SIEMENS

SIMATIC NET

Industrial Ethernet Switches SCALANCE Layer 2 Switches Web Based Management (WBM) V4.4

配置手册

SCALANCE XB-200
SCALANCE XC-200
SCALANCE XF-200BA
SCALANCE XF-200G
SCALANCE XP-200
SCALANCE XR-300WG

02/2023
C79000-G8952-C360-14

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 Siemens AG 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。

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
德国

C79000-G8952-C360-14
Ⓟ 02/2023 本公司保留更改的权利

目录

简介 1

1.1 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。其主要针对规划、调试和维护人员以及安保人员。其中包含了组态工业以太网交换机所需的信息。

如需了解如何正确安装和连接设备，请参见设备的操作说明。

1.2 手册适用范围

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 XF-200BA
- SCALANCE XF-200G
- SCALANCE XP-200
- SCALANCE XR-300WG

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，分别使用不同的订货号。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 4.4 起的 SCALANCE XB-200
- 自固件版本 4.4 起的 SCALANCE XC-200
- 自固件版本 4.4 起的 SCALANCE XF-200BA
- 自固件版本 4.4 起的 SCALANCE XF-200G
- 自固件版本 4.4 起的 SCALANCE XP-200
- 自固件版本 4.4 起的 SCALANCE XR-300WG

1.3 使用的标识

分类	说明	使用的术语
产品组	如果信息适用于产品组中的所有设备和设备变型，则会对产品组进行命名。	例如 SCALANCE XC-200
设备	如果信息与特定设备相关，则使用设备名称。	例如 SCALANCE XC206-2SFP
设备组	如果信息适用于某个特定的设备组，则使用相应的缩写表示。	-
	如果信息适用于 SCALANCE XC-200 的所有千兆位型号，则使用以下术语。	SCALANCE XC-200G

1.4 预定义默认设置

PROFINET 型号

- 环网冗余：开启
- 环网冗余模式：ARD 模式
- 生成树协议 (STP)：关闭
- 被动侦听：开启
- VLAN 提醒：关闭
- PROFINET 设备诊断：开启
- IGMP 监听：关闭
- IGMP 查询器：关闭
- IPv4 地址冲突检测 - 防御方法：Never give up
- EtherNet/IP 设备诊断：关闭
- QoS 信任模式：信任

EtherNet/IP 型号

- 环网冗余：关闭
- 环网冗余模式：关闭

- 生成树协议 (STP)：开启
- 被动侦听：关闭
- VLAN 提醒：开启
- PROFINET 设备诊断：关闭
- IGMP 监听：开启
- IGMP 查询器：开启
- IPv4 地址冲突检测 - 防御方法：Attempt to defend
- EtherNet/IP 设备诊断：开启
- QoS 信任模式：信任 CoS-DSCP

工业以太网配置文件

- 环网冗余：关闭
- 环网冗余模式：关闭
- 生成树协议 (STP)：开启
- 被动侦听：关闭
- VLAN 提醒：开启
- PROFINET 设备诊断：开启
- IGMP 监听：关闭
- IGMP 查询器：关闭
- IPv4 地址冲突检测 - 防御方法：Never give up
- EtherNet/IP 设备诊断：关闭
- QoS 信任模式：信任 CoS-DSCP

1.5 补充文档

Internet 上的文档

可访问 Internet 网址 (https://support.industry.siemens.com/cs/cn/zh/ps/15273/man)获取文档的最新版本

在搜索过滤器中输入产品的名称或订货号。

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：

- 《SCALANCE 第 2 层交换机命令行接口 (CLI)》组态手册，适用于 SCALANCE XB-200/XC-200/XF-200BA/XF-200G/XP-200/XR-300WG
  本文档包含工业以太网交换机支持的 CLI 命令。
- “SCALANCE XB-200”、“SCALANCE XC-200”、“SCALANCE XF-200BA”、“SCALANCE XF-200G”、“SCALANCE XP-200”和“SCALANCE XR-300WG”操作说明
  这些文档包含产品安装、连接和认证的相关信息。
  - 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 XF-200BA (https://support.industry.siemens.com/cs/ww/zh/ps/15287/man)
  - SCALANCE XF-200G (https://support.industry.siemens.com/cs/ww/en/ps/15285/man)
  - SCALANCE XP-200 (https://support.industry.siemens.com/cs/ww/zh/ps/21869/man)
  - SCALANCE XR-300WG (https://support.industry.siemens.com/cs/ww/zh/ps/15296/man)

1.6 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：

- Siemens 工业在线支持的 Internet 页面中的以下条目 ID：
  - 27069465 (https://support.industry.siemens.com/cs/de/en/view/27069465)
    《工业以太网/PROFINET 工业以太网》系统手册
  - 84922825 (https://support.industry.siemens.com/cs/de/en/view/84922825)
    《工业以太网/PROFINET - 无源网络组件》系统手册

1.7 本版本新增内容

V4.4 中引入了“默认安全”概念。此概念需要在工厂进行安全默认组态设置。在 V4.4 版本中，为 DCP 和 DHCP 客户端组态请求新增了“Setup”选项。有关更多信息，请参见“组态 (Configuration) (页 158)”和“DHCP 客户端 (页 199)”部分。此外，在交付状态下，无法通过 HTTP 和 Telnet 端口访问设备。

以下 WBM 页面已扩展为包含新的系统功能或参数：

- 信息 > 日志表：事件类型“警告/严重”（过去 24 小时） (页 116)
- 信息 > 以太网统计信息 > 接口统计信息：丢弃的数据包（过去 24 小时）/（过去 7 天） (页 130)
- 系统 > 组态：最低组态文件版本 (页 158)
- 系统 > NTP 服务器 (页 246)
- 系统 > DNS (页 167)
- 系统 > 故障监视 > 链路变化：摆动功能 (页 264)
- 系统 > 诊断 (页 267)
- 第 2 层 > RMON > 历史：默认值 (页 392)

自 V4.4 起，已针对以下设备或接口发布了现有系统功能：

- SCALANCE XR300WG：光纤监视协议 (FMP) 和端口类型“交换机端口 VLAN 中继”
- SCALANCE XF200、XB200、XR300WG：可组态多个 VLAN IP 接口
- 对于 SCALANCE XC200 PoE 的 10 Gbps 端口：端口精确时间协议 (PTP)

1.8 SIMATIC NET 词汇表

SIMATIC NET 词汇表

SIMATIC NET 词汇表描述了本文档中可能使用的术语。

要获取完整的 SIMATIC NET 词汇表，请访问西门子工业在线支持，网址为：

50305045 (https://support.industry.siemens.com/cs/ww/zh/view/50305045)

1.9 安全性信息

Siemens 为其产品及解决方案提供了工业信息安全功能，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信息安全保护机制。Siemens 的产品和解决方案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。只有在有必要连接时并仅在采取适当安全措施（例如，防火墙和/或网络分段）的情况下，才能将该等系统、机器和组件连接到企业网络或 Internet。

关于可采取的工业信息安全措施的更多信息，请访问 https://www.siemens.com/industrialsecurity (https://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 工业信息安全 RSS 源，网址为 https://www.siemens.com/cert (https://www.siemens.com/cert)

1.10 固件

固件/软件支持的说明

定期检查新固件/软件版本或安全更新并加以应用。新版本发布后，先前版本不再受支持，也不再进行维护。

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。

此固件可从西门子工业在线支持 (https://support.industry.siemens.com/cs/cn/zh/ps/15273/dl)的 Internet 页面获取：

1.11 开源许可证条款

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。

在所提供的数据介质中，下列文档提供有许可证条款：

- OSS_Siemens_86.pdf
- OSS_SCALANCE-XB-200-XC-200-XF-200BA-XP-200-XR-300WG_86.pdf

可在产品 DVD 中找到这些文档。

1.12 Marken

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：

SCALANCE, C-PLUG, OLM

说明 2

2.1 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 SCALANCE XC206-2SFP、SCALANCE XC-200G、SCALANCE XF-200G、SCALANCE XP216 和 SCALANCE XR-300WG）
  - 10 Gbps 全双工（带相应可插拔收发器的 SCALANCE XC-200G PoE、SCALANCE XC-200G PoE EEC 和 SCALANCE XR-300PoE WG）
  - 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较少网络中的负载。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。此外，还支持通过精确时间同步协议（PTP，IEEE 1588）进行时间同步。
- 型号标识中包含“PoE”的以太网供电 (PoE)
  设备支持“以太网供电”。

- 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)
- H-Sync 支持
  有关详细信息，请参见“环网 (页 325)”部分
- S2 设备（具有简单系统冗余的 PROFINET 组态）
  S2 设备可以建立两个到自动化系统的连接，每个应用关系 (AR) 都与两个 IO 控制器相连。当通信连接中断时，所有的数据和诊断功能仍可基于第二个连接使用。
  有关可用作 S2 设备的工业以太网交换机的信息，请参见“系统功能和硬件设备”部分。
  只能通过 STEP 7 Basic 或 Professional 组态 S2 设备。
  有关详细信息，另请参见：SIMATIC PCS 7 中的 PROFINET (https://support.industry.siemens.com/cs/ww/zh/view/72887082)
- CiR/H-CiR 支持（运行中组态）
  Configuration in Run (CiR) 是一种在运行期间进行系统和组态更改的功能。对于标准自动化系统和 H 系统 (H-CiR)，此功能的可用程度不同。
  有关支持 CiR 的工业以太网交换机的信息，请参见“系统功能和硬件设备”部分。
  只能通过 STEP 7 Basic 或 Professional 组态 CiR。
  有关详细信息，另请参见：SIMATIC PCS 7 中的 PROFINET (https://support.industry.siemens.com/cs/ww/zh/view/72887082)

2.2 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 XR-300WG	SCALANCE XC-200	SCALANCE XF-200G	SCALANCE XP-200	SCALANCE XF-200BA
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	✓ 1)	✓ 1)	✓	✓	✓	✓
	SNMP	✓	✓	✓	✓	✓	✓
	手动设置时间	✓	✓	✓	✓	✓	✓
	DST	✓	✓	✓	✓	✓	✓
	SNTP	✓	✓	✓	✓	✓	✓
	NTP	✓	✓	✓	✓	✓	✓
	SIMATIC 时间客户端	✓	✓	✓	✓	✓	✓
	自动注销	✓	✓	✓	✓	✓	✓
	Syslog 客户端	✓	✓	✓	✓	✓	✓
	NOA 交换机功能	-	-	✓ 4)	-	-	-
	故障监视	✓	✓	✓	✓	✓	✓
	PROFINET	✓	✓	✓	✓	✓	✓
	EtherNet/IP	✓	✓	✓	✓	✓	✓ 2)
	电缆测试器	✓	✓	✓	✓	✓	✓
	SFP 诊断	-	✓	✓	-	-	-

		SCALANCE XB-200	SCALANCE XR-300WG	SCALANCE XC-200	SCALANCE XF-200G	SCALANCE XP-200	SCALANCE XF-200BA
第 2 层	发送优先级	-	-	✓	✓	✓	✓
	CoS 映射	✓	✓	✓	✓	✓	✓
	DSCP 映射	✓	✓	✓	✓	✓	✓
	QoS 优先级	✓	✓	✓	✓	✓	✓
	CoS 端口重新分配	-	-	✓	✓	✓	✓
	下载控制	✓	✓	✓	✓	✓	✓
	GVRP	-	-	✓	✓	✓	✓
	基于端口的 VLAN	✓	✓	✓	✓	✓	✓ 2)
	专用 VLAN	-	-	✓	✓	✓	-
	提供商网桥	-	-	✓	✓	✓	-
	交换机端口 VLAN 中继	-	✓	✓	✓	✓	✓ 2)
	基于端口的镜像	✓	✓	✓	✓	✓	✓
	动态 MAC 老化	✓	✓	✓	✓	✓	✓
	环网冗余	✓	✓	✓	✓	✓	✓
	H-Sync 支持	-	-	✓	✓	✓	✓
	S2 设备	-	-	✓	✓	✓	✓
	CiR/H-CiR 支持	-	-	✓	✓	✓	✓
	采用 RSTP 的环网	✓	✓	✓	✓	✓	✓
	备用 (HRP)	✓	✓	✓	✓	✓	✓
	观察器 (HRP)	-	-	✓	✓	✓	✓
	链路检查	✓	✓	✓	-	-	✓
	MRP 多环网	✓	✓	✓	-	✓	-
	MRP 互连	✓	✓	✓	✓	✓	✓
	生成树	✓	✓	✓	✓	✓	✓
	RSTP	✓	✓	✓	✓	✓	✓
	RSTP+	✓	✓	✓	✓	✓	✓
	MSTP	-	-	✓	✓	✓	-
	增强的被动侦听兼容性	✓	✓	✓	✓	✓	✓

		SCALANCE XB-200	SCALANCE XR-300WG	SCALANCE XC-200	SCALANCE XF-200G	SCALANCE XP-200	SCALANCE XF-200BA
	回路检测	✓	✓	✓	✓	✓	✓
	链路汇聚/LACP	-	-	✓	✓	✓	✓
	DCP 转发	✓	✓	✓	✓	✓	✓
	LLDP	✓	✓	✓	✓	✓	✓
	光纤监视	-	✓	✓	-	-	-
	单播过滤器	✓	✓	✓	✓	✓	✓
	锁定端口	✓	✓	✓	✓	✓	✓
	单播学习	✓	✓	✓	✓	✓	✓
	单播阻止	✓	✓	✓	✓	✓	✓
	组播组	✓	✓	✓	✓	✓	✓
	IGMP	✓	✓	✓	✓	✓	✓
	GMRP	-	-	✓	✓	✓	✓
	组播阻止	✓	✓	✓	✓	✓	✓
	广播阻止	✓	✓	✓	✓	✓	✓
	PTP	-	-	✓ 3)	✓	-	-
	RMON	✓	✓	✓	✓	✓	✓
	RMON 历史	✓	✓	✓	✓	✓	✓
第 3 层	单跳 VLAN 间路由	-	-	✓	✓	✓	-
	DHCP 中继代理	✓	✓	✓	✓	✓	✓
	公共代理地址	-	-	✓	✓	✓	-
	NAT/NAPT	-	-	✓	✓	✓	-
Security	用户	✓	✓	✓	✓	✓	✓
	密码	✓	✓	✓	✓	✓	✓
	RADIUS 验证	✓	✓	✓	✓	✓	✓
	MAC 验证	✓	✓	✓	✓	✓	✓
	访客 VLAN	-	-	✓	✓	✓	✓
	802.1X 重新验证	✓	✓	✓	✓	✓	✓
	管理 ACL	✓	✓	✓	✓	✓	✓
	暴力破解预防	✓	✓	✓	✓	✓	✓

1) 受限

2) 不包括 DNA 设备

3) 仅 SCALANCE XC-200G

4) 仅 SCALANCE XC-200G EEC

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 XR-300WG	SCALANCE XC-200	SCALANCE XF-200G	SCALANCE XP-200	SCALANCE XF-200BA
C-PLUG 支持	-	-	✓	✓	✓	✓
SELECT/SET 按钮	-	-	✓ 2) 3)	-	✓ 3)	-
RESET 按钮	✓ 2)	✓ 2)	-	✓	✓ 2)	-
SET 按钮	-	-	-	-	-	✓ 2)
信号触点	-	-	✓	-	✓	✓
串口	✓	✓	✓	✓	✓	-
显示模式	-	-	✓	-	✓	-
可插拔收发器插槽	-	-	✓	-	-	-
组合端口	-	✓	✓	-	-	-
总线适配器插槽	-	-	-	-	-	✓
以太网供电	-	✓ 1)	✓ 1)	-	✓ 1)	-

1) 设备名称中有标识符“PoE”

按钮的功能：

2) 恢复出厂默认设置

3) 设置故障掩码

2.3 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 XR-300WG**	**SCALANCE XC-200**	**SCALANCE XF-200G**	**SCALANCE XP-200**	**SCALANCE XF-200BA**
系统	最大帧大小（传入）	1632 字节	10 KB	1632 字节/ 2048 字节 / 10 KB [7)]	10 KB	1632 字节/ 10 KB [8)]	1632 字节
	Syslog 服务器	3					
	电子邮件服务器	3					
	DHCP 池	16 [1)]	28 [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)]	28 [1)]	576			
	每个 DHCP 池的 DHCP 静态分配	-		24			
	SNMPv1 陷阱接收方	10					
	SNMPv3 用户	48					
	SNMPv3 组	41					
	SNMPv3 视图（包括两个默认视图）	46					
	SNTP 服务器	1 [9)]					
	NTP 服务器	1		4 [9)]			1
	代理/TIA 接口 [2)]	1					
	通过 DCP Discovery 显示的设备	100					

	可组态的功能	最大数量					
		SCALANCE XB-200	**SCALANCE XR-300WG**	**SCALANCE XC-200**	**SCALANCE XF-200G**	**SCALANCE XP-200**	**SCALANCE XF-200BA**
第 2 层	QoS 优先级队列	4		4/8 [6]	8	4	
	虚拟 LAN（基于端口，包括 VLAN 1）	257 [3]					
	专用 VLAN	-		1			-
	主 PVLAN	-		1			-
	隔离的次级 PVLAN	-		24			-
	次级社区 PVLAN	-		256			-
	镜像会话	1					
	备用端口	1					
	MRP 环网	4			1	4	1
	已组态 MRP 互连连接	64					
	已启用 MRP 互连连接	1		2			
	环网中启用了 MRP 互连的最大设备数	10					
	多重生成树实例	-		4			-
	链路汇聚	-		2/4/8 [5]			
	一个链路汇聚中的端口数	-		8	4	8	4
	静态单播地址	128					
	无活动 GMRP 的静态组播地址	256					
	有活动 GMRP 的静态组播地址	-		50			
	使用 IGMP 探听学习的地址	512					
第 3 层	VLAN IP 接口	24					
	DHCP 中继代理接口	1		24			1
	DHCP 中继代理服务器	4					
	NAT 接口	-		1			-
	动态 NAT 组态（池）	-		100			-
	静态 NAT 组态	-		100			-

	可组态的功能	最大数量					
		SCALANCE XB-200	**SCALANCE XR-300WG**	**SCALANCE XC-200**	**SCALANCE XF-200G**	**SCALANCE XP-200**	**SCALANCE XF-200BA**
安全性	用户	30 （包括出厂时预设的用户“admin”）					
	角色	29					
	组	32					
	RADIUS 服务器的 IP 地址	6					
	每台设备的同步 MAC 验证（验证和屏蔽）[4]	2000	-	2000			
	每个端口（可组态）的同步 MAC 验证（验证和屏蔽）[4]	200					
	管理 ACL（管理性访问规则）	10					

[1] 使用 SCALANCE XB-200 和 SCALANCE XR-300WG 时，DHCP 池和可管理 IPv4 地址数量取决于端口数量。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。

[3] 具有 Y 功能的设备不支持 VLAN。

[4] 如果超出每个设备的最大 MAC 验证数量，则重置数值超限的端口的所有 MAC 验证。
如果超出每个端口的最大 MAC 验证数量，则重置所有端口 MAC 验证。

[5] 由于一个链路汇聚至少包含 2 个端口，因此链路汇聚的最大数量取决于端口数量。
- 具有最多 4 个端口的设备最多可以有 2 个链路汇聚。
- 具有最多 8 个端口的设备最多可以有 4 个链路汇聚。
- 具有 8 个以上端口的设备最多可以有 8 个链路汇聚。

[6] SCALANCE XC-200G 产品组的设备支持 8 个队列。所有其它 XC-200 设备都支持 4 个队列。

[7] 对于以下设备，最大帧大小（入口）为 2048 字节：
- 具有组合端口的设备（型号标识的后缀为“C”）
- PoE 型（型号标识的后缀为“PoE”）

以下设备支持 10 KB 巨型帧：
- 所有千兆位型号（型号标识的后缀为“G”），还包括具有组合端口的型号
- 所有支持以太网供电的设备（型号标识的后缀为“PoE”）
- SCALANCE XC216-4C

对于其它所有 XC-200 设备，最大帧大小为 1632 字节。

[8] SCALANCE XP-200 的千兆位端口支持 10 KB 的巨型帧。对于其它所有端口，最大帧大小为 1632 字节。

[9] 可为设备组态的 NTP/SNTP 服务器的最大数。

2.4 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。如果没有可用的 DHCP 服务器，则必须使用安装了 SINEC PNI 的 PG/PC 来为工业以太网交换机首次分配 IP 地址。其它组态设置需要一台带有 Web 浏览器 (HTTPS) 或终端软件（SSH 客户端）的客户端 PC。

2.5 C-PLUG

注意
切勿在运行期间插拔 C-PLUG 只允许在设备关闭后取出或插入 C-PLUG。

保存组态数据

C-PLUG 是一种用于存储设备组态数据的可互换存储介质。设备更换将因此变得既方便又简单。将 C-PLUG 从原设备中取出并插入新设备中。在其首次启动时，更换设备将具有与原设备相同的组态（除了由供应商设置的设备特定的 MAC 地址之外）。

C-PLUG 存储设备组态的当前信息。

说明

没有 C-PLUG，设备也可以运行。

工作原理

运行模式

就 C-PLUG 而言，设备共有三种模式：

- 不带 C-PLUG
  设备将组态存储在内部存储器中。
  未插入 C-PLUG 时会激活此模式。
- C-PLUG 未写入数据
  如果使用未写入数据的 C-PLUG（出厂状态或使用“清理”功能删除），则在设备启动时，设备中已存在的本地组态将自动存储到插入的 C-PLUG 中。
  插入未写入数据的 C-PLUG 时会激活此模式。
- C-PLUG 已写入数据
  已写入并已接受 C-PLUG 的设备将在启动时自动使用 C-PLUG 中的组态数据。接受要求是以兼容设备类型写入数据。
  如果设备存储器中有组态数据，则会将其覆盖。
  插入已写入 C-PLUG 时就会激活此模式。

带 C-PLUG 情况下的操作

通过用户界面显示存储在 C-PLUG 中的组态。

如果更改了组态，则设备会将组态信息直接存储在 C-PLUG（如果处于“ACCEPTED”状态）上和内部存储器中。

对错误的响应

如果插入不包含兼容设备类型的组态数据的 C-PLUG、意外卸下 C-PLUG 或 C-PLUG 出现常规故障，则设备的诊断机制会进行指示。

- 故障 LED
- 基于 Web 的管理 (WBM)
- SNMP
- 命令行接口 (CLI)
- PROFINET 诊断

用户随即可以选择再次取出该 C-PLUG，或者选择重新格式化该 C-PLUG。

安全建议 3

3.1 安全建议

软件（安全功能）

- 保持固件为最新。定期检查设备的安全更新。有关这方面的信息，请参见工业安全(https://www.siemens.com/industrialsecurity)网站。
- 请持续关注由 Siemens ProductCERT (https://www.siemens.com/cert) 出版的安全建议。
- 仅激活使用设备所需的协议。
- 通过访问控制列表 (ACL) 中的规则限制对设备管理的访问。
- VLAN 结构化选项可针对 DoS 攻击和未经授权的访问提供保护。请检查该功能在您的环境下是否实用或有效。
- 通过中央记录服务器对更改和访问进行记录。在受保护的网络区域内运行记录服务器，并定期检查记录信息。

验证

说明

可访问性风险 - 数据损失风险

请勿丢失设备的密码。只能通过将设备复位为出厂设置（这会完全删除所有组态数据）来恢复对设备的访问。

- 使用设备之前，请更换所有用户帐户、访问模式和应用程序（如适用）的默认密码。
- 定义密码分配规则。
- 使用密码强度高的密码。避免使用密码强度弱的密码（如，password1、123456789、abcdefgh）或重复字符（如，abcabc）。
  此建议也适用于对设备组态的对称密码/密钥。
- 确保密码受保护且只透露给授权的人员。
- 请勿对多个用户名和系统使用相同的密码。
- 将密码存储在安全位置（非在线），以便在丢失时使用。
- 定期更改密码以提高安全性。

- 如果已知或者疑似有未经授权的人员知道了密码，则必须更改密码。
- 通过 RADIUS 执行用户验证时，请确保所有通信均在安全环境中进行或均受到安全通道的保护。
- 注意在端点之间不提供自身验证的链路层协议，例如 ARP 或 IPv4。攻击者可利用这些协议中的漏洞来攻击连接到您的第 2 层网络的主机、交换机和路由器，例如，通过操纵子网中系统的 ARP 缓存或使其中毒并随后拦截数据流量。对于非安全第 2 层协议，必须采取适当的安全措施，以防对网络进行未经授权的访问。对本地网络的物理访问可以是安全的，也可以使用更高层的协议。

证书和密钥

- 设备中有一个密钥长度为 2048 位的预设 SSL/TLS (RSA) 证书。将此证书替换为用户生成的含密钥高质量证书。使用由可靠外部或内部认证机构签署的证书。可通过 WBM（“System > Load and Save”）安装证书。
- 使用密钥长度为 4096 位的证书。
- 使用认证机构，包括密钥撤销与管理，来签署证书。
- 确保用户自定义的私人密钥都受到保护，未授权人员无法访问。
- 如果存在可疑的安全违规，请立即更改所有证书和密钥。
- 使用“PKCS #12”格式的具有密码保护的证书。
- 基于服务器和客户端侧的指纹验证证书，避免“中间人”攻击。为此，请使用第二条安全传输路径。
- 将设备送至 Siemens 进行维修之前，请使用临时的一次性证书和密钥替换当前证书和密钥，这些证书和密钥在设备返厂时会被销毁。

安全/非安全协议和服务

- 应避免使用或禁用非安全协议或服务，例如，HTTP、Telnet 和 TFTP。由于历史原因，这些协议可用，但并不适用于安全应用。请慎重对设备使用非安全协议。
- 检查是否有必要使用以下协议和服务：
  - 未验证和未加密的端口
  - MRP、HRP
  - IGMP 监听
  - LLDP
  - DCP
  - Syslog
  - RADIUS
  - DHCP 选项 66/67
  - TFTP
  - GMRP 和 GVRP
- 以下协议具有安全备选方法：
  - HTTP → HTTPS
  - Telnet → SSH
  - SNMPv1/v2c → SNMPv3
    检查是否有必要使用 SNMPv1/v2c。SNMPv1/v2c 的分类为非安全协议。使用阻止写访问的选项。设备会为您提供适合的设置选项。
    如果 SNMP 已启用，请更改团体名称。如果不需要不受限制的访问，请通过 SNMP 限制访问。
    使用 SNMPv3 的验证和加密机制。
  - TFTP → SFTP
  - NTP → NTPsecure
- 在物理保护措施未阻止设备访问时使用安全协议。
- 如果需要非安全协议和服务，请仅在受保护的网络区域内运行该设备。
- 将可用于外部的服务和协议限制到最少。
- 如果使用 RADIUS 来管理对设备的访问，需激活安全协议和服务。

3.2 可用服务

可用服务列表

以下是所有可用服务及其端口的列表，通过这些服务和端口可对设备进行访问。

该表包括以下列：

- **服务**
  设备支持的服务
- **默认端口状态**
  此为交付状态（出厂设置）下的端口状态。
- **可组态端口/服务**
  指示是否可通过 WBM/CLI 组态端口号或服务。
- **验证**
  指定是否对通信伙伴进行验证。
  如果可选，可根据需要组态验证。
- **加密**
  指定传输是否加密。
  如果可选，可根据需要组态加密。

以下是所有可用协议和服务以及用于访问设备的相应端口的列表。

服务	协议/端口号	默认端口状态	可组态		验证	加密 [5]
			端口	服务		
DHCPv4 Server	UDP/67	关闭	-	✓	-	-
DHCPv4 Client	UDP/68	打开	-	✓	-	-
EtherNet/IP	TCP/44818 UDP/2222 UDP/44818	已关闭（使用 EtherNetIP 型号打开）	-	✓	-	-
HTTP Server/Client [3]	TCP/80	关闭	✓	✓	✓	-
HTTPS WBM Server/ Client	TCP/443	打开	✓	✓	✓	✓
NTP Client	UDP/123	关闭	✓	✓	-	-
NTP (secure)	UDP/123	关闭	✓	✓	✓	-
PROFINET	UDP/34964 UDP/49151 ... 49159 [1]	打开	--	✓	-	-

服务	协议/端口号	默认端口状态	可组态		验证	加密 [5]
			端口	服务		
RADIUS Client	UPD/1812 [4] UPD/1813 [4]	仅限出站端口	✓	✓	-	-
	UDP/3799	打开	✓	✓	-	-
SFTP Server	UDP/22	仅限出站端口	✓	✓	✓	✓
SMTP Client	TCP/25	关闭	✓	✓	-	-
SMTP Client (secure)	TCP/465	关闭	✓	✓	✓	✓
SNMPv1/v2c [2] [3]	UDP/161	打开	✓	✓	-	-
SNMPv3	UDP/161	打开	✓	✓	可选	可选
SNMP Traps	UDP/162	仅限出站端口	--	✓	-	-
SNTP Client	UDP/123	关闭	✓	✓	-	-
SSH CLI Server	TCP/22	打开	✓	✓	✓	✓
Syslog Client	UDP/514	关闭	✓	✓	-	-
Syslog (secure) Client	TCP/6514	关闭	✓	✓	-	✓
Telnet [3]	TCP/23	关闭	✓	✓	✓	-
TFTP Client	UDP/69	仅限出站端口	✓	✓	-	-

1) 端口号可通过 WBM 组态。

2) 仅只读访问。

3) 协议符合默认安全。

4) 此端口默认关闭，并在组态了 RADIUS 服务器时显示。端口号可通过 WBM 组态。

5) 有关更多信息，请参见 WBM 附录“使用的加密方法”中使用的加密方法。

以下是所有可用第 2 层服务的列表，通过这些服务可对设备进行访问。

该表包括以下列：

- **第 2 层服务**
  设备支持的第 2 层服务。
- **默认状态**
  服务的默认状态（打开或关闭）。
- **服务可组态**
  指示是否可通过 WBM/CLI 组态服务。

第 2 层服务	默认值 状态	服务可组态
DCP	设置模式 [1)]	✓
LLDP	打开	✓
RSTP	关闭	✓
MSTP	打开	✓

1) 设置符合默认安全。

IP 地址分配

4

4.1 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 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。

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”。

4.2 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）
- **SINEC PNI** (SINEC Primary Network Initialization)
  此程序用于对网络设备进行初始调试，采用 DCP 协议检测网络中的设备并分配 IP 地址。有关详细信息，请参见“PNI (https://support.industry.siemens.com/cs/products?mfn=ps&pnid=26672&lc=zh-CN)”

- **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 XP-200：V5.5.4 HF9 及更高版本
    SCALANCE XC-200：V5.5.4 HF11 及更高版本
    SCALANCE XR-300WG：V5.6 及更高版本
    SCALANCE XF-200BA：V5.6 HF3 及更高版本
    SCALANCE XF-200G：Vxxx 及更高版本
    SCALANCE XC-200G：V5.6 HSP11 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
    SCALANCE XR-300WG：V15 及更高版本
    SCALANCE XF-200BA：V15 及更高版本
    SCALANCE XF-200G：Vxxx 及更高版本
    SCALANCE XC-200G，具有 8 个端口的设备：V15 及更高版本
    SCALANCE XC-200G，具有 8 个以上端口的设备：V16 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 地址的更多信息，请参见“SCALANCE Layer 2 Switches Command Line Interface (CLI)”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

交付产品时以及恢复出厂设置后，DHCP 为启用状态。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。

支持以下 DHCP 选项：

- DHCP 选项 66：分配动态 TFTP 服务器名称
- DHCP 选项 67：分配动态引导文件名称

4.3 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。
- 如果在经过租用时间后对新 IP 地址的请求未成功，则 IP 组态取决于“保持连接”功能。如果启用保持连接，则发生通信故障时，将保留 IP 地址，不会将其复位为 0.0.0.0。默认情况下保持连接处于启用状态。如果禁用保持连接，则发生通信故障时，IP 地址会复位为 0.0.0.0。
- 如果通过 DHCP 组态 IP 地址而 DHCP 遭到禁用，则 IP 组态取决于“保持连接”功能。如果禁用保持连接，则 IP 组态会复位为 0.0.0.0（“未组态”）。如果启用保持连接，将保留 IP 地址，不会将其复位为 0.0.0.0。
- 如果通过 DHCP 组态 IP 地址，而与网络的连接暂时中断（接口状态由“接通”变为“断开”，然后再变为“接通”），则首先需要由 DHCP 服务器确认 IP 组态。如果无法确认，则 IP 组态将复位为 0.0.0.0（“未组态”），并会从 DHCP 服务器请求新的 IP 组态。
- 如果某一设备的 DHCP 曾处于活动状态，则首先需要在 DHCP 服务器重启后从该服务器请求新的 IP 地址。
- 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。地址可通过 MAC 地址、DHCP 客户端 ID、PROFINET 或系统名称进行分配。在“系统 > DHCP > DHCP 客户端”(System > DHCP > DHCP Client (页 199)) 中组态参数。
- 如果组态了静态 IP 地址并启用了 DHCP，则 IP 组态取决于“保持连接”功能。如果禁用“保持连接”，则开启 DHCP 时，IP 地址会设置为 0.0.0.0，并且 DHCP 服务器预计会提供新的 IP 地址。如果 DHCP 服务器未分配地址，将无法再通过 IP 访问交换机。

技术基础

5

5.1 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 269) 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。

5.2 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 271)”(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 173)”(System > Load&Save) 中找到 EtherNet/IP 操作所需的 EDS。

5.3 冗余机制

5.3.1 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。

5.3.1.1 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 BPDU，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 BPDU，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）
- 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。

5.3.2 RSTP+

5.3.2.1 RSTP+ 的属性和功能

RSTP+ 主要用于将 MRP 环网冗余集成到 RSTP 网络中。通常，只需使用 RSTP 即可管理此类网络。但是，在环型拓扑中，MRP 方法更高效且更快速。MRP 环网冗余模式不受 RSTP+ 的影响，因为这两种模式相互独立地工作。

另一个应用实例是 MRP 环网的冗余连接。还可以使用 RSTP+ 基于一个 MRP 环网连接两个 RSTP 网络。如果不使用 RSTP+，则无法实现该连接，因为生成树在环网端口上已禁用。

说明

多环网管理器阻止生成树组态

如果在一台设备上组态了多个环网，则不能同时组态 RSTP 或 RSTP+。这也适用于已为环网端口禁用生成树的情况。

不使用 RSTP+ 时的设备兼容性

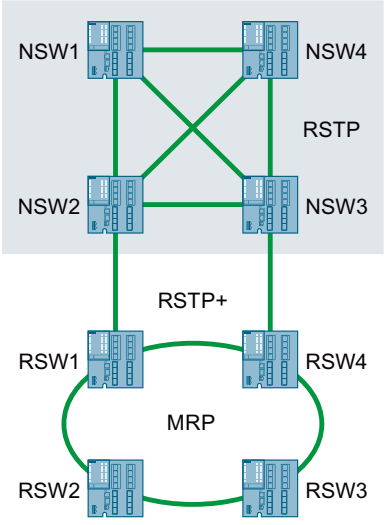
原则上，RSTP 网络与 MRP 环网之间连接点处的所有设备都必须支持 RSTP+ 方法。MRP 环网中的所有其它设备都必须转发 BPDU（桥接协议数据单元）。

5.3.2.2 RSTP+ 的拓扑

RSTP 网络和 MRP 环网

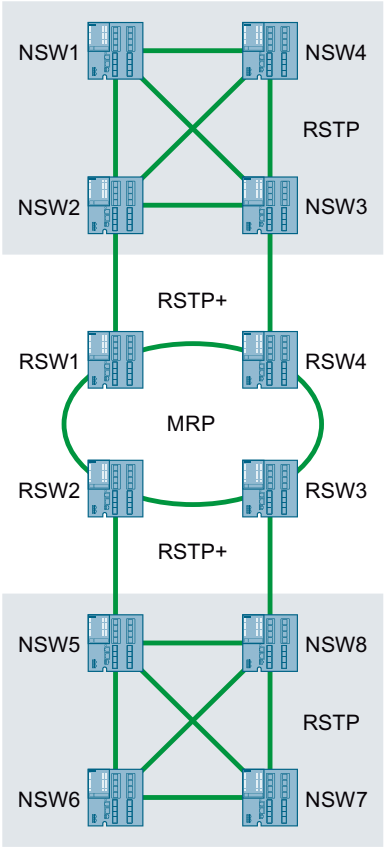
如果不使用 RSTP+，则无法将 MRP 环网冗余集成到 RSTP 网络中，因为不允许在一个端口上并行操作 RSTP 和 MRP。只有连接到 RSTP 网络的 MRP 环网的设备必须支持 RSTP+。在显示的示例拓扑中，这些设备为 RSW1 和 RSW4。其它设备必须转发 BPDU。

图形中设备的标识是指设备各自的功能。“NSW”是“网络交换机”(network switch) 的缩写，“RSW”是“环网交换机”(ring switch) 的缩写。



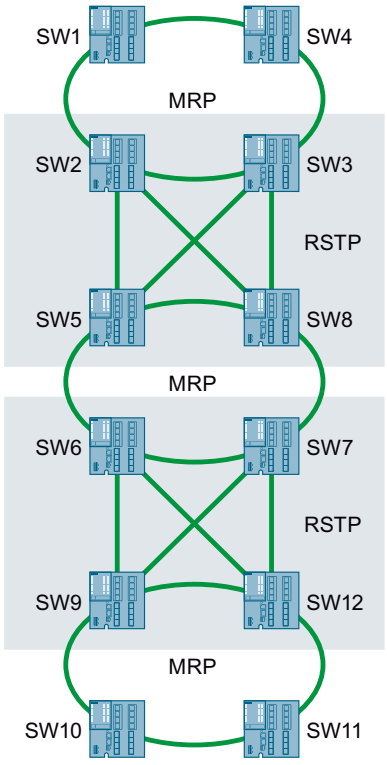
多个 RSTP 网络区域和 MRP 环网

RSTP+ 的另一个应用实例是基于一个 MRP 环网连接两个或多个 RSTP 网络区域。连接到其中一个 RSTP 网络的 MRP 环网中的所有设备都必须启用 RSTP+。在此处示例中，这些设备为 RSW1、RSW2、RSW3 和 RSW4。



多 MRP 环网

RSTP+ 还可用于通过 RSTP 将多个 MRP 环网彼此相互连接。在这种情况下，RSTP+ 确保 MRP 仍可管理环网冗余且不受 RSTP 影响。

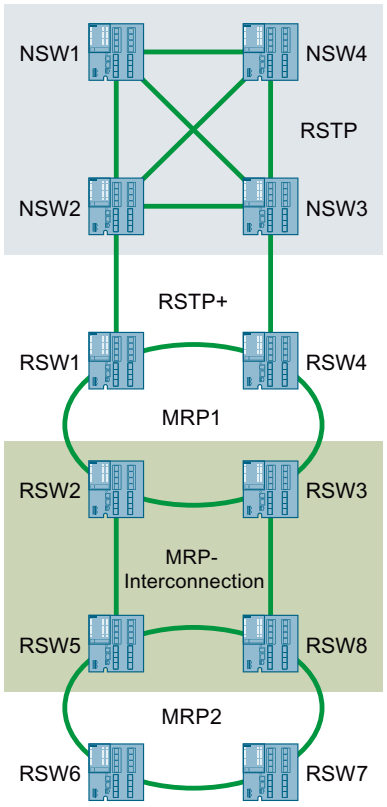


RSTP 网络和两个使用 MRP 互连的 MRP 环网

RSTP+ 还可以将 RSTP 网络连接到两个通过 MRP 互连链接的 MRP 环网。在显示的示例拓扑中，设备 RSW1 和 RSW4 必须支持 RSTP+。两个 MRP 环网连接中涉及的设备（RSW2、RSW3、RSW5 和 RSW8）必须支持 MRP 互连。此外，设备 RSW2 和 RSW3 必须转发 BPDU（桥接协议数据单元）。

以下规则适用于所示示例中的 RSTP+ MRP 互连域 ID：

- 必须为设备 RSW1 和 RSW4 组态相同的 RSTP+ MRP 互连域 ID。
- 必须为设备 RSW2、RSW3、RSW5 和 RSW8 组态相同的 RSTP+ MRP 互连域 ID。
- 设备 RSW1 和 RSW4 的 RSTP+ MRP 互连域 ID 必须不同于设备 RSW2、RSW3、RSW5 和 RSW8 的 RSTP+ MRP 互连域 ID。



5.3.2.3 组态 RSTP+

本部分详细介绍 RSTP+ 组态期间的步骤。为要在其中启用 RSTP+ 的所有设备执行组态步骤。屏幕截图中的位置编号是指步骤序列的相应编号。说明适用于尚未组态（出厂设置）的设备。

说明包括三个部分：

- 组态生成树：步骤 1 至 4 (页 49)
- 启用 RSTP+：步骤 5 (页 52)
- 组态环网冗余：步骤 6 至 8 (页 52)
- 插入电缆：步骤 9 (页 53)

常规组态规则

在组态期间请遵守以下规则；无论是否为特定网络拓扑，这些规则都适用：

- RSTP+ 只能与生成树协议结合使用。
- 在位于 MRP 环网中 RSTP 网络的两个链路点的交换机上启用 RSTP+。

- 还必须在两个链路设备上组态环网冗余。不应将冗余管理器的功能分配给 RSTP/MRP 链路的两个设备之一。
- 链路设备的两个环网端口之间应该存在直接 LAN 连接。
- 对于与 RSTP 相连的环网中除链路设备外的环网节点，建议在 RSTP 上启用“被动侦听”(Passive Listening)。在“第 2 层 > 组态”(Layer 2 > Configuration) 页面上启用“被动侦听”(Passive Listening)。

5.3.2.4 组态 RSTP+ 的生成树

在 WBM 中，可以使用菜单“第 2 层 > 生成树”(Layer 2 > Spanning Tree) 来组态生成树。

组态过程取决于要组态的设备的默认设置。因此，设备根据其默认设置分为两组：

- 组 1：启用环网冗余并禁用生成树。
- 组 2：禁用环网冗余并启用生成树。

对于第一组中的设备，首先需要禁用环网冗余并启用生成树。从第 3 步开始，两个组的组态相同。有关预定义设备设置的信息，请参见“预定义默认设置 (页 12)”部分。

对第一组中具有默认设置的设备执行步骤 1 至 2，或对第二组中的设备执行步骤 3 及后续步骤，然后为要启用 RSTP+ 的每个设备继续执行组态（步骤 3 至 4）。

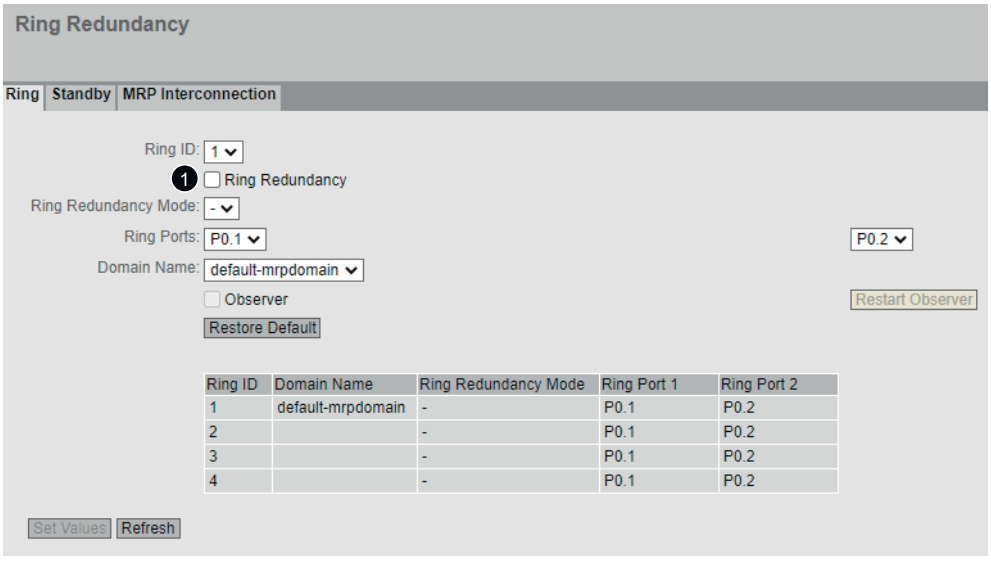
在此过程中会自动进行所需的端口设置。

步骤 1：禁用环网冗余

说明

只需对第 1 组具有默认设置的设备执行此步骤。

导航到菜单“第 2 层 > 环网冗余 > 环网”(Layer 2 > Ring Redundancy > Ring)，然后清除“环网冗余”(Ring Redundancy) 复选框。单击“设置值”(Set Values)。

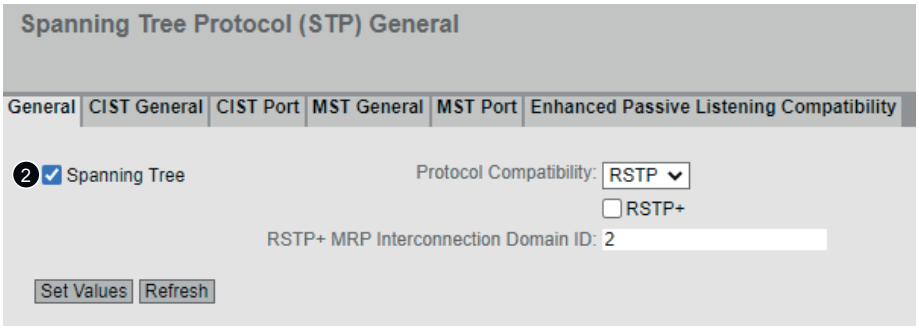


步骤 2：启用生成树

说明

只需对第 1 组具有默认设置的设备执行此步骤。

导航到菜单“第 2 层 > 生成树 > 常规”(Layer 2 > Spanning Tree > General)，然后选中“生成树”(Spanning Tree) 复选框。

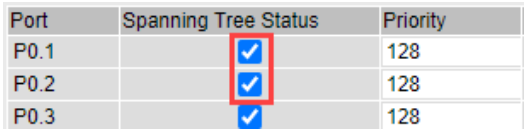


在“CIST 端口”(CIST Port) 或“ST 端口”(ST Port) 页面上，检查菜单“Layer 2 > Spanning Tree”中的环网端口设置。

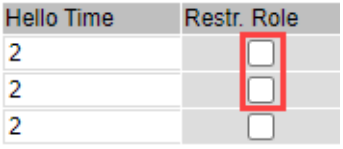
可通过该页面上的表格来组态各个端口的“生成树”(Spanning Tree)。

必要时，可根据要求调整以下设置：

- 必须选中表格列“生成树状态”(Spanning Tree Status) 中两个环网端口的复选框。

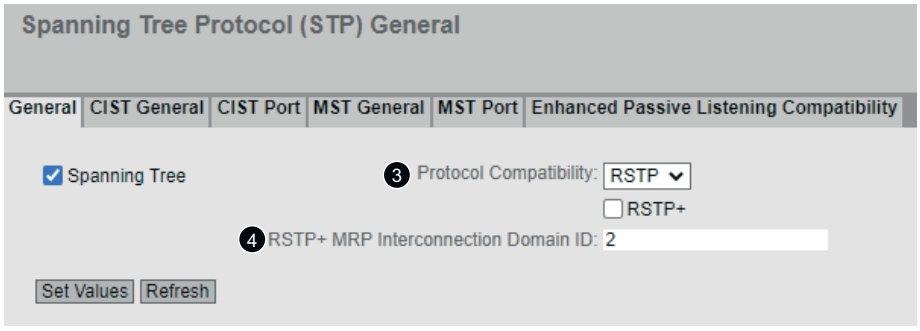


- 必须清除表格列“受限角色”(Restr. Role) 中两个环网端口的复选框。这是必要的，以便环网端口的行为完全由 MRP（冗余管理器）控制。MRP 的功能不受 RSTP+ 影响。



步骤 3：组态协议兼容性

在“协议兼容性”(Protocol Compatibility) 下拉列表中，选择项“RSTP”。



步骤 4：指定 RSTP+ MRP 互连域 ID

输入 RSTP+ MRP 互连域 ID 的值。

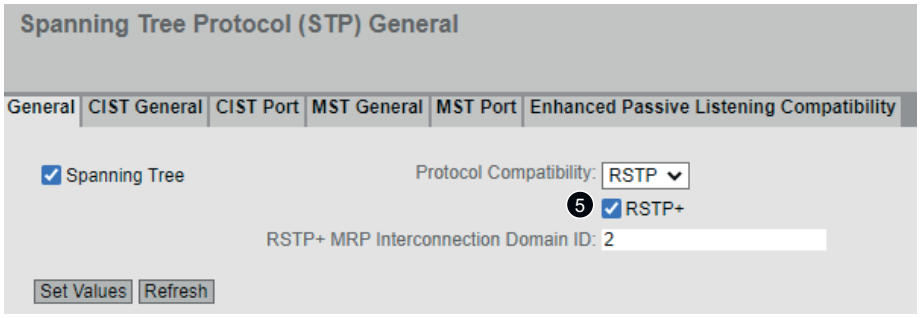
RSTP+ MRP 互连域 ID 在整个网络中必须唯一且不同于可能需要组态的任何 MRP 互连域 ID。需要使用不同的 ID 来区分 RSTP 网络的 TCN（拓扑更改通知）与 MRP 环网的 TCN。可通过此分配仅删除受拓扑更改影响的 FDB 条目（转发数据库条目）。

每个设备检查是否为这两个参数组态了不同的值。如果 ID 相同，则设备将输出一条错误消息。网络管理员负责确保这些 ID 在整个网络中也是唯一的。单个设备不能进行此类检查。

5.3.2.5 启用 RSTP+

步骤 5：启用 RSTP+

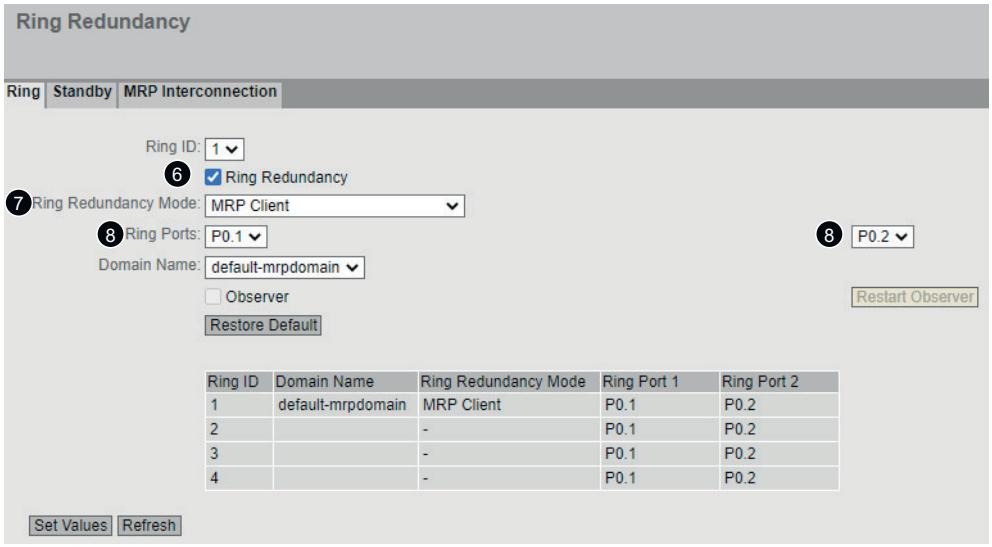
在“第 2 层 > 生成树 > 常规”(Layer 2 > Spanning Tree > General) 菜单中，选中“RSTP+”复选框，然后单击“设置值”(Set Values) 按钮保存组态。



当 RSTP+ 已启用时，无法更改以前组态的参数。

5.3.2.6 组态 RSTP+ 的环网冗余

在 WBM 中，可以使用菜单“第 2 层 > 环网冗余”(Layer 2 > Ring Redundancy) 来组态环网冗余。在“环网”(Ring) 页面上，为要在其中启用 RSTP+ 的每个设备执行步骤 6 至 8。



步骤 6：启用环网冗余

从“环网 ID”(Ring ID) 下拉列表中选择要组态的冗余环网 1，然后在此环网上选择“环网冗余”(Ring Redundancy) 来启用 MRP。

步骤 7：分配 MRP 角色

在“环网冗余模式”(Ring Redundancy Mode) 下拉列表中选择“MRP 客户端”(MRP Client)、“MRP 管理器”(MRP Manager) 或“MRP 自动管理器”(MRP Auto Manager) 条目。不应将冗余管理器的角色分配给 RSTP MRP 链路的两个设备中的任何一个。

步骤 8：指定环网端口

从两个下拉列表中选择环网端口的匹配条目。

最后，单击“设置值”(Set Values) 按钮保存组态。

5.3.2.7 插入电缆

步骤 9：插入电缆

当已组态了所有设备时，根据计划的拓扑插入电缆。RSTP+ 方法现已激活。

5.3.3 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

HRP

- 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。
- 备用端口必须在生成树中禁用。
- 您可在基于 Web 的管理、命令行接口中或通过 SNMP 组态 HRP。

备用冗余

- 如有备用耦合伙伴，HRP 必须永久设置。
- 备用耦合伙伴端口必须在生成树中禁用。
- 您可在基于 Web 的管理、命令行接口中或通过 SNMP 来组态备用冗余。

5.3.4 MRP

5.3.4.1 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 62439-2:2016 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。

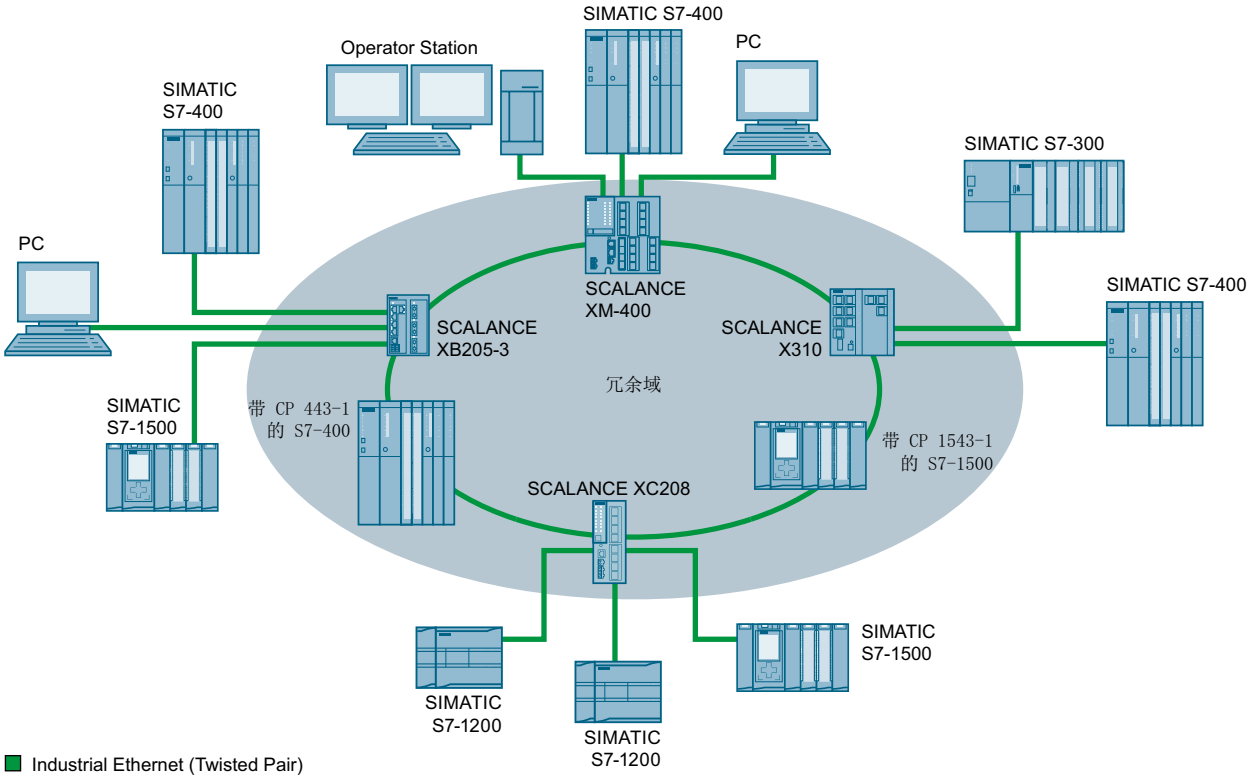


图 5-1　支持 MRP 介质冗余协议的环型拓扑示例

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启用“MRP”。
- 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。

说明

设备数

除了 PROFINET IO 系统，含有多达 120 个 SCALANCE X 交换机固件版本 4.3.1 及更高版本的 MRP 环网拓扑也已成功通过测试。

要求：

- 所有环网端口的连接设置（传送介质/双工）必须已设置为全双工和至少 1 Gbps。

5.3.4.2 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 290)
- 环网 (页 325)

5.3.4.3 STEP 7 中的组态

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“Media redundancy”。

为设备的 MRP 组态设置以下参数：

- 域
- 角色
- 环网端口
- 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 XC-200（EtherNet/IP 型号）
- SCALANCE XC-300
- SCALANCE XP-200（EtherNet/IP 型号）
- SCALANCE XR-300
- SCALANCE XR-300WG
- SCALANCE XM-400
- SCALANCE XR-500

要将采用 MRP 的 PROFINET 组态下载到其中一个指定的设备中，请禁用设备上的“生成树”(Spanning Tree)。也可以仅为环网端口禁用生成树。

说明

只有环网处于打开状态时才能重新组态

在执行下述操作之前，首先打开环网

- 更改 MRP 角色，或
- 重新组态环网端口。

说明

启动和重启

设备重启或电源故障和热启动后，只要组态更改之后 90 秒内未发生电源故障，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“Not a node in the ring”。

域

单 MRP 环网

如果要组态单 MRP 环网，请在“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。在单个环网中，一台设备不能属于一个以上的冗余域。

多 MRP 环网

借助 MRP 多环网功能，可使用一台中央冗余管理器控制多个 MRP 环网。如果组态多个单独 MRP 环网，将使用“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。

如果要组态 MRP 多环网，可选择能够处理多个环网的设备作为中央冗余管理器。为所有环网实例指定不同的域，并将其分配给冗余管理器的相应环网端口。将其它设备组态为客户端。必须为环网内的所有设备设置相同的域。

下图显示的可能组态由 4 个 MRP 多环网组成，这 4 个 MRP 多环网由作为中央冗余管理器的 SCALANCE XC208 管理。

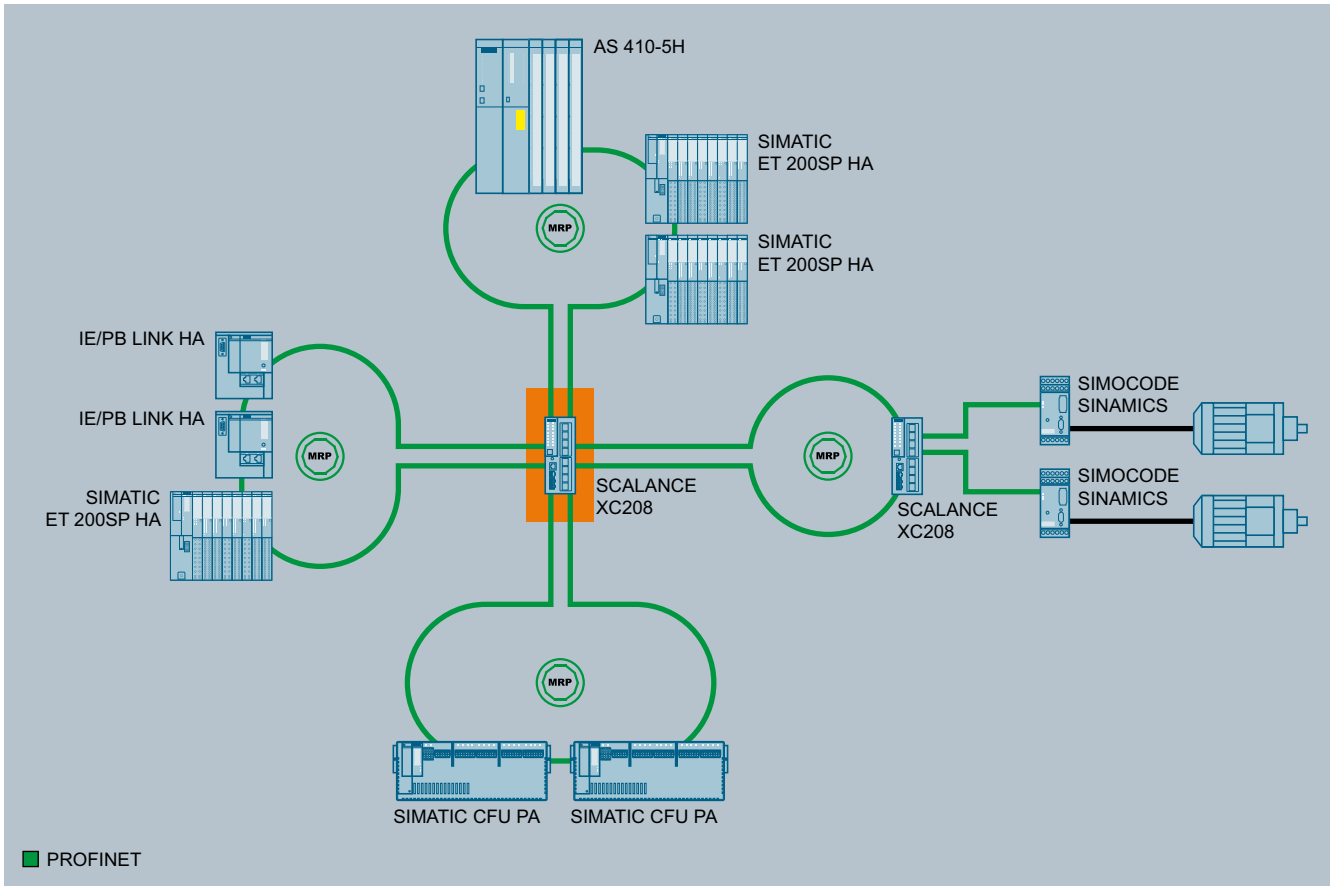


图 5-2　MRP 多环网拓扑

说明

适合 MRP 多环网的设备

可将以下产品线中的所有产品用作连接多环网的冗余管理器：

- 自固件版本 V4.0 起的 SCALANCE X-300
- 自固件版本 V4.0 起的 SCALANCE X408-2
- 自固件版本 V3.10 起的 SCALANCE X414-3E
- 自固件版本 V4.3 起的 SCALANCE XB-200
- 自固件版本 V4.3 起的 SCALANCE XC-200
- 自固件版本 V1.0 起的 SCALANCE XC-300
- 自固件版本 V4.3 起的 SCALANCE XP-200
- 自固件版本 V1.0 起的 SCALANCE XR-300
- 自固件版本 V4.3 起的 SCALANCE XR-300WG
- 自固件版本 V6.4 起的 SCALANCE XM-400
- 自固件版本 V6.4 起的 SCALANCE XR-500

说明

适合 MRP 互连的设备

可将以下产品线中的所有产品用作介质冗余互连管理器和介质冗余互连客户端：

- 自固件版本 V4.3 起的 SCALANCE XB-200
- 自固件版本 V4.2 起的 SCALANCE XC-200
- 自固件版本 V1.0 起的 SCALANCE XC-300
- 自固件版本 V4.2 起的 SCALANCE XF-200BA
- 自固件版本 V4.4 起的 SCALANCE XF-200G
- 自固件版本 V4.2 起的 SCALANCE XP-200
- 自固件版本 V1.0 起的 SCALANCE XR-300
- 自固件版本 V4.3 起的 SCALANCE XR-300WG
- 自固件版本 V6.3 起或自固件版本 V6.2 起（对于同构网络）的 SCALANCE XM-400
- 自固件版本 V6.3 起或自固件版本 V6.2 起（对于同构网络）的 SCALANCE XR-500

角色

说明

只有环网处于打开状态时才能重新组态

在重新组态环网管理器的环网端口之前，先打开环网。

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。
- 希望在仅包含西门子设备的**多环网**拓扑中使用 MRP 且不监视诊断中断：
  – 为连接到环网的设备的所有实例分配“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

在将环网中的设备复位为出厂设置之前，请先打开环网。

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 XB-200（PROFINET 型号）
  - SCALANCE XC-200（PROFINET 型号）
  - SCALANCE XF-200BA
  - SCALANCE XF-200G
  - SCALANCE XP-200（PROFINET 型号）
  - SCALANCE X-300
  - SCALANCE X-400

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 XC-200（EtherNet/IP 型号）
- SCALANCE XC-300
- SCALANCE XP-200（EtherNet/IP 型号）
- SCALANCE XR-300
- SCALANCE XR-300WG
- 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。

说明

只有环网处于打开状态时才能重新组态

在重新组态环网管理器的环网端口之前，先打开环网。

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 STEP7 设置冗余参数分配（冗余替代）

该选项会影响所有 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，在 STEP7 中进行组态时，请选择该选项。

如果启用该选项，则保留现有冗余设置，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。

说明

为环网中的设备启用“备用冗余”(Alternative redundancy) 选项并且通过 STEP7（控制器）监视拓扑时，还必须为环网中的其它设备启用“备用冗余”(Alternative redundancy) 选项。

5.3.5 MRP 互连

5.3.5.1 拓扑及其工作原理

MRP 互连模式是 MRP 的扩展，可实现两个或多个 MRP 环网的冗余链接。等时同步实时 (IRT) 网络不具有此功能。如同 MRP，MRP 互连是在标准 IEC 62439-2 中指定的。MRP 互连允许非常快速的重新组态；重新组态时间通常小于 200 毫秒。

拓扑

下图显示两个 MRP 环网的冗余链路。每个环网中需要一个耦合对来实现冗余耦合。每个 MRP 环网最多允许出现 5 个耦合对。

有关每台设备的最大活动 MRP 互连连接数的信息，请参见“组态限制”部分。

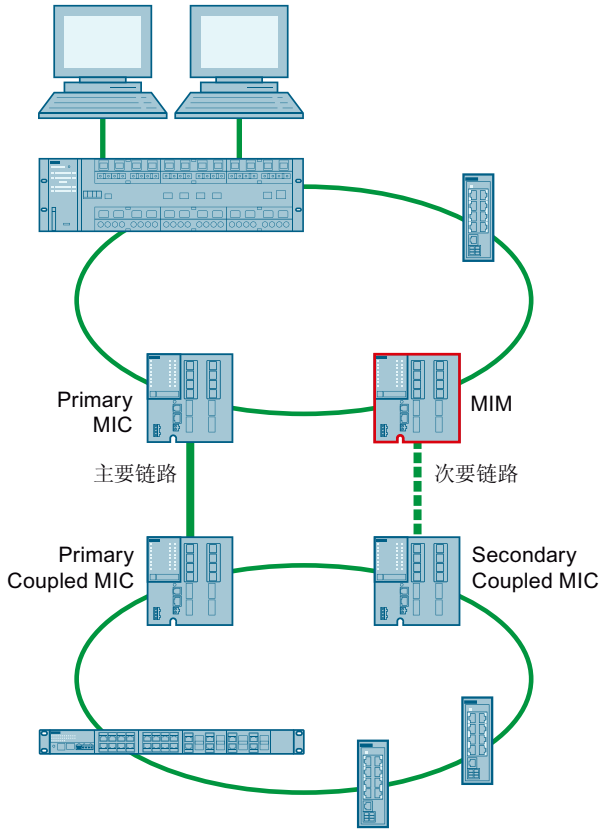


图 5-3　使用 MRP 互连冗余连接两个 MRP 环网

工作原理

MRP 互连的要求是在所有涉及的环网中使用 MRP。两个 MRP 互连连接需要四台设备：

- 一个介质冗余互连管理器（MIM，在图中用红色边框显示）
- 三个介质冗余互连客户端（主要 MIC、主要耦合 MIC 和次要耦合 MIC）

因为每个设备都是 MRP 环网的一部分，所以每个设备也用作为 MRP 定义的其中一个角色，即 MRP-Client 或 MRP-Manager。

根据互连端口的连接状态，Primary MIC 和 Primary Coupled MIC 将状态消息（“链路接通”(Link up) 或“链路断开”(Link down)）发送给 MIM。互连端口是通过主要或次要链路进行连接的端口。这意味着 MIM 始终获得关于主要 MIC 和主要耦合 MIC（“主要链路”）之间的连接状态以及其自身与次要耦合 MIC（“次要链路”）的连接的通知。在常规操作中，两个环网之间的数据交换是通过主要链路进行的并且 MIM 会阻止其互连端口。如果将主要链路的“链路断开”(Link down) 信号发送给 MIM，则 MIM 会将其互连端口切换到“转发”(Forwarding) 状态，且两个环网之间的数据交换会通过 MIM 和次要耦合 MIC 之间的次要链路进行。

5.3.5.2 适合 MRP 互连的设备

适合 MRP 互连的设备

互连管理器、互连客户端和所有环网管理器都必须支持 MRP 互连。以下设备就是这种情况：

- 自固件版本 V4.3 起的 SCALANCE XB-200
- 自固件版本 V4.2 起的 SCALANCE XC-200
- 自固件版本 V1.0 起的 SCALANCE XC-300
- 自固件版本 V4.2 起的 SCALANCE XF-200BA
- 自固件版本 V4.4 起的 SCALANCE XF-200G
- 自固件版本 V4.2 起的 SCALANCE XP-200
- 自固件版本 V1.0 起的 SCALANCE XR-300
- 自固件版本 V4.3 起的 SCALANCE XR-300WG
- 自固件版本 V6.3 起或自固件版本 V6.2 起（对于同构网络）的 SCALANCE XM-400
- 自固件版本 V6.3 起或自固件版本 V6.2 起（对于同构网络）的 SCALANCE XR-500

IEC62439-2 Ed.2 和 IEC62439-2 Ed.3

从 IEC62439-2 版本 2 转换到 IEC62439-2 版本 3 时，添加或编辑了一些与 MRP 互连有关的定义。出于互操作性的原因，引入了用于 MRP 互连的其它 MAC 地址等。因此，相对于以前标准中的要求，用于 MRP 互连的 MAC 地址已更改。本节描述了此更改对 SCALANCE 设备操作的影响。

SCALANCE XM-400 和 SCALANCE XR-500 的固件版本 V6.2

当所有设备的固件版本均为 V6.2 时，基于固件版本 V6.2 的 MRP 互连仅适用于 SCALANCE XM-400 和 SCALANCE XR-500 的同构网络。

注意
固件版本 V6.2 的异构网络中没有 MRP 互连 使用 SCALANCE XM-400/SCALANCE XR-500 和固件版本 V6.2 在异构网络中激活 MRP 互连会导致网络故障。通常不应在此类网络中启用 MRP 互连功能。

SCALANCE XM-400 和 SCALANCE XR-500 的固件版本 V6.3

自固件版本 V6.3 起，MRP 互连已发布用于 SCALANCE XM-400 和 SCALANCE XR-500 设备，并且使用不受限制。

注意
针对 MRP 互连的固件更新 对于网络中已存在的 SCALANCE XM-400 和 SCALANCE XR-500 设备，需要将固件版本更新到 V6.3 才能确保 MRP 互连功能正常。

在以下情况中，异构网络中的 SCALANCE 设备可以使用 MRP 互连功能：

- 所有 SCALANCE XM-400 和 SCALANCE XR-500 设备的固件版本均为 V6.3 或更高版本。
- 所有 SCALANCE XC-200、SCALANCE XF-200BA 和 SCALANCE XP-200 设备的固件版本均为 V4.2 或更高版本。
- 所有 SCALANCE XB-200 和 SCALANCE XR300WG 设备的固件版本均为 V4.3 或更高版本。
- 所有 SCALANCE XF-200G 设备的固件版本均为 V4.4 或更高版本。
- 所有 SCALANCE XC-300 和 SCALANCE XR-300 设备的固件版本均为 V1.0 或更高版本
- 所有其它网络组件均符合 IEC 62439-2 版本 3 的要求。

SCALANCE XC-200、SCALANCE XF-200BA 和 SCALANCE XP-200 的固件版本 V4.2

自固件版本 V4.2 起，MRP 互连已发布用于 SCALANCE XC-200、SCALANCE XF-200BA 和 SCALANCE XP-200 设备，并且使用不受限制。自固件版本 V6.3 起，可以通过 MRP 互连将指定设备与 SCALANCE XM-400 和 SCALANCE XR-500 设备耦连在一起。

SCALANCE XB-200 和 SCALANCE XR-300WG 的固件版本为 V4.3

自固件版本 V4.3 起，MRP 互连已发布用于 SCALANCE XB-200 和 SCALANCE XR-300WG 设备，并且使用不受限制。自固件版本 V6.3 起，可以通过 MRP 互连将指定设备与 SCALANCE XM-400 和 SCALANCE XR-500 设备耦连在一起。

SCALANCE XF-200G 的固件版本为 V4.4

自固件版本 V4.4 起，MRP 互连已发布用于 SCALANCE XF-200G 设备，并且使用不受限制。

SCALANCE XC-300 和 SCALANCE XR-300 的固件版本为 V1.0

自固件版本 V1.0 起，MRP 互连已发布用于 SCALANCE XC-300 和 SCALANCE XR-300 设备，并且使用不受限制。

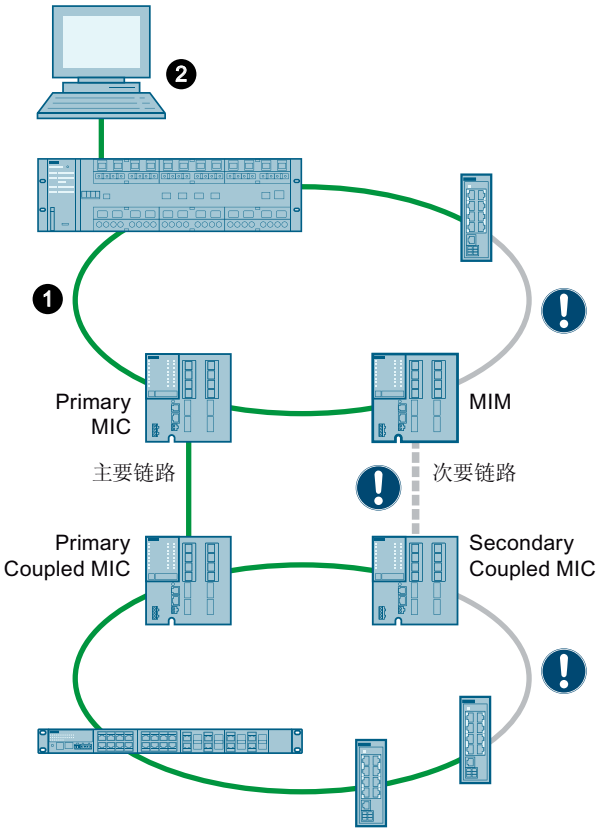
5.3.5.3 组态 MRP 互连连接

以下部分详细介绍 MRP 互连连接组态期间的步骤。按此处列出的顺序执行组态步骤以避免生成网络回路。在组态期间，并非所有设备都可始终通过组态 PC 访问。指定的组态顺序确保至少可以访问尚未组态的设备。图中的位置编号是指步骤序列的相应编号。

说明包括三个部分：

- 连接设备和基本组态（步骤 1 至步骤 3）
- 环网冗余组态（步骤 4 至步骤 7）
- MRP 互连组态（步骤 8 至步骤 16）

5.3.5.4 连接设备和基本组态



步骤 1：插入电缆

除了每个环网中的一个连接距离之外，根据计划的拓扑连接设备。用于次要链路的两个设备（MIM 和次要耦合 MIC）尚不能连接。

步骤 2：分配 IP 地址

使用连接到网络的 PC 访问设备。通过 SINEC PNI 等将一个 IP 地址分配给每台设备。然后使用 WBM 或 CLI 组态设备。

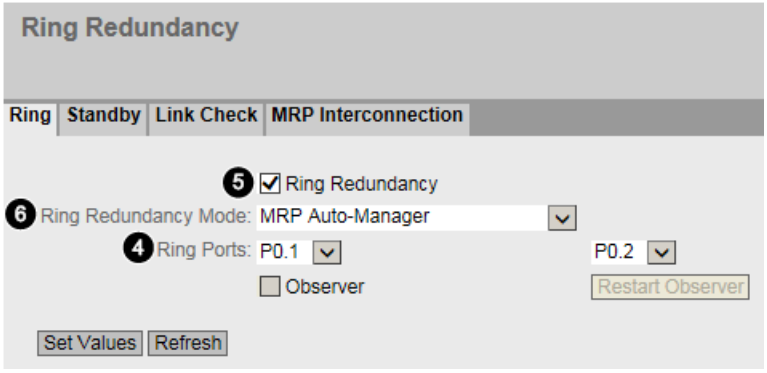
步骤 3：组态生成树

如果用户网络拓扑需要生成树，则为每个设备执行以下两个步骤。如果不需要，则为每个设备禁用生成树。

- 指定协议兼容性“RSTP”。
  （WBM 菜单命令“第 2 层 > 生成树”(Layer 2 > Spanning Tree)，“常规”(General) 选项卡，“协议兼容性”(Protocol Compatibility) 下拉列表）
- 为环网端口和 MRP 互连端口禁用生成树。
  （WBM 菜单命令“第 2 层 > 生成树”(Layer 2 > Spanning Tree)，“CIST 端口”(CIST Port) 选项卡，“生成树状态”(Spanning Tree Status) 表格列）

5.3.5.5 环网冗余组态

在 WBM 中，可以使用菜单“第 2 层 > 环网冗余”(Layer 2 > Ring Redundancy) 来组态环网冗余。在“环网”(Ring) 选项卡中，为每个设备执行步骤 4 至 6。



步骤 4：指定环网端口

从两个下拉列表中选择环网端口的匹配条目。

说明

如果所选端口具有不同的硬件特性，则显示消息“环网端口的端口组态不同”(Port Configuration of the Ring Ports is different)。消息的原因可能有：

- 传输速度不同（千兆位以太网端口/快速以太网端口）
- 传输模式不同（全双工/半双工）
- 传输介质不同（铜线电缆/光纤电缆）

在这种情况下，应检查组态是否实际上预期采用此形式。一般来说，即使可进行数据传输，不同的端口特性通常也会限制环网端口的功能。

有关端口特性的详细信息，请转至“系统 > 端口”(System > Ports)。

步骤 5：启用 MRP

选择“环网冗余”(Ring Redundancy) 复选框以启用 MRP。

步骤 6：分配 MRP 角色

以下条目存在于 MRP 模式的“环网冗余模式”(Ring Redundancy Mode) 下拉列表中：

- MRP 自动管理器 (MRP Auto-Manager)
- MRP 客户端 (MRP Client)

为每个环网中的两个设备组态环网冗余模式“MRP 自动管理器”(MRP Auto-Manager)，以便其中一个设备发生故障时也能立即重新组态 MRP 环网。

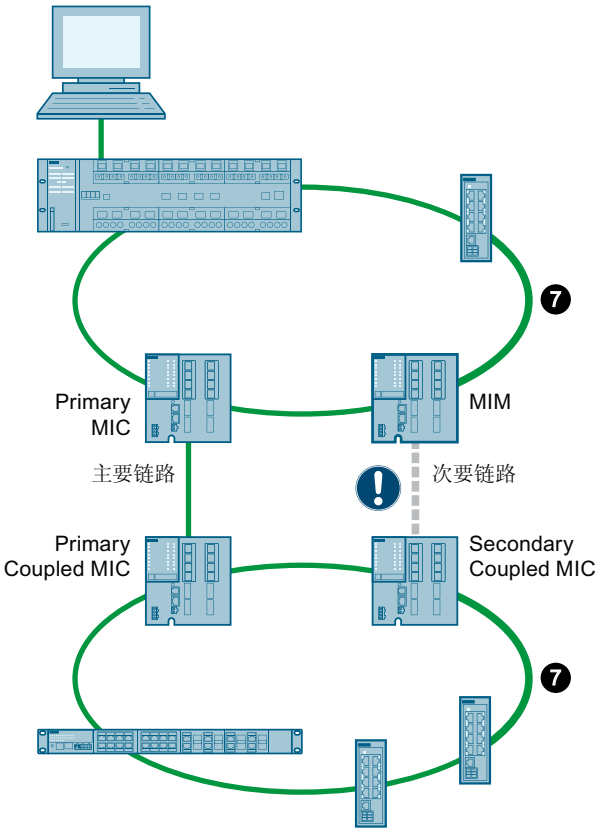
说明

如果将环网冗余模式“MRP 自动管理器”(MRP Auto-Manager) 分配给多个设备，则 MAC 地址最低的设备将成为管理器。其它设备将自动设置为“MRP 客户端”(MRP Client) 模式。

最后，单击“设置值”(Set Values) 按钮保存组态。

步骤 7：关闭环网

已在两个 MRP 环网中组态所有设备后，便可通过在尚未连接的设备之间插入电缆关闭两个 MRP 环网。请勿在 MIM 和次要耦合 MIC 之间插入电缆。



有关环网冗余的信息

可以在 WBM 中和 CLI 中找到有关环网冗余当前状态的信息：

- **WBM**
  “信息 > 冗余”(Information > Redundancy) 菜单， “环网冗余”(Ring Redundancy) 选项卡
- **CLI**
  User EXEC 模式或 Privileged EXEC 模式下的命令 `show ring-redundancy`

5.3.5.6 MRP 互连组态

使用 MRP 互连的两个环网的冗余链路中涉及四个设备。当组态这些设备时，必须遵守特定的顺序，以便可通过组态 PC 访问尚未组态的设备。需遵守以下规则：

首先对组态 PC 未连接到的 MRP 环网中的 MRP 互连连接设备进行组态。从尚未插入 MRP 互连连接电缆的设备开始；这表示从此处显示的示例中的设备“次要耦合 MIC”开始。

其组态顺序如下：

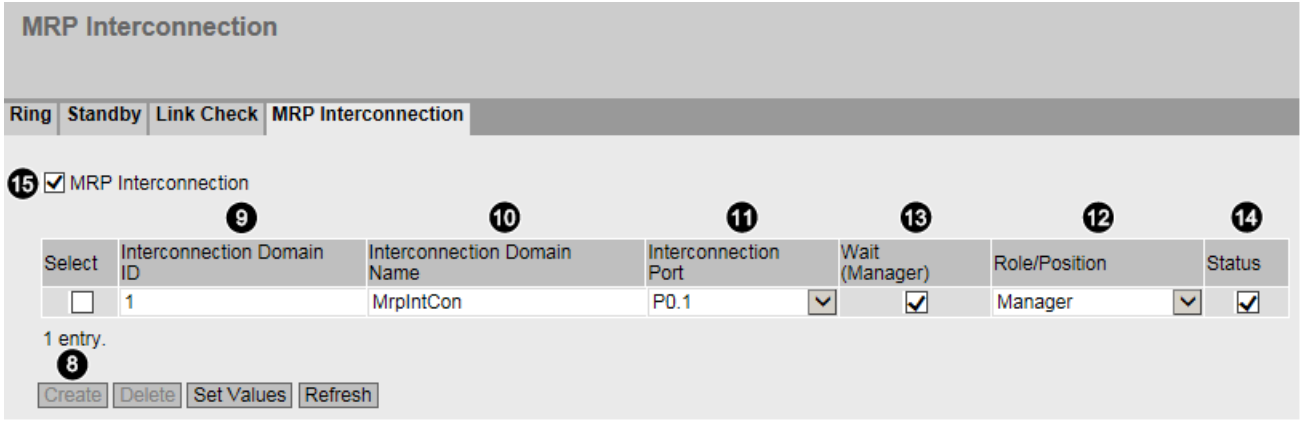
1. 次要耦合 MIC
2. 主要耦合 MIC
3. 主要 MIC
4. MIM

说明

设备的可访问性和因缺少电缆而产生的错误信息

- 在组态次要耦合 MIC 和主要耦合 MIC 之后，断开两个环网的连接，并且开始无法再访问两个列出的设备。
- 在组态主要 MIC 之后，可再次访问次要耦合 MIC 和主要耦合 MIC 以及第二个环网的所有其它设备。
- 在组态 MIM 之后，将显示一条错误消息。错误原因是尚未在 MIM 和次要耦合 MIC 之间插入电缆。组态完成后（步骤 16）插入电缆，此错误就会消失。

在 WBM 中，可以使用菜单“第 2 层 > 环网冗余”(Layer 2 > Ring Redundancy) 来组态 MRP 互连。在“MRP 互连”(MRP Interconnection) 选项卡中，为每个设备执行步骤 8 至 15。



步骤 8：为新连接创建表条目

单击“创建”(Create) 按钮在具有 MRP 互连连接的表格中创建新行。

步骤 9：分配互连域 ID

输入互连域 ID。指定 ID 时，请遵守以下规则：

- 互连域 ID 不能为 0。
- 需要为用于连接环网的所有四台设备组态相同的互连域 ID。

步骤 10：分配互连域名称

为互连连接输入任何名称。必须指定一个名称，但该名称对组态没有影响。名称中的有效字符包括字母“A”到“Z”和“a”到“z”、数字“0”到“9”以及“-”符号。名称的第一个字符或最后一个字符不得使用连字符。名称中不得包含任何空格。互连域名必须至少包含一个字符且不超过 240 个字符。

步骤 11：指定互连端口

从该下拉列表中，选择用于 MRP 互连连接的端口。请注意以下限制：

- 该端口不能被禁用或阻止。该端口的“单播阻止”(Unicast Blocking) 功能不能被启用。
- 该端口不能用于链路汇聚。
- 该端口不能为“镜像”(Mirroring) 功能的监视端口。
- 该端口不能为生成树端口。
- 该端口不能为环网端口。
- 该端口不能为 802.1X 验证器端口。
- 该端口不能为 802.1X 请求端口。
- 除了设备 SCALANCE XM-400 和 SCALANCE XR-500 外：该端口不能为路由器端口。

步骤 12：选择设备的角色和位置

必须为 MRP 互连连接中涉及的每个设备分配一个角色。可分配的两个角色是“管理器”(Manager) 和“客户端”(Client)。对于客户端，还可以指定位置（“主要”(Primary) 或“次要”(Secondary)）。在表格列“角色/位置”(Role/Position) 的下拉列表中进行选择。在此处显示的示例中，向设备分配了以下角色：

设备	角色
次要耦合 MIC	次客户端
主要耦合 MIC	主客户端

设备	角色
主要 MIC	主客户端
MIM	管理器

步骤 13：为管理器启用“等待”(Wait) 选项

对于具有“客户端”(Client) 角色的设备，清除此列中的复选框。对于具有“管理器”(Manager) 角色的设备，选中“等待（管理器）”(Wait (Manager)) 复选框，以便在 MRP 互连的主客户端运行准备就绪后开始数据传输。

步骤 14：启用 MRP 互连连接

选中“状态”(Status) 复选框以启用 MRP 互连连接。请遵守以下规则：

- 如果没有至少一个启用的 MRP 互连连接，则无法为该设备启用 MRP 互连。
- 以下最大值适用于启用的 MRP 互连数量：
  - **两个连接**
    自固件版本 V6.3 起的 SCALANCE XM-400 和 SCALANCE XR-500
    自固件版本 V4.3 起的 SCALANCE XC-200、SCALANCE XP-200、SCALANCE XF-200BA
    自固件版本 V4.4 起的 SCALANCE XF-200G
    自固件版本 V1.0 起的 SCALANCE XC-300 和 SCALANCE XR-300
  - **一个连接**
    自固件版本 V4.3 起的 SCALANCE XB-200 和 SCALANCE XR-300WG

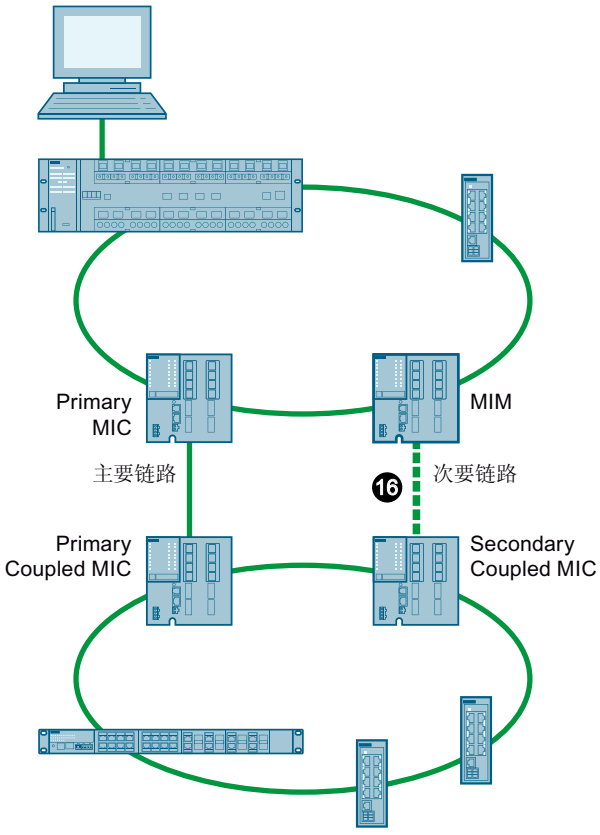
单击“设置值”(Set Values) 按钮。

步骤 15：为设备启用 MRP 互连

选中“MRP 互连”(MRP Interconnection) 复选框可启用 MRP 互连。最后，单击“设置值”(Set Values) 按钮保存组态。

步骤 16：插入次要链路的电缆

已在两个 MRP 互连环网中组态所有设备后，在 MIM 和次要耦合 MIC 设备之间插入次要链路的电缆。故障 LED 随后不再亮起。之后，MRP 互连连接即可使用。



有关 MRP 互连的信息

可以在 WBM 中和 CLI 中获得有关 MRP 互连的最新信息：

- **WBM**
  “信息 > 冗余”(Information > Redundancy) 菜单，“MRP 互连”(MRP Interconnection) 选项卡
- **CLI**
  User EXEC 模式或 Privileged EXEC 模式下的命令 `show ring-redundancy`

5.3.6 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

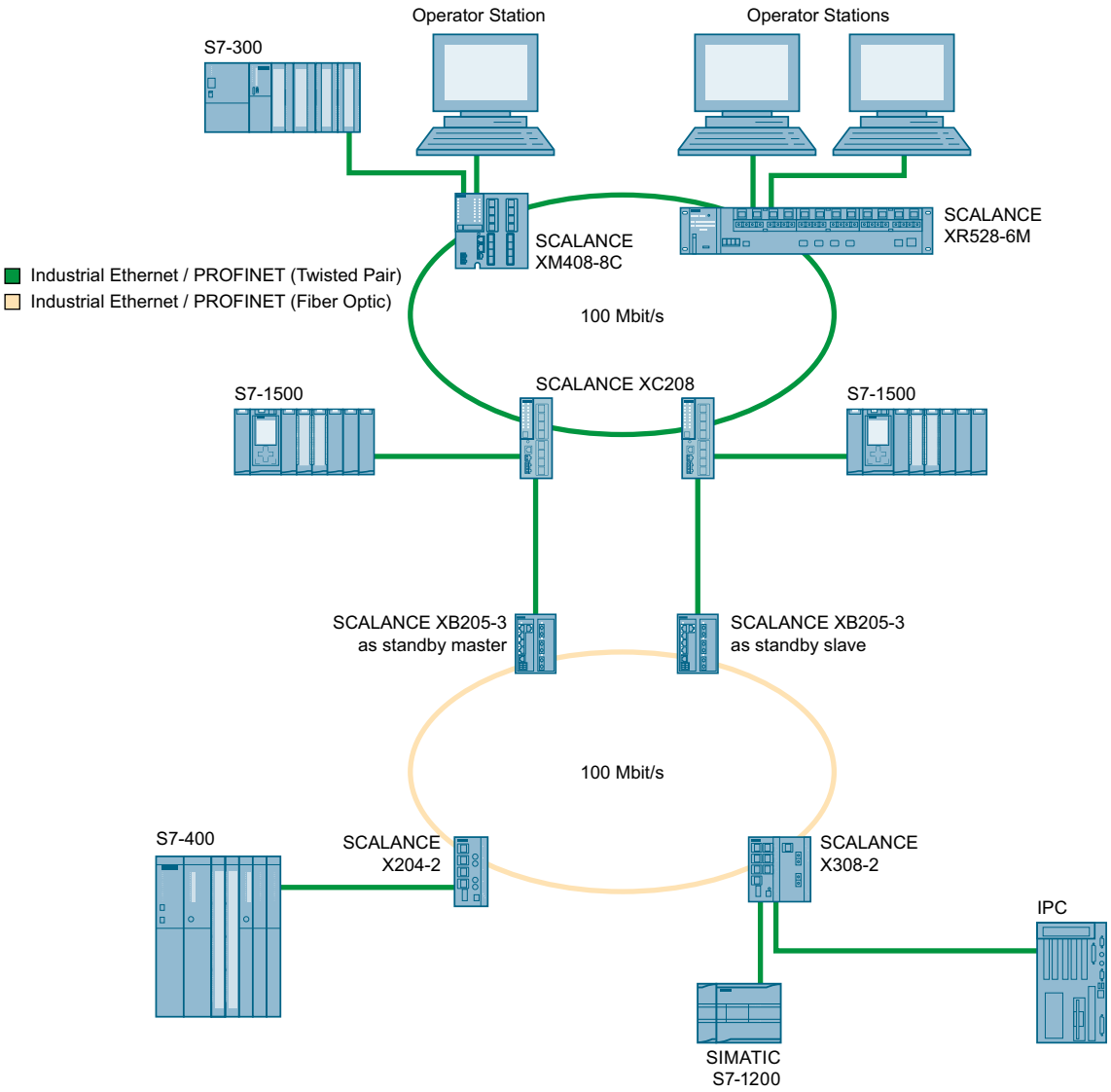


图 5-4　环网间的冗余链路示例

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。

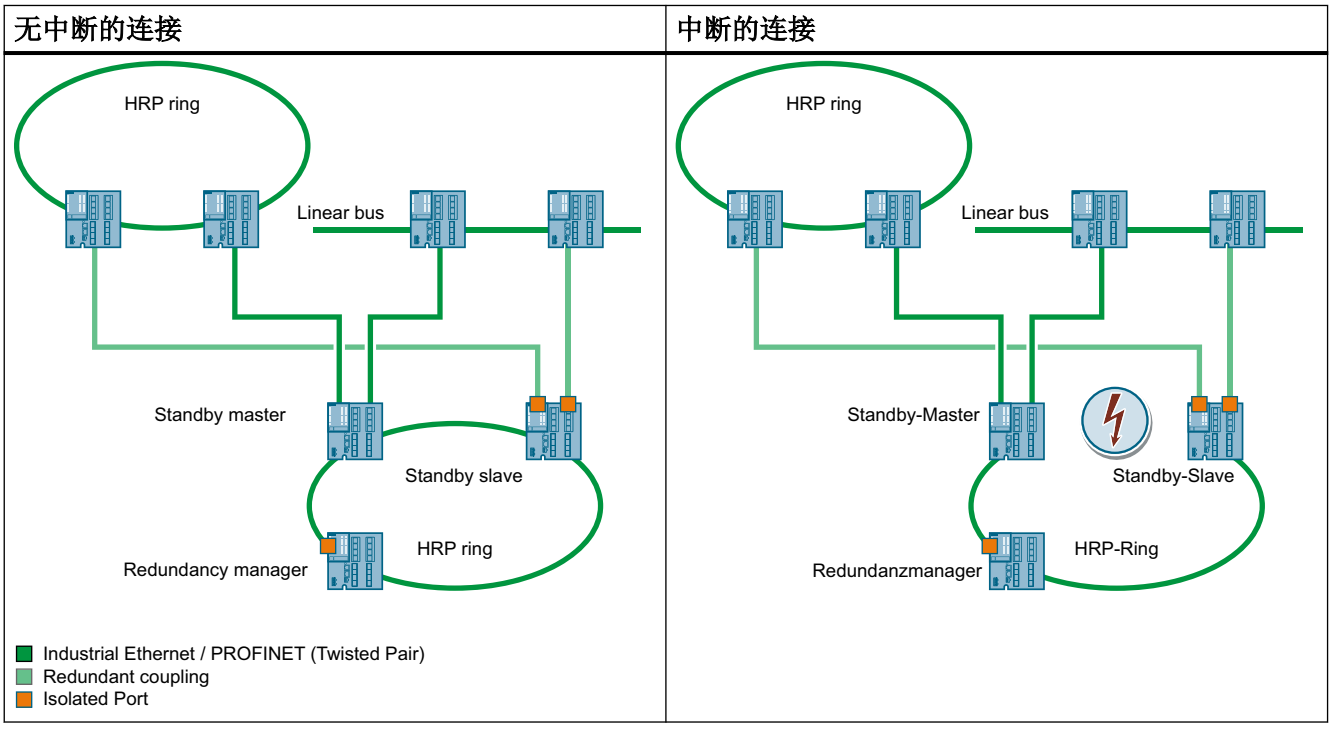
在组态中连接的两个备用冗余交换机彼此交换数据帧，以同步其工作状态（一个设备为主站，另一个为从站）。如果没发生问题，仅激活从主设备到另一网段的连接。如果此连接失败（例如，由于连接断开或设备故障），只要问题仍然存在，从设备就会激活其连接。

多个 HRP 网段的耦合

如果使用备用冗余连接多个 HRP 环网或链路，则备用主站和备用从站必须位于封闭的网段中。在任何情况下，此网段都不能开放（即直线）。

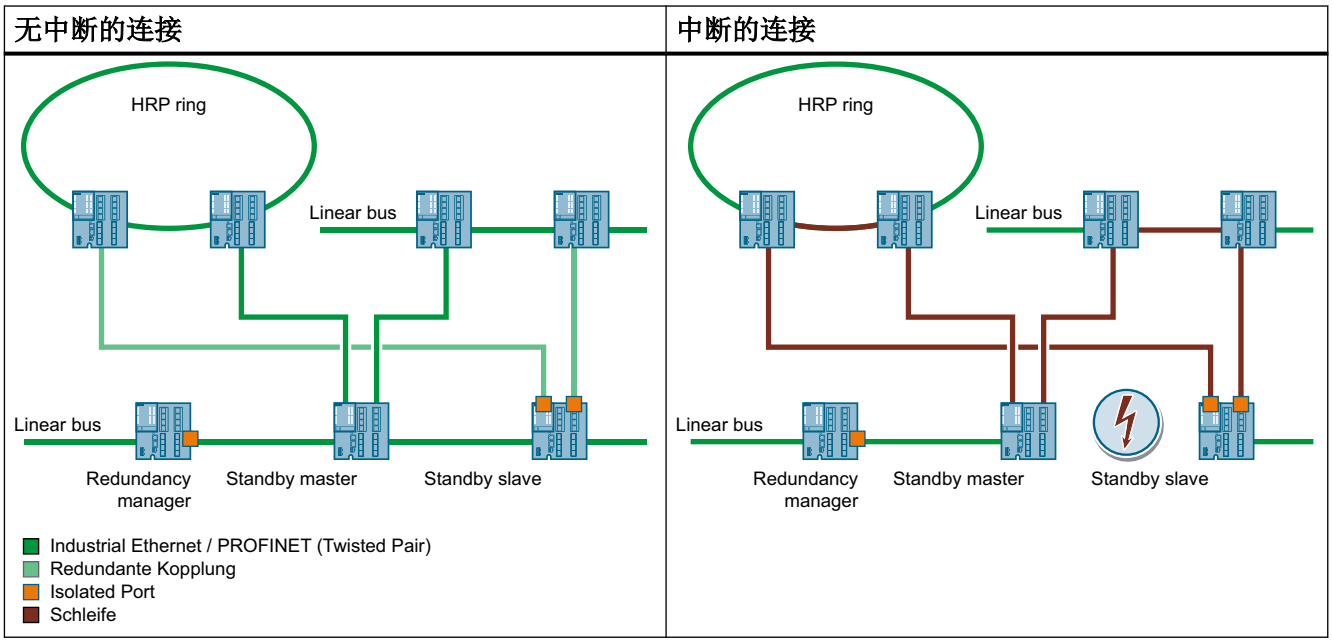
封闭网段中的备用主站和从站

即使备用主站和从站之间的连接被中断，这两个设备也能够通过 HRP 冗余管理器的冗余链路进行通信。



开放网段中的备用主站和从站

如果备用主站和从站之间的连接被中断，则这两个设备无法再进行通信。这将产生一个回路（基于耦合网段）。



5.3.7 Link Check

监视环网中的光纤连接

光纤连接中可能会出现故障，其中光纤连接并未完全中断，但偶尔会丢失帧。导致此类问题的原因可能是光纤电缆损坏、连接器污染或设备故障。

采用光纤连接的 HRP 或 MRP 环网的冗余管理器检测到一个具有此类故障的“无法恢复的环网错误”。冗余管理器无法通过关闭环网来消除故障。在此情况下，关闭环网可导致循环消息帧。

通过链路检查功能，可监视 HRP 或 MRP 环网内光纤部分的传输质量，确认故障连接以及在某些情况下将其关闭。故障部分关闭后，冗余管理器可以关闭环网并恢复通信。

链路检查的工作方式

无故障连接的行为

如果在两个连接的环网端口上启用链路检查，则这两个连接伙伴会在这些端口上周期性地交换链路检查帧。一个连接伙伴接收到的帧会被送回至另一个连接伙伴。

当设备从连接伙伴收回其发送的帧时，会为链路检查准备好连接。随后，连接伙伴会增加链路检查测试帧的发送频率，且实际连接监视处于激活状态。

故障的行为

启用连接监视后，可在“信息 > 冗余 > 链路检查”(Information > Redundancy > Link Check)页面上查看已发送和接收到的链路检查帧数。根据这些统计数据，可以识别更小的扰动，通常这些扰动尚不至于通过链路检查关断传输线路。

若在给定时段内丢失过多测试帧，链路检查功能将相关连接视为受扰动并将其断开。链路检查功能使用多个时间间隔以识别错误突然发生和连续低错误率的情况。

由链路检查关闭的端口必须复位后才能再次通信。为此，有两种选择：

- 拔出连接电缆并再次插入。
- 使用“复位”(Reset) 按钮复位两个连接伙伴上的功能。必须在 30 s 内在两个设备上完成这一操作。

说明

使用“复位”(Reset) 按钮时，会暂时形成回路，导致数据流量丢失。将再次自动清除回路。如果您的应用程序不接受，可通过拔出线缆并再次插入来复位链路检查。

复位链路检查后，会重新启动端口功能并复位统计数据。

通过 PROFINET IO 控制器组态

如果通过 PROFINET IO 控制器对 MRP 进行了组态，则可以通过 WBM 或 CLI 为第一个 MRP 环网实例的可选环网端口启用链路检查功能。

传送新的组态后，会在所有端口上自动禁用链路检查，这些端口未被组态为第一个 MRP 环网实例的环网端口。

说明

PROFINET IO 仅会间接报告与链路检查功能有关的事件。如果通过链路检查启用 MRP 诊断中断、禁用环网端口，PROFINET IO 会生成连接已不存在的错误消息。

5.3.8 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。

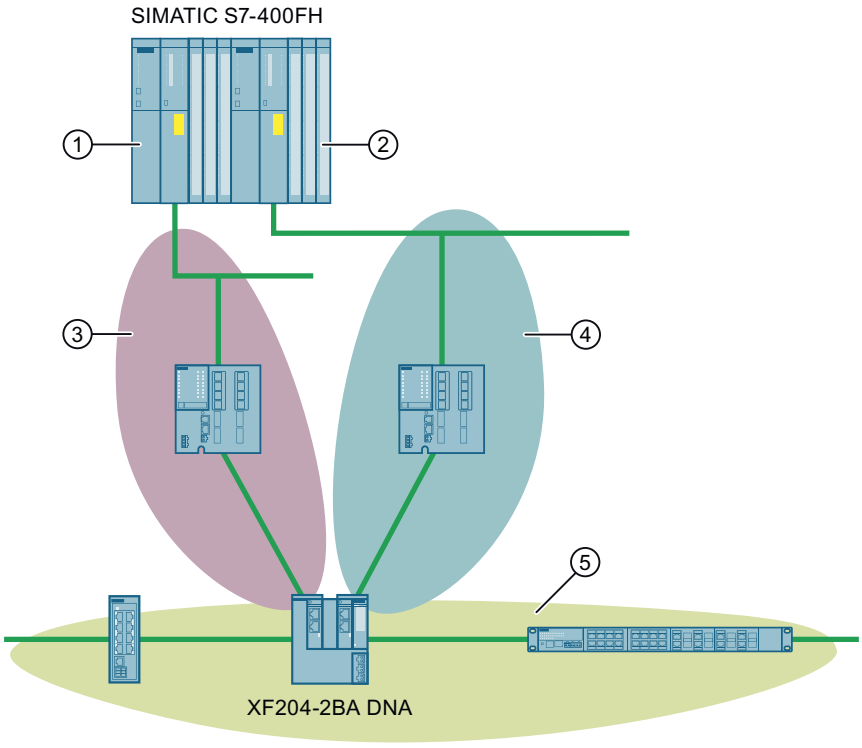
本手册中介绍的设备可在 PRP 网络中使用，另请参见 “组态限制 (页 24)”部分。

5.3.9 双网接入 (DNA)

工作原理和拓扑结构

双网接入 (DNA) 是一种将一个网络与两个网络相连（两者彼此解耦）的技术。实现此功能的交换机也称为“Y 型交换机”。是指交换机与另外两个网络的连接。Y 型交换机用于连接到两个解耦网络的端口是 DNA 端口。

一种常见用例是将冗余控制器连接到 MRP 环网。但是也可以实现线型拓扑的连接（如下图中所示）：



① 冗余控制系统的第一个控制器

② 冗余控制系统的第二个控制器

③ 第一个控制器的网络

④ 第二个控制器的网络

⑤ 共享网络（在此示例中：线型拓扑），这两个控制器都能访问此网络。

Y 型交换机的第一个 DNA 端口连接到网络 ③，第二个 DNA 端口连接到网络 ④。Y 型交换机确保了两个网络 ③ 和 ④ 彼此解耦。网络 ④ 中的设备无法访问网络 ③ 中的设备，反之亦然。

Y 型交换机中另外两个非 DNA 端口将两个端口 ③ 和 ④ 与网络 ⑤ 连接到一起。网络 ⑤ 中的设备可以通过网络 ③ 和网络 ④ 来访问。在网络 ⑤ 中，设备作为 S2 设备使用该功能，并且作为 S2 设备与两个控制器建立连接。

说明

可使用以下设备作为 Y 型交换机：

- SCALANCE XF204-2BA DNA

5.3.10 Dual Network Access-Redundanz (DNA-Redundanz)

工作原理和拓扑结构

DNA冗余表示使用冗余双网接入将一个网络与两个彼此解耦的网络相连接。为此，使用两个Y型交换机：一个 DNA 管理器和一个 DNA 客户端。DNA 冗余仅适用于 MRP 环网。一个 Y 型交换机承担 MRP 管理器和 DNA 管理器的角色，另一个 Y 型交换机承担 MRP 客户端和 DNA 客户端的角色。当至少一个 Y 型交换机运行时，将连接到两个解耦网络。

在常规操作中，DNA 客户端的 DNA 端口将被拦截，并且 DNA 管理器的 DNA 端口处于“Forwarding”状态。如果DNA不再从管理器接收MRP帧（例如，由于管理器关闭），则DNA客户端会将其两个 DNA 端口切换到“Forwarding”状态。

说明

可使用以下设备作为 DNA 管理器或 DNA 客户端：

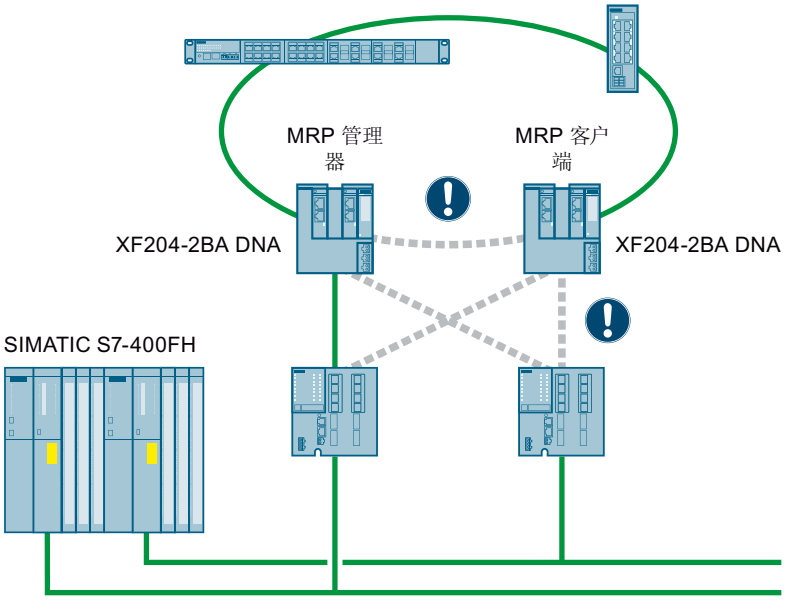
- SCALANCE XF204-2BA DNA

组态 DNA 冗余

以下部分详细介绍了组态 DNA 冗余的步骤。按此处列出的顺序执行组态步骤，避免形成网络回路。

步骤 1：连接设备

连接 MRP 环网的所有设备（MRP 管理器与 MRP 客户端之间的连接除外）。仅将 MRP 管理器的一个 NDA 端口与其中一个控制器相连或与控制器所连的交换机相连。

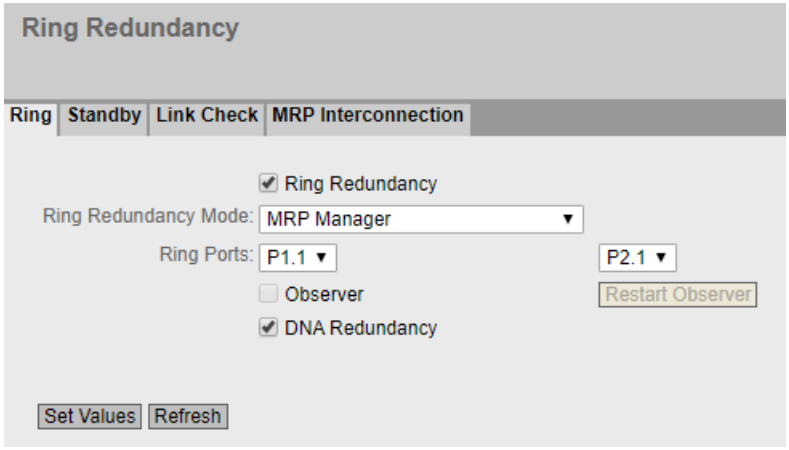


步骤 2：检查和调整

如果设备不会使用 PROFINET 功能，则在设置 DNA 冗余时可以不使用 STEP 7 Classic。直接使用 WBM 或 CLI 来访问设备，从而配置 MRP 和 DNA 冗余。两个设备均可通过 MRP 环网进行访问。由于 MRP 环网仍处于断开状态，因此不会产生循环帧，即使没有有效的 MRP 组态时也是如此。

第 2 步在基于 Web 的管理中不使用 PROFINET 功能

1. 打开将承担 DNA 管理器角色的 Y 型交换机的 WBM。
2. 打开 WBM 页面“第 2 层 > 环网冗余 > 环网”(Layer 2 > Ring Redundancy > Ring)：



3. 选择“环网冗余”(Ring Redundancy) 复选框。
4. 在“环网冗余模式”(Ring Redundancy Mode) 下拉列表中选择“MRP 管理器”(MRP Manager) 条目。
5. 在两个“环网端口”(Ring Ports) 下拉列表中选择 MRP 管理器的环网端口。
6. 选中“DNA 冗余”(DNA Redundancy) 复选框。不属于环网端口的两个端口是 DNA 端口。
7. 单击“设置值”(Set Values) 按钮。
8. 打开将承担 DNA 客户端角色的 Y 型交换机的 WBM。
9. 打开 WBM 页面“第 2 层 > 环网冗余 > 环网”(Layer 2 > Ring Redundancy > Ring)。
10. 选择“环网冗余”(Ring Redundancy) 复选框。
11. 在“环网冗余模式”(Ring Redundancy Mode) 下拉列表中选择“MRP 客户端”(MRP Client) 条目。
12. 在两个“环网端口”(Ring Ports) 下拉列表中选择 MRP 客户端的环网端口。
13. 选中“DNA 冗余”(DNA Redundancy) 复选框。不属于环网端口的两个端口是 DNA 端口。
14. 单击“设置值”(Set Values) 按钮。
15. 将环网中的其余设备组态为 MRP 客户端。

第 2 步中不使用 PROFINET 功能，但使用命令行界面

1. 在 Windows 控制台中，打开将承担 DNA 管理器角色的 Y 型交换机的 CLI。
2. 在全局组态模式下执行以下命令：
   `ring-redundancy mode mrpmanager`

3. 使用以下命令在冗余组态模式下配置环网端口：
   `ring ports <interface-type> <interface-id> <interface-type> <interface-id>`
   这些参数是两个环网端口的接口类型和接口名称。
   示例：
   要在上一个屏幕截图中组态相同的环网端口，需要使用以下命令：
   `ring ports fa 1/1 fa 2/1`
   不属于环网端口的两个端口是 DNA 端口。在这个示例中，它们是端口 1/2 和 2/2。
4. 使用以下命令在全局组态模式下启用 DNA 冗余：
   `ring-redundancy dna-redundancy`
5. 在 Windows 控制台中，打开将承担 DNA 客户端角色的 Y 型交换机的 CLI。
6. 在全局组态模式下执行以下命令：
   `ring-redundancy mode mrpclient`
7. 使用以下命令在冗余组态模式下配置环网端口：
   `ring ports <interface-type> <interface-id> <interface-type> <interface-id>`
   这些参数是两个环网端口的接口类型和接口名称。不属于环网端口的两个端口是 DNA 端口。
8. 使用以下命令在全局组态模式下启用 DNA 冗余：
   `ring-redundancy dna-redundancy`
9. 将环网中的其余设备组态为 MRP 客户端。

说明

使用以下命令在全局组态模式下禁用 DNA 冗余：

`no ring-redundancy dna-redundancy`

第 2 步，包含 PROFINET 功能

如果设备将使用 PROFINET 功能，则需要在 STEP 7 Classic 中组态 DNA 冗余。请按照下面列出的步骤进行操作：

说明

将 GSDML 文件下载到 STEP 7 Classic 中

自固件版本 V4.2 开始提供 DNA 冗余。要在 STEP 7 Classic 中组态不含 PROFINET 功能的 DNA 冗余，可能需要首先将 Y 型交换机的 GSDML 文件下载到 STEP 7 Classic 中。可在以下 WBM 菜单中找到设备的 GSDML 文件：“系统 > 系统 > 加载和保存 > GSDML>”(System > Load&Save > GSDML)。

1. 打开 HW Config 程序。
2. 选择将承担 DNA 管理器角色的 Y 型交换机，然后打开“PNIO 属性”(PNIO Properties) 对话框。

3. 单击“介质冗余”(Media redundancy) 选项卡并组态以下参数：
   – 角色 (Role)
     选择“管理器”(Manager) 设置。
   – 环网端口 (Ring ports)
     MRP 管理器的环网端口。
   – 域 (Domain)
     Y 型交换机必须位于同一个域中。
4. 单击“参数”(Parameters) 选项卡，然后选中“DNA 冗余”(DNA Redundancy) 复选框。MRP 管理器也将是 DNA 管理器。
5. 单击“确定”(OK) 可完成 DNA 管理器的组态。
6. 选择将承担 DNA 客户端角色的 Y 型交换机，然后打开“PNIO 属性”(PNIO Properties) 对话框。
7. 单击“介质冗余”(Media redundancy) 选项卡并组态以下参数：
   – 角色 (Role)
     选择“客户端”(Client) 设置。
   – 环网端口 (Ring ports)
     MRP 客户端的环网端口。
   – 域 (Domain)
     Y 型交换机必须位于同一个域中。
8. 单击“参数”(Parameters) 选项卡，然后选中“DNA 冗余”(DNA Redundancy) 复选框。MRP 客户端也将是 DNA 客户端。
9. 单击“确定”(OK) 可完成 DNA 客户端的组态。
10. 将环网中的其余设备组态为 MRP 客户端。所有 MRP 客户端必须属于 MRP 管理器的域。
11. 将组态下载到控制器中。

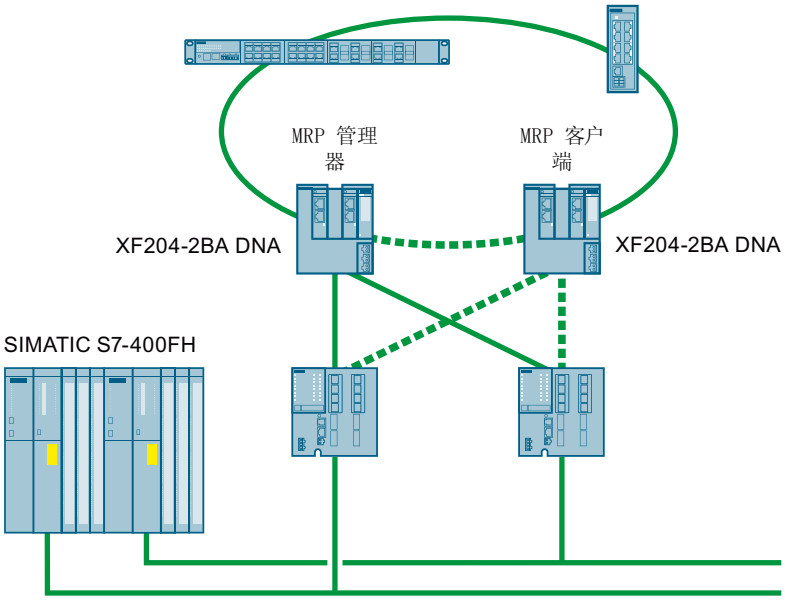
说明

在 STEP 7 Classic 中组态拓扑。

无法使用控制器的“MRP 诊断报警”功能监控 DNA 端口的状态。要监控 Y 型交换机与控制器之间的连接，需要在 STEP 7 Classic 中组态此拓扑。

步骤 3：进行连接

将 MRP 环网闭合。将剩余的 DNA 端口与控制器相连或与控制器所连的交换机相连。



5.4 VLAN

5.4.1 基础

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 88)）。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 312) 中组态基于端口的 VLAN。

5.4.2 VLAN 标记

用四个字节扩展以太网帧

对于 CoS（Class of Service，服务等级，即帧优先级）和 VLAN（虚拟网络），IEEE 802.1Q 标准规定可通过添加 VLAN 标记来扩展以太网帧。

说明

VLAN 标记将帧允许的总长度从 1518 字节增加到 1522 字节。
必须对网络上的终端节点进行检查，以确定它们是否能处理此长度/帧类型。如果不能处理，则仅可向这些节点发送标准长度的帧。

附加的 4 个字节在以太网帧头中，位于源地址和以太网类型/长度字段之间：

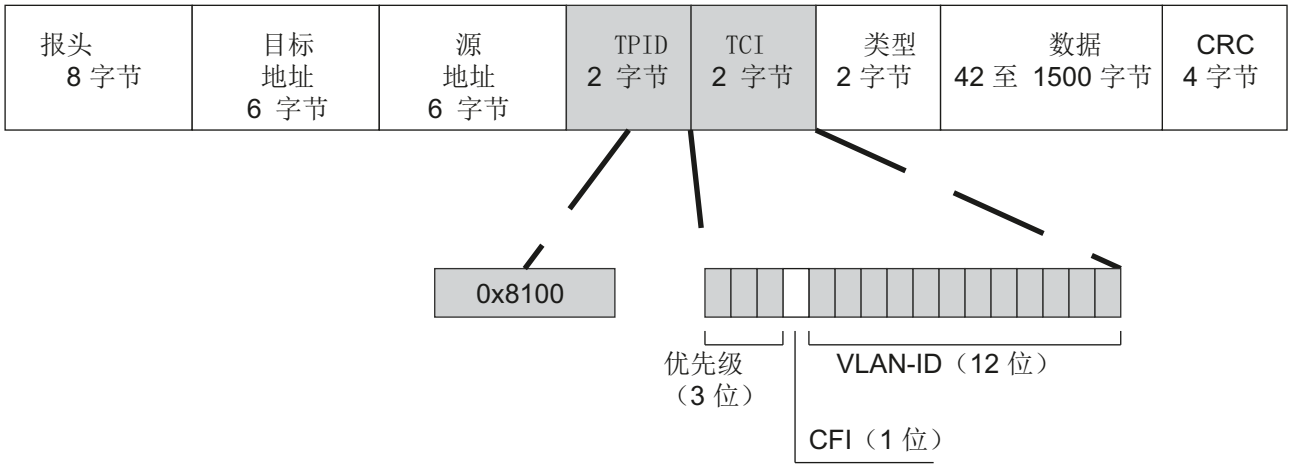


图 5-5 扩展的以太网帧结构

附加字节中包含标记协议标识符 (TPID) 和标记控制信息 (TCI)。

标记协议标识符 (TPID)

前两个字节构成标记协议标识符 (TPID)，且始终包含值 0x8100。此值指定该数据包包含 VLAN 信息或优先级信息。

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。

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

5.4.3 私有 VLAN

借助私有 VLAN (PVLAN)，可将一个 VLAN 二层广播域划分为多个子区域。

私有 VLAN 由以下单元组成：

- 主私有 VLAN（主 PVLAN）
  主私有 VLAN 是指被划分的 VLAN。
- 次私有 VLAN（次 PVLAN）
  次 PVLAN 只存在于主 PVLAN 内。每个次 PVLAN 都有一个特定的 VLAN ID，并且与主 PVLAN 相连。
  次 PVLAN 分为以下两类：
  - Isolated Secondary PVLAN
    隔离次 PVLAN 内的各设备之间不能通过第 2 层进行通信。
  - Community Secondary PVLAN
    公共次 PVLAN 内的各设备之间可直接通过第 2 层进行通信。隶属不同 PVLAN 团体的设备之间不能通过第 2 层进行通信。

说明

次 PVLAN 的 VLAN ID

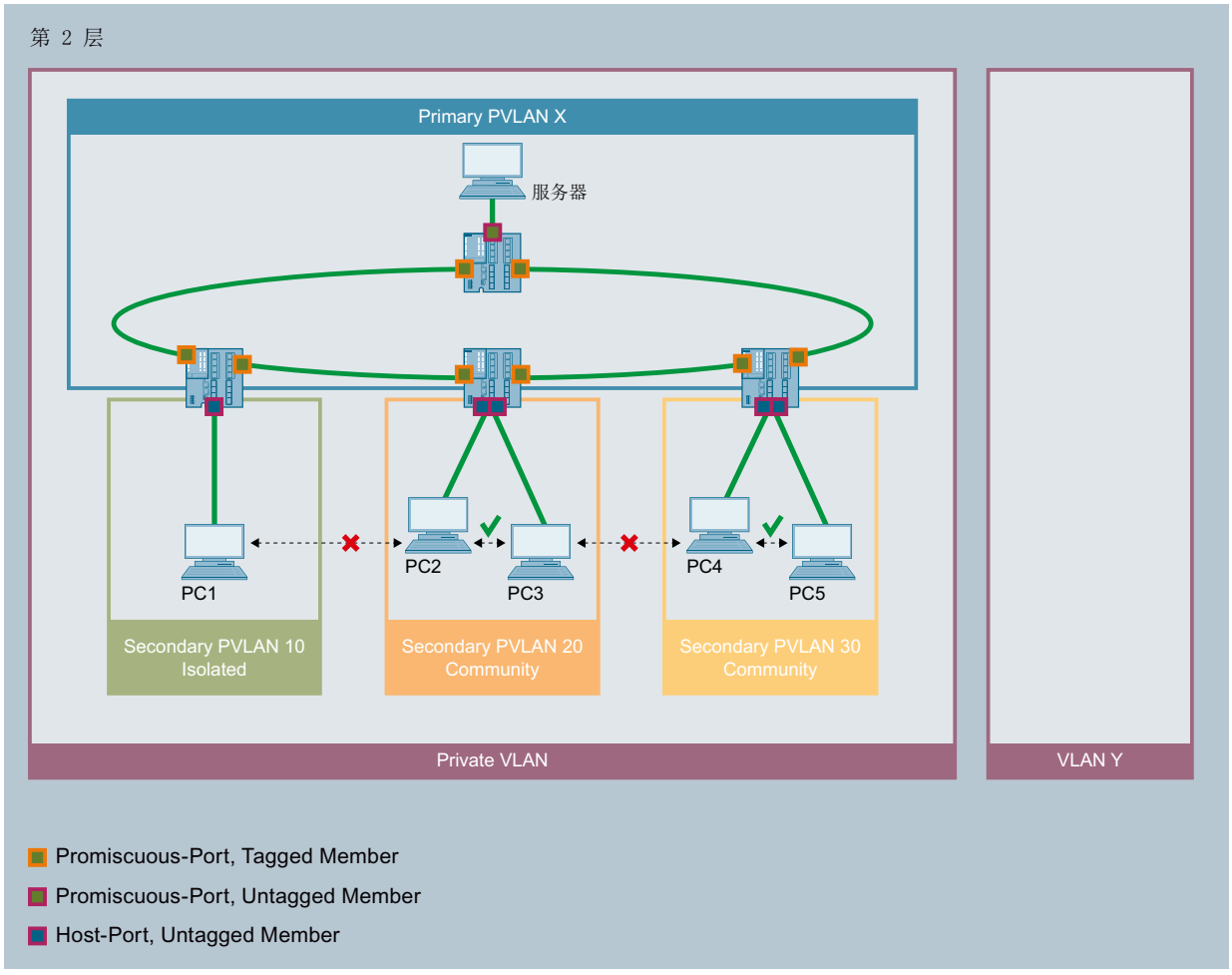
如果不同工业以太网交换机上的次 PVLAN 采用相同的 VLAN ID，则这些次 PVLAN 中的终端设备可以在不同交换机上通过第 2 层与其它设备进行通信。前提条件是将连接不同 IE 交换机的端口组态为混合端口。如果将这些端口组态为中继端口，并为隔离的各个次级 PVLAN 使用相同 VLAN ID，则终端设备仍然处于隔离状态。

说明

私有 VLAN 功能和 RADIUS 验证

当通过 RADIUS 验证为 VLAN 的一个或多个端口启用 VLAN 分配时，不应将此 VLAN 另外组态为私有 VLAN。

与通过 RADIUS 验证进行 VLAN 分配相关的私有 VLAN 功能可能会导致系统状态不一致。



在本示例中，各工业以太网交换机之间使用混合端口进行互连。这些网络端口在所有 PVLAN（主 PVLAN 和所有次 PVLAN）中均为带标记的成员。

用于连接 PC 的端口是主机端口。主机端口在主 PVLAN 及其次 PVLAN 中均为无标记的成员。

用于连接服务器的端口是混合端口。该混合端口在所有 PVLAN（主 PVLAN 和所有次 PVLAN）中均为带标记的成员。

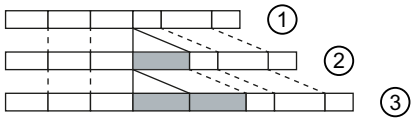
在本示例中，所有 PC 均可与服务器通信，反之亦然。PC1 不能与任何其它 PC 通信。公共次 PVLAN 内的设备之间可以相互通信，但不能与其它次 PVLAN 内的 PC 通信。

5.4.4 VLAN 通道

使用 Q-in-Q VLAN 隧道功能，可通过提供商网络转发具有 VLAN 隧道的各种客户网络的数据通信。每个客户网络均有完备的可用 VLAN。

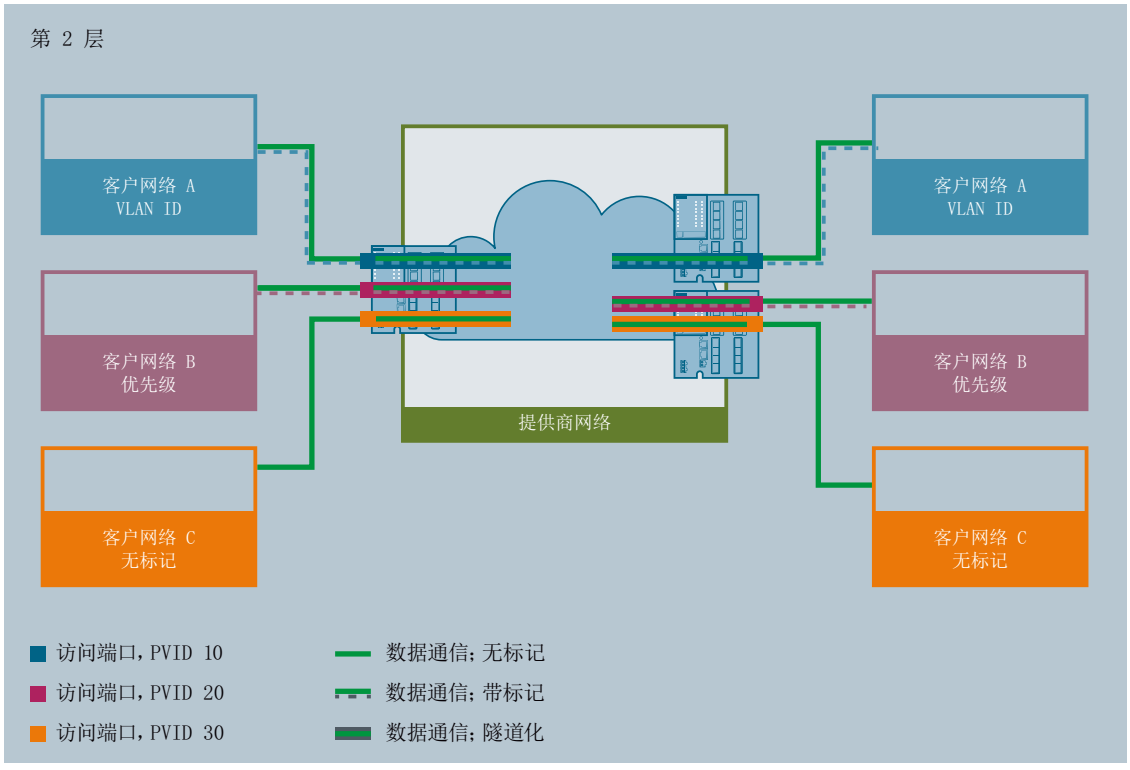
VLAN 隧道在提供商网络边界组态的交换机之间建立。一个提供商交换机具有以下端口类型：

- 访问端口
  提供商交换机通过访问端口连接到客户网络。
  - 传入数据通信
    访问端口处的传入数据通信视为无标记 ①。所有的传入帧均由具有访问端口端口 VID 的标签扩展 ②。所有帧均已标记，这意味着它们已由第二个 802.1Q 标签（外部 VLAN 标签）③ 扩展。



  - 传出数据通信
    使用访问端口的传出数据通信，将外部标签再次删除。

- 核心端口
  提供商交换机通过核心端口连接到提供商网络。
  核心端口为访问端口的端口 VLAN 的成员，或者使用端口类型“Switch-Port VLAN Trunk”组态。



在本示例中，来自客户网络 A、B 和 C 的数据通信使用 VLAN 通道通过提供商网络转发。来自客户网络 A 的帧带有 VLAN ID 标记。来自客户网络 B 的帧带有优先级标记。来自客户网络 C 的帧没有标记。

帧在到达相关访问端口时，即由具有访问端口端口 VID 的标签扩展，并通过提供商网络隧道化。帧离开提供商网络时，将立即再次删除外部 VLAN 标签 (PVID)。帧以其原始格式转发。保留帧的优先级。

5.5 镜像

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。

说明

转发 RSPAN 流

如果设备要转发 RSPAN 流，必须满足两个要求：

- 输入端口和输出端口必须属于同一个端口组。
- 对于输入端口，必须禁用“学习”功能。
  在 WBM 中：“系统 > 端口 > 组态 > 单播 MAC 学习”(System > Ports > Configuration > Unicast MAC Learning)
  在 CLI 中：no unicast mac learning

5.6 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。
- INFORM
  像一个陷阱，只是它会被接收方确认。

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

5.7 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 295)”页上设置的优先级。
   交换机将根据“CoS 映射 (CoS Map) (页 297)”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 295)”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 297)”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 300)”页面上组态。

参见

常规 (页 305)

5.8 NAT/NAPT

说明

NAT/NAPT 仅在 ISO/OSI 参考模型的第 3 层可用。要使用 NAT 功能，网络必须使用 IP 协议。使用运行在第 2 层的 ISO 协议时，不能使用 NAT。

在网络地址转换 (NAT) 中，IP 子网分为“Inside”和“Outside”。此划分是从 NAT 接口角度来看的。可通过自身的 NAT 接口进行访问的所有网络均被视为该接口的“Outside”。可通过同一设备的其它 IP 接口进行访问的所有网络均被视为 NAT 接口的“Inside”。

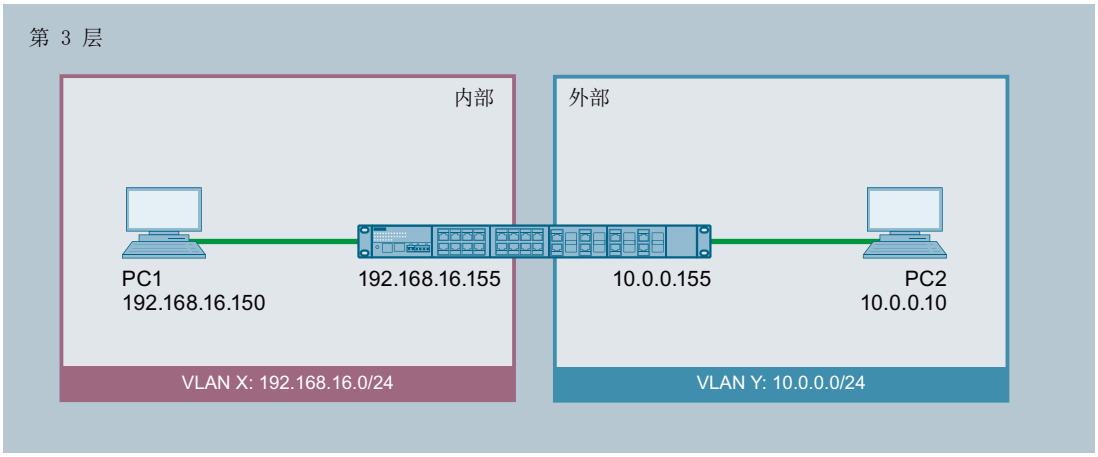
如果存在通过 NAT 接口进行的路由过程，则在“Inside”与“Outside”之间进行切换时，所传送数据包的源或目标 IP 地址会发生改变。源或目标 IP 地址是否发生改变取决于通信方向。做

出调整的 IP 地址总是为位于“Inside”的通信节点的 IP 地址。根据角度的不同，通信节点的 IP 地址总是会被标识为“Local”或“Global”。

		角度	
		Local	**Global**
位置	**Inside**	分配给内部网络中某个设备的实际 IP 地址。外部网络无法访问该地址。	可供外部网络访问内部设备的 IP 地址。
	Outside	分配给外部网络中某个设备的实际 IP 地址。 由于仅转换了“内部”地址，因此外部局部和外部全局没有任何区别。	

示例

本示例中，两个 IP 子网通过工业以太网交换机连接。此划分是从 NAT 接口 10.0.0.155 角度来看的。通过 NAT/NAPT 执行 PC2 和 PC1 之间的通信。



PC1 的实际 IP 地址（内部局部）通过 NAT 进行静态分配。对于 PC2，可以通过内部全局地址访问 PC1。

		角度	
		Local	**Global**
位置	**Inside**	192.168.16.150	10.0.0.7
	Outside	10.0.0.10	

PC1 的实际 IP 地址（内部局部）通过 NAPT (Network Address and Port Translation) 进行分配。对于 PC2，可以通过内部全局地址访问 PC1。

		角度	
		Local	**Global**
位置	**Inside**	192.168.16.150:80	10.0.0.7:80
	Outside	10.0.0.10:1660	

计算容量

由于 CPU 存在负载限制，设备每秒钟可接收的数据包数目最多为 300 个。这意味着，最大数据吞吐量为 1.7 Mbps。该负载限制的对象并非每个接口，而是针对发往 CPU 的全部数据包。

整个 NAT 通信通过 CPU 进行，因此会与发往 CPU 的 IP 通信，例如 WBM 和 Telnet。

请注意，使用 NAT 时会占用很大一部分计算容量。这可以减缓通过 Telnet 或 WBM 的访问。

NAT

利用网络地址转换 (NAT)，可将数据包中的 IP 地址替换为另一个。NAT 通常用在内部网络和外部网络之间的网关上。

对于源 NAT，NAT 设备会将内部网络中设备的 IP 数据包的内部局部源地址重写到网关处的内部全局地址中。

对于目标 NAT，NAT 设备会将外部网络中设备的 IP 数据包的内部全局源地址重写到网关处的内部局部地址中。

NAT 设备会维护转换列表，以将内部 IP 地址转换为外部 IP 地址以及反向转换。地址既可以动态分配，也可以静态分配。NAT 在“第 3 层 (IPv4) > NAT”(Layer 3 (IPv4) > NAT) (页 404) 中组态。

NAPT

在“网络地址端口转换”(NAPT) 中，多个内部源 IP 地址被转换为同一个外部 IP 地址。为了识别各个节点，内部设备的端口也会存储在 NAT 设备的转换列表中并针对外部地址进行转换。

如果多个内部设备通过 NAT 设备向同一外部目标 IP 地址发送查询，NAT 设备会在这些转发帧的帧头中输入其自身的外部源 IP 地址。由于转发的帧具有同一个外部源 IP 地址，NAT 设备会通过不同的端口号将帧分配各个设备。

如果外部网络中的设备要使用内部网络中的服务，则需组态静态地址分配的转换列表。NAPT 在“第 3 层 (IPv4) > NAT > NAPT”(Layer 3 (IPv4) > NAT > NAPT) (页 410) 中组态。

NAT/NAPT 和 IP 路由

可以同时启用 NAT/NAPT 和 IP 路由。在这种情况下，需要使用 ACL 规则来控制外部网络对内部地址的访问。

5.9 单跳 VLAN 间路由

简介

物理网络由 VLAN 分成广播域和子网。

VLAN 中的设备（主机）可通过第 2 层直接与其它设备通信。帧转发至基于 MAC 地址的相关设备。

来自不同 VLAN 的设备无法直接通过第 2 层相互通信。数据通信必须基于 IP 地址路由。

属于不同 VLAN 的设备无需路由器即可通过单跳 VLAN 间路由功能互相通信。

要求

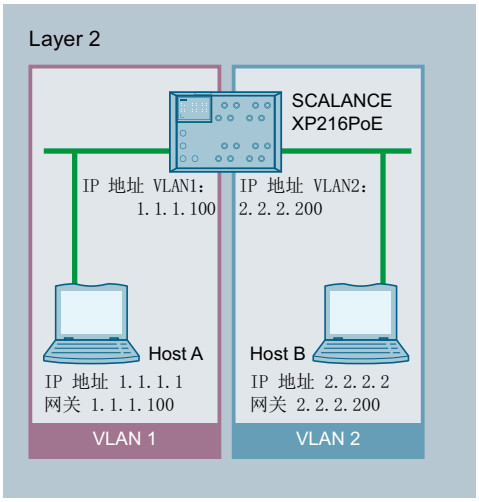
- 工业以太网交换机可以管理多个 IP 地址：
- 该交换机是待路由的 VLAN 成员。
- 在主机中，VLAN 的 IP 地址作为默认网关输入。

单跳 VLAN 间路由

工业以太网交换机接收帧并识别在另一 VLAN 的设备中寻址。它在 VLAN 中将帧转发至相关端口。

工业以太网交换机仅能识别与其直接相连的 VLAN (Connected)。通过单跳 VLAN 间路由，仅可在两本地 IP 接口间路由。

示例



在本例中，主机 A 通过 VLAN1 连接到 IE 开关。主机 A 通过 VLAN2 连接到 IE 开关。在主机 A 中，VLAN 1 的 IP 地址作为默认网关输入。在主机 B 中，VLAN 2 的 IP 地址作为默认网关输入。

如果启用 SCALANCE XP216PoE 上的单跳 VLAN 间路由功能，那么主机 A 和主机 B 能够相互通信。

使用“基于 Web 的管理”进行组态 6

6.1 基于 Web 的管理

要访问设备的基于 Web 的管理 (WBM)，可通过网络在客户端 PC 和设备之间建立远程连接。设备为 WBM 集成了 HTTPS 服务器。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。

要求

- 设备具有 IP 地址。

  说明

  使用 DHCP 或 SINEC PNI 为设备分配 IP 地址。

- 设备与客户端 PC 之间存在网络连接。
- 设备的网络设置与客户端 PC 的网络设置相匹配。

  说明

  可以使用“ping”检查是否存在连接以及是否可以进行通信。

- 通过 HTTP(S) 的访问已在设备上激活。
- 客户端 PC 上已存在 Internet 浏览器。
- 在 Internet 浏览器中激活 JavaScript。
- Internet 浏览器不得组态成每次访问页面时都从服务器重载页面。页面动态内容的更新是通过其它机制来确保的。
- 如果使用的是防火墙，请启用相应的端口。
  - 若使用 HTTPS 进行访问：TCP 端口 443
  - 若使用 HTTP 进行访问：TCP 端口 80

WBM 显示

WBM 的显示情况已使用如下桌面 Internet 浏览器测试过：

- Mozilla Firefox
- Google Chrome
- Microsoft Edge

WBM 采用固件发布之时可提供的最新版 Internet 浏览器进行测试。

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	Internet 浏览器
960 x 640 像素	Android（自版本 4.2.1 起） iOS（自版本 6.0.2 起）	基于 Android 的 Chrome（自版本 18 起） 基于 iOS 的 Safari（自版本 6 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 版本 8.1.3 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

在移动设备上显示和操作 WBM 页面的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。

6.2 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：

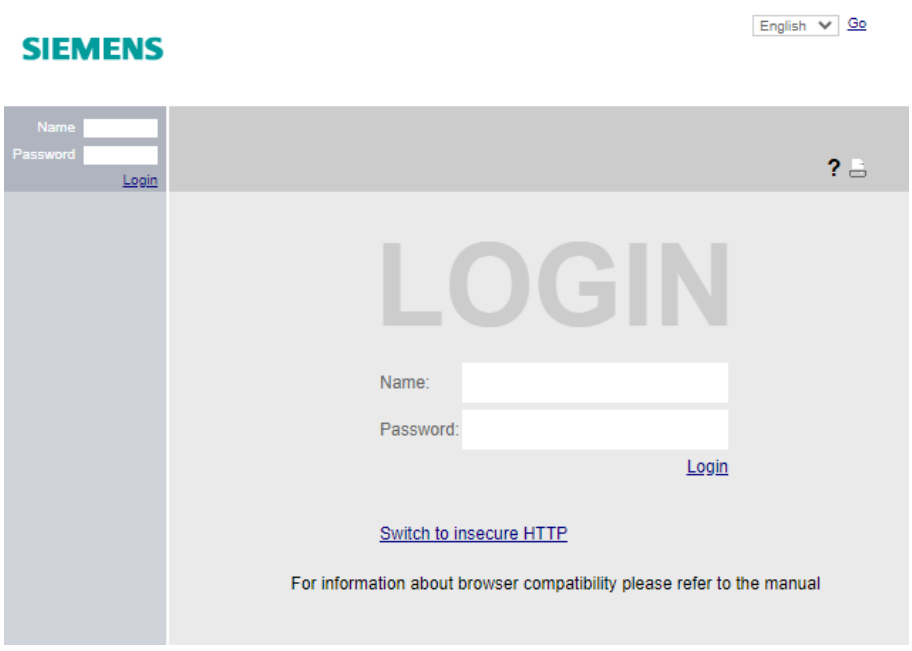
1. 设备与 Admin PC 之间存在连接。可以通过 ping 命令检查设备是否可供访问。
2. 在 Web 浏览器的地址栏中输入“https://”，后接要组态的设备的 IP 地址或其 URL，例如 https://192.168.16.178。
   默认启用通过 HTTPS 进行的访问。

   说明

   有关安全证书的信息

   因为设备只能使用加密访问进行管理，所以会与自签名证书一起交付。如果使用的证书包含操作系统无法识别的签名，则会显示一条安全消息。可以显示证书。

   将显示一条与安全证书相关的消息。确认该消息然后继续加载页面。
   如果使用非标准端口，则请在 IP 地址与端口号之间输入“:”作为分隔符。
   示例：https://192.168.16.178:49152
   在“系统 > 组态”(System > Configuration) 中更改端口。
3. 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。
   如果希望通过非安全 HTTP 连接访问 WBM，请在“系统 > 组态”(System > Configuration) 中激活 HTTP 服务器。下次登录时，单击登录页面上的链接“切换到非安全 HTTP”(Switch to insecure HTTP)，或在 Web 浏览器地址框中输入“http://”和设备的 IP 地址。



更改语言

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。

个性化登录页面

可以在登录页面上显示附加文本。

1. 创建一个包含所需文本或 ASCII 类型的 txt 文件。如果是 ASCII 类型，将根据可用字符显示象形图，例如西门子公司徽标。最多支持 50 个文本行，每行 255 个字符（包括空格）。

   说明

   不支持使用以下特殊字符：
   - 反斜线 (\)
   - 问号 (?)
   - Tab 制表符：使用空格代替制表符

2. 使用“系统 > 加载和保存”(System > Load&Save) 将文本文件加载到设备。为此，请使用表格行 LoginWelcomeMessage”中的“上传”(Upload) 按钮，无需考虑使用的协议。
3. 注销。组态的文本显示在登录页面上凭据的下方。

登录 WBM

通过 HTTPS 登录有以下几种方式。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，都可以按照以下步骤进行操作。

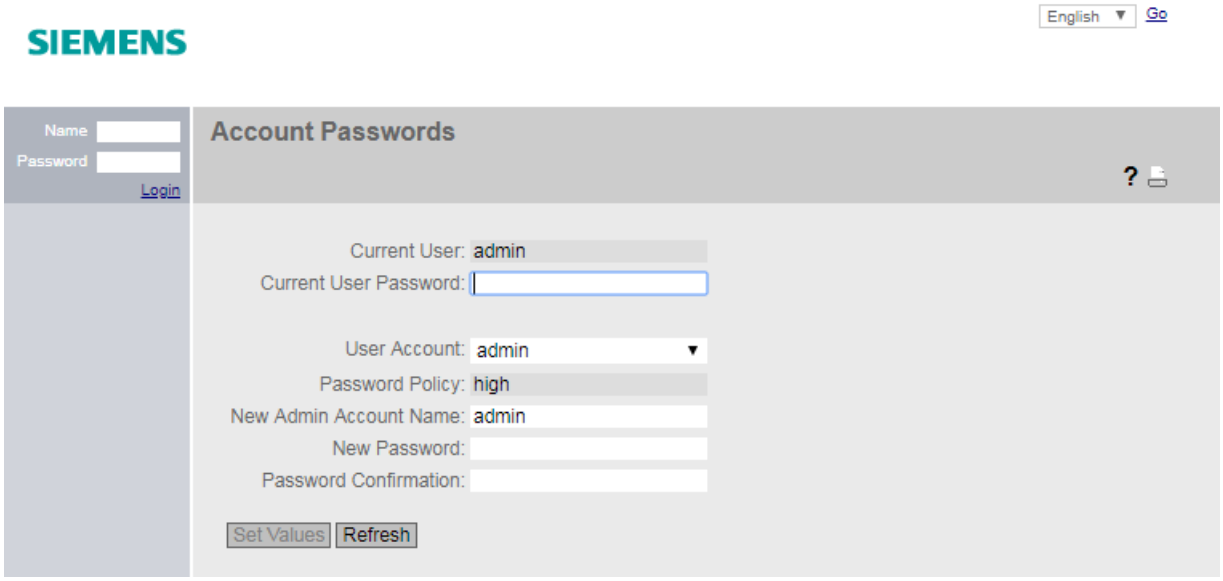
1. “名称”(Name) 输入框：
   – 如果是首次登录或是在“恢复出厂默认设置并重启”(Restore Factory Defaults and Restart) 后登录，则输入出厂时预设的用户“admin”。
     使用这种用户帐户时，可以更改设备的设置（对组态数据进行读写访问）。
   – 输入已创建用户帐户的用户名。可在“安全 > 用户”(Security > Users) 中组态本地用户帐户和角色。
2. “密码”(Password) 输入框：
   – 如果是首次登录或是在“恢复出厂默认设置并重启”(Restore Factory Defaults and Restart) 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。

说明

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，则可以对出厂时预设的用户“admin”进行一次重命名。之后，不可再重命名“admin”。在相应的输入框中输入新名称。

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) 之后登录，则会提示您更改密码。



新密码必须符合“高强度”密码策略：

- 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（不允许使用特殊字符 | § ? " ; : ß \）
- 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。

4. 单击“设置值”(Set Values) 按钮完成操作。
该更改立即生效。在更改管理密码后，通过 DCP 进行的访问受写保护。网络参数可使用 SINEC PNI 或“DCP Discovery”进行读取，但无法更改。

成功登录后，即会显示起始页面。

防范暴力破解

为了防范暴力破解，在多次登录尝试失败后，将拒绝用户或用户的 IP 地址登录设备。默认情况下，登录尝试次数预设为每个用户 12 次，每个 IP 地址 10 次。每次无效登录尝试后，页面锁定以等待新登录尝试的等待时间都会增加。可以在“安全 > 暴力破解预防”(Security > Brute Force Prevention (页 440)) 页面上更改这些设置。

6.3 “Information”菜单

6.3.1 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

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“系统 > 常规 > 设备”(System > General > Device) 更改本次显示的内容。

- 用于选择语言的下拉列表
- 具有状态显示的系统日期和系统时间
  可以在“系统 > 系统时间”(System > System Time) 中更改本次显示的内容。
  若未设置系统时间，则状态为 。若组态了系统时间却无法同步，则会显示黄色三角警告 。检查是否可以与时间服务器通信。如有必要，请调整组态。若设置了系统时间和/或能够同步，则状态为 。

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。
- **设备名称**
  显示设备的名称。
- **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。对于每个菜单项/子菜单，打开后将显示此窗口，并可根据需要移动此窗口。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。
  在每个搜索页面的顶部，都有一个用于搜索的输入框。在此输入框中，输入需要更多相关信息的条目，然后按 Enter 键开始搜索。随即出现一个对话框，其中会列出包含搜索条目的 WBM 页面。单击其中一个列表元素后，将在浏览器的新标签页中打开相应的 WBM 页面。
- **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。

- **收藏夹**
  交付产品时，该按钮在所有页面上均为禁用状态 。
  如果单击该按钮，符号会变为 ，当前打开的页面或选项卡被标记为收藏内容。启用该按钮后，导航区域将分为两个选项卡。第一个选项卡“Menu”包含启用该按钮前的所有可用菜单。第二个选项卡 “收藏夹”(Favorites) 包含用户选作收藏内容的所有页面/选项卡。在 “收藏夹”(Favorites) 选项卡上，页面/选项卡按照 “菜单”(Menu) 选项卡中的结构排列。如果禁用已创建的所有收藏夹， “收藏夹”(Favorites) 选项卡将再次被移除。为此，单击相关页面/选项卡中的 按钮。
  可以在 “系统 > 加载和保存”(System > Load&Save) 页面使用 HTTP 或者 TFTP 保存、上传和删除设备的收藏夹组态。

- **故障**
  该按钮仅在故障状态下可见，并在设备检测到故障时闪烁。
  单击此按钮时，将进入 “信息 > 故障”(Information > Faults) 页面，其中包含所发生错误的描述。

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。

如果已创建收藏夹，导航区域将分为两个选项卡： “菜单”(Menu) 和 “收藏夹”(Favorites)。

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。

- **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“后退”(Back) 按钮，可向上翻页查看数据记录。
- **使用“清除”(Clear)**删除显示画面
  无论是否选择了过滤器，在有序列日志的页面中，可以同时清除所有表格条目。此操作可清除显示画面。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。单击“清除”(Clear) 按钮可完全删除数据记录。
- **按钮“全部显示”(Show all)**
  可以在包含大量数据记录的页面上显示所有条目。单击“全部显示”(Show all) 按钮可在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。
- **用于页面切换的下拉列表**
  在包含大量数据记录的页面中，可以导航至所需页面。从下拉列表中选择要显示的相关页面。
- **“复位计数器”(Reset counter) 按钮**
  单击“复位计数器”(Reset counter) 可复位所有计数器。还可以通过重启复位计数器。

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‘写入启动组态’可立即保存”(Changes will be saved automatically in x seconds. Press 'Write Startup Config' to save immediately)。

说明

中断保存

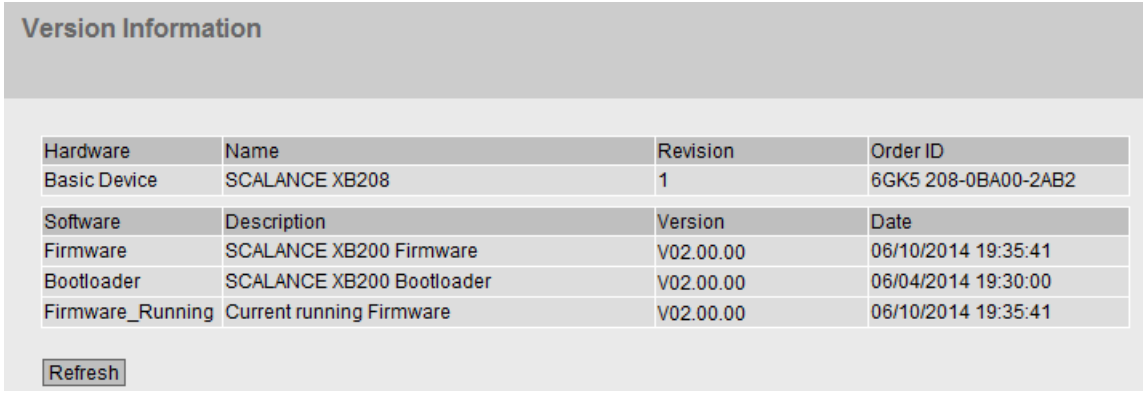
只有消息中的定时器到期后，才会启动保存。此时将显示如下消息：“正在保存组态数据。请勿关闭设备”(Saving configuration data in progress. Please do not switch off the device)。保存所需的时间取决于设备。

- 不要在定时器到期后立即关闭设备。

6.3.2 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。



显示值说明

表 1 包含以下列：

- **“硬件”(Hardware)**
  - “基本设备”(Basic Device)
    显示基本设备。
  - Px.x
    x.x 指定插入 SFP 模块的端口。
- **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。

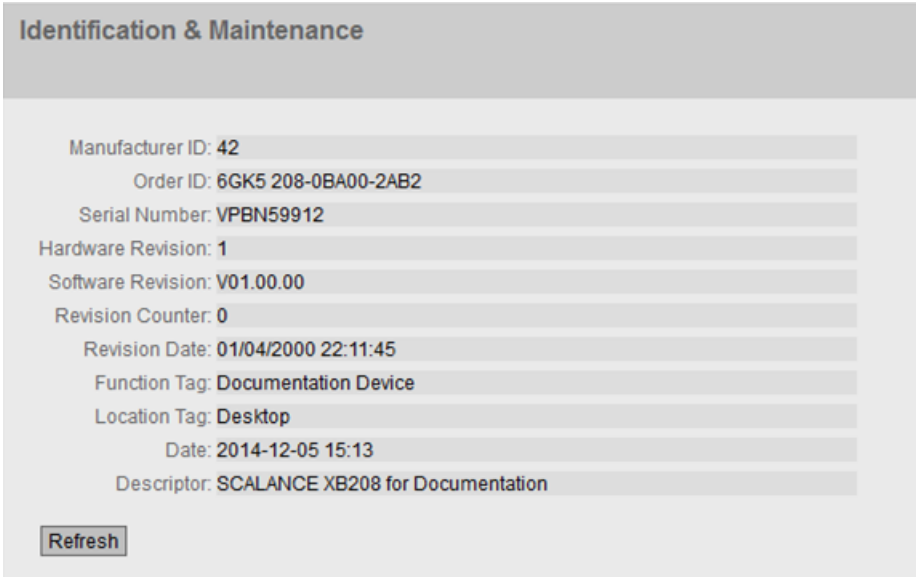
表 2 包含以下列：

- **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。

6.3.3 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。



显示值说明

该表格包括以下行：

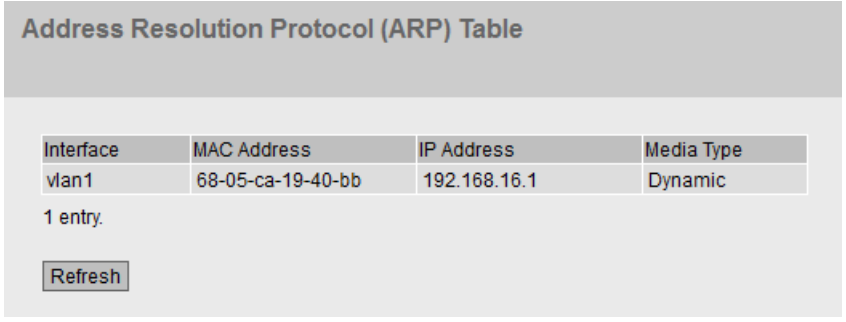
- **“制造商 ID”(Manufacturer ID)**
  显示制造商 ID。
- **“订货号”(Order ID)**
  显示订货号。
- **“序列号”(Serial Number)**
  显示序列号。
- **“硬件版本”(Hardware Revision)**
  显示硬件版本。
- **软件版本 (Software version)**
  显示软件版本。
- **修订计数器 (Revision Counter)**
  无论何种版本，此框始终显示值“0”。

- **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。

6.3.4 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。



显示值说明

该表格包括以下列：

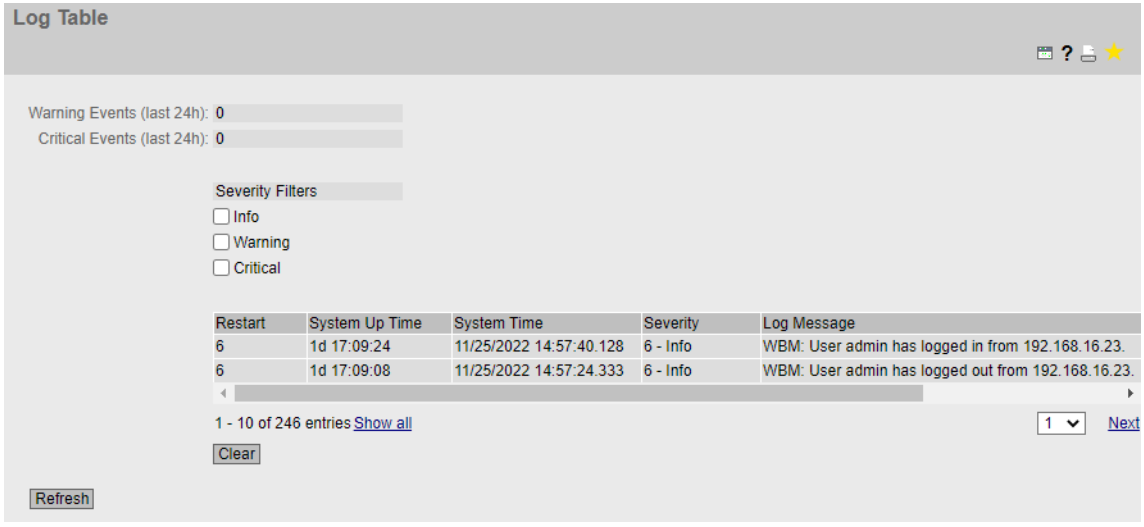
- **“接口”(Interface)**
  显示获取行条目所用的接口。
- **MAC Address**
  显示目标设备或源设备的 MAC 地址。
- **IP 地址 (IP Address)**
  显示目标设备的 IPv4 地址。
- **“介质类型”(Media Type)**
  显示连接的类型。
  - “动态”(Dynamic)
    设备自动识别到地址数据。
  - “静态”(Static)
    地址作为静态地址输入。

6.3.5 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“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。



显示值说明

该页面包含以下框：

- **'Warning' event (last 24 hr)**
  显示最近 24 小时发生的“Warning”类别的事件数量。
- **'Critical' event (last 24 hr)**
  显示最近 24 小时发生的“Critical”类别的事件数量。

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：

- **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。
- **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。
- **System Time**
  显示该事件发生的日期和时间。
- **Severity**
  将条目分入以上类别。
- **Log Message**
  显示已发生事件的简要说明。

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。

6.3.6 故障

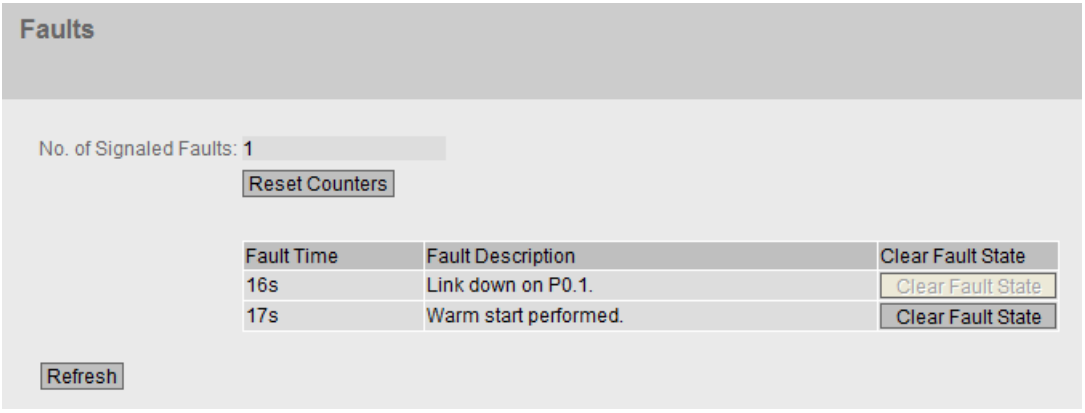
错误状态

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：

- “System > Events”
- “System > Fault Monitoring”

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。



说明

- **No. of Signaled Faults**
  指示故障 LED 点亮的频率，而不是出现故障的次数。

该表包含以下列：

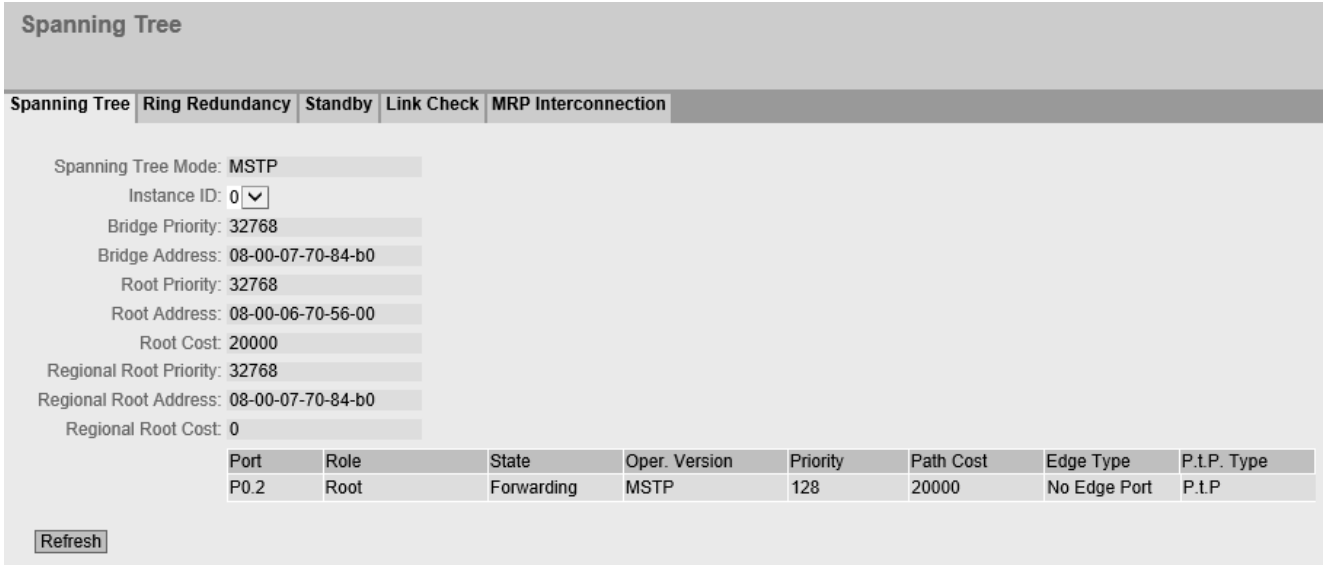
- **Fault Time**
  显示自系统上一次因发生所描述的错误/故障而导致重启以来已持续运行的时间。
- **Fault Description**
  显示已发生故障/错误的简要说明。
- **Clear Fault State**
  有些故障可以确认，并将它们从故障列表中删除，例如，“Cold/Warm Start”事件中的故障。如果启用了“Clear Fault State”按钮，则可删除错误。

6.3.7 冗余

6.3.7.1 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。



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 > 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。

- **网桥优先级 (Bridge Priority)/根优先级 (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：

- **端口 (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。
- **角色 (Role)**
  显示端口状态。可能的值包括：
  - 已禁用 (Disabled)
    已从生成树中手动移除端口，生成树将不再考虑该端口。
  - 指定 (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
  - 备用 (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。
  - 根 (Root)
    端口提供指向根网桥的最佳路径。
  - 主设备 (Master)
    此端口指向 MST 区域外部的根网桥。
  - RSTP+
    启用了 RSTP+ 的设备的环网端口。
- **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：
  - 丢弃 (Discarding)
    端口接收 BPDU 帧。其它进入或离开的帧会被丢弃。
  - 侦听 (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。
  - 学习 (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。
  - 转发 (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。

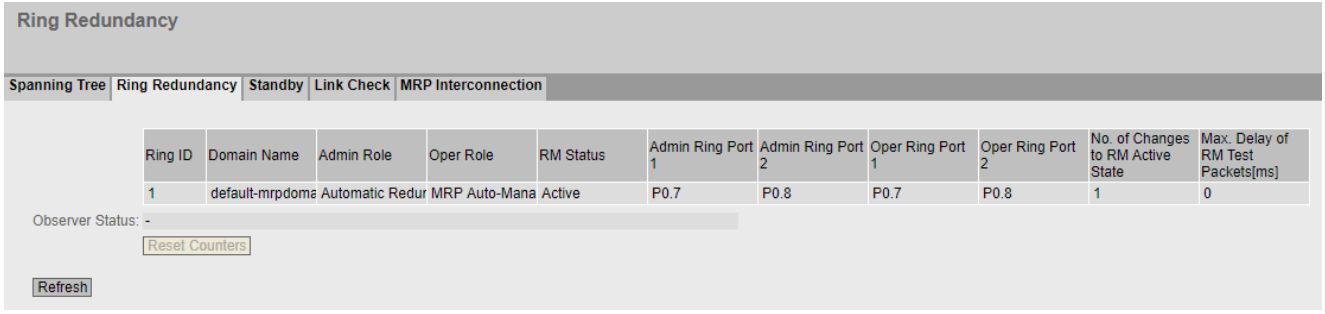
- **路径开销 (Path Cost)**
  此参数用于计算将要选择的路径。选择具有最小值的路径。如果设备的多个端口具有相同的值，则选择端口号最小的端口。
  路径开销的计算主要基于传输速度。可达到的传输速度越高，路径成本的值就越低。
  快速生成树的典型路径成本值如下：
  - 10,000 Mbps = 2,000
  - 1000 Mbps = 20,000
  - 100 Mbps = 200,000
  - 10 Mbps = 2,000,000

  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“成本计算”(Cost Calc.)。
- **边缘类型 (Edge Type)**
  显示连接类型。可能的值包括：
  - 边缘端口 (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。

6.3.7.2 环网冗余

有关环网冗余的信息

在此页面中，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。禁用环网冗余时，表格为空。



显示值说明

该表格包括以下列：

- **环网 ID (Ring ID)**
  环网的 ID。
- **域名 (Domain Name)**
  唯一分配给每个环网的名称。
- **管理员角色 (Admin Role)**
  环网冗余模式。
- **操作员角色 (Oper. Role)**
  设备在环网内的角色：
  - 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。通过 WBM 为设备设置“MRP 管理器”角色或通过 STEP 7 为设备设置“管理器”角色。
  - 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。
- **管理员环网端口 1 (Admin Ring Port 1) 和管理员环网端口 2 (Admin Ring Port 2)**
  这两列显示已组态为环网端口的端口。
- **操作员环网端口 1 (Oper. Ring Port 1) 和操作员环网端口 2 (Oper. Ring Port 2)**
  这两列显示用作环网端口的端口。
- **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”，则将显示文本“Redundancy manager disabled”。
- **RM 测试包的最大延迟 [ms] (Max. Delay of 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”，则将显示文本“Redundancy manager disabled”。

显示以下对话框：

- **观察器状态 (Observer Status)**
  显示观察器的当前状态。
- **“复位计数器”(Reset counter) 按钮**

  说明

  当组态了环网冗余模式“HRP 管理器”(HRP Manager)、“MRP 管理器”(MRP Manager) 或“MRP 自动管理器”(MRP Auto Manager) 时，“复位计数器”(Reset Counters) 按钮有效。

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

6.3.7.3 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。

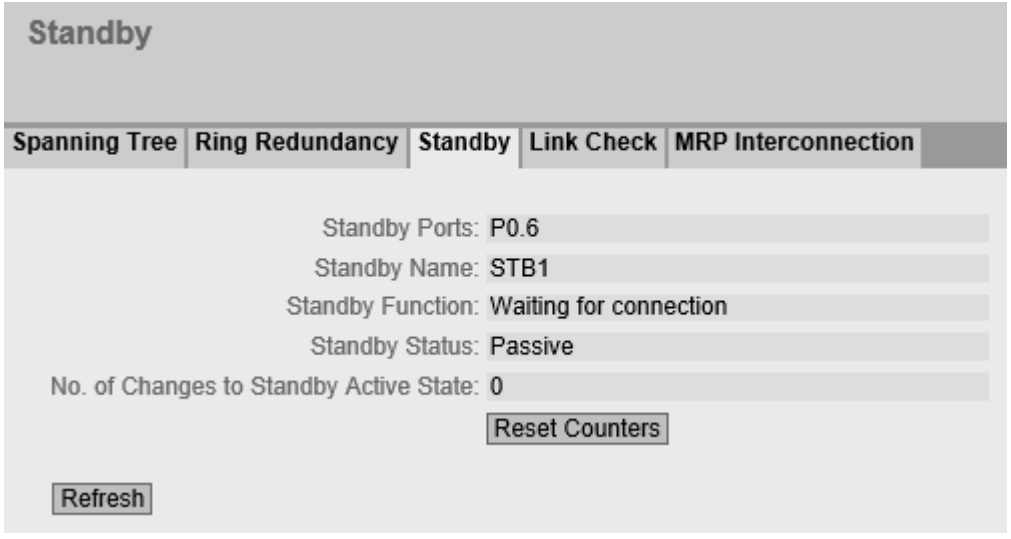
说明

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：



显示值说明

该页面显示以下字段：

- **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。

6.3.7.4 链路检查

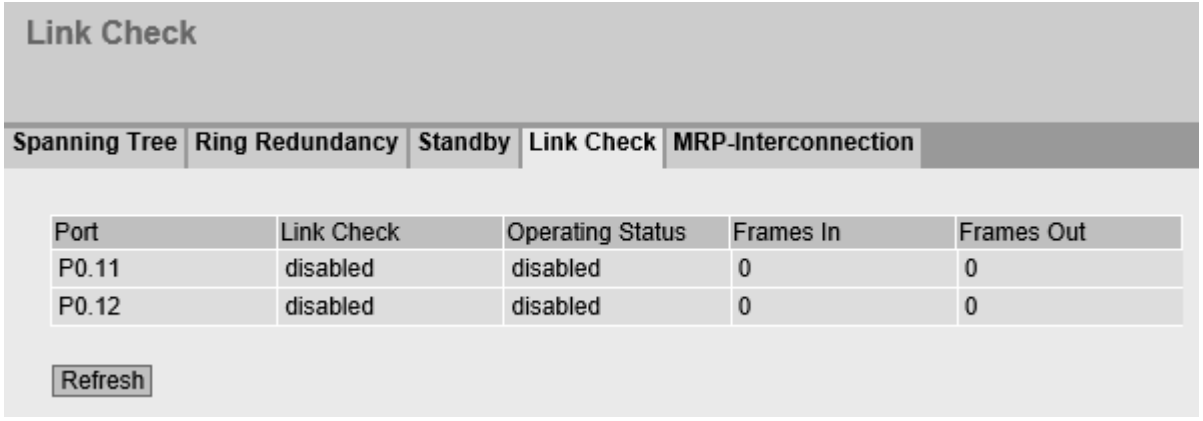
监视环网中的光纤连接

本页显示了链路检查的以下信息：

- 环网端口
- 当前状态（激活或未激活）
- 已发送或接收到的监视连接的链路检查帧的统计数据。

说明

如果将“链路检查”与冗余协议（例如 HRP）搭配使用，则已发送和接收的“链路检查”帧的值可能有所不同。



显示值说明

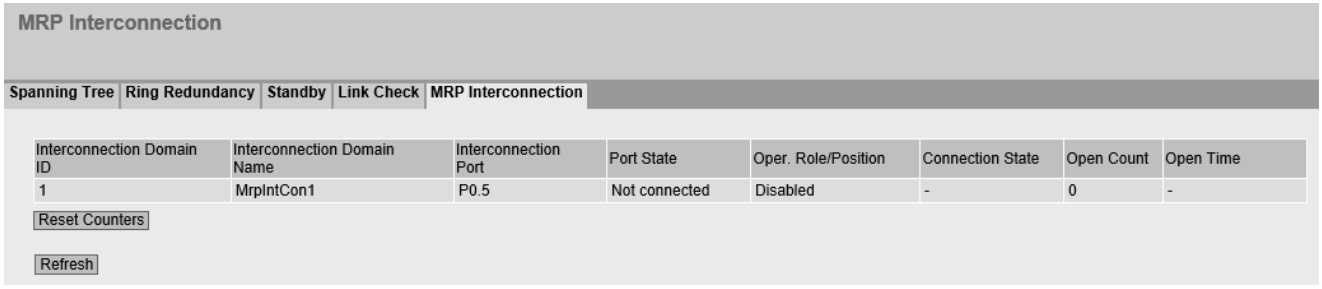
该页面显示以下字段：

- **端口 (Port)**
  显示了后面信息所涉及的端口。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。
- **链路检查 (Link Check)**
  显示链路检查功能是启用还是禁用状态。只能为光纤端口启用“链路检查”(Link Check)。

- **操作状态 (OperState)**
  显示链路检查功能的状态。可能的状态如下：
  - 禁用 (Disabled)
    将禁用该功能。
  - 启用 (Enabled)
    将启用该功能。连接伙伴尚未确认该监视。
  - 运行 (Running)
    将启用该功能。连接监视已启用。将对传出和传入测试帧进行计数并匹配。
  - 故障 (Faults)
    将启用该功能。链路检查在监视部分检测到故障并关闭了端口。
- **帧输入 (Frames in)**
  显示接收到的链路检查测试帧数量。
- **帧输出 (Frames out)**
  显示发出的链路检查测试帧数量。

6.3.7.5 MRP 互连

环网冗余链路



说明

该页面显示以下字段：

- **互连域 ID (Interconnection Domain ID)**
  MRP 互连连接的 ID。
- **互连域名称 (Interconnection Domain Name)**
  MRP 互连连接的名称。
- **“互连端口”(Interconnection Port)**
  用于 MRP 互连连接的端口。

- **“端口状态”(Port Status)**
  显示端口是启用还是禁用状态。数据通信只能通过已启用的端口实现。可使用以下选项：
  - “转发”(Forwarding)
    端口在使用中。
  - “已阻止”(Blocked)
    端口被阻止。
  - “已禁用”(Disabled)
    端口已禁用。
  - “未连接”(Not connected)
    端口未连接。
- **“运行角色/位置”(Oper. Role/Position)**
  显示设备的角色。如果是“客户端”角色，还会显示客户端的位置。可使用以下选项：
  - 禁用 (Disabled)
  - “管理器”(Manager)
  - 主客户端 (Primary Client)
  - 次客户端 (Secondary Client)
- **“连接状态”(Connection Status)**
  MRP 互连域的状态。可使用以下选项：
  - 禁用 (Disabled)
  - “未定义”(Not defined)
  - “断开”(Open)
    冗余连接不可用。
  - “闭合”(Close)
    冗余连接可用。
- **“断开计数”(Open Count)**
  显示自 MIM 上次计数器复位以来，“断开”(Open) 状态出现的频率。对于 MIC，该值始终为“0”。
- **“断开时间”(Open Time)**
  自上次呈现“断开”(Open) 状态后所经过的时间。对于 MIC，此处不显示任何值。
- **“复位计数器”(Reset Counter)**
  单击“复位计数器”(Reset Counter) 可将计数器复位。重启后，计数器将复位。

6.3.8 以太网统计信息

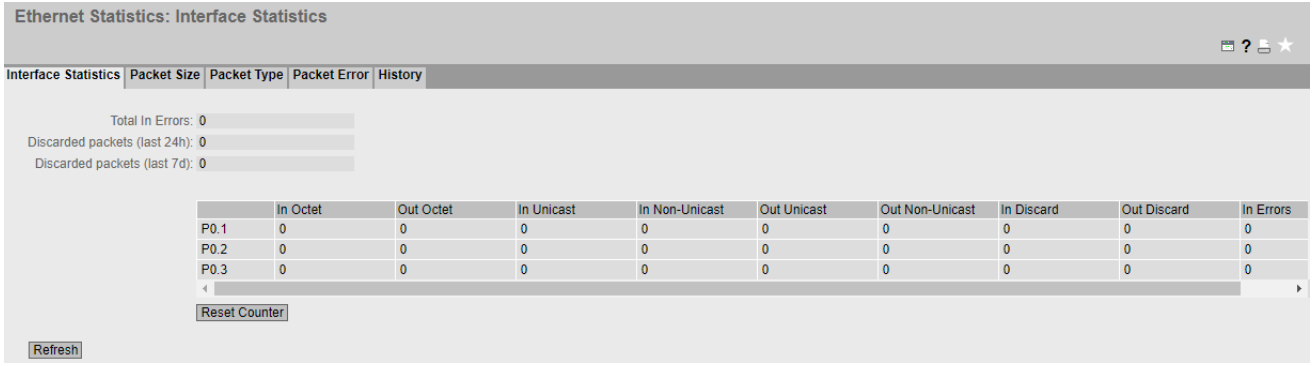
6.3.8.1 接口统计信息

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。

说明

接口统计信息指定每个端口接收或发送的总字节数。与之相反的是，VLAN 接口的信息仅与对应接口的第 3 层数据通信有关。



显示值说明

该页面包含以下框：

- **In Errors (total)**
  显示所有接收的错误总数。
- **Discarded packets (last 24 hrs)**
  显示最近 24 小时内所有丢弃的数据包总数。
- **Discarded packets (last 7 days)**
  显示最近 7 天内所有丢弃的数据包总数。

该表格包括以下列：

- **In Octet**
  显示接收到的字节数。
- **Out Octet**
  显示发送的字节数。

- **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。
- **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 Discard**
  显示已丢弃的传入帧数。
- **Out Discard**
  显示已丢弃的传出帧数。
- **In Errors**
  显示所有可能的 RX 错误数，请参见“Packet Error”选项卡。

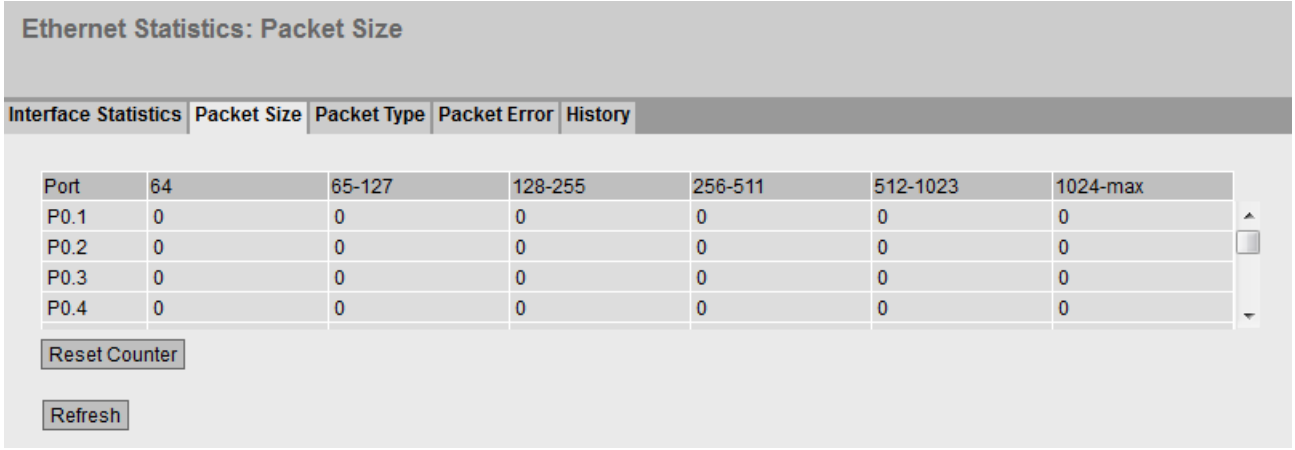
6.3.8.2 数据包大小 (Packet Size)

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。



显示值说明

该表格包括以下列：

- **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。

- **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。

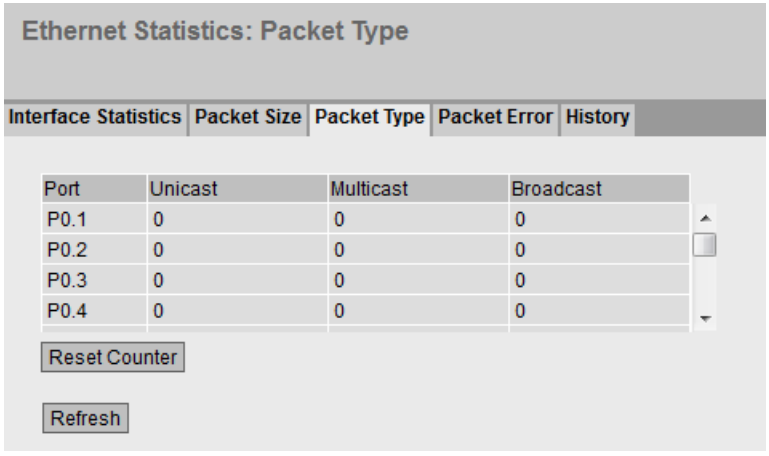
6.3.8.3 数据包类型 (Packet Type)

按数据包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“Unicast”、“Multicast”和“Broadcast”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。



显示值说明

该表格包括以下列：

- **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**
  端口号之后的其它各列包括按照其 Packet Type“Unicast”、“Multicast”和“Broadcast”分类的到达帧的绝对数量。

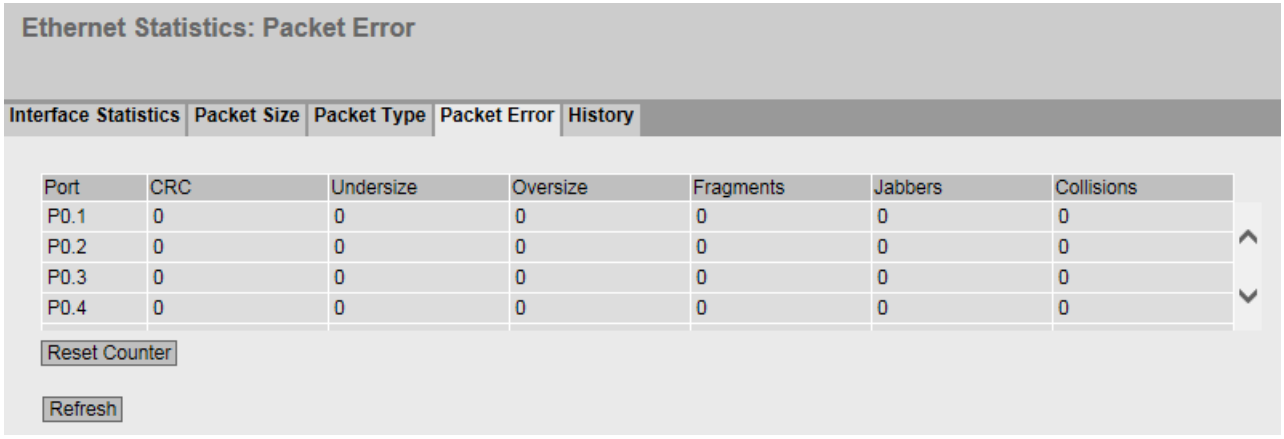
6.3.8.4 数据包错误

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。



显示值说明

该表格包括以下列：

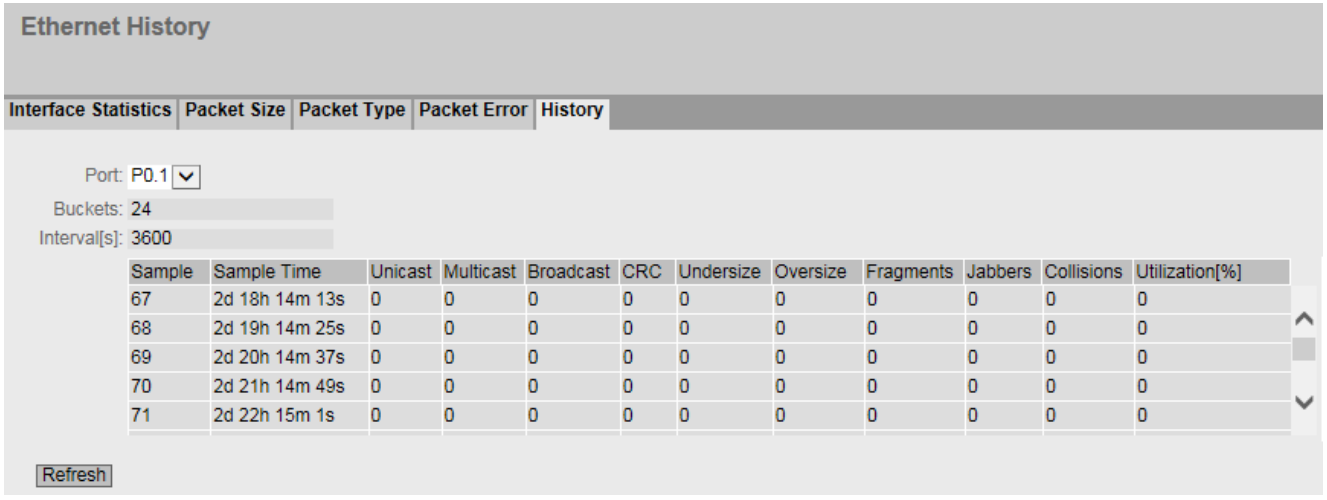
- **Port**
  显示可用端口和链路汇聚。端口由模块号和端口号组成，例如，端口 0.1 表示模块 0，端口 1。
- **Error types**
  端口号之后的其它各列包括按照其错误类型分类的到达帧的绝对数量。
  在该表的各列中，将根据以下错误类型进行区分：
  - CRC
    数据包内容与 CRC 校验和不符。
  - Undersize
    数据包长度小于 64 字节。
  - Oversize
    由于长度过长而被丢弃的数据包。
  - Fragments
    数据包长度小于 64 字节，且 CRC 校验和错误。
  - Jabber
    包含错误 CRC 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。

6.3.8.5 历史信息

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。

可在“Layer 2 > RMON > History”页面中设置要对哪个端口进行采样。



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

设置

- **Port**
  选择要为其显示历史记录的端口。

显示值说明

- **Buckets**
  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：

- **Sample**
  样本的编号
- **Sample Time**
  获取样本时的系统运行时间。
- **Unicast**
  已接收的单播帧数。

- **Multicast**
  已接收的组播帧数。
- **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。

6.3.9 Unicast

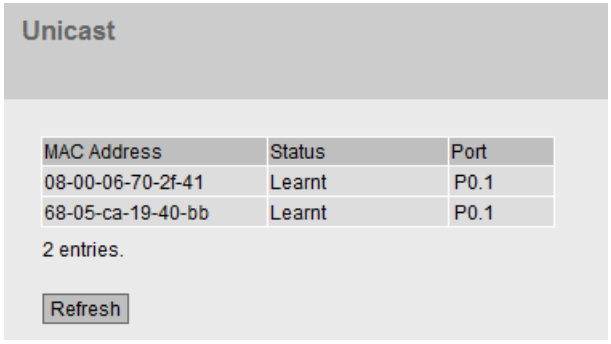
单播过滤表的状态

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。

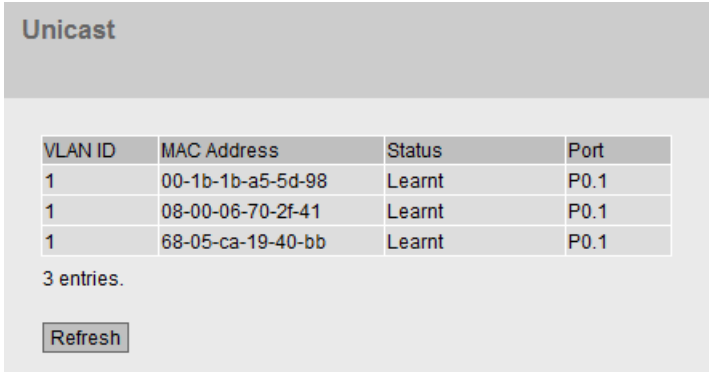
“Base bridge mode”的相关性

显示的列取决于所设置的“Base bridge mode”。如果更改“Base bridge mode”，现有条目将丢失。

基础网桥模式“802.1D 透明网桥”的 WBM 页面：



基础网桥模式“802.1Q VLAN 网桥”的 WBM 页面：



说明

该表包含以下列：

- **VLAN ID**
  显示分配给此 MAC 地址的 VLAN ID。
- **MAC Address**
  显示设备已学习或用户已组态的节点 MAC 地址。

- **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。
  - Other
    指定的地址通过专用 VLAN 间接识别。
- **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。

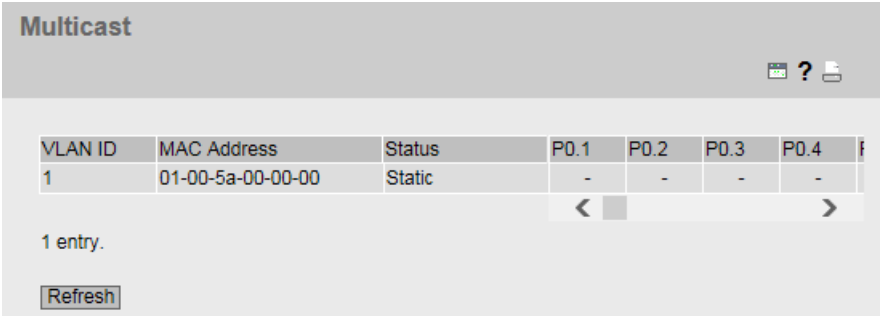
6.3.10 组播

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）。

“Base bridge mode”的相关性

如果更改“Base bridge mode”，现有条目将丢失。



说明

该表包含以下列：

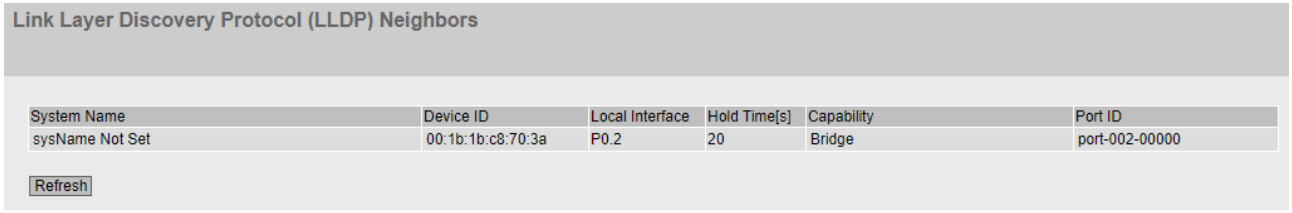
- **VLAN ID**
  显示要向其分配 MAC 组播地址的 VLAN 的 VLAN ID。
- **MAC Address**
  显示设备已学习或用户已组态的 MAC 组播地址。
- **Status**
  显示每个地址条目的状态。可能的信息如下：
  - Static
    此地址是由用户以静态方式输入的。静态地址会永久存储；也就是说，当老化时间结束或设备重启时，静态地址不会被删除。这些地址可由用户删除。
  - IGMP
    此地址的目标端口通过 IGMP 获得。
  - GMRP
    此地址的目标端口由收到的 GMRP 帧注册。
- **Port List**
  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

6.3.11 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)。



显示值说明

该表包含以下列：

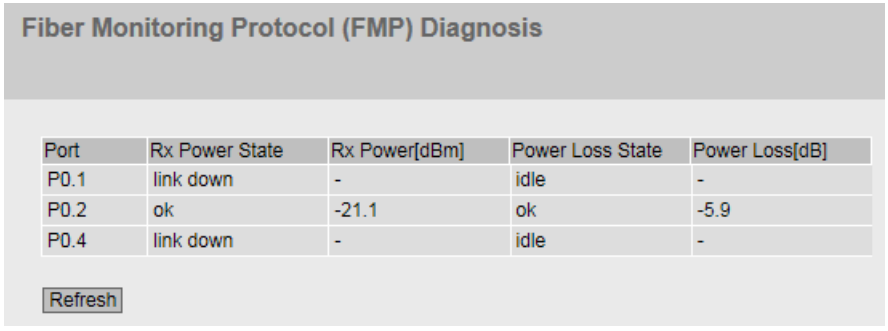
- **系统名称 (System Name)**
  所连接设备的系统名称。
- **设备 ID (Device ID)**
  所连设备的设备 ID。设备 ID 与通过 SINEC PNI 等分配的设备名称相对应。如果未分配设备名称，则显示设备的 MAC 地址。
- **本地接口 (Local Interface)**
  工业以太网交换机接收信息的端口
- **保持时间[s] (Hold Time[s])**
  以秒为单位的保持时间
  此处指定的时间是条目持续存储在设备中的时间。在这段时间内，如果工业以太网交换机未从所连设备接收到任何新信息，则将删除该条目。
- **性能 (Capability)**
  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
- **端口 ID (Port ID)**
  连接工业以太网交换机的设备端口。

6.3.12 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)。



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。
  - **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（链接中断）、光纤监视功能已禁用或者伙伴端口不支持光纤监视功能，则显示“-”。

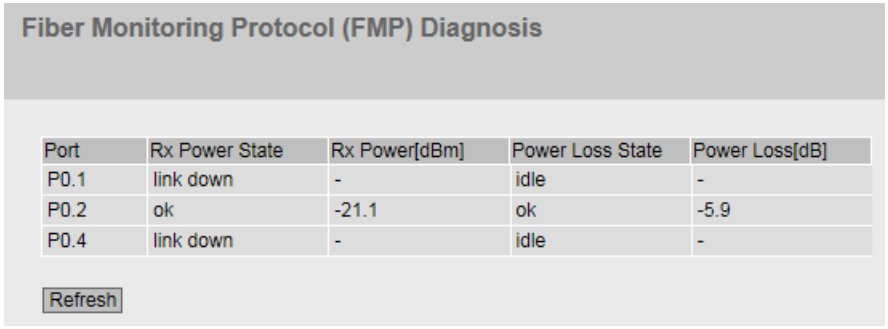
6.3.13 塑料光纤

POF 端口监视

此页面显示连接塑料光纤 (POF) 的接口的诊断数据。

每个 POF 端口当前可用的链接功率裕量显示为数值。

链接功率裕量指示可承受的发送器和接收器之间连接的衰减。链接功率裕量越高，维持功能链接时可承受的衰减也越高。如果链接功率裕量缩减，则说明衰减已提高，例如由于老化或故障。所用电缆越长，可用的链接功率裕量就越低。



显示值说明

该表包含以下列：

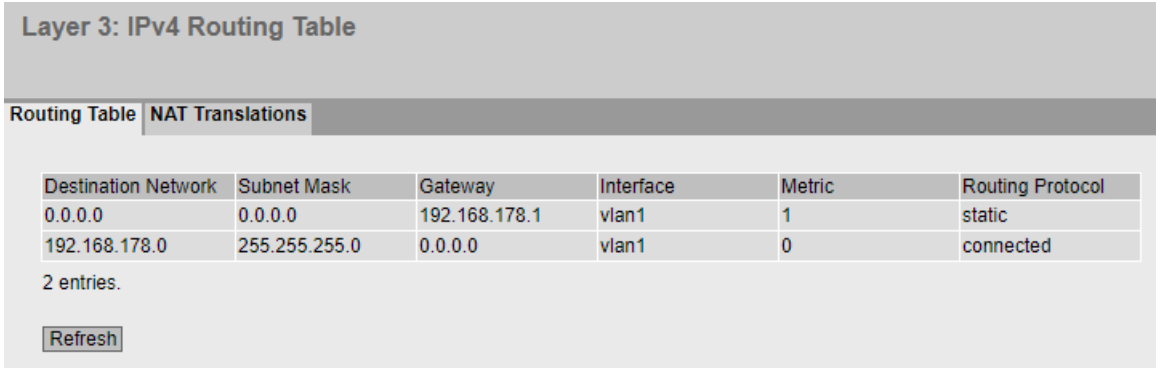
- **端口 (Port)**
  显示所有 POF 端口。
- **功率状态 (Power State)**
  显示端口的当前状态。
  - **disabled**
    监视已禁用。
  - **ok**
    对于无故障操作，具有充足的链接功率裕量。
  - **maint. req.**
    检查链接。
    发出了报警信号。
  - **maint. dem.**
    需要检查链接。
    已发出报警信号，故障 LED 亮起。
  - **link down**
    与通信伙伴的连接已中断。未检测到连接。
- **功率 (Power)**
  显示链接功率余量的当前值。
  如果不存在连接 (Link down) 或监视功能已禁用，则会显示“-”。如果伙伴端口上的监视功能未启用，则会显示值 0.0。
- **需要功率 [dBm] 维护（警告）(Power [dBm] Maintenance Required (warning))**
  显示通过严重等级为“Warning”的消息来通知用户链接功率余量超限时所处的值。
- **要求功率 [dBm] 维护（严重）(Power [dBm] Maintenance Demanded (critical))**
  显示通过严重等级为“Critical”的消息来通知用户链接功率余量超限时所处的值。

6.3.14 路由

6.3.14.1 路由表

简介

该页面显示了当前使用的路由。



显示值说明

该表格包括以下列：

- **目标网络 (Destination Network)**
  显示此路由的目标地址。
- **子网掩码 (Subnet Mask)**
  显示此路由的子网掩码。
- **网关 (Gateway)**
  显示此路由的网关。对于接收设备路由，将显示信息“接收设备”(Sink)，而不是 IP 地址。
- **接口 (Interface)**
  显示此路由的接口。

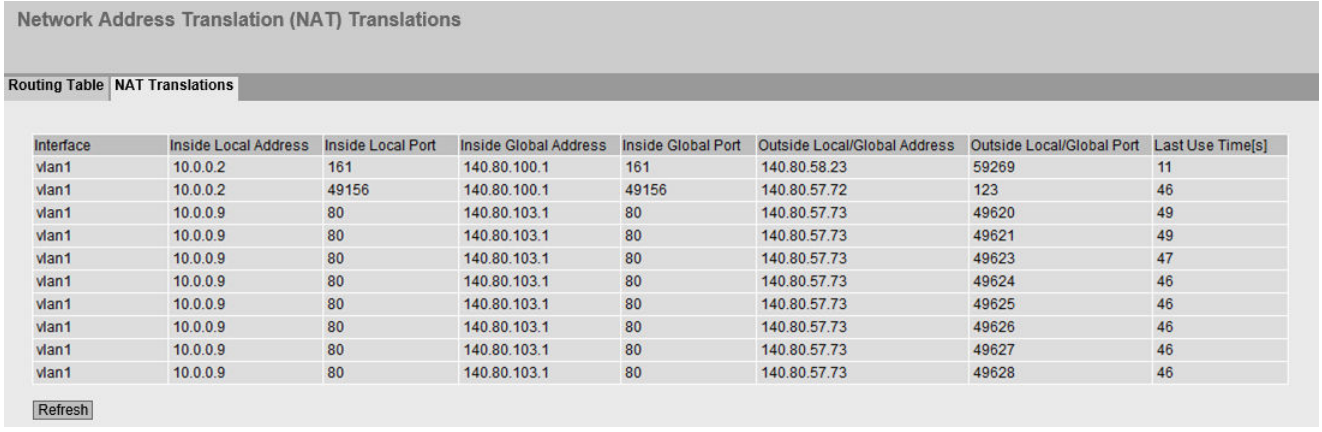
- **度量 (Metric)**
  显示此路由的度量。值越大，数据包到达目的地所需的距离越长。
- **路由协议 (Routing Protocol)**
  显示来源于端口路由表的路由协议。可以是以下条目：
  - Connected：已连接路由
  - Static：静态路由
  - RIP：通过 RIP 路由
  - OSPF：通过 OSPF 路由
  - Other：其它路由

6.3.14.2 NAT 转换

概述

该页面显示激活的 NAT 连接。

显示值说明



Interface	Inside Local Address	Inside Local Port	Inside Global Address	Inside Global Port	Outside Local/Global Address	Outside Local/Global Port	Last Use Time[s]
vlan1	10.0.0.2	161	140.80.100.1	161	140.80.58.23	59269	11
vlan1	10.0.0.2	49156	140.80.100.1	49156	140.80.57.72	123	46
vlan1	10.0.0.9	80	140.80.103.1	80	140.80.57.73	49620	49
vlan1	10.0.0.9	80	140.80.103.1	80	140.80.57.73	49621	49
vlan1	10.0.0.9	80	140.80.103.1	80	140.80.57.73	49623	47
vlan1	10.0.0.9	80	140.80.103.1	80	140.80.57.73	49624	46
vlan1	10.0.0.9	80	140.80.103.1	80	140.80.57.73	49625	46
vlan1	10.0.0.9	80	140.80.103.1	80	140.80.57.73	49626	46
vlan1	10.0.0.9	80	140.80.103.1	80	140.80.57.73	49627	46
vlan1	10.0.0.9	80	140.80.103.1	80	140.80.57.73	49628	46

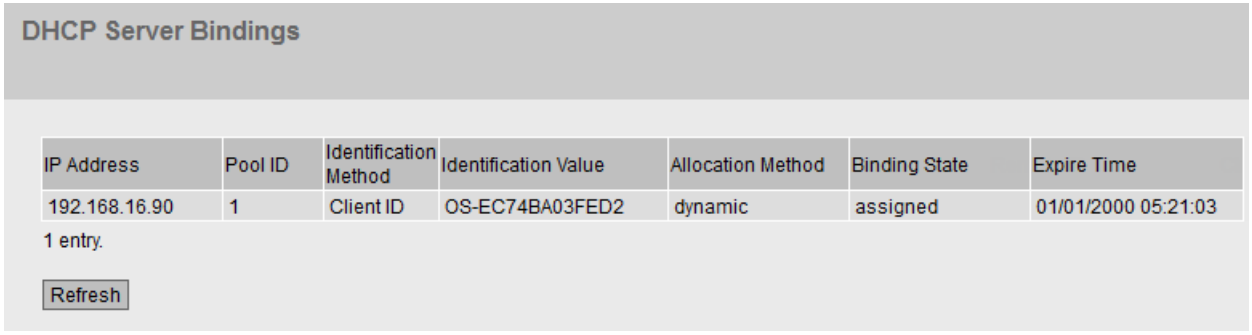
该表格包括以下列：

- **接口 (Interface)**
  显示 IP 接口。
- **内部本地地址 (Inside Local Address)**
  显示外部可访问的设备的实际地址。
- **内部本地端口 (Inside Local Port)**
  显示分配到内部本地地址的端口。

- **内部全局地址 (Inside Global Address)**
  显示可供外部访问设备的地址。
- **内部全局端口 (Inside Global Port)**
  显示分配到内部全局地址的端口。
- **外部本地/全局地址 (Outside Local/Global Address)**
  显示通信伙伴的地址。
- **外部本地/全局端口 (Outside Local/Global Port)**
  显示外部通信伙伴的端口。
- **最后使用时间 [s] (Last Use Time [s])**
  显示最后一次传输数据包的时间。

6.3.15 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。



说明

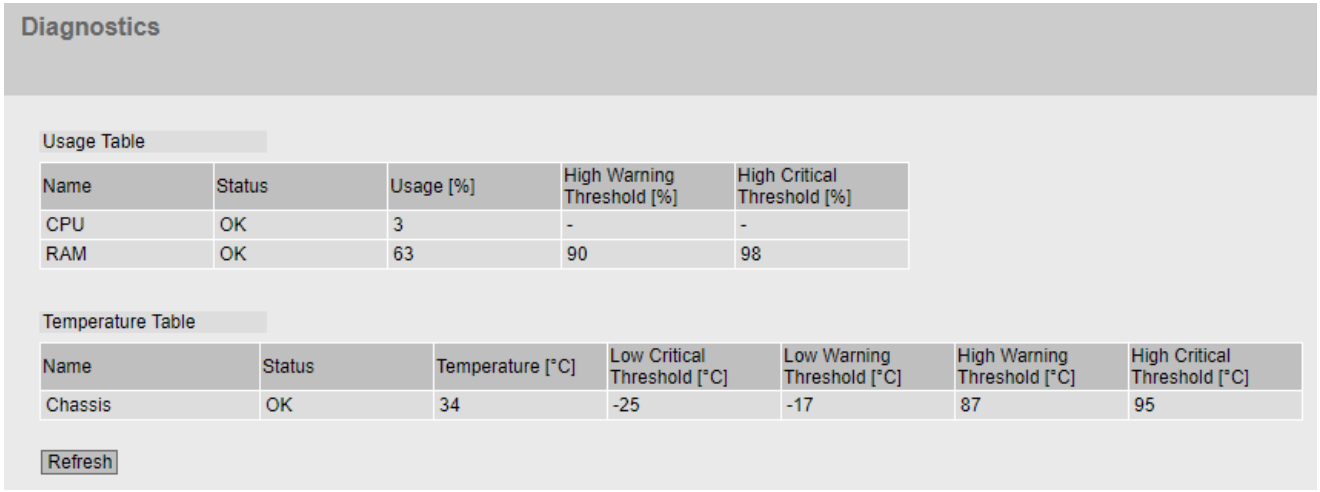
- **IP 地址 (IP Address)**
  显示分配给 DHCP 客户端的 IPv4 地址。
- **池 ID (Pool ID)**
  显示 IPv4 地址段编号。
- **标识方法 (Identification Method)**
  显示标识 DHCP 客户端的方法。
- **标识值 (Identification value)**
  显示 DHCP 客户端的 MAC 地址和客户端 ID。

- **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。
- **过期时间 (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 地址或扩展所分配的 IPv4 地址的租用时间。

6.3.16 诊断 (Diagnostics)

此页用于显示设备内部和外部模块的占用率值和温度值。只有当模块提供相应信息时，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。如果占用率值超出所显示阈值，则状态会相应地发生变化。对于温度值，当其低于阈值下限时，状态也会变化。

阈值由设备预先设定且无法修改。若未设置阈值，将显示“-”。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。



说明

占用率表格包括以下列：

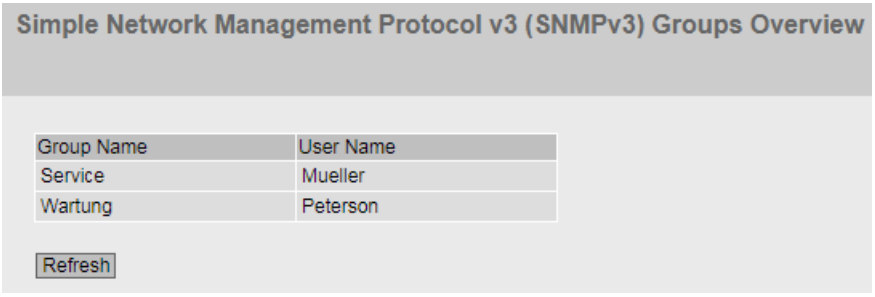
- **名称 (Name)**
  显示模块名称。
- **状态 (Status)**
  基于阈值与当前占用率之间的关系，以优先级升序显示以下状态值。
  - **OK**
    占用率处于预设的阈值范围内。
  - **WARNING**
    已超出“Warning”严重级别对应的上限阈值。占用率仍处在正常范围。应检查设备的操作条件。
  - **CRITICAL**
    已超出“Critical”严重级别对应的上限阈值。需检查设备。设备过载可能导致故障。
  - **INVALID**
    占用率无法确定或无效。 “ 占用率 [%]”(Usage [%]) 框显示“-”。
  - **INITIAL**
    尚未读取任何数据。所有框中都显示“-”。
- **占用率 [%] (Usage [%])**
  显示设备占用率的当前值。显示画面会定期更新。
- **警告阈值上限 [%] (High Warning Threshold [%])**
  如果超出该值，状态会切换为“WARNING”。您可组态为发生此事件时通过消息进行通知。
- **临界阈值上限 [%] (High Critical Threshold [%])**
  如果超出该值，状态会切换为“CRITICAL”。您可组态为发生此事件时通过消息进行通知。

温度表格包含以下列：

- **名称 (Name)**
  显示模块名称。
  “Chassis”行中的信息指的是外壳的内部温度。
  指定了可拔插收发器的端口和类型。
- **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。温度仍处在正常范围。设备已经检测到了温度的上升和下降，例如，由于柜体变冷。应检查温度。
  - **CRITICAL**
    已超出“Critical”严重级别对应的上限或下限阈值。需检查设备。温度过高或过低会导致设备性能受到限制，甚至损坏设备。
  - **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。
  温度值可以有 +/- 3 °C 的偏差。这意味着，对于具有类似环境温度的相同的设备，其值可能不同。
- **下限阈值 [°C]（严重）(Lower Thrshold [°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))**
  如果超出该值，状态会切换为“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))**
  如果超出该值，状态会切换为“CRITICAL”。您可组态为发生此事件时通过消息进行通知。

6.3.17 SNMP

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



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。

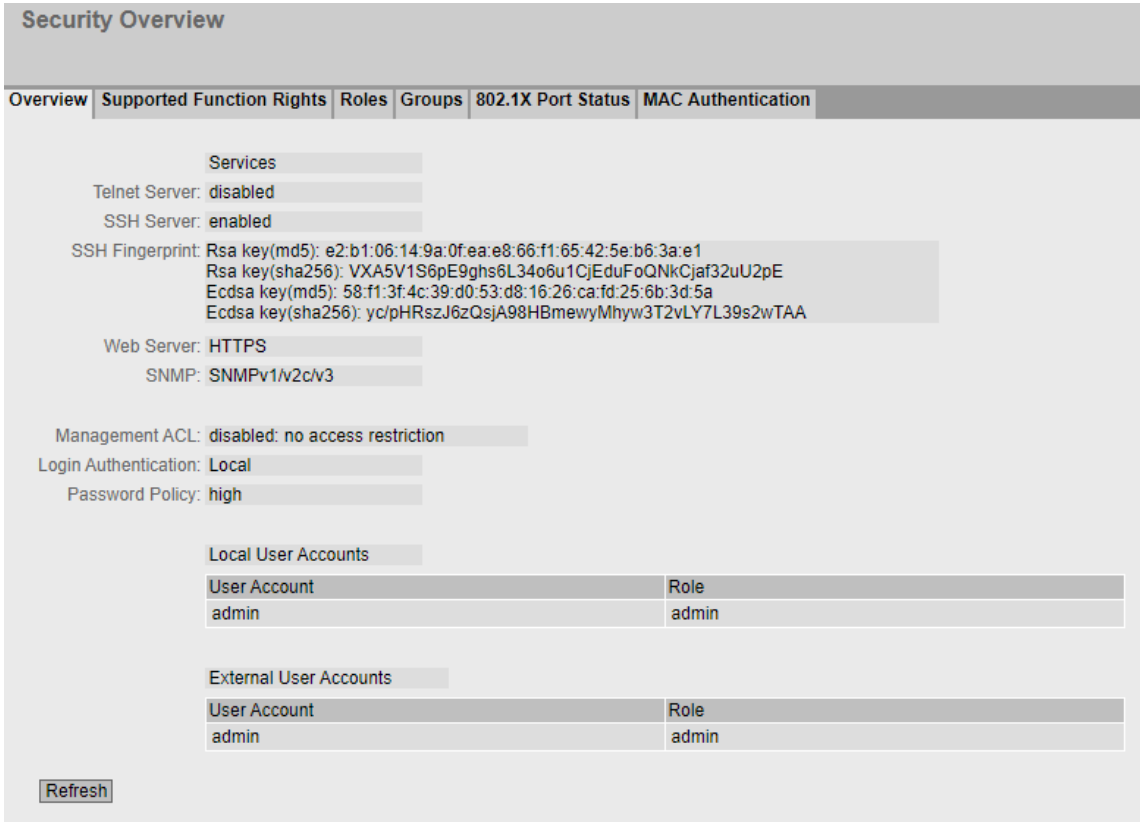
6.3.18 安全性

6.3.18.1 概述

说明

显示的值取决于已登录用户的权限。

该页面显示了安全设置和本地以及外部用户帐户。



说明

服务

“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
- **SSH 指纹 (SSH Fingerprint)**
  该字段显示 SSH 识别码。

- **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：现在，只能通过 HTTPS 访问 WBM。
  - HTTP：现在，只能通过 HTTP 访问 WBM。
- **SNMP**
  可以在“系统 > SNMP > 常规”(System > SNMP > General) 中组态设置。
  - “-”（禁用 SNMP）
    无法使用 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。
- **管理 ACL (Management ACL)**
  在“安全 > 管理 ACL”(Security > Management ACL) 下组态设置
  - 启用：仅受限访问 (Enabled: Restricted access only)：使用管理访问控制列表 (ACL) 访问受限。
  - 禁用：无访问限制 (Disabled: No access restriction)：管理 ACL 未启用。
- **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。如果用户不存在，则将发送 ADIUS 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。
- **密码策略** (Password Policy)
  显示当前正在使用的密码策略。

本地和外部用户帐户

可在“安全 > 用户”(Security > Users) 中组态本地用户帐户和角色。

创建本地用户帐户时，会自动生成外部用户帐户。

本地用户帐户所涉及的各个用户均具备登录设备所需的密码。

在表“外部用户帐户”(External User Accounts) 中，用户与角色相关联。在该示例中，用户“Service”与“user”角色相关联。用户在 RADIUS 服务器上定义。角色在设备本地定义。RADIUS 服务器对用户进行了授权，但相应的组未知或不存在，则设备会检查表“外部用户帐户”(External User Accounts) 中是否存在用户条目。如果存在相应的条目，则表示用户已使用相关角色的权限进行了登录。如果相应的组在设备上为已知状态，则对两个表进行了评估。为用户分配了较高权限的角色。

说明

仅当在“RADIUS 授权模式”(RADIUS Authorization Mode) 下设置“SiemensVSA”的情况下，才会对“外部用户帐户”(External User Accounts) 表进行评估。

借助 CLI 可以访问外部用户帐户。

“本地用户帐户”(Local User Accounts) 和“外部用户帐户”(External User Accounts) 表格具有以下列：

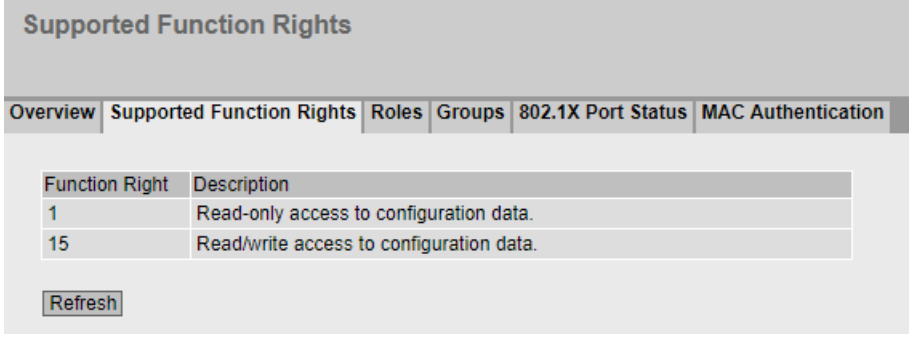
- **帐户 (Account)**
  显示本地用户的名称。
- **角色 (Role)**
  显示用户角色。在“信息 > 安全 > 角色”(Information > Security > Roles) 中可以了解有关角色的功能权限的更多信息。

6.3.18.2 所支持的功能权限

说明

所显示的值取决于登录的用户的角色。

此页面显示可在设备上本地使用的功能权限。



显示值说明

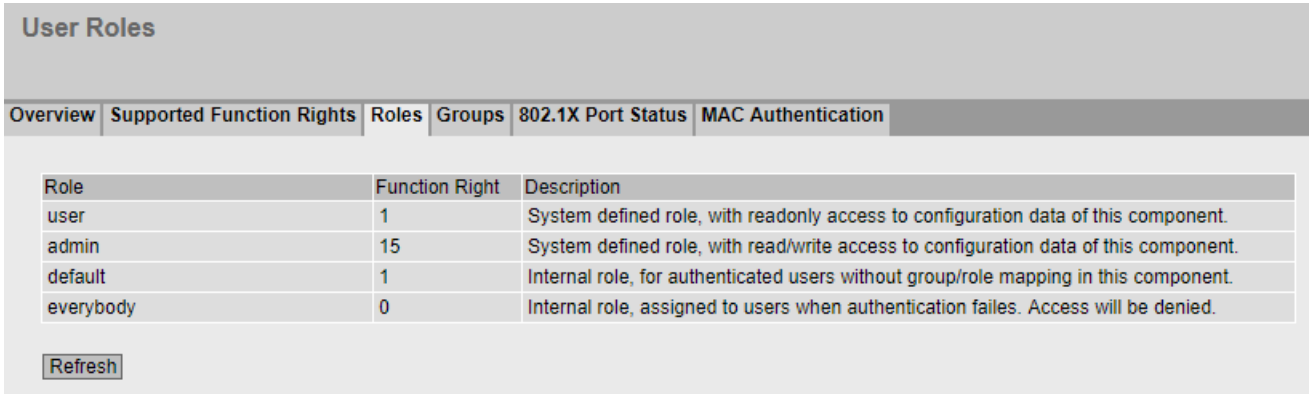
- **Function Right**
  显示功能权限的编号。将与设备参数相关的不同权限分配给不同的编号。
- **Description**
  显示功能权限的说明。

6.3.18.3 角色

说明

所显示的值取决于登录用户的角色。

此页面显示在设备上本地有效的角色。



说明

该表包含以下列：

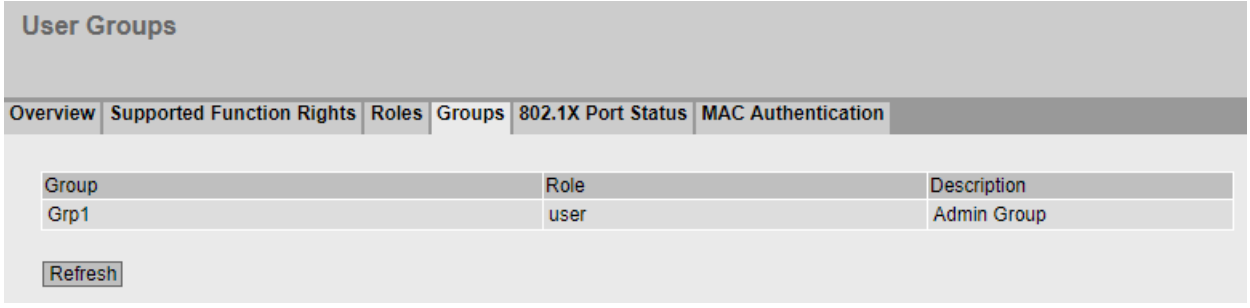
- **Role**
  显示角色的名称。
- **Function Right**
  显示角色的功能权限：
  - 1
    拥有此角色的用户可读取设备参数，但不可更改这些参数。
  - 15
    拥有此角色的用户既可读取也可更改设备参数。
  - 0
    该角色是在无法对用户进行身份验证时设备在内部分配的角色。用户被拒绝访问设备。
- **Description**
  显示角色的说明。

6.3.18.4 组

说明

所显示的值取决于登录用户的角色。

该页面显示了组与角色之间的对应关系。组在 RADIUS 服务器上定义。角色在设备本地定义。



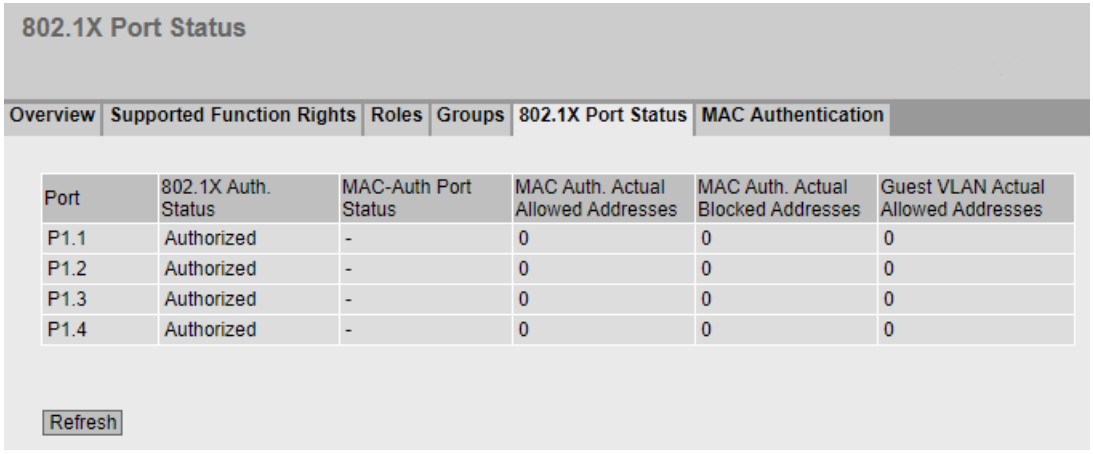
显示值说明

该表包括以下列：

- **Group**
  显示组的名称。名称与 RADIUS 服务器上的组相匹配。
- **Role**
  显示角色的名称。通过 RADIUS 服务器上所链接的组进行身份验证的用户会在设备本地获得此角色的权限。
- **Description**
  显示链接的说明。

6.3.18.5 802.1X 端口状态

此页面显示各端口的 802.1X 身份验证以及 MAC 身份验证的状态。



说明

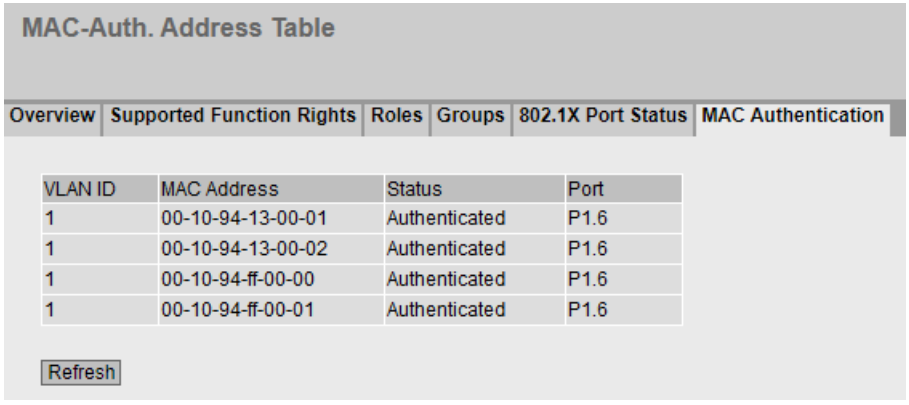
该表格包括以下列：

- **Port**
  设备的所有端口均显示在此列中。
- **802.1X Auth.Status**
  节点的身份验证状态。可用选项如下：
  - Authorized
    通过“802.1X”方法成功进行身份验证后，可通过该端口进行数据通信。
  - Unauthorized
    由于尚未通过“802.1X”方法进行身份验证，或身份验证方法不成功，无法通过端口进行数据通信。

- **MAC Auth.Port Status**
  显示端口 MAC 验证的状态。可用选项如下：
  - -
    已禁用端口的 MAC 验证。
  - Individual
    为端口组态了 MAC 验证。可使用相应的 MAC 地址单独验证客户端。
  - Blocked
    为端口组态了 MAC 验证。客户端未单独验证。验证的第一个客户端可打开所有客户端的端口。尚未验证客户端。
  - open
    为端口组态了 MAC 验证。客户端未单独验证。验证的第一个客户端可打开所有客户端的端口。成功验证客户端后，端口已打开。
  - Sticky
    为端口组态了 MAC 验证。
    如果端口上的新 MAC 地址请求数与端口上当前验证的 MAC 地址数 < 允许的最大 MAC 地址数，则请求自动成功。
    如果端口上的新 MAC 地址请求数与端口上当前验证的 MAC 地址数 ≥ 允许的最大 MAC 地址数，则请求自动失败。
- **MAC Auth.Actual Allowed Addresses**
  显示成功进行 MAC 身份验证后允许访问的节点数。
- **MAC Auth.Actual Blocked Addresses**
  显示 MAC 身份验证失败后允许访问的节点数。
- **Guest VLAN Actual Allowed Addresses**
  显示通过“访客 VLAN”功能允许访问的节点数。

6.3.18.6 MAC 身份验证地址表 (MAC Authentication Address Table)

此页面显示执行了 MAC 身份验证的 MAC 地址。



说明

该表格包括以下列：

- **VLAN ID**
  显示分配给此 MAC 地址的 VLAN ID。
- **MAC 地址 (MAC Address)**
  显示身份验证状态已显示的节点的 MAC 地址。
- **状态 (Status)**
  节点的身份验证状态。可能的选项如下：
  - **已授权 (Authorized)**
    使用“MAC 身份验证”方法成功进行身份验证后，可通过该端口进行数据通信。
  - **未授权 (Unauthorized)**
    由于尚未使用“MAC 身份验证”方法进行身份验证，或身份验证方法不成功，无法通过该端口进行数据通信。
- **端口 (Port)**
  显示访问指定地址的节点时所使用的端口。

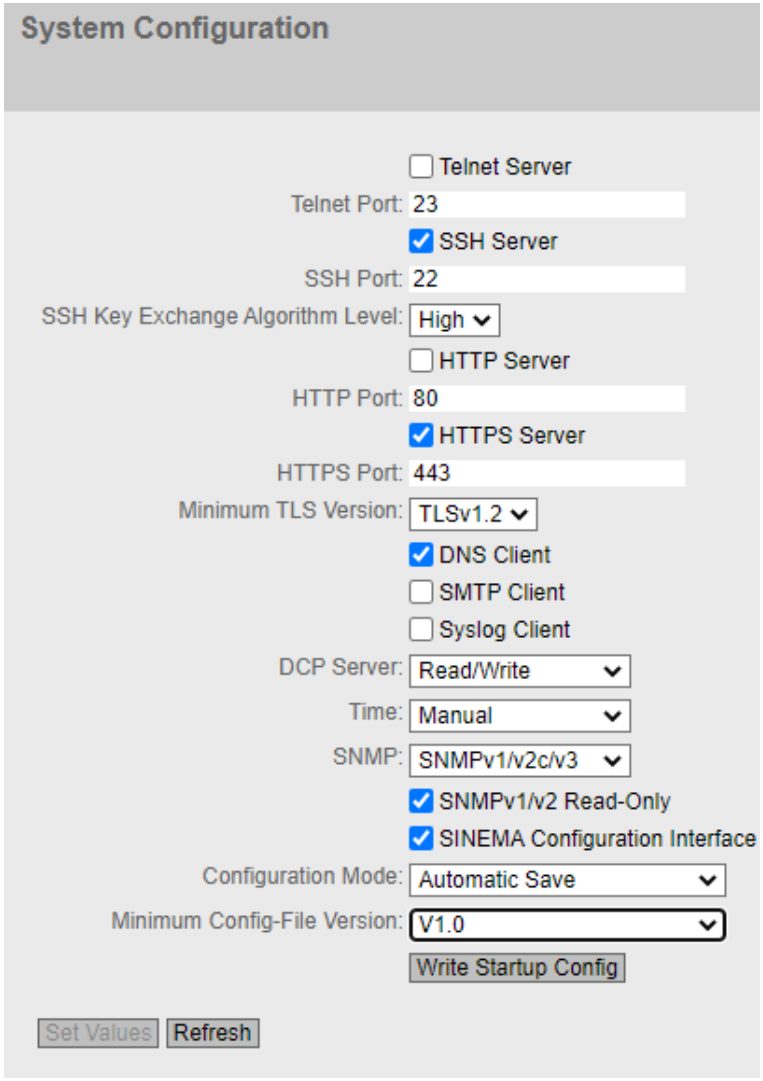
6.4 “System”菜单

6.4.1 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。



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，以便不加密访问 CLI。
- **Telnet 端口 (Telnet Port)**
  标准端口 23 为默认端口。可以选择输入 1024 ... 49151 或 49500 ... 65535 范围内的端口号。
- **SSH 服务器 (SSH Server)**
  启用或禁用“SSH 服务器”(SSH Server) 服务，以便加密访问 CLI。

- **SSH 端口 (SSH Port)**
  标准端口 22 为默认端口。可以选择输入 1024 ... 49151 或 49500 ... 65535 范围内的端口号。

- **SSH 密钥交换算法级别**
  从下拉列表中选择 SSH 密钥交换算法的级别。可能的设置是“低”(Low) 和“高”(High)。两种级别包含以下加密算法：
  - 低 (Low)
    Curve25519-sha256
    Curve25519-sha256@libssh.org
    Ecdh-sha2-nistp256
    Ecdh-sha2-nistp384
    Ecdh-sha2-nistp521
    Diffie-hellman-group16-sha512
    Diffie-hellman-group18-sha512
    Diffie-hellman-group14-sha256
    Diffie-hellman-group14-sha1
  - 高 (High)
    Curve25519-sha256
    Curve25519-sha256@libssh.org
    Ecdh-sha2-nistp256
    Ecdh-sha2-nistp384
    Ecdh-sha2-nistp521

  说明

  如果在连接到 SSH 客户端 (TeraTerm, PuTTY, STS) 时遇到问题，则当级别设置为“高”(High) 时，可能的原因是 SSH 客户端不支持设置为“高”(High) 时的交换算法。请务必使用最新版的 SSH 客户端。

- **HTTP 服务器 (HTTP Server)**
  启用或禁用“HTTP 服务器”服务，以对 WBM 进行未加密的访问。

- **HTTP 端口 (HTTP Port)**
  标准端口 80 为默认端口。可以选择输入 1024 ... 49151 或 49500 ... 65535 范围内的端口号。

- **HTTPS 服务器 (HTTPS Server)**
  启用 HTTPS 服务器服务，以对 WBM 进行加密的访问。

- **HTTPS 端口 (HTTPS Port)**
  标准端口 443 为默认端口。可以选择输入 1024 ... 49151 或 49500 ... 65535 范围内的端口号。

- **“最低 TLS 版本”(Min. TLS version)**
  从下拉列表中选择要用于加密的最低 TLS 版本。无法与不支持所需 TLS 版本的设备进行通信。
- **DNS 客户端 (DNS Client)**
  根据是否将工业以太网交换机用作 DNS 客户端来启用或禁用。可以在“System > DNS”中组态其它设置。
- **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)**
  指定是否可通过 DCP (Discovery and Configuration Protocol) 访问设备：
  - “-”（禁用）
    禁用 DCP。既不能读取也不能修改设备参数。
  - 读/写 (Read/write)
    通过 DCP，既可读取也可修改设备参数。
  - 只读 (Read-Only)
    通过 DCP，可读取但不能修改设备参数。
  - 读取/设置 (Read/Setup)
    只要管理员的默认密码未更改，便可通过 DCP 读取和更改设备参数。一旦默认密码更改，则不能通过 DCP 更改设备参数。

- **时间 (Time)**
  从下拉列表中选择设置。可进行以下设置：
  - 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 服务器设置系统时间。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 (SNTP Client)
    通过 NTP 服务器设置系统时间。可以在“System > System Time > NTP Client”中组态其它设置。
  - PTP 客户端 (PTP Client)（仅适用于支持 PTP 的设备）
    通过 PTP 设置系统时间。可以在“系统 > 系统时间 > PTP 客户端”(System > System time > PTP client) 中组态其它设置。
- **SNMP**
  从下拉列表中选择协议。可进行以下设置：
  - “-”（禁用 SNMP）
    无法使用 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。
- **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。

- **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.按下‘写入启动组态’可立即保存”(Changes will be saved automatically in x seconds. Press 'Write Startup Config' to save 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，显示区就仍会显示消息“试用模式已激活 - 请按‘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。

    说明

    设备的 PROFINET IO 功能在“Trial”组态模式下关闭。然后设备不再响应 PROFINET 请求。因此，控制器不会从设备接收任何 PROFINET 信息。

    在“Trial”组态模式中，SINEC NMS 或 SINEMA 服务器不能通过 PROFINET 协议监控设备。

- **最低组态文件版本 (Minimum Config-File Version)**
  指定必须将组态文件下载到设备中的最低版本。
  这些版本在文件头的签名上有所不同。2.0 版本的组态文件具有更好的防窜改保护功能。
  组态文件的保存与此设置无关。使用 V4.3 及以下固件版本保存的组态文件始终等同于 V1.0。使用 V4.4 及以上固件版本保存的组态文件始终等同于 V2.0。
  - V1.0
    使用此设置，可以将组态文件 V1.0 和 V2.0 一起下载到设备。
  - V2.0
    使用此设置，仅可以将组态文件 V2.0 下载到设备。

组态步骤

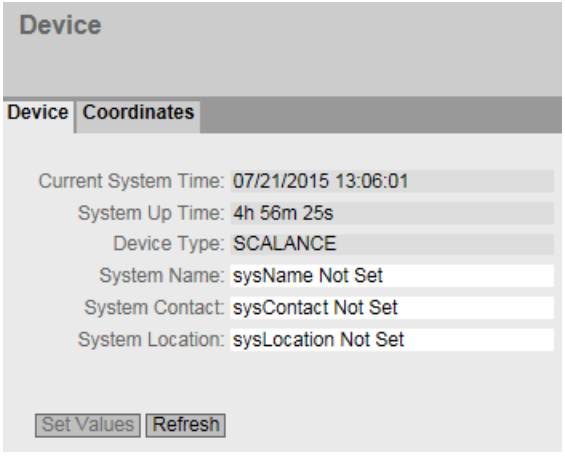
1. 要使用所需功能，请选中相应的复选框。
2. 从下拉列表中选择所需选项。
3. 单击“设置值”(Set Values) 按钮。

6.4.2 常规 (General)

6.4.2.1 设备 (Device)

常规设备信息

该页面包含常规设备信息。



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**
  可在此框中输入设备的名称。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。
- **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。

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“设置值”(Set Values) 按钮。

6.4.2.2 坐标 (Coordinates)

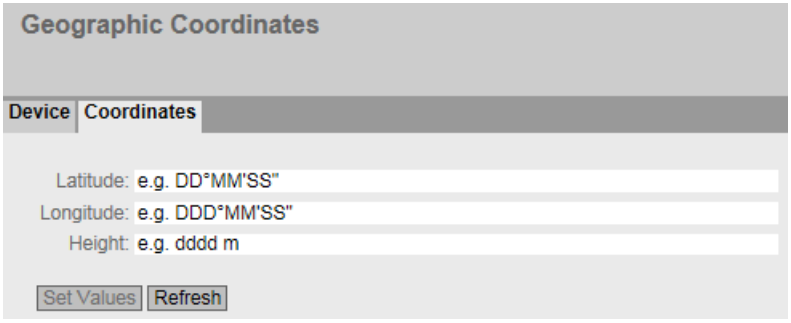
有关地理坐标的信息

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。这些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。



说明

该页包含以下输入框，这些输入框最多可包含 32 个字符。

- **“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° 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° 1´31.67" 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° 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° 20´58.73" 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。

6.4.3 代理 IP (Agent IP)

在此处为设备指定 IP 组态。

对于具有多个 IP 接口的设备，此调用引用“第 3 层”(Layer 3) 菜单中的“子网 > 组态”(Subnets > Configuration) 菜单项以及其中的 TIA 接口组态。

6.4.4 DNS

6.4.4.1 DNS 客户端 (DNS Client)

DNS (Domain Name System) 服务器可为域名分配唯一 IP 地址，以便唯一标识设备。

在此页面上，可通过 IPv4 或 IPv6 地址手动组态最多三个 DNS 服务器。为手动组态的 DNS 服务器分配索引 1 到 3。设备可通过 DHCP 学习两个具有 IPv4 地址的 DNS 服务器。此外，还可以学习另外两个具有 IPv6 地址的 DNS 服务器。对已学习的 DNS 服务器自动分配索引 4 到 7。

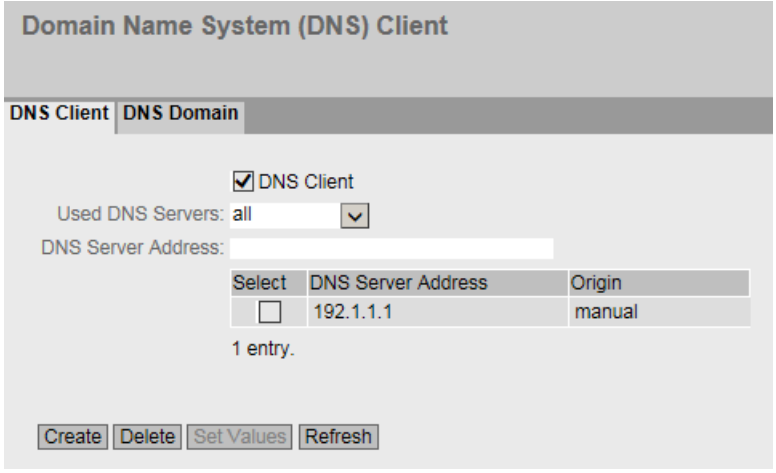
如果有多个 DNS 服务器，则表中的顺序可以指定服务器的查询顺序。最上面的服务器最先查询。设备上最多可组态七个 DNS 服务器。手动组态的 DNS 服务器优先级较高。

如果启用此功能，设备可以作为 DNS 客户端与 DNS 服务器通信。IP 地址对话框中有输入名称的选项。

说明

只有在网络中存在 DNS 服务器时才能使用“DNS 客户端”功能。

说明



该页面包含以下框：

- **DNS 客户端 (DNS Client)**
  根据是否将设备用作 DNS 客户端来启用或禁用。
- **使用的 DNS 服务器 (Used DNS Servers)**
  在此指定设备使用的 DNS 服务器：
  - learned only
    设备仅使用 DHCP 分配的 DNS 服务器。
  - manual only
    设备仅使用手动组态的 DNS 服务器。最多可组态三个 DNS 服务器。
  - all
    设备使用所有可用的 DNS 服务器。
- **DNS 服务器地址 (DNS Server Address)**
  输入 DNS 服务器的 IP 地址。

该表包含以下列：

- **选择 (Select)**
  选中要删除的行中的复选框。
- **DNS 服务器地址 (DNS Server Address)**
  显示 DNS 服务器的 IP 地址。
- **来源 (Origin)**
  该列用于显示 DNS 服务器为手动组态还是由 DHCP 分配。

步骤

激活 DNS

1. 选中“DNS-Client”复选框。
2. 单击“设置值”(Set Values) 按钮。

创建 DNS 服务

1. 在“DNS 服务器地址”(DNS Server Address) 框中，输入 DNS 服务器的 IP 地址。
2. 单击“创建”(Create) 按钮。

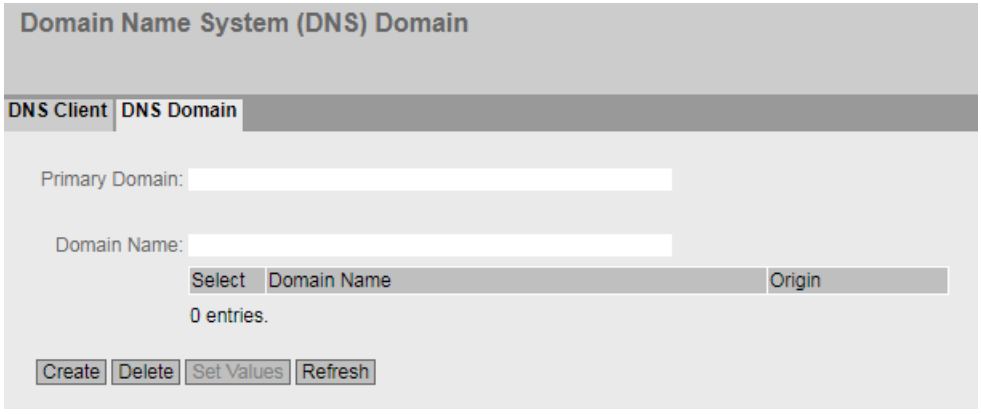
过滤 DNS 服务器

1. 在“已使用的 DNS 服务器”(Used DNS Servers) 下拉列表中，选择要使用的 DNS 服务器。
2. 单击“设置值”(Set Values) 按钮。

6.4.4.2 DNS 域

在此页面上，可以手动定义最多四个域名。首先使用主域名来解析主机名称。

可在此页面上识别或手动组态域名 2 到 4。如果有多个 DNS 服务器，则表中的顺序可以指定域名的使用顺序。



说明

该页面包含以下框：

- **主域 (Primary Domain)**
  输入主域的名称。首先使用该条目来解析主机名称。
- **域名 (Domain Name)**
  输入其它域的名称。

该表包含以下列：

- **选择 (Select)**
  选中要删除的行中的复选框。
- **域名 (Domain Name)**
  显示其它域的名称。
- **来源 (Origin)**
  显示域名为手动组态还是由 DHCP 分配。

步骤

指定主域名

1. 在“主域名”(Primary Domain) 字段中，输入主域的名称。
2. 单击“设置值”(Set Values) 按钮。

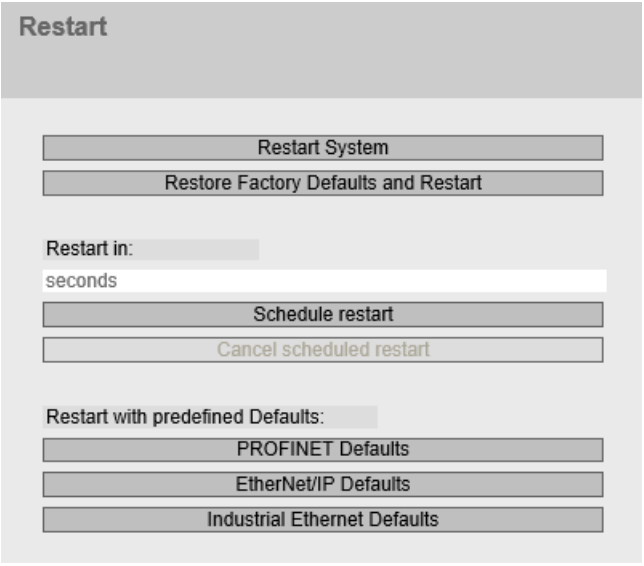
指定其他域名

1. 在“域名”(Domain Name) 字段中，输入其他域的名称。
2. 单击“创建”(Create) 按钮。

6.4.5 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

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“Set values”按钮后才会在设备上生效。
- 如果设备在“Automatic Save”模式下，会在设备重启之前自动保存最后的更改。

恢复出厂默认设置

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，设备只能通过串行接口、SINEC PNI 或 DHCP 寻址。

注意
根据具体连接，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。与复位为出厂默认设置不同，用户和密码在重启后保持不变。组态的 IP 地址丢失，因此之后只能通过串行接口、SINEC PNI 或使用 DHCP 访问设备。

注意
根据具体连接，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。

为重启设备，该页面上的按钮提供了以下选项：

- **Restart System**
  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。
- **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。出厂设置取决于设备。

- **Restart in:**
  在此处指定经过多少秒后设备重启。当“Automatic Save”组态模式激活时，会显示一个附加对话框。在此对话框中，可以指定设备是否应保存当前组态并切换到“Trial”模式。在任何情况下，设备都会在经过指定的时间后重新启动。
- **Schedule restart**
  单击该按钮时，定时器将启动并倒计时定义的时间。定时器过期后，设备将重新启动。
- **Cancel scheduled restart**
  使用此按钮可以禁用计划重启的定时器。

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 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 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。
- **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。

6.4.6 加载和保存

文件类型概述

文件类型表包含以下区域。

区域	文件类型	说明	下载	保存	删除 1)
更新 (Update)	Firmware	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。	X	X	--

区域	文件类型	说明	下载	保存	删除 [1)]
组态 (Configuration)	Config	此文件包含启动组态。 此外，该文件还包含用户、角色、组和功能权限的相关定义。密码存储在“Users”文件中。	X	X	--
	ConfigPack	详细组态信息。例如，启动组态、用户、证书、收藏夹和设备固件（如果已保存）。	X	X	--
	LoginWelcomeMessage	txt 文件包含所需的文本或 ASCII 类型。仅支持 ASCII 格式的纯文本文件。	X	X	X
	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。密码在此文件中的隐藏方式如下：[PASSWORD] 可下载此文本文件。如果此文件未更改，则不会再次上传。	--	X	--
	RunningSINEMAConfig	将当前设备组态保存为此文件类型，以便传送到 STEP 7 Basic/Professional。该文件可导入 STEP 7 Basic/Professional 并可安装在具有相同订货号和固件版本的设备上。 在可保存文件之前，必须在 WBM 中的“System > Load&Save > Passwords”下为“RunningSINEMAConfig”分配一个密码。另外，还需要该密码以将文件导入 STEP 7 Basic/Professional。 另请参见“SINEMAConfig”	--	X	--
	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。 用于保存和加载文件的 CLI 命令不能使用 CLI 脚本文件来执行。	X	--	--
	SINEMAConfig	加载通过 STEP 7 Basic/Professional 导出的组态数据，以使用该文件类型传送到 WBM。 要加载文件，必须在“System > Load&Save > Passwords”下为“SINEMAConfig”分配一个密码。另外，还需要该密码以将文件从 STEP 7 Basic/Professional 导出。 另请参见“RunningSINEMAConfig”	X	--	--
	Users	带有用户名和密码的文件	X	X	--

区域	文件类型	说明	下载	保存	删除 [1)]
	WBMFav	WBM 收藏夹 此文件包含在 WBM 中创建的收藏夹。可以下载该文件并将其上传至其它设备。	X	X	X
证书和密钥 (Certificate & Key)	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。 可将以下文件类型加载至设备中。 • .pem 要将具有此数据类型的 HTTPS 证书成功下载到设备中，该证书必须包含未加密的私钥。 • .p12 对于具有此文件类型的 HTTPS 证书，私钥已加密并受到密码保护。 要将这些证书成功加载至设备，请在“密码 (页 188)”(Passwords) WBM 页面中输入为该文件指定的密码。 **建议使用 PKCS#12 格式的受密码保护的证书。** 支持的证书如下： • 通过 secp521r1 (NIST P-521) 创建的 ECDSA 证书 • 最大密钥长度为 4096 位的 RSA 证书	X	X	X
	SSHPrivateKey ECDSA	SSH 私钥 (ECDSA) 支持 SSH 密钥 ecdsa-sha2-nistp521。 有些文件的访问受密码保护。要将这些文件成功加载至设备，请在“密码” (页 188)(Passwords) WBM 页面中输入为该文件指定的密码。	X	X	X
	SSHPrivateKey RSA	带和不带密码的 SSH 私钥 (RSA) 支持以下 SSH 密钥： • rsa-sha2-512 • rsa-sha2-256 有些文件的访问受密码保护。要将这些文件成功加载至设备，请在“密码” (页 188)(Passwords) WBM 页面中输入为该文件指定的密码。	X	X	X

区域	文件类型	说明	下载	保存	删除 [1]
服务和日志 (Service & Log)	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。	--	X	X
	DebugExt	此文件包含有关西门子支持的更多详细信息。 它已被加密，可通过电子邮件发送给西门子支持且不会带来安全风险。保存文件可能需要一些时间。	--	X	--
	LogFile	带有事件日志表中条目的文件	--	X	--
	StartupInfo	启动日志文件 该文件包含上次启动时已在日志文件中输入的消息。	--	X	--
信息 (Information)	EDS	电子数据表 (EDS) 电子数据表用于描述 EtherNet/IP 模式下的设备	--	X	--
	GSDML	有关设备属性的 PROFINET 信息	--	X	--
	MIB	专有 MSPS MIB 文件“Scalance_m_msps.mib”	--	X	--

[1] 仅可通过 HTTP/HTTPS 删除。

6.4.6.1 HTTP

通过 HTTP 加载和保存数据

WBM 使您可以将设备数据存储在客户端 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，但更改不会保存至组态文件（ConfigPack 和 Config）。在 “System > Configuration”WBM 页面中使用“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。

通过 STEP 7 Basic/Professional 使用文件交换组态数据

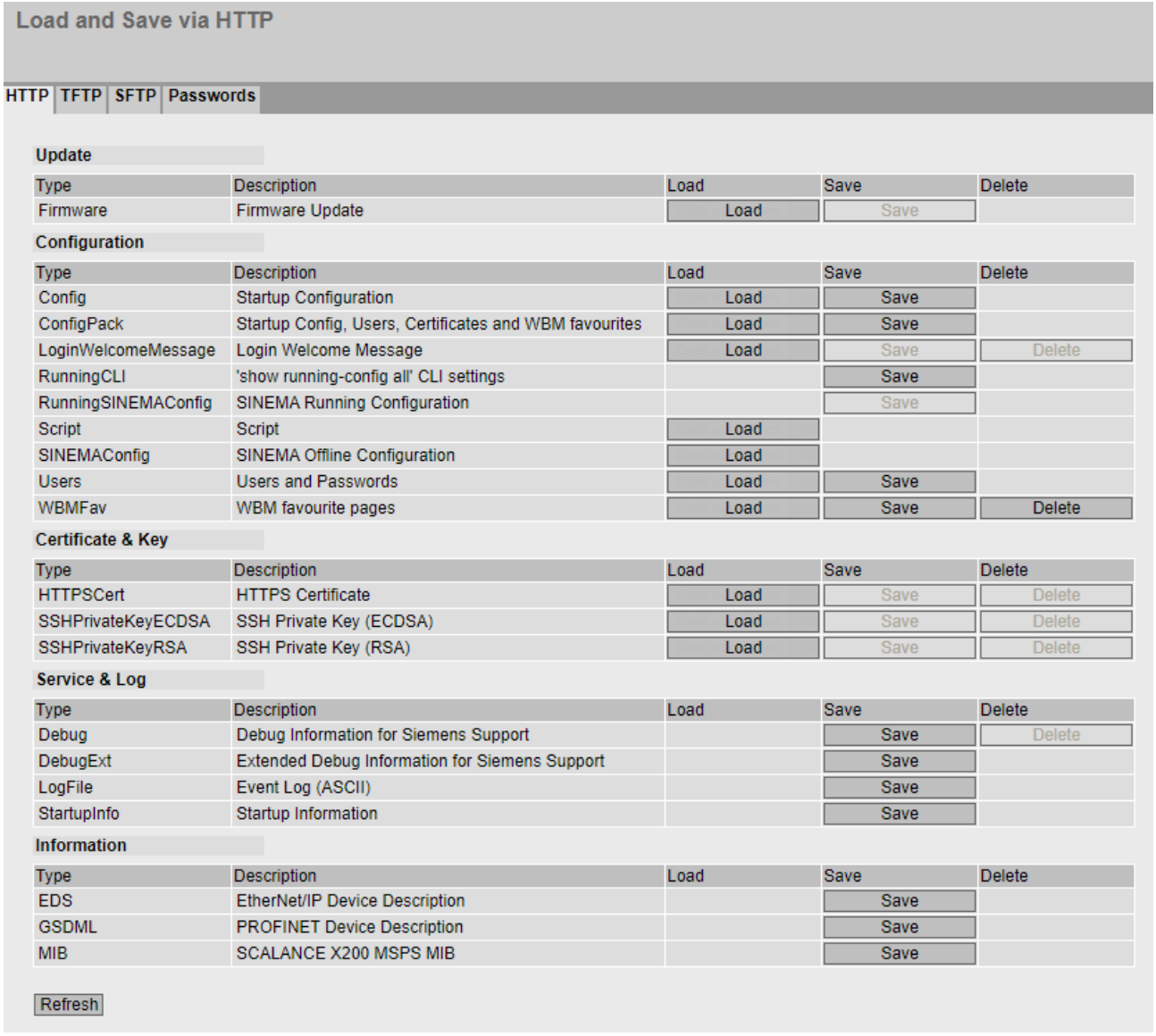
使用两种文件类型“RunningSINEMAConfig”和“SINEMAConfig”通过文件在设备 (WBM) 和 STEP 7 Basic/Professional 之间交换组态数据。

要求：

- 订货号相同
- 固件版本相同
- 密码
  可在 WBM 中的“系统 > 加载和保存 > 密码”(System > Load&Save > Passwords) 下分配密码。

可以使用以下文件类型：

- 对于离线诊断
  可通过 WBM 将故障组态保存为“RunningSINEMAConfig”，并将其导入 STEP 7 Basic/Professional。在 STEP 7 Basic/Professional 中诊断时无需连接到实际设备。可导出正确组态，并通过 WBM 再次将其加载为“SINEMAConfig”。
- 对于组态
  在 STEP 7 Basic/Professional 中组态设备时无需连接到实际设备。可导出组态，并通过 WBM 将其作为“SINEMAConfig”加载至实际设备。



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。
- **下载 (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。
- **删除 (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 上传数据

1. 单击“下载”(Load) 按钮之一启动上传功能。
   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“OK”按钮运行重新启动。如果单击“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 上传数据

1. 单击“保存”(Save) 按钮之一启动下载操作。
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 删除数据

1. 单击“删除”(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. 按这种方式将这些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。

6.4.6.2 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。

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，但更改不会保存至组态文件（ConfigPack 和 Config）。在“System > Configuration”WBM 页面中使用“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。

通过 STEP 7 Basic/Professional 使用文件交换组态数据

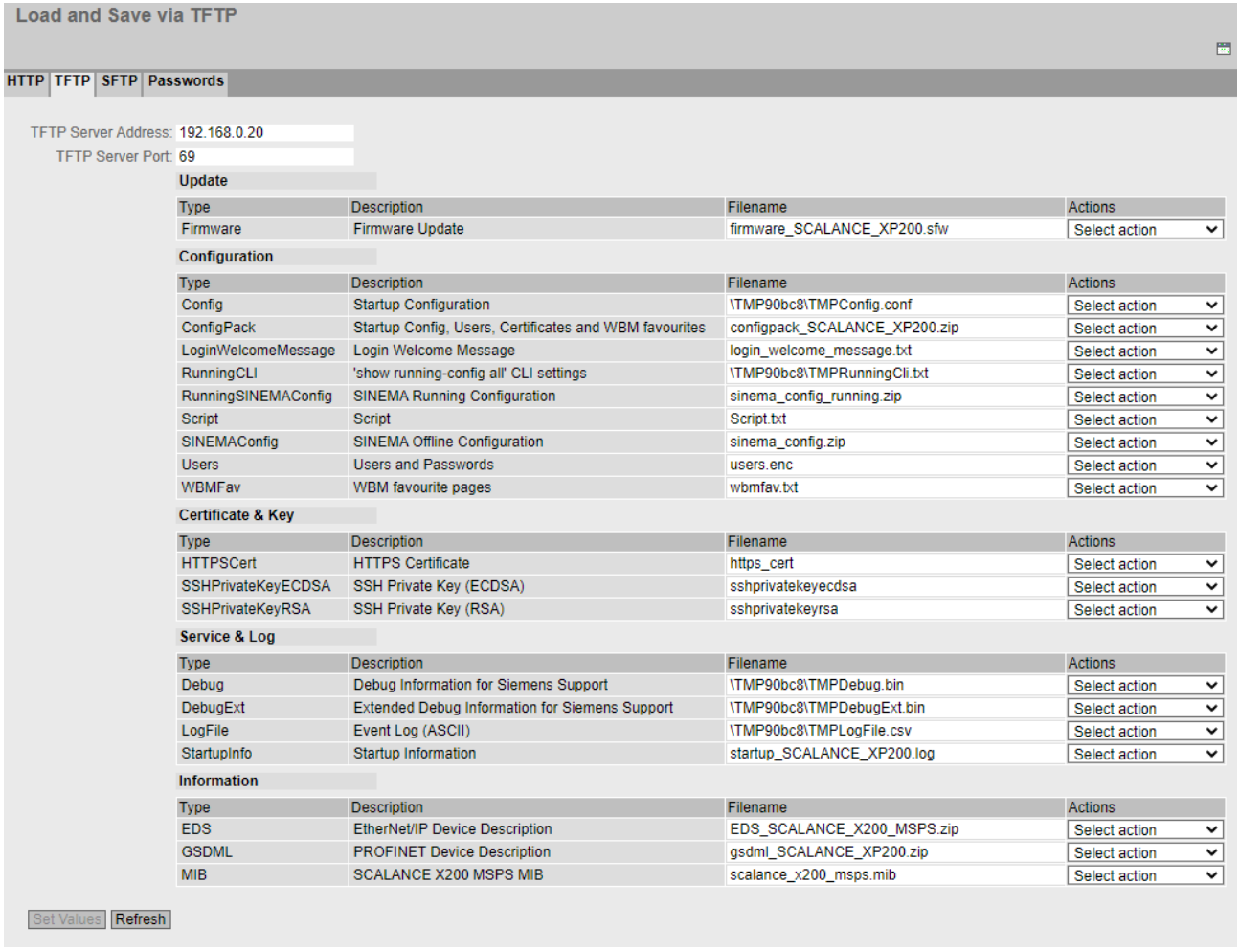
使用两种文件类型“RunningSINEMAConfig”和“SINEMAConfig”通过文件在设备 (WBM) 和 STEP 7 Basic/Professional 之间交换组态数据。

要求：

- 订货号相同
- 固件版本相同
- 密码
  可在 WBM 中的“系统 > 加载和保存 > 密码”(System > Load&Save > Passwords) 下分配密码。

可以使用以下文件类型：

- 对于离线诊断
  可通过 WBM 将故障组态保存为“RunningSINEMAConfig”，并将其导入 STEP 7 Basic/Professional。在 STEP 7 Basic/Professional 中诊断时无需连接到实际设备。可导出正确组态，并通过 WBM 再次将其加载为“SINEMAConfig”。
- 对于组态
  在 STEP 7 Basic/Professional 中组态设备时无需连接到实际设备。可导出组态，并通过 WBM 将其作为“SINEMAConfig”加载至实际设备。



显示框说明

该页面包含以下框：

- **TFTP 服务器地址 (TFTP Server Address)**
  输入用于交换数据的 TFTP 服务器的 IP 地址或 FQDN。
- **TFTP 服务器端口 (TFTP Server Port)**
  输入用于处理数据交换的 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 (Action)**
  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。
  - **下载文件 (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 服务器的端口。
3. 如果适用，在“文件名”(Filename) 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“OK”按钮运行重新启动。如果单击“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. 按这种方式将这些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。

6.4.6.3 SFTP

通过 SFTP 服务器加载和保存数据

SFTP (SSH File Transfer Protocol) 传输加密文件。在此页面中组态 SFTP 服务器的访问数据。

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

在此页面上，还可以加载建立安全 VPN 连接所需的证书。

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。

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，但更改不会保存至组态文件（ConfigPack 和 Config）。在“System > Configuration”WBM 页面中使用“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。
用于保存和加载文件的 CLI 命令不能使用 CLI 脚本文件 (Script) 来执行。

通过 STEP 7 Basic/Professional 使用文件交换组态数据

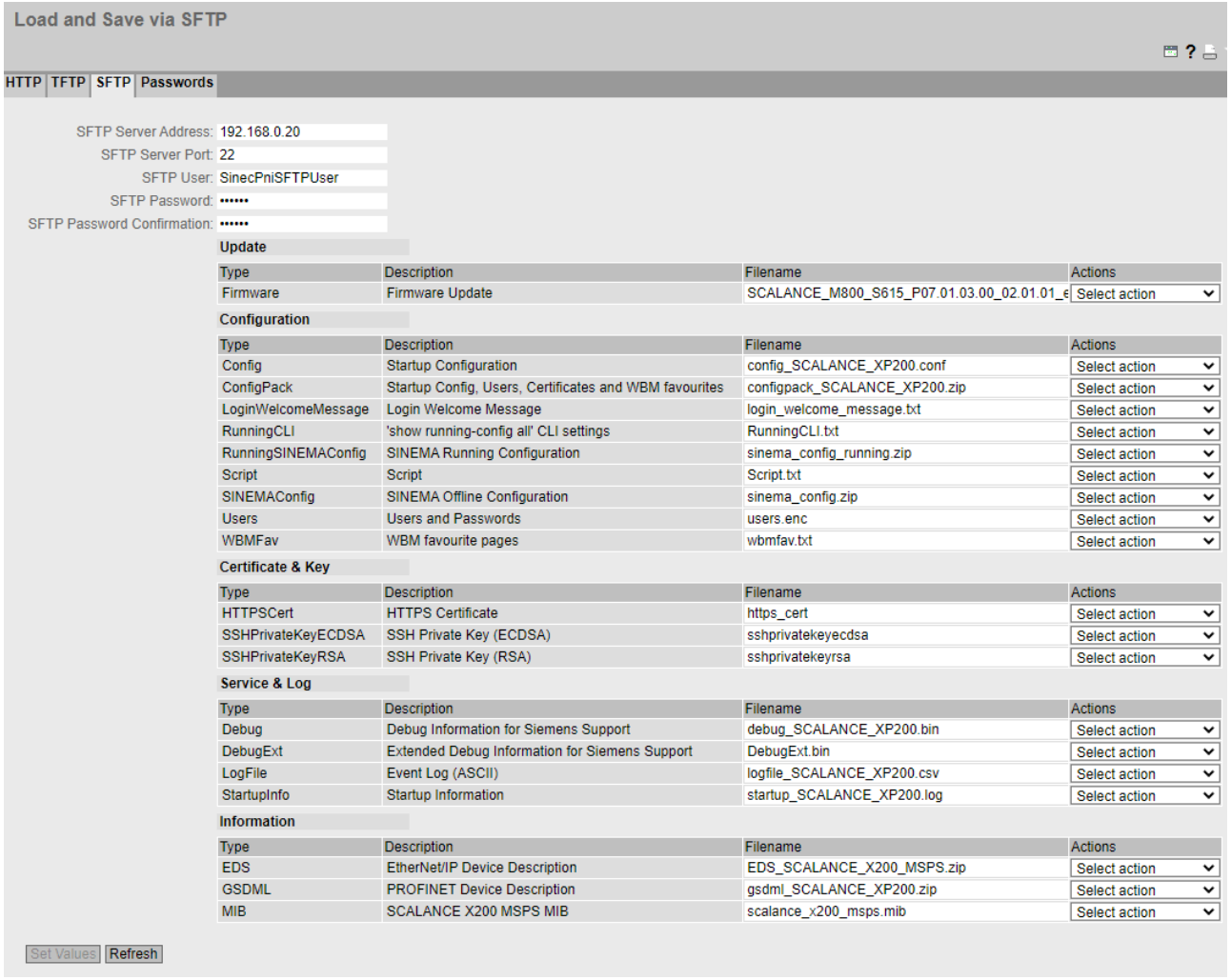
使用两种文件类型“RunningSINEMAConfig”和“SINEMAConfig”通过文件在设备 (WBM) 和 STEP 7 Basic/Professional 之间交换组态数据。

要求：

- 订货号相同
- 固件版本相同
- 密码
  可在 WBM 中的“系统 > 加载和保存 > 密码”(System > Load&Save > Passwords) 下分配密码。

可以使用以下文件类型：

- 对于离线诊断
  可通过 WBM 将故障组态保存为“RunningSINEMAConfig”，并将其导入 STEP 7 Basic/Professional。在 STEP 7 Basic/Professional 中诊断时无需连接到实际设备。可导出正确组态，并通过 WBM 再次将其加载为“SINEMAConfig”。
- 对于组态
  在 STEP 7 Basic/Professional 中组态设备时无需连接到实际设备。可导出组态，并通过 WBM 将其作为“SINEMAConfig”加载至实际设备。



说明

该页面包含以下框：

- **SFTP 服务器地址 (SFTP Server Address)**
  输入要与其交换数据的 SFTP 服务器的 IP 地址或 FQDN。
- **SFTP 服务器端口 (SFTP Server Port)**
  输入 SFTP 服务器要用于交换数据的端口。如有必要，可以将默认值 22 更改为适合您需要的值。
- **SFTP 用户 (SFTP User)**
  输入要访问 SFTP 服务器的用户。这里假设已在 SFTP 服务器中创建具有相应权限的用户。
- **SFTP 密码 (SFTP Password)**
  输入用户的密码。
- **SFTP 密码确认 (SFTP Password Confirmation)**
  确认密码。

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 (Action)**
  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 SFTP 服务器上。
  - **下载文件 (Load file)**
    通过该选项加载 SFTP 服务器中的文件。

步骤

通过 SFTP 加载或保存数据

1. 在“SFTP 服务器地址”(SFTP Server Address) 中输入 SFTP 服务器地址。
2. 在“SFTP 服务器端口”(SFTP Server Port) 中输入要使用的 SFTP 服务器端口。
3. 输入访问 SFTP 服务器所需的用户数据（用户名和密码）。
4. 如果适用，在“文件名”(Filename) 中输入要保存数据或从中获取数据的文件的名称。

说明

访问受密码保护的文件

为了能够在设备上成功加载这些文件，需要在“系统 > 加载和保存 > 密码”(System > Load&Save > Passwords) 中输入为文件指定的密码。

5. 从“操作”(Actions) 下拉列表中选择要执行的操作。
6. 单击“设置值”(Set Values) 启动所选操作。
7. 如果需要重启，将输出相应消息。单击“OK”按钮运行重新启动。如果单击“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：

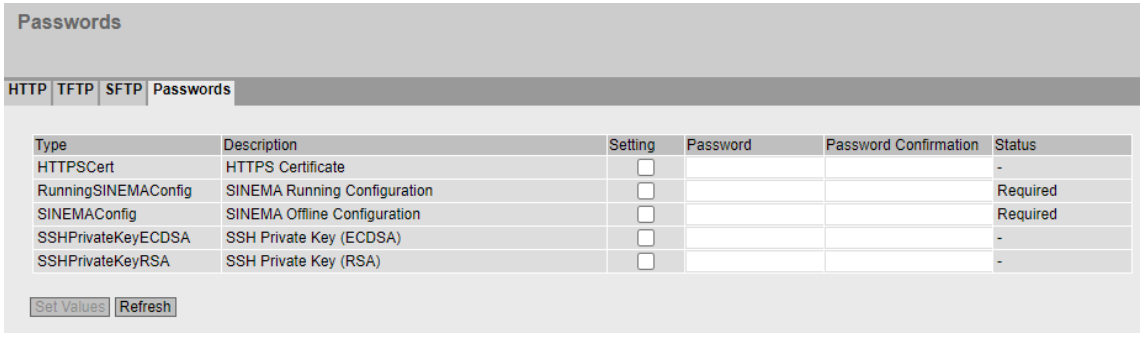
1. 将已组态设备的组态数据保存在 PC 上。
2. 按这种方式将这些组态文件加载到要组态的所有其它设备中。
3. 如果有必要对特定设备进行单独设置，则必须在相关设备上在线进行设置。

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。

6.4.6.4 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。



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。
- **设置 (Setting)**
  启用后，将使用文件。只有在组态了密码的情况下才能启用。
- **密码 (Password)**
  输入文件的密码。
- **密码确认 (Password Confirmation)**
  确认密码。
- **状态 (Status)**
  显示文件的当前设置是否与设备相匹配。
  - 有效 (valid)
    “设置”(Setting) 复选框已选中且密码与文件匹配。
  - 无效 (Invalid)
    “设置”(Setting) 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“设置”(Setting) 复选框。
  - 必选项 (Required)
    需要输入密码才能使用指定的文件类型。未选中“设置”(Setting) 复选框。

步骤

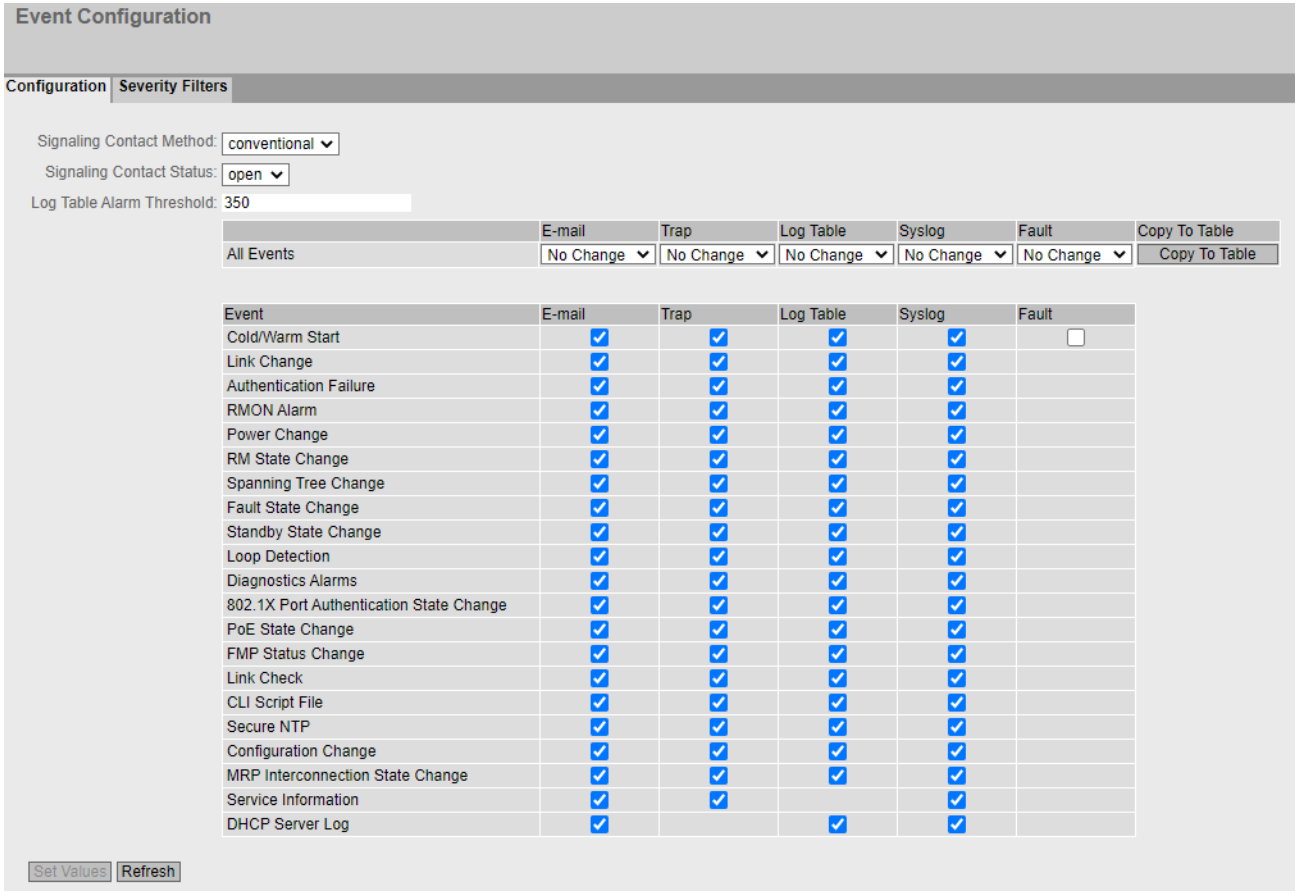
1. 在“Password”中输入密码。
2. 要确认密码，在“Password Confirmation”中再次输入密码。
3. 启用“设置”(Setting) 选项。
4. 单击“设置值”(Set Values) 按钮。

6.4.7 事件

6.4.7.1 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。



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的行为。可能的响应包括：
  - 标准 (Standard)
    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
    信号触点闭合。
  - 断开
    信号触点断开。
- **日志表报警阈值 (Log Table Alarm Threshold)**
  指定生成日志消息的条目数。
  如果接收下一条目将达到指定的限值，则会输出报警消息，例如，如果指定了 300，接收条目 299 后，将输出已达到限值 300 的消息。

利用表 1，可以一次选中或清除表 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”(Fault)**
  启用或禁用所有事件的所需通知类型。如果选中“不变”(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/暖启动 (Cold/Warm Start)
    设备已由用户开启或重启。在设备的故障存储器中生成新条目，其中包含所执行的重启的类型。
  - 链路变化 (Link Change)
    只有在对接口状态进行监视并做出更改时才会发生该事件，请参见“系统 > 故障监视 > 链路变化”。
  - 身份验证失败 (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。
  - 诊断报警 (Diagnostics Alarms)
    诊断值已降至特定限值以下或超出特定限值。
  - 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。
  - PoE 状态变化 (PoE State Change)
    PoE 状态已发生变化。

    说明

    只能在支持 PoE 的设备中组态此事件。

– “FMP 状态变化”(FMP Status Change)
接收功率或功率损耗值已超出特定的限值或已经降到特定限值下。

说明

只能在支持 FMP 的设备中组态此事件。

– 链路检查 (Link Check)
光纤传输链路中检测到中断。

说明

只能在具有光纤接口的设备中组态此事件。

– CLI 脚本文件 (CLI Script File)
在 CLI 脚本文件中检查到错误。
– 安全 NTP (Secure NTP)
使用安全 NTP 时发生错误，例如指定的密钥长度错误。
– “组态更改”(Configuration Change)
组态被保留。
– “MRP 互连状态更改”(MRP Interconnection State Change)
当冗余连接不再可用时将触发此事件。原因可能是主要或次要 MRP 互连连接丢失。
– 服务信息 (Service Information)
对于某些事件（例如有关时间同步的时间消息、密码更改或常规组态更改），即使没有组态，也会在日志表中输入内容。对于这些事件，用户可以在此组态其它后续操作（电子邮件、陷阱、系统日志）。
– DHCP 服务器日志 (DHCP Server Log)
记录 DHCP 事件。前提是设备上启用了 DHCP 服务器。

- **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，该类型才可用。
- **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，请参见“信息 > 日志表”
- **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 (Fault)**
设备触发故障。错误 LED 亮起

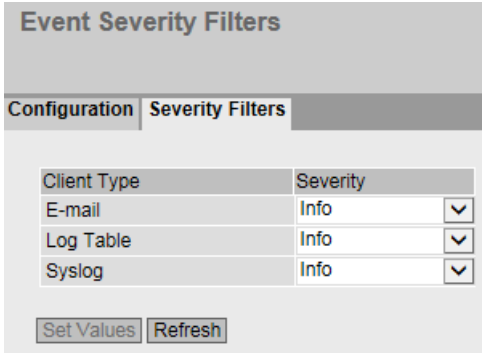
组态步骤

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 (Fault)
2. 单击“设置值”(Set Values) 按钮。

6.4.7.2 严重程度过滤器 (Severity Filters)

设置 Severity Filters

在此页面上组态决定系统事件通知发送方式的严重程度。



说明

该表格包括以下列：

- **Client Type**
  选择要设置的客户端类型：
  - 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。
- **Severity**
  选择所需严重程度。可进行以下设置：
  - **Critical**
    处理严重程度为 Critical 的系统事件。
  - **Warning**
    处理严重程度至少为 Warning 的系统事件：这意味着“Warning”和“Critical”类别的事件。
  - **Info**
    处理严重程度至少为 Info 的系统事件：这意味着“Info”、“Warning”和“Critical”类别的事件。

步骤

按以下步骤组态所需级别：

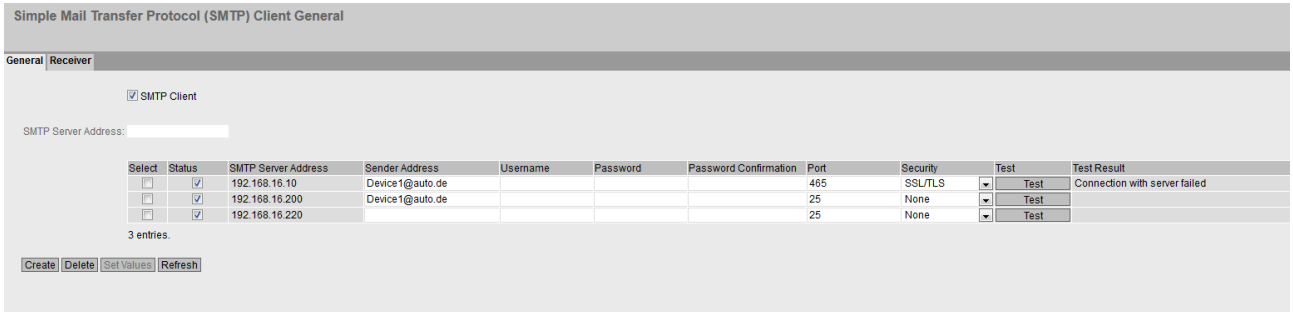
1. 组态客户端类型后，从表格第二列的下拉列表中选择所需值。
2. 单击“Set Values”按钮。

6.4.8 SMTP 客户端

6.4.8.1 常规

通过电子邮件进行网络监视

如果发生事件，设备可自动向维修技工等人员发送电子邮件。该电子邮件包含发送设备的标识、以普通文本描述的原因以及时间戳。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。



发送电子邮件的要求

- 在“系统 >事件 > 组态”(System > Events > Configuration) 中，已针对相关事件激活“电子邮件”(E-mail)。
- 所需严重程度是在“系统 > 事件 > 严重等级”(System > Events > Severity level) 下组态的。
- “系统 > SMTP 客户端 > 接收方”(System > SMTP Client > Receiver) 下至少存在一个条目，且“发送”(Send) 设置已激活。

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。
- **SMTP 服务器地址 (SMTP Server Address)**
  输入 SMTP 服务器的 IP 地址或 FQDN。

该表包含以下列：

- **选择 (Select)**
  选中要删除的行中的复选框。
- **Status**
  指定是否要使用该 SMTP 服务器。
- **SMTP 服务器地址 (SMTP Server Address)**
  显示 SMTP 服务器的 IP 地址。
- **发送方电子邮件地址 (Sender Email Address)**
  输入在电子邮件中指定的发送方电子邮件地址。
- **用户名 (User Name)**
  如有必要，可输入用于在 SMTP 服务器上进行验证的用户名。
- **密码 (Password)**
  如有必要，可输入用于在 SMTP 服务器上进行验证的密码。
- **密码确认 (Password Confirmation)**
  再次输入密码。
- **端口 (Port)**
  输入可用来访问 SMTP 服务器的端口。
  出厂设置：
  – 25（无）
  – 465（SSL/TLS 和 StartTLS）
- **Security**
  指定将电子邮件从设备传送到 SMTP 服务器时是否加密。仅当 SMTP 服务器支持所选设置时才可实现。

  说明

  双因素验证 (2FA)

  不支持双因素验证。

  – SSL/TLS
  – StartTLS
  – 无 (None)：电子邮件以未加密形式传送。
- **测试 (Test)**
  向组态的接收方发送一封测试电子邮件。
- **测试结果 (Test Result)**
  显示电子邮件是否发送成功。如果发送不成功，消息中会包含可能的原因。

步骤

组态 SMTP 服务器

1. 启用“SMTP 客户端”(SMTP Client) 功能。
2. 在“SMTP 服务器地址”(SMTP Server Address) 中输入 SMTP 服务器的 IP 地址。
3. 单击“创建”(Create) 按钮。会在表中生成一个新条目。
4. 为“发送方电子邮件地址”(Sender Email Address) 输入电子邮件中将包含的发送方名称。
5. 如果 SMTP 服务器提示登录，输入用户名和密码。
6. 在“Security”下，指定传送到 SMTP 服务器时是否加密。
7. 启用 SMTP 服务器条目。
8. 单击“设置值”(Set Values) 按钮。

说明

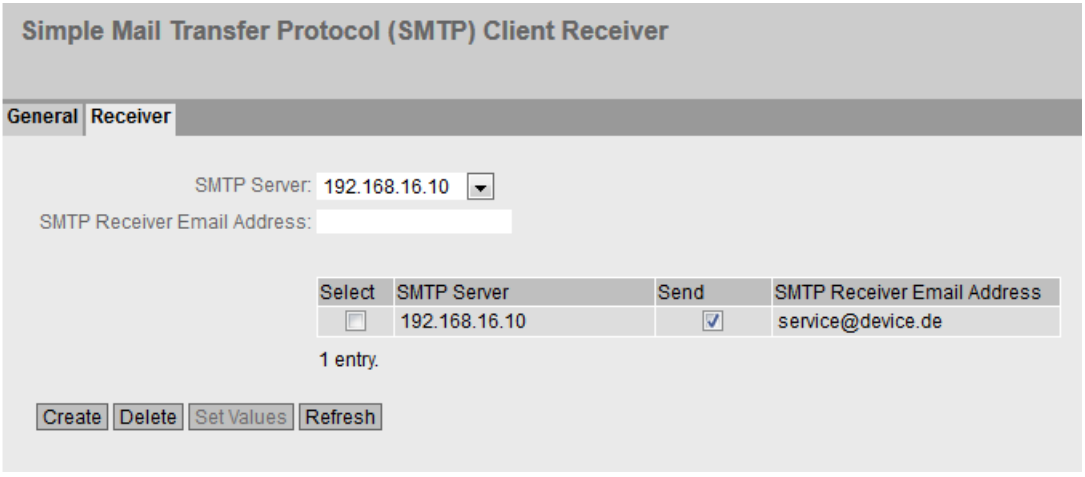
根据 SMTP 服务器特性和组态，可能需要针对电子邮件修改“发送方电子邮件地址”(Sender E-Mail Address) 输入。请与 SMTP 服务器的管理员联系。

测试 SMTP 服务器组态

1. 组态接收方
   - 单击“接收方”(Receiver) 选项卡。
   - 在“SMTP 服务器”(SMTP server) 下选择所需 SMTP 服务器。
   - 在“SMTP 接收方电子邮件地址”(E-mail address of the SMTP recipient) 下输入所需地址。
   - 单击“创建”(Create) 按钮。会在表中生成一个新条目。设置“发送”(Send) 默认启用。
2. 发送测试电子邮件
   - 单击“常规”(General) 选项卡。
   - 单击 SMTP 服务器条目旁的“测试”(Test) 按钮。设备会向每个组态的接收方发送测试电子邮件。
   - 检查测试结果。如果发送不成功，消息中会包含可能的原因。

6.4.8.2 接收人

在此页面上指定发生事件时电子邮件的接收方。



说明

该页面包含以下框：

- **SMTP Server**
  指定发送电子邮件所使用的 SMTP 服务器。
- **Email address of the SMTP receiver**
  输入设备会将电子邮件发送到的电子邮件地址。

该表包含以下列：

- **Select**
  选中要删除的行中的复选框。
- **SMTP Server**
  显示与条目相关的 SMTP 服务器的 IP 地址。
- **Send**
  当启用时，设备将向此接收方发送一封电子邮件。
- **Email address of the SMTP receiver**
  显示电子邮件地址，发生故障时，设备会将电子邮件发送到该地址。

步骤

组态 SMTP 接收方

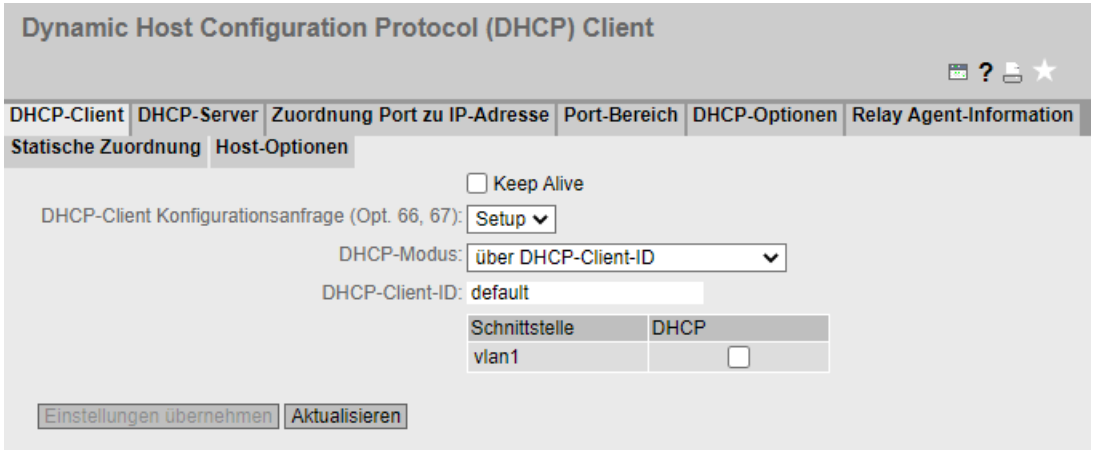
1. 选择所需“SMTP server”。
2. 输入 SMTP 接收方电子邮件地址。
3. 单击“Create”按钮。将在表中生成一个新条目。
4. 激活条目的“Send”选项。
5. 单击“Set Values”按钮。

6.4.9 DHCP

6.4.9.1 DHCP 客户端

设置 DHCP 模式

如果设备组态为 DHCP 客户端，则它将启动 DHCP 请求。作为对请求的回复，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。



说明

该页面包含以下框：

- **保持连接 (Keep Alive)**
  默认情况下保持连接处于启用状态。如果禁用“保持连接”(Keep Alive)，则与 DHCP 服务器的连接断开或租用时间到期时，IP 地址会复位为 0.0.0.0。
  如果启用该功能，则与 DHCP 服务器的连接断开或租用时间到期时，IP 地址会保持连接，而不会复位为 0.0.0.0。
- **DHCP 客户端组态请求（选项 66, 67)**
  启用后，DHCP 客户端使用这些选项从 TFTP 服务器（选项 66）下载组态文件（选项 67）。重新启动后，设备将使用组态文件中的数据。

注意
安全风险 - 未经授权访问和/或滥用的风险 此功能可能用于更改设备的功能，从而导致数据通信故障。有恶意的用户可能会导致设备加载受操纵的组态文件以更改对其有益的组态。 要防止未经授权访问和/或滥用，如果不使用此功能，则将其禁用 (**Off**)。 在具有默认设置 (**Setup**) 的设备中，使用默认用户配置文件 **admin** 和分配的新密码首次登录后，即使选项 66 和 67 仍包含在 DHCP 客户端的 DHCP 请求中，也不会从 DHCP 服务器加载其它组态文件。

  - Setup
    默认设置。该功能取决于设备的状态。
    在交付状态下和复位为默认设置后，该功能的行为与设置 **On** 时相同，并会为所有 DHCP 客户端接口启用此功能。
    以下事件触发设备的状态更改：使用默认用户配置文件 admin 和分配的相关新密码并加载组态文件首次登录。之后，设备处于安全工作状态，该功能的行为与设置 **Off** 选项时相同：已为所有 DHCP 客户端接口禁用此选项。
    状态自动更改。
  - On
    将启用该功能。DHCP 客户端使用下一个 DHCP 请求来请求组态文件。
  - Off
    将禁用该功能。DHCP 客户端不请求组态文件。

- **DHCP 模式 (DHCP Mode)**
  指定 DHCP 客户端登录其 DHCP 服务器所需的标识符类型：
  - 基于 MAC 地址 (via MAC Address)
    默认设置。标识基于 MAC 地址。
  - 基于 DHCP 客户端 ID (via DHCP Client ID)
    基于自由定义的 DHCP 客户端 ID 进行识别。
  - 基于系统名称 (via System Name)
    基于系统名称进行识别。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。
  - 基于站的 PROFINET 名称 (via PROFINET Name of Station)
    标识基于 PROFINET 设备名称运行。
- **DHCP 客户端 ID (DHCP Client ID)**
  如果选择 DHCP 模式“基于 DHCP 客户端 ID”(via DHCP Client ID)，则将出现输入框。输入“DHCP 客户端 ID”(DHCP Client ID)。

该表格包括以下列：

- **接口 (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

请按照以下步骤使用 DHCP 客户端 ID 组态 IP 地址：

1. 在“DHCP 模式”(DHCP Mode) 下拉列表中选择标识方法。
   如果选择 DHCP 模式“基于 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. 如果 DHCP 客户端要使用选项 66 和 67 下载并随后启用某个组态文件，则选择“DHCP 客户端组态请求（选项 66、67）”(DHCP Client Configuration Request (Opt. 66, 67)) 选项。
3. 在表中启用“DHCP”选项。
4. 单击“设置值”(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下载组态文件中的组态不同，则系统将重启。

确保不再在此组态文件中设置选项“DHCP 客户端组态请求（选项 66、67）”(DHCP Client Configuration Request (Opt. 66, 67))。

6.4.9.2 DHCP 服务器 (DHCP Server)

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。

说明

删除 DHCP 服务器绑定。

如果您禁用或删除 IPv4 地址段，或重启 DHCP 服务器，则 DHCP 服务器分配将删除。请参见“信息 > DHCP 服务器”(Information > DHCP Server)。

该页面的结构取决于设备。因此，设备分为两组：

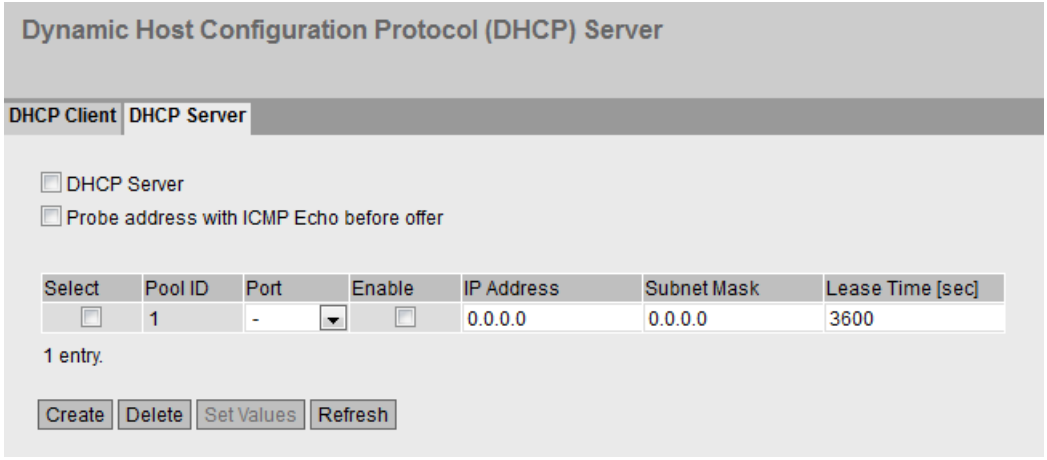
- SCALANCE XB-200、SCALANCE XR-300WG 和 SCALANCE XF-200BA
- SCALANCE XC-200、SCALANCE XF-200G 和 SCALANCE XP-200

要求

- 将所连设备组态成从 DHCP 服务器中获取 IP 地址。
- 已启用基础网桥模式 802.1Q VLAN Bridge。有关详细信息，请参见“Layer 2 > VLAN > 常规 (页 305)”。

SCALANCE XB-200、SCALANCE XR-300WG 和 SCALANCE XF-200BA

在本页面上，指定通过特定端口分配的 IPv4 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

  此检查不用于静态分配。

  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）。
- **端口 (Port)**
  指定将分配此 DHCP 池 IPv4 地址的端口。
- **启用 (Enable)**
  指定是否会使用此 IPv4 地址。

  说明

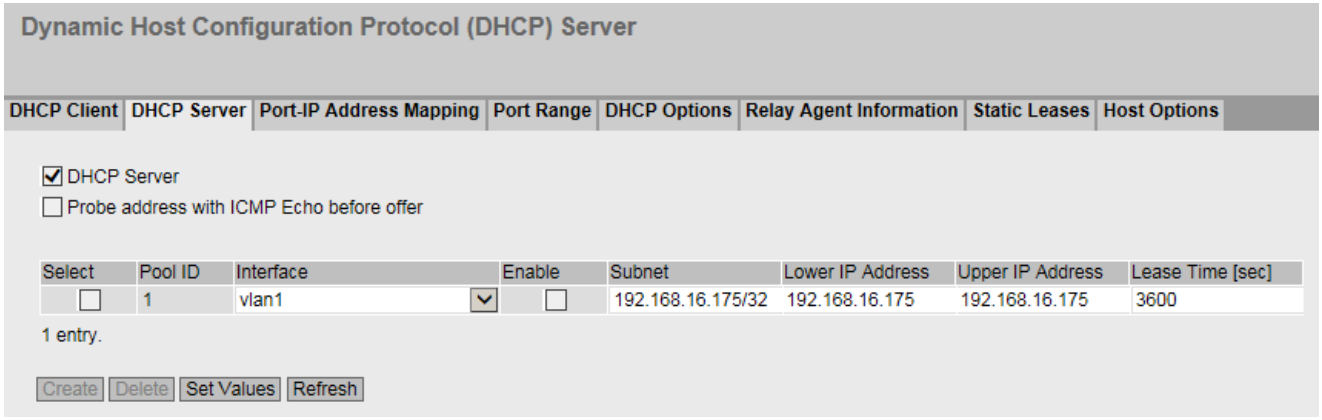
  如果启用 IPv4 地址，在此 DHCP 选项卡中的设置将呈灰显状态，不能进行编辑。

- **IP 地址 (IP Address)**
  输入将通过指定端口分配的 IPv4 地址。

- **子网 (Subnet)**
  输入与 IPv4 地址匹配的子网掩码。使用 CIDR 表示法。
- **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。

SCALANCE XC-200、SCALANCE XF-200G 和 SCALANCE XP-200

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。



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。

  说明

  对其它选项卡的影响

  当组态复选框“子网”(Subnet)、“低位 IP 地址”(Lower IP address) 和“高位 IP 地址”(Upper IP address) 时，“端口 IP 地址映射”(Port-IP Address Mapping) 选项卡相应 DHCP 池中的行将被删除。如果删除组态信息，“端口 IP 地址映射”(Port-IP Address Mapping) 选项卡中的行再次可用。

- **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。
- **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。

在 SCALANCE XB-200、XR-300WG 和 XF-200BA 上组态 DHCP 服务器

1. 单击“创建”(Create) 按钮。
   随即会创建一个具有唯一编号（池 ID）的新行。
2. 选择所需端口。
3. 输入 IPv4 地址和子网掩码。
4. 输入租用时间。
5. 单击“设置值”(Set Values) 按钮。
6. 选中此选项卡上的“启用”(Enable) 复选框。
7. 单击“设置值”(Set Values) 按钮。

在 SCALANCE XC-200、XF-200G 和 XP-200 上组态 DHCP 服务器

1. 单击“创建”(Create) 按钮。
   随即会创建一个具有唯一编号（池 ID）的新行。
2. 选择 VLAN IP 接口。
3. 单击“设置值”(Set Values) 按钮。
   在“端口 IP 地址映射”(Port-IP Address Mapping) 选项卡中，可为池 ID 创建新行。在“端口”(Port) 选项卡中，可以选择当前属于所选 VLAN 的所有端口。
   在“端口范围”(Port Range) 选项卡中，可为池 ID 创建新行。在该行里，可以启用目前属于所选 VLAN 的所有端口。
   池的标准选项在“DHCP 选项”(DHCP Options) 选项卡中创建。
4. 可做以下选择来组态池：
   为 IPv4 地址段配置 DHCP 池
   - 输入子网、低位和高位 IPv4 地址。
   - 输入租用时间。
   - 单击“设置值”(Set Values) 按钮。

   为一个 IPv4 地址配置 DHCP 池
   - 改为“端口 IP 地址映射”(Port-IP Address Mapping) 选项卡。
   - 选择所需端口。
     在“端口范围”(Port Range) 选项卡中，仅启用所选端口。
   - 输入 IPv4 地址和子网掩码。
   - 单击“设置值”(Set Values) 按钮。
     在“DHCP 服务器”(DHCP Server) 选项卡中，相应地勾选“子网”(Subnet)、“低位 IP 地址”(Lower IP address) 和“高位 IP 地址”(Upper IP address) 复选框。
   - 在“DHCP 服务器”(DHCP Server) 选项卡上组态租用时间。
5. 在其它 DHCP 选项卡中，完成池所需的设置。

启用 DHCP 池 (Enable DHCP pool)

1. 在“DHCP 服务器”(DHCP Server) 选项卡中，勾选“启用”(Enable) 复选框。
2. 单击“设置值”(Set Values) 按钮。

删除 DHCP 池

说明

只能删除未启用的条目。

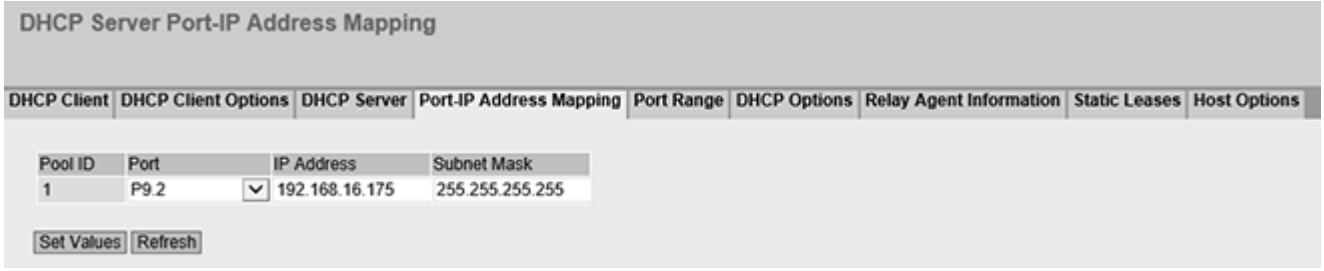
1. 启用要删除的行中的“选中”(Select) 复选框。
   对所有要删除的条目重复此步骤。
2. 单击“删除”(Delete) 按钮。
   删除了相关条目。

6.4.9.3 端口 IP 地址映射

在该页面上，为特定端口分配一个 IP 地址。

在“DHCP 服务器”(DHCP Server) 选项卡中创建一个池后，将在此页面的表中创建一个新行。在相应的下拉列表中，选择分配给此端口的端口。

本页面上的组态影响“DHCP 服务器”(DHCP Server) 和“端口范围”(Port Range) 选项卡。



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。
- **端口 (Port)**
  从下拉列表中选择设置。可选择以下设置选项：
  - Px.y
    指定将分配此 IPv4 地址的端口。只能选择位于相应 VLAN 内的端口。
    如果您选择一个端口，在“端口范围”(Port Range) 选项卡中，仅启用此端口。
  - 不选择 (Not Selected)
    使用此设置后，在“端口范围”(Port Range) 选项卡中，不选中端口或选中不止一个端口。
    如果您选择“不选择”(Not Selected)，将禁用“端口范围”(Port Range) 选项卡中的所有端口。
- **IP 地址 (IP Address)**
  输入 IPv4 地址。
  在“DHCP 服务器”(DHCP Server) 选项卡中，相应地勾选“低位 IP 地址”(Lower IP address) 和“高位 IP 地址”(Upper IP address) 复选框。
- **子网掩码 (Subnet Mask)**
  输入相应的子网掩码。
  在“DHCP 服务器”(DHCP Server) 选项卡中，相应地勾选“子网”(Subnet) 复选框。

步骤

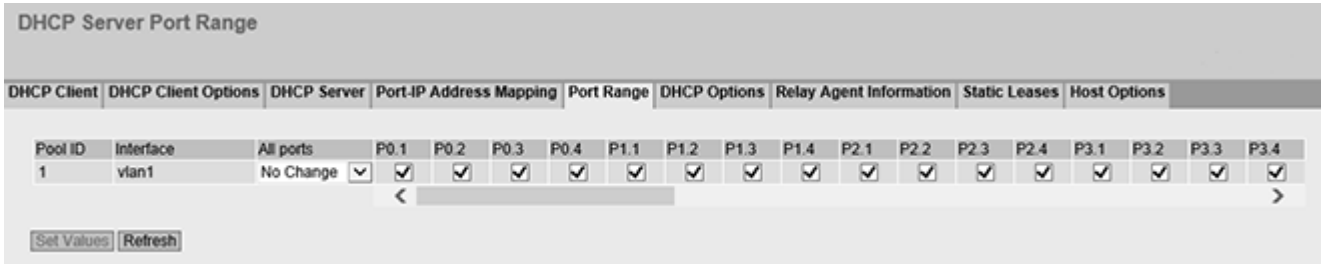
为端口分配 IP 地址

1. 选择所需端口。
2. 输入 IPv4 地址和子网掩码。
3. 单击“设置值”(Set Values) 按钮。
   在“端口范围”(Port Range) 选项卡中，仅为相关 DHCP 池启用所选端口。
   在“DHCP 服务器”(DHCP Server) 选项卡中，相应地为相关 DHCP 池勾选“子网”(Subnet)、“低位 IP 地址”(Lower IP address) 和“高位 IP 地址”(Upper IP address) 复选框。

6.4.9.4 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。



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 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。
- **Px.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。

说明

对其它选项卡的影响

如果要仅启用一个端口，应勾选“端口 IP 地址映射”(Port-IP Address Mapping) 选项卡中的该项。

如果“端口地址映射”(Port-IP Address Mapping) 选项卡中没有端口或者不止一个端口被启用，选择“不选择”(Not Selected)。

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。

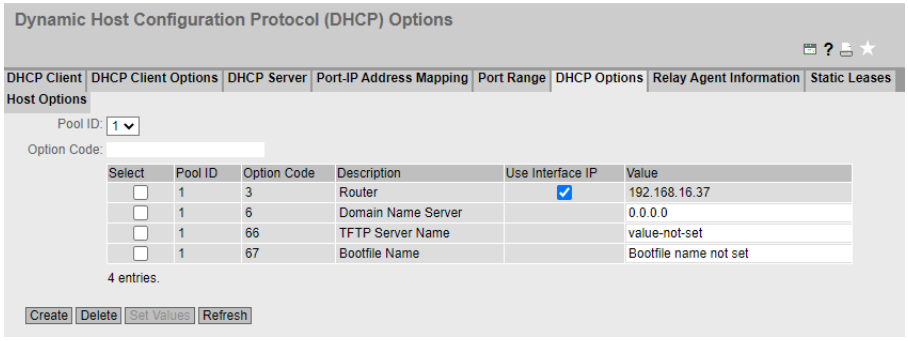
组态所有端口

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。

6.4.9.5 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 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 DHCP 服务器的内部 IPv4 地址设置为 DHCP 参数。



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 地址用作默认网关，被分配给地址段的 IP 接口。如果已清除该复选框，则可以输入 IPv4 地址。
- **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 服务器）
    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 15（域名）
    输入客户端所在的域的名称。
  - DHCP 选项 43（供应商特定信息）
    以字符串格式输入信息。
  - DHCP 选项 66（TFTP 服务器）
    输入 DHCP 参数作为 IPv4 地址或 FQDN，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。

所支持的 DHCP 选项

支持以下 DHCP 选项：

- 选项 1
- 选项 3
- 选项 6

- 选项 12
- 选项 15
- 选项 43
- 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，则为选项 3 选中“Use Interface IP”复选框。
6. 单击“设置值”(Set Values) 按钮。

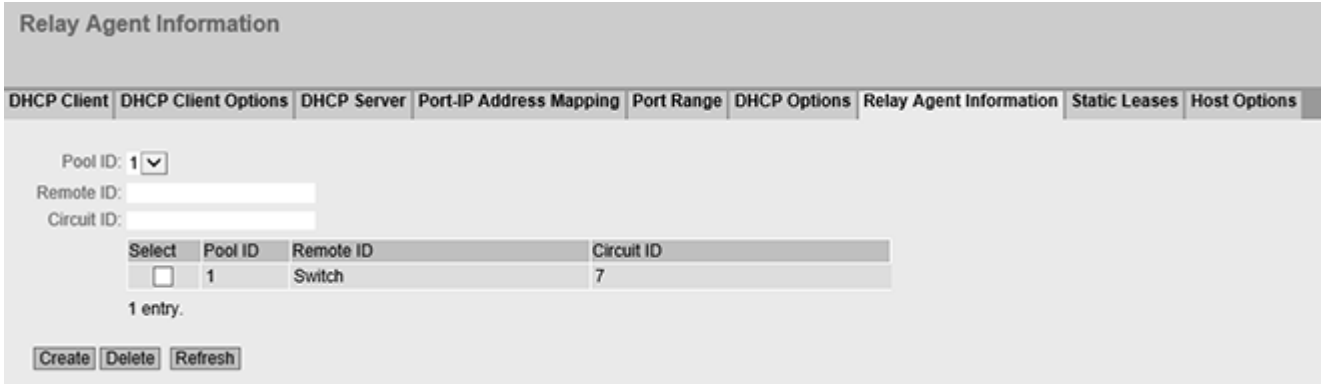
删除 DHCP 选项

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。

6.4.9.6 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 IP 接口创建更多地址段，以使端口响应不同请求。



说明

该页面包含以下框：

- **Pool ID**
  选择所需的 IPv4 地址段。
- **Remote ID**
  输入远程 ID。
- **Circuit ID**
  输入电路 ID。

该表格包括以下列：

- **Select**
  选中要删除的行中的复选框。
- **Pool ID**
  显示 IPv4 地址段编号。
- **Remote ID**
  显示远程 ID。
- **Circuit ID**
  显示电路 ID。

步骤

创建条目

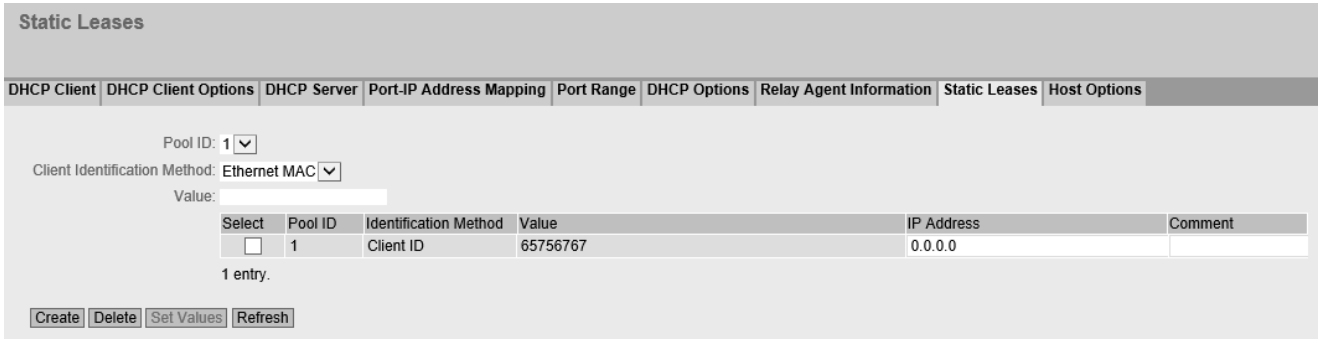
1. 选择一个池 ID。
2. 输入远程 ID。
3. 输入电路 ID。
4. 单击“Create”按钮。

删除一个条目

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

6.4.9.7 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。



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。
- **值 (Value)**
  输入显示客户端的 MAC 地址 (Ethernet MAC)、客户端 ID (Client ID) 或 DUID (DUID)。

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、客户端 ID、还是 DUID 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。
- **注释 (Comment)**
  如有必要，输入注释。

步骤

创建静态租用

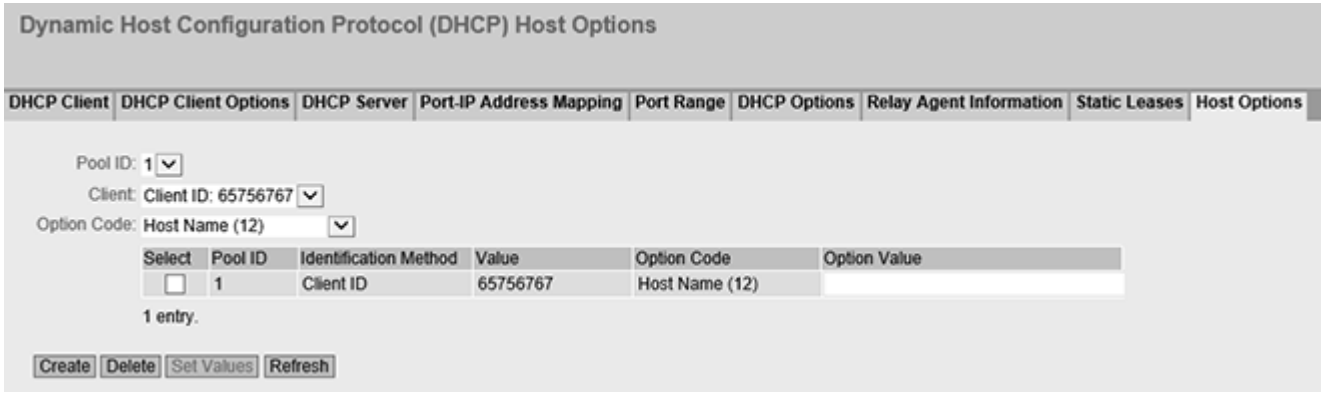
1. 选择一个池 ID。
2. 选择客户端标识方法。
3. 输入值。
4. 单击“创建”(Create) 按钮。
5. 指定将分配给客户端的 IPv4 地址。
6. 单击“设置值”(Set Values) 按钮。

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。

6.4.9.8 主机选项

在此页面上，可以为已向其分配静态 IP 地址的设备指定 DHCP 选项。通过 DHCP 选项，DHCP 服务器可为客户端提供其他组态参数。



说明

该页面包含以下框：

- **Pool ID**
  选择所需的 IPv4 地址段。
- **Client**
  选择想要设置 DHCP 选项的设备。
- **Option Code**
  从此下拉列表中选择 DHCP 选项。可选择以下选项：
  - Host Name (12)
  - TFTP Server Name (66)
  - Bootfile Name (67)

该表格包括以下列：

- **Select**
  选中此复选框以标记要删除的行。
- **Pool ID**
  显示 IPv4 地址段编号。
- **Identification Method**
  显示标识客户端的方式。可能的选项如下：
  - MAC
  - 客户端 ID
- **Value**
  显示在“Static Leases”下分配的“Identification Method”的值。
- **Option Code**
  显示 DHCP 选项。
- **Option Value**
  根据所选选项代码，输入主机名称、TFTP 服务器名称或启动文件名。

步骤

定义选项

1. 选择一个池 ID。
2. 选择客户端。
3. 选择 Option Code。
4. 单击“Create”按钮。随即会在表中创建一个附加行。

5. 在新创建的行中输入 DHCP 选项的 Option Value。
6. 单击“Set Values”按钮。

删除选项

1. 选择要删除的行的复选框。
2. 单击“Delete”按钮。

6.4.10 SNMP

也可参见“技术基础”章节的“SNMP (页 93)”部分。

6.4.10.1 常规

SNMP 组态

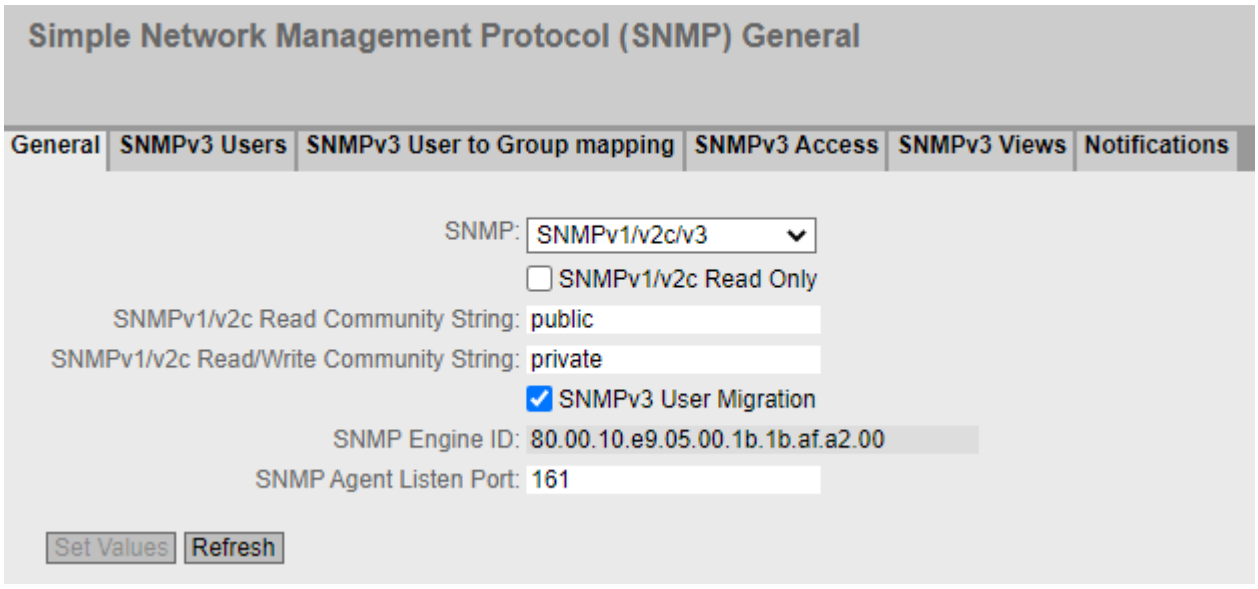
说明

删除 SNMPv3 组态

要删除 SNMPv3 组态，请按以下步骤操作：

1. 删除预定义视图 **SIMATICNETRD** 和 **SIMATICNETWR** 以外的所有 SNMPv3 视图。
2. 删除所有 SNMPv3 访问。
3. 删除“SNMPv3 用户与组的映射”(SNMPv3 User to Group mapping) 表中的所有条目。
4. 删除所有 SNMPv3 用户。

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选项。


Simple Network Management Protocol (SNMP) General
General
SNMPv3 Users
SNMPv3 User to Group mapping
SNMPv3 Access
SNMPv3 Views
Notifications
SNMP:
SNMPv1/v2c/v3
SNMPv1/v2c Read Only
SNMPv1/v2c Read Community String:
public
SNMPv1/v2c Read/Write Community String:
private
SNMPv3 User Migration
SNMP Engine ID:
80.00.10.e9.05.00.1b.1b.af.a2.00
SNMP Agent Listen Port:
161
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。可进行以下设置：
  - “-”（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 只读 (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，请勿使用默认值“public”或“private”。请在初始安装之后更改团体字符串。

  建议团体字符串的最小长度为 6 个字符。

  出于安全原因，只能通过 SNMPv1/v2c Read Community String 对 SNMPCommunityMIB 的对象进行有限访问。通过 SNMPv1/v2c Read/Write Community String，可以对 SNMPCommunityMIB 进行完全访问。
- **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。
- **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。
  - **Disabled**
    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 用户组态传送至其它设备。
    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。
- **SNMP 代理侦听端口 (SNMP Agent Listen Port)**
  指定 SNMP 代理等待 SNMP 查询所使用的端口。标准端口 161 为默认端口。可以选择输入标准端口 162 或 1024 ... 49151 或 49500 ... 65535 范围内的端口号。

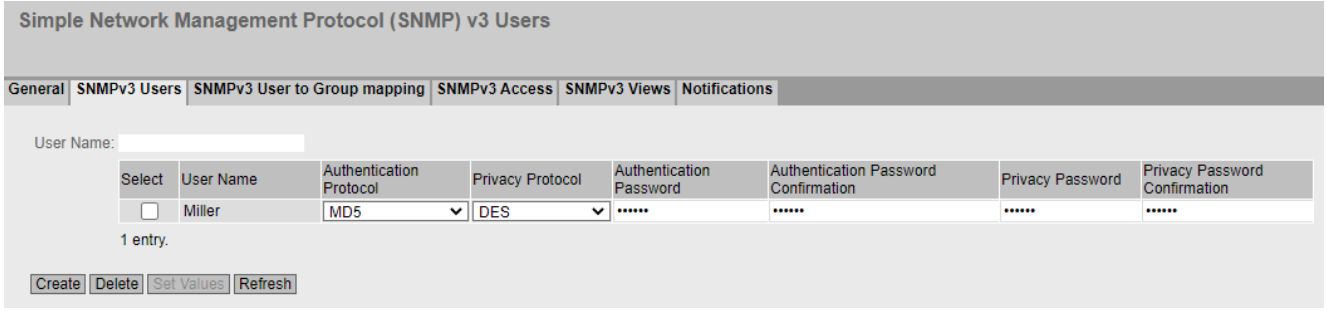
步骤

1. 从“SNMP”下拉列表中选择所需选项：
   – “-”（禁用）
   – SNMPv1/v2c/v3
   – SNMPv3
2. 如果只需要使用 SNMPv1/v2c 对 SNMP 变量进行读访问，请选中“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“设置值”(Set Values) 按钮。

6.4.10.2 SNMPv3 用户 (SNMPv3 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。



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。

该表包括以下列：

- **Select**
  选择要删除的行。
- **User Name**
  显示已创建的用户。
- **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
- **Privacy Protocol**
  指定加密协议以为其存储密码。此下拉列表仅在已选择验证协议后方可启用。
  可使用以下设置：
  – None
  – DES
  – AES
- **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 1 个字符，最多 32 个字符。

  说明

  密码的长度

  作为实现最优安全性的重要举措，我们建议，密码的最小长度为 6 个字符，且应包含特殊字符、大/小写字母和数字。
- **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 1 个字符，最多 32 个字符。

  说明

  密码的长度

  作为实现最优安全性的重要举措，我们建议，密码的最小长度为 6 个字符，且应包含特殊字符、大/小写字母和数字。

- **Privacy Password Confirmation**
  再次输入加密密码以进行确认。

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。将在表中生成一个新条目。
3. 选择“Authentication Protocol”的验证算法。在相应的输入框中，输入验证密码和确认密码。
4. 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。
5. 单击“Set Values”按钮。

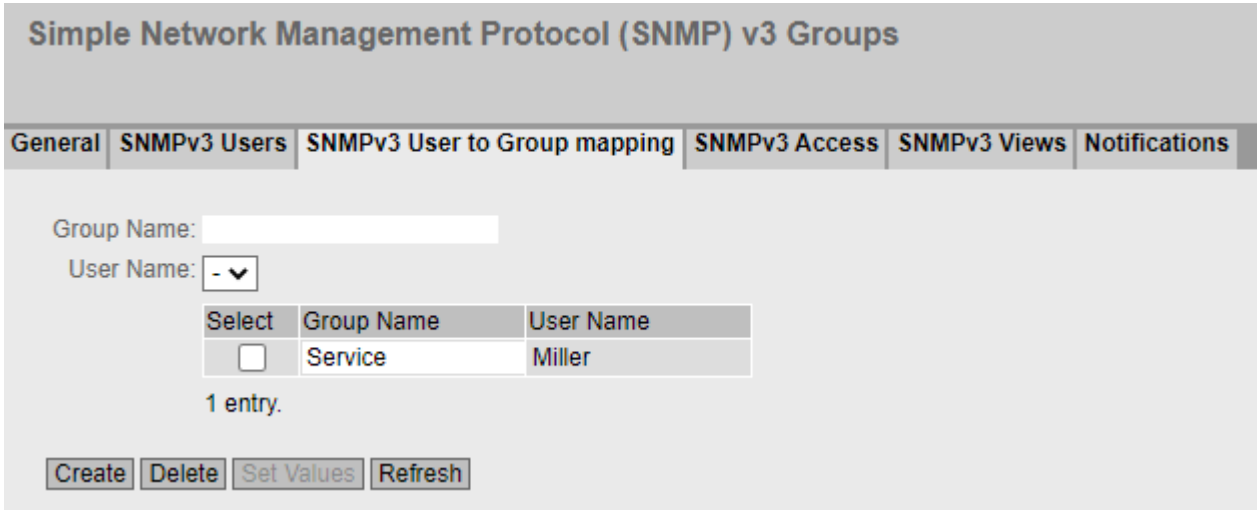
删除用户

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。

6.4.10.3 SNMPv3 用户与组的映射 (SNMPv3 User to Group mapping)

组态组成员

在该 WBM 页面上将用户分配给 SNMPv3 组。每个用户只能是一个组的成员。



说明

该页面包含以下框：

- **Group Name**
  输入将要分配给用户的组。
- **User Name**
  选择将成为指定组的成员的用户。下拉列表仅包含尚未分配给组的用户。

该表包括以下列：

- **Select**
  选择要删除的行。
- **Group Name**
  显示 SNMPv3 组。如果尚未为组定义访问权限，则只能稍后再更改组名称。
- **User Name**
  显示属于该组成员的用户。

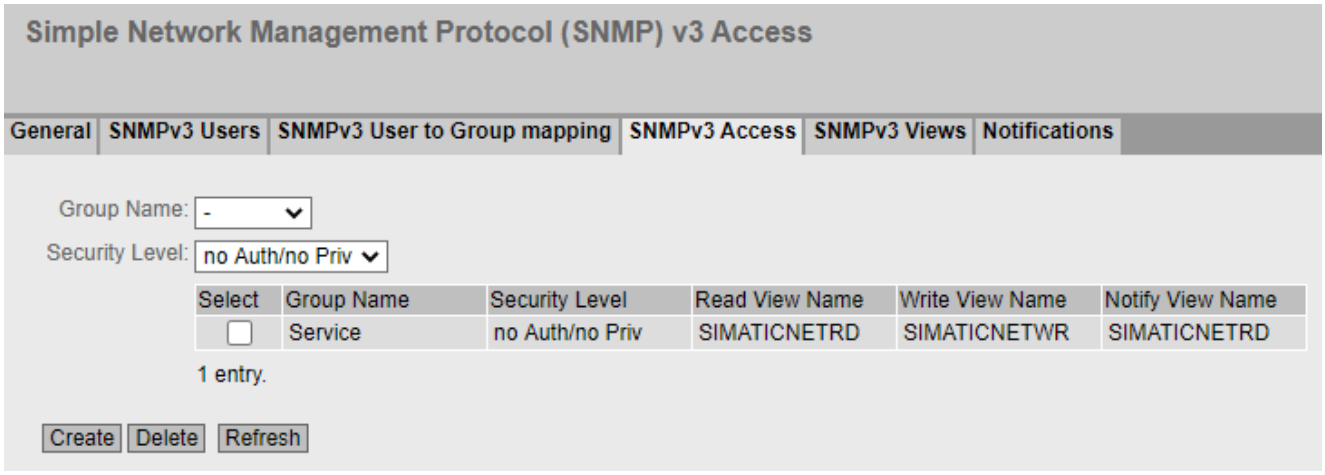
6.4.10.4 SNMPv3 访问 (SNMPv3 Access)

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。

说明

可为组分配不同安全等级的不同访问权限。如果没有为某一安全等级定义访问权限，对于使用该安全等级的组的成员来说，不能对设备进行访问。



说明

该页面包含以下框：

- **Group Name**
  选择组的名称。
- **Security Level**
  选择要为其定义组访问权限的安全等级（身份验证、加密）：
  - **no Auth/no Priv**
    未启用验证，未启用加密。
  - **Auth/no Priv**
    启用验证/未启用加密。
  - **Auth/Priv**
    启用验证/启用加密。

该表包括以下列：

- **Select**
  选择要删除的行。
- **Group Name**
  显示 SNMPv3 组的名称。
- **Security Level**
  显示该访问权限适用于的安全等级。
- **Read View Name**
  输入一个 SNMPv3 视图，以对具有指定 Security Level 的组成员分配读访问权限。
- **Write View Name**
  输入一个 SNMPv3 视图，以对具有指定 Security Level 的组成员分配写访问权限。

  说明

  要实现写访问，还需启用读访问。

- **Notification View Name**
  输入一个 SNMPv3 视图，以供具有已定义安全等级的组成员在进行 SNMP 通知时使用。

步骤

创建新组

1. 选择为其组态 SNMP 访问的组的名称。
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 View Name”字段，输入用于进行读访问的 SNMPv3 视图。
5. 在“Write View Name”字段，输入用于进行写访问的 SNMPv3 视图。
6. 在“Notification View Name”字段，输入用于获取通知的 SNMPv3 视图。
7. 单击“Set Values”按钮。

修改组

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，将必须删除该组并创建新组，然后为其组态新名称。

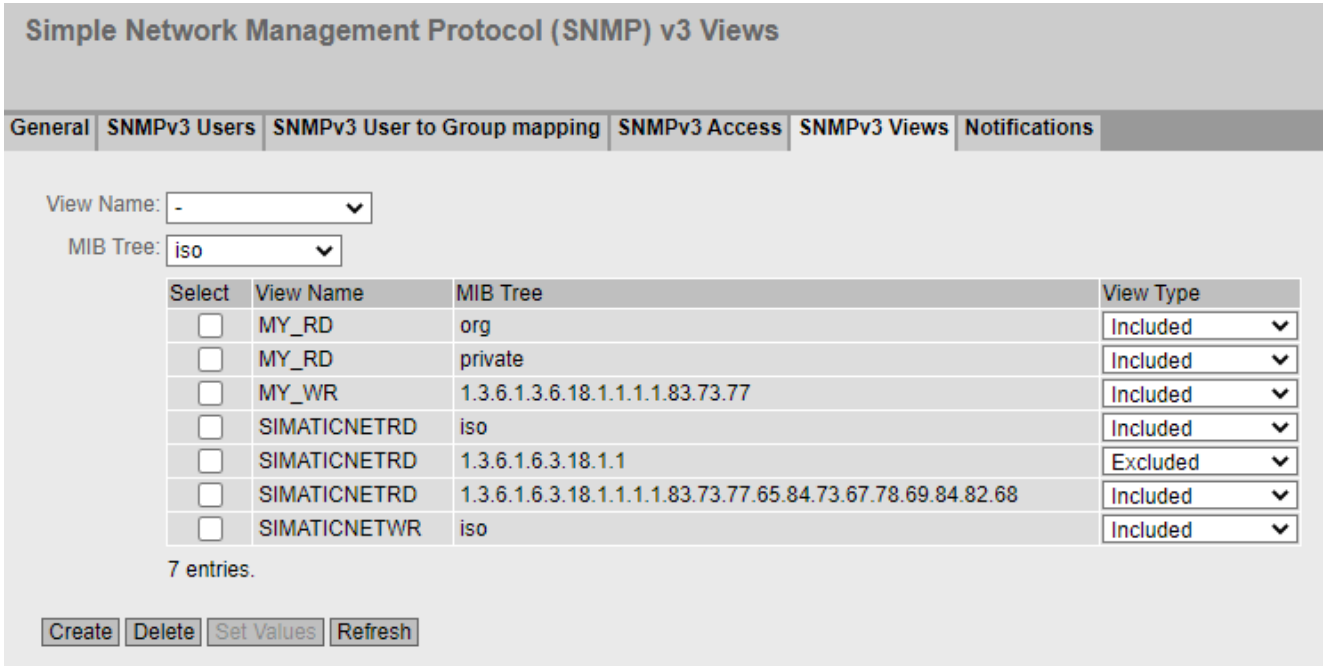
删除组

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。

6.4.10.5 SNMPv3 视图 (SNMPv3 Views)

组态 SNMPv3 视图

在此 WBM 页面中组态 SNMP 视图的参数。



说明

控制所有 SNMPv1 和 SNMPv2c 访问

在内部使用预组态的 **SIMATICNETRD** 和 **SIMATICNETWR** 视图控制 SNMPv1 和 SNMPv2c 访问。如果删除或更改这些视图，会直接影响 SNMPv1 和 SNMPv2c 访问。

说明

该页面包含以下框：

- **View Name**
  选择要组态的视图名称。始终需要将 SNMPv3 视图分配给 SNMPv3 访问。因此，需要在“SNMP Access”选项卡的表中输入新的 SNMPv3 视图。
- **MIB Tree**
  选择将用于 SNMPv3 视图的 MIB 区域的 Object Identifier (OID)。可能的选项如下：
  - **iso**
  - **std**
  - **member-body**
  - **org**
  - **mgmt**
  - **private**
  - **snmpV2**

  下拉列表仅包含常用的 OID。如果需要使用未列出的特定 OID 的组态，可通过 CLI 使用 `snmp view` 命令进行组态。该 OID 随后也会显示在 WBM 的概览表中。

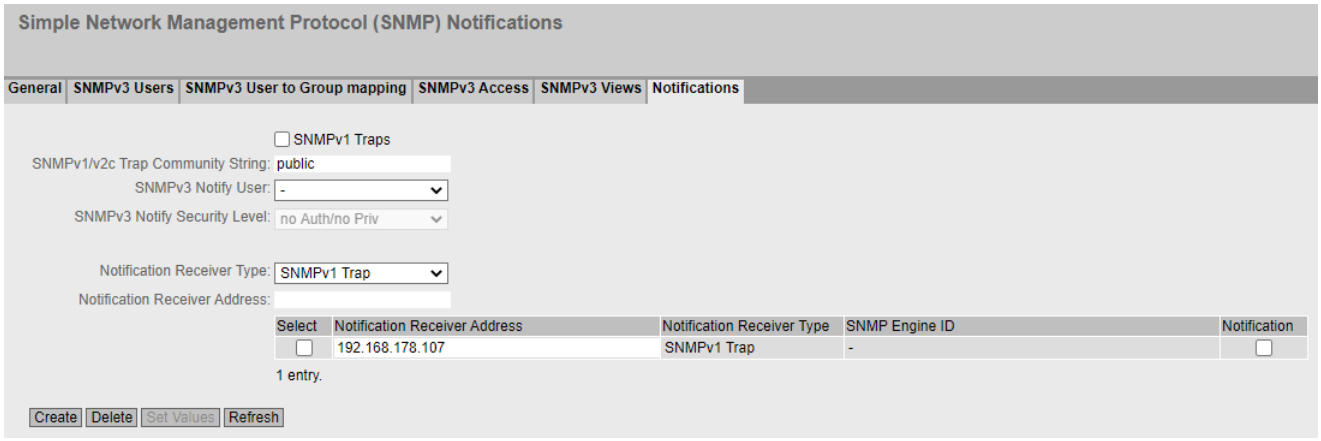
该表格包括以下列：

- **选择 (Select)**
  选择要删除的行。
- **View Name**
  SNMPv3 视图的名称。
- **MIB Tree**
  SNMPv3 视图的 MIB 区域的 OID。
- **View Type**
  可用选项如下：
  - **Included**
    MIB OID 及其下级节点是 SNMPv3 视图的组成部分。可以访问相应的 MIB 对象。
  - **Excluded**
    MIB OID 及其下级节点不是 SNMPv3 视图的组成部分。不能访问相应的 MIB 对象。

6.4.10.6 通知

SNMP 陷阱和 SNMPv3 通知

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 通知（陷阱和通知信息）。仅对“事件”(Events) 菜单中指定的事件发送通知。



说明

该页面包含以下框：

- **SNMPv1 陷阱 (SNMPv1 Traps)**
  启用或禁用发送 SNMPv1 陷阱。此设置将影响 SNMPv1 陷阱的所有接收方，对 SNMPv2c 和 SNMPv3 通知的接收方无影响。
- **SNMPv1/v2c Trap Community String**
  输入用于发送 SNMPv1/v2c 通知的团体字符串。
- **SNMPv3 通知用户 (SNMPv3 Notify User)**
  选择 SNMPv3 通知将发送至的用户。
- **SNMPv3 通知安全等级 (SNMPv3 Notify Security Level)**
  选择要用于 SNMPv3 通知的安全等级（身份验证、加密）。可能的选项如下：
  - 无验证/无加密 (no Auth/no Priv)
    未启用验证/未启用加密。
  - 验证/无加密 (Auth/no Priv)
    已启用验证/未启用加密。
  - 验证/加密 (Auth/Priv)
    已启用验证/已启用加密。

- **通知接收方类型 (Notification Receiver Type)**
  接收方类型定义 SNMP 版本和通知类型。SNMP Inform 通知必须由接收方确认，SNMP 陷阱则无需如此。可能的选项如下：
  - SNMPv1 Trap
  - SNMPv2c Trap
  - SNMPv2c Inform
  - SNMPv3 Trap
  - SNMPv3 Inform
- **通知接收方地址 (Notification Receiver Address)**
  输入设备发送 SNMP 通知的接收方站 IP 地址。最多可指定十个不同的接收方服务器。

该表包括以下列：

- **Select**
  选择要删除的行。
- **通知接收方地址 (Notification Receiver Address)**
  如有必要，请更改站的 IP 操作数地址。
- **通知接收方类型 (Notification Receiver Type)**
  显示定义的接收方类型。
- **SNMP 引擎 ID (SNMP Engine ID)**
  SNMPv3 Inform 通知将发送至的 SNMP 引擎的 ID。只能为接收方类型“SNMPv3-Inform”组态此参数。
- **通知 (Notification)**
  启用或禁用 SNMP 通知的发送。已输入但未选择的工作站不会接收任何 SNMP 通知。

说明

如果表行呈灰显，则表示相应通知已通过 CLI 组态，因此只能通过 CLI 删除。

步骤

组态通知

1. 在“SNMPv3 通知用户”(SNMPv3 Notify User) 下拉列表中选择 SNMPv3 通知的接收方。
2. 在“SNMPv3 通知安全等级”(SNMPv3 Notify Security Level) 下拉列表中选择 SNMPv3 通知的安全等级。
3. 在 “通知接收方类型”(Notification Receiver Type) 下拉列表中选择接收方类型。
4. 在 “通知接收方地址”(Notification Receiver Address) 中输入设备应向其发送陷阱或通知的目标站的 IP 地址。
5. 单击“Create”按钮以创建新的陷阱条目。

6. 激活所需行中的“通知”(Notification)。
7. 单击“Set Values”按钮。

删除陷阱条目

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

6.4.11 系统时间 (System Time)

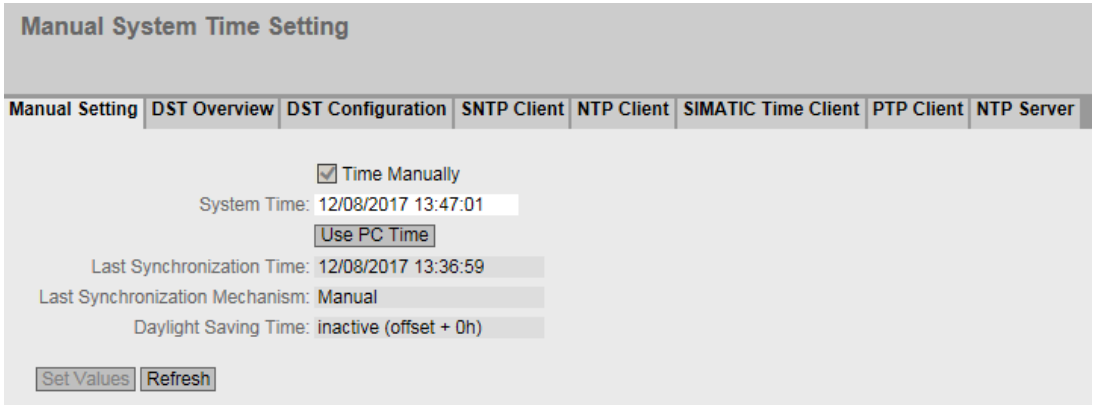
可以采用不同的方法来设置设备的系统时间。每次只能采用一种方法。

激活一种方法后，将自动禁止之前激活的方法。

6.4.11.1 手动设置

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“Time Manually”。



说明

该页面包含以下框：

- **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。
- **System Time**
  按“MM/DD/YYYY HH:MM:SS”格式输入日期和时间。

- **Use PC Time**
  单击该按钮以使用 PC 的时间设置。
- **Last Synchronization Time**
  显示上一次时钟同步发生的时间。如果无法进行日时钟同步，该框会显示“Date/time not set”。
- **Last Synchronization Mechanism**
  显示上次时钟同步是如何执行的。
  - Not set
    未设置时间。
  - 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
  - PTP
    使用 PTP 自动进行时钟同步。此选项仅适用于支持 PTP 的设备。
- **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“System Time”框中显示。
  - inactive (offset +0 h)
    不会更改当前系统时间。

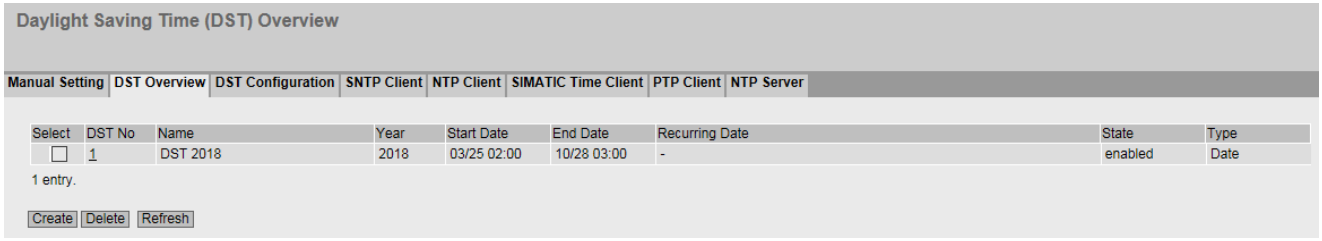
步骤

1. 启用“Time Manually”选项。
2. 单击“System Time”输入框。
3. 在“System Time”输入框中，按“MM/DD/YYYY HH:MM:SS”格式输入日期和时间。
4. 单击“Set Values”按钮。
   将采用该日期和时间，并在“Last Synchronization Mechanism”框中输入“Manual”。

6.4.11.2 DST 概述

夏令时切换

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

该页面包含以下框：

- **Select**
  选择要删除的行。
- **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。
- **Name**
  显示条目名称。
- **Year**
  显示条目的创建年份。
- **Start Date**
  显示夏令时的起始月、日和时间。
- **End Date**
  显示夏令时的结束月、日和时间。
- **Recurring Date**
  输入“重复”(Recurring) 类型后，激活了夏令时的周期将以周、日、月和时钟的形式显示。
  输入“Date”类型后，将显示“-”。

- **Status**
  显示条目的状态：
  - 启用 (Enabled)
    条目已正确创建。
  - 无效 (Invalid)
    条目已新建，但起始和结束日期完全相同。
- **Type**
  显示如何进行夏令时切换：
  - Date
    输入固定日期作为夏令时切换的时间。
  - 重复 (Recurring)
    定义夏令时切换的规则。

步骤

创建条目

1. 单击“Create”按钮。
   随即会在表中创建一个新条目。
2. 在“DST No”列中单击所需的条目。
   切换到“DST Configuration”页面。
3. 在“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“Name”框中输入一个名称。
5. 如果已选择类型“Date”，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）
6. 如果已选择类型“重复”(Recurring)，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“Set Values”按钮。

删除条目

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

6.4.11.3 DST 组态

组态夏令时切换

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。

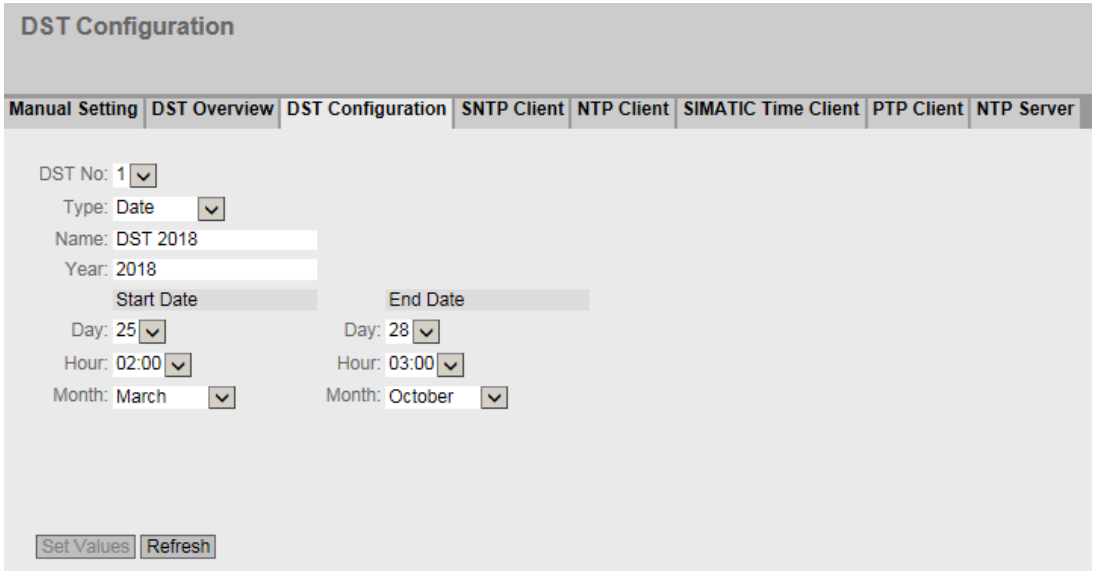
设置

说明

此页面包含的内容取决于您在“Type”框中做出的选择。
始终都会显示“DST No.”、“Type”和“Name”框。

- **DST No.**
  选择条目的类型。
- **Type**
  选择夏令时切换方式：
  - 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。
  - 重复 (Recurring)
    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。
- **Name**
  输入条目名称。
  名称最长为 16 个字符。

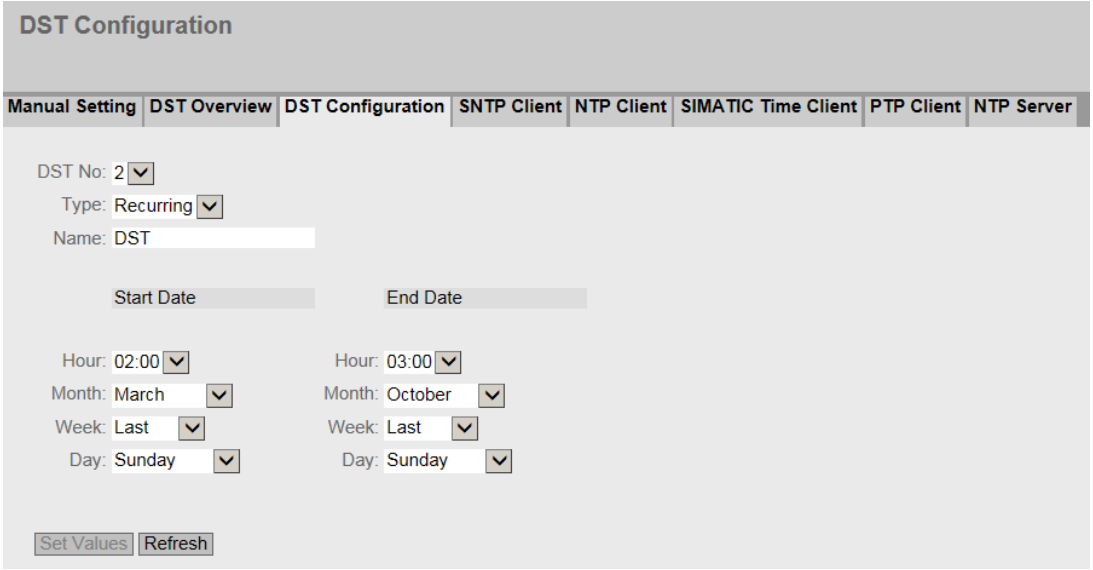
选择“日期” (Date) 时的设置



可设置夏令时开始和结束的固定日期。

- **Year**
  输入夏令时切换的年份。
- **Start Date**
  输入以下值作为夏令时的起点：
  - 日 (Day)
    指定日期。
  - Hour
    指定小时。
  - Month
    指定月份。
- **End Date**
  输入以下值作为夏令时的终点：
  - 日 (Day)
    指定日期。
  - Hour
    指定小时。
  - Month
    指定月份。

选择“重复” (Recurring) 时的设置



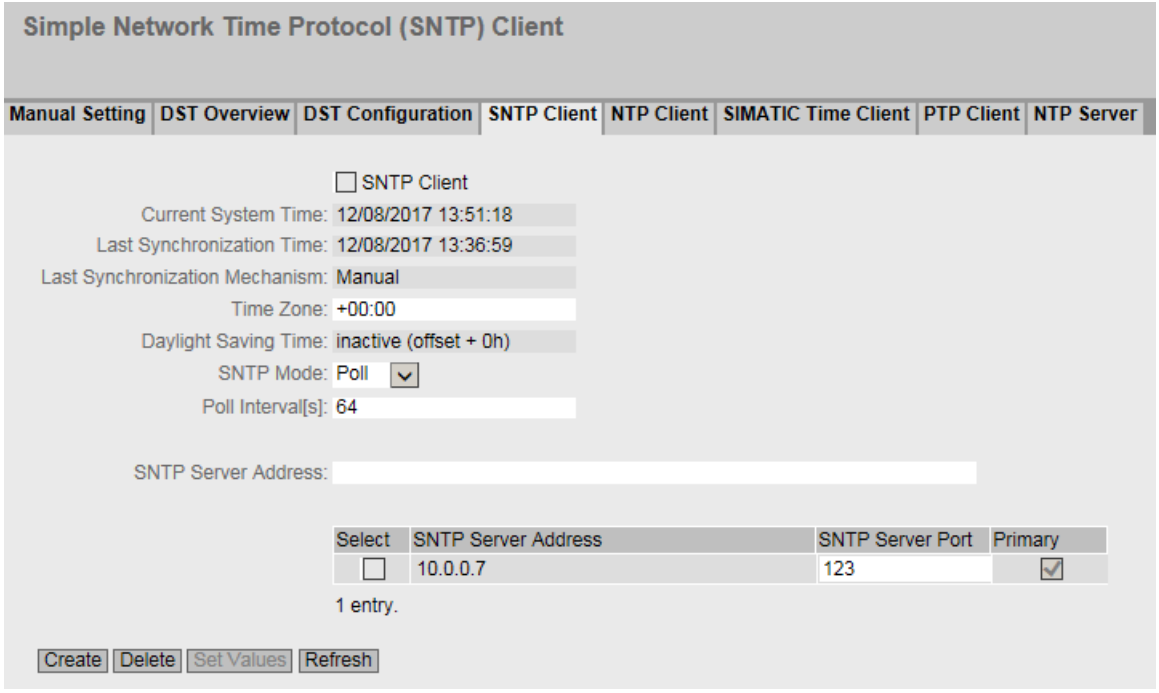
可以创建夏令时切换规则。

- **Start Date**
  输入以下值作为夏令时的起点：
  - Hour
    指定小时。
  - Month
    指定月份。
  - 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。
- **End Date**
  输入以下值作为夏令时的终点：
  - Hour
    指定小时。
  - Month
    指定月份。
  - 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。

6.4.11.4 SNTP 客户端

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时间帧。



说明

该页面包含以下框：

- **SNTP Client**
  启用或禁用使用 SNTP 自动进行时钟同步。
- **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。
- **Last Synchronization Time**
  显示上一次时钟同步发生的时间。

- **Last Synchronization Mechanism**
  显示上次时钟同步的执行方式。可能的方法如下：
  - Not set
    未设置时间。
  - 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
  - PTP
    使用 PTP 自动进行时钟同步。此选项仅适用于支持 PTP 的设备。
- **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“Current System Time”框中的时间。
- **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。
    “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 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。在该模式下，输入框“SNTP Server Address”、“SNTP Server Port”中的设置没有影响。
    在此模式下，仅支持 IPv4 地址。

    说明

    在侦听模式下的 SNTP 客户端和 NTP 服务器不能同时启用。
  - Poll
    如果选择该模式，则会显示输入框“Poll Interval[s]”，以便进一步进行组态。在该模式下，需考虑输入框“SNTP Server Address”、“SNTP Server Port”中的设置。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。
    在此模式下，支持 IPv4 和 IPv6 地址。

- **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。
- **SNTP Server Address**
  输入 SNTP 服务器的 IP 地址或 FQDN（完全限定域名，Fully Qualified Domain Name）。
- **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
- **Primary**
  为第一个创建的 SNTP 服务器设置此复选标记。如果已创建多个 SNTP 服务器，将首先查询主服务器。

步骤

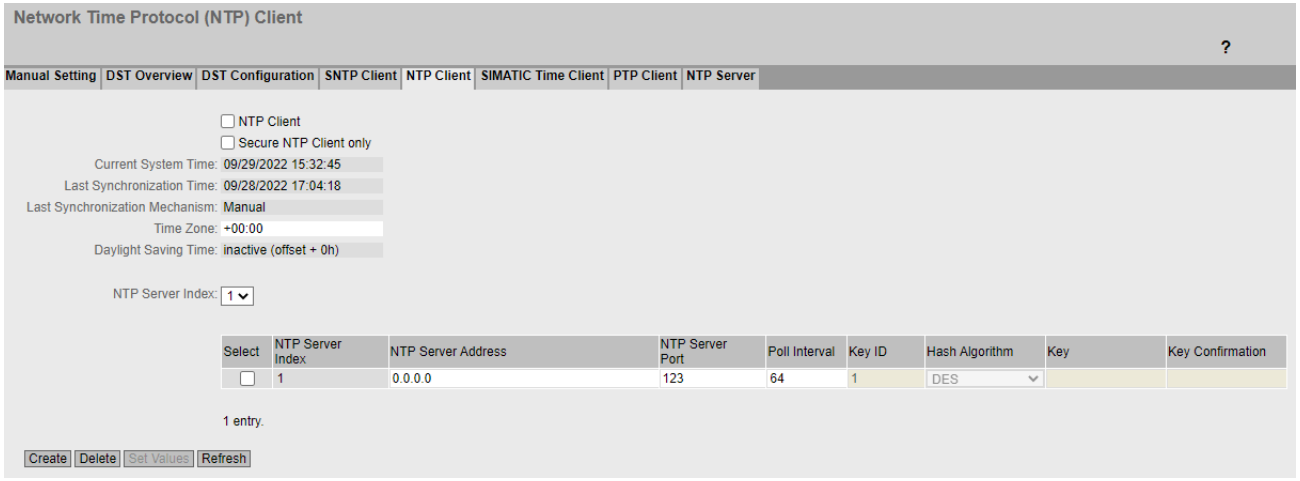
1. 单击“SNTP Client”复选框以启用自动时间设置。
2. 在“Time Zone”输入框中输入当地时间与世界时间 (UTC) 的时差。由于 SNTP 服务器始终发送 UTC 时间，因此输入格式为“+/-HH:MM”（例如，对于 CEST 是 +02:00）。该时间随后会根据指定的时区重新计算为当地时间。可以在“System > System Time > DST Overview”和“System > System Time > DST Configuration”页面组态夏令时切换。完成“Time Zone”输入框时，还需要考虑到这一点。
3. 从下拉列表“SNTP Mode”中选择下列选项之一：
   – Poll
     对于该模式，需要组态以下内容：
     - 时区时差（第 2 步）
     - 查询间隔（第 4 步）
     - 时间服务器（第 5 步）
     - 端口（第 7 步）
     - 通过第 8 步完成组态。
   – 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）
     - 时间服务器（第 5 步）
     - 端口（第 7 步）
     - 通过第 8 步完成组态。
4. 在“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。
5. 在“SNTP Server Address”输入框中，输入 SNTP 服务器的 IP 地址或 FQDN，该服务器的帧将用于同步时钟。

6. 单击“Create”按钮。
   将在表中为 SNTP 服务器插入一个新行。
7. 在“SNTP Server Port”列中，输入可用来使用 SNTP 服务器的端口。仅当输入 SNTP 服务器的 IPv4 地址或 FQDN 名称之后，才可以修改该端口。
8. 单击“Set Values”按钮将更改传输到设备。

6.4.11.5 NTP 客户端

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

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。
- **仅限安全 NTP 客户端 (Secure NTP Client only)**
  启用后，设备将接收安全 NTP 服务器的系统时间。该设置适用于所有服务器条目。
  要启用安全 NTP 客户端，必须对用于验证的参数（密钥 ID、散列算法和密钥）进行组态。

  说明

  我们强烈建议使用安全 NTP 服务器。

- **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
  - PTP
    使用 PTP 自动进行时钟同步。此选项仅适用于支持 PTP 的设备。
- **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。
- **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 选择区域的右上角看到当前系统时间。
    “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 服务器索引 (NTP Server Index)**
  选择 NTP 服务器的索引。最多可指定四个 NTP 服务器或安全 NTP 服务器。按照 NTP 服务器索引的顺序查询 NTP 服务器。系统时间由等级最高的服务器应用。如果接收到层值较小的 NTP 服务器的时间帧，则应用该时间。切换到较小层值的时间大约需要 30 分钟。

该表格包括以下列：

- **选择 (Select)**
  选中要删除的行中的复选框。
- **NTP 服务器索引 (NTP Server Index)**
  NTP 服务器的索引。
- **NTP 服务器地址 (NTP Server Address)**
  输入 NTP 服务器的 IP 地址、FQDN（完全限定域名）或主机名。
- **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。时间间隔越大，设备时间的准确性就越差。可能的值介于 64 到 1024 秒之间。

以下输入框仅与安全 NTP 客户端相关：如果未选中“仅限安全 NTP 客户端”(Secure NTP Client only) 复选框，则这些框呈灰色显示：

- **密钥 ID (Key ID)**
  输入验证密钥的 ID。
- **散列算法 (Hash Algorithm)**
  指定验证密钥的格式。
- **密钥 (Key)**
  输入验证密钥。该密钥只能包含可打印的 ASCII 字符。
- **密钥确认 (Key Confirmation)**
  输入验证密钥进行确认。

步骤

通过 NTP 服务器进行时钟同步

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“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 NTP 服务器始终发送 UTC 时间，因此输入格式为“+/-HH:MM”（例如，对于 CEST（中欧夏令时间）是 +02:00）。该时间随后会根据指定的时区重新计算为当地时间。可以在“系统 > 系统时间 > DST 概述”(System > System Time > DST Overview) 和“系统 > 系统时间 > DST 组态”(System > System Time > DST Configuration) 页面组态夏令时切换。完成“Time Zone”输入框时，还需要考虑到这一点。

3. 选择“NTP 服务器索引(NTP Server Index)。
4. 单击“创建”(Create) 按钮。
   将在表中为 NTP 服务器插入一个新行。
5. 在“NTP 服务器地址”(NTP Server Address) 输入框中，输入 NTP 服务器的 IP 地址、FQDN 或主机名，该服务器的帧将用于同步时钟。
6. 在“NTP 服务器端口”(NTP Server Port) 列中，输入可用来使用 NTP 服务器的端口。仅当输入 NTP 服务器的 IPv4 地址或 FQDN 名称之后，才可以修改该端口。
7. 在“轮询间隔”(Poll Interval) 列中，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。
8. 单击“设置值”(Set Values) 按钮。

通过安全 NTP 服务器进行时钟同步

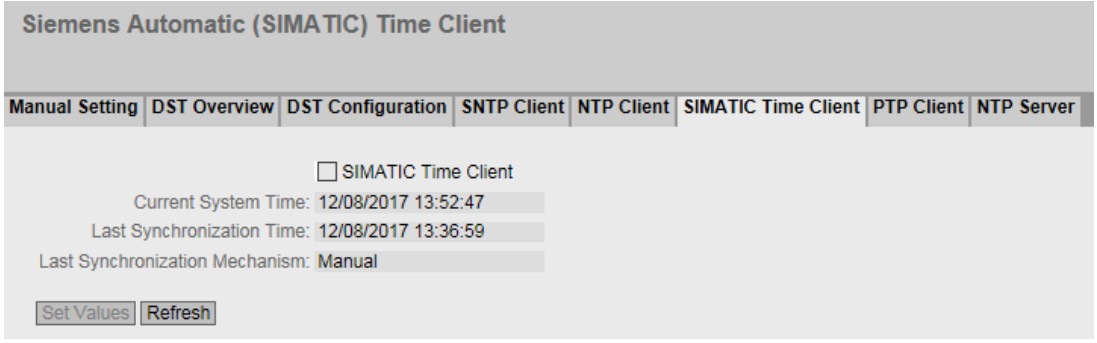
要通过安全 NTP 服务器同步时钟，需要执行以下附加步骤：

1. 单击“仅安全 NTP 客户端”(Secure NTP Client only) 复选框激活通过安全 NTP 自动进行时间设置。
2. 组态验证。
   - 在“密钥 ID”(Key ID) 中输入验证密钥的 ID。
   - 在“散列算法”(Hash Algorithm) 中选择所需的格式。
   - 在“密钥”(Key) 中输入验证密钥。

   通过这些条目，NTP 客户端会基于安全 NTP 服务器自行验证。安全 NTP 服务器上必须具有这些条目。
3. 单击“设置值”(Set Values) 按钮。

6.4.11.6 SIMATIC 时间客户端

通过 SIMATIC 时间客户端设置时间



说明

该页面包含以下框：

- **SIMATIC 时间客户端 (SIMATIC Time Client)**
  选中此复选框可使设备作为 SIMATIC 时间客户端。
- **Current System Time**
  显示当前系统时间。
- **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：
  - Not set
    未设置时间。
  - 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
  - PTP
    使用 PTP 自动进行时钟同步。此选项仅适用于支持 PTP 的设备。

步骤

1. 单击“SIMATIC 时间客户端”(SIMATIC Time Client) 复选框以启用 SIMATIC 时间客户端。
2. 单击“Set Values”按钮。

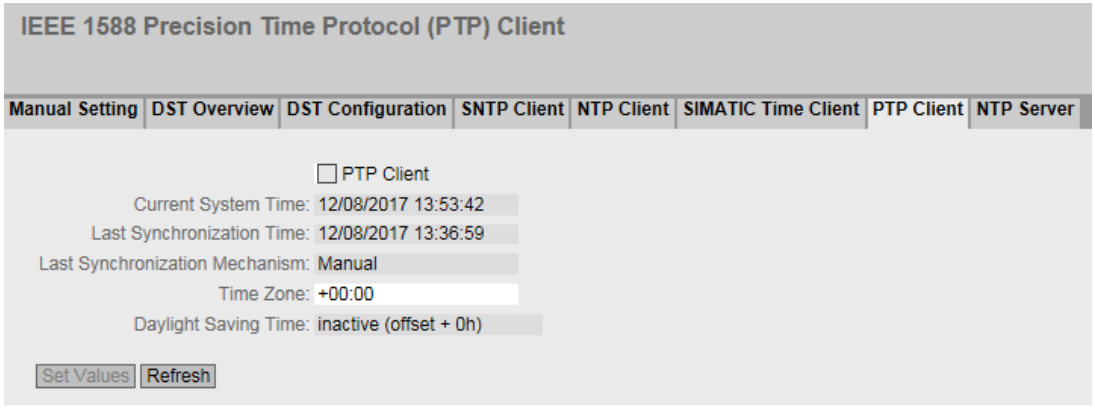
6.4.11.7 PTP 客户端

使用 PTP 自动设置时钟

如果需要使用 PTP 进行时钟同步，可以在此做相关设置。

说明

仅当设备的域编号与时间发送器的域编号匹配时，才可以通过 PTP 进行时间同步。可在“第 2 层 > PTP > TC 常规”(Layer 2 > PTP > TC General) 中组态设备的域编号。



说明

该页面包含以下框：

- **PTP Client**
  选中此复选框可启用使用 PTP 自动进行时钟同步。
- **Current System Time**
  显示因网络中的时间同步而获取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。
- **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。提供以下方法：
  - Not set
    未设置时间。
  - 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
  - PTP
    使用 PTP 自动进行时钟同步

- **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“Current System Time”框中的时间。
- **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。

步骤

1. 单击“PTP Client”复选框启用使用 PTP 自动进行时间设置。
2. 如果适用，则指定时区。
3. 单击“设置值”(Set Values) 按钮。

6.4.11.8 NTP 服务器

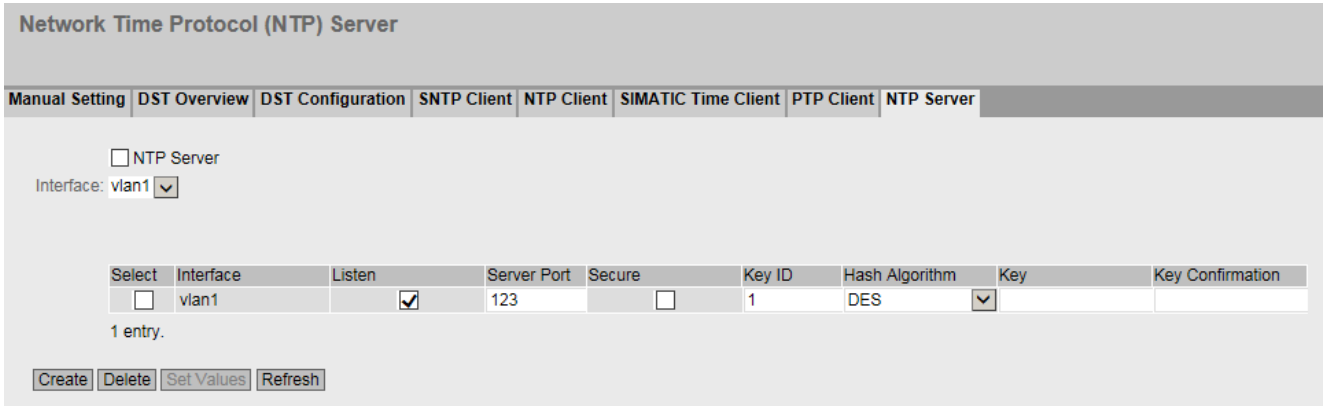
在此 WBM 页面中，将设备组态为 NTP 服务器或“NTP（安全）”类型的 NTP 服务器。其它设备可以通过此 NTP 服务器调用该设备提供的时间。这意味着所提供的设备独立于与外部时间服务器的连接。

说明

时间同步

为了确保设备将所连设备同步到正确的时间，还应将其组态为支持时间同步协议（NTP、SNTP、PTP 或 SIMATIC 时钟帧）的客户端。

NTP 服务器不会发送带有时间信息的循环消息，而只响应相应的请求。作为客户端的功能设置（时区和夏令时）不会影响设备作为服务器发送的时间信息。



说明

该页面包含以下框：

- **NTP 服务器 (NTP Server)**
  启用或禁用 NTP 服务器的服务。

  说明
  在侦听模式下的 SNTP 客户端和 NTP 服务器不能同时启用。

- **接口 (Interface)**
  指定将为其组态 NTP 服务器的接口。在表中创建新行时，默认情况下会为相应的接口激活与 NTP 的时钟同步（“侦听”(Listen) 列）。

该表格包括以下列：

- **选择 (Select)**
  选择要删除的行。
- **接口 (Interface)**
  要为其组态 NTP 服务器的接口的名称。
- **侦听 (Listen)**
  如果选中此复选框，则通过 NTP 同步相应接口的时间。
- **服务器端口 (Server Port)**
  指定 NTP 服务器的端口。
  可能的端口包括：
  - 123（标准端口）
  - 1025 到 36564
- **安全 (Secure)**
  启用此项后，NTP 服务器变为“NTP（安全）”类型的 NTP 服务器。

设备通过“NTP（安全）”进行同步时，仅使用以下各列的内容。

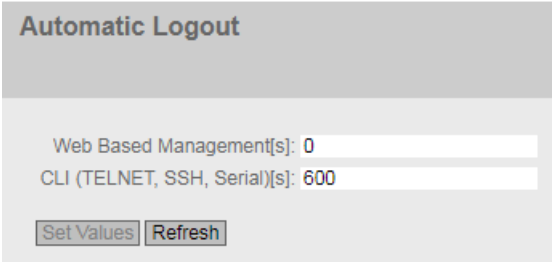
- **密钥 ID (Key ID)**
  输入验证密钥的 ID。
- **散列算法 (Hash Algorithm)**
  指定验证密钥的格式。
- **密匙 (Key)**
  输入验证密钥。密钥长度取决于散列算法。
  散列算法建议使用以下最小长度：
  - DES：8 个 ASCII 字符
  - MD5：16 个 ASCII 字符
  - SHA1：20 个 ASCII 字符
- **密钥确认 (Key Confirmation)**
  输入验证密钥进行确认。

6.4.12 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。



组态

1. 在“Web Based Management[s]”输入框中输入一个介于 60 和 3600 之间的值（单位：秒）。如果输入值 0，则禁用自动注销。
2. 在“CLI (TELNET, SSH, Serial)[s]”输入框中输入一个介于 60 和 600 之间的值（单位：秒）。如果输入值 0，则禁用自动注销。
3. 单击“Set Values”按钮。

6.4.13 SELECT/SET 按钮的组态

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 20)”。

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：

- **Restore Factory Defaults**
  如果选中该复选框，则可通过按钮执行功能“Restore Factory Defaults”。

  ⚠ 小心

  启动期间，按钮功能“恢复出厂默认设置”处于激活状态

  如果在组态中禁用此功能，则仅将在运行期间禁用。启动（例如断电后启动）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交付状态。

- **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

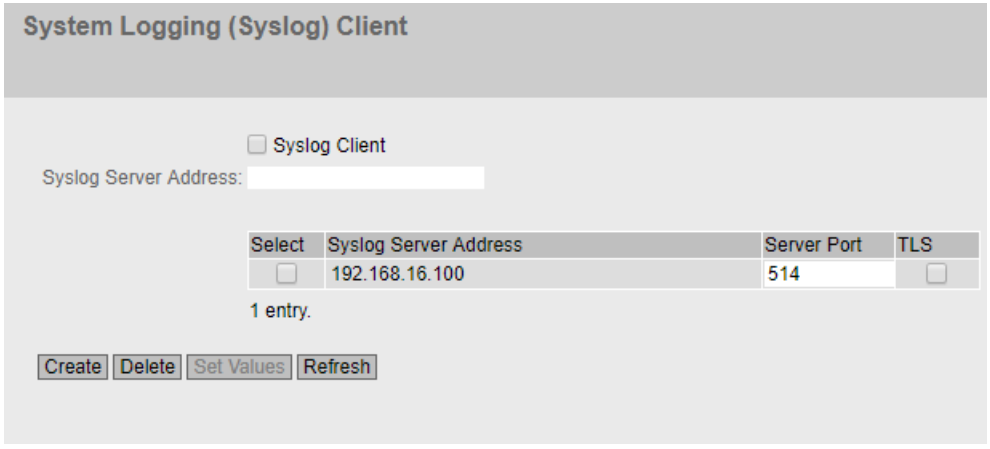
1. 要使用此功能，请选中相应的复选框。
2. 单击“Set Values”按钮。

6.4.14 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。
- 在设备上输入了 Syslog 服务器的 IP 地址或 FQDN。



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 地址或 FQDN。

- **服务器端口 (Server Port)**
  输入要使用的 Syslog 服务器端口。
- **TLS**
  选中此复选框后，与 Syslog 服务器的通信将被加密。

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 Server Address”输入框中，输入将保存日志条目的 Syslog 服务器的 IP 地址和 FQDN。
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

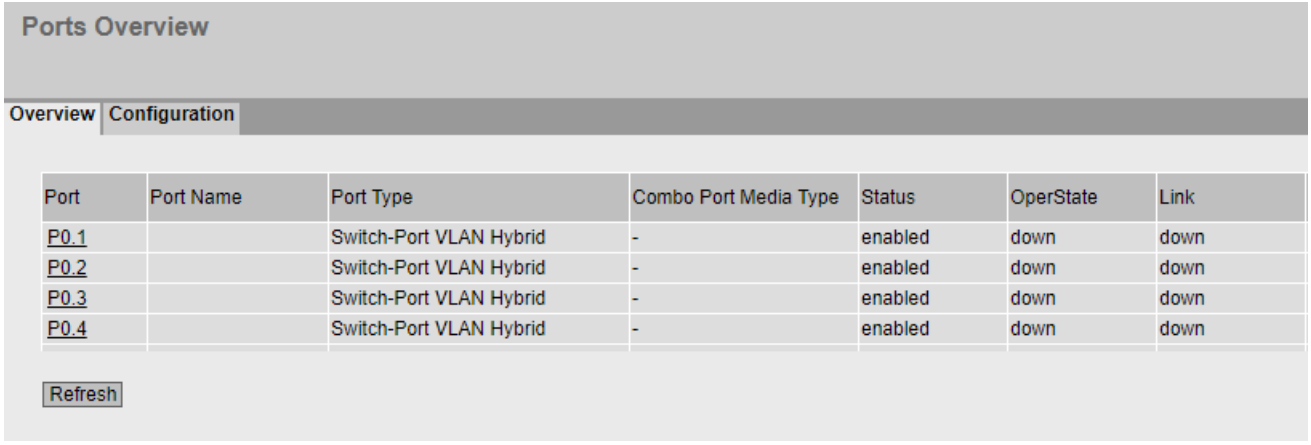
1. 选中要删除的行中的复选框。
2. 单击“删除”(Delete) 按钮。会删除所有选中的条目并刷新显示。

6.4.15 端口

6.4.15.1 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。



Port	Port Name	Port Type	Combo Port Media Type	Status	OperState	Link
P0.1		Switch-Port VLAN Hybrid	-	enabled	down	down
P0.2		Switch-Port VLAN Hybrid	-	enabled	down	down
P0.3		Switch-Port VLAN Hybrid	-	enabled	down	down
P0.4		Switch-Port VLAN Hybrid	-	enabled	down	down

（续表）

Mode	Negotiation	Flow Ctrl. Type	Flow Ctrl.	Maximum Nodes	Learnt Nodes	MAC Address	Blocked by	Unicast MAC Learning
1G FD	enabled		disabled	0	0	08-00-06-70-33-e1	Link down	enabled
1G FD	enabled		disabled	0	0	08-00-06-70-33-e2	Link down	enabled
1G FD	enabled		disabled	0	0	08-00-06-70-33-e3	Link down	enabled
1G FD	enabled		disabled	0	0	08-00-06-70-33-e4	Link down	enabled

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)**
  显示端口的名称。

- **端口类型 (Port Type)**
  显示端口的类型。可能的类型如下：
  - Switch-Port VLAN Hybrid
  - Switch-Port VLAN Trunk
  - Switch-Port PVLAN Host
  - Switch-Port PVLAN Promiscuous
  - Switch-Port VLAN Access
- **组合端口介质类型 (Combo Port Media Type)**
  此列包含一个仅适用于组合端口的值。
  显示组合端口的模式：
  - auto
  - rj45
  - sfp
- **状态 (Status)**
  显示端口是启用还是禁用状态。
  - enabled
    端口启用。数据通信只能通过已启用的端口实现。
  - disabled
    禁用端口但保持连接。
  - Link down
    禁用端口并且中止到伙伴设备的连接。
  - Power down
    禁用端口。
- **OperState**
  显示当前运行状态。运行状态取决于已组态的“状态”(Status) 和“链路”(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。

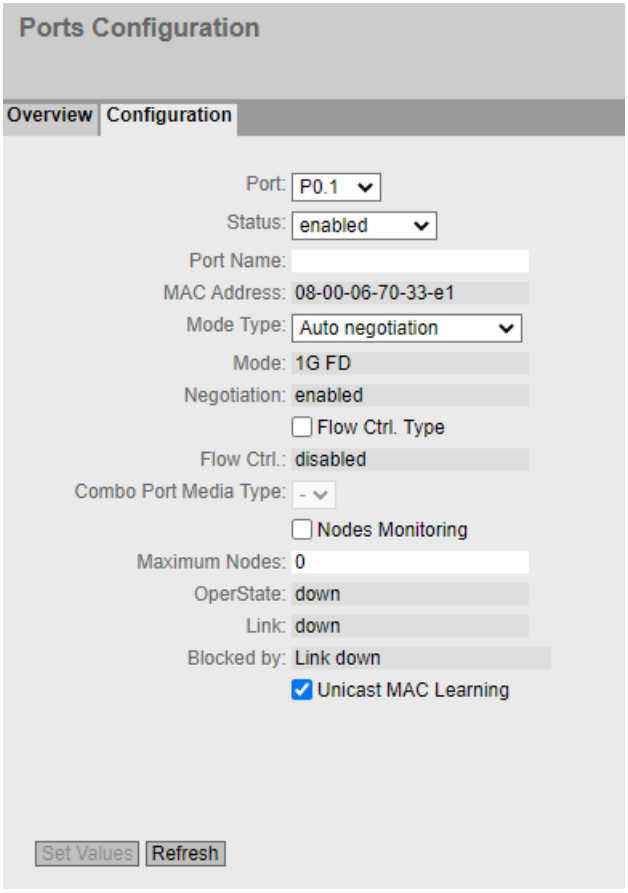
- **链路 (Link)**
  显示网络连接状态。有以下连接状态：
  - 接通 (up)
    端口与网络之间存在有效连接，正在接收“链路完整性信号”。
  - 中断 (down)
    连接中断，例如原因可能是关闭了所连接的设备。
- **模式 (Mode)**
  显示端口的传输参数。
- **协商 (Negotiation)**
  显示自动组态是启用还是禁用状态。
- **流控制类型 (Flow Ctrl.Type)**
  显示此端口的流控制是启用还是禁用状态。
- **流控制 (Flow Ctrl.)**
  显示此端口上的流量控制是否正常工作。
- **最大节点数 (Maximum Nodes)**
  已学习的 MAC 地址数，超出该数后会输出警告。如果显示值“0”，说明此功能已禁用。如果显示的值大于“0”，说明此功能已启用。
- **学习的节点数 (Learnt Nodes)**
  已为该端口学习的 MAC 地址数。
- **MAC 地址 (MAC Address)**
  显示端口的 MAC 地址。

- **受阻原因 (Blocked by)**
  显示端口之所以处于“受阻”状态的原因：
  - -
    端口未被阻止。
  - Ring Redundancy
    端口属于冗余管理器。冗余管理器处于“Passive”状态时，其中一个环网端口处于“受阻”状态。
  - Spanning Tree
    端口在生成树中为“Discarding”状态。端口是生成树的一部分，但位于冗余路径中且数据通信已被禁用。
  - Loop Detection
    已检测到回路，并因此将端口状态组态为“禁用”。
  - Link Check
    在光纤传输链路上检测到中断，并且端口状态因此组态为“disable”。
  - Link Aggregation Member
    端口是链路汇聚的一部分，且已由 LACP 禁用。
  - Link Aggregation (LoopD)
    端口是链路汇聚的一部分。已检测到回路，并且为响应回路，已将链路汇聚状态组态为“disable”。
  - Link Aggregation (STP)
    端口是链路汇聚的一部分。链路汇聚已由生成树切换为状态“Discarding”。
  - Admin down
    已将端口状态组态为“disabled”，请参见“System > Ports > Configuration”。
  - Link down
    已将端口状态组态为“enabled”，但没有任何连接，请参见“System > Ports > Configuration”。
  - Spannungsversorgung aus
    已将端口状态组态为“Link down”或“Power down”；请参见“System > Ports > Configuration”。
  - Standby
    已在设备上启用备用冗余。端口为备用端口，且状态为“Passive”。
  - MRP-Interconnection
    端口为 MRP 互连端口且状态为“blocking”。
- **NOA**
  该功能并非适用于所有设备组，请参见“系统功能和硬件设备”部分。
  显示端口所属的网络。
- **单播 MAC 学习 (Unicast MAC Learning)**
  显示端口的单播地址学习功能是已启用还是已禁用。

6.4.15.2 组态

组态端口

在此页面上可组态设备的所有端口。



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。
- **状态 (Status)**
  指示端口处于启用还是禁用状态。
  - enabled
    端口启用。数据通信只能通过已启用的端口实现。
  - disabled
    禁用端口但保持连接。
  - Link down
    禁用端口并且中止到伙伴设备的连接。

    说明

    减小电流消耗

    对于每个设置为“link down”的光纤端口，设备的电流消耗可减少 30 mA。
  - Power down
    禁用端口。
- **端口名称 (Port Name)**
  输入端口名称。
- **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。
  在某个端口与伙伴端口相互通信之前，两端必须都有匹配的设置。
  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。

说明

“Auto negotiation”模式

如果已连接伙伴不支持“Auto negotiation”，则必须将连接该伙伴的端口永久设为该伙伴的值（传输速度、复用性）

说明

“Auto negotiation”和自动跨接

- SCALANCE XB-200/SCALANCE XC-200/XR-300WG：如果禁用了“Auto negotiation”功能，则“MDI/MDI-X 自动跨接”功能也会关闭。本例中，使用的是跨接电缆。
- SCALANCE XP-200：如果禁用了“Auto negotiation”功能，则“MDI/MDI-X”自动跨接功能保持激活状态。

说明

SCALANCE XR300 WG 的传输方式

通过 SCALANCE XR300 WG PoE 的 10 Gb 端口，还可实现“2.5 Gbps 全双工”和“5 Gbps 全双工”传输模式。“Auto negotiation”功能也可设置这两种传输方式。

- **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、1000 Mbps 或 10 Gbps。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)**
  为端口启用或禁用流量控制功能。

说明

若要使用流量控制功能，请在正确的输入和输出端口启用流量控制。

如果启用流量控制的输入端口将数据包发送至启用流量控制的输出端口，即使发生过载也不会丢弃数据包。如果仅在输入端口启用流量控制，则发生过载时可能丢弃数据包。

说明

使用“自动协商”开启/关闭流量控制

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”。

- **流控制 (Flow Ctrl.)**
  显示此端口上的流量控制是否正常工作。
- **端口类型 (Port Type)**（并非对所有设备组均可用）
  从下拉列表中选择端口类型。

  说明

  私有 VLAN 功能和 RADIUS 验证

  当通过 RADIUS 验证为 VLAN 的一个或多个端口启用 VLAN 分配时，不应将此 VLAN 另外组态为私有 VLAN。

  与通过 RADIUS 验证进行 VLAN 分配相关的私有 VLAN 功能可能会导致系统状态不一致。

  – 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。
  – 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。
  – Switch-Port PVLAN Host
    主机端口属于辅助 PVLAN。
    将设备连接到仅用于与 PVLAN 的特定设备进行通信的主机端口。
  – Switch-Port PVLAN Promiscuous
    混合端口属于主 PVLAN。
    将设备连接到用于与 PVLAN 的所有其它设备进行通信的混合端口。
  – Switch-Port VLAN Access
    访问端口属于支持 Q-in-Q VLAN 隧道功能的提供商交换机。
    将用户网络连接到访问端口。

- **组合端口介质类型 (Combo Port Media Type)**（并非对所有设备组均可用）
  指定组合端口的模式：
  - auto
    如果您选择此模式，可插拔收发器端口具有更高的优先级。
    插入可插拔收发器后，RJ45 固定端口上的现有连接将立即终止。如果未插入可插拔收发器，则可经由 RJ45 固定端口建立连接。
  - rj45
    如果您选择此模式，RJ45 固定端口的使用与可插拔收发器端口无关。
    如果插入可插拔收发器，其将禁用且电源关闭。
  - sfp
    如果您选择此模式，可插拔收发器端口的使用与 RJ45 固定端口无关。
    如果已建立 RJ45 连接，则由于 RJ45 端口的电源关闭，连接将会终止。

  组合端口的出厂设置为 auto 模式。

说明

通过 PROFINET 组态实现自动调整

建立 PROFINET 连接时，将自动调整组合端口介质类型的设置：
- 如果组态可插拔收发器，则组合端口介质类型将设为“sfp”。
- 如果组态了 RJ45 内置端口，则组合端口介质类型将设为“rj45”。

为了能够实现自动调整，组合端口介质类型必须设为“auto”。

使用 WBM 或 CLI 相应地组态组合端口介质类型。

- **节点监视 (Nodes Monitoring)**
  如果选中此复选框，超出最大节点数时会输出警告。选中此复选框时，“Maximum Nodes”输入框中的值会自动设为“1”；取消选中此复选框后，该值会自动设为“0”。

- **最大节点数 (Maximum Nodes)**
  已学习的 MAC 地址数，超出该数后会输出警告。如果此输入框中的值大于“0”，则会自动选中“Nodes Monitoring”复选框。如果值为“0”，则会自动取消选中“Nodes Monitoring”复选框。

- **OperState**
  显示当前运行状态。运行状态取决于已组态的“Status”和“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连接，正在接收“链路完整性信号”。
  - 中断 (down)
    连接中断，例如原因可能是关闭了所连接的设备。
- **受阻原因 (Blocked by)**
  显示端口之所以处于“受阻”状态的原因：
  - -
    端口未被阻止。
  - Ring Redundancy
    端口属于冗余管理器。冗余管理器处于“Passive”状态时，其中一个环网端口处于“受阻”状态。
  - Spanning Tree
    端口在生成树中为“Discarding”状态。端口是生成树的一部分，但位于冗余路径中且数据通信已被禁用。
  - Loop Detection
    已检测到回路，并因此将端口状态组态为“禁用”。
  - Link Check
    在光纤传输链路上检测到中断，并且端口状态因此被组态为“禁用”。
  - Link Aggregation Member
    端口是链路汇聚的一部分，且已由 LACP 禁用。
  - Link Aggregation (LoopD)
    端口是链路汇聚的一部分。已检测到回路，并且为响应回路，已将链路汇聚状态组态为“disable”。
  - Link Aggregation (STP)
    端口是链路汇聚的一部分。链路汇聚已由生成树切换为状态“Discarding”。
  - Admin down
    已将端口状态组态为“disabled”，请参见“System > Ports > Configuration”。
  - Link down
    已将端口状态组态为“enabled”，但没有任何连接，请参见“System > Ports > Configuration”。
  - Spannungsversorgung aus
    已将端口状态组态为“Link down”或“Power down”；请参见“System > Ports > Configuration”。
  - Standby
    已在设备上启用备用冗余。端口为备用端口，且状态为“Passive”。
  - MRP-Interconnection State Change
    端口为 MRP 互连端口且状态为“blocking”。

- **NOA**
  该功能并非适用于所有设备组，请参见“系统功能和硬件设备”部分。

  说明

  只有在设备在透明网桥模式下运行时才能组态此功能 (Layer 2 > VLAN > "General" tab > "Base Bridge Mode" drop-down list:802.1D Transparent Bridge)。在 NOA 组态中的“802.1Q VLAN Bridge”模式下，会显示一条错误消息。

  NOA（NAMUR 开放式架构）是一个针对过程工业中的数据交换的概念，用于将数据从现场级传送到云端。SCALANCE XC-200 可实现 NOA IT/OT 交换机的功能，并将纯 IT 网络与纯 OT 网络分离开。也可以与这两个网络通信。交换机可基于端口将网络分离开，即端口可能属于 IT 网络或 OT 网络，也可能同时属于这两个网络。从下拉列表中选择端口所属的网络。要导出 IT 数据或 OT 数据，必须在每种情况下相应地组态一个端口。选择下列选项之一：

  – Both
    端口属于 IT 网络和 OT 网络。
  – IT
    端口属于 IT 网络。
  – OT
    端口属于 OT 网络。

- **Unicast MAC Learning**
  为端口启用单播地址学习。

更改端口组态

单击相应的框可更改组态。

说明

光学端口始终以最大传输速度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
- 传输模式

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。

6.4.16 故障监视

6.4.16.1 电源

监视电源的设置

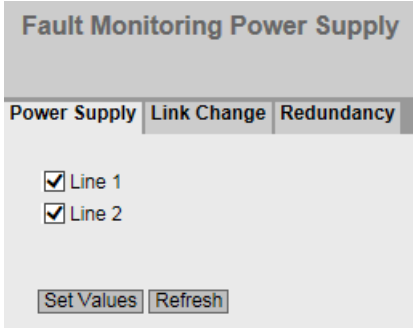
组态是否通过消息系统监视电源。根据硬件型号，会有一个或两个电源连接器（电源 1/电源 2）。带冗余电源时，应对每个单独的进线线路分别组态监视。

当所监视的电源线路（电源 1 或电源 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“Set Values”按钮。

6.4.16.2 链路变化

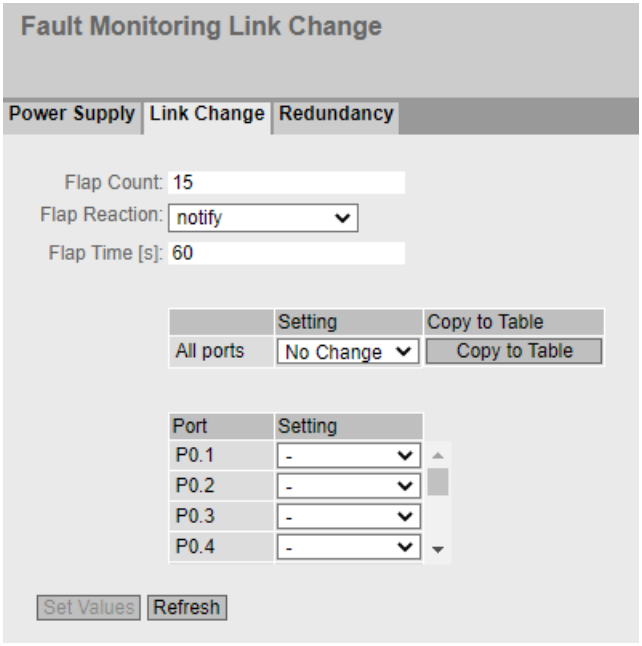
连接状态变化的故障监视组态

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故障信号：

- 当端口上应当有链路但链路缺失时。
- 当端口上不应有链路却检测到链路时。
- 当端口上的链路频繁改变时。

故障会导致信号触点被触发，使设备上的故障 LED 亮起，并将根据组态触发陷阱、电子邮件或在事件日志表中增加条目。



显示框说明

该页面包含以下框：

- **摆动计数 (Flap Count)**
  组态在摆动时间内允许在“链路接通”与“链路中断”之间切换的最大次数。
- **摆动响应 (Flap Reaction)**
  选择出现错误时执行的操作：
  - 通知 (Notifications)
    将创建一个日志条目。
  - 通知断电 (Notify power down)
    将创建一个日志条目，且端口将关闭。

  在“信息 > 错误”(Information > Error) 下手动确认错误消息。
  在“系统 > 端口 > 组态”(System > Ports > Configuration) 下手动激活端口。
- **摆动时间 [s] (Flap Time [s])**
  组态监视“链路接通与“链路中断”之间允许的最大切换次数时采用的时间间隔。
  如果摆动时间内端口在“链路接通”与“链路中断”之间切换的次数超过摆动计数的值，则会触发故障。
  如果摆动时间内端口在“链路接通”与“链路中断”之间切换的次数小于摆动计数的值，则会开始监视。

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）
  - 接通 (Up)
  - 中断 (down)
  - 摆动 (Flap)：参见下面的解释
  - 无变化 (No Change)：表 2 中的设置保持不变。
- **复制到表 (Copy to Table)**
  如果单击此按钮，则为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **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。
- **设置 (Setting)**
  从下拉列表中选择设置。可做以下选择：
  – “-”（禁用）
    不触发错误处理。
  – 接通 (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)）
  – 中断 (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)）
  – 摆动 (Flap)
    如果摆动时间内端口在“链路接通”与“链路中断”之间切换的次数超过摆动计数的值，则会触发错误处理。

组态步骤

为端口组态错误监视

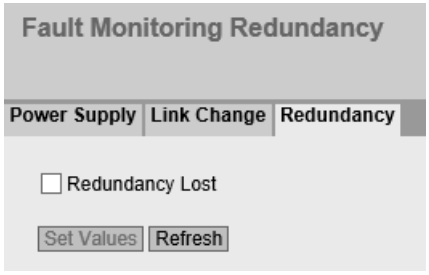
1. 调整用于摆动监视的值。
2. 从相应的下拉列表中，选择要监视连接状态的插槽/端口对应的选项。
3. 单击“设置值”(Set Values) 按钮。

为所有端口组态错误监视

1. 调整用于摆动监视的值。
2. 从“设置”(Setting) 列的下拉列表中选择所需设置。
3. 单击“复制到表”(Copy to Table) 按钮。会为表 2 的所有端口应用此设置。
4. 单击“设置值”(Set Values) 按钮。

6.4.16.3 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

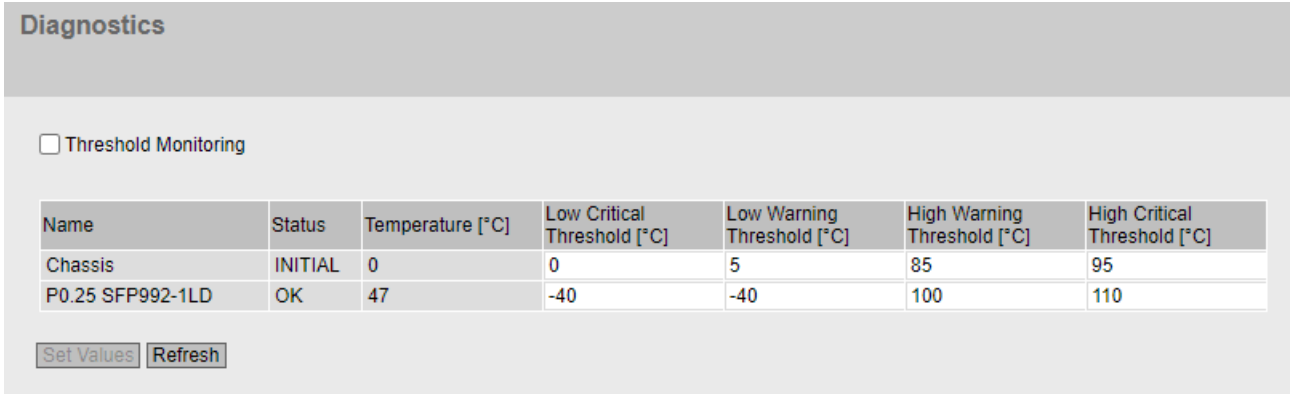
- **Redundancy Lost**
  选中此复选框后，在环网切换（MRP 或 HRP，阻止的端口已关闭）时，相应环网管理器的错误 LED 将激活。

6.4.17 诊断

在此页面上，可为设备的内部和外部模块组态阈值。只有当模块提供诊断信息时，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。

如果诊断值降至组态的阈值以下或超过组态的阈值，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。



说明

该页面包含以下框：

- **阈值监视 (Threshold Monitoring)**
  启用或禁用阈值监视。
  如果启用监视，则仅当超过阈值 15 分钟以上时才会触发事件。

该表包含以下列：

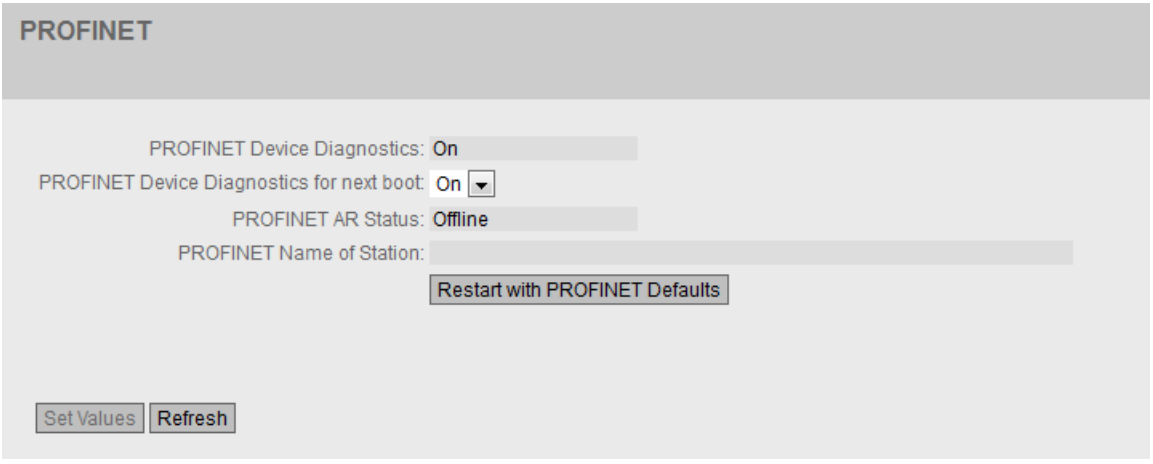
- **名称 (Name)**
  显示模块名称。
  “Chassis”行中的信息指的是外壳的内部温度。
  对于可插拔收发器，指定了端口和类型。
- **状态 (Status)**
  基于阈值与当前温度的关系，将以优先级升序显示以下状态。
  - OK
    温度值处于预设的阈值范围内。
  - WARNING
    分别低于或超过严重级别为“Warning”的阈值下限或阈值上限。温度仍处在正常范围。设备已经检测到了温度的上升和下降，例如，由于柜体变冷。应检查设备。
  - CRITICAL
    分别低于或超过严重级别为“Critical”的阈值下限或阈值上限。必须检查设备。温度过高或过低会导致设备性能受到限制，甚至损坏设备。
  - 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。
- **温度 [°C] (Temperature [°C])**
  显示温度的当前值。显示画面会定期更新。
  温度值可以有 +/- 3 °C 的偏差。因此，在类似环境条件下，同型号的设备其值可能不同。
- **下限阈值 [°C]（严重）(Lower Thrshold [°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。

6.4.18 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 Device Diagnostics**
  显示启用（“On”）还是禁用（“Off”）PROFINET。
- **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 Status**
  此框显示 PROFINET 连接的状态；也就是说，设备与 PROFINET 控制器的连接是处于“Online”状态还是“Offline”状态。
  在此处，“在线”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 Name of Station**
  此框根据 STEP 7 HW Config 中的组态显示 PROFINET 设备名称。
- **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。

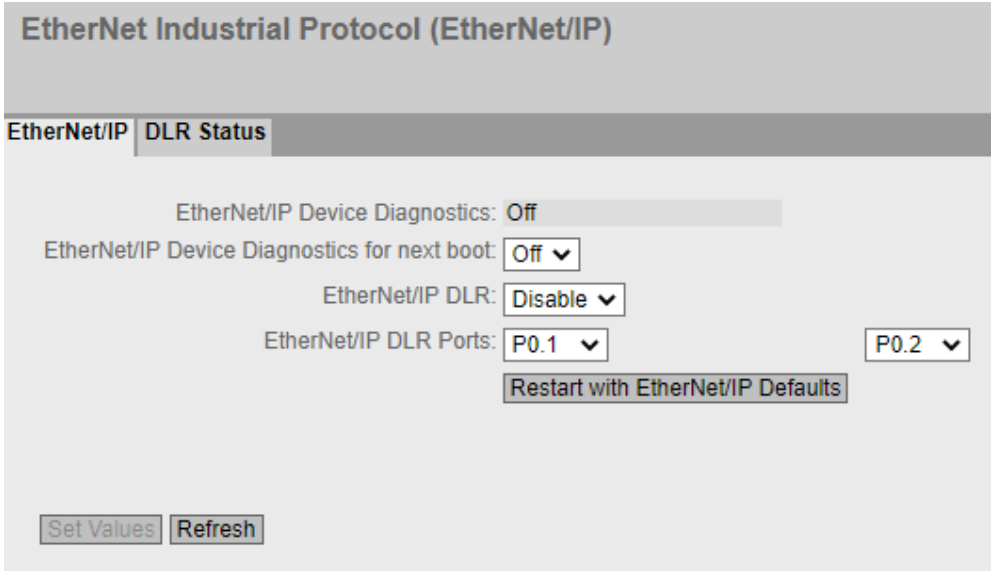
注意
将设置复位为配置文件的默认设置后，IP 地址也会丢失。之后，设备只能通过串行接口、SINEC PNI 或 DHCP 寻址。 在特定连接情况下，之前已正确组态的设备复位后可能会引起数据帧循环传送，从而导致数据通信故障。

6.4.19 EtherNet/IP

6.4.19.1 EtherNet/IP

EtherNet 工业协议 (EtherNet/IP)

在此页面中组态 EtherNet/IP 协议。



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。

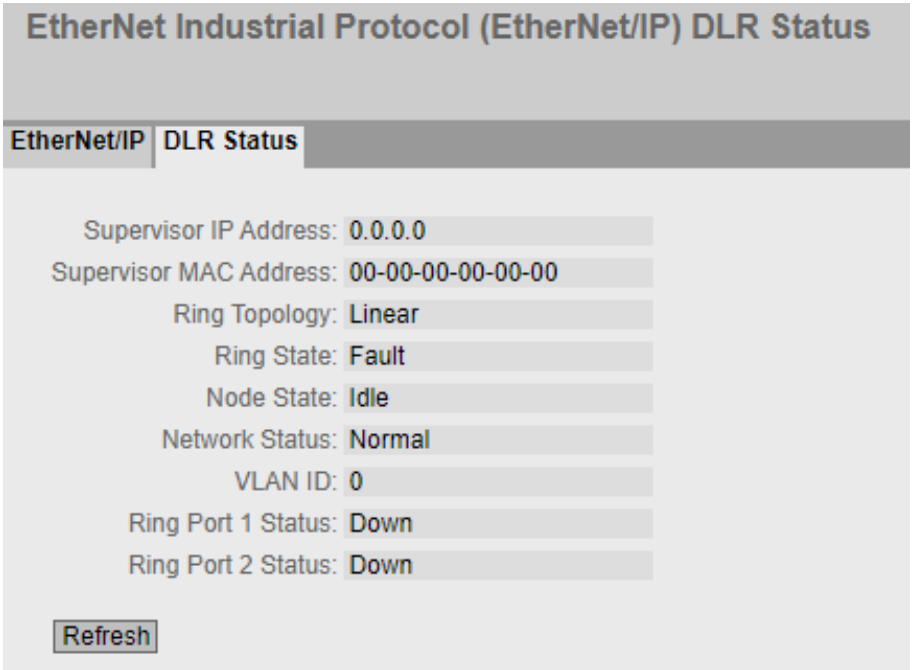
- **EtherNet/IP DLR**
  设置激活（“启用”(Enable)）或取消激活（“禁用”(Disable)）设备级环网 (DLR) 协议。
- **EtherNet/IP DLR 端口 (EtherNet/IP DLR Ports)**
  在下拉列表中选择两个 DLR 端口。
- **以 EtherNet/IP 默认设置重启 (Restart with EtherNet/IP Defaults)**
  单击该按钮可恢复 EtherNet/IP 配置文件的默认设置并重启设备。必须在对话框中确认重启操作。对话框将显示专门针对使用 EtherNet/IP 协议的操作进行的设置。

注意
复位为默认设置后发生数据通信故障 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，设备只能通过串行接口、SINEC PNI 或 DHCP 寻址。 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。

6.4.19.2 DLR 状态 (DLR Status)

设备级环网状态

此页面显示关于设备级环网 (DLR) 协议的信息。无法对该页面上的参数进行组态。



说明

该页面包含以下框：

- **管理器 IP 地址 (Supervisor IP Address)**
  起着 DLR 管理器作用的设备的 IP 地址。
- **管理器 MAC 地址 (Supervisor MAC Address)**
  起着 DLR 管理器作用的设备的 MAC 地址。
- **环型拓扑 (Ring Topology)**
  两个 DLR 端口构成的网络的拓扑。
- **环网状态 (Ring State)**
  显示 DLR 环网是否正常工作。
- **节点状态 (Node State)**
  显示 DLR 管理器的状态。
- **网络状态 (Network Status)**
  显示网络的功能。
- **VLAN ID**
  EtherNet/IP 的 VLAN ID。不支持 VLAN ID“0”。仅当未启用 EtherNet/IP DLR 且未识别任何管理器时，VLAN ID“0”才会显示在 WBM 中。DRL 的 VLAN ID 的组态取决于具体设备：
  - **SCALANCE XR-300WG PoE、型号标识中包含“G”（千兆型）的 SCALANCE XC-200 和 SCALANCE XC216-4C**
    DLR VLAN 与设备的 VLAN 组态无关。
  - **所有其它设备**
    DLR VLAN 取决于设备的 VLAN 组态。
    无论设备组态中是否存在 VLAN，EtherNet/IP DLR 端口都会以 1 到 4095 之间的 ID 值自动添加为所有 VLAN 的成员。在 WBM 中，EtherNet/IP DLR 端口以标签“E”显示在所有现有 VLAN 中。
- **环网端口 1 状态 (Ring Port 1 Status)**
  DLR 端口 1 的端口状态。
- **环网端口 2 状态 (Ring Port 2 Status)**
  DLR 端口 2 的端口状态。

6.4.20 PLUG

6.4.20.1 组态

注意
切勿在运行期间插拔 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。如果在运行期间拔除 PLUG，可能会导致数据丢失。

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“设置值”(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“刷新”(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。

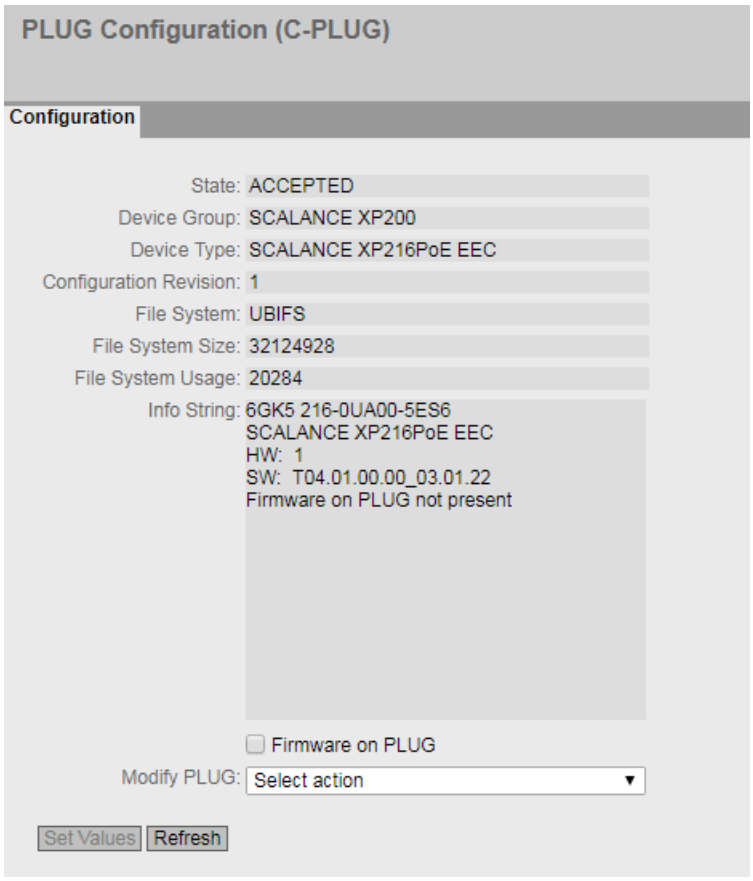
说明

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。此时，设备在安装固件后，将使用出厂设置复位。

在这种情况下，如果在设备中插入了 PLUG，则设备重启后，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。



显示框说明

该表格包括以下行：

- **“状态”(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。

- **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。
- **组态版本 (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。
- **文件系统 (File System)**
  显示 PLUG 上的文件系统类型。
- **文件系统大小 (File System Size)**
  显示 PLUG 上文件系统的最大存储容量（以字节为单位）。
- **文件系统使用情况 (File System Usage)**
  显示 PLUG 文件系统中已使用的存储空间（以字节为单位）。
- **信息字符串 (Infor 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。
- **PLUG 上的固件 (Firmware on PLUG)**
  启用该功能（默认）后，固件将会存储在 PLUG 上。这意味着可通过 PLUG 自动进行固件升级/降级。“信息字符串”(Infor String) 框显示固件是否存储在 PLUG 上。
- **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：
  – 将当前组态写入到 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。
  – 将 PLUG 擦除到出厂默认值
    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. 如需在 PLUG 上保存固件，请选择复选框“PLUG 上的固件”(Firmware on PLUG)。
3. 从“修改 PLUG”(Modify PLUG) 下拉列表中选择所需选项。
4. 单击“设置值”(Set Values) 按钮。

6.4.21 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。

说明

该表格包括以下列：

- **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。

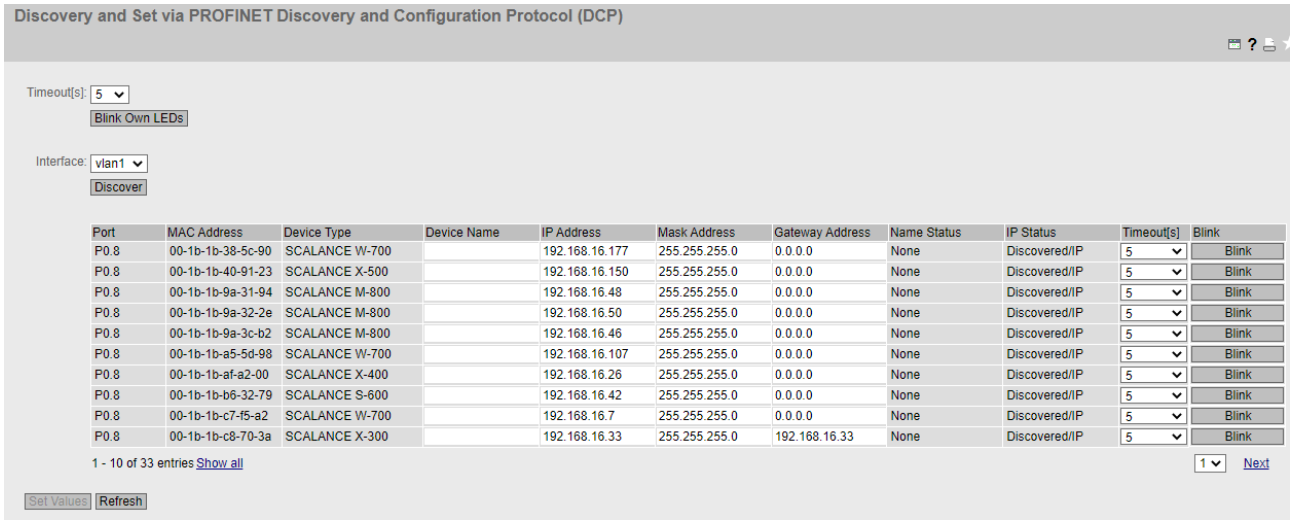
6.4.22 DCP Discovery

在此页面上，可以选择一个接口并搜索可通过该接口访问以及支持 DCP 的设备。DCP Discovery 仅搜索与接口位于同一子网中的设备。并将可访问设备列在表格中。在此表格中，可以检查并调整设备的网络参数。要识别和组态设备，请采用发现组态协议 (DCP)。

说明

DCP Discovery

此功能仅适用于与 TIA 接口相关的 VLAN。可在 System > Agent IP 中组态 TIA 接口。



要求：

要调整网络参数，DCP 需要对设备具有写访问权限。如果访问受到写保护，则无法组态网络参数。

在 SCALANCE 设备上的“System > Configuration”下组态访问。

说明

该页面包含以下框：

- **Timeout[s]**
  选择 LED 闪烁的时间段。
- **Blink Own LEDs**
  启动设备 LED 闪烁。

- **Interface**
  选择所需接口。
- **Discover**
  开始搜索可通过选定接口访问的设备。
  搜索完成后，将可访问设备列在表格中。该表最多列出 100 个条目。

该表格包括以下列：

- **Port**
  显示访问设备所需的端口。
- **MAC Address**
  显示设备的 MAC 地址。
- **Device Type**
  显示设备所属的产品系列或产品组。
- **Device Name**
  如有必要，请更改 PROFINET 设备名称。设备名称必须符合 DNS 标准。
  如果未使用设备名称，则该框为空。
- **IP Address**
  如有必要，请更改设备的 IPv4 地址。
  IPv4 地址在网络中应唯一并与网络匹配。IPv4 地址 0.0.0.0 表示尚未设置 IPv4 地址。
- **Subnet mask**
  如有必要，请更改设备的子网掩码。
- **Gateway Address**
  如有必要，请更改网关的 IPv4 地址。
- **Status Device Name**
  - None：未使用设备名称。
  - Discoverd：使用设置的设备名称。
  - Configured：为设备分配了新的设备名称。
- **IP Status**
  - Discovered/IP：设备使用静态 IPv4 地址。
  - Discovered/DHCP：设备已从 DHCP 服务器获取 IPv4 地址。
  - Configured：为设备分配了新的 IPv4 地址。
- **Timeout[s]**
  指定闪烁时间。经过该时间后，停止闪烁。
- **Blink**
  使所选设备的端口 LED 闪烁。

组态步骤

1. 选择 TIA 接口。
2. 要显示可通过 TIA 接口访问的所有设备，请单击“Discover”按钮。
3. 更改所需的属性。
4. 单击“Set Values”按钮。
   修改后的属性状态更改为“Configured”。
5. 为确保正确应用属性，请再次单击“Discover”按钮。
   修改后的属性状态更改为“Discovered”。

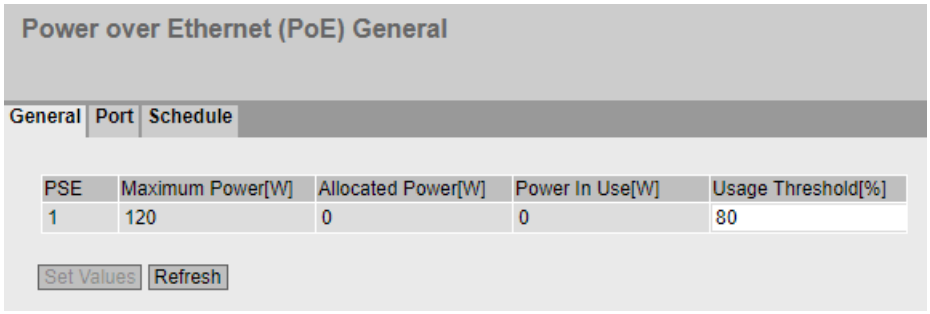
6.4.23 以太网供电 (PoE)

6.4.23.1 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）。



显示框说明

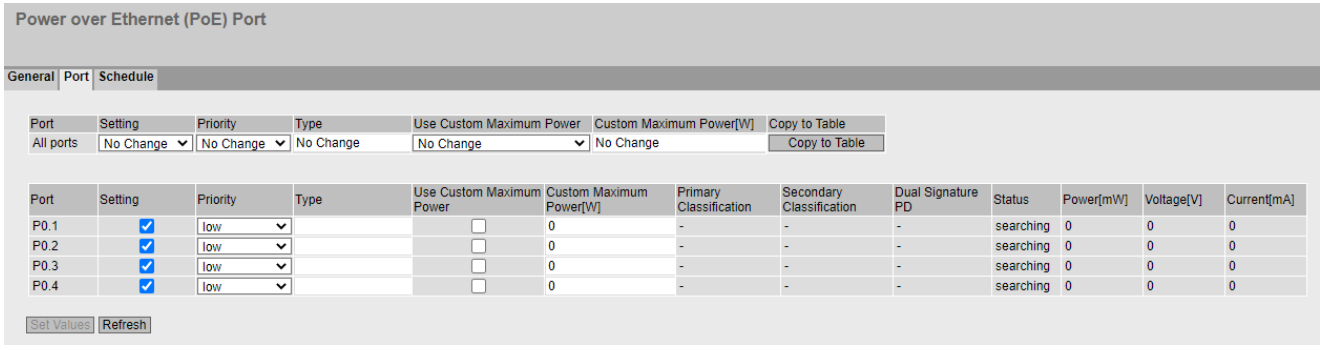
- **PSE（只读）**
  显示 PSE 编号。
- **Maximum Power [W]**
  PSE 为 PoE 设备提供的最大功率。对于设备类型 SCALANCE XR326-2C PoE WG，可组态最大功率；对于其它设备，此框是只读的。
- **Allocated Power [W]（只读）**
  PoE 设备根据“分类”保留的功率总和。

- **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。

6.4.23.2 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用电设备设置优先级。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。



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：

- **端口 (Port)**
  显示设置对于所有端口有效。
- **设置 (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。
- **优先级 (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。

- **类型 (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。
- **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“不变”(No Change)，则表 2 中的条目保持不变
- **复制到表 (Copy to Table)**
  如果单击此按钮，则为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **端口 (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。
- **设置 (Setting)**
  启用对此端口的 PoE 供电或中断供电。
- **优先级 (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)
  – 高 (High)
  – 关键 (Critical)
  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。
- **类型 (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。
- **使用自定义最大功率 (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])**
  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。
  用户定义的功率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。
- **“分类”(Classification)**（只读）
  借助可为标准 IEEE802.af 类型 1 或 IEEE802.at 类型 2 的耗电设备供电的设备。
  分类指定设备的类别。通过该设置可识别设备的最大功率。
- **Primary Classification**（只读）
  通过可为标准 IEEE802.af 类型 1、IEEE802.at 类型 2 或 IEEE802.3bt 类型 3 的耗电设备供电的设备。
  该端口上设备的初级分类。
- **Secondary Classification**（只读）
  通过可为标准 IEEE802.af 类型 1、IEEE802.at 类型 2 或 IEEE802.3bt 类型 3 的耗电设备供电的设备。
  该端口上设备的二级分类。
- **Dual Signature PD**（只读）
  通过可为标准 IEEE802.af 类型 1、IEEE802.at 类型 2 或 IEEE802.3bt 类型 3 的耗电设备供电的设备。
  指定所连接的能源消耗设备是单签名 PD 还是双签名 PD。
  - **“是”(Yes)**
    此端口上设备的电源必须与初级分类和二级分类相对应。
  - **“否”(No)**
    此端口上设备的电源必须与初级分类相对应。

- **“状态”(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。

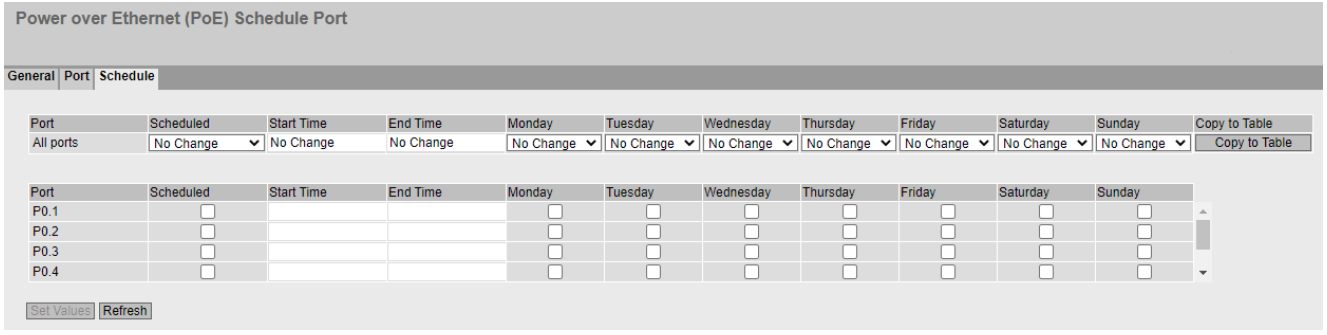
  如果端口的电源不足，则即使在“设置”(Setting) 中启用 PoE，端口的状态仍为“disabled”。这意味着，端口因 PoE 电源管理而禁用。

- **“功率 [mW]”(Power [mW])**（只读）
  显示 SCALANCE 在此端口提供的功率。
- **“电压 [V]”(Voltage [V])**（只读）
  显示施加到此端口的电压。
- **“电流 [mA]”(Current [mA])**（只读）
  显示为连接到此端口的设备提供的电流。

6.4.23.3 计划 (Schedule)

以太网供电 (PoE) 的时间限制

在此页面组态可通过各个 PoE 端口实现供电的时间段。如果耗电设备处于不中断操作状态，可通过此方法降低能耗。



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**
  可能的选项如下：
  - **Enabled**
    会选中表 2 第二列中的所有复选框。
  - **Disabled**
    会取消选中表 2 第二列中的所有复选框。
  - **No Change**
    表 2 中的条目保持不变。
- **Start Time**
  输入通过 PoE 供电的开始时间，格式为 **hh:mm**。如果选择“No Change”，则表 2 中的条目保持不变。
- **End Time**
  输入通过 PoE 供电的结束时间，格式为 **hh:mm**。如果选择“No Change”，则表 2 中的条目保持不变。
  如果结束时间的值小于开始时间的值或两者相同，则在下一个工作日结束 PoE 供电。
- **Monday ... Sunday**
  可能的选项如下：
  - **Enabled**
    会选中表 2 第二列中相应周日对应的所有复选框。
  - **Disabled**
    会取消选中表 2 第二列中相应周日对应的所有复选框。
  - **No Change**
    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**
  选择该复选框时，相应端口仅可在组态的时间段内实现 PoE 供电。
- **Start Time**
  输入通过 PoE 供电的开始时间，格式为 **hh:mm**。
- **End Time**
  输入通过 PoE 供电的结束时间，格式为 **hh:mm**。
- **Monday ... Sunday**
  选择应提供 PoE 供电的周日对应的复选框。

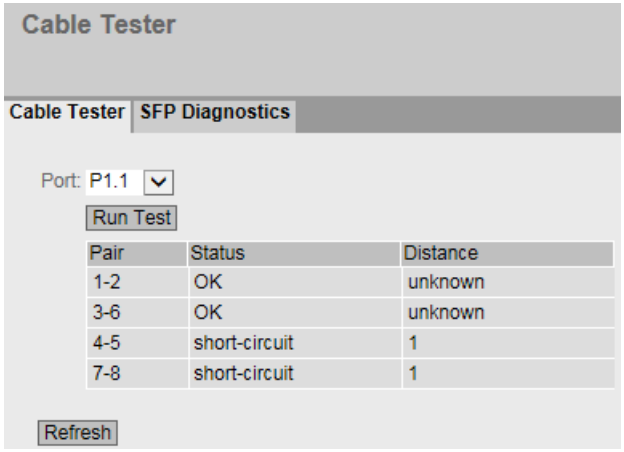
6.4.24 端口诊断

6.4.24.1 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；在这种情况下，需要手动重新建立连接。



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

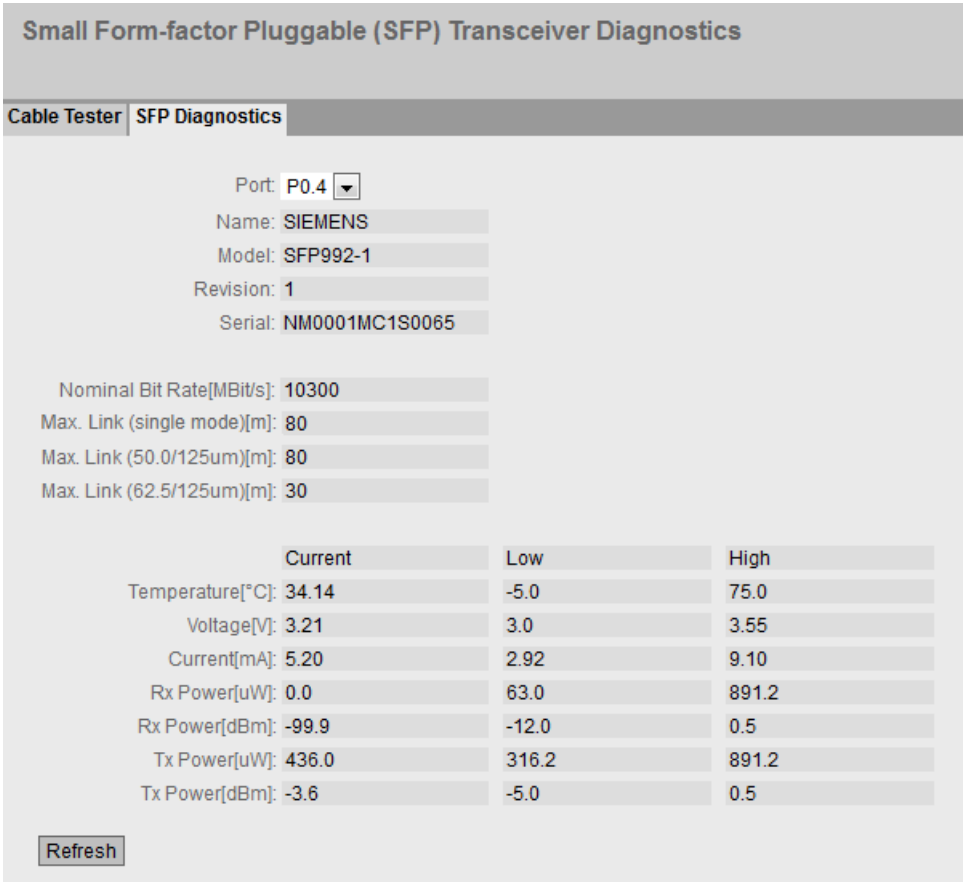
- **状态 (Status)**
  显示电缆的状态。
- **距离 (Distance)**
  显示到开放电缆末端、电缆断线点或短路点的距离（以米为单位）。距离值的允许误差为 +/- 1 m。
  如果状态为“正常”(OK)，则指定长度为“未知”(unknown)。

6.4.24.2 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。

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；在这种情况下，需要手动重新建立连接。



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。
- **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。
- **额定位速率 [Mbps] (Nominal Bit Rate [Mbps]）**
  显示接口的额定位速率。
- **最长链路（单模）[米] (Max. Link (single mode) [m])**
  显示使用此介质时支持的最远距离（单位为米）。
- **最大链路 (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）。
- **最大链路 (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：

说明

显示值与技术规范值的差异

最小和最大发送或接收功率的显示值可能与操作说明中指定的值略有不同。WBM 页面上显示的值是相关的。

- **温度[°C]**
  显示接口的温度。
- **电压[V]**
  显示施加到接口的电压 [V]。
- **电流[mA]**
  显示接口的电流消耗（单位：毫安）。
- **Rx 功率[µW]/Rx 功率[dBm]**
  显示接口的接收功率（单位：微瓦/分贝毫瓦）。
- **Tx 功率[µW]/Tx 功率[dBm]**
  显示接口的发射功率（单位：微瓦/分贝毫瓦）。

- **当前列**
  显示当前值。
- **低列**
  显示最低值。
- **高列**
  显示最高值。

6.5 “Layer 2”菜单

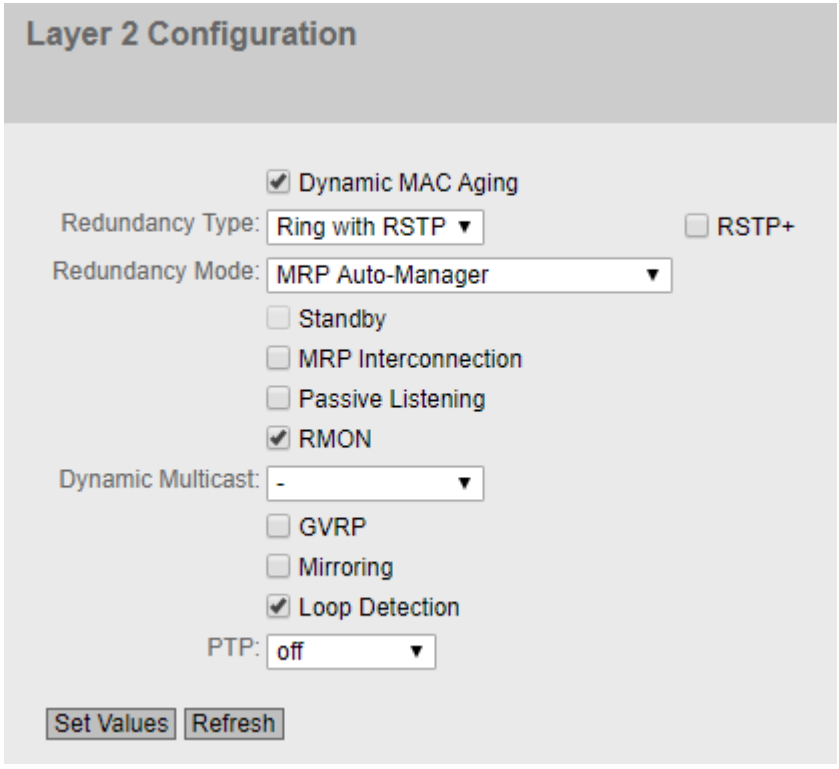
6.5.1 组态

组态第 2 层

在此页面中为第 2 层功能创建基本组态。可在这些功能的组态页面中进行更加详细的设置。也可以在组态页面中检查设置。

说明

显示的参数部分取决于功能或设备。


Layer 2 Configuration
Dynamic MAC Aging
Redundancy Type:
Ring with RSTP
RSTP+
Redundancy Mode:
MRP Auto-Manager
Standby
MRP Interconnection
Passive Listening
RMON
Dynamic Multicast:
-
GVRP
Mirroring
Loop Detection
PTP:
off
Set Values
Refresh

显示框说明

- **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。
- **Redundancy Type**
  可使用以下设置：
  - “-”（禁用）
    禁用冗余功能。
  - Spanning Tree
    如果选择此选项，则可在“Redundancy Mode”下拉列表中指定所需冗余模式。
  - Ring
    如果选择此选项，则可在“Redundancy Mode”下拉列表中指定所需冗余模式。
  - Ring with RSTP
    如果选中此选项，生成树的兼容模式将永久设置为 RSTP。在“Redundancy Mode”下拉列表中，指定环网冗余的冗余模式。
    可在“Ring Redundancy”和“Spanning Tree”菜单中更改当前设置。

    说明

    与具备“Ring with RSTP”选项的端口有关的限制条件

    如果已启用“Ring with RSTP”选项，则生成树中不得包含以下端口：
    - 环网端口
    - 备用端口
    - 备用耦合端口
    - MRP 互连端口
- **RSTP+**
  启用 RSTP+。仅当 MRP 组态为冗余模式时才可选中此复选框。

- **Redundancy Mode**

  如果在“Redundancy Type”下拉列表中选择“Ring”或“Ring with RSTP”，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“Automatic Redundancy Detection”模式下，设备会自动检测环网中是否存在充当“HRP Manager”角色的设备。如果存在，该设备将获得“HRP client”的角色。
  如果未找到 HRP 管理器，则所有设置为“Automatic Redundancy Detection”或“MRP Auto Manager”的设备将通过彼此协商来确定哪台设备将获得“MRP Manager”的角色。MAC 地址最低的设备将始终为“MRP Manager”。其它设备将自动设置为“MRP Client”模式。

  – MRP Auto-Manager
  在“MRP Auto Manager”模式下，设备通过彼此协商来确定哪个设备获得“MRP Manager”的角色。MAC 地址最低的设备将始终为“MRP Manager”。其它设备将自动设置为“MRP Client”模式。
  与“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。

  – MRP Client
  设备采用 MRP 客户端角色。

  – MRP Manager
  设备采用 MRP 管理器角色。设备不能自动采用客户端角色。

  – HRP Client
  设备采用 HRP 客户端角色。

  – 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 Client”或“Automatic Redundancy Detection”。

  如果在“Redundancy Type”下拉列表中选择“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“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“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。如果特定应用不能接受这种情况，需使用较慢的标准生成树机制。

  – MSTP
  启用 Multiple Spanning Tree Protocol (MSTP)。可以在“Layer 2 > Spanning Tree”中组态其它设置。

如果在“Redundancy Type”下拉列表中选择“Ring with RSTP”，则会显示生成树和环网冗余的当前冗余模式。

- **Standby**
  启用或禁用备用冗余功能。可在“Layer 2 > Ring Redundancy”中找到其它设置。
- **MRP Interconnection**
  启用或禁用 MRP 互连功能。可在“Layer 2 > Ring Redundancy > MRP Interconnection”下找到其它设置。只有在满足以下要求时才可启用 MRP 互连：
  – 已启用环网冗余。
  – “MRP 自动管理器”或“MRP 客户端”用作环网冗余模式。
  – 存在已激活的 MRP 互连连接。

  说明
  为每个环网中的两个设备组态环网冗余模式“MRP 自动管理器”(MRP Auto-Manager)，以便其中一个设备发生故障时也能立即重新组态 MRP 环网。
- **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“Information > Ethernet Statistics”中的“Ethernet statistics counter”。
- **Dynamic Multicast**
  可能的设置如下：
  – “-”（禁用）
  – IGMP Snooping
    启用 IGMP (Internet Group Management Protocol)。可以在“Layer 2 > Multicast > IGMP”中组态其它设置。
  – GMRP
    启用 GMRP (GARP Multicast Registration Protocol)。可以在“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 Registration Protocol)。可以在“Layer 2 > VLAN > GVRP”中组态其它设置。
- **Mirroring**
  启用或禁用端口镜像。可以在“Layer 2 > Mirroring”中组态其它设置。
- **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。可以在“Layer 2 > Loop Detection”中找到其它设置。
- **PTP**
  可进行以下设置：
  – off
    设备不转发 PTP 消息。
  – transparent
    设备不会将自身与时间主站同步，但会在时间主站和要同步的从站之间转发 PTP 消息。
  可在“Layer 2 > PTP”下面找到其它设置。

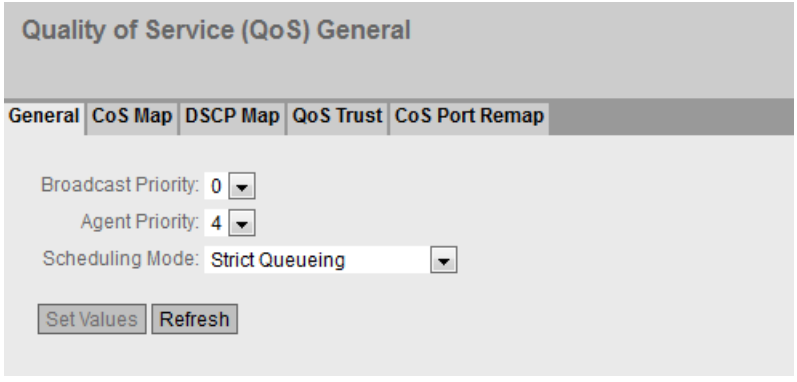
6.5.2 Quality of Service (QoS)

也可参见“技术基础”章节的“服务质量 (页 95)”部分。

6.5.2.1 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。

说明

对于无法设置计划模式的设备，请使用“严格排队”方法。

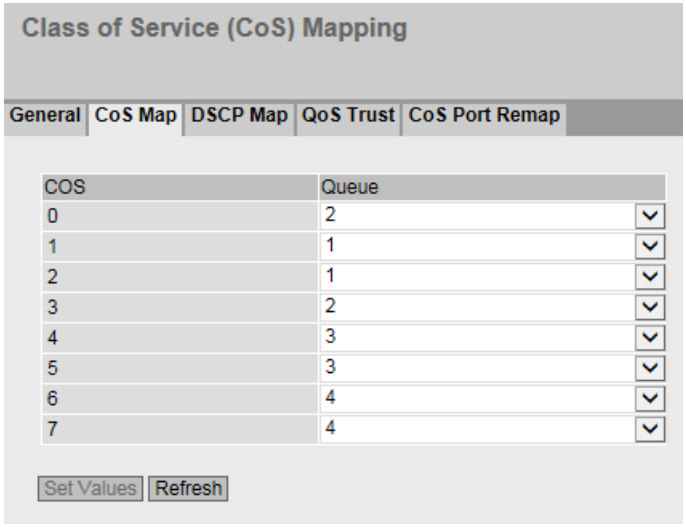
组态步骤

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“设置值”(Set Values) 按钮。

6.5.2.2 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。



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。

服务等级 (CoS) 按如下默认方式分配给各个队列：

COS	具有 4 个队列的设备	具有 8 个队列的设备
0	队列 2	队列 2
1	队列 1	队列 1
2	队列 1	队列 3
3	队列 2	队列 4
4	队列 3	队列 5
5	队列 3	队列 6

COS	具有 4 个队列的设备	具有 8 个队列的设备
6	队列 4	队列 7
7	队列 4	队列 8

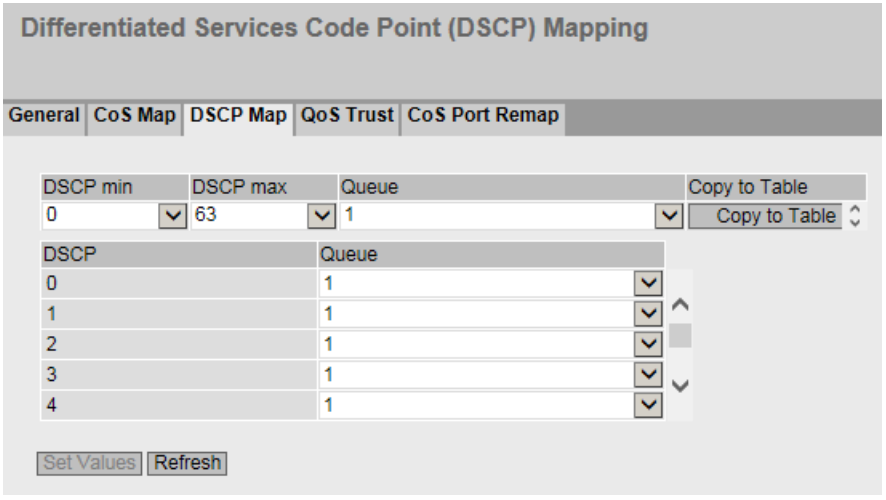
组态步骤

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“设置值”(Set Values) 按钮。

6.5.2.3 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。



显示值说明

表 1 包含以下列：

- **DSCP 最小值 (DSCP min)**
  从该下拉列表中，选择要向其分配队列的 DSCP 编码范围的最小值。
- **DSCP 最大值 (DSCP max)**
  从该下拉列表中，选择要向其分配队列的 DSCP 编码范围的最大值。

- **队列 (Queue)**
  从该下拉列表中，选择要分配给 DSCP 编码范围的转发队列（发送优先级）。
- **复制到表 (Copy to Table)**
  单击此按钮后，选中的转发队列（发送优先级）将分配至指定范围内的 DSCP 编码。

表 2 包含以下列：

- **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	具有 4 个队列的设备
0 - 15	队列 1
16 - 31	队列 2
32 - 47	队列 3
48 - 63	队列 4

DSCP 编码	具有 8 个队列的设备
0 - 7	队列 2
8 - 15	队列 1
16 - 23	队列 3
24 - 31	队列 4
32 - 39	队列 5
40 - 47	队列 6
48 - 55	队列 7
56 - 63	队列 8

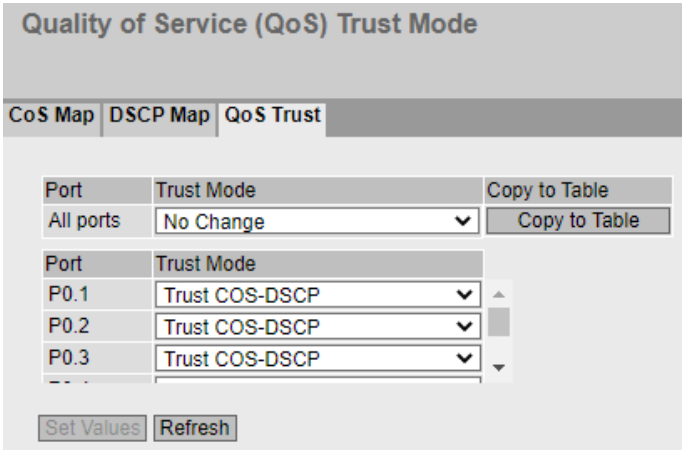
组态步骤

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 “设置值”(Set Values) 按钮。

6.5.2.4 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。



显示值说明

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。
- **信任模式 (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。
- **复制到表 (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“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 > DSCP 映射”(Layer 2 > QoS > DSCP Map) 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 VALN 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 VALN 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 DCSP”(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。

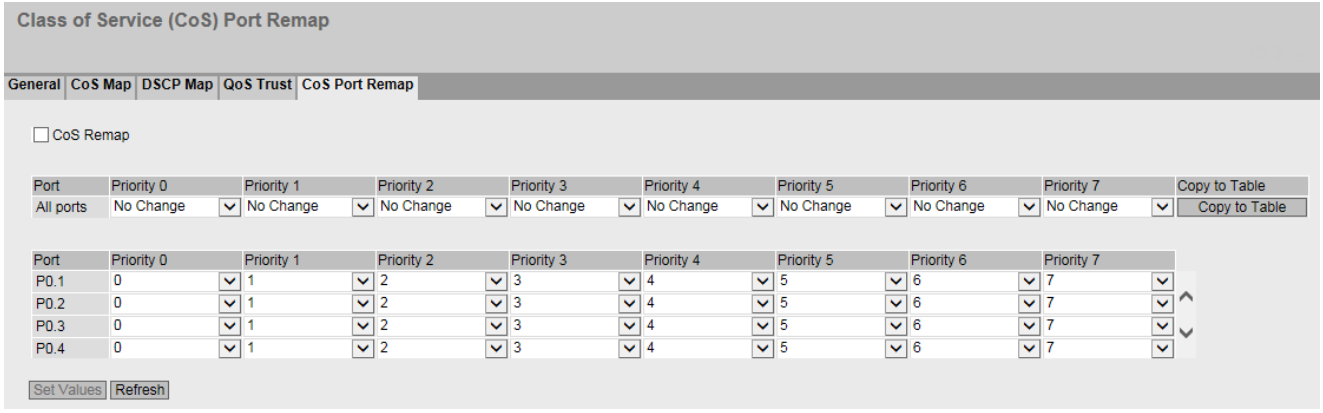
组态步骤

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。

6.5.2.5 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。新优先级仅影响以下接收帧的设备。



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。
  - 不变 (No Change)
    表 2 不变。
- **复制到表 (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。

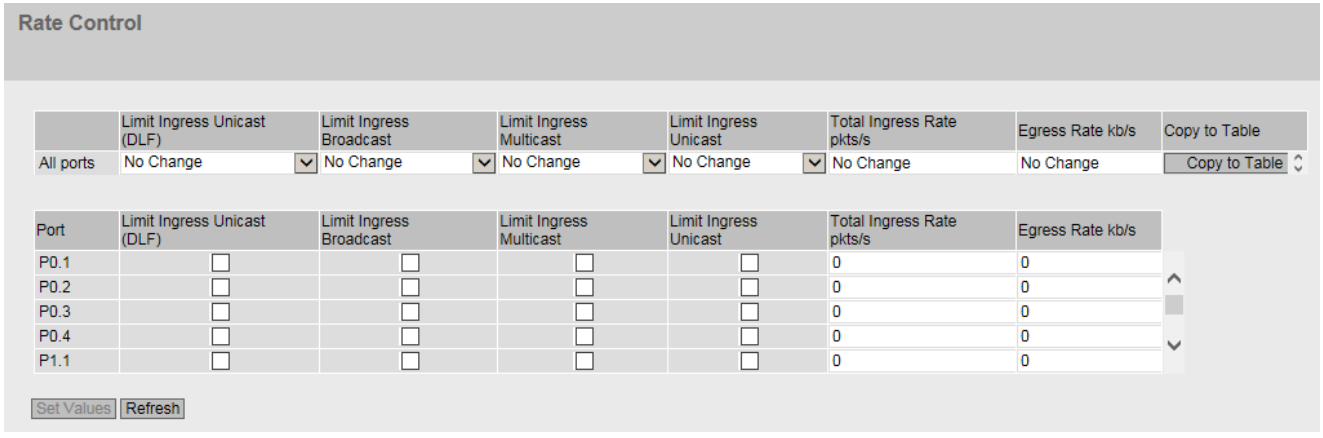
组态步骤

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 “设置值”(Set Values) 按钮。

6.5.3 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。



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/限制入站单播 (Limit Ingress Unicast (DLF)/Limit Ingress Broadcast/Limit Ingress Multicast/Limit Ingress Unicast)**
  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
- **复制到表 (Copy to Table)**
  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：

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

- **总入站速率 kb/s (Total Ingress Rate kb/s)**
  指定所有入站帧的数据速率。

  说明

  仅当至少已为相关端口选中以下列中的一个复选框时，设备才会将数据通信限制为输入的值：
  - 限制入站广播 (Limit Ingress Broadcast)
  - 限制入站组播 (Limit Ingress Multicast)
  - 限制入站单播 (Limit Ingress Unicast)

  如果未选中任何复选框，则即使“总入站速率 pkts/s”(Total Ingress Rate pkts/s) 字段中有一个条目，传入数据通信也不会受到限制。如果选中了多个复选框，则所有激活类别的数据包总数对于限制数据通信起决定性作用。

- **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。

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。

6.5.4 VLAN

6.5.4.1 常规

VLAN 组态页面

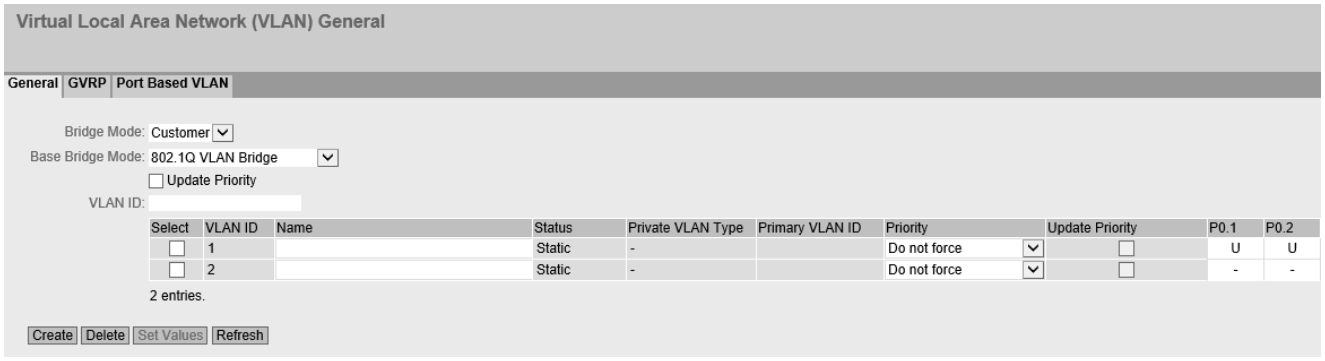
在该页面，可以指定设备是否以透明方式转发带有 VLAN 标记的帧（IEEE 802.1D/VLAN 不识别模式），或者指定设备是否考虑 VLAN 信息（IEEE 802.1Q/VLAN 识别模式）。如果设备处于“802.1Q VLAN Bridge”模式下，则可以定义 VLAN 并指定端口的使用。

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。



显示框说明

该页面包含以下框：

- **网桥模式 (Bridge Mode)**
  选择设备的角色。以下角色可选：
  - Customer
    如果以“Customer”角色操作设备，则设备与标准以太网交换机的功能相同。
  - Provider
    如果以“Provider”角色操作设备，除了“Customer”角色属性外，该设备还可提供用于管理外部 VLAN 标签的选项。在此角色中，可使用 Q-in-Q VLAN 隧道功能。

    说明

    提供商角色会对 VLAN 标签产生以下影响：所有未从访问端口发送的数据包都会收到一个 VLAN 标签。如果其它设备的 VLAN 组态未相应调整，则可能形成网络环路或无法再访问网段。

- **“基础网桥模式”(Base Bridge Mode)**

  说明

  切换“基础网桥模式”(Base Bridge Mode)

  请参见本节中的“切换基础网桥模式”段落。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，不会更改 VLAN 标记，而会以透明方式转发这些标记。为 CoS 评估 VLAN 优先级。在此模式下，无法创建任何 VLAN。仅管理 VLAN 可用：VLAN 1。

- **“更新优先级”(Update Priority)**
  选中此复选框后，“优先级”(Priority) 列中的值即作为新的“服务等级”(Class of Service) 输入到此 VLAN 所有传入帧的 VLAN 变量中。

- **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被分配一次，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。
- **私有 VLAN 类型 (Private VLAN Type)**
  显示 PVLAN 的类型。
- **“主要 VLAN ID”(Primary VLAN ID)**
  对于次要 PVLAN，显示对应的主要 PVLAN 的 ID。
- **优先级 (Priority)**
  选择一个优先级应用到此 VLAN 的所有传入帧中，以作为新的服务等级 (CoS)。无论端口优先级或者无标记帧中的优先次序如何，交换机都会根据选定的优先级进一步处理帧。帧中包含的 VLAN 标签不会更改。
  如果选择“非强制”(Do not force)，帧的优先级将保持不变。根据端口优先级或 VLAN 标签确定帧的优先顺序。

- **“更新优先级”(Update Priority)**
  该列在所有 VLAN 的页面开头显示“更新优先级”(Update Priority) 复选框的状态。无法进行特定于某个 VLAN 的设置。
- **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”(Base Bridge Mode)

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）

若将“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。
- 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。
- 不可组态端口类型。
- 定义的访问规则必须适用于所有 VLAN。在“安全 > 管理 ACL”(Security > Management ACL) 页面上，必须为参数“允许 VLAN ”(VLANs Allowed) 定义值“1-4094”。

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）。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

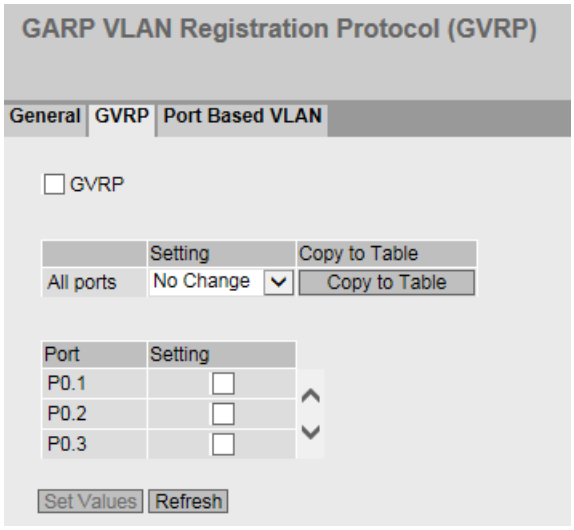
1. 如果未设置“802.1Q VLAN 网桥”(802.1Q VLAN Bridge)，则从下拉列表中选择“802.1Q VLAN 网桥”(802.1Q VLAN Bridge)。单击“设置值”(Set Values) 按钮。
2. 在“VLAN ID”输入框中输入 ID。
3. 单击“创建”(Create) 按钮。会在表中生成一个新条目。默认情况下，各个框均输入“-”。
4. 如果适用，输入 VLAN 的名称。
5. 指定 VLAN 中端口的使用。例如，如果选择“M”，则该端口是 VLAN 的成员。此 VLAN 中发送的帧在转发时带有相应 VLAN 标记。
6. 单击“设置值”(Set Values) 按钮。

6.5.4.2 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。



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

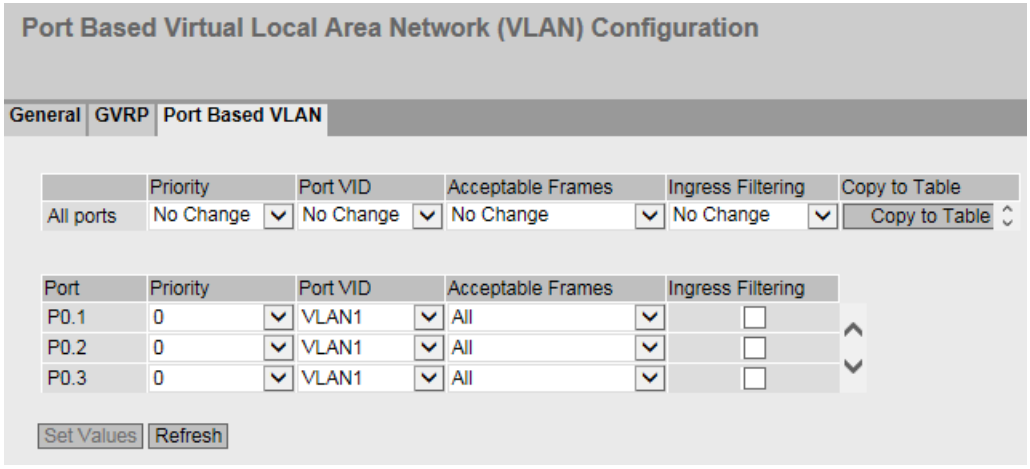
1. 单击“GVRP”复选框。
2. 单击“Setting”(Setting) 列中端口之后的复选框以启用或禁用此端口的 GVRP。
   对需要启用或禁用此功能的每个端口重复此操作。
3. 单击“设置值”(Set Values) 按钮。

6.5.4.3 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。



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。
- **复制到表 (Copy to Table)**
  单击此按钮后，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。
  - 仅限无标记和带优先级标记 (Untagged and Priority Tagged Only)
    设备会丢弃所有带标记的帧，而转发所有无标记帧及具备优先级的帧（带优先级标记的帧）。否则，按照组态应用转发规则。
    如果已组态网桥模式“Provider”，则表示设备将所有传入帧按无标记帧处理。
- **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

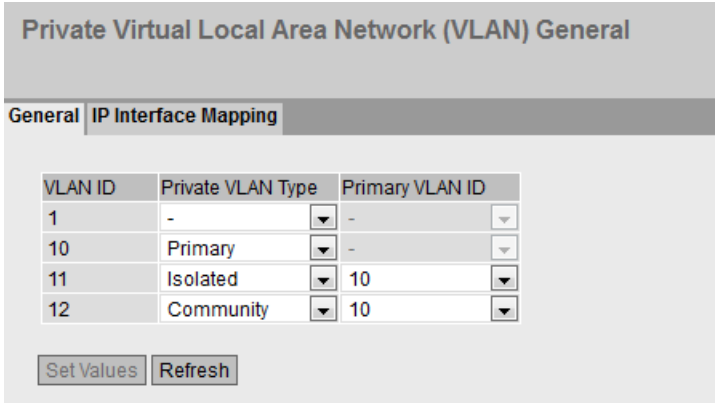
1. 在待组态端口的行中，单击表格中的相关单元格进行组态。
2. 在以下输入框中输入要设置的值。
3. 从下拉列表中选择要设置的数值。
4. 单击“设置值”(Set Values) 按钮。

6.5.5 Private VLAN

6.5.5.1 常规

私有 VLAN 组态页面

在此页面上定义 PVLAN 的类型并将辅助 PVLAN 分配给主 PVLAN。



显示框说明

该表格包括以下列：

- **VLAN ID**
  显示 VLAN ID。
- **私有 VLAN 类型 (Private VLAN Type)**
  指定 PVLAN 的类型：
  - -
    这些 VLAN 不是私有 VLAN。
  - Primary
    对于该类型，定义主 PVLAN。在 PVLAN 中，只能定义一个主 PVLAN。主 PVLAN 使用 VLAN 的 VLAN ID。
  - Isolated
    对于该类型，定义辅助 PVLAN。隔离次 PVLAN 内的各设备之间不能通过第 2 层进行通信。辅助 PVLAN 具有特定的 VLAN ID。
  - Community
    对于该类型，定义辅助 PVLAN。此辅助 PVLAN 内的各设备彼此之间可直接通过第 2 层进行通信。辅助 PVLAN 具有特定的 VLAN ID。
- **主 VLAN ID (Primary VLAN ID)**
  对于辅助 PVLAN，选择主 PVLAN 的 VLAN ID。

组态步骤

1. 在“第 2 层 > VLAN > 常规”(Layer 2 > VLAN > General) 页面上创建所需的 VLAN。

   说明

   所有辅助 PVLAN 在 PVLAN 的全部工业以太网交换机上必须已知。即使工业以太网交换机在辅助 PVLAN 中没有主机端口，辅助 PVLAN 也必须在工业以太网交换机上已知。

2. 切换至页面“第 2 层 > 私有 VLAN > 常规”(Layer 2 > Private VLAN > General)。在此为每个 VLAN 创建一行。
3. 在此页面中指定“私有 VLAN 类型”。
4. 单击“设置值”(Set Values) 按钮。
5. 对于辅助 PVLAN，指定对应的主 PVLAN。
6. 单击“设置值”(Set Values) 按钮。
7. 选择所需的端口，具体可在“系统 > 端口 > 组态”(System > Ports > Configuration) 页面上选择相应的端口类型：
   - 交换机端口 PVLAN 混合 (Switch-Port PVLAN Promiscuous)
   - 交换机端口 VLAN 主机 (Switch Port VLAN Host)
8. 在“第 2 层 > VLAN > 常规”(Layer 2 > VLAN > General) 页面上指定端口的用途。
   - 对于连接其它混合端口的混合端口，在所有 PVLAN 中选择设置“M”。
   - 对于连接终端设备的混合端口，在所有 PVLAN 中选择设置“u”（小写）。
     在主 PVLAN 中，该设置在保存后自动更改为“U”（大写）。
   - 对于主 PVLAN 及其辅助 PVLAN 中的主机端口，选择设置“u”（小写）。
     在其辅助 PVLAN 中，该设置在保存后自动更改为“U”（大写）。

   对于入站无标记帧，通过输入采用设置“U”（大写）的端口来设置 VLAN 的端口 VLAN-ID。

6.5.5.2 IP 接口映射

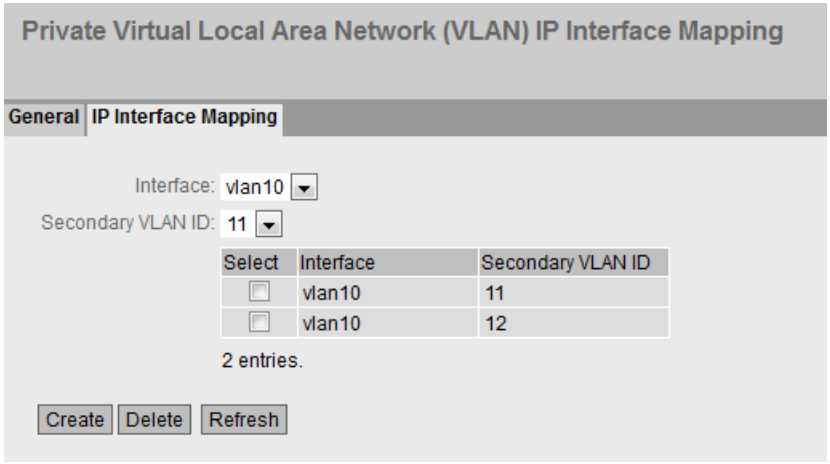
私有 VLAN 组态页面

在此页面上指定可访问主 PVLAN 的 IP 接口的辅助 PVLAN。

为所有相关功能组态 IP 接口分配，终端设备在使用这些功能时需要通过辅助 PVLAN 与主 PVLAN 的 IP 接口通信。

示例：

- 将辅助 PVLAN 中的某个终端设备组态为 DHCP 客户端。设置远程 DHCP 服务器。将 PVLAN 交换机组态为 DHCP 中继代理。在 DHCP 中继代理的主 PVLAN 中组态 IP 接口。将包含 DHCP 客户端的次要 PVLAN 分配给此 IP 接口。
- 将 PVLAN 交换机组态为路由器。在路由器的主 PVLAN 中组态 IP 接口。将包含终端设备（使用路由器作为网关）的次要 PVLAN 分配给此 IP 接口。



显示框说明

该页面包含以下框：

- **Interface**
  选择带 IP 接口的主 PVLAN。
- **Secondary VLAN ID**
  选择可访问主 PVLAN 的 IP 接口的辅助 VLAN ID。

该表格包括以下列：

- **Select**
  选择要删除的行。
- **Interface**
  显示 IP 接口。
- **Secondary VLAN-ID**
  显示可访问主 PVLAN 的 IP 接口的辅助 PVLAN 的辅助 VLAN-ID。

组态步骤

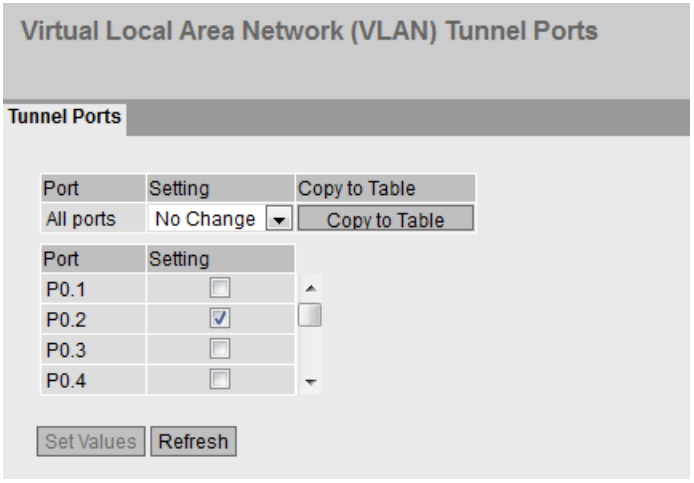
1. 为主 PVLAN 创建 IP 接口。
2. 选择带 IP 接口的主 PVLAN。
3. 选择辅助 VLAN ID。
4. 单击“Create”按钮。

6.5.6 提供商网桥

6.5.6.1 隧道端口

通道端口的组态页面

在此页面上，可启用 Q-in-Q VLAN 隧道功能。用外部 VLAN 标记（端口的 PVID）扩展隧道端口接收到的帧。



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：
  - Enabled
    启用所有端口的 Q-in-Q VLAN 隧道功能。
  - Disabled
    禁用所有端口的 Q-in-Q VLAN 隧道功能。
  - No Change
    表 2 保持不变。
- **Copy to Table**
  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**
  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。
- **Setting**
  为此端口启用或禁用该功能。

组态步骤

要组态一个端口作为隧道端口，请按以下方式操作：

1. 切换至页面“Layer 2 > VLAN > General”。
2. 组态 Bridge mode“Provider”。
3. 单击“Set Values”按钮。
   第 2 层端口设置（VLAN，生成树）恢复为出厂设置且设备重启。
4. 切换至页面“Layer 2 > VLAN > General”。
5. 输入所需 VLAN ID。
6. 单击“Create”按钮。
7. 切换至页面“Layer 2 > VLAN > Port Based VLAN”。
8. 对于该端口，选择所创建 VLAN 的端口 VID。
9. 对于“Acceptable Frames”中的端口，选择设置“Untagged and Priority Tagged Only”。
10. 单击“Set Values”按钮。
11. 切换至页面“Layer 2 > VLAN > Port Mapping”。
12. 对于所需 VLAN 中的端口，请选择设置“U”（大写）。
13. 对于所有其它 VLAN 中的端口，请选择设置“-”。
14. 单击“Set Values”按钮。
15. 禁用端口上的以下协议：
    - 在页面“Layer 2 > VLAN > GVRP”，选择“Setting”旁的复选框。
    - 在页面“Layer 2 > Spanning Tree > CIST Port”，选择“Spanning Tree”旁的复选框。
    - 在页面“Layer 2 > Multicast > GMRP”，选择“Setting”旁的复选框。
16. 切换至页面“System > Ports > Configuration”
17. 选择所需端口。
18. 选择 port type“Switch-Port VLAN Access”。
19. 单击“Set Values”按钮。
20. 切换至页面“Layer 2 > Provider-Bridge > Tunnel-Ports”。
21. 选择所需端口的复选框。
22. 单击“Set Values”按钮。
    在“Layer 2 > VLAN > Port Mapping”页面，该设置在保存后会自动切换回“Q”。

6.5.7 镜像

6.5.7.1 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。

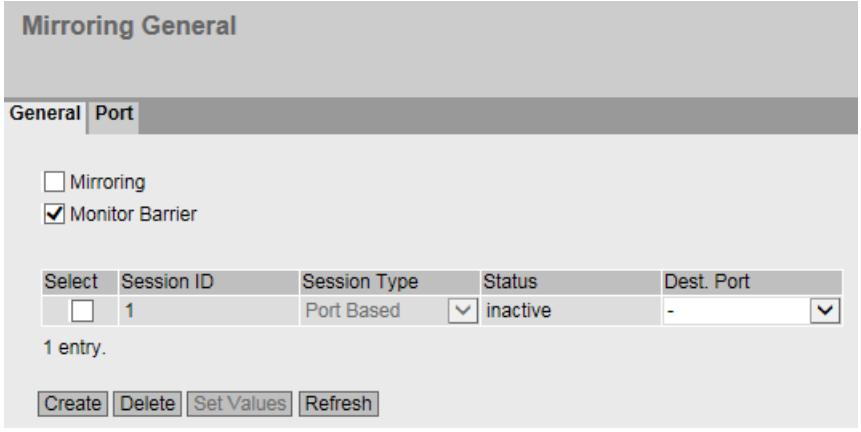
注意数据传输率

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



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。
- **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。

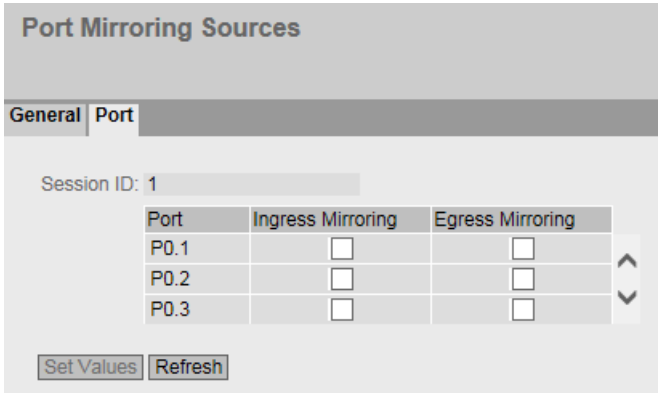
删除镜像会话

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。

6.5.7.2 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。



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。

- **入站镜像 (Ingress Mirroring)**
  启用或禁用监听所需端口的入站数据包。
- **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。

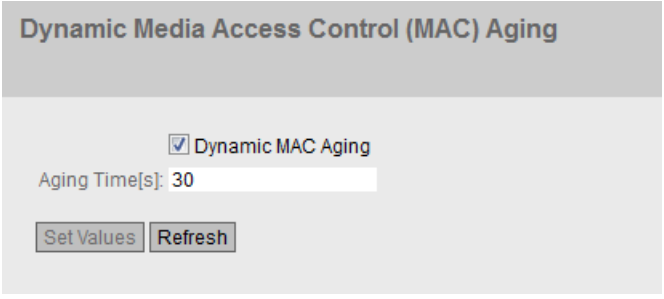
6.5.8 Dynamic MAC Aging

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：

- **Dynamic MAC Aging**
  启用或禁用学习的 MAC 地址的动态老化功能。
- **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

当输入老化时间时，请注意该值会取整为正确的值。如果输入的值不能被 15 整除，则会自动向下取整。

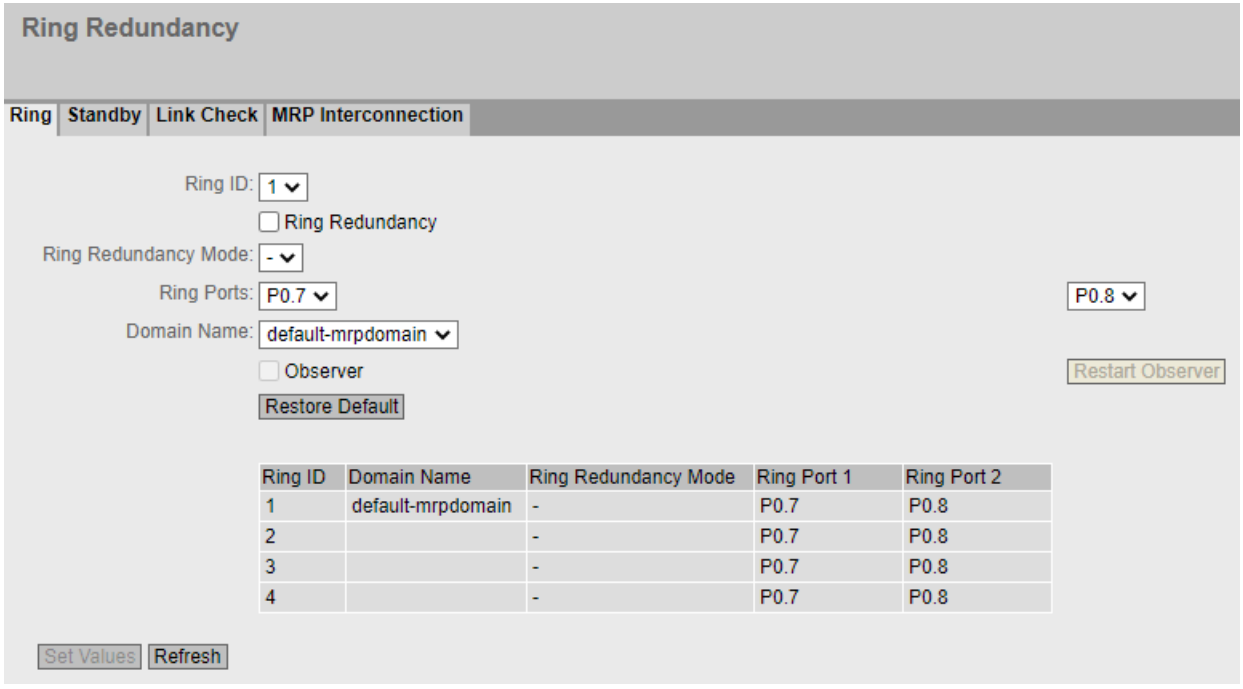
组态步骤

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。

6.5.9 环网冗余

6.5.9.1 环网

组态环网冗余



- **环网 ID (Ring ID)**
  选择要组态的环网的 ID。
- **环网冗余 (Ring Redundancy)**
  如果选中“环网冗余”(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。

  说明

  如果组态多个冗余环网，需要为每个环网选择“MRP Manager”环网冗余模式。

  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“Automatic Redundancy Detection”模式下，设备会自动检测环网中是否存在充当“HRP Manager”角色的设备。如果存在，该设备将获得“HRP client”的角色。
    如果未找到 HRP 管理器，则所有设置为“Automatic Redundancy Detection”或“MRP Auto Manager”的设备将通过彼此协商来确定哪台设备将获得“MRP Manager”的角色。MAC 地址最低的设备将始终为“MRP Manager”。其余设备将自动设置为“MRP Client”模式。
  – MRP Auto-Manager
    在“MRP Auto Manager”模式下，设备通过彼此协商来确定哪个设备获得“MRP Manager”的角色。MAC 地址最低的设备将始终为“MRP Manager”。其余设备将自动设置为“MRP Client”模式。
    与“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。
  – MRP Client
    设备采用 MRP 客户端角色。
  – HRP Client
    设备采用 HRP 客户端角色。
  – MRP Manager
    设备采用 MRP 管理器角色。设备不能自动采用客户端角色。
  – 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 Client”或“Automatic Redundancy Detection”。

- **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。

说明

环网端口的代理 VLAN ID

需要为环网端口组态“Agent VLAN ID”。因此，也可以为环网端口组态值范围为 1 到 4094 的 VLAN ID。

在左侧下拉列表中选择的环网端口是 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
XB208 XB216	P0.1 和 P0.2
XB205-3	P0.7 和 P0.8
XB206-2	P0.7 和 P0.8
XB213-3	P0.15 和 P0.16

设备	环网端口出厂设置
XC206-2G PoE XC206-2G PoE EEC XC206-2SFP XC206-2SFP G XC206-2SFP EEC XC206-2SFP G EEC XC208 XC208G XC208EEC XC208G EEC XC208G PoE XC216 XC216EEC XC216-4C XC216-4C G XC216-4C G EEC XC224 XC224-4C G XC224-4C G EEC	P0.1 和 P0.2
XC216-3G PoE	P0.4 和 P0.5
XC206-2	P0.7 和 P0.8
XF-200BA	P1.1 和 P2.1
XF204G	P0.1 和 P0.2
XP208	P0.1 和 P0.2
XP216	P0.10 和 P0.12
XR324WG XR328-4C WG (GE)	P0.1 和 P0.2
XR326-2C PoE WG XR328-4C WG	P0.25 和 P0.26

面向端口数多于 8 个的设备的端口组

MRP 环网的环网端口应属于同一个逻辑端口组。

XB-200

设备	订货号	端口组
SCALANCE XB216	6GK5 216-0BA00-2AB2 6GK5 216-0BA00-2TB2	**组 1** 端口 1 ... 端口 8
SCALANCE XB213-3 (SC)	6GK5 213-3BD00-2AB2 6GK5 213-3BD00-2TB2	**组 2** 端口 9 ... 端口 16
SCALANCE XB213-3 (ST/ BFOC)	6GK5 213-3BB00-2AB2 6GK5 213-3BB00-2TB2	
SCALANCE XB213-3LD	6GK5 213-3BF00-2AB2 6GK5 213-3BF00-2TB2	

XC-200

设备	订货号	端口组
SCALANCE XC216	6GK5 216-0BA00-2AC2	**组 1**
SCALANCE XC216 EEC	6GK5 216-0BA00-2FC2	端口 1 ... 端口 4 端口 9 ... 端口 12 **组 2** 端口 5 ... 端口 8 端口 13 ... 端口 16
SCALANCE XC224	6GK5 224-0BA00-2AC2	**组 1** 端口 1 ... 端口 8 **组 2** 端口 9 ... 端口 12 端口 17 ... 端口 20 **组 3** 端口 13 ... 端口 16 端口 21 ... 端口 24

XP-200

设备	订货号	端口组
SCALANCE XP216	6GK5 216-0HA00-2AS6	**组 1**
SCALANCE XP216	6GK5 216-0HA00-2TS6	端口 1 ... 端口 5，端口 7
SCALANCE XP216 EEC	6GK5 216-0HA00-2ES6	**组 2**
SCALANCE XP216 PoE EEC	6GK5 216-0UA00-5ES6	端口 6、端口 8、端口 9、 端口 11、端口 13、端口 15 **组 3** 端口 10、端口 12 端口 14、端口 16

XR-300WG

设备	订货号	端口组
SCALANCE XR324WG	6GK5 324-0BA00-2AR3	**组 1**
SCALANCE XR324WG	6GK5 324-0BA00-3AR3	端口 1 ... 端口 4 端口 13 ... 端口 16 **组 2** 端口 5 ... 端口 8 端口 17 ... 端口 20 **组 3** 端口 9 ... 端口 12 端口 21 ... 端口 24
SCALANCE XR328-4C WG	6GK5 328-4FS00-2AR3	**组 1**
SCALANCE XR328-4C WG	6GK5 328-4FS00-2RR3	端口 1 ... 端口 4
SCALANCE XR328-4C WG	6GK5 328-4FS00-3AR3	端口 13 ... 端口 16
SCALANCE XR328-4C WG	6GK5 328-4FS00-3RR3	**组 2**
SCALANCE XR328-4C WG	6GK5 328-4SS00-2AR3	端口 5 ... 端口 8
SCALANCE XR328-4C WG	6GK5 328-4SS00-3AR3	端口 17 ... 端口 20 **组 3** 端口 9 ... 端口 12 端口 21 ... 端口 24 **组 4** 端口 25 ... 端口 28

说明

转发 RSPAN 流

如果设备要转发 RSPAN 流，必须满足两个要求：

- 输入端口和输出端口必须属于同一个端口组。
- 对于输入端口，必须禁用“学习”功能。
  在 WBM 中：“系统 > 端口 > 组态 > 单播 MAC 学习”(System > Ports > Configuration > Unicast MAC Learning)
  在 CLI 中：no unicast mac learning

H-Sync

H-Sync 是第 2 层协议，在冗余控制系统中可基于该协议通过 PROFINET 同步过程数据。对于 SIMATIC S7-1500R：

这两个控制器通过 MRP 环网冗余连接，且必须在一条路径上彼此直接连接相连。同时，两个控制器均组态为“MRP Auto-Manager”，因此其中一个控制器为 MRP 管理器。环网中的所有其它设备为 MRP 客户端。这两个控制器在环网的两个方向上发送 H-Sync 帧 (Provider)。设备接收到的 H-Sync 帧不会被转发 (Consumer)。环网中的所有其它设备仅转发环网端口两个方向之间的 H-Sync 帧 (Forwarder)。在所有其它端口上对 H-Sync 帧进行过滤。

H-Sync 是工业以太网交换机的一种透明协议。有关可用作 H-Sync 转发方的工业以太网交换机的信息，请参见“系统功能和硬件设备”部分。

只能通过 STEP 7 Basic 或 Professional 组态 H-Sync。但请注意，不符合以下规则的设置可能会导致组态混乱：

– 冗余模式：MRP 客户端

- **域名 (Domain Name)**
  从下拉列表中选择域名。每个名称只能分配给一个环网。

说明

如果组态多个冗余环网，则不能为任何环网使用“default-mrpdomain”域名。

- **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的环网端口连接到 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。

- **恢复默认设置 (Restore Default)**
  此按钮仅在多个冗余环网处于活动状态时有效。单击该按钮可将环网冗余组态复位为出厂设置。
- **DNA 冗余 (DNA Redundancy)**
  启用/禁用 DNA 冗余。只有在满足以下要求时才可启用 DNA 冗余：
  – 已启用环网冗余。
  – 将“MRP 管理器”(MRP Manager) 或“MRP 客户端”(MRP Client) 组态为“环网冗余模式”(Ring Redundancy Mode)。
  DNA 冗余仅适用于 MRP。

说明

可以在“技术基础知识 → 冗余机制 → 双网接入冗余（DNA 冗余）”一节中找到 DNA 冗余的组态的详细分步描述。

该表格包括以下列：

- **环网 ID (Ring ID)**
  环网的 ID。
- **域名 (Domain Name)**
  冗余域的名称。
- **环网冗余模式 (Ring Redundancy Mode)**
  该环网中使用的冗余模式。如果显示“-”，说明环网冗余未启用。
- **环网端口 1 (Ring Port 1)**
  环网的第一个环网端口。
- **环网端口 2 (Ring Port 2)**
  环网的第二个环网端口。

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 / 工业以太网型号

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。

6.5.9.2 备用

环网冗余链路

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。

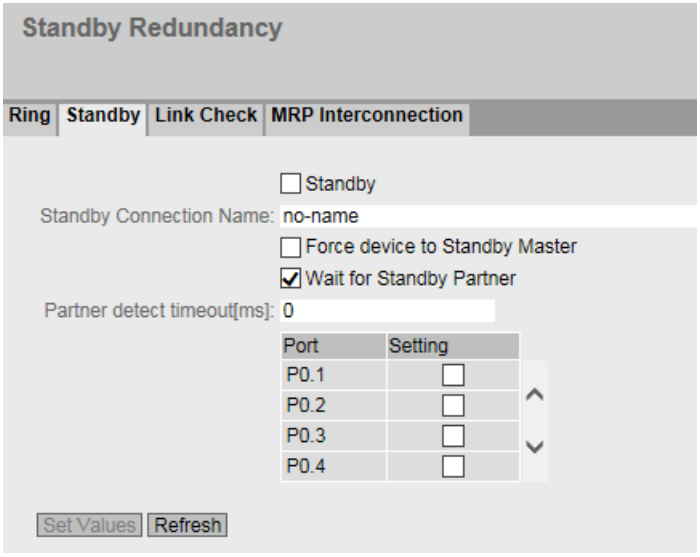
对于“备用连接名称”(Standby Connection Name)，必须为两个伙伴指定一个在环网中唯一的名称。该名称标识彼此为备用伙伴的两个模块。

说明

为了能够使用此功能，必须激活 HRP。

说明

当线路拓扑中的备用主站和备用从站的连接在中断后恢复时，可能会暂时出现数据通信增加的情况。



显示框说明

- **Standby**
  启用或禁用备用功能。

  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。

- **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。

- **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

  如果在备用耦合的两个设备上均启用了选项“将设备强制为备用主站”(Force device to Standby Master)，则会导致帧循环，进而造成数据通信失败。因此，只能在备用耦合的一个设备上启用“将设备强制为备用主站”(Force device to Standby Master)。

- **等待备用伙伴 (Wait for Standby Partner)**
  – 启用
    只在备用主站和备用从站以及它们的备用伙伴建立连接后才启用备用连接。这可确保在启用通过备用连接实现的通信之前，冗余连接真正可用。
  – 禁用
    即使备用主设备未与备用从设备建立连接，也启用备用连接。
    如果已启用另一个备用连接，则会导致帧循环传送以及数据通信失败。例如，如果将不同的备用连接名称分配给备用主站和备用从站，则会因组态错误而产生多个备用连接。

- **“伙伴检测超时 [ms]”(Partner detect timeout [ms])**
  仅在取消选中“等待备用伙伴”(Wait for Standby Partner) 复选框时才会显示此输入框。在这种情况下，可以定义设备在建立备用连接之前等待的时间。经过此时间段后，即使备用主设备未与备用从设备建立连接，也启用备用连接。

- **端口 (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。

6.5.9.3 链路检查

要求

说明

更改组合端口的介质类型：光纤 → 电气

如果为介质类型是“SFP”的组合端口激活了链路检查，并且想要启用“RJ45”介质类型，请先禁用链路检查。

- 请勿以 10 Gbps 速率启用端口上的链路检查。
- 只能使用 HRP 或 MRP 环网的光纤环网端口启用链路检查功能。
- 必须在一个 HRP 或 MRP 环网内的两个相邻设备（连接伙伴）上启用链路检查。
- 启用链路检查的端口必须处于连接状态。
- 链路检查不适用于多个环网。仅当没有其它环网处于活动状态时，才能在 ID 为 1 的环网中启用链路检查。

监视环网中的光纤连接

通过链路检查功能，可监视 HRP 或 MRP 环网内光纤部分的传输质量，确认故障连接以及在某些情况下将其关闭。故障部分关闭后，冗余管理器可以关闭环网并恢复通信。

注意
确保链路检查时用于监视光纤连接的帧不会被网络中高优先级帧的过载所取代。 以下原因可导致高优先级帧过载，例如： • 可导致高优先级帧重复的网络回路。 • 更改转发帧的优先级

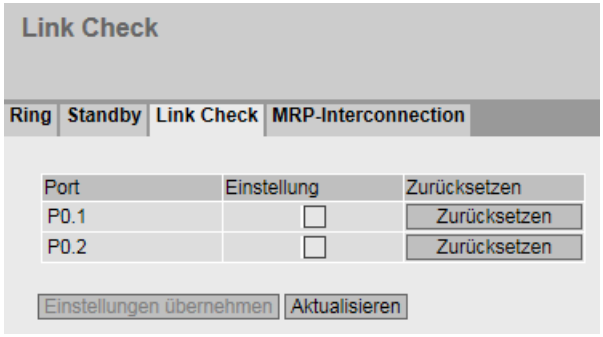
说明

请勿仅为两个连接伙伴中的一个启用链路检查。否则会导致错误的行为。

说明

如果在一个环网的所有设备上同时启用了链路检查，而且在环网内有多个连接发生故障，则会导致环网崩溃。

1. 在调试期间，通过为连接在一条线路上的两个连接伙伴启用链路检查，可为连接部分逐一启用链路检查功能。
2. 为确保无错连接，等待一分钟后再为下一个连接启用链路检查。



显示框说明

该表包含以下列：

- **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)**
  使用此复选框，可为端口启用或禁用链路检查功能。
  启用连接监视后，可在“信息 > 冗余 > 链路检查”(Information > Redundancy > Link Check) 页面上查看已发送和接收到的链路检查帧数。
- **复位 (Reset)**
  复位链路检查后，会重新启动端口功能并复位统计数据。
  如果使用“复位”(Reset) 按钮，必须在 30 s 内在两个连接伙伴上同时执行复位。

说明

使用“复位”(Reset) 按钮时，会暂时形成回路，导致数据流量丢失。将再次自动清除回路。如果您的应用程序不接受，可通过拔出线缆并再次插入来复位链路检查。

组态步骤

启用链路检查

按照下列步骤激活环网端口的监视：

1. 在“设置”(Setting) 列中选择相应的复选框。
2. 单击“设置值”(Set Values) 按钮。

禁用链路检查

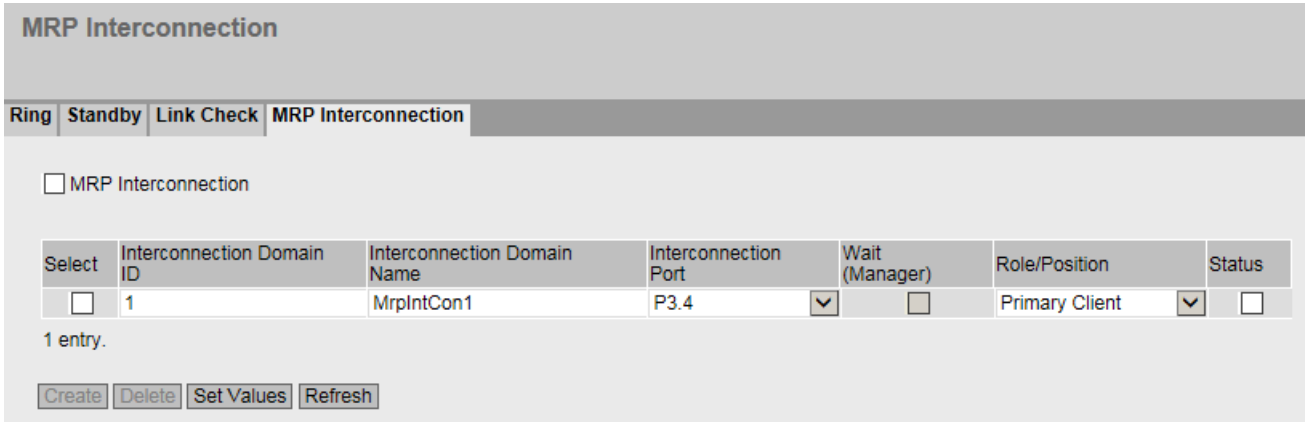
按照下列步骤取消激活环网端口的监视：

1. 在“设置”(Setting) 列中取消激活相应的复选框。
2. 单击“设置值”(Set Values) 按钮。

6.5.9.4 MRP-Interconnection

环网冗余链路

在此页面上创建、删除和组态 MRP 互连连接。



说明

该页面包含以下框：

- **MRP 互连 (MRP Interconnection)**
  选中此复选框以激活设备的 MRP 互连。只有在满足以下要求时才可启用 MRP 互连：
  – 已启用环网冗余。
  – “MRP 自动管理器”或“MRP 客户端”用作环网冗余模式。
  – 存在已激活的 MRP 互连连接。

  说明
  为每个环网中的两个设备组态环网冗余模式“MRP 自动管理器”(MRP Auto-Manager)，以便其中一个设备发生故障时也能立即重新组态 MRP 环网。

该表格包括以下列：

- **选择 (Select)**
  选择要删除的行。
- **互联域 ID (Interconnection Domain ID)**
  指定 MRP 互连连接的 ID。指定 ID 时，请遵守以下规则：
  – 互连 ID 不能为 0。
  – 需要为用于连接环网的所有四台设备组态相同的互连 ID。

- **互连域名称 (Interconnection Domain Name)**
  输入 MRP 互连连接的任何名称。还可以为用于连接环网的四台设备定义不同的名称。名称中的有效字符包括字母“A”到“Z”和“a”到“z”、数字“0”到“9”以及“-”符号。名称的第一个字符或最后一个字符不得使用连字符。互连名称必须至少包含一个字符且不超过 240 个字符。

- **互连端口 (Interconnection Port)**
  从此下拉列表中，选择用于 MRP 互连连接的端口。请注意以下限制：
  – 该端口不能被禁用或阻止。该端口的“单播阻止”(Unicast Blocking) 功能不能被启用。
  – 该端口不能用于链路汇聚。
  – 该端口不能为“镜像”(Mirroring) 功能的监视端口。
  – 该端口不能为生成树端口。
  – 该端口不能为环网端口。
  – 该端口不能为路由器端口。
  – 该端口不能为 802.1X 验证器端口。
  – 该端口不能为 802.1X 请求端口。

- **等待（管理器）(Wait (Manager))**
  对于具有“客户端”(Client) 角色的设备，不能选中此列中的复选框。当为具有“管理器”(Manager) 角色的设备选中此复选框时，MRP 互连管理器将等待数据传输，直到 MRP 互连的主客户端准备就绪。如果未选中该复选框，无论主客户端的操作状态如何，MRP 互连管理器都会等待 200 毫秒后开始数据传输。

- **角色/位置 (Role/Position)**
  有两种角色：“管理器”(Manager) 与“客户端”(Client)。对于客户端，还可以指定位置（“主要”(Primary) 或“次要”(Secondary)）。因此，该下拉列表提供
  以下选择选项：
  – 管理器 (Manager)
  – 主客户端 (Primary Client)
  – 次客户端 (Secondary Client)

- **状态 (Status)**
  选中此复选框可启用 MRP 互连连接。请遵守以下规则：
  – 如果未激活任何 MRP 互连连接，则无法为设备启用 MRP 互连。
  – 以下最大值适用于启用的 MRP 互连数量：
    SCALANCE XC-200、SCALANCE XC-300、SCALANCE XF-200BA、SCALANCE XP-200、SCALANCE XM-400 和 SCALANCE XR-500
    两个连接
    SCALANCE XB-200 和 SCALANCE XR-300WG
    一个连接

组态步骤

说明

可以在“技术基础知识 → 冗余机制 → MRP 互连”一节中找到 MRP 互连组态的详细分步描述。

组态要求

1. 按照规划的拓扑插入电缆，但以下连接除外：
   – 每个环中有一根连接线，这表示环还不能闭合。
   – 用于次要链路的两个设备（MIM 和次要耦合 MIC）尚不能连接。
2. 为每个设备分配 IP 地址以使用 WBM。

网络拓扑需要生成树时的组态要求

1. 为生成树组态协议兼容性“RSTP”。
2. 为环网端口和 MRP 互连端口禁用生成树。

环网冗余组态

为每个设备组态以下参数以实现环网冗余：

1. 指定环网端口。
2. 启用 MRP。
3. 为设备分配 MRP 角色。
4. 为每个环网中的两个设备组态环网冗余模式“MRP 自动管理器”(MRP Auto-Manager)，以便其中一个设备发生故障时也能立即重新组态 MRP 环网。

已在两个 MRP 环网中组态所有设备后，便可通过在尚未连接的设备之间插入电缆关闭两个 MRP 环网。还未在 MIM 和次要耦合 MIC 之间插入电缆。

MRP 互连组态

当组态这些设备时，必须遵守特定的顺序，以便组态 PC 可随时访问这些设备。首先对组态 PC 未连接到的 MRP 环网中的 MRP 互连连接设备进行组态。从尚未插入 MRP 互连连接电缆的设备开始。必须对每个设备执行以下步骤:

1. 单击“创建”(Create) 按钮在具有 MRP 互连连接的表格中创建新行。
2. 根据上述说明组态 MRP 互连连接的参数。
3. 选中“MRP 互连”(MRP Interconnection) 复选框可启用 MRP 互连。

已在两个 MRP 互连环网中组态所有设备后，在 MIM 和 次要耦合 MIC 设备之间插入次要链路的电缆。之后，MRP 互连连接即可使用。

说明

重新组态

在重新组态拓扑之前先打开环网，以避免数据帧循环传送。

6.5.10 生成树

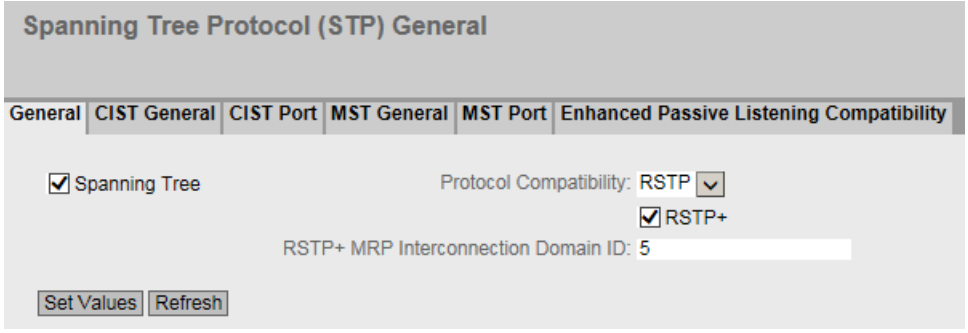
6.5.10.1 常规

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。



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。
  具有激活环网协议的端口不能参与 RSTP。因此，在“第 2 层 > 环网冗余”(Layer 2 > Ring Redundancy (页 325)) 页面上，通过“状态”(Status) 复选框禁用所有环网协议和 MRP 互连连接。
  可使用以下设置：
  – STP
  – RSTP
    Rapid Spanning Tree Protocol
    使用 RSTP，可以在同一设备上激活生成树和 MRP 环网，但不能在同一端口上激活。只有使用 RSTP+，才能同时在 MRP 环网端口上激活生成树。
  – MSTP
    Multiple Spanning Tree Protocol
- **RSTP+**
  可以将生成树激活的网段与 MRP 环网连接起来。
  选中此复选框前，请确保满足以下要求：
  – 必须将 MRP 启用为冗余方式。
  – 如果已激活环网冗余，则需要禁用生成树的环网端口。
  激活 RSTP+ 时，环网端口将成为 MRP 环网的一部分以及生成树网段的一部分。如果不使用 RSTP+，则环网端口不属于生成树网段。
- **RSTP+ MRP 互连域 ID (RSTP+ MRP Interconnection Domain ID)**
  在此处组态 RSTP+ 的 MRP 互连域 ID。该值不能与为激活 MRP 互连连接组态的 MRP 互连域 ID 相匹配。

说明

多环网管理器阻止生成树组态

如果在一台设备上组态了多个环网，则不能同时组态 RSTP 或 RSTP+。这也适用于已为环网端口禁用生成树的情况。

组态步骤

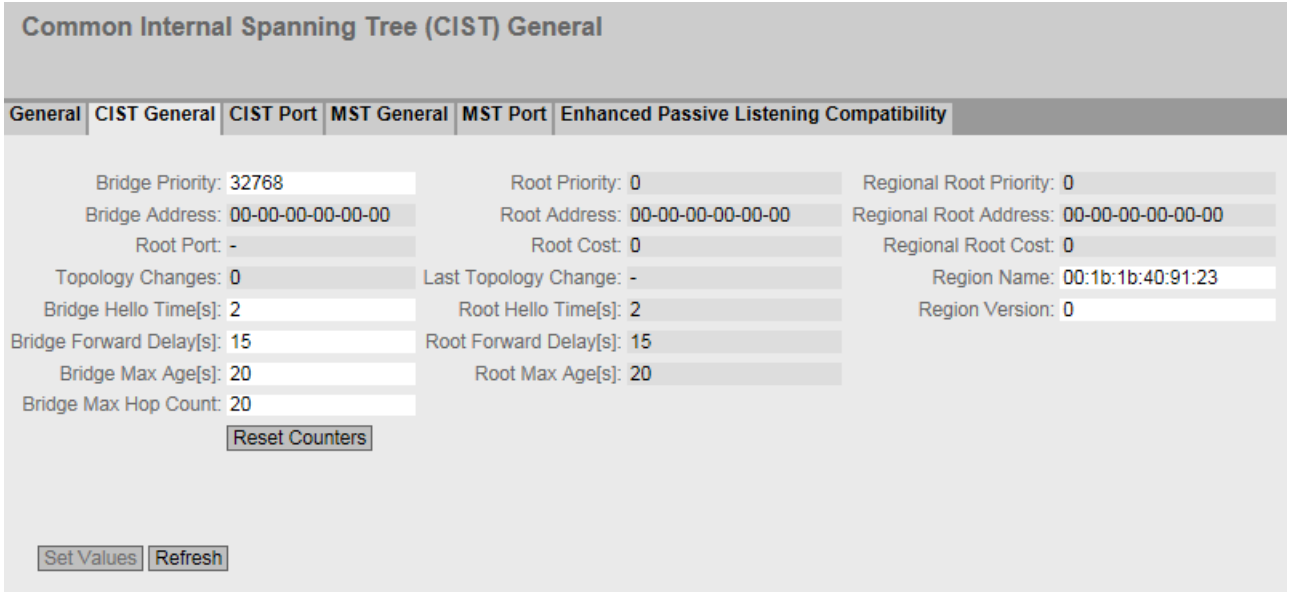
1. 选中“生成树”(Spanning Tree) 复选框。
2. 从“协议兼容性(Protocol Compatibility) 下拉列表中选择兼容类型。
3. 单击“设置值”(Set Values) 按钮。

6.5.10.2 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 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。



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
- **Bridge Address/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。
- **Root Cost**
  从该设备到根网桥的路径成本。
- **Topology Changes/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“sec”
  – 分钟：数字后的单位为“min”
  – 小时：数字后的单位为“hr”
- **Bridge hello time [s] / Root hello time [s]**
  每个网桥都会定期发送组态帧 (BPDU)。“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“Protocol compatibility”RSTP 时才能对“Bridge Hello Time”进行设置。如果设置了“Protocol compatibility”MSTP，则将使用“Layer 2 > Spanning Tree > CIST Port”页面上的“Hello Time”参数。

- **Bridge Forward Delay[s] / Root Forward Delay[s]**
  网桥不会立即使用新组态数据，而是在“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
- **Bridge Max Age[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”
- **Regional Root Address**
  设备的 MAC 地址。
- **Regional Root Cost**
  从该设备到根网桥的路径成本。
- **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。
- **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。在属于相同 MSTP 区域的所有设备上，该值必须相同。
- **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。

组态步骤

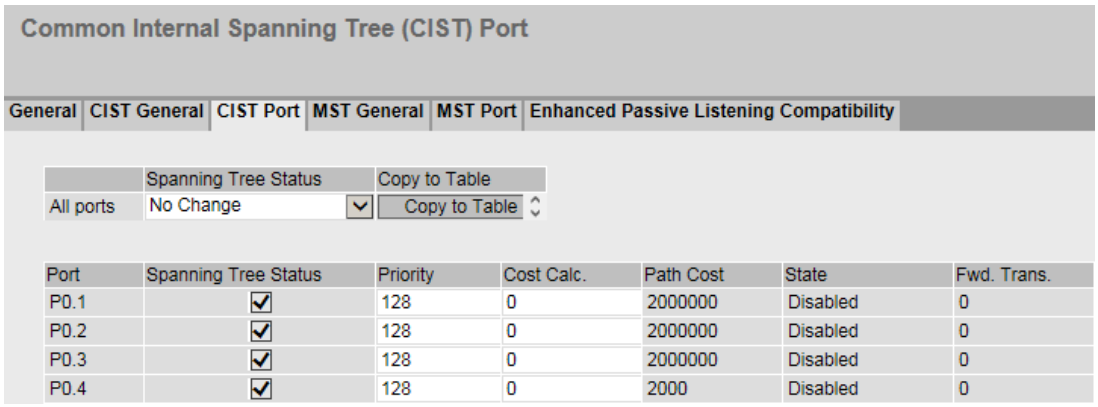
1. 在输入框中输入组态所需的数据。
2. 单击“Set Values”按钮。

6.5.10.3 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。



（续表）

Edge Type	Edge	P.t.P. Type	P.t.P.	Hello Time	Restr. Role	Restr. TCN	Limited TCN
Auto	☐	-	☐	2	☐	☐	☐
Auto	☐	-	☐	2	☐	☐	☐
Auto	☐	-	☐	2	☐	☐	☐
Auto	☐	-	☑	2	☐	☐	☐

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。
  - 不变 (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。
  如果“开销计算”(Cost Calc.) 框中的值为“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：
  - 禁用 (Disabled)
    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。
  - 侦听 (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（即节点寻址）。
  - 转发 (Forwarding)
    重新组态时间后，端口在网络中激活；并接收和转发数据帧。
- **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
    如果要在此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。

- **P.t.P.**
  复选框处于选中状态表明端口的操作状态对应于“点对点类型”(P.t.P. Type) 列中的组态。

- **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。取值范围：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。

- **受限角色 (Restr. Role)**
  如果选中此复选框，则无论优先级值如何，都不会将相应端口选作根端口。如果选中此复选框，则优先级最低的端口也不会成为根端口。仅当要限制管理范围外的网桥对生成树拓扑产生的影响时才激活此选项。

- **受限 TCN (Limited TCN)**
  如果选中此复选框，则相应端口不会将已接收或检测到的拓扑更改（拓扑更改通知）转发到其它端口。仅当要限制管理范围外的网桥对生成树拓扑产生的影响时才激活此选项。
- **受限 TCN (Limited TCN)**
  如果选中此复选框，则相应的端口将接受已接收和检测到的拓扑更改，但不会将拓扑更改转发到其它端口。只有在满足以下要求时才可选中此列的复选框：
  – 必须启用 RSTP+。
  – 必须清除此端口的“受限 TCN”(Restr. TCN) 复选框。
  如果未满足指定要求，此列的复选框将呈灰色显示：

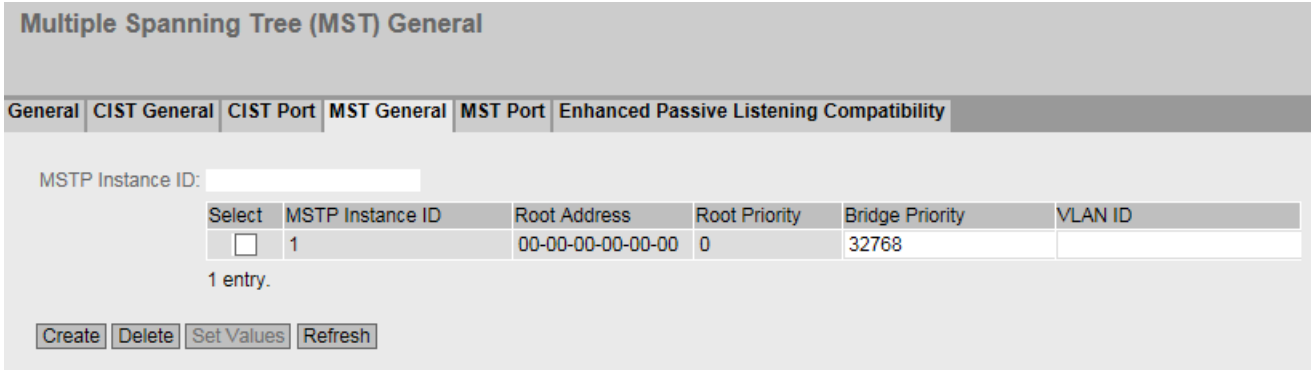
组态步骤

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。

6.5.10.4 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。



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。

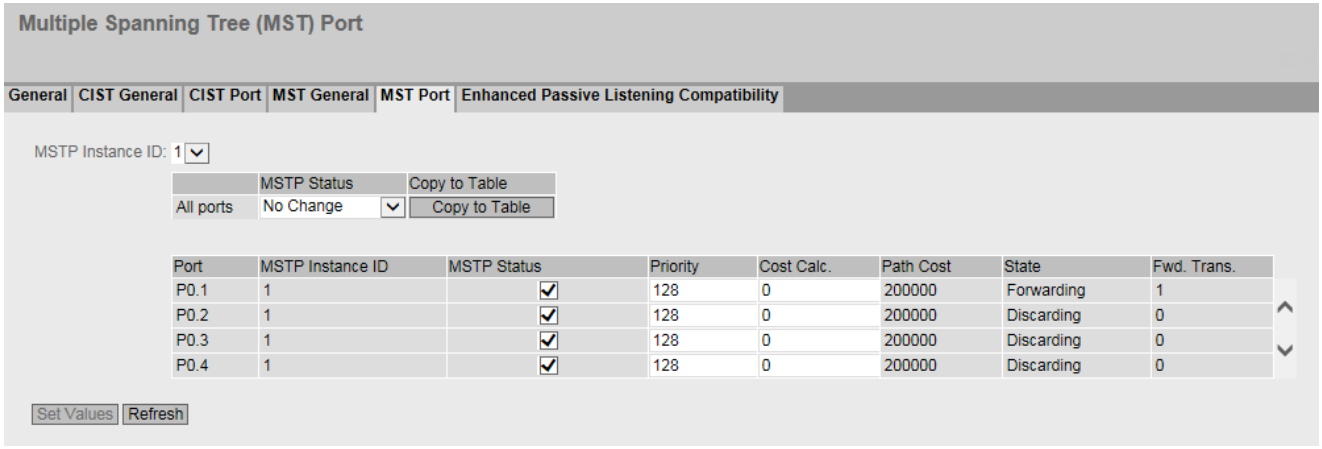
删除条目

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。

6.5.10.5 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。



显示框说明

该页面包含以下框：

- **MSTP 实例 ID (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 (Copy to Table)**
  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 实例 ID (MSTP Instance ID)**
  MSTP 实例的 ID。
- **MSTP 状态 (MSTP Status)**
  选中属于此实例的端口对应的复选框。
- **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
- **成本计算 (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。
- **路径开销 (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。

- **状态 (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。
- **转发转换 (Fwd.Trans.)**
  指定端口状态从“放弃”(Discarding) 到“转发”(Forwarding) 或从“转发”(Forwarding) 到“放弃”(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。

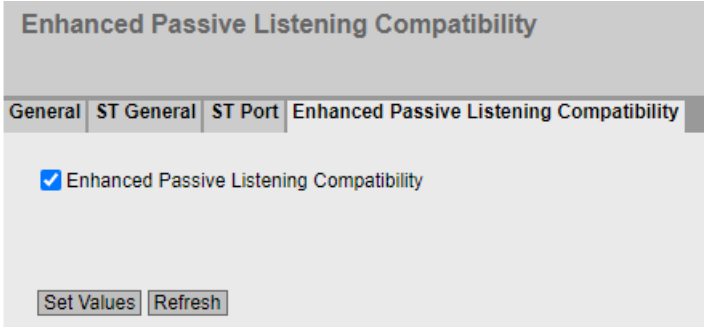
6.5.10.6 增强的被动侦听兼容性

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。

6.5.11 回路检测 (Loop Detection)

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。

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)。

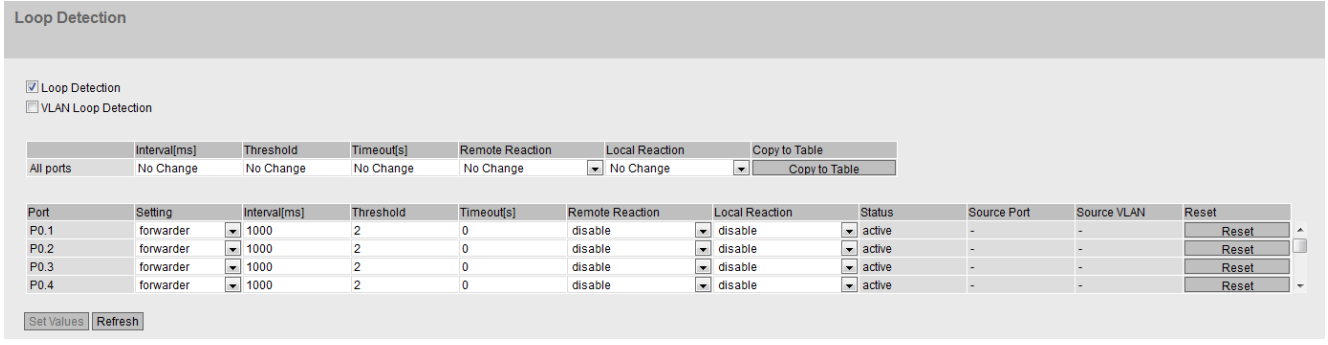
说明

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，在以下端口上不能进行回路检测：

- 环网端口
- 备用端口
- MRP 互连端口



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。
  如果启用此选项，则设备将发送未标记 LLC 帧。
- **VLAN 回路检测 (VLAN Loop Detection)**
  启用或禁用 VLAN 回路检测。
  如果启用此选项，则设备将使用在相应端口设置的 VLAN 信息发送 LLC 帧。

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。
- **间隔 [ms] (Interval [ms])/阈值 (Threshold value)/超时 [s] (Timeout [s])/远程响应 (Remote reaction)/本地响应 (Local reaction)**
  进行所需设置。
- **复制到表 (Copy to Table)**
  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”。

  生成树端口不能组态为“Sender”。

  – 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。
- **时间间隔[毫秒] (Interval[ms])**
  指定回路检测帧的发送间隔（单位：毫秒）。

- **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。
- **超时[秒] (Timeout[s])**
  指定设备自动切换到回路之前所处的状态前经过的时间。如果将该值设置为“0”，则环路后需要使用“复位”(Reset) 按钮再次手动启用该端口。还可通过拔出端口电缆并再次插入的方式复位端口。
- **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。
- **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。

6.5.12 链路汇聚

6.5.12.1 常规

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)。

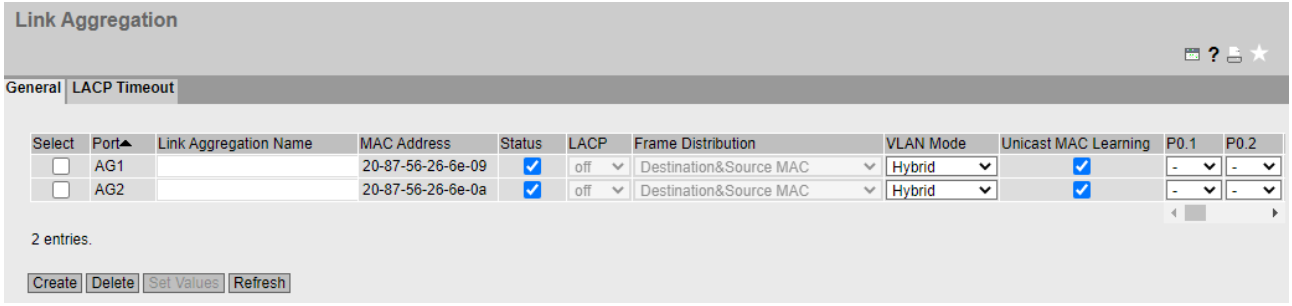
说明

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。



显示框说明

该表格包括以下列：

- **选择 (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 地址 (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 LACP 帧的发送。
  - 关闭 (Off)
    禁用 LACP 帧的发送。
- **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。
- **VLAN 模式 (VLAN Mode)**
  指定在 VLAN 中登记链路汇聚的方式：
  - 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。
  - 访问 (Access)
    该端口属于支持 Q-in-Q VLAN 隧道功能的提供商交换机。

- **单播 MAC 学习 (Unicast MAC Learning)**
  启用或禁用端口的单播地址学习功能。这些单播地址作为动态学习的地址输入 FDB 中。
- **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，并仅在接收到 LACP 帧时参与链路汇聚。
  – “p”（被动）
  端口仅在接收到 LACP 帧时参与链路汇聚。
  – “o”（开启）
  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“创建”(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。

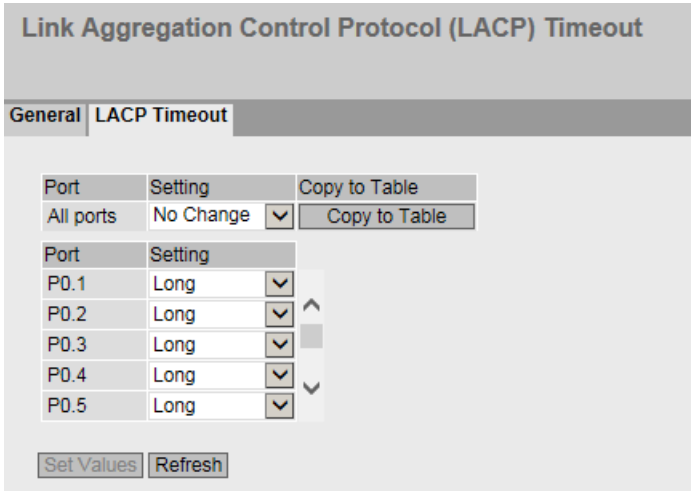
更改链路汇聚

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。

6.5.12.2 LACP 超时

LACP 超时组态

在 IEEE 802.3ad 标准中，为超时时长定义了两个可能的值：“长”（90 秒）和“短”（3 秒）。该值定义发送 LACPDU 的时间间隔。所有端口默认组态“Long”值。要启用对称的 LACP 组态，可以选择“Short”值。对于链路汇聚的所有端口，请为超时选择相同的值。



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。
- **设置 (Setting)**
  从下拉列表中选择设置。可选择以下设置选项：
  - 短 (Short)
    LACP 超时时长为 3 秒。
  - 长 (Long)
    LACP 超时时长为 90 秒。
  - 不变 (No Change)
    表 2 保持不变。
- **复制到表 (Copy to Table)**
  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：

- **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。
- **设置 (Setting)**
  为此端口选择“短”(Short) 值或“长”(Long) 值。

6.5.13 DCP 转发

应用

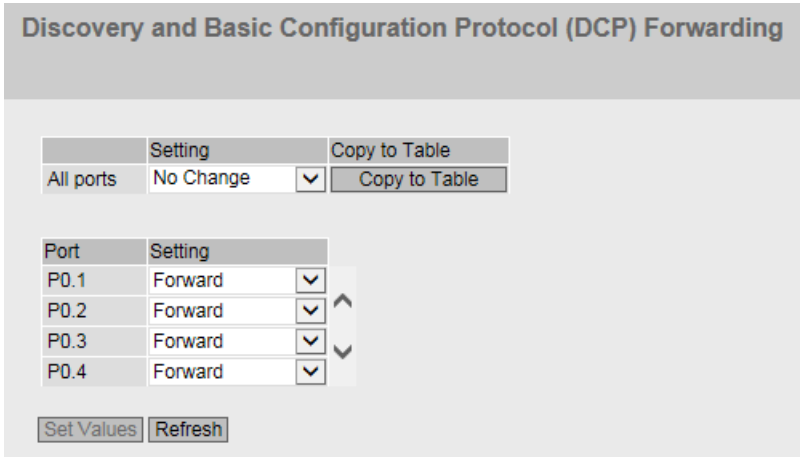
STEP 7 和 SINEC PNI 使用 DCP 协议进行组态和诊断。发货时，对所有端口都启用 DCP；换句话说，在所有端口都转发 DCP 帧。利用此选项，可以针对每个端口禁止转发帧，例如，使用 SINEC PNI 组态时排除网络的个别部分，或者将整个网络分成较小子网以进行组态和诊断。

说明

PROFINET 组态

由于 DCP 是一种 PROFINET 协议，因此在此创建的组态只对与 TIA 接口相关的 VLAN 有效。

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。



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。如果选择“无变化”(No Change)，则表 2 中的条目保持不变。
- **复制到表 (Copy to Table)**
  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 (Foward)
    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。

6.5.14 LLDP

识别网络拓扑

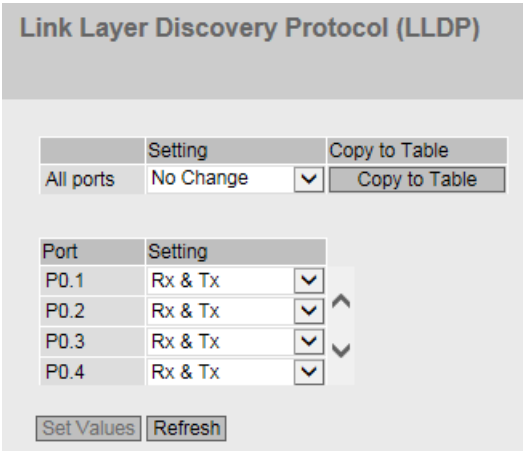
LLDP (Link Layer Discovery Protocol) 在 IEEE 802.1AB 标准中定义。

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。



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。
- **Setting**
  从下拉列表中选择设置。如果选择“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：

- **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**
    此端口可以接收和发送 LLDP 帧。
  - “-”（禁用）
    此端口既不能接受也不能发送 LLDP 帧。

组态步骤

1. 从“Setting”的下拉列表中选择端口的 LLDP 功能。
2. 单击“Set Values”按钮。

6.5.15 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。

如果在某光纤端口上启用了光纤监视，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。

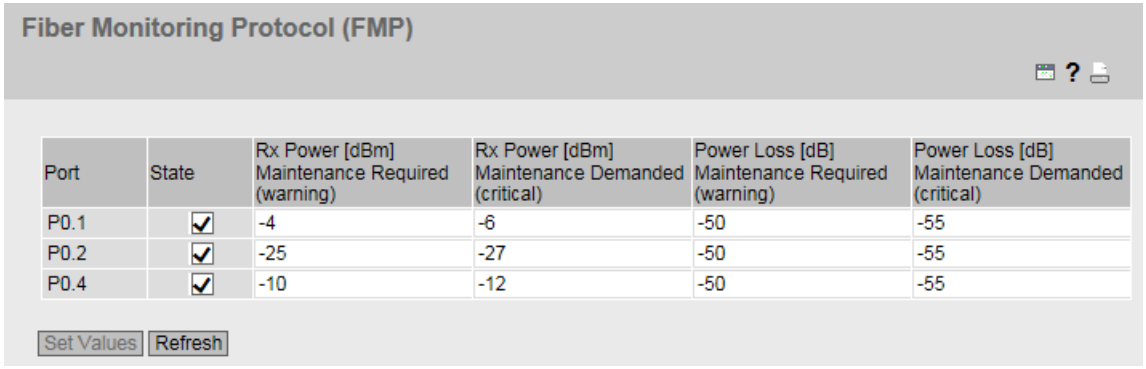
如果连接伙伴上启用了光纤监视，连接伙伴会将端口发射功率的当前值传递给设备。设备会将接收到的发射功率值与实际接收的功率进行比较。接收功率与发射功率之间存在的差异代表链路汇总存在损耗。计算得到的功率损失也会进行监视，判断是否超出设定的限值。

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“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。



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。

- **Port**
  显示支持光纤监视的光纤端口。它与收发器有关。
- **Status**
  启用或禁用光纤监视。
  默认情况下会禁用该功能。
- **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。
  如果输入值“0”，则不会监视接收功率。
  默认值取决于相应收发器。
- **Rx Power [dBm] Maintenance Demanded (Critical)**
  指定在什么值时候通过严重等级为“Critical”的消息来通知您接收功率超限。
  如果输入值“0”，则不会监视接收功率。
  默认值取决于相应收发器。

- **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。
  如果输入值“0”，则不会监视功率损耗。
  默认值：-50 dB
- **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。
  如果输入值“0”，则不会监视功率损耗。
  默认值：-55 dB

组态步骤

启用光纤监视

按照下列步骤启用端口的监视：

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。

禁用光纤监视

按照下列步骤禁用端口的监视：

1. 在“Status”列中清除相应的复选框。
2. 单击“Set Values”按钮。

按照以下步骤禁用对接收功率或功率损耗的监视：

1. 在相应的框中输入值“0”。
2. 单击“Set Values”按钮。

6.5.16 单播

6.5.16.1 过滤

地址过滤

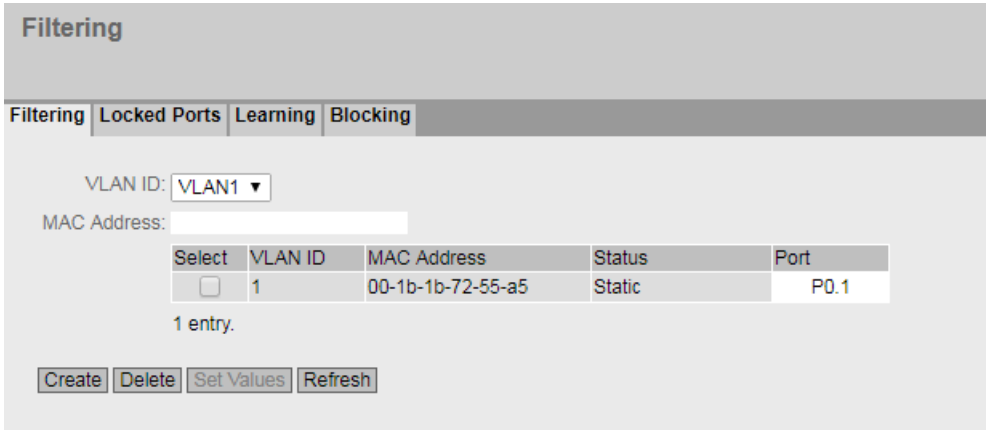
此表中显示的是参数分配期间由用户以静态方式输入的单播地址帧的源地址。

在此页面中，还可定义静态单播过滤器。

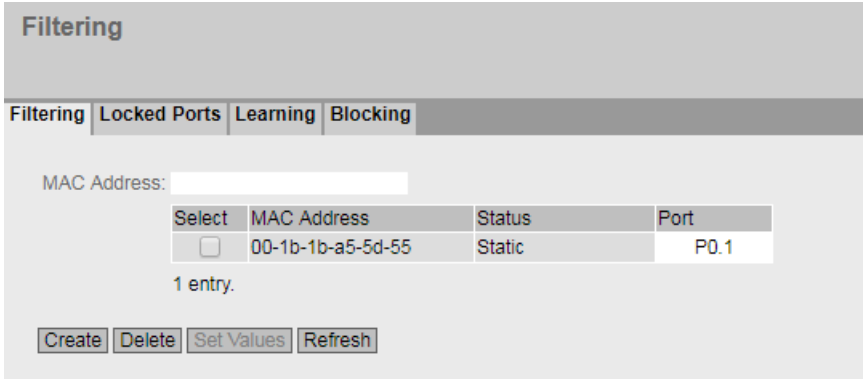
“基础网桥模式”(Base bridge mode) 的相关性

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。以下几张图显示了“802.1Q VLAN 网桥”(802.1Q VLAN Bridge) 和“802.1D 透明网桥”(802.1D Transparent Bridge)”这两种操作模式下 WBM 页面的不同内容。

基础网桥模式：802.1Q VLAN 网桥 (802.1Q VLAN Bridge)



基础网桥模式：“802.1D 透明网桥”(802.1D Transparent Bridge)”



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 (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。

  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 地址”(MAC Address) 输入框中输入 MAC 地址。
3. 单击“创建”(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。

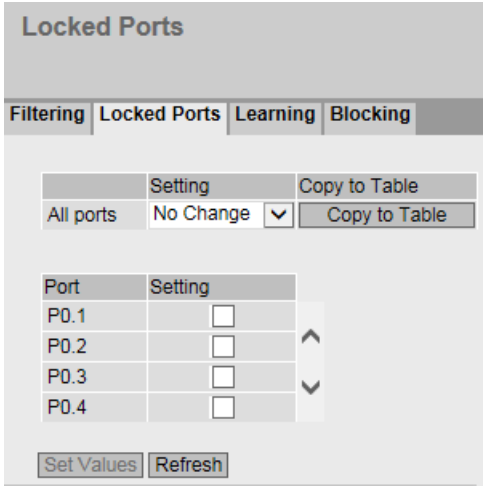
6.5.16.2 锁定端口 (Locked Ports)

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。该端口仅接受之前手动创建或通过“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”）。



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。
  - 不变 (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。

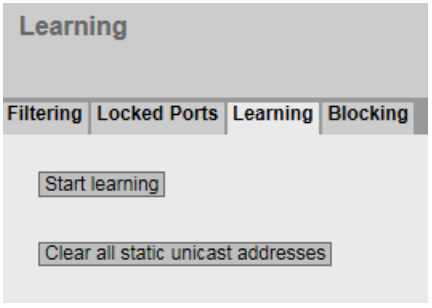
6.5.16.3 学习

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。
只有单击“停止学习”(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。



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。将已学习的条目存储至“第 2 层 > 单播 > 过滤”(Layer 2 > Unicast > Filtering) 中，并在其中列出。

说明

数据速率非常高时，静态输入的单播地址可能会在单播表中显示为学习地址。在这种情况下，建议采用以下步骤：

1. 单击“开始学习”(Start learning) 按钮即可开始学习过程。
2. 启动数据通信。
3. 等待至单播表显示所有 MAC 地址为“Learnt”（菜单“信息 > 单播”(Information > Unicast)）。
4. 锁定端口（菜单“第 2 层 > 单播 > 锁定端口”(Layer 2 > Unicast > Locked Ports)）。
5. 单击“停止学习”(Stop learning) 按钮即可停止学习过程。

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。

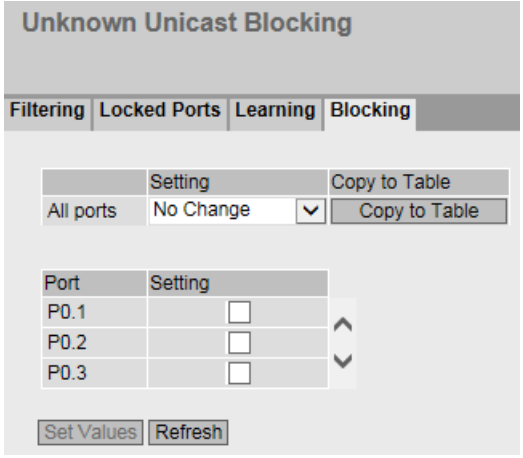
   说明

   根据涉及的条目数，删除过程可能需要一些时间。

6.5.16.4 受阻

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。



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。
  - 不变 (No change)
    表 2 保持不变。
- **复制到表 (Copy to Table)**
  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

  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。

对所有端口启用阻止功能

1. 在“设置”(Setting) 下拉菜单中，选择表 1 中的“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。

6.5.17 组播

6.5.17.1 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。

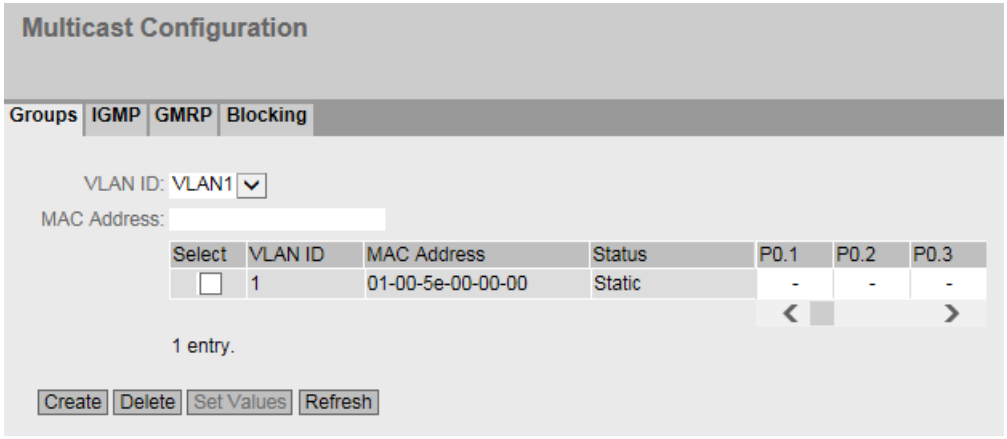
所有这些方法的结果是，组播帧只会被发送到输入了相应地址的端口。

“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。

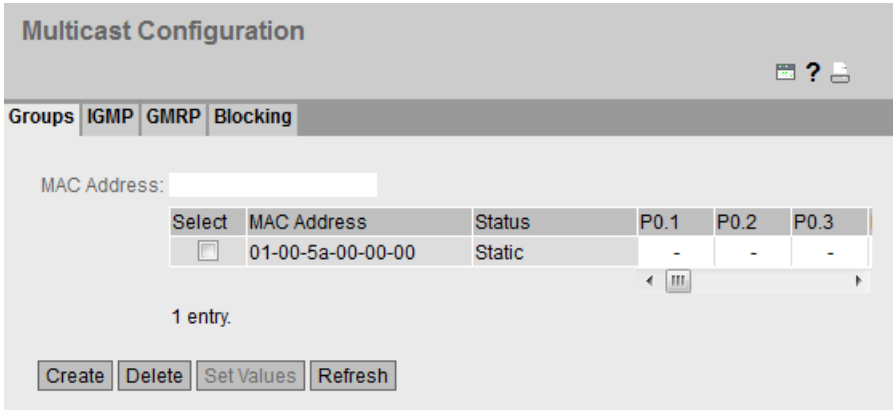
“基础网桥模式”(Base bridge mode) 的相关性

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。以下几张图显示了“802.1Q VLAN 网桥”(802.1Q VLAN Bridge) 和“802.1D 透明网桥”(802.1D Transparent Bridge)”这两种操作模式下 WBM 页面的不同内容。

基础网桥模式：802.1Q VLAN 网桥



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。

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。
  - 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。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。
  - F
    （已禁止）不是组播组的成员。此地址也不能是使用 GMRP 或 IGMP 动态获取的地址。

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。

6.5.17.2 IGMP

功能

设备支持“IGMP Snooping”和“IGMP Querier”功能。如果启用了“IGMP Snooping”，则会评估 IGMP 帧（Internet 组管理协议），并用该评估信息更新组播过滤表。如果还启用了“IGMP Querier”，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。

这适用于所有端口和 VLAN；但无法进行具体组态。

取决于查询器的 IGMP 监听老化时间

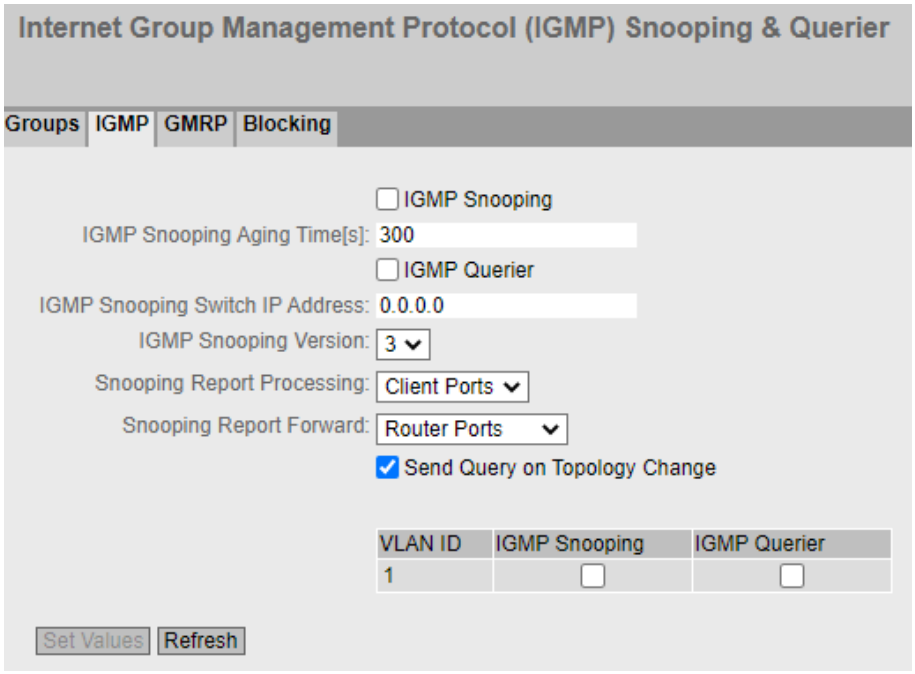
工业以太网交换机用作 IGMP 查询器

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 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 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 Snooping**
  启用或禁用 IGMP 监听。该功能会在所有接口上启用 IGMP 监听，并允许将 IP 地址分配给组播组。如果启用此功能，可将通过 IGMP 监听识别的组播地址输入组播过滤表并转发 IGMP 帧。
- **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
  取值范围：130 - 1225 秒
- **IGMP Querier**
  启用或禁用“IGMP Querier”。设备会循环发送 IGMP 查询。
- **IGMP Snooping Switch IP Address**
  该 IP 地址用于发送 IGMP 查询。如果在网络中发送多个 IGMP 查询器查询，则 IP 地址最小的查询器将具有查询器的功能。
  如果设置的 IP 地址为 0.0.0.0，则会使用自有 IP 地址发送 IGMP 查询。此外，还可输入任意 IP 地址，以在网络中存在多个 Querier 时，指定活动 Querier 的顺序。
- **IGMP Snooping Version**
  从下拉列表中选择 IGMP Snooping Version。

- **Snooping Report Processing**
  可能的设置如下：
  - Client Ports
    设备仅处理客户端端口上的 IGMP 连接。
  - All Ports
    设备处理所有端口上的 IGMP 连接。
- **Snooping Report Forward**
  可能的设置如下：
  - All Ports
    设备将 IGMP 连接转发给所有端口。
  - Router Ports
    设备将 IGMP 连接转发给路由器端口。
  - Non Edge Ports
    设备将 IGMP 连接转发给所有非边缘端口。
- **Send Query on Topology Change**
  启用或禁用在拓扑变化时发送额外的 IGMP 查询。在大型生成树拓扑中，发送额外的 IGMP 查询可导致不必要的查询泛洪。

该表格包括以下列：

- **VLAN ID**
  应激活 IGMP Snooping 或 IGMP Querier 的 VLAN ID。
- **IGMP Snooping**
  选中此列中应激活 IGMP Snooping 的 VLAN 对应的复选框。为设备启用 IGMP Snooping（该页中的第一个复选框）后，此列中的规范才有效。
- **IGMP Querier**
  选中此列中应激活 IGMP Querier 的 VLAN 对应的复选框。
  如果选中设备的 IGMP Snooping 复选框与 VLAN 的 IGMP Snooping 复选框，则当选中表中对应复选框时，将执行 IGMP Querier。对设备而言，无论 IGMP Querier 复选框状态如何，均如此。

组态步骤

启动 IGMP Snooping

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. 从下拉列表中选择 IGMP Snooping Version。
4. 从下拉列表中，选择设备是应仅在客户端端口还是应在所有端口上处理 IGMP 连接。
5. 在“IGMP Snooping”表列中，选中所需 VLAN ID 的复选框。

关闭 IGMP Snooping

1. 清除“IGMP Snooping”复选框。

启动 IGMP Querier

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 Snooping Aging Time”复选框。
4. 在“IGMP Snooping Switch IP Address”字段中，输入将用于发送 IGMP 查询的 IP 地址。
5. 在“IGMP Querier”表列中，选中所需 VLAN ID 的复选框。

关闭 IGMP Querier

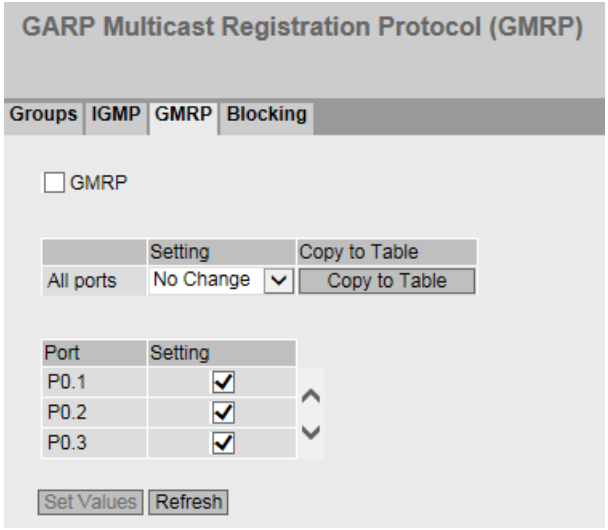
1. 清除“IGMP Querier”复选框。

6.5.17.3 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。

要使 GMRP 生效，需要在端口上全局地启用该功能。



显示框说明

该页面包含以下框：

- **GMRP**
  启用或禁用 GMRP 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。
- **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“GMRP”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

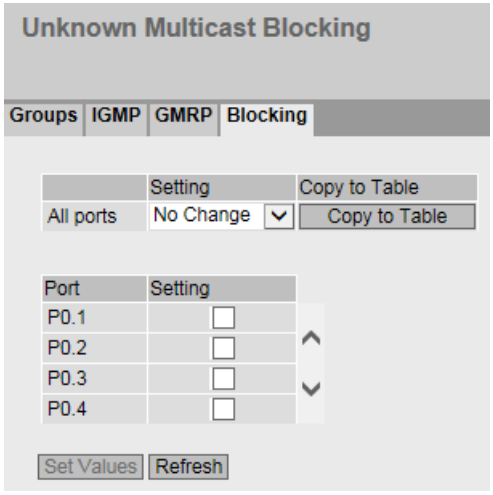
1. 选择“GMRP”复选框。
2. 在“设置”(Setting) 下拉列表中，选择“启用”(Enabled) 条目。

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。

6.5.17.4 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。



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。

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。

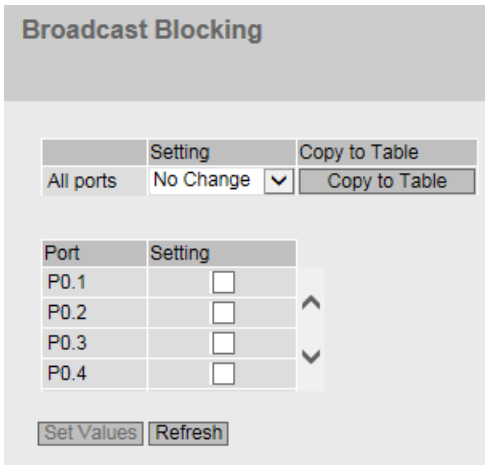
6.5.18 广播

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。



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。

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

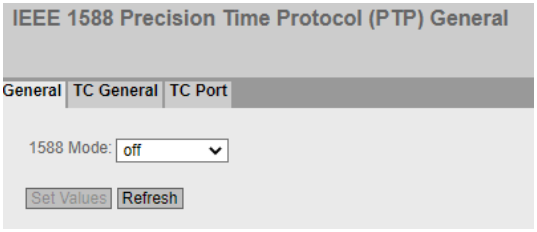
1. 在表 1“设置”(Setting) 下拉菜单中，选择“启用”(Enabled) 条目。
2. 单击“复制到表”(Copy to Table) 按钮。将为表 2 中的所有端口启用该复选框。
3. 要应用更改，请单击“设置值”(Set Values) 按钮。

6.5.19 PTP

6.5.19.1 常规

IEEE 1588 与 SCALANCE 设备

IEEE 1588v2 标准定义的机制可以使网络中的设备实现精确的时钟同步。配有合适硬件的 SCALANCE 设备支持 IEEE 1588v2 规定的时间同步。该功能在设备出厂时以及将设备复位为出厂设置后处于禁用状态。要使用 PTP，请启用此功能并组态同步路径上的每个端口以及由于冗余机制而阻塞的端口。PTP 还可以在 HRP、环网备用链路、MRP 和 RSTP 等环网中与冗余机制配合使用。以下几个部分将介绍基于 Web 的管理的组态选项。



IEEE 1588 组态

在此页面中，可指定设备处理 PTP 消息的方式。

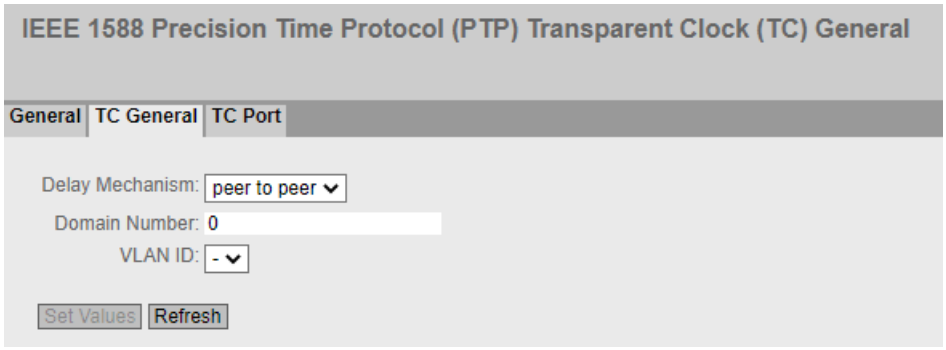
模式 1588 (Mode 1588)
可进行以下设置：

- **关闭 (off)**
  设备不处理任何 PTP 消息。但是，将根据交换机的规则转发 PTP 消息。
- **透明 (transparent)**
  设备采用透明时钟的功能并将 PTP 消息转发到其它节点，同时在 PTP 消息的修正字段中输入内容。

6.5.19.2 TC 常规

TC 常规

在此选项卡上提供有 PTP 常规设置。



IEEE 1588 透明时钟的组态

- **延迟机制 (Delay Mechanism)**
  指定设备将使用的延迟机制：
  - 端对端
    将使用延迟请求响应机制。

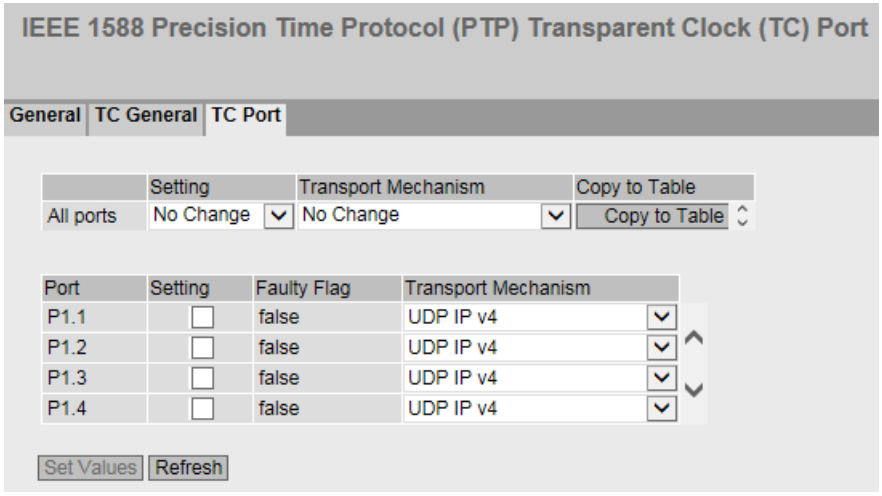
    说明

    通过与 2 个以上从站进行端对端同步，偏移量中可能出现 > 100 ns 的异常值。
  - 对等
    将使用对等延迟机制。
- **域编号 (Domain Number)**
  在此处输入设备的域编号。一个 SCALANCE 设备只能分配给一个同步域。
- **VLAN ID**
  设置选项取决于组态的“基础网桥模式”(Base Bridge Mode)（“第 2 层菜单 > VLAN > 常规”(Layer 2 Menu > VLAN > General)）：
  - “802.1D 透明网桥”(802.1D Transparent Bridge)”
    由于 VLAN 变量在该模式下没有任何作用，因此下拉列表中会显示“-”。设备在每个 VLAN 中对自身进行同步。
  - 802.1Q VLAN 网桥 (802.1Q VLAN Bridge)
    所有已组态的 VLAN 均包含在下拉列表中。选择设备对自身进行同步应处于的 VLAN。

6.5.19.3 TC 端口

端口设置

此选项卡中包含 PTP 的端口设置。



IEEE 1588 透明时钟端口参数的组态

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“No Change”，则表 2 中的条目保持不变。
- **Transport Mechanism**
  可能的设置如下：
  - Ethernet
  - UDP IPv4
  - No Change
    如果选择“No Change”，则表 2 中的条目保持不变。

表 2 显示了各个端口的详细信息：

- **Port**
  端口号。对于模块化设备，插槽号和端口号使用点分隔显示。
  SFP+ 端口不支持 PTP。
- **Setting**
  端口状态。可以是以下条目：
  - Disabled
    端口不包括在 PTP 中。
  - Enabled
    端口处理 PTP 消息。

- **Faulty Flag**
  与 PTP 有关的错误状态。
  - true
    发生错误。
  - false
    该端口未发生错误。
- **Transport Mechanism**
  选择此端口处理 PTP 消息数据通信的方式。可以对设备的多个端口进行不同的设置，但是，相关的通信伙伴必须支持所选的传输机制。可能的设置如下：
  - Ethernet
  - UDP IPv4

6.5.20 RMON

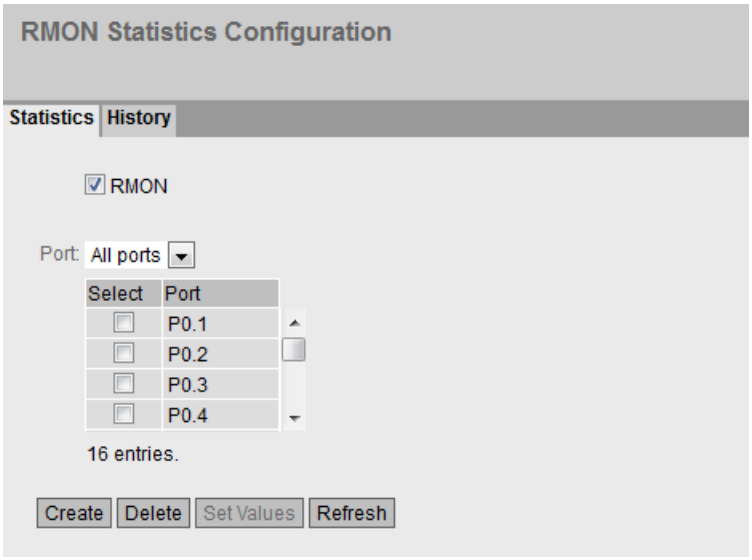
6.5.20.1 Statistics

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**
  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。

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。

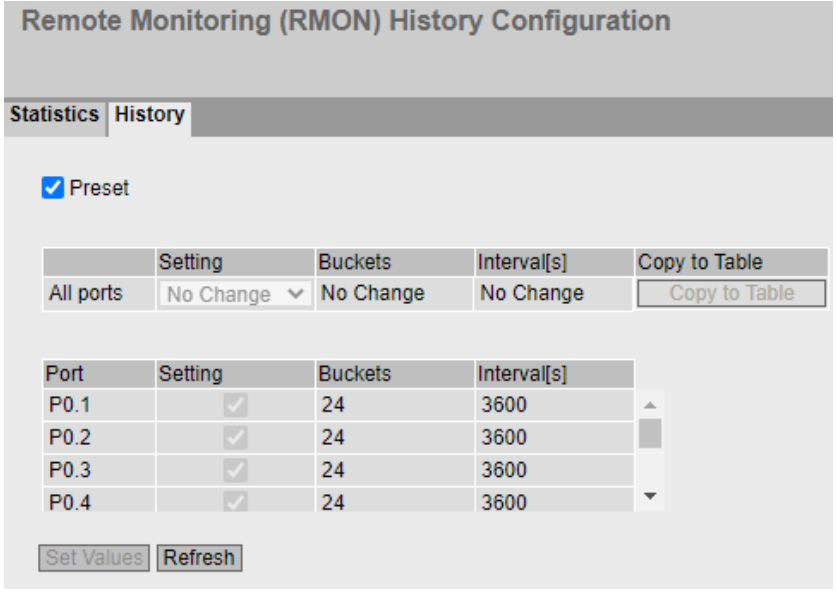
6.5.20.2 历史

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。

启用的 RMON 统计信息显示在 WBM 页面“Information > Ethernet statistics > History”中。

设置



该页面包含以下框：

- **Default**
  如果启用该选项，所有自定义 RMON 历史设置将被删除并被所有端口的以下设置覆盖：
  - Setting：已启用
  - Entries：24
  - Interval[s]：3600

  只要启用 RMON 历史记录的 Default，单个组态的值就会被锁定。
  如果禁用该选项，设置将保留，但可以再次单独组态。

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“No Change”，则表 2 中的条目保持不变。
- **Buckets**
  输入可同时保存的条目的最大数量。如果输入“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版本保存为样本之前的间隔。如果输入“No Change”，则表 2 中的条目保持不变

  说明

  定义时间间隔时，请注意时间间隔只能为 3 秒的倍数。统计信息每 3 秒更新一次。在两个时间间隔之间输出值“0”。

- **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。

- **Buckets**
  输入可同时保存的条目的最大数量。
  设备可限制的最大条目数。
  取值范围：1 - 65535
  出厂设置：24
- **Interval [s]**
  输入将统计信息的当前版本保存为样本之前的间隔。
  取值范围：1 - 3600
  出厂设置：3600

说明

定义时间间隔时，请注意时间间隔只能为 3 秒的倍数。统计信息每 3 秒更新一次。在两个时间间隔之间输出值“0”。

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“Setting”。
   “Buckets”和“Interval[s]”变为激活状态并采用出厂设置。
2. 在“Buckets”和“Interval[s]”输入框内输入所需值。
3. 单击“Set Values”按钮。

为所有端口启用 RMON 统计信息

1. 在“Setting”下拉菜单中，选择表 1 中的“Enabled”条目。
2. 在“Buckets”和“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“Copy to Table”按钮。
   表 2 的所有端口均采用这些设置。
4. 单击“Set Values”按钮。

激活 RMON 默认值

1. 选择“Default”复选框。
2. 单击“Set Values”按钮。

6.6 “第 3 层”(Layer 3) 菜单

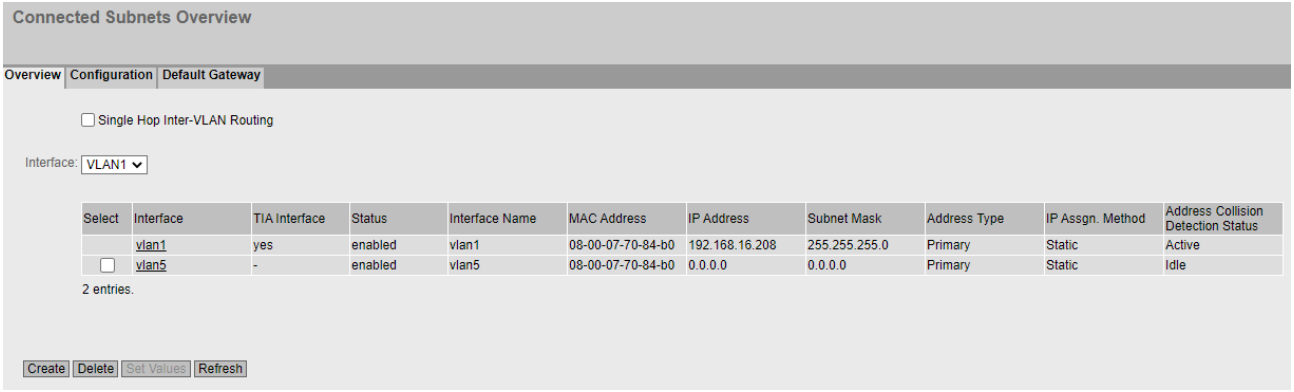
6.6.1 子网

6.6.1.1 概述

创建子网

在此页面上，您可以为设备创建多个 VLAN IP 接口。

子网总是与 VLAN 相关。IP 地址在“组态”(Configuration) 选项卡中分配。



显示值说明

该页面包含以下框：

- **单跳 VLAN 间路由 (Single-Hop Inter-VLAN-Routing)**
  启用或禁用本地 IP 接口之间的路由。
- **接口 (Interface)**
  选择要用于组态其它 IP 子网的接口。

该表格包括以下列：

- **选择 (Select)**
  选择要删除的行。
- **接口 (Interface)**
  显示接口。
- **TIA 接口 (TIA Interface)**
  显示是否将该接口用作 TIA 接口。

- **状态 (Status)**
  显示接口状态。
- **接口名称 (Interface Name)**
  显示接口名称。
- **MAC 地址 (MAC Address)**
  显示 MAC 地址。
- **IP 地址 (IP Address)**
  显示子网的 IPv4 地址。
- **子网掩码 (Subnet Mask)**
  显示子网掩码。
- **地址类型 (Address Type)**
  显示地址类型。可能的值包括：
  – Primary
    在 IPv4 接口上组态的首个 IPv4 地址。

- **IP 分配方式 (IP Assgn Method)**
  显示分配 IPv4 地址的方式。可能的值包括：
  - Static
    IPv4 地址是静态的。在“IP 地址”(IP Address) 和 “子网掩码”(Subnet Mask) 中输入设置。
  - Dynamic (DHCP)
    设备从 DHCPv4 服务器获得动态 IPv4 地址。
- **地址冲突检测状态 (Address Collision Detection Status)**
  如果网络中激活新的 IPv4 地址，则“Address Collision Detection”功能将检测上述操作是否会引起地址冲突。通过此功能，可以检测出被分配两次的 IPv4 地址。

  说明

  此功能不执行周期性检查。

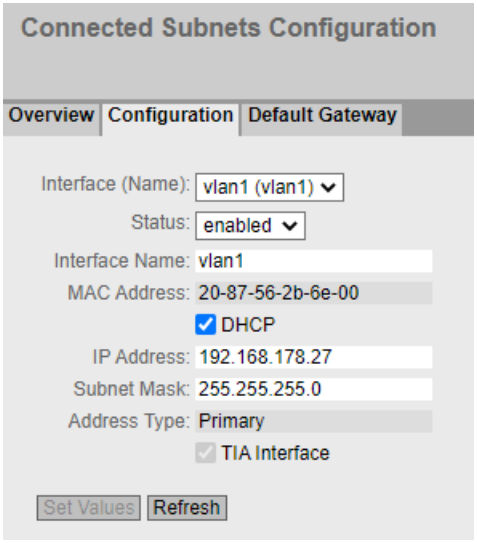
  此列显示功能的当前状态。可能的值包括：
  - Idle
    未启用该接口，因此也没有 IPv4 地址。
  - Starting
    该状态表示启动阶段。在该阶段中，设备首先会发送查询，以了解规划的 IPv4 地址是否已经存在。如果该地址尚未分配，设备将发送现在开始使用此 IP 地址的消息。
  - Conflict
    接口未启用。接口试图使用已经分配的 IPv4 地址。
  - Defending
    接口使用唯一的 IPv4 地址。另一接口正试图使用相同的 IPv4 地址。
  - Active
    接口使用唯一的 IPv4 地址。未发生冲突。
  - Disabled
    禁用地址冲突检测功能。

组态步骤

1. 从 “接口”(Interface) 下拉列表中选择接口。
2. 单击 “创建”(Create) 按钮。将在表中插入一个新行。
3. 单击 “设置值”(Set Values) 按钮。
4. 在 “组态”(Configuration) 选项卡中组态子网。

6.6.1.2 组态

在此页面中组态 IPv4 接口。



显示值说明

该页面包含以下框：

- **接口（名称）(Interface (Name))**
  从下拉列表中选择信息。
- **状态 (Status)**
  指定启用或禁用接口。
  - 已启用
    接口已启用。数据通信只能通过已启用的接口进行。
  - 已禁用
    接口已禁用。
- **接口名称 (Interface Name)**
  输入接口的名称。
- **MAC 地址 (MAC Address)**
  显示所选接口的 MAC 地址。
- **DHCP**
  为此 IPv4 接口启用或禁用 DHCP 客户端。
- **IP 地址 (IP Address)**
  输入接口的 IPv4 地址。IPv4 地址不能多次使用。

- **子网掩码 (Subnet Mask)**
  输入正在创建的子网的子网掩码。不同接口上的子网不得重叠。
- **地址类型 (Address Type)**
  显示地址类型。可能的值包括：
  – 主要 (Primary)
    接口的第一个子网。
- **TIA 接口 (TIA Interface)**
  选择该接口是否应成为 TIA 接口。

组态步骤

1. 从“接口（名称）”(Interface (Name)) 下拉列表中选择接口。
2. 在“接口名称”(Interface Name) 中输入接口的名称。
3. 在“IP 地址”(IP Address) 列中输入子网的 IPv4 地址。
4. 在“子网掩码”(Subnet Mask) 列中输入属于该 IPv4 地址的子网掩码。
5. 单击“设置值”(Set Values) 按钮。

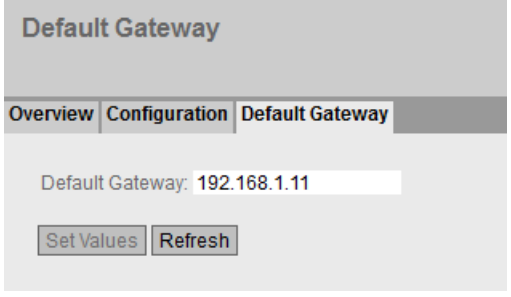
6.6.1.3 默认网关

创建子网

在此页面上定义默认网关。

说明

如果为默认网关组态静态 IP 地址，则会自动对 TIA 接口禁用 DHCP。这可以防止 DHCP 覆盖网关地址。必要时，随后可再次启用 DHCP。



显示值说明

该页面包含以下框：

- **默认网关 (Default Gateway)**
  输入用作默认网关的接口 IP 地址。

组态步骤

1. 输入默认网关。
2. 单击“设置值”(Set Values) 按钮。

6.6.2 DHCP 中继代理

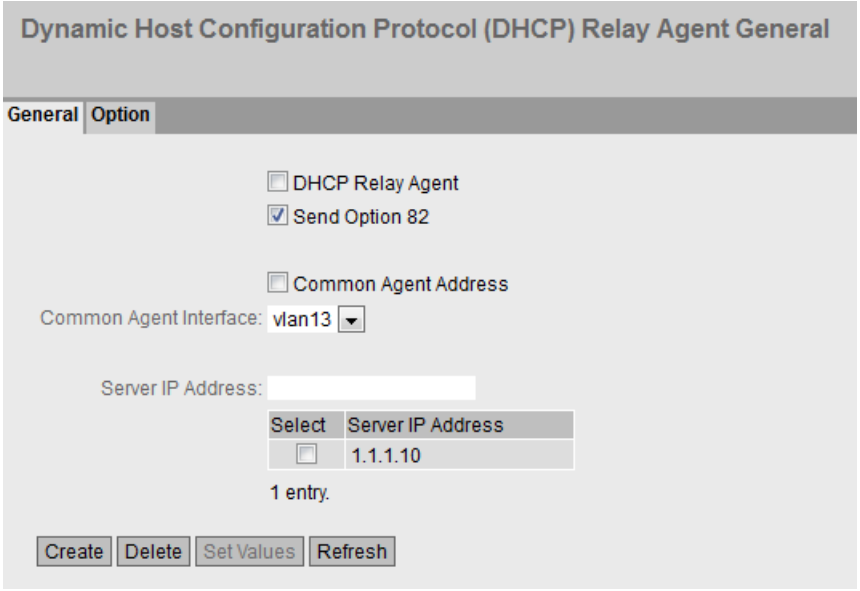
6.6.2.1 常规

DHCP 中继代理

如果 DHCP 服务器与 DHCP 客户端处于不同的网络中，客户端将无法访问服务器。DHCP 中继代理可在 DHCP 服务器与 DHCP 客户端之间进行调停。

如果组态选项 82，则 DHCP 中继代理将通过电路 ID 和远程 ID 将数据包扩展到 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。



显示值说明

该页面包含以下框：

- **DHCP Relay Agent**
  启用或禁用 DHCP 中继代理。
- **Send Option 82**
  启用或禁用选项 82。
- **Common Agent Address**
  启用或禁用公共代理地址。
  当功能激活时，在 DHCP 请求中，中继代理使用“Common Agent Interface”中组态接口的地址替换接收端口的地址。
- **Common Agent Interface**
  中继代理使用此处选择的接口的 IP 地址作为 DHCP 请求中的源地址 (giaddr)。
- **Server IP Address**
  输入 DHCP 服务器的 IPv4 地址。

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

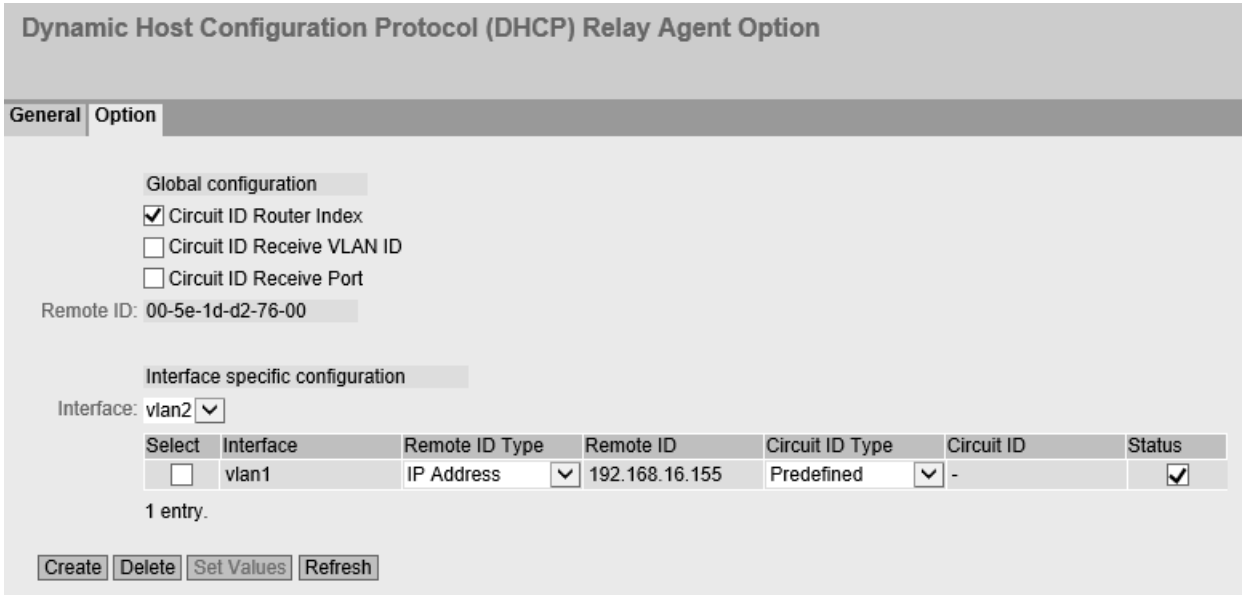
1. 在“Server IP Address”输入框中输入 DHCP 服务器的 IPv4 地址。
2. 单击“Create”按钮。会在表中生成一个新条目。
3. 选中“DHCP Relay Agent”复选框。
4. 选中“Send Option 82”复选框。
5. 单击“Set Values”按钮。

6.6.2.2 选项

DHCP 中继代理的参数

在此页面上，可以指定 DHCP 服务器的参数，例如电路 ID。
电路 ID 描述了 DHCP 查询的来源，例如哪个端口收到了 DHCP 查询。

在“General”选项卡中指定 DHCP 服务器。



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。
- **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。
- **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。

在 IfTable 中使用 SNMP，您将找到有关路由器索引（电路 ID 路由器索引）和端口索引（电路 ID 接收端口）的更多信息。

可在 WBM 页面“Layer 2 > VLAN > General”上找到 VLAN ID。

- **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。
- **Interface**
  显示接口。
- **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。
  - Free Text
    如果使用“Free Text”，可在“Remote ID”中输入设备名称作为设备标识符。
- **Remote ID**
  输入设备名称。只有在为“Remote ID Type”选择条目“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：
  - Predefined
    根据路由器索引、VLAN ID 或端口自动创建电路 ID。
  - Free Number
    如果使用“Free Number”，可为“Circuit ID”输入 ID。
- **Circuit ID**
  输入电路 ID。只有在为“Circuit ID Type”选择“Free Number”条目时才能编辑该框。
- **Status**
  选中该复选框后，将启用对应接口的 DHCP 中继代理。在表中创建新行时，会默认启用 DHCP 中继代理。

组态步骤

按照以下步骤手动指定参数：

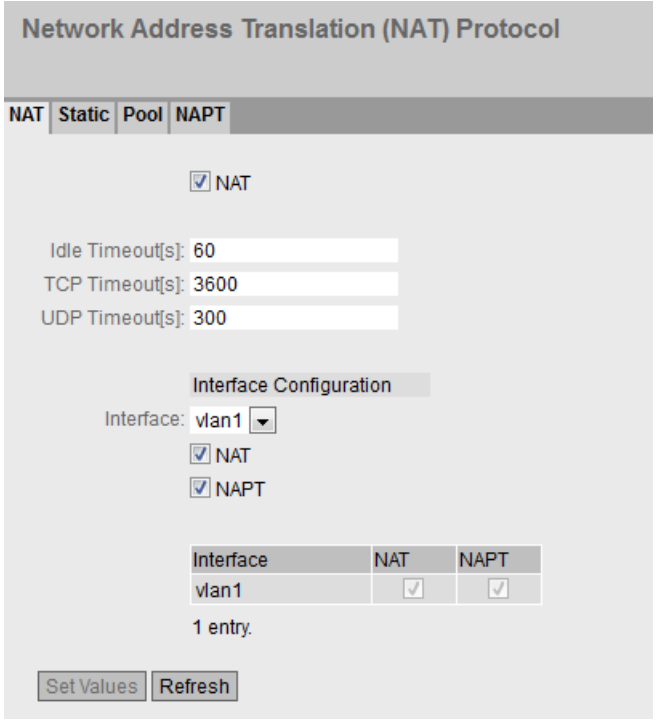
1. 在“Global configuration”中启用所需选项。
   - Circuit ID Router Index
   - Circuit ID Receive VLAN ID
   - Circuit ID Receive Port
2. 单击“Set Values”按钮。
3. 从“Interface”下拉列表中选择接口。

4. 单击“Create”按钮。将在表中插入一个新行。
5. 从该“Remote ID Type”下拉列表中选择所需条目。
   – IP Address
     会将 IPv4 地址用作设备 ID。
   – MAC Address
     将 MAC 地址用作设备 ID。
   – Free Text
     在“Remote ID”中输入设备 ID。
6. 从该“Circuit ID Type”下拉列表中选择所需条目。
   – Predefined
     路由器索引会添加到生成的电路 ID 中。
   – Free Number
     在“Circuit ID”中输入 ID。
7. 单击“Set Values”按钮。

6.6.3 NAT

6.6.3.1 NAT

在此 WBM 页面中可指定 NAT 的基本设置。



说明

该页面包含以下框：

- **NAT**
  对整个设备启用或禁用 NAT/NAPT。启用后，设备将用作 NAT 路由器。
- **Idle Timeout[s]**
  输入所需时间。设备会以该设定时间周期性地检查 TCP 和 UDP 连接的老化时间是否结束。自上次检查后老化时间已结束的连接将从“NAT 转换”表中删除。
- **TCP Timeout[s]**
  为 TCP 连接输入所需的老化时间。只有在该设定时间内未发生数据交换的 TCP 连接才会被存储。根据周期性检查，如果空闲超时已结束，则连接将从“NAT 转换”表中删除。
- **UDP Timeout[s]**
  为 UDP 连接输入所需的老化时间。只有在该设定时间内未发生数据交换的 UDP 连接才会被存储。根据周期性检查，如果空闲超时已结束，则连接将从“NAT 转换”表中删除。
- **Interface**
  从下拉列表中选择您希望在其上组态 NAT 的 IP 接口。
  只要将接口组态为 NAT 接口，所有其它组态都将被视为从该接口开始。这意味着可通过自身接口进行访问的所有网络均被视为“Outside”。所有其它网络均为“Inside”。

  说明

  如果已在设备上组态了多个 NAT 接口，这意味着网络从一个 NAT 接口角度来看为“Outside”，而从另一个 NAT 接口角度来看为“Inside”。

- **NAT**
  为 IP 接口启用或禁用 NAT。
  “Pool”选项卡中将自动创建一个条目。可以使用 IP 接口的 IP 地址从外部网络访问设备。
  如果为 IP 接口禁用 NAT 且 NAT 接口上不存在组态，则将自动删除表中的相关条目。
- **NAPT**
  为 IP 接口启用或禁用 NAPT。

该表格包括以下列：

- **Interface**
  存在 NAT 组态的接口。
- **NAT**
  显示所选 IP 接口的 NAT 是启用还是禁用状态。
  只有为整个设备启用 NAT，NAT 才为启用状态。
- **NAPT**
  显示所选 IP 接口的 NAPT 是启用还是禁用状态。
  只有为整个设备启用 NAT，NAPT 才为启用状态。
  如果不为 NAPT 创建任何更多的组态，将自动启用动态端口转换。
  默认情况下，无法从外部网络访问内部网络中的设备。如果内部设备要在外部网络中进行通信，需为 IP 接口的内部本地地址和 IP 地址添加端口，并为内部设备分配内部本地地址和内部全局地址。使用该内部全局地址，在连接定时器结束之前都可以从外部网络访问内部设备。

步骤

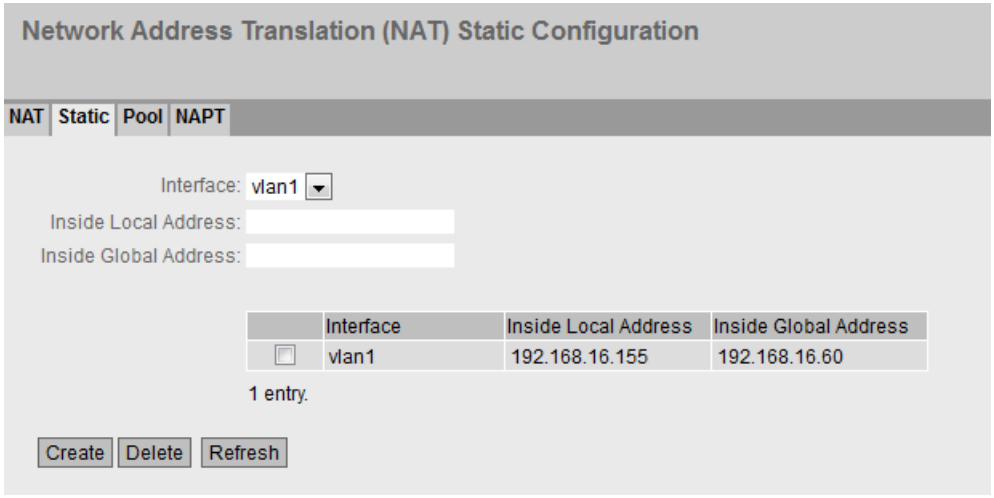
要组态 NAT/NAPT，请执行以下操作：

1. 输入所需时间。
2. 选择所需 IP 接口。
3. 为所选 IP 接口启用 NAT/NAPT。
4. 单击“Set Values”按钮。
5. 在 NAT/NAPT 选项卡中，完成 NAT/NAPT 所需的设置。
6. 选中此选项卡上的“NAT”复选框。
7. 单击“Set Values”按钮。

6.6.3.2 静态 (Static)

在此 WBM 页面中，可组态静态 1:1 地址转换。

用户可指定将与设备的内部本地地址进行相互转换的内部全局地址。此变量允许建立双向连接。这样，便可从外部网络访问内部网络中的设备。



说明

该页面包含以下框：

- **接口 (Interface)**
  从下拉列表中选择您希望为其创建更多 NAT 组态的 NAT 接口。
- **内部本地地址 (Inside Local Address)**
  输入外部可访问的设备的实际地址。
- **内部全局地址 (Inside Global Address)**
  输入可供外部访问设备的地址。

该表格包括以下列：

- **第 1 列 (1st column)**
  选中要删除的行中的复选框。
- **接口 (Interface)**
  与设置相关的 NAT 接口。
- **内部本地地址 (Inside Local Address)**
  显示外部可访问的设备的实际地址。
- **内部全局地址 (Inside Global Address)**
  显示可供外部访问设备的地址。

步骤

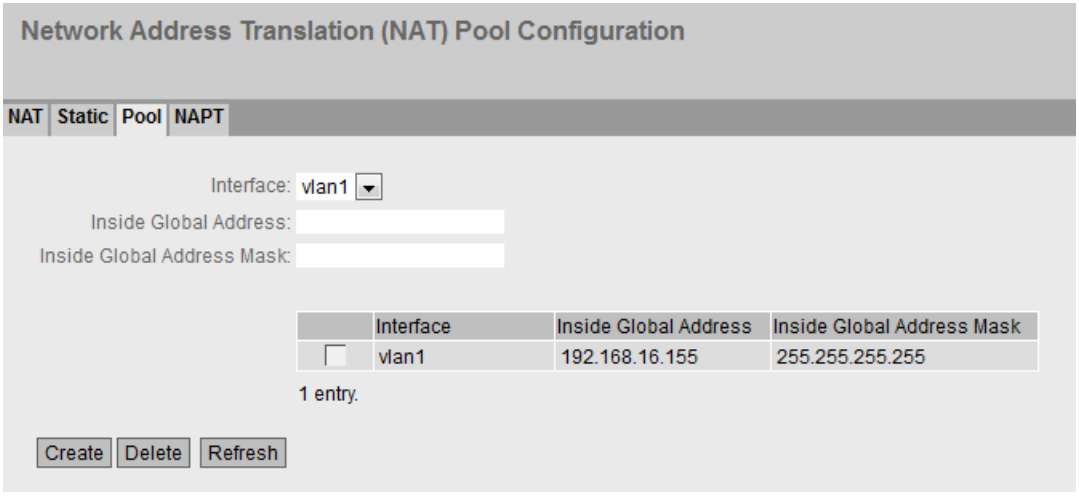
要创建 1:1 地址转换，请按照以下步骤操作：

1. 从“接口”(Interface) 下拉列表中选择 NAT 接口。
2. 在“内部本地地址”(Inside Local Address) 中，输入外部可访问的设备的实际地址。
3. 在“内部全局地址”(Inside Global Address) 中，输入可供外部访问设备的地址。

6.6.3.3 Pool

在此 WBM 页面中，可组态动态地址转换。

默认情况下，无法从外部网络访问内部网络中的设备。如果内部设备要在外部网络中进行通信，需为其动态分配内部全局地址。使用该内部全局地址，在连接定时器结束之前都可以从外部网络访问内部设备。



说明

该页面包含以下框：

- **接口 (Interface)**
  从下拉列表中选择您希望为其创建更多 NAT 组态的 NAT 接口。
- **内部全局地址 (Inside Global Address)**
  输入地址动态分配过程的起始地址，外部可从该地址处访问设备。

  说明

  动态地址转换的地址范围不能包含任何全局 IP 地址。
- **内部全局地址掩码 (Inside Global Address Mask)**
  输入外部子网的地址掩码。

该表格包括以下列：

- **第 1 列 (1st column)**
  选中要删除的行中的复选框。
- **接口 (Interface)**
  与设置相关的 NAT 接口。
- **内部全局地址 (Inside Global Address)**
  显示地址动态分配过程的起始地址，外部可从该地址处访问设备。
- **内部全局地址掩码 (Inside Global Address Mask)**
  显示外部子网的地址掩码。

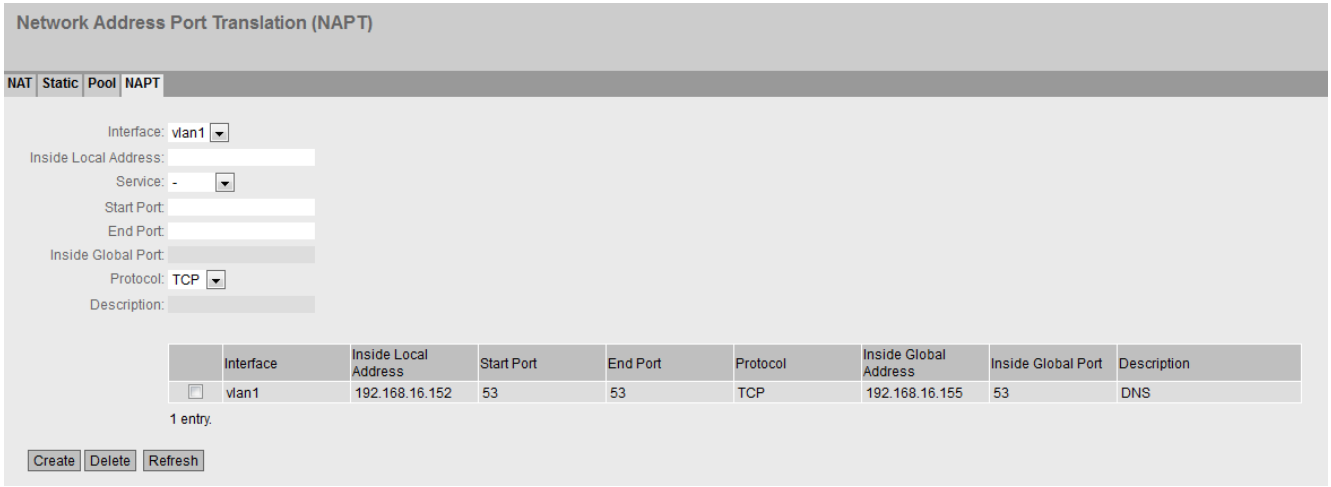
步骤

要创建动态地址转换，请按照以下步骤操作：

1. 从“接口”(Interface) 下拉列表中选择 NAT 接口。
2. 在“内部全局地址”(Inside Global Address) 中，输入地址动态分配过程的起始地址，外部可从该地址处访问设备。
3. 在“内部全局地址掩码”(Inside Global Address Mask) 中，输入外部子网的地址掩码。

6.6.3.4 NAPT

在此 WBM 页面中，可组态静态端口转换。



说明

该页面包含以下框：

- **接口 (Interface)**
  从下拉列表中选择您希望为其创建更多 NAT 组态的 NAT 接口。
- **内部本地地址 (Inside Local Address)**
  输入外部可访问的设备的实际地址。
- **服务 (Service)**
  选择端口转换有效的服务。
  选择服务时，在“起始端口”(Start Port) 和“结束端口”(End Port) 框中输入同一端口。如果更改起始端口，结束端口也会相应地发生变化。
  如果选择条目“-”，则可以随意输入起始端口和结束端口。
- **起始端口 (Start Port)**
  输入一个内部本地端口。
- **结束端口 (End Port)**
  根据您在“服务”(Service) 下拉列表中的选择，可输入一个内部本地端口或显示端口。
  如果在“起始端口”(Start Port) 和“结束端口”(End Port) 框中输入的端口不同，则需在“内部全局端口”(Inside Global Port) 中输入相同的端口范围。端口范围必须相同才能相互转换。
  如果在“起始端口”(Start Port) 和“结束端口”(End Port) 框中输入的端口相同，则可以在“内部全局端口”(Inside Global Port) 中输入任意端口。

- **内部全局端口 (Inside Global Port)**
  根据您在“服务”(Service) 下拉列表中的选择，可输入一个端口或显示端口。
- **协议 (Protocol)**
  选择端口转换有效的协议。
- **说明 (Description)**
  输入端口转换的说明。

该表格包括以下列：

- **第 1 列 (1st column)**
  选中要删除的行中的复选框。
- **接口 (Interface)**
  与设置相关的 NAT 接口。
- **内部本地地址 (Inside Local Address)**
  显示外部可访问的设备的实际地址。
- **起始端口 (Start Port)**
  显示将分配到内部本地地址的起始端口。
- **结束端口 (End Port)**
  显示将分配到内部本地地址的结束端口。
- **协议 (Protocol)**
  显示端口转换有效的协议。
- **内部全局地址 (Inside Global Address)**
  显示可供外部访问设备的地址。
- **内部全局端口 (Inside Global Port)**
  显示将分配到内部全局地址的端口。
- **说明 (Description)**
  显示端口转换的说明。

步骤

要创建静态端口转换，请按照以下步骤操作：

1. 从“接口”(Interface) 下拉列表中选择 NAT 接口。
2. 在“内部本地地址”(Inside Local Address) 中，输入外部可访问的设备的实际地址。
3. 选择服务。
4. 根据您在“服务”(Service) 下拉列表中的选择，指定起始地址、结束地址和内部全局地址。

5. 选择协议。
6. 输入端口转换的说明。

6.7 “Security”菜单

6.7.1 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) 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。

SINEC INS（基础设施网络服务）软件工具中包含用于工业网络的 RADIUS 服务器。SINEC INS 提供管理工业网络所需的所有服务，例如 RADIUS、Syslog、NTP、DHCP、TFTP、SFTP 和 DNS 服务器。

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，并会向设备的属性“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。

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。

6.7.2 用户

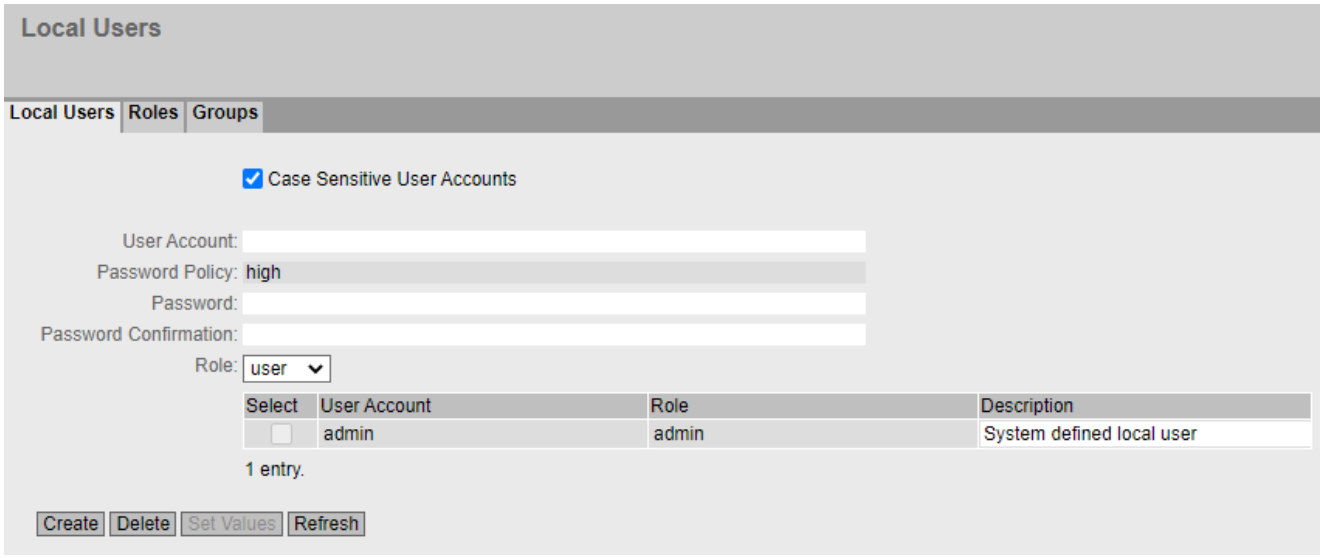
6.7.2.1 本地用户

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。



说明

该页面包含以下框：

- **Case Sensitive User Accounts**
  选中此复选框后，用户名称区分大小写。如果创建的用户名仅大小写不同，则无法再清除此复选框。
- **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 32 个字符之间。
  – 不能包含以下字符：|?";:§°
  也不能包含 Space 和 Delete 字符。

说明

用户名无法更改

创建用户后，便无法再更改用户名。

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

出厂时预设的**用户“user”**

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

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（“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：
  – **High**
  密码长度：至少 8 个字符，最多 32 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
  – **Low**
  密码长度：至少 6 个字符，最多 32 个字符
  – **User defined**
  用户指定密码策略的细节。

  在“Security > Passwords > Options”页面组态设备的密码策略。
- **Password**
  指定密码。密码强度取决于设置的密码策略。

- **Password Confirmation**
  再次输入该密码以进行确认。
- **Role**
  选择角色：
  - user
    读权限：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
    读/写权限：拥有此角色的用户既可读取也可更改设备参数。还可以更改所有用户帐户的密码。

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

说明

“Trial”模式下的更改

即使设备处于“Trial”模式，在此页面上执行的更改也会立即保存。

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“Create”按钮。

删除用户

1. 选中要删除的行中的复选框。
2. 单击“Delete”按钮。将删除条目并更新页面。

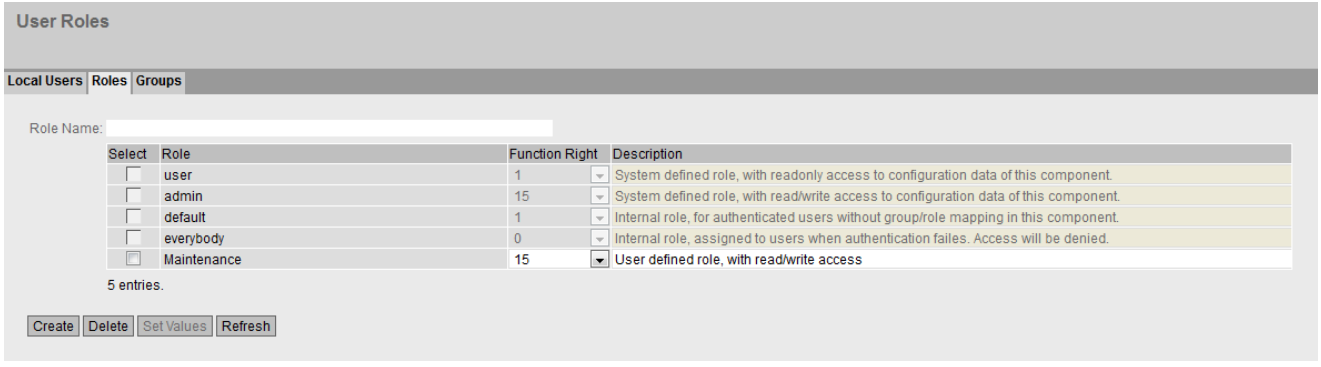
6.7.2.2 角色

角色

在此页面中，可创建在设备本地有效的角色。

说明

显示的值取决于已登录用户的权限。



说明

该页面包含以下内容：

- **Role Name**
  输入角色的名称。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 64 个字符之间。

  说明

  角色名不可更改

  在创建角色后，角色的名称便不可更改。
  如果角色的名称需要更改，则必须删除该角色并创建一个新角色。

该表包含以下列：

- **Select**
  选中要删除的行中的复选框。

  说明

  重新定义的的角色和已分配的角色无法删除或修改。

- **Role**
  显示角色的名称。
- **Function Right**
  选择角色的功能权限：
  - **0**
    如果验证失败，将为用户分配角色。无法访问设备。
  - **1**
    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。
  - **15**
    拥有此角色的用户既可读取也可更改设备参数。

  说明

  功能权限无法更改

  如果您已分配了一个角色，则您无法再更改该角色的功能权限。

  如果要更改角色的功能权限，按照以下列出的步骤操作：

  1. 删除所有已分配的用户。
  2. 更改角色的功能权限：
  3. 再次分配该角色。

- **Description**
  输入角色的说明。对于预定义的角色，将显示一个说明。说明文本最长 100 个字节。

步骤

Creating a role

1. 输入角色的名称。
2. 单击“Create”按钮。
3. 选择角色的功能权限。
4. 输入角色的说明。
5. 单击“Set Values”按钮。

Deleting a role

1. 选中要删除的行中的复选框。
2. 单击“Delete”按钮。将删除条目并更新页面。

6.7.2.3 组

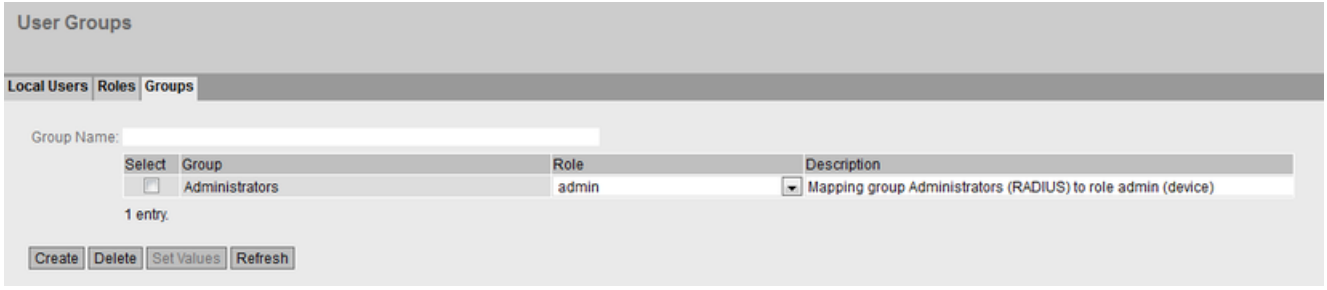
用户组

在此页面中，可将一个组链接到一个角色。

在此示例中，组“Administrators”被链接到“admin”角色：组在 RADIUS 服务器上定义。角色在设备本地定义。当 RADIUS 服务器为用户授权，并将用户分配到“Administrators”组时，此用户便拥有“admin”角色。

说明

显示的值取决于已登录用户的权限。



说明

该页面包含以下内容：

- **Group Name**
  输入组的名称。此名称必须与 RADIUS 服务器上的组相匹配。
  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 64 个字符之间。
  - 不允许使用以下字符：§ ? " ; :

该表包含以下列：

- **Select**
  选中要删除的行中的复选框。
- **Group**
  显示组的名称。
- **Role**
  选择一个角色。通过 RADIUS 服务器上所链接的组进行身份验证的用户会在设备本地获得此角色的权限。
  您可在系统定义的角色和自定义的角色之间选择，请参见页面“Security > Users > Roles”。
- **Description**
  为组与角色的链接输入说明。说明文本最长 100 个字节。

步骤

将组链接到一个角色。

1. 输入组的名称。
2. 单击“Create”按钮。
3. 选择一个角色。
4. 为组与角色的链接输入说明。
5. 单击“Set Values”按钮。

删除组合角色之间的链接

1. 选中要删除的行中的复选框。
2. 单击“Delete”按钮。将删除条目并更新页面。

6.7.3 密码

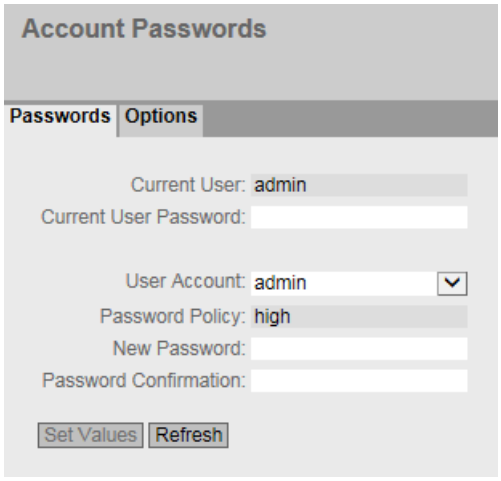
6.7.3.1 密码

组态设备密码

说明

如果通过 RADIUS 服务器登录，则无法更改本地设备的任何密码。

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。如果登录后只具有读权限，则只能更改自己的密码。



显示值说明

该页面包含以下框：

- **Current User**
  显示当前登录的用户。
- **Current User Password**
  输入当前已登录的用户的密码。
- **User Account**
  选择要更改其密码的用户。
- **Password Policy**
  显示分配新密码时正在使用的密码策略。
  - **High**
    密码长度：至少 8 个字符，最多 32 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
  - **Low**
    密码长度：至少 6 个字符，最多 32 个字符
  - **User defined**
    自定义密码策略

  在“Security > Passwords > Options”页面组态密码策略。

- **New Password**
  为所选用户输入新密码。
  不能包含以下字符：
  – § ? " ; :
  – 也不能包含 Delete 字符和空格。
- **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。有一次重命名出厂预设用户的机会“admin”。

出厂时设置的用户名和密码如下：

- admin: admin

说明

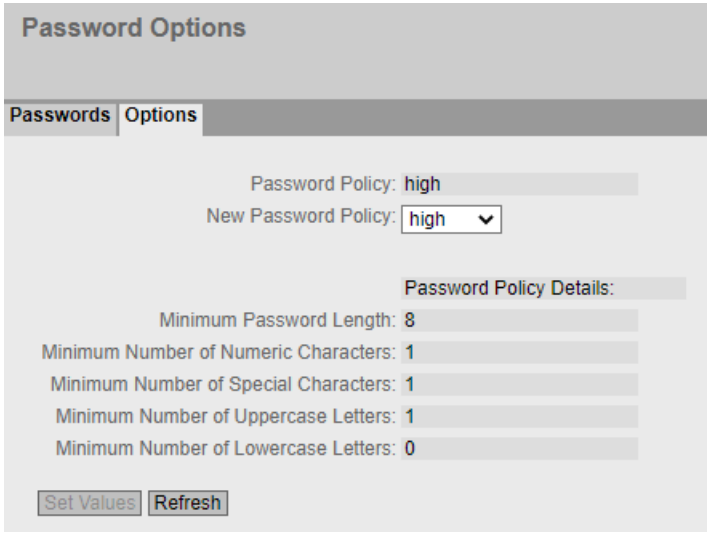
在“Trial”模式下更改密码

即使在“Trial”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。

6.7.3.2 选项

在此页面指定分配新密码时将使用的密码策略。



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 (High)
    密码长度：至少 8 个字符，最长 128 个字符
    至少 1 个数字
    至少 1 个特殊字符
    至少 1 个大写字母
  - 低 (Low)
    密码长度：至少 6 个字符，最长 128 个字符
  - 用户自定义 (User-defined)
    在“密码策略详细信息”(Password Policy Details) 下组态所需密码要求。
- **密码策略详细信息 (Password Policy Details)**
  如果选择了“高”(High) 或“低”(Low) 密码策略，则会显示相关的密码要求。
  如果选择了“用户自定义”(User-defined) 密码策略，可靠组态相关的密码要求。
  - 最短密码长度 (Minimum Password Length)
    指定密码的最短长度。
  - 最少数字字符数 (Minimum Number of Numeric Characters)
    指定密码中的最少数字字符数。
  - 最少特殊字符数 (Minimum Number of Special Characters)
    指定密码中的最少特殊字符数。
  - 最少大写字母数 (Minimum Number of Uppercase Letters)
    指定密码中的最少大写字母数。
  - 最少小写字母数 (Minimum Number of Lowercase Letters)
    指定密码中的最少小写字母数。

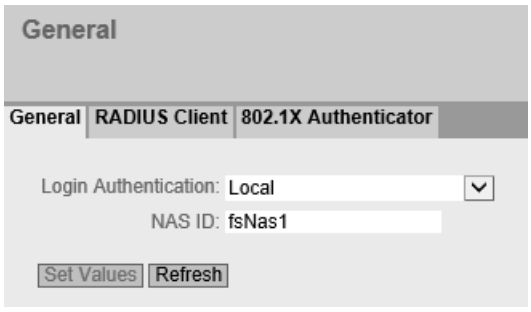
6.7.4 AAA

6.7.4.1 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。



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 ADIUS 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。
- **NAS ID**
  在此文本框中输入 NAS ID (Network Access Server Identifier)。NAS ID 用于识别向 RADIUS 服务器发送请求的设备。

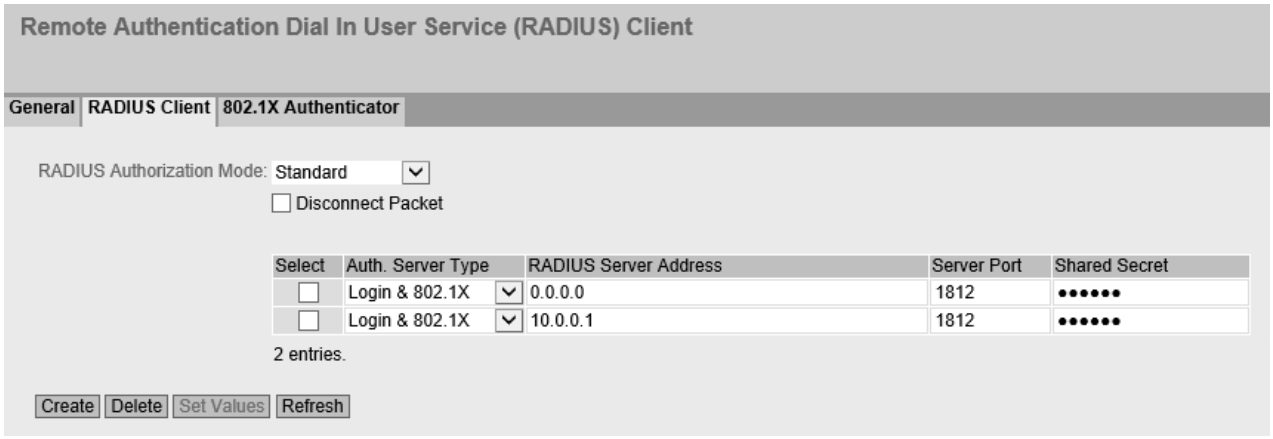
6.7.4.2 RADIUS 客户端

通过外部服务器进行验证

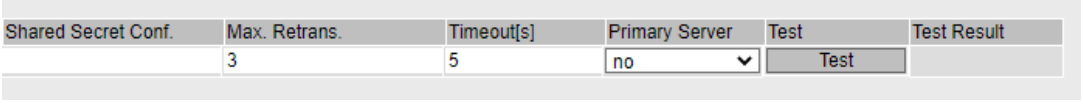
RADIUS 的概念基于外部验证服务器。

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。



续表：



显示框说明

该页面包含以下框：

- **RADIUS 验证模式 (RADIUS Authorization Mode)**
  对于登录验证，RADIUS 验证模式会指定如何为已成功通过身份验证 (页 412)的用户分配权限。
  - 标准 (Standard)
    在此模式下，如果服务器为属性“Service Type”返回值“Administrative User”并发送给设备，则用户将以管理员权限登录。在所有其它情况下，用户将按照读取权限登录。
  - 供应商特定 (Vendor Specific)
    在此模式下，权限的分配取决于服务器是否为用户返回组和具体返回哪个组，以及在“External User Accounts”表中是否存在该用户的对应条目。
- **断开数据包 (Disconnect Packet)**
  如果选中此复选框，则设备会评估 RADIUS 服务器的断开消息。

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 (Auth.Server Type)**
  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。
  - 登录与 802.1X (Login & 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 IP 地址或 FQDN。
- **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。值范围是 1 到 65535。
- **共享密钥 (Shared Secret)**
  在此处输入访问 ID。值范围是 1...128 个字符。
- **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。值范围是 1 到 5。
- **超时 [s] (Timeout [s])**
  在此处输入客户端等待 RADIUS 服务器响应的时间。
- **主服务器 (Primary Server)**
  使用该下拉列表中的选项，指定此服务器是否是主服务器。可选择选项“是”(yes) 或“否”(no) 之一。

- **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：
  - 不可访问 (Not reachable)
    无法访问 IP 地址。
    可以访问 IP 地址，但 RADIUS 服务器尚未运行。
    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：登录与 802.1X (Login & 802.1X)
   - RADIUS 服务器地址：0.0.0.0
   - 服务器端口：1812
   - 最大重传次数：3
   - 主服务器：否
2. 在相关行中，在输入框中输入以下数据：
   - 所需验证服务器类型
   - RADIUS 服务器地址
   - 服务器端口 (Server Port)
   - Shared Secret
   - 确认共享密钥
   - 最大重传次数：3
   - 主服务器：是/否
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：
   - RADIUS 服务器地址
   - 服务器端口 (Server Port)
   - Shared Secret
   - 确认共享密钥
   - 最大重传次数 (Max. Retrans.)
   - 主服务器
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。

对每个要修改其输入内容的服务器重复此步骤

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。将从设备内存中删除此数据并更新该页面。

6.7.4.3 802.1X 验证器

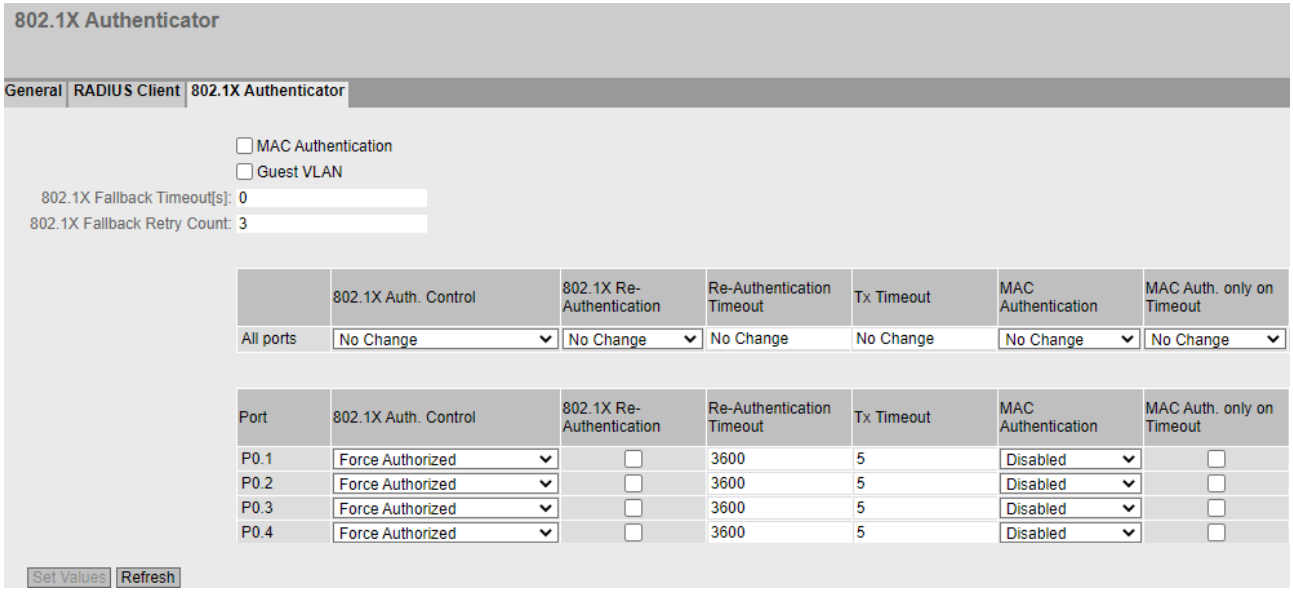
设置网络访问

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。

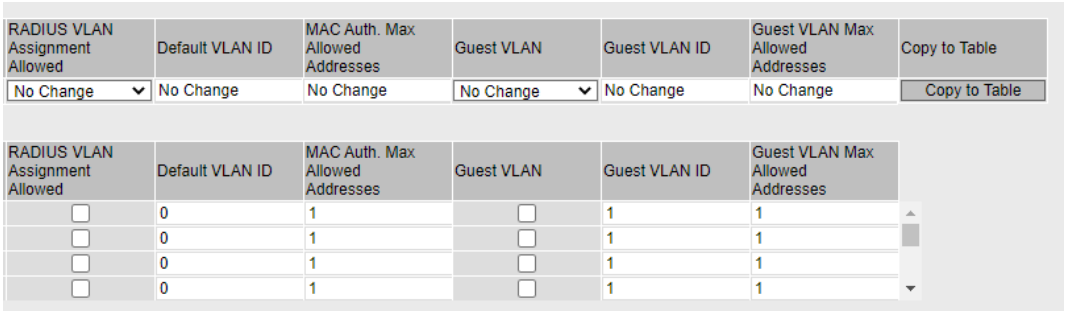
使用 802.1X 进行身份验证时，终端设备和验证服务器都必须支持 EAP 协议 (Extensive Authentication Protocol)。

对单独的端口启用验证

通过启用相应选项，可以为每个端口指定是否在此端口上启用符合 IEEE 802.1X 的网络访问保护。



续表：



显示框说明

该页面包含以下框：

- **MAC 身份验证 (MAC Authentication)**
  为设备启用或禁用“MAC 身份验证”(MAC Authentication)。
- **访客 VLAN (Guest VLAN)**
  为设备启用或禁用 “访客 VLAN”(Guest VLAN) 功能。

- **802.1X 回退超时 [s] (802.1X Fallback Timeout[s])**
  指定 MAC 身份验证失败时设备在相关端口对设备重新初始化以进行 802.1X 身份验证之前经过的时间间隔（以秒为单位）。默认值为 0 秒，即没有回退超时，且不会重新初始化以进行 802.1X 身份验证。
- **802.1X 回退重试计数 (802.1X Fallback Retry Count)**
  指定 MAC 身份验证失败时对端口重新初始化以进行 802.1X 身份验证的频率。

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.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。
- **重新验证超时 (Re-Authentication Timeout)**
  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。
- **Tx 超时 (Tx Timeout)**
  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 身份验证 (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。
- **仅限超时时进行 MAC 验证 (MAC Auth. only on Timeout)**
  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。

- **允许的 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。

  说明

  仅在尚未为此VLAN组态端口时，才会应用RADIUS进行的VLAN分配。如果端口VLAN ID与由 RADIUS 分配的 VLAN ID 匹配，则必须已预组态此 VLAN 中的成员类型。

  说明

  私有 VLAN 功能和 RADIUS 验证

  当通过 RADIUS 验证为 VLAN 的一个或多个端口启用 VLAN 分配时，不应将此 VLAN 另外组态为私有 VLAN。

  与通过 RADIUS 验证进行 VLAN 分配相关的私有 VLAN 功能可能会导致系统状态不一致。

- **默认 VLAN ID (Default VLAN ID)**
  指定所需的 VLAN ID。
  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.最大允许地址数 (Max Allowed Addresses)**
  指定可以同时在端口上通信的 MAC 地址数目。
  如果输入“不变”(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)**
  指定端口的 VLAN ID。
  如果输入“不变”(No Change)，则表 2 中的条目保持不变
- **访客 VLAN 的最大允许地址数 (Guest VLAN Max Allowed Addresses)**
  指定“访客 VLAN”的此端口上可同时允许的终端设备数目。
  如果输入“不变”(No Change)，则表 2 中的条目保持不变
- **复制到表 (Copy to Table)**
  如果单击此按钮，则为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **端口 (Port)**
  此列会列出此设备上的全部可用端口。
- **802.1X 验证控制 (802.1X Auth.控制 (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。
    出厂设置
  - 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 重新验证 (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。
- **重新验证超时 (Re-Authentication Timeout)**
  指定设备在相关接口中进行重新验证之前经过的时间间隔（以秒为单位）。
  默认值为 3600 秒。
- **Tx 超时 (Tx Timeout)**
  该值指定无客户端响应的情况下发送 EAP 请求数据包之前经过的时长（以秒为单位）。如果已启用 MAC 身份验证，会在发送第三个 EAP 请求数据包后从 802.1X 身份验证切换为 MAC 身份验证。
  默认值为 5 秒。

- **MAC 身份验证 (MAC Authentication)**
  组态端口的 MAC 验证：
  - 禁用 (Disabled)
    端口的 MAC 验证已禁用。
  - 启用 (Enabled)
    如果要通过“MAC 身份验证”方法对终端设备进行身份验证，请为端口选择此选项。如果 “802.1X 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”步骤的超时为 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。
  - Sticky
    如果组态此参数，则会根据端口上当前验证的 MAC 地址自动验证或拒绝新 MAC 地址（MAC 身份验证允许的最大地址数）。
    如果端口上的新 MAC 地址请求数与端口上当前验证的 MAC 地址数 < 允许的最大 MAC 地址数，则请求自动成功。
    如果端口上的新 MAC 地址请求数与端口上当前验证的 MAC 地址数 ≥ 允许的最大 MAC 地址数，则请求自动失败。
    通过此机制验证的 MAC 地址作为静态 MAC 地址进行存储。链路变化事件以及设备重启过程中，会保留验证状态。必须手动删除 MAC 地址。

    说明

    要求：
    - 仅当已在全局为设备启用 MAC 身份验证时，此参数才会激活。
    - “802.1X 身份验证控制”(802.1X Auth. Control) 组态为 “强制授权”(Force Authorized)。
    - 为“MAC 身份验证允许的最大地址数”(MAC Auth. Max Allowed Addresses) 组态 ≥ 1 且 ≤ 5 的值。
    - 端口上静态组态的 MAC 地址数 ≤ 允许的最大地址数。

    说明

    不需要为此参数进行 RADIUS 服务器组态。

    如果组态了此参数，则以下内容适用于对应端口：
    - 仅可为“MAC 身份验证允许的最大地址数”(MAC Auth. Max Allowed Addresses) 组态 ≤ 5 的值。
    - 仅当静态 MAC 地址数 < 允许的最大 MAC 地址数（“MAC 身份验证允许的最大地址数”）时，才能组态新的静态 MAC 地址。

- **仅限超时时进行 MAC 验证 (MAC Auth. only on Timeout)**
  选中该复选框后，只有在 802.1X 超时后才能进行 MAC 验证，但在 802.1X 验证失败后不能进行。如果未选中该复选框，则在 802.1X 超时和 802.1X 验证失败后均可进行 MAC 验证。

- **“允许的 RADIUS VLAN 分配”(RADIUS VLAN Assignment Allowed)**
  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 412)。
  如果在验证期间使用此功能将端口动态分配到 VLAN，则可使用 VLAN ID 或 VLAN 名称进行分配。组态 RADIUS 服务器中的以下值：
  - Tunnel-Type = VLAN
  - Tunnel-Medium-Type = IEEE-802
  - Tunnel-Private-Group-Id = VLAN ID 或 VLAN 名称

  工业以太网交换机的区别如下：
  - VLAN ID：RADIUS 服务器传输参数“Tunnel-Private-Group-Id”的数字字符串。
  - VLAN 名称：RADIUS 服务器传输参数“Tunnel-Private-Group-Id”的字母数字字符串。
- **默认 VLAN ID (Default VLAN ID)**
  如果在成功验证之后通过 RADIUS 服务器发送 VLAN ID，并选中了“允许的 RADIUS VLAN 分配”(RADIUS VLAN Assignment Allowed) 复选框，则端口的当前 PVID 会更改为 RADIUS 服务器发送的值。此外，可能会在相关 VLAN 中建立端口的“无标记成员关系”(Untagged membership)，以实现在相应 VLAN 中的通信。
  选中“允许的 RADIUS VLAN 分配”(RADIUS VLAN Assignment Allowed) 后，“默认 VLAN ID”(Default VLAN ID) 会确定 VLAN ID 的分配，但在成功验证后，RADIUS 服务器不会发送 VLAN ID。有两个选项：
  - **为“默认 VLAN ID”**(Default VLAN ID) 组态值“0”
    当前为端口组态的 PVID 会继续使用。
  - **为“默认 VLAN ID”**(Default VLAN ID) 组态处于“1 ... 4094”范围内的值
    端口的 PVID 更改为该列中组态的“默认 VLAN ID”(Default VLAN ID)，如同由 RADIUS 服务器传输的一样。

  在所有情况下，设备注销后，更改的 PVID 会复位为初始组态的值。建立的任意“端口成员关系”(Port membership) 会再次被删除。这适用于 802.1X 验证和 MAC 验证。
- **MAC 验证允许的最大地址数 (MAC Auth.最大允许地址数 (Max Allowed Addresses)**
  指定可以同时在端口上通信的 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 Auth.Max Permitted Addresses) 框中输入数字。
- **访客 VLAN (Guest VLAN)**
  如果希望在身份验证失败的情况下允许在“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 412)。
  该功能也称为“Authentication failed VLAN”。

- **访客 VLAN ID (Guest VLAN ID)**
  输入访客 VLAN 的 VLAN ID。
- **访客 VLAN 的最大允许地址数 (Guest VLAN Max Allowed Addresses)**
  指定“访客 VLAN”的此端口上可同时允许的终端设备数目。

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“设置值”(Set Values) 按钮。

对所有端口启用验证

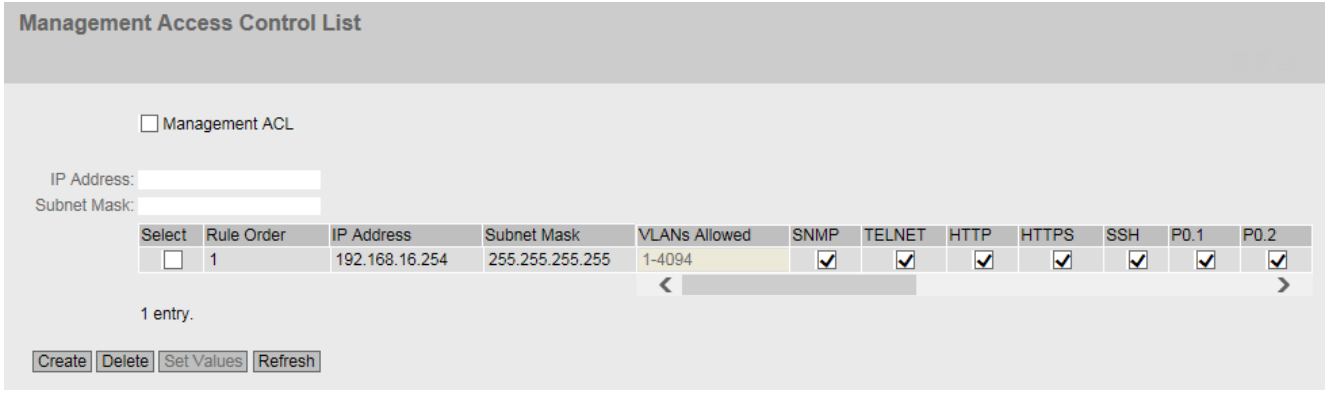
1. 在表 1 中选中所需选项。
2. 单击“复制到表”(Copy to Table) 按钮。表 2 中所有端口均采用相关设置。
3. 要应用更改，请单击“设置值”(Set Values) 按钮。

6.7.5 Management 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。



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)**
  - 基础网桥模式“802.1Q VLAN 网桥”中
    输入设备所在的 VLAN 的编号。仅当设备位于该组态 VLAN 中时，站才能访问该设备。
    如果该输入框留空，则没有关于 VLAN 的限制。
  - 基础网桥模式“802.1D 透明网桥”中
    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。
- **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。

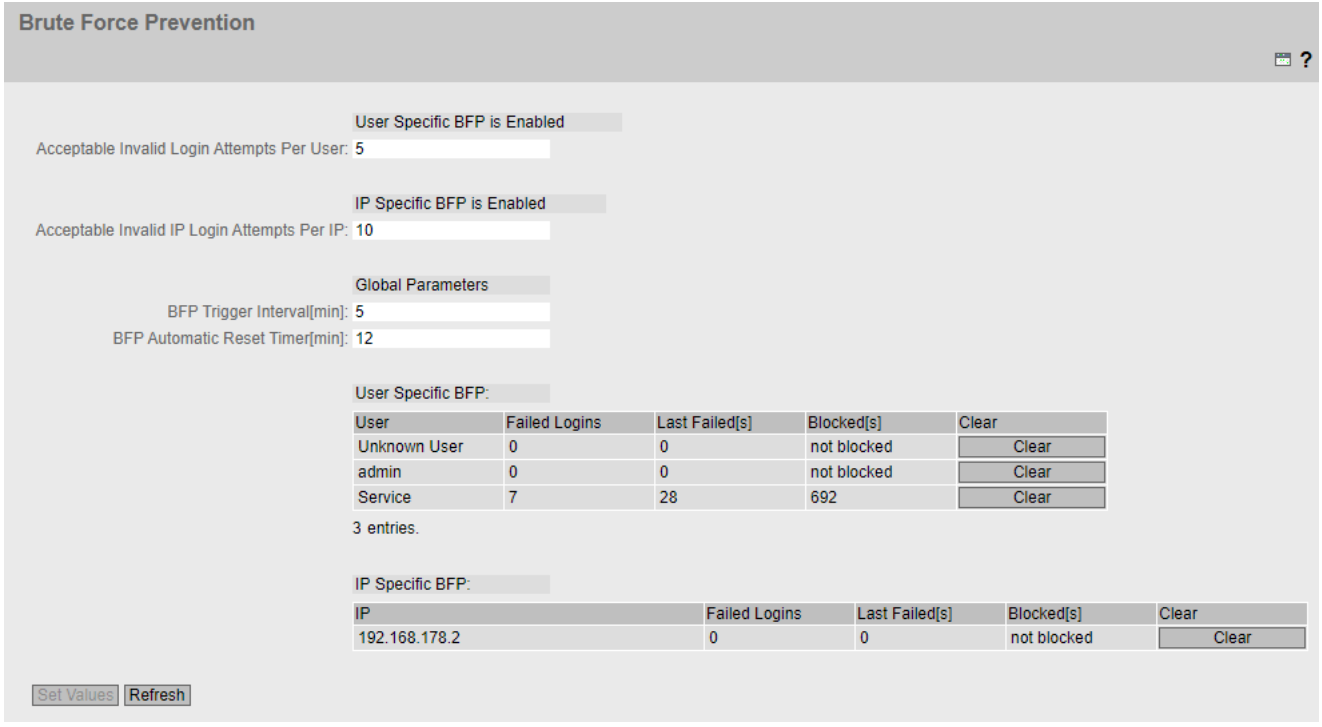
删除规则

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。

6.7.6 暴力破解预防

组态说明

暴力破解预防是指试图通过数量足够大的密码防止设备受到未授权访问。会通过限制特定时间段内的错误登录尝试次数实现此目的。



显示框说明

该页面包含以下框：

- **用户特定的 BFP 已启用/用户特定的 BFP 已禁用 (User Specific BFP is Enabled / User Specific BFP is Disabled)**
  显示是否启用用户特定的“暴力破解预防”(Brute Force Prevention)。
  登录身份验证决定了是否可启用用户特定的“暴力破解预防”(Brute Force Prevention)。在“安全 > AAA > 常规”(Security > AAA > General) 菜单中的“登录身份验证”(Login Authentication) 下拉列表中组态登录身份验证。用户特定的“暴力破解预防”(Brute Force Prevention) 可用于“本地”(Local) 和“本地和 RADIUS”(Local and RADIUS) 模式，不可用于“RADIUS”和“RADIUS 和本地回退”(RADIUS and Fallback Local) 模式。
- **每个用户的可接受无效登录尝试次数 (Acceptable Invalid Login Attempts Per User)**
  用户的最大无效登录尝试次数，超过此次数后，将禁止登录。所有未组态为设备本地用户的用户均会归纳到用户名“UnknownUser”下。
  如果组态值“0”，则会禁用用户特定的“暴力破解预防”(Brute Force Prevention)。
  默认值为“12”。
- **IP 特定的 BFP 已启用 (IP Specific BFP is Enabled)**
  显示是否启用用户特定的 “暴力破解预防”(Brute Force Prevention)。
- **每个 IP 的可接受无效 IP 登录尝试次数 (Acceptable Invalid IP Login Attempts Per IP)**
  IP 地址的最大无效登录尝试次数，超过此次数后，将禁止登录。
  如果组态值“0”，则会禁用 IP 特定的“暴力破解预防”(Brute Force Prevention)。
  默认值为“10”。
- **BFP 触发间隔 [分钟] (BFP Trigger Interval [min])**
  与计算无效登录尝试次数相关的时间（以分钟为单位）。如果在此时间内达到允许的无效登录尝试次数（每个用户和每个 IP 地址），设备会在特定时间段内禁止登录。每个用户和每个 IP 地址的无效登录尝试次数是彼此独立处理的。可输入 5 到 255 分钟之间的值。
  默认值为 5 分钟。
- **BFP 自动复位定时器 [分钟] (BFP Automatic Reset Timer[min])**
  设备因超出最大无效登录尝试次数而禁止登录的持续时间。可输入 0 到 255 分钟之间的值。
  如果组态的值为“0”，则在达到最大无效登录尝试次数后即将无限期地禁止登录。
  默认值为 12 分钟。

用户特定的 BFP (User Specific BFP) 表包括以下列：

- **用户 (User)**
  尝试登录的用户。
- **登录失败次数 (Failed Logins)**
  登录尝试失败次数。

- **上次失败时间（秒）(Last Failed[s])**
  上次登录尝试失败的时间（以秒为单位）。要显示当前值，请单击“Refresh”按钮。
- **禁止时间（秒）(Blocked[s])**
  显示用户的状态：
  - 未禁止 (Not blocked)
    可以使用此用户名登录。
  - 持续时间 (Duration)
    禁止使用该用户名登录的时间（以秒为单位）。要显示当前值，请单击“刷新”(Refresh) 按钮。
    如果由于“BFP 自动复位定时器”(BFP Automatic Reset Timer) 中组态的时间已到而解除了禁止，则用户的状态会变为“未禁止”(Not blocked)。
  - 无限期禁止 (Indefinitely blocked)
    禁止使用该用户名登录，直至手动删除禁止或重新启动设备。
- **删除 (Delete)**
  结束对此用户的禁止并复位以下显示值：
  - “上次失败时间”(Last Failed) 框中的值复位为“0”。
  - “禁止”(Blocked) 框中用户的状态设为“未禁止”(Not blocked)。

“IP 特定的 BFP”(IP Specific BFP) 表包括以下列：

- **IP**
  用于登录尝试的设备的 IP 地址。
- **登录失败次数 (Failed Logins)**
  登录尝试失败次数。
- **上次失败时间 (Last Failed)**
  上次登录尝试失败的时间（以秒为单位）。要显示当前值，请单击“刷新”(Refresh) 按钮。

- **禁止时间（秒）(Blocked[s])**
  显示 IP 地址的状态：
  - 未禁止 (Not blocked)
    可以使用此 IP 地址登录。
  - 持续时间 (Duration)
    禁止使用该 IP 地址登录的时间（以秒为单位）。要显示当前值，请单击“刷新”(Refresh) 按钮。
    如果由于“BFP 自动复位定时器”(BFP Automatic Reset Timer) 中组态的时间已到而解除了禁止，则 IP 地址的状态会变为“未禁止”(Not blocked)。
  - 无限期禁止 (Indefinitely blocked)
    禁止使用该 IP 地址登录，直至手动删除禁止或重新启动设备。
- **删除 (Delete)**
  结束对 IP 地址的禁止并复位以下显示值：
  - “上次失败时间”(Last Failed) 框中的值复位为“0”。
  - “禁止”(Blocked) 框中 IP 地址的状态设为“未禁止”(Not blocked)。

故障排除/FAQ

7

7.1 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。

轻轻地按下 SCALANCE XB-200 上的“RESET”按钮。

按 SCALANCE XC-200 上的“SELECT/SET”按钮。

按 SCALANCE XF-200BA 上的“SET”按钮。

轻轻地按下 SCALANCE XF-200G 上的“RESET”按钮。

用力按下 SCALANCE XP-200 上的“RESET”按钮。

按 SCALANCE XR-300WG 上的“RESET”按钮

在 Microsoft Windows 下的步骤

可以使用 TFTP 将新固件下载到设备中。这样，无需使用“基于 Web 的管理”(WBM) 和“命令行接口”(CLI) 便可访问设备。如果在固件更新期间断电，可能会出现这种情况。

对该按钮进行按压操作时，请遵循“使用 TFTP 下载新固件（无需 WBM 和 CLI） (页 445)”部分提供的信息。

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 SELECT/SET 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。
   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 与设备的以太网端口相连。

6. 使用 DHCP 或 SINEC PNI 为设备分配 IP 地址。
7. 在 Windows 命令提示中，转到保存新固件文件的目录，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)

固件完全传送到设备并经过验证后，设备将重启。该过程可能需要数分钟时间。

7.2 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。

7.3 通过 STEP 7 Basic/Professional 使用文件交换组态数据

通过两种文件类型"RunningSINEMAConfig"和"SINEMAConfig"（"System > Load&Save > HTTP/TFTP/SFTP"）使用文件在设备 (WBM) 和 STEP 7 Basic/Professional 之间交换组态数据。通过 STEP 7 Basic/Professional 导出/导入文件的操作如下所述。

通过 STEP 7 Basic/Professional 导出组态数据

要通过 STEP 7 Basic/Professional 导出组态数据，请按以下步骤操作：

1. 在 STEP 7 Basic/Professional 中打开相关的 STEP 7 项目。
2. 打开项目视图。
3. 打开网络视图或拓扑视图。
4. 打开硬件目录。
5. 在硬件目录中，导航到包含相关订货号的设备。
6. 单击鼠标选择所需设备。
7. 通过硬件目录的下拉列表设置匹配的固件版本。
8. 将设备拖放至网络视图或拓扑视图。
9. 在网络视图或拓扑视图中选择设备。
10. 在巡视窗口的"Properties > General"中组态设备。
11. 在巡视窗口中，导航到"Properties > General"下的"Management"参数。
12. 在参数组"Load / save file"中，单击"Save to file"按钮。
13. 选择文件的存储位置。
14. 分配文件名称。
15. 单击"Save"按钮。
    "Save configuration file"对话框随即打开。
16. 分配文件加密密码。

    说明

    通过 WBM 将文件加载到设备时需要此密码。

17. 单击"OK"按钮。

通过 STEP 7 Basic/Professional 导入组态数据

要通过 STEP 7 Basic/Professional 导入组态数据，请按以下步骤操作：

1. 在 STEP 7 Basic/Professional 中打开相关的 STEP 7 项目。
2. 打开项目视图。
3. 打开网络视图或拓扑视图。

4. 打开硬件目录。
5. 在硬件目录中，导航到包含相关订货号的设备。
6. 单击鼠标选择所需设备。
7. 通过硬件目录的下拉列表设置匹配的固件版本。
8. 将设备拖放至网络视图或拓扑视图。
9. 在网络视图或拓扑视图中选择设备。
10. 在巡视窗口中，导航到“Properties > General”下的“Management”参数。
11. 在参数组“Load / save file”中，单击“Load from file”按钮。
12. 选择所需文件。
13. 单击“打开”(Open) 按钮。
    “Load configuration file”对话框随即打开。
14. 输入文件解密密码。

    说明

    可在 WBM 中的“系统 > 加载和保存 > 密码”(System > Load&Save > Passwords) 下分配该密码。

15. 单击“OK”按钮。

附录 A“Syslog 消息”

A

Syslog 消息可包含以下参数：

参数	说明	可能值或示例
ip address	IPv4 或 IPv6 地址	IP 地址（符合 RFC1035 或 RFC4291 第 2.2 部分）
src port dest port	显示为十进制数的端口。 格式：%d	0 ... 65535
dest mac src mac	MAC 地址 格式：%02x:%02x:%02x;%02x:%02x:%02x	00:0C:29:2F:09:B3
protocol	生成此事件的服务的名称或使用的第 4 层协议的名称。 格式：%s	可能的条目： UDP | TCP | WBM | Telnet | SSH | TFTP | SFTP
group	用于根据名称标识组的字符串 格式：%s	it-service
user name	根据他/她的姓名识别经验证的用户的字符串（无空格） 格式：%s	maier
action user name	根据他/她的名称识别用户。此用户不是经验证的用户。 格式：%s	Peter.Maier
role	组角色的符号名 格式：%s	管理员
time minute timeout	分钟数 格式：%d	44
failed login count	登录失败次数 格式：%d	10
max sessions	会话数目 格式：%d	10

参数	说明	可能值或示例
trigger pin	用于触发事件的 IO 引脚的字符串 （无空格） 格式：%s	DI1
firewall rule	用于防火墙规则的字符串 （带空格） 格式：%s	Rule1
subject	用于证书中的主题的字符串。用作基于证书的验证的一部分 带空格，还必须包含 Unicode 字符 格式：(% S) 或 (% S% S)（对于 UTF8 代码）。	(Peter Maier)
config detail	用于组态的字符串 （带空格） 格式：%s	OpenVPN
connection name	VPN 连接的名称	to_Baugruppe1
firewall accept	执行的防火墙操作（已接受数据包）	ACCEPT
firewall action reject	执行的防火墙操作（已拒绝数据包）	REJECT DROP
length	网络数据包长度（以字节为单位） 格式：%d	52
network interface	网络接口的符号名称 格式：%s	vlan1

用户标识和验证

{Local interface}: User {User name} logged in.

示例	Console: User admin logged in.
说明	用户已通过本地界面成功登录设备。 在示例中，“admin”用户通过控制台接口成功登录。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 1.1

{Local interface}: User {User name} failed to log in.

示例	Console: User admin failed to log in.
说明	登录期间指定的用户名称或密码错误。
Severity	Warning
Facility	local0
标准	IEC 62443-3-3 参考：SR 1.1

{Protocol}: User {User name} logged in from {IP address}.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin logged in from 192.168.0.1.
说明	登录期间指定的有效登录信息。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 Reference: SR 1.1

{Protocol}: User {User name} failed to log in from {IP address}.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin failed to log in from 192.168.0.1.
说明	登录期间指定的用户名称或密码错误。
Severity	Warning
Facility	local0
标准	IEC 62443-3-3 Reference: SR 1.1

{Local interface}: User {User name} logged out.

示例	Console: User admin logged out.
说明	用户已通过设备的本地接口注销。 在示例中，"admin"用户通过控制台接口手动注销。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 1.1

{Protocol}: User {User name} logged out from {IP address}.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin logged out from 192.168.0.1.
说明	会话以用户注销结束。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 Reference: SR 1.1

{Local interface}: Default user {User name} logged in.

示例	Console: Default user admin logged in.
说明	用户已使用默认用户配置文件和密码通过本地设备接口成功登录设备。 在示例中，默认用户“admin”通过控制台接口成功登录。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：n/a (NERC-CIP 007-R5)

{Protocol}: Default user {User name} logged in from {IP address}.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: Default user <user name> logged in from 192.168.0.1.
说明	默认用户已通过 IP 地址登录。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 Reference: n/a (NERC-CIP 007-R5)

{Protocol}: {IP address} - No response from the RADIUS server.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: 192.168.1.105 - No response from the RADIUS server.
说明	未对服务器进行访问或服务器无响应。
Severity	Warning
Facility	local0
标准	IEC 62443-3-3 参考：SR 1.1

{Protocol}: {IP address} - No response from the IdP server.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: 192.168.1.105 - No response from the IdP server.
说明	未对服务器进行访问或服务器无响应。
Severity	Warning
Facility	local0
标准	IEC 62443-3-3 参考：SR 1.1

用户帐户管理

{Protocol}: Password protection was enabled for resource {Resource}.

示例	WBM: Password protection was enabled for resource FullReadAccess.
说明	已为该资源启用密码保护。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 1.3

{Protocol}: Authentication was enabled.

示例	WBM: Authentication was enabled.
说明	已启用验证。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 1.3

{Protocol}: Password protection was disabled for resource {Resource}.

示例	WBM: Password protection was disabled for resource FullReadAccess.
说明	已为该资源禁用密码保护。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 1.3

{Protocol}: Authentication was disabled.

示例	WBM: Authentication was disabled.
说明	已禁用验证。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 1.3

{Protocol}: User {User name} changed own password.

示例	WBM: User admin changed own password.
说明	用户已更改自己的密码。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR1.3

{Protocol}: User {User name} changed password of user {Action user name}.

示例	Telnet: User admin changed password of user test.
说明	用户已更改其它用户的密码。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR1.3

{Protocol}: User {User name} disabled user-account {Destination user name}.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User <User name> disabled user-account {Destination user name}.
说明	经过身份验证的用户屏蔽了其他用户的用户帐户。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 2.4

{Protocol}: User {User name} enabled user-account {Destination user name}.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User <User name> enabled user-account {Destination user name}.
说明	经过身份验证的用户屏蔽了其他用户的用户帐户。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 2.4

{Protocol}: Default admin account was changed to {User name}.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: Default admin account was changed to maier.
说明	默认管理员帐户已更改。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 1.3

{Protocol}: Default user account was changed to {User name}.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: Default user account was changed to <new user>.
说明	默认帐户已更改
Severity	Info
Facility	local0
标准	IEC 62443-3-3 Reference: SR 1.3

{Protocol}: User {User name} created user-account {Action user name}.

示例	WBM: User admin created user-account service.
说明	用户已创建一个帐户。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR1.3

{Protocol}: User {User name} changed user-account {Destination user name} with role {Role}.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin changed user-account admin2 with role Administrator.
说明	管理员已更改现有帐户。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 1.3

{Protocol}: User {User name} deleted user-account {Action user name}.

示例	WBM: User admin deleted user-account service.
说明	管理员已删除现有帐户。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR1.3

授权执行

{Protocol}: The firewall {Firewall rule} for User {User name} was granted. Timeout is {Timeout} min.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: The firewall Rule 1 for User admin was granted. Timeout is 44 min.
说明	已保证重要资源的访问权限。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：n/a (NERC-CIP 005-R2)

{Protocol}: The firewall {Firewall rule} for {Trigger pin} was granted. Timeout is {Timeout} min.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: The firewall Rule 1 for DI1 was granted. Timeout is 44 min.
说明	已保证重要资源的访问权限。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：n/a (NERC-CIP 005-R2)

{Protocol}: The firewall {Firewall rule} for User {User name} was denied.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: The firewall Rule 1 for User admin was denied.
说明	重要资源的访问被拒绝。
Severity	Warning
Facility	local0
标准	IEC 62443-3-3 参考：SR 2.1

{Protocol}: The firewall {Firewall rule} for {Trigger pin} was denied.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: The firewall Rule 1 for DI1 was denied.
说明	重要资源的访问被拒绝。
Severity	Warning
Facility	local0
标准	IEC 62443-3-3 参考：SR 2.1

{Protocol}: The firewall {Firewall rule} for User {User name} was denied by administrator.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: The firewall Rule 1 for User maier was denied by administrator.
说明	重要资源的访问被拒绝。
Severity	Warning
Facility	local0
标准	IEC 62443-3-3 参考：SR 2.1

标识符管理

{Protocol}: User {User name} created group {Group} and assigned to role {Role}.

示例	WBM: User admin created group it-service and assigned to role service.
说明	管理员已创建组并为其分配角色。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 1.4

{Protocol}: User {User name} deleted group {Group} and the role {Role} assignment.

示例	WBM: User maier deleted group it-service and the role service assignment.
说明	管理员已删除现有组及角色分配。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 1.4

{Protocol}: User {User name} created role {Role}.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User <User name> created role <Role>.
说明	已创建角色。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 4.7

{Protocol}: User {User name} deleted role {Role}.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User <User name> deleted role <Role>.
说明	已删除角色。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 4.8

{Protocol}: User {User name} changed role {Role}.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User <User name> changed role <Role>.
说明	已更改角色。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 4.9

登录尝试失败

{User name} account is locked for {Time minute} minutes after {Failed login count} unsuccessful login attempts.

示例	User service account is locked for 44 minutes after 10 unsuccessful login attempts.
说明	如果登录失败次数过多，则相应的用户帐户将被锁定一段特定的时间。
Severity	Warning
Facility	local0
标准	IEC 62443-3-3 参考：SR 1.11

{Protocol}: {IP address} is blocked for {Time second} seconds after {Failed login count} unsuccessful login attempts.

示例	WBM: 192.168.1.105 is blocked for 600 seconds after 11 unsuccessful login attempts.
说明	如果登录失败次数过多，则相应的 IP 地址将被锁定一段特定的时间。
Severity	Warning
Facility	local0
标准	IEC 62443-3-3 参考：SR 1.11

会话锁定

The session of user {User name} was closed after {Time} seconds of inactivity.

示例	The session of user admin was closed after 60 seconds of inactivity.
说明	当前会话因非活动状态而被锁定。
Severity	Warning
Facility	local0
标准	IEC 62443-3-3 参考：SR 2.5

关闭远程访问会话

{Protocol}: Remote session {Config detail} was closed after {Time second} seconds of inactivity.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: Remote session OpenVPN was closed after 44 seconds of inactivity.
说明	一段时间无活动后，远程会话终止。
Severity	Info

Facility	local0
标准	IEC 62443-3-3 Reference: SR 2.6

通过不受信任的网络访问

{Protocol}: Remote access enabled via {Trigger condition}.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: Remote access enabled via E/A-Pin.
说明	允许远程访问。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 1.13

{Protocol}: Remote access disabled via {Trigger condition}.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: Remote access disabled via E/A-Pin.
说明	远程访问被拒绝。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 1.13

{Protocol}: User {User name} logged in from {IP address}.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin logged in from 192.168.1.105.
说明	用户已成功登录远程设备。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 1.13

{Protocol}: User {User name} failed to login from {IP address}.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin failed to login from 192.168.1.105.
说明	用户无法登录远程设备。
Severity	Warning

Facility	local0
标准	IEC 62443-3-3 参考：SR 1.13

{Protocol}: User {User name} has logged out.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin has logged out.
说明	用户已注销。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 1.13

{Protocol}: Connection from {IP address} established.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: Connection from 192.168.1.105 established.
说明	已建立 VPN 连接。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：n/a (NERC-CIP 005-R1)

{Protocol}: Connection from {IP address} closed.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: Connection from 192.168.1.105 closed.
说明	已关闭 VPN 连接。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：n/a (NERC-CIP 005-R1)

{Protocol}: Connection from {IP address} failed. Reason: {Reason}.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: Connection from 192.168.1.105 failed. Reason: unsuccessful authentication.
说明	由于验证无效，无法建立连接。
Severity	Warning

Facility	local0
标准	IEC 62443-3-3 参考：n/a (NERC-CIP 005-R3)

设备标识和验证

{Protocol}: Device {Src mac} access granted.

示例	WBM: Device 00:0C:29:2F:09:B3 access granted.
说明	由于端口验证成功，设备访问得到保证。 在本示例中，可保证通过源 MAC 地址“00:0C:29:2F:09:B3”访问设备。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 1.2

{Protocol}: {IP address} access granted.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: 192.168.1.105 access granted.
说明	满足防火墙规则或 ACL，授予访问权限。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 1.2

{Protocol}: {IP address} access granted.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: 192.168.1.105 access granted.
说明	保证通过云连接器进行访问。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 1.2

{Protocol}: Device {Src mac} access denied.

示例	WBM: Device 00:0C:29:2F:09:B3 access denied.
说明	由于端口验证失败，设备访问被拒绝。 在本示例中，通过源 MAC 地址“00:0C:29:2F:09:B3”访问设备被拒绝。
Severity	Warning

Facility	local0
标准	IEC 62443-3-3 参考：SR 1.2

{Protocol}: {IP address} access blocked.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: 192.168.1.105 access blocked.
说明	通过防火墙规则或访问控制列表拒绝访问。
Severity	Warning
Facility	local0
标准	IEC 62443-3-3 参考：SR 1.2

{Protocol}: {IP address} access blocked.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: 192.168.1.105 access blocked.
说明	禁止通过云连接器进行访问。
Severity	Warning
Facility	local0
标准	IEC 62443-3-3 参考：SR 1.2

{Protocol}: Connection from device {IP address} subject {Subject} successfully established.

示例	WBM: Connection from device 192.168.1.105 subject (Peter Maier) successfully established.
说明	设备验证成功。 在本示例中，IP 地址为"192.168.1.105"的设备与 SINEC OS 设备成功建立了连接。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 1.2

{Protocol}: Connection from device {IP address} subject {Subject} failed.

示例	WBM: Connection from device 192.168.1.105 subject (Peter Maier) failed.
说明	设备验证失败。

Severity	Warning
Facility	local0
标准	IEC 62443-3-3 参考：SR 1.2

限制并发会话的数量

{Protocol}: The maximum number of {Max sessions} concurrent login session exceeded.

示例	SSH: The maximum number of 8 concurrent login sessions exceeded.
说明	已经超出了并行会话的最大数目。 在示例中，超过了通过 SSH 进行的 8 个同时会话最大数。
Severity	Warning
Facility	local0
标准	IEC 62443-3-3 参考：SR 2.7

检查信息保护

{Protocol}: User {User name} has cleared the logging buffer.

示例	SSH: User admin has cleared the logging buffer.
说明	用户已删除本地日志。 在本示例中，用户“admin”已删除本地日志。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 3.9

不可否认性

{Protocol}: User {User name} has changed the configuration.

示例	SSH: User admin has changed the configuration.
说明	用户已更改组态。 在本示例中，用户“admin”已更改组态。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 2.12

{Protocol}: User {User name} has deactivated {Config detail} configuration.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User admin has deactivated OpenVPN configuration.
说明	用户已禁用特定组态数据。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 2.12

{Protocol}: User {User name} has initiated a reset to factory defaults.

示例	SSH: User admin has initiated a reset to factory defaults.
说明	用户已发起复位为默认设置的操作。 在本示例中，用户"admin"已发起复位为默认设置的操作。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 2.12

Device configuration changed.

示例	Device configuration changed.
说明	设备组态已永久性更改。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR2.12

通信完整性

{Protocol}: Integrity verification failed.

示例	Console: Integrity verification failed.
说明	检查消息的通信完整性时检测到完整性故障。只能进行基于证书的通信。
Severity	Warning
Facility	local0
标准	IEC 62443-3-3 参考：SR 3.1

软件和信息完整性

Firmware integrity verification failed. Backup firmware started.

示例	Firmware integrity verification failed. Backup firmware started.
说明	检查固件完整性时检测到完整性故障。加载了备份固件。
Severity	Warning
Facility	local0
标准	IEC 62443-3-3 参考：SR 3.4

{Protocol}: Software integrity verification failed.

示例	WBM: Software integrity verification failed.
说明	检查软件完整性时检测到完整性故障。
Severity	Warning
Facility	local0
标准	IEC 62443-3-3 参考：SR 3.4

Integrity violations in configuration data detected

示例	Integrity violations in configuration data detected
说明	检查组态完整性时检测到完整性故障。
Severity	Warning
Facility	local0
标准	IEC 62443-3-3 参考：SR 3.4

会话完整性

{Protocol}: Session ID verification failed.

示例	WBM: Session ID verification failed.
说明	会话 ID 无效。
Severity	Warning
Facility	local0
标准	IEC 62443-3-3 参考：SR 3.8

防御 DoS 攻击

{Protocol}: Dos attack detected.

示例	WBM: Dos attack detected.
说明	检测到拒绝访问攻击。
Severity	Warning
Facility	local0
标准	IEC 62443-3-3 参考：SR 3.8

在自动系统中备份数据

{Protocol}: User {User name} created backup file.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User maier created backup file.
说明	用户已创建备份文件。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 Reference: SR 7.3

{Protocol}: User {User name} failed to create backup file.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User <user name> failed to create backup file.
说明	用户创建备份文件失败。
Severity	Warning
Facility	local0
标准	IEC 62443-3-3 Reference: SR 7.3

自动化系统恢复

{Protocol}: User {User name} failed to apply backup file.

示例	WBM / UDP / TCP / Telnet / SSH / Console / PNIO / PB / OPC: User <user name> failed to apply backup file.
说明	用户使用备份文件失败。
Severity	Warning

Facility	local0
标准	IEC 62443-3-3 Reference: SR 7.4

{Protocol}: User {User name} loaded file type ConfigPack (restart required).

示例	WBM: User admin loaded file type ConfigPack (restart required).
说明	已应用组态。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR7.4

{Protocol}: Failed to load file type Firmware.

示例	WBM: Failed to load file type Firmware.
说明	固件上传失败。
Severity	Warning
Facility	local0
标准	IEC 62443-3-3 参考：SR7.4

{Protocol}: Loaded file type Firmware {Version} (restart required).

示例	TFTP: Loaded file type Firmware V02.00.00 (restart required).
说明	已成功加载固件。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR7.4

{Protocol}: User {User name} loaded file type Firmware {Version} (restart required).

示例	WBM: User admin loaded file type Firmware V02.00.00 (restart required).
说明	用户已成功加载固件。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR7.4

{Protocol}: Software {Version} was activated.

示例	WBM: Software V02.00.00 was activated.
说明	软件已成功激活。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 7.4

{Protocol}: User {User name} activated the Software {Version}.

示例	WBM: User <User name> activated the Software V02.00.00.
说明	用户已成功激活软件。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 7.4

{Protocol}: Software activation failed.

示例	WBM: Software activation failed.
说明	软件激活失败。
Severity	Warning
Facility	local0
标准	IEC 62443-3-3 参考：SR 7.4

{Protocol}: User {User name} failed to activate Software {Version}.

示例	WBM: User <User name> failed to activate Software V02.00.00.
说明	用户激活软件失败。
Severity	Warning
Facility	local0
标准	IEC 62443-3-3 参考：SR 7.4

附录 B“使用的加密方法”

B

B.1 使用的加密方法

下表列出了 SCALANCE X 设备使用的加密方法（密码）。

SSL

HTTPS WBM Server

类别	IANA 名称	十六进制值	默认启用
加密套件	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	c030	✓
加密套件	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	c02f	✓
加密套件	TLS_AES_256_GCM_SHA384	1302	✓
加密套件	TLS_CHACHA20_POLY1305_SHA256	1303	✓
加密套件	TLS_AES_128_GCM_SHA256	1301	✓
协议版本	TLSv1.2	-	✓
协议版本	TLSv1.3	-	✓

SMTP Client (secure)

类别	IANA 名称	十六进制值	默认启用
加密套件	TLS_AES_128_GCM_SHA256	1301	✓
加密套件	TLS_CHACHA20_POLY1305_SHA256	1303	✓
加密套件	TLS_AES_256_GCM_SHA384	1302	✓
加密套件	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	c02c	✓
加密套件	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	c02b	✓
加密套件	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	c02f	✓

类别	IANA 名称	十六进制值	默认启用
加密套件	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	c030	✓
协议版本	TLSv1.2	-	✓
协议版本	TLSv1.3	-	✓

Syslog (secure) Client

类别	IANA 名称	十六进制值	默认启用
加密套件	TLS_AES_128_GCM_SHA256	1301	✓
加密套件	TLS_CHACHA20_POLY1305_SHA256	1303	✓
加密套件	TLS_AES_256_GCM_SHA384	1302	✓
加密套件	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	c02c	✓
加密套件	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	c02b	✓
加密套件	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	c02f	✓
加密套件	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	c030	✓
协议版本	TLSv1.2	-	✓
协议版本	TLSv1.3	-	✓

SSH

SSH Server

类别	IANA 名称	十六进制值	默认启用
加密方法 (enc)	aes256-ctr	-	✓
主机密钥	ecdsa-sha2-nistp521	-	✓
密钥交换 (kex)	curve25519-sha256	-	✓
密钥交换 (kex)	curve25519-sha256@libssh.org	-	✓
密钥交换 (kex)	ecdh-sha2-nistp256	-	✓
密钥交换 (kex)	ecdh-sha2-nistp384	-	✓

类别	IANA 名称	十六进制值	默认启用
密钥交换 (kex)	ecdh-sha2-nistp521	-	✓
MAC	hmac-sha2-256	-	✓
协议版本	SSHv2.0	-	✓

SSH CLI Client

类别	IANA 名称	十六进制值	默认启用
加密方法 (enc)	aes256-ctr	-	✓
主机密钥	ecdsa-sha2-nistp521	-	✓
主机密钥	ecdsa-sha2-nistp256	-	✓
密钥交换 (kex)	curve25519-sha256	-	✓
密钥交换 (kex)	curve25519-sha256@libssh.org	-	✓
密钥交换 (kex)	ecdh-sha2-nistp256	-	✓
密钥交换 (kex)	ecdh-sha2-nistp384	-	✓
密钥交换 (kex)	ecdh-sha2-nistp521	-	✓
MAC	hmac-sha2-256	-	✓
协议版本	SSHv2.0	-	✓

SNMP

SNMP Server

类别	过程	十六进制值	默认启用
身份验证	HMAC-MD5-96	-	-
身份验证	HMAC-SHA-96	-	-
加密	des-cbc	-	-
加密	aes128-cbc	-	-

RADIUS

RADIUS Client

类别	过程	十六进制值	默认启用
完整性算法	MD5	-	-
完整性算法	HMAC-SHA1	--	-

索引