

Modicon

MCSESM, MCSESM-E, MCSESP 管理型交换机
图形用户界面参考手册

本文档中提供的信息包含有关此处所涉及产品之性能的一般说明和/或技术特性。本文档并非用于（也不代替）确定这些产品对于特定用户应用场合的适用性或可靠性。任何此类用户或设备集成商都有责任就相关特定应用场合或使用方面对产品执行适当且完整的风险分析、评估和测试。Schneider Electric 或其任何附属机构或子公司对于误用此处包含的信息而产生的后果概不负责。如果您有关于改进或更正此出版物的任何建议、或者从中发现错误、请通知我们。

本手册可用于法律所界定的个人以及非商业用途。在未获得施耐德电气书面授权的情况下，不得翻印传播本手册全部或部分相关内容、亦不可建立任何有关本手册或其内容的超文本链接。施耐德电气不对个人和非商业机构进行非独占许可以外的授权或许可。请遵照本手册或其内容原义并自负风险。与此有关的所有其他权利均由施耐德电气保留。

在安装和使用本产品时，必须遵守国家、地区和当地的所有相关的安全法规。出于安全方面的考虑和为了帮助确保符合归档的系统数据，只允许制造商对各个组件进行维修。

当设备用于具有技术安全要求的应用场合时，必须遵守有关的使用说明。

未能使用施耐德电气软件或认可的软件配合我们的硬件，则可能导致人身伤害、设备损坏或不正确的运行结果。

不遵守此信息可能导致人身伤害或设备损坏。

作为负责任、具有包容性的企业中的一员，我们将更新包含非包容性术语的内容。然而，在我们完成更新流程之前，我们的内容可能仍然包含客户认为不恰当的标准化行业术语。

© 2022 Schneider Electric. All Rights Reserved.

目录

	安全提示	9
	关于本手册	11
	重要说明	12
	关于图形用户界面的说明	13
1	Basic Settings	19
1.1	System	19
1.2	Network.	23
1.2.1	Global	24
1.2.2	IPv4	26
1.2.3	IPv6	29
1.3	Out of Band over USB	32
1.4	Software	34
1.5	Load/Save.	37
1.6	External Memory.	48
1.7	Port	51
1.8	Power over Ethernet (MCSESP).	58
1.8.1	PoE Global	59
1.8.2	PoE Port	62
1.9	Restart.	65
2	Time	69
2.1	Basic Settings	69
2.2	SNTP	73
2.2.1	SNTP Client.	74
2.2.2	SNTP Server.	78
2.3	PTP.	80
2.3.1	PTP Global	81
2.3.2	PTP Boundary Clock	83
2.3.2.1	PTP Boundary Clock Global.	84
2.3.2.2	PTP Boundary Clock Port.	88
2.3.3	PTP Transparent Clock.	91
2.3.3.1	PTP Transparent Clock Global	92
2.3.3.2	PTP Transparent Clock Port	95
2.4	802.1AS.	96
2.4.1	802.1AS Global	97
2.4.2	802.1AS Port	101
2.4.3	802.1AS Statistics	105
3	Device Security	107
3.1	User Management.	107
3.2	Authentication List.	113
3.3	LDAP	115
3.3.1	LDAP Configuration	116

3.3.2	LDAP Role Mapping.	121
3.4	Management Access.	123
3.4.1	Server	124
3.4.2	IP Access Restriction.	137
3.4.3	Web.	141
3.4.4	Command Line Interface	142
3.4.5	SNMPv1/v2 Community.	145
3.5	Pre-login Banner	146
4	Network Security	149
4.1	Network Security Overview.	149
4.2	Port Security.	151
4.3	802.1X Port Authentication	157
4.3.1	802.1X Global.	158
4.3.2	802.1X Port Configuration.	161
4.3.3	802.1X Port Clients.	167
4.3.4	802.1X EAPOL Port Statistics	169
4.3.5	802.1X Port Authentication History	171
4.3.6	802.1X Integrated Authentication Server.	173
4.4	RADIUS	174
4.4.1	RADIUS Global.	175
4.4.2	RADIUS Authentication Server	177
4.4.3	RADIUS Accounting Server	179
4.4.4	RADIUS Authentication Statistics	181
4.4.5	RADIUS Accounting Statistics	183
4.5	DoS.	184
4.5.1	DoS Global	185
4.6	DHCP Snooping.	188
4.6.1	DHCP Snooping Global	190
4.6.2	DHCP Snooping Configuration.	192
4.6.3	DHCP Snooping Statistics	195
4.6.4	DHCP Snooping Bindings	196
4.7	IP Source Guard.	197
4.7.1	IP Source Guard Port	199
4.7.2	IP Source Guard Bindings	200
4.8	Dynamic ARP Inspection	201
4.8.1	Dynamic ARP Inspection Global.	203
4.8.2	Dynamic ARP Inspection Configuration	205
4.8.3	Dynamic ARP Inspection ARP Rules	208
4.8.4	Dynamic ARP Inspection Statistics.	209
4.9	ACL.	210
4.9.1	ACL IPv4 Rule.	211
4.9.2	ACL MAC Rule	214
4.9.3	ACL Assignment	216
5	Switching.	219
5.1	Switching Global	219
5.2	Rate Limiter	221

5.3	Filter for MAC Addresses	224
5.4	IGMP Snooping.	225
5.4.1	IGMP Snooping Global	227
5.4.2	IGMP Snooping Configuration.	229
5.4.3	IGMP Snooping Enhancements	233
5.4.4	IGMP Snooping Querier.	236
5.4.5	IGMP Snooping Multicasts	239
5.5	Time-Sensitive Networking.	240
5.5.1	TSN Configuration.	241
5.5.2	TSN Gate Control List.	243
5.5.2.1	TSN Configured Gate Control List	244
5.5.2.2	TSN Current Gate Control List.	246
5.6	MRP-IEEE	247
5.6.1	MRP-IEEE Configuration	248
5.6.2	MRP-IEEE Multiple MAC Registration Protocol.	249
5.6.3	MRP-IEEE Multiple VLAN Registration Protocol	253
5.7	GARP	256
5.7.1	GMRP	257
5.7.2	GVRP	259
5.8	QoS/Priority	260
5.8.1	QoS/Priority Global.	261
5.8.2	QoS/Priority Port Configuration.	262
5.8.3	802.1D/p Mapping	264
5.8.4	IP DSCP Mapping.	266
5.8.5	Queue Management	268
5.9	VLAN	269
5.9.1	VLAN Global.	270
5.9.2	VLAN Configuration	271
5.9.3	VLAN Port.	273
5.9.4	VLAN Voice	275
5.10	L2-Redundancy.	277
5.10.1	MRP.	278
5.10.2	HIPER Ring	282
5.10.3	Spanning Tree.	284
5.10.3.1	Spanning Tree Global	285
5.10.3.2	Spanning Tree Dual RSTP (MCSESM-E).	291
5.10.3.3	Spanning Tree Port	297
5.10.4	Link Aggregation	303
5.10.5	Link Backup.	310
5.10.6	FuseNet.	313
5.10.6.1	Sub Ring	314
5.10.6.2	Ring/Network Coupling.	319
5.10.6.3	Redundant Coupling Protocol (MCSESM-E).	325
6	Diagnostics.	329
6.1	Status Configuration	329
6.1.1	Device Status.	330

6.1.2	Security Status	334
6.1.3	Signal Contact	340
6.1.3.1	Signal Contact 1 / Signal Contact 2.	342
6.1.4	MAC Notification	346
6.1.5	Alarms (Traps)	349
6.2	System	351
6.2.1	System Information	352
6.2.2	Hardware State	353
6.2.3	IP Address Conflict Detection.	354
6.2.4	ARP.	358
6.2.5	Selftest	359
6.3	Email Notification	360
6.3.1	Email Notification Global.	362
6.3.2	Email Notification Recipients.	366
6.3.3	Email Notification Mail Server	367
6.4	Syslog	369
6.5	Ports.	373
6.5.1	SFP.	374
6.5.2	TP cable diagnosis	376
6.5.3	Port Monitor	378
6.5.4	Auto-Disable	389
6.5.5	Port Mirroring	393
6.6	LLDP	395
6.6.1	LLDP Configuration	396
6.6.2	LLDP Topology Discovery.	400
6.7	Loop Protection.	403
6.8	Report	408
6.8.1	Report Global.	409
6.8.2	Persistent Logging	414
6.8.3	System Log	417
6.8.4	Audit Trail.	418
7	Advanced	419
7.1	DHCP L2 Relay.	419
7.1.1	DHCP L2 Relay Configuration.	421
7.1.2	DHCP L2 Relay Statistics	424
7.2	DHCP Server.	425
7.2.1	DHCP Server Global	426
7.2.2	DHCP Server Pool	428
7.2.3	DHCP Server Lease Table.	433
7.3	DNS.	434
7.3.1	DNS Client	434
7.3.1.1	DNS Client Global.	435
7.3.1.2	DNS Client Current	436
7.3.1.3	DNS Client Static.	437
7.3.1.4	DNS Client Static Hosts.	439
7.4	Industrial Protocols	440

7.4.1	IEC61850-MMS	441
7.4.2	Modbus TCP	444
7.4.3	EtherNet/IP.	446
7.5	Digital IO Module.	448
7.6	Command Line Interface	451
A	关键词目录	453

安全提示

请注意：在安装、运行或维护之前请仔细通读本说明，并熟悉设备。下列提示可能包含在本文件的各个位置，或在设备上出现。这些提示将警告可能发生的危险状况、提请人们对某些信息加以注意、解释或简化过程。



在“危险”或“警告”标签上添加此符号表示存在触电危险，如果不遵守使用说明，会导致人身伤害。



这是一个常规警告符号。它提示请注意可能发生的受伤危险。请注意该符号下所列的所有提示，以避免受伤或者造成致命后果。

危险

危险 提示请注意即将发生的危险状况，忽视该提示**无疑**会造成严重的甚至导致死亡的后果。

警告

警告 提示请注意可能发生的危险，如未避免会造成死亡或重伤的后果。

小心

小心 提示请注意可能发生的危险，如未避免会造成轻伤的后果。

提示

提示 提供能避免受伤的工作方法。

请注意：电气设备的安装、操作、维修和维护工作仅限于合格人员执行。Schneider Electric 不承担由于使用本资料所引起的任何后果。

专业人员是指掌握与电气设备的制造和操作及其安装相关的技能和知识的人员，他们经过安全培训能够发现和避免相关的危险。

© 2022 Schneider Electric. All Rights Reserved.

关于本手册

适用范围

本手册中包含的数据和插图不具有约束力。我们保留在持续的产品研发方案 框架内更改我们产品的权利。本资料中的信息可能在不公布的情况下更改，不得将此视为 Schneider Electric 的义务。

用户意见

我们随时乐于听取您的意见和建议。我们的电子邮箱是：techpub@schneider-electric.com

更多文档

“配置”用户手册包含了用户开始操作设备时所需的信息。它将指导用户在用户环境中逐步完成从首次启动操作一直到基本操作设置的全部工作。

“安装”用户手册包含了用户安装设备时所需的设备描述、安全说明、显示描述和其他信息。

“图形用户界面”参考手册包含了关于使用图形用户界面操作设备各种功能的详细信息。



“命令行界面”参考手册包含了关于使用命令行界面操作设备各种功能的详细信息。


ConneXium Network Manager 网络管理软件为用户提供了更多的便捷配置和监控选择：


- ▶ 自动拓扑识别
- ▶ 浏览器界面
- ▶ 客户端/服务器结构
- ▶ 事件处理
- ▶ 事件日志
- ▶ 同时配置多个设备
- ▶ 带网络布局的图形用户界面
- ▶ SNMP/OPC 网关

重要说明

本手册中使用的图标具有以下含义：

	列表
	工作步骤
Link	包含链接的交叉引用
提示：	注意强调了重要事实或提请用户注意相关信息。
<code>Courier</code>	图形用户界面中 CLI 命令或字段内容的表示

 图形用户界面中的执行

 命令行界面中的执行

关于图形用户界面的说明

设备支持以下操作系统：

- ▶ Windows 10
- ▶ Linux

设备的图形用户界面划分如下：

- ▶ 导航区域
- ▶ 对话框区域
- ▶ 按钮

导航区域

导航区域位于图形用户界面左侧。

导航区域包含以下元素：

- ▶ 工具栏
- ▶ 筛选器
- ▶ 菜单

用户可以选择折叠整个导航区域，例如，在小屏幕上显示图形用户界面时。要折叠或展开，请点击导航区域顶部的小箭头。

工具栏

导航区域顶部的工具栏包含几个按钮。

- 将鼠标指针置于一个按钮之上时，工具提示会显示更多信息。
- 如果与设备的连接中断，工具栏会变为灰色。



设备每隔 5 秒钟自动刷新一次工具栏信息。

点击该按钮可手动刷新工具栏。



将鼠标指针置于该按钮之上时，工具提示会显示以下信息：

- ▶ *User:*
登录用户的姓名
- ▶ *Device name:*
设备名称

点击该按钮可打开 *Device Security > User Management* 对话框。



将鼠标指针置于该按钮之上时，工具提示会显示 *Diagnostics > System > Configuration Check* 对话框的摘要。

点击该按钮可打开 *Diagnostics > System > Configuration Check* 对话框。



点击该按钮可注销当前用户并显示登录对话框。

如果非永久性存储器（*RAM*）中的配置概要文件与永久存储器（*NVM*）中的“选定”配置概要文件不同，则设备会显示 *Warning* 对话框。

- 要永久保存这些更改，请点击 *Warning* 对话框中的 *Yes* 按钮。
- 要丢弃这些更改，请点击 *Warning* 对话框中的 *No* 按钮。



显示设备自动注销非活跃用户之前的剩余时间（秒）。

点击该按钮可打开 *Device Security > Management Access > Web* 对话框。在此，用户可以指定超时。



当非永久性存储器（*RAM*）中的配置概要文件与永久存储器（*NVM*）中的“选定”配置概要文件不同时，此按钮为可见。否则，此按钮为隐藏。

点击该按钮可打开 *Basic Settings > Load/Save* 对话框。

右键点击该按钮，用户可以保存永久存储器（*NVM*）中的当前设置。



将鼠标指针置于该按钮之上时，工具提示会显示以下信息：

- ▶ *Device Status*: 此部分显示 *Basic Settings > System* 对话框中 *Device status* 框的压缩视图。此部分显示当前为活动状态且其发生首先得到记录的警报。
- ▶ *Security Status*: 此部分显示 *Basic Settings > System* 对话框中 *Security status* 框的压缩视图。此部分显示当前为活动状态且其发生首先得到记录的警报。
- ▶ *Boot Parameter*: 如果用户永久保存对设置的更改且至少一个引导参数与上次重新启动期间使用的配置概要文件不同，则此部分会显示一个注意。
以下设置会导致引导参数发生改变：
 - *Basic Settings > External Memory* 对话框，*Software auto update* 参数
 - *Basic Settings > External Memory* 对话框，*Config priority* 参数
 - *Device Security > Management Access > Server* 对话框，*SNMP* 选项卡，*UDP port* 参数
 - *Diagnostics > System > Selftest* 对话框，*RAM test* 参数
 - *Diagnostics > System > Selftest* 对话框，*SysMon1 is available* 参数
 - *Diagnostics > System > Selftest* 对话框，*Load default config on error* 参数

点击该按钮可打开 *Diagnostics > Status Configuration > Device Status* 对话框。

筛选器

筛选器使用户能够减少菜单中菜单项的数量。筛选后，菜单只显示与筛选器字段中输入的搜索字符串匹配的菜单项。

菜单

菜单显示菜单项。

用户可以选择对菜单项进行筛选。参见“[筛选器](#)”一节。

要在对话框区域中显示相应对话框，请点击所需菜单项。如果所选菜单项是一个包含子项目的节点，则可点击该节点进行展开或折叠。对话框区域会保留之前显示的对话框。

用户可以选择同时对菜单中的每个节点进行展开或折叠。右键点击菜单中的任意位置后，一个上下文菜单会显示以下条目：

- ▶ *Expand*
同时展开菜单中的每个节点。菜单显示每个级别的菜单项。
- ▶ *Collapse*
同时折叠菜单中的每个节点。菜单显示最高级别的菜单项。

对话框区域

对话框区域位于图形用户界面右侧。点击导航区域中的一个菜单项后，对话框区域会显示相应对话框。

更新显示

如果一个对话框较长时间保持打开，则设备中的数值在此期间可能已经改变。



- 要更新对话框中的显示，请点击  按钮。对话框中未保存的信息会丢失。

保存设置

保存，将更改的设置传送到设备的非永久性存储器 (*RAM*)。执行以下步骤：

- 点击  按钮。

如需在重新启动设备之后继续保留更改的设置，请执行以下步骤：

- 打开 *Basic Settings > Load/Save* 对话框。
- 在表格中，突出显示所需配置概要文件。
- 当在 *Selected* 列中复选框为未勾选时，请点击  按钮，然后点击 *Select* 项目。
- 点击  按钮，然后点击 *Save* 项目。

提示：无意中更改设置可能会终止用户 PC 和设备之间的连接。要使设备保持可访问，请在更改任何设置之前启用 *Basic Settings > Load/Save* 对话框中的 *Undo configuration modifications* 功能。利用此功能，设备可持续检查是否仍然可以通过用户 PC 的 IP 地址访问设备。如果连接中断，则设备在经过指定时间之后会加载永久存储器 (*NVM*) 中保存的配置概要文件。之后，可以再次访问设备。

处理表格

对话框以表格形式显示各种设置。

修改一个表格单元格后，该表格单元格会在其左上角显示一个红色标记。该红色标记表示用户的修改尚未传送到设备的非永久性存储器（RAM）。

用户可以选择根据自己的需要对表格外观进行定制。将鼠标指针置于一个列标题之上时，该列标题会显示一个下拉列表按钮。点击此按钮后，下拉列表会显示以下条目：

- ▶ 升序排序
根据所选列的条目按照升序对表格条目进行排序。
用户可以通过列标题中的箭头识别已排序的表格条目。
- ▶ 降序排序
根据所选列的条目按照降序对表格条目进行排序。
用户可以通过列标题中的箭头识别已排序的表格条目。
- ▶ 列
显示或隐藏列。
用户可以通过下拉列表中的未勾选复选框识别隐藏列。
- ▶ 筛选器
表格只显示内容与所选列的指定筛选条件匹配的条目。
用户可以通过突显列标题识别筛选出的表格条目。

用户可以选择同时选择多个表格条目，然后对它们应用一个操作。当用户想要同时删除多个表格条目时，可使用此功能。



- ▶ 选择几个连续的表格条目：
 - 点击第一个需要的表格条目，使其突出显示。
 - 按住 <SHIFT> 键。
 - 点击最后一个需要的表格条目，使每个需要的表格条目都突出显示。
- ▶ 选择多个单独的表格条目：
 - 点击第一个需要的表格条目，使其突出显示。
 - 按住 <CTRL> 键。
 - 点击下一个需要的表格条目，使其突出显示。重复此操作，直到每个需要的表格条目都突出显示为止。

按钮

此处提供了标准按钮的描述。相应的对话框帮助文本中描述了特殊的特定对话框按钮。



将更改传送到设备的非永久性存储器（RAM）并将其应用到设备。要将更改保存到永久存储器中，请按照以下步骤操作：

- 打开 *Basic Settings > Load/Save* 对话框。
- 在表格中，突出显示所需配置概要文件。
- 当在 *Selected* 列中复选框为未勾选时，请点击  按钮，然后点击 *Select* 项目。
- 点击  按钮保存用户的当前更改。



使用设备的非永久性存储器（RAM）中保存的数值对字段进行更新。



将设置从非永久性存储器 (*RAM*) 传送到永久存储器 (*NVM*) 中指定为“选定”的配置概要文件中。

当在 *Basic Settings > External Memory* 对话框中 *Backup config when saving* 列中的复选框已勾选时，则设备会在外部存储器中生成配置概要文件的一份副本。



显示菜单项对应于相应对话框的子菜单。



打开 *Wizard* 对话框。



添加一个新的表格条目。



删除突出显示的表格条目。



打开在线帮助。

1 Basic Settings

该菜单包含以下对话框：

- ▶ System
- ▶ Network
- ▶ Out of Band over USB
- ▶ Software
- ▶ Load/Save
- ▶ External Memory
- ▶ Port
- ▶ Power over Ethernet (MCSESP)
- ▶ Restart

1.1 System

[Basic Settings > System]

在此对话框中，可以监控各种操作状态。

Device status

此框中的字段显示设备状态并通知用户已发生的警报。当前存在警报时，此框突出显示。

可在 *Diagnostics > Status Configuration > Device Status* 对话框中指定设备监控的参数。

提示： 如果用户只将一个具有供电电压的电源单元连接到一个具有冗余电源单元的设备上，则设备报告警报。为了帮助避免这种警报，可在 *Diagnostics > Status Configuration > Device Status* 对话框中停用缺失电源单元的监控。

Alarm counter

显示当前存在警报的数量。



当有至少一个当前存在警报时，此图标可见。

将鼠标指针置于该图标之上时，工具提示会显示当前存在警报的原因以及设备触发该警报的时间。

如果监控的参数与所期望的状态不同，则设备会触发警报。*Diagnostics > Status Configuration > Device Status* 对话框的 *Status* 选项卡会显示警报概览。

Security status

此框中的字段会显示安全状态并通知用户已发生的警报。当前存在警报时，此框突出显示。

可在 *Diagnostics > Status Configuration > Security Status* 对话框中指定设备监控的参数。

Alarm counter

显示当前存在警报的数量。



当有至少一个当前存在警报时，此图标可见。

将鼠标指针置于该图标之上时，工具提示会显示当前存在警报的原因以及设备触发该警报的时间。

如果监控的参数与所期望的状态不同，则设备会触发警报。[Diagnostics > Status Configuration > Security Status](#) 对话框的 *Status* 选项卡会显示警报概览。

Signal contact status

此框中的字段显示信号触点状态并通知用户已发生的警报。当前存在警报时，此框突出显示。

可在 [Diagnostics > Status Configuration > Signal Contact > Signal Contact 1/Signal Contact 2](#) 对话框中指定设备监控的参数。

Alarm counter

显示当前存在警报的数量。



当有至少一个当前存在警报时，此图标可见。

将鼠标指针置于该图标之上时，工具提示会显示当前存在警报的原因以及设备触发该警报的时间。

如果监控的参数与所期望的状态不同，则设备会触发警报。[Diagnostics > Status Configuration > Signal Contact > Signal Contact 1/Signal Contact 2](#) 对话框的 *Status* 选项卡会显示警报概览。

System data

此框中的字段显示设备的操作数据和位置信息。

System name

指定网络中所知的设备的名称。

可能的值：

- ▶ 带有 0..255 个字符的字母数字 ASCII 字符串
允许以下字符：
 - 0..9
 - a..z
 - A..Z
 - !#\$%&'()*+,-./:;<=>?@[\\]^_`{|}~
 - <device name>-<MAC address> (默认设置)

创建 HTTPS X.509 证书时，生成证书的应用程序会使用指定值作为域名和通用名。

以下功能使用指定值作为主机名称或 FQDN (Fully Qualified Domain Name)。对于兼容性，建议只使用小写字母，这是因为，并非每个系统都会比较 FQDN 中的大小写。请验证此名称在整个网络中是否是唯一的。

- ▶ DHCP 客户端
- ▶ *Syslog*
- ▶ *IEC61850-MMS*

Location

指定设备位置。

可能的值：

- ▶ 带有 0..255 个字符的字母数字 ASCII 字符串

Contact person

指定此设备的联系人。

可能的值：

- ▶ 带有 0..255 个字符的字母数字 ASCII 字符串

Device type

显示设备的产品名称。

Power supply 1 Power supply 2

显示相关电压供应连接上电源单元的状态。

可能的值：

- ▶ *present*
- ▶ *defective*
- ▶ *not installed*
- ▶ *unknown*

Uptime

显示此设备上上次重新启动以来经过的时间。

可能的值：

- ▶ 日 ...小时 ...分钟 ...秒钟格式的时间

Temperature [°C]

显示设备中的当前温度 (° C)。

可在 *Diagnostics > Status Configuration > Device Status* 对话框中激活温度阈值的监控。

Upper temp. limit [°C]

指定温度阈值上限 (° C)。

可能的值:

- ▶ -99..99 (整数)

如果设备中的温度高于此值，则设备发出警报。

Lower temp. limit [°C]

指定温度阈值下限 (° C)。

可能的值:

- ▶ -99..99 (整数)

如果设备中的温度低于此值，则设备发出警报。

LED status

此框显示上次更新之时设备状态 LED 指示灯的状态。“安装”用户手册包含关于设备状态 LED 指示灯的详细信息。

参数	颜色	含义
<i>Status</i>	●	当前没有设备状态警报。设备状态正常。
	●	当前至少有一个设备状态警报。因此，请参见以上 <i>Device status</i> 框。
<i>Power</i>	●	带有 2 个电源单元的设备型号： 只有一个供电电压激活。
	●	带有 1 个电源单元的设备型号： 供电电压激活。
	●	带有 2 个电源单元的设备型号： 两个供电电压都激活。
<i>EAM</i>	●	未连接外部存储器。
	●	外部存储器已连接，但未处于运行准备就绪状态。
	●	外部存储器已连接且已处于运行准备就绪状态。

Port status

此框显示上次更新之时设备端口的简化视图。

图标表示各个端口的状态。在某些情况下，以下图标会相互干扰。将鼠标指针置于相应的端口图标之上时，工具提示会显示关于端口状态的详细信息。

参数	状态	含义
<Port number>		端口已停用。 端口不发送或接收任何数据。
		端口已停用。 电缆已连接。链路已激活。
		端口已激活。 电缆未连接或链路未激活。
		端口已激活。 电缆已连接。连接正常。链路已激活。全双工模式
		半双工模式已启用。 在 <i>Basic Settings > Ports</i> 对话框的 <i>Configuration</i> 选项卡中对设置进行验证。
		冗余功能导致该端口处于阻断状态。
		该端口作为路由器接口运行。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

1.2 Network

[Basic Settings > Network]

该菜单包含以下对话框：

- ▶ Global
- ▶ IPv4
- ▶ IPv6

1.2.1 Global

[Basic Settings > Network > Global]

此对话框可用于指定通过网络访问设备管理所需的 VLAN 和 Ethernet Switch Configurator 设置。

Management interface

此框允许用户指定可在其中访问设备管理的 VLAN。

VLAN ID

指定可在其中通过网络访问设备管理的 VLAN。可通过属于此 VLAN 成员的端口对设备管理进行访问。

可能的值：

▶ 1..4042（默认设置：1）

前提条件是已配置 VLAN。参见 *Switching > VLAN > Configuration* 对话框。

更改值后点击 按钮时，*Information* 窗口会打开。选择将来连接到设备时所用的端口。点击 *Ok* 按钮后，新的设备管理 VLAN 设置会分配到该端口。

- 此后，该端口成为 VLAN 的一员并且该端口传输的数据包无 VLAN 标签（不标记）。参见 *Switching > VLAN > Configuration* 对话框。
- 设备将设备管理 VLAN 的端口 VLAN ID 分配到该端口。参见 *Switching > VLAN > Port* 对话框。

很快即可通过新的设备管理 VLAN 中的新端口访问设备。

MAC address

显示设备的 MAC 地址。可通过使用 MAC 地址的网络访问设备管理。

Ethernet Switch Configurator protocol v1/v2

此框可用于指定使用 Ethernet Switch Configurator 协议访问设备的设置。

在 PC 上，Ethernet Switch Configurator 软件显示可在网络中访问的 Schneider Electric 设备，该网络启用了 Ethernet Switch Configurator 功能。即使这些设备具有无效的 IP 参数或没有分配 IP 参数，也可以访问它们。Ethernet Switch Configurator 软件可用于分配或更改设备中的 IP 参数。

提示：使用 Ethernet Switch Configurator 软件时，只能通过与设备管理属于相同 VLAN 的端口访问设备。可在 *Switching > VLAN > Configuration* 对话框中指定将某个特定端口分配给哪个 VLAN。

Operation

启用/禁用设备中的 Ethernet Switch Configurator 功能。

可能的值：

- ▶ *On* (默认设置)
Ethernet Switch Configurator 已启用。
用户可以使用 Ethernet Switch Configurator 软件从用户 PC 访问设备。
- ▶ *Off*
Ethernet Switch Configurator 已禁用。

Access

启用/禁用使用 Ethernet Switch Configurator 对设备的写访问。

可能的值：

- ▶ *readWrite* (默认设置)
Ethernet Switch Configurator 软件已获得设备的写访问权限。
通过此设置，可以更改设备中的 IP 参数。
- ▶ *readOnly*
Ethernet Switch Configurator 软件已获得设备的只读访问权限。
通过此设置，可以查看设备中的 IP 参数。

建议：只有在设备投入运行之后才能将该设置更改为值 *readOnly*。

Signal

激活/停用端口的 LED 闪烁，如同 Ethernet Switch Configurator 软件中具有相同名称的功能。
该功能可用于识别现场设备。

可能的值：

- ▶ 勾选
端口 LED 指示灯闪烁已激活。
端口 LED 指示灯闪烁，直到再次禁用该功能为止。
- ▶ 未勾选 (默认设置)
端口 LED 指示灯闪烁已停用。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

1.2.2 IPv4

[Basic Settings > Network > IPv4]

此对话框允许用户指定通过网络访问设备管理所需的 IPv4 设置。

Management interface

IP address assignment

指定设备管理从其接收 IP 参数的源。

可能的值：

- ▶ *Local*
设备使用来自内部存储器的 IP 参数。用户在 *IP parameter* 框中为 IP 参数指定设置。
- ▶ *BOOTP*
设备从 BOOTP 或 DHCP 服务器接收其 IP 参数。
服务器评估设备的 MAC 地址，然后分配 IP 参数。
- ▶ *DHCP* (默认设置)
设备从 DHCP 服务器接收其 IP 参数。
服务器评估设备的 MAC 地址、DHCP 名称或其他参数，然后分配 IP 参数。
当服务器也提供 DNS 服务器的地址时，设备会在 *Advanced > DNS > Cache > Current* 对话框中显示这些地址。

提示：如果 BOOTP 或 DHCP 服务器无响应，则设备将 IP 地址设置为 0.0.0.0 并再次尝试获取有效的 IP 地址。

BOOTP/DHCP

Client ID

显示设备发送到 BOOTP 或 DHCP 服务器的 DHCP 客户端 ID。如果该服务器已经相应配置完毕，则它将为此 DHCP 客户端 ID 保留一个 IP 地址。因此，设备每次请求时都从该服务器接收相同的 IP。

设备发送的 DHCP 客户端 ID 为在 *Basic Settings > System* 对话框的 *System name* 字段中指定的设备名称。

DHCP option 66/67/4/42

启用/禁用设备中的 *DHCP option 66/67/4/42* 功能。

可能的值：

▶ *On* (默认设置)

DHCP option 66/67/4/42 功能已启用。

设备加载配置概要文件，并使用以下 DHCP 选项接收时间服务器信息：

- Option 66: TFTP server name

Option 67: Boot file name

设备使用 TFTP 协议自动将来自 DHCP 服务器的配置概要文件加载到非永久性存储器 (*RAM*)。

设备使用 *running-config* 中导入的配置概要文件的设置。

- Option 4: Time Server

Option 42: Network Time Protocol Servers

设备接收来自 DHCP 服务器的时间服务器信息。

▶ *Off*

DHCP option 66/67/4/42 功能已禁用。

- 设备不使用 DHCP 选项 66/67 加载配置概要文件。
- 设备不使用 DHCP 选项 4/42 接收时间服务器信息。

IP parameter

此框可用于手动分配 IP 参数。如果用户选择了 *Management interface* 框 *IP address assignment* 选项列表中的 *Local* 单选按钮，则可以编辑这些字段。

IP address

指定可以通过网络访问设备管理的 IP 地址。

可能的值：

- ▶ 有效的 IPv4 地址

Netmask

指定子网掩码。

可能的值：

- ▶ 有效的 IPv4 子网掩码

Gateway address

指定路由器的 IP 地址，设备通过该地址访问其自己网络以外的其他设备。


可能的值：

- ▶ 有效的 IPv4 地址

Remaining lease time

Lease time [s]

显示 DHCP 服务器分配到设备管理的 IP 地址仍然有效的剩余时间（秒）。

若要更新显示，请点击  按钮。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

1.2.3 IPv6

[Basic Settings > Network > IPv6]

此对话框允许用户指定通过 网络访问设备管理所需的 IPv6 设置。

Operation

Operation

启用/禁用设备中的 IPv6 协议。

IPv4 和 IPv6 协议可在设备中同时运行。使用双 IP 层技术（也称为双堆栈）可实现这一目标。

可能的值：

- ▶ *On*（默认设置）
IPv6 协议已启用。
- ▶ *Off*
IPv6 协议已禁用。
如果希望设备仅使用 IPv4 协议运行，请禁用设备中的 IPv6 协议。

Configuration

Dynamic IP address assignment

指定设备管理从中接收其 IPv6 参数的源。

可能的值：

- ▶ *None*
设备手动接收其 IPv6 参数。
用户可手动指定最多 4 个 IPv6 地址。无法将环回、链路本地和 *Multicast* 地址指定为静态 IPv6 地址。
- ▶ *Auto*（默认设置）
设备动态接收其 IPv6 参数。设备接收最多 2 个 IPv6 地址。
这里的示例是路由器通告守护程序（radvd）。radvd 使用 *Router Solicitation* 和 *Router Advertisement* 消息自动配置 IPv6 地址。RFC 4861 中介绍了 *Router Solicitation* 和 *Router Advertisement* 消息。
- ▶ *DHCPv6*
设备从 DHCPv6 服务器接收其 IPv6 参数。
- ▶ *All*
如果选择 *All* 单选按钮，则设备使用动态和手动分配的每个替代项来接收其 IPv6 参数。

DHCP

Client ID

显示设备发送到 DHCPv6 服务器的 DHCPv6 客户端 ID。如果该服务器已进行相应配置，则它将接收此 DHCPv6 客户端 ID 的 IPv6 地址。

从 DHCPv6 服务器接收的 IPv6 地址的 *PrefixLength* 为 128。根据 RFC 8415，此时 DHCPv6 服务器无法用于提供 *Gateway address* 或 *PrefixLength* 信息。

设备仅可从 DHCPv6 服务器接收一个 IPv6 地址。

IP parameter

Gateway address

指定路由器的 IPv6 地址，设备通过该地址访问其自己网络以外的其他设备。

可能的值：

- ▶ 有效的 IPv6 地址（环回和 *Multicast* 地址除外）

提示：如果选择 *Auto* 单选按钮并且使用路由器通告守护程序（radvd），则设备自动接收度量值高于手动设置的 *Gateway address* 的链路本地类型 *Gateway address*。

Duplicate Address Detection

在此字段中，用户可指定设备为 *Duplicate Address Detection* 功能发送的连续 *Neighbor Solicitation* 消息的数量。此功能用于确定接口上的 IPv6 单播地址的唯一性。

Number of neighbor solicitants

指定设备为 *Duplicate Address Detection* 功能发送的 *Neighbor Solicitation* 消息的数量。

可能的值：

- ▶ 0
该功能已禁用。
- ▶ 1..5（默认设置：1）

如果 *Duplicate Address Detection* 功能发现 IPv6 地址在链路上不唯一，则设备不再在日志文件（系统日志）中记录此事件。

表格

此表格显示为设备管理配置的 IPv6 地址的列表。

Prefix

以压缩格式显示 IPv6 地址的前缀。该前缀显示 IPv6 地址最左边的位，也称为地址的网络部分。

PrefixLength

显示 IPv6 地址的前缀长度。

与 IPv4 地址不同，IPv6 地址不使用子网掩码来识别地址的网络部分。此角色在 IPv6 中由前缀长度执行。

可能的值：

- ▶ 0..128

IP address

以压缩格式显示完整 IPv6 地址。

无论设备管理从哪个来源接收其 IPv6 参数，压缩格式都会自动应用到每个 IPv6 地址。

可能的值：

- ▶ 有效的 IPv6 地址
若要在 URL 中使用 IPv6 地址，请使用以下 URL 语法：[https://\[<ipv6_address>\]](https://[<ipv6_address>])。

有关 IPv6 压缩规则和地址类型的更多信息，请参阅“配置”手册。

EUI option

指定是否将 *EUI option* 功能应用到 IPv6 地址。

勾选此复选框后，将自动配置 IPv6 地址的接口 ID。设备使用其接口的 MAC 地址，并在第 3 和第 4 个字节之间添加值 *ff* 和 *fe*，以生成 64 位接口 ID。

仅可为前缀长度等于 64 的 IPv6 地址选择此选项。

可能的值：

- ▶ 勾选
EUI option 功能激活。
- ▶ 未勾选（默认设置）
EUI option 功能停用。

Origin

指定设备接收其 IPv6 参数的方式。

可能的值：

- ▶ *Autoconf*
在选择 *Auto* 单选按钮后，设备会动态接收 IPv6 地址。
- ▶ *Manual*
设备手动接收 IPv6 地址。
- ▶ *DHCP*
设备从 DHCPv6 服务器接收 IPv6 地址。
- ▶ *Linklayer*
设备自动配置链路本地类型 IPv6 地址。无法更改链路本地地址。

Status

显示 IPv6 地址的当前状态。

可能的值：

- ▶ *active*
IPv6 地址已激活。
- ▶ *notInService*
IPv6 地址已停用。
- ▶ *notReady*
已指定 IPv6 地址，但当前不是 *active*，因为某些配置参数仍然缺失。

提示：手动指定 IPv6 地址后，您可以手动在 *active* 和 *notInService* 状态之间进行更改。要进行此更改，请在 *Status* 列中与您的条目相关的下拉列表中选择所需的状态。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

1.3 Out of Band over USB

[Basic Settings > Out of Band over USB]

设备带有允许用户对设备管理进行带外访问的 USB 网络接口。当交换机端口上存在较高带内负载时，您仍然可以通过 USB 网络接口访问设备管理。

设备允许用户使用以下协议通过 USB 网络接口访问设备管理：

- ▶ HTTP
- ▶ HTTPS
- ▶ SSH
- ▶ Telnet
- ▶ SNMP
- ▶ FTP
- ▶ TFTP
- ▶ SFTP
- ▶ SCP

访问设备管理时，存在以下限制：

- ▶ 管理站直接连接到 USB 端口。
- ▶ USB 网络接口不支持以下特性：
 - 优先级标记包
 - 带有 *VLAN* 标签的数据包
 - *DHCP L2 Relay*
 - *LLDP*
 - *DiffServ*
 - *ACL*
 - *Industrial Protocols*

如有需要，您可以在此对话框中更改 IP 参数并禁用 USB 网络接口。

Operation

Operation

启用/禁用 USB 网络接口。

可能的值：

- ▶ *On* (默认设置)
设备允许用户通过 USB 网络接口访问设备管理。
- ▶ *Off*
设备禁止通过 USB 网络接口访问设备管理。

Management interface

Device MAC address

显示 USB 网络接口的 MAC 地址。

Host MAC address

显示已连接的管理站的 MAC 地址。

IP parameter

验证此网络接口的 IP 子网与连接到设备另一个接口的任何子网是否不重叠：

- 管理接口

IP address

指定通过 USB 网络接口进行访问时，设备管理的 IP 地址。

可能的值：

- ▶ 有效的 IPv4 地址
(默认设置: 91.0.0.100)
设备将此 IP 地址增加 1 后，分配给连接到设备的管理站。
示例：USB 网络接口的 IP 为 91.0.0.100，则管理站的 IP 为 91.0.0.101。

Netmask

指定子网掩码。

可能的值：

- ▶ 有效的 IPv4 子网掩码
(默认设置: 255.255.255.0)

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

1.4 Software

[Basic Settings > Software]

此对话框可用于更新设备软件并显示有关设备软件的信息。

用户还可以选择恢复保存在设备中的设备软件的备份。

提示：在更新设备软件之前，请参阅 [Readme](#)（自述）文本文件中的特定版本说明。

Version

Stored version

显示闪存中存储的设备软件的版本号和创建日期。设备在下一次重新启动时加载设备软件。

Running version

显示设备在上一次重新启动时加载且目前正在运行的设备软件的版本号和创建日期。

Backup version

显示闪存中作为备份保存的设备软件的版本号和创建日期。设备在上一次软件更新时或在用户点击 [Restore](#) 按钮后将此设备软件复制到备份存储器之中。

Restore

恢复作为备份保存的设备软件。在此过程中，设备会更改设备软件的 [Stored version](#) 和 [Backup version](#)。

重新启动时，设备会加载 [Stored version](#)。

Bootcode

显示启动代码的版本号和创建日期。

Software update


此外，当镜像文件位于外部存储器中时，设备还允许用户通过右键点击表格更新设备软件。

URL

指定用于更新设备软件的镜像文件的路径和文件名。

设备提供以下设备软件更新选项：

- ▶ 从 PC 进行软件更新

当该文件位于用户 PC 中或网络驱动器上时，请将该文件拖放到  区域中。也可点击该区域以选择该文件。

- ▶ 从 FTP 服务器进行软件更新

当该文件位于 FTP 服务器上时，请以如下形式指定该文件的 URL：

ftp://<???:<??>@<IP ???:<??>/<??>>

- ▶ 从 TFTP 服务器进行软件更新
当该文件位于 TFTP 服务器上时，请以如下形式指定该文件的 URL：
tftp://<IP ??>/<??>/<??>
- ▶ 从 SCP 或 SFTP 服务器进行软件更新
当该文件位于 SCP 或 SFTP 服务器上时，请以如下任一形式指定该文件的 URL：
 - scp:// 或 sftp://<IP ??>/<??>/<??>
 - 点击 *Start* 按钮后，设备会显示 *Credentials* 窗口。在该处输入 *User name* 和 *Password* 以登录服务器。
 - scp:// 或 sftp://<??>:<??>@<IP ??>/<??>/<??>

Start

更新设备软件。

设备将所选文件安装到闪存中，替换之前保存的设备软件。重新启动时，设备会加载安装的设备软件。

设备将现有软件复制到备份存储器中。

在软件更新期间要保持登录到设备，请偶尔移动一下鼠标指针。此外，也可在软件更新之前在 *Device Security > Management Access > Web* 对话框的 *Web interface session timeout [min]* 字段中指定一个足够大的值。

表格

File location

显示设备软件的存储位置。

可能的值：

- ▶ *ram*
设备的非永久性存储器
- ▶ *flash*
设备的永久存储器 (*NVM*)
- ▶ *usb*
外部 USB 存储器 (EAM)

Index

显示设备软件的索引。

对于闪存中的设备软件，该索引具有以下含义：

- ▶ 1
重新启动时，设备会加载此设备软件。
- ▶ 2
设备在上一次软件更新期间将此设备软件复制到备份区域之中。

File name

显示设备软件的设备内部文件名。

Firmware

显示设备软件的版本号和创建日期。

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

1.5 Load/Save

[Basic Settings > Load/Save]

此对话框可用于将设备设置永久保存到一个配置概要文件中。

设备可以保存多个配置概要文件。激活一个备选配置概要文件后，即可切换到其他设备设置。用户可以选择将配置概要文件导出至用户 PC 或服务器。用户还可以选择将配置概要文件从用户 PC 或服务器导入到设备。

默认设置下，设备会保存未加密的配置概要文件。如果用户在 *Configuration encryption* 框中输入密码，则设备以加密格式保存当前和未来的配置概要文件。

无意中更改设置可能会终止用户 PC 和设备之间的连接。要使设备保持可访问，请在更改任何设置之前启用 *Undo configuration modifications* 功能。如果连接中断，则设备在经过指定时间之后会加载永久存储器 (NVM) 中保存的配置概要文件。

External memory

Selected external memory

显示外部存储器的类型。

可能的值：

- ▶ *usb*
外部 USB 存储器 (EAM)

Status

显示外部存储器的工作状态。

可能的值：

- ▶ *notPresent*
未连接外部存储器。
- ▶ *removed*
有人在操作期间从设备中移除了外部存储器。
- ▶ *ok*
外部存储器已连接且已处于运行准备就绪状态。
- ▶ *outOfMemory*
外部存储器内存空间被占用。
- ▶ *genericErr*
设备检测到错误。

Configuration encryption

Active

显示设备中的配置加密是已激活还是已停用。

可能的值：

▶ **勾选**

配置加密已激活。

如果配置概要文件已加密并且密码与设备中存储的密码匹配，则设备从永久存储器（*NVM*）中加载一个配置概要文件。

▶ **未勾选**

配置加密已停用。

如果配置概要文件未加密，则设备只从永久存储器（*NVM*）中加载一个配置概要文件。

如果在 *Basic Settings > External Memory* 对话框中，*Config priority* 列的值为 *first* 并且配置概要文件未加密，则 *Basic Settings > System* 对话框中的 *Security status* 框会显示一个警报。

在 *Diagnostics > Status Configuration > Security Status* 对话框 *Global* 选项卡的 *Monitor* 列中，可以指定设备是否监控 *Load unencrypted config from external memory* 参数。

Set password

打开帮助用户输入配置概要文件加密所需的密码的 *Set password* 窗口。对配置概要文件进行加密可使非授权访问变得更加困难。为此，请执行以下步骤：

- 更改现有密码时，请在 *Old password* 字段中输入现有密码。要以明文而非 *****（若干星号）形式显示密码，请勾选 *Display content* 复选框。
- 在 *New password* 字段中，输入密码。
要以明文而非 *****（若干星号）形式显示密码，请勾选 *Display content* 复选框。
- 勾选 *Save configuration afterwards* 复选框，对永久存储器（*NVM*）和外部存储器中的选定配置概要文件也使用加密。

提示： 如果设备的永久存储器（*NVM*）中最多存储一份配置概要文件，则只使用此功能。在创建更多配置概要文件之前，请确定是否在设备中永久激活配置加密。对更多配置概要文件进行不加密保存或同一密码加密保存。

如果您要使用加密的配置文件替换设备，例如由于设备不工作，请执行以下步骤：

- 重新启动新设备并分配 *IP* 参数。
- 打开新设备上的 *Basic Settings > Load/Save* 对话框。
- 对新设备中的配置概要文件进行加密。如上。输入您在不工作的设备中使用的相同密码。
- 在新设备中安装来自不工作设备的外部存储器。
- 重新启动新设备。
当您重新启动设备时，设备会从外部存储器加载配置文件以及不工作设备的设置。设备将设置复制到非永久性存储器（*RAM*）和永久存储器（*NVM*）中。

Delete

打开帮助用户取消设备中的配置加密的 *Delete* 窗口。要取消配置加密，请执行以下步骤：

- 在 *Old password* 字段中，输入现有密码。
要以明文而非 *****（若干星号）形式显示密码，请勾选 *Display content* 复选框。
- 勾选 *Save configuration afterwards* 复选框，对永久存储器（*NVM*）和外部存储器中的选定配置概要文件也取消加密。

提示：如果在存储器中保留更多的加密配置概要文件，则设备可以帮助用户防止以“选定”状态激活或指定这些配置概要文件。

Information

NVM in sync with running config

显示非永久性存储器（*RAM*）中的配置概要文件与永久存储器（*NVM*）中的“选定”配置概要文件是否相同。

可能的值：

- ▶ *勾选*
这两个配置概要文件相同。
- ▶ *未勾选*
这两个配置概要文件不同。

External memory in sync with NVM

显示外部存储器中的“选定”配置概要文件与永久存储器（*NVM*）中的“选定”配置概要文件是否相同。

可能的值：

- ▶ *勾选*
这两个配置概要文件相同。
- ▶ *未勾选*
这两个配置概要文件不同。
可能的原因：
 - 设备没有连接外部存储器。
 - 在 *Basic Settings > External Memory* 对话框中，*Backup config when saving* 功能已禁用。

Backup config on a remote server when saving

Operation

启用/禁用 *Backup config on a remote server when saving* 功能。

可能的值：

- ▶ *Enabled*
Backup config on a remote server when saving 功能已启用。
将配置概要文件保存到永久存储器（*NVM*）中时，设备会将该配置概要文件自动备份到 *URL* 字段中指定的远程服务器上。
- ▶ *Disabled*（默认设置）
Backup config on a remote server when saving 功能已禁用。

URL

指定远程服务器上备份配置概要文件的路径和文件名。

可能的值：

- ▶ 带有 0..128 个字符的字母数字 ASCII 字符串
示例：tftp://192.9.200.1/cfg/config.xml
设备支持以下通配符：
 - %d
YYYY-mm-dd 格式的系统日期
 - %t
HH_MM_SS 格式的系统时间
 - %i
设备的 IP 地址
 - %m
AA-BB-CC-DD-EE-FF 格式的设备 MAC 地址
 - %p
设备的产品名称

Set credentials

打开可以帮助用户输入在远程服务器上身份验证所需的登录凭证的 *Credentials* 窗口。为此，请执行以下步骤：

- 在 *User name* 字段中，输入用户名。
要以明文而非 *****（若干星号）形式显示用户名，请勾选 *Display content* 复选框。
可能的值：
 - 带有 1..32 个字符的字母数字 ASCII 字符串
- 在 *Password* 字段中，输入密码。
要以明文而非 *****（若干星号）形式显示密码，请勾选 *Display content* 复选框。
可能的值：
 - ▶ 带有 6..64 个字符的字母数字 ASCII 字符串
允许以下字符：
 - a..z
 - A..Z
 - 0..9
 - !#\$%&'()*+,-./:;<=>?@[\\]^_`{|}~

Undo configuration modifications

Operation

启用/禁用 *Undo configuration modifications* 功能。利用此功能，设备可持续检查是否仍然可以通过用户 PC 的 IP 地址访问设备。如果连接中断，经过指定时间期限后，设备会从永久存储器 (NVM) 加载“选定”配置概要文件。之后，可以再次访问设备。

可能的值：

▶ *On*

该功能已启用。

- 可以在 *Timeout [s] to recover after connection loss* 字段中指定连接中断与配置概要文件加载之间的时间期限。
- 当永久存储器 (NVM) 包含多个配置概要文件时，设备会加载指定为“选定”的配置概要文件。

▶ *Off* (默认设置)

该功能已禁用。

在关闭图形用户界面之前，请再次禁用该功能。如此可帮助防止设备恢复指定为“选定”的配置概要文件。

提示： 启用该功能之前，请保存配置概要文件中的设置。因此，设备中会保留临时保存的当前更改。

Timeout [s] to recover after connection loss

指定在连接中断时设备从永久存储器 (NVM) 加载“选定”配置概要文件之前经过的时间（秒）。

可能的值：

▶ 30..600 (默认设置：600)

请指定一个足够大的值。请考虑用户查看图形用户界面对话框但不做任何更改或更新所花费的时间。

Watchdog IP address

显示启用该功能的 PC 的 IP 地址。

可能的值：

▶ IPv4 地址 (默认设置：0.0.0.0)

表格

Storage type

显示配置概要文件的存储位置。

可能的值：

▶ *RAM* (设备的非永久性存储器)


在非永久性存储器中，设备会存储当前操作的设置。

▶ *NVM* (设备的永久存储器)

在应用 *Undo configuration modifications* 功能时或重新启动期间，设备会从永久存储器加载“选定”配置概要文件。

永久存储器为多个配置概要文件提供空间，具体视配置概要文件中保存的设置的数量而定。设备在永久存储器中管理最多 20 个配置概要文件。

可以将一个配置概要文件加载到非永久性存储器 (*RAM*) 中。为此，请执行以下步骤：

- 在表格中，突出显示该配置概要文件。
- 点击  按钮，然后点击 *Activate* 项目。

▶ *ENVM* (外部存储器)

在外部存储器中，设备保存“选定”配置概要文件的备份副本。

前提条件是，在 *Basic Settings > External Memory* 对话框中，用户勾选了 *Backup config when saving* 复选框。

Profile name

显示配置概要文件的名称。

可能的值：


▶ *running-config*

非永久性存储器 (*RAM*) 中配置概要文件的名称。


▶ *config*

永久存储器 (*NVM*) 中出厂设置配置概要文件的名称。

▶ 用户自定义名称

设备允许用户突出显示表格中一个现有的配置概要文件，点击  按钮，然后点击 *Save as...* 项目，从而保存具有用户自定义名称的配置概要文件。

要将配置概要文件以 XML 文件格式导出至用户 PC，请点击该链接。然后，选择存储位置并指定文件名。


要将该文件保存到远程服务器上，请点击  按钮，然后点击 *Export...* 项目。

Modification date (UTC)

显示用户上次保存配置概要文件的时间 (UTC)。

Selected

显示配置概要文件是否被指定为“选定”。


要将另一个配置概要文件指定为“选定”，请突出显示表格中的所需配置概要文件，点击  按钮，然后点击 *Activate* 项目。

可能的值：

▶ 勾选

配置概要文件被指定为“选定”。

- 在应用 *Undo configuration modifications* 功能时或重新启动期间，设备会将配置概要文件加载到非永久性存储器 (*RAM*) 中。

- 点击  按钮后，设备会将临时保存的设置保存到此配置概要文件中。

▶ 未勾选

另一个配置概要文件被指定为“选定”。

Encrypted

显示是否对配置概要文件进行加密。

可能的值：

- ▶ 勾选
配置概要文件已加密。
- ▶ 未勾选
配置概要文件未加密。

可以在 *Configuration encryption* 框中激活/停用配置概要文件的加密。

Encryption verified

显示加密配置概要文件的密码是否与存储在设备中的密码匹配。

可能的值：

- ▶ 勾选
这两个密码匹配。设备能够解除配置概要文件的加密。
- ▶ 未勾选
这两个密码不同。设备不能解除配置概要文件的加密。

Software version

显示设备在保存配置概要文件时运行的设备软件的版本号。

Fingerprint

显示配置概要文件中保存的校验和。

保存设置时，设备会计算校验和并将其插入配置概要文件中。

Fingerprint verified

显示配置概要文件中保存的校验和是否有效。

设备会计算标记为“选定”的配置概要文件的校验和，并将其与该配置概要文件中保存的校验和进行比较。

可能的值：

- ▶ 勾选
计算的校验和与保存的校验和相匹配。
保存的设置一致。
- ▶ 未勾选
对于适用的标记为“选定”的配置概要文件：
计算的校验和与保存的校验和不同。
该配置概要文件包含修改过的设置。
可能的原因：
 - 文件已损坏。
 - 外部存储器中的文件系统不一致。
 - 某用户导出了配置概要文件并在设备外部更改了 XML 文件。对于其他配置概要文件，设备没有计算校验和。

只有当按照以下步骤提前保存了配置概要文件时，设备才能正确地验证校验和：

- 在同一设备上
- 使用设备正在运行的同一软件版本

提示：此功能可以识别对配置概要文件中设置的更改。该功能不提供针对使用修改过的设置操作设备的保护。

按钮

“按钮” 页 16一节中提供了标准按钮的描述。



从永久存储器 (NVM) 或外部存储器中删除表格中突出显示的配置概要文件。

如果该配置概要文件被指定为“选定”，则设备可以帮助用户防止删除该配置概要文件。

Save as..

复制表格中突出显示的配置概要文件，并使用用户指定名称将其保存到永久存储器 (NVM) 中。设备将新的配置概要文件指定为“选定”。

提示：在创建更多配置概要文件之前，请确定是否在设备中永久激活配置加密。对更多配置概要文件进行不加密保存或同一密码加密保存。

如果在 *Basic Settings > External Memory* 对话框中，*Backup config when saving* 列中的复选框被勾选，则设备会将外部存储器中名称相同的配置概要文件指定为“选定”。

Activate

将表格中突出显示的配置概要文件的设置加载到非永久性存储器 (RAM) 中。

- ▶ 设备终止与图形用户界面的连接。要再次访问设备管理，请执行以下步骤：
 - 重新加载图形用户界面。
 - 再次登录。
- ▶ 设备立即动态地使用配置概要文件的设置。

在激活另一个配置概要文件之前，请启用 *Undo configuration modifications* 功能。如果以后连接中断，则设备会从永久存储器 (NVM) 加载上一个指定为“选定”的配置概要文件。然后，可以再次访问设备。

如果配置加密已停用，则设备会加载一个未加密的配置概要文件。如果配置加密已激活并且密码与设备中存储的密码相匹配，则设备会加载一个加密的配置概要文件。

激活一个较早的配置概要文件后，设备将沿用此软件版本中包含的功能的设置。设备将新功能的值设置为默认值。

Select

将表格中突出显示的配置概要文件指定为“选定”。然后，在 *Selected* 列中，复选框变为勾选。

在应用 *Undo configuration modifications* 功能时或重新启动期间，设备会将此配置概要文件的设置加载到非永久性存储器 (RAM) 中。

- ▶ 如果设备中的配置加密已禁用，则只将一个未加密的配置概要文件指定为“选定”。
- ▶ 如果设备中的配置加密已启用并且配置概要文件的密码与设备中保存的密码相匹配，则只将一个加密的配置概要文件指定为“选定”。

否则，设备在下次重新启动时将无法加载和加密配置概要文件中的设置。对于这种情况，可以在 *Diagnostics > System > Selftest* 对话框中指定设备是使用默认设置进行启动还是终止重新启动并停止。


提示： 只勾选永久存储器（*NVM*）中保存的配置概要文件。

如果在 *Basic Settings > External Memory* 对话框中，*Backup config when saving* 列中的复选框被勾选，则设备会将外部存储器中名称相同的配置概要文件指定为“选定”。

Import...

打开 *Import...* 窗口导入一个配置概要文件。

前提条件是，用户已使用 *Export...* 按钮或使用 *Profile name* 列中的链接导出了配置概要文件。

- 在 *Select source* 下拉列表中，选择设备从哪里导入配置概要文件。
 - ▶ *PC/URL*
设备从本地 PC 或远程服务器导入配置概要文件。
 - ▶ *External memory*
设备从外部存储器导入配置概要文件。
- 在上面选择 *PC/URL* 后，用户可在 *Import profile from PC/URL* 框中指定要导入的配置概要文件。
 - 从 PC 导入
当该文件位于用户 PC 中或网络驱动器上时，请将该文件拖放到  区域中。也可点击该区域以选择该文件。
 - 从 FTP 服务器导入
当该文件位于 FTP 服务器上时，请以如下形式指定该文件的 URL：
ftp://<???:<???:@<IP ???:<???:<???:<???:>
 - 从 TFTP 服务器导入
当该文件位于 TFTP 服务器上时，请以如下形式指定该文件的 URL：
tftp://<IP ???:<???:<???:<???:>
 - 从 SCP 或 SFTP 服务器导入
当该文件位于 SCP 或 SFTP 服务器上时，请以如下任一形式指定该文件的 URL：
scp:// 或 sftp://<IP ???:<???:<???:<???:>
点击 *Start* 按钮后，设备会显示 *Credentials* 窗口。在该处输入 *User name* 和 *Password* 以登录服务器。
scp:// 或 sftp://<???:<???:@<IP ???:<???:<???:<???:>
- 在上面选择 *External memory* 后，用户可在 *Import profile from external memory* 框中指定要导入的配置概要文件。
 - 在 *Profile name* 下拉列表中，选择要导入的配置概要文件的名称。
- 在 *Destination* 框中，可以指定设备在哪里保存导入的配置概要文件。
 - 在 *Profile name* 字段中，可以指定设备用以保存配置概要文件的名称。
 - 在 *Storage type* 字段中，可以指定配置概要文件的存储位置。前提条件是，在 *Select source* 下拉列表中选择 *PC/URL* 项目。
 - ▶ *RAM*
设备将配置概要文件保存到设备的非永久性存储器（*RAM*）中。这将取代 *running-config*，设备会立即使用导入的配置概要文件的设置。设备终止与图形用户界面的连接。重新加载图形用户界面。再次登录。
 - ▶ *NVM*
设备将配置概要文件保存到设备的永久存储器（*NVM*）中。

导入一个配置概要文件后，设备将按照以下步骤沿用设置：

- 如果配置概要文件是在相同的设备上或在相同类型和相同配置的设备上导出的，则：设备将完全沿用设置。
- 如果配置概要文件是在其他设备上导出的，则：设备将沿用它根据硬件设备和软件级别可以解释的设置。设备从其 *running-config* 配置概要文件中沿用的剩余设置。

对于配置概要文件加密，也请阅读 *Configuration encryption* 框的帮助文本。在以下条件下，设备会导入一个配置概要文件：

- 设备的配置加密已停用。配置概要文件未加密。
- 设备的配置加密已激活。配置概要文件使用设备当前使用的同一密码进行了加密。

Export...

导出表格中突出显示的配置概要文件并将其另存为远程服务器上的 XML 文件。

要将该文件保存到用户 PC 上，请点击 *Profile name* 列中的链接，选择存储位置并指定文件名。

设备为用户提供导出配置概要文件的以下选项：

▶ 导出至 FTP 服务器

要将该文件保存到 FTP 服务器上，请以如下形式指定该文件的 URL：

`ftp://<???:<??>@<IP ??>:<??>/<??>>`

▶ 导出至 TFTP 服务器

要将该文件保存到 TFTP 服务器上，请以如下形式指定该文件的 URL：

`tftp://<IP ??>/<??>/<??>>`

▶ 导出至 SCP 或 SFTP 服务器

要将该文件保存到 SCP 或 SFTP 服务器上，请以如下任一形式指定该文件的 URL：

- `scp:// 或 sftp://<IP ??>/<??>/<??>>`

点击 *Ok* 按钮后，设备会显示 *Credentials* 窗口。在该处输入 *User name* 和 *Password* 以登录服务器。


- `scp:// 或 sftp://<???:<??>@<IP ??>/<??>/<??>>`

Load running-config as script

导入一个修改当前 *running config* 配置概要文件的脚本文件。

设备为用户提供导入脚本文件的以下选项：

▶ 从 PC 导入

当该文件位于用户 PC 中或网络驱动器上时，请将该文件拖放到  区域中。也可点击该区域以选择该文件。

▶ 从 FTP 服务器导入

当该文件位于 FTP 服务器上时，请以如下形式指定该文件的 URL：

`ftp://<???:<??>@<IP ??>:<??>/<??>>`

▶ 从 TFTP 服务器导入

当该文件位于 TFTP 服务器上时，请以如下形式指定该文件的 URL：

`tftp://<IP ??>/<??>/<??>>`

▶ 从 SCP 或 SFTP 服务器导入

当该文件位于 SCP 或 SFTP 服务器上时，请以如下任一形式指定该文件的 URL：

`scp:// 或 sftp://<IP ??>/<??>/<??>>`

提示：设备将脚本文件附加到当前设置。验证脚本文件不包含与当前设置冲突的任何部分。

Save running-config as script

将 *running config* 配置概要文件另存为本地 PC 上的脚本文件。这可用于对当前设备设置进行备份或在不同设备上使用这些设置。

Back to factory...

将设备中的设置重置为默认值。

- ▶ 设备从非永久性存储器 (*RAM*) 和永久存储器 (*NVM*) 中删除保存的配置概要文件。
- ▶ 设备删除网络服务器使用的设备中的 HTTPS 证书。
- ▶ 设备删除 SSH 服务器使用的设备中的 RSA 密钥 (主机密钥)。
- ▶ 当连接了外部存储器时, 设备会删除外部存储器中保存的配置概要文件。
- ▶ 稍后, 设备会重新启动并加载默认值。

Back to default

从非永久性存储器 (*running config*) 中删除当前运行的 (*RAM*) 设置。

1.6 External Memory

[Basic Settings > External Memory]

此对话框可用于激活设备与外部存储器一起自动执行的功能。此对话框还显示外部存储器的工作状态和标识特征。

表格

Type

显示外部存储器的类型。

可能的值：

- ▶ *usb*
外部 USB 存储器 (EAM)

Status

显示外部存储器的工作状态。

可能的值：

- ▶ *notPresent*
未连接外部存储器。
- ▶ *removed*
有人在操作期间从设备中移除了外部存储器。
- ▶ *ok*
外部存储器已连接且已处于运行准备就绪状态。
- ▶ *outOfMemory*
外部存储器内存空间被占用。
- ▶ *genericErr*
设备检测到错误。

Writable

显示设备是否具有对外部存储器的写访问权限。

可能的值：

- ▶ 勾选
设备具有对外部存储器的写访问权限。
- ▶ 未勾选
设备具有对外部存储器的只读访问权限。外部存储器中可能激活了写保护。

Software auto update

激活/停用重新启动期间的自动设备软件更新。

可能的值：

▶ **勾选** (默认设置)

重新启动期间的自动设备软件更新已激活。当以下文件位于外部存储器中时，设备会更新设备软件：

- 设备软件的镜像文件
- 内容为 `cwvqWrfcvg?>kocigahkngapcog@0dkp` 的文本文件 `startup.txt`

▶ **未勾选**

重新启动期间的自动设备软件更新已停用。

SSH key auto upload

激活/停用重新启动时从外部存储器加载 RSA 密钥。

可能的值：

▶ **勾选** (默认设置)

RSA 密钥加载已激活。

当以下文件位于外部存储器中时，在重新启动期间，设备会从外部存储器加载 RSA 密钥：

- SSH RSA 密钥文件
- 具有以下内容的文本文件 `startup.txt`

```
autoUpdateRSA=<filename_of_the_SSH_RSA_key>
```

设备在串行接口的系统控制台显示消息。

▶ **未勾选**

RSA 密钥加载已停用。

提示：从外部存储器 (*ENVM*) 加载 RSA 密钥时，设备会覆盖永久存储器 (*NVM*) 中的现有密钥。

Config priority

指定设备在重新启动时从其中加载配置概要文件的存储器。

可能的值：

▶ **disable**

设备从永久存储器 (*NVM*) 加载配置概要文件。

▶ **first**

设备从外部存储器加载配置概要文件。

当设备在外部存储器中找不到配置概要文件时，它会从永久存储器 (*NVM*) 加载配置概要文件。

提示：从外部存储器 (*ENVM*) 加载配置概要文件时，设备会覆盖永久存储器 (*NVM*) 中选定配置概要文件的设置。

如果 *Config priority* 列的值为 *first* 并且配置概要文件未加密，则 *Basic Settings > System* 对话框中的 *Security status* 框会显示一个警报。

在 *Diagnostics > Status Configuration > Security Status* 对话框 *Global* 选项卡的 *Monitor* 列中，可以指定设备是否监控 *Load unencrypted config from external memory* 参数。

Backup config when saving

激活/停用在外部存储器中创建配置概要文件的副本。

可能的值：

- ▶ **勾选**（默认设置）

副本创建已激活。点击 *Basic Settings > Load/Save* 对话框中的 *Save* 按钮时，设备会在活动的外部存储器中生成配置概要文件的副本。

- ▶ **未勾选**

副本创建已停用。设备不生成配置概要文件的副本。

Manufacturer ID

显示存储器制造商的名称。

Revision

显示存储器制造商指定的修订版本号。

Version

显示存储器制造商指定的版本号。

Name

显示存储器制造商指定的产品名称。

Serial number

显示存储器制造商指定的序列号。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

1.7 Port

[Basic Settings > Port]

此对话框可用于指定各个端口的设置。此对话框还显示每个端口的运行模式、连接状态、比特率和双工模式。

该对话框包含以下选项卡：

- ▶ [Configuration]
- ▶ [Statistics]
- ▶ [Utilization]

[Configuration]

表格

Port

显示端口编号。

Name

端口名称。

可能的值：

- ▶ 带有 0..64 个字符的字母数字 ASCII 字符串
允许以下字符：
 - <space>
 - 0..9
 - a..z
 - A..Z
 - !#\$%&'()*+,-./:;<=>?@[\\]^_`{|}~

Port on

激活/停用端口。

可能的值：

- ▶ 勾选（默认设置）
端口已激活。
- ▶ 未勾选
端口已停用。端口不发送或接收任何数据。

State

显示端口当前是物理启用还是物理禁用。

可能的值：

- ▶ **勾选**
端口已物理启用。
- ▶ **未勾选**
端口已物理禁用。
当 *Port on* 功能激活时，*Auto-Disable* 功能禁用了该端口。
可在 *Diagnostics > Ports > Auto-Disable* 对话框中指定 *Auto-Disable* 功能的设置。

Power state (port off)

指定使用 *Port on* 功能停用端口后端口是物理打开还是物理关闭。

可能的值：

- ▶ **勾选**
端口保持物理启用状态。一个相连设备接收一个活动链接。
- ▶ **未勾选**（默认设置）
端口已物理禁用。

Auto power down

指定没有连接电缆时端口的行为。

可能的值：

- ▶ *no-power-save*（默认设置）
端口保持激活状态。
- ▶ *auto-power-down*
端口切换到省电模式。
- ▶ *unsupported*
端口不支持此功能并保持激活状态。

Automatic configuration

激活/停用端口运行模式的自动选择。

可能的值：

- ▶ **勾选**（默认设置）
运行模式自动选择已激活。
端口通过自动协商独立协商运行模式，并自动检测连接到 TP 端口的设备（自动电缆交叉）。
此设置优先于手动端口设置。
经过几秒钟，直到端口设置了运行模式为止。
- ▶ **未勾选**
运行模式自动选择已停用。
端口使用用户在 *Manual configuration* 列中以及 *Manual cable crossing (Auto. conf. off)* 列中指定的值进行工作。
- ▶ **灰色显示**
无运行模式自动选择。

Manual configuration

指定 *Automatic configuration* 功能禁用时端口的运行模式。

可能的值：

- ▶ 10 Mbit/s HDX
半双工连接
- ▶ 10 Mbit/s FDX
全双工连接
- ▶ 100 Mbit/s HDX
半双工连接
- ▶ 100 Mbit/s FDX
全双工连接
- ▶ 1000 Mbit/s FDX
全双工连接
- ▶ 2500 Mbit/s FDX
全双工连接

提示： 实际可用的端口的运行模式取决于设备配置。

Link/Current settings

显示端口当前使用的运行模式。

可能的值：

- ▶ -
未连接电缆，无链路。
- ▶ 10 Mbit/s HDX
半双工连接
- ▶ 10 Mbit/s FDX
全双工连接
- ▶ 100 Mbit/s HDX
半双工连接
- ▶ 100 Mbit/s FDX
全双工连接
- ▶ 1000 Mbit/s FDX
全双工连接
- ▶ 2500 Mbit/s FDX
全双工连接

提示： 实际可用的端口的运行模式取决于设备配置。

Manual cable crossing (Auto. conf. off)

指定连接到 TP 端口的设备。

前提条件是 *Automatic configuration* 功能已禁用。

可能的值：

- ▶ *mdi*
设备在端口上交换发送和接收线对。
- ▶ *mdix* (TP 端口上的默认设置)
设备帮助用户防止端口上发送和接收线对的交换。

▶ *auto-mdix*

设备检测所连接设备的发送和接收线对，并自动进行适应。

示例：当用户使用交叉电缆连接终端设备时，设备会将端口从 *mdix* 自动重置为 *mdi*。

▶ *unsupported*（光学端口或 TP-SFP 端口上的默认设置）

端口不支持此功能。

Flow control

激活/停用端口上的流量控制。

可能的值：

▶ *勾选*（默认设置）

端口上的流量控制已激活。

端口上激活了暂停数据包（全双工运行）或冲突（半双工运行）的发送和评估。

要启用设备中的流量控制，也请激活 *Switching > Global* 对话框中的 *Flow control* 功能。

也请激活连接到此端口的设备的端口上的流量控制。

在一个上行链路端口上，激活流量控制可能会导致上一级网段中产生意外的发送中断（“流浪反向压力”）。

▶ *未勾选*

端口上的流量控制已停用。

如果用户正在使用冗余功能，则停用参与端口上的流量控制。如果流量控制和冗余功能同时激活，则冗余功能的运行可能与预期有所不同。

Send trap (Link up/down)

激活/停用当设备检测到此端口上行/下行状态发生变化时 SNMP 陷阱的发送。

可能的值：

▶ *勾选*（默认设置）

SNMP 陷阱发送激活。

当设备检测到上行/下行状态发生变化时，设备发送一个 SNMP 陷阱。

▶ *未勾选*

SNMP 陷阱发送停用。

发送 SNMP 陷阱的前提条件是，用户在 *Diagnostics > Status Configuration > Alarms (Traps)* 中启用该功能并至少指定一个陷阱目的地。

MTU

以字节为单位指定端口上以太网数据包的最大允许大小。

可能的值：

▶ *1518..9720*（默认设置：*1518*）

使用 *1518* 设置时，端口会传输不超过以下大小的以太网数据包：

- 1518 字节，无 VLAN 标签
（1514 字节 + 4 字节 CRC）
- 1522 字节，包含 VLAN 标签
（1518 字节 + 4 字节 CRC）

用户可使用此设置增加此端口能够接收或传输的以太网数据包的最大允许大小。

以下列表包含了可能的应用：

- ▶ 当用户在传输网络中使用带有双 VLAN 标签的设备时，可能需要大出 4 个字节的 *MTU*。

在其他接口上，可按照以下步骤指定以太网数据包的最大允许大小：

- *Link Aggregation* 接口
Switching > L2-Redundancy > Link Aggregation 对话框，*MTU* 列

Signal

激活/停用端口 LED 指示灯闪烁。此功能可用于识别现场端口。

可能的值：

- ▶ 勾选
 端口 LED 指示灯闪烁已激活。
 端口 LED 指示灯闪烁，直到再次禁用该功能为止。
- ▶ 未勾选（默认设置）
 端口 LED 指示灯闪烁已停用。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

Clear port statistics

将端口统计计数器重置为 0。

[Statistics]

此选项卡显示每个端口的如下概览：

- ▶ 设备接收的数据包/字节的数量
 - *Received packets*
 - *Received octets*
 - *Received unicast packets*
 - *Received multicast packets*
 - *Received broadcast packets*
- ▶ 设备发送的数据包/字节的数量
 - *Transmitted packets*
 - *Transmitted octets*
 - *Transmitted unicast packets*
 - *Transmitted multicast packets*
 - *Transmitted broadcast packets*
- ▶ 设备检测到的错误的数量
 - *Received fragments*
 - *Detected CRC errors*
 - *Detected collisions*

- ▶ 设备接收的每种大小类别的数据包的数量
 - *Packets 64 bytes*
 - *Packets 65 to 127 bytes*
 - *Packets 128 to 255 bytes*
 - *Packets 256 to 511 bytes*
 - *Packets 512 to 1023 bytes*
 - *Packets 1024 to 1518 bytes*
- ▶ 设备丢弃的数据包的数量
 - *Received discards*
 - *Transmitted discards*

要根据特定条件对表格进行排序，请点击相应行的标题。

例如，要根据所收到字节数量按升序对表格进行排序，请点击一次 *Received octets* 列的标题。要按降序进行排序，请再点击一次该标题。

要将表格中端口统计计数器重置为 0，请执行以下步骤：

- 在 *Basic Settings > Port* 对话框中，点击  按钮，然后点击 *Clear port statistics* 项目。
或者
- 在 *Basic Settings > Restart* 对话框中，点击 *Clear port statistics* 按钮。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

Clear port statistics

将端口统计计数器重置为 0。

[Utilization]

此选项卡显示各个端口的利用率（网络负载）。

表格

Port

显示端口编号。

Utilization [%]

显示相对于 *Control interval [s]* 列中指定的时间间隔的当前利用率（百分比）。

利用率指的是在当前配置的数据速率下接收的数据量与最大可能的数据量的关系。

Lower threshold [%]

指定利用率阈值下限。如果端口利用率低于此值，则 *Alarm* 列会显示一个警报。

可能的值：

▶ 0.00..100.00（默认设置：0.00）

值 0 会停用阈值下限。

Upper threshold [%]

指定利用率阈值上限。如果端口利用率高于此值，则 *Alarm* 列会显示一个警报。

可能的值：

▶ 0.00..100.00（默认设置：0.00）

值 0 会停用阈值上限。

Control interval [s]

指定间隔（秒）。

可能的值：

▶ 1..3600（默认设置：30）

Alarm

显示利用率警报状态。

可能的值：

▶ 勾选

端口利用率低于 *Lower threshold [%]* 列中指定的值或高于 *Upper threshold [%]* 列中指定的值。设备发送一个 SNMP 陷阱。

▶ 未勾选

端口利用率高于 *Lower threshold [%]* 列中指定的值且低于 *Upper threshold [%]* 列中指定的值。发送 SNMP 陷阱的前提条件是，用户在 *Diagnostics > Status Configuration > Alarms (Traps)* 中启用该功能并至少指定一个陷阱目的地。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

Clear port statistics

将端口统计计数器重置为 0。

1.8 Power over Ethernet (MCSESP)

[Basic Settings > Power over Ethernet]

在以太网供电 (PoE) 中，电源设备 (PSE) 通过双绞线向 IP 电话等受电设备 (PD) 供电。

PSE 设备外壳上的产品代码和 PoE 特定标签指示设备是否支持 *Power over Ethernet*。按照 IEEE 802.3at 的规定，设备的 PoE 端口支持以太网供电。

系统可针对端口提供内部最大功率预算。端口根据检测到的已连接受电设备的类别来保留功率。实际提供的功率等于或小于保留的功率。

用户通过 *Priority* 参数来管理功率输出。当已连接的设备所需的功率总和超过可用功率时，设备会根据已配置的优先级停止向端口供电。设备首先从配置为低优先级的端口开始停止向端口供电。当多个端口配置为低优先级时，设备从编号较高的端口开始停止供电。

该菜单包含以下对话框：

- ▶ PoE Global
- ▶ PoE Port

1.8.1 PoE Global

[Basic Settings > Power over Ethernet > Global]

根据在此对话框中指定的设置，设备向最终用户设备供电。如果功率消耗达到用户指定的阈值，则设备会发送 SNMP 陷阱。

Operation

Operation

启用/禁用 *Power over Ethernet* 功能。

可能的值：

- ▶ *On* (默认设置)
Power over Ethernet 功能已启用。
- ▶ *Off*
Power over Ethernet 功能已禁用。

Configuration

Send trap

激活/停用发送 SNMP 陷阱。

如果功率消耗超过用户指定的阈值，则设备会发送 SNMP 陷阱。

可能的值：

- ▶ 勾选 (默认设置)
设备发送 SNMP 陷阱。
- ▶ 未勾选
设备不发送任何 SNMP 陷阱。

发送 SNMP 陷阱的前提条件是，用户在 *Diagnostics > Status Configuration > Alarms (Traps)* 中启用该功能并至少指定一个陷阱目的地。

Threshold [%]

以百分比为单位指定功率消耗的阈值。

如果功率输出超过此阈值，则设备会测量总输出功率并发送 SNMP 陷阱。

可能的值:

▶ 0..99 (默认设置: 90)

System power

Budget [W]

显示可用于全局预算的功率总和。

Reserved [W]

显示全局保留的功率。设备根据检测到的已连接受电设备的类别来保留功率。保留的功率等于或小于实际提供的功率。

Delivered [W]

以瓦为单位显示向模块提供的实际功率。

Delivered [mA]

以毫安为单位显示向模块提供的实际电流。

表格

Module

与表格条目相关的设备模块。

Configured power budget [W]

指定在端口上分配的模块功率。

可能的值:

▶ 0..n (默认设置: n)

此处, n 对应于 *Max. power budget [W]* 列中的值。

Max. power budget [W]

显示可用于此模块的最大功率。

Reserved power [W]

显示根据检测到的已连接受电设备的类别为模块保留的功率。

Delivered power [W]

以瓦为单位显示向连接到此端口的受电设备提供的实际功率。

Delivered current [mA]

以毫安为单位显示向连接到此端口的受电设备提供的实际电流。

Power source

显示设备的电源设备。

可能的值：

- ▶ *internal*
内部电源
- ▶ *external*
外部电源

Threshold [%]

以百分比为单位指定模块的功率消耗的阈值。如果功率输出超过此阈值，则设备会测量总输出功率并发送 SNMP 陷阱。

可能的值：

- ▶ 0..99（默认设置：90）

Send trap

如果设备检测到超过功率消耗的阈值，则会激活/停用 SNMP 陷阱的发送。

可能的值：

- ▶ 勾选
SNMP 陷阱发送激活。
如果模块功率消耗超过用户定义的阈值，则设备会发送 SNMP 陷阱。
- ▶ 未勾选（默认设置）
SNMP 陷阱发送停用。

发送 SNMP 陷阱的前提条件是，用户在 *Diagnostics > Status Configuration > Alarms (Traps)* 中启用该功能并至少指定一个陷阱目的地。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

1.8.2 PoE Port

[Basic Settings > Power over Ethernet > Port]

当功率消耗高于可提供的功率时，设备会根据优先级和端口编号停止向受电设备（PD）供电。当已连接的 PD 需要的功率高于设备提供的功率时，设备会停用端口上的 *Power over Ethernet* 功能。设备首先会禁用优先级最低的端口上的 *Power over Ethernet* 功能。当多个端口的优先级相同时，设备会首先禁用端口编号较高的端口上的 *Power over Ethernet* 功能。设备还会在指定的时间段内停止向受电设备（PD）供电。

表格

Port

显示端口编号。

PoE enable

激活/停用向端口提供的 PoE 功率。

激活或停用该功能后，设备会在日志文件（System Log）中记录事件。

可能的值：

- ▶ *勾选*（默认设置）
向端口提供 PoE 功率已激活。
- ▶ *未勾选*
向端口提供 PoE 功率已停用。

Fast startup

激活/停用端口上的以太网供电快速启动功能。

前提条件是已勾选 *PoE enable* 列中的复选框。

可能的值：

- ▶ *勾选*
快速启动功能已激活。在开始向设备供电之后，设备会立即向受电设备（PD）送电。
- ▶ *未勾选*（默认设置）
快速启动功能已停用。在加载自己的配置之后，设备会向受电设备（PD）供电。

Priority

指定端口优先级。

为帮助防止电流过载，设备会首先禁用低优先级端口。为帮助防止设备禁用为必要设备供电的端口，请为这些端口指定高优先级。

可能的值：

- ▶ *critical*
- ▶ *high*
- ▶ *low*（默认设置）

Status

显示端口受电设备 (PD) 检测的状态。

可能的值:

- ▶ *disabled*
设备处于“已禁用”状态，不会向受电设备供电。
- ▶ *deliveringPower*
设备识别出已连接的 PD 的类别，并且处于“通电”状态。
- ▶ *fault*
设备处于“测试错误”状态。
- ▶ *otherFault*
设备处于“空闲”状态。
- ▶ *searching*
设备处于列出的状态以外的状态。
- ▶ *test*
设备处于“测试模式”。

Detected class

显示已连接到端口的受电设备的功率类别。

可能的值:

- ▶ *Class 0*
- ▶ *Class 1*
- ▶ *Class 2*
- ▶ *Class 3*
- ▶ *Class 4*

Class 0
Class 1
Class 2
Class 3
Class 4

激活/停用端口上类别 0 至 4 的电流。

可能的值:

- ▶ 勾选 (默认设置)
- ▶ 未勾选

Consumption [W]

以瓦为单位显示端口的当前功率消耗。

可能的值:

▶ 0, 0..30, 0

Consumption [mA]

以毫安为单位显示向端口提供的电流。

可能的值:

▶ 0..600

Power limit [W]

以瓦为单位指定端口输出的最大功率。

此功能允许用户根据需要在 PoE 之间分配可用的功率预算。

例如，对于未提供“功率类别”的已连接设备，即使设备需要更小的功率，端口也会保留 15.4 W（类别 0）的固定功率。多余的功率不可用于任何其他端口。

通过指定功率限制，用户可将保留的功率减少到已连接设备的实际需求。未使用的功率可用于其他端口。

如果已连接受电设备的实际功率消耗未知，则设备会在 *Max. consumption [W]* 列中显示值。验证功率限制是否高于 *Max. consumption [W]* 列中的值。

如果最大观测功率高于设置的功率限制，则设备会将功率限制视为无效。在这种情况下，设备会将 PoE 类别用于计算。

可能的值:

▶ 0, 0..30, 0（默认设置：0）

Max. consumption [W]

以瓦为单位显示设备目前为止已消耗的最大功率。

当用户禁用端口上的 PoE 或终止已连接设备的连接时，会重置该值。

Name

指定端口的名称。

指定用户选择的名称。

可能的值:

- ▶ 带有 0..32 个字符的字母数字 ASCII 字符串

Auto-shutdown power

根据设置激活/停用 *Auto-shutdown power* 功能。

可能的值:

- ▶ 勾选
- ▶ 未勾选 (默认设置)

Disable power at [hh:mm]

指定设备在激活 *Auto-shutdown power* 功能时禁用端口功率的时间。

可能的值:

- ▶ 00:00..23:59 (默认设置: 00:00)

Re-enable power at [hh:mm]

指定设备在激活 *Auto-shutdown power* 功能时启用端口功率的时间。

可能的值:

- ▶ 00:00..23:59 (默认设置: 00:00)

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

1.9 Restart


[Basic Settings > Restart]

此对话框可用于重新启动设备、重置端口计数器和地址表以及删除日志文件。

Restart

Restart in

显示设备重新启动之前的剩余时间。

要更新剩余时间显示, 请点击  按钮。

Cancel

中止延迟重新启动。

Cold start...

打开 *Restart* 对话框，发起设备的立即或延迟重新启动。

如果非永久性存储器（*RAM*）中的配置概要文件与永久存储器（*NVM*）中的“选定”配置概要文件不同，则设备会显示 *Warning* 对话框。

- 要永久保存这些更改，请点击 *Warning* 对话框中的 *Yes* 按钮。
- 要丢弃这些更改，请点击 *Warning* 对话框中的 *No* 按钮。
- 在 *Restart in* 字段中，可以指定延迟重新启动的延迟时间。
可能的值：
 - 00:00:00..596:31:23（默认设置：00:00:00）

当延迟时间过去后，设备会重新启动并经历以下阶段：

- ▶ 如果用户在 *Diagnostics > System > Selftest* 对话框中激活该功能，则设备会进行一次 RAM 测试。
- ▶ 设备启动 *Basic Settings > Software* 对话框中 *Stored version* 字段显示的设备软件。
- ▶ 设备从“选定”配置概要文件加载设置。参见 *Basic Settings > Load/Save* 对话框。

提示：在重新启动期间，设备不传输任何数据。在此期间，图形用户界面或其他管理系统无法访问设备。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

Reset MAC address table

从转发表中删除在 *Switching > Filter for MAC Addresses* 对话框 *Status* 列中具有值 *learned* 的 MAC 地址。

Reset ARP table

从 ARP 表中删除动态设置的地址。

参见 *Diagnostics > System > ARP* 对话框。

Clear port statistics

将端口统计计数器重置为 0。

参见 *Basic Settings > Port* 对话框的 *Statistics* 选项卡。

Clear management access statistics

将设备管理访问上的统计计数器重置为 0。

参见 *Diagnostics > System > System Information* 对话框的 *Used Management Ports* 表格。

Reset IGMP snooping data

删除 IGMP 窥探条目并将 *Information* 框中的计数器重置为 0。

参见 *Switching > IGMP Snooping > Global* 对话框。

Delete log file

从日志文件中删除已记录的事件。

参见 *Diagnostics > Report > System Log* 对话框。

Delete persistent log file

从外部存储器中删除日志文件。

参见 *Diagnostics > Report > Persistent Logging* 对话框。

Clear email notification statistics

将 *Information* 框中的计数器重置为 0。

参见 *Diagnostics > Email Notification > Global* 对话框。

2 Time

该菜单包含以下对话框：

- ▶ Basic Settings
- ▶ SNTP
- ▶ PTP
- ▶ 802.1AS

2.1 Basic Settings

[Time > Basic Settings]

设备配有一个缓冲硬件时钟。如果电源无法运行或您断开设备与电源的连接，该时钟会保持正确的时间。设备启动之后，当前时间对于用户可用，例如，对于日志条目。

硬件时钟可覆盖的电源停机时间为 3 小时。前提条件是，设备电源之前已连续连接至少 5 分钟。

在此对话框中，可以独立于指定的时间同步协议指定与时间相关的设置。

该对话框包含以下选项卡：

- ▶ [Global]
- ▶ [Daylight saving time]

[Global]

在此选项卡中，可以指定设备中的系统时间和时区。

Configuration

System time (UTC)

显示参考协调世界时（UTC）的当前日期和时间。

Set time from PC

设备使用 PC 上的时间作为系统时间。

System time

显示参考本地时间的当前日期和时间： $System\ time = System\ time\ (UTC) + Local\ offset\ [min] + Daylight\ saving\ time$

Time source

显示设备从中获取时间信息的时间源。

设备自动选择精度最高的可用时间源。

可能的值:

- ▶ *local*
设备的系统时钟。
- ▶ *sntp*
SNTP 客户端激活, *SNTP* 服务器对设备进行同步。
- ▶ *ptp*
PTP 已激活, 设备的时钟已与 *PTP* 主时钟同步。

Local offset [min]

指定本地时间与 *System time (UTC)* 之间的时间差 (分钟): $Local\ offset\ [min] = System\ time - System\ time\ (UTC)$

可能的值:

- ▶ -780..840 (默认设置: 60)

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

[Daylight saving time]

在此选项卡中, 可以激活自动夏令时功能。可以使用预定义的概要文件指定夏季的开始和结束, 也可以分别指定这些设置。在夏季期间, 设备会将本地时间提前 1 小时。

Operation

Daylight saving time

启用/禁用 *Daylight saving time* 模式。

可能的值:

- ▶ *On*
Daylight saving time 模式已启用。
设备在夏季和冬季之间自动切换。
- ▶ *Off* (默认设置)
Daylight saving time 模式已禁用。

Summertime begin 框和 *Summertime end* 框中指定了设备在夏季和冬季之间切换的时间。

Profile...

显示 *Profile...* 对话框。在此可以为夏季开始和结束选择一个预定义概要文件。此概要文件可覆盖 *Summertime begin* 框和 *Summertime end* 框中的设置。

Summertime begin

在前三个字段中，可以指定夏季开始日期，在最后一个字段中，可以指定时间。

当 *System time* 字段中的时间达到此处输入的值时，设备会切换到夏季。

Week

指定当前月份中的星期。

可能的值：

- ▶ *none* (默认设置)
- ▶ *first*
- ▶ *second*
- ▶ *third*
- ▶ *fourth*
- ▶ *last*

Day

指定星期几。

可能的值：

- ▶ *none* (默认设置)
- ▶ *Sunday*
- ▶ *Monday*
- ▶ *Tuesday*
- ▶ *Wednesday*
- ▶ *Thursday*
- ▶ *Friday*
- ▶ *Saturday*

Month

指定月份。

可能的值：

- ▶ *none* (默认设置)
- ▶ *January*
- ▶ *February*
- ▶ *March*
- ▶ *April*
- ▶ *May*
- ▶ *June*
- ▶ *July*
- ▶ *August*
- ▶ *September*
- ▶ *October*

- ▶ *November*
- ▶ *December*

System time

指定时间。

可能的值:

- ▶ *<HH:MM>* (默认设置: 00:00)

Summertime end

在前三个字段中，可以指定夏季结束日期，在最后一个字段中，可以指定时间。

当 *System time* 字段中的时间达到此处输入的值时，设备会切换到冬季。

Week

指定当前月份中的星期。

可能的值:

- ▶ *none* (默认设置)
- ▶ *first*
- ▶ *second*
- ▶ *third*
- ▶ *fourth*
- ▶ *last*

Day

指定星期几。

可能的值:

- ▶ *none* (默认设置)
- ▶ *Sunday*
- ▶ *Monday*
- ▶ *Tuesday*
- ▶ *Wednesday*
- ▶ *Thursday*
- ▶ *Friday*
- ▶ *Saturday*

Month

指定月份。

可能的值：

- ▶ *none* (默认设置)
- ▶ *January*
- ▶ *February*
- ▶ *March*
- ▶ *April*
- ▶ *May*
- ▶ *June*
- ▶ *July*
- ▶ *August*
- ▶ *September*
- ▶ *October*
- ▶ *November*
- ▶ *December*

System time

指定时间。

可能的值：

- ▶ *<HH:MM>* (默认设置: 00:00)

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

2.2 SNTP

[Time > SNTP]

Simple Network Time Protocol (SNTP) 是一种 RFC 4330 中为网络中的时间同步规定的程序。

设备允许用户对作为 *SNTP* 客户端的设备中的系统时间进行同步。作为 *SNTP* 服务器，设备向其他设备提供时间信息。

该菜单包含以下对话框：

- ▶ *SNTP Client*
- ▶ *SNTP Server*

2.2.1 SNTP Client

[Time > SNTP > Client]

在此对话框中，可以指定设备作为 *SNTP* 客户端工作时使用的设置。

作为 *SNTP* 客户端，设备同时从 *SNTP* 服务器和 *NTP* 服务器获得时间信息，并使用时间服务器的时间对本地时钟进行同步。

Operation

Operation

启用/禁用设备的 *SNTP Client* 功能。

可能的值：

- ▶ *On*
SNTP Client 功能已启用。
设备作为 *SNTP* 客户端进行工作。
- ▶ *Off* (默认设置)
SNTP Client 功能已禁用。

Configuration

Mode

指定设备是从网络中已知且已配置的 *SNTP* 服务器主动请求时间信息（单播模式），还是被动等待来自一个随机 *SNTP* 服务器的时间信息（广播模式）。

可能的值：

- ▶ *unicast* (默认设置)
设备只从已配置的 *SNTP* 服务器获取时间信息。设备向 *SNTP* 服务器发送单播请求，并对其响应进行评估。
- ▶ *broadcast*
设备从一个或多个 *SNTP* 或 *NTP* 服务器获取时间信息。设备只对来自这些服务器的广播或多播进行评估。

Request interval [s]

指定设备从 *SNTP* 服务器请求时间信息的间隔（秒）。

可能的值：

- ▶ 5..3600（默认设置：30）

Broadcast rcv timeout [s]

指定当客户端没有接收到广播数据包时在该字段中的值从 *syncToRemoteServer* 变为 *notSynchronized* 之前处于广播客户端模式的客户端等待的时间（秒）。

可能的值：

- ▶ 128..2048（默认设置：320）

Disable client after successful sync

在设备成功同步时间之后激活/停用 *SNTP* 客户端的禁用。

可能的值：

- ▶ 勾选
SNTP 客户端的禁用已激活。
设备在时间同步成功后停用 *SNTP* 客户端。
- ▶ 未勾选（默认设置）
SNTP 客户端的禁用已停用。
时间同步成功后 *SNTP* 客户端保持活动状态。

State

State

显示 *SNTP* 客户端的状态。

可能的值：

- ▶ *disabled*
SNTP 客户端已禁用。
- ▶ *notSynchronized*
SNTP 客户端没有与任何 *SNTP* 或 *NTP* 服务器同步。
- ▶ *synchronizedToRemoteServer*
SNTP 客户端与 *SNTP* 或 *NTP* 服务器同步。

表格

在此表格中，可以为最多 4 个 *SNTP* 服务器指定设置。

Index

显示与表格条目相关的索引编号。

可能的值：

- ▶ 1..4

设备自动分配此数字。

删除一个表格条目后，会留下一个编号空缺。创建一个新的表格条目后，设备将填补第一个空缺。

启动后，设备向在第一个表格条目中配置的 *SNTP* 服务器发送请求。当服务器没有作出应答时，设备向在下一个表格条目中配置的 *SNTP* 服务器发送请求。

如果在此期间没有任何已配置的 *SNTP* 服务器作出响应，则 *SNTP* 客户端中断其同步。设备向每个 *SNTP* 服务器循环发送请求，直到某个服务器提供有效时间为止。即使以后能够再次访问其他服务器，设备本身仍然与此 *SNTP* 服务器进行同步。

Name

指定 *SNTP* 服务器的名称。

可能的值：

- ▶ 带有 1..32 个字符的字母数字 ASCII 字符串

Address

指定 *SNTP* 服务器的 IP 地址。

可能的值：

- ▶ 有效的 IPv4 地址（默认设置：0.0.0.0）
- ▶ 有效的 IPv6 地址
- ▶ 主机名

Destination UDP port

指定 *SNTP* 服务器希望通过其获得时间信息的 UDP 端口。

可能的值：

- ▶ 1..65535（默认设置：123）
例外：端口 2222 预留给内部功能。

Status

显示 *SNTP* 客户端和 *SNTP* 服务器之间的连接状态。

可能的值：

- ▶ *success*
设备已经成功与 *SNTP* 服务器实现时间同步。
- ▶ *badDateEncoded*
收到的时间信息包含协议错误 - 同步不成功。

- ▶ *other*
 - 为 *SNTP* 服务器的 IP 地址输入了值 0.0.0.0 - 同步失败。
或者
 - *SNTP* 客户端正在使用一个不同的 *SNTP* 服务器。
- ▶ *requestTimedOut*

设备没有收到来自 *SNTP* 服务器的应答 - 同步失败。
- ▶ *serverKissOfDeath*

SNTP 服务器过载。设备被请求与另一个 *SNTP* 服务器进行同步。当没有其他 *SNTP* 服务器可用时，如果服务器仍然过载，则设备以长于 *Request interval [s]* 字段中的设置的间隔进行检查。
- ▶ *serverUnsynchronized*

SNTP 服务器未与本地或外部参考时间源同步 - 同步不成功。
- ▶ *versionNotSupported*

SNTP 客户端和服务器上的版本相互不兼容 - 同步不成功。

Active

激活/停用至 *SNTP* 服务器的连接。

可能的值：

- ▶ 勾选
 - 至 *SNTP* 服务器的连接已激活。
 - SNTP* 客户端可以访问 *SNTP* 服务器。
- ▶ 未勾选（默认设置）
 - 至 *SNTP* 服务器的连接已停用。
 - SNTP* 客户端不能访问 *SNTP* 服务器。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

2.2.2 SNTP Server

[Time > SNTP > Server]

在此对话框中，可以指定设备作为 *SNTP* 服务器工作时使用的设置。

SNTP 服务器提供协调世界时 (UTC)，不考虑本地时差。

如果设置适当，则 *SNTP* 服务器在广播模式下工作。在广播模式下，*SNTP* 服务器会根据广播发送间隔自动发送广播消息或多播消息。

Operation

Operation

启用/禁用设备的 *SNTP Server* 功能。

可能的值：

- ▶ *On*
SNTP Server 功能已启用。
设备作为 *SNTP* 服务器进行工作。
- ▶ *Off* (默认设置)
SNTP Server 功能已禁用。

请注意 *Configuration* 框中 *Disable server at local time source* 复选框中的设置。

Configuration

UDP port

指定设备的 *SNTP* 服务器通过其接收来自其他客户端的请求的 UDP 端口的编号。

可能的值：

- ▶ 1..65535 (默认设置：123)
例外：端口 2222 预留给内部功能。

Broadcast admin mode

激活/停用广播模式。

- ▶ 勾选
SNTP 服务器在单播模式下对来自 *SNTP* 客户端的请求作出应答，并在广播模式下发送作为广播或多播的 *SNTP* 数据包。
- ▶ 未勾选 (默认设置)
SNTP 服务器在单播模式下对来自 *SNTP* 客户端的请求作出应答。

Broadcast destination address

指定设备的 *SNTP* 服务器在广播模式下向其发送 *SNTP* 数据包的 IP 地址。

可能的值：

- ▶ 有效的 IPv4 地址（默认设置：0.0.0.0）

允许广播和多播地址。

Broadcast UDP port

指定 *SNTP* 服务器在广播模式下通过其发送 *SNTP* 数据包的 UDP 端口的编号。

可能的值：

- ▶ 1..65535（默认设置：123）
例外：端口 2222 预留给内部功能。

Broadcast VLAN ID

指定设备的 *SNTP* 服务器在广播模式下在其中发送 *SNTP* 数据包的 VLAN 的 ID。

可能的值：

- ▶ 0
SNTP 服务器在可访问设备管理的同一个 VLAN 中发送 *SNTP* 数据包。参见 [Basic Settings > Network](#) 对话框。
- ▶ 1..4042（默认设置：1）

Broadcast send interval [s]

指定设备的 *SNTP* 服务器发送 *SNTP* 广播数据包的时间间隔。

可能的值：

- ▶ 64..1024（默认设置：128）

Disable server at local time source

当设备同步到本地时钟时激活/停用 *SNTP* 服务器的禁用。

可能的值：

- ▶ 勾选
SNTP 服务器的禁用已激活。
如果设备与本地时钟同步，则设备禁用 *SNTP* 服务器。*SNTP* 服务器继续对来自 *SNTP* 客户端的请求作出应答。在 *SNTP* 数据包中，*SNTP* 服务器通知客户端它已实现本地同步。
- ▶ 未勾选（默认设置）
SNTP 服务器的禁用已停用。
如果设备与本地时钟同步，则 *SNTP* 服务器保持活动状态。

State

State

显示 *SNTP* 服务器的状态。

可能的值：

- ▶ *disabled*
SNTP 服务器已禁用。
- ▶ *notSynchronized*
SNTP 服务器与本地或外部参考时间源未同步。
- ▶ *syncToLocal*
SNTP 服务器已与设备硬件时钟同步。
- ▶ *syncToRefclock*
SNTP 服务器已与外部参考时间源同步，例如 PTP。
- ▶ *syncToRemoteServer*
SNTP 服务器已与比级联中设备更高的一个 *SNTP* 服务器同步。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

2.3 PTP

[Time > PTP]

该菜单包含以下对话框：

- ▶ PTP Global
- ▶ PTP Boundary Clock
- ▶ PTP Transparent Clock

2.3.1 PTP Global

[Time > PTP > Global]

在此对话框中，可以指定 *PTP* 协议的基本设置。

Precision Time Protocol (PTP) 是 IEEE 1588-2008 标准中所述的程序，为网络中的设备提供精确的时间。该方法以数百 ns 的精度同步网络中的时钟。该协议使用多播通信，所以网络上因 *PTP* 同步消息而造成的负载可忽略不计。

PTP 的准确度显著高于 SNTP。如果同时在设备中启用了 *SNTP* 功能和 *PTP* 功能，则 *PTP* 功能拥有更高的优先级。

通过最佳主时钟算法，网络中的设备可以确定哪个设备具有最准确的时间。设备将具有最准确的时间的设备用作参考时间源 (*Grandmaster*)。随后，参与设备自行与参考时间源进行同步。

如果要通过网络准确地传输 PTP 时间，则在传输路径上仅使用具有 PTP 硬件支持的设备。

协议区分以下时钟：

▶ *Boundary Clock (BC)*

此时钟具有任意数量的 PTP 端口，并作为 *PTP* 主设备和 *PTP* 从设备进行工作。在其各自的网段中，时钟作为普通时钟运行。

- 作为 *PTP* 从设备，时钟自行与比级联中设备更高的 *PTP* 主设备同步。
- 作为 *PTP* 主设备，时钟通过网络将时间信息转发到比级联中设备更高的 *PTP* 从设备。

▶ *Transparent Clock (TC)*

此时钟具有任意数量的 PTP 端口。与 *Boundary Clock* 不同，此时钟会在转发时间信息之前纠正时间信息，而不会自行进行同步。

Operation IEEE1588/PTP

Operation IEEE1588/PTP

启用/禁用 *PTP* 功能。

在设备中，可以同时启用 *802.1AS* 功能或 *PTP* 功能。

可能的值：

▶ *On*

PTP 功能已启用。

设备与 PTP 同步其时钟。

如果同时在设备中启用了 *SNTP* 功能和 *PTP* 功能，则 *PTP* 功能拥有更高的优先级。

▶ *Off* (默认设置)

PTP 功能已禁用。

设备传输 *PTP* 同步消息，而不在每个端口上进行任何纠正。

Configuration IEEE1588/PTP

PTP mode

指定本地时钟的 PTP 版本和模式。

可能的值：

- ▶ *v2-transparent-clock* (默认设置)
- ▶ *v2-boundary-clock*

Sync lower bound [ns]

以纳秒为单位，指定本地时钟与参考时间源 (*Grandmaster*) 之间的路径差的阈值下限。如果路径差低于此值一次，则本地时钟被分类为已同步。

可能的值：

- ▶ 0..999999999 (默认设置：30)

Sync upper bound [ns]

以纳秒为单位，指定本地时钟与参考时间源 (*Grandmaster*) 之间的路径差的阈值上限。如果路径差超过此值一次，则本地时钟被分类为未同步。

可能的值：

- ▶ 31..1000000000 (默认设置：5000)

PTP management

激活/停用 PTP 标准中定义的 PTP 管理。

可能的值：

- ▶ 勾选
PTP 管理已激活。
- ▶ 未勾选 (默认设置)
PTP 管理已停用。

Status

Is synchronized

显示本地时钟是否与参考时间源 (*Grandmaster*) 同步。

如果本地时钟与参考时间源 (*Grandmaster*) 之间的路径差低于同步阈值下限一次，则本地时钟已同步。此状态保持到路径差超过同步阈值上限一次为止。

用户可在 *Configuration IEEE1588/PTP* 框中指定同步阈值。

Max. offset absolute [ns]

以纳秒为单位，显示自从本地时钟与参考时间源 (*Grandmaster*) 同步以来已发生的最大路径差。

PTP time

显示当本地时钟与参考时间源 (*Grandmaster*) 同步时的 PTP 时间刻度的日期和时间。格式：年月日上午/下午小时:分钟:秒钟

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

2.3.2 PTP Boundary Clock

[Time > PTP > Boundary Clock]

通过此菜单，用户可以为本地时钟配置边界时钟模式。

该菜单包含以下对话框：

- ▶ PTP Boundary Clock Global
- ▶ PTP Boundary Clock Port

2.3.2.1 PTP Boundary Clock Global

[Time > PTP > Boundary Clock > Global]

在此对话框中，为本地时钟的 *Boundary Clock* 模式输入通用跨端口设置。*Boundary Clock (BC)* 按照 PTP 版本 2 (IEEE1588-2008) 进行工作。

当本地时钟作为 *Boundary Clock (BC)* 进行工作时，这些设置有效。为此，在 *Time > PTP > Global* 对话框的 *PTP mode* 字段中选择值 *v2-boundary-clock*。

Operation IEEE1588/PTPv2 BC

Priority 1

为设置指定优先级 1。

可能的值：

▶ 0..255 (默认设置：128)

最佳主时钟算法首先在参与设备之间评估优先级 1，以便确定参考时间源 (*Grandmaster*)。

将此值设置得越低，设备成为参考时间源 (*Grandmaster*) 的可能性就越高。参见 *Grandmaster* 框。

Priority 2

为设备指定优先级 2。

可能的值：

▶ 0..255 (默认设置：128)

如果之前评估的条件对于多个设备都是相同的，则最佳主时钟算法会评估参与设备的优先级 2。

将此值设置得越低，设备成为参考时间源 (*Grandmaster*) 的可能性就越高。参见 *Grandmaster* 框。

Domain number

将设备分配到 *PTP* 域。

可能的值：

▶ 0..255 (默认设置：0)

设备仅在处于同一个域中的设备之间传输时间信息。

Status IEEE1588/PTPv2 BC

Two step

显示时钟正在双步模式下工作。

Steps removed

显示在设备的本地时钟与参考时间源 (*Grandmaster*) 之间通过的通信路径的数量。

对于 *PTP* 从设备, 值 1 表示时钟已通过 1 个通信路径直接与参考时间源 (*Grandmaster*) 连接。

Offset to master [ns]

以纳秒为单位, 显示在本地时钟与参考时间源 (*Grandmaster*) 之间测量的差值 (偏移量)。 *PTP* 从设备计算与收到的时间信息的差值。

在双步模式下, 每个时间信息包含由 *PTP* 主设备循环发送的 2 条 *PTP* 同步消息:

- ▶ 第一条同步消息 (同步消息) 包含消息的确切发送时间的估计值。
- ▶ 第二条同步消息 (后续消息) 包含第一条消息的确切发送时间。

PTP 从设备使用两条 *PTP* 同步消息来计算与主设备的差值 (偏移量), 并通过此差值来纠正其时钟。此处, *PTP* 从设备也考虑 *Delay to master [ns]* 值。

Delay to master [ns]

以纳秒为单位, 显示将 *PTP* 同步消息从 *PTP* 主设备传输到 *PTP* 从设备时的延迟。

PTP 从设备将“延迟请求”数据包发送到 *PTP* 主设备, 从而确定数据包的确切发送时间。收到数据包后, *PTP* 主设备生成时间戳并在“延迟响应”数据包中将此时间戳发回到 *PTP* 从设备。*PTP* 从设备使用两个数据包来计算延迟, 并从下一次偏移量测量开始考虑此延迟。

前提条件是将端口的延迟机制值指定为 *e2e*。

Grandmaster

此框显示最佳主时钟算法在评估参考时间源 (*Grandmaster*) 时使用的条件。

算法首先评估参与设备的优先级 1。优先级 1 值最低的设备被指定为参考时间源 (*Grandmaster*)。如果该值对于多个设备都是相同时的, 则算法采用下一个条件, 当此条件也相同时, 算法采用此条件之后的下一个条件。当多个设备的每个值都相同时, *Clock identity* 字段中的最低值决定将哪个设备指定为参考时间源 (*Grandmaster*)。

设备允许用户参与决定将网络中的哪个设备指定为参考时间源 (*Grandmaster*)。为此, 修改 *Operation IEEE1588/PTPv2 BC* 框中的 *Priority 1* 字段或 *Priority 2* 字段中的值。

Priority 1

显示当前作为参考时间源 (*Grandmaster*) 的设备的优先级 1。

Clock class

显示参考时间源 (*Grandmaster*) 的类别。最佳主时钟算法的参数。

Clock accuracy

显示参考时间源 (*Grandmaster*) 的估计精度。最佳主时钟算法的参数。

Clock variance

显示参考时间源 (*Grandmaster*) 的偏差, 也称为偏移量缩放日志偏差。最佳主时钟算法的参数。

Priority 2

显示当前作为参考时间源 (*Grandmaster*) 的设备的优先级 2。

Local time properties

Time source

指定本地时钟从中获取其时间信息的时间源。

可能的值:

- ▶ *atomicClock*
- ▶ *gps*
- ▶ *terrestrialRadio*
- ▶ *ptp*
- ▶ *ntp*
- ▶ *handSet*
- ▶ *other*
- ▶ *internalOscillator* (默认设置)

UTC offset [s]

指定 *PTP* 时间刻度与 UTC 之间的差值。

参见 *PTP timescale* 复选框。

可能的值:

- ▶ -32768..32767

提示: 默认设置是在设备软件的创建日期有效的值。可在地球自转和参考系服务 (IERS) 的“公告 C”中找到更多信息: <http://www.iers.org/IERS/EN/Publications/Bulletins/bulletins.html>

UTC offset valid

指定在 *UTC offset [s]* 字段中指定的值是否正确。

可能的值:

- ▶ 勾选
- ▶ 未勾选 (默认设置)

Time traceable

显示设备是否从原始 UTC 参考获取时间, 例如 NTP 服务器。

可能的值:

- ▶ 勾选
- ▶ 未勾选

Frequency traceable

显示设备是否从原始 UTC 参考获取频率，例如 NTP 服务器。

可能的值：

- ▶ 勾选
- ▶ 未勾选

PTP timescale

显示设备是否使用 PTP 时间刻度。

可能的值：

- ▶ 勾选
- ▶ 未勾选

按照 IEEE 1588 的规定，PTP 时间刻度是从 1970 年 1 月 1 日开始的 TAI 原子时间。

与 UTC 不同，TAI 不使用闰秒。

截至 2020 年 7 月 1 日，TAI 时间比 UTC 时间快 37 秒。

Identities

设备将标识显示为用十六进制表示的字节序列。

识别码 (UUID) 的组成如下：

- ▶ 设备识别码包含设备的 MAC 地址，在字节 3 和字节 4 之间添加值 `ff` 和 `fe`。
- ▶ 端口 UUID 包含设备识别码，后接 16 位端口 ID。

Clock identity

显示设备自己的识别码 (UUID)。

Parent port identity

显示直接上级主设备的端口识别码 (UUID)。

Grandmaster identity

显示参考时间源 (*Grandmaster*) 设备的识别码 (UUID)。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

2.3.2.2 PTP Boundary Clock Port

[Time > PTP > Boundary Clock > Port]

在此对话框中，可以指定每个端口上的 *Boundary Clock (BC)* 设置。

当本地时钟作为 *Boundary Clock (BC)* 进行工作时，这些设置有效。为此，在 *Time > PTP > Global* 对话框的 *PTP mode* 字段中选择值 *v2-boundary-clock*。

表格

Port

显示端口编号。

PTP enable

激活/停用端口上的 *PTP* 同步消息传输。

可能的值：

- ▶ *勾选*（默认设置）
传输已激活。端口转发和接收 *PTP* 同步消息。
- ▶ *未勾选*
传输已停用。端口会阻止 *PTP* 同步消息。

PTP status

显示端口的当前状态。

可能的值：

- ▶ *initializing*
初始化阶段
- ▶ *faulty*
故障模式：PTP 协议中出错。
- ▶ *disabled*
已在端口上禁用 PTP。
- ▶ *listening*
设备端口正在等待 *PTP* 同步消息。
- ▶ *pre-master*
PTP 预主模式
- ▶ *master*
PTP 主模式
- ▶ *passive*
PTP 被动模式
- ▶ *uncalibrated*
PTP 未校准模式
- ▶ *slave*
PTP 从模式

Sync interval

指定端口传输 *PTP* 同步消息的间隔（秒）。

可能的值：

- ▶ 0.25
- ▶ 0.5
- ▶ 1（默认设置）
- ▶ 2

Delay mechanism

指定设备用于测量传输 *PTP* 同步消息的延迟的机制。

可能的值：

- ▶ *disabled*
已连接的 *PTP* 设备的 *PTP* 同步消息延迟测量已停用。
- ▶ *e2e*（默认设置）
端到端：作为 *PTP* 从设备，端口会测量向 *PTP* 主设备传输的 *PTP* 同步消息的延迟。
设备在 *Time > PTP > Boundary Clock > Global* 对话框中显示测量值。
- ▶ *p2p*
点对点：设备会测量已连接的 *PTP* 设备的 *PTP* 同步消息的延迟，前提是这些设备支持 P2P。
在重新配置的情况下，此机制使设备不必再次确定延迟。

P2P delay

显示 *PTP* 同步消息的测量的点对点延迟。

前提条件是在 *Delay mechanism* 列中选择值 *p2p*。

P2P delay interval [s]

指定端口测量点对点延迟的间隔（秒）。

前提条件是已在此端口和远程设备的端口上指定值 *p2p*。

可能的值：

- ▶ 1（默认设置）
- ▶ 2
- ▶ 4
- ▶ 8
- ▶ 16
- ▶ 32

Network protocol

指定端口使用哪个协议传输 *PTP* 同步消息。

可能的值：

- ▶ *IEEE 802.3*（默认设置）
- ▶ *UDP/IPv4*

Announce interval [s]

指定端口传输 PTP 拓扑发现的消息的间隔（秒）。

为 PTP 域的每个设备分配相同的值。

可能的值：

- ▶ 1
- ▶ 2（默认设置）
- ▶ 4
- ▶ 8
- ▶ 16

Announce timeout

指定公告间隔的数量。

示例：

对于默认设置（*Announce interval [s]* = 2 和 *Announce timeout* = 3），超时为 $3 \times 2 \text{ s} = 6 \text{ s}$ 。

可能的值：

- ▶ 2..10（默认设置：3）
为 PTP 域的每个设备分配相同的值。

E2E delay interval [s]

显示端口测量端到端延迟的间隔（秒）：

- ▶ 当端口作为 PTP 主设备进行工作时，设备会为端口分配值 8。
- ▶ 当端口作为 PTP 从设备进行工作时，值由连接到端口的 PTP 主设备指定。

V1 hardware compatibility

指定当用户已在 *Network protocol* 列中设置值 *udpIpv4* 时，端口是否调整 PTP 同步消息的长度。

网络中的其他设备有可能预期 PTP 同步消息的长度与 PTPv1 消息相同。

可能的值：

- ▶ *auto*（默认设置）
设备自动检测网络中的其他设备是否预期 PTP 同步消息的长度与 PTPv1 消息相同。如果是这样，则设备会在传输 PTP 同步消息之前延伸其长度。
- ▶ *on*
设备在传输 PTP 同步消息之前延伸其长度。
- ▶ *off*
设备传输 PTP 同步消息而不更改其长度。

Asymmetry

纠正被非对称传输路径损坏的测量延迟值。

可能的值：

- ▶ -2000000000..2000000000（默认设置：0）

值代表延迟对称（纳秒）。

y ns 的测量延迟值对应于 $y \times 2$ ns 的非对称性。

如果从 *PTP* 主设备到 *PTP* 从设备的延迟高于相反方向的延迟，则值为正。

VLAN

指定设备用于标记此端口上的 *PTP* 同步消息的 VLAN ID。

可能的值：

- ▶ *none* (默认设置)
设备传输不带 VLAN 标签的 *PTP* 同步消息。
- ▶ 0..4042
用户从列表中指定已在设备中设置的 VLAN。

验证端口是否为 VLAN 的成员。

参见 *Switching > VLAN > Configuration* 对话框。

VLAN priority

指定设备用于传输标有 VLAN ID (第二层, IEEE 802.1D) 的 *PTP* 同步消息的优先级。

可能的值：

- ▶ 0..7 (默认设置: 6)

如果在 *VLAN* 列中指定值 *none*，则设备会忽略 VLAN 优先级。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

2.3.3 PTP Transparent Clock

[Time > PTP > Transparent Clock]

通过此菜单，用户可以为本地时钟配置 *Transparent Clock* 模式。

该菜单包含以下对话框：

- ▶ PTP Transparent Clock Global
- ▶ PTP Transparent Clock Port

2.3.3.1 PTP Transparent Clock Global

[Time > PTP > Transparent Clock > Global]

在此对话框中，为本地时钟的 *Transparent Clock* 模式输入通用跨端口设置。*Transparent Clock (TC)* 按照 PTP 版本 2 (IEEE1588-2008) 进行工作。

当本地时钟作为 *Transparent Clock (TC)* 进行工作时，这些设置有效。为此，在 *Time > PTP > Global* 对话框的 *PTP mode* 字段中选择值 *v2-transparent-clock*。

Operation IEEE1588/PTPv2 TC

Delay mechanism

指定设备用于测量传输 *PTP* 同步消息的延迟的机制。

可能的值：

▶ *e2e* (默认设置)

作为 *PTP* 从设备，端口会测量向 *PTP* 主设备传输的 *PTP* 同步消息的延迟。设备在 *Time > PTP > Transparent Clock > Global* 对话框中显示测量值。

▶ *p2p*

设备测量每个已连接 *PTP* 设备的 *PTP* 同步消息的延迟，前提是设备支持 P2P。在重新配置的情况下，此机制使设备不必再次确定延迟。如果指定此值，则值 *IEEE 802.3* 仅在 *Network protocol* 字段中可用。

▶ *e2e-optimized*

类似于 *e2e*，带有以下特殊字符：

- 设备仅将 *PTP* 从设备的延迟请求传输到 *PTP* 主设备，即使这些请求为多播消息也是如此。设备因此使其他设备无需处理不必要的多播请求。
- 如果主从拓扑发生变化，则设备在收到来自其他 *PTP* 主设备的同步消息时重新示教 *PTP* 主设备的端口。
- 如果设备不知道 *PTP* 主设备，则设备将延迟请求传输到端口。

▶ *disabled*

端口上的延迟测量已禁用。设备丢弃延迟测量的消息。

Primary domain

将设备分配到 *PTP* 域。

可能的值：

▶ *0..255* (默认设置：0)

设备仅在处于同一个域中的设备之间传输时间信息。

Network protocol

指定端口使用哪个协议传输 *PTP* 同步消息。

可能的值：

▶ *ieee8023* (默认设置)

▶ *udpIpv4*

Multi domain mode

激活/停用每个 *PTP* 域中的 *PTP* 同步消息纠正。

可能的值：

- ▶ **勾选**
设备纠正每个 *PTP* 域中的 *PTP* 同步消息。
- ▶ **未勾选**（默认设置）
设备仅纠正主 *PTP* 域中的 *PTP* 同步消息。参见 *Primary domain* 字段。

VLAN ID

指定设备用于标记此端口上的 *PTP* 同步消息的 VLAN ID。

可能的值：

- ▶ **none**（默认设置）
设备传输不带 VLAN 标签的 *PTP* 同步消息。
- ▶ **0..4042**
用户从列表中指定已在设备中设置的 VLAN。

VLAN priority

指定设备用于传输标有 VLAN ID（第二层，IEEE 802.1D）的 *PTP* 同步消息的优先级。

可能的值：

- ▶ **0..7**（默认设置：6）

如果在 *VLAN ID* 字段中指定了值 *none*，则设备会忽略指定的值。

Local synchronization

Syntonize

激活/停用 *Transparent Clock* 与 *PTP* 主设备的频率同步。

可能的值：

- ▶ **勾选**（默认设置）
频率同步已激活。
设备会同步频率。
- ▶ **未勾选**
频率同步已停用。
频率保持恒定。

Synchronize local clock

激活/停用本地系统时间的同步。

可能的值：

- ▶ **勾选**
同步已激活。
设备将本地系统时间与通过 PTP 收到的时间同步。前提是已勾选 *Syntonize* 复选框。
- ▶ **未勾选**（默认设置）
同步已停用。
本地系统时间保持恒定。

Current master

显示设备直接上级主设备的端口识别码（UUID），设备在该主设备上同步其频率。

如果值仅包含零，则是因为：

- ▶ *Syntonize* 功能已禁用。
或者
- ▶ 设备无法找到 *PTP* 主设备。

Offset to master [ns]

以纳秒为单位，显示在本地时钟与 *PTP* 主设备之间测量的差值（偏移量）。设备计算与收到的时间信息的差值。

前提是已启用 *Synchronize local clock* 功能。

Delay to master [ns]

以纳秒为单位，显示将 *PTP* 同步消息从 *PTP* 主设备传输到 *PTP* 从设备时的延迟。

前提条件：

- ▶ *Synchronize local clock* 功能已启用。
- ▶ 在 *Delay mechanism* 字段中，选中值 *e2e*。

Status IEEE1588/PTPv2 TC

Clock identity

显示设备自己的识别码（UUID）。

设备将标识显示为用十六进制表示的字节序列。

设备识别码包含设备的 MAC 地址，在字节 3 和字节 4 之间添加值 *ff* 和 *fe*。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

2.3.3.2 PTP Transparent Clock Port

[Time > PTP > Transparent Clock > Port]

在此对话框中，可以指定每个端口上的 *Transparent Clock (TC)* 设置。

当本地时钟作为 *Transparent Clock (TC)* 进行工作时，这些设置有效。为此，在 *Time > PTP > Global* 对话框的 *PTP mode* 字段中选择值 *v2-transparent-clock*。

表格

Port

显示端口编号。

PTP enable

激活/停用端口上的 *PTP* 同步消息传输。

可能的值：

- ▶ **勾选**（默认设置）
传输已激活。
端口转发和接收 *PTP* 同步消息。
- ▶ **未勾选**
传输已停用。
端口会阻止 *PTP* 同步消息。

P2P delay interval [s]

指定端口测量点对点延迟的间隔（秒）。

前提条件是在此端口和远程终端的端口上指定值 *p2p*。参见 *Time > PTP > Transparent Clock > Global* 对话框中的 *Delay mechanism* 选项列表。

可能的值：

- ▶ **1**（默认设置）
- ▶ 2
- ▶ 4
- ▶ 8
- ▶ 16
- ▶ 32

P2P delay

显示 *PTP* 同步消息的测量的点对点延迟。

前提条件是在 *Delay mechanism* 选项列表中选择 *p2p* 单选按钮。参见 *Time > PTP > Transparent Clock > Global* 对话框中的 *Delay mechanism* 字段。

Asymmetry

纠正被非对称传输路径损坏的测量延迟值。

可能的值：

▶ `-2000000000..2000000000`（默认设置：0）

值代表延迟对称（纳秒）。

y ns 的测量延迟值对应于 $y \times 2$ ns 的非对称性。

如果从 *PTP* 主设备到 *PTP* 从设备的延迟高于相反方向的延迟，则值为正。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

2.4 802.1AS

[Time > 802.1AS]

802.1AS 协议是 IEEE 802.1AS-2011 标准中所述的程序，用于定义如何在网络中的设备之间准确地同步时间。在以太网上使用 *802.1AS* 协议时，可将该协议视为 IEEE 1588-2008 标准的概要文件。

通过**最佳主时钟算法**，网络中的设备可以确定哪个设备具有最准确的时间。设备将具有最准确的时间的设备用作参考时间源（*Grandmaster*）。随后，参与设备自行与参考时间源进行同步。

802.1AS 协议具有以下规格：

- ▶ 在设备中，可以启用 *802.1AS* 功能或 *PTP* 功能。
- ▶ 如果同时在设备中启用了 *SNTP* 功能和 *802.1AS* 功能，则 *802.1AS* 功能拥有更高的优先级。
- ▶ *802.1AS* 功能仅支持一个域。

该菜单包含以下对话框：

- ▶ 802.1AS Global
- ▶ 802.1AS Port
- ▶ 802.1AS Statistics

2.4.1 802.1AS Global

[Time > 802.1AS > Global]

在此对话框中，可以指定 *802.1AS* 协议的基本设置。

Operation

Operation

启用/禁用 *802.1AS* 功能。

可能的值：

- ▶ *On*
802.1AS 功能已启用。
设备使用 *802.1AS* 协议来同步其时钟。
考虑在各个端口上激活 *802.1AS* 协议。
- ▶ *Off* (默认设置)
802.1AS 功能已禁用。

Configuration

Priority 1

为设置指定优先级 *1*。

可能的值：

- ▶ *0..255* (默认设置: *246*)

最佳主时钟算法首先在参与设备之间评估优先级 *1*，以便确定参考时间源 (*Grandmaster*)。

将此值设置得越低，设备被指定为参考时间源 (*Grandmaster*) 的可能性就越高。

如果指定值 *255*，则设备不会被指定为参考时间源 (*Grandmaster*)。参见 *Grandmaster* 框。

Priority 2

为设备指定优先级 *2*。

可能的值：

- ▶ *0..255* (默认设置: *248*)

如果之前评估的条件对于多个设备都是相同的，则最佳主时钟算法会评估参与设备的优先级 *2*。

将此值设置得越低，设备被指定为参考时间源 (*Grandmaster*) 的可能性就越高。参见 *Grandmaster* 框。

Sync lower bound [ns]

以纳秒为单位，指定本地时钟与参考时间源 (*Grandmaster*) 之间测量的时间差的阈值下限。如果测量的时间差低于此值一次，则本地时钟被分类为已同步。

可能的值：

- ▶ 0..999999999 (默认设置：30)

Sync upper bound [ns]

以纳秒为单位，指定本地时钟与参考时间源 (*Grandmaster*) 之间测量的时间差的阈值上限。如果测量的时间差超过此值一次，则本地时钟被分类为未同步。

可能的值：

- ▶ 31..1000000000 (默认设置：5000)

UTC offset [s]

显示 *802.1AS* 时间刻度与 UTC 之间的差值。

UTC offset valid

显示在 *UTC offset [s]* 字段中显示的值是否正确。

可能的值：

- ▶ 勾选
- ▶ 未勾选

Status

Offset to master [ns]

以纳秒为单位，显示在本地时钟与参考时间源 (*Grandmaster*) 之间测量的差值 (偏移量)。设备计算与收到的时间信息的差值。

Max. offset absolute [ns]

以纳秒为单位，显示自从本地时钟与参考时间源 (*Grandmaster*) 同步以来已发生的最大测量的时间差。

Is synchronized

显示本地时钟是否与参考时间源 (*Grandmaster*) 同步。

如果本地时钟与参考时间源 (*Grandmaster*) 之间测量的时间差低于同步阈值下限，则本地时钟已同步。此状态保持到测量的时间差超过同步阈值上限为止。

用户可在 *Configuration* 框中指定同步阈值。

Steps removed

显示在设备的本地时钟与参考时间源 (*Grandmaster*) 之间通过的通信路径的数量。

对于 *802.1AS* 从设备, 值 1 表示时钟已通过 1 个通信路径直接与参考时间源 (*Grandmaster*) 连接。

Clock identity

显示设备的时钟识别码。

设备将识别码显示为用十六进制表示的字节序列。

设备识别码包含设备的 MAC 地址, 在字节 3 和字节 4 之间添加值 *ff* 和 *fe*。

Grandmaster

此框显示最佳主时钟算法在评估参考时间源 (*Grandmaster*) 时使用的条件。

算法首先评估参与设备的优先级 1。优先级 1 值最低的设备被指定为参考时间源 (*Grandmaster*)。如果该值对于多个设备都是相同时的, 则算法采用下一个条件, 当此条件也相同时, 算法采用此条件之后的下一个条件。当多个设备的每个值都相同时, *Clock identity* 字段中的最低值决定将哪个设备指定为参考时间源 (*Grandmaster*)。

设备允许用户参与决定将网络中的哪个设备指定为参考时间源 (*Grandmaster*)。为此, 修改 *Configuration* 框中的 *Priority 1* 字段或 *Priority 2* 字段中的值。

Priority 1

显示当前作为参考时间源 (*Grandmaster*) 的设备的优先级 1。

Clock class

显示参考时间源 (*Grandmaster*) 的类别。最佳主时钟算法的参数。

Clock accuracy

显示参考时间源 (*Grandmaster*) 的估计精度。最佳主时钟算法的参数。

Clock variance

显示参考时间源 (*Grandmaster*) 的偏差, 也称为偏移量缩放日志偏差。最佳主时钟算法的参数。

Priority 2

显示当前作为参考时间源 (*Grandmaster*) 的设备的优先级 2。

Clock identity

显示参考时间源 (*Grandmaster*) 设备的识别码。设备将识别码显示为用十六进制表示的字节序列。

Parent

Clock identity

显示直接上级主设备的端口识别码。设备将识别码显示为用十六进制表示的字节序列。

Port

显示直接上级主设备的端口编号。

Cumulative rate ratio [ppm]

以百万分率显示本地时钟相对于参考时间源（*Grandmaster*）测量的频率差。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

2.4.2 802.1AS Port

[Time > 802.1AS > Port]

在此对话框中，可以指定每个端口上的 *802.1AS* 设置。

表格

Port

显示端口编号。

Active

激活/停用端口上的 *802.1AS* 协议。

可能的值：

- ▶ *勾选*（默认设置）
端口上的协议已激活。
在端口上，设备使用 *802.1AS* 协议来同步其时钟。
- ▶ *未勾选*
端口上的协议已停用。

Role

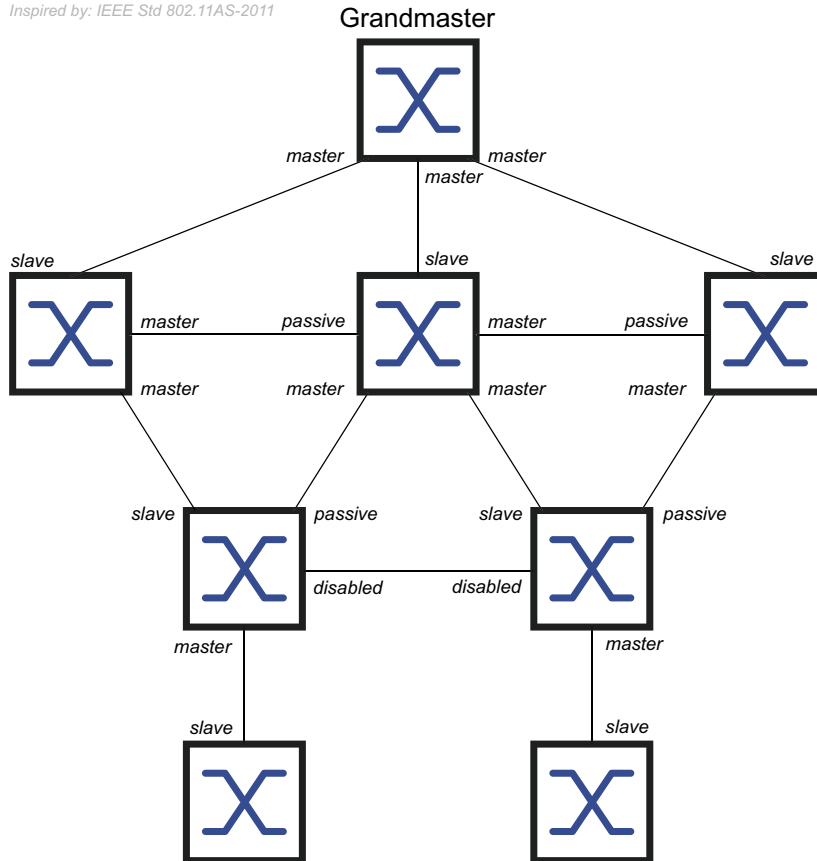
显示端口的当前角色，同时考虑 *802.1AS* 协议。

可能的值：

- ▶ *disabled*
端口以 *Disabled Port* 角色进行工作。端口不支持 *802.1AS*。
- ▶ *master*
端口以 *Master Port* 角色进行工作。

- ▶ *passive*
端口以*Passive Port*角色进行工作。
- ▶ *slave*
端口以*Slave Port*角色进行工作。

Inspired by: IEEE Std 802.11AS-2011



AS capable

显示端口上的 *802.11AS* 协议是否已激活。

可能的值：

- ▶ 勾选
端口上的 *802.11AS* 协议已激活。前提条件是：
 - 端口测量 *Peer delay*，已勾选 *Measuring delay* 列中的复选框。
 - *Peer delay [ns]* 列中的值低于 *Peer delay threshold [ns]* 列中的值。
- ▶ 未勾选
端口上的 *802.11AS* 协议已停用。

Announce interval [s]

指定端口（以*Master Port*角色）传输 *802.11AS* 拓扑发现的*Announce*消息的间隔（秒）。

可能的值：

- ▶ 1..2（默认设置：1）
为 *802.11AS* 域的每个设备分配相同的值。
- ▶ -
端口不传输*Announce*消息。

Announce timeout

指定端口（以*Slave Port*角色）等待*Announce*消息的 *Announce interval [s]* 的数量。

如果经过间隔数而未收到*Announce*消息，则设备会使用最佳主时钟算法尝试找到参考时间源的新路径。如果设备找到参考时间源（*Grandmaster*），则其会将*Slave Port*角色分配到新路径通向的端口。否则，设备将成为参考时间源（*Grandmaster*）并将*Master Port*角色分配到其端口。

示例：在默认设置下（*Announce interval [s]* = 1, *Announce timeout* = 3），超时为 $3 \times 1 \text{ s} = 3 \text{ s}$ 。

可能的值：

- ▶ 2..10（默认设置：3）
将相同的值分配到属于同一个 *802.1AS* 域 的每个端口。

Sync interval [s]

指定端口（以*Master Port*角色）传输时间同步的*Sync*消息的间隔（秒）。

可能的值：

- ▶ 0.125（默认设置）
- ▶ 0.250
- ▶ 0.5
- ▶ 1
- ▶ -
端口不传输*Sync*消息。

Sync timeout

指定端口（以*Slave Port*角色）等待*Sync*消息的 *Sync interval [s]* 的数量。

如果经过间隔数而未收到*Sync*消息，则设备会使用最佳主时钟算法尝试找到参考时间源的新路径。如果设备找到参考时间源（*Grandmaster*），则其会将*Slave Port*角色分配到新路径通向的端口。否则，设备将成为参考时间源（*Grandmaster*）并将*Master Port*角色分配到其端口。

示例：在默认设置下（*Sync interval [s]* = 0.125, *Sync timeout* = 3），超时为 $3 \times 0.125 \text{ s} = 0.375 \text{ s}$ 。

可能的值：

- ▶ 2..10（默认设置：3）
将相同的值分配到属于同一个 *802.1AS* 域 的每个端口。

Peer delay interval [s]

指定端口（以*Master Port*、*Passive Port*或*Slave Port*角色）传输*Peer delay request*消息以测量*Peer delay*的间隔（秒）。

可能的值：

- ▶ 1（默认设置）
- ▶ 2
- ▶ 4
- ▶ 8
- ▶ -
端口不传输*Peer delay request*消息。

Peer delay timeout

指定端口（以*Master Port*、*Passive Port*或*Slave Port*角色）等待*Delay response*消息的 *Peer delay interval [s]* 的数量。

如果经过间隔数而未收到*Delay response*消息，则设备会将*Disabled Port*角色分配到端口。端口不再支持 *802.1AS*。

可能的值：

- ▶ 2..10（默认设置：3）

Peer delay threshold [ns]

以纳秒为单位指定*Peer delay*的阈值上限。如果 *Peer delay [ns]* 列中的值大于此值，则设备会将*Disabled Port*角色分配到端口。端口不再支持 *802.1AS*。

可能的值：

- ▶ 0..1000000000（默认设置：10000）

Measuring delay

显示端口是否测量*Peer delay*。

可能的值：

- ▶ 勾选
端口测量*Peer delay*。可在 *Peer delay [ns]* 列中找到测量的值。
- ▶ 未勾选
端口不测量*Peer delay*。

Peer delay [ns]

以纳秒为单位显示测量的*Peer delay*值。前提条件是已勾选 *Measuring delay* 列中的复选框。

Neighbor rate ratio [ppm]

以百万分率为单位显示本地时钟相对于邻近设备中的时钟测量的频率差。

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

2.4.3 802.1AS Statistics

[Time > 802.1AS > Statistics]

此对话框显示关于在端口上接收、发送或丢弃的消息数量的信息。对话框还显示在每次发生超时事件时增加的计数器。

表格

Port

显示端口编号。

Received messages

显示在端口上接收的消息的计数器：

Sync messages

显示Sync消息的数量。

Sync follow-up messages

显示Sync *follow-up*消息的数量。

Delay request messages

显示Peer *delay request*消息的数量。

Delay response messages

显示Peer *delay response*消息的数量。

Delay response follow-up messages

显示Peer *delay response follow-up*消息的数量。

Announce messages

显示Announce消息的数量。

Discarded messages

显示设备在此端口上丢弃的Sync消息的数量。例如，如果端口未收到相应Sync消息的Sync *follow-up*消息，则设备会丢弃Sync消息。

Sync timeout

显示在端口上发生的 *Sync timeout* 事件的次数。参见 [Time > 802.1AS > Port](#) 对话框中的 *Sync timeout* 列。

Announce timeout

显示在此端口上发生的 *Announce timeout* 事件的次数。参见 *Time > 802.1AS > Port* 对话框中的 *Announce timeout* 列。

Delay timeout

显示在此端口上发生的 *Peer delay timeout* 事件的次数。参见 *Time > 802.1AS > Port* 对话框中的 *Peer delay timeout* 列。

Transmitted messages

显示在端口上传输的消息的计数器：

Sync messages

显示*Sync*消息的数量。

Sync follow-up messages

显示*Sync follow-up*消息的数量。

Delay request messages

显示*Peer delay request*消息的数量。

Delay response messages

显示*Peer delay response*消息的数量。

Delay response follow-up messages

显示*Peer delay response follow-up*消息的数量。

Announce messages

显示*Announce*消息的数量。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

3 Device Security

该菜单包含以下对话框：

- ▶ User Management
- ▶ Authentication List
- ▶ LDAP
- ▶ Management Access
- ▶ Pre-login Banner

3.1 User Management

[Device Security > User Management]

如果用户使用有效登录数据登录，则设备允许他们访问该设备的设备管理。

在此对话框中，可以管理本地用户管理的用户。在此还可以指定以下设置：

- ▶ 登录设置
- ▶ 密码保存设置
- ▶ 指定有效密码策略

设备针对用户在 *Device Security > Authentication List* 对话框中指定的身份验证所使用的方法。

Configuration

此框可用于指定登录设置。

Login attempts

指定用户使用图形用户界面和命令行界面访问设备管理时，可能的登录尝试次数。

提示： 当通过串行连接使用命令行界面来访问设备管理时，登录尝试的次数为无限。

可能的值：

- ▶ 0..5 (默认设置：0)

如果用户再进行一次不成功的登录尝试，则设备将锁定该用户的访问权限。

设备只允许具有 *administrator* 权限的用户解除锁定。

0 值会停用锁定。用户具有无限的登录尝试次数。

Login attempts period (min.)

显示设备重置 *Login attempts* 字段中的计数器之前的时间期限。

可能的值：

▶ 0..60（默认设置：0）

Min. password length

如果密码至少包含此处指定的字符数，则设备接受该密码。

无论 *Policy check* 复选框的设置如何，设备都会根据此设置检查密码。

可能的值：

▶ 1..64（默认设置：6）

Password policy

此框可用于指定有效密码策略。设备根据此策略检查每个新密码和每次密码更改。

这些设置会影响 *Password* 列。前提条件是用户勾选 *Policy check* 列中的复选框。

Upper-case characters (min.)

如果密码至少包含此处指定之多的大写字母，则设备接受该密码。

可能的值：

▶ 0..16（默认设置：1）

0 值会停用此设置。

Lower-case characters (min.)

如果密码至少包含此处指定之多的小写字母，则设备接受该密码。

可能的值：

▶ 0..16（默认设置：1）

0 值会停用此设置。

Digits (min.)

如果密码至少包含此处指定之多的数字，则设备接受该密码。

可能的值：

▶ 0..16（默认设置：1）

0 值会停用此设置。

Special characters (min.)

如果密码至少包含此处指定之多的特殊字符，则设备接受该密码。

可能的值：

▶ 0..16（默认设置：1）

0 值会停用此设置。


表格

每个用户都需要一个活动用户帐户来获得对设备管理的访问权限。表格可用于设置和管理用户帐户。

要更改设置，请点击表格中的所需参数并修改参数值。

User name

显示用户帐户的名称。

要创建新的用户帐户，请点击  按钮。

Active

激活/停用用户帐户。

可能的值：

▶ 勾选

用户帐户已激活。设备接受使用此用户名的用户的登录。

▶ 未勾选（默认设置）

用户帐户已停用。设备拒绝使用此用户名的用户的登录。

当存在一个具有 *administrator* 访问角色的用户帐户时，该用户帐户一直处于活动状态。

Password

指定用户使用图形用户界面或命令行界面访问设备管理时应用的密码。

显示 *********（若干星号），而非用户在登录时使用的密码。要更改密码，请点击相关字段。

首次指定密码时，设备在 *SNMP auth password* 和 *SNMP encryption password* 列中使用相同的密码。

- 设备允许用户在 *SNMP auth password* 和 *SNMP encryption password* 列中指定不同的密码。
- 如果用户更改当前列中的密码，则设备也会更改 *SNMP auth password* 和 *SNMP encryption password* 列的密码，但前提是之前未单独指定这些密码。

可能的值：

▶ 带有 6..64 个字符的字母数字 ASCII 字符串

允许以下字符：

- a..z
- A..Z
- 0..9
- !#\$%&'()*+,-./:;<=>?@[\\]^_`{|}~

在 *Configuration* 框中可以指定密码最小长度。设备区分大小写。

如果 *Policy check* 列中的复选框被勾选，则设备会根据 *Password policy* 框中指定的策略对密码进行检查。

即使 *Policy check* 列中的复选框未被勾选，设备仍会不断检查密码最小长度。

Role

指定管控用户对设备各种功能的访问权限的用户角色。

可能的值：

- ▶ *unauthorized*
用户被阻止，并且设备拒绝用户登录。
分配此值以临时锁定用户帐户。如果在分配另一个角色时设备检测到错误，则设备会将该角色分配给用户帐户。
- ▶ *guest*（默认设置）
该用户有权监视设备。
- ▶ *auditor*
用户有权对设备进行监控并在 *Diagnostics > Report > Audit Trail* 对话框中保存日志文件。
- ▶ *operator*
该用户有权监视设备和更改设置 - 针对设备访问的安全设置除外。
- ▶ *administrator*
该用户有权监视设备和更改设置。

设备按如下所示将 RADIUS 服务器的响应中传送的服务类型分配给用户角色：

- *Administrative-User*: *administrator*
- *Login-User*: *operator*
- *NAS-Prompt-User*: *guest*

User locked

解锁用户帐户。

可能的值：

- ▶ 勾选
用户帐户已锁定。该用户没有访问设备管理的权限。
如果用户进行太多不成功的登录尝试，则设备将自动锁定该用户。
- ▶ 未勾选（灰色）（默认设置）
用户帐户已解锁。该用户拥有设备管理的访问权限。

Policy check

激活/停用密码检查。

可能的值：

- ▶ 勾选
密码检查已激活。
当用户设置或更改密码时，设备会根据 *Password policy* 框中指定的策略对密码进行检查。
- ▶ 未勾选（默认设置）
密码检查已停用。

SNMP auth type

为通过 SNMPv3 的用户访问指定设备应用的身份验证协议。

可能的值：

- ▶ *hmacmd5* （默认值）
对于该用户帐户，设备使用 HMACMD5 协议。
- ▶ *hmacsha*
对于该用户帐户，设备使用 HMACSHA 协议。

SNMP auth password

为通过 SNMPv3 的用户访问指定设备应用的密码。

显示 *****（若干星号），而非用户在登录时使用的密码。要更改密码，请点击相关字段。

默认情况下，设备使用与用户在 *Password* 列中指定的相同的密码。

- 对于当前列，设备允许用户指定与 *Password* 列中不同的密码。
- 如果用户更改 *Password* 列中的密码，则设备也会更改当前列的密码，但前提是之前未单独指定该密码。

可能的值：

- ▶ 带有 6..64 个字符的字母数字 ASCII 字符串
允许以下字符：
 - a..z
 - A..Z
 - 0..9
 - !#\$%&'()*+,-./:;<=>?@[\\]^_`{|}~

SNMP encryption type

为通过 SNMPv3 的用户访问指定设备应用的加密协议。

可能的值：

- ▶ *none*
无加密。
- ▶ *des* （默认值）
DES 加密
- ▶ *aesCfb128*
AES128 加密

SNMP encryption password

为通过 SNMPv3 加密用户访问指定设备应用的密码。

显示 *****（若干星号），而非用户在登录时使用的密码。要更改密码，请点击相关字段。

默认情况下，设备使用与用户在 *Password* 列中指定的相同的密码。

- 对于当前列，设备允许用户指定与 *Password* 列中不同的密码。
- 如果用户更改 *Password* 列中的密码，则设备也会更改当前列的密码，但前提是之前未单独指定该密码。

可能的值:

- ▶ 带有 6..64 个字符的字母数字 ASCII 字符串
允许以下字符:
 - a..z
 - A..Z
 - 0..9
 - !#\$%&'()*+,-./:;<=>?@[\\]^_`{|}~

按钮

“按钮” 页 16一节中提供了标准按钮的描述。



打开 *Create* 窗口，向表格中添加一个新的条目。

- ▶ 在 *User name* 字段中，可以指定用户帐户的名称。
可能的值:
 - 带有 1..32 个字符的字母数字 ASCII 字符串

3.2 Authentication List

[Device Security > Authentication List]

在此对话框中，可以管理身份验证列表。在身份验证列表中，可以指定设备用于身份验证的方法。用户还可以选择将预定义应用程序分配给身份验证列表。

如果用户使用有效登录数据登录，则设备允许他们访问该设备的设备管理。设备使用以下方法对用户进行身份验证：

- ▶ 设备的用户管理
- ▶ LDAP
- ▶ RADIUS

借助 IEEE 802.1X 规定的基于端口的访问控制，如果相连终端设备使用有效登录数据进行登录，则设备允许其访问网络。设备使用以下方法对终端设备进行身份验证：

- ▶ RADIUS
- ▶ IAS（集成身份验证服务器）

默认设置下，提供以下身份验证列表：


- ▶ `defaultDot1x8021AuthList`
- ▶ `defaultLoginAuthList`
- ▶ `defaultV24AuthList`

表格

提示：如果表格中不包含列表，则只能通过设备的串行接口使用命令行界面来访问设备管理。在这种情况下，设备使用本地用户管理对用户进行身份验证。参见 [Device Security > User Management](#) 对话框。

Name

显示列表名称。

要创建新的列表，请点击  按钮。

可能的值：

- ▶ 带有 1..32 个字符的字母数字 ASCII 字符串

Policy 1
Policy 2
Policy 3
Policy 4
Policy 5

指定设备使用 *Dedicated applications* 列中指定的应用程序进行访问的身份验证策略。

设备为用户提供后退解决方案选项。为此，可以在每个策略字段中指定另一个策略。如果使用指定策略进行的身份验证不成功，则设备可以使用下一个策略，具体视每个策略中输入的值的顺序而定。

可能的值：

- ▶ *local*（默认设置）
设备使用本地用户管理对用户进行身份验证。参见 [Device Security > User Management](#) 对话框。不能将此值分配给身份验证列表 `defaultDot1x8021AuthList`。

▶ *radius*

设备使用网络中的 RADIUS 服务器对用户进行身份验证。可在 [Network Security > RADIUS > Authentication Server](#) 对话框中指定 RADIUS 服务器。

▶ *reject*

设备根据用户首先尝试哪种策略来接受或拒绝身份验证。以下列表包含了各种身份验证场景：

- 如果身份验证列表中的第一个策略是 *local*，并且设备接受用户的登录凭据，则设备会在不尝试其他策略的情况下让用户登录。
- 如果身份验证列表中的第一个策略是 *local*，并且设备拒绝用户的登录凭据，则设备会按指定的顺序尝试使用其他策略让用户登录。
- 如果身份验证列表中的第一个策略是 *radius* 或 *ldap*，并且设备拒绝登录，则登录会立即被拒绝，同时不尝试使用其他策略让用户登录。
如果 RADIUS 或 LDAP 服务器无响应，则设备会尝试使用下一个策略对用户进行身份验证。
- 如果身份验证列表中的第一个策略是 *reject*，则设备会在不尝试其他策略的情况下立即拒绝用户登录。
- 验证身份验证列表 `defaultV24AuthList` 至少包含一个与 *reject* 不同的策略。

▶ *ias*

设备使用集成身份验证服务器 (IAS) 对通过 802.1X 登录的终端设备进行身份验证。集成身份验证服务器在单独的数据库中管理登录数据。参见 [Network Security > 802.1X Port Authentication > Integrated Authentication Server](#) 对话框。


只能将此值分配给身份验证列表 `defaultDot1x8021AuthList`。

▶ *ldap*

设备使用保存在中心位置的身份验证数据和访问角色，对用户进行身份验证。可以在 [Network Security > LDAP > Configuration](#) 对话框中指定设备使用的 Active Directory 服务器。

Dedicated applications

显示专用应用程序。当用户使用相关应用程序访问设备时，设备会使用指定策略进行身份验证。

要将另一个应用程序分配给列表或删除分配，请点击  按钮，然后点击 [Allocate applications](#) 项目。设备允许用户将每个应用程序分配到一个列表。

Active

激活/停用列表。

可能的值：

▶ *勾选*

列表已激活。当用户使用相关应用程序访问设备时，设备会使用此列表中的策略。

▶ *未勾选* (默认设置)

列表已停用。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

Allocate applications

打开 *Allocate applications* 窗口。

- ▶ 左侧字段显示可以分配给突出显示的列表的应用程序。
- ▶ 右侧字段显示已经分配给突出显示的列表的应用程序。
- ▶ 按钮：
 - 将每个条目移动到右侧字段。
 - ➡ 将突出显示的条目从左侧字段移动到右侧字段。
 - ➠ 将突出显示的条目从右侧字段移动到左侧字段。
 - ◀ 将每个条目移动到左侧字段。

提示： 将条目 *WebInterface* 移动到左侧字段后，与设备的连接将在您点击 *Ok* 按钮后断开。

3.3 LDAP

[Device Security > LDAP]

Lightweight Directory Access Protocol (LDAP) 允许您在网络中的中心点对用户进行身份验证和授权。Active Directory 是可通过 LDAP 访问且广泛使用的目录服务[®]。

设备使用 LDAP 协议将用户的登录数据转发到身份验证服务器。该身份验证服务器决定登录数据是否有效，并将用户授权传输给设备。

在成功登录后，设备会在缓存中临时保存登录数据。这样可以在用户再次登录时加快登录过程。在这种情况下，无需进行复杂的 LDAP 搜索操作。

该菜单包含以下对话框：

- ▶ LDAP Configuration
- ▶ LDAP Role Mapping

3.3.1 LDAP Configuration

[Device Security > LDAP > Configuration]

此对话框允许用户指定最多 4 个身份验证服务器。当设备将登录数据转发给一个身份验证服务器时，该服务器会对用户进行身份验证和授权。

设备将登录数据发送到第一个身份验证服务器。当此服务器没有响应时，设备会与表格中的下一个服务器联系。

Operation

Operation

启用/禁用 *LDAP* 客户端。

如果在 *Device Security > Authentication List* 对话框的行 *Policy 1*到*Policy 5* 之一中指定值 *ldap*，则设备会使用 *LDAP* 客户端。在此之前，在 *Device Security > LDAP > Role Mapping* 对话框中为此角色 *administrator* 至少指定一个映射。这样可在通过 *LDAP* 登录之后，以管理员身份访问设备。

可能的值：

- ▶ *On*
LDAP 客户端已启用。
- ▶ *Off* (默认设置)
LDAP 客户端已禁用。

Configuration

Client cache timeout [min]

指定在成功登录之后用户的登录数据保持有效的分钟数。当用户在此时间内再次登录时，无需进行复杂的 *LDAP* 搜索操作。登录过程显著加快。

可能的值：

- ▶ *1..1440* (默认设置: 10)

Bind user

以“可分辨名称”(DN)形式指定设备用于登录 *LDAP* 服务器的用户 ID。

如果 *LDAP* 服务器要求将“可分辨名称”(DN)形式的用户 ID 用于登录，则需要此信息。在 *Active Directory* 环境中，不需要此信息。

设备通过用户 ID 登录 *LDAP* 服务器以查找登录用户的“可分辨名称”(DN)。设备根据 *Base DN* 和 *User name attribute* 字段中的设置进行搜索。

可能的值:

- ▶ 带有 0..64 个字符的字母数字 ASCII 字符串

Bind user password

指定设备在登录 LDAP 服务器时与在 *Bind user* 字段中指定的用户 ID 一起使用的密码。

可能的值:

- ▶ 带有 0..64 个字符的字母数字 ASCII 字符串

Base DN

以“可分辨名称”(DN)形式指定在目录树中进行搜索的起点。

可能的值:

- ▶ 带有 0..255 个字符的字母数字 ASCII 字符串

User name attribute

指定包含一对一用户名的 LDAP 属性。之后,用户使用此属性中包含的用户名登录。

LDAP 属性 *userPrincipalName*、*mail*、*sAMAccountName* 和 *uid* 通常包含唯一用户名。

在以下条件下,设备将在 *Default domain* 字段中指定的字符串添加到用户名:

- 属性中包含的用户名不包含 @ 字符。
- 在 *Default domain* 字段中指定了域名。

可能的值:

- ▶ 带有 0..64 个字符的字母数字 ASCII 字符串
(默认设置: *userPrincipalName*)

Default domain

指定当用户名不包含 @ 字符时设备添加到登录用户的用户名的字符串。

可能的值:

- ▶ 带有 0..64 个字符的字母数字 ASCII 字符串

CA certificate

URL

指定证书的路径和文件名。


设备接受具有以下属性的证书:

- X.509 格式
- .PEM 文件扩展名
- Base64 编码,括在
-----BEGIN CERTIFICATE-----
和
-----END CERTIFICATE-----

出于安全原因，我们建议持续使用由认证机构签名的证书。

设备为用户提供将证书复制到设备的以下选项：

▶ 从 PC 导入

当证书位于用户 PC 中或网络驱动器上时，将该证书拖放到  区域中。也可点击该区域内部选择该证书。

▶ 从 FTP 服务器导入

当该证书位于 FTP 服务器上时，以如下形式指定该文件的 URL：
ftp://<???:<??>@<IP ???:<??>/<??>/<??>>

▶ 从 TFTP 服务器导入

当该证书位于 TFTP 服务器上时，以如下形式指定该文件的 URL：
tftp://<IP ??>/<??>/<??>>

▶ 从 SCP 或 SFTP 服务器导入

当该证书位于 SCP 或 SFTP 服务器上时，以如下形式指定该文件的 URL：

- scp:// 或 sftp://<IP ??>/<??>/<??>>

点击 *Start* 按钮后，设备会显示 *Credentials* 窗口。在该处输入 *User name* 和 *Password* 以登录服务器。

- scp:// 或 sftp://<???:<??>@<IP ??>/<??>/<??>>

Start

将 *URL* 字段中指定的证书复制到设备。

表格

Index

显示与表格条目相关的索引编号。

Description

指定描述。

用户可以选择在此处描述身份验证服务器或备注其他信息。

可能的值：

- ▶ 带有 0..255 个字符的字母数字 ASCII 字符串

Address

指定服务器的 IP 地址或 DNS 名称。

可能的值：

- ▶ IPv4 地址（默认设置：0.0.0.0）

- ▶ IPv6 地址

- ▶ <domain>.<tld> 或 <host>.<domain>.<tld> 格式的 DNS 名称

- ▶ _ldap._tcp.<domain>.<tld>

使用 DNS 名称，设备从 DNS 服务器查询 LDAP 服务器列表（SRV 资源记录）。

如果在 *Connection security* 行中指定了 *none* 以外的值，并且证书仅包含服务器的 DNS 名称，则使用 DNS 名称。在 *Advanced > DNS > Client > Global* 对话框中启用 *Client* 功能。

Destination TCP port

指定服务器预期在其上收到请求的 TCP 端口。

如果已在 *Address* 列中指定值 `_ldap._tcp.domain.tld`，则设备会忽略此值。

可能的值：

- ▶ `0..65535`（默认设置：389）
例外：端口 2222 预留给内部功能。

常用的 TCP 端口：

- LDAP： 389
- LDAP over SSL： 636
- Active Directory Global Catalogue： 3268
- Active Directory Global Catalogue SSL： 3269

Connection security

指定对设备与身份验证服务器之间的通信进行加密的协议。

可能的值：

- ▶ `none`
无加密。
设备与服务器建立 LDAP 连接，并以明文方式传输包括密码在内的通信。
- ▶ `ssl`
使用 SSL 进行加密。
设备与服务器建立 TLS 连接，并通过该连接用隧道传输 LDAP 通信。
- ▶ `startTLS`（默认设置）
使用 startTLS 扩展进行加密。
设备与服务器建立 LDAP 连接并对通信进行加密。

加密通信的前提条件是设备使用正确的时间。如果证书仅包含 DNS 名称，则可以在 *Address* 行中指定服务器的 DNS 名称。在 *Advanced > DNS > Client > Global* 对话框中启用 *Client* 功能。

如果证书在“使用者可选名称”字段中包含服务器的 IP 地址，则设备能够在无需 DNS 配置的情况下验证服务器的身份。

Server status

显示与身份验证服务器的连接状态和身份验证。

可能的值：

- ▶ `ok`
服务器可访问。
如果在 *Connection security* 行中指定了 `none` 以外的值，则设备已验证服务器的证书。
- ▶ `unreachable`
服务器不可访问。
- ▶ `other`
设备尚未与服务器建立连接。

Active

激活/停用服务器的使用。

可能的值：

- ▶ **勾选**
设备使用服务器。
- ▶ **未勾选**（默认设置）
设备不使用服务器。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

Flush cache

删除已成功登录的用户的缓存登录数据。

3.3.2 LDAP Role Mapping

[Device Security > LDAP > Role Mapping]

此对话框允许用户创建最多 64 个映射，以便将角色分配到用户。

在表格中指定设备是否根据具有特定值的属性还是根据组成员资格将角色分配到用户。

- ▶ 设备在用户对象中搜索属性和属性值。
- ▶ 通过评估成员属性中包含的“可分辨名称” (DN)，设备可在组中检查成员资格。

在用户登录后，设备会在 LDAP 服务器上搜索以下信息：

- ▶ 在相关的用户项目中，设备会搜索在映射中指定的属性。
- ▶ 在映射中指定的组的组对象中，设备会搜索成员属性。

在此基础上，设备会对任何映射进行检查。

- 用户对象是否包含所需的属性？
或者
- 用户是否为组的成员？

如果设备未找到匹配项，则用户未获得设备的访问权限。

如果设备找到多个适用于用户的映射，则由 *Matching policy* 字段中的设置决定。用户要么获得具有更广泛的授权的角色，要么获得表格中适用的第一个角色。

Configuration

Matching policy

指定当多个映射适用于用户时设备应用的角色。

可能的值：

- ▶ *highest* (默认设置)
设备应用具有更广泛的授权的角色。
- ▶ *first*
设备将 *Index* 列中值更小的规则应用于用户。

表格

Index

显示与表格条目相关的索引编号。

Role

指定管控用户对设备各种功能的访问权限的用户角色。

可能的值：

- ▶ *unauthorized*
用户被阻止，并且设备拒绝用户登录。
分配此值以临时锁定用户帐户。如果在分配另一个角色时检测到错误，则设备会将此角色分配给用户帐户。

- ▶ *guest* (默认设置)
该用户有权监视设备。
- ▶ *auditor*
用户有权对设备进行监控并在 *Diagnostics > Report > Audit Trail* 对话框中保存日志文件。
- ▶ *operator*
该用户有权监视设备和更改设置 - 针对设备访问的安全设置除外。
- ▶ *administrator*
该用户有权监视设备和更改设置。

Type

指定是否在 *Parameter* 列中设置组或具有属性值的属性。

可能的值:

- ▶ *attribute* (默认设置)
Parameter 列包含具有属性值的属性。
- ▶ *group*
Parameter 列包含组的“可分辨名称”(DN)。

Parameter

指定组或具有属性值的属性，具体取决于 *Type* 列中的设置。

可能的值:

- ▶ 带有 0..255 个字符的字母数字 ASCII 字符串
设备区分大小写。
 - 如果在 *Type* 列中指定了值 *attribute*，则以 *Attribute_name=Attribute_value* 形式指定属性。
示例: *l=Germany*
 - 如果在 *Type* 列中指定了值 *group*，则指定组的“可分辨名称”(DN)。
示例: *CN=admin-users,OU=Groups,DC=example,DC=com*

Active

激活/停用角色映射。

可能的值:

- ▶ *勾选* (默认设置)
角色映射已激活。
- ▶ *未勾选*
角色映射已停用。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。



打开 *Create* 窗口，向表格中添加一个新的条目。

- ▶ 在 *Index* 字段中，可以指定索引编号。

可能的值:

- 1..64

3.4 Management Access

[Device Security > Management Access]

该菜单包含以下对话框：

- ▶ Server
- ▶ IP Access Restriction
- ▶ Web
- ▶ Command Line Interface
- ▶ SNMPv1/v2 Community

3.4.1 Server

[Device Security > Management Access > Server]

此对话框可用于设置允许用户或应用程序访问设备管理的服务器服务。

该对话框包含以下选项卡：

- ▶ [Information]
- ▶ [SNMP]
- ▶ [Telnet]
- ▶ [SSH]
- ▶ [HTTP]
- ▶ [HTTPS]

[Information]

此选项卡以概览形式显示启用了哪些服务器服务。

表格

SNMPv1

显示服务器服务是已激活还是已停用，该服务授权使用 SNMP 版本 1 访问设备。参见 [SNMP](#) 选项卡。

可能的值：

- ▶ [勾选](#)
服务器服务已激活。
- ▶ [未勾选](#)
服务器服务已停用。

SNMPv2

显示服务器服务是已激活还是已停用，该服务授权使用 SNMP 版本 2 访问设备。参见 [SNMP](#) 选项卡。

可能的值：

- ▶ [勾选](#)
服务器服务已激活。
- ▶ [未勾选](#)
服务器服务已停用。

SNMPv3

显示服务器服务是已激活还是已停用，该服务授权使用 SNMP 版本 3 访问设备。参见 *SNMP* 选项卡。

可能的值：

- ▶ **勾选**
服务器服务已激活。
- ▶ **未勾选**
服务器服务已停用。

Telnet server

显示服务器服务是已激活还是已停用，该服务授权使用 Telnet 访问设备。参见 *Telnet* 选项卡。

可能的值：

- ▶ **勾选**
服务器服务已激活。
- ▶ **未勾选**
服务器服务已停用。

SSH server

显示服务器服务是已激活还是已停用，该服务授权使用 Secure Shell 访问设备。参见 *SSH* 选项卡。

可能的值：

- ▶ **勾选**
服务器服务已激活。
- ▶ **未勾选**
服务器服务已停用。

HTTP server

显示服务器服务是已激活还是已停用，该服务授权通过 HTTP 使用图形用户界面访问设备。参见 *HTTP* 选项卡。

可能的值：

- ▶ **勾选**
服务器服务已激活。
- ▶ **未勾选**
服务器服务已停用。

HTTPS server

显示服务器服务是已激活还是已停用，该服务授权通过 HTTPS 使用图形用户界面访问设备。参见 *HTTPS* 选项卡。

可能的值：

- ▶ **勾选**
服务器服务已激活。
- ▶ **未勾选**
服务器服务已停用。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

[SNMP]

此选项卡可用于为设备的 SNMP 代理指定设置以及启用/禁用使用不同 SNMP 版本进行设备访问。SNMP 代理允许使用基于 SNMP 的应用程序访问设备管理。

Configuration

SNMPv1

激活/停用使用 SNMP 版本 1 进行设备访问。

可能的值:

- ▶ 勾选 (默认设置)
访问已激活。
- ▶ 未勾选
访问已停用。

可在 *Device Security > Management Access > SNMPv1/v2 Community* 对话框中指定团体名称。

SNMPv2

激活/停用使用 SNMP 版本 2 进行设备访问。

可能的值:

- ▶ 勾选 (默认设置)
访问已激活。
- ▶ 未勾选
访问已停用。

可在 *Device Security > Management Access > SNMPv1/v2 Community* 对话框中指定团体名称。

SNMPv3

激活/停用使用 SNMP 版本 3 进行设备访问。

可能的值:

- ▶ 勾选 (默认设置)
访问已激活。
- ▶ 未勾选
访问已停用。

像 *ConneXium Network Manager* 这样的网络管理系统使用此协议与设备通信。


UDP port

指定 SNMP 代理通过其接收来自客户端的请求的 UDP 端口的编号。

可能的值：

- ▶ 1..65535（默认设置：161）
例外：端口 2222 预留给内部功能。

要使 SNMP 代理能够在更改后使用新端口，请按照以下步骤操作：

- 点击 按钮。
- 在 *Basic Settings* > *Load/Save* 对话框中选择活动的配置概要文件。
- 点击  按钮保存当前更改。
- 重新启动设备。

SNMPover802

激活/停用通过 IEEE-802 上的 SNMP 进行设备访问。

可能的值：

- ▶ 勾选
访问已激活。
- ▶ 未勾选（默认设置）
访问已停用。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

[Telnet]

此选项卡可用于启用/禁用设备中的 Telnet 服务器并指定其设置。

Telnet 服务器允许用户通过命令行界面远程访问设备管理。Telnet 连接不加密。

Operation

Telnet server

启用/禁用 Telnet 服务器。

可能的值：

- ▶ Telnet 服务器已启用。
可以使用不加密的 Telnet 连接通过命令行界面远程访问设备管理。
- ▶ Telnet 服务器已禁用。

提示：如果 SSH 服务器已禁用，并且用户同时禁用了 Telnet 服务，则仅可通过设备的串行接口访问命令行界面。

Configuration

TCP port

指定设备通过其接收来自客户端的 Telnet 请求的 TCP 端口编号。

可能的值：

- ▶ 1..65535（默认设置：23）
例外：端口 2222 预留给内部功能。

更改端口后，服务器会自动重新启动。现有连接保持不变。

Connections

显示当前与设备建立了多少个 Telnet 连接。

Connections (max.)

指定可以同时设置的至设备的 Telnet 连接最大数目。

可能的值：

- ▶ 1..5（默认设置：5）

Session timeout [min]

指定超时时间（分钟）。当设备在此时间内处于非活动状态之后，它会终止已登录用户的会话。

值的更改会在用户下次登录时生效。

可能的值：

- ▶ 0
停用此功能。在不活动的情况下，连接保持建立状态。
- ▶ 1..160（默认设置：5）

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

[SSH]

此选项卡可用于启用/禁用设备中的 SSH 服务器并指定 SSH 所需的设置。服务器支持 SSH 版本 2。

SSH 服务器允许用户通过命令行界面远程访问设备管理。SSH 连接会加密。

SSH 服务器使用其公共 RSA 密钥向客户端表明自己的身份。首次设置连接时，客户端程序会向用户显示此密钥的指纹。指纹包含一个很容易检查的 Base64 编码字符序列。通过可靠渠道向用户提供此字符序列时，他们可以选择对这两个指纹进行比较。如果这两个字符序列相互匹配，则客户端会连接到正确的服务器。

设备允许用户在设备中为 RSA 直接创建所需的私有和公共密钥（主机密钥）。否则，用户可以选择以 PEM 格式将自己的密钥复制到设备。

此外，设备还允许用户在重新启动时从外部存储器加载 RSA 密钥（主机密钥）。可在 *Basic Settings > External Memory* 对话框 *SSH key auto upload* 列中激活此功能。

Operation

SSH server

启用/禁用 SSH 服务器。

可能的值：

▶ *On*（默认设置）

SSH 服务器已启用。

可以使用加密 SSH 连接通过命令行界面访问设备管理。

只有当设备中存在 RSA 签名时才能启动服务器。

▶ *Off*

SSH 服务器已禁用。

禁用 SSH 服务器后，现有连接会保持建立状态。但是，设备有助于防止新连接的建立。

提示：如果 *Telnet* 服务器已禁用，并且用户同时禁用了 *SSH* 服务，则仅可通过设备的串行接口访问命令行界面。

Configuration

TCP port

指定设备通过其接收来自客户端的 SSH 请求的 TCP 端口编号。

可能的值：

▶ 1..65535（默认设置：22）

例外：端口 2222 预留给内部功能。

更改端口后，服务器会自动重新启动。现有连接保持不变。

Sessions

显示当前与设备建立了多少个 SSH 连接。

Sessions (max.)

指定可以同时设置的至设备的 SSH 连接最大数目。

可能的值:

- ▶ 1..5 (默认设置: 5)

Session timeout [min]

指定超时时间 (分钟)。当已登录用户在此时间内处于非活动状态之后, 设备会终止连接。

值的更改会在用户下次登录时生效。

可能的值:

- ▶ 0
停用此功能。在不活动的情况下, 连接保持建立状态。
- ▶ 1..160 (默认设置: 5)

Fingerprint

指纹是一个易于验证的字符串, 可唯一标识 SSH 服务器的主机密钥。

导入一个新的主机密钥之后, 设备会继续显示现有指纹, 直到用户重新启动服务器为止。

Fingerprint type


指定 *RSA fingerprint* 字段显示哪个指纹。

可能的值:

- ▶ *md5*
RSA fingerprint 字段将指纹显示为十六进制 MD5 哈希。
- ▶ *sha256*
RSA fingerprint 字段将指纹显示为 Base64 编码的 SHA256 哈希。

RSA fingerprint

显示 SSH 服务器的公共主机密钥的指纹。

更改 *Fingerprint type* 字段中的设置时, 之后点击 按钮, 然后点击  按钮, 以更新显示。

Signature

RSA present

显示设备中是否存在 RSA 主机密钥。

可能的值:

- ▶ 勾选
存在密钥。
- ▶ 未勾选
不存在密钥。

Start

将 *URL* 字段中指定的密钥复制到设备。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

[HTTP]

此选项卡可用于为网络服务器启用/禁用 HTTP 协议并指定 HTTP 所需的设置。

网络服务器通过未加密 HTTP 连接提供图形用户界面。出于安全原因，请禁用 HTTP 协议，改为使用 HTTPS 协议。

设备支持多达 10 个使用 HTTP 或 HTTPS 的同时连接。

提示：如果更改此选项卡中的设置并点击 按钮，则设备会结束会话并断开每个打开的连接。若要继续使用图形用户界面，请重新登录。

Operation

HTTP server

为网络服务器启用/禁用 *HTTP* 协议。

可能的值：

- ▶ *On* (默认设置)
HTTP 协议已启用。
可以通过不加密的 *HTTP* 连接访问设备管理。
当 *HTTPS* 协议也已启用时，设备会自动将对 *HTTP* 连接的请求重定向至一个加密的 *HTTPS* 连接。
- ▶ *Off*
HTTP 协议已禁用。
当 *HTTPS* 协议启用时，可以通过加密的 *HTTPS* 连接访问设备管理。

提示：如果 *HTTP* 和 *HTTPS* 协议都已禁用，则可使用 `http server` 命令行界面命令启用 *HTTP* 协议，以获取图形用户界面。

Configuration

TCP port

指定网络服务器通过其接收来自客户端的 HTTP 请求的 TCP 端口编号。

可能的值：

- ▶ 1..65535 (默认设置：80)
例外：端口 2222 预留给内部功能。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

[HTTPS]

此选项卡可用于为网络服务器启用/禁用 HTTPS 协议并指定 HTTPS 所需的设置。

网络服务器通过加密的 HTTP 连接提供图形用户界面。

HTTP 连接加密需要数字证书。设备允许用户自行创建此证书或将现有证书加载到设备上。

设备支持多达 10 个使用 HTTP 或 HTTPS 的同时连接。

提示：如果更改此选项卡中的设置并点击 按钮，则设备会结束会话并断开每个打开的连接。若要继续使用图形用户界面，请重新登录。

Operation

HTTPS server

为网络服务器启用/禁用 HTTPS 协议。

可能的值：

- ▶ *On* (默认设置)
HTTPS 协议已启用。
可以通过加密的 HTTPS 连接访问设备管理。
当不存在数字证书时，设备会在启用 HTTPS 协议之前生成一个数字证书。
- ▶ *Off*
HTTPS 协议已禁用。
当 HTTP 协议启用时，可以通过不加密的 HTTP 连接访问设备管理。

提示：如果 HTTP 和 HTTPS 协议都已禁用，则可使用 `https server` 命令行界面命令启用 HTTPS 协议，以获取图形用户界面。

Configuration

TCP port

指定网络服务器通过其接收来自客户端的 HTTPS 请求的 TCP 端口编号。

可能的值：

- ▶ *1..65535* (默认设置: 443)
例外：端口 2222 预留给内部功能。

Fingerprint

指纹是一个易于验证的十六进制数字序列，可唯一标识 HTTPS 服务器的数字证书。

导入一个新的数字证书后，设备会显示当前指纹，直到用户重新启动服务器为止。

Fingerprint type


指定 *Fingerprint* 字段显示哪个指纹。

可能的值：

- ▶ *sha1*
Fingerprint 字段显示证书的 SHA1 指纹。
- ▶ *sha256*
Fingerprint 字段显示证书的 SHA256 指纹。

Fingerprint

服务器使用的数字证书的字符序列。

更改 *Fingerprint type* 字段中的设置时，之后点击 按钮，然后点击  按钮，以更新显示。

Certificate

提示：如果设备使用未经认证机构签名的证书，则 Web 浏览器在加载图形用户界面的同时会显示一条消息。要继续，请在 Web 浏览器中为该证书添加一条例外规则。

Present

显示设备中是否存在数字证书。

可能的值：

- ▶ 勾选
存在证书。
- ▶ 未勾选
证书已被删除。

Create

在设备中生成一个数字证书。

在重新启动之前，网络服务器会一直使用之前的证书。

要让网络服务器使用新生成的证书，请重新启动网络服务器。只能通过命令行界面重新启动网络服务器。

此外，用户还可以选择将自己的证书复制到设备。参见 *Certificate import* 框。

Delete

删除数字证书。

在重新启动之前，网络服务器会一直使用之前的证书。

Start

将 *URL* 字段中指定的证书复制到设备。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

3.4.2 IP Access Restriction

[Device Security > Management Access > IP Access Restriction]

此对话框允许用户将对设备管理的访问限制为特定的 IP 地址范围和选定的基于 IP 的应用程序。

- ▶ 如果禁用该功能，则可从任何 IP 地址使用任何应用程序访问设备管理。
- ▶ 如果该功能已启用，则访问受到限制。用户仅在以下条件下才拥有设备管理访问权限：
 - 至少激活了一个表格条目。
 - 和
 - 用户正在使用允许的应用程序从允许的 IP 地址范围访问设备。

Operation

提示：在启用该功能之前，请验证表格中是否至少有一个活动条目允许用户访问。否则，如果更改设置，与设备的连接会终止。只能通过串行接口使用命令行界面访问设备管理。

Operation

启用/禁用 *IP Access Restriction* 功能。

可能的值：

- ▶ *On*
IP Access Restriction 功能已启用。
对设备管理的访问受到限制。
- ▶ *Off* (默认设置)
IP Access Restriction 功能已禁用。

表格

用户可以选择定义并分别激活最多 16 个表格条目。

Index

显示与表格条目相关的索引编号。

删除一个表格条目后，会留下一个编号空缺。创建一个新的表格条目后，设备将填补第一个空缺。

可能的值:

- ▶ 1..16

Address

指定允许从其中访问设备管理的网络的 IP 地址。可在 *Netmask* 列中指定网络范围。

可能的值:

- ▶ 有效的 IPv4 地址 (默认设置: 0.0.0.0)

Netmask

指定 *Address* 列中指定的网络的范围。

可能的值:

- ▶ 有效的子网掩码 (默认设置: 0.0.0.0)

HTTP

激活/停用 HTTP 访问。

可能的值:

- ▶ 勾选 (默认设置)
为相邻 IP 地址范围激活了访问。
- ▶ 未勾选
访问已停用。

HTTPS

激活/停用 HTTPS 访问。

可能的值:

- ▶ 勾选 (默认设置)
为相邻 IP 地址范围激活了访问。
- ▶ 未勾选
访问已停用。

SNMP

激活/停用 SNMP 访问。

可能的值:

- ▶ 勾选 (默认设置)
为相邻 IP 地址范围激活了访问。
- ▶ 未勾选
访问已停用。

Telnet

激活/停用 Telnet 访问。

可能的值：

- ▶ 勾选（默认设置）
为相邻 IP 地址范围激活了访问。
- ▶ 未勾选
访问已停用。

SSH

激活/停用 SSH 访问。

可能的值：

- ▶ 勾选（默认设置）
为相邻 IP 地址范围激活了访问。
- ▶ 未勾选
访问已停用。

IEC61850-MMS

激活/停用对 MMS 服务器的访问。

可能的值：

- ▶ 勾选（默认设置）
为相邻 IP 地址范围激活了访问。
- ▶ 未勾选
访问已停用。

Modbus TCP

激活/停用对 *Modbus TCP* 服务器的访问。

可能的值：

- ▶ 勾选（默认设置）
为相邻 IP 地址范围激活了访问。
- ▶ 未勾选
访问已停用。

EtherNet/IP

激活/停用对 *EtherNet/IP* 服务器的访问。

可能的值：

- ▶ 勾选（默认设置）
为相邻 IP 地址范围激活了访问。
- ▶ 未勾选
访问已停用。

Active

激活/停用表格条目。

可能的值：

- ▶ **勾选** (默认设置)
表格条目已激活。设备限制对相邻 IP 地址范围和选定的基于 IP 的应用程序的设备管理的访问。
- ▶ **未勾选**
表格条目已停用。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

3.4.3 Web

[Device Security > Management Access > Web]

在此对话框中，可以指定图形用户界面的设置。

Configuration

Web interface session timeout [min]

指定超时时间（分钟）。当设备在此时间内处于非活动状态之后，它会终止已登录用户的会话。

可能的值：

► 0..160（默认设置：5）

值 0 停用该功能，并且用户在不活动时保持登录。

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

3.4.4 Command Line Interface

[Device Security > Management Access > CLI]

在此对话框中，可以指定命令行界面的设置。“命令行界面”参考手册中提供了有关命令行界面的详细信息。

该对话框包含以下选项卡：

- ▶ [Global]
- ▶ [Login banner]

[Global]

此选项卡可用于更改命令行界面中的提示符并指定自动关闭不活动的串行接口会话。

设备具有以下串行接口。

- ▶ USB-C 接口

Configuration

Login prompt

指定设备在命令行界面中每个命令行开始处显示的字符串。

可能的值：

- ▶ 带有 0..128 个字符的字母数字 ASCII 字符串 (0x20..0x7E) 含空格符
通配符
 - %d 日期
 - %i IP 地址
 - %m MAC 地址
 - %p 产品名称
 - %t 时间

默认设置： (MCSESM-E)

对此设置的更改会在活动命令行界面会话中立即生效。

Serial interface timeout [min]

指定设备自动关闭不活动用户（通过串行接口使用命令行界面登录）的会话之前经过的时间（分钟）。

可能的值：

- ▶ 0..160（默认设置：5）
值 0 停用该功能，并且用户在不活动时保持登录。

值的更改会在用户下次登录时生效。

对于 *Telnet* 服务器和 *SSH* 服务器，用户可以在 *Device Security > Management Access > Server* 对话框中指定超时。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

[Login banner]

在此选项卡中，可将命令行界面的启动屏幕替换为用户自己的文本。

在默认设置下，启动屏幕会显示关于设备的信息，如软件版本和设备设置等。借助此选项卡中的功能，可以停用此信息并将其替换为单独指定的文本。

要在命令行界面和图形用户界面中登录之前显示您自己的文本，请使用 *Device Security > Pre-login Banner* 对话框。

Operation

Operation

启用/禁用 *Login banner* 功能。

可能的值：

- ▶ *On*
Login banner 功能已启用。
设备向使用命令行界面登录的用户显示在 *Banner text* 字段中指定的文本信息。
- ▶ *Off* (默认设置)
Login banner 功能已禁用。
启动屏幕会显示关于设备的信息。会保留 *Banner text* 字段中的文本信息。

Banner text

Banner text

指定设备在命令行界面中每个会话开始处显示的字符串。

可能的值：

- ▶ 带有 0..1024 个字符的字母数字 ASCII 字符串
(0x20..0x7E) 含空格符
- ▶ <制表符>
- ▶ <换行符>

Remaining characters

显示 *Banner text* 字段中仍然剩余多少个用于文本信息的字符。

可能的值:

▶ 1024..0

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

3.4.5 SNMPv1/v2 Community

[Device Security > Management Access > SNMPv1/v2 Community]

在此对话框中，可以指定 SNMPv1/v2 应用程序的团体名称。

应用程序通过 SNMPv1/v2 发送在 SNMP 数据包报头中带有团体名称的请求。视团体名称而定，应用程序获得针对设备的读授权或读写授权。

可在 *Device Security > Management Access > Server* 对话框中激活通过 SNMPv1/v2 访问设备的权限。

表格

Community

显示 SNMPv1/v2 应用程序对设备的的授权：

- ▶ Write
对于输入了团体名称的请求，应用程序会获得针对设备的读写授权。
- ▶ Read
对于输入了团体名称的请求，应用程序会获得针对设备的读授权。

Name

为相邻授权指定团体名称。

可能的值：

- ▶ 带有 0..32 个字符的字母数字 ASCII 字符串
 - admin （针对读写授权的默认设置）
 - user （针对读授权的默认设置）

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

3.5 Pre-login Banner

[Device Security > Pre-login Banner]

此对话框可用于在用户登录之前向用户显示问候或信息文本。

用户在图形用户界面和命令行界面的登录对话框中会看到此文本。不管使用什么客户端，使用 SSH 登录的用户在登录之前或期间都会看到此文本。

要只在命令行界面中显示文本，请使用 *Device Security > Management Access > CLI* 对话框中的设置。

Operation

Operation

启用/禁用 *Pre-login Banner* 功能。

使用 *Pre-login Banner* 功能时，设备在图形用户界面和命令行界面的登录对话框中会显示问候语或信息文本。

可能的值：

- ▶ *On*
Pre-login Banner 功能已启用。
设备在登录对话框中显示 *Banner text* 字段中指定的文本。
- ▶ *Off* (默认设置)
Pre-login Banner 功能已禁用。
设备在登录对话框中不显示文本。在 *Banner text* 字段中输入文本时，此文本会保存到设备中。

Banner text

Banner text

指定设备在图形用户界面和命令行界面的登录对话框中显示的信息文本。

可能的值：

- ▶ 带有 0..512 个字符的字母数字 ASCII 字符串
(0x20..0x7E) 含空格符
- ▶ <制表符>
- ▶ <换行符>

Remaining characters

显示 *Banner text* 字段中仍然剩余多少个字符。

可能的值:

▶ 512..0

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

4 Network Security

该菜单包含以下对话框：

- ▶ Network Security Overview
- ▶ Port Security
- ▶ 802.1X Port Authentication
- ▶ RADIUS
- ▶ DoS
- ▶ DHCP Snooping
- ▶ IP Source Guard
- ▶ Dynamic ARP Inspection
- ▶ ACL

4.1 Network Security Overview

[Network Security > Overview]

此对话框显示设备中使用的网络安全规则。

参数

Port/VLAN

指定设备是否显示基于 VLAN 和/或基于端口的规则。

可能的值：

- ▶ *All* (默认设置)
设备显示用户指定的基于 VLAN 和基于端口的规则。
- ▶ 端口: <Port Number>
设备显示特定端口的基于端口的规则。为此端口指定一个或多个规则时，此选择可用。
- ▶ VLAN: <VLAN ID>
设备显示特定 VLAN 的基于 VLAN 的规则。为此 VLAN 指定一个或多个规则时，此选择可用。

ACL

在概览中显示 *ACL* 规则。

您可以在 *Network Security > ACL* 对话框中编辑 *ACL* 规则。

All

勾选相邻复选框。设备在概览中显示相关规则。

None

取消勾选相邻复选框。设备在概览中不显示任何规则。

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

4.2 Port Security

[Network Security > Port Security]


设备只允许用户在一个端口上传输来自所需发送者的数据包。此功能启用后，设备在传输数据包之前会检查发送者的 VLAN ID 和 MAC 地址或 VLAN ID 和 IP 地址。设备丢弃来自其他发送者的数据包并记录此事件。

设备还提供用于在传输数据包之前检查发送者的 IP 地址的功能。

提示：如果在 *Mode* 框中选择了 *IP* 单选按钮，则 *Port Security* 功能会在第二层上间接发挥作用。在设置允许的 IP 地址后，设备会检索当前与该 ID 地址关联的 MAC 地址。设备使用 ARP 请求并在内部保存关联的 MAC 地址。指定允许的 IP 地址的前提条件是，可以访问已连接的设备，并且该设备响应 ARP 请求。

如果已连接的设备使用允许的 IP 地址，但使用与关联的 MAC 地址不同的 MAC 地址发送数据包，则设备将丢弃相关的数据包。如果用户更换已连接的设备，并且使用与之前相同的 IP 地址，则会将该 IP 地址重新指定为允许的地址。在此步骤之后，设备将使用新的关联的 MAC 地址。

如果 *Auto-Disable* 功能已激活，则设备会禁用该端口。此限制使得 MAC 欺骗攻击变得更加困难。当不再超过参数时，*Auto-Disable* 功能再次自动启用相关端口。

在此对话框中，*Wizard* 窗口可以帮助用户将端口与一个或多个所需的源连接起来。在设备中，这些地址称为 *Static entries (x/y)*。要查看指定的静态地址，请突出显示相关端口，然后点击  按钮。

为了简化设置过程，设备允许用户自动记录所需的发送者。设备对收到的数据包进行评估，以此“示教”发送者。在设备中，这些地址称为 *Dynamic entries*。当达到用户自定义上限 (*Dynamic limit*) 时，设备在相关端口上停止“示教”并且只传输已经记录的发送者的数据包。将上限调整为预期发送者的数量时，可使 MAC 泛洪攻击变得更加困难。

提示：借助 *Dynamic entries* 的自动记录，设备会不断丢弃来自未知发送者的第一个数据包。使用此第一个数据包，设备可以检查是否已达到上限。设备会针对发送者进行记录，直到达到上限为止。之后，设备传输在相关端口上收到的来自该发送者的数据包。

Operation

Operation

启用/禁用 *Port Security* 功能。

可能的值：

► *On*

Port Security 功能已启用。

设备在传输数据包之前检查 VLAN ID 和源 MAC 地址。

仅当相关的端口上允许数据包的 VLAN ID 和源 MAC 地址时，设备才会传输收到的数据包。为使此设置生效，用户还需要激活相关端口上的源地址检查。

► *Off* (默认设置)

Port Security 功能已禁用。

设备在不检查源地址的情况下传输每个收到的数据包。

提示：如果在 *Mode* 框中选择了 *MAC* 单选按钮，则设备会针对允许的源 MAC 地址检查源 MAC 地址。如果选择了 *IP* 按钮，则设备会针对与允许的源 IP 关联的 MAC 地址检查源 MAC 地址。

Configuration

Auto-disable

激活/停用 *Port Security* 的 *Auto-Disable* 功能。

可能的值：

- ▶ 勾选
Port Security 的 *Auto-Disable* 功能已激活。
也为相关端口勾选 *Auto-disable* 列中的复选框。
- ▶ 未勾选（默认设置）
Port Security 的 *Auto-Disable* 功能已停用。

Mode

Mode

指定 *Port Security* 功能是否使用允许的 MAC 地址或允许的 IP 地址来检查收到的数据包。

可能的值：

- ▶ *MAC*（默认设置）
Port Security 功能使用允许的源 MAC 地址。
设备在传输数据包之前针对允许的源 MAC 地址检查 VLAN ID 和源 MAC 地址。
- ▶ *IP*
Port Security 功能使用允许的源 IP 地址。
设备在传输数据包之前针对与允许的源 IP 地址关联的 MAC 地址检查 VLAN ID 和源 MAC 地址。

表格

Port

显示端口编号。

Active

激活/停用端口上的源地址检查。

可能的值：

- ▶ 勾选
设备会检查端口上收到的每个数据包，只有当数据包的源地址得到允许时，才会传输这些数据包。此外，也会启用 *Operation* 框中的 *Port Security* 功能。
- ▶ 未勾选（默认设置）
设备传输在端口上收到的每个数据包，而不会检查源地址。

提示： 当您作为 *MRP* 环 或 *HIPER Ring*, we recommend that you unmark the checkbox for the ring ports.

提示： 当您作为 *Ring/Network Coupling* 或 *RCP* 的活动参与者操作设备时，我们建议您取消勾选相关耦合端口的复选框。

Auto-disable

为 *Port Security* 功能在端口上监控的参数激活/停用 *Auto-Disable* 功能。

可能的值：

▶ 勾选（默认设置）

端口上的 *Auto-Disable* 功能已激活。

前提条件是用户勾选 *Configuration* 框中的 *Auto-disable* 复选框。

- 如果端口注册了不允许的源 MAC 地址或注册了比 *Dynamic limit* 列中所指定数量更多的源 MAC 地址，则设备禁用该端口。端口的“链路状态”LED 指示灯每个周期闪烁 3 次。
- *Diagnostics > Ports > Auto-Disable* 对话框显示超过参数导致哪些端口当前被禁用。
- *Auto-Disable* 功能自动重新激活端口。为此，可以切换至 *Diagnostics > Ports > Auto-Disable* 对话框并在 *Reset timer [s]* 列中为相关端口指定等待期。

▶ 未勾选

端口上的 *Auto-Disable* 功能已停用。

Send trap

激活/停用当设备在端口上丢弃来自非所需发送者的数据包时 SNMP 陷阱的发送。

可能的值：

▶ 勾选

SNMP 陷阱发送激活。

如果设备在端口上丢弃来自不允许的发送者的数据包，则设备会发送一个 SNMP 陷阱。

▶ 未勾选（默认设置）

SNMP 陷阱发送停用。

发送 SNMP 陷阱的前提条件是，用户在 *Diagnostics > Status Configuration > Alarms (Traps)* 中启用该功能并至少指定一个陷阱目的地。

Trap interval [s]

指定设备在发送一个 SNMP 陷阱之后发送下一个 SNMP 陷阱之前等待的延迟时间（秒）。

可能的值：

▶ 0..3600（默认设置：0）

值 0 会停用该延迟时间。

Dynamic limit

指定自动注册源的数量的上限 (*Dynamic entries*)。达到该上限时，设备在此端口上停止“示教”。

将数值调整为预期源的数量。

如果端口注册了比此处所指定数量更多的发送者，则端口禁用 *Auto-Disable* 功能。前提条件是用户勾选 *Auto-disable* 列中的复选框以及 *Configuration* 框中的 *Auto-disable* 复选框。

可能的值：

▶ 0

停用此端口上源的自动注册。

▶ 1..600（默认设置：600）

Static limit

指定连接到端口的源的数量上限 (*Static entries (x/y)*)。 *Wizard* 窗口和 *MAC addresses* 对话框可以帮助用户将端口与一个或多个所需的源连接起来。

可能的值:

▶ 0..64 (默认设置: 64)

值 0 可以帮助用户防止将源与端口连接起来。

Dynamic entries

显示设备自动确定的发送者的数量。

参见 *Wizard* 窗口 *MAC addresses* 对话框中的 *Dynamic entries* 字段。

如果选择 *Mode* 框 *IP* 中的值, 则 *Dynamic entries* 列将显示值 0。

Static MAC entries

显示与端口连接的发送者的数量。

参见 *Wizard* 窗口 *MAC addresses* 对话框中的 *Static entries (x/y)* 字段。

Static IP entries

显示端口上允许的 IP 地址的数量。

参见 *Wizard* 窗口 *IP addresses* 对话框中的 *Static entries (x/y)* 字段。

Last violating VLAN ID/MAC

显示设备上上次在此端口上丢弃数据包的非所需发送者的 VLAN ID 和 MAC 地址。

Sent traps

显示导致设备发送 SNMP 陷阱的此端口上所丢弃数据包的数量。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

[Port security (Wizard)]

Wizard 窗口可以帮助用户将端口与一个或多个所需的源连接起来。指定设置后, 点击 *Finish* 按钮。

提示: 设备保存与端口连接的源, 直到用户在相关端口上或 *Operation* 框中停用源的检查为止。

关闭 *Wizard* 窗口后, 点击 按钮保存您的设置。

[Port security (Wizard) - Select port]

Port

指定在下一步中分配给发送者的端口。

[Port security (Wizard) - MAC addresses]

VLAN ID

指定所需源的 VLAN ID。

可能的值：

▶ 1..4042

要将 VLAN ID 和 MAC 地址传送到 *Static entries (x/y)* 字段，请点击 *Add* 按钮。

MAC address

指定所需源的 MAC 地址。

可能的值：

▶ 有效单播 MAC 地址
使用冒号分隔符指定值，如 00:11:22:33:44:55。

要将 VLAN ID 和 MAC 地址传送到 *Static entries (x/y)* 字段，请点击 *Add* 按钮。

Add

将 *VLAN ID* 字段和 *MAC address* 字段中指定的值传送到 *Static entries (x/y)* 字段。

Static entries (x/y)

显示连接到端口的所需发送者的 VLAN ID 和 MAC 地址。

设备使用此字段显示连接到端口的发送者的数量和上限。可在表格的 *Static limit* 字段中指定条目数量上限。

提示：无法将分配给此端口的 MAC 地址分配给任何其他端口。

Remove

删除 *Static entries (x/y)* 字段中突出显示的条目。



将 *Dynamic entries* 字段中突出显示的条目移动到 *Static entries (x/y)* 字段。



将每个条目从 *Dynamic entries* 字段移动到 *Static entries (x/y)* 字段。

当 *Dynamic entries* 字段含有比 *Static entries (x/y)* 字段中所允许数量更多的条目时，设备移动最前面的条目，直到达到上限为止。

Dynamic entries

按升序显示此端口上自动记录的发送者的 VLAN ID 和 MAC 地址。在此端口上接收数据包时，设备传输来自这些发送者的数据包。

设备显示 MAC 地址的前提条件是：

- *Port Security* 功能已启用。参见 *Operation* 框。
- 设备会检查在端口上收到的每个数据包。*Active* 列中的复选框为勾选。

可在表格的 *Dynamic limit* 字段中指定条目数量上限。

按钮和 按钮允许用户将条目从这个字段传送到 *Static entries (x/y)* 字段中。通过这种方式，可以将相关发送者与端口连接起来。

[Port security (Wizard) - IP addresses]

VLAN ID

指定所需源的 VLAN ID。

可能的值：

▶ 1..4042

提示： 分配管理 VLAN 的 VLAN ID。

要将 *VLAN ID* 和 *IP address* 传送到 *Static entries (x/y)* 字段，请点击 *Add* 按钮。

IP address

指定所需源的 IP 地址。

可能的值：

▶ 有效的 IPv4 地址

要将 *VLAN ID* 和 *IP address* 传送到 *Static entries (x/y)* 字段，请点击 *Add* 按钮。

Add

将 *VLAN ID* 字段和 *IP address* 字段中指定的值传送到 *Static entries (x/y)* 字段。

Static entries (x/y)

显示连接到端口的所需发送者的 VLAN ID 和 IP 地址。

设备使用此字段显示连接到端口的发送者的数量和上限。用户可指定最多 10 个 IP 地址。

Remove

删除 *Static entries (x/y)* 字段中突出显示的条目。

4.3 802.1X Port Authentication

[Network Security > 802.1X Port Authentication]

使用符合 IEEE 802.1X 的基于端口的访问控制，设备可以监控从相连终端设备对网络进行的访问。如果使用有效登录数据进行登录，则设备（身份验证器）允许终端设备（申请者）访问网络。身份验证器与终端设备通过 EAPoL（局域网上的可扩展身份验证协议）身份验证协议进行通信。

设备支持以下终端设备身份验证方法：

- ▶ radius
网络中的 RADIUS 服务器对终端设备进行身份验证。
- ▶ ias
设备中实施的集成身份验证服务器（IAS）对终端设备进行身份验证。与 RADIUS 相比，IAS 只提供基本功能。

该菜单包含以下对话框：

- ▶ 802.1X Global
- ▶ 802.1X Port Configuration
- ▶ 802.1X Port Clients
- ▶ 802.1X EAPoL Port Statistics
- ▶ 802.1X Port Authentication History
- ▶ 802.1X Integrated Authentication Server

4.3.1 802.1X Global

[Network Security > 802.1X Port Authentication > Global]

此对话框可用于为基于端口的访问控制指定基本设置。

Operation

Operation

启用/禁用 *802.1X Port Authentication* 功能。

可能的值：

- ▶ *On*
802.1X Port Authentication 功能已启用。
设备检查从相连终端设备对网络的访问。
基于端口的访问控制已启用。
- ▶ *Off* (默认设置)
802.1X Port Authentication 功能已禁用。
基于端口的访问控制已禁用。

Configuration

VLAN assignment

激活/停用相关端口向 VLAN 的分配。此功能允许用户为此 VLAN 中的相连终端设备提供选定的服务。

可能的值：

- ▶ *勾选*
分配已激活。
如果终端设备成功完成自我身份验证，则设备将 RADIUS 身份验证服务器传送的 VLAN ID 分配给相关端口。
- ▶ *未勾选* (默认设置)
分配已停用。
相关端口被分配给 *Network Security > 802.1X Port Authentication > Port Configuration* 对话框 *Assigned VLAN ID* 行中指定的 VLAN。

Dynamic VLAN creation

激活/停用不存在 VLAN 时 RADIUS 身份验证服务器分配的 VLAN 的自动创建。

可能的值：

- ▶ *勾选*
自动 VLAN 创建已激活。
如果不存在 VLAN，则设备创建 VLAN。
- ▶ *未勾选* (默认设置)
自动 VLAN 创建已停用。
如果不存在分配的 VLAN，则端口仍然分配给原始 VLAN。

Monitor mode

激活/停用监控器模式。

可能的值：

- ▶ **勾选**
监控器模式已激活。
设备对身份验证进行监控并帮助用户对检测到的错误进行诊断。如果终端设备没有成功登录，则设备允许终端设备访问网络。
- ▶ **未勾选**（默认设置）
监控器模式已停用。

MAC authentication bypass format options

Group size

指定 MAC 地址组的大小。设备将用于身份验证的 MAC 地址分为多个组。组的大小以半字节指定，每个半字节由一个字符表示。

可能的值：

- ▶ **1**
设备将 MAC 地址分为 12 组，每组 1 个字符。
示例：**A:A:B:B:C:C:D:D:E:E:F:F**
- ▶ **2**
设备将 MAC 地址分为 6 组，每组 2 个字符。
示例：**AA:BB:CC:DD:EE:FF**
- ▶ **4**
设备将 MAC 地址分为 3 组，每组 4 个字符。
示例：**AABB:CCDD:EEFF**
- ▶ **12**（默认设置）
设备将 MAC 地址格式化为 1 组，包含 12 个字符。
示例：**AABCCDDEEFF**

Group separator

指定将组分隔的字符。

可能的值：

- ▶ **-**
破折号
- ▶ **:**
冒号
- ▶ **.**
点

Upper or lower case

指定设备将身份验证数据格式化为小写字母还是大写字母。

可能的值：

- ▶ **lower-case**
- ▶ **upper-case**

Password

指定使用身份验证绕过的客户端的可选密码。

可能的值：

- ▶ 带有 0..64 个字符的字母数字 ASCII 字符串
输入后，字段显示 *****（星号），而不是密码。
- ▶ <空>
设备也会将客户端的用户名用作密码。

Information

Monitor mode clients

显示即使没有成功登录，设备也会向其授予网络访问权限的终端设备数。

前提条件是用户激活了 *Monitor mode* 功能。参见 *Configuration* 框。

Non monitor mode clients

显示成功登录后设备为其提供网络访问权限的终端设备的数量。

Policy 1

显示设备当前对使用 IEEE 802.1X 的终端设备进行身份验证所使用的方法。

可在 *Device Security > Authentication List* 对话框中指定使用的方法。

- 要通过 RADIUS 服务器对终端设备进行身份验证，可将 *radius* 策略分配给 *8021x* 列表。
- 要通过集成身份验证服务器（IAS）对终端设备进行身份验证，可将 *ias* 策略分配给 *8021x* 列表。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

4.3.2 802.1X Port Configuration

[Network Security > 802.1X Port Authentication > Port Configuration]

此对话框可用于为每个端口指定访问设置。

当多个终端设备连接到一个端口时，设备允许用户单独对各终端设备进行身份验证（多客户端身份验证）。在这种情况下，设备允许已登录的终端设备访问网络。与之相反，设备将阻止未经身份验证或身份验证过期的终端设备的访问。

表格

Port

显示端口编号。

Port initialization

激活/停用端口初始化，以激活端口上的访问控制或将其重置为初始状态。请仅在其中 *Port control* 列包含值 *auto* 或 *multiClient* 的端口上使用此功能。

可能的值：

- ▶ *勾选*
端口初始化已激活。
初始化完成后，设备再次将该值更改为*未勾选*。
- ▶ *未勾选*（默认设置）
端口初始化已停用。
设备保持当前端口状态。

Port reauthentication

激活/停用一次性重新身份验证请求。

请仅在其中 *Port control* 列包含值 *auto* 或 *multiClient* 的端口上使用此功能。

设备还允许用户定期请求终端设备再次登录。参见 *Periodic reauthentication* 列。

可能的值：

- ▶ *勾选*
一次性重新身份验证请求已激活。
设备请求终端设备再次登录。之后，设备会再次将该值更改为*未勾选*。
- ▶ *未勾选*（默认设置）
一次性重新身份验证请求已停用。
设备保持终端设备登录状态。

Authentication activity

显示身份验证器的当前状态（*Authenticator PAE state*）。

可能的值：

- ▶ *initialize*
- ▶ *disconnected*
- ▶ *connecting*

- ▶ *authenticating*
- ▶ *authenticated*
- ▶ *aborting*
- ▶ *held*
- ▶ *forceAuth*
- ▶ *forceUnauth*

Backend authentication state

显示至身份验证服务器的连接的当前状态 (Backend Authentication state)。

可能的值:

- ▶ *request*
- ▶ *response*
- ▶ *success*
- ▶ *fail*
- ▶ *timeout*
- ▶ *idle*
- ▶ *initialize*

Authentication state

显示端口上身份验证的当前状态 (Controlled Port Status)。

可能的值:

- ▶ *authorized*
终端设备成功登录。
- ▶ *unauthorized*
终端设备未登录。

Users (max.)

指定设备可以在此端口上同时进行身份验证的终端设备的数量上限。此上限只适用于其中 *Port control* 列包含 *multiClient* 值的端口。

可能的值:

- ▶ 1..16 (默认设置: 16)

Port control

指定设备如何授予对网络的访问权限 (Port control mode)。

可能的值:

- ▶ *forceUnauthorized*
设备阻止对网络的访问。如果终端设备连接到没有获得网络访问权限的端口, 可使用此设置。
- ▶ *auto*
如果终端设备成功登录, 则设备授予对网络的访问权限。如果终端设备连接到通过身份验证器登录的端口, 可使用此设置。

提示: 如果有其他终端设备通过同一端口进行连接, 则它们无需额外的身份验证即可访问网络。

▶ *forceAuthorized* (默认设置)

当终端设备不支持 IEEE 802.1X 时，设备授予对网络的访问权限。如果终端设备连接到无需登录即可访问网络的端口，可使用此设置。

▶ *multiClient*

如果终端设备成功登录，则设备授予其网络访问权限。

如果终端设备未发送任何 EAPOL 数据包，则设备根据终端设备的 MAC 地址分别授予或拒绝其网络访问权限。参见 *MAC authorized bypass* 列。

如果多个终端设备连接到端口或需要 *MAC authorized bypass* 功能，则使用此设置。

Quiet period [s]

指定在登录尝试失败后身份验证器不再接受来自终端设备的任何登录的时间段（秒）（*Quiet period [s]*）。

可能的值：

- ▶ 0..65535（默认设置：60）

Transmit period [s]

指定身份验证器请求终端设备再次登录之前的时间段（秒）。在经过此等待期之后，设备会向终端设备发送一个 EAP 请求/身份数据包。

可能的值：

- ▶ 1..65535（默认设置：30）

Supplicant timeout period [s]

指定身份验证器等待终端设备登录的时间段（秒）。

可能的值：

- ▶ 1..65535（默认设置：30）

Server timeout [s]

指定身份验证器等待来自身份验证服务器（RADIUS 或 IAS）的响应的时间段（秒）。

可能的值：

- ▶ 1..65535（默认设置：30）

Requests (max.)

指定在 *Supplicant timeout period [s]* 列中指定的时间过去之前，身份验证器请求终端设备进行登录的次数。设备按照此处指定的频率向终端设备发送 EAP 请求/身份数据包。

可能的值：

- ▶ 0..10（默认设置：2）

Assigned VLAN ID

显示身份验证器分配给端口的 VLAN 的 ID。此值只适用于其中 *Port control* 列含有值 *auto* 的端口。

可能的值：

- ▶ 0..4042（默认设置：0）

可在 *Network Security > 802.1X Port Authentication > Port Clients* 对话框中找到身份验证器分配给端口的 VLAN ID。

对于其中 *Port control* 列包含 *multiClient* 值的端口，设备将在接收到不包含 VLAN 标签的数据包时，根据终端设备的 MAC 地址分配 VLAN 标签。

Assignment reason

显示分配 VLAN ID 的原因。此值只适用于其中 *Port control* 列含有值 *auto* 的端口。

可能的值：

- ▶ *notAssigned* (默认设置)
- ▶ *radius*
- ▶ *guestVlan*
- ▶ *unauthenticatedVlan*

可在 *Network Security > 802.1X Port Authentication > Port Clients* 对话框中找到身份验证器为申请者分配给端口的 VLAN ID。

Reauthentication period [s]

指定身份验证器定期请求终端设备再次登录之前的时间段（秒）。

可能的值：

- ▶ 1..65535 (默认设置：3600)

Periodic reauthentication

激活/停用周期性重新身份验证请求。

可能的值：

- ▶ 勾选
周期性重新身份验证请求已激活。
设备定期请求终端设备再次登录。可在 *Reauthentication period [s]* 列中指定此时间段。
如果身份验证器将语音 VLAN、未经身份验证的 VLAN 或访客 VLAN 的 ID 分配给终端设备，则此设置失效。
- ▶ 未勾选 (默认设置)
周期性重新身份验证请求已停用。
设备保持终端设备登录状态。

Guest VLAN ID

指定当终端设备在 *Guest VLAN period* 列中指定的时间期限内没有进行登录时身份验证器分配给端口的 VLAN 的 ID。此值只适用于其中 *Port control* 列包含值 *auto* 或 *multiClient* 的端口。

此功能可用于允许没有 IEEE 802.1X 支持的终端设备访问网络中的选定服务。

可能的值：

- ▶ 0 (默认设置)
身份验证器不会向端口分配访客 VLAN。
如果用户在 *MAC authorized bypass* 列中启用基于 MAC 的身份验证，则设备会自动将其值设为 0。
- ▶ 1..4042

提示： *MAC authorized bypass* 功能和 *Guest VLAN ID* 功能不能同时使用。

Guest VLAN period

指定终端设备连接后身份验证器等待 EAPOL 数据包的时间段（秒）。如果此期限已经过去，则身份验证器允许终端设备访问网络并将端口分配给 *Guest VLAN ID* 列中指定的访客访客 VLAN。

可能的值：

- ▶ 1..300（默认设置：90）

Unauthenticated VLAN ID

指定当终端设备登录失败时身份验证器分配给端口的 VLAN 的 ID。此值只适用于其中 *Port control* 列含有值 *auto* 的端口。

此功能可用于允许没有有效登录数据的终端设备访问网络中的选定服务。

可能的值：

- ▶ 0..4042（默认设置：0）

值 0 的作用是，身份验证器不会向端口分配未经身份验证的 VLAN。

提示：向端口分配一个在设备中静态设置的 VLAN。

MAC authorized bypass

激活/停用基于 MAC 的身份验证。

此功能允许对不支持 IEEE 802.1X 的终端设备进行基于 MAC 地址的身份验证。

可能的值：

- ▶ 勾选
基于 MAC 的身份验证已激活。
设备将终端设备的 MAC 地址发送到 RADIUS 身份验证服务器。设备根据申请者的 MAC 地址将其分配到相应的 VLAN，如同直接通过 IEEE 802.1X 执行身份验证一样。
- ▶ 未勾选（默认设置）
基于 MAC 的身份验证已停用。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

4.3.3 802.1X Port Clients

[Network Security > 802.1X Port Authentication > Port Clients]

此对话框显示关于相连终端设备的信息。

表格

Port

显示端口编号。

User name

显示终端设备登录时使用的用户名。

MAC address

显示终端设备的 MAC 地址。

Assigned VLAN ID

显示终端设备身份验证成功后身份验证器分配给端口的 VLAN ID。

对于 *Network Security > 802.1X Port Authentication > Port Configuration* 对话框中的端口，如果指定了 *Port control* 列中的 *multiClient* 值，则设备将在接收到不包含 VLAN 标签的数据包时，根据终端设备的 MAC 地址分配 VLAN 标签。

Assignment reason

显示分配 VLAN 的原因。

可能的值：

- ▶ *default*
- ▶ *radius*
- ▶ *unauthenticatedVlan*
- ▶ *guestVlan*
- ▶ *monitorVlan*
- ▶ *invalid*

只要客户端经过了身份验证，该字段只显示有效值。

Session timeout

显示终端设备登录过期之前的剩余时间（秒）。此值只适用于在 *Network Security > 802.1X Port Authentication > Port Configuration* 对话框 *Port control* 列中为其指定了值 *auto* 或 *multiClient* 的端口。

身份验证服务器通过 RADIUS 向设备分配超时期限。值 0 表示身份验证服务器未分配超时。

Termination action

显示登录时间过去后设备执行的操作。

可能的值：

▶ *default*

▶ *reauthenticate*

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

4.3.4 802.1X EAPOL Port Statistics

[Network Security > 802.1X Port Authentication > Statistics]

此对话框显示为了对终端设备进行身份验证，终端设备发送和接收了哪些 EAPOL 数据包。

表格

Port

显示端口编号。

Received packets

显示设备在端口上接收的 EAPOL 数据包的总数。

Transmitted packets

显示设备在端口上发送的 EAPOL 数据包的总数。

Start packets

显示设备在端口上接收的 EAPOL 开始数据包的数量。

Logoff packets

显示设备在端口上接收的 EAPOL 注销数据包的数量。

Response/ID packets

显示设备在端口上接收的 EAP 响应/身份数据包的数量。

Response packets

显示设备在端口上接收的有效 EAP 响应数据包的数量（无 EAP 响应/身份数据包）。

Request/ID packets

显示设备在端口上接收的 EAP 请求/身份数据包的数量。

Request packets

显示设备在端口上接收的有效 EAP 请求数据包的数量（无 EAP 请求/身份数据包）。

Invalid packets

显示设备在端口上接收的具有未知帧类型的 EAPOL 数据包的数量。

Received error packets

显示设备在端口上接收的具有无效包体长度字段的 EAPOL 数据包的数量。

Packet version

显示设备上上次在端口上接收的 EAPOL 数据包的协议版本号。

Source of last received packet

显示设备上上次在端口上接收的 EAPOL 数据包的发送者 MAC 地址。

值 `00:00:00:00:00:00` 表示端口尚未收到任何 EAPOL 数据包。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

4.3.5 802.1X Port Authentication History

[Network Security > 802.1X Port Authentication > Port Authentication History]

设备对连接到其端口的终端设备的身份验证过程进行注册。此对话框显示身份验证期间记录的信息。

表格

Port

显示端口编号。

Authentication time stamp

显示身份验证器对终端设备进行身份验证的时间。

Result age

显示表格中最初输入此条目的时间。

MAC address

显示终端设备的 MAC 地址。

VLAN ID

显示登录前分配给终端设备的 VLAN 的 ID。

Authentication status

显示端口上身份验证的状态。

可能的值：

- ▶ *success*
身份验证成功。
- ▶ *failure*
身份验证没有成功。

Access status

显示设备是否允许终端设备访问网络。

可能的值：

- ▶ *granted*
设备允许终端设备访问网络。
- ▶ *denied*
设备拒绝终端设备访问网络。

Assigned VLAN ID

显示身份验证器分配给端口的 VLAN 的 ID。

Assignment type

显示身份验证器分配给端口的 VLAN 的类型。

可能的值:

- ▶ *default*
- ▶ *radius*
- ▶ *unauthenticatedVlan*
- ▶ *guestVlan*
- ▶ *monitorVlan*
- ▶ *notAssigned*

Assignment reason

显示分配 VLAN ID 和 VLAN 类型的原因。

802.1X Port Authentication History

Port

简化表格并且只显示与此处选择的端口相关的条目。这使用户能够更容易地记录表格并根据需要对其进行排序。

可能的值:

- ▶ *all*
该表格显示每个端口的条目。
- ▶ *<Port number>*
该表格显示适用于此处所选端口的条目。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

4.3.6 802.1X Integrated Authentication Server

[Network Security > 802.1X Port Authentication > Integrated Authentication Server]

集成身份验证服务器 (IAS) 允许用户使用 IEEE 802.1X 对终端设备进行身份验证。与 RADIUS 相比, IAS 的功能范围非常有限。身份验证仅基于用户名和密码。


在此对话框中, 可以对终端设备的登录数据进行管理。设备允许用户设置最多 100 组登录数据。

要通过集成身份验证服务器对终端设备进行身份验证, 可在 *Device Security > Authentication List* 对话框中将 *ias* 策略分配给 8021x 列表。

表格

User name

显示终端设备的用户名。

要创建新的用户, 请点击  按钮。

Password

指定用户进行身份验证时使用的密码。

可能的值:

- ▶ 带有 0..64 个字符的字母数字 ASCII 字符串

设备区分大小写。

Active

激活/停用登录数据。

可能的值:

- ▶ **勾选**
登录数据已激活。终端设备可以选择使用此登录数据通过 IEEE 802.1X 进行登录。
- ▶ **未勾选** (默认设置)
登录数据已停用。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

4.4 RADIUS

[Network Security > RADIUS]

使用其出厂设置，设备根据本地用户管理对用户进行身份验证。但是，随着网络规模的增大，在不同设备之间保持用户登录数据一致性的难度也越来越大。

RADIUS（远程身份验证拨号用户服务）允许您在网络中的中心点对用户进行身份验证和授权。

RADIUS 服务器在此执行以下任务：

- ▶ 身份验证
当接入点处的 RADIUS 客户端将用户登录数据转发给服务器时，身份验证服务器对用户进行身份验证。
- ▶ 授权
身份验证服务器将相关终端设备的各种参数分配给接入点处的 RADIUS 客户端，进而授权登录用户使用选定服务。
- ▶ 记账
记账服务器对根据 IEEE 802.1X 进行端口身份验证期间产生的流量数据进行记录。这使您能够随后确定用户在多大程度上使用了哪些服务。

如果在 `radius` 对话框中将 `Device Security > Authentication List` 策略分配给一个应用程序，则设备以 RADIUS 客户端角色运行。设备将用户登录数据转发给一级身份验证服务器。该身份验证服务器决定登录数据是否有效，并将用户授权传输给设备。

设备按如下所示将 RADIUS 服务器的响应中传送的服务类型分配给设备中存在的一个用户角色：

- Administrative-User: `administrator`
- Login-User: `operator`
- NAS-Prompt-User: `guest`

设备还允许用户使用 IEEE 802.1X 通过身份验证服务器对终端设备进行身份验证。为此，可在 `radius` 对话框中将 `8021x` 策略分配给 `Device Security > Authentication List` 列表。

该菜单包含以下对话框：

- ▶ RADIUS Global
- ▶ RADIUS Authentication Server
- ▶ RADIUS Accounting Server
- ▶ RADIUS Authentication Statistics
- ▶ RADIUS Accounting Statistics

4.4.1 RADIUS Global

[Network Security > RADIUS > Global]

此对话框可用于为 RADIUS 指定基本设置。

RADIUS configuration

Retransmits (max.)

指定在设备将请求发送到另一个身份验证服务器之前，设备将未应答的请求重新发送到身份验证服务器的次数。

可能的值：

- ▶ 1..15（默认设置：4）

Timeout [s]

指定设备在向身份验证服务器发送请求后重新发送该请求之前等待响应的时间（秒）。

可能的值：

- ▶ 1..30（默认设置：5）

Accounting

激活/停用记账。

可能的值：

- ▶ 勾选
记账已激活。
设备向 *Network Security > RADIUS > Accounting Server* 对话框中指定的记账服务器发送流量数据。
- ▶ 未勾选（默认设置）
记账已停用。

NAS IP address (attribute 4)

指定设备作为属性 4 传送到身份验证服务器的 IP 地址。指定设备的 IP 地址或另一个可用地址。

提示：如果数据包由终端设备（申请者）的 *802.1X* 身份验证请求所触发，则设备仅包括属性 4。

可能的值：

- ▶ 有效的 IPv4 地址（默认设置：0.0.0.0）

在很多情况下，设备与身份验证服务器之间有防火墙。如果防火墙中的网络地址转换（NAT）更改了原始 IP 地址，则身份验证服务器将收到设备的转换 IP 地址。

设备在整个网络地址转换（NAT）中不加改变地传送此字段中的 IP 地址。

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

Reset

删除 *Network Security > RADIUS > Authentication Statistics* 对话框和 *Network Security > RADIUS > Accounting Statistics* 对话框中的统计数据。

4.4.2 RADIUS Authentication Server

[Network Security > RADIUS > Authentication Server]

此对话框可用于指定最多 8 个身份验证服务器。当设备将登录数据转发给一个身份验证服务器时，该服务器会对用户进行身份验证和授权。

设备将登录数据发送到指定的一级身份验证服务器。当该服务器没有响应时，设备会与表格中排序最高的指定身份验证服务器联系。当此服务器也没有响应时，设备会与表格中的下一个服务器联系。

表格

Index

显示与表格条目相关的索引编号。

Name

显示服务器名称。

要更改数值，请点击相关字段。

可能的值：

- ▶ 带有 1..32 个字符的字母数字 ASCII 字符串
(默认设置: `Default-RADIUS-Server`)

Address

指定服务器的 IP 地址。

可能的值：

- ▶ 有效的 IPv4 地址

Destination UDP port

指定服务器通过其接收请求的 UDP 端口的编号。

可能的值：

- ▶ `0..65535` (默认设置: `1812`)
例外: 端口 `2222` 预留给内部功能。

Secret

指定设备登录服务器时使用的密码时显示 `*****` (若干星号)。要更改密码，请点击相关字段。

可能的值：

- ▶ 带有 1..64 个字符的字母数字 ASCII 字符串

用户可从身份验证服务器管理员那里获得密码。

Primary server

将身份验证服务器指定为一级或二级。

可能的值：

- ▶ **勾选**
服务器被指定为一级身份验证服务器。设备将用于对用户进行身份验证的登录数据发送到此身份验证服务器。
激活多个服务器时，设备将最后一个激活的服务器指定为一级身份验证服务器。
- ▶ **未勾选**（默认设置）
服务器是二级身份验证服务器。当设备没有收到来自一级身份验证服务器的响应时，设备将登录数据发送到二级身份验证服务器。

Active

激活/停用至服务器的连接。

如果在 *Device Security > Authentication List* 对话框的 *Policy 1* 至 *Policy 5* 任一行中指定值 *radius*，则设备使用该服务器。

可能的值：

- ▶ **勾选**（默认设置）
连接已激活。如果满足上述前提条件，则设备将用于对用户进行身份验证的登录数据发送到此服务器。
- ▶ **未勾选**
连接已停用。设备不向此服务器发送任何登录数据。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。



打开 *Create* 窗口，向表格中添加一个新的条目。

- ▶ 在 *Index* 字段中，可以指定索引编号。
- ▶ 在 *Address* 字段中，可以指定服务器的 IP 地址。

4.4.3 RADIUS Accounting Server

[Network Security > RADIUS > Accounting Server]

此对话框可用于指定最多 8 个记账服务器。记账服务器对根据 IEEE 802.1X 进行端口身份验证期间产生的流量数据进行记录。前提条件是用户在 *Network Security > RADIUS > Global* 菜单中激活了 *Accounting* 功能。

设备将流量数据发送到可以到达的第一个记账服务器。当记账服务器没有响应时，设备会与表格中的下一个服务器联系。

表格

Index

显示与表格条目相关的索引编号。

可能的值：

▶ 1..8

Name

显示服务器名称。

要更改数值，请点击相关字段。

可能的值：

▶ 带有 1..32 个字符的字母数字 ASCII 字符串
(默认设置: *Default-RADIUS-Server*)

Address

指定服务器的 IP 地址。

可能的值：

▶ 有效的 IPv4 地址

Destination UDP port

指定服务器通过其接收请求的 UDP 端口的编号。

可能的值：

▶ 0..65535 (默认设置: 1813)
例外: 端口 2222 预留给内部功能。

Secret

指定设备登录服务器时使用的密码时显示 ******* (若干星号)。要更改密码，请点击相关字段。

可能的值：

▶ 带有 1..16 个字符的字母数字 ASCII 字符串

用户可从身份验证服务器管理员那里获得密码。

Active

激活/停用至服务器的连接。

可能的值：

- ▶ **勾选** (默认设置)
连接已激活。如果满足上述前提条件，则设备将流量数据发送到此服务器。
- ▶ **未勾选**
连接已停用。设备不向此服务器发送任何流量数据。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。



打开 *Create* 窗口，向表格中添加一个新的条目。

- ▶ 在 *Index* 字段中，可以指定索引编号。
- ▶ 在 *Address* 字段中，可以指定服务器的 IP 地址。

4.4.4 RADIUS Authentication Statistics

[Network Security > RADIUS > Authentication Statistics]

此对话框显示有关设备与身份验证服务器之间通信的信息。该表格在单独一行中显示每个服务器的信息。

要删除统计数据，请点击 *Network Security > RADIUS > Global* 对话框中的  按钮，然后点击 *Reset* 项目。

表格

Name

显示服务器名称。

Address

显示服务器的 IP 地址。

Round trip time

显示从收到来自服务器的最后一个响应（访问应答/访问挑战）到发送相应数据包（访问请求）之间的时间间隔（百分之一秒）。

Access requests

显示设备发送到服务器的访问数据包的数量。此值不考虑重复。

Retransmitted access-request packets

显示设备重新发送到服务器的访问数据包的数量。

Access accepts

显示设备从服务器接收到的访问接受数据包的数量。

Access rejects

显示设备从服务器接收到的访问拒绝数据包的数量。

Access challenges

显示设备从服务器接收到的访问挑战数据包的数量。

Malformed access responses

显示设备从服务器接收到的格式错误的访问响应数据包的数量（包括具有无效长度的数据包）。

Bad authenticators

显示设备从服务器接收到的带有无效身份验证器的访问响应数据包的数量。

Pending requests

显示设备发送到服务器但尚未收到来自服务器的响应的访问请求数据包的数量。

Timeouts

显示在指定等待时间过去之前没有收到对服务器的响应的次数。

Unknown types

显示设备通过身份验证端口从服务器接收到的带有未知数据类型的数据包的数量。

Packets dropped

显示设备通过身份验证端口从服务器接收并随后丢弃的数据包的数量。

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

4.4.5 RADIUS Accounting Statistics

[Network Security > RADIUS > Accounting Statistics]

此对话框显示有关设备与记账服务器之间通信的信息。该表格在单独一行中显示每个服务器的信息。

要删除统计数据，请点击 *Network Security > RADIUS > Global* 对话框中的  按钮，然后点击 *Reset* 项目。

表格

Name

显示服务器名称。

Address

显示服务器的 IP 地址。

Round trip time

显示从收到来自服务器的最后一个响应（记账响应）到发送相应数据包（记账请求）之间的时间间隔（百分之一秒）。

Accounting-request packets

显示设备发送到服务器的记账请求数据包的数量。此值不考虑重复。

Retransmitted accounting-request packets

显示设备重新发送到服务器的记账请求数据包的数量。

Received packets

显示设备从服务器接收到的记账响应数据包的数量。

Malformed packets

显示设备从服务器接收到的格式错误的记账响应数据包的数量（包括具有无效长度的数据包）。

Bad authenticators

显示设备从服务器接收到的带有无效身份验证器的记账响应数据包的数量。

Pending requests

显示设备发送到服务器但尚未收到来自服务器的响应的记账请求数据包的数量。

Timeouts

显示在指定等待时间过去之前没有收到对服务器的响应的次数。

Unknown types

显示设备通过记账端口从服务器接收到的带有未知数据类型的数据包的数量。

Packets dropped

显示设备通过记账端口从服务器接收并随后丢弃的数据包的数量。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

4.5 DoS

[Network Security > DoS]

拒绝服务 (DoS) 是一种旨在破坏特定服务或设备的网络攻击。在此对话框中，用户可以设置多个筛选器，帮助保护设备本身和网络中的其他设备免受 DoS 攻击。

该菜单包含以下对话框：

▶ [DoS Global](#)

4.5.1 DoS Global

[Network Security > DoS > Global]

用户可在此对话框中为 TCP/UDP、IP 和 ICMP 等协议指定 DoS 设置。

TCP/UDP

扫描器使用端口扫描来准备网络攻击。扫描器使用不同技术来确定正在运行的设备和打开的端口。此框允许用户为特定扫描技术激活筛选器。

设备支持以下扫描类型的检测：

- ▶ Null 扫描
- ▶ Xmas 扫描
- ▶ SYN/FIN 扫描
- ▶ TCP 偏移量攻击
- ▶ TCP SYN 攻击
- ▶ 第四层端口攻击
- ▶ 最小报头扫描

Null Scan filter

激活/停用 Null 扫描筛选器。

设备检测并丢弃具有以下属性的传入 TCP 数据包：

- ▶ 未设置任何 TCP 标志。
- ▶ TCP 序列号为 0。

可能的值：

- ▶ 勾选
筛选器已激活。
- ▶ 未勾选（默认设置）
筛选器已停用。

Xmas filter

激活/停用 Xmas 筛选器。

设备检测并丢弃具有以下属性的传入 TCP 数据包：

- ▶ 同时设置了 TCP 标志 *FIN*、*URG* 和 *PSH*。
- ▶ TCP 序列号为 0。

可能的值：

- ▶ 勾选
筛选器已激活。
- ▶ 未勾选（默认设置）
筛选器已停用。

SYN/FIN filter

激活/停用 SYN/FIN 筛选器。

设备会检测并丢弃同时设置了 TCP 标志 *SYN* 和 *FIN* 的传入数据包。

可能的值：

- ▶ 勾选
筛选器已激活。
- ▶ 未勾选（默认设置）
筛选器已停用。

TCP Offset protection

激活/停用 TCP 偏移量保护。

TCP 偏移量保护会检测并丢弃其 IP 报头的片段偏移字段等于 1 的传入 TCP 数据包。

TCP 偏移量保护会接受其 IP 报头的片段偏移字段等于 1 的 UDP 和 ICMP 数据包。

可能的值：

- ▶ 勾选
保护已激活。
- ▶ 未勾选（默认设置）
保护已停用。

TCP SYN protection

激活/停用 TCP SYN 保护。

TCP SYN 保护会检测并丢弃设置了 TCP 标志 SYN 且有一个第四层源端口 <1024 的传入数据包。

可能的值：

- ▶ 勾选
保护已激活。
- ▶ 未勾选（默认设置）
保护已停用。

L4 Port protection

激活/停用第四层端口保护。

第四层端口保护会检测并丢弃其源端口编号与目标端口编号相同的传入 TCP 和 UDP 数据包。

可能的值：

- ▶ 勾选
保护已激活。
- ▶ 未勾选（默认设置）
保护已停用。

IP

此框可用于激活或停用着陆攻击筛选器。使用着陆攻击方法，攻击站点会发送其源地址和目标地址与接收者的源地址和目标地址相同的数据包。激活此筛选器之后，设备会检测并丢弃具有相同源地址和目标地址的数据包。

Land Attack filter

激活/停用着陆攻击筛选器。

着陆攻击筛选器会检测并丢弃具有相同源 IP 地址和目标 IP 地址的传入 IP 数据包。

可能的值：

- ▶ 勾选
筛选器已激活。
- ▶ 未勾选（默认设置）
筛选器已停用。

ICMP

此对话框为以下 ICMP 参数提供了筛选器选项：

- ▶ 分片数据包
- ▶ 特定大小以上的 ICMP 数据包
- ▶ 广播 ping

Filter fragmented packets

激活/停用分片 ICMP 数据包的筛选器。

该筛选器检测并丢弃分片 ICMP 数据包。

可能的值：

- ▶ 勾选
筛选器已激活。
- ▶ 未勾选（默认设置）
筛选器已停用。

Filter by packet size

激活/停用传入 ICMP 数据包的筛选器。

该筛选器检测并丢弃其有效负载大小超过 *Allowed payload size [byte]* 字段中指定的大小的 ICMP 数据包。

可能的值：

- ▶ 勾选
筛选器已激活。
- ▶ 未勾选（默认设置）
筛选器已停用。

Allowed payload size [byte]

指定 ICMP 数据包的最大允许有效负载大小（字节）。

如果您希望设备丢弃其有效负载大小超过了 ICMP 数据包的最大允许大小的发入数据包，请勾选 *Filter by packet size* 复选框。

可能的值：

- ▶ 0..1472（默认设置：512）

Drop broadcast ping

激活/停用广播 Ping 的筛选器。广播 Ping 是已知的 Smurf 攻击的证据。

可能的值：

- ▶ 勾选
筛选器已激活。
设备检测并丢弃广播 Ping。
- ▶ 未勾选（默认设置）
筛选器已停用。

Information

Packets dropped

显示设备丢弃的数据包的数量。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

4.6 DHCP Snooping

[Network Security > DHCP Snooping]

DHCP 窥探功能支持网络安全。DHCP 窥探可监控 DHCP 客户端与 DHCP 服务器之间的 DHCP 数据包，并充当不安全的主机与安全的 DHCP 服务器之间的防火墙。

用户可在此对话框中配置和监控以下设备属性：

- ▶ 对来自不可信来源的 DHCP 数据包进行验证并筛选出无效的数据包。
- ▶ 限制来自可信来源和不可信来源的 DHCP 数据流量。
- ▶ 设置和更新 DHCP 窥探绑定数据库。此数据库包含处于不可信端口的 DHCP 客户端的 MAC 地址、IP 地址、VLAN 和端口。
- ▶ 在 DHCP 窥探绑定数据库的基础上，对来自不可信主机的后续请求进行验证。

用户可以全局激活 DHCP 窥探，也可以为特定 VLAN 激活 DHCP 窥探。用户可指定各个端口上的安全状态（可信或不可信）。验证是否能够通过可信端口访问 DHCP 服务器。对于 DHCP 窥探，用户通常会将用户/客户端端口配置为不可信，并将上行链路端口配置为可信。

该菜单包含以下对话框：

- ▶ DHCP Snooping Global
- ▶ DHCP Snooping Configuration
- ▶ DHCP Snooping Statistics
- ▶ DHCP Snooping Bindings

4.6.1 DHCP Snooping Global

[Network Security > DHCP Snooping > Global]

此对话框可用于为用户的设备配置全局 DHCP 窥探参数。

- ▶ 全局激活/停用 *DHCP Snooping*。
- ▶ 全局激活/停用 *Auto-Disable*。
- ▶ 启用/禁用源 MAC 地址检查。
- ▶ 配置绑定数据库的名称、存储位置和存储间隔。

Operation

Operation

全局启用/禁用 DHCP 窥探功能。

可能的值：

- ▶ *On*
- ▶ *Off* (默认设置)

Configuration

Verify MAC

激活/停用以太网数据包中的源 MAC 地址验证。

可能的值：

- ▶ 勾选
源 MAC 地址验证已激活。
设备将源 MAC 地址与收到的 DHCP 数据包中的客户端的 MAC 地址进行比较。
- ▶ 未勾选 (默认设置)
源 MAC 地址验证已停用。

Auto-disable

激活/停用 *DHCP Snooping* 的 *Auto-Disable* 功能。

可能的值：

- ▶ 勾选
DHCP Snooping 的 *Auto-Disable* 功能已激活。
此外，也为相关端口勾选 *Network Security > DHCP Snooping > Configuration* 对话框 *Port* 选项卡 *Auto-disable* 列中的复选框。
- ▶ 未勾选 (默认设置)
DHCP Snooping 的 *Auto-Disable* 功能已停用。

Binding database

Remote file name

指定文件的名称，设备会在其中保存 DHCP 窥探绑定数据库。

提示：

设备在持久绑定数据库中仅保存动态绑定。设备在配置概要文件中保存静态绑定。

Remote IP address

指定远程 IP 地址，设备会将持久性 DHCP 窥探绑定数据库保存在该地址下。对于值 `0.0.0.0`，设备在本地保存绑定数据库。

可能的值：

- ▶ 有效的 IPv4 地址
- ▶ `0.0.0.0`（默认设置）
设备在本地保存 DHCP 窥探绑定数据库。

Store interval [s]

指定当设备识别到数据库中的更改时，设备保存 DHCP 窥探绑定数据库之前经过的时间延迟（秒）。

可能的值：

- ▶ `15..86400`（默认设置：300）

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

4.6.2 DHCP Snooping Configuration

[Network Security > DHCP Snooping > Configuration]

用户可使用此对话框为各个端口和各个 VLAN 配置 DHCP 窥探。

该对话框包含以下选项卡：

- ▶ [Port]
- ▶ [VLAN ID]

[Port]

在此选项卡中，可以为各个端口配置 *DHCP Snooping* 功能。

- ▶ 将端口配置为可信/不可信。
- ▶ 激活/停用各个端口的无效数据库包的日志记录。
- ▶ 限制 DHCP 数据库的数量。
- ▶ 如果 DHCP 数据库流量超过指定的限制，则自动停用端口。

表格

Port

显示端口编号。

Trust

激活/停用端口的安全状态（可信、不可信）。

在此功能激活后，端口将被配置为可信。通常，用户已将可信端口连接到 DHCP 服务器。

在此功能停用后，端口将被配置为不可信。

可能的值：

- ▶ **勾选**
该端口被指定为可信。DHCP 窥探通过可信端口转发允许的客户端数据包。
- ▶ **未勾选**（默认设置）
该端口被配置为不可信。在不可信端口上，设备将接收器端口与绑定数据库中的客户端端口进行比较。

Log

激活/停用设备在此端口上确定的无效数据库的日志记录。

可能的值：

- ▶ **勾选**
无效数据包的日志记录已激活。
- ▶ **未勾选**（默认设置）
无效数据包的日志记录已停用。

Rate limit

指定此端口的每个突发间隔的最大 DHCP 数据包数量。如果传入 DHCP 数据包的数量当前超过在突发间隔中指定的限制，则设备会丢弃更多传入 DHCP 数据包。

可能的值：

- ▶ -1（默认设置）
停用此端口上每个突发间隔的 DHCP 数据包数量的限制。
- ▶ 每个间隔 0..150 个数据包
限制此端口上每个突发间隔的最大 DHCP 数据包数量。

可在 *Burst interval* 列中指定突发间隔。

如果用户激活自动禁用功能，则设备也会禁用该端口。可在 *Auto-disable* 列中找到自动禁用功能。

Burst interval

指定此端口上的突发间隔的长度（秒）。突发间隔与速率限制功能相关。

可在 *Rate limit* 列中指定每个突发间隔的最大 DHCP 数据包数量。

可能的值：

- ▶ 1..15（默认设置：1）

Auto-disable

为 *DHCP Snooping* 功能在端口上监控的参数激活/停用 *Auto-Disable* 功能。

可能的值：

- ▶ 勾选（默认设置）
端口上的 *Auto-Disable* 功能已激活。
前提条件是已勾选 *Network Security > DHCP Snooping > Global* 对话框 *Auto-disable* 框中的 *Configuration* 复选框。
 - 如果端口在 *Burst interval* 列中指定的时间内收到的 DHCP 数据包超过在 *Rate limit* 字段中指定的数量，则设备会禁用该端口。端口的“链路状态”LED 指示灯每个周期闪烁 3 次。
 - *Diagnostics > Ports > Auto-Disable* 对话框显示超过参数导致哪些端口当前被禁用。
 - *Auto-Disable* 功能自动重新激活端口。为此，可以切换至 *Diagnostics > Ports > Auto-Disable* 对话框并在 *Reset timer [s]* 列中为相关端口指定等待期。
- ▶ 未勾选
端口上的 *Auto-Disable* 功能已停用。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

[VLAN ID]

用户可在此选项卡中为各个 VLAN 配置 *DHCP Snooping* 功能。

表格

VLAN ID

显示与表格条目相关的 VLAN ID。

Active

激活/停用此 VLAN 中的 *DHCP Snooping* 功能。

DHCP Snooping 功能将有效的 DHCP 客户端消息转发到无 *Routing* 功能的 VLAN 中的可信端口。

可能的值：

▶ 勾选

此 VLAN 中的 *DHCP Snooping* 功能已激活。

▶ 未勾选（默认设置）

此 VLAN 中的 *DHCP Snooping* 功能已停用。

设备根据交换设置转发 DHCP 数据包而不监控数据包。绑定数据库保持不变。

提示： 要为端口启用 DHCP 窥探，请在 *Network Security > DHCP Snooping > Global* 对话框中全局启用 *DHCP Snooping* 功能。验证是否已将端口分配到在其中启用了 DHCP 窥探的 VLAN。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

4.6.3 DHCP Snooping Statistics

[Network Security > DHCP Snooping > Statistics]

设备会利用 DHCP 窥探记录检测到的错误并生成统计数据。用户可在此对话框中监控每个端口的 DHCP 窥探统计数据。

设备记录以下内容：

- ▶ 在验证 DHCP 客户端的 MAC 地址时检测到的错误
- ▶ 通过检测到的不正确端口发送的 DHCP 客户端消息
- ▶ 发送到不可信端口的 DHCP 服务器消息

表格

Port

显示端口编号。

MAC verify failures

显示 DHCP 数据包的“chaddr”字段中的 DHCP 客户端的 MAC 地址与以太网数据包中的源地址之间的差异数量。

Invalid client messages

显示在端口上收到的传入 DHCP 客户端消息的数量，设备会根据 DHCP 窥探绑定数据库预期在另一个端口上收到这些消息。

Invalid server messages

显示在不可信端口上收到的 DHCP 服务器消息的数量。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

Reset

重置整个表格。

4.6.4 DHCP Snooping Bindings

[Network Security > DHCP Snooping > Bindings]

DHCP 窥探使用 DHCP 消息来设置和更新绑定数据库。

- ▶ 静态绑定
设备允许用户在数据库中输入最多 256 个静态 DHCP 窥探绑定。
- ▶ 动态绑定
动态绑定数据库仅包含不可信端口上的客户端的数据库。

此菜单可用于指定静态和动态绑定的设置。

- ▶ 设置新的静态绑定并将其设置为激活/停用。
- ▶ 显示、激活/停用或删除已设置的静态绑定。

表格

MAC address

指定绑定到 *IP address* 和 *VLAN ID* 的表格条目中的 MAC 地址。

可能的值:

- ▶ 有效单播 MAC 地址
使用冒号分隔符指定值, 如 00:11:22:33:44:55。

IP address

指定静态 DHCP 窥探绑定的 IP 地址。

可能的值:

- ▶ 小于 224.x.x.x 并且在 127.0.0.0/8 范围以外的有效单播 IPv4 地址 (默认设置: 0.0.0.0)

VLAN ID

指定对其应用了表格条目的 VLAN 的 ID。

可能的值:

- ▶ <已设置的 VLAN 的 ID>

Port

指定用于静态 DHCP 窥探绑定的端口。

可能的值:

- ▶ 可用的端口

Remaining binding time

显示动态 DHCP 窥探绑定的剩余时间。

Active

激活/停用指定的静态 DHCP 窥探绑定。

可能的值：

- ▶ **勾选**
静态 DHCP 窥探绑定已激活。
- ▶ **未勾选**（默认设置）
静态 DHCP 窥探绑定已停用。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。



打开 *Create* 窗口，向表格中添加一个新的条目。

在 *MAC address* 字段中，指定绑定到 IP 地址和 VLAN ID 的 MAC 地址。



删除突出显示的表格条目。

前提条件是 *Active* 列中的复选框为未勾选。

此外，设备还会删除通过 *IP Source Guard* 功能创建的此端口的动态绑定。

4.7 IP Source Guard

[Network Security > IP Source Guard]

IP Source Guard (IPSG) 功能支持网络安全。该功能根据用户的源 ID（源 IP 地址或源 MAC 地址）筛选 IP 数据包。IPSG 可支持用户保护网络免遭通过 IP/MAC 地址欺骗进行的攻击。

IPSG 和 DHCP 窥探

IP 源保护与端口 *DHCP Snooping* 功能一起发挥作用。

DHCP Snooping 丢弃不可信端口上的 IP 数据包，DHCP 消息除外。当设备收到 DHCP 响应并且已设置 DHCP 窥探绑定数据库时，设备会为每个包含用户的源 ID 的端口创建 VLAN 访问控制列表 (VAACL)。

可在 *Network Security > DHCP Snooping > Configuration* 对话框中为各个端口和各个 VLAN 配置 *DHCP Snooping* 功能的参数。

IPSG 和端口安全

IP Source Guard 与 *Port Security* 功能合作。参见 *Network Security > Port Security* 对话框。在收到请求后，IPSG 会根据请求向 *Port Security* 功能通知某个 MAC 地址是否属于有效的绑定。

- ▶ 如果用户停用入口端口上的 IPSG，则 IPSG 会将数据包识别为有效。
- ▶ 如果用户激活入口端口上的 IPSG，则 IPSG 会使用绑定数据库来检查 MAC 地址。如果在绑定数据库中输入了 MAC 地址，则 IPSG 会将数据包识别为有效，否则为无效。

Port Security 功能接管无效数据包的后续处理。可在 *Network Security > Port Security*对话框中指定 *Port Security* 功能的设置。

提示：为使设备检查在端口上收到的数据包的 IP 地址和 MAC 地址，请启用 *Verify MAC* 功能。

为使设备在转发数据包之前检查源的 VLAN ID 和 MAC 地址，另请启用 *Port Security* 功能。参见 *Network Security > Port Security* 对话框。

该菜单包含以下对话框：

- ▶ *IP Source Guard Port*
- ▶ *IP Source Guard Bindings*

4.7.1 IP Source Guard Port

[Network Security > IP Source Guard > Port]

此对话框可用于显示和配置每个端口的以下设备属性：

- ▶ 在筛选中包括/排除 MAC 地址。
- ▶ 激活/停用 *IP Source Guard* 功能。

表格

Port

显示端口编号。

Verify MAC

如果 *IP Source Guard* 功能已激活，则激活/停用基于源 MAC 地址的筛选。除了基于源 IP 地址的筛选，设备还会执行此筛选。

可能的值：

- ▶ 勾选
基于源 MAC 地址的筛选已激活。
要激活该功能，请勾选 *Active* 复选框。
- ▶ 未勾选（默认设置）
基于源 MAC 地址的筛选已停用。
如需停用该功能，还要取消勾选 *Active* 复选框。

Active

激活/停用端口上的 *IP Source Guard* 功能。

可能的值：

- ▶ 勾选
IP Source Guard 功能激活。
还可在 *Network Security > DHCP Snooping > Global* 对话框中启用 *DHCP Snooping* 功能。
- ▶ 未勾选（默认设置）
IP Source Guard 功能停用。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

4.7.2 IP Source Guard Bindings

[Network Security > IP Source Guard > Bindings]

此对话框显示静态和动态 IP 源保护绑定。

- ▶ 设备通过 DHCP 窥探来学习动态绑定。参见 [Network Security > DHCP Snooping > Configuration](#) 对话框。
- ▶ 静态绑定是由用户手动设置的 IP 源保护绑定。该对话框可用于编辑静态绑定。

表格

MAC address

显示绑定的 MAC 地址。

IP address

显示服务器的 IP 地址。

VLAN ID

显示绑定的 VLAN ID。

Port

显示绑定的端口的编号。

Hardware status

显示绑定的硬件状态。

仅当设置正确时，设备才会将绑定应用于硬件。在将静态 IPSPG 绑定应用于硬件之前，设备会检查以下前提条件：

- *Active* 复选框已勾选。
- 端口上的 *IP Source Guard* 功能已激活，已勾选 [Network Security > IP Source Guard > Port](#) 对话框中的 *Active* 复选框。

可能的值：

- ▶ *勾选*
绑定已激活，设备会将绑定应用于硬件。
- ▶ *未勾选*
绑定已停用。

Active

针对在指定的端口上指定的 VLAN，激活/停用指定的 MAC 地址与指定的 IP 地址之间指定的静态 IPSPG 绑定。

可能的值：

- ▶ **勾选**
静态 IPSPG 绑定已激活。
- ▶ **未勾选**（默认设置）
静态 IPSPG 绑定已停用。

提示：要使静态绑定生效，请在相应的端口上激活 *IP Source Guard* 功能。在 *Network Security > IP Source Guard > Port* 对话框中，勾选 *Active* 复选框。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。



打开 *Create* 窗口，向表格中添加一个新的条目。

- ▶ 在 *MAC address* 字段中，可以指定静态绑定的 MAC 地址。
- ▶ 在 *IP address* 字段中，可以指定静态绑定的 IP 地址。
- ▶ 在 *VLAN ID* 字段中，可以指定 VLAN ID。
- ▶ 在 *Port* 字段中，可以指定 VLAN 的 ID。



删除突出显示的表格条目。

前提条件是 *Active* 列中的复选框为未勾选。

4.8 Dynamic ARP Inspection

[*Network Security > Dynamic ARP Inspection*]

Dynamic ARP Inspection 功能支持网络安全。此功能可对 ARP 数据包进行分析、记录并丢弃无效和恶意的 ARP 数据包。

Dynamic ARP Inspection 功能可帮助防止一系列中间人攻击。恶意站通过此类攻击对保护不足的邻居之 ARP 缓存进行侵占，并窃听来自其他用户的数据流量。恶意站会发送 ARP 请求和 ARP 响应，并在 IP 与 MAC 地址关系（绑定）中，为其自己的 MAC 地址输入其他用户的 IP 地址。

通过使用以下措施，*Dynamic ARP Inspection* 功能可帮助确保设备仅转发有效的 ARP 请求和 ARP 响应。

- ▶ 窃听不可信端口上的 ARP 请求和 ARP 响应。
- ▶ 在设备更新本地 ARP 缓存和设备将数据包转发到相关的目标地址之前，验证已确定的数据包是否具备有效的 IP 与 MAC 地址关系（绑定）。
- ▶ 丢弃无效的 ARP 数据包。

设备允许指定最多 100 个活动的 ARP ACL（访问控制列表）。用户可为每个 ARP ACL 激活最多 20 条规则。

该菜单包含以下对话框：

- ▶ *Dynamic ARP Inspection Global*
- ▶ *Dynamic ARP Inspection Configuration*
- ▶ *Dynamic ARP Inspection ARP Rules*
- ▶ *Dynamic ARP Inspection Statistics*

4.8.1 Dynamic ARP Inspection Global

[Network Security > Dynamic ARP Inspection > Global]

Configuration

Verify source MAC

激活/停用源 MAC 地址验证。设备在 ARP 请求和 ARP 响应中执行检查。

可能的值：

▶ **勾选**

源 MAC 地址验证已激活。

设备检查收到的 ARP 数据包的源 MAC 地址。

- 设备将具备有效的源 MAC 地址的 ARP 数据包传输到相关的目标地址并更新本地 ARP 缓存。
- 设备丢弃具有无效的源 MAC 地址的 ARP 数据包。

▶ **未勾选**（默认设置）

源 MAC 地址验证已停用。

Verify destination MAC

激活/停用目标 MAC 地址验证。设备在 ARP 响应中执行检查。

可能的值：

▶ **勾选**

目标 MAC 地址验证已激活。

设备检查传入 ARP 数据包的目标 MAC 地址。

- 设备将具备有效的目标 MAC 地址的 ARP 数据包传输到相关的目标地址并更新本地 ARP 缓存。
- 设备丢弃具有无效目标 MAC 地址的 ARP 数据包。

▶ **未勾选**（默认设置）

传入 ARP 数据包的目标 MAC 地址检查已激活。

Verify IP address

激活/停用 IP 地址验证。

在 ARP 请求中，设备会检查源 IP 地址。在 ARP 响应中，设备会检查目标和源 IP 地址。

设备将以下 IP 地址指定为无效：

- 0.0.0.0
- 广播地址 255.255.255.255
- 多播地址 224.0.0.0/4（类别 D）
- 类别 E 地址 240.0.0.0/4（保留用于后续用途）
- 127.0.0.0/8 范围中的环回地址。

可能的值：

▶ **勾选**

IP 地址验证已激活。

设备检查传入 ARP 数据包的 IP 地址。设备将具备有效 IP 地址的 ARP 数据包传输到相关的目标地址并更新本地 ARP 缓存。设备丢弃具有无效 IP 地址的 ARP 数据包。

▶ **未勾选**（默认设置）

IP 地址验证已停用。

Auto-disable

激活/停用 *Dynamic ARP Inspection* 的 *Auto-Disable* 功能。

可能的值：

▶ 勾选

Dynamic ARP Inspection 的 *Auto-Disable* 功能已激活。

此外，也为相关端口勾选 *Network Security > Dynamic ARP Inspection > Configuration* 对话框 *Auto-disable* 选项卡 *Port* 列中的复选框。

▶ 未勾选（默认设置）

Dynamic ARP Inspection 的 *Auto-Disable* 功能已停用。

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

4.8.2 Dynamic ARP Inspection Configuration

[Network Security > Dynamic ARP Inspection > Configuration]

该对话框包含以下选项卡：

- ▶ [Port]
- ▶ [VLAN ID]

[Port]

表格

Port

显示端口编号。

Trust

激活/停用不可信端口上的 ARP 数据包监控。

可能的值：

- ▶ 勾选
监控已激活。
设备监控不可信端口上的 ARP 数据包。
设备立即转发可信端口上的 ARP 数据包。
- ▶ 未勾选（默认设置）
监控已停用。

Rate limit

指定此端口上每个间隔的最大 ARP 数据包数量。如果传入 ARP 数据包的速率当前超过在突发间隔中指定的限制，则设备会丢弃更多传入 ARP 数据包。可在 *Burst interval* 列中指定突发间隔。

或者，如果用户已激活自动禁用功能，设备还会停用该端口。可在 *Auto-disable* 列中启用/禁用 *Auto-Disable* 功能。

可能的值：

- ▶ -1（默认设置）
停用此端口上每个突发间隔的 ARP 数据包数量的限制。
- ▶ 每个间隔 0..300 个数据包
限制此端口上每个突发间隔的最大 ARP 数据包数量。

Burst interval

指定此端口上的突发间隔的长度（秒）。突发间隔与速率限制功能相关。

可在 *Rate limit* 列中指定每个突发间隔的最大 ARP 数据包数量。

可能的值：

- ▶ 1..15（默认设置：1）

Auto-disable

为 *Dynamic ARP Inspection* 功能在端口上监控的参数激活/停用 *Auto-Disable* 功能。

可能的值：

- ▶ 勾选（默认设置）

端口上的 *Auto-Disable* 功能已激活。

前提是已勾选 *Network Security > Dynamic ARP Inspection > Global* 对话框 *Auto-disable* 框中的 *Configuration* 复选框。

- 如果端口在 *Burst interval* 列中指定的时间内收到的 ARP 数据包超过在 *Rate limit* 字段中指定的数量，则设备会禁用该端口。端口的“链路状态”LED 指示灯每个周期闪烁 3 次。
- *Diagnostics > Ports > Auto-Disable* 对话框显示超过参数导致哪些端口当前被禁用。
- *Auto-Disable* 功能自动重新激活端口。为此，可以切换至 *Diagnostics > Ports > Auto-Disable* 对话框并在 *Reset timer [s]* 列中为相关端口指定等待期。

- ▶ 未勾选

端口上的 *Auto-Disable* 功能已停用。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

[VLAN ID]

表格

VLAN ID

显示与表格条目相关的 VLAN ID。

Log

激活/停用设备在此 VLAN 中确定的无效 ARP 数据包的日志记录。如果设备在检查 IP、源 MAC 或目标 MAC 地址或者 IP 与 MAC 地址关系（绑定）时检测到错误，则设备会将 ARP 数据包识别为无效。

可能的值：

- ▶ 勾选

无效数据包的日志记录已激活。
设备注册无效的 ARP 数据包。

- ▶ 未勾选（默认设置）

无效数据包的日志记录已停用。

Binding check

激活/停用设备在不可信端口上和 *Dynamic ARP Inspection* 功能已激活的 VLAN 上收到的传入 ARP 数据包的检查。对于这些 ARP 数据包，设备会检查 ARP ACL 与 DHCP 窥探关系（绑定）。

可能的值：

- ▶ **勾选**（默认设置）
ARP 数据包的绑定检查已激活。
- ▶ **未勾选**
ARP 数据包的绑定检查已停用。

ACL strict

激活/停用基于指定的 ARP ACL 规则的传入 ARP 数据包的严格检查。

可能的值：

- ▶ **勾选**
严格检查已激活。
设备根据在 *ARP ACL* 列中指定的 ARP ACL 规则来检查传入 ARP 数据包。
- ▶ **未勾选**（默认设置）
严格检查已停用。
设备根据在 *ARP ACL* 列中指定的 ARP ACL 规则，然后根据 DHCP 窥探数据库中的条目来检查传入 ARP 数据包。

ARP ACL

指定设备使用的 ARP ACL。

可能的值：

- ▶ **<规则名称>**
可在 *Network Security > Dynamic ARP Inspection > ARP Rules* 对话框中创建和编辑规则。

Active

激活/停用此 VLAN 中的 *Dynamic ARP Inspection* 功能。

可能的值：

- ▶ **勾选**
此 VLAN 中的 *Dynamic ARP Inspection* 功能已激活。
- ▶ **未勾选**（默认设置）
此 VLAN 中的 *Dynamic ARP Inspection* 功能已停用。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

4.8.3 Dynamic ARP Inspection ARP Rules

[Network Security > Dynamic ARP Inspection > ARP Rules]

用户可使用此对话框指定用于检查和筛选 ARP 数据包的规则。

表格

Name

显示 ARP 规则的名称。

Source IP address

指定设备向其应用规则的 IP 数据包的源地址。

可能的值：

- ▶ 有效的 IPv4 地址
设备将规则应用于具有指定源地址的 IP 数据包。

Source MAC address

指定设备向其应用规则的 MAC 数据包的源地址。

可能的值：

- ▶ 有效 MAC 地址
设备将规则应用于具有指定源地址的 MAC 数据包。

Active

激活/停用 ARP 规则。

可能的值：

- ▶ 勾选（默认设置）
规则已激活。
- ▶ 未勾选
规则已停用。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。



打开 *Create* 窗口，向表格中添加一个新的条目。

- ▶ 在 *Name* 字段中，可以指定 ARP 规则的名称。
- ▶ 在 *Source IP address* 字段中，可以指定 ARP 规则的源 IP 地址。
- ▶ 在 *Source MAC address* 字段中，可以指定 ARP 规则的源 MAC 地址。

4.8.4 Dynamic ARP Inspection Statistics

[Network Security > Dynamic ARP Inspection > Statistics]

此窗口会在概览中显示已丢弃和已转发的 ARP 数据包。

表格

VLAN ID

显示与表格条目相关的 VLAN ID。

Packets forwarded

显示设备在使用 *Dynamic ARP Inspection* 功能来检查 ARP 数据包之后转发的 ARP 数据包的数量。

Packets dropped

显示设备在使用 *Dynamic ARP Inspection* 功能来检查 ARP 数据包之后丢弃的 ARP 数据包的数量。

DHCP drops

显示设备在检查 DHCP 窥探关系（绑定）之后丢弃的 ARP 数据包的数量。

DHCP permits

显示设备在检查 DHCP 窥探关系（绑定）之后转发的 ARP 数据包的数量。

ACL drops

显示设备在使用 ARP ACL 规则来检查 ARP 数据包之后丢弃的 ARP 数据包的数量。

ACL permits

显示设备在使用 ARP ACL 规则来检查 ARP 数据包之后转发的 ARP 数据包的数量。

Bad source MAC

显示设备在 *Dynamic ARP Inspection* 功能检测到源 MAC 地址中的错误之后丢弃的 ARP 数据包的数量。

Bad destination MAC

显示设备在 *Dynamic ARP Inspection* 功能检测到目标 MAC 地址中的错误之后丢弃的 ARP 数据包的数量。

Invalid IP address

显示设备在 *Dynamic ARP Inspection* 功能检测到 IP 地址中的错误之后丢弃的 ARP 数据包的数量。

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

Reset

重置整个表格。

4.9 ACL

[Network Security > ACL]

在此菜单中，可以指定访问控制列表（ACL）的设置。访问控制列表包含了设备依次应用于其端口或 VLAN 上的数据流的规则。

如果数据包符合一个或多个规则的标准，则设备应用在应用于数据流的第一个规则中指定的操作。设备忽略其后的规则。可能的操作包括：

- ▶ *permit*: 设备将数据包传输到端口或 VLAN。
- ▶ *deny*: 设备丢弃数据包。

在默认设置下，设备对每个数据包都进行转发。一旦将访问控制列表分配给接口或 VLAN，这种行为就会改变。设备在访问控制列表的末尾输入一个隐式 Deny-All 规则。因此，设备丢弃不符合其中任一规则的数据包。如果想要得到不同的行为，可在访问控制列表的末尾添加一个“允许”规则。

请按照以下步骤进行操作，设置访问控制列表和规则：

- 创建一个规则并指定规则设置。参见 *Network Security > ACL > IPv4 Rule* 对话框或 *Network Security > ACL > MAC Rule* 对话框。
- 将该访问控制列表分配给设备的端口和 VLAN。参见 *Network Security > ACL > Assignment* 对话框。

该菜单包含以下对话框：

- ▶ ACL IPv4 Rule
- ▶ ACL MAC Rule
- ▶ ACL Assignment

4.9.1 ACL IPv4 Rule

[Network Security > ACL > IPv4 Rule]

在此对话框中，可以指定设备应用于 IP 数据包的规则。

一个访问控制列表（组）包含一个或多个规则。设备依次应用访问控制列表的规则，首先应用 *Index* 列中数值最小的规则。

设备允许用户按照以下标准进行筛选：

- ▶ 数据包的源或目标 IP 地址
- ▶ 传输协议的类型
- ▶ 数据包的源或目标端口

表格

Group name

显示访问控制列表的名称。访问控制列表包含规则。

Index

显示访问控制列表中规则的数量。

如果访问控制列表包含多个规则，则设备首先处理数值最小的规则。

Match every packet

指定设备将规则应用于哪些 IP 数据包。

可能的值：

- ▶ 勾选（默认设置）
设备将规则应用于每个 IP 数据包。
- ▶ 未勾选
设备根据 *Source IP address*、*Destination IP address* 和 *Protocol* 字段中的值将规则应用于 IP 数据包。

Source IP address

指定设备向其应用规则的 IP 数据包的源地址。

可能的值：

- ▶ *?.?.?.?*（默认设置）
设备将规则应用于具有任何源地址的 IP 数据包。
- ▶ 有效的 IPv4 地址
设备将规则应用于具有指定源地址的 IP 数据包。
可以使用 *?* 字符作为通配符。
示例 *192.?.?.32*：设备将规则应用于源地址以 *192.* 开始并以 *.32* 结束的 IP 数据包。
- ▶ 有效的 IPv4 地址/位掩码
设备将规则应用于具有指定源地址的 IP 数据包。反位掩码允许用户指定具有位级精度的地址范围。
示例 *192.168.1.0/0.0.0.127*：设备将规则应用于源地址在 *192.168.1.0* 到 *...127* 范围内的 IP 数据包。

Destination IP address

指定设备向其应用规则的 IP 数据包的目标地址。

可能的值：

- ▶ `?.?.?.?`（默认设置）
设备将规则应用于具有任意目标地址的数据包。
- ▶ 有效的 IPv4 地址
设备将规则应用于具有指定的目标地址的数据包。
可以使用 `?` 字符作为通配符。
示例 `192.?.?.32`：设备将规则应用于源地址以 `192.` 开始并以 `.32` 结束的 IP 数据包。
- ▶ 有效的 IPv4 地址/位掩码
设备将规则应用于具有指定的目标地址的数据包。反位掩码允许用户指定具有位级精度的地址范围。
示例 `192.168.1.0/0.0.0.127`：设备将规则应用于目标地址在 `192.168.1.0` 到 `...127` 范围内的 IP 数据包。

Protocol

指定设备向其应用规则的 IP 数据包的协议类型。

可能的值：

- ▶ `any`（默认设置）
设备不考虑协议类型将规则应用于每个 IP 数据包。
- ▶ `icmp`
- ▶ `igmp`
- ▶ `ip-in-ip`
- ▶ `tcp`
- ▶ `udp`
- ▶ `ip`

Source TCP/UDP port

指定设备向其应用规则的 IP 数据包的源端口。前提条件是用户在 *Protocol* 列中指定值 `TCP` 或 `UDP`。

可能的值：

- ▶ `any`（默认设置）
设备不考虑源端口将规则应用于每个 IP 数据包。
- ▶ `1..65535`
设备将规则只应用于包含指定源端口的 IP 数据包。

Destination TCP/UDP port

指定设备向其应用规则的 IP 数据包的目标端口。前提条件是用户在 *Protocol* 列中指定值 `TCP` 或 `UDP`。

可能的值：

- ▶ `any`（默认设置）
设备不考虑目标端口将规则应用于每个 IP 数据包。
- ▶ `1..65535`
设备将规则只应用于包含指定目标端口的 IP 数据包。

Action

指定当设备应用规则时设备如何处理收到的 IP 数据包。

可能的值：

- ▶ *permit*（默认设置）
设备传输 IP 数据包。
- ▶ *deny*
设备丢弃 IP 数据包。

Log

激活/停用日志文件记录。参见 *Diagnostics > Report > System Log* 对话框。

可能的值：

- ▶ 勾选
记录激活。
前提条件是用户在 *Network Security > ACL > Assignment* 对话框中向 VLAN 或端口分配访问控制列表。
设备以 30 秒间隔在日志文件中注册向 IP 数据包应用拒绝规则的次数。
- ▶ 未勾选（默认设置）
记录停用。

设备允许用户为最多 128 条拒绝规则激活此功能。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。



打开 *Create* 窗口，向表格中添加一个新的条目。

- ▶ 在 *Group name* 字段中，可以指定规则所属的访问控制列表的名称。
- ▶ 在 *Index* 字段中，可以指定访问控制列表中规则的数量。如果访问控制列表包含多个规则，则设备首先处理数值最小的规则。

4.9.2 ACL MAC Rule

[Network Security > ACL > MAC Rule]

在此对话框中，可以指定设备应用于 MAC 数据包的规则。

一个访问控制列表（组）包含一个或多个规则。设备依次应用访问控制列表的规则，首先应用 *Index* 列中数值最小的规则。

设备允许用户对数据包的源或目标 MAC 地址进行筛选。

表格

Group name

显示访问控制列表的名称。访问控制列表包含规则。

Index

显示访问控制列表中规则的数量。

如果访问控制列表包含多个规则，则设备首先处理数值最小的规则。

Match every packet

指定设备将规则应用于哪些 MAC 数据包。

可能的值：

- ▶ **勾选**（默认设置）
设备将规则应用于每个 MAC 数据包。
- ▶ **未勾选**
设备根据 *Source MAC address* 和 *Destination MAC address* 字段中的值将规则应用于 MAC 数据包。

Source MAC address

指定设备向其应用规则的 MAC 数据包的源地址。

可能的值：

- ▶ **?:?:?:?:?:?:?:?**（默认设置）
设备将规则应用于具有任何源地址的MAC 数据包。
- ▶ **有效 MAC 地址**
设备将规则应用于具有指定源地址的 MAC 数据包。
可以使用 ? 字符作为通配符。
示例 **00:11:?:?:?:?:?**：设备将规则应用于源地址以 **00:11** 开始的 MAC 数据包。
- ▶ **有效的 MAC 地址/位掩码**
设备将规则应用于具有指定源地址的 MAC 数据包。位掩码允许用户指定具有位级精度的地址范围。
示例 **00:11:22:33:44:54/FF:FF:FF:FF:FF:FC**：设备将规则应用于源地址在 **00:11:22:33:44:54** 到 **...:57** 范围内的 MAC 数据包。

Destination MAC address

指定设备向其应用规则的 MAC 数据包的目标地址。

可能的值：

- ▶ `?:?:?:?:?:?:?`（默认设置）
设备将规则应用于具有任何目标地址的 MAC 数据包。
- ▶ 有效 MAC 地址
设备将规则应用于具有指定目标地址的 MAC 数据包。
可以使用 `?` 字符作为通配符。
示例 `00:11:?:?:?:?:?`：设备将规则应用于目标地址以 `00:11` 开始的 MAC 数据包。
- ▶ 有效的 MAC 地址/位掩码
设备将规则应用于具有指定源地址的 MAC 数据包。位掩码允许用户指定具有位级精度的地址范围。
示例 `00:11:22:33:44:54/FF:FF:FF:FF:FF:FC`：设备将规则应用于目标地址在 `00:11:22:33:44:54` 到 `...:57` 范围内的 MAC 数据包。

Action

指定当设备应用规则时设备如何处理收到的MAC数据包。

可能的值：

- ▶ `permit`（默认设置）
设备传输 MAC 数据包。
- ▶ `deny`
设备丢弃 MAC 数据包。

Log

激活/停用日志文件记录。参见 [Diagnostics > Report > System Log](#) 对话框。

可能的值：

- ▶ 勾选
记录激活。
前提条件是用户在 [Network Security > ACL > Assignment](#) 对话框中向 VLAN 或端口分配访问控制列表。
设备以 30 秒间隔在日志文件中注册向 MAC 数据包应用拒绝规则的次数。
- ▶ 未勾选（默认设置）
记录停用。

设备允许用户为最多 128 条拒绝规则激活此功能。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。



打开 `Create` 窗口，向表格中添加一个新的条目。

- ▶ 在 `Group name` 字段中，可以指定规则所属的访问控制列表的名称。
- ▶ 在 `Index` 字段中，可以指定访问控制列表中规则的数量。如果访问控制列表包含多个规则，则设备首先处理数值最小的规则。

4.9.3 ACL Assignment

[Network Security > ACL > Assignment]

此对话框允许用户向设备的端口和 VLAN 分配一个或多个访问控制列表。通过分配优先级，可以指定处理顺序，条件是，向端口或 VLAN 分配一个或多个访问控制列表。

设备按照规则索引中指定的顺序依次应用规则。可在 *Priority* 列中指定一个组的优先级。数字越小，优先级越高。在此过程中，设备首先应用优先级较高的规则，然后再应用优先级较低的规则。

向端口和 VLAN 分配访问控制列表后，会产生以下不同类型的 ACL：

- ▶ 基于端口的 IPv4-ACL
- ▶ 基于端口的 MAC ACL
- ▶ 基于 VLAN 的 IPv4 ACL
- ▶ 基于 VLAN 的 MAC ACL

设备允许将访问控制列表应用于收到的 (*inbound*) 数据包。

提示：在启用该功能之前，请验证表格中是否至少有一个活动条目允许用户访问。否则，如果更改设置，与设备的连接会中断。只有通过设备的串行接口使用 CLI 才能访问设备管理。

表格

Group name

显示访问控制列表的名称。访问控制列表包含规则。

Type

显示访问控制列表是否包含 MAC 规则或 IPv4 规则。

可能的值：

- ▶ *mac*
访问控制列表包含 MAC 规则。
- ▶ *ip*
访问控制列表包含 IPv4 规则。

可以在 *Network Security > ACL > IPv4 Rule* 对话框中对具有 IPv4 规则的访问控制列表进行编辑。

可以在 *Network Security > ACL > MAC Rule* 对话框中对具有 MAC 规则的访问控制列表进行编辑。

Port

显示为其分配了访问控制列表的端口。向 VLAN 分配访问控制列表后，该字段保持为空。

VLAN ID

显示为其分配了访问控制列表的 VLAN。向端口分配访问控制列表后，该字段保持为空。

Direction

显示设备将访问控制列表应用于接收的数据包。

Priority

显示访问控制列表的优先级。

使用优先级，可以指定设备向数据流应用访问控制列表的顺序。设备从优先级 1 开始按升序应用规则。

可能的值：

- ▶ 1..4294967295

如果将访问控制列表分配给具有相同优先级的端口和 VLAN，则设备首先将规则应用于端口。

Active

显示端口上或 VLAN 中的访问控制列表是否已激活。

可能的值：

- ▶ 勾选（默认设置）
访问控制列表已激活。
- ▶ 未勾选
访问控制列表已停用。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。



打开 *Create* 对话框，向端口或 VLAN 分配一个规则。

- ▶ 在 *Port/VLAN* 字段中，可以指定端口或 VLAN ID。
- ▶ 在 *Priority* 字段中，可以指定 ARP 规则的源 MAC 地址。
- ▶ 在 *Direction* 字段中，可以指定设备向其应用规则的数据包。
- ▶ 在 *Group name* 字段中，可以指定设备将哪个规则分配给端口或 VLAN。

5 Switching

该菜单包含以下对话框：

- ▶ Switching Global
- ▶ Rate Limiter
- ▶ Filter for MAC Addresses
- ▶ IGMP Snooping
- ▶ Time-Sensitive Networking
- ▶ MRP-IEEE
- ▶ GARP
- ▶ QoS/Priority
- ▶ VLAN
- ▶ L2-Redundancy

5.1 Switching Global

[Switching > Global]

此对话框可用于指定以下设置：

- ▶ 更改地址表的老化时间
- ▶ 启用设备中的流量控制

如果在一个端口的优先队列中同时接收到大量数据包，则这会导致端口内存溢出。例如，当设备在千兆端口上接收数据并将其转发到带宽较低的端口时，就会发生这种情况。设备会丢弃多余的数据包。

IEEE 802.3 标准中介绍的流量控制机制有助于确保端口内存溢出不会导致数据包丢失。在端口内存完全占满之前不久，设备会示意相连设备注意它不再接受来自这些设备的任何数据包。

- ▶ 在全双工模式下，设备会发送一个暂停数据包。
- ▶ 在半双工模式下，设备会模拟一次冲突。

然后，在示意生效的时间内，相连设备不再发送任何数据包。在上行链路端口上，这可能会导致上一级网段中产生意外的发送中断（“流浪反向压力”）。

Configuration

MAC address

显示设备的 MAC 地址。

Aging time [s]

指定老化时间（秒）。

可能的值：

- ▶ 10..500000（默认设置：30）

设备会监控示教单播 MAC 地址的年龄。设备从其地址表中删除超过特定年龄（老化时间）的地址条目。

可在 *Switching > Filter for MAC Addresses* 对话框中找到地址表。

Flow control

激活/停用设备中的流量控制。

可能的值：

- ▶ 勾选

设备中的流量控制已激活。

进一步激活所需端口上的流量控制。参见 *Basic Settings > Port* 对话框 *Configuration* 选项卡 *Flow control* 列中的复选框。

- ▶ 未勾选（默认设置）

设备中的流量控制已停用。

如果用户正在使用冗余功能，则停用参与端口上的流量控制。如果流量控制和冗余功能同时激活，则冗余功能的运行可能与预期有所不同。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

5.2 Rate Limiter

[Switching > Rate Limiter]

设备允许用户限制端口上的流量，以便在流量较大时仍提供稳定的运行。如果端口上的流量超过输入的流量值，则设备会丢弃此端口上多余的流量。

速率限制器功能只在第二层上工作，用于限制导致设备泛洪的数据包风暴的影响（一般是广播）。

速率限制器功能会忽略处于更高层（例如 IP 或 TCP）的协议信息。

该对话框包含以下选项卡：

▶ [Ingress]

▶ [Egress]

[Ingress]

在此对话框中，可以启用 *Rate Limiter* 功能。阈值指定端口接收的最大流量。如果端口上的流量超过阈值，则设备将丢弃此端口上多余的流量。

表格

Port

显示端口编号。

Threshold unit

指定阈值的单位：

可能的值：

▶ *percent*（默认设置）
将阈值指定为端口数据速率的百分率。

▶ *pps*
以每秒数据包数量为单位指定阈值。

Broadcast mode

为收到的广播数据包激活/停用速率限制器功能。

可能的值：

▶ 勾选

▶ 未勾选（默认设置）

如果超过了阈值，则设备将丢弃此端口上多余的广播数据包。

Broadcast threshold

指定此端口上收到的广播的阈值。

可能的值：

▶ 0.14880000（默认设置：0）

值 0 将停用此端口上的速率限制器功能。

如果用户已在 *Threshold unit* 列中选择值 *percent*，则请输入从 1 到 100 的百分比值。

如果用户已在 *Threshold unit* 列中选择值 *pps*，则请输入数据速率的绝对值。

Known multicast mode

为收到的已知多播数据包激活/停用速率限制器功能。

可能的值：

▶ 勾选

▶ 未勾选（默认设置）

如果超过了阈值，则设备将丢弃此端口上多余的多播数据包。

Known multicast threshold

指定此端口上收到的多播的阈值。

可能的值：

▶ 0.14880000（默认设置：0）

值 0 将停用此端口上的速率限制器功能。

如果用户已在 *Threshold unit* 列中选择值 *percent*，则请输入从 0 到 100 的百分比值。

如果用户已在 *Threshold unit* 列中选择值 *pps*，则请输入数据速率的绝对值。

Unknown frame mode

为收到的带有未知目标地址的单播和多播数据包激活/停用速率限制器功能。

可能的值：

▶ 勾选

▶ 未勾选（默认设置）

如果超过了阈值，则设备将丢弃此端口上多余的单播数据包。

Unknown frame threshold

指定此端口上收到的且带有未知目标地址的单播的阈值。

可能的值：

▶ 0.14880000（默认设置：0）

值 0 将停用此端口上的速率限制器功能。

如果用户已在 *Threshold unit* 中选择值 *percent*，则请输入从 0 到 100 的百分比值。

如果用户已在 *Threshold unit* 列中选择值 *pps*，则请输入数据速率的绝对值。

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

[Egress]

在此选项卡中，可以指定端口上的出口传输速率。

表格

Port

显示端口编号。

Bandwidth [%]

指定出口传输速率。

可能的值：

- ▶ 0（默认设置）
带宽限制已禁用。
- ▶ 1..100
带宽限制已启用。
此值以 1% 的增量指定端口的总链路速度百分率。

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

5.3 Filter for MAC Addresses

[Switching > Filter for MAC Addresses]

此对话框可用于显示和编辑地址表的地址筛选器。地址筛选器指定设备中根据目标 MAC 地址转发数据包的方式。

表格中的每一行代表一个筛选器。设备自动设置筛选器。设备允许用户手动设置更多筛选器。

设备以如下方式传输数据包：

- ▶ 当表格包含某个数据包的目标地址的条目时，设备会将该数据包从接收端口传输到该表格条目中指定的端口。
- ▶ 当不存在目标地址的表格条目时，设备会将该数据包从接收端口传输到所有其他端口。

表格

要从地址表中删除示教 MAC 地址，请在 *Basic Settings > Restart* 对话框中点击 *Reset MAC address table* 按钮。

Address

显示对其应用了表格条目的目标 MAC 地址。

VLAN ID

显示对其应用了表格条目的 VLAN 的 ID。

设备分别学习每个 VLAN 的 MAC 地址（独立 VLAN 示教）。

Status

显示设备如何设置地址筛选器。

可能的值：

- ▶ *learned*
设备根据收到的数据包自动设置地址筛选器。
- ▶ *permanent*
手动设置地址筛选器。地址筛选器永久保持设置状态。
- ▶ *IGMP*
由 IGMP 窥探自动设置地址筛选器。
- ▶ *mgmt*
设备的 MAC 地址。地址筛选器具有防更改保护。
- ▶ *MRP-MMRP*
由 MMRP 自动设置多播地址筛选器。
- ▶ *GMRP*
由 GMRP 自动设置多播地址筛选器。

<Port number>

显示对应端口如何传输指向相邻目标地址的数据包。

可能的值：

- ▶ -
端口不向目标地址传输任何数据包。
- ▶ **learned**
端口向目标地址传输数据包。设备根据收到的数据包自动创建了筛选器。
- ▶ **IGMP learned**
端口向目标地址传输数据包。设备根据 IGMP 自动创建了筛选器。
- ▶ **unicast static**
端口向目标地址传输数据包。用户创建了筛选器。
- ▶ **multicast static**
端口向目标地址传输数据包。用户创建了筛选器。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。



打开 *Create* 窗口，向表格中添加一个新的条目。

- ▶ 在 *Address* 字段中，可以指定目标 MAC 地址。
- ▶ 在 *VLAN ID* 字段中，可以指定 VLAN 的 ID。
- ▶ 在 *Port* 字段中，可以指定端口。
 - 如果目标 MAC 地址是单播地址，请选择一个端口。
 - 如果目标 MAC 地址是多播地址，请选择一个或多个端口。
 - 要创建丢弃筛选器，请不要选择端口。设备丢弃带有表格条目中指定的目标 MAC 地址的数据包。

Reset MAC address table

从转发表中删除在 *Status* 列中具有值 **learned** 的 MAC 地址。

5.4 IGMP Snooping

[Switching > IGMP Snooping]

Internet Group Management Protocol (IGMP) 是一种用于动态管理多播组的协议。该协议描述了第三层上路由器和终端设备之间多播数据包的分布。

设备允许用户借助 IGMP 窥探功能也使用第二层上的 IGMP 机制：

- ▶ 如果没有 IGMP 窥探，则设备向所有端口传输多播数据包。
- ▶ 借助激活的 IGMP 窥探功能，设备仅在与多播接收器连接的端口上传多播数据包。这可降低网络负载。设备对在第三层上传输的 IGMP 数据包进行评估，并使用第二层上的信息。

在满足以下条件后，方可激活 IGMP 窥探功能：

- ▶ 网络中有一个创建 IGMP 查询（定期查询）的多播路由器。
- ▶ 参与 IGMP 窥探的设备转发 IGMP 查询。

设备将 IGMP 报告与其地址表中的条目链接起来。当一个多播接收器加入一个多播组时，设备会在 *Switching > Filter for MAC Addresses* 对话框中为此端口创建一个表格条目。当多播接收器离开多播组时，设备会删除该表格条目。

该菜单包含以下对话框：

- ▶ IGMP Snooping Global
- ▶ IGMP Snooping Configuration
- ▶ IGMP Snooping Enhancements
- ▶ IGMP Snooping Querier
- ▶ IGMP Snooping Multicasts

5.4.1 IGMP Snooping Global

[Switching > IGMP Snooping > Global]

此对话框允许用户启用设备中的 *IGMP Snooping* 协议并为每个端口和每个 VLAN 配置该协议。

Operation

Operation

启用/禁用设备中的 *IGMP Snooping* 功能。

可能的值：

- ▶ *On*
设备中的 *IGMP Snooping* 功能是根据 RFC 4541 启用的（考虑互联网组管理协议（IGMP）和多播侦听器发现（MLD）窥探交换机）。
- ▶ *Off*（默认设置）
设备中的 *IGMP Snooping* 功能已禁用。
设备不作评估即传输收到的查询、报告和离开数据包。接收到的带有多播目标地址的数据包由设备传输到每个端口。

Information

Multicast control packets processed

显示处理的多播控制数据包的数量。

此统计包括以下数据包类型：

- IGMP 报告
- IGMP 查询器版本 V1
- IGMP 查询器版本 V2
- IGMP 查询器版本 V3
- 具有错误版本的 IGMP 查询器
- PIM 或 DVMRP 数据包

设备使用多播控制数据包创建用于传输多播数据包的地址表。

可能的值：

- ▶ $0..2^{31}-1$

可以使用 *Basic Settings > Restart* 对话框中的 *Reset IGMP snooping data* 按钮或者在命令行界面中使用 `clear igmp-snooping` 命令重置 IGMP 窥探条目，包括处理的多播控制数据包的计数器。

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

Reset IGMP snooping counters

删除 IGMP 窥探条目并将 *Information* 框中的计数器重置为 0。

5.4.2 IGMP Snooping Configuration

[Switching > IGMP Snooping > Configuration]

此对话框允许用户启用设备中的 *IGMP Snooping* 功能并为每个端口和每个 VLAN 配置该功能。

该对话框包含以下选项卡：

▶ [VLAN ID]

▶ [Port]

[VLAN ID]

在此选项卡中，可以为每个 VLAN 配置 *IGMP Snooping* 功能。

表格

VLAN ID

显示对其应用了表格条目的 VLAN 的 ID。

Active

激活/停用此 VLAN 的 *IGMP Snooping* 功能。

前提条件是全局启用了 *IGMP Snooping* 功能。

可能的值：

▶ 勾选

此 VLAN 的 IGMP 窥探已激活。该 VLAN 已加入多播数据流。

▶ 未勾选（默认设置）

此 VLAN 的 IGMP 窥探已停用。该 VLAN 已离开多播数据流。

Group membership interval

指定当设备不再从来自动态多播组的 VLAN 接收到任何报告数据包时该 VLAN 在地址表中保持输入状态的时间（秒）。

指定一个比 *Max. response time* 列中的值更大的值。

可能的值：

▶ 2..3600（默认设置：260）

Max. response time

指定多播组的成员响应查询数据包的时间（以秒为单位）。对于成员的响应，他们可以在响应时间内指定一个随机时间。因此，这有助于防止多播组成员同时响应查询。

指定一个比 *Group membership interval* 列中的值更小的值。

可能的值:

- ▶ 1..25 (默认设置: 10)

Fast leave admin mode

激活/停用此 VLAN 的快速离开功能。

可能的值:

- ▶ 勾选
当快速离开功能已激活且设备接收到来自多播组的 IGMP 离开消息时, 设备将立即从其地址表中删除该条目。
- ▶ 未勾选 (默认设置)
当快速离开功能已停用时, 设备会首先向多播组的成员发送基于 MAC 的查询, 并在 VLAN 不再发送任何报告消息时删除一个条目。

MRP expiration time

多播路由器当前到期时间。指定设备在这个属于 VLAN 的端口上等待查询的时间 (秒)。当端口不接收查询数据包时, 设备会从具有连接的多播路由器的端口列表中删除该端口。

只有当该端口属于一个现有 VLAN 时, 用户方可选择配置此参数。

可能的值:

- ▶ 0
无限超时 - 无到期时间
- ▶ 1..3600 (默认设置: 260)

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

[Port]

在此选项卡中, 可以为每个端口配置 *IGMP Snooping* 功能。

表格

Port

显示端口编号。

Active

激活/停用此端口的 *IGMP Snooping* 功能。

前提条件是全局启用了 *IGMP Snooping* 功能。

可能的值:

- ▶ 勾选
此端口上的 IGMP 窥探已激活。设备将该端口包括在多播数据流中。
- ▶ 未勾选 (默认设置)
此端口上的 IGMP 窥探已停用。该端口已离开多播数据流。

Group membership interval

指定当设备不再从来自动态多播组的端口接收到任何报告数据包时该端口在地址表中保持输入状态的时间 (秒)。

可能的值:

- ▶ 2..3600 (默认设置: 260)

指定一个比 *Max. response time* 列中的值更大的值。

Max. response time

指定多播组的成员响应查询数据包的时间 (以秒为单位)。对于成员的响应, 他们可以在响应时间内指定一个随机时间。因此, 这有助于防止多播组成员同时响应查询。

可能的值:

- ▶ 1..25 (默认设置: 10)

指定一个比 *Group membership interval* 列中的值更小的值。

MRP expiration time

指定多播路由器当前到期时间。MRP 到期时间是设备在此端口上等待查询数据包的时间 (秒)。当端口不接收查询数据包时, 设备会从具有连接的多播路由器的端口列表中删除该端口。

可能的值:

- ▶ 0
无限超时 - 无到期时间
- ▶ 1..3600 (默认设置: 260)

Fast leave admin mode

激活/停用此端口的快速离开功能。

可能的值:

- ▶ 勾选
当快速离开功能已激活且设备接收到来自多播组的 IGMP 离开消息时, 设备将立即从其地址表中删除该条目。
- ▶ 未勾选 (默认设置)
当快速离开功能已停用时, 设备会首先向多播组的成员发送基于 MAC 的查询, 并在端口不再发送任何报告消息时删除一个条目。

Static query port

激活/停用 *Static query port* 模式。

可能的值：

▶ 勾选

Static query port 模式已激活。

该端口是已设置的 VLAN 中的一个静态查询端口。

如果使用 *Redundant Coupling Protocol* 功能且设备作为从站进行工作，则不要为二级环网/网络上的端口激活 *Static query port* 模式。

▶ 未勾选（默认设置）

Static query port 模式已停用。

该端口不是静态查询端口。只有当端口接收 IGMP 查询时，设备才向端口传输 IGMP 报告消息。

VLAN IDs

显示对其应用了表格条目的 VLAN 的 ID。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

5.4.3 IGMP Snooping Enhancements

[Switching > IGMP Snooping > Snooping Enhancements]

此对话框可用于为 VLAN ID 选择和配置端口。

表格

VLAN ID

显示对其应用了表格条目的 VLAN 的 ID。

<Port number>

如果相关的端口为查询端口，则显示设备中设置的每个 VLAN。此外，该字段还会显示设备是否将 VLAN 中的每个多播流都传输到此端口。

可能的值：

- ▶ -
该端口不是此 VLAN 中的查询端口。
- ▶ L= Learned
设备检测到此端口是查询端口，因为该端口在此 VLAN 中接收到 IGMP 查询。该端口不是静态配置的查询端口。
- ▶ A= Automatic
设备检测到该端口是查询端口。前提条件是用户将该端口配置为 *Learn by LLDP*。
- ▶ S= Static (手动设置)
用户将端口指定为静态查询端口。设备只将 IGMP 报告传输到之前通过其接收到 IGMP 查询的端口，以及传输到静态配置的查询端口。
要分配此值，请执行以下步骤：
 - 打开 *Wizard* 窗口。
 - 在 *Configuration* 对话框中，勾选 *Static* 复选框。
- ▶ P= Learn by LLDP (手动设置)
用户将端口指定为 *Learn by LLDP*。
设备通过 Link Layer Discovery Protocol (LLDP) 检测到直接连接到端口的 Schneider Electric 设备。设备将检测到的查询端口标记为 A。
要分配此值，请执行以下步骤：
 - 打开 *Wizard* 窗口。
 - 在 *Configuration* 对话框中，勾选 *Learn by LLDP* 复选框。
- ▶ F= Forward All (手动设置)
用户指定该端口，使设备将在 VLAN 中收到的每个多播流都传输到此端口。例如，可以使用此设置进行诊断。
要分配此值，请执行以下步骤：
 - 打开 *Wizard* 窗口。
 - 在 *Configuration* 对话框中，勾选 *Forward all* 复选框。

Display categories

增强显示的清晰度。表格强调包含指定值的单元格。这有助于根据用户需要对表格进行分析和排序。

- ▶ *Learned (L)*
表格显示包含值 L 以及可能更多值的单元格。对于包含仅除 L 以外的其他值的单元格，表格用“-”符号显示。

- ▶ *Static (S)*
表格显示包含值 **S** 以及可能更多值的单元格。对于包含仅除 **S** 以外的其他值的单元格，表格用“-”符号显示。
- ▶ *Automatic (A)*
表格显示包含值 **A** 以及可能更多值的单元格。对于包含仅除 **A** 以外的其他值的单元格，表格用“-”符号显示。
- ▶ *Learned by LLDP (P)*
表格显示包含值 **P** 以及可能更多值的单元格。对于包含仅除 **P** 以外的其他值的单元格，表格用“-”符号显示。
- ▶ *Forward all (F)*
表格显示包含值 **F** 以及可能更多值的单元格。对于包含仅除 **F** 以外的其他值的单元格，表格用“-”符号显示。

按钮

“按钮” 页 16一节中提供了标准按钮的描述。



打开帮助您选择和配置端口的 *Wizard* 窗口。

[Selection VLAN/Port (Wizard)]

在 *Selection VLAN/Port* 对话框中，可以将 VLAN ID 分配到端口。

在 *Configuration* 对话框中，可以指定端口的设置。

关闭 *Wizard* 窗口后，点击 按钮保存您的设置。

[Selection VLAN/Port (Wizard) - Selection VLAN/Port]

VLAN ID

选择 VLAN 的 ID。

可能的值：

▶ 1..4042

Port

选择端口。

可能的值：

▶ <Port number>

[Selection VLAN/Port (Wizard) - Configuration]

VLAN ID

显示所选 VLAN 的 ID。

Port

显示所选端口的编号。

Static

将端口指定为已设置的 VLAN 中的静态查询端口。设备将 IGMP 报告消息传输到设备通过其接收 IGMP 查询的端口。这还允许用户将 IGMP 报告消息传输到其他选定的端口（启用）或连接的 Schneider Electric 设备 (*Automatic*)。

Learn by LLDP

将端口指定为 *Learn by LLDP*。让设备检测直接连接的 Schneider Electric 设备，并作为查询端口获知相关端口。

Forward all

将端口指定为 *Forward all*。使用 *Forward all* 设置，设备通过此端口传输在目标地址字段中具有多播地址的所有数据包。

5.4.4 IGMP Snooping Querier

[Switching > IGMP Snooping > Querier]

设备允许用户只将多播流发送到与多播接收器连接的那些端口。

为了确定多播接收器连接到哪些端口，设备以可定义间隔向端口发送查询数据包。当连接了多播接收器时，它会使用一个报告数据包对设备作出响应，进而连接多播流。

此对话框可用于以全局方式以及为已设置的 VLAN 配置窥探查询器设置。

Operation

Operation

全局启用/禁用设备中的 IGMP 查询器功能。

可能的值：

- ▶ *On*
- ▶ *Off* (默认设置)

Configuration

在此框中，可以为一般查询数据包指定 IGMP 窥探查询器设置。

Protocol version

指定一般查询数据包的 IGMP 版本。

可能的值：

- ▶ *1*
IGMP v1
- ▶ *2* (默认设置)
IGMP v2
- ▶ *3*
IGMP v3

Query interval [s]

指定设备在接收到来自多播路由器的查询数据包时自行生成一般查询数据包之前的时间（秒）。

可能的值：

- ▶ 1..1800（默认设置：60）

Expiry interval [s]

指定活动查询器在超过此处指定的时间内没有收到任何查询数据包时从被动状态切换回主动状态之前的时间（秒）。

可能的值：

- ▶ 60..300（默认设置：125）

表格

在此表格中，可以为已设置的 VLAN 指定窥探查询器设置。

VLAN ID

显示对其应用了表格条目的 VLAN 的 ID。

Active

激活/停用此 VLAN 的 IGMP 窥探查询器功能。

可能的值：

- ▶ 勾选
此 VLAN 的 IGMP 窥探查询器功能已激活。
- ▶ 未勾选（默认设置）
此 VLAN 的 IGMP 窥探查询器功能已停用。

Current state

显示此 VLAN 的窥探查询器是否已激活。

可能的值：

- ▶ 勾选
此 VLAN 的窥探查询器已激活。
- ▶ 未勾选
此 VLAN 的窥探查询器已停用。

Address

指定设备在生成的一般查询数据包中作为源地址添加的 IP 地址。用户使用多播路由器的地址。

可能的值：

- ▶ 有效的 IPv4 地址（默认设置：0.0.0.0）

Protocol version

显示一般查询数据包的 IGMP 协议版本。

可能的值：

- ▶ 1
IGMP v1
- ▶ 2
IGMP v2
- ▶ 3
IGMP v3

Max. response time

显示多播组成员响应查询数据包的时间（以秒为单位）。对于成员的响应，他们可以在响应时间内指定一个随机时间。这有助于防止所有多播组成员同时响应查询。

Last querier address

显示通过其发送最后一次收到的 IGMP 查询的多播路由器的 IP 地址。

Last querier version

显示多播路由器发送在此 VLAN 中收到的最后一个 IGMP 查询时使用的 IGMP 版本。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

5.4.5 IGMP Snooping Multicasts

[Switching > IGMP Snooping > Multicasts]

设备允许用户指定设备如何传输具有未知多播地址的数据包：设备要么丢弃这些数据包，要么将其发送到所有端口，要么只将其传输到之前接收到查询数据包的端口。

设备还允许用户将具有已知多播地址的数据包传输到查询端口。

Configuration

Unknown multicasts

指定设备如何传输具有未知多播地址的数据包。

可能的值：

- ▶ *discard*
设备丢弃具有未知 MAC/IP 多播地址的数据包。
- ▶ *flood*（默认设置）
设备将具有未知 MAC/IP 多播地址的数据包转发到每个端口。

表格

在此表格中，可以为已设置的 VLAN 的已知多播指定设置。

VLAN ID

显示对其应用了表格条目的 VLAN 的 ID。

Known multicasts

指定设备如何传输具有已知多播地址的数据包。

可能的值：

- ▶ *send to query and registered ports*
设备将具有未知 MAC/IP 多播地址的数据包转发到查询端口和注册端口。
- ▶ *send to registered ports*（默认设置）
设备将具有未知 MAC/IP 多播地址的数据包转发到注册端口。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

5.5 Time-Sensitive Networking

[Switching > TSN]

该菜单包含以下对话框：

- ▶ TSN Configuration
- ▶ TSN Gate Control List

5.5.1 TSN Configuration

[Switching > TSN > Configuration]

在此对话框中，可以启用 *TSN* 功能并指定特定于时间的设置。

设置支持 IEEE 802.1 Qbv 中定义的时间感知型队列。此 *TSN* 功能允许支持 TSN 的端口传输相对于门控制列表中定义的周期而计划的每个流量类别的数据包。以太网数据包的 VLAN 标签（或者无标签数据包端口优先级）包含优先级。

此功能可帮助避免保留的数据流出现延迟和拥塞丢失。使用 IEEE1588 (PTP) 的周期和门状态进行精确同步，使实现无拥塞的低延迟通信成为可能。前提条件是网络中的每个设备都支持 IEEE 802.1 Qbv。

提示：与命令行界面不同，在用户点击 按钮后，会立即执行设置。

Operation

Operation

启用/禁用设备中的 *TSN* 功能。

可能的值：

▶ *On*

TSN 功能已全局启用。

设备以流量类别6的优先级处理支持 TSN 的端口上的链路本地帧。因此，链路本地帧在转发时会与优先级相同或更高的其他数据包竞争。这会影响以下帧类型：

- RSTP
- LLDP
- IEEE 802.1AS
- PTP Peer Delay

▶ *Off* (默认设置)

TSN 功能已全局禁用。

只要端口上的 *TSN* 功能处于活动状态，端口就会使用打开的门 0, 1, 2, 3, 4, 5, 6, 7。此设置由制造商预设置。

Base time

Date
Time
[ns]

指定与 UTC 时间相关的周期开始时间。

设备直接将值转换为 PTP 时间刻度，而不考虑闰秒。

可能的值：

▶ 年/月/日

年/月/日

(具体取决于用户 Web 浏览器的语言偏好)

- ▶ `hh:mm:ss`
小时:分钟:秒钟
- ▶ `0..999999999`
指定以纳秒为单位的偏移量。

提示: 指定未来的基准时间时, 周期会比 `UTC offset [s]` 字段中指定的时间早几秒开始。参见 [Time > PTP > Boundary Clock > Global](#) 对话框。

Configuration

Cycle time [ns]

指定周期的持续时间 (纳秒)。

可能的值:

- ▶ `50000..10000000` (默认设置: `1000000`)
`50 μs .. 10 ms`

表格

Port

显示端口编号。

Active

激活/停用端口上的 `TSN` 功能。

可能的值:

- ▶ **勾选**
端口上的 `TSN` 功能已激活。
指定未来的基准时间时, 周期会在 `Base time` 框中指定的时间开始。
前提条件是已启用 `PTP` 功能并且设备已同步。
只要已全局启用 `TSN` 功能, 端口就会使用 [Switching > TSN > Gate Control List > Configured](#) 对话框中指定的周期。
- ▶ **未勾选** (默认设置)
端口上的 `TSN` 功能已停用。
只要已全局启用 `TSN` 功能, 端口就会使用打开的门 `0, 1, 2, 3, 4, 5, 6, 7`。

Port state

显示端口上周期的状态。

可能的值:

- ▶ `running`
周期正在运行。
端口使用 [Switching > TSN > Gate Control List > Configured](#) 对话框中指定的周期。

- ▶ *waitForTimeSync*
周期尚未开始。
设备的时钟未同步。
检查 *PTP* 设置。
- ▶ *pending*
周期尚未开始。
已指定未来的基准时间。
- ▶ *disabled*
周期未运行。
端口上的 *TSN* 功能已停用。
 - 检查 *Operation* 框中的设置。
 - 检查 *Active* 列中的设置。端口使用 *Default gate states* 列中指定的门状态。
- ▶ *error*
周期未运行。
检测到错误。

Time of last activation

显示时间设置上次变为活动状态时的日期和时间。

此值与 *PTP* 时间相关。

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

5.5.2 TSN Gate Control List

[Switching > TSN > Gate Control List]

该菜单包含以下对话框：

- ▶ TSN Configured Gate Control List
- ▶ TSN Current Gate Control List

5.5.2.1 TSN Configured Gate Control List

[Switching > TSN > Gate Control List > Configured]

在此对话框中，可以为支持 TSN 的端口指定周期的时间段。添加为打开的门和时间段的持续时间指定的表格条目。

提示：与命令行界面不同，在用户点击 按钮后，会立即执行设置。

该对话框包含以下选项卡：

- ▶ 每个支持 TSN 的端口各一个选项卡。
支持 TSN 端口的数量取决于设备。

[<Port number>]

Configuration

Status

显示分配到门控制列表的模板。

可能的值：

- ▶ -
无模板。未将任何条目分配到门控制列表。
- ▶ *default 2 time slots*
包含 3 个条目的模板：
 - 第一个条目是流量类别 7。
 - 第二个条目是流量类别 6 到 0。
 - 第三个条目是保护带。
- ▶ *default 3 time slots*
包含 5 个条目的模板：
 - 第一个条目是流量类别 7。
 - 第二个条目是保护带。
 - 第三个条目是流量类别 6。
 - 第四个条目是流量类别 5 到 0。
 - 第五个条目是保护带。
- ▶ <any other template name>
使用命令行界面来分配模板。

Template

打开 *Template* 窗口以将其他模板分配到门控制列表。在用户选择其他模板并点击 *Ok* 按钮后，设备会替换表格中的条目。

在下拉列表中，可以选择以下模板之一：

- ▶ *default 2 time slots*
- ▶ *default 3 time slots*

设备允许用户使用命令行界面来分配更多模板。

Delete

删除分配到门控制列表的模板。在此之后，不会再将任何条目分配到门控制列表。

表格

Index

显示门控制列表中的条目的索引编号，该编号用于指定时间段的时间顺序。

Gate states

指定当端口上的 *TSN* 功能处于活动状态时打开的门。

- 其流量类别被分配到选择的门的数据包被选择用于传输 - 门状态 OPEN。
- 其流量类别未被分配到选择的门的数据包不被选择用于传输 - 门状态 CLOSED。

可能的值：

► - (默认设置)

未选择任何门。

设备在处理时间段期间未打开端口上的任何门。在下拉列表中，取消选择每个门。

► 0..7

设备在处理时间段期间打开端口上选择的门。在下拉列表中，选择一个或多个门。

可在 *Switching > QoS/Priority > 802.1D/p Mapping* 对话框中将 VLAN 优先级分配到流量类别。

Interval [ns]

指定时间段的持续时间（纳秒）。

可能的值：

► 1000..10000000

在指定时间段的持续时间时，应考虑以下条件：

- 单个时间段
 - 确认时间段的长度至少足够端口传输最长的预期数据包。
 - 确认时间段小于或等于周期的持续时间。
- 指定的时间段的总和
 - 我们建议时间段的总和等于周期的持续时间。
 - 如果总和超过周期的持续时间，则会丢弃重叠的时间段，并且周期重新开始。
 - 如果总和小于周期的持续时间，则会延长最后一个时间段的间隔以适应周期。

提示： *Switching > TSN > Gate Control List > Current* 对话框中未突出显示指定的时间段与周期持续时间之间的差异。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

5.5.2.2 TSN Current Gate Control List

[Switching > TSN > Gate Control List > Current]

在此对话框中，用户可以对支持 TSN 的端口的周期的当前设置进行监控。每个表格条目代表一个指定的时间段。

如果周期的开始时间 (*Base time*) 在未来，则显示的值与 *Switching > TSN > Gate Control List > Configured* 对话框中指定的值不同。

在 *Switching > TSN > Configuration* 对话框中，*Port state* 列显示周期是否正在端口上运行。

该对话框包含以下选项卡：

- ▶ 每个支持 TSN 的端口各一个选项卡。
支持 TSN 端口的数量取决于设备。

[<Port number>]

表格

Index

显示门控制列表中的条目的索引编号，该编号用于指定时间段的时间顺序。

Gate states

显示当端口上的 TSN 功能处于活动状态时打开的门。

Interval [ns]

显示时间段的持续时间（纳秒）。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

5.6 MRP-IEEE

[Switching > MRP-IEEE]

针对 IEEE 802.1Q 标准的 IEEE 802.1ak 修订引入了 Multiple Registration Protocol (MRP)，以取代 Generic Attribute Registration Protocol (GARP)。IEEE 还修改并替换了 GARP 应用程序、GARP Multicast Registration Protocol (GMRP) 和 GARP VLAN Registration Protocol (GVRP)。Multiple MAC Registration Protocol (MMRP) 和 Multiple VLAN Registration Protocol (MVRP) 替换了这些协议。

MRP-IEEE 可帮助将流量限制到 LAN 的所需区域。为限制流量，MRP-IEEE 应用程序会将属性值分配到 LAN 注册和取消注册多播组成员资格以及 VLAN 标识符之间参加的 MRP-IEEE 设备。

组参与者的注册允许用户为在局域网上传输的特定流量保留资源。通过定义资源需求可以调控流量水平，允许设备确定所需资源，并对分配的资源进行动态维护。

该菜单包含以下对话框：

- ▶ MRP-IEEE Configuration
- ▶ MRP-IEEE Multiple MAC Registration Protocol
- ▶ MRP-IEEE Multiple VLAN Registration Protocol

5.6.1 MRP-IEEE Configuration

[Switching > MRP-IEEE > Configuration]

此对话框可用于设置各种 MRP 计时器。通过保持各种计时器值之间的关系，协议可高效运行，并降低不必要的属性撤消和重新注册的可能性。默认计时器数值可以有效地维护这些关系。

对计时器进行重新配置时，可以维护以下关系：

- ▶ 即使出现消息丢失时，要在 Leave（离开）或 LeaveAll（离开全部）事件后进行重新注册，可将 LeaveTime（离开时间）指定为： $\geq (2x \text{JoinTime}) + 60$ 。
- ▶ 要最大限度减少 LeaveAll（离开全部）事件后产生的重新加入流量的数量，可将 LeaveAll（离开全部）计时器的数值指定为大于 LeaveTime（离开时间）数值。

表格

Port

显示端口编号。

Join time [1/100s]

指定控制应用于申请者状态机的各种传输机会之间间隔的加入计时器。

可能的值：

- ▶ 10..100（默认设置：20）

Leave time [1/100s]

指定控制注册者状态机过渡到空（MT）状态之前在离开（LV）状态下等待的时间的离开计时器。

可能的值：

- ▶ 20..600（默认设置：60）

Leave all time [1/100s]

指定控制 LeaveAll（离开全部）状态机生成 LeaveAll PDU（离开全部 PDU）的频率的 LeaveAll（离开全部）计时器。

可能的值：

- ▶ 200..6000（默认设置：1000）

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

5.6.2 MRP-IEEE Multiple MAC Registration Protocol

[Switching > MRP-IEEE > MMRP]

Multiple MAC Registration Protocol (MMRP) 允许终端设备和 MAC 交换机向位于同一局域网中的交换机注册和注销组成员资格以及单个 MAC 地址信息。局域网中的交换机通过支持扩展筛选服务的交换机传播该信息。利用 MAC 地址信息，MMRP 允许用户将多播流量限制到第二层网络的所需区域。

有关 MMRP 工作原理的例子，可考虑一个安装在桅杆上、俯瞰建筑物的安保摄像头。摄像头向局域网发送多播数据包。我们在不同地点安装了两个监视终端设备。我们将摄像头和两个终端设备的 MAC 地址注册到同一个多播组中。然后，我们在端口上指定 MMRP 设置，向两个终端设备发送多播组数据包。

该对话框包含以下选项卡：

- ▶ [Configuration]
- ▶ [Service requirement]
- ▶ [Statistics]

[Configuration]

在此选项卡中，可以选择活动的 MMRP 端口参与者并将设备设置为传输定期事件。该对话框还允许用户启用 VLAN 注册的 MAC 地址广播。

每个端口都有一个周期性状态机，该状态机定期向与活动端口相关的申请者状态机传输周期性事件。周期性事件包含指示活动端口相关设备的状态的信息。

Operation

Operation

启用/禁用设备中的全局 *MMRP* 功能。设备参与 MMRP 消息交换。

可能的值：

- ▶ *On*
设备是 MMRP 消息交换的正常参与者。
- ▶ *Off* (默认设置)
设备忽略 MMRP 消息。

Configuration

Periodic state machine

启用/禁用设备中的全局周期性状态机。

可能的值：

- ▶ *On*
全局启用 MMRP *Operation* 后，设备通过 MMRP 参与端口以一秒间隔传输 MMRP 消息。
- ▶ *Off*（默认设置）
禁用设备中的周期性状态机。

表格

Port

显示端口编号。

Active

激活/停用端口 MMRP 参与。

可能的值：

- ▶ *勾选*（默认设置）
在此端口上全局启用 MMRP 后，设备通过此端口发送和接收 MMRP 消息。
- ▶ *未勾选*
禁用端口 MMRP 参与。

Restricted group registration

在端口上激活/停用对使用 MMRP 的动态 MAC 地址注册的限制。

可能的值：

- ▶ *勾选*
如果已启用并且相关 VLAN 上存在 MAC 地址的静态筛选器条目，则设备动态注册 MAC 地址属性。
- ▶ *未勾选*（默认设置）
在端口上激活/停用对使用 MMRP 的动态 MAC 地址注册的限制。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

[Service requirement]

此选项卡包含每个活动 VLAN 的转发参数，并指定对其应用多播转发的端口。设备允许用户将 VLAN 端口静态设置为 *Forward all* 或 *Forbidden*。只能通过图形用户界面或命令行界面静态设置 *Forbidden* MMRP 服务需求。

端口只能设置为 *ForwardAll* 或 *Forbidden*。

表格**VLAN ID**

显示 VLAN 的 ID。

<Port number>

为端口指定服务需求处理。

可能的值：

- ▶ **FA**
指定端口上的 *ForwardAll* 流量设置。设备在 VLAN 上转发指向 MMRP 注册多播 MAC 地址的流量。设备将流量转发给 MMRP 动态设置的端口或管理员静态设置为 *ForwardAll* 端口的端口。
- ▶ **F**
指定端口上的 *Forbidden* 流量设置。设备阻塞动态 MMRP *ForwardAll* 服务需求。此 VLAN 中的此端口上阻塞 *ForwardAll* 请求后，设备在此端口上阻塞指向 MMRP 注册多播 MAC 地址的流量。此外，设备还阻塞更改此端口上此值的 MMRP 服务请求。
- ▶ **-**（默认设置）
禁用此端口上的转发功能。
- ▶ **Learned**
显示 MMRP 服务请求所设置的值。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

[Statistics]

局域网上的设备交换 Multiple MAC Registration Protocol Data Units (MMRPDU)，以保持活动 MMRP 端口上设备的状态。此选项卡可用于监控每个端口的 MMRP 流量统计。

Information**Transmitted MMRP PDU**

显示设备中传输的 MMRPDU 的数量。

Received MMRP PDU

显示设备中接收的 MMRPDU 的数量。

Received bad header PDU

显示设备中接收的带有损坏报头的 MMRPDU 的数量。

Received bad format PDU

显示并非在设备中传输的带有损坏数据字段的 MMRPDU 的数量。

Transmission failed

显示并非在设备中传输的 MMRPDU 的数量。

表格

Port

显示端口编号。

Transmitted MMRP PDU

显示端口上传输的 MMRPDU 的数量。

Received MMRP PDU

显示端口上接收的 MMRPDU 的数量。

Received bad header PDU

显示端口上接收的带有损坏报头的 MMRPDU 的数量。

Received bad format PDU

显示并非在端口上传输的带有损坏数据字段的 MMRPDU 的数量。

Transmission failed

显示并非在端口上传输的 MMRPDU 的数量。

Last received MAC address

显示端口从其接收到 MMRPPDU 的最后一个 MAC 地址。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

Reset

重置 *Last received MAC address* 列中的端口统计计数器和数值。

5.6.3 MRP-IEEE Multiple VLAN Registration Protocol

[Switching > MRP-IEEE > MVRP]

Multiple VLAN Registration Protocol (MVRP) 提供了一种允许用户动态分发 VLAN 信息和配置 VLAN 的机制。例如，在活动 MVRP 端口上配置 VLAN 时，设备将 VLAN 信息分发给其他启用了 MVRP 的设备。利用收到的信息，启用了 MVRP 的设备可以根据需要在其他启用了 MVRP 的设备上动态创建 VLAN 中继。

该对话框包含以下选项卡：

- ▶ [Configuration]
- ▶ [Statistics]

[Configuration]

在此选项卡中，可以选择活动的 MVRP 端口参与者并将设备设置为传输定期事件。

每个端口都有一个周期性状态机，该状态机定期向与活动端口相关的申请者状态机传输周期性事件。周期性事件包含指示活动端口相关 VLAN 的状态的信息。使用周期性事件，启用了 MVRP 的交换机可以动态维护 VLAN。

Operation

Operation

启用/禁用全局申请者管理控制，该控制用于指定申请者状态机是否参与 MMRP 消息交换。

可能的值：

- ▶ *On*
正常参与者。申请者状态机参与 MMRP 消息交换。
- ▶ *Off* (默认设置)
非参与者。申请者状态机忽略 MMRP 消息。

Configuration

Periodic state machine

启用/禁用设备中的周期性状态机。

可能的值：

- ▶ *On*
周期性状态机已启用。
全局启用 MVRP *Operation* 后，设备通过 MVRP 参与端口以一秒间隔传输 MVRP 周期性事件。
- ▶ *Off* (默认设置)
周期性状态机已禁用。
禁用设备中的周期性状态机。

表格

Port

显示端口编号。

Active

激活/停用端口 MVRP 参与。

可能的值：

- ▶ **勾选**（默认设置）
在此端口上全局启用 MVRP 后，设备向连接到此端口的知道 MVRP 的设备分发 VLAN 成员资格信息。
- ▶ **未勾选**
禁用端口 MVRP 参与。

Restricted VLAN registration

激活/停用此端口的 *Restricted VLAN registration* 功能。

可能的值：

- ▶ **勾选**
如果启用且存在一个静态 VLAN 注册条目，则设备允许用户为此条目创建一个动态 VLAN。
- ▶ **未勾选**（默认设置）
禁用此端口上的 *Restricted VLAN registration* 功能。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

[Statistics]

局域网上的设备交换 Multiple VLAN Registration Protocol Data Units (MVRPDU)，以保持活动端口上 VLAN 的状态。此选项卡可用于监控 MVRP 流量。

Information

Transmitted MVRP PDU

显示设备中传输的 MVRPDU 的数量。

Received MVRP PDU

显示设备中接收的 MVRPDU 的数量。

Received bad header PDU

显示设备中接收的带有损坏报头的 MVRPDU 的数量。

Received bad format PDU

显示设备阻塞的带有损坏数据字段的 MVRPDU 的数量。

Transmission failed

显示在将消息添加到 MVRP 队列时检测到的故障数。

Message queue failures

显示设备阻塞的 MVRPDU 的数量。

表格**Port**

显示端口编号。

Transmitted MVRP PDU

显示端口上传输的 MVRPDU 的数量。

Received MVRP PDU

显示端口上接收的 MVRPDU 的数量。

Received bad header PDU

显示设备在端口上接收的带有损坏报头的 MVRPDU 的数量。

Received bad format PDU

显示设备在端口上阻塞的带有损坏数据字段的 MVRPDU 的数量。

Transmission failed

显示设备在端口上阻塞的 MVRPDU 的数量。

Registrations failed

显示在端口上尝试注册失败的次数。

Last received MAC address

显示端口从其接收到 MVRPDU 的最后一个 MAC 地址。

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

Reset

重置 *Last received MAC address* 列中的端口统计计数器和数值。

5.7

GARP

[Switching > GARP]

IEEE 定义的 Generic Attribute Registration Protocol (GARP) 提供了一个通用框架，使交换机能够注册和注销 VLAN 标识符和多播组成员资格等属性值。

根据 GARP 注册或注销一个成员的一个属性时，根据特定规则对该参与者进行修改。参与者是一组可达的终端站和网络设备。在任意给定时间定义的参与者集合及其属性是网络拓扑子集的可达性树。设备只向注册终端站转发数据帧。站注册有助于防止向不可达终端站发送数据的企图。

提示： 启用 *GMRP* 功能之前，请验证 *MMRP* 功能是否已禁用。

该菜单包含以下对话框：

- ▶ *GMRP*
- ▶ *GVRP*

5.7.1 GMRP

[Switching > GARP > GMRP]

GARP Multicast Registration Protocol (GMRP) 是一种提供了允许网络设备和终端站动态注册组成员资格的机制的 Generic Attribute Registration Protocol (GARP)。这些设备向连接到同一局域网段的设备注册组成员资格信息。GARP 还允许这些设备向支持扩展筛选服务的网络设备分发信息。

GMRP 和 GARP 都是由 IEEE 802.1P 定义的行业标准协议。

Operation

Operation

启用/禁用设备中的全局 *GMRP* 功能。设备参与 MVRP 消息交换。

可能的值：

- ▶ *On*
GMRP 已启用。
- ▶ *Off* (默认设置)
设备忽略 MVRP 消息。

Multicasts

Unknown multicasts

启用/禁用未知多播数据的泛洪或丢弃。

可能的值：

- ▶ *discard*
设备丢弃未知多播数据。
- ▶ *flood* (默认设置)
设备向所有端口转发未知多播数据。

表格

Port

显示端口编号。

GMRP active

激活/停用端口 *GMRP* 参与。

前提条件是全局启用了 *GMRP* 功能。

可能的值：

- ▶ **勾选**（默认设置）
端口 *GMRP* 参与已激活。
- ▶ **未勾选**
端口 *GMRP* 参与已停用。

Service requirement

指定应用多播转发的端口。

可能的值：

- ▶ *Forward all unregistered groups*（默认设置）
设备在 VLAN 上转发指向 *GMRP* 注册多播 MAC 地址的数据。设备向未注册的组转发数据。
- ▶ *Forward all groups*
设备转发指向注册或未注册的所有组的数据。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

5.7.2 GVRP

[Switching > GARP > GVRP]

GARP VLAN Registration Protocol (GVRP) 或 Generic VLAN Registration Protocol 是一种便于对更大网络中的虚拟局域网 (VLAN) 进行控制的协议。GVRP 是一种第二层网络协议，用于对 VLAN 网络中的设备进行自动配置。

GVRP 是一种 GARP 应用程序，可提供符合 IEEE 802.1Q 的 VLAN 修剪并在 802.1Q 中继端口上创建动态 VLAN。利用 GVRP，设备与其他 GVRP 设备交换 VLAN 配置信息。因此，设备可减少不必要的广播和未知的单播流量。交换 VLAN 配置信息还允许用户动态创建和管理通过 802.1Q 中继端口连接的 VLAN。

Operation

Operation

全局启用/禁用设备中的 *GVRP* 功能。设备参与 *GVRP* 消息交换。如果该功能已禁用，则设备忽略 *GVRP* 消息。

可能的值：

- ▶ *On*
GVRP 功能已启用。
- ▶ *Off* (默认设置)
GVRP 功能已禁用。

表格

Port

显示端口编号。

GVRP active

激活/停用端口 *GVRP* 参与。

前提条件是全局启用了 *GVRP* 功能。

可能的值：

- ▶ 勾选 (默认设置)
端口 *GVRP* 参与已激活。
- ▶ 未勾选
端口 *GVRP* 参与已停用。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

5.8 QoS/Priority

[Switching > QoS/Priority]

通信网络同时传输很多种在可用性、带宽和延时时间等方面有不同要求的应用程序。

QoS（服务质量）是 IEEE 802.1D 中定义的一项程序。它用于在网络中分配资源。因此，用户有可能为必要的应用程序提供最小带宽。前提条件是，终端设备以及网络中的设备支持优先化数据传输。由网络中的设备进行传输时，优先级较高的数据包将优先传输。当没有优先级更高的数据包需要传输时，用户可以传输优先级较低的数据包。

设备提供以下设置选项：

- ▶ 用户指定设备如何评估输入数据包的 QoS/优先化信息。
- ▶ 对于输出数据包，用户可以指定设备在数据包中写入哪些 QoS/优先化信息（例如：管理数据包优先、端口优先）。

提示：如果使用此菜单中的功能，则请禁用流量控制。如果 *Switching > Global* 对话框 *Configuration* 框中的 *Flow control* 复选框未勾选，则流量控制已停用。

该菜单包含以下对话框：

- ▶ QoS/Priority Global
- ▶ QoS/Priority Port Configuration
- ▶ 802.1D/p Mapping
- ▶ IP DSCP Mapping
- ▶ Queue Management

5.8.1 QoS/Priority Global

[Switching > QoS/Priority > Global]

即使在利用率很高的情况下，设备仍允许用户访问设备管理。在此对话框中，可以指定所需 QoS/优先级设置。

Configuration

VLAN priority for management packets

为发送管理数据包指定 VLAN 优先级。视 VLAN 优先级而定，设备将数据包分配给特定的流量类别，进而分配给端口的特定优先级队列。

可能的值：

▶ 0..7 (默认设置：0)

在 *Switching > QoS/Priority > 802.1D/p Mapping* 对话框中，可以将一个流量类别分配给每个 VLAN 优先级。

IP DSCP value for management packets

为发送管理数据包指定 IP DSCP 值。视 IP DSCP 值而定，设备将数据包分配给特定的流量类别，进而分配给端口的特定优先级队列。

可能的值：

▶ 0 (be/cs0)..63 (默认设置：0 (be/cs0))

列表中的某些值还有一个 DSCP 关键字，如：0 (be/cs0)、10 (af11) 和 46 (ef)。这些值都与 IP 优先级模型兼容。

在 *Switching > QoS/Priority > IP DSCP Mapping* 对话框中，可以将一个流量类别分配给每个 IP DSCP 值。

Queues per port

显示每个端口的优先级队列的数量。

设备每个端口都有 8 个优先级队列。可以将每个优先级队列分配给一个特定流量类别（流量类别需符合 IEEE 802.1D）。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

5.8.2 QoS/Priority Port Configuration

[Switching > QoS/Priority > Port Configuration]

在此对话框中，可以为每个端口指定设备如何根据其 QoS/优先级信息来处理收到的数据包。

表格

Port

显示端口编号。

Port priority

指定当数据包不包含优先级信息时设备向数据包中写入哪些 VLAN 优先级信息。之后，设备根据 *Trust mode* 列中指定的值传输数据包。

可能的值：

- ▶ 0..7（默认设置：0）

Trust mode

指定当数据包包含 QoS/优先级信息时设备如何处理收到的数据包。

可能的值：

- ▶ *untrusted*
设备根据 *Port priority* 列中指定的优先级传输数据包。设备忽略数据包中包含的优先级信息。
在 *Switching > QoS/Priority > 802.1D/p Mapping* 对话框中，可以将一个流量类别分配给每个 VLAN 优先级。
- ▶ *trustDot1p*（默认设置）
设备根据 VLAN 标签中的优先级信息传输数据包。
在 *Switching > QoS/Priority > 802.1D/p Mapping* 对话框中，可以将一个流量类别分配给每个 VLAN 优先级。
- ▶ *trustIpDscp*
 - 如果数据包是 IP 数据包，则：
设备根据数据包中包含的 IP DSCP 值传输数据包。
在 *Switching > QoS/Priority > IP DSCP Mapping* 对话框中，可以将一个流量类别分配给每个 IP DSCP 值。
 - 如果数据包不是 IP 数据包，则：
设备根据 *Port priority* 列中指定的优先级传输数据包。
在 *Switching > QoS/Priority > 802.1D/p Mapping* 对话框中，可以将一个流量类别分配给每个 VLAN 优先级。

Untrusted traffic class

显示分配给 *Port priority* 列中指定的 VLAN 优先级信息的流量类别。在 *Switching > QoS/Priority > 802.1D/p Mapping* 对话框中，可以将一个流量类别分配给每个 VLAN 优先级。

可能的值：

▶ 0..7

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

5.8.3 802.1D/p Mapping

[Switching > QoS/Priority > 802.1D/p Mapping]

设备根据所包含的具有较高或较低优先级的 QoS/优先级信息传输带有 VLAN 标签的数据包。

在此对话框中，可以将一个流量类别分配给每个 VLAN 优先级。可以将流量类别分配给端口的优先级队列。

表格

VLAN priority

显示 VLAN 优先级。

Traffic class

指定分配给 VLAN 优先级的流量类别。

可能的值：

► 0..7

0 被分配给具有最低优先级的优先级队列。

7 被分配给具有最高优先级的优先级队列。

提示：除其他功能之外，冗余机制使用最高的流量类别。因此，请为应用程序数据选择另一个流量类别。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

VLAN 优先级向流量类别的默认分配

VLAN 优先级	流量类别	符合 IEEE 802.1D 的内容描述
0	2	Best Effort 无优先化的普通数据
1	0	Background 对时间不敏感的数据和后台服务
2	1	Standard 普通数据
3	3	Excellent Effort 关键数据
4	4	Controlled Load 具有较高优先级的时间敏感数据

VLAN 优先级	流量类别	符合 IEEE 802.1D 的内容描述
5	5	Video 延迟和抖动小于 100 毫秒的视频传输
6	6	Voice 延迟和抖动小于 10 毫秒的语音传输
7	7	Network Control 用于网络管理和冗余机制的数据

5.8.4 IP DSCP Mapping

[Switching > QoS/Priority > IP DSCP Mapping]

设备根据具有较高或较低优先级的数据包中包含的 DSCP 值传输 IP 数据包。

在此对话框中，可以将一个流量类别分配给每个 DSCP 值。可以将流量类别分配给端口的优先级队列。

表格

DSCP value

显示 DSCP 值。

Traffic class

指定分配给 DSCP 值的流量类别。

可能的值：

► 0..7

0 被分配给具有最低优先级的优先级队列。

7 被分配给具有最高优先级的优先级队列。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

DSCP 值向流量类别的默认分配

DSCP 值	DSCP 名称	流量类别
0	Best Effort /CS0	2
1-7		2
8	CS1	0
9, 11, 13, 15		0
10, 12, 14	AF11, AF12, AF13	0
16	CS2	1
17, 19, 21, 23		1
18, 20, 22	AF21, AF22, AF23	1
24	CS3	3
25, 27, 29, 31		3
26, 28, 30	AF31, AF32, AF33	3
32	CS4	4
33, 35, 37, 39		4
34, 36, 38	AF41, AF42, AF43	4
40	CS5	5

DSCP 值	DSCP 名称	流量类别
41, 42, 43, 44, 45, 47		5
46	EF	5
48	CS6	6
49-55		6
56	CS7	7
57-63		7

5.8.5 Queue Management

[Switching > QoS/Priority > Queue Management]

此对话框可用于为流量类别启用和禁用 *Strict priority* 功能。禁用 *Strict priority* 功能后，设备会使用“加权公平排队”处理端口的优先级队列。

用户还可选择为每个流量类别分配最小带宽，以便设备用来处理“加权公平排队”的优先级队列。

表格

Traffic class

显示流量类别。

Strict priority

为此流量类别激活/停用具有 *Strict priority* 的端口优先级队列的处理。

可能的值：

▶ 勾选（默认设置）

具有 *Strict priority* 的端口优先级队列的处理已激活。

- 端口只转发优先级队列中具有最高优先级的数据包。当此优先级队列变空时，端口会转发优先级队列中具有下一个较低优先级的数据包。
- 当具有更高优先级的优先级队列变空后，端口会转发具有更低流量类别的数据包。在不利的情况下，端口不发送这些数据包。
- 为某个流量类别选择此设置后，设备还为具有更高优先级的流量类别启用此功能。
- 对于 VoIP 或视频等需要尽可能最小延迟的应用程序，可以使用此设置。

▶ 未勾选

具有 *Strict priority* 的端口优先级队列的处理已停用。设备使用“加权公平排队”/“加权轮询”（WRR）处理端口优先级队列。

- 设备向每个流量类别分配最小带宽。
- 即使在较高的网络负载下，端口仍传输具有较低流量类别的数据包。
- 为某个流量类别选择此设置后，设备还为具有更低优先级的流量类别禁用此功能。

Min. bandwidth [%]

当设备正在使用“加权公平排队”处理端口的优先级队列时为此流量类别指定最小带宽。

可能的值：

▶ 0..100（默认设置：0 = 设备不为此流量类别保留任何带宽）

以百分比为单位指定的值表示端口上的可用带宽。为每个流量类别都禁用 *Strict priority* 功能后，端口上的最大带宽可用于“加权公平排队”。

所分配带宽的最大总数为 100%。

Max. bandwidth [%]

指定流量类别传输数据包的成形率（队列成形）。

可能的值：

- ▶ 0（默认设置）
设备不为此流量类别保留任何带宽。
- ▶ 1..100
设备为此流量类别保留指定带宽。以百分比为单位指定的值表示此端口上的最大可用带宽。

例如，使用队列成形可使用户限制极高优先级队列的速率。限制极高优先级队列使设备还能够处理低优先级队列。要使用队列成形，用户应为特定队列设置最大带宽。

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

5.9 VLAN

[Switching > VLAN]

借助 VLAN（虚拟局域网），可将物理网络中的数据流量分布到逻辑子网络。这可提供以下优势：

- ▶ 灵活性高
 - 借助 VLAN，可将数据流量分布到现有基础设施中的逻辑网络。如果没有 VLAN，可能就需要安装更多设备并进行复杂布线。
 - 利用 VLAN，可以指定与各个终端设备的位置无关的网段。
- ▶ 吞吐量更大
 - 在 VLAN 中，数据包可以按照优先级进行传输。
当优先级较高时，设备优先传输 VLAN 的数据，例如，对于 VoIP 电话通话等时间敏感型应用程序。
 - 当数据包和广播分布在小型网段而非整个网络之中时，网络负载大大降低。
- ▶ 安全性更高
将数据流量分布在各个逻辑网络之间，可使不需要的访问变得更加困难，并可增强系统抵御 MAC 泛洪或 MAC 欺骗等攻击的能力。

设备支持符合 IEEE 802.1Q 标准的基于数据包的“标记”VLAN。数据包中的 VLAN 标记指示数据包所属的 VLAN。

设备仅在分配给相同 VLAN 的端口上传输该 VLAN 的标记数据包。这可降低网络负载。

设备分别学习每个 VLAN 的 MAC 地址（独立 VLAN 示教）。

设备按照以下顺序确定接收到的数据流的优先级：

- ▶ 语音 VLAN
- ▶ 基于端口的 VLAN

该菜单包含以下对话框：

- ▶ VLAN Global
- ▶ VLAN Configuration
- ▶ VLAN Port
- ▶ VLAN Voice

5.9.1 VLAN Global

[Switching > VLAN > Global]

此对话框允许用户查看设备的一般 VLAN 参数。

Configuration

Max. VLAN ID

可以分配给 VLAN 的最高 ID。

参见 [Switching > VLAN > Configuration](#) 对话框。

VLANs (max.)

显示可能的 VLAN 的最大数量。

参见 [Switching > VLAN > Configuration](#) 对话框。

VLANs

设备中当前配置的 VLAN 的数量。

参见 [Switching > VLAN > Configuration](#) 对话框。

VLAN ID 1 会在设备中持续存在。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

Clear...

将设备的 VLAN 设置重置为默认设置。

请注意，如果在 [Basic Settings > Network](#) 对话框中更改了设备管理的 VLAN ID，则至设备的连接会中断。

5.9.2 VLAN Configuration

[Switching > VLAN > Configuration]

在此对话框中，可以管理 VLAN。要设置 VLAN，请在表格中另外创建一行。在该行中，可以为每个端口指定该端口是否传输相应 VLAN 的数据包以及这些数据包是否包含 VLAN 标签。

可以区分以下 VLAN：

- ▶ 用户设置静态 VLAN。
- ▶ 设备自动设置并在前提条件不再适用时删除动态 VLAN。

对于以下功能，设备创建动态 VLAN：

- *MRP*：如果向环网端口分配一个不存在的 VLAN，则设备会创建此 VLAN。
- *MVRP*：设备根据相邻设备的消息创建一个 VLAN。

表格

VLAN ID

VLAN 的 ID。

设备支持最多同时设置 128 个 VLAN。

可能的值：

- ▶ 1..4042

Status

显示 VLAN 是如何设置的。

可能的值：

- ▶ *other*

VLAN 1

或者

使用 *802.1X Port Authentication* 功能设置 VLAN。参见 *Network Security > 802.1X Port Authentication* 对话框。

- ▶ *permanent*

由用户设置 VLAN。

或者

使用 *MRP* 功能设置 VLAN。参见 *Switching > L2-Redundancy > MRP* 对话框。

如果将更改保存到永久存储器中，则具有此设置的 VLAN 在重新启动之后保持设置状态。

- ▶ *dynamicMvrp*

使用 *MVRP* 功能设置 VLAN。参见 *Switching > MRP-IEEE > MVRP* 对话框。

采用此设置的 VLAN 具有写保护。最后一个端口离开 VLAN 后，设备立即从表格中删除 VLAN。

Creation time

显示 VLAN 创建的时间。

该字段显示运行时间（系统正常运行时间）的时间戳。

Name

指定 VLAN 的名称。

可能的值：

- ▶ 带有 1..32 个字符的字母数字 ASCII 字符串

<Port number>

指定相应端口是否传输 VLAN 的数据包以及这些数据包是否包含 VLAN 标签。

可能的值：

- ▶ - (默认设置)
端口不是 VLAN 的成员且不传输 VLAN 的数据包。
- ▶ T = Tagged
端口是 VLAN 的成员且传输带有 VLAN 标签的数据包。例如，可以为上行链路端口使用此设置。
- ▶ LT = Tagged Learned
端口是 VLAN 的成员且传输带有 VLAN 标签的数据包。
设备根据 *GVRP* 或 *MVRP* 功能自动创建了该条目。
- ▶ F = Forbidden
端口不是 VLAN 的成员且不传输此 VLAN 的数据包。
此外，设备有助于通过 *MVRP* 功能防止端口成为 VLAN 成员。
- ▶ U = Untagged (VLAN 1 的默认设置)
端口是 VLAN 的成员且传输不带 VLAN 标签的数据包。如果相连设备不对任何 VLAN 标签进行评估，例如在终端端口上，则可使用此设置。
- ▶ LU = Untagged Learned
端口是 VLAN 的成员且传输不带 VLAN 标签的数据包。
设备根据 *GVRP* 或 *MVRP* 功能自动创建了该条目。

提示： 验证网络管理站所连接的端口是否是设备在其中传输管理数据的 VLAN 的成员。在默认设置下，设备在 VLAN 1 上传输管理数据。否则，将更改传输到设备时，至设备的连接将终止。只能通过串行接口使用命令行界面访问设备管理。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。



打开 *Create* 窗口，向表格中添加一个新的条目。

在 *VLAN ID* 字段中，可以指定 VLAN 的 ID。

5.9.3 VLAN Port

[Switching > VLAN > Port]

在此对话框中，可以指定设备如何处理接收到的不带 VLAN 标签的数据包或其 VLAN 标签与端口 VLAN ID 不同的数据包。

此对话框可用于向端口分配 VLAN 以及指定端口 VLAN ID。

此外，还可以为每个端口指定在出现以下任一情况时设备如何传输数据包：

- ▶ 端口接收不带 VLAN 标签的数据包。
- ▶ 端口接收带有 VLAN 优先级信息的数据包（VLAN ID 0、优先级标签）。
- ▶ 数据包 VLAN 标签与端口的 VLAN ID 不同。

表格

Port

显示端口编号。

Port-VLAN ID

指定设备分配到不带 VLAN 标签的数据包的 VLAN 的 ID。

前提条件：

- 用户可在 *Acceptable packet types* 列中指定值 *admitAll*。

可能的值：

- ▶ 用户设置的 VLAN 的 ID（默认设置：1）

如果使用 *MRP* 功能并且没有向环网端口分配 VLAN，则可在此处为环网端口指定值 1。否则，设备自动将该值分配给环网端口。

Acceptable packet types

指定端口是传输还是丢弃收到的不带 VLAN 标签的数据包。

可能的值：

- ▶ *admitAll*（默认设置）
端口同时接受带有和不带 VLAN 标签的数据包。
- ▶ *admitOnlyVlanTagged*
端口只接受带有 VLAN ID ≥ 1 标签的数据包。

Ingress filtering

激活/停用入口筛选。

可能的值：

▶ **勾选**

入口筛选已激活。

设备将数据包中的 VLAN ID 与设备所属的 VLAN 进行比较。参见 [Switching > VLAN > Configuration](#) 对话框。如果数据包中的 VLAN ID 与其中一个 VLAN 匹配，则端口传输该数据包。否则，设备丢弃该数据包。

▶ **未勾选**（默认设置）

入口筛选已停用。

设备在不比较 VLAN ID 的情况下传输接收到的数据包。因此，端口还传输带有非端口所属的 VLAN ID 的数据包。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

5.9.4 VLAN Voice

[Switching > VLAN > Voice]

使用语音 VLAN 功能按 VLAN 和/或优先级将端口上的语音流量和数据流量分开。语音 VLAN 的一个主要优点是，在端口上的数据流量较高时，可以保证语音流量的质量。

设备使用 Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) 检测 VoIP 电话。然后，设备将适当的端口添加到已配置语音 VLAN 的成员集中。该成员集既可带标签，也可不带标签。标签取决于语音 VLAN 接口模式 (VLAN ID、Dot1p、无、不带标签)。

语音 VLAN 功能的另一个优点是，VoIP 电话可以通过 LLDP-MED 从设备获取 VLAN ID 或优先级信息。因此，VoIP 电话会发送标记为优先级或未标记的语音数据。这取决于已配置的语音 VLAN 接口模式。可在正在连接到 VoIP 电话的端口上激活语音 VLAN。

Operation

Operation

全局启用/禁用设备的 *VLAN Voice* 功能。

可能的值：

- ▶ *On*
- ▶ *Off* (默认设置)

表格

Port

显示端口编号。

Voice VLAN mode

指定端口是传输还是丢弃收到的不带语音 VLAN 标签或带语音 VLAN 优先级信息的数据包。

可能的值：

- ▶ *disabled* (默认设置)
为此表格条目停用 *VLAN Voice* 功能。
- ▶ *none*
让 IP 电话使用自己的配置发送无标记的语音流量。
- ▶ *vlan/dot1p-priority*
端口筛选使用 *vlan* 和 *dot1p* 优先级标签的语音 VLAN 的数据包。
- ▶ *untagged*
端口筛选不带语音 VLAN 标签的数据包。
- ▶ *vlan*
端口筛选使用 *vlan* 标签的语音 VLAN 的数据包。
- ▶ *dot1p-priority*
端口筛选使用 *dot1p* 优先级标签的语音 VLAN 的数据包。如果选择此值，则需另外在 *Priority* 列中指定一个适当的值。

Data priority mode

为特定端口上的数据流量指定信任模式。

当设备检测到 VoIP 电话和 PC 并且当这些设备使用同一根电缆传输和接收数据时，设备会对语音 VLAN 上的数据流量使用此模式。

可能的值：

- ▶ *trust* (默认设置)
如果接口上存在语音流量，则数据流量会使用此设置的正常优先级。
- ▶ *untrust*
如果存在语音流量且 *Voice VLAN mode* 设置为 *dot1p-priority*，则数据具有 0 优先级。如果接口只传输数据，则数据具有正常优先级。

Status

显示端口上语音 VLAN 的状态。

可能的值：

- ▶ *勾选*
语音 VLAN 已启用。
- ▶ *未勾选*
语音 VLAN 已禁用。

VLAN ID

指定对其应用了表格条目的 VLAN 的 ID。

要将流量转发到使用此筛选器的此 VLAN ID，请在 *Voice VLAN mode* 列中选择值 *vlan*。

可能的值：

- ▶ *0..4042*

Priority

指定端口的语音 VLAN 优先级。

前提条件：

- 用户可在 *Voice VLAN mode* 列中指定值 *dot1p-priority*。

可能的值：

- ▶ *0..7*
- ▶ *none*
停用端口的语音 VLAN 优先级。

Bypass authentication

激活语音 VLAN 身份验证模式。

如果停用该功能并且将 *Voice VLAN mode* 列中的值设置为 *dot1p-priority*，则语音设备需要身份验证。

可能的值:

- ▶ 勾选 (默认设置)

如果用户在 *Network Security > 802.1X Port Authentication > Global* 对话框中激活了该功能, 则应在激活此功能之前将此端口的 *Port control* 参数设置为 *multiClient*。可在 *Port control* 对话框中找到 *Network Security > 802.1X Port Authentication > Global* 参数。

- ▶ 未勾选

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

5.10 L2-Redundancy

[Switching > L2-Redundancy]

该菜单包含以下对话框:

- ▶ MRP
- ▶ HIPER Ring
- ▶ Spanning Tree
- ▶ Link Aggregation
- ▶ Link Backup
- ▶ FuseNet

5.10.1 MRP

[Switching > L2-Redundancy > MRP]

警告

不允许的设备操作

为帮助避免在配置阶段出现环路，请分别配置 *MRP* 配置的每个设备。在连接冗余线路之前，应完成环网配置的其他设备的配置。

如果不遵循这些说明，则会导致死亡、重伤或设备损坏。

Media Redundancy Protocol (MRP) 是一种允许用户设置高可用性环形网络结构的协议。采用 Schneider Electric 设备的 MRP 环网由支持符合 IEC 62439 的 MRP 协议的多达 100 台设备组成。

如果某个部分未运行，则 MRP 环的环结构变回线结构。可以配置最大恢复时间。

设备的环网管理器功能可将线形结构骨干两端闭合起来，形成冗余环网。

提示： *Spanning Tree* 和环网冗余可以彼此影响。为连接到 MRP 环网的端口停用 *Spanning Tree* 协议。参见 *Switching > L2-Redundancy > Spanning Tree > Port* 对话框。

处理超大以太网数据包时（*MTU* 列中针对端口的值大于 1518，参见 *Basic Settings > Port* 对话框），MRP 环网重新配置的切换时间取决于以下参数：

- ▶ 环形线路的带宽
- ▶ 以太网数据包的大小
- ▶ 环网中设备的数量

设置足够长的恢复时间，有助于避免设备中的延时导致的 MRP 数据包延迟。IEC 62439-2 第 9.5 节中提供了计算切换时间的公式。

Operation

Operation

启用/禁用 *MRP* 功能。

为 MRP 环网配置了参数后，可在此处启用该功能。

可能的值：

- ▶ *On*
MRP 功能已启用。
对 MRP 环网中的设备进行配置后，冗余激活。
- ▶ *Off*（默认设置）
MRP 功能已禁用。

Ring port 1/Ring port 2

Port

指定作为环网端口工作的端口的编号。

可能的值：

- ▶ *<Port number>*
环网端口的编号

Operation

显示环网端口的工作状态。

可能的值：

- ▶ *forwarding*
端口已启用，存在连接。
- ▶ *blocked*
端口已阻塞，存在连接。
- ▶ *disabled*
端口已禁用。
- ▶ *not-connected*
不存在连接。

Fixed backup

为 *Ring port 2* 激活/停用备份端口功能。

提示： 向主端口的切换会超过最大环网恢复时间。

可能的值：

- ▶ 勾选
Ring port 2 备用功能已激活。环网闭合后，环网管理器会切换回一级环网端口。
- ▶ 未勾选（默认设置）
Ring port 2 备用功能已停用。环网闭合后，环网管理器继续在二级环网端口上发送数据。

Configuration

Ring manager

启用/禁用 *Ring manager* 功能。

如果线路每一端都有一个设备，则激活此功能。

可能的值：

- ▶ *On*
Ring manager 功能已启用。
设备作为环网管理器进行工作。
- ▶ *Off*（默认设置）
Ring manager 功能已禁用。
设备作为环网客户端进行工作。

Advanced mode

激活/停用快速恢复时间的高级模式。

可能的值：

- ▶ **勾选**（默认设置）
高级模式已激活。
支持 MRP 的 Schneider Electric 设备支持此模式。
- ▶ **未勾选**
高级模式已停用。
如果环网中的另一个设备不支持此模式，请选择此设置。

Ring recovery

为环网的重新配置指定最大恢复时间（毫秒）。如果设备作为环网管理器进行工作，则此设置生效。

可能的值：

- ▶ **500ms**
- ▶ **200ms**（默认设置）

如果切换时间较短，则对环网中每个单独设备的响应时间的要求会更高。如果环网中的其他设备也支持这一较短的恢复时间，请使用小于 **500ms** 的数值。

处理超大以太网数据包时，环网中设备的数量受到限制。请注意，切换时间取决于若干个参数。请参见以上描述。

VLAN ID

指定分配给环网端口的 VLAN 的 ID。

可能的值：

- ▶ **0**（默认设置）
未分配 VLAN。
在 *Switching > VLAN > Configuration* 对话框中向 VLAN 1 的环网端口分配值 **U**。
- ▶ **1..4042**
已分配 VLAN。
如果向环网端口分配一个不存在的 VLAN，则设备会创建此 VLAN。在 *Switching > VLAN > Configuration* 对话框中，设备在表格中为该 VLAN 创建一个条目并将值 **T** 分配给环网端口。

Information

Information

显示冗余配置的消息以及检测到错误的可能原因。

当设备作为环网客户端或环网管理器进行工作时，可能会显示以下消息：

- ▶ **Redundancy available**
冗余已设置。当环网的某个组件发生故障时，冗余线路会接替其功能。
- ▶ **Configuration error: Error on ringport link.**
在环网端口的布线中检测到错误。

当设备作为环网管理器进行工作时，可能会显示以下消息：

- ▶ *Configuration error: Packets from another ring manager received.*
环网中存在另一个作为环网管理器进行工作的设备。
只在环网中的一个设备上启用 *Ring manager* 功能。
- ▶ *Configuration error: Ring link is connected to wrong port.*
环网中的一条线路连接至不同的端口，而非环网端口。设备仅在一个环端口上接收测试数据包。

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

Delete ring configuration

禁用冗余功能并将对话框中的设置重置为默认设置。

5.10.2 HIPER Ring

[Switching > L2-Redundancy > HIPER Ring]

警告

不允许的设备操作

为帮助避免在配置阶段出现环路，请分别配置 *HIPER Ring* 配置的每个设备。在连接冗余线路之前，应完成环网配置的其他设备的配置。

如果不遵循这些说明，则会导致死亡、重伤或设备损坏。

HIPER 环网冗余概念可以构成高可用性环形网络。本设备提供一个 HIPER 环网客户端。此功能允许用户对现有 HIPER 环网进行扩展，或替换已经作为客户端参与 HIPER 环网的设备。

HIPER 环网包含一个负责控制环网的环网管理器 (RM)。该 RM 在一级和二级端口上同时向环网发送看门狗数据包。当 RM 在这两个端口上收到看门狗数据包时，一级端口将保持转发状态，二级端口将保持丢弃状态。

设备只在环网客户端模式下工作。也就是说，设备能够识别和转发环网端口上的看门狗数据包，还能够将链路状态变化转发到 RM，如 LinkDown（链路中断）和 LinkUp（链路连接）数据包。

设备只支持将快速以太网和千兆以太网端口作为环网端口。此外，设备仅支持 VLAN 1 中的 HIPER 环。

提示： *Spanning Tree* 和环网冗余可以彼此影响。为连接到 HIPER 环网的端口停用 *Spanning Tree* 协议。参见 *Switching > L2-Redundancy > Spanning Tree > Port* 对话框。

提示： 分别配置 HIPER 环网中的设备。在连接冗余链路之前，应完成 HIPER 环网的每个设备的配置。这样有助于避免在配置阶段出现环路。

Operation

Operation

启用/禁用 *HIPER Ring* 客户端。

可能的值：

- ▶ *On*
HIPER Ring 客户端已启用。
- ▶ *Off*（默认设置）
HIPER Ring 客户端已禁用。

Ring port 1/Ring port 2

Port

指定一级/二级环网端口的端口编号。

可能的值：

- ▶ - (默认设置)
未选择一级/二级环网端口。
- ▶ `<Port number>`
环网端口的编号

State

显示一级/二级环网端口的状态。

可能的值：

- ▶ `not-available`
`HIPER Ring` 客户端已禁用。
或者
未选择一级或二级环网端口。
- ▶ `active`
环网端口已启用，逻辑上已启动。
- ▶ `inactive`
环网端口逻辑上已关闭。
环网端口上的链路中断后，设备立即向其他环网端口上的环网管理器发送一个 LinkDown（链路中断）数据包。

Information

Mode

显示设备能够在环网客户端模式下运行。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

5.10.3 Spanning Tree

[Switching > L2-Redundancy > Spanning Tree]

警告

不允许的设备操作

为帮助避免在配置阶段出现环路，请分别配置 *Spanning Tree* 配置的每个设备。在连接冗余线路之前，应完成 *Spanning Tree* 配置的其他设备的配置。

如果不遵循这些说明，则会导致死亡、重伤或设备损坏。

生成树协议（STP）是一种可以停用网络的冗余路径，以帮助避免出现环路的协议。如果路径上的某个网络组件无法工作，则设备将计算新的拓扑并重新激活这些路径。

快速生成树协议（RSTP）允许在不中断现有连接的情况下快速切换到新计算的拓扑。RSTP 的平均重新配置时间能够小于一秒。在一个由 10 至 20 台设备组成的环网中使用 RSTP 时，重新配置时间能够达到毫秒数量级。

提示：通过双绞线 SFP 而非通常的双绞线端口将设备连接到网络时，网络的重新配置需要稍长的时间。

该菜单包含以下对话框：

- ▶ Spanning Tree Global
- ▶ Spanning Tree Dual RSTP (MCSESM-E)
- ▶ Spanning Tree Port

5.10.3.1 Spanning Tree Global

[Switching > L2-Redundancy > Spanning Tree > Global]

在此对话框中，可以启用/禁用 *Spanning Tree* 功能并指定网桥设置。

Operation

Operation

启用/禁用设备中的生成树功能。

可能的值：

- ▶ *On* (默认设置)
- ▶ *Off*

设备行为透明。设备将多播数据包等接收到的生成树数据包大量发送到端口。

Variant

Variant

显示 *Spanning Tree* 功能使用的协议：

可能的值：

- ▶ *rstp*

协议 RSTP 已激活。

借助 RSTP (IEEE 802.1Q-2005)，*Spanning Tree* 功能对基础物理层产生影响。

Traps

Send trap

为以下事件激活/停用 SNMP 陷阱的发送：

- 另一个网桥接替了根网桥角色。
- 拓扑发生变化。某个端口的 *Port state* 从 *forwarding* 变为 *discarding* 或从 *discarding* 变为 *forwarding*。

可能的值：

- ▶ 勾选
SNMP 陷阱发送激活。
- ▶ 未勾选 (默认设置)
SNMP 陷阱发送停用。

Bridge configuration

Bridge ID

显示设备的网桥 ID。

网桥 ID 数值最小的设备接替网络中根网桥的角色。

可能的值：

- ▶ `<Bridge priority> / <MAC address>`
Priority 字段中的值/设备的 MAC 地址

Priority

指定设备的网桥优先级。

可能的值：

- ▶ `0..61440`（步长为 4096）（默认设置：`32768`）

要使本设备成为根网桥，可将网络中最小的优先级数值分配给设备。

Hello time [s]

指定两条配置消息（Hello 数据包）的发送之间的时间（秒）。

可能的值：

- ▶ `1..2`（默认设置：`2`）

如果设备接替根网桥角色，则网络中的其他设备使用此处指定的值。

否则，设备使用根网桥指定的值。参见 *Root information* 框。

由于与 *Tx holds* 参数的相互影响，我们建议用户不要更改默认设置。

Forward delay [s]

为状态变化指定延迟时间（秒）。

可能的值：

- ▶ `4..30`（默认设置：`15`）

如果设备接替根网桥角色，则网络中的其他设备使用此处指定的值。

否则，设备使用根网桥指定的值。参见 *Root information* 框。

在 RSTP 协议中，网桥协商没有指定延迟的状态变化。

Spanning Tree 协议使用该参数来延迟 *disabled*、*discarding*、*learning* 和 *forwarding* 等状态之间的状态变化。

参数 *Forward delay [s]* 与参数 *Max age* 有以下关系：

$$\textit{Forward delay [s]} \geq (\textit{Max age}/2) + 1$$

如果在这些字段中输入违反这种关系的值，则设备会将这些值替换为最后一个有效值或默认值。

Max age

指定最大允许分支长度，如连接到根网桥的设备的数量。

可能的值：

- ▶ 6..40（默认设置：20）

如果设备接替根网桥角色，则网络中的其他设备使用此处指定的值。

否则，设备使用根网桥指定的值。参见 *Root information* 框。

Spanning Tree 协议使用该参数指定 STP-BPDU 的有效期（秒）。

Tx holds

限制发送 BPDU 的最大传输速率。

可能的值：

- ▶ 1..40（默认设置：10）

当设备发送 BPDU 时，设备会使此端口上的一个计数器进行递增。

如果该计数器达到此处指定的值，则端口会停止发送 BPDU。一方面，这可降低 RSTP 产生的负载，另一方面，当设备不接收 BPDU 时，会导致通信中断。

设备使该计数器每秒递减 1。在下一秒期间，设备最多发送 1 个新的 BPDU。

BPDU guard

激活/停用设备中的 BPDU 保护功能。

利用此功能，设备可帮助保护用户网络免遭错误配置、STP-BPDU 攻击和不需要的拓扑更改。

可能的值：

- ▶ 勾选

BPDU guard 已激活。

- 设备将该功能应用于手动指定的边缘端口。对于这些端口，*Switching > L2-Redundancy > Spanning Tree > Port* 对话框 *CIST* 选项卡 *Admin edge port* 列中的复选框为勾选。
- 如果一个边缘端口收到一个 STP-BPDU，则设备会禁用该端口。对于此端口，*Basic Settings > Port* 对话框 *Configuration* 选项卡 *Port on* 列中的复选框为未勾选。

- ▶ 未勾选（默认设置）

BPDU guard 已停用。

要将端口状态重置为值 *forwarding*，请按照以下步骤进行操作：

- 如果端口仍在接收 BPDU，则：
 - 在 *Switching > L2-Redundancy > Spanning Tree > Port* 对话框的 *CIST* 选项卡中，取消勾选 *Admin edge port* 列中的复选框。
 - 或者
 - 在 *Switching > L2-Redundancy > Spanning Tree > Global* 对话框中，取消勾选 *BPDU guard* 复选框。
- 要再次重新启用该端口，可使用 *Auto-Disable* 功能。或者，请按照以下步骤进行操作：
 - 打开 *Basic Settings > Port* 对话框的 *Configuration* 选项卡。
 - 勾选 *Port on* 列中的复选框。

BPDU filter (all admin edge ports)

在每个手动指定的边缘端口上激活/停用 STP-BPDU 筛选器。对于这些端口，[Switching > L2-Redundancy > Spanning Tree > Port](#) 对话框 *CIST* 选项卡 *Admin edge port* 列中的复选框为勾选。

可能的值：

▶ 勾选

- 每个边缘端口上的 BPDU 筛选器都已激活。
该功能在 [Spanning Tree](#) 操作中不使用这些端口。
- 设备不在这些端口上发送 STP-BPDU。
 - 设备丢弃在这些端口上收到的所有 STP-BPDU。

▶ 未勾选（默认设置）

- 全局 BPDU 筛选器已停用。
可以选择为单个端口明确激活 BPDU 筛选器。参见 [Switching > L2-Redundancy > Spanning Tree > Port](#) 对话框中的 *Port BPDU filter* 列。

Auto-disable

为 [BPDU guard](#) 在端口上监控的参数激活/停用 [Auto-Disable](#) 功能。

可能的值：

▶ 勾选

- [BPDU guard](#) 的 [Auto-Disable](#) 功能已激活。
- 当端口接收到一个 STP-BPDU 时，设备会禁用一个边缘端口。端口的“链路状态”LED 指示灯每个周期闪烁 3 次。
 - [Diagnostics > Ports > Auto-Disable](#) 对话框显示超过参数导致哪些端口当前被禁用。
 - [Auto-Disable](#) 功能自动重新激活端口。为此，可以切换至 [Diagnostics > Ports > Auto-Disable](#) 对话框并在 *Reset timer [s]* 列中为相关端口指定等待期。

▶ 未勾选（默认设置）

- [BPDU guard](#) 的 [Auto-Disable](#) 功能已停用。

Root information

Bridge ID

显示当前根网桥的网桥 ID。

可能的值：

▶ `<Bridge priority> / <MAC address>`

Priority

显示当前根网桥的网桥优先级。

可能的值：

▶ `0..61440`（步长为 4096）

Hello time [s]

显示根网桥指定的两条配置消息（Hello 数据包）发送之间的时间（秒）。

可能的值：

▶ `1..2`

设备使用此指定值。参见 *Bridge configuration* 框。

Forward delay [s]

指定根网桥为状态变化设置的延迟时间（秒）。

可能的值：

▶ `4..30`

设备使用此指定值。参见 *Bridge configuration* 框。

在 RSTP 协议中，网桥协商没有指定延迟的状态变化。

Spanning Tree 协议使用该参数来延迟 *disabled*、*discarding*、*learning* 和 *forwarding* 等状态之间的状态变化。

Max age

指定根网桥设置的最大允许分支长度，如连接到根网桥的设备的数量。

可能的值：

▶ `6..40`（默认设置：20）

Spanning Tree 协议使用该参数指定 STP-BPDU 的有效期（秒）。

Topology information

Bridge is root

显示设备当前是否具有根网桥角色。

可能的值：

- ▶ **勾选**
设备当前具有根网桥角色。
- ▶ **未勾选**
另一个设备当前具有根网桥角色。

Root port

显示当前路径从其连接到根网桥的端口的编号。

如果设备接替根网桥角色，则该字段显示值 **no Port**。

Root path cost

指定从设备根端口连接到第二层网络根网桥的路径的路径开销。

可能的值：

- ▶ **0..200000000**
如果指定了值 **0**，则设备接替根网桥角色。

Topology changes

显示自 *Spanning Tree* 实例开始以来设备使用 *Spanning Tree* 功能将一个端口置于 *forwarding* 状态的次数。

Time since topology change

显示自上次拓扑更改以来的时间。

可能的值：

- ▶ **<days, hours:minutes:seconds>**

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

5.10.3.2 Spanning Tree Dual RSTP (MCSESM-E)

[Switching > L2-Redundancy > Spanning Tree > Dual RSTP]

警告

不允许的设备操作

为帮助避免在配置阶段出现环路，请分别配置 *RCP* 和 *Dual RSTP* 配置的每个设备。在连接冗余线路之前，应完成环网配置的其他设备的配置。

如果不遵循这些说明，则会导致死亡、重伤或设备损坏。

在此对话框中，您指定对应于第二个 *Spanning Tree* 实例的网桥设置

Dual RSTP 功能与 *RCP* 功能一起使用。使用 *RCP* 功能，可以选择将一个或多个 RSTP 环网与一级环网中的 RSTP 实例耦合起来。对两个 *Spanning Tree* 网段进行耦合时，二级环网代表 *Dual RSTP* 功能设置适用的一个不同的 RSTP 实例。此 *Dual RSTP* 实例在工作时独立于一级环网的 RSTP 实例以及其他二级环网。当 RSTP 是仅要在要耦合的一个环网中使用的协议时，不需要 *Dual RSTP* 功能。

可在 *Switching > L2-Redundancy > FuseNet > RCP* 对话框中指定 *RCP* 功能设置。

Operation

Operation

显示设备中的 *Dual RSTP* 功能已启用/禁用。

可能的值：

► On

设备中的 *Dual RSTP* 功能已启用。

如果满足以下条件，则设备启用 *Dual RSTP* 功能：

- 在 *Switching > L2-Redundancy > FuseNet > RCP* 对话框中，您已为 *Primary ring/network* 和 *Secondary ring/network* 设置指定了端口。
- 在 *Switching > L2-Redundancy > FuseNet > RCP* 对话框的 *Operation* 框中，您已启用 *RCP* 功能。
- 在 *Spanning Tree Global* 对话框的 *Operation* 框中，您已启用 *Spanning Tree* 功能。
- 次环中没有配置冗余协议。

► Off (默认设置)

设备中的 *Dual RSTP* 功能已禁用。

Traps

Send trap

为以下事件激活/停用 SNMP 陷阱的发送：

- 另一个网桥接替了根网桥角色。
- 拓扑发生变化。某个端口的 *Port state* 从 *forwarding* 变为 *discarding* 或从 *discarding* 变为 *forwarding*。

可能的值:

- ▶ 勾选 (默认设置)
SNMP 陷阱发送激活。
- ▶ 未勾选
SNMP 陷阱发送停用。

Bridge configuration

Bridge ID

显示设备的网桥 ID。

网桥 ID 数值最小的设备接替网络中根网桥的角色。

可能的值:

- ▶ `<Bridge priority> / <MAC address>`
Priority 字段中的值/设备的 MAC 地址

Priority

指定设备的网桥优先级。

可能的值:

- ▶ `0..61440` (步长为 4096) (默认设置: `32768`)

要使本设备成为根网桥, 可将网络中最小的优先级数值分配给设备。

Hello time [s]

指定两条配置消息 (Hello 数据包) 的发送之间的时间 (秒)。

可能的值:

- ▶ `1..2` (默认设置: `2`)

如果设备接替根网桥角色, 则网络中的其他设备使用此处指定的值。

否则, 设备使用根网桥指定的值。参见 *Root information* 框。

由于与 *Tx holds* 参数的相互影响, 我们建议用户不要更改默认设置。

Forward delay [s]

为状态变化指定延迟时间 (秒)。

可能的值:

- ▶ `4..30` (默认设置: `15`)

如果设备接替根网桥角色, 则网络中的其他设备使用此处指定的值。否则, 设备使用根网桥指定的值。参见 *Root information* 框。

在 RSTP 协议中, 网桥协商没有指定延迟的状态变化。

Spanning Tree 协议使用该参数来延迟 *disabled*、*discarding*、*learning* 和 *forwarding* 等状态之间的状态变化。

参数 *Forward delay [s]* 与参数 *Max age* 有以下关系：

$$\text{Forward delay [s]} \geq (\text{Max age}/2) + 1$$

Max age

指定根网桥路径中允许的最大设备数。

可能的值：

- ▶ 6..40（默认设置：20）

如果设备接替根网桥角色，则网络中的其他设备使用此处指定的值。否则，设备使用根网桥指定的值。参见 *Root information* 框。

Tx holds

限制发送 BPDU 的最大传输速率。

可能的值：

- ▶ 1..40（默认设置：10）

当设备发送 BPDU 时，设备会使此端口上的一个计数器进行递增。

当该计数器达到此处指定的值时，端口将停止发送 BPDU。一方面，这可降低 RSTP 产生的负载，另一方面，当设备不接收 BPDU 时，会导致通信中断。

设备使该计数器每秒递减 1。在下一秒期间，设备最多发送 1 个新的 BPDU。

BPDU guard

激活/停用设备中的 BPDU 保护功能。

利用此功能，设备可帮助保护用户网络免遭错误配置、STP-BPDU 攻击和不需要的拓扑更改。

可能的值：

- ▶ 勾选
 - BPDU guard* 已激活。
 - 设备将该功能应用于手动指定的边缘端口。对于这些端口，*Switching > L2-Redundancy > Spanning Tree > Port* 对话框 *CIST* 选项卡 *Admin edge port* 列中的复选框为勾选。
 - 如果一个边缘端口收到一个 STP-BPDU，则设备会禁用该端口。对于此端口，*Basic Settings > Port* 对话框 *Configuration* 选项卡 *Port on* 列中的复选框为未勾选。
- ▶ 未勾选（默认设置）
 - BPDU guard* 已停用。

要将端口状态重置为值 *forwarding*，请按照以下步骤进行操作：

- 如果端口仍在接收 BPDU：
 - 在 *Switching > L2-Redundancy > Spanning Tree > Port* 对话框的 *CIST* 选项卡中，取消勾选 *Admin edge port* 列中的复选框。
 - 或者
 - 在 *Switching > L2-Redundancy > Spanning Tree > Dual RSTP* 对话框中，取消勾选 *BPDU guard* 复选框。
- 要再次重新启用该端口，请按照以下步骤进行操作：
 - 打开 *Basic Settings > Port* 对话框的 *Configuration* 选项卡。
 - 勾选 *Port on* 列中的复选框。

BPDU filter (all admin edge ports)

在每个手动指定的边缘端口上激活/停用 STP-BPDU 筛选器。对于这些端口，*Switching > L2-Redundancy > Spanning Tree > Port* 对话框 *CIST* 选项卡 *Admin edge port* 列中的复选框为勾选。

可能的值：

- ▶ **勾选**
每个边缘端口上的 BPDU 筛选器都已激活。
该功能在 *Spanning Tree* 操作中不使用这些端口。
 - 设备不在这些端口上发送 STP-BPDU。
 - 设备丢弃在这些端口上收到的所有 STP-BPDU。
- ▶ **未勾选**（默认设置）
全局 BPDU 筛选器已停用。
可以选择为单个端口明确激活 BPDU 筛选器。参见 *Switching > L2-Redundancy > Spanning Tree > Port* 对话框中的 *Port BPDU filter* 列。

Root information

Root ID

显示当前根网桥的网桥 ID。

可能的值：

- ▶ *<Bridge priority> / <MAC address>*

Priority

显示当前根网桥的网桥优先级。

可能的值：

- ▶ *0..61440*（步长为 4096）

Hello time [s]

显示根网桥指定的两条配置消息（Hello 数据包）发送之间的时间（秒）。

可能的值：

- ▶ *1..2*

设备使用此指定值。参见 *Bridge configuration* 框。

Forward delay [s]

指定根网桥为状态变化设置的延迟时间（秒）。

可能的值：

► 4..30

设备使用此指定值。参见 *Bridge configuration* 框。

在 RSTP 协议中，网桥协商没有指定延迟的状态变化。

Spanning Tree 协议使用该参数来延迟 *disabled*、*discarding*、*learning* 和 *forwarding* 等状态之间的状态变化。

Max age

指定根网桥设置的最大允许分支长度，如连接到根网桥的设备的数量。

可能的值：

► 6..40（默认设置：20）

Spanning Tree 协议使用该参数指定 STP-BPDU 的有效期（秒）。

Topology information**Bridge is root**

显示设备当前是否具有根网桥角色。

可能的值：

► 勾选

设备当前具有根网桥角色。

► 未勾选

另一个设备当前具有根网桥角色。

Root port

显示当前路径从其连接到根网桥的端口的编号。

如果设备接替根网桥角色，则该字段显示值 *no Port*。

Root path cost

指定从设备根端口连接到第二层网络根网桥的路径的路径开销。

可能的值：

► 0..200000000

如果指定了值 0，则设备接替根网桥角色。

Topology changes

显示自 *Spanning Tree* 实例开始以来设备使用 *Spanning Tree* 功能将一个端口置于 *forwarding* 状态的次数。

Time since topology change

显示自上次拓扑更改以来的时间。

可能的值：

▶ `<days, hours:minutes:seconds>`

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

5.10.3.3 Spanning Tree Port

[Switching > L2-Redundancy > Spanning Tree > Port]

在此对话框中，可以激活端口上的生成树功能、指定边缘端口和指定各种保护功能的设置。

该对话框包含以下选项卡：

- ▶ [CIST]
- ▶ [Guards]

[CIST]

在此选项卡中，可以选择单独激活端口上的生成树功能、指定边缘端口的设置和查看当前值。缩写词 CIST 表示公共和内部生成树。

提示： 停用正在参与其他第二层冗余协议的端口上的 *Spanning Tree* 功能。否则，冗余协议的运行有可能与预期有所不同。这会导致出现环路。

表格

Port

显示端口编号。

STP active

激活/停用端口上的生成树功能。

可能的值：

- ▶ *勾选* (默认设置)
端口上的 *Spanning Tree* 功能已激活。
- ▶ *未勾选*
端口上的 *Spanning Tree* 功能已停用。
如果 *Spanning Tree* 功能在设备中已启用而在端口上已停用，则端口不会发送 STP-BPDU，并且会丢弃任何收到的 STP-BPDU。

Port state

显示端口的传输状态。

可能的值：

- ▶ *discarding*
端口被阻塞并且只转发 STP-BPDU。
- ▶ *learning*
端口被阻塞，但可以学习接收到的数据包中的 MAC 地址。
- ▶ *forwarding*
端口转发数据包。
- ▶ *disabled*
端口已停用。参见 *Basic Settings > Port* 对话框的 *Configuration* 选项卡。

- ▶ *manualFwd*
端口上的 *Spanning Tree* 功能已禁用。端口转发 STP-BPDU。
- ▶ *notParticipate*
端口不参与 STP。

Port role

显示 CIST 中端口的当前角色。

可能的值：

- ▶ *root*
具有至根网桥的最便宜路径的端口。
- ▶ *alternate*
具有至根网桥的替代路径的端口（当前正在阻塞）。
- ▶ *designated*
避开根网桥的树的一侧的端口（当前正在阻塞）。
- ▶ *backup*
端口接收来自它自己的设备的 STP-BPDU。
- ▶ *disabled*
端口已停用。参见 *Basic Settings > Port* 对话框的 *Configuration* 选项卡。

Port path cost

指定端口的路径开销。

可能的值：

- ▶ 0..200000000（默认设置：0）

当值为 0 时，设备根据端口的数据速率自动计算路径开销。

Port priority

指定端口的优先级。

可能的值：

- ▶ 16..240（步长为 16）（默认设置：128）

此值代表端口 ID 的前四位。

Received bridge ID

显示此端口上次从其接收到 STP-BPDU 的设备的网桥 ID。

可能的值：

- ▶ 对于具有 *designated* 角色的端口，设备显示该端口上次接收到的 STP-BPDU 的信息。这有助于对网络中可能的 STP 问题进行诊断。
- ▶ 对于 *alternate*、*backup*、*master* 和 *root* 等端口角色，在静止状态下（静态拓扑），此信息与 *designated* 端口角色的信息相同。
- ▶ 如果端口没有连接或如果该端口尚未接收到任何 STP-BPDU，则设备显示该端口可以利用 *designated* 角色发送的值。

Received port ID

显示此端口上次从其接收到 STP-BPDU 的设备的端口 ID。

可能的值：

- ▶ 对于具有 *designated* 角色的端口，设备显示该端口上次接收到的 STP-BPDU 的信息。这有助于对网络中可能的 STP 问题进行诊断。
- ▶ 对于 *alternate*、*backup*、*master* 和 *root* 等端口角色，在静止状态下（静态拓扑），此信息与 *designated* 端口角色的信息相同。
- ▶ 如果端口没有连接或如果该端口尚未接收到任何 STP-BPDU，则设备显示该端口可以利用 *designated* 角色发送的值。

Received path cost

显示更高级别网桥具有的从其根端口到根网桥的路径开销。

可能的值：

- ▶ 对于具有 *designated* 角色的端口，设备显示该端口上次接收到的 STP-BPDU 的信息。这有助于对网络中可能的 STP 问题进行诊断。
- ▶ 对于 *alternate*、*backup*、*master* 和 *root* 等端口角色，在静止状态下（静态拓扑），此信息与 *designated* 端口角色的信息相同。
- ▶ 如果端口没有连接或如果该端口尚未接收到任何 STP-BPDU，则设备显示该端口可以利用 *designated* 角色发送的值。

Admin edge port

激活/停用 *Admin edge port* 模式。如果端口连接到一个终端设备，则使用 *Admin edge port* 模式。此设置允许边缘端口在连接后更快地切换到转发状态，从而使终端设备具有更快的可访问性。

可能的值：

- ▶ **勾选**
Admin edge port 模式已激活。
端口连接到一个终端设备。
 - 连接建立后，端口切换到 *forwarding* 状态，而不是预先切换到 *learning* 状态。
 - 如果端口接收到 STP-BPDU 且 BPDU 保护功能已激活，则设备停用该端口。参见 [Switching > L2-Redundancy > Spanning Tree > Global](#)对话框。
- ▶ **未勾选**（默认设置）
Admin edge port 模式已停用。
端口连接到另一个 STP 网桥。
连接建立后，端口切换到 *learning* 状态，然后再切换到 *forwarding* 状态（如果适用的话）。

Auto edge port

激活/停用对用户是否将终端设备连接到端口的自动检测。前提条件是 *Admin edge port* 列中的复选框为未勾选。

可能的值：

- ▶ **勾选**（默认设置）
自动检测已激活。
连接建立之后以及经过 $1.5 \times \text{Hello time [s]}$ 之后，如果端口在此期间没有接收到任何 STP-BPDU，则设备将端口设置为 *forwarding* 状态（默认设置 1.5×2 秒）。
- ▶ **未勾选**
自动检测已停用。
连接建立之后以及经过 *Max age* 之后，设备将端口设置为 *forwarding* 状态。
（默认设置：20 秒）

Oper edge port

显示是否有终端设备或 STP 网桥连接到端口。

可能的值：

- ▶ **勾选**
有一个终端设备连接到端口。该端口不接收任何 STP-BPDU。
- ▶ **未勾选**
有一个 STP 网桥连接到端口。该端口接收 STP-BPDU。

Oper PointToPoint

显示端口是否通过直接全双工链路连接到 STP 设备。

可能的值：

- ▶ **勾选**
端口通过全双工链路直接连接到 STP 设备。两个网桥之间的直接分散通信可以缩短重新配置时间。
- ▶ **未勾选**
端口以另一种方式连接，例如，通过半双工链路或通过集线器。

Port BPDU filter

明确激活/停用端口上的 STP-BPDU 的筛选。

前提条件是该端口是一个手动指定的边缘端口。对于这些端口，*Admin edge port* 列中的复选框为勾选。

可能的值：

- ▶ **勾选**
端口上的 BPDU 筛选器已激活。
该功能不允许该端口执行 *Spanning Tree* 操作。
 - 设备不在该端口上发送 STP-BPDU。
 - 设备丢弃在该端口上收到的所有 STP-BPDU。
- ▶ **未勾选**（默认设置）
端口上的 BPDU 筛选器已停用。
可以选择为每个边缘端口全局激活 BPDU 筛选器。参见 *Switching > L2-Redundancy > Spanning Tree > Global* 对话框的 *Bridge configuration* 框。
如果 *BPDU filter (all admin edge ports)* 复选框为勾选，则端口上的 BPDU 筛选器仍为激活。

BPDU filter status

显示端口上的 BPDU 筛选器是否已激活。

可能的值：

- ▶ **勾选**
以下设置导致端口上的 BPDU 筛选器激活：
 - *Port BPDU filter* 列中的复选框为勾选。
和/或
 - *BPDU filter (all admin edge ports)* 列中的复选框为勾选。参见 *Switching > L2-Redundancy > Spanning Tree > Global* 对话框的 *Bridge configuration* 框。
- ▶ **未勾选**
端口上的 BPDU 筛选器已停用。

BPDU flood

即使端口上的 *Spanning Tree* 功能已停用，仍激活/停用端口上的 *BPDU flood* 模式。设备将端口上收到的 STP-BPDU 泛洪到 *Spanning Tree* 功能已停用并且 *BPDU flood* 模式已激活的端口。

可能的值：

- ▶ 勾选
BPDU flood 模式已激活。
- ▶ 未勾选（默认设置）
BPDU flood 模式已停用。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

[Guards]

此选项卡可用于为端口上的各种保护功能指定设置。

表格

Port

显示端口编号。

Root guard

激活/停用端口上的 STP-BPDU 的监控。前提条件是 *Loop guard* 功能已停用。

借助此设置，设备可帮助保护用户网络免遭错误配置或试图更改拓扑的使用 STP-BPDU 进行的攻击。此设置只适用于具有 *designated* STP 角色的端口。

可能的值：

- ▶ 勾选
STP-BPDU 的监控已激活。
 - 如果端口接收到至根网桥的具有更优路径信息的 STP-BPDU，则设备丢弃该 STP-BPDU 并将端口状态设置为值 *discarding*，而非值 *root*。
 - 如果没有至根网桥的具有更优路径信息的 STP-BPDU，则设备在 $2 \times \text{Hello time [s]}$ 之后重置端口状态。
- ▶ 未勾选（默认设置）
STP-BPDU 的监控已停用。

TCN guard

激活/停用端口上“拓扑更改通知”的监控。借助此设置，设备可帮助保护用户网络免遭试图更改拓扑的使用 STP-BPDU 进行的攻击。

可能的值：

▶ 勾选

“拓扑更改通知”的监控已启用。

- 端口忽略收到的 STP-BPDU 中的拓扑更改标志。
- 如果收到的 BPDU 包含导致拓扑更改的其他信息，则即使 TCN 保护已启用，设备仍对 BPDU 进行处理。

示例：设备接收到针对根网桥的更优路径信息。

▶ 未勾选（默认设置）

“拓扑更改通知”的监控已禁用。

如果设备接收到带有拓扑更改标志的 STP-BPDU，则设备删除端口的地址表并转发拓扑更改通知。

Loop guard

激活/停用端口上环路的监控。前提条件是 *Root guard* 功能已停用。

借助此设置，设备可帮助在端口不再接收到任何 STP-BPDU 时防止环路。仅对具有 *alternate*、*backup* 或 *root* STP 角色的端口使用此设置。

可能的值：

▶ 勾选

环路的监控已激活。例如，如果在远程设备上禁用生成树功能或如果只在接收方向出现连接中断，则这可帮助防止出现环路。

- 如果端口暂时没有接收到任何 STP-BPDU，则设备会将端口状态设置为值 *discarding*，并且勾选 *Loop state* 列中的复选框。
- 如果端口再次接收到 STP-BPDU，则设备会根据 *Port role* 设置端口状态，并且取消勾选 *Loop state* 列中的复选框。

▶ 未勾选（默认设置）

环路的监控已停用。

如果端口暂时没有接收到任何 STP-BPDU，则设备将端口状态设置为值 *forwarding*。

Loop state

显示端口的环路状态是否不一致。

可能的值：

▶ 勾选

端口的环路状态不一致：

- 端口没有接收到任何 STP-BPDU 且 *Loop guard* 功能已启用。
- 设备将端口状态设置为值 *discarding*。因此，设备有助于防止任何潜在的环路。

▶ 未勾选

端口的环路状态一致。该端口接收 STP-BPDU。

Trans. into loop

显示端口的环路状态不一致的次数（勾选 *Loop state* 列中的复选框）。

Trans. out of loop

显示端口的环路状态一致的次数（取消勾选 *Loop state* 列中的复选框）。

BPDU guard effect

显示端口是否作为边缘端口接收到 STP-BPDU。

前提条件：

- 该端口是一个手动指定的边缘端口。在 *Port* 对话框中，*Admin edge port* 列中对应该端口的复选框为勾选。
- 在 *Switching > L2-Redundancy > Spanning Tree > Global* 对话框中，BPDU 保护功能已激活。

可能的值：

▶ 勾选

该端口是一个边缘端口并且接收到了一个 STP-BPDU。设备停用了该端口。对于此端口，*Basic Settings > Port* 对话框 *Configuration* 选项卡 *Port on* 列中的复选框为未勾选。

▶ 未勾选

该端口是一个边缘端口并且没有接收到任何 STP-BPDU，或者该端口不是边缘端口。

要将端口状态重置为值 *forwarding*，请按照以下步骤进行操作：

- 如果端口仍在接收 BPDU，则：
 - 在 *CIST* 选项卡中，取消勾选 *Admin edge port* 列中的复选框。
 - 或者
 - 在 *Switching > L2-Redundancy > Spanning Tree > Global* 对话框中，取消勾选 *BPDU guard* 复选框。
- 要激活该端口，请按照以下步骤进行操作：
 - 打开 *Basic Settings > Port* 对话框的 *Configuration* 选项卡。
 - 勾选 *Port on* 列中的复选框。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

5.10.4 Link Aggregation

[Switching > L2-Redundancy > Link Aggregation]

警告

不允许的设备操作

为帮助避免在配置阶段出现环路，请分别配置 *Link Aggregation* 配置的每个设备。在连接冗余线路之前，应完成 *Link Aggregation* 配置的其他设备的配置。

如果不遵循这些说明，则会导致死亡、重伤或设备损坏。

Link Aggregation 功能允许用户聚合多个并行链路。前提条件是，这些链路具有相同的速度并且均为全双工。与使用单个线路的传统连接相比，其优点在于可用性更高，传输带宽也更高。

借助链路聚合控制协议 (LACP)，可以对物理端口上基于数据包的连续链路状态进行监控。LACP 还有助于确保链路合作伙伴满足聚合前提条件。

如果远程一端不支持链路聚合控制协议 (LACP)，则用户可以使用 *Static link aggregation* 功能。在这种情况下，设备根据链路、链路速度和双工设置对链路进行聚合。

表格

Trunk port

显示 LAG 接口编号。

Name

指定 LAG 接口的名称。

可能的值：

- ▶ 带有 1..15 个字符的字母数字 ASCII 字符串

Link/Status

显示 LAG 接口和物理端口的当前工作状态。

可能的值：

- ▶ *up* (lag/... 行)
LAG 接口处于正常工作状态。
前提条件是：
 - 此 LAG 接口上的 *Static link aggregation* 功能已激活。
 - 或者
 - 分配给 LAG 接口的物理端口上的 LACP 已激活，参见 *LACP active* 列。和
在 *LACP admin key* 列中为 LAG 接口指定的密钥与在 *LACP port actor admin key* 列中为物理端口指定的密钥匹配。
- 和
分配给 LAG 接口的正常工作物理端口的数量大于或等于 *Active ports (min.)* 列中指定的值。
- ▶ *up*
物理端口处于正常工作状态。
- ▶ *down* (lag/... 行)
LAG 接口已关闭。
- ▶ *down*
物理端口已禁用。
或者
电缆未连接或链路未激活。

Active

激活/停用 LAG 接口。

可能的值：

- ▶ **勾选**（默认设置）
LAG 接口已激活。
在激活 LAG 接口时，应考虑以下协议在物理端口上不会正常工作：
 - *PTP*
 - *802.1AS*
- ▶ **未勾选**
LAG 接口已停用。

STP active

激活/停用此 LAG 接口上的 *Spanning Tree* 协议。前提条件是用户在 *Switching > L2-Redundancy > Spanning Tree > Global* 对话框中全局启用了 *Spanning Tree* 功能。

还可以在 *Switching > L2-Redundancy > Spanning Tree > Port* 对话框中激活/停用 LAG 接口上的 *Spanning Tree* 协议。

可能的值：

- ▶ **勾选**（默认设置）
此 LAG 接口上的 *Spanning Tree* 协议已激活。
- ▶ **未勾选**
此 LAG 接口上的 *Spanning Tree* 协议已停用。

Static link aggregation

激活/停用 LAG 接口上的 *Static link aggregation* 功能。即使远程站点不支持 LACP，设备仍将分配的物理端口聚合到 LAG 接口。

可能的值：

- ▶ **勾选**
此 LAG 接口上的 *Static link aggregation* 功能已激活。物理端口获得链路后，设备立即将分配的物理端口聚合到 LAG 接口。设备不发送 LACPDU 并且丢弃收到的 LACPDU。
- ▶ **未勾选**（默认设置）
此 LAG 接口上的 *Static link aggregation* 功能已停用。如果使用 LACP 成功协商了连接，则设备将一个分配的物理端口聚合到 LAG 接口。

MTU

以字节为单位指定 LAG 接口上以太网数据包的最大允许大小。对任何当前的 VLAN 标签均不予考虑。

此设置可用于针对特定应用程序增加以太网数据包的大小。

可能的值：

- ▶ **1518..9720**（默认设置：**1518**）
使用值 **1518** 时，LAG 接口会传输不超过以下大小的以太网数据包：
 - 1518 字节，无 VLAN 标签
(1514 字节 + 4 字节 CRC)
 - 1522 字节，包含 VLAN 标签
(1518 字节 + 4 字节 CRC)

Active ports (min.)

指定要使 LAG 接口保持活动状态而需要激活的物理端口的最小数量。如果活动物理端口的数量小于指定值，则设备停用 LAG 接口。

如果设备中的 *Spanning Tree* 或 *MRP over LAG* 等冗余功能已激活，则使用此功能强制设备自动切换到冗余线路。

可能的值：

- ▶ 1 (默认设置)
- ▶ 2
- ▶ 视硬件而定：
 - 4
 - 8
 - 32

Type

显示 LAG 接口是基于 *Static link aggregation* 功能还是基于 LACP。

可能的值：

- ▶ *static*
LAG 接口基于 *Static link aggregation* 功能。
- ▶ *dynamic*
LAG 接口基于 LACP。

Send trap (Link up/down)

激活/停用当设备检测到此接口上行/下行状态发生变化时 SNMP 陷阱的发送。

可能的值：

- ▶ 勾选 (默认设置)
SNMP 陷阱发送激活。
如果设备检测到上行/下行状态发生变化，则设备发送一个 SNMP 陷阱。
- ▶ 未勾选
SNMP 陷阱发送停用。

发送 SNMP 陷阱的前提条件是，用户在 *Diagnostics > Status Configuration > Alarms (Traps)* 中启用该功能并至少指定一个陷阱目的地。

LACP admin key

指定 LAG 接口密钥。设备使用此密钥识别可以聚合到 LAG 接口的端口。

可能的值：

- ▶ 0..65535
可以在 *LACP port actor admin key* 列中为物理端口指定对应值。

Port

显示分配给 LAG 接口的物理端口编号。

Aggregation port status

显示 LAG 接口是否聚合该物理端口。

可能的值：

- ▶ *active*
LAG 接口聚合该物理端口。
- ▶ *inactive*
LAG 接口不聚合该物理端口。

LACP active

激活/停用物理端口上的 LACP。

可能的值：

- ▶ 勾选（默认设置）
物理端口上的 LACP 已激活。
- ▶ 未勾选
物理端口上的 LACP 已停用。

LACP port actor admin key

指定物理端口密钥。设备使用此密钥识别可以聚合到 LAG 接口的端口。

可能的值：

- ▶ 0
设备在决定将端口聚合到 LAG 接口时忽略此物理端口上的密钥。
- ▶ 1..65535
如果该值与 *LACP admin key* 列中指定的 LAG 接口的值匹配，则设备只将此物理端口聚合到 LAG 接口。

LACP actor admin state

指定 LAG 接口在 LACPDU 中传输的参与者状态值。这可用于控制 LACPDU 参数。

设备允许用户对这些值进行混合。在下拉列表中，选择一个或多个值。

可能的值：

- ▶ *ACT*
(*LACP_Activity* 状态)
选中后，链路循环传输 LACPDU，否则，仅在请求时才传输。
- ▶ *STO*
(*LACP_Timeout* 状态)
选中后，链路使用较短超时循环传输 LACPDU，否则，使用较长超时进行传输。
- ▶ *AGG*
(*Aggregation* 状态)
选中后，设备将链路解释为聚合候选者，否则，解释为单独链路。

有关值的更多信息，请参见 IEEE 802.1AX-2014 标准。

LACP actor oper state

显示 LAG 接口在 LACPDU 中传输的参与者状态值。

可能的值：

- ▶ *ACT*
(*LACP_Activity* 状态)
可见时，链路循环传输 LACPDU，否则，仅在请求时才传输。
- ▶ *STO*
(*LACP_Timeout* 状态)
可见时，链路使用较短超时循环传输 LACPDU，否则，使用较长超时进行传输。
- ▶ *AGG*
(*Aggregation* 状态)
可见时，设备将链路解释为聚合候选者，否则，解释为单独链路。
- ▶ *SYN*
(*Synchronization* 状态)
可见时，设备将链路解释为 *IN_SYNC*，否则，解释为 *OUT_OF_SYNC*。
- ▶ *COL*
(*Collecting* 状态)
可见时，此链路上启用发入帧的收集，否则禁用。
- ▶ *DST*
(*Distributing* 状态)
可见时，此链路上启用发出帧的分发，否则禁用。
- ▶ *DFT*
(*Defaulted* 状态)
可见时，链路使用管理员为合作伙伴指定的默认运行信息。否则，链路使用从 LACPDU 收到的运行信息。
- ▶ *EXP*
(*Expired* 状态)
可见时，链路接收器处于 *EXPIRED* 状态。

LACP partner oper SysID

显示连接到此物理端口的远程设备的 MAC 地址。

LAG 接口在来自合作伙伴的 LACPDU 中接收到此信息。

LACP partner oper port

显示连接到此物理端口的远程设备的端口编号。

LAG 接口在来自合作伙伴的 LACPDU 中接收到此信息。

LACP partner oper port state

显示 LAG 接口在 LACPDU 中接收到的合作伙伴状态值。

可能的值：

- ▶ *ACT*
- ▶ *STO*
- ▶ *AGG*
- ▶ *SYN*
- ▶ *COL*
- ▶ *DST*

- ▶ *DFT*
- ▶ *EXP*

有关值的更多信息，请参见 *LACP actor oper state* 列的描述以及 IEEE 802.1AX-2014 标准。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。



打开 *Create* 窗口，向表格中添加一个新的 LAG 接口条目或向 LAG 接口分配一个物理端口。

- ▶ 在 *Trunk port* 下拉列表中，可以选择 LAG 接口编号。
- ▶ 在 *Port* 下拉列表中，可以选择要分配给 LAG 接口的物理端口的编号。

创建 LAG 接口后，设备会将该 LAG 接口添加到 *Basic Settings > Port* 对话框 *Statistics* 选项卡的表格中。

5.10.5 Link Backup

[Switching > L2-Redundancy > Link Backup]

警告

不允许的设备操作

为帮助避免在配置阶段出现环路，请分别配置 *Link Backup* 配置的每个设备。在连接冗余线路之前，应完成 *Link Backup* 配置的其他设备的配置。

如果不遵循这些说明，则会导致死亡、重伤或设备损坏。

借助链路备份，可以配置成对的冗余链路。每一对都有一个主端口和一个备份端口。主端口转发流量，直到设备检测到错误为止。如果设备在主端口上检测到错误，则链路备份功能会将流量传输到备份端口。

该对话框还可用于设置故障恢复选项。如果启用故障恢复功能且主端口恢复正常运行，则设备首先阻塞备份端口上的流量，然后转发主端口上的流量。此过程有助于防止设备在网络中形成环路。

Operation

Operation

全局启用/禁用设备中的链路备份功能。

可能的值：

- ▶ *On*
启用链路备份功能。
- ▶ *Off* (默认设置)
禁用链路备份功能。

表格

Primary port

显示接口对的主端口。启用链路备份功能后，此端口负责转发流量。

可能的值：

- ▶ 物理端口

Backup port

显示当设备在主端口上检测到错误时设备转发流量所用的备份端口。

可能的值：

- ▶ 除被设为主端口的端口以外的物理端口。

Description

指定链路备份对。输入一个标识备份对的名称。

可能的值：

- ▶ 带有 0..255 个字符的字母数字 ASCII 字符串

Primary port status

显示此链路备份对的主端口的状态。

可能的值：

- ▶ *forwarding*
链路正常工作，无关闭，正在转发流量。
- ▶ *blocking*
链路正常工作，无关闭，正在阻塞流量。
- ▶ *down*
端口链路断开、电缆拔出、在软件中被禁用或关闭。
- ▶ *unknown*
链路备份功能被全局禁用或端口对已停用。因此，设备忽略端口对设置。

Backup port status

显示此链路备份对的备份端口的状态。

可能的值：

- ▶ *forwarding*
链路正常工作，无关闭，正在转发流量。
- ▶ *blocking*
链路正常工作，无关闭，正在阻塞流量。
- ▶ *down*
端口链路断开、电缆拔出、在软件中被禁用或关闭。
- ▶ *unknown*
链路备份功能被全局禁用或端口对已停用。因此，设备忽略端口对设置。

Fail back

激活/停用自动故障恢复。

可能的值：

- ▶ **勾选**（默认设置）
自动故障恢复已激活。
延迟计时器到期后，备份端口变为 *blocking*，主端口变为 *forwarding*。
- ▶ **未勾选**
自动故障恢复已停用。
即使在主端口重新建立一个链路或用户手动将主端口的管理状态从 *shutdown* 改为 *no shutdown* 之后，备份端口仍继续转发流量。

Fail back delay [s]

指定设备在主端口重新建立链路后等待的延迟时间（秒）。此外，当用户手动将主端口的管理状态从 *shutdown* 设为 *no shutdown* 时，此计时器也适用。延迟计时器到期后，备份端口变为 *blocking*，主端口变为 *forwarding*。

可能的值：

- ▶ **0..3600**（默认设置：30）
设置为 0 时，在主端口重新建立链路之后，备份端口立即变为 *blocking*，主端口立即变为 *forwarding*。此外，在用户手动将管理状态从 *shutdown* 设为 *no shutdown* 之后，备份端口立即变为 *blocking*，主端口立即变为 *forwarding*。

Active

激活/停用链路备份对配置。

可能的值：

- ▶ **勾选**
链路备份对已激活。设备感知链路和管理状态，并根据对配置转发流量。
- ▶ **未勾选**（默认设置）
链路备份对已停用。端口按照标准交换转发流量。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

Create

Primary port

指定备份接口对的主端口。在正常运行期间，此端口负责转发流量。

可能的值：

- ▶ 物理端口

Backup port

指定当设备在主端口上检测到错误时向其传输流量的备份端口。

可能的值：

- ▶ 除被设为主端口的端口以外的物理端口。

5.10.6 FuseNet

[Switching > L2-Redundancy > FuseNet]

FuseNet 协议允许用户对使用以下任一冗余协议工作的环网进行耦合：

- ▶ MRP
- ▶ HIPER 环网
- ▶ RSTP

提示： 如果使用 *Ring/Network Coupling* 协议对网络进行耦合，则应验证网络是否只包含 Schneider Electric 设备。

使用下表选择要在用户网络中使用的 *FuseNet* 耦合协议：

主环网	连接的网络		
	MRP	HIPER 环网	RSTP
MRP	<i>Sub Ring</i> ¹⁾	<i>Redundant Coupling Protocol</i> <i>Ring/Network Coupling</i>	<i>Redundant Coupling Protocol</i> <i>Ring/Network Coupling</i>
HIPER 环网	<i>Sub Ring</i>	<i>Ring/Network Coupling</i>	<i>Redundant Coupling Protocol</i> <i>Ring/Network Coupling</i>
RSTP	<i>Redundant Coupling Protocol</i>	<i>Redundant Coupling Protocol</i>	<i>Dual RSTP</i>

- 无适用的耦合协议

1) 使用在不同 VLAN 上配置的 *MRP*

该菜单包含以下对话框：

- ▶ *Sub Ring*
- ▶ *Ring/Network Coupling*
- ▶ *Redundant Coupling Protocol (MCSESM-E)*

5.10.6.1 Sub Ring

[Switching > L2-Redundancy > FuseNet > Sub Ring]

警告

不允许的设备操作

为帮助避免在配置阶段出现环路，请分别配置 *Sub Ring* 配置的每个设备。在连接冗余线路之前，应完成环网配置的其他设备的配置。

如果不遵循这些说明，则会导致死亡、重伤或设备损坏。

此对话框允许用户将设备设置为子环网管理器。

Sub Ring 功能允许用户将网段轻松耦合到现有冗余环网。子环网管理器 (SRM) 可将子环网耦合到现有环网 (基础环网)。

在子环网中，可以使用支持 MRP 的任何设备作为环网参与者。这些设备不需要子环网管理器功能。

设置子环网时，请记住以下规则：

- ▶ 设备支持子环网中的 *Link Aggregation*
- ▶ 子环网端口上不允许生成树
- ▶ 一个子环网中设备上的 *MRP domain* 相同
- ▶ 基础环网和子环网的 VLAN 不同

按如下方式指定 VLAN 设置：

- ▶ VLAN X 用于基础环网
 - 在基础环网参与者的环网端口上
 - 在子环网管理器的基础环网端口上
- ▶ VLAN Y 用于子环网
 - 在子环网参与者的环网端口上
 - 在子环网管理器的子环网端口上

提示：为帮助避免环路，仅在参与环网的每个设备中都指定了设置后再关闭冗余线路。

Operation

Operation

启用/禁用 *Sub Ring* 功能。

可能的值：

- ▶ *On*
Sub Ring 功能已启用。
- ▶ *Off* (默认设置)
Sub Ring 功能已禁用。

Information

Table entries (max.)

显示设备支持的子环网的最大数量。

表格

Sub ring ID

显示此子环网的唯一标识符。

可能的值:

- ▶ 1..8

Name

指定子环网的可选名称。

可能的值:

- ▶ 带有 0..255 个字符的字母数字 ASCII 字符串

Active

激活/停用子环网。

当每个子环网设备的配置完成时激活子环网。仅在激活 *Sub Ring* 功能之后闭合子环网。

可能的值:

- ▶ 勾选
子环网已激活。
- ▶ 未勾选 (默认设置)
子环网已停用。

Configuration status

显示子环网配置的工作状态。

可能的值:

- ▶ *noError*
设备检测一个可接受的子环网配置。
- ▶ *ringPortLinkError*
 - 环网端口无链路。
 - 其中一个子环网线路连接到设备的又一个端口。但是，该子环网线路没有连接到设备的任一环网端口。
- ▶ *multipleSRM*
子环网管理器接收到来自子环网中一个以上子环网管理器的数据包。
- ▶ *noPartnerManager*
子环网管理器接收到它自己的帧。
- ▶ *concurrentVLAN*
基础环网中的 MRP 协议使用子环网管理器域的 VLAN。

- ▶ *concurrentPort*
又一个冗余协议使用子环网管理器域的环网端口。
- ▶ *concurrentRedundancy*
又一个冗余协议激活导致子环网管理器域停用。
- ▶ *trunkMember*
子环网管理器域的环网端口是 *Link Aggregation* 连接的成员。
- ▶ *sharedVLAN*
共享 VLAN 激活且主环网也使用 MRP 协议导致子环网管理器域停用。

Redundancy available

显示子环网中环网冗余的工作状态。

可能的值：

- ▶ *redGuaranteed*
冗余储备可用。
- ▶ *redNotGuaranteed*
冗余储备丧失。

Port

指定将设备连接到子环网的端口。

可能的值：

- ▶ *<Port number>*

SRM mode

指定子环网管理器的模式。

一个子环网同时具有两个将子环网耦合到基础环网的管理器。只要物理关闭子环网，一个管理器就会阻止其子环网端口。

可能的值：

- ▶ *manager*（默认设置）
子环网端口转发数据包。
当在将子环网耦合到基础环网的两个设备上设置了此值时，具有较高 MAC 地址的设备将作为 *redundantManager*。
- ▶ *redundantManager*
当子环网在物理上闭合时子环网端口被阻塞。如果子环网出现中断，则子环网端口传输数据包。
当在将子环网耦合到基础环网的两个设备上设置了此值时，具有较高 MAC 地址的设备将作为 *redundantManager*。
- ▶ *singleManager*
当子环网通过一个设备耦合到基础环网时，请使用此值。前提条件是表格中存在子环网的 2 个实例。将此值分配给这两个实例。当子环网在物理上闭合时具有较高端口编号的实例的子环网端口被阻塞。

SRM status

显示子环网管理器的当前模式。

可能的值：

- ▶ *manager*
子环网端口转发数据包。
- ▶ *redundantManager*
当子环网在物理上闭合时子环网端口被阻塞。如果子环网出现中断，则子环网端口传输数据包。
- ▶ *singleManager*
子环网通过一个设备耦合到基础环网。当子环网在物理上闭合时具有较高端口编号的实例的子环网端口被阻塞。
- ▶ *disabled*
子环网已停用。

Port status

显示子环网端口的连接状态。

可能的值：

- ▶ *forwarding*
端口根据 IEEE 802.1D 的转发行为传送帧。
- ▶ *disabled*
端口丢弃每个帧。
- ▶ *blocked*
除以下情况之外端口丢弃每个帧：
 - 端口传送指定用于通过被阻塞端口的选定环网协议所使用的帧。
 - 端口传送来自指定用于通过被阻塞端口的其他协议的帧。
- ▶ *not-connected*
端口链路关闭。

VLAN

指定对其分配了此子环网的 VLAN。如果输入的 VLAN ID 项下不存在 VLAN，则设备自动创建一个 VLAN。

可能的值：

- ▶ 可用的已配置 VLAN（默认设置：0）
如果不希望为此子环网使用一个单独的 VLAN，则可将该条目留为 0。

Partner MAC

显示子环网另一端子环网管理器的 MAC 地址。

MRP domain

指定子环网管理器的 MRP 域。向一个子环网的每个成员分配相同的 MRP 域名。如果用户仅使用 Schneider Electric 设备，则可使用 MRP 域的默认值，否则，应根据需要调整此值。使用多个子环网时，该功能允许用户对这些子环网使用相同的 MRP 域名。

可能的值：

▶ 允许的 MRP 域名（默认设置：

`255.255.255.255.255.255.255.255.255.255.255.255.255.255`）

Protocol

指定协议。

可能的值：

▶ `iec-62439-mrp`

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

5.10.6.2 Ring/Network Coupling

[Switching > L2-Redundancy > FuseNet > Ring/Network Coupling]

警告

不允许的设备操作

为帮助避免在配置阶段出现环路，请分别配置 *Ring/Network Coupling* 配置的每个设备。在连接冗余线路之前，应完成环网配置的其他设备的配置。

如果不遵循这些说明，则会导致死亡、重伤或设备损坏。

可以使用 *Ring/Network Coupling* 功能将一个现有的 HIPER 环网、MRP 环网或 Fast HIPER 环网冗余地耦合到另一个网络或另一个环网。验证耦合伙伴是否为 Schneider Electric 设备。

提示：使用双交换机耦合时，请验证在配置 *Ring/Network Coupling* 功能之前是否已配置 HIPER 环网、MRP 环网或 Fast HIPER 环网。

在 *Ring/Network Coupling* 对话框中，可以执行以下任务：

- ▶ 显示现有 *Ring/Network Coupling* 的概览
- ▶ 配置 *Ring/Network Coupling*
- ▶ 创建新的 *Ring/Network Coupling*
- ▶ 删除 *Ring/Network Coupling*
- ▶ 启用/禁用 *Ring/Network Coupling*

配置耦合端口时，可在 *Basic Settings > Port* 对话框中指定以下设置：

端口类型	比特率	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	勾选	未勾选	100 Mbit/s FDX
TX	1 Gbit/s	勾选	勾选	-
Optical	100 Mbit/s	勾选	未勾选	100 Mbit/s FDX
Optical	1 Gbit/s	勾选	勾选	-
光学	2.5 Gbit/s	勾选	-	2.5 Gbit/s FDX

提示：实际可用的端口的运行模式取决于设备配置。

如果配置了 VLAN，则请注意耦合和合作伙伴耦合端口的 VLAN 配置。在 *Ring/Network Coupling* 配置中，为耦合和合作伙伴耦合端口选择以下值：

- ▶ VLAN ID 1 并在端口表中禁用 *Ingress filtering*
- ▶ *VLAN Configuration* 表中的 VLAN 成员资格 T

独立于 VLAN 设置，设备发送带有 VLAN ID 1 和优先级 7 的环网耦合帧。验证设备在本地环网和相连网络中是否发送带标签的 VLAN 1 帧。在 VLAN 帧上添加标签后，可保持环网耦合帧的优先级。

Ring/Network Coupling 功能可对测试数据包进行操作。设备发送其带有 VLAN 标签的测试数据包，包括 VLAN ID 1 和最高 VLAN 优先级 7。如果转发端口是 VLAN 1 中的成员并且传输不带 VLAN 标签的数据包，则设备也会发送测试数据包。

Operation

Operation

启用/禁用 *Ring/Network Coupling* 功能。

可能的值:

- ▶ *On*
Ring/Network Coupling 功能已启用。
- ▶ *Off* (默认设置)
Ring/Network Coupling 功能已禁用。

Mode

Type

指定用于将网络耦合在一起的方法。

可能的值:

- ▶ *one-switch coupling*
可用于在 *Coupling port* 框中和 *Partner coupling port* 框中指定端口设置。
- ▶ *two-switch coupling, master*
可用于在 *Coupling port* 框中指定端口设置。
- ▶ *two-switch coupling, slave*
可用于在 *Coupling port* 框中指定端口设置。
- ▶ *two-switch coupling with control line, master*
可用于在 *Coupling port* 框中和 *Control port* 框中指定端口设置。
- ▶ *two-switch coupling with control line, slave*
可用于在 *Coupling port* 框中和 *Control port* 框中指定端口设置。

Coupling port

Port

指定向其连接冗余链路的端口。

可能的值:

- ▶ -
未选择端口。
- ▶ <Port number>

如果还配置了环网端口，则在不同端口上指定耦合端口和环网端口。

为帮助防止出现连续环路，设备在以下情况下禁用耦合端口：

- ▶ 禁用功能时
- ▶ 在端口上存在工作的连接的情况下更改配置时

当设备已禁用耦合端口时，*Basic Settings > Port* 对话框 *Configuration* 选项卡中的 *Port on* 复选框为未勾选。

State

显示所选端口的状态。

可能的值：

- ▶ *active*
端口已激活。
- ▶ *standby*
端口处于待机模式。
- ▶ *not-connected*
端口未连接。
- ▶ *not-applicable*
端口与配置的控制模式不兼容。

Partner coupling port

Port

指定通过其连接合作伙伴端口的端口。

可能的值：

- ▶ -
未选择端口。
- ▶ <Port number>

如果还配置了环网端口，则在不同端口上指定耦合端口和环网端口。

State

显示所选端口的状态。

可能的值：

- ▶ *active*
端口已激活。
- ▶ *standby*
端口处于待机模式。
- ▶ *not-connected*
端口未连接。
- ▶ *not-applicable*
端口与配置的控制模式不兼容。

IP address

显示连接设备后合作伙伴的 IP 地址。

前提条件是选择一种双交换机耦合方法并在网络中启用合作伙伴。

Control port

Port

指定通过其连接控制线路的端口。

可能的值：

- ▶ -
未选择端口。
- ▶ <Port number>

State

显示所选端口的状态。

可能的值：

- ▶ *active*
端口已激活。
- ▶ *standby*
端口处于待机模式。
- ▶ *not-connected*
端口未连接。
- ▶ *not-applicable*
端口与配置的控制模式不兼容。

Configuration

Redundancy mode

指定设备是否响应在远程环或网络中检测到的故障。

可能的值：

- ▶ *redundant ring/network coupling*
主线路或冗余线路已激活。两条线路未同时激活。如果设备检测到在相连网络中的设备之间出现链路中断，则备用设备会使冗余端口保持在待机模式。
- ▶ *extended redundancy*
主线路和冗余线路同时激活。如果设备检测到在相连网络中的设备之间出现连接问题，则备用设备会在冗余端口上转发数据。使用该设置，可以保持远程网络中的连续性。

提示：在重新配置期间，会出现数据包重复。因此，如果用户的应用程序能够检测数据包重复，则可选择此设置。

Coupling mode

指定耦合特定类型网络的模式。

可能的值：

- ▶ *ring coupling*
设备对冗余环网进行耦合。设备允许用户对使用以下冗余协议的环网进行耦合：
 - HIPER 环网
 - Fast HIPER 环网
 - MRP 环网
- ▶ *network coupling*
设备对网段进行耦合。该功能允许用户将网状网络和总线网络耦合在一起。

Information

Redundancy available

显示冗余是否可用。

当环网的某个组件发生故障时，冗余线路会接替其功能。

可能的值：

- ▶ *redGuaranteed*
冗余可用。
- ▶ *redNotGuaranteed*
冗余不可用。

Configuration failure

功能配置错误或环网端口连接不存在。

可能的值：

- ▶ *noError*
- ▶ *slaveCouplingLinkError*
耦合线路未连接到从设备的耦合端口。相反，耦合线路连接到从设备的另一个端口。
- ▶ *slaveControlLinkError*
从设备的控制端口没有数据链路。
- ▶ *masterControlLinkError*
控制线路未连接到主设备的控制端口。相反，控制线路连接到主设备的另一个端口。
- ▶ *twoSlaves*
控制线路连接了两个从设备。
- ▶ *localPartnerLinkError*
合作伙伴耦合线路未连接到从设备的合作伙伴耦合端口。相反，合作伙伴耦合线路连接到 *one-switch coupling* 模式下从设备的另一个端口。
- ▶ *localInvalidCouplingPort*
在 *one-switch coupling* 模式下，耦合线路未作为合作伙伴线路连接在同一个设备上。相反，耦合线路连接到另一个设备。
- ▶ *couplingPortNotAvailable*
耦合端口不可用，因为端口引用的模块不可用或此模块上不存在该端口。

- ▶ *controlPortNotAvailable*
控制端口不可用，因为端口引用的模块不可用或此模块上不存在该端口。
- ▶ *partnerPortNotAvailable*
合作伙伴耦合端口不可用，因为端口引用的模块不可用或此模块上不存在该端口。

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

Reset

禁用冗余功能并将对话框中的参数重置为默认设置。

5.10.6.3 Redundant Coupling Protocol (MCSESM-E)

[Switching > L2-Redundancy > FuseNet > RCP]

警告

不允许的设备操作

为帮助避免在配置阶段出现环路，请分别配置 *RCP* 配置的每个设备。在连接冗余线路之前，应完成环网配置的其他设备的配置。

如果不遵循这些说明，则会导致死亡、重伤或设备损坏。

警告

环路危险

- ▶ 分别配置 *RCP* 和 *Dual RSTP* 配置的每个设备。在连接冗余线路之前，应完成环网配置的其他设备的配置。
- ▶ 将 *RCP* 耦合配置中的超时配置为长于针对冗余协议的更快速实例的最长假设中断时间。
- ▶ 在一个具有两个耦合网桥的拓扑中，将两个设备的耦合角色只配置为 *master*、*slave* 或 *auto*。
- ▶ 只通过 1 个 *RCP* 网桥（对于具有 1 个 *RCP* 网桥的拓扑）或通过 2 个 *RCP* 网桥（对于具有 2 个 *RCP* 网桥的拓扑）对主实例和辅助实例进行耦合。将主实例的端口与每个辅助实例的端口分开。
- ▶ 只在有终端设备连接到端口的情况下激活端口上的 *Admin edge port* 设置。

如果不遵循这些说明，则会导致死亡、重伤或设备损坏。

环网拓扑的特点是过渡时间短、资源使用最少。但是，要将这些环网冗余地耦合到更高级别网络，难度也更大。

当您希望使用 MRP 等标准协议实现环网冗余并使用 RSTP 将环网耦合在一起时，*Redundant Coupling Protocol* 有助于为您提供选择。

不要在 *RCP* 一级环网和 *RCP* 二级环网的端口上使用以下冗余协议：

- ▶ *Sub Ring*
- ▶ *Ring/Network Coupling*

如果您希望对一级和二级环网使用 RSTP，则 *RCP* 功能会将二级环网的端口分配给 *Dual RSTP* 实例。这会创建通过 *RCP* 耦合的两个独立的 RSTP 网络。可在 *Switching > L2-Redundancy* 对话框中指定 *Dual RSTP* 功能的设置。

如果在网络中配置 *RCP* 功能且配置尚未完成，则设备可能会暂时断开二级环网与一级环网的连接。在这种情况下，从二级环网无法访问 *RCP* 网桥的设备管理。在此配置阶段，请将您的管理站连接到一级环网。

Operation

Operation

启用/禁用 *RCP* 功能。

可能的值:

- ▶ *On*
RCP 功能已启用。
- ▶ *Off* (默认设置)
RCP 功能已禁用。

Primary ring/network / Secondary ring/network

如果设备作为从设备进行工作 (*Role* 字段中的值为 *slave*)，则不要为二级环网/网络上的端口激活 *Static query port* 模式。

Inner port

指定一级环网/二级环网中的内部端口编号。端口直接连接到合作伙伴网桥。

可能的值:

- ▶ - (默认设置)
未选择端口。
- ▶ <Port number>

Outer port

指定一级环网/二级环网中的外部端口编号。

可能的值:

- ▶ - (默认设置)
未选择端口。
- ▶ <Port number>

Primary Ring protocol/Secondary Ring protocol

显示一级/二级环网冗余耦合端口上活动的协议。

Coupler configuration

Role

指定本地设备的角色。

可能的值:

- ▶ *master*
设备作为主设备进行工作。
- ▶ *slave*
设备作为从设备进行工作。

- ▶ *single*
设备使用一个网桥将两个 RSTP 网络与一个 *Dual RSTP* 实例耦合起来。
- ▶ *auto* (默认设置)
设备自动选择角色 *master* 或 *slave*。

Current role

显示本地设备的当前角色。该值可能与配置的角色不同：

- ▶ 如果将两个合作伙伴网桥都配置为 *auto*，则当前正在耦合实例的合作伙伴网桥承担 *master* 角色。另一个合作伙伴网桥承担 *slave* 角色。
- ▶ 如果将两个合作伙伴网桥都配置为 *master* 或都配置为 *slave*，则基本 MAC 地址较小的合作伙伴网桥承担 *master* 角色。
另一个合作伙伴网桥承担 *slave* 角色。
- ▶ 如果协议已启动并且在配置的角色 *master*、*slave* 或 *auto* 中找不到某个网桥的合作伙伴网桥，则该网桥将自己的角色设置为 *listening*。
- ▶ 如果设备检测到配置问题，例如，内部环网端口交叉连接，则设备将其角色设置为 *error*。

Timeout [ms]

指定从设备接替耦合之前在外端口上等待来自主设备的测试数据包的最长时间（毫秒）。这只适用于从设备的两个内部端口都与主设备失去连接的状况。

将超时配置为长于针对更快速实例的冗余协议的最长假设中断时间。否则，会出现环路。

可能的值：

- ▶ 5..60000 (默认设置：45)

Partner MAC address

显示合作伙伴设备的基本 MAC 地址。

Partner IP address

显示合作伙伴设备的 IP 地址。

Coupling state

显示本地设备的耦合状态。

可能的值：

- ▶ *forwarding*
端口的耦合状态为转发。
- ▶ *blocking*
端口的耦合状态为阻塞。

Redundancy state

显示冗余是否可用。

对于主-从配置，两个网桥都显示此信息。

可能的值：

- ▶ *redAvailable*
冗余可用。
- ▶ *redNotAvailable*
冗余不可用。

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

6 Diagnostics

该菜单包含以下对话框：

- ▶ Status Configuration
- ▶ System
- ▶ Email Notification
- ▶ Syslog
- ▶ Ports
- ▶ Loop Protection
- ▶ LLDP
- ▶ Report

6.1 Status Configuration

[Diagnostics > Status Configuration]

该菜单包含以下对话框：

- ▶ Device Status
- ▶ Security Status
- ▶ Signal Contact
- ▶ MAC Notification
- ▶ Alarms (Traps)

6.1.1 Device Status

[Diagnostics > Status Configuration > Device Status]

设备状态提供了设备整体状况的概览。很多过程可视化系统都会记录设备的设备状态，以便以图形形式呈现设备的状况。

设备在 *Device status* 框中将其当前状态显示为 *error* 或 *ok*。设备根据各个监控结果确定这种状态。

设备会在 *Status* 选项卡中以及 *Basic Settings > System* 对话框的 *Device Status* 框中显示检测到的故障。

该对话框包含以下选项卡：

- ▶ [Global]
- ▶ [Port]
- ▶ [Status]

[Global]

Device status

Device status

显示设备的当前状态。设备根据各个被监控参数确定状态。

可能的值：

- ▶ *error*
设备显示此值以指示任一被监控参数中检测到的错误。
- ▶ *ok*

Traps

Send trap

激活/停用当设备检测到监控的功能变化时 SNMP 陷阱的发送。

可能的值：

- ▶ 勾选（默认设置）
SNMP 陷阱发送激活。
如果设备检测到被监控功能出现变化，则设备发送一个 SNMP 陷阱。
- ▶ 未勾选
SNMP 陷阱发送停用。

发送 SNMP 陷阱的前提条件是，用户在 *Diagnostics > Status Configuration > Alarms (Traps)* 中启用该功能并至少指定一个陷阱目的地。

表格

Temperature

激活/停用设备中的温度监控。

可能的值:

- ▶ **勾选** (默认设置)
监控已激活。
如果温度高于或低于指定限值, 则在 *Device status* 框中, 值会变为 *error*。
- ▶ **未勾选**
监控已停用。

可在 *Basic Settings > System* 对话框的 *Upper temp. limit [° C]* 字段和 *Lower temp. limit [° C]* 字段中指定温度阈值。

Ring redundancy

激活/停用环网冗余的监控。

可能的值:

- ▶ **勾选**
监控已激活。
在 *Device status* 框中, 值在以下情况下会变为 *error*:
 - 冗余功能变为活动状态 (冗余储备丧失)。
 - 设备是一个普通的环网参与者, 并检测到其设置中的错误。
- ▶ **未勾选** (默认设置)
监控已停用。

Connection errors

激活/停用对端口/接口的链路状态的监控。

可能的值:

- ▶ **勾选**
监控已激活。
如果被监控端口/接口上的链路中断, 则在 *Device status* 框中, 值会变为 *error*。
在 *Port* 选项卡中, 用户可以选择要分别监控的端口/接口。
- ▶ **未勾选** (默认设置)
监控已停用。

External memory removal

激活/停用活动的外部存储器的监控。

可能的值:

- ▶ **勾选**
监控已激活。
如果从设备中删除活动的外部存储器, 则在 *Device status* 框中, 值变为 *error*。
- ▶ **未勾选** (默认设置)
监控已停用。

External memory not in sync

激活/停用设备和外部存储器中的配置概要文件的监控。

可能的值：

- ▶ 勾选
监控已激活。
在 *Device status* 框中，值在以下情况下会变为 *error*：
 - 配置概要文件只存在于设备中。
 - 设备中的配置概要文件与外部存储器中的配置概要文件不同。
- ▶ 未勾选（默认设置）
监控已停用。

Power supply

激活/停用电源单元的监控。

可能的值：

- ▶ 勾选（默认设置）
监控已激活。
如果设备检测到电源故障，则在 *Device status* 框中，值会变为 *error*。
- ▶ 未勾选
监控已停用。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

[Port]

表格

Port

显示端口编号。

Propagate connection error

激活/停用端口/接口上的链路的监控。

可能的值：

- ▶ 勾选
监控已激活。
如果所选端口/接口上的链路中断，则在 *Device status* 框中，值会变为 *error*。
- ▶ 未勾选（默认设置）
监控已停用。

当用户勾选 *Global* 选项卡中的 *Connection errors* 复选框时，此设置生效。

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

[Status]**表格**

Timestamp

以年月日上午/下午小时:分钟:秒钟格式显示事件的日期和时间。

Cause

显示导致 SNMP 陷阱的事件。

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

6.1.2 Security Status

[Diagnostics > Status Configuration > Security Status]

此对话框为用户提供了设备中安全相关设置的状态的概览。

设备在 *Security status* 框中将其当前状态显示为 *error* 或 *ok*。设备根据各个监控结果确定这种状态。

设备会在 *Status* 选项卡中以及 *Basic Settings > System* 对话框的 *Security status* 框中显示检测到的故障。

该对话框包含以下选项卡：

- ▶ [Global]
- ▶ [Port]
- ▶ [Status]

[Global]

Security status

Security status

显示设备中安全相关设置的当前状态。设备根据各个被监控参数确定状态。

可能的值：

- ▶ *error*
设备显示此值以指示任一被监控参数中检测到的错误。
- ▶ *ok*

Traps

Send trap

激活/停用当设备检测到监控的功能变化时 SNMP 陷阱的发送。

可能的值：

- ▶ 勾选
SNMP 陷阱发送激活。
如果设备检测到被监控功能出现变化，则设备发送一个 SNMP 陷阱。
- ▶ 未勾选（默认设置）
SNMP 陷阱发送停用。

发送 SNMP 陷阱的前提条件是，用户在 *Diagnostics > Status Configuration > Alarms (Traps)* 中启用该功能并至少指定一个陷阱目的地。

表格

Password default settings unchanged

为本地设置的用户帐户 `user` 和 `admin` 激活/停用密码的监控。

可能的值:

▶ 勾选 (默认设置)

监控已激活。

如果密码设置为 `user` 或 `admin` 用户帐户的默认设置, 则在 *Security status* 框中, 值会变为 *error*。

▶ 未勾选

监控已停用。

可在 *Device Security > User Management* 对话框中设置密码。

Min. password length < 8

激活/停用 *Min. password length* 策略的监控。

可能的值:

▶ 勾选 (默认设置)

监控已激活。

如果 *Min. password length* 策略的值小于 8, 则在 *Security status* 框中, 值会变为 *error*。

▶ 未勾选

监控已停用。

可在 *Device Security > User Management* 对话框的 *Configuration* 框中指定 *Min. password length* 策略。

Password policy settings deactivated

激活/停用密码策略设置的监控。

可能的值:

▶ 勾选 (默认设置)

监控已激活。

如果以下至少一个策略的值小于 1, 则在 *Security status* 框中, 值会变为 *error*。

- *Upper-case characters (min.)*

- *Lower-case characters (min.)*

- *Digits (min.)*

- *Special characters (min.)*

▶ 未勾选

监控已停用。

可在 *Device Security > User Management* 对话框的 *Password policy* 框中指定策略设置。

User account password policy check deactivated

激活/停用对 *Policy check* 功能的监控。

可能的值:

- ▶ **勾选**
监控已激活。
如果至少一个用户帐户的 *Policy check* 功能已停用，则 *Security status* 框中的值变为 *error*。
- ▶ **未勾选** (默认设置)
监控已停用。

可在 *Device Security > User Management* 对话框中激活 *Policy check* 功能。

Telnet server active

激活/停用 Telnet 服务器的监控。

可能的值:

- ▶ **勾选** (默认设置)
监控已激活。
如果用户启用 Telnet 服务器，则在 *Security status* 框中，值会变为 *error*。
- ▶ **未勾选**
监控已停用。

可在 *Device Security > Management Access > Server* 对话框的 *Telnet* 选项卡中启用/禁用 Telnet 服务器。

HTTP server active

激活/停用 HTTP 服务器的监控。

可能的值:

- ▶ **勾选** (默认设置)
监控已激活。
如果用户启用 HTTP 服务器，则在 *Security status* 框中，值会变为 *error*。
- ▶ **未勾选**
监控已停用。

可在 *Device Security > Management Access > Server* 对话框的 *HTTP* 选项卡中启用/禁用 HTTP 服务器。

SNMP unencrypted

激活/停用 SNMP 服务器的监控。

可能的值：

▶ 勾选（默认设置）

监控已激活。

如果以下至少一种条件适用，则在 *Security status* 框中，值会变为 *error*：

- *SNMPv1* 功能已启用。
- *SNMPv2* 功能已启用。
- SNMPv3 加密已禁用。

可在 *Device Security > User Management* 对话框的 *SNMP encryption type* 列中启用加密。

▶ 未勾选

监控已停用。

可在 *Device Security > Management Access > Server* 对话框的 *SNMP* 选项卡中为 SNMP 代理指定设置。

Access to system monitor with serial interface possible

激活/停用系统监控器的监控。

激活系统监控器后，用户可以通过串行连接对系统监控器进行更改。

可能的值：

▶ 勾选

监控已激活。

如果用户激活系统监控器，则在 *Security status* 框中，值会变为 *error*。

▶ 未勾选（默认设置）

监控已停用。

可在 *Diagnostics > System > Selftest* 对话框中激活/停用系统监控器。

Saving the configuration profile on the external memory possible

激活/停用外部存储器中配置概要文件的监控。

可能的值：

▶ 勾选

监控已激活。

如果用户激活外部存储器中配置概要文件的保存，则在 *Security status* 框中，值会变为 *error*。

▶ 未勾选（默认设置）

监控已停用。

可在 *Basic Settings > External Memory* 对话框中激活/停用外部存储器中配置概要文件的保存。

Link interrupted on enabled device ports

激活/停用活动端口上链路的监控。

可能的值：

- ▶ **勾选**
监控已激活。
如果活动端口上的链路中断，则在 *Security status* 框中，值会变为 *error*。在 *Port* 选项卡中，用户可以选择要分别监控的端口。
- ▶ **未勾选**（默认设置）
监控已停用。

Access with Ethernet Switch Configurator possible

激活/停用对 Ethernet Switch Configurator 功能的监控。

可能的值：

- ▶ **勾选**（默认设置）
监控已激活。
如果用户启用 Ethernet Switch Configurator 功能，则在 *Security status* 框中，值会变为 *error*。
- ▶ **未勾选**
监控已停用。

可在 *Basic Settings > Network* 对话框中启用/禁用 Ethernet Switch Configurator 功能。

Load unencrypted config from external memory

激活/停用对从外部存储器加载未加密配置概要文件的监控。

可能的值：

- ▶ **勾选**（默认设置）
监控已激活。
如果设置允许设备从外部存储器加载未加密配置概要文件，则在 *Security status* 框中，值会变为 *error*。
如果满足以下先决条件，则 *Basic Settings > System* 对话框的 *Security status* 框中会显示一个警报。
 - 外部存储器中存储的配置概要文件未加密。
 - 和
 - *Basic Settings > External Memory* 对话框的 *Config priority* 列中的值为 *first*。
- ▶ **未勾选**
监控已停用。

IEC61850-MMS active

激活/停用对 *IEC61850-MMS* 功能的监控。

可能的值：

- ▶ **勾选**（默认设置）
监控已激活。
如果用户启用 *IEC61850-MMS* 功能，则在 *Security status* 框中，值会变为 *error*。
- ▶ **未勾选**
监控已停用。

可在 *Industrial Protocols > IEC61850-MMS* 对话框的 *Operation* 框中启用/禁用 *IEC61850-MMS* 功能。

Self-signed HTTPS certificate present

激活/停用对 HTTPS 证书的监控。

可能的值：

- ▶ **勾选**（默认设置）
监控已激活。
如果 HTTPS 服务器使用自己创建的数字证书，则在 *Security status* 框中，值会变为 *error*。
- ▶ **未勾选**
监控已停用。

Modbus TCP active

激活/停用对 *Modbus TCP* 功能的监控。

可能的值：

- ▶ **勾选**（默认设置）
监控已激活。
如果用户启用 *Modbus TCP* 功能，则在 *Security status* 框中，值会变为 *error*。
- ▶ **未勾选**
监控已停用。

可在 *Advanced > Industrial Protocols > Modbus TCP* 对话框的 *Operation* 框中启用/禁用 *Modbus TCP* 功能。

EtherNet/IP active

激活/停用对 *EtherNet/IP* 功能的监控。

可能的值：

- ▶ **勾选**（默认设置）
监控已激活。
如果用户启用 *EtherNet/IP* 功能，则在 *Security status* 框中，值会变为 *error*。
- ▶ **未勾选**
监控已停用。

可在 *Advanced > Industrial Protocols > EtherNet/IP* 对话框的 *Operation* 框中启用/禁用 *EtherNet/IP* 功能。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

[Port]

表格

Port

显示端口编号。

Link interrupted on enabled device ports

激活/停用活动端口上链路的监控。

可能的值：

▶ 勾选

监控已激活。

如果端口已启用 (*Basic Settings* > *Port* 对话框 *Configuration* 选项卡中的 *Port on* 复选框被勾选) 且端口上的链路中断，则在 *Security status* 框中，值会变为 *error*。

▶ 未勾选 (默认设置)

监控已停用。

当用户勾选 *Diagnostics* > *Status Configuration* > *Security Status* 对话框 *Global* 选项卡中的 *Link interrupted on enabled device ports* 复选框时，此设置生效。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

[Status]

表格

Timestamp

以年月日上午/下午小时:分钟:秒钟格式显示事件的日期和时间。

Cause

显示导致 SNMP 陷阱的事件。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

6.1.3 Signal Contact

[*Diagnostics* > *Status Configuration* > *Signal Contact*]

信号触点是无电位中继触点。因此，设备允许用户进行远程诊断。设备会使用中继触点，打开中继触点并断开闭合电路，以此指示事件的发生。

提示：设备可以包含多个信号触点。每个触点都包含相同的监控功能。多个触点允许用户将各种功能组合在一起，实现系统监控的灵活性。

该菜单包含以下对话框:

▶ Signal Contact 1 / Signal Contact 2

6.1.3.1 Signal Contact 1 / Signal Contact 2

[Diagnostics > Status Configuration > Signal Contact > Signal Contact 1]

在此对话框中，可以指定信号触点的触发条件。

信号触点为用户提供以下选项：

- ▶ 监控设备的正确运行。
- ▶ 指示设备的设备状态。
- ▶ 指示设备的安全状态。
- ▶ 通过手动设置信号触点来控制外部设备。

设备会在 *Status* 选项卡中以及 *Basic Settings > System* 对话框的 *Signal contact status* 框中显示检测到的故障。

该对话框包含以下选项卡：

- ▶ [Global]
- ▶ [Port]
- ▶ [Status]

[Global]

Configuration

Mode

指定信号触点指示哪些事件。

可能的值：

- ▶ *Manual setting* (*Signal Contact 2* 的默认设置（如果存在））
可以使用此设置手动打开或关闭信号触点，例如，打开或关闭远程设备。参见 *Contact* 选项列表。
- ▶ *Monitoring correct operation*（默认设置）
使用此设置，信号触点可以指示下表中指定的参数的状态。
- ▶ *Device status*
使用此设置，信号触点可以指示在 *Diagnostics > Status Configuration > Device Status* 对话框中监控的参数的状态。此外，还可查看 *Signal contact status* 框中的状态。
- ▶ *Security status*
使用此设置，信号触点可以指示在 *Diagnostics > Status Configuration > Security Status* 对话框中监控的参数的状态。此外，还可查看 *Signal contact status* 框中的状态。
- ▶ *Device/Security status*
使用此设置，信号触点可以指示在 *Diagnostics > Status Configuration > Device Status* 对话框和 *Diagnostics > Status Configuration > Security Status* 对话框中监控的参数的状态。此外，还可查看 *Signal contact status* 框中的状态。

Contact

手动切换信号触点。前提条件是，在 *Mode* 下拉列表中选择 *Manual setting* 项目。

可能的值：

- ▶ *open*
信号触点已打开。
- ▶ *close*
信号触点已关闭。

Signal contact status

Signal contact status

显示信号触点的当前状态。

可能的值：

- ▶ *Opened (error)*
信号触点已打开。电路中断。
- ▶ *Closed (ok)*
信号触点已关闭。电路关闭。

Trap configuration

Send trap

激活/停用当设备检测到监控的功能变化时 SNMP 陷阱的发送。

可能的值：

- ▶ 勾选
SNMP 陷阱发送激活。
如果设备检测到被监控功能出现变化，则设备发送一个 SNMP 陷阱。
- ▶ 未勾选（默认设置）
SNMP 陷阱发送停用。

发送 SNMP 陷阱的前提条件是，用户在 *Diagnostics > Status Configuration > Alarms (Traps)* 中启用该功能并至少指定一个陷阱目的地。

Monitoring correct operation

在此表格中，可以指定设备监控的参数。设备打开信号触点，以此指示事件的发生。

Connection errors

激活/停用对端口/接口的链路状态的监控。

可能的值：

- ▶ **勾选**
监控已激活。
如果被监控端口/接口上的链路中断，则信号触点打开。
在 *Port* 选项卡中，用户可以选择要分别监控的端口/接口。
- ▶ **未勾选**（默认设置）
监控已停用。

Temperature

激活/停用设备中的温度监控。

可能的值：

- ▶ **勾选**（默认设置）
监控已激活。
如果温度高于/低于阈值，则信号触点打开。
- ▶ **未勾选**
监控已停用。

可在 *Basic Settings > System* 对话框的 *Upper temp. limit [° C]* 字段和 *Lower temp. limit [° C]* 字段中指定温度阈值。

Ring redundancy

激活/停用环网冗余的监控。

可能的值：

- ▶ **勾选**
监控已激活。
信号触点在以下情况下打开：
 - 冗余功能变为活动状态（冗余储备丧失）。
 - 设备是一个普通的环网参与者，并检测到其设置中的错误。
- ▶ **未勾选**（默认设置）
监控已停用。

External memory removed

激活/停用活动的外部存储器的监控。

可能的值：

- ▶ **勾选**
监控已激活。
如果从设备中删除活动的外部存储器，则信号触点打开。
- ▶ **未勾选**（默认设置）
监控已停用。

External memory not in sync with NVM

激活/停用设备和外部存储器中的配置概要文件的监控。

可能的值：

- ▶ **勾选**
监控已激活。
信号触点在以下情况下打开：
 - 配置概要文件只存在于设备中。
 - 设备中的配置概要文件与外部存储器中的配置概要文件不同。
- ▶ **未勾选**（默认设置）
监控已停用。

Ethernet loops

激活/停用第二层以太网环路的监控。可在 *Diagnostics > Loop Protection* 对话框中指定 *Loop Protection* 功能的设置。

可能的值：

- ▶ **勾选**
监控已激活。
如果设备检测到以太网环路，则信号触点会打开。
- ▶ **未勾选**（默认设置）
监控已停用。

Power supply

激活/停用电源单元的监控。

可能的值：

- ▶ **勾选**（默认设置）
监控已激活。
如果设备检测到电源故障，则信号触点打开。
- ▶ **未勾选**
监控已停用。

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

[Port]

表格

Port

显示端口编号。

Propagate connection error

激活/停用端口/接口上的链路的监控。

可能的值：

- ▶ **勾选**
监控已激活。
如果所选端口/接口上的链路中断，则信号触点打开。
- ▶ **未勾选**（默认设置）
监控已停用。

当用户勾选 *Global* 选项卡中的 *Connection errors* 复选框时，此设置生效。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

[Status]

表格

Timestamp

以年月日上午/下午小时:分钟:秒钟格式显示事件的日期和时间。

Cause

显示导致 SNMP 陷阱的事件。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

6.1.4 MAC Notification

[Diagnostics > Status Configuration > MAC Notification]

设备允许用户使用网络中设备的 MAC 地址跟踪网络中的更改。设备将端口和 MAC 地址的组合保存在其 MAC 地址表中。如果设备学习（忘记）所连接（未连接）设备的 MAC 地址，则设备发送一个 SNMP 陷阱。

此功能用于用户连接终端设备的端口，因此，MAC 地址很少改变。

Operation

Operation

启用/禁用设备中的 *MAC Notification* 功能。

可能的值：

- ▶ *On*
MAC Notification 功能已启用。
- ▶ *Off* (默认设置)
MAC Notification 功能已禁用。

Configuration

Interval [s]

指定发送间隔（秒）。如果设备学习（忘记）所连接（未连接）设备的 MAC 地址，则设备在此之后发送一个 SNMP 陷阱。

可能的值：

- ▶ 0..2147483647 (默认设置：30)

在发送 SNMP 陷阱之前，设备会注册最多 20 个 MAC 地址。如果设备检测到很多变化，则设备在发送间隔到期之前发送 SNMP 陷阱。

表格

Port

显示端口编号。

Active

激活/停用端口上的 *MAC Notification* 功能。

可能的值：

- ▶ 勾选
端口上的 *MAC Notification* 功能已激活。
当发生以下事件之一时，设备发送 SNMP 陷阱：
 - 设备学习一个新连接的设备的 MAC 地址。
 - 设备忘记一个断开连接的设备的 MAC 地址。
- ▶ 未勾选 (默认设置)
端口上的 *MAC Notification* 功能已停用。

发送 SNMP 陷阱的前提条件是，用户在 *Diagnostics > Status Configuration > Alarms (Traps)* 中启用该功能并至少指定一个陷阱目的地。

Last MAC address

显示端口上次连接或断开连接的设备的 MAC 地址。

设备检测通过以下方式连接的设备的 MAC 地址：

- 直接连接到端口
- 通过网络中的其他设备连接到端口

Last MAC status

显示此端口上 *Last MAC address* 值的状态。

可能的值：

- ▶ **added**
设备检测到端口上连接了另一个设备。
- ▶ **removed**
设备检测到连接的设备已从端口移除。
- ▶ **other**
设备未检测到状态。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

6.1.5 Alarms (Traps)

[Diagnostics > Status Configuration > Alarms (Traps)]

设备允许用户发送 SNMP 陷阱作为对特定事件的响应。在此对话框中，可以指定设备向其发送 SNMP 陷阱的陷阱目标。

例如，可在以下对话框中指定导致设备触发 SNMP 陷阱的事件：

- ▶ 在 *Diagnostics > Status Configuration > Device Status* 对话框中
- ▶ 在 *Diagnostics > Status Configuration > Security Status* 对话框中
- ▶ 在 *Diagnostics > Status Configuration > MAC Notification* 对话框中

Operation

Operation

启用/禁用向陷阱目标发送 SNMP 陷阱。

可能的值：

- ▶ *On* (默认设置)
SNMP 陷阱发送已启用。
- ▶ *Off*
SNMP 陷阱发送已禁用。

表格

Name

指定陷阱目标的名称。

可能的值：

- ▶ 带有 1..32 个字符的字母数字 ASCII 字符串

Address

指定陷阱目标的 IP 地址和端口编号。

可能的值：

- ▶ <有效的 IPv4 地址>:<端口编号>

Active

激活/停用向此陷阱目标发送 SNMP 陷阱。

可能的值：

- ▶ 勾选 (默认设置)
向此陷阱目标发送 SNMP 陷阱已激活。
- ▶ 未勾选
向此陷阱目标发送 SNMP 陷阱已停用。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。



打开 *Create* 窗口，向表格中添加一个新的条目。

- ▶ 在 *Name* 字段中，可以为陷阱目标指定名称。
- ▶ 在 *Address* 字段中，可以指定陷阱目标的 IP 地址和端口编号。
如果选择不输入端口编号，则设备自动添加端口编号 162。

6.2 System

[Diagnostics > System]

该菜单包含以下对话框：

- ▶ System Information
- ▶ Hardware State
- ▶ IP Address Conflict Detection
- ▶ ARP
- ▶ Selftest

6.2.1 System Information

[Diagnostics > System > System Information]

此对话框显示设备中各个组件的当前运行状态。显示的数值是快照；它们表示该对话框载入页面时的运行状态。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

Save system information

在新的 Web 浏览器窗口或选项卡中打开 HTML 页面。可以使用适当的 Web 浏览器命令将该 HTML 页面保存到用户 PC。

6.2.2 Hardware State

[Diagnostics > System > Hardware State]

此对话框提供有关设备闪存的分配和状态的信息。

Information

Uptime

显示设备自交付以来的总运行时间。

可能的值：

▶ `..d ..h ..m ..s`
日 小时 分钟 秒钟

表格

Flash region

显示各自存储区域的名称。

Description

显示设备使用存储区域的目的的描述。

Flash sectors

显示向存储区域分配了多少个扇区。

Sector erase operations

显示设备覆盖存储区域扇区的次数。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

6.2.3 IP Address Conflict Detection

[Diagnostics > System > IP Address Conflict Detection]

使用 *IP Address Conflict Detection* 功能，设备可以验证其 IP 地址在网络中是否是唯一的。为此，设备会对收到的 ARP 数据包进行分析。

在此对话框中，可以指定设备检测地址冲突时使用的程序并为此指定所需设置。

设备在表格中会显示检测到的地址冲突。

当设备检测到地址冲突时，设备的状态 LED 指示灯会以红色闪烁 4 次。

Operation

Operation

启用/禁用 *IP Address Conflict Detection* 功能。

可能的值：

- ▶ *On* (默认设置)
IP Address Conflict Detection 功能已启用。
设备验证其 IP 地址在网络中是否是唯一的。
- ▶ *Off*
IP Address Conflict Detection 功能已禁用。

Configuration

Detection mode

指定设备检测地址冲突时使用的程序。

可能的值：

- ▶ *active and passive* (默认设置)
设备使用主动和被动地址冲突检测。

▶ *active*

主动地址冲突检测。设备主动帮助避免与网络中已经存在的 IP 地址进行通信。将设备连接到网络或更改其 IP 参数时，地址冲突检测立即开始。

- 设备以 *Detection delay [ms]* 字段中指定的间隔发送 4 个 ARP 探测数据包。如果设备接收到对这些数据包的响应，则存在地址冲突。
- 如果设备没有检测到地址冲突，则会发送 2 个免费 ARP 数据包作为公告。地址冲突检测禁用时，设备也会发送这些数据包。
- 如果网络中已经存在 IP 地址，则设备将更改回以前使用的 IP 参数（如果可能的话）。如果设备从 DHCP 服务器接收其 IP 参数，则设备将一条 DHCPDECLINE 消息发回到 DHCP 服务器。
- 经过 *Release delay [s]* 字段中指定的一段时间后，设备会检查地址冲突是否仍然存在。当设备接连检测到 10 个地址冲突时，设备会将下次检查的等待时间延长到 60 秒。
- 当设备解决了地址冲突时，设备管理会再次返回到网络。

▶ *passive*

被动地址冲突检测。设备对网络中的数据流量进行分析。如果网络中的另一个设备正在使用相同的 IP 地址，则设备最初会“保护”其 IP 地址。如果另一个设备继续使用相同的 IP 地址进行发送，则设备停止发送。

- 作为“保护”措施，设备会发送免费 ARP 数据包。设备按照 *Address protections* 字段中指定的次数重复此程序。
- 如果另一个设备继续使用相同的 IP 地址进行发送，则经过 *Release delay [s]* 字段中指定的一段时间后，设备会定期检查地址冲突是否仍然存在。
- 当设备解决了地址冲突时，设备管理会再次返回到网络。

Send periodic ARP probes

激活/停用定期地址冲突检测。

可能的值：

▶ *勾选*（默认设置）

定期地址冲突检测已激活。

- 设备每隔 90 到 150 秒定期发送一个 ARP 探测数据包，并在 *Detection delay [ms]* 字段中指定的时间内等待响应。
- 如果设备检测到地址冲突，则设备应用被动检测模式功能。如果 *Send trap* 功能已激活，则设备发送一个 SNMP 陷阱。

▶ *未勾选*

定期地址冲突检测已停用。

Detection delay [ms]

指定设备在发送 ARP 数据包之后等待响应的时间（毫秒）。

可能的值：

- ▶ 20..500（默认设置：200）

Release delay [s]

指定设备再次检查地址冲突是否仍然存在之前经过的时间（秒）。

可能的值：

- ▶ 3..3600（默认设置：15）

Address protections

指定设备为了“保护”其 IP 地址在被动检测模式下发送免费 ARP 数据包的次数。

可能的值：

- ▶ 0..100（默认设置：3）

Protection interval [ms]

指定设备为了“保护”其 IP 地址在被动检测模式下再次发送免费 ARP 数据包之前经过的时间（毫秒）。

可能的值：

- ▶ 20..5000（默认设置：200）

Send trap

激活/停用当设备检测到地址冲突时 SNMP 陷阱的发送。

可能的值：

- ▶ 勾选
SNMP 陷阱发送激活。
如果设备检测到地址冲突，则设备发送一个 SNMP 陷阱。
- ▶ 未勾选（默认设置）
SNMP 陷阱发送停用。

发送 SNMP 陷阱的前提条件是，用户在 *Diagnostics > Status Configuration > Alarms (Traps)* 中启用该功能并至少指定一个陷阱目的地。

Information

Conflict detected

显示当前是否存在地址冲突。

可能的值：

- ▶ 勾选
设备检测到地址冲突。
- ▶ 未勾选
设备未检测到地址冲突。

表格

Timestamp

显示设备检测到地址冲突的时间。

Port

显示设备检测到地址冲突时所用端口的编号。

IP address

显示导致地址冲突的 IP 地址。

MAC address

显示存在地址冲突的设备的 MAC 地址。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

6.2.4 ARP

[Diagnostics > System > ARP]

此对话框显示连接到设备管理的相邻设备的 MAC 和 IP 地址。

设备可显示 IPv4 和 IPv6 地址。对于 IPv6 协议，可使用邻居发现协议 (NDP) 来获取邻近设备的地址。

表格

Port

显示端口编号。

IP address

显示邻近设备的 IPv4 地址 或 IPv6 地址。

MAC address

显示邻近设备的 MAC 地址。

Last updated

显示在 ARP 表中注册条目的当前设置以来的时间（秒）。

Type

显示条目的类型。

可能的值：

▶ **static**

静态条目。删除 ARP 表后，设备会保留静态条目。

▶ **dynamic**

动态条目当已超过 *Aging time [s]* 并且设备在此期间未从此设备收到任何数据时，设备会删除动态条目。

▶ **local**

设备管理的 IP 和 MAC 地址。

Active

显示 ARP 表包含作为活动条目的 IP/MAC 地址分配。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

Reset ARP table

从 ARP 表中删除动态设置的地址。

6.2.5 Selftest

[Diagnostics > System > Selftest]

此对话框可用于进行以下操作：

- ▶ 激活/停用启动设备时的 RAM 测试。
- ▶ 启用/禁用在系统启动时进入系统监控器的选项。
- ▶ 指定在检测到错误时设备的行为方式。

Configuration

如果设备在重新启动时没有检测到任何可读的配置概要文件，则以下设置将永久阻止用户访问设备。

- ▶ *SysMon1 is available* 复选框为未勾选。
- ▶ *Load default config on error* 复选框为未勾选。

例如，如果用户正在加载的配置概要文件的密码与在设备中设置的密码不同，就属于这种情况。要使设备再次解锁，请与您的销售合作伙伴联系。

RAM test

激活/停用重新启动期间的 RAM 存储器检查。

可能的值：

- ▶ 勾选（默认设置）
RAM 存储器检查已激活。在重新启动期间，设备会检查 RAM 存储器。
- ▶ 未勾选
RAM 存储器检查已停用。这可缩短设备的启动时间。

SysMon1 is available

激活/停用重新启动期间对系统监控器的访问。

可能的值：

- ▶ 勾选（默认设置）
设备允许用户在重新启动期间打开系统监控器。
- ▶ 未勾选
设备启动时没有打开系统监控器的选择。

除其他操作之外，系统监控器允许用户更新设备软件并删除保存的配置概要文件。

Load default config on error

激活/停用当设备在重新启动期间没有检测到任何可读的配置概要文件时默认设置的加载。

可能的值：

- ▶ 勾选（默认设置）
设备加载默认设置。
- ▶ 未勾选
设备中断重启并停止。只能通过串行接口使用命令行界面访问设备管理。
要重新获得通过网络访问设备的权限，请打开系统监控器并重置设置。重新启动时，设备会加载默认设置。

表格

在此表中，您可以指定在检测到错误时设备的行为方式。

Cause

检测到设备对其做出反应的错误原因。

可能的值：

- ▶ **task**
设备在所执行的应用程序中检测到错误，例如，任务终止或不可用时。
- ▶ **resource**
设备在可用资源中检测到错误，例如，存储器空间不足时。
- ▶ **software**
设备检测到软件错误，例如，一致性检查错误。
- ▶ **hardware**
设备检测到硬件错误，例如，芯片组错误。

Action

指定相邻事件发生时设备的行为。

可能的值：

- ▶ **reboot**（默认设置）
设备触发重新启动。
- ▶ **logOnly**
设备将检测到的错误注册到日志文件中。参见 *Diagnostics > Report > System Log* 对话框。
- ▶ **sendTrap**
设备发送一个 SNMP 陷阱。
发送 SNMP 陷阱的前提条件是，用户在 *Diagnostics > Status Configuration > Alarms (Traps)* 中启用该功能并至少指定一个陷阱目的地。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

6.3 Email Notification

[Diagnostics > Email Notification]

设备允许用户通过电子邮件向多个收件人通知已发生的事件。

设备会立即或定期发送电子邮件，具体取决于事件严重程度。通常将严重程度高的事件指定为立即发送。

用户可以指定多个收件人，设备会立即或定期向其发送电子邮件。

该菜单包含以下对话框：

- ▶ Email Notification Global
- ▶ Email Notification Recipients
- ▶ Email Notification Mail Server

6.3.1 Email Notification Global

[Diagnostics > Email Notification > Global]

在此对话框中，可以指定发件人设置。此外，用户还可以指定设备立即发送和定期发送电子邮件的事件严重程度。

Operation

Operation

启用/禁用电子邮件发送：

可能的值：

- ▶ *On*
电子邮件发送已启用。
- ▶ *Off* (默认设置)
电子邮件发送已禁用。

Certificate

设备可能通过不安全的网络将消息发送到服务器。为帮助防止“中间人”攻击，应请求证书机构为服务器创建证书。将服务器配置为使用证书。将证书传输到设备上。

如果用户已为邮件服务器指定设置，则应使用证书中提供为 *Common Name* 或 *Subject Alternative Name* 的 IP 地址或 DNS 名称。否则证书验证将不成功。

URL


指定证书的路径和文件名。

设备接受具有以下属性的证书：

- X.509 格式
- .PEM 文件扩展名
- Base64 编码，括在
-----BEGIN CERTIFICATE-----
和
-----END CERTIFICATE-----

出于安全原因，我们建议一直使用由认证机构签名的证书。

设备为用户提供将证书复制到设备的以下选项：

- ▶ 从 PC 导入
当证书位于用户 PC 中或网络驱动器上时，将该证书拖放到  区域中。也可点击该区域内部选择该证书。
- ▶ 从 FTP 服务器导入
当该证书位于 FTP 服务器上时，以如下形式指定该文件的 URL：
ftp://<???:<??>@<IP ??>:<??>/<??>/<??>

- ▶ 从 TFTP 服务器导入
当该证书位于 TFTP 服务器上时，以如下形式指定该文件的 URL：
tftp://<IP ??>/<??>/<??>
- ▶ 从 SCP 或 SFTP 服务器导入
当该证书位于 SCP 或 SFTP 服务器上时，以如下形式指定该文件的 URL：
 - scp:// 或 sftp://<IP ??>/<??>/<??>
点击 *Start* 按钮后，设备会显示 *Credentials* 窗口。在该处输入 *User name* 和 *Password* 以登录服务器。
 - scp:// 或 sftp://<??>:<??>@<IP ??>/<??>/<??>

Start

将 *URL* 字段中指定的证书复制到设备。

Sender

Address

指定设备的电子邮件地址。

设备使用此电子邮件作为发件人发送电子邮件。

可能的值：

- ▶ 带有 0..255 个字符的字母数字 ASCII 字符串

Notification immediate

用户可在此处为设备立即发送的电子邮件指定设置。

Severity

指定设备立即发送电子邮件的最低事件严重程度。如果发生符合此严重程度或者更紧急严重程度的事件，则设备会向收件人发送电子邮件。

可能的值：

- ▶ *emergency*
- ▶ *alert* (默认设置)
- ▶ *critical*
- ▶ *error*
- ▶ *warning*
- ▶ *notice*
- ▶ *informational*
- ▶ *debug*

Subject

指定电子邮件的主题。

可能的值：

- ▶ 带有 0..255 个字符的字母数字 ASCII 字符串

Notification periodic

用户可在此处为设备定期发送的电子邮件指定设置。

Severity

指定设备定期发送电子邮件的最低事件严重程度。如果发生符合此严重程度或者更紧急严重程度的事件，则设备会在缓冲区中注册事件。设备会定期或在缓冲区溢出时发送缓冲区内容。

如果发生严重程度不那么紧急的事件，则设备不会在缓冲区中注册事件。

可能的值：

- ▶ *emergency*
- ▶ *alert*
- ▶ *critical*
- ▶ *error*
- ▶ *warning* (默认设置)
- ▶ *notice*
- ▶ *informational*
- ▶ *debug*

Subject

指定电子邮件的主题。

可能的值：

- ▶ 带有 0..255 个字符的字母数字 ASCII 字符串

Sending interval [min]

指定发送间隔（分钟）。

如果设备已至少注册一个事件，则设备会在时间到期之后发送包含日志文件的电子邮件。

可能的值：

- ▶ 30..1440 (默认设置: 30)

Send

立即发送包含缓冲区内容的电子邮件并清除缓冲区。

Information

Sent messages

显示设备已成功向邮件服务器发送电子邮件的次数。

Undeliverable messages

显示设备未成功尝试向邮件服务器发送电子邮件的次数。

Time of the last messages sent

显示设备已向邮件服务器发送电子邮件的日期和时间。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

Clear email notification statistics

将 *Information* 框中的计数器重置为 0。

事件严重程度的含义

严重程度	含义
emergency	设备未处于运行准备就绪状态
alert	需要立即进行用户干预
critical	重要状态
error	错误状态
warning	警告
notice	重要正常状态
informational	非正式消息
debug	调试消息

6.3.2 Email Notification Recipients

[Diagnostics > Email Notification > Recipients]

用户可在此对话框中指定收件人，设备会向其发送电子邮件。设备允许指定最多 10 个收件人。

表格

Index

显示与表格条目相关的索引编号。

Notification type

指定设备是立即还是定期向此收件人发送电子邮件。

可能的值：

- ▶ *immediate*
设备立即向此收件人发送电子邮件。
- ▶ *periodic*
设备定期向此收件人发送电子邮件。

Address

指定收件人的电子邮件地址。

可能的值：

- ▶ 包含最多 255 个字符的有效电子邮件地址

Active

激活/停用收件人通知。

可能的值：

- ▶ *勾选*（默认设置）
收件人通知已激活。
- ▶ *未勾选*
收件人通知已停用。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

6.3.3 Email Notification Mail Server

[Diagnostics > Email Notification > Mail Server]

在此对话框中，可以指定邮件服务器的设置。设备支持与邮件服务器建立加密和未加密的连接。

表格

Index

显示与表格条目相关的索引编号。

Description

指定服务器的名称。

可能的值：

- ▶ 带有 0..255 个字符的字母数字 ASCII 字符串

IP address

指定服务器的 IP 地址或 DNS 名称。

可能的值：

- ▶ 有效的 IPv4 地址（默认设置：0.0.0.0）
- ▶ domain.tld 或 host.domain.tld 格式的 DNS 名称
如果用户已指定 DNS 名称，则将同时启用 *Advanced > DNS > Client > Global* 对话框中的 *Client* 功能。
如果用户使用证书建立加密连接，则会验证 DNS 名称是否与证书中提到的服务器 DNS 名称相同。

Destination TCP port

指定服务器的 TCP 端口。

可能的值：

- ▶ 1..65535（默认设置：25）
例外：端口 2222 预留给内部功能。

常用的 TCP 端口：

- SMTP 25
- Message Submission 587

Encryption

指定使用哪个协议对设备与邮件服务器之间的连接进行加密。

可能的值：

- ▶ none（默认设置）
设备与服务器建立未加密的连接。
- ▶ tlsv1
设备使用 startTLS 扩展与服务器建立加密连接。

User name

指定设备用于在邮件服务器上进行身份验证的帐户的用户名。

可能的值:

- ▶ 带有 0..255 个字符的字母数字 ASCII 字符串

Password

指定设备用于在邮件服务器上进行身份验证的帐户的密码。

可能的值:

- ▶ 带有 0..255 个字符的字母数字 ASCII 字符串

Timeout [s]

指定设备再次发送电子邮件之前经过的时间（秒）。前提是设备由于连接错误而未能成功发送完整的电子邮件。

可能的值:

- ▶ 1..15（默认设置：3）

Active

激活/停用邮件服务器的使用。

可能的值:

- ▶ **勾选**
邮件服务器已激活。
设备向此邮件服务器发送电子邮件。
- ▶ **未勾选**（默认设置）
邮件服务器已停用。
设备不向此邮件服务器发送电子邮件。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

Connection test

打开 *Connection test* 对话框以发送测试电子邮件。

如果邮件服务器设置正确，则所选收件人会收到测试电子邮件。

- ▶ 用户可以在 *Recipient* 字段中指定收件人，设备会向其发送测试电子邮件：
 - *immediate*
设备会先向收件人发送测试电子邮件，并在随后立即向其发送电子邮件。
 - *periodic*
设备会先向收件人发送测试电子邮件，然后会定期向其发送电子邮件。
- ▶ 在 *Message text* 字段中，可以指定测试电子邮件的文本。

6.4 Syslog

[Diagnostics > Syslog]

设备允许用户向不同的系统日志服务器报告所选事件（与事件严重程度无关）。在此对话框中，可以指定此功能的设置并管理最多 8 个系统日志服务器。

Operation

Operation

启用/禁用向系统日志服务器发送事件。

可能的值：

- ▶ *On*
事件发送已启用。
设备将表格中指定的事件发送给指定的系统日志服务器。
- ▶ *Off*（默认设置）
事件发送已禁用。

Certificate

设备可能通过不安全的网络将消息发送到服务器。为帮助防止“中间人”攻击，应请求证书机构为服务器创建证书。将服务器配置为使用证书。将证书传输到设备上。

如果您在服务器上指定参数，则验证您将证书中提供的 IP 地址和 DNS 名称指定为 *Common Name* 或 *Subject Alternative Name*。否则证书验证将不成功。

提示：为使更改在加载新的证书之后生效，请重新启动 *Syslog* 功能。

URL


指定证书的路径和文件名。

设备接受具有以下属性的证书：

- X.509 格式
- .PEM 文件扩展名
- Base64 编码，括在
-----BEGIN CERTIFICATE-----
和
-----END CERTIFICATE-----

出于安全原因，我们建议一直使用由认证机构签名的证书。

设备为用户提供将证书复制到设备的以下选项：

- ▶ 从 PC 导入
当证书位于用户 PC 中或网络驱动器上时，将该证书拖放到  区域中。也可点击该区域内部选择该证书。

- ▶ 从 FTP 服务器导入
当该证书位于 FTP 服务器上时，以如下形式指定该文件的 URL：
ftp://<??>:<??>@<IP ??>:<??>/<??>/<??>
- ▶ 从 TFTP 服务器导入
当该证书位于 TFTP 服务器上时，以如下形式指定该文件的 URL：
tftp://<IP ??>/<??>/<??>
- ▶ 从 SCP 或 SFTP 服务器导入
当该证书位于 SCP 或 SFTP 服务器上时，以如下形式指定该文件的 URL：
 - scp:// 或 sftp://<IP ??>/<??>/<??>
点击 *Start* 按钮后，设备会显示 *Credentials* 窗口。在该处输入 *User name* 和 *Password* 以登录服务器。
 - scp:// 或 sftp://<??>:<??>@<IP ??>/<??>/<??>

Start

将 *URL* 字段中指定的证书复制到设备。

表格

Index

显示与表格条目相关的索引编号。

删除一个表格条目后，会留下一个编号空缺。创建一个新的表格条目后，设备将填补第一个空缺。

可能的值：

- ▶ 1..8

IP address

指定系统日志服务器的 IP 地址。

可能的值：

- ▶ 有效的 IPv4 地址（默认设置：0.0.0.0）
- ▶ 有效的 IPv6 地址
- ▶ 主机名

Destination UDP port

指定系统日志服务器预期在其上收到日志条目的 TCP 或 UDP 端口。

可能的值:

- ▶ 1..65535 (默认设置: 514)

Transport type

指定设备用于向系统日志服务器发送事件的传输类型。

可能的值:

- ▶ udp (默认设置)
设备通过 *Destination UDP port* 列中指定的 UDP 端口发送事件。
- ▶ tls
设备在 *Destination UDP port* 列中指定的 TCP 端口上通过 TLS 发送事件。

Min. severity

指定事件的最低严重程度。设备向系统日志服务器发送一个针对具有这种严重程度以及具有更紧迫严重程度的事件的日志条目。

可能的值:

- ▶ emergency
- ▶ alert
- ▶ critical
- ▶ error
- ▶ warning (默认设置)
- ▶ notice
- ▶ informational
- ▶ debug

Type

指定设备传输的日志条目的类型。

可能的值:

- ▶ systemlog (默认设置)
- ▶ audittrail

Active

激活/停用向系统日志服务器发送事件:

- ▶ 勾选
设备向系统日志服务器发送事件。
- ▶ 未勾选 (默认设置)
向系统日志服务器发送事件已停用。

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

6.5 Ports

[Diagnostics > Ports]

该菜单包含以下对话框：

- ▶ SFP
- ▶ TP cable diagnosis
- ▶ Port Monitor
- ▶ Auto-Disable
- ▶ Port Mirroring

6.5.1 SFP

[Diagnostics > Ports > SFP]

此对话框允许用户查看当前连接到设备的 SFP 收发器及其属性。

表格

如果设备配备了 SFP 收发器，则表格会显示有效值。

Port

显示端口编号。

Module type

SFP 收发器的类型，例如 M-SFP-SX/LC。

Serial number

显示 SFP 收发器的序列号。

Connector type

显示连接器类型。

Supported

显示设备是否支持 SFP 收发器。

Temperature [°C]

SFP 收发器的工作温度（摄氏度）。

Tx power [mW]

SFP 收发器的发送功率（毫瓦）。

Rx power [mW]

SFP 收发器的接收功率（毫瓦）。

Tx power [dBm]

SFP 收发器的发送功率（dBm）。

Rx power [dBm]

SFP 收发器的接收功率（dBm）。

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

6.5.2 TP cable diagnosis

[Diagnostics > Ports > TP cable diagnosis]

此功能测试连接至接口的铜电缆是否短路或开路。该表格显示电缆状态和预估长度。设备还会显示连接至端口的各个电缆对。当设备检测到电缆短路或断路时，它还会显示问题的预估距离。

为获得可靠结果，请将 *TP cable diagnosis* 功能用于最小长度为 3 米的双绞线。

提示： 此测试会中断端口上的流量。

Information


Port

显示端口编号。

Status

虚拟电缆测试仪的状态。

可能的值：

- ▶ *active*
电缆测试正在进行中。
要开始测试，请点击  按钮，然后点击 *Start cable diagnosis...* 项目。此操作可打开 *Select port* 对话框。
- ▶ *success*
执行测试成功后，设备将显示此条目。
- ▶ *failure*
测试中断后，设备将显示此条目。
- ▶ *uninitialized*
在待机状态下，设备将显示此条目。

表格

Cable pair

显示与此条目相关的电缆对。设备使用支持的第一个 PHY 索引来显示这些值。

Result

显示电缆测试的结果。

可能的值：

- ▶ *normal*
电缆运行正常。
- ▶ *open*
电缆断裂导致中断。

▶ *short*
电缆中的电线互相接触会造成短路。

▶ *unknown*
对于对未测试的电缆对，设备将显示此值。

以下情况下，设备显示的值与预期值不同：

- 如果没有连接至端口的电缆，则设备将显示 *unknown* 值，而非 *open*。
- 如果端口已停用，则设备将显示 *short* 值。

Min. length

显示电缆的最小预估长度（以米为单位）。

如果电缆长度未知，或在框架中 *Information* 字段 *Status* 显示 *active* 值，*failure* 或 *uninitialized*，则设备将显示 0 值。

Max. length

显示电缆的最大预估长度（以米为单位）。

如果电缆长度未知，或在框架中 *Information* 字段 *Status* 显示 *active* 值，*failure* 或 *uninitialized*，则设备将显示 0 值。

Distance [m]

显示从电缆一端到另一端或到电缆中断处的估计距离（以米为单位）。

如果电缆长度未知，或在框架中 *Information* 字段 *Status* 显示 *active* 值，*failure* 或 *uninitialized*，则设备将显示 0 值。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

Start cable diagnosis...

打开 *Select port* 对话框。

从 *Port* 下拉列表中选择要测试的端口。仅用于铜基端口。

请点击 *Ok* 按钮，在所选端口上启动电缆测试。

6.5.3 Port Monitor

[Diagnostics > Ports > Port Monitor]

Port Monitor 功能可监控与端口上指定参数的符合情况。如果 *Port Monitor* 功能检测到超过了参数，则设备将执行一项操作。

若要应用 *Port Monitor* 功能，请执行以下步骤：

- ▶ *Global* 选项卡
 - 在 *Port Monitor* 框中启用 *Operation* 功能。
 - 为每个端口激活您希望 *Port Monitor* 功能监控的参数。
- ▶ *Link flap*、*CRC/Fragments* 和 *Overload detection* 选项卡
 - 为每个端口的参数指定阈值。
- ▶ *Link speed/Duplex mode detection* 选项卡
 - 为每个端口激活允许的速度和双工模式组合。
- ▶ *Global* 选项卡
 - 为每个端口指定一项设备在 *Port Monitor* 功能检测到超过参数时将执行的操作。
- ▶ *Auto-disable* 选项卡
 - 如果至少一次指定了 *auto-disable* 操作，请为被监控参数勾选 *Auto-disable* 复选框。

该对话框包含以下选项卡：

- ▶ [Global]
- ▶ [Auto-disable]
- ▶ [Link flap]
- ▶ [CRC/Fragments]
- ▶ [Overload detection]
- ▶ [Link speed/Duplex mode detection]

[Global]

在此选项卡中，可以启用 *Port Monitor* 功能并指定 *Port Monitor* 功能监控的参数。也可指定设备在 *Port Monitor* 功能检测到超过参数时将执行的操作。

Operation

Operation

全局启用/禁用 *Port Monitor* 功能。

可能的值：

- ▶ *On*
Port Monitor 功能已启用。
- ▶ *Off*（默认设置）
Port Monitor 功能已禁用。

表格

Port

显示端口编号。

Link flap on

激活/停用端口上链路振荡的监控。

可能的值：

- ▶ **勾选**
监控已激活。
 - *Port Monitor* 功能可监控端口上的链路振荡。
 - 如果设备检测到太多的链路振荡，则设备将执行 *Action* 列中指定的操作。
 - 在 *Link flap* 选项卡上，指定要监控的参数。
- ▶ **未勾选**（默认设置）
监控已停用。

CRC/Fragments on

激活/停用对端口上检测到的 CRC/片段错误的监控。

可能的值：

- ▶ **勾选**
监控已激活。
 - *Port Monitor* 功能监视在端口上检测到的 CRC/片段错误。
 - 如果设备检测到太多的 CRC/碎片错误，则设备将执行 *Action* 列中指定的操作。
 - 在 *CRC/Fragments* 选项卡上，指定要监控的参数。
- ▶ **未勾选**（默认设置）
监控已停用。

Duplex mismatch detection active

激活/停用端口上双工不匹配的监控。

可能的值：

- ▶ **勾选**
监控已激活。
 - *Port Monitor* 功能可监控端口上的双工不匹配。
 - 如果设备检测到双工不匹配，则设备将执行 *Action* 列中指定的操作。
- ▶ **未勾选**（默认设置）
监控已停用。

Overload detection on

激活/停用端口上的过载检测。

可能的值：

- ▶ **勾选**
监控已激活。
 - *Port Monitor* 功能可监控端口上的数据负载。
 - 如果设备检测到端口上的数据过载，则设备将执行 *Action* 列中指定的操作。
 - 在 *Overload detection* 选项卡上，指定要监控的参数。
- ▶ **未勾选**（默认设置）
监控已停用。

Link speed/Duplex mode detection on

激活/停用端口上链路速度和双工模式的监控。

可能的值：

- ▶ **勾选**
监控已激活。
 - *Port Monitor* 功能可监控端口上的链路速度和双工模式。
 - 如果设备检测到不允许的链路速度和双工模式组合，则设备将执行 *Action* 列中指定的操作。
 - 在 *Link speed/Duplex mode detection* 选项卡上，指定要监控的参数。
- ▶ **未勾选**（默认设置）
监控已停用。

Active condition

显示导致端口上操作的被监控参数。

可能的值：

- ▶ -
无被监控参数。
设备不执行任何操作。
- ▶ *Link flap*
在观察期内链接更改过多。
- ▶ *CRC/Fragments*
在观察期间检测到过多的 CRC/片段错误。
- ▶ *Duplex mismatch*
检测到双工不匹配。
- ▶ *Overload detection*
在观察期间检测到过载。
- ▶ *Link speed/Duplex mode detection*
检测到不允许的速度和双工模式组合。

Action

指定设备在 *Port Monitor* 功能检测到超过参数时将执行的操作。

可能的值：

▶ *disable port*

设备禁用该端口并发送一个 SNMP 陷阱。

端口的“链路状态”LED 指示灯每个周期闪烁 3 次。

- 要重新启用该端口，请突出显示该端口，点击  按钮，然后点击 *Reset* 项目。
- 如果不再超过这些参数，则 *Auto-Disable* 功能将在指定等待时间之后再次启用相关端口。前提是，在 *Auto-disable* 选项卡上，勾选被监控参数的复选框。

▶ *send trap*

设备发送一个 SNMP 陷阱。

发送 SNMP 陷阱的前提条件是，用户在 *Diagnostics > Status Configuration > Alarms (Traps)* 中启用该功能并至少指定一个陷阱目的地。

▶ *auto-disable* (默认设置)

设备禁用该端口并发送一个 SNMP 陷阱。

端口的“链路状态”LED 指示灯每个周期闪烁 3 次。

前提是，在 *Auto-disable* 选项卡上，勾选被监控参数的复选框。

- *Diagnostics > Ports > Auto-Disable* 对话框显示超过参数导致哪些端口当前被禁用。
- *Auto-Disable* 功能自动重新激活端口。为此，可以切换至 *Diagnostics > Ports > Auto-Disable* 对话框并在 *Reset timer [s]* 列中为相关端口指定等待期。

Port status

显示端口的工作状态。

可能的值：

▶ *up*

端口已启用。

▶ *down*

端口已禁用。

▶ *notPresent*

物理端口不可用。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

Reset

再次启用表格中突出显示的端口并将其计数器重置为 0。这将影响以下对话框中的计数器：

▶ *Diagnostics > Ports > Port Monitor* 对话框

- *Link flap* 选项卡
- *CRC/Fragments* 选项卡
- *Overload detection* 选项卡

▶ *Diagnostics > Ports > Auto-Disable* 对话框

[Auto-disable]

在此选项卡中，可以为 *Port Monitor* 功能监控的参数激活 *Auto-Disable* 功能。

表格

Reason

显示 *Port Monitor* 功能监控的参数。

勾选相邻复选框，使 *Port Monitor* 功能在检测到超过被监控参数时执行 *auto-disable* 操作。

Auto-disable

为相邻参数激活/停用 *Auto-Disable* 功能。

可能的值：

- ▶ 勾选
相邻参数的 *Auto-Disable* 功能已激活。
如果超过了相邻参数且 *Action* 列中指定了 *auto-disable* 值，则设备将执行 *Auto-Disable* 功能。
- ▶ 未勾选（默认设置）
相邻参数的 *Auto-Disable* 功能已停用。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

Reset

再次启用表格中突出显示的端口并将其计数器重置为 0。这将影响以下对话框中的计数器：

- ▶ *Diagnostics > Ports > Port Monitor* 对话框
 - *Link flap* 选项卡
 - *CRC/Fragments* 选项卡
 - *Overload detection* 选项卡
- ▶ *Diagnostics > Ports > Auto-Disable* 对话框

[Link flap]

在此选项卡中，可以单独为每个端口指定以下设置：

- ▶ 链路变化次数。
- ▶ *Port Monitor* 功能监控一个参数以检测差异的时间段。

还可以查看截至目前 *Port Monitor* 功能检测到的链路变化次数。

Port Monitor 功能可监控在 *Global* 选项卡的 *Link flap on* 列中勾选了其相应复选框的端口。

表格

Port

显示端口编号。

Sampling interval [s]

指定 *Port Monitor* 功能监控一个参数以检测差异的时间段（秒）。

可能的值：

▶ 1..180（默认设置：10）

Link flaps

指定链路变化次数。

如果 *Port Monitor* 功能在被监控时间段之内检测到此链路变化次数，则设备将执行指定操作。

可能的值：

▶ 1..100（默认设置：5）

Last sampling interval

显示设备在过去一段时间内检测到的错误的数量。

Total

显示自启用端口以来设备检测到的错误的总数。

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

Reset

再次启用表格中突出显示的端口并将其计数器重置为 0。这将影响以下对话框中的计数器：

- ▶ *Diagnostics > Ports > Port Monitor* 对话框
 - *Link flap* 选项卡
 - *CRC/Fragments* 选项卡
 - *Overload detection* 选项卡
- ▶ *Diagnostics > Ports > Auto-Disable* 对话框

[CRC/Fragments]

在此选项卡中，可以单独为每个端口指定以下设置：

- ▶ 检测到的片段错误率。
- ▶ *Port Monitor* 功能监控一个参数以检测差异的时间段。

还可以查看截至目前设备检测到的碎片错误率。

Port Monitor 功能可监控在 *Global* 选项卡的 *CRC/Fragments on* 列中勾选了其相应复选框的端口。

表格

Port

显示端口编号。

Sampling interval [s]

指定 *Port Monitor* 功能监控一个参数以检测差异的时间段（秒）。

可能的值：

▶ 5..180（默认设置：10）

CRC/Fragments count [ppm]

指定检测到的片段错误率（百万分之几）。

如果 *Port Monitor* 功能在被监控时间段之内检测到此碎片错误率，则设备将执行指定操作。

可能的值：

▶ 1..1000000（默认设置：1000）

Last active interval [ppm]

显示设备在过去的一段时间内检测到的碎片错误率。

Total [ppm]

显示自启用端口以来设备检测到的碎片错误率。

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

Reset

再次启用表格中突出显示的端口并将其计数器重置为 0。这将影响以下对话框中的计数器：

- ▶ *Diagnostics > Ports > Port Monitor* 对话框
 - *Link flap* 选项卡
 - *CRC/Fragments* 选项卡
 - *Overload detection* 选项卡
- ▶ *Diagnostics > Ports > Auto-Disable* 对话框

[Overload detection]

在此选项卡中，可以单独为每个端口指定以下设置：

- ▶ 负载阈值。
- ▶ *Port Monitor* 功能监控一个参数以检测差异的时间段。

还可以查看截至目前设备检测到的数据包的数量。

Port Monitor 功能可监控在 *Global* 选项卡的 *Overload detection on* 列中勾选了其相应复选框的端口。

Port Monitor 功能不对属于链路聚合组成员的任何端口进行监控。

表格

Port

显示端口编号。

Traffic type

指定设备在监控端口上的负载时考虑的数据包类型。

可能的值：

- ▶ all
Port Monitor 功能对广播、多播和单播数据包进行监控。
- ▶ bc（默认设置）
Port Monitor 功能只对广播数据包进行监控。
- ▶ bc-mc
Port Monitor 功能只对广播和多播数据包进行监控。

Threshold type

指定数据速率的单位。

可能的值：

- ▶ pps（默认设置）
每秒数据包数量
- ▶ kbps
每秒千比特
前提条件是 *Traffic type* 列中的值 = all。

Lower threshold

指定数据速率的阈值下限。

只有当端口上的负载小于此处指定的值时，*Auto-Disable* 功能才会再次启用端口。

可能的值:

▶ 0..10000000 (默认设置: 0)

Upper threshold

指定数据速率的阈值上限。

如果 *Port Monitor* 功能在被监控时间段之内检测到此负载，则设备将执行指定操作。

可能的值:

▶ 0..10000000 (默认设置: 0)

Interval [s]

指定 *Port Monitor* 功能观测一个参数以检测超过此参数的时间段 (秒)。

可能的值:

▶ 1..20 (默认设置: 1)

Packets

显示设备在过去一段时间内检测到的广播、多播和单播数据包的数量。

Broadcast packets

显示设备在过去一段时间内检测到的广播数据包的数量。

Multicast packets

显示设备在过去一段时间内检测到的多播数据包的数量。

Kbit/s

显示设备在过去一段时间内检测到的数据速率 (每秒千比特)。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

Reset

再次启用表格中突出显示的端口并将其计数器重置为 0。这将影响以下对话框中的计数器:

- ▶ *Diagnostics > Ports > Port Monitor* 对话框
 - *Link flap* 选项卡
 - *CRC/Fragments* 选项卡
 - *Overload detection* 选项卡
- ▶ *Diagnostics > Ports > Auto-Disable* 对话框

[Link speed/Duplex mode detection]

在此选项卡中，可以为每个端口激活允许的速度和双工模式组合。

Port Monitor 功能可监控在 *Global* 选项卡的 *Link speed/Duplex mode detection on* 列中勾选了其相应复选框的端口。

Port Monitor 功能只对启用的物理端口进行监控。

表格

Port

显示端口编号。

10 Mbit/s HDX

激活/停用端口监控器以便在端口上接受半双工和 10 Mbit/s 数据速率组合。

可能的值：

- ▶ 勾选
端口监控器考虑速度和双工组合。
- ▶ 未勾选
如果端口监控器在端口上检测到速度和双工组合，则设备将执行 *Global* 选项卡中指定的操作。

10 Mbit/s FDX

激活/停用端口监控器以便在端口上接受全双工和 10 Mbit/s 数据速率组合。

可能的值：

- ▶ 勾选
端口监控器考虑速度和双工组合。
- ▶ 未勾选
如果端口监控器在端口上检测到速度和双工组合，则设备将执行 *Global* 选项卡中指定的操作。

100 Mbit/s HDX

激活/停用端口监控器以便在端口上接受半双工和 100 Mbit/s 数据速率组合。

可能的值：

- ▶ 勾选
端口监控器考虑速度和双工组合。
- ▶ 未勾选
如果端口监控器在端口上检测到速度和双工组合，则设备将执行 *Global* 选项卡中指定的操作。

100 Mbit/s FDX

激活/停用端口监控器以便在端口上接受全双工和 100 Mbit/s 数据速率组合。

可能的值:

- ▶ [勾选](#)
端口监控器考虑速度和双工组合。
- ▶ [未勾选](#)
如果端口监控器在端口上检测到速度和双工组合，则设备将执行 *Global* 选项卡中指定的操作。

1,000 Mbit/s FDX

激活/停用端口监控器以便在端口上接受全双工和 1 Gbit/s 数据速率组合。

可能的值:

- ▶ [勾选](#)
端口监控器考虑速度和双工组合。
- ▶ [未勾选](#)
如果端口监控器在端口上检测到速度和双工组合，则设备将执行 *Global* 选项卡中指定的操作。

2.5 Gbit/s FDX

激活/停用端口监控器以便在端口上接受全双工和 2.5 Gbit/s 数据速率组合。

可能的值:

- ▶ [勾选](#)
端口监控器考虑速度和双工组合。
- ▶ [未勾选](#)
如果端口监控器在端口上检测到速度和双工组合，则设备将执行 *Global* 选项卡中指定的操作。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

Reset

再次启用表格中突出显示的端口并将其计数器重置为 0。这将影响以下对话框中的计数器:

- ▶ [Diagnostics > Ports > Port Monitor](#) 对话框
 - [Link flap](#) 选项卡
 - [CRC/Fragments](#) 选项卡
 - [Overload detection](#) 选项卡
- ▶ [Diagnostics > Ports > Auto-Disable](#) 对话框

6.5.4 Auto-Disable

[Diagnostics > Ports > Auto-Disable]

Auto-Disable 功能允许用户自动禁用并根据需要再次启用被监控端口。

例如，如果超过了被监控参数，则 *Port Monitor* 功能和 *Network Security* 菜单中的选定功能将使用 *Auto-Disable* 功能禁用端口。

如果不再超过这些参数，则 *Auto-Disable* 功能将在指定等待时间之后再次启用相关端口。

该对话框包含以下选项卡：

- ▶ [Port]
- ▶ [Status]

[Port]

此选项卡显示超过参数导致哪些端口当前被禁用。如果不再超过这些参数且用户在 *Reset timer [s]* 列中指定了等待期，则 *Auto-Disable* 功能将再次自动启用相关端口。

表格

Port

显示端口编号。

Reset timer [s]

指定 *Auto-Disable* 功能再次启用端口之前的等待期（秒）。

可能的值：

- ▶ 0（默认设置）
计时器已停用。端口保持禁用状态。
- ▶ 30..4294967295
如果不再超过这些参数，则 *Auto-Disable* 功能将在此处指定的等待期之后再次启用端口。

Error time

显示超过参数导致设备禁用端口的时间。

Remaining time [s]

显示 *Auto-Disable* 功能再次启用端口之前的剩余时间（秒）。

Component

显示设备中禁用了端口的软件组件。

可能的值：

- ▶ **PORT_MON**
Port Monitor
参见 *Diagnostics > Ports > Port Monitor* 对话框。
- ▶ **PORT_ML**
Port Security
参见 *Network Security > Port Security* 对话框。
- ▶ **DHCP_SNP**
DHCP Snooping
参见 *Network Security > DHCP Snooping* 对话框。
- ▶ **DOT1S**
BPDU guard
参见 *Switching > L2-Redundancy > Spanning Tree > Global*对话框。
- ▶ **DAI**
Dynamic ARP Inspection
参见 *Network Security > Dynamic ARP Inspection* 对话框。

Reason

显示导致端口被禁用的被监控参数。

可能的值：

- ▶ **none**
无被监控参数。
端口已启用。
- ▶ **link-flap**
链路变化次数太多。参见 *Diagnostics > Ports > Port Monitor* 对话框的 *Link flap* 选项卡。
- ▶ **crc-error**
检测到过多的 CRC/片段错误。参见 *Diagnostics > Ports > Port Monitor* 对话框的 *CRC/Fragments* 选项卡。
- ▶ **duplex-mismatch**
检测到双工不匹配。参见 *Diagnostics > Ports > Port Monitor* 对话框的 *Global* 选项卡。
- ▶ **dhcp-snooping**
来自不可信来源的 DHCP 数据包太多。参见 *Network Security > DHCP Snooping > Configuration* 对话框的 *Port* 选项卡。
- ▶ **arp-rate**
来自不可信来源的 ARP 数据包太多。参见 *Network Security > Dynamic ARP Inspection > Configuration* 对话框的 *Port* 选项卡。
- ▶ **bpdu-rate**
收到了 STP-BPDU。参见 *Switching > L2-Redundancy > Spanning Tree > Global*对话框。
- ▶ **mac-based-port-security**
来自不需要的发送者的数据包太多。参见 *Network Security > Port Security* 对话框。
- ▶ **overload-detection**
过载。参见 *Diagnostics > Ports > Port Monitor* 对话框的 *Overload detection* 选项卡。

- ▶ **speed-duplex**
检测到不允许的速度和双工模式组合。参见 *Diagnostics > Ports > Port Monitor* 对话框的 *Link speed/Duplex mode detection* 选项卡。
- ▶ **Loop protection**
在端口上检测到第二层网络环路。参见 *Diagnostics > Loop Protection* 对话框的 *Loop detected* 列。

Active

显示端口当前是否因超过参数而被禁用。

可能的值：

- ▶ **勾选**
端口当前已禁用。
- ▶ **未勾选**
端口已启用。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

[Status]

此选项卡显示为其激活了 *Auto-Disable* 功能的被监控参数。

表格

Reason

显示设备监控的参数。

勾选相邻复选框，使 *Auto-Disable* 功能在超过被监控参数时禁用并视情况再次启用端口。

Category

显示相邻参数属于哪个功能。

可能的值：

- ▶ **port-monitor**
参数属于 *Diagnostics > Port > Port Monitor* 菜单中的功能。
- ▶ **network-security**
参数属于 *Network Security* 菜单中的功能。
- ▶ **l2-redundancy**
参数属于 *Switching > L2-Redundancy* 菜单中的功能。

Auto-disable

显示是否已针对相邻参数激活/停用 *Auto-Disable* 功能。

可能的值：

- ▶ 勾选
相邻参数的 *Auto-Disable* 功能已激活。
Auto-Disable 功能在超过被监控参数时将禁用并视情况再次启用相关端口。
- ▶ 未勾选（默认设置）
相邻参数的 *Auto-Disable* 功能已停用。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

Reset

再次启用表格中突出显示的端口并将其计数器重置为 0。这将影响以下对话框中的计数器：

- ▶ *Diagnostics > Ports > Port Monitor* 对话框
 - *Link flap* 选项卡
 - *CRC/Fragments* 选项卡
 - *Overload detection* 选项卡
- ▶ *Diagnostics > Ports > Auto-Disable* 对话框

6.5.5 Port Mirroring

[Diagnostics > Ports > Port Mirroring]

Port Mirroring 功能允许用户将接收和发送的数据包从选定端口复制到目标端口。可以使用连接到目标端口的分析仪或 RMON 探测器对数据流进行观察和处理。源端口上的数据包保持不变。

提示：要启用使用目标端口访问设备管理，请在启用 *Port Mirroring* 功能之前勾选 *Destination port* 框中的 *Allow management* 复选框。

Operation

Operation

启用/禁用 *Port Mirroring* 功能。

可能的值：

- ▶ *On*
Port Mirroring 功能已启用。
设备将数据包从选定源端口复制到目标端口。
- ▶ *Off* (默认设置)
Port Mirroring 功能已禁用。

Destination port

Primary port

指定目标端口。

合适的端口是不用于以下目的的端口：

- 源端口
- 第二层冗余协议

可能的值：

- ▶ *no Port* (默认设置)
未选择目标端口。
- ▶ *<Port number>*
目标端口的数量。设备将数据包从源端口复制到该端口。

在目标端口上，设备向源端口传输的数据包中添加一个 VLAN 标记。目标端口传输源端口接收到的未经修改的数据包。

提示：目标端口需要足够的带宽来吸收数据流。如果复制的数据流超过目标端口的带宽，则设备将在目标端口上丢弃多余的数据包。

Secondary port

指定第二个目标端口。前提条件是用户已指定主端口。

可能的值：

- ▶ **no Port**（默认设置）
未选择目标端口。
- ▶ **<Port number>**
目标端口的数量。设备将数据包从源端口复制到该端口。

Allow management

激活/停用使用目标端口访问设备管理。

可能的值：

- ▶ **勾选**
使用目标端口访问设备管理已激活。
设备允许用户在不中断活动 *Port Mirroring* 会话的前提下访问使用目标端口的设备管理。
 - 设备在目标端口上复制多播、广播和未知单播。
 - 目标端口上的 VLAN 设置保持不变。使用目标端口访问设备管理的前提条件是，目标端口不是设备管理 VLAN 的成员。
- ▶ **未勾选**（默认设置）
使用目标端口访问设备管理已停用。
设备禁止使用目标端口访问设备管理。

表格

Source port

指定端口编号。

可能的值：

- ▶ **<Port number>**

Enabled

激活/停用将数据包从源端口复制到目标端口。

可能的值：

- ▶ **勾选**
数据包复制已激活。
该端口被指定为源端口。
- ▶ **未勾选**（默认设置）
数据包复制已停用。
- ▶ **（灰色显示）**
无法复制此端口的数据包。
可能的原因：
 - 该端口已经被指定为目标端口。
 - 该端口是逻辑端口，而不是物理端口。

提示：设备允许用户将除目标端口之外的每个物理端口激活为源端口。

Type

指定设备将哪些数据包复制到目标端口。

在目标端口上，设备向源端口传输的数据包中添加一个 VLAN 标记。目标端口传输源端口接收到的未经修改的数据包。

可能的值：

- ▶ `none`（默认设置）
无数据包。
- ▶ `tx`
源端口传输的数据包。
- ▶ `rx`
源端口接收的数据包。
- ▶ `txrx`
源端口传输和接收的数据包。

提示：使用 `txrx` 设置，设备将复制传输和接收的数据包。目标端口至少需要与源端口的发送和接收通道之和相对应的带宽。例如，对于类似的端口，当源端口的发送和接收通道分别达到 50% 的容量时，目标端口容量为 100%。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

Reset config

将对话框中的设置重置为默认设置并将更改传送到设备的易失性存储器 (*RAM*)。

6.6 LLDP

[Diagnostics > LLDP]

设备允许用户收集关于相邻设备的信息。为此，设备将使用 Link Layer Discovery Protocol (LLDP)。此信息使网络管理站能够映射用户网络结构。

此菜单允许用户配置拓扑识别并以表格形式显示接收到的信息。

该菜单包含以下对话框：

- ▶ [LLDP Configuration](#)
- ▶ [LLDP Topology Discovery](#)

6.6.1 LLDP Configuration

[Diagnostics > LLDP > Configuration]

此对话框可用于为每个端口配置拓扑识别。

Operation

Operation

启用/禁用 *LLDP* 功能。

可能的值：

- ▶ *On* (默认设置)
LLDP 功能已启用。
设备中使用 *LLDP* 的拓扑识别已激活。
- ▶ *Off*
LLDP 功能已禁用。

Configuration

Transmit interval [s]

指定设备传输 *LLDP* 数据包的间隔（秒）。

可能的值：

- ▶ 5..32768 (默认设置：30)

Transmit interval multiplier

为 *LLDP* 数据包指定确定生存时间值的系数。

可能的值：

- ▶ 2..10 (默认设置：4)

LLDP 报头中编码的生存时间值是使用此值乘以 *Transmit interval [s]* 字段中的值得出的。

Reinit delay [s]

指定端口重新初始化的延迟（秒）。

可能的值：

- ▶ 1..10 (默认设置：2)

如果在 *Operation* 列中指定的值是 *Off*，则设备在经过此处指定的时间后将尝试重新初始化端口。

Transmit delay [s]

指定在设备中发生配置更改后传输连续 LLDP 数据包的延迟（秒）。

可能的值：

- ▶ 1..8192（默认设置：2）

建议的值介于最小为 1 与最大为 *Transmit interval [s]* 字段中的值的四分之一之间。

Notification interval [s]

指定传输 LLDP 通知的间隔（秒）。

可能的值：

- ▶ 5..3600（默认设置：5）

传输一个通知陷阱后，设备至少等待此处指定的时间，然后再传输下一个通知陷阱。

表格

Port

显示端口编号。

Operation

指定端口是否传输和接收 LLDP 数据包。

可能的值：

- ▶ *transmit*
端口传输 LLDP 数据包，但不保存任何关于相邻设备的信息。
- ▶ *receive*
端口接收 LLDP 数据包，但不向相邻设备传输任何信息。
- ▶ *receive and transmit*（默认设置）
端口传输 LLDP 数据包，并保存关于相邻设备的信息。
- ▶ *disabled*
端口不传输 LLDP 数据包，也不保存关于相邻设备的信息。

Notification

激活/停用端口上的 LLDP 通知。

可能的值：

- ▶ 勾选
端口上的 LLDP 通知已激活。
- ▶ 未勾选（默认设置）
端口上的 LLDP 通知已停用。

Transmit port description

激活/停用带有端口描述的 TLV（类型长度值）的传输。

可能的值：

- ▶ **勾选**（默认设置）
TLV 传输已激活。
设备传输带有端口描述的 TLV。
- ▶ **未勾选**
TLV 传输已停用。
设备不传输带有端口描述的 TLV。

Transmit system name

激活/停用带有设备名称的 TLV（类型长度值）的传输。

可能的值：

- ▶ **勾选**（默认设置）
TLV 传输已激活。
设备传输带有设备名称的 TLV。
- ▶ **未勾选**
TLV 传输已停用。
设备不传输带有设备名称的 TLV。

Transmit system description

激活/停用带有系统描述的 TLV（类型长度值）的传输。

可能的值：

- ▶ **勾选**（默认设置）
TLV 传输已激活。
设备传输带有系统描述的 TLV。
- ▶ **未勾选**
TLV 传输已停用。
设备不传输带有系统描述的 TLV。

Transmit system capabilities

激活/停用带有系统功能的 TLV（类型长度值）的传输。

可能的值：

- ▶ **勾选**（默认设置）
TLV 传输已激活。
设备传输带有系统功能的 TLV。
- ▶ **未勾选**
TLV 传输已停用。
设备不传输带有系统功能的 TLV。

Neighbors (max.)

限制此端口要记录的相邻设备的数量。

可能的值：

- ▶ 1..50（默认设置：10）

FDB mode

指定设备使用哪个功能记录此端口上的相邻设备。

可能的值：

- ▶ `lldpOnly`
设备只使用 LLDP 数据包记录此端口上的相邻设备。
- ▶ `macOnly`
设备使用示教 MAC 地址记录此端口上的相邻设备。只有当此端口的地址表中没有其他条目（FDB，转发数据库）时，设备才使用 MAC 地址。
- ▶ `both`
设备使用 LLDP 数据包和示教 MAC 地址记录此端口上的相邻设备。
- ▶ `autoDetect`（默认设置）
如果设备在此端口接收 LLDP 数据包，则设备将执行与 `lldpOnly` 设置相同的操作。否则，设备将执行与 `macOnly` 设置相同的操作。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

6.6.2 LLDP Topology Discovery

[Diagnostics > LLDP > Topology Discovery]

网络中的设备以也称为“LLDPDU”（LLDP 数据单元）的数据包的形式发送通知。通过 LLDPDU 发送和接收的数据有很多用处。为此，设备会检测网络中的哪些设备是邻居，以及它们通过哪些端口进行连接。

该对话框允许用户显示网络并检测连接的设备及其特定功能。

该对话框包含以下选项卡：

- ▶ [LLDP]
- ▶ [LLDP-MED]

[LLDP]

此选项卡显示为相邻设备收集的 LLDP 信息。此信息使网络管理站能够映射用户网络结构。

当端口上同时连接了具有和不具有活动拓扑识别功能的设备时，拓扑表将隐藏没有活动拓扑识别的设备。

当端口上只连接了不具有活动拓扑识别的设备时，该表格包含使该端口表示每个设备的一行。此行包含连接的设备的数量。

转发数据库（FDB）地址表包含拓扑表为了清晰起见而隐藏的设备的 MAC 地址。

当用户使用一个端口连接多个设备时（例如通过集线器），表格会为每个已连接的设备包含一行。

表格

Port

显示端口编号。

Neighbor identifier

显示相邻设备的机箱 ID。例如，这可以是相邻设备的基础 MAC 地址。

FDB

显示已连接设备是否具备有效的 LLDP 支持。

可能的值：

- ▶ 勾选
相连设备不具有活动的 LLDP 支持。
设备使用来自其地址表的信息（FDB, Forwarding Database）
- ▶ 未勾选（默认设置）
相连设备具有活动的 LLDP 支持。

Neighbor IP address

显示访问相邻设备的设备管理时可以使用的 IP 地址。

Neighbor port description

显示相邻设备的端口的描述。

Neighbor system name

显示相邻设备的设备名称。

Neighbor system description

显示相邻设备的描述。

Port ID

显示将相邻设备连接到设备时使用的端口的 ID。

Autonegotiation supported

显示相邻设备的端口是否支持自动协商。

Autonegotiation

显示相邻设备的端口上是否已启用自动协商。

PoE supported

显示相邻设备的端口是否支持以太网供电 (PoE)。

PoE enabled

显示相邻设备的端口上是否已启用以太网供电 (PoE)。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

[LLDP-MED]

用于介质端点设备的 LLDP (LLDP-MED) 是对 LLDP 的扩展，它在端点设备和网络设备之间运行。它专门为 VoIP 应用程序提供支持。在此支持规则下，它额外提供一组普通公告、类型长度值 (TLV) 和消息。设备使用 TLV 进行网络策略、以太网供电、库存管理和位置信息等功能发现。

表格**Port**

显示端口编号。

Device class

显示远程连接设备的设备类别。

- ▶ 值 `notDefined` 表示设备具有任何 `LLDP-MED` 类别都没有覆盖的功能。
- ▶ 值 `endpointClass1.3` 表示设备具有“端点类别 1.3”功能。
- ▶ 值 `networkConnectivity` 表示设备具有网络连通性设备功能。

VLAN ID

根据 IEEE 802.3 中的定义显示连接到此端口的远程系统的 VLAN 标识符的扩展名。

- ▶ 设备使用一个从 1 一直到 4042 的值指定一个有效的端口 VLAN ID。
- ▶ 对于优先级标记数据包，设备将显示值 0。这意味着，只有 802.1D 优先级是重要的，且设备使用入口端口的默认 VLAN ID。

Priority

显示与连接到端口的远程系统相关联的 802.1D 优先级的值。

DSCP

显示与连接到端口的远程系统相关联的区分服务代码点 (DSCP) 的值。

Unknown bit status

显示发入流量的未知位状态。

- ▶ 值 `true` 表示指定应用程序类型的网络策略当前为未知。在这种情况下，VLAN ID 将忽略第二层优先级以及 `DSCP` 字段的值。
- ▶ 值 `false` 表示指定的网络策略。

Tagged bit status

显示标记位状态。

- ▶ 值 `true` 表示应用程序使用标记 VLAN。
- ▶ 值 `false` 表示对于特定应用程序，设备使用未标记 VLAN 操作。在这种情况下，设备同时忽略 VLAN ID 字段和第二层优先级字段。但是，DSCP 值仍然有意义。

Hardware revision

显示远程端点所公布的特定供应商硬件修订字符串。

Firmware revision

显示远程端点所公布的特定供应商固件修订字符串。

Software revision

显示远程端点所公布的特定供应商软件修订字符串。

Serial number

显示远程端点所公布的特定供应商序列号。

Manufacturer name

显示远程端点所公布的特定供应商制造商名称。

Model name

显示远程端点所公布的特定供应商型号名称。

Asset ID

显示远程端点所公布的特定供应商资产跟踪标识符。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

6.7 Loop Protection

[Diagnostics > Loop Protection]

Loop Protection 功能可帮助防止第二层网络环路。

网络环路可能因过载而导致网络停顿。一个可能的原因是，由错误配置造成的数据包持续复制。例如，原因可能是电缆连接不良或设备中的设置不正确。

例如，如果未激活任何冗余协议，则可能在以下情况中发生第二层环路：

- 同一个设备的两个端口直接相互连接。
- 两个设备之间建立了多个活动连接。

在冗余网络拓扑中，通常已激活多个冗余协议。通常在涉及其他冗余协议的端口上禁用 *Spanning Tree* 功能。冗余协议已经帮助避免环路。

Operation

Operation

启用/禁用 *Loop Protection* 功能。

可能的值：

▶ *On*

Loop Protection 功能已启用。

- 在主动和被动端口上，设备会评估收到的 *环路检测数据包*。

在主动端口上，设备以 *Transmit interval* 字段中指定的定期间隔发送 *环路检测数据包*。
前提条件是端口上已激活 *Loop Protection* 功能。

- 设备允许用户通过信号触点来监控以太网环路。参见 *Diagnostics > Status Configuration > Signal Contact > Signal Contact 1* 对话框中 *Ethernet loops* 参数的复选框。

▶ *Off* (默认设置)

Loop Protection 功能已禁用。

设备既不发送 *环路检测数据包*，也不评估收到的 *环路检测数据包*。

Global

Transmit interval

指定当端口上已激活 *Loop Protection* 功能时设备发送 *环路检测* 数据包的间隔（秒）。

可能的值：

- ▶ 1..10

Receive threshold

指定连续接收的 *环路检测* 数据包数量的阈值。如果数量达到或超过此阈值，则设备将执行 *Action* 列中指定的操作。

可能的值：

- ▶ 1..50

Configuration

Auto-disable

激活/停用 *Loop Protection* 的 *Auto-Disable* 功能。

可能的值：

- ▶ 勾选
Loop Protection 的 *Auto-Disable* 功能已激活。
禁用端口的前提条件是已在 *Action* 列中指定 *auto-disable* 或 *all* 操作。
设备允许用户指定 *Auto-Disable* 功能再次启用端口之前的等待期（秒）。为此，请在 *Diagnostics > Ports > Auto-Disable* 对话框的 *Reset timer [s]* 列中指定等待期。
- ▶ 未勾选（默认设置）
Loop Protection 的 *Auto-Disable* 功能已停用。

表格

Port

显示端口编号。

Active

激活/停用端口上的 *Loop Protection* 功能。

可能的值：

- ▶ *勾选*
端口上的 *Loop Protection* 功能已激活。
仅在不属于冗余网络路径的端口上激活该功能。这样可帮助避免冗余网络路径意外关闭。
如果设备在此端口上收到从同一个设备上的其他端口发送的 *环路检测数据包*，则设备将执行 *Action* 列中指定的操作。
- ▶ *未勾选*（默认设置）
端口上的 *Loop Protection* 功能已停用。端口既不发送 *环路检测数据包*，也不评估收到的 *环路检测数据包*。

Mode

指定端口上的 *Loop Protection* 功能的行为。

可能的值：

- ▶ *active*
设备发送 *环路检测数据包*，并且评估收到的 *环路检测数据包*。
- ▶ *passive*
设备评估收到的 *环路检测数据包*。

Action

指定设备在此端口上检测到第二层网络环路时执行的操作。

可能的值：

- ▶ *trap*
设备发送陷阱。
- ▶ *auto-disable*
设备使用 *Auto-Disable* 功能来禁用端口。
前提条件是已勾选 *Configuration* 框中的 *Auto-disable* 复选框。
- ▶ *all*
设备发送陷阱。然后，设备使用 *Auto-Disable* 功能来禁用端口。
前提条件是已勾选 *Configuration* 框中的 *Auto-disable* 复选框。

VLAN ID

指定设备在其中发送 *环路检测数据包* 的 VLAN。

可能的值：

- ▶ *0*（默认设置）
设备发送不包含 VLAN 标签的 *环路检测数据包*。
- ▶ *1..4042*
设备在指定的 VLAN 中发送 *环路检测数据包*。前提条件是已配置 VLAN 并且端口是 VLAN 的成员。参见 *Switching > VLAN > Port* 对话框。

Loop detected

显示设备是否已在端口上检测到第二层网络环路。

可能的值：

- ▶ *yes*
设备已在端口上检测到第二层网络环路。
在环路已终止并且再次启用端口之后，设备会将值重置为 *no*。
- ▶ *no*
设备未在端口上检测到第二层网络环路。

Loop count

显示自上次端口统计数据重置以来或自上次设备重新启动以来，设备已在端口上检测到的环路的数量。

Last loop time

显示设备在端口上检测到上一个环路的时间。

值的正确评估的前提条件是，将设备的系统时间与适当的参考时间同步。参见 [Time > Basic Settings](#) 对话框。

Sent frames

显示自上次端口统计数据重置以来或自上次设备重新启动以来，在端口上发送的环路检测数据包的数量。

Received frames

显示自上次端口统计数据重置以来或自上次设备重新启动以来，在端口上发送和接收回来的环路检测数据包的数量。

Discarded frames

显示在端口上丢弃的环路检测数据包的数量。

丢弃的数据包的原因示例：

- 设备检测到格式不正确的数据包。
- 设备检测到时间戳已过期的数据包（在发送之后超过 5 秒收到的数据包）。
- 设备收到包含意外 VLAN 信息的数据包。
- 设备检测到在已禁用的端口上收到的数据包。

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

Clear port statistics

重置以下列中的值：

- *Loop count*
- *Sent frames*
- *Received frames*

6.8 Report

[Diagnostics > Report]

该菜单包含以下对话框：

- ▶ Report Global
- ▶ Persistent Logging
- ▶ System Log
- ▶ Audit Trail

6.8.1 Report Global

[Diagnostics > Report > Global]

设备允许用户使用以下输出记录特定事件：

- ▶ 在控制台上
- ▶ 在一个或多个系统日志服务器上
- ▶ 在使用 SSH 建立的命令行界面连接上
- ▶ 在使用 Telnet 建立的命令行界面连接上

在此对话框中，可以指定所需的设置。通过分配严重程度，可以指定设备对哪些事件进行注册。

该对话框允许用户将带有系统信息的 ZIP 文档保存到用户 PC 上。

Console logging

Operation

启用/禁用 *Console logging* 功能。

可能的值：

- ▶ *On*
Console logging 功能已启用。
设备在控制台上记录事件。
- ▶ *Off* (默认设置)
Console logging 功能已禁用。

Severity

指定事件的最低严重程度。设备记录具有这种严重程度以及具有更加紧迫的严重程度的事件。

设备在串行接口上输出消息。

可能的值：

- ▶ *emergency*
- ▶ *alert*
- ▶ *critical*
- ▶ *error*
- ▶ *warning* (默认设置)
- ▶ *notice*
- ▶ *informational*
- ▶ *debug*

Buffered logging

设备将记录的事件缓冲到两个单独的存储区域中，使紧急事件的日志条目得到保留。

此对话框允许用户为设备在存储区域中缓冲的具有较高优先级的事件指定最低严重程度。

Severity

指定事件的最低严重程度。设备将具有这种严重程度以及具有更紧迫严重程度的事件的日志条目缓冲到具有较高优先级的存储区域中。

可能的值：

- ▶ emergency
- ▶ alert
- ▶ critical
- ▶ error
- ▶ warning (默认设置)
- ▶ notice
- ▶ informational
- ▶ debug

SNMP logging

在启用 SNMP 请求记录时，设备将这些请求作为具有预设严重程度 `notice` 的事件发送到系统日志服务器列表。一个系统日志服务器条目的预设最低严重程度为 `critical`。

要向系统日志服务器发送 SNMP 请求，可以通过多种方式更改默认设置。请选择最符合要求的方式。

- 将设备以事件形式创建 SNMP 请求的严重程度设置为 `warning` 或 `error`。将一个或多个系统日志服务器的系统日志条目的最低严重程度更改为相同的值。
用户还可以选择为此创建一个单独的系统日志服务器条目。
- 仅将 SNMP 请求的严重程度设置为 `critical` 或以上。然后，设备将 SNMP 请求作为具有 `critical` 或以上严重程度的事件发送到系统日志服务器。
- 仅将一个或多个系统日志服务器条目的最低严重程度设置为 `notice` 或以下。然后，设备可以将很多事件发送到系统日志服务器。

Log SNMP get request

启用/禁用 SNMP Get requests 的记录。

可能的值：

- ▶ `On`
记录已启用。
设备将 SNMP Get requests 作为事件注册到系统日志中。
在 `Severity get request` 下拉列表中，可以选择此事件的严重程度。
- ▶ `Off` (默认设置)
记录已禁用。

Log SNMP set request

启用/禁用 SNMP Set requests 的记录。

可能的值：

- ▶ *On*
记录已启用。
设备将 SNMP Set requests 作为事件注册到系统日志中。
在 *Severity set request* 下拉列表中，可以选择此事件的严重程度。
- ▶ *Off* (默认设置)
记录已禁用。

Severity get request

指定设备为 SNMP Get requests 注册的事件的严重程度。

可能的值：

- ▶ *emergency*
- ▶ *alert*
- ▶ *critical*
- ▶ *error*
- ▶ *warning*
- ▶ *notice* (默认设置)
- ▶ *informational*
- ▶ *debug*

Severity set request

指定设备为 SNMP Set requests 注册的事件的严重程度。

可能的值：

- ▶ *emergency*
- ▶ *alert*
- ▶ *critical*
- ▶ *error*
- ▶ *warning*
- ▶ *notice* (默认设置)
- ▶ *informational*
- ▶ *debug*

CLI logging

Operation

启用/禁用 *CLI logging* 功能。

可能的值：

- ▶ *On*
CLI logging 功能已启用。
设备记录使用命令行界面接收的每个命令。
- ▶ *Off* (默认设置)
CLI logging 功能已禁用。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

Download support information

生成一个 Web 浏览器允许用户从设备中下载的 ZIP 文档。

该 ZIP 文档包含关于设备的系统信息。下节中提供了 ZIP 文档中包含的文件的解释。

支持信息：ZIP 文档中包含的文件

文件名	格式	注释
audittrail.html	HTML	包含系统事件的时序记录以及 Audit Trail 中保存的用户更改。
defaultconfig.xml	XML	包含带有默认设置的配置概要文件。
script	TEXT	包含命令 <code>show running-config script</code> 的输出。
runningconfig.xml	XML	包含带有当前操作设置的配置概要文件。
supportinfo.html	TEXT	包含设备内部服务信息。
systeminfo.html	HTML	包含有关当前设置和操作参数的信息。
systemlog.html	HTML	包含日志文件中的已记录事件。参见 Diagnostics > Report > System Log 对话框。

事件严重程度的含义

严重程度	含义
emergency	设备未处于运行准备就绪状态
alert	需要立即进行用户干预
critical	重要状态
error	错误状态
warning	警告

严重程度	含义
notice	重要正常状态
informational	非正式消息
debug	调试消息

6.8.2 Persistent Logging

[Diagnostics > Report > Persistent Logging]

设备允许用户将日志条目永久保存到外部存储器的文件中。因此，即使在设备重新启动之后，用户仍然可以访问这些日志条目。

在此对话框中，可以限制日志文件的大小并指定要保存的事件的最低严重程度。当日志文件达到指定的大小时，设备将对此文件进行存档并将以下日志条目保存到新创建的文件中。

在该表格中，设备将显示外部存储器中保存的日志文件。达到指定的最大文件数量后，设备将立即删除最老的文件并对剩余的文件进行重命名。这有助于确保外部存储器中有足够的内存空间。

提示： 验证是否已连接外部存储器。要验证是否已连接外部存储器，请参见 [Basic Settings > External Memory](#) 对话框中的 *Status* 列。我们建议使用 *Device Status* 功能对外部存储器连接进行监控，请参见 [Diagnostics > Status Configuration > Device Status](#) 对话框中的 *External memory removal* 参数。

Operation

Operation

启用/禁用 *Persistent Logging* 功能。

只有当设备中的外部存储器可用时，才能激活此功能。

可能的值：

- ▶ *On* (默认设置)
Persistent Logging 功能已启用。
设备将日志条目保存到外部存储器的文件中。
- ▶ *Off*
Persistent Logging 功能已禁用。

Configuration

Max. file size [kbyte]

指定日志文件的最大大小（千字节）。当日志文件达到指定的大小时，设备将对此文件进行存档并将以下日志条目保存到新创建的文件中。

可能的值：

- ▶ *0..4096* (默认设置: *1024*)

0 值会停用将日志条目保存到日志文件中。

Files (max.)

指定设备在外部存储器中保存的日志文件的数量。

达到指定的最大文件数量后，设备将立即删除最老的文件并对剩余的文件进行重命名。

可能的值:

- ▶ 0..25 (默认设置: 4)

0 值会停用将日志条目保存到日志文件中。

Severity

指定事件的最低严重程度。设备将具有这种严重程度以及具有更紧迫严重程度的事件的日志条目保存到外部存储器的日志文件中。

可能的值:

- ▶ emergency
- ▶ alert
- ▶ critical
- ▶ error
- ▶ warning (默认设置)
- ▶ notice
- ▶ informational
- ▶ debug

Log file target

指定用于记录的外部存储器设备。

可能的值:

- ▶ usb
外部 USB 存储器 (EAM)

表格

Index

显示与表格条目相关的索引编号。

可能的值:

- ▶ 1..25

设备自动分配此数字。

File name

显示外部存储器中日志文件的文件名。

可能的值:

- ▶ messages
- ▶ messages.X

File size [byte]

显示外部存储器中日志文件的大小 (字节)。

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

Delete persistent log file

从外部存储器中删除日志文件。

6.8.3 System Log

[Diagnostics > Report > System Log]

设备将设备内部事件记录到日志文件（System Log）中。

此对话框显示日志文件（System Log）。该对话框允许用户将日志文件以 HTML 格式保存到用户 PC 上。

要在日志文件中搜索搜索项，请使用 Web 浏览器的搜索功能。

日志文件将一直保存到设备中进行重新启动为止。重新启动后，设备会再次创建该文件。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

Save log file

在新的 Web 浏览器窗口或选项卡中打开 HTML 页面。可以使用适当的 Web 浏览器命令将该 HTML 页面保存到用户 PC。

Delete log file

从日志文件中删除已记录的事件。

6.8.4 Audit Trail

[Diagnostics > Report > Audit Trail]

此对话框显示日志文件 (Audit Trail)。该对话框允许用户将日志文件保存为用户 PC 上的 HTML 文件。

要在日志文件中搜索搜索项，请使用 Web 浏览器的搜索功能。

设备对系统事件进行记录并将用户操作写入设备中。这可以让用户跟踪谁在何时更改了设备中的哪些内容。前提条件是，向您的用户帐户分配了 `auditor` 或 `administrator` 用户角色。

除其他操作之外，设备还对以下用户操作进行记录：

- ▶ 用户使用命令行界面登录（本地或远程）
- ▶ 用户手动注销
- ▶ 经过指定的不活动时间后自动注销命令行界面中的用户
- ▶ 设备重新启动
- ▶ 因失败的登录尝试次数过多而锁定用户帐户
- ▶ 因失败的登录尝试而锁定对设备管理的访问
- ▶ 在命令行界面中执行命令，`show` 命令除外。
- ▶ 对配置变量进行更改
- ▶ 对系统时间进行更改
- ▶ 文件传输操作，包括固件更新
- ▶ 配置更改，来自 Ethernet Switch Configurator
- ▶ 通过外部存储器对设备进行固件更新和自动配置
- ▶ 通过 HTTPS 隧道打开和关闭 SNMP

设备不记录密码。记录的条目具有写入保护并在重启后仍保存在设备中。

在重新启动期间，可以使用设备的默认设置访问系统监控器。如果攻击者获得对设备的物理访问权限，则其就能使用系统监控器将设备设置重置为默认值。在此之后，可以使用标准密码访问设备和日志文件。

警告

不允许的设备操作

请采取适当措施限制对设备的物理访问。否则，请停用对系统监控器的访问。参见 [Diagnostics > System > Selftest](#) 对话框的 `SysMon1 is available` 复选框。

如果不遵循这些说明，则会导致死亡、重伤或设备损坏。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

Save audit trail file

在新的 Web 浏览器窗口或选项卡中打开 HTML 页面。可以使用适当的 Web 浏览器命令将该 HTML 页面保存到用户 PC。

7 Advanced


该菜单包含以下对话框：

- ▶ DHCP L2 Relay
- ▶ DHCP Server
- ▶ DNS
- ▶ Industrial Protocols
- ▶ Digital IO Module
- ▶ Command Line Interface

7.1 DHCP L2 Relay

[Advanced > DHCP L2 Relay]

在设备的前置面板上，可以看到以下危险信息：

 警告
<p>非预期操作</p> <p>如果 DHCP 选项 82 已启用，请勿改变电缆位置。检修前请查看用户手册。</p> <p>如果不遵循这些说明，则会导致死亡、重伤或设备损坏。</p>

网络管理员使用 DHCP 第二层 *中继代理* 添加 DHCP 客户端信息。第三层 *中继代理* 和 DHCP 服务器需要使用 DHCP 客户端信息向客户端分配 IP 地址和配置。

激活后，该中继会将此对话框中配置的 *Option 82* 信息添加到数据包中，然后再将 DHCP 请求从客户端中继转发到服务器。*Option 82* 字段提供有关客户端和中继的唯一信息。该唯一标识符由客户端的 *电路 ID* 和中继的 *远程 ID* 组成。

除类型、长度和多播字段之外，*电路 ID* 还包括已连接客户端的 VLAN ID、单元编号、插槽编号和端口编号。

远程 ID 由一个类型和长度字段以及一个 MAC 地址、IP 地址、客户端标识符或用户自定义设备描述组成。客户端标识符是设备的用户自定义系统名称。

对于 DHCPv6 协议，设备使用 *中继代理* 将 *中继代理* 选项添加到在客户端与 DHCPv6 服务器之间交换的 DHCPv6 数据包。RFC 6221 中介绍了轻量级 DHCPv6 中继代理 (LDRA)。

LDRA 处理 2 种类型的消息：

- ▶ *中继转发消息*
中继代理 转发 *中继转发消息*，该消息包含关于客户端的唯一信息。客户端信息包括对等地址，表示客户端的 IPv6 链路本地地址，以及 *接口 ID* 信息。*接口 ID* 信息也称为 *Option 18*，其提供的信息可用于识别在其上发送客户端请求的接口。
- ▶ *中继应答消息*
 DHCPv6 服务器发送 *中继应答消息*。*中继代理* 对消息进行验证，以包括在初始 *中继转发消息* 中封装的信息。如果信息有效，则 *中继代理* 将数据包转发到客户端。

该菜单包含以下对话框：

- ▶ DHCP L2 Relay Configuration
- ▶ DHCP L2 Relay Statistics

7.1.1 DHCP L2 Relay Configuration

[Advanced > DHCP L2 Relay > Configuration]

此对话框允许用户激活接口和 VLAN 上的中继功能。当用户激活某个端口上的此功能时，设备要么中继转发 *Option 82* 信息，要么删除不可信端口上的信息。此外，设备还允许用户指定远程标识符。

Option 82 信息特定于 DHCPv4 第二层中继功能。对于 DHCPv6 第二层中继功能，*Option 18* 信息用于在客户端与 DHCPv6 服务器之间交换数据包。设备丢弃在端口上接收的不包含 *Option 18* 信息的 DHCPv6 数据包。

该对话框包含以下选项卡：

- ▶ [Interface]
- ▶ [VLAN ID]

Operation

Operation

全局启用/禁用设备的 DHCP 第二层中继功能。

启用此功能后，DHCPv4 第二层中继和 DHCPv6 第二层中继功能可在设备中同时运行。

可能的值：

- ▶ *On*
启用设备中的 *DHCP L2 Relay* 功能。
- ▶ *Off* (默认设置)
禁用设备中的 *DHCP L2 Relay* 功能。

[Interface]

表格

Port

显示端口编号。

Active

激活/停用端口上的 *DHCP L2 Relay* 功能。

前提条件是全局启用该功能。

可能的值：

- ▶ 勾选
DHCP L2 Relay 功能激活。
- ▶ 未勾选 (默认设置)
DHCP L2 Relay 功能停用。

Trusted port

激活/停用相应端口的安全 *DHCP L2 Relay* 模式。

可能的值：

- ▶ **勾选**
设备接受带有 *Option 82* 信息的 DHCPv4 数据包。
设备接受带有 *Option 18* 信息的 DHCPv6 数据包。
- ▶ **未勾选**（默认设置）
设备丢弃在非安全端口上接收的包含 *Option 82* 信息的 DHCPv4 数据包。
设备丢弃在端口上接收的不包含 *Option 18* 信息的 DHCPv6 数据包。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

[VLAN ID]

表格

VLAN ID

与表格条目相关的 VLAN。

Active

激活/停用 VLAN 上的 *DHCP L2 Relay* 功能。

前提条件是全局启用该功能。

可能的值：

- ▶ **勾选**
DHCP L2 Relay 功能激活。
- ▶ **未勾选**（默认设置）
DHCP L2 Relay 功能停用。

Circuit ID

激活或停用向 *Option 82* 信息中添加 *电路 ID*。

可能的值：

- ▶ **勾选**（默认设置）
允许同时发送 *电路 ID* 和 *远程 ID*。
- ▶ **未勾选**
设备只发送 *远程 ID*。

Remote ID type

为此 VLAN 指定 *远程 ID* 的组成要素。

可能的值：

- ▶ `ip`
将设备的 IP 地址指定为 *远程 ID*。
- ▶ `mac`（默认设置）
将设备的 MAC 地址指定为 *远程 ID*。
- ▶ `client-id`
将设备的系统名称指定为 *远程 ID*。
- ▶ `other`
使用此值时，请在 *Remote ID* 列用户自定义信息中输入。

Remote ID

显示 VLAN 的 *远程 ID*。

在 *Remote ID type* 列中指定 `other` 值时，请指定标识符。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

7.1.2 DHCP L2 Relay Statistics

[Advanced > DHCP L2 Relay > Statistics]

设备监控端口上的流量，并以表格形式显示结果。

此表格划分为各种不同类别，以使用户进行流量分析。

统计表中不显示 DHCPv6 中继选项。

表格

Port

显示端口编号。

Untrusted server messages with Option 82

显示在不可信接口上接收的带有 *Option 82* 信息的 DHCP 服务器消息的数量。

Untrusted client messages with Option 82

显示在不可信接口上接收的带有 *Option 82* 信息的 DHCP 客户端消息的数量。

Trusted server messages without Option 82

显示在可信接口上接收的不带 *Option 82* 信息的 DHCP 服务器消息的数量。

Trusted client messages without Option 82

显示在可信接口上接收的不带 *Option 82* 信息的 DHCP 客户端消息的数量。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

Reset

重置整个表格。

7.2 DHCP Server

[Advanced > DHCP Server]

利用 DHCP 服务器，用户可以管理可用 IP 地址和配置信息数据库。当设备接收到来自客户端的请求时，DHCP 服务器会对 DHCP 客户端网络进行验证，然后出租一个 IP 地址。激活后，DHCP 服务器还会分配对于该客户端适当的配置信息。例如，该配置信息可以指定一个客户端使用哪个 IP 地址、DNS 服务器和默认路由。

在用户自定义间隔期间，DHCP 服务器会向一个客户端分配一个 IP 地址。DHCP 客户端负责在该时间间隔过期之前更新 IP 地址。当 DHCP 客户端无法更新该地址时，该地址会退回到地址库进行重新分配。

该菜单包含以下对话框：

- ▶ DHCP Server Global
- ▶ DHCP Server Pool
- ▶ DHCP Server Lease Table

7.2.1 DHCP Server Global

[Advanced > DHCP Server > Global]

根据用户的要求全局或按端口激活该功能。

Operation

Operation

全局启用/禁用设备的 DHCP 服务器功能。

可能的值：

- ▶ *On*
- ▶ *Off* (默认设置)

Configuration

IP Probe

激活/停用对单一IP地址的检测。在分配一个IP地址之前，服务器使用 *ICMP Echo* 回应请求来检查这个IP地址是否已经在网络上被使用。

可能的值：

- ▶ *勾选* (默认设置)
IP Probe 功能激活。
- ▶ *未勾选*
IP Probe 功能停用。

表格

Port

显示端口编号。

DHCP server active

激活/停用此端口上的 DHCP 服务器功能。

前提条件是全局启用该功能。

可能的值：

- ▶ *勾选* (默认设置)
DHCP 服务器功能激活。
- ▶ *未勾选*
DHCP 服务器功能停用。

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

7.2.2 DHCP Server Pool


[Advanced > DHCP Server > Pool]

向连接到一个端口或包含在 VLAN 中的终端设备或交换机分配一个 IP 地址。

DHCP 服务器提供可从中向客户端分配 IP 地址的 IP 地址库。一个地址库由若干条目组成。将一个条目静态指定给一个特定 IP 地址或动态指定给一个 IP 地址范围。设备最多可保存 128 个地址库。所有地址库最多可保存 1000 个条目。

对于静态分配，DHCP 服务器会向一个特定客户端分配一个 IP 地址。DHCP 服务器通过唯一的硬件 ID 识别客户端。一个静态地址条目包含一个 IP 地址。用户可将此 IP 地址应用于设备的每个端口或某个特定端口。对于静态分配，请在 *IP address* 字段中输入一个需要分配的 IP 地址，并将 *Last IP address* 列留为空白。输入 DHCP 服务器用于明确识别客户端的硬件 ID。该 ID 可以是 MAC 地址、客户端 ID、远程 ID 或电路 ID。当客户端使用已知硬件 ID 与设备联系时，DHCP 服务器会分配静态 IP 地址。

在动态分配中，当一个 DHCP 客户端在一个端口上进行联系时，DHCP 服务器会从地址库中为该端口分配一个可用的 IP 地址。对于动态分配，会通过分配一个 IP 地址范围为端口创建一个地址库。指定 IP 地址范围的第一个和最后一个 IP 地址。将 *MAC address*、*Client ID*、*Remote ID* 和 *Circuit ID* 字段留为空白。用户可以选择创建多个地址库条目。这允许用户创建包含空缺的 IP 地址范围。

此对话框显示为端口或 VLAN 分配 IP 地址所需的不同信息。使用  按钮添加一个条目。设备添加一个可写可读条目。

表格

Index

显示与表格条目相关的索引编号。

Active

激活/停用此端口上的 DHCP 服务器功能。

可能的值：

- ▶ 勾选
DHCP 服务器功能激活。
- ▶ 未勾选（默认设置）
DHCP 服务器功能停用。

IP address

为静态 IP 地址分配指定 IP 地址。使用动态 IP 地址分配时，此值指定了 IP 地址范围的起点。

可能的值：

- ▶ 有效的 IPv4 地址

Last IP address

使用动态 IP 地址分配时，此值指定了 IP 地址范围的终点。

可能的值：

- ▶ 有效的 IPv4 地址

Port

显示端口编号。

VLAN ID

显示与表格条目相关的 VLAN。

值 1 对应于默认设备管理 VLAN。

可能的值：

- ▶ 1..4042

MAC address

指定租用 IP 地址的设备的 MAC 地址。

可能的值：

- ▶ 有效单播 MAC 地址
使用冒号分隔符指定值，如 00:11:22:33:44:55。
- ▶ -
对于 IP 地址分配，服务器会忽略此变量。

DHCP relay

指定客户端通过其向 DHCP 服务器传输请求的 DHCP 中继的 IP 地址。当 DHCP 服务器通过另一个 DHCP 中继接收客户端的请求时，它会忽略该请求。

可能的值：

- ▶ 有效的 IPv4 地址
DHCP 中继的 IP 地址。
- ▶ -
在客户端和 DHCP 服务器之间没有 DHCP 中继。

Client ID

指定租用 IP 地址的客户端设备的标识。

可能的值：

- ▶ 1..80 字节（格式为 `XX XX .. XX`）
- ▶ -
对于 IP 地址分配，服务器会忽略此变量。

Remote ID

指定租用 IP 地址的远程设备的标识。

可能的值：

- ▶ 1..80 字节（格式为 `XX XX .. XX`）
- ▶ -
对于 IP 地址分配，服务器会忽略此变量。

Circuit ID

指定租用 IP 地址的设备的电路 ID。

可能的值：

- ▶ 1..80 字节（格式为 `XX XX .. XX`）
- ▶ -
对于 IP 地址分配，服务器会忽略此变量。

Schneider Electric device

激活/停用 Schneider Electric 多播。

如果此 IP 地址范围内的设备只为 Schneider Electric 设备提供服务，则激活此功能。

可能的值：

- ▶ 勾选
在此 IP 地址范围内，设备只为 Schneider Electric 设备提供服务。Schneider Electric 多播已激活。
- ▶ 未勾选（默认设置）
在此 IP 地址范围内，设备为不同制造商的设备提供服务。Schneider Electric 多播已停用。

Configuration URL

指定要使用的协议以及配置文件的名称和路径。

可能的值：

- ▶ 带有 0..70 个字符的字母数字 ASCII 字符串
示例：`tftp://192.9.200.1/cfg/config.xml`

当用户将此字段留为空白时，设备会将 DHCP 消息中的此选项字段留为空白。

Lease time [s]

指定租用时间（秒）。

可能的值：

▶ 60..220752000（默认设置：86400）

▶ 4294967295

使用此值进行不限时间的分配以及通过 BOOTP 进行分配。

Default gateway

指定默认网关的 IP 地址。

0.0.0.0 值禁用在 DHCP 消息中附加选项字段。

可能的值：

▶ 有效的 IPv4 地址

Netmask

指定客户端所属网络的掩码。

0.0.0.0 值禁用在 DHCP 消息中附加选项字段。

可能的值：

▶ 有效的 IPv4 子网掩码

WINS server

指定转换 NetBIOS 名称的 Windows Internet 名称服务器的 IP 地址。

0.0.0.0 值禁用在 DHCP 消息中附加选项字段。

可能的值：

▶ 有效的 IPv4 地址

DNS server

指定 DNS 服务器的 IP 地址。

0.0.0.0 值禁用在 DHCP 消息中附加选项字段。

可能的值：

▶ 有效的 IPv4 地址

Hostname

指定主机名称。

当用户将此字段留为空白时，设备会将 DHCP 消息中的此选项字段留为空白。

可能的值:

- ▶ 带有 0..64 个字符的字母数字 ASCII 字符串

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

7.2.3 DHCP Server Lease Table

[Advanced > DHCP Server > Lease Table]

此对话框显示逐个端口 IP 地址租用的状态。

表格

Port

显示当前租用地址的端口编号。

IP address

显示条目所引用的租用 IP 地址。

Status

显示租用阶段。

根据 DHCP 操作标准，租用 IP 地址包括 4 个阶段：发现、提供、请求和确认。

可能的值：

- ▶ **bootp**
一个 DHCP 客户端正在试图发现进行 IP 地址分配的 DHCP 服务器。
- ▶ **offering**
DHCP 服务器正在验证该 IP 地址是否适合于该客户端。
- ▶ **requesting**
一个 DHCP 客户端正在获取提供的 IP 地址。
- ▶ **bound**
DHCP 服务器正在将该 IP 地址出租给一个客户端。
- ▶ **renewing**
DHCP 客户端正在请求延长租期。
- ▶ **rebinding**
DHCP 服务器正于成功更新后将 IP 地址分配给客户端。
- ▶ **declined**
DHCP 服务器拒绝了对该 IP 地址的请求。
- ▶ **released**
该 IP 地址可用于其他客户端。

Remaining lifetime

显示租用 IP 地址上的剩余时间。

Leased MAC address

显示租用 IP 地址的设备的 MAC 地址。

Gateway

显示租用 IP 地址的设备的网关 IP 地址。

Client ID

显示租用 IP 地址的设备的客户端标识符。

Remote ID

显示租用 IP 地址的设备的远程标识符。

Circuit ID

显示租用 IP 地址的设备的电路 ID。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

7.3 DNS

[[Advanced](#) > [DNS](#)]

该菜单包含以下对话框：

▶ [DNS Client](#)

7.3.1 DNS Client

[[Advanced](#) > [DNS](#) > [Client](#)]

DNS（域名系统）是网络中将主机名转换为 IP 地址的服务。此名称解析功能允许用户使用其他设备的名称（而不是 IP 地址）与之进行联系。

Client 功能让设备能够将解析 IP 地址中的主机名的请求发送到 DNS 服务器。

该菜单包含以下对话框：

- ▶ [DNS Client Global](#)
- ▶ [DNS Client Current](#)
- ▶ [DNS Client Static](#)
- ▶ [DNS Client Static Hosts](#)

7.3.1.1 DNS Client Global

[Advanced > DNS > Client > Global]

在此对话框中，可以启用 *Client* 功能和 *Cache* 功能。

Operation

Operation

启用/禁用 *Client* 功能。

可能的值：

- ▶ *On*
Client 功能已启用。
设备将解析 IP 地址中的主机名的请求发送到 DNS 服务器。
- ▶ *Off* (默认设置)
Client 功能已禁用。

Cache

Cache

启用/禁用 *Cache* 功能。

可能的值：

- ▶ *On* (默认设置)
Cache 功能已启用。
设备可在缓存中临时保存最多 128 条 DNS 服务器响应（主机名和相应的 IP 地址）。如果缓存包含匹配的条目，则设备会自行解析新请求的主机名。这使得无需向 DNS 服务器发送新查询。
- ▶ *Off*
Cache 功能已禁用。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

Flush cache

从 DNS 缓存中删除每个条目。

7.3.1.2 DNS Client Current

[Advanced > DNS > Client > Current]

此对话框显示设备将解析 IP 地址中的主机名的请求发送到哪些 DNS 服务器。

表格

Index

显示 DNS 服务器的序列号。

Address

显示 DNS 服务器的 IP 地址。设备将解析 IP 地址中的主机名的请求发送到具有此 IP 地址的 DNS 服务器。

按钮

“按钮” [页 16](#)一节中提供了标准按钮的描述。

7.3.1.3 DNS Client Static

[Advanced > DNS > Client > Static]

在此对话框中，指定设备将解析 IP 地址中的主机名的请求转发到哪些 DNS 服务器。

设备允许用户自行指定最多 4 个 IP 地址，或者传送来自 DHCP 服务器的 IP 地址。

Configuration

Configuration source

指定设备从中获取 DNS 服务器的 IP 地址的来源，设备会处理这些 DNS 服务器的请求。

可能的值：

- ▶ **user**
设备使用表格中指定的 IP 地址。
- ▶ **mgmt-dhcp**（默认设置）
设备使用 DHCP 服务器向设备提供的 IP 地址。

Domain name

按照 RFC1034 的规定，指定设备添加到不带域后缀的主机名的域名。

可能的值：

- ▶ 带有 0..255 个字符的字母数字 ASCII 字符串

Request timeout [s]

指定再次向服务器发送请求的时间间隔（秒）。

可能的值：

- ▶ **0**
停用此功能。设备不会再次向服务器发送请求。
- ▶ **1..3600**（默认设置：3）

Request retransmits

指定设备重新传输请求的次数。

前提条件是，在 *Request timeout [s]* 字段中指定值 >0。

可能的值:

- ▶ 0..100 (默认设置: 2)

表格

Index

显示 DNS 服务器的序列号。

设备允许用户指定最多 4 个 DNS 服务器。

Address

指定 DNS 服务器的 IP 地址。

可能的值:

- ▶ 有效的 IPv4 地址 (默认设置: 0.0.0.0)
- ▶ 有效的 IPv6 地址

Active

激活/停用表格条目。

设备将请求发送到在第一个活动表条目中配置的 DNS 服务器。如果设备未收到来自此服务器的响应，它会将请求发送到在下一个活动表条目中配置的 DNS 服务器。

可能的值:

- ▶ **勾选**
DNS 客户端将请求发送到此 DNS 服务器。
前提条件:
 - 在 *Advanced > DNS > Global* 对话框中启用 DNS 客户端功能。
 - 在 *Configuration* 框的 *Configuration source* 下拉列表中选择值 *user*。
- ▶ **未勾选** (默认设置)
设备不会将请求发送到此 DNS 服务器。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

7.3.1.4 DNS Client Static Hosts

[Advanced > DNS > Client > Static Hosts]

此对话框允许用户指定最多 64 个主机名，每个主机名与一个 IP 地址链接。在收到解析 IP 地址中的主机名的请求后，设备会在此表格中搜索相应的条目。如果设备未找到相应的条目，则它会转发请求。

表格

Index

显示与表格条目相关的索引编号。

可能的值：

- ▶ 1..64

Name

指定主机名称。

可能的值：

- ▶ 带有 0..255 个字符的字母数字 ASCII 字符串

IP address

指定可用于访问主机的 IP 地址。

可能的值：

- ▶ 有效的 IPv4 地址

Active

激活/停用表格条目。

可能的值：

- ▶ 勾选
设备解析此条目的主机名的请求。
- ▶ 未勾选
在收到此主机名的请求之后，设备将请求发送到已配置的名称服务器之一进行解析。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

7.4 Industrial Protocols

[Advanced > Industrial Protocols]

该菜单包含以下对话框：

- ▶ IEC61850-MMS
- ▶ Modbus TCP
- ▶ EtherNet/IP

7.4.1 IEC61850-MMS

[Advanced > Industrial Protocols > IEC61850-MMS]

IEC61850-MMS 是 International Electrotechnical Commission (IEC) 发布的标准化工业通信协议。例如，自动交换设备在与电站设备通信时会使用此协议。

该面向数据包的协议定义了一种基于 TCP/IP 传输协议的统一通信语言。该协议使用制造报文规范 (MMS) 服务器来执行客户端服务器通信。该协议包括适用于 SCADA、智能电子装置 (IED) 和网络控制系统的功能。

提示： IEC61850/MMS 不提供任何身份验证机制。如果激活 IEC61850/MMS 的写访问，则每个能使用 TCP/IP 访问设备的客户端都能够更改设备的设置。这反过来又会导致设备的不正确配置和网络中可能出现的问题。

请在采取了额外措施（例如防火墙、VPN 等）的情况下激活写访问，以减少可能的未经授权的访问。

此对话框可用于指定以下 MMS 服务器设置：

- ▶ 激活/停用 MMS 服务器。
- ▶ 激活/停用对 MMS 服务器的写访问。
- ▶ MMS 服务器 TCP 端口。
- ▶ MMS 服务器会话的最大数量。

Operation

Operation

启用/禁用 *IEC61850-MMS* 服务器。

可能的值：

- ▶ *On*
IEC61850-MMS 服务器已启用。
- ▶ *Off* (默认设置)
IEC61850-MMS 服务器已禁用。
IEC61850 MIB 可持续访问。

Configuration

Write access

激活/停用对 MMS 服务器的写访问。

可能的值：

- ▶ *勾选*
对 MMS 服务器的写访问已激活。此设置允许您使用 IEC 61850 MMS 协议来更改设备配置。
- ▶ *未勾选* (默认设置)
对 MMS 服务器的写访问已停用。MMS 服务器可作为只读设备进行访问。

Technical key

指定 IED 名称。

IED 名称与系统名称无关。

可能的值：

- ▶ 带有 0..32 个字符的字母数字 ASCII 字符串
允许以下字符：
 - `0..9`
 - `a..z`
 - `A..Z` (默认设置: `KEY`)

要让 MMS 服务器使用 IED 名称，请点击 按钮并重新启动 MMS 服务器。然后，与已连接客户端的连接中断。

TCP port

指定用于访问 MMS 服务器的 TCP 端口。

可能的值：

- ▶ `1..65535` (默认设置: `102`)
例外：端口 `2222` 预留给内部功能。

提示： 在更改端口后，服务器会自动重新启动。在此过程中，设备会终止与服务器的开放连接。

Sessions (max.)

指定 MMS 服务器连接的最大数量。

可能的值：

- ▶ `1..15` (默认设置: `5`)

Information

Status

显示当前的 `IEC61850-MMS` 服务器状态。

可能的值：

- ▶ `unavailable`
- ▶ `starting`
- ▶ `running`
- ▶ `stopping`
- ▶ `halted`
- ▶ `error`

Active sessions

显示活动的 MMS 服务器连接的数量。

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

Download ICD file

将 ICD 文件复制到您的 PC。

7.4.2 Modbus TCP

[Advanced > Industrial Protocols > Modbus TCP]

Modbus TCP 是用于监测控制和数据采集 (SCADA) 系统集成的协议。*Modbus TCP* 是用于监控和控制可编程逻辑控制器 (PLC) 等工业自动化设备的供应商中立的协议。

此对话框可用于指定协议的参数。要监控和控制设备的参数，您需要使用人机界面 (HMI) 软件和存储器映射表。有关支持的对象和存储器映射，请参阅“配置”用户手册中的表格。

此对话框允许用户启用功能、激活写访问以及控制人机界面 (HMI) 用于轮询数据的 TCP 端口。您还可以指定允许同时打开的会话数量。

提示： 激活 *Modbus TCP* 写访问可能造成不可避免的安全风险，因为该协议不会对用户访问进行身份验证。

为帮助最大限度降低不可避免的安全风险，请在 *Device Security > Management Access* 对话框中指定 IP 地址范围。请仅输入在启用功能前为您的设备分配的 IP 地址。此外，在 *Diagnostics > Status Configuration > Security Status* 对话框的 *Global* 选项卡中，监控功能激活的默认设置为已激活。

Operation

Operation

启用/禁用设备中的 *Modbus TCP* 服务器。

可能的值：

- ▶ *On*
Modbus TCP 服务器已启用。
- ▶ *Off* (默认设置)
Modbus TCP 服务器已禁用。

Configuration

Write access

激活/停用对 *Modbus TCP* 参数的写访问。

提示： 激活 *Modbus TCP* 写访问可能造成不可避免的安全风险，因为该协议不会对用户访问进行身份验证。

可能的值：

- ▶ 勾选 (默认设置)
Modbus TCP 服务器的读/写访问已激活。这将允许您使用 *Modbus TCP* 协议更改设备配置。
- ▶ 未勾选
Modbus TCP 服务器的只读访问已激活。

TCP port

指定 *Modbus TCP* 服务器用于通信的 TCP 端口编号。

可能的值:

- ▶ <TCP 端口编号> (默认设置: 502)
不允许指定为 0。

Sessions (max.)

指定 *Modbus TCP* 服务器可以维持的最大并发会话数量。

可能的值:

- ▶ 1..5 (默认设置: 5)

按钮

“按钮” 页 16一节中提供了标准按钮的描述。

7.4.3 EtherNet/IP

[Advanced > Industrial Protocols > EtherNet/IP]

此对话框允许用户指定 *EtherNet/IP* 设置。您有以下选项：

- ▶ 启用/禁用设备中的 *EtherNet/IP* 功能。
- ▶ 指定专门转发 *EtherNet/IP* 数据包的 VLAN。
- ▶ 激活/停用 *EtherNet/IP* 协议的读/写功能。
- ▶ 从设备中下载电子数据表 (EDS) 文件。

Operation

Operation

启用/禁用设备中的 *EtherNet/IP* 功能。

可能的值：

- ▶ *On*
EtherNet/IP 功能已启用。
- ▶ *Off* (默认设置)
EtherNet/IP 功能已禁用。

VLAN Configuration

设置 VLAN 的优势：

- 减少 *EtherNet/IP* 数据包泛洪。设备在您分配的 VLAN 中转发 *EtherNet/IP* 数据包。
- 改进网络安全和隐私。

VLAN ID

指定设备在其中转发 *EtherNet/IP* 数据包的 VLAN。

可能的值：

- ▶ *mgmt* (默认设置)
设备在 VLAN 中转发 *EtherNet/IP* 数据包，可通过网络访问该 VLAN 的设备管理。在 *Basic Settings > Network > Global* 对话框的 *Management interface* 框的 *VLAN ID* 字段中指定此 VLAN。
- ▶ 1..4042
在下拉列表中，选择一个项目。设备在此 VLAN 中转发 *EtherNet/IP* 数据包。
前提条件：
 - 已在设备中设置 VLAN。
参见 *Switching > VLAN > Configuration* 对话框。
 - 设备用于转发 *EtherNet/IP* 数据包的端口是您分配的 VLAN 的成员，并且传输带有 VLAN 标签的数据包。
参见 *Switching > VLAN > Configuration* 对话框。
 - *IP Access Restriction* 功能已启用。
参见 *Device Security > Management Access > IP Access Restriction* 对话框。

Configuration

Write access

激活/停用 *EtherNet/IP* 协议的读/写功能。

可能的值:

- ▶ 勾选
EtherNet/IP 协议接受 set/get 请求。
- ▶ 未勾选 (默认设置)
EtherNet/IP 协议仅接受 get 请求。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

Download EDS file

将 zip 文件中的以下信息复制到您的 PC:

- ▶ 包含设备相关信息的电子数据表 (EDS)
- ▶ 设备图标

7.5 Digital I/O Module

[Advanced > Digital I/O Module]

数字输入允许用户捕获和转发来自数字传感器的信号。数字输出允许用户将从输入中继转发的信号应用于执行机构。24 VDC 输出电压允许用户操作指示灯等执行机构。

设备在整个网络中传输传感器信号，以激活适当的执行机构。该模块通过输入连接捕获信号并将其转发到输出。根据执行机构的位置，设备将信号转发到位于同一设备或不同设备中同一模块或不同模块上的输出。

当设备将数字输入端口映射到数字输出端口时，则建立 1:N 关系。设备将一个数字输入端口的数据流映射到任意数量的数字输出端口。

当设备将数字输出端口映射到数字输入端口时，则建立 1:1 关系。一个数字输出端口对一个数字输入端口的数据流进行映射。

该对话框包含以下选项卡：

▶ [I/O input]

[I/O input]

此选项卡允许用户：

- ▶ 全局激活/停用数字输入查询
- ▶ 配置设备查询数字输入值的时间间隔
- ▶ 激活/停用事件记录
- ▶ 激活/停用 SNMP 陷阱发送

Operation

Operation

启用/禁用来自数字输入的循环查询（IO 输入）。

可能的值：

- ▶ *On*
允许用户查询输入值。
- ▶ *Off*（默认设置）

Configuration

Refresh interval [ms]

指定设备查询来自数字输入的值的時間间隔（毫秒）。

可能的值：

- ▶ 1000..10000（默认设置：1000）

表格

Input ID

显示模块（x）的插槽编号以及应用于此条目的数字输入（i）的数量。

表示法：x.i

可能的值：

- ▶ x =0..7
0 值等于主单元（MU）。
- ▶ i =1..4

Value

指定数字输入级别。

可能的值：

- ▶ low
数字输入的输入电压为 0 V。
- ▶ high
数字输入的输入电压为 +24 VDC。
- ▶ not-available
数字输入的输入电压为除 0 V 或 +24 VDC 以外的其他值。验证模块是否存在且正确就位。

Log event

激活/停用日志文件记录。参见 *Diagnostics > Report > System Log* 对话框。

可能的值：

- ▶ 勾选
记录激活。
设备根据 *Configuration* 框 *Refresh interval [ms]* 字段中指定的时间间隔检查数字输入的状态。当数字输入发生改变时，设备会在 System Log 日志文件中记录一个条目。
- ▶ 未勾选（默认设置）
记录停用。

Send trap

激活/停用当设备检测到数字输入变化时发送 SNMP 陷阱。

设备根据 *Configuration* 框 *Refresh interval [ms]* 字段中指定的时间间隔检查数字输入的状态。

可能的值：

- ▶ **勾选**
SNMP 陷阱发送激活。
当设备检测到数字输入变化时，设备会发送一个 SNMP 陷阱。
- ▶ **未勾选**（默认设置）
SNMP 陷阱发送停用。

发送 SNMP 陷阱的前提条件是，用户在 *Diagnostics > Status Configuration > Alarms (Traps)* 中启用该功能并至少指定一个陷阱目的地。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

7.6 Command Line Interface

[Advanced > CLI]

此对话框允许用户使用命令行界面访问设备。

前提条件是：

- 在设备中，在 *Device Security > Management Access > Server* 对话框的 *SSH* 选项卡中启用 SSH 服务器。
- 在用户的工作站中，安装一个支持 SSH 的客户端应用程序，该应用程序会在用户的操作系统中注册一个以 `ssh://` 开头的 URL 处理程序。

按钮

“按钮” 页 16 一节中提供了标准按钮的描述。

Open SSH connection

打开支持 SSH 的客户端应用程序。

点击该按钮后，该 Web 应用程序将传递以 `ssh://` 开头的设备 URL 以及当前登录用户的用户名。

如果 Web 浏览器找到一个支持 SSH 的客户端应用程序，则该支持 SSH 的客户端会使用 SSH 协议与设备建立连接。

A 关键词目录

0-9	
802.1D/p mapping <802.1D/p 映射>	264
802.1X	113, 157
A	
Access control <访问控制>	157
Access control lists <访问控制列表>	210
Access restriction <访问限制>	137
ACL	210
Address conflict detection <地址冲突检测>	354
Aging time <老化时间>	219, 358
Alarms <警报>	349
ARP	354
ARP table <ARP 表>	358
ARP 检查	201
Authentication history <身份验证历史记录>	171
B	
Bridge <网桥>	285
C	
CLI	142
Community names <团体名称>	145
Configuration profile <配置概要文件>	15, 37
ConneXium Network Manager	11, 126
Context menu <上下文菜单>	15
Counter reset <计数器复位>	65
D	
Daylight saving time <夏令时>	70
Device software backup <设备软件备份>	34
Device status <设备状态>	19, 330
DHCP L2 relay <DHCP 第二层中继>	419
DHCP 服务器	425
DHCP 窥探	188
DHCPv6 第二层中继	419
DNS	434
DNS client <SNTP 客户端>	435
DNS 缓存	435
DoS	184
DSCP	266
E	
EAPOL	169
Egress rate limiter <出口速率限制器>	221
Encryption <加密>	37
ENVM	35, 37, 42, 48, 331, 337, 344, 415
Ethernet Switch Configurator	24, 338, 418
EtherNet/IP	339, 446
EtherNet/IP 的 VLAN	446
EtherNet/IP 的读/写功能	446
EtherNet/IP, VLAN	446
EtherNet/IP, 下载 EDS	446
EtherNet/IP, 读/写功能	446
Event severity <事件严重程度>	365, 412
External memory <外部存储器>	35, 37, 42, 48, 415

F	
FDB	224
Filter MAC addresses <筛选 MAC 地址>	224
Fingerprint <指纹>	130, 134
Flash memory <闪存>	35, 353
Forwarding database <转发数据库>	224
G	
GARP	256
GMRP	257
GVRP	259
H	
Hardware clock <硬件时钟>	69
Hardware state <硬件状态>	353
HIPER 环网	282
Host key <主机密钥>	131
HTML	352, 417
HTTP	132
HTTP server <HTTP 服务器>	336
HTTPS	133
I	
IAS	113, 173
IEC61850-MMS	338, 441
IEEE 802.1X	113
IGMP 窥探	225
Ingress filtering <入口筛选>	274
Ingress rate limiter <入口速率限制器>	221
IO 输入	448
IP address conflict detection <IP 地址冲突检测>	354
IP DSCP mapping <IP DSCP 映射>	266
IP 源保护	197
IP 访问限制	137
IPv4 rule <IPv4 规则>	211
L	
L2 relay <第二层中继>	419
LDAP	113
LLDP	395
Load/save <加载/保存>	37
Log file <日志文件>	65, 417
Loops <环路>	284
M	
MAC address table <MAC 地址表>	224
MAC flood <MAC 泛洪>	151
MAC rule <MAC 规则>	214
MAC spoof <MAC 欺骗>	151
Management access <管理访问>	24, 29, 137
Media redundancy protocol <介质冗余协议>	278
MMRP	249
MMS	441
Modbus TCP	339, 444
MRP	278
MRP-IEEE	247
MVRP	253

N	
Network load <网络负载>	56
NVM	14, 15, 22, 35, 42
P	
Password <密码>	108, 335
Password length <密码长度>	108, 335
PoE	58
Port clients <端口客户端>	167
Port configuration <端口配置>	161, 262
Port mirroring <端口镜像>	393
Port monitor <端口监控器>	389
Port priority <端口优先级>	262
Port security <端口安全>	151
Port VLAN <端口 VLAN>	273
Port-based access control <基于端口的访问控制>	157
Power supply <电源>	21, 332, 345
Pre-Login banner <预登录横幅>	146
Priority queue <优先级队列>	261
R	
RADIUS	113, 174
RAM	41
RAM test <RAM 测试>	359
RCP	325
Reboot <重启>	65
Redundant coupling protocol <冗余耦合协议>	325
Relay <中继>	419
Request interval <请求间隔>	75
Ring structure <环形结构>	278
RNC	319
Root bridge <根网桥>	285
RSTP	284, 285
S	
Secure Shell	128
Settings <设置>	37
SFP module <SFP 模块>	374
Signal contact <信号触点>	20, 340
SNMP server <SNMP 服务器>	126, 337
SNMP 陷阱	54, 59, 61, 153, 285, 291, 306, 330, 334, 343, 349, 356, 381, 449
SNMPv1/v2	145
SNTP	73
SNTP client <SNTP 客户端>	74
SNTP server <SNTP 服务器>	78
Software backup <软件备份>	34
Software update <软件更新>	34
Spanning tree protocol <生成树协议>	284
SSH server <SSH 服务器>	128
Switch dump <交换机转存数据>	412
System information <系统信息>	352

T	
Telnet server <Telnet 服务器>	127, 336
Temperature <温度>	21, 331, 344
Threshold values network load <网络负载阈值>	221
Trap destination <陷阱目标>	349
Trust mode <信任模式>	262
TSN 配置	241
TSN 门控制列表	244, 246
U	
USB 网络接口	32
Utilization <利用率>	56
V	
Virtual local area network <虚拟局域网>	269
VLAN	24, 269, 405
VLAN configuration <VLAN 配置>	271
VLAN ports <VLAN 端口>	273
W	
Web server <网络服务器>	132, 133
Z	
ZIP archive <ZIP 文档>	412
?	
下载 EtherNet/IP 的 EDS	446
严	
严重程度	365, 412
中	
串行接口	337
以	
以太网供电	58
保	
保护	301
利	
制造报文规范	441
动	
动态 ARP 检查	201
双	
双绞线	376
命	
命令行界面	142
地	
域名系统	434
子	
子环网	314

安	
安全状态	19, 334
实	
审计跟踪	418
密	
对时间敏感的网络	241
带	
带外管理端口	32
拓	
拓扑识别	400
持久记录	414
故	
数字输入端	448
流	
流量控制	219
源	
源保护	197
环	
环网/网络耦合	319
环路保护	345
用	
用户管理	107
电	
电子邮件通知	360
电缆诊断	376
登	
登录横幅	143, 146
目	
看门狗	37, 41
端	
端口统计	169
简	
管理 VLAN	24
系	
系统日志	369, 417
系统时间	69
系统监控器	359
自	
自动禁用	152, 190, 204, 206, 287, 294, 381, 382, 389, 404
自检	359
菜单	15

设	
设备软件	34
访	
证书	20, 47, 117, 134, 135, 339, 362, 369
路	
身份验证列表	113
边	
边界时钟	83
退	
透明时钟	91
通	
速率限制器	221
重	
重复地址检测	30
链路备份	310
链路聚合	303
队	
队列	261
队列管理	268
陷	
陷阱	54, 59, 61, 153, 285, 291, 306, 330, 334, 343, 349, 356, 381, 449
集成身份验证服务器	113, 173

