

SIEMENS

SIMATIC NET

工业以太网交换机 SCALANCE X-500 基于 Web 的管理

配置手册

简介

1

说明

2

IP 地址分配

3

技术基础

4

使用“基于 Web 的管理”进行组态

5




故障排除/FAQ

6

法律资讯

警告提示系统

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

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


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

合格的专业人员

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

按规定使用 Siemens 产品

请注意下列说明：

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

商标

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

责任免除

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

目录

1	简介	7
1.1	有关组态手册的信息.....	7
2	说明	9
2.1	产品特征.....	9
2.2	SCALANCE X-500 的安装和操作要求.....	11
2.3	C-PLUG.....	12
2.4	以太网供电 (PoE).....	13
3	IP 地址分配	17
3.1	IP 地址的结构.....	17
3.2	IP 地址的初始分配.....	18
3.3	用 DHCP 进行地址分配.....	19
3.4	用 Primary Setup Tool 进行地址分配.....	20
4	技术基础	21
4.1	VLAN.....	21
4.2	VLAN 标记.....	22
4.3	SNMP.....	25
4.4	生成树.....	27
4.4.1	RSTP、MSTP、CIST.....	28
4.5	路由功能.....	29
4.5.1	OSPFv2.....	30
5	使用“基于 Web 的管理”进行组态	35
5.1	基于 Web 的管理.....	35
5.2	登录.....	36
5.3	“Information”菜单.....	39
5.3.1	起始页面.....	39
5.3.2	Versions.....	44
5.3.3	ARP 表.....	46
5.3.4	日志表.....	47
5.3.5	故障.....	49
5.3.6	冗余.....	50
5.3.6.1	生成树.....	50

5.3.6.2	VRRP 统计信息	54
5.3.7	以太网统计信息	56
5.3.7.1	数据包大小	56
5.3.7.2	数据包类型	58
5.3.7.3	数据包错误	59
5.3.8	路由	61
5.3.8.1	路由表	61
5.3.8.2	OSPFv2 接口	62
5.3.8.3	OSPFv2 邻居	64
5.3.8.4	OSPFv2 虚拟邻居	66
5.3.8.5	OSPFv2 LSDB	68
5.4	“System”菜单	70
5.4.1	组态	70
5.4.2	General	73
5.4.2.1	设备	73
5.4.2.2	坐标	74
5.4.3	Agent IP	76
5.4.4	重启	78
5.4.5	加载和保存	80
5.4.5.1	HTTP	80
5.4.5.2	TFTP	83
5.4.6	事件	86
5.4.7	SMTP 客户端	89
5.4.8	DHCP 客户端	91
5.4.9	SNMP	93
5.4.9.1	常规	93
5.4.9.2	Traps	95
5.4.10	系统时间	96
5.4.10.1	手动设置	96
5.4.10.2	SNTP 客户端	98
5.4.10.3	NTP 客户端	101
5.4.10.4	SIMATIC 时间客户端	104
5.4.11	自动注销	105
5.4.12	Select/Set 按钮组态	106
5.4.13	Syslog 客户端	107
5.4.14	端口	109
5.4.14.1	概述	109
5.4.14.2	组态	111
5.4.15	故障监视	114
5.4.15.1	电源	114
5.4.15.2	Link Change	115
5.4.16	C-PLUG	117
5.4.17	Ping	120
5.4.18	PoE	121

5.4.18.1	常规.....	121
5.4.18.2	端口.....	122
5.5	“第 2 层”菜单.....	125
5.5.1	组态.....	125
5.5.2	Qos.....	127
5.5.2.1	CoS 队列映射.....	127
5.5.2.2	DSCP 映射.....	129
5.5.3	速率控制.....	130
5.5.4	VLAN.....	132
5.5.4.1	常规.....	132
5.5.4.2	GVRP.....	135
5.5.4.3	基于端口的 VLAN.....	137
5.5.4.4	基于协议的 VLAN 组.....	139
5.5.4.5	基于协议的 VLAN 端口.....	141
5.5.4.6	基于 Ipv4 子网的 VLAN.....	142
5.5.5	端口镜像.....	143
5.5.6	动态 MAC 老化.....	146
5.5.7	MSTP.....	147
5.5.7.1	常规.....	147
5.5.7.2	CIST 概述.....	148
5.5.7.3	CIST 端口.....	150
5.5.7.4	MST 概述.....	154
5.5.7.5	MST 端口.....	156
5.5.8	链路汇聚.....	159
5.5.9	DCP 转发.....	162
5.5.10	LLDP.....	164
5.5.11	单播.....	166
5.5.11.1	过滤.....	166
5.5.11.2	锁定端口.....	169
5.5.11.3	学习.....	171
5.5.11.4	未知单播阻止.....	173
5.5.12	组播.....	175
5.5.12.1	组.....	175
5.5.12.2	IGMP.....	178
5.5.12.3	GMRP.....	180
5.5.13	广播.....	183
5.6	“Security”菜单.....	185
5.6.1	密码.....	185
5.6.2	AAA.....	187
5.6.2.1	常规.....	187
5.6.2.2	Radius 客户端.....	188
5.6.2.3	Authenticator port.....	191
5.6.3	端口 ACL MAC.....	193

5.6.3.1	规则组态.....	193
5.6.3.2	端口进站规则.....	194
5.6.3.3	端口出站规则.....	196
5.6.4	端口 ACL IP	198
5.6.4.1	规则组态.....	198
5.6.4.2	端口进站规则.....	200
5.6.4.3	端口出站规则.....	202
5.6.5	管理 ACL.....	204
5.7	“Layer 3”菜单.....	207
5.7.1	组态.....	207
5.7.2	子网.....	208
5.7.2.1	概述.....	208
5.7.2.2	组态.....	210
5.7.3	路由.....	211
5.7.4	DHCP 中继代理.....	213
5.7.4.1	常规.....	213
5.7.4.2	选项.....	215
5.7.5	VRRP	218
5.7.5.1	路由器	218
5.7.5.2	组态.....	221
5.7.5.3	地址概述.....	223
5.7.5.4	地址组态.....	224
5.7.6	OSPFv2	225
5.7.6.1	组态.....	225
5.7.6.2	区域.....	227
5.7.6.3	区域范围.....	229
5.7.6.4	接口.....	231
5.7.6.5	虚拟链路.....	234
6	故障排除/FAQ.....	237
6.1	不能通过 WBM 或 CLI 进行固件更新	237
	索引.....	239

简介

1.1 有关组态手册的信息

组态手册的有效性

本组态手册涵盖了以下产品：

- XR552-12M
- XR528-6M

上述设备不一定具有路由功能。具有路由功能的设备也支持第 3 层路由功能 VRRP 和 OSPF。

本组态手册适用于以下软件版本：

- 自固件版本 V2.0 开始的 SCALANCE X-500

本组态手册的用途

本组态手册旨在为用户提供安装、调试和运行设备所需的信息。其中包含了组态设备所需的信息。

文档说明

除了您当前阅读的组态手册外，还可以从 **SIMATIC NET** 的工业以太网主题下获取以下文档：

- 组态手册 **SCALANCE X-500** 命令行接口

本文档包含 **SCALANCE X.500** 设备支持的 CLI 命令，在 **SCALANCE X-500 CD** 上提供有电子版本。

- 精简版操作说明

本文档以纸质形式随设备一起提供，也可在 **SCALANCE X-500 CD** 上获取其电子版本。本文档包含有关产品安装、连接和认证方面的信息。

提供了下列对象的精简版操作说明：

- **SCALANCE XR-500M**
- **SCALANCE XR-500M** 的 **MM900** 媒介模块
- **SCALANCE XR-500M** 的风扇单元 **FAN597-1**
- **SCALANCE XR-500M** 的电源 **PS598-1**

SIMATIC NET 词汇表

在 **SIMATIC NET** 词汇表部分针对本文档中所用的专业术语进行了解释。

用户可在以下位置找到 **SIMATIC NET** 词汇表：

- **SIMATIC NET** 手册集

该 DVD 随一些 **SIMATIC NET** 产品一起提供。

- 请参见 Internet 上的以下条目 ID：

50305045 (<http://support.automation.siemens.com/WW/view/zh/50305045>)

说明

2.1 产品特征

SCALANCE X-500 设备的特征

- 以太网接口支持以下模式：
 - 全双工和半双工 10 Mbps 和 100 Mbps
 - 1000 Mbps 全双工
 - 自动跨接
 - 自动极性变换
- SCALANCE X-500 设备支持以下标准冗余协议：多重生成树协议 (Multiple Spanning Tree Protocol, MSTP)、快速生成树协议 (Rapid Spanning Tree Protocol, RSTP) 和生成树协议 (Spanning Tree Protocol, STP)。这使得子网可以冗余连接到更高层的公司网络，同时减少重新组态的时间（只需数秒时间）。
- 具有路由功能的 SCALANCE X-500 设备支持路由协议“开放式最短路径优先”(Open Shortest Path First, OSPF) 和冗余协议“虚拟路由器冗余协议”(Virtual Router Redundancy Protocol, VRRP)。这使得工业路由于网可以冗余连接到更高层的公司网络。
- 支持虚拟网络 (VLAN)
要想构建节点数快速增加的工业以太网，可以将一个物理网络分成若干个虚拟子网。支持基于端口、协议和 IP 的 VLAN。
- 可限制使用组播协议时（例如，视频传输）的负载
SCALANCE X-500 设备通过学习组播源和目标（IGMP 监听、IGMP 查询器），还可以对组播数据通信进行过滤并限制网络中的负载。可以对组播和广播通信加以限制。
- 时钟同步
- 诊断消息（日志表条目、电子邮件）具有时间戳。通过与 SICLOCK 时间发送器或 SNTP/NTP 服务器进行同步，本地时间在整个网络中保持一致，这使得识别多个设备的诊断消息更为轻松。

2.1 产品特征

- 使用链路汇聚 (IEEE 802.1AX) 捆绑数据流
- 用于对网络流量进行分类的服务质量符合 COS (Class of Service, 服务等级 - IEEE 802.11Q) 和 DSCP (Differentiated Services Code Point, 区分服务代码点 - RFC 2474)。

第 3 层功能

仅具有路由功能的设备提供下列功能:

- 路由
- OSPF
- VRRP

以下设备具有路由功能。

设备	订货号
XR552-12M	6GK5 552-0AR00-2AR2
	6GK5 552-0AR00-2HR2
XR528-6M	6GK5 528-0AR00-2AR2
	6GK5 528-0AR00-2HR2

2.2 SCALANCE X-500 的安装和操作要求

设备的安装和操作要求

必须具有能够联网的 PG/PC，才能对设备进行组态。如果没有可用的 DHCP 服务器，则必须使用安装了 Primary Setup Tool (PST) 的 PC 来为设备首次分配 IP 地址。对于其它组态设置，需要使用有 Telnet 和 Internet 浏览器的计算机。

串口

SCALANCE X.500 设备也有一个串行接口。通过该串行接口，无需 IP 地址便可访问该设备。另外，还随产品提供了串行电缆。

可为连接设置以下参数：

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

2.3 C-PLUG

C-PLUG 中的组态信息

在更换设备时，可使用 C-PLUG 将旧设备的组态传送到新设备中。

注意

只允许在设备关闭后取出或插入 C-PLUG。有关取出和插入 C-PLUG 的更多信息，请参见 SCALANCE X-500 的精简版操作说明。

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

如果使用基于 MAC 地址的功能，则需要重新进行组态。

说明

就 C-PLUG 而言，SCALANCE 设备可在两种模式下工作：

- **无 C-PLUG**

设备将组态存储在内部存储器中。未插入 C-PLUG 时会激活此模式。

- **有 C-PLUG**

通过用户界面显示存储在 C-PLUG 中的组态。如果更改了组态，则设备会将组态信息直接存储在 C-PLUG 和内部存储器中。未插入 C-PLUG 时会激活此模式。一旦插入 C-PLUG 来启动设备，SCALANCE X500 设备就会使用 C-PLUG 中的组态数据来启动。

2.4 以太网供电 (PoE)

概述

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

用于供电的电缆

- **型号 1 (冗余电线)**

在快速以太网中，电线对 1、2 和 3、6 用于传输数据。电线对 4、5 和 7、8 用于供电。如果仅有四根线，则会将电压调制到电线 1、2 和 3、6 上（参见型号 2）。这种选择适合数据传输率为 10/100 Mbps 的情况。这种供电类型不适合数据传输率为 1 Gbps 的情况，这是因为在千兆位以太网中，全部的 8 根电线都用于数据传输。

- **型号 2 (幻象电源)**

应用幻象电源时，会通过用于数据传输的电线对来供电，即全部的八根 (1 Gbps) 或四根 (10/100 Mbps) 电线既用于数据传输，又用于供电。

PoE 兼容终端设备必须支持基于冗余电线的型号 1 和型号 2。

PoE 兼容的交换机可以通过以下方式对终端设备供电：

- 型号 1 或
- 型号 2 或
- 型号 1 和型号 2。

端跨


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

2.4 以太网供电 (PoE)

中跨

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

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

 警告
<p>仅当符合以下条件时使用电源插头：</p> <ul style="list-style-type: none"> • 采用超低电压 SELV，即符合 IEC 60364-4-41 的 PELV • 在美国/加拿大，采用符合 NEC 的 2 类电源 • 在美国/加拿大，布线必须符合 NEC/CEC 的要求 • 电源负载最大 0.5 A。

电缆长度

表格 2-1 允许的电缆长度（铜质电缆 - 快速以太网）

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

表格 2-2 允许的电缆长度（铜质电缆 - 千兆位以太网）

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

表格 2-3 安装接头

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

2.4 以太网供电 (PoE)

IP 地址分配

3.1 IP 地址的结构

地址类别

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

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

XXX.XXX.XXX.XXX

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

子网掩码

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

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

B 类网络示例：

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

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。

3.2 IP 地址的初始分配

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”）。

3.2 IP 地址的初始分配

组态选项

不能使用基于 Web 的管理 (WBM) 来为 SCALANCE X-500 分配初始 IP 地址，因为此组态工具要求 IP 地址已存在。

可通过以下方法将 IP 地址分配给未组态的设备：

- DHCP（默认）
- Primary Setup Tool
- STEP 7
- 使用 CLI 通过串行接口分配
有关使用 CLI 分配 IP 地址的详细信息，请参见 SCALANCE X-500 命令行接口文档。
- NCM PC

说明

交付产品时以及执行“Restore Factory Defaults and Restart”后，DHCP 为启用状态。如果局域网中有 DHCP 服务器，且其能回应 SCALANCE X-500 的 DHCP 请求，则在初次启动设备时会自动分配 IP 地址、子网掩码和网关。“Restore Memory Defaults and Restart”不会删除由 DHCP 或用户分配的 IP 地址。

3.3 用 DHCP 进行地址分配

DHCP 属性

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

- 可在设备启动时或运行期间使用 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, 客户端必须请求新 IP 地址, 或延长现有 IP 地址的租用时间。
- 通常不会分配固定的地址; 即, 当客户端再次请求 IP 地址时, 它通常会接收到一个与之前不同的地址。可以对 DHCP 服务器进行组态, 使得 DHCP 客户端发出请求后, 总是接收到同一个固定地址。用来将 DHCP 客户端标识为固定地址分配的参数在 DHCP 客户端上设置。可以通过 MAC 地址、DHCP 客户端 ID 或系统名称分配地址。在“System > DHCP Client”中组态参数。
- 支持 DHCP 选项 66、67
 - DHCP 选项 66: 分配动态 TFTP 服务器名称
 - DHCP 选项 67: 分配动态引导文件名称

说明

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

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

由于 DHCP 客户端也会向服务器发送 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

- 将设备的 IP 地址改为不是由 DHCP 分配的地址
- 或
- 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。

3.4 用 Primary Setup Tool 进行地址分配

3.4 用 Primary Setup Tool 进行地址分配

简介

PST (Primary Setup Tool) 能够为没有组态 IP 地址的设备分配一个地址。

要求

仅在可通过以太网访问设备的情况下可行。

说明

有关详细信息，请参见 Primary Setup Tool 组态手册。

有关 PST 的更多信息，可访问 Internet 上 Siemens 工业自动化与驱动的服务与支持页面的条目 ID 19440762。该条目的 URL 是：

<http://support.automation.siemens.com/WW/view/en/19440762>

参见

19440762 (<http://support.automation.siemens.com/WW/view/en/19440762>)

技术基础

4.1 VLAN

与节点的空间位置无关的网络定义

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

VLAN 的独特优势是可减少其它 VLAN 的节点和网段的网络负载。

要确定数据包属于哪个 VLAN，需要将帧扩展 4 个字节（VLAN 标记（页 22））。这种扩展不仅包括 VLAN ID，还包括优先级信息。

VLAN 分配选项

对 VLAN 分配有多种选项。

- 基于端口的 VLAN

为设备的每个端口分配一个 VLAN ID。可在“第 2 层 > VLAN > 基于端口的 VLAN”(Layer 2 > VLAN > Port-based VLAN) (页 137) 中组态基于端口的 VLAN。

- 基于协议的 VLAN

为设备的每个端口分配一个协议组。可在“第 2 层 > VLAN > 基于协议的 VLAN 端口”(Layer 2 > VLAN > Protocol Based VLAN Port) (页 141) 中组态基于协议的 VLAN。

- 基于子网的 VLAN

为设备的 IP 地址分配 VLAN ID。可在“第 2 层 > VLAN > 基于 Ipv4 子网的 VLAN”(Layer 2 > VLAN > Ipv4 Subnet Based VLAN) (页 142) 中组态基于子网的 VLAN。

4.2 VLAN 标记

处理 VLAN 分配

如果在设备上创建多个 VLAN 分配，则按以下顺序处理这些分配：

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

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

4.2 VLAN 标记

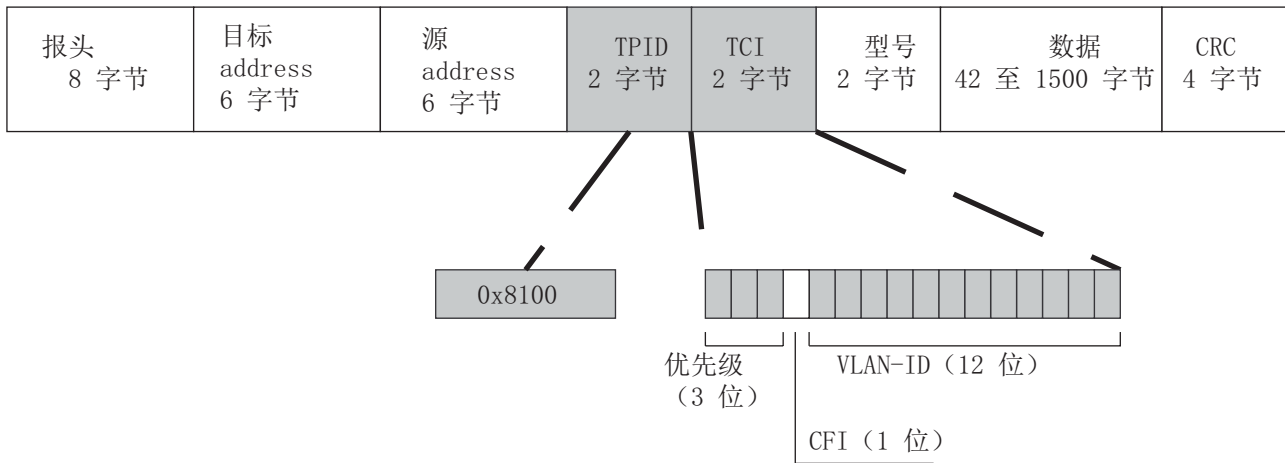
用四个字节扩展以太网帧

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

说明

VLAN 标记使允许的帧总长度从 1518 字节增加到 1522 字节。对于 SCALANCE X-500 设备, 标准 MTU 大小为 1536 字节。该 MTU 大小可更改为 64 到 9216 字节。必须对网络上的终端设备进行检查, 以确定它们是否能处理此长度/帧类型。如果不能处理, 则仅可向这些节点发送标准长度的帧。

附加的 4 个字节在以太网帧头中，位于源地址和以太网类型/长度字段之间：



4.2 VLAN 标记

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

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

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

设备具有八个并行队列，可在其中处理各种优先级的帧。首先会处理具有最高优先级（“严格优先级”方法）的帧。此方法可确保即使在数据通信繁忙时，具有最高优先级的帧仍能得到发送。

规范格式标识符 (CFI)

CFI 用于表示以太网与令牌环之间的兼容性。

值的含义如下：

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

VLAN ID

在 12 位数据字段中，最多可构成 4095 个 VLAN ID。存在以下惯例：

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

4.3 SNMP

简介

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

SNMP 的任务：

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

版本 v1 和 v2c 的 SNMP 没有安全机制。网络中的所有用户都可以访问数据，还可使用适当的软件来更改参数分配。

如果只需对访问权限进行简单控制而无需考虑安全性，则可使用团体字符串。

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

团体字符串的标准值

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

说明

由于安全考虑，请勿使用标准值“**public**”或“**private**”。请在初始安装之后更改该值。

设备级的更多简单保护机制：

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

SNMP 数据包未加密，其他用户可轻松读取。

中央站也称为管理站。SNMP 代理安装在与管理站交换数据的被监视设备上。

管理站发送以下类型的数据包：

- **GET**
向代理请求数据记录
- **GETNEXT**
调用下一条数据记录。
- **GETBULK (verfügbar ab SNMPv2)**
每次请求多条数据记录，例如，表中的多行。
- **SET**
包含相关设备的参数分配数据。

SNMP 代理发送以下类型的数据包：

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

SNMPv1、SNMPv2 和 SNMPv3 使用 UDP（用户数据报协议）。管理信息库 (Management Information Base, MIB) 对该数据进行了介绍。

SNMP v3

与先前版本的 SNMP v1 和 SNMP v2 相比，SNMP v3 引入了综合安全概念。

SNMP v3 支持

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

4.4 生成树

避免在冗余连接中形成环路

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

使用组态帧定义网络拓扑

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

对网络拓扑变化的响应

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

使组态信息保持最新

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

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

4.4.1 RSTP、MSTP、CIST

快速生成树协议 (RSTP)

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

通过使用以下功能可以实现这一点：

- 边缘端口
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。如果经过特定的时间（3 倍呼叫时间）后没有再接收到任何 BPDU，则该端口返回到边缘端口状态。
- 点对点（两个邻近设备之间直接通信）
通过直接连接两个设备，可以无延迟地进行状态变化（重新组态端口）
- 备用端口（根端口的替代端口）
组态根端口的替代端口。如果失去与根网桥的连接，设备可以通过备用端口建立连接，不存在由重新组态导致的延迟。
- 对事件的反应
快速生成树可无延迟地对事件（例如连接中止）做出反应。不用像在生成树中一样等待计时器。
- 最大网桥跳跃计数器
数据包自动变为无效之前所允许的网桥跳跃数。

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

多重生成树协议 (MSTP)

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

公共内部生成树 (CIST)

CIST 是多重生生成树中的术语。CIST 可识别交换机使用的在原理上与 RSTP 内部实例类似的内部实例。

4.5 路由功能

简介

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

SCALANCE X 支持以下路由功能：

- 静态路由
对于静态路由，需在路由表中手动输入路径。
- 路由器冗余
通过标准化 VRRP（Virtual Router Redundancy Protocol，虚拟路由器冗余协议），可使用冗余路由器来提高重要网关的可用性。
- 动态路由
路由表中的条目会动态变化并持续进行更新。这些条目通过路由协议来创建。
 - OSPF v2（开放式最短路径优先）

静态路由

在路由表中手动输入路径。有关在路由表中输入路径的信息，请参阅 WBM 页面“Routes (页 211)”。

使用 VRRP 的路由器冗余

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

网段中的多个 VRRP 路由器以逻辑组的形式组合在一起，从而形成一个虚拟路由器 (Virtual Router, VR)。该组使用虚拟 ID (VRID) 进行定义。组中的 VRID 必须相同。该 VRID 不能再用于其它组。

为虚拟路由器分配一个虚拟 IP 地址和一个虚拟 MAC 地址。将组中的其中一个 VRRP 路由器指定为主路由器。主路由器的优先级为 255。其它 VRRP 路由器为备用路由器。主路由器将虚拟 IP 地址和虚拟 MAC 地址分配给其网络接口。主路由器以指定的时间间隔

将 VRRP 数据包（广播）发送给备用路由器。主路由器通过 VRRP 数据包指示自己仍处于活动状态。主路由器还会对 ARP 查询做出响应。

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

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

在“Layer 3 > VRRP (页 218)”中组态 VRRP。

4.5.1 OSPFv2

使用 OSPF v2 的动态路由

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

可在“Layer 3 > OSPFv2 (页 225)”中组态 OSPFv2。

OSPF v2 将自治系统 (Autonomous System, AS) 分成不同的区域。

OSPF 中的区域

存在以下区域：

- 骨干
骨干区域是指区域 0.0.0.0。骨干区域连接所有其它区域。骨干区域可以直接与其它区域连接，也可以通过虚拟连接与其它区域相连。
骨干区域提供所有路由信息。因此，骨干区域负责在不同区域之间转发信息。
- 存根区域
此区域包含自治系统中该区域的路径，以及自治系统外的标准路径。此自治系统外的目标会被分配给标准路径。
- 完全存根区域
此区域仅识别该区域内的路径，以及该区域外的标准路径。
- 次存根区域 (Not So Stubby Area, NSSA)
此区域可以将来自其它自治系统中的数据包转发（重新分发）到自身自治系统的区域中。这些数据包将由 NSSA 路由器进一步分发。

OSPF 的路由器

OSPF 区分以下路由器类型：

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

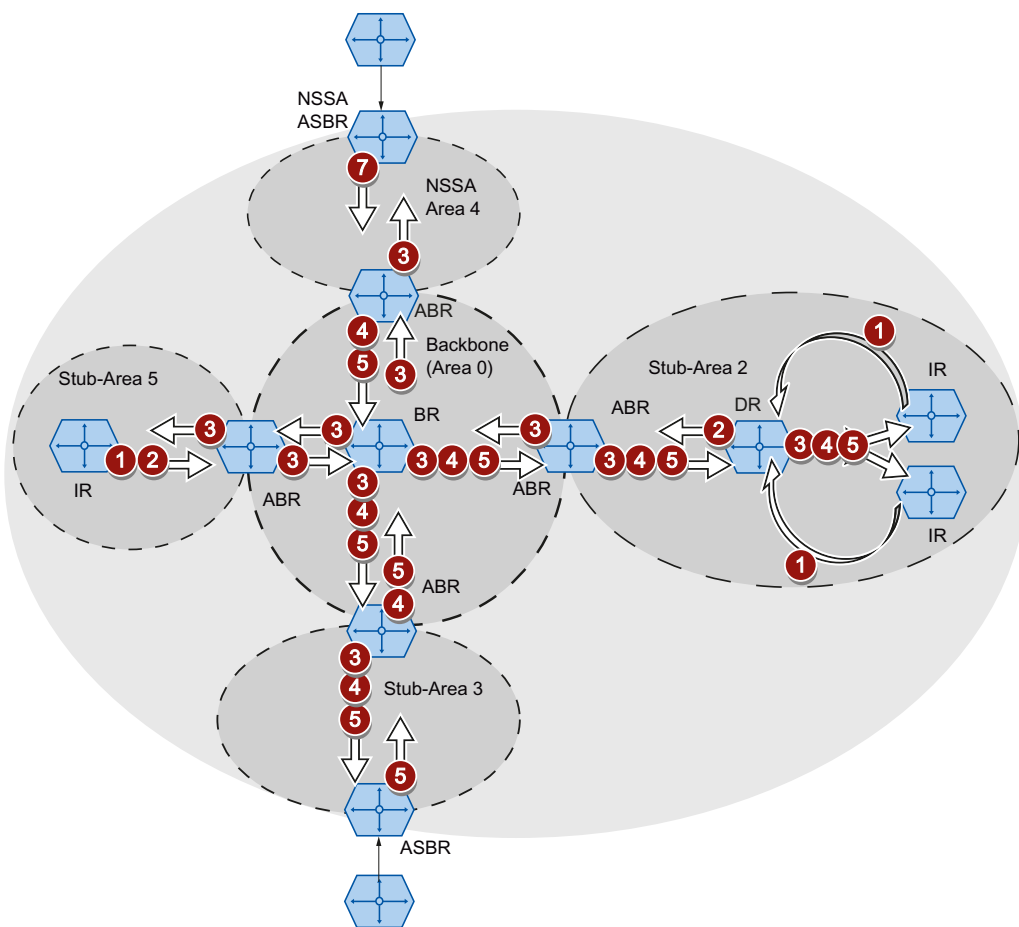
虚拟连接

每个区域都必须从物理上连接到骨干区域。在某些情况下，可能无法实现物理连接。远程路由器通过虚拟连接与骨干路由器相连。在采用虚拟连接的区域，没有指定路由器或备用指定路由器。

LSA 类型

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

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



1 路由器 LSA (LSA 类型 1)

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

2 网络 LSA (LSA 类型 2)

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

- ③ 汇总 LSA (LSA 类型 3/LSA 类型 4)
- ④ Summary LSA 由区域边界路由器生成并发送到区域中。“汇总 LSA”包含有关 AS 中不属于某个区域的路由器的信息。并且，在可能的情况下将路径组合在一起。
 - 汇总 LSA (LSA 类型 3)
LSA 类型 3 标识用于描述访问网络的路径以及将标准路径通知给区域。
 - AS 汇总 LSA (LSA 类型 4)
LSA 类型 4 标识用于描述到 ASBR 的路径。
- ⑤ 外部 LSA (LSA 类型 5/LSA 类型 7)
- ⑦ 外部 LSA 由 ASBR 生成。LSA 类型取决于区域。
 - AS 外部 LSA (LSA 类型 5)
LSA 类型 5 标识由 AS 边界路由器发送到自治系统的区域中，但存根区域和 NSSA 区域除外。LSA 包含有关到另一个 AS 中的某个网络的路径信息。路径可手动创建，也可从外部学习得到。ASBR 使用 LSA 类型 5 将标准路径分配给骨干区域。
 - NSSA 外部 LSA (LSA 类型 7)
LSA 类型 7 标识由 NSSA 的 AS 边界路由器生成。该路由器也称为 NSSA ASBR。LSA 类型 7 标识仅在 NSSA 内发送。如果 LSA 类型 7 标识的 P 位为 1，则这些 LSA 将由 ABR 转换为 LSA 类型 5 标识并发送到骨干区域。

建立近邻关系

路由器遍历以下状态来与相邻路由器建立连接。

1. 尝试状态/初始化状态

路由器激活 OSPF，并开始发送和接收呼叫数据包。路由器根据收到的呼叫数据包了解附近有哪些 OSPF 路由器。路由器会检查呼叫数据包的内容。呼叫数据包还包含“发送方”的邻居路由器的列表（邻居表）。

2. 双向状态

例如，如果区域 ID、区域类型以及时间设置相符，则可与邻居建立连接（邻接）。在点对点网络中，可直接建立连接。如果可以访问网络中的多个邻居路由器，则根据呼叫数据包识别指定路由器 (Designated Router, DR) 和备用指定路由器 (Designated Backup Router, DBR)。优先级最高的路由器将变为指定路由器。如果两个路由器的优先级相同，则 ID 较小的路由器将变为指定的路由器。路由器与指定路由器建立连接。

3. 开始交换状态

邻居路由器决定由哪个路由器启动通信。ID 较大的路由器将成为主路由器。

4. 交换状态

邻居路由器发送用来描述其近邻数据库内容的数据包。近邻数据库（链路状态数据库 - LSDB）包含有关网络拓扑的信息。

5. 加载状态

路由器完成接收的信息。如果路由器对具体连接的状态仍有疑问，它将发送链路状态请求。邻居路由器发出响应（链路状态更新）。该响应包含适当的 LSA。路由器确认已收到响应（链路状态确认）。

6. 完美状态

完成与邻居路由器交换信息。邻居路由器的近邻数据库完全相同。路由器根据“短路径优先”算法计算到各个目标的路径。路径被输入到路由表中。

检查近邻关系

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

更新近邻数据库

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

使用“基于 Web 的管理”进行组态

5.1 基于 Web 的管理

工作原理

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

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

这种方法的优势在于只需要在客户端上安装 Internet 浏览器。

说明

安全连接

WBM 也可用来通过 HTTPS 建立安全连接。

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

要求

- 设备具有 IP 地址
- 设备与客户端 PC 之间存在连接。可以通过 ping 命令检查是否存在连接。
- 允许通过 HTTPS 进行访问。
- 推荐使用的 Internet 浏览器：
 - Microsoft Internet Explorer 版本 8.0
 - Mozilla Firefox 版本 7.0
- 在 Internet 浏览器中激活 JavaScript。

5.2 登录

- 不可将 Internet 浏览器设置成每次从服务器访问页面时，浏览器都会重载页面。页面动态内容的更新是通过其它机制来确保的。在 Internet Explorer 中，可以在“选项 > Internet 选项 > 常规”(Options > Internet Options > General) 菜单的“浏览历史记录”(Browsing history) 部分，用“设置”(Settings) 按钮进行适当的设置。在“检查所存网页的较新版本：”(Check for newer versions of stored pages:) 下，选择“自动”(Automatically)。
- 如果使用了防火墙，则必须打开相关端口。
 - 若使用 HTTP 进行访问： 端口 80
 - 若使用 HTTPS 进行访问： 端口 443

5.2 登录

使用 Internet 浏览器登录

选择 WBM 的语言

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

说明

可用语言

在本版本中，只提供了英语。后续版本将添加其它语言。

The screenshot shows the Siemens WBM login interface. At the top left is the Siemens logo. In the top right corner, there is a language selection dropdown menu set to 'English' and a 'Go' button. Below the logo, there is a login form with fields for 'Name' and 'Password', and a 'Login' button. A large 'LOGIN' watermark is visible in the background. At the bottom, there is a link to 'Switch to secure HTTP'.

建立与设备的连接

使用 Internet 浏览器按照以下步骤与设备建立连接：

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

使用 HTTP 登录

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

无论选择以上哪一种方法登录，都可以按照以下步骤进行操作：

1. 在“Name”输入框中输入以下内容：
 - “admin”：使用这种用户类型时，可以更改设备的设置（对组态数据进行读写访问）。
 - “user”：使用这种用户类型时，无法更改设备的任何设置（对组态数据进行读访问）。
2. 在“Password”输入框中输入密码。

如果是首次登录或是在“恢复出厂默认设置并重启”后登录，则在“Password”输入框中输入标准密码。“admin”的默认密码为“admin”，“user”的默认密码为“user”。
3. 单击“Login”按钮或按“Enter”键确认输入。

如果是首次登录或是在“恢复出厂默认设置并重启”之后登录，系统会提示您更改密码。新密码不可少于 6 个字符长。

成功登录后，将显示起始页面。

5.2 登录

使用 HTTPS 登录

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

1. 单击登录页面上的链接“Switch to secure HTTP”，或在 Internet 浏览器地址框中输入“https://”和设备的 IP 地址。

将显示“Certification Error Warning”，并询问您是否继续执行该操作。

2. 如果要继续执行该操作，请单击“Yes”。

将显示“基于 Web 的管理”的登录页面。

3. 在“Name”输入框中输入以下内容：

- “admin”：使用这种用户类型时，可以更改设备的设置（对组态数据进行读写访问）。
- “user”：使用这种用户类型时，无法更改设备的任何设置（对组态数据进行读访问）。

4. 在“Password”输入框中输入密码。

如果是首次登录或是在“恢复出厂默认设置并重启”后登录，则在“Password”输入框中输入标准密码。“admin”的默认密码为“admin”，“user”的默认密码为“user”。

5. 单击“Login”按钮或按“Enter”键确认输入。

如果是首次登录或是在“恢复出厂默认设置并重启”之后登录，系统会提示您更改密码。新密码不可少于 6 个字符长。

成功登录后，将显示起始页面。

5.3 “Information”菜单

5.3.1 起始页面

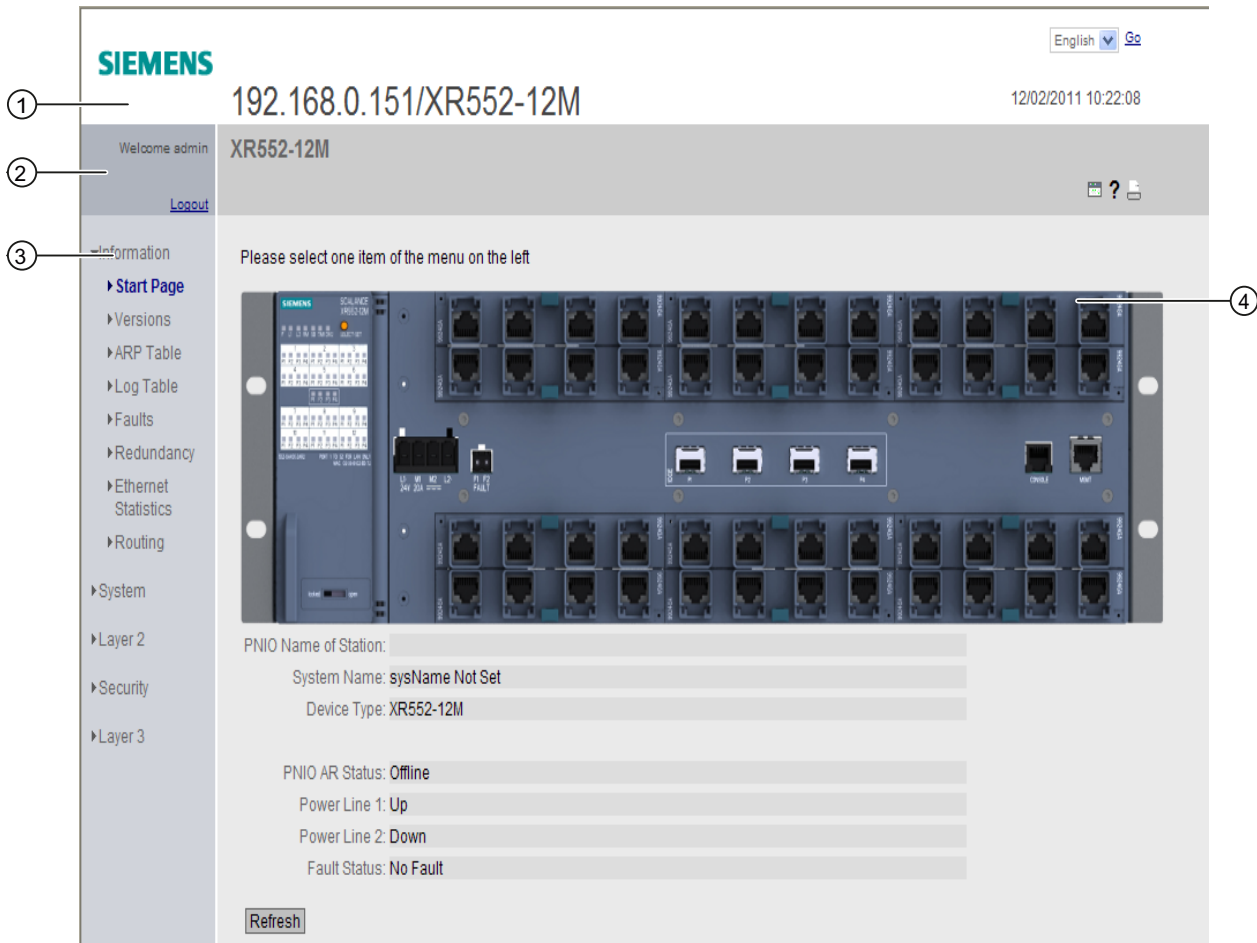
起始页面视图

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

WBM 页面的常规布局

每个 WBM 页面通常都会有以下几个区域：

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



选择区 (1)

选择区中有以下内容：

- Siemens AG 徽标
- 显示：“System Location/System Name”。
 - “System Location” 包含设备的位置。
如果使用设备出厂时的设置，则会显示设备的带内端口 IP 地址。
 - “System Name” 是设备名称。
如果使用设备出厂时的设置，则会显示设备类型。

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




- 用于选择语言的下拉列表
- 系统时间和日期

可以通过“System > System Time”更改该显示画面的内容。

显示区 (2)

在显示区的左侧，始终会显示当前所选菜单项的完整标题。

显示区的右侧包含以下项目：

- **Printer** 
单击此按钮时，将打开一个弹出窗口，其中显示针对打印机优化过的页面内容视图。
- **Help** 
单击此按钮时，将在新的浏览器窗口中打开当前所选菜单项的帮助页面。
帮助页面包含内容区的说明。在某些情况下，还会对设备上不可用的选项进行说明。
- **LED simulation** 
设备的每个组件都具有一个或多个 LED，这些 LED 会提供有关设备工作状态的信息。根据其安装位置，可能不是总能直接访问设备。因此“基于 Web 的管理”显示的是仿真 LED。未占用的插槽或未使用的连接器会显示为呈灰色显示的 LED。各种 LED 显示的含义在操作说明（精简版）进行了说明。
单击仿真的“Select/Set”按钮，可更改显示模式（LED DM 或 D1/D2）。
单击该按钮后，可以打开 LED 仿真窗口。可以在切换菜单过程中显示该窗口，并根据需要进行移动。要关闭 LED 仿真，请单击 LED 仿真窗口中的关闭按钮。
- **注销**
可以单击“Logout”链接从任何 WBM 页面注销。

浏览区 (3)

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

5.3 “Information”菜单

内容区 (4)

在导航区中单击菜单，可在内容区中显示相关 WBM 页面。

起始页面的内容区域显示以下框：

- **PNIO Name of Station**
显示 PROFINET IO 设备名称。
- **System Name**
显示设备的系统名称。
- **Device Type**
显示设备类型。
- **PNIO AR Status**
显示 PROFINET IO 应用关系状态。
 - **Online**
存在与 PROFINET IO 控制器的连接。PROFINET IO 控制器已将其组态数据下载到设备。设备可以将状态数据发送到 PROFINET IO 控制器。
在这种状态下，无法在设备上组态 PROFINET IO 控制器所设置的参数。
 - **Offline**
没有与 PROFINET IO 控制器的连接。
- **Power Line 1/Power Line 2**
 - **Up**
电源 1 或 2 已接通。
 - **Down**
电源 1 或 2 未接通或电压低于允许值。
- **Faults Status**
显示设备的故障状态。

常用按钮

WBM 页面中包含下列标准按钮：

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

说明

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

- **使用“Set Values”保存条目**

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

说明

仅在以“admin”身份登录后才可以更改组态数据。

- **使用“Create”创建条目**

在可以创建新条目的页面底部有一个“Create”按钮。单击该按钮可创建新条目。

- **使用“Delete”删除条目**

在可以删除条目的页面底部有一个“Delete”按钮。单击该按钮可将之前选择的条目从设备内存中删除。执行删除操作之后，将更新 WBM 中的页面。

- **使用“Next”向下翻页**

页面上能够显示的数据记录数受到限制。单击“Next”按钮，可向下翻页查看数据记录。

- **使用“Prev”向上翻页**

页面上能够显示的数据记录数受到限制。单击“Prev”按钮，可向上翻页查看数据记录。

5.3.2 Versions

硬件和软件的版本

该页面会显示设备的硬件和软件版本。无法对该页面上的任何内容进行组态。

Version Information			
Hardware	Name	Revision	Order ID
Basic Device	XR552-12M	3	6GK5 552-0AA00-2AR2
Slot1	MM992-4CUC	1	6GK5 992-4GA00-8AA0
Slot2	MM992-4CUC	1	6GK5 992-4GA00-8AA0
Slot4	MM992-4CUC	1	6GK5 992-4GA00-8AA0
Slot11	MM992-4CUC	1	6GK5 992-4GA00-8AA0
Software	Description	Version	Date
Firmware	X500 Firmware Signed (Test Keys)	T02.00.00.00_15.01.01	01/24/2012 20:00:00
Bootloader	X500 Release Bootloader Signed (Test-Keys) V0	T01.00.00.00_01.01.16	12/15/2011 17:30:00

显示值说明

表 1 包含以下列：

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

表 2 包含以下列：

- **Software**
 - **Firmware**

显示当前固件版本。如果下载了新的固件文件，并且尚未重启设备，则在此处显示已下载固件文件的固件版本。下次重启后会激活并使用下载的固件。
 - **Bootloader**

显示存储在设备上的引导软件的版本。
- **Description**

显示软件的简要说明。
- **Version**

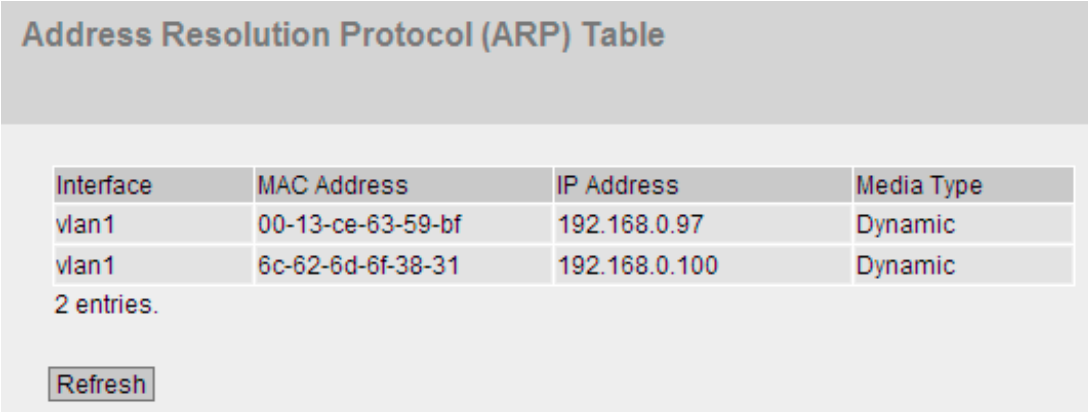
显示软件版本的版本号。
- **Date**

显示软件版本的创建日期。

5.3.3 ARP 表

MAC 地址和 IP 地址的分配

ARP 表（地址解析协议）显示已知 IP 地址对应的 MAC 地址。该子菜单页面还会指示访问相关地址时所使用的接口。最后一列指示如何获取信息。无法对该页面上的任何内容进行组态。



Interface	MAC Address	IP Address	Media Type
vlan1	00-13-ce-63-59-bf	192.168.0.97	Dynamic
vlan1	6c-62-6d-6f-38-31	192.168.0.100	Dynamic

2 entries.

显示值说明

该表格包括以下列：

- **Interface**
显示获取行条目所用的接口。
- **MAC Address**
显示目标设备的 MAC 地址。
- **IP Address**
显示目标设备的 IP 地址。
- **Media Type**
显示连接的类型。
 - **Dynamic**
设备自动识别到地址数据。

5.3.4 日志表

记录事件

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

即使在设备关闭后，事件日志表的内容仍可保留。

无法对该页面上的任何内容进行组态。

Restart	System Up Time	Log Message
1	00:48:35	09/14/2011 10:39:04 (R)STP: topology change detected.
1	00:44:46	09/14/2011 10:35:15 Link up on P1.4.
1	00:27:48	09/14/2011 10:18:17 (R)STP: topology change detected.
1	00:27:48	09/14/2011 10:18:17 Link down on P1.4.
1	00:27:28	09/14/2011 10:17:57 Link up on P1.4.
1	00:19:39	09/14/2011 10:10:08 (R)STP: topology change detected.
1	00:19:39	09/14/2011 10:10:08 Link up on LA1.
1	00:16:45	09/14/2011 10:07:14 (R)STP: topology change detected.
		09/14/2011 10:07:14

1 - 10 of 28 entries. [Show all](#) 1 ▾ [Next](#)

5.3 “Information”菜单

显示值说明

该表格包括以下列：

- **System > Events**
统计自上次复位为出厂设置以来的重启次数，并显示在其后发生过相应事件的设备重启。
- **系统运行时间 (System Up Time)**
显示在所描述的事件发生时设备自上次重启以来已持续运行的时间。
- **Log Message**
显示已发生事件的简要说明。

如果已设定系统时间，则还会显示事件发生的时间。

按钮描述

“Clear”按钮

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

说明

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

按钮“Show all”

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

“Next”按钮

单击该按钮可转至下一页。

“Prev”按钮

单击该按钮可转至上一页。

用于更改页面的下拉列表

从该下拉列表中选择要转至的页面。

5.3.5 故障

错误状态

此页面显示所发生的所有错误。“Cold/Warm Start”事件的错误可在确认后删除。

如果已没有未回应的错误/故障消息，则故障 LED 将熄灭。

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

Faults		
System Up Time	Fault Description	Clear Fault State
9s	Power down on line 2.	<input type="button" value="Clear Fault State"/>
10s	Link down on P1.	<input type="button" value="Clear Fault State"/>
10s	Warm start performed.	<input type="button" value="Clear Fault State"/>

显示值说明

该表包含以下列：

- **系统运行时间 (System Up Time)**
显示在所描述的故障发生时设备自上次重启以来已持续运行的时间。
- **Fault Description**
显示设备的故障状态。
- **Clear Fault State**
要删除“Cold/Warm Start”事件的文件，可单击“Clear Fault State”按钮。

5.3 “Information”菜单

5.3.6 冗余

5.3.6.1 生成树

简介

该页面显示有关生成树和根网桥设置的最新信息。

Spanning Tree

Spanning Tree | VRRP Statistics

Spanning Tree Mode: MSTP

Instance ID: 0

Bridge Priority: 32768

Bridge Address: 08-00-06-4b-67-01

Root Priority: 32768

Root Address: 00-0e-8c-8d-09-34

Regional Root Priority: 32768

Regional Root Address: 08-00-06-4b-67-01

Port	Role	State	Priority	Path Cost	Edge Type	P.t.P. Type
P0.4	Designated	Forwarding	128	20000	No Edge Port	Shared Media
P1.1	Designated	Forwarding	128	20000	Edge Port	P.t.P
P1.3	Designated	Forwarding	128	20000	Edge Port	P.t.P
P1.4	Designated	Forwarding	128	20000	Edge Port	P.t.P
P10.3	Designated	Forwarding	128	20000	No Edge Port	P.t.P
P11.1	Designated	Forwarding	128	20000	No Edge Port	P.t.P
P11.4	Root	Forwarding	128	20000	No Edge Port	P.t.P

Set Values Refresh

显示值说明

该页面显示以下字段：

- **Spanning Tree Mode**
显示设置的模式。在“Layer 2 > Configuration”和“Layer 2 > MSTP > General”中指定模式。
可以使用以下值：
 - '1'
 - STP
 - RSTP
 - MSTP
- **Instance ID**
显示实例编号。该参数取决于组态的模式。
- **Bridge Priority / Root Priority**
哪个设备成为根网桥由网桥优先级决定。优先级最高的网桥（换句话说，此参数的值最小）将成为根网桥。如果网络中有多个设备具有相同优先级，则 MAC 地址数值最小的设备将成为根网桥。网桥优先级和 MAC 地址这两个参数一起构成网桥标识符。由于根网桥管理所有路径的变更，出于帧延迟的考虑，根网桥应该尽可能处在中心位置。网桥优先级的值是 4096 的整数倍数，值范围从 0 到 32768。
- **Bridge Address/ Root Address**
网桥地址显示设备的 MAC 地址，根地址显示根交换机的 MAC 地址。
- **Regional Root Priority**（仅适用于 MSTP）
相关描述，请参见“Bridge Priority/Root Priority”。
- **Regional Root Address**（仅适用于 MSTP）
显示设备的 MAC 地址。

该表格包括以下列：

5.3 “Information”菜单

- **Port**

显示设备通信所用的端口。
- **Role**

显示端口状态。可能的值包括：

 - **Disabled**

已从生成树中手动移除端口，生成树将不再考虑该端口。
 - **Designated**

端口从根网桥中转移数据。
 - **Alternate**

端口具有指向网段的备用路径。
 - **Backup**

如果交换机具有多个指向同一网段的端口，则“较差”端口将变为备用端口。
 - **Root**

端口提供指向根网桥的最佳路径。
 - **Master**

此端口指向 MST 区域外部的根网桥。
- **State**

显示端口的当前状态。仅显示这些值。具体参数取决于组态的协议。可能的状态如下：

 - **Discarding**

端口接收 BPDU 帧。其它进入或离开的帧会被丢弃。
 - **Listening**

端口接收和发送 BPDU 帧。端口包括在生成树算法中。其它进入或离开的帧会被丢弃。
 - **Learning**

端口主动学习拓扑，即学习节点地址。其它进入或离开的帧会被丢弃。
 - **Forwarding**

经过重新组态时间后，端口在网络中激活。该端口接收和发送数据帧。
- **Priority**

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

- **Path Cost**

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

如果“Cost Calc”字段中的值为“0”，则显示自动计算出的值。否则，显示“Cost Calc”字段的值。

路径成本的计算很大程度上基于传输速度。可达到的传输速度越高，路径成本的值就越低。

快速生成树的典型路径成本值如下：

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

- **Edge Type**

显示连接类型。可能的值包括：

- **Edge Port**
此端口上有终端设备。
- **No Edge Port**
此端口上有生成树或快速生成树设备。

- **P.t.P. Type**

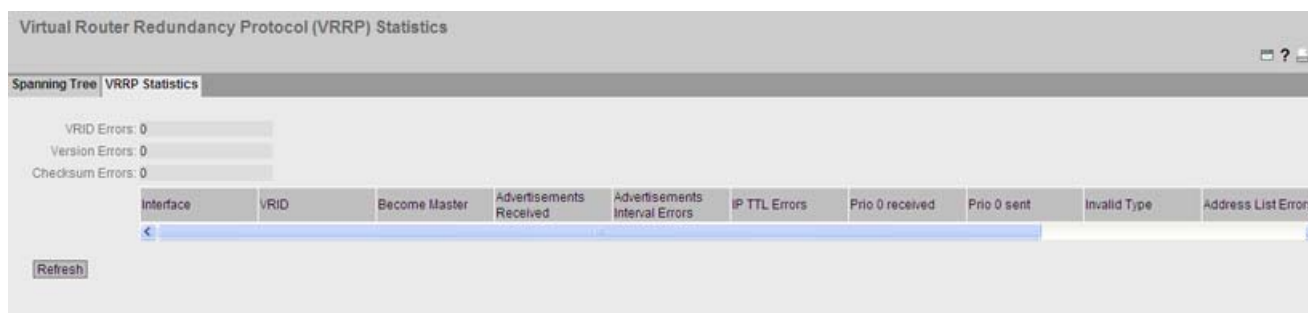
显示点对点链路类型。可能的值包括：

- **P.t.P.**
即使为半双工，也认为是点对点链路。
- **Shared Media**
即使为全双工连接，也不认为是点对点链路。

5.3.6.2 VRRP 统计信息

简介

此页面显示 VRRP 协议以及全部组态虚拟路由器的统计信息。



显示值说明

该页面显示以下字段：

- **VRID Errors**
显示包含不受支持的 VRID 的已接收 VRRP 数据包的数量。
- **Version Errors**
显示包含无效版本号的已接收 VRRP 数据包的数量。
- **Checksum Errors**
显示包含无效校验和的已接收 VRRP 数据包的数量。

该表格包括以下列：

- **Interfaces**
与设置相关的接口。
- **VRID**
显示虚拟路由器的 ID。
有效值为 1 到 255。
- **Become Master**
显示该虚拟路由器变为“主设备”状态的频率。
- **Advertisements Received**
显示接收到包含不良地址列表的 VRRP 数据包的频率。
- **Advertisements Interval Errors**
显示已接收到间隔与本地设置的值不匹配的不良 VRRP 数据包的数量。

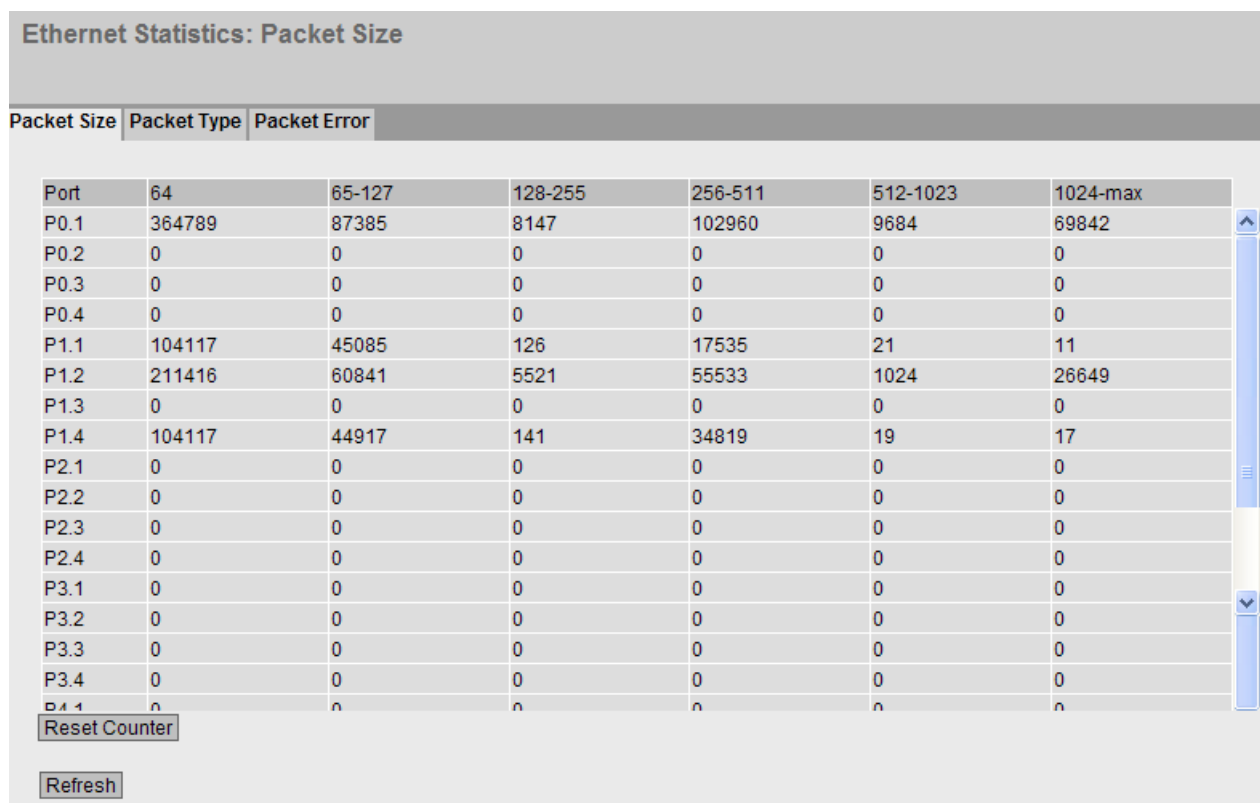
- **IP TTL Errors**
显示已接收到 IP 报头中的 TTL（Time to live，生存时间）值不正确的不良 VRRP 数据包的数目。
- **Prio 0 received**
显示已接收的优先级为 0 的 VRRP 数据包的数目。主路由器关闭时，发送优先级为 0 的 VRRP 数据包。这些数据包允许快速切换至相关的备用路由器。
- **Prio 0 sent**
显示已发送的优先级为 0 的 VRRP 数据包的数目。主路由器关闭时，将发送优先级为 0 的数据包。这些数据包允许快速切换至相关的备用路由器。
- **Invalid Auth. Type**
显示已接收到验证类型不为类型 0 的不良 VRRP 数据包的数目。类型 0 表示“无验证”。
- **Auth. Type Mismatch**
显示已接收到验证类型不匹配的不良 VRRP 数据包的数目。
- **Packet Length Error**
显示已接收到长度不正确的不良 VRRP 数据包的数目。

5.3.7 以太网统计信息

5.3.7.1 数据包大小

按长度分类的帧

该页面会显示每个端口发送并接收了多少个不同大小的帧。无法对该页面上的任何内容进行组态。



The screenshot shows a table titled "Ethernet Statistics: Packet Size". The table has columns for "Packet Size" (64, 65-127, 128-255, 256-511, 512-1023, 1024-max), "Packet Type", and "Packet Error". The "Packet Size" column is further divided into sub-columns for each size range. The rows represent different ports (P0.1 to P3.4). A "Reset Counter" button is visible at the bottom left, and a "Refresh" button is at the bottom center. A vertical scrollbar is on the right side of the table.

Port	Packet Size						Packet Type	Packet Error
	64	65-127	128-255	256-511	512-1023	1024-max		
P0.1	364789	87385	8147	102960	9684	69842		
P0.2	0	0	0	0	0	0		
P0.3	0	0	0	0	0	0		
P0.4	0	0	0	0	0	0		
P1.1	104117	45085	126	17535	21	11		
P1.2	211416	60841	5521	55533	1024	26649		
P1.3	0	0	0	0	0	0		
P1.4	104117	44917	141	34819	19	17		
P2.1	0	0	0	0	0	0		
P2.2	0	0	0	0	0	0		
P2.3	0	0	0	0	0	0		
P2.4	0	0	0	0	0	0		
P3.1	0	0	0	0	0	0		
P3.2	0	0	0	0	0	0		
P3.3	0	0	0	0	0	0		
P3.4	0	0	0	0	0	0		

显示值说明

该表格包括以下列：

- **Port**
显示可用端口和链路汇聚。端口由端口号和插槽号组成，例如，端口 0.1 表示插槽 0，端口 1。

说明

帧统计信息显示

在与帧大小相关的统计信息中，需要注意的是，会同时对进入帧和离开帧进行计数。

- **Frame lengths**

端口号后面的其它各列包含按照帧长度分类的进入帧的绝对数量。

帧长度分为以下几类：

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

按钮描述

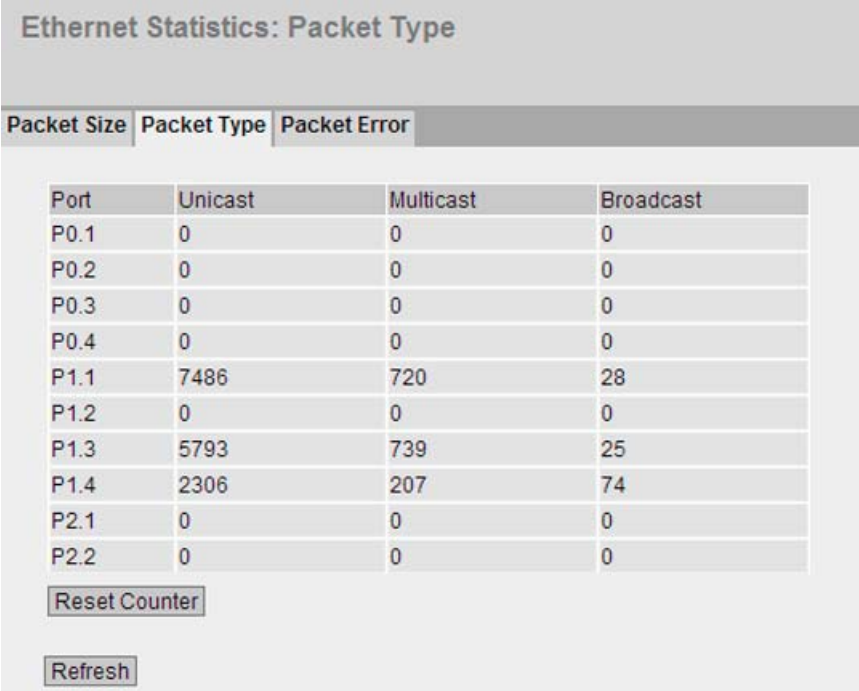
“Reset Counters”按钮

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

5.3.7.2 数据包类型

按类型分类的已接收帧

该页面显示每个端口接收到多少“Unicast”、“Multicast”和“Broadcast”类型的帧。无法对该页面上的任何内容进行组态。



Packet Size	Packet Type	Packet Error	
Port	Unicast	Multicast	Broadcast
P0.1	0	0	0
P0.2	0	0	0
P0.3	0	0	0
P0.4	0	0	0
P1.1	7486	720	28
P1.2	0	0	0
P1.3	5793	739	25
P1.4	2306	207	74
P2.1	0	0	0
P2.2	0	0	0

Reset Counter

Refresh

显示值说明

该表格包括以下列：

- **Port**
显示可用端口和链路汇聚。端口由端口号和插槽号组成，例如，端口 0.1 表示插槽 0，端口 1。
- **Unicast/Multicast/Broadcast**
端口号之后的其它各列包括按照其帧类型“Unicast”、“Multicast”和“Broadcast”分类的到达帧的绝对数量。

按钮描述

“Reset Counters”按钮

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

5.3.7.3 数据包错误

接收到的坏帧

该页面显示每个端口接收到多少坏帧。无法对该页面上的任何内容进行组态。

Ethernet Statistics: Packet Error						
Packet Size	Packet Type	Packet Error				
Port	CRC	Undersize	Oversize	Fragments	Jabbers	Collisions
P0.1	0	0	0	0	0	0
P0.2	0	0	0	0	0	0
P0.3	0	0	0	0	0	0
P0.4	0	0	0	0	0	0
P1.1	0	0	0	0	0	0
P1.2	0	0	0	0	0	0
P1.3	0	0	0	6	0	6
P1.4	0	0	0	0	0	0

Reset Counter

Refresh

显示值说明

该表格包括以下列：

- **Port**
显示可用端口和链路汇聚。端口由端口号和插槽号组成，例如，端口 0.1 表示插槽 0，端口 1。
- **错误类型**
端口号之后的其它各列包括按照其错误类型分类的到达帧的绝对数量。

在该表的各列中，将根据以下错误类型进行区分：

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

5.3 “Information”菜单

- **Jabbers**
包含错误 CRC 校验和且由于长度过长而被丢弃的带 VLAN 标记的数据包。
- **Collisions**
检测到的冲突。

按钮描述

“Reset Counters”按钮

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

5.3.8 路由

5.3.8.1 路由表

简介

此页用于显示设备的路由表。

Layer 3: Routing Table					
Routing Table	OSPFv2 Interfaces	OSPFv2 Neighbors	OSPFv2 Virtual Neighbors	OSPFv2 LSDB	
Destination Network	Subnet Mask	Gateway	Interface	Metric	Routing Protocol
120.80.0.0	255.255.0.0	0.0.0.0	vlan1	0	Connected
152.80.1.0	255.255.255.0	162.80.1.1	P3.1	2	OSPF
162.80.1.0	255.255.255.0	0.0.0.0	P3.1	0	Connected
172.80.1.0	255.255.255.0	0.0.0.0	vlan3	0	Connected
182.80.1.0	255.255.255.0	172.80.1.2	vlan3	2	OSPF

显示值说明

该表格包括以下列：

- **Destination Network**
显示此路由的目标地址。
- **Subnet Mask**
显示此路由的子网掩码。
- **Gateway**
显示此路由的网关。
- **Interface**
显示此路由的接口。

5.3 “Information”菜单

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

5.3.8.2 OSPFv2 接口

概述

此页面用于显示 OSPF 接口的组态。

Open Shortest Path First v2 (OSPFv2) Interfaces						
Routing Table	OSPFv2 Interfaces	OSPFv2 Neighbors	OSPFv2 Virtual Neighbors	OSPFv2 LSDB		
IP Address	Area ID	Interface Status	OSPF Status	Designated Router	Backup Designated Router	Events
120.80.1.18	0.0.0.0	Designated Router	enabled	120.80.1.18	0.0.0.0	2
162.80.1.2	3.0.0.0	Designated Router	enabled	162.80.1.2	162.80.1.1	3
172.80.1.1	3.0.0.0	Backup D. Router	enabled	172.80.1.2	172.80.1.1	4

Refresh

显示值说明

该表格包括以下列：

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

- **Interface Status**

显示接口状态：

- Down
接口无法使用。
- Loop back
回路反向接口。
- Waiting
启动并协商接口。
- Point to Point
点对点链路
- Designated Router
路由器为指定路由器并生成网络 LSA。
- Backup D. Router
路由器为指定路由器的备用路由器。
- Other D. Router
接口已启动。该路由器既不是指定路由器也不是指定备用路由器。

- **OSPF Status**

显示 OSPF 状态。

- Enabled: 在接口中启用 OSPF。
- Disabled: 在接口中禁用 OSPF。

- **Designated Router**

显示针对该 OSPF 接口指定的路由器的 IP 地址。

- **Backup Designated Router**

显示针对该 OSPF 接口指定的备用路由器的 IP 地址。

- **Events**

显示 OSPF 状态变化次数。

5.3.8.3 OSPFv2 邻居

概述

该页面用于显示在相关网络中动态检测到的邻近路由器。

Open Short Path First v2 (OSPFv2) Neighbors							
Routing Table	OSPFv2 Interfaces	OSPFv2 Neighbors	OSPFv2 Virtual Neighbors	OSPFv2 LSDB			
IP Address	Router ID	Status	Assoc. Area Type	Priority	Hello Suppr.	Retrans Queue	Events
162.80.1.1	1.1.1.1	full	Normal	1	2	0	6
172.80.1.2	3.3.3.3	full	Normal	1	2	0	6

Refresh

显示值说明

该表格包括以下列：

- **IP Address**
显示该网络中邻居路由器的 IP 地址。
- **Neighbor Router ID**
显示邻居路由器的 ID。这两个地址可以相同。
- **Status**
显示邻居路由器状态。状态可采用以下值：
 - unknown
邻居路由器的状态未知。
 - down
无法访问邻居路由器。
 - attempt and init
初始化过程中的状态概要
 - two-way
双向接收呼叫数据包。指定路由器和指定备份路由器的规范。
 - exchangestart, exchange and loading
交换 LSA 时的状态
 - full
数据库在区域中完整并同步。现在可以检测到路由。

说明

标准状态

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

- **Assoc. Area Type**

显示用以维持邻居关系的区域类型。存在以下区域类型：

- 标准 (Standard)
- 存根 (Stub)
- NSSA
- 骨干

- **Priority**

显示邻居路由器优先级。仅在选择网络中的指定路由器时有意义。该信息与虚拟邻居路由器无关。

- **Hello Suppr.**

显示发送给邻居路由器的受抑制呼叫数据包。该字段通常显示“no”。

- **Retrans Queue**

显示仍要传输的呼叫数据包的队列长度。

- **Events**

显示状态变化次数。

5.3.8.4 OSPFv2 虚拟邻居

概述

此页面用于显示已组态的虚拟邻居。

Open Short Path First v2 (OSPFv2) Neighbors						
Routing Table	OSPFv2 Interfaces	OSPFv2 Neighbors	OSPFv2 Virtual Neighbors	OSPFv2 LSDB		
IP Address	Router ID	Status	Transit Area ID	Hello Suppr.	Retrans Queue	Events
162.80.1.1	1.1.1.1	full	3.0.0.0	1	0	5
172.80.1.2	3.3.3.3	full	3.0.0.0	1	0	5

Refresh

显示值说明

该表格包括以下列：

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

- **Status**

显示邻居路由器状态。状态可采用以下值：

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

说明

标准状态

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

- **Trans.Area ID**

显示通过其存在虚拟邻居关系的区域的 ID。

- **Hello Suppr.**

显示是否有发送给虚拟邻居路由器的受抑制呼叫数据包。

- **no:** 没有受抑制呼叫数据包。（默认值）
- **yes:** 有受抑制呼叫数据包。

- **Retrans Queue**

显示仍要传输的呼叫数据包的队列长度。

- **Events**

显示状态变化次数。

5.3.8.5 OSPFv2 LSDB

概述

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

Open Shortest Path First v2 (OSPFv2) Link State Database				
Routing Table	OSPFv2 Interfaces	OSPFv2 Neighbors	OSPFv2 Virtual Neighbors	OSPFv2 LSDB
Area ID	Link State Type	Link State ID	Router ID	Sequence No
0.0.0.0	Router	1.1.1.1	1.1.1.1	-2147483645
0.0.0.0	Router	2.2.2.2	2.2.2.2	-2147483600
0.0.0.0	Router	3.3.3.3	3.3.3.3	-2147483645
3.0.0.0	Network	162.80.1.2	2.2.2.2	-2147483606
3.0.0.0	Network	172.80.1.2	3.3.3.3	-2147483606
3.0.0.0	Summary	120.80.0.0	2.2.2.2	-2147483605
3.0.0.0	Summary	152.80.1.0	1.1.1.1	-2147483606
3.0.0.0	Summary	182.80.1.0	3.3.3.3	-2147483605

Refresh

显示框说明

该表格包括以下列：

- **Area ID**
显示 LSA 所属的区域的 ID。如果 LSA 是外部连接，则显示“-”。
- **Link State Type**
显示 LSA 类型。可能的值包括：
 - unknown
LSA 类型未知。
 - Router
路由器 LSA（类型 1）在一定区域中由 OSPF 路由器发送。LSA 包含了所有路由器接口状态方面的信息。
 - Network
网络 LSA（类型 2）在一定区域中由指定路由器发送。LSA 包含了连接到网络的路由器的列表。

- **NSSA External**
NSSA 外部 LSA（类型 7）在一定 NSSA 中由 NSSA-ASBR 发送。NSSA-ASBR 接收类型 5 的 LSA 并将其信息转换为类型 7 的 LSA。NSSA 路由器可以在一定 NSSA 中转发这些 LSA。
- **Summary**
汇总 LSA（类型 3）在一定区域中由 ABR 发送。LSA 包含了到其它网络的路由的信息。
- **AS Summary**
AS 汇总 LSA（类型 4）在一定区域中由区域边界路由器发送。LSA 包含了到其它自治系统的路由的信息。
- **AS External**
AS 外部 LSA（类型 5）在自治系统中由 AS 边界路由器发送。LSA 包含了从一个网络到另一个网络路由器的信息。
- **Link State ID**
显示 LSA 的 ID。
- **Router ID**
显示发送此 LSA 的路由器 ID。
- **Sequence No.**
显示 LSA 的序号。每次更新 LSA 后，该序号就会加一。

5.4 “System”菜单

5.4.1 组态

系统组态

该页面包含设备访问选项的组态概览。

可在此指定访问设备时要使用的服务。对于某些服务提供了更多组态页面，可在其中进行更加具体的设置。

System Configuration

[Trial Mode Active – Press "Write Startup Config" button to make your settings persistent](#)

Telnet Server
 SSH Server
 HTTPS Server only
 SMTP Client
 Syslog Client

DCP Server: Read-Only

Time: Manual

SNMP: SNMPv1v2cv3
 SNMPv1v2 Read-Only
 SNMPv1 Traps
 DHCP Client

Configuration Mode: Trial

显示框说明

该页面包含以下框：

- **复选框“Telnet Server”**
启用或禁用“Telnet Server”服务，以便不加密访问 CLI。
- **复选框“SSH Server”**
启用或禁用“SSH Server”服务，以便加密访问 CLI。
- **复选框“HTTPS Server only”**
启用或禁用通过 HTTPS 进行访问。

- **复选框 SMTP Client**
启用或禁用 SMTP 客户端。可以在“System > SMTP Client”中组态其它设置。
- **复选框“Syslog Client”**
启用或禁用 Syslog 客户端。可以在“System > Syslog Client”中组态其它设置。
- **下拉列表“DCP Server”**
指定是否可通过 DCP（Discovery and Configuration Protocol，发现和组态协议）访问设备：
 - “-”（已禁用）
DCP 已禁用。既不能读取也不能修改设备参数。
 - Read/Write
通过 DCP，既可读取又可修改设备参数。
 - Read Only
可用 DCP 读取设备参数，但不能对设备参数进行修改。
- **下拉列表“Time”**
从下拉列表中选择设置。可能的设置如下：
 - Manual
手动设置系统时间。可以在“System > Time > Manual Setting”中组态其它设置。
 - SNTP Client
通过 SNTP 服务器设置系统时间。可以在“System > System Time > SNTP Client”中组态其它设置。
 - NTP Client
通过 NTP 服务器设置系统时间。可以在“System > System Time > NTP Client”中组态其它设置。
 - SIMATIC Time
通过 SIMATIC 时间发送器设置系统时间。可以在“System > System Time > SIMATIC Time Client”中组态其它设置。
- **下拉列表“SNMP”：**
从下拉列表中选择协议。可能的设置如下：
 - “-”（SNMP 已禁用）
不能通过 SNMP 访问设备参数。
 - SNMPv1/v2c/v3
可以通过 SNMP 版本 1、2c 或 3 访问设备参数。可以在“System > SNMP > General”中组态其它设置。
 - SNMPv3
只能通过 SNMP 版本 3 访问设备参数。可以在“System > SNMP > General”中组态其它设置。

5.4 “System”菜单

- **复选框“SNMPv1/v2 Read-Only”**
启用或禁用通过 SNMPv1/v2c 对 SNMP 变量进行写访问。
- **复选框“SNMPv1 Traps”**
启用或禁用发送陷阱（报警帧）。可以在“System > SNMP > Traps”中组态其它设置。
- **复选框“DHCP Client”**
启用或禁用 DHCP 客户端。可以在“System > DHCP Client”中组态其它设置。
- **下拉列表“Configuration Mode”:**

从下拉列表中选择模式。可能的模式如下：

– **Automatic**

自动保存模式。在最后修改参数的约 1 分钟后或重启设备时，自动保存组态。

– **Trial**

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

要将更改保存在组态文件中，需使用“Write Startup Config”按钮。设置了试用模式时会显示“Write Startup Config”按钮。在显示区中，只要存在未保存的更改，就会显示消息“Trial Mode Active - Press "Write Startup Config" button to make your settings persistent.”。可以在每个 WBM 页面上看到这条消息，直至所做的更改已保存或设备已重启。

组态步骤

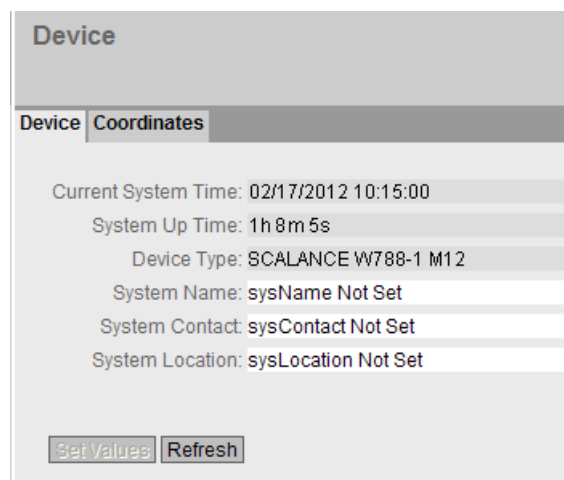
1. 要使用所需功能，请选中相应的复选框。
2. 从下拉列表中选择所需选项。
3. 单击“Set Values”按钮。

5.4.2 General

5.4.2.1 设备

常规设备信息

该页面包含常规设备信息。



The screenshot shows a web interface titled "Device" with a tabbed menu where "Coordinates" is selected. Below the menu, several system parameters are displayed in a list:

- Current System Time: 02/17/2012 10:15:00
- System Up Time: 1h 8m 5s
- Device Type: SCALANCE W788-1 M12
- System Name: sysName Not Set
- System Contact: sysContact Not Set
- System Location: sysLocation Not Set

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

无法更改“Current System Time”、“System Up Time”和“Device Type”框。

显示框说明

该页面包含以下框：

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

5.4 “System”菜单

- **输入框“System Contact”**
可输入设备管理责任人的名字。最多支持 255 个字符。
- **输入框“System Location”**
可输入设备的安装位置。输入的安装位置显示在选择区域中。最多支持 255 个字符。

说明

输入框中使用 ASCII 码 0x20 至 0x7e。

组态步骤

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

5.4.2.2 坐标

有关地理坐标的信息

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

获取坐标

使用适当的地图来获取设备的地理坐标。

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

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

Set Values Refresh

显示框说明

该页面包含以下框。这些是最多可包含 32 个字符的纯信息框。

- **输入框“Latitude”**

地理纬度：在此输入设备位置的北纬值或南纬值。

例如， $+49^{\circ} 1' 31.67''$ 表示设备位于北纬 49 度、1 弧分和 31.67 弧秒。

通过在前面加上负号显示南纬度。

还可以在数字信息后面附加字母 N（北纬）或 S（南纬），如 $49^{\circ} 1' 31.67'' N$ 。

- **输入框“Longitude”**

地理经度：在此输入设备位置的东经或西经值。

例如， $+8^{\circ} 20' 58.73''$ 表示设备位于东经 8 度、20 分和 58.73 秒。

通过在经度前面加上负号表示西经。

还可以在数字信息前面加上字母 E（东经）或 W（西经），如 $8^{\circ} 20' 58.73'' E$ 。

- **输入框：“Height”**

地理高度：在此输入地理海拔高度的米数值。

例如，158 m 表示设备位于海平面上 158 m 高的位置。

对于低于海平面的高度（例如死海），可在前面添加负号来表示。

组态步骤

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

5.4.3 Agent IP

组态 IP 地址

在此处为设备指定 IP 组态。

Agent Internet Protocol (IP)	
In-Band	Out-Band
IP Address: 192.168.0.154	IP Address: 0.0.0.0
Subnet Mask: 255.255.255.0	Subnet Mask: 0.0.0.0
Default Gateway: 192.168.0.254	
Agent VLAN ID: VLAN1	
MAC Address: 08-00-06-4b-67-3f	MAC Address: 08-00-06-4b-67-3e

Set Values Refresh

说明

带内接口以及带外接口的 IP 地址必须属于分属不同的子网。

显示框说明

该页面包含以下框：

- **输入框“IP Address”**
在“In-Band”中输入 IP 地址，经由此 IP 地址，可以通过交换机端口访问管理工具。在“Out-Band”中输入 IP 地址，经由此 IP 地址，可以通过带外端口访问管理工具。如果更改 IP 地址，网页浏览器会自动调整到新地址。如果未发生自动导向，则请在 Web 浏览器中手动输入新地址。
- **文本框“Subnet Mask”**
在“In-Band”中输入 CPU 模块的子网掩码，在“Out-Band”中输入带外端口的子网掩码。

- **文本框“Default Gateway”**

如果需要设备与其它子网中的设备（诊断站、电子邮件服务器等）进行通信，则应在此输入默认网关的 IP 地址。不可通过其它子网访问带外端口。

- **下拉列表“Agent VLAN ID”**

从下拉列表中选择带内管理的 VLAN ID。只可以选择已组态的 VLAN。

说明**更改代理 VLAN ID**

如果组态 PC 通过以太网直接连接到设备，并且更改了代理 VLAN ID，则更改后不再可以通过以太网访问该设备。

- **文本框“MAC Address”**

显示设备的 MAC 地址。MAC 地址与硬件关联，且无法修改。

组态步骤

请按照以下步骤组态带内接口：

1. 在“In Band”下的输入框中，输入 IP 地址、子网掩码和默认网关。
2. 从“Agent VLAN ID”下拉列表中选择分配的 VLAN ID。
3. 单击“Set Values”按钮。

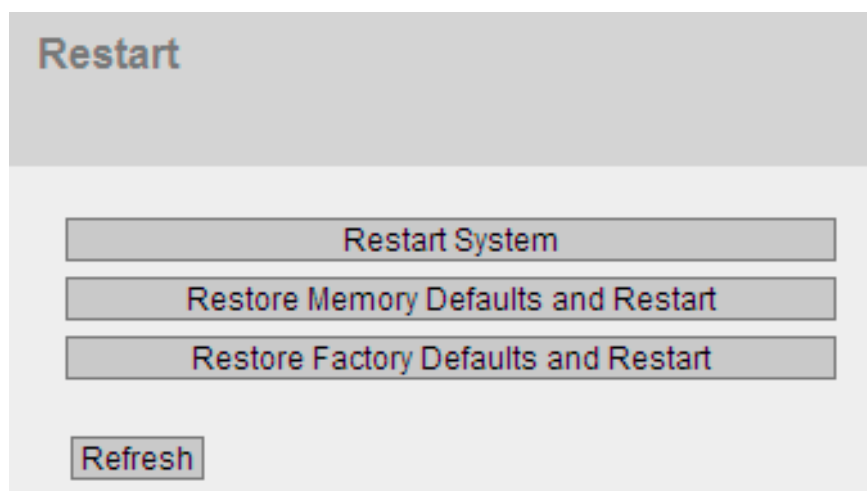
请按照以下步骤组态带外接口：

1. 在“Out Band”下的输入框中，输入 IP 地址和子网掩码。
2. 单击“Set Values”按钮。

5.4.4 重启

复位为默认设置

在此菜单中，有一个可用来重新启动设备的按钮，以及用于复位到设备默认值的各种选项。



说明

对于重启设备，请注意以下几点：

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

显示框说明

为重启设备，该页面上的按钮提供了以下选项：

- **“Restart System”按钮**

单击该按钮可重启系统。必须在对话框中确认重启操作。重启期间，将重新初始化设备，重新加载内部固件，并且设备会执行自检。此外会删除地址表中已学习到的条目。在设备重启期间，可以不关闭浏览器窗口。然后需要再次登录。

- **“Restore Memory Defaults and Restart”按钮**

单击此按钮可以恢复除以下参数外的出厂组态设置并重启：

- IP 地址
- 子网掩码
- 默认网关的 IP 地址
- DHCP 客户端 ID
- DHCP
- 系统名称
- 系统位置
- 系统联系人
- STP 设置
- 链路汇聚

- **“Restore Factory Defaults and Restart”按钮**

单击此按钮可以恢复组态的出厂默认设置。同时会复位受保护的默认设置。将触发自动重启。

说明

将所有默认设置复位为出厂设置时，IP 地址和密码均会丢失。之后，只能通过 Primary Setup Tool 或 DHCP 访问设备。

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

5.4 “System”菜单

5.4.5 加载和保存

5.4.5.1 HTTP

通过 HTTP 加载和保存数据

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

说明

与先前版本的不兼容性

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

说明

组态文件和试用模式/自动保存模式

在自动保存模式下，组态文件（ConfigPack 和 Config）传输前数据会自动保存。在试用模式下，虽然会采用更改，但不会将更改保存在组态文件（ConfigPack 和 Config）中。在“System > Configuration”WBM 页面中使用“Write Startup Config”按钮将更改保存在组态文件中。

Load and Save via HTTP				
HTTP TFTP				
Type ▲	Description	Load	Save	Delete
Config	Startup Configuration	Load	Save	
ConfigPack	Startup Config, Users and Certificates	Load	Save	
Debug	Debug Information for Siemens Support		Save	Delete
Firmware	Firmware Update	Load	Save	
HTTPSCert	HTTPS Certificate	Load	Save	Delete
LogFile	Event Log (ASCII)		Save	
MIB	SCALANCE MSPS MIB		Save	
Users	Users and Passwords	Load	Save	

Refresh

显示框说明

该表格包括以下列：

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

说明

更新固件之后，请删除 Web 浏览器的缓存。

组态步骤

使用 HTTP 加载文件

1. 单击“Load”按钮之一启动加载功能。
将打开用于上传文件的对话框。
2. 转至要上传的文件。
3. 单击对话框中的“Open”按钮。
随即可上传文件。
4. 加载后，请重启设备。更改只在重启后生效。

使用 HTTP 保存文件

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

使用 HTTP 删除文件

1. 单击“Delete”按钮之一启动删除功能。
文件将被删除。

复用组态数据

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

要复用组态数据，请按以下步骤操作：

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

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

5.4.5.2 TFTP

通过 TFTP 服务器加载和保存数据

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

说明

与先前版本的不兼容性

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

说明

组态文件和试用模式/自动保存模式

在自动保存模式下，组态文件（ConfigPack 和 Config）传输前数据会自动保存。在试用模式下，虽然会采用更改，但不会将更改保存在组态文件（ConfigPack 和 Config）中。在“System > Configuration”WBM 页面中使用“Write Startup Config”按钮将更改保存在组态文件中。

Load and Save via TFTP

TFTP TFTP

TFTP Server IP Address: 0.0.0.0
TFTP Server Port: 69

Type ▲	Description	Filename	Actions
Config	Startup Configuration	config_SCALANCE_XR-500.conf	Select action ▼
ConfigPack	Startup Config, Users and Certificates	configpack_SCALANCE_XR-500.zip	Select action ▼
Debug	Debug Information for Siemens Support	debug_SCALANCE_XR-500.bin	Select action ▼
Firmware	Firmware Update	firmware_SCALANCE_XR-500.sfw	Select action ▼
HTTPSCert	HTTPS Certificate	https_cert	Select action ▼
LogFile	Event Log (ASCII)	logfile_SCALANCE_XR-500.log	Select action ▼
MIB	SCALANCE MSPS MIB	msspsmaster.mib	Select action ▼
Users	Users and Passwords	users.enc	Select action ▼

Get Values Refresh

显示框说明

该页面包含以下框：

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

该表格包括以下列：

- **Type**
显示文件类型。
- **Description**
显示文件类型的简要说明。
- **输入框“Filename”**
输入文件名。
- **下拉列表“Actions”**
从下拉列表中选择动作。可供选择的选项取决于所选文件类型，例如，只能保存日志文件。
相关选项如下：
 - **Save file**
通过该选项将文件保存到 TFTP 服务器上。
 - **Load file**
通过该选项加载 TFTP 服务器中的文件。

组态步骤

通过 TFTP 加载或保存数据

1. 在“TFTP Server IP Address”输入框中输入 TFTP 服务器的 IP 地址。
2. 在“TFTP Server Port”输入框中输入要使用的服务器端口。
3. 在“Filename”输入框中输入要保存数据或从中获取数据的文件的名称。
4. 从“Actions”下拉列表中选择要执行的操作。
5. 单击“Set Values”按钮启动所选操作。
6. 加载组态和 SSL 证书之后，重启设备。更改只在重启后生效。

复用组态数据

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

要复用组态数据，请按以下步骤操作：

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

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

5.4.6 事件

选择系统事件

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

Events

Signaling Contact Method: conventional ▾

Signaling Contact Status: open ▾

Event	E-Mail	Trap	Log Table	Syslog	Fault
Cold/Warm Start	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Link Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Authentication Failure	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
RMON Alarm	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Power Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
STP/RSTP/MSTP Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
Fault State Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	
VRRP State Change	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	

Set Values
Refresh

显示框说明

该页面包含以下框：

- **下拉列表“Signaling Contact Method”**

从下拉列表中选择信号触点反应。可能的响应包括：

- **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。

- **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。

- **下拉列表“Signaling Contact Status”**

从下拉列表中选择信号触点状态。可能的状态有：

- **close**
信号触点闭合。
- **open**
信号触点断开。

该表格包括以下列：

- **E-Mail**
设备发送电子邮件。仅当已设置 SMTP 服务器并已启用“SMTP client”功能时，该功能才可用。
- **Trap**
设备发送 SNMP 陷阱。仅当已在“System > Configuration”中启用 SNMPv1 Traps 时，该功能才可用。
- **Log Table**
设备在事件日志表中写入一个条目，请参阅“Information > Log Table”
- **Syslog**
设备将一个条目写入系统日志服务器。仅当已设置系统日志服务器并已启用“Syslog client”功能时，该功能才可用。
- **Fault**
设备触发故障。错误 LED 亮起

5.4 “System”菜单

- **Event**

“Event”列包含以下值：

- **Cold/Warm Start**
用户打开或重启设备。
- **Link Change**
仅当对接口状态进行监视和更改时才会发生该事件，请参阅“System > Fault Monitoring > Link Change”。
- **Authentication Failure**
当试图用错误的密码访问时才会发生该事件。
- **Power Change**
仅当对电源线路 1 和 2 进行监视时才会发生该事件。表明线路 1 或线路 2 有改变，请参阅“System > Fault Monitoring > Power Supply”。
- **STP/RSTP/MSTP Change**
STP、RSTP 或 MSTP 拓扑发生变化。
- **Fault State Change**
故障状态发生变化。故障状态可能涉及已激活的端口监视、信号触点的响应或电源监视。
- **RMON Alarm**
发生了与系统远程监视相关的报警或事件。
- **VRRP State Change**（仅限通过 VRRP 进行路由选择时）
虚拟路由器的状态发生变化。

组态步骤

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

5.4.7 SMTP 客户端

通过电子邮件进行网络监视

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

在此页可组态最多三个 SMTP 服务器和相应的电子邮件地址。

Simple Mail Transfer Protocol (SMTP) Client

SMTP Client

'From'-Field: W-700@SCALANCE

Send Test Mail

SMTP Port: 25

SMTP Server IP Address:

SMTP Server IP Address	Receiver Email Address
<input type="checkbox"/> 192.168.3.100	service@scalande.de

1 entry.

Create Delete Set Values Refresh

显示框说明

该页面包含以下框：

- **复选框“SMTP Client”**
启用或禁用 SMTP 客户端。
- **输入字段“From'-Field”**
输入电子邮件中包含的名称，例如设备名称。
- **“SMTP Port”输入框**
如果不能通过端口 25 访问 SMTP 服务器，则更改端口。

5.4 “System”菜单

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

该表包含以下各列：

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

组态步骤

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

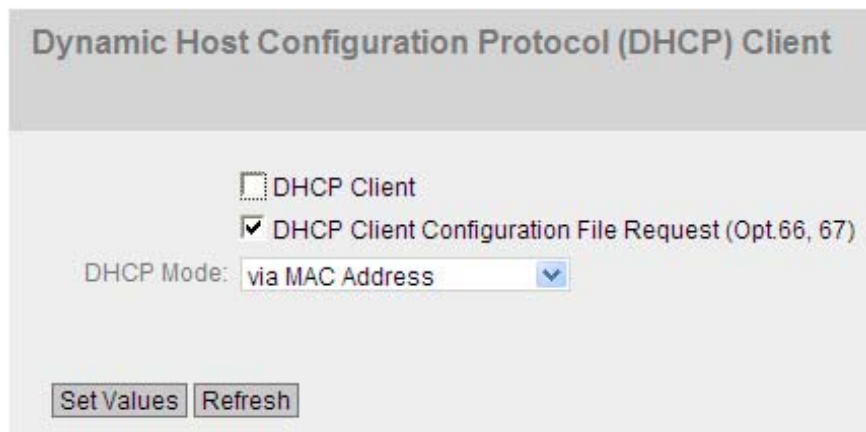
说明

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

5.4.8 DHCP 客户端

设置 DHCP 模式

如果激活 DHCP 模式，则 DHCP 客户端会向组态的 DHCP 服务器发出 DHCP 请求，然后服务器会为其分配 IP 地址以进行响应。服务器管理一个地址范围，并且分配该范围内的 IP 地址。还可以对服务器进行组态，使得客户端发出请求后，总是接收到同一个 IP 地址。



Dynamic Host Configuration Protocol (DHCP) Client

DHCP Client

DHCP Client Configuration File Request (Opt.66, 67)

DHCP Mode:

显示框说明

该页面包含以下框：

- **复选框“DHCP Client”**
启用或禁用 DHCP 客户端。
- **复选框“DHCP Client Config File Request (Opt. 66, 67)”**
如果想要 DHCP 客户端使用选项 66 和 67 下载并随后启用某个组态文件，则启用此选项。
- **下拉列表“DHCP Mode”**
从下拉列表中选择 DHCP 模式。可能的模式如下：
 - **via MAC Address**
基于该 MAC 地址识别设备。
 - **via DHCP Client ID**
基于自由定义的 DHCP 客户端 ID 识别设备。
 - **via System Name**
基于系统名称识别设备。如果系统名称的长度为 255 个字符，则最后一个字符不用于识别设备。

组态步骤

请按照以下步骤使用 DHCP 客户端 ID 组态 IP 地址：

1. 启用“DHCP Client”选项。
2. 从“DHCP Mode”下拉列表中选择“via DHCP Client ID”模式。
3. 在启用的“DHCP Client ID”输入框中输入字符串来识别设备。DHCP 服务器随即会评估该字符串。
4. 如果希望 DHCP 客户端使用选项 66 和 67 下载并随后启用某个组态文件，请选择“Client Config File Request (Opt.66, 67)”选项。
5. 单击“Set Values”按钮。

说明

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

5.4.9 SNMP

5.4.9.1 常规

SNMP 组态

在该页面对 SNMP 进行基本设置。根据希望应用的功能启用相应的复选框。

Simple Network Management Protocol (SNMP) General

General Traps

SNMP: SNMPv1/v2c/v3

SNMPv1/v2c Read Only

SNMPv1/v2c Read Community String: public

SNMPv1/v2c Read/Write Community String: private

SNMPv1 Traps

SNMPv1/v2c Trap Community String: public

Set Values Refresh

显示框说明

该页面包含以下框：

- **下拉列表“SNMPv1/v2c/v3”**
从下拉列表中选择 SNMP 协议。可能的设置如下：
 - “-”（禁用）
禁用 SNMP。
 - SNMPv1/v2c/v3
支持 SNMPv1/v2c/v3。
 - SNMPv3
仅支持 SNMPv3。

5.4 “System”菜单

- **复选框“SNMPv1/v2c Read Only”**
如果启用此选项，则 SNMPv1/v2c 仅可读取 SNMP 变量。

说明

团体字符串

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

- **输入框“SNMPv1/v2c Read/Write Community String”**
输入 SNMP 协议的读取/写入访问团体字符串。
- **输入框“SNMPv1/v2c Read Community String”**
输入 SNMP 协议的访问团体字符串。
- **复选框“SNMPv1 Traps”**
启用或禁用发送 SNMP 陷阱（报警帧）。在“Trap”选项卡上，指定 SNMP 陷阱将发送到的设备的 IP 地址。
- **输入框“SNMPv1/v2c Trap Community String”**
输入发送 SNMPv1/v2 消息的团体字符串。

组态步骤

1. 从“SNMP”下拉列表中选择所需选项：
 - “-”（禁用）
 - SNMPv1/v2c/v3
 - SNMPv3
2. 如果只需要使用 SNMPv1/v2c 对 SNMP 变量进行读访问，请选择“SNMPv1/v2c Read only”复选框。
3. 在“SNMPv1/v2c Read Community String”输入框中，输入所需字符串。
4. 在“SNMPv1/v2c Read/Write Community String”输入框中，输入所需字符串。
5. 单击“设置值”(Set Values) 按钮。

5.4.9.2 Traps

报警事件的 SNMP 陷阱

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

说明

仅当在“General”菜单中选择了“SNMPv1 Traps”选项时，才会发送陷阱。

	IP Address	Trap
<input type="checkbox"/>	192.168.3.116	<input checked="" type="checkbox"/>
<input type="checkbox"/>	192.168.3.115	<input type="checkbox"/>

2 entries.

Create Delete Set Values Refresh

显示框说明

该表格包括以下列：

- **第 1 列**
选中要删除的行中的复选框。
- **IP Address**
输入设备发送 SNMP 陷阱的目标站 IP 地址。最多可指定十个不同的 IP 地址作为不同的接收方。
- **Trap**
启用或禁止发送陷阱。已输入但未选择的工作站不会接收 SNMP 陷阱。

5.4 “System”菜单

组态步骤

创建陷阱条目

1. 单击“Create”按钮以创建新的陷阱条目。
2. 在“IP Address”列中，输入工作站的 IP 地址，设备将向该工作站发送陷阱。
3. 选择相应 IP 地址的复选框。
4. 单击“Set Values”按钮。

删除陷阱条目

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

5.4.10 系统时间

可以采用四种不同的方法来设置设备的系统时间。每次只能采用一种方法。激活一种方法后，将自动禁止之前激活的方法。

5.4.10.1 手动设置

手动设置系统时间

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

The screenshot shows a web interface titled "Manual System Time Setting". It features a tabbed menu with four options: "Manual Setting", "SNTP Client", "NTP Client", and "SIMATIC Time Client". The "Manual Setting" tab is currently selected. Below the tabs, there is a checkbox labeled "Time Manually" which is checked. Underneath, the "System Time" is displayed as "01/01/2000 23:02:51". There is a button labeled "Use PC Time". Below that, two fields are shown: "Last Synchronization Time: Date/time not set" and "Last Synchronization Mechanism: Not set". At the bottom of the interface, there are two buttons: "Set Values" and "Refresh".

显示框说明

该页面包含以下框：

- **复选框“Time Manually”**
启用或禁用手动时间设置。如果启用该选项，则可以编辑“System Time”输入框。
- **输入框“System Time”**
按“MM/DD/YYYY HH:MM:SS”格式输入日期和时间。

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

组态步骤

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

5.4.10.2 SNTP 客户端

网络中的时间同步

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

Simple Network Time Protocol (SNTP) Client

Manual Setting | SNTP Client | NTP Client | SIMATIC Time Client

SNTP Client

Current System Time: 09/14/2011 11:03:22

Last Synchronization Time: 09/14/2011 10:04:33

Last Synchronization Mechanism: NTP

Time Zone: +00:00

SNTP Mode: Poll

SNTP Server IP Address: 0.0.0.0

SNTP Server Port: 123

Poll Interval(s): 64

Set Values Refresh

显示框说明

该页面包含以下框：

- **复选框“SNTP Client”**
启用或禁用使用 SNTP 自动进行时钟同步。
如果启用该复选框，则“Time Zone”输入框和“SNTP Mode”下拉列表会激活。
- **显示框“Current System Time”**
显示系统中当前设置的日期和时间值。
- **显示框“Last Synchronization Time”**
该框为只读，显示上次进行日时钟同步时的时间。

- **显示框“Last Synchronization Mechanism”**

该框显示上次时钟同步是如何执行的。可能的方法如下：

 - Not set
未设置系统时间。
 - Manual
手动设置时间
 - SNTP
通过 SNTP 自动进行时钟同步
 - SIMATIC
使用 SIMATIC 时钟帧自动进行时钟同步。
 - NTP
使用 NTP 自动进行时钟同步
- **输入框“Time Zone”**

在此框中，以“+/- HH:MM”的格式输入所使用的时区。时区与 UTC 标准世界时间相关。在此框中通过指定时间偏移量将夏令时和标准时间的设置考虑在内。
- **下拉列表“SNTP Mode”**

从下拉列表中选择同步模式。可以使用下列同步类型：

 - Poll
如果选择该协议类型，则会显示输入框“SNTP Server IP Address”、“SNTP Server Port”和“Poll Interval(s)”以便进一步组态。若使用该同步类型，设备会激活，并向 SNTP 服务器发送时间查询。
 - Listen
若使用该同步类型，设备不会激活，但会“侦听”传递时钟的 SNTP 帧。
- **输入框“SNTP Server IP Address”**

输入 SNTP 服务器的 IP 地址。
- **输入框“SNTP Server Port”**

输入 SNTP 服务器的端口。
可用的端口如下：

 - 123（标准端口）
 - 1025 到 36564
- **输入框“Poll Interval(s)”**

在此输入两次时间查询间的时间间隔。在此框中输入查询间隔的秒数值。可能的值介于 16 到 16284 秒之间。

组态步骤

1. 单击“SNTP Client”复选框以启用自动时间设置。
2. 在“Time Zone”输入框中输入当地时间与世界时间 (UTC) 的时差。由于 SNTP 服务器始终发送 UTC 时间，因此输入格式为“+/-HH:MM”（例如，对于 CEST 是 +02:00）。该时间随后会被重新计算并根据指定的时区显示为当地时间。在设备本身不会将夏令时转换为标准时间。完成“Time Zone”输入框时，还需要考虑到这一点。
3. 从下拉列表“SNTP Mode”中选择下列选项之一：
 - Poll
对于该模式，需要组态以下内容：
 - 时区时差（第 2 步）
 - 时间服务器（第 4 步）
 - 端口（第 5 步）
 - 查询间隔（第 6 步）
 - 通过第 7 步完成组态。
 - Listen
对于该模式，需要组态以下内容：
 - 与服务器发送的时间之间的时差（第 2 步）
 - 通过第 7 步完成组态。
4. 在“SNTP Server IP Address”输入框中，输入 SNTP 服务器的 IP 地址，将使用该服务器的帧同步时钟。
5. 在“SNTP Server Port”输入框中，输入可用来使用 SNTP 服务器的端口。仅当输入 SNTP 服务器的 IP 地址之后，才可以修改该端口。
6. 在“Poll Interval(s)”输入框中，输入以秒表示的时间值，经过这段时间后，会向时间服务器发送新的时间查询。
7. 单击“Set Values”按钮将更改传输到设备。

5.4.10.3 NTP 客户端

使用 NTP 自动设置时钟

如果需要使用 NTP 进行时钟同步，可以在此做相关设置。

Network Time Protocol (NTP) Client

Manual Setting | SNTP Client | **NTP Client** | SIMATIC Time Client

NTP Client

Current System Time: 09/14/2011 11:03:36

Last Synchronization Time: 09/14/2011 10:04:33

Last Synchronization Mechanism: Manual

Time Zone: +00:00

NTP Server IP Address: 0.0.0.0

NTP Server Port: 123

Poll Interval(s): 64

Set Values Refresh

显示框说明

该页面包含以下框：

- **复选框“NTP Client”**
选中此复选框可启用使用 NTP 自动进行时钟同步。如果选中此复选框，则会启用“Time Zone”、“NTP Server IP Address”、“NTP Server Port”和“Poll Interval(s)”输入框。
- **显示框“System Time”**
此框显示当前系统时间。
- **显示框“Last Synchronization Time”**
该框为只读，显示上次进行日时钟同步时的时间。

5.4 “System”菜单

- **显示框“Last Synchronization Mechanism”**

该框显示上次时钟同步是如何执行的。可能的方法如下：

 - Not set
未设置系统时间。
 - Manual
手动设置时间
 - SNTP
通过 SNTP 自动进行时钟同步
 - NTP
使用 NTP 自动进行时钟同步
 - SIMATIC
使用 SIMATIC 时钟帧自动进行时钟同步。
- **输入框“Time Zone”**

在此框中，以“+/- HH:MM”的格式输入所使用的时区。时区与 UTC 标准世界时间相关。在此框中通过指定时间偏移量将夏令时和标准时间的设置考虑在内。
- **输入框“NTP Server IP Address”**

输入 NTP 服务器的 IP 地址。
- **输入框“NTP Server Port”**

输入 NTP 服务器的端口。
可能的端口包括：

 - 123（标准端口）
 - 1025 到 36564
- **输入框“Poll Interval(s)”**

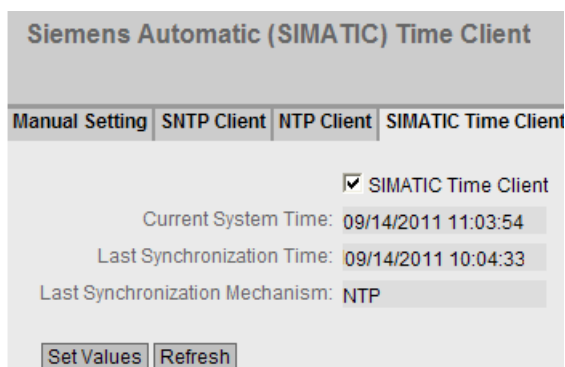
在此输入两次时间查询的时间间隔。在此框中输入查询间隔的秒数值。可能的值介于 16 到 16284 秒之间。

组态步骤

1. 单击“NTP Client”复选框以启用通过 NTP 自动设置时间。
2. 在以下框中输入需要的值：
 - 时区
 - NTP 服务器 IP 地址
 - NTP 服务器端口
 - 查询间隔
3. 单击“Set Values”按钮。

5.4.10.4 SIMATIC 时间客户端

通过 SIMATIC 时间客户端设置时间



显示框说明

该页面包含以下框：

- **复选框“SIMATIC Time Client”**
选中此复选框可启用设备作为 SIMATIC 时间客户端。
- **显示框“System Time”**
此框显示当前系统时间。
- **显示框“Last Synchronization Time”**
该框为只读，显示上次进行日时钟同步时的时间。
- **显示框“Last Synchronization Mechanism”**
该框显示上次时钟同步是如何执行的。可能的方法如下：
 - Not set
未设置系统时间。
 - Manual
手动设置时间
 - SNTP
通过 SNTP 自动进行时钟同步
 - NTP
使用 NTP 自动进行时钟同步
 - SIMATIC
使用 SIMATIC 时钟帧自动进行时钟同步。

组态步骤

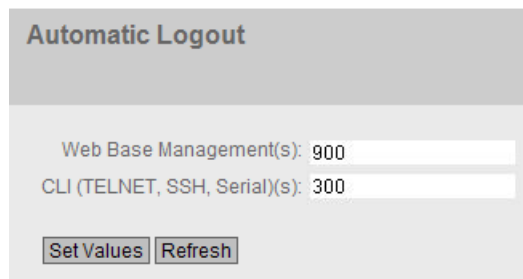
1. 单击“SIMATIC Time Client”复选框可启用 SIMATIC Time Client。
2. 单击“Set Values”按钮。

5.4.11 自动注销

设置自动注销

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

如果您已经自动注销，则需要再次登录。



Automatic Logout

Web Base Management(s): 900

CLI (TELNET, SSH, Serial)(s): 300

Set Values Refresh

组态

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

5.4.12 Select/Set 按钮组态

Select/Set 按钮说明

“Select/Set”按钮可用于：

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

有关各项按钮功能的详细说明，请参见设备操作说明。

在此页面中，可限制或完全禁用 Select/Set 按钮的功能。



显示框说明

支持以下功能：

- **复选框“Restore Factory Defaults”**
使用 Select/Set 按钮启用或禁用“恢复为出厂默认设置”功能。
- **复选框“Set Fault Mask”**
使用 Select/Set 按钮启用或禁用“通过 LED 显示定义故障屏蔽”功能。该功能仅在显示模式 D 下可用。

组态步骤

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

5.4.13 Syslog 客户端

系统事件代理

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

发送日志条目的要求:

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

	Server IP Address	Server Port
<input type="checkbox"/>	192.168.0.1	514
<input type="checkbox"/>	1.2.3.4	514

显示框说明

该页面包含以下框:

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

5.4 “System”菜单

该表包含以下各列

- **第 1 列**
选中要删除的行中的复选框。
- **Server IP Address**
显示 Syslog 服务器的 IP 地址。
- **Server Port**
输入 Syslog 服务器所使用的端口。

组态步骤

启用功能

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

创建新条目

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

说明

服务器端口的默认设置是 514。
最多可创建一个 Syslog 服务器。

更改条目

1. 删除条目。
2. 创建新条目。

删除条目

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

5.4.14 端口

5.4.14.1 概述

端口组态概述

此页面显示设备所有端口的数据传送组态。无法对该页面上的任何内容进行组态。

Ports Overview									
Overview		Configuration							
Port	Port Name	Mode	Negotiation	Flow Ctrl. Type	Flow Ctrl.	MTU	Port Type	Status	Link
P0.1		1G FD	enabled	<input type="checkbox"/>	disabled	1536	Switch-Port	enabled	up
P0.2		10G FD	enabled	<input type="checkbox"/>	disabled	1536	Switch-Port	enabled	down
P0.3		10G FD	enabled	<input type="checkbox"/>	disabled	1536	Switch-Port	enabled	down
P0.4		10G FD	enabled	<input type="checkbox"/>	disabled	1536	Switch-Port	enabled	down
P1.1		1G HD	enabled	<input type="checkbox"/>	disabled	1536	Switch-Port	enabled	down
P1.2		1G HD	enabled	<input type="checkbox"/>	disabled	1536	Switch-Port	enabled	down
P1.3		1G HD	enabled	<input type="checkbox"/>	disabled	1536	Switch-Port	enabled	down
P1.4		100M HD	enabled	<input type="checkbox"/>	disabled	1536	Switch-Port	enabled	down
P2.1		1G FD	enabled	<input type="checkbox"/>	disabled	1536	Switch-Port	enabled	down

显示框说明

该表格包括以下列：

- Port**
 显示可组态端口。条目是一个链接。如果单击该链接，相应组态页便会打开。端口由端口号和插槽号组成，例如，端口 0.1 表示插槽 0，端口 1。
- Port Name**
 显示端口名称。
- Mode**
 显示端口的传输参数。
- Negotiation**
 显示自动组态是启用还是禁用状态。
- Flow Ctrl. Type**
 显示此端口的流量控制是启用还是禁用状态。

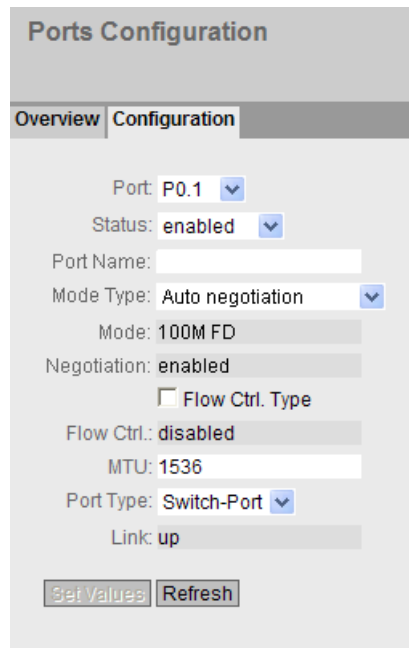
5.4 “System”菜单

- **Flow Ctrl.**
显示此端口上的流量控制是否正常工作。
- **MTU (Maximum Transmission Unit)**
显示包大小。
- **Port type (仅限路由)**
显示端口类型。可能的类型如下：
 - 交换机端口
 - 路由器端口
- **Status**
显示端口是开启还是关闭状态。数据通信只能通过已启用的端口。
- **Link**
显示网络连接状态。有以下连接状态：
 - 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。
 - Down
链路中断，例如由于关闭了所连接的设备。

5.4.14.2 组态

组态端口

通过本页面，可以组态设备的所有端口。



Ports Configuration

Overview Configuration

Port: P0.1

Status: enabled

Port Name:

Mode Type: Auto negotiation

Mode: 100M FD

Negotiation: enabled

Flow Ctrl. Type

Flow Ctrl.: disabled

MTU: 1536

Port Type: Switch-Port

Link: up

Set Values Refresh

显示框说明

该表格包括以下行：

- **下拉列表“Port”**
从下拉列表中选择要组态的端口。端口由端口号和插槽号组成，例如，端口 0.1 表示插槽 0，端口 1。
- **下拉列表“Status”**
指定是启用还是禁用端口。
 - **enabled**
启用端口。数据通信只能通过已启用的端口。
 - **disabled**
禁用端口但保持连接。
 - **link down**
禁用端口并且中断到伙伴设备的连接。

5.4 “System”菜单

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

说明

在某个端口与伙伴端口互相通讯之前，两端必须具有匹配的设置。

- **显示框“Mode”**
显示端口的传输速度和传输方法。传输速度可以是 10 Mbps、100 Mbps、1000 Mbps 或 10 Gbps。对于传输模式，可以组态为全双工 (FD) 或半双工 (HD)。
- **显示框“Negotiation”**
显示连接伙伴端口的自动组态是启用还是禁用状态。
- **复选框“Flow Ctrl. Type”**
启用或禁用端口的流控制。
- **Flow Ctrl.**
显示此端口上的流量控制是否正常工作。
- **输入框“MTU”**
输入包大小。
- **下拉列表“Port Type”（仅限路由）**
从下拉列表中选择端口类型。
 - 交换机端口
 - 路由器端口
- **显示框“Link”**
显示网络连接状态。可用选项如下：
 - 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。
 - Down
链路中断，例如由于关闭了所连接的设备。

更改端口组态

单击相应的框可更改组态。

说明

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

- 自动组态
- 传输速度
- 传输技术

说明

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

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

组态步骤

1. 根据组态更改设置。
2. 单击“Set Values”按钮。

5.4 “System”菜单

5.4.15 故障监视

5.4.15.1 电源

监视电源的设置

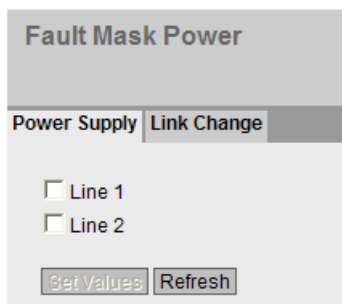
组态是否通过消息系统监视电源。根据硬件型号，有一个或两个电源连接器（线路 1/线路 2）。带冗余电源时，应对每个单独的进线线路分别组态监视。

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

说明

设备的精简版操作说明中包含允许的工作电压限值。

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



组态步骤

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

5.4.15.2 Link Change

连接状态变化的故障监视组态

在此页面上组态出现网络连接状态变化时是否触发错误信息。

如果启用连接监视，则发出错误信号

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

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

Port	Setting
P0.1	-
P0.2	-
P0.3	-
P0.4	-
P1.1	-
P1.2	-
P1.3	-
P1.4	-
P2.1	-
P2.2	-
P2.3	-
P2.4	-
P3.1	-
P3.2	-

显示框说明

表 1 包含以下列：

- **第 1 列**
显示设置对于所有端口有效。

5.4 “System”菜单

- **Setting**
从下拉列表中选择设置。 可选择以下设置选项：
 - “-”（禁用）
 - Up
 - Down
 - No Change: 表 2 中的设置保持不变。

- **Copy to Table**
如果单击此按钮，则为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **Port**
显示可用端口和链路汇聚。 端口由端口号和插槽号组成，例如，端口 0.1 表示插槽 0，端口 1。
- **Setting** 从下拉列表中选择设置。可做以下选择：
 - Up
当端口变为激活状态时触发错误处理。
(从“Link down”到“Link up”)
 - Down
当端口变为未激活状态时触发错误处理。
(从“Link up”到“Link down”)
 - “-”（禁用）
不触发错误处理。

组态步骤

为端口组态错误监视

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

为所有端口组态错误监视

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

5.4.16 C-PLUG

C-PLUG 内容的相关信息

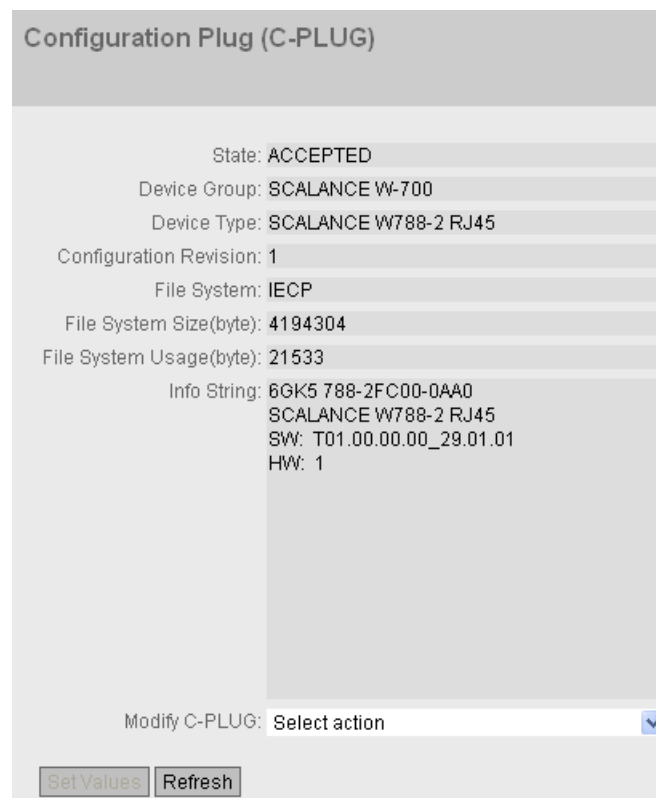
此页面可提供有关 C-PLUG 的详细信息。可以格式化 C-PLUG 或向其中加入新内容。

说明

只有在单击“Set Values”按钮后，才会执行此操作。

此操作无法撤销。

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



The screenshot displays the 'Configuration Plug (C-PLUG)' interface. It features a list of configuration parameters and their values, followed by an 'Info String' section and a 'Modify C-PLUG' dropdown menu. At the bottom, there are two buttons: 'Set Values' and 'Refresh'.

Parameter	Value
State	ACCEPTED
Device Group	SCALANCE W-700
Device Type	SCALANCE W788-2 RJ45
Configuration Revision	1
File System	IECP
File System Size(byte)	4194304
File System Usage(byte)	21533
Info String	6GK5 788-2FC00-0AA0 SCALANCE W788-2 RJ45 SW: T01.00.00.00_29.01.01 HW: 1

Modify C-PLUG: ▼

显示框说明

该表格包括以下行：

- **State**
显示 C-PLUG 的状态。可能的状态包括：
 - ACCEPTED
设备中已插入内容有效且相配的 C-PLUG。
 - NOT ACCEPTED
插入的 C-PLUG 内容无效或不兼容。
 - NOT PRESENT
设备中未插入 C-PLUG。
 - FACTORY
C-PLUG 已插入，并且为空。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。
- **Device Group**
显示先前使用该 C-PLUG 的 SIMATIC NET 产品线。
- **Device Type**
显示先前使用该 C-PLUG 的产品线的设备类型。
- **Configuration Revision**
组态结构的版本。此信息与设备支持的组态选项相关，而与具体的硬件配置无关。因此，在添加或移除附加组件（模块或扩展器）时，此版本信息不会改变，但是如果更新固件，则该信息可能会发生改变。
- **File System**
显示 C-PLUG 上的文件系统类型。
- **File System Size(byte)**
显示 C-PLUG 的文件系统的最大存储空间。
- **File System Usage(byte)**
显示 C-PLUG 文件系统中当前已被使用的存储空间。
- **Info String**
显示有关之前使用该 C-PLUG 的设备的所有附加信息，例如：订货号、型号标识以及硬件与软件的版本。显示的软件版本与上次更改了组态的版本相对应。

- 状态为“NOT ACCEPTED”时，将显示有关问题原因的更多信息。如果 C-PLUG 组态与设备组态不符，则会代之显示 C-PLUG 的信息字符串。
- **下拉列表“Modify C-PLUG”**
从下拉列表中选择设置。用户可使用以下选项更改 C-PLUG：
 - **Write current configuration to C-PLUG**
仅当 C-PLUG 的状态为“NOT ACCEPTED”或“FACTORY”时，此选项才可用。
会将设备内部闪存中的组态复制到 C-PLUG。
 - **Erase C-PLUG to factory default**
删除 C-PLUG 中的所有数据并触发低级格式化功能。

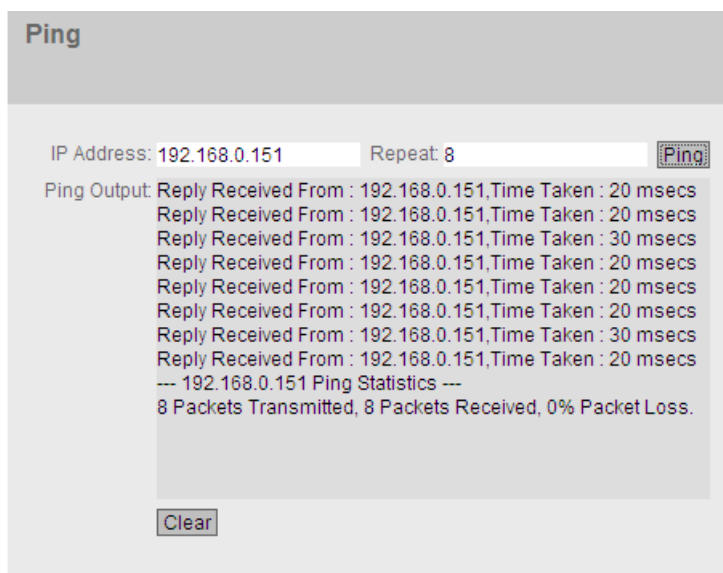
组态步骤

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

5.4.17 Ping

IP 网络中地址的可达性

通过 ping 功能，可检查某一 IP 地址在网络中是否可到达。



显示框说明

该表格包括以下列：

- **输入框“IP address”**
输入要 ping 的设备的 IP 地址，以测试其是否可到达。
- **输入框“Repeat”**
输入要发送的数据包。
- **“Ping”按钮**
单击此按钮开始发送数据包。
- **Ping Output**
该框会显示 ping 功能的输出。

5.4.18 PoE

5.4.18.1 常规

以太网供电 (PoE) 的设置

在此页面上，可以查看由 SCALANCE X500 通过 PoE 供电的相关信息。

Power over Ethernet (PoE) General	
General	Port
Maximum Power(W): 189	Power In Use(W): 10
Allocated Power(W): 62	Usage Threshold(%): 80
<input type="button" value="Set Values"/>	<input type="button" value="Refresh"/>

显示框说明

该页面包含以下框：

最大功率 [W]（只读）

SCALANCE X500 为 PoE 设备提供的最大功率。

分配的功率 [W]（只读）

PoE 设备根据“分类”保留的功率总和。

使用功率 [W]（只读）

终端设备使用的功率总和。

使用阈值 [%]

只要终端设备使用的功率超过此处显示的百分比，就会触发事件。

5.4.18.2 端口

端口的设置

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

在此页面上，可以查看各个 PoE 端口的详细信息。

Power over Ethernet (PoE) Port

General | **Port**

Port	Setting	Priority	Type	Copy to Table
All ports	No Change	No Change	No Change	Copy to Table

Port	Setting	Priority	Type	Classification	Status	Power(mW)	Voltage(V)	Current(mA)
P3.1	<input checked="" type="checkbox"/>	low	Wlan AP 1	Class 3	delivering	4644	54	86
P3.2	<input checked="" type="checkbox"/>	critical	Webcam	Class 3	delivering	3240	54	60
P3.3	<input checked="" type="checkbox"/>	low		Class 4	delivering	4320	54	80
P3.4	<input type="checkbox"/>	low		-	disabled	0	0	0

Set Values Refresh

显示框说明

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

表 1 包含以下列：

- **端口 (Port)**

显示设置对于所有端口有效。

- **设置 (Setting)**

从下拉列表中选择设置。可选择以下设置选项：

- 启用 (enabled)

启用该功能

- 禁用 (disabled)

禁用该功能

- 无变化 (No Change)

表 2 中的设置保持不变

- **优先级 (Priority)**

从下拉列表中选择端口的优先级。如果在表 1 中设置了优先级并将值复制到表 2，则所有端口具有相同优先级。

可进行以下设置（按相关性以升序排列）：

- 低
低优先级
- 高
中优先级
- 关键
高优先级
- 无变化 (No Change)
表 2 中的设置保持不变

- **类型 (Type)**

在此处可输入字符串，更详细地描述所连接的设备。最大长度为 255 个字符。

- **复制到表 (Copy to Table)**

如果单击此按钮，则为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **端口 (Port)**

显示可组态的 PoE 端口。

端口由端口号和插槽号组成，例如，端口 0.1 表示插槽 0，端口 1。

- **设置 (Setting)**

启用对此端口的 PoE 供电或中断供电。

- **优先级 (Priority)**

从下拉列表中选择此端口的供电优先级。

可进行以下设置（按相关性以升序排列）：

- 低
- 高
- 关键

如果为两个端口设置相同的优先级，则必要时优先选择编号较低的端口。

5.4 “System”菜单

- **类型 (Type)**

在此处可输入字符串，更详细地描述所连接的设备。最大长度为 255 个字符。

- **分类 (Classification) (只读)**

分类指定设备的类别。通过该设置可识别设备的最大功率。

- **状态 (Status) (只读)**

显示端口的当前状态。

可能的状态有：

- 禁用 (disabled)

禁止对此端口进行 PoE 供电。

- 输出功率 (delivering Power)

激活对此端口的 PoE 供电并连接一台设备。

- 搜索 (searching)

激活对此端口的 PoE 供电，但未连接设备。

- **功耗 [mW] (Power [mW]) (只读)**

显示 SCALANCE 为此端口提供的功率。

- **电压 [V] (Voltage [V]) (只读)**

显示施加到此端口的电压。

- **电流 [mA] (Current [mA]) (只读)**

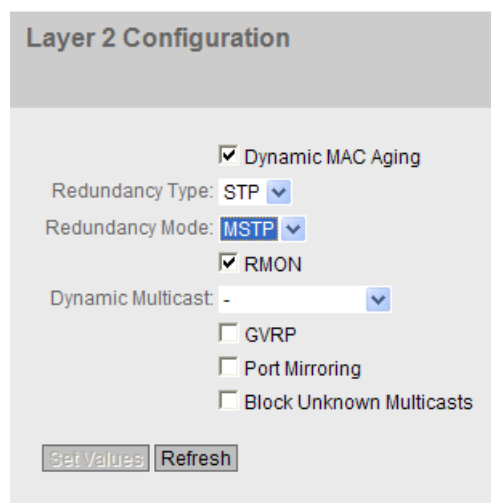
显示为连接到此端口的设备提供的电流。

5.5 “第 2 层”菜单

5.5.1 组态

组态第 2 层

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



The screenshot shows the 'Layer 2 Configuration' web interface. It features several configuration options: 'Dynamic MAC Aging' is checked; 'Redundancy Type' is set to 'STP'; 'Redundancy Mode' is set to 'MSTP'; 'RMON' is checked; 'Dynamic Multicast' is set to '-'; 'GVRP', 'Port Mirroring', and 'Block Unknown Multicasts' are unchecked. At the bottom, there are 'Set Values' and 'Refresh' buttons.

显示框说明

- **复选框“Dynamic MAC Aging”**
启用或禁用“老化”机制。可以在“Layer 2 > Dynamic MAC Aging”中组态其它设置。
- **下拉列表“Redundancy Type”**
以下设置可用
 - “-”（禁用）
禁用冗余功能。
 - **STP**
如果选择此选项，则可在“Redundancy Mode”下拉列表中指定所需冗余模式。

5.5 “第 2 层”菜单

- 下拉列表“Redundancy Mode”

如果在“Redundancy Type”下拉列表中选择“STP”，则可使用以下选项：

- **STP**

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

- **RSTP**

启用 Rapid Spanning Tree Protocol (RSTP)。如果在某个端口上检测到生成树帧，该端口会从 RSTP 恢复为生成树。可以在“Layer 2 > MSTP”中组态其它设置。

说明

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

- **MSTP**

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

- 复选框“RMON”

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

- 下拉列表“Dynamic Multicast”

可能的设置如下：

- “-”（禁用）

- **IGMP Snooping**

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

- **GMRP**

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

说明

GMRP 和 IGMP 不能同时起作用。

- **复选框“GVRP”**
启用或禁用“GVRP”（GARP VLAN 注册协议）。可以在“Layer 2 > VLAN > GVRP”中组态其它设置。
- **复选框“Port Mirroring”**
启用或禁用端口镜像。可以在“Layer 2 > Port Mirroring”中组态其它设置。
- **复选框“Block Unknown Multicasts”**
启用“阻止未知组播”。设备不会转发任何未知来源的组播数据包。). 可以在“Layer 2 > Multicast > Groups”中组态其它设置。

5.5.2 Qos

5.5.2.1 CoS 队列映射

COS Queue Mapping

在此处将 CoS 优先级分配给特定队列 (Traffic Queues)。

COS	Queue
0	1
1	2
2	3
3	4
4	5
5	6
6	7
7	8

5.5 “第 2 层”菜单

显示框说明

该表格包括以下列：

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

组态步骤

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

5.5.2.2 DSCP 映射

DSCP 队列

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

DSCP	Queue
0	1
1	1
2	1
3	1
4	1
5	1
6	1
7	1
8	2
9	2
10	2
11	2
12	2
13	2
14	2
15	2
16	3
17	3
18	3

显示值说明

该表格包括以下列：

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

组态步骤

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

5.5.3 速率控制

限制进入和离开数据的传输速率

在此页面上组态各个端口的负载限值（每秒最大数据包数）。您可以指定将应用这些限制值的帧的类别。

Rate Control

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

Port	Limit Ingress Unicast(DLF)	Limit Ingress Broadcast	Limit Ingress Multicast	Total Ingress Rate pkts/s	Egress Rate kb/s
P0.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P0.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P0.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P0.4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P1.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P1.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P1.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P1.4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P2.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P2.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P2.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P2.4	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P3.1	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P3.2	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0
P3.3	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	0	0

显示值说明

表 1 包含以下列：

- **第 1 列**
显示设置对于所有端口有效。
- **Limit Ingress Unicast (DLF)/Limit Ingress Broadcast/Limit Ingress Multicast**
在下拉列表中选择所需设置。
 - **enabled:** 启用此功能。
 - **disabled:** 禁用此功能
 - **No Change:** 表 2 中的设置保持不变

- **Total Ingress Rate pkts/s**
指定设备处理的最大入站数据包数。如果输入“No Change”，则表中的条目保持不变。
- **Egress Rate kb/s**
指定所有出站帧的数据传输率。如果输入“No Change”，则表中的条目保持不变。
- **Copy to Table**
如果单击此按钮，则会为表 2 的所有端口应用这些设置。

表 2 包含以下列：

- **Port**
显示其它信息所关联的插槽和端口。不能组态此字段。
- **Limit Ingress Unicast (DLF)**
启用或禁用数据传输率，以限制无法解析地址的入站单播帧 (Destination Lookup Failure)。
- **Limit Ingress Broadcast**
启用或禁用数据传输率，以限制入站广播帧。
- **Limit Ingress Multicast**
启用或禁用数据传输率，以限制入站组播帧。
- **Total Ingress Rate pkts/s**
指定设备处理的最大入站数据包数。
- **Egress Rate kb/s**
指定所有出站帧的数据传输率。

说明

对数值取整，与期望值的偏差

输入速率值时，请注意 WBM 会取整为正确的值。

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

组态步骤

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

5.5 “第 2 层”菜单

5.5.4 VLAN

5.5.4.1 常规

VLAN 组态页面

在此页面中定义 VLAN 并指定端口的使用。

说明

更改代理 VLAN ID

如果组态 PC 通过以太网直接连接到设备，并且更改了代理 VLAN ID，则更改后不再可以通过以太网访问该设备。

Virtual Local Area Network (VLAN) General

General | GVRP | Port Based VLAN | Protocol Based VLAN Group | Protocol Based VLAN Port | Ipv4 Subnet Based VLAN

VLAN ID:

	VLAN ID	Name	Status	P0.1	P0.2	P0.3	P0.4	P1.1	P1.2	P
<input type="checkbox"/>	1		Static	U	U	U	U	U	U	P
<input type="checkbox"/>	2		Static	-	-	-	-	-	-	
<input type="checkbox"/>	3		Static	-	-	-	-	-	-	

3 entries.

VLAN 的重要规则

组态和运行 VLAN 时，确保遵守以下规则：

VLAN ID 为“0”的帧会按照无标记帧处理，但会保留其优先级值。

默认情况下，设备上的所有端口均发送不带 VLAN 标记的帧，以确保终端节点可接收这些帧。

对于 SCALANCE X500 设备，所有端口的默认 VLAN ID 为 1。

如果终端节点连接到端口，发送的离开帧不应带标记（静态访问端口）。但是，如果此端口有另一台交换机，则发送的帧应添加标记（中继端口）。

显示框说明

该页面包含以下框：

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

说明

VLAN-ID 500 保留供将来使用，且已经组态

该表格包括以下列：

- **第 1 列**
选中要删除的行中的复选框。
- **VLAN ID**
显示 VLAN ID。VLAN ID（介于 1 到 4094 之间的数字）只能在创建新数据记录时分配一次，之后不能更改。如要更改，必须删除整个数据记录并重新创建。可最多定义 257 个 VLAN。
- **Name**
输入 VLAN 的名称。此名称仅提供信息，对组态没有影响。最大长度为 32 个字符。
- **Status**
显示端口过滤表中条目的状态类型。此处，“静态”(static) 表示地址由用户作为静态地址输入。条目 GVRP 表示组态由 GVRP 帧注册。但是，仅当设备启用 GVRP 时，此条目才可用。

5.5 “第 2 层”菜单

- **List of ports**

指定端口的使用。可使用以下选项：

- "-"

该端口不是 VLAN 的成员。

对于新定义，所有端口的标识符均为“-”。

- M

该端口是 VLAN 的成员。此 VLAN 中发送的帧在转发时带有相应 VLAN 标记。

- R

该端口是 VLAN 的成员。GVRP 帧用于注册。

- U (大写)

该端口是无标记的 VLAN 成员。此 VLAN 中发送的帧在转发时不带 VLAN 标记。

不带 VLAN 标记的帧通过此端口发送。

- u (小写)

此端口是无标记 VLAN 成员，但是此 VLAN 未组态为端口 VLAN。此 VLAN 中发送的帧在转发时不带 VLAN 标记。

- F

该端口不是指定 VLAN 的成员，在此端口不能使用 GVRP 动态注册 VLAN。可以在“Layer 2 > VLAN > Port-based VLAN”中组态其它设置。

组态步骤

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

5.5.4.2 GVRP

组态 GVRP 功能

通过 GVRP 帧，不同设备可在设备的端口处注册特定 VID。不同设备可以是终端设备或交换机等。设备也可以通过此端口发送 GVRP 帧。

可在此页面上启用各个端口的 GVRP 功能。

GARP VLAN Registration Protocol (GVRP)

General | **GVRP** | Port Based VLAN | Protocol Based VLAN Group | Protocol Based VLAN Port | Ipv4 Subnet Based VLAN

GVRP

	Setting	Copy to Table
All ports	No Change <input type="button" value="v"/>	<input type="button" value="Copy to Table"/>

Port	Setting	
P0.1	<input checked="" type="checkbox"/>	<input type="button" value="v"/>
P0.2	<input checked="" type="checkbox"/>	
P0.3	<input checked="" type="checkbox"/>	
P0.4	<input checked="" type="checkbox"/>	
P1.1	<input checked="" type="checkbox"/>	
P1.2	<input checked="" type="checkbox"/>	
P1.3	<input checked="" type="checkbox"/>	
P1.4	<input checked="" type="checkbox"/>	
P2.1	<input checked="" type="checkbox"/>	
P2.2	<input checked="" type="checkbox"/>	
P2.3	<input checked="" type="checkbox"/>	
P2.4	<input checked="" type="checkbox"/>	
P3.1	<input checked="" type="checkbox"/>	
P3.2	<input checked="" type="checkbox"/>	<input type="button" value="v"/>

5.5 “第 2 层”菜单

显示框说明

该页面包含以下框：

- **复选框“GVRP”**
启用或禁用 GVRP 功能。

表 1 包含以下列：

- **第 1 列**
说明设置对于表 2 的所有端口都有效。
- **Setting**
从下拉列表中选择设置。可选择以下设置选项：
 - enabled
启用发送 GVRP 帧。
 - disabled
禁用发送 GVRP 帧。
 - No Change
表 2 中无变化。
- **Copy to Table**
如果单击此按钮，将为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **Port**
显示可用端口。端口由端口号和插槽号组成，例如，端口 0.1 表示插槽 0，端口 1。
- **Setting**
启用或禁用发送 GVRP 帧。

组态步骤

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

5.5.4.3 基于端口的 VLAN

处理接收到的帧

在此页面中，指定用于接收帧的端口属性组态。

Port Based Virtual Local Area Network (VLAN) Configuration

General | GVRP | **Port Based VLAN** | Protocol Based VLAN Group | Protocol Based VLAN Port | Ipv4 Subnet Based VLAN

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

Port	Priority	Port VID	Acceptable Frames	Ingress Filtering
P0.1	0	VLAN1	All	<input type="checkbox"/>
P0.2	0	VLAN1	All	<input type="checkbox"/>
P0.3	0	VLAN1	All	<input type="checkbox"/>
P0.4	0	VLAN1	All	<input type="checkbox"/>
P2.1	0	VLAN1	All	<input type="checkbox"/>
P2.2	0	VLAN1	All	<input type="checkbox"/>
P2.3	0	VLAN1	All	<input type="checkbox"/>
P2.4	0	VLAN1	All	<input type="checkbox"/>
P3.1	0	VLAN1	All	<input type="checkbox"/>
P3.2	0	VLAN1	All	<input type="checkbox"/>
P3.3	0	VLAN1	All	<input type="checkbox"/>
P3.4	0	VLAN1	All	<input type="checkbox"/>
P4.1	0	VLAN1	All	<input type="checkbox"/>
P4.2	0	VLAN1	All	<input type="checkbox"/>
P4.3	0	VLAN1	All	<input type="checkbox"/>
P4.4	0	VLAN1	All	<input type="checkbox"/>

Set Values Refresh

显示框说明

表 1 包含以下列：

- **Port**
显示设置对于所有端口有效。
- **Priority/Port VID/Acceptable Frames/Ingress Filtering**
在下拉列表中选择设置。如果选择“No Change”，则表 2 中的条目保持不变。
- **Copy to Table**
如果单击此按钮，将为表 2 的所有端口应用此设置。

5.5 “第 2 层”菜单

表 2 包含以下列：

- **Port**

显示可用端口和链路汇聚。端口由端口号和插槽号组成，例如，端口 0.1 表示插槽 0，端口 1。

- **Priority**

从下拉列表中选择分配给无标记帧的优先级。

VLAN 标记中使用的 CoS（服务类别）优先级。如果接收到无标记的帧，将为其分配此优先级。此优先级指定了将该帧与其它帧相比较后，如何进一步处理该帧。总共有 8 个优先级，值分别为 0 到 7，其中 7 表示最高优先级（IEEE 802.1p 端口优先级）。

- **Port VID**

从下拉列表中选择 VLAN ID。只能选择在“VLAN > General”页面中定义的 VLAN ID。

如果接收到的帧没有 VLAN 标记，则会为其添加此处指定的 VLAN ID 作为标记，然后按照端口规则发送出去。

- **Acceptable Frames**

指定将接受哪些类型的帧。可能的选项如下：

- **Tagged Frames Only**

设备会丢弃所有无标记帧。否则，按照组态应用转发规则。

- **All**

设备会转发所有帧。

- **Ingress Filtering**

指定是否评估已接收帧的 VID

可做以下选择：

- **启用**

由接收到的帧的 VLAN-ID 决定是否转发：要转发 VLAN 标记帧，接收端口必须是相同 VLAN 的成员。在接收端口会丢弃来自未知 VLAN 的帧。

- **禁用**

转发所有帧。

组态步骤

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

5.5.4.4 基于协议的 VLAN 组

简介

在此页面中，指定将为其分配协议的组。

Protocol based Virtual Local Area Network (VLAN) - Group

General | GVRP | Port Based VLAN | **Protocol Based VLAN Group** | Protocol Based VLAN Port | Ipv4 Subnet Based VLAN

Protocol Based VLAN

Protocol Value:

Group Identifier:

	Protocol Value	Group Identifier
<input type="checkbox"/>	00:80	1
<input type="checkbox"/>	00:90	2

显示框说明

该页面包含以下框：

- **复选框“Protocol Based VLAN”**
启用或禁用基于协议的 VLAN 分配。
- **输入框“Protocol Value”**
输入十六进制的协议值。
下面列出几个示例：
 - PROFINET: 88:92
 - IP: 08:00
 - Novell: ff:ff
 - netbios: f0:f0
 - appletalk: 80:9b
- **输入框“Group Identifier”**
输入组的 ID。

5.5 “第 2 层”菜单

该表格包括以下列：

- **第 1 列**
选中要删除的行中的复选框。
- **Protocol Value**
显示协议值。
- **Group Identifier**
显示组 ID。

组态步骤

添加条目

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

删除条目

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

5.5.4.5 基于协议的 VLAN 端口

简介

在此页面中，指定分配给单独端口的协议和 VLAN。

Protocol based Virtual Local Area Network (VLAN) - Port

General | GVRP | Port Based VLAN | Protocol Based VLAN Group | Protocol Based VLAN Port | Ipv4 Subnet Based VLAN

Port: P0.1

Group Identifier: 1

	Port	Group Identifier	VLAN ID
<input type="checkbox"/>	P0.1	1	VLAN1
<input type="checkbox"/>	P0.2	2	VLAN1

Create Delete Set Values Refresh

显示框说明

该页面包含以下框：

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

该表格包括以下列：

- **第 1 列**
选中要删除的行中的复选框。
- **Port**
显示所有可用端口及链路汇聚。
- **Group Identifier**
显示分配给端口的组 ID。
- **VLAN ID**
从下拉列表中选择要分配给端口的 VLAN ID。

组态步骤

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

5.5.4.6 基于 Ipv4 子网的 VLAN

简介

在此页面中，指定分配给子网的 VLAN ID。

IPV4 Subnet based Virtual Local Area Network (VLAN)

General | GVRP | Port Based VLAN | Protocol Based VLAN Group | Protocol Based VLAN Port | Ipv4 Subnet Based VLAN

Subnet Based VLAN

Port: P0.1

Subnet:

Port	Subnet	VLAN ID
<input type="checkbox"/> P0.1	192.168.10.0	VLAN1

Create Delete Set Values Refresh

显示框说明

该页面包含以下框：

- **复选框“Subnet Based VLAN”**
启用或禁用基于子网的 VLAN 分配。
- **下拉列表“Port”**
从下拉列表中选择端口。可以选择所有可用端口和链路汇聚。
- **Subnet**
输入网络地址。
示例：192.168.10.0 是指包含节点 192.168.10.1 到 192.168.10.254 的网络 192.168.10.x。

该表格包括以下列：

- **第 1 列**
选中要删除的行中的复选框。
- **Port**
显示所有可用端口及链路汇聚。
- **Subnet** 显示分配给端口的子网。
- **下拉列表“VLAN ID”**
选择要分配给端口或子网的 VLAN ID。

组态步骤

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

5.5.5 端口镜像

镜像端口

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

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

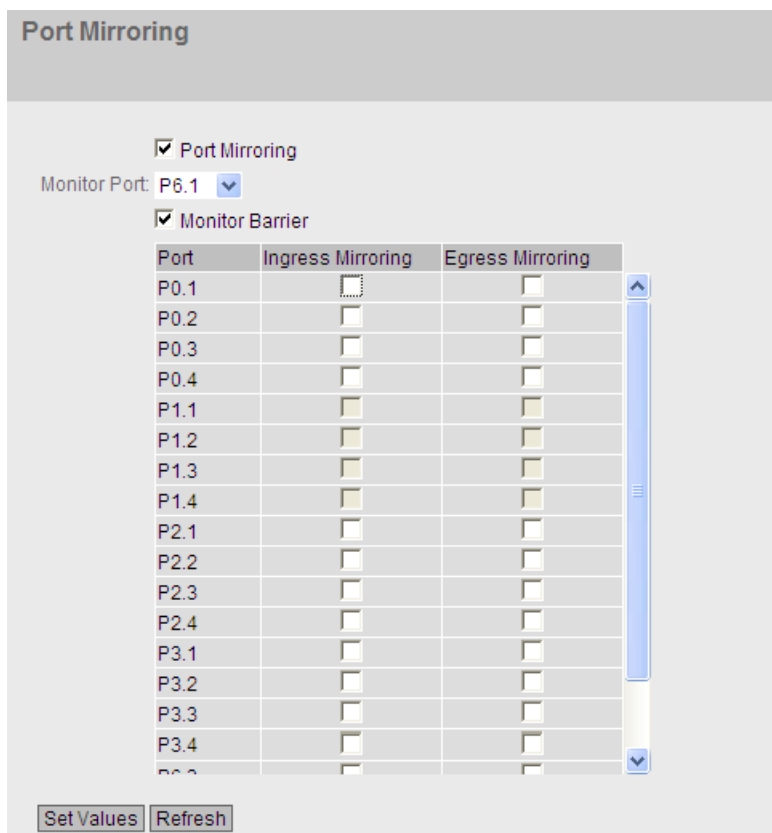
说明

如果镜像端口的最大数据速率大于监视端口的最大数据速率，则数据可能丢失，同时监视端口不再反映镜像端口上的数据通信。可同时将多个端口镜像到一个监视端口。

不能超出交换机核心界限对端口进行镜像。

如果想要将常规终端设备连接到监视端口，请禁用端口镜像功能。

5.5 “第 2 层”菜单



显示框说明

- **复选框“Port Mirroring”**
启用或禁用端口镜像。
- **复选框“Monitor Barrier Enabled”**
启用或禁用此选项可限制通过监视端口进行通信。
 - Enabled
监视端口将无法进行常规帧交换。
 - Disabled
通过监视端口进行通信不受限制。
- **下拉列表“Monitor Port”**
选择要监视的端口。
- **Ingress Mirroring**
启用或禁用监听所需端口的入站数据包。
- **Egress Mirroring**
启用或禁用监听所需端口的出站数据包。

组态步骤

1. 选中“Port Mirroring”复选框。
2. 在“Monitor Port”下拉列表中，选择将监视镜像端口的端口。监视端口必须不同于镜像端口。
3. 在表格中，单击待镜像端口后的行复选框。
选择要监视进入数据包还是离开数据包。
要监视端口的整个数据通信，请同时选中这两个复选框。
4. 单击“Set Values”按钮。

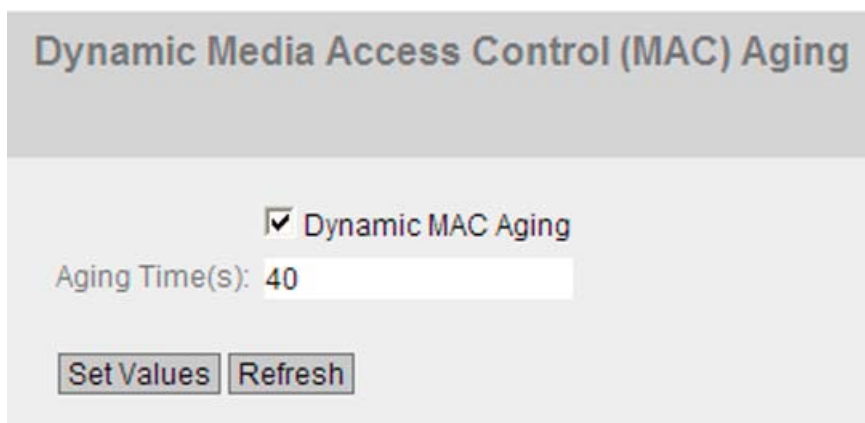
5.5.6 动态 MAC 老化

协议设置和交换机功能

设备自动学习连接节点的源地址。此信息用于将数据帧转发到具体涉及的节点。这将减少其它节点的网络负载。

如果设备在特定时间内未收到源地址与学习的地址相匹配的帧，则设备会删除学习的地址。这种机制称为“**Aging**”。老化可以防止错误地转发帧，例如当某个终端设备（如编程设备）连接到不同的交换机端口时。

如果未启用该复选框，则设备不会自动删除学习的地址。



显示框说明

该页面包含以下框：

- **复选框“Dynamic MAC Aging”**
启用或禁用获取的 MAC 地址的自动老化功能：
- **输入框“Aging Time (s)”**
输入时间（以秒为单位）。经过此时间后，如果设备没有从该发送方地址接收到任何其它帧，则会删除获取的地址。取值范围为 10 秒到 630 秒。

组态步骤

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

5.5.7 MSTP

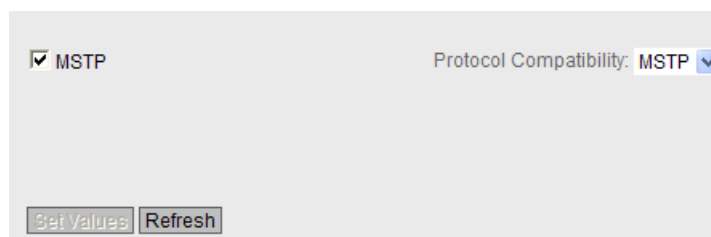
5.5.7.1 常规

MSTP 的常规设置

在此页面，组态 MSTP 的设置。默认情况下会启用快速生成树，可设置为 MSTP、RSTP 或 STP 交换机兼容模式。

在这些功能的组态页面，可进行详细设置。

根据具体的兼容性模式，可以在相关组态页面组态相应的功能。



显示框说明

该页面包含以下框：

- **复选框“MSTP”**
启用或禁用 MSTP。
- **下拉列表“Protocol Compatibility”**
选择 MSTP 的兼容模式，例如，如果选择 RSTP，则 MSTP 的运作方式与 RSTP 类似。

可使用以下设置：

- STP
- RSTP
- MSTP

组态步骤

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

5.5.7.2 CIST 概述

MSTP-CIST 组态

此页面由以下几部分组成。

- 页面的左侧显示设备的组态。
- 中间部分显示根网桥的组态，该组态可从设备接收到的生成树帧获得。
- 右侧显示区域根网桥的组态，该组态可从设备接收到的 MSTP 帧获得。只有在“General”页面上启用“MSTP”，并且为“Protocol Compatibility”设置“MSTP”时，显示的数据才可见。这同样适用于“Bridge Max Hop Count”参数。如果设备是根网桥，则左右两侧显示的信息相匹配。

Bridge Priority: 32768	Root Priority: 0	Regional Root Priority: 0
Bridge Address: 00-00-00-00-00-00	Root Address: 00-00-00-00-00-00	Regional Root Address: 00-00-00-00-00-00
Root Port: -	Root Cost: 0	Regional Root Cost: 0
Topology Changes: 0	Last Topology Change: -	Region Name: 08:00:06:4b:06:01
Bridge Hello Time(s): 2	Root Hello Time(s): 2	Region Version: 0
Bridge Forward Delay(s): 15	Root Forward Delay(s): 15	
Bridge Max Age(s): 20	Root Max Age(s): 20	
Bridge Max Hop Count: 20		

显示框说明

该页面包含以下框：

- **输入框“Bridge Priority”/Root Priority**
Bridge 优先级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。这两个参数（网桥优先级和 MAC 地址）一起形成 Bridge 标识符。由于根网桥管理所有路径的变更，出于帧延迟的考虑，根网桥应该尽可能处在中心位置。网桥优先级的值是 4096 的整数倍数，值范围从 0 到 61440。
- **Bridge Address/Root Address**
网桥地址显示设备的 MAC 地址，根地址显示根网桥的 MAC 地址。
- **Root Port**
显示交换机与根网桥通信时所使用的端口。

- **Root Cost**
从该设备到根网桥的路径成本。
- **Topology Changes/Last Topology Change**
该设备条目显示自上次启动以来，由于生成树机制而执行的重新组态操作次数。对于根网桥，自上次重新组态到现在的时间显示如下：
 - 秒： 数字后的秒单位
 - 分钟： 数字后的分钟单位
 - 小时： 数字后的小时单位
- **Bridge Hello Time(s)/Root Hello Time(s)**
每个网桥都会定期发送组态帧 (BPDU)。 呼叫时间即为两个此类帧之间的时间间隔。此参数的默认值为 2 秒。
- **Bridge Forward Delay(s)/Root Forward Delay(s)**
网桥不会立即使用新组态数据，而是在经过“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。
- **Bridge Max Age/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”。 此参数默认为 20。
- **Regional Root Priority**
相关描述，请参见 Bridge Priority/Root Priority
- **Regional Root Address**
设备的 MAC 地址。
- **Regional Root Cost**
从该设备到根网桥的路径成本。
- **Bridge Max Hop Count**
此参数指定 BPDU 会通过多少个 MSTP 节点。 如果接收到一个 MSTP BPDU 并且其跳跃计数超过此处组态的值，则会将其丢弃。 此参数默认为 20。
- **输入框“Region Name”**
输入此设备所属的 MSTP 区域的名称。 默认情况下，在此处输入此设备的 MAC 地址。 所有属于相同 MSTP 区域的设备上的值必须相同。
- **输入框“Region Version”**
输入设备所在的 MSTP 区域的版本号。 所有属于相同 MSTP 区域的设备上的该值必须相同

5.5 “第 2 层”菜单

组态步骤

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

5.5.7.3 CIST 端口

MSTP-CIST 端口组态

调用此页面时，表中显示端口参数组态的当前状态。

要进行组态，请单击端口表中的相关单元格。

Common Internal Spanning Tree (CIST) Port											
General CIST General CIST Port MST General MST Port											
		MSTP Status		Copy to Table							
All ports		No Change		Copy to Table							
Port	MSTP Status	Priority	Cost Calc.	Path Cost	State	Fwd. Trans	Edge Type	Edge	P.t.P. Type	P.t.P.	Hello Tim
P0.1	<input checked="" type="checkbox"/>	128	0	20000	Forwarding	2	Auto	<input type="checkbox"/>	-	<input checked="" type="checkbox"/>	2
P0.2	<input checked="" type="checkbox"/>	128	0	2000000	Discarding	0	Auto	<input type="checkbox"/>	-	<input type="checkbox"/>	2
P0.3	<input checked="" type="checkbox"/>	128	0	2000000	Discarding	0	Auto	<input type="checkbox"/>	-	<input type="checkbox"/>	2
P0.4	<input checked="" type="checkbox"/>	128	0	2000000	Discarding	0	Auto	<input type="checkbox"/>	-	<input type="checkbox"/>	2
P1.1	<input checked="" type="checkbox"/>	128	0	20000	Discarding	1	Auto	<input type="checkbox"/>	-	<input checked="" type="checkbox"/>	2
P1.2	<input checked="" type="checkbox"/>	128	0	20000	Discarding	3	Auto	<input type="checkbox"/>	-	<input checked="" type="checkbox"/>	2
P1.3	<input checked="" type="checkbox"/>	128	0	20000	Discarding	0	Auto	<input type="checkbox"/>	-	<input type="checkbox"/>	2
P1.4	<input checked="" type="checkbox"/>	128	0	200000	Discarding	5	Auto	<input type="checkbox"/>	-	<input checked="" type="checkbox"/>	2
P2.1	<input checked="" type="checkbox"/>	128	0	200000000	Discarding	0	Auto	<input type="checkbox"/>	-	<input type="checkbox"/>	2
P2.2	<input checked="" type="checkbox"/>	128	0	200000000	Discarding	0	Auto	<input type="checkbox"/>	-	<input type="checkbox"/>	2
P2.3	<input checked="" type="checkbox"/>	128	0	200000000	Discarding	0	Auto	<input type="checkbox"/>	-	<input type="checkbox"/>	2
P2.4	<input checked="" type="checkbox"/>	128	0	200000000	Discarding	0	Auto	<input type="checkbox"/>	-	<input type="checkbox"/>	2
P3.1	<input checked="" type="checkbox"/>	128	0	200000000	Discarding	0	Auto	<input type="checkbox"/>	-	<input type="checkbox"/>	2
P3.2	<input checked="" type="checkbox"/>	128	0	200000000	Discarding	0	Auto	<input type="checkbox"/>	-	<input type="checkbox"/>	2
P3.3	<input checked="" type="checkbox"/>	128	0	200000000	Discarding	0	Auto	<input type="checkbox"/>	-	<input type="checkbox"/>	2
P3.4	<input checked="" type="checkbox"/>	128	0	200000000	Discarding	0	Auto	<input type="checkbox"/>	-	<input type="checkbox"/>	2
P4.1	<input checked="" type="checkbox"/>	128	0	200000000	Discarding	0	Auto	<input type="checkbox"/>	-	<input type="checkbox"/>	2
P4.2	<input checked="" type="checkbox"/>	128	0	200000000	Discarding	0	Auto	<input type="checkbox"/>	-	<input type="checkbox"/>	2
P4.3	<input checked="" type="checkbox"/>	128	0	200000000	Discarding	0	Auto	<input type="checkbox"/>	-	<input type="checkbox"/>	2
P4.4	<input checked="" type="checkbox"/>	128	0	200000000	Discarding	0	Auto	<input type="checkbox"/>	-	<input type="checkbox"/>	2
P5.1	<input checked="" type="checkbox"/>	128	0	200000000	Discarding	0	Auto	<input type="checkbox"/>	-	<input type="checkbox"/>	2
P5.2	<input checked="" type="checkbox"/>	128	0	200000000	Discarding	0	Auto	<input type="checkbox"/>	-	<input type="checkbox"/>	2
P5.3	<input checked="" type="checkbox"/>	128	0	200000000	Discarding	0	Auto	<input type="checkbox"/>	-	<input type="checkbox"/>	2
P5.4	<input checked="" type="checkbox"/>	128	0	200000000	Discarding	0	Auto	<input type="checkbox"/>	-	<input type="checkbox"/>	2
P6.1	<input checked="" type="checkbox"/>	128	0	200000000	Discarding	0	Auto	<input type="checkbox"/>	-	<input type="checkbox"/>	2
P6.2	<input checked="" type="checkbox"/>	128	0	200000000	Discarding	0	Auto	<input type="checkbox"/>	-	<input type="checkbox"/>	2

显示框说明

表 1 包含以下列：

- **第 1 列**
说明设置对于表 2 的所有端口都有效。
- **MSTP Status**
从下拉列表中选择设置。可选择以下设置选项：
 - enabled
将端口集成到生成树中。
 - disabled
不将端口集成到生成树中。
 - No Change
表 2 保持不变。
- **Copy to Table**
如果单击此按钮，将为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **Port**
显示可用端口。端口由端口号和插槽号组成，例如，端口 0.1 表示插槽 0，端口 1。
- **MSTP Status**
指定是否将端口集成到生成树中。

说明

如果禁用端口的“MSTP Status”选项，可能导致形成环路。必须留意拓扑。

- **Priority**
输入端口的优先级。仅当路径成本相同时才评估优先级。
该值必须能被 16 整除。如果该值不能被 16 整除，则会自动调整该值。
值范围：0 - 240。
默认值为 128。
- **Cost Calc**
输入路径成本计算。如果输入值“0”，则自动计算出的值会显示在“Path Cost”框中。
- **Path Cost**
此参数用于计算将要选择的路径。选择值最小的路径作为路径。如果设备的多个端口的路径成本值相同，则选择端口号最小的端口。
如果“Cost Calc”字段中的值为“0”，则会显示自动计算出的值。

5.5 “第 2 层”菜单

否则会显示“Cost Calc”字段的值。

主要根据传输速度来计算路径成本。可达到的传输速度越高，路径成本的值就越低。

快速生成树的典型路径成本值如下：

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

但是，也可以单独设置各个值。

- **Status**

显示端口的当前状态。这些值只能显示，但无法组态。“Status”参数取决于组态的协议。可能的状态有：

- **Disabled**
该端口仅接收，并且不包括在 STP、MSTP 和 RSTP 中。
- **Discarding**
在“Discarding”模式下，接收 BPDU 帧。其它进入或离开的帧会被丢弃。
- **listening**
在此状态下，接收和发送 BPDU。端口包括在生成树算法中。
- **Learning**
转发状态之前的阶段，端口主动学习拓扑（换句话说，节点寻址）。
- **Forwarding**
在重新组态时间后，端口在网络中激活；端口接收和转发数据帧。

- **Fwd. Trans**

指定从“Discarding”状态变为“Forwarding”状态的次数。

- **Edge Type**

指定边缘端口的类型。可做以下选择：

- "-"

禁用边缘端口。端口被视为“无边缘端口”。

- Admin

当此端口上始终有终端设备时，选择此选项。否则，每次更改连接时都会触发对网络的重新组态。

- Auto

如果想要自动检测此端口上连接的终端设备，则选择此选项。首次建立连接时，会将端口视为“无边缘端口”。

- Admin/Auto

如果要在该端口上结合这两个选项，则同时选择这些选项。首次建立连接时，会将端口视为“边缘端口”。

- **Edge**

显示端口的状态。

- Enabled

终端设备连接到此端口。

- Disabled

此端口上有生成树或快速生成树设备。

有了终端设备，交换机可以通过端口更快地进行切换，而无需考虑生成树帧。如果忽略此设置而接收生成树帧，则该端口将针对交换机自动切换为“Disabled”设置。

- **P.t.P. Type**

从下拉列表中选择所需选项。选择项取决于设置的端口。

- "-"

自动计算点对点。如果端口被设置为半双工，则不认为是点对点链路。

- P.t.P.

即使为半双工，也认为是点对点链路。

- Shared Media

即使为全双工连接，也不认为是点对点链路。

说明

点对点连接表示在两个设备之间直接连接。而共享介质连接可以是与集线器的连接。

5.5 “第 2 层”菜单

- **Hello Time**

输入时间间隔，经过该时间后，网桥会发送组态 BPDU。默认情况下，会设置 2 秒。
值范围： 1-2 秒

说明

只有在 MSTP 兼容模式下才能对呼叫时间进行端口特定的设置。

组态步骤

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

5.5.7.4 MST 概述

多重生成树组态

除 RSTP 之外，通过 MSTP 也可以在 LAN 中使用单独的 RSTP 树管理多个 VLAN。

Multiple Spanning Tree (MST) General

General | CIST General | CIST Port | MST General | MST Port

MSTP Instance ID:

	MSTP Instance ID	Root Address	Root Priority	Bridge Priority	VLAN ID
<input type="checkbox"/>	1	08-00-06-4b-69-01	32768	32768	1
<input type="checkbox"/>	2	08-00-06-4b-69-01	32768	32768	2
<input type="checkbox"/>	3	08-00-06-4b-69-01	32768	32768	3

Create Delete Set Values Refresh

显示框说明

该页面包含以下框：

- **输入框“MSTP Instance ID”**

输入 MSTP 实例数。

允许值： 0 - 64

该表格包括以下列：

- **第 1 列**
选中要删除的行中的复选框。
- **MSTP Instance ID**
显示 MSTP 实例数。
- **Root Address**
显示根网桥的 MAC 地址。
- **Root Priority**
显示根网桥的优先级。
- **Bridge Priority**
在此框中输入网桥优先级。网桥优先级的值是 4096 的整数倍数，值范围从 0 到 61440。
- **VLAN ID**
输入 VLAN ID。在此处还可以通过“起始 ID”、“-”、“结束 ID”来指定范围。用“,”分隔多个范围或 ID。
允许值：1 - 4094

组态步骤

创建新条目

1. 在“MSTP Instance ID”框中输入 MSTP 实例数。
2. 单击“Create”按钮。
3. 在“VLAN ID”输入框中输入虚拟 LAN 的标识符。
4. 在“Bridge Priority”输入框中输入网桥的优先级。
5. 单击“Set Values”按钮。

删除条目

1. 使用相关行开始位置的复选框，选择要删除的条目。
2. 单击“Delete”按钮从内存中删除所选的条目。从设备的内存中删除条目并更新该页面的显示。

5.5 “第 2 层”菜单

5.5.7.5 MST 端口

组态多重生成树端口参数

在此页面，设置所组态多重生成树实例的端口参数。

Multiple Spanning Tree (MST) Port

General | CIST General | CIST Port | MST General | **MST Port**

MSTP Instance ID: 3

	MSTP Status	Copy to Table
All ports	No Change	Copy to Table

Port	MSTP Instance ID	MSTP Status	Priority	Cost Calc.	Path Cost	State	Fwd. Trans.
P0.1	3	<input type="checkbox"/>	128	0	2000000	Discarding	0
P0.2	3	<input type="checkbox"/>	128	0	2000000	Discarding	0
P0.3	3	<input type="checkbox"/>	128	0	2000000	Discarding	0
P0.4	3	<input type="checkbox"/>	128	0	2000000	Discarding	0
P2.1	3	<input type="checkbox"/>	128	0	20000	Discarding	0
P2.2	3	<input type="checkbox"/>	128	0	20000	Discarding	0
P2.3	3	<input type="checkbox"/>	128	0	20000	Forwarding	0
P2.4	3	<input type="checkbox"/>	128	0	20000	Forwarding	0
P3.1	3	<input type="checkbox"/>	128	0	200000000	Discarding	0
P3.2	3	<input type="checkbox"/>	128	0	200000000	Discarding	0
P3.3	3	<input type="checkbox"/>	128	0	200000000	Discarding	0
P3.4	3	<input type="checkbox"/>	128	0	200000000	Discarding	0
P4.1	3	<input type="checkbox"/>	128	0	20000	Discarding	0

显示框说明

该页面包含以下框：

- 下拉列表“MSTP Instance ID”
在下拉列表中选择 MSTP 实例的 ID。

表 1 包含以下列：

- 第 1 列
显示设置对于所有端口有效。
- MSTP Status
从下拉列表中选择设置。可选择以下设置选项：
 - enabled
 - disabled
 - No Change: 表 2 保持不变。

- **Copy to Table**

如果单击此按钮，将为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **Port**

显示所有可用端口和链路汇聚。

- **MSTP Instance ID**

MSTP 实例的 ID。

- **MSTP Status**

单击此复选框可启用或禁用此选项。

- **Priority**

输入端口的优先级。仅当路径成本相同时才评估优先级。

该值必须能被 16 整除。如果该值不能被 16 整除，则会自动调整该值。

值范围：0 - 240。

默认值为 128。

- **Cost Calc**

在该输入框中输入路径成本计算。如果在此输入值“0”，则自动计算出的值会显示在下一个“Path Cost”框中。

- **Path Cost**

从该端口到根网桥的路径成本。选择值最小的路径作为路径。如果设备的多个端口具有相同的值，则选择端口号最小的端口。

如果“Cost Calc”字段中的值为“0”，则显示自动计算出的值。

否则会显示“Cost Calc”字段的值。

主要根据传输速度来计算路径成本。可达到的传输速度越高，路径成本的值就越低。

快速生成树的典型值如下：

– 1000 Mbps = 20,000

– 100 Mbps = 200,000

– 10 Mbps = 2,000,000

但是，也可以单独设置各个值。

5.5 “第 2 层”菜单

- **State**

显示端口的当前状态。这些值只能显示，但无法组态。可能的状态有：

- **Discarding**

端口会交换 MSTP 信息，但不会参与数据通信。

- **Blocked**

在阻止模式下，接收 BPDU 帧。

- **Forwarding**

端口接收和发送数据帧。

组态步骤

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

5.5.8 链路汇聚

捆绑网络连接以实现冗余和更高带宽

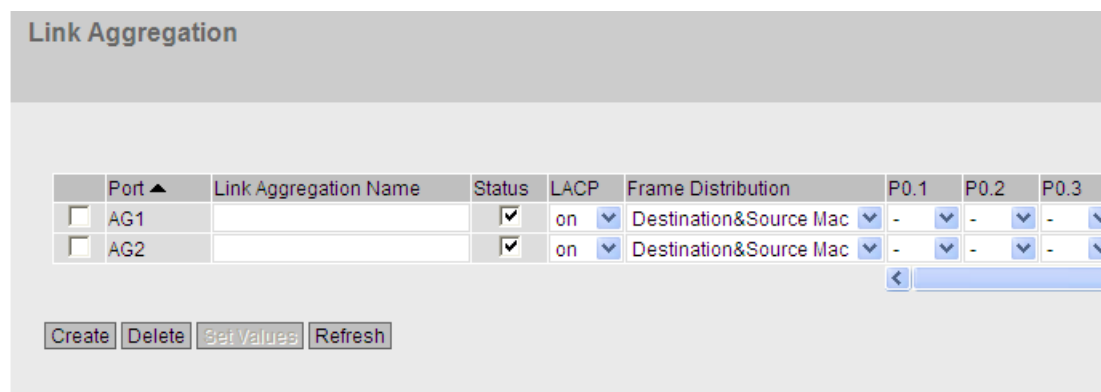
根据 IEEE 802.3ad，链路汇聚允许将相邻设备之间的多个连接捆绑在一起，以实现更高的带宽并防止发生故障。

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

可最多定义 8 个链路汇聚。最多可为每个链路汇聚分配 8 个端口。

显示已组态的汇聚

该菜单显示所有已组态的链路汇聚。



Port ▲	Link Aggregation Name	Status	LACP	Frame Distribution	P0.1	P0.2	P0.3
<input type="checkbox"/> AG1		<input checked="" type="checkbox"/>	on ▼	Destination&Source Mac ▼	- ▼	- ▼	- ▼
<input type="checkbox"/> AG2		<input checked="" type="checkbox"/>	on ▼	Destination&Source Mac ▼	- ▼	- ▼	- ▼

Buttons: Create, Delete, Set Values, Refresh

显示框说明

该表格包括以下列：

- **第 1 列**
选中要删除的行中的复选框。
- **Port**
显示此链路汇聚的虚拟端口号。该标识符是由固件内部分配的。
- **Link Aggregation Name**
显示链路汇聚的名称。此名称可由用户在组态期间指定。名称并非绝对必要，但对于区分多个链路汇聚会很有用。

5.5 “第 2 层”菜单

- **LACP**
 - On
启用发送 LACP 帧。
 - Off
禁用发送 LACP 帧。
- **Status**

启用或禁用链路汇聚。
- **Frame Distribution**

设置汇聚的各个连接上的数据包分发类型。

 - Source MAC
根据源 MAC 地址进行分发。
 - Destination MAC
根据目标 MAC 地址进行分发。
 - Destination&Source MAC
根据目标 MAC 地址与源 MAC 地址的组合进行分发。
 - Source IP
根据源 IP 地址进行分发
 - Destination IP
根据目标 IP 地址进行分发。
 - Destination&Source IP
根据目标 IP 地址与源 IP 地址的组合进行分发。
- **Port**

显示属于此链路汇聚的端口。可以从下拉列表中选择下列值：

 - "-"（禁用）
禁用链路汇聚。
 - "a"（主动）
端口发送 LACP 帧，并只在接收到 LACP 帧时参与链路汇聚。
 - "p"（被动）
端口只在接收到 LACP 帧时参与链路汇聚。
 - "o"（启用）
端口参与链路汇聚，并且不会发送任何 LACP 帧。

说明

在“链路汇聚”内，仅可使用具有以下组态的端口：

- 所有带“o”的端口
 - 所有带“a”或“p”的端口。
-

组态步骤**组态前的基本设置**

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

说明

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

创建新链路汇聚

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

删除汇聚

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

更改汇聚

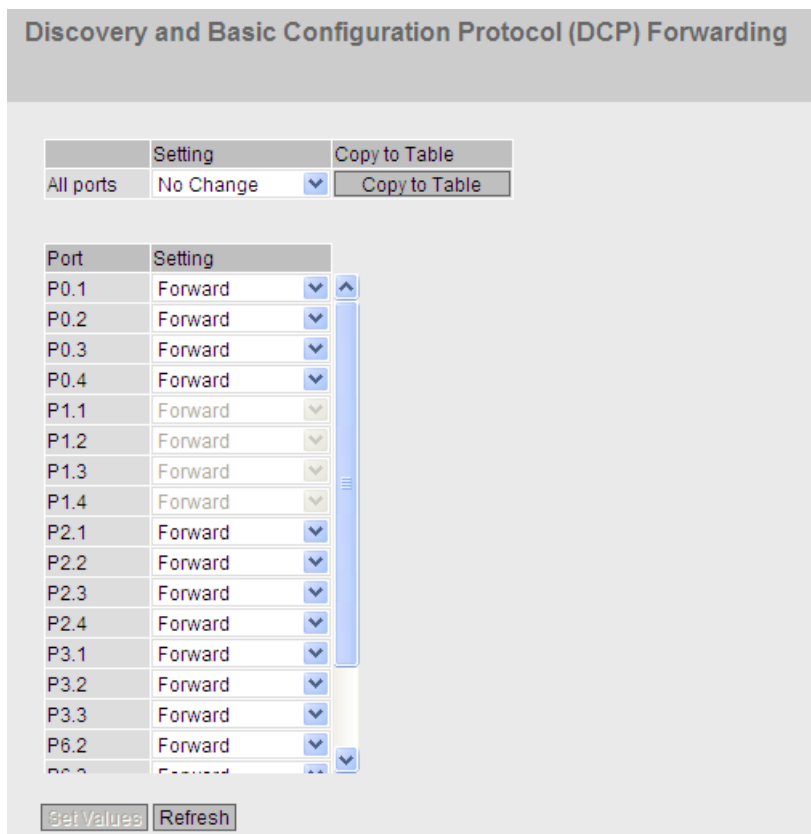
1. 在总览中，单击相关的表条目来更改所创建链路汇聚的组态。
2. 进行所有更改。
3. 单击“Set Values”按钮。

5.5.9 DCP 转发

应用

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

设备的所有端口都在此页面上显示。在每个显示的端口后面，有一个用来选择功能的下拉列表。



显示值说明

表 1 包含以下列：

- **第 1 列**
说明设置对于表 2 的所有端口都有效。
- **Setting**
从下拉列表中选择设置。 如果选择“**No Change**”，则表 2 中的条目保持不变。
- **Copy to Table**
如果单击此按钮，将为表 2 的所有端口应用此设置。

表 2 包含以下列：

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

组态步骤

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

5.5 “第 2 层”菜单

5.5.10 LLDP

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。

Link Layer Discovery Protocol (LLDP)

	Setting	Copy to Table
All ports	No Change	Copy to Table

Port	Setting
P0.1	Rx & Tx
P0.2	Rx & Tx
P0.3	Rx & Tx
P0.4	Rx & Tx
P1.1	Rx & Tx
P1.2	Rx & Tx
P1.3	Rx & Tx
P1.4	Rx & Tx
P2.1	Rx & Tx
P2.2	Rx & Tx
P2.3	Rx & Tx
P2.4	Rx & Tx
P3.1	Rx & Tx
P3.2	Rx & Tx
P6.2	Rx & Tx
P6.3	Rx & Tx

Set Values Refresh

显示框说明

表 1 包含以下列：

- **第 1 列**
显示设置对于所有端口有效。
- **Setting**
从下拉列表中选择设置。如果选择“No Change”，则表 2 中的条目保持不变。
- **Copy to Table**
如果单击此按钮，将为表 2 的所有端口应用此设置。

表 2 包含以下列：

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

组态步骤

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

5.5 “第 2 层”菜单

5.5.11 单播

5.5.11.1 过滤

地址过滤

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

在此页面中，还可定义静态单播过滤器。

	VLAN ID	MAC Address	Status	Port
<input type="checkbox"/>	1	08-00-06-01-00-00	Learnt	P11.1
<input type="checkbox"/>	1	08-00-06-4b-67-04	Learnt	P0.1
<input type="checkbox"/>	1	08-00-06-4b-67-3f	Learnt	P0.1
<input type="checkbox"/>	1	08-00-06-4b-8f-09	Learnt	P11.1
<input type="checkbox"/>	1	6c-62-6d-6f-38-31	Learnt	P11.1

显示框说明

该页面包含以下框：

- **下拉列表“VLAN ID”**
选择 VLAN ID，以此来组态新静态 MAC 地址。如果未进行任何设置，则会将“VLAN1”设置为基本设置。
- **输入框“MAC Address”**
输入 MAC 地址。

该表包含以下各列：

- **第 1 列**
选中要删除的行中的复选框。
- **VLAN ID**
显示分配给此 MAC 地址的 VLAN-ID。

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

说明

您只能为单播地址指定一个端口。

组态步骤

要编辑条目，请按以下步骤操作。请注意，无法修改自动学习的条目（状态 =“Learnt”）。

创建新条目

1. 选择相关 VLAN ID。
2. 在“MAC Address”输入框中输入 MAC 地址。
3. 单击“Create”按钮在表中创建新条目。
4. 从下拉列表中选择相关端口。
5. 单击“Set Values”按钮。

更改条目

1. 选择相关端口。
2. 单击“Set Values”按钮。

5.5 “第 2 层”菜单

删除条目

1. 选中要删除的行中的复选框。
对所有要删除的条目重复此步骤。
2. 单击“Delete”按钮从过滤表中删除所选的条目。

5.5.11.2 锁定端口

激活访问控制

在此页面中，可以针对未知节点阻止各个端口。

如果启用了“端口锁定”功能，则从未知 MAC 地址到达此端口的数据包会被立即丢弃。端口会接受已知节点发出的数据包。

由于启用了“端口锁定”功能的端口无法获取任何 MAC 地址，因此在启用“端口锁定”功能后，这些端口上之前获取的地址将被自动删除。

该端口仅接受之前手动创建或使用“Start Learning”功能和“Stop Learning”功能创建的静态 MAC 地址。

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

Port	Setting
P0.1	<input type="checkbox"/>
P0.2	<input type="checkbox"/>
P0.3	<input type="checkbox"/>
P0.4	<input type="checkbox"/>
P1.1	<input type="checkbox"/>
P1.2	<input type="checkbox"/>
P1.3	<input type="checkbox"/>
P1.4	<input type="checkbox"/>
P2.1	<input type="checkbox"/>
P2.2	<input type="checkbox"/>
P2.3	<input type="checkbox"/>
P2.4	<input type="checkbox"/>
P3.1	<input type="checkbox"/>
P6.1	<input type="checkbox"/>

5.5 “第 2 层”菜单

显示框说明

表 1 包含以下列：

- **第 1 列**
说明设置对于表 2 的所有端口都有效。
- **Setting**
从下拉列表中选择设置。可选择以下设置选项：
 - **enabled**
启用端口锁定功能。
 - **disabled**
禁用端口锁定功能。
 - **No Change**
表 2 保持不变。
- **Copy to Table**
如果单击此按钮，将为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **Port**
此列会列出此设备上的全部可用端口。
- **复选框“Setting”**
启用或禁用对端口的访问控制。

组态步骤

对单独的端口启用访问控制

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

对所有端口启用访问控制

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

5.5.11.3 学习

开始/停止学习

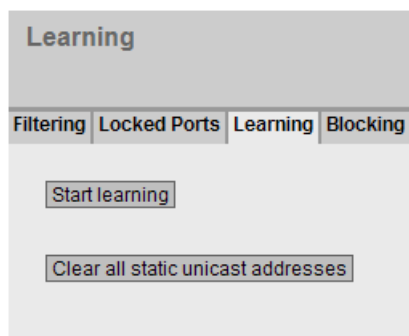
通过自动学习功能，在单播过滤器表中将自动输入所有相连的设备。只要启用“Start learning”功能，所有学习的单播地址就会立即被创建为静态单播条目。

只有单击“Stop learning”按钮后，才会结束学习过程。使用此方法时，较大网络中的学习过程可能会花费数分钟或数小时，才能真正学习到所有节点。只能找到在学习阶段发送数据包的节点。

通过随后启用“端口锁定”功能，在相关端口上将只接受来自学习阶段结束时识别的节点（静态单播条目）的数据包。

说明

如果在自动学习阶段之前已对各个端口激活“端口锁定”功能，则在这些端口上将不会学习到任何地址。这样便可限制特定端口的学习行为。为此，可先针对不希望其学习地址的端口，启用“端口锁定”功能。



组态步骤

学习地址

1. 单击“Start learning”按钮开始学习阶段。
开始学习阶段后，“Start learning”按钮将被“Stop learning”按钮代替。
设备随即会输入所连接设备的地址，直到您停止此功能。
2. 单击“Stop learning”按钮可停止学习功能。
此按钮再次被“Start Learning”按钮所代替。存储已学习的条目。

5.5 “第 2 层”菜单

删除所有静态单播地址。

1. 单击“Clear all static unicast addresses”按钮可删除所有静态条目。

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

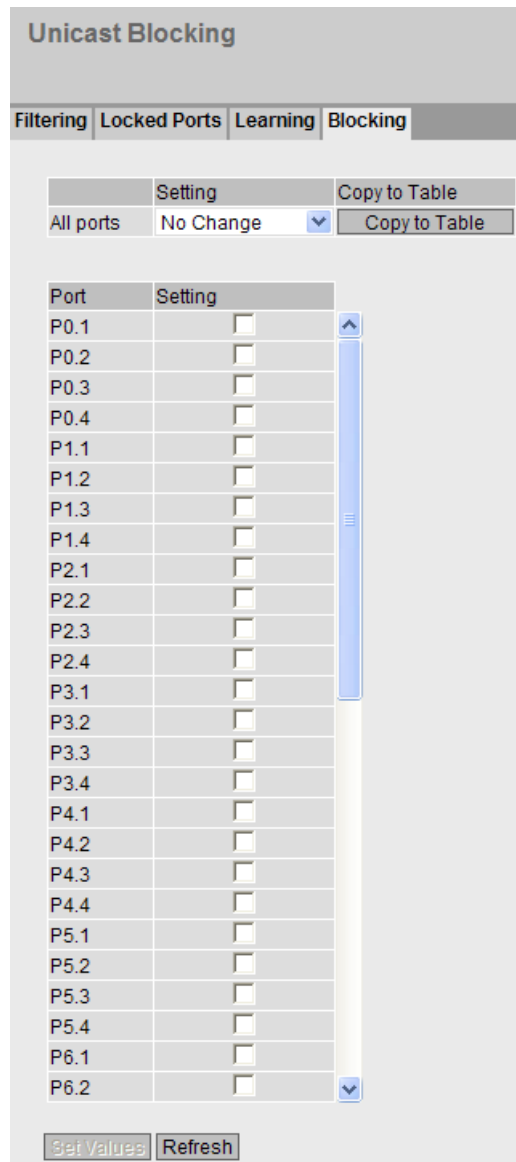
说明

根据涉及的条目数，删除过程可能需要一些时间。

5.5.11.4 未知单播阻止

阻止转发未知单播帧

在此页面上，可阻止各个端口转发未知单播帧。



The image shows a web-based configuration interface for "Unicast Blocking". It features a tabbed menu with "Filtering", "Locked Ports", "Learning", and "Blocking" selected. Below the tabs, there is a summary row with "All ports" and a "Setting" dropdown menu set to "No Change", along with a "Copy to Table" button. The main area contains a table with two columns: "Port" and "Setting". The "Port" column lists ports from P0.1 to P6.2. The "Setting" column contains checkboxes, all of which are currently unchecked. A vertical scrollbar is visible on the right side of the table. At the bottom of the page, there are two buttons: "Set Values" and "Refresh".

Port	Setting
P0.1	<input type="checkbox"/>
P0.2	<input type="checkbox"/>
P0.3	<input type="checkbox"/>
P0.4	<input type="checkbox"/>
P1.1	<input type="checkbox"/>
P1.2	<input type="checkbox"/>
P1.3	<input type="checkbox"/>
P1.4	<input type="checkbox"/>
P2.1	<input type="checkbox"/>
P2.2	<input type="checkbox"/>
P2.3	<input type="checkbox"/>
P2.4	<input type="checkbox"/>
P3.1	<input type="checkbox"/>
P3.2	<input type="checkbox"/>
P3.3	<input type="checkbox"/>
P3.4	<input type="checkbox"/>
P4.1	<input type="checkbox"/>
P4.2	<input type="checkbox"/>
P4.3	<input type="checkbox"/>
P4.4	<input type="checkbox"/>
P5.1	<input type="checkbox"/>
P5.2	<input type="checkbox"/>
P5.3	<input type="checkbox"/>
P5.4	<input type="checkbox"/>
P6.1	<input type="checkbox"/>
P6.2	<input type="checkbox"/>

5.5 “第 2 层”菜单

显示值说明

表 1 包含以下列：

- **第 1 列**
说明设置对于表 2 的所有端口都有效。
- **Setting**
从下拉列表中选择设置。可选择以下设置选项：
 - **enabled**
单播帧阻止功能已启用。
 - **disabled**
单播帧阻止功能已禁用。
 - **No Change**
表 2 保持不变。
- **Copy to Table**
如果单击此按钮，将为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **Port**
所有可用端口均列于此列中。不显示不可用端口。
- **Setting**
启用或禁用单播帧阻止功能。

组态步骤

对单独的端口启用阻止功能

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

对所有端口启用阻止功能

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

5.5.12 组播

5.5.12.1 组

组播应用

在多数情况下，具有单播地址的帧将被发送到一个特定接收方。如果某个应用向多个接收方发送相同的数据，则使用一个组播地址发送数据可以减少数据量。对于某些应用，存在固定的组播地址（NTP、IETF1 音频、IETF1 视频等）。

减少网络负载

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

- 组播过滤表中地址的静态条目。
- 通过监听 IGMP 参数分配帧（IGMP 组态）生成地址的动态条目。
- 通过 GMRP 帧激活动态地址分配。

所有这些方法的结果是，组播帧只会被发送到输入了相应地址的端口。

“Multicast”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（设备已学习），也可以是静态的（由用户设置）。

组态组播地址

Multicast Configuration

Groups
IGMP
GMRP

Block Unknown Multicasts

VLAN ID: VLAN1

MAC Address:

VLAN ID	MAC Address	Status	P0.1	P0.2	P0.3	P0.4	P1.1	P1.2
0 entries.								

Create
Delete
Set Values
Refresh

显示框说明

该页面包含以下框：

- **复选框“Block Unknown Multicasts”**
如果启用此复选框，则工业以太网交换机不会将任何组播数据包转发到未知目标地址。要进行转发，必须使组播地址已知。
- **下拉列表“VLAN ID”**
单击此文本框，将显示一个下拉列表。此处可选择要组态的新 MAC 地址的 VLAN ID。
- **文本框“MAC Address”**
在此处输入要组态的新 MAC 组播地址。

该表格包括以下列：

- **第 1 列**
选中要删除的行中的复选框。
- **VLAN ID**
此处显示 VLAN 的 VLAN ID，该行的 MAC 组播地址分配给此 ID。
- **MAC Address**
此处显示设备已学习或用户已组态的组播地址。
- **Status**
显示每个地址条目的状态。可能的信息如下：
 - **Static**
该地址是由用户以静态方式输入的。静态地址会永久存储；也就是说，当老化时间结束或设备重启时，静态地址不会被删除。这些地址必须由用户删除。
 - **IGMP**
此地址的目标端口通过 IGMP 组态获得。
 - **GMRP**
此地址的目标端口由收到的 GMRP 帧注册。

- **Port List**

每个插槽都有一列对应。在每一列内，端口所属的组播组显示如下。该下拉列表提供以下选项：

- M

（成员）通过此端口发送组播帧。

- R

- （已注册）组播组的成员，由 GMRP 帧注册。

- I

（IGMP）组播组的成员，由 IGMP 帧注册。

- -

不是组播组的成员。不通过此端口发送包含所定义组播 MAC 地址的组播帧。

- F

（已禁止）不是组播组的成员。此地址也不能是使用 GMRP 或 IGMP 动态学习的地址。

组态步骤

创建新条目

1. 在“VLAN ID”文本框中指定所需的 ID。
2. 在“MAC Address”输入框中输入 MAC 地址。
3. 单击“Create”按钮。会在表中生成一个新条目。
4. 将相关端口分配给 MAC 地址。
5. 单击“Set Values”按钮。

删除条目

1. 选中要删除的行中的复选框。
2. 单击“Delete”按钮。
将从显示画面以及设备的内存中删除该行。

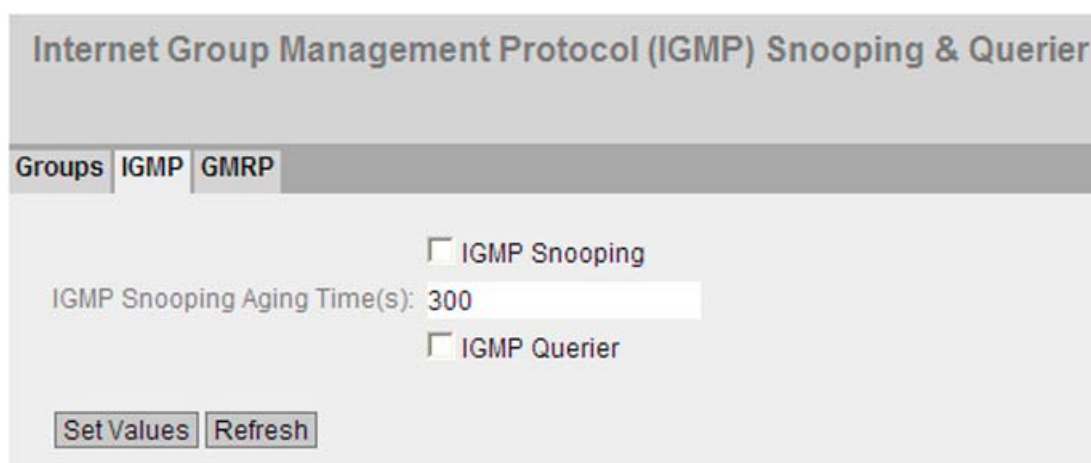
5.5.12.2 IGMP

指定 IGMP 监听老化时间

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

这适用于所有端口；但无法对具体端口进行组态。

工业以太网交换机不但支持“IGMP snooping”，还支持 IGMP querier 功能。如果启用“IGMP snooping”，就会评估 IGMP 帧，并用该评估信息更新组播过滤表。如果还启用了 IGMP 查询，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。



Internet Group Management Protocol (IGMP) Snooping & Querier

Groups IGMP GMRP

IGMP Snooping

IGMP Snooping Aging Time(s): 300

IGMP Querier

Set Values Refresh

显示框说明

该页面包含以下框：

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

组态步骤

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

5.5 “第 2 层”菜单

5.5.12.3 GMRP

激活 GMRP

通过选中该复选框，来指定是否对各个端口使用 GMRP。如果对某个端口禁用“GMRP”，则不会注册该端口，且该端口也不能发送 GMRP 帧。

GARP Multicast Registration Protocol (GMRP)

Groups | IGMP | GMRP

GMRP

	Setting	Copy to Table
All ports	No Change	Copy to Table

Port	Setting
P0.1	<input checked="" type="checkbox"/>
P0.2	<input checked="" type="checkbox"/>
P0.3	<input checked="" type="checkbox"/>
P0.4	<input checked="" type="checkbox"/>
P1.1	<input checked="" type="checkbox"/>
P1.2	<input checked="" type="checkbox"/>
P1.3	<input checked="" type="checkbox"/>
P1.4	<input checked="" type="checkbox"/>
P2.1	<input checked="" type="checkbox"/>
P2.2	<input checked="" type="checkbox"/>
P2.3	<input checked="" type="checkbox"/>
P2.4	<input checked="" type="checkbox"/>
P3.1	<input checked="" type="checkbox"/>
P3.2	<input checked="" type="checkbox"/>
P3.3	<input checked="" type="checkbox"/>
P3.4	<input checked="" type="checkbox"/>
P4.1	<input checked="" type="checkbox"/>
P4.2	<input checked="" type="checkbox"/>
P4.3	<input checked="" type="checkbox"/>
P4.4	<input checked="" type="checkbox"/>
P5.1	<input checked="" type="checkbox"/>
P5.2	<input checked="" type="checkbox"/>
P5.3	<input checked="" type="checkbox"/>
P5.4	<input checked="" type="checkbox"/>

Set Values Refresh

显示框说明

该页面包含以下框：

- **复选框“GMRP”**
启用或禁用 GMRP 功能。

表 1 包含以下列：

- **第 1 列**
说明设置对于表 2 的所有端口都有效。
- **Setting**
从下拉列表中选择设置。可选择以下设置选项：
 - **enabled**
启用发送 GRMP 帧。
 - **disabled**
禁用发送 GRMP 帧。
 - **No Change**
表 2 保持不变。
- **Copy to Table**
如果单击此按钮，将为表 2 的所有端口应用这些设置。

表 2 包含以下列：

- **Port**
该列会显示设备上的所有可用端口以及链路汇聚。
- **Setting**
使用此复选框，可针对每个端口或链路汇聚启用或禁用 GMRP。

组态步骤

针对单独端口启用发送 GMRP 帧

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

5.5 “第 2 层”菜单

针对所有端口启用发送 GMRP 帧

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

5.5.13 广播

阻止广播帧的转发

在此页面上，可阻止各个端口转发广播帧。

说明

某些通信协议只有在广播的支持下才能起作用。在这种情况下，阻止功能可能导致数据通信丢失。因此，只有确实不需要广播时，才阻止广播。

Setting	Copy to Table
All ports No Change	Copy to Table

Port	Setting
P0.1	<input type="checkbox"/>
P0.2	<input type="checkbox"/>
P0.3	<input type="checkbox"/>
P0.4	<input type="checkbox"/>
P1.1	<input type="checkbox"/>
P1.2	<input type="checkbox"/>
P1.3	<input type="checkbox"/>
P1.4	<input type="checkbox"/>
P2.1	<input type="checkbox"/>
P2.2	<input type="checkbox"/>
P2.3	<input type="checkbox"/>
P2.4	<input type="checkbox"/>
P3.1	<input type="checkbox"/>
P3.2	<input type="checkbox"/>
P3.3	<input type="checkbox"/>
P3.4	<input type="checkbox"/>
P4.1	<input type="checkbox"/>
P4.2	<input type="checkbox"/>

Set Values Refresh

5.5 “第 2 层”菜单

显示框说明

表 1 包含以下列：

- **第 1 列**
说明设置对于表 2 的所有端口都有效。
- **Setting**
从下拉列表中选择设置。可选择以下设置选项：
 - **enabled**
对广播帧的阻止已启用。
 - **disabled**
对广播帧的阻止已禁用。
 - **No Change**
表 2 保持不变。
- **Copy to Table**
如果单击此按钮，将为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **Port**
显示所有可用端口及链路汇聚。
- **Setting**
启用或禁用对广播帧的阻止。

组态步骤

针对单独端口启用对广播帧的阻止

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

针对所有端口启用对广播帧的阻止

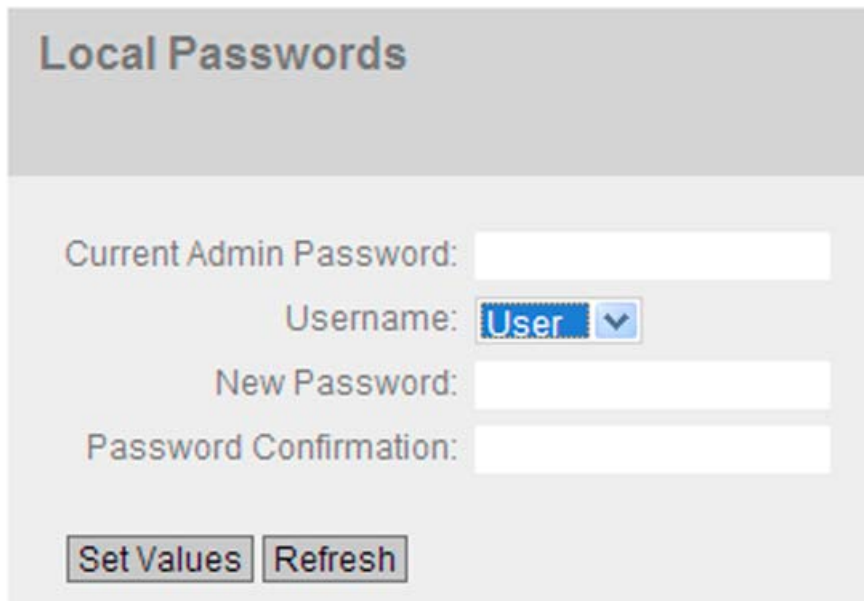
1. 在“Setting”下拉列表中，选择“enabled”条目。
2. 单击“Copy to Table”按钮。将为表 2 中的所有端口启用该复选框。
3. 要应用更改，请单击“Set Values”按钮。

5.6 “Security”菜单

5.6.1 密码

组态设备密码

只能由管理员本地更改管理员和用户的设备密码。



Local Passwords

Current Admin Password:

Username:

New Password:

Password Confirmation:

5.6 “Security”菜单

组态步骤

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

说明

设备出厂时的密码设置如下：

- 管理员： admin
- 用户： user

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

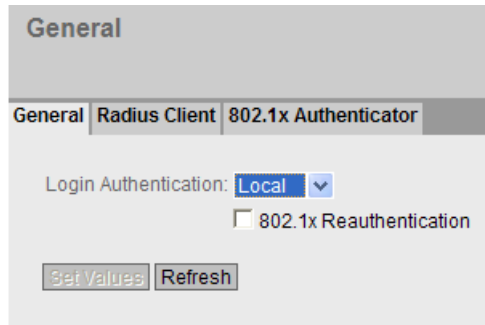
说明

在试用模式下更改密码

即使在试用模式下更改密码，此更改也会立即保存。

5.6.2 AAA

5.6.2.1 常规



The screenshot shows a web-based configuration interface for AAA. The main heading is 'General'. Below it are three tabs: 'General', 'Radius Client', and '802.1x Authenticator'. The 'General' tab is selected. The configuration area includes a 'Login Authentication' dropdown menu currently set to 'Local', and a checkbox for '802.1x Reauthentication' which is unchecked. At the bottom of the configuration area are two buttons: 'Set Values' and 'Refresh'.

显示框说明

该页面包含以下框：

- **下拉列表“Login Authentication”**
指定如何登录：
 - Local
通过本地用户名和密码登录。
 - Server
使用 Radius 服务器登录。
- **复选框“802.1x Reauthentication”**
如果选中此复选框，将强制对已验证的 802.1X 请求者进行周期性重新验证。默认情况下会设置一个小时 (3,600 s)。

组态步骤

1. 如果要启用强制重新验证，请选中“802.1x Reauthentication”复选框。
2. 单击“Set Values”按钮。

5.6 “Security”菜单

5.6.2.2 Radius 客户端

通过外部服务器进行验证

RADIUS 的概念基于外部验证服务器。只有在设备利用验证服务器对终端设备的登录数据进行验证后，该终端设备才能访问网络。终端设备和验证服务器都必须支持 EAP 协议（可扩展验证协议）。

表中的每一列包含一台服务器的访问数据。按照搜索顺序，将首先查询主服务器。如果无法访问主服务器，则会以服务器的输入顺序查询其它辅助服务器。

如果没有服务器响应，则表示没有验证。尽管端口上指示有链路，但客户端仍无法访问网络。

	Server IP Address	Server Port	Shared Secret	Shared Secret Conf	Max. Retrans.	Primary Server	Status
<input type="checkbox"/>	1.2.3.4	1812			3	no	<input type="checkbox"/>

显示框说明

该表格包括以下列：

- **相关行的复选框**
单击该复选框来此行中要删除的条目。
- **输入框“Server IP Address”**
输入服务器的 IP 地址。
- **输入框“Server Port”**
在此处输入 RADIUS 服务器上的输入端口。默认情况下会设置输入端口 1812。值范围是 1 到 65535。
- **输入框“Shared Secret”**
在此处输入访问 ID。
- **输入框“Shared Secret Conf.”**
再次输入访问 ID 以进行确认。

- **输入框“Max. Retrans.”**

在此处输入查询另一个组态的 RADIUS 服务器或将登录视为失败前，查询尝试的最大次数。默认情况下会设置 3。值范围是 1 到 254。

- **下拉列表“Primary Server”**

使用该下拉列表中的选项，指定此服务器是否是主服务器。可选择选项“yes”或“no”之一。

- **复选框“Status”**

使用此复选框，可启用或禁用 RADIUS 服务器。

说明

可在此页面上最多组态两个服务器。

组态步骤

输入新服务器

1. 单击“Create”按钮。会在表中生成一个新条目。

在表中将输入以下默认值：

- 服务器 IP 地址： 0.0.0.0
- 端口号： 1812
- 传输重试的最大次数： 3
- 主服务器： No

2. 在相关行中，在输入框中输入以下数据：

- 服务器 IP 地址
- 目标的端口号
- 秘密访问 ID
- 重复输入秘密访问 ID
- 传输重试的最大次数
- 主服务器

3. 单击“Set Values”按钮。

对每个要输入的服务器重复此步骤。

5.6 “Security”菜单

修改服务器

1. 在相关行中，在输入框中输入以下数据：

- IP 地址
- 目标的端口号
- 秘密访问 ID
- 重复输入秘密访问 ID
- 传输重试的最大次数
- 主服务器

2. 单击“Set Values”按钮。

对每个要修改其输入内容的服务器重复此步骤

删除服务器

1. 单击第一列中要删除的行前的复选框，以选择要删除的条目。

对所有要删除的条目重复此操作。

2. 单击“Delete”按钮。 将从设备内存中删除此数据并更新该页面。

说明

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

5.6.2.3 Authenticator port

对单独的端口启用验证

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

Setting	Copy to Table
All ports	No Change

Port	Setting
P0.1	<input type="checkbox"/>
P0.2	<input type="checkbox"/>
P0.3	<input type="checkbox"/>
P0.4	<input type="checkbox"/>
P1.1	<input type="checkbox"/>
P1.2	<input type="checkbox"/>
P1.3	<input type="checkbox"/>
P1.4	<input type="checkbox"/>
P2.1	<input type="checkbox"/>
P2.2	<input type="checkbox"/>
P2.3	<input type="checkbox"/>
P2.4	<input type="checkbox"/>
P3.1	<input type="checkbox"/>
P3.2	<input type="checkbox"/>
P3.3	<input type="checkbox"/>
P3.4	<input type="checkbox"/>

Set Values Refresh

5.6 “Security”菜单

显示框说明

表 1 包含以下列：

- **第 1 列**
说明设置对于表 2 的所有端口都有效。
- **Setting**
从下拉列表中选择设置。可选择以下设置选项：
 - **enabled**
访问保护已启用。
 - **disabled**
访问保护已禁用。
 - **No Change**
表 2 保持不变。
- **Copy to Table**
如果单击此按钮，将为表 2 的所有端口应用这些设置。

表 2 包含以下列：

- **Port**
此列会列出此设备上的全部可用端口。
- **复选框“Setting”**
在此列中，选中此复选框可对此端口启用验证。空复选框表示没有对相关端口启用验证。如果无法对某个端口进行此组态，则该复选框呈灰色显示并且用户无法修改此设置。

组态步骤

对单独的端口启用验证

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

对所有端口启用验证

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

5.6.3 端口 ACL MAC

5.6.3.1 规则组态

简介

在此页面上为基于 MAC 的 ACL 指定 ACL 规则。

Rule Number	Source MAC	Dest. MAC	Action
1	00-00-00-00-00-00	00-00-00-00-00-00	Forward

显示框说明

该表格包括以下列：

- **Rule Number**
显示 ACL 规则的编号。如果单击“Create”按钮，会创建一个具有唯一编号的新行。
- **Source MAC**
输入源的单播 MAC 地址。
- **Dest. MAC**
输入目标的单播 MAC 地址。
- **Action**
从下拉列表中选择操作。可选操作包括：
 - Forward
如果帧符合 ACL 规则，则转发该帧。
 - Discard
如果帧符合 ACL 规则，则不转发该帧。

5.6 “Security”菜单

组态步骤

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

5.6.3.2 端口入站规则

简介

在此页面上指定 ACL 规则，端口将根据此规则处理进站帧。

Rule Order	Rule Number	Source MAC	Dest. MAC	Action
1	1	00-00-00-00-00-00	00-00-00-00-00-00	Forward

显示框说明

该页面包含以下框

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

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

该表格包括以下列：

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

组态步骤

按照以下步骤为端口分配 ACL 规则：

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

按照以下步骤删除端口的 ACL 规则：

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

5.6.3.3 端口出站规则

简介

在此页面上指定 ACL 规则，端口将根据此规则处理出站帧。

Rule Order	Rule Number	Source MAC	Dest. MAC	Action
1	1	00-00-00-00-00-00	00-00-00-00-00-00	Forward

显示框说明

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

该表格包括以下列：

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

组态步骤

按照以下步骤为端口分配 ACL 规则：

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

按照以下步骤删除端口的 ACL 规则：

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

5.6.4 端口 ACL IP

5.6.4.1 规则组态

简介

在此页面上为基于 IP 的 ACL 指定规则。

Rule Number	Source IP	Source Subnet Mask	Dest. IP	Dest. Subnet Mask	Action
1	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	Forward

显示框说明

该表格包括以下列：

- **Rule Number**
显示 ACL 规则的编号。如果单击“Create”按钮，会创建一个具有唯一编号的新行。
- **Source IP**
输入源的 IP 地址。
- **Source Subnet Mask**
输入源所在子网的子网掩码。
- **Dest. IP**
输入目标的 IP 地址。

- **Source Dest. Mask**
输入目标所在子网的子网掩码。
- **Action**
从下拉列表中选择操作。 可选操作包括：
 - **Forward**
如果帧符合 ACL 规则，则转发该帧。
 - **Discard**
如果帧符合 ACL 规则，则不转发该帧。

组态步骤

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

5.6.4.2 端口入站规则

简介

在此页面上指定 ACL 规则，端口将根据此规则处理入站帧。



显示框说明

该页面包含以下框

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

该表格包括以下列：

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

组态步骤

按照以下步骤为端口分配 ACL 规则：

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

按照以下步骤删除端口的 ACL 规则：

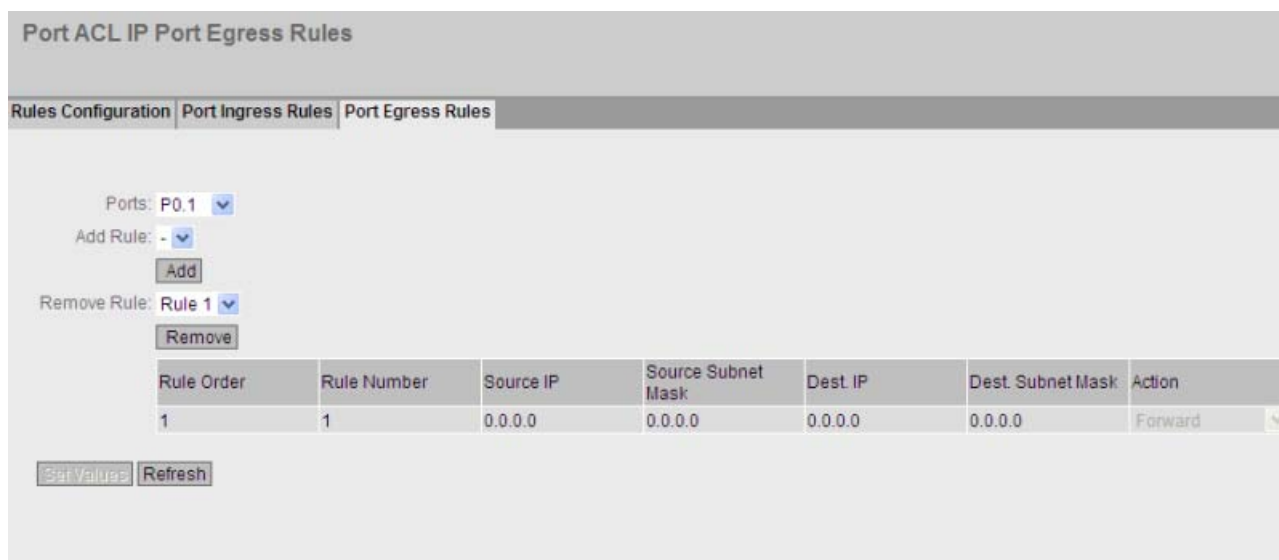
1. 在“Ports”下拉列表中选择端口。
2. 在“Rules”下拉列表中选择 ACL 规则。
3. 单击“Remove”按钮。将从表中删除相应的条目。

5.6 “Security”菜单

5.6.4.3 端口出站规则

简介

在此页面上指定 ACL 规则，端口将根据此规则处理出站帧。



显示框说明

该页面包含以下框

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

该表格包括以下列：

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

组态步骤

按照以下步骤为端口分配 ACL 规则：

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

按照以下步骤删除端口的 ACL 规则：

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

5.6.5 管理 ACL

组态说明

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

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

Management Access Control List

IP Address:

Subnet Mask:

	IP Address	Subnet Mask	VLANs Allowed	SNMP	TELNET	HTTP	HTTPS	SSH	P1	WLAN 1
<input type="checkbox"/>	192.168.0.99	255.255.255.255	1-4094	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

1 entries.

显示框说明

该页面包含以下框：

- **输入框“IP Address”**
输入将应用该规则的 IP 地址或网络地址。如果使用 IP 地址 0.0.0.0，此设置将适用于所有 IP 地址。
- **Subnet Mask**
输入子网掩码。子网掩码 255.255.255.255 用于特定的 IP 地址。如果要允许使用子网（如 C 子网），则输入 255.255.255.0。子网掩码 0.0.0.0 适用于所有子网。

该表格包括以下列：

- **第 1 列**
选中要删除的行中的复选框。
- **IP Address**
显示 IP 地址。
- **Subnet Mask**
显示子网掩码。

- **VLANs Allowed**
输入设备所在 VLAN 的编号。仅当设备位于该组态 VLAN 中时，站才能访问该设备。如果该输入框留空，则没有关于 VLAN 的限制。
- **Out-Band**
指定 IP 地址是否可以通过带外端口访问交换机。
- **SNMP**
指定工作站（或 IP 地址）是否可以使用 SNMP 协议访问设备。
- **TELNET**
指定工作站（或 IP 地址）是否可以使用 TELNET 协议访问设备。
- **HTTP**
指定工作站（或 IP 地址）是否可以使用 HTTP 协议访问设备。
- **HTTPS**
指定工作站（或 IP 地址）是否可以使用 HTTPS 协议访问设备。
- **SSH**
指定工作站（或 IP 地址）是否可以使用 SSH 协议访问设备。
- **Px**
指定站点（或 IP 地址）是否可以通过此端口访问该设备。
- **WLAN 1**（客户端模式）
指定该站点（或 IP 地址）是否可以通过 WLAN 接口访问设备。
- **VAP X.Y**（接入点模式）
指定站点（或 IP 地址）是否可以通过 VAP 接口访问设备。
- **WDS X.Y**（接入点模式）
指定站点（或 IP 地址）是否可以通过 WDS 接口访问设备。

组态步骤

更改条目

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

5.6 “Security”菜单

创建新条目

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

删除条目

1. 选中要删除的行中的复选框。
2. 对每个要删除的条目重复此步骤。
3. 单击“Delete”按钮。 将删除条目并更新页面。

说明

请注意，错误的组态可能意味着您再不能访问设备。

5.7 “Layer 3”菜单

5.7.1 组态

简介

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

具有路由功能的设备提供“Routing”、“VRRP”和“OSPF”功能。



显示框说明

该页面包含以下框：

- **复选框“Routing”**（仅具有路由功能的设备提供）
启用或禁用路由功能。
- **复选框“DHCP Relay Agent”**
启用或禁用 DHCP 中继代理。可以在“Layer 3 > DHCP Relay Agent”中组态其它设置。
- **复选框“VRRP”**（仅具有路由功能的设备提供）
启用或禁用使用 VRRP 的路由功能。要使用 VRRP，应先启用路由功能。可以在“Layer 3 > VRRP”中组态其它设置。
- **复选框“OSPF”**（仅具有路由功能的设备提供）
启用或禁用使用 OSPF 的路由。可以在“Layer 3 > OSPF”中组态其它设置。

5.7 “Layer 3”菜单

组态步骤

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

5.7.2 子网

5.7.2.1 概述

创建子网

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

接口的第一个子网对应于代理 IP 组态。在“SYSTEM > AGENT IP”中组态管理 VLAN 的第一个子网以及带外接口的子网。

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

Connected Subnets Overview

Overview | Configuration

Interface: **VLAN1** ▼

Interface	Interface Name	IP Address	Subnet Mask	Address Type
<u>Out-Band</u>	eth0	0.0.0.0	0.0.0.0	Primary
<u>vlan1</u>	vlan1	192.168.0.151	255.255.255.0	Primary
<u>loopback0</u>	loopback0	127.0.0.1	255.0.0.0	Primary
<input checked="" type="checkbox"/> <u>vlan1</u>	vlan1-1	0.0.0.0	0.0.0.0	Secondary

4 entries.

显示值说明

该页面包含以下框：

- **下拉列表“Interface”**

在“Interface”下拉列表中，选择要为其组态其它子网的接口。

该表格包括以下列：

- **第 1 列**

选中要删除的行中的复选框。

- **Interface**

显示接口。

- **Interface Name**

显示接口名称。

- **IP Address**

显示子网的 IP 地址。

- **Subnet Mask**

显示子网掩码。

- **Address Type**

显示地址类型。可能的值包括：

- **Primary**

管理 VLAN 的第一个子网和带外接口的子网。只能通过代理 IP 更改子网。

- **Secondary**

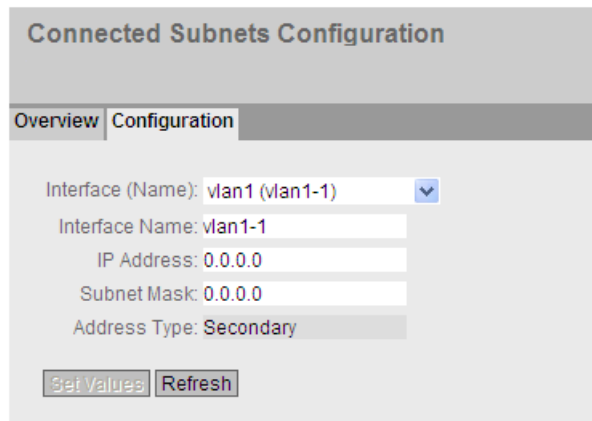
接口的所有其它子网。

组态步骤

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

5.7.2.2 组态

在此页面上指定接口的名称。



显示值说明

该页面包含以下框：

- **下拉列表“Interface (Name)”**
从下拉列表中选择接口。
- **输入框“Interface Name”**
输入接口的名称。
- **输入框“IP Address”**
输入接口的 IP 地址。IP 地址不能多次使用。
- **输入框“Subnet Mask”**
输入要创建的子网的子网掩码。不同接口上的子网不得重叠。
- **Address Type**
显示地址类型。可能的值包括：
 - Primary
管理 VLAN 的第一个子网和带外接口的子网。只能通过代理 IP 更改子网。
 - Secondary
接口的所有其它子网。

组态步骤

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

5.7.3 路由

静态路由

在此页面上创建静态路由。

Routes

Destination Network:

Subnet Mask:

Gateway:

	Destination Network	Subnet Mask	Gateway	Interface	Metric	Status
<input type="checkbox"/>	192.168.0.0	255.255.0.0	192.152.0.1		Not used	inactive

显示值说明

该页面包含以下框：

- **输入框“Destination Network”**
输入目标的网络地址。
- **输入框“Subnet Mask”**
输入相应的子网掩码。
- **输入框“Gateway”**
输入相邻网关的 IP 地址。

该表格包括以下列：

- **第 1 列**
选中要删除的行中的复选框。
- **Destination Network**
显示目标的网络地址。
- **Subnet Mask**
显示相应的子网掩码。

5.7 “Layer 3”菜单

- **Gateway**
显示相邻网关的 IP 地址。
- **Interface**
显示路由的接口。
- **Metric**
输入路由的度量。创建路由时，会自动输入“not used”。度量对应于连接质量，如速度、成本。如果存在多条等效路由，则会使用度量值最小的路由。
值范围： 1 - 15
- **Status**
显示路由是否激活。

组态步骤

1. 在“Destination Network”输入框中输入目标的网络地址。
2. 单击“Create”按钮。会在表中生成一个新条目。
3. 在“Subnet Mask”输入框中输入相应的子网掩码。
4. 在“Gateway”输入框中输入网关。
5. 在“Metric”中输入路由的权重。
6. 单击“Set Values”按钮。

5.7.4 DHCP 中继代理

5.7.4.1 常规

DHCP 中继代理

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

最多可以为 DHCP 中继代理指定 4 个 DHCP 服务器 IP 地址。如果 DHCP 服务器不可访问，设备可切换到其它 DHCP 服务器。

Server IP Address
<input type="checkbox"/> 192.168.0.1

显示值说明

该页面包含以下框：

- 复选框“DHCP Relay Agent (Opt. 82)”
启用或禁用 DHCP 中继代理。
- 输入框“Server IP Address”
输入 DHCP 服务器的 IP 地址。

该表格包括以下列：

- 第 1 列
选中要删除的行中的复选框。
- Server IP Address
显示 DHCP 服务器的 IP 地址。

组态步骤

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

5.7.4.2 选项

DHCP 中继代理的参数

在此页面上，可以指定 DHCP 服务器的参数，例如电路 ID。

电路 ID 描述了 DHCP 查询的来源，例如哪个端口收到了 DHCP 查询。

在“General”选项卡中指定 DHCP 服务器。

Dynamic Host Configuration Protocol (DHCP) Relay Agent Option

General
Option

Global Configuration

Circuit ID Router Index

Circuit ID Receive VLAN ID

Circuit ID Receive Port

Remote ID:

Interface specific configuration

Interface:

Interface	Remote ID Type	Remote ID	Circuit ID Type	Circuit ID
<input type="checkbox"/> vlan1	MAC Address	08-00-06-4b-69-3f	Predefined	-

显示值说明

该页面包含以下框：

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

说明

至少需要选择一个选项。

5.7 “Layer 3”菜单

- **Remote ID**
显示设备 ID。
- 从“**Interface**”下拉列表中选择接口。

该表格包括以下列：

- **第 1 列**
选中要删除的行中的复选框。
- **Interface**
显示接口。
- **Remote ID Type**
从下拉列表中选择设备 ID 的类型。可做以下选择：
 - IP Address
将设备的 IP 地址用作设备 ID。
 - MAC Address
将设备的 MAC 地址用作设备 ID。
 - Free Text
如果使用“Free Text”，可在“Remote ID”中输入设备名称作为设备 ID。
- **Remote ID**
输入设备名称。仅当为“Remote ID Type”选择条目“Free Text”时才能编辑该框。
- **Circuit ID Type**
从下拉列表中选择电路 ID 的类型。可做以下选择：
 - Predefined
根据路由器索引、VLAN ID 或端口自动创建电路 ID。
 - Free Number
如果使用“Free Number”，可为“Circuit ID”输入 ID。
- **Circuit ID**
输入电路 ID。仅当为“Circuit ID Type”选择“Free number”条目时才能编辑该框。
值范围：1 - 188

组态步骤

按照以下步骤指定自动分配参数：

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

按照以下步骤手动指定参数：

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

5.7.5 VRRP

5.7.5.1 路由器

简介

使用“Create”按钮可创建新的虚拟路由器。最多可组态 10 个虚拟路由器。可在“Configuration”选项卡中组态其它参数。

说明

此选项卡仅在具有路由功能的设备中可用。

选中“VRRP”复选框，以组态 VRRP。

The screenshot shows the 'Virtual Router Redundancy Protocol (VRRP) Router' configuration page. At the top, there are tabs for 'Router', 'Configuration', 'Addresses Overview', and 'Addresses Configuration'. Below the tabs, there is a checkbox for 'VRRP' which is currently unchecked. Below the checkbox is a dropdown menu for 'Interface' and an input field for 'VRID'. Below these fields is a table with the following columns: 'Interface', 'VRID', 'Virtual MAC Address', 'Primary IP Address', 'Router State', 'Master IP Address', 'Priority', 'Advert. Interval', and 'Preempt'. At the bottom of the page, there are four buttons: 'Create', 'Delete', 'Set Values', and 'Refresh'.

显示值说明

该页面包含以下框：

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

该表格包括以下列：

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

5.7 “Layer 3”菜单

- **Advert. Interval**
显示主路由器发送 VRRP 数据包的时间间隔。
- **Preempt**
显示优先级较高的路由器是否将替换优先级较低的主路由器成为主路由器。
 - **yes**
优先级较高的路由器可以替换优先级较低的主路由器成为主路由器。
 - **no**
优先级较高的路由器不能替换优先级较低的主路由器成为主路由器。

组态步骤

1. 选中“VRRP”复选框。
2. 从“Interface”下拉列表中选择接口。
3. 在“VRID”输入框中输入虚拟路由器的 ID。
4. 单击“Create”按钮。将在表中插入一个新行。
5. 单击“Set Values”按钮。要组态虚拟路由器，请单击“Configuration”选项卡。

5.7.5.2 组态

简介

在此页面上组态虚拟路由器。

说明

此选项卡仅在具有路由功能的设备中可用。

Virtual Router Redundancy Protocol (VRRP) Configuration

Router | Configuration | Addresses Overview | Addresses Configuration

Interface / VRID:

Status

Primary IP Address: 0.0.0.0

Master

Priority:

Advertisement Interval:

Preempt lower priority Master

显示值说明

该页面包含以下框：

- **下拉列表“Interface/VRID”**
从下拉列表中选择要组态的虚拟路由器的 ID。
- **复选框“Status”**
启用或禁用“Status”功能。

- **下拉列表“Primary IP Address”**

从下拉列表中选择主 IP 地址。如果路由器成为主路由器，路由器会使用此 IP 地址。

说明

如果仅为该 VLAN 组态了一个子网，则不需要任何输入。该条目为 0.0.0.0。

如果为该 VLAN 组态了多个子网，并且想要将特定 IP 地址用作 VRRP 数据包的源地址，则从该下拉列表中选择 IP 地址。否则，将使用具有优先级的 IP 地址。

- **复选框“Master”**

如果启用此选项，则会为“Associated IP Address”输入优先级最高的 IP 地址。这表示 VRRP 路由器优先级最高的 IP 地址将用作虚拟主路由器的虚拟 IP 地址。必须为该组中的备用路由器禁用此选项，并且必须使用“Associated IP Address”中的路由器的 IP 地址。

- **输入框“Priority”**

输入该虚拟路由器的优先级。有效值为 1-254。

当前的主路由器始终会分配优先级 255。可以在冗余路由器之间自由分配其它优先级。优先级越高，路由器就越早变为“主路由器”。

- **输入框“Advertisement Interval”**

输入以秒为单位的时间间隔，在该时间间隔后，主路由器将再次发送 VRRP 数据包。

- **复选框“Preempt lower priority Master”**

指定是否允许该路由器中断优先级较低的路由器。

组态步骤

要将虚拟路由器组态为主路由器，请按以下步骤操作：

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

5.7.5.3 地址概述

概述

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

说明

此选项卡仅在具有路由功能的设备中可用。

Virtual Router Redundancy Protocol (VRRP) Associated IP Addresses Overview						
Router	Configuration	Addresses Overview	Addresses Configuration			
Interface	VRID	Number of Addresses	Associated IP Address (1)	Associated IP Address (2)	Associated IP Address (3)	Associated IP Address (4)
<input type="button" value="Refresh"/>						

显示框说明：

该表格包括以下列：

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

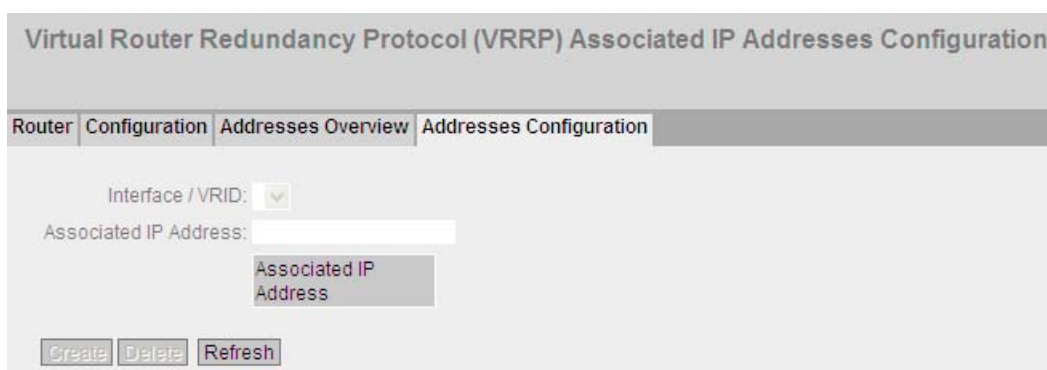
5.7.5.4 地址组态

创建或更改受监视的 IP 地址

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

说明

此选项卡仅在具有路由功能的设备中可用。



显示值说明

该页面包含以下框：

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

该表格包括以下列：

- **第 1 列**
选中要删除的行中的复选框。
- **Associated IP Address**
显示虚拟路由器监视的 IP 地址。

组态步骤

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

5.7.6 OSPFv2

5.7.6.1 组态

简介

在此页面上，可以组态使用 OSPF 的路由。

说明

此选项卡仅在具有路由功能的设备中可用。

Open Shortest Path First v2 (OSPFv2) Configuration

Configuration | Areas | Area Range | Interfaces | Virtual Links

OSPFv2

Router ID: 0.0.0.0

Border Router: Not Area Border Router

New LSA Received: 0

External LSA Maximum: -

Exit Interval(s): -

New LSA Configured: 0

OSPFv2 RFC1583 Compatibility

AS Border Router

Redistribute Routes

Default

Connected

Static

RIP

Set Values Refresh

显示值说明

该页面包含以下框

- **复选框“OSPFv2”**
启用或禁用使用 OSPF 的路由。
- **输入框“Router ID”**
输入其中一个 OSPF 接口的地址。以 IP 地址格式输入该地址，不需要与本地 IP 地址匹配。
- **复选框“OSPFv2 RFC 1583 Compatibility”**
如果仍然有与 RFC 2328 不兼容的 OSPF 路由器在工作中，则启用该选项。
- **Border Router** 显示 OSPF 路由器的状态。如果本地系统至少是 2 个区域中的有效成员，则路由器是区域边界路由器。
- **复选框“AS Border Router”**
指定路由器是否为 AS 边界路由器。AS 边界路由器可在多个自治系统之间进行调停，例如存在其它 RIP 网络时。要添加和分配静态路由，AS 边界路由器也是必需的。
- **New LSA Received**
显示接收到的 LSA 数目。不会包括更新及其自身的 LSA。
- **New LSA Configured**
该本地系统发送的不同 LSA 数。
- **External LSA Maximum**
要限制数据库中外部 LSA 的条目数，请输入最大外部 LSA 数。
- **Exit Interval (s)**
输入时间间隔，经过该时间间隔后，OSPF 路由器会再次尝试脱离溢出状态。0 表示 OSPF 路由器只会在重启后尝试退出溢出状态。
- **Redistribute Routes (Default/Connected/Static/RIP)**
指定通过 OSPF 分配哪些已知路由。您需要从“默认”、“静态”和“RIP”路由类型中作出选择。

说明

只能在 AS 边界路由器中启用这些选项。特别是启用 Default 和 Static 选项时，如果网络中启用这些选项的节点过多，可能出现问题（例如转发回路）。

组态步骤

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

5.7.6.2 区域

概述

自治系统可分为多个较小的区域。

在此页面上，可以查看、创建、修改或删除路由器的区域。

说明

此选项卡仅在具有路由功能的设备中可用。

Open Shortest Path First v2 (OSPF v2) Areas

Configuration	Areas	Area Range	Interfaces	Virtual Links					
Area ID: <input style="width: 150px;" type="text"/>									
	<input type="checkbox"/>	0.0.0.0	Backbone	No Summary	0	53	7	0	0
	<input type="checkbox"/>	3.0.0.0	Normal	No Summary	0	53	5	1	0

显示值说明

该页面包含以下框：

- **输入框“Area ID”**
输入区域的 ID。数据库针对区域的所有路由器同步
输入格式：x.x.x.x
x = 0 ... 255

5.7 “Layer 3”菜单

该表包含以下各列：

- **第 1 列**
选中要删除的行中的复选框。
- **Area ID**
显示区域的 ID。
- **Area Type**
从下拉列表中选择区域类型。
 - 标准 (Standard)
 - 存根 (Stub)
 - NSSA
 - 骨干
- **Summary**
指定是否生成该区域的总结 LSA。
 - Summary: 将总结 LSA 发送至该区域。
 - No Summary: 不将总结 LSA 发送至区域。
- **Updates**
显示路由表的计算次数。
- **LSA Count**
显示数据库中的 LSA 数。
- **Area BR**
显示该区域中可到达的区域边界路由器 (ABR) 的数目。
- **AS BR**
显示该区域中可到达的自治系统边界路由器 (ASBR) 的数目。

组态步骤

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

5.7.6.3 区域范围

创建新 OSPFv2 区域范围

使用“OSPFv2 Area Ranges”菜单中的“New Entry”按钮，最多可将四个网络分组在一个区域 ID 下。

说明

此选项卡仅在具有路由功能的设备中可用。

Open Shortest Path First v2 (OSPF v2) Area Range

Configuration Areas Area Range Interfaces Virtual Links

Area ID: 0.0.0.1

Subnet Address:

Subnet Mask:

	Area ID	Subnet Address	Subnet Mask	Advertise
<input type="checkbox"/>	0.0.0.1	192.168.0.20	255.255.255.0	<input checked="" type="checkbox"/>

Create Delete Set Values Refresh

显示框说明

该页面包含以下框：

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

5.7 “Layer 3”菜单

该表包含以下各列：

- **第 1 列**
选中要删除的行中的复选框。
- **Area ID**
显示区域的 ID。
- **Subnet Addr.**
显示将被分组的网络的地址。
- **Subnet Mask**
显示将被分组的网络的子网掩码。
- **Advertise**
启用该选项以通告分组网络。

组态步骤

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

5.7.6.4 接口

概述

在此页面上，可以组态 OSPF 接口。

说明

此选项卡仅在具有路由功能的设备中可用。

Open Shortest Path First v2 (OSPFv2) Interfaces

Configuration Areas Area Range Interfaces Virtual Links

IP Address:

	IP Address	Area ID	OSPF Status	Metric	Priority	Trans. Delay	Retrans. Delay	Hello Interval	Dead Interval	Authentication Protocol	Authentication Password	Authentication Password Confirmation	Authentication Key ID
<input type="checkbox"/>	120.80.1.18	0.0.0.0	<input checked="" type="checkbox"/>	1	1	1	5	10	40	none			
<input type="checkbox"/>	162.80.1.2	3.0.0.0	<input checked="" type="checkbox"/>	1	1	1	5	10	40	none			
<input type="checkbox"/>	172.80.1.1	3.0.0.0	<input checked="" type="checkbox"/>	1	1	1	5	10	40	none			

Create Delete Set Values Refresh

显示框说明

该页面包含以下框：

- **下拉列表“IP Address”**
从下拉列表中选择 OSPF 接口的 IP 地址。

该表包含以下各列：

- **第 1 列**
选中要删除的行中的复选框。
- **IP Address**
显示 OSPF 接口的 IP 地址。
- **Area ID**
从下拉列表中选择连接到 OSPF 接口的区域的 ID。

5.7 “Layer 3”菜单

- **OSPF Status**

指定是否在接口中激活 OSPF。

 - Enabled: 在接口中启用 OSPF。
 - Disabled: 在接口中禁用 OSPF。
- **Metric**

输入 OSPF 接口的开销。
- **Priority**

输入路由器优先级。 优先级只与选择指定路由器有关。 对于同一子网内的不同路由器，该参数的选择可以不同。
- **Transit Delay**

输入发送连接更新时期望的延迟。
值范围： 1 s 到 3600 s
默认值： 1 s
- **Retrans. Interval**

输入时间值，经过该时间后，如果未收到确认，则会再次传送 VRRP 数据包。
值范围： 1 s 到 3600 s
默认值： 5 s
- **Hello Interval**

输入两个呼叫数据包之间的时间间隔。
值范围： 1 s 到 65,535 s
默认值： 10 s
- **Dead Interval**

输入时间间隔，如果在此时间内未从临近路由器接收到呼叫数据包，则在此时间间隔后会将该路由器标记为“故障”。
默认值： 40 s
- **Authentication Protocol**

选择虚拟链路的验证方法。可做以下选择：

 - none: 无验证
 - simple: 使用密码进行验证。
 - MD5: 使用 MD5 进行验证
- **Authentication Password**

输入密码。

- **Authentication Password Confirmation**

确认输入的密码。

- **Authentication Key ID**

输入将密码用作密钥的 ID。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。

说明

仅当验证方法设置为 MD5 时才能编辑“Authentication Key ID”列。只有这时才能使用多个密钥。

组态步骤

1. 从“IP Address”下拉列表中选择 OSPF 接口的 IP 地址。
2. 单击“Create”按钮。会在表中生成一个新条目。
3. 从“Area ID”下拉列表中选择与 OSPF 接口相连的区域的 ID。
4. 选中“OSPF Status”旁边的复选框。
5. 为“Transit Delay”、“Retrans. Delay”和“Dead Interval”输入适当值或使用默认设置。
6. 在“Authentication Protocol”中指定验证方法。
7. 单击“Set Values”按钮。

5.7.6.5 虚拟链路

概述

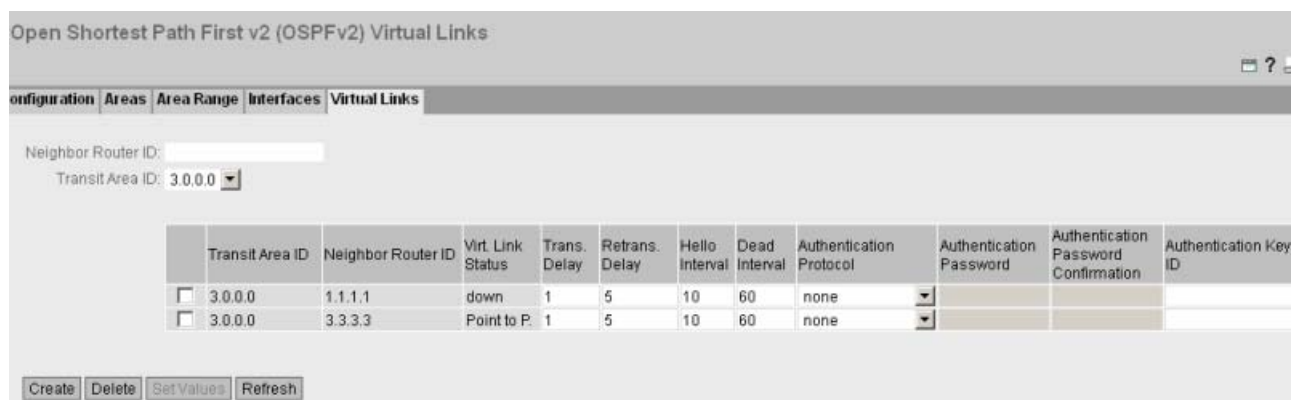
由于协议的原因，每个区域边界路由器都必须访问骨干区域。如果路由器未直接连接到骨干区域，则会创建到骨干区域的虚拟链路。

说明

此选项卡仅在具有路由功能的设备中可用。

说明

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



显示框说明

该页面包含以下框：

- **输入框“Neighbor Router ID”**
输入虚拟连接另一端的临近路由器的 ID。
- **下拉列表“Transit Area ID”**
从下拉列表中选择连接两台路由器的区域的 ID。

该表包含以下各列：

- **第 1 列**
选中要删除的行中的复选框。
- **Transit Area ID**
显示连接两台路由器时使用的 ID。

- **Neighbor Router ID**
显示虚拟链路另一端的临近路由器的 ID。
- **Virt. Link Status**
指定虚拟链路的状态。可能的状态有：
 - 断开 (Down): 虚拟链路未激活。
 - 点到点 (point-to-point): 虚拟链路已激活。
- **Transit Delay**
输入发送链路更新数据包时期望的延迟。
值范围: 1 s 到 3600 s
默认值: 1 s
- **Retrans. Interval**
输入时间值, 如果经过该时间后未接收到任何确认, 则会再次传送数据包。
值范围: 1 s 到 3600 s
默认值: 5 s
- **Hello Interval**
输入两个呼叫数据包之间的时间间隔。
值范围: 1 s 到 65,535 s
默认值: 10 s
- **Dead Interval**
输入时间间隔, 如果在此时间内未从临近路由器接收到呼叫数据包, 则在此时间间隔后会将该路由器视为“故障”。
默认设置: 40 s
- **Authentication Protocol**
选择虚拟链路的验证方法。可做以下选择：
 - none: 无验证
 - simple: 使用密码进行验证
 - MD5: 使用 MD5 进行验证
- **Authentication Password**
输入密码。

5.7 “Layer 3”菜单

- **Authentication Password Confirmation**

确认输入的密码。

- **Authentication Key ID**

输入将密码用作密钥的 ID。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。

说明

仅当验证方法设置为 MD5 时，才会显示“Key ID”文本框。只有这时才能使用多个密钥。

组态步骤

1. 在“Neighbor Router ID”中输入虚拟链路另一端的临近路由器的 ID。
2. 从“Transit Area ID”下拉列表中选择连接两台路由器的区域 ID。
3. 单击“Create”按钮。会在表中生成一个新条目。
4. 在“Transit Delay”、“Retrans. Delay”和“Dead Interval”中输入适当值。
5. 在“Authentication Protocol”中指定验证方法。
6. 单击“Set Values”按钮。

故障排除/FAQ

6.1 不能通过 WBM 或 CLI 进行固件更新

原因

如果固件更新期间发生电源故障，可能无法再通过基于 Web 的管理或 CLI 访问设备。

解决方法

可以使用 TFTP 将固件分配给 SCALANCE X500。

按照以下步骤使用 TFTP 加载新固件：

1. 关闭设备的电源。
2. 现在按“复位”(Reset) 按钮并按住，同时重新连接设备的电源。
3. 按住按钮，直至约 30 秒后红色故障 LED (F) 开始闪烁。
4. 现在松开按钮。引导加载程序在此状态下等待新固件文件，您可通过 TFTP 进行下载。
5. 通过以太网接口将 PC 与 SCALANCE X-500 的带外接口连接。
6. 使用 Primary Setup Tool 为 SCALANCE X-500 分配一个 IP 地址。
7. 在命令提示符中，切换到包含新固件的文件所在的目录，然后执行命令“tftp -i <ip 地址> PUT <固件>”。也可以使用不同的 TFTP 客户端。

结果

固件传送到设备。

说明

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

固件完全传送到设备后，设备将自动重启。

6.1 不能通过 WBM 或 CLI 进行固件更新

索引

A

ACL, 171

C

Collisions, 60

CoS, 127

通信队列, 128

CoS (Class of Service, 服务类别), 23

C-PLUG, 12, 117

保存组态, 119

格式化, 119

CRC, 59

D

DCP 服务器, 71, 162

DHCP

客户端, 91

DSCP, 129

F

Fragments, 59

G

GMRP, 180

GVRP, 135

I

IGMP, 178

J

Jabbers, 60

L

LACP, 159

M

MSTP, 154

端口, 150

端口参数, 156

MSTP 实例, 156, 157

N

Negotiation, 109

NTP, 175

客户端, 101

O

OSPF

OSPFv2 LSDB (信息), 68

OSPFv2 邻居, 64

OSPFv2 接口, 62, 231

OSPFv2 虚拟邻居, 66

区域, 30, 227

区域范围, 229

- 组态, 225
- 虚拟链路, 234
- 链路状态广播, 30
- 路由器, 30
- 路由器状态, 30

Oversize, 59

P

PST 工具, 162

R

RADIUS, 188

RFC

- RFC 1518, 17

S

SIMATIC NET 词汇表, 8

SNMP, 25, 71

- SNMP 陷阱, 95

- SNMPv1, 25

- SNMPv2c, 25

- SNMPv3, 25

STEP 7, 162

T

TFTP

- 加载/保存, 83

U

Undersize, 59

V

VLAN, 21

- VLAN ID, 25

- VLAN 标记, 22

- 优先级, 138

- 标记, 138

- 端口 VID, 138

VRRP

- VRRP 统计信息, 54

- VRRP 路由器, 29

- 主路由器, 29

- 地址组态, 224

- 地址概述, 223

- 备用路由器, 29

- 组态, 221

- 虚拟路由器, 29

- 路由器, 218

三划

子网掩码, 17

广播, 183

四划

冗余网络, 148

手册适用范围, 7

以太网

- 数据包大小, 56

- 数据包类型, 58

- 数据包错误, 59

以太网供电, 13

五划

生成树

- 快速生成树, 28

- 信息, 50
- 电子邮件功能, 89
 - 报警事件, 89
 - 线路监视, 89
- 电源
 - 监视, 114

六划

- 地理坐标, 74
- 多重生成树, 150, 154
- 老化, 146
- 老化时间, 178
- 访问控制, 169, 171
 - 自动学习, 171
- 过滤器
 - 过滤器组态, 167

七划

- 位置, 74
- 报警事件, 89
- 时间设置, 71
- 时钟
 - SNTP (简单网络时间协议), 98
 - UTC 时间, 100
 - 手动设置, 97
 - 时区, 100
 - 时钟同步, 98
 - 系统时间, 96
- 系统
 - 组态, 70
 - 常规信息, 73
- 系统事件
 - 组态, 86
- 系统事件日志
 - 代理, 107
- 词汇表, 8

八划

- 事件
 - 日志表, 47
- 事件日志表, 47
- 服务等级 (Class of Service), 127
- 注销
 - 自动, 105
- 线路监视, 89
- 组态模式, 72
- 组播, 175
- 转发延迟, 149

九划

- 信息
 - ARP 表, 46
 - Versions, 44
 - 日志表, 47
 - 生成树, 50
 - 起始页面, 39
- 复位, 78
- 故障监视
 - 连接状态变化, 115
- 点对点, 28
- 重启, 78

十划

- 起始页面, 39
- 验证, 191

十一划

- 基于 Web 的管理, 35
 - 要求, 35

十二划

登录

通过 HTTP, 36

通过 HTTPS, 36

十三划

数据包错误统计信息, 59

路由, 29

VRRP, 29

路由表, 61

静态路由, 29

错误状态, 49

十四划

端口

端口组态, 109, 113

端口组态, 113

十六划

镜像, 143