SIEMENS

SIMATIC NET

工业以太网交换机 SCALANCE XM-400/XR-500 Web Based Management

配置手册

03/2014
C79000-G8952-C248-06

法律资讯

警告提示系统

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

⚠ 危险
表示如果不采取相应的小心措施，**将会**导致死亡或者严重的人身伤害。

⚠ 警告
表示如果不采取相应的小心措施，**可能**导致死亡或者严重的人身伤害。

⚠ 小心
表示如果不采取相应的小心措施，可能导致轻微的人身伤害。

注意
表示如果不采取相应的小心措施，可能导致财产损失。

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

合格的专业人员

本文件所属的产品/系统只允许由符合各项工作要求的**合格人员**进行操作。其操作必须遵照各自附带的文件说明，特别是其中的安全及警告提示。 由于具备相关培训及经验，合格人员可以察觉本产品/系统的风险，并避免可能的危险。

按规定使用 Siemens 产品

请注意下列说明：

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

商标

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

责任免除

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

Siemens AG
Industry Sector
Postfach 48 48
90026 NÜRNBERG
德国

文件订购号: C79000-G8952-C248
℗ 03/2014 本公司保留更改的权利

目录

简介 1

1.1 有关组态手册的信息 (WBM)

组态手册的有效性

本组态手册涵盖了以下产品：

- SCALANCE XR-500
  - SCALANCE XR552-12M
  - SCALANCE XR528-6M

  上述设备提供有路由功能和无路由功能两种版本。 对于没有路由功能的设备，这些功能可由 KEY-PLUG 启用。
- SCALANCE XM-400
  - SCALANCE XM408-8C
  - SCALANCE XM416-4C

  上述设备提供有路由功能和无路由功能两种版本。对于没有路由功能的设备，这些功能可由 KEY-PLUG 启用。

本组态手册适用于以下软件版本：

- 自固件版本 V4.0 开始的 SCALANCE XR-500
- 自固件版本 V4.0 开始的 SCALANCE XM-400

本组态手册的用途

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

文档说明

除了您当前阅读的组态手册外，产品还包含下列文档：

- 组态手册
  - SCALANCE XM-400/XR-500 Command Line Interface
    本文档包含工业以太网交换机 SCALANCE XM-400 和 SCALANCE X-500 支持的 CLI 命令。
- 操作说明：
  - SCALANCE XR-500M
  - SCALANCE XR-500M 的 MM900 媒介模块
  - SCALANCE XR-500M 的风扇单元 FAN597-1
  - SCALANCE XR-500M 的电源 PS598-1
  - SCALANCE XM-400
  - SCALANCE XM-400 的扩展器
    这些文档包含有关产品安装、连接和认证方面的信息。

下列文档也可以从 SIMATIC NET 的工业以太网主题下获取：

- 《工业以太网/PROFINET》系统手册
- 《工业以太网/PROFINET - 无源网络组件》系统手册

所有这些文档在 SCALANCE X DVD 上都提供电子版本。

SIMATIC NET 词汇表

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

用户可在以下位置找到 SIMATIC NET 词汇表：

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

1.2 长版

西门子自动化和驱动产品具有某些工业安全功能，以支持工厂或设备安全操作。这些功能是整个工业安全机制的重要组成部分。基于此我们对产品进行持续开发。因此，建议您随时关注产品的更新信息并确保您仅使用最新版本。更多信息，请访问：http://support.automation.siemens.com.

此外，要确保工厂或设备的安全操作，还须采取适当的预防措施（例如：设备单元保护机制），并将自动化和驱动组件纳入整个工厂或设备先进且全面的工业安全保护机制中。可能使用的任何第三方产品须一并考虑。更多信息，请访问：http://www.siemens.com/industrialsecurity

说明 2

2.1 产品特征

工业以太网交换机的属性

- 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
  - 自动跨接
  - 自动极性变换
- 冗余协议：多重生成树协议 (Multiple Spanning Tree Protocol, MSTP)、快速生成树协议 (Rapid Spanning Tree Protocol, RSTP) 和生成树协议 (Spanning Tree Protocol, STP)。
  这就意味着，部分网络可以冗余连接到更高层的公司网络。 网络的重新组态时间为秒级，因此所花时间长于环网冗余方法。
- 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。 支持基于端口、协议和子网的 VLAN。
- 可限制使用组播协议时（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限制网络中的负载。 可以对组播和广播数据通信加以限制。
- 时钟同步
  诊断消息（日志表条目、电子邮件）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。
- 使用链路汇聚 (IEEE 802.1AX) 捆绑数据流
- 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）

第 3 层功能

下列功能仅在带有路由功能的设备上可用：

- 静态路由
- OSPF
- VRRP
- RIP

下列设备带有路由功能：

设备		订货号
SCALANCE XM-400	XM408-8C	6GK5 408-8GR00-2AM2
	XM416-4C	6GK5 416-4GR00-2AM2
SCALANCE XR-500	XR552-12M	6GK5 552-0AR00-2AR2
		6GK5 552-0AR00-2HR2
	XR528-6M	6GK5 528-0AR00-2AR2
		6GK5 528-0AR00-2HR2

在只支持第 2 层的设备上，路由功能可由 KEY-PLUG 启用。

2.2 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 Primary Setup Tool (PST) 的 PG/PC 来为工业以太网交换机首次分配 IP 地址。 对于其它组态设置，需要使用有 Telnet 或 Internet 浏览器的 PG/PC。

串口

工业以太网交换机有一个串行接口。 通过该串行接口，无需 IP 地址便可访问该设备。 另外，还随产品提供了串行电缆。

可为连接设置以下参数：

- 每秒位数： 115200
- 数据位： 8
- 奇偶校验： 无
- 停止位： 1
- 流控制： 无

2.3 C-PLUG/KEY-PLUG

C-PLUG/KEY-PLUG 中的组态信息

在更换设备时，可使用 C-PLUG/KEY-PLUG 将旧设备的组态传送到新设备中。

注意
操作期间请勿卸下或插入 C-PLUG/KEY-PLUG！ 只能在设备关闭后取出或插入 C-PLUG/KEY-PLUG。 设备定期检查是否存在 KEY-PLUG。 如果检测到 KEY-PLUG 被卸下，则会重启。如果在设备中插入了有效 KEY-PLUG，设备会在重启后切换到预定的错误状态。

使用该 C-PLUG/KEY-PLUG 启动新设备时，新设备会自动以与旧设备完全相同的组态继续运行。 如果通过 DHCP 设置 IP 组态，且没有重新对 DHCP 服务器进行相应的组态，则只有 IP 组态可能不同。

如果使用基于 MAC 地址的功能，则需要重新进行组态。

说明

就 C-PLUG/KEY-PLUG 而言，SCALANCE 设备可在两种模式下工作：

- **无 C-PLUG/KEY-PLUG**
  设备将组态存储在内部存储器中。 未插入 C-PLUG/KEY-PLUG 时会激活此模式。
- **有 C-PLUG/KEY-PLUG**
  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/KEY-PLUG 和内部存储器中。 只要插入 C-PLUG/KEY-PLUG，就会激活此模式。 使用插入的 C-PLUG/KEY-PLUG 启动设备时，设备会以 C-PLUG/KEY-PLUG 上的组态数据启动。

说明

先前版本与插入的 C-PLUG/KEY-PLUG 的不兼容性

在安装先前版本固件的过程中，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。 在这种情况下，如果在设备中插入 C-PLUG/KEY-PLUG，则重启后，由于 C-PLUG/KEY-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 C-PLUG/KEY-PLUG 上的原始组态，则可手动删除或重写 C-PLUG/KEY-PLUG。

KEY-PLUG 中的许可证信息

除组态外，KEY-PLUG 还包含允许使用第 3 层功能的许可证。

2.4 以太网供电 (PoE)

常规

“以太网供电”(Power over Ethernet, PoE) 是一种符合 IEEE 802.3af 或 IEEE 802.3at 标准的网络组件供电技术。 通过将各种网络组件连接在一起的以太网电缆进行供电。 如此就无需额外的电源线。 PoE 可用于所有与 PoE 兼容且所需最大功率为 25.50 W 的网络组件。

用于供电的电缆

- **型号 1（冗余电线）**
  在快速以太网中，电线对 1、2 和 3、6 用于传输数据。 电线对 4、5 和 7、8 用于供电。 如果仅有四根线可用，则会将电压调制到电线 1、2 和 3、6 上（参见型号 2）。 这种选择适合数据传输率为 10/100 Mbps 的情况。 这种供电类型不适合数据传输率为 1 Gbps 的情况，这是因为在千兆位中，全部的八根电线都用于数据传输。
- **型号 2（幻象电源）**
  应用幻象电源时，会通过用于数据传输的电线对来供电，即全部的八根 (1 Gbps) 或四根 (10/100 Mbps) 电线既用于数据传输，又用于供电。

PoE 兼容终端设备必须支持基于冗余电线的型号 1 和型号 2。
带有 PoE 功能的交换机可以通过以下方式为终端设备供电

- 型号 1 或
- 型号 2 或
- 型号 1 和型号 2。

端跨

采用端跨供电时，通过可经由以太网电缆访问设备的交换机进行供电。 该交换机必须具有 PoE 功能，如 SCALANCE X108PoE、SCALANCE X308-2M PoE、所有带 PE408PoE 的 SCALANCE XM-400 交换机、SCALANCE XR552-12M。

中跨

交换机不是 PoE 兼容设备时，使用中跨供电。 此时，通过交换机和终端设备之间的附加设备来供电。 在这种情况下，由于通过冗余电线供电，因此仅能实现 10/100 Mbps 的数据传输率。

也可将 Siemens 电源插头用作电源输入的接口。 由于电源插头支持 24 VDC 的电源，因此不符合 802.3af 或 IEEE 802.3at。 请注意以下有关电源插头的使用限制：

⚠ 警告

仅当符合以下条件时使用电源插头：

- 采用超低电压 SELV，即符合 IEC 60364-4-41 的 PELV
- 在美国/加拿大，采用符合 NEC 的 2 类电源
- 在美国/加拿大，布线必须符合 NEC/CEC 的要求
- 电流负载最大 0.5 A

电缆长度

表格 2-1　允许的电缆长度（铜质电缆 - 快速以太网）

电缆类型	附件（插头、插座和 TP 线）	允许的电缆长度
IE TP 抗扭电缆	带有 IE FC 插座 RJ-45 + 10 m TP 线	0 到 45 m + 10 m TP 线
	带有 IE FC RJ-45 插头 180	0 到 55 m
IE FC TP 船用电缆 IE FC TP 拖拽电缆 IE FC TP 软电缆	带有 IE FC 插座 RJ-45 + 10 m TP 线	0 到 75 m + 10 m TP 线
	带有 IE FC RJ-45 插头 180	0 到 85 m
IE FC TP 标准电缆	带有 IE FC 插座 RJ-45 + 10 m TP 线	0 到 90 m + 10 m TP 线
	带有 IE FC RJ-45 插头 180	0 到 100 m

表格 2-2　允许的电缆长度（铜质电缆 - 千兆位以太网）

电缆类型	附件（插头、插座和 TP 线）	允许的电缆长度
IE FC 标准电缆，4×2，24 AWG IE FC 软电缆，4×2，24 AWG	带有 IE FC RJ-45 插头 180，4x2	0 到 90 m
IE FC 标准电缆，4x2，22 AWG	带有 IE FC 插座 RJ-45 + 10 m TP 线	0 到 60 m + 10 m TP 线
IE FC 软电缆，4x2，22 AWG	带有 IE FC 插座 RJ-45 + 10 m TP 线	0 到 90 m + 10 m TP 线

表格 2-3　安装接头

引脚	IE FC 插座 RJ-45	IE FC RJ-45 模块化插座	应用	
			1000BaseT	10BaseT、100BaseTX
1	黄色	绿色/白色	D1+	TX+
2	橙色	绿色	D1-	RX+
3	白色	橙色/白色	D2+	Tx-
6	蓝色	橙色	D2-	Rx-
4	-	蓝色	D3-	-
5	-	蓝色/白色	D3+	-
7	-	棕色/白色	D4-	-
8	-	棕色	D4+	-

IP 地址分配

3

3.1 IP 地址的结构

地址类别

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

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

XXX.XXX.XXX.XXX

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

子网掩码

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

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

B 类网络示例：

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

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

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

说明

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

3.2 IP 地址的初始分配

组态选项

不能使用基于 Web 的管理 (Web Based Management, WBM) 为工业以太网交换机分配初始 IP 地址，因为这个组态工具只能在事先已经具有 IP 地址的情况下使用。

可通过以下方法将 IP 地址分配给未组态的设备：

- **DHCP**（默认）
- **Primary Setup Tool** (PST)
  - 要使用 PST 将 IP 地址分配给工业以太网交换机，必须能通过以太网访问工业以太网交换机。
  - 可在 Internet 上 Siemens 工业自动化与驱动产品部门的服务与支持中心的条目 ID 19440762 (http://support.automation.siemens.com/WW/view/zh/19440762) 下找到 PST。
  - 有关使用 PST 分配 IP 地址的详细信息，请参见文档“Primary Setup Tool (PST)”。
- **STEP 7 Classic**
  - 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。
  - 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 V12 SP1 及更高版本**
  有关使用 STEP 7（V12 SP1 及更高版本）分配 IP 地址的详细信息，请参见在线帮助“信息系统”的“寻址 PROFINET 设备”部分。
- 使用 **CLI** 通过串行接口分配
  有关使用 CLI 分配 IP 地址的详细信息，请参见“SCALANCE XM-400/XR-500 命令行接口”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

交付产品时以及执行“Restore Factory Defaults and Restart”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。

3.3 用 DHCP 进行地址分配

DHCP 属性

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

- 启动设备时和设备运行期间均可使用 DHCP。
- 分配的 IP 地址仅在有限时间（称为租用时间）内有效。 超过该时间后，客户端必须请求新 IP 地址，或延长现有 IP 地址的租用时间。
- 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 客户端上设置。 可以通过 MAC 地址、DHCP 客户端 ID 或系统名称分配地址。 在“System > DHCP Client”中组态参数。
- 支持 DHCP 选项 66、67
  - 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

说明

DHCP 采用的机制是 IP 地址仅分配一小段时间（租用时间）。 如果设备在租用时间到期之前没有将新请求发送到 DHCP 服务器，则继续使用已分配的 IP 地址、子网掩码和网关。

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

技术基础 4

4.1 组态限制

设备的组态限制

下表列出了设备基于 Web 的管理和命令行解释程序的组态限制。

各种功能是否可用取决于所用的设备类型以及是否插入了 KEY-PLUG。

	可组态的功能	最大数量
系统	Syslog 服务器	3
	电子邮件服务器	3
	SNMPv1 陷阱接收方	10
第 2 层	虚拟 LAN（基于端口；包括 VLAN 1）	257
	每个端口基于协议的 VLAN 组	12
	基于 IPv4 子网的 VLAN	150
	多重生成树实例	16
	链路汇聚或以太信道（每个汇聚最多 8 个端口）	8
	一个链路汇聚中的端口数	8
	转发数据库 (FDB) 中的静态 MAC 地址	256
	无活动 GMRP 的组播地址	512
	有活动 GMRP 的组播地址	50
	数据通信可镜像到监视端口的 VLAN	255
安全性	RADIUS 服务器的 IP 地址	3
	管理 ACL（管理性访问规则）	10
	端口 ACL MAC 的规则	128
	端口 ACL MAC 的入站和出站规则	256
	端口 ACL IP 的规则	128
	端口 ACL IP 的入站和出站规则	256
第 3 层	第 3 层接口	127
	硬件路由表中的条目	4096

	可组态的功能	最大数量
	静态路由	100
	去往同一目的地的可能路由	8
	DHCP 中继代理接口	127
	DHCP 中继代理服务器	4
	VRRP 路由器接口（仅 VLAN 接口）	52
	每个设备的 OSPF 区域	5
	每个 OSPF 区域的 OSPF 区域范围条目（区域内汇总）	3
	OSPF 接口	40
	每个 OSPF 区域的 OSPF 接口	40
	OSPF 虚拟链路（自治系统内）	8
	OSPF 接口验证密钥	200 （40 个接口，每个接口 5 个密钥）
	OSPF 虚拟链路验证密钥	40 （8 个虚拟链路，每个链路 5 个密钥）

4.2 VLAN

与节点的空间位置无关的网络定义

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

VLAN 的独特优势是可减少其它 VLAN 的节点和网段的网络负载。

要确定数据包属于哪个 VLAN，需要将帧扩展 4 个字节（VLAN 标记 (页 28)）。 这种扩展不仅包括 VLAN ID，还包括优先级信息。

VLAN 分配选项

对 VLAN 分配有多种选项。

- 基于端口的 VLAN
  为设备的每个端口分配一个 VLAN ID。可在“第 2 层 > VLAN > 基于端口的 VLAN” (Layer 2 > VLAN > Port-based VLAN) (页 186) 中组态基于端口的 VLAN。
- 基于协议的 VLAN
  为设备的每个端口分配一个协议组。 可在“第 2 层 > VLAN > 基于协议的 VLAN 端口” (Layer 2 > VLAN > Protocol Based VLAN Port) (页 189) 中组态基于协议的 VLAN。
- 基于子网的 VLAN
  为设备的 IP 地址分配 VLAN ID。可在“第 2 层 > VLAN > 基于 IPv4 子网的 VLAN” (Layer 2 > VLAN > Ipv4 Subnet Based VLAN) (页 191) 中组态基于子网的 VLAN。

处理 VLAN 分配

如果在设备上创建多个 VLAN 分配，则按以下顺序处理这些分配：

1. 基于子网的 VLAN
2. 基于协议的 VLAN
3. 基于端口的 VLAN

首先检查帧的 IP 地址。 如果采用“基于 IPv4 子网的 VLAN”(Ipv4 Subnet Based VLAN) 选项卡上的规则，则将帧发送给相应的 VLAN。 如果不采用任何规则，则检查帧的协议类型。 如果采用“基于协议的 VLAN 端口”(Protocol Based VLAN Port) 选项卡上的规则，则将帧发送给相应的 VLAN。 如果不采用任何规则，则通过基于端口的 VLAN 发送帧。 基于端口的 VLAN 的规则在“基于端口的 VLAN”(Port Based VLAN) 选项卡上指定。

4.3 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 802.1 Q 标准规定可通过添加 VLAN 标记来扩展以太网帧。

说明

VLAN 标记使允许的帧总长度从 1518 字节增加到 1522 字节。 对于工业以太网交换机，标准 MTU 大小为 1536 字节。 该 MTU 大小可更改为 64 到 9216 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：

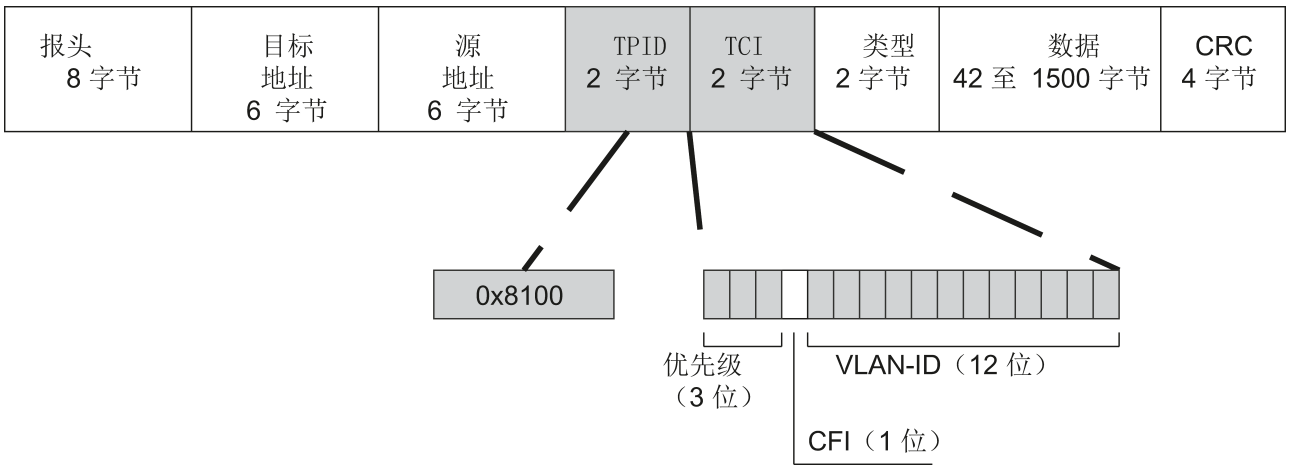


图 4-1 扩展的以太网帧结构

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：

CoS 优先级

标记帧有 3 个位用于优先级，又称为服务类别 (Class of Service, CoS)。 根据 IEEE 802.1p，优先级如下：

CoS 位	数据类型
000	非时间关键数据通信（少于尽力服务 [基本设置]）
001	正常数据通信（尽力服务 [背景]）
010	预留（标准）
011	预留（优秀服务）
100	最大延迟为 100 ms 的数据传输
101	有保证的服务，交互式多媒体
110	有保证的服务，交互式语音传输
111	预留

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。

设备具有八个并行队列，可在其中处理各种优先级的帧。 首先会处理具有最高优先级（“严格优先级”方法）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

4.4 SNMP

简介

借助简单网络管理协议 (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
  向代理请求数据记录
- GETNEXT
  调用下一条数据记录。
- GETBULK （SNMPv2 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
  代理返回管理器请求的数据。
- TRAP
  如果发生特定事件，SNMP 代理将发送陷阱。

SNMPv1、SNMPv2 和 SNMPv3 使用 UDP（用户数据报协议）。 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 SNMPv2 比较， SNMPv3 引入了可扩展安全概念。

SNMPv3 支持：

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

4.5 路由功能

简介

术语“路由”描述不同网络之间通信的路径规范，也就是说，数据包如何从子网 A 传送到子网 B。

SCALANCE X 支持以下路由功能：

- 静态路由
  对于静态路由，需在路由表中手动输入路径。
- 路由器冗余
  通过标准化 VRRP（Virtual Router Redundancy Protocol，虚拟路由器冗余协议），可使用冗余路由器来提高重要网关的可用性。
- 动态路由
  路由表中的条目会动态变化并持续进行更新。 使用以下动态路由协议之一创建条目：
  - OSPFv2
  - RIPv2

静态路由

在路由表中手动输入路径。 有关在路由表中输入路径的信息，请参见“第 3 层 > 路由 (页 257)”页面。

参见

VRRP (页 269)

4.5.1 VRRP

使用 VRRP 的路由器冗余

通过虚拟路由器冗余协议 (Virtual Router Redundancy Protocol, VRRP)，可以排除网络中的路由器故障。

VRRP 仅可用于虚拟 IP 接口（VLAN 接口），不可用于路由器端口。

网段中的多个 VRRP 路由器以逻辑组的形式组合在一起，成为一个虚拟路由器 (Virtual Router, VR)。该组使用虚拟 ID (VRID) 进行定义。组中的 VRID 必须相同。该 VRID 不能再用于其它组。

为虚拟路由器分配一个虚拟 IP 地址和一个虚拟 MAC 地址。将组中的其中一个 VRRP 路由器指定为主路由器。主路由器的优先级为 255。其它 VRRP 路由器为备用路由器。主路由器将虚拟 IP 地址和虚拟 MAC 地址分配给其网络接口。主路由器以指定的时间间隔将 VRRP 数据包（广播）发送给备用路由器。 主路由器通过 VRRP 数据包指示自己仍处于运行状态。主路由器还会对 ARP 查询做出响应。

如果虚拟主路由器出现故障，则由一个备用路由器承担主路由器的角色。优先级最高的备用路由器将变为主路由器。如果备用路由器的优先级相同，则采用 MAC 地址较高的备用路由器。该备用路由器将变为新的虚拟主路由器。

新的虚拟主路由器采用虚拟 MAC 地址和 IP 地址。这表示，不需要更新任何路由表或 ARP 表。因此，将设备故障的影响减至最低。

在“第 3 层 > VRRP”(Layer 3 > VRRP) 中组态 VRRP。

4.5.2 OSPFv2

使用 OSPFv2 的动态路由

OSPF（Open Shortest Path First，开放式最短路径优先）是基于开销的路由协议。 使用 Dijkstra 提出的“短路径优先”算法计算最经济高效且最短的路径。 OSPF 由 IETF（Internet Engineering Task Force，Internet 工程任务组）开发。
可在“Layer 3 > OSPFv2 (页 275)”中组态 OSPFv2。

OSPFv2 将自治系统 (Autonomous System, AS) 分成不同的区域。

OSPF 中的区域

存在以下区域：

- Backbone
  骨干区域是指区域 0.0.0.0。 所有其它区域都与此区域相连。 骨干区域可以直接与其它区域连接，也可以通过虚拟连接与其它区域相连。
  骨干区域提供所有路由信息。 因此，骨干区域负责在不同区域之间转发信息。
- Stub Area
  此区域包含自治系统中该区域内的路径，以及自治系统外的标准路径。 此自治系统外的目标会被分配给标准路径。

- Totally Stubby Area
  此区域仅识别该区域内的路径，以及该区域外的标准路径。
- Not So Stubby Area (NSSA)
  此区域可以将来自其它自治系统中的数据包转发（重新分发）到自身自治系统的区域中。这些数据包将由 NSSA 路由器进一步分发。

OSPF 的路由器

OSPF 区分以下路由器类型：

- 内部路由器 (IR)
  将路由器的所有 OSPF 接口分配给同一区域。
- 区域边界路由器 (ABR)
  将路由器的 OSPF 接口分配给不同区域。 将一个 OSPF 接口分配给骨干区域。 如有可能，将路径组合在一起。
- 骨干路由器 (BR)
  将至少一个 OSPF 接口分配给骨干区域。
- 自治系统区域边界路由器 (ASBR)
  将路由器的一个接口连接到另一个 AS，例如，使用路由协议 RIP 的 AS。

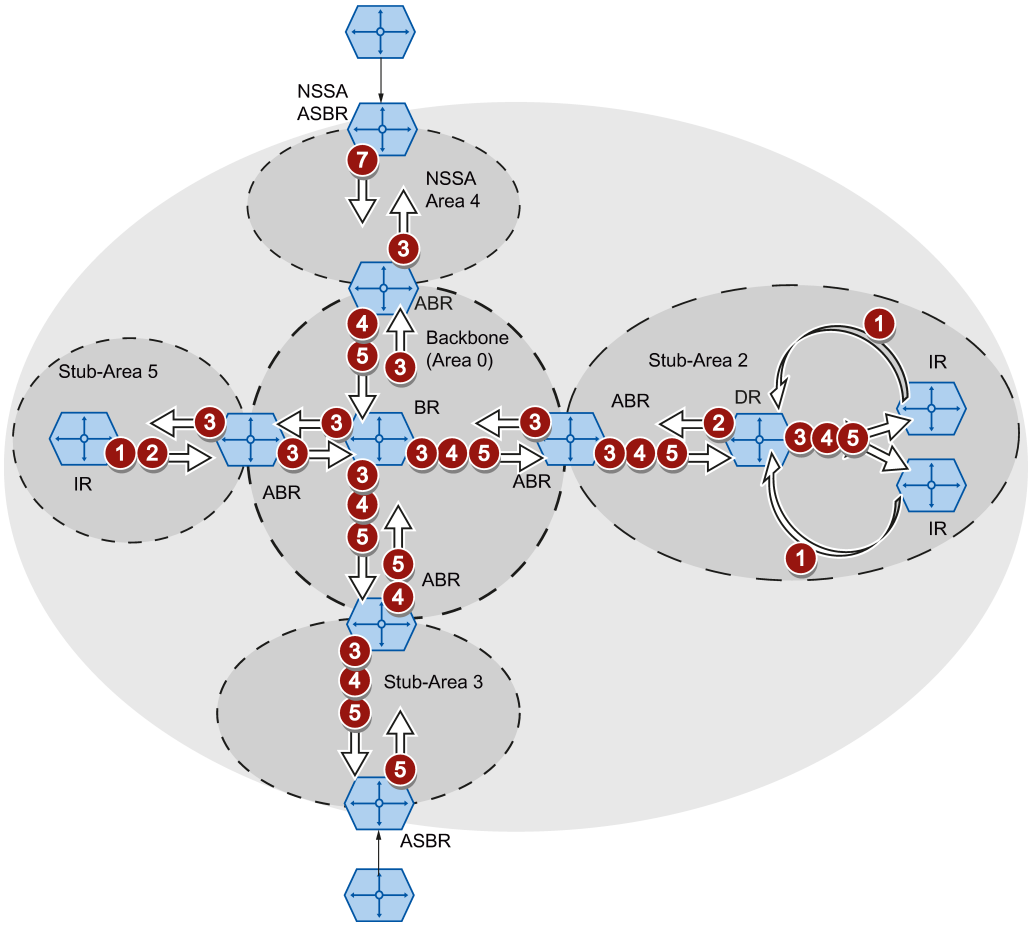
虚拟连接

每个区域都必须连接到骨干区域。 在某些情况下，可能无法实现直接物理连接。 在这种情况下，相关区域的路由器必须通过虚拟连接与骨干路由器相连。

LSA 类型

在自治系统中，交换的数据包中包含有关路由器连接和连接状态消息的信息。 此类数据包也称为 LSA（Link State Advertisements，链路状态广播）。 LSA 始终在两个相邻的路由器之间传递。

如果网络有变化，则会将 LSA 发送到网络中的所有路由器。 具体信息取决于 LSA 类型。



1 **路由器 LSA（LSA 类型 1）**

LSA 类型 1 标识仅在某个区域内发送。 如果路由器属于相关区域，则对于该路由器的每个活动连接，都会生成一个 LSA 类型 1 标识。 LSA 类型 1 标识包含有关连接状态和开销的信息，例如，IP 地址、网络掩码和网络类型。

2 **网络 LSA（LSA 类型 2)**

LSA 类型 2 标识仅在某个区域内发送。 路由器为属于相关区域的每个网络生成一个 LSA 类型 2 标识。如果网络中有多个互连的路由器，则由指定路由器 (Designated Router, DR) 负责发送 LSA 类型 2 标识。 LSA 类型 2 标识包含网络地址、网络掩码以及连接到网络的路由器的列表。

3 **汇总 LSA（LSA 类型 3/LSA 类型 4）**

4 Summary LSA 由区域边界路由器生成并发送到区域中。“汇总 LSA”包含有关 AS 中不属于某个区域的路由器的信息。 并且，在可能的情况下将路径组合在一起。

- 汇总 LSA（LSA 类型 3）
  LSA 类型 3 标识用于描述访问网络的路径以及将标准路径通知给区域。
- AS 汇总 LSA（LSA 类型 4)
  LSA 类型 4 标识用于描述到 ASBR 的路径。

5 **外部 LSA（LSA 类型 5/LSA 类型 7)**

7 外部 LSA 由 ASBR 生成。 LSA 类型取决于区域。

- AS 外部 LSA（LSA 类型 5）
  LSA 类型 5 标识由 AS 边界路由器发送到自治系统的区域中，但存根区域和 NSSA 区域除外。 LSA 包含有关到另一个 AS 中的某个网络的路径信息。 路径可手动创建，也可从外部学习得到。 ASBR 使用 LSA 类型 5 将标准路径分配给骨干区域。
- NSSA 外部 LSA（LSA 类型 7）
  LSA 类型 7 标识由 NSSA 的 AS 边界路由器生成。 该路由器也称为 NSSA ASBR。 LSA 类型 7 标识仅在 NSSA 内发送。 如果 LSA 类型 7 标识的 P 位为 1，则这些 LSA 将由 ABR 转换为 LSA 类型 5 标识并发送到骨干区域。

建立近邻关系

路由器遍历以下状态来与相邻路由器建立连接。

1. 尝试状态/初始化状态
   路由器激活 OSPF，并开始发送和接收呼叫数据包。 路由器根据收到的呼叫数据包了解附近有哪些 OSPF 路由器。 路由器会检查呼叫数据包的内容。 呼叫数据包还包含“发送方”的邻居路由器的列表（邻居表）。
2. 双向状态
   例如，如果区域 ID、区域类型以及时间设置相符，则可与邻居建立连接（邻接）。 在点对点网络中，可直接建立连接。 如果可以访问网络中的多个邻居路由器，则根据呼叫数据包识别指定路由器 (Designated Router, DR) 和备用指定路由器 (Designated Backup Router, DBR)。 优先级最高的路由器将变为指定路由器。 如果两个路由器的优先级相同，则 ID 较小的路由器将变为指定的路由器。 路由器与指定路由器建立连接。
3. 开始交换状态
   邻居路由器决定由哪个路由器启动通信。 ID 较大的路由器将成为主路由器。
4. 交换状态
   邻居路由器发送用来描述其近邻数据库内容的数据包。 近邻数据库（链路状态数据库 - LSDB）包含有关网络拓扑的信息。
5. 加载状态
   路由器完成接收的信息。 如果路由器对具体连接的状态仍有疑问，它将发送链路状态请求。 邻居路由器发出响应（链路状态更新）。 该响应包含适当的 LSA。 路由器确认已收到响应（链路状态确认）。
6. 完美状态
   完成与邻居路由器交换信息。 邻居路由器的近邻数据库完全相同。 路由器根据“短路径优先”算法计算到各个目标的路径。 路径被输入到路由表中。

检查近邻关系

呼叫数据包仅用于建立邻近关系。 通过周期性发送呼叫数据包来检查与邻居路由器的连接。 如果在特定间隔（停顿间隔）内未收到呼叫数据包，则与邻居的连接将标识为“断开”。 相关条目将被删除。

更新近邻数据库

建立近邻数据库后，如果拓扑有变化，则会将 LSA 发送给网络中的所有路由器。

4.5.3 RIPv2

使用 RIPv2 的动态路由

路由信息协议 (RIPv2) 用于自动创建路由表。 RIPv2 在自治系统 (AS) 中使用，最多支持 15 个路由器。 它基于距离向量算法。

RIPv2 由 IETF（Internet Engineering Task Force，Internet 工程任务组）开发，在 RFC 2453 中有相关说明。
可在“第 3 层 > RIPv2”(Layer 3 > RIPv2) 中组态 RIPv2。

设置路由表

由于路由器最初只识别其直接连接的网络，因此它会向直接邻居路由器发送请求。 之后，它会收到邻居路由器的路由表作为回复。 该路由器将根据收到的信息设置自己的路由表。

路由表包含所有可能目标的条目。 每个条目都包含到目标的距离和路径上的第一个路由器。

该距离也称为度量。 它表示要在指向目标的路径上通过的路由器数量（跳跃计数）。 最大距离为 15 个路由器（跳跃数）。

更新路由表

建立路由表后，路由器每隔 30 秒便会将其路由表发送给每个直接邻居路由器。

路由器会将新路由信息与现有路由表进行比较。 如果新信息中包含更短的路径，则会覆盖现有路径。 路由器只保留通向目标的最短路径。

检查邻居路由器

如果某个路由器超过 180 秒未从某邻居路由器收到消息，那么它会将该路由器标记为无效。路由器会将该邻居路由器分配大小为 16 的度量。

4.6 冗余机制

4.6.1 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站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

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

根网桥是控制所有相关组件的生成树算法的网桥。

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

对网络拓扑变化的响应

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

使组态信息保持最新

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

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

4.6.1.1 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。

说明

默认设置

已在设备上默认启用 HTTP。

公共内部生成树 (CIST)

CIST 可识别交换机使用的在原理上与 RSTP 内部实例类似的内部实例。

4.6.2 HRP

HRP - 高速冗余协议

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

如果由于网络中断导致 RM 发送的测试帧无法到达其它环网端口，则 RM 将在自身的两个环网端口之间切换并立即将切换情况通知给冗余客户端。 环中断后的重新组态时间最长为 0.3 秒。

备用冗余

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

要求

- 在具有最多 50 个设备的环型拓扑中支持 HRP。 超过此设备数可能导致通信数据丢失。
- 只有支持 HRP 功能的设备才能在环网中使用。

- 所有设备必须通过其环网端口互连。
- 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。

4.6.3 MRP

4.6.3.1 MRP - 介质冗余协议

“MRP”方法符合以下标准中规定的“介质冗余协议”(MRP, Media Redundancy Protocol)：

IEC 62439-2 版本 1.0 (2010-02) Industrial communication networks - High availability automation networks Part 2: Media Redundancy Protocol (MRP)

环中断后的重新组态时间最长为 0.2 秒。

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。
  除了 PROFINET IO 系统，含有最多 100 台 SCALANCE X-200 和 SCALANCE X-300 工业以太网交换机的拓扑也已成功通过测试。
  超过此设备数可能导致通信数据丢失。
- 要在其中使用 MRP 的环只能包括支持此功能的设备。
  这些设备包括某些工业以太网 SCALANCE X 交换机、某些适用于 SIMATIC S7 和 PG/PC 的通信处理器 (CP) 或支持此功能的非 Siemens 设备等。
- 所有设备必须通过其环网端口互连。
  在两台 SCALANCE X 工业以太网交换机之间可实现最长 3 km 的多模连接和最长 26 km 的单模连接。 在更远的距离，指定的重新组态时间可能更长。
- 必须在环中的所有设备上激活“MRP”（请参见“在 STEP 7 中组态 (页 44)”部分）。
- 所有环网端口的连接设置（传送介质/双工）必须设置为全双工和至少 100 Mbps。 否则，可能丢失通信数据。
  - STEP 7： 在属性对话框的“选项”(Options) 选项卡中将环中涉及的所有端口设置为“自动设置”(Automatic settings)。
  - WBM： 如果通过基于 Web 的管理进行组态，环网端口会自动设置为自动协商。

拓扑

以下示意图显示了使用 MRP 的环中设备的可能拓扑。

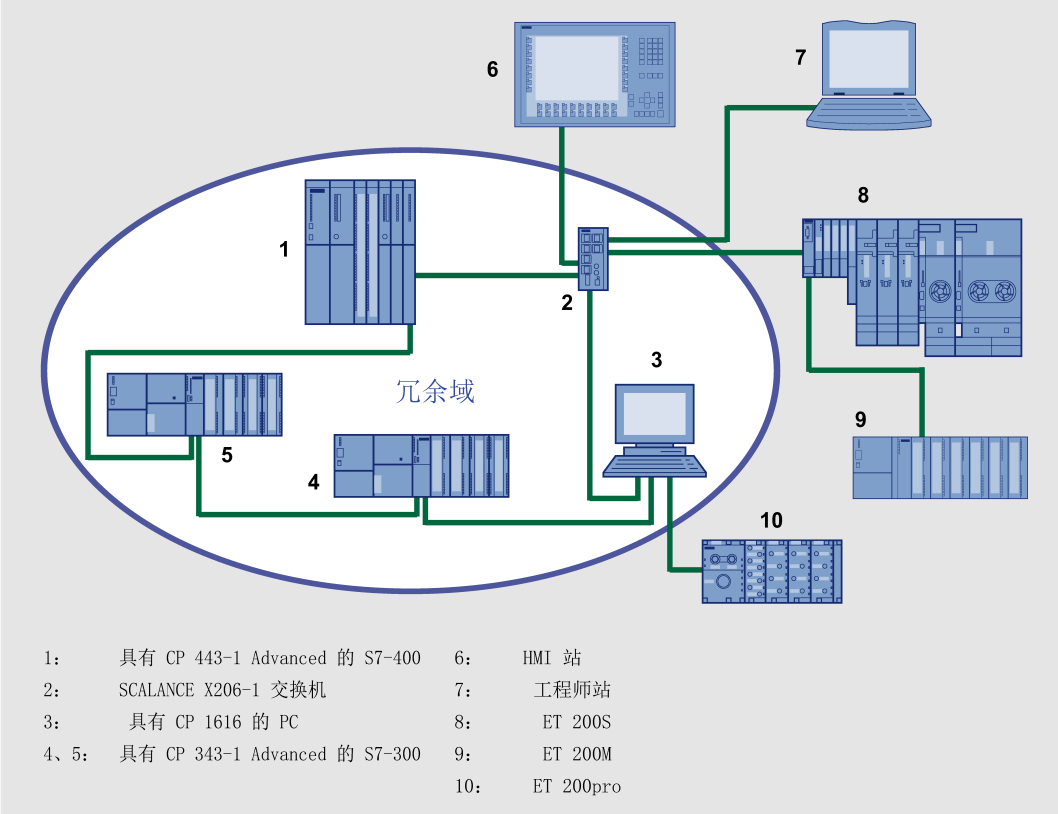


图 4-2 支持 MRP 介质冗余协议的环型拓扑示例

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 交换机或具有 CP 1616 的 PC 连接到环中。

4.6.3.2 在 WBM 中组态

角色

请根据以下使用案例来选择角色：

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

说明

使用非西门子设备时，无法使用“自动冗余检测”。

组态

在 WBM 中，您可以按照以下页面组态 MRP：

- 组态 (页 172)
- 环网冗余 (页 201)

4.6.3.3 在 STEP 7 中组态

STEP 7 中的组态

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

为设备的 MRP 组态设置以下参数：

- 域
- 角色
- 环网端口 (Ring port)
- 诊断中断

下文介绍了这些设置。

说明

优先级启动

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

如果想要使用“优先级启动”功能，则在组态中禁用 MRP。

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

域

在“域”(Domain) 下拉列表中，保留出厂设置中的默认条目“mrpdomain 1”。

环网中组态有 MRP 的所有设备都必须属于同一个冗余域。 一台设备不能属于一个以上的冗余域。

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

设备重启或关闭电源和热启动之后，MRP 设置仍然有效。

角色

请根据以下使用案例来选择角色。

- 希望在仅包含 Siemens 设备的环型拓扑使用 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”）：
  - 只为环中一台设备分配“冗余管理器”角色。
  - 对于环型拓扑中的其它设备，选择“客户机”(Client) 角色。

  说明

  为确保在环网中采用非 Siemens 设备作为冗余管理器运行时不出现问题，请确保在闭合环网之前将固定角色“客户端”(Client) 分配给环网中的其它设备。 否则，可能出现导致网络故障的循环数据帧。

- 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

  全新的 Siemens 设备以及复位为出厂设置的设备具有 MRP 角色“管理器（自动）”(CP) 或“自动冗余检测”(SCALANCE X)。 如果在环网中将非 Siemens 设备用作冗余管理器运行，可能导致通信数据丢失。

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。 ● CP 获得“管理器（自动）”MRP 角色。 ● 对于交换机，激活冗余方法“自动冗余检测”(ARD)。 如果复位前已将其它端口用作环网端口，则在特定的连接情况下，之前已正确组态的设备可能会引起数据帧循环传送，从而导致数据通信故障。

诊断中断

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

可能生成以下诊断中断：

- 接线或端口错误
  如果环网端口出现以下错误，就会生成诊断中断：
  - 环网端口上的连接中止
  - 环网端口的邻居不支持 MRP。
  - 环网端口连接到非环网端口。
  - 环网端口连接到其它 MRP 域的环网端口。
- 中断/恢复（仅限冗余管理器）
  如果环中断或者是恢复了原始组态时，将生成诊断中断。
  若是在 0.2 秒内生成了这两个中断，说明环网出现中断。

不通过 STEP 7 设置冗余参数分配（冗余替代）

该选项仅会影响交换机。 如果想要使用其它方式或工具（例如，基于 Web 的管理 (WBM)、CLI 或 SNMP）设置冗余介质的属性，则选择该选项。

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

4.6.4 备用

常规

SCALANCE X 交换机不但支持环网内的环冗余，还支持在环网之间或开放网段（线性总线）之间采用冗余连接。 在冗余链路中，环网通过以太网连接相连在一起。 实现的方法是在一个环网中组态一个主/从设备对，使设备对的设备能彼此监视对方，并且能在发生故障时将数据通信从常用的主以太网连接重定向到替代（从）以太网连接。

备用冗余

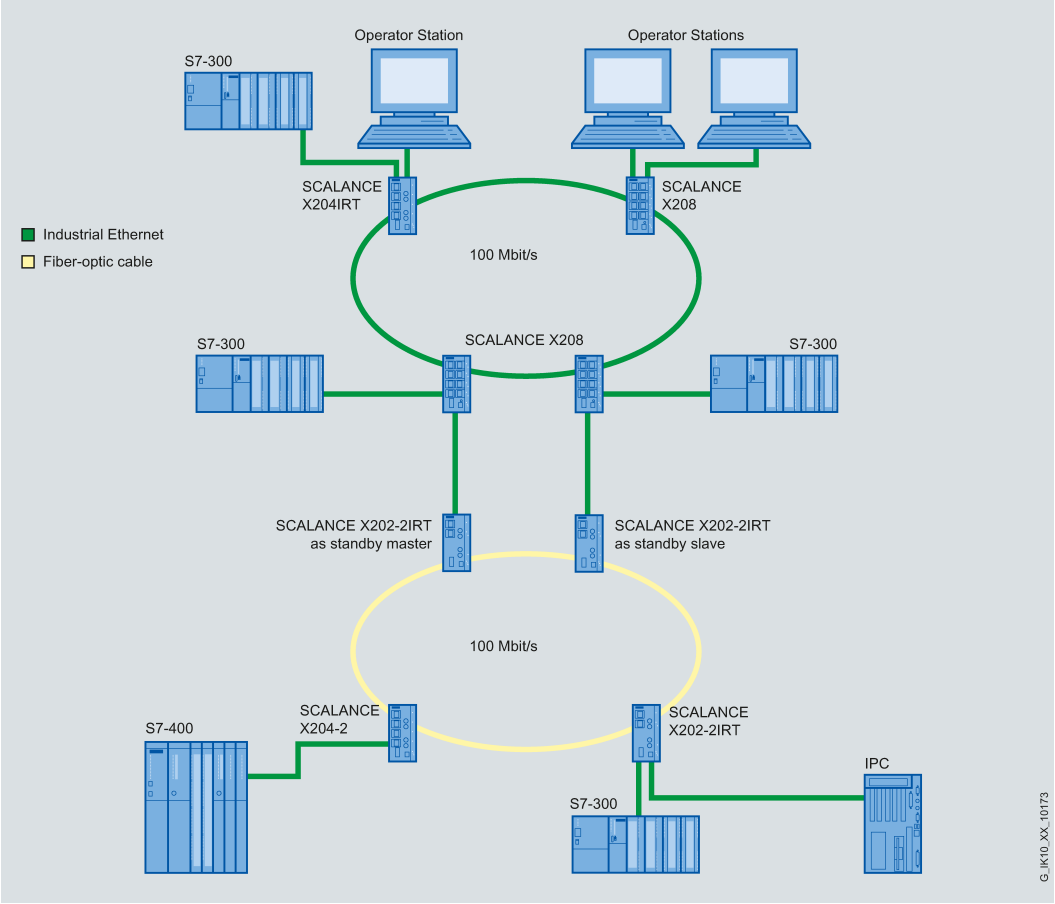


图 4-3 两个 SCALANCE X-200 IRT 环网的冗余连接示例

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。 图中的网段是包含冗余管理器（RM，本例中为 SCALANCE X202-2IRT 交换机）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 X202 设备彼此交换数据帧，以同步工作状态（一个为主设备，另一个为从设备）。 如果没发生问题，仅激活从主设备到另一网段的连接。 如果此连接失败（例如，由于连接断开或设备故障），只要问题仍然存在，从设备就会激活其连接。

4.7 链路汇聚

链路汇聚

通过链路汇聚，能够将传输速率相同的多个并行物理连接分组到一起，构成传输速率更高的逻辑连接。 这种基于 IEEE 802.3ad 的方法又称为端口聚合或信道捆绑。

链路汇聚仅适用于点对点模式下传输速率相同的全双工连接。 该技术可加倍提升带宽或传输速率。 如果其中部分连接失败，将通过剩余的连接进行数据通信。

可使用 Link Aggregation Control Layer (LACL) 和 Link Aggregation Control Protocol (LACP) 进行监控。

使用“基于 Web 的管理”进行组态 5

5.1 基于 Web 的管理

工作原理

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

用户在设备发送的 HTML 页面中输入组态数据。 设备评估该信息，并动态生成响应页面。

这种方法的优势在于只需要在客户端上安装 Internet 浏览器。

说明

安全连接

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

要求

WBM 显示

- 设备具有 IP 地址
- 设备与客户端 PC 之间存在连接。 可以通过 Windows ping 命令检查是否存在连接。
- 已启用通过 HTTPS 进行的访问。
- 在 Internet 浏览器中激活 JavaScript。
- 不可将 Internet 浏览器设置成每次从服务器访问页面时，浏览器都会重载页面。 页面动态内容的更新是通过其它机制来确保的。 在 Internet Explorer 中，可以在“选项 > Internet 选项 > 常规”(Options > Internet Options > General) 菜单的“浏览历史记录”(Browsing history) 部分，用“设置”(Settings) 按钮进行适当的设置。 在“检查所存网页的较新版本：”(Check for newer versions of stored pages:) 下，选择“自动”(Automatically)。
- 如果使用了防火墙，则必须打开相关端口。
  - 若使用 HTTP 进行访问： 端口 80
  - 若使用 HTTPS 进行访问： 端口 443

WBM 的显示情况已使用如下桌面 Internet 浏览器测试过：

- Microsoft Internet Explorer 10
- Mozilla Firefox 24ESR
- Chrome V30

说明

兼容性视图

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

在移动设备上显示 WBM

对于移动设备，必须满足以下最低要求：

分辨率	操作系统	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 6.1 的 Safari（iPad Mini 和 iPod Touch 4 代）
- 基于 Android 的 Chrome 版本 27（Galaxy Nexus 4 和 Galaxy Nexus 7）

说明

在移动设备上使用 WBM 及其显示

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

5.2 登录

建立与设备的连接

使用 Internet 浏览器按照以下步骤与设备建立连接：

1. 设备与客户端 PC 之间存在连接。 可以通过 ping 命令检查是否存在连接。
2. 在 Web 浏览器的地址框中，输入设备的 IP 地址或 URL。 如果设备的连接无故障，就会显示“基于 Web 的管理”(WBM) 的登录页面。

使用 Web 浏览器登录

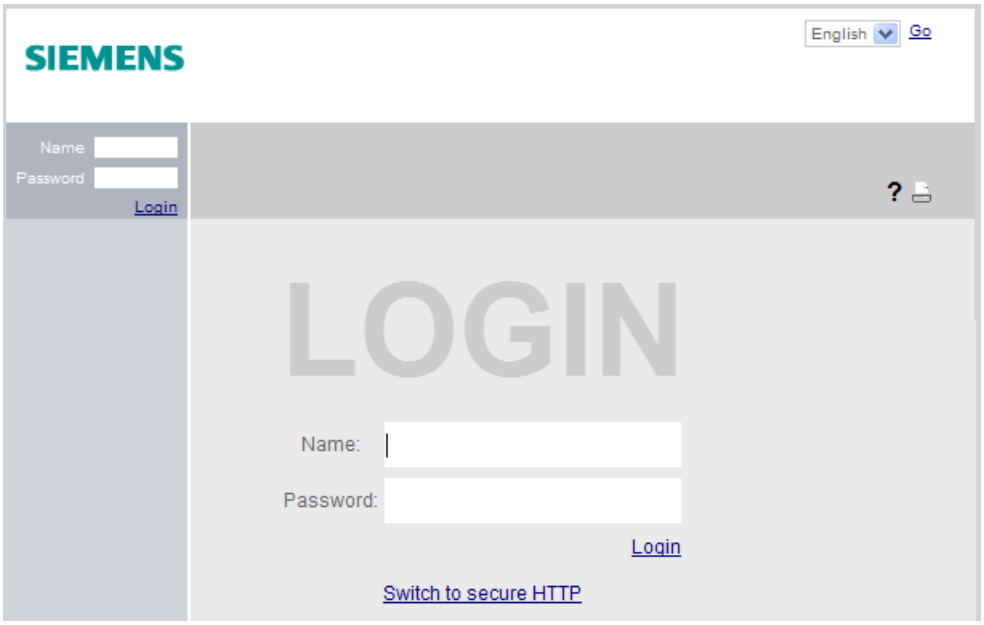
选择 WBM 的语言

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

说明

可用语言

在本版本中，只提供了英语。 后续版本将添加其它语言。



使用 HTTP 登录

可以采用两种方法通过 HTTP 进行登录。 可以使用浏览器窗口中央的登录选项进行登录，也可以使用其左上方区域的登录选项进行登录。

无论选择以上哪一种方法登录，都可以按照以下步骤进行操作：

1. 在“Name”输入框中输入以下内容：
   - "admin”：使用这种用户类型时，可以更改设备的设置（对组态数据进行读写访问）。
   - "user”：使用这种用户类型时，无法更改设备的任何设置（对组态数据进行读访问）。
2. 在“Password”输入框中输入密码。
   如果是首次登录或是在“Restore Factory Defaults und Restart”后登录，则在“Password”输入框中输入标准密码。
   - "admin”：标准密码“admin”
   - "user”：标准密码“user”
3. 单击“Login”按钮或按“Enter”键确认输入。
   如果是首次登录或是在“Restore Factory Defaults and Restart”之后登录，系统会提示您更改密码。 新密码不可少于 6 个字符长。 您需要重新输入密码进行确认。 密码输入必须匹配。
   单击“Set Values”，完成操作并激活新密码。

成功登录后，将显示起始页面。

使用 HTTPS 登录

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

1. 单击登录页面上的链接“Switch to secure HTTP”，或在 Internet 浏览器地址框中输入“https://”和设备的 IP 地址。
2. 确认显示的证书警告。
   将显示“基于 Web 的管理”登录页面。
3. 在“Name”输入框中输入以下内容：
   - "admin”：使用这种用户类型时，可以更改设备的设置（对组态数据进行读写访问）。
   - "user”：使用这种用户类型时，无法更改设备的任何设置（对组态数据进行读访问）。
4. 在“Password”输入框中输入密码。
   如果是首次登录或是在“Restore Factory Defaults und Restart”后登录，则在“Password”输入框中输入标准密码。
   - "admin”：标准密码“admin”
   - "user”：标准密码“user”
5. 单击“Login”按钮或按“Enter”键确认输入。
   如果是首次登录或是在“Restore Factory Defaults and Restart”之后登录，系统会提示您更改密码。 新密码不可少于 6 个字符长。 您需要重新输入密码进行确认。 密码输入必须匹配。
   单击“Set Values”，完成操作并激活新密码。

成功登录后，将显示起始页面。

5.3 “Information”菜单

5.3.1 起始页面

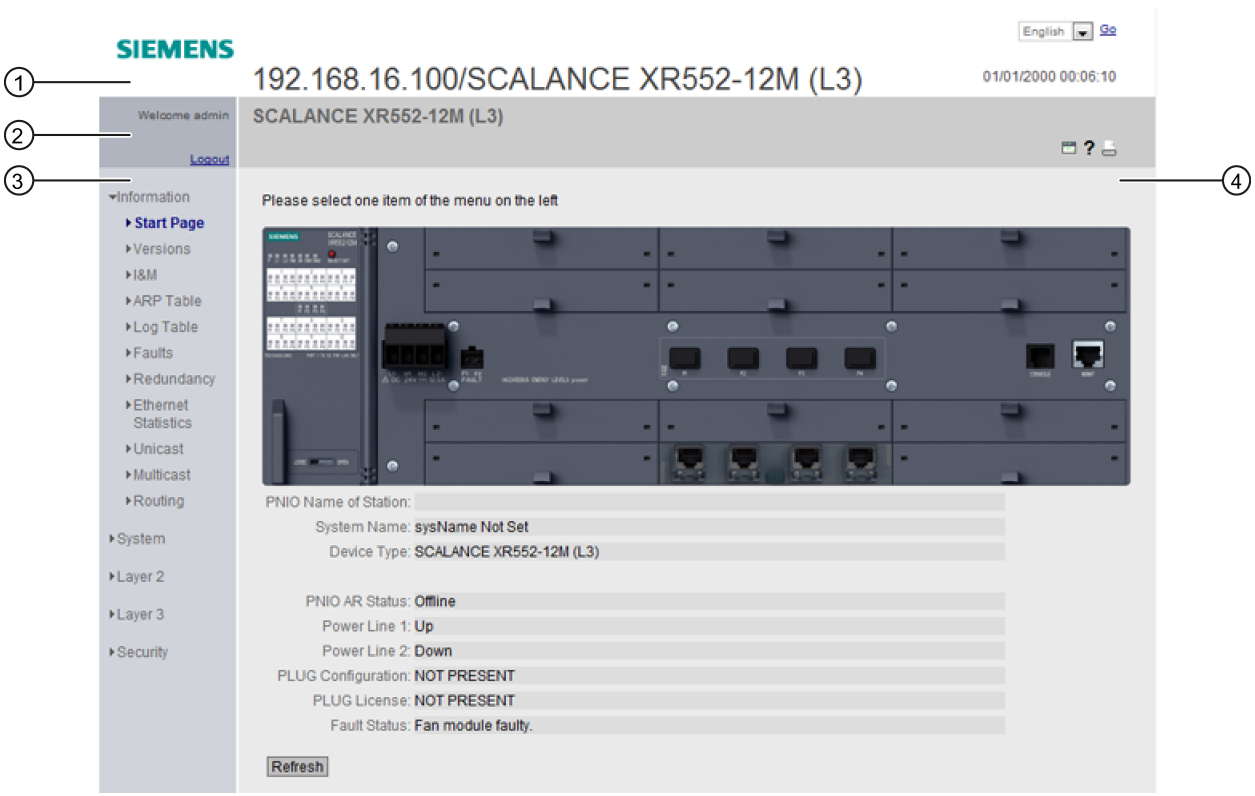
起始页面视图

输入设备的 IP 地址并成功登录后，将显示起始页面。 无法对该页面上的任何内容进行组态。

WBM 页面的常规布局

每个 WBM 页面通常都会有以下几个区域：

- 选择区 (1)： 上方区域
- 显示区 (2)： 上方区域
- 浏览区 (3)： 左侧区域
- 内容区 (4)： 中间区域



选择区 (1)

选择区中有以下内容：

- Siemens AG 徽标
- 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，则会显示设备的带内端口 IP 地址。
  - ""系统名称"(System Name) 是设备名称。
    如果使用设备出厂时的设置，则会显示设备类型。

  可以通过“System > General > Device”更改该显示画面的内容。
- 用于选择语言的下拉列表
- 系统时间和日期
  可以通过“System > System Time”更改该显示画面的内容。

显示区 (2)

在显示区的上半部分，您可以看到当前选择菜单项的完整标题。

显示区的下半部分包含以下项目：

- **打印机** 
  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，请使用浏览器的“打印预览”功能。

- **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。

- **LED 模拟**
  设备的每个组件都具有一个或多个 LED，这些 LED 会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。 未占用的插槽或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。
  单击仿真的“Select/Set”按钮，可更改显示模式（LED DM 或 D1/D2）。
  单击该按钮后，可以打开 LED 仿真窗口。 可以在切换菜单过程中显示该窗口，并根据需要进行移动。 要关闭 LED 仿真，请单击 LED 仿真窗口中的关闭按钮。
- **注销**
  可以单击“注销”(Logout) 链接从任何 WBM 页面注销。

浏览区 (3)

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

内容区 (4)

内容区显示设备图形。 图形为动态。 始终显示基本设备。 如果扩展器/媒介模块连接至基本设备，则会同时显示。

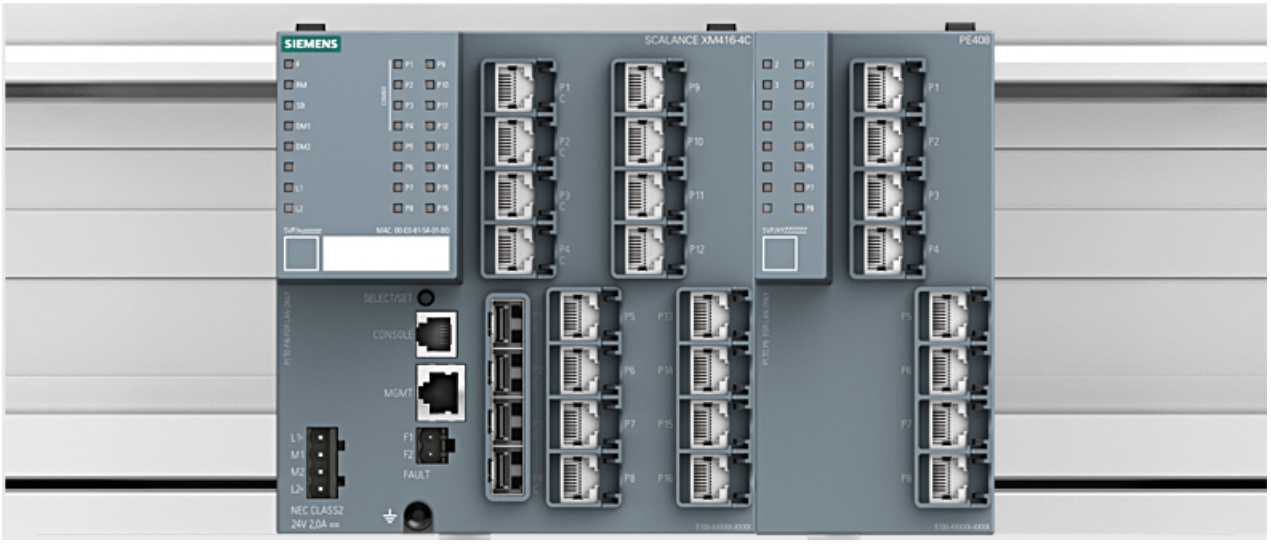


图 5-1　　设备图形示例： 带有一个端口扩展器 PE408 的 SCALANCE XM416-4C

设备图形下面会显示以下项目：

- **“PNIO 站名称”(PNIO Name of Station)**
  显示 PROFINET IO 设备名称。
- **“系统名称”(System Name)**
  显示设备的系统名称。
- **“设备类型”(Device Type)**
  显示设备类型。
- **“PNIO AR 状态”(PNIO AR Status)**
  显示 PROFINET IO 应用关系状态。
  – “在线”(Online)
    存在与 PROFINET IO 控制器的连接。 PROFINET IO 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 IO 控制器。
    在这种状态下，无法在设备上组态 PROFINET IO 控制器所设置的参数。
  – “离线”(Offline)
    没有与 PROFINET IO 控制器的连接。
- **Power Line 1/Power Line 2**
  – “生效”(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 组态 (PLUG configuration)**
  在 PLUG 上显示组态数据状态，请参见“系统 > PLUG 组态 (页 157)”部分。
- **PLUG 许可证 (PLUG license)**
  在 PLUG 上显示许可证状态，请参见“系统 > PLUG 许可证 (页 160)”部分。
- **“故障状态”(Faults 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) 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“Set Values”按钮将组态更改传送到设备之前单击“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

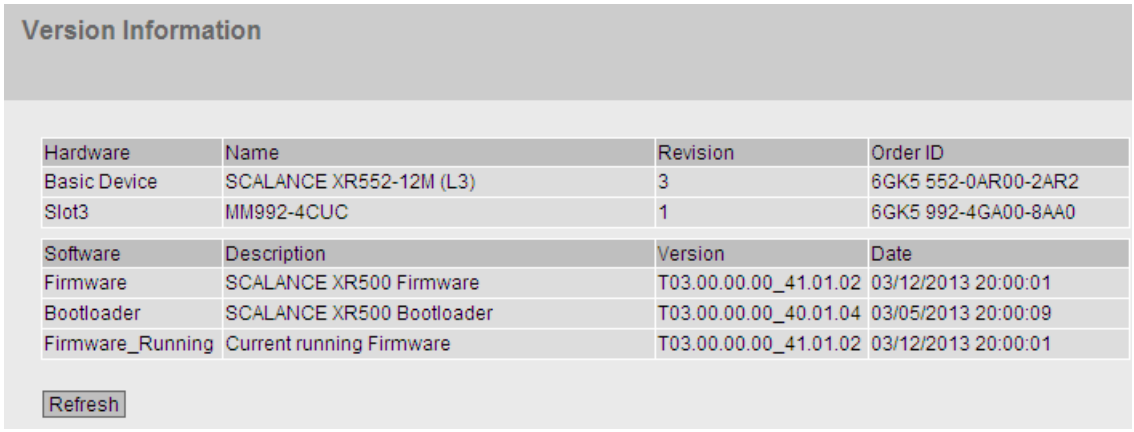
  仅在以“admin”身份登录后才可以更改组态数据。

- **使用“创建”(Create) 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。
- **使用“删除”(Delete) 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。 执行删除操作之后，将更新 WBM 中的页面。
- **使用“下一页”(Next) 向下翻页**
  页面上能够显示的数据记录数受到限制。 单击“Next”按钮，可向下翻页查看数据记录。
- **使用“上一页”(Prev) 向上翻页**
  页面上能够显示的数据记录数受到限制。 单击“Prev”按钮，可向上翻页查看数据记录。

5.3.2 Versions

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：

- **Hardware**
  - Basic Device
    显示基本设备
  - PX.X
    X.X = 插入 SFP 模块的端口。
  - 插槽 X
    “X”= 插槽号： 插入该插槽的模块。
- **Name**
  显示设备或模块的名称。
- **Revision**
  显示设备的硬件版本。
- **Order ID**
  显示设备或模块的订货号。

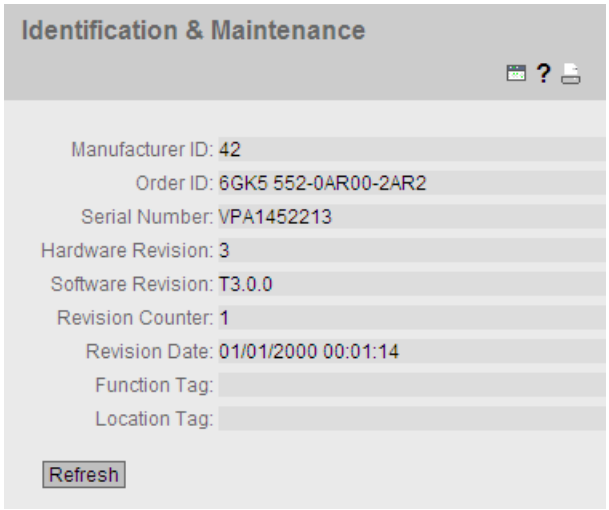
表 2 包含以下列：

- **Software**
  - 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。
  - Bootloader
    显示存储在设备上的引导软件的版本。
- **Description**
  显示软件的简要说明。
- **Version**
  显示软件版本的版本号。
- **Date**
  显示软件版本的创建日期。

5.3.3 I&M

标识和维护数据

该页面包含具体设备的供应商信息以及维护数据（如订货号、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

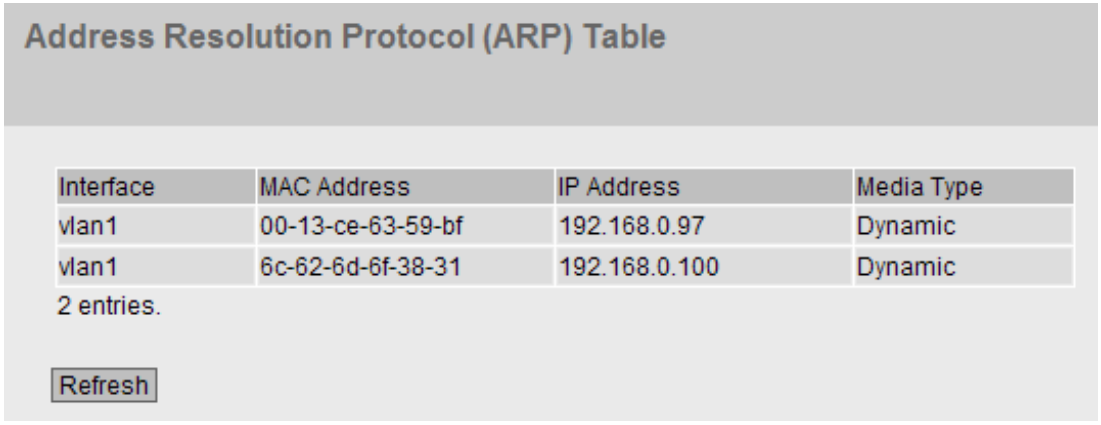
该表格包括以下行：

- **“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 Revision)**
  显示软件版本。
- **“修订版计数器”(Revision Counter)**
  显示修订版计数器： 从初始调试开始计数的修订版计数器
- **“修订日期”(Revision Date)**
  修订日期： 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）。 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。

5.3.4 ARP 表

MAC 地址和 IP 地址的分配

使用地址解析协议 (ARP, Address Resolution Protocol) 时，MAC 地址到 IP 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。



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 地址”(MAC Address)**
  显示目标设备的 MAC 地址。
- **“IP 地址”(IP Address)**
  显示目标设备的 IP 地址。
- **“介质类型”(Media Type)**
  显示连接的类型。
  - “动态”(Dynamic)
    设备自动识别到地址数据。
  - “静态”(Static)
    地址作为静态地址输入。

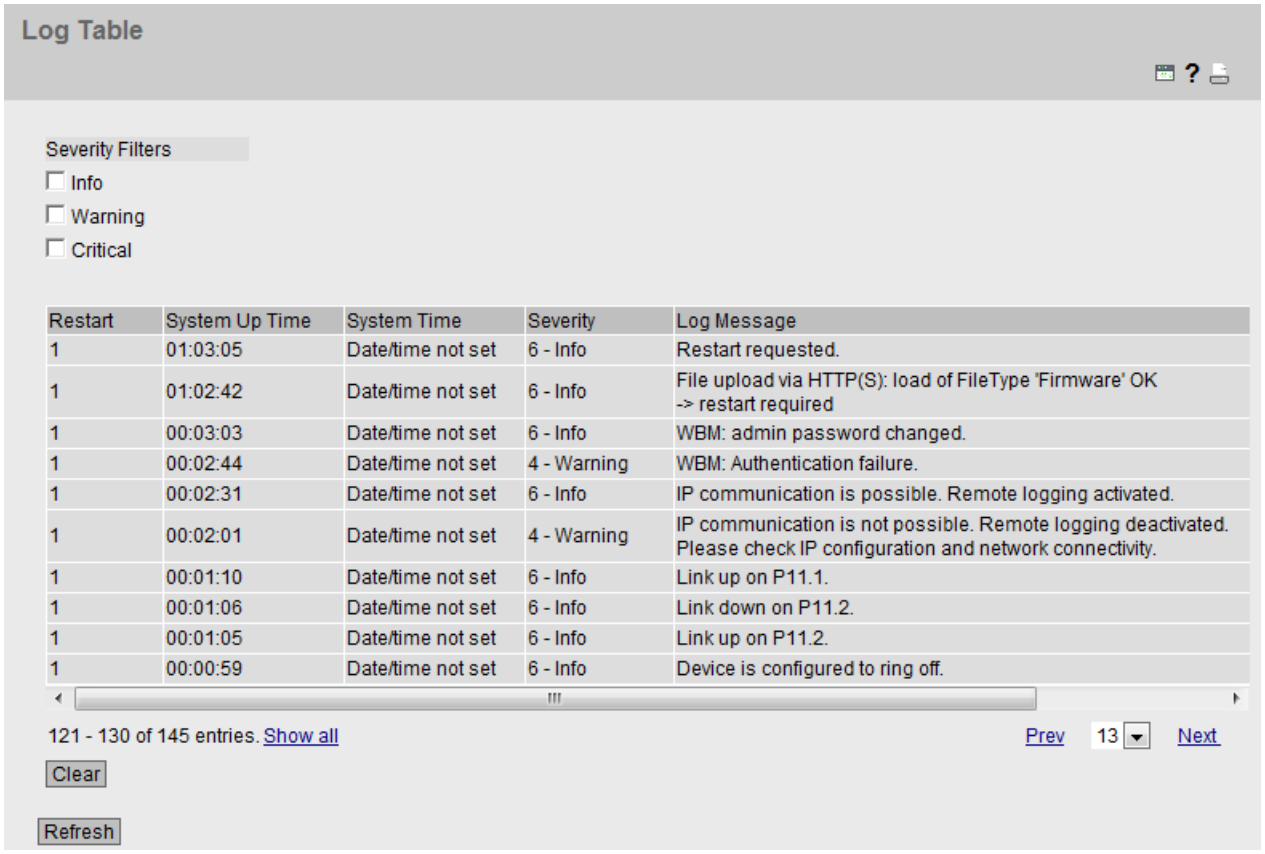
5.3.5 日志表

记录事件

设备允许用户记录正在发生的事件，有些事件可以在 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。

无法对该页面上的任何内容进行组态。



严重程度过滤器

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。

- **“信息”(Info)**
  信息
- **“警告”(Warning)**
  警告
- **“严重”(Critical)**
  严重

要显示所有条目，可选中所有复选框，或将它们留空。

显示值说明

该表格包括以下列：

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

按钮和输入框说明

“Clear”按钮

单击此按钮可删除事件日志文件的内容。 还会清空显示画面。 仅当将设备恢复为出厂设置并重启设备后，才会复位重启计数器。

说明

该表中的条目数限制为 400 条。达到这一数目之后，会丢弃最早的条目。 该表会永久保存在内存中。

“全部显示”(Show all) 按钮

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

“Next”按钮

单击该按钮可转至下一页。

“Prev”按钮

单击该按钮可转至上一页。

用于更改页面的下拉列表

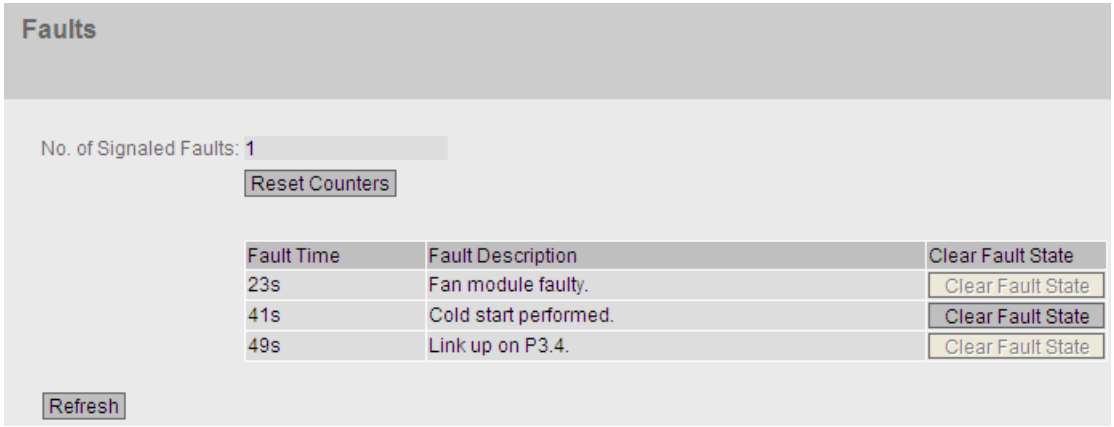
从该下拉列表中选择要转至的页面。

5.3.6 故障

错误状态

此页面显示所发生的所有错误。“Cold/Warm Start”事件的错误可在确认后删除。
如果已没有未回应的错误/故障消息，则故障 LED 将熄灭。

始终从上次启动系统后计算时间。 重新启动系统时，会在故障存储器中创建包含重启类型信息的新条目。



说明

“**No. of Signaled Faults**”框显示自上次启动后发生故障的次数。 单击“复位计数器”(Reset Counters) 按钮可复位该值。

该表包含以下列：

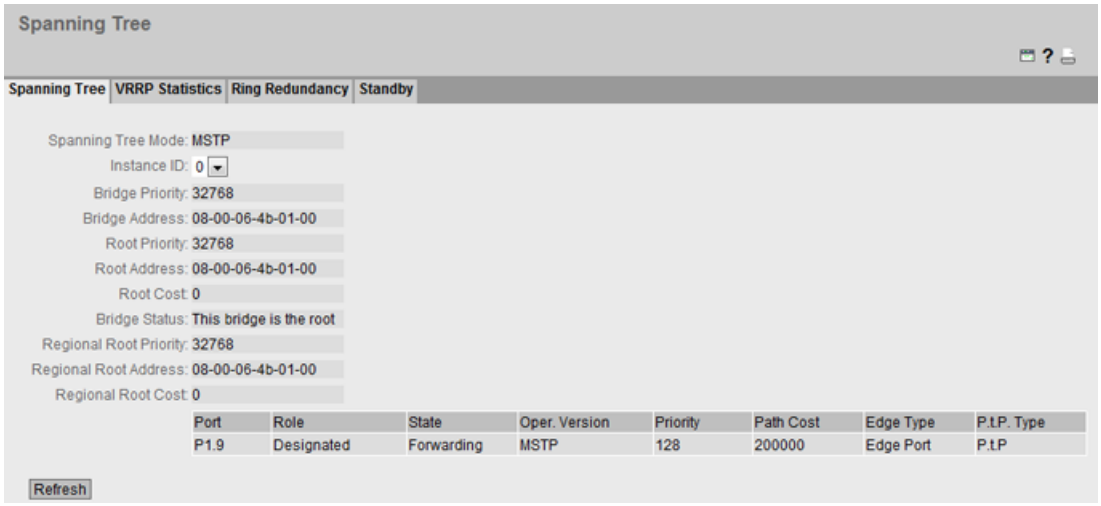
- **Fault Time**
  显示在所描述的故障发生时设备自上次重启以来已持续运行的时间。
- **Fault Description**
  显示设备的故障状态。
- **Clear Fault State**
  如果启用了“清除故障状态”(Clear Fault State) 按钮，则可删除故障。

5.3.7 冗余

5.3.7.1 生成树

简介

该页面显示有关生成树和根网桥设置的最新信息。



显示值说明

该页面显示以下字段：

- **Spanning Tree Mode**
  显示设置的模式。 在“Layer 2 > Configuration”和“Layer 2 > MSTP > General”中指定模式。
  可以使用以下值：
  - '-'
  - STP
  - RSTP
  - MSTP
- **Instance ID**
  显示实例编号。 该参数取决于组态的模式。
- **Bridge Priority / Root Priority**
  哪个设备成为根网桥由网桥优先级决定。 优先级最高的网桥（换句话说，此参数的值最小）将成为根网桥。 如果网络中有多个设备具有相同优先级，则 MAC 地址数值最小的设备将成为根网桥。 网桥优先级和 MAC 地址这两个参数一起构成网桥标识符。 由于根网桥管理所有路径的变更，出于帧延迟的考虑，根网桥应该尽可能处在中心位置。 网桥优先级的值是 4096 的整数倍数，值范围从 0 到 32768。
- **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。
- **Regional Root Priority**（仅适用于 MSTP）
  相关描述，请参见“Bridge Priority/Root Priority”。
- **Regional Root Address**（仅适用于 MSTP）
  显示设备的 MAC 地址。
- **区域根开销 (Regional Root Cost)**（仅适用于 MSTP）
  显示从区域根网桥到根网桥的路径开销。

该表格包括以下列：

- **Port**
  显示设备通信所用的端口。 端口由模块号和端口号组成，例如，端口 0.1 表示模块 0，端口 1。

- **Role**
  显示端口状态。 可能的值包括：
  - Disabled
    已从生成树中手动移除端口，生成树将不再考虑该端口。
  - Designated
    端口从根网桥中转移数据。
  - Alternate
    端口具有指向网段的备用路径。
  - Backup
    如果交换机具有多个指向同一网段的端口，则“较差”端口将变为备用端口。
  - Root
    端口提供指向根网桥的最佳路径。
  - Master
    此端口指向 MST 区域外部的根网桥。

- **状态 (State)**
  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。 可能的状态如下：
  - Discarding
    端口接收 BPDU 帧。 其它进入或离开的帧会被丢弃。
  - Listening
    端口接收和发送 BPDU 帧。 端口包括在生成树算法中。 其它进入或离开的帧会被丢弃。
  - Learning
    端口主动学习拓扑，即学习节点地址。 其它进入或离开的帧会被丢弃。
  - Forwarding
    经过重新组态时间后，端口在网络中激活。 该端口接收和发送数据帧。

- **运行 版本 (Oper. Version)**
  描述端口以何种生成树类型运行

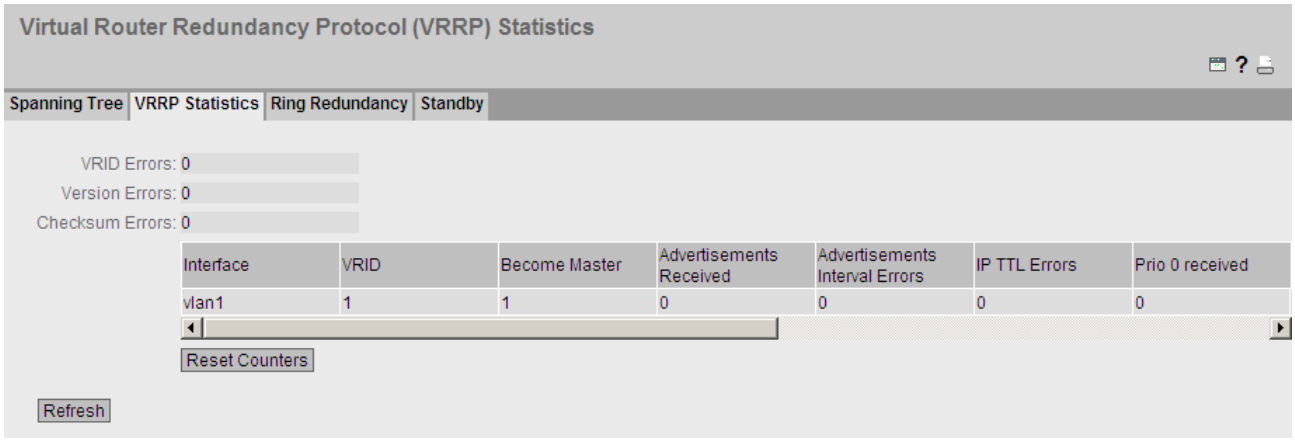
- **Priority**
  如果由生成树计算出的路径可能经过设备的多个端口，则选择优先级最高的端口（也就是此参数值最小的端口）。 可以输入作为优先级的值为 0 到 240，步长是 16。如果输入的值不能被 16 整除，则值会自动调整。 默认值为 128。

- **路径开销 (Path Cost)**
  此参数用于计算将要选择的路径。 选择具有最小值的路径。 如果设备的多个端口具有相同的值，则选择端口号最小的端口。
  如果“开销计算”(Cost Calc)字段中的值为“0”，则显示自动计算出的值。 否则会显示“开销计算”(Cost Calc) 字段的值。
  路径成本的计算很大程度上基于传输速度。 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。
- **Edge Type**
  显示连接类型。 可能的值包括：
  - Edge Port
    此端口上有终端设备。
  - No Edge Port
    此端口上有生成树或快速生成树设备。
- **P.t.P. Type**
  显示点对点链路类型。 可能的值包括：
  - P.t.P.
    对于半双工，认为是点对点链路。
  -
    “共享介质”(Shared Media)
    对于全双工连接，不认为是点对点链路。

5.3.7.2 VRRP 统计信息

简介

此页面显示 VRRP 协议以及全部组态虚拟路由器的统计信息。



显示值说明

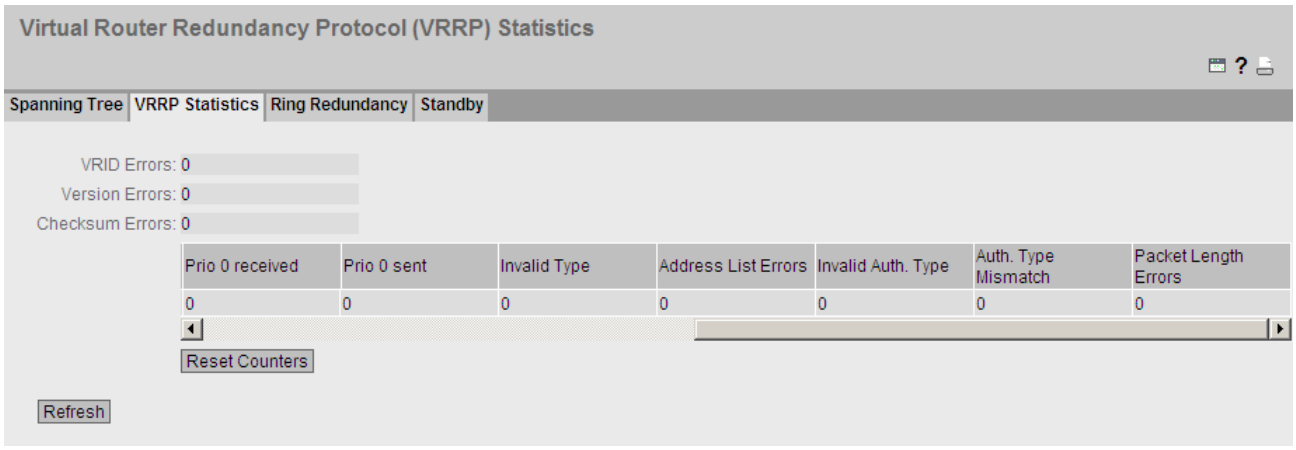
该页面显示以下字段：

- **“VRID 错误”(VRID Errors)**
  显示包含不受支持的 VRID 的已接收 VRRP 数据包的数目。
- **“版本错误”(Version Errors)**
  显示包含无效版本号的已接收 VRRP 数据包的数目。
- **“校验和错误”(Checksum Errors)**
  显示包含无效校验和的已接收 VRRP 数据包的数目。

该表格包括以下列：

- **“接口”(Interfaces)**
  与设置相关的接口。
- **VRID**
  显示虚拟路由器的 ID。
  有效值为 1 到 255。
- **“成为主设备”(Become Master)**
  显示该虚拟路由器变为“主设备”状态的频率。
- **“接收到通告”(Advertisements Received)**
  显示接收到包含不良地址列表的 VRRP 数据包的频率。

- **“通告间隔错误”(Advertisements Interval Errors)**
  显示已接收到间隔与本地设置的值不匹配的不良 VRRP 数据包的数目。
- **“IP TTL 错误”(IP TTL Errors)**
  显示已接收到 IP 报头中的 TTL（Time to live，生存时间）值不正确的不良 VRRP 数据包的数目。
- **“接收到优先级 0”(Prio 0 received)**
  显示已接收的优先级为 0 的 VRRP 数据包的数目。 主路由器关闭时，发送优先级为 0 的 VRRP 数据包。 这些数据包允许快速切换至相关的备用路由器。
- **“已发送优先级 0”(Prio 0 sent)**
  显示已发送的优先级为 0 的 VRRP 数据包的数目。 主路由器关闭时，将发送优先级为 0 的数据包。这些数据包允许快速切换至相关的备用路由器。

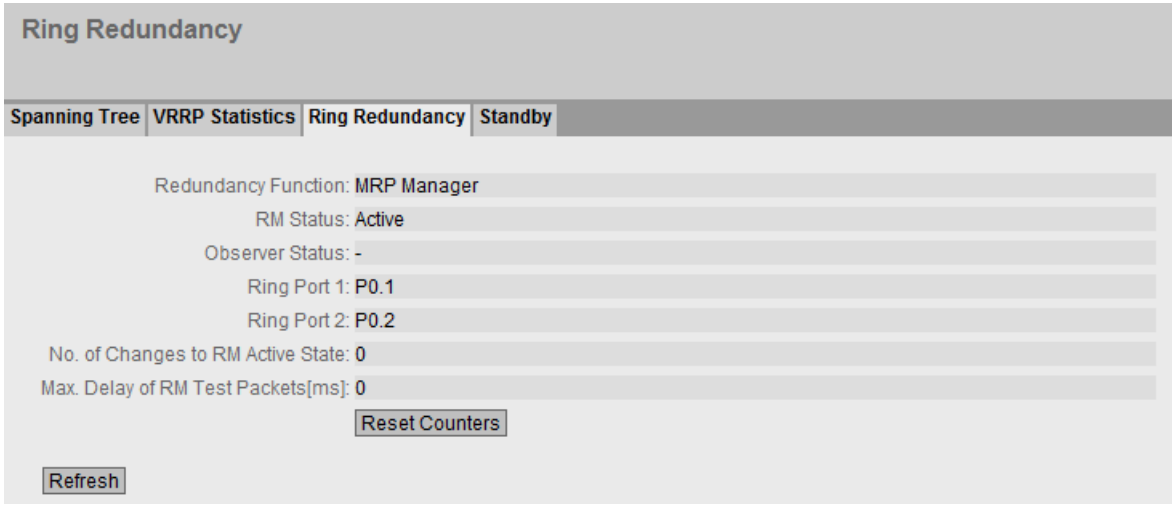


- **“无效验证类型”(Invalid Auth. Type)**
  显示已接收到验证类型不为类型 0 的不良 VRRP 数据包的数目。类型 0 表示“无验证”。
- **“验证类型不匹配”(Auth. Type Mismatch)**
  显示已接收到验证类型不匹配的不良 VRRP 数据包的数目。
- **“数据包长度错误”(Packet Length Error)**
  显示已接收到长度不正确的不良 VRRP 数据包的数目。

5.3.7.3 环网冗余

有关环网冗余的信息

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



该表格包括以下列：

- **Redundancy Function**
  “冗余功能”(Redundancy Function) 列显示设备在环网内的角色：
  - No Ring Redundancy (off)
    工业以太网交换机正在无冗余功能的情况下运行。
  - HRP Client
    工业以太网交换机充当 HRP 客户端。
  - HRP Manager
    工业以太网交换机充当 HRP 管理器。
  - MRP Client
    工业以太网交换机正在充当 MRP 客户端。
  - MRP Manager
    工业以太网交换机正在充当 MRP 管理器。
- **RM Status**
  “RM 状态”(RM Status) 列显示工业以太网交换机是否用作冗余管理器，以及此角色是断开环网还是闭合环网。
  - Passive：
    工业以太网交换机充当冗余管理器，并已断开环网；即：与环网端口相连的交换机线路处于无故障运行中。 在工业以太网交换机并未充当冗余管理器时（RM 功能已禁用），也将显示未激活状态。
  - Active：
    工业以太网交换机充当冗余管理器，并已闭合环网；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。
  - 如果完全禁用环型拓扑中的介质冗余，则会显示最后组态的环网端口，并显示文本“环网冗余已禁用”(Ring Redundancy disabled)。
- **Observer Status**
  显示观察器的当前状态。
- **Ring Port 1 以及 Ring Port 2**
  “环网端口 1”(Ring Port 1) 和“环网端口 2”(Ring Port 2) 两列显示正用作环网端口的端口。
- **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“冗余管理器已禁用”(Redundancy Manager Disabled)。
- **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“冗余管理器已禁用”(Redundancy Manager Disabled)。
- 在此页面上单击“复位计数器”(Reset Counters) 按钮复位计数器。

5.3.7.4 备用冗余

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。

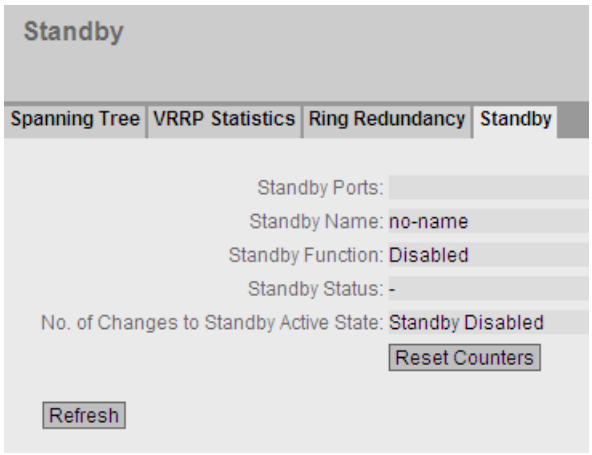
说明

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：



显示的框的含义如下：

- **Standby Port**
  “备用端口”(Standby Port) 显示框中显示一个或多个备用端口。

  说明

  可以组态一个或多个备用端口。 在以下段落中，指多个“备用”端口。

- **Standby Name**
  备用连接名称

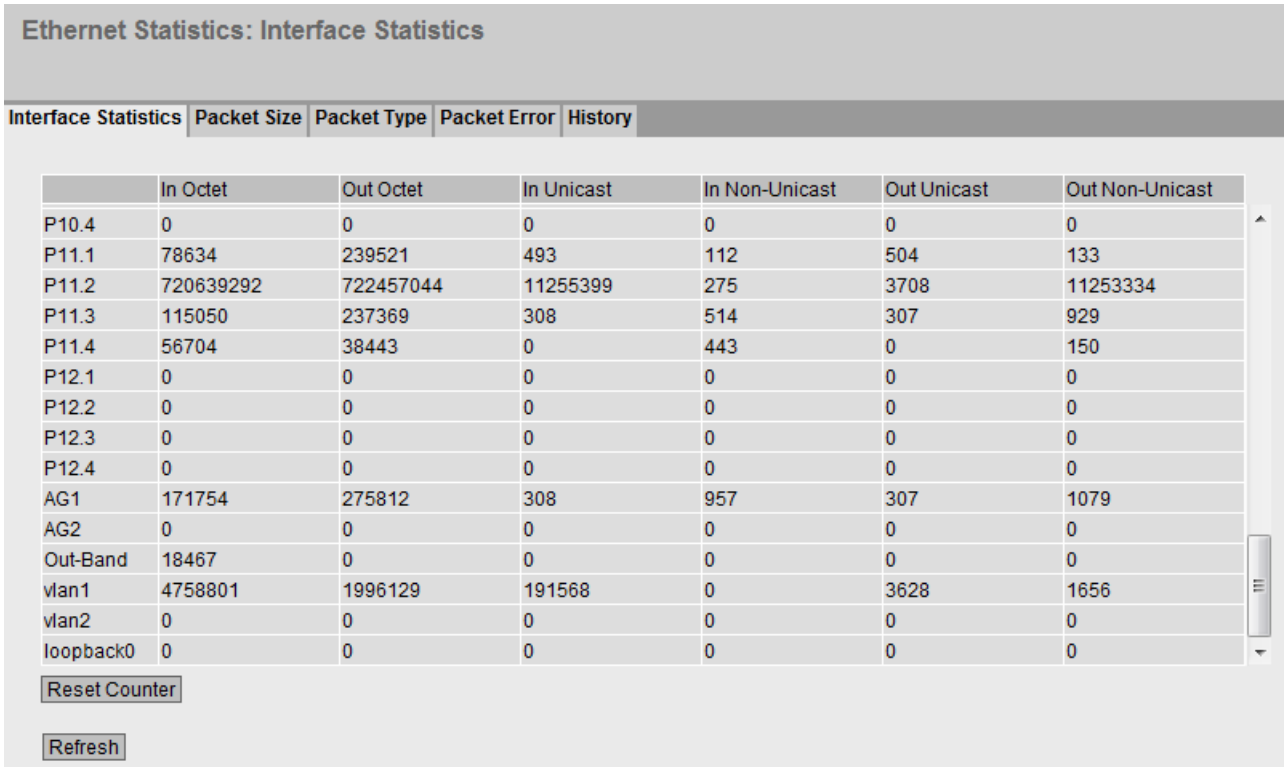
- **Standby Function**
  - Master：
    该设备与伙伴设备相连并充当主设备。正常运行时，此设备的备用端口处于激活状态。
  - Slave：
    该设备与伙伴设备相连并充当从设备。正常运行时，此设备的备用端口处于未激活状态。
  - Disabled：
    禁用备用链路。 该设备既不充当主设备也不充当从设备。备用端口将用作不具有备用功能的常规端口。
  - Waiting for Connection....：
    尚未与伙伴设备建立连接。备用端口处于未激活状态。 在这种情况下，或是伙伴设备中的组态不一致（例如，连接名错误、备用链路被禁用），或是存在实际故障（例如，设备故障、链路中断）。
  - Connection Lost：
    与伙伴设备的现有连接已丢失。 在这种情况下，或是存在实际故障（例如，设备故障、链路中断），或是伙伴设备的组态已被修改（例如，连接名不同、备用链路被禁用）。
- **Standby Status**
  “备用状态”(Standby Status) 显示框中显示备用端口的状态：
  - 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。
  - Passive：
    该设备的备用端口处于未激活状态；即备用端口已禁用，无法进行帧通信。
- **No. of Changes to Standby Active State**
  显示工业以太网交换机的备用状态从“未激活”变为“激活”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”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)。
  在此页面上单击“复位计数器”(Reset Counters) 按钮复位计数器。
  每次重启设备后，计数器将自动复位。

5.3.8 以太网统计信息

5.3.8.1 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。



	In Octet	Out Octet	In Unicast	In Non-Unicast	Out Unicast	Out Non-Unicast
P10.4	0	0	0	0	0	0
P11.1	78634	239521	493	112	504	133
P11.2	720639292	722457044	11255399	275	3708	11253334
P11.3	115050	237369	308	514	307	929
P11.4	56704	38443	0	443	0	150
P12.1	0	0	0	0	0	0
P12.2	0	0	0	0	0	0
P12.3	0	0	0	0	0	0
P12.4	0	0	0	0	0	0
AG1	171754	275812	308	957	307	1079
AG2	0	0	0	0	0	0
Out-Band	18467	0	0	0	0	0
vlan1	4758801	1996129	191568	0	3628	1656
vlan2	0	0	0	0	0	0
loopback0	0	0	0	0	0	0

图 5-2 接口统计信息

显示值

该表格包括以下列：

- **输入八位位组 (In Octet)**
  显示接收到的字节数。
- **输出八位位组 (Out Octet)**
  显示发送的字节数。
- **输入单播 (In Unicast)**
  显示已接收的单播帧数。

- **输入非单播 (In Non-Unicast)**
  显示接收到的非单播类型帧的数目。
- **输出单播 (Out Unicast)**
  显示已发送的单播帧数。
- **输出非单播 (Out Non-Unicast)**
  显示发送的非单播类型帧的数目。

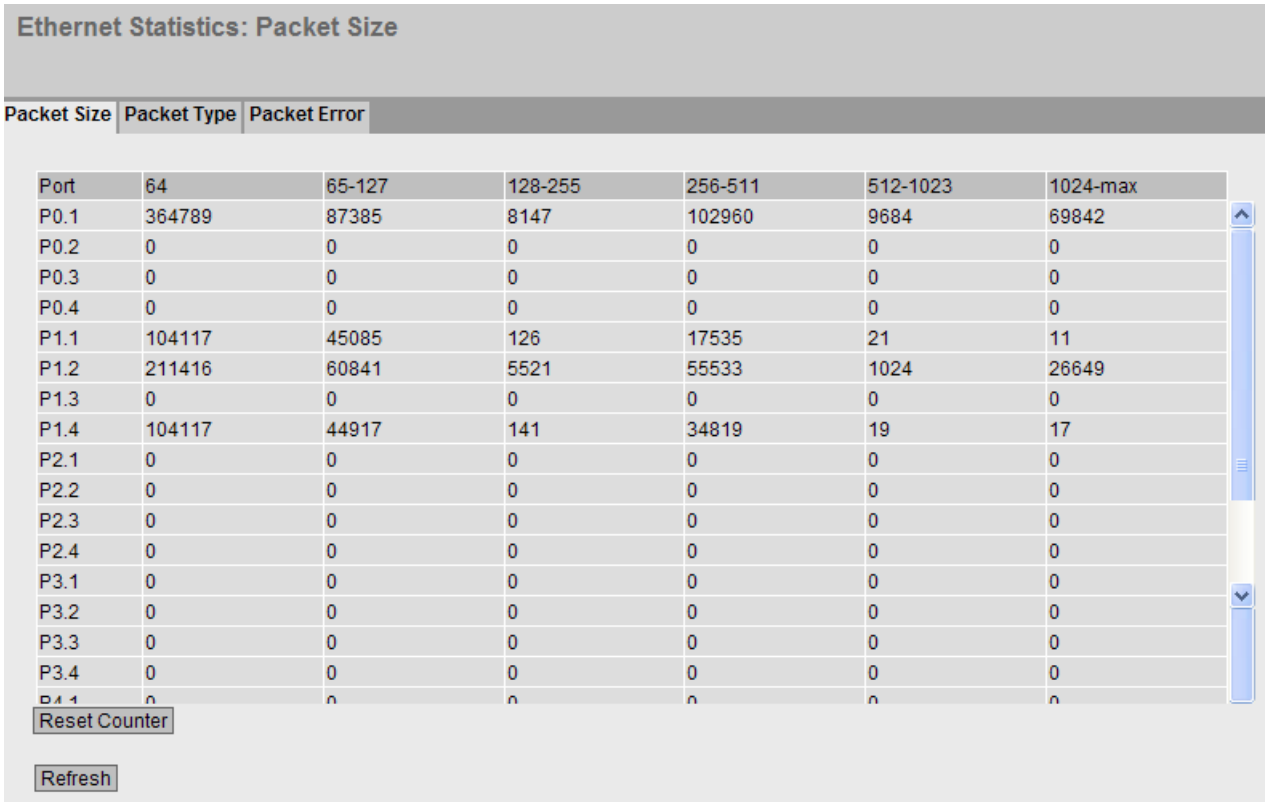
5.3.8.2 数据包大小

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不同大小的帧。 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“第 2 层 > RMON > 统计信息”(Layer 2 > RMON > Statistics) 页面中，可以设置要显示其值的端口。



显示值说明

该表格包括以下列：

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

  说明

  帧统计信息显示

  在与帧大小相关的统计信息中，需要注意的是，会同时对进入帧和离开帧进行计数。

- **“帧长度”(Frame lengths)**
  端口号后面的其它各列包含按照帧长度分类的进入帧的绝对数量。
  帧长度分为以下几类：
  - 64 字节
  - 65 - 127 字节
  - 128 - 255 字节
  - 256 - 511 字节
  - 512 - 1023 字节
  - 1024 - 最大值

说明

封锁端口上的数据通信

由于技术原因，可根据需要显示封锁端口上的数据包信息。

按钮描述

“复位计数器”(Reset Counter) 按钮

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

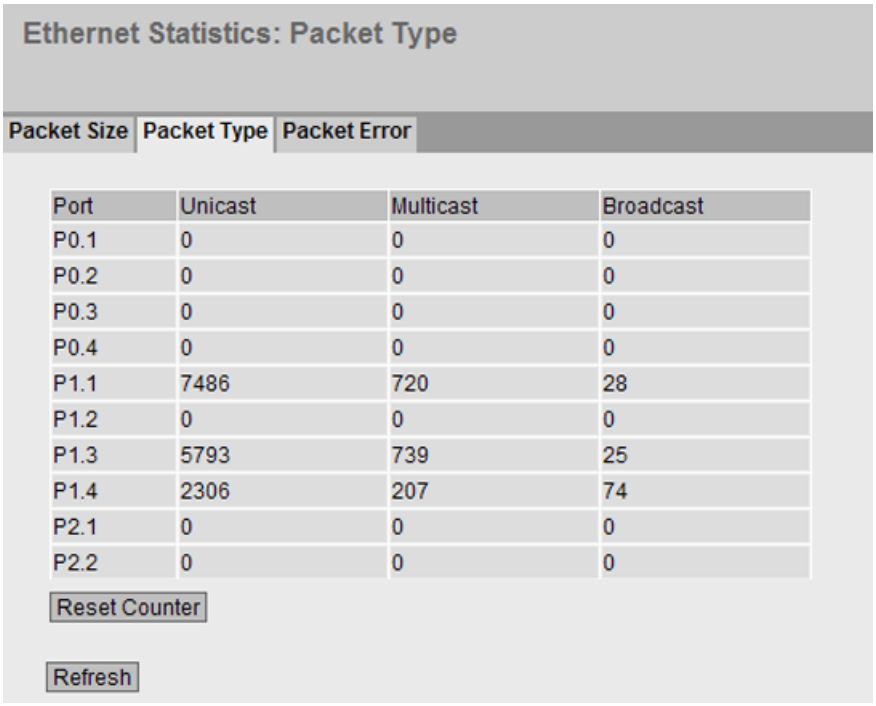
5.3.8.3 数据包类型

按类型分类的已接收帧

该页面显示每个端口接收到多少“Unicast”、“Multicast”和“Broadcast”类型的帧。 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“第 2 层 > RMON > 统计信息”(Layer 2 > RMON > Statistics) 页面中，可以设置要显示其值的端口。



显示值说明

该表格包括以下列：

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

按钮描述

“Reset Counters”按钮

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

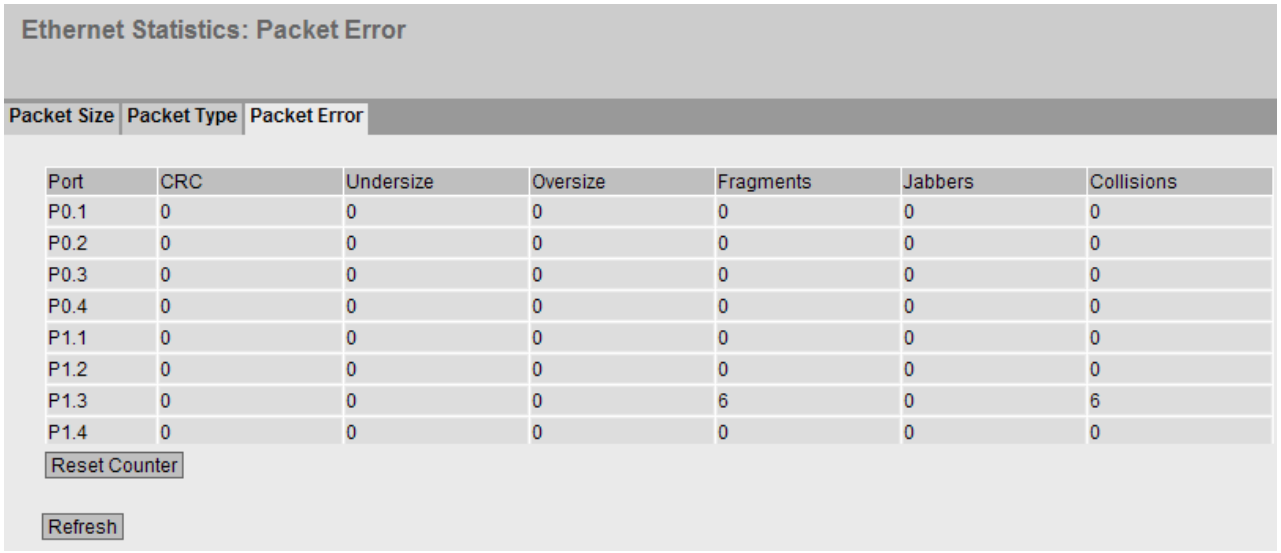
5.3.8.4 数据包错误

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“第 2 层 > RMON > 统计信息”(Layer 2 > RMON > Statistics) 页面中，可以设置要显示其值的端口。



显示值说明

该表格包括以下列：

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

    检测到的冲突。

按钮描述

“Reset Counters”按钮

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

5.3.8.5 历史

统计信息的样本

此页面显示每个端口的 RMON 统计信息的样本。

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

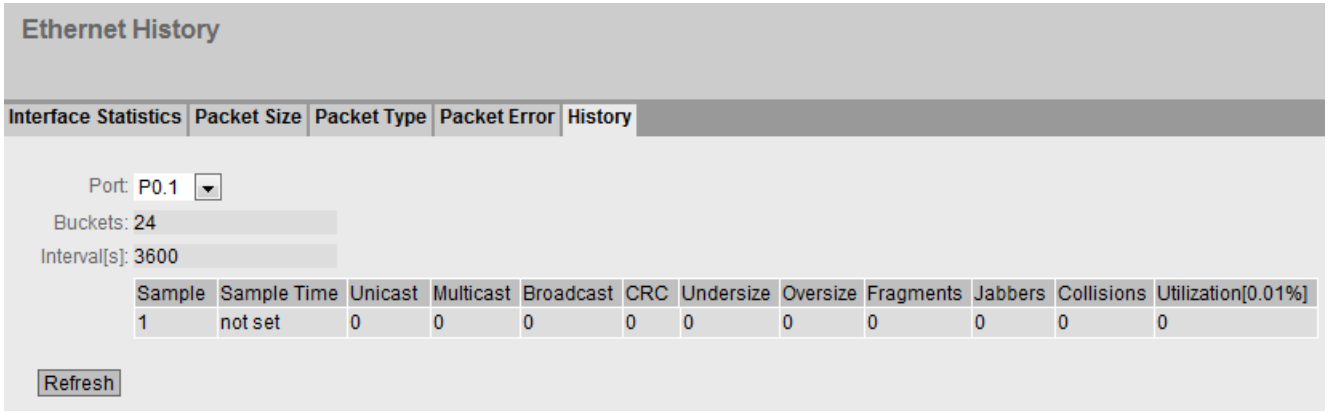


图 5-3 历史

设置

- **端口**
  选择要为其显示历史记录的端口。

显示值

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

该表格包括以下列：

- **样本 (Sample)**
  样本的编号
- **采样时间 (Sample Time)**
  获取样本时的系统运行时间。
- **单播**
  已接收的单播帧数。
- **组播**
  已接收的组播帧数。
- **广播 (Broadcast)**
  已接收的广播帧数。
- **CRC**
  CRC 校验和错误的帧的数目。

- **Undersize**
  长度小于 64 字节的帧的数目。
- **Oversize**
  由于长度过长而被丢弃的帧的数目。
- **Fragments**
  长度小于 64 字节并且 CRC 校验和错误的帧的数目。
- **Jabbers**
  带有 CRC 校验和错误的 VLAN 标记，并由于长度过长而被丢弃的帧的数目。
- **Collisions**
  接收到的帧的冲突数目。
- **利用率 (Utilization) [0.01%]**
  端口在获取样本期间的利用率。

5.3.9 单播

单播过滤表的状态

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

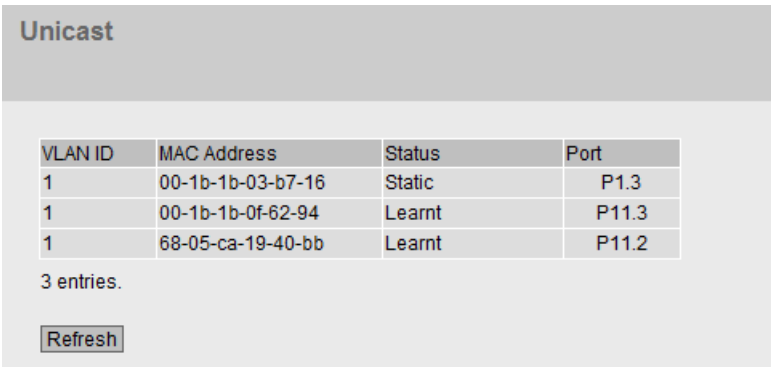


图 5-4 单播

说明

该表包含以下各列：

- **VLAN ID**
  显示分配给此 MAC 地址的 VLAN ID。
- **MAC 地址 (MAC Address)**
  显示设备已学习或用户已组态的节点 MAC 地址。
- **状态 (Status)**
  显示每个地址条目的状态：
  - Learnt
    通过从节点接收帧，学习相应的地址；如果从此节点再没接收到数据包，则在老化时间结束时删除该地址。
  - Static
    由用户组态。 静态地址会永久存储；也就是说，当老化时间结束或交换机重启时，静态地址不会被删除。
- **端口 (Port)**
  显示访问指定地址的节点时所使用的端口。 设备接收到的目标地址与此地址相匹配的帧将被转发到此端口。

5.3.10 组播

组播过滤表的状态

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

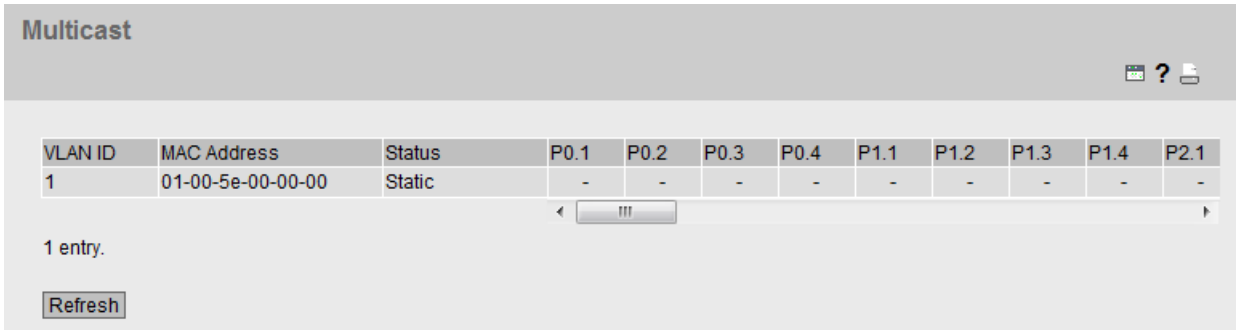


图 5-5 组播

说明

该表包含以下各列：

- **VLAN ID**
  显示要向其分配 MAC 组播地址的 VLAN 的 VLAN ID。
- **MAC 地址 (MAC Address)**
  显示设备已学习或用户已组态的 MAC 组播地址。
- **状态 (Status)**
  显示每个地址条目的状态。 可能的信息如下：
  - static
    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。
  - IGMP
    此地址的目标端口通过 IGMP 组态获得。
  - GMRP
    此地址的目标端口由收到的 GMRP 帧注册。 端口列表 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。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。 - 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 动态学习的地址。
- **端口列表 (Port List)**
  每个插槽都有一列对应。 在每一列内，端口所属的组播组显示如下：
  - M
    （成员）通过此端口发送组播帧。
  - R
    （已注册）组播组的成员，由 GMRP 帧注册。
  - I
    (IGMP) 组播组的成员，由 IGMP 帧注册。
  - –
    不是组播组的成员。不通过此端口发送包含所定义组播 MAC 地址的组播帧。
  - F
    （已禁止）不是组播组的成员。此地址也不能是使用 GMRP 或 IGMP 动态学习的地址。

5.3.11 LLDP

邻居表状态

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

在以下部分设置 LLDP 代理接收或发送信息所使用的接口：“第 2 层 > LLDP (页 226)”。

图 5-6 信息 LLDP

显示值说明

该表包含以下各列：

- **设备 ID (Device ID)**
  所连设备的设备 ID。
- **本地接口 (Local Interface)**
  工业以太网交换机接收信息的端口。
- **保存时间 (Hold Time)**
  此处指定的时间是条目存储在 MIB 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。

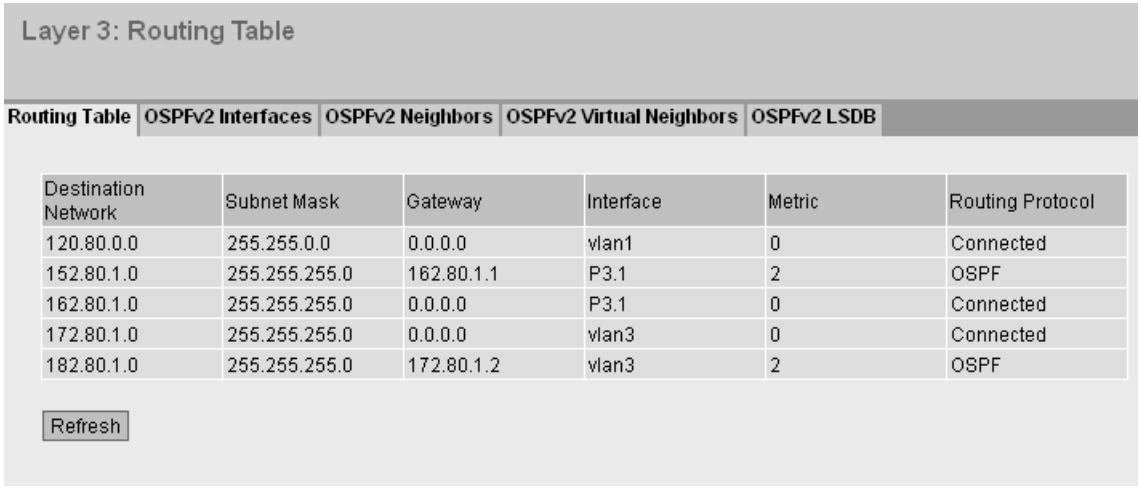
- **性能 (Capability)**
  显示所连设备的属性：
  - 路由器
  - 网桥
  - 电话
  - DOCSIS 电缆设备
  - WLAN 接入点
  - 中继器
  - 站
  - 其它
- **端口 ID (Port ID)**
  连接工业以太网交换机的设备端口。

5.3.12 路由

5.3.12.1 路由表

简介

此页用于显示设备的路由表。



显示值说明

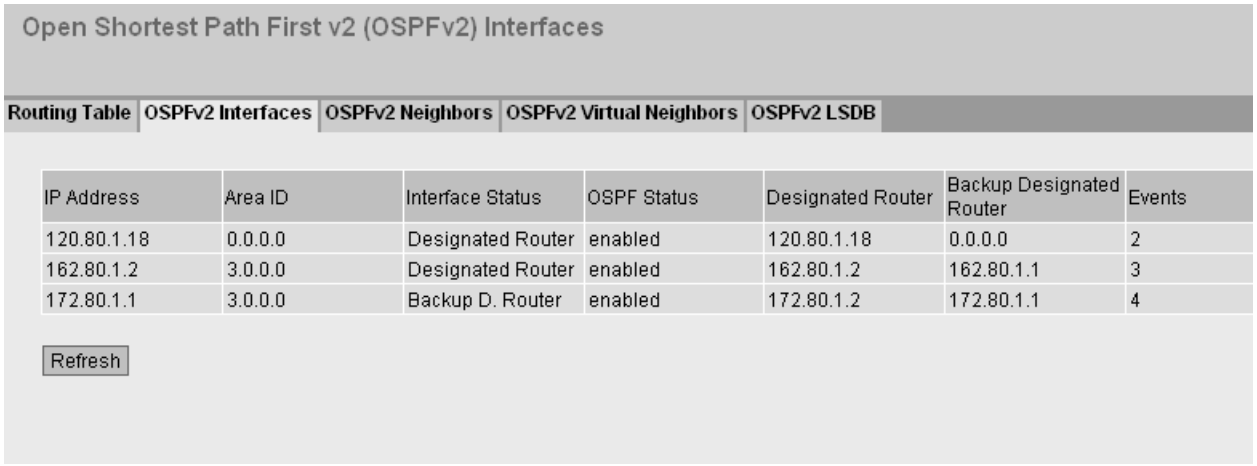
该表格包括以下列：

- **Destination Network**
  显示此路由的目标地址。
- **Subnet Mask**
  显示此路由的子网掩码。
- **Gateway**
  显示此路由的网关。
- **Interface**
  显示此路由的接口。
- **Metric**
  显示路由器的度量。值越大，数据包到达目的地所需的距离越长。
- **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

5.3.12.2 OSPFv2 接口

概述

此页面用于显示 OSPF 接口的组态。



显示值说明

该表格包括以下列：

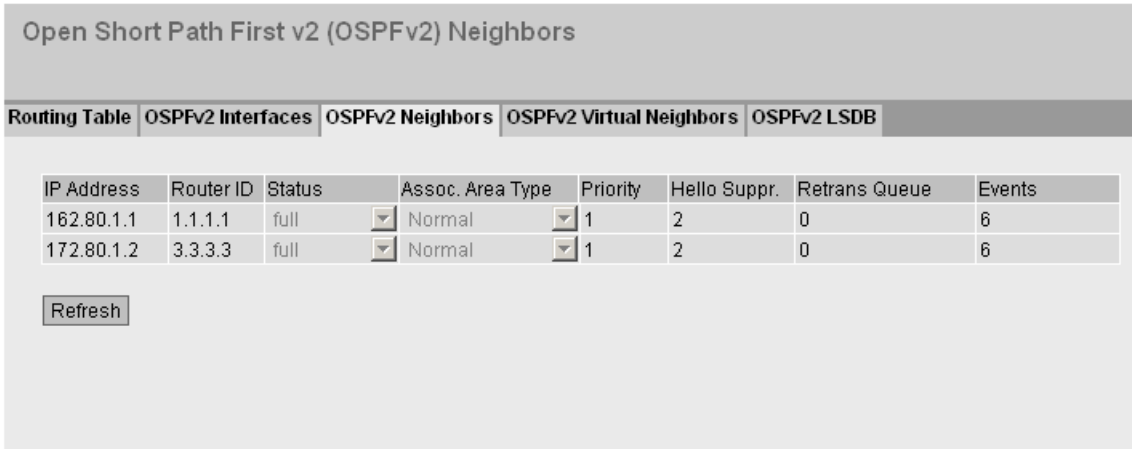
- **“IP 地址”(IP Address)**
  显示 OSPF 接口的 IP 地址
- **“区域 ID”(Area ID)**
  显示 OSPF 接口所属的区域 ID。

- **“接口状态”(Interface Status)**
  显示接口状态：
  - “无效”(Down)
    接口无法使用。
  - “回环”(Loop back)
    回环接口
  - “等待”(Waiting)
    启动并协商接口。
  - “点对点”(Point to Point)
    点对点链路
  - “指定路由器”(Designated Router)
    路由器为指定路由器并生成网络 LSA。
  - “备用指定路由器”(Backup D. Router)
    路由器为指定路由器的备用路由器。
  - “其它指定路由器”(Other D. Router)
    接口已启动。 该路由器既不是指定路由器也不是指定备用路由器。
- **“OSPF 状态”(OSPF Status)**
  显示 OSPF 状态。
  - Enabled： 在接口中启用 OSPF。
  - Disabled： 在接口中禁用 OSPF。
- **“指定路由器”(Designated Router)**
  显示针对该 OSPF 接口指定的路由器的 IP 地址。
- **“备用指定路由器”(Backup Designated Router)**
  显示针对该 OSPF 接口指定的备用路由器的 IP 地址。
- **“事件”(Events)**
  显示 OSPF 状态变化次数。

5.3.12.3 OSPFv2 邻居

概述

该页面用于显示在相关网络中动态检测到的邻近路由器。



显示值说明

该表格包括以下列：

- **IP Address**
  显示该网络中邻居路由器的 IP 地址。
- **Neighbor Router ID**
  显示邻居路由器的 ID。 这两个地址可以相同。

- **Status**
  显示邻居路由器状态。 状态可采用以下值：
  - unknown
    邻居路由器的状态未知。
  - down
    无法访问邻居路由器。
  - attempt and init
    初始化过程中的状态概要
  - two-way
    双向接收呼叫数据包。 指定路由器和指定备份路由器的规范。
  - exchangestart, exchange and loading
    交换 LSA 时的状态
  - full
    数据库在区域中完整并同步。 现在可以检测到路由。

  说明

  标准状态

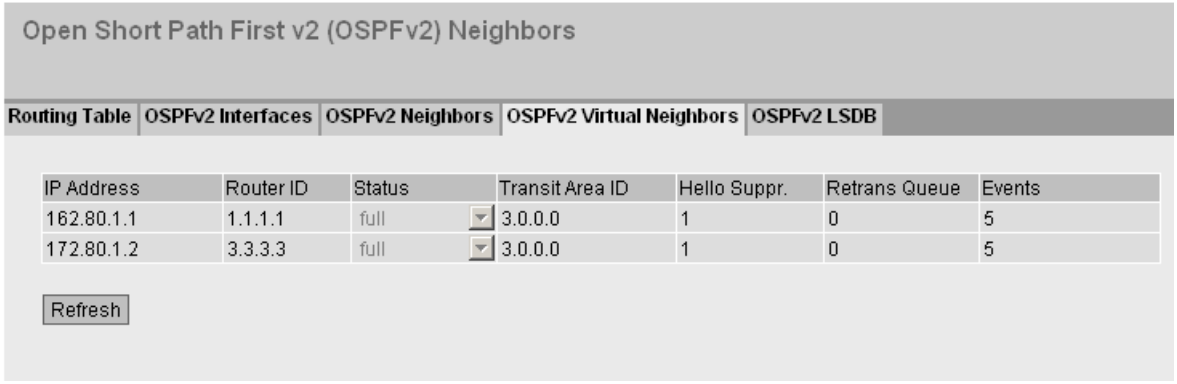
  如果伙伴路由器是指定路由器或指定备用路由器，则状态为“full”。 否则状态为“two-way”。

- **Assoc. Area Type**
  显示用以维持邻居关系的区域类型。 存在以下区域类型：
  - 标准 (Standard)
  - 存根 (Stub)
  - NSSA
  - 骨干
- **Priority**
  显示邻居路由器优先级。 仅在选择网络中的指定路由器时有意义。 该信息与虚拟邻居路由器无关。
- **Hello Suppr.**
  显示发送给邻居路由器的受抑制呼叫数据包。 该字段通常显示“no”。
- **Retrans Queue**
  显示仍要传输的呼叫数据包的队列长度。
- **Events**
  显示状态变化次数。

5.3.12.4 OSPFv2 虚拟邻居

概述

此页面用于显示已组态的虚拟邻居。



显示值说明

该表格包括以下列：

- **IP Address**
  显示该网络中虚拟邻居路由器的 IP 地址。
- **Router ID**
  显示虚拟邻居路由器的路由器 ID。

- **Status**
  显示邻居路由器状态。状态可采用以下值：
  - unknown
    邻居路由器的状态未知。
  - down
    无法访问邻居路由器。
  - attempt and init
    初始化过程中的状态概要
  - two-way
    双向接收呼叫数据包。 指定路由器和指定备份路由器的规范。
  - exchangestart, exchange and loading
    交换 LSA 时的状态
  - full
    数据库在区域中完整并同步。现在可以检测到路由。

  说明

  标准状态

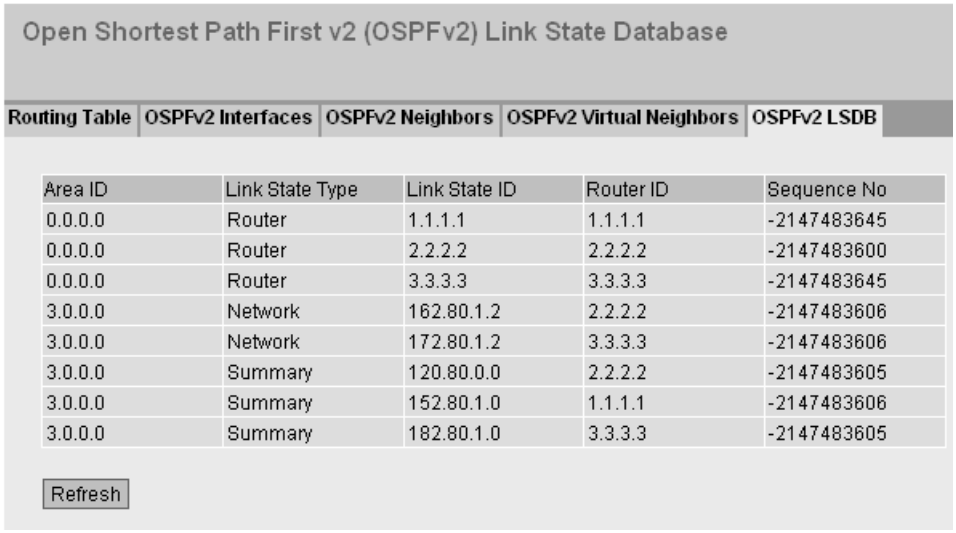
  如果伙伴路由器是指定路由器或指定备用路由器，则状态为“full”。 否则状态为“two-way”。

- **Trans.Area ID**
  显示通过其存在虚拟邻居关系的区域的 ID。
- **Hello Suppr.**
  显示是否有发送给虚拟邻居路由器的受抑制呼叫数据包。
  - no： 没有受抑制呼叫数据包。（默认值）
  - yes： 有受抑制呼叫数据包。
- **Retrans Queue**
  显示仍要传输的呼叫数据包的队列长度。
- **Events**
  显示状态变化次数。

5.3.12.5 OSPFv2 LSDB

概述

链路状态数据库是管理区域内所有链路的中央数据库。 它由链路状态广播 (LSA) 组成。 这些 LSA 中最重要的数据显示在该 WBM 页面中。



显示框说明

该表格包括以下列：

- **Area ID**
  显示 LSA 所属的区域的 ID。 如果 LSA 是外部连接，则显示“-”。
- **Link State Type**
  显示 LSA 类型。 可能的值包括：
  - “未知”(unknown)
    LSA 类型未知。
  - Router
    路由器 LSA（类型 1）在一定区域中由 OSPF 路由器发送。 LSA 包含了所有路由器接口状态方面的信息。
  - Network
    网络 LSA（类型 2）在一定区域中由指定路由器发送。 LSA 包含了连接到网络的路由器的列表。
  - NSSA External
    NSSA 外部 LSA（类型 7）在一定 NSSA 中由 NSSA-ASBR 发送。 NSSA-ASBR 接收类型 5 的 LSA 并将其信息转换为类型 7 的 LSA。NSSA 路由器可以在一定 NSSA 中转发这些 LSA。
  - Summary
    汇总 LSA（类型 3）在一定区域中由 ABR 发送。 LSA 包含了到其它网络的路由的信息。
  - AS Summary
    AS 汇总 LSA（类型 4）在一定区域中由区域边界路由器发送。 LSA 包含了到其它自治系统的路由的信息。
  - AS External
    AS 外部 LSA（类型 5）在自治系统中由 AS 边界路由器发送。 LSA 包含了从一个网络到另一个网络路由器的信息。
- **Link State ID**
  显示 LSA 的 ID。
- **Router ID**
  显示发送此 LSA 的路由器 ID。
- **Sequence No.**
  显示 LSA 的顺序号。 每次更新 LSA 后，该顺序号就会加一。

5.3.12.6 RIPv2 Statistics

概述

此页面用于显示 RIP 接口的统计信息。

显示值说明

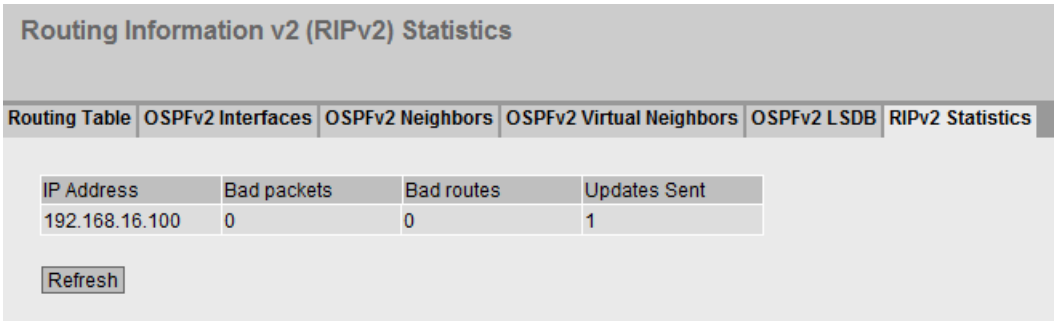


图 5-7 RIPv2 统计信息

该表格包括以下列：

- **IP Address**
  显示 RIPv2 接口的 IP 地址
- **Bad packets**
  接收到的 RIP 数据包中被删除以及因此被忽略的数据包数。
- **Bad routes**
  无法考虑到的有效 RIP 数据包的路由数。
- **Updates Sent**
  显示路由器将其路由表发送给邻居路由器的频率。

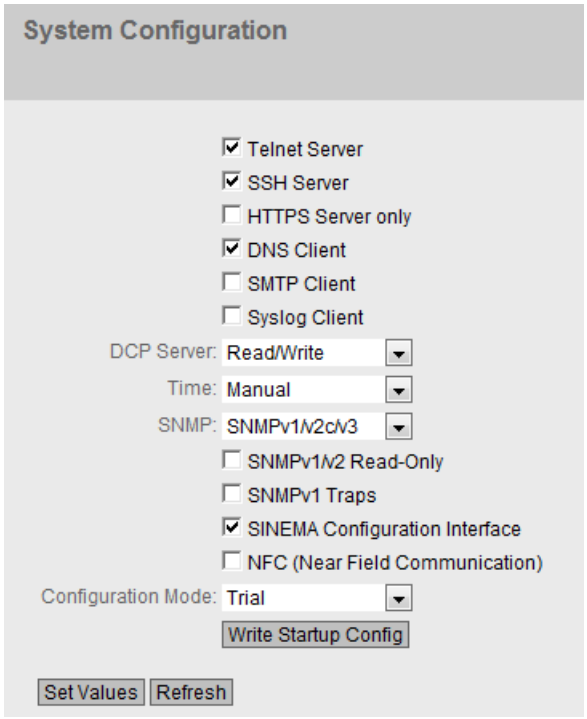
5.4 “System”菜单

5.4.1 组态

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 Server**
  启用或禁用“Telnet 服务器”(Telnet Server) 服务，以便不加密访问 CLI。
- **SSH Server**
  启用或禁用“SSH 服务器”(SSH Server) 服务，以便加密访问 CLI。
- **HTTPS Server only**
  启用此功能后，只能通过 HTTPS 访问设备。

- **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 Client**
  启用或禁用 SMTP 客户端。 可以在“System > SMTP Client”中组态其它设置。
- **Syslog Client**
  启用或禁用 Syslog 客户端。 可以在“System > Syslog Client”中组态其它设置。
- **DCP Server**
  指定是否可用 DCP（Discovery and Configuration Protocol，发现和组态协议）访问设备：
  - “-”（已禁用）
    DCP 已禁用。 既不能读取也不能修改设备参数。
  - Read/Write
    通过 DCP，既可读取又可修改设备参数。
  - Read-Only
    通过 DCP，可读取但不能修改设备参数。
- **Time**
  从下拉列表中选择设置。 可能的设置如下：
  - Manual
    手动设置系统时间。 可以在“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“System > System Time > SIMATIC Time Client”中组态其它设置。
  - 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 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 Client （仅适用于 SCALANCE XR-500）
    通过 PTP 服务器设置系统时间。 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。 可能的设置如下：
  - “-”（SNMP 已禁用）
    不能通过 SNMP 访问设备参数。
  - SNMPv1/v2c/v3
    可以通过 SNMP 版本 1、2c 或 3 访问设备参数。可以在“系统 > SNMP > 常规” (System > SNMP > General) 中组态其它设置。
  - SNMPv3
    可以通过 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 Read-Only**
  启用或禁用通过 SNMPv1/v2c 对 SNMP 变量进行写访问。
- **SNMPv1 Traps**
  启用或禁用发送陷阱（报警帧）。 可以在“System > SNMP > Traps”中组态其它设置。
- **SINEMA Configuration Interface**
  如果启用了 SINEMA 组态接口，可通过 TIA Portal 将组态下载到工业以太网交换机中。
- **NFC** （仅适用于 SCALANCE XM-400）
  激活或取消激活“NFC”（近场通信）功能。
  有关 NFC 的详细信息，请参见“SCALANCE XM400”操作说明。
- **Configuration Mode**
  从下拉列表中选择模式。 可能的模式如下：
  - Automatic Save
    自动保存模式。 在最后修改参数的约 1 分钟后或重启设备时，自动保存组态。
  - 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，需使用“Write Startup Config”按钮。 设置了试用模式时会显示“Write Startup Config”按钮。 只要存在未保存的更改，消息“Trial Mode Active – Press "Write Startup Config" button to make your settings persistent”就还会在显示区域中显示。 可以在每个 WBM 页面上看到这条消息，直至所做的更改已保存或设备已重启。

组态步骤

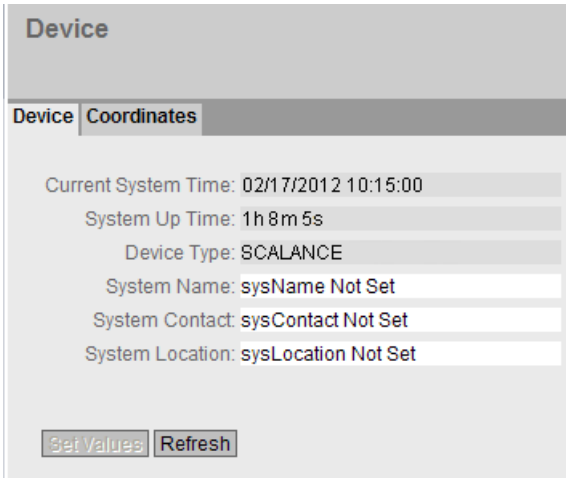
1. 要使用所需功能，请选中相应的复选框。
2. 从下拉列表中选择所需选项。
3. 单击“Set Values”按钮。

5.4.2 概述

5.4.2.1 设备

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**
  显示设备类型。 （只读）
- **“系统名称”(System Name) 输入框**
  可输入设备的名称。 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。

- **“系统联系人”(System Contact) 输入框**
  可输入设备管理责任人的名字。 最多支持 255 个字符。
- **“系统位置”(System Location) 输入框**
  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。

“系统名称”(System Name)、**“系统联系人”(System Contact)** 和 **“系统位置”(System Location)** 框中不允许使用“**<**”“**>**”和“空格”字符开头与结束。

步骤

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

5.4.2.2 坐标

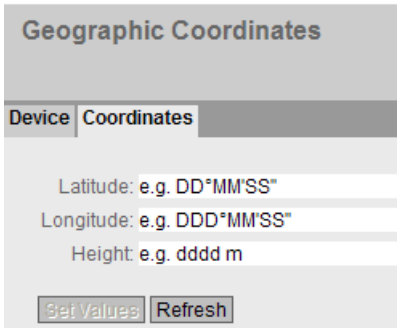
有关地理坐标的信息

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

获取坐标

使用适当的地图来获取设备的地理坐标。

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



说明

该页面包含以下框。 这些是最多可包含 32 个字符的纯信息框。

- **“Latitude”输入框**
  地理纬度： 在此输入设备位置的北纬值或南纬值。
  例如，值 +49° 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”**
  地理高度： 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表示。

步骤

1. 在“Latitude”输入框中输入纬度。
2. 在“Longitude”输入框中输入经度。
3. 在“Height”输入框中输入高度。
4. 单击“Set Values”按钮。

5.4.3 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“Layer 3”菜单中的“Subnets Configuration”菜单项以及其中的 TIA 接口组态。

5.4.4 DNS

DNS 服务器（域名系统）可将域名分配给某个 IP 地址，以便唯一标识设备。

如果启用此功能，工业以太网交换机可以作为 DNS 客户端与 DNS 服务器通信。

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

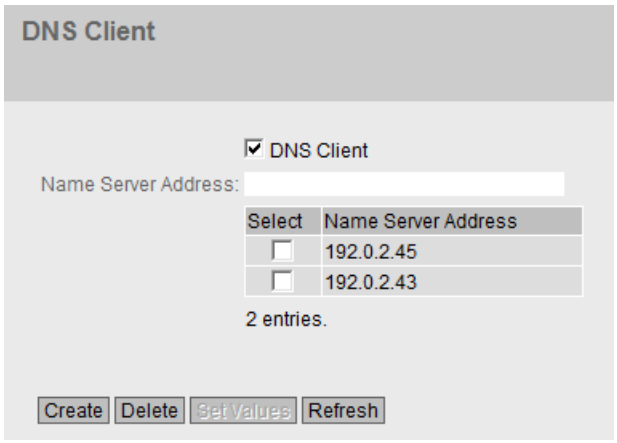


图 5-8 DNS 客户端

该页面包含以下框：

- **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。
- **Name Server Address**
  输入 DNS 服务器的 IP 地址。

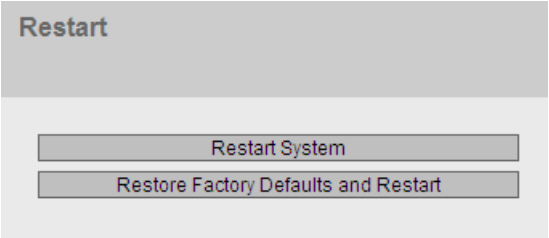
该表包含以下各列：

- **Select**
  选中要删除的行中的复选框。
- **Name Server Address**
  显示 DNS 服务器的 IP 地址。

5.4.5 重启

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，以及用于复位到设备默认值的选项。



说明

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。
- 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。 如果设备处于“试用模式”，则必须在重启之前手动保存组态修改。 在“自动保存模式”下，会在设备重启之前自动保存最后的更改。

显示框说明

为重启设备，该页面上的按钮提供了以下选项：

- **“重启系统”(Restart System) 按钮**
  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。 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。 然后需要再次登录。
- **“恢复出厂默认设置并重启”(Restore Factory Defaults and Restart) 按钮**
  单击此按钮可以恢复组态的出厂默认设置。 同时会复位受保护的默认设置。
  将触发自动重启。

  说明

  将所有默认设置复位为出厂设置时，IP 地址和密码均会丢失。 之后，只能通过 Primary Setup Tool 或 DHCP 访问设备。
  在特定连接情况下，之前已正确组态的设备可能会引起数据帧循环传送，从而导致数据通信故障。

5.4.6 加载和保存

5.4.6.1 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 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

与先前版本的不兼容性

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。

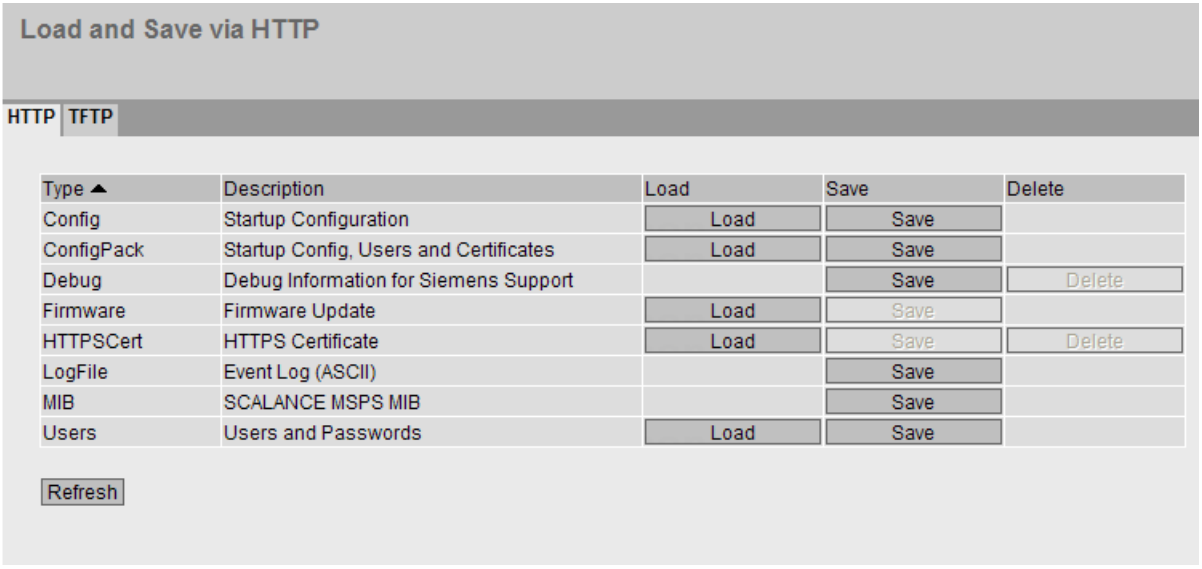
插入的 PLUG 组态与先前版本不兼容

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了 PLUG，则重启后，由于 PLUG 仍具有之前最新固件的组态数据，因此状态为“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“系统 > PLUG”(System > PLUG) 手动删除或重写 PLUG。

说明

组态文件和试用模式/自动保存模式

在自动保存模式下，组态文件（ConfigPack 和 Config）传输前数据会自动保存。
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（ConfigPack 和 Config）中。 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。



显示框说明

该表格包括以下列：

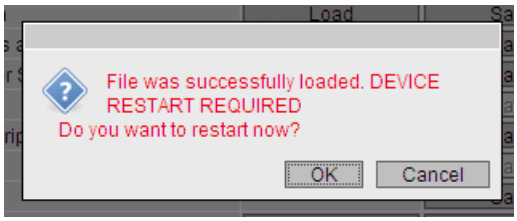
- **Type**
  显示文件类型。
- **Description**
  显示文件类型的简要说明。
- **Load**
  可以使用此按钮将文件上传到设备。 如果文件类型支持该功能，将启用该按钮。
- **Save**
  可以使用此按钮保存设备中的文件。 仅当文件类型支持该功能且文件存在于设备上时，才会启用该按钮。
- **Delete**
  可以使用此按钮删除设备中的文件。 仅当文件类型支持该功能且文件存在于设备上时，才会启用该按钮。
- **是 (Yes)**
  启动操作
- **否 (No)**
  放弃操作。

说明

更新固件之后，请删除 Web 浏览器的缓存。

加载新固件

成功下载固件后，系统将要求您重启设备。



请重启设备并继续组态新启动的固件。

组态步骤

使用 HTTP 加载文件

1. 单击“Load”按钮之一启动加载功能。
   将打开用于上传文件的对话框。
2. 转至要上传的文件。
3. 单击对话框中的“打开”(Open) 按钮。
   随即可上传文件。
4. 当出现消息“需要重启”(restart required) 时，请单击“是”(OK) 按钮触发重启。 如果单击“取消”(Cancel) 按钮，设备将不会重启。 所做的更改只在重启后生效。

使用 HTTP 保存文件

1. 单击“Save”按钮之一启动保存功能。
2. 系统将提示您选择存储位置和文件名称。 或者可以接受推荐的文件名。 若要进行选择，请使用浏览器中的对话框。 进行选择之后，单击“Save”按钮。

使用 HTTP 删除文件

1. 单击“Delete”按钮之一启动删除功能。
   文件将被删除。

复用组态数据

如果多台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组态过程。

要复用组态数据，请按以下步骤操作：

1. 将已组态设备的组态数据保存在 PC 上。
2. 按这种方式将该组态文件下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。

请注意，在保存组态数据时会对其进行编码。 这意味着无法使用文本编辑器对这些文件进行编辑。

5.4.6.2 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 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，您也可以通过位于客户端 PC 上的文件加载新固件等。

说明

与先前版本的不兼容性

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。

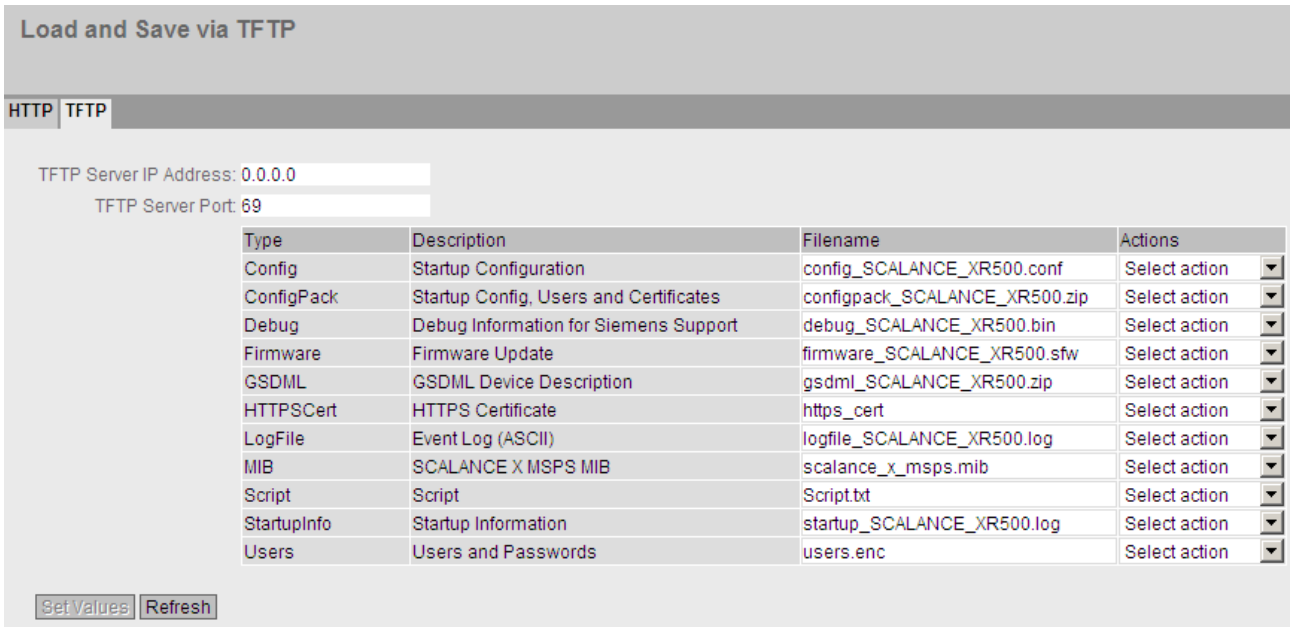
插入的 PLUG 组态与先前版本不兼容

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了 PLUG，则重启后，由于 PLUG 仍具有之前最新固件的组态数据，因此状态为“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“系统 > PLUG”(System > PLUG) 手动删除或重写 PLUG。

说明

组态文件和试用模式/自动保存模式

在自动保存模式下，组态文件（ConfigPack 和 Config）传输前数据会自动保存。
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（ConfigPack 和 Config）中。 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。



显示框说明

该页面包含以下框：

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

该表格包括以下列：

- **Type**
  显示文件类型。
- **Description**
  显示文件类型的简要说明。
- **“文件名”(Filename) 输入框**
  在这里为每种文件类型预设一个文件名。

说明

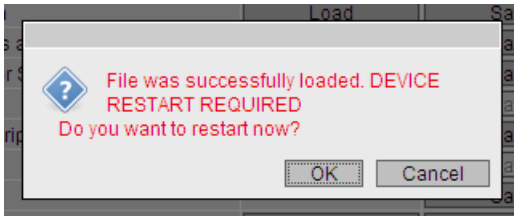
更改文件名

可以更改此列中预设的文件名。 单击“设置值”(Set Values) 按钮后，更改的文件名会存储在设备上，并可用于命令行接口。

- **“操作”(Actions) 下拉列表**
  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。 相关选项如下：
  - **Save file**
    通过该选项将文件保存到 TFTP 服务器上。
  - **Load file**
    通过该选项加载 TFTP 服务器中的文件。
- **“是”(Yes) 按钮**
  执行请求的操作。
- **“否”(No) 按钮**
  不执行请求的操作

加载新固件

成功下载固件后，系统将要求您重启设备。



请重启设备并继续组态新启动的固件。

组态步骤

通过 TFTP 加载或保存数据

1. 在“TFTP Server IP Address”输入框中输入 TFTP 服务器的 IP 地址。
2. 在“TFTP Server Port”输入框中输入要使用的服务器端口。
3. 在“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“Actions”下拉列表中选择要执行的操作。
5. 单击“Set Values”按钮启动所选操作。
6. 出现消息“需要重启”(restart required) 时，请单击“是”(OK) 按钮触发设备重启。 如果单击“取消”(Cancel) 按钮，则不会重启。 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组态过程。

要复用组态数据，请按以下步骤操作：

1. 将已组态设备的组态数据保存在 PC 上。
2. 按这种方式将该组态文件下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。

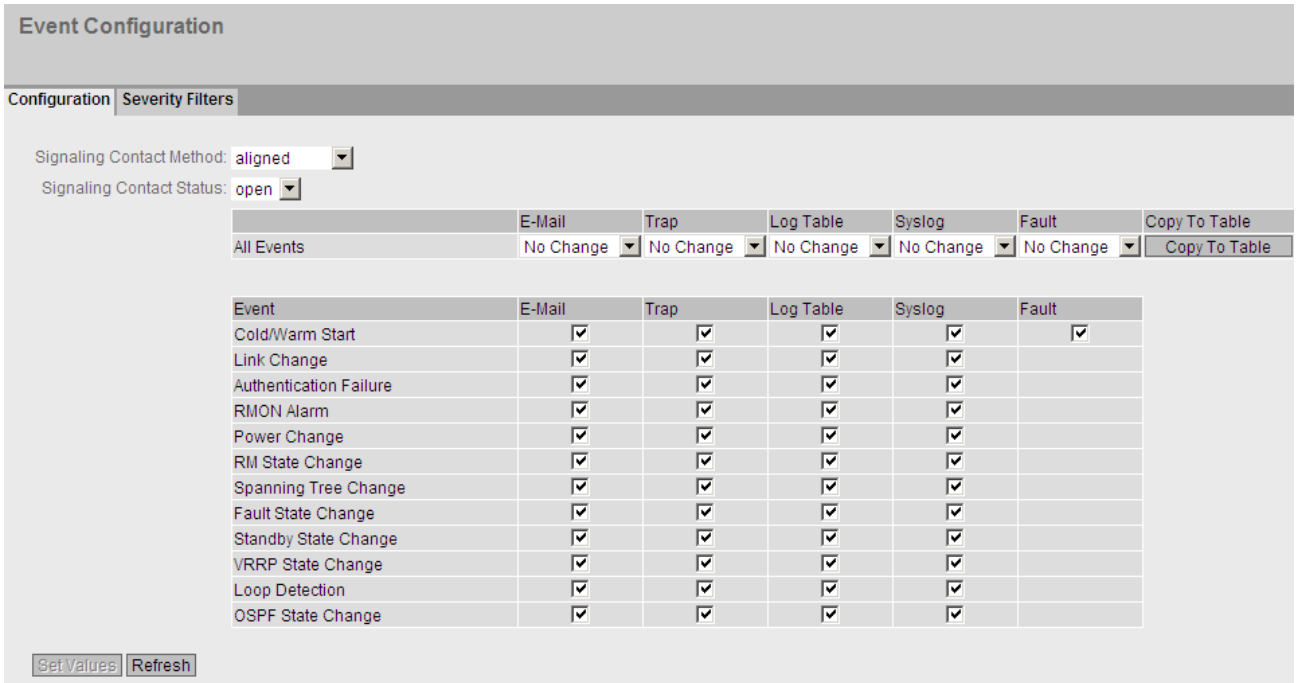
请注意，在保存组态数据时会对其进行编码。 这意味着无法使用文本编辑器对这些文件进行编辑。

5.4.7 事件

5.4.7.1 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。 通过启用相应的选项，指定设备对事件的响应方式。 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) 下拉列表**
  从下拉列表中选择信号触点反应。 可能的响应包括：
  - “传统”(conventional)
    默认的信号触点设置。 由故障 LED 显示错误/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”(aligned)
    信号触点的工作方式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) 下拉列表**
  从下拉列表中选择信号触点的状态。 可能的状态有：
  - “闭合”(close)
    信号触点闭合。
  - “断开”(open)
    信号触点断开。

该表格包括以下列：

- **“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 client”功能时，该功能才可用。
- **“陷阱”(Trap)**
  设备发送 SNMP 陷阱。 仅当已在“System > Configuration”中启用 SNMPv1 Traps 时，该功能才可用。
- **“日志表”(Log Table)**
  设备在事件日志表中写入一个条目，请参阅“信息 > 日志表”(Information > Log Table)
- **Syslog**
  设备将一个条目写入系统日志服务器。 仅当已设置系统日志服务器并已启用“Syslog client”功能时，该功能才可用。

- **“故障”(Fault)**
  设备触发故障。 错误 LED 亮起
- **“事件”(Event)**
  “事件”(Event) 列包含以下值：
  - “冷/暖启动”(Cold/Warm Start)
    用户打开或重启设备。
  - “链路变化”(Link Change)
    仅当对接口状态进行监视和更改时才会发生该事件，请参阅“系统 > 故障监视 > 链路变化”(System > Fault Monitoring > Link Change)。
  - “验证失败”(Authentication Failure)
    当试图用错误的密码访问时才会发生该事件。
  - “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。 表明线路 1 或线路 2 有改变，请参阅“系统 > 故障监视 > 电源”(System > Fault Monitoring > Power Supply)。
  - “STP/RSTP/MSTP 变化”(STP/RSTP/MSTP Change)
    STP、RSTP 或 MSTP 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。
  - “RMON 报警”(RMON Alarm)
    发生了与系统远程监视相关的报警或事件。
  - “VRRP 状态变化”(VRRP State Change)（仅限通过 VRRP 进行路由选择时）
    虚拟路由器的状态发生变化。
  - “回路检测”(Loop Detection)
    在网段中检测到回路。
  - “OSPF 状态变化”(OSPF State Change)
    OSPF 的状态已发生变化。

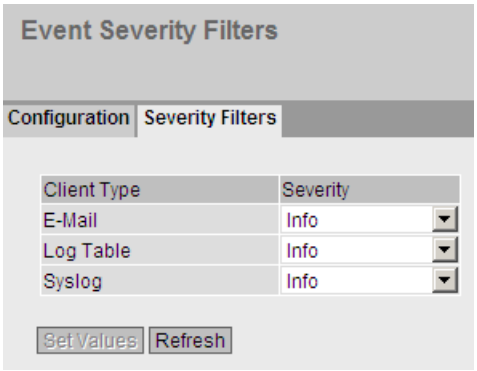
组态步骤

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
   - 陷阱
   - 日志表
   - Syslog
   - 故障
2. 单击“设置值”(Set Values) 按钮。

5.4.7.2 严重程度过滤器

设置严重程度过滤器

在此页面上，设置发送系统事件通知的阈值级别。



表格首列显示了要进行设置的客户端类型：

- **E-Mail**
  通过电子邮件发送系统事件消息
- **Log Table**
  在日志表中输入系统事件
- **Syslog**
  在 Syslog 文件中输入系统事件

从表格第二列的下拉列表中选择所需等级。

您可以从以下值中选择：

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

步骤

按以下步骤组态所需级别：

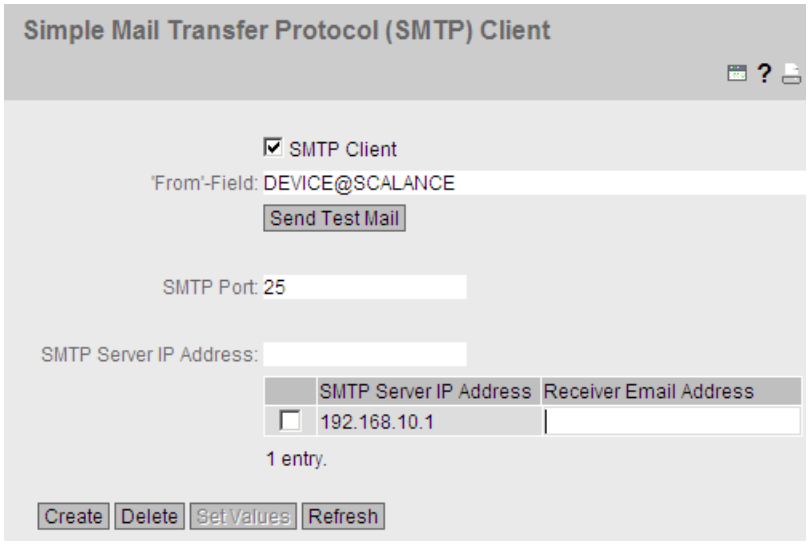
1. 组态客户端类型后，从表格第二列的下拉列表中选择所需值。
2. 单击“Set Values”按钮。

5.4.8 SMTP 客户端

通过电子邮件进行网络监视

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

在此页可组态最多三个 SMTP 服务器和相应的电子邮件地址。



说明

该页面包含以下框：

- **“SMTP Client”复选框**
  启用或禁用 SMTP 客户端。
- **“'From'-Field”输入框**
  输入电子邮件中的发送方名称，如设备名称。
- **“SMTP Port”输入框**
  如果不能通过端口 25 访问 SMTP 服务器，则更改端口。

- **“SMTP Server IP Address”输入框**
  输入 SMTP 服务器的 IP 地址。
- **“Send Test Mail”按钮**
  发送用于测试的电子邮件。

该表包含以下各列：

- **第 1 列**
  选中要删除的行中的复选框。
- **SMTP Server IP Address**
  显示 SMTP 服务器的 IP 地址。
- **Receiver Email Address**
  输入电子邮件地址，发生故障时，设备会将电子邮件发送到该地址。 电子邮件地址可以是个人地址或分配列表地址。

步骤

1. 启用“SMTP Client”选项。
2. 在“SMTP Server IP Address”输入框中输入 NTP 服务器的 IP 地址。
3. 单击“Create”按钮。 会在表中生成一个新条目。
4. 在“Receiver Email Address”输入框中，输入电子邮件地址，发生故障时，设备会将电子邮件发送到该地址。
5. 单击“Set Values”按钮。

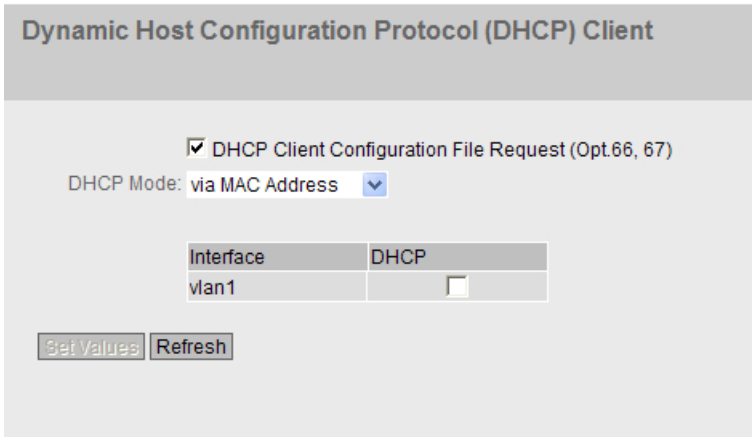
说明

根据 SMTP 服务器属性和组态，可能需要针对电子邮件修改“'From'-Field”框。 请与 SMTP 服务器的管理员联系。

5.4.9 DHCP 客户端

设置 DHCP 模式

如果激活 DHCP 模式，则 DHCP 客户端会向组态的 DHCP 服务器发出 DHCP 请求，然后服务器会为其分配 IP 地址以进行响应。 服务器管理一个地址范围，并且分配该范围内的 IP 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 IP 地址。



说明

该页面包含以下框：

- **“DHCP Client Config File Request (Opt.66, 67)”复选框**
  如果想要 DHCP 客户机使用选项 66 和 67 下载并随后启用某个组态文件，则选择此选项。
- **“DHCP Mode”下拉列表**
  从下拉列表中选择 DHCP 模式。 可能的模式如下：
  - via MAC Address
    基于该 MAC 地址进行识别。
  - via DHCP Client ID
    基于自由定义的 DHCP 客户端 ID 进行识别。
  - 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。
- **“DHCP”复选框**
  为相关 IP 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. 启用“DHCP Client”选项。
2. 从“DHCP Mode”下拉列表中选择 DHCP 模式“via DHCP Client ID”。
3. 在启用的“DHCP Client ID”输入框中输入字符串来识别设备。 DHCP 服务器随即会评估该字符串。
4. 如果希望 DHCP 客户端使用选项 66 和 67 下载并随后启用某个组态文件，请选择“Client Config File Request (Opt.66, 67)”选项。
5. 单击“Set Values”按钮。

说明

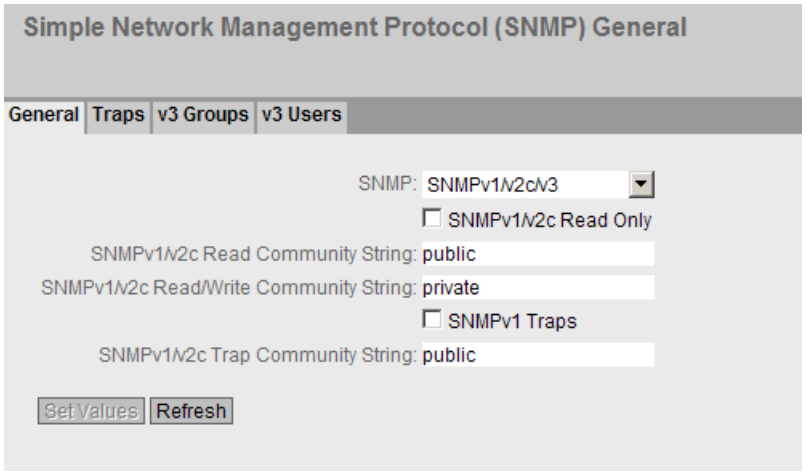
如果下载组态文件，这会触发系统重启。 确保该组态文件中不再设置选项“Client Config File Request (Opt.66, 67)”。

5.4.10 SNMP

5.4.10.1 概述

SNMP 组态

在该页面对 SNMP 进行基本设置。 根据希望应用的功能启用相应的复选框。



说明

该页面包含以下框：

- **“SNMPv1/v2c/v3”下拉列表**
  从下拉列表中选择 SNMP 协议。 可能的设置如下：
  - “-”（禁用）
    禁用 SNMP。
  - SNMPv1/v2c/v3
    支持 SNMPv1/v2c/v3。
  - SNMPv3
    仅支持 SNMPv3。
- **“SNMPv1/v2c Read Only”复选框**
  如果启用此选项，则 SNMPv1/v2c 仅可读取 SNMP 变量。

  说明

  团体字符串

  由于安全考虑，请勿使用标准值“public”或“private”。 请在初始安装之后更改团体字符串。
- **“SNMPv1/v2c Read/Write Community String”输入框**
  输入 SNMP 协议的读写访问团体字符串。
- **“SNMPv1/v2c Read Community String”输入框**
  输入 SNMP 协议的访问团体字符串。
- **“SNMPv1 Traps”**复选框
  启用或禁用发送陷阱（报警帧）。 在“Trap”选项卡上，指定 SNMP 陷阱将发送到的设备的 IP 地址。
- **“SNMPv1/v2c Trap Community String”输入框**
  输入用于发送 SNMPv1/v2 消息的团体字符串。

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，请启用“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. 单击“Set Values”按钮。

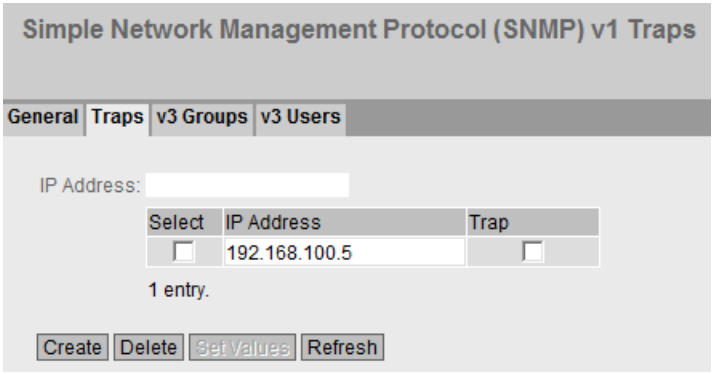
5.4.10.2 Traps

报警事件的 SNMP 陷阱

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

说明

仅当在“General”或“System > Confguration”选项卡中选择了“SNMPv1 Traps”选项时，才会发送陷阱。



说明

- **IP Address**
  输入设备发送 SNMP 陷阱的目标站 IP 地址。 最多可指定十个不同的 IP 地址作为不同的接收方。

该表格包括以下列：

- **Select**
  选择要删除的行。
- **IP Address**
  如有必要，请更改站的 IP 地址。
- **Trap**
  启用或禁止发送陷阱。 已输入但未选择的工作站不会接收 SNMP 陷阱。

步骤

创建陷阱条目

1. 在“IP Address”中，输入设备发送 SNMP 陷阱的目标站 IP 地址。
2. 单击“Create”按钮以创建新的陷阱条目。
3. 选择相应 IP 地址的复选框。
4. 单击“Set Values”按钮。

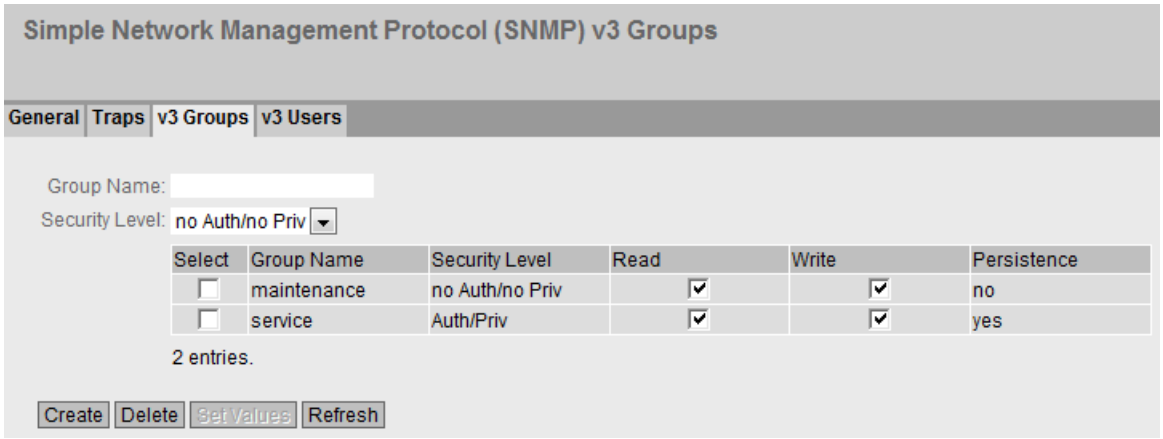
删除陷阱条目

1. 选中要删除的行中的复选框。
2. 单击“Delete”按钮。 删除了相关条目。

5.4.10.3 组

安全设置和权限分配

SNMP 版本 3 允许在协议级分配权限，以及身份验证和加密。 安全等级和读/写权限按照组来分配。 这些设置会自动应用到组内的每个成员。



说明

该页面包含以下框：

- **Group Name**
  输入组的名称。 最大长度为 32 个字符。
- **Security Level**
  为所选组选择有效的
  安全等级（验证、加密）。 在安全等级中，有如下选项：
  - No Auth/no Priv
    未启用验证，未启用加密。
  - Auth/no Priv
    已启用验证/未启用加密。
  - Auth/Priv
    已启用验证/已启用加密。

该表格包括以下列：

- **Select**
  选择要删除的行。
- **Group Name**
  显示定义的组名称。
- **Security Level**
  显示组态的安全等级。
- **Read**
  启用或禁用所需组的读访问。
- **Write**
  启用或禁用所需组的写访问。

  说明

  要实现写访问，还需启用读访问。

- **Persistence**
  显示组是否已分配至 SNMPv3 用户。如果组未分配至 SNMPv3 用户，则不会触发自动保存，并且在重启设备之后已组态的组会再次消失。
  - Yes
    组已分配至 SNMPV3 用户。
  - No
    组未分配至 SNMPV3 用户。

步骤

创建新组

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

修改组

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

说明

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

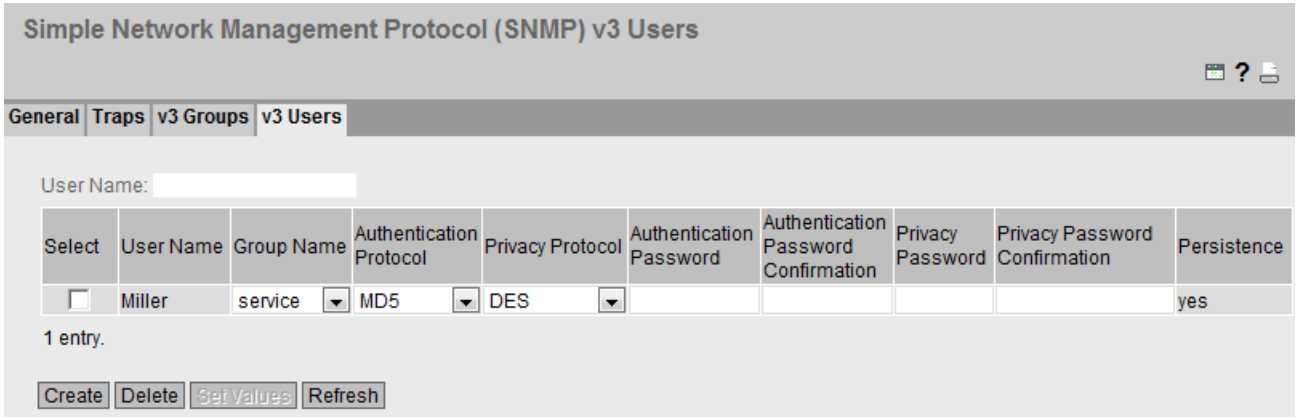
删除组

1. 选中要删除的行中的复选框。
   对所有要删除的组重复此步骤。
2. 单击“Delete”按钮。 将删除相关条目。

5.4.10.4 用户

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。

该表格包括以下列：

- **Select**
  选择要删除的行。
- **User Name**
  显示已创建的用户。
- **Group Name**
  选择待分配用户的组。
- **Authentication Protocol**
  指定验证协议。 仅当该组支持此功能时才能启用。
  可使用以下设置：
  - 无
  - MD5
  - SHA

- **Privacy Protocol**
  指定用户是否使用 DES 算法。 仅当该组支持此功能时才能启用。
- **Authentication Password**
  在第一个输入框中输入验证密码。 该密码必须至少 6 个字符，最多 32 个字符。
- **Authentication Password Confirmation**
  重复输入以确认密码。
- **Privacy Password**
  输入加密密码。 该密码必须至少 6 个字符，最多 32 个字符。
- **Privacy Password Confirmation**
  重复输入以确认加密密码。
- **Persistence**
  显示用户是否已分配至 SNMPv3 组。如果用户未分配至 SNMPv3 组，则不会触发自动保存，并且在重启设备之后已组态的用户会再次消失。
  - Yes
    用户已分配至 SNMPV3 组。
  - No
    用户未分配至 SNMPV3 组。

步骤

创建新用户

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

删除用户

1. 选中要删除的行中的复选框。
   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。

说明

如果在执行该步骤之前单击其它按钮（例如，“Refresh”按钮），则将取消删除操作。 将保留所选行的数据。 同时会取消选择内容。 如果要重复此操作，则必须重新选择要删除的数据记录。

5.4.11 系统时间

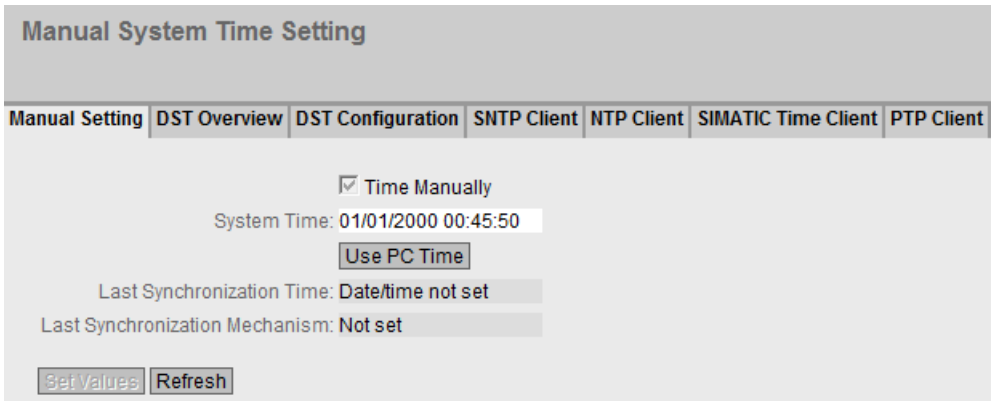
可以采用不同的方法来设置设备的系统时间。 每次只能采用一种方法。

激活一种方法后，将自动禁止之前激活的方法。

5.4.11.1 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**
  启用或禁用手动设置时间。 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。
  重启之后，时钟从 01/01/2000 00:00:00 开始
- **Use PC Time**
  单击该按钮使用 PC 的时间设置。
- **Last Synchronization Time**
  该框为只读，显示上次进行时钟同步时的时间。 如果无法进行时钟同步，该框会显示“Date/time not set”。
- **Last Synchronization Mechanism**
  该框显示上次时钟同步是如何执行的。
  - Not set
    尚未设置系统时间。
  - 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

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”。

5.4.11.2 DST Overview

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

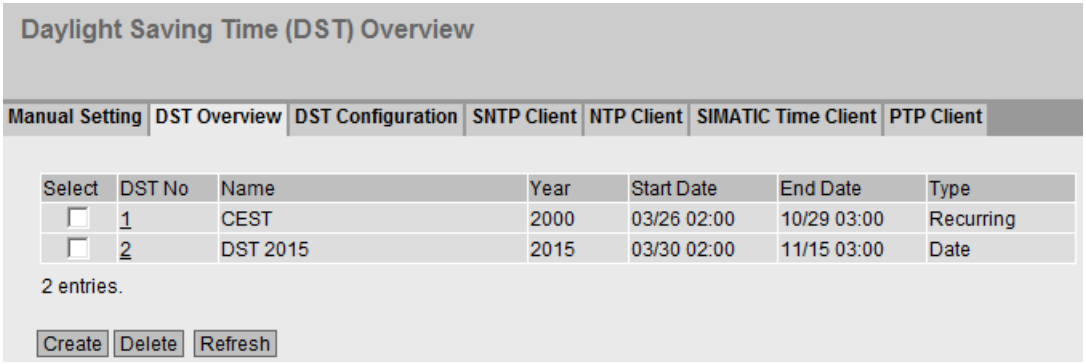


图 5-9 DST 概述

- **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。
- **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。
  - Recurring
    定义夏令时切换的规则。

5.4.11.3 DST Configuration

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

可定义夏令时切换规则，也可指定固定日期。

设置

说明

此页面包含的内容取决于您在“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**
  选择如何进行夏令时切换：
  - 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。
  - 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。

选择“Date”时的设置

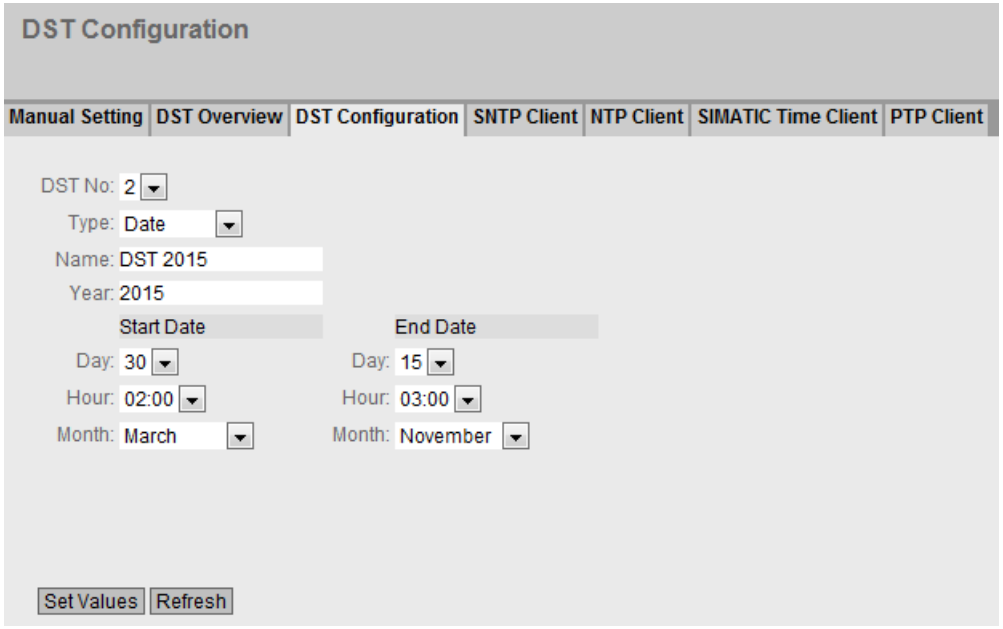


图 5-10　　DST 组态日期

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：
  - 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：
  - Day
    指定日期。
  - Hour
    指定小时。
  - Month
    指定月份。

选择“Recurring”时的设置

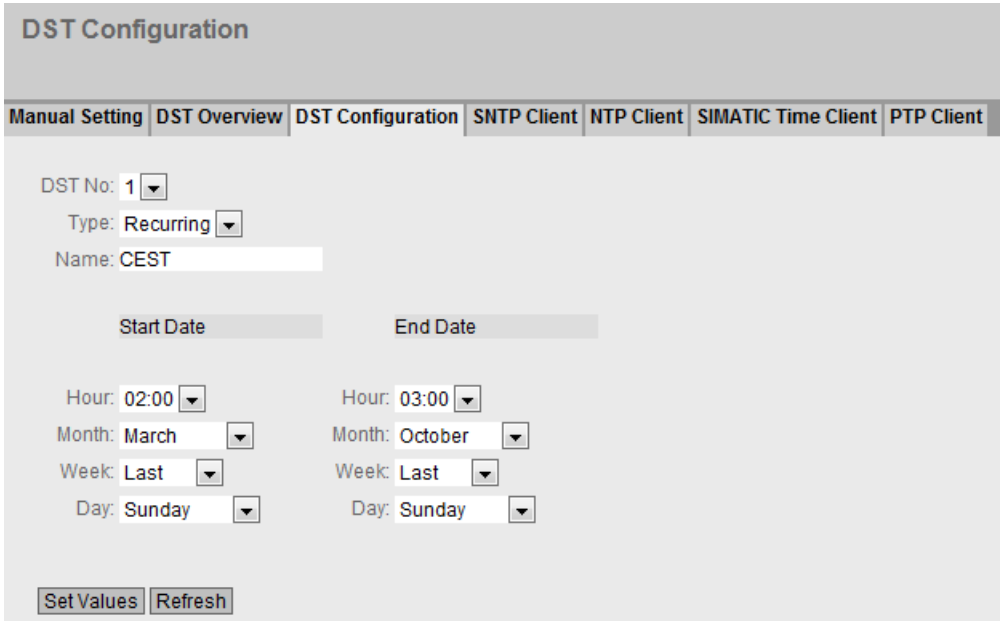


图 5-11 DST 组态重复

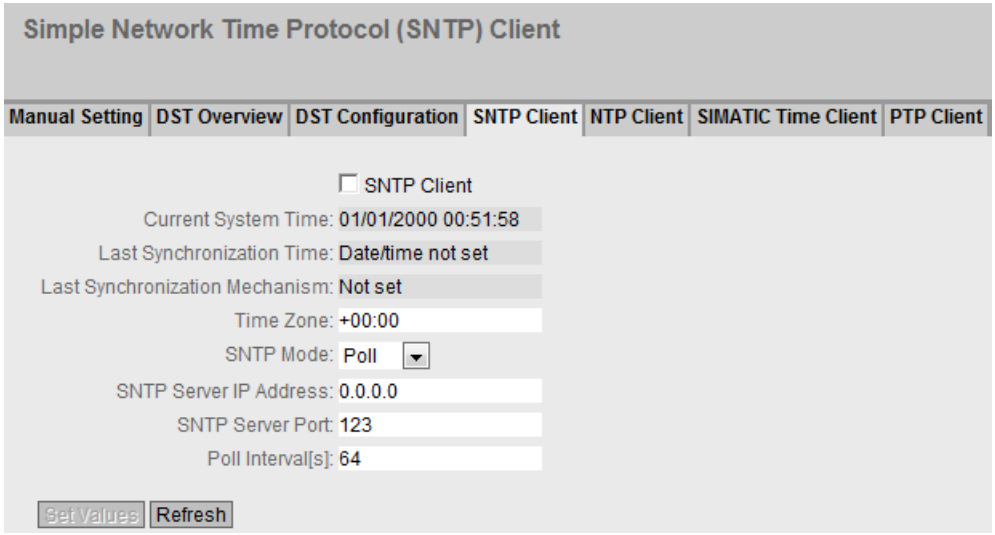
可以创建夏令时切换规则。

- **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 5 周或最后一周。
  - Weekday
    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 5 周或最后一周。
  - Weekday
    指定工作日。

5.4.11.4 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适当的帧。



说明

该页面包含以下框：

- **SNTP Client**
  使用 SNTP 启用或禁用自动时钟同步。
- **Current System Time**
  显示系统中当前设置的日期和时间值。
- **Last Synchronization Time**
  该框为只读，显示上次进行时钟同步时的时间。

- **Last Synchronization Mechanism**
  该框显示上次时钟同步是如何执行的。 可能的方法如下：
  - Not set
    尚未设置系统时间。
  - 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**
  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。在此框中通过指定时间偏移量将夏令时和标准时间的设置考虑在内。
- **SNTP Mode**
  从下拉列表中选择同步模式。 可以使用下列同步类型：
  - Poll
    如果选择该协议类型，则会显示输入框“SNTP Server IP Address”、“SNTP Server Port”和“Poll Interval(s)”以便进一步组态。 若使用该同步类型，设备会激活，并向 SNTP 服务器发送时间查询。
  - Listen
    若使用该同步类型，设备不会激活，但会“侦听”传递时钟的 SNTP 帧。
- **SNTP Server IP Address**
  输入 SNTP 服务器的 IP 地址。
- **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
- **Poll Interval(s)**
  在此输入两次时间查询间的时间间隔。 在此框中输入查询间隔的秒数值。 可能的值介于 16 到 16284 秒之间。

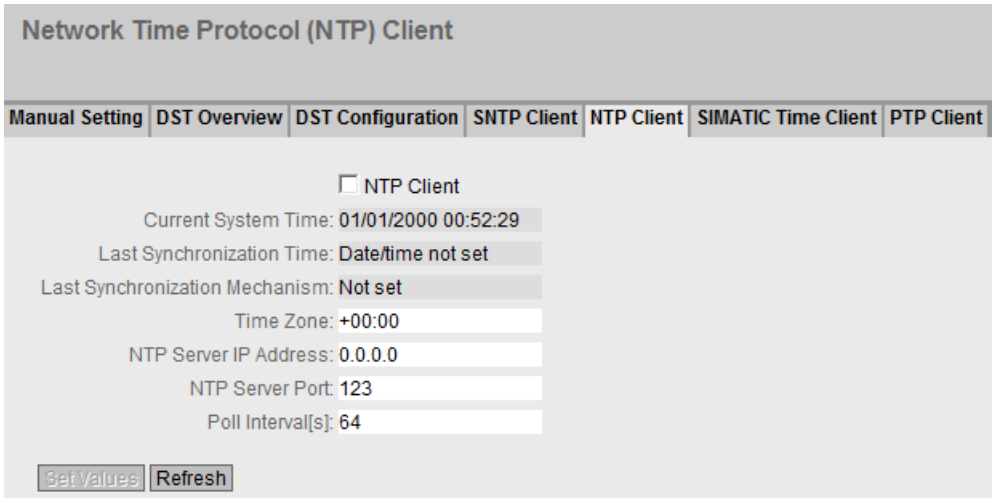
步骤

1. 单击“SNTP 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）。 该时间随后会被重新计算并根据指定的时区显示为当地时间。 在设备本身不会将夏令时转换为标准时间。 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）
     - 时间服务器（第 4 步）
     - 端口（第 5 步）
     - 查询间隔（第 6 步）
     - 通过第 7 步完成组态。
   - Listen
     对于该模式，需要组态以下内容：
     - 与服务器发送的时间之间的时差（第 2 步）
     - 通过第 7 步完成组态。
4. 在“SNTP Server IP Address”输入框中，输入 SNTP 服务器的 IP 地址，将使用该服务器的帧同步时钟。
5. 在“SNTP Server Port”输入框中，输入可用来使用 SNTP 服务器的端口。 仅当输入 SNTP 服务器的 IP 地址之后，才可以修改该端口。
6. 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，向时间服务器发送新的时间查询。
7. 单击“Set Values”按钮将更改传输到设备。

5.4.11.5 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 Client**
  选中此复选框可启用使用 NTP 自动进行时钟同步。
- **Current System Time**
  此框显示当前系统时间。
- **Last Synchronization Time**
  该框为只读，显示上次进行时钟同步时的时间。

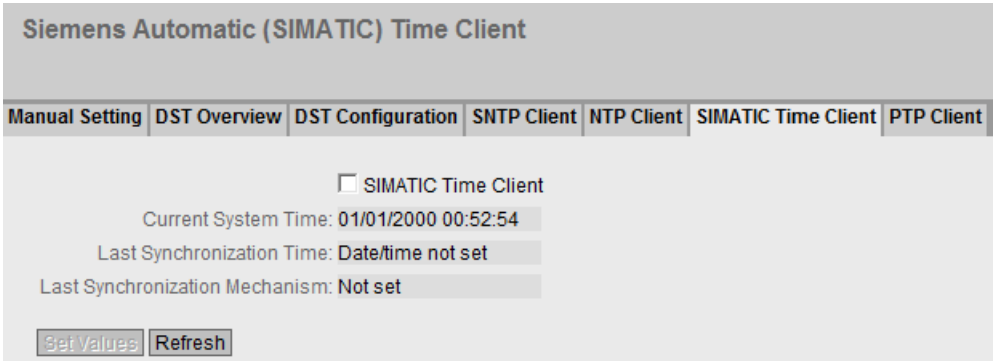
- **Last Synchronization Mechanism**
  该框显示上次时钟同步是如何执行的。可能的方法如下：
  - Not set
    尚未设置系统时间。
  - Manual
    手动设置时间
  - SNTP
    使用 SNTP 自动进行时钟同步
  - NTP
    使用 NTP 自动进行时钟同步
  - SIMATIC
    使用 SIMATIC 时钟帧自动进行时钟同步
  - PTP
    使用 PTP 自动进行时钟同步
- **Time Zone**
  在此框中，以“+/- HH:MM”的格式输入所使用的时区。时区与 UTC 标准世界时间相关。在此框中通过指定时间偏移量将夏令时和标准时间的设置考虑在内。
- **NTP Server IP Address**
  输入 NTP 服务器的 IP 地址。
- **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
- **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 64 到 1024 秒之间。

步骤

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

5.4.11.6 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 Time Client**
  选中此复选框可启用设备作为 SIMATIC 时间客户端。
- **Current System Time**
  此框显示当前系统时间。
- **Last Synchronization Time**
  该框为只读，显示上次进行时钟同步时的时间。
- **Last Synchronization Mechanism**
  该框显示上次时钟同步是如何执行的。可能的方法如下：
  - Not set
    尚未设置系统时间。
  - 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

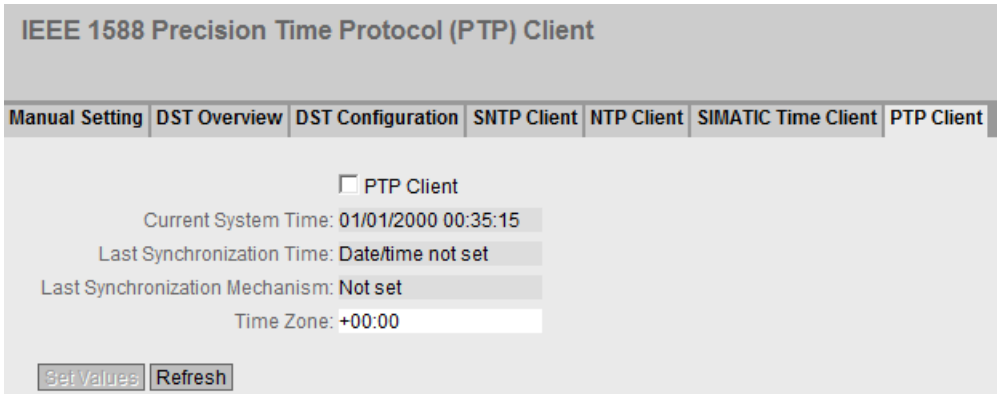
步骤

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

5.4.11.7 PTP 客户端（仅适用于 SCALANCE XR-500）

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

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**
  此框显示当前系统时间。
- **Last Synchronization Time**
  该框为只读，显示上次进行时钟同步时的时间。

- **Last Synchronization Mechanism**
  该框显示上次时钟同步是如何执行的。 可能的方法如下：
  - Not set
    尚未设置系统时间。
  - 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。在此框中通过指定时间偏移量将夏令时和标准时间的设置考虑在内。

步骤

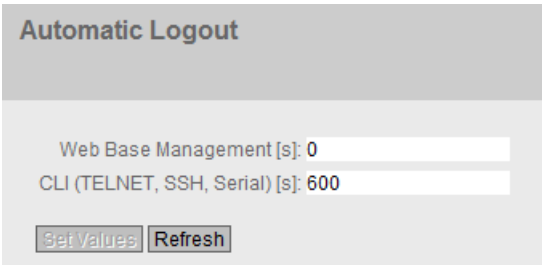
1. 单击“PTP Client”复选框启用使用 PTP 自动进行时间设置。
2. 单击“Set Values”按钮。

5.4.12 自动注销

设置自动注销

在该页面，设置从用户不处于活动状态开始，从 WBM 或 CLI 自动注销前所需经过的时间。

如果您已经自动注销，则需要再次登录。



组态

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

5.4.13 Select/Set 按钮组态

Select/Set 按钮说明

“Select/Set”按钮可用于：

- 更改显示模式，
- 复位为出厂默认设置，
- 定义故障屏蔽和 LED 显示，

有关各项按钮功能的详细说明，请参见设备操作说明。

在此页面中，可限制或完全禁用 Select/Set 按钮的功能。

显示框说明

支持以下功能：

- **“恢复出厂默认设置”(Restore Factory Defaults) 复选框**
  使用“选择/设置”(Select/Set) 按钮启用或禁用“恢复出厂默认设置”功能。

  ⚠ 小心

  启动期间，“恢复出厂默认设置”按钮功能处于激活状态

  如果在组态中禁用此功能，则仅将在运行期间禁用。 重启（例如断电后重启）时，在组态加载前此功能将处于激活状态，因而设备可能无意间被复位为出厂设置。 这可能导致网络运行意外中断，因为发生这种情况时，设备需要进行重新组态。 另外，插入的 PLUG 也会被清空并恢复至出厂时的状态。

- **“设置故障屏蔽”(Set Fault Mask) 复选框**
  使用“选择/设置”(Select/set) 按钮启用或禁用“通过 LED 显示定义故障屏蔽”功能。
- **“冗余管理器”(Redundancy Manager) 复选框**
  启用/禁用冗余管理器功能。

组态步骤

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

5.4.14 Syslog 客户端

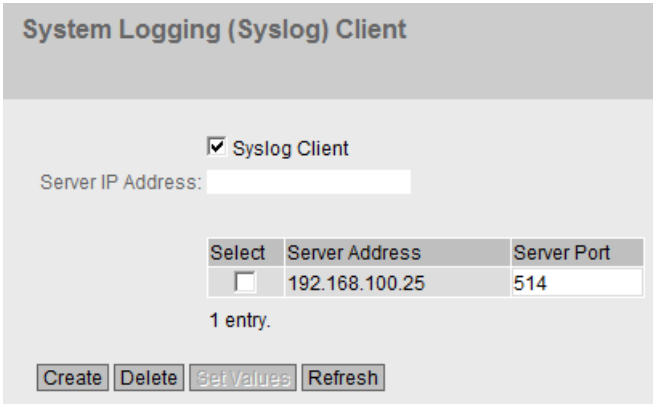
系统事件代理

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

发送日志条目的要求：

- 已在设备上启用 Syslog 功能。
- 已为相关事件启用 Syslog 功能。

- 网络中存在可接收日志条目的 Syslog 服务器。（由于这是一个 UDP 连接，因此不会向发送方发送确认）
- 在设备中已输入 Syslog 服务器的 IP 地址。



说明

该页面包含以下框：

- **Syslog Client**
  启用或禁用 Syslog 功能。
- **Server IP Address**
  在此输入 Syslog 服务器的 IP 地址。

该表包含以下各列

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

步骤

启用功能

1. 选中“Syslog Client”复选框。
2. 单击“Set Values”按钮。

创建新条目

1. 在“Server IP Address”输入框中，输入将保存日志条目的 Syslog 服务器的 IP 地址。
2. 单击“Create”按钮。 将在表中插入一个新行。
3. 在“Server Port”输入框中，输入该服务器 UDP 端口的端口号。
4. 单击“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

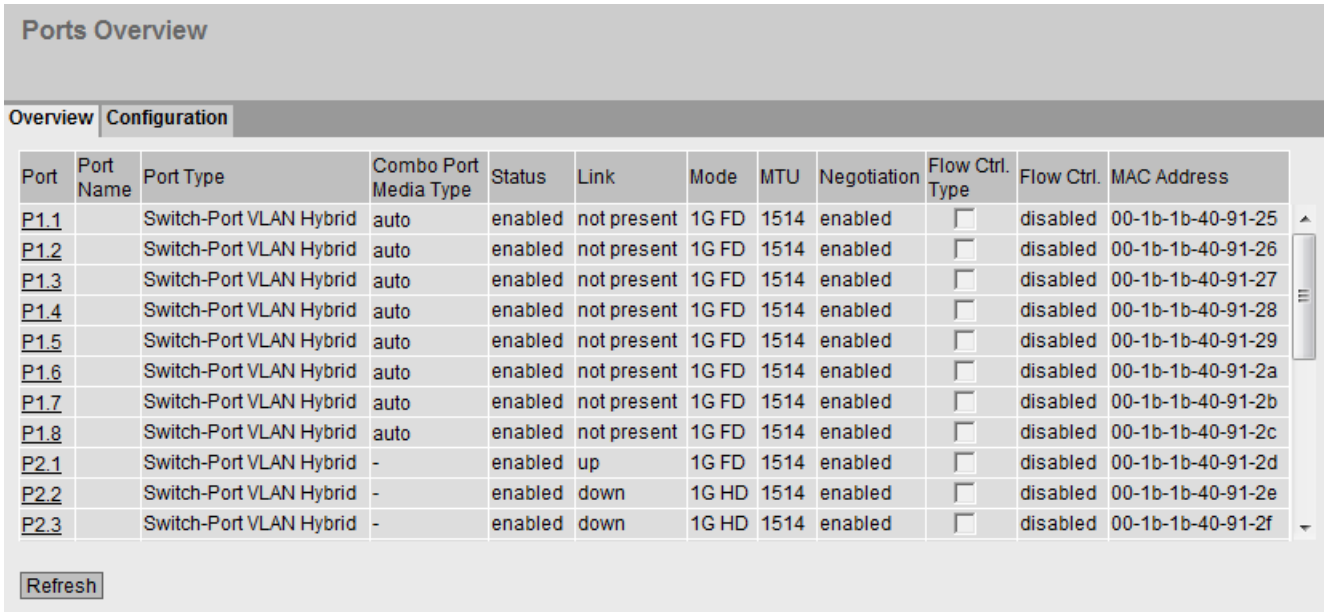
1. 选中要删除的行中的复选框。
2. 单击“Delete”按钮。 会删除所有选中的条目并刷新显示。

5.4.15 端口

5.4.15.1 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	Link	Mode	MTU	Negotiation	Flow Ctrl. Type	Flow Ctrl.	MAC Address
P1.1		Switch-Port VLAN Hybrid	auto	enabled	not present	1G FD	1514	enabled		disabled	00-1b-1b-40-91-25
P1.2		Switch-Port VLAN Hybrid	auto	enabled	not present	1G FD	1514	enabled		disabled	00-1b-1b-40-91-26
P1.3		Switch-Port VLAN Hybrid	auto	enabled	not present	1G FD	1514	enabled		disabled	00-1b-1b-40-91-27
P1.4		Switch-Port VLAN Hybrid	auto	enabled	not present	1G FD	1514	enabled		disabled	00-1b-1b-40-91-28
P1.5		Switch-Port VLAN Hybrid	auto	enabled	not present	1G FD	1514	enabled		disabled	00-1b-1b-40-91-29
P1.6		Switch-Port VLAN Hybrid	auto	enabled	not present	1G FD	1514	enabled		disabled	00-1b-1b-40-91-2a
P1.7		Switch-Port VLAN Hybrid	auto	enabled	not present	1G FD	1514	enabled		disabled	00-1b-1b-40-91-2b
P1.8		Switch-Port VLAN Hybrid	auto	enabled	not present	1G FD	1514	enabled		disabled	00-1b-1b-40-91-2c
P2.1		Switch-Port VLAN Hybrid	-	enabled	up	1G FD	1514	enabled		disabled	00-1b-1b-40-91-2d
P2.2		Switch-Port VLAN Hybrid	-	enabled	down	1G HD	1514	enabled		disabled	00-1b-1b-40-91-2e
P2.3		Switch-Port VLAN Hybrid	-	enabled	down	1G HD	1514	enabled		disabled	00-1b-1b-40-91-2f

显示框说明

该表格包括以下列：

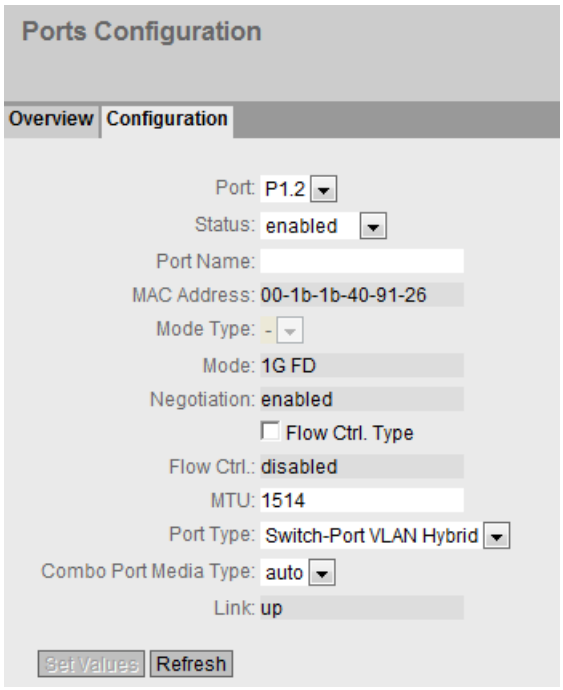
- **端口 (Port)**
  显示可组态端口。 条目是一个链接。 如果单击该链接，相应组态页便会打开。 端口由模块号和端口号组成，例如，端口 0.1 表示模块 0，端口 1。
- **端口名称 (Port Name)**
  显示端口名称。
- **端口类型 (Port type)**（仅限路由）
  显示端口类型。 可能的类型如下：
  - 路由器端口 (Router port)
  - 交换机端口 VLAN 混合 (Switch Port VLAN Hybrid)
  - 交换机端口 VLAN 中继 (Switch-Port VLAN Trunk)

- **组合端口介质类型 (Combo Port Media Type)**（仅限 SCALANCE XM400）
  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)**
  显示端口是开启还是关闭状态。 数据通信只能通过已启用的端口。
- **链路 (Link)**
  显示网络连接状态。 有以下连接状态：
  - “有效”(Up)
    端口与网络之间存在有效链路，正在接收链路完整性信号。
  - “无效”(Down)
    链路中断，例如由于关闭了所连接的设备。
- **模式 (Mode)**
  显示端口的传输参数。
- **MTU (Maximum Transmission Unit)**
  显示包大小。
- **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)**
  显示此端口的流量控制是启用还是禁用状态。
- **流控制 (Flow Ctrl.)**
  显示此端口上的流量控制是否正常工作。
- **MAC 地址 (MAC Address)**
  显示端口的 MAC 地址。

5.4.15.2 组态

组态端口

通过本页面，可以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)**
  指定端口是启用还是禁用状态。
  - 启用 (enabled)
    启用端口。 数据通信只能通过已启用的端口。
  - 禁用 (disabled)
    禁用端口但保持连接。
  - 链路中断 (link down)
    禁用端口并且中断到伙伴设备的连接。
- **“名称”(Name)**
  输入端口的名称。
- **“MAC 地址”(MAC address)**
  显示端口的 MAC 地址。

- **“模式类型”(Mode Type)**
  在此下拉列表中，选择端口的传输速度和传输方法。 如果将模式设置为“Auto negotiation”，会自动与连接的终端设备协商这些参数。 还必须处于“Autonegotiation”模式。

  说明

  在某个端口与伙伴端口互相通讯之前，两端必须具有匹配的设置。

  说明

  组合端口的“模式类型”

  要设置组合端口的“模式类型”，将“组合端口介质类型”(Combo Port Media Type) 改为“rj45”。

  如果“组合端口介质类型”(Combo Port Media Type) 设置为“自动”(auto)，且 RJ-45 端口已被使用，则无法设置“模式类型”。

- **“模式”(Mode)**
  显示端口的传输速度和传输方法。 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。

  说明

  自动协商与开启/关闭流控制

  只有关闭“自动协商”(autonegotiation) 功能，才可启用或禁用流控制。 之后无法再次启用该功能。

- **“流控制类型”(Flow Ctrl. Type)**
  启用或禁用端口的流控制。
- **流控制 (Flow Ctrl.)**
  显示此端口上的流量控制是否正常工作。
- **MTU**
  输入包大小。

- **“端口类型”(Port Type)**（仅限路由）
  从下拉列表中选择端口类型。
  - 路由器端口 (Router port)
    端口是第 3 层接口。它不支持第 2 层功能。
  - 交换机端口 VLAN 混合 (Switch Port VLAN Hybrid)
    端口发送有标记和无标记的帧。它不会自动成为 VLAN 的成员。
  - 交换机端口 VLAN 中继 (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。
- **组合端口介质类型 (Combo Port Media Type)**（仅限 SCALANCE XM400）
  指定组合端口的模式：
  - auto
    如果您选择此模式，SFP 收发器端口具有较高优先级。
    插入 SFP 收发器时，将立即终止 RJ-45 固定端口上的现有连接。 如果未插入 SFC 收发器，则可经由 RJ-45 固定端口建立连接。
  - rj45
    如果您选择此模式，RJ-45 固定端口的使用与 SFP 收发器端口无关。
    如果插入 SFP 收发器，会将其禁用并关闭电源。
  - sfp
    如果您选择此模式，SFP 收发器端口的使用与内置 RJ-45 端口无关。
    如果已建立 RJ-45 连接，则将关闭 RJ-45 端口的电源，连接终止。

  组合端口的出厂设置为 auto 模式。
- **链路 (Link)**
  显示网络连接状态。 可用选项如下：
  - “有效”(Up)
    端口与网络之间存在有效链路，正在接收链路完整性信号。
  - “无效”(Down)
    链路中断，例如由于关闭了所连接的设备。

更改端口组态

单击相应的框可更改组态。

说明

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

- 自动组态
- 传输速度
- 传输技术

说明

利用各个自动功能，设备可以在某个端口过载时，防止或降低对其它端口和优先级 (Class of Service) 的影响。 这意味着即使启用流量控制，帧也可能被丢弃。
当设备接收的帧多于它可以发送的帧时（例如由于不同的传输速度），会发生端口过载。

更改 PROFINET 组合端口设置

默认情况下，组合端口的“组合端口介质类型”(Combo Port Media Type) 参数设置为“自动”(auto)。

如果 PROFINET 组合端口设置为“自动”(auto)，将无法执行传输速率设置等操作。

如果使用 PROFINET，将“组合端口介质类型”(Combo Port Media Type) 参数设置更改为“sfp”或“rj45”。

组态步骤

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

5.4.16 故障监视

5.4.16.1 电源

监视电源的设置

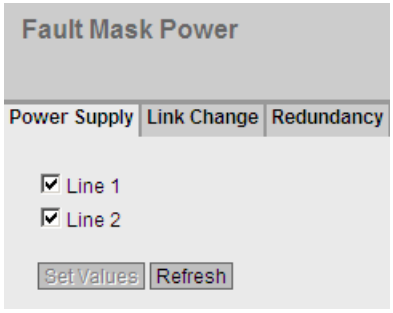
组态是否通过消息系统监视电源。 根据硬件型号，有一个或两个电源连接器（线路 1/线路 2）。 带冗余电源时，应对每个单独的进线线路分别组态监视。

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

说明

设备的精简版操作说明中包含允许的工作电压限值。

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。



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。

5.4.16.2 Link Change

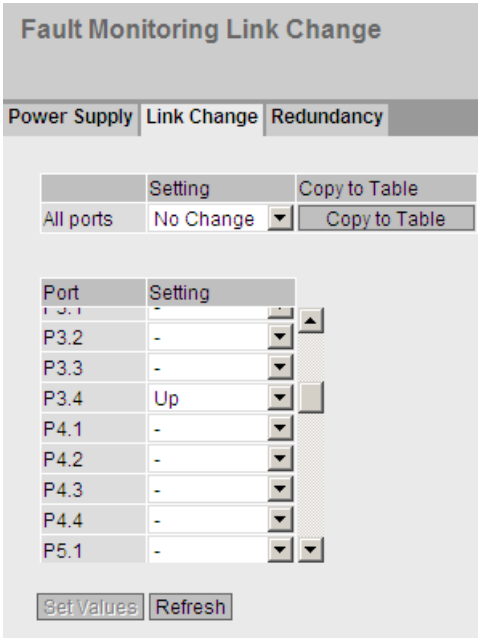
连接状态变化的故障监视组态

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，则发出错误信号

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

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

表 1 包含以下列：

- **第 1 列**
  显示设置对于所有端口有效。
- **设置 (Setting)**
  从下拉列表中选择设置。 可选择以下设置选项：
  - “-”（禁用）
  - Up
  - Down
  - 无变化 (No Change)： 表 2 中的设置保持不变。
- **复制到表中 (Copy to Table)**
  如果单击此按钮，则为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **端口 (Port)**
  显示可用端口和链路汇聚。 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：
  – 有效 (Up)
    当端口变为激活状态时触发错误处理。
    （从“链路中断”(Link down) 到“链路接通”(Link up)）
  – 无效 (Down)
    当端口变为未激活状态时触发错误处理。
    （从“链路接通”(Link up) 到“链路中断”(Link down)）
  – “-”（禁用）
    不触发错误处理。

组态步骤

为端口组态错误监视

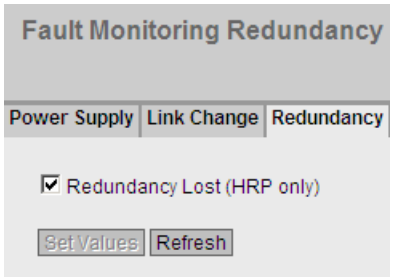
1. 从相应的下拉列表中，选择要监视连接状态的插槽/端口对应的选项。
2. 单击“设置值”(Set Values) 按钮。

为所有端口组态错误监视

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

5.4.16.3 冗余

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。



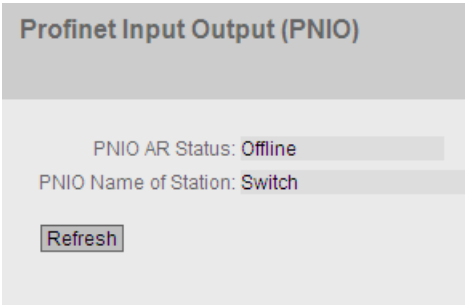
设置

- **冗余丢失（仅 HRP）**
  启用或禁用连接监视。 若失去连接冗余，则指示出错。

5.4.17 PNIO

PROFINET IO 的设置

此页面显示 PROFINET IO AR 状态和设备名称。



显示框说明

该页面包含以下框：

- **PNIO AR 状态 (PNIO AR Status)**
  此框显示 PROFINET IO 连接的状态；也就是说，设备与 PROFINET IO 控制器连接“Online”(在线) 还是“Offline”(离线)。
  在此处，“Online”表示存在到 PROFINET IO 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 IO 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 IO 控制器的参数集进行组态。
- **PNIO 站名称 (PNIO Name of Station)**
  此框根据 STEP 7 HW Config 中的组态显示 PROFINET IO 设备名称。

5.4.18 PLUG 组态

注意
操作期间请勿卸下或插入 C-PLUG/KEY-PLUG！ 只有在设备关闭情况下才可以插拔 PLUG。 设备以 1 秒的间隔检查 PLUG 是否存在。如果检测到 PLUG 被卸下，则会重启。 如果在设备中插入了有效 KEY-PLUG，设备会在重启后切换到预定的错误状态。

C-PLUG/KEY-PLUG 组态的相关信息

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

说明

只有在单击“Set Values”按钮后，才会执行此操作。

此操作无法撤销。

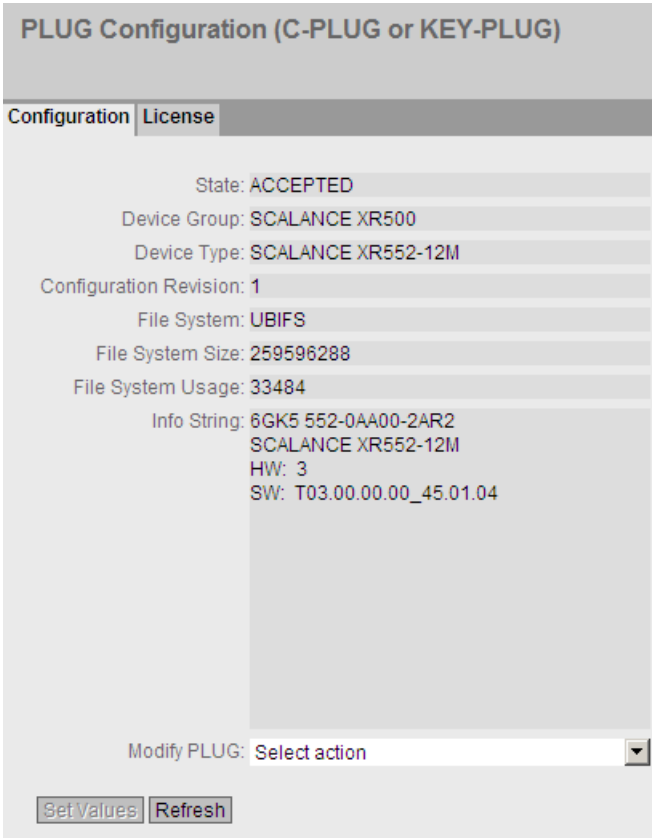
如果进行选择之后您决定不执行此功能，则单击“Refresh”按钮。 随后将再次从设备中读取此页面数据，并会取消选择。

说明

插入的 PLUG 组态与先前版本不兼容

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了 PLUG，则重启后，由于 PLUG 仍具有之前最新固件的组态数据，因此状态为“Not Accepted”。这样，您便可以返回之前的最新固件而不丢失任何组态数据。

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



显示框说明

该表格包括以下行：

- **State**
  显示 PLUG 的状态。 可能的状态包括：
  - ACCEPTED
    设备中存在具有有效且适当组态的 PLUG。
  - NOT ACCEPTED
    插入的 PLUG 上的组态无效或不兼容。
  - NOT PRESENT
    设备中未插入 C-PLUG 或 KEY-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。
  - MISSING
    未插入 PLUG。 将在需要许可证的设备上组态功能。
- **Device Group**
  显示先前使用该 C-PLUG 或 KEY-PLUG 的 SIMATIC NET 产品线。

- **Device Type**
  显示先前使用该 C-PLUG 或 KEY-PLUG 的产品线的设备类型。
- **Configuration Revision**
  组态结构的版本。 此信息与设备支持的组态选项相关，而与具体的硬件配置无关。 因此，在添加或移除附加组件（模块或扩展器）时，此版本信息不会改变，但是如果更新固件，则该信息可能会发生改变。
- **File System**
  显示 PLUG 上的文件系统类型。

注意
新文件系统 UBI 自固件版本 3.0 起，用于 C-PLUG 或 KEY-PLUG 的标准文件系统为 UBI。 如果在这类设备中检测到了带有先前文件系统 IECP 的 C-PLUG，则会将此 C-PLUG 格式化为 UBI 文件系统，并将数据重写到 C-PLUG 中。 固件更新至 V3.0 后文件系统也会发生变化。若之后降级到相应固件的先前版本，则会引发故障。 固件既无法读取也无法写入 C-PLUG 或 KEY-PLUG，甚至无法“将 PLUG 恢复为出厂默认设置”。

- **File System Size [byte]**
  显示 PLUG 的文件系统的最大存储空间。
- **File System Usage [byte]**
  显示 PLUG 文件系统中当前已被使用的存储空间。
- **Info String**
  显示有关之前使用该 PLUG 的设备的所有附加信息，例如：订货号、型号标识以及硬件与软件的版本。 显示的软件版本与上次更改了组态的版本相对应。 状态为“NOT ACCEPTED”时，将显示有关问题原因的更多信息。
- **“修改 PLUG”(Modify PLUG) 下拉列表**
  从下拉列表中选择设置。 用户可使用以下选项更改 C-PLUG 或 KEY-PLUG 上的组态：
  - Write current configuration to PLUG
    仅当 PLUG 的状态为“NOT ACCEPTED”或“FACTORY”时，此选项才可用。
    会将设备内部闪存中的组态复制到 PLUG。
  - Erase PLUG to factory default
    删除 C-PLUG 中的所有数据并触发低级格式化功能。

组态步骤

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

5.4.19 PLUG 许可证

注意
操作期间请勿卸下或插入 C-PLUG/KEY-PLUG！ 只有在设备关闭情况下才可以插拔 PLUG。 设备以 1 秒的间隔检查 PLUG 是否存在。 如果检测到 PLUG 被卸下，则会重启。 如果在设备中插入了有效 KEY-PLUG，设备会在重启后切换到预定的错误状态。 若设备先前组态了 PLUG，则该设备再无法在缺少此 PLUG 的情况下使用。为再次使用该设备，请将设备重置为出厂设置。

说明

插入的 PLUG 组态与先前版本不兼容

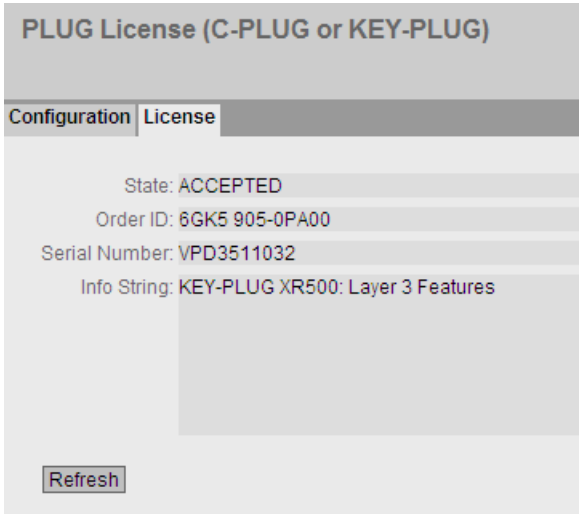
在安装先前版本的过程中，组态数据可能丢失。 在这种情况下，安装固件后，设备会使用出厂设置启动。 如果此时设备中插入了 PLUG，则重启后，由于 PLUG 仍具有之前最新固件的组态数据，因此状态为“Not Accepted”。 这样，您便可以返回之前的最新固件而不丢失任何组态数据。

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

KEY-PLUG 许可证的相关信息

C-PLUG 只能存储设备的组态。 除组态外，KEY-PLUG 还包含一个可启用 SIMATIC NET 设备的特定功能的许可证。

此页面提供了有关 KEY-PLUG 上的许可证的详细信息。 在此例中，KEY-PLUG 包含用于启用设备第 3 层功能的数据。



显示框说明

- **State**
  显示 KEY-PLUG 的状态。 可能的状态包括：
  - ACCEPTED
    设备中的 KEY-PLUG 包含合适且有效的许可证。
  - NOT ACCEPTED
    插入的 KEY-PLUG 的许可证无效。
  - NOT PRESENT
    设备中未插入 KEY-PLUG。
  - MISSING
    设备中未插入状态为“FACTORY”的 KEY-PLUG 或 C-PLUG。 将在需要许可证的设备上组态功能。
  - WRONG
    插入的 KEY-PLUG 不适用于设备。
  - UNKNOWN
    KEY-PLUG 的内容未知。
  - DEFECTIVE
    KEY-PLUG 的内容包含错误。
- **Order ID**
  显示 KEY-PLUG 的订货号。 KEY-PLUG 可用于各种功能增强和各种目标系统。

- **Serial Number**
  显示 KEY-PLUG 的序列号。
- **Info String**
  显示有关之前使用该 KEY-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。

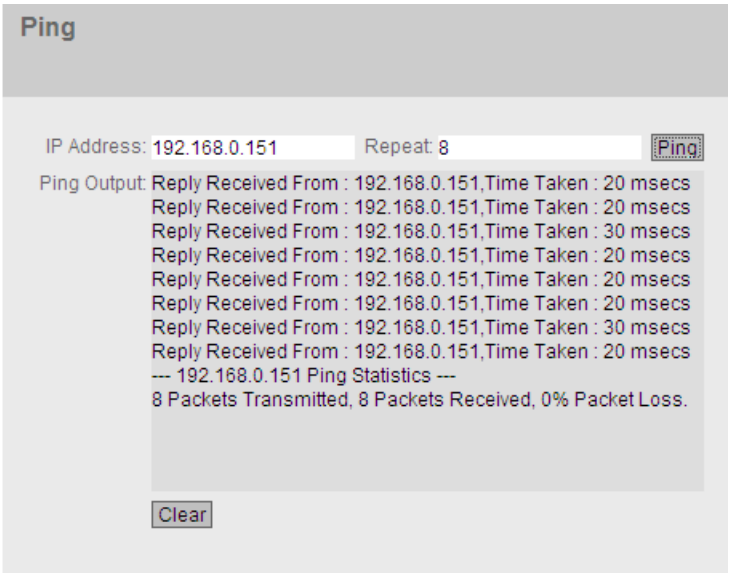
说明

保存组态时，将同时保存当时设备中是否插入了 KEY-PLUG 的信息。 之后，只有插入了具有相同订货号/许可证的 KEY-PLUG 时，该组态才起作用。

5.4.20 Ping

IP 网络中地址的可达性

通过 ping 功能，可检查某一 IP 地址在网络中是否可到达。



说明

该表格包括以下列：

- **“IP Address”输入框**
  输入设备的 IP 地址。
- **“Repeat”输入框**
  输入 ping 请求数量。
- **“Ping”按钮**
  单击此按钮可启动 ping 功能。
- **Ping Output**
  该框会显示 ping 功能的输出。
- **“Clear”按钮**
  单击该按钮可清空“Ping Output”框。

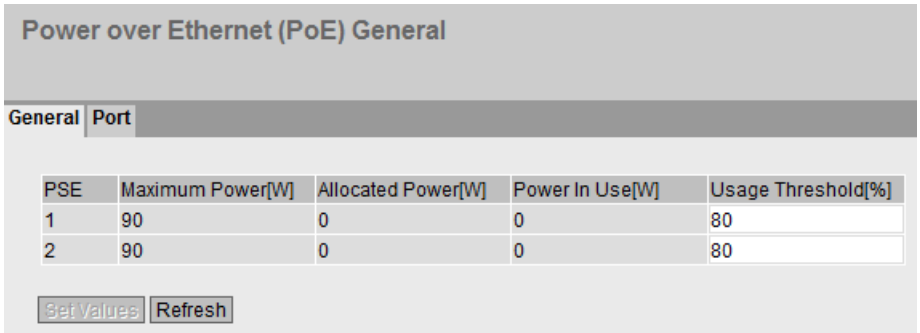
5.4.21 PoE

5.4.21.1 概述

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 X-500 是一种 PSE（供电设备）。 对于 SCALANCE XM400，带有 PoE 功能的四个端口为一组，每组称为一个 PSE。 显示值仅适用于相应的 PSE。



显示框说明

- **PSE（只读）**
  显示 PSE 编号。
- **最大功率 [W]（只读）**
  PSE 为 PoE 设备提供的最大功率。
  可设置 SCALANCE XM-400 的“最大功率”值。
- **分配的功率 [W]（只读）**
  PoE 设备根据“分类”保留的功率总和。
- **使用功率 [W]（只读）**
  终端设备使用的功率总和。
- **使用阈值 [%]**
  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。

使用 SCALANCE XM-400 进行以太网供电

对于 SCALANCE XM-400，可通过端口扩展器 PE408PoE 使用“以太网供电”功能。

PoE 电源

PoE 电源采用外部连接。 每个 PE408PoE 端口扩展器可连接 2 个 PoE 电源。 因此每个 PE408PoE 具有 2 个 PSE 单元（供电设备），其中每个 PSE 有 4 个端口。

PSE 单元的编号

为了在组态中区分 PSE 单元，对其进行如下编号：

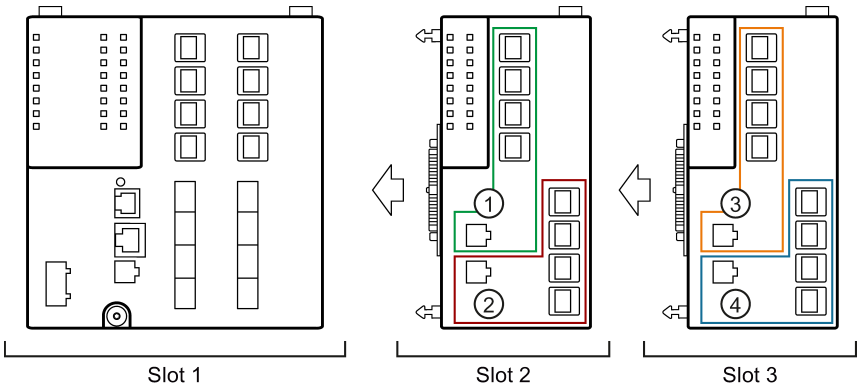


图 5-12　　带 2 个 PE408PoE 端口扩展器的 SCALANCE XM-400

如果 PE408PoE 插入插槽 2，则其两个 PSE 插槽的索引分别为 1 和 2。如果 PE408PoE 插入插槽 3，则其两个 PSE 插槽的索引分别为 3 和 4。

PSE 单元的编号取决于插槽。 如果插槽 2 中插有不带 PoE 的端口扩展器，插槽 3 中插有 PE408PoE，则插槽 3 中 PSE 单元的索引仍为 3 和 4。

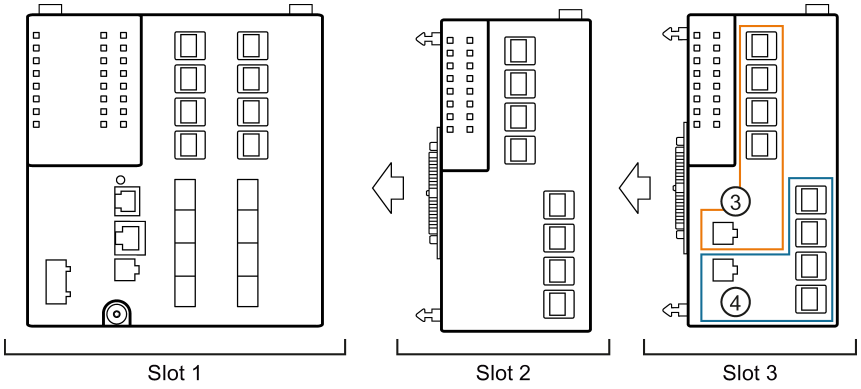


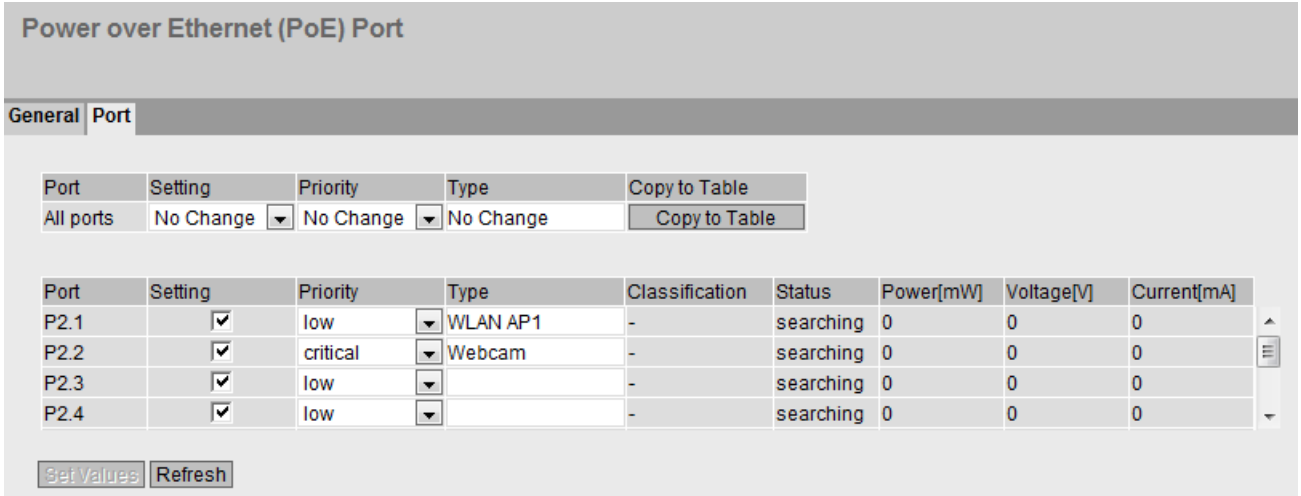
图 5-13　带 2 个端口扩展器的 SCALANCE XM-400（1 个不带 PoE 的端口扩展器和 1 个 PE408PoE）

SCALANCE XM416-4C 只能连接一个端口扩展器，PSE 单元的索引分别为 1 和 2。

5.4.21.2　端口

端口的设置

对于每个 PoE 端口，都可以指定是否通过以太网供电。 还可以为各个连接的受电设备 (PD) 设置优先级。 优先级高的设备优先于其它受电设备。
在此页面上，可以查看各个 PoE 端口的详细信息。



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)**
  从下拉列表中选择设置。 可选择以下设置选项：
  - enabled
    启用该功能
  - disabled
    禁用该功能
  - No Change
    表 2 中的设置保持不变
- **优先级 (Priority)**
  从下拉列表中选择端口的优先级。 如果在表 1 中设置了优先级并将值复制到表 2，则所有端口具有相同优先级。
  可进行以下设置（按相关性以升序排列）：
  - low
    低优先级
  - high
    中优先级
  - critical
    高优先级
  - 无变化 (No Change)
    表 2 中的设置保持不变
- **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。
- **复制到表中 (Copy to Table)**
  如果单击此按钮，则为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **端口 (Port)**
  显示可组态的 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
  - 高
  - 关键

  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。
- **分类 (Classification)（只读）**
  分类指定设备的类别。 通过该设置可识别设备的最大功率。
- **状态 (Status)（只读）**
  显示端口的当前状态。
  可能的状态有：
  - 禁用 (disabled)
    禁止对此端口进行 PoE 供电。
  - 输出功率 (delivering Power)
    激活对此端口的 PoE 供电并连接一台设备。
  - 搜索 (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。

  如果端口的电源不合适，则尽管在 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。
- **功耗 [mW] (Power [mW])（只读）**
  显示 SCALANCE 为此端口提供的功率。
- **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。

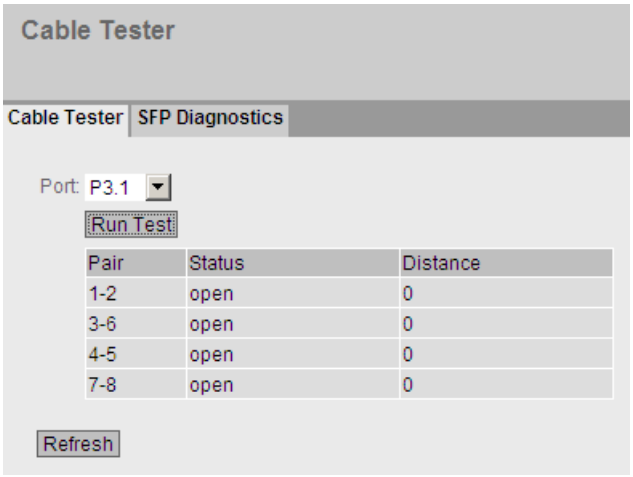
5.4.22 端口诊断

5.4.22.1 电缆测试器

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

说明

请注意，只有在要测试的端口上没有建立任何数据连接时才允许该测试。
而如果要测试的端口上存在数据连接，则会出现短暂的中断。
自动重新建立连接可能会失败，之后需要手动连接。



说明

该页面包含以下框：

- **“端口”(Port) 下拉列表**
  从下拉列表中选择要组态的端口。
- **“运行测试”(Run Test) 按钮**
  激活错误诊断。结果会显示在表中。

该表包含以下各列：

- **线对 (Pair)**
  显示电缆中的线对。

  说明

  线对

  未使用 10/100 Mbps 网络电缆中的线对 4-5 和 7-8。

  1000 Mbps 或千兆位以太网则使用所有 4 个线对。

  线对分配 - 引脚分配如下 (DIN 50173)：

  线对 1 = 引脚 4-5

  线对 2 = 引脚 1-2

  线对 3 = 引脚 3-6

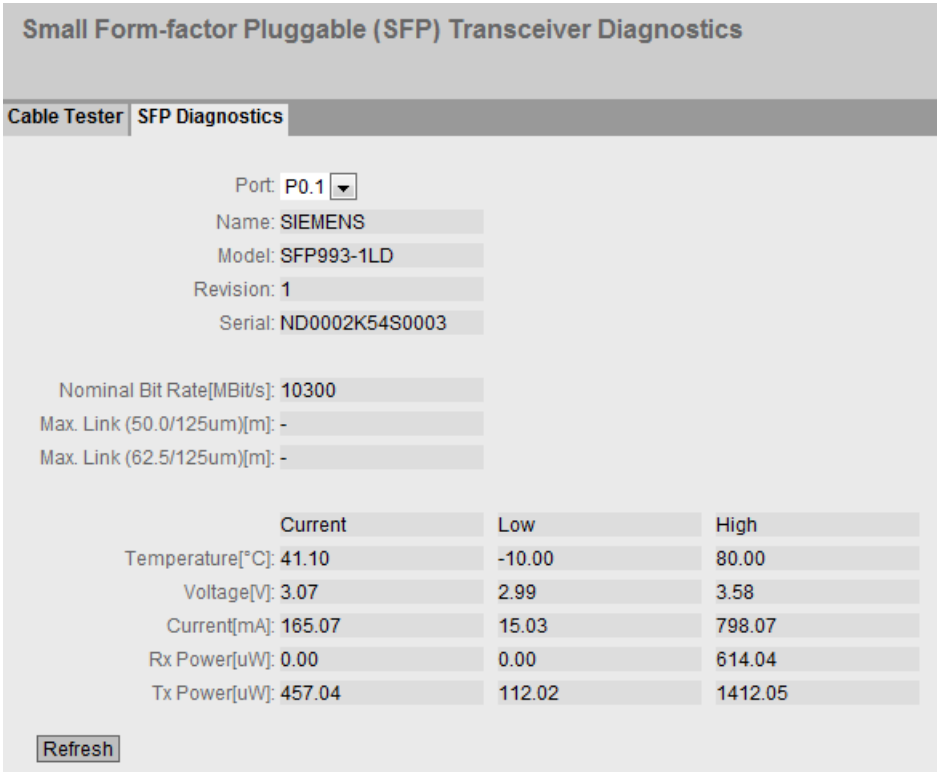
  线对 4 = 引脚 7-8

- **状态 (Status)**
  显示电缆的状态。

- **距离 [m] (Distance [m])**
  显示离电缆末端、电缆断点或短路位置的距离。

5.4.22.2 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

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 [MBit/s])**
  显示接口的额定位速率。
- **最长链路 (50.0/125um) [m] (Max. Link (50.0/125um) [m])**
  显示使用此介质时支持的最远距离（单位为米）。
- **最长链路 (62.5/125um) [m] (Max. Link (62.5/125um) [m])**
  显示使用此介质时支持的最远距离（单位为米）。

下表显示了此端口中使用的 SFP 收发器的值：

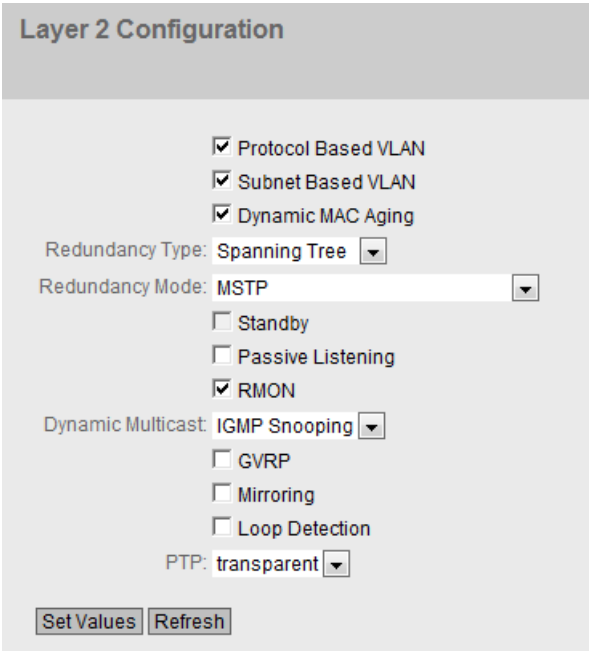
- **温度 [°C] (Temperature [°C])**
  显示接口的温度。
- **电压 [V] (Voltage [V])**
  显示施加到接口的电压 [V]。
- **电流 [mA] (Current [mA])**
  显示接口的电流消耗 [mA]。
- **接收功率 [uW] (Rx Power [uW])**
  显示接口的接收功率 [mW]。
- **发送功率 [uW] (Tx Power [uW])**
  显示接口的发送功率 [mW]。
- **“当前”(Current)** 列
  显示当前值。
- **“低”(Low)** 列
  显示最低值。
- **“高”(High)**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

5.5 “第 2 层”菜单

5.5.1 组态

组态第 2 层

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



显示框说明

- **基于协议的 VLAN (Protocol Based VLAN)**
  启用或禁用基于协议的 VLAN。 其它设置位于“第 2 层 > VLAN”(Layer 2 > VLAN) 中。
- **基于子网的 VLAN (Subnet Based VLAN)**
  启用或禁用基于子网的 VLAN。 其它设置位于“第 2 层 > VLAN”(Layer 2 > VLAN) 中。
- **动态 MAC 老化 (Dynamic MAC Aging)**
  启用或禁用“老化”机制。 可以在“Layer 2 > Dynamic MAC Aging”中组态其它设置。

- **冗余类型 (Redundancy Type)**
  可使用以下设置：
  - **“-”（禁用）**
    禁用冗余功能。
  - **生成树 (Spanning Tree)**
    如果选择此选项，则可在“冗余模式”(Redundancy Mode) 下拉列表中指定所需冗余模式。
  - **环网 (Ring)**
    如果选择此选项，则可在“冗余模式”(Redundancy Mode) 下拉列表中指定所需冗余模式。
  - **采用生成树的环网 (Ring with Spanning Tree)**
    如果选择此选项，则“冗余模式”(Redundancy Mode) 下拉列表呈灰显。 该框显示生成树和环网冗余的当前冗余模式，例如“MSTP/HRP 客户端”(MSTP/HRP Client)。可在“环网冗余”(Ring Redundancy) 和“生成树”(Spanning Tree) 菜单中更改当前设置。

    说明

    如果启用“采用生成树的环网”(Ring with Spanning Tree)，则生成树中的环网端口为“禁用状态”。

- **冗余模式 (Redundancy Mode)**
  如果在“冗余类型”(Redundancy Type) 下拉列表中选择“环网”(Ring)，则可使用以下选项：
  - -
    无
  - Automatic Redundancy Detection
    选择此设置可自动组态冗余模式。
    在“自动冗余检测”模式下，
    工业以太网交换机将自动检测环网中是否存在
    充当“HRP 管理器”的设备。 如果存在，该设备将
    获得“HRP”客户端的角色。
    如果未找到 HRP 管理器，则所有设置为“自动冗余检测”或“MRP
    自动管理器”的设备将通过彼此协商来确定哪台设备将获得“MRP 管理器”的
    角色。 MAC 地址最低的设备将始终为
    “MRP 管理器”。 其余设备将自动设置为
    “MRP 客户端”模式。
  - MRP Auto-Manager
    自动介质冗余管理器
  - MRP Client
    介质冗余客户端
  - HRP Client
    高速冗余协议客户端
  - HRP Manager
    高速冗余协议管理器

  如果在“Redundancy Type”下拉列表中选择“STP”，则可使用以下选项：
  - **STP**
    启用 Spanning Tree Protocol。 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 > MSTP”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 > MSTP”中组态其它设置。

    说明

    使用 RSTP（Rapid Spanning Tree Protocol，快速生成树协议）时，可能短暂出现环路包含重复帧或帧乱序的情况。 如果具体应用不能接受这种情况，应使用较慢的标准生成树机制。

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

  如果在“冗余类型”(Redundancy Type) 下拉列表中选择“采用生成树的环网”(Ring with Spanning Tree)，则会显示生成树和环网冗余的当前冗余模式。

- **备用**
  启用或禁用备用冗余功能。 可在“第 2 层 > 环网冗余”(Layer 2 > Ring Redundancy) 中找到其它设置。
- **被动侦听 (Passive Listening)**
  启用或禁用被动侦听功能。
- **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“以太网统计信息计数器”。
- **动态组播 (Dynamic Multicast)**
  可能的设置如下：
  - **“-”（禁用）**
  - **IGMP Snooping**
    启用 IGMP（Internet 组管理协议）。 可以在“Layer 2 > Multicast > IGMP”中组态其它设置。
  - **GMRP**
    启用 GMRP（GARP 组播注册协议）。 可以在“Layer 2 > Multicast > GMRP”中组态其它设置。

    说明

    GMRP 和 IGMP 不能同时起作用。
- **GVRP**
  启用或禁用“GVRP”（GARP VLAN 注册协议）。 可以在“Layer 2 > VLAN > GVRP”中组态其它设置。
- **镜像 (Mirroring)**
  启用或禁用端口镜像。 可以在“第 2 层 > 镜像”(Layer 2 > Mirroring) 中组态其它设置。

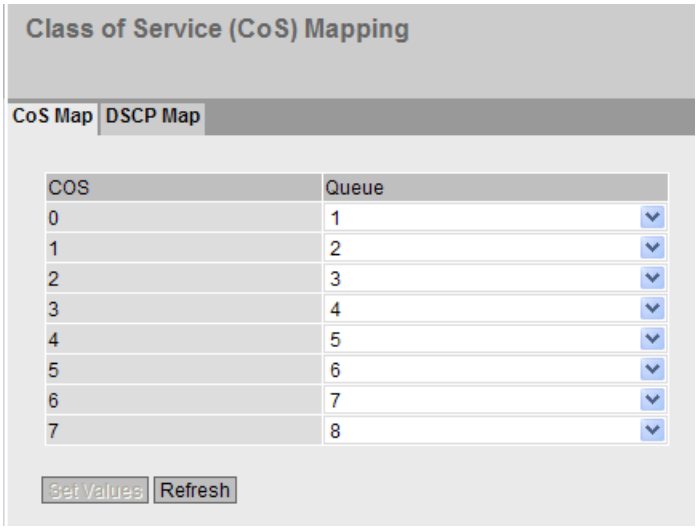
- **回路检测 (Loop Detection)**
  启用或禁用回路检测功能。 通过该功能可检测网络中的回路。 可在“第 2 层 > 回路检测”(Layer 2 > Loop Detection) 中找到其它设置。
- **PTP**
  可为精确时间协议进行以下设置：
  - **关闭 (off)**
    设备不处理任何 PTP 消息。 但是，将根据设备的规则转发 PTP 消息
  - **透明 (Transparent)**
    设备采用透明时钟的功能并将 PTP 消息转发到其它节点，同时在 PTP 消息的修正字段中输入内容。

5.5.2 Qos

5.5.2.1 CoS 队列映射

COS Queue Mapping

在此处将 CoS 优先级分配给特定队列 (Traffic Queues)。



显示框说明

该表格包括以下列：

- **COS**
  显示入站数据包的 CoS 优先级。
- **Queue**
  从下拉列表中选择分配给 CoS 优先级的转发队列（发送优先级）。
  队列编号越高，发送优先级越高。

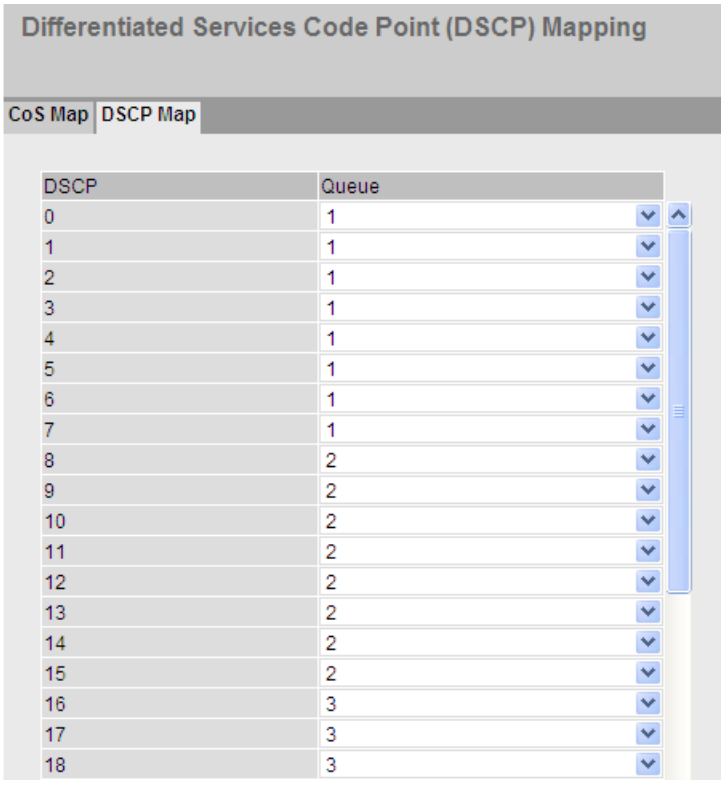
组态步骤

1. 对于“COS”列中的每个值，请从“Queue”下拉列表中选择转发队列。
2. 单击“Set Values”按钮。

5.5.2.2 DSCP 映射

DSCP 队列

在此页面中，将 DSCP 设置分配给各个队列 (Traffic Queues)。



显示值说明

该表格包括以下列：

- **DSCP**
  显示入站数据包的 DSCP 优先级。
- **Queue**
  从下拉列表中选择分配给 DSCP 值的转发队列（发送优先级）。
  队列编号越高，发送优先级越高。

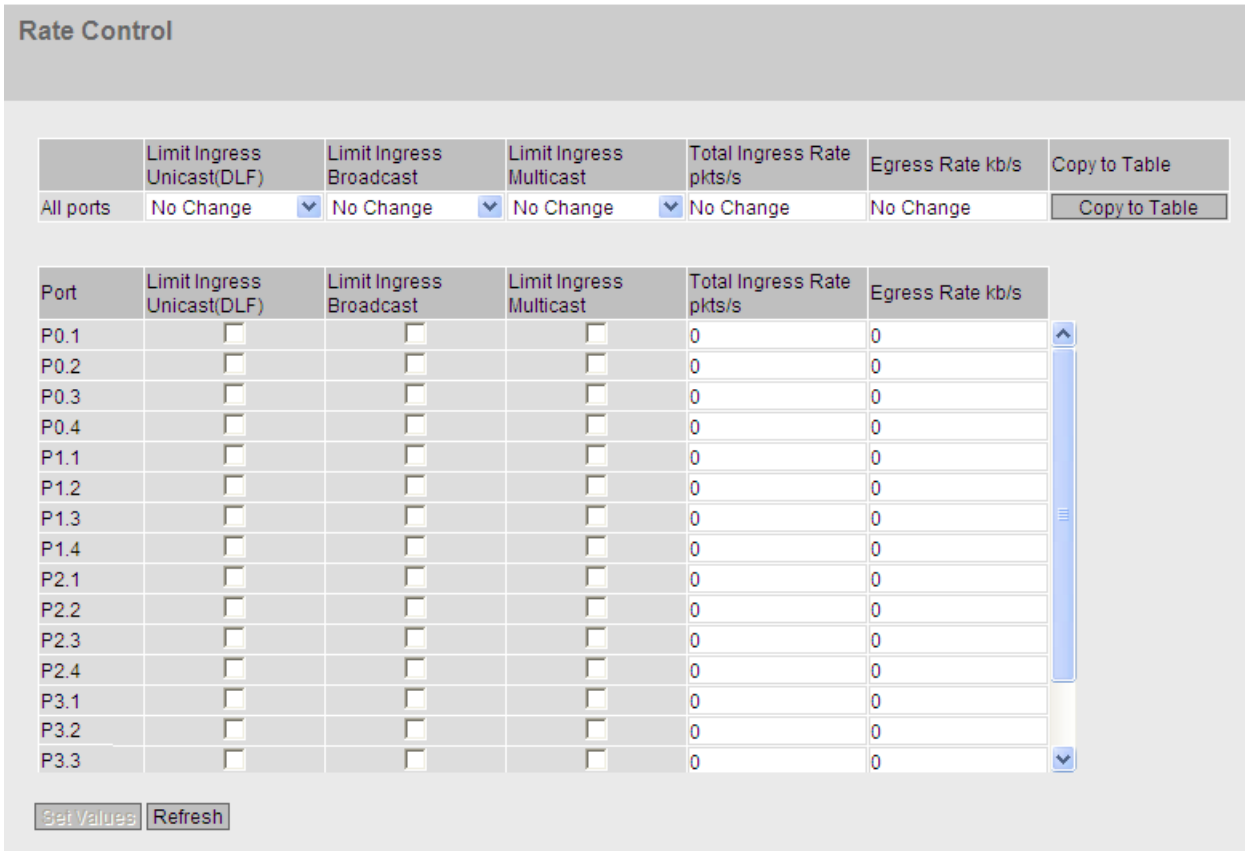
组态步骤

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

5.5.3 速率控制

限制进入和离开数据的传输速率

在此页面上组态各个端口的负载限值（每秒最大数据包数）。 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 (Limit Ingress Unicast (DLF) / Limit Ingress Broadcast / Limit Ingress Multicast)**
  在下拉列表中选择所需设置。
  - 启用： 启用此功能。
  - 禁用： 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 pkts/s (Total Ingress Rate pkts/s)**
  指定设备处理的最大入站数据包数。 如果输入“No Change”，则表中的条目保持不变。
- **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“No Change”，则表中的条目保持不变
- **复制到表中 (Copy to Table)**
  如果单击此按钮，则会为表 2 的所有端口应用这些设置。

表 2 包含以下列：

- **端口 (Port)**
  显示其它信息所关联的插槽和端口。 不能组态此字段。 端口由模块号和端口号组成，例如，端口 0.1 表示模块 0，端口 1。
- **限制入站单播 (DLF) (Limit Ingress Unicast (DLF))**
  启用或禁用数据传输率，以限制无法解析地址的入站单播帧 (Destination Lookup Failure)。
- **限制入站广播(Limit Ingress Broadcast)**
  启用或禁用数据传输率，以限制入站广播帧。
- **限制入站组播 (Limit Ingress Multicast)**
  启用或禁用数据传输率，以限制入站组播帧。

- **总入站速率 pkts/s (Total Ingress Rate pkts/s)**
  指定设备处理的最大入站数据包数。
- **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

输入速率值时，请注意 WBM 会取整为正确的值。

如果组态了 Total Ingress Rate 和 Egress Rate 的值，则运行中的实际值可能超出或低于该设定值 10%。

组态步骤

1. 在所组态端口行的“Total Ingress Rate”和“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“Egress Rate”列中的值。
3. 单击“设置值”(Set Values) 按钮。

5.5.4 VLAN

5.5.4.1 概述

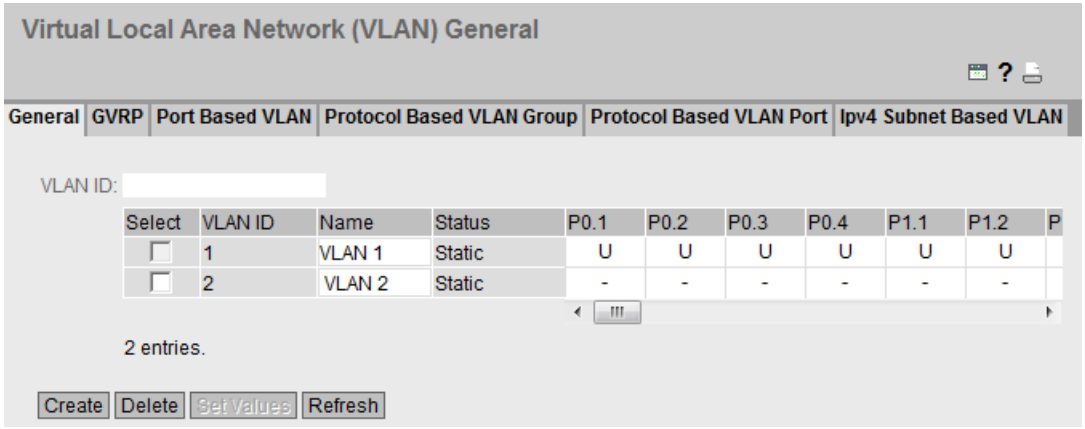
VLAN 组态页面

在此页面中定义 VLAN 并指定端口的使用。

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，则更改后不再可以通过以太网访问该设备。



VLAN 的重要规则

组态和运行 VLAN 时，确保遵守以下规则：

- VLAN ID 为“0”的帧会按照无标记帧处理，但会保留其优先级值。
- 默认情况下，设备上的所有端口均发送不带 VLAN 标记的帧，以确保终端节点可接收这些帧。
- 对于 SCALANCE X 设备，所有端口的默认 VLAN ID 为“1”。
- 如果终端节点连接到端口，发送的离开帧不应带标记（静态访问端口）。 但是，如果此端口有另一台交换机，则发送的帧应添加标记（中继端口）。
- 对于中继端口，VLAN 分配是动态的。除中继端口属性外，仅当端口也作为所涉及 VLAN 中的成员以静态方式输入时，才能创建静态组态。静态组态的示例是某些 VLAN 中多个组播组的分配。

显示框说明

该页面包含以下框：

- **“VLAN ID”输入框**
  在该输入框中输入 VLAN ID。
  值范围： 1 ... 4094

该表格包括以下列：

- **Select**
  选择要删除的行。
- **VLAN ID**
  显示 VLAN ID。VLAN ID（介于 1 到 4094 之间的数字）只能在创建新数据记录时分配一次，之后不能更改。 如要更改，必须删除整个数据记录并重新创建。 可最多定义 257 个 VLAN。
- **名称 (Name)**
  输入 VLAN 的名称。 此名称仅提供信息，对组态没有影响。 最大长度为 32 个字符。
- **状态 (Status)**
  显示端口过滤表中条目的状态类型。 此处，“静态”(static) 表示地址由用户作为静态地址输入。 条目 GVRP 表示组态由 GVRP 帧注册。 但是，仅当设备启用 GVRP 时，此条目才可用。
- **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 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）
    该端口是无标记的 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，在此端口不能使用 GVRP 动态注册 VLAN。 如果 VLAN 中的某个端口带有此选项，则即使该端口组态为中继端口，也无法成为此 VLAN 的成员。
    可以在“第 2 层 > VLAN > 基于端口的 VLAN”(Layer 2 > VLAN > Port Based VLAN) 中组态其它设置。
  - 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。
    可在 CLI（命令行接口）中使用“`switchport mode trunk`”命令组态此功能。

组态步骤

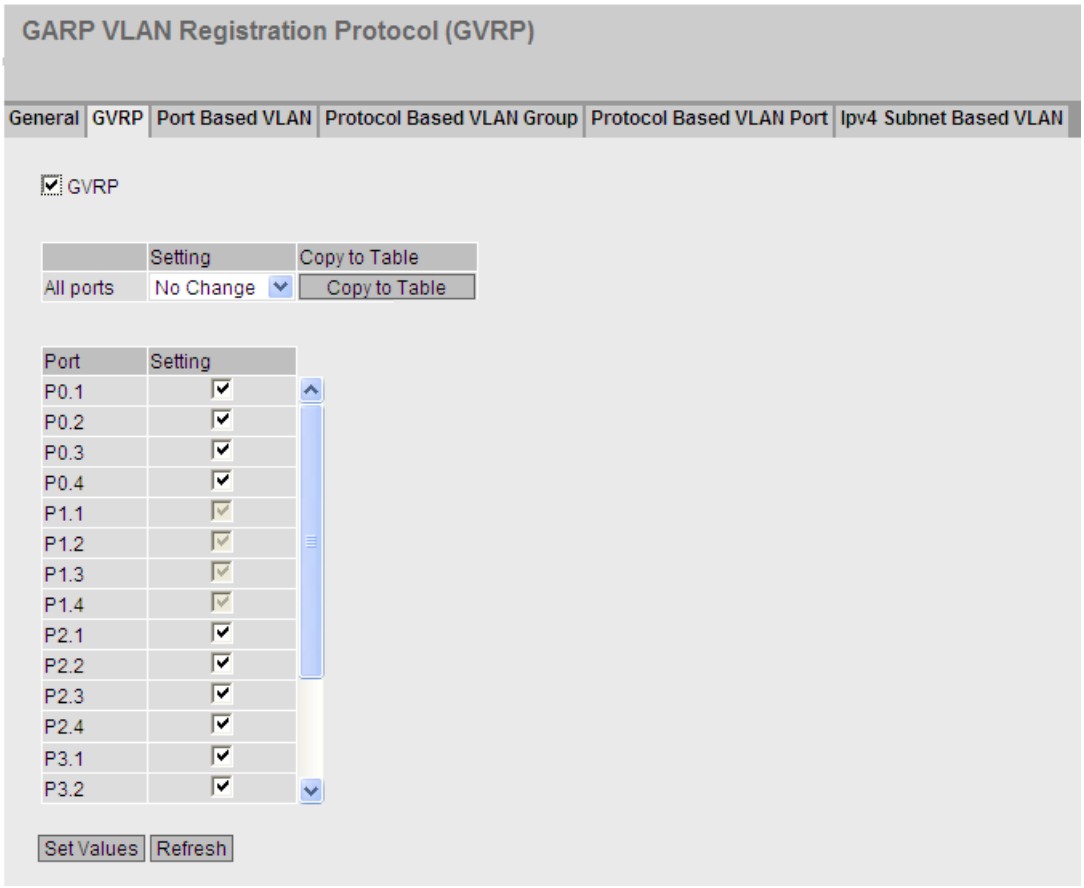
1. 在“VLAN ID”输入框中输入 ID。
2. 单击“创建”(Create) 按钮。 会在表中生成一个新条目。 默认情况下，各个框均输入“-”。
3. 在 Name 下输入 VLAN 的名称。
4. 指定 VLAN 中端口的使用。 例如，如果选择 M，则该端口是 VLAN 的成员。 在此 VLAN 中发送的帧在转发时带有相应 VLAN 标记。
5. 单击“设置值”(Set Values) 按钮。

5.5.4.2 GVRP

组态 GVRP 功能

通过 GVRP 帧，不同设备可在设备的端口处注册特定 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”复选框**
  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：
  - enabled
    启用发送 GVRP 帧。
  - disabled
    禁用发送 GVRP 帧。
  - No Change
    表 2 中无变化。
- **复制到表中 (Copy to Table)**
  如果单击此按钮，将为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **端口 (Port)**
  显示可用端口。 端口由模块号和端口号组成，例如，端口 0.1 表示模块 0，端口 1。
- **设置 (Setting)**
  启用或禁用发送 GVRP 帧。

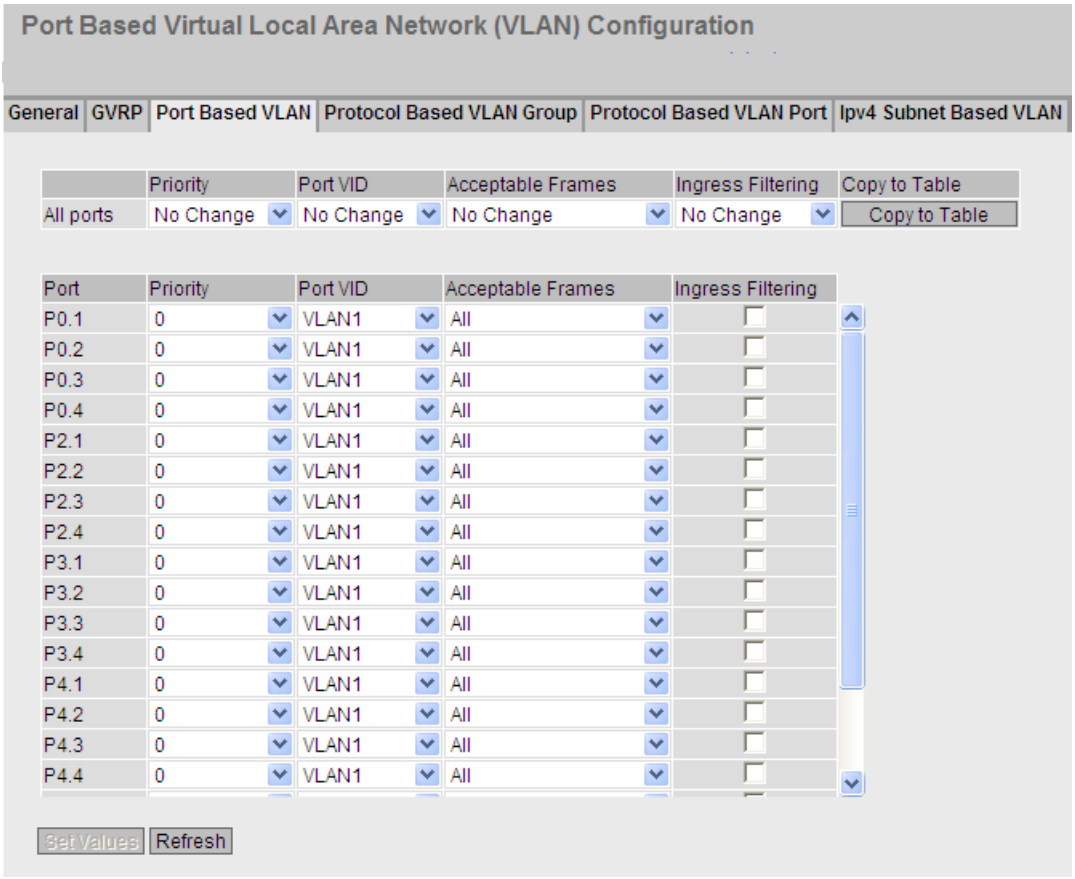
组态步骤

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

5.5.4.3 基于端口的 VLAN

处理接收到的帧

在此页面中，指定用于接收帧的端口属性组态。



显示框说明

表 1 包含以下列：

- **端口 (Port)**
  显示设置对于所有端口有效。
- **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。
- **优先级 (Priority)**
  从下拉列表中选择分配给无标记帧的优先级。
  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。 此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）。
- **端口 VID (Port VID)**
  从下拉列表中选择 VLAN ID。 只能选择在“VLAN > 常规”(VLAN > General) 页面中定义的 VLAN ID。
  如果接收到的帧没有 VLAN 标记，则会为其添加此处指定的 VLAN ID 作为标记，然后按照端口规则发送出去。
- **可接受帧 (Acceptable Frames)**
  指定将接受哪些类型的帧。 可能的选项如下：
  – 仅限带标记的帧 (Tagged Frames Only)
    设备会丢弃所有无标记帧。 否则，按照组态应用转发规则。
  – 全部 (All)
    设备会转发所有帧。
- **入站过滤 (Ingress Filtering)**
  指定是否评估已接收帧的 VID
  可做以下选择：
  – 启用
    由接收到的帧的 VLAN ID 决定是否转发： 要转发 VLAN 标记帧，接收端口必须是相同 VLAN 的成员。 在接收端口会丢弃来自未知 VLAN 的帧。
  – 禁用
    转发所有帧。

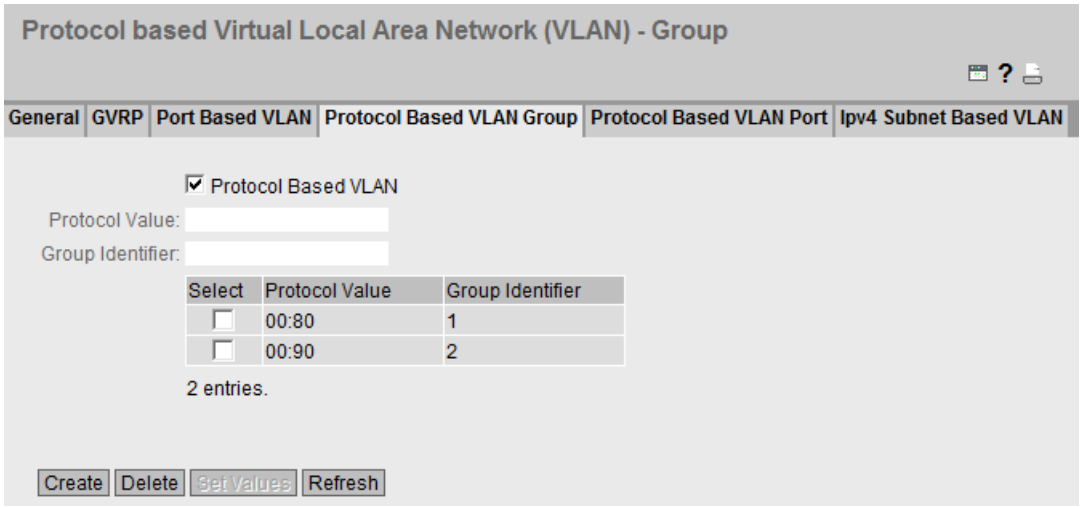
组态步骤

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

5.5.4.4 基于协议的 VLAN 组

简介

在此页面上，指定组并为其分配协议。



显示框说明

该页面包含以下框：

- **基于协议的 VLAN (Protocol Based VLAN)**
  启用或禁用基于协议的 VLAN 分配。
- **协议值 (Protocol Value)**
  输入十六进制协议值。
  下面列出几个示例：
  - PROFINET： 88:92
  - IP： 08:00
  - Novell： 81:37
  - netbios： f0:f0
  - appletalk： 80:9b
- **组标识符 (Group Identifier)**
  输入组的 ID。

该表格包括以下列：

- **Select**
  选择要删除的行。
- **协议值 (Protocol Value)**
  显示协议值。
- **组标识符 (Group Identifier)**
  显示组 ID。

组态步骤

添加条目

1. 在“Protocol Value”输入框中输入协议值。
2. 在“Group Identifier”输入框中输入组 ID。
3. 单击“创建”(Create) 按钮。 会在表中生成一个新条目。
4. 单击“设置值”(Set Values) 按钮。

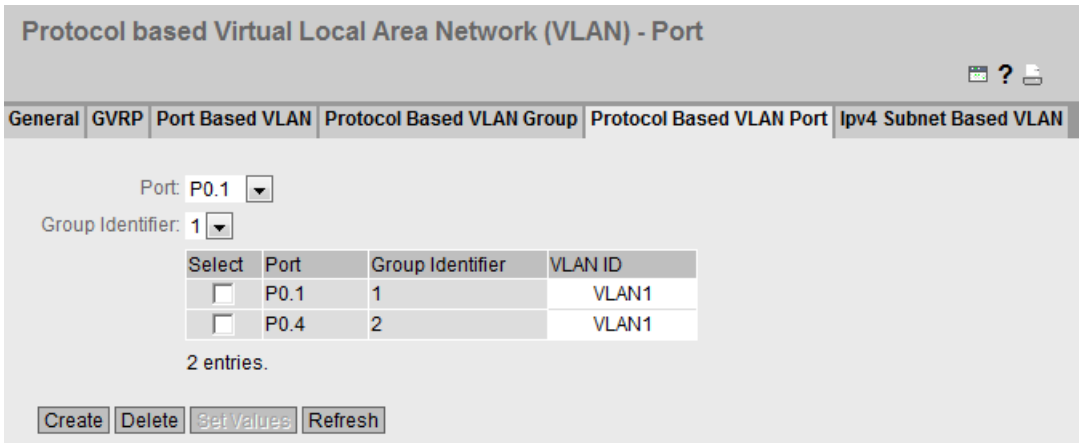
删除条目

1. 在“Protocol Based VLAN Port”选项卡中，检查该协议组是否未在任何端口中使用。
2. 选中要删除的行中的复选框。
3. 单击“删除”(Delete) 按钮。
4. 单击“设置值”(Set Values) 按钮。

5.5.4.5 基于协议的 VLAN 端口

简介

在此页面中，指定分配给单独端口的协议和 VLAN。



显示框说明

该页面包含以下框：

- **端口 (Port)**
  从下拉列表中选择端口。可以选择所有可用端口和链路汇聚。
- **组标识符 (Group Identifier)**
  从下拉列表中选择组 ID。 在 WBM 页面“Protocol Based VLAN Group”中指定 ID。

该表格包括以下列：

- **Select**
  选择要删除的行。
- **端口 (Port)**
  显示所有可用端口及链路汇聚。
- **组标识符 (Group Identifier)**
  显示分配给端口的组 ID。
- **VLAN ID**
  从下拉列表中选择要分配给端口的 VLAN ID。

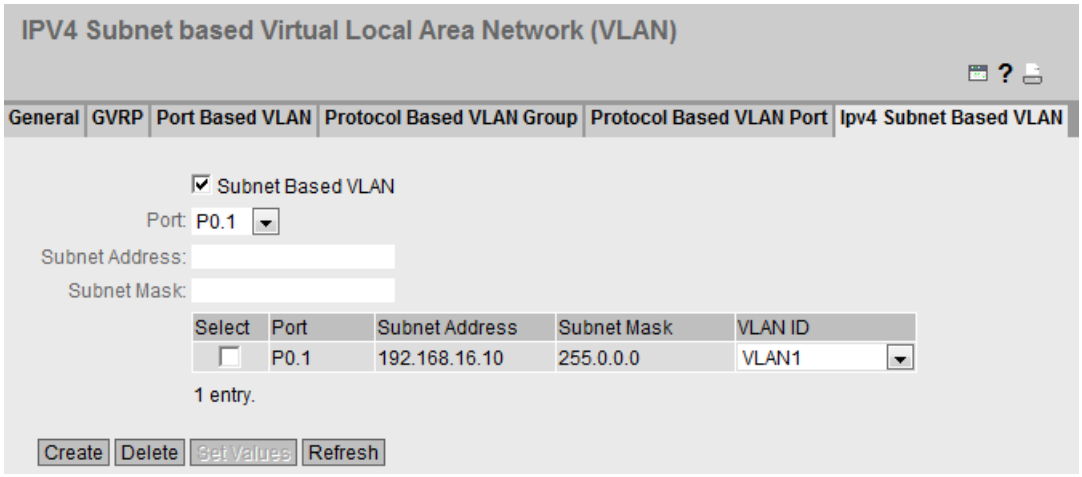
组态步骤

1. 从“Port”下拉列表中选择端口。
2. 从“Group Identifier”下拉列表中选择组 ID。
3. 单击“创建”(Create) 按钮。 会在表中生成一个新条目。
4. 在“VLAN ID”中指定 VLAN ID。
5. 单击“设置值”(Set Values) 按钮。

5.5.4.6 基于 Ipv4 子网的 VLAN

简介

在此页面中，指定分配给子网的 VLAN ID。



显示框说明

该页面包含以下框：

- **基于子网的 VLAN (Subnet Based VLAN)**
  启用或禁用基于子网的 VLAN 分配。
- **端口 (Port)**
  从下拉列表中选择端口。 可以选择所有可用端口和链路汇聚。
- **子网地址 (Subnet Address)**
  输入子网的 IP 地址。
  示例： 192.168.10.0 是指包含节点 192.168.10.1 到 192.168.10.254 的网络 192.168.10.x。
- **子网掩码 (Subnet Mask)**
  输入子网掩码。

该表格包括以下列：

- **Select**
  选择要删除的行。
- **端口 (Port)**
  显示所有可用端口及链路汇聚。

- **子网地址 (Subnet Address)**
  显示端口的 IP 地址。
- **子网掩码 (Subnet Mask)**
  显示分配给端口的子网。
- **VLAN ID**
  选择要分配给端口或子网的 VLAN ID。

组态步骤

1. 从“Port”下拉列表中选择端口。
2. 在“Subnet”中输入子网掩码。
3. 单击“创建”(Create) 按钮。 会在表中生成一个新条目。
4. 从 VLAN ID 下拉列表中选择 VLAN ID。
5. 单击“设置值”(Set Values) 按钮。

5.5.5 镜像

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。

5.5.5.1 常规

镜像 - 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。

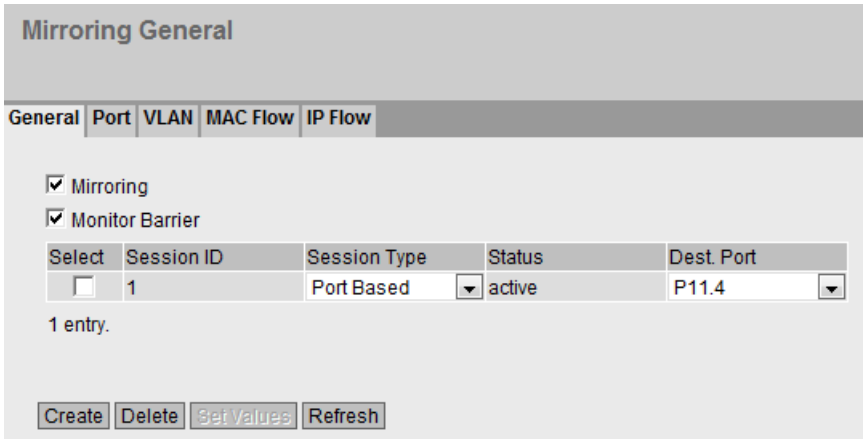
说明

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。

不能超出交换机核心界限对端口进行镜像。

如果想要将常规终端设备连接到监视端口，请禁用端口镜像功能。

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
- **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，也可手动重新组态这些功能。 将再次允许在监视端口上进行数据通信。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自动组态，都将发生复位。

基本设置表格包括以下对话框：

- **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。
- **会话类型 (Session Type)**
  从该下拉列表中选择所需条目：
  - -
    无
  - 基于端口
    基于端口
  - VLAN
    基于 VLAN 的镜像
  - MAC ACL
    镜像 MAC 访问控制列表
  - IP ACL
    镜像 IP 访问控制列表

- **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。

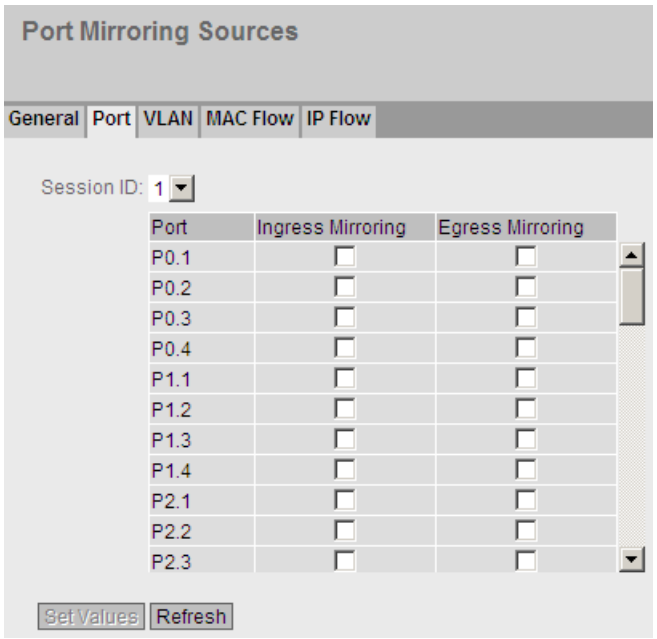
步骤

1. 单击“Create”按钮在表中创建新条目。
   将自动分配会话 ID。 根据所选的会话类型，可创建一个或多个镜像会话。
2. 选择设置。
3. 单击“Set Values”按钮保存并激活所选设置。
4. 切换至以下选项卡为相关会话 ID 进行更详细的设置。
5. 单击首列的复选框选择行。
   单击 “删除”(Delete) 按钮可删除所选行。

5.5.5.2 端口

镜像端口

只有已在 “常规”(General) 选项卡设置了会话类型 “基于端口”(Port Based) 并生成了一个会话 ID 时，才能在此页面上组态相关设置。



显示框说明

- **会话 ID (Session ID)**
  选择要监视的会话。
- **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。

组态步骤

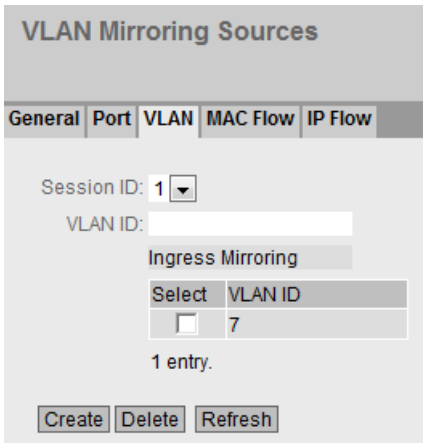
1. 在“会话 ID”(Session ID) 下拉列表中，选择先前在“常规”(General) 选项卡上创建的会话。
2. 在表格中，单击待镜像端口后的行复选框。
   选择要监视进入数据包还是离开数据包。
   要监视端口的整个数据通信，请同时选中这两个复选框。
3. 单击“设置值”(Set Values) 按钮。

5.5.5.3 VLAN

端口镜像的 VLAN 源

只有已在“常规”(General) 选项卡设置了会话类型“VLAN”并生成了一个会话 ID 时，才能在此页面上组态相关设置。

在此页面上指定 VLAN，以将其入站数据通信镜像到监视端口。



显示框说明

该页面包含以下框：

- **会话 ID (Session ID)**
  选择会话 ID。值范围为 1 到 20。
- **VLAN ID**
  在“VLAN ID”输入框中输入 VLAN ID。
  值范围： 1 ... 4094

“入站镜像”表格包括以下列：

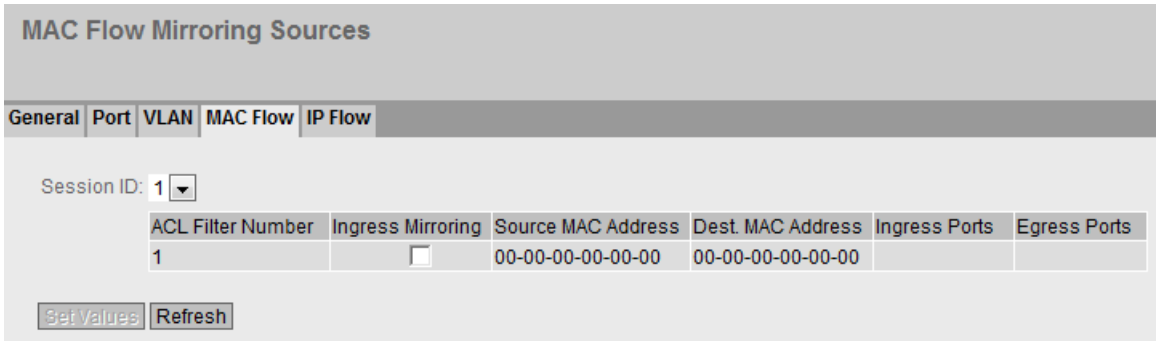
- **Select**
  选择要删除的行。
- **VLAN ID**
  显示镜像入站帧的 VLAN ID。 VLAN ID（介于 1 到 4094 之间的数字）只能在创建新数据记录时分配一次，之后不能更改。 如要更改，必须删除整个数据记录并重新创建。
  可最多定义 257 个 VLAN。

5.5.5.4 MAC 流

端口镜像的 ACL 过滤器

只有已在“常规”(General) 选项卡设置了会话类型“MAC ACL”并生成了一个会话 ID 时，才能在此页面上组态相关设置。

ACL 过滤器决定监视端口上可用的数据。 通过入站监视和出站监视框决定在监视端口上是仅监视入站帧还是也监视出站帧。



显示框说明

- **会话 ID (Session ID)**
  选择端口镜像的会话编号。 值范围是 1 到 20。
- **ACL 过滤器编号 (ACL Filter Number)**
  显示 ACL 过滤器的编号。
- **入站镜像 (Ingress Mirroring)**
  显示是否镜像入站数据包。

说明

规则

所选的入站镜像规则必须在至少一个端口上已组态为端口入站规则才有效。 请参见“端口入站规则 (页 303)”部分

- **源 MAC 地址 (Source MAC Address)**
  显示发送方的 MAC 地址。
- **目标 MAC 地址 (Dest. MAC Address)**
  显示接收方的 MAC 地址。
- **入站端口 (Ingress Ports)**
  显示应用此规则的所有端口的列表。 端口的入站数据流镜像至监视端口（目标 端口）。
- **出站端口 (Egress Ports)**
  显示应用此规则的所有端口的列表。 端口的出站数据流镜像至监视端口（目标 端口）。

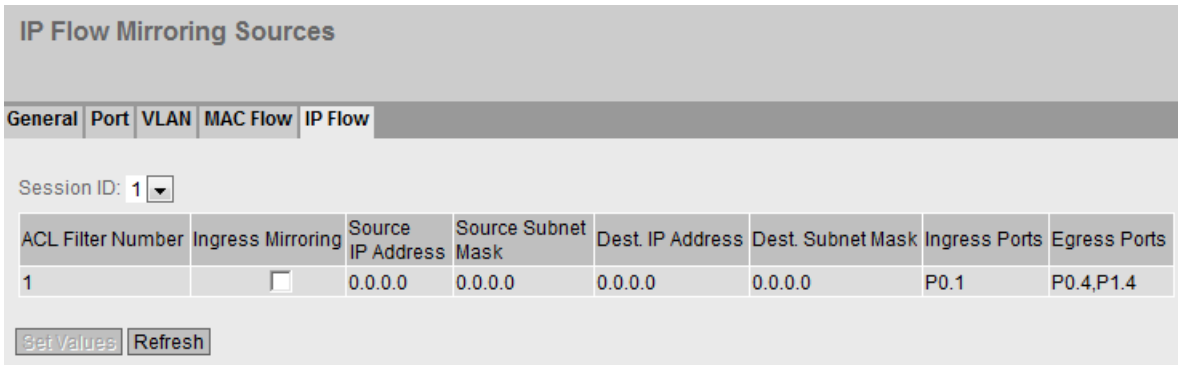
5.5.5.5 IP 流

端口镜像的 ACL 过滤器

只有已在“常规”(General) 选项卡设置了会话类型“IP ACL”并生成了一个会话 ID 时，才能在此页面上组态相关设置。

ACL 过滤器决定监视端口上可用的数据。

在此列表中，将输出监视端口的 IP 数据。



显示框说明

- **会话 ID (Session ID)**
  选择端口镜像的会话编号。 值范围是 1 到 20。
- **ACL 过滤器编号 (ACL Filter Number)**
  显示 ACL 过滤器的编号。
- **入站镜像 (Ingress Mirroring)**
  显示是否镜像入站数据包。

  说明

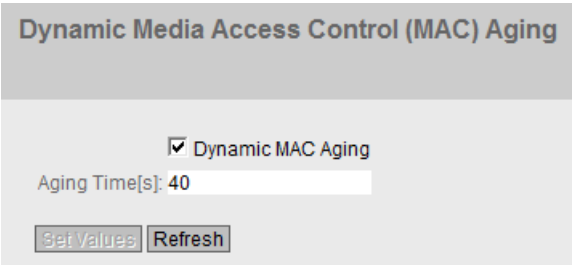
  规则

  所选的入站镜像规则必须在至少一个端口上已组态为端口入站规则才有效。 请参见“端口入站规则 (页 310)”部分
- **源 IP 地址 (Source IP address)**
  显示发送方的 IP 地址。
- **源子网掩码 (Source Subnet Mask)**
  显示发送方的子网掩码。
- **目标 IP 地址 (Dest. IP Address)**
  显示接收方的 IP 地址。
- **目标 子网掩码 (Dest. Subnet Mask)**
  显示接收方的子网掩码。
- **入站端口 (Ingress Ports)**
  显示应用此规则的所有端口的列表。 端口的入站数据流镜像至监视端口（目标 端口）。
- **出站端口 (Egress Ports)**
  显示应用此规则的所有端口的列表。 端口的出站数据流镜像至监视端口（目标 端口）。

5.5.6 动态 MAC 老化

协议设置和交换机功能

设备自动学习连接节点的源地址。 此信息用于将数据帧转发到具体涉及的节点。 这将减少其它节点的网络负载。
如果设备在特定时间内未收到源地址与学习的地址相匹配的帧，则设备会删除学习的地址。这种机制称为“Aging”。 老化可以防止错误地转发帧，例如当某个终端设备（如编程设备）连接到不同的交换机端口时。
如果未启用该复选框，则设备不会自动删除学习的地址。



显示框说明

该页面包含以下框：

- **动态 MAC 老化 (Dynamic MAC Aging)**
  启用或禁用获取的 MAC 地址的自动老化功能：
- **老化时间 [s] (Aging Time [s])**
  输入时间（单位：秒）。 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。 取值范围为 10 秒到 630 秒

组态步骤

1. 选中“Dynamic MAC Aging”复选框。
2. 在“老化时间 [s]”(Aging Time [s]) 输入框中输入时间（以秒为单位）。
3. 单击“设置值”(Set Values) 按钮。

5.5.7 环网冗余

5.5.7.1 环网冗余

环网冗余规则

出厂设置

- 出厂设置将 MSTP 定义为冗余方法。
- 对于 SCALANCE XM-400，出厂设置将端口 P1.1 和 P1.2 定义为环网端口。
- 对于 SCALANCE XM-500，出厂设置将端口 P0.1 和 P0.2 定义为环网端口。

环网端口

SCALANCE XR-500 的预定义环网端口为 10 Gbps 端口。

如果将 1000 Mbps SFP 收发器插入其中一个 10 Gbps 环网端口中，则无法启用环网冗余。

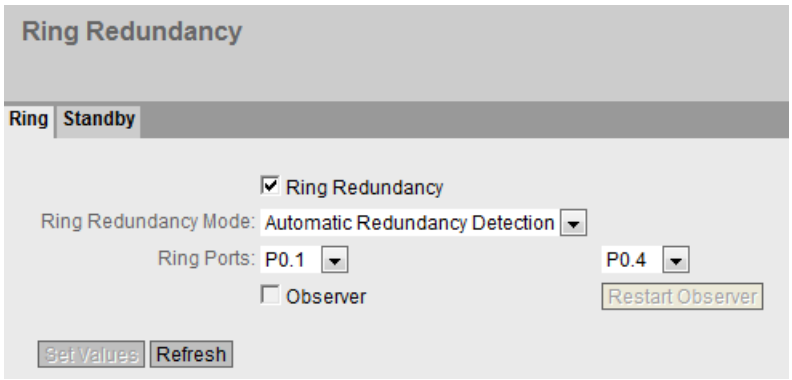
移除 1000 Mbps SFP 收发器。

启用冗余

可通过如下方式启用环网冗余：

- 使用 WBM
- 使用 CLI
- 使用 SELECT/SET 按钮
- 使用 PNIO 组态下载

组态环网冗余



- **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。

- **Ring Redundancy Mode**
  在此设置环网冗余的模式。
  可使用以下模式：
  - Automatic Redundancy Detection
    选择此设置可创建冗余模式的自动组态。
    在“自动冗余检测”模式下，设备会自动检测环网中是否存在充当“HRP 管理器”角色的设备。 如果存在，该设备将获得“HRP”客户端的角色。
    如果未找到 HRP 管理器，则所有设置为“自动冗余检测”或“MRP 自动管理器”的设备将通过彼此协商来确定哪台设备将获得“MRP 管理器”的角色。MAC 地址最低的设备将始终为“MRP 管理器”。 其余设备将自动设置为“MRP 客户端”模式。
  - MRP Auto-Manager
    自动介质冗余管理器
  - MRP Client
    介质冗余客户端
  - HRP Client
    高速冗余协议客户端
  - HRP Manager
    高速冗余协议管理器

- **Ring Ports**
  在此设置将在环网冗余中用作环网端口的端口。
  在左侧的下拉菜单中选择的环网端口是 HRP 中的“隔离端口”。

- **Observer**
  启用或禁用观察器。“Observer”功能仅在 HRP 环网中可用。
  在左侧的下拉菜单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。

- **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。

恢复出厂设置

如果已恢复出厂默认设置，将禁用环网冗余并将默认端口用作环网端口。 如果在之前的组态中使用了其它设置，则这会导致帧循环传送以及数据通信失败。

更改带有冗余管理器的环网端口的状态

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。

5.5.7.2 备用

冗余环网连接

备用冗余支持多个 HRP 环网的冗余链路。

可建立多个备用连接。 如果备用主站部分出现故障，则所有备用连接均出现故障。

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。

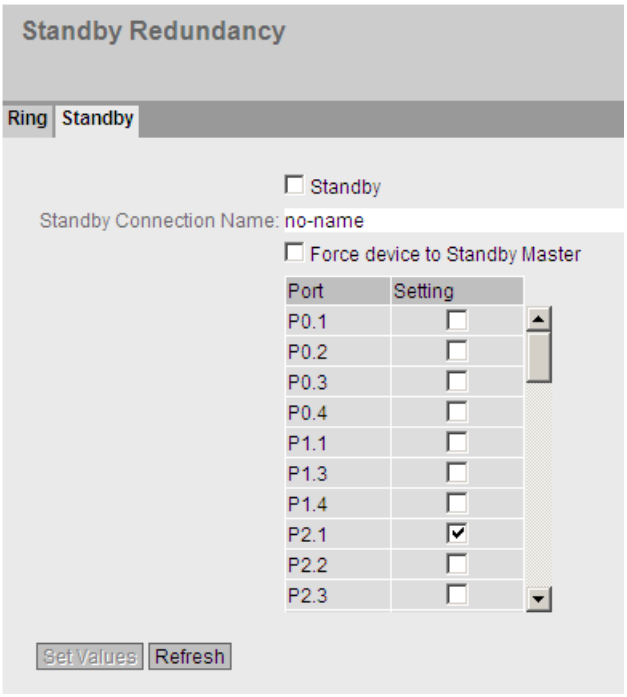
在无故障运行中，通过主站在两个环网之间交换消息。 如果主站线路受到干扰，从站会接管两个环网之间的消息转发。

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台设备。

说明

为了能够使用此功能，必须激活 HRP。
备用管理器始终需要一台已激活的 HRP 客户端。



显示框说明

- **Standby**
  单击此复选框可启用或禁用此功能。

- **Standby Port**
  选择用作备用端口的端口。 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（链路）出现故障，则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。

  说明

  链接多个环网

  如果链接多个环网，也就是说，当启用多个端口作为备用端口时，备用主站和备用从站只能与一个环网建立一条以太网连接。否则将产生帧循环传送从而导致数据通信丢失。

- **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，而不考虑其 MAC 地址。
  – 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“Force device to Standby Master”（将设备强制为备用主站）属性，则也会根据 MAC 地址选择备用主站。

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

说明

如果两个设备通过备用功能相链接，则这两个设备上一定启用了“备用”功能。

- **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。

5.5.8 生成树

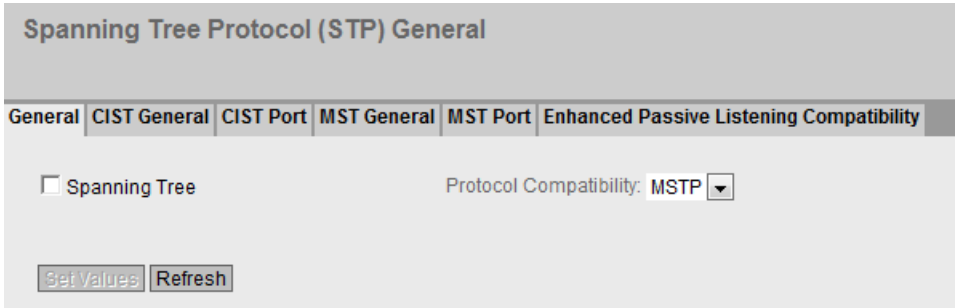
5.5.8.1 常规

MSTP 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。 默认情况下会启用多重生成树。

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 MSTP 的兼容模式，例如，如果选择 RSTP，则 MSTP 的运作方式与 RSTP 类似。
  可使用以下设置：
  - STP
  - RSTP
  - MSTP

组态步骤

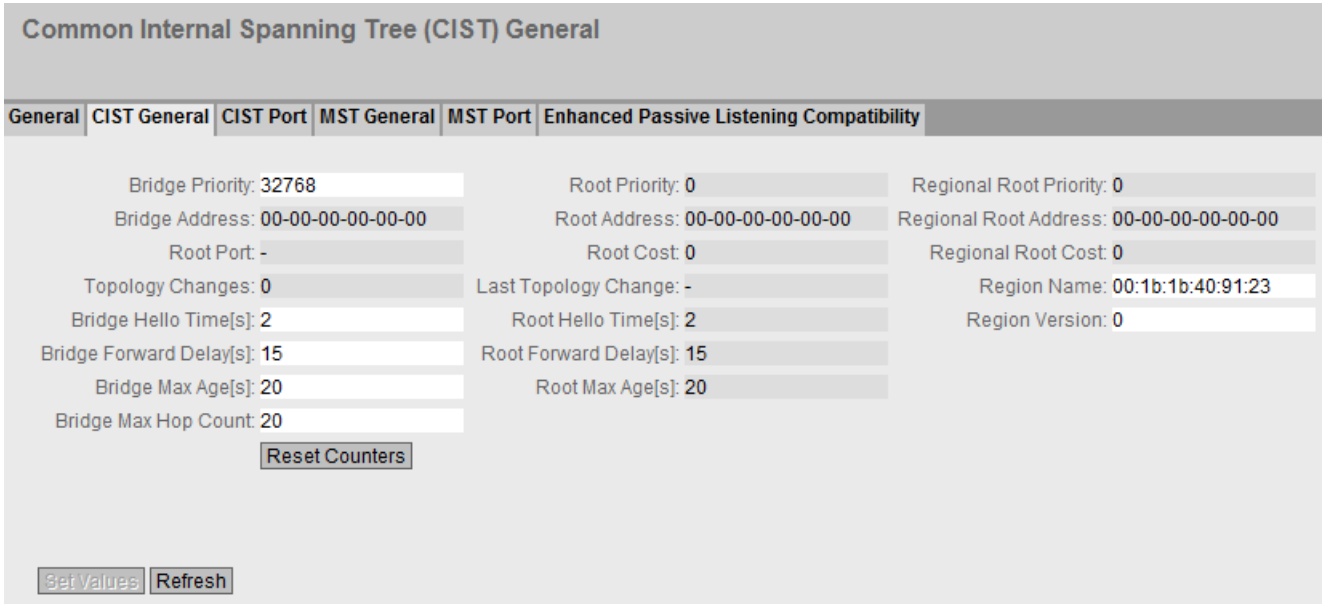
1. 选中“MSTP”复选框。
2. 从“Protocol Compatibility”下拉列表中选择兼容类型。
3. 单击“设置值”(Set Values) 按钮。

5.5.8.2 CIST 概述

MSTP-CIST 组态

此页面由以下几部分组成。

- 页面的左侧显示设备的组态。
- 中间部分显示根网桥的组态，该组态可从设备接收到的生成树帧获得。
- 右侧显示区域根网桥的组态，该组态可从设备接收到的 MSTP 帧获得。 只有在“General”页面上启用“MSTP”，并且为“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**
  Bridge Priority 指定哪个设备成为 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。 这两个参数（网桥优先级和 MAC 地址）一起形成 Bridge 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 61440。
- **网桥地址 (Bridge Address)/根地址 (Root Address)**
  网桥地址显示设备的 MAC 地址，根地址显示根网桥的 MAC 地址。
- **根端口 (Root Port)**
  显示交换机与根网桥通信时所使用的端口。
- **根成本 (Root Cost)**
  从该设备到根网桥的路径成本。

- **拓扑变更 (Topology Changes)/上次拓扑变更 (Last Topology Change)**
  该设备条目显示自上次启动以来，由于生成树机制而执行的重新组态操作次数。 对于根网桥，自上次重新组态到现在的时间显示如下：
  - 秒： 数字后的秒单位
  - 分钟： 数字后的分钟单位
  - 小时： 数字后的小时单位
- **网桥呼叫时间 [s] (Bridge hello time [s])/根呼叫时间 [s] (Root hello time [s])**
  每个网桥都会定期发送组态帧 (BPDU)。 呼叫时间即为两个此类帧之间的时间间隔。 此参数的默认值为 2 秒。
- **网桥转发延迟 [s] (Bridge forward delay [s])/根转发延迟 [s] (Root Forward Delay [s])**
  网桥不会立即使用新组态数据，而是在经过参数中指定的时间段之后才使用。 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。 此参数的默认值为 15 秒。
- **网桥最大老化时间 (Bridge Max Age)/根最大老化时间 (Root Max Age)**
  “网桥最大老化时间”定义接收到的 BPDU 可被交换机作为有效信息接受的最长“期限”。 此参数默认为 20。
- **区域根优先级 (Regional Root Priority)**
  相关描述，请参见“网桥优先级/根优先级”
- **区域根地址 (Regional Root Address)**
  设备的 MAC 地址。
- **区域根成本 (Regional Root Cost)**
  从该设备到根网桥的路径成本。
- **网桥最大跳跃数 (Bridge Max Hop Count)**
  此参数指定 BPDU 会通过多少个 MSTP 节点。 如果接收到一个 MSTP BPDU 并且其跳跃计数超过此处组态的值，则会将其丢弃。 此参数默认为 20。
- **复位计数器 (Reset Counters)**
  单击该按钮可复位此页面上的计数器。
- **区域名称 (Region Name)**
  输入此设备所属的 MSTP 区域的名称。 默认情况下，在此处输入此设备的 MAC 地址。 所有属于相同 MSTP 区域的设备上的值必须相同。
- **区域版本 (Region Version)**
  输入设备所在的 MSTP 区域的版本号。 所有属于相同 MSTP 区域的设备上的该值必须相同

组态步骤

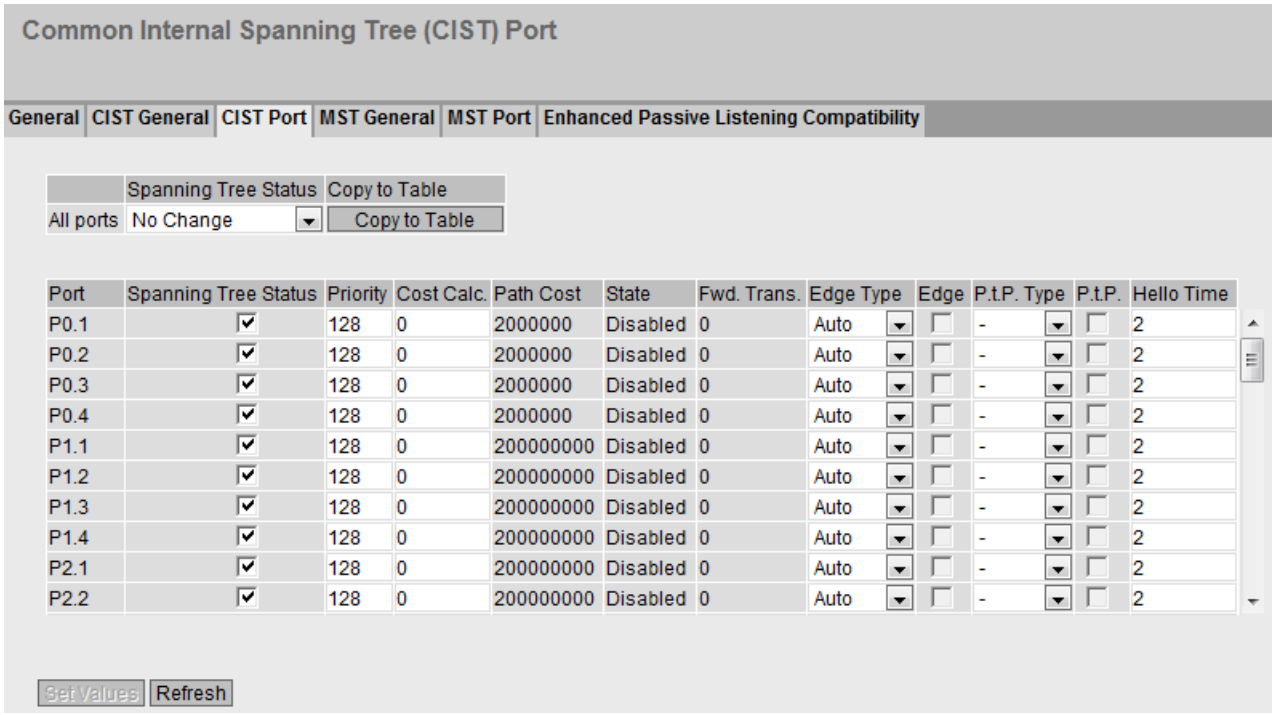
1. 在输入框中输入组态所需的数据。
2. 单击“设置值”(Set Values) 按钮。

5.5.8.3 CIST 端口

MSTP-CIST 端口组态

调用此页面时，表中显示端口参数组态的当前状态。

要进行组态，请单击端口表中的相关单元格。



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：
  - enabled
    将端口集成到生成树中。
  - disabled
    不将端口集成到生成树中。
  - 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。
  值范围： 0 - 240.
  默认值为 128。
- **开销计算 (Cost Calc)**
  输入路径开销计算。 如果输入值“0”，则自动计算出的值会显示在“Path Cost”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) 字段中的值为“0”，则会显示自动计算出的值。
  否则会显示“开销计算”(Cost Calc) 字段的值。
  路径成本的计算很大程度上基于传输速度。 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

  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。“Status”参数取决于组态的协议。
  可能的状态有：
  - Disabled
    该端口仅接收，并且不包括在 STP、MSTP 和 RSTP 中。
  - Discarding
    在“Discarding”模式下，接收 BPDU 帧。 其它进入或离开的帧会被丢弃。
  - listening

    在此状态下，接收和发送 BPDU。 端口包括在生成树算法中。
  - Learning
    转发状态之前的阶段，端口主动学习拓扑（换句话说，节点寻址）。
  - Forwarding
    在重新组态时间后，端口在网络中激活；端口接收和转发数据帧。
- **转发 传输 (Fwd. Trans)**
  指定从“Discarding”状态变为“Forwarding”状态的次数。

- **边缘类型 (Edge Type)**
  指定边缘端口的类型。 可做以下选择：
  - "-"
    禁用边缘端口。 端口被视为“无边缘端口”。
  - Admin
    当此端口上始终有终端设备时，选择此选项。 否则，每次更改连接时都会触发对网络的重新组态。
  - Auto
    如果想要自动检测此端口上连接的终端设备，则选择此选项。 首次建立连接时，会将端口视为“无边缘端口”。
  - Admin/Auto
    如果要在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，则该端口将针对交换机自动切换为“Disabled”设置。

- **点对点类型 (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。

- **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 BPDU。 默认情况下，会设置 2 秒。
  值范围： 1-2 秒

  说明

  只有在 MSTP 兼容模式下才能对呼叫时间进行端口特定的设置。

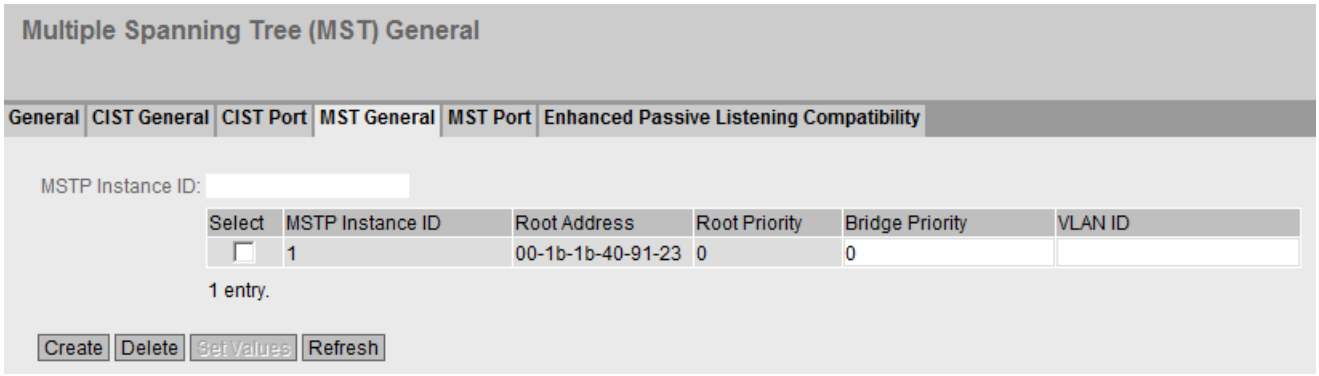
组态步骤

1. 在表行的输入单元格中，输入要组态的端口值。
2. 在表行单元格的下拉列表中，选择要组态的端口值。
3. 单击“设置值”(Set Values) 按钮。

5.5.8.4 MST 概述

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： 0 - 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。
- **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 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”输入框中输入虚拟 LAN 的标识符。
4. 在“Bridge Priority”输入框中输入网桥的优先级。
5. 单击“设置值”(Set Values) 按钮。

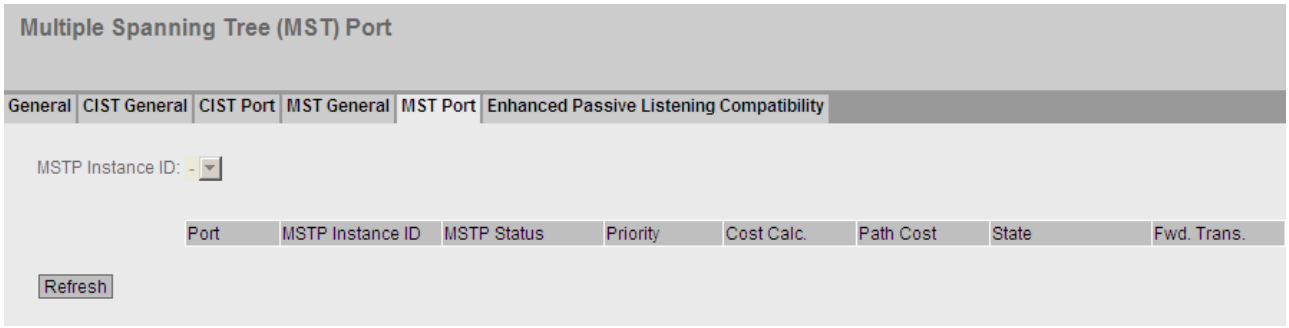
删除条目

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。

5.5.8.5 MST 端口

组态多重生成树端口参数

在此页面，设置所组态多重生成树实例的端口参数。



显示框说明

该页面包含以下框：

- 下拉列表 **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
  – 禁用
  – No Change： 表 2 保持不变。
- **复制到表中 (Copy to Table)**
  如果单击此按钮，将为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **端口 (Port)**
  显示所有可用端口和链路汇聚。
- **MSTP 实例 ID (MSTP Instance ID)**
  MSTP 实例的 ID。
- **MSTP 状态 (MSTP Status)**
  单击此复选框可启用或禁用此选项。
- **优先级 (Priority)**
  输入端口的优先级。仅当路径成本相同时才评估优先级。
  该值必须能被 16 整除。如果该值不能被 16 整除，则会自动调整该值。
  值范围：0 - 240.
  默认值为 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”，则自动计算出的值会显示在下一个“Path Cost”框中。

- **路径成本 (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“开销计算”(Cost Calc.) 字段中的值为“0”，则显示自动计算出的值。
  否则会显示“开销计算”(Cost Calc) 字段的值。
  路径成本的计算很大程度上基于传输速度。可达到的传输速度越高，路径成本的值就越低。
  快速生成树的典型值如下：
  - 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 (State)**
  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。

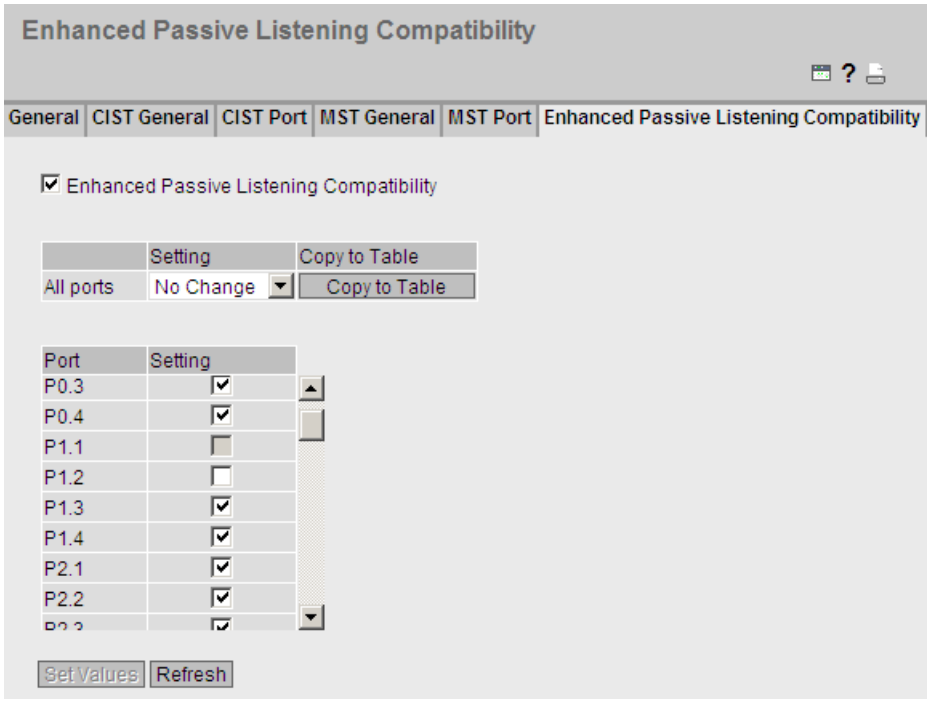
组态步骤

1. 在表行的输入单元格中，输入要组态的端口值。
2. 在表行单元格的下拉列表中，选择要组态的端口值。
3. 单击“设置值”(Set Values) 按钮。

5.5.8.6 增强的被动侦听兼容性

启用该功能

在此页面上，可启用被动侦听兼容性。



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) 复选框**
  为整个设备启用或禁用此功能。
- **“设置”(Setting) 下拉列表**
  - 启用 (enabled)
    为设备的所有端口启用该功能
  - 禁用 (disabled)
    为设备的所有端口禁用该功能
  - 无变化 (No Change)
    无变化
- **“复制到表中”(Copy to Table) 按钮**
  将在“设置”(Setting) 中所做的设置写入下表

特定端口表：
如果为整个设备启用该功能，则在各端口上启用或禁用该功能。

- **端口 (Port)**
  显示设备的端口。
- **“设置”(Setting) 复选框**
  为此端口启用或禁用该功能

组态步骤

为整个设备启用该功能

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。

对于设备的所有端口：

1. 从下拉列表中，选择该功能应启用、禁用还是保持不变。
2. 单击“复制到表中”(Copy to Table) 按钮。
3. 单击“设置值”(Set Values) 按钮。

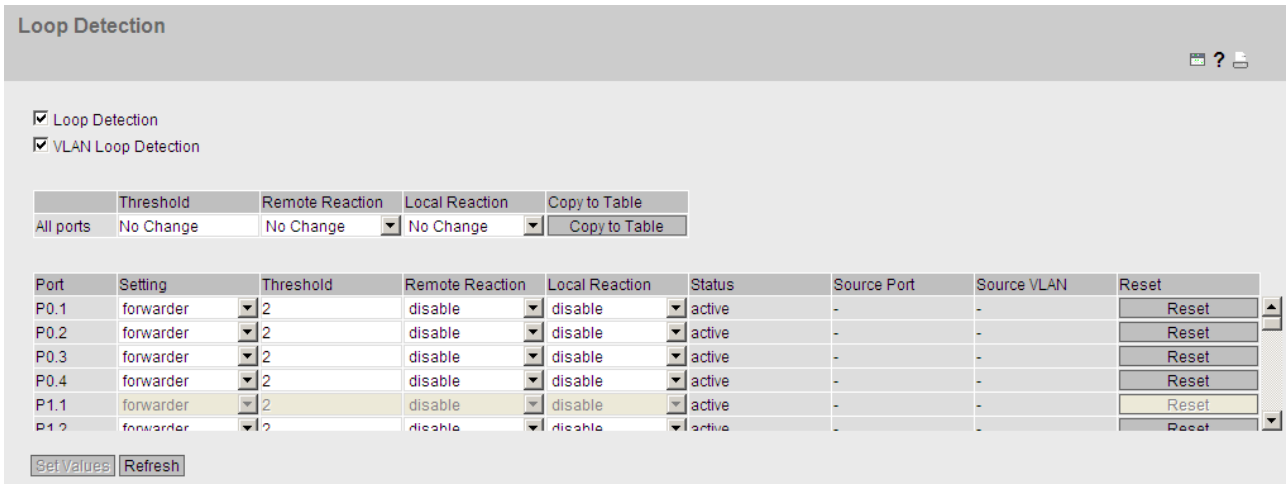
对于设备的各个端口：

1. 单击端口表中所需端口后的复选框，启用或禁用该功能。
2. 单击“设置值”(Set Values) 按钮。

5.5.9 回路检测

使用“回路检测”(Loop detection) 功能时，需指定要激活回路检测功能的端口。 所涉及的端口会发送特殊的测试帧，即回路测试帧。 如果这些帧被发送回设备，则说明存在回路。

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”。



说明

回路是必须消除的网络结构错误。 回路检测有助于更快地找到此错误，但并不会消除相关错误。 回路检测不适用于通过故意包含回路来提高网络可用性的情况。

说明

请注意，仅可为未组态为环网端口或备用端口的端口激活回路检测。

说明

- **“回路检测”(Loop detection) 选项按钮**
  启用或禁用回路检测功能。
- **“VLAN 回路检测”(VLAN loop detection)** 选项按钮
  启用或禁用 VLAN 回路检测功能。

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
- **阈值 (Threshold Value)/远程反应 (Remote Reaction)/本地反应 (Local Reaction)**
  进行所需设置。
- **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。
- **设置 (Setting)**
  指定端口处理回路检测帧的方式。 从下拉列表中选择下列选项之一：

  说明

  测试帧会导致额外的网络负载。 建议您仅在环网的分支点处等将单独的交换机组态为“Sender”，并将其它交换机组态为“Forwarder”。

  – 发送方 (Sender)
    发送并转发回路检测帧。
  – 转发方 (Forwarder)
    转发来自其它设备的回路检测帧。
  – 阻止 (blocked)
    阻止转发回路检测帧。
- **阈值 (Threshold)**
  通过输入一个数值指定接收到多少回路检测帧后才视为存在回路。
- **远程反应 (Remote reaction)**
  指定在出现远程回路时端口的响应方式。 从下拉列表中选择两个选项之一：
  – 无操作 (No action)： 回路对端口不起作用。
  – 禁用 (Disable)： 屏蔽端口。
- **本地反应 (Local reaction)**
  指定在出现本地回路时端口的响应方式。 从下拉列表中选择两个选项之一：
  – 无操作 (No action)： 回路对端口不起作用。
  – 禁用 (Disable)： 屏蔽端口
- **状态 (Status)**
  该框显示对此端口是启用还是禁用回路检测。
- **源端口 (Source port)**
  显示触发了上一次响应的回路检测帧的输出端口。
- **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。
  该选项仅当之前在“回路检测组态”(Loop Detection Configuration) 页面上选择了“启用 VLAN 支持”(VLAN Support Enabled) 时才可用。
- **复位 (Reset)**
  消除网络中的回路后，可单击“复位计数器”(Reset counters) 按钮再次复位端口。

5.5.10 链路汇聚

捆绑网络连接以实现冗余和更高带宽

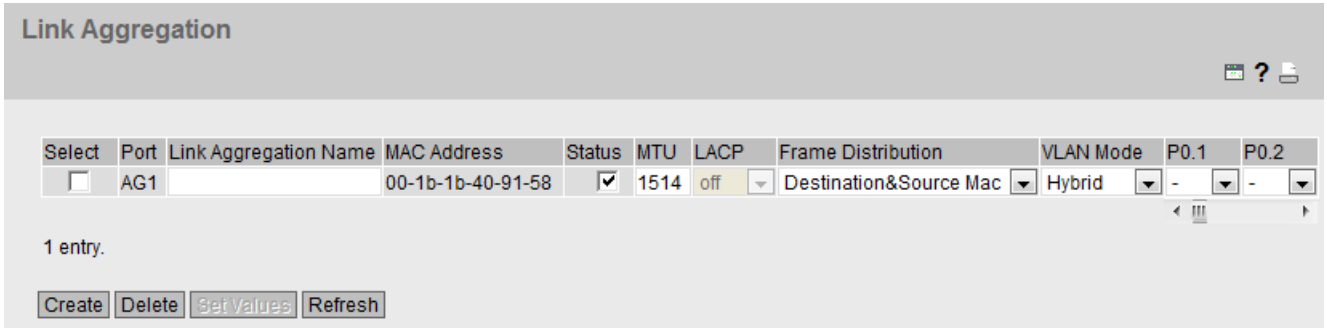
根据 IEEE 802.3ad，链路汇聚允许将相邻设备之间的多个连接捆绑在一起，以实现更高的带宽并防止发生故障。

两个伙伴设备中的端口均包括在链路汇聚中，通过这些端口连接设备。 要将端口（或者说链路）正确分配给伙伴设备，应使用 IEEE 802.3ad 标准中的链路汇聚控制协议 (LACP)。

可最多定义 8 个链路汇聚。 最多可为每个链路汇聚分配 8 个端口。

显示已组态的汇聚

该菜单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：

- **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。
- **MTU**
  指定包大小。
- **LACP**
  - 启用 (On)
    启用发送 LACP 帧。
  - 禁用 (Off)
    禁用发送 LACP 帧。
- **帧分发 (Frame Distribution)**
  设置汇聚的各个连接上的数据包分发类型。
  - 目标和源 MAC (Destination&Source MAC)
    根据目标 MAC 地址与源 MAC 地址的组合进行分发。
  - 目标和源 IP MAC (Destination&Source IP MAC)
    根据目标和源 IP 和 MAC 地址的组合进行分发。
- **VLAN 模式 (VLAN Mode)**
  指定在 VLAN 中如何登记链路汇聚：
  - 混合 (Hybrid)
    链路汇聚发送有标记和无标记的帧。它不会自动成为 VLAN 的成员。
  - 中继 (Trunk)
    链路汇聚仅发送有标记的帧，并且自动成为所有 VLAN 的成员。
- **端口 (Port)**
  显示属于此链路汇聚的端口。 可以从下拉列表中选择下列值：
  - "-”（禁用）
    禁用链路汇聚。
  - "a”（主动）
    端口发送 LACP 帧，并只在接收到 LACP 帧时参与链路汇聚。
  - "p”（被动）
    端口只在接收到 LACP 帧时参与链路汇聚。
  - "o”（启用）
    端口参与链路汇聚，并且不会发送任何 LACP 帧。

  说明

  在“链路汇聚”内，仅可使用具有以下组态的端口：
  - 所有带“o”的端口
  - 所有带“a”或“p”的端口。

组态步骤

组态前的基本设置

1. 首先，确定想要组合在一起，在设备之间形成链路汇聚的端口。
2. 在设备上组态链路汇聚。
3. 对所有设备采用该组态。
4. 执行最后一步，布线。

说明

如果在组态之前用电缆连接已汇聚的链路，则可能在网络中形成环路！ 因此可能使相关网络变得糟糕或者完全瘫痪。

创建新链路汇聚

1. 单击“Create”按钮以创建新的链路汇聚。
   此操作将创建一个新行。
2. 选择属于此链路汇聚的端口。
3. 单击“设置值”(Set Values) 按钮。

删除汇聚

1. 使用行开始位置的复选框，选择要删除的链路汇聚。
2. 单击“删除”(Delete) 按钮。

更改汇聚

1. 在总览中，单击相关的表条目来更改所创建链路汇聚的组态。
2. 进行所有更改。
3. 单击“设置值”(Set Values) 按钮。

5.5.11 DCP 转发

应用

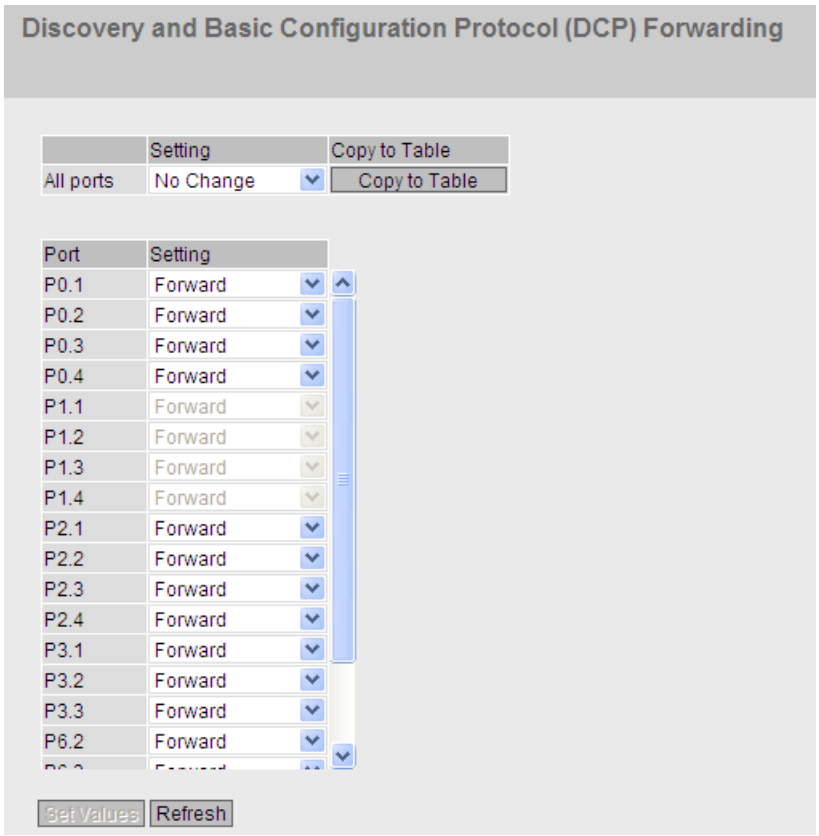
STEP 7 和 PST 工具使用 DCP 协议组态和诊断。 发货时，对所有端口都启用 DCP；换句话说，在所有端口都转发 DCP 帧。 利用此选项，可以针对每个端口禁止发送这些帧，例如，防止使用 PST 工具组态网络的各个部分，或者将整个网络分成多个较小部分，以进行组态和诊断。

说明

PNIO 组态

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

表 2 包含以下列：

- **端口 (Port)**
  显示可用端口。 端口由模块号和端口号组成，例如，端口 0.1 表示模块 0，端口 1。
- **设置 (Setting)**
  从该下拉列表中，选择端口是应阻止还是转发出站 DCP 帧。 可做以下选择：
  - **转发 (Forward)**
    通过此端口转发 DCP 帧。
  - **阻止 (Block)**
    不通过此端口转发出站 DCP 帧。 不过，仍可通过此端口接收帧。

组态步骤

1. 通过行中下拉列表内的选项，选择支持发送 DCP 帧的端口。
2. 单击“设置值”(Set Values) 按钮。

5.5.12 LLDP

识别网络拓扑

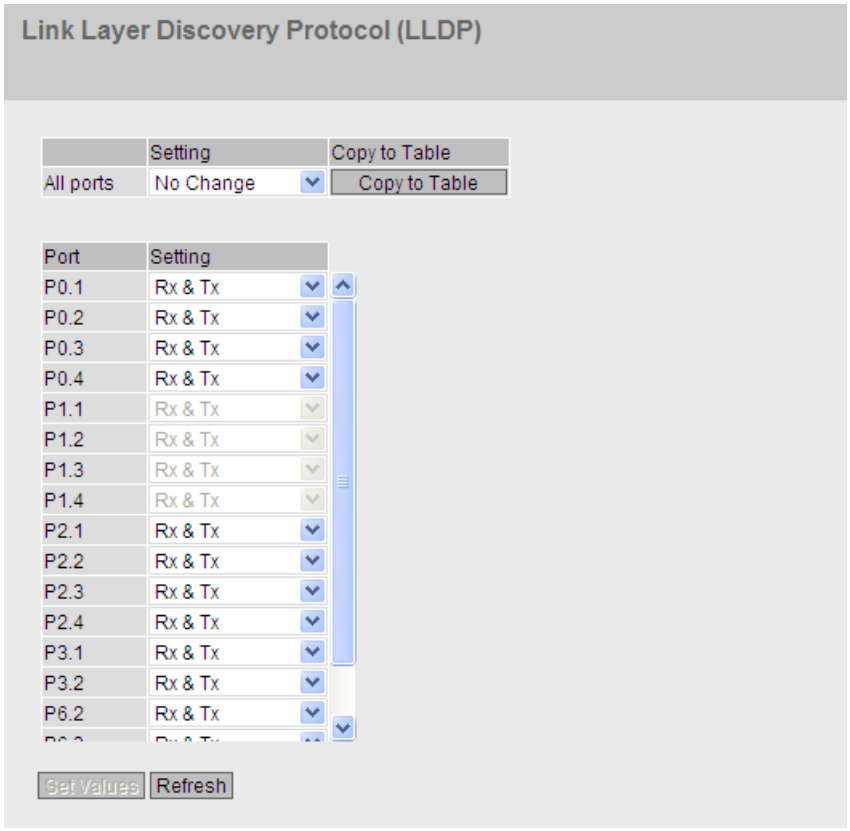
IEEE 802.AB 标准中定义了 LLDP（Link Layer Discovery Protocol，链路层发现协议）。

LLDP 是一种用来发现网络拓扑的方法。 网络组件使用 LLDP 与其相邻设备交换信息。

支持 LLDP 的网络组件具有 LLDP 代理。 LLDP 代理会定期发送与其自身有关的信息，并从所连接设备接收信息。 接收到的信息存储在 MIB 中。

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。
- **设置 (Setting)**
  从下拉列表中选择设置。如果选择“无变化”(No Change)，则表 2 中的条目保持不变。
- **复制到表中 (Copy to Table)**
  如果单击此按钮，将为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **端口 (Port)**
  显示端口。
- **设置 (Setting)**
  从该下拉列表中，选择端口将发送还是接收 LLDP 帧。 可做以下选择：
  - Rx
    此端口只能接收 LLDP 帧。
  - Tx
    此端口只能发送 LLDP 帧。
  - Rx & Tx
    此端口可以发送和接收 LLDP 帧。
  - "-" (disabled)
    此端口既不接收也不发送 LLDP 帧。

组态步骤

1. 在要组态的端口的行内，通过其下拉列表选择 LLDP 功能。
2. 单击“设置值”(Set Values) 按钮。

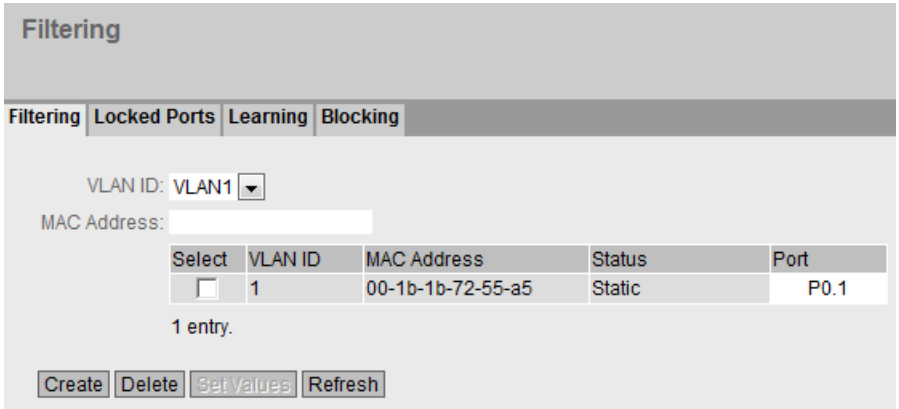
5.5.13 单播

5.5.13.1 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。



显示框说明

该页面包含以下框：

- **VLAN ID**
  选择 VLAN ID，以此来组态新静态 MAC 地址。 如果未进行任何设置，则会将“VLAN1”设置为基本设置。
- **MAC 地址 (MAC Address)**
  在此处输入 MAC 地址。

该表包含以下各列：

- **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 (Status)**
  显示每个地址条目的状态：
  - 静态 (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。
  - 无效 (Invalid)
    不评估这些值。
- **端口**
  显示访问指定地址的节点时所使用的端口。 设备接收到的目标地址与此地址相匹配的帧将被转发到此端口。

  说明

  您只能为单播地址指定一个端口。

组态步骤

要编辑条目，请按以下步骤操作。

创建新条目

1. 选择相关 VLAN ID。
2. 在“MAC Address”输入框中输入 MAC 地址。
3. 单击“Create”按钮在表中创建新条目。

4. 从下拉列表中选择相关端口。
5. 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。

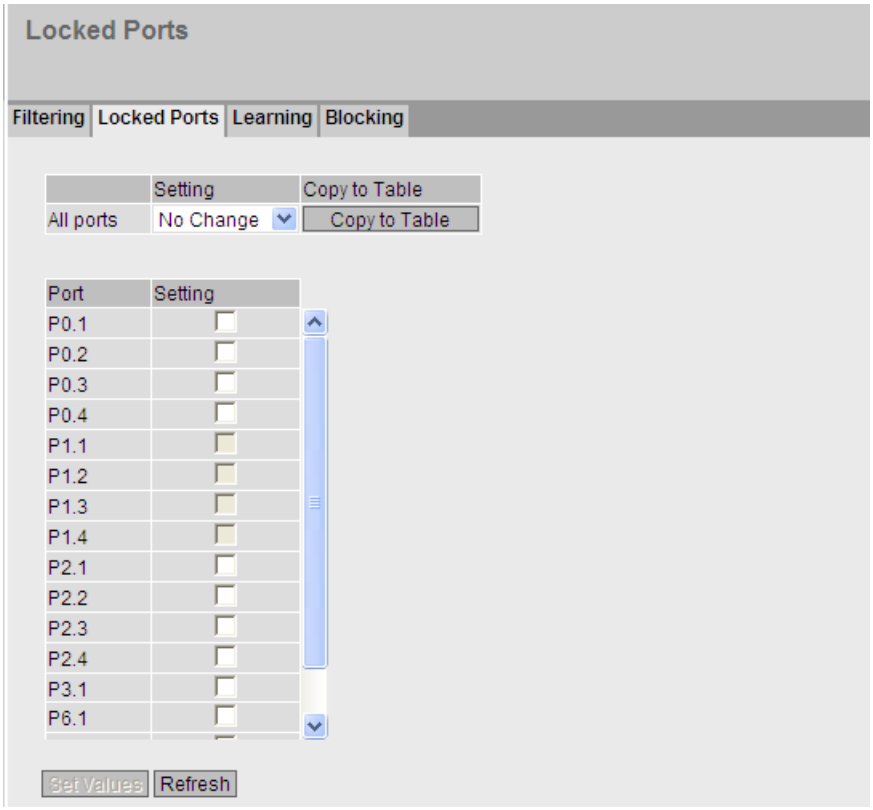
5.5.13.2 锁定端口

激活访问控制

在此页面中，可以针对未知节点阻止各个端口。

如果启用了“端口锁定”功能，则从未知 MAC 地址到达此端口的数据包会被立即丢弃。端口会接受已知节点发出的数据包。
由于启用了“端口锁定”功能的端口无法获取任何 MAC 地址，因此在启用“端口锁定”功能后，这些端口上之前获取的地址将被自动删除。
该端口仅接受之前手动创建或使用“Start Learning”功能和“Stop Learning”功能创建的静态 MAC 地址。

要自动输入所有连接的节点，可使用自动获取功能（请参见“Layer 2 > Unicast > Learning”）。



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
    启用端口锁定功能。
  - disabled
    禁用端口锁定功能。
  - 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。
- **复选框“Setting”**
  启用或禁用对端口的访问控制。

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“Setting”下拉列表中，选择“enabled”条目。
2. 单击“Copy to Table”按钮。 将为表 2 中的所有端口启用该复选框。
3. 要应用更改，请单击“Set Values”按钮。

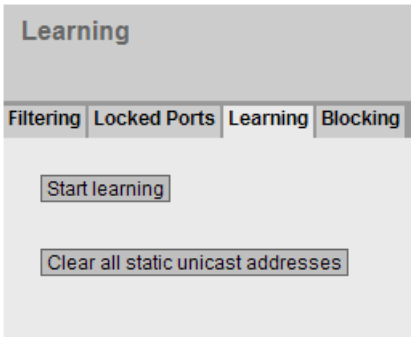
5.5.13.3 学习

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输入所有相连的设备。 只要启用“Start learning”功能，所有学习的单播地址就会立即被创建为静态单播条目。
只有单击“Stop learning”按钮后，才会结束学习过程。 使用此方法时，较大网络中的学习过程可能会花费数分钟或数小时，才能真正学习到所有节点。 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。
   此按钮再次被“Start Learning”按钮所代替。 存储已学习的条目。

删除所有静态单播地址。

1. 单击“Clear all static unicast addresses”按钮可删除所有静态条目。
   在具有许多节点的大型网络中，自动学习可能导致大量不需要的静态条目。 为避免必须分别删除这些条目，可使用此按钮删除所有静态条目。 自动学习期间会禁用此功能。

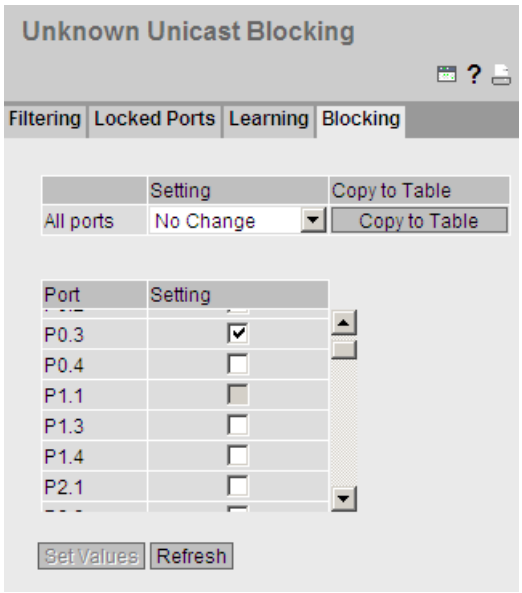
说明

根据涉及的条目数，删除过程可能需要一些时间。

5.5.13.4 单播阻止

阻止转发未知单播帧

在此页面上，可阻止各个端口转发未知单播帧。



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：
  - enabled
    启用单播帧阻止功能。
  - disabled
    禁用单播帧阻止功能。
  - 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)**
  启用或禁用单播帧阻止功能。

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。

组态步骤

对单独的端口启用阻止功能

1. 选中表 2 相关行中的复选框。
2. 要应用更改，请单击“设置值”(Set Values) 按钮。

对所有端口启用阻止功能

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

5.5.14 组播

5.5.14.1 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

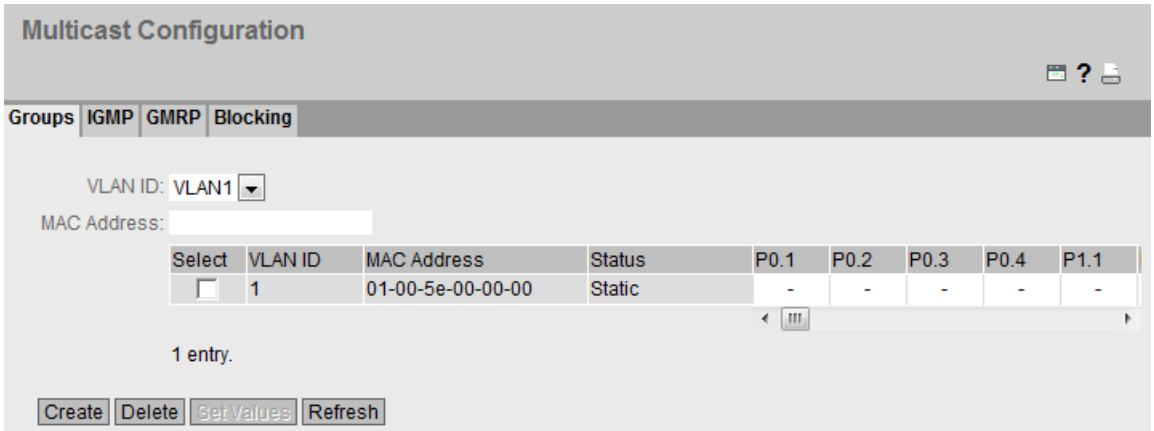
与单播帧相反，组播帧将对设备造成更高的负载。 一般来说，组播帧会被发送到所有端口。有三种方法可以减少由组播帧产生的负载：

- 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。

组态组播地址



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：

- **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。 该下拉列表提供以下选项：
  - M
    （成员）通过此端口发送组播帧。
  - F
    （已禁止）不是组播组的成员。 此地址也不能是使用 GMRP 或 IGMP 动态学习的地址。
  - –
    不是组播组的成员。 不通过此端口发送包含所定义组播 MAC 地址的组播帧。

组态步骤

创建新条目

1. 在“VLAN ID”文本框中指定所需的 ID。
2. 在“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。
   将从显示画面以及设备的内存中删除该行。

5.5.14.2 IGMP

功能

工业以太网交换机支持“IGMP 监听”和“IGMP 查询器”功能。 如果启用“IGMP snooping”，就会评估 IGMP 帧，并用该评估信息更新组播过滤表。如果还启用了“IGMP 查询器”，则工业以太网交换机还会发送可触发 IGMP 兼容节点响应的 IGMP 查询。

IGMP 监听老化时间

在此菜单中，可以组态“IGMP 组态”的老化时间。 经过该时间后，如果 IGMP 创建的条目未被新的 IGMP 帧更新，将从地址表中删除这些条目。

这适用于所有端口；但无法对具体端口进行组态。

取决于查询器的 IGMP 监听老化时间

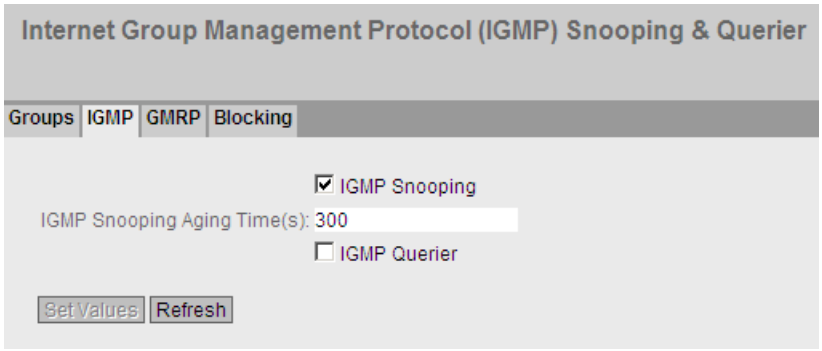
SCALANCE XR500 作为 IGMP 查询器

如果 SCALANCE XR500 用作 IGMP 查询器，则查询间隔为 125 秒。对于“IGMP 监听老化时间”(IGMP Snooping Aging Time)，至少设置为 250 秒。

其它 IGMP 查询器

如果使用其它 IGMP 查询器，则“IGMP 监听老化时间”(IGMP Snooping Aging Time) 的值应至少为查询间隔的 2 倍。

显示框说明



该页面包含以下框：

- **IGMP 监听 (IGMP Snooping)**
  启用或禁用 IGMP（Internet 组管理协议）。 该功能允许将 IP 地址分配给组播组。 如果选中该复选框，IGMP 条目将包括在表中，并且 IGMP 帧会被转发。
- **IGMP 监听老化时间 (IGMP Snooping Aging Time)**
  在此框中，输入老化时间的秒数值。默认情况下，会设置 300 秒。
  有效值为： 130 - 300（秒）
- **IGMP 查询器 (IGMP Querier)**
  启用或禁用“IGMP 查询器”(IGMP Querier)。 设备会发送 IGMP 查询。

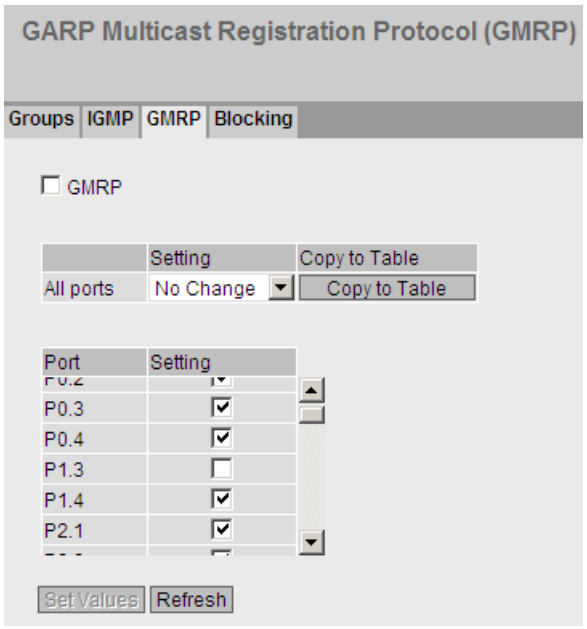
组态步骤

1. 选中“IGMP Snooping”复选框。
2. 在“IGMP Snooping Aging Time”框中，输入老化时间的秒数值。
3. 选中“IGMP Querier”复选框。
4. 单击“设置值”(Set Values) 按钮。

5.5.14.3 GMRP

激活 GMRP

通过选中该复选框，来指定是否对各个端口使用 GMRP。 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。



显示框说明

该页面包含以下框：

- **“GMRP”复选框**
  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。
- **设置 (Setting)**
  从下拉列表中选择设置。 可选择以下设置选项：
  - enabled
    启用发送 GRMP 帧。
  - disabled
    禁用发送 GRMP 帧。
  - 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 的所有端口应用这些设置。

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。
- **Setting**
  使用此复选框，可针对每个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. 选中“GRMP”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。

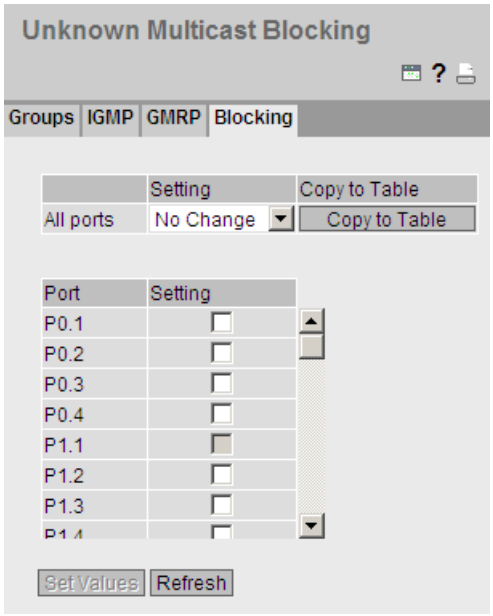
针对所有端口启用发送 GMRP 帧

1. 选中“GRMP”复选框。
2. 在“Setting”下拉列表中，选择“enabled”条目。
3. 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。
4. 要应用更改，请单击“Set Values”按钮。

5.5.14.4 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)
    启用组播帧阻止功能。
  - 禁用 (disabled)
    禁用组播帧阻止功能。
  - 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。

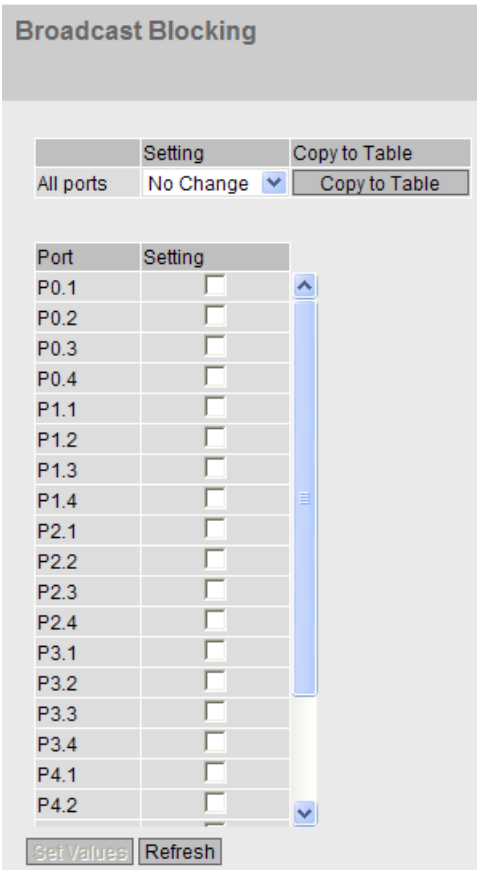
5.5.15 广播

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，只有确实不需要广播时，才阻止广播。



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
    对广播帧的阻止已启用。
  - disabled
    对广播帧的阻止已禁用。
  - 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**
  显示所有可用端口及链路汇聚。
- **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“Set Values”按钮。

针对所有端口启用对广播帧的阻止

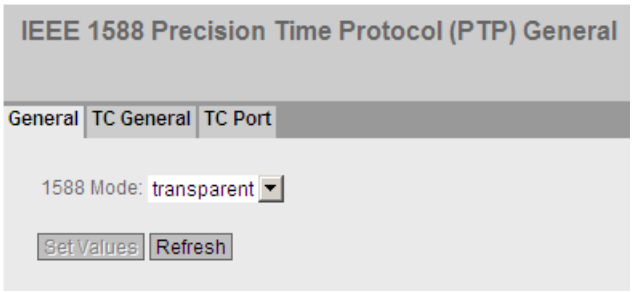
1. 在“Setting”下拉列表中，选择“enabled”条目。
2. 单击“Copy to Table”按钮。 将为表 2 中的所有端口启用该复选框。
3. 要应用更改，请单击“Set Values”按钮。

5.5.16 PTP（仅 SCALANCE XR-500）

5.5.16.1 General

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对设备执行“复位为出厂默认设置”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。



1588 组态

在此页面中，可指定设备处理 PTP 消息的方式。

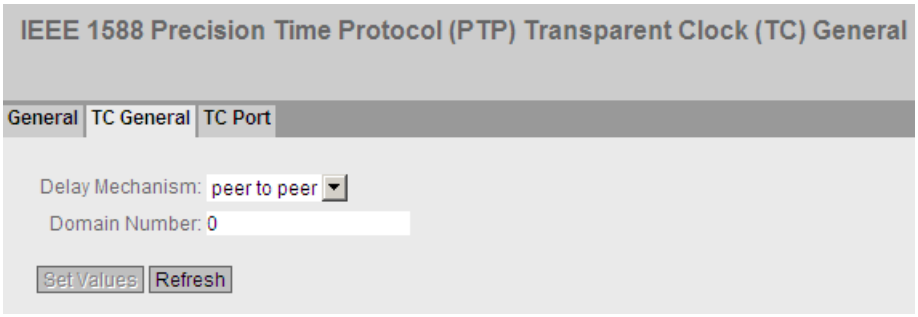
1588 模式 (1588 Mode)
可进行以下设置：

- **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。

5.5.16.2 TC General

TC 常规

在此选项卡上提供有 PTP 常规设置。



1588 透明时钟组态

延时机制 (Delay Mechanism)
指定设备将使用的延时机制：

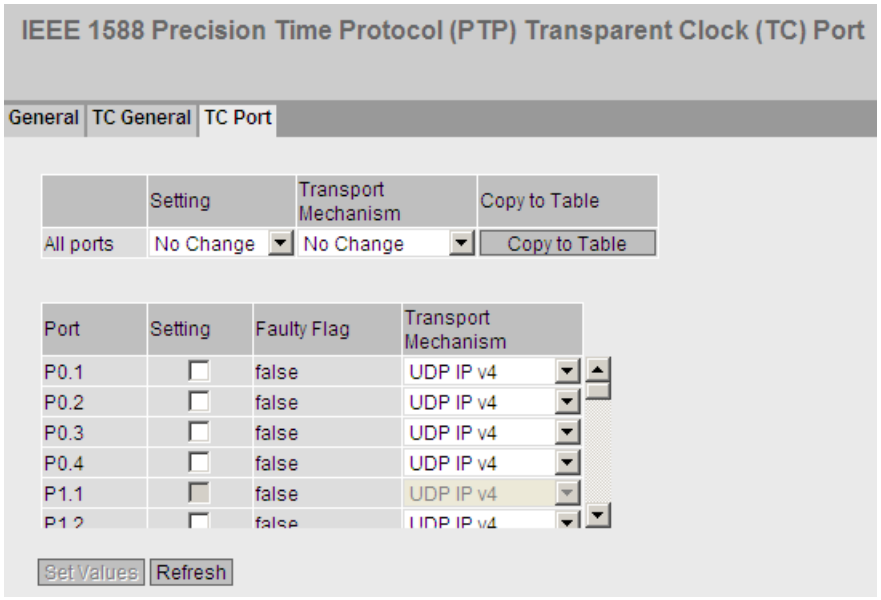
- 端对端 (End-to-end)（将使用延迟请求响应机制）
- 对等 (Peer-to-peer)（将使用对等延迟机制）

域编号 (Domain Number)
在此处输入设备的域编号。 设备将忽略具有不同域编号的 PTP 消息。 一个 SCALANCE 设备只能分配给一个同步域。

5.5.16.3 TC Port

TC 端口

此选项卡中包含 PTP 的端口设置。



1588 透明时钟端口参数

该表显示了各个端口的详细信息：

- **端口 (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。
- **设置 (Setting)**
  端口状态。 可以是以下条目：
  - 禁用 (disabled)
    端口不包括在 PTP 中。
  - 启用 (enabled)
    端口处理 PTP 消息。

- **故障标志 (Faulty Flag)**
  与 PTP 有关的错误状态。
  - 真 (true)
    发生错误。
  - 假 (false)
    该端口未发生错误。
- **传输机制 (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：
  - 以太网
  - UDP IPv4

5.5.17 RMON

5.5.17.1 统计信息

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“数据包大小”(Packet Size)、“数据包类型”(Packet Type) 和“数据包错误”(Packet Error) 选项卡的“信息 > 以太网统计信息”(Information > Ethernet Statistics) 页面中。

设置

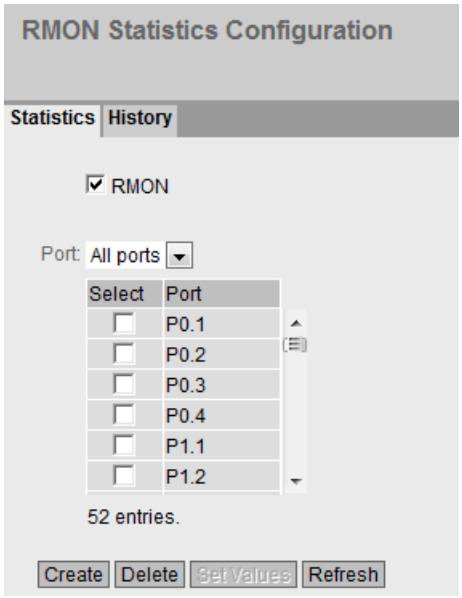


图 5-14　　RMON 统计信息

- **RMON**
  如果选择该复选框，则远程监视 (RMON) 允许在设备上收集和准备诊断数据，并由同样支持 RMON 的网络管理站使用 SNMP 读出诊断数据。 凭借此诊断数据（例如，端口相关的负载趋势）可以在早期发现并排除网络中的故障。

  说明
  如果禁用 RMON，这些统计信息不会被删除，而会保持其前一个状态。

- **Port**
  选择要显示其统计信息的端口。

该表格包括以下列：

- **Select**
  选择要删除的行。
- **Port**
  表示要显示其统计信息的端口。

5.5.17.2 历史

统计信息的样本

在此页面中，可以指定是否保存端口的统计信息样本。 可以指定要保存的条目数量和采集样本的时间间隔。

设置

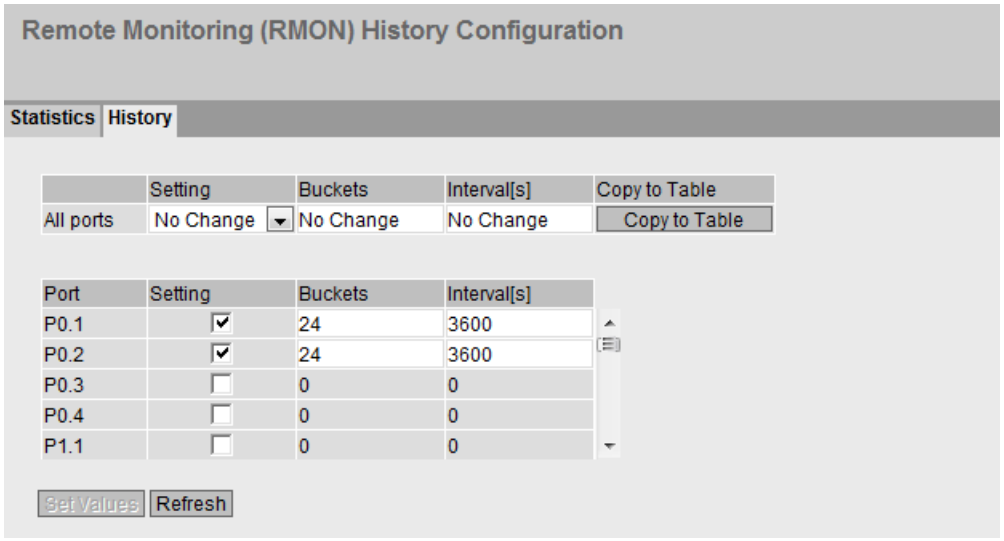


图 5-15 RMON 历史

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状态保存为样本的间隔。 如果输入“No Change”，则表 2 中的条目保持不变。
- **Copy to Table**
  如果单击此按钮，则为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **端口**
  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。
- **Interval[s]**
  输入将统计信息的当前状态保存为样本的间隔。

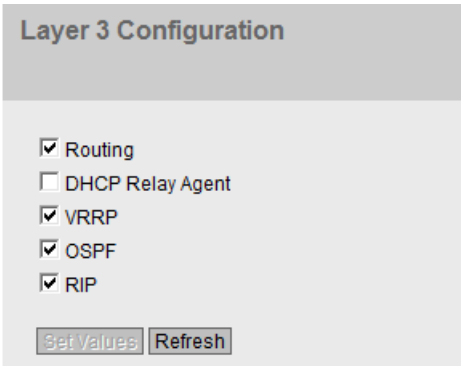
5.6 “Layer 3”菜单

5.6.1 组态

简介

该页面包含设备第 3 层功能的概览。 在此页面上启用或禁用所需的第 3 层功能。

只对第 3 层提供“路由”(Routing)、“VRRP”、“RIP”和“OSPF”功能。



显示框说明

该页面包含以下框：

- **路由 (Routing)**（仅适用于具有第 3 层许可证的设备）
  启用或禁用路由功能。

  说明
  仅当禁用所有已组态接口上的 DHCP 时才能启用路由功能。

- **DHCP 中继代理 (DHCP Relay Agent)**
  启用或禁用 DHCP 中继代理。 可以在“Layer 3 > DHCP Relay Agent”中组态其它设置。

- **VRRP**（如果启用了“路由”(Routing)，则仅适用于具有第 3 层许可证的设备）
  启用或禁用基于 VRRP 的路由。 要使用 VRRP，应先启用路由功能。 可以在“Layer 3 > VRRP”中组态其它设置。

- **VRRP**（如果启用了路由，则仅适用于具有第 3 层许可证的设备）
  启用或禁用基于 OSPF 的路由。 可以在“Layer 3 > OSPF”中组态其它设置。
- **RIP**（如果启用了路由，则仅适用于具有第 3 层许可证的设备）
  启用或禁用基于 RIP 的路由。 可以在“Layer 3 > RIP”中组态其它设置。

组态步骤

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

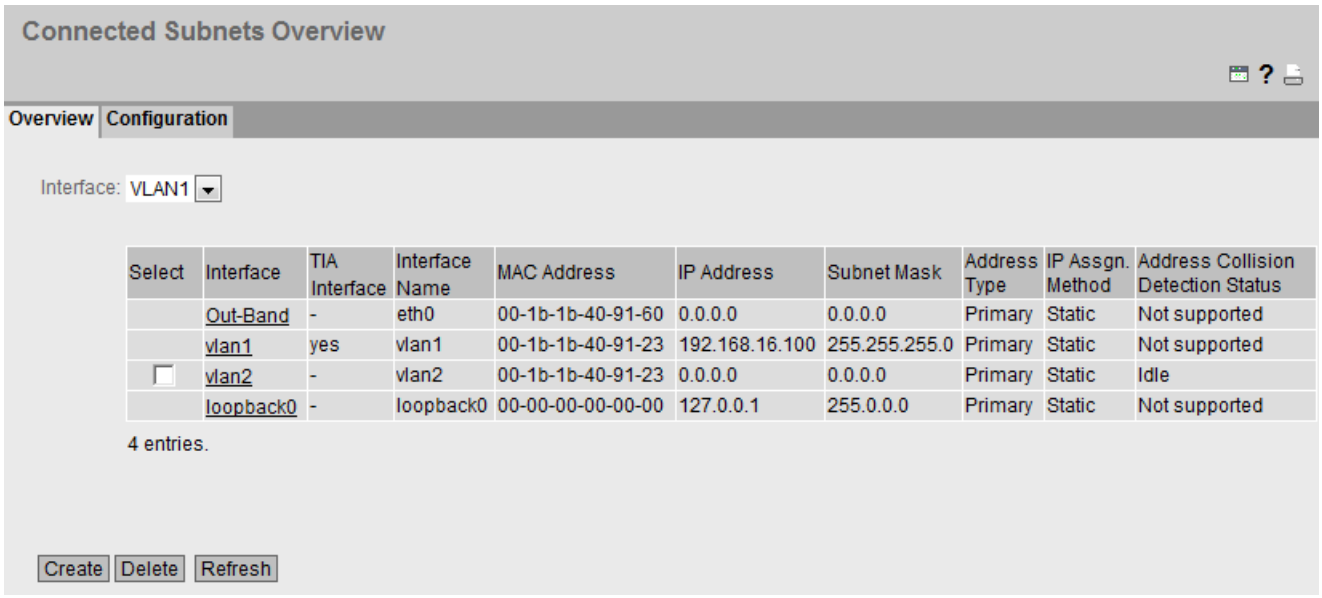
5.6.2 子网

5.6.2.1 概述

创建子网

此页面会显示所选接口的子网。 如果接口有多个可用子网，则该接口第一个条目是地址类型为“Primary”的子网。

在此页面中创建所有其它子网。 子网总是与接口相关。 在“Configuration”选项卡中创建接口。



显示值说明

该页面包含以下框：

- **接口 (Interface)**
  在“接口”(Interface) 下拉列表中，选择要为其组态其它子网的接口。

该表格包括以下列：

- **Select**
  选择要删除的行。
- **接口 (Interface)**
  显示接口。
- **TIA 接口 (TIA Interface)**
  显示所选的 TIA 接口。
- **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 IP 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 IP 接口上组态的首个 IP 地址。
  - Secondary
    在 IP 接口上组态的其它所有 IP 地址。

- **IP 分配方法 (IP Assign. Method)**
  显示如何分配 IP 地址。 可能的值包括：
  - 静态 (Static)
    IP 地址是静态的。 在“IP 地址”(IP Address) 和 “子网掩码”(Subnet Mask) 中输入 IP 设置。
  - 动态 (DHCP) (Dynamic (DHCP))
    设备从 DHCP 服务器获得动态 IP 地址。
- **地址冲突检测状态 (Address Collision Detection Status)**
  如果网络中激活新的 IP 地址，则“地址冲突检测”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 IP 地址。

  说明

  此功能不执行周期性检查。

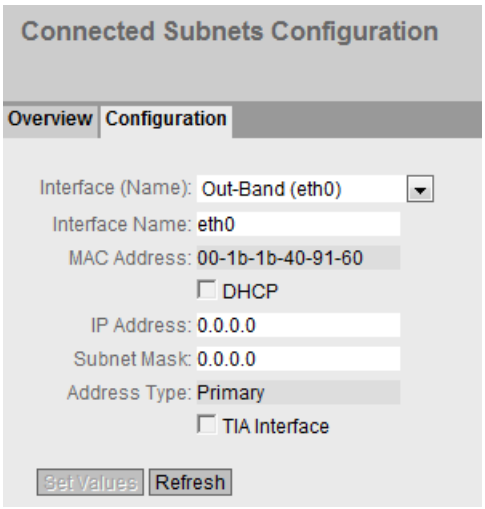
  此列显示功能的当前状态。可能的值包括：
  - Idle
    未启用该接口，因此也没有 IP 地址。
  - Starting
    该状态表示启动阶段。在该阶段中，设备首先会发送查询，以了解规划的 IP 地址是否已经存在。如果该地址尚未分配，设备将发送现在开始使用此 IP 地址的消息。
  - Conflict
    接口未启用。 接口试图使用已经分配的 IP 地址。
  - Defending
    接口使用唯一的 IP 地址。另一接口正试图使用相同的 IP 地址。
  - Active
    接口使用唯一的 IP 地址。未发生冲突。
  - Not supported
    不支持地址冲突检测功能。
  - Disabled
    禁用地址冲突检测功能。

组态步骤

1. 从“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。 在“Configuration”选项卡中组态子网。

5.6.2.2 组态

在此页面上指定接口的名称。



显示值说明

该页面包含以下框：

- **接口（名称）(Interface (Name))**
  从下拉列表中选择接口。
- **接口名称 (Interface Name)**
  输入接口名称。
- **MAC 地址 (MAC Address)**
  显示所选接口的 MAC 地址。
- **DHCP**
  为此 IP 接口启用或禁用 DHCP 客户端。

  说明
  如果想要将设备作为多个接口的路由器运行，则需禁用所有接口上的 DHCP。
- **IP 地址 (IP Address)**
  输入接口的 IP 地址。 IP 地址不能多次使用。
- **子网掩码 (Subnet Mask)**
  输入要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 (Primary)
    接口的第一个子网。
  - 辅助 (Secondary)
    接口的所有其它子网。
- **TIA 接口 (TIA Interface)**
  指定该接口是否将成为 TIA 接口。

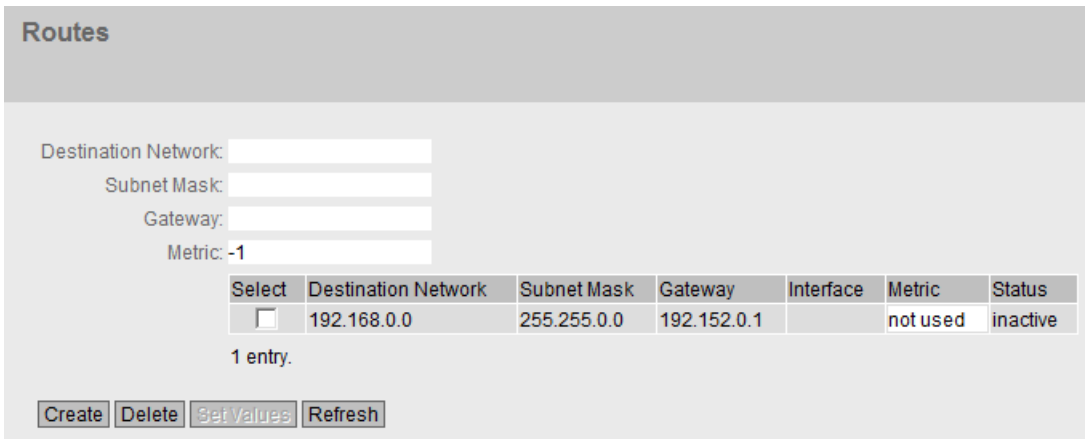
组态步骤

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

5.6.3 路由

静态路由

在此页面上创建静态路由。



显示值说明

该页面包含以下框：

- **目标网络 (Destination Network)**
  输入目标的网络地址。
- **子网掩码 (Subnet Mask)**
  输入相应的子网掩码。
- **网关 (Gateway)**
  输入相邻网关的 IP 地址。
- **Metric**
  输入路由的度量。度量对应于连接质量，如速度、成本。 如果存在多条等效路由，则会使用度量值最小的路由。
  值范围：1 - 254

该表格包括以下列：

- **Select**
  选择要删除的行。
- **目标网络 (Destination Network)**
  显示目标的网络地址。
- **子网掩码 (Subnet Mask)**
  显示相应的子网掩码。
- **网关 (Gateway)**
  显示相邻网关的 IP 地址。
- **接口 (Interface)**
  显示路由的接口。
- **Metric**
  输入路由的度量。 创建路由时，会自动输入“not used”。 度量对应于连接质量，如速度、成本。如果存在多条等效路由，则会使用度量值最小的路由。
  值范围： 1 - 254
- **状态 (Status)**
  显示路由是否激活。

组态步骤

1. 在“Destination Network”输入框中输入目标的网络地址。
2. 在“Subnet Mask”输入框中输入相应的子网掩码。

3. 在“Gateway”输入框中输入网关。
4. 在“Metric”中输入路由的权重。
5. 单击“创建”(Create) 按钮。 会在表中生成一个新条目。
6. 单击“设置值”(Set Values) 按钮。

5.6.4 Route Maps

5.6.4.1 General

路由映射

利用路由映射，可控制进一步处理路由信息的方式。 可以过滤路由信息并指定进一步处理、修改还是丢弃信息。

根据以下原理操作路由映射：

- 将路由信息与路由映射的过滤器进行比较。
- 比较过程会持续到路由映射的过滤器与信息项的属性匹配为止。
- 随后根据路由映射设置对信息进行处理：
  - 丢弃路由信息。
  - 更改路由信息的属性。

设置

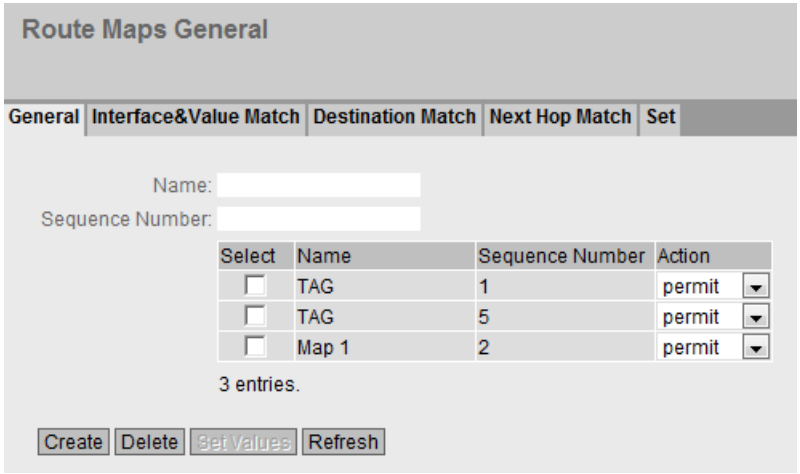


图 5-16 路由映射常规

- **Name**
  输入路由映射的名称。
- **Sequence Number**
  输入路由映射的编号。
  可创建多个名称相同但顺序号不同的路由映射。 顺序号指定路由映射的处理顺序。

该表格包括以下列：

- **Select**
  选择要删除的行。
- **Name**
  显示路由映射的名称。
- **Sequence Number**
  显示路由映射的顺序号。
- **Action**
  指定对匹配路由映射设置的路由信息所执行的操作：
  - permit
    根据在“设置”(Set) 选项卡中进行的设置进一步处理路由信息。
  - deny
    丢弃路由信息。

5.6.4.2 Inferface&Value Match

在此页面中，可以指定是否根据接口、度量或变量来过滤路由映射的路由信息。

设置

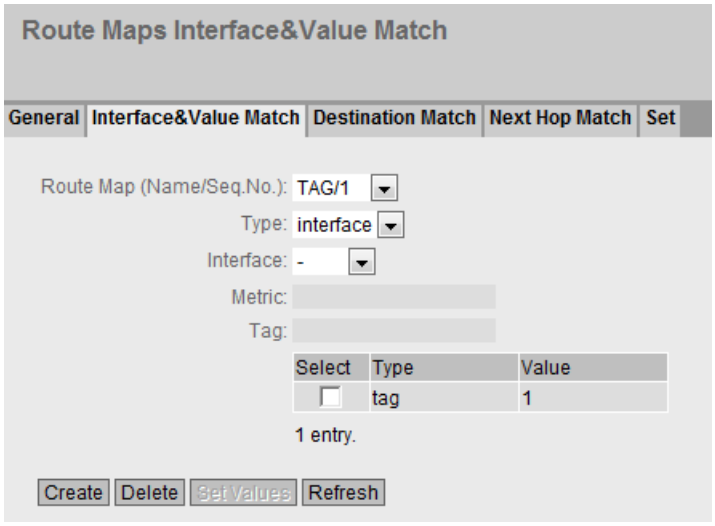


图 5-17　　路由映射接口和度量匹配

- **Route Map (Name/Seq.No.)**
  选择路由映射。
  您可以使用已创建的路由映射。
- **Type**
  选择过滤的依据：
  – Interface
  – Metric
  – Tag
- **Interface**
  选择接口。
  只有从“Type”下拉列表中选择了“Interface”条目后，才能激活该框。
- **Metric**
  输入度量的值。
  只有从“Type”下拉列表中选择了“Metric”条目后，才能激活该框。
- **Tag**
  输入变量的值。
  只有从“Type”下拉列表中选择了“Tag”条目后，才能激活该框。

该表格包括以下列：

- **Select**
  选择要删除的行。
- **Type**
  显示所选类型：
  - Interface
  - Metric
  - Tag
- **Value**
  显示所选的接口、度量值或变量值。

5.6.4.3 Destination Match

在此页面中，可以指定是否根据目标 IP 地址过滤路由映射的路由信息。

设置

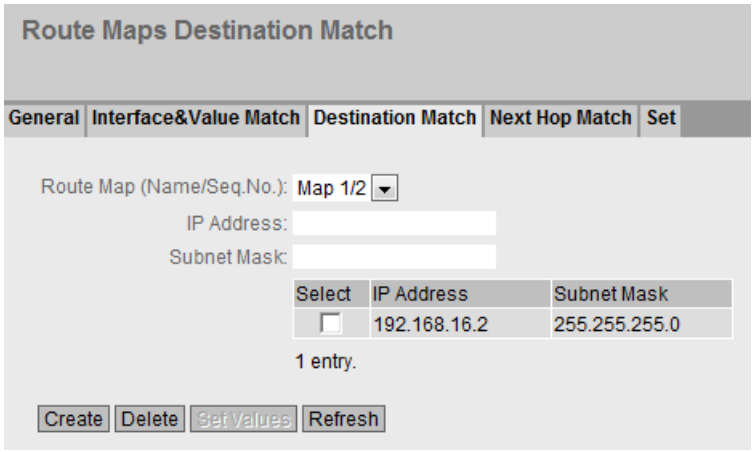


图 5-18　　路由映射目标匹配

- **Route Map (Name/Seq.No.)**
  选择路由映射。
- **IP Address**
  输入过滤依据的目标 IP 地址。
- **Subnet Mask**
  输入过滤依据的目标的子网掩码。

该表格包括以下列：

- **Select**
  选择要删除的行。
- **IP Address**
  显示目标的 IP 地址。
- **Subnet Mask**
  显示目标的子网掩码。

5.6.4.4 Next Hop Match

在该页面中，可以指定路由映射的过滤是否以下一次路由信息发送的目标路由器为依据。

设置

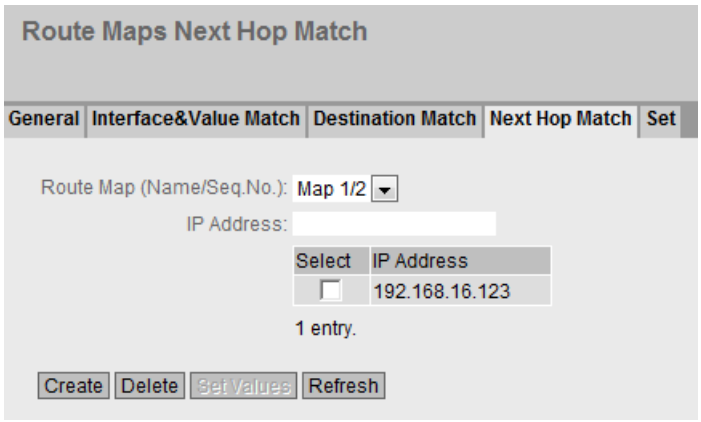


图 5-19　　路由映射下一次跳跃匹配

- **Route Map (Name/Seq.No.)**
  选择路由映射。
- **IP Address**
  输入下一次发送路由信息的目标路由器的 IP 地址。

该表格包括以下列：

- **Select**
  选择要删除的行。
- **IP Address**
  显示下一个路由器的 IP 地址。

5.6.4.5 Set Configuration

在该页面中，可以指定路由映射是否将更改路由信息。

只能更改“许可”路由映射的信息。

例如，如果已经根据特定的度量进行过滤，可以在此处更改度量值。 之后将使用新值转发路由信息。

设置

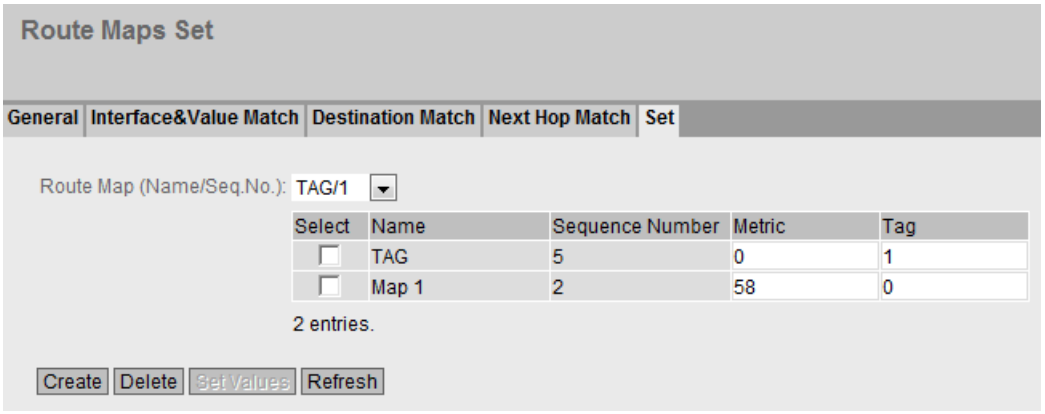


图 5-20 路由映射设置

- **Route Map (Name/Seq.No.)**
  选择路由映射。

该表格包括以下列：

- **Select**
  选择要删除的行。
- **Name**
  显示路由映射的名称。
- **Sequence Number**
  显示路由映射的顺序号。
- **Metric**
  输入新的度量值，将通过该值转发路由信息。
- **Tag**
  输入新的变量值，将通过该值转发路由信息。

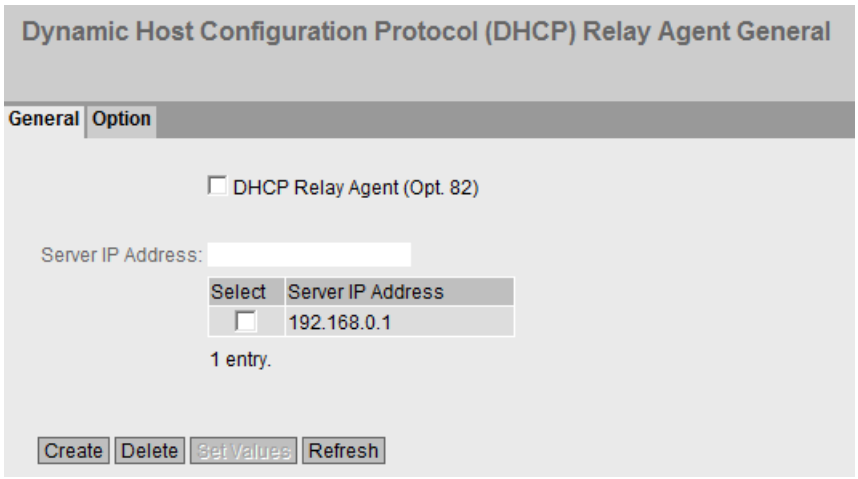
5.6.5 DHCP 中继代理

5.6.5.1 常规

DHCP 中继代理

如果 DHCP 服务器在不同网络中，则设备无法访问 DHCP 服务器。 DHCP 中继代理可在 DHCP 服务器与设备之间进行调停。 DHCP 中继代理会将设备的端口号与 DHCP 查询一同转发至 DHCP 服务器。

最多可以为 DHCP 中继代理指定 4 个 DHCP 服务器 IP 地址。 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 中继代理（选项 82）(DHCP Relay Agent (opt.82))**
  启用或禁用 DHCP 中继代理。
- **服务器 IP 地址 (Server IP Address)**
  输入 DHCP 服务器的 IP 地址。

该表格包括以下列：

- **Select**
  选择要删除的行。
- **服务器 IP 地址 (Server IP Address)**
  显示 DHCP 服务器的 IP 地址。

组态步骤

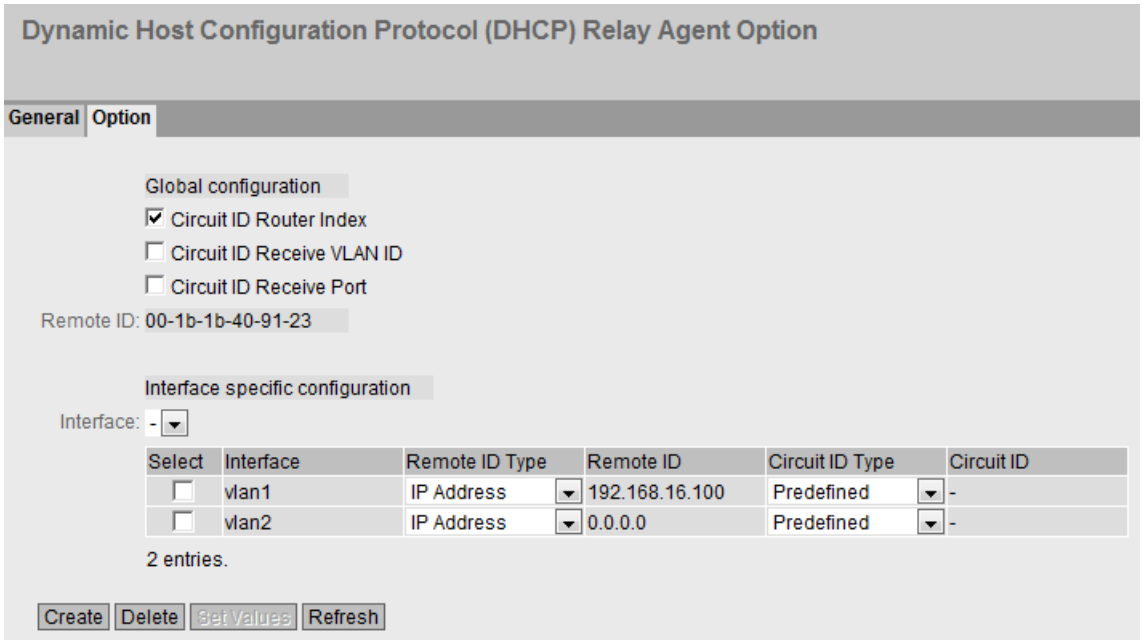
1. 在“Server IP Address”输入框中输入 DHCP 服务器的 IP 地址。
2. 单击“创建”(Create) 按钮。 会在表中生成一个新条目。
3. 选中“DHCP 中继代理（选项 82）”(DHCP Relay Agent (Opt. 82)) 复选框。
4. 单击“设置值”(Set Values) 按钮。

5.6.5.2 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：

- **电路 ID 路由器索引 (Circuit ID Router Index)**
  启用或禁用该复选框。 如果启用该复选框，则生成的电路 ID 会将路由器索引加入其中。
- **电路 ID 接收 VLAN ID (Circuit ID Receive VLAN ID)**
  启用或禁用该复选框。 如果启用该复选框，则生成的电路 ID 会将 VLAN ID 加入其中。
- **电路 ID 接收端口 (Circuit ID Receive Port)**
  启用或禁用该复选框。 如果启用该复选框，则生成的电路 ID 会将接收端口加入其中。

说明

至少需要选择一个选项。

- **Remote ID**
  显示设备 ID。
- **接口 (Interface)**
  从下拉列表中选择接口。

该表格包括以下列：

- **Select**
  选择要删除的行。
- **接口 (Interface)**
  显示接口。
- **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 IP 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 ID。
- **Remote ID**
  输入设备名称。 仅当为“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。仅当为“Circuit ID Type”选择“Free number”条目时才能编辑该框。
  值范围： 1- 188

组态步骤

按照以下步骤指定自动分配参数：

1. 选中“Circuit ID Router Index”复选框。
2. 从“Interface”下拉列表中选择接口。
3. 单击“创建”(Create) 按钮。 将在表中插入一个新行
4. 在“Remote ID Type”下拉列表中选择条目“IP Address”。 会将 IP 地址用作设备 ID。
5. 在“Circuit ID Type”下拉列表中选择“Predefined”条目。 路由器索引会添加到生成的电路 ID 中。
6. 单击“设置值”(Set Values) 按钮。

按照以下步骤手动指定参数：

1. 选中“Circuit ID Router Index”复选框。
2. 从“Interface”下拉列表中选择接口。
3. 单击“创建”(Create) 按钮。 将在表中插入一个新行
4. 在“Remote ID Type”下拉列表中选择条目“Free Text”。 在“Remote ID”中输入设备 ID。
5. 在“Circuit ID Type”下拉列表中选择条目“Free Number”。 在“Circuit ID”中输入 ID。
6. 单击“设置值”(Set Values) 按钮。

5.6.6 VRRP

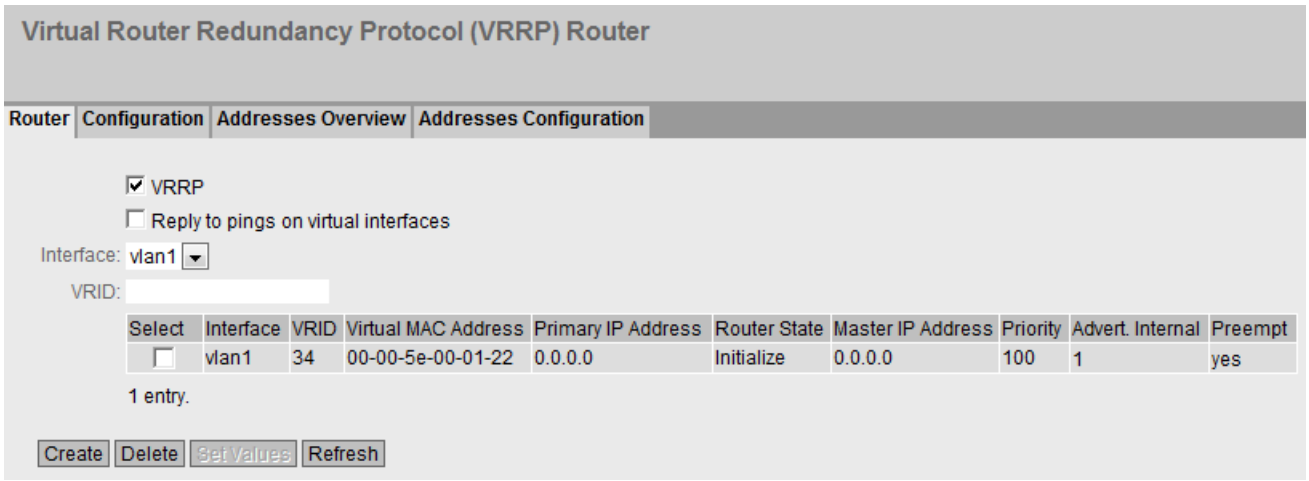
5.6.6.1 路由器

简介

使用“Create”按钮可创建新的虚拟路由器。 最多可组态 52 个虚拟路由器。 可在“Configuration”选项卡中组态其它参数。

说明

- 此功能只适用于第 3 层。
- 选中“VRRP”复选框，以组态 VRRP。
- 只能将 VRRP 与 VLAN 接口配合使用。 不支持路由器端口。



显示值说明

该页面包含以下框：

- **VRRP**
  使用 VRRP 启用或禁用路由功能。
- **虚拟接口响应 ping 请求 (Reply to pings on virtual interfaces)**
  启用后，虚拟 IP 地址也会对 ping 请求做出响应。

- **接口 (Interface)**
  从下拉列表中选择起虚拟路由器作用的接口。
- **VRID**
  在输入框中输入虚拟路由器的 ID。 此 ID 定义形成虚拟路由器 (VR) 的路由器组。 在该组中，ID 是相同的。 它不能再用于其它组。
  有效值为 1...255。

该表格包括以下列：

- **Select**
  选择要删除的行。
- **接口 (Interface)**
  显示起虚拟路由器作用的接口。
- **VRID**
  显示虚拟路由器的 ID。
- **虚拟 MAC 地址 (Virtual MAC Address)**
  显示虚拟路由器的虚拟 MAC 地址。
- **主 IP 地址 (Primary IP Address)**
  显示该 VLAN 的主 IP 地址。 条目 0.0.0.0 表示使用的是该 VLAN 的“主”地址。 否则，在“Subnets”菜单中对该 VLAN 组态的所有 IP 地址都是有效地址。
- **路由器状态 (Router State)**
  显示虚拟路由器的当前状态。 可能的值有：
  - 主站 (Master)
    该路由器为主路由器，为所有已分配的 IP 地址处理路由功能。
  - 备用站 (Backup)
    该路由器为备用路由器。 如果主路由器发生故障，备用路由器会接管主路由器的任务。
  - 初始化 (Initialize)
    虚拟路由器刚刚开启。 它将很快切换为“主设备”或“备用”状态。
- **主站 IP 地址 (Master IP Address)**
  显示主路由器的 IP 地址。
- **优先级 (Priority)**
  显示虚拟路由器的优先级。
  有效值为 1-254。
  当前主路由器会自动分配优先级 255。 可以在 VRRP 路由器之间自由分配其它优先级。 优先级越高，VRRP 路由器越早变为“主路由器”。

- **通告间隔 (Advert. Interval)**
  显示主路由器发送 VRRP 数据包的时间间隔。
- **先占 (Preempt)**
  显示在备用设备和主设备之间切换角色时路由器是否有优先权。
  - 是 (yes)
    路由器在切换角色时有优先权。
  - 否 (no)
    路由器在切换角色时无优先权。
- **虚拟接口响应 ping 请求 (Reply to pings on virtual interfaces)**
  显示该虚拟 IP 地址是否响应 ping 请求。

组态步骤

1. 选中“VRRP”复选框。
2. 从“Interface”下拉列表中选择接口。
3. 在“VRID”输入框中输入虚拟路由器的 ID。
4. 选中“虚拟接口响应 ping 请求”(Reply to pings on virtual interfaces) 复选框，虚拟 IP 地址便可响应 ping 请求。
5. 单击“创建”(Create) 按钮。 将在表中插入一个新行。
6. 单击“设置值”(Set Values) 按钮。 要组态虚拟路由器，请单击“Configuration”选项卡。

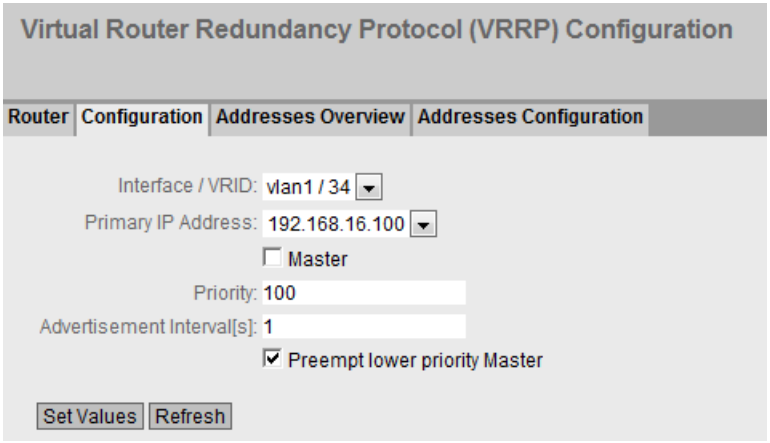
5.6.6.2 组态

简介

在此页面上组态虚拟路由器。

说明

此功能只适用于第 3 层。



显示值说明

该页面包含以下框：

- **接口/VRID (Interface/VRID)**
  从功能下拉列表中选择要组态的虚拟路由器的 ID。
- **主 IP 地址 (Primary IP Address)**
  从下拉列表中选择主 IP 地址。 如果路由器成为主路由器，路由器会使用此 IP 地址。

  说明

  如果仅为该 VLAN 组态了一个子网，则不需要任何输入。 该条目为 0.0.0.0。
  如果为该 VLAN 组态了多个子网，并且想要将特定 IP 地址用作 VRRP 数据包的源地址，则从该下拉列表中选择 IP 地址。 否则，将使用具有优先级的 IP 地址。

- **主设备 (Master)**
  如果启用此选项，则会为“关联 IP 地址”(Associated IP Address) 输入优先级最高的 IP 地址。 这表示 VRRP 路由器优先级最高的 IP 地址将用作虚拟主路由器的虚拟 IP 地址。
  必须为该组中的备用路由器禁用此选项，并且必须使用“Associated IP Address”中的路由器的 IP 地址。
- **优先级 (Priority)**
  输入此虚拟路由器的优先级。 有效值为 1-254。
  当前的主路由器始终会分配优先级 255。可以在冗余路由器之间自由分配其它优先级。优先级越高，路由器就越早变为“主路由器”。
- **通告间隔 (Advertisement Interval)**
  输入以秒为单位的时间间隔，在该时间间隔后，主路由器将再次发送 VRRP 数据包。
- **取代优先级较低的主设备 (Preempt lower priority Master)**
  允许根据选择过程在备用设备和主设备之间切换角色时取代。

组态步骤

要将虚拟路由器组态为主路由器，请按以下步骤操作：

1. 从“Interface/VRID”下拉列表中选择要组态的虚拟路由器的 ID。
2. 选中“Status”复选框。
3. 从“Primary IP Address”下拉列表中选择源地址。
4. 在“Priority”下拉列表中输入该虚拟路由器的优先级。
5. 选中“Master”复选框。
6. 在“Advertisement Interval”中输入时间间隔。
7. 选中“Preempt lower priority Master”复选框。
8. 单击“设置值”(Set Values) 按钮。

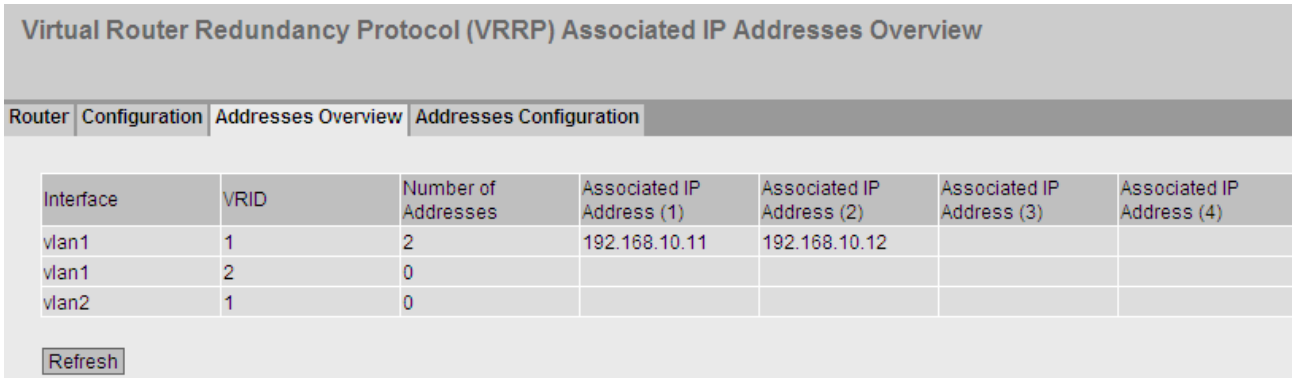
5.6.6.3 地址概述

概述

此页面显示虚拟路由器监视的 IP 地址。 每个虚拟路由器最多可监视 10 个 IP 地址。

说明

此功能只适用于第 3 层。



显示框说明：

该表格包括以下列：

- **接口 (Interface)**
  显示起虚拟路由器作用的接口。
- **VR ID**
  显示该虚拟路由器的 ID。
- **地址数量 (Number of Addresses)**
  显示 IP 地址的数量。
- **“关联的 IP 地址 (1) ... 关联的 IP 地址 (10)”(Associated IP Address (1) ... Associated IP Address (10))**
  显示该虚拟路由器监视的路由器 IP 地址。 如果路由器作为主路由器运行，该路由器就会接管与所有这些 IP 地址有关的路由功能。

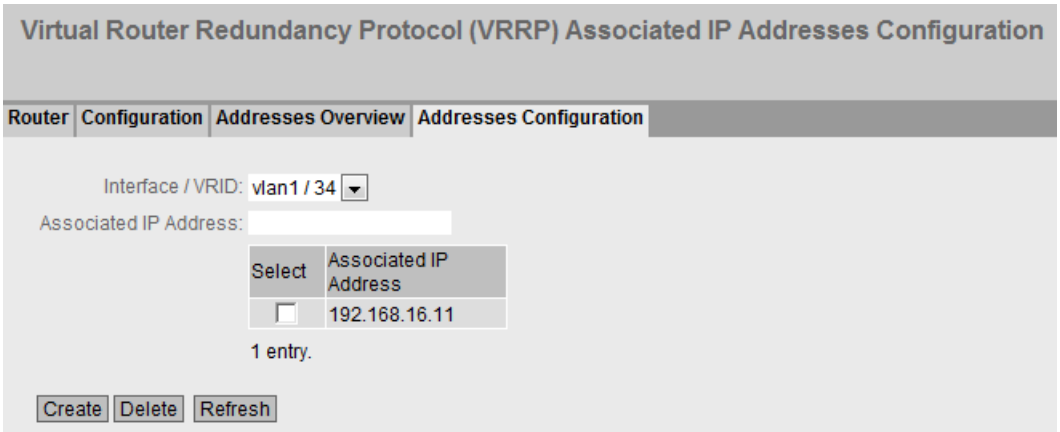
5.6.6.4 地址组态

创建或更改受监视的 IP 地址

在此页面上，可以创建、修改或删除要监视的 IP 地址。 一个虚拟路由器最多可监视 10 个 IP 地址。

说明

此功能只适用于第 3 层。



显示值说明

该页面包含以下框：

- **接口/VRID (Interface/VRID)**
  从下拉列表中选择虚拟路由器。
- **关联的 IP 地址 (Associated IP Address)**
  输入虚拟路由器将监视的 IP 地址。
  最多可输入 10 个 IP 地址。

该表格包括以下列：

- **Select**
  选择要删除的行。
- **关联的 IP 地址 (Associated IP Address)**
  显示虚拟路由器监视的 IP 地址。

组态步骤

1. 从“Interface/VRID”下拉列表中选择虚拟路由器的 ID。
2. 输入虚拟路由器将监视的 IP 地址。
3. 单击“创建”(Create) 按钮。 会在表中生成一个新条目。

5.6.7 OSPFv2

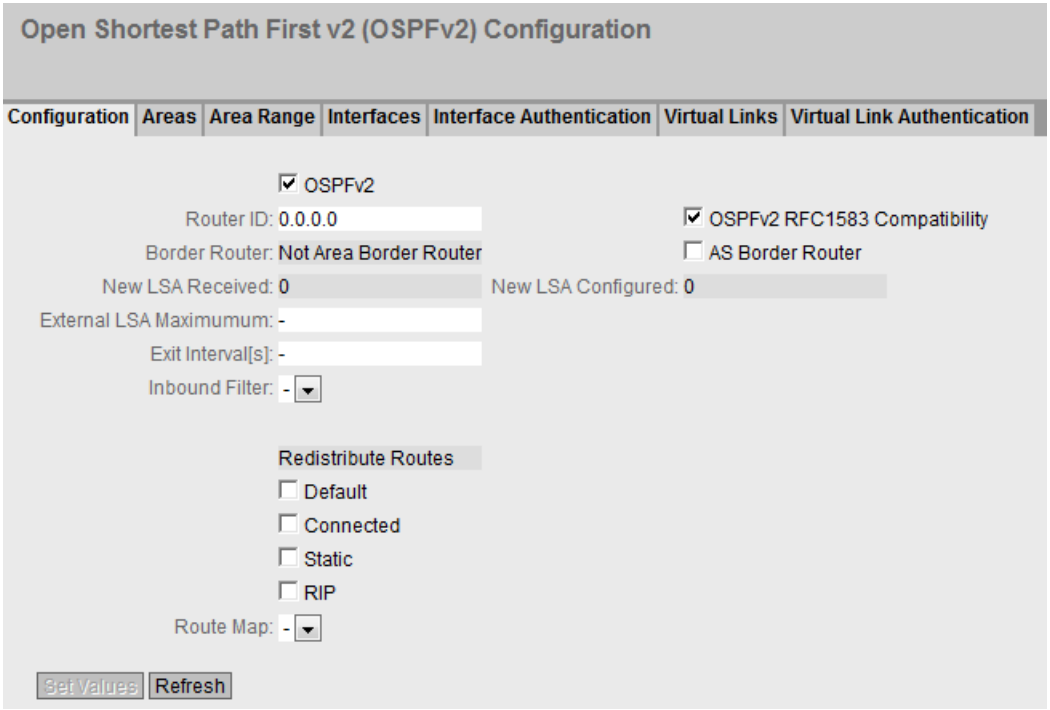
5.6.7.1 组态

简介

在此页面上，可以组态使用 OSPF 的路由。

说明

此功能只适用于第 3 层。



显示值说明

该页面包含以下框

- **OSPFv2**
  启用或禁用使用 OSPF 的路由。
- **路由器 ID (Router ID)**
  输入其中一个 OSPF 接口的名称。 以 IP 地址格式输入该名称，不需要与本地 IP 地址匹配。 路由器 ID 必须在网络中是唯一的。
- **OSPFv2 RFC 1583 兼容性 (OSPFv2 RFC 1583 Compatibility)**
  如果仍然有与 RFC 2328 不兼容的 OSPF 路由器在工作中，则启用该选项。
- **“边界路由器”(Border Router)**
  显示 OSPF 路由器的状态。 如果本地系统至少是 2 个区域中的有效成员，则路由器是区域边界路由器。
- **AS 边界路由器 (AS Border Router)**
  指定路由器是否为 AS 边界路由器。 AS 边界路由器可在多个自治系统之间进行调停，例如存在其它 RIP 网络时。 要添加和分配静态路由，AS 边界路由器也是必需的。
- **接收到的新 LSA (New LSA Received)**
  显示接收到的 LSA 的数量。
  不包括更新和本地 LSA。

- **组态的新 LSA (New LSA Configured)**
  该本地系统发送的不同 LSA 数。
- **最大外部 LSA (External LSA Maximum)**
  要限制数据库中外部 LSA 的条目数，请输入最大外部 LSA 数。
- **退出间隔 (s) (Exit Interval (s))**
  输入时间间隔，经过该时间间隔后，OSPF 路由器会再次尝试脱离溢出状态。 0 表示 OSPF 路由器只会在重启后尝试退出溢出状态。
- **入站过滤器**
  选择用于过滤入站路由的路由映射。
- **“重新分配路由”(Redistribute Routes)（“默认”(Default)/“连接”(Connected)/“静态”(Static)/RIP）**
  指定通过 OSPF 分配哪些已知路由。 您需要从“默认”(Default)、“连接”(Connected) 和“静态”(Static) 路由类型中作出选择。

  说明

  只能在 AS 边界路由器中启用这些选项。 特别是启用 Default 和 Static 选项时，如果网络中启用这些选项的节点过多，可能出现问题（例如转发回路）。
- **路由映射**
  选择用于过滤使用 RIPv2 转发的路由的路由映射。

组态步骤

1. 选中“OSPFv2”复选框。
2. 在“Router ID”输入框中输入路由器的 ID。
3. 选中“AS Border Router”复选框。
4. 单击“设置值”(Set Values) 按钮。

5.6.7.2 区域

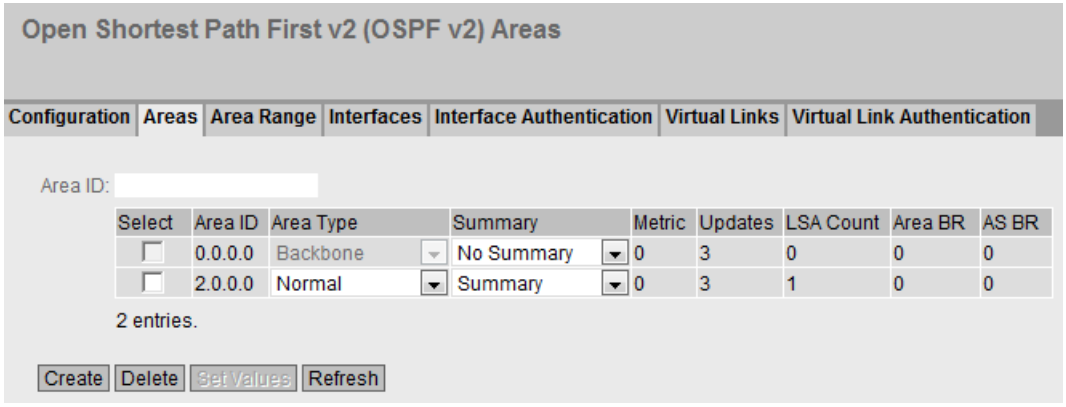
概述

自治系统可分为多个较小的区域。

在此页面上，可以查看、创建、修改或删除路由器的区域。

说明

此功能只适用于第 3 层。



显示值说明

该页面包含以下框：

- **区域 ID (Area ID)**
  输入区域的标识符。 数据库针对区域的所有路由器同步。 区域标识符在网络中必须唯一。
  区域标识符是具有以下格式的 32 位数： x.x.x.x，其中 x = 0 ... 255
  区域标识符 0.0.0.0 预留给了主干区域。

该表包含以下各列：

- **Select**
  选择要删除的行。
- **区域 ID (Area ID)**
  显示区域的标识符。

- **区域类型 (Area Type)**
  从下拉列表中选择区域类型。
  - 标准 (Standard)
  - 存根 (Stub)
  - NSSA
  - 骨干
- **汇总 (Summary)**
  指定是否生成该区域的汇总 LSA。
  - Summary： 生成汇总 LSA 并将其发送至该区域。
  - No Summary： 不生成汇总 LSA，也不将其发送至该区域。
- **度量 (Metric)**
  显示 OSPF 接口的开销。
- **更新 (Updates)**
  显示路由表的重新计算次数。
- **LSA 计数 (LSA Count)**
  显示数据库中的 LSA 数。
- **区域 BR (Area BR)**
  显示该区域中可到达的区域边界路由器 (ABR) 的数目。
- **AS BR**
  显示该区域中可到达的自治系统边界路由器 (ASBR) 的数目。

组态步骤

1. 在“Area ID”输入框中输入区域的 ID。
2. 单击“创建”(Create) 按钮。 会在表中生成一个新条目。
3. 在“Area Type”下拉列表中选择区域类型，例如 Stub。
4. 在“Summary”下拉列表中选择“Summary LSA”条目。
5. 单击“设置值”(Set Values) 按钮。

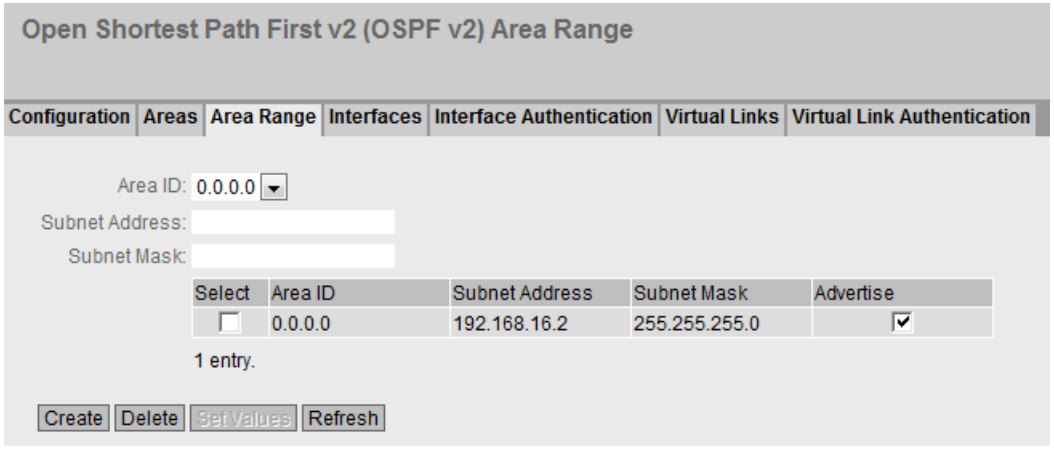
5.6.7.3 区域范围

创建新 OSPFv2 区域范围

使用“OSPFv2 区域范围”(OSPFv2 Area Ranges) 菜单中的 “新条目”(New Entry) 按钮，最多可将四个网络分组在一个区域 ID 下。此方法只适用于区域边界路由器。 这意味着，区域边界路由器只能为每个地址区域通告一条外发路径。

说明

此功能只适用于第 3 层。



显示框说明

该页面包含以下框：

- **区域 ID (Area ID)**
  从下拉列表中选择区域的 ID。 在“Areas”选项卡中指定 ID。
- **子网地址 (Subnet Address)**
  输入将被分组的网络的 IP 地址。
- **子网掩码 (Subnet Mask)**
  输入将被分组的网络的子网掩码。

该表包含以下各列：

- **Select**
  选择要删除的行。
- **区域 ID (Area ID)**
  显示区域的 ID。

- **子网地址 (Subnet Address)**
  显示将被分组的网络的 IP 地址。
- **子网掩码 (Subnet Mask)**
  显示将被分组的网络的子网掩码。
- **通告 (Advertise)**
  启用该选项以通告分组网络。

组态步骤

1. 从下拉列表中选择区域的 ID。
2. 输入将被分组的网络的 IP 地址。
3. 输入将被分组的网络的子网掩码。
4. 单击“创建”(Create) 按钮。 会在表中生成一个新条目。
5. 启用“通告”(Advertise) 选项以通告分组网络。
6. 单击“设置值”(Set Values) 按钮。

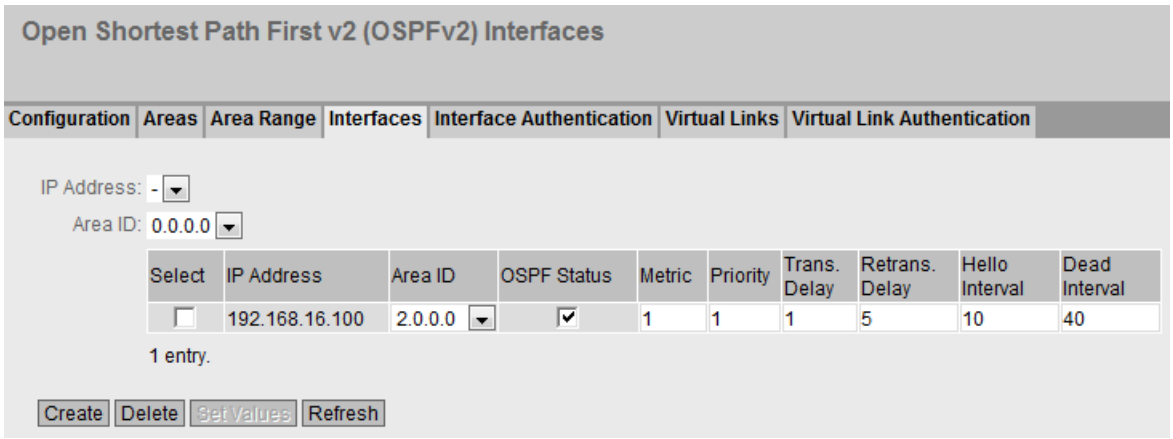
5.6.7.4 接口

概述

在此页面上，可以组态 OSPF 接口。

说明

此功能只适用于第 3 层。



显示框说明

该页面包含以下框：

- **IP 地址 (IP Address)**
  从下拉列表中选择 OSPF 接口的 IP 地址。
- **区域 ID (Area ID)**
  从下拉列表中选择连接到 OSPF 接口的区域的 ID。

> **说明**
> 对于次级接口，选择与其对应的初级接口相同的“区域 ID”(Area ID)。
> 有关接口是初级接口还是次级接口的信息，请参见“子网”>“概述 (页 253)”页面的“地址类型”(Address Type) 列。

从下拉列表中选择连接到 OSPF 接口的区域的 ID。该表格包括以下列：

- **Select**
  选择要删除的行。
- **IP 地址 (IP Address)**
  显示 OSPF 接口的 IP 地址。
- **区域 ID (Area ID)**
  从下拉列表中选择连接到 OSPF 接口的区域的 ID。
- **OSPF 状态 (OSPF Status)**
  指定是否在接口中激活 OSPF。
  - 启用： 在接口中启用 OSPF。
  - 禁用： 在接口中禁用 OSPF。
- **度量 (Metric)**
  输入 OSPF 接口的开销。
- **优先级 (Priority)**
  输入路由器优先级。 优先级只与选择指定路由器或指定边界路由器有关。 对于同一子网内的不同路由器，该参数的选择可以不同。
  值范围： 0 到 255
  默认值：1.
- **中转延迟 (Trans. Delay)**
  输入发送连接更新时期望的延迟。
  值范围： 1 s 到 3600 s
  默认值： 1 s

- **重传 间隔 (Retrans. Interval)**
  输入时间值，如果经过该时间后未接收到任何确认，则会再次传送 OSPF 数据包。
  值范围： 1 s 到 3600 s
  默认值： 5 s
- **呼叫间隔 (Hello Interval)**
  输入两个呼叫数据包之间的时间间隔。
  值范围： 1 s 到 65,535 s
  默认值： 10 s
- **停顿间隔 (Dead Interval)**
  输入时间间隔，如果在此时间内未从临近路由器接收到呼叫数据包，则在此时间间隔后会将该路由器标记为“故障”。
  默认值： 40 s

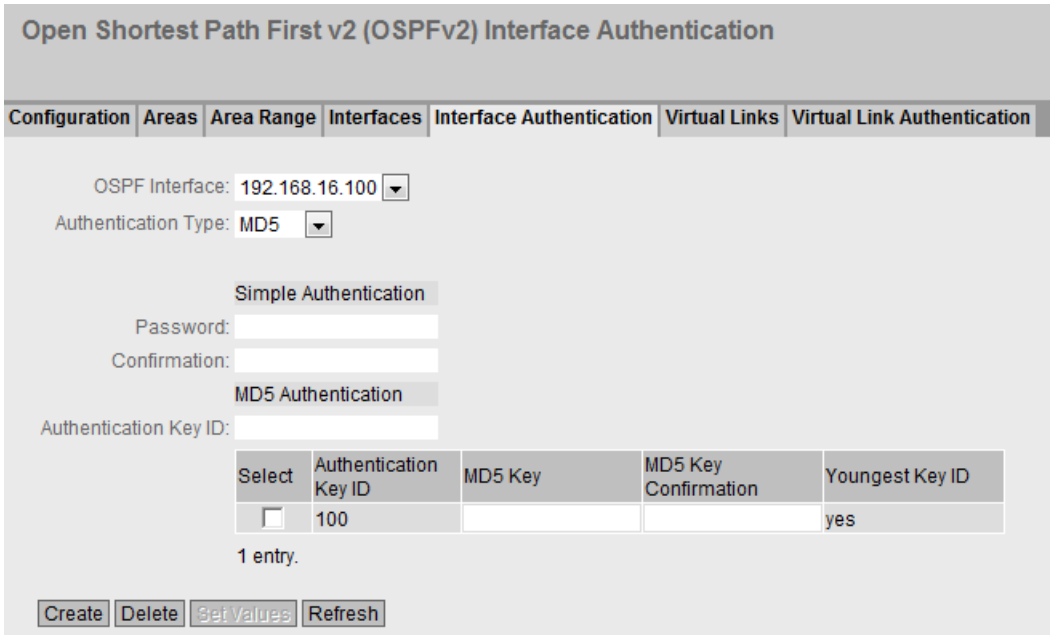
组态步骤

1. 从“IP Address”下拉列表中选择 OSPF 接口的 IP 地址。
2. 从“Area ID”下拉列表中选择与 OSPF 接口相连的区域的 ID。
3. 单击“创建”(Create) 按钮。会在表中生成一个新条目。
4. 选中“OSPF Status”旁边的复选框。
5. 为“中转延迟”(Transit Delay)、“重传 延迟”(Retrans. Delay) 和“停顿间隔”(Dead Interval) 输入适当值或使用默认设置。
6. 单击“设置值”(Set Values) 按钮。

5.6.7.5 接口验证

组态接口验证

在此页面上定义接口的验证。



显示框说明

该页面包含以下框：

- **OSPF 接口 (OSPF interface)**
  选择想要组态验证的 OSPF 接口。
- **验证类型 (Authentication Type)**
  选择验证方法。可做以下选择：
  - 无
    无验证
  - 简单 (simple)
    使用未加密密码进行验证
  - MD5
    使用 MD5 进行验证

“简单验证”部分

- **密码**
  输入密码。
- **确认 (Confirmation)**
  确认输入的密码。

“MD5 验证”部分

- **验证密钥 ID (Authentication Key ID)**
  输入 MD5 验证密钥的标识符。
  输入用于 MD5 验证的 ID，通过该 ID 可将密码用作密钥。
  由于密钥 ID 是通过协议传输的，因此，必须使用相同的密钥 ID 将同一个密钥存储到全部的邻近路由器中。

该表格包括以下列：

- **Select**
  选择要删除的行。
- **验证密钥 ID (Authentication Key ID)**
  仅当在设置 MD5 验证方法时才能编辑。只有此时才能使用多个密钥。
- **MD5 密钥 (MD5 Key)**
  输入 MD5 密钥。
- **MD5 密钥确认 (MD5 Key Confirmation)**
  确认输入的密钥。
- **最新的密钥 ID (Youngest Key ID)**
  显示 MD5 密钥是否为最新的密钥 ID。

组态步骤

1. 从下拉列表中选择 OSPF 接口和验证方法。
2. 在相应的输入框中输入以下数据：
   – 密码
   – 密码确认
   – MD5 验证密钥的标识符
3. 单击“创建”(Create) 按钮。

5.6.7.6 虚拟链路

概述

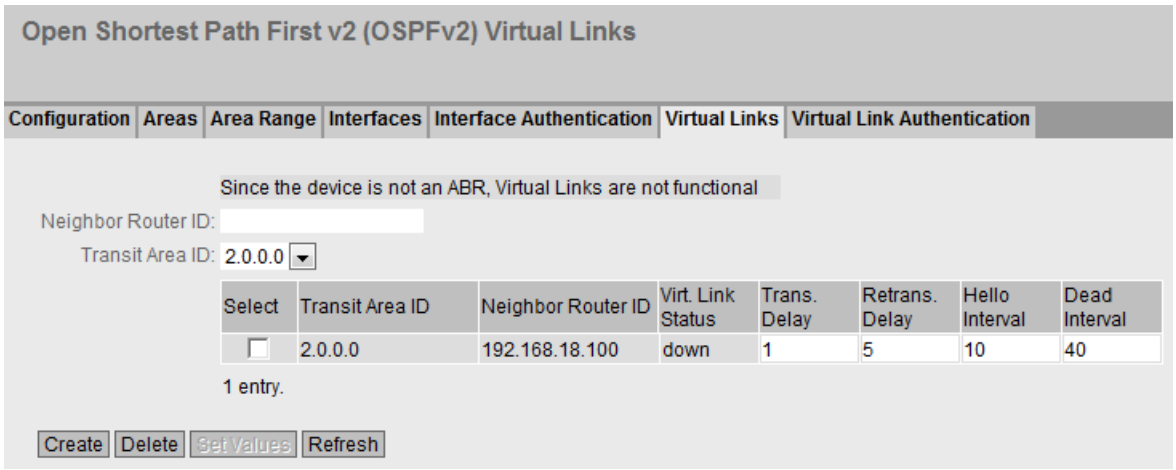
由于协议的原因，每个区域边界路由器都必须访问骨干区域。 如果路由器未直接连接到骨干区域，则会创建到骨干区域的虚拟链路。

说明

此功能只适用于第 3 层。

说明

请注意，创建虚拟链路时，中转区域和骨干区域必须都已组态完毕。
虚拟链路两端的组态必须相同。



显示框说明

该页面包含如下注释：

- **设备不是 ABR，虚拟链路不能正常工作**
  当至少已组态一个虚拟链路条目且设备不是区域边界路由器时，会显示此消息。

该页面包含以下框：

- **邻居路由器 ID (Neighbor Router ID)**
  输入虚拟连接另一端的邻近路由器的 ID。
- **中转区域 ID (Transit Area ID)**
  从下拉列表中选择连接两台路由器的区域 ID。

该表包含以下各列：

- **Select**
  选择要删除的行。
- **中转区域 ID (Transit Area ID)**
  显示连接两台路由器时使用的 ID。
- **邻居路由器 ID (Neighbor Router ID)**
  显示虚拟链路另一端的邻近路由器的 ID。
- **虚拟链路状态 (Virt. Link Status)**
  指定虚拟链路的状态。 可能的状态有：
  – 断开 (Down)： 虚拟链路未激活。
  – 点到点 (point-to-point)： 虚拟链路已激活。
- **中转延迟 (Trans. Delay)**
  输入发送链路更新数据包时期望的延迟。
  值范围： 1 s 到 3600 s
  默认值： 1 s
- **重传间隔 (Retrans. Delay)**
  输入时间值，经过该时间后，如果未收到确认，则会再次传送数据包。
  值范围：1 s 到 3600 s
  默认值： 5 s
- **呼叫间隔 (Hello Interval)**
  输入两个呼叫数据包之间的时间间隔。
  值范围： 1 s 到 65,535 s
  默认值： 10 s
- **停顿间隔 (Dead Interval)**
  输入时间间隔，如果在此时间内未从临近路由器接收到呼叫数据包，则在此时间间隔后会将该路由器视为“故障”。
  默认设置： 40 s

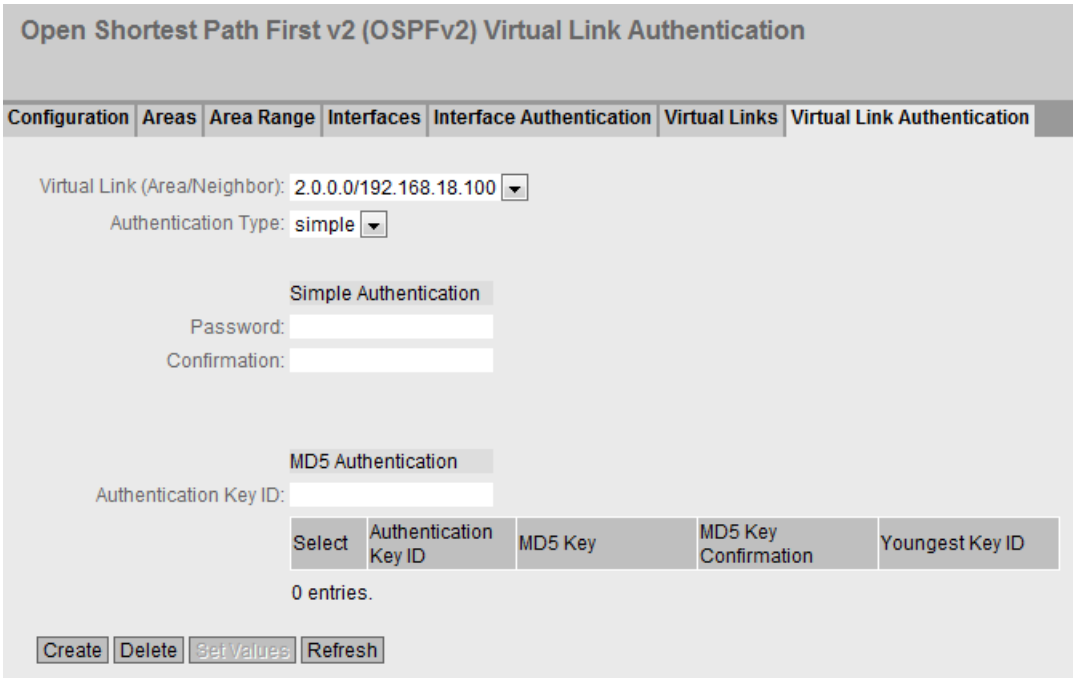
组态步骤

1. 在“Neighbor Router ID”中输入虚拟链路另一端的临近路由器的 ID。
2. 从“Transit Area ID”下拉列表中选择连接两台路由器的区域 ID。
3. 单击“创建”(Create) 按钮。 会在表中生成一个新条目。
4. 在“中转延迟”(Transit Delay)、“重传延迟”(Retrans. Delay) 和“停顿间隔”(Dead Interval) 输入适当值或使用默认设置。
5. 单击“设置值”(Set Values) 按钮。

5.6.7.7 虚拟链路验证

组态接口登录

在此页面上定义接口的验证。



显示框说明

该页面包含以下框：

- **虚拟链路 (区域/邻近) (Virtual Link (Area/Neighbor))**
  选择想要组态验证的虚拟链路。
- **验证类型 (Authentication Type)**
  选择验证方法。可做以下选择：
  - 无
    无验证
  - 简单 (simple)
    使用未加密密码进行验证
  - MD5
    使用 MD5 进行验证

“简单验证”部分

- **密码**
  输入密码。
- **确认 (Confirmation)**
  确认输入的密码。

“MD5 验证”部分

- **验证密钥 ID (Authentication Key ID)**
  输入 MD5 验证密钥的标识符。
  输入用于 MD5 验证的 ID，通过该 ID 可将密码用作密钥。
  由于密钥 ID 是通过协议传输的，因此，必须使用相同的密钥 ID 将同一个密钥存储到全部的邻近路由器中。

该表格包括以下列：

- **Select**
  选择要删除的行。
- **验证密钥 ID (Authentication Key ID)**
  仅当在设置 MD5 验证方法时才能编辑。只有此时才能使用多个密钥。
- **MD5 密钥 (MD5 Key)**
  输入 MD5 密钥。
- **MD5 密钥确认 (MD5 Key Confirmation)**
  确认输入的密钥。
- **最新的密钥 ID (Youngest Key ID)**
  显示 MD5 密钥是否为最新的密钥 ID。

组态步骤

请按下列步骤操作：

1. 从下拉列表中选择虚拟连接和验证方法。
2. 在相应的输入框中输入以下数据：
   - 密码
   - 密码确认
   - MD5 验证密钥的标识符
3. 单击“设置值”(Set Values) 按钮。

5.6.8 RIPv2

5.6.8.1 RIPv2 Configuration

在此页面上，可以组态使用 RIP 的路由。

说明

RIPv2 只在第 3 层上可用。

设置

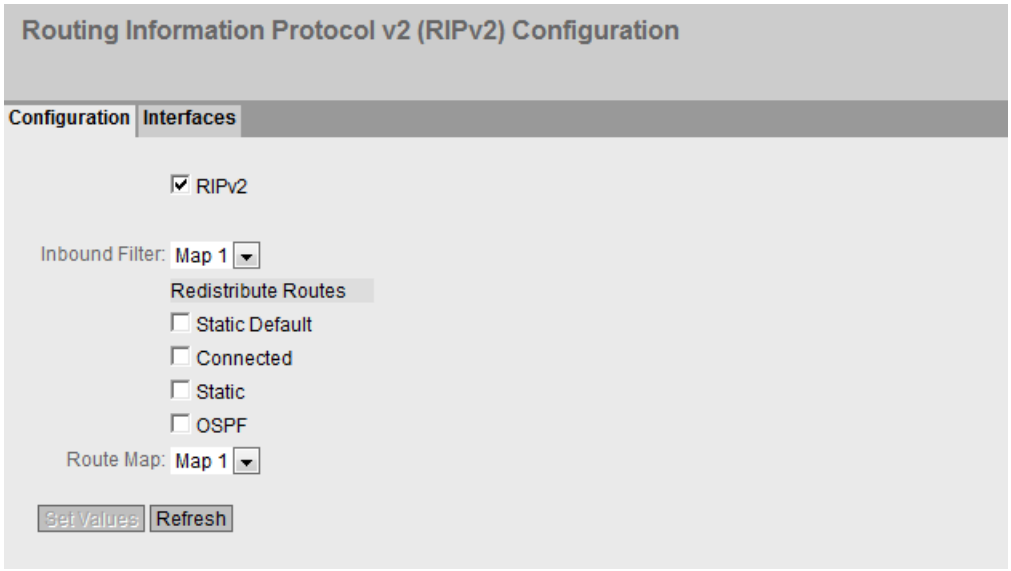


图 5-21 RIPv2 组态

- **RIPv2**
  启用或禁用使用 RIPv2 的路由。
- **Inbound Filter**
  选择用于过滤入站路由的路由映射。

- **Redistribute Routes**
  指定通过 RIPv2 分配哪些已知路由。
  路由包括以下类型：
  - Static Default
  - Connected
  - Static
  - OSPF
- **Route Map**
  选择用于过滤使用 RIPv2 转发的路由的路由映射。

5.6.8.2 RIPv2 接口 (RIPv2 Interfaces)

概述

在此页面上，可以组态 RIPv2 接口。

说明

RIPv2 只在第 3 层上可用。

设置

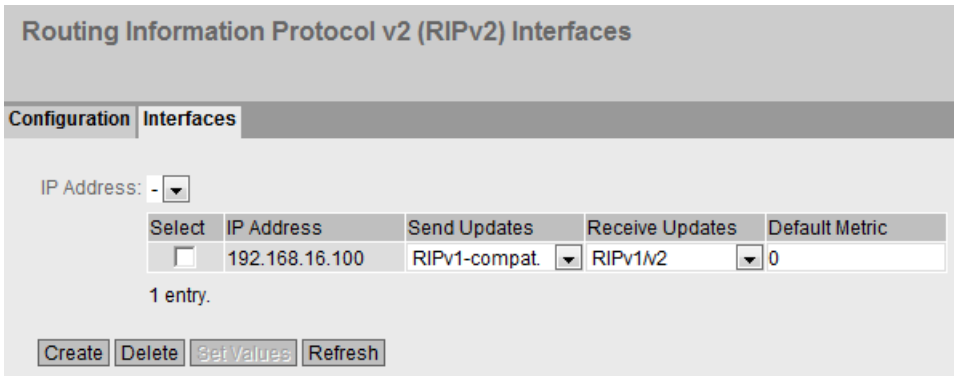


图 5-22 RIPv2 接口 (RIPv2 Interfaces)

- **IP Address**
  选择 RIPv2 接口的 IP 地址。

该表包含以下各列：

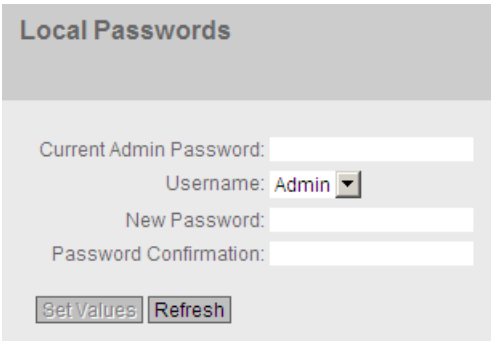
- **Select**
  选择要删除的行。
- **IP Address**
  显示 RIPv2 接口的 IP 地址。
- **Send Updates**
  选择更新的发送方式：
  - no send
    不发送更新。
  - RIPv1
    已发送 RIPv1 更新。
  - RIPv1-compat.
    根据 RIPv1 规则以多播形式发送 RIPv2 更新。
  - RIPv2
    以多播形式发送 RIPv2 更新。
  - RIPv1 demand/RIPv2 demand
    RIP 数据包只作为对显式查询的响应进行发送。
- **Receive Updates**
  选择接收更新的接受形式：
  - no receive
    不接收更新。
  - RIPv1
    只接收 RIPv1 的更新。
  - RIPv2
    只接收 RIPv2 的更新。
  - RIPv1/v2
    接收 RIPv1 和 RIPv2 的更新。
- **Default Metric**
  输入 RIPv2 接口的开销。

5.7 “Security”菜单

5.7.1 Passwords

组态设备密码

只能由管理员本地更改管理员和用户的设备密码。



步骤

1. 从“用户名”(Username) 下拉列表中，选择要更改其密码的用户。
   在“管理员”(Admin) 和“用户”(User) 之间选择。
2. 在“Current Admin Password”输入框中，输入有效的管理员密码。
3. 在“New Password”输入框中为所选用户输入新密码。 新密码不可少于 6 个字符长。
4. 在“Password Confirmation”输入框中重复输入新密码。
5. 单击“Set Values”按钮。

说明

设备出厂时的密码设置如下：

- “管理员”(admin)： admin
- “用户”(user)： user

如果是首次登录或是在“恢复出厂默认设置并重启”之后登录，则会提示您更改密码。

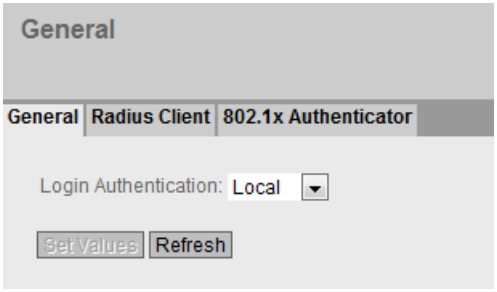
说明

在试用模式下更改密码

即使在试用模式下更改密码，此更改也会立即保存。

5.7.2 AAA

5.7.2.1 常规



显示框说明

该页面包含以下框：

- **登录验证 (Login Authentication)**
  指定登录方式：
  - “本地”(Local)
    通过本地用户名和密码登录。
  - Radius
    通过 Radius 服务器登录。

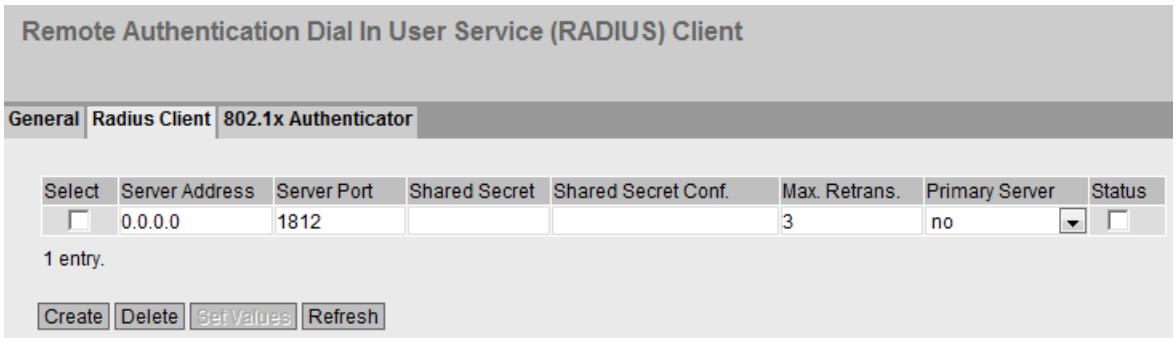
5.7.2.2 Radius 客户端

通过外部服务器进行验证

RADIUS 的概念基于外部验证服务器。 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。 终端设备和验证服务器都必须支持 EAP 协议（可扩展验证协议）。

表中的每一列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。 尽管端口上指示有链路，但客户端仍无法访问网络。



显示框说明

该表格包括以下列：

- **Select**
  选择要删除的行。
- **服务器地址 (Server Address)**
  在此输入服务器的 IP 地址。
- **服务器端口 (Server Port)**
  在此处输入 RADIUS 服务器的输入端口。 默认情况下会设置输入端口 1812。 值范围是 1 到 65535。
- **共享密钥 (Shared Secret)**
  在此处输入访问 ID。
- **共享密钥确认 (Shared Secret Conf).**
  再次输入访问 ID 以进行确认。
- **最大重传次数 (Max. Retrans.)**
  在此处输入查询另一个组态的 RADIUS 服务器或将登录视为失败前，查询尝试的最大次数。 默认情况下会设置 3。 值范围是 1 到 254。
- **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“yes”或“no”之一。
- **状态 (Status)**
  使用此复选框，可启用或禁用 RADIUS 服务器

说明

可在此页面上最多组态两个服务器。

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：
   - 服务器 IP 地址： 0.0.0.0
   - 端口号： 1812
   - 传输重试的最大次数： 3
   - 主服务器： 否 (No)
2. 在相关行中，在输入框中输入以下数据：
   - 服务器 IP 地址
   - 目标的端口号
   - 秘密访问 ID
   - 重复输入秘密访问 ID
   - 传输重试的最大次数
   - 主服务器
3. 单击“设置值”(Set Values) 按钮。

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：
   - IP 地址
   - 目标的端口号
   - 秘密访问 ID
   - 重复输入秘密访问 ID
   - 传输重试的最大次数
   - 主服务器
2. 单击“设置值”(Set Values) 按钮。

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。

说明

如果在使用“Set Values”或“Delete”按钮传送组态更改前单击“Refresh”按钮，则会取消更改，从设备内存加载之前的组态进行显示。

5.7.2.3 802.1x 验证器

对单独的端口启用验证

通过选中该复选框，可指定是否在此端口上启用符合 IEEE 802.1x 的网络访问保护。

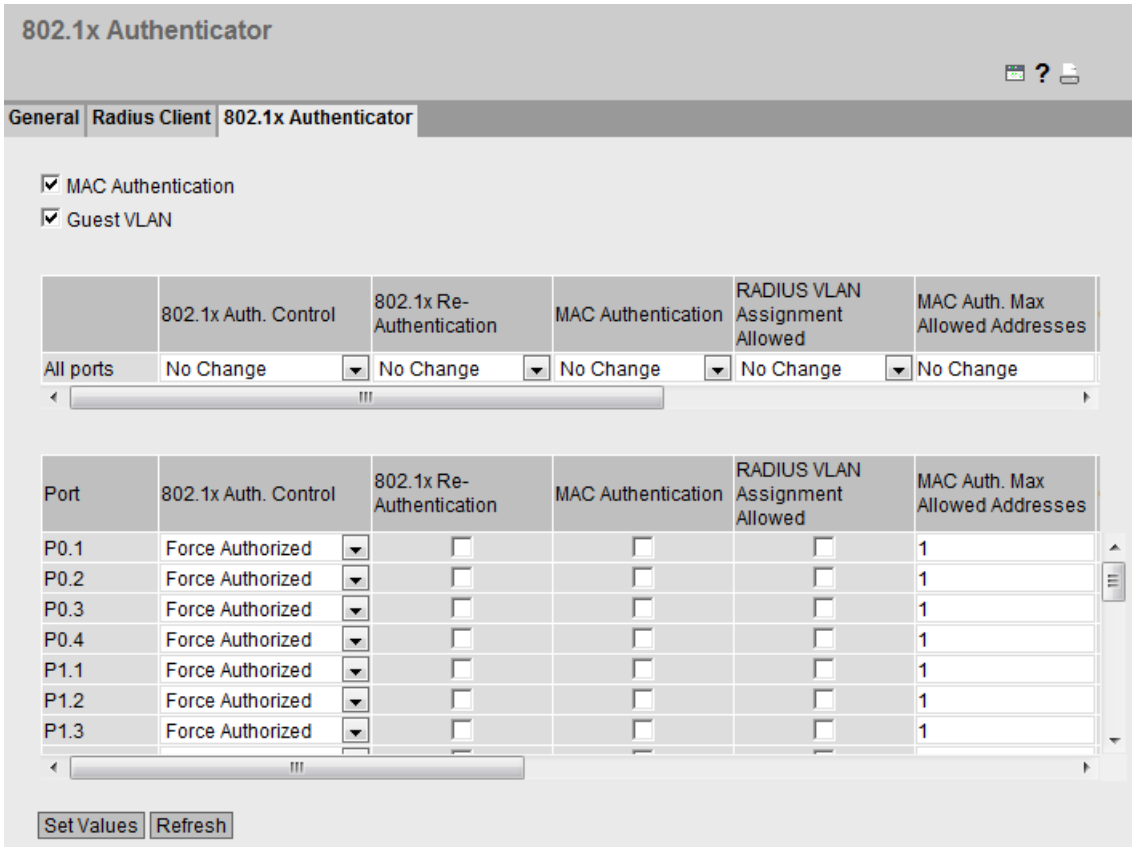


图 5-23 802.1x 验证器 - 表的第一部分

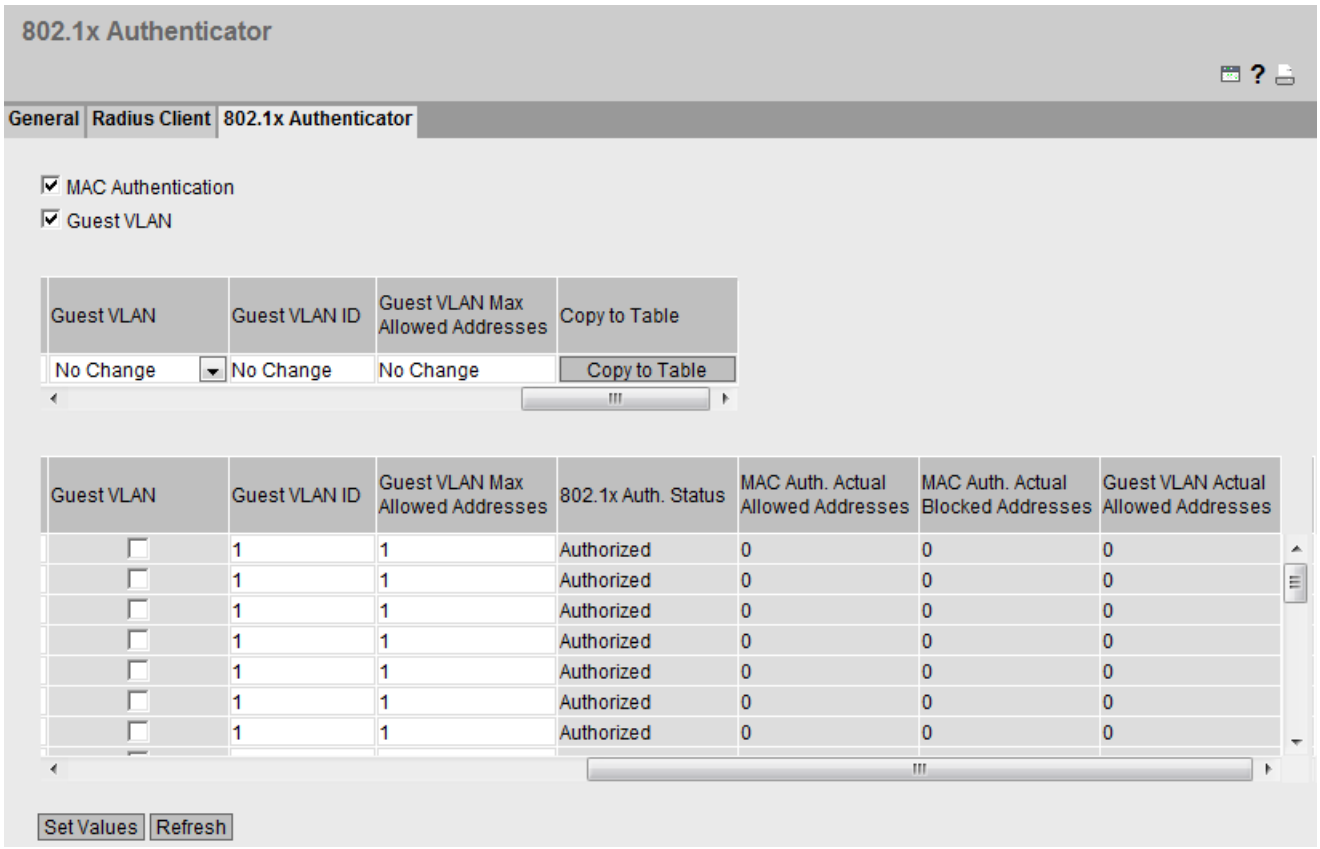


图 5-24　802.1x 验证器 - 表的第二部分

显示框说明

该页面包含以下框：

- **MAC 身份验证 (MAC Authentication)**
  为设备启用或禁用 MAC 验证。
- **访客 VLAN**
  为设备启用或禁用“访客 VLAN”功能。

表 1 包含以下列：

- **第 1 列**
  说明设置对于表 2 的所有端口都有效。
- **802.1x 验证控制 (802.1x Auth. Control)**
  选择所需设置。
  如果选择“无变化”(No Change)，则表 2 中的条目保持不变。

- **802.1x 重新验证 (802.1x Re-Authentication)**
  选择所需设置。
  如果选择“无变化”(No Change)，则表 2 中的条目保持不变。
- **MAC 验证 (MAC Authentication)**
  选择所需设置。
  如果选择“无变化”(No Change)，则表 2 中的条目保持不变。
- **支持的 RADIUS VLAN 分配 (RADIUS VLAN Assignment Allowed)**
  选择所需设置。
  如果选择“无变化”(No Change)，则表 2 中的条目保持不变。
- **MAC 验证允许的最大地址数 (MAC Auth. Max Allowed Addresses)**
  指定端口可同时连接几个终端设备。
  如果选择“无变化”(No Change)，则表 2 中的条目保持不变。
- **访客 VLAN (Guest VLAN)**
  选择所需设置。
  如果选择“无变化”(No Change)，则表 2 中的条目保持不变。
- **访客 VLAN ID (Guest VLAN ID)**
  选择所需设置。
  如果选择“无变化”(No Change)，则表 2 中的条目保持不变。
- **访客 VLAN 允许的最大地址数 (Guest VLAN Max Allowed Addresses)**
  指定访客 VLAN 中允许同时存在几个终端设备。
  如果选择“无变化”(No Change)，则表 2 中的条目保持不变。
- **复制到表中 (Copy to Table)**
  如果单击此按钮，将为表 2 的所有端口应用这些设置。

表 2 包含以下列：

- **Port**
  此列会列出此设备上的全部可用端口。
- **802.1x 验证控制 (802.1x Auth. Control)**
  指定端口的身份验证：
  - 强制未授权 (Force Unauthorized)
    阻止通过该端口进行数据通信。
  - 强制授权 (Force Authorized)
    允许通过该端口进行数据通信，无任何限制。
    默认设置
  - 自动 (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。
- **MAC 身份验证 (MAC Authentication)**
  如果想要使用“MAC 身份验证”方法对终端设备进行身份验证，请启用此选项。
- **支持的 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。该端口随后便属于相应的 VLAN。
  如果禁用此选项，则会丢弃 VLAN 信息。
- **MAC 验证允许的最大地址数 (MAC Auth. Max Allowed Addresses)**
  输入允许同时连接到端口的终端设备数量。
- **访客 VLAN (Guest VLAN)**
  如果想要在身份验证失败时在“访客 VLAN”中使用终端设备，请启用此选项。
- **访客 VLAN ID (Guest VLAN ID)**
  输入端口的 VLAN ID。
- **访客 VLAN 允许的最大地址数 (Guest VLAN Max Allowed Addresses)**
  输入允许同时连接到访客 VLAN 的终端设备数量。
- **802.1x 验证状态 (802.1x Auth. Status)**
  显示端口身份验证的状态：
  - 强制未授权 (Force Unauthorized)
  - 强制授权 (Force Authorized)
  - 自动 (Auto)
- **MAC 身份验证实际允许的地址数 (MAC Auth. Actual Allowed Addresses)**
  显示当前已连接的终端设备数量。
- **MAC 身份验证实际拦截的地址数 (MAC Auth. Actual Blocked Addresses)**
  显示当前已拦截的终端设备数量。
- **访客 VLAN 实际允许的地址数 (Guest VLAN Actual Allowed Addresses)**
  显示访客 VLAN 中当前允许的终端设备数量。

组态步骤

对单独的端口启用验证

1. 在表 2 相关行中选中所需选项。
2. 要应用更改，请单击“Set Values”按钮。

对所有端口启用验证

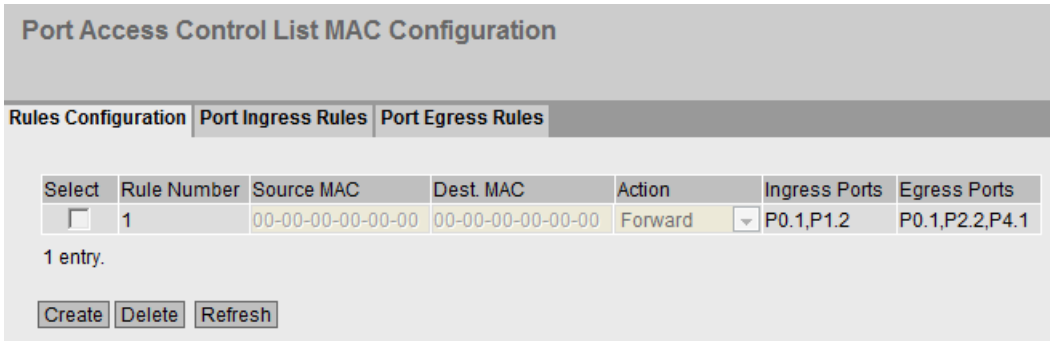
1. 在表 1 中选中所需选项。
2. 单击“复制到表中 (Copy to Table)”按钮。 将为表 2 中的所有端口启用该复选框。
3. 要应用更改，请单击“Set Values”按钮。

5.7.3 端口 ACL MAC

5.7.3.1 规则组态

简介

在此页面上为基于 MAC 的 ACL 指定访问规则。



显示框说明

该表格包括以下列：

- **Select**
  选择要删除的行。
- **规则编号 (Rule Number)**
  显示 ACL 规则的编号。 如果单击“创建”(Create) 按钮，会创建一个具有唯一编号的新行。
- **源 MAC (Source MAC)**
  输入源的单播 MAC 地址。
- **目标 MAC**
  输入目标的单播 MAC 地址。

- **操作 (Action)**
  从下拉列表中选择操作。 可选操作包括：
  - 转发 (Forward)
    如果帧符合 ACL 规则，则转发该帧。
  - 放弃 (Discard)
    如果帧符合 ACL 规则，则不转发该帧。
- **入站端口 (Ingress Ports)**
  显示应用此规则的所有入站端口的列表
- **出站端口 (Egress Ports)**
  显示应用此规则的所有出站端口的列表

说明

输入 MAC 地址

如果为源和/或目标 MAC 地址输入地址“00:00:00:00:00:00”，则采用此方法创建的规则将应用到所有的源或目标 MAC 地址。

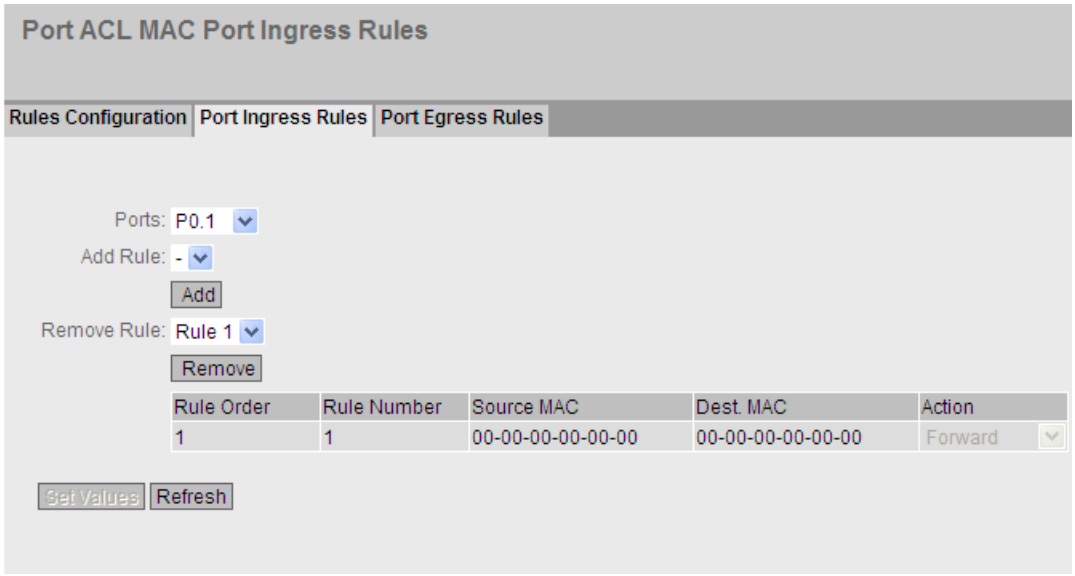
组态步骤

1. 单击“创建”(Create) 按钮。 会在表中创建一个具有唯一编号（规则编号）的新行。
2. 在“Source Mac”中输入源的 MAC 地址。
3. 在“目标 Mac”(Dest. Mac) 中输入目标的 MAC 地址。
4. 对于“Action”，指定在帧符合 ACL 规则的情况下，是转发还是拒绝该帧。

5.7.3.2 端口入站规则

简介

在此页面上指定 ACL 规则，端口将根据此规则过滤入站帧。



显示框说明

该页面包含以下框

- **“端口”(Ports) 下拉列表**
  从下拉列表中选择所需端口。
- **“添加规则”(Add Rules) 下拉列表**
  从下拉列表中选择将分配给端口的 ACL 规则。 在“规则组态”(Rules Configuration) 选项卡中指定 ACL 规则。
- **“添加”(Add) 按钮**
  要将 ACL 规则永久分配给端口，请单击“添加”(Add) 按钮。 组态会显示在表中。
- **“移除规则”(Remove Rule) 下拉列表**
  从“移除规则”(Remove Rule) 下拉列表中选择要删除的 ACL 规则。
- **“移除”(Remove) 按钮**
  要删除端口的 ACL 规则，请单击“移除”(Remove) 按钮。

该表格包括以下列：

- **规则顺序 (Rule Order)**
  显示 ACL 规则的顺序。
- **规则编号 (Rule Number)**
  显示 ACL 规则的编号。
- **源 MAC (Source MAC)**
  显示源的单播 MAC 地址。
- **目标 MAC (Dest. MAC)**
  显示目标的单播 MAC 地址。
- **操作 (Action)**
  显示操作。
  - 转发 (Forward)
    如果帧符合 ACL 规则，则转发该帧。
  - 放弃 (Discard)
    如果帧符合 ACL 规则，则不转发该帧。

组态步骤

按照以下步骤为端口分配 ACL 规则：

1. 在“Ports”下拉列表中选择端口。
2. 在“Rules”下拉列表中选择 ACL 规则。
3. 单击“Add”按钮。 会在表中生成一个新条目。

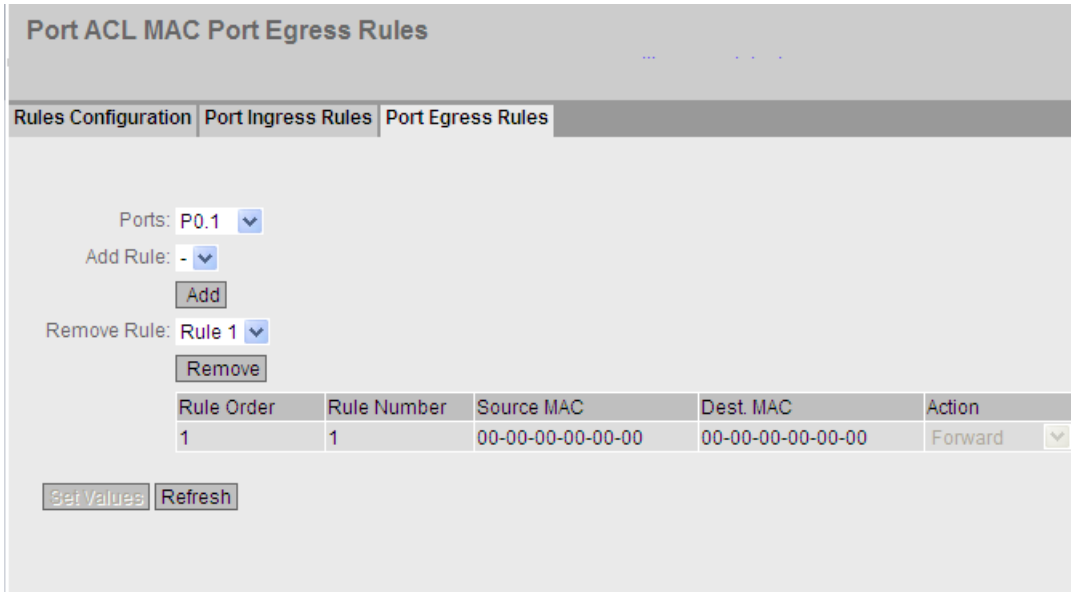
按照以下步骤删除端口的 ACL 规则：

1. 在“Ports”下拉列表中选择端口。
2. 在“Rules”下拉列表中选择 ACL 规则。
3. 单击“Remove”按钮。 将从表中删除相应的条目。

5.7.3.3 端口出站规则

简介

在此页面上指定 ACL 规则，端口将根据此规则过滤出站帧。



显示框说明

- **“端口”(Ports) 下拉列表**
  从下拉列表中选择所需端口。
- **“添加规则”(Add Rules) 下拉列表**
  从下拉列表中选择将分配给端口的 ACL 规则。在“规则组态”(Rules Configuration) 选项卡中指定 ACL 规则。
- **“添加”(Add) 按钮**
  要将 ACL 规则永久分配给端口，请单击“添加”(Add) 按钮。组态会显示在表中。
- **“移除规则”(Remove Rule) 下拉列表**
  从“移除规则”(Remove Rule) 下拉列表中选择要删除的 ACL 规则。
- **“移除”(Remove) 按钮**
  要删除端口的 ACL 规则，请单击“移除”(Remove) 按钮。

该表格包括以下列：

- **规则顺序 (Rule Order)**
  显示 ACL 规则的顺序。
- **规则编号 (Rule Number)**
  显示 ACL 规则的编号。
- **源 MAC (Source MAC)**
  显示源的单播 MAC 地址。
- **目标 MAC (Dest. MAC)**
  显示目标的单播 MAC 地址。
- **操作 (Action)**
  显示操作。
  - 转发 (Forward)
    如果帧符合 ACL 规则，则转发该帧。
  - 放弃 (Discard)
    如果帧符合 ACL 规则，则不转发该帧。

组态步骤

按照以下步骤为端口分配 ACL 规则：

1. 在“Ports”下拉列表中选择端口。
2. 在“Rules”下拉列表中选择 ACL 规则。
3. 单击“Add”按钮。 会在表中生成一个新条目。

按照以下步骤删除端口的 ACL 规则：

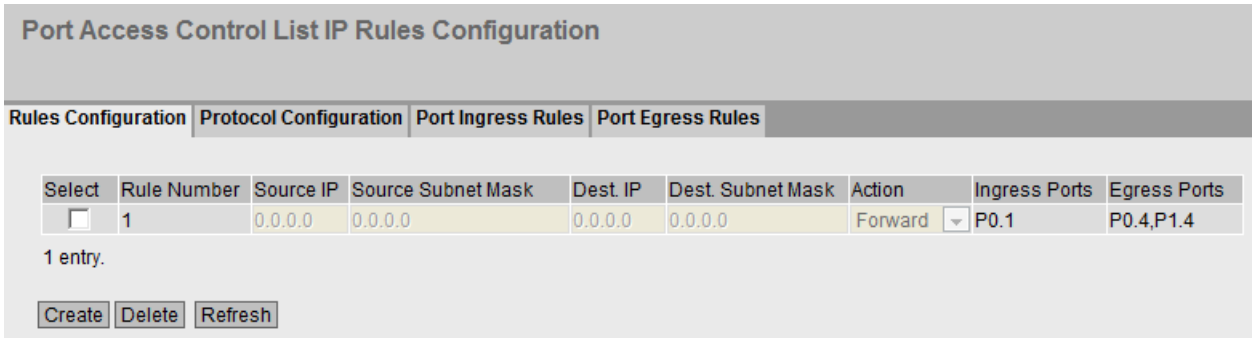
1. 在“Ports”下拉列表中选择端口。
2. 在“Rules”下拉列表中选择 ACL 规则。
3. 单击“Remove”按钮。 将从表中删除相应的条目。

5.7.4 端口 ACL IP

5.7.4.1 规则组态

简介

在此页面上为基于 IP 的 ACL 指定规则。



显示框说明

该表格包括以下列：

- **Select**
  选择要删除的行。
- **规则编号 (Rule Number)**
  显示 ACL 规则的编号。 如果单击 “创建”(Create) 按钮，会创建一个具有唯一编号的新行。
- **源 IP (Source IP)**
  输入源的 IP 地址。
- **源子网掩码 (Source Subnet Mask)**
  输入源所在子网的子网掩码。
- **目标 IP (Dest. IP)**
  输入目标的 IP 地址。
- **目标子网 掩码 (Dest. Subnet Mask)**
  输入目标所在的子网掩码。

- **操作 (Action)**
  从下拉列表中选择操作。 可选操作包括：
  - 转发 (Forward)
    如果帧符合 ACL 规则，则转发该帧。
  - 放弃 (Discard)
    如果帧符合 ACL 规则，则不转发该帧。
- **入站端口 (Ingress Ports)**
  显示应用此规则的所有入站端口的列表
- **出站端口 (Egress Ports)**
  显示应用此规则的所有出站端口的列表

说明

各主机的子网掩码

如果为单个系统（一个 IP 地址）创建规则，则需要指定长度为 32 Bit 的子网掩码。 该掩码为“255.255.255.255”。

组态步骤

1. 单击“创建”(Create) 按钮。 会在表中创建一个具有唯一编号（规则编号）的新行。
2. 在“Source IP”和“Source Subnet Mask”中输入源的数据。
3. 在“Source IP”和“Source Dest Mask”中输入目标的数据。
4. 对于操作，指定在帧符合 ACL 规则的情况下，是转发还是拒绝该帧。

5.7.4.2 Protocol Configuration

可在此页面中为协议指定规则。

设置

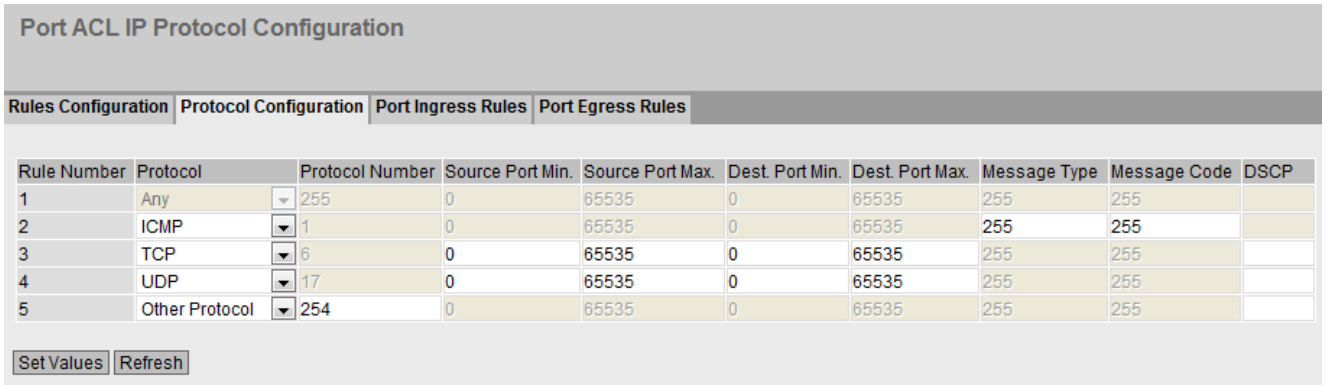


图 5-25　　端口 ACL IP 协议组态

该表格包括以下列：

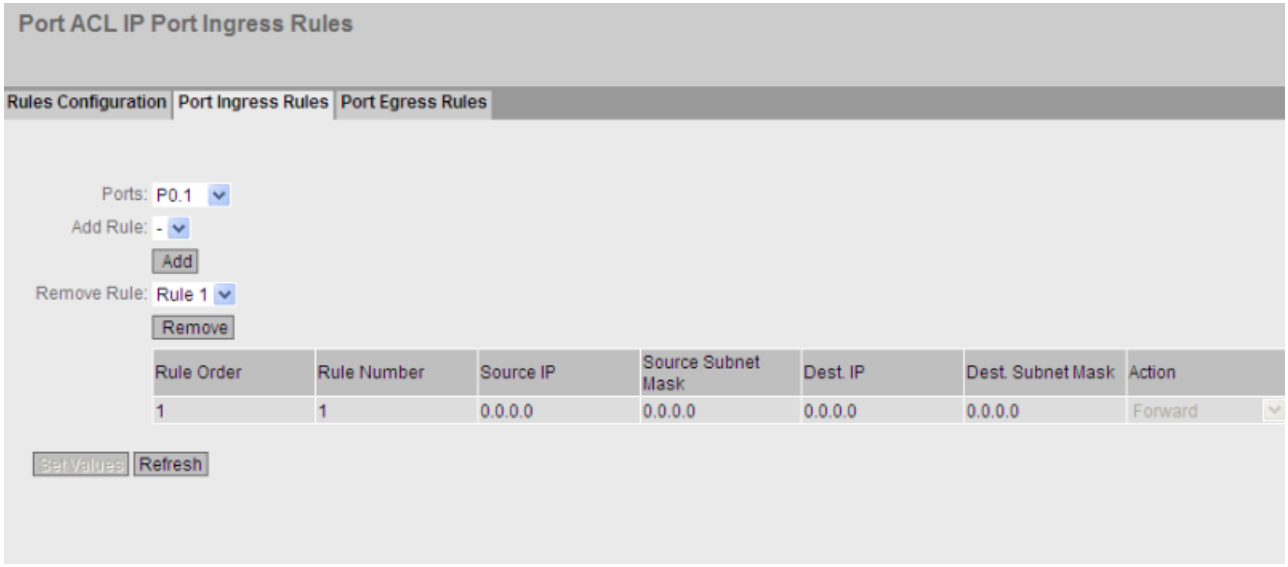
- **Rule Number**
  显示协议规则的编号。 创建规则时，会创建一个具有唯一编号的新行。
- **Protocol**
  选择该规则对其有效的协议。
- **Protocol Number**
  输入协议编号以定义其它协议。
  只有为协议设置了“Other Protocol”时才能编辑该输入框。
- **Soure Port Min.**
  输入源端口可能的最小端口号。
  只有为协议设置了“TCP”或“UDP”时才能编辑该输入框。
- **Source Port Max.**
  输入源端口可能的最大端口号。
  只有为协议设置了“TCP”或“UDP”时才能编辑该输入框。
- **Dest. Port Min.**
  输入目标端口可能的最小端口号。
  只有为协议设置了“TCP”或“UDP”时才能编辑该输入框。
- **Dest. Port Max.**
  输入目标端口可能的最大端口号。
  只有为协议设置了“TCP”或“UDP”时才能编辑该输入框。
- **Message Type**
  输入消息类型以决定消息的格式。
  只有为协议设置了“ICMP”时才能编辑该输入框。

- **Message Code**
  输入消息代码以指定消息的功能。
  只有为协议设置了“ICMP”时才能编辑该输入框。
- **DSCP**
  输入用于划分优先级的值。
  如果为协议设置了“ICMP”，则无法编辑该输入框。

5.7.4.3 端口入站规则

简介

在此页面上指定 ACL 规则，端口将根据此规则处理入站帧。



显示框说明

该页面包含以下框

- **下拉列表“Ports”**
  从下拉列表中选择所需端口。
- **下拉列表“Add Rules”**
  从下拉列表中选择将分配给端口的 ACL 规则。 在“Rules Configuration”选项卡中指定 ACL 规则。
- **“Add”按钮**
  要将 ACL 规则永久分配给端口，请单击“Add”按钮。 组态会显示在表中。

- **下拉列表“Remove Rule”**
  从“Remove Rule”下拉列表中选择要删除的 ACL 规则。
- **“Remove”按钮**
  要删除端口的 ACL 规则，请单击“Remove”按钮。

该表格包括以下列：

- **Rule Order**
  显示 ACL 规则的顺序。 In
- **Rule Number**
  显示 ACL 规则的编号。 如果单击“Create”按钮，会创建一个具有唯一编号的新行。
- **Source IP**
  显示源的 IP 地址。
- **Source Subnet Mask**
  显示源所在子网的子网掩码。
- **Dest. IP**
  显示目标的 IP 地址。
- **Source Dest. Mask**
  显示目标所在子网的子网掩码。
- **Action**
  从下拉列表中选择操作。 可能的响应包括：
  - Forward
    如果帧符合 ACL 规则，则转发该帧。
  - Discard
    如果帧符合 ACL 规则，则不转发该帧。

组态步骤

按照以下步骤为端口分配 ACL 规则：

1. 在“Ports”下拉列表中选择端口。
2. 在“Rules”下拉列表中选择 ACL 规则。
3. 单击“Add”按钮。 会在表中生成一个新条目。

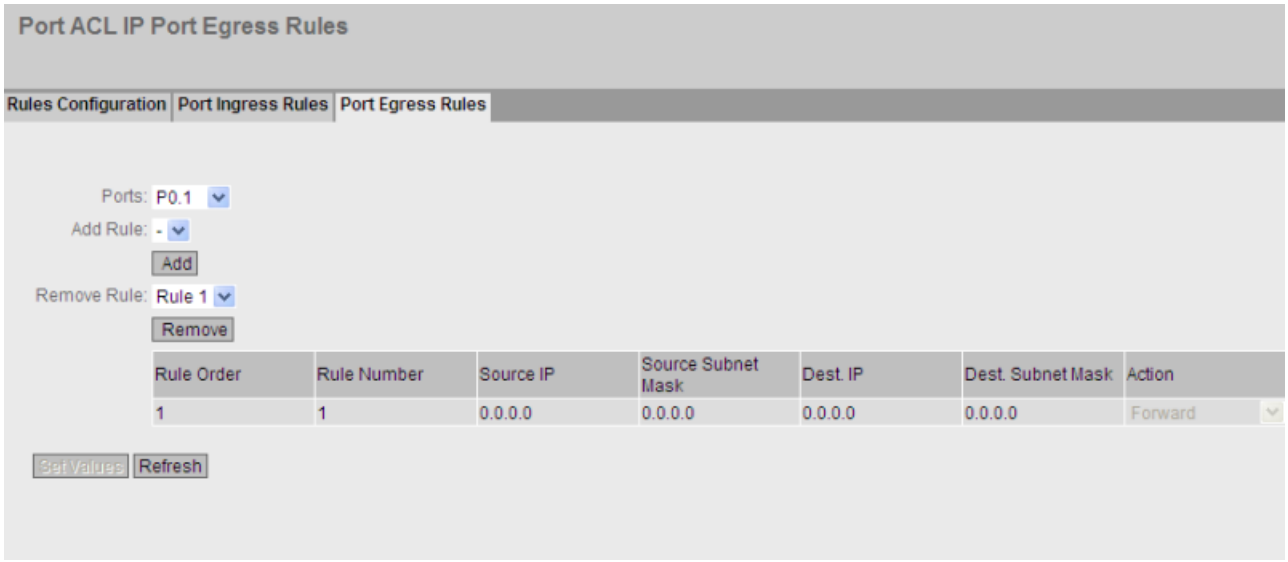
按照以下步骤删除端口的 ACL 规则：

1. 在“Ports”下拉列表中选择端口。
2. 在“Rules”下拉列表中选择 ACL 规则。
3. 单击“Remove”按钮。 将从表中删除相应的条目。

5.7.4.4 端口出站规则

简介

在此页面上指定 ACL 规则，端口将根据此规则处理出站帧。



显示框说明

该页面包含以下框

- **下拉列表“Ports”**
  从下拉列表中选择所需端口。
- **下拉列表“Add Rules”**
  从下拉列表中选择将分配给端口的 ACL 规则。 在“Rules Configuration”选项卡中指定 ACL 规则。
- **“Add”按钮**
  要将 ACL 规则永久分配给端口，请单击“Add”按钮。 组态会显示在表中。
- **下拉列表“Remove Rule”**
  从“Remove Rule”下拉列表中选择要删除的 ACL 规则。
- **“Remove”按钮**
  要删除端口的 ACL 规则，请单击“Remove”按钮。

该表格包括以下列：

- **Rule Order**
  显示 ACL 规则的顺序。 In
- **Rule Number**
  显示 ACL 规则的编号。 如果单击“Create”按钮，会创建一个具有唯一编号的新行。
- **Source IP**
  显示源的 IP 地址。
- **Source Subnet Mask**
  显示源所在子网的子网掩码。
- **Dest. IP**
  显示目标的 IP 地址。
- **Source Dest. Mask**
  显示目标所在子网的子网掩码。
- **Action**
  从下拉列表中选择操作。 可能的响应包括：
  - Forward
    如果帧符合 ACL 规则，则转发该帧。
  - Discard
    如果帧符合 ACL 规则，则不转发该帧。

组态步骤

按照以下步骤为端口分配 ACL 规则：

1. 在“Ports”下拉列表中选择端口。
2. 在“Rules”下拉列表中选择 ACL 规则。
3. 单击“Add”按钮。 会在表中生成一个新条目。

按照以下步骤删除端口的 ACL 规则：

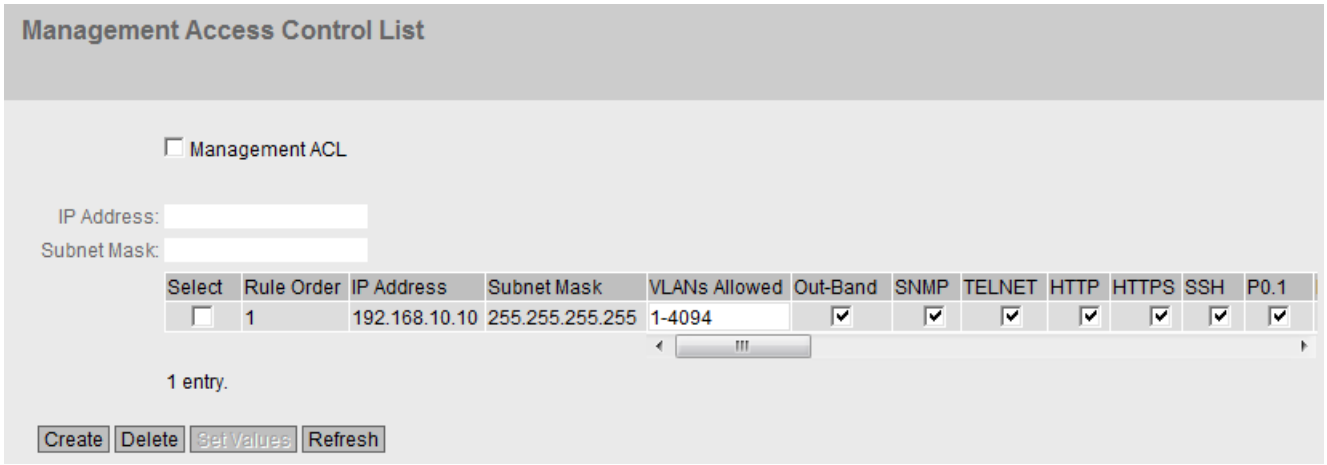
1. 在“Ports”下拉列表中选择端口。
2. 在“Rules”下拉列表中选择 ACL 规则。
3. 单击“Remove”按钮。 将从表中删除相应的条目。

5.7.5 管理 ACL

组态说明

在此页面上，可提高设备的安全性。 要指定具有哪个 IP 地址的工作站允许访问设备，必须组态相应的 IP 地址或一个地址范围。

可选择协议和端口，以便相关工作站可使用此信息访问设备。 可定义该工作站所在的VLAN。这可确保仅 VLAN 内的某些站具有设备的访问权限。



显示框说明

说明

如果启用此功能，请注意以下几点

“管理访问控制列表”(Management Access Control List) 页面上的不正确组态可能会导致无法访问设备。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 IP 地址或网络地址。 如果使用 IP 地址 0.0.0.0，此设置将适用于所有 IP 地址。

- **子网掩码 (Subnet Mask)**
  输入子网掩码。 子网掩码 255.255.255.255 用于特定的 IP 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：

- **Select**
  选择要删除的行。
- **规则顺序 (Rule Order)**
  显示 ACL 规则的顺序。
- **IP 地址 (IP Address)**
  显示 IP 地址。
- **子网掩码 (Subnet Mask)**
  显示子网掩码。
- **允许的 VLAN (VLANs Allowed)**
  输入设备所在 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。
- **Out-Band**
  指定 IP 地址是否可以通过带外端口访问交换机。
- **SNMP**
  指定工作站（或 IP 地址）是否可以使用 SNMP 协议访问设备。
- **TELNET**
  指定工作站（或 IP 地址）是否可以使用 TELNET 协议访问设备。
- **HTTP**
  指定工作站（或 IP 地址）是否可以使用 HTTP 协议访问设备。

- **HTTPS**
  指定工作站（或 IP 地址）是否可以使用 HTTPS 协议访问设备。
- **SSH**
  指定工作站（或 IP 地址）是否可以使用 SSH 协议访问设备。
- **Px.y**
  指定站点（或 IP 地址）是否可以通过此端口（插槽端口）访问该设备。

组态步骤

更改条目

1. 组态要修改的条目数据。
2. 单击“Set Values”按钮将更改传输到设备。

创建新条目

说明

请注意，错误的组态可能意味着您再不能访问设备。
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。

1. 在“IP Address”输入框中输入设备的 IP 地址，在“Subnet Mask”输入框中输入相应的子网掩码。
2. 单击“Create”按钮在表中创建新行。
3. 组态新行的条目。
4. 单击“Set Values”按钮将新条目传输到设备。

删除条目

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。 将删除条目并更新页面。

故障排除/FAQ

6

6.1 不能通过 WBM 或 CLI 进行固件更新

原因

如果固件更新期间发生电源故障，可能无法再通过基于 Web 的管理或命令行接口访问工业以太网交换机。

解决方法

如果使用 WBM 或 CLI 无法访问工业以太网交换机，您可以使用 TFTP 将固件下载到您的工业以太网交换机。

按照以下步骤操作，使用 TFTP 加载新固件：

1. 关闭工业以太网交换机的电源。
2. 按住“复位”(Reset) 按钮，同时重新连接工业以太网交换机的电源。
3. 按住按钮，直至约 30 秒后红色故障 LED (F) 开始闪烁。
4. 释放按钮。
   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. 通过以太网接口将 PC 与工业以太网交换机的带外接口连接。
6. 使用 Primary Setup Tool 为工业以太网交换机分配一个 IP 地址。
7. 在命令提示符中，切换到包含新固件的文件所在的目录，然后执行命令“tftp -i <ip 地址> PUT <固件>”。 也可以使用不同的 TFTP 客户端。

结果

固件传送到工业以太网交换机。

说明

请注意，传送固件可能需要几分钟的时间。 传送过程中，红色错误 LED (F) 会闪烁。

固件完全传送到工业以太网交换机后，工业以太网交换机将自动重启。

索引

硬

优

制

重

注

转

子

组