接一台设备。

- **searching**

激活对此端口的 PoE 供电，但未连接设备。

说明

如果设备连接到带有 PoE

功能的端口，则进行检查，以确定端口的电源是否适用于已连接设备。

如果端口的电源不足，则即使在“设置”(Setting) 中启用

PoE，端口的状态仍为“disabled”。这意味着，端口因 PoE 电源管理而禁用。

- **Power [mW] (只读)**

显示 SCALANCE 为此端口提供的功率。

5.4 “System”菜单

- **Voltage [V]**（只读）
显示施加到此端口的电压。
- **Current [mA]**（只读）
显示为连接到此端口的设备提供的电流。

5.4.21 端口诊断

5.4.21.1 电缆测试器

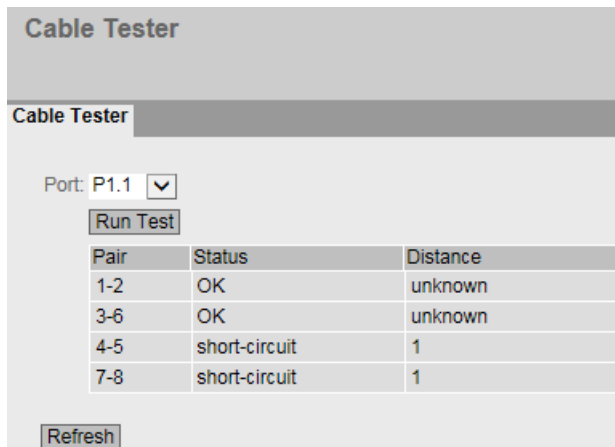
使用该页面，每个以太网端口均可用来诊断独立的电缆故障。无需移除电缆、连接电缆连接器以及在另一端安装回送模块，便可进行测试。这能够将短路和电缆断线点定位到几米之内。

说明

请注意，只有在要测试的端口上没有建立任何数据连接时才允许该测试。

而如果要测试的端口上存在数据连接，则会出现短暂的中断。

自动重新建立连接可能会失败，之后需要手动连接。



说明

该页面包含以下框：

- **端口 (Port)**
从下拉列表中选择所需端口。
- **运行测试 (Run Test)**
激活错误诊断。结果会显示在表中。

该表包含以下各列：

- **线对 (Pair)**
显示电缆中的线对。

说明

线对

未使用 10/100 Mbps 网络电缆中的线对 4-5 和 7-8。

线对分配 - 引脚分配如下 (DIN 50173)：

线对 1 = 引脚 1-2

线对 2 = 引脚 3-6

线对 3 = 引脚 4-5

线对 4 = 引脚 7-8

-
- **状态 (Status)**
显示电缆的状态。
 - **距离 (Distance)**
显示到电缆末端、电缆断线点或短路点的距离（米）。距离值的允许误差为 +/- 1 m。

5.4.21.2 SFP 诊断

在此页面中，可以为每个 SFP 端口运行独立故障诊断。无需移除电缆、连接电缆连接器或在另一端安装回送模块，便可进行测试。

Small Form-factor Pluggable (SFP) Transceiver Diagnostics

Cable Tester
SFP Diagnostics

Port:

Name:

Model:

Revision:

Serial:

Nominal Bit Rate[MBit/s]:

Max. Link (50.0/125um)[m]:

Max. Link (62.5/125um)[m]:

	Current	Low	High
Temperature[°C]:	<input type="text" value="40.19"/>	<input type="text" value="-5.00"/>	<input type="text" value="75.00"/>
Voltage[V]:	<input type="text" value="3.21"/>	<input type="text" value="3.00"/>	<input type="text" value="3.55"/>
Current[mA]:	<input type="text" value="5.44"/>	<input type="text" value="2.92"/>	<input type="text" value="9.10"/>
Rx Power[uW]:	<input type="text" value="0.00"/>	<input type="text" value="63.00"/>	<input type="text" value="891.02"/>
Tx Power[uW]:	<input type="text" value="453.08"/>	<input type="text" value="316.02"/>	<input type="text" value="891.02"/>

说明

该页面包含以下框：

- **端口 (Port)**
从下拉列表中选择所需端口。
- **刷新 (Refresh)**
刷新设定端口的值显示。结果会显示在表中。

相应值显示在以下框中：

- **名称 (Name)**
显示接口名称。
- **型号 (Model)**
显示接口的类型。

- **修订 (Revision)**
显示 SFP 的硬件版本。
- **序列 (Serial)**
显示 SFP 的序列号。
- **Nominal Bit Rate [Mbps]**
显示接口的额定位速率。
- **最长链路 (50.0/125um) [m] (Max. Link (50.0/125um) [m])**
显示使用此介质时支持的最远距离（单位为米）。
- **最长链路 (62.5/125um) [m] (Max. Link (62.5/125um) [m])**
显示使用此介质时支持的最远距离（单位为米）。

下表显示了此端口中使用的 SFP 收发器的值：

- **温度 [°C] (Temperature [°C])**
显示接口的温度。
- **电压 [V] (Voltage [V])**
显示施加到接口的电压 [V]。
- **电流 [mA] (Current [mA])**
显示接口的电流消耗 [mA]。
- **Rx Power [μW]**
显示接口的接收功率 [μW]。
- **Tx Power [μW]**
显示接口的发送功率 [μW]。
- **“当前”(Current) 列**
显示当前值。
- **“低”(Low) 列**
显示最低值。
- **“高”(High) 列**
显示最高值。

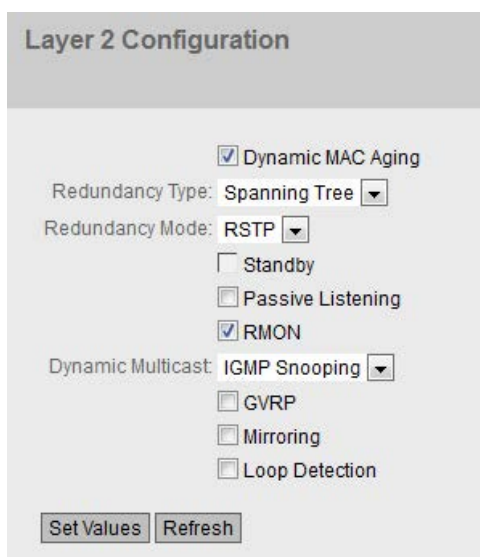
5.5 “第 2 层”菜单

5.5 “第 2 层”菜单

5.5.1 组态

组态第 2 层

在此页面中为第 2 层功能创建基本组态。在这些功能的组态页面，可进行详细设置。也可以在组态页面中检查设置。



The screenshot shows a web interface titled "Layer 2 Configuration". It contains several configuration options:

- Dynamic MAC Aging
- Redundancy Type: Spanning Tree (dropdown menu)
- Redundancy Mode: RSTP (dropdown menu)
- Standby
- Passive Listening
- RMON
- Dynamic Multicast: IGMP Snooping (dropdown menu)
- GVRP
- Mirroring
- Loop Detection

At the bottom of the configuration area, there are two buttons: "Set Values" and "Refresh".

显示框说明

- **动态 MAC 老化 (Dynamic MAC Aging)**
启用或禁用“老化”机制。可以在“Layer 2 > Dynamic MAC Aging”中组态其它设置。

- **冗余类型 (Redundancy Type)**

可使用以下设置：

- **“-” (禁用)**

禁用冗余功能。

- **生成树 (Spanning Tree)**

如果选择此选项，则可在“冗余模式”(Redundancy Mode)

下拉列表中指定所需冗余模式。

- **环网 (Ring)**

如果选择此选项，则可在“冗余模式”(Redundancy Mode)

下拉列表中指定所需冗余模式。

- **冗余模式 (Redundancy Mode)**

如果在“冗余类型”(Redundancy Type)

下拉列表中选择“环网”(Ring)，则可使用以下选项：

- **Automatic Redundancy Detection**

选择此设置可创建冗余模式的自动组态。

在“自动冗余检测”模式下，设备会自动检测环网中是否存在充当“HRP 管理器”角色的设备。如果存在，该设备将获得“HRP”客户端的角色。

如果未找到 HRP 管理器，则所有设置为“自动冗余检测”或“MRP 自动管理器”的设备将通过彼此协商来确定哪台设备将获得“MRP 管理器”的角色。MAC 地址最低的设备将始终为“MRP 管理器”。其余设备将自动设置为“MRP 客户端”模式。

- **MRP Auto-Manager**

在“MRP 自动管理器”模式下，设备通过彼此协商来确定哪个设备获得“MRP 管理器”的角色。MAC 地址最低的设备将始终为“MRP 管理器”。其余设备将自动设置为“MRP 客户端”模式。

与“自动冗余检测”(Automatic Redundancy Detection)

设置不同，设备在此模式下无法检测环网中是否存在 HRP 管理器。

说明

STEP 7 中的 MRP 组态

如果在 STEP 7

中为设备设置“管理器（自动）”或“管理器”角色，则在两种情况下，“MRP 自动管理器”都会显示在该 WBM 页面中。在 CLI 的显示中，会对这两个角色进行区分。

5.5 “第 2 层”菜单

- **MRP 客户端 (MRP Client)**

设备采用 MRP 客户端角色。

- **HRP 客户端 (HRP Client)**

设备采用 HRP 客户端角色。

- **HRP 管理器 (HRP Manager)**

设备采用 HRP 管理器角色。

组态 HRP 环网时，必须将其中一个设备设置为 HRP

管理器。针对所有其它设备，必须设置“HRP 客户端”或“自动冗余检测”。

如果在“冗余类型”(Redundancy Type) 下拉列表中选择“生成树”(Spanning Tree)，则可使用以下选项：

- **STP**

启用 Spanning Tree Protocol (STP)。生成树的典型重新组态时间介于 20 到 30 秒之间。可以在“第 2 层 > 生成树”(Layer 2 > Spanning Tree) 中组态其它设置。

- **RSTP**

启用 Rapid Spanning Tree Protocol

(RSTP)。如果在某个端口上检测到生成树帧，该端口会从 RSTP

恢复为生成树。可以在“第 2 层 > 生成树”(Layer 2 > Spanning Tree)

中组态其它设置。

说明

使用 RSTP

时，可能短暂出现环路包含重复帧的或帧乱序的情况。如果具体应用不能接受这种情况，应使用较慢的标准生成树机制。

- **MSTP**

启用 Multiple 生成树协议 (STP)。可以在“第 2 层 > 生成树”(Layer 2 > Spanning Tree) 中组态其它设置。

- **备用 (Standby)**

启用或禁用备用冗余功能。可在“第 2 层 > 环网冗余”(Layer 2 > Ring Redundancy) 中找到其它设置。

- **被动侦听 (Passive Listening)**

启用或禁用被动侦听功能。

凭借被动侦听，可将生成树网络连接到 MRP/HRP 环网。环网节点将转发生成树 BPDU，从而对拓扑变化做出反应。接收到拓扑变更帧后，则删除 MAC 地址表。

- **RMON**

如果选择该复选框，则远程监视 (RMON)

允许在设备上收集和准备诊断数据，并由同样支持 RMON 的网络管理站使用 SNMP 读出诊断数据。凭借此诊断数据（例如，端口相关的负载趋势）可以在早期发现并排除网络中的故障。某些“以太网统计信息计数器”是 RMON 功能的一部分。如果禁用 RMON，则不再更新“信息 > 以太网统计信息”(Information > Ethernet statistics) 中的“以太网统计信息计数器”(Ethernet statistics counter)。

- **动态组播 (Dynamic Multicast)**

可能的设置如下：

- “-”（禁用）

- **IGMP Snooping**

启用 IGMP（Internet 组管理协议，Internet Group Management Protocol）。可以在“Layer 2 > Multicast > IGMP”中组态其它设置。

- **GMRP**

启用 GMRP（GARP 组播注册协议）。可以在“第 2 层 > 组播 > GMRP”(Layer 2 > Multicast > GMRP) 中组态其它设置。

说明

GMRP 和 IGMP 不能同时起作用。

- **GVRP**

启用或禁用“GVRP”（GARP VLAN 注册协议）。可以在“第 2 层 > VLAN > GVRP”(Layer 2 > VLAN > GVRP) 中组态其它设置。

- **镜像 (Mirroring)**

启用或禁用端口镜像。可以在“第 2 层 > 镜像”(Layer 2 > Mirroring) 中组态其它设置。

- **回路检测 (Loop Detection)**

启用或禁用回路检测功能。通过该功能可检测网络中的回路。可在“第 2 层 > 回路检测”(Layer 2 > Loop Detection) 中找到其它设置。

5.5 “第 2 层”菜单

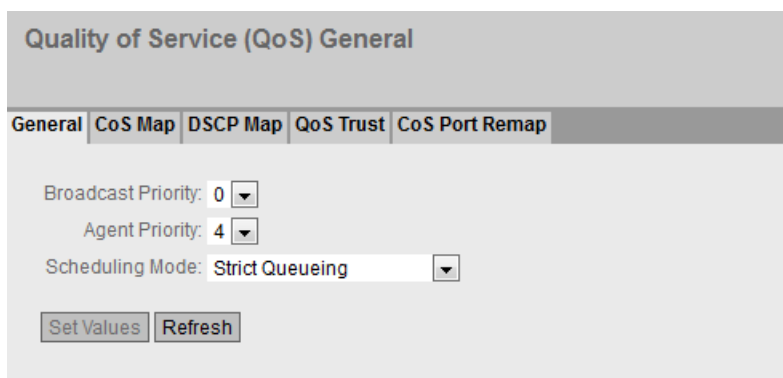
5.5.2 Quality of Service (QoS)

也可参见“技术基础”章节的“服务质量 (页 45)”部分。

5.5.2.1 常规

传输优先级

在此页面中，可以指定不同帧的优先级。此外，您可以基于优先级设置用于指定帧处理顺序的方法。



显示值说明

该页面包含以下框：

- **广播优先级 (Broadcast Priority)**

指定广播帧的优先级。交换机将根据此优先级将帧排序到 Queue 中。在“第 2 层 > QoS > CoS 映射”(Layer 2 > QoS > CoS Map) 页面上，组态优先级至队列的分配。

- **代理优先级 (Agent Priority)**

指定代理帧的优先级。交换机将根据此优先级将帧分类到队列中。在“第 2 层 > QoS > CoS 映射”(Layer 2 > QoS > CoS Map) 页面上，组态优先级至队列的分配。

- **计划模式 (Scheduling Mode)**

选择队列中帧的处理顺序。

- **Strict Queueing**

只要队列中存在优先级更高的帧，就只处理这些高优先级的帧。

- **Weighted Fair Queueing**

即使队列中存在优先级更高的帧，偶尔还是会处理优先级较低的帧。

组态步骤

1. 从“广播优先级”(Broadcast Priority) 和“代理优先级”(Agent Priority) 下拉列表中，选择在内部处理帧的优先级。
2. 在“计划模式”(Scheduling Mode) 下拉列表中，选择确定帧处理顺序的方法。
3. 单击“Set Values”按钮。

5.5.2.2 CoS 映射 (CoS Map)

CoS 映射 (CoS Map)

在此页面上，可将 CoS 优先级分配给不同的队列。

Class of Service (CoS) Mapping				
General	CoS Map	DSCP Map	QoS Trust	CoS Port Remap
COS	Queue			
0	2			▼
1	1			▼
2	1			▼
3	2			▼
4	3			▼
5	3			▼
6	4			▼
7	4			▼

Set Values Refresh

显示框说明

该表格包括以下列：

- **CoS**
显示入站帧的 CoS 优先级。
- **队列 (Queue)**
从下拉列表中选择分配给 CoS 优先级的队列。
队列编号越高，处理优先级越高。

5.5 “第 2 层”菜单

服务等级 (CoS) 按如下默认方式分配给各个队列：

- COS 0 → 队列 2
- COS 1 → 队列 1
- COS 2 → 队列 1
- COS 3 → 队列 2
- COS 4 → 队列 3
- COS 5 → 队列 3
- COS 6 → 队列 4
- COS 7 → 队列 4

组态步骤

1. 对于“CoS”列中的每个值，请从“队列”(Queue) 下拉列表中选择队列。
2. 单击“Set Values”按钮。

5.5.2.3 DSCP 映射 (DSCP Map)

DSCP 队列

在此页面上，可将 DSCP 优先级分配给不同的 Queues。

DSCP	Queue
0	1
1	1
2	1
3	1
4	1

Set Values Refresh

显示值说明

该表格包括以下列：

- **DSCP**
显示入站帧的 DSCP 优先级。
- **队列 (Queue)**
从下拉列表中选择分配给 DSCP 优先级的队列。
队列编号越高，处理优先级越高

DSCP 优先级按如下默认方式分配给各个队列：

- DSCP 编码 0 - 15 → 队列 1
- DSCP 编码 16 - 31 → 队列 2
- DSCP 编码 32 - 47 → 队列 3
- DSCP 编码 48 - 63 → 队列 4

组态步骤

1. 对于“DSCP”列中的每个值，请从“队列”(Queue) 下拉列表中选择队列。
2. 单击“Set Values”按钮。

5.5.2.4 QoS 信任 (QoS Trust)

指定子网优先级

在此页面上，可逐个端口设置按优先级转发帧所依据的方法。

Port	Trust Mode	Copy to Table
All ports	No Change	Copy to Table

Port	Trust Mode
P0.1	Trust COS-DSCP
P0.2	Trust COS-DSCP
P0.3	Trust COS-DSCP
P0.4	Trust COS-DSCP

Set Values Refresh

5.5 “第 2 层”菜单

显示值说明

表 1 包含以下列：

- **Port**

说明设置对于表 2 的所有端口都有效。

- **Trust Mode**

从下拉列表中选择设置。可选择以下设置选项：

- No Trust
- Trust COS
- Trust DSCP
- Trust COS-DSCP
- 无变化 (No Change)

表 2 保持不变。

- **Copy to Table**

如果单击此按钮，则为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **Port**

显示可组态的端口。

端口由模块号和端口号组成，例如，端口 0.1 表示模块 0，端口 1。

- **信任模式 (Trust Mode)**

从下拉列表中选择需要的模式:

说明

在“第 2 层 > VLAN > 基于端口的 VLAN”(Layer 2 > VLAN > Port Based VLAN)页面上，组态接收端口的优先级。

在“第 2 层 > QoS > CoS 映射”(Layer 2 > QoS > CoS Map)页面上，组态以下优先级到队列的分配。

- 接收端口
- VLAN 标记
- 广播和代理帧

在“第 2 层 > QoS > CoS 映射”(Layer 2 > QoS > CoS Mapping)页面上，组态 DSCP 优先级到队列的分配。

– **No Trust**

交换机将根据接收端口的优先级将入站帧分类到队列中。

如果 IP 报头中存在 DSCP 值，则忽略此参数。如果存在 VLAN 标记，则由接收端口的优先级值替代其优先级值。

– **Trust COS**

如果入站帧包含 VLAN 标记，交换机将根据此优先级将帧分类到队列中。

如果帧不包含 VLAN 标记，交换机将根据接收端口的优先级将帧分类到队列中。

如果 IP 报头中存在 DSCP 值，则忽略此参数。

– **Trust DSCP**

如果入站帧包含 DSCP 优先级，交换机将根据此优先级将帧分类到队列中。

如果帧不包含 DSCP 优先级，交换机将根据接收端口的优先级将帧分类到队列中。

如果帧包含 VLAN 标记，则忽略此参数。

– **Trust COS-DSCP**

对于入站帧，将对其包含的优先级进行连续检查。

如果其中包含 DSCP 优先级，则将其处理为“信任 DSCP”(Trust DSCP) 模式。

如果其中不包含 DSCP 优先级，则交换机会检查是否包含 VLAN 标记。如果帧不包含 VLAN 标记，交换机将根据此优先级将帧分类到队列中。

如果帧既不包含 DSCP 优先级也不包含 VLAN

标记，交换机将根据接收端口的优先级将帧分类到队列中。

5.5 “第 2 层”菜单

组态步骤

1. 从下拉列表中选择需要的“信任模式”(Trust Mode)。
2. 单击“设置值”(Set Values) 按钮。

5.5.2.5 CoS 端口重映射

发送时更改优先级

在此页面上，可以根据接收帧时的优先级，更改发送帧时所用的优先级。

Class of Service (CoS) Port Remap

General | CoS Map | DSCP Map | QoS Trust | CoS Port Remap

CoS Remap

Port	Priority 0	Priority 1	Priority 2	Priority 3	Priority 4	Priority 5	Priority 6	Priority 7	Copy to Table		
All ports	No Change	▼	No Change	▼	No Change	▼	No Change	▼	No Change	▼	Copy to Table

Port	Priority 0	Priority 1	Priority 2	Priority 3	Priority 4	Priority 5	Priority 6	Priority 7								
P0.1	0	▼	1	▼	2	▼	3	▼	4	▼	5	▼	6	▼	7	▼
P0.2	0	▼	1	▼	2	▼	3	▼	4	▼	5	▼	6	▼	7	▼
P0.3	0	▼	1	▼	2	▼	3	▼	4	▼	5	▼	6	▼	7	▼
P0.4	0	▼	1	▼	2	▼	3	▼	4	▼	5	▼	6	▼	7	▼

Set Values Refresh

显示框说明

该页面包含以下框：

- **CoS 重映射 (CoS Remap)**

根据表 2 启用或禁用根据已更改优先级发送的帧。

表 1 包含以下列：

- **端口 (Port)**

说明设置对于表 2 的所有端口都有效。

- **优先级 0 - 7**

列中的优先级表示接收帧时所用的优先级。

- 0 - 7

选择发送帧时所用的优先级。

- 无变化 (No Change)

表 2 无变化。

- **复制到表中 (Copy to Table)**

如果单击此按钮，则为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **端口 (Port)**

显示所有可用端口。端口由模块号和端口号组成，例如，端口 0.1 表示模块 0，端口 1。

- **优先级 0 - 7**

列中的优先级表示接收帧时所用的优先级。

在下拉列表中，选择发送帧时所用的优先级。

组态步骤

1. 选择“CoS 重映射”(CoS Remap) 复选框。
2. 使用下拉列表，根据每个端口的接收优先级选择发送优先级。
3. 单击“Set Values”按钮。

5.5.3 速率控制

限制进入和离开数据的传输速率

在此页面上组态各个端口的负载限值。您可以指定将应用这些限制值的帧的类别。

Rate Control

	Limit Ingress Unicast (DLF)	Limit Ingress Broadcast	Limit Ingress Multicast	Total Ingress Rate kb/s	Egress Rate kb/s	Copy to Table
All ports	No Change <input type="button" value="v"/>	No Change <input type="button" value="v"/>	No Change <input type="button" value="v"/>	No Change	No Change	<input type="button" value="Copy to Table"/>

Port	Limit Ingress Unicast (DLF)	Limit Ingress Broadcast	Limit Ingress Multicast	Total Ingress Rate kb/s	Egress Rate kb/s
P0.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P0.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P0.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P0.4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0

显示值说明

表 1 包含以下列：

- **第 1 列**
显示设置对于所有端口有效。
- **限制入站单播 (DLF)/限制入站广播/限制入站组播 (Limit Ingress Unicast (DLF) / Limit Ingress Broadcast / Limit Ingress Multicast)**
在下拉列表中选择所需设置。
 - 启用 (Enabled): 启用此功能。
 - 禁用 (Disabled): 禁用该功能
 - 无变化 (No Change): 表 2 中的设置保持不变
- **总入站速率 kb/s (Total Ingress Rate kb/s)**
指定所有入站帧的数据速率。如果输入“无变化”(No Change)，则表 2 中的条目保持不变

- **出站速率 kb/s (Egress Rate kb/s)**

指定所有出站帧的数据传输率。如果输入“无变化”(No Change)，则表 2 中的条目保持不变

- **Copy to Table**

如果单击此按钮，将为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **端口 (Port)**

显示所有可用端口。端口由模块号和端口号组成，例如，端口 0.1 表示模块 0，端口 1。

- **限制入站单播 (DLF) (Limit Ingress Unicast (DLF))**

启用或禁用数据传输率，以限制无法解析地址的入站单播帧 (Destination Lookup Failure)。

- **限制入站广播(Limit Ingress Broadcast)**

启用或禁用数据传输率，以限制入站广播帧。

- **限制入站组播 (Limit Ingress Multicast)**

启用或禁用数据传输率，以限制入站组播帧。

- **总入站速率 kb/s (Total Ingress Rate kb/s)**

指定所有入站帧的数据速率。

- **出站速率 kb/s (Egress Rate kb/s)**

指定所有出站帧的数据传输率。

说明

对数值取整，与期望值的偏差

输入时，请注意 WBM 会取整为正确的值。

如果组态了“总入站速率”(Total Ingress Rate) 和“出站速率”(Egress Rate) 的值，则运行中的实际值可能与设定值稍有不同。

5.5 “第 2 层”菜单

组态步骤

1. 在所组态端口行的“总入站速率”(Total Ingress Rate) 和“出站速率”(Egress Rate) 列中输入相关值。
2. 要使用入站帧限制，请选中该行中的复选框。对于出站帧，会使用“出站速率”(Egress Rate) 列中的值。
3. 单击“设置值”(Set Values) 按钮。

5.5.4 VLAN

5.5.4.1 常规

VLAN 组态页面

在该页面，可以指定设备是否以透明方式转发带有 VLAN 标记的帧（IEEE 802.1D/VLAN 非感知模式），或者指定设备是否考虑 VLAN 信息（IEEE 802.1Q/VLAN 感知模式）。如果设备处于“802.1Q VLAN Bridge”模式下，则可以定义 VLAN 并指定端口的使用。

在该页面上可以进行的设置取决于在“基础网桥模式”(Base Bridge Mode) 框中的选择。

说明

更改代理 VLAN ID

如果组态 PC 通过以太网直接连接到设备，并且更改了代理 VLAN ID，则更改后无法再通过以太网访问该设备。

Virtual Local Area Network (VLAN) General

General | GVRP | Port Based VLAN

Base Bridge Mode: 802.1Q VLAN Bridge

VLAN ID:

Select	VLAN ID	Name	Status	Priority	P0.1	P0.2	P0.3	P0.4
<input type="checkbox"/>	1		Static	Do not force	U	U	U	U
<input type="checkbox"/>	5		Static	Do not force	-	-	-	-

2 entries.

Create Delete Set Values Refresh

显示框说明

该页面包含以下框：

- **基础网桥模式 (Base Bridge Mode)**

说明

切换基础网桥模式

请参见本章中的“切换基础网桥模式”部分。此部分介绍模式切换对现有组态的影响。

从下拉列表中选择需要的模式。可能的模式如下：

- 802.1Q VLAN Bridge

将设备模式设置为“VLAN 识别”。在此模式下，会将 VLAN 信息考虑在内。

- 802.1D Transparent Bridge

将设备模式设置为“VLAN 不识别”。在此模式下，不会考虑或更改 VLAN 标记，而会以透明方式转发这些标记。在此模式下，无法创建任何 VLAN。仅管理 VLAN 可用：VLAN 1。

- **VLAN ID**

在“VLAN ID”输入框中输入 VLAN ID。

值范围：1 ... 4094

该表格包括以下列：

- **选择 (Select)**

选择要删除的行。

- **VLAN ID**

显示 VLAN ID。VLAN ID（介于 1 到 4094

之间的数字）只能在创建新数据记录时分配一次，之后不能更改。如要更改，必须删除整个数据记录并重新创建。

- **名称 (Name)**

输入 VLAN 的名称。此名称仅提供信息，对组态没有影响。

长度：最多 32 个字符

- **状态 (State)**

显示内部端口过滤器表中条目的状态类型。此处的“Static”表示该 VLAN 是由用户以静态方式输入的。

5.5 “第 2 层”菜单

- **Priority**

选择为 VLAN 强制执行的优先级。所选的优先级将输入此 VLAN 的所有进入帧中。交换机将根据所选优先级转发进入帧。

如果选择“非强制”(Do not force)，帧的优先级将保持不变。

- **端口列表 (List of ports)**

指定端口的使用。可使用以下选项：

- “-”

该端口不是指定 VLAN 的成员。

对于新定义，所有端口的标识符均为“-”。

- M

该端口是 VLAN 的成员。此 VLAN 中发送的帧在转发时带有相应 VLAN 标记。

- R

该端口是 VLAN 的成员。GVRP 帧用于注册。

- U (大写)

此端口是无标记的 VLAN 成员。此 VLAN 中发送的帧在转发时不带 VLAN 标记。不带 VLAN 标记的帧通过此端口发送。

- u (小写)

此端口是无标记 VLAN 成员，但是此 VLAN 未组态为端口 VLAN。此 VLAN 中发送的帧在转发时不带 VLAN 标记。

- F

该端口不是指定 VLAN 的成员，即使该端口组态为中继端口，也无法成为此 VLAN 的成员。

- T

该选项只显示，无法在 WBM 中选择。

此端口是中继端口，可成为所有 VLAN 的成员。

切换基础网桥模式

VLAN 不识别 (802.1D 透明网桥) → VLAN 识别 (802.1Q VLAN 网桥)

如果将“基础网桥模式”(Base bridge mode) 从“VLAN 不识别”切换为“VLAN 识别”，则会产生以下影响

- 所有静态和动态单播条目都将被删除。
- 所有静态和动态多播条目都将被删除。
- 凭借生成树，可以设置以下协议兼容性：STP、RSTP 和 MSTP。

VLAN 识别 (802.1Q VLAN 网桥) → VLAN 不识别 (802.1D 透明网桥)

如果将“基础网桥模式”(Base bridge mode) 从“VLAN 识别”切换为“VLAN 不识别”，则会产生以下影响

- 所有 VLAN 组态均被删除。
- 绝对地址将创建一个管理 VLAN: VLAN 1。
- 所有静态和动态单播条目都将被删除。
- 所有静态和动态多播条目都将被删除。
- 凭借生成树，可以设置以下协议兼容性: STP 和 RSTP。
- 无法使用 GVRP。
- 无法使用访客 VLAN。
- 无法从 RADIUS 服务器采用 VLAN 分配。
- 可组态端口类型。

802.1Q VLAN 网桥: VLAN 的重要规则

组态和运行 VLAN 时，确保遵守以下规则:

- VLAN ID 为“0”的帧会按照无标记帧处理，但会保留其优先级值。
- 默认情况下，设备上的所有端口均发送不带 VLAN 标记的帧，以确保终端节点可接收这些帧。
- 对于 SCALANCE X 设备，所有端口的默认 VLAN ID 为“1”。
- 如果终端节点连接到端口，发送的离开帧不应带标记（静态访问端口）。但是，如果此端口有另一台交换机，则发送的帧应添加标记（中继端口）。

组态步骤

1. 如果未设置“802.1Q VLAN 网桥”(802.1Q VLAN bridge)，则从下拉列表“基础网桥模式”(Base Bridge Mode) 中选择条目“802.1Q VLAN 网桥”(802.1Q VLAN Bridge)。单击“设置值”(Set Values) 按钮。
2. 在“VLAN ID”输入框中输入 ID。
3. 单击“创建”(Create) 按钮。会在表中生成一个新条目。默认情况下，各个框均输入“-”。
4. 如果适用，输入 VLAN 的名称。

5.5 “第 2 层”菜单

5. 指定 VLAN 中端口的使用。例如，如果选择“M”，则该端口是 VLAN 的成员。此 VLAN 中发送的帧在转发时带有相应 VLAN 标记。
6. 单击“设置值”(Set Values) 按钮。

5.5.4.2 GVRP

组态 GVRP 功能

通过 GVRP 帧，不同设备可在设备的端口处注册特定 VLAN VID。不同设备可以是终端设备或交换机等。设备也可以通过此端口发送 GVRP 帧。可在此页面上启用各个端口的 GVRP 功能。

GARP VLAN Registration Protocol (GVRP)

General | **GVRP** | Port Based VLAN

GVRP

	Setting	Copy to Table
All ports	No Change	Copy to Table

Port	Setting
P0.1	<input type="checkbox"/>
P0.2	<input type="checkbox"/>
P0.3	<input type="checkbox"/>

显示框说明

该页面包含以下框：

- **GVRP**
启用或禁用 GVRP 功能。

表 1 包含以下列：

- **第 1 列**
说明设置对于表 2 的所有端口都有效。
- **设置 (Setting)**
从下拉列表中选择设置。可选择以下设置选项：
 - 启用 (Enabled)
启用发送 GVRP 帧。
 - 禁用 (Disabled)
禁用发送 GVRP 帧。
 - 无变化 (No change)
表 2 中无变化。
- **Copy to Table**
如果单击此按钮，将为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **端口 (Port)**
显示可用端口。端口由模块号和端口号组成，例如，端口 0.1 表示模块 0，端口 1。
- **设置 (Setting)**
启用或禁用发送 GVRP 帧。

组态步骤

1. 单击“GVRP”复选框。
2. 单击“Setting”(Setting) 列中端口之后的复选框以启用或禁用此端口的 GVRP。
对需要启用或禁用此功能的每个端口重复此操作。
3. 单击“设置值”(Set Values) 按钮。

5.5.4.3 基于端口的 VLAN

处理接收到的帧

在此页面中，指定用于接收帧的端口属性组态。

只有预先在“常规”(General) 选项卡上选择“基础网桥模式”(Base Bridge Mode) 802.1Q VLAN Bridge 时，才能在此页面上组态相关设置。

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

Port	Priority	Port VID	Acceptable Frames	Ingress Filtering
P0.1	0	VLAN1	All	<input type="checkbox"/>
P0.2	0	VLAN1	All	<input type="checkbox"/>
P0.3	0	VLAN1	All	<input type="checkbox"/>

显示框说明

表 1 包含以下列：

- **第 1 列**
显示设置对于所有端口有效。
- **优先级/端口 VID/可接受帧/入站过滤 (Priority / Port VID / Acceptable Frames / Ingress Filtering)**
在下拉列表中选择设置。如果选择“无变化”(No Change)，则表 2 中的条目保持不变。
- **Copy to Table**
如果单击此按钮，将为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **端口 (Port)**
显示可用端口。端口由模块号和端口号组成，例如，端口 0.1 表示模块 0，端口 1。
- **优先级 (Priority)**
VLAN 标记中使用的 CoS（服务类别）优先级。如果接收到无标记的帧，将为其分配此优先级。优先级指定了将该帧与其它帧相比较后，如何进一步处理该帧。
总共有 8 个优先级，值分别为 0 到 7，其中 7 表示最高优先级（IEEE 802.1p 端口优先级）。
从下拉列表中选择分配给无标记帧的优先级。
- **端口 VID (Port VID)**
从下拉列表中选择 VLAN ID。只能选择在“VLAN > General”页面中定义的 VLAN ID。如果接收到的帧没有 VLAN 标记，则会为其添加此处指定的 VLAN ID 作为标记，然后按照端口规则发送出去。

- **可接受帧 (Acceptable Frames)**

指定将接受哪些类型的帧。可能的选项如下：

- 仅限带标记的帧 (Tagged Frames Only)

设备会丢弃所有无标记帧。否则，按照组态应用转发规则。

- 全部 (All)

设备会转发所有帧。

- **入站过滤 (Ingress Filtering)**

指定是否评估已接收帧的 VID

可做以下选择：

- 启用

由接收到的帧的 VLAN ID 决定是否转发：要转发 VLAN

标记帧，接收端口必须是相同 VLAN 的成员。在接收端口会丢弃来自未知 VLAN 的帧。

- 禁用

转发所有帧。

组态步骤

1. 在待组态端口的行中，单击表格中的相关单元格进行组态。
2. 在以下输入框中输入要设置的值。
3. 从下拉列表中选择要设置的数值。
4. 单击“设置值”(Set Values) 按钮。

5.5 “第 2 层”菜单

5.5.5 镜像

5.5.5.1 常规

在此页面上，可以启用或禁用镜像功能并进行基本设置。

说明

在对数据通信进行镜像时，无法保证对所有数据包均进行了镜像。这主要取决于镜像端口上的负载以及会话数量。为了实现最大精度，建议将会话数量限制为一个。

注意数据传输率

如果镜像端口的最大数据速率大于监视端口的最大数据速率，则数据可能丢失，同时监视端口不再反映镜像端口上的数据通信。可同时将多个端口镜像到一个监视端口。

同一个 VLAN 的多个源端口

如果在 VLAN 中为基于端口的出口镜像选择了多个源端口，则仅向目标端口转发一次未知单播与组播帧以及广播帧。

设置

Mirroring General

General | Port

Mirroring
 Monitor Barrier

Select	Session ID	Session Type	Status	Dest. Port
<input type="checkbox"/>	1	Port Based	inactive	-

1 entry.

Create Delete Set Values Refresh

该页面包含以下框：

- **镜像**

单击此复选框启用或禁用镜像。

说明

如果想要将常规终端设备连接到监视端口，则需禁用端口镜像功能。

- **监视屏障**

单击此复选框启用或禁用“监视屏障”(Monitor Barrier)。

说明

监视屏障的影响

如果启用此选项，则无法再通过监视端口来管理交换机。以下端口特定功能将发生变化：

- “DCP 转发”(DCP Forwarding) 关闭。
- LLDP 关闭。
- 单播、组播和广播阻止开启。

再次禁用监视屏障后，无法恢复这些功能的先前状态。它们会复位为默认值，可能需要重新组态。

即使开启监视屏障时，也可手动组态这些功能。重新允许监视端口上的数据通信。如果不需要，则确保只将想要监视的数据通信转发到接口。

如果禁用镜像，所列的端口特定功能将复位为默认值。无论功能是手动组态还是通过启用“监视屏障”(Monitor Barrier) 自动组态，都将发生复位。

基本设置表格包括以下对话框：

- **选择 (Select)**

选择要删除的行。

- **会话 ID (Session ID)**

创建新条目时，将自动分配会话 ID。只可创建一个会话。

- **会话类型 (Session Type)**

显示镜像会话的类型。

5.5 “第 2 层”菜单

- **状态 (Status)**

显示是否已启用镜像。

- **目标端口**

从该下拉列表中，选择作为此会话期间数据镜像目标的输出端口。

步骤

创建镜像会话

1. 激活镜像。
2. 单击“创建”(Create) 按钮在表中创建条目。
将自动分配会话 ID。
3. 选择目标端口。
4. 单击“设置值”(Set Values) 按钮保存并激活所选设置。
5. 切换至以下选项卡为会话 ID 进行更详细的设置。

删除镜像会话

1. 单击首列的复选框选择行。
2. 单击“删除”(Delete) 按钮可删除所选行。

5.5.5.2 端口

镜像端口

仅当已在“常规”(General) 选项卡中生成会话类型设置为“基于端口”(Port-based) 的会话 ID 时，才能在此页面上组态相关设置。

Port	Ingress Mirroring	Egress Mirroring
P0.1	<input type="checkbox"/>	<input type="checkbox"/>
P0.2	<input type="checkbox"/>	<input type="checkbox"/>
P0.3	<input type="checkbox"/>	<input type="checkbox"/>

显示框说明

该页面包含以下框：

- **会话 ID (Session ID)**

显示会话。

- **端口 (Port)**

显示所有可用端口。端口由模块号和端口号组成，例如，端口 0.1 表示模块 0，端口 1。

- **进站镜像 (Ingress Mirroring)**

启用或禁用监听所需端口的进站数据包。

- **出站镜像 (Egress Mirroring)**

启用或禁用监听所需端口的出站数据包。

说明

环网端口的镜像

如果启用环网端口的镜像功能，则环网端口即使在“链路中断”状态下也会发送测试帧。

组态步骤

1. 在表格中，单击待镜像端口后的行复选框。
选择要监视进入数据包还是离开数据包。
要监视端口的整个数据通信，请同时选中这两个复选框。
2. 单击“设置值”(Set Values) 按钮。

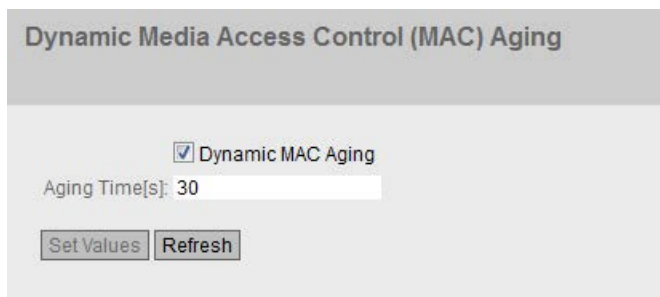
5.5.6 动态 MAC 老化

协议设置和交换机功能

设备自动学习连接节点的源地址。此信息用于将数据帧转发到具体涉及的节点。这将减少其它节点的网络负载。

如果设备在特定时间内未收到源地址与学习的地址相匹配的帧，则设备会删除学习的地址。这种机制称为“**Aging**”。老化可以防止错误地转发帧，例如当某个终端设备连接到不同的交换机端口时。

如果未启用该复选框，则设备不会自动删除学习的地址。



显示框说明

该页面包含以下框：

- **动态 MAC 老化 (Dynamic MAC Aging)**

启用或禁用获取的 MAC 地址的自动老化功能。

- **老化时间[s] (Aging Time[s])**

以步长 15

输入秒数时间值。经过此时间后，如果设备没有从该发送方地址接收到任何其它帧，则会删除获取的地址。

取值范围：15 - 630 (秒)

出厂设置：30

说明

对数值取整，与期望值的偏差

输入“老化时间”(Aging Time) 时，请注意 WBM 会取整为正确的值。如果输入的值不能被 15 整除，则会自动向下取整。

组态步骤

1. 选中“Dynamic MAC Aging”复选框。
2. 在“老化时间[s]”(Aging Time[s]) 输入框中输入时间（以秒为单位）。
3. 单击“设置值”(Set Values) 按钮。

5.5.7 环网冗余

5.5.7.1 环网

组态环网冗余

- **环网冗余 (Ring Redundancy)**
如果选中“Ring Redundancy”复选框，将启用环网冗余。将使用此页面上设置的环网端口。
- **环网冗余模式 (Ring Redundancy mode)**
在此设置环网冗余的模式。
可使用以下模式：
 - **Automatic Redundancy Detection**
选择此设置可创建冗余模式的自动组态。
在“自动冗余检测”模式下，设备会自动检测环网中是否存在充当“HRP 管理器”角色的设备。如果存在，该设备将获得“HRP”客户端的角色。如果未找到 HRP 管理器，则所有设置为“自动冗余检测”或“MRP 自动管理器”的设备将通过彼此协商来确定哪台设备将获得“MRP

5.5 “第 2 层”菜单

管理器”的角色。MAC 地址最低的设备将始终为“MRP 管理器”。其余设备将自动设置为“MRP 客户端”模式。

– MRP 自动管理器 (MRP Auto-Manager)

在“MRP 自动管理器”模式下，设备通过彼此协商来确定哪个设备获得“MRP 管理器”的角色。MAC 地址最低的设备将始终为“MRP 管理器”。其余设备将自动设置为“MRP 客户端”模式。

与“自动冗余检测”(Automatic Redundancy Detection) 设置不同，设备在此模式下无法检测环网中是否存在 HRP 管理器。

说明

STEP 7 中的 MRP 组态

如果在 STEP 7 中为设备设置“管理器（自动）”或“管理器”角色，则在两种情况下，“MRP 自动管理器”都会显示在该 WBM 页面中。在 CLI 的显示中，会对这两个角色进行区分。

– MRP 客户端 (MRP Client)

设备采用 MRP 客户端角色。

– HRP 客户端 (HRP Client)

设备采用 HRP 客户端角色。

– HRP 管理器 (HRP Manager)

设备采用 HRP 管理器角色。

组态 HRP 环网时，必须将其中一个设备设置为 HRP 管理器。针对所有其它设备，必须设置“HRP 客户端”或“自动冗余检测”。

- **环网端口 (Ring ports)**

在此设置将在环网冗余中用作环网端口的端口。

在左侧下拉列表中选择环网端口是 HRP 中的“隔离端口”。

出厂设置定义了以下环网端口：

设备	环网端口出厂设置
SCALANCE XB208 和 XB216	P0.1 和 P0.2
SCALANCE XB205-3	P0.7 和 P0.8
SCALANCE XB213-3	P0.15 和 P0.16
SCALANCE XC206-2SFP、XC208、XC216 和 XC224	P0.1 和 P0.2
SCALANCE XC206-2	P0.7 和 P0.8
SCALANCE XP208	P0.1 和 P0.2
SCALANCE XP216	P0.10 和 P0.12

- **Observer**

启用或禁用观察器。“Observer”功能仅在 HRP 环网中可用。

在左侧的下拉列表中选择环网端口连接到 HRP 管理器的“隔离端口”。

观察器可对冗余管理器故障或 HRP 环网的错误组态情况进行监视。

如果启用了观察器，则其可以在检测到错误时中断已连接的环网。为此，观察器将一个环网端口切换至“屏蔽”状态。错误消除后，观察器再次启用该端口。

- **重启观察器 (Restart Observer)**

如果连续发生许多错误，则观察器不再自动启用其端口。环网端口会一直保持在“屏蔽”状态。这种现象通过错误 LED 和消息文本进行指示。

错误消除后，可使用“重启观察器”(Restart Observer) 按钮再次启用端口。

组态步骤

1. 选择“环网冗余”(Ring Redundancy) 复选框。
2. 选择冗余模式。
3. 指定环网端口。
4. 单击“设置值”(Set Values) 按钮。

恢复出厂设置

EtherNet/IP 型号

如果已恢复了出厂默认设置，将禁用环网冗余并复位环网端口设置。生成树已启用。

PROFINET 型号

如果已恢复出厂默认设置，将启用环网冗余。如果复位为出厂设置，也会复位环网端口设置。如果复位前已将其它端口用作环网端口，则之前已正确组态的设备可能会导致帧循环传送，从而导致数据通信故障。

更改带有冗余管理器 (HRP) 的环网端口的状态

如果组态冗余管理器，请设置环网端口的状态。第一个环网端口改为“**blocking**”状态，第二个环网端口改为“**forwarding**”状态。只要启用环网冗余，就无法更改这些环网端口的状态。

说明

确保首先断开环网，使网络中没有帧循环。

更改环网端口

要更改环网端口，请按以下步骤操作：

1. 打开环网。
2. 选择新的环网端口。
3. 更改电缆连接。
4. 关闭环网。

5.5.7.2 备用

冗余环网连接

备用冗余支持 HRP 环网的冗余链路。

要建立备用连接，需将环网中两个相邻设备组态为备用主站或备用从站。备用主站和备用从站必须通过并行电缆连接至另一个环网中的两个设备。

在无故障运行中，通过主站在两个环网之间交换消息。如果主站线路受到干扰，从站会接管两个环网之间的消息转发。

为两个备用伙伴启用备用冗余，并选择用于将设备与想要链接到的环网相连接的端口。

对于“备用连接名称”(Standby Connection Name)，必须为两个伙伴指定一个在环网中唯一的名称。该名称标识彼此为备用伙伴的两个模块。

说明

为了能够使用此功能，必须激活 HRP。

备用管理器始终需要一台已激活的 HSR 客户端或 HSR 管理器。

显示框说明

- Standby**
 启用或禁用备用功能。
- Standby Connection Name**
 该名称定义了主/从设备对。两个设备必须处于同一个环网中。
 在此处输入备用连接的名称。该名称必须与在备用伙伴上输入的名称相同。您可以选择满足需要的任何名称，但是在整个网络中一个名称仅可用于一对设备。

5.5 “第 2 层”菜单

- **Force device to Standby Master**

如果选中该复选框，则会将设备组态为备用主站，这与其 MAC 地址无关。

- 如果没有为任一启用了备用主站的设备选中该复选框，则会假定未发生任何错误，并且 MAC 地址较高的设备会成为备用主站。
- 如果为两台设备都选择了该选项，或只有一台设备支持“将设备强制为备用主站”(Force device to Standby Master) 属性，则也会根据 MAC 地址选择备用主站。

这种类型的分配很重要，尤其是在更换设备时。根据 MAC 地址，前一台具有从站功能的设备可接管备用主站角色。

说明

如果两个设备通过备用功能相链接，则这两个设备上都必须启用了“备用”(Standby) 功能。

- **备用端口 (Standby Port)**

选择要作为备用端口的端口。通过备用端口链接到其它环网。

备用端口参与数据通信的重新导向。在没有故障的情况下，仅启用主站的备用端口来处理进入相连 HRP 环网或 HRP 总线的数据通信。

如果主站或主站上某备用端口的以太网连接出现故障，将禁用主站的备用端口，并启用从站的备用端口。因此，到所连接网段（HRP 环网或 HRP 线性总线）的以太网连接都能恢复正常。

5.5.8 生成树

5.5.8.1 常规

生成树的常规设置

这是生成树的基本页面。从下拉列表中选择兼容模式。

在这些功能的组态页面上，可进行进一步设置。

根据具体的兼容性模式，可以在相关组态页面组态相应的功能。

Spanning Tree Protocol (STP) General

General | CIST General | CIST Port | MST General | MST Port | Enhanced Passive Listening Compatibility

Spanning Tree Protocol Compatibility: MSTP ▾

Set Values Refresh

显示框说明

该页面包含以下框：

- **Spanning Tree**
启用或禁用生成树。
- **协议兼容性 (Protocol Compatibility)**
选择协议兼容性。可使用以下设置：
 - STP
 - RSTP
 - MSTP

组态步骤

1. 选中“生成树”(Spanning Tree) 复选框。
2. 从“Protocol Compatibility”下拉列表中选择兼容类型。
3. 单击“设置值”(Set Values) 按钮。

5.5.8.2 CIST 概述

MSTP-CIST 组态

此页面由以下几部分组成。

- 页面的左侧显示设备的组态。
- 中间部分显示根网桥的组态，该组态可从设备接收到的生成树帧获得。
- 右侧显示区域根网桥的组态，该组态可从 MSTP 帧获得。只有在“General”页面上启用“Spanning Tree”，以及为“Protocol

5.5 “第 2 层”菜单

Compatibility”设置“MSTP”时，显示的数据才可见。这同样适用于“Bridge Max Hop Count”参数。如果设备是根网桥，则左右两侧显示的信息相匹配。

Common Internal Spanning Tree (CIST) General					
General	CIST General	CIST Port	MST General	MST Port	Enhanced Passive Listening Compatibility
Bridge Priority: 32768	Root Priority: 0	Regional Root Priority: 0			
Bridge Address: 00-00-00-00-00-00	Root Address: 00-00-00-00-00-00	Regional Root Address: 00-00-00-00-00-00			
Root Port: -	Root Cost: 0	Regional Root Cost: 0			
Topology Changes: 0	Last Topology Change: -	Region Name: 00:1b:1b:40:91:23			
Bridge Hello Time[s]: 2	Root Hello Time[s]: 2	Region Version: 0			
Bridge Forward Delay[s]: 15	Root Forward Delay[s]: 15				
Bridge Max Age[s]: 20	Root Max Age[s]: 20				
Bridge Max Hop Count: 20					
<input type="button" value="Reset Counters"/>					
<input type="button" value="Set Values"/> <input type="button" value="Refresh"/>					

显示框说明

该页面包含以下框：

- **Bridge Priority/Root Priority**

将根据 Bridge Priority 确定哪台设备会成为 Root Bridge。优先级最高的 Bridge 会成为 Root Bridge。数值越小，优先级越高。如果网络中有多个设备具有相同优先级，则 MAC 地址数值最小的设备将成为根网桥。网桥优先级和 MAC 地址这两个参数一起构成

网桥标识符。由于根网桥管理所有路径的变更，出于帧延迟的考虑，根网桥应该尽可能处在中心位置。

网桥优先级的值是 4096 的整数倍。取值范围：0 - 61440

- **网桥地址 (Bridge Address)/根地址 (Root Address)**

网桥地址显示设备的 MAC 地址，根地址显示根网桥的 MAC 地址。

- **Root port**

显示交换机与根网桥通信时所使用的端口。

- **根成本 (Root Cost)**

从该设备到根网桥的路径成本。

- **拓扑变更 (Topology Changes)/上次拓扑变更 (Last Topology Change)**
该设备条目显示自上次启动以来，由于生成树机制而执行的重新组态操作次数。对于根网桥，自上次重新组态到现在的时间显示如下：
 - 秒：数字后的单位为“秒”(sec)
 - 分钟：数字后的单位为“分钟”(min)
 - 小时：数字后的单位为“小时”(hr)
- **网桥呼叫时间 [s] (Bridge hello time [s])/根呼叫时间 [s] (Root hello time [s])**
每个网桥都会定期发送组态帧 (BPDU)。“呼叫时间”(Hello Time) 即为两个组态帧之间的时间间隔。
出厂设置：2 秒

说明

只有使用“协议兼容性”(Protocol compatibility) RSTP 时才能对“网桥呼叫时间”(Bridge Hello Time) 进行设置。如果设置了“协议兼容性”(Protocol compatibility) MSTP，则将使用“第 2 层 > 生成树 > CIST 端口”(Layer 2 > Spanning Tree > CIST Port) 页面上的“呼叫时间”(Hello Time) 参数。

- **网桥转发延迟[s] (Bridge Forward Delay[s])/根转发延迟 [s] (Root Forward Delay[s])**
网桥不会立即使用新组态数据，而是在“转发延迟”(Forward Delay) 参数中指定的时间段过后才使用。这样可确保只有在所有网桥均获得所需信息之后才以新拓扑运行。
出厂设置：15 秒
- **网桥最大老化时间[s](Bridge Max Age[s])/根最大老化时间[s](Root Max Age[s])**
如果 BPDU 大于指定的“最大老化时间”(Max Age)，则被丢弃。
出厂设置：20 秒
- **Regional root priority**
相关描述，请参见“网桥优先级/根优先级”
- **区域根地址 (Regional Root Address)**
设备的 MAC 地址。
- **区域根成本 (Regional Root Cost)**
从该设备到根网桥的路径成本。
- **网桥最大跳跃数 (Bridge Max Hop Count)**
此参数指定 BPDU 会通过多少个 MSTP 节点。如果接收到一个 MSTP BPDU 并且其跳跃计数超过此处组态的值，则会将其丢弃。此参数默认为 20。

5.5 “第 2 层”菜单

- **区域名称 (Region Name)**
输入此设备所属的 MSTP 区域的名称。默认情况下，在此处输入此设备的 MAC 地址。所有属于相同 MSTP 区域的设备上的值必须相同。
- **区域版本 (Region Version)**
输入设备所在的 MSTP 区域的版本号。在属于相同 MSTP 区域的所有设备上，该值必须相同。
- **复位计数器 (Reset Counters)**
单击该按钮可复位此页面上的计数器。

组态步骤

1. 在输入框中输入组态所需的数据。
2. 单击“设置值”(Set Values) 按钮。

5.5.8.3 CIST 端口

MSTP-CIST 端口组态

调用此页面时，表中显示端口参数组态的当前状态。

要进行组态，请单击端口表中的相关单元格。

Common Internal Spanning Tree (CIST) Port

General | CIST General | CIST Port | MST General | MST Port | Enhanced Passive Listening Compatibility

Spanning Tree Status Copy to Table
All ports No Change Copy to Table

Port	Spanning Tree Status	Priority	Cost Calc.	Path Cost	State	Fwd. Trans.	Edge Type	Edge	P.t.P. Type	P.t.P.	Hello Time
P0.1	<input checked="" type="checkbox"/>	128	0	200000	Forwarding	1	Auto	<input type="checkbox"/>	-	<input checked="" type="checkbox"/>	2
P0.2	<input checked="" type="checkbox"/>	128	0	200000	Discarding	0	Auto	<input type="checkbox"/>	-	<input type="checkbox"/>	2
P0.3	<input checked="" type="checkbox"/>	128	0	200000	Discarding	0	Auto	<input type="checkbox"/>	-	<input type="checkbox"/>	2
P0.4	<input checked="" type="checkbox"/>	128	0	200000	Discarding	0	Auto	<input type="checkbox"/>	-	<input type="checkbox"/>	2

Set Values Refresh

显示框说明

表 1 包含以下列：

- **第 1 列**
说明设置对于表 2 的所有端口都有效。
- **生成树状态 (Spanning Tree Status)**
从下拉列表中选择设置。可选择以下设置选项：
 - 启用 (Enabled)
将端口集成到生成树中。
 - 禁用 (Disabled)
不将端口集成到生成树中。
 - 无变化 (No change)
表 2 保持不变。
- **复制到表中 (Copy to Table)**
如果单击此按钮，将为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **端口 (Port)**
显示可用端口。端口由模块号和端口号组成，例如，端口 0.1 表示模块 0，端口 1。
- **生成树状态 (Spanning Tree Status)**
指定是否将端口集成到生成树中。

说明

如果禁用端口的“生成树状态”(Spanning Tree Status) 选项，可能导致形成环路。必须留意拓扑。

- **优先级 (Priority)**
输入端口的优先级。仅当路径成本相同时才评估优先级。
该值必须能被 16 整除。如果该值不能被 16 整除，则会自动调整该值。
取值范围：0 - 240。
默认值为 128。
- **Cost Calc.**
输入路径成本计算。如果在此输入值“0”，则自动计算出的值会显示在“路径成本”(Path costs) 框中。
- **路径开销 (Path Cost)**
此参数用于计算将要选择的路径。选择值最小的路径作为路径。如果设备的多个端口的路径开销值相同，则选择端口号最小的端口。

5.5 “第 2 层”菜单

如果“开销计算”(Cost Calc)

中的值为“0”，则会显示自动计算出的值。否则会显示“开销计算”(Cost Calc.) 框的值。主要根据传输速度来计算路径开销。可达到的传输速度越高，路径成本的值就越低。

快速生成树的典型路径成本值如下：

- 10,000 Mbps = 2,000
- 1000 Mbps = 20,000
- 100 Mbps = 200,000
- 10 Mbps = 2,000,000

但是，也可以单独设置各个值。

- **状态 (Status)**

显示端口的当前状态。这些值只能显示，但无法组态。状态 (Status) 参数取决于组态的协议。可能的值包括：

- **Disabled**
该端口仅接收，并且不包括在 STP、MSTP 和 RSTP 中。
- **Discarding**
在“Discarding”模式下，接收 BPDU 帧。其它进入或离开的帧会被丢弃。
- **listening**
在此状态下，接收和发送 BPDU。端口包括在生成树算法中。
- **学习 (Learning)**
“转发”(Forwarding)
状态之前的阶段，端口主动学习拓扑（换句话说，节点寻址）。
- **Forwarding**
在重新组态时间后，端口在网络中激活；端口接收和转发数据帧。

- **转发传输 (Fwd. Trans)**

指定从“Discarding”状态变为“Forwarding”状态的次数。

- **边缘类型 (Edge Type)**

指定“边缘端口”的类型。可做以下选择：

- “-”

禁用边缘端口。端口被视为“无边缘端口”。

- **Admin**

当此端口上始终有终端设备时，选择此选项。否则，每次更改连接时都会触发对网络的重新组态。

- **Auto**

如果想要自动检测此端口上连接的终端设备，则选择此选项。首次建立连接时，会将端口视为“无边缘端口”。

- **Admin/Auto**

如果要在该端口上结合这两个选项，则同时选择这些选项。首次建立连接时，会将端口视为“边缘端口”。

- **边缘 (Edge)**

显示端口的状态。

- **Enabled**

终端设备连接到此端口。

- **Disabled**

此端口上有生成树或快速生成树设备。

有了终端设备，交换机可以通过端口更快地进行切换，而无需考虑生成树帧。如果忽略此设置而接收生成树帧，则该端口将自动切换为“禁用”设置。

- **P.t.P.Type**

从下拉列表中选择所需选项。选择项取决于设置的端口。

- “-”

自动计算点对点。如果端口被设置为半双工，则不认为是点对点链路。

- **P.t.P.**

即使为半双工，也认为是点对点链路。

- **共享介质 (Shared Media)**

即使为全双工连接，也不认为是点对点链路。

说明

点对点连接表示在两个设备之间直接连接。而共享介质连接可以是与集线器的连接。

5.5 “第 2 层”菜单

- **呼叫时间 (Hello Time)**

输入时间间隔，经过该时间后，网桥会发送组态帧 (BPDU)。默认情况下，会设置 2 秒。

值范围：1-2 秒

说明

只有使用“协议兼容性”(Protocol compatibility) MSTP 时才能对呼叫时间进行端口特定的设置。如果设置了“协议兼容性”(Protocol compatibility) RSTP，则将使用“第 2 层 > 生成树 > CIST 端口”(Layer 2 > Spanning Tree > CIST Port) 页面上的“网桥呼叫时间”(Bridge Hello Time) 参数。

组态步骤

1. 在表行的输入单元格中，输入要组态的端口值。
2. 在表行单元格的下拉列表中，选择要组态的端口值。
3. 单击“设置值”(Set Values) 按钮。

5.5.8.4 MST General

多重生成树组态

除 RSTP 之外，通过 MSTP 也可以在 LAN 中使用单独的 RSTP 树管理多个 VLAN。

Select	MSTP Instance ID	Root Address	Root Priority	Bridge Priority	VLAN ID
<input type="checkbox"/>	1	00-00-00-00-00-00	0	32768	

说明

该页面包含以下框：

- **MSTP Instance ID**
输入 MSTP 实例数。
允许值：1 - 64

该表格包括以下列：

- **Select**
选择要删除的行。
- **MSTP instance ID**
显示 MSTP 实例数。
- **根地址 (Root Address)**
显示根网桥的 MAC 地址。
- **Root Priority**
显示根网桥的优先级。
- **Bridge Priority**
在此框中输入网桥优先级。网桥优先级的值是 4096 的整数倍数，值范围从 0 到 61440。
- **VLAN ID**
输入 VLAN ID。在此处还可以通过“起始 ID”、“-”、“结束 ID”来指定范围。用“,”分隔多个范围或 ID。
允许值：1- 4094

步骤

创建新条目

1. 在“MSTP Instance ID”框中输入 MSTP 实例数。
2. 单击“创建”(Create) 按钮。
3. 在“VLAN ID”输入框中输入 VLAN 的 ID。
4. 在“Bridge Priority”框中输入网桥的优先级。
5. 单击“设置值”(Set Values) 按钮。

5.5 “第 2 层”菜单

删除条目

1. 使用相关行开始位置的复选框，选择要删除的条目。
2. 单击“Delete”按钮从内存中删除所选的条目。从设备的内存中删除条目并更新该页面的显示。

5.5.8.5 MST 端口

组态多重生成树端口参数

在此页面，设置所组态多重生成树实例的端口参数。

Multiple Spanning Tree (MST) Port

General CIST General CIST Port MST General MST Port Enhanced Passive Listening Compatibility

MSTP Instance ID: 1

MSTP Status	Copy to Table
All ports No Change	Copy to Table

Port	MSTP Instance ID	MSTP Status	Priority	Cost Calc.	Path Cost	State	Fwd. Trans.
P0.1	1	<input checked="" type="checkbox"/>	128	0	200000	Forwarding	1
P0.2	1	<input checked="" type="checkbox"/>	128	0	200000	Discarding	0
P0.3	1	<input checked="" type="checkbox"/>	128	0	200000	Discarding	0
P0.4	1	<input checked="" type="checkbox"/>	128	0	200000	Discarding	0

Set Values Refresh

显示框说明

该页面包含以下框：

- **MSTP Instance ID**
在下拉列表中选择 MSTP 实例的 ID。

表 1 包含以下列：

- **第 1 列**
显示设置对于所有端口有效。
- **MSTP 状态 (MSTP Status)**
从下拉列表中选择设置。可选择以下设置选项：
 - 启用 (Enabled)
 - 禁用 (Disabled)
 - 无变化 (No Change)：表 2 保持不变。
- **复制到表中 (Copy to Table)**
如果单击此按钮，将为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **端口 (Port)**
显示所有可用端口和链路汇聚。
- **MSTP Instance ID**
MSTP 实例的 ID。
- **MSTP 状态 (MSTP Status)**
单击此复选框可启用或禁用此选项。
- **优先级 (Priority)**
输入端口的优先级。仅当路径成本相同时才评估优先级。
该值必须能被 16 整除。如果该值不能被 16 整除，则会自动调整该值。
取值范围：0 - 240。
出厂设置：128
- **Cost Calc.**
在该输入框中输入路径成本计算。如果在此输入值“0”，则“路径成本”(Path Costs)框中会显示自动计算出的值。

5.5 “第 2 层”菜单

- **Path Cost**

从该端口到根网桥的路径成本。选择值最小的路径作为路径。如果设备的多个端口具有相同的值，则选择端口号最小的端口。

如果“成本计算”(Cost Calc.)

为“0”，则显示自动计算出的值。否则会显示“开销计算”(Cost Calc.) 框的值。

主要根据传输速度来计算路径开销。可达到的传输速度越高，路径成本的值就越低。

快速生成树的典型值如下：

- 10,000 Mbps = 2,000
- 1000 Mbps = 20,000
- 100 Mbps = 200,000
- 10 Mbps = 2,000,000

但是，也可以单独设置各个值。

- **Status**

显示端口的当前状态。这些值只能显示，但无法组态。可能的状态有：

- **放弃 (Discarding)**
端口会交换 MSTP 信息，但不会参与数据通信。
- **阻止 (Blocked)**
在阻止模式下，接收 BPDU 帧。
- **转发 (Forwarding)**
端口接收和发送数据帧。

- **Fwd.Trans.**

指定端口状态从 Discarding 到 Forwarding 或从 Forwarding 到 Discarding 的变化次数。

组态步骤

1. 在表行的输入单元格中，输入要组态的端口值。
2. 在表行单元格的下拉列表中，选择要组态的端口值。
3. 单击“设置值”(Set Values) 按钮。

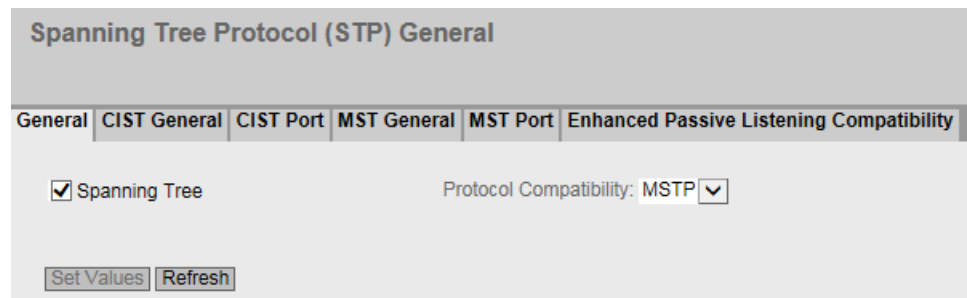
5.5.8.6 增强的被动侦听兼容性

生成树和环网冗余

如果启用“增强的被动侦听兼容性”(Enhanced Passive Listening Compatibility)，将通过 RSTP 边缘端口发送拓扑变更通知。要将生成树网络与 HRP 环网连接起来，必须将此参数与“边缘类型”功能结合在一起（请参见“第 2 层 > 生成树 > CIST 端口”）。否则将不会通过边缘端口发送 TCN 帧；但这对环网节点上的被动侦听功能来说是必要的。

启用该功能

在此页面上，可启用“增强的被动侦听兼容性”功能。



显示框说明

该页面包含以下框：

- **增强的被动侦听兼容性 (Enhanced Passive Listening Compatibility)**
为整个设备启用或禁用此功能。

组态步骤

1. 启用或禁用“增强的被动侦听兼容性”(Enhanced Passive Listening Compatibility)
2. 单击“设置值”(Set Values) 按钮。

5.5.9 回路检测

使用“回路检测”(Loop detection)

功能时，需指定要激活回路检测功能的端口。所涉及的端口会发送特殊的测试帧，即回路测试帧。如果这些帧被发送回设备，则说明存在回路。

5.5 “第 2 层”菜单

如果存在与此设备相关的“本地回路”，则将在同一设备的不同端口再次接收到这些帧。如果再次在同一端口接收到已发送的帧，则说明存在与其它网络组件相关的“远程回路”(Remote Loop)。

说明

回路是必须消除的网络结构错误。回路检测有助于更快地找到此错误，但并不会消除相关错误。回路检测不适用于通过故意包含回路来提高网络可用性的情况。

说明

请注意，仅可为未组态为环网端口或备用端口的端口激活回路检测。

Loop Detection

Loop Detection
 VLAN Loop Detection

	Threshold	Remote Reaction	Local Reaction	Copy to Table
All ports	No Change	No Change	No Change	Copy to Table

Port	Setting	Threshold	Remote Reaction	Local Reaction	Status	Source Port	Source VLAN	Reset
P0.1	forwarder	2	disable	disable	active	-	-	Reset
P0.2	forwarder	2	disable	disable	active	-	-	Reset
P0.3	forwarder	2	disable	disable	active	-	-	Reset
P0.4	forwarder	2	disable	disable	active	-	-	Reset

显示框说明

该页面包含以下框：

- **回路检测 (Loop Detection)**
启用或禁用回路检测。
- **VLAN 回路检测 (VLAN Loop Detection)**
启用或禁用 VLAN 回路检测。

表 1 包含以下列：

- **第 1 列**
说明设置对于表 2 的所有端口都有效。
- **阈值/远程反应/本地反应 (Threshold Value / Remote Reaction / Local Reaction)**
进行所需设置。
- **复制到表 (Copy to Table)**
如果单击此按钮，将为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **“端口”(Port)**
显示可用端口。

- **设置 (Setting)**
指定端口处理回路检测帧的方式。从下拉列表中选择下列选项之一：

说明

测试帧会导致额外的网络负载。建议您仅在环网的分支点处等将单独的交换机组态为“Sender”，并将其它交换机组态为“Forwarder”。

- 发送方 (Sender)
发送并转发回路检测帧。
- 转发方 (Forwarder)
转发来自其它设备的回路检测帧。
- 阻止 (blocked)
阻止转发回路检测帧。
- **阈值 (Threshold)**
通过输入一个数值指定接收到多少回路检测帧后才视为存在回路。
- **远程反应 (Remote Reaction)**
指定在出现远程回路时端口的响应方式。从下拉列表中选择两个选项之一：
 - 无操作 (No action): 回路对端口不起作用。
 - 禁用 (Disable): 屏蔽端口。
- **本地反应 (Local reaction)**
指定在出现本地回路时端口的响应方式。从下拉列表中选择两个选项之一：
 - 无操作 (No action): 回路对端口不起作用。
 - 禁用 (Disable): 屏蔽端口
- **状态 (Status)**
该框显示对此端口是启用还是禁用回路检测。
- **源端口 (Source Port)**
显示触发了上一次响应的回路检测帧的接收端口。

5.5 “第 2 层”菜单

- **源 VLAN (Source VLAN)**

该框显示触发了上一次响应的回路检测帧的 VLAN ID。

这需要选中“VLAN 回路检测”(VLAN Loop Detection) 复选框。

- **重置 (Reset)**

消除网络中的回路后，可单击“重置”(Reset) 按钮再次重置端口。

使用回路检测更改已组态的端口状态

端口状态的组态可使用“回路检测”功能更改。例如，如果管理员已 disabled 某个端口，则可在使用“enabled”重启设备后再次启用此端口。“回路检测”不会更改“Link down”端口状态。

5.5.10 链路汇聚

捆绑网络连接以实现冗余和更高带宽

根据 IEEE

802.3AD，链路汇聚允许将相邻设备之间的多个连接捆绑在一起，以实现更高的带宽并防止发生故障。

两个伙伴设备中的端口均包括在链路汇聚中，通过这些端口连接设备。要将端口正确分配给伙伴设备，应使用 IEEE 802.3AD 标准中的链路汇聚控制协议 (LACP)。

可最多定义 8 个链路汇聚。最多可为每个链路汇聚分配 8 个端口。

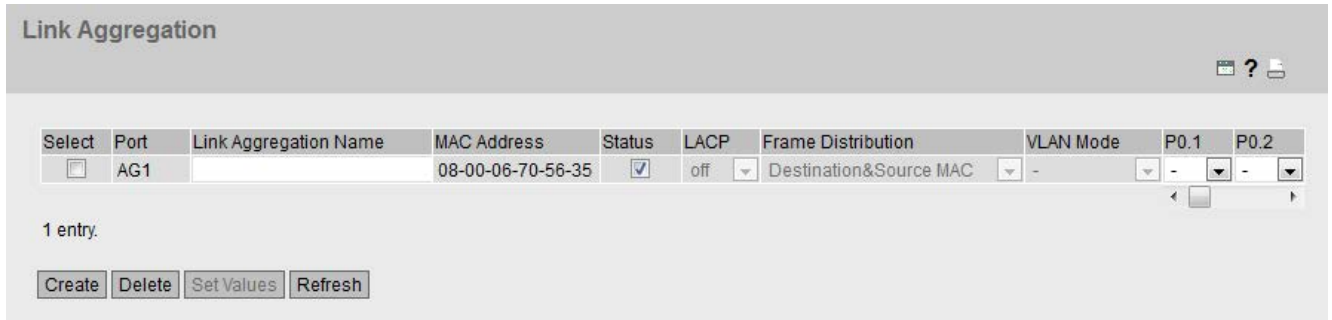
说明

当端口已分配给链路汇聚但未激活（例如链路中断）时，显示的值与为链路汇聚组态的值可能不同。

如果链路汇聚中的端口激活，则会使用链路汇聚的组态值覆盖 DCP 转发等各个端口组态。

显示已组态的汇聚

该页面显示所有已组态的链路汇聚。



The screenshot shows a web interface titled "Link Aggregation". It contains a table with the following columns: Select, Port, Link Aggregation Name, MAC Address, Status, LACP, Frame Distribution, VLAN Mode, P0.1, and P0.2. There is one row of data with the following values: in the Select column, AG1 in the Port column, an empty text box in the Link Aggregation Name column, 08-00-06-70-56-35 in the MAC Address column, a checked checkbox in the Status column, off in the LACP column, Destination&Source MAC in the Frame Distribution column, - in the VLAN Mode column, - in the P0.1 column, and - in the P0.2 column. Below the table, it says "1 entry." and there are four buttons: Create, Delete, Set Values, and Refresh.

Select	Port	Link Aggregation Name	MAC Address	Status	LACP	Frame Distribution	VLAN Mode	P0.1	P0.2
<input type="checkbox"/>	AG1		08-00-06-70-56-35	<input checked="" type="checkbox"/>	off	Destination&Source MAC	-	-	-

1 entry.

显示框说明

该表格包括以下列：

- **Select**
选择要删除的行。
- **端口 (Port)**
显示此链路汇聚的虚拟端口号。该标识符是由固件内部分配的。
- **链路汇聚名称 (Link Aggregation Name)**
显示链路汇聚的名称。此名称可由用户在组态期间指定。名称并非绝对必要，但对于区分多个链路汇聚会很有用。
- **MAC Address**
显示 MAC 地址。
- **状态 (Status)**
启用或禁用链路汇聚。
- **LACP**
 - 开启 (On)
启用发送 LACP 帧。
 - 关闭 (Off)
禁用发送 LACP 帧。
- **帧分发 (Frame Distribution) - 目标 MAC 和源 MAC (Destination&Source MAC)**
根据目标 MAC 地址与源 MAC 地址的组合将数据包分发给汇聚的各个链路。

5.5 “第 2 层”菜单

- **VLAN Mode**

指定在 VLAN 中如何登记链路汇聚：

- 混合 (Hybrid)
链路汇聚发送有标记和无标记的帧。它不会自动成为 VLAN 的成员。
- 中继 (Trunk)
链路汇聚仅发送有标记的帧，并且自动成为所有 VLAN 的成员。

- **端口 (Port)**

显示属于此链路汇聚的端口。可以从下拉列表中选择下列值：

- “-” (禁用)
链路汇聚已禁用。
- “a” (主动)
端口发送 LACP 帧，并只在接收到 LACP 帧时参与链路汇聚。
- “p” (被动)
端口只在接收到 LACP 帧时参与链路汇聚。
- “o” (启用)
端口参与链路汇聚，并且不会发送任何 LACP 帧。

说明

在链路汇聚内，仅可使用具有以下组态的端口：

- 所有带“o”的端口
 - 所有带“a”或“p”的端口。
-

组态步骤

组态前的基本设置

1. 首先，确定想要连接在一起，在设备之间形成链路汇聚的端口。
2. 在设备上组态链路汇聚。
3. 对所有设备采用该组态。
4. 执行最后一步，布线。

说明

如果在组态之前用电缆连接已汇聚的链路，则可能在网络中形成环路。因此可能使相关网络变得糟糕或者完全瘫痪。

创建新链路汇聚

1. 单击“Create”按钮以创建新的链路汇聚。

此操作将创建一个新行。

2. 选择属于此链路汇聚的端口。
3. 单击“设置值”(Set Values) 按钮。

删除链路汇聚

1. 选中要删除的行中的复选框。

对所有要删除的条目重复此步骤。

2. 单击“删除”(Delete) 按钮。

更改链路汇聚

1. 在总览中，单击相关的表条目来更改所创建链路汇聚的组态。
2. 进行所有更改。
3. 单击“设置值”(Set Values) 按钮。

5.5.11 DCP 转发

应用

STEP 7 和 Primary Setup Tool (PST) 使用 DCP

协议组态和诊断。发货时，对所有端口都启用 DCP；换句话说，在所有端口都转发 DCP 帧。利用此选项，可以针对每个端口禁止发送这些帧，例如，防止使用 PST 组态网络的各个部分，或者将整个网络分成较小子网络，以进行组态和诊断。

设备的所有端口都在此页面上显示。在每个显示的端口后面，有一个用来选择功能的下拉列表。

Discovery and Basic Configuration Protocol (DCP) Forwarding

	Setting	Copy to Table
All ports	No Change	Copy to Table

Port	Setting
P0.1	Forward
P0.2	Forward
P0.3	Forward
P0.4	Forward

Set Values Refresh

显示值说明

表 1 包含以下列：

- **“第 1 列”(1st column)**
说明设置对于表 2 的所有端口都有效。
- **“设置”(Setting)**
从下拉列表中选择设置。如果选择“无变化”(No Change)，则表 2 中的条目保持不变。
- **“复制到表中”(Copy to Table)**
如果单击此按钮，将为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **“端口”(Port)**
显示可用端口。端口由模块号和端口号组成，例如，端口 0.1 表示模块 0，端口 1。
- **设置 (Setting)**
从该下拉列表中，选择端口是应阻止还是转发出站 DCP 帧。可做以下选择：
 - 转发 (Forward)
通过此端口转发 DCP 帧。
 - 阻止 (Block)
不通过此端口转发出站 DCP 帧。不过，仍可通过此端口接收帧。

组态步骤

1. 通过行中下拉列表内的选项，选择支持发送 DCP 帧的端口。
2. 单击“设置值”(Set Values) 按钮。

5.5.12 LLDP

识别网络拓扑

IEEE 802.1AB 标准中定义了 LLDP (Link Layer Discovery Protocol, 链路层发现协议)。

LLDP 是一种用来发现网络拓扑的方法。网络组件使用 LLDP 与其相邻设备交换信息。

支持 LLDP 的网络组件具有 LLDP 代理。LLDP 代理会定期发送与其自身有关的信息, 并从所连接设备接收信息。接收到的信息存储在设备上。

应用

PROFINET 使用 LLDP 进行拓扑诊断。在默认设置中, 对所有端口都启用 LLDP; 换句话说, 所有端口都发送和接收 LLDP 帧。利用此功能, 可以为每个端口选择启用或禁用发送和/或接收。

Link Layer Discovery Protocol (LLDP)					
	<table border="1"> <thead> <tr> <th>Setting</th> <th>Copy to Table</th> </tr> </thead> <tbody> <tr> <td>All ports</td> <td>No Change <input type="button" value="Copy to Table"/></td> </tr> </tbody> </table>	Setting	Copy to Table	All ports	No Change <input type="button" value="Copy to Table"/>
Setting	Copy to Table				
All ports	No Change <input type="button" value="Copy to Table"/>				
Port	Setting				
P0.1	Rx & Tx <input type="button" value="^"/>				
P0.2	Rx & Tx <input type="button" value="^"/>				
P0.3	Rx & Tx <input type="button" value="^"/>				
P0.4	Rx & Tx <input type="button" value="^"/>				
<input type="button" value="Set Values"/> <input type="button" value="Refresh"/>					

显示框说明

表 1 包含以下列:

- **第 1 列**
显示设置对于所有端口有效。
- **设置 (Setting)**
从下拉列表中选择设置。如果选择“无变化”(No Change), 则表 2 中的条目保持不变。
- **复制到表中 (Copy to Table)**
如果单击此按钮, 将为表 2 的所有端口应用此设置。

5.5 “第 2 层”菜单

表 2 包含以下列：

- **端口 (Port)**
显示可用端口。端口由模块号和端口号组成，例如，端口 0.1 表示模块 0，端口 1。
- **Setting**
从该下拉列表中，选择端口将发送还是接收 LLDP 帧。可做以下选择：
 - Rx
此端口只能接收 LLDP 帧。
 - Tx
此端口只能发送 LLDP 帧。
 - Rx & Tx
此端口可以发送和接收 LLDP 帧。
 - "-" (disabled)
此端口既不接收也不发送 LLDP 帧。

组态步骤

1. 从“设置”(Setting) 的下拉列表中选择端口的 LLDP 功能。
2. 单击“设置值”(Set Values) 按钮。

5.5.13 光纤监视协议

要求

- 仅能对带诊断功能的收发器使用光纤监视。请注意设备的相关文档。
- 为了能够使用光纤监视功能，需启用 LLDP。已将光纤监视信息添加到 LLDP 数据包中。

监视光链接

对于“光纤监视”，您可监视两个交换机之间光纤连接的接收功率和功率损耗。

如果启用某光纤端口的光纤监视，设备会通过 LLDP 数据包将端口的当前传送功率发送到其连接伙伴。除了发送外，设备还会检查是否已从连接伙伴接收相应信息。

无论工业以太网交换机是否从连接伙伴接收到诊断信息，它都会监视在光纤端口测得的接收功率并将其与设置的限值进行比较。

如果连接伙伴上启用了光纤监视，连接伙伴会将端口发射功率的当前值传递给设备。设备会将接收到的发射功率值与实际接收的功率进行比较。接收功率与发射功率之间存在的差异代表链路汇总存在损耗。计算得到的功率损失也会进行监视，判断是否超出设置的限值。

如果接收功率或功率损耗值降到设置限值以下或超出限值，则将触发事件。可按两个等级设置限值，分别发送严重级别为“Warning”和“Critical”的消息。

在“系统 > 事件 > 组态”(System > Events > Configuration) 中，可指定工业以太网交换机指示事件的方式。

说明

如果已启用光纤监视，并且带有诊断功能的可插拔收发器已拔出，则将自动为此端口禁用光纤监视，并且设置的限值和可能的未决错误状态将被删除。

Fiber Monitoring Protocol (FMP)					
Port	State	Rx Power [dBm] Maintenance Required (warning)	Rx Power [dBm] Maintenance Demanded (critical)	Power Loss [dB] Maintenance Required (warning)	Power Loss [dB] Maintenance Demanded (critical)
P0.1	<input checked="" type="checkbox"/>	-4	-6	-50	-55
P0.2	<input checked="" type="checkbox"/>	-25	-27	-50	-55
P0.4	<input checked="" type="checkbox"/>	-10	-12	-50	-55

Set Values Refresh

显示框说明

在表中，可为将被监测的测量所得接收电源和计算所得电源损耗指定限制值。

- **端口 (Port)**

显示支持光纤监视的光纤端口。它与收发器有关。

- **状态 (Status)**

启用或禁用光纤监视。

默认情况下会禁用该功能。

5.5 “第 2 层”菜单

- **需要接收功率 [dBm] 维护 (Rx Power [dBm] maintenance required (Warning))**
指定在什么值时候通过严重等级为“Warning”的消息来通知您接收功率超限。
默认值取决于相关收发器。
- **要求接收功率 [dBm] 维护 (Rx Power [dBm] maintenance demanded (Critical))**
指定在什么值时通过严重等级为“Critical”的消息来通知您接收功率超限。
默认值取决于相关收发器。
- **需要功率损耗 [dB] 维护 (Power Loss [dB] maintenance required (Warning))**
指定在什么值时通过严重等级为“Warning”的消息来通知您连接存在功率损耗。
默认值： -50 dB
- **要求功率损耗 [dB] 维护 (Power Loss [dB] maintenance demanded (Critical))**
指定在什么值时通过严重等级为“Critical”的消息来通知您连接存在功率损耗。
默认值： -55 dB

组态步骤

激活光纤监视

按照下列步骤激活端口的监视：

1. 在“Status”列中选择相应的复选框。
2. 根据您的设置，输入您要在输入值为多少时获得接收功率超限和连接存在功率损耗的通知。
3. 单击“Set Values”按钮。

取消激活光纤监视

按照下列步骤取消激活端口的监视：

1. 在“Status”列中取消选择相应的复选框。
2. 单击“Set Values”按钮。

5.5.14 单播

5.5.14.1 过滤

地址过滤

此表中显示的是参数分配期间由用户以静态方式输入的单播地址帧的源地址。

在此页面中，还可定义静态单播过滤器。

“基础网桥模式”(Base bridge mode) 的相关性

显示的框取决于所设置的“基础网桥模式”(Base bridge mode)。如果更改“基础网桥模式”(Base bridge mode)，现有条目将丢失。

Filtering

Filtering | Locked Ports | Learning | Blocking

VLAN ID: VLAN1

MAC Address:

Select	VLAN ID	MAC Address	Status	Port
<input type="checkbox"/>	1	00-1b-1b-a5-5d-55	Static	P0.1

1 entry.

Create Delete Set Values Refresh

图 5-7 基础网桥模式：802.1Q VLAN 网桥

Filtering

Filtering | Locked Ports | Learning | Blocking

MAC Address:

Select	MAC Address	Status	Port
<input type="checkbox"/>	00-1b-1b-72-55-a5	Static	-

1 entry.

Create Delete Set Values Refresh

图 5-8 基础网桥模式：802.1D 透明网桥

显示框说明

该页面包含以下框：

- **VLAN ID**

选择要为其组态新静态 MAC 地址的 VLAN ID。如果未进行任何设置，则会将“VLAN1”设置为基本设置。

- **MAC 地址 (MAC Address)**

在此处输入 MAC 地址。

该表包含以下各列：

- **选择 (Select)**

选择要删除的行。

- **VLAN ID**

显示分配给此 MAC 地址的 VLAN ID。

- **MAC 地址 (MAC Address)**

显示设备已学习或用户已组态的节点 MAC 地址。

- **状态 - 静态 (Status - Static)**

显示每个地址条目的状态。该地址是由用户以静态方式输入的。静态地址会永久存储；也就是说，当老化时间结束或设备重启时，静态地址不会被删除。这些地址必须由用户删除。

- **端口**

显示访问指定地址的节点时所使用的端口。设备接收到的目标地址与此地址相匹配的帧将被转发到此端口。

说明

您只能为单播地址指定一个端口。

组态步骤

要编辑条目，请按以下步骤操作。

创建新条目

1. 在“基础网桥模式：802.1Q VLAN 网桥”(Base Bridge Mode: 802.1Q VLAN Bridge) 中，选择适当的 VLAN ID。
2. 在“MAC Address”输入框中输入 MAC 地址。

3. 单击“Create”按钮在表中创建新条目。
4. 单击“刷新”(Refresh) 按钮。
5. 从下拉列表中选择相关端口。
6. 单击“设置值”(Set Values) 按钮。

更改条目

1. 选择相关端口。
2. 单击“设置值”(Set Values) 按钮。

删除条目

1. 选中要删除的行中的复选框。
对所有要删除的条目重复此步骤。
2. 单击“Delete”按钮从过滤表中删除所选的条目。
3. 单击“刷新”(Refresh) 按钮。

5.5.14.2 锁定端口 (Locked Ports)

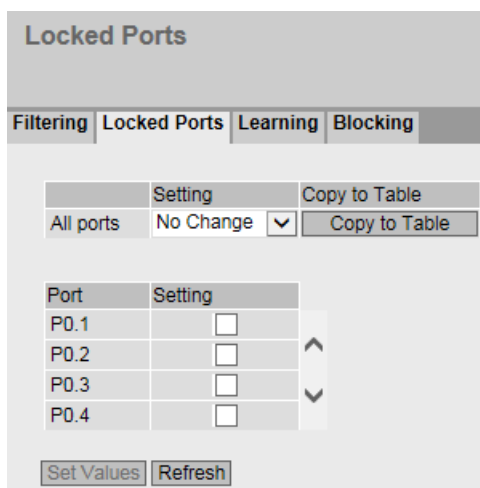
激活访问控制

在此页面中，可以针对未知节点阻止各个端口。

如果启用了“端口锁定”功能，则从未知 MAC 地址到达此端口的数据包会被立即丢弃。端口会接受已知节点发出的数据包。由于启用了“端口锁定”功能的端口无法获取任何 MAC 地址，因此在启用“端口锁定”功能后，这些端口上之前获取的地址将被自动删除。该端口仅接受之前手动创建或使用“开始学习”(Start learning) 功能和“停止学习”(Stop learning) 功能创建的静态 MAC 地址。

要自动输入所有连接的节点，可使用自动学习功能（请参见“第 2 层 > 单播 > 获取”）。

5.5 “第 2 层”菜单



显示框说明

表 1 包含以下列：

- **第 1 列**
说明设置对于表 2 的所有端口都有效。
- **Setting**
从下拉列表中选择设置。可选择以下设置选项：
 - 启用 (Enabled)
启用端口锁定功能。
 - 禁用 (Disabled)
禁用端口锁定功能。
 - 无变化 (No change)
表 2 保持不变。
- **Copy to Table**
如果单击此按钮，将为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **Port**
此列会列出此设备上的全部可用端口。
- **Setting**
启用或禁用端口的访问控制。

组态步骤

对单独的端口启用访问控制

1. 选中表 2 相关行中的复选框。
2. 要应用更改，请单击“Set Values”按钮。

对所有端口启用访问控制

1. 在“设置”(Setting) 下拉列表中，选择“启用”(Enabled) 条目。
2. 单击“Copy to table”按钮。将为表 2 中的所有端口启用该复选框。
3. 要应用更改，请单击“Set Values”按钮。

5.5.14.3 学习

开始/停止学习

通过自动学习功能，在单播过滤器表中将自动静态输入所有相连的设备。只要启用“Start learning”功能，所有学习的单播地址就会立即被创建为静态单播条目。

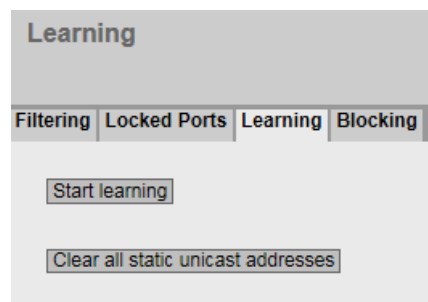
只有单击“Stop

learning”按钮后，才会结束学习过程。使用此方法时，较大网络中的找到所有节点可能会花费数分钟或数小时。只能找到在学习阶段发送数据包的节点。

通过随后启用“端口锁定”功能，在相关端口上将只接受来自学习阶段结束时识别的节点（静态单播条目）的数据包。

说明

如果在自动学习阶段之前已对各个端口激活“端口锁定”功能，则在这些端口上将不会学习到任何地址。这样便可限制特定端口的学习行为。为此，可先针对不希望其学习地址的端口，启用“端口锁定”功能。



5.5 “第 2 层”菜单

组态步骤

学习地址

1. 单击“Start learning”按钮开始学习阶段。
开始学习阶段后，“Start learning”按钮将被“Stop learning”按钮代替。
设备随即会输入所连接设备的地址，直到您停止此功能。
2. 单击“Stop learning”按钮可停止学习功能。
此按钮再次由“Start learning”按钮代替。存储已学习的条目。

删除所有静态单播地址。

1. 单击“Clear all static unicast addresses”按钮可删除所有静态条目。
在具有许多节点的大型网络中，自动学习可能导致大量不需要的静态条目。为避免必须分别删除这些条目，可使用此按钮删除所有静态条目。自动学习期间会禁用此功能。

说明

根据涉及的条目数，删除过程可能需要一些时间。

5.5.14.4 未知单播阻止

阻止转发未知单播帧

在此页面上，可阻止各个端口转发未知单播帧。

Unknown Unicast Blocking			
Filtering	Locked Ports	Learning	Blocking
All ports	Setting	Copy to Table	
	No Change	▼	Copy to Table
Port	Setting		
P0.1	<input type="checkbox"/>		
P0.2	<input type="checkbox"/>		
P0.3	<input type="checkbox"/>		
Set Values		Refresh	

显示值说明

表 1 包含以下列：

- **第 1 列**
说明设置对于表 2 的所有端口都有效。
- **设置 (Setting)**
从下拉列表中选择设置。可选择以下设置选项：
 - 启用 (Enabled)
单播帧阻止功能已启用。
 - 禁用 (Disabled)
单播帧阻止功能已禁用。
 - 无变化 (No change)
表 2 保持不变。
- **复制到表中 (Copy to Table)**
如果单击此按钮，将为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **端口 (Port)**
显示可用端口。端口由模块号和端口号组成，例如，端口 0.1 表示模块 0，端口 1。

说明

显示可用端口。端口由模块号和端口号组成，例如，端口 0.1 表示模块 0，端口

1. 环网冗余/备用

如果启用环网冗余或备用，则为此组态的端口不受单播帧阻止功能的限制。

-
- **设置 (Setting)**
启用或禁用单播帧阻止功能。

组态步骤

对单独的端口启用阻止功能

1. 选中表 2 相关行中的复选框。
2. 要应用更改，请单击“设置值”(Set Values) 按钮。

5.5 “第 2 层”菜单

对所有端口启用阻止功能

1. 在“设置”(Setting) 下拉列表中，选择“启用”(Enabled) 条目。
2. 单击“复制到表中”(Copy to table) 按钮。将为表 2 中的所有端口启用该复选框。
3. 要应用更改，请单击“设置值”(Set Values) 按钮。

5.5.15 组播

5.5.15.1 组

组播应用

在多数情况下，具有单播地址的帧将被发送到一个特定接收方。如果某个应用向多个接收方发送相同的数据，则使用一个组播地址发送数据可以减少数据量。对于某些应用，存在固定的组播地址（NTP、IETF1 音频、IETF1 视频等）。

减少网络负载

与单播帧相反，组播帧将对设备造成更高的负载。一般来说，组播帧会被发送到所有端口。以下选项可减少由组播帧产生的负载：

- 组播过滤表中地址的静态条目。
- 通过监听 IGMP 参数分配帧（IGMP 组态）生成地址的动态条目。
- 通过 GMRP 帧激活动态地址分配。

所有这些方法的结果是，组播帧只会被发送到输入了相应地址的端口。

“组播组”(Multicast Groups)

菜单项显示的是过滤表中当前输入的组播帧及用户在参数中设置的目标端口。

“基础网桥模式”(Base bridge mode) 的相关性

显示的框取决于所设置的“基础网桥模式”(Base bridge mode)。如果更改“基础网桥模式”(Base bridge mode)，现有条目将丢失。

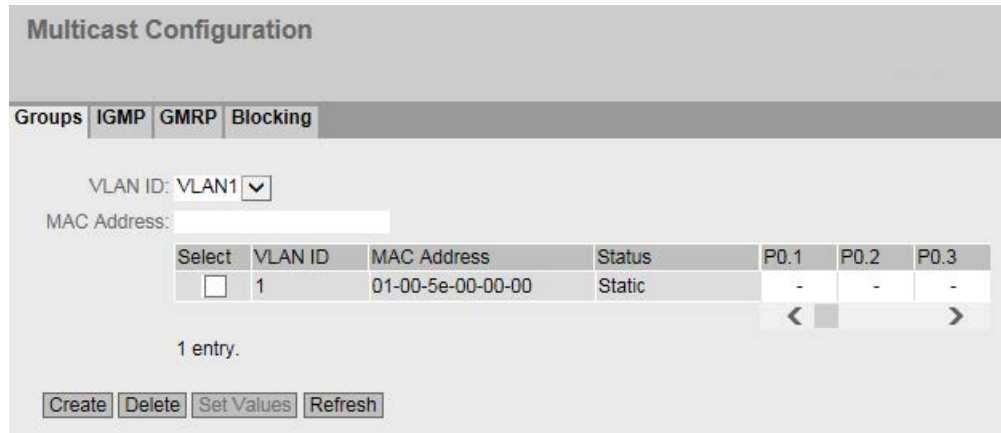


图 5-9 基础网桥模式：802.1Q VLAN 网桥

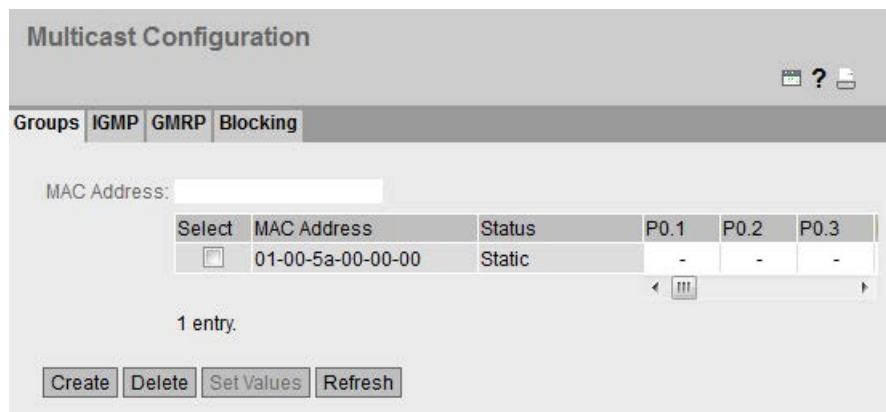


图 5-10 基础网桥模式：802.1D 透明网桥

显示框说明

该页面包含以下框：

- VLAN ID**
 单击此文本框，将显示一个下拉列表。此处可选择要组态的新 MAC 地址的 VLAN ID。
- MAC 地址 (MAC Address)**
 在此处输入要组态的新 MAC 组播地址。

5.5 “第 2 层”菜单

该表格包括以下列：

- **选择 (Select)**
选择要删除的行。
- **VLAN ID**
此处显示 VLAN 的 VLAN ID，该行的 MAC 组播地址分配给此 ID。
- **MAC 地址 (MAC Address)**
此处显示设备已学习或用户已组态的 MAC 组播地址。
- **状态 - 静态 (Status - Static)**
显示每个地址条目的状态。该地址是由用户以静态方式输入的。静态地址会永久存储；也就是说，当老化时间结束或设备重启时，静态地址不会被删除。这些地址必须由用户删除。
- **端口列表 (Port List)**
每个端口有一列。在每一列内，端口所属的组播组显示如下。该下拉列表提供以下选项：
 - M
(成员) 通过此端口发送组播帧。
 - F
(已禁止) 不是组播组的成员。此地址也不能是使用 GMRP 或 IGMP 动态学习的地址。
 - I
(IGMP) 组播组的成员，由 IGMP 帧注册。只能动态分配此值。
 - -
不是组播组的成员。不通过此端口发送包含所定义组播 MAC 地址的组播帧。

组态步骤

创建新条目

说明

如果启用 GMRP，则无法创建任何静态组播条目。

1. 在“基础网桥模式：802.1Q VLAN 网桥”，从“VLAN ID”下拉列表中选择所需 VLAN ID。
2. 在“MAC 地址”(MAC Address) 输入框中输入 MAC 地址。

3. 单击“创建”(Create) 按钮。会在表中生成一个新条目。
4. 将相关端口分配给 MAC 地址。
5. 单击“设置值”(Set Values) 按钮。

删除条目

1. 选中要删除的行中的复选框。
2. 单击“删除”(Delete) 按钮。
将删除所有选中条目并刷新显示。

使用脚本和 GMRP 创建第 2 层组播地址。

如果要使用脚本创建多个第 2 层组播地址，则只要脚本正在执行，就必须禁用 GMRP。请按照下面列出的步骤进行操作：

1. 如果已启用 GMRP，请将其禁用。在“Layer 2 > Multicast > GMRP”页面中组态 GMRP。
2. 运行脚本。
3. 仅在脚本全部完成且第 2 层组播地址创建后才启用 GMRP。

5.5.15.2 IGMP

功能

设备支持“IGMP 监听”(IGMP Snooping) 和“IGMP 查询器”(IGMP Querier) 功能。如果启用了“IGMP 监听”，则会评估 IGMP 帧（Internet 组管理协议）且组播过滤表会更新此信息。如果还启用了“IGMP 查询器”，设备也会发送 IGMP 查询，从而触发 IGMP 兼容节点的响应。

IGMP 监听老化时间

在此菜单中，可以组态“IGMP 组态”的老化时间。经过该时间后，如果 IGMP 创建的条目未被新的 IGMP 帧更新，将从地址表中删除这些条目。

这适用于所有端口；但无法对具体端口进行组态。

取决于查询器的 IGMP 监听老化时间

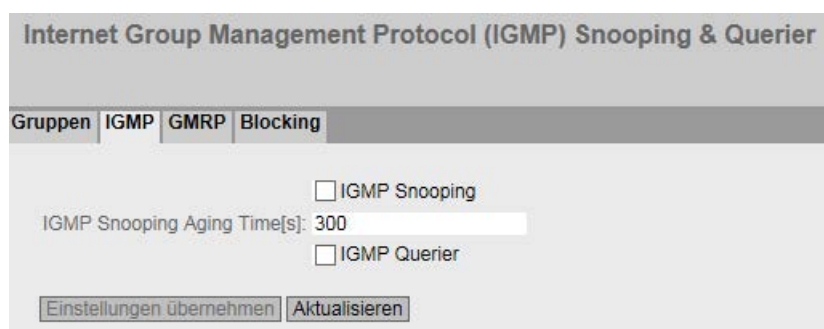
工业以太网交换机用作 IGMP 查询器

如果工业以太网交换机用作 IGMP 查询器，则查询间隔为 125 秒。对于“IGMP 监听老化时间”(IGMP Snooping Aging Time)，至少设置为 250 秒。

其它 IGMP 查询器

如果使用其它 IGMP 查询器，则“IGMP 监听老化时间”(IGMP Snooping Aging Time) 的值应至少为查询间隔的 2 倍。

显示框说明



该页面包含以下框：

- **IGMP 监听 (IGMP Snooping)**
启用或禁用 IGMP 监听。该功能允许将 IP 地址分配给组播组。如果选中该复选框，IGMP 条目将包括在表中，并且 IGMP 帧会被转发。
- **IGMP 监听老化时间[s] (IGMP Snooping Aging Time[s])**
在此框中，输入老化时间的秒数值。默认情况下，会设置 300 秒。
有效值为：130 - 1225 秒
- **IGMP 查询器 (IGMP Querier)**
启用或禁用“IGMP 查询器”(IGMP Querier)。设备会发送 IGMP 查询。

组态步骤

1. 选中“IGMP Snooping”复选框。
2. 在“IGMP Snooping Aging Time”框中，输入老化时间的秒数值。
3. 选中“IGMP Querier”复选框。
4. 单击“设置值”(Set Values) 按钮。

5.5.15.3 GMRP

激活 GMRP

在此页，指定 GMRP

是否被用于每个单独端口。如果对某个端口禁用“GMRP”，则不会注册该端口，且该端口也不能发送 GMRP 帧。

GARP Multicast Registration Protocol (GMRP)

Groups | IGMP | **GMRP** | Blocking

GMRP

	Setting	Copy to Table
All ports	No Change	Copy to Table

Port	Setting
P0.1	<input checked="" type="checkbox"/>
P0.2	<input checked="" type="checkbox"/>
P0.3	<input checked="" type="checkbox"/>

Set Values Refresh

显示框说明

该页面包含以下框：

- **GMRP**
启用或禁用 GMRP 功能。

5.5 “第 2 层”菜单

表 1 包含以下列：

- **第 1 列**
说明设置对于表 2 的所有端口都有效。
- **Setting**
从下拉列表中选择设置。可选择以下设置选项：
 - 启用 (Enabled)
启用发送 GMRP 帧。
 - 禁用 (Disabled)
禁用发送 GMRP 帧。
 - 无变化 (No change)
表 2 保持不变。
- **Copy to Table**
如果单击此按钮，将为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **Port**
该列会显示设备上的所有可用端口以及链路汇聚。
- **设置 (Setting)**
使用此复选框为端口或链路汇聚启用或禁用 GMRP。

组态步骤

针对单独端口启用发送 GMRP 帧

1. 选择“GMRPGMRP”复选框。
2. 选中表 2 相关行中的复选框。
3. 要应用更改，请单击“Set Values”按钮。

针对所有端口启用发送 GMRP 帧

1. 选择“GMRPGMRP”复选框。
2. 在“设置”(Setting) 下拉列表中，选择“启用”(Enabled) 条目。
3. 单击“Copy to table”按钮。将为表 2 中的所有端口启用该复选框。
4. 要应用更改，请单击“Set Values”按钮。

5.5.15.4 组播阻止

禁止转发未知组播帧

在此页面上，可阻止各个端口转发未知组播帧。

Port	Setting
P0.1	<input type="checkbox"/>
P0.2	<input type="checkbox"/>
P0.3	<input type="checkbox"/>
P0.4	<input type="checkbox"/>

显示值说明

表 1 包含以下列：

- **第 1 列**
说明设置对于表 2 的所有端口都有效。
- **设置 (Setting)**
从下拉列表中选择设置。可选择以下设置选项：
 - 启用 (Enabled)
组播帧阻止功能已启用。
 - 禁用 (Disabled)
组播帧阻止功能已禁用。
 - 无变化 (No change)
表 2 保持不变。
- **复制到表中 (Copy to Table)**
如果单击此按钮，将为表 2 的所有端口应用此设置。

5.5 “第 2 层”菜单

表 2 包含以下列：

- **端口 (Port)**
所有可用端口均列于此列中。不显示不可用端口。
- **设置 (Setting)**
启用或禁用组播帧阻止功能。

组态步骤

对单独的端口启用阻止功能

1. 选中表 2 相关行中的复选框。
2. 要应用更改，请单击“设置值”(Set Values) 按钮。

对所有端口启用阻止功能

1. 在“设置”(Setting) 下拉列表中，选择“启用”(Enabled) 条目。
2. 单击“复制到表中”(Copy to table) 按钮。将为表 2 中的所有端口启用该复选框。
3. 要应用更改，请单击“设置值”(Set Values) 按钮。

5.5.16 广播

阻止广播帧的转发

在此页面上，可阻止各个端口转发广播帧。

说明

某些通信协议只有在广播的支持下才能起作用。在这种情况下，阻止功能可能导致数据通信丢失。因此，只有确定在所选端口上不需要广播时才将阻止广播。

	Setting	Copy to Table
All ports	No Change ▼	Copy to Table

Port	Setting
P0.1	<input type="checkbox"/>
P0.2	<input type="checkbox"/>
P0.3	<input type="checkbox"/>
P0.4	<input type="checkbox"/>

显示框说明

表 1 包含以下列：

- **“第 1 列”(1st column)**
说明设置对于表 2 的所有端口都有效。
- **“设置”(Setting)**
从下拉列表中选择设置。可选择以下设置选项：
 - 启用 (Enabled)
对广播帧的阻止已启用。
 - 禁用 (Disabled)
对广播帧的阻止已禁用。
 - 无变化 (No change)
表 2 保持不变。
- **复制到表 (Copy to Table)**
如果单击此按钮，将为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **“端口”(Port)**
显示所有可用端口。
- **“设置”(Setting)**
启用或禁用对广播帧的阻止。

5.5 “第 2 层”菜单

组态步骤

针对单独端口启用对广播帧的阻止

1. 选中表 2 相关行中的复选框。
2. 要应用更改，请单击“设置值”(Set Values) 按钮。

针对所有端口启用对广播帧的阻止

1. 在表 1“设置”(Setting) 下拉菜单中，选择“启用”(Enabled) 条目。
2. 单击“复制到表”(Copy to Table) 按钮。将为表 2 中的所有端口启用该复选框。
3. 要应用更改，请单击“设置值”(Set Values) 按钮。

5.5.17 RMON

5.5.17.1 Statistics

统计信息

在此页面中，可以指定要显示其 RMON 统计信息的端口。

RMON 统计信息显示在“信息 > 以太网统计信息”(Information > Ethernet Statistics) 页面的“数据包大小”(Packet Size)、“帧类型”(Frame Type) 和“数据包错误”(Packet Error) 中。

设置

RMON Statistics Configuration

Statistics | History

RMON

Port: All ports

Select	Port
<input type="checkbox"/>	P0.1
<input type="checkbox"/>	P0.2
<input type="checkbox"/>	P0.3
<input type="checkbox"/>	P0.4

16 entries.

Create Delete Set Values Refresh

- **RMON**

如果选择该复选框，则远程监视 (RMON)

允许在设备上收集和准备诊断数据，并由同样支持 RMON 的网络管理站使用 SNMP 读出诊断数据。凭借此诊断数据（例如，端口相关的负载趋势）可以在早期发现并排除网络中的故障。

说明

如果禁用 RMON，这些统计信息不会被删除，而会保持其前一个状态。

- **Port**

选择要显示其统计信息的端口。

该表格包括以下列：

- **Select**

选择要删除的行。

- **Port**

表示要显示其统计信息的端口。

5.5 “第 2 层”菜单

组态步骤

启用该功能

1. 选择“RMON”复选框。
2. 单击“设置值”(Set Values) 按钮。

“RMON”功能已启用。

启用端口的 RMON 统计信息

说明

要求

要显示端口的 RMON 统计信息，必须启用“RMON”功能。

1. 从“端口”(Port) 下拉列表中选择所需端口或选择“所有端口”(All Ports)。
2. 单击“创建”(Create) 按钮。

可显示所选端口或所有端口的 RMON 统计信息。

禁用端口的 RMON 统计信息

1. 在“选择”(Select) 列中选择要删除的行。
2. 单击“删除”(Delete) 按钮。

将不再显示所选端口的 RMON 统计信息。

5.5.17.2 历史

统计信息的样本

在此页面中，可以指定是否保存端口的统计信息样本。可以指定要保存的条目数量和采集样本的时间间隔。

设置

Setting	Buckets	Interval[s]	Copy to Table
All ports	No Change	No Change	No Change

Port	Setting	Buckets	Interval[s]
P0.1	<input type="checkbox"/>	0	0
P0.2	<input type="checkbox"/>	0	0
P0.3	<input type="checkbox"/>	0	0
P0.4	<input type="checkbox"/>	0	0

表 1 包含以下列：

- **第 1 列**
显示设置对于所有端口有效。
- **Setting**
选择所需设置。如果选择“无变化”(No Change)，则表 2 中的条目保持不变。
- **Entries**
输入可同时保存的条目的最大数量。如果输入“无变化”(No Change)，则表 2 中的条目保持不变
- **Interval [s]**
输入将统计信息的当前状态保存为样本的间隔。如果输入“无变化”(No Change)，则表 2 中的条目保持不变
- **Copy to Table**
如果单击此按钮，则为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **Port**
显示设置所关联的端口。
- **Setting**
启用或禁用相关端口的历史记录。

5.5 “第 2 层”菜单

- **Entries**

输入可同时保存的条目的最大数量。

取值范围：1 - 65535

出厂设置：24

- **Interval [s]**

输入将统计信息的当前状态保存为样本的间隔。

取值范围：1 - 3600

出厂设置：3600

组态步骤

为单独端口启用 RMON 数据

1. 在表 2 中的相关行选中复选框“设置”(Setting)。
“条目”(Entries) 和“时间间隔[s]”(Interval[s]) 变为激活状态并采用出厂设置。
2. 在“条目”(Entries) 和“时间间隔[s]”(Interval[s]) 输入框内输入所需值。
3. 单击“设置值”(Set Values) 按钮。

为所有端口启用 RMON 统计信息

1. 在“设置”(Setting) 下拉菜单中，选择表 1 中的“启用”(Enabled) 条目。
2. 在“条目”(Entries) 和“时间间隔[s]”(Interval[s]) 输入框内输入所需值。若不更改两个框内的条目，则所有端口都应用出厂默认设置。
3. 单击“复制到表”(Copy to Table) 按钮。
表 2 的所有端口均采用这些设置。
4. 单击“设置值”(Set Values) 按钮。

5.6 “第 3 层”(Layer 3) 菜单

5.6.1 DHCP 中继代理

5.6.1.1 常规

DHCP 中继代理

如果 DHCP 服务器在不同网络中，则设备无法访问 DHCP 服务器。DHCP 中继代理可在 DHCP 服务器与设备之间进行调停。DHCP 中继代理会将设备的端口号与 DHCP 查询一同转发至 DHCP 服务器。

最多可为 DHCP 继电器代理指定 4 个 DHCP 服务器。如果 DHCP 服务器不可访问，设备可切换到其它 DHCP 服务器。

Dynamic Host Configuration Protocol (DHCP) Relay Agent General

General Option

DHCP Relay Agent (Opt. 82)

Server IP Address:

Select	Server IP Address
<input type="checkbox"/>	192.168.0.1

1 entry.

Create Delete Set Values Refresh

显示值说明

该页面包含以下框：

- **DHCP Relay Agent (opt.82)**
启用或禁用 DHCP 继电器代理。
- **Server IP Address**
输入 DHCP 服务器的 IPv4 地址。

5.6 “第 3 层”(Layer 3) 菜单

该表格包括以下列：

- **Select**
选择要删除的行。
- **Server IP Address**
显示 DHCP 服务器的 IPv4 地址。

组态步骤

1. 在“Server IP Address”输入框中输入 DHCP 服务器的 IPv4 地址。
2. 单击“创建”(Create) 按钮。会在表中生成一个新条目。
3. 选中“DHCP Relay Agent (Opt.82)”复选框
4. 单击“设置值”(Set Values) 按钮。

5.6.1.2 选项

DHCP 中继代理的参数

在此页面，可为 DHCP 服务器指定参数，举个例子，电路 ID。电路 ID 介绍了 DHCP 查询的原点，比如哪个端口接收了 DHCP 查询。在“常规”(General) 选项卡中指定 DHCP 服务器。

Dynamic Host Configuration Protocol (DHCP) Relay Agent Option

General | Option

Global configuration

- Circuit ID Router Index
- Circuit ID Receive VLAN ID
- Circuit ID Receive Port

Remote ID: 08-00-06-70-56-00

Interface specific configuration

Interface: -

Select	Interface	Remote ID Type	Remote ID	Circuit ID Type	Circuit ID
<input type="checkbox"/>	vlan1	IP Address	192.168.16.202	Predefined	-

1 entry.

Create Delete Set Values Refresh

显示值说明

该页面包含以下框：

全局组态

- **Circuit ID router index**

启用或禁用该复选框。若启用该复选框，则在生成的电路 ID 中添加路由器索引。

- **电路 ID 接收 VLAN ID (Circuit ID Receive VLAN ID)**

启用或禁用该复选框。如果选中该复选框，则会将 VLAN ID 添加至生成的电路 ID。

- **电路 ID 接收端口 (Circuit ID Receive Port)**

启用或禁用该复选框。若启用该复选框，则在生成的电路 ID 中添加接收端口。

说明

至少需要选择一个选项。

- **Remote ID**

显示设备 ID。

接口特定组态

- **Interface**

从下拉列表中选择接口。

该表格包括以下列：

- **Select**

选择要删除的行。

- **接口 (Interface)**

显示接口。

说明

如果尚未创建接口特定的组态，则会将带有 MAC 地址的全局组态用作设备 ID。

5.6 “第 3 层”(Layer 3) 菜单

- **Remote ID Type**

从下拉列表中选择设备 ID 的类型。可做以下选择：

- IP Address

将设备的 IPv4 地址用作设备 ID。

- MAC Address

将设备的 MAC 地址用作设备 ID。

- 自由文本 (Free Text)

如果使用“自由文本”(Free Text)，可在“远程 ID”(Remote ID) 中输入设备名称作为设备标识符。

- **Remote ID**

输入设备名称。仅当为“远程 ID 类型”(Remote ID Type) 选择条目“自由文本”(Free Text) 时才能编辑该框。

- **Circuit ID Type**

从下拉列表中选择电路 ID 的类型。可做以下选择：

- 预定义 (Predefined)

根据路由器索引、VLAN ID 或端口自动创建电路 ID。

- 自由编号 (Free Number)

如果使用“自由编号”(Free Number)，可为“电路 ID”(Circuit ID) 输入 ID。

- **Circuit ID**

输入电路 ID。仅当为“电路 ID 类型”(Circuit ID Type) 选择“自由编号”(Free Number) 条目时，才能对此框进行编辑。

组态步骤

按照以下步骤指定自动分配参数：

1. 选中“Circuit ID router index”复选框。
2. 从“Interface”下拉列表中选择接口。
3. 单击“Create”按钮。将在表中插入一个新行。
4. 在“Remote ID Type”下拉列表中选择条目“IP Address”。会将 IPv4 地址用作设备 ID。
5. 在“Circuit ID Type”下拉列表中选择“Predefined”条目。路由器索引会添加到生成的电路 ID 中。
6. 单击“设置值”(Set Values) 按钮。

按照以下步骤手动指定参数：

1. 选中“Circuit ID router index”复选框。
2. 从“Interface”下拉列表中选择接口。
3. 单击“Create”按钮。将在表中插入一个新行
4. 在“Remote ID Type”下拉列表中选择条目“Free Text”。在“Remote ID”中输入设备 ID。
5. 在“Circuit ID Type”下拉列表中选择“Free Number”条目。在“Circuit ID”中输入 ID。
6. 单击“设置值”(Set Values) 按钮。

5.7 “Security”菜单

5.7.1 用户管理

用户管理概述

通过可组态的用户设置来管理对设备的访问。使用密码设置用户以供验证。为用户分配具有适当权限的角色。

用户的身份验证可在本地由设备执行，也可由外部 RADIUS 服务器执行。可在“安全 > AAA > 常规”(Security > AAA > General) 页面中组态身份验证的处理方式。

说明

向 STEP 7 (TIA Portal) 传送设备组态时，不会传送组态的用户。

本地登录

用户本地登录时设备的工作方式如下：

1. 用户通过用户名和密码在设备上登录。
2. 设备检查是否存在该用户的条目。
 - 如果存在条目，该用户成功登录并具有所关联角色的权限。
 - 如果不存在相应的条目，则拒绝该用户登录。

通过外部 RADIUS 服务器登录

RADIUS (Remote Authentication Dial-In User Service, 拨入用户远程认证服务) 是通过集中存储用户数据的服务器来验证用户和为用户授权的协议。

按如下说明通过 RADIUS 服务器验证用户身份:

1. 用户通过用户名和密码在设备上登录。
2. 设备将带有登录数据的身份验证请求发送到 RADIUS 服务器。
3. RADIUS 服务器执行检查并将结果发送回设备。
 - RADIUS 服务器报告身份验证成功, 并向设备的属性“Service Type”返回值“Administrative User”。
 - 用户登录并具有读/写权限。
 - RADIUS 服务器会报告身份验证成功, 并向设备的属性“Service Type”返回差异或甚至是无值。
 - 用户登录并具有读取权限。
 - RADIUS 服务器向设备报告身份验证失败:
 - 用户被拒绝访问。

在基础网桥模式“802.1Q VLAN 网桥”下通过 RADIUS 或访客 VLAN 分配 VLAN。

更改 VLAN 组态情况下的身份验证

如果在验证期间使用“允许 RADIUS VLAN 分配”或“访客 VLAN”功能将一个端口动态地分配给 VLAN, 则有如下选项:

- 如果设备上尚未创建待分配的 VLAN, 则会拒绝身份验证。
- 如果设备上已创建待分配的 VLAN:
 - 该端口将成为已分配 VLAN 中的无标记成员 (如果尚未成为)。
 - 这样, 便可以覆盖此 VLAN 中端口的静态组态, 并在取消身份验证时不进行恢复。
 - 端口的端口 VID 会变为所分配 VLAN 的 ID。

说明

如果端口只分配给一个 VLAN, 则需要相应地手动调整 VLAN 组态。默认情况下, 所有端口在“VLAN 1”中为无标记成员。

5.7 “Security”菜单

如果取消身份验证（即通过链路中断），则会取消动态更改。

- 端口不再是已分配 VLAN 中的成员。
- 端口的端口 VID 被重设为验证之前的值。

说明

如果端口 VID 与验证之前分配的端口 VID 一致，则该端口保持为此 VLAN 中的无标记成员。

未更改 VLAN 组态情况下的身份验证

在身份验证期间，如果未通过“支持的 RADIUS VLAN 分配”(RADIUS VLAN Assignment Allowed) 或“访客 VLAN”(Guest VLAN) 功能分配任何 VLAN，则端口的 VLAN 组态保持不变。

5.7.2 用户

5.7.2.1 本地用户

本地用户

在此页面上，创建具有相应权限的本地用户。

说明

显示的值取决于已登录用户的权限。

The screenshot shows the 'Local Users' configuration page. It includes a header 'Local Users' and a sub-header 'Local Users'. Below the header, there are input fields for 'User Account', 'Password Policy' (set to 'high'), 'Password', and 'Password Confirmation'. A 'Role' dropdown menu is set to 'user'. Below these fields is a table with two columns: 'Select' and 'Role'. The table contains two entries: 'user' and 'admin'. At the bottom of the page, there are three buttons: 'Create', 'Delete', and 'Refresh'.

Select	User Account	Role
<input type="checkbox"/>	user	user
<input type="checkbox"/>	admin	admin

2 entries.

Create Delete Refresh

说明

该页面包含以下内容：

- **User Account**

输入用户的名称。该名称必须满足以下条件：

- 名称必须唯一。
- 名称长度必须在 1 到 250 个字符之间。

说明

用户名无法更改

创建用户后，无法再修改用户名称。

如果需要更改用户名，则必须删除该用户并创建一个新用户。

说明

出厂时设置的默认用户“user”

自固件版本 V2.1 起，出厂时设置的默认用户“user”在产品交付后不再可用。

如果将设备固件版本更新到

V2.1，用户“user”起初仍然可用。如果将设备复位为出厂设置（“恢复出厂默认设置并重启”(Restore Factory Defaults and Restart)），则用户“user”将被删除。

可以使用“user”角色创建新用户。

- **Password Policy**

显示设备上使用的密码策略：

- 高 (High)

密码长度：至少 8 个字符，最长 128 个字符

至少 1 个大写字母

至少 1 个特殊字符

至少 1 个数字

- 低 (Low)

密码长度：至少 6 个字符，最长 128 个字符

在“安全 > 密码 > 选项”(Security > Passwords > Options) 页面组态设备的密码策略。

- **密码 (Password)**

输入密码。密码强度取决于设置的密码策略。

5.7 “Security”菜单

- **Password Confirmation**

再次输入该密码以进行确认。

- **Role**

选择角色：

- **user**

拥有此角色的用户可读取设备参数，但不可更改这些参数。拥有此角色的用户可以更改他们自己的密码。

- **admin**

拥有此角色的用户既可读取也可更改设备参数。

该表包含以下列：

- **Select**

选中要删除的行中的复选框。

说明

工厂预设的用户和登录用户无法删除或更改。

- **User Account**

显示用户名。

- **Role**

显示用户角色。

步骤

创建用户

1. 输入用户的名称。
2. 输入用户的密码。
3. 再次输入该密码以进行确认。
4. 选择用户角色。
5. 单击“创建”(Create) 按钮。

删除用户

1. 选中要删除的行中的复选框。
2. 单击“删除”(Delete) 按钮。将删除条目并更新页面。

5.7.3 密码

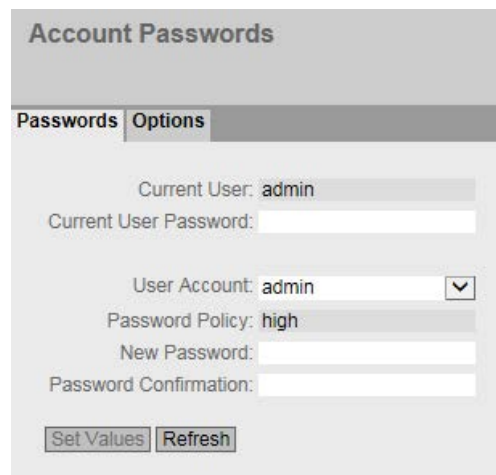
5.7.3.1 密码

组态设备密码

说明

如果通过 RADIUS 服务器登录，则无法更改任何密码。

在此页面上，可以更改密码。若登录后具有读/写权限，则可以更改所有用户帐户的密码。如果已读取权限登录，则只能更改您自有的密码。



Account Passwords

Passwords | Options

Current User: admin

Current User Password:

User Account: admin

Password Policy: high

New Password:

Password Confirmation:

显示框说明

- **Current User**
显示当前已登录的用户。
- **Current User Password**
输入当前已登录的用户的密码。

5.7 “Security”菜单

- **User Account**

选择要更改其密码的用户。

- **密码策略 (Password Policy)**

显示分配新密码时正在使用的密码策略。

- 高

密码长度：至少 8 个字符，最长 128 个字符

至少 1 个大写字母

至少 1 个特殊字符

至少 1 个数字

- 低

密码长度：至少 6 个字符，最长 128 个字符

- **新密码 (New Password)**

为所选用户输入新密码。

- **Password Confirmation**

再次输入新密码以进行确认。

步骤

说明

如果是以预设用户“admin”的身份首次登录，或是在“恢复出厂默认设置并重启”之后登录，系统会提示您更改密码。

设备交付时的密码出厂设置如下：

- “管理员”(admin): admin
-

说明

在试用模式下更改密码

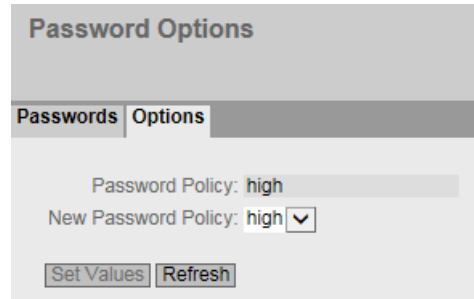
即使在试用模式下更改密码，此更改也会立即保存。

1. 在“Current User Password”输入框中输入当前已登录的用户的密码。
2. 从“User Account”下拉列表中，选择要更改其密码的用户。
3. 在“New Password”输入框中为所选用户输入新密码。

4. 在“Password Confirmation”输入框中重复输入新密码。
5. 单击“Set Values”按钮。

5.7.3.2 选项

在此页面指定分配新密码时将使用的密码策略。



Password Options

Passwords Options

Password Policy: high

New Password Policy: high ▾

Set Values Refresh

说明

- **密码策略 (Password Policy)**
显示当前正在使用的密码策略
- **新密码策略 (New Password Policy)**
从该下拉列表中选择所需的设置。
 - 高
密码长度：至少 8 个字符，最长 128 个字符
至少 1 个大写字母
至少 1 个特殊字符
至少 1 个数字
 - 低
密码长度：至少 6 个字符，最长 128 个字符

5.7 “Security”菜单

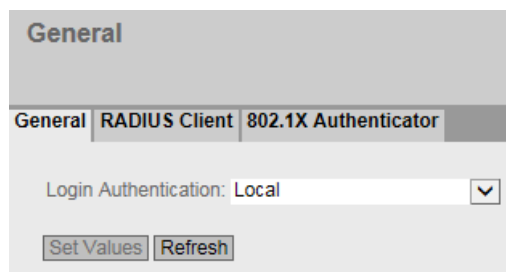
5.7.4 AAA

5.7.4.1 常规

网络节点登录

使用“AAA”的标识表示“Authentication, Authorization, Accounting”。该功能用于识别和允许网络节点，并为网络节点提供相应的服务。

在此页面中组态登录信息。



The screenshot shows a web-based configuration interface for AAA. At the top, there is a header labeled "General". Below this, there are three tabs: "General", "RADIUS Client", and "802.1X Authenticator". The "General" tab is currently selected. Underneath the tabs, there is a label "Login Authentication:" followed by a dropdown menu showing "Local". At the bottom of the form, there are two buttons: "Set Values" and "Refresh".

显示框说明

该页面包含以下框：

说明

要使用登录验证“RADIUS”，必须存储和组态用于用户验证的 RADIUS 服务器。

- **登录验证 (Login Authentication)**

指定登录方式：

- 本地 (Local)

必须在设备上进行本地验证。

- RADIUS

必须通过 RADIUS 服务器处理验证。

- 本地和 RADIUS (Local and RADIUS)

使用设备上的用户（用户名和密码）以及通过 RADIUS 服务器都可以进行验证。

首先在本地数据库中搜索用户。如果用户不存在，则将发送 RADIUS 请求。

- RADIUS 和本地回退 (RADIUS and fallback Local)

必须通过 RADIUS 服务器处理验证。

只有在无法在网络中访问 RADIUS 服务器时，才执行本地验证。

5.7.4.2 RADIUS 客户端

通过外部服务器登录

RADIUS 的概念基于外部验证服务器。

表中的每一行包含一台服务器的访问数据。按照搜索顺序，将首先查询主服务器。如果无法访问主服务器，则会以服务器的输入顺序查询其它辅助服务器。

如果没有服务器响应，则表示没有验证。

Remote Authentication Dial In User Service (RADIUS) Client						
General RADIUS Client 802.1X Authenticator						
Select	RADIUS Server Address	Server Port	Shared Secret	Shared Secret Conf.	Max. Retrans.	Primary Server
<input type="checkbox"/>	0.0.0.0	1812			3	no <input type="checkbox"/>
1 entry.						
<input type="button" value="Create"/> <input type="button" value="Delete"/> <input type="button" value="Set Values"/> <input type="button" value="Refresh"/>						

显示框说明

该表格包括以下列：

- **选择 (Select)**

选择要删除的行。

- **身份验证服务器类型**

选择服务器将用于哪种身份验证方法。

- 登录 (Login)

服务器仅用于登录验证。

- 802.1X

服务器仅用于 802.1X 身份验证。

- 登录 & 802.1X

服务器用于两种身份验证程序。

- **RADIUS 服务器地址 (RADIUS Server Address)**

输入 RADIUS 服务器的 IPv4 地址。

- **服务器端口 (Server Port)**

在此处输入 RADIUS 服务器的输入端口。默认情况下会设置输入端口 1812。

取值范围：1 - 65535

- **共享密钥 (Shared Secret)**

输入 RADIUS 服务器的访问标识符。

取值范围：1 ... 128 个字符

- **共享密钥确认 (Shared Secret Conf.)**

再次输入访问 ID 以进行确认。

- **最大重传次数 (Max. Retrans.)**

在此，输入尝试请求的最大重试次数。

初始连接请求将重试此处指定的次数，然后才会查询另一个已组态的 RADIUS 服务器或将登录视为失败。由于默认设置为 3 次重试，这意味着会尝试进行 4 次连接。

取值范围：1 - 5

- **主服务器 (Primary Server)**

使用下拉菜单中的选项，指定一个服务器是否为主服务器。可选择选项“yes”或“no”之一。只能定义一个主服务器。

- **测试 (Test)**

可以使用此按钮测试指定的 RADIUS 服务器是否可用。该测试执行一次，并非循环执行。

- **测试结果 (Test Result)**

显示 RADIUS 服务器是否可用：

- 失败，未发送测试包 (Failed, no test packet sent)
无法访问 IP 地址。
可以访问 IP 地址，但 RADIUS 服务器尚未运行。
- 可访问，但不接受密钥 (Reachable, key not accepted)
可以访问 IP 地址，但 RADIUS 服务器不接受指定的共享密钥。
- 可访问，且接受密钥 (Reachable, key accepted)
可以访问 IP 地址，且 RADIUS 服务器接受指定的共享密钥。

测试结果不会自动更新。要删除测试结果，请单击“刷新”(Refresh) 按钮。

组态步骤

输入新服务器

1. 单击“创建”(Create) 按钮。会在表中生成一个新条目。
在表中将输入以下默认值：
 - 身份验证服务器类型：登录 & 802.1X
 - RADIUS 服务器地址：0.0.0.0
 - 服务器端口 (Server Port)：1812
 - 最大重传次数 (Max. Retrans.)：3
 - 主服务器 (Primary Server)：否 (No)

5.7 “Security”菜单

2. 在相关行中，在输入框中输入以下数据：
 - 身份验证服务器类型
 - RADIUS 服务器地址 (RADIUS Server Address)
 - 服务器端口 (Server Port)
 - Shared Secret
 - 共享密钥确认 (Shared Secret Confirmation)
 - 最大重传次数 (Max. Retrans.): 3
 - 主服务器: 否 (No)
3. 单击“设置值”(Set Values) 按钮。
4. 如果必要，测试 RADIUS 服务器的可访问性。

对每个要输入的服务器重复此步骤。

修改服务器

1. 在相关行中，在输入框中输入以下数据：
 - 身份验证服务器类型
 - RADIUS 服务器地址 (RADIUS Server Address)
 - 服务器端口 (Server Port)
 - Shared Secret
 - 共享密钥确认 (Shared Secret Confirmation)
 - 最大重传次数 (Max. Retrans.)
 - 主服务器 (Primary Server)
2. 单击“设置值”(Set Values) 按钮。
3. 如果必要，测试 RADIUS 服务器的可访问性。

对要修改的输入内容所属的每台服务器重复此步骤。

删除服务器

1. 单击第一列中要删除的行前的复选框，以选择要删除的条目。
对所有要删除的条目重复此操作。
2. 单击“删除”(Delete) 按钮。
会删除所有选中的条目并刷新显示。

5.7.4.3 802.1x 验证器

设置网络访问

只有在设备利用验证服务器对终端设备的登录数据进行验证后，该终端设备才能访问网络。可以通过 802.1X 或 MAC 地址进行身份验证。

使用 802.1X 进行身份验证时，终端设备和验证服务器都必须支持 EAP 协议 (Extensive Authentication Protocol)。

对单独的端口启用验证

通过启用相应选项，可指定是否在此端口上启用符合 IEEE 802.1x 的网络访问保护。

802.1X Authenticator

General
RADIUS Client
802.1X Authenticator

MAC Authentication

Guest VLAN

	802.1X Auth. Control	802.1X Re-Authentication	MAC Authentication	RADIUS VLAN Assignment Allowed	MAC Auth. Max Allowed Addresses
All ports	No Change ▼	No Change ▼	No Change ▼	No Change ▼	No Change

Port	802.1X Auth. Control	802.1X Re-Authentication	MAC Authentication	RADIUS VLAN Assignment Allowed	MAC Auth. Max Allowed Addresses
P0.1	Force Authorized ▼	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1
P0.2	Force Authorized ▼	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1
P0.3	Force Authorized ▼	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1
P0.4	Force Authorized ▼	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	1

图 5-11 802.1x 验证器 - 表的第一部分

5.7 “Security”菜单

Guest VLAN	Guest VLAN ID	Guest VLAN Max Allowed Addresses	Copy to Table
No Change	No Change	No Change	Copy to Table

Guest VLAN	Guest VLAN ID	Guest VLAN Max Allowed Addresses	802.1X Auth. Status	MAC Auth. Actual Allowed Addresses	MAC Auth. Actual Blocked Addresses	Guest VLAN Actual Allowed Addresses
<input type="checkbox"/>	1	1	Authorized	0	0	0
<input type="checkbox"/>	1	1	Authorized	0	0	0
<input type="checkbox"/>	1	1	Authorized	0	0	0
<input type="checkbox"/>	1	1	Authorized	0	0	0

图 5-12 802.1X 验证器 - 表的第二部分

显示框说明

该页面包含以下框：

- MAC Authentication**

为设备启用或禁用 MAC 验证。
- Guest VLAN**

为设备启用或禁用“访客 VLAN”(Guest VLAN) 功能。

表 1 包含以下列：

- 第 1 列**

说明设置对于表 2 的所有端口都有效。
- 802.1X 验证控制 (802.1X Auth.Control)**

选择所需设置。

如果选择“无变化”(No Change)，则表 2 中的条目保持不变。
- 802.1x 重新验证 (802.1x Re-authentication)**

选择所需设置。

如果选择“无变化”(No Change)，则表 2 中的条目保持不变。

- **MAC 验证 (MAC Authentication)**
选择所需设置。
如果选择“无变化”(No Change), 则表 2 中的条目保持不变。
- **支持的 RADIUS VLAN 分配 (RADIUS VLAN Assignment Allowed)**
选择所需设置。
如果选择“无变化”(No Change), 则表 2 中的条目保持不变。
- **MAC 验证允许的最大地址数 (MAC Auth.Max Allowed Addresses)**
指定可以同时端口上通信的 MAC 地址数目。
如果选择了“无变化”(No Change), 则表 2 中的条目保持不变。
- **访客 VLAN (Guest VLAN)**
选择所需设置。
如果选择“无变化”(No Change), 则表 2 中的条目保持不变。
- **访客 VLAN ID (Guest VLAN ID)**
选择所需设置。
如果选择“无变化”(No Change), 则表 2 中的条目保持不变。
- **访客 VLAN 允许的最大地址数 (Guest VLAN Max Allowed Addresses)**
指定“访客 VLAN”中此端口上允许同时存在几个终端设备。
如果选择“无变化”(No Change), 则表 2 中的条目保持不变。
- **Copy to table**
如果单击此按钮, 将为表 2 的所有端口应用这些设置。

表 2 包含以下列：

- **Port**
此列会列出此设备上的全部可用端口。
- **802.1X Auth.Control**
指定端口的身份验证：
 - **Force Unauthorized**
阻止通过该端口进行数据通信。
 - **Force Authorized**
允许通过该端口进行数据通信，无任何限制。
默认设置
 - **Auto**
在端口上使用“802.1X”方法对终端设备进行身份验证。
根据验证结果允许或阻止通过该端口进行数据通信。
- **802.1x Re-Authentication**
如果想要对已经过身份验证的终端设备周期性重复进行身份重新验证，请启用此选项。
- **MAC 身份验证 (MAC Authentication)**
如果想要使用“MAC 身份验证”方法对终端设备进行身份验证，请启用此选项。
如果“802.1x 身份验证控制”(802.1x Auth. Control) 组态为“自动”(Auto) 且“MAC 身份验证 (MAC Authentication) 已启用，则“802.1X 程序”的超时为 5 秒。如果使用 802.1X 程序进行身份验证时需要在端口上进行手动输入，5 秒时间可能不够。为了能够使用“802.1X”进行身份验证，需在该端口上禁用 MAC 身份验证。
- **采用 RADIUS VLAN 分配 (Adopt RADIUS VLAN Assignment)**
RADIUS 服务器将端口所属的 VLAN 通知工业以太网交换机。如果要考虑服务器通知的信息，请启用此选项。
如果设备上已创建 VLAN，则端口只能分配给 VLAN。否则拒绝身份验证 (页 274)。

- **MAC 验证允许的最大地址数**

指定可以同时端口上通信的 MAC 地址数目。

说明

如果设备使用多个 MAC 地址，则必须对所有 MAC 地址进行身份验证。将所有待身份验证的 MAC 地址存储到 RADIUS 服务器上。在“MAC 身份验证允许的最大地址数”(MAC Auth.Max Permitted Addresses) 框中输入数字。

- **访客 VLAN (Guest VLAN)**

如果想要在身份验证失败时在访客 VLAN 中使用终端设备，请启用此选项。

如果设备上已创建 VLAN，则端口只能分配给 VLAN。否则拒绝身份验证 (页 274)。

该功能也称为“Authentication failed VLAN”。

- **Guest VLAN ID**

输入访客 VLAN 的 VLAN ID。

- **访客 VLAN 允许的最大地址数**

输入“访客 VLAN”的此端口上可同时允许的终端设备数目。

- **802.1X Auth.Status**

显示端口身份验证的状态：

- Authorized
- Not Authorized

- **MAC 验证实际允许的地址数**

显示当前允许的 MAC 地址数。

- **MAC 验证实际屏蔽的地址数**

显示当前屏蔽的 MAC 地址数。

- **访客 VLAN 实际允许的地址数 (Guest VLAN Actual Allowed Addresses)**

显示“访客 VLAN”中当前允许的终端设备数量。

组态步骤

对单独的端口启用验证

1. 在表 2 相关行中选中所需选项。
2. 要应用更改，请单击“Set Values”按钮。

5.7 “Security”菜单

对所有端口启用验证

1. 在表 1 中选中所需选项。
2. 单击“Copy to table”按钮。表 2 中所有端口均采用相关设置。
3. 要应用更改，请单击“Set Values”按钮。

5.7.5 管理 ACL

组态说明

在此页面上，可提高设备的安全性。要指定具有哪个 IP 地址的工作站允许访问设备，必须组态相应的 IP 地址或一个地址范围。

可选择协议和端口，以便相关工作站可使用此信息访问设备。

Management Access Control List

Management ACL

IP Address:

Subnet Mask:

Select	Rule Order	IP Address	Subnet Mask	VLANs Allowed	SNMP	TELNET	HTTP	HTTPS	SSH	P0.1	P0.2
<input type="checkbox"/>	1	192.168.16.254	255.255.255.255	1-4094	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

1 entry.

显示框说明

说明

启用此功能前，请注意以下几点

组态错误可能意味着无法再对设备进行访问。只能通过将设备先复位到出厂默认设置，然后重新组态来解决此问题。因此应组态一个访问规则，以便在启用该功能前可对管理功能进行访问。

该页面包含以下框：

- **管理 ACL (Management ACL)**

启用或禁用针对管理工业以太网交换机进行的访问控制。

默认情况下会禁用该功能。

说明

如果禁用了该功能，则对工业以太网交换机管理功能的访问不受限制。组态的访问规则仅在该功能启用后有效。

- **IP 地址 (IP Address)**

输入将应用规则的 IPv4 地址或网络地址。如果使用 Pv4 地址 0.0.0.0，此设置适用于所有 IPv4 地址。

- **子网掩码 (Subnet Mask)**

输入子网掩码。子网掩码 255.255.255.255 适用于特定的 IPv4 地址。如果要允许使用子网（如 C 子网），则输入 255.255.255.0。子网掩码 0.0.0.0 适用于所有子网。

该表格包括以下列：

- **选择 (Select)**

选择要删除的行。

- **“规则顺序”(Rule Order)**

显示检查 ACL

规则的顺序。只要有规格符合要求，则立即启用。随后的规则将被忽略。

- **IP 地址 (IP Address)**

显示 IPv4 地址。

- **子网掩码 (Subnet Mask)**

显示子网掩码。

- **允许的 VLAN (VLANs Allowed)**

不能定义与 VLAN 相关的任何访问规则。规则适用于所有 VLAN。

说明

与旧固件版本的兼容性

如果已定义了固件版本低于 1.2 的 VLAN，则会在使用默认值“1-4094”进行固件更新时替换 VLAN 组态。

- **SNMP**

指定工作站（或 IPv4 地址）是否可以使用 SNMP 协议访问设备。

5.7 “Security”菜单

- **TELNET**
指定工作站（或 IPv4 地址）是否可以使用 TELNET 协议访问设备。
- **HTTP**
指定工作站（或 IPv4 地址）是否可以使用 HTTP 协议访问设备。
- **HTTPS**
指定相应工作站（或 IPv4 地址）是否可以使用 HTTPS 协议访问设备。
- **SSH**
指定相应工作站（或 IPv4 地址）是否可以使用 SSH 协议访问设备。
- **Px.y**
指定相应工作站（或 IPv4 地址）是否可以通过此端口访问设备。

端口由模块号和端口号组成，例如，端口 0.1 表示模块 0，端口 1。

组态步骤

说明

启用此功能前，请注意以下几点

错误的组态可能意味着无法再对设备进行访问。只能通过将设备先复位到出厂默认设置，然后重新组态来解决此问题。因此应组态一个访问规则，以便在启用该功能前可对管理功能进行访问。

说明

按顺序执行

创建 ACL

规则的顺序与检查这些规则的顺序一致。只要有规格符合要求，则立即启用。随后的规则将被忽略。

创建新的规则

1. 在“IP 地址”(IP Address) 输入框中输入 IP 地址。
2. 在“子网掩码”(Subnet Mask) 输入框中输入子网掩码。
3. 单击“Create”按钮在表中创建新行。
4. 组态新行的条目。
5. 单击“设置值”(Set Values) 按钮将新条目传输到设备。

启用功能

1. 选中“管理 ACL”(Management ACL) 复选框。
2. 单击“设置值”(Set value) 按钮启用组态的访问规则。

更改规则

1. 组态要更改的规则数据。
2. 单击“Set Values”按钮将更改传输到设备。

删除规则

1. 选中要删除的行中的复选框。
2. 对每个要删除的条目重复此步骤。
3. 单击“删除”(Delete) 按钮。将删除规则并更新页面。

5.7 “Security”菜单

故障排除/FAQ

6.1 使用 TFTP 下载新固件（无需 WBM 和 CLI）

固件

固件已签名且加密。这可确保只能将 Siemens 创建的固件下载到设备。

操作按钮

加载新固件需要该按钮。按下按钮时，请牢记相应操作说明中的信息。

轻按 SCALANCE XB-200 上的 RESET 按钮。

按 SCALANCE XC-200 上的 SELECT/SET 按钮。

用力按 SCALANCE XP-200 上的 RESET 按钮。

在 Microsoft Windows 下的步骤

即使在使用 WBM 或 CLI 无法访问设备的情况下，也可使用 TFTP 为设备提供新固件。本部分基于 Microsoft Windows 示例来说明步骤。

按照以下步骤使用 TFTP 加载新固件：

1. 关闭设备的电源。
2. 按下按钮并按住，重新连接设备的电源。
3. 按住按钮，直至红色故障 LED“F”开始闪烁。
4. 红色错误 LED 仍然处于闪烁状态时，释放该按钮。

说明

闪烁时间仅有几秒钟。

设备的引导加载程序在此状态下等待新固件文件，您可通过 TFTP 进行下载。

5. 通过以太网电缆将 PC 连接到端口 0.1。
6. 使用 DHCP 或 Primary Setup Tool 为设备分配 IP 地址。

6.1 使用 TFTP 下载新固件（无需 WBM 和 CLI）

7. 打开 Windows 命令提示并切换到保存新固件文件的路径，然后执行以下命令：

```
tftp -i <IP 地址> put <固件文件>
```

说明

可通过如下方式在 Microsoft Windows 中启用 TFTP：

“控制面板 > 程序和功能 > 打开或关闭 Windows 功能 > TFTP 客户端”(Control Panel > Programs and Features > Turn Windows features on or off > TFTP Client)

8. 固件完全传送到设备并经过验证后，设备将自动重启。这可能需要几分钟。

6.2 消息：尚未接受 SINEMA 组态

当显示区域中显示以下消息时，说明在将组态从 STEP 7 Basic / Professional（自版本 V13 起）传送到设备的过程中发生了错误：

“尚未接受 SINEMA 组态。重启设备后，所有组态更改都将丢失”(SINEMA Configuration not accepted yet. With restart of device, all configuration changes will be lost.)

其中一个可能原因是，设备在传输期间无法访问。

如果现在直接更改设备 (WBM/CLI/SNMP) 上的参数，这些更改将在设备重启时丢失。

解决方法

1. 在 STEP 7 Basic / Professional 中打开相关的 STEP 7 项目
2. 打开项目视图。
3. 在项目树中选择设备。
4. 在快捷菜单中选择“转到网络视图”(Go to network view) 命令。
5. 在网络视图中选择设备。
6. 在所选设备的快捷菜单中，选择命令“SCALANCE 组态 > 另存为启动组态”(SCALANCE configuration > Save as start configuration)。

结果

组态保存在设备上。显示区域中不再显示该消息。直接在设备上进行的组态更改不再因设备重启而丢失。

6.2 消息：尚未接受 SINEMA 组态

索引

A

ACL, 251, 292

C

CoS, 195

通信队列, 195

CoS (Class of Service, 服务类别), 41

C-PLUG, 178

保存组态, 180

格式化, 180

CRC, 78

D

DCP 转发, **Fehler! Textmarke nicht definiert.**

DCP 服务器, 96

DHCP

服务器, 126

客户端, 124

DSCP, 196

DST

夏令时, 148, 150

G

GMRP, 259

GVRP, 208

H

HRP, 220

HTTP

加载/保存, 108

HTTPS

服务器, 96

I

IGMP, 257

L

LACP, 238

LLDP, 84, 243

M

MSTP, 223, 230

端口, 226

端口参数, 232

MSTP 实例, 232, 233

N

Negotiation, 166

NFC, 98

NTP, 254

客户端, 157

P

Ping, 181

PLUG, 178

C-PLUG, (C-PLUG)

PoE, 182, 183

端口, 183

Primary Setup Tool, 241

PROFINET, 25, 174

PROFINET IO, 25

PST, Fehler! Textmarke nicht definiert.

Q

QoS, 197

QoS 信任, 41

R

RADIUS, 283

RESET 按钮, 162

RMON

历史, 266

统计信息, 264

RSTP, 223

S

SELECT/SET 按钮, 162, 297

SFP 诊断, 188

SHA 算法, 141

SIMATIC NET 手册, 11

SIMATIC NET 词汇表, 11

SMTP

客户端, 96

SNMP, 43, 97, 137, 141

SNMPv1, 43

SNMPv2c, 43

SNMPv3, 43

用户, 143

组, 141

陷阱, 139

概述, 91

SSH

服务器, 95

STEP 7, Fehler! Textmarke nicht definiert.

STP, 223

Syslog, 163

客户端, 96

T

Telnet

服务器, 95

TFTP

加载/保存, 111

V

VLAN, 39

VLAN ID, 42

VLAN 标记, 40

优先级, 210

标记, 210

端口 VID, 210

G

广播, 262

Z

子网掩码, 19

S H

手册适用范围, 9

R

冗余, 217, 220

冗余网络, 223

冗余程序

HRP, 28

Y

以太网供电, 182

端口, 183

以太网统计信息

历史, 79

帧类型, 77

接口统计信息, 74

数据包大小, 75

数据包错误, 78

B

本地用户, 276

K

可用的系统功能, 13

D

电子邮件功能, 122

报警事件, 122

线路监视, 122

电缆测试, 186

电源

监视, 171

S H

生成树, 222

MSTP, 223

RSTP, 223

快速生成树, 27

信息, 65

增强的被动侦听兼容性, 235

L

老化

动态 MAC 老化, 216

老化时间, 257

D

地理坐标, 100

G

过滤器

过滤器组态, 248

H

回路, 235

回路检测, 235, 235

W

网桥, 224

网桥优先级, 224

根网桥, 224

网桥最大老化时间, 225

网桥最大跳跃数, 225

Y

优先级, 197, 197, 225

D

多重生成树, 226, 230

A

安全设置, 141

F

访问控制, 249, 251
自动学习, 251

B

报警事件, 122

S H

时间设置, 96
时钟
NTP (网络时间协议), 157
SIMATIC 时间客户端, 160
SNTP (简单网络时间协议), 154
UTC 时间, 156, 158
手动设置, 146
时区, 156, 159
时钟同步, 154, 157
系统时间, 146

W

位置, 100

X

系统
组态, 95
常规信息, 99
系统手册, 11
系统事件
严重程度过滤器, 121
组态, 117

系统事件日志
代理, 163
序列号, 60

C

词汇表, 11

H

环网冗余, 217
HRP, 192, 218
MRP, 191, 218
环网端口, 219
备用, 220

S H

事件
日志表, 62
事件日志表, 62

Z H

转发延迟, 225

R

软件版本, 60

G

固件, 297

H

呼叫时间, 225

Z H

制造商, 59

G

供应商 ID, 60

M

命令行接口 (CLI), 297

F

服务等级 (Class of Service), 195

B

备用, 220

备用冗余, 38

Z H

注销

 自动, 161

X

线路监视, 122

Z

组态模式, 98

组播, 254

A

按钮, 162, 297

G

故障监视

 冗余, 174

 连接状态变化, 172

D

点对点, 27

Z H

重启, 104

F

复位, 104

X

信任模式, 197

信息

 ARP 表, 61

 LLDP, 84

 SNMP, 91, 92

 日志表, 62

 生成树, 65

 安全性, 93

 环网冗余, 69, 71

 版本, 58

 起始页面, 52

Q

起始页面, 52

G

根最大老化时间, 225

S

速率控制, 202

B

部件编号, 60

Y

验证, **Fehler! Textmarke nicht definiert.**, 287

J

基于 Web 的管理, 47

 要求, 47

基于 Web 的管理 (WBM), 297

D

第 2 层, 190

M

密码, 279

 选项, 281

W

维护数据, 59

Y

硬件版本, 60

D

登录

 通过 HTTP, 49

 通过 HTTPS, 49

C

错误状态, 64

错误类型

 CRC, 78

 Oversize, 78

 Undersize, 78

 长帧, 78

 过大, 78

 过小, 78

 冲突, 78

 碎片, 78

S H

数据包错误

 CRC, 78

 长帧, 78

 过大, 78

 过小, 78

 冲突, 78

 碎片, 78

数据包错误统计信息, 78

G

管理 ACL, 292

D

端口, 167

 端口组态, 165, 170

端口诊断

 SFP 诊断, 188

 电缆测试, 186

端口组态, 167, 170

J

镜像, 42

 常规, 212

 端口, 214

