SIEMENS

SIMATIC NET

工业以太网交换机 SCALANCE X-300/X408-2 V4.1.8 / SCALANCE X414-3E V3.10.2

配置手册

前言

安全建议 1

简介 2

工业网络的网络管理 3

IP 地址分配 4

使用基于 Web 的管理和命令行接口进行组态 5

通过 SNMP 进行组态和诊断 6

PROFINET IO 功能 7

C-PLUG 8

固件更新 9

附录 A A

附录 B B

附录 C C

附录 D D

附录 E E

使用的加密方法 F

07/2024
C79000-G8952-C187-35

法律资讯

警告提示系统

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

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

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

⚠ 小心
表示如果不采取相应的小心措施，可能导致轻微的人身伤害。

注意
表示如果不采取相应的小心措施，可能导致财产损失。

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

合格的专业人员

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

按规定使用 Siemens 产品

请注意下列说明：

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

商标

所有带有标记符号 ® 的都是 Siemens Aktiengesellschaft 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 Aktiengesellschaft
Digital Industries
Postfach 48 48
90026 NÜRNBERG
德国

C79000-G8952-C187-35
Ⓟ 07/2024 本公司保留更改的权利

前言

本手册的用途

本手册可用来协助您组态 SCALANCE X-300 和 X-400 工业以太网交换机。它概要说明了 SCALANCE X-300/X-400 提供的技术选项，并讲述了如何用基于 Web 的管理以及命令行接口进行组态。

本手册的有效性

本手册适用于下列软件版本：

- 自固件版本 4.1.7 起的 SCALANCE X-300/X408-2
- 自固件版本 3.10.2 开始的 SCALANCE X414-3E
- 自版本 1.0 起的 SINEC PNI
- 截至版本 6.2.1 的 SNMP/OPC 服务器

本手册适用于下列产品线：

- SCALANCE X-300
- SCALANCE X-400

SCALANCE X-300 产品线包含一些产品组（另请参见《工业以太网交换机 SCALANCE X-300 操作说明》中的产品概述）。

本组态手册中的设备名称

本组态手册中的说明总适用于手册中的“手册有效性”下列出的 SCALANCE X-300 和 SCALANCE X-400 产品线设备，仅在该说明与特定产品线设备相关时例外。在后文的说明中，将设备称作“以太网交换机”。

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。
- Internet 上的以下地址：
  50305045 (http://support.automation.siemens.com/WW/view/zh/50305045)

网络安全说明

网络安全性信息

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

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

客户负责防止其工厂、系统、机器和网络受到未经授权的访问。只有在有必要连接时并仅在采取适当安全措施（例如，防火墙和/或网络分段）的情况下，才能将该等系统、机器和组件连接到企业网络或 互联网。关于可采取的工业网络安全措施的更多信息，请访问 https://www.siemens.com/cybersecurity-industry (http://www.siemens.com/industrialsecurity) 。

西门子 不断对产品和解决方案进行开发和完善以提高安全性。西门子 强烈建议您及时更新产品并始终使用最新产品版本。如果使用的产品版本不再受支持，或者未能应用最新的更新程序，客户遭受网络攻击的风险会增加。

要及时了解有关产品更新的信息，请订阅西门子工业网络安全 RSS 源，网址为 https://www.siemens.com/cert (https://www.siemens.com/cert) 。

固件/软件支持的说明

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

商标

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

SCALANCE, C-PLUG, OLM

许可证条款

说明

开源软件

在使用本产品之前，请仔细阅读开源软件的许可证条款。

在所提供的数据介质中，下列文档提供有许可证条款：

- OSS_Siemens_86.pdf
- OSS_SCALANCE-X-300-X408_86.pdf
- OSS_SCALANCE-X414_74.pdf

可在产品 DVD 的以下文件夹中找到这些文档：/Open Source Information

目录

前言 **3**

1 安全建议 **13**

2 简介 **19**

2.1 SCALANCE X-300/X-400 的技术文档 19

3 工业网络的网络管理 **21**

3.1 SCALANCE X-300/X-400 的组态选项 21

3.2 SCALANCE X-300/X-400 的功能和属性 22

3.3 介质冗余选项 28
3.3.1 环型拓扑中的介质冗余 28
3.3.2 MRP 29
3.3.3 MRP 多环网 33
3.3.4 HRP 34

4 IP 地址分配 **35**

4.1 IP 地址的结构 35

4.2 IP 地址的初始分配 36

4.3 通过 SCALANCE X-400 的串行接口分配 IP 地址 37

4.4 用 BOOTP 客户机分配地址 38

4.5 用 DHCP 客户机分配地址 39

4.6 用 SINEC PNI 进行地址分配 40

5 使用基于 Web 的管理和命令行接口进行组态 **41**

5.1 基于 Web 的管理和命令行接口的一般性信息 42
5.1.1 简介 42
5.1.2 “基于 Web 的管理”(WBM) 的 LED 仿真 44
5.1.3 使用基于 Web 的管理 46
5.1.4 命令行接口 (CLI) 46

5.2 系统菜单 50
5.2.1 系统组态 50
5.2.2 系统标识和维护 (I&M) 52
5.2.3 系统重启和默认设置 53
5.2.4 通过 HTTP 进行系统保存与加载 56
5.2.5 通过 TFTP 进行系统保存和加载 61
5.2.6 系统版本号 64

5.2.7 系统密码和登录模式 65
5.2.8 系统 RADIUS 用户组 68
5.2.9 系统 SELECT/SET 按钮 70
5.2.10 系统事件日志表 72
5.2.11 C-PLUG 信息 73
5.2.12 地理坐标 76

5.3 X-300/X-400 菜单 78
5.3.1 X-300/X-400 状态页面 78
5.3.2 环网冗余 82
5.3.2.1 X-300/X-400 环网冗余信息 82
5.3.2.2 X-300/X-400 环网组态 86
5.3.2.3 X-300/X-400 HRP 冗余管理器观察器 90
5.3.2.4 X-300/X-400 备用屏蔽 92
5.3.2.5 X-300/X-400 备用观察器 95
5.3.3 X-300/X-400 故障屏蔽 98
5.3.4 X-300/X-400 计数器 100

5.4 代理菜单 102
5.4.1 代理组态 102
5.4.2 Ping 110
5.4.3 SNMP 111
5.4.3.1 代理 SNMP 组态 111
5.4.3.2 SNMPv1 陷阱组态 116
5.4.3.3 SNMPv3 组的组态 117
5.4.3.4 SNMPv3 用户组态 121
5.4.4 代理超时组态 125
5.4.5 代理事件组态 126
5.4.6 代理数字量输入组态 (SCALANCE X414-3E) 131
5.4.7 代理电子邮件组态 (Agent E-Mail Configuration) 133
5.4.8 代理 Syslog 组态 (Agent Syslog Configuration) 135
5.4.9 代理 DHCP 组态 (Agent DHCP Configuration) 137
5.4.10 时间组态 138
5.4.10.1 代理时间组态 (Agent Time Configuration) 138
5.4.10.2 SNTP 客户端组态 140
5.4.10.3 NTP 客户端组态 142
5.4.10.4 夏令时 (Daylight Saving Time) 144
5.4.11 代理 PNIO 组态 (Agent PNIO Configuration) 148
5.4.12 管理访问控制列表 149

5.5 “交换机”(Switch) 菜单 154
5.5.1 交换机组态 (Switch Configuration) 155
5.5.2 端口状态 (Port status) 160
5.5.3 Link Check (SCALANCE X-300/X408-2) 166
5.5.4 端口镜像 171
5.5.5 链路汇聚 173

5.5.5.1 链路汇聚 173
5.5.5.2 LACP 组态 (LACP Configuration) 178
5.5.6 IEEE 802.1x 179
5.5.6.1 802.1x RADIUS 组态 (802.1x RADIUS Configuration) 179
5.5.6.2 802.1x 端口参数 181
5.5.6.3 802.1x 端口组态 183
5.5.7 单播过滤器 (ACL) 186
5.5.7.1 Current Unicast Filter (Access Control List) 186
5.5.7.2 访问控制列表学习 (Access Control List Learning) 191
5.5.7.3 访问控制端口组态 (Access Control Port Configuration) 192
5.5.7.4 未知单播屏蔽掩码 193
5.5.8 组播组 194
5.5.8.1 当前组播组 (Current Multicast Groups) 194
5.5.8.2 GMRP 组态 (GMRP Configuration) 199
5.5.8.3 IGMP 组态 (IGMP Configuration) 200
5.5.8.4 未知单播屏蔽掩码 201
5.5.9 广播阻止掩码 (Broadcast Blocking Mask) 202
5.5.10 快速学习 203
5.5.11 负载限制组态 (Load Limits Configuration) (SCALANCE X414-3E) 204
5.5.12 负载限制速率 (Load Limits Rates) (SCALANCE X-300/X408-2) 207
5.5.13 VLAN 210
5.5.13.1 当前 VLAN 组态 (Current VLAN Configuration) 210
5.5.13.2 VLAN 端口参数 (VLAN Port Parameters) 217
5.5.13.3 GVRP 组态 (GVRP Configuration) 221
5.5.13.4 VLAN 学习 222
5.5.13.5 X-300 VLAN 端口优先级映射 223
5.5.14 STP/RSTP 225
5.5.14.1 生成树组态 (Spanning Tree Configuration) 225
5.5.14.2 生成树端口参数 (Spanning Tree Port Parameters) 229
5.5.14.3 生成树端口组态 232
5.5.15 MSTP (SCALANCE X-300/X408) 235
5.5.15.1 多重生成树组态 235
5.5.15.2 CIST 端口参数 239
5.5.15.3 MSTP 实例组态 245
5.5.15.4 多重生成树端口组态 247
5.5.16 QoS 251
5.5.16.1 QoS 组态 (QoS Configuration) 251
5.5.16.2 CoS 到队列映射 (CoS to Queue Mapping) 254
5.5.16.3 DSCP 到队列映射 (DSCP to Queue Mapping) 255
5.5.17 LLDP 256
5.5.17.1 LLDP 组态 (LLDP Configuration) 256
5.5.17.2 LLDP 邻居 258
5.5.18 光纤监视协议 259
5.5.19 DCP 组态 (DCP Configuration) 265
5.5.20 DHCP 中继代理 266

5.5.20.1 DHCP 中继代理组态 (DHCP Relay Agent Configuration) 266
5.5.20.2 DHCP 中继代理端口组态 (DHCP Relay Agent Port Configuration) 269
5.5.21 符合 IEEE 1588 的精确时间协议 (PTP) 271
5.5.22 通过 WBM 组态精确时间协议 278
5.5.23 通过 CLI 组态精确时间协议 282
5.5.24 端口诊断 283
5.5.24.1 电缆测试器 (SCALANCE X-300/X408-2) 283
5.5.24.2 SFP 诊断 285
5.5.24.3 POF 诊断 287
5.5.24.4 FM 诊断 288
5.5.24.5 POF 端口 290
5.5.25 回路检测 292
5.5.26 NAT - 网络地址转换 300
5.5.27 统计信息 303
5.5.27.1 数据包大小统计信息 (Packet Size Statistic) 304
5.5.27.2 数据包类型统计信息 (Packet Type Statistic) 307
5.5.27.3 错误统计信息 (Error Statistic) 310
5.6 PoE 菜单项 313
5.7 “路由器”(Router) 菜单 (SCALANCE X414-3E) 317
5.7.1 路由器组态 (Router Configuration) 318
5.7.2 路由器子网 (Router Subnets) 319
5.7.3 当前路由 (Current Routes) 322
5.7.4 RIPv2 组态 (RIPv2 Configuration) 326
5.7.5 RIPv2 接口 (RIPv2 Interfaces) 327
5.7.6 OSPFv2 组态 333
5.7.7 OSPFv2 区域 335
5.7.8 OSPFv2 区域范围 339
5.7.9 OSPFv2 接口 341
5.7.10 OSPFv2 虚拟链路 346
5.7.11 OSPFv2 邻居 351
5.7.12 OSPFv2 状态数据库 353
5.7.13 VRRP 354
5.7.14 VRRP 虚拟路由器 354
5.7.15 VRRP 关联 IP 地址 358
5.7.16 VRRP 统计信息 360
6 通过 SNMP 进行组态和诊断 363
7 PROFINET IO 功能 367
7.1 用 PROFINET IO 进行组态 367
7.2 HW Config 中的设置 374
7.3 通过 PROFINET IO 提供的访问选项 380
7.4 数据记录 0x802A (PDPortDataReal) 391

7.5 MRP 组态 396
8 C-PLUG 405
9 固件更新 409
9.1 通过功能性固件更新固件 409
9.1.1 通过 HTTP/HTTPS 更新固件 409
9.1.2 通过 TFTP 更新固件 409
9.1.3 通过 FTP 更新固件 409
9.2 通过 IE Switch X-400/XR-300 使用引导软件更新固件 410
9.2.1 通过串口更新固件 411
9.2.2 通过以太网端口和 FTP 更新固件 414
9.3 固件降级 414
A 附录 A 415
A.1 SCALANCE X400 串口处的 PC 连接 415
A.2 SCALANCE X300 串口处的 PC 连接 416
B 附录 B 419
B.1 SCALANCE X300/X400 的 MIB 变量 419
C 附录 C 431
C.1 标记帧 431
D 附录 D 433
D.1 SCALANCE X300/X400 的错误消息 433
E 附录 E 441
E.1 在多台工业以太网交换机上使用相同的组态 441
F 使用的加密方法 455
索引 457

安全建议

1

注意
信息安全 在运行设备之前，连接设备并更改用户“admin”和“user”的标准密码。要更改密码，登录时需具有组态数据的写访问权限。

为防止设备和/或网络受到未经授权的访问，请遵循以下安全建议。

常规

- 定期检查设备，以确保遵守这些建议和/或其它内部安全策略。
- 评估位置安全性，并将单元保护机制与适当的产品 (https://www.industry.siemens.com/topics/global/en/industrial-security/pages/default.aspx)配合使用。
- 断开内部和外部网络时，攻击者无法从外部访问内部数据。因此请仅在受保护的网络区域内运行该设备。
- 对于在非安全基础架构中的操作，Siemens 不承担任何产品责任。
- 使用 VPN 进行加密和验证与设备进行的通信。
- 对于通过非安全网络进行的数据传输，使用加密的 VPN 隧道（IPsec、OpenVPN）。
- 正确单独连接（WBM、SSH 等）。
- 查看与设备一起使用的其它 Siemens 产品的用户文档，以获取更多安全建议。
- 通过远程记录，可确保将系统协议转发到中央记录服务器。确保服务器位于受保护的网络内，并定期检查协议是否存在潜在的安全违规情况或漏洞。

物理访问

- 应将该设备限制为仅允许合格人员进行物理访问，因为插入式数据介质可能包含敏感数据。
- 锁定设备上未使用的物理接口。因为即使未经许可，也可以通过未使用的接口对工厂进行访问。

软件（安全功能）

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

验证

说明

可访问性风险 - 数据损失风险

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

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

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

证书和密钥

说明

SCALANCE X300 和 SCALANCE X408-2 的 ECDSA 证书

以下内容适用于 SCALANCE X-300 产品系列的设备和 SCALANCE X408-2 类型的设备（SCALANCE X414-3E 类型的设备不受影响）：

自固件版本 V4.1.4 起，已由之前的 RSA 证书转为使用可实现椭圆形曲线加密的证书（“ECDSA”证书）。仅可使用通过以下曲线生成的 PEM 格式的 ECDSA 证书：

- secp256r1 (NIST P-256)
- secp384r1 (NIST P-384)
- secp521r1 (NIST P-521)

自该固件版本开始，不再支持 RSA 证书。设备中现有的 RSA 证书会自动替换为自签名 ECDSA 证书。

- 设备上预设的密钥长度为 256 位的 SSL 证书可用于椭圆形曲线加密。将该证书替换为自制的含密钥证书。建议您使用由可靠外部或内部认证机构签署的证书。
- 使用认证机构（包括密钥撤销与管理）来签署证书。
- 确保用户自定义的私人密钥都受到保护，未授权人员无法访问。
- 验证服务器和客户端上的证书和指纹，避免“中间人”的攻击。
- 建议使用密钥长度至少为 256 位的证书。
- 如果怀疑发生泄露，请立即更改证书和密钥。

安全/非安全协议

- 应避免使用或禁用非安全协议，例如 Telnet 和 TFTP。由于历史原因，这些协议可用，但并不适用于安全应用。请慎重对设备使用非安全协议。
- 检查是否有必要使用以下协议和服务：
  - 未验证和未加密的端口
  - MRP、HRP
  - LLDP
  - DHCP 选项 66/67

  以下协议具有安全备选方法：
  - HTTP → HTTPS
  - TFTP → FTPS
  - Telnet → SSH
  - SNTP → NTP
    检查是否有必要使用 NTP。NTP 的分类为非安全协议。在 NTP 服务器支持安全 NTP 的情况下激活此协议，并使用安全 NTP 的验证和加密机制。
  - SNMPv1/v2c → SNMPv3
    检查是否有必要使用 SNMPv1/v2c。SNMPv1/v2c 被归为非安全协议。使用阻止写访问的选项。设备会为您提供适合的设置选项。
    如果 SNMP 已启用，请更改社区名称。如果不需要不受限制的访问，请通过 SNMP 限制访问。
    使用 SNMPv3 的验证和加密机制。
- 在物理保护措施未阻止设备访问时使用安全协议。
- 如果需要非安全协议和服务，请仅在受保护的网络区域内运行该设备。
- 、将可用于外部的服务和协议限制到最少。
- 要使用 DCP 功能，请在调试后启用"DCP 只读"(DCP Read Only) 模式。

可用协议

以下列表概要介绍了打开的协议端口。

该表包括以下列：

- **协议**
- **端口号**
- **端口状态**
  - 打开
  - 关闭

- **出厂设置**
  表示产品交付时或复位为出厂设置时的状态。
- **验证**
  指定是否对通信伙伴进行验证。
- **加密**
  指定传输是否已加密。

协议	端口号	端口状态	出厂设置	身份验证	加密 [1]
FTP	TCP/21	打开	打开	✓	-
SSH	TCP/22	打开	打开	✓	✓
TELNET	TCP/23	打开（组态后）	关闭	✓	-
HTTP	TCP/80	打开（组态后）	打开	✓	-
PROFINET 服务	TCP/84	打开	打开	-	-
HTTPS	TCP/443	打开	打开	✓	✓
DHCP	UDP/68	打开（组态后）	打开	-	-
SNTP	UDP/123	打开（组态后）	关闭	-	-
NTP（安全）					✓
SNMP	UDP/161	打开（组态后）	打开	✓	✓ (SNMPv3)
RADIUS	UDP/1812、1813	打开	打开	✓	-
PROFINET	UDP/34964 UDP/ 49152、49153 *)	打开（组态后）	打开	-	-

[1] 有关更多信息，请参见 WBM 附录“使用的加密方法 (页 455)”中使用的加密方法。

*) 这些端口动态分配，可能与此处指定的值有所不同。

解除调试

正确关闭设备，以防止未经授权的人员访问设备内存中的机密数据。

为此，需要恢复设备的出厂设置。

还要恢复存储介质的出厂设置。

简介 2

2.1 SCALANCE X-300/X-400 的技术文档

本组态手册的内容

本手册介绍了以太网交换机的组态。

如果要使用如 SNMP、快速生成树、VLAN、路由 (SCALANCE X414-3E) 或电子邮件等功能，则需要对工业以太网交换机进行组态。 手册还介绍了固件更新以及 C-PLUG 方面的问题。

进行组态之前，必须安装并连接好设备。 可以在操作说明中找到安装及连接设备的必要步骤。

下表给出了相关信息所对应的章节。

主题	章节
希望从总体上了解 工业以太网交换机的文档。	第 1 章
想要了解以太网交换机有哪些功能和组态选项。	第 2 章
想要了解如何构造 IP 地址，以及为以太网交换机分配 IP 地址时有哪些办法。	第 3 章
想要对以太网交换机进行组态以及需要获取相关 CLI 命令的信息，或者要了解需要对“基于 Web 的管理”的哪一页进行编辑。	第 4 章
要了解如何用 SNMP 管理以太网交换机。	第 5 章
要了解如何对所连接的以太网交换机使用 PROFINET IO 选项。	第 6 章
想要了解组态卡 C-PLUG 的可用选项。	第 7 章
想要更新固件。	第 8 章

操作说明的内容

“工业以太网交换机 SCALANCE X-400 操作说明”以及“工业以太网交换机 SCALANCE X-300 操作说明”不仅包含有关交换机的基本信息，还包含了对以太网交换机、媒介模块及扩展模块的产品说明。 这些说明还描述了以太网交换机的调试（安装、布线、使用模块等）。

工业以太网交换机 X-300 和 X-400 技术文档概述

X-300 产品线的技术文档分为硬件和软件文档，并且可在以下文档中找到：

- **PH** - 组态手册 (PDF)
  产品线 X-300 和 X-400 的组态手册 (PH) 介绍了软件。
- **BAK** - 纸质精简版操作说明
  精简版操作说明 (BAK) 介绍了各产品组的硬件。
- **BA** - 操作说明 (PDF)
  可以在该操作说明 (BA) 中找到所有产品组的硬件和一般性信息。

内容	产品组	文档类型	文档标识号
软件说明	X-300 和 X-400 产品线的所有设备	**PH X-300/X-400**	C79000-G89000-C187
硬件说明	X-300 产品线的所有设备	**BA X-300**	A5E01113043
	X-300	**BAK X-300**	A5E00982643
	X-300M	**BAK X-300M**	A5E02630801
	XR-300M	**BAK XR-300M**	A5E02661171
	X-300 EEC	**BAK X-300 EEC**	A5E02630809
	XR-300M EEC	**BAK XR-300M EEC**	A5E02661176
	X-300 PoE	**BAK X-300 PoE**	A5E02630809
	XR-300M PoE	**BAK XR-300M PoE**	A5E02630810
	MM900（媒介模块）	**BAK MM900**	A5E02661178
	SFP（收发器）	**BAK SFP** **注意事项宣传册**	A5E02630804 A5E02648904
	X-400 产品线的所有设备	**BA X-400**	C79000-G8976-C186
	X-400	**BAK X-400**	A5E01020054
	X-400EM（扩展模块）	**BAK X-400EM**	A5E00367421
	X-400 媒介模块	**BAK X-400 媒介模块**	A5E00367420

工业网络的网络管理 3

3.1 SCALANCE X-300/X-400 的组态选项

以太网端口

如果已分配 IP 地址（参见"IP 地址分配"部分），则可通过交换机端口（带内端口）对工业以太网交换机进行组态。

通过以太网接口，可以使用以下协议或服务：

- 基于 Web 的管理（基于 HTTP 和 HTTPS）
- TELNET
- SSH
- SNMP
- Trap
- FTP
- TFTP
- 电子邮件
- Syslog

  说明

  使用 SCALANCE X414-3E 时，在 CPU 模块上还有一个快速以太网端口（带外端口）。

- SMTP

RS 232 接口

工业以太网交换机 X-400/XR-300 具有 RS 232 接口。可以用空调制解调器电缆和终端程序（如 Windows 下的 HyperTerminal，另请参见附录 A）将 PC 或 PG 连接到该端口。使用该端口为带外端口（仅 SCALANCE X414-3E）或带内端口（参见“通过串行端口分配 IP 地址”部分）手动分配 IP 地址。也可用整个 CLI 命令集。

说明

也可以在网络中断时通过串行端口或 CPU 模块的以太网端口访问工业以太网交换机管理程序（带外管理）。

3.2 SCALANCE X-300/X-400 的功能和属性

现有 10 Mbps 和 100 Mbps 子网的集成

工业以太网交换机会在其双绞线端口自动检测以下内容：

- 发送和接收电缆对（自动跨接）
- 数据传输速率（10 Mbps 或 100 Mbps）
- 运行模式（全双工或半双工）

如此将允许用户很容易地通过双绞线将子网和工业以太网交换机相集成。

说明

即使在使用直通电缆时，也可能在以太网网络中出现不合法环路，如将两个端口连接到同一台工业以太网交换机。此类环路可能导致网络过载和网络故障。

说明

如果将工业以太网交换机连接到不是在自动协商模式下运行的伙伴设备，则必须将端口永久设置成与伙伴设备的参数一致。

如果不手动设置连接的两端，则检测不到双工模式。此时会使用半双工模式，造成性能下降和通信冲突。

如果关闭自动协商，也会禁用自动跨接，可能需要使用交叉网络电缆。

千兆位以太网端口

这些端口尤其适合交换机之间的高性能连接，并具有以下特性：

- 自动检测发送和接收电缆对（自动跨接）。
- 数据传输率为 10 Mbps、100 Mbps 或 1000 Mbps
- 全双工

说明

1 Gbps 的数据传输至少需要 4 x 2 线的 Cat 5e 双绞线电缆。使用 4 线电缆（2 x 2 线）时，最大数据传输速率为 100 Mbps。

环网中的快速冗余

从固件版本 V3.0.0 开始，工业以太网交换机可以处理以下冗余过程：

- 环网中 MRP 的最长重新组态时间为 200 ms
- HRP 的最长重新组态时间为 300 ms

网段的冗余连接

通过适当的布线和相应的组态，可以使得由工业以太网交换机（SCALANCE X-200 或 X-300/X-400 或 OSM/ESM）组成的环形或线性总线结构实现冗余连接。（另请参见"X-400 Standby Mask"菜单项部分）。
最长故障切换时间为 300 ms。

有关网段的冗余连接和环型拓扑中的介质冗余的详细信息，请参见操作说明“工业以太网交换机 SCALANCE X-400"或“工业以太网交换机 SCALANCE X-300"。

存储并转发

工业以太网交换机会计算入站数据包的 CRC 总数，仅转发包含有效校验和的数据（存储并转发）。交换机不会转发不良数据包。存储并转发功能也允许通过不同传输率在同一个网络中的不同连接上运行。

虚拟网络支持（基于 VLAN 端口）

虚拟网络 (VLAN) 和正常 LAN 之间并没有物理上的差异。VLAN 的特性是可以在组态期间将设备分配给一个设备组。多个这样的设备组共用在物理上实际仅存在一次的网络基础结构。在同一个物理网络中便形成了多个“虚拟网络”。仅可以在同一个 VLAN 内进行数据交换、甚至是传输广播数据。

通过扩展帧来实现 VLAN 分配。将四个字节的附加信息插在目标地址和源地址之后。有关帧标记的详细信息，请参见附录 C。

为能将不支持 VLAN 的终端设备和子网集成到虚拟网络中，交换机还可以处理 VLAN 附加信息（VLAN 标记）的添加和删除。工业以太网交换机支持基于端口进行分配，然后通过这些端口连接设备（基于端口的 VLAN）。

- X-400
  可组态多达 62 个基于端口的 VLAN 以及两个预定义的 VLAN。VLAN 对应于 IEEE 802.1Q 标准。
- X-300
  可组态多达 253 个基于端口的 VLAN 以及两个预定义的 VLAN。VLAN 对应于 IEEE 802.1Q 标准。

生成树

生成树协议 (STP) 允许创建在两个站之间有多个连接的网络结构。生成树只允许使用一条路径并且禁止其它（冗余）端口进行数据通信。这样可防止在网络中形成环路。如果发生网络中断，则会找到一条备用路径用于传送数据。

生成树在 IEEE 802.1D-1998 标准中定义。

快速生成树

快速生成树协议 (RSTP) 是生成树协议 (STP) 的扩展。RSTP 在正常运行期间已经收集到有关备选路径的信息，这是其与 STP 的主要区别。如果发生故障，此信息立即可用。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。工业以太网交换机既支持快速生成树，也支持生成树。

快速生成树在 IEEE 802.1D-2004 标准中定义。

多重生成树

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，MSTP 还允许在不同的 VLAN 或 VLAN 组中使用单独的 RSTP 实例。例如，这使通信路径在各个 VLAN 中可用，而简单的快速生成树协议则会造成数据通信全局阻塞。

多重生成树在 IEEE 802.1Q 标准中定义。

C-PLUG

C-PLUG 是一种可互换存储介质，工业以太网交换机的全部组态信息都存储在其中。更换工业以太网交换机时，仅需将之前设备的 C-PLUG 插入新设备即可。然后，该新的工业以太网交换机就会以之前设备的组态启动。

MAC 地址表

工业以太网交换机的 MAC 地址表包含了有关应将接收帧转发到哪个（哪些）端口的信息。该表可能既包含静态条目（由用户插入），又包含动态条目（通过工业以太网交换机接收的帧获得）。

访问控制

说明

在 2.2.0 之前的固件版本中，该属性称为“锁定端口”。

如果激活端口的这一功能，则在地址表中存在相应源地址的情况下，工业以太网交换机仅转发在此端口接收到的帧。

可以自动将全部连接的节点输入访问控制列表。

说明

不能在访问控制*启用*的情况下对环网端口进行组态。

符合 IEEE 802.1x 标准的网络访问保护

根据 IEEE 802.1x，可以为支持验证的终端设备组态端口。通过 RADIUS 服务器进行验证，且必须能通过网络访问到该服务器。

镜像

镜像功能允许将一个端口的数据流镜像到另一个端口。然后可在该监视端口对数据流进行分析，而不影响正常通信。

电子邮件功能

可以对工业以太网交换机进行组态，以便在特定事件发生时发送电子邮件通知。

事件日志表

事件日志表记录工业以太网交换机在操作期间发生的事件。用户可以指定将生成表中条目的事件。

时钟同步

工业以太网交换机允许将系统时间与外部时间发送器同步。要使用该功能，必须有像 SICLOCK 这样的时间发送器，或者有工业以太网交换机可对其帧进行评估的 SNTP 服务器或 NTP 服务器。然后，事件日志表中的条目将具有在整个系统内一致的时间戳。因此可以根据事件在系统中发生的时间对其进行分类，从而加快对问题原因的识别。

流量控制

工业以太网交换机支持半双工和全双工模式下的流量控制。

BOOTP/DHCP

工业以太网交换机可从 BOOTP 或 DHCP 服务器动态获取 IP 地址。

从固件版本 2.0 开始，只要 DHCP 已启用，就可以选择 DHCP 模式。在之前的固件版本中，通过 MAC 地址来运行 DHCP。

说明

如果已启用路由功能（仅 SCALANCE X414-3E），则 DHCP 和 BOOTP 无效。

说明

DHCP 和 BOOTP 仅对带内代理 IP 组态有效。只能手动设置 SCALANCE X414-3E 的带外代理 IP。

也可以通过 DHCP 选项 66 或 67 加载组态文件。

PROFINET IO

从固件版本 2.0 开始，支持将交换机作为 PROFINET IO 设备进行操作。

TELNET

可使用 TELNET 通过 LAN 或 Internet 控制工业以太网交换机的命令行接口。

说明

最多可同时有三个 CLI 连接，即串口连接（仅以太网交换机 X-400）和 LAN 连接。
自固件版本 4.1.3 起，在交付状态下或设备复位为出厂设置后，TELNET 将被禁用。出于安全考虑，建议使用 SSH。

SSH

可使用 SSH 通过 LAN 或 Internet 控制工业以太网交换机的命令行接口。

说明

最多可同时有三个 CLI 连接，即串口连接（仅以太网交换机 X-400）和 LAN 连接。

SNMPv3

工业以太网交换机支持 SNMPv1、SNMPv2c 和 SNMPv3。此外，SNMPv3 提供协议级的用户管理功能以及安全功能（如验证）。可使用基于 Web 的管理、命令行接口或通过直接访问 MIB 对象对 SNMPv3 的用户和组进行组态。

Syslog

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。这需要一个标准 Syslog 服务器。

DHCP 选项 82

DHCP 中继功能允许根据所连接的交换机端口对终端设备的 IP 地址进行初始化。该功能支持“DHCP 选项 82”(DHCP Option 82)。

IGMP 监听和 IGMP 查询器

工业以太网交换机不但支持 IGMP 监听，还支持 IGMP 查询器功能。如果启用 IGMP 监听，就会评估 IGMP 数据包，并用该评估信息更新组播过滤表。如果还启用了 IGMP 查询，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。

仅限 SCALANCE X414-3E：第 3 层功能（路由）

也可以将 SCALANCE X414-3E 组态成路由器。这样就可以连接到各种 IP 子网。可以输入静态路径和/或启用 RIP/OSPF 和 VRRP 路由器协议。通过使用这些标准化协议，SCALANCE X414-3E 可以使组态与网络中的其它路由器进行同步。

3.3 介质冗余选项

可以采用多种办法来增强具有光学或电气线性总线拓扑的工业以太网网络的可用性。

- 网络网格化
- 并联传输路径
- 使线性总线拓扑闭合成环型拓扑

3.3.1 环型拓扑中的介质冗余

环型拓扑的结构

环型拓扑中的节点可以是外部交换机和/或通信模块的集成交换机。

要建立具有介质冗余的环型拓扑，需要将线性总线拓扑的两个自由端接到同一个设备中。使用环中某设备的两个端口（环网端口）可使线性总线拓扑闭合成环网。该设备就是冗余管理器。环中的所有其它设备是冗余客户端。

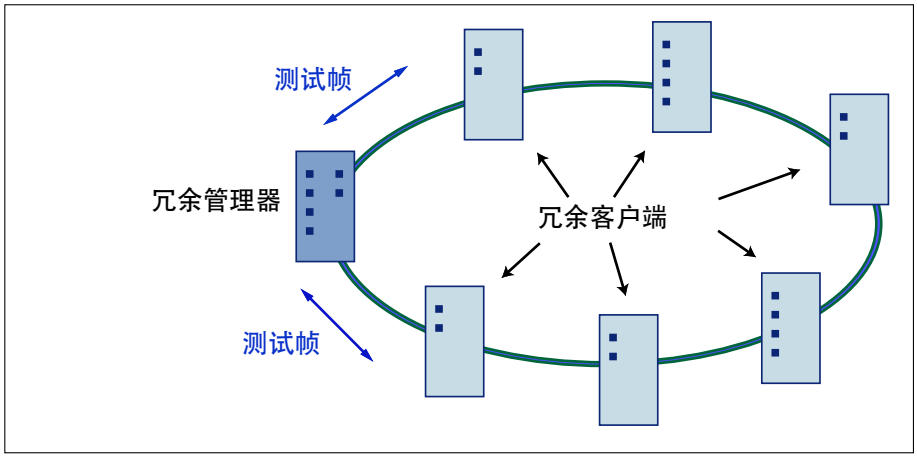


图 3-1　具有介质冗余的环型拓扑中的设备

设备的两个环网端口是用来与环型拓扑中相邻两个设备建立连接的端口。可在相关设备的组态中选择并设置环网端口。在 STEP 7 和 S7 以太网 CP 模块上，环网端口的端口号后标有“R”。

说明

在物理关闭环网之前，请将 STEP 7 项目的组态下载到各个设备。

环型拓扑中介质冗余的工作原理

使用介质冗余功能时，如果环在某点中断，则将重新组态各设备间的数据路径。重新组态拓扑后，可再次在生成的新拓扑中访问到设备。

在冗余管理器中，如果网络未中断，则 2 个环网端口彼此是断开的。这可防止数据帧循环传送。就数据传输而言，该环型拓扑是一个线性总线拓扑。冗余管理器用于监视环型拓扑。它通过从环网端口 1 和环网端口 2 发送测试帧来执行监视。测试帧沿两个方向在环中传播直到到达冗余管理器的另一个环网端口。

环中两个设备间的连接中断或其中某个设备发生故障都会导致环中断。

如果冗余管理器的测试帧由于环网内的中断不再能够到达另一个环网端口，则冗余管理器将连通自身的两个环网端口。这一替代路径将以线性总线拓扑形式再次恢复所有剩余设备的功能性连接。

中断消失后，将再次建立原通信路径，断开冗余管理器的两个环网端口并通知冗余客户机该变化。然后，冗余客户机使用新路径连接到其它设备。

环中断到恢复线性拓扑的时间称为重新组态时间。

如果冗余管理器故障，环将变成普通的线性总线。

介质冗余方法

SIMATIC NET 产品支持以下介质冗余方法：

- HRP（高速冗余协议）
  重新组态时间：0.3 秒
- MRP（Media Redundancy Protocol，介质冗余协议）
  重新组态时间：0.2 秒

这些方法的机制相类似。不能在一个环中同时使用 HRP 和 MRP。

3.3.2 MRP

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

IEC 62439-2:2021 Industrial communication networks - High availability automation networks Part 2: Media Redundancy Protocol (MRP)

环中断后的重新组态时间最长为 200 ms。

拓扑

下图显示了使用 MRP 的环中设备的可能拓扑。

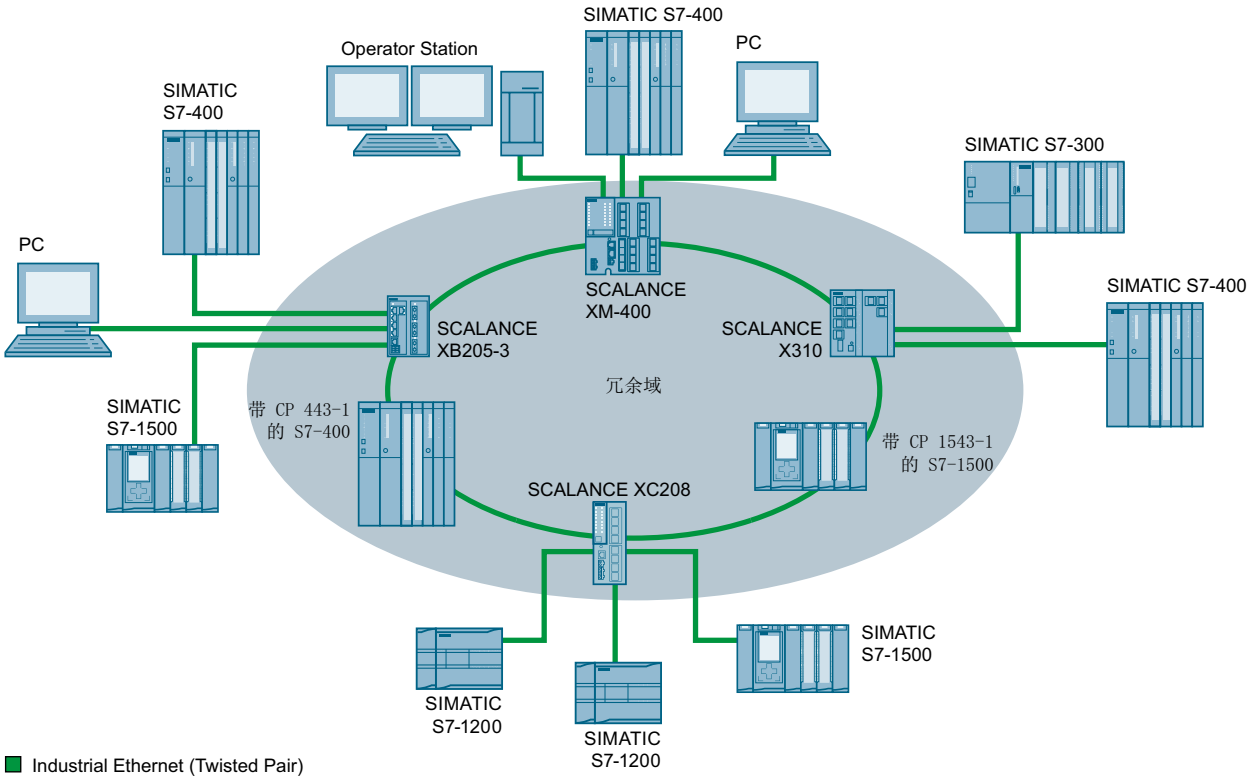


图 3-2　支持 MRP 介质冗余协议的环型拓扑示例

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 交换机或带具有 MRP 功能的 CP 的 PC 连接到环中。

要求

使用 MRP 介质冗余协议进行无故障操作的要求如下：

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

参见

X-300/X-400 环网组态 (页 86)

说明

设备数

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。

组态

可如下组态单 MRP 环网：

- 使用基于 Web 的管理，请参见 "环网冗余 (页 82)"部分
- 使用 STEP 7，请参见 "MRP 组态 (页 396)"部分

支持 MRP 的设备

要在环型拓扑中使用 MRP，拓扑中只能包括支持此功能的设备。 例如，这包括下列设备：

- 工业以太网交换机
  - 自固件版本 V4.0 开始的 SCALANCE X-200
  - 自固件版本 V4.0 开始的 SCALANCE X-200IRT
  - 自固件版本 V3.0 开始的 SCALANCE X-300
  - 自固件版本 V3.0 开始的 SCALANCE X-400
- 通信处理器
  - 自固件版本 V2.0 开始的 CP 443-1 Advanced (6GK7 443-1GX20-0XE0)
  - 自固件版本 V1.0 开始的 CP 343-1 Advanced (6GK7 343-1GX30-0XE0)
  - 自固件版本 V2.2 开始的 CP 1616 (6GK1 161-6AA00)
  - 自固件版本 V2.2 开始的 CP 1604 (6GK1 160-4AA00)
- 支持 MRP 的第三方设备。

SCALANCE X-300 模块化交换机的连接

说明

SCALANCE X-300 - 模块化设备 (M)

请记住，在模块化交换机中，环网端口位于 MM900 媒介模块上。

3.3.3 MRP 多环网

拓扑

借助 MRP 多环网功能，可使用一台中央冗余管理器控制最多 4 个 MRP 环网。

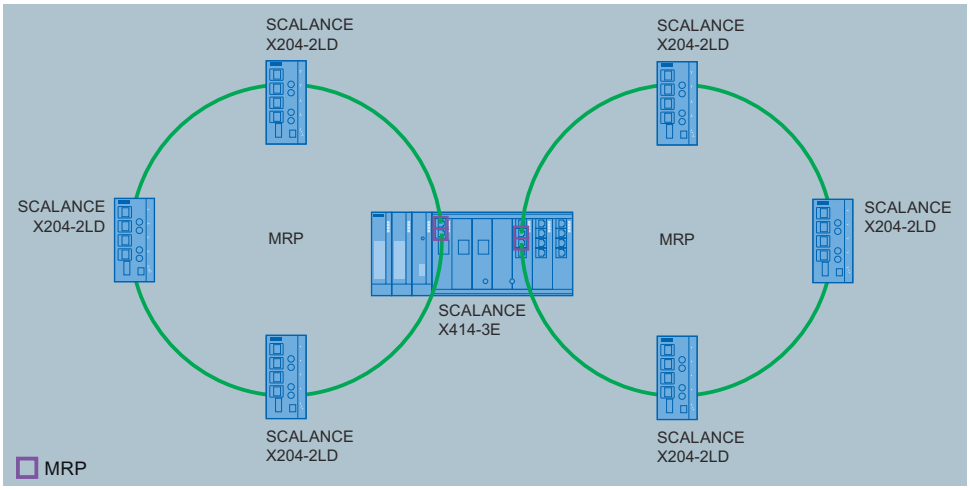


图 3-3 MRP 多环网

组态

只能使用 PROFINET 来组态 MRP 多环网，请参见 “MRP 组态 (页 396)”部分。

带 MRP 多环网的冗余管理器

可将下列产品线的所有设备用作连接多环网的冗余管理器：

- 自固件版本 V4.0 开始的 SCALANCE X-300
- SCALANCE X-400
  - 自固件版本 V4.0 开始的 SCALANCE X408-2
  - 自固件版本 V3.10 开始的 SCALANCE X414-3E

3.3.4 HRP

说明

名称更改

介质冗余协议“高速冗余协议”的缩写已经从 HSR 更改为 HRP。
这只是名称的更改；功能并未修改。 HSR 和 HRP 节点可以在环网中一起运行。

使用“HRP”媒介冗余方法，可在环中断后的 0.3 秒时间内完成重新组态。

要求

要无故障运行 HRP，必须满足以下要求：

- 在具有最多 50 个设备的环型拓扑中支持 HRP。
  在含有 SCALANCE X-200 和 SCALANCE X-300 工业以太网交换机的拓扑中，最多支持 100 个节点。
  超过此设备数可能导致通信数据丢失。
- 要在其中使用 HRP 的环只能包括支持此功能的设备。 例如，这包括下列设备： X-400 工业以太网交换机、X-300 工业以太网交换机、X-200 工业以太网交换机和 OSM/ESM。
- 所有设备必须通过其环网端口互连。
  在两台工业以太网交换机之间可实现最长 3 km 的多模连接和最长 26 km 的单模连接。 在更远的距离，指定的重新组态时间可能更长。
- 必须将环中一个设备组态为冗余管理器，通过选择“HRP 管理器”(HRP Manager) 设置来执行。 可以通过设备前面板上的按钮、基于 Web 的管理、CLI 或 SNMP 来完成此组态。
- 在环中所有其它设备上，必须激活“HRP 客户机”(HRP Client) 或“自动冗余检测”(Automatic Redundancy Detection) 模式。
  可以通过基于 Web 的管理、CLI 或 SNMP 来执行此操作。
- 最初的默认设置是“HRP 客户机”或“自动冗余检测”模式。

IP 地址分配

4

简介

工业以太网交换机提供范围广泛的设置和诊断功能。 要通过网络访问这些功能，可使用 Internet 协议。

Internet 协议具有自身的使用 IP 地址的寻址机制。 作为 ISO/OSI 参考模型第 3 层协议，IP 协议与允许灵活地址分配的硬件无关。 与第 2 层通信（其中，MAC 地址永久性地分配给设备）不同，这要求必须明确为设备分配一个地址。

本部分介绍了 IP 地址的结构以及用工业以太网交换机进行地址分配的各种选项。

工业以太网交换机的 IP 地址类型

工业以太网交换机可以有多个 IP 地址：

- 带外 IP 地址（仅限 SCALANCE X414-3E）用于管理。
- 带内代理 IP 地址用于管理。
- 其它 IP 地址
  仅在出于路由目的设置这些 IP 地址（仅限 SCALANCE X414-3E）。 不能通过 DHCP 组态这些地址，而是必须用 WBM、CLI 或 SNMP 进行分配。

4.1 IP 地址的结构

符合 RFC 1518 和 RFC 1519 的地址类别

IP 地址范围	最大网络数	最大主机/网络数	类别	CIDR
1.x.x.x 到 126.x.x.x	126	16777214	A	/8
128.0.x.x 到 191.255.x.x	16383	65534	B	/16
192.0.0.x 到 223.255.255.x	2097151	254	C	/24
组播组			D	
为试验用途保留			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计算机地址。

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。如果将要定义 16 个子网，则必须将子网地址的第 3 个字节设为 11110000（二进制计数法）。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”（即“1”之间不能有“0”）。

4.2 IP 地址的初始分配

组态选项

不能使用基于 Web 的管理或命令行接口通过 Telnet 或 SSH 为以太网交换机分配初始 IP 地址，因为这些组态工具要求事先已经有 IP 地址。

可通过以下方式将此类地址分配给当前尚没有 IP 地址的未组态设备：

- 使用 CLI 通过串行接口（仅限工业以太网交换机 X-400）
- DHCP（仅通过带内端口）

- BOOTP（仅通过带内端口）
- STEP 7（仅通过带内端口）
- NCM PC
- SINEC PNI（仅通过带内端口）

说明

在模块出厂时或在*复位为出厂默认设置*之后，会默认设置为 DHCP。如果局域网中有 DHCP 服务器，且其能回应工业以太网交换机的 DHCP 请求，则在模块初次启动时会自动分配 IP 地址、子网掩码和网关。通过 DHCP 和 BOOTP 分配的地址就如同永久设置的 IP 地址那样，不会因*复位为出厂默认设置*而被删除。

说明

使用 SCALANCE X414-3E 时，带外端口和带内端口的 IP 地址必须属于不同的子网。

示例：

IP 地址（带外端口）：140.90.45.66

IP 地址（带内端口）：140.91.23.66

子网掩码

（带外端口/带内端口）：255.255.0.0

使用路由功能时，SCALANCE X414-3E 可以有一个以上的带内地址。使用 SINEC PNI 时，只可以分配一个带内地址（代理 IP 地址）。必须用 WBM、CLI 或 SNMP 分配其它地址。

说明

只有 SCALANCE X414-3E 有路由功能。

说明

如果启用路由功能，就不可以用 DHCP/BOOTP 来设置地址。

4.3 通过 SCALANCE X-400 的串行接口分配 IP 地址

通过空调制解调电缆连接和登录

请按如下步骤通过串行端口指定以太网交换机 Switch X-400 的 IP 地址：

1. 通过非调制解调电缆将以太网交换机 X-400 的串行端口连接到 PC。
2. 启动终端仿真程序，如 Windows 中可用的 HyperTerminal 程序（相关设置请参见附录 A）。

3. 建立连接后，消息“登录：”出现。 假设您具有相应访问权限，请输入“admin”（对于管理员）并按回车。
4. 在提示您输入“密码：”(Password:) 时， 输入密码。 请务必阅读以下注意事项。
5. 在出现消息 CLI> 时输入“AGENT”；然后可切换到所需的子菜单。 接下来，您就可以输入组态 IP 地址的命令。 在下一部分对这些命令进行了说明。

说明

如果还未分配新密码（默认出厂设置），则管理员登录的有效密码是“admin”，受限权限用户登录的有效密码是“user”。

通过串行接口成功登录之后，就可以输入命令，直至使用“exit”命令注销为止。 如果 5 分钟内无进一步动作，该会话会自动关闭。

说明

如果密码丢失，可以用 CPU 模块上的 SET/SEL 按钮将以太网交换机 X-300/X-400 复位为出厂设置。 要复位出厂设置，在基本状态显示模式 A 下（LED D1 和 D2 熄灭）按住 SET/SEL 按钮 12 秒钟。 在经过 12 秒钟之前松开该按钮可取消复位。 之前的全部设置都会被出厂默认设置覆盖。 之后，密码“admin”和“user”再次有效。

命令行接口的命令

在“Agent Configuration 菜单项”中对通过 CLI 子菜单 AGENT 发出的 IP 地址组态命令进行了说明。

有关命令行接口的一般性信息，请参见“命令行接口 (CLI)”部分。

4.4 用 BOOTP 客户机分配地址

地址分配的工作原理

BOOTP（Bootstrap Protocol，自举协议）是可用于自动分配 IP 地址的协议。仅当网络中存在 BOOTP 服务器时，才能实现这种地址分配操作。

没有 IP 地址的节点（BOOTP 客户机）将其 MAC 地址与 BOOTP 查询发送给网络中的所有其它设备（MAC 广播地址 FF-FF-FF-FF-FF-FF）。服务器发来的响应也会以广播形式发送，不仅包含 IP 地址，也包含客户机的 MAC 地址。接收到这类响应的客户机可基于 MAC 地址识别出该 IP 地址是否是要分配给自己的。

BOOTP 基于 UDP 协议，BOOTP 服务器使用 UDP 端口 67，客户机使用端口 68。

工业以太网交换机的 BOOTP

发货时，会启用 DCP（因此可通过 SINEC PNI 或 NCM 进行访问）和 DHCP，禁用 BOOTP。

4.5 用 DHCP 客户机分配地址

DHCP 属性

DHCP（Dynamic Host Configuration Protocol，动态主机配置协议）是 BOOTP 的扩展；然而，与 BOOTP 相比，存在几项重大的差异：

- DHCP 的应用不局限在引导阶段；也可以在正常运行期间使用 DHCP。
- 分配的 IP 地址仅在特定时间（称为租用时间）内有效。 超过该时间后，客户机必须请求新 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，当客户机再次请求 IP 地址时，它通常会接收到一个与之前不同的地址。 可是，也可以组态 DHCP 服务器，让它分配固定地址。

说明

一旦 PROFINET IO 控制器分配过一次 IP 地址，DHCP 本身就会自动禁用，而且必须根据需要重新将其激活。

说明

DHCP 采用的机制是 IP 地址仅分配一小段时间（租用时间）。 如果工业以太网交换机在租用时间到期之前没有将新请求发送到 DHCP 服务器，则已分配的 IP 地址、子网掩码和网关都会变为静态条目。

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。

由于 DHCP 客户机也会向服务器发送 RELEASE 命令，因此，服务器可以将该地址分配给其它设备，这样就会在网络中产生冲突。

解决方法：

禁用 DHCP 之后，您应执行下列操作之一

- 将以太网交换机的 IP 地址更改为未由 DHCP 分配的地址
- 将分配给设备的 IP 地址从 DHCP 服务器地址池中删除。

建议不要使用动态地址分配和静态地址分配相结合的方式。

4.6 用 SINEC PNI 进行地址分配

简介

SINEC PNI (SINEC Primary Network Initialization) 用于对网络设备进行初始调试，采用 DCP 协议检测网络中的设备并分配 IP 地址。

先决条件

仅在可通过以太网访问设备的情况下可行。

说明

有关使用的更多信息，请参见 SINEC PNI 文档。

有关详细信息，请参见“PNI (https://support.industry.siemens.com/cs/products?mfn=ps&pnid=26672&lc=zh-CN)”

使用基于 Web 的管理和命令行接口进行组态 5

简介

为尽可能发挥工业以太网交换机的技术潜力，可以根据设备的具体应用环境来调整设备的组态。有两种组态工业太网交换机的途径：

- 使用命令行接口可通过 Telnet（假设存在以太网连接）或串行接口（仅限 IE Switch X-400）访问以太网交换机。
- 使用基于 Web 的管理可通过 Web 浏览器访问工业以太网交换机的组态。必须要有到工业以太网交换机的以太网连接。

说明

根据所选组态方法，集成了以下机制来防止对工业以太网交换机进行未经授权的访问：

- 使用 CLI 通过串行接口（仅限 IE Switch X-400）、TELNET 或 SSK
- 基于 Web 的管理

经过 5 分钟 (CLI) 、15 分钟 (WBM) 或在“代理超时组态”(Agent Timeout Configuration) 菜单中组态的时间过后，会自动注销。也可通过用户界面中相应的按钮进行手动注销。退出浏览器不会关闭会话。如果在超时时间内再次打开浏览器，则会继续使用该会话。

说明

只有在大约 1 分钟后或暖启动前，才会将全部的组态更改应用到闪存中。因此，应在关闭设备之前在命令行接口或基于 Web 的管理中运行“Restart”（重启）命令。这样可以确保已保存了全部的组态更改。

说明

要使用 SNMP 管理、RMON 和陷阱，将需要网络管理站。网络管理站没有随工业以太网交换机一起提供。

5.1 基于 Web 的管理和命令行接口的一般性信息

5.1.1 简介

说明

本部分描述的屏幕对 SCALANCE X-300 和 SCALANCE X-400 均适用。文中显示的屏幕是基于 SCALANCE X-400 给出的。根据组态和设备的不同，可能会有偏差。

基于 Web 的管理原理

工业以太网交换机集成有 HTTP 服务器可供基于 Web 的管理使用。 如果使用 Web 浏览器对工业以太网交换机进行寻址，则交换机会根据用户输入向客户机计算机返回 HTML 页面。

用户在工业以太网交换机发送的 HTML 页面中输入组态数据。 工业以太网交换机评估该信息，并动态生成响应页面。 这种方法最大的优点是，除了 Web 浏览器外，不需要在客户机中安装任何其它特殊软件。

对基于 Web 的管理的要求

- 使用基于 Web 的管理之前，工业以太网交换机必须有 IP 地址。
- 要使用基于 Web 的管理，工业以太网交换机和客户机计算机之间必须存在以太网连接。
- 推荐使用 Microsoft Internet Explorer 版本 5.5 或更高版本。
- 基于 Web 的管理的所有页面都要求 JavaScript。 因此，请确保在浏览器设置中启用 Java 脚本。

说明

不可将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)* 的 *“临时 Internet 文件”(Temporary Internet Files)* 部分，用“设置”(Settings) 按钮进行适当的设置。

在文本 *“检查所存网页的较新版本”(Check for newer versions of stored pages)* 下，必须选中 *“自动”(Automatically)* 复选框。

- 基于 Web 的管理是基于 HTTP 或 HTTPS 的，因此，如果安装了防火墙，还必须允许访问端口 80 或端口 443。

启动基于 Web 的管理并登录

说明

出于安全考虑，请务必更改原始出厂设置的密码：

- 用户名“admin”对应密码“admin”
- 用户名“user”对应密码“user”。

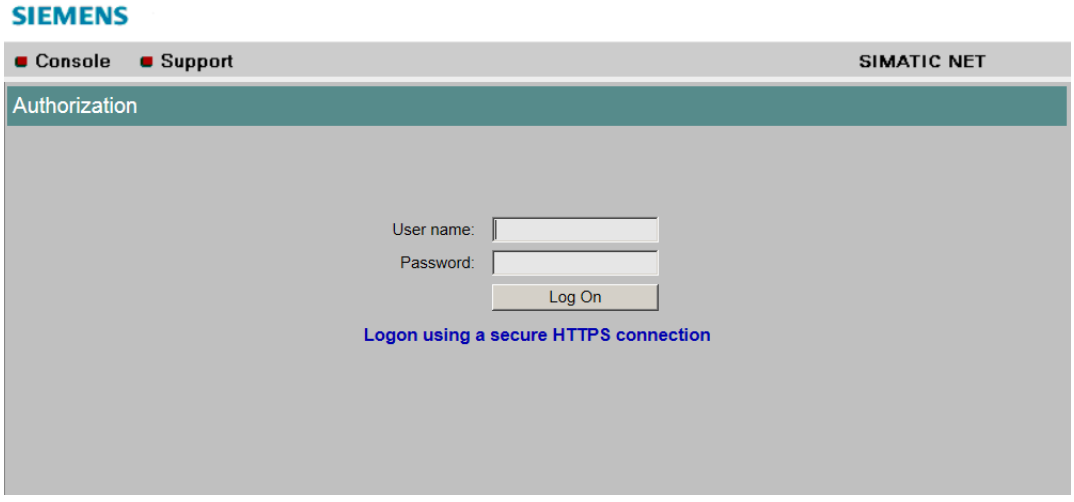


图 5-1　登录对话框

1. 在 Web 浏览器的地址栏中输入工业以太网交换机的 IP 地址或 URL。
   如果工业以太网交换机的连接无故障，则会显示上图所示的基于 Web 的管理登录对话框。
2. 在“用户名”(User name) 输入框中输入用户名。
   可以是以下条目：
   - admin： 使用该用户名时，具有读取和写入访问权限。
   - user： 使用该用户名时，只具有读取访问权限。
   - 存储在 RADIUS 服务器上的用户名： 请参见系统密码和登录模式 (页 65)和 802.1x RADIUS 组态 (802.1x RADIUS Configuration) (页 179)。
3. 输入密码。
4. 单击“登录”(Log On) 按钮启动登录。

5.1.2 “基于 Web 的管理”(WBM) 的 LED 仿真

运行状态显示

工业以太网交换机的每个组件都使用了一个或多个 LED 来提供设备运行状态信息。根据其安装位置，可能不是总能直接访问工业以太网交换机。因此基于 Web 的管理显示的是仿真 LED。

屏幕上方有四分之一的区域用图形方式显示 IE Switch X-300 或 IE Switch X-400 及其现有模块和相应的 LED。通信显示并没有真实地反映实际情况（LED 不闪烁）。有关 LED 显示的含义，可参见操作说明“工业以太网交换机 SCALANCE X-300”或操作说明“工业以太网交换机 SCALANCE X-400”。

单击图形化显示模块上的标签，可以更改仿真的显示模式（LED DM 或 D1/D2），就如同是操作设备上的按钮一样。

说明

只有在插入至少一个模块时，SCALANCE X414-3E 的媒介模块扩展器才会在仿真中显示。

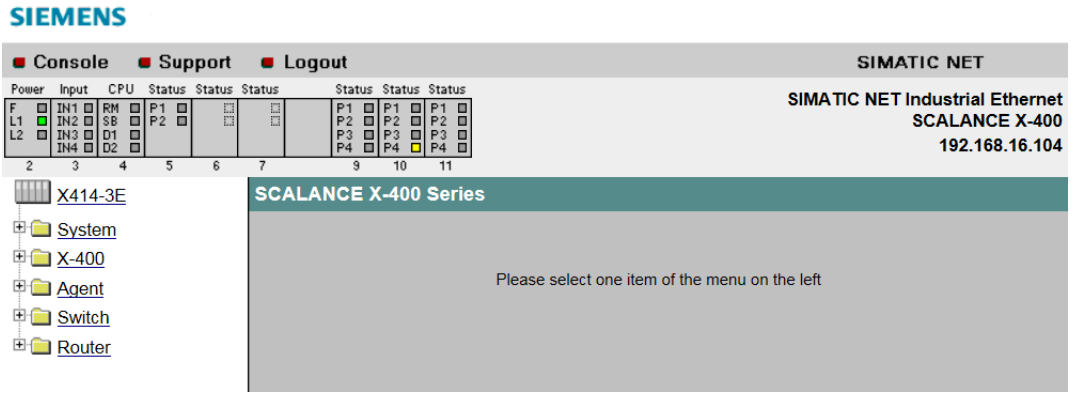


图 5-2 SCALANCE X414-3E LED 仿真

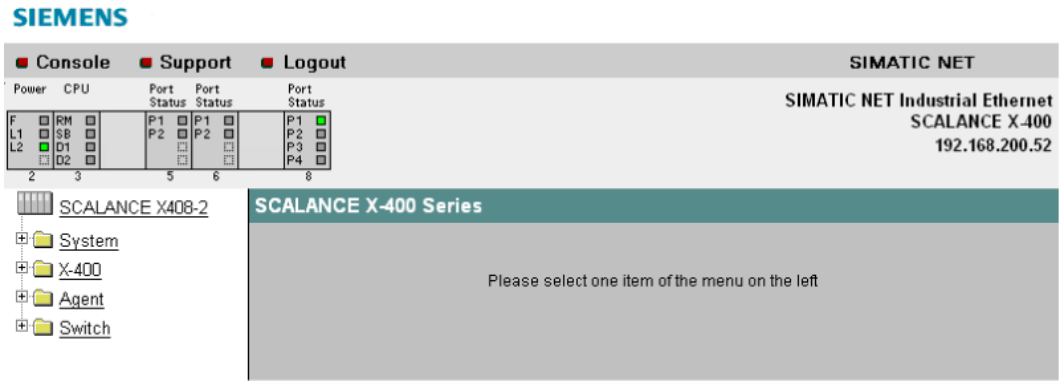


图 5-3 SCALANCE X408-2 LED 仿真

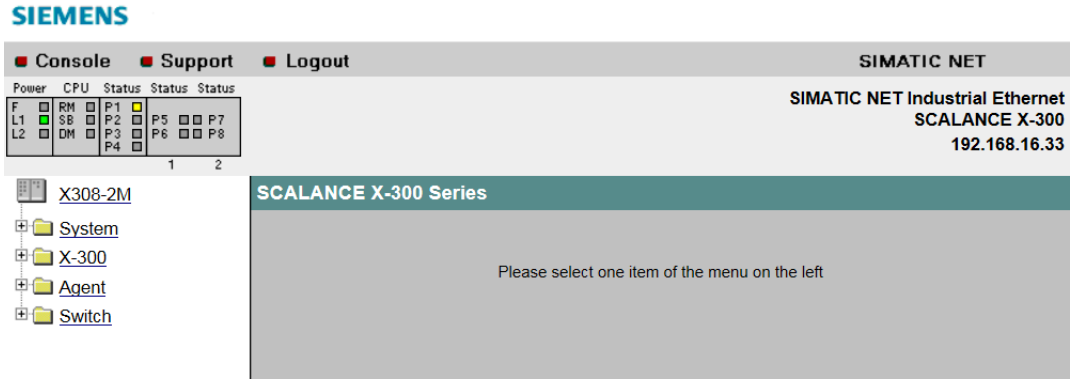


图 5-4 SCALANCE X308-2M LED 仿真

5.1.3 使用基于 Web 的管理

导航栏

WBM 上方的菜单栏包含以下链接：

- 控制台 (Console)

  通过该链接可打开控制台窗口，可以在其中输入 CLI 命令。 然后可通过 TELNET 连接到交换机。

- 支持 (Support)
  单击该链接将打开 SIEMENS AG 支持页面。 但只有 PC 具有 Internet 连接时，才能访问“SIEMENS 支持”页面。

- 注销 (Logout)
  单击该链接可以从设备注销。

用“刷新”(Refresh) 更新显示

基于 Web 的管理中的各个页面底部都有一个“刷新”(Refresh) 按钮。 单击该按钮可为当前页面请求以太网交换机的最新信息。

用“设置值”(Set Values) 来存储条目

在进行组态设置的页面底部有一个“设置值”(Set Values) 按钮。 单击该按钮，可保存在工业以太网交换机中输入的组态数据。

说明

仅在以管理员身份登录后可以更改组态数据。

5.1.4 命令行接口 (CLI)

在 Windows 控制台中启动 CLI

请按以下步骤在 Windows 控制台中启动命令行接口：

1. 打开 Windows 控制台，输入后跟工业以太网交换机的 IP 地址的 telnet 命令：*C:\>ssh <IP 地址>*
2. 输入登录用户名和密码。

在基于 Web 的管理中启动 CLI

单击基于 Web 的管理中上方菜单栏中的 “控制台”(Console)。将自动打开 Telnet 连接，随后可通过用户名和密码登录。

命令快捷方式

另一种方法是，不用输入完整的 CLI 命令，而只输入首字母或开头几个字母，然后按 Tab 键。命令行接口随即会显示以输入的一个或多个字母开头的命令。如果显示的命令不符合要求，可再按 Tab 键，显示下一个命令。

目录结构

在命令行接口中输入命令之前，必须先打开所需的菜单或子菜单。本部分在单独的表格中列出了每个菜单的命令。该表格仅列出命令本身。

IE Switch X-400 端口的寻址方案

以下寻址方案适用于标记 IE Switch X-400 的端口：

- 首个数字表示插槽。
- 第二个数字由句点号分隔，用于指定端口。

例如，标识符 6.2 表示第二个端口在第六个插槽上。

IE Switch X-300 端口的寻址方案

以下寻址方案适用于标记 IE Switch X-300 的端口：

- 该数字与端口直接相关。

标签 2 表示 IE Switch X-300 的第二个端口。

表示 CLI 命令的符号

CLI 命令通常有一个或多个参数，这些参数的语法说明如下：

CLI 命令语法		参数的使用	说明	示例
< >	尖括号	必须	必要参数显示在尖括号中。 注：如果省略必要参数，大部分命令会输出当前值。	<ip 地址>
[ ]	方括号	可选	可选参数显示在方括号中。	[D|A]

CLI 命令语法		参数的使用	说明	示例	
|	管道字符	可替代	用管道字符显示可替代参数。 输入 a 或 b ，或数值范围 1 或数值范围 2	<a | b> <... | ....>	[a | b] [.... | ...]
...	句点	取值范围	参数的取值范围由三个句点表示。	<0...255> >	[0...255]
string		文本	文本等同于字符串。（参见示例）	• 文件名 • 地理坐标 • 名称和标识 • 密码	
端口		端口名称	端口名称	5.1（适用于 X-400） 或 7（适用于 X-300）	
Number		数字值	数字值	1	
MAC		MAC 地址	MAC 地址	80:fe:11:f3:4d:d6	
IP		IP 地址	IP 地址	192.168.1.1	
mode		功能模式	如果某项功能具有一个以上的运行模式，则由模式参数来表示。 可使用"?"参数显示全部可用模式	• D 禁用功能	

跨越菜单的命令

您可以在任意菜单或子菜单中使用下表中的命令。

表格 5-1　命令行接口 - CLI\ ... >

命令	说明	注释
/	切换到最高的菜单等级。	管理员和用户
..	切换到上一个菜单等级。	管理员和用户
?	显示菜单中的可用命令。	管理员和用户
exit	关闭 CLI 会话。	管理员和用户
restart	重新启动工业以太网交换机	仅限管理员
Info	显示有关当前菜单项的信息。	管理员和用户

命令行接口顶部菜单级别中的命令

可以在菜单 CLI> 中调用下表中的命令。

表格 5-2　命令行接口 - CLI>

命令	说明	注释
service debugloginenable <password>	使用用户名“debug”和相应的密码启用临时诊断访问。其在重启后会自动禁用。 诊断访问仅供西门子人员使用。错误使用访问权限可能会导致故障。	仅限管理员
service debuglogindisable	禁用“debug”用户。	仅限管理员

CLI 命令帮助

- 可以用“?”参数调出更多信息（如有必要，且对于命令可用时）。
- 如果没有更多信息，则会显示菜单概览中的命令语法。

5.2 系统菜单

5.2.1 系统组态

一般性设备信息

单击 *“系统”(System)* 文件夹图标时会显示该屏幕：

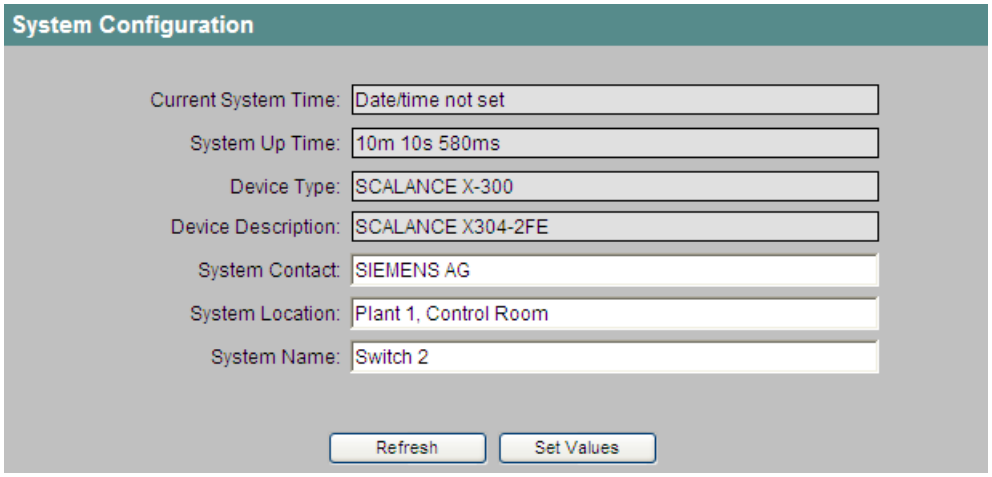


图 5-5 系统组态

当前系统时间（只读）
系统时间可由用户设置，也可通过时间帧（SINEC H1 时间帧或 SNTP）进行同步。可以了解何时以及如何设置系统时间：

- **(m)** 已手动进行设置。
- **(t)** 使用 SIMATIC 时间帧进行设置，但不与时间发送器同步。
- **(s)** 通过 SIMATIC 时间帧进行设置，且与时间发送器同步。
- **(p)** 通过 SNTP 协议进行设置。

系统运行时间 (System Up Time)（只读）
上一次重启到现在的时间。

设备类型 (Device Type)（只读）
设备的型号标识。

设备描述 (Device Description)（只读）
设备的描述。

系统联系人 (System Contact)
在该框中输入负责管理设备的联系人的姓名。

系统位置 (System Location)
在该框中输入设备的位置，例如房间号。

系统名称 (System Name)
在此框中输入设备的描述。

命令行接口语法

表格 5-3　系统组态 - CLI\SYSTEM>

命令	说明	注释
syscon [string]	设置/显示 syscontact MIB 变量。	仅限管理员。
sysloc [string]	设置/显示 syslocation MIB 变量。	仅限管理员。
sysname [string]	设置/显示 sysname MIB 变量。	仅限管理员。
debug.bin* [create | delete]	创建或删除包含诊断数据的文件。该文件可由登录的管理员通过网络浏览器从设备加载，地址为“http(s)://<IP 地址>/debug.bin”。 包含诊断数据的文件受密码保护，仅供西门子人员评估。为此，请联系您的西门子代理商。	仅限管理员。

5.2.2 系统标识和维护 (I&M)

系统标识和维护 (System Identification & Maintenance)

以下屏幕包含具体设备的供应商信息以及维护数据（如订货号、序列号和版本号等）。

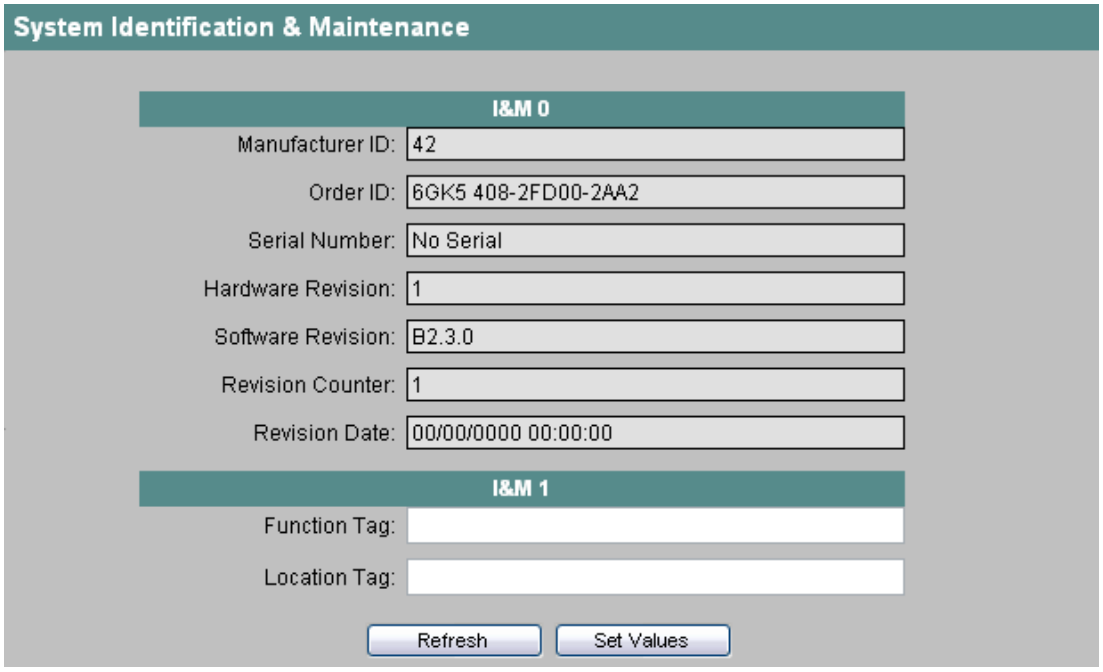


图 5-6 系统标识和维护

I&M 0

可以在此找到用于设备标识和维护的各种参数。

I&M 1

功能标签 (Function Tag)

可以在此输入功能标记（工厂标识）。

位置标签 (Location Tag)

可以在此输入位置标签（位置标识符）。

命令行接口语法

表格 5-4　系统标识和维护 - CLI\SYSTEM\IM>

命令	说明	注释
info	显示有关 “标识和维护”(Identification & Maintenance) 菜单项的信息。	-
revcnt [E|D]	启用/禁用修订版计数器。无需参数，此命令可显示修订版计数器为启用状态还是禁用状态。	仅限管理员。
function [string]	指定工厂标识（最多 32 个字符）。	仅限管理员。
location [string]	指定位置标识符（最多 32 个字符）。	仅限管理员。

5.2.3　系统重启和默认设置

复位为默认设置

该屏幕有一个用来重启工业以太网交换机的按钮，以及几个用于复位为工业以太网交换机默认设置的选项。

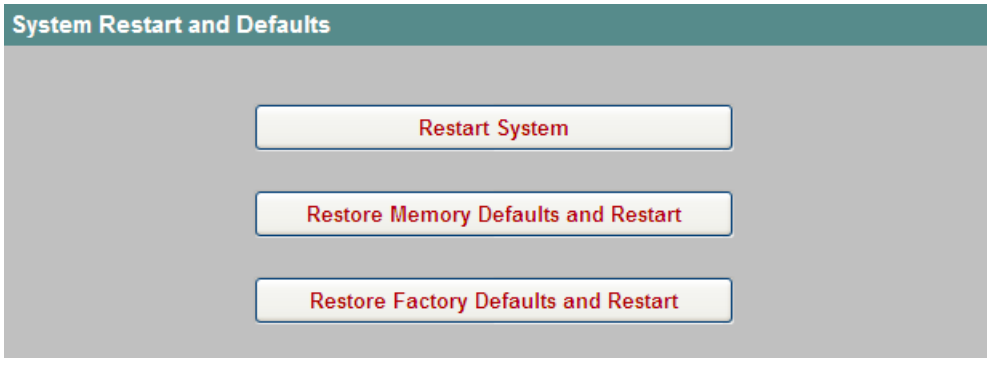


图 5-7　系统重启和默认设置

说明

有关重启工业以太网交换机，请注意以下几点：

- 仅在拥有管理员权限时才能重启工业以太网交换机。
- 工业以太网交换机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。
- 所做的任何更改仅会在单击 WBM 相应页面上的“设置值”(Set Value) 按钮后保存在设备中，在重启之前保存组态数据既不必要，也不可行。
- 不可将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)* 的 *“临时 Internet 文件”(Temporary Internet Files)* 部分，用“设置”(Settings) 按钮进行适当的设置。
- 在文本 *“检查所存网页的较新版本”(Check for newer versions of stored pages)* 下，必须选中 *“自动”(Automatically)* 复选框。

重启系统 (Restart System)

单击该按钮可重启工业以太网交换机。必须在对话框中确认重启操作。重启期间，将重新初始化工业以太网交换机，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。在工业以太网交换机重启期间，可以不关闭浏览器窗口。

恢复存储器默认值并重启 (Restore Memory Defaults and Restart)

单击该按钮将恢复出厂时的组态设置，但以下参数例外：

- IP 地址（带内和带外）
- 子网掩码（带内和带外）
- 默认网关的 IP 地址
- DHCP/BOOTP 标志
- 系统名称
- 系统位置
- 系统联系人
- 环网冗余
- 备用功能
- (R)STP
- PNIO 设备名称（站名称）

将触发自动重启。

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

单击该按钮会将组态恢复为出厂默认设置。同时会复位受保护的默认设置。将触发自动重启。

说明

复位全部默认设置后，IP 地址也会丢失。工业以太网交换机只能通过 SINEC PNI 或串行接口访问（仅限工业以太网交换机 X-400）。

命令行接口语法

表格 5-5　系统重启和默认设置 - CLI>

命令	说明	注释
restart	重新启动工业以太网交换机	仅限管理员。 可以在所有菜单中执行该命令。

表格 5-6　系统重启和默认设置 - CLI\SYSTEM>

命令	说明	注释
defaults	恢复出厂默认设置。同时会复位受保护的设置。设备将重启。	仅限管理员。 该命令与单击 WBM 中的 *“恢复出厂默认设置并重启”(Restore Factory Defaults and Restart)* 按钮作用相同。
memreset	恢复出厂默认设置。但会保留受保护的设置。将自动重启设备。	仅限管理员。 该命令与单击 WBM 中的 *“恢复存储器默认值并重启”(Restore Memory Defaults and Restart)* 按钮作用相同。

5.2.4 通过 HTTP 进行系统保存与加载

通过 HTTP 进行系统保存与加载 (System Save & Load via HTTP)

WBM 使您可以将组态信息存储在客户端 PC 上的外部文件中，或将此数据从此 PC 的外部文件装载到工业以太网交换机。您也可以通过位于客户机 PC 上的文件加载新固件。

说明

更新固件之后，请删除 Web 浏览器的缓存。

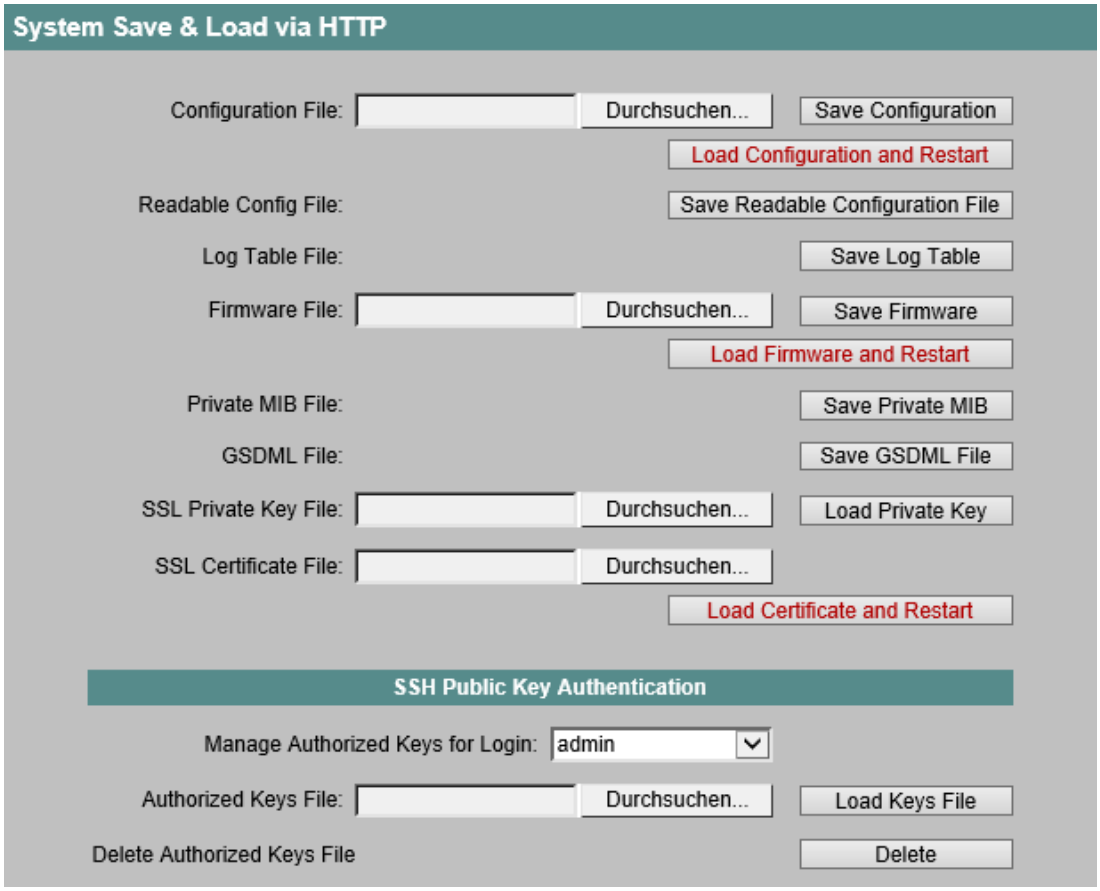


图 5-8 通过 HTTP 进行系统保存与加载

组态文件 (Configuration File)

要加载到工业以太网交换机的组态文件的名称以及目录路径。

可读的组态文件 (Readable Config File)

可以使用 CLI 命令将工业以太网交换机的组态文件保存为文本文件。

日志表文件 (Log Table File)
可以保存工业以太网交换机的事件日志表的条目。

固件文件 (Firmware File)
要用来加载新固件的文件的名称以及目录路径。

专有 MIB 文件 (Private MIB File)
可以保存专有 MIB 文件。

GSDML 文件 (GSDML File)
可以保存有关设备属性的 PROFINET 信息。

SSL 私钥文件 (SSL Private Key File)
要用来将 SSL 私钥加载到设备的文件的名称以及目录路径。

SSL 证书文件 (SSL Certificate File)
要用来将 SSL 证书加载到设备的文件的名称以及目录路径。

说明

由于私钥和证书构成一个整体，所以仅在密钥和证书均已下载完成之后才会保存文件。加载证书时，会对证书进行检查，以确保证书与加载的密钥匹配。采用新 SSL 文件之前要进行重启。

以下内容适用于 SCALANCE X414-3E 类型的设备：

仅接受最大长度为 2048 字节的 RSA 私钥。私钥不可以是受密码保护的密钥。SSL 证书必须经过 PEM 编码。

以下内容适用于 SCALANCE X-300 产品系列设备和 SCALANCE X408-2 类型的设备：

自固件版本 V4.1.4 起，已由之前的 RSA 证书转为使用可实现椭圆形曲线加密的证书（“ECDSA” 证书）。仅可使用通过以下曲线生成的 PEM 格式的 ECDSA 证书：

- secp256r1 (NIST P-256)
- secp384r1 (NIST P-384)
- secp521r1 (NIST P-521)

自该固件版本开始，不再支持 RSA 证书。设备中现有的 RSA 证书会自动替换为自签名 ECDSA 证书。

SSH 公钥身份验证的工作方式

使用 SSH，可以通过密码或公钥程序进行身份验证。公钥身份验证的优点是相关密钥会保存在文件中，用户无需手动输入。需要为每个客户端生成一个密钥对，以便通过公钥身份验证与交换机建立 SSH 连接。公钥存储在与客户端建立 SSH 连接的交换机上。私钥仅存储在相应客户端上。在建立 SSH 连接期间，客户端使用私钥生成签名并将其发送至交换机。交换机基于公钥检查签名，并可以通过这种方式对客户端进行身份验证。

通过 SCALANCE 设备进行 SSH 公钥身份验证

固件版本不高于 V4.1.3 的 SCALANCE 设备支持以下公钥类型和密钥长度：

方法	最大密钥长度
SSH-RSA	16 kb
SSH-DSS	8 kb（DSA 密钥）

固件版本自 V4.1.4 起的 SCALANCE 设备仅支持以下方法：

- ecdsa-sha2-nistp256
- ecdsa-sha2-nistp384
- ecdsa-sha2-nistp512
- ssh-ed25519

说明

从 V4.1.3 到 V4.1.4 的固件更新

在从固件版本 V4.1.3 更新到固件版本 V4.1.4 或更高版本期间，之前存储的公钥将被自动删除。用户需要使用其中一种新方法存储新密钥。

密钥必须以 OpenSSH 公钥格式提供。以下两个程序可用于生成密钥对：

- **ssh-keygen**
  各种操作系统的 SSH 实现组件。
- **PUTTYgen**
  用于 Windows 操作系统的客户端。

所有已授权的登录公钥必须保存在一个大小不超过 32 kB 的通用文本文件中。对于“admin”和“user”用户的密钥，存在单独的文件。命令行必须以“#”字符开头。您可以“管理员”用户身份将该文件加载到 SCALANCE 设备中。

包含公钥的文件示例：

```
. . .
# public key for host 1.2.3.4
ecdsa-sha2-nistp256 AAAAB3N[... long string of
characters ...]UH0= key-comment
# public key for host 1.2.3.5
ssh-ed25519 AAAAB3N[... long string of characters ...]UH0= key-
```

```
comment
. . .
```

说明

插入 C-PLUG 时，保存在 SCALANCE 设备上的公钥将被传输到其它设备。保存的公钥不是组态文件的一部分。

对于以下设备，仅当插入 C-PLUG 时才可以进行 SSH 公钥身份验证：

设备	订货号
SCALANCE X307-3	6GK5307-3BL00-2AA3
SCALANCE X307-3LD	6GK5307-3BM00-2AA3
SCALANCE X308-2	6GK5308-2FL00-2AA3
SCALANCE X308-2LD	6GK5308-2FM00-2AA3
SCALANCE X308-2LH	6GK5308-2FN00-2AA3
SCALANCE X308-2LH+	6GK5308-2FP00-2AA3
SCALANCE X310FE	6GK5310-0BA00-2AA3
SCALANCE X310	6GK5310-0FA00-2AA3

SSH 公钥身份验证的组态

用于登录的托管授权密钥

选择要应用 SSH 公钥身份验证的登录。可为每个登录加载一个包含公钥的单独文件。

授权密钥文件

加载包含用于 SSH 公钥身份验证的公钥的文件。

删除授权密钥文件

删除此前加载的公钥。这将同时禁用 SSH 公钥身份验证。

如何通过 HTTP/HTTPS 加载数据

1. 在对应的文本框中，输入要用来获取相关数据的文件的名称和目录路径。
2. 单击“加载固件并重启”(Load Firmware and Restart)、“加载组态并重启”(Load Configuration and Restart)、“加载私钥”(Load Private Key) 或“加载证书并重启”(Load Certificate and Restart) 按钮之一，开始加载相应的文件。
   除了执行“加载私钥”(Load Private Key) 之外，下载之后都会自动重启，并且设备会使用新数据再次启动。

如何通过 HTTP/HTTPS 保存数据

1. 单击“保存组态”(Save Configuratio)、“保存日志表”(Save Log Table)、“保存固件”(Save Firmware)、“保存私有 MIB”(Save Private MIB) 或“保存 GSDML 文件”(Save GSDML File) 按钮之一，启动保存操作。
2. 系统会提示用户选择存储位置及文件名称，或接受建议的文件名称。

复用组态数据

如果几台工业以太网交换机具有相同的组态，且是通过 DHCP 获取 IP 地址时，保存和读取组态数据就有助于提高效率。

说明

在多台工业以太网交换机上使用相同的组态

工业以太网交换机的组态无法加载到其它所有工业以太网交换机上。

有关兼容设备列表，请参见“在多台工业以太网交换机上使用相同的组态 (页 441)”部分。

组态完一台工业以太网交换机后，可将组态数据保存在计算机中。也可以将数据保存在 TFTP 服务器 (页 61)中。

将该文件下载到要组态的所有其它以太网交换机中。

如果有必要对特定设备进行单独设置，则必须在线进行设置。

存储后的组态数据已经过编码，因此，不能用文本编辑器编辑这些文件。

使用 FTP 下载组态文件

除了使用 HTTP/HTTPS 和 TFTP，也可以使用 FTP 将组态文件下载到设备。要使用 FTP 将组态文件下载到设备，请按照以下步骤操作：

1. 打开控制台窗口并输入命令“ftp”，然后输入工业以太网交换机的 IP 地址。
   例如：
   ```
   ftp 192.168.20.54
   ```
2. 登录帐户和密码可使用与 WBM 和 CLI 相同的值。
3. 输入“put”命令，然后输入固件文件的名称。
   例如：
   ```
   put X308-2M.cfg
   ```
4. 加载文件之后，工业以太网交换机将关闭 FTP 连接并进行重启。

5.2.5 通过 TFTP 进行系统保存和加载

用 TFTP 服务器进行数据交换

WBM 允许用户将组态信息存储在外部文件中，并将此信息从外部文件加载到工业以太网交换机中。也可以将日志信息保存在文件中，或通过文件加载新固件。可以在“保存与加载”(Save & Load) 菜单中输入所需条目。

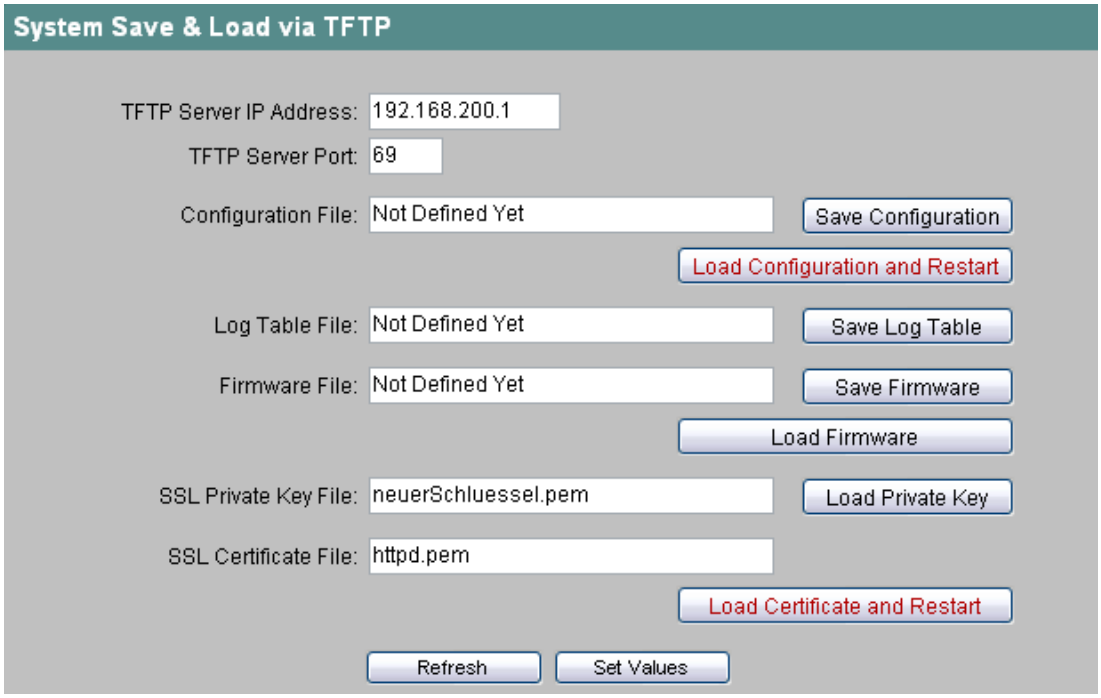


图 5-9 系统保存与加载

TFTP 服务器 IP 地址 (TFTP Server IP Address)
用于交换数据的 TFTP 服务器的 IP 地址。

TFTP 服务器端口 (TFTP Server Port)
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。

组态文件 (Configuration File)
要加载到工业以太网交换机或存储当前组态信息的组态文件（最大为 32 个字符）的名称和文件夹路径（如有必要）。

日志表文件 (Log Table Filee)
要保存日志表内容的文件（最大 32 个字符）的名称和路径（如有必要）。

固件文件 (Firmware File)
要用来加载新固件或保存当前固件信息的文件（最大为 32 个字符）的名称和文件夹路径（如有必要）。

SSL 私钥文件 (SSL Private Key File)
要用来将 SSL 私钥加载到设备的文件的名称以及目录路径。该框中的条目限制为最长 32 个字符。

SSL 证书文件 (SSL Certificate File)
要用来将 SSL 证书加载到设备的文件的名称以及目录路径。
该框中的条目限制为最长 32 个字符。

说明

由于私钥和证书构成一个整体，所以仅在密钥和证书均已下载完成之后才会保存文件。加载证书时，会对证书进行检查，以确保证书与加载的密钥匹配。采用新 SSL 文件之前要进行重启。

仅接受最大长度为 1280 字节的私有 RSA 密钥，私钥不可以是受密码保护的密钥。

SSL 证书必须经过 PEM 编码，其长度不能超过 2560 字节。

如何通过 TFTP 加载或保存数据

1. 在“TFTP 服务器 IP 地址”(TFTP Server IP Address) 文本框中输入 TFTP 服务器的 IP 地址。
2. 在文本框中输入要保存数据或从中获取数据的文件的名称（最多 32 个字符）。
3. 输入更多条目之前请单击“设置值”(Set Values) 按钮以保存或加载数据。
4. 单击相应的“保存”(Save) 或“加载”(Load) 按钮，启用保存/加载功能。

加载组态和 SSL 证书后，设备将采用新数据重启。

复用组态数据

如果几台工业以太网交换机具有相同的组态，且是通过 DHCP 获取 IP 地址时，保存和读取组态数据就有助于提高效率。

说明

在多台工业以太网交换机上使用相同的组态

工业以太网交换机的组态无法加载到其它所有工业以太网交换机上。

有关兼容设备列表，请参见“在多台工业以太网交换机上使用相同的组态 (页 441)”部分。

组态完一台工业以太网交换机后，可将组态数据保存到 TFTP 服务器中。也可以将数据保存在计算机 (页 56)中。

将该文件下载到要组态的所有其它以太网交换机中。

如果有必要对特定设备进行单独设置，则必须在线进行设置。

存储后的组态数据已经过编码，因此，不能用文本编辑器编辑这些文件。

命令行接口语法

表格 5-7　系统保存与加载 - CLI\SYSTEM\SAVELOAD>

命令	说明	注释
server [<ip>[:port]]	指定 IP 地址以及用来执行数据交换的 TFTP 服务器的端口（可选）。	仅限管理员。 默认值：0.0.0.0
cfgname <string>	指定要用来加载或保存组态数据的文件的名称（最多 32 个字符）。	仅限管理员。
cfgsave	将组态数据保存在 TFTP 服务器的文件中。	仅限管理员。
cfgload	通过 TFTP 服务器的文件加载组态数据。	仅限管理员。
logname <string>	指定存储日志表的文件的名称（最多 32 个字符）。	仅限管理员。
logsave	将日志表保存在 TFTP 服务器的文件中。	仅限管理员。
fwname <string>	指定要用来加载固件的文件的名称（最多 32 个字符）。	仅限管理员。 默认值：未定义。
fwload	从文件加载固件。	仅限管理员。
fwsave	将固件保存在 TFTP 服务器的文件中。	仅限管理员。
keyload	从文件加载 SSL 私钥。	仅限管理员。
certload	从文件加载 SSL 证书。	仅限管理员。

表格 5-8　系统保存与加载 - CLI\SYSTEM>

命令	说明	注释
authkeys [admin | user]	显示已加载公钥的 SSH 识别码。 作为参数，需要指定显示 SSH 识别码的登录名。	仅限管理员。

5.2.6 系统版本号

硬件和软件的版本

此页面显示工业以太网交换机所使用的硬件版本和软件版本：

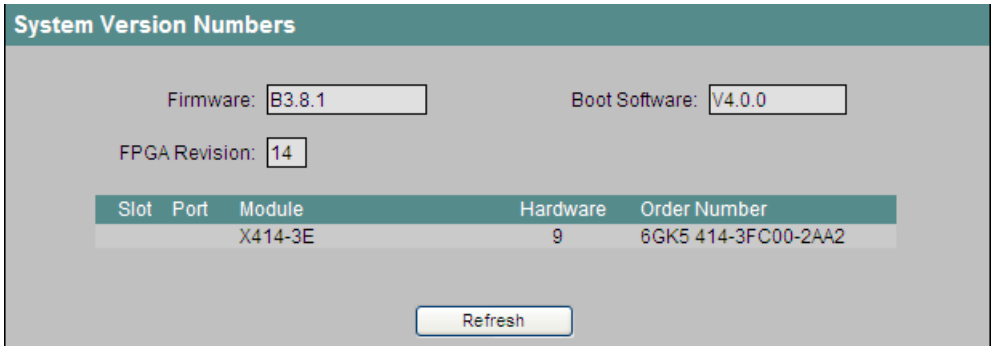


图 5-10 系统版本号

固件 (Firmware)
工业以太网交换机运行的固件版本。

引导软件 (Boot Software)
此处显示引导软件的版本。 引导软件永久存储在工业以太网交换机中。

FPGA 修订版 (FPGA Revision)
工业以太网交换机上使用的 FPGA 修订版。

基本设备和模块条目表
表格的第一行表示工业以太网交换机的版本。 “插槽”(Slot) 列显示基本设备上的插槽。 如果该信息与基本设备本身相关，则该列中将显示“-”。 “硬件”(Hardware) 列显示相应的版本，“订货号”(Order Number) 列则显示工业以太网交换机或模块的订货号。

命令行接口语法

表格 5-9 系统版本号 - CLI>

命令	说明	注释
info	此命令可显示工业以太网交换机所使用的软件版本，以及其它信息。	-

表格 5-10　系统版本号 - CLI\SYSTEM>

命令	说明	注释
version	显示工业以太网交换机的固件、硬件和引导软件版本，并提供有关基本设备和各模块的更多详细信息。	-

5.2.7 系统密码和登录模式

密码和登录模式

说明

供货时的默认密码

管理员密码：admin
用户密码：user

在此对话框中，如果您是管理员，则可更改“管理员”和“用户”的密码。密码长度最多为 16 个字符（7 位 ASCII 码）。

还可以通过选择登录模式来指定可用于登录的用户名。

说明

RADIUS

要使用登录模式“RADIUS”或“RADIUS 和本地”(RADIUS and Local)，必须存储和组态用于用户验证的 RADIUS 服务器。在“交换机”(Switch) 菜单的“802.1x RADIUS 组态”(802.1x RADIUS Configuration) 页面上组态此信息。

说明

SSH 公钥身份验证

对于 SSH 公钥身份验证，必须启用“本地”(Local) 或“RADIUS 和本地”(RADIUS and Local) 登录模式。本地用户的 SSH 公钥身份验证适用于“RADIUS 和本地”(RADIUS and Local)。SSH 公钥身份验证无法用于“RADIUS”登录模式。

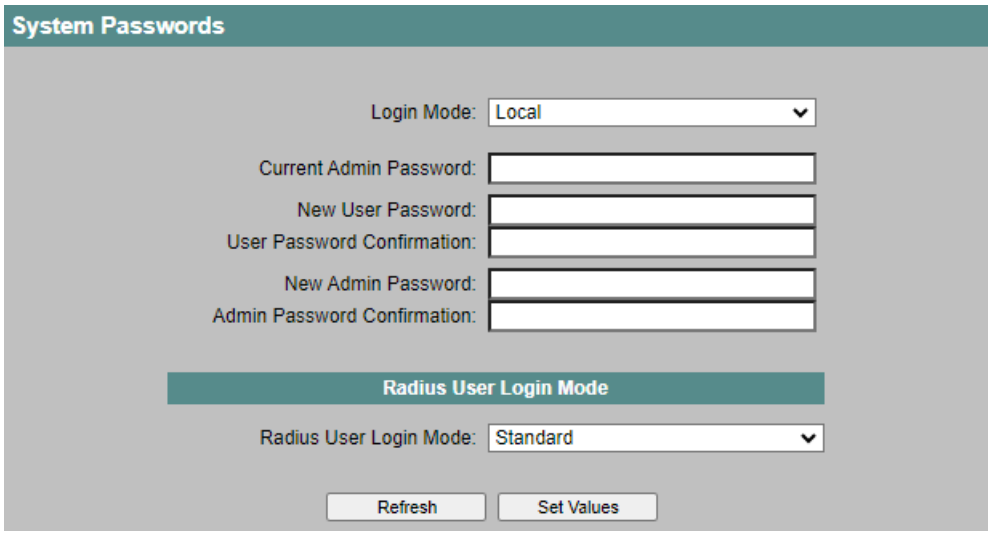


图 5-11　系统密码

“登录模式”(Login Mode) 下拉列表

登录模式列表框提供了下列选项：

本地 (Local)：	只有使用存在于固件中的用户名（user 和 admin）才可以登录。
RADIUS 和本地 (RADIUS and Local)：	使用存在于固件中的用户名（user 和 admin）以及通过 RADIUS 服务器都可以实现登录。RADIUS 服务器上的用户名具有优先级。
RADIUS：	只有使用存储在 RADIUS 服务器上的登录数据才可以登录。本地用户名被禁用。

“Radius 用户登录模式”(Radius User Login Mode) 下拉列表

登录模式列表框提供了下列选项：

标准：	RADIUS 身份验证不考虑供应商特定的属性。
供应商特定：	供应商特定属性（Vendor Specific Attributes，VSA）在 RADIUS 身份验证中评估。

保存

通过单击“设置值”(Set Values) 按钮保存条目。

说明

RADIUS 验证失败

如果组态为主服务器的 RADIUS 服务器出现故障，则初始验证将失败。只有在下次尝试登录时才会将请求发送至备份服务器。

命令行接口语法

表格 5-11　系统密码 - CLI\SYSTEM>

命令	说明	注释
passwd [admin | user]	为“管理员”或“用户”设置新密码。	仅限管理员。
loginmod [L | B | R]	指定登录模式： • **L** 仅限存在于固件中的用户名。 • **B** 固件中的用户名以及存储在 RADIUS 服务器上的用户名（后者具有优先权）。 • **R** 仅限存储在 RADIUS 服务器上的用户名。 如果不指定参数，则显示登录模式。	仅限管理员。
radiusmod [S | VS]	指定 RADIUS 身份验证的模式： • **S** 标准 RADIUS 身份验证不考虑供应商特定的属性。 • **VS** 供应商特定 供应商特定属性在 RADIUS 身份验证中评估。 如果不指定参数，则显示 RADIUS 身份验证模式。	仅限管理员。

5.2.8 系统 RADIUS 用户组

显示和管理用户组

此页面显示现有的 RADIUS 用户组及为其分配的角色。可以创建新的角色分配并删除现有的角色分配。

组在 RADIUS 服务器上定义。角色在设备本地定义。当 RADIUS 服务器为用户授权，并将用户分配到“Administrators”组时，此用户便拥有“admin”角色。

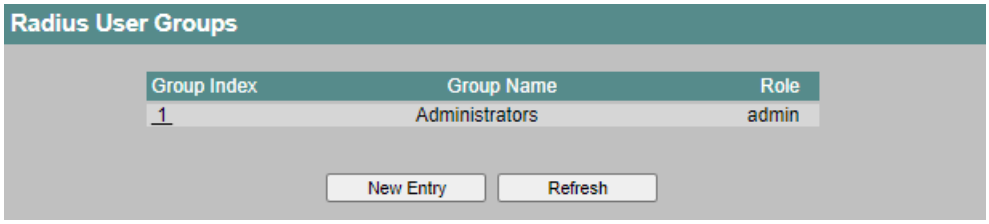


图 5-12 RADIUS 用户组

该表包含以下列：

- **组索引**
  UMC Radius 用户组索引。要打开表行的“Radius 用户组组态”(Radius User Group Configuration)，请单击索引。
  取值范围：1 ... 32
- **Group Name**
  用户组的名称。此名称必须与 RADIUS 服务器上的组相匹配。
  该名称必须满足以下条件：
  – 名称必须唯一。
  – 名称长度必须在 1 到 64 个字符之间。
  – 不允许使用以下字符：§ ? " ; :
- **Role**
  分配给用户组成员的角色。

如何创建新的角色分配

1. 单击“新条目”(New Entry) 按钮。会显示“Radius 用户组组态”(Radius User Group Configuration) 页面：

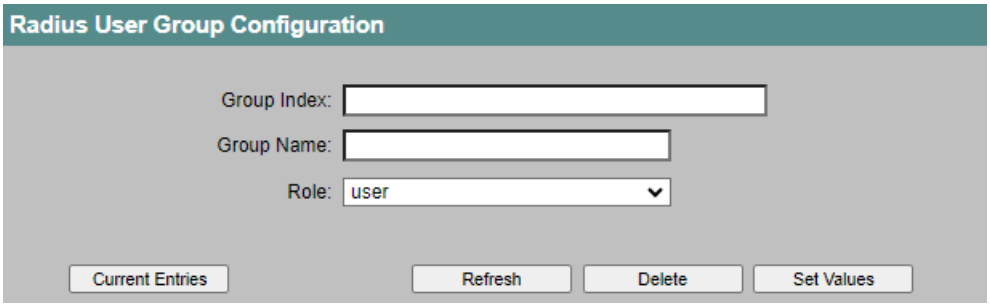


图 5-13 RADIUS 用户组组态

2. 在“组索引”(Group Index) 输入框中输入用户组的索引。1 ... 32 值范围内的索引必须唯一。
3. 在“组名称”(Group Name) 输入框中输入用户组的名称。
4. 在“角色”(Role) 下拉列表中，选择分配给用户组成员的角色。
5. 单击“Set Values”按钮。角色分配已创建。输入框的内容已删除。如有必要，创建额外的角色分配。
6. 要返回到用户组表，单击“当前条目”(Current Entries)。

如何更改角色分配

1. 在“组索引”(Group Index) 列中，单击要更改的角色分配的索引。会显示“Radius 用户组组态”(Radius User Group Configuration) 页面。
2. 更改“组名称”(Group Name) 和“角色”(Role) 参数。
3. 单击“Set Values”按钮。角色分配已更新。
4. 要返回到用户组表，单击“当前条目”(Current Entries)。

如何删除角色分配

1. 在里面“组索引”(Group Index) 列中，单击要删除的角色分配的索引。会显示“Radius 用户组组态”(Radius User Group Configuration) 页面。
2. 单击“Delete”按钮。将显示一个包含以下消息的对话框：
“Radius 用户组将被删除。您想继续吗？”(The Radius User Group will be deleted. Do you want to continue?)
3. 单击“OK”按钮。角色分配和输入框的内容已删除。
4. 要返回到用户组表，单击“当前条目”(Current Entries)。

命令行接口语法

表格 5-12　Radius 用户组组态 - CLI\SYSTEM\USERGROUP>

命令	说明	注释
添加 <索引> <名称> <角色>	创建新的角色分配。角色具有以下选项： • **admin** • **user**	仅限管理员。
name <索引> [名称]	指定具有指定索引的用户组的名称。 如果没有指定名称，则显示相应索引的名称。	仅限管理员。
role <索引> [角色]	为具有指定索引的用户组指定角色。 如果没有指定角色，则显示相应索引的角色。	仅限管理员。
delete <索引>	删除具有指定索引的用户组。	仅限管理员。

5.2.9　系统 SELECT/SET 按钮

禁用 SELECT/SET 按钮

在工业以太网交换机上，SELECT/SET 按钮的可用于

- 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
- 启用/禁用冗余管理器。

有关各项按钮功能的详细说明，请参见 SCALANCE X-400 操作说明。

在此页面中，可限制或完全禁用 SELECT/SET 按钮的功能。 这适用于以下三种功能：

- 恢复出厂默认设置
- 启用/禁用冗余管理器
- 设置故障屏蔽

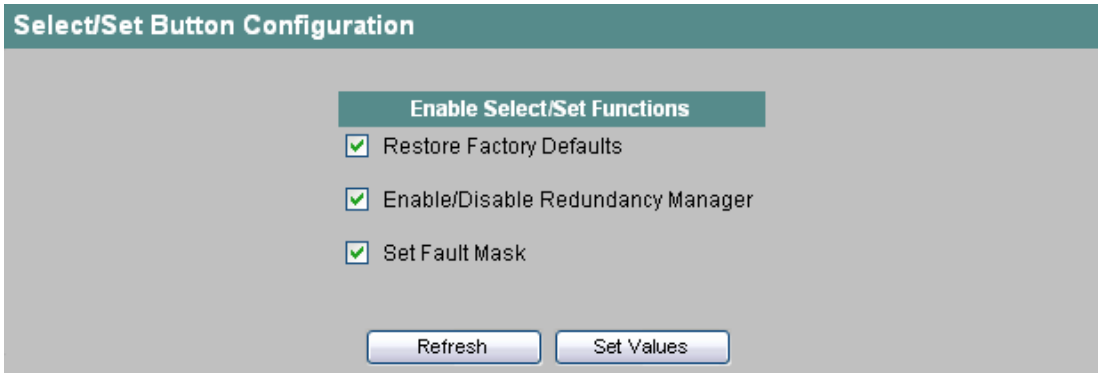


图 5-14　SELECT/SET 按钮组态

启用 SELECT/SET 功能

可通过选中或取消选中相应的复选框来启用或禁用该按钮的各项功能。

系统命令行接口

表格 5-13　系统组态 - CLI\SYSTEM\SELSET>

命令	说明	注释
info	显示按钮的功能。	-
defaults	启用/禁用该按钮的“恢复出厂默认设置”功能。	仅限管理员。
rm [E|D]	启用/禁用该按钮的“启用/禁用冗余管理器”功能。	仅限管理员。
faultmsk	启用/禁用该按钮的“设置故障屏蔽”功能。	仅限管理员。

5.2.10 系统事件日志表

记录事件

工业以太网交换机允许记录事件并将其显示在“日志表”(Log Table) 菜单的页面上。这样（举例来说）便可记录 SNMP 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。您可以指定要在“代理事件组态”(Agent Event Configuration) 菜单项中记录哪些事件。即使在工业以太网交换机关闭后，日志表的内容仍可保留。

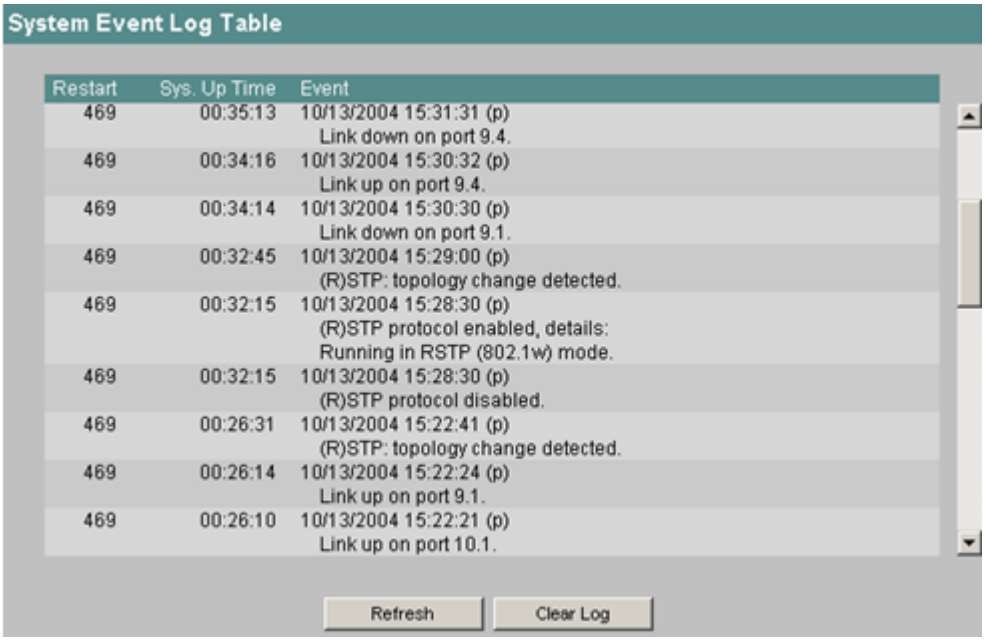


图 5-15 系统事件日志表

“重启”(Restart) 列指示相应事件发生时的设备重启次数。

“系统运行时间”(Sys.Up Time) 列显示从工业以太网交换机上次重启到目前所经过的时间，格式为 HH:MM:SS。

说明

使用 NTP 或 Siclock 同步时间时，在日志表中会输入条目的实际时间，而不是自上次重启后所经过的时间。

刷新 (Refresh)

单击此按钮可刷新显示画面。

清除记录 (Clear Log)

使用此按钮可删除日志表的内容。

命令行接口语法

表格 5-14　系统事件日志表 - CLI\SYSTEM>

命令	说明	注释
events [clear]	显示日志表的内容。可使用 [clear] 参数删除日志表的内容。	只有管理员能删除日志表。即使在工业以太网交换机关闭后，日志表的内容仍可保留。
addlog <字符串>	在日志表中插入文本。包括字符串中的空格。	仅限管理员。

5.2.11　C-PLUG 信息

C-PLUG 内容的相关信息

此菜单可提供有关 C-PLUG 的详细信息。 可以格式化 C-PLUG 或向其中加入新内容。

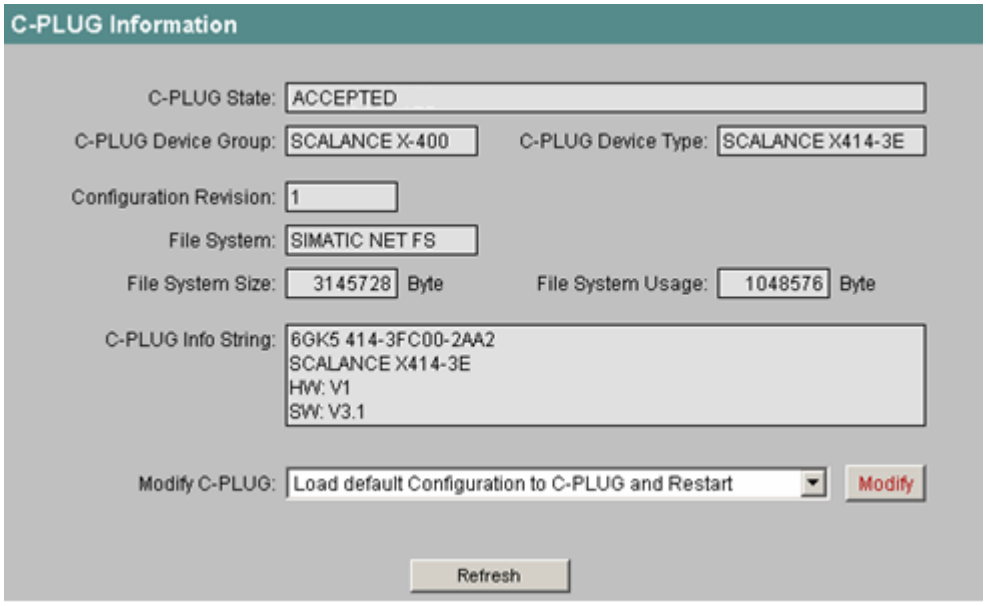


图 5-16　C-PLUG 信息

此菜单的各文本框均为只读模式。

C-PLUG 状态 (C-PLUG State)
此处显示 C-PLUG 的状态。 可能的状态包括：

- 已接受 (ACCEPTED)
  工业以太网交换机中插入的 C-PLUG 内容有效且匹配。
- 不接受 (NOT ACCEPTED)
  插入的 C-PLUG 内容无效或不兼容。 如果在操作过程中对 C-PLUG 进行了格式化，则也会显示此状态。
- 不接受，头文件 CRC 错误 (NOT ACCEPTED, HEADER CRC ERROR)
  插入的 C-PLUG 内容有错。
- 不存在 (NOT PRESENT)
  工业以太网交换机中未插入 C-PLUG。

C-PLUG 设备组 (C-PLUG Device Group)
表示先前曾使用 C-PLUG 的 SIMATIC NET 产品线。

C-PLUG 设备类型 (C-PLUG Device Type)
表示先前曾使用 C-PLUG 的产品线中的设备类型。

组态版本 (Configuration Revision)
组态结构的版本。 此信息与工业以太网交换机支持的组态选项相关，而与具体的硬件配置无关。 因此，在添加或移除模块或扩展器时，此版本信息不会改变；但是如果更新固件，则该信息可能会发生改变。

文件系统 (File System)
显示 C-PLUG 上的文件系统类型。

文件系统大小 (File System Size)
显示 C-PLUG 的文件系统的最大存储空间。

文件系统利用率 (File System Usage)
显示 C-PLUG 文件系统中当前已被使用的存储空间。

C-PLUG 信息字符串 (C-PLUG Info String)
在此处，您可查看有关在之前操作中使用过 C-PLUG 的设备的所有附加信息，例如订货号、型号标识和软硬件版本。

修改 C-PLUG (Modify C-PLUG)，修改 (Modify)
只有在以“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 C-PLUG 内容的方式。 可能的选项如下：

- “将内部组态复制到 C-PLUG 并重启”(Copy internal Configuration to C-PLUG and Restart)
  会将工业以太网交换机内部闪存中的组态复制到 C-PLUG；随后进行重启。
  需要使用此功能的重要情况有： 工业以太网交换机完成启动所用的 C-PLUG 包含错误组态或不同于工业以太网交换机的组态。 如果在启动设备后尚未对组态进行任何更改，则可使用此功能将 C-PLUG 覆盖为初始设备组态。
- 将默认组态复制到 C-PLUG 并重启 (Copy default Configuration to C-PLUG and Restart)
  将各项均为出厂默认值的组态存储到 C-PLUG 中。 随后将重启，并且工业以太网交换机将使用这些默认值启动。
- 清除 C-PLUG（低级格式化，组态将丢失）(Clean C-PLUG (Low Level Format, Configuration lost))
  删除 C-PLUG 中的所有数据并启动低级格式化功能。 随后不会自动重启，而且工业以太网交换机将显示错误。 可通过重启或卸下 C-PLUG 来清除此错误状态。

在下拉列表中选择所需的条目并单击“修改”(Modify)，以根据需要更改 C-PLUG。

命令行接口语法

表格 5-15　C-PLUG 信息 - CLI\SYSTEM\C-PLUG>

命令	说明	注释
info	显示 C-PLUG 的当前状态。	将显示与 WBM 的“X-400 C-PLUG 信息页面”相同的信息。
copyint	用主内存中的内容覆盖 C-PLUG。	仅限管理员。 与 WBM 中“将内部组态复制到 C-PLUG 并重启”(Copy internal Configuration to C-PLUG and Restart) 命令的功能相同。

命令	说明	注释
copydef	使用默认参数初始化 C-PLUG。	仅限管理员。 与 WBM 中“将默认组态复制到 C-PLUG 并重启”(Copy default Configuration to C-PLUG and Restart) 命令的功能相同。
clean	删除 C-PLUG 中的所有数据并运行低级格式化功能。	仅限管理员。 与 WBM 中“清除 C-PLUG”(Clean C-PLUG) 命令的功能相同。

5.2.12 地理坐标

地理坐标的相关信息

在“地理坐标”(Geographic Coordinates) 窗口中，可以输入或读取地理坐标的相关信息。 为了能够读取地理坐标，必须曾经将设备的地理位置正确地输入到地理坐标中。 可以在“地理坐标”(Geographic Coordinates) 窗口中直接输入地理坐标的参数（基于 WGS84 的椭球面纬度、经度和高度）。

举例来说，地理坐标可通过 GPS 接收器来计算。 通常情况下，这些设备都能直接显示地理坐标。 经过组态后，SCALANCE 设备可通过 SNMP 私有 MIB、Telnet 或 WEB 为您提供此地理数据以用于管理。

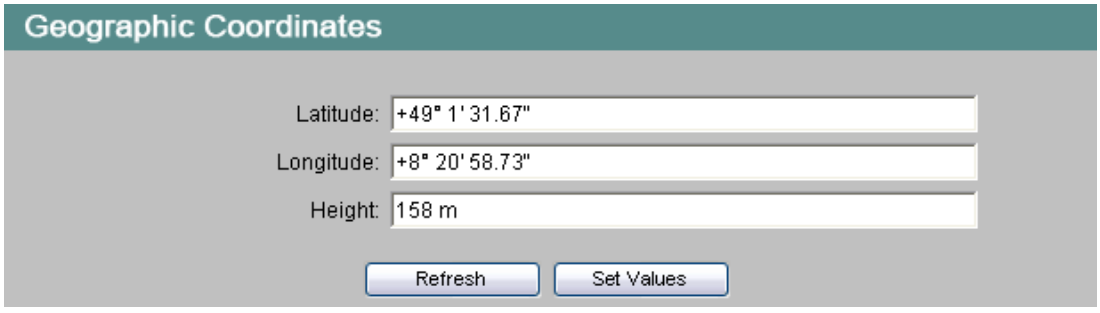


图 5-17 地理坐标

纬度 (Latitude)
在此处应输入设备所在位置的北纬或南纬值。

例如，+49° 1´ 31.67" 表示该设备位于北纬 49 度 1 分 31.67 秒。
南纬则通过在前面添加负号来表示。

您也可以在数字后面附加字母 N（北）或 S（南）(49° 1´ 31.67" N)。

经度 (Longitude)
在此处应输入设备所在位置的东经或西经值。
例如，+8° 20´ 58.73" 表示该设备位于东经 8 度 20 分 58.73 秒。
西经则通过在前面添加负号来表示。

您也可以在数字后面附加字母 O 或 E（东）或 W（西）(8° 20´ 58.73" E)。

高度（地理高度）(Height (geographic height))
在此处输入以米为单位的海拔地理高度。
例如，158 m 表示设备位于海平面以上 158 m 高的位置。
对于低于海平面的高度，可在前面添加负号来表示。

输入地理坐标

可在文本框中输入地理坐标值，例如：

- 格式中包含分秒的度数：
  DD°MM.MMM´，DD°MM´SS，DD°MM´SS.SSS
- 十进制格式的度数： DD.DDD°
- 带或不带符号，或附加字母 S、N、E（或 O）和 W

地理坐标的命令行接口语法

表格 5-16　地理坐标 - CLI\SYSTEM\GEO>

命令	说明	注释
info	显示地理坐标的当前状态。	-
lat [字符串]	显示/设置地理纬度坐标。	仅限管理员。
long [字符串]	显示/设置地理经度坐标。	仅限管理员。
height [字符串]	显示/设置地理高度坐标。	仅限管理员。

5.3 X-300/X-400 菜单

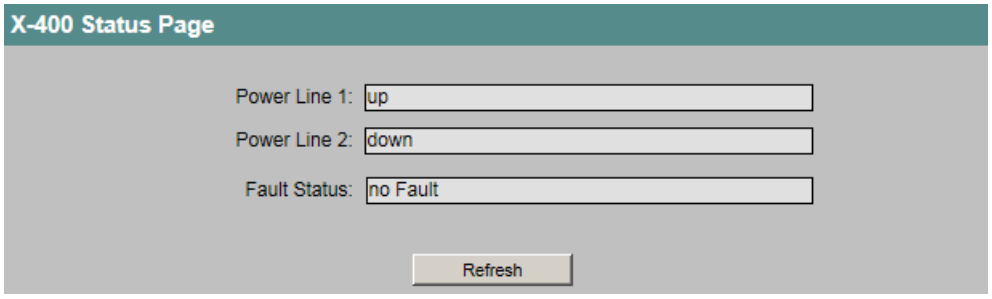
5.3.1 X-300/X-400 状态页面

工作状态的相关信息

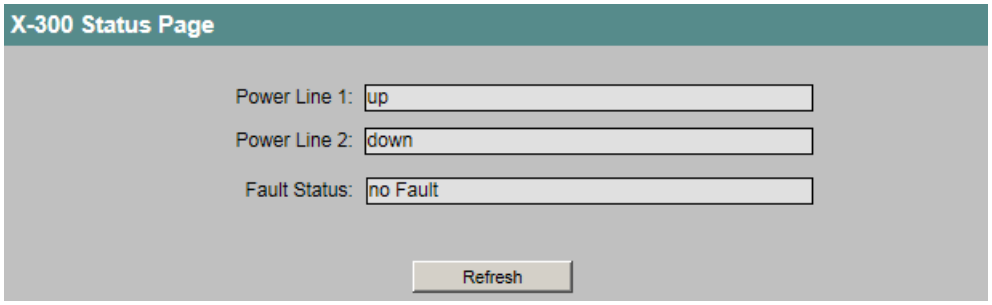
单击“X-400”或“X-300”文件夹图标时将显示此画面。

此画面中的信息取决于工业以太网交换机。对于 X-400 工业以太网交换机，此画面显示关于电源和错误/故障状态的信息。对于 X-300 工业以太网交换机，此画面显示有关环网冗余和备用功能的附加信息。
此画面的文本框为只读。

X-400 状态页面



X-300 状态页面



冗余功能 (Redundancy Function)

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

- 无环网冗余（关）(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 客户端 (HRP-Clt) (HRP Client (HRP-Clt))
  工业以太网交换机充当 HRP 客户端。

- HRP 管理器 (HRP-Mgr) (HRP Manager (HRP-Mgr))
  工业以太网交换机充当 HRP 管理器。
- MRP 客户端 (MRP-Clt) (MRP Client (MRP-Clt))
  工业以太网交换机充当 MRP 客户端。
- MRP 管理器 (MRP-Mgr) (MRP Manager (MRP-Mgr))
  工业以太网交换机充当 MRP 管理器。

RM 状态 (RM Status)

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

- 被动 (Passive)
  工业以太网交换机充当冗余管理器，并已打开环网；即：与环网端口相连的交换机线路处于无故障运行中。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。
- 主动 (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，则不会显示任何环网端口，并将显示文本"环网冗余已禁用"(Ring Redundancy disabled)。

环网端口 (Ring Ports)

显示用作环网端口的端口。

备用功能 (Standby Function)

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，前一个行使从站功能的设备将获得备用主设备的角色。

显示备用功能的状态：

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

- 禁用 (Disabled)
  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。
- 等待连接... (Waiting for Connection...)
  尚未与伙伴设备建立连接。备用端口处于未激活状态。在这种情况下，或是伙伴设备中的组态不一致（例如，连接名错误、备用链路被禁用），或是存在实际故障（例如，设备故障、链路中断）。
- 连接丢失 (Connection Lost)
  与伙伴设备的现有连接已丢失。在这种情况下，或是存在实际故障（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）。

备用状态 (Standby Status)

显示备用端口的状态：

- 主动 (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。
- 被动 (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。

备用端口 (Standby Ports)

显示备用端口。

电源线路 1 (Power Line 1)

- 接通 (Up)：
  电源 1（线路 1）已接通。
- 断开 (Down)：
  电源 1 未接通或电压低于允许值。

电源线路 2 (Power Line 2)

- 接通 (Up)：
  电源 2（线路 2）已接通。
- 断开 (Down)：
  电源 2 未接通或电压低于允许值。

故障状态 (Fault Status)

此处显示工业以太网交换机的故障状态。下表中包含可能出现的错误消息**示例**。如果出现多

个故障，则将在文本框中从下到上逐个列出。在“SCALANCE X300/X400 的错误消息 (页 433)”部分提供了完整的错误消息列表。

错误消息	含义
冗余电源线故障 (Redundant power line down)	冗余电源出现故障。
所监视端口的链路中断 (Link down on monitored port)	与所监视端口的连接已中断。
环网中有多个 RM (More than one RM in ring)	环网中有多个设备获得了冗余管理器的功能。
不可恢复的环网错误 (Non-recoverable ring error)	冗余管理器无法消除这些错误。例如，在未出现链路中断故障的情况下，某一端上丢失了冗余管理器发出的冗余帧。环网中的第二个冗余管理器若组态不正确，也会导致该错误消息出现。 在第一种情况下，请检查环网端口的组态： • 运行模式（全双工/半双工）设置是否合理？ • 使用光纤电缆时：发送和接收电缆是否已正确插入？ 在第二种情况下： 重新组态环网中的另一个冗余管理器，以便其采用适当的客户端角色或从环网中删除该设备。
无故障 (No Fault)	交换机未检测出故障（信号触点未响应，故障 LED 未亮起）

命令行接口语法

表格 5-17　X-400 状态 - CLI\X-400> 或
X-300 状态 - CLI\X-300>

命令	说明	注释
info	显示工业以太网交换机的状态信息。	-

5.3.2 环网冗余

5.3.2.1 X-300/X-400 环网冗余信息

有关环网冗余的信息

单击“环网冗余”(Ring Redundancy) 文件夹图标时将显示该画面。

该画面显示与环网冗余、备用功能和 RM 观察器有关的设备的状态。此页面中的文本框均为只读模式。

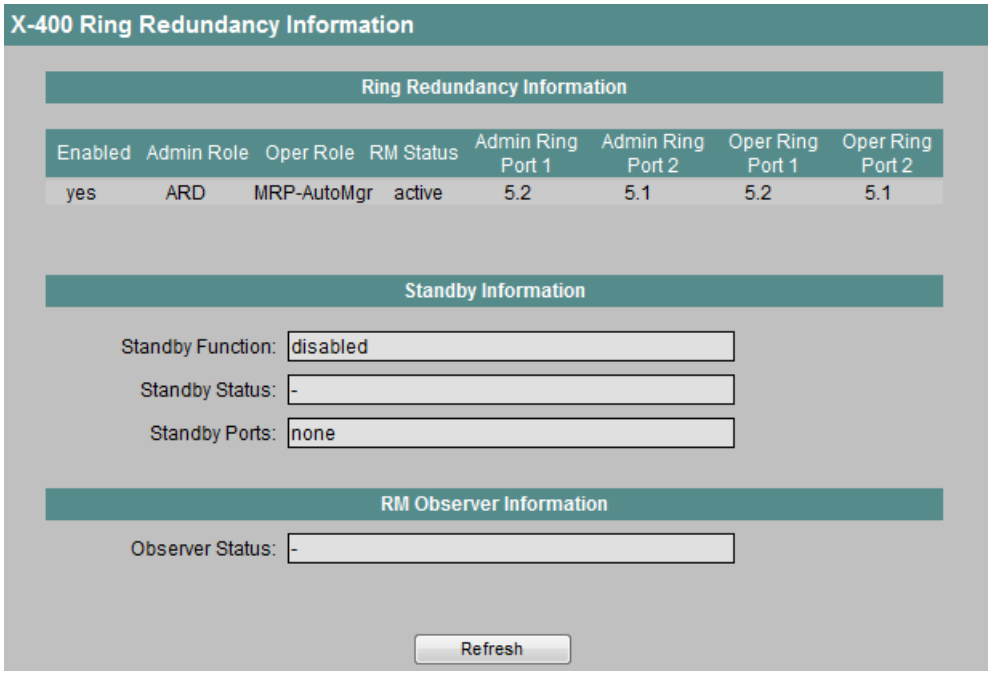


图 5-18 SCALANCE X-300/X-400 环网冗余信息

该画面包含以下部分和输入框：

“环网冗余信息”(Ring Redundancy Information) 部分

该表格包括以下列：

- **启用 (Enabled)**
  “启用”(Enabled) 列显示组态的环网是已激活还是已禁用。
- **管理员角色 (Admin Role)**
  “管理员角色”(Admin Role) 列显示已经为设备组态的模式：
  - 无环网冗余（关）(No Ring Redundancy (off))
    工业以太网交换机未使用冗余功能。
  - HRP 客户端 (HRP-Clt) (HRP Client (HRP-Clt))
    工业以太网交换机充当 HRP 客户端。
  - HRP 管理器 (HRP-Mgr) (HRP Manager (HRP-Mgr))
    工业以太网交换机充当 HRP 管理器。
  - MRP 客户端 (MRP-Clt) (MRP Client (MRP-Clt))
    工业以太网交换机充当 MRP 客户端。
  - MRP 管理器 (MRP-Mgr) (MRP Manager (MRP-Mgr))
    工业以太网交换机充当 MRP 管理器。
- **操作员角色 (Oper Role)**
  “操作员角色”(Oper Role) 列显示设备在环网中所采用的模式：
  - 无环网冗余（关）(No Ring Redundancy (off))
    工业以太网交换机未使用冗余功能。
  - HRP 客户端 (HRP-Clt) (HRP Client (HRP-Clt))
    工业以太网交换机充当 HRP 客户端。
  - HRP 管理器 (HRP-Mgr) (HRP Manager (HRP-Mgr))
    工业以太网交换机充当 HRP 管理器。
  - MRP 客户端 (MRP-Clt) (MRP Client (MRP-Clt))
    工业以太网交换机充当 MRP 客户端。
  - MRP 管理器 (MRP-Mgr) (MRP Manager (MRP-Mgr))
    工业以太网交换机充当 MRP 管理器。

- **RM 状态 (RM Status)**
  "RM 状态"(RM Status) 列显示工业以太网交换机是否充当冗余管理器，以及此角色是断开环网还是闭合环网。
  - 被动 (Passive)：
    工业以太网交换机充当冗余管理器，并已打开环网；即：与环网端口相连的交换机线路处于无故障运行中。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。
  - 主动 (Active)：
    工业以太网交换机充当冗余管理器，并已关闭环网；即：与环网端口相连的交换机线路已中断（故障）。冗余管理器将接通其环网端口并恢复未中断的线性拓扑。
  - 如果完全禁用环型拓扑中的介质冗余，则不会显示任何环网端口，并将显示文本"环网冗余已禁用"(Ring Redundancy disabled)。
- **管理员环网端口 1 (Admin Ring Port 1) 和管理员环网端口 2 (Admin Ring Port 2)**
  "管理员环网端口 1"(Admin Ring Port 1) 和 "管理员环网端口 2"(Admin Ring Port 2) 两列显示已组态为环网端口的端口。
- **操作员环网端口 1 (Oper Ring Port 1) 和操作员环网端口 2 (Oper Ring Port 2)**
  "操作员环网端口 1"(Oper Ring Port 1) 和 "操作员环网端口 2"(Oper Ring Port 2) 两列显示正用作环网端口的端口。

“备用信息”(Standby Informatio) 部分

- **备用功能 (Standby Function)**

  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。

  “备用功能”(Standby Function) 显示框中显示备用功能的状态：

  – 主设备 (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。
  – 从设备 (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。
  – 已禁用 (Disabled)：
    备用连接已禁用。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。
  – 等待连接... (Waiting for Connection...)：
    尚未与伙伴设备建立连接。备用端口处于未激活状态。在这种情况下，或是伙伴设备中的组态不一致（例如，连接名错误、备用链路被禁用），或是存在实际故障（例如，设备故障、链路中断）。
  – 连接丢失 (Connection Lost)：
    与伙伴设备的现有连接已丢失。在这种情况下，或是存在实际故障（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）。

- **备用状态 (Standby Status)**

  “备用状态”(Standby Status) 显示框中显示备用端口的状态：

  – 主动 (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。
  – 被动 (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。

- **备用端口 (Standby Ports)**

  “备用端口”(Standby Port) 显示框中显示备用端口。

“RM 观察器信息”(RM Observer Information) 部分

- **观察器状态 (Observer Status)**
  “观察器状态”(Observer Status) 显示框显示观察器的当前状态：
  – 被动 (passive)
    观察器没有检测到任何错误。
  – 主动 (active)
    观察器已检测到错误。
  – -
    禁用观察器功能。

命令行接口语法

表格 5-18 X-300 环网冗余 - CLI\X-300\RING>
X-400 环网冗余 - CLI\X-400\RING>

命令	说明	注释
info	显示工业以太网交换机当前的环网组态。	-

5.3.2.2 X-300/X-400 环网组态

介质冗余协议 (MRP)

自固件版本 V 3.0.0 起支持介质冗余协议 (MRP)。自动冗余检测 (ARD) 是工业以太网交换机出厂时的默认设置。如要使用之前的高速冗余协议 (HRP)，则必须组态 HRP。

- MRP 中故障切换后的帧通信重新组态时间：200 ms
- HRP 中故障切换后的帧通信重新组态时间：300 ms

说明

有关详细信息，请参见 SCALANCE X-300 或 SCALANCE X-400 操作说明。

工业以太网交换机的环网组态

说明

对于 SCALANCE X414-3E，仅当两个 DIL 开关（R1 和 R2）都设置为“ON”（打开）时才能使用软件（CLI 或 WBM）进行组态。对于其它情况下的设置，请参见操作说明《工业以太网交换机 SCALANCE X-400》中的“SCALANCE X414-3E 的 DIL 开关”部分。

说明

对于 SCALANCE X414-3E，还可以使用 DIL 开关设置环型拓扑和环网端口中的介质冗余。

如果单击“环网组态”(Ring Config) 菜单项，将显示“环网组态”(Ring Configuration) 画面。

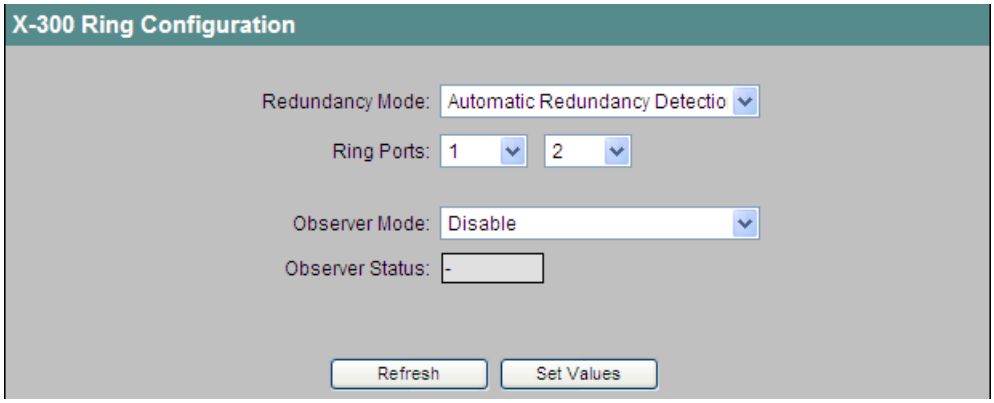


图 5-19　SCALANCE X-300/X-400 环网组态

冗余模式 (Redundancy Mode)

在“冗余模式”(Redundancy Mode) 下拉列表中，选择将在环网内指定设备角色的方式：

- 禁用 (Disabled)
- 自动冗余检测 (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，则该设备将获得“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 自动管理器 (MRP Auto Manager)
  设置为“自动冗余管理器”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”。与“自动冗余检测”(Automatic Redundancy Detection) 设置不同，设备在此模式下无法检测环网中是否存在 HRP 管理器。这意味着它们不可能获得“HRP 客户端”的角色。

- MRP 客户端 (MRP Client)
  在此处，可以选择"MRP 客户端"角色。
  在通过 MRP 组态设备的环网中，至少有一台设备必须设置为"自动冗余检测"或"MRP 自动管理器"的模式。您还可选择将其它所有设备都设置为"MRP 客户端"角色。如果环网中除某一设备外的其余设备都被组态为"MRP 客户端"，则该设备将自动获得"MRP 管理器"的角色。
  如果要在环网中将此设备与非 Siemens 生产的组件一起使用，请选择"MRP 客户端"模式。
- HRP 客户端 (HRP Client)
  在此处，可以选择"HRP 客户端"角色。
- HRP 管理器 (HRP Manager)
  此处，可以选择"HRP 管理器"角色。组态 HRP 环网时，必须将其中一个设备设置为 HRP 管理器。所有其它设备必须组态为 HRP 客户端。

说明

在复位为出厂默认设置后，将启用冗余模式"自动冗余检测"(ARD)。
环网端口的组态也会复位为出厂设置的端口：

- X-300：端口 9 和端口 10
- X-300 EEC：端口 8 和端口 9
- X304-2：端口 5 和 6
- X308-2M：端口 1 和端口 2
- XR324-4M：端口 1 和端口 2
- XR324-12M：端口 1.1 和端口 1.2
- X408-2：端口 5.1 和 5.2
- X414-3E：端口 5.1 和 5.2

如果先前已将其他端口用作环网端口，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。

环网端口 (Ring Ports)

在这两个下拉列表中，选择将用作环网端口的端口。

观察器模式 (Observer Mode)

说明

有关观察器功能的信息，请参见"X-300/X-400 HRP 冗余管理器观察器 (页 90)"部分。

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。观察器还能在检测出故障时断开相连的环网（保护模式）。

使用“观察器模式”(Observer Mode) 下拉列表，设置观察器的以下功能：

- 禁用 (Disable)
  禁用观察器功能。
- 保护模式 (Protection Mode)
  在保护模式下运行观察器功能。
- 重启观察器 (Restart Observer)
  将观察器功能复位并重新启用保护模式。

观察器状态 (Observer Status)

“观察器状态”(Observer Status) 显示框显示观察器的当前状态：

- 如果观察器未检测到故障，则该显示框中会显示“被动”(Passive)。
- 如果观察器检测到故障，则该显示框中会显示“主动”(active)。
- 如果禁用了观察器功能，则该显示框中会显示一个短破折号。

命令行接口语法

表格 5-19　X-300 环网组态 - CLI\X-300\RING>
X-400 环网组态 - CLI\X-400\RING>

命令	说明	注释
info	显示工业以太网交换机当前的环网组态。	-
red [模式]	启用/禁用环型拓扑中的 介质冗余。 可能的模式如下： • D 禁用环型拓扑中的介质冗余。 • HRPCL 工业以太网交换机为 HRP 客户端。 • HRPMGR 工业以太网交换机为 HRP 客户端。 • MRPCL 工业以太网交换机为 MRP 客户端。 • MRP 工业以太网交换机在 MRP 下工作并可自动成为冗余管理器。 • ARD 自动冗余检测。	仅限管理员。

命令	说明	注释
ports [<端口 1> <端口 2>]	指定环网端口。两个端口均需指定。	仅限管理员。
observer [D|R|P]	指定观察器功能： • D 禁用观察器功能。 • R 重启观察器功能。 • P 启用观察器功能。	仅限管理员。

5.3.2.3 X-300/X-400 HRP 冗余管理器观察器

HRP 环网中的观察器

HRP 冗余管理器观察器功能为错误诊断提供了更多选项，并可防止 HRP 出错。可用于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（保护模式），则其可以在检测到错误时中断已连接的环网。为此，观察器需将其状态从被动更改为主动并将环网端口（观察器端口）更改为“阻止”状态。错误消除后，观察器再次启用该端口。

如果某个时段内接连快速发生许多错误，则观察器不再自动启用其端口，而是永久保持为“主动”状态。这种现象将通过错误 LED 和下列消息文本进行指示：“观察器由于重复发生的错误过多（<错误数>）而停止恢复”。用户必须在错误消除后，从此状态开始重新激活观察器（重新启动观察器）。

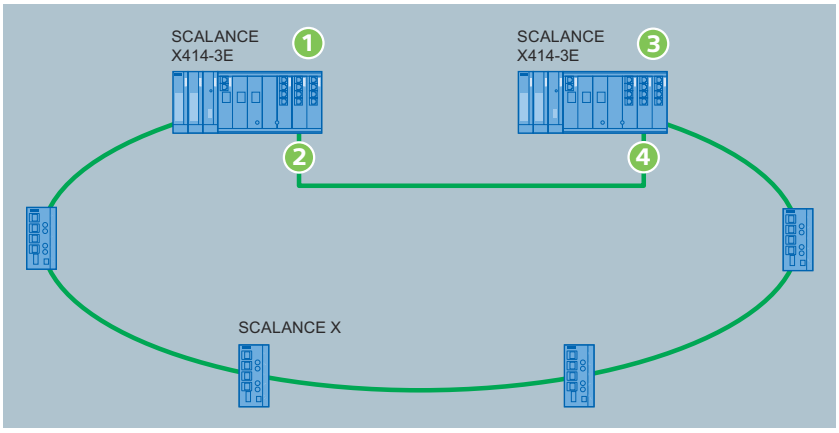
在设置带有 HRP 冗余管理器观察器的环网时，需注意以下几点：

- HRP 管理器上第一个组态的环网端口（阻塞端口）必须与观察器上第一个组态的环网端口（观察器端口）直接相连。
- 在工业以太网交换机上，可使用“命令行接口”(CLI) 或“基于 Web 的管理”(WBM) 启用观察器功能。
- 观察器和冗余管理器的固件版本均必须为 V2.2 或更高版本。

说明

为能够使用观察器功能，必须激活 HRP。

组态示例



① SCALANCE X414-3E 被组态为冗余管理器

② 冗余管理器的屏蔽端口

③ SCALANCE X414-3E 被组态为观察器

④ 第一个组态的观察器端口

图 5-20 通过观察器监视冗余管理器的冗余环网

启用或禁用

观察器功能为可选功能。默认情况下会将其禁用。

可在“环网组态”(Ring Config) 菜单中组态“观察器”(Observer) 功能。

错误消息

在观察器检测到错误时，将通过错误 LED、信号触点和相应的消息文本进行指示。将使用为报警事件“故障状态变化”(Fault State Change) 组态的消息发送方法，请参见“代理事件组态”。

可能的消息发送方法包括电子邮件、陷阱和/或事件日志表中的条目。

在附录 D“SCALANCE X-300/X-400 的错误消息”中提供了相关消息文本的列表。

5.3.2.4 X-300/X-400 备用屏蔽

冗余环网连接

自固件版本 1.2 起，除环型拓扑中的介质冗余外，工业以太网交换机还支持冗余 HRP 环网连接（包括中断 HRP 环网 = 线性拓扑）。在冗余链路中，两个 HRP 环网通过两个以太网连接相连在一起。实现的方法是在环网中组态主/从设备对，以使设备能通过环网端口彼此进行监视，并且能在发生故障时将数据通信从一个以太网连接（主设备的备用端口）引导至另一个以太网连接（从设备的备用端口）中。

有关以太网接线和主从设备拓扑位置的详细信息，请参见《SCALANCE X-400 工业以太网交换机操作说明》。

说明

要使用冗余环网连接功能，必须启用 HRP。

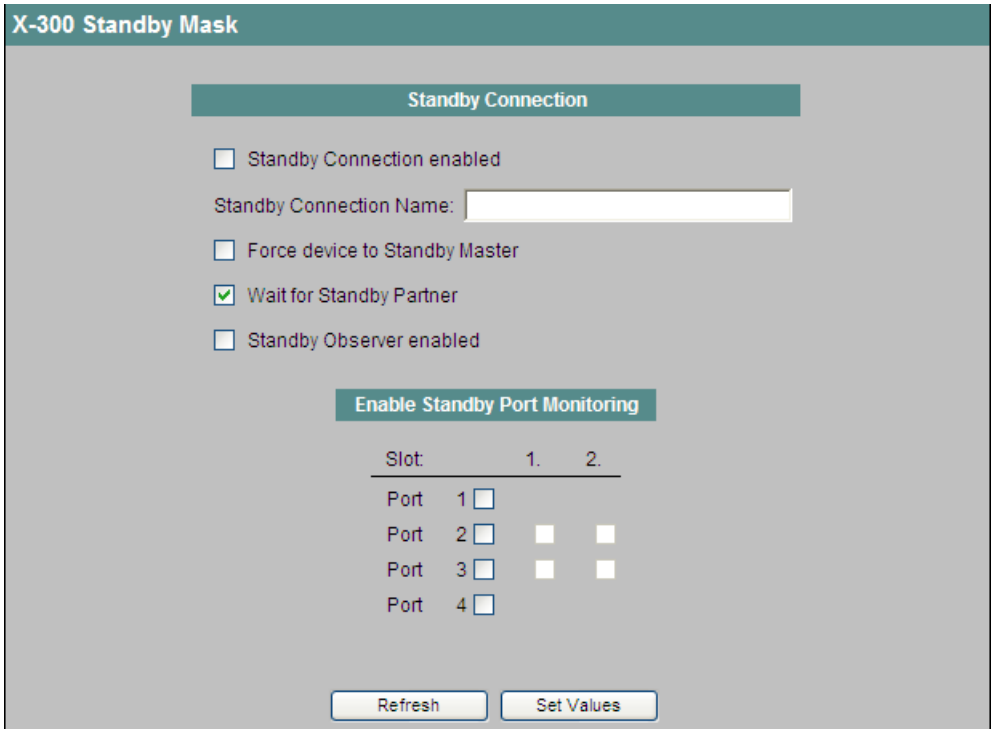


图 5-21 X-300 备用屏蔽

启用备用连接 (Standby Connection enabled)

在此处，您可决定是否启用备用功能。

备用连接名称 (Standby Connection Name)

在此处输入备用连接的名称。主/从设备对由此名称来进行定义（二者必须在同一环网中）。这可通过在环网中为两个设备输入相同的名称来实现。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。

将设备强制为备用主站 (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功能的设备选中该复选框，则会假定未发生任何错误，并且 MAC 地址较高的设备会成为备用主站。如果为两台设备都选择了该选项，或只有一台设备支持“将设备强制为备用主站”(Force Device to Standby Master) 属性，则也会根据 MAC 地址选择备用主站。这种类型的分配很重要，尤其是在更换设备时。根据 MAC 地址，前一个行使从站功能的设备将获得备用主设备的角色。

等待备用伙伴 (Wait for Standby Partner)（仅适用 SCALANCE X-300）

- 启用 (Enabled)
  只有在备用主设备和备用从设备以及它们的备用伙伴建立了连接后才会启用备用连接。这可确保在通过备用连接启动通信前冗余连接确实可用。
- 禁用 (Disabled)
  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。

启用备用观察器 (Standby Observer enabled)

通过选择该复选框来启用或禁用备用观察器功能。

有关此功能的详细信息，请参见“X-300/X-400 HRP 冗余管理器观察器 (页 90)”部分。

启用备用端口监视 (Enable Standby Port Monitoring)

说明

如果启用了备用观察器功能，则只能选择一个备用端口。

在此处指定用作备用端口的端口。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所连接 HRP 环网或 HRP 总线的数据通信。如果主设备或主设备上某备用端口的以太网连接（链路）出现故障，则将禁用主设备的所有备用端口，并启用从设备的备用端口。因此，到所连接网段（HRP 环网或 HRP 总线）的以太网连接都能恢复正常。

说明

如果有多个环网的链路（有多个端口启用“备用端口监视”），则备用主设备和备用从设备与每个环网之间只能有一个以太网连接。否则将产生帧循环传送从而导致数据通信丢失。

命令行接口语法

表格 5-20　X-400 备用屏蔽 - CLI\X-400\STANDBY> 或
X-300 备用屏蔽 - CLI\X-300\STANDBY>

命令	说明	注释
info	显示备用组态的相关信息。	-
standby [E|D]	启用/禁用备用功能。	仅限管理员
conname [字符串]	显示/指定备用连接名称。	仅限管理员
stbports [E|D> [端口]]	启用/禁用备用端口监视。	仅限管理员
wait [E|D]	指定是否只在备用主设备和备用从设备以及它们的备用伙伴建立连接后才启用备用连接。	仅限管理员
observer [E|D]	启用/禁用备用观察器监视。	仅限管理员

组态环网之间的冗余链路

请按以下步骤组态冗余 HRP 环网连接：

1. 计划好环网的哪些设备承担“备用主设备”角色，哪些执行“备用从设备”角色。此外还应计划好与其它环网的以太网连接相连的备用主设备和备用从设备端口。
   在出厂默认设置情况下，MAC 地址最高的设备将承担“备用主设备”角色。如果两个设备都支持“将设备强制为备用主站”(Force Device to Standby Master) 功能，则可将其中任意一个设备组态为备用主站，而不用考虑其 MAC 地址。

   说明

   确保在组态完成前不要插入冗余以太网连接。否则将产生帧循环传送从而导致数据通信丢失。这同样适用于禁用冗余链路的操作。

2. 指定备用连接的名称并为备用主设备和备用从设备输入该名称。

   说明

   确保（设备对的）备用连接名称在网络中仅被应用一次。

3. 通过选中“启用备用端口监视”(Enable Standby Port Monitoring) 下的相关复选框，指定备用主站和备用从站的备用端口。
4. 启用“启用备用连接”(Standby Connection enabled) 选项。

5. 用“设置值”(Set Values) 来确认组态。
6. **现在**，可以插入冗余以太网连接。

说明

确保将冗余以太网连接插入正确的端口中，即插入已组态的备用端口中。否则将产生帧循环传送从而导致数据通信丢失。

5.3.2.5 X-300/X-400 备用观察器

备用观察器

备用观察器是对简单冗余环网链路的扩展。它是另一个独立于主设备和从设备的备用链路。整个备用观察器链路由下图所示的两个互连的主/从设备对组成：

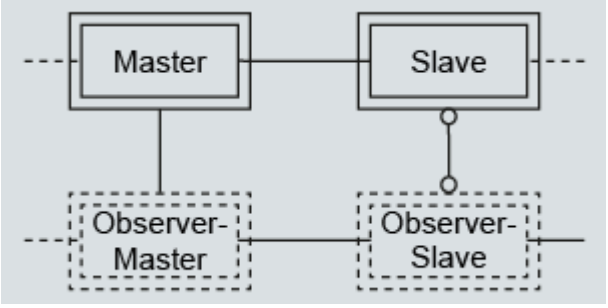


图 5-22 HRP 环网中的备用观察器链路

这两个主/从设备对可分别确保每次只启用两个链路路径中的一个。这可防止循环传送帧。

每个设备可通过将其当前状态与所连接设备的状态进行比较来检测故障。

但要检查某个链路是否已激活，必须查询链路上两个设备的状态；即，从设备和观察器从设备。

启用或禁用

可以不同的方式启用备用观察器功能：

- 通过主设备或从设备的“备用屏蔽”(Standby Mask) 页面上的设备组态。
  在建立了与连接设备的连接后，观察器功能会自动启动。这表示只需在两个连接设备之一上激活该功能。
- 在连接设备“观察器主设备”或“观察器从设备”上，在接收到观察器帧后会自动启用该功能。

注意
备用端口数 如果启用了备用观察器功能，则只能在“备用屏蔽”(Standby Mask) 页面上选择单个的备用端口。

说明

意外生成备用观察器实例

如果连接备用端口时启用了备用观察器功能，则会在所连接的交换机上另外激活一个备用观察器实例。可通过这种方式在拓扑中生成任意数量的备用观察器。

网络拓扑对备用观察器实例的生成没有任何影响。

说明

使用线性总线拓扑的限制

对于激活了备用观察器功能的线性总线的冗余连接，请注意下列限制：
只允许总线之间的链路路径冗余。如果备用主设备和备用从设备或观察器主设备和观察器从设备之间的总线中断，则相关从设备将保持被动状态。这表示将中断与从设备以及所有与该从设备相连的设备的通信。

伙伴设备不支持备用观察器功能

如果启用了备用观察器功能，但链路伙伴（SCALANCE X-200 或固件版本较早的 SCALANCE X-300/X-400）不支持此项功能，则该组态属于错误组态。将有至少一台备用观察器设备通过红色错误 LED 指示这一错误组态，同时显示以下错误消息：“新故障状态：备用观察器的‘主站’（‘从站’）角色与自身‘从站’（‘主站’）角色发生冲突。”

在这种情况下，需禁用备用观察器功能。如果无法对相应设备执行这一操作，则需要中断激活的备用链路。

与备用观察器功能相关的消息

在状态和事件消息中，“伙伴”表示位于相同环网中的设备。这表示上图中的主设备和从设备是伙伴，观察器主设备和观察器从设备也是伙伴。“观察器”在其它环网中为连接设备。

可能出现以下状态消息：

- “备用设备正在等待 <伙伴/观察器>。”
  备用观察器功能已启用，至此尚未联系上伙伴或观察器。
- “备用 <伙伴/观察器> 已连接至 <主设备/从设备> <MAC 地址> <端口号>。”
  已建立与伙伴或观察器的连接。

- “备用 <伙伴/观察器> 失去与 <主设备/从设备> <MAC 地址> <端口号> 的连接。”
  与伙伴或观察器的现有连接已中断。
- “备用 <伙伴/观察器> 与 <主动/被动> 状态相冲突。”
  由伙伴或观察器指示的状态与模块本身当前的主动/被动状态相冲突。将保持网络的完整性。在极端情况下（错误过多时），备用链路可能会中断。例如，此错误表示备用伙伴之间的连接中止或设备故障。
- “备用 <伙伴/观察器> 的状态冲突已解决。”
  上述状态已解决，例如，在消除故障后。
- “备用 <伙伴/观察器> 与 <主设备/从设备> 角色相冲突。”
  由伙伴或观察器指示的功能与本地主设备/从设备角色相冲突。
  当两个备用设备在环网中承担相同的主设备/从设备角色，或两个连接的观察器都没有承担主设备/从设备角色时，会出现这种情况。将保持网络的完整性。在极端情况下（错误过多时），备用链路可能会中断。例如，此错误表示备用伙伴之间的连接中止或设备故障。
- “备用 <伙伴/观察器> 与 <主设备/从设备> 角色的冲突已解决。”
  上述状态已解决，例如，在消除故障后。
- “备用 <伙伴/观察器> 与观察器 <开/关> 组态发生冲突。”
  由伙伴或观察器指示的组态与模块本身当前备用观察器设置相冲突。
- “备用 <伙伴/观察器> 观察器组态冲突已解决。”
  上述状态已解决；伙伴或观察器的组态与模块本身的备用观察器设置相匹配。
- “备用从设备 - 至少一个备用端口没有链路。”
  从设备的至少一个备用端口没有建立连接。
  如果相应主设备的一个备用端口出现此故障，则从设备无法通过其备用端口建立连接。
- “备用从设备 - 所有备用端口都已建立连接。”
  上述状态已解决；从设备的所有备用端口都具有连接。

可能出现以下事件消息：

- “备用观察器功能 <已启动/已停止>。”
  已启动或已停止备用观察器功能。
- “备用功能 <已启动/已停止>。”
  已启动或已停止备用功能。
- “从设备 - 承担 <主设备/从设备> 角色。”
  已获得主设备或从设备角色。

5.3.3 X-300/X-400 故障屏蔽

故障屏蔽的作用

使用故障屏蔽，可以指定受工业以太网交换机监视并会触发信号触点的故障/错误状态。 可能的故障/错误状态包括：无电源，电压过低，以及与伙伴设备的连接中断或意外连接。 如果信号触点被触发，这将导致设备上的故障 LED 亮起，并将根据事件表的组态触发陷阱、电子邮件或在日志表中增加条目。

端口的设备相关链路监视

工业以太网交换机具有设备相关链路监视功能。 如果工业以太网交换机进行了相应的组态，则链路接通或链路中断也会影响消息系统。

在设备上设置故障屏蔽

故障屏蔽还可通过工业以太网交换机前面板上的 SET/SEL 按钮进行设置；有关详细信息，请参见《SCALANCE X-400 工业以太网交换机操作说明》。

在 WBM 中设置

在 WBM 中，你可设置对电源的监视和设备相关链路监视。 有三项屏蔽需要分别设置：

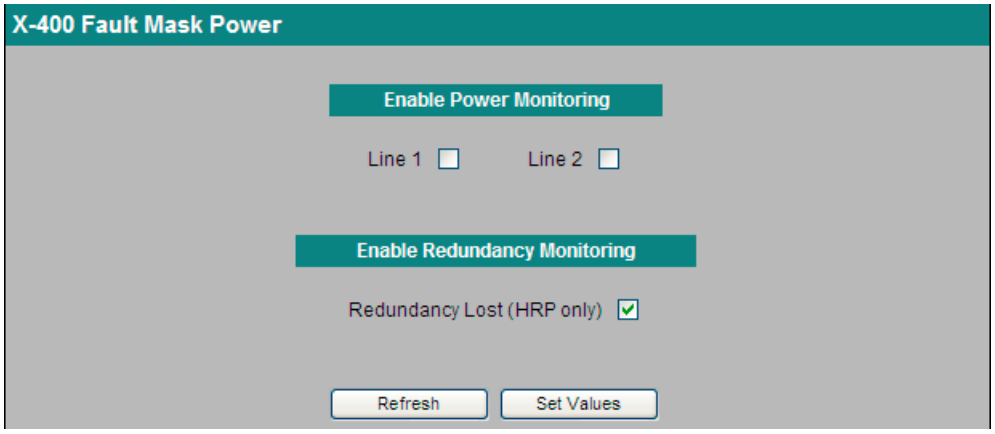


图 5-23 X-400 电源故障屏蔽

启用电源监视 (Enable Power Monitoring)

在此处，可以指定是否监视电源线路 1 或 2。 当所监视的电源线路（线路 1 或线路 2）未通电或电压过低（小于 14 V）时，消息系统将指示故障。

由故障 LED 通知冗余丢失情况（仅 HRP）(Signal Redundancy Lost by Fault LED (HRP only))

如选中此复选框，则 HRP 冗余丢失时将由冗余管理器的故障 LED 进行指示，并通过故障信号触点发出信号。 备用链路的冗余丢失由具有故障 LED 和故障信号触点的备用从站提供提示。 出厂时会启用该功能。

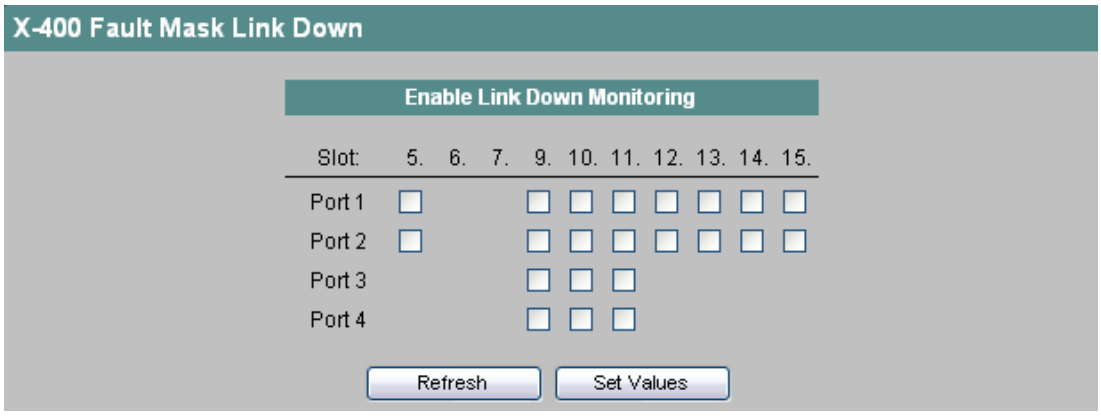


图 5-24　X-400 链路中断故障屏蔽

启用链路中断监视 (Enable Link Down Monitoring)

选中要监视连接状态的插槽/端口对应的复选框。 如果已激活链路监视，则当此端口无有效链路时（例如，因为电缆未插入或相连设备已关闭）将发出错误信号。

错误/故障可按照以下方式发送信号，具体取决于工业以太网交换机的组态： 信号触点、故障 LED、SNMP 陷阱、电子邮件、日志表中的条目、系统日志。

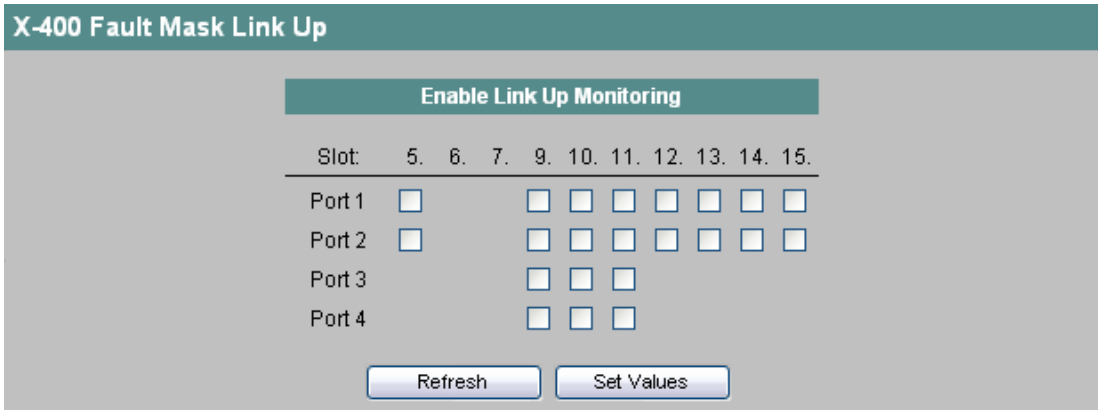


图 5-25　X-400 链路激活故障屏蔽

启用接通监视 (Enable Link Up Monitoring)

选中要监视连接状态的插槽/端口对应的复选框。 如果已激活链路监视，则当此端口存在有效连接时（例如，不应插入电缆）将发出错误信号。

错误/故障可按照以下方式发送信号，具体取决于工业以太网交换机的组态： 信号触点、故障 LED、SNMP 陷阱、电子邮件、日志表中的条目、系统日志。

命令行接口语法

表格 5-21　X-400 故障屏蔽 - CLI\X-400> 或
X-300 故障屏蔽 - CLI\X-300>

命令	说明	注释
power [<E|D> [线路]]	启用/禁用对电源连接器 L1 和 L2 的监视。	仅限管理员。
hrpfled [E|D]	启用/禁用在发生 HRP 冗余丢失时的故障 LED 指示和通过故障信号触点发出信号。	仅限管理员。
linkdown [<E|D> [端口]]	启用/禁用所选端口的链路监视。 如未指定任何端口，则所有端口都将被启用/禁用。	仅限管理员。 如果要在参数中指定多个端口，则各端口之间应使用空格隔开。
linkup [<E|D> [端口]]	启用/禁用所选端口的链路监视。 如未指定任何端口，则所有端口都将被启用/禁用。	仅限管理员。 如果要在参数中指定多个端口，则各端口之间应使用空格隔开。

5.3.4　X-300/X-400 计数器

信号触点和冗余电路的响应

利用计数器，可以监视运行中是否发生故障以及故障发生的频率（例如，信号触点响应的频率）。

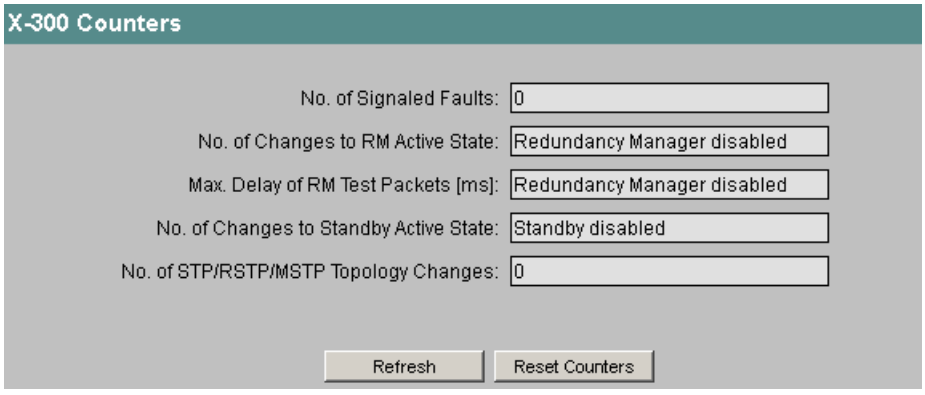


图 5-26　X-300 计数器

已通知故障数 (No. of Signaled Faults)
指示工业以太网交换机的信号触点响应的频率。

计数器会在每次设备重启时复位。

变为 RM 激活状态的次数 (No. of Changes to RM Active State)
只有在工业以太网交换机充当 HRP 管理器时（参见"X-300/X-400 环网组态"部分），此处才会显示值。

该值指示 HRP 管理器变为主动状态的频率。 当冗余管理器检测到与环网端口相连的线路发生中断时，将采用此状态。

计数器会在每次设备重启时复位。

RM 测试包的最大延迟 [ms] (Max. Delay of RM Test Packets[ms])
只有在工业以太网交换机充当 HRP 管理器（已选中"启用冗余管理器"(Redundancy Manager enabled) 复选框）时，此处才会显示值。

在冗余管理器模式下，工业以太网交换机将通过环网端口向相连的交换机线路发送测试帧，并测量这些测试帧的延迟。 这些测试包发生的最大延迟将被显示出来。

变为备用激活状态的次数 (No. of Changes to Standby Active State)
只有在启用备用功能时，此处才会显示值（参见"X-300/X-400 备用屏蔽"部分）。

此值表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。 当备用主设备的备用端口连接出现故障时，将采用此状态。

计数器会在每次设备重启时复位。

STP/RSTP/MSTP 拓扑变化的次数 (No. of STP/RSTP/MSTP Topology Changes)
显示由于生成树机制而执行的重新组态操作的频率。

复位计数器 (Reset Counters)
单击此按钮可复位工业以太网交换机的计数器。 重启（例如，由于工业以太网交换机的电源中断）将导致计数器复位。

命令行接口语法

表格 5-22　X-400 计数器 - CLI\X-400> 或 X-300 计数器 - CLI\X-300>

命令	说明	注释
counters	显示以下计数器读数： • 变为 RM 激活状态的次数 指示充当冗余管理器的工业以太网交换机闭合环网的频率。 • RM 测试包的最大延迟 (Max. delay of RM Test Packets) 指示冗余管理器发送的测试帧的最大延迟。	-
resetc	复位工业以太网交换机计数器。	仅限管理员。

5.4 代理菜单

5.4.1 代理组态

简介

如果单击“代理”(Agent) 文件夹图标，将显示“代理组态”(Agent Configration) 画面。此画面提供设置 IP 地址的选项。可将交换机指定为自动获取 IP 地址，或者为其分配一个固定地址。此外，还可以激活访问工业以太网交换机的选项，例如 SSH 或 RMON。

SCALANCE X414-3E 的 IP 组态

在此处，可以为 SCALANCE X414-3E 指定 IP 组态。交换机端口（“带内”(In-Band) 列）和交换机 CPU 的以太网端口（“带外”(Out-Band) 列）应有所区别。

说明

CPU 的 IP 地址应与交换机端口的 IP 地址分属不同的子网。

IP 地址 (IP Address)

SCALANCE X414-3E 或 CPU 模块的 IP 地址。如果更改 IP 地址，则将自动导向到新的地址。如果未发生自动导向，则请在 Web 浏览器中手动输入新地址。

子网掩码 (Subnet Mask)

在此处，可以输入 SCALANCE X414-3E 或 CPU 模块的子网掩码。

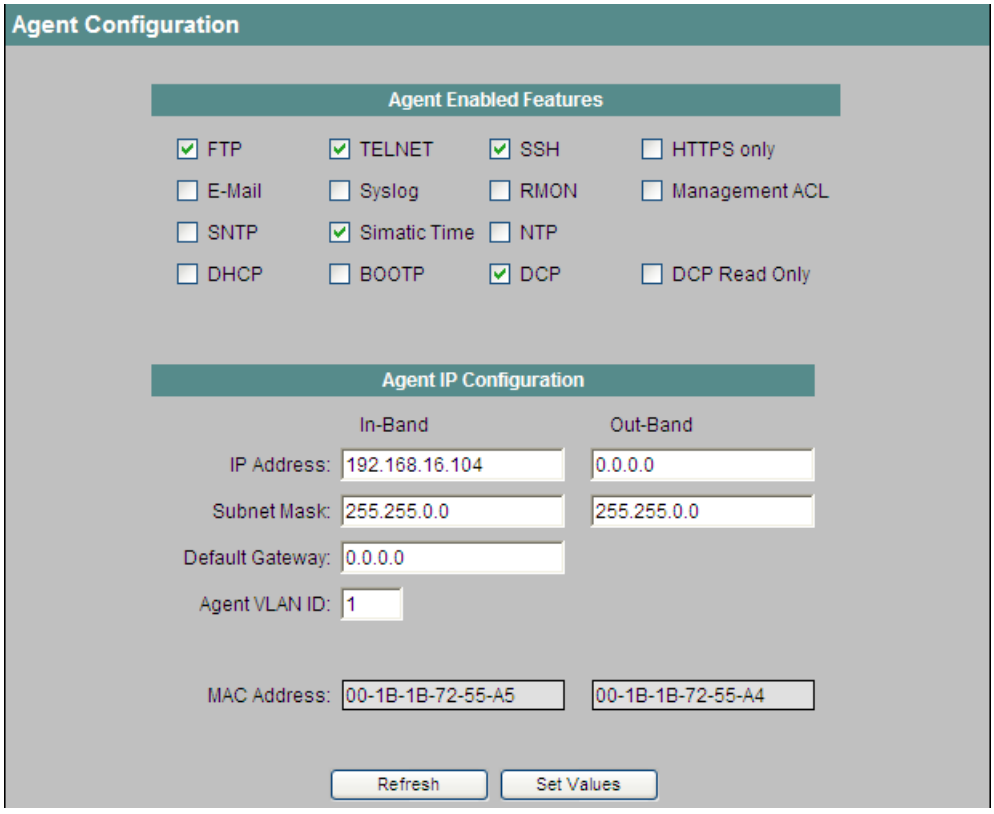


图 5-27　SCALANCE X414-3E 代理组态

SCALANCE X-300/X408-2 的 IP 组态

在此处，可以为 SCALANCE X-300/X408-2 指定 IP 组态。

说明

在 SCALANCE X-300/X408-2 上，不能组态任何 CPU 以太网端口（带外端口）。仅可以组态交换机端口。

子网掩码 (Subnet Mask)

在此处输入子网掩码。

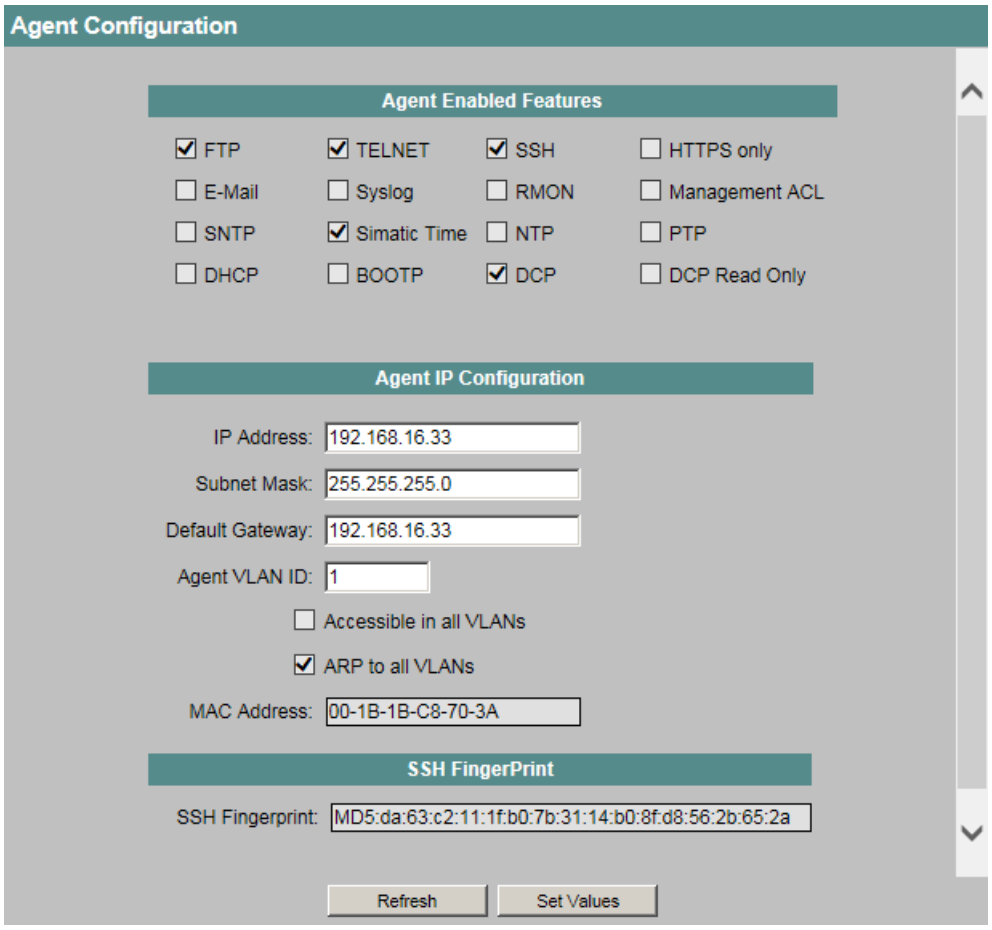


图 5-28　代理组态 SCALANCE X300

工业以太网交换机的设置

FTP

启用/禁用 FTP 服务器。FTP 可用于下载固件。有关此主题的详细信息，请参见“固件更新”部分。您还可通过 FTP 下载或备份组态数据。

如果工业以太网交换机具有 IP 地址并且与 PC 或 PG 之间存在以太网连接，则请按以下步骤下载组态数据：

1. 打开控制台窗口并输入命令 ftp，后接工业以太网交换机的 IP 地址。例如：
   ftp 192.168.20.54
2. 登录帐户和密码可使用与 WBM 和 CLI 相同的值。
3. 输入“put”命令，后接固件文件的名称。
   例如：
   put cfgdata.txt
4. 加载文件之后，工业以太网交换机将关闭 FTP 连接并进行重启。

TELNET

在此处，指定是否允许通过 TELNET 访问工业以太网交换机。

说明

自固件版本 4.1.3 起，在交付状态下或设备复位为出厂设置后，TELNET 将被禁用。出于安全考虑，建议使用 SSH。

SSH

在此处，指定是否允许通过 SSH 访问工业以太网交换机。

仅 HTTP (HTTPS Only)

在此处，指定是否仅允许通过 HTTP 来访问工业以太网交换机。如果未选中此选项，仍可通过 HTTP 进行访问。

电子邮件 (E-mail)

此项可启用/禁用工业以太网交换机的电子邮件功能。有关此功能的详细信息，请参见“代理电子邮件组态 (Agent E-Mail Configuration) 菜单项”部分。

Syslog

在此处，可以指定工业以太网交换机是否在 Syslog 服务器上存储了日志条目。有关此功能的详细信息，请参见“代理 Syslog 组态 (Agent Syslog Configuration) 菜单项”部分。

RMON

工业以太网交换机支持远程监视 (RMON)。远程监视允许在工业以太网交换机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。RMON 的设置并不会影响统计功能（请参见“统计菜单”部分）。

管理 ACL (Management ACL)

说明

启用该功能时请注意下列事项：“管理 ACL 组态”(Management ACL Configuration) 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。

可通过单击该复选框来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。

在“管理 ACL 组态”(Management ACL Configuration) 页面上对访问规则进行管理，请参见管理访问控制列表 (页 149)部分

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。

SNTP

启用/禁用通过网络中的 SNTP 服务器同步工业以太网交换机的系统时间。

支持的版本：SNTP V4

SIMATIC 时间 (SIMATIC Time)

启用/禁用通过 SIMATIC 时间协议同步工业以太网交换机的系统时间。

在这种情况下，将利用发送至地址 09-00-06-01-FF-EF 的组播帧进行同步。

工业以太网交换机在登录至 SNTP 服务器时还将评估 SIMATIC 时间帧。

NTP

启用/禁用通过网络中的 NTP 服务器同步工业以太网交换机的系统时间。

支持的版本：NTP V4

PTP

说明

此选项仅适用于支持 PTP 的交换机。

启用/禁用通过主设备发出的 PTP 时间同步工业以太网交换机的系统时间。要实现此目的，工业以太网交换机必须是 PTP 网络中的“Transparent Clock”。

有关 PTP 的更多信息，请参见“符合 IEEE 1588 的精确时间协议 (PTP) (页 271)”和“通过 WBM 组态精确时间协议 (页 278)”部分。

说明

避免时间跳跃

为避免时间跳跃，需确保网络中只有一台时间服务器（SICLOCK 时间发送器、(S)NTP 服务器、PTP 主站）。

即使网络中有多台时间服务器，也只能激活一个时间协议。

DHCP

如果启用此复选框，则工业以太网交换机将在网络中查找 DHCP 服务器并根据此服务器提供的数据来组态其 IP 参数。有关此功能的详细信息，请参见“通过工业以太网交换机的 DHCP 客户机分配地址”部分。

说明

一旦 PROFINET IO 控制器分配过一次 IP 地址，DHCP 本身就会自动禁用，而且必须根据需要重新将其激活。

BOOTP

如果启用此复选框，则工业以太网交换机将在网络中查找 BOOTP 服务器并根据此服务器提供的数据来组态其 IP 参数。有关此功能的详细信息，请参见“通过工业以太网交换机的 BOOTP 客户机分配地址”部分。

DCP

如果选中此选项，则可通过 DCP（SINEC PNI 和 STEP 7）对设备进行访问和组态。

DCP 只读 (DCP Read Only)

如果选择此选项，则仅可通过 DCP（SINEC PNI 和 STEP 7）读取组态数据。

默认网关

如果需要工业以太网交换机与不同子网中的设备（诊断站、电子邮件服务器等）通信，则需在此处输入默认网关的 IP 地址。

代理 VLAN ID (Agent VLAN ID)

在此处输入代理的 VLAN-ID。

可在所有 VLAN 中访问 (Accessible in all VLANs)

如果启用此选项，则可通过所有 VLAN 来访问全部代理功能（Ping、Telnet、Web 界面等）；如果禁用，则仅可通过代理 VLAN 访问这些功能。“可在所有 VLAN 中访问”功能对 DCP 没有影响。

ARP 到所有 VLAN (ARP to all VLANs)

只有在“可在所有 VLAN 中访问”(Accessible in all VLANs) 选项启用时，才会用到此选项。如果启用此选项，管理代理将 ARP 数据包发送到所有 VLAN。如果禁用此选项，管理代理仅将 ARP 数据包发送到“代理 VLAN ID”(Agent VLAN ID) 中组态的 VLAN。

MAC 地址 (MAC Address)

工业以太网交换机或 CPU 模块的 MAC 地址。

SSH 指纹（仅适用于 SCALANCE X-300）

SSH 指纹是 SSH 协议用以验证交换机的公共密钥的简称。根据 SSH 密钥，可以检查该密钥是否正确。

命令行接口语法

表格 5-23　代理组态 - CLI\AGENT>

命令	说明	注释
ip [IP 地址]	指定工业以太网交换机的带内 IP 地址。应输入四个十进制数字，用点分隔。 如果未指定任何参数，则将显示当前设置的带内 IP 地址。	仅限管理员。 如果要通过 Web 浏览器、TELNET 或 SNMP 来访问工业以太网交换机，则必须输入 IP 地址。IP 地址也可由 BOOTP/DHCP 自动分配。
subnet [子网掩码]	指定工业以太网交换机带内端口的子网掩码。应输入四个十进制数字，用点分隔。	仅限管理员。 如果要通过 Web 浏览器、TELNET 或 SNMP 来访问工业以太网交换机，则必须输入子网掩码。 IP 地址也可由 BOOTP/DHCP 自动分配。
gateway [IP 地址]	指定默认 IP 网关的 IP 地址。应输入四个十进制数字，用点分隔。	仅限管理员。 如果需要在工业以太网交换机上访问路由器，并且通信伙伴与工业以太网交换机不属于同一子网，则必须输入 IP 地址。网关必须在带内 IP 地址的子网中，或者在带外 IP 地址的子网中。 IP 地址也可由 BOOTP/DHCP 自动分配。
vid [编号]	指定代理 VLAN ID。	仅限管理员。 默认值：1
allvlans [E|D]	指定是否可通过所有 VLAN 或仅可通过代理 VLAN 访问代理功能。	仅限管理员。 默认值：禁用 (Disabled)

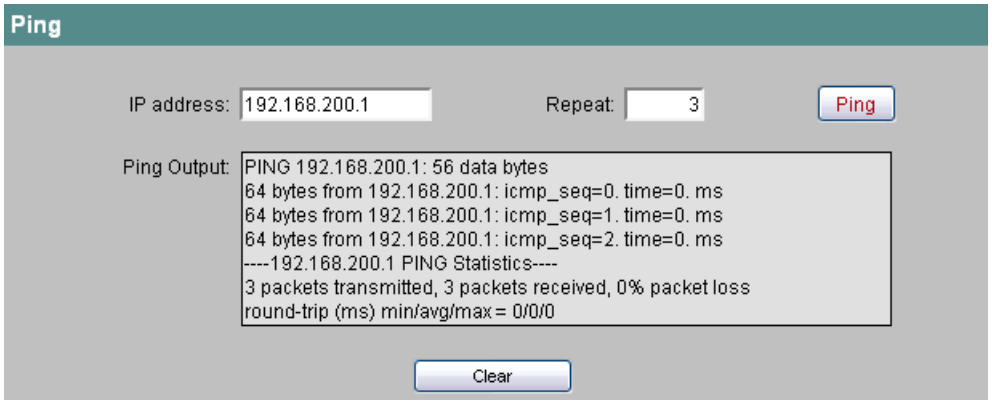
命令	说明	注释
bootp [E|D]	启用/禁用 BOOTP。	仅限管理员。 默认值：禁用 (Disabled)
dhcp [E|D]	启用/禁用 DHCP。	仅限管理员。 默认值：启用。
mail [E|D]	启用/禁用电子邮件功能。	仅限管理员。 默认值：禁用。
ftp [E|D]	启用/禁用 FTP。	仅限管理员。 默认值：启用
dcp [D|RO|RW]	启用/禁用 DCP • D 禁用 • RO 只读 • RW 读写	仅限管理员。 默认值：读写
telnet [E|D]	启用/禁用 TELNET。	仅限管理员。 默认值：启用。
rmon [E|D]	启用/禁用远程监视。	仅限管理员。 默认值：禁用 (Disabled)
macl [E|D]	启用/禁用管理访问控制列表。	仅限管理员。
sntp [E|D]	启用/禁用 SNTP。	仅限管理员。 默认值：禁用 (Disabled)
siclock	启用/禁用通过 SIMATIC 时间协议进行时间同步。	仅限管理员。 默认值：启用
ntp [E|D]	启用/禁用 NTP。	仅限管理员。 默认值：禁用 (Disabled)
ptp [E|D]	启用/禁用 PTP。	仅限管理员。 默认值：禁用 (Disabled)

命令	说明	注释
ping [-c 数量] [-s 长度] <IP 地址>	向指定 IP 地址发送一定数量的数据包。如果省略数量和长度参数，则工业以太网交换机将发送 10 个长度为 128 字节的包。 示例： ping -c 5 -s 256 192.168.1.1 5 个长度为 256 字节的包将被发送到 IP 地址 192.168.1.1。	-
ssh [E|D]	启用/禁用 SSH。	仅限管理员。 默认值：启用
httpso [E|D]	指定工业以太网交换机是否仅可通过 HTTP 访问（禁用时仍可通过 HTTP 访问）。	仅限管理员。 默认值：禁用。
slog [E|D]	启用/禁用 Syslog。	仅限管理员。

5.4.2 Ping

IP 网络中地址的可达性

基于 Web 的管理中的 ping 功能与同名的终端功能完全相同。该功能会检查某一地址是否存在于 IP 网络中。



IP 地址 (IP address)

输入要 ping 的网络设备的 IP 地址，以测试是否可访问该设备。

重复 (Repeat)
在此输入要发送的数据包的数目。

Ping
单击此按钮开始发送数据包。

Ping 输出 (Ping Output)
该框会显示 ping 功能的输出。

5.4.3 SNMP

5.4.3.1 代理 SNMP 组态

SNMP 的工作原理

通过 SNMP（Simple Network Management Protocol，简单网络管理协议），网络管理站可对 SNMP 兼容节点（例如工业以太网交换机）进行组态和监视。为实现这一点，在与管理站交换数据的工业以太网交换机中安装有管理代理。共有三种数据包类型：

- 读取（管理站从工业以太网交换机中获取值）
- 写入（管理站向工业以太网交换机中写入值）
- 将事件发送到注册节点（陷阱）。
  代理将向注册管理站发送消息。

SNMPv3（和 SNMPv2）与 SNMPv1 相比的增强功能

SNMPv3（和 SNMPv2）与原始的 SNMPv1 相比具有以下增强功能：

- 各管理站可彼此进行通信。
- 通过网络中唯一的 SNMP 引擎 ID 实现的多级别安全概念（数据加密、用户身份验证）。
- 用户定义的安全设置

SNMP 的访问权限

应用 SNMP 协议时，可通过团体字符串来指定访问权限。团体字符串以字符串形式包含用户名称和密码的相关信息。可以为不同的团体字符串定义读取和写入权限。仅部分 SNMPv2 版本和 SNMPv3 具有更复杂且更安全的身份验证功能。

说明

为保证安全性，不应使用默认值 public 或 private。

组态工业以太网交换机的 SNMP

如果单击“SNMP”文件夹图标，将显示“SNMP 组态”(SNMP Configration) 画面。

在“SNMP 组态”(SNMP Configuration) 画面中，可进行 SNMP 的基本设置。根据希望应用的 SNMP 功能启用相应的复选框。关于详细设置（陷阱、组、用户），WBM 中有独立的菜单项。在此处，即使并未选中启用 SNMPv3 选项，也可进行输入，但是输入内容并不生效。

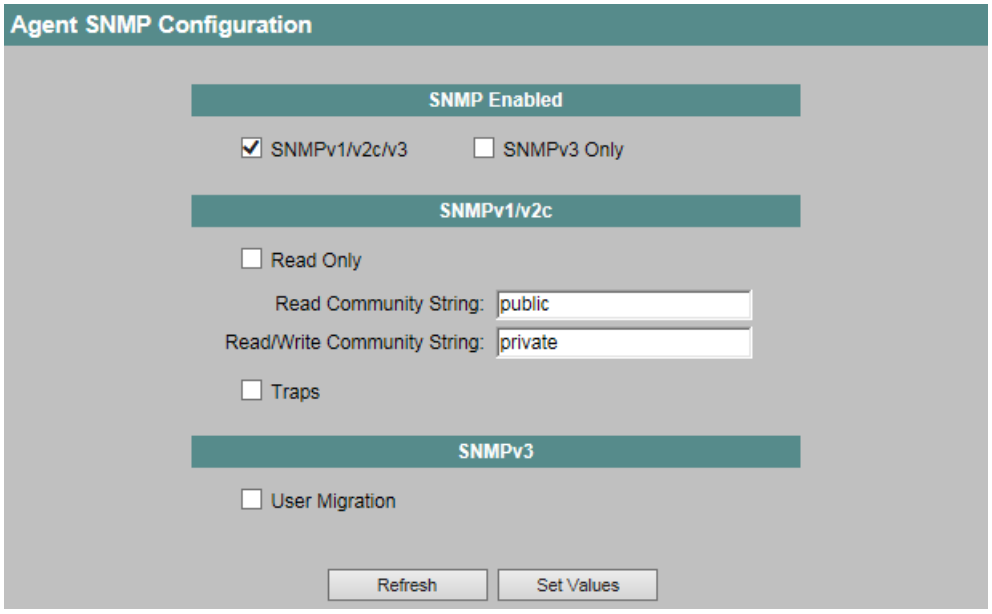


图 5-29　代理 SNMP 组态

SNMP 启用

- **SNMPv1/v2/v3**
  在此处，可以启用/禁用工业以太网交换机的 SNMPv1、SNMPv2 和 SNMPv3。
- **仅 SNMPv3 (SNMPv3 only)**
  如果选中此选项，则将仅启用 SNMPv3；SNMPv1 和 SNMPv2 的功能将不可用。

SNMPv1/V2c

- **只读 (Read Only)**
  如果选中此选项，则使用 SNMPv1/v2c 仅可读取 SNMP 变量。
- **读取团体字符串 (Read Community String)**
  在此处，可以输入 SNMP 协议的读取团体字符串（最多 20 个字符）。
- **读/写团体字符串 (Read/Write Community String)**
  在此处，可以输入 SNMP 协议的写入团体字符串（最多 20 个字符）。
- **陷阱 (Traps)**
  此项可启用/禁用 SNMPv1/v2c 陷阱的发送。

SNMPv3

引入 SNMPv3 后，不使用特殊操作（如加载组态文件或替换 C-PLUG）的情况下，无法再将用户组态传送至其他设备。

依据标准，SNMPv3 协议使用唯一的 SNMP 引擎 ID 作为 SNMP 代理的内部标识符。此 ID 在网络中必须是唯一的。用于验证 SNMPv3 用户的访问数据并对其进行加密。

根据“SNMPv3 用户移植”功能的启用情况，会以不同方式生成 SNMP 引擎 ID。

- **用户移植** (SCALANCE X-300/X408-2)
  - **已启用**
    如果启用该功能，会生成一个可移植的 SNMP 引擎 ID。可以将已组态的 SNMPv3 用户传送至不同的设备。
    如果启用该功能并将设备的组态加载到另一个设备，将保留组态的 SNMPv3 用户。
  - **已禁用**
    如果禁用该功能，会生成一个设备特定的 SNMP 引擎 ID。要生成此 ID，需要使用设备的代理 MAC 地址。不得将此 SNMP 用户组态传送至其他设备。
    如果将设备的组态加载到另一个设备，将删除所有组态的 SNMPv3 用户。

说明

启用或禁用“SNMPv3 用户移植”功能后，会始终删除组态的 SNMPv3 用户。禁用“SNMPv3 用户移植”功能后，SNMP 引擎 ID 会复位为设备特定值。

使用该功能时的限制

仅可在更换设备时使用“SNMPv3 用户移植”(SNMPv3 User Migration) 功能传送组态的 SNMPv3。

请勿使用该功能将组态的 SNMPv3 用户传送到多个设备。如果将具有已创建的 SNMPv3 用户的组态加载到多个设备，则这些设备会使用相同的 SNMP 引擎 ID。如果在同一网络中使用这些设备，则组态会与 SNMP 标准相矛盾。

默认值

- 升级到固件版本 4.0.2 以后：
  禁用
- 复位为出厂默认设置后：
  启用

与旧产品的兼容性

如果您已将用户创建为可移植用户，则可以将已组态的 SNMPv3 用户传送至不同的设备。为创建可移植用户，创建时必须激活“SNMPv3 用户移植”(SNMPv3 User Migration) 功能。如果已使用低于 4.0.2 版本的固件创建了 SNMPv3 用户，则将组态传送到不同设备时将删除这些用户。

命令行接口语法

说明

在影响 SNMP 的 CLI 命令中输入空格

如果空格作为参数的一部分输入，则需要使用波形字符 (~) 代替。

示例：
如果 SNMP 用户名由两个以空格分隔的字符串组成，则需输入以下条目：
<String1>~<String2>

表格 5-24　代理 SNMP 组态 - CLI\AGENT\SNMP>

命令	说明	注释
snmp [D|3|A]	禁用/启用 SNMP。参数的含义如下： • D 禁用 SNMP。 • 3 仅启用 SNMPv3。 • A 启用 SNMPv1、SNMPv2 和 SNMPv3。	仅限管理员。 默认值：SNMPv1、v2 和 v3 启用。
getcomm [字符串]	指定读取团体字符串（最长 20 个字符）。默认值为“public”。	仅限管理员。
setcomm [字符串]	指定读/写团体字符串（最长 20 个字符）。默认值为“private”。	仅限管理员。
traps [E|D]	启用/禁用 SNMPv1 陷阱。	仅限管理员。
usermigr [E|D]	在更换设备时，通过组态文件/C-PLUG 激活/取消激活传送组态的 SNMPv3 用户。	仅限管理员。 仅适用于 SCALANCE X-300/X408-2 默认值： • 升级到固件版本 4.0.2 以后： 禁用 • 复位为出厂默认设置后： 启用

5.4.3.2 SNMPv1 陷阱组态

报警事件的 SNMP 陷阱

如果发生报警事件，工业以太网交换机可同时向最多 10 个不同的（网络管理）站点发送陷阱（报警帧）。只有在发生“代理事件组态”(Agent Event Configuration) 菜单中指定的事件时，才会发送陷阱（请参见“代理事件组态”部分）。

说明

只有在“SNMP 组态”(SNMP Configuration) 中已选中“陷阱”(Traps) 选项时，才会发送陷阱。

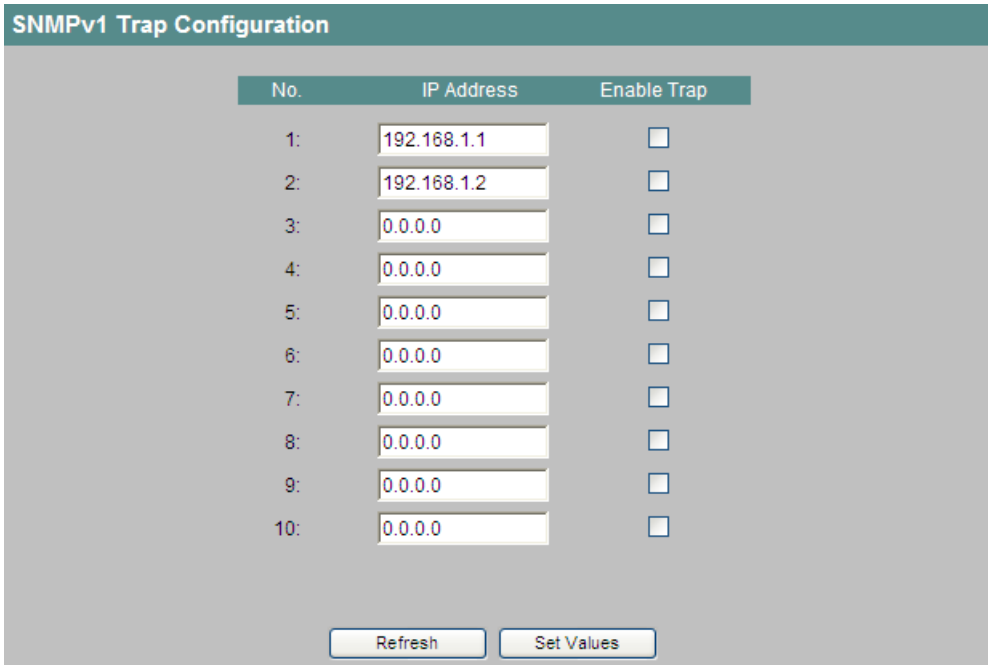


图 5-30 SNMPv1 陷阱组态

IP 地址 (IP Address)

在此处，可以输入工业以太网交换机发送陷阱的目标站地址。

启用陷阱 (Enable Trap)

单击 IP 地址旁的复选框可启用向相应站点发送陷阱的操作。

命令行接口语法

表格 5-25　SNMPv1 陷阱组态 - CLI\AGENT\SNMP\TRAPCONF>

命令	说明	注释
Info	显示当前陷阱组态。	-
ip <条目> <IP>	指定陷阱接收条目的 IP 地址（条目介于 1 和 10 之间）。	仅限管理员。 默认值： 0.0.0.0
state <条目><E|D>	启用/禁用向接收条目发送陷阱（条目介于 1 和 10 之间）	仅限管理员。 默认值： D

5.4.3.3　SNMPv3 组的组态

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。设置会自动应用于组内的各成员。

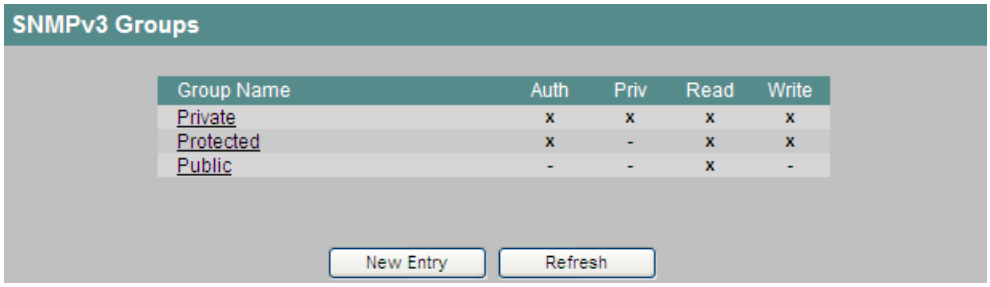


图 5-31　SNMPv3 组

组名称 (Group Name)

此处列有所有此前已定义的组名称。单击某组名称时，将弹出一个新窗口，可在其中更改该组的参数设置。

身份验证 (Auth)
此列中的叉表示相应的组已启用身份验证功能。

加密 (Priv)
此列中的叉表示相应的组已启用加密功能。

读取 (Read)
此列中的叉表示相应的组已启用读取访问功能。

写入 (Write)
此列中的叉表示相应的组已启用写入访问功能。

新条目 (New Entry)
单击该按钮可创建新组。

SNMPv3 组的组态

单击组名称时，将打开组态组属性的页面：

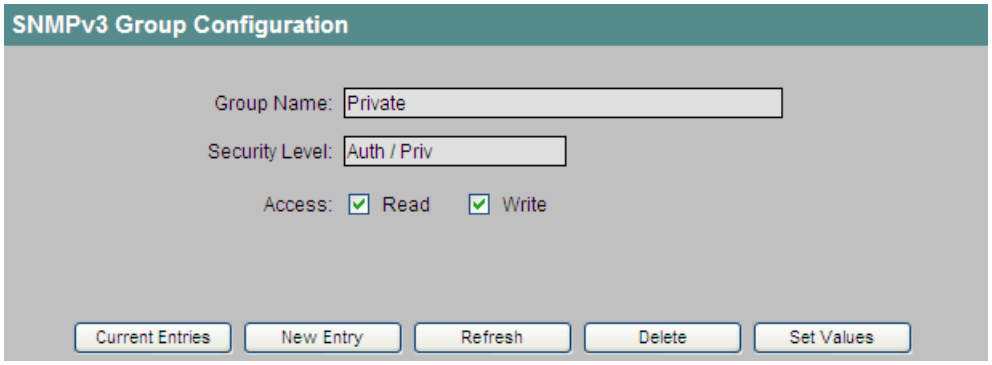


图 5-32　SNMPv3 组的组态

组名称 (Group Name)
组名称显示在该处。此文本框为只读，您只能在创建组时指定组名称，之后将无法修改。

安全等级 (Security Level)
此文本框显示是否应用身份验证和加密功能。可选择以下三种安全等级：

安全等级	特性	注释
无身份验证/无加密 (no Auth / no Priv)	无身份验证，无加密。	-
身份验证 (Auth)	使用 MD5 或 SHA 算法进行身份验证，无加密。	-
身份验证/加密 (Auth / Priv)	使用 MD5 或 SHA 算法进行身份验证，使用 DES3 算法进行加密。	-

读取 (Read) 和写入 (Write)
在此处，可以启用或禁用写入访问、读取访问和通知。

当前条目 (Current Entries)
单击此按钮可以返回到 SNMPv3 组列表。

新建条目 (New Entry)
单击此按钮后，将打开创建新组的页面。

删除 (Delete)
单击此按钮删除组。如果组内已有成员，则既不能删除该组，也不能更改该组的安全等级。

创建新组

单击“SNMPv3 组的组态”(SNMPv3 Group Configuration) 窗口中的 “新建条目”(New Entry) 按钮后，将打开创建新组的窗口：

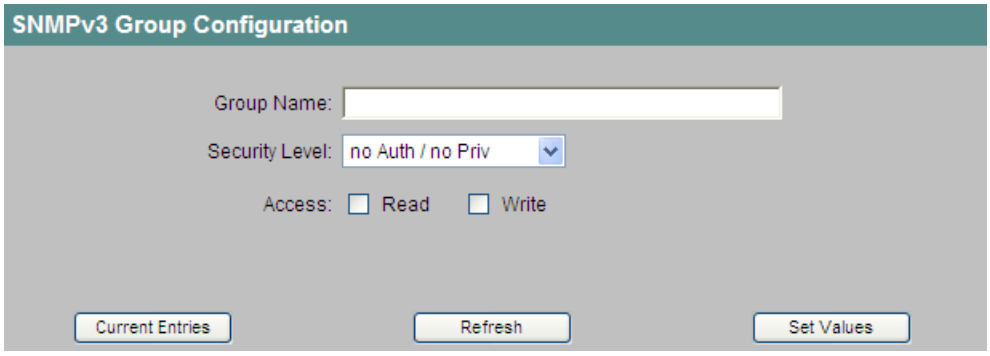


图 5-33　SNMPv3 组的组态 II

组名称 (Group Name)
在此处输入组的名称。此名称必须至少有两个字符，最大长度为 32 个字符。

安全等级 (Security Level)
在此处可选择应用于相应组的安全等级。

读 (Read) 和写 (Write)
此处可决定组内成员是否具有读取和/或写入权限。

命令行接口语法

表格 5-26　SNMPv3 组 - CLI\AGENT\SNMP\GROUP>

命令	说明	注释
info	显示所有 SNMPv3 组的列表。	-
add <组名称> [安全等级]	添加新 SNMPv3 组。通过以下参数指定安全等级： • NOAUTH 无身份验证，无加密。 • AUTH 使用 MD5 或 SHA 算法进行身份验证，无加密。 • PRIV 使用 MD5 或 SHA 算法进行身份验证，使用 DES3 算法进行加密。	仅限管理员。
access <组名称> <访问权限>	设置访问权限。 以下参数可用于设置读写权限： • - 既不允许写访问也不允许读访问。 • RO 仅允许读取访问。 • RW 允许读取和写入访问。	仅限管理员。
delete <组名称>	删除具有指定名称的 SNMPv3 组。	仅限管理员。
clearall	从列表中删除所有 SNMPv3 组。	仅限管理员。

5.4.3.4 SNMPv3 用户组态

用户特定的安全设置

基于用户的安全模型采用用户名的概念；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。 通过以下设置定义用户：

- 用户名：
  名称可随意选择。
- 安全名称：
  对应于身份验证协议的名称。
- 身份验证协议：
  身份验证协议的类型。
- 身份验证密钥：
  身份验证协议的私钥。
- 隐私协议：
  加密类型。
- 私钥：
  用于加密的私有密码。

此页面显示 SNMPv3 用户。 “用户名”(User Name) 列显示用户名， “组”(Group) 列显示用户所属组的名称：

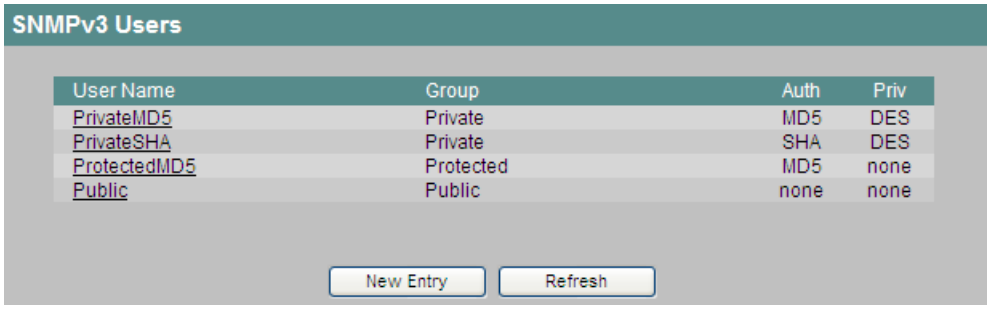


图 5-34 SNMPv3 用户

用户名 (User Name)
此处列有所有此前已定义的用户名。 单击某用户名时，将弹出一个新窗口，可在其中更改该用户的密码。

组 (Group)
此列中的条目显示各用户所属的组。

身份验证 (Auth)
此列显示用于相应用户的身份验证算法。

加密 (Priv)
此列显示用于相应用户的加密方法。

新建条目 (New Entry)
单击此按钮可新建用户。

SNMPv3 用户的组态

单击用户名时，将打开用户组态页面：

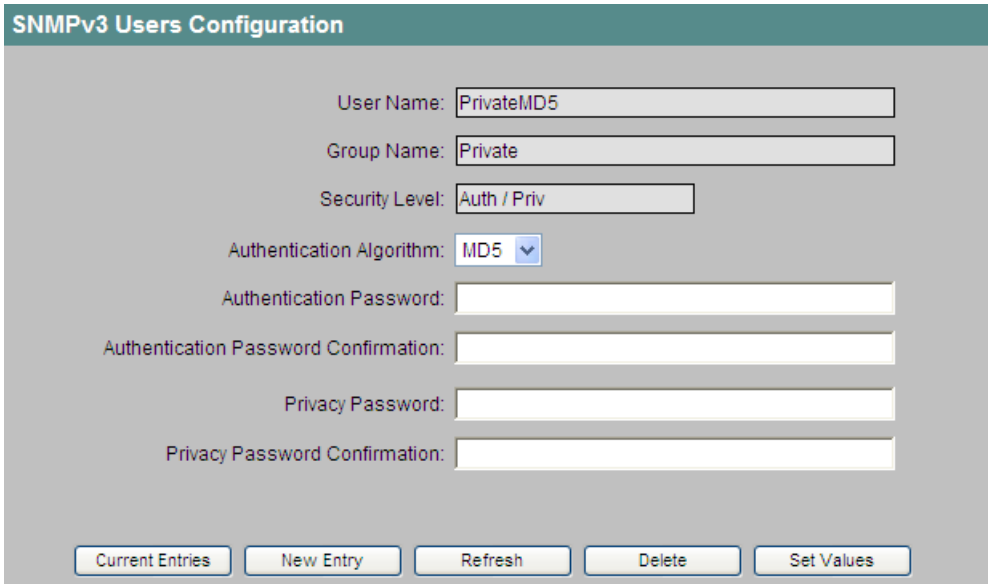


图 5-35　SNMPv3 用户组态

用户名 (User Name)
此处显示用户名。 此框为只读模式，因为用户名称一经创建便无法修改。

组名称 (Group Name)
此框显示用户所属的组。

如果所选的组有必要进行身份验证，请选择身份验证算法并输入身份验证密码。 如果还为该组选择了加密，请输入加密密码。

安全等级 (Security Level)
此框显示应用于该组的安全等级（身份验证、加密）。 第 70 页有各种安全等级的说明。

身份验证算法 (Authentication Algorithm)
您可以选择 MD5 算法或 SHA 算法。

身份验证密码 (Authentication password)/身份验证密码确认 (Authentication password confirmation)
在这些框中输入身份验证密码。 密码长度最多为 32 个字符。 可使用所有可用字符。

私有密码 (Privacy password)/私有密码确认 (Privacy password confirmation)
在这些框中输入加密密码。 密码长度最多为 32 个字符。

当前条目 (Current Entries)
单击此按钮可返回到 MAC SNMPv3 用户列表。

新建条目 (New Entry)
可通过单击“新建条目”(New Entry) 按钮，然后指定用户所属的组的名称来创建新用户。

删除 (Delete)
单击此按钮删除用户。

创建新用户

单击“SNMPv3 用户的组态”(SNMPv3 Users Configuration) 窗口中的“新建条目”(New Entry) 按钮后，将打开创建新用户的窗口：

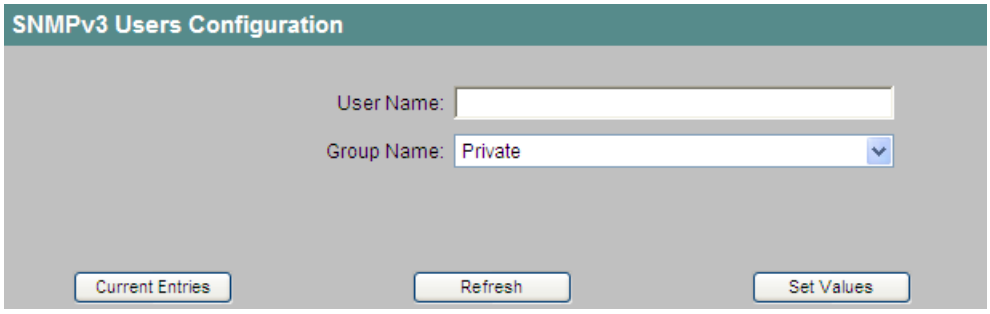


图 5-36 SNMPv3 用户组态 II

用户名 (User Name)
在此处输入新用户的名称。

组名称 (Group Name)
在此处选择新用户所属的组。

命令行接口语法

表格 5-27　SNMPv3 用户 - CLI\AGENT\SNMP\USER>

命令	说明	注释
info	显示所有 SNMPv3 用户的列表。	-
add <用户名> <组名称>	向组中添加 SNMPv3 用户。 如果该组有必要进行身份验证，则默认算法为 MD5	仅限管理员。
auth <用户名><MD5|SHA>	更改 SNMPv3 用户的身份验证算法（MD5 或 SHA）。 此命令仅可用于属于需要进行身份验证的组的成员。	仅限管理员。
pass <用户名><身份验证密码> [加密密码]	更改 SNMPv3 用户的密码（最大长度为 32 个字符）。 此命令仅可用于属于需要进行身份验证的组的成员。 加密密码只能在必要情况下指定。	仅限管理员。
delete <用户名>	删除具有指定名称的 SNMPv3 用户。	仅限管理员。
clearall	从列表中删除所有 SNMPv3 用户。	仅限管理员。

5.4.4 代理超时组态

设置超时

此处可以设置在 WBM 或 CLI 中自动注销前所需经过的时间。

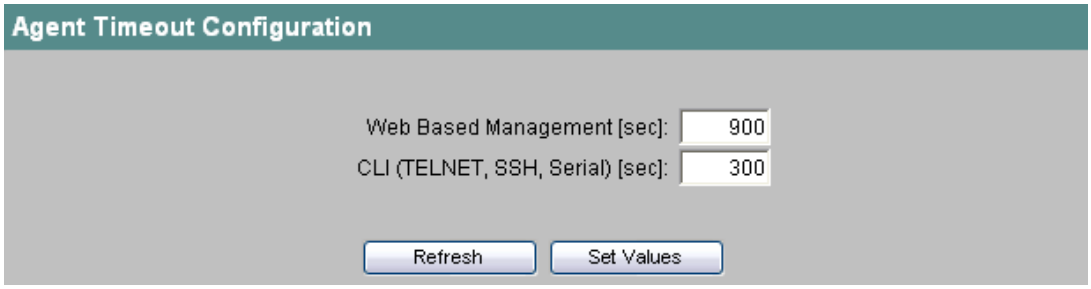


图 5-37 代理超时组态

基于 Web 的管理（秒）(Web Based Management (sec))
在此处指定 WBM 超时。
WBM 超时的允许范围： 60-3600（秒）

0 表示： 不会自动注销。

CLI（TELNET、SSH、串口）（秒）(CLI (TELNET, SSH, Serial) (sec))
在此处指定 CLI 超时。
CLI 超时的允许范围： 60-600 秒

0 表示： 不会自动注销。

命令行接口语法

表格 5-28 CLI\AGENT\TIMEOUT>

命令	说明	注释
info	显示当前超时设置。	-
wbmtime	设置 WBM 超时（单位：秒）。	仅限管理员。 默认值： 900
clitime	设置 CLI 超时（单位：秒）。	仅限管理员。 默认值：300

5.4.5 代理事件组态

工业以太网交换机的系统事件

在此页面中，可以指定工业以太网交换机对系统事件的响应方式。 通过启用相应的复选框，可以指定特定事件在工业以太网交换机上触发响应的方式。 可使用以下选项：

- 工业以太网交换机发送电子邮件。
- 工业以太网交换机触发 SNMP 陷阱。
- 工业以太网交换机在日志文件中写入一个条目。
- 工业以太网交换机向 Syslog 服务器写入一个条目。

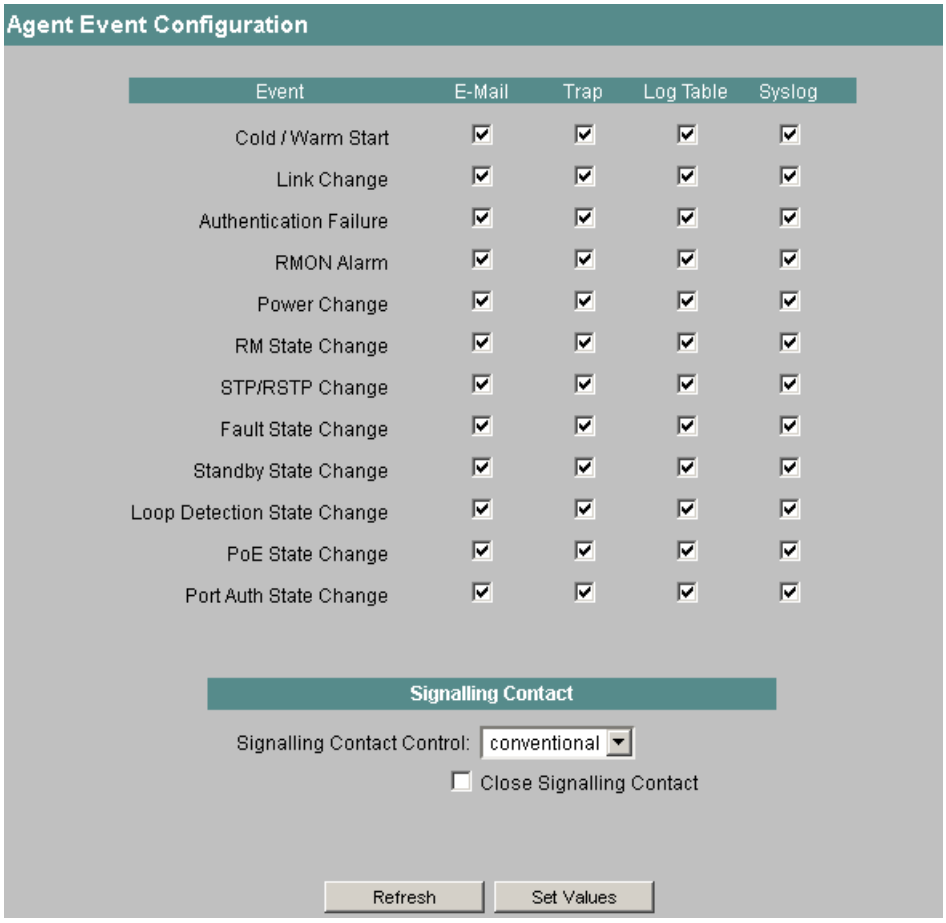


图 5-38 代理事件组态

可以组态工业以太网交换机对以下事件的响应方式：

冷/暖启动 (Cold/Warm Start)
用户打开或重启工业以太网交换机。

链路变化 (Link Change)
某端口故障，或之前故障的端口重新开始处理数据通信。

身份验证失败 (Authentication Failure)
通过 SNMP 访问时密码错误或访问权限不足。

RMON 报警 (RMON Alarm)
发生了与远程监视相关的报警或事件。

电源变化 (Power Change)
只有在电源线路 1 和 2 受到监视时才会发生此事件。 这表示线路 1 或线路 2 发生了变化。

RM 状态变化 (RM State Change)
冗余管理器检测到环网出现中断或重新建立的情况，并已相应地切换线路。 要使工业以太网交换机充当冗余管理器，需要对设备进行适当的组态（请参见"X-400 环网组态 (X-400 Ring Configuration) 菜单项"或"X-300 环网组态 (X-300 Ring Configuration) 菜单项"部分）。

备用状态变化 (Standby State Change)
已建立备用连接的设备（主设备或从设备）激活或禁用了与其它环网之间的链路（备用端口）。 数据通信将从一条以太网连接（主设备的备用端口）重新导向至其它以太网连接（从设备的备用端口）（请参见"X-400 备用屏蔽 (X-400 Standby Mask) 菜单项"或"X-300 备用屏蔽 (X-300 Standby Mask) 菜单项"部分）。

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。

STP/RSTP 变化 (STP/RSTP Change)
STP 或 RSTP 拓扑已发生变化；即已发生被动侦听事件。

环路检测状态变化 (Loop Detection State Change)
环路检测功能的状态已发生变化：

- 因检测到环路，设备已禁用端口。
- 环路消除后设备会再次启用端口。

VRRP 状态变化 (VRRP State Change)（仅限 SCALANCE X414）
虚拟路由器的状态发生变化。

PoE 状态变化 (PoE State Change)
PoE 状态已发生变化。

端口验证状态变化 (Port Auth State Change)
端口验证状态已发生变化。

光纤诊断
发生了与端口诊断相关的事件。

信号触点控制 (Signaling Contact Control)
可以通过该下拉列表指定信号触点的工作方式：

- **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。
- **调整 (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。

闭合信号触点 (Close Signaling Contact)
如果要闭合信号触点，请选中该复选框。

说明

仅当在“信号触点控制”(Signaling Contact Control) 下拉列表中选择了“调整”(aligned) 设置时，“闭合信号触点”(Close Signaling Contact) 复选框的设置才有效。

命令行接口语法

表格 5-29　代理事件组态 - CLI\AGENT\EVENT>

命令	说明	注释
info	显示当前的事件组态。	-

命令	说明	注释
setec [事件] <E|D> <E|D> <E|D> <E|D>	指定工业以太网交换机对系统事件的响应方式。 以下缩写可用于事件参数： • CW 冷/暖启动 • LC 链路变化 • AF 身份验证失败 • RA RMON 报警 • PC 电源变化 • RC RM 状态变化 • SC 备用状态变化 • FC 故障状态变化 • RS STP/RSTP 变化 • LD 环路检测状态变化 • PA	仅限管理员。

命令	说明	注释
	端口验证状态变化 • VE VRRP 状态变化 （仅限 X414） • FO 光纤诊断 如果已指定某类事件，则每次发生此类事件都将形成所组态的操作。 采用 <E> 或 <D> 形式的四个参数按以下顺序组态工业以太网交换机的响应方式： • 电子邮件 • 陷阱 • 日志表中的条目 • Syslog 服务器上的条目 示例： • setec LC E D D D 在链路变化时仅发送电子邮件。	
scontrol [C|A]	选择信号触点的工作方式： 传统 (conventional) 由 LED 显示错误/故障，并且信号触点断开。 调整 (aligned) 可根据要求断开或闭合信号触点，而不考虑故障/错误。	仅限管理员。
sclose [yes|no]	开闭信号触点： 是 (yes) 表示触点闭合。 否 (no) 表示触点断开	仅限管理员。

5.4.6 代理数字量输入组态 (SCALANCE X414-3E)

说明

数字量输入及其相关功能仅在 SCALANCE X414-3E 上可用。

数字量输入的应用示例

SCALANCE X414-3E 具有八点数字量输入，其用途十分多样：

- **示例 1，在没有 I/O 的过程控制中监视 OLM**
  假设您有一台不带中央 I/O 模块的 S7-400 控制器，I/O 通过 PROFIBUS OLM 的光学链路相连。 OLM 的信号触点适用于 SCALANCE X414-3E 的数字量输入，并可用于诊断。 如果将】现有 OLM 的信号触点用于 SCALANCE X414-3E 的数字量输入上，则可在不附加组件的情况下对 OLM 进行监视。
- **示例 2，门触点**
  某机柜的门触点与 SCALANCE X414-3E 的数字量输入相连。 通过对事件进行适当的组态，可以监视机柜内的所有干预情况。

变化事件和数字量输入

对于各个单独的数字量输入，可以指定在输入发生状态变化时（上升沿和下降沿均可）将触发哪个事件。 可使用以下选项：

- SCALANCE X414-3E 发送电子邮件。
- SCALANCE X414-3E 触发 SNMP 陷阱。
- SCALANCE X414-3E 在日志文件中写入一个条目。
- SCALANCE X414-3E 向 Syslog 服务器中写入一个条目。

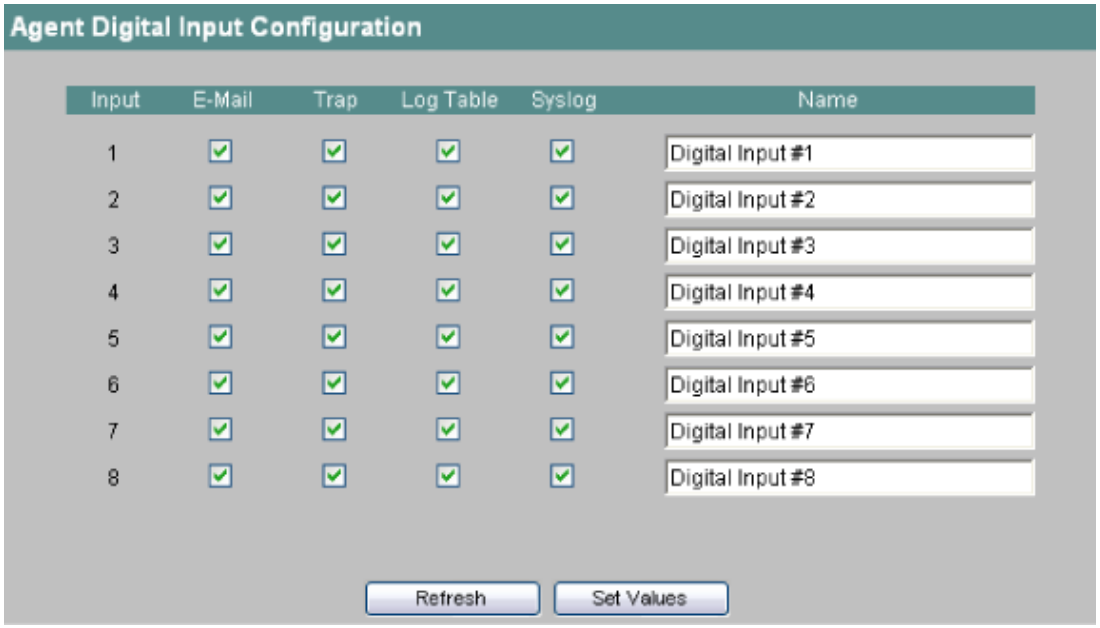


图 5-39　代理数字量输入组态

名称 (Name)
在此处，可以为每个数字量输入指定具有特定意义的名称。

命令行接口语法

表格 5-30　代理数字量输入组态 - CLI\AGENT\DIGIN>

命令	说明	注释
info	显示 SCALANCE X414-3E 数字量输入的状态。	-
showdic	显示 SCALANCE X414-3E 数字量输入的组态。	-
setdic [输入] <E|D> <E|D> <E|D> <E|D>	设置数字量输入的事件组态，其顺序为：电子邮件、陷阱、日志表条目、Syslog 服务器上的条目。如果未指定任何输入，则所指定的组态将应用于所有输入。 示例： • setdic 5 E D E D 如果输入 5 被置位，则 SCALANCE X414-3E 将发出一封电子邮件并在日志表中创建一个条目。 不会发送陷阱，也不会在 Syslog 服务器上添加新条目。	仅限管理员。
name <1 ... 8> <字符串>	为数字量输入指定符号名称。 此名称最长为 64 个字符。	仅限管理员。

5.4.7　代理电子邮件组态 (Agent E-Mail Configuration)

通过电子邮件进行网络监视

工业以太网交换机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、以简明语言描述的报警原因以及时间戳。 这样便可基于电子邮件系统使用很少的节点为网络建立集中式网络监视。 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。

只有在以下情况下，才会发送电子邮件

- 工业以太网交换机的电子邮件功能已激活，并且接收方的电子邮件地址已组态（请参见“代理组态菜单项”）。
- 已针对相关事件启用电子邮件功能（请参见“代理事件组态”(Agent Event Configuration) 菜单项）。
- 网络中存在工业以太网交换机可访问的 SMTP 服务器。
- 在工业以太网交换机中已输入 SMTP 服务器的 IP 地址。

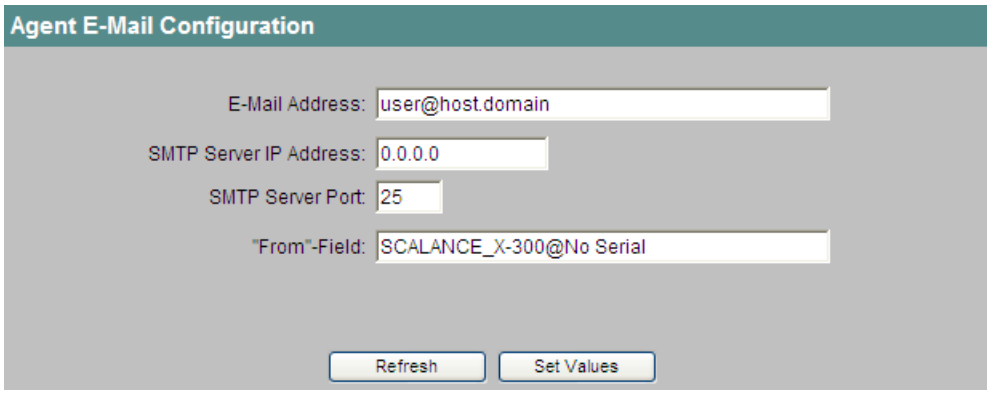


图 5-40　代理电子邮件组态 (Agent E-Mail Configuration)

电子邮件地址 (E-Mail Address)
在此处输入电子邮件地址，发生故障时工业以太网交换机将电子邮件发送到该地址。

SMTP 服务器 IP 地址 (SMTP Server IP Address)
在此处输入将用于发送电子邮件的 SMTP 服务器的 IP 地址。

SMTP 服务器端口 (SMTP Server Port)
发送邮件时使用的 IP 端口。 如有必要，可以将默认值 25 更改为适合您需要的值。

“发件人”字段 ("From" Field)
电子邮件发送方的地址。

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“发件人”(From) 框。 请与 SMTP 服务器的管理员联系。 您可以通过 WBM、CLI 或直接 SNMP 访问来设置“发件人”(From) 框。

命令行接口语法

表格 5-31　代理电子邮件组态 - CLI\AGENT\EMAIL>

命令	说明	注释
info	显示当前电子邮件组态。	-
server [<ip>[:port]]	指定 SMTP 服务器的 IP 地址和端口号。	仅限管理员。 默认值： 0.0.0.0:25
email <电子邮件地址>	指定工业以太网交换机将电子邮件发送到的地址。 该地址的长度最多为 50 个字符。	仅限管理员。 默认值： 禁用。 默认地址： user@host.domain
from [电子邮件地址]	指定工业以太网交换机发送的电子邮件的发送方。 该地址的长度最多为 50 个字符。	仅限管理员。

5.4.8　代理 Syslog 组态 (Agent Syslog Configuration)

应用

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。 这需要一个标准 Syslog 服务器。

只有在以下情况下，才会发送工作日志条目

- 工业以太网交换机上的 Syslog 功能已启用（请参见“代理组态”部分）
- 已针对相关事件启用 Syslog 功能（请参见“代理事件组态”(Agent Event Configuration) 菜单项）。

- 网络中存在可接收工业以太网交换机日志条目的 Syslog 服务器。（由于这是一个 UDP 连接，因此不会向工业以太网交换机发送确认）
- 在工业以太网交换机中已输入 Syslog 服务器的 IP 地址。

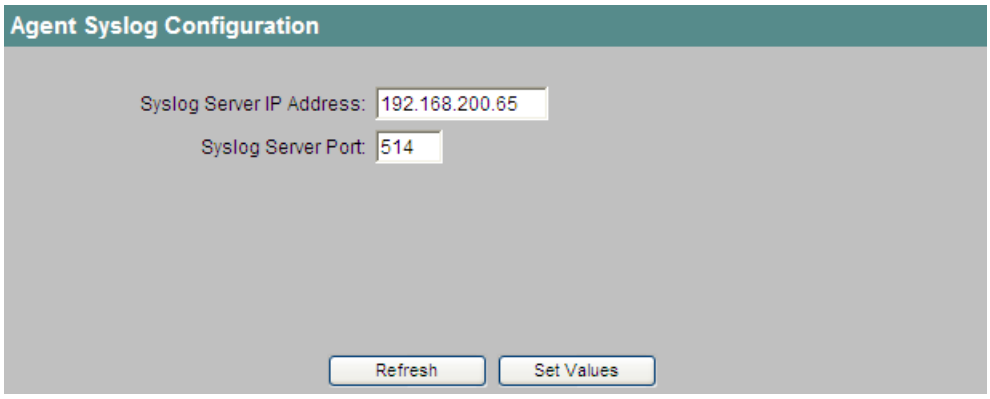


图 5-41　代理 Syslog 组态 (Agent Syslog Configuration)

Syslog 服务器 IP 地址 (Syslog Server IP Address)
在此处输入将存储日志条目的 Syslog 服务器的 IP 地址。

Syslog 服务器端口 (Syslog Server Port)
在服务器上存储日志条目时所使用的 UDP 端口。

命令行接口语法

表格 5-32　代理 Syslog 组态 - CLI\AGENT\SYSLOG>

命令	说明	注释
info	显示当前 Syslog 组态。	-
server [<ip>[:port]]	指定 Syslog 服务器的 IP 地址和端口号。	仅限管理员。 默认值： 0.0.0.0:514

5.4.9 代理 DHCP 组态 (Agent DHCP Configuration)

设置 DHCP 模式

在 DHCP 服务器的组态中，可使用以下几种方法识别 SCALANCE X-300 和 SCALANCE X408-2：

- 使用 MAC 地址
- 使用自由定义的客户机 ID
- 使用系统名称
- 使用 PROFINET IO 设备名称

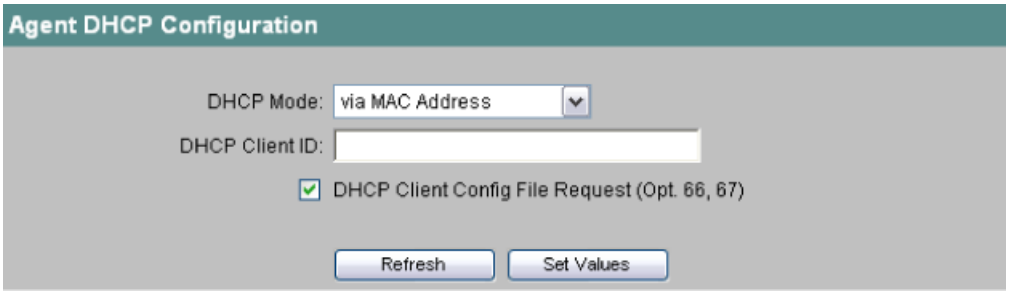


图 5-42 代理 DHCP 组态 (Agent DHCP Configuration)

DHCP 模式 (DHCP Mode)
在此处设置 DHCP 模式。

说明

如果在“代理组态”(Agent Configuration) 菜单项中未启用 DHCP，则无法选择任何模式，并显示文本“已禁用”(disabled)。

DHCP 客户机 ID (DHCP Client ID)
对于 DHCP 模式“通过客户机 ID”(via Client ID)，可在此处指定一个标识字符串，该字符串将分配给工业以太网交换机并由 DHCP 服务器评估。

DHCP 客户机组态文件请求（选项 66、67）(DHCP Client Config File Request (Op. 66, 67))
如果想要 DHCP 客户端使用选项 66 和 67 进行下载并随后启用某个组态文件，则选择此选项。

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“DHCP 客户机组态文件请求”(DHCP Client Config File Request)。

命令行接口语法

表格 5-33　代理 DHCP 组态 - CLI\AGENT\DHCPCONF>

命令	说明	注释
info	显示当前 DHCP 组态	-
dhcpmode [模式]	设置 DHCP 模式。可能的模式如下： • MAC MAC 地址 • CLID 客户机 ID • SYSN 设备名称 • DEVN PNIO 设备名称	仅限管理员。
clientid [客户机 ID]	指定 DHCP 客户机 ID。通过客户机 ID 设置 DHCP 时会使用该值。客户机 ID 可以自由定义。	仅限管理员。
cfgreq [E|D]	启用/禁用“组态文件请求（选项 66、67）”(Opt.66, 67)	仅限管理员。

5.4.10　时间组态

5.4.10.1　代理时间组态 (Agent Time Configuration)

网络中的时间同步

网络中的时间同步可使用以下协议：

- SNTP（简单网络时间协议）
- NTP（网络时间协议）
- SIMATIC 时间 (SIMATIC Time)
- PTP（精确时间协议）

在“代理时间组态”(Agent Time Configuration) 画面中进行常规设置。

SNTP 和 NTP 需要进一步设置，可通过菜单项“SNTP 客户端”(SNTP Client) 和“NTP 客户端”(NTP Client) 进行。

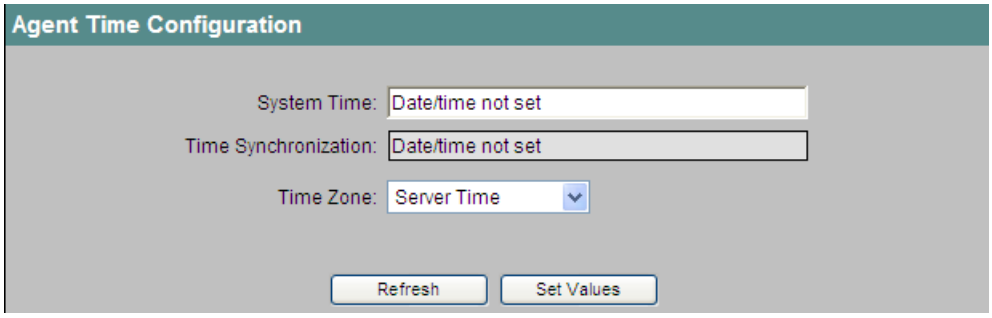


图 5-43　代理时间组态 (Agent Time Configuration)

系统时间 (System Time)

此框显示当前系统时间。
通过日期和时间后面的标识符，可了解系统时间的设置方式：

- (p)
  通过 SNTP 协议设置系统时间。
- (n)
  通过 NTP 协议设置系统时间。
- (i)
  通过 PTP 协议设置系统时间。
- (s)
  系统时间由 SIMATIC 时钟帧设置，并且与时间发送器同步。
- (t)
  系统时间由 SIMATIC 时钟帧设置，但不与时间发送器同步。
- (m)
  手动设置系统时间。
  也可以手动设置日期和时钟。 要求的输入格式如下： MM/DD/YYYY HH:MM:SS。

如果无法进行时钟同步，该框会显示“未设置日期/时间”(Date/time not set)。

时间同步

该框为只读框，显示上次进行时钟同步时的时间。

时区 (Time Zone)

在该框中，选择工业以太网交换机所在地点的时区，因为 SNTP 服务器始终发送 UTC 时间。该时间随后会被重新计算并根据时区显示为当地时间。 本工业以太网交换机没有标准/夏令时时间切换功能。

命令行接口语法

表格 5-34　代理时间组态 - CLI\AGENT\TIME>

命令	说明	注释
time [日期][时间]	显示或设置工业以太网交换机上的时间。 当显示日期和时间时，您还可以查看时间的设置时间和设置方式： • p 设置由 SNTP 进行。 • n 设置由 NTP 进行。 • i 设置由 PTP 进行。 • t 通过 SIMATIC 时间帧进行设置，但不与时间发送器同步。 • s 通过 SIMATIC 时间帧进行设置，并且它与时间发送器同步。 • m 设置是手动进行的。	仅限管理员。 输入格式： MM/DD/YYYY HH:MM:SS
timezone [-12 ... 13]	设置服务器与系统时间之间的时差（以小时为单位）。	仅限管理员。

5.4.10.2 SNTP 客户端组态

通过 SNTP 进行时钟同步

SNTP（Simple Network Time Protocol，简单网络时间协议）用于在网络中同步时间。 服务器在网络中发送相应的帧。 工业以太网交换机以该服务器的客户端身份登录，作为时间帧的接收方。

单击“SNTP 客户端”(SNTP Client) 子菜单，将显示“SNTP 客户端组态”(SNTP Client Configuration) 画面。

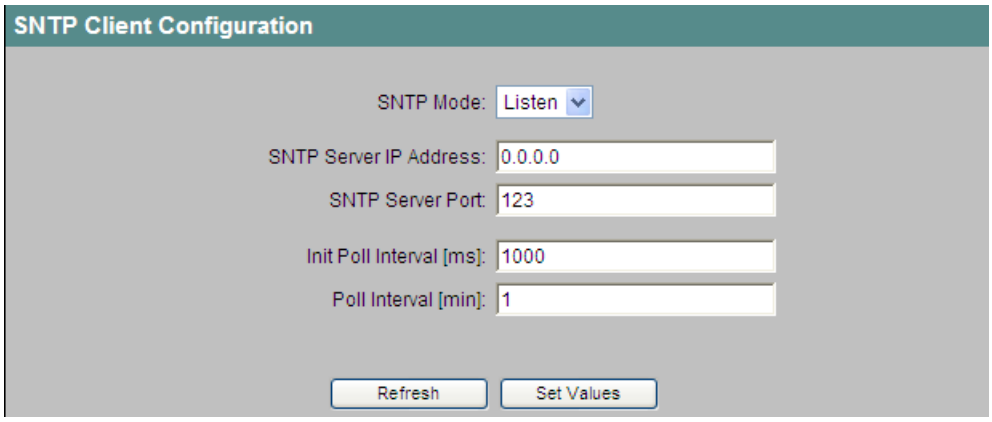


图 5-44　SNTP 客户端组态

SNTP 模式 (SNTP Mode)

可在以下协议类型中选择：

- 轮询 (Poll)
  如果选择此类协议，则需要设置 SNTP 服务器 IP 地址。
  可以修改以下设置：
  SNTP 服务器端口、初始轮询间隔、轮询间隔、时区偏移。
- 侦听 (Listen)
  如果选择此协议类型，除从服务器接收时间外，还可以选择时区偏移。

说明

时区偏移

时区偏移设置位于代理时间组态 (Agent Time Configuration) (页 138)菜单内。

SNTP 服务器 IP 地址 (SNTP Server IP Address)

输入 SNTP 服务器的 IP 地址，工业以太网交换机将使用该服务器发送的帧来同步时钟。

SNTP 服务器端口 (SNTP Server Port)

输入可用来访问 SNTP 服务器的端口。

初始轮询间隔 (Init poll interval)

输入一个时间间隔，如果工业以太网交换机对系统时间的第一次初始轮询没有成功，则以该间隔重复执行初始轮询。

轮询间隔 (Poll interval)

系统时间首次采用时间服务器的时间后，便会使用对时间服务器的新轮询进行定期更新。 指定系统时间的更新频率。

命令行接口语法

表格 5-35　SNTP 客户端组态 - CLI\AGENT\TIME\SNTP>

命令	说明	注释
server [<ip>[:port]]	设置 SNTP 服务器的 IP 地址和端口（可选）。	仅限管理员。
sntpmode [模式]	指定 SNTP 模式。 可能的模式如下： • 轮询 (POLL） 工业以太网交换机查询 SNTP 服务器上的时间 • 侦听 (LISTEN) 工业以太网交换机等待 SNTP 时钟帧	仅限管理员。
initint [1 ... 1000]	指定轮询间隔，范围从 1 到 10000 ms	仅限管理员。
Interval [1 ... 1440]	指定轮询间隔，范围从 1 到 1440 s	仅限管理员。

5.4.10.3　NTP 客户端组态

通过 NTP 进行时间同步

NTP（Network Time Protocol，网络时间协议）用于在网络中同步时间。工业以太网交换机作为时钟帧的接收方，以一台或多台服务器的客户端身份登录。NTP 服务器在网络中发送相应的帧。如果有多台服务器，NTP 会比较接收到的系统时间来决定质量最高的系统时间。

单击“NTP 客户端”(NTP Client) 子菜单，将显示“NTP 客户端组态”(NTP Client Configuration) 画面。

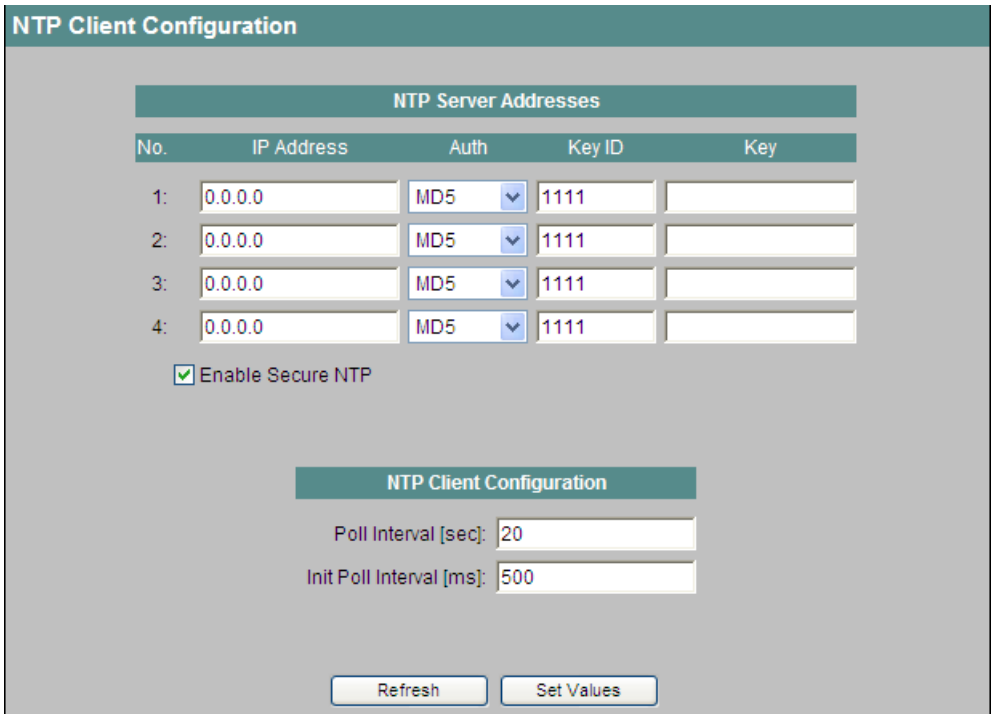


图 5-45　NTP 客户端组态

IP 地址 (IP Address)

输入 NTP 服务器的 IP 地址，客户端将向该服务器发送时钟同步帧。
可以指定最多四个不同的 NTP 服务器。

身份验证 (Auth)

选择帧的签名方式。
有两个选项：MD5 和 SHA。

密钥 ID (Key ID)

输入加密所使用的密钥 ID。密钥 ID 允许的值：1-65534。

密钥 (Key)

可输入最多包含 11 个字符的 ASCII 字符串作为密钥。WBM 或 CLI 均不支持十六进制数形式的输入。

启用安全 NTP (Enable Secure NTP)

启用此功能以发送加密帧。

轮询间隔 [s] (Poll Interval [sec])

输入客户端向时间服务器发送请求以更新系统时间的间隔。

初始轮询间隔 [ms] (Init Poll Interval [ms])

输入客户端首次连接到服务器后，向服务器查询系统时间之前经过的时间。

命令行接口语法

表格 5-36 NTP 客户端组态 - CLI\AGENT\TIME\NTP>

命令	说明	注释
server [<编号><IP>]	指定 NTP 服务器的服务器编号和 IP 地址。	仅限管理员。
initint [1 到 10000]	指定首次连接后查询系统时间之前经过的时间间隔。允许值：1 到 10000 ms。	仅限管理员。
interval [1 到 160]	指定用于查询和更新系统时间的间隔。 允许值：1 到 160 s。	仅限管理员。
secure <服务器编号><密钥 ID><MD5|SHA><密钥>	指定服务器编号、密钥 ID、算法和密钥以确保帧的传送安全。	仅限管理员。
security [E|D]	启用/禁用 NTP 安全。	仅限管理员。

5.4.10.4 夏令时 (Daylight Saving Time)

夏令时表 (Daylight Saving Time Table)

说明

只有 SCALANCE X-300 和 SCALANCE X408 设备具有该功能，SCALANCE X414 不具有该功能。

可在此页面控制夏令时切换，以便设置当地时区正确的系统时间。

可定义夏令时切换规则，也可指定固定日期。

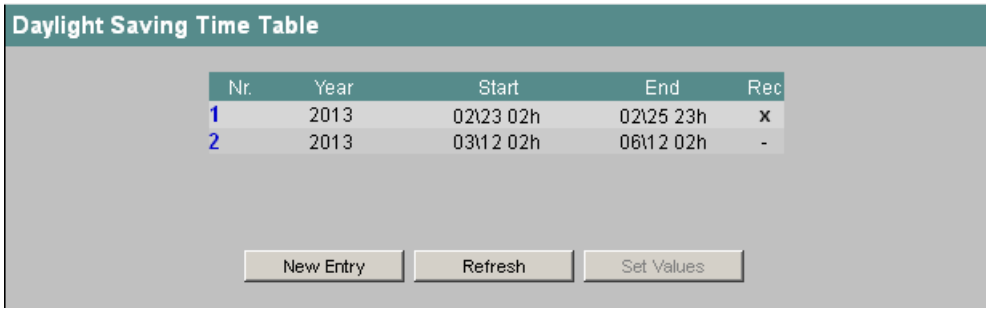


图 5-46　夏令时表 (Daylight Saving Time Table)

该表显示了夏令时切换的现有条目的概览。
如果已定义规则，则在超出条目的结束日期时将显示下一切换的数据。对于固定的条目，将删除该行。

编号 (Nr.)

显示条目编号。
如果创建新条目，则会创建具有唯一编号的新行。

年 (Year)

显示条目的创建年份。

起始 (Start)

显示夏令时的起始月、日和时间。

结束 (End)

显示夏令时的结束月、日和时间。

Rec

显示是否已定义夏令时切换规则：

- x
  已定义夏令时切换规则。
- -
  已输入夏令时切换的固定日期。

夏令时表新条目

在“夏令时表”(Daylight Saving Time Table) 页面上单击“新建条目”(New Entry) 按钮。

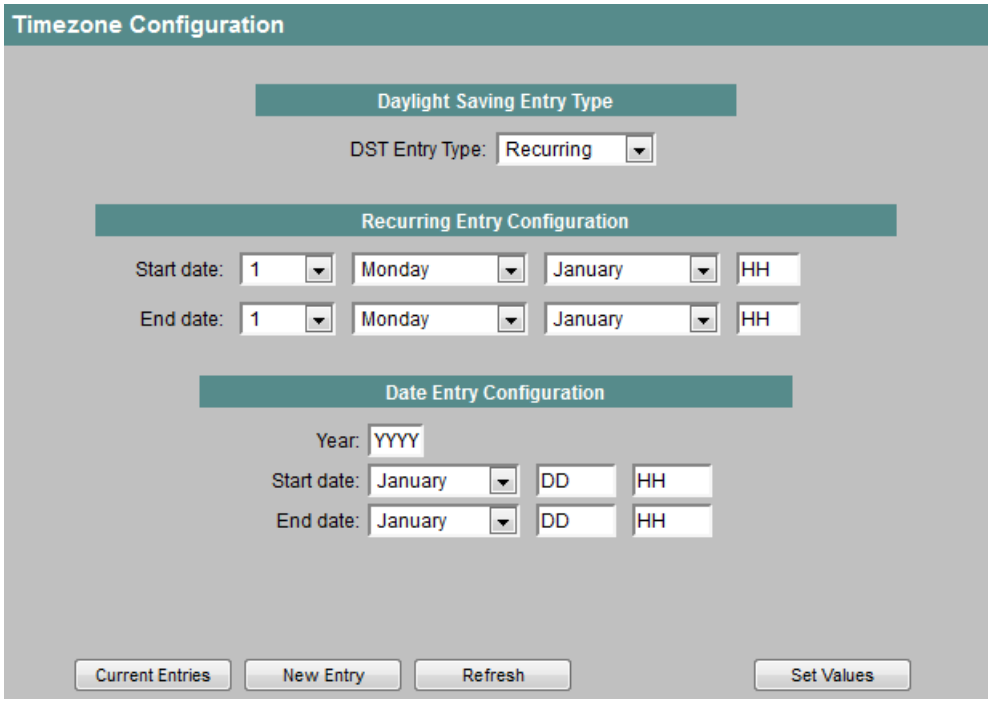
设置夏令时条目类型

指定如何进行夏令时切换。

DST 条目类型

从下拉列表中选择下列两个条目之一：

- **重复 (Recurring)**
  可定义夏令时切换规则。
  此设置适用于夏令时始终在特定工作日开始或结束的地区。
- **日期 (Date)**
  可定义夏令时切换的固定日期。
  此设置适用于没有任何管理夏令时切换的规则的地区。



“重复条目组态”(Recurring Entry Configuration) 的设置

已创建夏令时切换规则

起始日期 (Start date)

输入夏令时的以下起始值：

- 月中的某一周
  可以选择月中的第 1 周到第 5 周或最后一周。
- 工作日
- 月
- 日时钟（单位为小时）

结束日期 (End date)

输入夏令时的以下结束值：

- 月中的某一周
  可以选择月中的第 1 周到第 5 周或最后一周。
- 工作日
- 月
- 日时钟（单位为小时）

所选“日期条目组态”(Date Entry Configuration) 的设置

可设置夏令时开始和结束的固定日期。

年 (Year)

输入夏令时切换的年份。

起始日期 (Start date)

输入夏令时的以下起始值：

- 月
- 日
- 日时钟（单位为小时）

结束日期 (End date)

输入夏令时的以下结束值：

- 月
- 日
- 日时钟（单位为小时）

命令行接口语法

表格 5-37　夏令时表 - CLI\AGENT\TIME\DST>

命令	说明	注释
info	显示时区和夏令时切换的相关信息。	
recurring <起始日期> <结束日期>	创建一个“重复”类型的条目。 您需要为 <起始日期> 和 <结束日期> 输入以下信息： • 1-5 或 Last • 工作日 • 月 • 小时	仅限管理员 示例： recurring last sunday march 02 last sunday october 03
date <yyyy> <起始日期> <结束日期>	创建一个“日期”类型的条目。 对于 <起始日期> 和 <结束日期> 参数，输入以下形式的月、日和小时： • mmddhh	仅限管理员 示例： date 2010 040102 100103
delete <索引>	删除条目。必须使用“info”命令获得要删除的条目的索引。	仅限管理员

5.4.11　代理 PNIO 组态 (Agent PNIO Configuration)

PROFINET IO 的设置

此处的 PROFINET IO 设备名称是在使用 NCM 进行 PROFINET IO 硬件配置时为工业以太网交换机分配的。

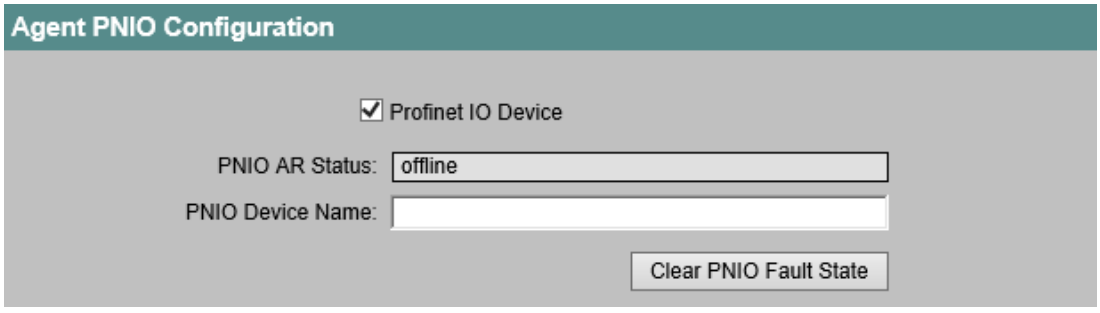


图 5-47　代理 PROFINET IO 组态

PROFINET IO 设备 (PROFINET IO Device)
如果选中该复选框，则会启用 PROFINET IO 设备功能。更改此设置后，交换机将自动重启。

PNIO AR 状态 (PNIO AR Status)
该框显示 PROFINET IO 应用关系状态；换句话说，工业以太网交换机与 PROFINET 控制器之间的连接状态是“在线”(online) 还是“离线”(offline)。

在这种情况下，“在线”(online) 是指存在与 PROFINET IO 控制器的连接，即控制器已将其组态数据下载到工业以太网交换机中，并且工业以太网交换机可以向 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，无法在工业以太网交换机上对 PROFINET IO 控制器的参数集进行组态。

PNIO 设备名称 (PNIO Device Name)
此处可根据 HW Config 中的组态输入 PROFINET IO 设备名称（站名称）。

清除 PNIO 故障状态 (Clear PNIO Fault State)
如果工业以太网交换机集成在 PROFINET IO 环境（含控制器）中，然后从 PROFINET IO 模式中将其移除，则故障 LED 会发出信号指示控制器丢失。可以使用此按钮清除该故障显示。

命令行接口语法

表格 5-38　代理 PROFINET IO 组态 - CLI\AGENT\PNIOCONF>

命令	说明	注释
info	显示当前 PROFINET IO 组态	-
devname [字符串]	设置 PROFINET IO 设备名称。	仅限管理员。
clear	清除 PROFINET IO 故障状态（如果存在）	仅限管理员。
pnio [E|D]	启用/禁用 PROFINET IO 设备功能。更改此设置后，交换机将自动重启。	仅限管理员。

5.4.12 管理访问控制列表

管理访问控制列表 - 总览

在此页面上，可以提高工业以太网交换机的安全性。 要指定哪台主机可以使用哪个 IP 地址访问您的工业以太网交换机管理功能，可为各个主机、子网或所有主机组态访问规则。

访问规则列表清晰地指出了该信息，如下图的示例所示：

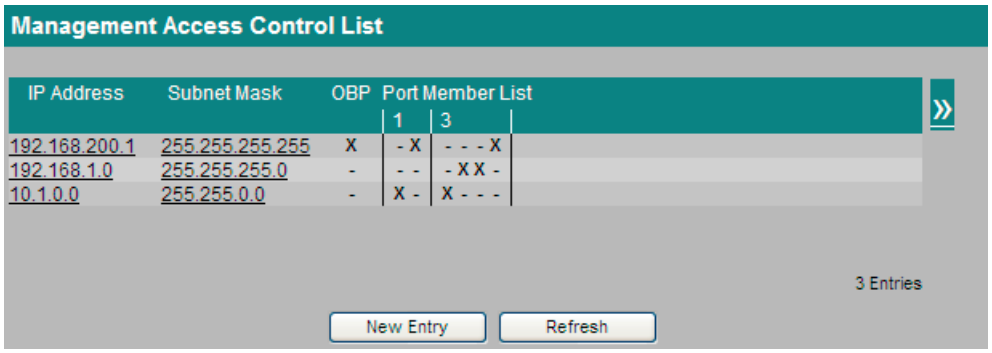


图 5-48 管理访问控制列表 - 总览

说明

选项“启用带外端口”(Out-Band Port Enabled) (OBP) 仅适用于 SCALANCE X414。

切换页面

单击“>>”和“<<”按钮可向后或向前翻页。 在第二页，您将看到已建立的所有链路汇聚，而不是端口。

访问规则

只要定义了访问规则，所有未在此规则中定义的其它访问选项最初都会被阻止。 如果想要允许其它主机或服务访问，则需要另外定义访问规则。

可以定义如下访问规则：

- 访问某个主机：
  使用一个主机 IP 地址和子网掩码 255.255.255.255。
- 访问所定义子网的全部主机：
  使用 IP 地址和子网掩码的有效组合。
- 访问所有主机：
  在 IP 地址和子网掩码下输入 0.0.0.0。

如果存在多个匹配的主机访问规则，则会应用限定更严格的“最佳匹配”规则。 例如，如果单个主机访问规则和整个子网的访问规则均适用，则会使用主机规则。

管理 ACL 组态

可以设置哪台主机可以通过哪个端口和使用哪种服务访问工业以太网交换机。

说明

注意： 错误的组态可能意味着无法再对设备进行访问。因此应组态一个访问规则，以便在代理组态 (页 102)页面上启用该功能前可对管理功能进行访问。

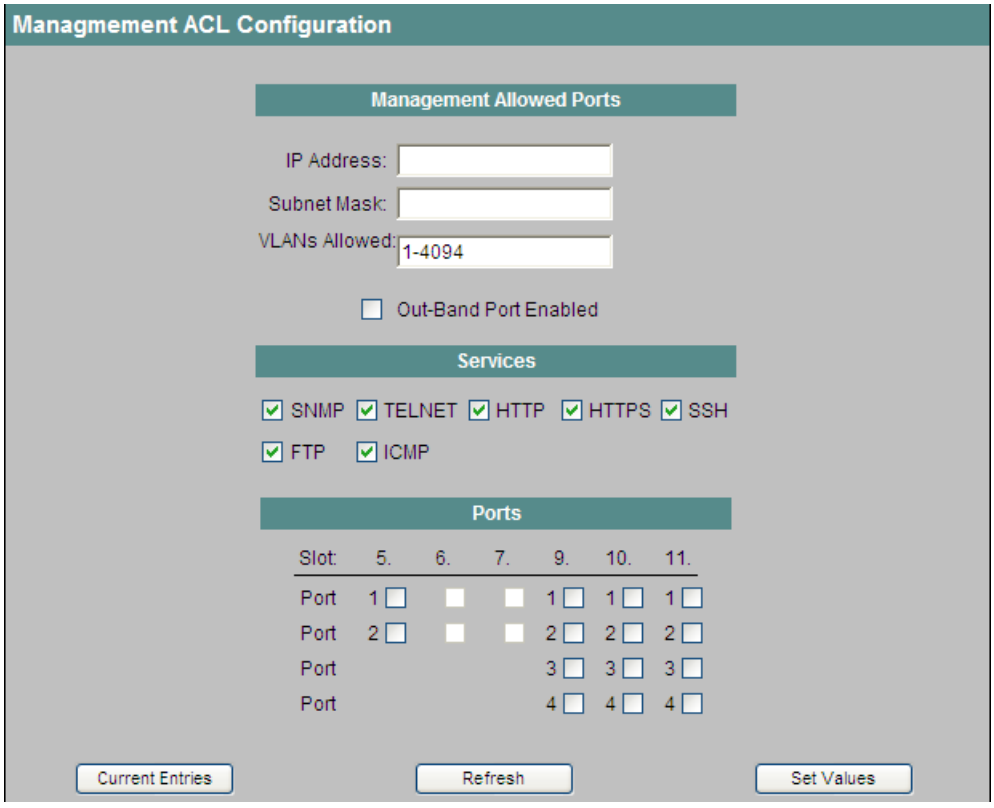


图 5-49 管理 ACL 组态 (SCALANCE X-400)

管理允许端口

IP 地址 (IP Address)

输入要应用规则的 IP 地址。
如果使用 IP 地址 0.0.0.0，则规则设置应用于所有 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。

允许的 VLAN (VLANs Allowed)

输入 VLAN 编号，允许来自该 VLAN 的访问。
可以输入多个 VLAN 以及 VLAN 范围，用逗号分隔，例如 1,5,10-12。

启用带外端口 (Out-Band Port Enabled)

如果启用“启用带外端口”(Out-Band Port Enabled) 选项，则 IP 地址可通过带外端口访问交换机。

服务

如果启用以下一种服务，则还允许使用此服务访问：

- SNMP
- TELNET
- HTTP
- HTTPS
- SSH
- FTP
- ICMP

以下服务只适用于 SCALANCE X300：

- DHCP 中继
  如果启用此服务，DHCP 中继将充当终端设备与不同网络中 DHCP 服务器之间的中介，从而可为终端设备分配 IP 地址。

  说明
  有关此功能的详细信息，请参见“DHCP 中继代理组态”和“DHCP 中继代理端口组态”部分。

端口 (Ports)

启用用于访问设备的端口。

创建新条目

请按照以下步骤创建新条目：

1. 单击“管理访问控制列表”(Management Access Control List) 页面上的“新建条目”(New Entry) 按钮。
   将出现“管理 ACL 组态”(Management ACL Configuration) 页面。
2. 在第一个输入框中输入路径成本计算。
3. 在第二个输入框中输入子网掩码。
4. 在第三个输入框中输入具体 VLAN 或 VLAN 范围。

5. 仅适用于 X414：
   如果希望 IP 地址通过带外端口访问交换机，则启用“启用带外端口”(Out-Band Port Enabled) 选项。
6. 启用所需的端口。
7. 启用所需的服务。
8. 请单击“设置值”(Set Values) 按钮将更改的信息传送到设备。
9. 单击“当前条目”(Current Entries) 按钮返回“管理访问控制列表”总览。

编辑现有条目

请按照以下步骤修改现有条目：

1. 在“管理访问控制列表”(Management Access Control List) 页面上单击要修改条目的 IP 地址。
2. 进行所需修改。
   “IP 地址”(IP Address) 和“子网掩码”(Subnet Mask) 框中的条目是只读条目。
3. 请单击“设置值”(Set Values) 按钮将更改的信息传送到设备。
4. 单击“当前条目”(Current Entries) 按钮返回“管理访问控制列表”总览。

删除条目

请按照以下步骤删除现有条目：

1. 在“管理访问控制列表”(Management Access Control List) 页面上单击要删除条目的 IP 地址。
   将出现“管理 ACL 组态”(Management ACL Configuration) 页面。
2. 单击“删除”(Delete) 按钮。
   将删除该条目。

命令行接口语法

表格 5-39 **管理访问控制列表 - CLI\AGENT\MGMNTACL\>**

命令	说明	注释
info	显示管理访问控制列表的当前设置。	
add <IP> <子网>	在管理访问控制列表中创建新条目。	仅限管理员。
ports <IP> <子网> <E|D> [端口]	指定可用来访问设备的端口。	仅限管理员。
outband <IP> <子网> <E|D>	仅适用于 X414： 指定 IP 地址是否可以通过带外端口访问交换机。	仅限管理员。

命令	说明	注释
vlans <IP> <子网> [1-4094]	对应于设备所在 VLAN 的编号。 指定只有相同 VLAN 中的主机才能访问该设备。	仅限管理员。
services <IP> <子网> <E|D> [服务...]	指定可用于访问该设备的协议。	仅限管理员。
delete <IP> <子网>	从管理访问控制列表中删除条目。	仅限管理员。

参见

用 DHCP 客户机分配地址 (页 39)

5.5 “交换机”(Switch) 菜单

简介

在此菜单中，可以为工业以太网交换机的交换机功能（将其分配给第 2 层）设置参数。 其中包括以下功能：

- 常规交换机设置，如镜像、老化和流量控制。
- 单播、组播和广播帧的过滤表。
- 通过 IGMP/GMRP 管理组播组。
- 使用生成树协议。
- 通过 GVRP 帧组态 VLAN 及其动态组态。
- 通过“CoS 到队列映射”以及“DSCP 到队列映射”指定传送优先级。
- DCP 端口过滤
- 通过 LLDP 进行拓扑诊断
- 通过 DHCP 中继实现 IP 地址初始化
- 回路检测
- 1:1 NAT
- 统计每个端口的帧数

5.5.1 交换机组态 (Switch Configuration)

协议设置和交换机功能

如果单击“交换机”(Switch) 文件夹图标，将显示“交换机组态”(Switch Configuration) 画面。在此画面中，可以指定启用工业以太网交换机上的哪个功能以及使用哪些协议管理数据通信。

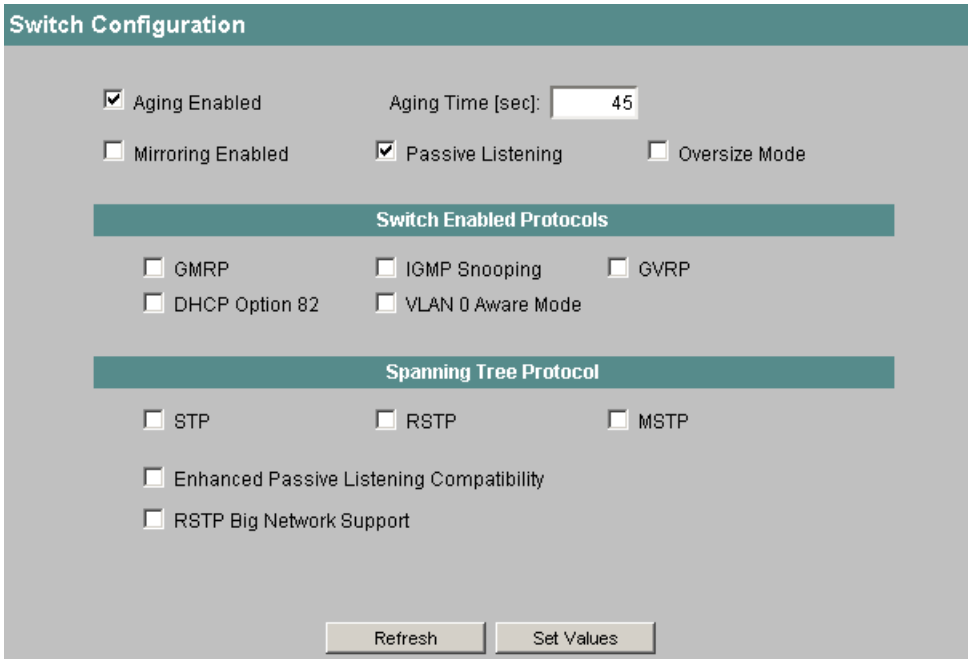


图 5-50 交换机组态 (Switch Configuration)

镜像和老化

在画面的上半部分，可以启用或禁用工业以太网交换机的以下功能：

启用老化 (Aging Enabled)

工业以太网交换机可自动识别与其连接的节点的源地址。在工业以太网交换机中，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。

如果工业以太网交换机在特定时间内未收到源地址与学习的地址相匹配的帧，则交换机会删除学习的地址。这种机制称为老化。老化可以防止将帧错误转发，例如在某个终端设备（如编程设备）连接到不同交换机端口时。

如果激活“启用老化”(Aging Enabled)，工业以太网交换机会在所选时间（老化时间）过后自动删除学习的地址。

老化时间 [秒] (Aging Time [sec])

输入一个时间，如果工业以太网交换机在此时间内未接收到包含相应发送方地址的帧，则会删除该地址。

在 SCALANCE X408-2 中，老化时间的默认值为 30 s。老化时间可设置为 15 到 3825 秒之间的值（步长为 15 s）。

在 SCALANCE X414-3E 中，老化时间的默认值为 40 s。可根据需要将老化时间设置为 10 到 1000000 秒之间的值。

启用镜像 (Mirroring Enabled)

镜像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）。

如果选中“启用镜像”(Mirroring Enabled)，则可将一个或多个端口镜像到监视端口。

被动侦听 (Passive Listening)

如果启用“被动侦听”(Passive Listening)，工业以太网交换机不在 (R)STP 模式下也可以对重新组态做出响应。接收到 RSTP 拓扑变更帧后，则删除 MAC 地址表。并且会转发生成树 BPDU。

说明

在被动侦听模式下，工业以太网交换机与 IEEE 802.1d 不兼容，因为当不在 (R)STP 模式下时，IEEE 802.1d 禁止转发生成树 BPDU。

说明

如果在作为冗余环网节点的交换机上激活 (R)STP 功能，则没有任何生成树 BPDU 会通过环网端口转发。启用被动侦听功能时这同样适用。

在这种情况下，必须不存在通过冗余环网链接的 (R)STP 网段，否则将会导致形成环路。

超长模式 (Oversize Mode)

如果启用“超长模式”(Oversize Mode)，则允许接收允许接收大于 1,522 字节（最大 1,632 字节）的帧。

说明

PRP 网络中的超长帧

在 PRP 网络中使用 SCALANCE X-300 或 X-400 工业以太网交换机时，请启用“超长模式”(Oversize Mode) 选项。

在 PRP 网络中，可能存在长度达 1528 个字节的超长帧。如果启用“超长模式”(Oversize Mode) 选项，将会转发超长帧。

交换机启用的协议

在画面的中心区域，可以启用或禁用以下数据通信管理协议：

GMRP

GMRP 是 GARP 组播注册协议的缩写。GARP 本身代表通用属性注册协议。GMRP 是一种用于高效转发组播帧的机制。

利用 GARP 信息声明 (GID)，节点可以将工业以太网交换机作为组播地址的接收方进行注册。工业以太网交换机会将此注册信息以 GARP 信息传播 (GIP) 帧的形式发送到其端口。之后，其它交换机也会获知该地址，并且它们会将有关该地址的组播帧只发送到已接收到该地址注册信息的端口。这可降低整个网络中由组播帧产生的负载以及没有为组播注册的节点的负载。

如果启用 GMRP，则会自动生成 GMRP 注册信息并在组播过滤表中为所有端口输入该信息。

如果未启用 GMRP

- 工业以太网交换机不会评估收到的 GMRP 帧。
- 工业以太网交换机不会发送其本身的 GMRP 帧。

IGMP 监听

IGMP 是 Internet 组管理协议的缩写。该协议是 IP 协议的增强，允许将 IP 地址分配给组播组。

工业以太网交换机会评估来自组播接收方的 IGMP 数据包，并将获得的信息存储在其组播过滤表中。由 IGMP 组态产生的过滤条目会在过滤表中相应指示。

如果启用“IGMP 监听”(IGMP snooping)，IGMP 条目将包括在过滤表中，并且 IGMP 数据包会被相应转发。

支持 IGMPv1、IGMPv2 和 IGMPv3。

说明

GMRP 和 IGMP 不能同时起作用。

GVRP

GVRP 是 GARP VLAN 注册协议的缩写。

如果启用 GVRP，可以使用 GVRP 动态设置端口所属的 VLAN。

说明

GMRP 和 IGMP 不能同时起作用。

DHCP 选项 82 (DHCP Option 82)

如果启用“DHCP 选项 82”(DHCP option 82)，则在工业以太网交换机将 DHCP 查询转发到 DHCP 服务器前，会将 “选项 82”(Option 82) 字段添加到该查询中（假定收到的查询有这样一个字段）。“Option 82”字段包含有关网络中新客户机定位的信息。

根据工业以太网交换机的设备标识符，可以设置 IP 地址或 MAC 地址。在“DHCP 中继代理组态”(DHCP Relay Agent Configuration) 菜单项中，可以组态设备标识符和一台或多台 DHCP 服务器的地址。

VLAN 0 感知模式 (VLAN 0 Aware Mode)（仅适用于 SCALANCE X-300）

如果启用“VLAN 0 感知模式”(VLAN 0 Aware mode)，将修改或删除 VLAN-ID 为 0 的帧的 VLAN 标记。

该设置仅影响作为 VLAN-ID 1 中无标记成员的端口。

如果启用“VLAN 0 感知模式”(VLAN 0 Aware mode)，则无法创建任何 VLAN 组态。要更改端口的 VLAN-ID，则需要禁用此选项。

生成树协议 (Spanning Tree Protocol)

在画面的下半部分，可以启用或禁用以下冗余方法：

STP

STP（Spanning Tree Protocol，生成树协议）是一种防止在冗余网络结构中形成环路的方法。

启用 STP 即表示启用生成树功能。

生成树的典型重新组态时间介于 20 到 30 秒之间。

RSTP

RSTP（Rapid Spanning Tree Protocol，快速生成树协议）是生成树协议的进一步发展。RSTP 的目标是实现更快的重新组态时间（数秒）。

启用 RSTP 即表示启用快速生成树功能。

如果在某个端口上检测到生成树帧，该端口将从 RSTP 恢复为 STP。

MSTP（仅适用于 SCALANCE X-300 和 SCALANCE X408）

MSTP（Multiple Spanning Tree Protocol，多重生成树协议）是快速生成树协议的进一步发展。MSTP 的目标是对同一工业以太网交换机上的不同 VLAN 内运行各自的 RSTP 实例。

启用 MSTP 即表示启用多重生成树功能。

说明

如果启用了被动侦听，即使对工业以太网交换机禁用 (R/M)STP，工业以太网交换机也将以透明方式转发 (R/M)STP 组态帧。如果识别出拓扑变更帧，则会在一段有限时间内减少老化时间，从而更快地更新节点列表。

经过这段时间后，将重新应用原始老化时间。

增强的被动侦听兼容性 (Enhanced Passive Listening Compatibility)

如果启用“增强的被动侦听兼容性”(Enhanced Passive Listening Compatibility)，边缘端口转至接通时，也会发送 TCN（Topology Change Notifications，拓扑变更通知）帧。否则，即使在边缘端口存在接通链路，也不会发送 TCN 帧。要将 (R)STP 网络与 HRP 环网连接起来，必须将此参数与“自动边缘端口”功能结合在一起（生成树端口参数 (Spanning Tree Port Parameters) (页 229)部分）。否则，不会通过边缘端口发送 TCN 帧；但这对于环网节点上的被动侦听功能来说是必要的（请参见相关交换机的操作说明）。

RSTP 大网络支持 (RSTP Big Network Support)

如果启用“RSTP 大网络支持”(RSTP Big Network Support)，则可支持包含最多 80 个网桥的大型 RSTP 环网。

命令行接口语法

表格 5-40　交换机组态 - CLI\SWITCH>

命令	说明	注释
info	显示“交换机”(Switch) 菜单中的当前设置。	-
aging [E|D]	启用/禁用老化功能。	仅限管理员 默认值：启用
agetime [秒]	指定老化时间（以秒为单位）。	仅限管理员 默认值为 30 秒（适用于 SCALANCE X408-2） 或 40 秒（适用于 SCALANCE X414-3E）。
mirror [E|D]	启用/禁用端口镜像。	仅限管理员
plisten [E|D]	启用/禁用被动侦听。	仅限管理员
超长 [E|D]	启用/禁用超长模式功能。	仅限管理员

命令	说明	注释
gmrp [E|D]	对所有工业以太网交换机端口启用/禁用 GMRP 功能。	仅限管理员
igmp [E|D]	对所有工业以太网交换机端口启用/禁用 IGMP 功能。	仅限管理员
gvrp [E|D]	对所有工业以太网交换机端口启用/禁用 GVRP 功能。	仅限管理员
opt82 [E|D]	启用/禁用 DHCP 选项 82。	仅限管理员
vlan0 [E|D]	启用/禁用 VLAN 0 感知模式。	仅限管理员
rstp [D|S|R|M]	对所有工业以太网交换机端口启用/禁用快速生成树功能。 参数的含义如下： • D 禁用 STP/RSTP • S 启用 STP • R 启用 RSTP • M 启用 MSTP	仅限管理员
eplc [E|D]	启用/禁用增强的被动侦听兼容性。	仅限管理员
bnsupp[E|D]	启用/禁用大网络支持。	仅限管理员
macl [E|D]	启用/禁用管理 ACL 功能	仅限管理员
blkucast [<E|D> [端口]]	显示/设置未知单播屏蔽掩码。	仅限管理员
blkmcast [<E|D> [端口]]	显示/设置未知组播屏蔽掩码。	仅限管理员
blkbcast [<E|D> [端口]]	显示/设置广播屏蔽掩码。	仅限管理员
fastlrn [<E|D> [端口]]	显示/设置快速识别组态。	仅限管理员

5.5.2 端口状态 (Port status)

端口组态概述

如果单击“端口”(Ports) 文件夹图标，将显示“端口状态”(Port Status) 画面。

该画面将显示工业以太网交换机所有端口（如果适用，还包括扩展端口）的数据传输组态。

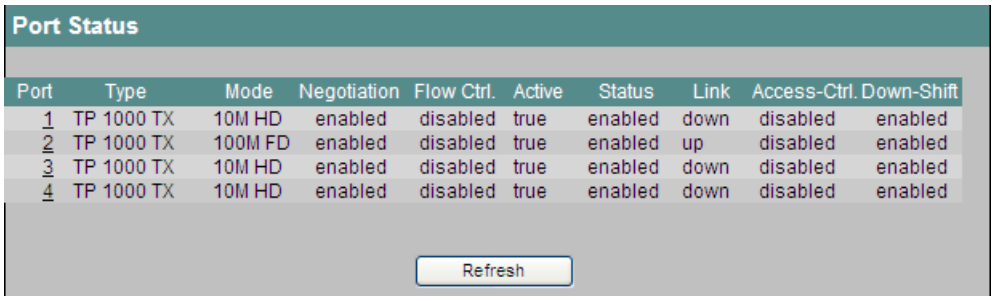


图 5-51　端口状态 (Port status)

该表的八个列显示了以下信息：

端口 (Port)
该列显示后面信息所涉及的插槽和端口。

类型 (Type)
显示端口类型。此信息非常重要，因为在某些插槽中可以使用不同的模块，相应地使用不同的端口。可能的端口类型如下：

- TP 100 TX
- FO 100 FX
- FO 100 LD
- FO 100 LH+
- TP 1000 TX
- FO 1000 SX
- FO 1000 LD
- FO 1000 LH
- FO 1000 LH+

模式 (Mode)
传输速率（10、100 或 1000 Mbps）和传输模式（全双工 (FD) 或半双工 (HD)）。

协商 (Negotiation)
指示自动协商是启用还是禁用状态。

流量控制 (Flow Ctrl.)
显示流量控制是启用还是禁用状态。

激活 (Active)
显示端口是处于激活（真）状态还是未激活（假）状态。对于未激活端口，通信伙伴指示连接状态“链路中断”。

状态 (Status)
显示端口是启用还是禁用状态。数据通信只能通过已启用的端口。另一方面，某个端口已关闭的通信伙伴会指示连接状态“接通”。

说明
“激活”和“未激活”状态对 PoE 端口的电源没有影响。电源的组态是独立的，并通过“PoE”菜单项进行。

链路 (Link)
与网络之间的链路状态。可能的选项如下：

- 上线 (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。
- 下线 (down)
  链路下线，例如由于关闭了所连接的设备。

访问控制 (Access Control)
“访问控制”(Access Control) 是一种输入滤波器，能够显示是否针对未知 MAC 地址锁定端口。可能有以下两种状态：

- 启用 (enabled)：
  目标地址不在工业以太网交换机地址表中的帧将被丢弃。工业以太网交换机不会在地址表中输入相应节点的源地址。
- 禁用 (disabled)（默认）：
  目标地址不在工业以太网交换机地址表中的帧将被转发。工业以太网交换机会将相应节点的源地址添加到地址表中。

  说明
  “访问控制”(Access Control) 自固件版本 2.2 起可用，并取代了以前的“锁定”(Lock) 功能。

减速 (Down-Shift)

显示是启用还是禁用减速功能。

更改端口组态

在“端口”(Port) 列中单击端口名称以打开“端口组态”(Port Configuration) 页面。您可以指定如何处理通过该端口的数据传输。

说明

光学端口只能工作在全双工模式以及最大传输速率。因此，不能对光学端口进行以下设置：

- 自动协商
- 传输速率
- 传输模式

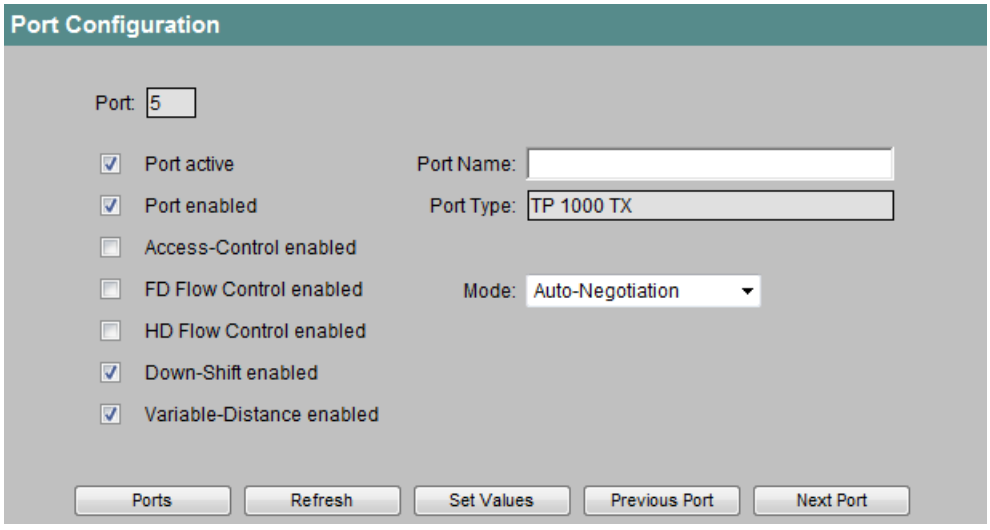


图 5-52 端口组态

端口 (Port)

指定将在页面上显示其组态的端口和插槽。

端口激活 (Port active)

通过该复选框，可以为端口设置“接通”和“链路中断”状态，这甚至适用于已关闭的端口（未选中“启用端口”(Port enabled)）。如果选中该复选框，将向端口的通信伙伴指示“接通”状态，即使对于已关闭的端口也是如此。

启用端口 (Port enabled)

选中此复选框使端口用于数据通信。如果未选中该复选框，则无论如何都会向该端口的通信伙伴指示“接通”状态。可以使用“端口激活”(Port active) 复选框更改连接状态。

启用访问控制 (Access Control enabled)

如果选中该复选框，工业以太网交换机不会在此端口学习单播地址。

启用全双工流量控制 (FD Flow Control enabled)
启用/禁用全双工模式的流量控制。但是，只有端口运行在全双工模式下，流量控制才有效。如果流量控制已启用但没有生效，则设置复选标记会在画面刷新后再次消失；但是，如果流量控制开始生效，则无需再次设置该标记。

启用半双工流量控制 (HD Flow Control enabled)
启用/禁用半双工模式的流量控制。但是，只有端口运行在半双工模式下，流量控制才有效。

说明

如果将该端口组态设置（固定）为环网端口，则冗余功能无法再正确运行。要正确运行该功能，环网端口必须处于全双工模式下。建议将环网端口设置为自动协商。

说明

利用各个自动功能，工业以太网交换机可以在某个端口过载时，防止或降低对其它端口和优先级类别（服务类别）的影响。这意味着即使启用流量控制，帧也可能被丢弃。
当工业以太网交换机接收的帧多于它可以发送的帧时（例如由于不同的传输速率），会发生端口过载。

启用减速功能 (Down-Shift enabled)
此设置只适用于 SCALANCE X-300/X408-2 使用双绞线传输的千兆位端口。
如果启用此选项，在线路出现问题时，端口传输率可降至 100 Mbps。

“启用可变距离”(Variable Distance enabled)
此设置只适用于位于 MM992-2VD 介质模块上的端口。
如果启用此选项，则端口在“可变距离”模式 (VD) 下运行。如果禁用此选项，则端口会作为标准千兆位端口运行。

模式 (Mode)
在“模式”(Mode) 列表框中，可以设置端口的传输速度和双工性。如果将模式设置为自动协商，工业以太网交换机和连接的终端设备会自动协商这些参数。

说明

如果要对伙伴端口使用自动跨接，请将模式设置为自动协商。

端口名称 (Port Name)
在此处可输入端口的名称。

端口类型 (Port Type)
此处显示端口的类型。无法编辑此框，因为该信息与硬件相关。

命令行接口语法

表格 5-41　端口状态 - CLI\SWITCH\PORTS>

命令	说明	注释
info [端口]	显示用于数据通信的端口的当前设置（实际状态）。	-
cfg [端口]	显示用于数据通信的端口的组态设置（所需状态）。	-
active [<T|F> [端口]]	激活 (T) 或禁用 (F) 指定端口。	仅限管理员。
status [<E|D> [端口]]	启用/禁用指定的端口用于数据通信。	仅限管理员。
fd_flow [<E|D> [端口]]	启用/禁用全双工模式下的流量控制。	仅限管理员。
hd_flow [<E|D> [端口]]	启用/禁用半双工模式下的流量控制。	仅限管理员。
autoneg [<E|D> [端口]]	启用/禁用自动协商。	仅限管理员。
name <端口> [字符串]	为指定端口分配一个名称（最长 64 个字符）。	仅限管理员。
actrl [<E|D> [端口]]	启用/禁用访问控制。 自固件版本 2.2 开始，“actrl”命令取代了“lock”命令。	仅限管理员。
speed [<速度>[端口]]	指定端口的传输速度和双工性： • 10H 10 Mbps/半双工 • 10F 10 Mbps/全双工 • 100H 100 Mbps/半双工 • 100F 100 Mbps/全双工	仅限管理员。
dwnshift [<E|D> [端口]]	对相关端口启用/禁用减速功能。	仅限管理员。
vd [<E|D>] [端口]	对相关端口启用/禁用“可变距离”(VD, Variable Distance) 模式。	仅限管理员。
vd_info	显示处于“可变距离”模式 (VD) 下的端口的信息。	-

5.5.3 Link Check (SCALANCE X-300/X408-2)

监视环网中的光纤连接

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

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

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

要求

- 只能使用 HRP 的光纤环网和备用端口或使用 MRP 环网的光纤环网端口启用链路检查功能。

  说明

  使用介质模块

  如果在介质模块的光纤端口上执行链路检查，请注意以下几点：
  - 在介质模块的相应光纤端口上激活链路检查。
  - 需要用不带光纤端口的模块替换介质模块。
  - 替换介质模块前请禁用链路检查。

- 必须在一个 HRP 或 MRP 环网内的两个相邻设备（连接伙伴）上启用链路检查。
- 启用链路检查的端口必须处于连接状态。
- 具有多个环网时，只能在第一个 MRP 环网实例上启用链路检查。

链路检查的工作方式

无故障连接的行为

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

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

故障的行为

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

链路检查是点对点协议，因此禁止通过交换机转发链路检查测试帧。为此，当启动链路检查伙伴时，链路检查将注册其 MAC 地址。如果此 MAC 地址在没有链路事件的情况下发生更改，则会触发故障状态。只有当链路中断并消除这一问题后才能结束该故障状态。

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

由链路检查关闭的端口必须复位后才能再次通信。有两种方法可以复位端口：

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

说明

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

复位链路检查后，会重新启动端口功能并复位统计数据。

通过 PROFINET IO 控制器组态

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

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

说明

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

连接监视

单击“链路检查”(Link Check) 菜单项，将显示“链路检查状态”(Link Check Status) 画面。

该画面显示以下内容：

- 可以启用链路检查的端口
- 当前状态
- 已发送或接收到的监视连接的链路检查帧的统计数据。

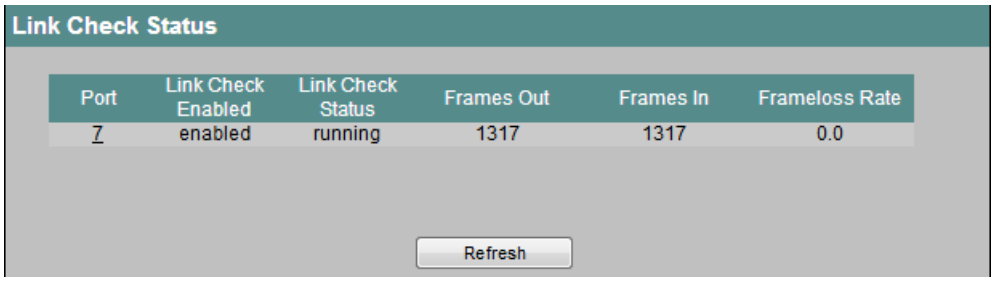


图 5-53 链路检查状态

该表显示以下信息：

端口 (Port)

显示后面信息所涉及的插槽和端口。

已启用链路检查

显示链路检查功能是启用还是禁用状态。

链路检查状态

显示链路检查功能的状态。可能的状态如下：

- 禁用
  将禁用该功能。
- 启用
  将启用该功能。连接伙伴尚未确认该监视。
- 正在运行
  将启用该功能。连接监视已启用。将对传出和传入测试帧进行计数并匹配。
- 故障
  将启用该功能。链路检查在监视部分检测到故障并关闭了端口。

帧输出

显示发出的链路检查测试帧数量

帧输入

显示接收到的链路检查测试帧数量。

丢帧率

以百分比 (%) 形式显示丢失的链路检查测试帧。该值始终与间隔相关，且不显示平均值。

如果链路检查状态为“running”，则该值显示上一次监视间隔丢失的链路检查测试帧。显示当前间隔值，直到下一个间隔值替换该值。

如果链路检查状态为“disabled”、“enabled”或“fault”，则该值不可用。显示“-”。

连接监视的组态

在“端口”(Port) 列中单击端口名称以打开“链路检查组态”(Link Check Configuration) 页面。在这里可针对此端口启用或禁用链路检查。

注意
确保链路检查使用的用于光纤连接的帧不会被网络中高优先级帧的过载所替代。 以下原因可导致高优先级消息帧过载： • 可导致高优先级帧重复的网络回路。 • 使用 SCALANCE X-300 更改转发帧的优先级

说明

仅为两个连接伙伴中的一个启用链路检查。这样会导致错误的行为。

说明

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

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

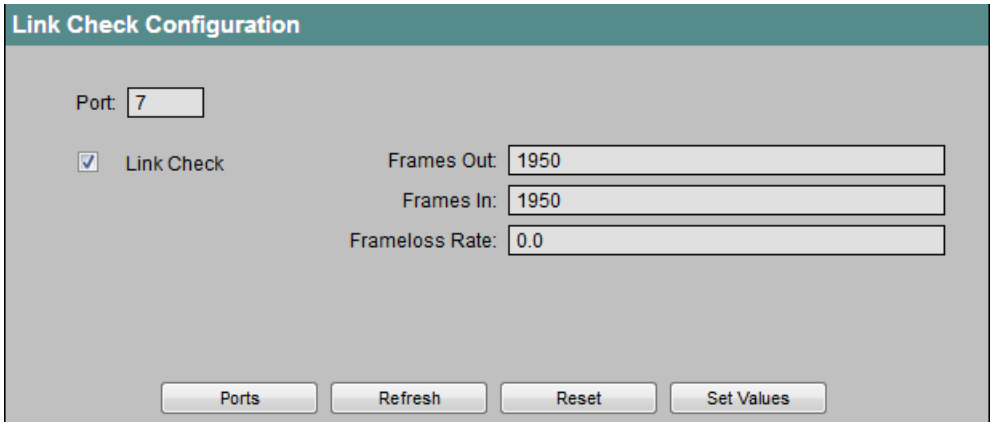


图 5-54　链路检查组态

端口 (Port)

指定将在页面上显示其组态的端口和插槽。

链路检查 (Link Check)

使用此复选框，可为端口启用或禁用链路检查功能。

帧输出

显示发出的链路检查测试帧数量

帧输入

显示接收到的链路检查测试帧数量。

丢帧率

以百分比 (%) 形式显示丢失的链路检查测试帧。该值始终与间隔相关，且不显示平均值。

如果链路检查状态为“running”，则该值显示上一次监视间隔丢失的链路检查测试帧。显示当前间隔值，直到下一个间隔值替换该值。

如果链路检查状态为“disabled”、“enabled”或“fault”，则该值不可用。显示“-”。

复位

复位链路检查后，会重新启动端口功能并复位统计数据。

如果使用“复位”(Reset) 按钮，必须在 30 s 内在两个连接伙伴上同时执行复位。

说明

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

命令行接口语法

表格 5-42　链路检查 - CLI\SWITCH\LINKCHK>

命令	说明	注释
info	显示端口的当前设置。	-
linkchk <E|D> [端口]	为指定端口启用/禁用链路检查功能。	仅限管理员。
复位 <所有端口>	为全部或部分端口复位链路检查功能。	仅限管理员。 使用“复位”(Reset) 命令时，会暂时形成回路，导致数据流量丢失。将再次自动清除回路。 如果您的应用程序不接受，可通过拔出线缆并再次插入来复位链路检查。

5.5.4 端口镜像

端口镜像信息

不同的数据速率造成的数据丢失

如果镜像端口的最大数据传输速率高于监视端口的最大数据传输速率，则数据可能会丢。监视端口此时不再能反映镜像端口上的数据流。

限制

端口镜像不会按照 1:1 的形式返回网络通信。例如，接收到错误帧时会将其丢弃而不通过镜像端口转发。

镜像端口的组态

单击 “镜像”(Mirroring) 菜单项，将显示 “镜像组态”(Mirroring Configuration) 画面。

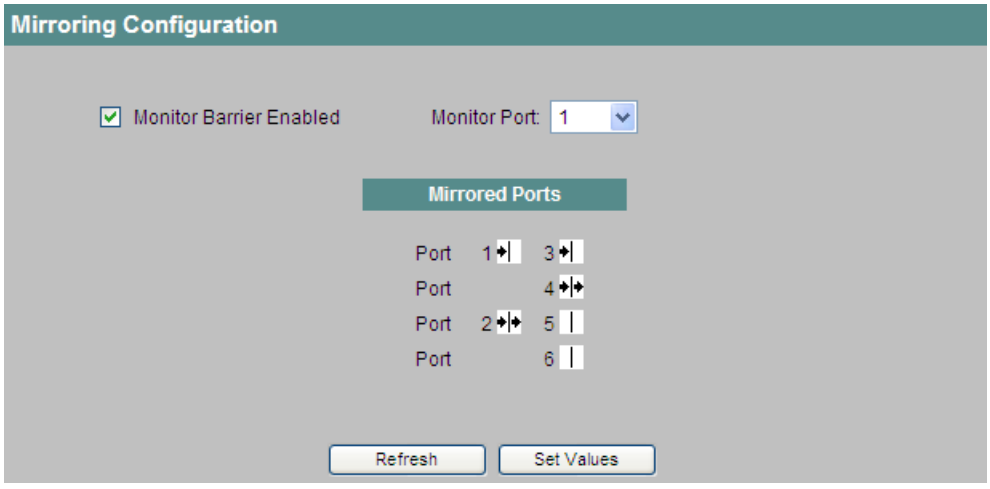


图 5-55 镜像组态

启用监视屏障 (Monitor Barrier Enabled)

通过该复选框，可以限制通过监视端口通信。

- 启用
  监视端口将无法进行常规帧交换。
  例如，无法使用 WBM 或 CLI 通过监视端口对设备进行组态或诊断。
- 禁用 (Disabled)
  通过监视端口通信不受限制。
  可以使用 WBM、CLI 和 SNMP 通过监视端口通信。

在模块出厂时会启用该选项。

监视端口

镜像端口中的数据通信将复制到监视端口。

从下拉列表中选择所需端口。

可同时将多个端口镜像到一个监视端口。

如果协议分析器与监视端口相连接，则可在不中断镜像端口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。只有工业以太网交换机上有空闲端口可用作监视端口时，才能实现此功能。

说明

环网端口不能用作监视端口。

镜像端口 (Mirrored Ports)

镜像端口的数据通信被复制到监视端口。

可对每个端口进行以下设置：

- 启用该框的左右两半部分。
  复制入站和出站数据通信。
- 启用该框的左半部分。
  仅复制入站数据通信。
- 启用该框的右半部分。
  仅复制出站数据通信。

说明

多个镜像端口

根据设备型号，如果选择了多个端口作为镜像端口，则可按不同的间隔发送来自监视端口的泛洪帧。根据设计，在这种组态下，监视器端口上可能出现帧丢失的情况。

泛洪帧包括广播帧、未学习的组播帧或未学习的单播帧。

命令行接口语法

表格 5-43　镜像组态 - CLI\SWITCH\MIRRORING>

命令	说明	注释
info	显示当前的端口监视设置。	
mirrport <模式> [端口]	指定要监视的端口（镜像端口）。	仅限管理员
moniport [<端口>]	指定监视端口。	仅限管理员
barrier [E|D]	启用/禁用监视屏障功能。	仅限管理员

5.5.5 链路汇聚

5.5.5.1 链路汇聚

捆绑网络链路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条链路捆绑在一起，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)。

说明

捆绑到链路汇聚中的端口被视为虚拟端口（例如 PLC1），可用于 CLI 命令来代替各端口号。

组态链路汇聚的步骤

1. 首先，确定想要组合在一起形成链路汇聚的端口。
2. 在两个设备上组态链路汇聚。
3. 然后连接电缆。

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！

主端口

链路汇聚的主端口是将其设置甚至其 MAC 地址传递到整个链路汇聚的端口。

如果在创建汇聚时没有组态主端口，则会将端口号最小的端口用作主端口。

显示已组态的链路汇聚

该菜单显示所有已组态的链路汇聚。

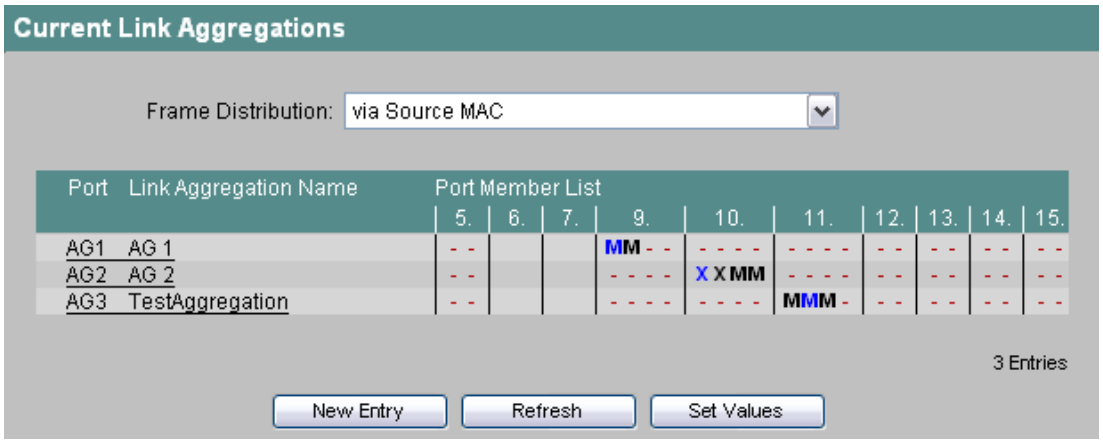


图 5-56 当前链路汇聚 (Current Link Aggregations)

帧分发 (Frame Distribution)

设置汇聚的各个连接上的数据包分发类型。 由于硬件限制，SCALANCE X-300/408 和 SCALANCE X414 上可以进行的设置不同。

端口 (Port)

显示此链路汇聚的虚拟端口号。 这是由固件内部分配的。

链路汇聚名称 (Link Aggregation Name)

显示链路汇聚的可自由组态的名称。 此名称可由用户在组态期间指定。

端口成员列表 (Port Member List)

显示属于此汇聚的端口。 含义如下：

- M（黑色）： 该端口是汇聚的成员。
- M（蓝色）： 该端口是汇聚的成员，并且是其主端口。

- X（黑色）：该端口是汇聚的成员，但当前未激活。
  在这种情况下，端口未激活意味着该端口已从汇聚中动态移除。 可能的原因如下：
  – 汇聚的端口具有不同的组态（例如速度）
  – 端口未与同一设备相连接
  – 端口没有链路
  – 未根据 802.1x 对端口进行验证
  – ...
- X（蓝色）：该端口是汇聚的成员，并且是其主端口，但未激活。

说明

在 SCALANCE X414-3E 上，尽管可在汇聚中将千兆位端口 5.1 和 5.2 组态为快速以太网端口，但它们始终不会与其它快速以太网端口一同激活，即使将它们设置为快速以太网。

创建新链路汇聚

单击 “新建条目”(New Entry) 按钮可创建新链路汇聚。 出现以下画面：

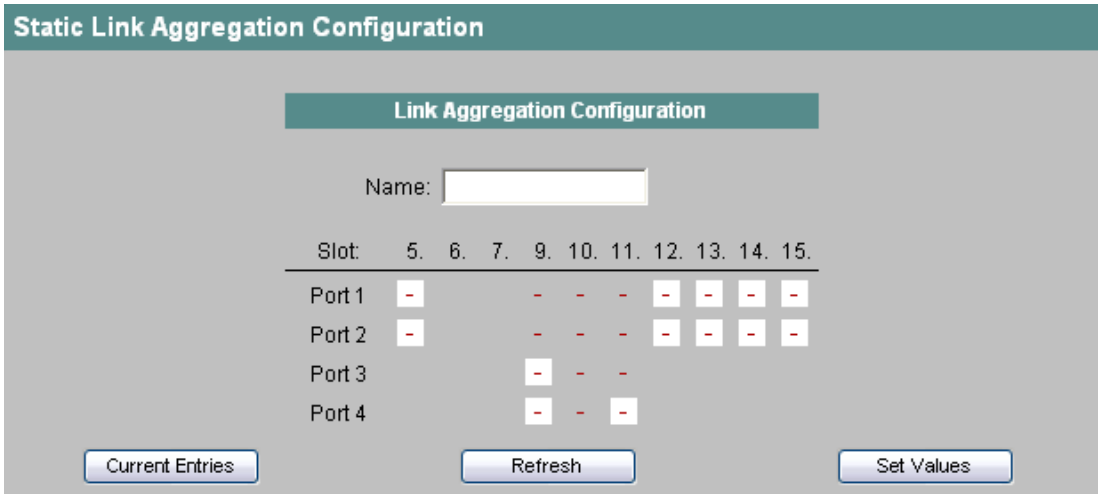


图 5-57 链路汇聚组态 (Link Aggregation Configuration)

名称 (Name)

在此处可为新链路汇聚指定一个符号名称。 如果未在此处输入名称，系统会自动设置一个名称。

插槽/端口 (Slot/Port)

在此处可以向新汇聚中添加特定端口。 只能添加不属于其它链路汇聚的端口。

含义如下：

- M（黑色）： 该端口是汇聚的成员。
- M（蓝色）： 该端口是汇聚的成员，并且是其主端口。

更改链路汇聚

在“当前链路汇聚”(Current Link Aggregation) 概览画面中，单击“端口”(Port) 列或“链路汇聚名称”(Link Aggregation Name) 来更改现有链路汇聚的组态。

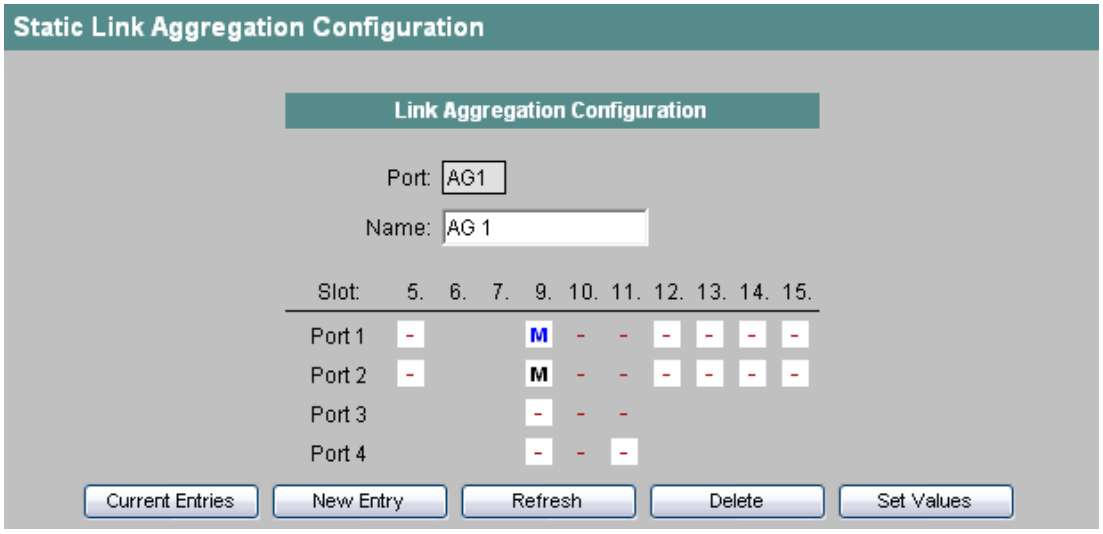


图 5-58 静态链路汇聚组态 (Static Link Aggregation Configuration)

端口 (Port)

显示汇聚的虚拟端口号。 这是由系统内部分配的，无法修改。

名称 (Name)

在此处可更改链路汇聚的名称。

插槽/端口 (Slot/Port)

可以选择向链路汇聚中添加特定端口或者从链路汇聚中移除特定端口。 只能修改不属于其它链路汇聚的端口。

含义如下：

- M（黑色）： 该端口是汇聚的成员。
- M（蓝色）： 该端口是汇聚的成员，并且是其主端口。

更改主端口

要更改主端口，请按以下步骤操作：

1. 单击原始主端口（蓝色 M）- 标记消失。 如果希望将端口保留在汇聚中，则再次单击该端口（黑色 M）
2. 单击新的主端口，直到出现蓝色 M。

命令行接口语法

当前链路汇聚 - CLI\SWITCH\LAG>

命令	说明	注释
info	显示链路汇聚组的当前设置（实际状态）。	-
frmdistr [模式]	设置汇聚的各个连接上的数据包分发类型。 X414 存在以下模式： • srcmac 源 MAC 地址 • dstmac 目标 MAC 地址 • mac 源和目标 MAC 地址 • srcip 源 IP 地址 • dstip 目标 IP 地址 • ip 源和目标 IP 地址 X408/X-300 存在以下模式： • hash 源和目标 MAC 地址散列 • xor 源和目标 MAC 地址异或	仅限管理员。
add <主端口>	创建包括指定主端口的新链路汇聚	仅限管理员。

命令	说明	注释
master <ID> <主端口>	更改链路汇聚的主端口。	仅限管理员。
name <ID> <字符串>	更改链路汇聚的名称。	仅限管理员。
ports <ID> <选项> [端口]	更改链路汇聚的成员（端口）- 主端口除外。 可能的选项如下： • - 该端口不是链路汇聚的成员。 • M 该端口是链路汇聚的成员。	仅限管理员。
delete <ID>	删除链路汇聚。	仅限管理员。

5.5.5.2 LACP 组态 (LACP Configuration)

启用 LACP 功能

LACP（Link Aggregation Control Protocol，链路汇聚控制协议）用于处理链路汇聚的激活端口选择。 您可以对每个链路汇聚启用 LACP。

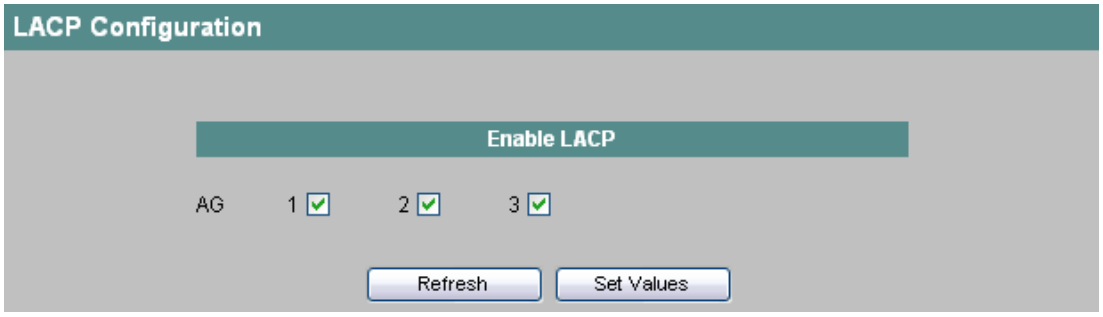


图 5-59 LACP 组态 (LACP Configuration)

启用 LACP (Enable LACP)

在此处启用 LACP。

如果启用 LACP，端口将发送相应的 LACP 帧。 如果伙伴设备返回 LACP 帧，则表示链路汇聚端口已启用。

如果禁用 LACP，则会立即启用链路汇聚端口。

命令行接口语法

表格 5-44　LACP 组态 - CLI\SWITCH\LAG>

命令	说明	注释
lacp [<E|D> [ID]]	对指定链路汇聚的所有端口启用/禁用 LACP。	仅限管理员。

5.5.6　IEEE 802.1x

5.5.6.1　802.1x RADIUS 组态 (802.1x RADIUS Configuration)

通过外部服务器进行验证

RADIUS 的概念基于外部验证服务器。 工业以太网交换机通过此服务器验证所连接的终端设备。 这可对终端设备通过工业以太网交换机访问网络进行限制。

为此，需组态 RADIUS 服务器并指定相关端口的验证方法。

802.1x RADIUS 组态 (802.1x RADIUS Configuration)

如果单击“RADIUS 组态”(RADIUS Config) 文件夹图标，将显示“802.1x RADIUS 组态”(802.1x RADIUS Configuration) 画面。

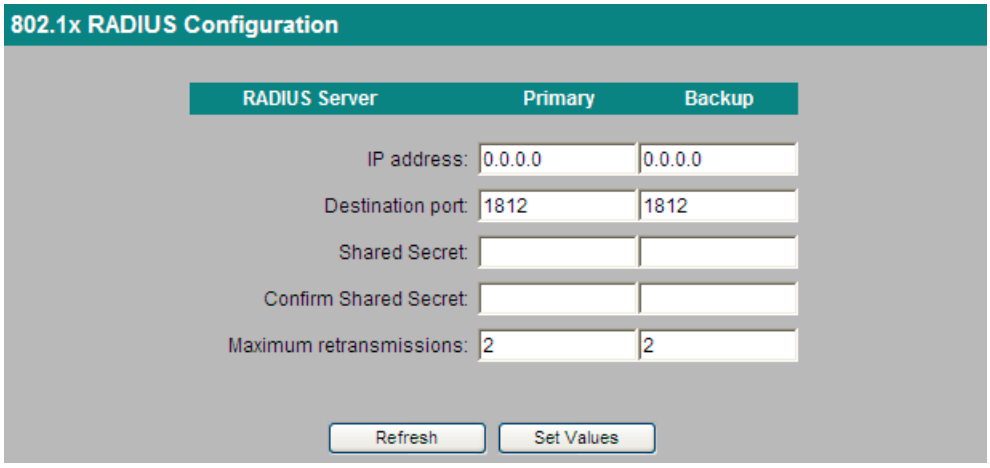


图 5-60　802.1x RADIUS 组态 (802.1x RADIUS Configuration)

在此画面中，指定执行验证方法的 RADIUS 服务器。

画面布局上的每个输入框分别为主服务器和备份服务器各显示一次。 首先会查询主服务器。如果无法到达主服务器，则查询备份服务器。

该画面包含以下输入框：

- **IP 地址 (IP address)**
  在"IP 地址"(IP address) 输入框中输入服务器的 IP 地址。
- **目标端口 (Destination port)**
  在 "目标端口"(Destination port) 输入框中输入 RADIUS 服务器上的输入端口。
  默认会设置输入端口 1812。值范围为 1 到 65535。
- **共享秘密**
  在 "共享秘密"(Shared Secret) 输入框中输入访问标识符。
- **确认共享秘密 (Confirm Shared Secret)**
  在 "确认共享秘密"(Confirm Shared Secret) 输入框中再次输入访问标识符。
- **最大重传次数 (Maximum retransmissions)**
  在 "最大重传次数"(Maximum retransmissions) 输入框中，输入查询另一个组态的 RADIUS 服务器或登录被视为失败之前尝试重传的最大次数。
  默认会设置为 2 次。值范围为 1 到 254。

RADIUS 服务器 (RADIUS Server)

可输入两台 RADIUS 服务器的数据。 如果在 "主"(Primary) 列中定义的服务器不可用，则使用 "备份"(Backup) 列中的服务器信息。

有关 "登录模式" 的 RADIUS 服务器

此处指定的 RADIUS 服务器同时也是用于登录模式"RADIUS"和"RADIUS 和本地"(RADIUS and Local) 的验证服务器，请参见系统密码和登录模式 (页 65)。

命令行接口语法

表格 5-45　802.1x RADIUS 组态 - CLI\SWITCH\DOT1X\RADIUS>

命令	说明	注释
info	显示当前 RADIUS 设置。	-
server [<ip>[:port]]	指定主服务器的 IP 地址和端口。	仅限管理员。
serverb [<ip>[:port]]	指定备份服务器的 IP 地址和端口。	仅限管理员。
secret <字符串>	指定主服务器的密码。	仅限管理员。

命令	说明	注释
secretb <字符串>	指定备份服务器的密码。	仅限管理员。
maxret [次数]	对主服务器的最大请求数。	仅限管理员。
maxretb [次数]	对备份服务器的最大请求数。	仅限管理员。

5.5.6.2 802.1x 端口参数

802.1x 端口参数

如果单击 “端口”(Ports) 子菜单，将显示“802.1x 端口参数”(802.1x Port Parameters) 画面。此画面显示当前身份验证设置的总览。

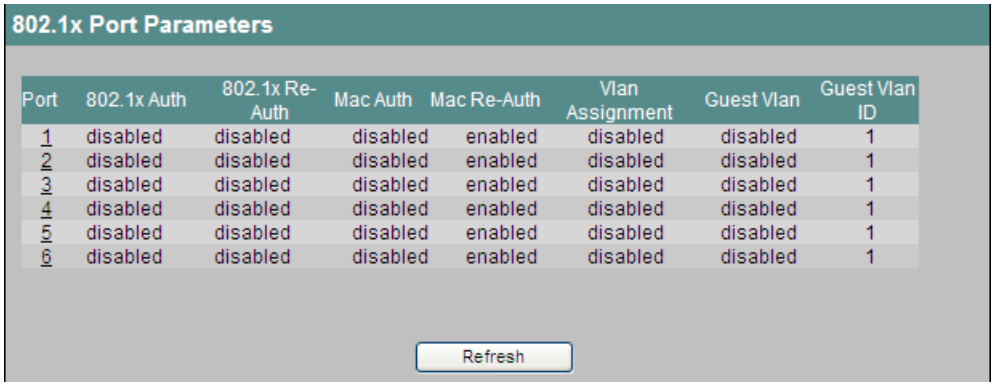


图 5-61 802.1x 端口参数

表中的列显示以下信息：

- **端口 (Port)**
  “端口”(Port) 列显示信息所关联的端口。
- **802.1X 身份验证 (802.1X Auth)**
  “802.1X 身份验证”(802.1X Auth) 列显示对该端口是启用还是禁用身份验证方法“802.1x”。
- **802.1X 身份重新验证 (802.1X Re-Auth)**
  “802.1X 身份重新验证”(802.1x Re-Auth) 列显示是（启用）否（禁用）周期性重复使用“802.1x”进行身份验证。
- **Mac 身份验证 (Mac Auth)**
  “Mac 身份验证”(Mac Auth) 列显示对端口是启用还是禁用身份验证方法“MAC 身份验证”(MAC Authentication)。
- **Mac 身份重新验证 (Mac Re-Auth)**
  “Mac 身份重新验证”(Mac Re-Auth) 列显示是（启用）否（禁用）周期性重复使用“MAC 身份验证”进行身份验证。

- **Vlan 分配 (Vlan Assignment)**
  "Vlan 分配"(Vlan Assignment) 列显示对该端口是采用（启用）还是丢弃（禁用）身份验证服务器的 VLAN 信息。
  此选项只适用于"MAC 身份验证"(MAC Authentication) 身份验证方法。
- **访客 Vlan (Guest Vlan)**
  "访客 Vlan"(Guest Vlan) 列显示对该端口是启用还是禁用 "访客 VLAN"(Guest VLAN) 选项。
- **访客 Vlan ID (Guest Vlan ID)**
  "访客 Vlan ID"(Guest Vlan ID) 列显示充当该端口的访客 VLAN 的 VLAN-ID。

命令行接口语法

表格 5-46　802.1x 端口参数 - CLI\SWITCH\DOT1X\PORTS>

命令	说明	注释
info	显示端口的当前设置。	-

5.5.6.3 802.1x 端口组态

802.1x 端口组态

如果单击“802.1x 端口参数”(802.1x Port Parameters) 页面 “端口”(Port) 列中的端口名称，将打开“802.1x 端口组态”(802.1x Port Configuration) 页面：

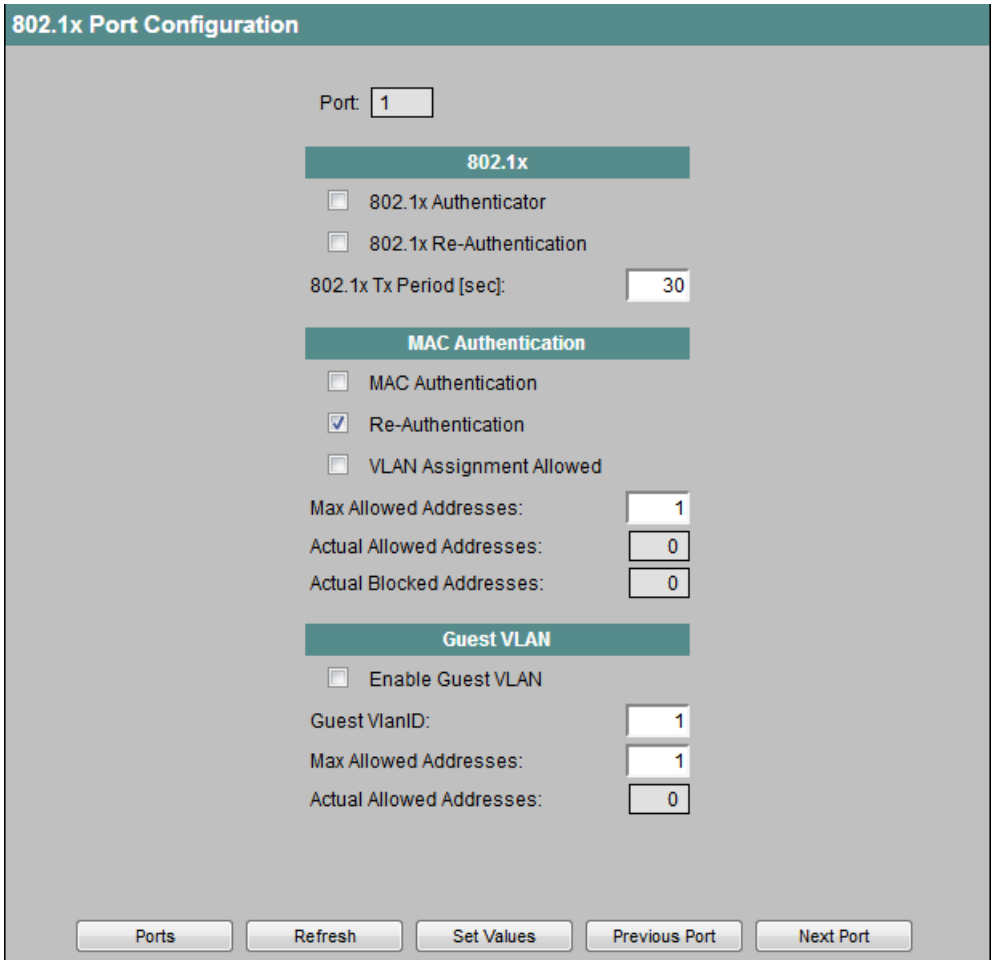


图 5-62 802.1x 端口组态

在此画面中，可以为所选端口组态身份验证方法“802.1x”和“MAC 身份验证”(MAC Authentication) 以及 “访客 VLAN”(Guest VLAN) 选项。

这些功能按层级顺序排列。如果启用了全部三项功能，则最初会尝试使用“802.1x”对终端设备进行身份验证。如果验证不成功，将启动“MAC 身份验证” 。如果验证还不成功，则允许终端设备在 “访客 VLAN”中通信。必须至少有一种身份验证方法激活，才能使用 “访客 VLAN”。

这两种身份验证方法都取决于终端设备。如果终端设备支持 EAP（Extensible Authentication Protocol，可扩展身份验证），则可使用"802.1x"方法进行身份验证。如果终端设备不支持 EAP，则可使用"MAC 身份验证"进行身份验证。在这种情况下，工业以太网交换机采用终端设备的角色，并将设备的 MAC 地址用作身份验证参数。

该画面包含以下部分和输入框：

端口 (Port)

"端口"(Port) 显示框中显示所选端口。

"802.1X"部分

"802.1x"身份验证方法的作用方式如下：
支持 EAP 的终端设备向工业以太网交换机发送身份验证信息。工业以太网交换机将该信息转发给 RADIUS 服务器。身份验证服务器核对信息，从而允许或拒绝终端设备访问网络。

- **802.1X 验证器**
  如果想要使用 802.1x 方法对终端设备进行身份验证，请启用此选项。
- **802.1X 身份重新验证 (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。默认情况下会设置一个小时 (3600 s)。
- **802.1x Tx 周期 [秒]**
  由 802.1X 协议使用的时间常数"txPeriod"（以秒为单位）。默认情况下，会设置 30 秒。

"MAC 身份验证"部分

"MAC 身份验证"身份验证方法的作用方式如下：
工业以太网交换机收到终端设备发来的帧时，随即向 RADIUS 服务器发出请求，从而允许或拒绝终端设备访问网络。

- **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。
- **MAC 身份重新验证 (MAC 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。默认情况下会设置一个小时 (3600 s)。
- **允许的 VLAN 分配 (VLAN Assignment Allowed)**
  RADIUS 服务器通知工业以太网交换机有关终端设备所属的 VLAN。
  如果要考虑服务器通知的信息，请启用此选项。终端设备于是便属于相应的 VLAN。
  如果禁用此选项，则会丢弃 VLAN 信息。
- **最大允许地址数 (Max Allowed Addresses)**
  在"最大允许地址数"(Max Allowed Addresses) 输入框中，输入允许同时连接到端口的终端设备的数量。

- **实际允许地址数 (Actual Allowed Addresses)**
  显示当前连接到端口的设备数量。
- **实际拦截地址数 (Actual Blocked Addresses)**
  显示当前被拦截的终端设备数量。

“访客 VLAN”部分

如果使用“802.1x”或“MAC 身份验证”都无法对终端设备进行身份验证，则可允许该终端设备在预组态的访客 VLAN 中通信。

- **启用访客 VLAN (Enable Guest VLAN)**
  如果想要在身份验证失败时在访客 VLAN 中启用终端设备，请启用此选项。
- **访客 VlanID (Guest VlanID)**
  在“访客 VlanID”(Guest VlanID) 输入框中输入端口的 VLAN-ID。
- **最大允许地址数 (Max Allowed Addresses)**
  在“最大允许地址数”(Max Allowed Addresses) 输入框中，输入允许同时连接到端口的终端设备的数量。
- **实际允许地址数 (Actual Allowed Addresses)**
  显示当前连接到端口的设备数量。

命令行接口语法

表格 5-47　802.1x 端口组态 - CLI\SWITCH\DOT1X\PORTS>

命令	说明	注释
auth　[<E|D> [端口]]	对所选端口启用/禁用“802.1x”身份验证方法。	仅限管理员。
reauth　[<E|D> [端口]]	对所选端口启用/禁用身份重新验证功能（“802.1x”）。	仅限管理员。
macauth　[<E|D> [端口]]	对所选端口启用/禁用身份验证方法“MAC 身份验证”。	仅限管理员。
macreauth[<E|D> [端口]]	对所选端口启用/禁用身份重新验证功能（“MAC 身份验证”）。	仅限管理员。
vlanassgn[<E|D> [端口]]	对所选端口启用/禁用“允许的 VLAN 分配”功能。	仅限管理员。
guestvlan[<E|D> [端口]]	对所选端口启用/禁用“启用访客 VLAN”功能。	仅限管理员。

命令	说明	注释
gvlanid [<1..4094> [端口]]	为所选端口显示/设置访客 VlanID。	仅限管理员。
maxaumac [<1..20> [端口]]	显示/设置可同时连接到端口的终端设备数量。	仅限管理员。
maxaugu [<1..20> [端口]]	显示/设置可同时连接到端口的终端设备数量。	仅限管理员。
txperiod [<1..3600> [端口]]	显示/设置由 802.1X 协议使用的时间常数“txPeriod”（以秒为单位）。默认情况下，会设置 30 秒。	仅限管理员。

5.5.7 单播过滤器 (ACL)

5.5.7.1 Current Unicast Filter (Access Control List)

地址过滤

此菜单显示过滤表的当前内容。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。

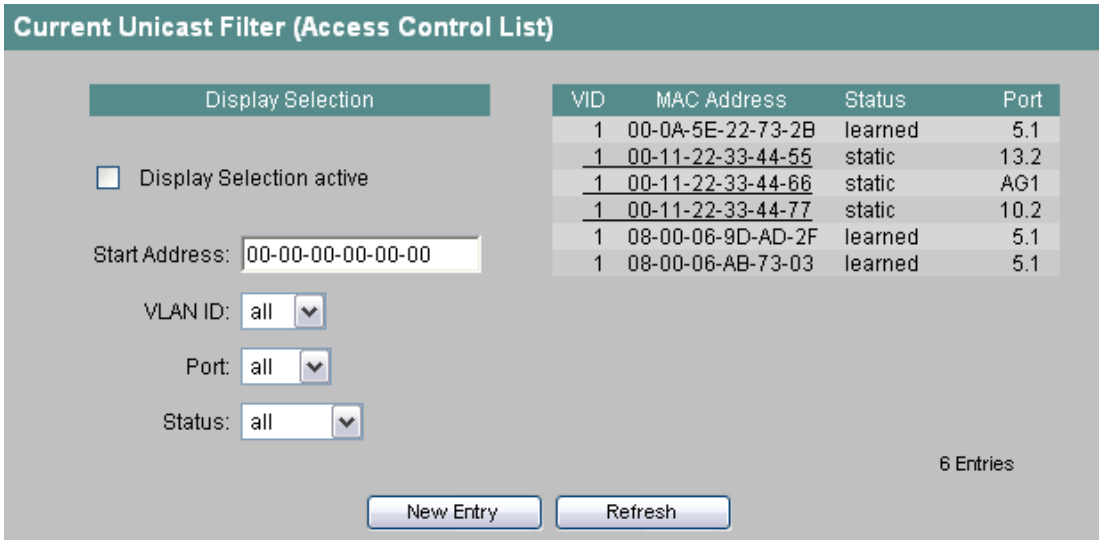


图 5-63 当前单播过滤器 (Current Unicast Filter)

选择显示的地址

显示激活选项 (Display Selection active)
选中此复选框时，仅显示所选元素，否则将显示所有地址。

起始地址 (Start Address)
此参数用于指定过滤表显示存储的 MAC 地址时的起始地址。如果在此处没有输入任何地址，将从 VLAN ID 开始显示。如果在此处输入了特定值，则仅显示具有相应 VLAN ID 的地址。VLAN ID 的有效值在 1 到 4094 之间。如果不想选择 VLAN ID，则选择“全部"(all) 条目。

端口 (Port)
在此处可以限制显示特定端口上的节点的地址。如果选择“全部"(all) 条目，则会显示所有端口上的地址。

状态 (Status)
使用此列表框，可以限制显示具有特定状态的地址。状态的可能值如下：

- 学习 (learned)（学习的地址）
- 静态 (static)（由用户组态）
- 全部 (all)（学习的地址和组态的地址）

访问控制列表

单播过滤器可用于访问控制。借助各端口的“访问控制”功能（自固件版本 2.2 开始 - 之前版本中该功能称为“锁定”！）（请参见“访问控制端口组态菜单项”或“端口状态菜单”），可针对未知节点锁定各个端口。如果对某个端口启用了“访问控制”功能，则来自未知 MAC 地址的数据包会被立即丢弃。

由于启用了“访问控制”的端口无法学习任何 MAC 地址，因此在启用“访问控制”后，这些端口上学习的地址将被自动删除。要将设备包含在已知节点的列表中，必须为其 MAC 地址创建一个单播条目（在相关端口上）。

要自动输入所有连接的节点，可使用自动学习功能（请参见"ACL 学习 (ACL Learning) 菜单项”部分）。

过滤表中的信息

过滤表的四个列显示以下信息：

- **VID**
  分配给此 MAC 地址的 VLAN-ID。如果没有给 MAC 地址分配 VLAN-ID，此处会显示 1
- **MAC 地址 (MAC Address)**
  工业以太网交换机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。此处，“学习”(learned) 表示由于从此节点接收到帧，因此已学习指定的地址。“静态”(static) 条目表示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，当老化时间结束或交换机重启时，静态地址不会被删除。“无效”(invalid) 表示这些值不会被 SCALANCE X408 评估。通过“基于 Web 的管理”(Web Based Management) 输入这些值时没有带端口号。
- **端口 (Port)**
  指定访问指定地址的节点时所使用的插槽和端口。工业以太网交换机收到的目标地址与此地址相匹配的帧将被转发到此端口。

组态过滤器

单击状态为*静态 (static)* 的 MAC 地址将打开用于组态过滤器的页面：

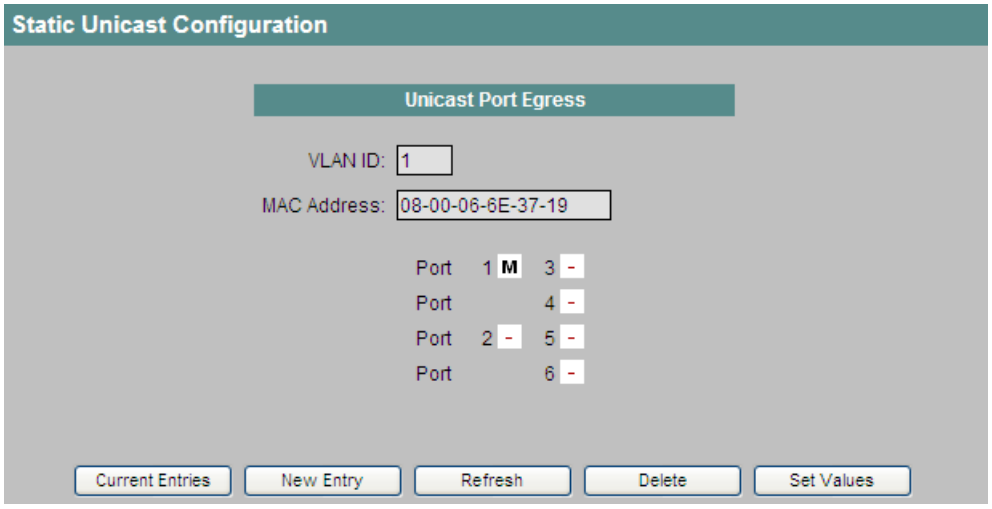


图 5-64　静态单播组态 (Static Unicast Configuration)

插槽/端口 (Slot/Port)

选择具有输入目标地址的帧将被转发到的插槽和端口。单击相应的框后，将显示状态信息，其含义如下：

- **M**
  （成员）通过此端口发送单播帧。
- **–**
  不通过此端口转发单播帧。

- **#**
  端口无效。
- **?**
  VLAN 组态与单播组态相矛盾。在不属于 VLAN 的单播组态中选择目标端口时，可能会发生这种情况。

创建新条目

单击“新建条目”(New Entry) 按钮可向地址表中添加一个条目。将打开“静态单播组态”(Static Unicast Configuration) 页面，在其中可进行必要的输入：

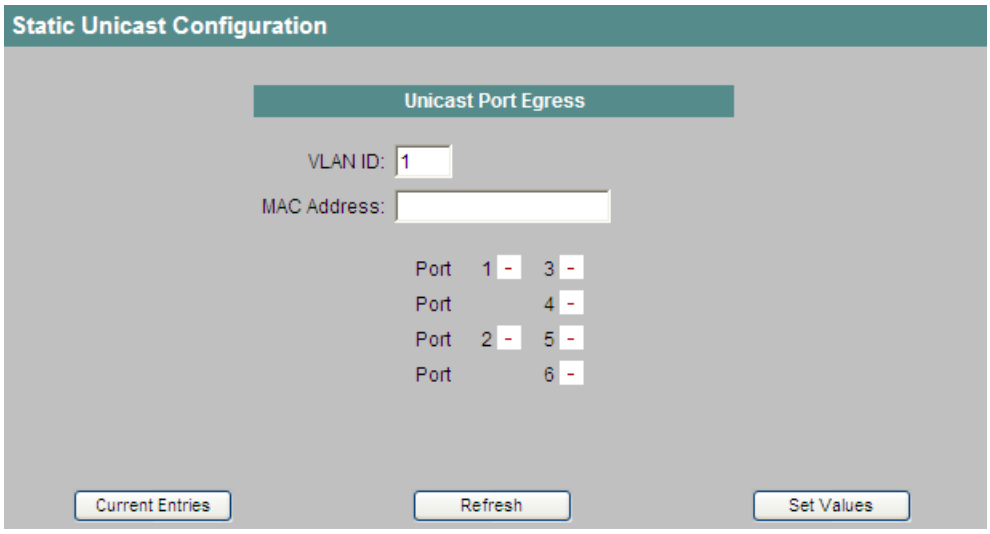


图 5-65　静态单播组态 II (Static Unicast Configuration II)

VLAN ID
输入 MAC 地址所属的 VLAN 的 ID。如果未进行任何设置，则会将 VLAN ID 1（默认 VLAN）设置为基本设置。

MAC 地址 (MAC Address)
输入想要添加到地址表的 MAC 地址。此地址与收到的帧的目标地址相匹配。

插槽/端口 (Slot/Port)
选择具有输入目标地址的帧将被转发到的插槽和端口。单击相应的框后，将出现“M”。

无效端口用“#”标记。如果某个端口用“?”标记，则表示 VLAN 组态与单播组态相矛盾。

说明
您只能为单播地址指定一个端口。

当前条目 (Current Entries)
单击此按钮可以返回到 MAC 地址列表。

新建条目 (New entry)
单击此按钮可在过滤表中创建新条目。

删除 (Delete)
单击此按钮可从过滤表中删除显示的条目。

命令行接口语法

表格 5-48　当前单播过滤器 - CLI\SWITCH\UCAST>

命令	说明	注释
info	显示工业以太网交换机地址表的内容。	-
find [VLAN-ID]<MAC 地址> [S|L] [端口]	在工业以太网交换机的地址表中搜索 MAC 地址。还可以看到收到的具有此（目标）地址的帧将被发送到的端口。 如果不指定 VLAN-ID，则会浏览所有 VLAN 以查找指定的 MAC 地址。 还可以指定端口作为选项。这样浏览范围将被限制为指定的端口。 还可以将浏览范围限制为静态条目和学习的条目，来作为进一步选项： • S 静态条目 • L 学习的条目	-
add [VLAN-ID]<MAC 地址> <端口>	向地址表中插入一个单播地址的静态条目。	仅限管理员。
edit [VLAN-ID] <MAC 地址> <端口>	更改地址表中的条目。	仅限管理员。
delete [VLAN-ID] <MAC 地址>	从地址表中删除一个静态条目。	仅限管理员。

5.5.7.2 访问控制列表学习 (Access Control List Learning)

开始学习/停止学习 (Start Learning/Stop Learning)

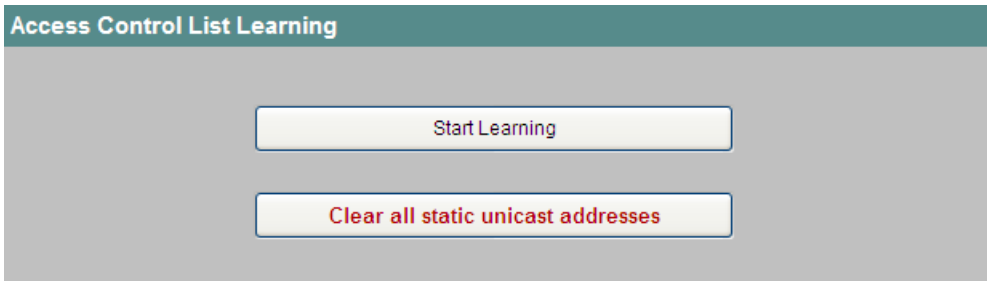


图 5-66 访问控制列表学习 (Access Control List Learning)

借助自动学习功能，与工业以太网交换机连接的所有设备都可以被自动输入到“访问控制列表”中（请参见“Current Unicast Filter (Access Control List) 菜单项”部分）。 只要启用该功能，所有学习的单播地址就会立即被创建为静态单播条目。 只有选择“停止学习”(Stop Learning) 后，学习才会停止。 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。 只有在学习阶段中发送数据包的节点会被找到。

启用“访问控制”功能后，只有在学习阶段完成的已知节点（静态单播条目）所发出的数据包才会被相关端口接受。

说明

如果在自动学习阶段之前已对各个端口激活“访问控制”功能，则在这些端口上将不会学习到任何地址。 这样便可限制对特定端口的学习。 如果不希望某个端口学习地址，只需在启用学习之前对该端口启用访问控制。

清除所有静态单播地址 (Clear all static unicast addresses)

在具有多个节点的大型网络中，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。

命令行接口语法

表格 5-49　访问控制列表学习 - CLI\SWITCH\UCAST>

命令	说明	注释
learning [start|stop]	无参数 显示自动学习的当前状态。 • start 开始自动学习。 • stop 停止自动学习。	仅限管理员。
clear	删除所有静态单播条目。	仅限管理员。

5.5.7.3　访问控制端口组态 (Access Control Port Configuration)

启用“访问控制”功能

通过选择相关选项，来指定是否对各个端口启用“访问控制”。 如果对某个端口启用该功能，则来自未知 MAC 地址的数据包会被立即丢弃。 只接受来自已知节点的数据包（请参见 Current Unicast Filter (Access Control List) 菜单项）。

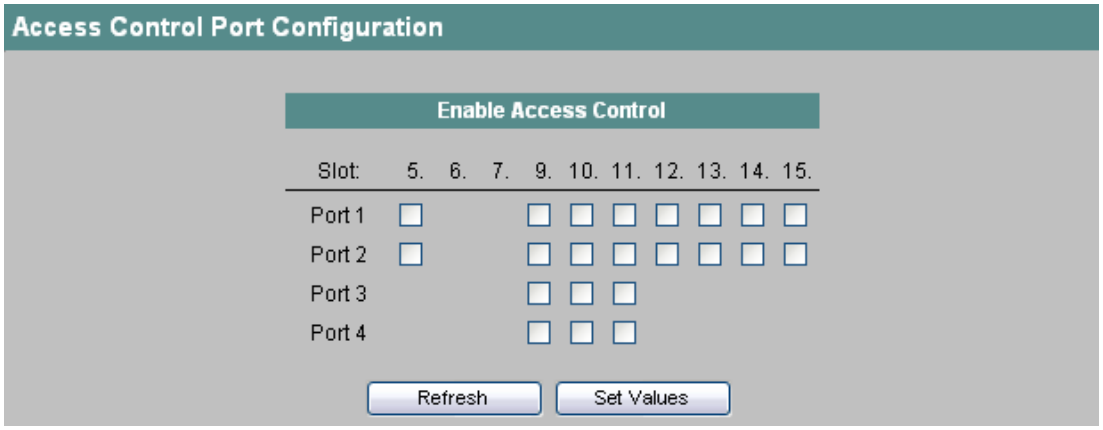


图 5-67　访问控制端口组态 (Access Control Port Configuration)

命令行接口语法

表格 5-50　访问控制端口组态 - CLI\SWITCH\UCAST>

命令	说明	注释
actrl [<E|D> [端口]]	对指定端口启用/禁用“访问控制”功能。 如果不指定任何端口，则会对所有端口启用/禁用“访问控制”。	仅限管理员。

5.5.7.4　未知单播屏蔽掩码

禁止转发未知单播帧

在此菜单中，可禁止各端口转发未知单播帧。

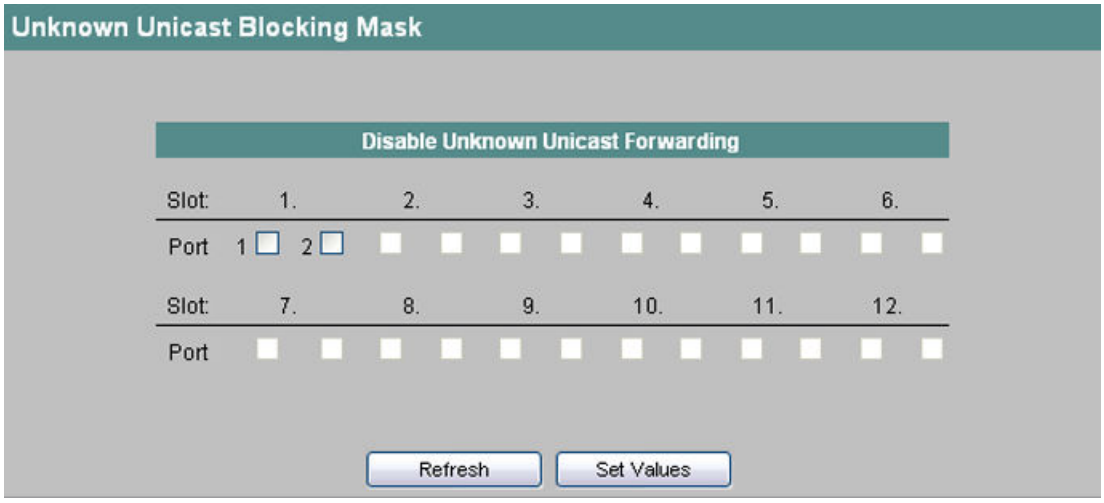


图 5-68　未知单播屏蔽掩码

禁用未知单播转发 (Disable Unknown Unicast Forwarding)

在此处指定将禁用未知单播帧转发的端口。

命令行接口语法

表格 5-51　未知单播屏蔽掩码 - CLI\SWITCH\>

命令	说明	注释
blkucast [<E|D> [端口]]	启用/禁用指定端口的单播屏蔽。	仅限管理员。

5.5.8 组播组

5.5.8.1 当前组播组 (Current Multicast Groups)

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

与单播帧的发送相比，组播帧会对交换机产生更高的负载。 一般来说，组播帧会被发送到交换机的所有端口。 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 参数分配数据包（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其目标端口。 这些条目可以是动态的（由工业以太网交换机学习），也可以是静态的（由用户设置）。

说明

如果 SCALANCE X414-3E 的过滤表包含的学习条目数多于 500，则冗余网络中的重新组态时间可能超过 300 ms（使用 HRP 时）或 200 毫秒（使用 MRP 时）。

切换页面

单击">>"或"<<"可向后或向前翻页。

在第二页，您将看到已建立的所有链路汇聚，而不是端口。

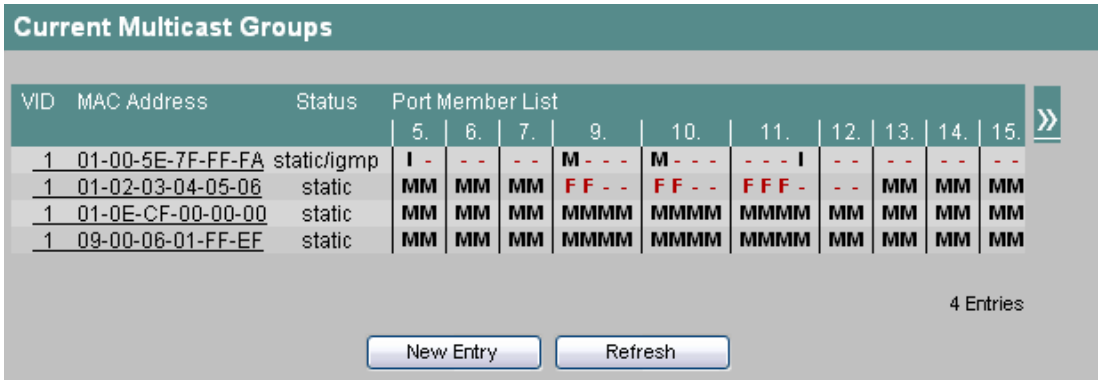


图 5-69　当前组播组 (Current Multicast Groups)

过滤表中的信息

过滤表的四个区域显示以下信息：

VID
分配给此 MAC 地址的 VLAN-ID。

MAC 地址 (MAC Address)
工业以太网交换机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。 可能的信息如下：

- **静态 (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，当老化时间结束或交换机重启时，静态地址不会被删除。
- **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 (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。
  M（红色）
  组播在 VLAN 中进行组态，而不在相关端口上组态。 由于 VLAN-ID 不同，无法通过此端口转发组播。
- **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 数据包注册。
- **–**
  不是组播组的成员，不会通过此端口发送任何组播帧。
- **F**
  （已禁止）不是组播组的成员。 此外，此地址不能是使用 GMRP 或 IGMP 动态学习的地址。

创建新条目

单击“新建条目”(New Entry) 按钮可向地址表中添加一个条目。 将打开“静态组播组态”(Static Multicast Configuration) 页面，在其中可进行必要的输入：

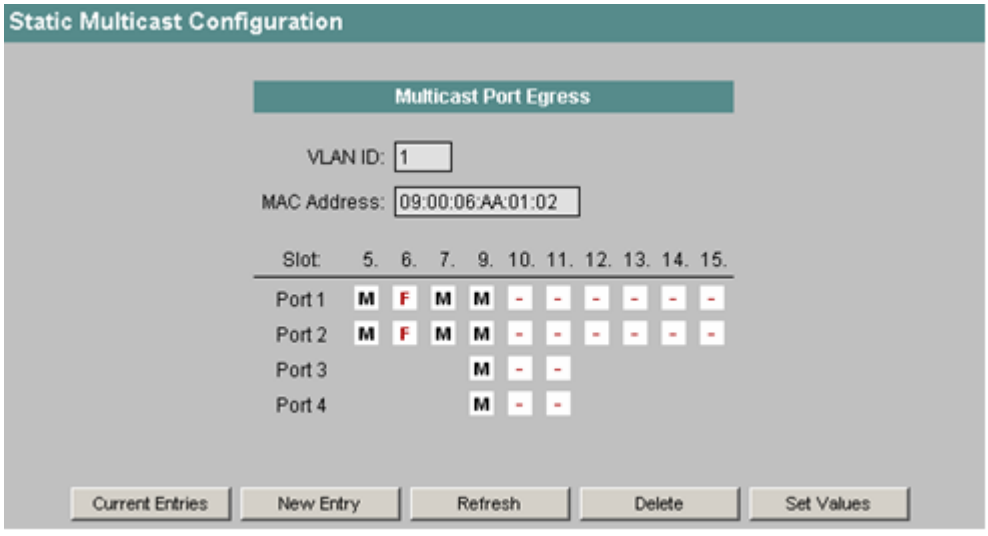


图 5-70　静态组播组态 (Static Multicast Configuration)

VLAN ID
输入 MAC 地址所属的 VLAN 的 ID。 如果未进行任何设置，则会将 VLAN ID 1 设置为基本设置。

MAC 地址 (MAC Address)
输入想要添加到地址表的 MAC 地址。

插槽/端口 (Slot/Port)
在此处选择端口应如何响应组播帧：

- **M**
  成员，通过此端口发送组播帧。
- **–**
  不是组播组的成员。 不通过此端口发送任何组播帧。
- **F**
  已禁止，不是组播组的成员。 此外，此地址不能是使用 GMRP 动态学习的地址。
- **#**
  端口无效。
- **?**
  该端口不是指定 VLAN 中的成员。

  说明
  对于组播地址，可以指定多个端口（目标节点）。

当前条目 (Current Entries)
单击此按钮可以返回到 MAC 地址列表。

新建条目 (New entry)
单击此按钮可在过滤表中创建新条目。

删除 (Delete)
单击此按钮可从过滤表中删除显示的条目。

更改地址条目

单击状态为 “静态”(static) 的 MAC 地址（地址列表中带下划线）可打开该地址的 “静态组播组态”(Static Multicast Configuration) 页面。 单击 “设置值”(Set Value) 来进行所需设置并确认输入。

命令行接口语法

表格 5-52　当前组播组 - CLI\SWITCH\MCAST>

命令	说明	注释
info	显示工业以太网交换机地址表的内容。	-
add <VLAN-ID> <MAC 地址> [<选项> [端口]]	向地址表中插入一个组播地址的静态条目。 以下缩写可用于 <选项> 参数： • – 不是组播组的成员。 不通过此端口发送任何组播帧。 • m 通过此端口发送组播帧。 • f 不是组播组的成员。 此外，此地址不能是使用 GMRP 动态学习的地址。 示例： • add 2 01:02:03:04:05:06 m 5.1-5.2 分配 VLAN-ID 2 的 MAC 地址，并且端口 5.1 和 5.2 是成员。 • add 3 01:02:03:04:05:06 m 为 VLAN-ID 3 创建一个条目，所有现有端口均为成员。	仅限管理员。
find [VLAN-ID] <MAC 地址>	在工业以太网交换机的地址表中搜索 MAC 地址。 还可以看到收到的具有此（目标）地址的帧将被发送到的端口。 如果不指定 VLAN-ID，则会浏览所有 VLAN 以查找指定的 MAC 地址。	-
edit <VLAN-ID> <MAC 地址> <选项> [端口]	更改地址表中的条目。 对于 <选项> 参数，可用的缩写范围与 add 命令的缩写范围相同。	仅限管理员。
delete <VLAN-ID> <MAC 地址>	从地址表中删除一个静态条目。	仅限管理员。

5.5.8.2 GMRP 组态 (GMRP Configuration)

启用 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，则不会对该端口进行任何注册，并且该端口无法发送 GMRP 帧。

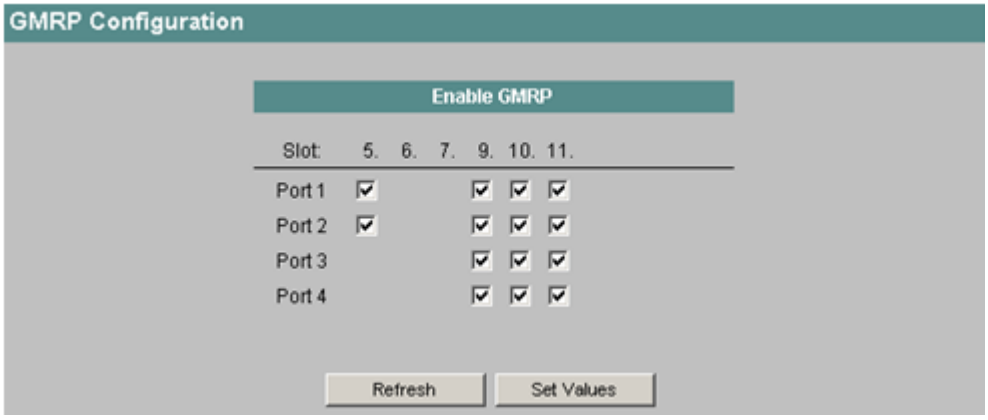


图 5-71 GMRP 组态 (GMRP Configuration)

命令行接口语法

表格 5-53 GMRP 组态 - CLI\SWITCH\MCAST>

命令	说明	注释
gmrpport [<E|D> [端口]]	为指定端口启用/禁用 GMRP 功能。 如果未指定任何端口，则会为所有端口启用/禁用 GMRP。	仅限管理员。

5.5.8.3 IGMP 组态 (IGMP Configuration)

指定老化时间

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 数据包更新，将从地址表中删除这些条目。 这适用于所有端口；在这种情况下，无法特定于端口进行组态。

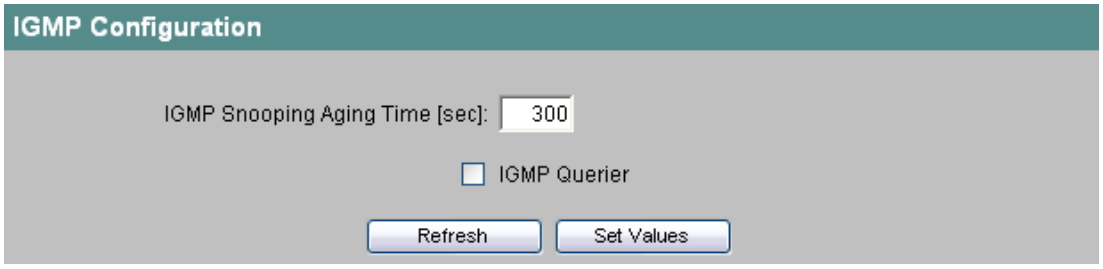


图 5-72 IGMP 组态 (IGMP Configuration)

IGMP 监听老化时间 [秒] (IGMP Snooping Aging Time [sec])
在此处输入老化时间（以秒为单位）的时间值。

IGMP 查询器 (IGMP Querier)
如果希望工业以太网交换机同时发送 IGMP 查询，则启用此选项。

命令行接口语法

表格 5-54 IGMP 组态 - CLI\SWITCH\MCAST\IGMP>

命令	说明	注释
igmptime [数字]	指定 IGMP 老化时间（以秒为单位）。 如果不带参数，此命令将显示 IGMP 老化时间。	仅限管理员。
igmpqry [E|D]	显示/设置 IGMP 查询启用	仅限管理员。

5.5.8.4 未知单播屏蔽掩码

阻止转发未知组播帧

在此菜单中，可阻止各端口转发未知组播帧。

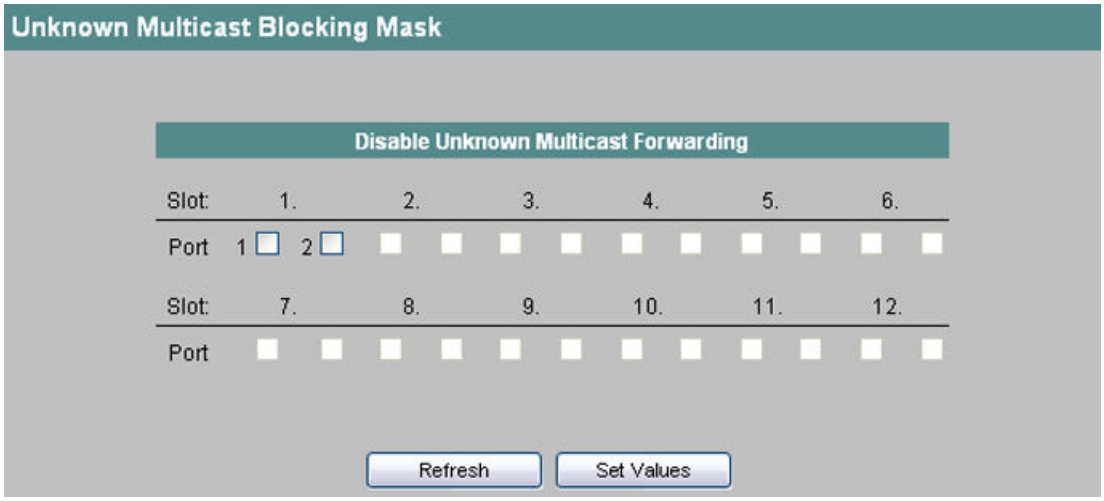


图 5-73 未知单播屏蔽掩码

禁用未知组播转发 (Disable Unknown Unicast Forwarding)

在此处指定将禁用未知组播帧转发的端口。

命令行接口语法

表格 5-55 未知组播屏蔽掩码 - CLI\SWITCH\>

命令	说明	注释
blkbmcast [<E|D> [端口]]	启用/禁用指定端口的组播屏蔽。	仅限管理员。

5.5.9 广播阻止掩码 (Broadcast Blocking Mask)

阻止转发广播帧

在此菜单中，可以阻止各个端口转发广播帧。

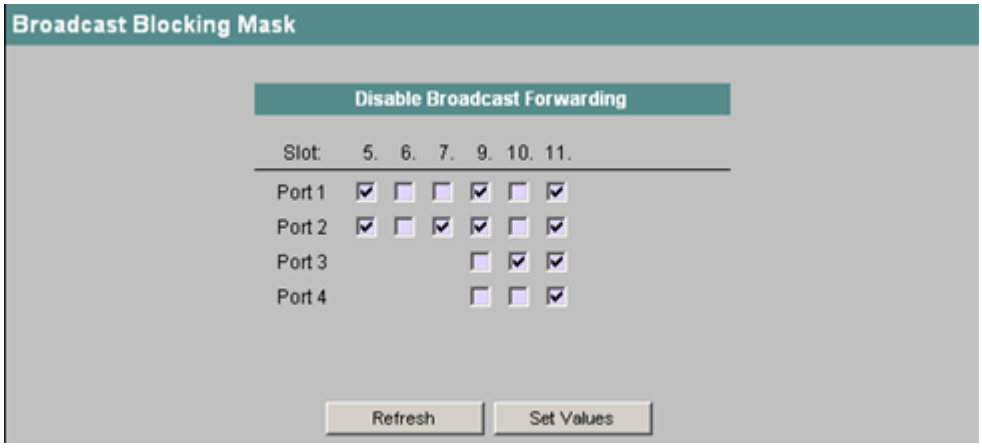


图 5-74 广播阻止掩码 (Broadcast Blocking Mask)

禁用广播转发 (Disable Broadcast Forwarding)
在此处指定将禁用转发广播帧的端口。

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，阻止可能导致数据通信的丢失。 只有在您确定不需要广播并且明确想要避免广播的情况下才在此处进行输入。

命令行接口语法

表格 5-56 广播阻止掩码 - CLI\SWITCH\>

命令	说明	注释
blkbcast [<E|D> [端口]]	对指定端口启用/禁用广播阻止。	仅限管理员。

5.5.10 快速学习

通过快速学习在某个端口动态学习到的 MAC 地址，将在该端口出现链路中断（例如，重新插上终端设备）后，立即从地址表中删除这些地址。 这表示交换机将被平常更快地识别端口分配是否有效。

可分别为每个端口指定快速学习。

端口组态

在如下所示的对话框中，单击要启用快速学习功能的端口的相关复选框。

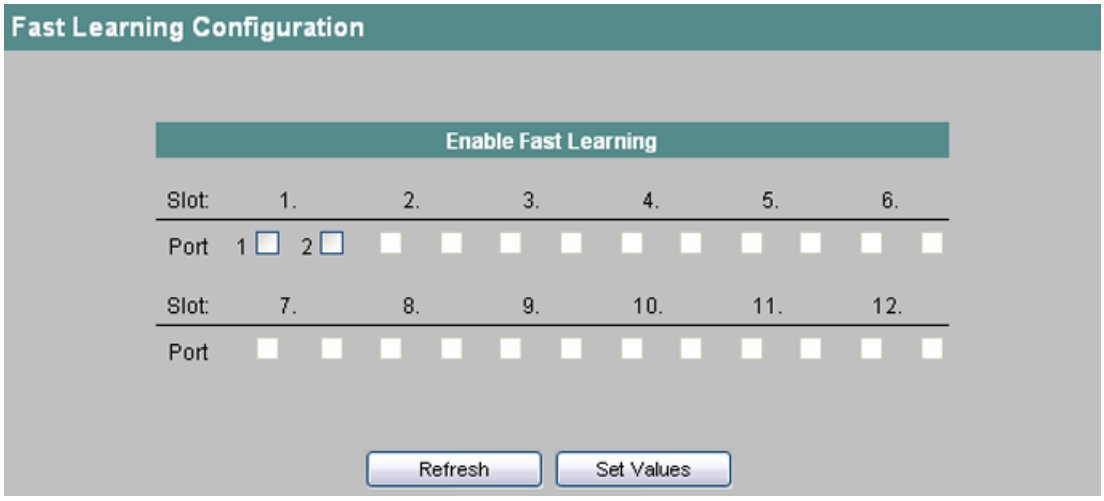


图 5-75 组态“快速学习”

命令行接口语法

表格 5-57 快速学习组态 - CLI\SWITCH\>

命令	说明	注释
fastlrn [<E|D> [端口]]	在相关端口启用/禁用快速学习。	仅限管理员。

5.5.11 负载限制组态 (Load Limits Configuration) (SCALANCE X414-3E)

限制进入帧的数量

在此对话框中，可以指定通过某个端口每秒接收的最大帧数。 出于硬件原因考虑，将多个端口组合成一个端口块。 但是，设置值 “数据包 [s]”(packets [s]) 对每个端口都有效。 您可以指定将应用输入限制值的帧的类别：

- 单播（目标查询失败）
- 组播
- 广播

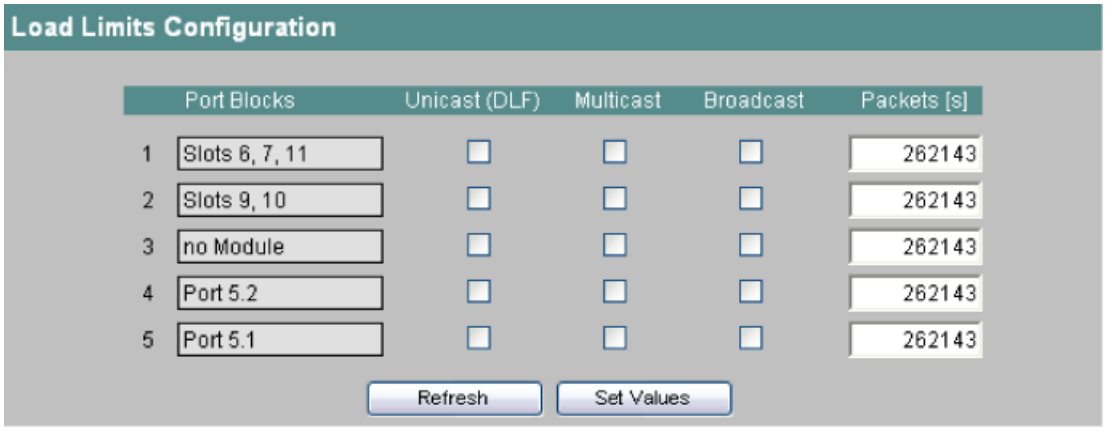


图 5-76 负载限制组态 (Load Limits Configuration)

端口块 (Port Blocks)

将端口分配给以下端口块；设置适用于一个端口块的所有端口：

- 端口块 1
  插槽 6、7 和 11 上的端口。
- 端口块 2
  插槽 9 和 10 上的端口。
- 端口块 3
  没有模块。
- 端口块 4
  插槽 5 上的端口 2。
- 端口块 5
  插槽 5 上的端口 1。

此列仅列出实际使用中的插槽。 各文本框均为只读。

单播 (DLF)、组播、广播 (Unicast (DLF), Multicast, Broadcast)
每秒最大帧数适用于对应复选框已选中的帧类别。

数据包 [s] (Packets [s])
端口块每秒接收的最大帧数。 超过此限值的数据包将被丢弃。

说明

环网端口会定期发送组播帧来检测线路中断。 因此对于包含环网端口的端口块，不应限制接收组播帧，以确保冗余管理器正确运行。

命令行接口语法

表格 5-58　负载限制组态 - CLI\SWITCH\LIMITS>

命令	说明	注释
info <块>	显示限制数据包的当前设置。 根据端口块来显示设置。 端口块定义如下： • 插槽 5 上的端口 1 • 插槽 5 上的端口 2 • 插槽 6、7 和 11 上的端口。 • 插槽 9 和 10 上的端口。 • 安装的扩展器的端口，也就是说，双绞线扩展器的插槽 12 和 13 的端口以及介质模块扩展器的端口 12 到 15。	如果指定了参数（块），CLI 将只显示所选值。
inmode <E|D> <E|D> <E|D> [块]	指定端口的进入限制模式。 E 或 D 的三个条目（以此顺序）对应于 • 单播 (DLF) • 组播 • 广播 端口块的定义方式与 info 命令的定义方式相同。 示例： • inmode E D E 1 对端口块 1 启用单播和广播，禁用组播。 • inmode D E D 对所有端口块禁用单播和广播、启用组播。	仅限管理员。 如果未指定参数（块），所有块均会被更改。
ingress <数据包> [块]	为每个端口块指定工业以太网交换机处理的最大进入数据包数。 端口块的定义方式与 info 命令的定义方式相同。	仅限管理员。 如果未指定参数（块），所有块均会被更改。

5.5.12 负载限制速率 (Load Limits Rates) (SCALANCE X-300/X408-2)

限制进入和离开数据的传输速率

此菜单显示了已组态的负载限值（每秒最大帧数）。 设置值对每个端口都有效。 您可以指定将应用输入限制值的帧的类别。 可通过单击相关条目进行组态。

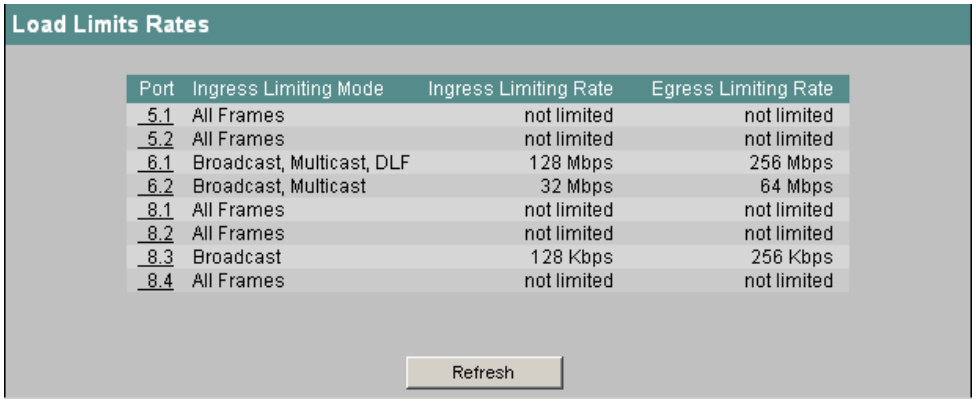


图 5-77 负载限制速率 (Load Limits Rates)

端口 (Port)
显示信息所关联的插槽和端口。 可以通过单击 “端口”(Port) 列中的相关条目来更改组态。

进入限制模式 (Ingress Limiting Mode)
显示进入数据的限值所关联的已组态帧类型。

进入限制速率 (Ingress Limiting Rate)
显示进入数据传输速率的已组态限值。

离开限制速率 (Ingress Limiting Rate)
显示离开数据传输速率的已组态限值。

说明
离开数据的限制始终与所有帧相关。

组态限制

如果单击“端口”(Port) 列中的条目，将打开“负载限制速率组态”(Load Limits Rates Configuration) 画面。

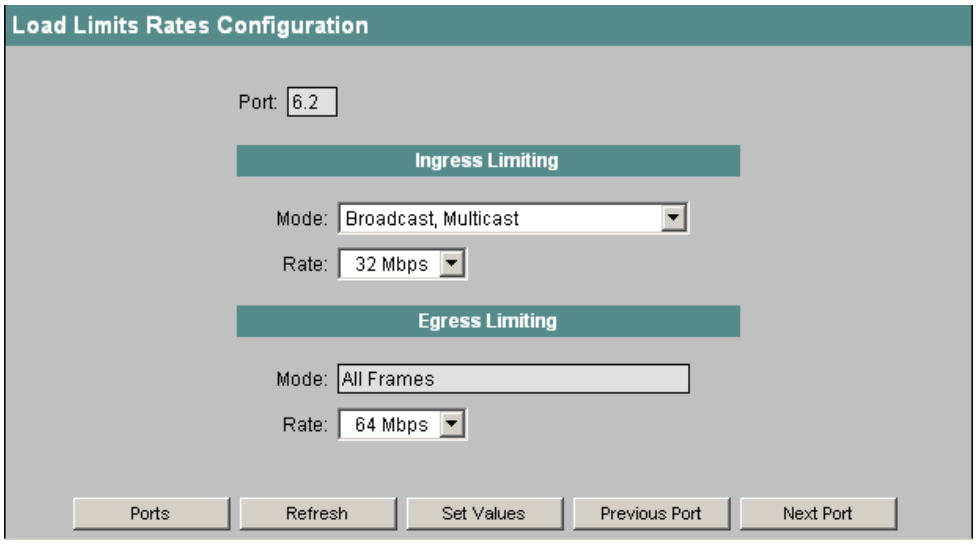


图 5-78　负载限制速率组态 (Load Limits Rates Configuration)

端口 (Port)
显示信息所关联的插槽和端口。 不能编辑此字段。

进入限制 (ingress limiting) 的**模式 (Mode)**
在此处指定进入数据的所选传输速率所关联的帧类别：

- 单播（目标查询失败）
- 组播
- 广播

进入限制 (ingress limiting) 的**速率 (Rate)**
在此处从可用值中选择进入数据的最大传输速率。 如果选择“不限制”(not limited)，则“进入限制模式”(Ingress Limiting Mode) 不起作用。

离开限制 (egress limiting) 的**模式 (Mode)**
指示离开数据的传输速率适用于所有帧。不能编辑此字段。

离开限制 (egress limiting) 的**速率 (Rate)**
在此处从可用值中选择离开数据的最大传输速率。

说明

环网端口会定期发送组播帧来检测线路中断。 因此对于环网端口，不应限制接收组播帧，以确保冗余管理器正确运行。

命令行接口语法

表格 5-59　负载限制组态 - CLI\SWITCH\LIMITS>

命令	说明	注释
info [端口]	显示限制数据包的当前设置。 根据端口来显示设置。	如果指定了参数（端口），CLI 将只显示所选值。
inmode <模式> [端口]	指定端口的进入限制模式。 <模式> 参数可为以下值： • B 广播 • BM 广播、组播 • BMU 广播、组播、单播 (DLF) • ALL 所有帧 示例： • inmode B 5.1 将端口 5.1 的限制模式设置为广播。	如果仅指定了 <模式> 参数，则会更改所有端口的设置。

命令	说明	注释
ingress <速率> [端口]	指定端口的进入限制速率。 <速率> 参数可为以下值： • 128k、256k、512k • 1m、2m、4m、8m、16m、32m、64m、128m、256m • k 代表千位每秒而 m 代表兆位每秒。 示例： • ingress 256k 5.1, 6.2 将端口 5.1 和 6.2 的进入限制速率设置为每秒 256 千位每秒。	如果仅指定了 <速率> 参数，则会更改所有端口的设置。
egress <速率> [端口]	指定端口的离开限制速率。 用于 <速率> 参数的缩写与用于 ingress 命令的缩写相同。 示例： • egress 2m 5.2, 8.1-8.4 将端口 5.2 和端口 8.1 到 8.4 的离开限制速率设置为 2 兆位每秒。	如果仅指定了 <速率> 参数，则会更改所有端口的设置。

5.5.13 VLAN

5.5.13.1 当前 VLAN 组态 (Current VLAN Configuration)

与节点的空间位置无关的网络定义

VLAN（虚拟 LAN）是可以被分配任何物理位置节点的网络。 组播帧和广播帧只能在逻辑网络结构设置的限制内，不能被发送到虚拟网络中。 因此，VLAN 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。

VLAN 的版本

有多种类型的 VLAN：

- 基于端口的 VLAN（2 层）
- 基于 MAC 地址的 VLAN（2 层）
- 基于 IP 地址的 VLAN（3 层）

工业以太网交换机支持基于端口的 VLAN。 这样便可以使用 GVRP 帧来设置工业以太网交换机的参数或对其进行组态。

如何组态基于端口的 VLAN

要组态 VLAN，请按以下步骤操作：

1. 指定各个 VLAN 的节点。
2. 为每个节点和每个工业以太网交换机分配 VLAN-ID，并指定要建立连接的设备以及通过哪个端口建立连接。
3. 在工业以太网交换机上设置以下组态：
   - 定义此设备上使用的所有 VLAN。
   - 指定哪个端口支持哪个 VLAN。
   - 指定如何处理进入和离开端口的帧（进入/离开过滤器）。
   - 指定通过端口发送帧时是否带标记。
   - 决定是以静态方式组态工业以太网交换机，还是使用 GVRP 以动态方式组态工业以太网交换机。

VLAN 的重要规则

组态和运行 VLAN 时，确保遵守以下规则：

- 使用 VLAN 或组播组时，要实现 300 ms 内的切换时间，必须以静态方式将所有环网端口创建为所有 VLAN 和所有组播组中的成员。
- VLAN-ID 为“0”的帧（例如，只有优先级标记的帧）将处理为无标记的帧。
- 默认情况下，工业以太网交换机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。 该基本设置很有必要，因为并不总是能确定一个节点是否能解释带标记的帧。
- 默认情况下，支持 VLAN 的工业以太网交换机的所有端口的参数分配均为 VLAN 标识符 1（默认 VLAN）。

说明

VLAN-ID 500 保留供将来使用，且已经组态。

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）。

VLAN 及工业以太网交换机

“当前 VLAN 组态”(Current VLAN Configuration) 页面显示 VLAN 组态的当前端口分配。

切换页面
单击“>>”或“<<”可向后或向前翻页。

在第二页，您将看到已建立的所有链路汇聚，而不是端口。

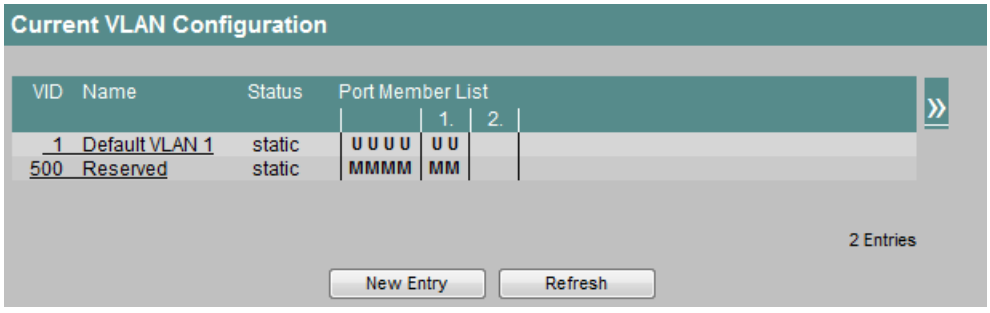


图 5-79　当前 VLAN 组态 - 第 1 页

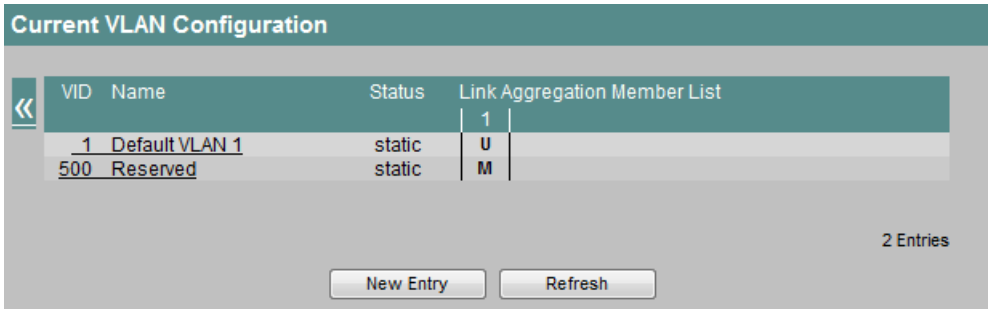


图 5-80　当前 VLAN 组态 - 第 2 页

表的四个区域显示以下信息：

VID
VLAN 标识符 (VID)，一个介于 1 到 4094 之间的数字。

名称 (Name)
定义 VLAN 时分配此名称。 此名称仅提供信息，对组态没有影响。

如果某一条目显示静态状态，则可以单击 VID 或名称打开 “静态 VLAN 组态”(Static VLAN Configuration) 页面。 在此处可以组态各个端口以指定端口所属的 VLAN。 但是，只能在创建新条目时指定 VLAN ID 和名称，并且以后不能再进行修改。 如果想要更改某个条目，必须先删除该条目，然后再次创建该条目，并包括所需的更改。

状态 (Status)
显示端口过滤器表中条目的类型。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，仅当工业以太网交换机启用 GVRP 时，此条目才可用。

端口成员列表 (Port Member List)
显示为插槽或端口设置的 VID。 条目的含义如下：

- "-""-"
  该端口不是指定 VLAN 的成员。
- M
  （成员）该端口是 VLAN 的成员，发送的帧中包括 VLAN 标记，其 VID 在第一列中指定。
- R
  （已注册）该端口是 VLAN 的成员，由 GVRP 帧注册。
- U
  （无标记）该端口是 VLAN 的成员，发送的帧不包括 VLAN 标记。
  U（红色）
  此 VLAN 未组态为端口 VLAN。 发送的帧不包含 VLAN 标记。
- F
  （已禁止）该端口不是 VLAN 的成员，在此端口不能通过 GVRP 动态注册 VLAN。
- G
  （访客 VLAN）该端口是访客 VLAN 的成员。 使用“访客 VLAN”身份验证动态注册过该端口，请参见“802.1x 端口组态 (页 183)”部分。
- A
  （经身份验证）该端口是 VLAN 的成员。 使用“MAC 身份验证”方法动态注册过该端口，请参见“802.1x 端口组态 (页 183)”部分。

对于新定义，所有端口的标识符均为“-”。

链路汇聚成员列表 (Link Aggregation Member List)
显示链路汇聚的设置。条目的含义如下：

- "-"
  该端口不是链路汇聚的成员。
- M
  （成员）该端口是链路汇聚的成员。

VLAN 组态 (VLAN configuration)

单击“新建条目”(New Entry) 按钮可指定当使用 VLAN 时如何通过端口发送帧。 将打开“静态 VLAN 组态”(Static VLAN Configuration) 页面，在其中可进行必要的输入：

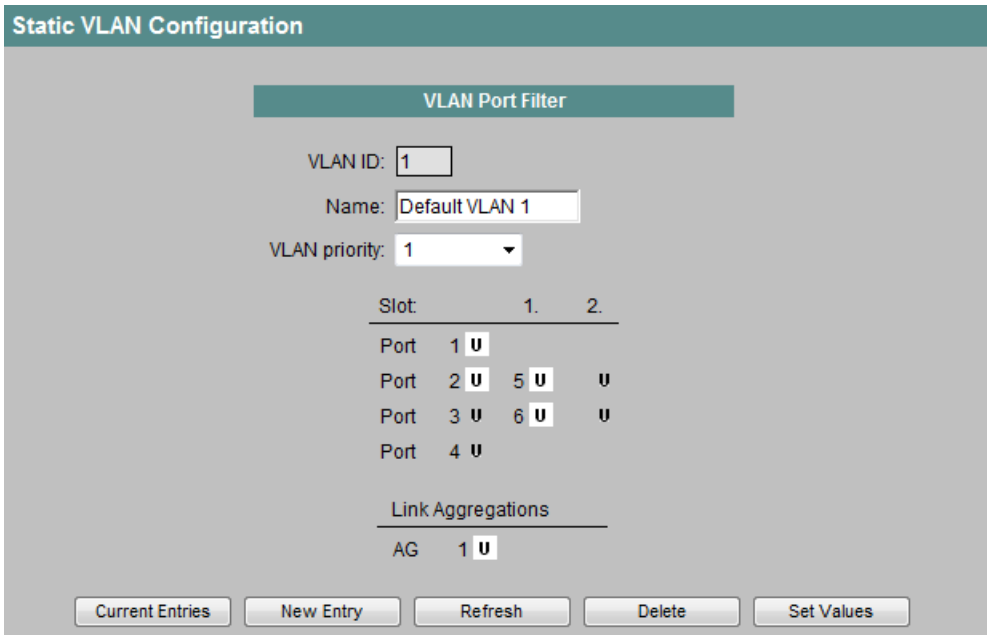


图 5-81 静态 VLAN 组态 (Static VLAN Configuration)

VLAN ID

在此处输入 VLAN 的 ID。 VLAN-ID 是介于 1 到 4094 之间的数字。

名称 (Name)

在此处输入 VLAN 的名称。 名称对组态没有影响。

VLAN 优先级 (VLAN priority)

在此选择为 VLAN 强制执行的优先级。 所选的优先级将输入此 VLAN 的所有进入帧中。 交换机将根据所选优先级转发进入帧。

如果选择“非强制”(Do not force)，帧的优先级将保持不变。

插槽/端口 (Slot/Port)

在此处可以指定发送帧时端口对指定的 VLAN 如何响应。 默认情况下，各个框均输入“-”。 通过重复单击，可从一个条目移动到下一个条目。 条目的含义如下：

- **“-”**
  该端口不是指定 VLAN 的成员。
- **M**
  （成员）该端口是 VLAN 的成员，发送的帧中包括 VLAN 标记，其 VID 在第一行中指定。

- **R**
  （已注册）该端口是 VLAN 的成员，由 GVRP 帧注册。
- **U**
  （无标记）该端口是 VLAN 的成员，发送的帧不包括 VLAN 标记。 如果通过此端口对不支持 VLAN 标记的终端设备进行寻址，则使用 U。
- **F**
  （已禁止）该端口不是 VLAN 的成员，在此端口不能通过 GVRP 动态注册 VLAN。
- **T**
  （中继端口）端口将自动成为所有已组态 VLAN 的成员并且仅发送有标记的帧。

说明

如果端口针对某个VLAN 被定义为"F"（已禁止），则如果端口为中继端口，将阻止该VLAN。已禁止的优先级高于中继。

当前条目 (Current Entries)
单击此按钮可以返回到 VLAN 列表。

新建条目 (New Entry)
单击此按钮可以对新 VLAN 进行设置。

设置值 (Set Values)
单击此按钮可存储已在工业以太网交换机的组态中输入的值。

删除 (Delete)
单击此按钮可删除显示的组态。

VLAN 组态和身份验证

如果要使用"802.1x"身份验证方法对端口进行身份验证，则需要组态一个 VLAN，再将端口分配给它。 若要在"802.1x"身份验证失败后使用"MAC 身份验证"或"访客 VLAN"对端口进行身份验证，则将该端口定义为"A"或"G"。

若要使用"MAC 身份验证"方法对端口进行身份验证且"允许的 VLAN 分配"(VLAN Assignment Allowed) 选项被禁用，则不会将 VLAN 分配给该端口（"-"）。 在这种情况下，需要首先分配 VLAN。

若要使用"MAC 身份验证"方法对端口进行身份验证且"允许的 VLAN 分配"(VLAN Assignment Allowed) 选项已启用，则将该端口定义为"A"。

命令行接口语法

表格 5-60　当前 VLAN 组态 - CLI\SWITCH\VLAN>

命令	说明	注释
info	显示当前组态的VLAN及其与各个端口的关系。	
add <VLAN-ID> [<选项> [端口]]	插入新 VLAN。 以下缩写可用于 <选项> 参数。 • - 该端口不是 VLAN 的成员。 • m 该端口是 VLAN 的成员，发送的帧包含 VLAN 标记。 • u 该端口是 VLAN 的成员，发送的帧不含 VLAN 标记。 • f 该端口不是 VLAN 的成员，且不能被 GVRP 动态组态为属于 VLAN。 • t 端口将自动成为所有已组态 VLAN 的成员并且仅发送有标记的帧。 示例： • add 2 创建 VLAN-ID 为 2、默认名称为 "Vlan 2"的条目。 • add 4 m 创建 VLAN-ID 为 4、默认名称为 "Vlan4"的条目。 所有现有端口均为成员。	仅限管理员。

命令	说明	注释
edit <VLAN-ID> [<选项> [端口]]	更改 VLAN 中端口的成员资格。 用于 <选项> 参数的缩写与用于 add 命令的缩写相同。 示例： • edit 3 - 10.1 从 ID 为 3 的 VLAN 中移除端口 10.1。	仅限管理员。
name <VLAN-ID> <名称>	更改 VLAN 的名称。	仅限管理员。
delete <VLAN-ID>	从工业以太网交换机的组态中删除具有指定 ID 的 VLAN。	仅限管理员。

5.5.13.2 VLAN 端口参数 (VLAN Port Parameters)

处理接收到的帧

此页面显示工业以太网交换机处理接收到的帧时所依据的规则：

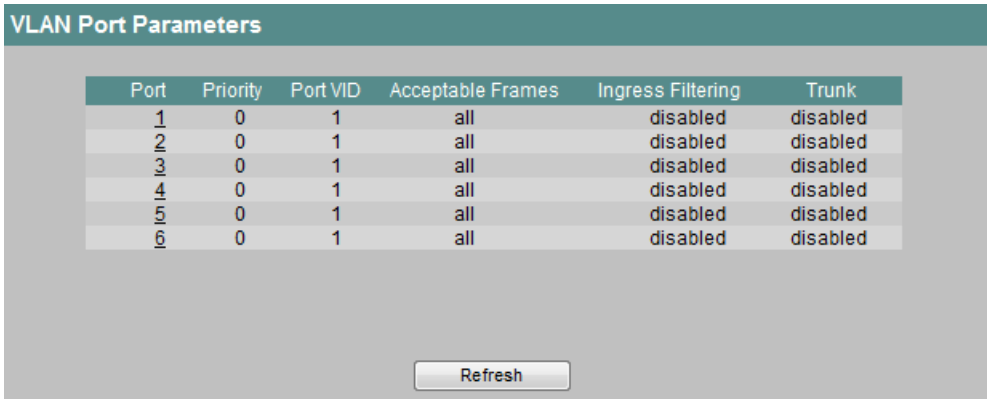


图 5-82 VLAN 端口参数 (VLAN Port Parameters)

表的五个列显示以下信息：

端口 (Port)
该列显示后面信息所涉及的插槽和端口。

优先级 (Priority)
VLAN 标记中使用的 CoS（服务类别）优先级。如果接收到无标记的帧，可根据端口为其分配优先级。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）。有关帧标记的详细信息，请参见附录 C。

端口 (Port VID)
如果接收到的帧没有 VLAN 标记，则会使用此处指定的 VLAN-ID 添加标记，然后按照适用于端口的交换机规则发送该帧。
如果端口的 VLAN-ID 已使用"MAC 身份验证"方法或"访客 LAN"动态定义过，则会自动组态该"端口 VID"。

可接受帧 (Acceptable Frames)
此列指定如何处理无标记帧。可能的选项如下：

- tagged frames

  工业以太网交换机将丢弃所有无标记帧。

- untagged frames

  工业以太网交换机将丢弃所有带标记帧。

- all

  工业以太网交换机转发所有帧。

进入过滤 (Ingress Filtering)
在此处可查看是否评估 (entry enabled/entry disabled) 接收到的帧的 VID (entry enabled/entry disabled)。

中继 (Trunk)
在此处可指定是否将端口组态为中继端口 (entry enabled/entry disabled)。

组态 VLAN 的端口

单击“端口”(Ports) 列中的一个条目后，将切换到用于组态接收帧的端口属性的页面：

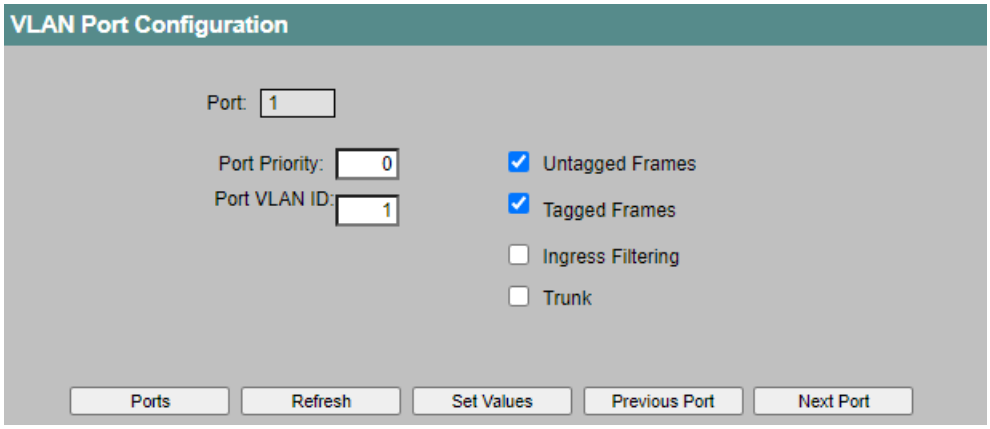


图 5-83　VLAN 端口组态 (VLAN Port Configuration)

端口 (Port)
该只读框显示与此页面上的信息相关的插槽和端口号。

端口优先级 (Port Priority)
分配给无标记帧的优先级。

端口 VLAN ID (Port VLAN ID)
分配给无标记帧的 VLAN ID。
如果端口的 VLAN-ID 已使用“MAC 身份验证”方法或“访客 LAN”动态定义过，则会自动组态该“端口 VLAN ID”。

无标记帧 (Untagged Frames)
如果启用此选项，设备会丢弃所有带标记帧，而转发所有无标记帧及具备优先级的帧（带优先级标记的帧）。否则，按照组态应用转发规则。

带标记帧 (Tagged Frames)
如果启用此选项，设备会丢弃所有无标记帧。设备转发所有带标记帧。否则，按照组态应用转发规则。

进入过滤 (Ingress Filtering)
如果启用此选项，则根据接收到的帧的 VLAN-ID 决定如何转发这些帧：要使用接收到的帧的 VLAN-ID，必须在工业以太网交换机上创建 VLAN，并且端口必须是 VLAN 的成员。
具有组态的端口 VLAN-ID 的帧在收到后将被转发，具有不同 VLAN-ID 的帧在收到后将被丢弃。
不带 VLAN-ID 的帧在收到后将被转发到端口 VLAN-ID。

中继 (Trunk)
如果启用此选项，则端口为中继端口。中继端口将自动成为所有已组态 VLAN 的成员并且仅发送有标记的帧。

如果禁用此选项，则将恢复启用此选项之前存在的 VLAN 组态。

命令行接口语法

表格 5-61　VLAN 端口参数 - CLI\SWITCH\VLAN\PORTS>

命令	说明	注释
info	显示端口总览和相应的 VLAN 设置。	-
vid [<VLAN-ID> [端口]]	在指定端口接收到的不带 VLAN 标记的帧将被指定给带 <VLAN-ID> 的 VLAN 标记。	仅限管理员。
prio [<0...7> [端口]]	指定端口的优先级。	仅限管理员。
ingress [<E|D> [端口]]	启用/禁用对接收到的帧的 VID 的评估。	仅限管理员。
untagged [<E|D> [端口]]	指定处理不带 VLAN 标记的帧。 启用此命令时，不带 VLAN 标记的帧会被接受，否则不被接受。	仅限管理员。
tagged [<E|D> [端口]]	指定处理带有 VLAN 标记的帧。 启用此命令时，带有 VLAN 标记的帧会被接受，否则不被接受。	仅限管理员。
trk [<E|D> [端口]]	启用/禁用中继属性。 中继端口将自动成为所有已组态 VLAN 的成员并且仅发送有标记的帧。	仅限管理员。

5.5.13.3 GVRP 组态 (GVRP Configuration)

启用 GVRP 功能

使用 GVRP 帧，终端节点或交换机可在工业以太网交换机的某一端口注册特定 VID。 可以在“GVRP 组态”(GVRP Configuration) 页面上为各个端口启用 GVRP 功能。

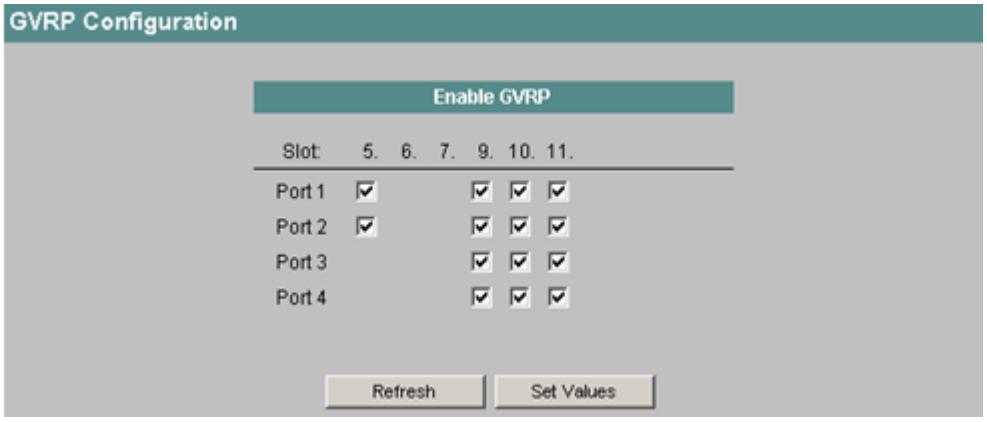


图 5-84 GVRP 组态 (GVRP Configuration)

启用 GVRP (Enable GVRP)
如果选择某个选项，工业以太网交换机允许在相关端口通过 GVRP 帧注册 VLAN。 工业以太网交换机也可以通过此端口发送 GVRP 帧。

命令行接口语法

表格 5-62 GVRP 组态 - CLI\SWITCH\VLAN>

命令	说明	注释
gvrpport [<E|D> [端口]]	启用/禁用通过 GVRP 针对指定端口动态注册 VLAN。	仅限管理员。

5.5.13.4 VLAN 学习

在 VLAN 中学习 MAC 地址

在此页面上，可以为每个端口组态“学习到所有 VLAN”(Learn to all VLANs) 选项。

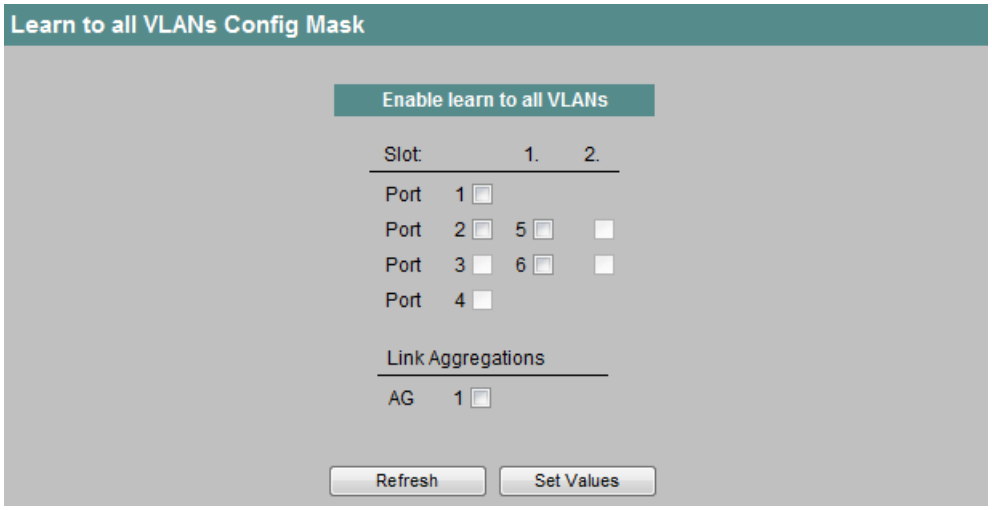


图 5-85 学习到所有 VLAN 组态掩码

启用学习到所有 VLAN

如果为端口启用此选项，则端口接收到的 MAC 地址会自动学习到所有已组态的 VLAN 中。

命令行接口语法

表格 5-63 学习到所有 VLAN - CLI\SWITCH\VLAN>

命令	说明	注释
lrnallv [<E|D> [端口]]	启用/禁用所有已组态 VLAN 中 MAC 地址的自动学习。	仅限管理员。

5.5.13.5 X-300 VLAN 端口优先级映射

VLAN 端口优先级映射

此页面显示端口发送已接收帧的优先级。

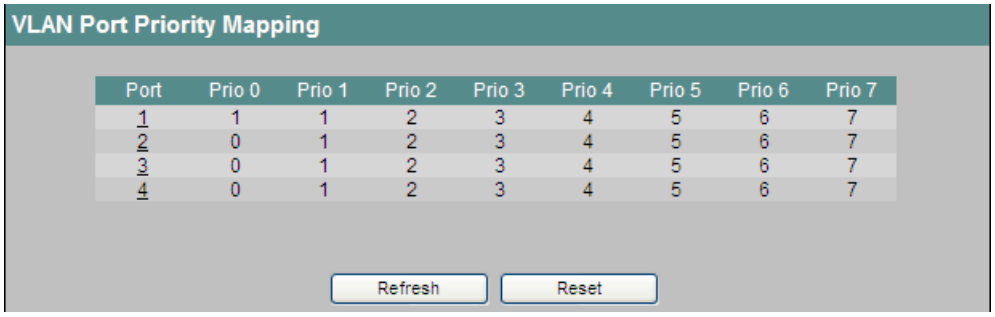


图 5-86 VLAN 端口优先级映射

端口 (Port)

后面信息所涉及的端口。

优先级 0 (Prio 0)

显示以优先级 0 接收的帧的发送优先级。

例如，对于端口 1 而言，图中的设置表示以优先级 0 接收的帧会以优先级 1 发送。

“优先级 1”(Prio 1) 到 “优先级 7”(Prio 7) 列可以完全相同的方式理解。

VLAN 优先级重新映射组态

单击“VLAN 端口优先级映射”(VLAN Port Priority Mapping) 页面上的一个端口，将显示“VLAN 优先级重新映射组态”(VLAN Priority Remap Configuration) 画面。

可以根据接收帧时的优先级，更改发送帧时所用的优先级。

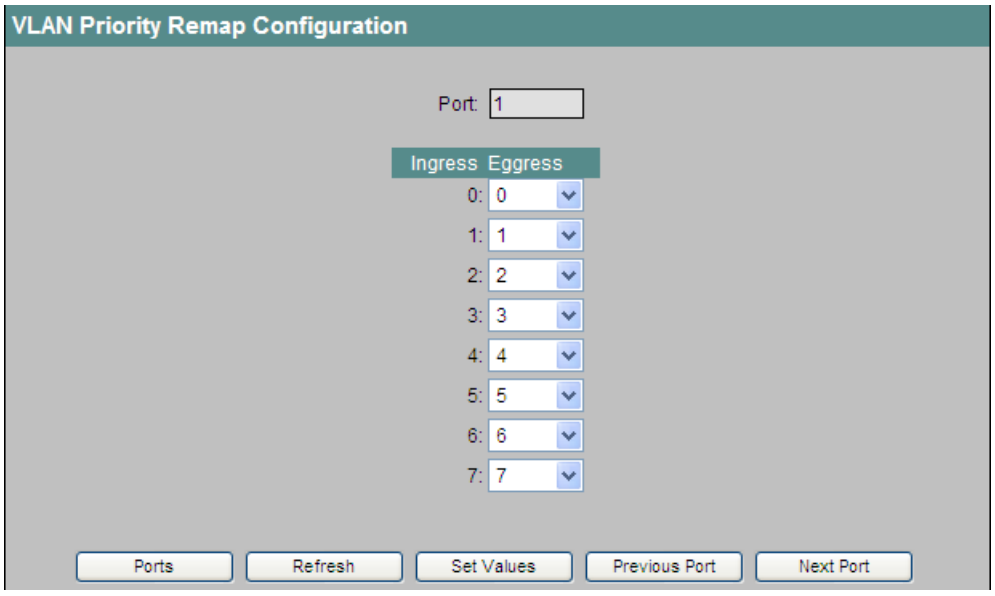


图 5-87 VLAN 优先级重新映射组态

端口 (Port)

该只读框显示与此页面上的信息相关的端口号。

进站 (Ingress)

接收帧时所用的优先级。

出站 (Egress)

发送帧时所用的优先级。

命令行接口语法

表格 5-64 VLAN 端口优先级映射 - CLI\SWITCH\VLAN\PRIO>

命令	说明	注释
info	显示端口发送已接收帧的优先级。	-
remap [端口] [<0..7><0..7>]	更改接收帧的优先级以进行发送。	仅限管理员。

命令	说明	注释
复位	重设接收帧的优先级。 接收时的优先级随即与发送时的优先级一致。	仅限管理员。
vprio <VID> [noforce | <0-7>]	根据接收帧所属的VLAN 更改其优先级。 将通过更改的优先级发送帧。 在基本状态"noforce"下，帧的优先级保持不变。	仅限管理员。

5.5.14 STP/RSTP

5.5.14.1 生成树组态 (Spanning Tree Configuration)

避免在冗余连接中形成环路

生成树协议 (STP) 允许创建在两个站之间有多个连接的网络结构。STP 只允许使用一条路径并且禁止其它（冗余）端口进行数据通信。这样可防止在网络中形成环路。如果发生网络中断，则会找到一条备用路径用于传送数据。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

交换机彼此之间交换称为 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。根网桥是控制所有相关组件的生成树算法的网桥。BPDU 还可引起网桥端口的状态变更。

快速生成树

快速生成树协议建立在生成树协议基础之上。使用 RSTP 时，设备将在无故障正常运行期间收集备用路由信息，以此优化网络的重新组态时间。生成树的典型重新组态时间介于 20 到 30 秒之间。而快速生成树的重新组态时间为大约一秒。这是通过以下方法实现的：

- 边缘端口
  定义为边缘端口的端口在连接建立后直接切换到激活状态。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。
- 点对点（在两个相邻交换机之间直接通信）

  通过直接连接两个交换机，可以立即进行状态变更（重新组态端口），而无任何延迟。
- 备用端口（根端口的替代端口）
  备用端口用作根端口的替代端口。如果失去与根网桥的连接，通过重新组态，工业以太网交换机可以通过备用端口建立连接，且无任何延迟。
- 过滤表

  在快速生成树中，受重新组态影响的端口会立即从过滤表中删除。另一方面，在生成树中，删除端口的时间由端口进入过滤表的时间决定。
- 对事件的反应

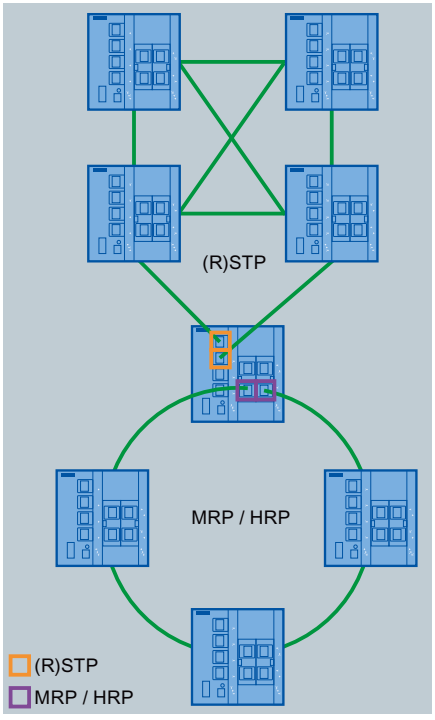
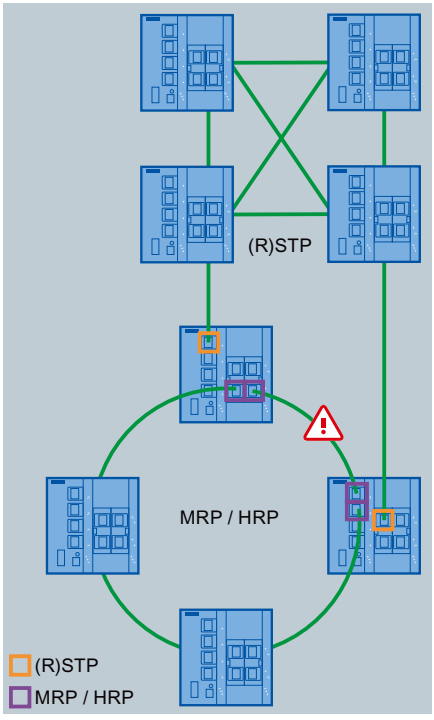
  快速生成树可无任何延迟地对事件（例如连接中止）做出反应。不用像在生成树中一样等待计时器。

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。

（快速）生成树、介质冗余和被动侦听

可使用以下选项将 (R)STP 网段连接到 MRP 或 HRP 环网：

- 使用 (R)STP 连接到环网中的一台设备
  可以在设备不同端口上启用介质冗余方法 MRP 或 HRP 的同时启用 (R)STP（请参见图 ①“允许的环网冗余 (R)STP 连接”）。
  不可使用 (R)STP 连接到环网的多台设备。由于 (R)STP BPDU 不通过 MRP 或 HRP 环网转发，因此造成帧循环传送和数据通信故障（请比较图 ②“不允许的环网冗余 (R)STP 连接”）。

① 允许的环网冗余 (R)STP 连接	② 不允许的环网冗余 (R)STP 连接
	

- 在环网中的各种设备上采用被动侦听
  如果想要将 (R)STP 网段连接到 MRP 或 HRP 环网的多个设备，则需要在环网的所有设备上启用被动侦听并禁用 (R)STP。由于被动侦听支持 (R)STP BPDU 的转发，因此不存在帧循环情况。

说明

如果使用 WBM 或 CLI 同时启用 (R)STP 和被动侦听，则不会激活被动侦听。

生成树组态与工业以太网交换机

在“生成树组态”(Spanning Tree Configuration) 对话框中显示和设置生成树协议的参数：

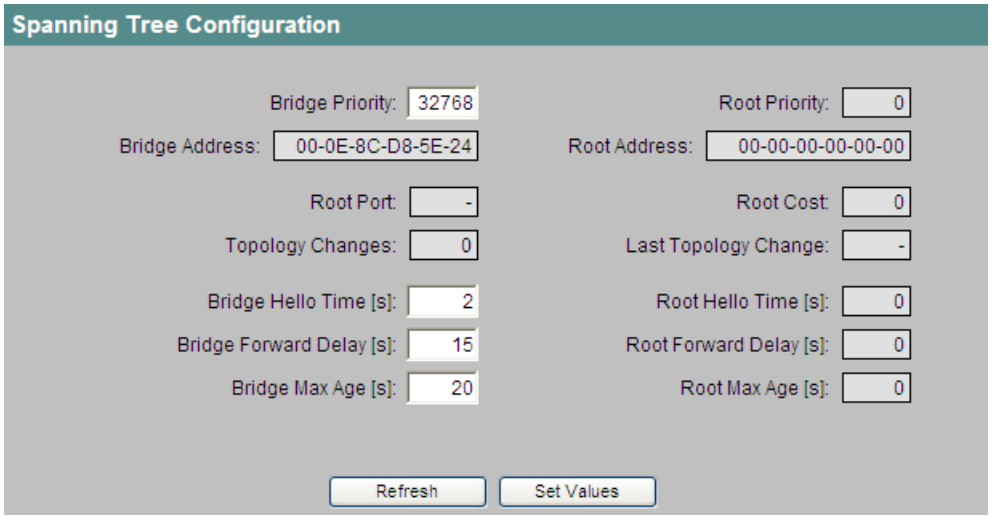


图 5-88　生成树组态 (Spanning Tree Configuration)

页面的左侧显示工业以太网交换机的组态。右侧显示根网桥的组态，该组态可从工业以太网交换机接收到的生成树帧获得。因此此处显示的数据是只读数据。如果工业以太网交换机是根网桥，则左右两侧显示的信息相匹配。参数的含义如下：

网桥优先级 (Bridge Priority)/根优先级 (Root Priority)
哪个交换机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。如果网络中有多个交换机具有相同优先级，则 MAC 地址数值最小的交换机将成为根网桥。这两个参数（网桥优先级和 MAC 地址）一起形成网桥标识符。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 65,535。

网桥地址 (Bridge Address)/根地址 (Root Address)
工业以太网交换机或根网桥的 MAC 地址。

根端口 (Root Port)
设备与根网桥通信时所使用的端口。

拓扑变更 (Topology Changes)/上次拓扑变更 (Last Topology Change)
该工业以太网交换机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，显示自上次重新组态以来的持续时间（以分钟为单位，在数字后面附加 m）。

网桥呼叫时间 (Bridge Hello Time)/根呼叫时间 (Root Hello Time)
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。

网桥转发延迟 (Bridge Forward Delay)/根转发延迟 (Root Forward Delay)
网桥不会立即使用新组态数据，而是在“转发延迟”(Forward Delay) 参数中指定的时间段之

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”(Bridge Max Age) 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”。此参数的默认值为 20。

命令行接口语法

表格 5-65　生成树组态 - CLI\SWITCH\STP>

命令	说明	注释
info	显示当前生成树组态。	-
bprio [0...61440]	指定工业以太网交换机的网桥优先级。	仅限管理员。
hellotm [1 ... 10]	指定两个 BPDU 之间的时间间隔，以秒为单位。	仅限管理员。
fwddelay [4 ... 30]	指定组态信息有效性的延迟时间（以秒为单位指定）。	仅限管理员。 默认值：15 s
maxage [6 ... 40]	组态信息的最大老化时间。	仅限管理员。 默认值：20 s

5.5.14.2　生成树端口参数 (Spanning Tree Port Parameters)

特定于端口的参数

此页面显示当前端口参数，这些参数由用户设置或由工业以太网交换机自动功能设置。

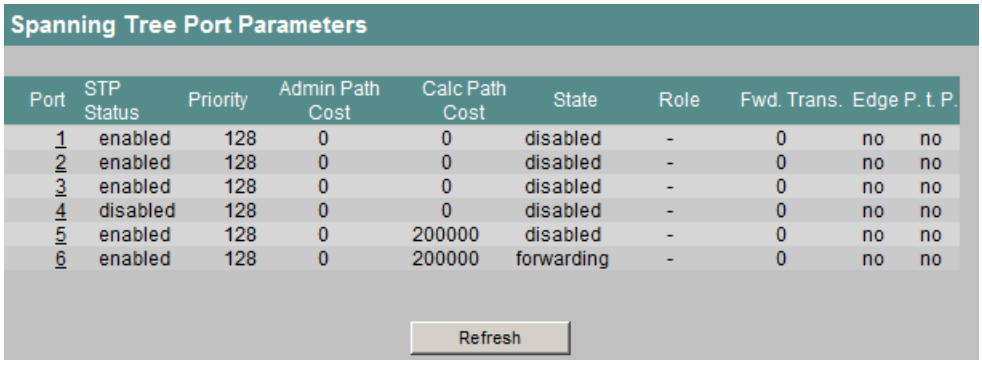


图 5-89　生成树端口参数 (Spanning Tree Port Parameters)

该表格包括以下列：

端口 (Port)
指定信息所关联的插槽和端口。

STP 状态 (STP Status)
显示对该端口是启用还是禁用生成树。

优先级 (Priority)
如果由生成树计算出的路径可能经过交换机的多个端口，则选择优先级最高的端口（也就是此参数值最小的端口）。可指定的优先级值范围为 0 到 255；默认值为 128。

管理路径开销 (Admin Path Cost)

显示要使用的路径开销的值。

计算路径开销 (Calc Path Cost)

如果管理路径开销值大于 0，则该值将作为计算出的路径开销值。
如果管理路径开销值等于 0，则将自动计算计算出的路径开销值。成本路径的计算很大程度上取决于传输速度。

可达到的传输速度越高，管理路径开销的值就应该越低。

快速生成树的典型路径开销值如下：

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

状态 (State)
显示端口的当前状态。可能的状态如下：

- 已禁用 (disabled)

  该端口仅接收，未包括在 STP 组态中。

- 阻止 (blocking)

  在阻止模式下，接收 BPDU。

- 侦听 (listening)

  在此状态下，接收和发送 BPDU。端口包括在生成树算法中。

- 学习 (learning)

  转发状态之前的阶段，端口再次主动学习拓扑（换句话说，节点寻址）。

- 转发 (forwarding)

  在重新组态时间后，端口在网络中再次激活；端口接收和转发数据帧。

转发转换 (FWD Transitions)
指定从侦听状态转换到转发状态的次数。

边缘 (Edge)

此列中有可能有以下条目：

- 是 (yes)

  一个边缘端口连接到此端口。

- 否 (no)
  此端口上有生成树或快速生成树设备。

  如果连接了边缘端口，工业以太网交换机可以更快速地切换端口，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“否”(no) 设置。

点对点 (P.t.P.)

通过此端口将两个 RSTP 兼容的网络组件连接在一起时，存在一个点对点链路。有 2 种可能状态：

- 是 (Yes)

  存在点对点链路。

- 否 (No)

  没有点对点链路。

命令行接口语法

表格 5-66 （快速）生成树端口参数 - SWITCH\STP\PORTS>

命令	说明	注释
info	显示端口总览和相应的快速生成树设置。	-

5.5.14.3 生成树端口组态

针对（快速）生成树组态端口

说明

不能在环网端口以及备用端口上启用 (R)STP。

如果单击“生成树端口参数”(Spanning Tree Port Parameters) 页面的“端口”(Port) 列中的端口名称，将打开“生成树端口组态”(Spanning Tree Port Configuration) 页面：

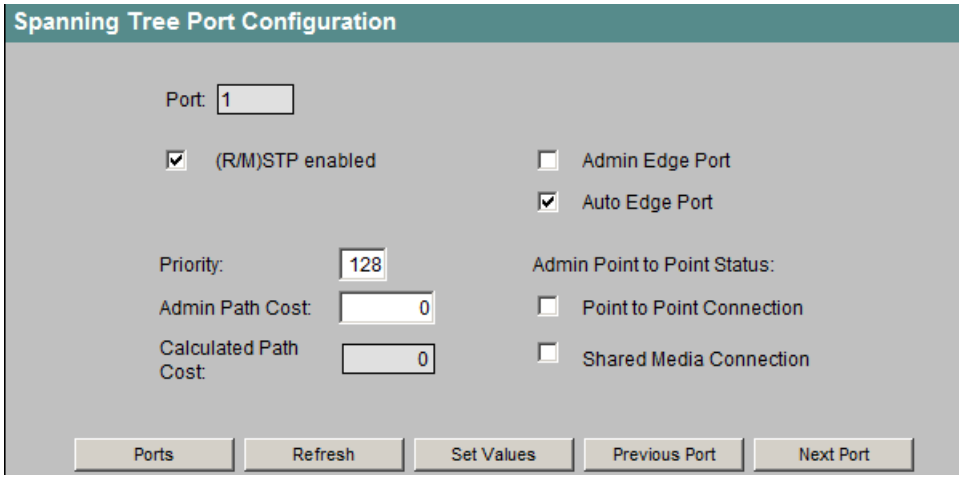


图 5-90 生成树端口组态

端口 (Port)

“端口”(Port) 显示框中显示所选端口。

启用 (R)STP ((R)STP enabled)

如果想要端口使用（快速）生成树协议，则启用此复选框。

管理边缘端口 (Admin Edge Port)

当此端口上有终端设备时请启用此选项。否则只要修改到此端口的链路，就将触发对网络的重新组态。

自动边缘端口 (Auto Edge Port)

如果想要自动检测此端口上连接的终端设备，则启用此选项。

与被动侦听功能结合使用时（请参见相关工业以太网交换机的操作说明），此选项非常有用，因为如果主链路出现故障，重新组态的速度更快。

优先级 (Priority)

在“优先级”(Priority) 输入框中输入端口优先级值。

允许的值：0 到 255

管理路径开销 (Admin Path Cost)

在此处可以手动设置每个端口要使用的路径开销值。

计算路径开销 (Calc Path Cost)

如果管理路径开销值大于 0，则该值将作为计算出的路径开销值。
如果管理路径开销值等于 0，则将自动计算计算出的路径开销值。成本路径的计算很大程度上取决于传输速度。

可达到的传输速度越高，管理路径开销的值就应该越低。

快速生成树的典型路径开销值如下：

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

管理点对点状态 (Admin Point to Point Status)
有三种可能设置：

- 不选择“点对点连接”(Point to Point Connection) 和“共享介质连接”(Shared Media Connection)：
  自动检测点对点。如果端口被设置为半双工，则不认为是点对点链路。
- 选择“共享介质连接”(Shared Media Connection)：

  不管是否为全双工连接，都不认为是点对点链路。
- 选择“点对点连接”(Point to Point Connection)：

  不管是否为半双工连接，都认为是点对点链路。

说明

点对点表示在两个交换机之间直接连接。而“共享介质连接”(Shared Media Connection) 可以是与集线器的连接。

命令行接口语法

表格 5-67 （快速）生成树端口组态 - SWITCH\STP\PORTS>

命令	说明	注释
stpport [<E|D> [端口]]	对指定端口启用/禁用生成树算法。	仅限管理员。 如果想要指定多个端口作为参数，可以使用空格或连字符分隔端口号。
prio [<0...255> [端口]]	指定端口的优先级。	仅限管理员。
pathcost [<0..200000000> [ports]]	指定端口的路径开销。	仅限管理员。
admedge [<T|F> [端口]]	指定是 • T 终端设备 或者 • F 交换机 与支持生成树或快速生成树的此端口连接。 如果接收（快速）生成树协议，则显示值 F。	

命令	说明	注释
autoedge [<T|F> [端口]]	指定在此端口是否应自动检测连接了 • T 终端设备 或者 • F 交换机 。	仅限管理员。
ptp [<A|T|F> [端口]]	点对点链路在两个交换机之间建立直接链路。 在这种情况下，有以下选项： • A 端口根据双工性识别 PtP 端口。对于全双工，将假定存在 PtP 链路；对于半双工，则假定不存在 PtP 链路（共享介质）。 • T 即使正在使用半双工，也指定点对点链路。 • F 即使使用全双工，也指定没有通过相关端口的点对点链路。	-

5.5.15 MSTP (SCALANCE X-300/X408)

5.5.15.1 多重生成树组态

多重生成树

多重生成树协议 (MSTP) 是对快速生成树协议 (RSTP) 的进一步发展。

与 RSTP 不同，使用 MSTP 时将建立不止一个快速生成树。 使用 MSTP 时，将针对多个 VLAN 创建多个独立的快速生成树实例。 这使得来自不同逻辑网络的通信数据可以通过不同的路径实现路由。

多重生成树组态与工业以太网交换机

单击"MSTP"文件夹图标，将打开 "多重生成树组态"(Multiple Spanning Tree Configuration) 画面。
在此画面中，可显示和设置多重生成树协议的参数。

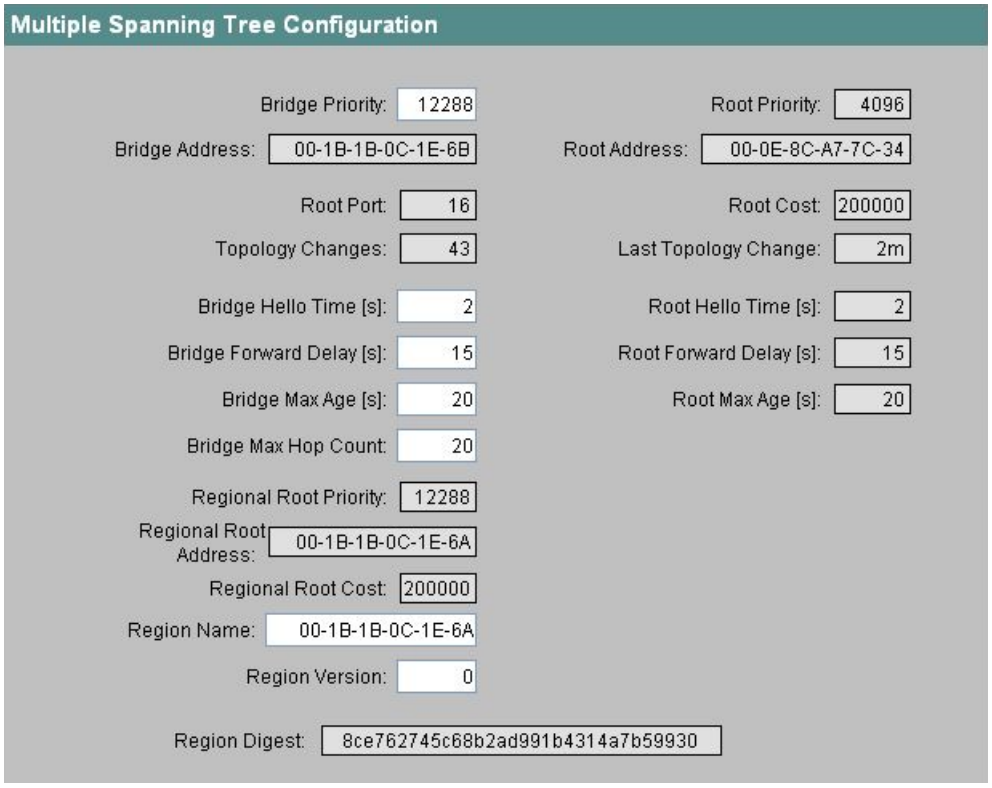


图 5-91　多重生成树组态

下列参数框与设备和根网桥的组态有关。
左侧列与设备的组态有关。 右侧列显示根网桥的组态，该组态可从设备接收到的生成树帧获得。 因此，此处显示的数据为只读。 如果设备是根网桥，则左右两侧显示的信息相匹配。

- **网桥优先级 (Bridge Priority)/根优先级 (Root Priority)**
  根据网桥优先级来确定哪台设备会成为根网桥。优先级最高的网桥会成为根网桥。 数值越小，优先级越高。
  如果网络中有多个设备具有相同优先级，则 MAC 地址数值最小的设备将成为根网桥。
  网桥优先级和 MAC 地址这两个参数一起构成网桥标识符。
  由于根网桥管理所有路径的变更，出于帧延迟的考虑，根网桥应该尽可能处在中心位置。
  在“网桥优先级”(Bridge Priority) 输入框中输入设备的优先级。
  网桥优先级的值是 4096 的整数倍数，值范围从 0 到 61440。
  “根优先级”(Root Priority) 显示框中显示 CIST 根网桥的优先级。
- **网桥地址 (Bridge Address)/根地址 (Root Address)**
  “网桥地址”(Bridge Address) 显示框中显示设备的 MAC 地址。
  “根地址”(Root Address) 显示框中显示 CIST 根网桥的 MAC 地址。
- **根端口 (Root Port)**
  “根端口”(Root Port) 显示框中显示设备与 CIST 根网桥通信时所使用的端口。
- **根开销 (Root Cost)**
  “根开销”(Root Cost) 显示框中显示从该设备到 CIST 根网桥的路径开销。
- **拓扑变更 (Topology Changes)/上次拓扑变更 (Last Topology Change)**
  “拓扑变更”(Topology Changes) 显示框中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。
  “上次拓扑变更”(Last Topology Change) 显示框中以如下单位显示自上次重新组态到现在的时间：
  - 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)。
  在“网桥呼叫时间”(Bridge Hello Time) 输入框中输入两个组态帧的时间间隔。
  此参数的默认值为 2 秒。
  “根呼叫时间”(Root Hello Time) 显示框中显示根网桥中两个组态帧的时间间隔。

- **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信息。 这样可确保只有在所有网桥均已获得所需信息时才开始按照新拓扑运行。
  在“网桥转发延迟”(Bridge Forward Delay) 输入框中，输入使用新信息之前的延迟时间。
  此参数的默认值为 15 秒。
  “根转发延迟”(Root Forward Delay) 显示框中显示根网桥使用新信息之前的延迟时间。

- **网桥最大老化时间 [s] (Bridge Max Age [s])/根最大老化时间 [s] (Root Max Age [s])**
  在“网桥最大老化时间”(Bridge Max Age) 输入框中，输入接收到的 BPDU 可被设备作为有效信息接受的最长“期限”。
  此参数的默认值为 20 秒。
  “根最大老化时间”(Root Max Age) 显示框中显示根网桥中接收到的 BPDU 的最大老化时间设置。

- **网桥最大跳跃数 (Bridge Max Hop Count)**
  只有在“常规”(General) 页面上启用“MSTP”并且“MSTP”被设置为“协议兼容”(Protocol Compatibility) 时，“网桥最大跳跃数”(Bridge Max Hop Count) 输入框才显示。
  在“网桥最大跳跃数”(Bridge Max Hop Count) 输入框中，输入 BPDU 可通过的 MSTP 节点数。
  如果接收到的 MSTP BPDU 的跳跃数大于此处组态的值，则会被丢弃。
  此参数的默认值为 20。

以下参数框与可从 MSTP 帧获得的 CIST 区域根网桥的组态有关。
只有在启用“常规”(General) 网页上的“MSTP”并且“MSTP”被设置为“协议兼容”(Protocol Compatibility) 时，此显示数据才可见。

- **区域根优先级 (Regional Root Priority)**
  “区域根优先级”(Regional Root Priority) 显示框中显示 CIST 区域根网桥的优先级。

- **区域根地址 (Regional Root Address)**
  “区域根地址”(Regional Root Address) 显示框中显示 CIST 区域根网桥的 MAC 地址。

- **区域根开销 (Regional Root Cost)**
  “区域根开销”(Regional Root Cost) 显示框中显示从该设备到 CIST 区域根网桥的路径开销。

- **区域名称 (Region Name)**
  在“区域名称”(Region Name) 输入框中，输入该设备所属的 MSTP 区域的名称。
  默认情况下，在此输入设备的 MAC 地址。
  对于属于相同 MSTP 区域的所有设备，此数值必须相同。

- **区域版本 (Region Version)**
  在“区域版本”(Region Version) 输入框中，输入该设备所在 MSTP 区域的版本号。
  对于属于相同 MSTP 区域的所有设备，此数值必须相同。
- **区域摘要 (Region Digest)**
  “区域摘要”(Region Digest) 显示框中显示校验和，可与各种设备的 VLAN 和 MSTP 示例组态进行比较。
  根据设备上可设置的 MSTP 参数，得到具体设备的校验和。 如果多个设备具有相同的校验和，说明这些参数的设置相同。

说明

对于属于相同 MSTP 区域的设备，它们的“区域名称”(Region Name)、“区域版本”(Region Version) 以及“区域摘要”(Region Digest) 必须相同。

命令行接口语法

表格 5-68　多重生成树组态 - CLI\SWITCH\MSTP>

命令	说明	注释
info	显示当前生成树组态。	-
bprio [0...61440]	指定工业以太网交换机的网桥优先级。	仅限管理员。
hellotm [1 ... 10]	指定两个 BPDU 之间的时间间隔，以秒为单位。	仅限管理员。
fwddelay [4 ... 30]	指定组态信息有效性的延迟时间（以秒为单位指定）。	仅限管理员。 默认值： 15 s
maxage [6 ... 40]	指定组态信息的最大老化时间。	仅限管理员。 默认值： 20 s
maxhopcnt [6 ... 40]	指定 BPDU 可通过的 MSTP 节点数。	仅限管理员。
regname	指定设备所属的 MSTP 区域的名称。	仅限管理员。
regvers	指定设备所在的 MSTP 区域的版本号。	仅限管理员。

5.5.15.2 CIST 端口参数

特定于端口的参数

单击“CIST 端口”(CIST Ports) 子菜单，将显示“CIST 端口参数”(CIST Port Parameters) 画面。

对于 MSTP，CIST（Common and Internal Spanning Tree，公共内部生成树）是交换机内部使用的实例，原则上相当于内部快速生成树。

此画面显示当前端口参数，这些参数由用户设置或由工业以太网交换机自动功能设置。

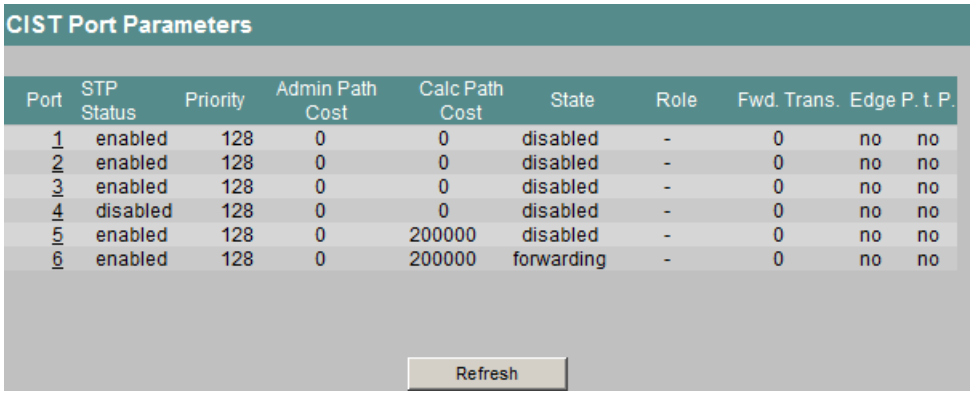


图 5-92　CIST 端口参数

调用此页面时，表中显示端口参数组态的当前状态。

该表格包括以下列：

- **端口 (Port)**
  “端口”(Port) 列显示信息所关联的端口。
- **STP 状态 (STP Status)**
  “STP 状态”(STP Status) 列显示对该端口是启用还是禁用生成树。
- **优先级 (Priority)**
  “优先级”(Priority) 列显示优先级的值。
  如果由生成树计算出的路径可能经过交换机的多个端口，则选择优先级最高的端口（也就是优先级数值最小的端口）。
  可输入的优先级数值介于 0 和 255 之间。默认值为 128。
  如果优先级相同，则选择路径开销最小的路径。
- **管理路径开销 (Admin Path Cost)**
  显示要使用的路径开销的值。

- **计算路径开销 (Calc Path Cost)**
  如果管理路径开销值大于 0，则该值将作为计算出的路径开销值。
  如果管理路径开销值等于 0，则将自动计算计算出的路径开销值。成本路径的计算很大程度上取决于传输速度。
  可达到的传输速度越高，管理路径开销的值就应该越低。
  快速生成树的典型路径开销值如下：
  - 1000 Mbps = 20,000
  - 100 Mbps = 200,000
  - 10 Mbps = 2,000,000
- **状态 (State)**
  “状态”(State) 列显示端口的当前状态。
  可能的状态如下：
  - 禁用 (disabled)

    该端口仅接收，未包括在 STP、MSTP 和 RSTP 中。
  - 拦截 (blocking)
    该端口接收 BPDU。
  - 侦听 (listening)
    该端口接收和发送 BPDU。端口包括在生成树算法中。
  - 学习 (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）。
  - 转发 (forwarding)

    在重新组态时间后，端口在网络中再次激活；端口接收和转发数据帧。
- **角色**
  “角色”(Role) 列指定端口获得的角色：
  - 根 (Root)
    端口具有从设备本身到 CIST 区域根网桥的最低路径开销。
  - 指定 (Designated)
    通过此端口，已连接的网段以最少的路径开销到达 CIST 区域根网桥。
  - 备用 (Alternate)
    端口被阻止，提供到 CIST 区域根网桥的备用路径。
  - 备份 (Backup)
    端口被阻止，提供到已经通过其它端口连接的冲突域的备用路径。
- **转发转换 (FWD Transitions)**
  “转发转换”(FWD Transitions) 列显示从侦听状态切换到转发状态的次数。

- **边缘 (Edge)**
  “边缘”(Edge) 列显示端口上是否连接有终端设备。
  连接终端设备时，工业以太网交换机可以更快速地切换端口，而无需考虑生成树帧。如果忽略此设置而接收生成树帧，则该端口将自动切换为无状态。
  – 是 (yes)

    一个边缘端口连接到此端口。
  – 否 (no)
    此端口上有生成树或快速生成树设备。
- **点对点 (P.t.P.)**
  通过此端口将两个 RSTP 兼容的网络组件连接在一起时，存在一个点对点链路。
  可能的状态如下：
  – 是 (Yes)

    存在点对点链路。
  – 否 (No)

    不存在点对点链路。

针对多重生成树组态端口

如果单击“CIST 端口参数”(CIST Port Parameters) 页面的 “端口”(Port) 列中的端口名称，将打开 “生成树端口组态”(Spanning Tree Port Configuration) 页面。

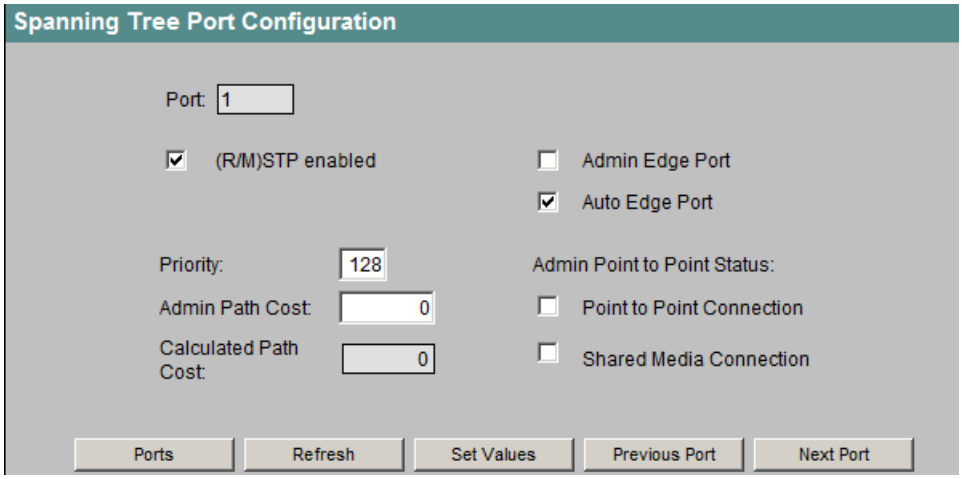


图 5-93　生成树端口组态

STP 和 RSTP 也采用 CIST 端口参数的端口特定组态。因此，该组态对于 MSTP、RSTP 和 STP 是相同的。

有关各页面元素和 CLI 命令的说明，请参见生成树端口组态 (页 232)部分。

命令行接口语法

表格 5-69 CIST 端口参数 - CLI\SWITCH\MSTP\CISTPORTS>

命令	说明	注释
info	显示端口总览和相应的快速生成树设置。	-
stpport [<E|D> [端口]]	对相关端口启用/禁用生成树。	仅限管理员。
prio [<0..255> [端口]]	指定相关端口的优先级。	仅限管理员。
pathcost [<0..200000000> [ports]]	指定相关端口的路径开销。	仅限管理员。
admedge [<T|F> [端口]]	指定相关端口连接的是终端设备还是交换机： • T 终端设备 • F 交换机	仅限管理员。

命令	说明	注释
autoedge [<T|F> [端口]]	指定自动检测相关端口上连接的终端设备或交换机： • T 终端设备 • F 交换机 如果接收到（快速）生成树协议，则显示值“F”。	仅限管理员。
ptp [<A|T|F> [端口]]	点对点链路在两个交换机之间建立直接链路。 指示相关端口是否为 PtP 端口： • A 自动检测 PtP。对于全双工，将假定存在 PtP 链路；对于半双工，则假定不存在 PtP 链路。 • T 即使正在使用半双工，也指定点对点链路。 • F 如果正在使用双工，则指示无 PtP 链路。	仅限管理员。

5.5.15.3 MSTP 实例组态

多重生成树组态

单击“MST 实例”(MST Instances) 子菜单，将打开“MSTP 实例组态”(MSTP Instances Configuration) 画面。
在此画面中，可以管理 LAN 中多个自有快速生成树的 VLAN。

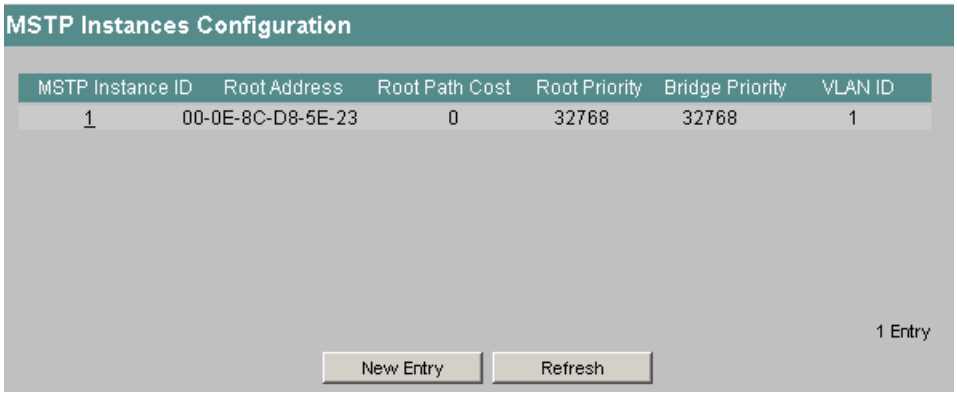


图 5-94 MSTP 实例组态

该表格包括以下列：

- **MSTP 实例 ID (MSTP Instance ID)**
  “MSTP 实例 ID”(MSTP Instance ID) 显示框中显示 MSTP 实例编号。
- **根地址 (Root Address)**
  “根地址”(Root Address) 显示框中显示 MST 实例区域根网桥的 MAC 地址。
- **根路径开销 (Root Path Cost)**
  “根路径开销”(Root Path Cost) 显示框中显示从设备到 MST 实例区域根网桥的路径开销。
- **根优先级 (Root Priority)**
  “根优先级”(Root Priority) 显示框中显示 MST 实例区域根网桥的优先级。
- **网桥优先级 (Bridge Priority)**
  “网桥优先级”(Bridge Priority) 显示框中显示设备的优先级。
- **VLAN ID**
  “VLAN ID”显示框中显示 VLAN 的编号。

创建新 MSTP 实例

1. 单击“MSTP 实例组态”(MSTP Instances Configuration) 窗口中的 “新建条目”(New Entry) 按钮。
   将打开“MSTP 实例组态”(MSTP Instances Configuration) 窗口。

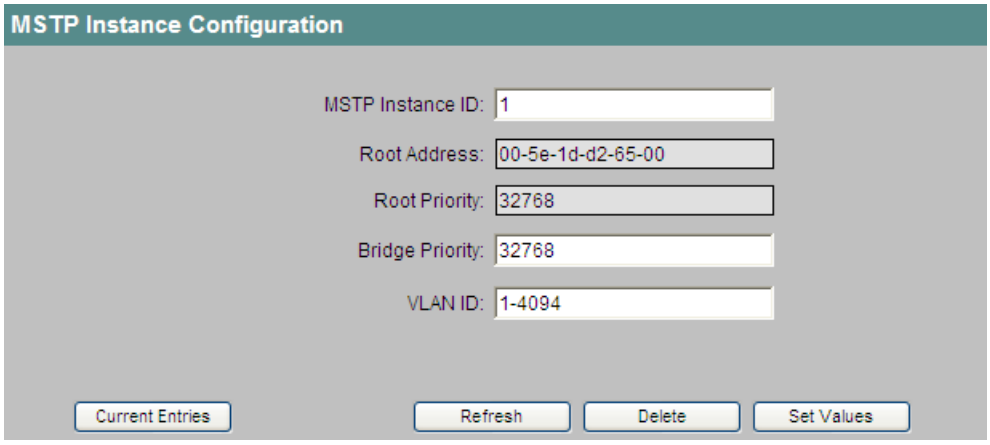


图 5-95 MSTP 实例组态

2. 在“MSTP 实例 ID”(MSTP Instance ID) 输入框中输入 MSTP 实例编号。
   允许值： 1 到 16
3. 在 “网桥优先级”(Bridge Priority) 输入框中输入网桥优先级。
   网桥优先级的值是 4096 的整数倍，值范围从 0 到 61440。
4. 在“VLAN ID”输入框中输入 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 到 4094
5. 要保存设置，请单击 “设置值”(Set Values) 按钮。
6. 要从 “当前条目”(Current Entries) 返回“MSTP 实例组态”(MSTP Instances Configuration) 画面，请单击 “当前条目”(Current Entries) 按钮。

删除 MSTP 实例

1. 在“MSTP 实例组态”(MSTP Instances Configuration) 窗口的“MSTP 实例 ID”(MSTP Instance ID) 列中，单击所需 ID。
   将显示“MSTP 实例组态”(MSTP Instances Configuration) 窗口。
2. 单击 “删除”(Delete) 按钮删除该 MSTP 实例。

命令行接口语法

表格 5-70　MSTP 实例组态 - CLI\SWITCH\MSTP\MSTI>
MSTP 实例组态 - CLI\SWITCH\MSTP\MSTI>

命令	说明	注释
info	显示有关 MSTP 实例的信息。	-
add <MST ID> <brgPrio> <vlans (1-4094)>	生成和修改 MSTP 实例。	仅限管理员。
delete <MST ID>	删除 MSTP 实例。	仅限管理员。

5.5.15.4　多重生成树端口组态

（多重）生成树端口

单击“MST 端口”(MST Ports) 子菜单，将显示“MST 端口”(MST Ports) 画面。
在此画面中，可设置所组态多重生成树实例的端口参数。

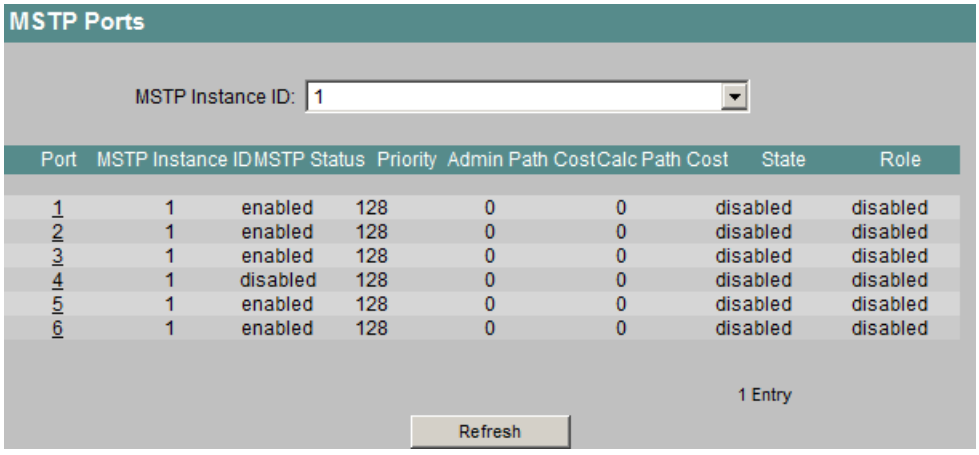


图 5-96　MSTP 端口

该页面包含以下框：

- **MSTP 实例 ID (MSTP Instance ID)**
  在“MSTP 实例 ID”(MSTP Instance ID) 下拉列表中，选择 MSTP 实例的 ID。

该表格包括以下列：

- **端口 (Port)**
  "端口"(Port) 列显示信息所关联的端口。
- **MSTP 实例 ID (MSTP Instance ID)**
  "MSTP 实例 ID"(MSTP Instance ID) 列显示 MSTP 实例编号。
- **MSTP 状态 (MSTP Status)**
  "MSTP 状态"(MSTP Status) 列显示对该端口是启用还是禁用多重生成树。
- **优先级 (Priority)**
  "优先级"(Priority) 列显示优先级的值。
  如果由生成树计算出的路径可能经过交换机的多个端口，则选择优先级最高的端口（也就是优先级数值最小的端口）。
  可输入的优先级值介于 0 和 255 之间。默认值为 128。
- **管理路径开销 (Admin Path Cost)**
  "管理路径开销"(Admin Path Cost) 列，显示要使用的路径开销的值。
- **计算路径开销 (Calc Path Cost)**
  如果管理路径开销值大于 0，则该值将作为计算出的路径开销值。
  如果管理路径开销值等于 0，则将自动计算计算出的路径开销值。成本路径的计算很大程度上取决于传输速度。
  可达到的传输速度越高，管理路径开销的值就应该越低。
  快速生成树的典型路径开销值如下：
  - 1000 Mbps = 20,000
  - 100 Mbps = 200,000
  - 10 Mbps = 2,000,000

- **状态 (State)**
  "状态"(State) 列显示端口的当前状态。
  可能的状态如下：
  – 禁用 (disabled)

    该端口仅接收，未包括在 STP、MSTP 和 RSTP 中。
  – 拦截 (blocking)
    该端口接收 BPDU。
  – 侦听 (listening)
    该端口接收和发送 BPDU。端口包括在生成树算法中。
  – 学习 (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）。
  – 转发 (forwarding)

    在重新组态时间后，端口在网络中再次激活；端口接收和转发数据帧。
- **角色 (Role)**
  "角色"(Role) 列指定端口获得的角色：
  可能的值包括：
  – 根 (Root)
    端口具有从设备本身到 MST 实例区域根网桥的最低路径开销。
  – 指定 (Designated)
    通过此端口，已连接的网段以最少的路径开销到达 MSTI 区域根网桥。
  – 备用 (Alternate)
    端口被阻止，提供到 MSTI 区域根网桥的备用路径。
  – 备份 (Backup)
    端口被阻止，提供到已经通过其它端口连接的冲突域的备用路径。

（多重）生成树端口组态

如果单击“MSTP 端口”(MSTP Ports) 页面的 “端口”(Port) 列中的端口名称，将打开 “（多重）生成树端口组态”((Multiple) Spanning Tree Port Configuration) 页面：

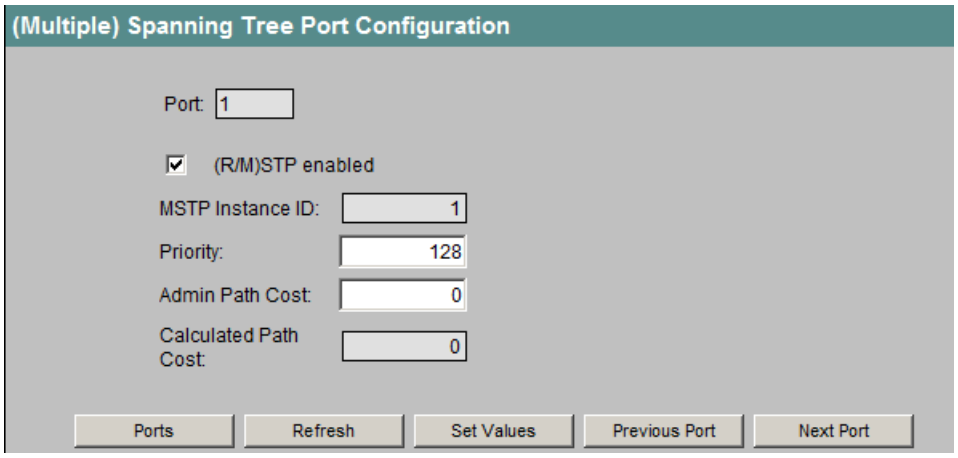


图 5-97　多重生成树端口组态

端口 (Port)

“端口”(Port) 显示框中显示所选端口。

启用 (R/M)STP ((R/M)STP enabled)

如果想要端口使用（多重）生成树协议，则选中此复选框。

MSTP 实例 ID (MSTP Instance ID)

“MSTP 实例 ID”(MSTP Instances ID) 显示框中显示所选端口的 MSTP 实例 ID。

优先级 (Priority)

在 “优先级”(Priority) 输入框中输入端口优先级的值。
允许的值：0 到 255

管理路径开销 (Admin Path Cost)

在此处可以手动设置每个端口和 MST 实例要使用的路径开销值。

计算出的路径开销 (Calculated Path Cost)

如果管理路径开销值大于 0，则该值将作为计算出的路径开销值。
如果管理路径开销值等于 0，则将自动计算计算出的路径开销值。成本路径的计算很大程度上取决于传输速度。

可达到的传输速度越高，管理路径开销的值就应该越低。

快速生成树的典型路径开销值如下：

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

命令行接口语法

表格 5-71 MSTP 端口/多重生成树端口组态 - CLI\SWITCH\MSTP\MSTPORTS>

命令	说明	注释
info <MST ID>	显示 MSTP 实例的端口信息。	-
prio <MST ID> <0..240> <ports>	指定端口的网桥优先级。	仅限管理员。
pathcost <MST-ID> <0..200000000>	指定示例中端口的路径开销。	仅限管理员。

5.5.16 QoS

5.5.16.1 QoS 组态 (QoS Configuration)

QoS

不同的应用对网络的需求不同。对于纯文件传输，总吞吐量是决定性因素，而个别延迟和丢失率则不是很重要。另一方面，对于实时通信（例如语音 IP），延迟、跳动和丢失率则重要得多，因为它们直接影响可理解性。

传输优先级

X-300/400 工业以太网交换机支持"CoS 到队列映射"(CoS to Queue Mapping) 和"DSCP 到队列映射"(DSCP to Queue Mapping)，利用这些映射，可以转发来自不同来源且优先级不同的数据包。为了保持与以前固件版本的向下兼容性，在默认设置中禁用了 DSCP 映射。

CoS 和 DSCP 信息的优先化

如果 DSCP 映射激活，将按照以下方式处理 CoS 和 DSCP 信息：

SCALANCE X-300/SCALANCE X-408

- 如果 DSCP 映射激活，帧包含 CoS 和 DSCP 信息，则根据 DSCP 优先级转发帧。CoS 信息被忽略。

SCALANCE X414

- 如果 DSCP 映射激活并且帧只含 DSCP 信息，则根据“CoS 到队列映射”(CoS to Queue Mapping) 设置，由交换机控制器将 DSCP 优先级映射到 CoS 值。必要时可以更改“CoS 到队列映射”(CoS to Queue Mapping) 的默认值。
- 如果 DSCP 映射激活，帧包含 CoS 和 DSCP 信息，则根据 DSCP 优先级转发帧。CoS 信息被忽略。

概述

该页面的内容取决于设备。

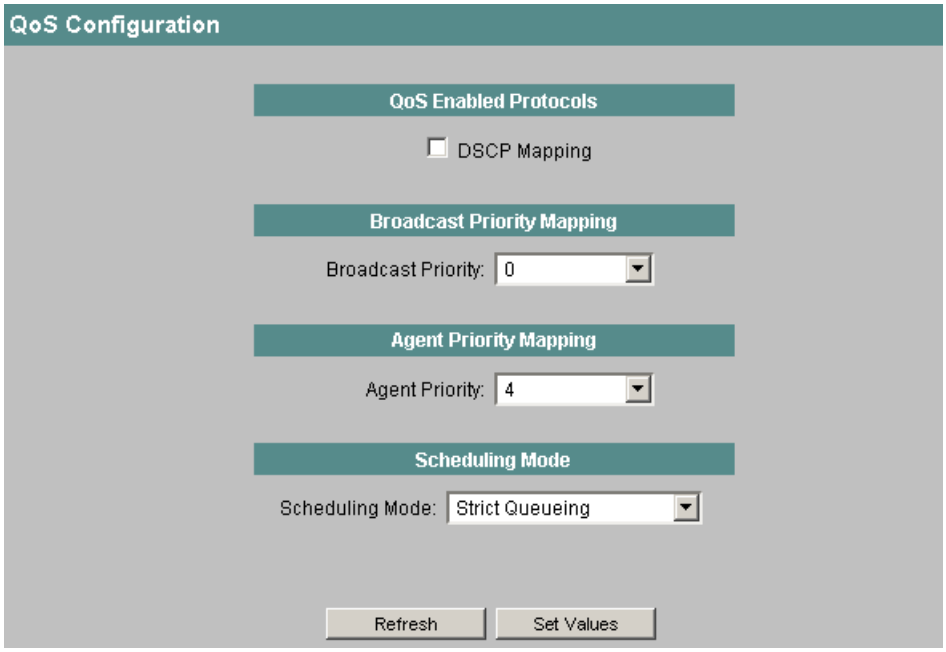


图 5-98　X-300 QoS 组态

DSCP 映射 (DSCP Mapping)
启用/禁用“DSCP 到队列映射”(DSCP to Queue Mapping)

下列设置仅适用于 X-300 IE 交换机：

广播优先级 (Broadcast Priority)

指定广播帧的发送优先级。

代理优先级 (Agent Priority)

指定代理帧的发送优先级。

计划模式 (Scheduling Mode)

- 严格排队 (Strict Queueing)
  只要队列中存在优先级更高的帧，就只处理这些高优先级的帧。
- 加权公平排队 (Weighted Fair Queueing)（仅适用于 SCALANCE X-300）
  即使队列中存在优先级更高的帧，偶尔还是会处理优先级较低的帧。

命令行接口语法

表格 5-72　QoS 组态 - CLI\SWITCH\QOS>

命令	说明	注释
dscpmap [E|D]	启用/禁用“DSCP 到队列映射”(DSCP to Queue Mapping)。	仅限管理员。
bcprio [noforce : <0-7>]	指定广播帧的发送优先级。	仅限管理员。
agentprio [noforce : <0-7>]	指定代理帧的发送优先级。	仅限管理员。
sched [模式]	指定计划模式。	仅限管理员。

5.5.16.2 CoS 到队列映射 (CoS to Queue Mapping)

CoS 队列 (CoS Queue)

在此处将 CoS 优先级分配给特定通信队列。

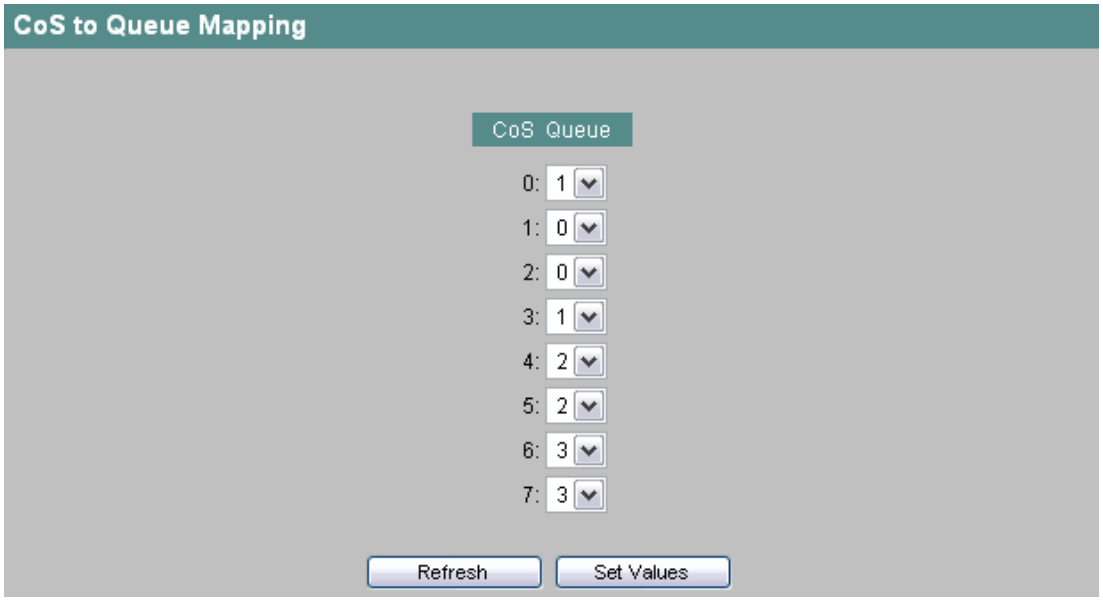


图 5-99 CoS 到队列映射 (CoS to Queue Mapping)

CoS
进入数据包的 CoS 优先级顺序。

队列 (Queue)
分配了 CoS 优先级的通信转发队列（发送优先级）。

命令行接口语法

表格 5-73 QOS 组态 - CLI\SWITCH\QOS>

命令	说明	注释
cos [<0..3> <0..7>]	将 CoS 优先级分配给特定通信队列： • 参数 1 队列 • 参数 2 CoS 优先级	仅限管理员。

5.5.16.3 DSCP 到队列映射 (DSCP to Queue Mapping)

DSCP 队列

在此处将 DSCP 设置分配给各个通信队列。

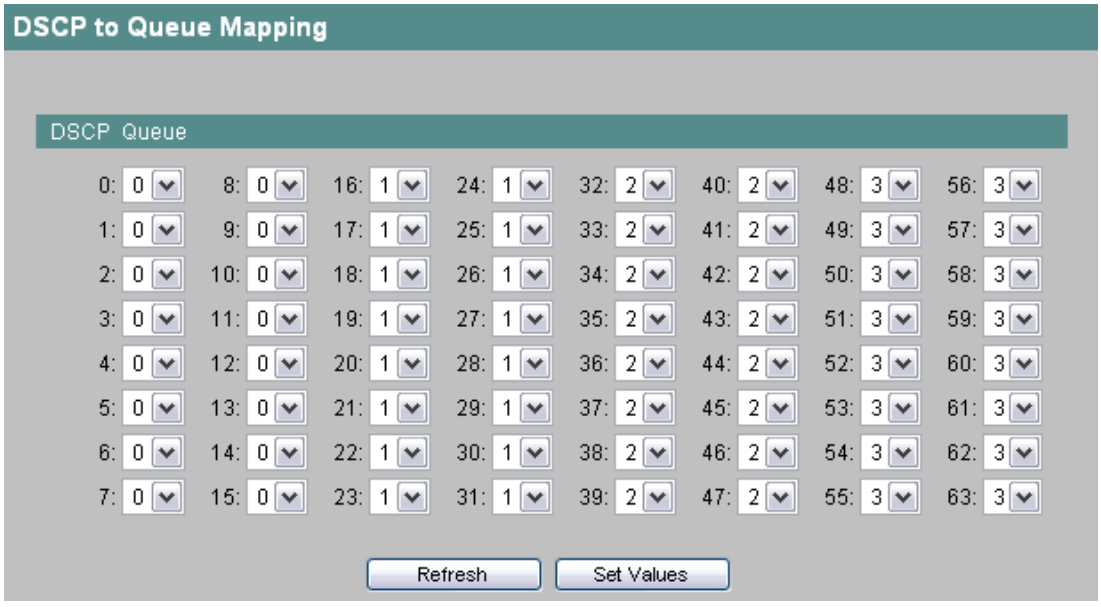


图 5-100 DSCP 到队列映射 (DSCP to Queue Mapping)

DSCP
进入数据包的 DSCP 优先级顺序。

队列 (Queue)
分配了 DSCP 值的通信转发队列（发送优先级）。

命令行接口语法

表格 5-74 QoS 组态 - CLI\SWITCH\QOS>

命令	说明	注释
dscp [<0..3> <0..63>]	将 DSCP 设置分配给特定通信队列： • 参数 1 队列 • 参数 2 DSCP 值	仅限管理员。

5.5.17 LLDP

5.5.17.1 LLDP 组态 (LLDP Configuration)

应用

PROFINET 使用 LLDP 协议进行拓扑诊断。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。

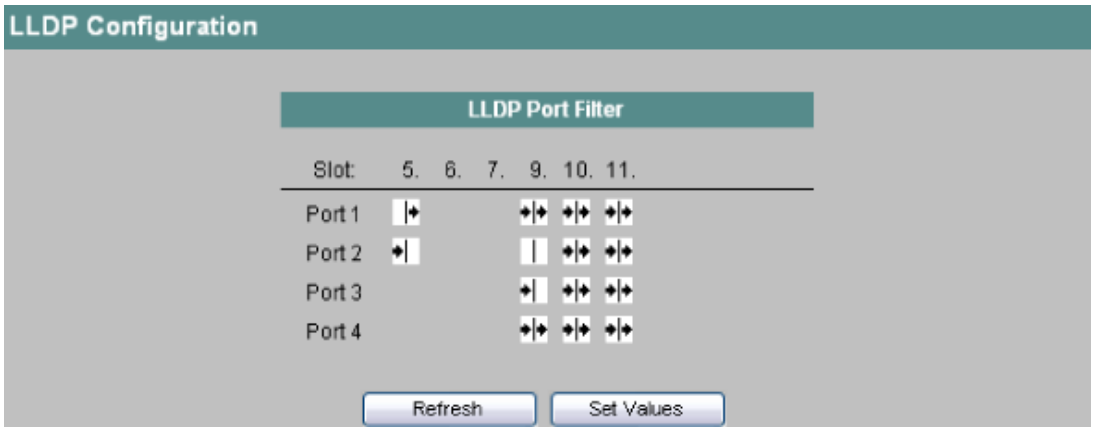


图 5-101 LLDP 组态 (LLDP Configuration)

插槽/端口 (Slot/Port)

在此处选择支持接收和/或发送 LLDP 帧的端口

:

仅接收：此端口只能接收 LLDP 帧。

仅发送：此端口只能发送 LLDP 帧。

发送和接收：此端口可以发送和接收 LLDP 帧。

禁用：此端口既不接收也不发送 LLDP 帧。

命令行接口语法

表格 5-75　当前组播组 - CLI\SWITCH\LLDP>

命令	说明	注释
info	显示当前 LLDP 设置。	-
lldpport <模式> [端口]	更改端口的 LLDP 设置。如果未指定任何端口，则更改所有端口。 <模式> 参数可为以下值： • rx 仅接收 • tx 仅发送 • e 接收和发送 • d 既不接收也不发送	仅限管理员。

5.5.17.2 LLDP 邻居

邻居表

该页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。

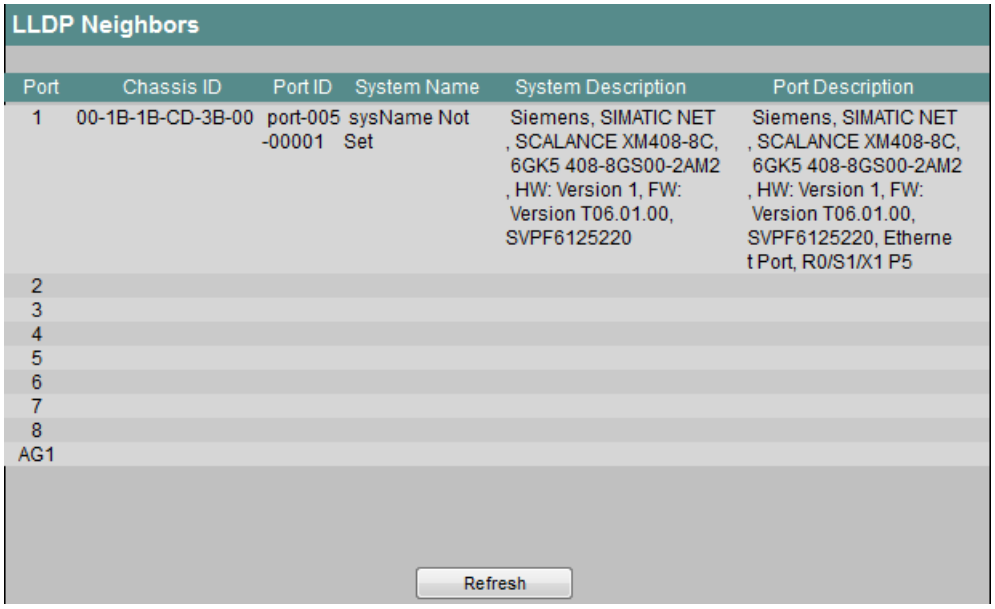


图 5-102 LLDP 邻居

端口 (Port)

显示工业以太网交换机可以接收信息的端口。

机架 ID (Chassis ID)

显示所连设备的设备 ID。设备 ID 与通过 SINEC PNI 等分配的设备名称相对应。如果未分配设备名称，则显示设备的 MAC 地址。

端口 ID (Port ID)

显示所连设备的端口。

系统名称 (System name)

显示所连接设备的系统名称。如果未分配系统名称，则显示“sysName Not Set”。

系统说明 (System Description)

显示所连设备的说明，例如设备、部件编号和固件版本。

端口说明 (Port Description)

显示端口说明。

命令行接口语法

表格 5-76　当前组播组 - CLI\SWITCH\LLDP>

命令	说明	注释
neighbors	显示邻居表的当前内容。	仅限管理员。

5.5.18　光纤监视协议

要求

- 仅能对带诊断功能的收发器使用光纤监视协议 (FMP)。含有带诊断功能的收发器的设备和模块名称中有补充标识“FM”。
- 为了能够使用光纤监视协议 (FMP)，需启用 LLDP。已将 FMP 信息添加到 LLDP 数据包中。

监视光链接

对于“光纤监视”，您可监视两个交换机之间光纤连接的接收功率和功率损耗。

如果启用某光纤端口的光纤监视，设备会通过 LLDP 数据包将端口的当前传送功率发送到其连接伙伴。除了发送外，设备还会检查是否已从连接伙伴接收相应信息。

无论工业以太网交换机是否接收到诊断信息，它都会监视在光纤端口测得的接收功率并将其与设置的限值进行比较。

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

如果接收功率或功率损耗值降到设置限值以下或超出限值，则将触发事件。可按两个等级设置限值。在“代理 > 事件组态”(Agent > Event Config) 中，可以指定工业以太网交换机指示事件的方式。在“X-300 > 故障屏蔽”(X-300 > Fault Mask) 中，还可以指定是否发出错误信号。

端口的状态

此页面显示用户所做的当前端口参数设置。

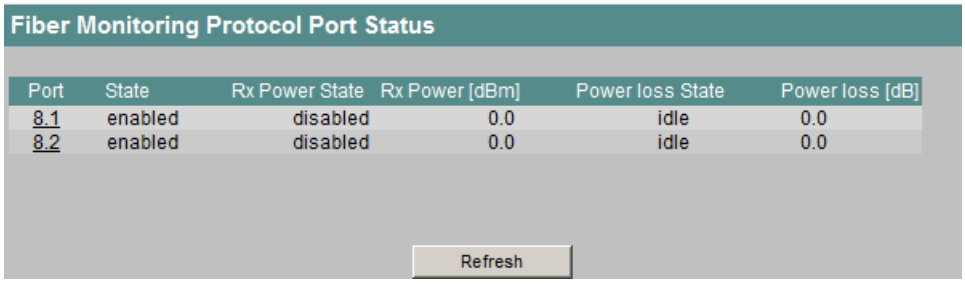


图 5-103　光纤监视协议端口状态

端口 (Port)

显示可用的光学端口。

状态 (State)

FMP 启用或禁用

接收功率状态 (Rx Power State)

- **禁用 (disabled)**
  FMP 禁用。
- **正常 (ok)**
  光链接的接收功率值正常。
- **需要维护 (maintenance required)**
  检查链接。
  已触发事件。
- **要求维护 (maintenance demanded)**
  需要检查链接。
  已触发事件。
- **链接停止 (link down)**
  连接已中断。

接收功率 [dBm] (Rx Power [dBm])

显示接收功率的当前值。

该值可以有 +/- 3 dB 的容差。

功率损耗状态 (Power loss State)

为了能够监视连接的功率损耗，端口需要链接到另一个已启用 FMP 的端口。

- **禁用 (disabled)**
  FMP 禁用。
- **正常 (ok)**
  光链接的功率损耗值正常。
- **需要维护 (maintenance required)**
  检查链接。
  已触发事件。
- **要求维护 (maintenance demanded)**
  需要检查链接。
  已触发事件。
- **空闲 (idle)**
  端口未与另一个已启用 FMP 的端口连接。
  如果 5 个周期内都未接收到诊断信息，则视为连接中断。一个周期持续 5 秒。

功率损耗 [dB] (Power loss [dB])

显示功率损耗的当前值。

该值可以有 +/- 3 dB 的容差。

设置功率限值

如果单击 “光纤监视协议端口状态”(Fiber Monitoring Protocol Port Status) 页面 “端口”(Port) 列中的端口名称，将打开“FMP 端口组态”(FMP Port Configuration) 页面：

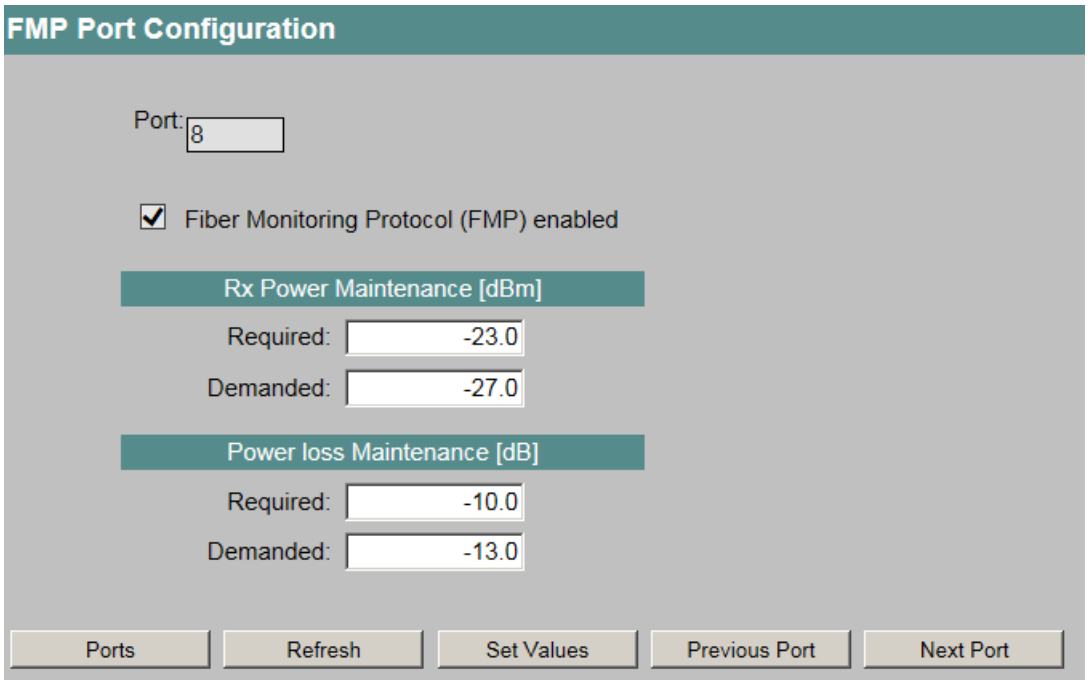


图 5-104　FM 端口组态

端口 (Port)

显示可用的光学端口。

光纤监视协议 (FMP) 已启用

启用或禁用 FMP。

接收功率维护 (Rx Power Maintenance)

- **所需 (Required)**
  输入第一次通知您接收功率超限的值。
  如果输入值 0，则不会监视接收功率。
- **要求 (Demanded)**
  输入第二次通知您接收功率超限的值。
  如果输入值 0，则不会监视接收功率。

说明

针对 SFP 可插拔收发器的 FMP

对于 SFP 可插拔收发器，您可以通过“交换机 > 端口诊断 > SFP 诊断”(Switch > Port Diagnostics > SFP Diagnostics)，在“接收功率 (dBm)”(RX Power (dBm)) 框中的“低”(Low) 列中读取最小接收功率。

建议将最小接收功率的值设置为“维护要求的接收功率”(Rx Power Maintenance Demanded)。对于“维护所需的接收功率”(Rx Power Maintenance Required)，请选择更高的值，例如，比最小接收功率高 3 dBm。这表示在功率降至低于 SFP 收发器的最小接收功率前，第一次通知您接收功率超限。

功率损耗维护 (Power loss Maintenance)

- **所需 (Required)**
  输入第一次通知您连接的功率损耗的值。
  如果输入值 0，则不会监视功率损耗。
- **要求 (Demanded)**
  输入第二次通知您连接的功率损耗的值。
  如果输入值 0，则不会监视功率损耗。

说明

针对 SFP 可插拔收发器的 FMP

利用 SFP 可插拔收发器，用户可计算允许的最大功耗：连接的两个 SFP 可插拔收发器最低接收功率与最低发射功率之差：

最低接收功率显示于“交换机 > 端口诊断 > SFP 诊断”(Switch > Port Diagnostics > SFP Diagnostics) 的“RX 功率 (dBm)”(RX Power (dBm)) 框的“低”(Low) 列中。

最低发射功率显示于“交换机 > 端口诊断 > SFP 诊断”(Switch > Port Diagnostics > SFP Diagnostics) 的“TX 功率 (dBm)”(TX Power (dBm)) 框的“低”(Low) 列中。

建议将允许的最大功率值设置为“维护所需的功耗”(Power loss Maintenance Demanded)。为“维护所需的功耗”(Power loss Maintenance Required) 选择较低数值。例如，低于允许的最大功耗 3 dBm。这表示在超出 SFP 可插拔接收器允许的最大功耗前，当功耗首次增加时，用户将得到通知。

命令行接口语法

表格 5-77　光纤监视协议 - CLI\SWITCH\FMP>

命令	说明	注释
info	显示 FMP 组态。	
limit [rx | loss] [req | dem] [<port>] [<limit>]	指定每个端口的接收功率和功率损耗限值： • rx 接收功率 • loss 功率损耗 • req 第一次通知 • dem 第二次通知 • port 应用设置的端口 • 限值 接收功率或功率损耗值的限值 (dBm)。	仅限管理员 如果输入值 0，则不会监视接收功率或功率损耗。
enable <D|E> [<Port>]	为指定端口启用/禁用 FMP。	仅限管理员

表格 5-78　光纤监视 - CLI\SWITCH\FM>

命令	说明	注释
info	显示收发器的常规信息，例如型号、序列号和诸如接收功率和发送功率等当前值。	

5.5.19 DCP 组态 (DCP Configuration)

应用

STEP 7 和 SINEC PNI 使用 DCP 协议进行工业以太网交换机的组态和诊断。在出厂设置中，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 DCP 多播帧，例如，防止使用 SINEC PNI 组态网络的各个部分，或者将整个网络分成多个较小子网，以进行组态和诊断。

说明

此功能对 DCP 消息帧的接收无影响。

经过适当设置，只禁止在管理 VLAN 中“未标记成员”端口上转发 DCP 消息帧。对于其它 VLAN，转发的消息帧为“未知多播”消息帧。

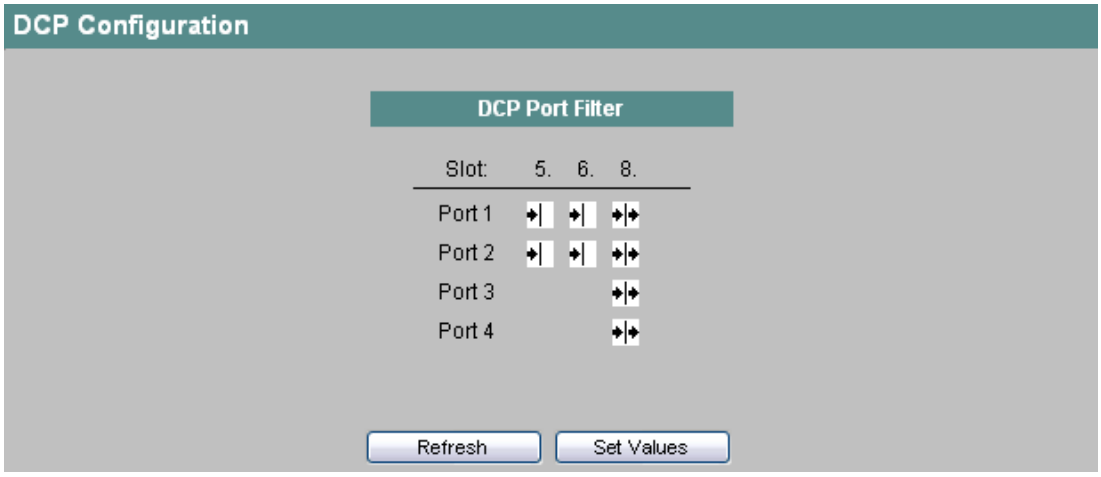


图 5-105 DCP 组态 (DCP Configuration)

在此处选择将支持发送 DCP 帧的端口：

仅接收：该端口不会发送任何 DCP 多播帧。采用单播的 DCP 通信未进行过滤。

发送和接收：该端口发送所有 DCP 消息帧。

命令行接口语法

表格 5-79　当前组播组 - CLI\SWITCH\DCP>

命令	说明	注释
info	显示当前 DCP 设置。	-
dcpport <模式> [端口]	修改端口的 DCP 设置。如果未指定任何端口，则更改所有端口。 <模式> 参数可为以下值： • rx 该端口接收所有 DCP 消息帧，但只转发 DCP 单播帧。 • e 该端口可接收和发送所有 DCP 消息帧。	仅限管理员。

5.5.20 DHCP 中继代理

5.5.20.1 DHCP 中继代理组态 (DHCP Relay Agent Configuration)

为终端设备分配 IP 地址

DHCP 中继功能可在 DHCP 服务器和连接至特定端口的终端设备之间进行调停，以将 IP 地址分配给此终端设备。要实现此目的，工业以太网交换机需将终端设备的端口号与 DHCP 请求一同转发至 DHCP 服务器。

指定 DHCP 服务器 IP 地址

最多可以为 DHCP 中继代理指定 4 个 DHCP 服务器 IP 地址，另请参见 "交换机组态"(Switch Configuration) 菜单项。

对于每一个 DHCP 服务器，均可组态其负责的端口和 VLAN，请参见 "DHCP 中继代理端口组态 (DHCP Relay Agent Port Configuration) (页 269)"。

接收到 DHCP 请求时，工业以太网交换机会先检查请求是否与 DHCP 服务器 1 的端口/VLAN 组态相匹配。

如果请求匹配，工业以太网交换机将转发 DHCP 请求且不会再搜索 DHCP 服务器列表。

如果请求不匹配，工业以太网交换机会将请求与 DHCP 服务器 2、3 和 4 的组态进行比较。

如果进入的 DHCP 请求与任何 DHCP 服务器均不匹配，可以将请求作为广播转发。

也可以将比较限制到可访问的 DHCP 服务器。

说明

只有当在“交换机组态”(Switch Configuration) 菜单中启用了“DHCP 选项 82”(DHCP Option 82) 选项，才能启用 DHCP 中继代理。

如果 DHCP 客户端和 DHCP 服务器不在同一 VLAN 中，只有激活“代理组态”(Agent Configuration) 菜单项中的“可在所有 VLAN 中访问”(Accessible in all VLANs) 选项时，才会转发 DHCP 请求。

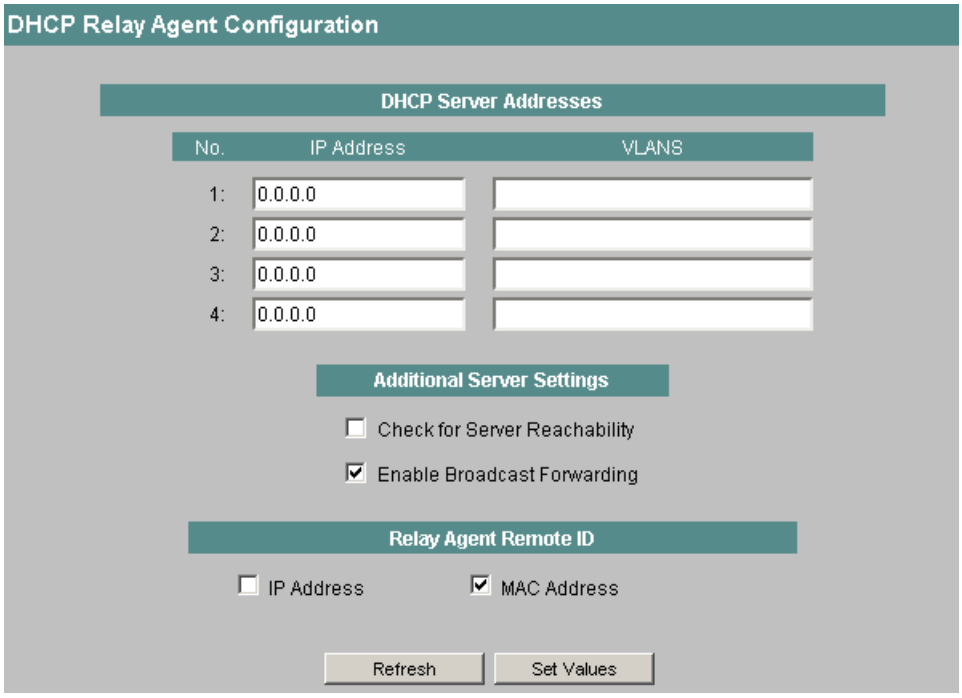


图 5-106　DHCP 中继代理组态 (DHCP Relay Agent Configuration)

IP 地址 (IP Address)

输入工业以太网交换机将 DHCP 请求转发到的 DHCP 服务器的地址。

VLAN (VLANs)

输入端口所在的 VLAN 的编号。

可以输入多个 VLAN 以及 VLAN 范围，用逗号分隔，例如 1,5,10-12。

中继代理远程 ID (Relay Agent Remote ID)

在此处可选择中继代理是使用代理组态中的 IP 地址还是使用其 MAC 地址作为远程 ID。

其它服务器设置

- 检查服务器可访问性 (Check for Server Reachability)
  如果启用该选项，每隔 30 s 将检查一次 DHCP 服务器的可访问性。如果无法访问服务器，则处理服务器列表时将忽略此服务器。
- 启用广播转发 (Enable Broadcast Forwarding)
  如果启用此选项，则在 DHCP 服务器列表中没有 DHCP 请求的匹配条目时，会将请求作为广播转发。

命令行接口语法

表格 5-80　DHCP 中继代理组态 - CLI\SWITCH\RELAGENT>

命令	说明	注释
info	显示 DHCP 中继代理的当前设置。	-
server <编号> [IP] [VLANs]	指定 IP 地址和 DHCP 服务器 <编号> 的 VLAN。	仅限管理员。 默认值：0.0.0.0
remoteid [IP|MAC]	指定中继代理远程 ID	仅限管理员。
bcastfwd [E|D]	启用/禁用 "启用广播转发"(Enable Broadcast Forwarding) 功能。	仅限管理员。
reachchk [E|D]	启用/禁用 "检查服务器可访问性"(Check for Server Reachability) 功能。	仅限管理员。

5.5.20.2 DHCP 中继代理端口组态 (DHCP Relay Agent Port Configuration)

DHCP 中继代理端口参数 (DHCP Relay Agent Port Parameters)

此页面显示 DHCP 中继代理当前组态的特定于端口的参数。

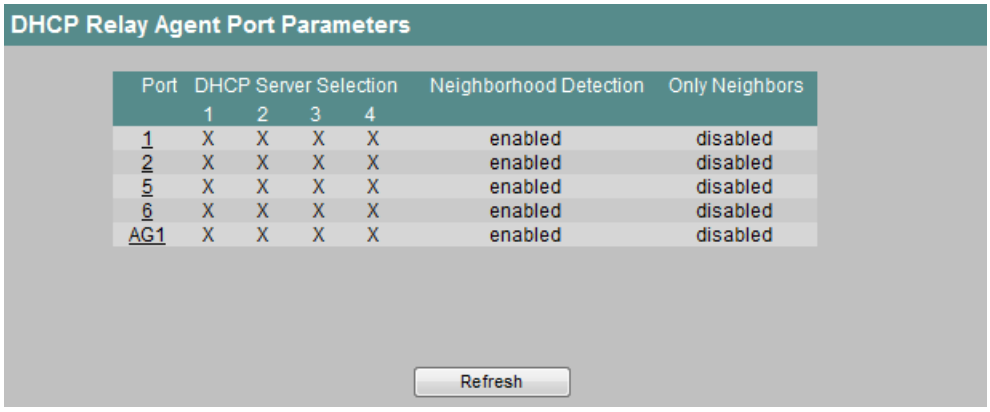


图 5-107 DHCP 中继代理端口参数 (DHCP Relay Agent Port Parameters)

端口表的三个列显示以下信息：

端口 (Port)
指定信息所关联的插槽和端口。 如果已组态链路汇聚，则此处显示该链路汇聚的名称。

DHCP 服务器选择 (DHCP Server Selection)
指示哪个 DHCP 服务器负责此端口。

邻近检测 (Neighborhood Detection)
显示是否为此端口启用邻近检测。

仅邻居 (Only Neighbors)
显示 DHCP 中继代理是否仅只对此端口的直接邻居起作用。

组态 DHCP 中继代理的端口

如果此时单击端口表第一列中的端口名称，将打开“DHCP 中继代理端口组态”(DHCP Relay Agent Port Configuration) 页面。

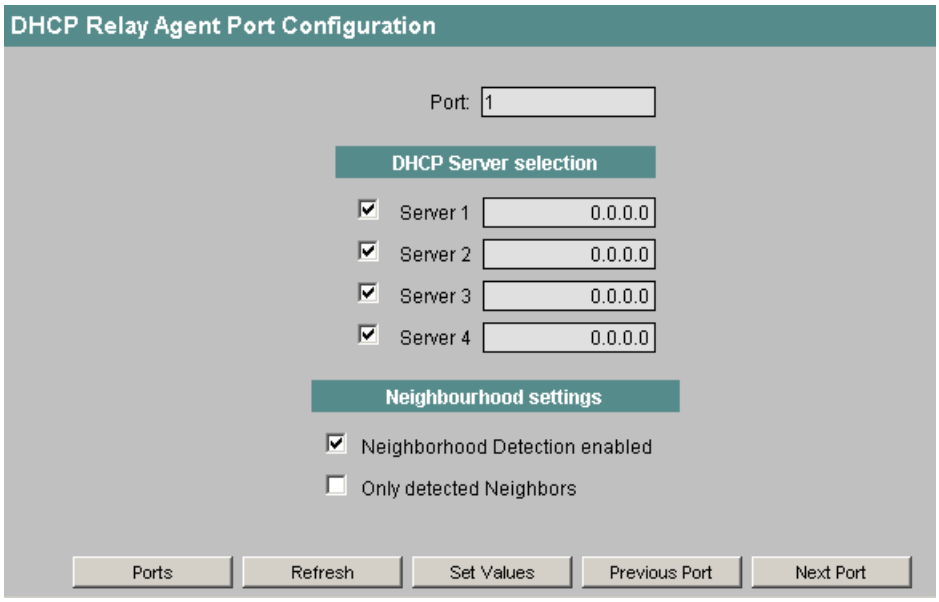


图 5-108 DHCP 中继代理组态

端口 (Port)
指定信息所关联的插槽和端口。 如果已组态链路汇聚，则此处显示该链路汇聚的名称。

DHCP 服务器选择 (DHCP Server Selection)
启用将负责该端口的 DHCP 服务器。

启用邻近检测 (Neighborhood Detection enabled)
如果想要尝试在转发之前将 DHCP 请求分配给邻居，则启用此选项。

仅限检测到的邻居 (Only detected Neighbors)
如果只想转发来源于检测到的邻居的 DHCP 请求，则启用此选项。

命令行接口语法

表格 5-81 DHCP 中继代理端口参数 - CLI\SWITCH\RELAGENT\PORTS>

命令	说明	注释
info	显示 DHCP 中继代理的所有端口参数	-
nbdetect [<E|D> [端口]]	启用/禁用 “启用邻近检测”(Neighborhood Detection enabled) 功能。	仅限管理员。

命令	说明	注释
onlynb [<E|D> [端口]]	启用/禁用“仅限检测到的邻居”(Only detected Neighbors) 功能。	仅限管理员。
sel [<S1|S2|S3|S4|all> <E|D> [端口]]	S1、S2、S3、S4 启用/禁用将负责该端口的 DHCP 服务器。 所有 启用/禁用 DHCP 服务器 S1 至 S4。	仅限管理员。

5.5.21 符合 IEEE 1588 的精确时间协议 (PTP)

简介

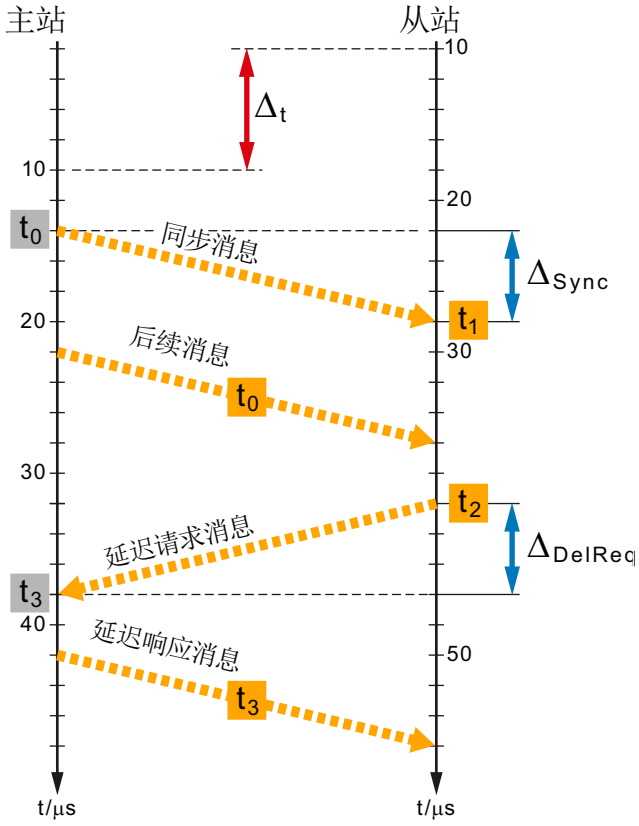
符合 IEEE 1588v2 的精确时间协议 (PTP) 允许连接至 SCALANCE X300 端口的设备（时间从站）进行时钟同步。这些设备使用“透明时钟”(Transparent Clock, TC) 机制通过网络转发同步帧。支持“端对端”和“对等”连接机制。

说明

PTP 仅受下列 SCALANCE X300 产品线的设备支持：

- 设备 X308-2M。
- X300 EEC 产品组的所有设备。
- XR300 产品组的所有设备。
- XR300 EEC 产品组的所有设备。

延迟请求响应机制



网络中的某个设备执行时间主站（最佳主站时钟，BMC）的功能，用于设置所有其它设备的基准时间。主站会周期性发送同步消息，如在示例中的时间 t_0 时。从站存储该消息到达时的时间 t_1。在第二条消息（后续消息）中，主设备将发送同步消息时的准确时间 t_0 通知给从站。

但是，仅通过这两个值无法计算从站时钟的偏差和消息延迟时间。为此，从站会再向主站发送一条延迟请求消息，并存储发送该消息的时间 t_2。利用延迟请求消息，主站将收到该消息的时间 t_3 通知给从站。

在接下来的计算中，假设消息从主站传送到从站所花费的时间与从站传送到主站的时间完全相同。这是使用电缆直接连接的情况。

根据 Δ_{Sync} 和 Δ_{DelReq} 的计算值，可以获得接收时间和发送时间的时间差：

$\Delta_{Sync} = t_1 - t_0$

$\Delta_{DelReq} = t_3 - t_2$

如果从站时间与主站时间的偏差为 Δ_t，则这两个计算公式仍无法提供消息延迟时间 Δ_D 的实际值，因为发送和接收时间基于不同的基准系统。计算实际消息延迟时间 Δ_D 的最简单方法是采用平均值：

$\Delta_D = (\Delta_{Sync} + \Delta_{DelReq}) / 2$

将 Δ_{Sync} 减去实际消息延迟时间 Δ_D 可获得从站时钟的偏差 Δ_t：

$\Delta_t = \Delta_{Sync} - \Delta_D$

如果 Δ_t 的值为正，则从站时钟“快”。如果 Δ_t 的值为负，则从时钟“慢”。

示例

在时间 $t_0 = 14$ µs 时，主站发送一条同步消息，该消息在时间 $t_1 = 28$ µs 时到达从站。Δ_{Sync} 的值计算如下：

$\Delta_{Sync} = t_1 - t_0 = 28\ \mu s - 14\ \mu s = 14\ \mu s$

如果主站时钟和从站时钟完全同步，则消息延迟时间为 14 µs，但不能仅靠这一次测量就得出结论。

为此，从站在时间 $t_2 = 40$ µs 时发送一条延迟请求消息，该消息在时间 $t_3 = 38$ µs 时到达主站。Δ_{DelReq} 的值为该消息的接收时间和发送时间之间的差值：

$\Delta_{DelReq} = t_3 - t_2 = 38\ \mu s - 40\ \mu s = -2\ \mu s$

实际消息延迟时间 Δ_D 是 Δ_{Sync} 和 Δ_{DelReq} 的平均值，因为这可消除两个设备时钟的时间偏差。

$\Delta_D = (\Delta_{Sync} + \Delta_{DelReq}) / 2$

$\Delta_D = (14\ \mu s - 2\ \mu s) / 2 = 6\ \mu s$

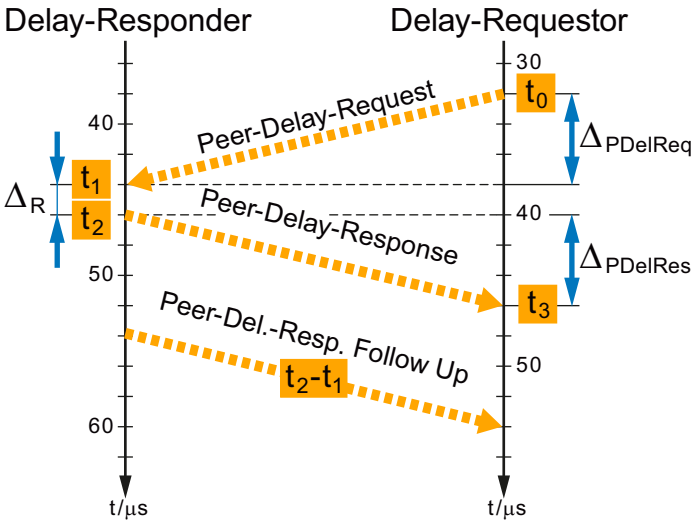
从站时钟的偏差为

$\Delta_t = \Delta_{Sync} - \Delta_D = 14\ \mu s - 6\ \mu s = 8\ \mu s$

因此，从站时钟“快”，需要调整 8 µs。

对等延迟机制

对等延迟机制的目的是计算符合 PTP 的设备的两个端口间消息的延迟时间。与在从站和主站之间传输并且经过多个网络节点的延迟请求响应消息相比，对等延迟消息仅与相关的邻近节点进行交换，因此称为“对等延迟”。



延迟请求器向邻近节点（延迟响应器）发送一条对等延迟请求消息，并存储发送该消息的时间 t_0。延迟响应器然后立即回复一条对等延迟响应消息。在对等延迟响应后续消息的修正字段中，将输入对等延迟响应消息的发送时间 t_2 与对等延迟请求消息的接收时间 t_1 之间的时间差：

$\Delta_R = t_2 - t_1$

在对等延迟响应消息的接收时间 t_3 时，延迟请求器具有计算邻近节点消息延迟时间所需的所有数据：

$\Delta_{PDelReq} = \Delta_{PDelRes} = (t_3 - t_0 - \Delta_R) / 2$

要计算从站时钟的偏差，同步消息和后续消息也必须通过对等延迟机制进行计算。“对等透明时钟”部分介绍了完整的同步周期。

与网络拓扑无关的同步

以上几个部分中介绍的计算仅适用于在两个通信伙伴之间通过直接电缆连接进行消息交换的情况。但通常情况下，网络包括多台交换机，这些交换机必须在时间主站和从站之间传输时钟消息。在多台交换机之间实现同步的方式取决于交换机所分配到的设备类别（边界时钟还是透明时钟）以及计算消息延迟时间所使用的方法（延迟请求响应机制还是对等延迟机制）。

用于处理 PTP 消息的机制必须针对每个设备进行组态。在一个网络区段中不能同时使用两种延迟机制。某个区段内的所有设备都必须针对延迟请求响应机制或对等延迟机制进行组态。

所涉及的所有交换机都应支持 PTP 以实现精确时钟同步。由于存在排队问题，不支持 PTP 的交换机无法保证在主站和从站之间保持恒定的消息延迟时间。

边界时钟

该交换机在一个端口执行从站功能，使自身与时间主站同步。对于其它连接的设备，该交换机执行主站功能并周期性将同步帧发送到这些节点。在具有多台交换机和终端设备的网络中，BMC 算法自动处理在网络中选择最精确时钟的任务。主站-从站层级决定了哪台交换机在 BMC 的指示下将自身与邻近交换机同步。

使用边界时钟的同步机制

如果为延迟请求响应机制组态了边界时钟，其将向时间主站发送延迟请求消息，向从站发送同步和后续消息。

在对等延迟机制下，边界时钟将计算与每个端口对应的邻近设备的消息延迟时间。其通过评估主站的同步和后续消息对自身进行同步。边界时钟允许通过发送同步和后续消息来同步从站。

透明时钟

透明时钟不会将自身与时间主站同步，但会在时间主站和要同步的从站之间转发 PTP 消息。与边界时钟相比，透明时钟可实现更精确的同步，因为忽略了边界时钟同步中的误差。因此，在线性总线或环形拓扑中串联使用交换机时，最好将它们配置为透明时钟。

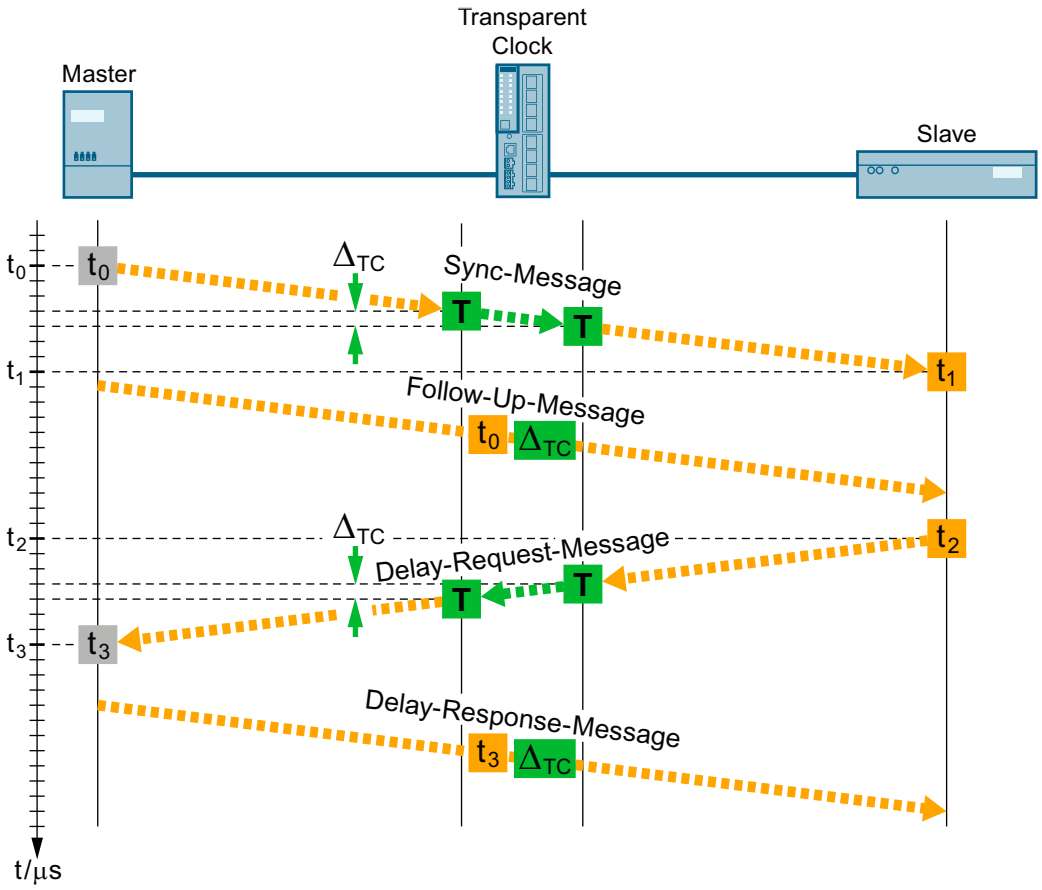
即使网络中的拓扑发生变化，透明时钟提供的同步仍然比边界时钟提供的同步更精确。无论在拓扑中的位置如何，透明时钟的功能都是转发同步帧。而对于边界时钟，会将主站和从站分配到各个端口，进而使整个同步层级发生变化。所有设备可能在数秒后才能与时间主站重新同步。

使用透明时钟的同步机制

计算多个网络节点上的实际消息延迟时间时，还必须考虑透明时钟中处理消息所需的时间。这意味着透明时钟必须计算在输入端口收到消息与在输出端口转发消息之间的时间，并将该值发送给从站。为此，PTP 消息中存在一个修正字段，交换机可在其中输入适当的值。从站在计算消息延迟时间时将考虑此信息。

透明时钟如何处理该修正信息取决于组态的延迟机制。在延迟请求响应机制下为端对端透明时钟，在对等延迟机制下则为对等透明时钟。

端对端透明时钟

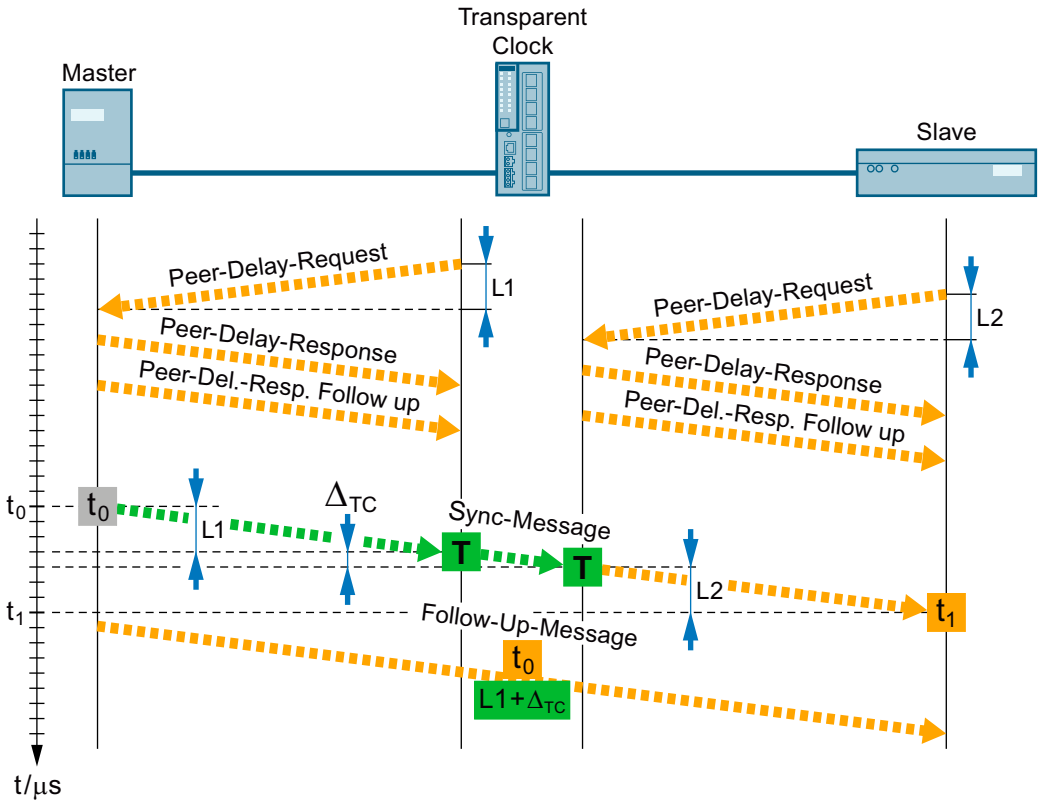


在显示的示例中，时间主站发送一条同步消息。在输入端口收到该消息和在输出端口转发该消息之间的时间 Δ_{TC} 由透明时钟在后续消息的修正字段中输入。发送该消息的时间 t_0 也由从站通过后续消息接收，可以如前文所述使用该信息进行所需计算。

如果发送至从站的消息被其它透明时钟转发，则每个设备都会将其时间 Δ_{TC} 添加到后续消息的修正字段内容中。当同步消息到达从站时，修正字段包含处理透明时钟中的消息所需的所有时间总和。设备也以相同的方式处理延迟请求消息。

从站通过值 Δ_{TC} 修正消息延迟时间，如果有多个透明时钟，则通过所有 Δ_{TC} 值的总进行修正，从而可按“延迟请求响应机制”部分中所述对其时钟进行同步。

对等透明时钟



在对等延迟机制下，每个设备都计算其端口邻近设备的消息延迟时间。透明时钟获取主站的消息延迟时间 L1，从站获取透明时钟的消息延迟时间 L2。

透明时钟花费时间 Δ_{TC} 处理同步消息。透明时钟在后续消息的修正字段中输入 L1 和 Δ_{TC} 的和。从站然后将修正字段的内容添加到用于接收输入同步消息的输入端口的消息延迟时间 L2 中。通过这种方式，可获得主站和从站之间的消息延迟时间。

如果发送至从站的消息被多个透明时钟转发，则每个透明时钟都会更改后续消息的修正字段内容：用于接收同步消息的邻近设备的消息延迟时间，以及处理消息的时间 Δ_{TC} 都将添加到修正字段的内容中。

对等透明时钟的一个特殊优势是还针对阻塞端口计算邻近设备的消息延迟时间。重新组态网络后，这意味着从站能够很快获得正确的消息延迟时间。

5.5.22 通过 WBM 组态精确时间协议

IEEE 1588 与 SCALANCE 设备

说明

以下设备从固件版本 3.5.0 开始提供 IEEE 1588 菜单项：

- SCALANCE X308-2M
- SCALANCE X308-2M PoE
- SCALANCE X302-7EEC
- SCALANCE X307-2EEC
- SCALANCE XR324-12M
- SCALANCE XR324-4M PoE
- SCALANCE XR324-4M EEC

同步帧使用“透明时钟”机制通过网络进行转发，并支持“端对端”和“对等”修正机制。

SCALANCE 设备以“两步时钟”的形式工作。 它们即支持在网络中使用一步时钟，也支持在网络中使用两步时钟。

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。 列出的 SCALANCE 设备还可通过适当的硬件支持符合 IEEE 1588v2 的时钟同步。 提供这些设备时以及对这些设备执行“复位为出厂默认设置”后，IEEE 1588v2 功能为禁用状态。 要使用 IEEE 1588v2，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。 IEEE 1588v2 还可以在 HRP、环网备用链接、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。

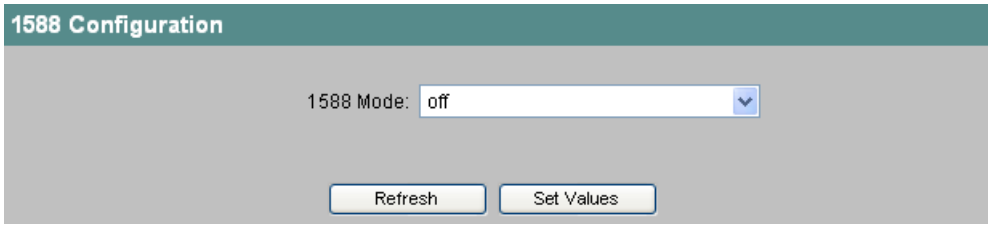


图 5-109 1588 组态

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。
- **透明时钟 (Transparent Clock)**
  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。

1588 透明时钟组态

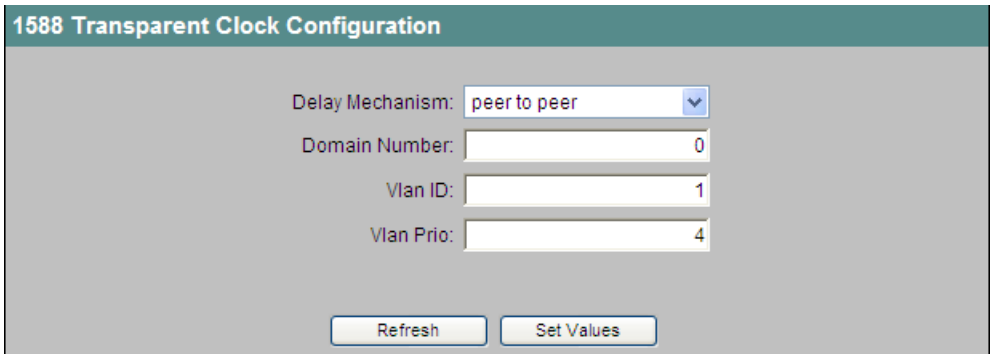


图 5-110　1588 透明时钟

延迟机制 (Delay Mechanism)
指定设备将使用的延迟机制：

- 端对端（将使用延迟请求响应机制）
- 对等（将使用对等延迟机制）

域编号 (Domain Number)
在此处输入设备的域编号。 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。

Vlan ID
在此处输入具有 “透明时钟”(Transparent Clock) 功能的设备的 Vlan ID。

Vlan 优先级 (Vlan Prio)
在此处输入 VLAN 的优先级。

1588 透明时钟端口参数

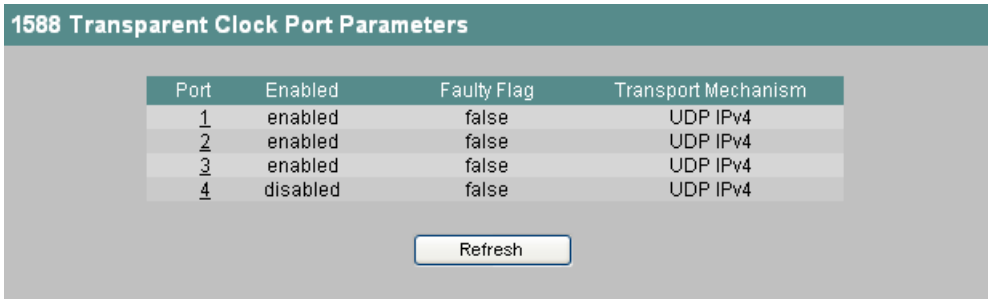


图 5-111　1588 透明时钟端口参数

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。 如果单击某个端口号，将显示相应的页面“1588 透明时钟端口组态”(1588 Transparent Clock Port Configuration)。

启用 (Enabled)
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)
“以太网”(Ethernet) 或“UDP IPv4”。

1588 透明时钟端口组态

如果单击 “透明时钟端口参数”(Transparent Clock Port Parameters) 页面上的表格中的某个端口号，则会打开此页面。

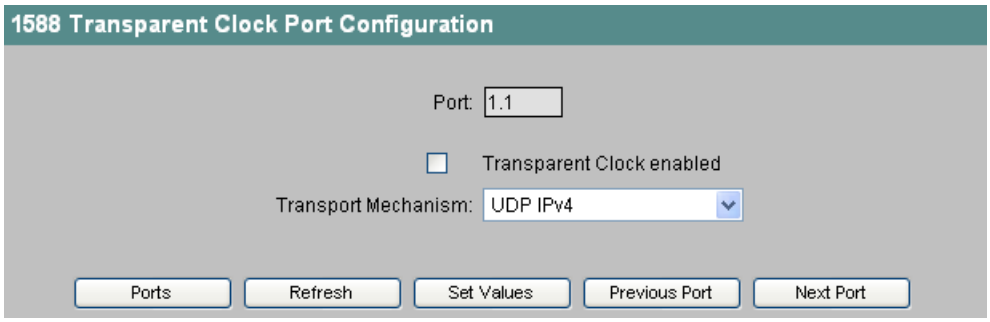


图 5-112　1588 透明时钟端口组态

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。

启用透明时钟 (Transparent Clock enabled)
如果想要设备通过此端口处理 PTP 消息，则选中此复选框。

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

端口 (Ports)
如果单击此按钮，将切换到 “透明时钟端口参数”(Transport Clock Port Parameter) 页面。

上一端口 (Previous Port) 和下一端口 (Next Port)
如果单击此按钮，将直接切换到前一个或后一个端口的组态页面，而无需调用 “透明时钟端口参数”(Transparent Clock Port Parameters) 页面。

5.5.23 通过 CLI 组态精确时间协议

CLI\SWITCH\1588>

命令	说明		注释
mode [off|TC]	对设备启用/禁用精确时间协议，并指定设备对 PTP 的响应方式：		仅限管理员。
	off	设备不处理任何 PTP 消息。	
	TC	透明时钟	
TC	打开用于将设备组态为透明时钟的菜单。		仅限管理员。

CLI\SWITCH\1588\TC>

命令	说明		注释
delaymec [E2E|P2P]	指定设备的延迟机制：		仅限管理员。
	E2E	端对端 （将使用延迟请求响应机制）。	
	P2P	对等 （将使用对等延迟机制）。	
domainnb [编号]	指定时间域的标识号。仅同步该域内的设备，具有不同域编号的 PTP 消息将被丢弃。		仅限管理员。
vlanid [VID]	指定 VLAN ID。		仅限管理员。
vlanprio [<0..7>]	指定 VLAN 优先级。		仅限管理员。
PORTS	打开 "端口"(PORTS) 菜单。		仅限管理员。

CLI\SWITCH\1588\TC\PORTS>

命令	说明		注释
tcport <E|D> [端口]	启用/禁用指定的端口。 使用连字符指定端口的范围。 用空格或逗号分隔多个端口。		仅限管理员。
transmec <IPv4|ETH> [端口]	指定用于传送 PTP 消息的协议。 端口的通信伙伴也必须支持该协议。		仅限管理员。
	IPv4	Internet 协议（第 3 层）	
	ETH	以太网（第 2 层）	

5.5.24 端口诊断

5.5.24.1 电缆测试器 (SCALANCE X-300/X408-2)

交换机电缆测试器

利用此对话框，每个以太网端口都可以对电缆运行独立的故障诊断。这样便可定位短路和电缆断开。

说明

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。
在启动“电缆测试器”功能之前，还需要禁用设备所有环网端口的“链路检查”功能。

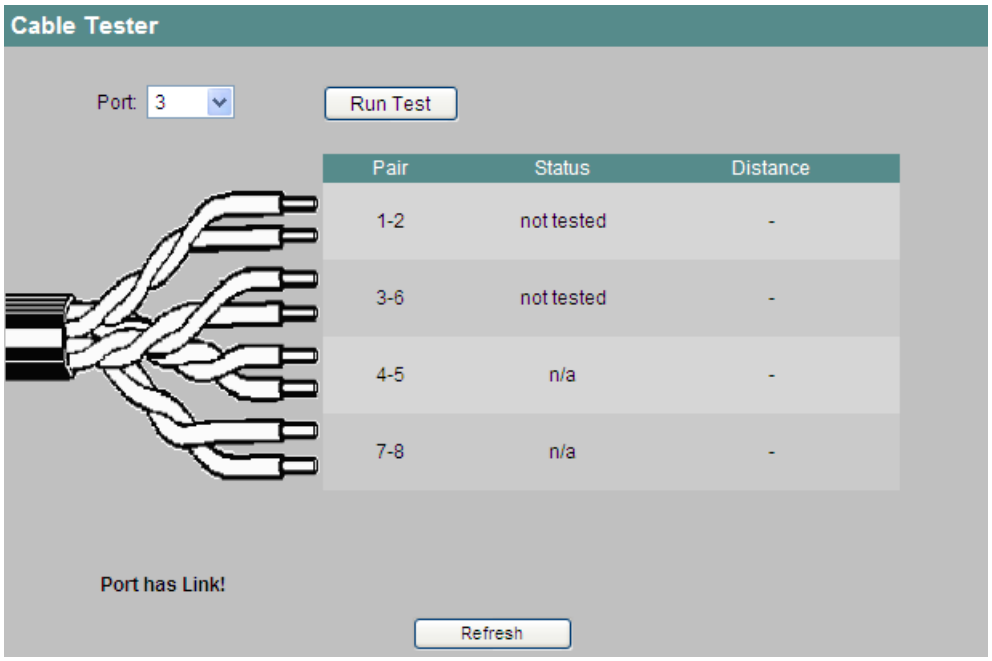


图 5-113　电缆测试器

端口 (Port)

在此处指定要测试的端口。

运行测试 (Run Test)

单击此按钮激活测试。

线对 (Pair)

显示电缆中的线对。
线对 4-5 和 7-8 不适用于快速以太网。

状态 (Status)

显示行状态。

距离 (Distance)

显示与电缆末端、电缆断点或短路位置的距离。

命令行接口语法

表格 5-82　电缆测试器 - CLI\SWITCH\PORTDIAG\CABLETESTER>

命令	说明	注释
runtest [端口]	测试指定的端口。 如果未指定任何端口，则测试所有端口。	仅限管理员。

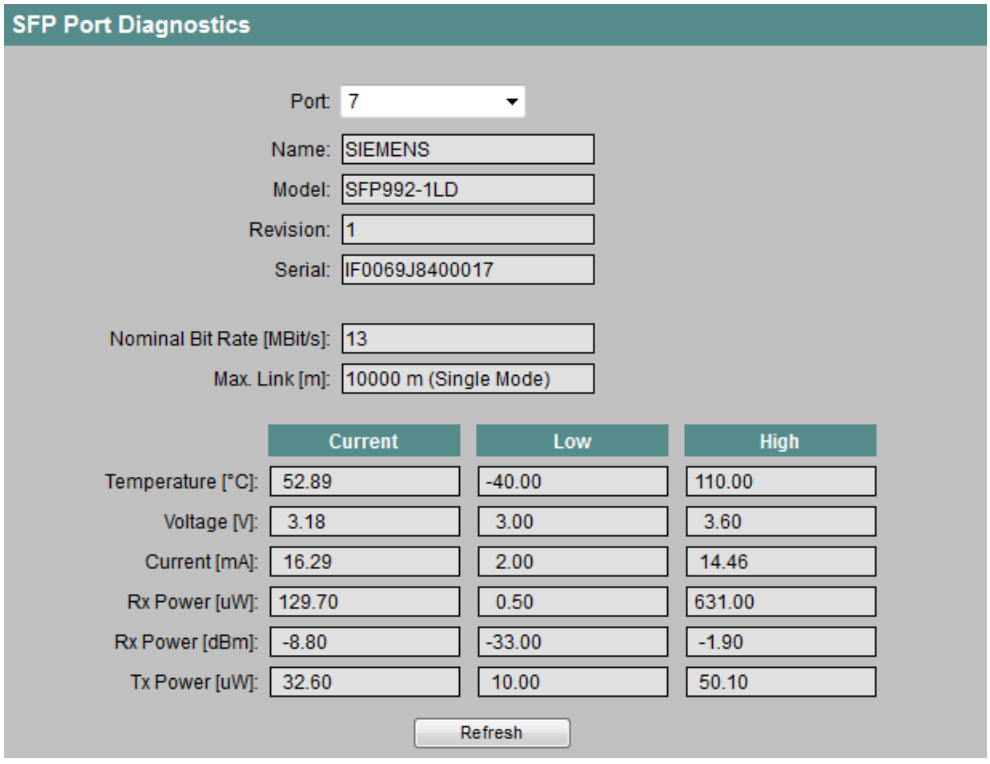
5.5.24.2　SFP 诊断

要求

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。

仅能对带诊断功能的收发器使用 SFP 诊断。

SFP 端口诊断



端口 (Port)
在此处指定要测试的 SFP 端口。

根据选择将显示以下内容：

- 名称 (Name)（只读）
  SFP 端口的名称
- 名称 (Name)（只读）
  使用的 SFP 收发器的名称
- 版本 (Revision)（只读）
  SFP 收发器的硬件版本
- 序列号 (Serial)（只读）
  SFP 收发器的序列号
- 额定位速率 (Nominal Bit Rate)（只读）
  SFP 端口的额定位速率
- 最长链路 (Max. Link)（只读）
  使用此介质时支持的最远距离（单位为米）。

表中始终显示以下参数的最新值 (Current)、最低值 (Low) 和最高值 (High)。

温度 (Temperature)（只读）

端口的温度。

电压 (Voltage)（只读）

施加到端口的电压。

电流 (Current)（只读）

为连接到此端口的设备提供的电流。

接收功率 (Rx Power)（只读）

端口的接收功率。

发送功率 (Tx Power)（只读）

端口的发送功率。

命令行接口语法

表格 5-83　SFPDIAGNOSTIC - CLI\SWITCH\PORTDIAG\SFPDIAG>

命令	说明	注释
details [端口]	测试指定的 SFP 端口。	仅限管理员。

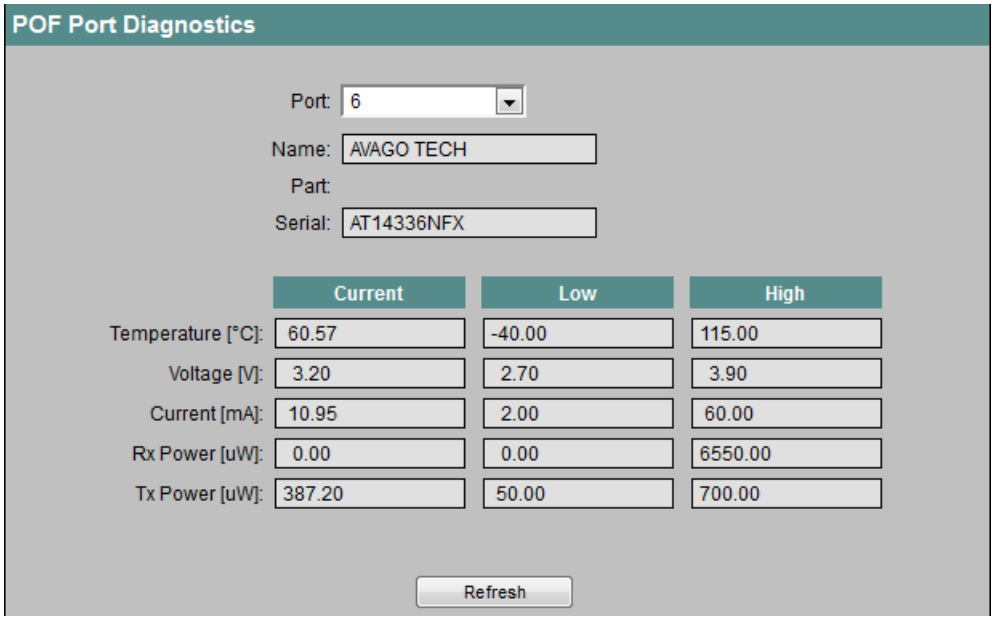
5.5.24.3　POF 诊断

要求

在此页面中，可以为每个 POF 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。

仅能对带诊断功能的收发器使用 POF 诊断。含有带诊断功能的收发器的设备和模块名称中有补充标识"P"。

POF 端口诊断



端口 (Port)
在此处指定要测试的端口。

根据选择将显示以下内容：

- 名称 (Name)（只读）
  POF 端口的名称
- 型号 (Model)（只读）
  所用的 POF 型号
- 序列号 (Serial)（只读）
  POF 模块的序列号

表中始终显示以下参数的最新值 (Current)、最低值 (Low) 和最高值 (High)。

温度 (Temperature)（只读）

端口的温度。

电压 (Voltage)（只读）

施加到端口的电压。

电流 (Current)（只读）

为连接到此端口的设备提供的电流。

接收功率 (Rx Power)（只读）

端口的接收功率。

发送功率 (Tx Power)（只读）

端口的发送功率。

命令行接口语法

表格 5-84　SFPDIAGNOSTIC - CLI\SWITCH\PORTDIAG\POFDIAG>

命令	说明	注释
details [端口]	测试指定的 POF 端口。	仅限管理员。

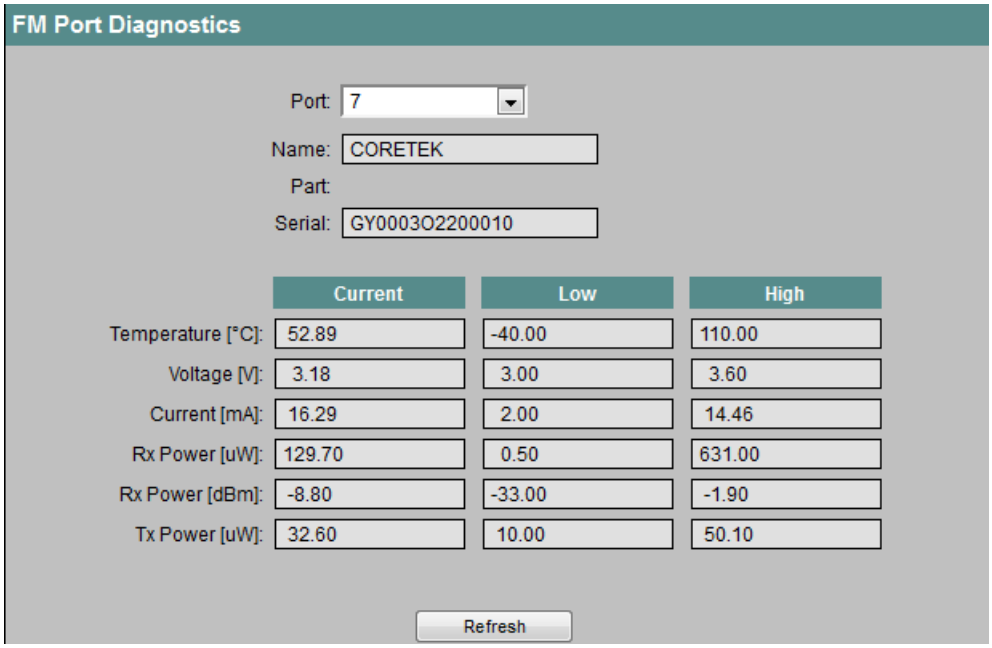
5.5.24.4　FM 诊断

要求

在此页面中，可以为每个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。

仅能对带诊断功能的收发器使用 FMP 诊断。含有带诊断功能的收发器的设备和模块名称中有补充标识“FM”。

FM 端口诊断



端口 (Port)
在此处指定要测试的端口。

根据选择将显示以下内容：

- 名称 (Name)（只读）
  端口的名称
- 型号 (Model)（只读）
  所用的 FM 收发器
- 序列号 (Serial)（只读）
  FM 收发器的序列号

表中始终显示以下参数的最新值 (Current)、最低值 (Low) 和最高值 (High)。

温度 (Temperature)（只读）

端口的温度。

电压 (Voltage)（只读）

施加到端口的电压。

电流 (Current)（只读）

为连接到此端口的设备提供的电流。

接收功率 (Rx Power)（只读）

端口的接收功率。

发送功率 (Tx Power)（只读）

端口的发送功率。

命令行接口语法

表格 5-85　SFPDIAGNOSTIC - CLI\SWITCH\PORTDIAG\FMDIAG>

命令	说明	注释
details [端口]	测试指定的端口。	仅限管理员。

5.5.24.5　POF 端口

要求

光纤电缆的诊断页面仅在使用塑料光纤（POF）时才显示正确的链接功率裕量。 如果使用聚合体覆层纤维（PCF），则不能进行诊断。

仅能对带诊断功能的收发器使用 POF 诊断。含有带诊断功能的收发器的设备和模块名称中有补充标识“P”。

塑料光纤管理

此页面显示连接塑料 FO 电缆的接口的诊断数据。

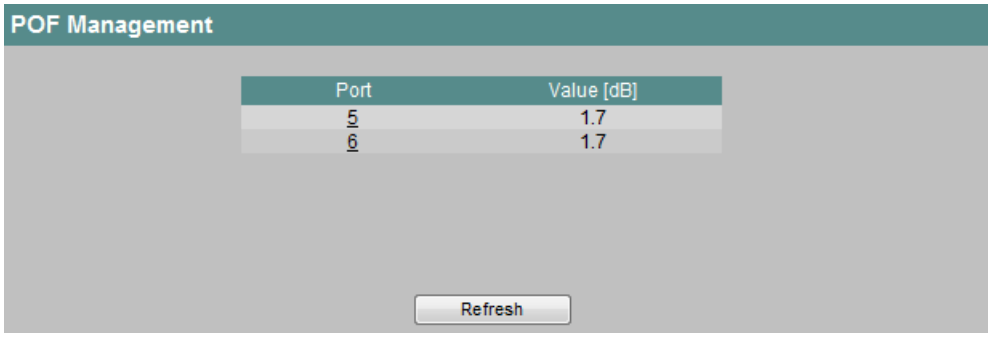


图 5-114　POF 管理

在此可看到每个 POF 端口当前可用的链接功率裕量的数值。

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

如果单击显示的某个端口，将显示诊断页面。它将显示随着时间的推移可用的链接功率裕量的信息。

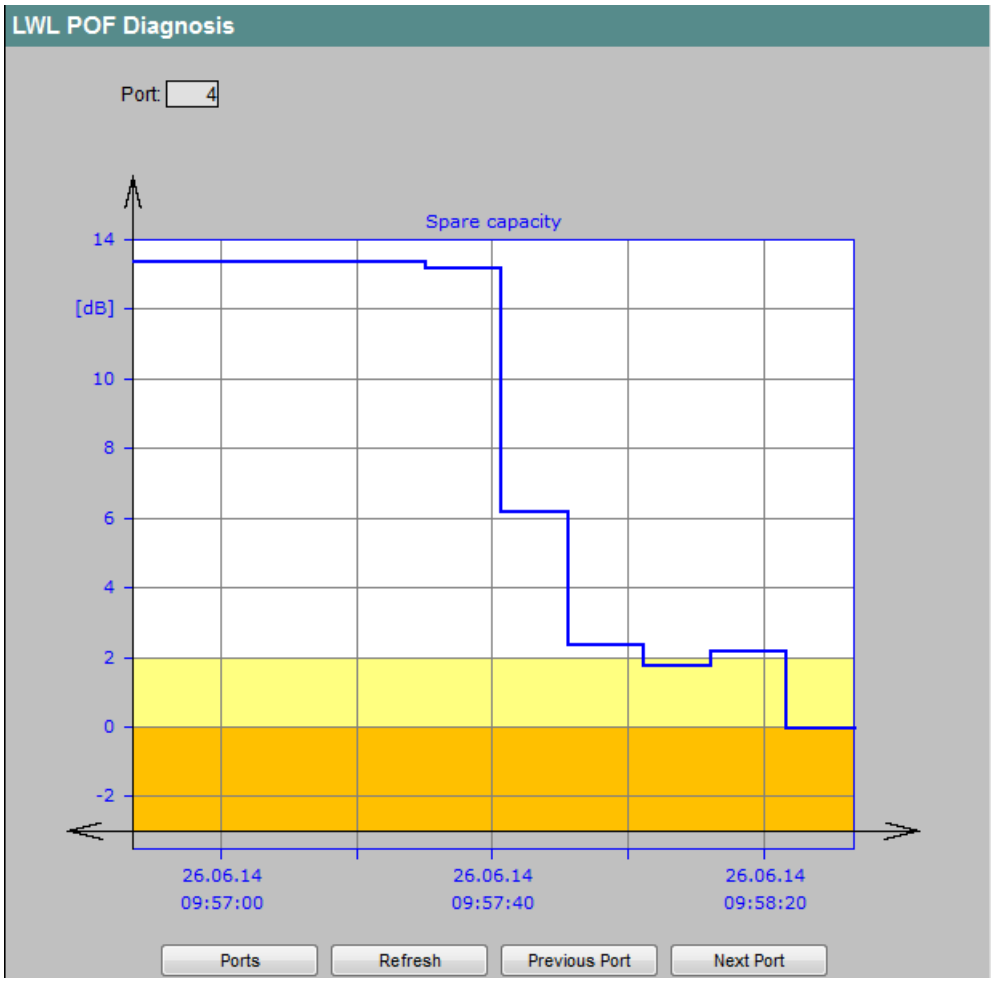


图 5-115　POF 光纤诊断

垂直轴将显示可用的链接功率裕量，单位为 dB。测量值仅具有能够在 0 dB 到 6 dB 范围内正确显示现有链接功率裕量所需的精度。

横轴显示从工业以太网交换机启动到当前时间的相对时间和当前日期。 将采用运行正在使用的 Web 浏览器的 PC 中的日期和时间信息。

该图可分成下列区域：

- **白色区域**
  对于无故障操作，具有充足的链接功率裕量。安装了 X-200 工业以太网交换机后，链接功率裕量应在该范围之内。
- **黄色区域**
  如果链接功率裕量在该范围之内，则需要维护。黄色区域的边界位于 2 dB 的链接功率裕量上。为确保系统的长期功能，应执行维护。如果链接功率裕量在黄色区域内，则将触发事件。
- **橙色区域**
  如果链接功率裕量在橙色范围内，则必须进行紧急维护。橙色区域的边界位于 0 dB 的链接功率裕量上。如果链接功率裕量在橙色范围内，则将触发事件且相关端口的 FO LED 亮起。

5.5.25 回路检测

工作原理

如果为端口设置了“环路检测”功能，则该端口将发送特殊的测试帧，即环路检测帧。如果这些帧被发送回设备，则说明存在 Loop。

如果设备在另一个端口再次接收到发出的帧，说明存在 Local Loop。设备本身是环路的一部分。

如果设备在同一端口接收到发出的帧，说明在其它网络组件上存在环路，即 Remote Loop。

网络中的环路

例如，环路可能因组态错误或插入电缆不当引起。电缆的机械性损坏也可能导致短路并造成环路。

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

启用该功能

说明

仅可为未组态为环网端口或备用端口的端口激活环路检测。

为设备启用该功能

要为设备普遍启用“环路检测”功能，请在“环路检测组态”(Loop Detection Config) 页面上选择“启用环路检测”(Loop Detection Enabled) 选项。在该页面上，可设置应用到所有端口的基本设置，请参见“环路检测组态”部分。

使用基本设置并不能为所有端口启用该功能。需要分别组态各个端口。

启用端口

对于各端口，可在“环路检测端口组态”(Loop Detection Port Configuration) 页面上设置“环路检测”功能，请参见“环路检测端口组态”部分。

如果有错误出现，则只有端口组态为“发送方”时才可以被屏蔽以防止形成环路。

应用示例

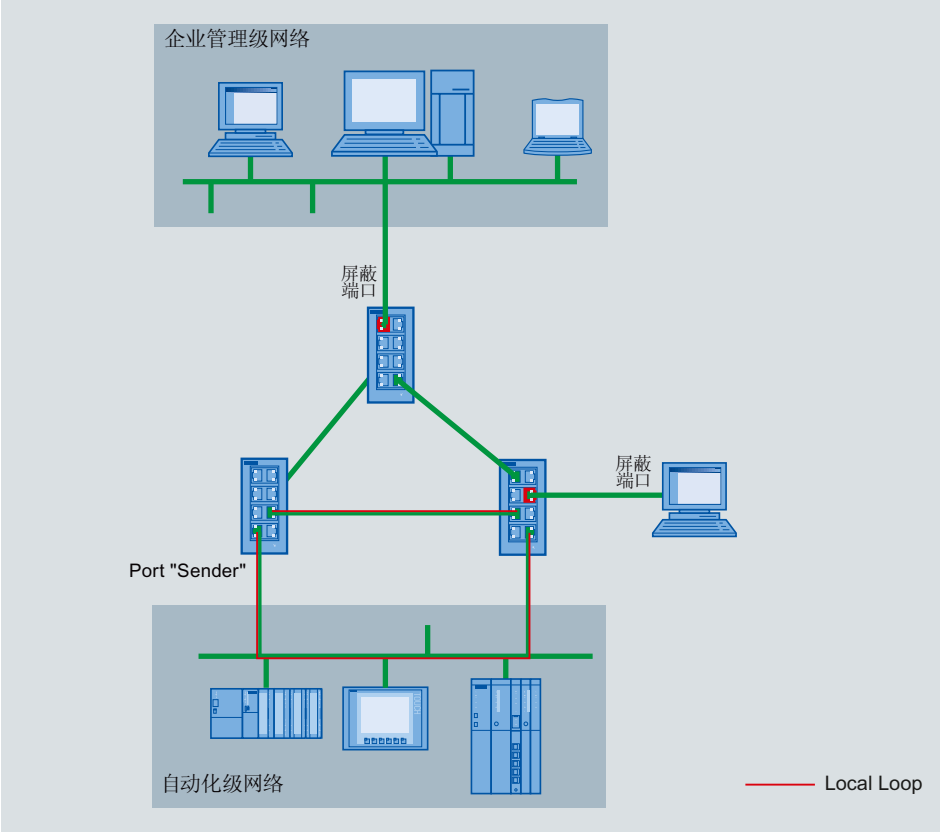


图 5-116　已组态发送方的环路检测

上图显示了通过 MRP/HRP 环网连接的企业层级和自动化层级网络。标红的屏蔽端口被设置为“禁用端口”。

如果环路出现在自动化层级的网络中，则在检测到此环路时会将其视为“Remote Loop”。由于存在这些屏蔽端口，环路检测帧将无法转发至企业层级的网络或终端设备。

如果出现了 Local Loop，则会在接收到指定的环路检测帧数后自动屏蔽相关端口。

接下来的几部分内容基于 WBM 页面说明了环路检测的设置。

环路检测组态

在该页面上，可对适用于所有端口的环路检测进行设置。

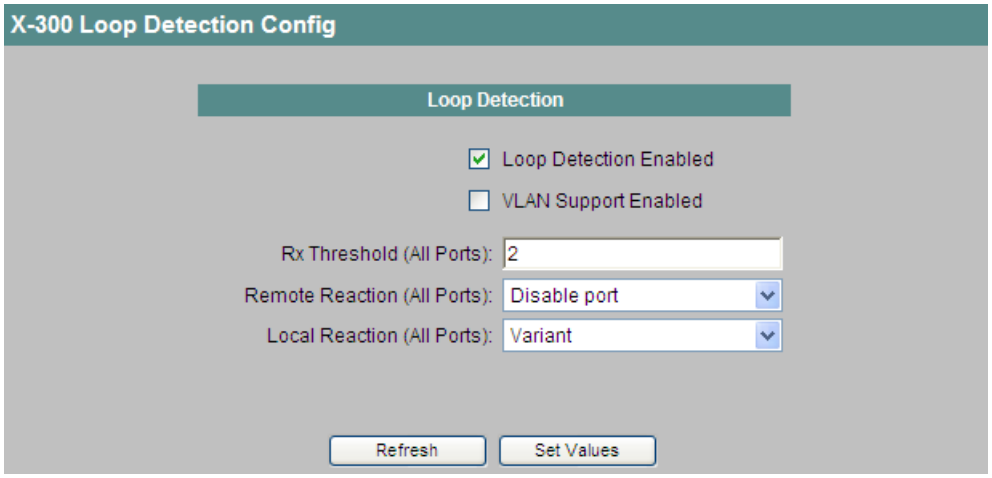


图 5-117　环路检测的组态

说明

只能在转发环路检测帧的设备之间检测到环路。无法检测到经由端口被屏蔽的网络组件构成的环路。

启用环路检测 (Loop Detection Enabled)

通过单击该复选框来启用或禁用回路检测。
如果禁用回路检测，则会转发其它设备的回路检测帧。

启用 VLAN 支持 (VLAN Support Enabled)

通过单击该复选框可为所有端口指定是否针对在相关端口的所有已组态 VLAN 发送环路检测帧。
如果禁用了 VLAN 支持，则只发送不带 VLAN 标记的环路检测帧。

Rx 阈值（所有端口）(Rx Threshold (All Ports))

输入一个数字，指定接收到多少环路检测帧后视为环路存在。
如果进行了特定于端口的设置，将显示“Variant”，请参见下文。

远程反应（所有端口）(Remote Reaction (All Ports))

指定在出现远程环路时设备的反应方式。从下拉列表中选择两个选项之一：

- 无反应 (No reaction)：
  环路对于出现环路的端口不起作用。
- 禁用端口 (Disable port)：
  屏蔽出现环路的端口。

如果进行了端口特定的设置，则会显示“Variant”，请参见下文。

本地反应（所有端口）(Local Reaction (All Ports))：

指定在出现本地环路时设备的反应方式。从下拉列表中选择两个选项之一：

- 无反应 (No reaction)：
  环路对于出现环路的端口不起作用。
- 禁用端口 (Disable port)：
  屏蔽端口。

如果进行了端口特定的设置，则会显示“Variant”，请参见下文。

环路检测端口控制

可在此页面上查看各个端口的具体设置。

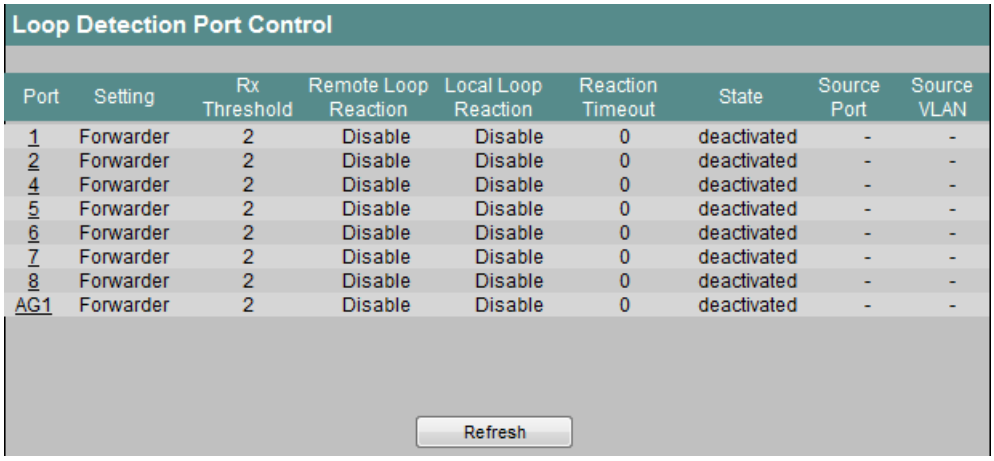


图 5-118　环路检测端口控制

要组态端口，请单击在“端口”(Port) 列中相关端口号。将出现“环路检测端口组态”(Loop Detection Port Configuration) 页面。

环路检测端口组态

在此页面上对各个端口进行这些特定设置。

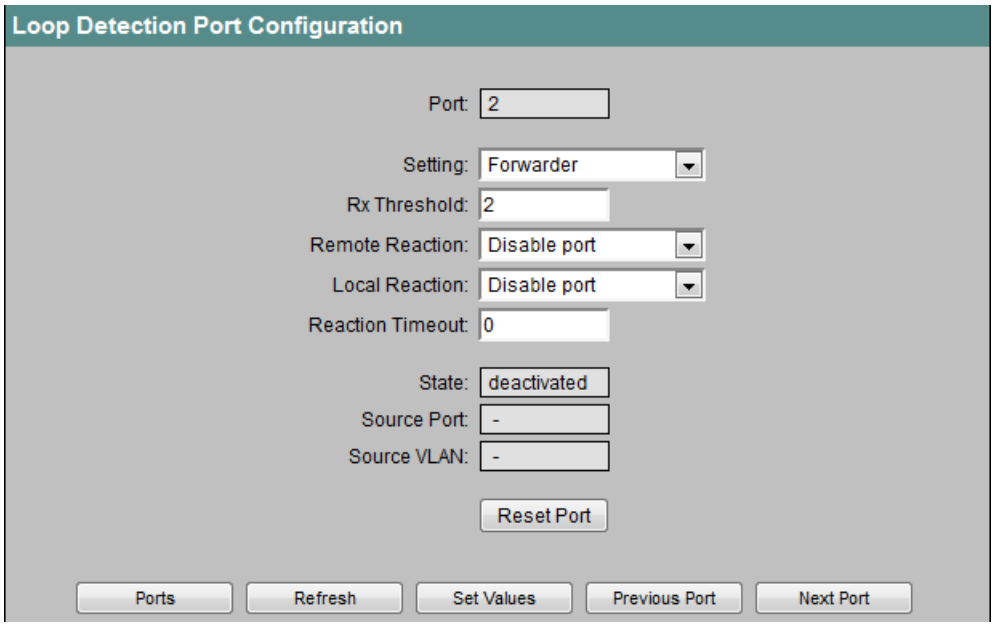


图 5-119　环路检测端口组态

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”。

端口

此框显示了所选端口的编号。

设置 (Setting)

指定端口处理环路检测帧的方式。从下拉列表中选择下列选项之一：

- 传送方 (Transmitter)
  发送并转发环路检测帧。
- 转发方 (Forwarder)
  转发来自其它设备的环路检测帧。
- 屏蔽 (Blocked)
  阻止转发环路检测帧。

Rx 阈值 (Rx Threshold)

通过输入一个数值指定接收到多少环路检测帧后才视为存在环路。

如果端口接收到的环路检测帧多于指定数量，则端口将不再转发环路检测帧。

远程反应 (Remote Reaction)

指定在出现远程环路时端口的响应方式。从下拉列表中选择两个选项之一：

- 无反应 (No reaction)：
  环路对端口不起作用。
- 禁用端口 (Disable port)：
  屏蔽端口。

本地反应 (Local Reaction)

指定在出现本地环路时端口的响应方式。从下拉列表中选择两个选项之一：

- 无反应 (No reaction)
  环路对端口不起作用。
- 禁用端口 (Disable port)
  屏蔽端口。

反应超时

指定经过多少秒后设备会自动切换到回路之前所处的状态。如果将该值设置为“0”，则环路后需要使用“端口复位”(Reset Port) 命令再次手动启用该端口。

状态 (State)

该框显示对此端口是启用还是禁用环路检测。

源端口 (Source Port)

该框显示触发了上一次响应的环路检测帧的接收方端口。

源 VLAN (Source VLAN)

该框显示触发了上一次响应的环路检测帧的 VLAN-ID。
仅当已在“环路检测组态”(Loop Detection Configuration) 页面上选择了“启用 VLAN 支持”(VLAN Support Enabled) 时才显示。

“复位端口”(Reset Port) 按钮

消除网络中的环路后，单击该按钮重置端口。

错误消息

如果“环路检测”(Loop Detection) 功能检测到环路，则通过故障 LED、信号触点与相应消息文本进行指示。将采用为事件“环路检测状态更改”所组态的相同指示方法显示消息文本，请参见“代理事件组态 (页 126)”部分。

可能的指示方法包括电子邮件、陷阱、日志文件中或 Syslog 服务器上的条目。

可在附录 D "SCALANCE X300/X400 的错误消息 (页 433)"中找到消息文本的列表。

故障 LED 和信号触点

如果检测到环路，则设备的故障 LED 点亮，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。

状态消息

可能出现以下状态消息：

- "<端口号> 上检测到本地环路。端口已禁用。"
  设备已检测到本地环路。相关端口已禁用。所连接的伙伴仍然认为处于"接通"状态。
- "<端口号> 上检测到本地环路。端口禁用 <等待时间> 秒。"
  设备已检测到本地环路。相关端口禁用一段特定时间。所连接的伙伴仍然认为处于"接通"状态。
- "<端口号> 上检测到远程环路。端口已禁用。"
  设备已检测到远程环路。相关端口已禁用。所连接的伙伴仍然认为处于"接通"状态。
- "<端口号> 上检测到远程环路。端口禁用 <等待时间> 秒。"
  设备已检测到远程环路。相关端口禁用一段特定时间。所连接的伙伴仍然认为处于"接通"状态。
- "<端口号> 上检测到本地环路。"
  设备已检测到本地环路。
- "<端口号> 上检测到远程环路。"
  设备已检测到远程环路。
- "再次启用 <端口号> 以进行环路检测。"
  对端口再次启用"环路检测"功能。
- "<端口号> 因环路检测而被禁用后再次启用。"
  再次启用因环路而禁用的端口。

命令行接口语法

表格 5-86　环路检测组态 - CLI\SWITCH\LOOPD >

命令	说明	注释
info	显示关于“环路检测组态”的信息。	
loopd [E | D]	启用/禁用环路检测。	仅限管理员。
vlansupp [E | D]	启用/禁用 VLAN 支持。	仅限管理员。

表格 5-87　环路检测组态 – CLI\SWITCH\LOOPD\PORTS >

命令	说明	注释
info	显示关于“环路检测端口组态”的信息。	
local <N | D> [ports]	指定对本地环路的响应。	仅限管理员。
loopd <B | F | S> [ports]	为环路检测定义端口行为： • “阻止” • “转发方” • “发送方”	仅限管理员。
remote <N | D> [ports]	指定对远程环路的响应。	仅限管理员。
reset [ports]	重新激活因检测到环路而被禁用的端口。	仅限管理员。
rxthres <count> [ports]	指定接收到多少个环路检测帧后才视为存在回路。	仅限管理员。
timeout [<0..86400> [ports]]	指定经过多少秒后设备会自动切换到回路之前所处的状态。 如果将该值设置为“0”，则环路后需要使用“reset”命令再次手动启用该端口。	仅限管理员。

5.5.26 NAT - 网络地址转换

说明

只有 SCALANCE X300 和 SCALANCE X408 支持 NAT 功能。

网络地址转换 (NAT, Network Address Translation) 是指与数据流相关的路由器中的网络地址转换。它并不一定只表示 IP 地址。如果具有本地地址的节点接管外部服务器功能，则路由器中的 IP 地址和端口号都将被替换。

使用 NAT 的最常见原因是由于不想将本地网络中的设备 IP 地址暴露给外部设备。

传统 NAT (Traditional NAT)

若使用传统 NAT，则只允许从本地网络发出的单向连接。传统 NAT 对基本 NAT 和 NAPT（网络地址端口转换）方法进行了区分。

在基本 NAT 中，将始终为实现转换提供一个全局/外部地址池，并将每个内部地址转换为一个外部地址。

若使用 NAPT，则会在转换中包括传输标识符，例如端口号。为此，该方法仅需要一个外部地址即可实现转换。

有关 SCALANCE X300/X400 的 1:1 NAT

用于 SCALANCE X300/X400 的 NAT 的一个特殊变型为 1:1 NAT，也称为双向 NAT。该变型允许在两个方向上建立连接；也就是说，也可以从外部网络连接至本地网络。使用静态表来执行网络地址转换。可在该表中指定全局 IP 地址与本地 IP 地址之间的 1:1 转换。

NAT 组态

说明

NAT 功能会占用许多的计算容量。因此，如果要将交换机用作 NAT 设备，则应该尽可能禁用其它功能和协议（RSTP、HRP/MRP、PTP 等）。从而实现更高的 NAT 数据包吞吐量。

在菜单树中单击“NAT”文件夹转到 “网络地址转换”(Network Address Translation) 窗口。该窗口显示当前的 NAT 设置。

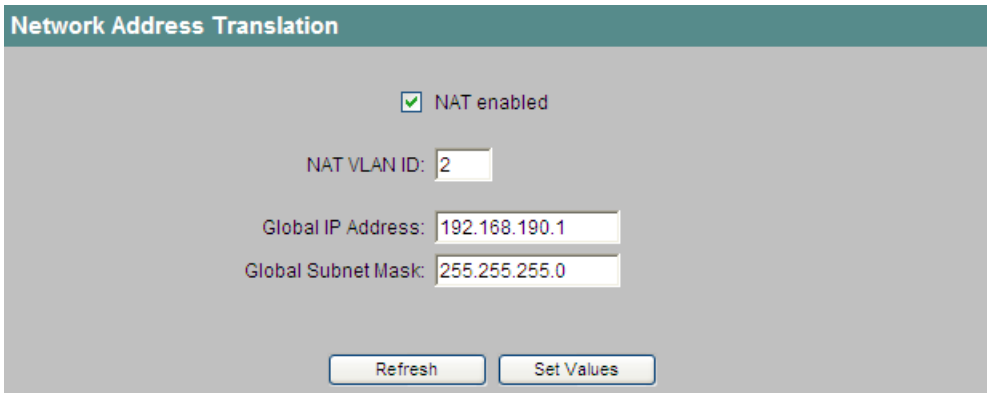


图 5-120　网络地址转换

启用 NAT (NAT enabled)

通过单击该复选框来启用或禁用 NAT 功能。

NAT VLAN ID：

在该输入框中，可为全局网络连接输入已组态虚拟 LAN 的 ID。

全局 IP 地址 (Global IP Address)：

在该输入框中，可为动态地址转换输入全局 IP 地址。

全局子网掩码 (Global Subnet Mask)：

可在该输入框中输入全局子网掩码。子网掩码必须是 255.255.255.0 形式的 C 类地址。

静态 NAT 表

在该菜单树中，“NAT”文件夹包含子部分“基本 NAT”(Basic NAT)。单击此项可转到静态地址表。

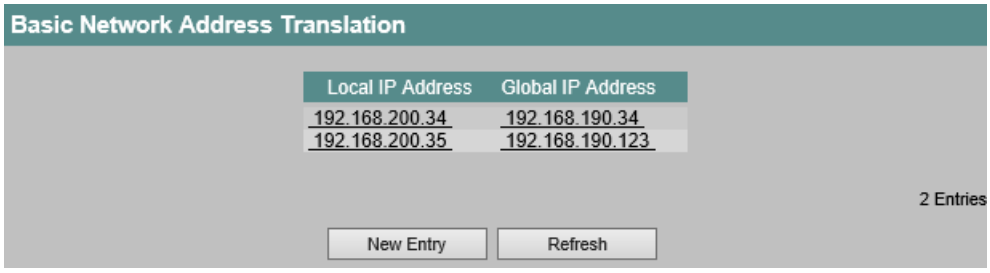


图 5-121　静态 NAT 表

创建新条目

1. 单击“新建条目”(New Entry) 按钮。
   将显示“基本网络地址转换条目”(Basic Network Address Translation Entry) 窗口。
2. 在“本地 IP”(Local IP) 输入框中，输入要转换的本地 IP 地址。

3. 在“全局 IP”(Global IP) 输入框中，输入相应的全局 IP 地址。
4. 单击“设置值”(Set Values) 按钮保存设置。

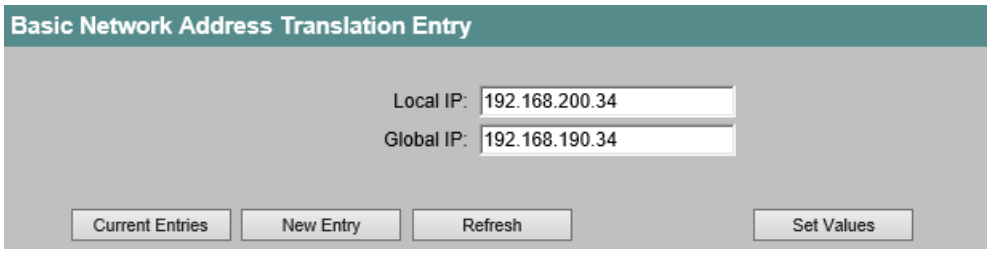


图 5-122　创建 NAT 条目

删除现有条目

1. 在“基本网络地址转换”(Basic Network Address Translation) 窗口中单击现有的 IP 地址。将显示“基本网络地址转换条目”(Basic Network Address Translation Entry) 窗口。
2. 单击“删除”(Delete) 按钮删除此条目。

命令行接口语法

NAT - 网络地址转换

表格 5-88　**CLI\SWITCH\NAT>**

命令	说明	注释
info	显示当前 NAT 设置。	
nat [<E|D]	启用/禁用 NAT 功能。	仅限管理员。
config <VID> <IP> <子网>	指定 VLAN ID、IP 地址和子网掩码等 NAT 设置。	仅限管理员。
BASIC	打开“基本 NAT”(Basic NAT) 菜单项。	仅限管理员。

表格 5-89　**CLI\SWITCH\NAT\BASIC>**

命令	说明	注释
info	显示当前 NAT 条目。	
add <本地 IP> <全局 IP>	创建新的 NAT 条目。	仅限管理员。
delete <本地 IP> <全局 IP>	删除现有 NAT 条目。	仅限管理员。

5.5.27 统计信息

计数和评估接收到的帧

工业以太网交换机内置统计信息计数器，通过此计数器按照以下条件对每个端口接收的帧数进行计数：

- 帧长度
- 帧类型
- 错误帧

该信息提供网络上的数据通信和所有问题的总览。

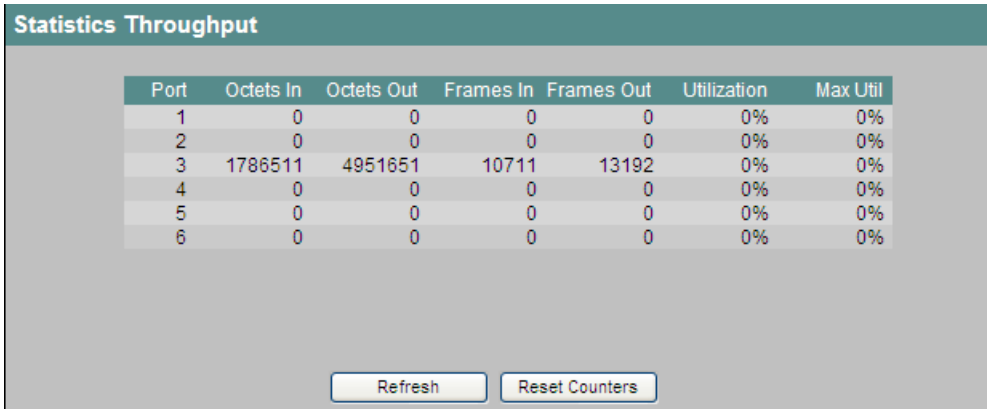


图 5-123 吞吐量统计

八位位组输入 (Octets In)

显示接收到的字节数。

八位位组输出 (Octets Out)

显示发送的字节数。

帧输入 (Frames In)

显示接收到的帧数。

帧输出 (Frames Out)

显示发送的帧数。

利用率 (Utilization)

以百分比 (%) 形式显示当前端口利用率。如果总线利用率低于 1%，则什么也不显示。根据不同的帧长度（取决于系统），由于帧之间停顿时间增加会使帧长度变短，最多可能产生 20% 的显示偏差。每隔 5 秒计算利用率值。

最大利用率 (Max. Utilization)

以百分比 (%) 形式显示端口利用率的峰值。

说明

使用 X300 时，根据进入帧计算利用率值。仅考虑正确的帧。

使用 X414 时，根据进入帧和离开帧计算利用率值。无论正确的还是错误的进入帧均加以考虑。仅考虑正确的离开帧。

命令行接口语法

表格 5-90　吞吐量统计 - CLI\SWITCH\STATS>

命令	说明	注释
info	显示有关已发送和已接收帧的统计信息。	仅限管理员。
size [端口]	显示有关已发送和已接收帧的长度信息。	仅限管理员。
type [端口]	显示有关已发送和已接收帧的类型信息。	仅限管理员。
error [端口]	显示有关已发送和已接收的错误帧信息。	仅限管理员。
clear	复位计数器。	仅限管理员。

5.5.27.1　数据包大小统计信息 (Packet Size Statistic)

按长度分类的接收到的帧

"数据包大小统计信息"(Packet Size Statistic) 页面显示各个端口收到的不同大小的帧数目。

如果单击 "复位计数器"(Reset Counters) 按钮，将复位所有端口的计数器。

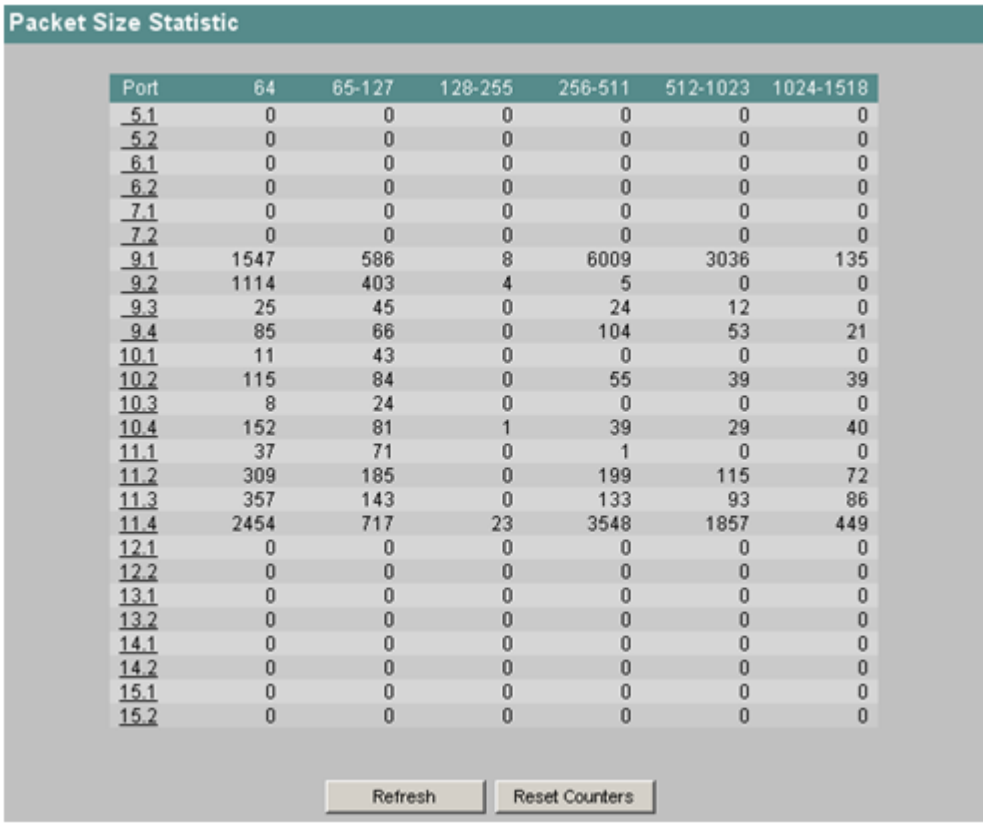


图 5-124　数据包大小统计信息 (Packet Size Statistic)

如果单击“端口”(Port) 列中的某个条目，将显示所选端口的“数据包大小统计信息图”(Packet Size Statistics Graphic)。 其中显示计数器值的可组态图形表示。

统计信息的图形表示

此页面以图形方式显示各个端口接收的帧数。 显示取决于帧长度。 以下每个范围在图形中都有一个单独的元素：

- 64 个字节
- 65 - 127 字节
- 128 - 255 字节
- 256 - 511 字节

- 512 - 1023 字节
- 1024 - 1518 字节

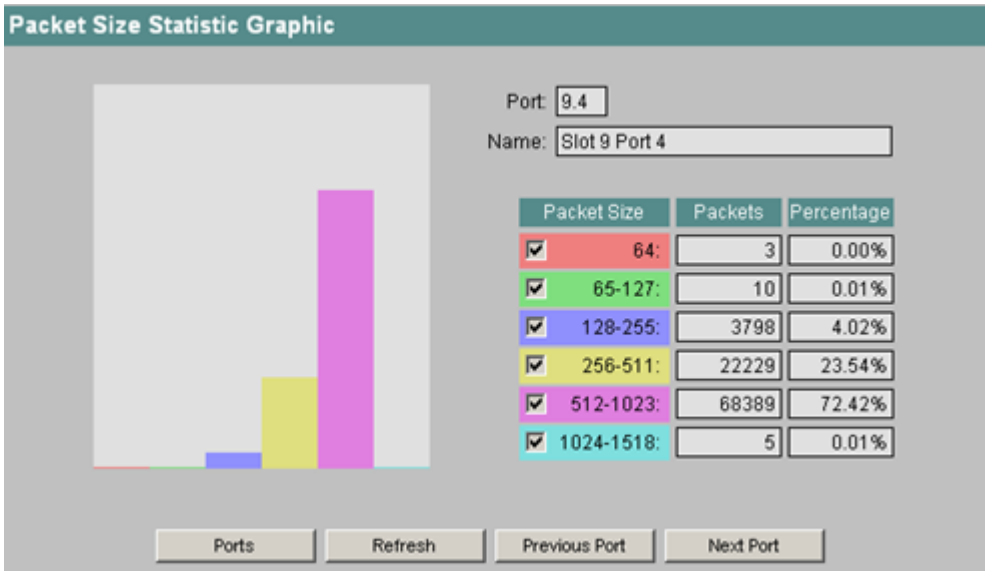


图 5-125　数据包大小统计信息图 (Packet Size Statistic Graphic)

通过“数据包大小”(Packet Size) 列中的复选框，可决定图形的内容。 只有选中某个范围对应的复选框，图形中的“数据包”(Packets) 列才会显示该范围的值。“百分比”(Percentage) 列显示某一长度范围内的数据包数占此端口数据包总数的百分比。 只有选中与范围对应的复选框，计算百分比时才会将范围包括在内。

单击“上一端口”(Previous Port) 和“下一端口”(Next Port) 按钮，可切换到上一端口或下一端口的显示。

命令行接口语法

表格 5-91　统计信息 - CLI\ SWITCH\STATS>

命令	说明	注释
size [端口]	显示按帧长度分类的接收帧数。 也可指定多个端口。 示例： • size 5.1, 6.1-7.2 显示在端口 5.1 以及端口 6.1 到 7.2 接收的帧的长度。	-

5.5.27.2　数据包类型统计信息 (Packet Type Statistic)

按类型分类的接收到的帧

“数据包类型统计信息”(Packet Type Statistic) 页面显示各个端口接收到的类型为“单播”、“组播”和“广播”的数据包数量。

如果单击“复位计数器”(Reset Counters) 按钮，将复位所有端口的计数器。

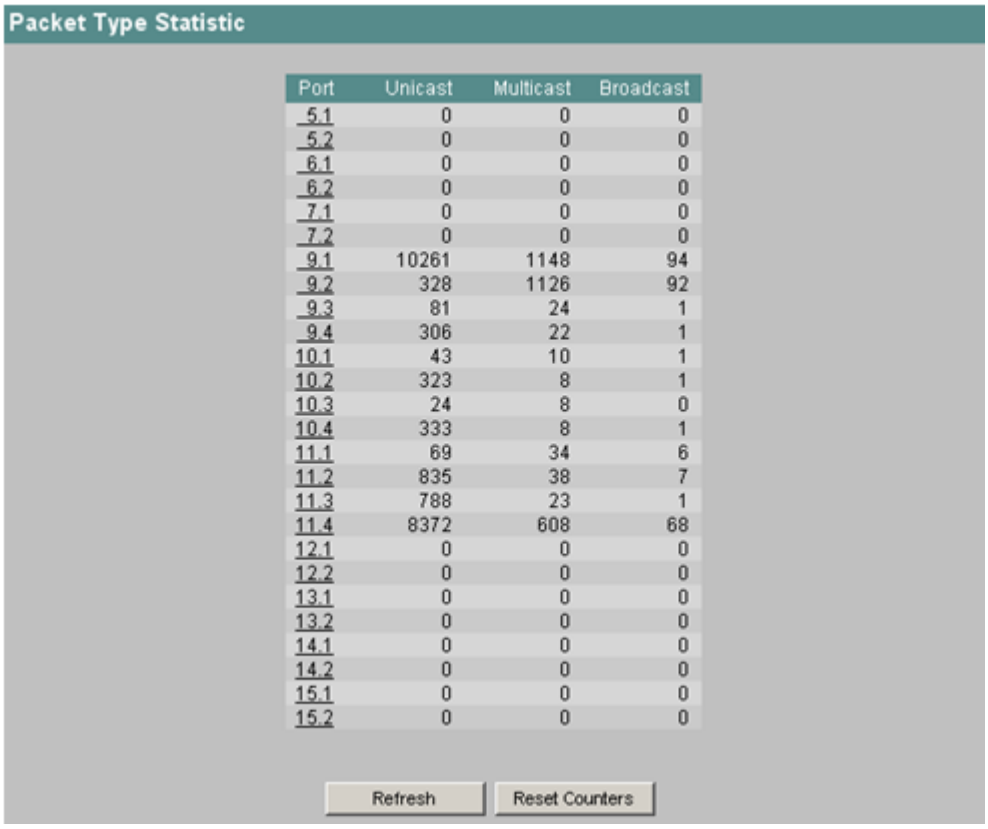


图 5-126 数据包类型统计信息 (Packet Type Statistic)

如果单击 “端口”(Port) 列中的某个条目，将显示所选端口的 “数据包类型统计信息图”(Packet Type Statistics Graphic)。 其中显示计数器值的可组态图形表示。

统计信息的图形表示

此页面以图形方式显示各个端口接收的帧数。 显示取决于帧类型。 以下每个范围在图形中都有一个单独的元素：

- 单播
- 组播
- 广播

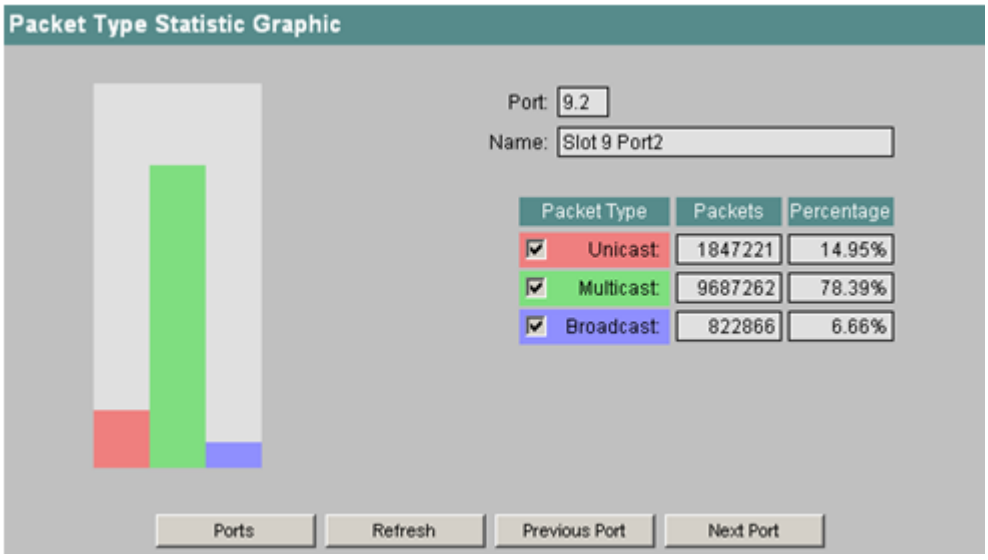


图 5-127　数据包类型统计信息图 (Packet Type Statistic Graphic)

通过 “数据包类型”(Packet Type) 列中的复选框，可决定图形的内容。 只有选中某个帧类型对应的复选框，图形中的 “数据包”(Packets) 列才会显示该类型的值。 “百分比”(Percentage) 列显示某个类型的数据包数占此端口数据包总数的百分比。 只有选中与帧类型对应的复选框，计算百分比时才会将该类型包括在内。

单击 “上一端口”(Previous Port) 和 “下一端口”(Next Port) 按钮，可切换到上一端口或下一端口的显示。

命令行接口语法

表格 5-92　统计信息 - CLI\SWITCH\STATS>

命令	说明	注释
type [端口]	显示按照帧类型分类的接收帧数。 也可指定多个端口。 示例： • type 5.1, 6.1-7.2 显示在端口 5.1 以及端口 6.1 到 7.2 接收的帧的类型。	-

5.5.27.3 错误统计信息 (Error Statistic)

接收帧中的错误

"数据包错误统计信息"(Packet Error Statistic) 页面显示每个端口接收到的错误帧数量。错误类型分为以下几种：

- CRC

  数据包的内容与 CRC 校验和不匹配。

- 过小 (Undersize)

  数据包的长度小 64 字节。

- 过大 (Oversize)

  数据包的长度大于 1518 字节或 1522 字节（帧带 VLAN 标记时）。

- 碎片 (Fragments)

  数据包的长度小于 64 字节并且 CRC 校验和错误。

- Jabbers

  数据包的长度大于 1518 字节或 1522 字节（帧带 VLAN 标记时），并且 CRC 校验和错误。

  说明

  SCALANCE X414-3E 将此类帧作为长于 1518 字节或 1522 字节的 jabber，并且具有正确的 CRC 校验和。

- 冲突 (Collisions)

  检测到冲突。

如果单击 "复位计数器"(Reset Counters) 按钮，将复位所有端口的计数器。

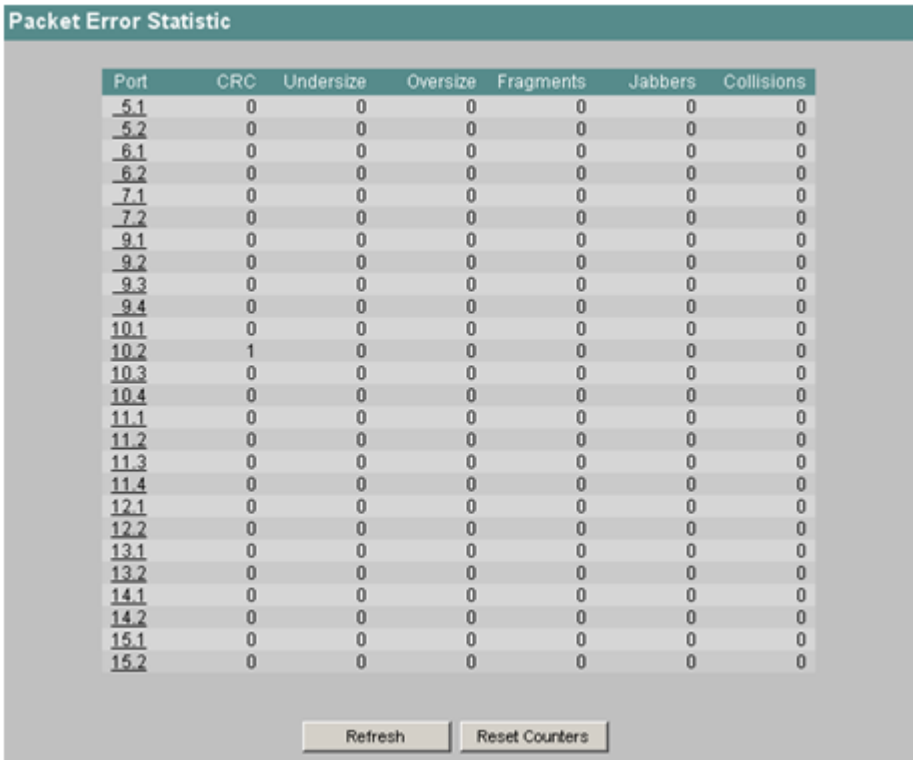


图 5-128　数据包错误统计信息 (Packet Error Statistic)

如果单击“端口”(Port) 列中的某个条目，将显示所选端口的“数据包错误统计信息图”(Packet Error Statistics Graphic)。其中显示计数器值的可组态图形表示。

统计信息的图形表示

此页面以图形方式显示错误帧数。显示取决于错误原因。以下每个错误原因在图形中都有一个单独的元素：

- CRC
- 过小 (Undersize)
- 过大 (Oversize)

- Jabbers
- 冲突 (Collisions)

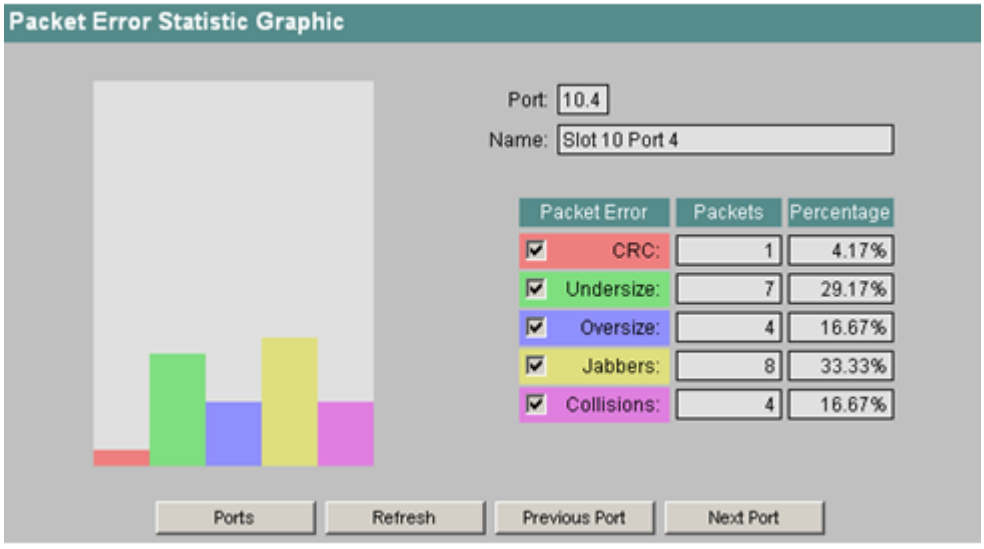


图 5-129　数据包错误统计信息图 (Packet Error Statistic Graphic)

通过“数据包错误”(Packet Error) 列中的复选框，可决定图形的内容。只有选中某个帧类型对应的复选框，图形中的“数据包”(Packets) 列才会显示该类型的值。“百分比”(Percentage) 列显示某个类型的错误数占此端口错误总数的百分比。只有选中与错误类型对应的复选框，计算百分比时才会将该类型包括在内。

单击“上一端口”(Previous Port) 和“下一端口”(Next Port) 按钮，可切换到上一端口或下一端口的显示。

命令行接口语法

表格 5-93　统计信息 - CLI\SWITCH\STATS>

命令	说明	注释
error [端口]	显示按照帧错误分类的接收帧数。 也可指定多个端口。 示例： • error 5.1, 6.1-7.2 显示在端口 5.1 以及端口 6.1 到 7.2 接收的错误帧数。	-

5.6 PoE 菜单项

以太网供电的设置

“PoE”版本的 SCALANCE 设备可通过以太网电缆为其它 PoE 兼容的设备供电。 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。

总览页面显示有关具有 PoE 功能的 SCALANCE 设备所提供功率的信息以及各个 PoE 端口的详细信息。

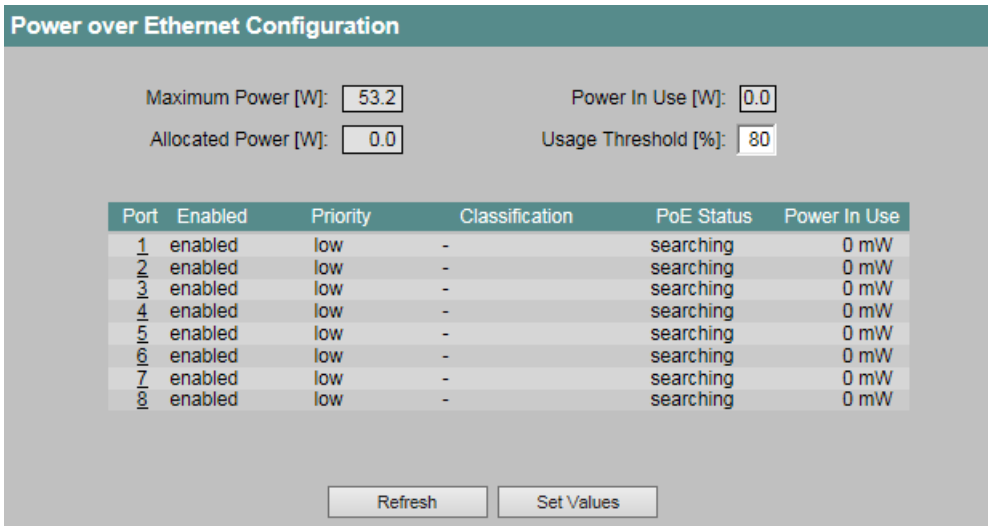


图 5-130　有关 SCALANCE PoE 组态的信息

下述对话框提供关于通过 PoE 供电的工业以太网交换机功率的信息。

- **最大功率 [W] (Maximum Power [W])**（只读）
  SCALANCE 为 PoE 设备供电所能提供的最大功率。
- **分配的功率 [W] (Allocated Power [W])**（只读）
  PoE 设备接收的功率总和。
- **使用功率 [W] (Power in Use [W])**（只读）
  终端设备正在使用的功率总和。
- **使用阈值 (Usage Threshold)** [%]
  只要所连接设备正在使用的功率超过此最大功率百分比，就会触发事件。

该表包含以下信息：

- **端口 (Port)**
  显示可组态的 PoE 端口。
- **启用 (Enabled)**
  显示启用还是禁用此端口的 PoE 供电功能。
- **优先级 (Priority)**
  显示为此端口考虑的供电优先级。
- **分类 (Classification)**
  分类指定设备的类别。通过该设置可识别设备的最大功率。

- **PoE 状态 (PoE Status)**
  显示端口的当前状态。可能的状态如下：
  - 禁用 (disabled)
    禁用此端口的 PoE 供电。
  - 输出功率 (delivering Power)
    激活此端口的 PoE 供电并连接一台设备。
  - 搜索 (searching)
    激活此端口的 PoE 供电，但未连接设备。
- **使用功率 (Power in Use)**
  显示在此端口中 SCALANCE 提供的功率。

进行端口设置

单击 “端口”(Port) 列中的某个端口号，将打开“PoE 端口组态”(PoE Port Configuration) 页面。

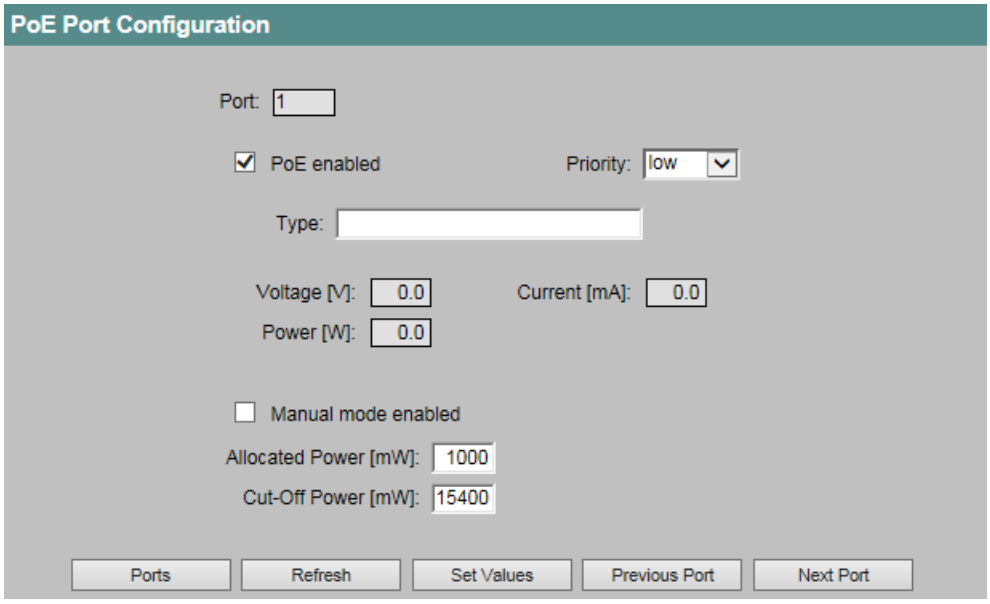


图 5-131　有关端口供电的详细信息

启用 PoE (PoE enabled)
如果选中该复选框，则启用此端口的 PoE 供电功能。

优先级 (Priority)
指定此端口的供电优先级。 可能的设置如下：

- 低 (low)
- 高 (high)
- 关键 (critical)

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 64 个字符。

电压 [V] (Voltage [V])（只读）
施加于此端口的电压。

功率 [W] (Power [W])（只读）
这是 SCALANCE 在此端口输出的功率。

电流 [mA] (Current [mA])（只读）
从此端口为设备供电的电流。

启用手动模式 (Manual mode enabled)
启用/禁用 PoE 的手动模式。
如果已启用手动模式，则可手动设置 PoE 端口的功率值。

分配的功率 [W] (Allocated Power [mW])
以 mW 为单位向端口分配具体功率（“分配的功率”）。
值范围：1000 mW - 20000 mW

截止功率 [mW] (Cut-Off Power [mW])
以 mW 为单位指定端口的截止功率。 如果超过此截止功率，则禁用端口。
值范围：1000 mW - 20000 mW

命令行接口语法

表格 5-94　CLI\POE>

命令	说明	注释
info [端口]	显示相关端口的 PoE 的信息。	-
pseusage [百分比]	为“使用阈值”(Usage Threshold) 参数设置值（百分比）。 只要所连接设备正在使用的功率超过此最大功率百分比，就会触发事件。 如果不带参数调用此命令，则显示当前值。	仅限管理员。
status [<E|D> [端口]]	启用/禁用指定端口的 PoE 供电。	仅限管理员。

命令	说明	注释
prio [<LOW|HIGH|CRITICAL> [端口]]	设置指定端口供电的优先级。 如果未指定任何端口，则设置的值将应用于所有端口。	仅限管理员。
type <端口> [字符串]	指定用于更详细描述所连接设备的字符串。 最大长度为 64 个字符。	仅限管理员。
manmode [<E|D>]	对端口启用/禁用“手动分配功率模式”(Manual Power Allocation Mode)。 如果启用了“手动分配功率模式”(Manual Power Allocation Mode)，则可手动设置 PoE 端口的功率值。	仅限管理员。
apower [<power> [端口]]	给端口分配具体功率值，单位 mW（“分配的功率”）。 取值范围： 1000 mW - 20000 mW	仅限管理员。
copower [<power> [端口]]	指定端口截止功率，单位 mW。 如果超过此截止功率，则禁用端口。 取值范围： 1000 mW - 20000 mW	仅限管理员。
assign [<port>]	将端口当前使用的功率作为“分配的功率”永久分配给端口。	仅限管理员。

5.7 “路由器”(Router) 菜单 (SCALANCE X414-3E)

说明

只有 SCALANCE X414-3E 有路由功能。

步骤简介

要将 SCALANCE X414-3E 设置为路由器，首先应至少创建两个子网，并将每个子网都分配给一个以前定义的 VLAN。 然后可输入静态路由，并且/或者启用路由器协议 RIP 或 OSPF。

有关组态 VLAN 的信息，请参见“当前 VLAN 组态 (Current VLAN Configuration) 菜单项”部分。

5.7.1 路由器组态 (Router Configuration)

简介

如果单击 *"路由器"(Router)* 文件夹图标，将显示“路由器组态"(Router Configration) 画面。在此画面中，可以将 SCALANCE X414-3E 设置为 IPv4 路由器。

要在网络中分发路由信息，可以使用 RIPv2 和 OSPFv2 协议（可在此处选择）。 可在相关子对话框中看到协议的详细设置。

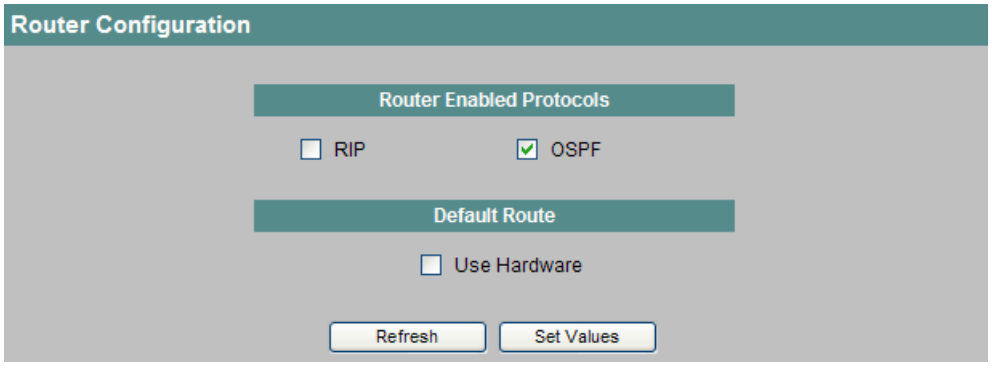


图 5-132 路由器组态 (Router Configuration)

SCALANCE X-400 的设置

RIP

启用“路由信息协议版本 2"选项 (RIP)。

说明

只要为 RIP 组态了至少一个接口，路由器就会使用 RIP 协议。

OSPF
启用“开放最短路径优先协议版本 2”选项 (OSPF)。

说明
只要为 OSPF 组态了至少一个接口，并且指定了路由器 ID，路由器就会使用 OSPF 协议。

使用硬件 (Use Hardware)
SCALANCE X-414 提供高速硬件路由的选项。 如果想要对默认地址启用硬件路由，则选中此复选框。

说明
如果在硬件中输入默认路由，则会将使用路由可到达的子网数量减少至 14。
对于动态学习的路由（RIP 或 OSPF），路由机制会在必要时自动从硬件中删除默认路由。

命令行接口语法

表格 5-95　路由器组态 - CLI\ROUTER>

命令	说明	注释
setrip <E|D>	启用/禁用 RIP	仅限管理员。
setospf <E|D>	启用/禁用 OSPF	仅限管理员。
defrthw <E|D>	对默认地址启用/禁用硬件路由。	仅限管理员。

5.7.2 路由器子网 (Router Subnets)

创建子网

要将 SCALANCE X414-3E 作为 IPv4 路由器运行，需要创建多个（至少两个）子网。

代理组态对应于第一个子网（请参见“代理 (Agent) 菜单”部分）。 只能在该处修改数据。

所有其它子网均可以在此处创建（“新建条目”(New Entry) 按钮）。 子网始终与之前在 VLAN 对话框中创建的 VLAN ID 有关。

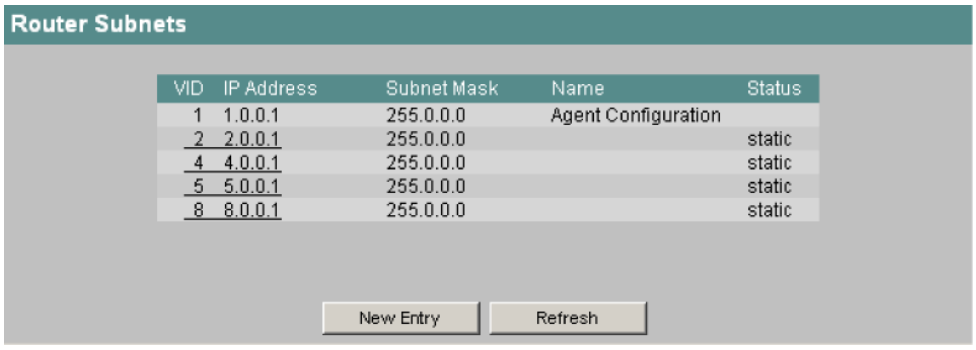


图 5-133　路由器子网 (Router Subnets)

VID
IP 子网的 VLAN ID。

IP 地址 (IP Address)
子网的 IP 地址（必须唯一）。

子网掩码 (Subnet Mask)
IP 子网的子网掩码。 以子网掩码的位表示形式左对齐输入的“反码”指定了 IP 地址的网络 ID。

名称 (Name)
可自由选择的子网名称。 必须与名称为“Agent Configuration”的代理组态相匹配的第一个子网的预定义名称。

状态 (State)
子网的状态。可能的状态如下：

- 静态 (Static)
- 无效 (invalid)
  状态为 “无效”(invalid) 的子网指示存在必须清除的组态错误。
- RIP
- OSPF

创建新 IP 子网

在“路由器子网”(Router Subnets) 对话框中单击“新建条目”(New Entry) 按钮，可以创建新子网。 在“路由器子网组态”(Router Subnet Configuration) 菜单中进行子网的设置。

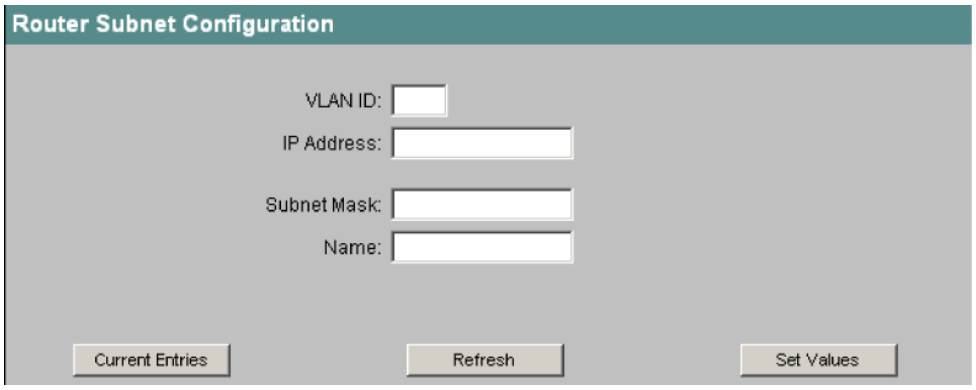


图 5-134　路由器子网组态 (Router Subnet Configuration)

VLAN ID
在此处输入 VLAN 的 ID（有关 VID 的信息，请参见“当前 VLAN 组态 (Current VLAN Configuration) 菜单项”部分），此 IP 子网的数据包将通过此 VID 传输（ID 的值范围： 1 到 4094）。

说明
不能再次使用代理 VLAN ID。 所有其它 ID 可以多次使用。

IP 地址 (IP Address)
输入 IP 子网的 IP 地址。 IP 地址不能多次使用。

说明
通过附加“/”字符和一个介于 1 到 30 之间的数字，也可以同时定义子网。

子网掩码 (Subnet Mask)
在此处输入正在创建的 IP 子网的子网掩码。 子网掩码必须由左对齐的反码位字段组成。

名称 (Name)
在此处输入子网的名称（这对功能无影响）。

命令行接口语法

表格 5-96　子网 - CLI\ROUTER\SUBNETS>

命令	说明	注释
info	显示当前子网。	仅限管理员。
add <VID> <IP> <子网> [名称]	添加新子网。"子网"参数用于标识子网掩码。	仅限管理员。
edit <VID> <IP> [子网] [名称]	修改子网。"子网"参数用于标识子网掩码。	仅限管理员。
delete <VID> <IP>	删除子网。	仅限管理员。

"info"CLI 命令将显示一个表（类似于 Web 界面中的表）。 但是，此处的 "状态"(Status) 列限制为两个字符 (St)。

可使用以下状态（另请参见 Web 界面）：

- RI (RIP)
- OS (OSPF)
- st (static)
- ?? (invalid)

5.7.3　当前路由 (Current Routes)

路由表

在此菜单中显示相应路由表。在此处也可以创建静态路由表条目。

路由表通常是多条规则的列表，按照这些规则转发接收到的数据包。如果某个数据包要等待路由，其目标地址将与路由表中的地址进行比较。随后，地址以及子网掩码最合适的条目（使用最长前缀匹配法）会描述将如何转发数据包。

路由表中状态为"本地"的条目指示已组态子网。

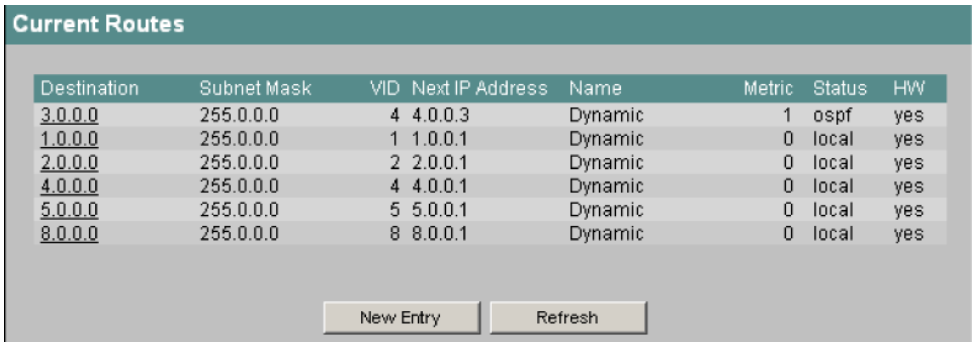


图 5-135 当前路由

目标 (Destination)
此路由的目标地址。

子网掩码 (Subnet Mask)
标识 “目标”(Destination) 列的有效位。必须由左对齐的反码组成。

VID
VID 用于标识 VLAN ID，使用此条规则时，将通过该 VLAN ID 的 IP 子网转发数据包。

下一个 IP 地址 (Next IP Address)
下一个 IP 地址用于标识下一个要访问的设备的 IP 地址。

名称 (Name)
名称不会影响路由过程。
对于静态路由，可输入名称。
对于动态路由，名称将设为 “动态”(Dynamic)。

度量 (Metric)
“度量”(Metric) 列显示路由器和目标之间的距离。

状态 (Status)
路由状态指示此路由通过 OSPF 或 RIP 协议作为静态路由还是本地路由生成。
静态路由通过 “新建条目”(New Entry) 按钮手动创建。
本地路由在创建子网时自动生成。

HW
HW（硬件）列标识是否将路由分配给硬件。可用选项如下：

- 是 (Yes)：
  可存储到硬件中
- 正在使用 (In use)：
  已存储到硬件中
- 否 (No)：
  无法存储在硬件中
  对于静态路由，可设置“是”(Yes) 或“否”(No)。只有实际使用路由时，路由才会存储在硬件中并显示为“正在使用”(In use)。

创建新静态路由

使用“当前路由”(Current Routes) 菜单中的“新建条目”(New Entry) 按钮可创建新路由。以这种方式创建的路由始终为静态路由。

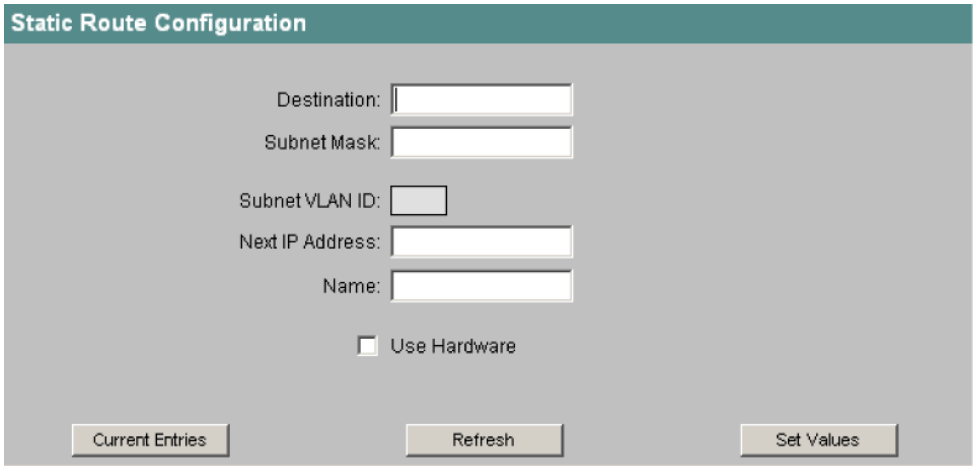


图 5-136　静态路由组态 (Static Route Configuration)

目标 (Destination)
在此输入路由表条目应参照的 IP 地址。

子网掩码 (Subnet Mask)
在此处输入路由条目的子网掩码。此处显示了地址中的哪些位可用于路由比较。

子网 VLAN ID (Subnet VLAN ID)
子网 VLAN ID 从下一个 IP 地址起自动计算，在新系统中为空。

下一个 IP 地址 (Next IP Address)
在此处输入此路由的数据包将被发送到的下一个路由器的地址。该路由器必须位于已连接的子网中。

名称 (Name)
在此处输入路由的名称（这对功能无影响）。

使用硬件 (Use Hardware)
如果要将路由写入硬件，请选中此复选框。如果启用此选项，则在第一次成功转发数据包后会将路由写入硬件，然后可以更快速地使用该路由。

说明
只有当硬件有足够的可用存储空间时，才能将路由写入硬件。

命令行接口语法

表格 5-97　当前路由 - CLI\ROUTER\ROUTES>

命令	说明	注释
info	显示当前路由。	仅限管理员
添加 <IP> 子网<下一 IP> [E|D] [名称]	添加新路由。 E|D 参数用于启用/禁用 “使用硬件”(Use Hardware)。	仅限管理员
编辑 <IP> [下一 IP] [E|D] [名称]	修改路由。 E|D 参数用于启用/禁用 “使用硬件”(Use Hardware)。	仅限管理员
delete <IP>	删除路由。	仅限管理员

“info”CLI 命令将显示一个表（类似于 Web 界面中的表）。但是，此处的 “度量”(Metric) 和 “状态”(Status) 列限制为两个字符（Me；St）。
可能的状态如下：

- OS (OSPF)
- RI (RIP)
- st (static)
- lo (local)
- ot (other)
- ??（无效）

“硬件”(Hardware, HW) 列中可使用以下状态（另请参见 Web 界面）：

- 是 (Yes)：X（大写 X）
- 正在使用 (In use)：*（星号）
- 否：-（减号）

5.7.4 RIPv2 组态 (RIPv2 Configuration)

简介

在“RIPv2 组态”(RIPv2 Configuration) 对话框中，可以设置 RIP 协议的常规参数，以及查看某些基本统计信息计数器。

说明

只有在 “路由器组态”(Router Configuration) 对话框中启用了 RIP 时，此处进行的设置才会生效。

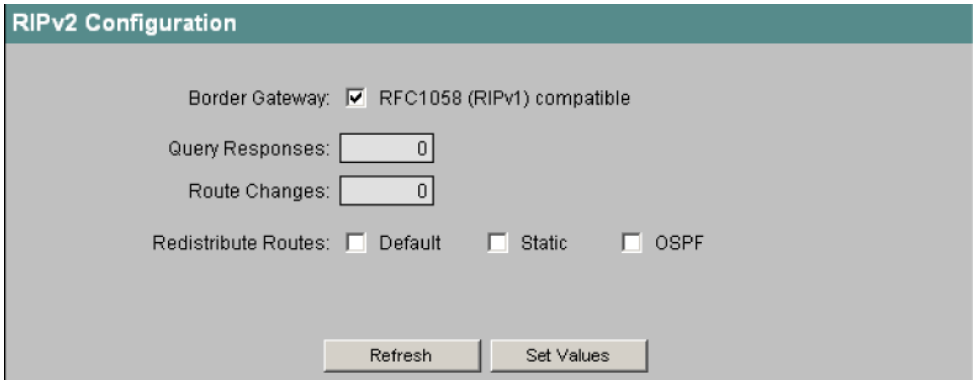


图 5-137 RIPv2 组态 (RIPv2 Configuration)

边界网关 (Border Gateway)
只有将路由器与原始 RIPv1 路由器一起运行时，才启用此复选框。 在这种情况下，子网路由按特定类别组合在一起，而不会传播所谓的超网。 这提供了与 RIPv1 路由器的最大可能兼容性。

查询响应 (Query Responses)
响应的特殊路由查询数。

路由变更 (Route Changes)
路由表的修改次数。

重新分配路由（默认/静态/OSPF）(Redistribute Routes) (Default/Static/OSPF)
在此处指定通过 RIP 转发哪些已知路径。 您需要从“默认”、“静态”和“OSPF”路由类型中作出选择。

说明

请仅对不同网络间的网关（边界网关）激活此复选框。 特别是启用“默认”(Default) 和“静态”(Static) 选项时，如果在网络中过多节点启用，可能出现问题（例如转发回路中的通信导致负载增加）。

命令行接口语法

表格 5-98 RIPv2 组态 - CLI\ROUTER\RIP>

命令	说明	注释
info	显示当前 RIP 组态。	-
rfc1058 <E|D>	设置 RFC1058 (RIPv1) 兼容性。	仅限管理员。
redistr <E|D> <E|D> <E|D>	启用/禁用“重新分配路由”(Redistribute Routes)。 • 参数 1 默认路由 • 参数 2 静态路由 • 参数 3 OSPF 路由	仅限管理员。

5.7.5 RIPv2 接口 (RIPv2 Interfaces)

简介

“RIPv2 接口”(RIPv2 Interfaces) 对话框显示使用 RIP 协议的所有 IP 子网的总览。

使用 “新建条目”(New Entry) 按钮可注册受 RIP 支持的新子网。

说明

在为 RIP 注册子网前，必须在 “路由器子网”(Router Subnets) 菜单中创建子网。

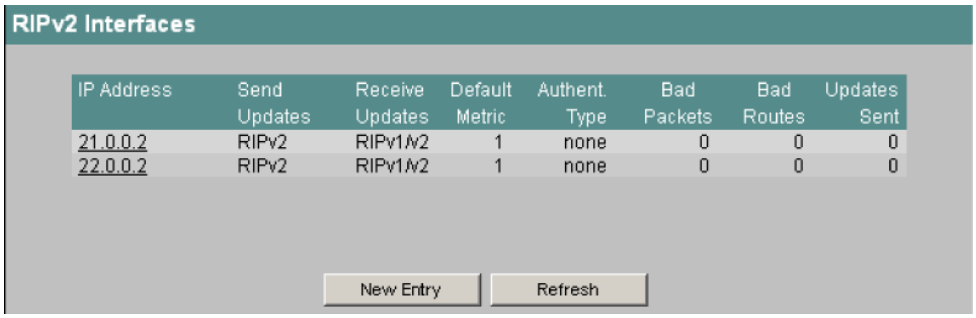


图 5-138 RIPv2 接口 (RIPv2 Interfaces)

IP 地址 (IP Address)

RIP 兼容子网的 IP 地址（仅此表的标识符）。 所有其它子网参数（如子网掩码）都可在 “路由器子网”(Router Subnets) 对话框中找到。

发送更新 (Send Updates)

此列显示如何发送更新。 可用的选项包括：

- 不发送 (no send)：
  不发送更新
- RIPv1：
  按照 RFC 1058 发送 RIPv1 更新
- RIPv1 兼容 (RIPv1-compat)：
  按照 RFC 1058 的规则以广播形式发送 RIPv2 更新
- RIPv2：
  以组播形式发送 RIPv2 更新
- RIPv1 要求和 RIPv2 要求 (RIPv1 demand and RIPv2 demand)：
  仅作为对显式查询的响应发送 RIP 数据包。
  只有当路由器需要通过 WAN 接口与另一个路由器通信时，才使用此选项。

接收更新 (Receive Updates)
此列显示接收到的 RIP 数据包的接受形式。 可用的选项包括：

- 不接收 (no receive)：
  不接受数据包。
- RIPv1：
  仅接受来自 RIPv1 路由器的数据包。
- RIPv2：
  仅接收和处理来自 RIPv2 路由器的数据包。
- RIPv1/v2：
  此接口接受 RIP 协议的所有变型。

默认度量 (Default Metric)
此列显示分配给此接口默认路由的度量。
值 0 指示不传播默认路由。
否则，值 1..15 有效。

验证 类型 (Authent. Type)
此列显示验证类型。 可能的类型是：

- 无验证
- 简单密码
- MD5 验证

不良数据包 (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计数器。

不良路由 (Bad Routes)
无法考虑到的有效 RIP 数据包的路由数。

已发送更新 (Updates Sent)
针对此接口的 "已触发更新"(Triggered Updates) 的数量。

创建新 RIPv2 接口

在“RIP 接口”(RIP Interfaces) 对话框中单击 “新建条目”(New Entry) 按钮，可以创建新接口。这将打开以下对话框。

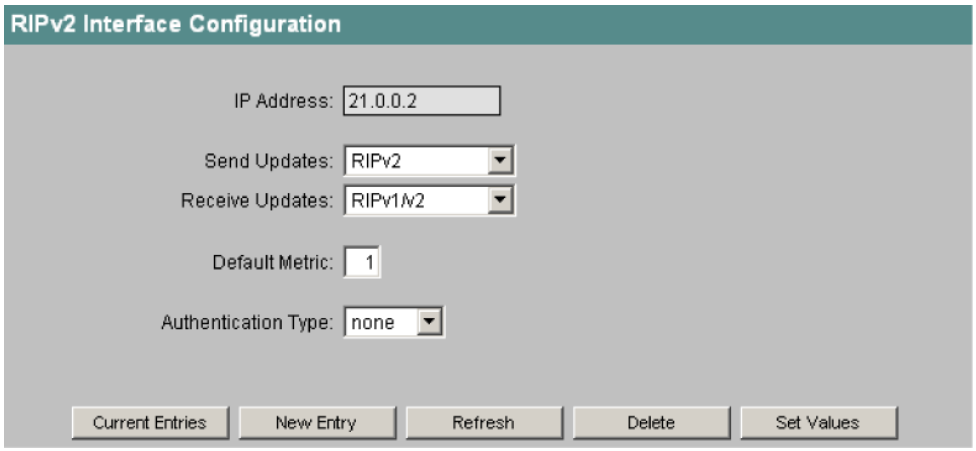


图 5-139 RIPv2 接口组态 (RIPv2 Interface Configuration)

IP 地址 (IP Address)
在此处输入将组态 RIP 的接口的 IP 地址。 此 IP 地址必须已组态为 IP 子网。

发送更新 (Send-Updates)
在此处选择如何发送 RIP 更新。 更新数据包包含本地系统的路由表。 可用的选项包括：

- 不发送 (no send)：
  不发送更新
- RIPv1：
  按照 RFC 1058 的规则发送 RIPv1 更新
- RIPv1 兼容 (RIPv1-compat)：
  按照 RFC 1058 的规则以广播形式发送 RIPv2 更新
- RIPv2：
  以组播形式发送 RIPv2 更新
- 只有 WAN 接口需要值“RIPv1 要求”(RIPv1 demand) 和“RIPv2 要求”(RIPv2 demand)。 在这种情况下，仅作为对显式查询的响应发送 RIP 数据包。

说明
如果网络中没有任何 RIPv1 设备，则应设置“RIPv2”。

接收更新 (Receive-Updates)
在此处选择接受收到的数据包所依据的规则。 可用的选项包括：

- 不接收 (no receive)：
  不接收更新
- RIPv1：
  接收 RIPv1 更新
- RIPv2：
  接收 RIPv2 更新
- RIPv1/v2：
  接收 RIPv1 和 RIPv2 更新

默认度量 (Default Metric)
在此处指定在此接口上传播默认路由的度量值。 RIP 使用跳跃式度量，其中距离被指定为 "使用的路由器数"(number of routers used)（值范围： 1-15（0 表示禁用默认路由））。
以下原则适用： 值越大，数据包到达目的地所需的距离越长。

验证类型 (Authentication Type)

在此处选择 RIP 数据包的验证方法。 可使用以下选项：

- 无 (none)： 不验证（默认）
- 简单 (simple)： 使用密码和确认进行验证
- MD5： 使用带密钥的 MD5 方法（密码、确认和密钥 ID）进行验证
- 这些方法只是用于确定数据包的真实性，并不加密数据。

密钥 ID (Key ID)

说明
仅当验证方法设为 MD5 时，才会显示 "密钥 ID"(Key ID) 文本框。

输入密钥 ID，以便将具有该 ID 的密码将用作密钥。 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。

密码/确认 (Password/Confirmation)

说明
仅当验证方法设置为 MD5 或 "简单"(simple) 时，才会显示 "密码/确认"(Password/Confirmation) 文本框。

如果使用密码进行验证，则需要可通过在此输入的 MD5 生成的密钥。

命令行接口语法

表格 5-99　RIPv2 接口 - CLI\ROUTER\RIP\RIP\IFACE>

命令	说明	注释
info	显示当前接口。	-
add <IP> [SendUpd] [RecvUpd] [Metric]	添加新接口。 SendUpd 的可能参数： • SV1 RIPv1 • SV1C RIPv1 兼容 • SV1D RIPv1 要求 • SV2 RIPv2 • SV2D RIPv2 要求 • SNO 不发送 RecvUpd 的可能参数： • RV1 RIPv1 • RV2 RIPv2 • RV1V2 RIPv1/v2 • RNO 不接收	仅限管理员。
edit <IP> [SendUpd] [RecvUpd] [Metric]	修改接口。 SendUpd 和 RecvUpd 的可能参数与 add 命令相同。	仅限管理员。

命令	说明	注释
auth <IP> <验证类型> [密码] [密钥 id]	修改接口的验证方法。 可能的类型： • 无 • 简单 (Simple) • MD5（只有此处要求“密钥 Id”）	仅限管理员。
delete <IP>	删除接口。	仅限管理员。

5.7.6 OSPFv2 组态

简介

在“OSPFv2 组态”(OSPFv2 Configuration) 对话框及其子对话框中，可以设置 OSPF 参数。

OSPFv2 将其管理 IPv4 网络（自治系统）分到不同区域中。 在这些区域内，将交换所有路由器的链路状态，从而每个路由器都有一张完整的网络地图。 在链路状态数据库 (LSDB) 中保留此地图。 每个路由器因此可根据 Dijkstra 算法自行确定区域内的全部路由。

区域间不存在统一的地图。 因此，路由交换仅限于可根据距离矢量算法确定的集体路由。

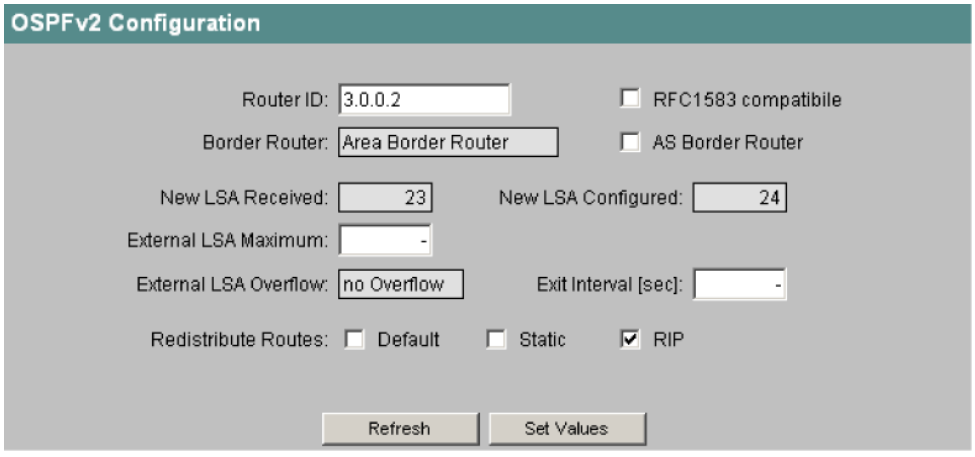


图 5-140 OSPFv2 组态

路由器 ID (Router ID)
可在此处设置 OSPF 接口的地址。 IP 地址必须唯一。

与 RFC 1583 兼容 (RFC 1583 compatible)
仅当您仍在使用与 RFC 2328 不兼容的 OSPFv2 路由器的情况下，才需要该设置。

边界路由器 (Border Router)
显示边界路由器状态。 如果本地系统至少是两个区域中的有效成员，则它就是区域边界路由器。

AS 边界路由器 (AS Border Router)
在路由器起 AS 边界路由器作用时启用该选项；即，传送到几个协议区（例如，如果用户运行一个附加的 RIP 网络）。

接收到的新 LSA (New LSA received)
接收到的链路状态广播数。 不会包括更新及其自身的 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 LAS (External LSA Maximum)
如果要限制外部 LSDB，可在此处输入外部 LAS 的最大数目。

外部 LAS 溢出 (External LSA Overflow)
表示是否超出外部 LAS 的最大数目。

退出间隔 Exit Interval (sec)
在此处输入以秒为单位的时间，经过该时间后，OSPF 路由器重新试图脱离溢出状态。 0 表示 OSPF 路由器仅在重启后尝试脱离溢出状态（通过路由器主菜单中的禁用和启用来触发）。

重新分配路由（默认/静态/RIP）(Redistribute Routes) (Default/Static/RIP)
在此处指定通过 OSPF 转发哪些已知路径。 您需要从“默认”、“静态”和"RIP"路由类型中作出选择。

说明
请仅对不同网络间的网关（边界网关）激活此复选框。 特别是启用“默认"(Default) 和“静态"(Static) 选项时，如果在网络中过多节点启用，可能出现问题（例如转发回路）。

命令行接口语法

表格 5-100 OSPFv2 组态 - CLI\ROUTER\OSPF>

命令	说明	注释
info	显示当前 OSPF 组态。	-
id <IP>	设置路由器 ID（IP 地址）。	仅限管理员。
rfc1583 <E|D>	设置 RFC1583 兼容性。	仅限管理员。
asbr <E|D>	启用/禁用 AS 边界路由器。	仅限管理员。
lsamax <number>	设置最大外部 LSA。	仅限管理员。

命令	说明	注释
exitint <sec>	设置外部退出间隔。	仅限管理员。
redistr <E|D> <E|D> <E|D>	启用/禁用 “重新分配路由”(Redistribute routes)。 • 参数 1 默认路由 • 参数 2 静态路由 • 参数 3 RIP 路由	仅限管理员。
ospfdbg [E|D] [debugtype]	启用/禁用 OSPF 调试功能。 输入“ospfdbg ?”以获取帮助。	仅限管理员。

5.7.7 OSPFv2 区域

概述

可将自治系统划分成一些更小的区域（请参见“OSPFv2 组态”菜单项部分）。

在该对话框中，可以监视路由器的 OSPF 区域。 除组态参数外，还可以看到统计值。

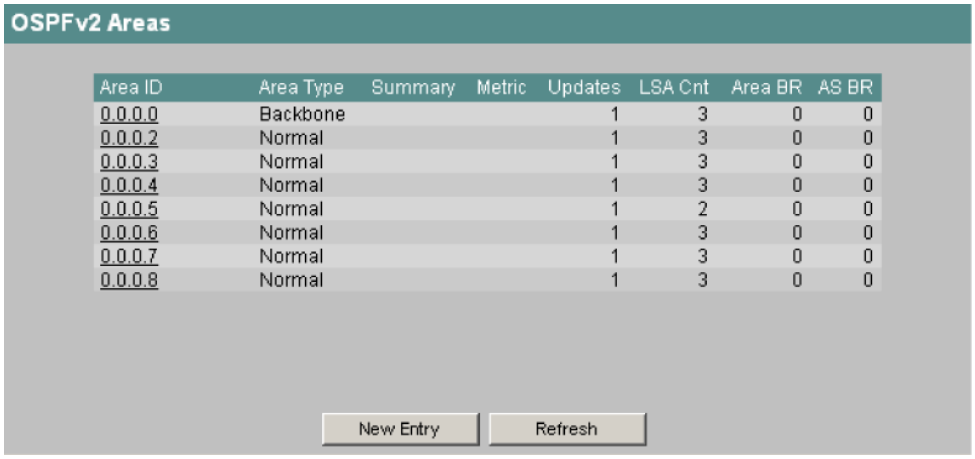


图 5-141 OSPFv2 区域

区域 ID (Area ID)

显示该区域的 ID。 区域 ID 由介于 0 和 255 之间的 4 个数字组成且必须有唯一性。

区域 0.0.0.0 被称为主干区域。
该区域的 LSDB 与区域中的全部路由器同步。

区域类型 (Area Type)
显示区域的类型。 可能的区域类型有：

- 标准 (Standard)
- 存根 (Stub)
- NSSA
- 骨干 (Backbone)： 此处选择了骨干区域。

总结 (Summary)
表示是否可生成该区域的总结 LAS。 该列仅对存根区域有意义。 可以是以下条目：

- 导入 (import)： 将总结 LAS 发送至该区域
- 忽略 (disregard)： 不将总结 LAS 发送至该区域

度量 (Metric)
显示在存根区域传播默认路由的度量值。 对于其它区域则不显示。

更新 (Updates)
路由表计算的数目

LSA Cnt
此区域 LSDB 中的 LSA 数

区域 BR (Area BR)
该区域中可到达的区域边界路由器 (ABR) 数量

ASBR
该区域中可到达的自治系统边界路由器 (ASBR) 数量。

创建新 OSPFv2 区域

使用“OSPFv2 区域”(OSPFv2 Areas) 对话框中的 “新建条目”(New Entry) 按钮可创建新区域。

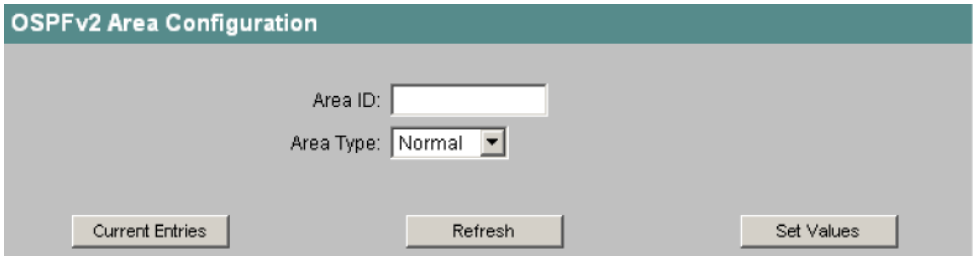


图 5-142 OSPFv2 区域组态

区域 ID (Area ID)
在此输入区域的 ID。

区域类型 (Area Type)
存在以下区域类型：

- 标准 (Standard)
- 存根 (Stub)
- NSSA

说明
对于骨干区域，所选区域类型必须是“普通”(Normal)，且区域 ID 为 0.0.0.0。

导入总结

说明
仅在设置“存根”(Stub) 区域类型时才会显示“导入总结”(Import Summary) 复选框。

启用该选项可在该区域生成和传播总结 LAS。 在这种情况下，不需要默认路由在整个网络中进行通信。

说明
如果该存根区域中仅有一个边界路由器，则不必激活该选项。

默认度量

说明
仅在设置了“存根”(Stub) 区域类型时才会显示“默认度量”(Default Metric) 复选框。

可在此输入将在该区域中传播的默认路由的度量值。

命令行接口语法

表格 5-101　OSPFv2 区域 - CLI\ROUTER\OSPF\AREAS>

命令	说明	注释
info	显示当前区域。	-
add <areaID> <type> [E|D] [metric]	添加新区域。 可能的类型： • 标准 (Standard) • 存根 (Stub) • NSSA [E|D] 和度量参数只能用于存根区域。 • E 启用导入总结 • D 禁用导入总结	仅限管理员。
edit <areaID> [type] [E|D] [metric]	修改区域。 可能的类型： • 标准 (Standard) • 存根 (Stub) • NSSA [E|D] 和度量参数只能用于存根区域。 • E 启用导入总结 • D 禁用导入总结	仅限管理员。
delete <areaID>	删除区域	仅限管理员。

示例

命令

```
add 0.0.0.3 Stub d 2
```

生成存根区域"0.0.0.3"，针对该区域不会生成任何汇总 LSA。 默认路由被分配度量"2"。

5.7.8 OSPFv2 区域范围

概述

可以在 “区域范围”(Area Ranges) 对话框中创建地址范围，该对话框允许在传播时将不同地址范围分组。 因此可减少区域中的总结 LSA 数。

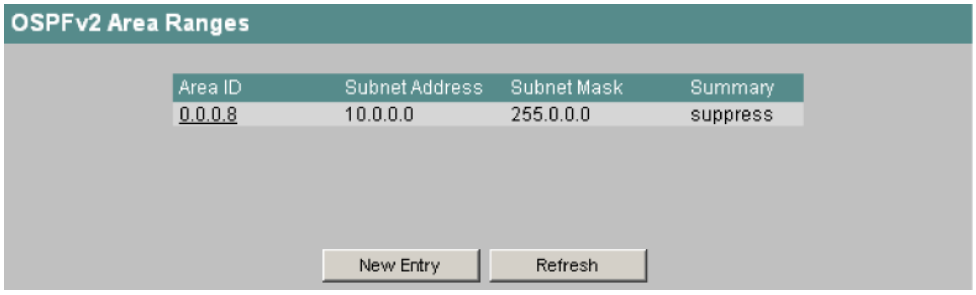


图 5-143 OSPFv2 区域范围

区域 ID (Area ID)
与地址范围相关的区域 ID。

子网地址 (Subnet Address)
要分组的网络区域地址。

子网掩码 (Subnet Mask)
分组网络区域的子网掩码。

总结 (Summary)
指出是要通告还是抑制分组地址范围。

创建新 OSPFv2 区域范围

使用"OSPFv2 区域范围"(OSPFv2 Areas Ranges) 对话框中的 "新建条目"(New Entry) 按钮，可为一个区域创建多达四个区域范围。

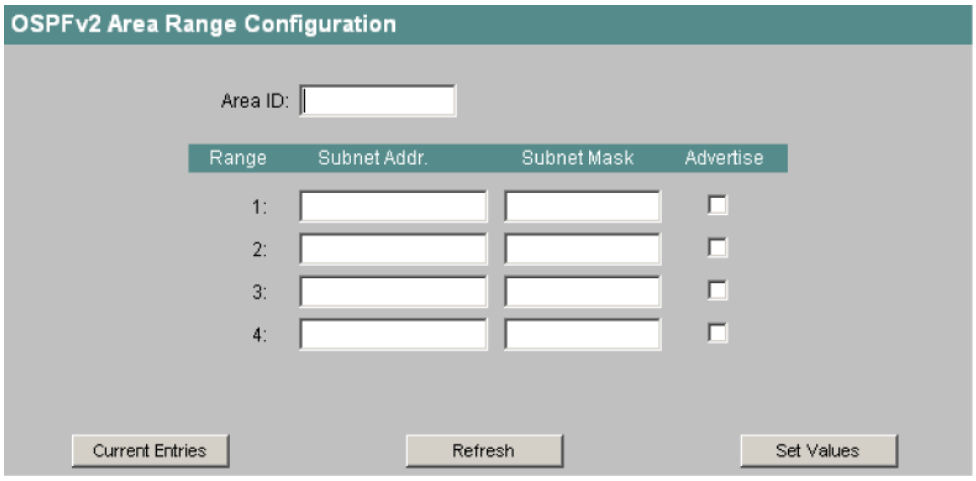


图 5-144　OSPFv2 区域范围组态

区域 ID (Area ID)
在此处输入要为其创建地址范围的区域的 ID。

子网地址 (Subnet Addr.)
在此处输入要分组的网络的地址。

子网掩码 (Subnet Mask)
在此处输入要分组的网络的子网掩码。

通告 (Advertise)
启用该选项以传播分组网络。

命令行接口语法

表格 5-102　OSPFv2 区域范围 - CLI\ROUTER\OSPF\AREAS\RANGES>

命令	说明	注释
info	显示当前区域范围。	-
add <AreaID> <SNAddr> <SNMask> [E|D]	添加新区域范围。 • E 启用通告摘要 • D 禁用通告总结	仅限管理员。

命令	说明	注释
edit <AreaID> <SNAddr> <SNMask> <E|D>	修改区域范围。	仅限管理员。
delete <AreaID> <SNAddr> <SNMask>	删除区域范围。	仅限管理员。

5.7.9 OSPFv2 接口

概述

在该对话框中，可以监视为 OSPF 组态的全部 IP 接口。 除组态参数外，还可以在双页面显示中监视某些统计值。

单击“>>”或“<<”可向后或向前翻页。

OSPFv2 接口： 第 1 页

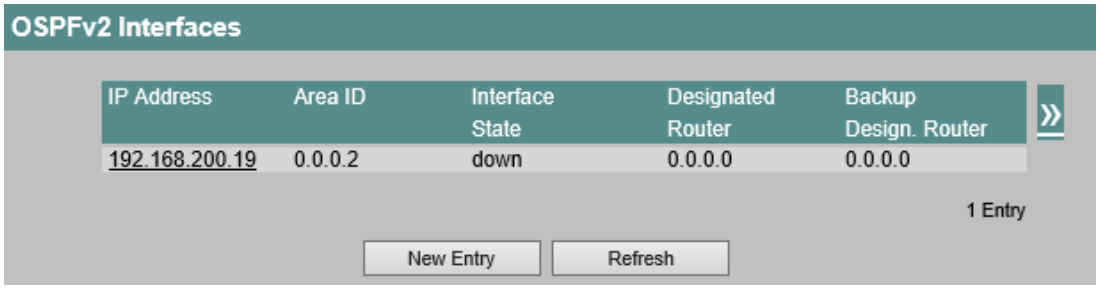


图 5-145 OSPFv2 接口第 1 页

IP 地址 (IP Address)
所组态 OSPF 接口的 IP 地址。

区域 ID (Area ID)
指定属于该接口的区域。

接口状态 (Interface State)
指示接口状态。 可能的状态是：

- 断开 (Down)： 接口上无任何连接
- 等待 (Waiting)： 启动并协商接口

- 指定路由器 (Designated Router)： 该路由器对该网络负主要责任，并且网络 LSA 将会生成
- 备用指定路由器 (Backup D. Router)： 该路由器为指定路由器的备份
- 其它 (Other)： 接口已启动，路由器既不是指定路由器，也不是备用指定路由器。

指定路由器 (Designated Router)
针对该接口指定的路由器的 IP 地址。

备用指定路由器 (Backup Designated Router)
针对该接口指定的备用路由器的 IP 地址。

OSPFv2 接口： 第 2 页

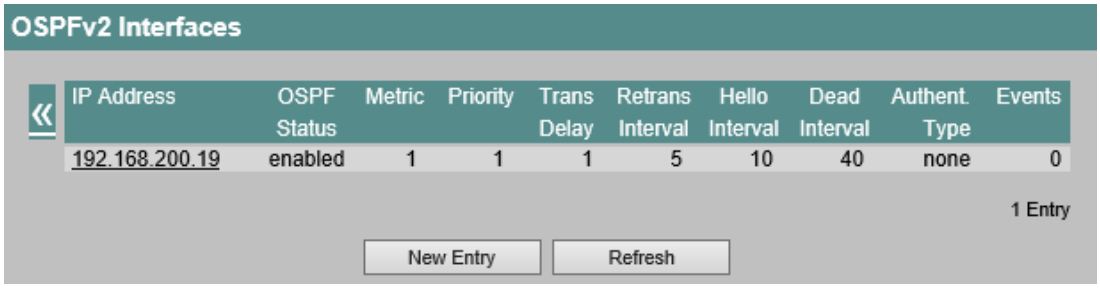


图 5-146 OSPFv2 接口第 2 页

IP 地址 (IP Address)
接口的 IP 地址。

OSPF 状态 (OSPF Status)
该接口的 OSPF 状态。 可能的状态如下：

- 启用 (Enabled)： 该接口可用于 OSPF。
- 禁用 (Disabled)： 该接口不可用于 OSPF。

度量 (Metric)
该接口上路由器的路径开销。

优先级 (Priority)
该接口上路由器的优先级。 优先级对如何选择网络中的指定路由器有影响。 数值越大，优先级越高。

传输延迟 (Trans Delay)
传输链路状态更新数据包所用的估计时间（以秒为单位）。 在 LAN 上，该参数通常为 1。

重传间隔 (Retrans Interval)
指定如果未在数据库同步期间确认数据包的接收，再次传输数据包要经过的时间间隔。

呼叫间隔 (Hello Interval)
指定发送呼叫数据包的时间间隔。

停顿间隔 (Dead Interval)
指定在未接收到其它呼叫数据包的情况下，路由器被分类为“不再存在”所经过的时间间隔。

验证 类型 (Authent. Type)
所选的接口验证方法。 可用的方法包括：

- 无 (none)： 无验证
- 简单 (simple)： 使用密码进行验证
- MD5： 使用加密的 MD5 方法进行验证

事件 (Events)
接口状态的变化次数。

创建新 OSPFv2 接口

使用“OSPFv2 接口”(OSPFv2 Areas) 对话框中的“新建条目”(New Entry) 按钮，可为 OSPF 组态新的 IP 接口。

说明

在将接口创建为 OSPF 接口之前，必须先将其创建为 IP 子网。

说明

选择参数时应格外小心。 仅当对 IP 子网的所有路由器组态了相同的参数时，才可能构成正确的邻居关系。 否则，会出现路由器无法识别对方的情况。

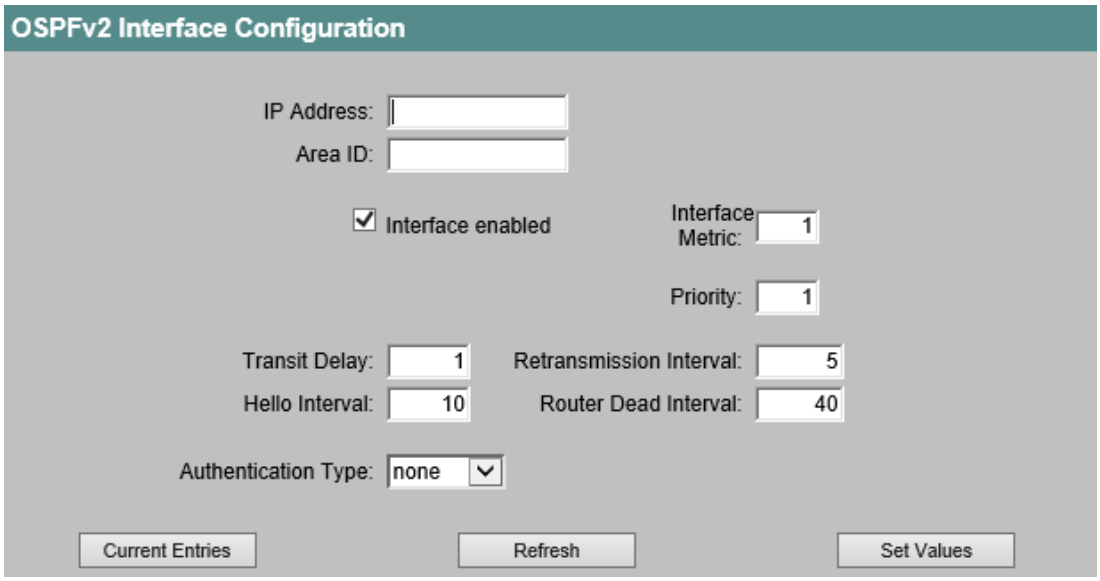


图 5-147 OSPFv2 接口组态

IP 地址 (IP Address)
要组态的接口的 IP 地址。

区域 ID (Area ID)
在此处输入该接口将属于的区域 ID。

接口已启用 (Interface enabled)
如果要将该接口包含在 OSPF 通信中，请选中该选项。

度量 (Metric)
该接口上路由器的路径开销。 默认值为 1。在此处输入的值越大，网络会越慢。

优先级 (Priority)
在此处输入路由器的优先级。 该值仅影响指定路由器的选择。 对同一 IP 子网内的不同路由器，该参数的选择可以不同。

中专延迟 (Transit Delay)
可在此处输入发送链路更新数据包时期望的延迟（以秒为单位）。 在局域网中，通常选择的值为 1（值范围： 1 到 3600）。

重传间隔 (Retransmission Interval)
在此处输入如果未收到确认的情况下，再次传递数据包应经过的时间间隔（以秒为单位）。在 LAN 中，通常选择值 5。

呼叫延迟 (Hello Delay)
在此处输入两个呼叫数据包之间的时间间隔（以秒为单位，值范围是： 1 到 65,535）。

路由器停顿间隔 (Router Dead Interval)
在此处输入在未接收到其它呼叫数据包的情况下，路由器显示为“故障”所经过的时间间隔。

验证类型 (Authentication Type)
在此处选择该接口的验证方法。 可以选择如下方法：

- 无 (none)： 无验证
- 简单 (simple)： 使用密码进行验证
- MD5： 使用加密的 MD5 方法进行验证

密钥 ID

说明
仅当验证方法设为 MD5 时，才会显示 “密钥 ID”(Key ID) 文本框。 只有这时才能使用多个密钥。

输入密钥 ID，以便将具有该 ID 的密码将用作密钥。 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。

密码/确认 (Password/Confirmation)
如果使用密码进行验证，则需要可通过在此输入的 MD5 生成的密钥。

命令行接口语法

表格 5-103 OSPFv2 接口 - CLI\ROUTER\OSPF\AREAS\IFACE>

命令	说明	注释
info	显示当前接口。	-
add <IP> <AreaID> [E|D] [priority]	添加新接口。 • E 启用接口 • D 禁用接口	仅限管理员。
edit <IP> [AreaID] [E|D] [priority]	修改接口。 • E 启用接口 • D 禁用接口	仅限管理员。

命令	说明	注释
timing <IP> [<setting=value>]	更改接口的定时设置。 可能的设置： • TD 传输 延迟 • RI 重传间隔 • HI 呼叫间隔 • DI 停顿间隔	仅限管理员。
auth <IP> <authtype> [password]	修改接口的验证方法 可能的类型： • 无 (None) • 简单 (Simple) • MD5	仅限管理员。
metric <IP> <metric>	更改接口的路径开销	仅限管理员。
delete <IP>	删除接口。	仅限管理员。

5.7.10 OSPFv2 虚拟链路

概述

出于与协议相关的原因，每个区域边界路由器（每个连接到两个或更多区域的路由器）必须可以访问骨干区域。如果此类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

只有当两个伙伴均通过 IP 网络直接连接且位于同一子网中时，才能创建虚拟链路。如果伙伴间存在路由器，则无法创建虚拟链路。

可以在该菜单中监视此虚拟链路。

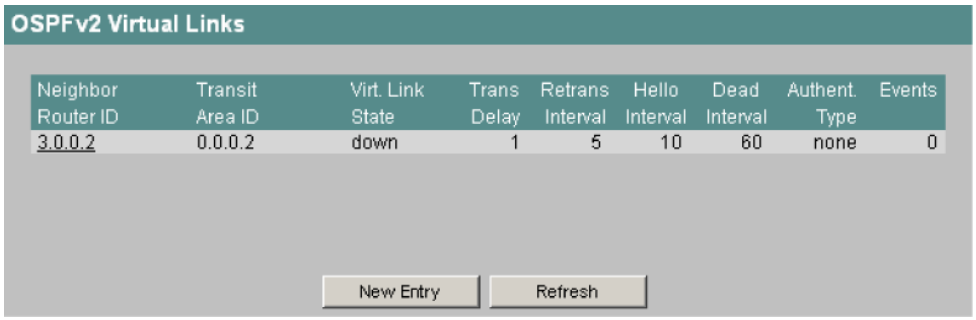


图 5-148 OSPFv2 虚拟链路

邻居路由器 ID (Neighbor Router ID)
所组态邻居的路由器 ID。

中转区域 ID (Transit Area ID)
区域 ID，路由器将通过该区域创建与邻居路由器的虚拟连接。

虚拟链路状态 (Virt. Link State)
虚拟链路的状态。可能的状态有：

- 断开 (Down)：无法使用该虚拟链路
- 点到点 (point-to-point)：可以使用虚拟链路

传输延迟 (Trans Delay)
通过虚拟链路传输链路状态更新数据包所需的估计时间（以秒为单位）。

重传间隔 (Retrans Interval)
如果未在数据库同步期间确认数据包的接收，再次传输数据包要经过的时间间隔（以秒为单位）。

呼叫间隔 (Hello Interval)
发送呼叫数据包的时间间隔（以秒为单位）。

停顿间隔 (Dead Interval)
在未接收到其它呼叫数据包的情况下，邻居路由器被分类为“故障”所经过的时间间隔（以秒为单位）。

验证类型 (Authent. Type)
虚拟链路的验证方法。可用的方法包括：

- 无 (none)：无验证
- 简单 (simple)：使用密码进行验证
- MD5：使用加密的 MD5 方法进行验证

事件 (Events)
接口状态的变化次数。

创建新的虚拟链路

使用"OSPFv2 虚拟链路"(OSPFv2 Virtual Links) 对话框中的 "新建条目"(New Entry) 按钮可创建新的虚拟链路。

说明

记住，在创建虚拟链路时，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。

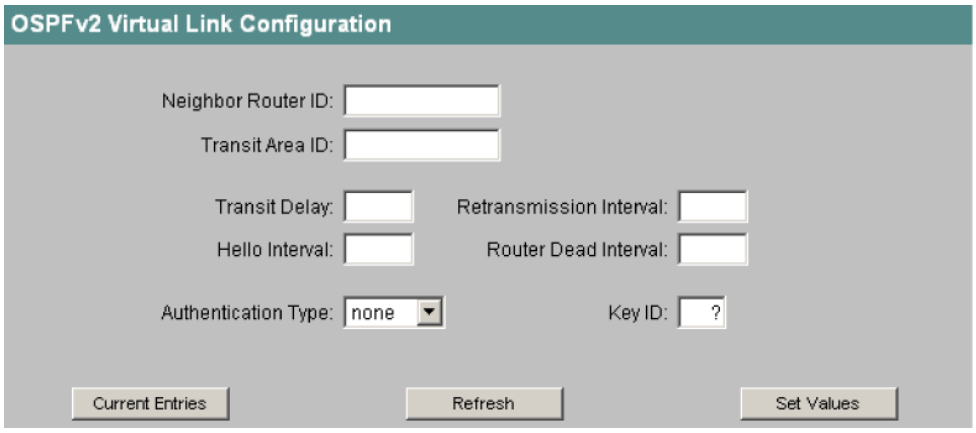


图 5-149 OSPFv2 虚拟链路组态

邻居路由器 ID (Neighbor Router ID)
在此处输入虚拟链路另一端的伙伴设备的路由器 ID。

中转区域 ID (Transit Area ID)
在此处输入区域 ID，两个伙伴设备通过该区域相连。

中专延迟 (Transit Delay)
可在此处输入发送链路更新数据包时期望的延迟（以秒为单位，值范围是：1 到 3600）。

重传间隔 (Retransmission Interval)
在此处输入如果未收到确认的情况下，再次传递数据包应经过的时间间隔（以秒为单位，值范围是：1 到 3600）。

呼叫延迟 (Hello Delay)
在此处输入两个呼叫数据包之间的时间间隔（以秒为单位，值范围是：1 到 65,535）。

路由器停顿间隔 (Router Dead Interval)
在此处输入在未接收到其它呼叫数据包的情况下，邻近路由器显示为 "故障" 所经过的时间间隔。

验证类型 (Authentication Type)
在此处选择虚拟链路的验证方法。可以选择如下方法

- 无 (none)：无验证
- 简单 (simple)：使用密码进行验证
- MD5：使用加密的 MD5 方法进行验证

密钥 ID

说明
仅当验证方法设为 MD5 时，才会显示“密钥 ID”(Key ID) 文本框。只有这时才能使用多个密钥。

输入密钥 ID，以便将具有该 ID 的密码将用作密钥。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。

密码/确认 (Password/Confirmation)
如果使用密码进行验证，则需要可通过在此输入的 MD5 生成的密钥。

命令行接口语法

表格 5-104 OSPFv2 虚拟链路 - CLI\ROUTER\OSPF\AREAS\VLINKS>

命令	说明	注释
info	显示当前虚拟链路。	-
add<RtrID> <AreaID> [<setting=value>]	添加新的虚拟链路。 可能的设置： • TD 传输延迟 • RI 重传间隔 • HI 呼叫间隔 • DI 停顿间隔	-

命令	说明	注释
edit <RtrID> <AreaID> [<setting=value>]	修改虚拟链路。 可能的设置： • TD 传输延迟 • RI 重传间隔 • HI 呼叫间隔 • DI 停顿间隔	-
auth <RtrID> <AreaID> <authtype> [password]	更改虚拟链路的验证方法。 可能的类型： • 无 (None) • 简单 (Simple) • MD5	-
Delete <RtrID> <AreaID>	删除虚拟链路。	-

示例

命令

```
add 1.1.1.51 0.0.0.2
```

通过中转区域“0.0.0.2”创建与 ID 为“1.1.1.51”的路由器的虚拟链路。其余参数设置为默认值。

5.7.11 OSPFv2 邻居

概述

可以在此对话框中监视 OSPF 邻居。 包括在相应网络中动态检测到的邻居和组态的虚拟邻居。

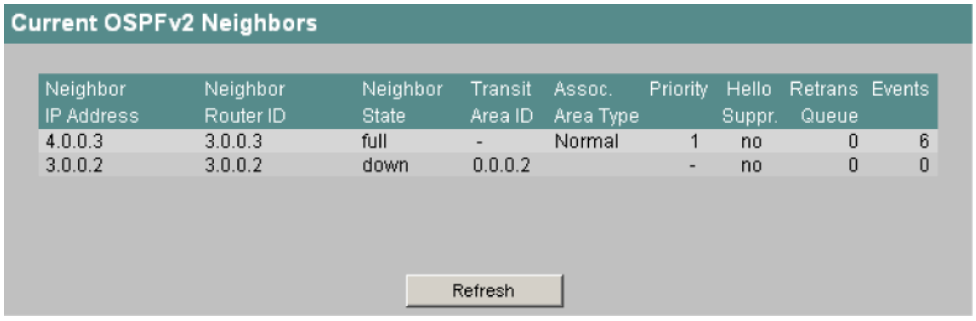


图 5-150 当前 OSPFv2 邻居

邻居 IP 地址 (Neighbor IP Address)
该网络中邻居的 IP 地址。

邻居路由器 ID (Neighbor Router ID)
邻居的路由器 ID。 这两个地址可以相同。

邻居状态 (Neighbor State)
邻居的状态。 状态可采用以下值：

- 断开 (Down)： 无法访问邻居。
- 尝试并初始化 (attempt and init)： 初始化期间的短时活动状态
- 双向 (two-way)： 双向接收呼叫数据包
- 开始交换、交换和加载 (exchange start, exchange and loading)： 交换链路状态数据库期间的状态
- 完整 (full)： 同步数据库时的状态。

说明

如果伙伴之一是指定路由器或备用指定路由器，则 “完整”(full) 状态是具有稳定邻居时的正常状态。 否则， “双向”(two-way) 状态是正常稳定状态。

中转区域 ID (Transit Area ID)
邻居是虚拟设备时，邻居的中转区域 ID。

相关区域类型 (Assoc. Area Type)
用于维持邻居关系的区域的状态。 可能的区域类型有：

- 标准 (Standard)
- 存根 (Stub)
- NSSA

优先级 (Priority)
邻居的路由器优先级。 仅在选择网络中的指定路由器时有意义。 该信息与虚拟邻居无关。

呼叫抑制 (Hello Suppr.)
显示发送给邻居的受抑制呼叫数据包。 该字段通常显示"无"(no)。

重传队列 (Retrans Queue)
包含仍要传输的数据包的队列长度。

事件 (Events)
状态变化次数。

说明

如果伙伴之一是指定路由器或备用指定路由器，则"完整"(full) 状态是具有稳定邻居时的正常状态。 否则，"双向"(two-way) 状态是正常稳定状态。

命令行接口语法

表格 5-105 OSPFv2 邻居 - CLI\ROUTER\OSPF>

命令	说明	注释
neighbrs	显示当前邻居。	-

5.7.12 OSPFv2 状态数据库

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 LAS 中最重要的数据显示在该对话框中。

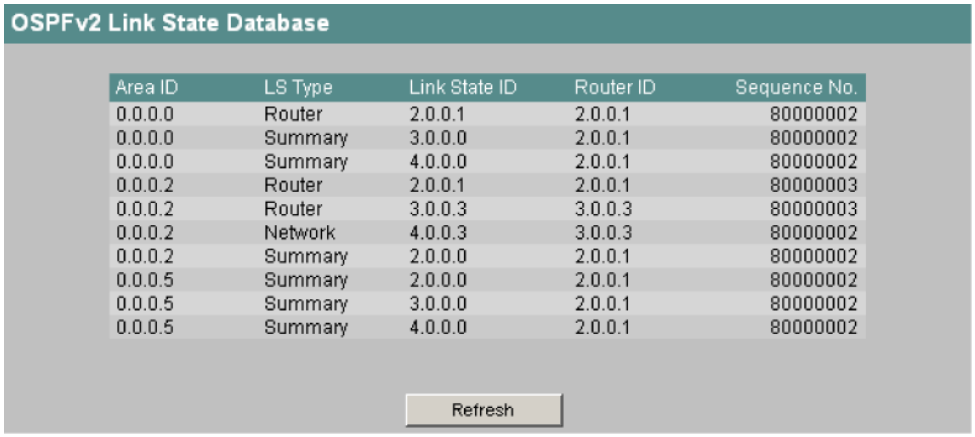


图 5-151 OSPFv2 链路状态数据库

区域 ID (Area ID)
该链路状态公告 (LSA) 所属的区域 ID。

LS 类型 (LS Type)
LSA 的类型。 可能的类型是：

- 路由器
- 网络
- 总结
- ASBR（Autonomous System Border Router，自治系统边界路由器）。

链路状态 ID (Link State ID)
LSA 的唯一 ID。

路由器 ID (Router ID)
生成该 LSA 的路由器。

顺序号 (Sequence No.)
LSA 的顺序号。 每次更新 LSA 后，该顺序号就会加一。

命令行接口语法

表格 5-106　OSPFv2 状态数据库 - CLI\ROUTER\OSPF>

命令	说明	注释
lnkstate	显示当前链路状态表。	-

说明

有关 LSA 的详细信息，请参见“通过 SNMP 进行组态和诊断”部分。

5.7.13　VRRP

简介

在“VRRP”菜单的子菜单中，可以设置 VRRP 参数。

VRRP 将冗余功能引入 IPv4 网络。 在实际路由器发生故障时，各种 IP 路由器可执行该路由器的路由功能。 要达到此目的，需将 IP 子网中的多台路由器进行分组，以形成一台虚拟路由器。为该虚拟路由器分配一个 IPv4 地址列表，相应的主机就可通过此列表来执行路由功能。

5.7.14　VRRP 虚拟路由器

简介

在该对话框中，可以监视系统的虚拟路由器。

可以用“新建条目”(New Entry) 按钮创建新的虚拟路由器。
最多可组态 32 台虚拟路由器。

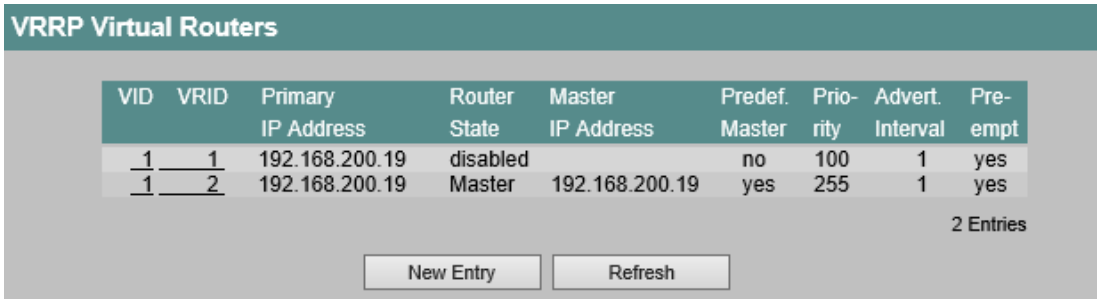


图 5-152　VRRP 虚拟路由器

VID
子网的 VLAN ID。 为此设置的 IP 地址以及全部子网参数均可在“路由器子网” (Router Subnets) 菜单中找到。

VRID
在该列显示虚拟路由器的 ID。 该分配的 ID 必须对此 VLAN 是唯一的。 有效值为 1 到 255。

主 IP 地址 (Primary IP Address)
在该列显示该 VLAN 的主 IP 地址。 条目 0.0.0.0 表示使用的是该 VLAN 的最小地址。 不然，在“路由器子网” (Router 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)
在该列显示当前的虚拟路由器状态。 可能的值有：

- 主设备 (Master)： 该路由器为全部分配的 IP 地址处理路由功能。
- 备用 (Backup)： 当前，另一台处理路由功能的路由器处于“主设备”(Master) 状态。 所显示的路由器承担冗余功能，并准备好在主设备发生故障时接管主设备的功能。
- 禁用 (Disabled)： 该路由器已被管理员禁用。 它不再处理路由器冗余。
- 初始化 (Initialize)： 已开启虚拟路由器。 它将很快切换为“主设备”或“备用”状态。
- 无效 (Invalid)： 该虚拟路由器的组态无效。 请检查组态。

主设备 IP 地址 (Master IP address)
在该列显示当前处理路由功能的路由器的 IP 地址。

预定义主设备 (Predef. Master)
该列指示是否有至少一个冗余路由器地址属于 IE Switch X-400。本例中，优先级被预定义为 255，
IE Switch X-400 在开启后会立即切换到“主设备”(Master) 状态。

优先级 (Priority)
在该列显示虚拟路由器的优先级。 有效值是 1 到 255。255 用于冗余路由器地址的所有者。 可以在冗余路由器之间自由分配其它优先级。 优先级越高，；路由器越早变为“主设备”。

通告 间隔 (Advert. Interval)
该列显示主路由器发送其广播数据包的时间间隔。

抢占 (Preempt)
该列指示优先级较高的路由器是否会中断其它优先级较低的路由器。

创建或更改虚拟路由器

使用"OSPFv2 虚拟路由器"(OSPFv2 Virtual Routers) 对话框中的 "新建条目"(New Entry) 按钮可创建新的虚拟路由器。

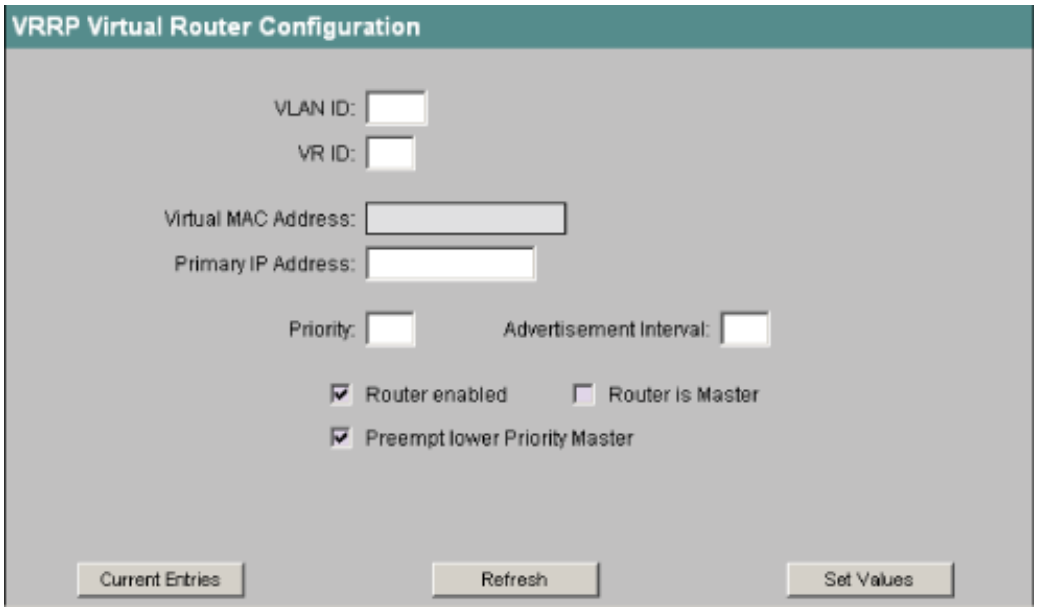


图 5-153 VRRP 虚拟路由器组态

VLAN ID
在此处输入将激活其中虚拟路由器的 VLAN。 有效值为至少拥有一个组态的 IP 子网的全部 VLAN 的 ID。

VR ID
在此处输入虚拟路由器的 ID。 该 ID 在连接的 LAN 中必须具有唯一性。

虚拟 MAC 地址 (Virtual MAC address)
虚拟 MAC 地址将通过虚拟路由器的 IP 自动生成，并具有固定的前缀。

主 IP 地址 (Primary IP Address)
在此处输入将在该虚拟路由器变为 "主设备"(Master) 状态时立即被用作 IP 源地址的地址。

说明

如果仅为该 VLAN 组态了一个 IP 子网，则不需要输入任何地址 (0.0.0.0)。 另一方面，如果为该 VLAN 组态了多个 IP 子网，并要将某个特殊地址用作 VRRP 数据包中的源地址，则需要在此处输入源地址。 否则，将使用数值最小的 IP 地址。

优先级 (Priority)
在此处输入虚拟路由器的优先级。有效值是 1 到 255。优先级 255 用于路由器地址的所有者。可以在冗余路由器之间自由分配其它优先级。 优先级越高，；路由器越早变为 "主设备"。

通告间隔 (Advertisement Interval)
在此处输入以秒为单位的时间间隔，经过该时间间隔后，处于“主设备”状态的路由器将再次发送广播数据包。

路由器已启用 (Router enabled)
在此处决定路由器是否参与 VRRP 协议。

路由器是主设备 (Router is Master)
在此处决定路由器是否应在启动时处于“主设备”状态。 在这种情况下，会立即将主要 IP 地址添加到路由器地址中。

取代优先级较低的主设备 (Preempt lower Priority Master)
在此处决定该路由器是否可以中断其它优先级较低的路由器。

命令行接口语法

VRRP - CLI\VRRP\ROUTERS>

命令	说明	注释
info	显示当前虚拟路由器。	-
add <VID> <VRID>	添加新的虚拟路由器。	仅限管理员。
status <VID> <VRID> <E|D>	启用/禁用虚拟路由器	仅限管理员。
master <VID> <VRID> <E|D>	指示该虚拟路由器是否为主路由器。	仅限管理员。
preempt <VID> <VRID> <E|D>	指定优先级较高的路由器是否可以中断优先级较低的路由器。	仅限管理员。
primip <VID> <VRID> <IP>	更改虚拟路由器的主 IP 地址。	仅限管理员。
priority <VID> <VRID> <0..255>	更改虚拟路由器的优先级。	仅限管理员。
advint <VID> <VRID> <0..255>	更改虚拟路由器发送广播数据包的时间间隔。	仅限管理员。
delete <VID> <VRID>	删除虚拟路由器。	仅限管理员。

5.7.15 VRRP 关联 IP 地址

简介

在该菜单项中，可以查看虚拟路由器的冗余 IP 地址。

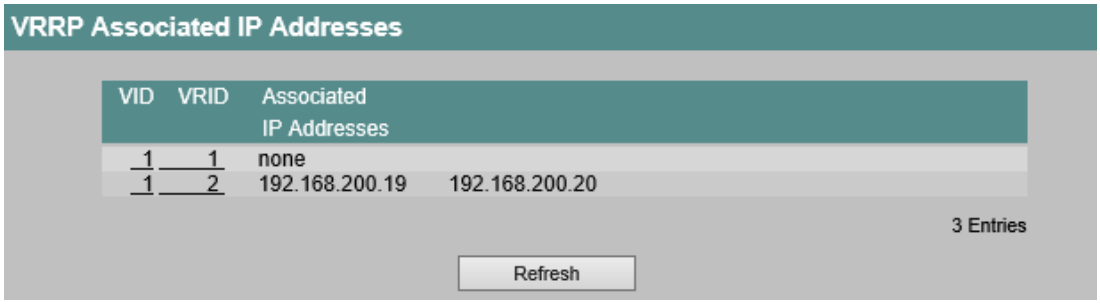


图 5-154 VRRP 关联 IP 地址

VID
子网的 VLAN ID。 为此设置的 IP 地址以及全部子网参数均可在 "路由器子网" (Router Subnets) 菜单中找到。

VRID
在该列显示虚拟路由器的 ID。 该分配的 ID 必须对此 VLAN 是唯一的。 有效值为 1 到 255。

关联 IP 地址 (Associated IP Address)
该列显示该虚拟路由器监控的路由器 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。

创建或更改受监视的 IP 地址

通过前两列中的链接，可添加、更改或删除要监视的 IP 地址。

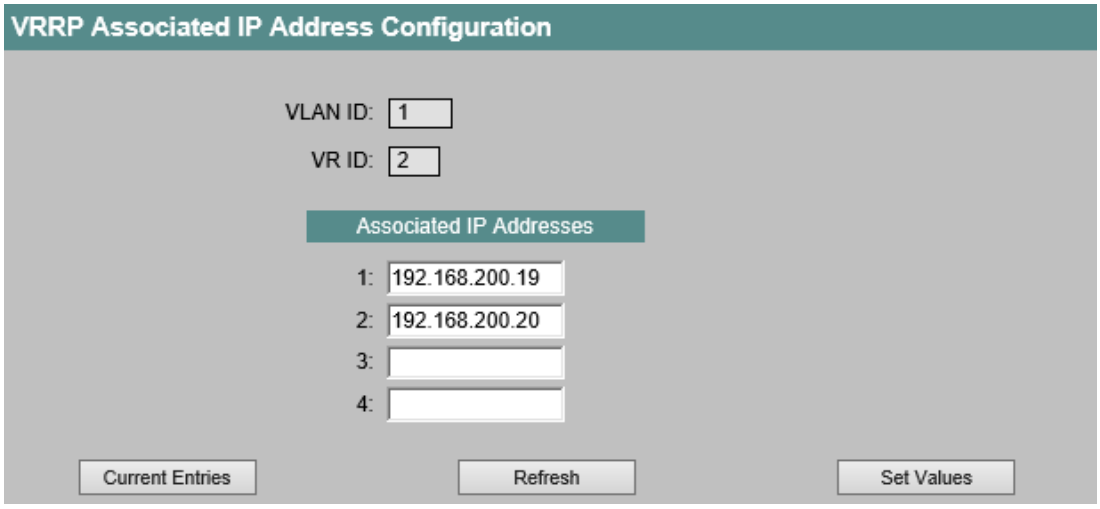


图 5-155　VRRP 关联 IP 地址组态

VLAN ID
显示所组态的虚拟路由器所在的 VLAN。

VR ID
显示该虚拟路由器的 ID。

文本框 1、文本框 2、文本框 3 和 文本框 4：
在此处输入要在该虚拟路由器中监视的冗余 IP 地址。

命令行接口语法

VRRP - CLI\ROUTER\VRRP\ADDR>

命令	说明	注释
info	显示当前监视的 IP 地址。	-
add <VID> <VRID> <IP>	添加要监视的新 IP 地址。	仅限管理员。
delete <VID> <VRID> <IP>	删除所监视的 IP 地址。	仅限管理员。

5.7.16 VRRP 统计信息

简介

在该菜单项中，可以查看 VRRP 协议以及全部组态虚拟路由器的统计信息。

可用“复位计数器”(Reset Counters） 按钮将这些统计值复位为 0。

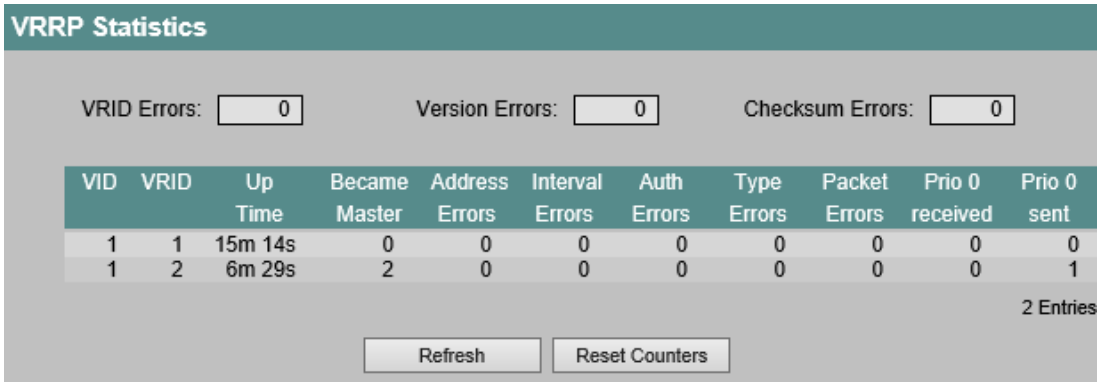


图 5-156 VRRP 统计信息

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)
显示包含无效检验和的已接收 VRRP 数据包的数目。

VID
子网的 VLAN ID。为此设置的 IP 地址以及全部子网参数均可在“路由器子网” (Router Subnets) 菜单中找到。

VRID
在该列显示虚拟路由器的 ID。该分配的 ID 必须对此 VLAN 是唯一的。有效值为 1 到 255。

接通时间 (Up Time)
此列显示虚拟路由器的调试时间。

说明

MIB 对象“vrrpOperVirtualRouterUpTime”表示虚拟路由器开启时的时间。为使信息更加清晰，“启动时间”(Up Time) 列显示虚拟路由器已开启了多长的时间。
更准确地说，“启动时间”(Up Time) 列显示当前 sysUpTime 与 MIB 对象之间的差值。

成为主设备 (Became Master)
显示该虚拟路由器变为“主设备”状态的频率。

地址错误 (Address Errors)
显示接收到包含不良地址列表的数据包的频率。

间隔错误 (Interval Errors)
该列显示接收到的不良数据包数目，这些不良数据包的通告间隔不再与本地设置的值相匹配。

验证错误 (Auth Errors)
此列显示验证类型不是类型 0 的不良接收数据包的数量。类型 0 是唯一可接受的类型，表示“无验证”。

说明

“验证错误”(Auth Errors) 列是 MIB 对象“vrrpStatsInvalidAthType”和“vrrpStatsAuthTypeMismatch”之和。

类型错误 (Type Errors)
该列显示接收到的未正确设置 VRRP 的不良数据包数目。

包错误 (Packet Errors)
该列显示接收到的不良数据包数目。这包括长度不正确的数据包和 IP 报头中 TTL 值不正确的数据包。

说明

“包错误” (Packet Errors) 列是 MIB 对象“vrrpStatsPacketLengthError”与“vrrpStatsIpTtlErrors”之和。

已接收的优先级 0 (Prio 0 received)
显示已接收的优先级为 0 的数据包数目。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。

已发送的优先级 0 (Prio 0 sent)
显示已发送的优先级为 0 的数据包数目。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。

命令行接口语法

VRRP - CLI\ROUTER\VRRP\STAT

命令	说明	注释
Info	显示 VRRP 统计信息。	-
resetc	将统计值复位为 0。	仅限管理员。

通过 SNMP 进行组态和诊断

6

通过 SNMP 组态工业以太网交换机

通过使用 SNMP（**S**imple **N**etwork **M**anagement **P**rotocol，简单网络管理协议），网络管理站可组态和监视 SNMP 兼容节点（例如工业以太网交换机）。为实现这一点，需在通过 Get 和 Set 请求与管理站交换数据的节点上安装管理代理。工业以太网交换机支持 SNMPv1、SNMPv2 和 SNMPv3。

可组态数据存储在工业以太网交换机上称为 MIB（**M**anagement **I**nformation **B**ase，管理信息库）的数据库中，可以通过管理站或基于 Web 的管理来访问该数据库。

说明

仅批准通过 WBM 和 CLI 完成的设置

与通过 WBM 或 CLI 进行组态相比，通过 SNMP 进行组态时，将只对设备组态进行有限的合理性和一致性检查，或者根本不检查。错误的设备组态可能导致数据丢失并导致整个网络受损。

只有通过 WBM 或 CLI 完成的组态设置才会经过测试和批准。

SIMATIC NET SNMP OPC 服务器

SNMP OPC 服务器通过 SNMP（Simple Network Management Protocol，简单网络管理协议）使来自 TCP/IP 网络的 SNMP 信息在 IOPC 接口上可用。借助 SNMP OPC 服务器，任何 OPC 客户端系统（如 WinCC）现在都可以访问 SNMP 兼容组件的诊断和参数数据。

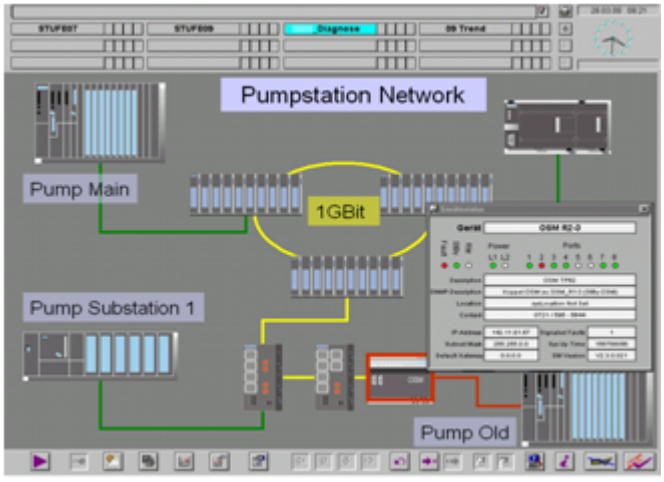


图 6-1　使用 SIMATIC NET SNMP OPC 服务器的 WinCC 网络诊断示例

对于工厂中非 SNMP 兼容的组件，也可通过其 IP 地址来实现可视化。例如，这样不仅可以显示简单的设备诊断信息，还可以显示详细的信息，如整个 TCP/IP 网络的冗余网络架构或网络负载分配情况。通过进一步监视这些数据，可实现快速检测并定位设备故障。因此可提高操作安全以及工厂可用性。使用 STEP 7（或者 NCM PC）来组态将由 SNMP OPC 服务器监视的设备。

有关 SIMATIC NET 提供的 SNMP OPC 服务器的详细信息，请访问以下链接：

SNMP OPC 服务器 (http://www.automation.siemens.com/mcms/industrial-communication/zh/ie/software/network-management/snmp-opc-server/Pages/snmp-opc-server.aspx)

SNMP OPC MIB 编译程序和配置文件

可通过装有 SNMP OPC 服务器的设备来监视的信息取决于具体的设备配置文件。可使用集成的 MIB 编译程序来修改现有的配置文件以及为任何 SNMP 兼容设备创建的新设备配置文件。

SNMP OPCM 服务器的 MIB 编译程序需要符合 SMIv1 标准的 MIB 文件。这意味着用户需要使用工业以太网交换机专有 SMIv2 MIB 文件的修改版本。可使用以下链接下载工业以太网交换机的 SMIv1 MIB 和完整的设备配置文件：

专有 MIB (http://support.automation.siemens.com/WW/view/zh/22015045)（条目 ID：22015045）

标准 MIB

RFC 中定义的标准 MIB 和专有 MIB 之间存在区别。专有 MIB 包含产品特定的扩展，而标准 MIB 中并不包含。

工业以太网交换机支持以下 MIB：

- RFC 1213：MIB II（除 egp 和传输之外的所有组）
- RFC 2233：接口 MIB（符合组 4、5、6、7、10、11、13）
- RFC 1286、RFC 1493：网桥 MIB（dot1dBase 和 dot1dStp）
- RFC 1724：RIP 版本 2 MIB 扩展（SCALANCE X414-3E）
- RFC 1757：RMON MIB（统计信息、历史、报警、事件）
- RFC 1850：OSPF 版本 2 管理信息库（SCALANCE X414-3E）
- RFC 2665：EtherLike MIB（适用于 SMIv2 的 dot3StatsTable）
- RFC 2674p：P BRIDGE MIB（符合组 1、2、3、4、6、8、9）
- RFC 2674q：P BRIDGE MIB（在一定程度上符合组 1、3、4、6、7、8、5）
- RFC 1907：SNMPv2 MIB（符合组 5、6、7、8、9）
- RFC 2571：SNMP FRAMEWORK MIB（SNMPv3 MIB：符合组 1）
- RFC 2572：SNMP MPD MIB（SNMPv3 MIB：符合组 1）
- RFC 2573：SNMP NOTIFICATION MIB
  （SNMPv3 MIB：符合组 1、2）
- RFC 2573：SNMP PROXY MIB
- RFC 2573：SNMP TARGET MIB（SNMPv3 MIB：符合组 1、2、3）
- RFC 2574：SNMP-USER-BASED-SM-MIB
  （SNMPv3 MIB：符合组 1）
- RFC 2575：SNMP VIEW-BASED ACM MIB
  （SNMPv3 MIB：符合组 1）
- RFC 2787：VRRP-MIB（虚拟路由器冗余协议，仅限 SCALANCE X414-3E）

专有 MIB

有关工业以太网交换机专有 MIB 的信息，请参见本手册附录 B。

访问工业以太网交换机的专有 MIB 文件

请按照以下步骤访问工业以太网交换机的专有 MIB 文件：

1. 打开基于 Web 的管理。
2. 选择“系统 -> 保存和加载 HTTP”(System -> Save & Load HTTP) 菜单项
3. 单击“保存专有 MIB”(Save Private MIB) 按钮。
4. 系统会提示用户选择存储位置及文件名称，或接受建议的文件名称。

PROFINET IO 功能

7

7.1 用 PROFINET IO 进行组态

使用 PROFINET IO

对工业以太网交换机进行诊断、参数分配和生成报警消息的其中一个选项是使用 PROFINET IO。

通过本部分内容，用户将了解针对所连接的工业以太网交换机如何使用 PROFINET IO 选项。

在本例中，假设 PROFINET IO 控制器 V2 已用 PROFINET IO 链进行了组态（另请参见《PROFINET IO 系统手册》）。

说明

需要 STEP 7 V5.4 SP5 或更高版本。

以下内容以 SCALANCE X-400 为例，给出了包含 PROFINET IO 线路的硬件配置。

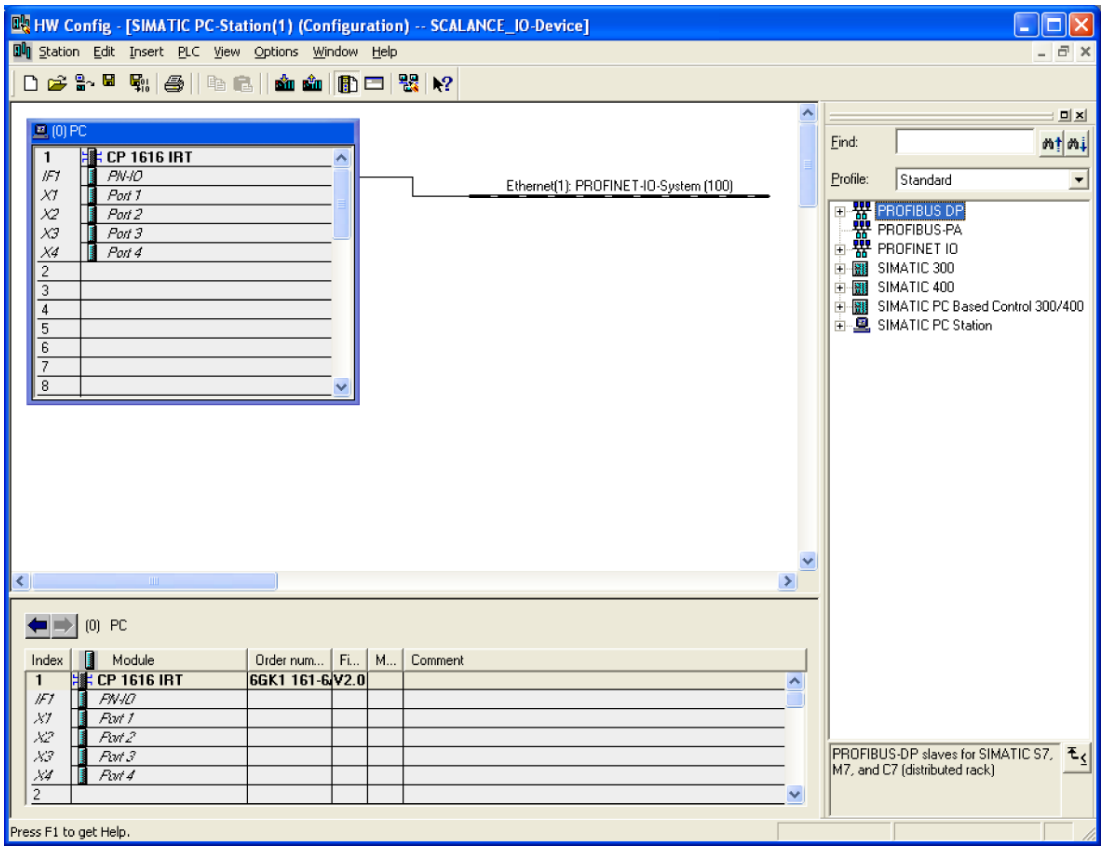


图 7-1　HW Config PROFINET IO 站设置

连接工业以太网交换机

相应的工业以太网交换机必须在模块目录的 PROFINET IO 下存在，才能将其用作 PN IO 设备。

步骤

如果 STEP 7 中尚未包括相应设备，请按照以下步骤操作：

1. 在对话框中，选择 HW Config -> 选项“安装 GSD 文件”(Install GSD files)。
   将出现以下屏幕：

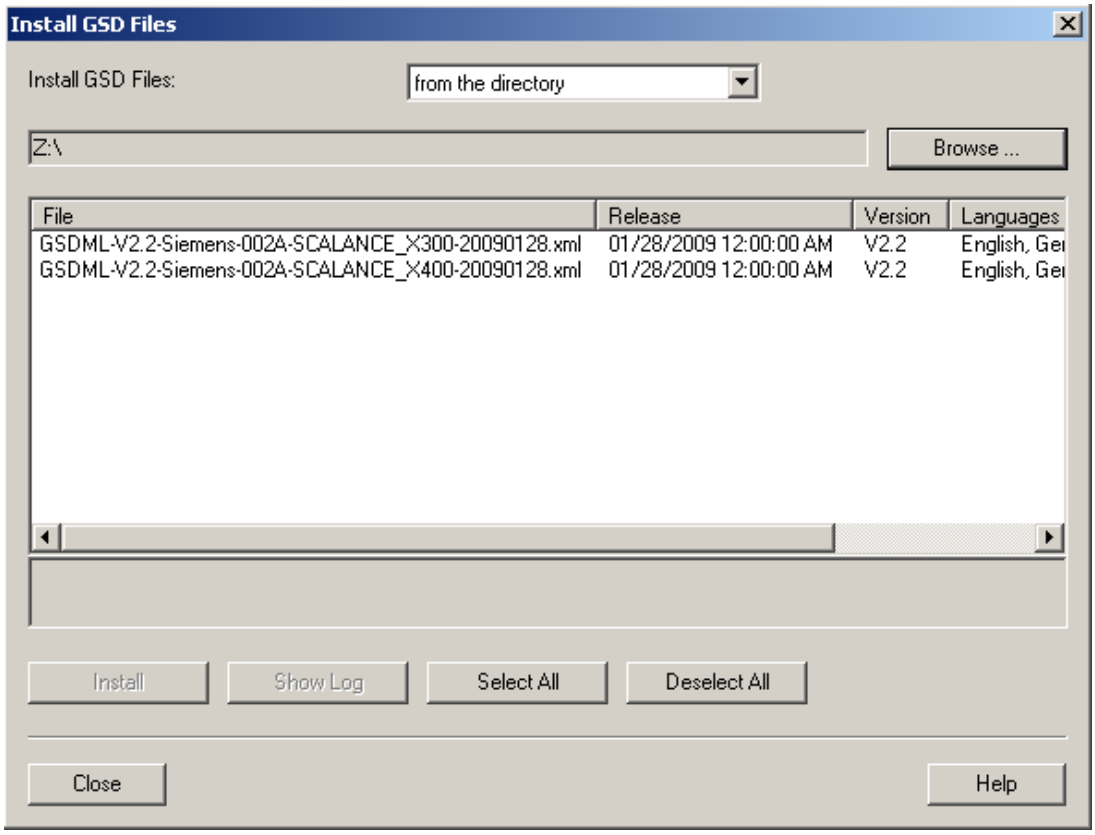


图 7-2　安装 GSD 文件

2. 使用“浏览”(Browse) 功能找到所提供的 xml 文件（例如 GSDML-Vx.x-Siemens-002A-SCALANCE_X400-YYYYMMDD.xml - Y、M 和 D 表示文件的发布日期）。

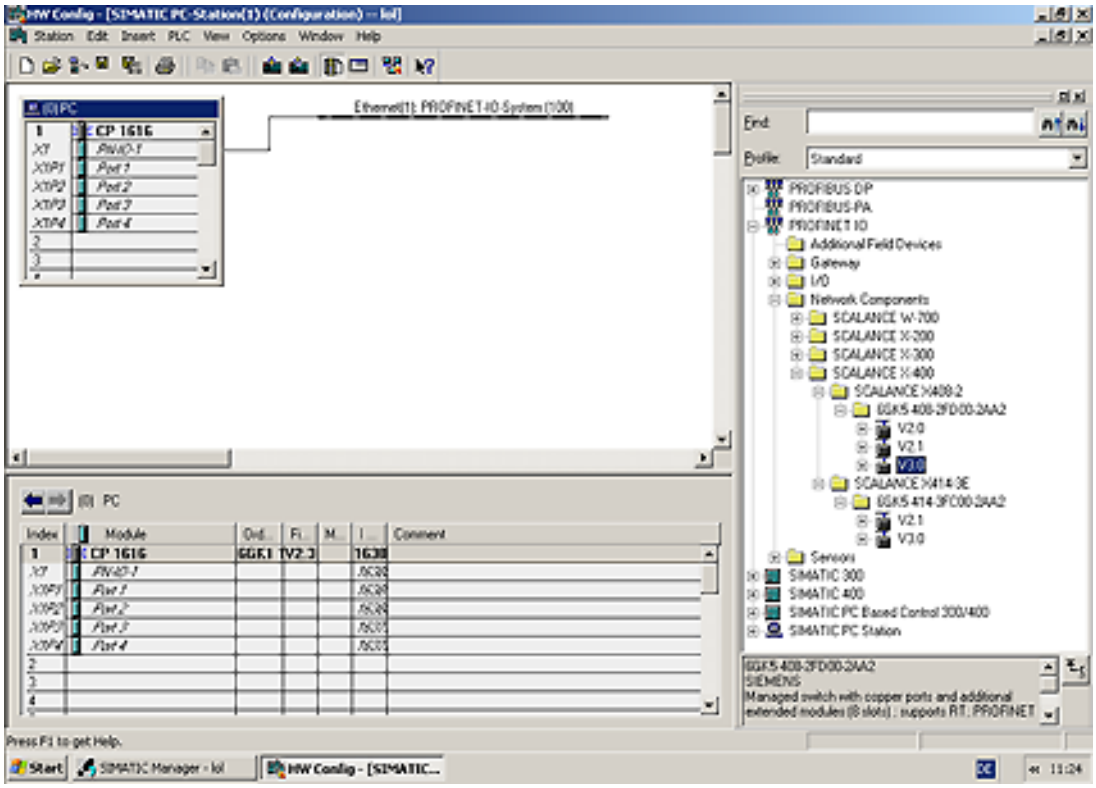


图 7-3　HW Config PROFINET IO - 插入 SCALANCE 交换机

3. 然后，使用“安装”(Install) 功能采用该文件。
   现在，工业以太网交换机即包含在模块目录中（见下图中的模块目录）。

4. 从硬件目录中选择所需的工业以太网交换机，例如，SCALANCE X408-2（PROFINET IO > 网络组件 > SCALANCE X-400 交换机 > SCALANCE X408-2）。 将所选的 SCALANCE 拖动到 PROFINET IO 系统中。

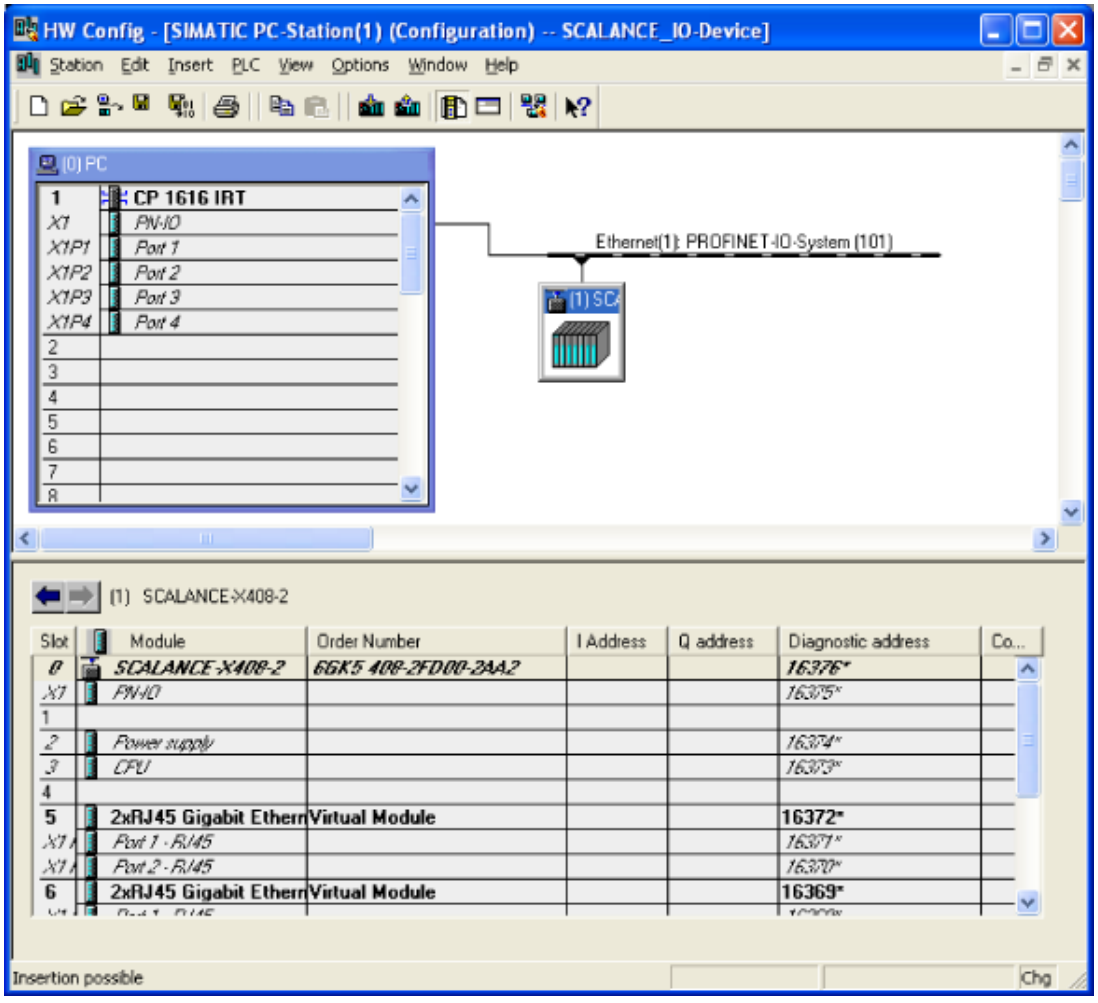


图 7-4　HW Config PROFINET IO - 设置全局参数

5. 单击"(1)SCALANCE"图标，该工业以太网交换机的插槽随即会在屏幕下方显示。 通过双击插槽 0，可以设置工业以太网交换机（替代模块）的全局参数，如图所示。
6. 可以通过双击插槽来查看和设置它的属性。

7. 单击端口的插槽，设置特定于端口的参数。

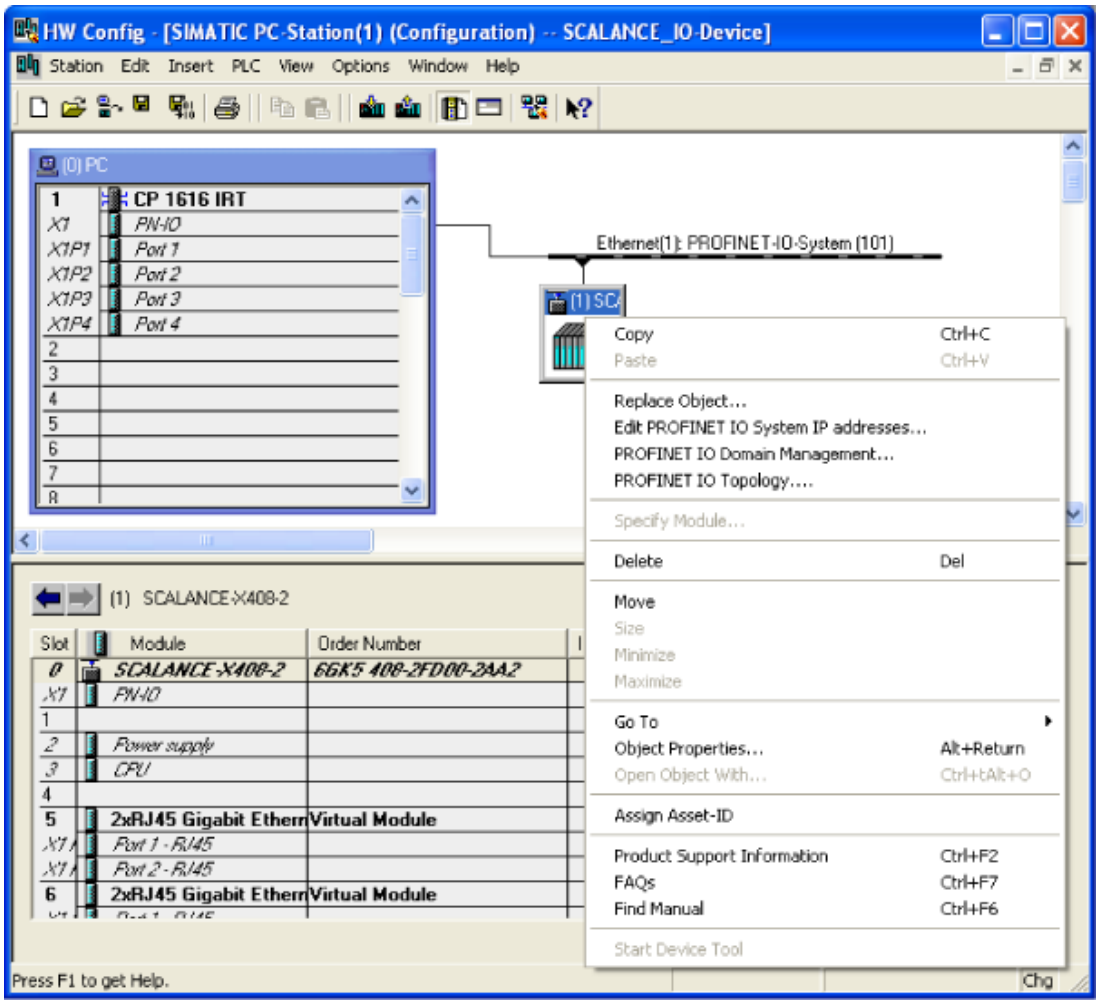


图 7-5 HW-Config

8. 在 HW Config 中打开“SCALANCE X408-2 对象属性”(Object Properties of the SCALANCE X408-2) 对话框（右键单击 “图标”(Icon) -> “对象属性”(Object Properties)），输入 PROFINET IO 设备的名称。 单击 “确定”(OK) 退出对话框。

9. 选择“站 > 保存并编译”(Station > Save and Compile) 菜单命令。
10. 通过网络使设备互连，并接通联网设备的电源。

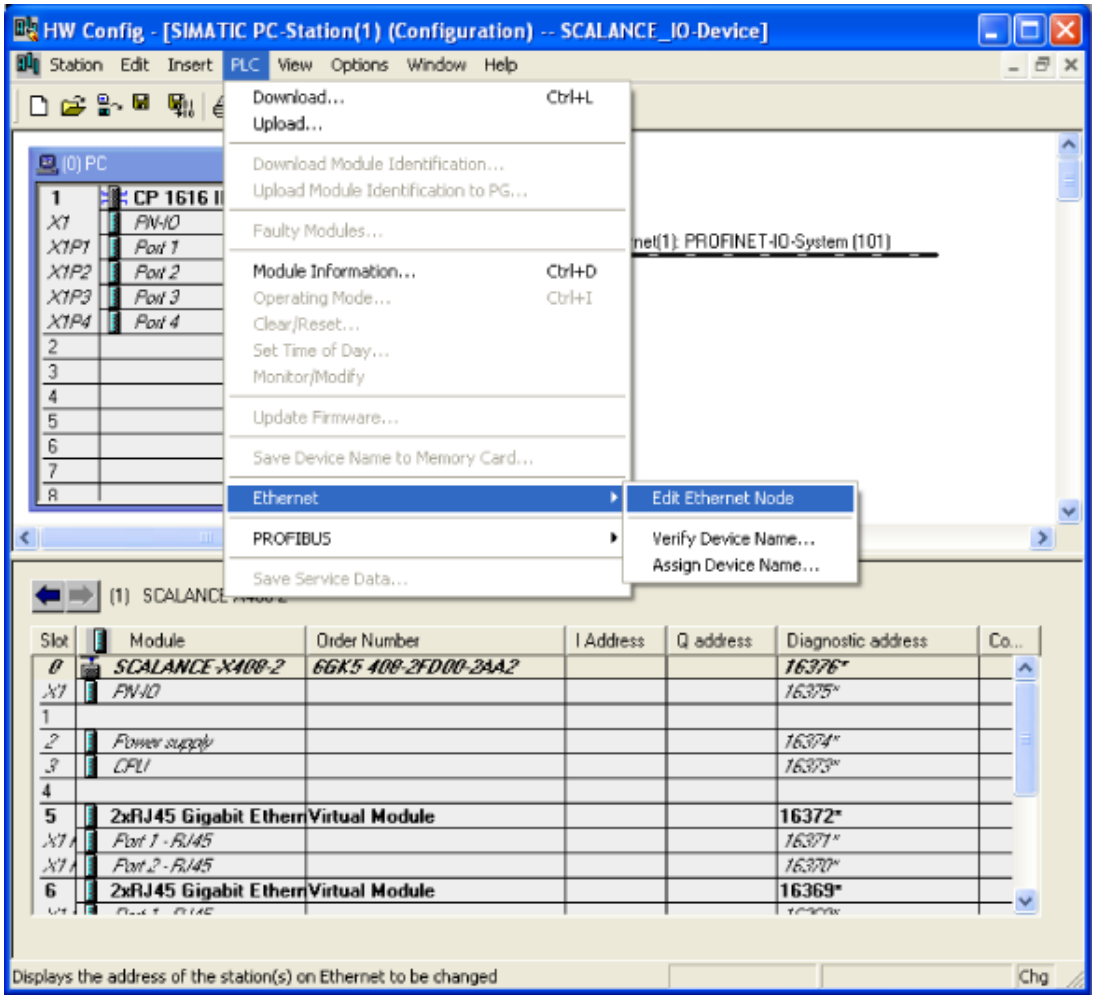


图 7-6　HW Config 分配 PROFINET IO 设备名称

要将该名称传送到 SCALANCE X408-2，需要从 PG 在线连接到 PROFINET IO 设备。

1. 可以通过“PLC > 以太网 > 分配设备名称”(PLC > Ethernet > Assign Device Name) 将设备名称传送到 SCALANCE X408-2。

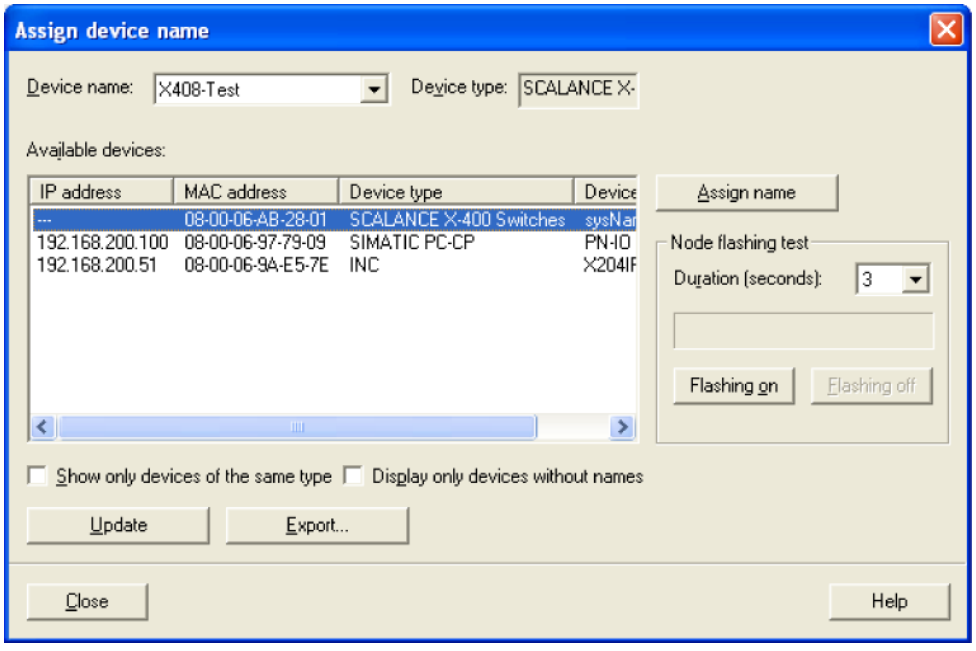


图 7-7　分配设备名称

如果正在使用多个 PROFINET IO 设备，则“分配设备名”(Assign device name) 对话框也将显示多个 PROFINET IO 设备。 在这种情况下，应该将设备的 MAC 地址与指定的 MAC 地址相比较，然后选正确的 IO 设备。 也可以使用“启用/禁用闪烁”(Flashing On/Off) 按钮（所选 SCALANCE 上的所有 LED 都会闪烁）用肉眼检查分配情况。

1. 单击“分配设备名称”(Assign Device Names) 对话框中的“分配名称”(Assign Names) 按钮。设备名称将永久存储在工业以太网交换机中。 在分配名称之后，所分配的设备名称将显示在对话框中。
2. 将硬件组态下载到控制器（本例中是 CP 1616）中。 选择“PLC > 下载到模块”(PLC > Download to Module)。

7.2 HW Config 中的设置

说明

对于 IE Switch X-400，电源和 C-PLUG 中断设置分布在“电源”(Power Supply) 和“CPU”这两个屏幕。 对于 IE Switch X-300，这些设置则集中在一个屏幕。

电源监视

在此设置与电源相关的工业以太网交换机参数。

冗余电源 (Redundant power supply)

- 不监视 (Not monitored)
  两个电源中的有一个出现故障时，不产生报警。
- 监视 (Monitored)
  两个电源中的有一个出现故障时，产生报警。

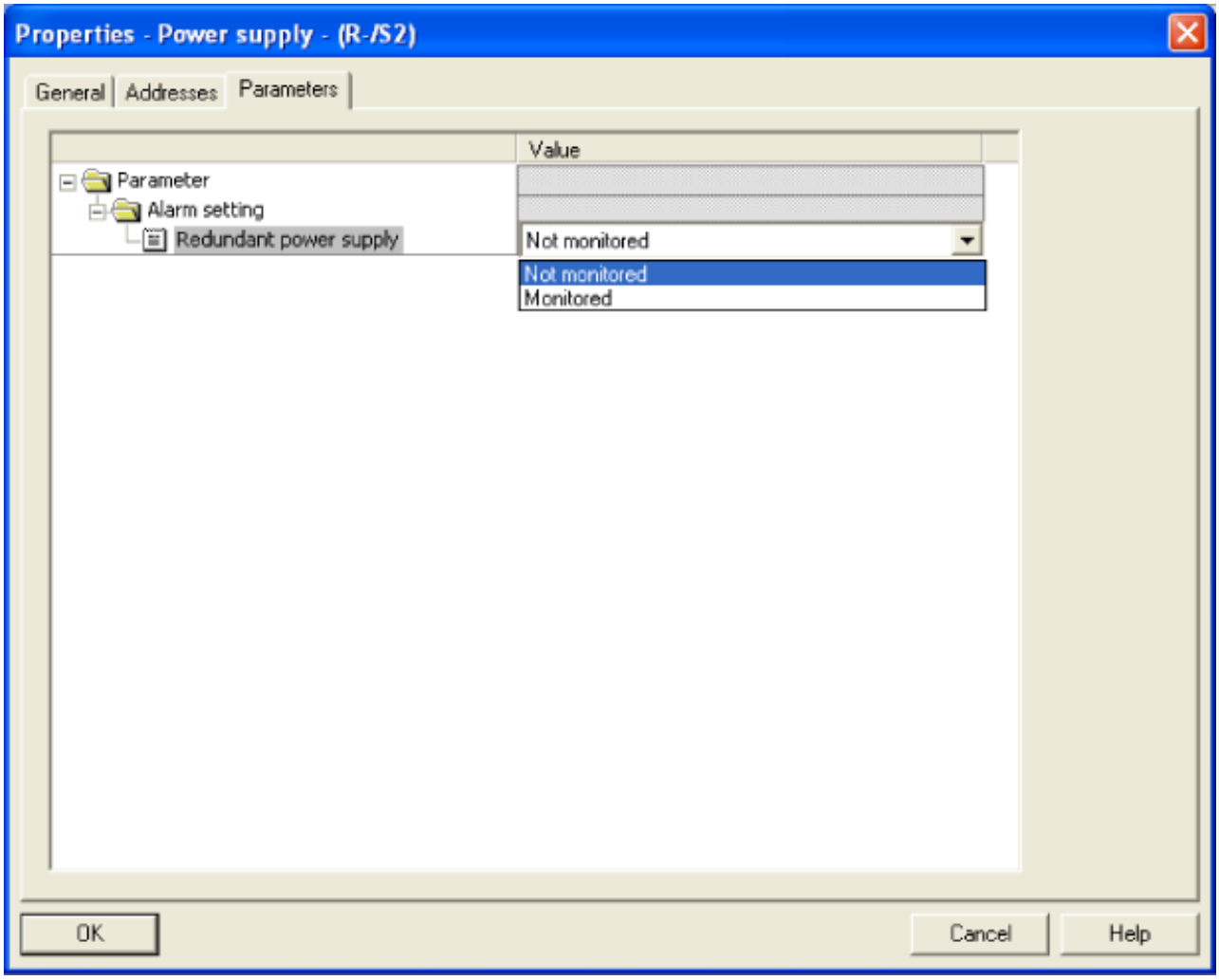


图 7-8　属性 - IE Switch X-400 的电源

CPU 监视

在此设置与 CPU 模块相关的工业以太网交换机参数。

C-PLUG

- 不监视 (Not monitored)
  不监视 C-PLUG。
- 监视 (Monitored)
  C-PLUG 故障将导致报警产生。

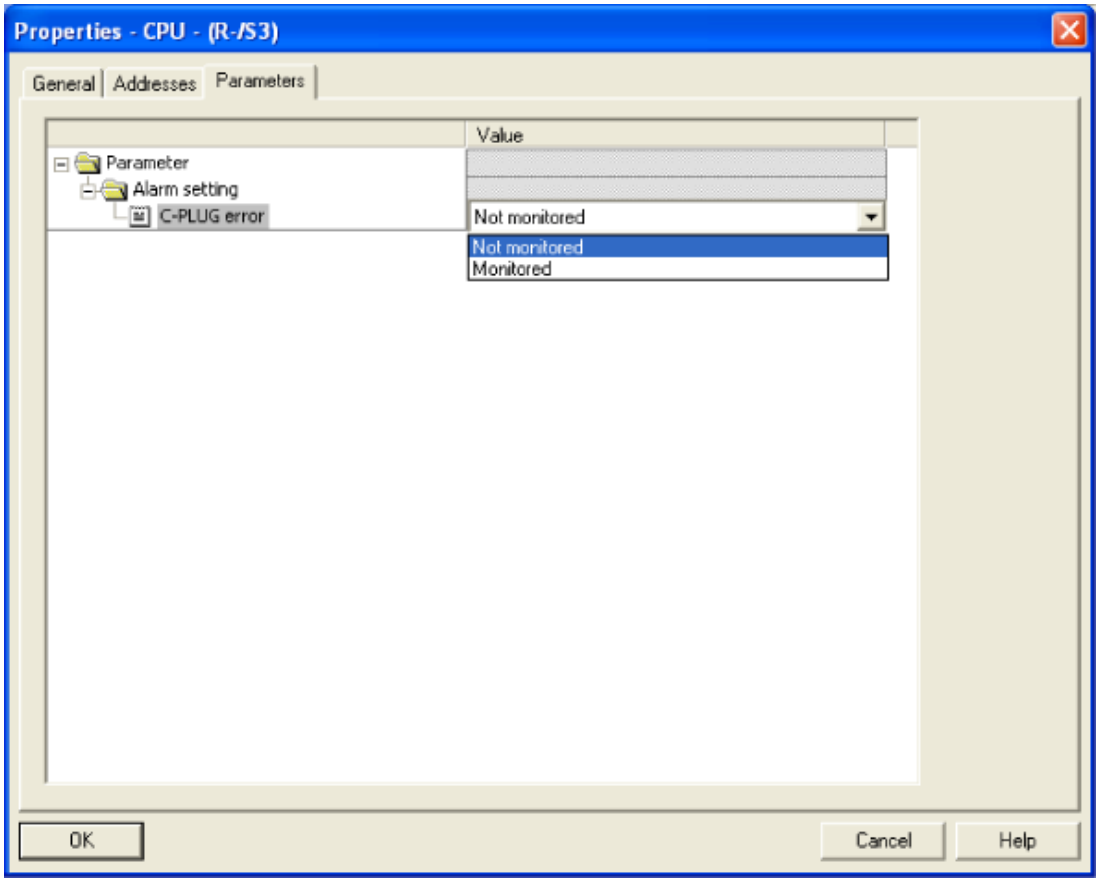


图 7-9　属性 - IE Switch X-400 的 CPU

E Switch X-300 的电源监视和 CPU 监视

此处的可用选项与本章前一部分描述的选项相同。

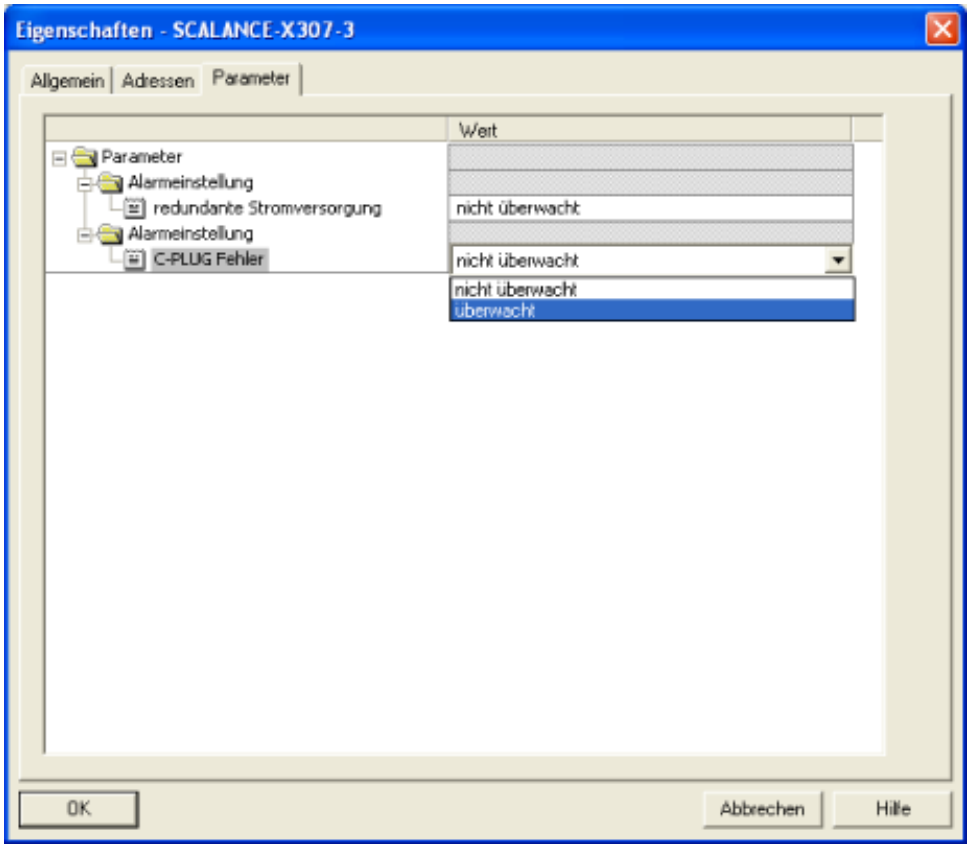


图 7-10　属性 - IE Switch X-300 的电源和 CPU

特定于端口的设置

可在此对工业以太网交换机的各个端口进行设置。
下面的屏幕显示了以 SCALANCE X408-2 为例的一些设置。

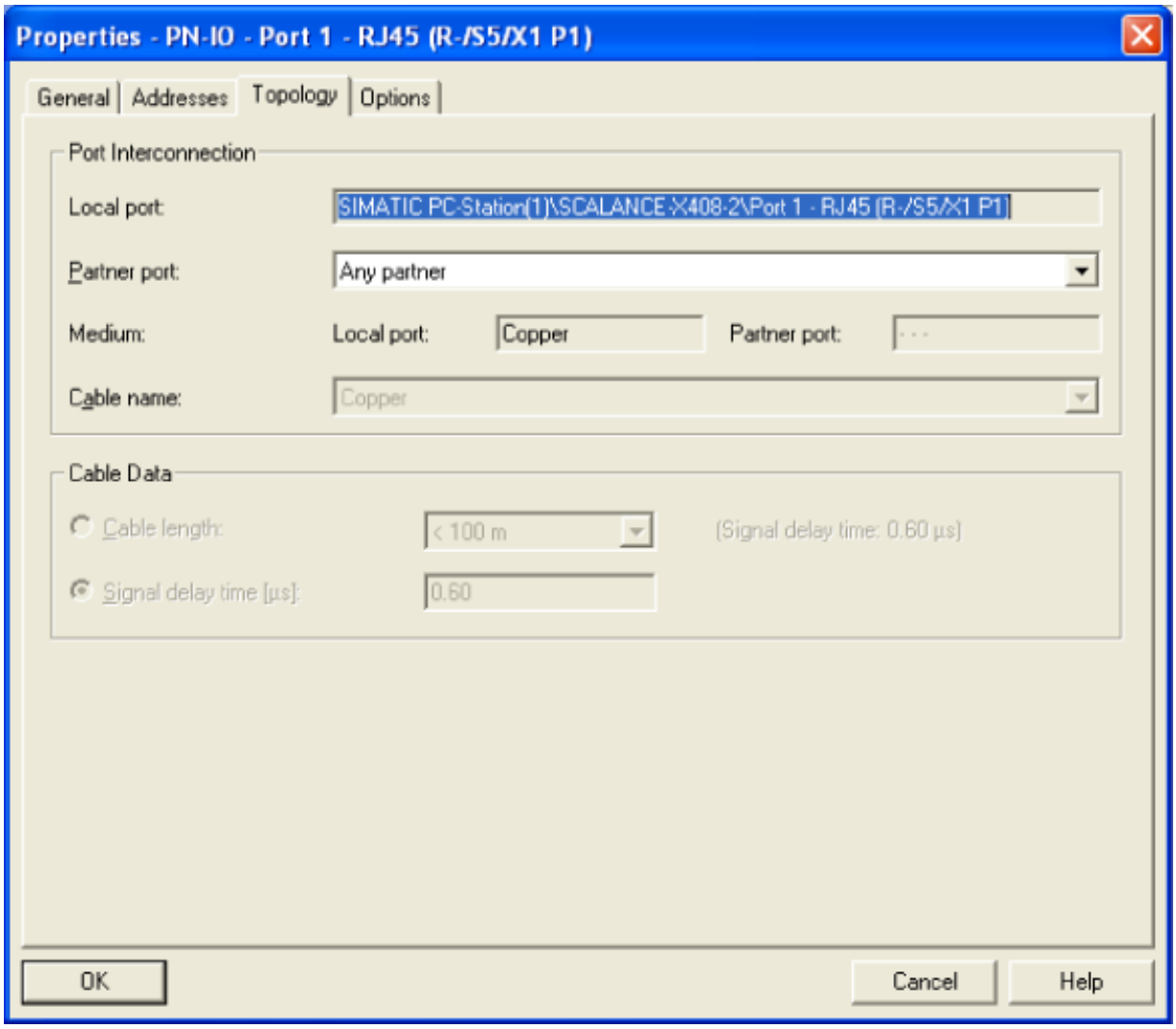


图 7-11　属性 - RJ-45 千兆位以太网

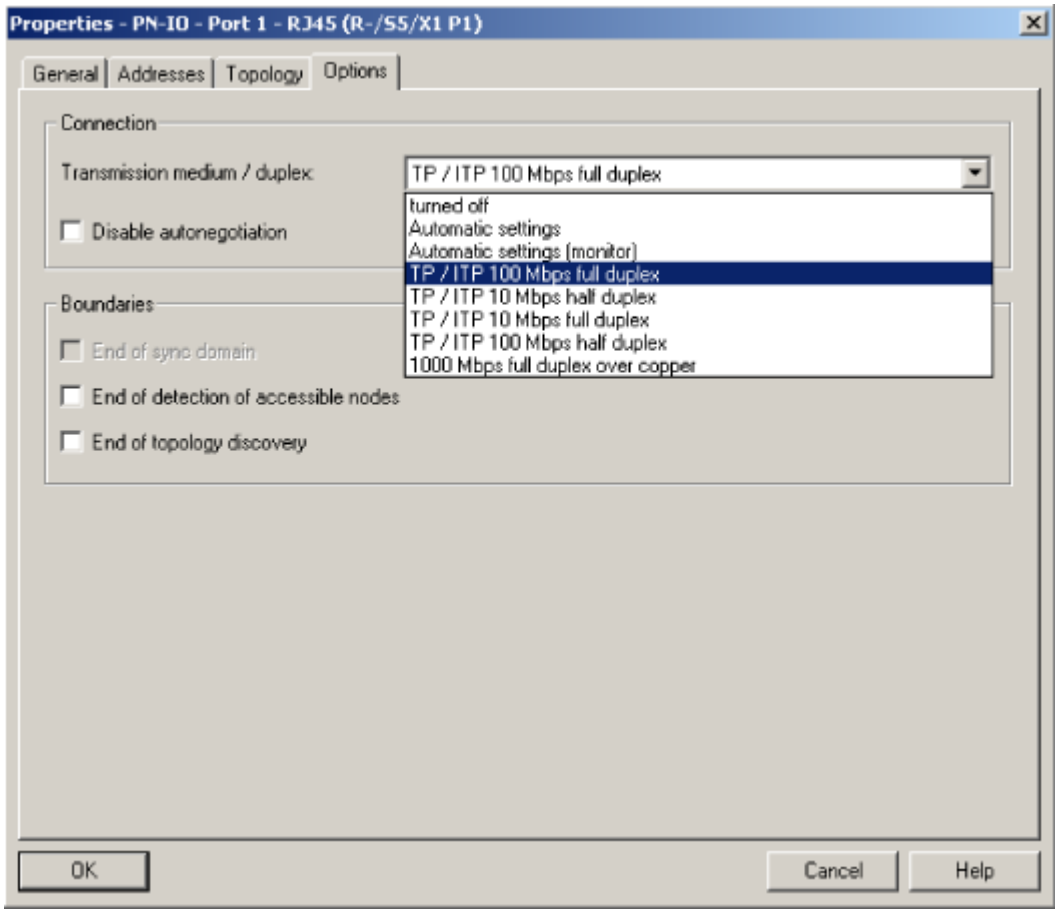


图 7-12　属性 - RJ-45 千兆位以太网端口选项

组态期间进行的设置

可将端口传输率设为自动协商传输率或固定传输率，例如，设为全双工 100 Mbps。

说明

如果选择固定速率和双工传输，则需要选中“禁用自动协商”(Disable autonegotiation)。

7.3 通过 PROFINET IO 提供的访问选项

说明

插槽功能 X-300 表适用于除以下自己拥有表的设备之外的所有 X-300 系列工业以太网交换机：

- X308-2M 插槽功能
- XR-324-12M 的插槽功能
- X302-7EEC 和 X307-2EEC 的插槽功能
- XR324-4M EEC 的插槽功能

X-300 的插槽功能

工业以太网交换机 X-300 的每个交换机端口在插槽 0 中都有一个子插槽。
将无法唯一分配给一个端口的功能分配给设备接入点（插槽 0）。

插槽 0	子插槽 1	• 报警 • 数据记录 (4.5)	设备接入点 (DAP) • 接口连接 • C-PLUG • 冗余电源
	子插槽 8001 - 8010 **SCALANCE X304-2FE：** 子插槽 8001 - 8006 **SCALANCE X306-1LD FE：** 子插槽 8001 - 8007 **SCALANCE X320-1FE：** 子插槽 8001 - 8021 **SCALANCE X320-3LD：** 子插槽 8001 - 8023	• 报警 (IEC) • 数据记录 (IEC)	交换机端口 1 - 10（或 1 - 6、1 - 7、1 - 21、1 - 23） • 报警响应 • 端口状态

X308-2M 插槽功能

工业以太网交换机 X308-2M 有 3 个插槽。固定插槽分配给了插槽 0。其它具有 2 个端口的插槽分配给插槽 1 和插槽 2。
将无法唯一分配给一个端口的功能分配给设备接入点（插槽 0）。

插槽 0	子插槽 1	• 报警 • 数据记录 (4.5)	设备接入点 (DAP) • 接口连接 • C-PLUG • 冗余电源
	子插槽 8001 - 8004	• 报警 (IEC) • 数据记录 (IEC)	交换机端口 1 - 4 • 报警响应 • 端口状态
插槽 1；插槽 2	子插槽 8001 - 8002	• 报警 (IEC) • 数据记录 (IEC)	交换机端口 5 - 6； 交换机端口 7 - 8 • 报警响应 • 端口状态

XR324-12M 的插槽功能

工业以太网交换机 XR324-12M 有多个插槽（插槽 1 - 插槽 12），每个插槽有 2 个端口。
无法具体分配给某一个端口的功能将被分配给设备接入点（插槽 0）。

插槽 0	子插槽 1	• 报警 • 数据记录 (4.5)	设备接入点 (DAP) • 接口连接 • C-PLUG • 冗余电源
插槽 1 到插槽 12	子插槽 8001 - 8002	• 报警 (IEC) • 数据记录 (IEC)	交换机端口 1.1 - 12.2 • 报警响应 • 端口状态

X302-7EEC 和 X307-2EEC 的插槽功能

工业以太网交换机 X302-7EEC 和 X307-2EEC 在插槽 0 中有一个子插槽。无法唯一分配给一个端口的功能将被分配给设备接入点（插槽 0）。

插槽 0	子插槽 1	• 报警 • 数据记录 (4.5)	设备接入点 (DAP) • 接口连接 • C-PLUG • 冗余电源
	子插槽 8001 - 8009	• 报警 (IEC) • 数据记录 (IEC)	交换机端口 1 - 9 • 报警响应 • 端口状态

XR324-4M EEC 的插槽功能

工业以太网交换机 XR324-4M EEC 有多个插槽。固定插槽分配给了插槽 0。其它具有 2 个端口的插槽分配给插槽 1 和插槽 4。
将无法具体分配给某一个端口的功能分配给设备接入点（插槽 0）。

插槽 0	子插槽 1	• 报警 • 数据记录 (4.5)	设备接入点 (DAP) • 接口连接 • C-PLUG • 冗余电源
	子插槽 8001-8016	• 报警 (IEC) • 数据记录 (IEC)	交换机端口 1-16 • 报警响应 • 端口状态
插槽 1 到 插槽 4	子插槽 8001 - 8002	• 报警 (IEC) • 数据记录 (IEC)	交换机端口 1.1 - 4.2 • 报警响应 • 端口状态

X-400 的插槽功能

工业以太网交换机 X-400 有多个插槽，每个插槽最多有四个端口。 将无法唯一配给某一个端口的功能分配给设备接入点（插槽 0），或分配给其它较高级别的模块（CPU 和电源模块）。

插槽 0	子插槽 1	• 报警 (IEC) • 数据记录 (IEC)	设备接入点 (DAP) • 接口连接
插槽 2	子插槽 1	• 报警 0x200 • 数据记录 10、12	电源模块 • 冗余电源
插槽 3 (X408) 插槽 4 (X414)	子插槽 1	• 报警 0x201、0x202、0x203、0x204 • 数据记录 11、13	CPU 模块 • C-PLUG
插槽 5、6 和 8 (X408)) 插槽 5-7、9-15 (X414)	子插槽 8001-800n	• 报警 (IEC) • 数据记录 (IEC)	交换机端口 5.1-8.4 (X408) 交换机端口 5.1-15.2 (X414) • 报警响应 • 端口状态

生成报警

用户对端口的分配和所需属性进行准确组态。 使得匹配组态和安装十分必要。 如果 STEP 7 中的设置要求端口 3 断开连接，则必须在安装期间对此加以考虑。 STEP 7 设置的电源故障屏蔽会采用保持性存储，并会复位端口故障屏蔽。 如果退出 DataEX，将保留 STEP 7 执行的故障屏蔽设置并继续使用，即使不执行 PROFINET 操作。

- DataEX 期间 SELECT/SET 按钮的作用。
  按下该按钮设置故障屏蔽时不起作用。 端口 LED 闪烁时，即是告知用户故障屏蔽无任何变化。
- DataEX 期间其它信号机制的作用
  在 Web 接口和 CLI 中显示通过 STEP 7 设置的故障屏蔽。 不能进行更改。 显示消息 “因 PROFINET IO 而不允许该设置”(Setting not possible because of PROFINET IO)。

数据记录的结构

说明

数据记录 4 和 5 与 IE Switch X-300 有关，数据记录 10 至 13 与 IE Switch X-400 相关。

数据记录 4：

访问： 读写，

结构：

typedef struct {

Word BlockType;

Word BlockLength;

Byte BlockVersionHigh:

Byte BlockVersionLow:

DWord Alarm_enable; };

BlockType：

1: 常量

BlockLength：

6: 设备数据中的常量，表示不带 Type+ Length 的长度

BlockVersionHigh：

1: 设备数据中的常量，表示主要版本

BlockVersionLow：

1: 设备数据中的常量，表示次要版本

Enable_alarms：

该位列表指定要监控的对象。 如果某个位置位，则会启用该报警源。

预留 **位 2 - 31**	**C-PLUG** **位 1**	**Red_power** **位 0**
0	0: 无 C-PLUG 监视	0: 不监视冗余电源
	1: C-PLUG 缺少或不正确时会生成报警	1: 监视冗余电源

数据记录 5：

为该端口提供最新报警设置

访问： 只读

typedef struct {

Word BlockType;

Word BlockLength;

Byte BlockVersionHigh;

Byte BlockVersionLow;

DWord status; };

BlockType：

1: 常量

BlockLength：

6: 设备数据中的常量，表示不带 Type+ Length 的长度

BlockVersionHigh：

1: 设备数据中的常量，表示主要版本

BlockVersionLow：

1: 设备数据中的常量，表示次要版本

状态：

预留 位 8-31	C-PLUG_status 位 4-7	预留 位 2-3	Fault_line_status 位 1	电源线路冗余 位 0
0	有关网络组件组态卡的信息 0: C-PLUG 已插入且功能正常 1：未插入 C-PLUG 2: C-PLUG 已插入但不正常（类型错误） 3: C-PLUG 已插入但不正常（校验和错误）		有关当前信号触点状态的信息 0: 故障线路未激活 1: 故障线路激活	该位提供有关冗余电源的信息 0: 非冗余 1: 冗余

数据记录 10（电源、参数分配）

访问： 读写，

结构：

typedef struct {

Word BlockType;

Word BlockLength;

Byte BlockVersionHigh:

Byte BlockVersionLow:

DWord Alarm_enable; };

BlockType

1: 常量

BlockLength

6: 设备数据中的常量，表示不带 Type+ Length 的长度

BlockVersionHigh

1: 设备数据中的常量，表示主要版本

BlockVersionLow

1: 设备数据中的常量，表示次要版本

Enable_alarms

预留 位 1-31	Red_power 位 0
0	0: 不监视冗余电源
	1: 监视冗余电源

数据记录 11（CPU、参数分配）

结构

```
typedef struct {
Word BlockType;
Word BlockLength;
Byte BlockVersionHigh:
Byte BlockVersionLow:
Word Alarm_Mode;
DWord Alarm_Parameter; };
```

BlockType

1: 常量

BlockLength

6: 设备数据中的常量，表示不带 Type+ Length 的长度

BlockVersionHigh

1: 设备数据中的常量，表示主要版本

BlockVersionLow

1: 设备数据中的常量，表示次要版本

Alarm_Mode

预留 位 2-31	**Enhanced_Alarm_Mode 位 1**	**Show_C-PLUG_Error 位 0**
0	无功能	0: 无 C-PLUG 监视
		1: C-PLUG 缺少或不正确时会生成报警。

数据记录 12（电源、模块状态）

为该端口提供最新报警设置

访问： 只读

typedef struct {

Word BlockType;

Word BlockLength;

Byte BlockVersionHigh;

Byte BlockVersionLow;

DWord status; };

BlockType

1: 常量

BlockLength

6: 设备数据中的常量，表示不带 Type+ Length 的长度

BlockVersionHigh

1: 设备数据中的常量，表示主要版本

BlockVersionLow

1: 设备数据中的常量，表示次要版本

状态

预留 位 2-31	Fault_line_status 位 1	电源线路冗余 位 0
0	有关当前信号触点状态的信息 0: 故障线路未激活 1: 故障线路激活	该位提供有关冗余电源的信息 0: 非冗余 1: 冗余

数据记录 13（CPU、模块状态）

结构

```
typedef struct {
Word BlockType;
Word BlockLength;
Byte BlockVersionHigh;
Byte BlockVersionLow;
DWord PortState;
byte PortType;
byte reserved; };
```

BlockType

1: 常量

BlockLength

6: 设备数据中的常量，表示不带 Type+ Length 的长度

BlockVersionHigh

1: 设备数据中的常量，表示主要版本

BlockVersionLow

1: 设备数据中的常量，表示次要版本

状态

预留 **位 2-31**	**C-PLUG_status** **位 0-1**
0	有关网络组件的 C-PLUG 的信息 0: C-PLUG 已插入且功能正常 1: 未插入 C-PLUG 2: C-PLUG 已插入但不正常（类型错误） 3: C-PLUG 已插入但不正常（校验和错误）

7.4 数据记录 0x802A (PDPortDataReal)

结构

```
typdef struct{
Word BlockType;
Word BlockLength;
Byte BlockVersionHigh;
Byte BlockVersionLow;
Word Padding;
Word SlotNumber;
Word SubslotNumber;
Byte LengthOwnPortID;
8 Byte OwnPortID;
Byte NumberOfPeers;
Word Padding;
Byte LengthPeerPortID;
8 Byte PeerPortID;
Byte LengthPeerChassisID;
8 Byte PeerChassisID;
Word Padding;
DWord LineDelay;
6 Byte PeerMACAddress;
Word Padding;
Word MAUType;
Word Padding;
DWord DomainBoundary;
DWord MulticastBoundary;
Word LinkState;
Word Padding;
DWord MediaType;};
```

BlockType

常量 = 0x020F

BlockLength

常量，表示不带 BlockType 和 BlockLength 字段的数据记录的长度。

BlockVersionHigh

常量 = 1，表示主要版本。

BlockVersionLow

常量 = 0，表示次要版本。

SlotNumber

插槽编号，请参见“通过 PROFINET IO 访问选项”部分

SubslotNumber

子插槽编号，请参见“通过 PROFINET IO 访问选项”部分

LengthOwnPortID

OwnPortID 字段的长度（字节）。

OwnPortID

所用端口的 ID。

NumberOfPeers

相邻端口数。

LengthPeerPortID

PeerPortID 字段的长度（字节）。

PeerPortID

相邻端口的 ID。

LengthPeerChassisID

PeerChassisID 字段的长度（字节）。

PeerChassisID

相邻设备的 ID。

LineDelay

LineDelay.FormatIndicator = 0

数值（十六进制）	含义
0x00000000	线路延迟和电缆延迟未知。
0x00000001 – 0x7FFFFFFF	线路延迟（纳秒）。

LineDelay.FormatIndicator = 1

数值（十六进制）	含义
0x00000000	预留
0x00000001 – 0x7FFFFFFF	电缆延迟（纳秒）。

PeerMACAddress

相邻设备的 MAC 地址。

MAUType

数值（十六进制）	含义
0x0000 – 0x0004	预留
0x0005	10BASET
0x0006-0x0009	预留
0x000A	10BASETXHD
0x000B	10BASETXFD
0x000C	10BASEFLHD
0x000D	10BASEFLFD
0x000F	100BASETXHD
0x0010	100BASETXFD（默认值）
0x0011	100BASEFXHD
0x0012	100BASEFXFD

数值（十六进制）	含义
0x0013 – 0x0014	预留
0x0015	1000BASEXHD
0x0016	1000BASEXFD
0x0017	1000BASELXHD
0x0018	1000BASELXFD
0x0019	1000BASESXHD
0x001A	1000BASESXFD
0x001B – 0x001C	预留
0x001D	1000BASETHD
0x001E	1000BASETFD
0x001F	10GigBASEFX
0x0020 – 0x002D	预留
0x002E	100BASELX10
0x002F – 0x0035	预留
0x0036	100BASEPXFD
0x0037 – 0xFFFF	预留

DomainBoundary

指定阻止使用哪些多播地址。

MulticastBoundary

DWord 变量的各个位指定要阻止 32 个首要 RT_CLASS_2 多播地址（从 01-0E-CF-00-02-00 到 01-0E-CF-00-02-1F）中的哪个地址。

位	值	含义
0	1	将阻止多播 MAC 地址 01-0E-CF-00-02-00。
	0	不阻止多播 MAC 地址 01-0E-CF-00-02-00。
...	1	将阻止多播 MAC 地址 01-0E-CF-00-02-xx。
	0	不阻止多播 MAC 地址 01-0E-CF-00-02-xx。
31	1	将阻止多播 MAC 地址 01-0E-CF-00-02-1F。
	0	不阻止多播 MAC 地址 01-0E-CF-00-02-1F。

LinkState

LinkState.Link

数值（十六进制）	含义
0x00	预留
0x01	接通（准备好发送数据包）
0x02	中断
0x03	测试（未传输用户数据）
0x04	未知（无法识别状态）
0x05	休眠（等待外部操作）
0x06	不存在
0x07	LowerLayerDown
0x08 - 0xFF	预留

LinkState.Port

数值（十六进制）	含义
0x00	未知
0x01	禁用/丢弃
0x02	屏蔽
0x03	已启用端口侦听
0x04	学习
0x05	转发
0x06	已中断
0x07 – 0xFF	预留

MediaType

数值（十六进制）	含义
0x00	未知
0x01	铜质电缆
0x02	光纤电缆

数值（十六进制）	含义
0x00	无线通信
0x04 – 0xFFFFFFFF	预留

说明

更多相关信息，请参见 IEC 61158 中的 IEC 数据记录。

7.5 MRP 组态

STEP 7 中的组态

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

为设备的 MRP 组态设置以下参数：

- 域
- 角色
- 环网端口
- 诊断中断

下文介绍了这些设置。

说明

有效的 MRP 组态

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

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

说明

注意出厂设置

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

- SCALANCE XB-200（EtherNet/IP 型号）
- SCALANCE XC-200（EtherNet/IP 型号）
- SCALANCE XP-200（EtherNet/IP 型号）
- SCALANCE XC-300
- SCALANCE XR-300
- SCALANCE XR-300WG
- SCALANCE XC-400
- SCALANCE XM-400
- SCALANCE XR-500

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

说明

只有环网处于打开状态时才能重新组态

在执行下述操作之前，首先打开环网

- 更改 MRP 角色，或
- 重新组态环网端口。

说明

启动和重启

设备重启或电源故障和热启动后，只要组态更改之后 90 秒内未发生电源故障，MRP 设置仍然有效。

说明

优先级启动

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

如果想要使用“优先级启动”功能，则在组态中禁用 MRP。

在 STEP 7 组态中，将相关设备的角色设置为“Not a node in the ring”。

域

单 MRP 环网

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

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

多 MRP 环网

借助 MRP 多环网功能，可使用一台中央冗余管理器控制多个 MRP 环网。如果组态多个单独 MRP 环网，将使用"Domain"参数将环网的节点分配给各个端口。为环网内的所有设备设置相同的域。为不同的环网设置不同的域。不属于同一环网的设备必须具有不同的域。

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

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

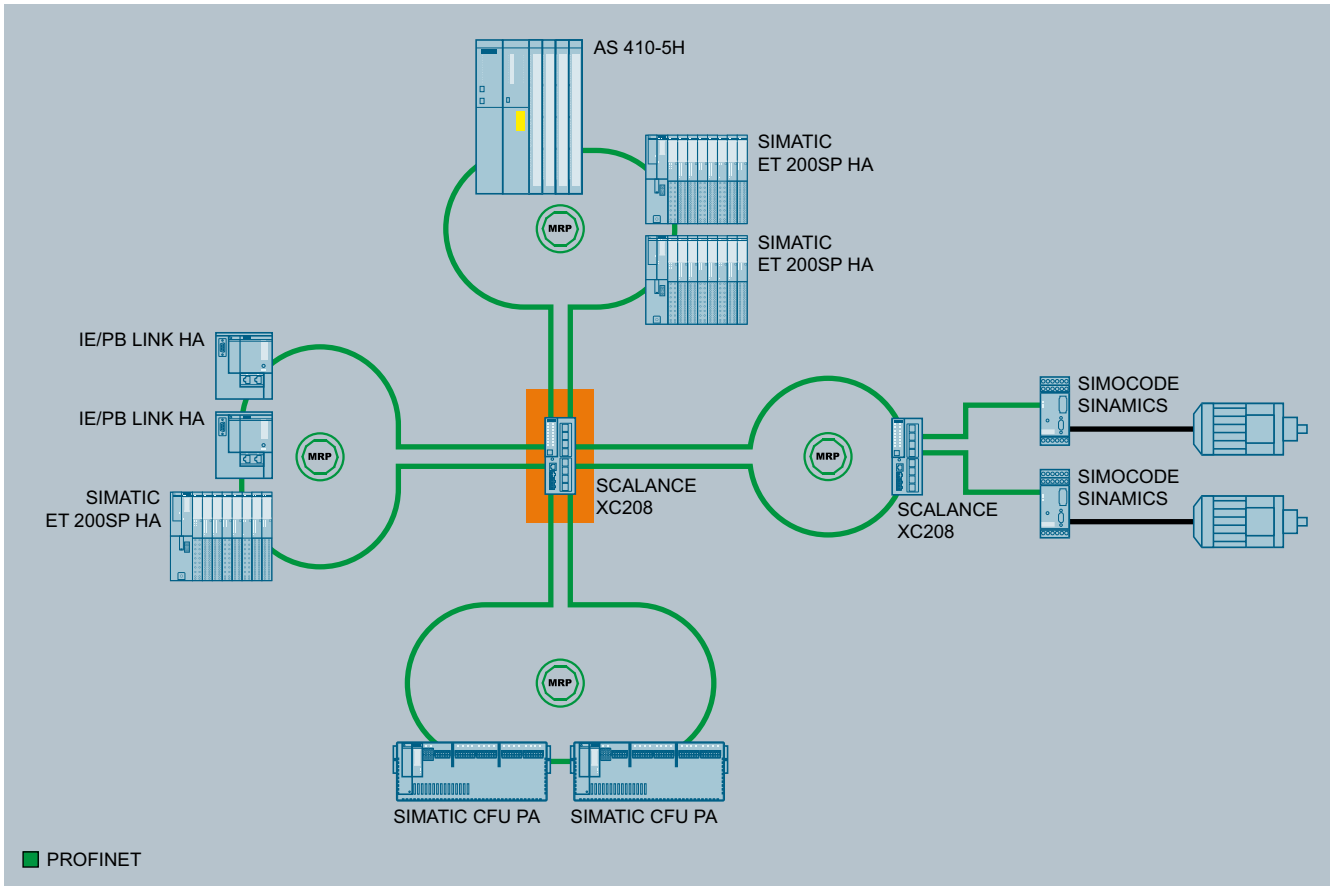


图 7-13　MRP 多环网拓扑

说明

适合 MRP 多环网的设备

可将以下产品线中的所有产品用作连接多环网的冗余管理器：

- 自固件版本 V4.0 起的 SCALANCE X-300
- 自固件版本 V4.0 起的 SCALANCE X408-2
- 自固件版本 V3.10 起的 SCALANCE X414-3E
- 自固件版本 V4.3 起的 SCALANCE XB-200
- 自固件版本 V4.3 起的 SCALANCE XC-200
- 自固件版本 V1.0 起的 SCALANCE XC-300
- 自固件版本 V4.3 起的 SCALANCE XP-200
- 自固件版本 V4.5 起的 SCALANCE XP-200G
- 自固件版本 V1.0 起的 SCALANCE XR-300
- 自固件版本 V4.3 起的 SCALANCE XR-300WG
- SCALANCE XC-400 固件版本 V1.1 及更高版本
- 自固件版本 V6.4 起的 SCALANCE XM-400
- SCALANCE XR-500 固件版本 V1.1 及更高版本
- 自固件版本 V6.4 起的 SCALANCE XR-500

说明

适合 MRP 互连的设备

可将以下产品线中的所有产品用作介质冗余互连管理器和介质冗余互连客户端：

- 自固件版本 V4.3 起的 SCALANCE XB-200
- 自固件版本 V4.2 起的 SCALANCE XC-200
- 自固件版本 V4.2 起的 SCALANCE XF-200BA
- 自固件版本 V4.4 起的 SCALANCE XF-200G
- 自固件版本 V4.2 起的 SCALANCE XP-200
- 自固件版本 V4.5 起的 SCALANCE XP-200G
- 自固件版本 V1.0 起的 SCALANCE XC-300
- 自固件版本 V1.0 起的 SCALANCE XR-300
- 自固件版本 V4.3 起的 SCALANCE XR-300WG
- SCALANCE XC-400 固件版本 V1.1 及更高版本
- 自固件版本 V6.3 起或自固件版本 V6.2 起（对于同构网络）的 SCALANCE XM-400
- 自固件版本 V6.3 起或自固件版本 V6.2 起（对于同构网络）的 SCALANCE XR-500
- SCALANCE XR-500 固件版本 V1.1 及更高版本

角色

说明

只有环网处于打开状态时才能重新组态

在重新组态环网管理器的环网端口之前，先打开环网。

请根据以下使用案例来选择角色。

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

- 希望在还包含非 Siemens 设备的环型拓扑中使用 MRP，或希望从设备接收与 MRP 状态相关的诊断中断（参见“诊断中断”）：
  – 只为环网中的一台设备分配“Manager (Auto)”或“MRP Manager”角色。
  – 对于环型拓扑中的其它设备，选择“客户端”(Client) 角色。
- 想要禁用 MRP：
  如果不想使用 MRP 来运行环型拓扑中的设备，请选择“不是环中的节点”(Not node in the ring) 选项。

说明

复位为出厂设置后的角色

在将环网中的设备复位为出厂设置之前，请先打开环网。

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

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

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

- SCALANCE XB-200（EtherNet/IP 型号）
- SCALANCE XC-200（EtherNet/IP 型号）
- SCALANCE XC-300
- SCALANCE XP-200（EtherNet/IP 型号）
- SCALANCE XR-300
- SCALANCE XR-300WG
- SCALANCE XC-400
- SCALANCE XM-400
- SCALANCE XR-500

环网端口 1/环网端口 2

请在此处将要组态的端口选作环网端口 1 和环网端口 2。

对于 8 个以上端口的设备，并不是所有端口都可以选作环网端口。

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

注意
复位为出厂设置后的环网端口 如果复位为出厂设置，也会复位环网端口设置。

说明

只有环网处于打开状态时才能重新组态

在重新组态环网管理器的环网端口之前，先打开环网。

诊断中断

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

可能生成以下诊断中断：

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

不通过 STEP7 设置冗余参数分配（冗余替代）

该选项会影响所有 SCALANCE X 交换机。如果想要使用 WBM、CLI 或 SNMP 等其它方式设置介质冗余的属性，在 STEP7 中进行组态时，请选择该选项。

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

说明

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

XR-324-12M 的特性

说明

SCALANCE XR-324-12M 的 PROFINET IO 操作

仅当插入介质模块时，才能执行 SCALANCE XR-324-12M 的 PROFINET IO 操作。“mrpdomain -1”的出厂设置指定 MRP 的端口 1 和 2，因此，需要通过在交换机上插入介质模块提供这两个端口。

⚠ 小心

STEP 7 项目中具有 XR-324-12M 时的环网端口默认值

使用 SCALANCE XR-324-12M 时，如果选择“mrpdomain 1”，则环网端口设置为 STEP 7 的 MRP 组态中的第一个组态端口。

因此，应检查组态的环网端口与连接的环网端口是否一致。

C-PLUG

8

应用

C-PLUG 是用于存储模块化交换机的组态数据的可互换介质，随产品一起提供。这意味着在更换基本设备后，组态数据仍然可用。

说明

必须在已关闭设备电源时取下或插入 C-PLUG。

工作原理

由终端设备供电。关闭电源后，C-PLUG 可永久保留所有数据。

如果插入空的 C-PLUG（出厂设置或使用“清除”功能删除数据），则在设备启动时，工业以太网交换机的所有组态数据都将自动保存到该 C-PLUG 中。如果此设备处于 *“已接受”(ACCEPTED)* 状态，则在运行期间对组态所做的更改也将保存到 C-PLUG 上，而无需任何操作员介入。

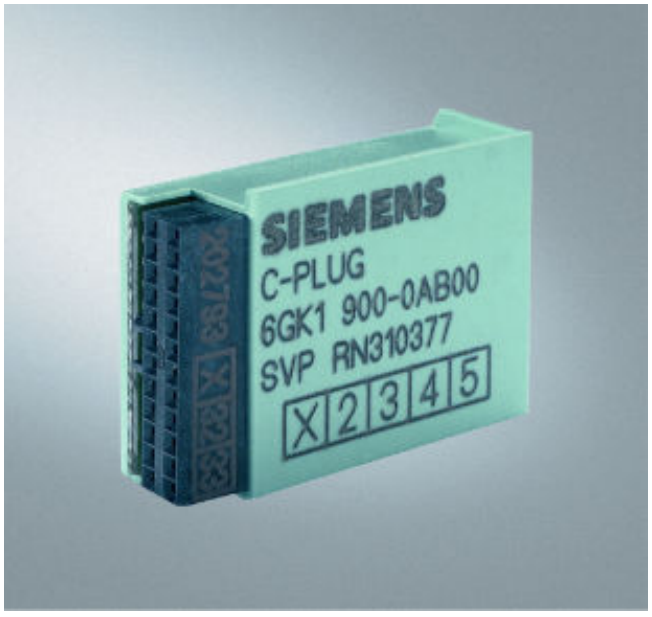


图 8-1 C-PLUG

插有“已接受”C-PLUG 的工业以太网交换机将在启动时自动使用 C-PLUG 中的组态数据。但是，仅当通过兼容设备类型写入数据时才可能接受。

说明

如果插入了 C-PLUG，所有组态更改将存储在 C-PLUG 以及设备内存中。

这允许快速而简单地更换基本设备。将 C-PLUG 从出现故障的组件中取出，并插入更换设备中。首次启动时，更换设备将具有与故障设备相同的组态（除了由供应商设置的 MAC 地址之外）。

说明

如果使用固件版本较早的设备替换带有最新版本固件和 C-PLUG 的设备，则在插入 C-PLUG 时，将不会采用当前的 C-PLUG 组态。要使用 C-PLUG 的组态，替换设备的固件版本必须不低于被更换设备的固件版本。

因此，如果有固件更新，则应该使用任何现有的替换设备。

说明

如果更换工业以太网交换机，则必须获取媒介模块的组态（使用 SCALANCE X414-3E 时还包括 DIL 开关的设置和扩展模块的可选组态）。

诊断

如果插入不包含兼容设备类型的组态数据的 C-PLUG、意外卸下 C-PLUG 或 C-PLUG 出现常规故障，该设备的诊断机制（LED、基于 WEB 的管理、SNMP 和 CLI）将发出信号。

启动特性

如果在具有相同固件版本的设备之间更换 C-PLUG，则会使用存储在 C-PLUG 上的组态启动设备。只有组态参数已更改并存储或设备由 CLI/WBM 命令重启时，设备的组态存储器才会采用 C-PLUG 组态。如果未对组态进行更改并在断电后再次拆下 C-PLUG，重启时，设备会使用未经更改的组态再次启动。

如果将固件版本较早设备的 C-PLUG 插入到固件版本较新的设备中，则在重新启动时，内部存储器将被 C-PLUG 的组态覆盖。即使在拆下 C-PLUG 后未更改组态，设备启动时也会使用 C-PLUG 中的组态。

	C-PLUG	工业以太网交换机启动时的情况
1	未找到	使用内部组态（如果存在）或出厂默认设置。
2	空	使用内部组态，并立即将此组态自动复制到 C-PLUG
3	写有自身的组态数据	使用 C-PLUG 的组态
4	写有其它的组态数据	使用第三方 C-PLUG 的组态
5	写有不同设备类型的组态数据	使用内部组态，电源模块的 LED 呈红色并记录日志条目
6	故障	使用内部组态，电源模块的 LED 呈红色并记录日志条目
7	带有更早固件版本的工业以太网交换机创建的组态数据	使用 C-PLUG 的组态

对于情况 2 和 3，交换机 CPU 中的组态数据和 C-PLUG 中的组态数据相同。

对于情况 4 和 5，组态数据不同，可手动同步。

对于情况 6，可尝试使用清除功能重新格式化 C-PLUG。如果故障仍然存在，请更换 C-PLUG。

说明

对于 SCALANCE X414-3E 的第 4 种情况（替换），将采用 C-PLUG 的 DIL 开关设置，而不会采用物理开关设置。诊断选项将发出偏差信号。

保存组态数据

如果以低于工业以太网交换机上现存版本的固件创建的 C-PLUG 启动设备，则在重启过程中设备的“内部”组态将被 C-PLUG 的组态数据覆盖。即使在拔出 C-PLUG 后，设备上也将只存在 C-PLUG 上的组态数据。

如果插入的 C-PLUG 上的组态信息由相同固件版本的工业以太网交换机创建，请注意以下几点：只有以下情况时，设备存储器才会采用 C-PLUG 中包含的组态信息：

- 通过“设定值”(Set Values) 按钮写入组态更改，或
- 运行“保存（重启）”(Save (Restart))。

如果未写入组态更改或运行“保存（重启）”(Save (Restart))，（关闭电源后）将视作未插入 C-PLUG 进行重启，组态数据仍保持为之前的内部组态数据。

说明

在“基于 Web 的管理”中输入 CLI 命令或单击“设定值”(Set Values) 按钮后的 90 秒内，非易失性设备存储区将采用组态数据的更改。

如果通过“基于 Web 的管理”中“系统重启和默认设置”(System Restart & Defaults) 菜单的“重启系统”(Restart System) 按钮或 CLI 的“重启”(restart) 命令运行重启，非易失性设备存储区也会采用组态数据的更改。

固件更新 9

9.1 通过功能性固件更新固件

9.1.1 通过 HTTP/HTTPS 更新固件

基于 Web 的管理或命令行接口

有关通过 HTTP/HTTPS 更新固件的信息，请参见“系统保存与加载 (System Save & Load) 菜单项”部分。

9.1.2 通过 TFTP 更新固件

基于 Web 的管理或命令行接口

有关通过 TFTP 更新固件的信息，请参见“系统保存与加载 (System Save & Load) 菜单项”部分。

9.1.3 通过 FTP 更新固件

通过控制台访问

如果工业以太网交换机具有 IP 地址并且与 PC 或 PG 之间存在以太网连接，则请按以下步骤更新固件：

1. 打开控制台窗口并输入命令 ftp，后接工业以太网交换机的 IP 地址。
   例如：
   ftp 192.168.20.54
2. 登录和密码可使用与 WBM 和 CLI 相同的值。
3. 输入“put”命令，后接固件文件的名称。
   例如：
   put v100031.lad
4. 加载文件之后，工业以太网交换机将关闭 FTP 连接并进行重启。

9.2 通过 IE Switch X-400/XR-300 使用引导软件更新固件

使用引导软件更新的必要性

当无法使用固件来执行更新时，就有必要使用引导软件来进行固件更新。 对于此情况，可能的原因包括固件缺陷或在闪存操作过程中发生了掉电。

注意
请勿使用引导软件 XMODEM 加载和更新 FPGA 如果使用 XMODEM，请勿使用该引导软件加载和更新 FPGA。

如何启动引导加载器模式

首先 PC 或 PG 必须与 IE Switch X 400/XR 300 的串口相连。然后按照以下步骤切换到引导加载器模式：

1. 例如，通过断开电源再重新连接来重启工业以太网交换机。
2. 在重启过程中，按下 PC 或 PG 键盘上的任意键。

如果 IE Switch X-400/XR-300 上没有功能性固件，则 IE Switch X-400/XR-300 将自动以能够与集成 FTP 服务器通信的模式启动。 这仅在 IE Switch X-400/XR-300 具有 IP 地址时才可能实现。

9.2.1 通过串口更新固件

步骤

请按以下步骤通过 IE Switch X-400/XR-300 的串口下载固件：

1. 将带有终端程序（例如 HyperTerminal）的 PC 连接到 IE Switch X-400/XR-300 的串行接口上，并启动该终端程序。 有关该主题的其它信息，请参见附录 A。
2. 复位 IE Switch X-400/XR-300。切换到显示模式 A 或显示模式 D（如果超过一分钟没有按 SET/SEL 按钮，设备将自动切换到显示模式 A）。 按住 SET/SEL 按钮 12 秒以上。 在启动过程中按下任意键可停止引导加载器。 HyperTerminal 将显示以下信息：

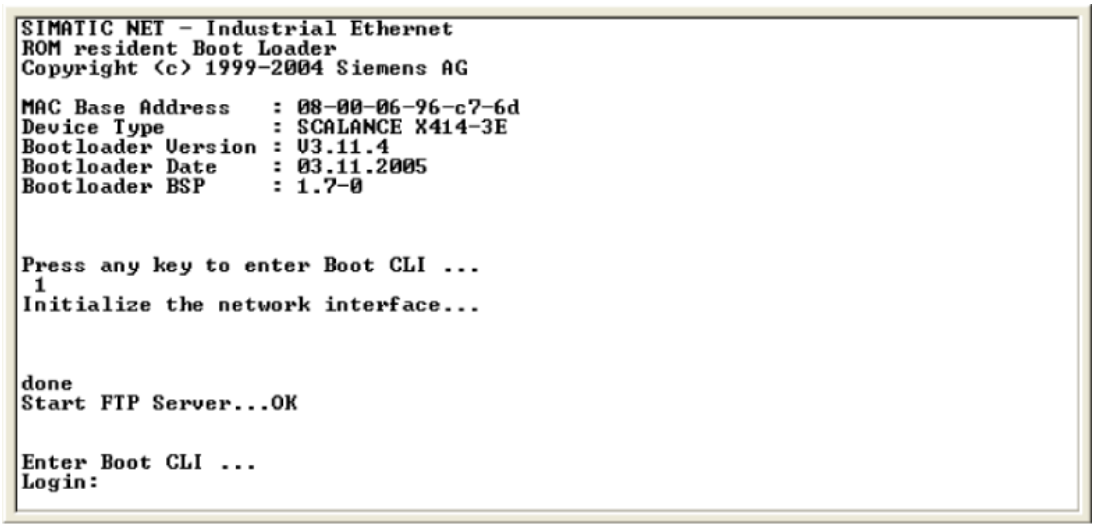


图 9-1 HyperTerminal

3. 利用以下信息登录引导加载器的命令行接口：
   Login（登录）： siemens
   Password（密码）： siemens
4. 输入 ldimage 命令。 Hyperterminal 将显示以下信息：
   XMODEM .... waiting for file（正在等待文件）
   ATTENTION: do not switch off till the COMPLETED or FAILED message appears
   ... CCCCCCC（注意：在出现“完成”或“失败”消息之前，请不要关闭 ... CCCCCCC）

5. 选择“传输 > 发送文件”(Transfer > Send File) 菜单命令。 HyperTerminal 将打开以下对话框：

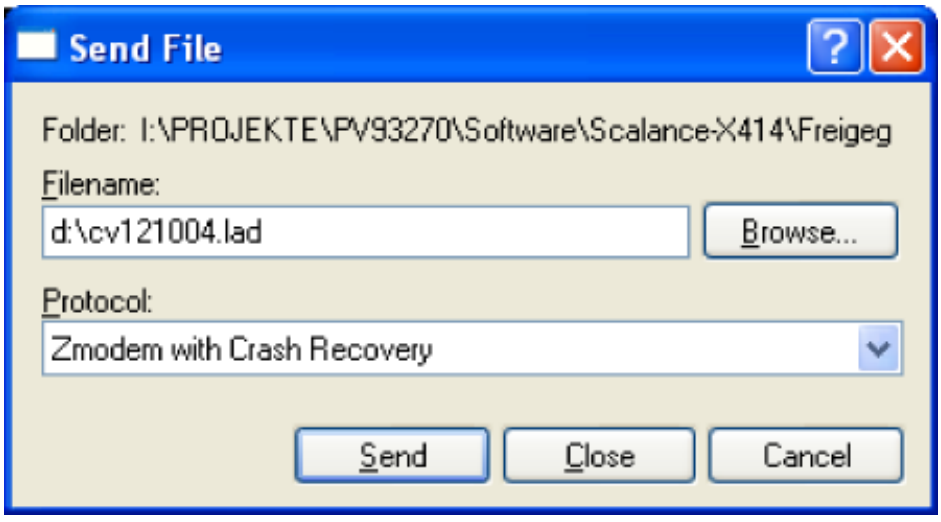


图 9-2 “发送文件”(Send File) 对话框

6. 输入待加载文件的名称并选择 Xmodem 作为协议。 单击“发送”(Send) 开始上传。 随即将打开显示上传进度的对话框：

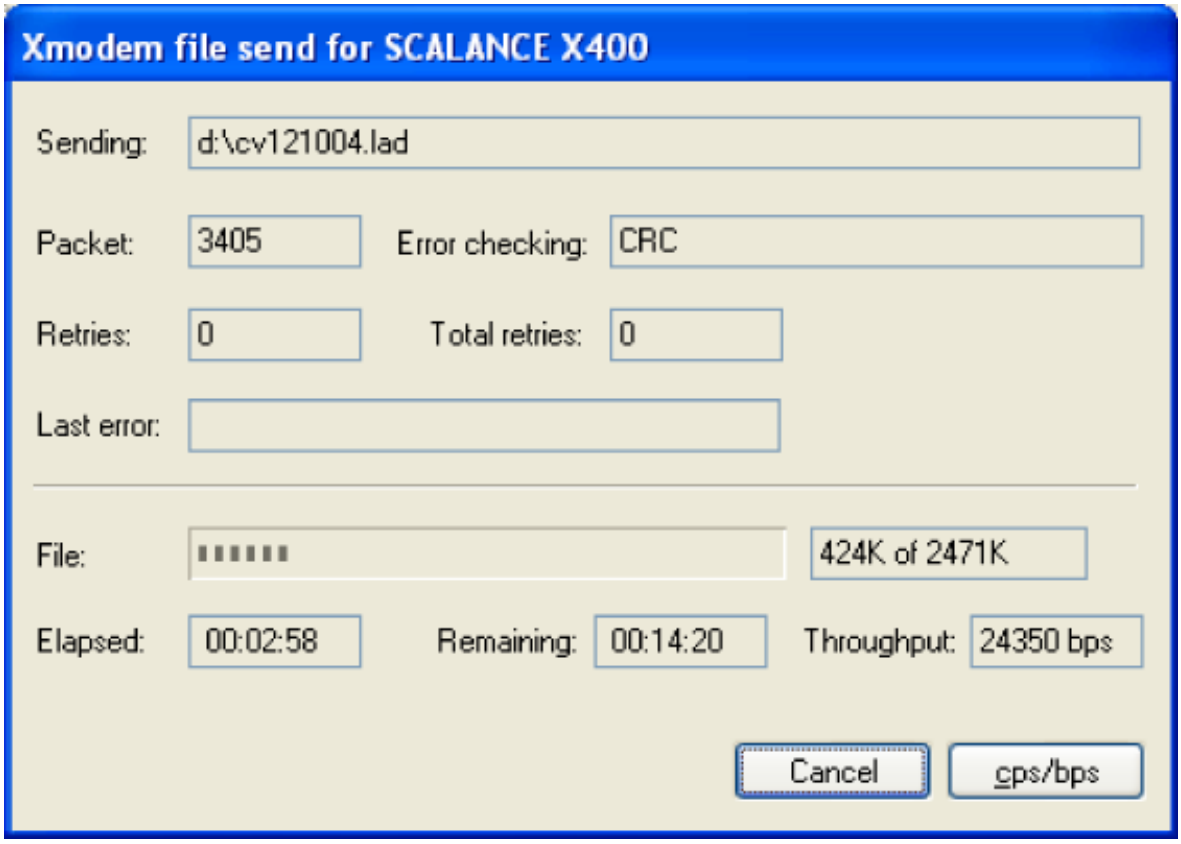


图 9-3　通过 Xmodem 发送文件

7. 上传完成后，HyperTerminal 将显示以下信息：

   FlashWrite .....COMPLETED（闪存写入 .....已完成）

   Restart the device.（重启设备。）

说明

在上传过程中，请勿中断 PC 与 IE Switch X-400/XR-300 之间的连接或关闭 IE Switch X-400/XR-300 的电源。

如果上传因受信号线上的故障影响而中断，则设备将在下一次启动时以旧固件进行引导。您将需要重新上传固件。

如果由于掉电而未能将固件完全存储到 IE Switch X-400/XR-300 中，则在引导后将显示消息“Can't load image from flash -> wrong crc”（无法加载闪存中的图像 -> 错误 CRC）。同样，您还需再次上传固件。

9.2.2 通过以太网端口和 FTP 更新固件

步骤

如果工业以太网交换机的引导功能具有 IP 地址并且与 PC 或 PG 之间存在以太网连接，则请按以下步骤更新固件：

说明

如果设备处于引导加载器模式，则必须通过设备的端口 1 建立以太网连接。

1. 打开控制台窗口并输入命令 ftp，后接工业以太网交换机的 IP 地址。例如：
   ftp 192.168.20.54
2. 登录名和密码均输入 *siemens*。
3. 输入命令 put 并后接固件文件的名称。例如：
   put V211005.lad
4. 加载文件之后，工业以太网交换机将关闭 FTP 连接并进行重启。请确保一直等到自动重启完成。

9.3 固件降级

自固件版本 V3.9.0 到固件版本 V4.0.2 的情况

自从固件版本 V3.9.0 开始，如果交付设备的固件更旧，则可以降级固件。

注意
固件降级后复位出厂设置 如果加载的固件比设备上的固件版本更早，则加载固件后必须将设备复位为出厂默认设置（“复位为出厂默认设置”(Reset to Factory Defaults)）。 使用 SET/SELECT 按钮将设备复位为出厂设置。固件降级后，对于指定的固件版本，无法通过 WBM 菜单“系统 > 重启并恢复默认设置”(System > Restart & Defaults) 复位为出厂设置。 复位设备前，组态如果不一致，则决不能将其保存或传送到另一个设备中。

自固件版本 V4.0.3 开始的情况

自固件版本 V4.0.3 起，可检测到版本高于 V4.0.3 的固件版本的固件降级。示例：从 V4.0.4 降级至 V4.0.3。固件降级后，设备将自动复位为出厂设置（“复位为出厂默认设置”(Reset to Factory Defaults)）。

附录 A

A

A.1 SCALANCE X400 串口处的 PC 连接

HyperTerminal

Windows 95/98/NT/2000/XP 操作系统都具有 HyperTerminal 程序，位置在“开始 > 所有程序 > 附件”(Start > Programs > Accessories) 菜单中。 可使用此程序完成以下任务：

- 通过 IE Switch X-400 的串口下载固件。
- 通过命令行接口输入命令

步骤

请按以下步骤将 PC 连接到 IE Switch X-400：

1. 使用市场上提供的空调制解调器电缆将 PC 的串口与 IE Switch X-400 的串口连接起来。
2. 在 HyperTerminal 程序中选择“文件 > 新建连接”(File > New Connection) 菜单命令。 将打开新建连接的“属性”(Properties) 窗口。
3. 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
   协议： 无

X-400 针脚分配（空调制解调器电缆）

为连接 PC，空调制解调器电缆的一端应具有 9 针或 24 针 D 型母连接器，另一端应具有 9 针 D 型母连接器。 下表列出了两种电缆的针脚分配情况：

	PC 连接器			SCALANCE X-400 连接器
信号名称	25 针插口 针	9 针插口 针	已连接至	9 针插口 针
TD（传输数据）	2	3		3
RD（接收数据）	3	2		2
RTS（请求发送）	4	7		7
CTS（清除发送）	5	8		8
SG（信号地）	7	5		5
DSR（数据集准备就绪）	6	6		6
DTR（数据终端准备就绪）	20	4		4

图 A-1　针脚分配表

说明

使用 SIMATIC 编程设备时，串口可能为 25 针母连接器。 在这种情况下，应使用市场上提供的对接转换器（两端均为 25 针插头）。

A.2　SCALANCE X300 串口处的 PC 连接

HyperTerminal

Windows 95/98/NT/2000/XP 操作系统都具有 HyperTerminal 程序，位置在“开始 > 所有程序 > 附件”(Start > Programs > Accessories) 菜单中。可使用此程序完成以下任务：

- 通过 IE Switch XR-300 的串口下载固件。
- 通过命令行接口输入命令

步骤

请按以下步骤将 PC 连接到 IE Switch XR-300：

1. 使用为诊断端口提供的连接电缆将 PC 的串口与 IE Switch XR-300 的串口连接起来。
2. 在 HyperTerminal 程序中选择“文件 > 新建连接”(File > New Connection) 菜单命令。 将打开新建连接的“属性”(Properties) 窗口。
3. 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
   协议： 无

XR-300（诊断端口的连接电缆）的针脚分配

说明

对于机架设备 (R)，诊断端口的连接电缆随产品一起提供。

诊断端口的连接电缆一端是用于连接 PC 的 9 针 D-sub 母连接器，电缆另一端是 RJ-11 插头。下表列出了针脚分配。

RJ-11 插头		**D 型（9 针，母）**	
针脚编号	**分配**	**针脚编号**	**分配**
1	n.c.	1	n.c.
2	n.c.	2	RD（接收数据）
3	TD（发送数据）	3	TD（发送数据）
4	SG（信号地）	4	n.c.
5	RD（接收数据）	5	SG（信号地）
6	n.c.	6	n.c.
		7	n.c.
		8	n.c.
		9	n.c.

附录 B

B

B.1 SCALANCE X300/X400 的 MIB 变量

MIB II 标准中的重要变量

下面是 MIB II 中一些用于监视设备状态的 SNMP 变量的列表。MIB II 介绍了通常任何 SNMP 兼容设备都支持的所有 SNMP 变量。

“系统”(System) 目录中的变量

表格 B-1 “系统”(System) 目录中的变量

变量	访问权限	说明
sysDescr	只读	字符串，至多使用 256 个字符。 此值包含供应商特定的设备 ID。
sysObjectID	只读	这是用于访问具体设备 SNMP 变量的地址（对象标识符）： **1.3.6.1.4.1.4196.1.1.5.4** 如果未声明任何专有 OID，则对象标识符为 [0,0]。此处，默认值为 0。
sysUpTime	只读	最近一次复位后经过的时间（例如，上电后）。该值以百分之一秒为单位显示。
sysContact	读取和写入	可在此处输入一个联系人。（默认值：空字符串）。 可能的值：最长 255 个字符的字符串。
sysName	读取和写入	可在此出输入设备的名称。（默认值：空字符串） 可能的值：最长 255 个字符的字符串。

变量	访问权限	说明
sysLocation	读取和写入	可在此处输入设备的位置（默认值：空字符串）。 可能的值：最长 255 个字符的字符串。
sysService	只读	根据 ISO/OSI 模型显示组件提供的功能（服务）。 层级功能： • 物理（例如，中继器） • 数据链路/子网（例如，网桥、交换机） • Internet（例如，IP 网关，路由器） • 端到端（例如，IP 主机） • 应用（例如，电子邮件服务器） 数据类型：32 位整型。

“接口”(Interface) 目录中的变量

表格 B-2 “接口”(Interface) 目录中的变量

变量	访问权限	说明
ifNumber	只读	组件中各种可用接口的数量。 使用 SCALANCE X414-3E 时，此变量的输出值为 68（26 个物理端口，42 内部（虚拟）端口）。 使用 SCALANCE X408-2 时，此变量的输出为值 17（8 个物理端口，9 个内部（虚拟）端口）。 使用 SCALANCE X-300 时，此变量的输出为值 21（10 个物理端口，11 个内部（虚拟）端口）。 数据类型：32 位整型
ifDescr	只读	端口的说明，也可能包含该端口的其它相关信息。 可能的值：最长 255 个字符的字符串。
ifType	只读	对于工业以太网交换机，输入的值为 ethernet-csmacd(6)、gigabitEthernet(117) 或 fastEther(62)。 数据类型：整型

变量	访问权限	说明
ifSpeed	只读	以每秒位数为单位的以太网端口数据传输速率。对于工业以太网交换机，可能显示 10 Mbps、100 Mbps 或 1000 Mbps。 数据类型：仪表。
ifOperStatus	只读	以太网端口当前的工作状态。可能的值包括： • up(1) • down(2) • testing(3) • unknown(4) • dormant(5) [等待外部操作] • notPresent(6) • lowerLayerDown(7) testing(3) 状态表示未传送任何用户数据。 数据类型：整型
ifLastChange	只读	所选端口在当前状态下的工作时长。该值以百分之一秒为单位显示。 数据类型：时间分段信号
ifInErrors	只读	已收数据包中由于错误而未能转发到较高协议层级的数据包数。 数据类型：计数器
ifOutErrors	只读	由于错误而未能发送的数据包数。 数据类型：计数器

端口索引

对于 SNMP，无法用“插槽.端口”的形式指定端口标识符。SNMP 使用接口索引对端口进行寻址。要通过 SNMP 更改端口的设置，请使用 AG 索引。利用 CLI 或 WBM 所做的更改仅在 AG 接口上可通过 SNMP 查看。如果使用陷阱，请注意：由于架构原因，AP 接口是通过 SNMP 绑定来指定的（例如接通陷阱）。下表显示了为端口分配接口索引的方式。

SCALANCE X-300、X408-2 和 X414-3E 的端口表

- 端口表示例（适用于 SCALANCE X-300/X408-2/X-414-3E）：
  “ifOperStatus.51380225”变量决定工业以太网交换机端口 1 的工作状态（接通、断开等）。

说明

可用端口数取决于设备版本

端口是否可用取决于设备版本，例如，对于设备 X 306-1LD FE，仅有 7 个端口可用。

表格 B-3　SCALANCE X-300 端口表

接口索引 AG/AP	端口	端口名称							
		X306-1LD FE	X307-3、X307-3LD、X308-2、X308-2LD、X308-2LH、X308-2LH+、X310、X310FE	X302-7 EEC、X307-2 EEC	X308-2M	X320-1 FE	X320-3LD FE	XR324-4M	XR324-12M
34603009/513802825	端口 1	1	1	1	1	1	1	1	1.1
34603010/513802826	端口 2	2	2	2	2	2	2	2	1.2
34603011/513802827	端口 3	3	3	3	3	3	3	3	2.1
34603012/513802828	端口 4	4	4	4	4	4	4	4	2.2
34603013/513802829	端口 5	5	5	5	5/1.1	5	5	5	3.1

接口索引 AG/AP	端口	端口名称							
		X306-1LD FE	X307-3、X307-3LD、X308-2、X308-2LD、X308-2LH、X308-2LH+、X310、X310FE	X302-7 EEC、X307-2 EEC	X308-2M	X320-1 FE	X320-3LD FE	XR324-4M	XR324-12M
34603014/51380230	端口 6	6	6	6	6/1.2	6	6	6	3.2
34603015/51380231	端口 7	7	7	7	7/2.1	7	7	7	4.1
34603016/51380232	端口 8	-	8	8	8/2.2	8	8	8	4.2
34603017/51380233	端口 9	-	9	9	-	9	9	9	5.1
34603018/51380234	端口 10	-	10	-	-	10	10	10	5.2
34603019/51380235	端口 11	-	-	-	-	11	11	11	6.1
34603020/51380236	端口 12	-	-	-	-	12	12	12	6.2
34603021/51380237	端口 13	-	-	-	-	13	13	13	7.1

接口索引 AG/AP	端口	端口名称							
		X306-1LD FE	X307-3、X307-3LD、X308-2、X308-2LD、X308-2LH、X308-2LH+、X310、X310FE	X302-7 EEC、X307-2 EEC	X308-2M	X320-1 FE	X320-3LD FE	XR324-4M	XR324-12M
34603022/51380238	端口 14	-	-	-	-	14	14	14	7.2
34603023/51380239	端口 15	-	-	-	-	15	15	15	8.1
34603024/51380240	端口 16	-	-	-	-	16	16	16	8.2
34603025/51380241	端口 17	-	-	-	-	17	17	1.1	9.1
34603026/51380242	端口 18	-	-	-	-	18	18	1.2	9.2
34603027/51380243	端口 19	-	-	-	-	19	19	2.1	10.1
34603028/51380244	端口 20	-	-	-	-	20	20	2.2	10.2
34603029/51380245	端口 21	-	-	-	-	21	21	3.1	11.1

接口 索引 AG/AP	端口	端口名称							
		X306-1LD FE	X307-3、X307-3LD、X308-2、X308-2LD、X308-2LH、X308-2LH+、X310、X310FE	X302-7 EEC、X307-2 EEC	X308-2M	X320-1 FE	X320-3LD FE	XR324-4M	XR324-12M
34603030/51380246	端口 22	-	-	-	-	-	22	3.2	11.2
34603031/51380247	端口 23	-	-	-	-	-	23	4.1	12.1
34603032/51380248	端口 24	-	-	-	-	-	-	4.2	12.2

表格 B-4　SCALANCE X408-2 和 X414-3E 的端口表

接口 索引 AG/AP	端口	端口名称			
		X408-2	X414-3E		
			无扩展器	带有电扩展器	带有光扩展器
34603009/51380225	端口 1	5.1	5.1	5.1	5.1
34603010/51380226	端口 2	5.2	5.2	5.2	5.2
34603011/51380227	端口 3	6.1	6.1	6.1	6.1

接口 索引 AG/AP	端口	端口名称			
		X408-2	X414-3E		
			无扩展器	带有电扩展器	带有光扩展器
34603012/51380228	端口 4	6.2	6.2	6.2	6.2
34603013/51380229	端口 5	8.1	7.1	7.1	7.1
34603014/51380230	端口 6	8.2	7.2	7.2	7.2
34603015/51380231	端口 7	8.3	9.1	9.1	9.1
34603016/51380232	端口 8	8.4	9.2	9.2	9.2
34603017/51380233	端口 9	-	9.3	9.3	9.3
34603018/51380234	端口 10	-	9.4	9.4	9.4
34603019/51380235	端口 11	-	10.1	10.1	10.1
34603020/51380236	端口 12	-	10.2	10.2	10.2
34603021/51380237	端口 13	-	10.3	10.3	10.3
34603022/51380238	端口 14	-	10.4	10.4	10.4
34603023/51380239	端口 15	-	11.1	11.1	11.1
34603024/51380240	端口 16	-	11.2	11.2	11.2
34603025/51380241	端口 17	-	11.3	11.3	11.3
34603026/51380242	端口 18	-	11.4	11.4	11.4
34603027/51380243	端口 19	-	-	12.1	12.1

接口 索引 AG/AP	端口	端口名称			
		X408-2	X414-3E		
			无扩展器	带有电扩展器	带有光扩展器
34603028/51380244	端口 20	-	-	12.2	12.2
34603029/51380245	端口 21	-	-	12.3	13.1
34603030/51380246	端口 22	-	-	12.4	13.2
34603031/51380247	端口 23	-	-	13.1	14.1
34603032/51380248	端口 24	-	-	13.2	14.2
34603033/51380249	端口 25	-	-	13.3	15.1
34603034/51380250	端口 26	-	-	13.4	15.2

工业以太网交换机的重要专有 MIB 变量

OID

工业以太网交换机的专有 MIB 变量具有以下对象标识符：

iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).ad(4196).adProductMibs(1).siematicNet(1).iScalanceX(5).iScalanceX300X400(4)

表格 B-5　工业以太网交换机的专有 MIB 变量

变量	访问权限	说明
snX300X400FaultState	只读	显示信号触点的状态。可能值： • 1 没有错误 • 2 有错误 数据类型：整型
snX300X400ReportFaultIndex	只读	将根据发生的顺序按升序为错误指定索引。该 4 字节变量可指定索引。
snX300X400ReportFaultState	只读	包含属于索引的错误消息。
snX300X400RmMode	只读	冗余管理器模式： • 工业以太网交换机是冗余管理器。 • 工业以太网交换机不是冗余管理器。
snX300X400RmState	只读	指示冗余管理器处于激活状态或未激活状态。 可能值： • 冗余管理器处于未激活状态。工业以太网交换机充当冗余管理器，并已打开环网；即：与之相连的交换机线路处于无故障运行中。冗余管理器模式被禁用时，也会显示“未激活”(Passive) 状态。 • 冗余管理器处于激活状态。工业以太网交换机充当冗余管理器，并已关闭环网；即：与之相连的交换机线路已中断（故障）。冗余管理器在环网端口之间切换连接，从而恢复总线的功能。 数据类型：整型
snX300X400RmStateChanges	只读	指示冗余管理器切换到“激活”(active) 状态的频率。 数据类型：计数器
snX300X400StandbyMode	只读	备用功能模式： • 备用功能启用。 • 备用功能禁用。

变量	访问权限	说明
snX300X400StandbyState	只读	显示备用状态： • 1 设备为主设备且未激活 • 3 设备为从设备且未激活 • 5 设备为主设备且已激活 • 7 设备为从设备且已激活 • 257 设备正在寻找备用连接的伙伴 • 300 备用功能已禁用 • 数据类型：整型
snX300X400StandbyStateChanges	只读	指示激活备用状态的频率。 数据类型：计数器
snBootStrapVersion	只读	引导加载器的固件版本，格式为*主.次*。
snHwVersion	只读	系统的硬件版本，格式为*主.次*。
snSwVersion	只读	系统的软件版本。
snInfoSerialNr	只读	产品的序列号。
snMacAddressBase	只读	工业以太网交换机的基本 MAC 地址。
snX300X400ModuleIdentMLFB	只读	模块的 MLFB 号。
snX300X400PowerSupply1State	只读	电源输入 1 的状态。
snX300X400PowerSupply2State	只读	电源输入 2 的状态。
snX300X400ReportDigitalInState	只读	数字量输入的状态。(SCALANCE X414-3E)

附录 C

C

C.1 标记帧

用四个字节扩展以太网帧

对于功能 CoS（Class of Service，服务类别，即帧优先级）和基于端口的 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 标记使允许的以太网帧总长度从 1518 字节增加到 1522 字节。 必须检查网络上的终端节点能否处理这样的长度/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 个字节在数据包的文件头中，位于源地址和以太网类型/长度字段之间：

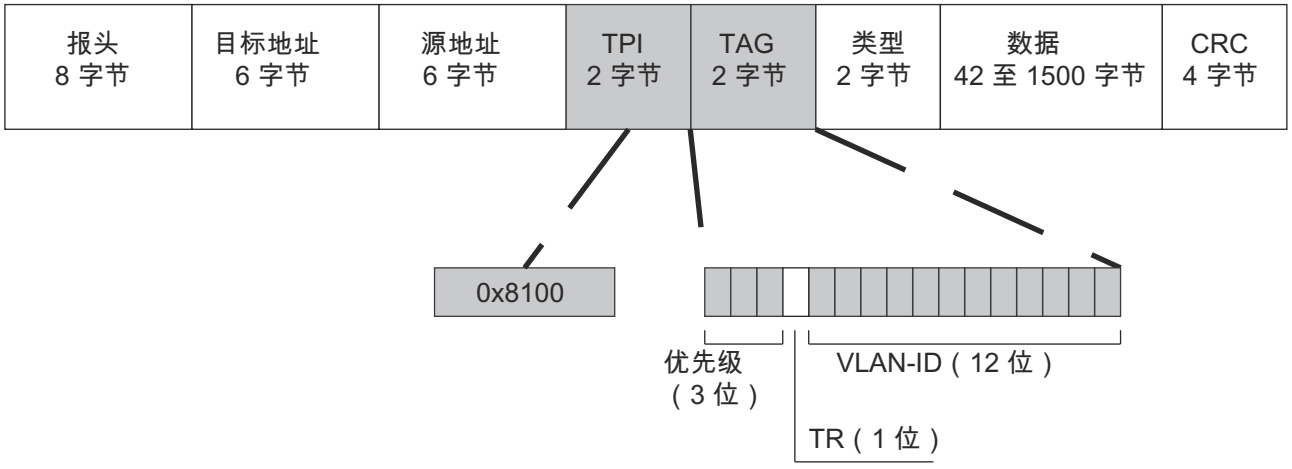


图 C-1 标记帧的结构

附加字节中包含标记协议标识符字段和标记控制信息字段。

标记协议标识符字段

前两个字节组成标记协议标识符字段 (TPI, **T**ag **P**rotocol **I**dentifier) 并始终包含值 0x8100。 此值指定该数据包包含 VLAN 信息或优先级信息。

标记控制信息字段

2 个字节的标记控制信息字段 (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 (CoS, **C**lass **o**f **S**ervice)。 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。

工业以太网交换机具有四个并行队列，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

TR 位被用作令牌环网封装过程的标识符。

VLAN–ID

利用余下的 12 个位，可形成最多 4095 个 VLAN-ID（不允许使用 VLAN ID 4095）。 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。

附录 D

D

D.1 SCALANCE X300/X400 的错误消息

说明

如果激活链路汇聚，还可以指定汇聚号（例如 AG1）来代替端口号。

发送错误时的消息以及接下来的错误消除

表格 D-1 分配至错误状态的错误消息（错误 LED）

出错时的消息	问题消除后的消息
<端口号> 的链路中断。	<端口号> 的链路接通。
<端口号> 发生不可恢复的环网错误。	<端口号> 的环网错误已消失。
检测到其它冗余管理器... <端口号> 上的 MAC <MAC 地址>。	其它冗余管理器已消失... <端口号> 上的 MAC <MAC 地址>。
<HRP> 环网管理器已激活。	<HRP> 环网管理器回退为客户端。
<HRP> 环网管理器进入主动状态。	<HRP> 环网管理器回退为被动状态。
备用设备进入主动状态。	备用设备进入被动状态。
备用设备正在等待 <主设备 | 从设备>。	备用设备已连接至 <端口号> 上的 <主设备 | 从设备> <MAC 地址>。
备用 <伙伴 | 观察器> 失去与 <端口号> 上的 <主设备 | 从设备> <MAC 地址> 的连接。	备用 <伙伴 | 观察器> 已重新与 <端口号> 上的 <主设备 | 从设备> <MAC 地址> 连接。
检测到备用协议不支持的版本 <版本号>。	备用协议不支持的版本 <版本号> 已消失。
检测到另一个观察器。 <端口号> 上的 <MAC 地址>。	另一个观察器已消失。 <端口号> 上的 <MAC 地址>。
观察器：RM 在隔离端口上切换帧。	观察器：RM 停止在独立端口上切换。
观察器 <端口号> 上收到意外的通信。	观察器 <端口号> 上的意外通信已消失。
观察器：RM 发出“被动”信号时端口 <端口号> 上检测到测试帧超时。	观察器：端口 <端口号> 上的测试帧超时已消失。
观察器：RM 发出激活信号，但在两个环网端口上均收到 RM 测试帧。	观察器：RM 发信号提示正确的状态。

出错时的消息	问题消除后的消息
观察器：RM 运行不兼容的软件版本 <版本号>。	观察器：RM 的不兼容软件版本 <版本号> 已消失。
观察器：两个环网端口上均发生 RM 测试帧超时。	观察器：收到 RM 测试帧。
观察器由于重复发生的错误过多（<错误数>）而停止恢复。 （需要手动重启 (WBM/CLI) 观察器）。	观察器由于用户命令而重新启动。
线路 <电源 ID> 断电。	线路 <电源 ID> 通电。
内部错误：<电压> V 断电。	内部错误消失：<电压> V 通电。
插槽 <插槽编号> 上的错误模块 <模块名称>（ID：模块 ID）。	插槽 <插槽号> 上的错误模块 <模块名称> 已删除。
不接受 C-PLUG。有关详细信息，请参见系统 C-PLUG 屏蔽。	C-PLUG 已接受。
C-PLUG 接口已卸载。需要重新启动。	C-PLUG 接口已挂载。
C-PLUG 缺失。	检测到 C-PLUG。
缺少环网 <端口号> 的介质模块。	检测到环网 <端口号> 的介质模块。
DIP 交换机 <交换机名称> 发生变化。需要重新启动。	DIP 交换机 <交换机名称> 已设置回原始状态。
DIP 交换机 <交换机名称> 与 C-PLUG 不同。需要重新启动。	DIP 交换机 <交换机名称> 已设置回 C-PLUG 上保存的状态。
发生内部错误和/或异常。	已确认内部错误和/或异常。
设备启动未完成。	设备启动已完成。
RM <MAC 地址> 丢失。	检测到 RM <MAC 地址>。
缺少备用 <端口号> 的介质模块。	检测到备用 <端口号> 的介质模块。
PNIO 故障 - 请使用 STEP 7 进行诊断。	PNIO 故障 - 消失。
PNIO 连接已建立。	PNIO 连接已终止。
检测到重大的模块更改。需要重新启动。	重大的模块更改已恢复。
DIP 开关设置已调整... → 下一次重新启动后将启动冗余。	DIP 开关设置复位... → 下一次重新启动后不会更改冗余模式。
<端口号> 上的验证状态：失败！原因：%s。	<端口号> 上的验证状态：OK。原因：%s。
备用 <观察器 | 伙伴> 冻结当前状态 <主动 | 被动>，因为 <主设备 | 从设备> <MAC 地址> 已消失。	取消冻结备用设备的状态 <主动 | 被动>，因为伙伴 <MAC 地址> 变为可见。

出错时的消息	问题消除后的消息
默认路由存储在硬件中。	默认路由不再存储在硬件中。
环网 %u 中不可恢复的错误：RM 仅从一个环网端口接收测试帧。	环网 %u 中不可恢复的错误消失：RM 同时从两个环网端口接收测试帧。
环网 %u 中不可恢复的错误：检测到另一个冗余管理器。	环网 %u 中不可恢复的错误消失：其它冗余管理器已消失。
环网 %d 中最后一个 MRP 管理器无法在环网端口 <端口号> 和 <端口号> 上停止（存在网络环路危险）。	MRP 环网 %d 管理器现在可以停止（不再存在网络环路危险）。
冗余模式转换未完成！\n 是：\"%s\"，应为：\"%s\"。	到 \"%s\" 的冗余模式转换完成。
<端口号> 上连接了错误的环网线路（应该在 <端口号> 上连接）。	<端口号> 上错误连接的环网线路已删除。
超过主电源使用量阈值。	主电源使用量再次低于阈值。
出现意外的端口组件。将设备名称更改为 %s。	端口组件已知。
<端口号> 上未知的 SFP 模块（供应商：\"%$str\"）。	<端口号> 上未知的 SFP 模块已删除。
<端口号> 上的 SFP 模块不受支持且保持禁用。	<端口号> 上不受支持的 SFP 模块已删除。
信号触点由用户组态控制。	信号触点由错误状态控制。
<端口号> 上检测到本地环路。端口已禁用。	<端口号> 因环路检测而被禁用后再次启用。
<端口号> 上检测到本地环路。端口禁用 <秒数> 秒。	<端口号> 因环路检测而被禁用后再次启用。
<端口号> 上检测到远程环路。端口已禁用。	<端口号> 因环路检测而被禁用后再次启用。
<端口号> 上检测到远程环路。端口禁用 <秒数> 秒。	<端口号> 因环路检测而被禁用后再次启用。
<端口号> 上检测到本地环路。	再次启用 <端口号> 以进行环路检测。
<端口号> 上检测到远程环路。	再次启用 <端口号> 以进行环路检测。
备用 <伙伴 | 观察器> 与 <主动 | 被动> 状态相冲突。	备用 <伙伴 | 观察器> 的状态冲突已解决。
备用 <伙伴 | 观察器> 与观察器 <开 | 关> 组态发生冲突。	备用 <伙伴 | 观察器> 观察器组态冲突已解决。
备用 <伙伴 | 观察器> 与 <主设备 | 从设备> 角色相冲突。	备用 <伙伴 | 观察器> 的角色冲突已解决。
备用从设备：至少有一个端口没有建立连接。	备用从设备：所有端口均已建立连接。

出错时的消息	问题消除后的消息
FMP 端口 <端口号>：需要维护，Rx-Power：<接收功率> [dBm]，功耗：<功耗> [dB]	FMP 端口 <端口号>：OK
FMP 端口 <端口号>：要求维护，Rx-Power：<接收功率> [dBm]，功耗：<功耗> [dB]	FMP 端口 <端口号>：OK
POF 端口 <端口号>：需要维护，接收功率：<接收功率> [dBm]，功率裕量：<功率裕量> [dB]	POF 端口 <端口号>：OK
POF 端口 <端口号>：要求维护，Rx-Power：<接收功率> [dBm]，剩余功率：<power margin> [dB]	POF 端口 <端口号>：OK
链路检查：<故障描述> 指示 <端口号> 上的链路中断。端口已禁用。	链路检查：<端口号> 上的链路正常。启用的端口。
链路检查：<端口号> 上检测到多个伙伴。	链路检查：<端口号> 上的伙伴检测复位。
链路检查：未批准组态<端口号> 上禁用链路检查。	链路检查：<端口号> 上的未批准组态已解决。

用于通知所发生事件的消息

下列消息提供了不与错误状态（错误 LED）直接相关的事件信息：

- 用户输入：<用户输入>
- 收到 <协议名称> 协议的未知命令 <命令>。
- 设备组态为环网 <关闭 | ARD | HRP 客户端 | MRP 客户端 | HRP 管理器 | MRP 管理器>。
- 备用功能 <主设备 | 从设备>。
- 观察器已启动。
- 观察器已停止。
- 观察器相关的冗余管理器 <MAC 地址>。
- 备用设备正在等待 <伙伴 | 观察器>。
- 备用 <伙伴 | 观察器> 已连接至 <主设备 | 从设备> <MAC 地址> <端口号>。
- 备用 <伙伴 | 观察器> 失去与 <主设备 | 从设备> <MAC 地址> <端口号> 的连接。
- 端口 <端口号> 是独立环网端口。
- 端口 <端口号> 是静态环网端口。

- 没有与邮件服务器的 SMTP 连接。
  服务器 IP 地址 <IP 地址> TCP 端口 <TCP 端口号>。
- 找不到 SMTP 应用程序。
  服务器 IP 地址 <IP 地址> TCP 端口 <TCP 端口号>。
- SMTP（电子邮件）连接已中止。服务器 IP 地址 <IP 地址>。
- 无法将消息发送至 syslog 服务器。请检查 syslog 套接字配置。
- 已连接到 syslog 服务器。
- SNMP：验证失败。
- (R)STP：检测到新的根网桥。
- (R)STP：检测到拓扑变化。
- 无法发送电子邮件。请检查 IP 组态。
- 无法发送陷阱。请检查 IP 组态。
- SMTP 服务器的应答失败代码 <错误代码>。
- 已请求重新启动。
- 未找到 C-PLUG。已使用内部闪存。
- 找到空 C-PLUG。
- C-PLUG 格式请求。
- 找到已填充的 C-PLUG。
- 找到损坏的 C-PLUG。
- C-PLUG 已在运行时移除。
- C-PLUG 已在运行时插入。
- 发生 RMON 增加报警。
- 发生 RMON 降低报警。
- 环网冗余已启用。
- 环网冗余已禁用。
- (R)STP 协议已启用。
- (R)STP 协议已禁用。
- (R)STP 已禁用，因为启用了环网冗余。

- DIP 设置取自 C-PLUG。
  RM=<ON|OFF>，STBY=<ON|OFF>，R1=<ON|OFF>，R2=<ON|OFF>
- (R)STP 关闭时检测到 (R)STP 拓扑变化。老化时间减少至 <时间 (s)>（在至少 <时间 (s)> 秒内完成）。
- 将老化时间设置回原始值 <时间 (s)> 秒。
- 没有与 SNTP 服务器的连接。服务器 IP 地址 <IP 地址>。
- 已连接到 SNTP 服务器。服务器 IP 地址 <IP 地址>。
- 在环网端口上启用了链路状态监视。
- 已将环网端口的 VLAN ID 更改为 1。
- GVRP 已禁用，因为启用了环网冗余。
- GMRP 已禁用，因为启用了环网冗余。
- 已禁用镜像，因为监视端口是环网端口。
- 已（重新）启用环网端口（由于被用户禁用）。
- 已禁用环网端口上的端口锁。
- 警告：环网端口具有不同的静态 VLAN 组态。
- 警告：环网端口具有不同的 VLAN 端口组态。
- 警告：环网端口具有不同的静态组播组态。
- 警告：环网端口具有不同的负载限制组态。
- 进入故障状态：已针对链路状态监视和链路中断启用端口 <端口号>。
- 离开故障状态：已针对链路状态监视禁用端口 <端口号>。
- 进入故障状态：已针对电源监视和断电启用电源线路 <电源 ID>。
- 离开故障状态：已针对电源监视禁用电源线路 <电源 ID>。
- <CLI | WBM | SSH>：验证失败。
- 警告：OSPF 消耗的内存过多，已被关闭。
- 发送自 <MAC 地址> 的重复 IP 地址 <IP 地址>
- IN <数字量输入的编号>（输入的名称）<高 | 低>
- VRRP：VLAN <VLAN-ID> 上的虚拟路由器 <路由器编号> 已转换至 <主站| 备用 | 禁用 | 初始化 | 无效> 状态。
- PNIO 组态无效，与备用设备冲突。

- PNIO 组态无效，与 HRP 冲突。
- PNIO 组态无效，与 MRP 环网端口冲突：<冲突原因>
- PNIO 组态无效，与备用冗余组态冲突：
- PNIO 组态无效，检测到冲突：<组态冲突说明>
- 备用观察器功能 <已启动 | 已停止>
- 备用设备：承担 <主设备 | 从设备> 角色
- 身份验证成功，端口：<端口号> VLAN：<VLAN ID> MAC：<MAC 地址>
- 身份验证失败，端口：<端口号> VLAN：<VLAN ID> MAC：<MAC 地址>
- 访客 VLAN 身份验证，端口：<端口号> VLAN：<VLAN ID> MAC：<MAC 地址>
- PoE 端口：<端口号> 通电，等级：<功率等级>，分配的功率：<预留功率> mW
- PoE 端口：<端口号> 断电
- PoE 端口：<端口号> 已启用
- PoE 端口：由于 <关闭原因> 而禁用了 <端口号>

附录 E

E

E.1 在多台工业以太网交换机上使用相同的组态

以下列表列出可使用相同组态的工业以太网交换机。

可通过部件编号识别设备。

设备	可加载组态
6GK5 307-3BL00-2AA3	6GK5 307-3BL00-2AA3 6GK5 307-3BL10-2AA3 6GK5 307-3BM00-2AA3 6GK5 307-3BM10-2AA3 6GK5 308-2FL00-2AA3 6GK5 308-2FL10-2AA3 6GK5 308-2FM00-2AA3 6GK5 308-2FM10-2AA3 6GK5 308-2FN00-2AA3 6GK5 308-2FN10-2AA3 6GK5 308-2FP00-2AA3 6GK5 308-2FP10-2AA3 6GK5 310-0BA00-2AA3 6GK5 310-0BA10-2AA3 6GK5 310-0FA00-2AA3 6GK5 310-0FA10-2AA3
6GK5 307-3BM00-2AA3	6GK5 307-3BL00-2AA3 6GK5 307-3BL10-2AA3 6GK5 307-3BM00-2AA3 6GK5 307-3BM10-2AA3 6GK5 308-2FL00-2AA3 6GK5 308-2FL10-2AA3 6GK5 308-2FM00-2AA3 6GK5 308-2FM10-2AA3 6GK5 308-2FN00-2AA3 6GK5 308-2FN10-2AA3 6GK5 308-2FP00-2AA3 6GK5 308-2FP10-2AA3 6GK5 310-0BA00-2AA3 6GK5 310-0BA10-2AA3 6GK5 310-0FA00-2AA3 6GK5 310-0FA10-2AA3

设备	可加载组态
6GK5 308-2FL00-2AA3	6GK5 307-3BL00-2AA3 6GK5 307-3BL10-2AA3 6GK5 307-3BM00-2AA3 6GK5 307-3BM10-2AA3 6GK5 308-2FL00-2AA3 6GK5 308-2FL10-2AA3 6GK5 308-2FM00-2AA3 6GK5 308-2FM10-2AA3 6GK5 308-2FN00-2AA3 6GK5 308-2FN10-2AA3 6GK5 308-2FP00-2AA3 6GK5 308-2FP10-2AA3 6GK5 310-0BA00-2AA3 6GK5 310-0BA10-2AA3 6GK5 310-0FA00-2AA3 6GK5 310-0FA10-2AA3
6GK5 308-2FM00-2AA3	6GK5 307-3BL00-2AA3 6GK5 307-3BL10-2AA3 6GK5 307-3BM00-2AA3 6GK5 307-3BM10-2AA3 6GK5 308-2FL00-2AA3 6GK5 308-2FL10-2AA3 6GK5 308-2FM00-2AA3 6GK5 308-2FM10-2AA3 6GK5 308-2FN00-2AA3 6GK5 308-2FN10-2AA3 6GK5 308-2FP00-2AA3 6GK5 308-2FP10-2AA3 6GK5 310-0BA00-2AA3 6GK5 310-0BA10-2AA3 6GK5 310-0FA00-2AA3 6GK5 310-0FA10-2AA3

设备	可加载组态
6GK5 308-2FN00-2AA3	6GK5 307-3BL00-2AA3 6GK5 307-3BL10-2AA3 6GK5 307-3BM00-2AA3 6GK5 307-3BM10-2AA3 6GK5 308-2FL00-2AA3 6GK5 308-2FL10-2AA3 6GK5 308-2FM00-2AA3 6GK5 308-2FM10-2AA3 6GK5 308-2FN00-2AA3 6GK5 308-2FN10-2AA3 6GK5 308-2FP00-2AA3 6GK5 308-2FP10-2AA3 6GK5 310-0BA00-2AA3 6GK5 310-0BA10-2AA3 6GK5 310-0FA00-2AA3 6GK5 310-0FA10-2AA3
6GK5 308-2FP00-2AA3	6GK5 307-3BL00-2AA3 6GK5 307-3BL10-2AA3 6GK5 307-3BM00-2AA3 6GK5 307-3BM10-2AA3 6GK5 308-2FL00-2AA3 6GK5 308-2FL10-2AA3 6GK5 308-2FM00-2AA3 6GK5 308-2FM10-2AA3 6GK5 308-2FN00-2AA3 6GK5 308-2FN10-2AA3 6GK5 308-2FP00-2AA3 6GK5 308-2FP10-2AA3 6GK5 310-0BA00-2AA3 6GK5 310-0BA10-2AA3 6GK5 310-0FA00-2AA3 6GK5 310-0FA10-2AA3

设备	可加载组态
6GK5 310-0BA00-2AA3	6GK5 307-3BL00-2AA3 6GK5 307-3BL10-2AA3 6GK5 307-3BM00-2AA3 6GK5 307-3BM10-2AA3 6GK5 308-2FL00-2AA3 6GK5 308-2FL10-2AA3 6GK5 308-2FM00-2AA3 6GK5 308-2FM10-2AA3 6GK5 308-2FN00-2AA3 6GK5 308-2FN10-2AA3 6GK5 308-2FP00-2AA3 6GK5 308-2FP10-2AA3 6GK5 310-0BA00-2AA3 6GK5 310-0BA10-2AA3 6GK5 310-0FA00-2AA3 6GK5 310-0FA10-2AA3
6GK5 310-0FA00-2AA3	6GK5 307-3BL00-2AA3 6GK5 307-3BL10-2AA3 6GK5 307-3BM00-2AA3 6GK5 307-3BM10-2AA3 6GK5 308-2FL00-2AA3 6GK5 308-2FL10-2AA3 6GK5 308-2FM00-2AA3 6GK5 308-2FM10-2AA3 6GK5 308-2FN00-2AA3 6GK5 308-2FN10-2AA3 6GK5 308-2FP00-2AA3 6GK5 308-2FP10-2AA3 6GK5 310-0BA00-2AA3 6GK5 310-0BA10-2AA3 6GK5 310-0FA00-2AA3 6GK5 310-0FA10-2AA3

设备	可加载组态
6GK5 307-3BL10-2AA3	6GK5 307-3BL00-2AA3 6GK5 307-3BL10-2AA3 6GK5 307-3BM00-2AA3 6GK5 307-3BM10-2AA3 6GK5 308-2FL00-2AA3 6GK5 308-2FL10-2AA3 6GK5 308-2FM00-2AA3 6GK5 308-2FM10-2AA3 6GK5 308-2FN00-2AA3 6GK5 308-2FN10-2AA3 6GK5 308-2FP00-2AA3 6GK5 308-2FP10-2AA3 6GK5 310-0BA00-2AA3 6GK5 310-0BA10-2AA3 6GK5 310-0FA00-2AA3 6GK5 310-0FA10-2AA3
6GK5 307-3BM10-2AA3	6GK5 307-3BL00-2AA3 6GK5 307-3BL10-2AA3 6GK5 307-3BM00-2AA3 6GK5 307-3BM10-2AA3 6GK5 308-2FL00-2AA3 6GK5 308-2FL10-2AA3 6GK5 308-2FM00-2AA3 6GK5 308-2FM10-2AA3 6GK5 308-2FN00-2AA3 6GK5 308-2FN10-2AA3 6GK5 308-2FP00-2AA3 6GK5 308-2FP10-2AA3 6GK5 310-0BA00-2AA3 6GK5 310-0BA10-2AA3 6GK5 310-0FA00-2AA3 6GK5 310-0FA10-2AA3

设备	可加载组态
6GK5 308-2FL10-2AA3	6GK5 307-3BL00-2AA3 6GK5 307-3BL10-2AA3 6GK5 307-3BM00-2AA3 6GK5 307-3BM10-2AA3 6GK5 308-2FL00-2AA3 6GK5 308-2FL10-2AA3 6GK5 308-2FM00-2AA3 6GK5 308-2FM10-2AA3 6GK5 308-2FN00-2AA3 6GK5 308-2FN10-2AA3 6GK5 308-2FP00-2AA3 6GK5 308-2FP10-2AA3 6GK5 310-0BA00-2AA3 6GK5 310-0BA10-2AA3 6GK5 310-0FA00-2AA3 6GK5 310-0FA10-2AA3
6GK5 308-2FM10-2AA3	6GK5 307-3BL00-2AA3 6GK5 307-3BL10-2AA3 6GK5 307-3BM00-2AA3 6GK5 307-3BM10-2AA3 6GK5 308-2FL00-2AA3 6GK5 308-2FL10-2AA3 6GK5 308-2FM00-2AA3 6GK5 308-2FM10-2AA3 6GK5 308-2FN00-2AA3 6GK5 308-2FN10-2AA3 6GK5 308-2FP00-2AA3 6GK5 308-2FP10-2AA3 6GK5 310-0BA00-2AA3 6GK5 310-0BA10-2AA3 6GK5 310-0FA00-2AA3 6GK5 310-0FA10-2AA3

设备	可加载组态
6GK5 308-2FN10-2AA3	6GK5 307-3BL00-2AA3 6GK5 307-3BL10-2AA3 6GK5 307-3BM00-2AA3 6GK5 307-3BM10-2AA3 6GK5 308-2FL00-2AA3 6GK5 308-2FL10-2AA3 6GK5 308-2FM00-2AA3 6GK5 308-2FM10-2AA3 6GK5 308-2FN00-2AA3 6GK5 308-2FN10-2AA3 6GK5 308-2FP00-2AA3 6GK5 308-2FP10-2AA3 6GK5 310-0BA00-2AA3 6GK5 310-0BA10-2AA3 6GK5 310-0FA00-2AA3 6GK5 310-0FA10-2AA3
6GK5 308-2FP10-2AA3	6GK5 307-3BL00-2AA3 6GK5 307-3BL10-2AA3 6GK5 307-3BM00-2AA3 6GK5 307-3BM10-2AA3 6GK5 308-2FL00-2AA3 6GK5 308-2FL10-2AA3 6GK5 308-2FM00-2AA3 6GK5 308-2FM10-2AA3 6GK5 308-2FN00-2AA3 6GK5 308-2FN10-2AA3 6GK5 308-2FP00-2AA3 6GK5 308-2FP10-2AA3 6GK5 310-0BA00-2AA3 6GK5 310-0BA10-2AA3 6GK5 310-0FA00-2AA3 6GK5 310-0FA10-2AA3

设备	可加载组态
6GK5 310-0BA10-2AA3	6GK5 307-3BL00-2AA3 6GK5 307-3BL10-2AA3 6GK5 307-3BM00-2AA3 6GK5 307-3BM10-2AA3 6GK5 308-2FL00-2AA3 6GK5 308-2FL10-2AA3 6GK5 308-2FM00-2AA3 6GK5 308-2FM10-2AA3 6GK5 308-2FN00-2AA3 6GK5 308-2FN10-2AA3 6GK5 308-2FP00-2AA3 6GK5 308-2FP10-2AA3 6GK5 310-0BA00-2AA3 6GK5 310-0BA10-2AA3 6GK5 310-0FA00-2AA3 6GK5 310-0FA10-2AA3
6GK5 310-0FA10-2AA3	6GK5 307-3BL00-2AA3 6GK5 307-3BL10-2AA3 6GK5 307-3BM00-2AA3 6GK5 307-3BM10-2AA3 6GK5 308-2FL00-2AA3 6GK5 308-2FL10-2AA3 6GK5 308-2FM00-2AA3 6GK5 308-2FM10-2AA3 6GK5 308-2FN00-2AA3 6GK5 308-2FN10-2AA3 6GK5 308-2FP00-2AA3 6GK5 308-2FP10-2AA3 6GK5 310-0BA00-2AA3 6GK5 310-0BA10-2AA3 6GK5 310-0FA00-2AA3 6GK5 310-0FA10-2AA3
6GK5 308-2GG00-2AA2	6GK5 308-2GG00-2AA2 6GK5 308-2GG00-2CA2
6GK5 308-2GG00-2CA2	6GK5 308-2GG00-2AA2 6GK5 308-2GG00-2CA2

设备	可加载组态
6GK5 308-2QG00-2AA2	6GK5 308-2GG00-2AA2 6GK5 308-2GG00-2CA2 6GK5 308-2QG00-2AA2
6GK5 302-7GD00-1EA3	6GK5 302-7GD00-1EA3 6GK5 302-7GD00-2EA3 6GK5 302-7GD00-1GA3 6GK5 302-7GD00-2GA3 6GK5 302-7GD00-3EA3 6GK5 302-7GD00-4EA3 6GK5 302-7GD00-3GA3 6GK5 302-7GD00-4GA3
6GK5 302-7GD00-2EA3	6GK5 302-7GD00-1EA3 6GK5 302-7GD00-2EA3 6GK5 302-7GD00-1GA3 6GK5 302-7GD00-2GA3 6GK5 302-7GD00-3EA3 6GK5 302-7GD00-4EA3 6GK5 302-7GD00-3GA3 6GK5 302-7GD00-4GA3
6GK5 302-7GD00-1GA3	6GK5 302-7GD00-1EA3 6GK5 302-7GD00-2EA3 6GK5 302-7GD00-1GA3 6GK5 302-7GD00-2GA3 6GK5 302-7GD00-3EA3 6GK5 302-7GD00-4EA3 6GK5 302-7GD00-3GA3 6GK5 302-7GD00-4GA3
6GK5 302-7GD00-2GA3	6GK5 302-7GD00-1EA3 6GK5 302-7GD00-2EA3 6GK5 302-7GD00-1GA3 6GK5 302-7GD00-2GA3 6GK5 302-7GD00-3EA3 6GK5 302-7GD00-4EA3 6GK5 302-7GD00-3GA3 6GK5 302-7GD00-4GA3

设备	可加载组态
6GK5 302-7GD00-3EA3	6GK5 302-7GD00-1EA3 6GK5 302-7GD00-2EA3 6GK5 302-7GD00-1GA3 6GK5 302-7GD00-2GA3 6GK5 302-7GD00-3EA3 6GK5 302-7GD00-4EA3 6GK5 302-7GD00-3GA3 6GK5 302-7GD00-4GA3
6GK5 302-7GD00-4EA3	6GK5 302-7GD00-1EA3 6GK5 302-7GD00-2EA3 6GK5 302-7GD00-1GA3 6GK5 302-7GD00-2GA3 6GK5 302-7GD00-3EA3 6GK5 302-7GD00-4EA3 6GK5 302-7GD00-3GA3 6GK5 302-7GD00-4GA3
6GK5 302-7GD00-3GA3	6GK5 302-7GD00-1EA3 6GK5 302-7GD00-2EA3 6GK5 302-7GD00-1GA3 6GK5 302-7GD00-2GA3 6GK5 302-7GD00-3EA3 6GK5 302-7GD00-4EA3 6GK5 302-7GD00-3GA3 6GK5 302-7GD00-4GA3
6GK5 302-7GD00-4GA3	6GK5 302-7GD00-1EA3 6GK5 302-7GD00-2EA3 6GK5 302-7GD00-1GA3 6GK5 302-7GD00-2GA3 6GK5 302-7GD00-3EA3 6GK5 302-7GD00-4EA3 6GK5 302-7GD00-3GA3 6GK5 302-7GD00-4GA3

设备	可加载组态
6GK5 307-2FD00-1EA3	6GK5 307-2FD00-1EA3 6GK5 307-2FD00-2EA3 6GK5 307-2FD00-1GA3 6GK5 307-2FD00-2GA3 6GK5 307-2FD00-3EA3 6GK5 307-2FD00-4EA3 6GK5 307-2FD00-3GA3 6GK5 307-2FD00-4GA3
6GK5 307-2FD00-2EA3	6GK5 307-2FD00-1EA3 6GK5 307-2FD00-2EA3 6GK5 307-2FD00-1GA3 6GK5 307-2FD00-2GA3 6GK5 307-2FD00-3EA3 6GK5 307-2FD00-4EA3 6GK5 307-2FD00-3GA3 6GK5 307-2FD00-4GA3
6GK5 307-2FD00-1GA3	6GK5 307-2FD00-1EA3 6GK5 307-2FD00-2EA3 6GK5 307-2FD00-1GA3 6GK5 307-2FD00-2GA3 6GK5 307-2FD00-3EA3 6GK5 307-2FD00-4EA3 6GK5 307-2FD00-3GA3 6GK5 307-2FD00-4GA3
6GK5 307-2FD00-2GA3	6GK5 307-2FD00-1EA3 6GK5 307-2FD00-2EA3 6GK5 307-2FD00-1GA3 6GK5 307-2FD00-2GA3 6GK5 307-2FD00-3EA3 6GK5 307-2FD00-4EA3 6GK5 307-2FD00-3GA3 6GK5 307-2FD00-4GA3

设备	可加载组态
6GK5 307-2FD00-3EA3	6GK5 307-2FD00-1EA3 6GK5 307-2FD00-2EA3 6GK5 307-2FD00-1GA3 6GK5 307-2FD00-2GA3 6GK5 307-2FD00-3EA3 6GK5 307-2FD00-4EA3 6GK5 307-2FD00-3GA3 6GK5 307-2FD00-4GA3
6GK5 307-2FD00-4EA3	6GK5 307-2FD00-1EA3 6GK5 307-2FD00-2EA3 6GK5 307-2FD00-1GA3 6GK5 307-2FD00-2GA3 6GK5 307-2FD00-3EA3 6GK5 307-2FD00-4EA3 6GK5 307-2FD00-3GA3 6GK5 307-2FD00-4GA3
6GK5 307-2FD00-3GA3	6GK5 307-2FD00-1EA3 6GK5 307-2FD00-2EA3 6GK5 307-2FD00-1GA3 6GK5 307-2FD00-2GA3 6GK5 307-2FD00-3EA3 6GK5 307-2FD00-4EA3 6GK5 307-2FD00-3GA3 6GK5 307-2FD00-4GA3
6GK5 307-2FD00-4GA3	6GK5 307-2FD00-1EA3 6GK5 307-2FD00-2EA3 6GK5 307-2FD00-1GA3 6GK5 307-2FD00-2GA3 6GK5 307-2FD00-3EA3 6GK5 307-2FD00-4EA3 6GK5 307-2FD00-3GA3 6GK5 307-2FD00-4GA3
6GK5 324-*	6GK5 324-* 可以在所有 SCALANCE XR324 设备（包括 EEC 和 PoE）中使用相同组态。
6GK5 414-3FC00-2AA2	6GK5 414-3FC10-2AA2
6GK5 414-3FC10-2AA2	6GK5 414-3FC00-2AA2

使用的加密方法

F

下表列出了 SCALANCE X-300/X-400 使用的加密方法（密码）。

SSL

类别	IANA 名称	十六进制值	默认启用
加密套件	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	0xc02c	✓
加密套件	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	0xc024	✓
加密套件	TLS_ECDHE_ECDSA_WITH_AES_256_CCM	0xc0ad	✓
加密套件	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	0xc02b	✓
加密套件	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	0xc023	✓
加密套件	TLS_ECDHE_ECDSA_WITH_AES_128_CCM	0xc0ac	✓
协议版本	TLSv1.2	-	✓

SSH

类别	IANA 名称	十六进制值	默认启用
加密方法 (enc)	aes128-ctr	-	✓
加密方法 (enc)	aes192-ctr	-	✓
加密方法 (enc)	aes256-ctr	-	✓
主机密钥	ecdsa-sha2-nistp256	-	✓
密钥交换 (kex)	curve25519-sha256	-	✓
密钥交换 (kex)	curve25519-sha256@libssh.org	-	✓
密钥交换 (kex)	ecdh-sha2-nistp256	-	✓
密钥交换 (kex)	ecdh-sha2-nistp384	-	✓

类别	IANA 名称	十六进制值	默认启用
密钥交换 (kex)	ecdh-sha2-nistp521	-	✓
MAC	umac-128-etm@openssh.com	-	✓
MAC	hmac-sha2-256-etm@openssh.com	-	✓
MAC	hmac-sha2-512-etm@openssh.com	-	✓
协议版本	SSHv2.0	-	✓

SNMP

类别	方法	十六进制值	默认启用
身份验证	HMAC-MD5-96	-	-
身份验证	HMAC-SHA-96	-	-
加密	des-cbc	-	-

索引

A

ACL, 186

B

BA - 操作说明, 20
BAK - 精简版操作说明, 20
BOOTP, 26, 37, 38, 107
BPDU（桥接协议数据单元）, 225

C

CIST 端口参数, 240
CLI 命令, 46
    符号表示法, 47
    命令快捷方式, 47
CoS（Class of Service，服务类别）, 432
C-PLUG, 25
CRC, 310

D

DCP, 107
DCP 只读 (DCP Read Only), 107
DHCP, 26, 36, 39, 107
DHCP 选项 82, 27
DLF（目标查询失败）, 204
DSCP, 251

F

FMP 诊断, 288

G

GMRP, 157, 199
GVRP, 157, 221, 228

H

HRP, 34
HTTP, 56
HyperTerminal, 37, 415, 416

I

IEEE 1588 时钟同步 (PTP), 271
IEEE 802.1x, 183
IEEE 802.1X, 179
IGMP, 157
IGMP 查询, 27
IGMP 组态, 27
IP 地址, 35, 36, 103
    组态选项, 36

J

Jabbers, 310

L

LACP, 178
LED 仿真, 44
LLDP, 256
LLDP 邻居, 258

M

MAC 地址表, 25
MAC 身份验证, 183
MD5, 331
MIB, 363
    MIB 变量, 419, 427
    标准 MIB, 365
    专有 MIB, 365
MSTP, 159, 235
    端口参数, 247
MSTP 实例, 247, 248
MSTP（多重生成树协议）, 245

N

NCM PC, 37
NTP, 194
NTP（网络时间协议）, 142

P

PH - 组态手册, 20

POF 诊断, 287
PROFINET IO, 367
PTP（精确时间协议）, 271

Q

QoS, 251

R

RADIUS 服务器, 179
RFC
  RFC 1213, 365
  RFC 1286, 365
  RFC 1518, 35
  RFC 1519, 35
  RFC 1724, 365
  RFC 1757, 365
  RFC 1850, 365
  RFC 1907, 365
  RFC 2233, 365
  RFC 2571, 365
  RFC 2572, 365
  RFC 2573, 365
  RFC 2574, 365
  RFC 2575, 365
  RFC 2665, 365
  RFC 2674p, 365
  RFC 2674q, 365
RMON, 105
RSTP, 158
RSTP 大网络支持, 159

S

SFP 诊断, 285
SHA 算法, 118
SICLOCK, 106
SICLOCK 时间发送器, 26
SIMATIC NET 词汇表, 3
SMTP 服务器, 134
SNMP, 111, 363
  SNMP 陷阱, 116
  SNMPv1, 363
  SNMPv2, 363
  SNMPv3, 27, 363
  SNMPv3 用户, 121
SNTP（简单网络时间协议）, 140
SSH 公钥身份验证, 57, 65
STEP 7, 37
STP, 158
SysLog, 27

T

TELNET, 105
TFTP 服务器, 61

U

UTC 时间, 139

V

VLAN, 24, 210
  VLAN 标记, 431
  VLAN-ID, 432

报

报警事件, 133

备

备用观察器, 95

被

被动侦听 (Passive Listening), 156

插

插槽功能, 380, 381, 383

超

超长模式, 156

冲

冲突, 310

词

词汇表, 3

存

存储并转发, 23

带

带内端口, 37
带外端口, 21, 37

单

单播过滤器, 186

登

登录, 37, 65

地

地址过滤, 186

第

第 3 层功能
    路由, 28
    路由功能, 37

点

点对点, 226

电

电源监视, 375
电子邮件功能, 26, 105, 133
    报警事件, 133
    线路监视, 133

端

端口
    带内端口, 37
    带外端口, 37
    端口组态, 160, 163
    链路检查 (Link Check), 167
端口诊断
    FMP 诊断, 288
    POF 端口, 290
    POF 诊断, 287
    SFP 诊断, 285
端口组态, 163

多

多重生成树, 235
多重生成树协议, 159

访

访客 VLAN, 183
访问控制, 25

复

复位为出厂设置, 414

固

固件更新, 409
固件降级, 414

故

故障屏蔽, 98

观

观察器, 90

过

过大, 310
过滤器
    地址过滤, 186
    过滤表, 187
    过滤器组态, 188
过小, 310

回

回路检测, 292

基

基于 Web 的管理, 42, 409

监

监视端口, 156

接

接口
- RS 232 接口, 22
- 串行端口, 22
- 串口, 415, 416
- 带外端口, 21
- 快速以太网端口, 21
- 千兆位以太网端口, 23
- 以太网端口, 21

介

介质冗余方法, 34

镜

镜像, 25, 156
- 监视端口, 156
- 镜像端口, 156

镜像端口, 156

空

空调制解调器电缆, 22, 37
- 针脚分配, 416

快

快速生成树, 158

老

老化, 155
老化时间, 156, 200

链

链路检查 (Link Check), 167
链路检查状态, 167
链路检查组态, 169

邻

邻居表, 258

流

流量控制, 26

路

路由
- 第 3 层功能, 28
- 路由功能, 37

默

默认网关, 54, 107

千

千兆位以太网端口, 23

冗

冗余
- 冗余连接, 23

设

设置值, 46

生

生成树, 24, 158
- 多重生成树, 24, 235, 245
- 快速生成树, 24, 226

时

时区, 139
时钟
- NTP（网络时间协议）, 142
- SICLOCK, 26, 106
- SNTP（简单网络时间协议）, 140
- UTC 时间, 139
- 时区, 139

时钟同步, 26, 138
系统时间, 138
时钟同步, 26

事

事件日志表, 26

数

数据传输率, 23
数字量输入, 132

刷

刷新, 46

碎

碎片, 310

统

统计信息, 303

线

线路监视, 133

验

验证, 179, 181
802.1x, 183
MAC 身份验证, 183
访客 VLAN, 183
身份验证服务器, 179
身份重新验证, 183

以

以太网端口, 21

优

优先级, 230

运

运行模式
半双工, 22, 26
全双工, 22, 23, 26

增

增强的被动侦听兼容性, 159

针

针脚分配
空调制解调器电缆, 416
诊断端口连接电缆, 417

诊

诊断端口连接电缆
针脚分配, 417

重

重启, 54

转

转发延迟, 229

子

子网掩码, 36, 103

自

自动跨接, 22, 23
自动协商, 161, 379

组

组播, 194