用户手册

Allen-Bradley

Stratix 5700 以太网管理型交换机

重要用户须知

在安装、配置、操作或维护设备之前，请仔细阅读本文档及“其它资源”部分列出的文档，了解设备的安装、配置和操作信息。用户需要了解安装和接线指南以及所有适用规范、法律和标准的相关要求。

安装、调节、投入使用、操作、装配、拆卸和维护等活动均要求由经过适当培训的人员遵照适用法规执行。

如果设备的使用方式与制造商指定的方式不同，则设备提供的保护功能可能会受到影响。

对于由于使用或应用此设备而导致的任何直接或间接的损害，罗克韦尔自动化公司在任何情况下都不承担任何责任和义务。

本手册中的示例和图表仅供说明之用。由于任何特定的安装都存在很多可变因素和要求，罗克韦尔自动化公司对于依据这些示例和图表所进行的实际应用不承担任何责任和义务。

对于因使用本手册中所述信息、电路、设备或软件而引起的专利问题，罗克韦尔自动化不承担任何责任。

未经罗克韦尔自动化公司的书面许可，禁止复制本手册的全部或部分内容。

在本手册中，在必要时我们使用注意事项来提醒您需要注意的安全问题。

	**警告：指明在危险环境下可能导致爆炸进而造成人身伤害或死亡、财产损坏或经济损失的行为或情况的信息。**
	**注意：指明可能造成人身伤害或死亡、财产损坏或经济损失的行为或情况的信息。“注意”可以帮助您识别危险、避免危险并了解后果。**
重要信息	**指明成功应用和理解产品的关键信息。**

标签可能位于设备上或设备内，可提供特定警示。

	**触电危险：标签可能位于设备上或设备内（例如驱动器或电机），提醒人们此处可能存在危险的高压。**
	**灼伤危险：标签可能位于设备上或设备内（例如驱动器或电机），提醒人们表面可能存在危险的高温。**
	**弧闪危险：位于设备（例如，电机控制中心）表面或内部的标签，提醒人们可能出现弧闪。弧闪将造成严重的人身伤害或死亡。穿戴适当的个人防护设备 (PPE)。遵守安全工作规范和个人防护设备 (PPE) 的所有法规要求。**

本手册包含一些新增的和更新的信息。

新信息和更新信息

下表包含了本版本所做的变更。

主题	页码
更新了设备管理器硬件和软件要求	23, 47
新增了“快速设置”窗口	49, 50
新增了路由启用过程	82
新增了设备管理器 Web 界面	85…141

注：

目录

第 3 章

交换机软件功能

第 4 章

通过设备管理器 Web 界面管理交换机

第 5 章

通过 Studio 5000 环境管理交换机

第 6 章

处理交换机故障

附录 A

模块定义的数据类型

附录 B

CIP 数据的端口分配

附录 C

电缆和连接器

附录 D

变更记录

索引

注：

本出版物介绍了配置和管理 Stratix 5700™ 管理型以太网交换机的嵌入式软件功能和工具。此外，本出版物还提供了故障处理信息，可帮助解决基本的交换机和网络问题。

如果要配置和监视 Stratix 5700 以太网管理型交换机，请使用本手册。本手册假定您已了解如下内容：

- 局域网 (LAN) 交换机基础知识
- 以太网协议和局域网的概念和术语

Studio 5000 环境

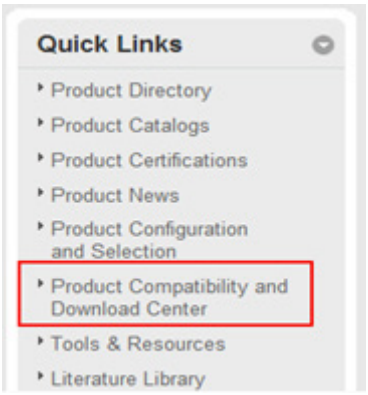
Studio 5000™ 工程和设计环境将工程和设计元素融合到一个通用环境中。Studio 5000 环境中的第一个元素是 Logix 设计器应用程序。Logix 设计器应用程序是 RSLogix™ 5000 软件的换代产品，将继续作为 Logix 5000™ 控制器的编程产品，用于离散、过程、批次、运动控制、安全和基于变频器的各种解决方案。

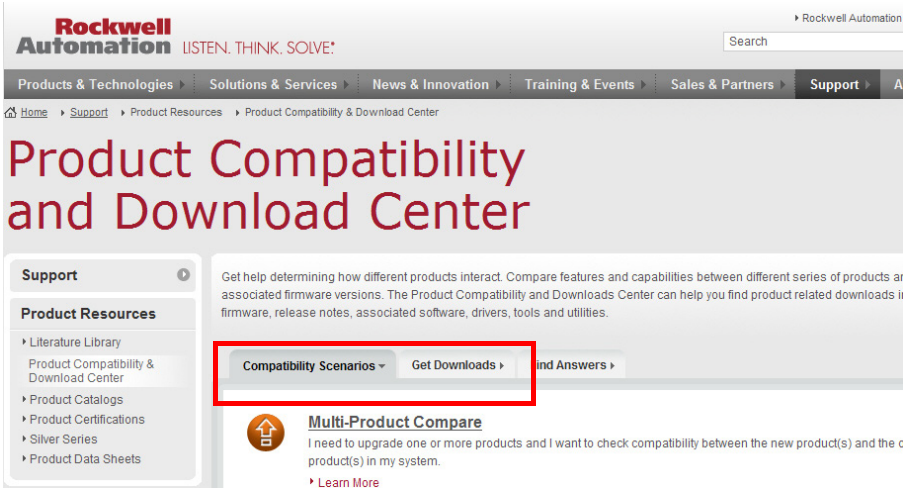
Studio5000 环境是未来罗克韦尔自动化工程设计工具和功能的基础。它是设计工程师开发控制系统全部元件所需的一站式软件。

访问产品版本说明

可从“产品兼容性和下载中心”在线获取产品版本说明。

1. 从 http://www.ab.com 上的“快速链接”列表中，选择 Product Compatibility and Download Center （产品兼容性和下载中心）。





2. 在 Compatibility Scenarios 或 Get Downloads 选项卡中，搜索并选择您的产品。

3. 单击下载图标  访问产品版本说明。

其它资源

这些文档包含有关罗克韦尔自动化相关产品的附加信息。

资源	描述
Stratix Ethernet Managed Switches Technical Data（出版物 1783-TD001）	提供交换机的技术参数信息。
Ethernet Design Considerations Reference Manual（出版物 ENET-RM002）	提供实现基于 EtherNet/IP 平台的系统的相关信息。
设备管理器 Web 界面在线帮助（随交换机一起提供）	提供有关配置和使用交换机的上下文相关信息，包括系统消息。
Industrial Automation Wiring and Grounding Guidelines（出版物 1770-4.1）	提供安装罗克韦尔自动化工业系统的通用准则。
产品认证网站，http://www.ab.com	提供符合性声明、认证和其它认证的详细信息。

可访问 http:/www.rockwellautomation.com/literature/ 查看或下载这些出版物。如需订购技术文档的纸印本，请联系当地的 Allen-Bradley 分销商或罗克韦尔自动化销售代表。

有关附加软件功能或进一步配置这些功能的信息，请参见 http://www.Cisco.com 上的 Cisco 出版物:

- 《Cisco IE-2000 命令行参考手册》(Cisco IE-2000 Command Line Reference Manual)
- 《Cisco IE-2000 软件配置指南》(Cisco IE-2000 Software Configuration Guide)
- 《Cisco IE-2000 交换机系统消息指南》(Cisco IE-2000 Switch System Message Guide)

注：

关于交换机

Stratix 5700 管理型以太网交换机提供了一种适用于恶劣环境的安全的交换基础设施。这些交换机可连接至网络设备，如服务器、路由器和其它交换机。在工业环境中，可连接工业以太网通信设备，包括可编程逻辑控制器 (PLC)、人机界面 (HMI)、驱动器、传感器以及 IO。

交换机目录号

这些 Stratix 5700 交换机具有精简版固件或完整版固件。

目录号	描述
1783-BMS06SL	6 端口（4 个以太网端口；2 个 SFP 插槽）管理型交换机；精简版固件
1783-BMS06SA	6 端口（4 个以太网端口；2 个 SFP 插槽）管理型交换机；完整版固件
1783-BMS06TL	6 端口（6 个以太网端口）管理型交换机；精简版固件
1783-BMS06TA	6 端口（6 个以太网端口）管理型交换机；完整版固件
1783-BMS06SGL	6 端口（4 个以太网端口；2 个 SFP 千兆插槽）管理型交换机；精简版固件
1783-BMS06SGA	6 端口（4 个以太网端口；2 个 SFP 千兆插槽）管理型交换机；完整版固件
1783-BMS06TGL	6 端口（4 个以太网端口；2 个千兆端口）管理型交换机；完整版固件
1783-BMS06TGA	6 端口（4 个以太网端口；2 个千兆端口）管理型交换机；完整版固件
1783-BMS10CL	10 端口（8 个以太网端口；2 个组合端口）管理型交换机；精简版固件
1783-BMS10CA	10 端口（8 个以太网端口；2 个组合端口）管理型交换机；完整版固件
1783-BMS10CGL	10 端口（8 个以太网端口；2 个组合千兆端口）管理型交换机；精简版固件
1783-BMS10CGA	10 端口（8 个以太网端口；2 个组合千兆端口）管理型交换机；完整版固件
1783-BMS10CGN	10 端口（8 个以太网端口；2 个组合千兆端口）管理型交换机；完整版固件；网络地址转换 (NAT)
1783-BMS10CGP	10 端口（8 个以太网端口；2 个组合千兆端口）管理型交换机；完整版固件；精密时间协议 (PTP)
1783-BMS12T4E2CGNK	18 端口（12 个以太网端口；4 个 PoE/PoE+ 端口；2 个组合千兆端口）管理型交换机；完整版固件；NAT；涂层防护
1783-BMS12T4E2CGP	18 端口（12 个以太网端口；4 个 PoE/PoE+ 端口；2 个组合千兆端口）管理型交换机；完整版固件，PTP
1783-BMS12T4E2CGL	18 端口（12 个以太网端口；4 个 PoE/PoE+ 端口；2 个组合千兆端口）管理型交换机；精简版固件
1783-BMS20CL	20 端口（16 个以太网端口；2 个 SFP 插槽；2 个组合端口）管理型交换机；精简版固件
1783-BMS20CA	20 端口（16 个以太网端口；2 个 SFP 插槽；2 个组合端口）管理型交换机；完整版固件
1783-BMS20CGL	20 端口（16 个以太网端口；2 个 SFP 插槽；2 个组合千兆端口）管理型交换机；精简版固件
1783-BMS20CGN	20 端口（16 个以太网端口；2 个 SFP 插槽；2 个组合千兆端口）管理型交换机；完整版固件；NAT
1783-BMS20CGP	20 端口（16 个以太网端口；2 个 SFP 插槽；2 个组合千兆端口）管理型交换机；完整版固件；PTP
1783-BMS20CGPK	20 端口（16 个以太网端口；2 个 SFP 插槽；2 个组合千兆端口）管理型交换机；完整版固件；PTP；涂层防护
SFP 模块	
1783-SFP100FX	100BASE-FX 多模光纤收发器
1783-SFP1GSX	1000BASE-SX 多模光纤收发器
1783-SFP100LX	100BASE-LX 单模光纤收发器
1783-SFP1GLX	1000BASE-LX 单模光纤收发器
电源	
1606-XL 系列（推荐） 1606-XLP 系列（推荐） 或同等系列	2 类，24V DC 输出电源
SD 卡	
1784-SD1	1 GB 工业 SD 卡

交换机软件功能

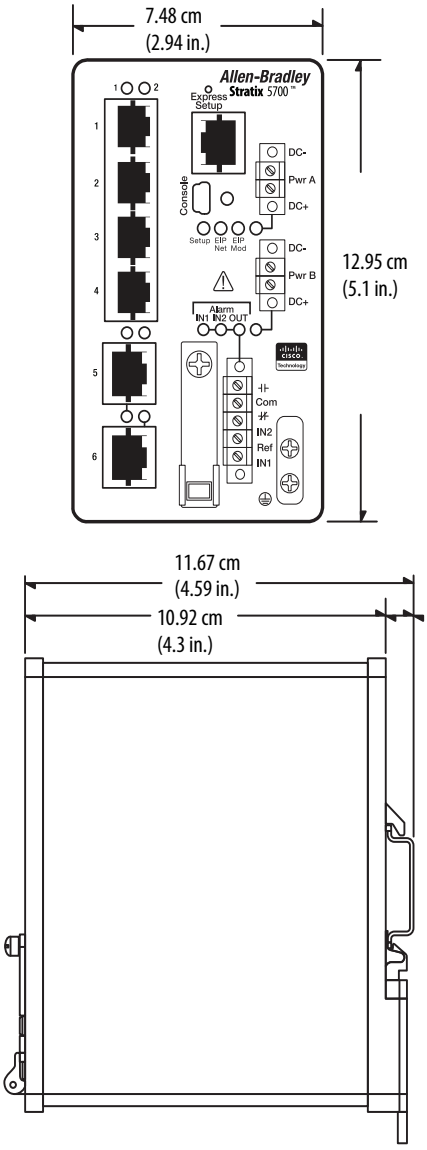
Stratix 5700 交换机具有以下软件功能。

功能	精简版固件	完整版固件
CIP Sync (IEEE 1588)		独立选项
弹性以太网协议 (REP)	•	•
FlexLink		•
服务质量 (QoS)		•
STP、RSTP、MST（实例）	64	128
IGMP 监听及查询器	•	•
具有中继功能的 VLAN	64	255
EtherChannel（链路聚合）		•
端口阈值（风暴控制和流量定形）		•
IPv6 支持		•
访问控制列表 (ACL)		•
静态和 interVLAN 路由		•
CIP 端口控制和故障检测	•	•
MAC ID 端口安全性		•
IEEE 802.1x 安全性		•
TACACS+、RADIUS 认证	•	•
加密（SSH、SNMPv3、HTTPS）		单独的 IOS 固件具有单独的目录项
端口镜像	•	•
Syslog	•	•
断线检测	•	•
IP 地址冲突检测		•
SNMP	•	•
智能端口	•	•
逐端口执行 DHCP	•	•
命令行接口 (CLI)	•	•
兼容思科工具. 思科网络助理 (CNA)；CiscoWorks	•	•
EtherNet/IP (CIP) 接口	•	•
网络地址转换 (NAT)		独立选项

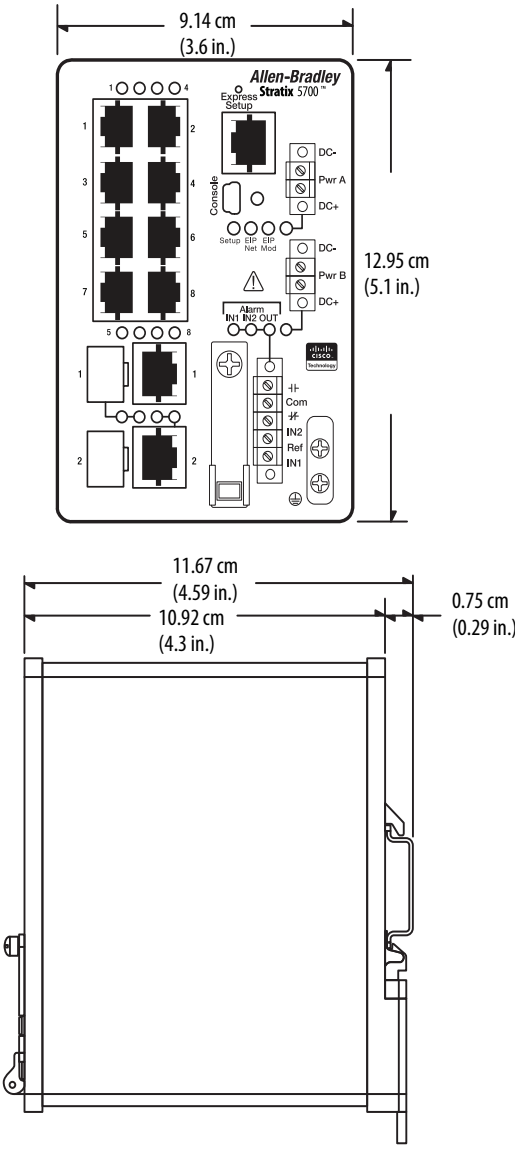
交换机尺寸

下列图示为代表性 Stratix 5700 交换机。实际面板根据目录号的不同而有所不同。

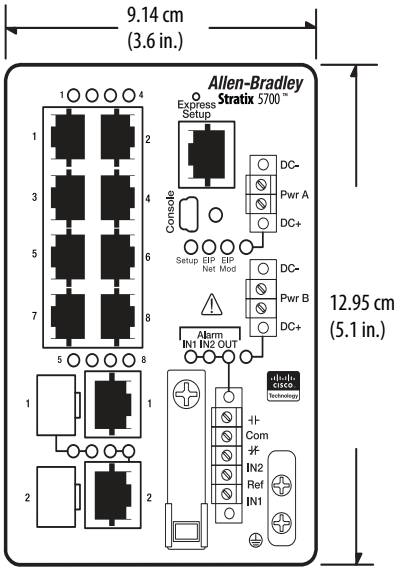
6 端口交换机
1783-BMS06SL、1783-BMS06SA、1783-BMS06TL、1783-BMS06TA、1783-BMS06SGL、1783-BMS06SGA、1783-BMS06TGL、1783-BMS06TGA



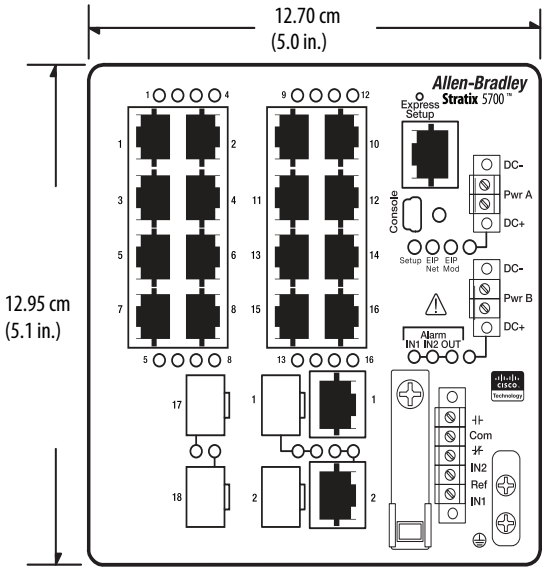
10 端口交换机
1783-BMS10CL、1783-BMS10CA、1783-BMS10CGL、1783-BMS10CGA

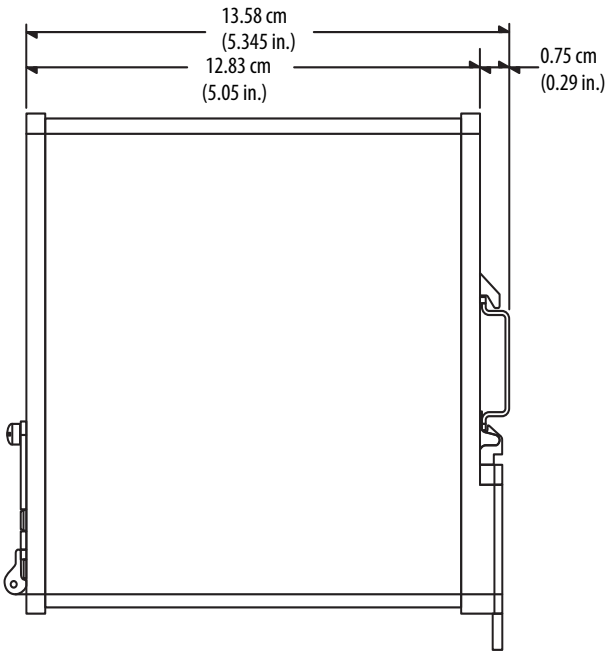


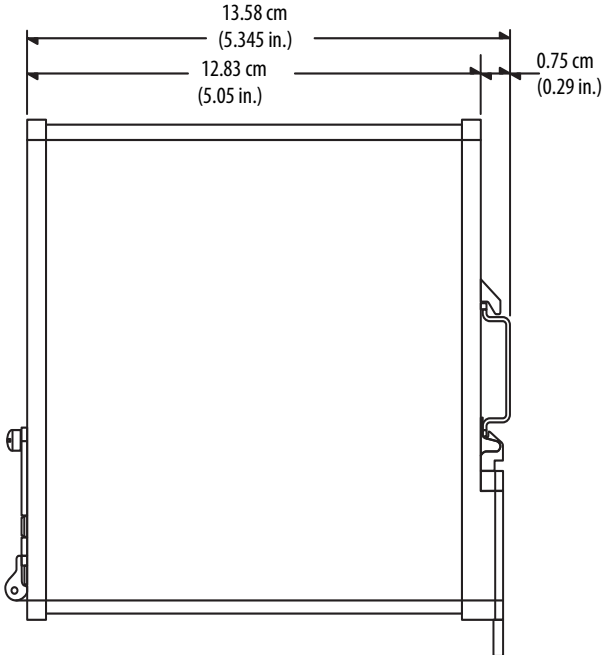
10端口交换机
1783-BMS10CGP、1783-BMS10CGN



18和20端口交换机
1783-BMS12T4E2CGNK、1783-BMS12T4E2CGP、1783-BMS12T4E2CGL、1783-BMS20CL、1783-BMS20CA、1783-BMS20CGL、1783-BMS20CGP、1783-BMS20CGN、1783-BMS20CGPK

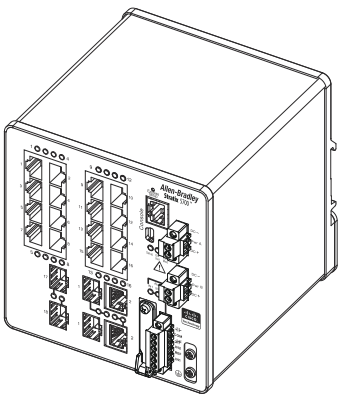






交换机前面板

交换机前面板包括端口、状态指示灯、电源和继电器连接器。



交换机硬件功能

Stratix 5700 交换机具有以下硬件功能。

功能	描述
电源和继电器连接器	直流电源和报警信号通过前面板上的两个连接器连接到交换机上。其中一个连接器提供主直流电源 (Pwr A)，另一个 (Pwr B) 提供辅助电源。两个连接器在物理结构上完全相同且都在前面板的右侧。 6 针报警连接器为一个输出报警继电器和两个输入报警提供接口。输出报警可根据环境、电源、端口状态等报警条件激活，并可配置为通过常开或常闭（C 型）触点来指示报警。通过 CLI，您可将输出报警配置为常励磁或非常励磁。输入报警终端可以用来激活交换机外部任何情况的报警。 交换机可使用单电源或双电源供电。存在两个电源时，交换机会从电压更大的直流电源获取电力。如果其中一个电源失效，另外一个将继续为交换机供电。
控制台端口	如需对交换机进行配置、监视和管理，可使用此控制台端口及 RJ45 转 DB-9 适配器电缆或迷你 USB 电缆（交换机未附带这两种电缆）将交换机连接到计算机。可从 http://www.rockwellautomation.com 固件下载区下载迷你 USB 驱动程序。
两用上行端口	某些型号的交换机上具有两个两用上行端口，其中的每一个都可配置为 RJ45（电口）或 SFP（光口）介质类型。在每个两用端口上，一次仅可使用其中一种连接。如果同时连接了两个端口，则优先使用 SFP 模块端口。 可以将 RJ45 电口设置成以 10、100 或 1000 Mbps（不是所有带组合端口的模块都支持 1000 Mbps）速度，全双工或半双工模式运行。用户可将其配置成固定的 10、100 或 1000 Mbps（千兆）以太网端口，同时也可以配置双工设置。 可使用经认可的千兆（或 100 Mbps）以太网 SFP 模块来建立与其它交换机的光纤连接。这些收发器模块可现场更换，并在插入 SFP 模块插槽后即可作为上行接口。用户需使用带 LC 连接器的光缆连接到光纤 SFP 模块。这些端口仅在全双工模式下运行。
10/100 端口	可以将 10/100 端口设置成以 10 或 100 Mbps 速度，全双工或半双工模式运行。也可按照 IEEE 802.3-2002 将这些端口设置为自动协商速度与双工设置。（默认设置为自动协商。） 设置为自动协商后，端口会检测所连接设备的速度和双工设置。如果相连设备也支持自动协商功能，那么该交换机端口会协商确定最佳连接（即两个设备都支持的最快线路速度，并且只要相连设备支持就会采用全双工传输）并对自身进行相应配置。在所有情况下，相连接设备都必须在距离交换机 100 m (328 ft) 的范围内。
PoE 端口	某些型号有 PoE 端口，这些端口可以配置为 PoE (IEEE 802.3af) 或 PoE+（IEEE 802.3at 类型 2）： • 对于 PoE 配置，PoE 端口需要 2 线 48V DC 外部输入电源。 • 对于 PoE+ 配置，PoE 端口需要 2 线 54V DC 外部输入电源。
自动 MDIX	将交换机连接到工作站、服务器和路由器时，通常使用直通电缆。不过，交换机默认情况下会启用自动线序交叉（自动 MDIX）功能，并将端口自动重新配置为使用直通电缆或交叉电缆类型。 自动 MDIX 功能在默认情况下处于启用状态。启用自动 MDIX 后，交换机会检测以太网连接所需的铜缆类型（直通或交叉）并相应配置接口。 用户可使用命令行接口 (CLI) 禁用自动 MDIX 功能。更多信息，请参见在线帮助。

配置文件

交换机配置文件 (config.txt) 为 ASCII 可读格式。此配置文件保存在非易失性内存中，并在交换机上电后作为运行配置读入交换机的随机存取存储器 (RAM) 中。更改配置后，变更将在运行配置中立即生效。设备管理器 Web 界面和 Logix 设计器应用程序的用户自定义配置文件 (AOP) 会将变更自动写入闪存，留存供下一个上电循环使用。通过 CLI 所做的任何变更都必须手动写入闪存，留存供下一个上电循环使用。

SD 卡

除了板载闪存外，交换机还配备了用于可选安全数字(SD)卡的插槽。SD 卡可以在发生故障时替代板载闪存来轻松恢复交换机配置，也可以在部署新网络时轻松复制配置。

如果在交换机上安装 SD 卡，则交换机将启动 SD 卡上的 IOS 和配置。如果未安装 SD 卡，或卡中不存在文件，交换机将读取板载启动参数并从板载闪存上的指定 IOS 映像重启。

您必须使用罗克韦尔自动化随交换机提供的 SD 卡（目录号为 1784-SD1）。

注意：如果在本产品中使用非罗克韦尔 SD 卡，罗克韦尔自动化将保留拒绝支持的权利。

如果您从 SD 卡启动，之后在交换机运行时移除 SD 卡，将发生以下情况：

- 设备管理器 Web 界面将无法访问。
- 使用 CLI 或 AOP 所做的变更会生效，但在交换机重启后不会保存。
- 如果将 SD 卡重新插入插槽，变更不会保存到卡中，除非执行新的变更。随后，整个配置将保存到卡中。

注意：SD 卡通常具有一个物理只读锁定开关。如果此开关处于打开状态，那么交换机可以从 SD 卡成功启动。使用 CLI、AOP 或设备管理器 Web 界面所做的变更会生效，但在交换机重启后不会保存。

SD 卡同步

您可以利用设备管理器 Web 界面或 Logix 设计器应用程序的 AOP 来同步 SD 卡获取配置和 IOS 更新。配置同步过程会在选定源和选择目标之间同步 config.text 和 vlan.dat。

IOS 映像同步过程会在选定源和选择目标之间同步现有的可启动 IOS 映像。完成此过程大约需要 5 分钟。

如果 SD 卡中还存在备用配置等其他文件，它们不会被同步。

注意：同步过程中，请注意您的启动源，以便了解同步的方向。设备管理器将在 SD Card Sync 选项卡中提供这一信息。如果同步的方向错误，您可以覆盖所需的配置。

交换机内存分配

下表列出了交换机默认内存分配的详细信息。

根据交换机在网络中的使用方法，您可以利用 SDM 模版配置交换机中的系统资源以优化对特定功能的支持。您可以选择某一模版为某些功能提供系统最大使用率；例如，使用默认模版平衡资源，使用访问模版获取 ACL 的最大使用率。为了给不同用途分配硬件资源，交换机 SDM 模版将系统资源划分优先级以优化对某些功能的支持。

提供以下 SDM 模版：

- 默认
- 路由
- 双 IPv4 和 IPv6

如果您启用静态路由或拥有 180 个以上的 IGMP 组或多播路由，请使用路由模版。如果您正在使用 IPv6，则请使用双 IPv4 和 IPv6 模版。

您可以为 IP 版本 4 (IPv4) 选择 SDM 模版以优化这些功能。

功能	内存分配		
	默认	路由	双 IPv4 和 IPv6
单播 MAC 地址	8 K	4 K	7.5 K
IPv4 IGMP 组 + 多播路由	0.25 K	0.25 K	0.25 K
IPv4 单播路由	0	4.25 K	0
IPv6 多播组	0	0	0.375 K
直连 IPv4 主机	0	4 K	
直连 IPv6 地址	0	0	o
间接 IPv4 路由	0	0.25 K	
间接 IPv6 路由	0	0	0
基于 IPv4 策略的路由 ACE	0	0	
IPv4/MAC QoS ACE	0.375 K	0.375 K	0.375 K
IPv4/MAC 安全性 ACE	0.375 K	0.375 K	0.375 K
基于 IPv6 策略的路由 ACE	0	0	0
IPv6 QOS ACE	0	0	0
IPv6 安全性 ACE	0	0	0.125 K

设备管理器 Web 界面

可以使用设备管理器 Web 界面配置和监视交换机，从而实现对交换机的管理。设备管理器 Web 界面是一个图形化设备管理工具，可用于对各交换机执行配置、监视和故障处理。

设备管理器 Web 界面可显示交换机配置和性能的实时信息。它通过智能端口等功能实现了交换机及其端口的快速设置，简化了配置工作。它还采用颜色编码的图形显示画面，例如前面板视图、图示和动态指示灯，简化了监视工作。同时还提供了报警工具，帮助用户识别并解决网络故障。

您可以通过 Microsoft Internet Explorer 等 Web 浏览器在网络中的任何位置显示设备管理器 Web 界面。

硬件要求

属性	要求
处理器速度	1 GHz 或更快（32 位或 64 位）
RAM	1 GB（32 位）或 2 GB（64 位）
可用硬盘空间	16 GB（32 位）或 20 GB（64 位）
颜色数	256
分辨率	1024 x 768
字号	小

软件要求

Web 浏览器	版本
Microsoft Internet Explorer	具有 JavaScript 功能的 9.0、10.0 或 11.0
Mozilla Firefox	具有 JavaScript 功能的 25 或 26

在开始会话时，设备管理器 Web 界面将检查浏览器版本，以确保支持该浏览器。

提示 **要使设备管理器 Web 界面正常运行，禁用浏览器软件中的所有弹出窗口阻止程序或代理设置，并禁用计算机或笔记本电脑中运行的所有无线客户端。**

Studio 5000 环境

可以在 Studio 5000 环境下使用 Logix 设计器应用程序管理交换机。Logix 设计器应用程序符合 IEC 61131-3 标准，它可以提供继电器梯形图、结构化文本、功能块图和顺序功能图编辑器，用户开发应用程序使用。

硬件要求

属性	要求
处理器速度	最低 Pentium II 450 MHz 推荐使用 Pentium III 733 MHz（或更高配置）
RAM	最小 128 MB 推荐使用 256 MB
可用硬盘空间	3 GB
光盘驱动器	DVD
视频要求	256 色 VGA 图形适配器 最低分辨率 800 x 600（推荐真彩 1024 x 768）
分辨率	最低分辨率 800 x 600（推荐真彩 1024 x 768）

思科网络助理

思科网络助理是一个 Web 界面，可从 Cisco网站下载到计算机上运行。它提供的高级选项可用于配置和监视多个设备，包括交换机、交换机群集、交换机堆叠、路由器和接入点。

要使用本软件，请按以下步骤操作。

1. 访问 http://www.cisco.com/go/NetworkAssistant。
   您必须是注册用户，但无需其它访问权限。
2. 找到网络助理安装程序。
3. 下载网络助理安装程序，然后运行该程序。

   如果浏览器允许，可从 Web 直接运行该程序。
4. 运行安装程序时，请按屏幕显示的说明操作。
5. 在最终的面板中，单击 Finish 完成网络助理的安装。
6. 更多信息，请参见网络助理在线帮助。

命令行接口

可将个人计算机直接连接到交换机控制台端口并使用命令行接口 (CLI) 来管理交换机，也可以使用 Telnet 通过网络实现交换机管理。

要通过控制台端口访问 CLI，按如下步骤操作。

1. 使用下列方法之一连接到控制台端口：
   - 使用 RJ45 转 DB-9 适配器电缆 （交换机未附带）连接到个人计算机的标准 9 针串口上。
   - 使用标准迷你 USB 电缆 （交换机未附带）连接到个人计算机上的迷你 USB 端口。
   - 如果您正在使用 USB 电缆，请从 http://www.rockwellautomation.com 为您的 Microsoft Windows 计算机下载驱动程序。
2. 将电缆的另一端连接到交换机上的控制台端口。

警告：控制台端口仅为了方便临时本地编程使用，不适合永久连接。如果在带电情况下连接或断开该模块或电缆另一端上所连编程设备的控制台电缆，将会产生电弧。如果在危险场所安装，将可能导致爆炸。因此，在操作前需确保已断开电源且安装区域不存在危险。

3. 在个人计算机上启动终端仿真程序。
4. 将个人计算机终端仿真软件配置为 9600 bps、8 个数据位、无奇偶校验、1 个停止位以及无流量控制。

注：

交换机安装

安装指南

注意：该设备仅适合在 I 类 2 分区 A、 B、 C、 D 组的危险场所或非危险场所使用。

使用寿命结束后，应将本设备与未分类的城市垃圾分离开，单独进行收集。

确定安置交换机的位置时，请遵循以下准则：

- 交换机周围的气流能自由流通。为防止交换机过热，应遵守以下最小间隙要求：
  - 顶部和底部：50.8 mm (2.0 in.)
  - 侧面：50.8 mm (2.0 in.)
  - 正面：50.8 mm (2.0 in.)
- 对于 10/100 端口和 10/100/1000 端口，交换机至连接设备的电缆长度不能超过 100 m (328 ft)。
- 交换机与其所连设备之间的光纤电缆长度不能超过附录C中规定的距离。
- 为实现最佳抗扰性，必须在下列交换机的 RJ45 上行端口（Gi1/1 和 Gi1/2）上使用屏蔽电缆：
  - 1783-BMS06TGL
  - 1783-BMS06TGA
  - 1783-BMS10CGL
  - 1783-BMS10CGA
  - 1783-BMS10CGN
  - 1783-BMS10CGP
  - 1783-BMS12T4E2CGNK
  - 1783-BMS12T4E2CGP
  - 1783-BMS12T4E2CGL
  - 1783-BMS20CGL
  - 1783-BMS20CGN
  - 1783-BMS20CGP
  - 1783-BMS20CGPK
- 设备周围温度不要超过 60 °C (140 °F)。

重要信息　**将交换机安装到工业机壳中后，机壳内的温度将比机壳外的正常室温高。**

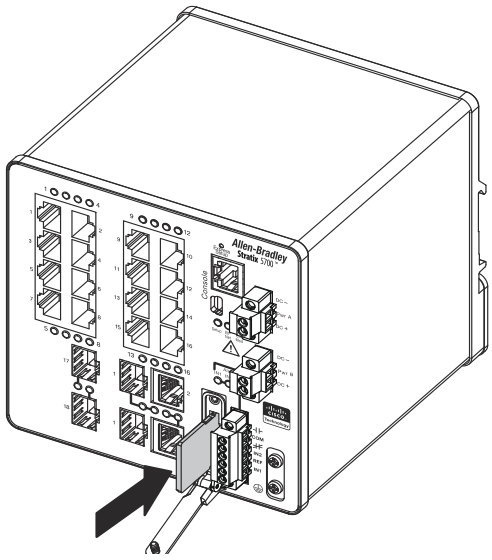
机壳内的温度不能超过交换机的最高环境机壳温度 140 °F (60 °C)。

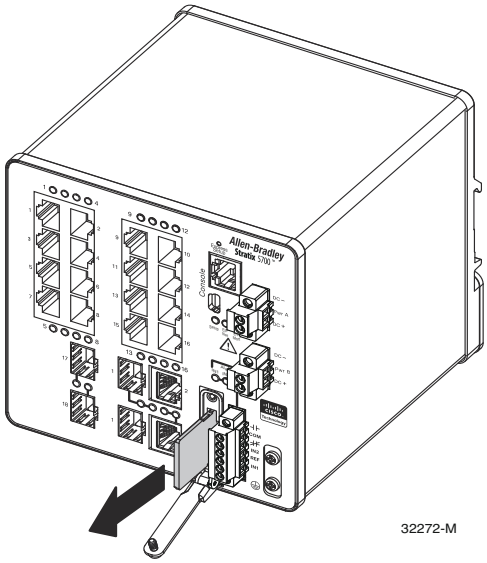
- 前后面板间隙应满足以下条件：
  - 可轻松看到前面板状态指示灯。
  - 端口周围必须有足够的空间可供布线。
  - 前面板直流 (DC) 电源连接器和报警继电器连接器能够连接到 DC 电源。
- 接线远离电噪声源，例如，无线电设备、电源线和荧光灯具。
- 只能将设备连接至 2 类 DC 电源。

安装或取出 SD 卡（可选）

要安装或替换 SD 卡，请按以下步骤操作。

1. 在交换机正面，找到保护 SD 卡槽的盖板。
2. 使用螺丝刀拧松盖板顶部的外加拇指螺丝，打开盖板。
   a. 要安装卡，首先将其滑入插槽，然后在适当位置按压，直到它利用弹簧机构锁定为止。
      卡为键控式，因此采用错误方式安装时不可能将卡完全插入。
   b. 要取出卡，首先将它向内推，使其借助弹簧机构弹出。
   c. 捏住卡的顶端往外拉。
      将其置于防静电袋中，防止发生静电放电。





3. 安装好卡之后，关闭保护盖板并使用螺丝刀将外加螺丝拧紧，使盖板锁紧到位。

验证交换机运行

在将交换机安装到最终位置之前，接通交换机的电源并确保交换机已上电。

交换机启动所需的时间与交换机配置直接相关。下列两项会对启动时间产生负面影响：

- 生成树学习模式
- 板载闪存中的文件或图像数

要测试交换机，请按以下步骤操作。

1. 接通交换机的电源。

   要给直接连接 DC 电源的交换机供电，需要确定面板上 DC 电路断路器的位置，并将断路器切换到 ON 位置。

2. 验证启动序列。

   上电后，交换机会自动开始执行一个快速启动例程。在 IOS 软件图像的加载过程中，System 状态指示灯将呈绿色闪烁状态。如果例程失败，System 状态指示灯将变为红色。

注意：启动故障对于交换机通常是致命的。如果您的交换机无法成功完成启动序列，请立即联系您的罗克韦尔自动化代表。

重要信息　**您可以使用 IOS CLI 禁用快速启动，并运行上电自检 (POST)。更多信息，请参见 http://www.Cisco.com 上的相关文档。**

3. 成功运行该测试后，请按照以下步骤操作：
   a. 切断交换机的电源。
   b. 断开电缆连接。
   c. 确定交换机的安装位置。

连接保护性接地和 DC 电源

以下部分将介绍为交换机连接保护性接地和 DC 电源所需要的步骤。

对于 DC 电源连接，使用 UL 和 CSA 等级的 1007 或 1569 式双绞- 铜电子线 (AWM)，例如，Belden 零件号 9318。

交换机接地

注意：该设备必须接地。切勿拆卸接地导线或在未安装合适接地导线的情况下运行设备。如果您不确定是否存在合适的接地，请联系相关电气检查机构或电工。

将该设备接地是为了符合辐射和干扰性要求。确保交换机功能性接地接线片在正常使用期间接地。

注意：为确保设备可靠接地，请遵循接地步骤说明，并使用适合 #10 到 #12 AWG 导线且经 UL 认证的环形端子接线片，例如 Thomas & Betts 零件号 10RC6 或同等产品。

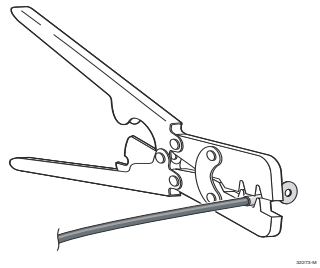
要连接到外部接地螺丝，至少需要使用 12 AWG (4 mm^2) 导线。

交换机未附带接地片。可使用下列选件之一：

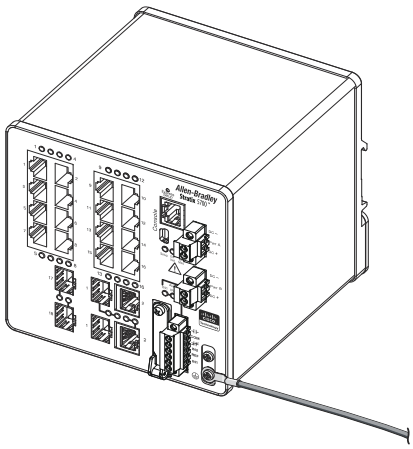
- 单环端子
- 两个单环端子

要将交换机接地，请按以下步骤操作。确保您的工厂满足所有接地要求。

1. 用十字螺丝刀或十字棘轮扭力螺丝刀卸下交换机前面板上的接地螺丝。保管好接地螺丝，以备后续使用。
2. 根据制造商准则确定剥线长度。
3. 将接地线插入环形端子接线片，用压线钳将端子压接在导线上。如果使用两个环形端子，则对第二个环形端子重复这一操作。



4. 将接地螺丝滑入端子。
5. 将接地螺丝插入前面板上的功能接地螺丝孔。



6. 用棘轮扭力螺丝刀将接地螺丝和环形端子接线片拧到交换机前面板上，扭矩应为 0.4 N•m (3.5 lb•in)。

   不要超过建议扭矩。

7. 将地线的另一端连接到接地的裸露金属表面，例如接地母线、已接地的 DIN 导轨或者已接地的裸露机架。

连接交换机 DC 电源

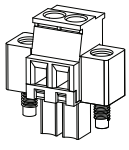
要为交换机连接 DC 电源，请按以下步骤操作。

注意：执行下列步骤前，确保 DC 电路已断电或该区域无危险：

- **该产品由额定值为 12、24 或 48V DC，2.5 A 的 2 类电源 （标记有 “2 类 ”） 供电。**
- **为符合 CE 低压指令 (LVD)，本设备供电电源必须符合安全超低电压 (SELV) 或保护性超低电压 (PELV) 标准。**
- **必须将易于操作的双极隔离装置集成到固定接线中。**
- **该产品依靠建筑物的设施提供短路（过流）保护。确保保护装置的额定电流不超过 3 A。**
- **设备安装必须符合当地和国际电气规范。**
- **只允许经过培训的合格人员安装、更换或维修此设备。**

注意：对于电源和继电器连接器的接线，必须采用 UL 和 CSA 等级的 1007 或 1569 式双绞铜电子线 (AWM)（例如，Belden 零件号 9318）。

1. 确定电源连接器的位置。

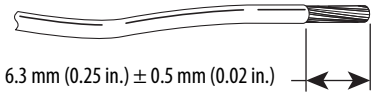


2. 标识 DC 电源正极和回路接点。

   DC 电源正极接点标记为 DC+，DC 电源负极接点为临近标有 DC- 的接点。

3. 量取足够长的 0.82...0.52 mm^2 (18...20 AWG) 铜线，用于连接 DC 电源。
4. 使用 18 号剥线钳，将这两条导线剥至 6.3 mm (0.25 in.) ± 0.5 mm (0.02 in.)。

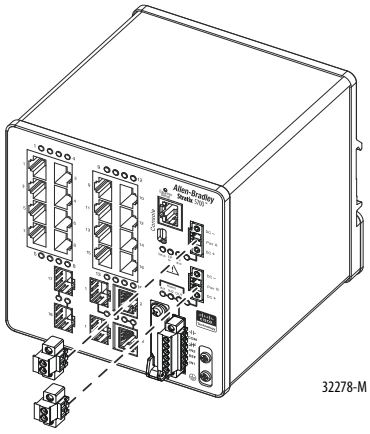
   剥离导线的绝缘层不要超过 6.8 mm (0.27 in.)。如果剥线长度大于推荐长度，安装后会使导线裸露在外。



31789-M

5. 旋松将电源连接器连接到交换机的两个外加螺丝，然后拆除电源连接器。

   如果连接了两个电源，则将两个连接器都拆除。

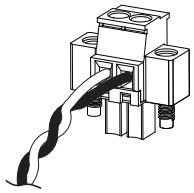


32278-M

6. 将正极接线裸露部分连接至标记为 DC+ 的接点，将回线裸露部分连接至标记为 DC- 的接点。

   确保看不到线芯。仅允许带绝缘层的导线从连接器伸出来。

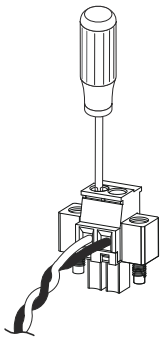
注意：DC 输入电源的裸露引线中可能会传导危害级别的电流。确保 DC 输入电源线的裸露部分不会从连接器或端子块伸出来。



32279-M

7. 用棘轮扭力螺丝刀将电源连接器外加螺丝（位于所安装导线的上方）拧至 0.23 N•m (2.0 lb•in)。

   不要超过建议扭矩。

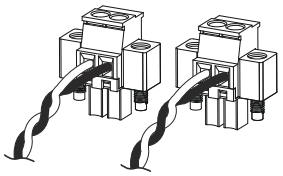


32281-M

8. 将正极的另一端连接至DC电源的正极端子，将回线的另一端连接至 DC 电源的回路端子。

   测试交换机时，连接一个电源便足够。要安装交换机并使用第二电源，请在第二电源连接器上重复该步骤。

   下图显示了主电源和可选第二电源的电源连接器上已完成的 DC 输入接线。

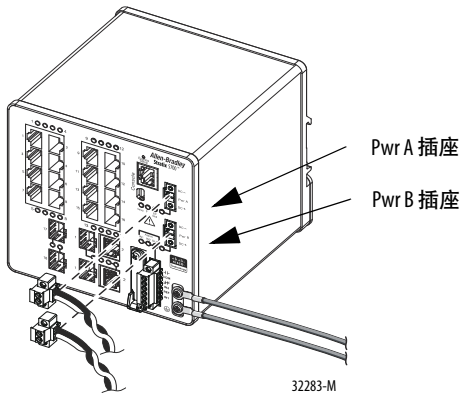


32282-M

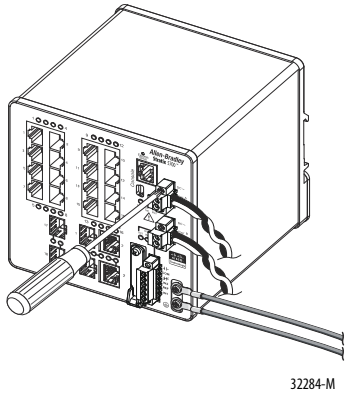
连接交换机电源连接器

要将交换机电源连接器连接到交换机的前面板，请按照以下步骤操作。

1. 将其中一个电源连接器插入交换机前面板上的 Pwr A 插座，然后将另一个电源连接器插入 Pwr B 插座。



2. 用棘轮扭力平头螺丝刀将电源连接器侧面的外加螺丝拧紧。



测试交换机时，连接一个电源便足够。要安装交换机并使用第二电源，请为第二电源连接器 (Pwr B) 重复执行该步骤，第二电源连接器就安装在主电源连接器 (Pwr A) 下面。

3. 安装交换机时，使用扎带将电源连接器的导线固定到机架上。

连接以太网供电 DC 电源（可选）

该步骤仅适用于带 PoE 端口的交换机。

警告： 控制台端口仅为了方便临时本地编程使用，不适合永久连接。如果在带电情况下连接或断开该模块或电缆另一端上所连编程设备的控制台电缆，将会产生电弧。如果在危险场所安装，将可能导致爆炸。因此，在操作前需确保已断开电源且安装区域不存在危险。

注意： 为符合 CE 低压指令 (LVD)，本设备供电电源必须符合安全超低电压 (SELV) 或保护性超低电压 (PELV) 标准。

为符合 UL 限制，本设备供电电源必须符合 2 类或受限电压 / 电流要求。

必须对交换机接线和接地。

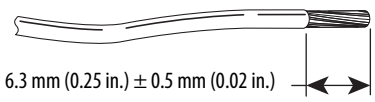
电源要求取决于具体应用。

应用	每个端口的电源	功耗	Allen-Bradley 产品
仅 PoE IEEE 802.3af	44…57V DC （标称值为 48V DC）	最大 15.4 W	开关模式电源 • 1606-XL 标准型 • 1606-XLE 基本型 • 1606-XLP 紧凑型 • 1606-XLS 性能型
PoE 和 PoE + IEEE 802.3at 类型 2	50…57V DC （标称值为 54V DC）	对于 PoE，最大 15.4 W 对于 PoE+，最大 30 W	

警告： 执行下列步骤前，确保 DC 电路已断电或该区域无危险。

1. 量取足够长的 0.82...0.52 mm2 (18...20 AWG) 铜线，用于连接 DC 电源。
2. 使用 18 号剥线钳，将这两条导线剥至 6.3mm (0.25 in.) ± 0.5 mm (0.02 in.)。

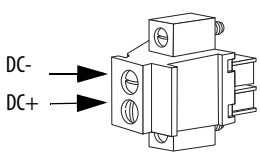
   剥离导线的绝缘层不要超过 6.8 mm (0.27 in.)。如果剥线长度大于推荐长度，安装后会使导线裸露在外。



31789-M

3. 确定电源连接器的位置。
4. 将正极接线裸露部分连接至 DC+ 接点，将回线裸露部分连接至 DC- 接点。

   确保看不到线芯。仅允许带绝缘层的导线从连接器伸出来。



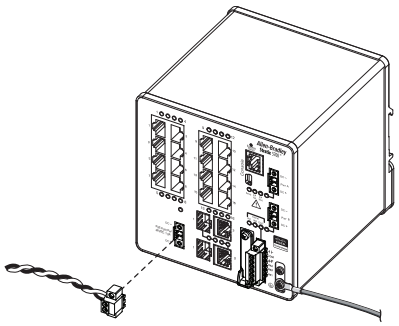
5. 用棘轮扭力螺丝刀将电源连接器外加螺丝（位于所安装导线的上方）拧至 0.23 N•m (2.0 lb•in)。

6. 将正极接线 (连接 DC+) 的另一端连接至 DC 电源的正极端子，将回线 (连接 DC-) 的另一端连接至 DC 电源的回路端子。

注意：如果使用多个电源，请不要超出规定的绝缘电压。

连接 PoE 电源连接器（可选）

1. 将电源连接器插入交换机前面板上的 DC 输入端子块。
2. 用螺丝刀将电源连接器侧面的外加螺丝拧紧。



注意: 设备暴露在某些化学品环境下时可能损害继电器中所用材料的密封特性。因此应定期检查继电器，以确认密封特性是否退化。

安装交换机

本部分将介绍如何安装交换机。

注意：本设备为敞开式设备。它必须安装在经过专门设计的机壳中，以确保能够适应特定的环境条件以及能防止因接触带电部件而导致人身伤害。必须确保只有使用工具才能打开机壳。外壳必须满足 IP 54 或 NEMA 类型 4 最低外壳防护等级标准。

注意：为防止交换机过热，应确保满足以下最小间隙要求：

- **顶部和底部：** 50.8 mm (2.0 in.)
- **裸露侧 （未连接至模块）：** 50.8 mm (2.0 in.)
- **正面：** 50.8 mm (2.0 in.)

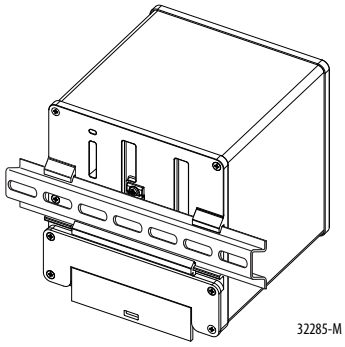
将交换机安装在 DIN 导轨上

交换机出厂时后面板上有一个弹簧锁，用于 DIN 导轨安装。

注意：使用 DIN 导轨安装时，将 DIN 导轨连接到机壳接地可实现辅助接地。请使用镀锌黄- 铬钢 DIN 导轨来确保正确接地。采用其它会腐蚀、氧化或导电不良的 DIN 导轨材质（例如，铝或塑料）可能导致接地不当。按每隔 200 mm (7.8 in.) 一个固定点将 DIN 导轨固定到安装表面，正确使用端锚且在整个 DIN 导轨使用垫片。

要将交换机安装到 DIN 导轨，请按以下步骤操作。

1. 将交换机后面板正对 DIN 导轨正面，确保 DIN 导轨固定在靠近交换机顶部的两个挂钩与靠近底部的弹簧锁之间。
2. 将交换机底部抬起，使其脱离 DIN 导轨，将交换机背面的两个挂钩放置在 DIN 导轨的上方。

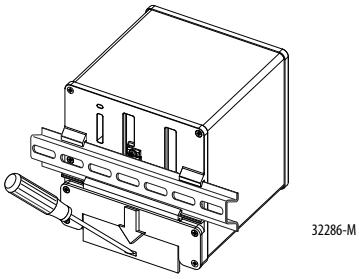


3. 朝 DIN 导轨方向推动交换机，使交换机背面底部的弹簧锁下移并卡入到位。

从 DIN 导轨上拆除交换机

要从 DIN 导轨或机架上拆除交换机，请按以下步骤操作。

1. 断开交换机电源，并拔除交换机前面板上的所有电缆和连接器。
2. 在弹簧锁底部插槽中插入一字螺丝刀或类似工具，从 DIN 导轨松开弹簧锁。



3. 从 DIN 导轨上拆除交换机。

安装 SFP 模块（可选）

对于支持通过光纤电缆进行通信的交换机目录号，SFP 模块插入交换机正面的 SFP 模块插槽中。这些模块支持现场更换，并提供了上行光学接口，发送 (TX) 和接收 (RX)。

您可以随意组合使用坚固的 SFP 模块。每个 SFP 模块的类型都必须与电缆另一端的 SFP 模块类型相同。电缆不得超过规定的电缆长度，以便实现可靠通信。

使用商用 SFP 模块（例如，CWDM 和 1000BX-U/D）时，将最高工作温度降低 15 °C (59 °F)。最低工作温度为 0 °C (32 °F)。

有关安装、拆卸和连接 SFP 模块的详细说明，请参见您的 SFP 模块文档。

注意：强烈建议不要在 SFP 模块连接有光纤电缆的情况下对其进行安装或拆卸，因为这有可能损坏电缆、电缆连接器或 SFP 模块中的光学接口。在拆卸或安装 SFP 模块之前，断开所有电缆的连接。

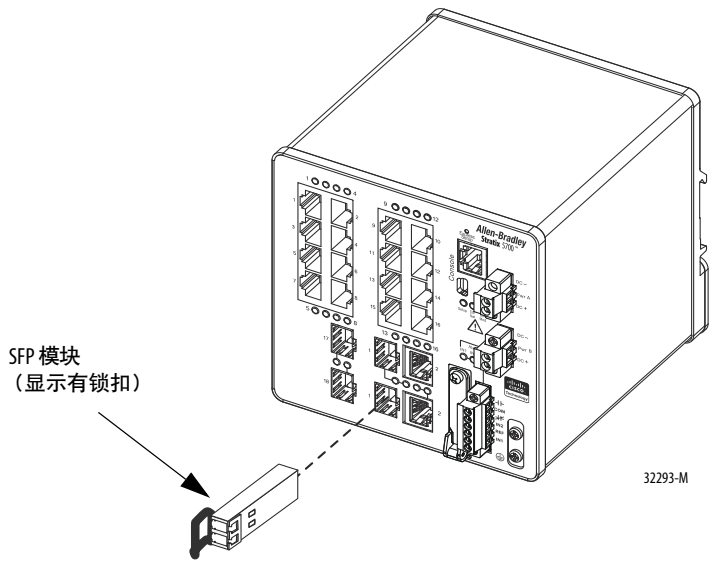
重要信息 **安装再拆除 SFP 模块会缩短其使用寿命。若非必要，不要频繁拆除和插入 SFP 模块。**

要将 SFP 模块插入 SFP 模块插槽，请按以下步骤操作。

1. 将 ESD 防护腕带的一端连接到您的手腕，另一端连接到接地的裸露金属表面。
2. 捏住 SFP 模块的两侧，并面对插槽将模块两侧与插槽开口对齐。

   注意：如果 SFP 模块不能完全插入，请停止操作！不要强行将模块插入插槽。将 SFP 模块旋转 180°，然后重试。

3. 向插槽中插入 SFP 模块（如下图所示），直到感觉到模块上的连接器在插槽后端咬合到位。



4. 将防尘塞从 SFP 模块光学端口上取下并存放起来，以备将来使用。

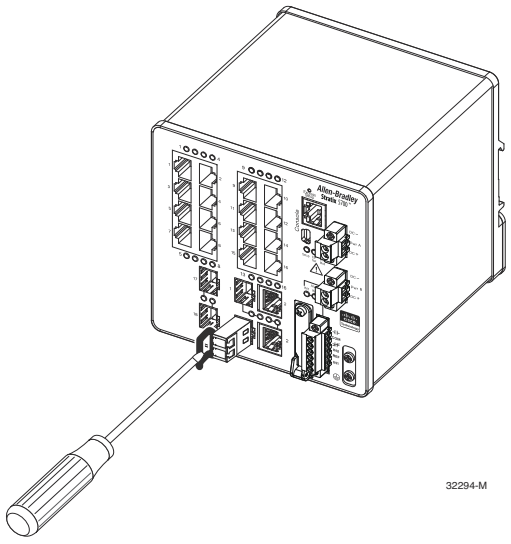
重要信息　**在准备好连接电缆之前，切勿将 SFP 模块端口上的防尘塞或光纤电缆上的橡胶帽取下。**
防尘塞和橡胶帽可保护 SFP 模块端口与电缆免遭污染以及环境光线的照射。

从 SFP 模块插槽中拆除 SFP 模块

要将 SFP 模块从模块插座中取出，请按以下步骤操作。

1. 将 ESD 防护腕带的一端连接到您的手腕，另一端连接到接地的裸露金属表面。
2. 断开光纤 LC 连接器与 SFP 模块之间的连接。
3. 向 SFP 模块的光学端口中插入防尘塞，以便使光学接口保持清洁。
4. 将 SFP 模块解除锁定并将其取出。

   如果模块带有锁扣，则可将锁扣旋转到您的面前，然后轻轻拉动，使其脱离模块。如果锁扣阻塞，用食指无法打开，则可以使用小型平头螺丝刀或者其它细长型工具。



5. 用拇指和食指捏住 SFP 模块，小心地从模块插槽中取出。
6. 将拆下的 SFP 模块置于防静电袋或者其它防护环境中。

连接外部报警装置

交换机具有两个报警输入继电器电路和一个 C 型（单刀双掷）报警输出继电器电路，用于进行外部报警。输入报警继电器电路主要用于检测报警输入相对于报警输入参考引脚是断开还是闭合。输出报警继电器电路具有一个 C 型继电器、一个常开 (NO) 触点和一个常闭 (NC) 触点。您可以使用 CLI 将输出报警继电器配置为常励磁或非常励磁状态。

有关报警装置接线示例，请参见附录 C。

报警信号通过 6 路报警继电器连接器连接到交换机。以下三个连接专用于两个报警输入电路：

- 报警输入 1 (IN1)
- 报警输入 2 (IN2)
- 隔离的参考接地点

要完成输入报警电路接线，需要进行报警输入和参考接地点接线连接。必须在参考接地点与 IN1 或 IN2 之间连接一个 NO 或 NC 干式触点才能完成报警电路接线。

注意：不要对 IN1 或 IN2 报警输入施加外部电压源。报警输出只能连接 48 V DC/0.5 A。

C 型输出报警电路的其余三个连接如下：

- NO 输出
- NC 输出
- 公共端

要完成输出报警电路接线，需要进行报警输出和公共端接线连接。C 型输出报警继电器提供了一个 NO 干式触点和一个 NC 干式触点。

注意：对于电源和继电器连接器的接线，必须采用 UL 和 CSA 等级的 1007 或 1569 式双绞铜电子线 (AWM)（例如，Belden 零件号 9318）。

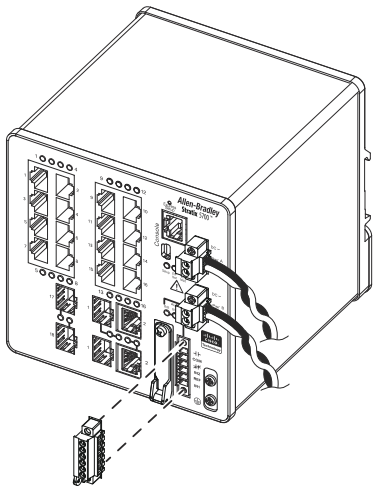
报警继电器连接器的标签位于交换机面板上。

表 1 - 报警继电器连接器标签

标签	连接
NO	报警输出常开 (NO) 连接
COM	报警输出公共端连接
NC	报警输出常闭 (NC) 连接
IN2	报警输入 2
REF	报警输入参考接地连接
IN1	报警输入 1

要将交换机连接到外部报警装置，请按以下步骤操作。

1. 拧松将报警继电器连接器固定在交换机上的外加螺丝，然后从交换机机架上取下连接器。



2. 采用两条足够长的双绞线 (18...20 AWG) 连接到外部报警装置。

   选择构建外部报警输入电路或外部报警输出电路。

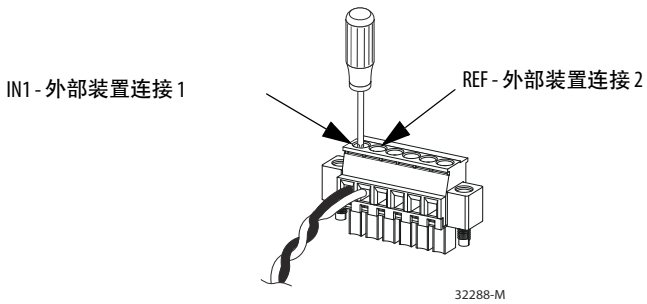
3. 用剥线器将每条导线两端的外皮剥去 6.3 mm (0.25 in.) ± 0.5 mm (0.02 in.)。

   剥离导线的绝缘层不要超过 6.8 mm (0.27 in.)。如果剥线长度大于推荐长度，安装后会使导线裸露在报警继电器连接器的外面。

4. 根据构建的是报警输入电路还是报警输出电路，将外部报警装置的裸露导线插入相应的接口。请参见第 41 页上的表 1。

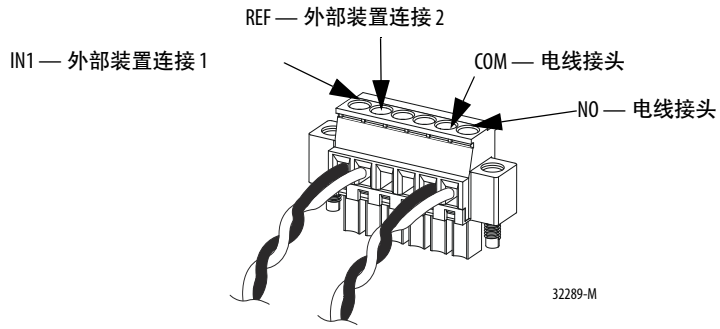
5. 用棘轮扭力平头螺丝刀将报警继电器连接器外加螺丝（位于所安装导线的上方）拧至 0.23 N•m (2.0 lb•in)。

   不要超过建议扭矩。



6. 重复上述步骤，将另一个外部报警装置的输入和输出导线插入报警继电器连接器。

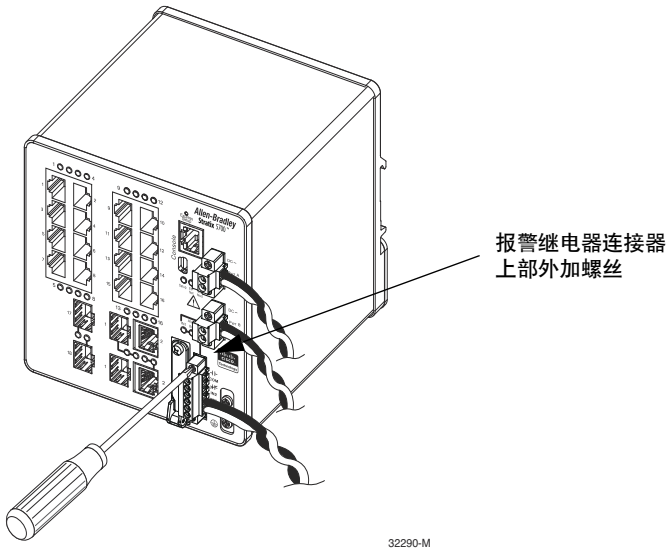
   下图所示为已完成的两个外部报警装置接线。第一个报警装置电路以报警继电器输入电路的方式接线 —连接 IN1 和 REF 即可完成电路。第二个报警装置电路以报警输出电路的方式接线，使用了 C 型继电器的常开触点。连接 NO 和 COM 即可完成电路。



将报警继电器连接器连接至交换机

要将报警继电器连接器连接到交换机的前面板，请按照以下步骤操作。

1. 将报警继电器连接器插入交换机前面板的插座。
2. 用棘轮扭力平头螺丝刀将报警继电器连接器侧面的外加螺丝拧紧。



连接目标端口

要连接至目标端口，请按以下步骤操作。

连接至 10/100 和 10/100/1000 端口

交换机 10/100/1000 端口会自动将自身配置为以所连设备的速度运行。如果所连端口不支持自动协商，您可以明确设置速度和双工参数。如果连接的设备不支持自动协商或者其速度和双工参数均采用手动设置，则可能会影响性能，甚至导致连接失败。

自动 MDIX 功能在默认情况下处于启用状态。只要未禁用此功能，您便可以使用直通电缆或交叉电缆来连接网络中的其它设备。

为实现最佳性能，请选择以下方式之一来配置以太网端口：

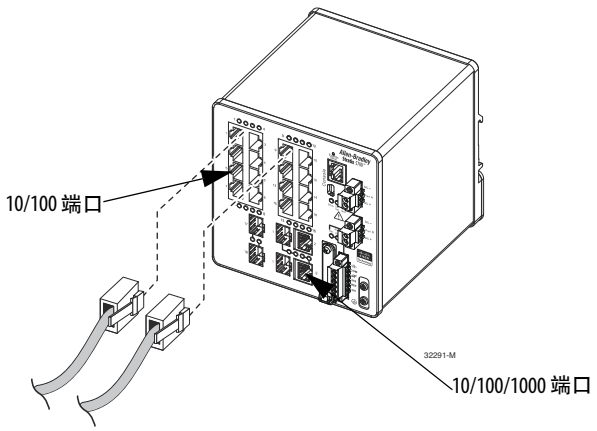
- 使端口自动协商速度和双工
- 在连接的两端均设置端口速度和双工参数

连接至 10BASE-T、100BASE-TX 或 1000BASE-T 端口

要连接至 10BASE-T、100BASE-TX 或 1000BASE-T 端口，请按以下步骤操作。

注意：为防止静电放电 (ESD) 损坏，请按建议的板和组件处理步骤执行。

1. 选择下列方式之一来连接设备：
   - 连接至工作站、服务器和路由器时，使用直通电缆连接到前面板的 RJ45 连接器。
   - 连接至 1000BASE-T 兼容设备时，使用 5e 类四对双绞线电缆或更高规格的电缆。



2. 将电缆的另一端连接至另一个设备的 RJ45 连接器。

   当交换机与所连设备建立链接后，Port 状态指示灯将点亮。

   当生成树协议 (STP) 发现拓扑并搜索回路时，Port 状态指示灯将呈琥珀色。这一过程持续 30 秒之后，Port 状态指示灯会变为绿色。

在下列情况下，Port 状态指示灯不会点亮：

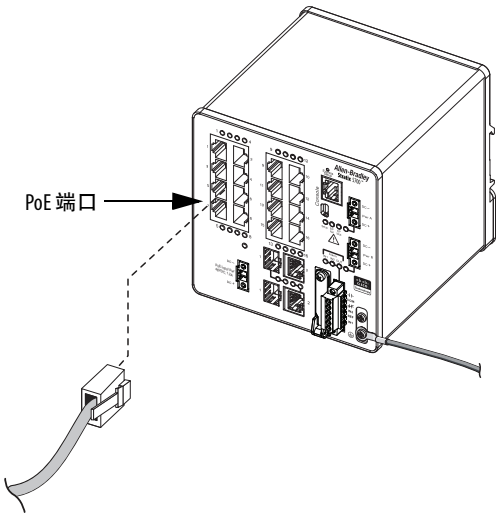
- 另一端的设备未启动。
- 电缆存在问题，或者所连接设备上安装的适配器存在问题。

3. 必要时重新配置所连接设备并重新启动。
4. 重复此步骤来连接每个设备。

连接至 PoE 端口

带 PoE 端口的交换机需要使用单独的电源。有关您应用的电源要求，请参见第 36 页。

1. 通过 RJ45 连接器将 5e 类直通四对双绞线电缆或更好的电缆插入 PoE 端口。



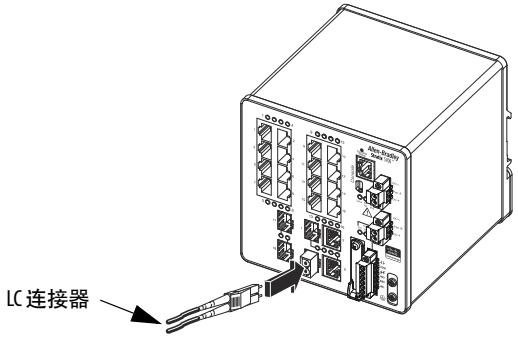
2. 将电缆另一端插入另一个 PoE 供电设备的 RJ45 连接器。

连接至 SFP 模块

要将光纤电缆连接至 SFP 模块，请按以下步骤操作。

注意：在准备好连接电缆之前，切勿将 SFP 模块端口上的橡胶塞或光纤电缆上的橡胶帽取下。防尘塞和橡胶帽可保护 SFP 模块端口与电缆免遭污染以及环境光线的照射。

1. 将模块端口和光纤电缆上的橡胶塞取下并存放起来，以备将来使用。
2. 将光纤电缆的一端插入 SFP 模块端口。



3. 将电缆的另一端插入目标设备的光纤插座。
4. 观察端口状态指示灯：
   - 当 SFP 发现网络拓扑并搜索回路时，状态指示灯会变成琥珀色。这一过程持续约 30 秒之后，端口状态指示灯会变为绿色。
   - 当交换机与目标设备建立链接后，状态指示灯会变为绿色。
   - 当目标设备未启动、电缆存在问题、或者目标设备中安装的适配器存在问题时，状态指示灯会熄灭。

   如有必要，重新配置交换机或目标设备并重新启动。

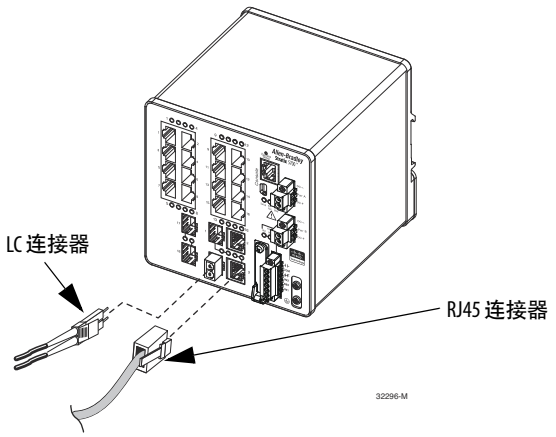
连接至两用端口

两用端口具有两个接口，一个用于 RJ45 电缆，另一个用于经认证的 SFP 模块。每次只有一个接口可以处于激活状态。如果同时连接了两个端口，则优先使用 SFP 模块端口。

注意：在准备好连接电缆之前，切勿将 SFP 模块端口上的橡胶塞或光纤电缆上的橡胶帽取下。防尘塞和橡胶帽可保护 SFP 模块端口与电缆免遭污染以及环境光线的照射。

要连接至两用端口，请按以下步骤操作。

1. 将 RJ45 连接器连接到 10/100/1000 端口，或者将 SFP 模块安装到 SFP 模块插槽中，然后将电缆连接到 SFP 模块端口。



2. 将电缆另一端连接到另一个设备。

   默认情况下，交换机会检测两用端口中连接的是 RJ45 连接器还是 SFP 模块，并相应地配置端口。您可以更改此设置，使用介质类型接口配置命令将端口配置为仅识别 RJ45 连接器或仅识别 SFP 模块。更多信息，请参见 http://www.Cisco.com 上的相关文档。

通过快速设置对交换机进行初始设置

首次设置交换机时，请使用快速设置功能输入初始 IP 地址。这样可以将交换机用作管理型交换机。然后，可通过该 IP 地址访问交换机，进行更多配置。

重要信息 不要在交换机中插有 SD 卡的情况下运行快速设置功能。

设置交换机需要以下设备：

- 装有 Windows 2000、Windows XP、Windows 2003 或 Windows Vista 操作系统的个人计算机
- 具有 JavaScript 功能的受支持 Web 浏览器（Internet Explorer 9.0、Internet Explorer 10.0、Internet Explorer 11.0 或 Firefox 25、Firefox 26）
- 一条用于连接个人计算机与交换机的 5 类直通或交叉以太网电缆

请执行以下操作来配置您的计算机：

- 禁用个人计算机上运行的所有无线接口。
- 禁用系统中的其它网络。
- 将您的计算机设置为自动确定其 IP 地址 (DHCP)，而不是配置静态 IP 地址。
- 禁用任何静态的 DNS 服务器。
- 禁用浏览器代理设置。

通常，浏览器设置位于 Tools > Internet Options > Connections > LAN Settings 中。

要运行快速设置，请按以下步骤操作。

1. 确保至少有一个交换机以太网端口可供快速设置使用。

   重要信息 不要对控制台端口使用快速设置。

   在执行快速设置过程中，交换机用作 DHCP 服务器。如果您的个人计算机使用静态 IP 地址，请在开始操作前将个人计算机设置更改为暂时使用 DHCP。

2. 接通交换机电源。

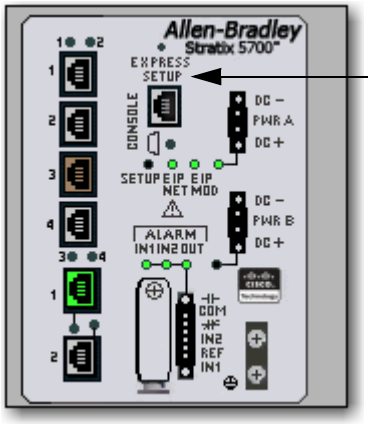
   交换机通电后，将开始执行上电序列。上电序列大概持续 60 秒。

3. 检查 EIP 模块和 Setup 状态指示灯是否呈绿色闪烁，以确保完成上电序列。

   如果交换机上电序列失败，EIP 模块状态指示灯会变为红色。

4. 按下并释放 Express Setup 按钮。等待数秒钟，直到某一空闲交换机端口的状态指示灯呈绿色闪烁为止。

   该按钮在前面板下凹 16 mm (0.63 in.) 位置。请使用小工具（例如，回形针）操作该按钮。



5. 使用 5 类以太网电缆（不提供）从闪烁的交换机端口连接到个人计算机上的以太网端口。

   提示　**如果等待连接电缆的时间过长，则 Setup 状态指示灯会熄灭。**

   在交换机配置连接期间，个人计算机和交换机上的端口状态指示灯都会闪烁。

6. 在 Setup 状态指示灯呈绿色闪烁期间，在个人计算机上启动 Internet 浏览器会话并导航到 http://169.254.0.1。

   如果您配置了主页，此时将不会正常加载主页，而会加载交换机配置。

   交换机会提示您输入默认的交换机用户名和密码。

7. 输入默认的交换机密码：**switch**。

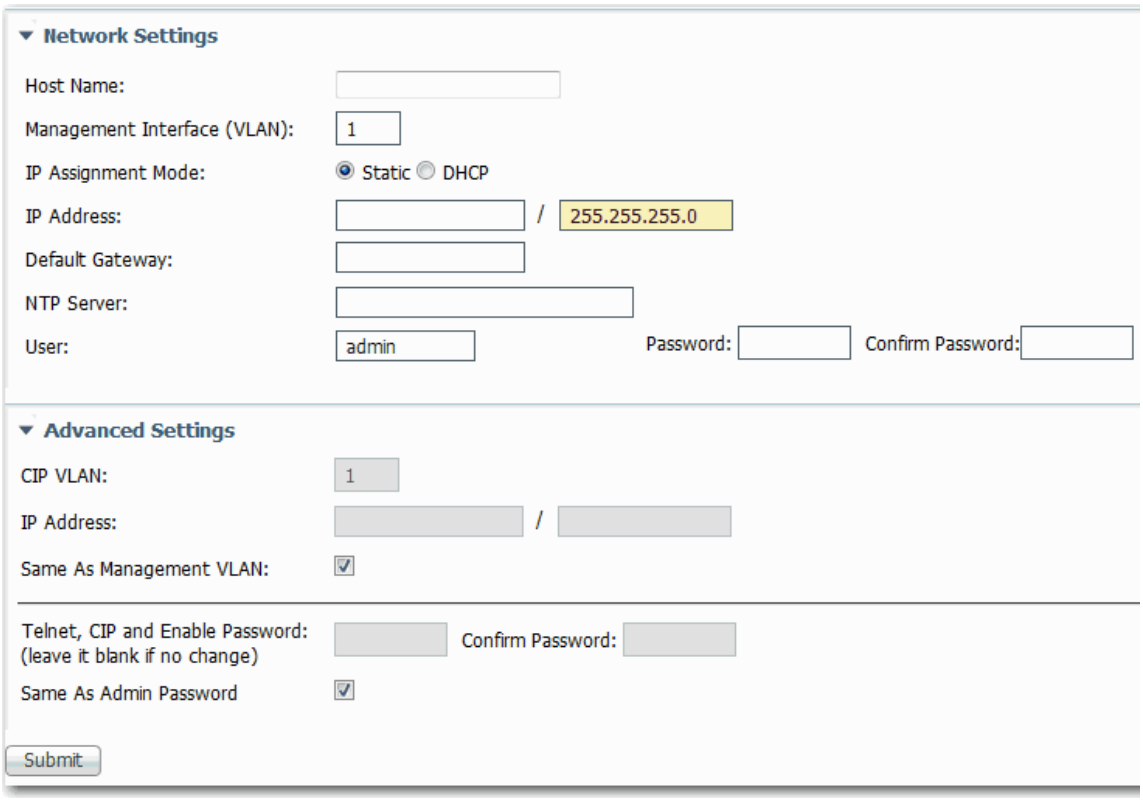
   默认用户名称为 **admin**。

   重要信息　**在某些情况下，您需要多次输入交换机密码，交换机才会接受它。**

8. 如果未出现 Express Setup 窗口，请执行以下操作：
   - 在浏览器中输入一个知名网站的 URL，确保浏览器工作正常。如果浏览器工作正常，它将自动跳转到 Express Setup Web 页面。
   - 确定已禁用浏览器中的代理设置或弹出窗口阻止程序。
   - 确定已禁用个人计算机上的全部无线接口。

9. 填写如下各字段。

   要查看通用工业协议 (CIP) 的字段，必须单击 Advanced Settings。



字段	描述
	网络设置
Host Name	设备的名称。
Management Interface (VLAN ID)	用于管理交换机的管理 VLAN 的名称和 ID。选择已有的 VLAN 作为管理 VLAN。 默认 ID 为 1。管理 VLAN 的默认名称为 default。该组数字的范围是 1...1001。请确保交换机和网络管理站位在同一 VLAN 中。否则，交换机的管理连接便会丢失。 管理 VLAN 是管理通信在特定用户或设备之间进行传送所通过的广播域。它为必须限定于特定用户组（例如网络管理员）使用的管理通信提供了广播控制及安全功能。它还可以确保任何时候对所有网络设备进行安全的管理访问。
IP Assignment Mode	IP 分配模式决定交换机的 IP 信息为手动分配（静态）还是由动态主机配置协议 (DHCP) 服务器自动分配。默认设置为 Static。 建议单击 Static 并手动为交换机分配 IP 地址。此后，如需访问设备管理器 Web 界面，则可随时使用该 IP 地址。 如果单击 DHCP，则 DHCP 服务器会自动为交换机分配 IP 地址、子网掩码和默认网关。只要交换机未重启，它便可继续使用已分配的 IP 信息，同时可以使用此 IP 地址访问设备管理器 Web 界面。 如果手动分配交换机 IP 地址，但网络使用了 DHCP 服务器，则需确保分配给交换机的 IP 地址不在 DHCP 服务器自动分配给其它设备的地址范围之内。这样可防止交换机与其它设备之间发生 IP 地址冲突。
IP Address	IP 地址和相应的子网掩码是交换机在网络中的唯一标识符： • IP 地址的格式是一个 32 位数字地址，共四组数字，之间用句点分隔。每组数字的范围都是 0...255。 • 子网掩码是标识交换机所属子网络（子网）的网络地址。子网用于在网络中将设备分成更小的组。默认值为 255.255.255.0。 此字段只有在 IP Assignment Mode 为 Static 时才可用。 确保为交换机分配的 IP 地址未被网络中的其它设备使用。IP 地址和默认网关不可相同。
Default Gateway（可选）	默认网关的 IP 地址。网关是交换机和其它网络或子网络中的设备实现通信所需的路由器或专用网络设备。默认网关的 IP 地址必须与交换机 IP 地址在同一子网中。交换机 IP 地址和默认网关 IP 地址不可相同。 如果所有设备都在同一网络中，且未使用默认网关，则无需在此字段中输入 IP 地址。此字段只有在 IP Assignment Mode 为 Static 时才可用。 如果网络管理站和交换机在不同的网络或子网络中，则必须指定默认网关。否则，交换机和网络管理站之间不能相互通信。
NTP Server	网络时间协议 (NTP) 服务器的 IP 地址。NTP 是实现数据包交换、可变延时数据网络上各计算机系统时钟同步的网络协议。
User	输入用户名称。
Password、Confirm Password	交换机的密码最多可以由 63 个字母数字字符组成，可以数字开头，区分大小写且中间可以包含空格。该密码不能为单个数字，也不能包含 ? 号或制表符，并且不能以空格开始或结束。默认值为 **switch**。 要完成初始化设置，必须更改默认密码 (**switch**)。 此密码也用作控制工业协议 (CIP) 的安全密码。建议您为交换机设置一个密码，以确保安全地访问设备管理器。
	Advanced Settings
CIP VLAN	启用通用工业协议 (CIP) 的 VLAN。CIP VLAN 可与管理 VLAN 相同，也可在设备上配置的另一个 VLAN 中单独进行 CIP 通信。
IP Address	CIP VLAN 的 IP 地址和子网掩码（CIP VLAN 与管理 VLAN 不同时）。IP 地址的格式是一个 32 位数字地址，共四组数字，之间用句点分隔。每组数字的范围都是 0...255。 确保为设备分配的 IP 地址未被网络中的其它设备使用。
Same As Management VLAN	指示 CIP VLAN 的设置是否与管理 VLAN 相同。
Telnet, CIP and Enable Password（可选）、Confirm Password	用于 Telnet 和 CIP 安全性的密码。
Same As Admin Password	将用于 Telnet 和 CIP 安全性的密码设置为与 Network Settings 下指定的用户密码相同。

10. 单击 Submit。

    交换机将初始化配置，以适合典型的工业 EtherNet/IP 应用。之后，交换机会跳转到设备管理器 Web 界面的登录页面。您可以继续启动设备管理器 Web 界面进行进一步配置，也可以退出该应用程序。

11. 关闭总直流电源，断开所有连接到交换机的电缆，然后将交换机安装到网络中。

12. 在完成快速设置后，刷新个人计算机 IP 地址：

    - 如需动态分配 IP 地址，请断开交换机与个人计算机的连接，然后再将个人计算机重新连接到网络中。网络 DHCP 服务器会为个人计算机分配一个新 IP 地址。
    - 如需静态分配 IP 地址，则可将其更改为先前配置的 IP 地址。

注：

交换机软件功能

端口编号

端口 ID 由端口类型（千兆以太网表示千兆端口，高速以太网表示 10/100 Mbps 端口）、单元编号（始终为 1）和端口编号（1-2 用于千兆端口、1-18 用于所有其它端口，具体取决于目录号）组成。千兆以太网缩写为 Gi，高速以太网缩写为 Fa。

下表列出了交换机的端口编号。

表 2 - 端口编号

目录号	描述	交换机标签上的端口编号	config.text 文件中的端口编号
1783-BMS06SL	6 端口（4 个以太网端口；2 个 SFP 插槽）管理型交换机；精简版固件	1 2 3 4 5 6	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6
1783-BMS06SA	6 端口（4 个以太网端口；2 个 SFP 插槽）管理型交换机；完整版固件	1 2 3 4 5 6	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6
1783-BMS06TL	6 端口（6 个以太网端口）管理型交换机；精简版固件	1 2 3 4 5 6	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6
1783-BMS06TA	6 端口（6 个以太网端口）管理型交换机；完整版固件	1 2 3 4 5 6	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6
1783-BMS06SGL	6 端口（4 个以太网端口；2 个 SFP 千兆插槽）管理型交换机；精简版固件	1 2 3 4 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Gi1/1 Gi1/2
1783-BM06SGA	6 端口（4 个以太网端口；2 个 SFP 千兆插槽）管理型交换机；完整版固件	1 2 3 4 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Gi1/1 Gi1/2
1783-BMS06TGL	6 端口（4 个以太网端口；2 个千兆端口）管理型交换机；完整版固件	1 2 3 4 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Gi1/1 Gi1/2
1783-BMS06TGA	6 端口（4 个以太网端口；2 个千兆端口）管理型交换机；完整版固件	1 2 3 4 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Gi1/1 Gi1/2

表 2 - 端口编号 （续）

目录号	描述	交换机标签上的端口编号	config.text 文件中的端口编号
1783-BMS10CL	10 端口（8 个以太网端口；2 个组合端口）管理型交换机；精简版固件	1 2 3 4 5 6 7 8 9 10	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Fa1/9 Fa1/10
1783-BMS10CA	10 端口（8 个以太网端口；2 个组合端口）管理型交换机；完整版固件	1 2 3 4 5 6 7 8 9 10	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Fa1/9 Fa1/10
1783-BMS10CGL	10 端口（8 个以太网端口；2 个组合千兆端口）管理型交换机；精简版固件	1 2 3 4 5 6 7 8 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Gi1/1 Gi1/2
1783-BMS10CGA	10 端口（8 个以太网端口；2 个组合千兆端口）管理型交换机；完整版固件	1 2 3 4 5 6 7 8 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Gi1/1 Gi1/2
1783-BMS10CGN	10 端口（8 个以太网端口；2 个组合千兆端口）管理型交换机；完整版固件；NAT	1 2 3 4 5 6 7 8 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Gi1/1 Gi1/2
1783-BMS10CGP	10 端口（8 个以太网端口；2 个组合千兆端口）管理型交换机；完整版固件；PTP	1 2 3 4 5 6 7 8 1 2	Fa1/1 Fa1/2 Fa1/3 Fa1/4 Fa1/5 Fa1/6 Fa1/7 Fa1/8 Gi1/1 Gi1/2

表 2 - 端口编号 （续）

目录号	描述	交换机标签上的端口编号	config.text 文件中的端口编号
1783-BMS12T4E2CGNK	18 端口（12 个以太网端口；4 个 PoE/PoE+ 端口；2 个组合千兆端口）管理型交换机；完整版固件；NAT；涂层防护	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		1	Gi1/1
		2	Gi1/2
1783-BMS12T4E2CGP	18 端口（12 个以太网端口；4 个 PoE/PoE+ 端口；2 个组合千兆端口）管理型交换机；完整版固件	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		1	Gi1/1
		2	Gi1/2
1783-BMS12T4E2CGL	18 端口（12 个以太网端口；4 个 PoE/PoE+ 端口；2 个组合千兆端口）管理型交换机；精简版固件	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		1	Gi1/1
		2	Gi1/2

表 2 - 端口编号 （续）

目录号	描述	交换机标签上的端口编号	config.text 文件中的端口编号
1783-BMS20CL	20 端口（16 个以太网端口；2 个 SFP 插槽；2 个组合端口）管理型交换机；精简版固件	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		17	Fa1/17
		18	Fa1/18
		19	Fa1/19
		20	Fa1/20
1783-BMS20CA	20 端口（16 个以太网端口；2 个 SFP 插槽；2 个组合端口）管理型交换机；完整版固件	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		17	Fa1/17
		18	Fa1/18
		19	Fa1/19
		20	Fa1/20
1783-BMS20CGL	20 端口（16 个以太网端口；2 个 SFP 插槽；2 个组合千兆端口）管理型交换机；精简版固件	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		17	Fa1/17
		18	Fa1/18
		1	Gi1/1
		2	Gi1/2

表 2 - 端口编号 （续）

目录号	描述	交换机标签上的端口编号	config.text 文件中的端口编号
1783-BMS20CGN	20 端口（16 个以太网端口；2 个 SFP 插槽；2 个组合千兆端口）管理型交换机；完整版固件；NAT	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		17	Fa1/17
		18	Fa1/18
		1	Gi1/1
		2	Gi1/2
1783-BMS20CGP	20 端口（16 个以太网端口；2 个 SFP 插槽；2 个组合千兆端口）管理型交换机；完整版固件；PTP	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		17	Fa1/17
		18	Fa1/18
		1	Gi1/1
		2	Gi1/2
1783-BMS20CGPK	20 端口（16 个以太网端口；2 个 SFP 插槽；2 个组合千兆端口）管理型交换机；完整版固件；PTP；涂层防护	1	Fa1/1
		2	Fa1/2
		3	Fa1/3
		4	Fa1/4
		5	Fa1/5
		6	Fa1/6
		7	Fa1/7
		8	Fa1/8
		9	Fa1/9
		10	Fa1/10
		11	Fa1/11
		12	Fa1/12
		13	Fa1/13
		14	Fa1/14
		15	Fa1/15
		16	Fa1/16
		17	Fa1/17
		18	Fa1/18
		1	Gi1/1
		2	Gi1/2

全局宏

按第 47 页所述完成“快速设置”后，交换机将执行一个全局宏 (ab-global)。该宏用于为采用 EtherNet/IP 协议的典型工业自动化应用配置交换机。该宏将设置多个参数，包括以下主要设置：

- 启用 IGMP 监听和查询器
- 启用 CIP
- 配置 QoS 设置并对 CIP、PTP 和其它通信进行分类（不适用于带精简版固件的交换机）
- 启用报警、SYSLOG 和 SNMP 通知
- 启用快速生成树协议 (RSTP)、BPDU 防护、BPDU 过滤和环路保护

如果没有运行“快速设置”来初始化交换机，全局宏不会运行。您可以使用 CLU 来运行全局宏。

智能端口

智能端口是交换机端口的建议配置。这些配置（称为端口角色）将优化交换机连接，并确保交换机端口通信的安全性、传输质量和可靠性。端口角色还有助于防止端口错误配置。

提示 **请在交换机初始设置完成后立即使用智能端口角色，以使交换机端口在与设备连接之前即已正确配置。**

通过智能端口角色优化端口

表 3 中介绍的端口角色取决于将连接到交换机端口的设备类型。例如，“自动化桌面”端口角色专门用于与桌面计算机和便携式计算机连接的交换机端口。

自定义智能端口角色

利用 Stratix 5700 交换机，用户可创建和修改多达 10 个自定义智能端口角色，以适应各种自定义应用。仅当用户使用的浏览器是版本 3.6 及更高版本的

Mozilla Firefox Web 浏览器时，才能导入或导出自定义智能端口角色。默认情况下，交换机端口设置为 None 端口角色。

表 3 - 智能端口角色

端口角色	描述
自动化设备	此角色适用于与 Ethernet/IP（以太网工业协议）设备连接的端口。它可用于工业自动化设备，如逻辑控制器和 I/O： • 端口被设为访问模式。 • 只允许一个 MAC ID 以确保端口安全性。 • 优化 CIP 通信的队列管理。
多端口自动化设备	此角色适用于与多端口 Ethernet/IP 设备（如以线型拓扑或菊花链拓扑排布的多端口 EtherNet/IP 设备、1783-ETAP 模块（仅用于连接设备端口）、非管理型交换机（例如 Stratix 2000™）以及已禁用远程生成树协议 (RSTP) 的管理型交换机）连接的端口： • 端口被设为访问模式。 • 不具有端口安全性。 • 优化 CIP 通信的队列管理。
自动化桌面	此角色适用于与桌面设备（如桌面计算机、工作站、笔记本电脑及其它基于客户端的主机）连接的端口： • 端口被设为访问模式。 • 启用快速端口。 • 只允许一个 MAC ID 以确保端口安全性。 不适用于与交换机、路由器或接入点连接的端口。
自动化虚拟桌面	此角色适用于与运行虚拟化软件的计算机连接的端口。可将其用于最多运行两个 MAC 地址的设备： • 端口被设为访问模式。 • 启用快速端口。 • 端口安全性设置支持两个 MAC ID。 **重要信息：**自动化虚拟桌面角色不适用于与交换机、路由器或接入点连接的端口。
自动化交换机	此角色适用于与其它已启用生成树协议的交换机连接的端口。 端口被设为干线模式。
自动化路由器	此角色适用于与路由器或已启用路由服务的第三层交换机连接的端口。
自动化电话	此角色适用于与 IP 电话连接的端口。可以将桌面设备（如计算机）与 IP 电话连接。IP 电话与连接的计算机均通过此端口访问网络： • 端口被设为干线模式。 • 端口安全性设置支持三个 MAC ID 使用此端口。 此角色将语音通信的优先级排在常规数据通信之前，以确保 IP 电话接收到清晰的语音。
自动化无线	此角色适用于与无线接入点连接的端口。接入点最多可以为 30 个无线用户提供网络接入。
端口镜像	此角色适用于受网络分析器监视的端口。有关端口镜像的详细信息，请参见第 82 页上的端口镜像。
无	如果不想在端口上应用专门的智能端口角色，则对端口应用此角色。此角色可用于与任何设备的连接，包括上述角色中的设备。
CS1…CS10	自定义智能端口角色。用户可创建具有用户定义的名称的端口角色。有关创建自定义智能端口角色的详细信息，请参见第4章，通过设备管理器Web 界面管理交换机。

避免智能端口不匹配

当连接的设备与应用于交换机端口的智能端口角色不匹配时，将出现智能端口不匹配。不匹配会对设备和网络造成不利影响。

不匹配可导致以下情况：

- 影响已连接设备的行为
- 降低 CIP、语音、无线、交换机和路由器通信的网络性能（降低服务质量 [QoS] 级别）
- 减少对来宾用户访问网络的限制
- 减弱网络对拒绝服务 (denial of service, DoS) 攻击的防护
- 禁用或关闭端口

我们建议您始终在将设备连接到端口或重新连接设备之前，对应用于该端口的智能端口角色进行验证。

以太网供电 (PoE)

具有 PoE 端口的交换机可通过软件进行配置，并且具备下列功能：

- 支持 IEEE 802.3af (PoE) 兼容设备。
- 支持 IEEE 802.3at 类型 2 (PoE+)，可提高受电设备所能获得的可用功率，每个端口为 15.4...30 W。
- 自动检测和功率预算。交换机可保持功率预算、监视和跟踪功率请求，并且仅在有可用功率时才同意供电。
- 当交换机检测到电路中没有电源时，会为所连接的思科预标准和 IEEE 802.3af 兼容受电设备供电。
- 支持功耗相关的思科发现协议 (CDP)。仅当交换机与思科终端设备搭配使用时才能应用此功能。思科受电终端设备将自身的功耗情况通知给交换机。交换机根据功耗情况选择为 PoE 端口供电，也可以停止为 PoE 端口供电。
- 支持思科智能电源管理。思科受电终端设备与交换机通过功率协商 CDP 消息进行协商，以在功耗水平上达成一致。通过协商，功耗超过 7 W 的大功率受电设备可以以最高功耗模式工作。受电设备起初以低功耗模式（功耗不足 7 W）启动，然后通过协商获得足够的功率，从而以高功耗模式运行。设备只有在收到交换机的确认后，才能切换至高功耗模式。

  思科智能电源管理向后兼容与功耗相关的 CDP。模块根据接收到的 CDP 消息作出响应。第三方受电设备不支持 CDP，因此模块将使用 IEEE 分类来确定设备使用的功率。

受电设备检测和初始功率分配

当具有 PoE 功能的端口处于活动状态，PoE 已启用（默认），并且连接的设备未由其他电源供电时，交换机会对受电设备进行检测。

交换机完成设备检测后，会根据设备类型确定设备的功率需求：

- 交换机从功耗角度对检测到的 802.3 af/at 兼容 IEEE 设备进行分类。根据功率预算中的可用功率，交换机确定是否可以为 PoE 端口供电。下表中列出了各个等级。

表 4 - IEEE 功率分类

类别	为每个端口提供的最大功率
0（类别状态未知）	15.4 W
1	4 W
2	7 W
3	15.4 W
4	30 W，仅限 PoE+ 设备

- 交换机在检测思科预标准受电设备时，这类设备不会提供功率需求。未配置为 PoE+ 的端口会分配 15.4 W，作为功率预算的初始分配。配置为 PoE+ 交换机的端口会分配 30 W。

  初始功率分配是受电设备所需的最大功率。交换机在检测到受电设备并为其供电时，起初会分配上述功率。当交换机收到来自受电设备的 CDP 消息时，以及当受电设备通过 CDP 功率协商消息与模块协商功率水平时，交换机可调整初始功率分配。

交换机可监视和跟踪功率请求，并且仅在有可用功率时才同意供电。交换机可跟踪功率预算，即每个 PoE 端口的可用功率量。无论端口接受还是拒绝提供的功率，交换机都会执行功率核算以了解最新的功率预算。

为 PoE 端口供电后，交换机会使用 CDP（如果思科受电终端设备支持 CDP）来确定所连受电设备的实际功耗需求，并相应调整功率预算。交换机会处理请求，并选择同意或拒绝供电。如果同意请求，交换机会更新功率预算。如果拒绝请求，交换机会验证是否已停止为端口供电，并生成一条 syslog 消息，同时更新状态指示灯状态。受电设备还可与模块进行协商，以获得更多的功率。

如果交换机检测到因欠压、过压、超温、振荡器故障或短路所引发的故障，则将停止为端口供电，并生成一条 syslog 消息，同时更新功率预算和状态指示灯。

电源管理模式

PoE 端口支持以下模式：

- 自动（默认）— 端口自动检测所连设备是否需要供电。此为默认模式。如果端口检测到所连的受电设备，并且模块拥有足够的功率，则会同意供电，并更新功率预算，同时根据先到先得的原则为端口供电，并更新状态指示灯状态。

  如果可用功率足以为所有与交换机连接的受电设备供电，则会为所有设备供电。当可用功率不足以为连接的所有设备供电时，以及当某个设备断开连接又重新连接的同时其他设备在等待供电，则无法确定同意或拒绝为哪些设备供电。

  如果提供的功率超出了系统功率预算，则交换机会拒绝供电，并验证是否已停止向端口供电，同时会生成一条 syslog 消息，并更新状态指示灯状态。交换机拒绝供电后，会定期重新检查功率预算，并不断尝试同意供电请求。

  如果由交换机供电的设备同时还连接了壁式电源，交换机仍能继续为设备供电。无论设备是在由交换机供电，还是通过交流电源供电，交换机都会继续报告其仍然在为设备供电。

  当移除受电设备时，交换机会自动检测到连接断开，并停止为该端口供电。用户此时可连接未被供电的设备，而不会损坏设备。

  用户可指定端口所允许的最大功率。如果受电设备的最大 IEEE 分类功率超出了配置的最大值，则交换机不会向该端口供电。如果交换机为思科受电终端设备供电，但受电设备随后通过 CDP 消息发送的请求超出了配置的最大值，则交换机会停止为该端口供电。为受电设备分配的功率会重新计入总功率预算。如果您不指定功率，交换机会提供最大值。

- 静态 — 即使未连接受电设备，交换机也仍会向端口预分配功率以保证该端口有功率可用。交换机会分配端口配置的最大功率，但无法通过 IEEE 分类或来自思科受电终端设备的 CDP 消息进行调整。因为功率是预分配的，因此任何功耗低于或等于最大功率的受电设备在连接静态端口后都将被供电。端口不再遵循先到先得模式。

  但是，如果受电设备的 IEEE 分类大于最大功率，交换机则不会为其供电。如果交换机通过 CDP 消息获悉思科受电终端设备需要的功率超出了最大功率，则会停止为受电设备供电。

  如果您不指定功率，交换机将预分配最大值。交换机仅在检测到受电设备时，才会为端口供电。对于优先级较高接口，采用静态设置。

- 关闭 — 无论是否已连接待供电设备，交换机都将禁用受电设备检测，并且绝不会为 PoE 端口供电。只有希望确保不会为 PoE 端口供电，仅将该端口用作数据端口时，才采用该模式。

PoE 端口上的最大功率分配 （截止功率）

交换机将采用以下方式确定 PoE 端口的截止功率。

1. 配置为端口预算的功率水平时，采用手动方式
2. 配置用于限制分配给端口的功率的功率水平时，采用手动方式
3. 交换机通过 IEEE 分类和 LLDP 功率协商或 CDP 功率协商来设置设备使用的功率时，采用自动方式

如果您未手动配置截止功率值，则交换机会在连接思科终端设备后通过 CDP 功率协商自动确定。如果交换机使用上述方法无法确定该值，则会采用默认值 15.4 W。

对于 PoE+，如果未手动配置截止功率值，则交换机会通过设备 IEEE 分类以及与思科终端设备之间的 LLDP 功率协商或 CDP 功率协商自动确定。如果未启用 CDP 或 LLDP，则应用默认值 30 W。不过，如果不启用 CDP 或 LLDP，交换机为设备提供的功率不会超过 15.4 W，因为只能根据 CDP 或 LLDP 请求才会分配 15,400...30,000 mW 的功率。如果受电设备未经过 CDP 或 LLDP 协商而消耗了 15.4 W 以上的功率，则可能会超过最大电流限制，从而因流经的电流超过最大电流限制而产生故障。端口会保持故障状态一段时间，然后才会尝试重新上电。如果端口持续消耗 15.4 W 以上的功率，则将重复发生上述循环。

功耗值

您可以配置端口的初始功率分配和最大功率分配。不过，这些配置值仅用于确定交换机何时开始或停止为 PoE 端口供电。最大功率分配与受电设备的实际功耗不同。当您手动设置最大功率分配时，必须考虑连接端口与受电设备的电缆上的功率损耗。截止功率是受电设备的额定功耗与电缆最大功率损耗的总和。

PoE 端口上的受电设备消耗的实际功率是截止功率值加上校准因数 500 mW (0.5 W)。实际截止功率值是近似值，与配置值相差若干个百分点。例如，如果配置的截止功率是 12 W，则实际的截止功率为 11.4 W，比配置值小 0.05%。

由于交换机支持外部可拆卸电源为 PoE/PoE+ 供电，并且可根据使用的电源配置预算，因此为受电设备提供的总功率量会随着电源配置的不同而不同：

- 如果将电源替换为一个功率较低的新电源，此时模块将无法为受电设备提供足够的功率，则交换机将按照端口编号降序的顺序拒绝为处于自动模式的 PoE 端口供电。如果交换机功率仍不足，则将按照端口编号降序的顺序拒绝为处于静态模式的 PoE 端口供电。

- 如果将电源替换为一个功率较高的新电源，此时交换机可提供更多的功率，则交换机将按照端口编号升序的顺序为处于静态模式的 PoE 端口供电。如果交换机仍有可用功率，则将按照端口编号升序的顺序为处于自动模式的 PoE 端口供电。

重要信息　**为精确地分配功率，必须通过设备管理器 Web 界面或 CIP 手动配置电源的总功率。**

VLAN

虚拟局域网 (VLAN) 是按照功能、团体或应用划分的网络用户和资源组的逻辑分段。此分段无需考虑用户和资源的物理位置。例如，可根据公司中的部门或根据相互间经常通信的用户组建立 VLAN。

交换机上已配置一个默认 VLAN，每个交换机端口最初都属于该 VLAN。交换机最多支持 255 个 VLAN（包括默认 VLAN 在内）。

每个 VLAN 都通过其名称和 ID 编号进行标识。默认 VLAN 名为 default。ID 的取值范围为 1...1001 和 1005...4094，其中 1 为默认 ID。

可以将交换机端口分配给默认 VLAN，也可以分配给已创建的 VLAN。根据网络的规模和要求，默认 VLAN 就已足够。我们建议您首先确定 VLAN 需求，再创建 VLAN。

对于自定义智能端口，可以指定该端口要实施的 VLAN 类型。

默认 VLAN 也是管理 VLAN。完成初始设置后，可以创建 VLAN 并将交换机上的任何 VLAN 指定为管理 VLAN。管理 VLAN 用于实现对交换机的管理权限。必须将一个交换机端口分配给管理 VLAN。否则，您对交换机不具有管理权限。初始状态下，所有端口均被分配给管理 VLAN。

您可以将所有端口都分配给默认 VLAN (default)，而无需考虑端口的智能端口角色。

隔离通信和用户

通过使用 VLAN，您可以隔离不同类型的通信（如语音和数据）以保持传输质量并将逻辑分段间的过度通信减至最少。还可以使用 VLAN 来隔离不同类型的用户。例如，出于安全目的，可以限制对特定逻辑工作组的特定数据广播，如仅在为薪资相关通信创建的 VLAN 中的设备上保留员工薪资的相关信息。

使用 VLAN 的另外一个好处是减少不断检查网络资源请求所需的管理工作量。

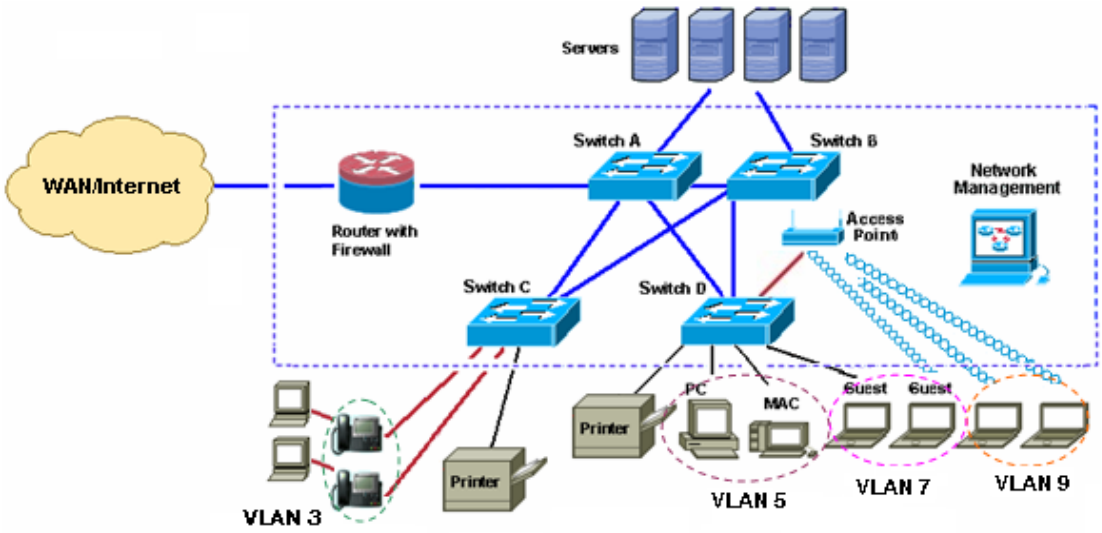
VLAN 将网络隔离为若干部分。因此，连接到处于同一 VLAN 的交换机端口的设备（处于同一 VLAN 的网络用户）可以仅在相互间进行通信并可以共享相同的数据。

除非将交换机配置为用于路由，否则连接到处于不同 VLAN 的交换机端口的设备无法通过交换机相互进行通信。Stratix 5700 交换机、路由器或第三层交换机必须配置为允许跨 VLAN 的路由（VLAN 间路由），还必须设置额外的安全策略。

如果您的网络还使用 DHCP 服务器，请确保所有 VLAN 中的设备均可访问该服务器。

下图为使用基于不同网络通信和网络用户的 VLAN 的网络示例。围绕这些因素来组织网络有助于定义网络中 VLAN 的大小和成员。

图 1 - VLAN 示例



隔离不同的通信类型

将数据通信与延迟敏感的通信（如语音通信）隔离可提高语音传输的质量。在上图中，连接到 IP 电话的交换机端口属于 VLAN 3，该 VLAN 被配置为在这些连接上提供语音 IP (VoIP, Voice over IP) 服务，这意味着语音通信的优先级高于常规 IP 数据通信。与连接到 IP 电话的桌面设备的通信相比，对 IP PBX 服务器的电话和 IP 电话服务请求的语音通信具有更高的优先级。

要进一步隔离数据通信和语音通信，可以将连接的桌面设备的数据通信分配到单独的 VLAN。

用户组

图 1 中所示的网络为三种类型的网络用户提供访问权限：

- 使用有线的员工
- 使用无线的员工
- 使用有线或无线的公司访客

各种用户类型需要不同的公司网络访问权限级别。路由器和第三层交换机上的 VLAN 和安全策略可针对不同的用户类型实施权限和限制。

请参见第 65 页上的图 1：

- VLAN 5 提供员工级别的公司资源访问权限。这种网络访问权限要求直接连接到特定的交换机端口。
- VLAN 7 为公司访客提供仅限 Internet 的访问权限。通过有线或无线连接到交换机端口的访客将被分配到此 VLAN，此 VLAN 会自动将来宾的访问权限限制为仅 Internet。
- VLAN 9 具有一个或多个连接到无线接入点的交换机端口，实施安全策略以标识无线用户（如员工或访客）并确定用户在网络上可进行的操作（如只访问 Internet 或访问其他网络资源）。

IGMP 监听及查询器

第二层交换机可以动态配置第 二层接口，以便多播通信只会转发到与 IP多播设备关联的接口，从而使用 IGMP 监听来限制过度的多播通信。顾名思义，IGMP 监听需要 LAN 交换机监听主机与路由器之间的 IGMP 传输，并记录多播组和成员端口。当交换机从主机接收到某个特定多播组的 IGMP 报告时，交换机会将该主机的端口编号添加到转发表条目中；当其从主机接收到 IGMP 离开组消息时，它会从转发表条目中移除该主机端口。如果交换机没有从多播客户端接收到 IGMP 成员报告，它还会定期删除条目。

多播路由器向所有 VLAN 发出周期性一般查询。与此多播通信有关的所有主机都会发送加入请求并被添加到转发表条目中。交换机在 IGMP 监听 IP 多播转发表中根据 VLAN 为每个向其发送 IGMP 加入请求的组创建一个条目。

交换机支持基于 IP 多播组的桥接，而不支持基于 MAC 编址的组。对于基于多播 MAC 地址的组，如果将配置的 IP 地址转换（更改别名）为之前配置的 MAC 地址或任何保留的多播 MAC 地址（在 224.0.0.xxx 范围内），命令将失败。因为交换机使用 IP 多播组，所以不存在地址别名问题。

交换机支持的默认多播组数为 256。如果多播组数超过 180，我们建议您使用 CLI 切换至路由 SDM 模板。

通过 IGMP 监听获取的 IP 多播组是动态的。如果以静态方式为多播组地址指定组成员，则所做的设置将取代 IGMP 监听的所有自动操作。多播组成员列表可以由用户定义的设置和通过 IGMP 监听获取的设置构成。EtherNet/IP 网络用于 I/O 通信的多播 IP 地址通过交换机获取。

交换机中的 IGMP 实现为 IGMP V2。此版本向后- 兼容运行 IGMP V1 的交换机。交换机内置查询器功能，全局宏可启用 IGMP 监听和查询器。

生成树协议

生成树协议 (STP, Spanning Tree Protocol) 是提供路径冗余同时防止网络中出现环路的第二层链路管理协议。为了使第二层以太网络正常工作，任何两个站之间只能存在一个活动路径。终端站之间存在多个活动路径会导致网络中出现环路。如果网络中存在环路，终端站可能会接收到重复消息。交换机也可能在多个第二层接口获取终端站 MAC 地址。上述情况会造成网络不稳定。对于无法检测到是连接到单个的 LAN 段还是多个段的交换式 LAN 的终端站来说，生成树操作是透明的。

STP 使用生成树算法从冗余连接的网络中选择一个交换机作为生成树的根。该算法根据活动拓扑中的端口角色为每个端口分配角色，从而计算出通过交换式第二层网络的最佳无环路路径：

- 根角色 — 为生成树拓扑选出的转发端口
- 指定角色 — 为每个交换式 LAN 段选出的转发端口
- 备用角色 — 在生成树中提供根桥备用路径的阻塞端口
- 备份角色 — 回路配置中的阻塞端口

将所有端口作为指定角色或备份角色的交换机是根交换机。至少一个端口为指定角色的交换机称为指定交换机。

生成树会强制冗余数据路径进入备用 (阻塞) 状态。如果生成树中的网段失效且存在冗余路径，生成树算法将重新计算生成树拓扑并激活备用路径。交换机会定期发送和接收称为桥接协议数据单元 (BPDU, bridge protocol data unit) 的生成树帧。交换机不会转发这些帧，但会使用它们构建无环路路径。BPDU 包含发送交换机及其端口的相关信息，包括交换机和 MAC 地址、交换机优先级、端口优先级以及路径开销。生成树使用上述信息选出交换网络的根交换机和根端口，以及每个交换网段的根端口和指定端口。

可选择下列选项之一：

- 默认的快速生成树协议 (RSTP) (也称为多生成树协议 [MST])
- 每 VLAN 生成树协议 (Per-VLAN Spanning Tree Protocol, PVST+)
- 快速的每 VLAN 生成树协议 (Rapid Per-VLAN Spanning Tree Protocol, RPVST+)

提示 **如果要将交换机连接到思科网络交换机，典型的默认设置是 PVST+ 而不是 RSTP。为了实现兼容性，必须对其中一台交换机进行修改。**

端口阈值

端口阈值可防止 LAN 中的通信被某个物理接口上的广播、多播或单播风暴打断。端口阈值不适用于带有精简版固件的交换机。

当数据包淹没 LAN 时会发生 LAN 风暴，从而产生过量通信并降低网络性能。协议栈实现中的错误、网络配置错误或用户发起拒绝服务攻击都可能导致风暴。

传入（风暴控制）

传入端口阈值（或通信抑制）可监视从某个接口传送到交换总线的数据包，并确定数据包为单播、多播还是广播。交换机将对 1 秒钟时间间隔内收到的特定类型数据包进行计数，并将测量结果与预定义的抑制级别阈值进行比较。

端口阈值使用以下方法之一来测量通信活动：

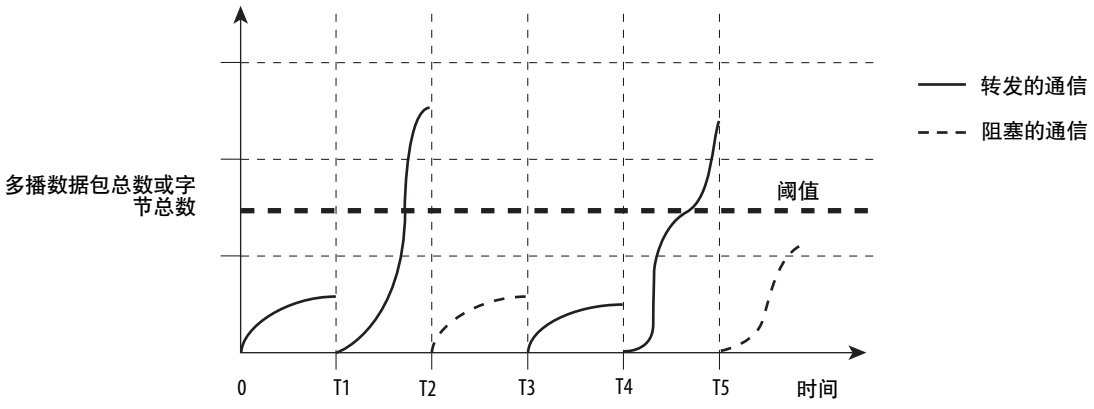
- 广播、多播或单播通信所使用的带宽占端口总可用带宽的百分比。
- 接收广播、多播或单播数据包的通信速率（以每秒数据包数为单位）。
- 接收广播、多播或单播数据包的通信速率（以每秒位数为单位）。

无论采用哪种方法，在达到上升阈值时端口都会阻塞通信。端口将一直保持阻塞状态，直到通信率降至下降阈值以下，然后恢复正常转发。一般来说，级别越高，对广播风暴的防护作用越小。

重要信息　**达到多播通信的端口阈值时，除网络管理通信（如桥接协议数据单元 (BDPU) 和思科发现协议 (CDP)）之外的所有多播通信都将被阻塞。**

下图显示了在一定时期内某接口上的广播通信模式。此示例也适用于多播和单播通信。在此示例中，所转发的广播通信在 T1 到 T2 和 T4 到 T5 这两个时间间隔内超出了配置的阈值。当特定的通信量超出阈值时，所有此类通信在下一时间段内都会被丢弃。因此，在 T2 和 T5 之后的时间间隔内，广播通信会受到阻塞。在下一时间间隔内（如 T3），如果广播通信没有超出阈值，它将被重新转发。

图 2 - 端口阈值示例



风暴控制抑制级别和 1 秒钟时间间隔共同控制了端口阈值算法的工作方式。较高的阈值允许通过较多的数据包。100% 的阈值表示不对通信做任何限制。0.0 的阈值表示端口上的所有广播、多播或单播通信都被阻塞。

重要信息　**由于数据包并不在一致的时间间隔内到达，因此测量通信活动的 1 秒钟时间间隔会影响端口阈值的行为。**

传出（速率限制）

传出端口阈值会以网速百分比（速率限制量占总网速的百分比）的形式限制交换机与客户端设备进行通信的速率。限制特定用户和端口的带宽有助于控制网络拥堵、提高网络性能、构建高效网络并能够防止少数设备独占网络带宽。还可以通过限制不能处理大量通信的终端设备的最大带宽来提高可靠性。在设备管理器 Web 界面或 Logix 设计器应用程序 AOP 中，可启用或禁用每个端口的速率限制。

默认端口阈值配置

默认情况下，将禁用传入单播、广播和多播端口阈值。另外，还将禁用传出端口阈值。

端口安全性

Stratix 5700 交换机可基于 MAC 地址实现端口安全。MAC 地址是分配给每个支持以太网的设备的唯一地址。这意味着，交换机可以强制每个 MAC 地址以动态或静态形式通信。

对于动态端口安全，交换机端口可同时与一定量的设备（MAC 地址）进行通信。端口仅跟踪这些设备的数量，而不会跟踪这些设备的 MAC 地址。静态端口安全会根据 MAC 地址将设备添加到端口安全表中。对于静态端口安全，只有 MAC 地址列于安全表中的设备才能够通过该端口进行通信。

带有完整版固件的 Stratix 5700 交换机的每个端口都可以使用上述一种或两种方法。端口安全性不适用于带有精简版固件的交换机。

动态安全 MAC 地址 (MAC ID)

许多智能端口角色都拥有可使用端口的最大 MAC ID 数。例如，智能端口角色“自动化设备”将端口设置为最多一个 MAC ID。该 MAC ID 是动态的，意味着交换机会认为第一个源 MAC ID 使用该端口。任何其他 MAC ID 尝试访问该端口时都将被拒绝。

如果链路变为不活动状态，交换机将动态地重新获取认为安全的 MAC ID。

在设备管理器 Web 界面或 Logix 设计器应用程序的 Port Security 选项卡上可更改默认的 MAC ID 数。

下表中所示为智能端口角色及其支持的最大 MAC ID 数。

表 5 - 每个智能端口角色支持的最大 MAC ID 数

智能端口角色	最大 MAC ID 数
自动化设备	1
自动化桌面	1
自动化交换机	无限制
自动化路由器	无限制
自动化电话	3

表 5 - 每个智能端口角色支持的最大 MAC ID 数

智能端口角色	最大 MAC ID 数
自动化无线	无限制
多端口自动化设备	无限制
自动化虚拟桌面	2
端口镜像	无限制
无	无限制

静态安全 MAC 地址 (MAC ID)

限制 MAC ID 的另一种方法是在设备管理器 Web 界面的端口安全中定义端口的一个或多个 MAC ID，从而以静态方式配置 MAC ID。这些地址将成为交换机已保存配置的一部分。此方法可实现强大的安全性。但更换与端口连接的设备时，必须重新配置 MAC ID，因为新设备的 MAC ID 与原来的设备不同。

安全侵犯

发生以下任一种情况时视为安全侵犯：

- 已将为某一端口配置的最大数量的安全 MAC 地址添加到地址表中，且 MAC 地址不在该地址表中的站试图访问接口。
- 一个安全接口获取或配置的地址显示在同一 VLAN 中的另一个安全接口上。

当发生安全侵犯时，端口将进入“限制”模式。在此模式下，带有未知源地址的数据包将被丢弃，并且系统会通知您发生了安全侵犯。还会发送一个 SNMP 陷阱，记录一条 syslog 消息，并增加侵犯计数器的计数。

EtherChannel

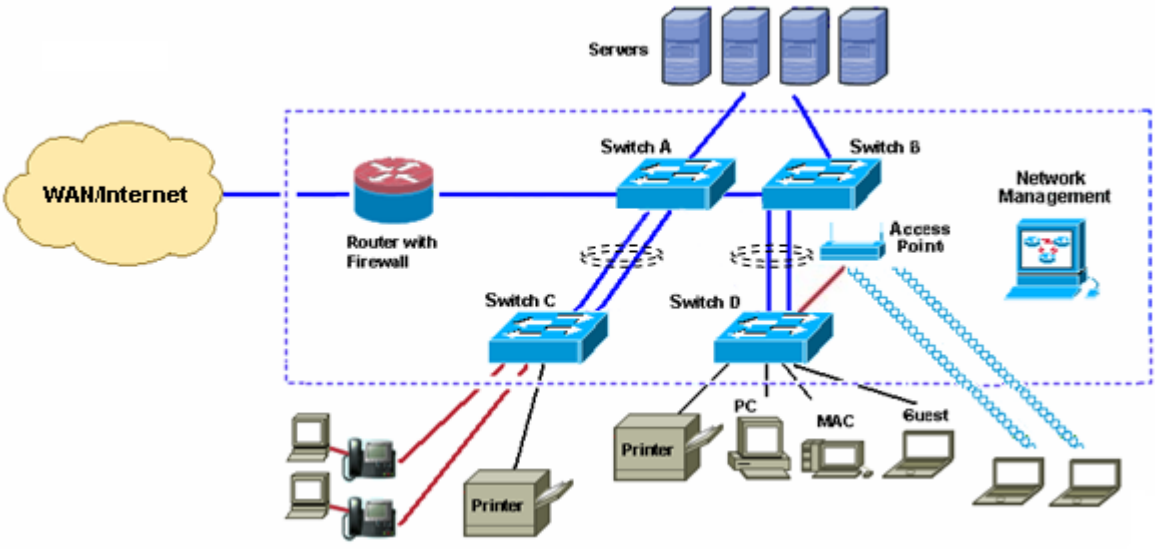
EtherChannel（或端口组）是捆绑为单一逻辑链路的两个或多个高速以太网或千兆以太网交换机端口的组，可在两个交换机之间创建更高带宽的链路。

交换机最多可支持六个 EtherChannel。每个 EtherChannel 最多可包含八个已配置的以太网兼容端口。EtherChannel 不适用于带有精简版固件的交换机。

下图显示了两个 EtherChannel。交换机 A 和 C 上的两个全双工 10/100/1000 Mbps 端口在两个交换机之间创建了一个带宽高达 4 Gbps 的 EtherChannel。同样，交换机 B 和 D 上的两个全双工 10/100 Mbps 端口在两个交换机之间创建了一个带宽高达 400 Mbps 的 EtherChannel。

如果 EtherChannel 中的某个端口不可用，将通过 EtherChannel 中的其余端口来发送通信。

图 3 - EtherChannel 示例



您可在以下任一模式下配置 EtherChannel：

- 端口聚合协议 (PAgP)
- 链路聚合控制协议 (LACP)
- 开启

请在同一模式下配置 EtherChannel 的两端：

- 在 PAgP 或 LACP 模式下配置 EtherChannel 的一端时，系统将与通道的另一端进行协商以确定哪些端口应变为活动状态。不兼容的端口将被挂起。本地端口将被置于独立状态而不是挂起状态，并继续像任何其他单一链路一样传送数据通信。该端口的配置不会发生改变，但该端口也不会参与 EtherChannel。

- 在开启模式下配置 EtherChannel 时，不会进行任何协商。交换机会强制 EtherChannel 中的所有兼容端口变为活动状态。通道的另一端（在另一台交换机上）也必须在开启模式下配置；否则，可能会丢失数据包。

如果 EtherChannel 中的某条链路出现故障，则之前通过该故障链路传送的通信将转移到 EtherChannel 中的其余链路。如果交换机上启用了陷阱，则将发送一个标识了交换机、EtherChannel 和故障链路的故障陷阱。EtherChannel 中某条链路上的入站广播和多播数据包会被阻止在该 EtherChannel 的任何其他链路上返回。

DHCP 持久性

基于 IP 的网络中的每个设备都必须具有唯一的 IP 地址。动态主机配置协议 (DHCP) 会自动将可用地址池中的 IP 地址信息分配给网络中新连接的设备（DHCP 客户端）。如果某个设备离开后又重新加入网络，该设备将收到下一个可用 IP 地址，此地址与其之前的地址可能相同也可能不同。

可将交换机设置为作为 DHCP 服务器运行，从而实现 DHCP 持久性。利用 DHCP 持久性，可以为每个端口分配一个特定的 IP 地址，从而确保连接到给定端口的设备获得同一个 IP 地址。该功能仅适用于与配置为 DHCP 持久性的各个端口连接的单个设备。

重要信息　　为了确保 DHCP 持久性正常工作，请遵循应用规则。

CIP Sync 时间同步（精密时间协议）

IEEE 1588 标准定义了一个名为精密时间协议 (PTP) 的协议，通过该协议可以使测量系统和控制系统的时钟精确同步。我们称其为 CIP Sync 时间同步。时钟通过 EtherNet/IP 通信网络进行同步。PTP 可以使包含不同精度、分辨率和稳定性的时钟的各系统达到同步。PTP 在系统的各个时钟之间生成主从关系。所有时钟的时间最终都会与选作主时钟的时钟一致。

有三种 PTP 模式可供交换机使用：

- 边界时钟
- 透明时钟
- 转发（选择转发模式时将禁用 PTP）

有关这些模式的详细信息，请参见 Converged Plantwide Ethernet Design and Implementation Guide，出版号 ENET-TD001。

默认 PTP 模式为转发模式。

网络地址转换 (NAT)

NAT 是一项服务，它通过 NAT 配置的交换机将一个 IP 地址转换为另一个 IP 地址。当通信在子网间传输时，交换机会转换数据包内的源地址和目标地址。

如果需要在整个网络中重复使用 IP 地址，则可使用此项服务。例如，NAT 可以将在专用子网上共用一个 IP 地址的设备划分到多个完全相同的专用子网，同时在公共子网上保持唯一标识。(1)

在 Stratix 5700 交换机中进行 NAT 可以采用以下不同方式：

- 一对一 NAT — 交换机使用一对一 NAT，而不是一- 对- 多 NAT。一- 对- 一 NAT 要求将各个源地址都转换为唯一的一个目标地址。与一- 对- 多 NAT 不同，多个源地址不能共用同一目标地址。
- 第 2 层实现 — 交换机在第 2 (MAC) 层实现 NAT。在这一层，交换机只能更换 IP 地址，而不会用作路由器。

配置概述

要配置 NAT，需要创建一个或多个特定的 NAT 实例。在典型的实现方式中，只需要一个实例。NAT 实例包含定义每个地址转换的条目以及其他配置参数。

所定义的转换取决于通信是通过第 3 层交换机或路由器还是第 2 层交换机路由。

- 如果通信通过第 3 层交换机或路由器（图 4）路由，可定义以下内容：
  - 对于在专用子网中需要在公共子网进行通信的各个设备的专用到公共转换。
  - 对于第 3 层交换机或路由器的网关转换。

(1) 请注意，这里使用术语“专用”和“公共”来区分位于 NAT 设备任一侧的两种网络。这并非指公共网络一定可通过 Internet 路由。

不需要为专用子网中的所有设备配置 NAT。例如，在实现 NAT 时可以省去一些设备，以增加安全性、减少通信或节省公共地址空间。

重要信息　**作为一项最佳实践，建议您通过第 3 层交换机或路由器路由通信。**

- 如果通信通过第 2 层交换机（图 5）路由，可定义以下内容：
  - 对于在专用子网中需要在公共子网进行通信的各个设备的专用到公共转换。
  - 对于在公共子网中需要在专用子网进行通信的各个设备的公共到专用转换。

图 4 - 第 3 层示例

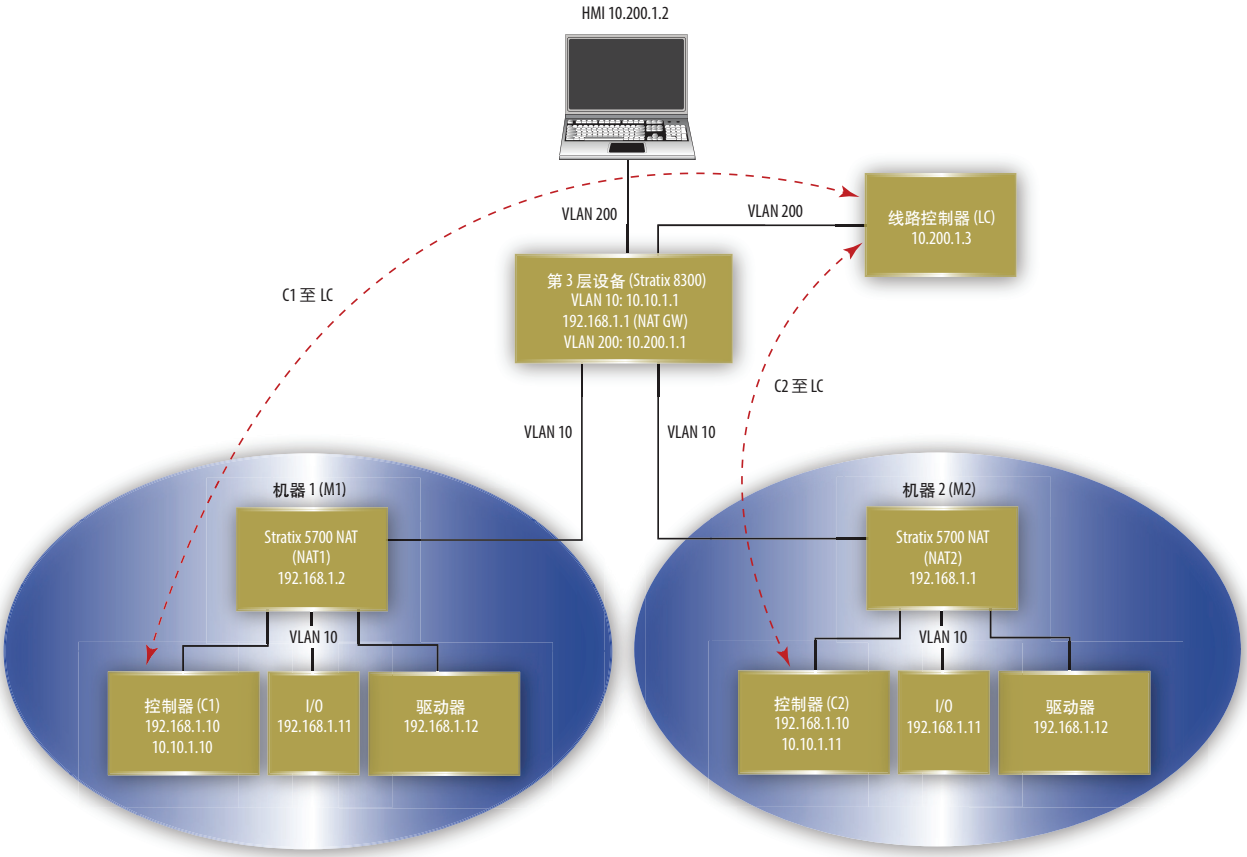
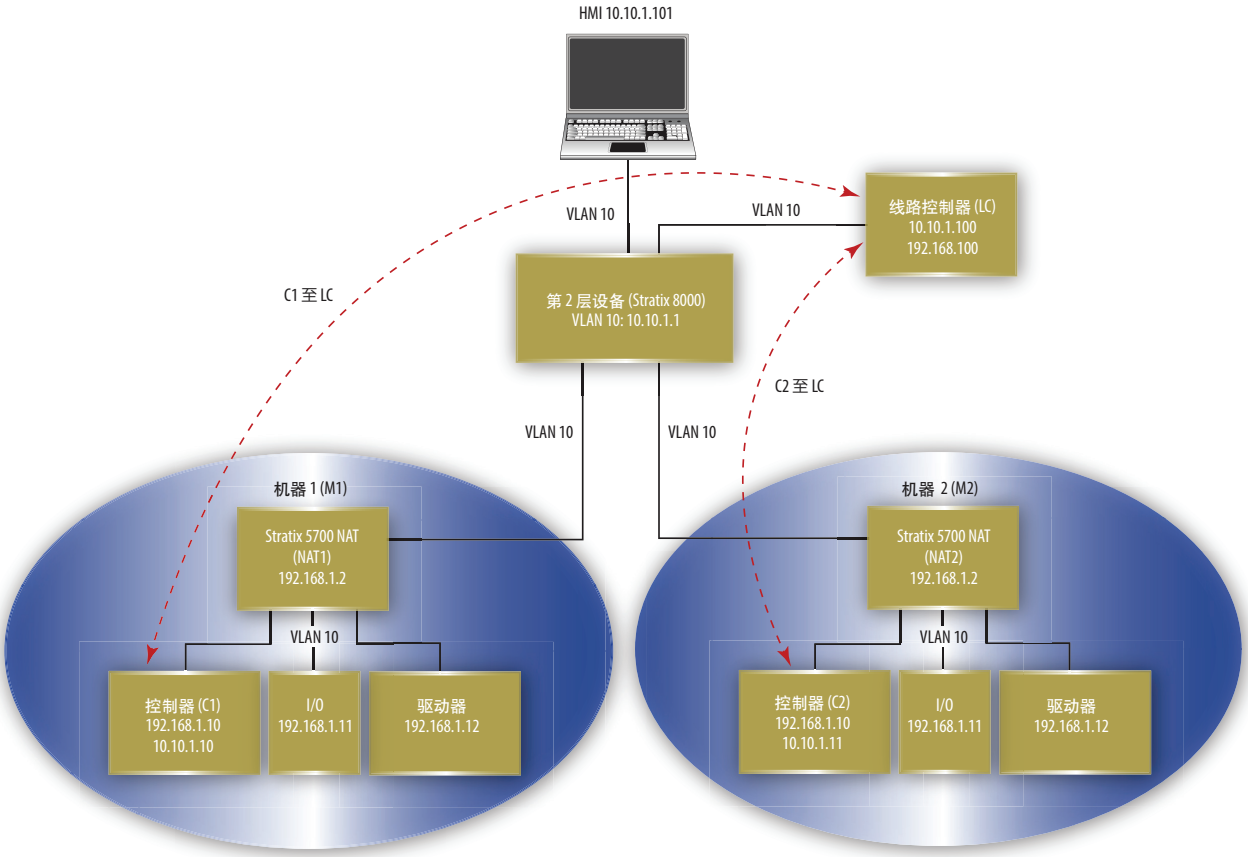


图 5 - 第 2 层示例



地址转换分为三种类型。转换的类型决定转换条目数。一台交换机最多可有 128 个转换条目。

表 6 - 每种转换类型对应的转换条目数

转换类型	转换条目	描述
单个	1	转换单个 IP 地址。 由以下部分组成： • 一个专用 IP 地址 • 一个公共 IP 地址
范围	多个	转换一定范围内的 IP 地址。 由以下部分组成： • 一个起始专用 IP 地址 • 一个起始公共 IP 地址 • 基于指定范围的多个条目
子网	1	转换子网内或部分子网的全部 IP 地址。 由以下部分组成： • 一个起始专用 IP 地址 • 一个起始公共 IP 地址，该地址与有效的子网边界相符 • 子网掩码

示例

以下转换类型视为 10 个转换条目：

- 一个设备的单个转换
- 八个设备的多个转换
- 子网上所有设备的子网转换

对于单个和范围转换类型，转换条目与要转换的地址之间具有一对一的关系。但是，子网转换是一对多的关系，一个转换条目可以对应多个地址。

VLAN 分配

配置 NAT 时，可以将一个或多个 VLAN 分配给一个 NAT 实例。将 VLAN 分配给 NAT 实例时，与该 VLAN 相关的通信受 NAT 实例配置参数的约束。配置参数包括通信是否被转换、修复、阻塞或传送。

重要信息 **创建 NAT 实例前，设置所有的智能端口角色和 VLAN。**

如果为与 NAT 实例关联的端口更改了智能端口角色或本机 VLAN，则必须将 VLAN 重新分配到 NAT 实例。

将 VLAN 分配给 NAT 实例时，请考虑以下内容：

- NAT 支持干线端口和访问端口。
- NAT 不更改 VLAN 标签。
- 最多可以将 128 个 VLAN 分配给一个或多个实例。
- 只要 VLAN 与不同端口相关，就可以将同一个 VLAN 分配给多个实例。例如，只要 VLAN 1 与实例 A 上的端口 Gi1/1 和实例 B 上的端口 Gi1/2 相关，就可以将 VLAN 1 分配给实例 A 和 实例 B。
- 默认情况下，所有 VLAN 都会分配给端口 Gi1/1 上的各个实例，而不会分配给端口 Gi1/2 上的任何实例。

与干线端口相关的 VLAN 可能被分配给 NAT 实例，也可能不会：

- 如果 VLAN 被分配给 NAT 实例，则其通信受 NAT 实例配置参数的约束。
- 如果 VLAN 未被分配给 NAT 实例，则其通信将保持未转换状态，且可始终通过干线端口。

管理界面和 *VLAN*

管理界面可与 VLAN 相关联，该 VLAN 可以被分配给 NAT 实例，也可以未被分配：

- 如果与管理界面相关联的 VLAN 被分配给 NAT 实例，则管理界面在默认情况下位于专用子网。要通过专用子网管理交换机，不需要额外进行配置。要通过公共子网管理交换机，必须配置专用到公共转换。
- 如果与管理界面相关联的 VLAN 未被分配给 NAT 实例，则管理界面的通信将保持未转换状态，且可始终通过该端口。

配置注意事项

配置 NAT 时，请考虑以下准则和限制：

- 交换机只能转换 IPv4 地址。
- 一台交换机最多可有 128 个 NAT 实例、128 个与 NAT 相关的 VLAN 以及 128 个转换条目。一个子网转换仅视为一个转换条目，但包含多个设备的转换。
- 可以在交换机的一个或两个上行端口上配置 NAT。

重要信息　**某些 NAT 配置会导致在专用子网和公共子网上出现超出预期的通信负荷。也可能出现意外的通信。**
NAT 不能替代防火墙。在应用到生产环境之前，请确保进行的配置能够达到性能要求。

由于内置的 IP 地址未修复、IP 地址被加密或使用多播通信，针对 NAT 配置的端口**不**支持跨 NAT 边界的以下内容：

- 通常与 NAT 不兼容的通信加密和完整性检查协议，包括 IPsec 传输模式（1756-EN2TSC 模块）
- 动态发起会话的应用程序（如 NetMeeting）
- 文件传输协议 (FTP)
- 用于开放式平台通信 (OPC) 的 Microsoft 分布式组件对象模型 (DCOM)
- 多播通信，包括使用多播的应用程序，如 CIP Sync (IEEE1588) 和 CLX 冗余

通信许可和修复

尽管 NAT 配置的端口可以转换多种通信类型，但仅支持单播和广播通信。可以选择阻塞或传送 NAT 不支持的以下通信类型：

- 未转换的单播通信
- 多播通信
- IGMP 通信

默认情况下，会阻塞上述所有通信类型。

某些通信类型必须修复才能与 NAT 配合使用，因为其数据包中包括内置的 IP 地址。交换机支持修复以下通信类型：

- 地址解析协议 (ARP)
- Internet 控制消息协议 (ICMP)

默认情况下，ARP 和 ICMP 的修复处于启用状态。

弹性以太网协议

弹性以太网协议 (REP) 为生成树协议 (STP) 提供了一种控制网络环网与环路、处理链路故障和改进收敛时间的备选方法。REP 可控制一组连接到同一网段的端口，确保该网段不会产生任何桥接环路，并对网段中的链路故障作出响应。REP 为构造更复杂的网络提供了基础，并且支持 VLAN 负载平衡。

REP 是一种网段协议。一个 REP 网段是一连串相互连接并配置了同一网段 ID 的端口。每个网段都由标准（中转）网段端口和两个用户配置的边缘端口组成。一台交换机不能包含两个以上属于同一网段的端口，而且每个网段端口只能有一个外部邻居。网段可通过共享介质实现，但在任何链路上只有两个端口可以属于同一网段。REP 仅在第二层干线接口上受支持。选择“自动化交换机”智能端口将启用第二层干线。EtherChannel 支持 REP，但属于 EtherChannel 的单个端口不支持 REP。

基于 REP 网段可以构造几乎任何类型的网络。REP 还支持 VLAN 负载平衡，该功能由主要边缘端口控制，但可在网段中的任意端口起作用。

在设备管理器 Web 界面中可选择以下类型的 REP 端口：

- Primary — 此端口为主要边缘端口。此端口始终参与 REP 网段中的 VLAN 负载平衡。
- Edge — 此端口为次要边缘端口。此端口也参与 REP 网段中的 VLAN 负载平衡。

  边缘端口为 REP 网段的端点。用户必须为每个 REP 网段配置两个边缘端口，其中包括一个主要边缘端口。只输入“边缘”不输入“主要”会将端口配置为次要边缘端口。即使不需要 VLAN 平衡的支持，也必须配置主要和次要边缘端口。
- Transit — 此端口为 REP 网段中的非边缘端口。
- No-Neighbor Primary — 此端口为连接到非 REP 交换机的主要边缘端口。
- No-Neighbor — 此端口为连接到非 REP 交换机的次要边缘端口。

  无邻边缘端口具有常规边缘端口的所有属性。这些端口可用于构造包含不支持 REP 协议的交换机的 REP 环网。
- None — 此端口不在 REP 网段中。

REP 和 STP 可在同一台交换机上共存，但无法在同一个端口上共存。REP 不与 STP 发生交互。例如，如果将某个端口配置为 REP 端口，则在该端口上将禁用 STP。在 REP 端口上不接受也不发送 STP 桥接协议数据单元 (BPDU)。但是，相邻的 REP 和 STP 环网或域可共享一条共有链路。该共有链路可用于传送 REP 和 STP 数据面通信，或用于 STP 控制面通信。

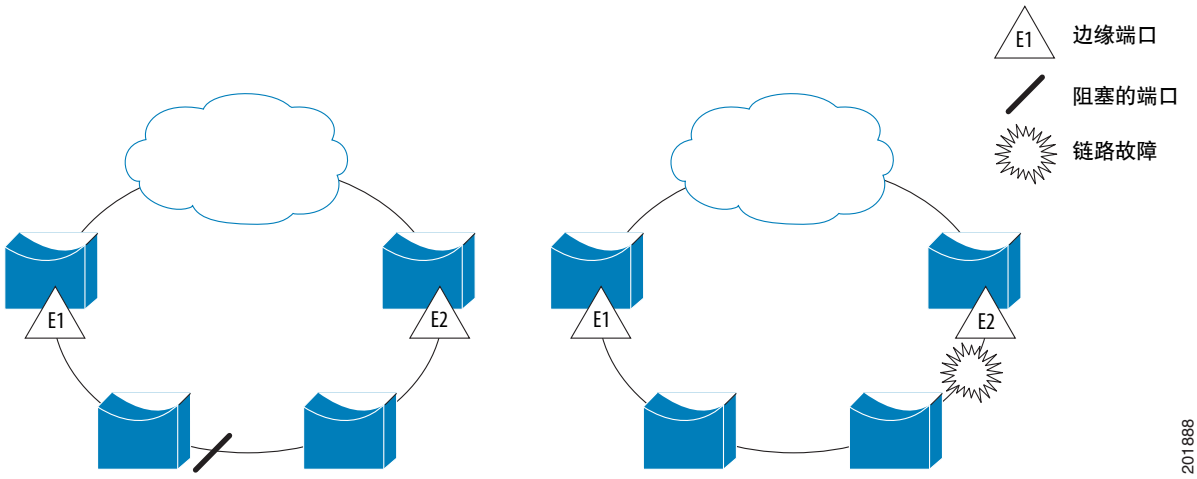
图 6 显示了一个网段示例，其中包含六个分布于四台交换机的端口。端口 E1 和 E2 被配置为边缘端口。所有端口正常运作时（如左侧网段所示），单个端口处于阻塞状态，用斜线表示。网络中出现故障时（如右侧网段所示），阻塞的端口将返回到转发状态以最大限度地减少网络中断。

REP 开放网段

图 6 中显示的网段为开放网段。在两个边缘端口之间没有任何连接。REP 网段不会导致桥接环路，将网段边缘端口连接到任何网络都是安全的。连接到网段中交换机的所有主机都可以有两种方式通过边缘端口连接到网络的其余部分，但任何时候都只能使用一个连接。如果故障导致主机无法访问其常用网关，REP 将开启所有端口以确保可通过另一个网关实现连接。

在以下示例中，E1 或 E2 可被配置为主要边缘端口。

图 6 - 开放网段示例

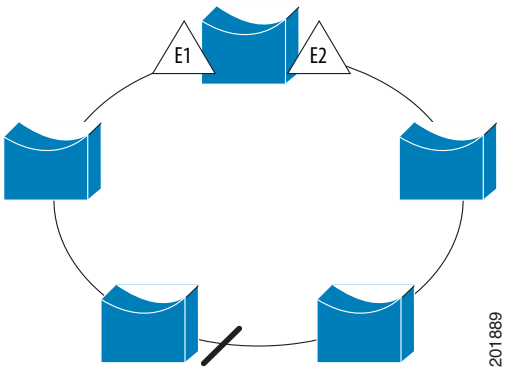


REP 环型网段

图 7 中所示的网段为环型网段，其中两个边缘端口位于同一台交换机上。在此配置中，边缘端口之间通过网段连接。使用此配置，可在网段中的任意两台交换机之间创建冗余连接。

在下图中，E1 或 E2 可被配置为主要边缘端口。

图 7 - 环型网段示例



REP 网段具有以下特征：

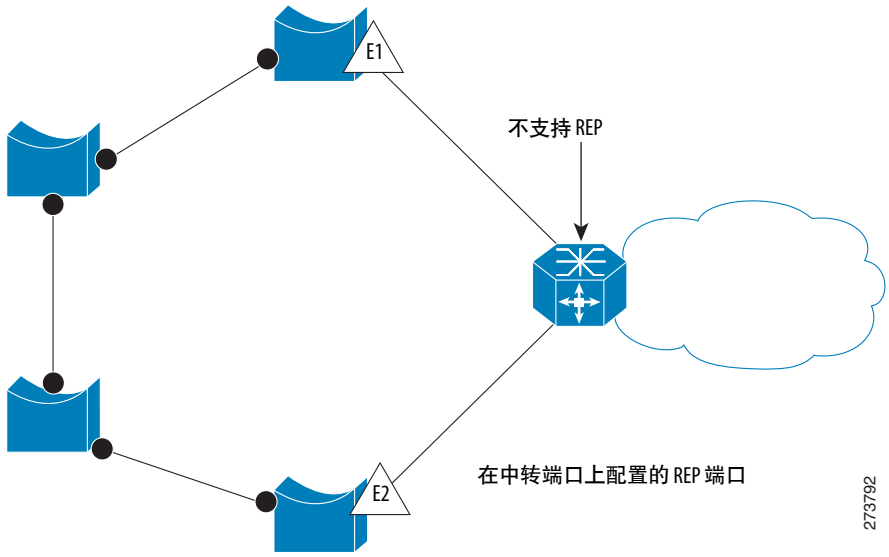
- 如果网段中的所有端口都正常运行，则每个 VLAN 中都有一个端口（称为备用端口）处于阻塞状态。
- 如果已配置 VLAN 负载平衡，则网段中的两个端口控制 VLAN 的阻塞状态。
- 如果网段中有一个或多个端口不能正常运行而导致链路故障，则所有端口将转发所有 VLAN 中的通信以支持持续的连通性。
- 发生链路故障时，备用端口会尽快开启。当故障链路恢复正常后，将以尽量减少网络中断为前提在每个 VLAN 中选择一个端口从逻辑上进行阻塞。

接入环网拓扑

在接入环网拓扑中，相邻交换机可能不支持 REP，如图 8 所示。在这种情况下，可以将不面向 REP 的端口（E1 和 E2）配置为非邻边缘端口。这些端口继承了边缘端口的所有属性，可以像配置任何边缘端口一样对它们进行配置，包括将它们配置为向聚合交换机发送 STP 或 REP 拓扑变更通知。在这种情况下，发送的 STP 拓扑变更通知 (TCN, topology change notice) 为多生成树 (MST) STP 消息。

在以下示例中，E1 或 E2 可被配置为主要非邻端口。

图 8 - 环型拓扑示例



REP 具有以下限制：

- 必须配置每个网段端口；错误的配置会导致网络中出现转发环路。
- REP 只能管理网段中的单个故障端口； REP 网段中的多个端口发生故障会导致失去网络连通性。

只在带冗余的网络中配置 REP。在不带冗余的网络中配置 REP 会导致失去连通性。

链路完整性

REP 并不在边缘端口之间使用端到端轮询机制来验证链路完整性。它执行本地链路故障检测。REP 链路状态层 (LSL, Link Status Layer) 会检测 REP 感知的相邻端口并在网段中建立连接。在检测到相邻端口之前，接口上的所有 VLAN 都会被阻塞。识别相邻端口后，REP 会确定哪些相邻端口成为备用端口，哪些端口转发通信。

网段中的每个端口都具有唯一的端口 ID。端口 ID 格式与生成树算法所使用的格式相似：端口编号（在网桥中唯一），与 MAC 地址（在网络中唯一）相关联。要使用某个网段端口时，其 LSL 将开始发送包含网段 ID 和端口 ID 的数据包。当该端口与同一网段中的相邻端口进行三向握手后，即被声明为正常运行。

SNMP

交换机支持简单网络管理协议 (SNMP, Simple Network Management Protocol) 版本 1、2C 和 3。SNMP 允许通过其他网络管理软件远程管理交换机。默认情况下禁用此功能。

SNMP 基于以下三个概念：

- SNMP 管理器（客户端软件）
- SNMP 代理（网络设备）
- 管理信息库 (MIB)

请参见第81 页上的支持的 MIB，了解有关交换机支持的 MIB 的信息。

SNMP 管理器运行 SNMP 管理软件。要管理的网络设备（例如网桥、路由器、服务器和工作站）都具有一个代理软件模块。通过代理可访问对象的本地 MIB，该 MIB 反映了设备的资源和活动。代理还会对管理器从 MIB 检索值和在 MIB 中设置值的命令作出响应。代理和 MIB 都在交换机上。要在交换机上配置 SNMP，需定义管理器和代理之间的关系。

SNMPv1 和 v2C 都使用基于社区的安全形式。SNMP 管理器可通过被称为社区字符串的密码来访问代理 MIB。SNMPv1 和 v2C 通常用于不进行网络控制的网络监视。

SNMPv3 实现网络监控。它通过验证和加密网络上的数据包，提供对设备的安全访问权限。SNMPv3 使用的安全模型是为用户和用户组建立的验证策略。安全级别是指安全模型中允许的安全级别。安全模型和安全级别共同决定了用于 SNMP 数据包的安全机制。

以下是有关 SNMPv3 对象的一些准则：

重要信息　SNMPv.3 仅在加密版本的交换机固件中可用。

- 每个用户都属于一个组。
- 组用于定义一组用户的访问策略。
- 访问策略用于定义可访问哪些 SNMP 对象进行读、写和创建等操作。

- 组用于确定其用户可接收的通知列表。
- 组还用于定义其用户的安全模型和安全级别。
- SNMP 视图是组可以访问的 MIB 列表。
- 可以从 SNMP 设备中安全地收集数据，而不必担心数据被篡改或被损坏。
- 可以对机密信息（例如更改路由器配置的 SNMP Set 命令数据包）进行加密以防止其内容暴露在网络上。

支持的 MIB

Stratix 5700 交换机支持以下 MIB。

表 7 - 支持的 MIB

MIB 名称		
BRIDGE-MIB	CISCO-MEMORY-POOL-MIB	IP-MIB
CALISTA-DPA-MIB	CISCO-PAE-MIB	LLDP-EXT-MED-MIB
CISCO-ACCESS-ENVMON-MIB	CISCO-PAGP-MIB	LLDP-MIB
CISCO-ADMISSION-POLICY-MIB	CISCO-PING-MIB	NETRANGER
CISCO-AUTH-FRAMEWORK-MIB	CISCO-PORT-QOS-MIB	NOTIFICATION-LOG-MIB
CISCO-BRIDGE-EXT-MIB	CISCO-PORT-SECURITY-MIB	OLD-CISCO-CHASSIS-MIB
CISCO-BULK-FILE-MIB	CISCO-PORT-STORM-CONTROL-MIB	OLD-CISCO-CPU-MIB
CISCO-CABLE-DIAG-MIB	CISCO-PRIVATE-VLAN-MIB	OLD-CISCO-FLASH-MIB
CISCO-CALLHOME-MIB	CISCO-PROCESS-MIB	OLD-CISCO-INTERFACES-MIB
CISCO-CAR-MIB	CISCO-PRODUCTS-MIB	OLD-CISCO-IP-MIB
CISCO-CDP-MIB	CISCO-RESILIENT-ETHERNET-PROTOCOL-MIB	OLD-CISCO-MEMORY-MIB
CISCO-CIRCUIT-INTERFACE-MIB	CISCO-RTTMON-ICMP-MIB	OLD-CISCO-SYS-MIB
CISCO-CLUSTER-MIB	CISCO-RTTMON-IP-EXT-MIB	OLD-CISCO-SYSTEM-MIB
CISCO-CONFIG-COPY-MIB	CISCO-RTTMON-MIB	OLD-CISCO-TCP-MIB
CISCO-CONFIG-MAN-MIB	CISCO-RTTMON-RTP-MIB	OLD-CISCO-TS-MIB
CISCO-DATA-COLLECTION-MIB	CISCO-SNMP-TARGET-EXT-MIB	RMON-MIB
CISCO-DHCP-SNOOPING-MIB	CISCO-STACK-MIB	RMON2-MIB
CISCO-EMBEDDED-EVENT-MGR-MIB	CISCO-STACKMAKER-MIB	SMON-MIB
CISCO-ENTITY-ALARM-MIB	CISCO-STP-EXTENSIONS-MIB	SNMP-COMMUNITY-MIB
CISCO-ENTITY-VENDORTYPE-OID-MIB	CISCO-SYSLOG-MIB	SNMP-FRAMEWORK-MIB
CISCO-ENVMON-MIB	CISCO-TCP-MIB	SNMP-MPD-MIB
CISCO-ERR-DISABLE-MIB	CISCO-UDLDP-MIB	SNMP-NOTIFICATION-MIB
CISCO-FLASH-MIB	CISCO-VLAN-IFTABLE-RELATIONSHIP-MIB	SNMP-PROXY-MIB
CISCO-FTP-CLIENT-MIB	CISCO-VLAN-MEMBERSHIP-MIB	SNMP-TARGET-MIB
CISCO-IF-EXTENSION-MIB	CISCO-VTP-MIB	SNMP-USM-MIB
CISCO-IGMP-FILTER-MIB	ENTITY-MIB	SNMP-VIEW-BASED-ACM-MIB
CISCO-IMAGE-MIB	ETHERLIKE-MIB	SNMPv2-MIB
CISCO-IP-STAT-MIB	HC-RMON-MIB	TCP-MIB
CISCO-LAG-MIB	IEEE8021-PAE-MIB	UDP-MIB
CISCO-LICENSE-MGMT-MIB	IEEE8023-LAG-MIB	
CISCO-MAC-AUTH-BYPASS-MIB	IF-MIB	
CISCO-MAC-NOTIFICATION-MIB	IP-FORWARD-MIB	

端口镜像

端口镜像适用于对解决网络通信和协议问题有一定经验的高级用户。端口镜像功能将一个端口上的通信复制（或镜像）到另一个可通过网络协议分析器工具捕获数据包的监视端口。将端口镜像作为诊断工具或调试功能使用。

端口镜像不会影响被监视端口上的网络通信交换。必须将一个监视端口专门用于端口镜像。除了为端口镜像对话而复制的通信，监视端口不会接收或转发通信。

可以通过设备管理器 Web 界面将“端口镜像”智能端口角色分配给某个交换机端口，来配置端口镜像。

路由

交换机支持以下形式的路由：

- 静态路由—定义两个设备（路由和交换机）间的显式路径。必须手动定义路由信息，包括目标 IP 地址、目标子网掩码和下一跳路由器 IP 地址。
- 直连路由 — 如果任意 VLAN 中使用交换机进行彼此间通信的所有设备将交换机用作默认网关，则启用这些设备。如果启用静态路由，则会自动启用直连路由。要禁用直连路由并防止 VLAN 间进行通信，必须使用 CLI 配置访问控制列表 (ACL)。

在设备管理器 Web 界面中，启用路由分为如下两步：

1. 通过将交换机数据库管理 (SDM) 模版从默认模版更改为基于局域网的路由模版，为路由重新分配交换机内存。
2. 仅启用直连路由。

   或

   启用并配置静态路由，默认情况下，会启用直连路由。

配置管理

交换机可将其配置存储在内部存储器或外部 SD 卡中。默认情况下，SD 卡的优先级始终高于内部存储器。如果在 SD 卡上具有有效的 IOS 映像和配置文件，且在插入 SD 卡的情况下启动交换机，则交换机会从 SD 卡加载这些文件。

通常，交换机的启动方法会成为存储对配置所做任何更改的源。例如，如果通过 SD 卡启动交换机，则所有更改都会保存在 SD 卡中。如果通过内部存储器启动交换机，则即使在启动系统过程中插入了 SD 卡，所做的更改也会保存在内部存储器中。要确定启动方法，可在设备管理器 Web 界面中单击 SD Sync 选项卡。

配置文件（config.text 和 vlan.dat）的格式为可读的 ASCII 格式。可以通过下列方法之一将文件下载到计算机：

- FTP
- AOP
- 使用计算机读取 SD 卡

您也可以在 Logix 设计器应用程序中，将配置文件作为控制器项目的一部分进行存储。

设备管理器 Web 界面用于自动或根据需要同步 IOS 映像和配置文件。

SD 卡同步

SD 卡同步功能可用于将 SD 卡与板载闪存同步。您可以同步配置文件或 IOS 映像。如果存在 SD 卡，则交换机从 SD 卡启动，并具有相应配置。如果不存在 SD 卡，则交换机会从内部存储器存储的指定 IOS 映像中读取启动参数。

重要信息 如果同步的方向错误，您可以覆盖所需的配置。

报警

最多可以在系统环境中连接来自外部设备的两个报警输入（如门或温度计）连接到交换机前面板上的报警输入端口。输出报警触点可使用 CLI 进行配置。默认输出也可由超温报警、欠温报警或未处于转发状态的端口所触发。输出报警继电器可使用 CLI 配置为常励磁或非常励磁电路。

加密 IOS 软件 （可选）

Stratix 5700 加密 IOS（可作为独立的目录号下载）通过在 Telnet 和 SNMP 会话中加密管理员通信来确保网络安全。该加密 IOS 支持标准 IOS 的所有功能以及如下协议：

- 安全外壳 (SSH) 协议 v2
- SNMPv3
- HTTPS

电缆诊断

电缆诊断功能用于对交换机的各端口进行测试，以确定与 RJ45（电口）端口相连的电缆是否完好。此功能对光口不适用。

测试可确定每条电缆断开处到交换机的距离，并分别列有正负误差值。

高级软件功能

交换机还具有更高级的软件功能，其中一些要通过本手册介绍的全局宏或用于典型自动化应用的智能端口来进行配置。

有关如何对设备管理器 Web 界面或 Logix 设计器应用程序未提供的功能进行配置的信息，请参见以下手册：

- Cisco IE2000 Switch Software Configuration Manual，可从 http://www.Cisco.com 获取。
- Cisco IE2000 Switch Command-Line Interface Manual，可从 http://www.Cisco.com 获取。

注：

通过设备管理器 Web 界面管理交换机

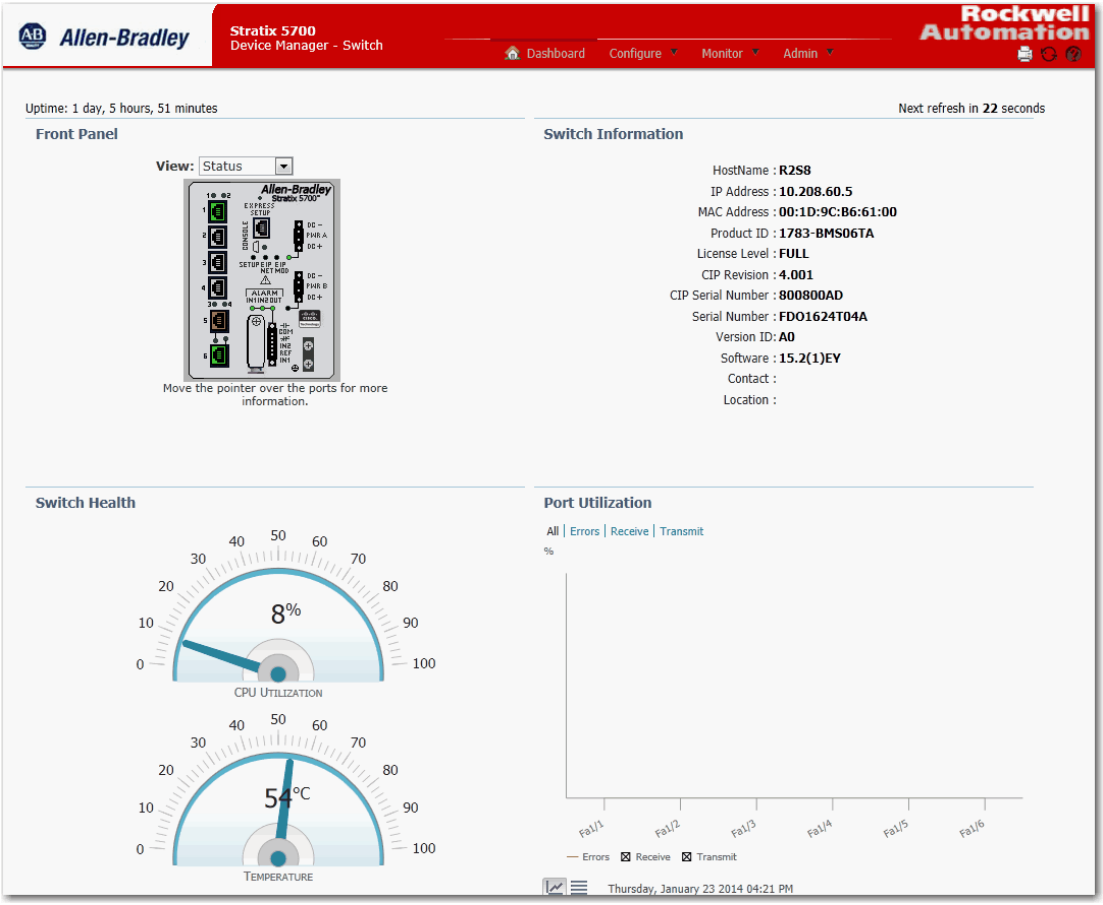
完成快速设置后，可以使用交换机附带的设备管理器 Web 界面管理交换机。

为简单起见，本章中的大部分插图显示的都是 6 端口交换机。

访问设备管理器 Web 界面

要访问设备管理器 Web 界面，请按以下步骤操作。

1. 启动工作站上的 Web 浏览器。
2. 在 Web 浏览器中输入交换机 IP 地址，然后单击 Enter。
3. 输入用户名和密码。



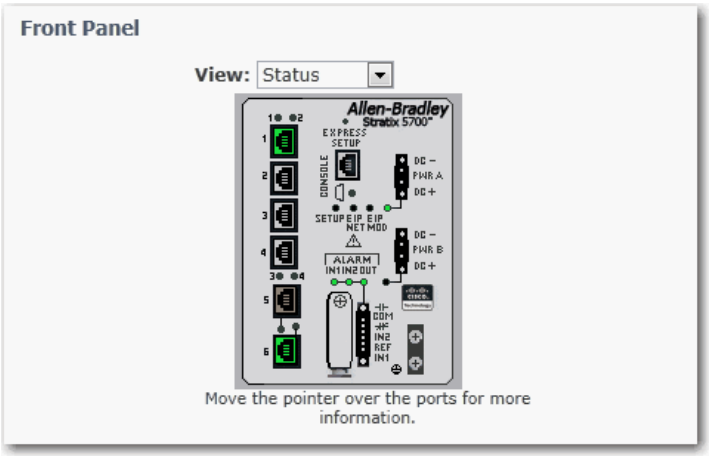
操控板概述

可以使用操控板监视交换机的状态和性能。

Dashboard 窗口与 Monitor > Trends 窗口类似。Dashboard 窗口显示瞬时状态，而 Trends 窗口则显示历史状态。将两者结合使用，可收集交换机及其端口的详细情况。有关 Trends 窗口的详细信息，请参见第 127 页。

前面板和状态指示灯

Front Panel 视图为交换机前面板的图形画面。



前面板视图上的交换机元件按状态进行颜色编码。通过颜色可快速了解是否存在故障或错误情况。前面板视图上显示的系统- 级状态指示灯和端口级状态指示灯对应于交换机上的指示灯。

表 8 - 前面板状态指示灯

指示灯	状态	描述
EIP Mod	EIP Mod 状态指示灯显示交换机的状态。	
	熄灭	交换机电源断开或连接不当。
	绿色常亮	交换机正常运行。
	绿色闪烁	未配置交换机（例如，交换机未配置 IP 地址）。
	红色闪烁	交换机检测到可恢复的系统故障。
	红色常亮	交换机检测到不可恢复的系统故障。
	红色和绿色交替闪烁	交换机正在运行上电自检 (POST)。
DC_A DC_B	熄灭	交换机电源断开或连接不当。
	绿色常亮	关联电路已通电。
	红色常亮	关联电路未通电，并且交换机配置为采用双输入电源。
Alarm Out	熄灭	未配置报警输出，或交换机已关闭。
	绿色常亮	已配置报警输出；但未检测到报警。
	红色闪烁	交换机检测到主要报警。
Alarm In 1 Alarm In 2	熄灭	未配置报警输入。
	绿色常亮	已配置报警输入；但未检测到报警。
	红色闪烁	检测到主要报警。
	红色常亮	检测到次要报警。
Setup	熄灭	交换机已被配置为管理型交换机。
	绿色常亮	交换机正在进行初始设置。
	绿色闪烁	交换机正在进行初始设置、故障恢复，或者初始设置未完成。
	红色常亮	由于没有可用于连接管理站的交换机端口，交换机启动初始设置或恢复失败。断开交换机端口上连接的设备，然后按下交换机上的 Express Setup 按钮。
Ports — 每个组合端口上有两个状态指示灯：一个用于 SFP 模块，一个用于 RJ45 连接器。活动端口对应的指示灯将激活。		

表 8 - 前面板状态指示灯 （续）

指示灯	状态	描述
	熄灭	端口上没有链路。
	绿色常亮	端口链路；无活动。
	绿色闪烁然后熄灭	链路处于正常的活动状态。
	绿色和琥珀色交替闪烁	链路存在故障或错误。
	琥珀色常亮	端口已禁用。
EIP Net—EIP Net 状态指示灯显示交换机的网络状态。		
	熄灭	交换机电源断开或连接不当。
	绿色常亮	交换机已与一个或多个相连的设备建立 CIP 连接。
	绿色闪烁	交换机具有 IP 地址，但未与任何相连的设备建立连接。
	红色闪烁	与一个或多个相连设备的连接超时。
	红色常亮	交换机检测到其 IP 地址已经被网络中的另一设备使用。
	红色和绿色交替闪烁	交换机正在运行上电自检 (POST)。
Status — 在该模式下，端口状态指示灯显示端口状态。此为默认模式。		
	熄灭	无链路。
	绿色常亮	链路上无活动。
	绿色闪烁	链路上存在活动。
	棕色常亮	端口已禁用。
	黄色	错误已禁用该端口。
	绿色和琥珀色交替闪烁	链路故障。
	琥珀色闪烁	智能端口配置与端口不匹配。
	琥珀色常亮	端口存在故障、因错误而禁用，或处于 STP 阻止状态。
Smartports — 该模式下，各端口映像显示应用的端口角色。有关智能端口的详细信息，请参见第 59 页上的通过智能端口角色优化端口。		

可以通过从前面板视图上的 View 列表中选择一个端口模式来更改端口状态指示灯的行为。

将鼠标指针移动到端口上即可显示该端口及其状态的特定信息。

提示　**如果将指针移动到绿色和黄色交替闪烁的端口上方，可能为以下状态中的一种：**
- **链路存在故障**
- **链路存在冲突**

任意状态下，端口都可接收和发送通信。

注意以下事项：

- 只有设备与端口相连后才会显示端口的速度和双工模式。
- 对于两用端口，无论端口是否处于活动状态，Type 字段均显示上行电口为 10/100/1000BaseTX。Type 字段还显示已安装的 SFO 模块的类型，如果未安装模块，将显示 Empty。
- 选择智能端口模式后将显示智能端口类型和 VLAN 类型及名称。
- Uptime 字段显示交换机自上次接通电源或重启以来的运行时间。状态每隔 60 秒会自动刷新，也可单击 Refresh 手动刷新。刷新计数器显示下一个刷新周期开始前剩余的秒数。

交换机信息

Dashboard 上的 Switch Information 区域显示交换机的相关信息，如下表中所述。

字段	描述
Host Name	该交换机的描述性名称。默认名称为 Switch。可以在 Admin > Express Setup 窗口中设置该参数。
IP Address	该交换机的 IP 地址。可以在 Admin > Express Setup 窗口中配置该设置。
MAC Address	该交换机的 MAC 地址。此信息无法更改。
Product ID	该交换机的型号。此信息无法更改。
License Level	安装的许可证的类型。此信息无法更改。
CIP Revision	该交换机上支持的通用工业协议 (CIP) 的版本。此信息无法更改。
CIP Serial Number	CIP 序列号。此信息无法更改。
Serial Number	该交换机的序列号。此信息无法更改。
Version ID	硬件版本。此信息无法更改。
Software	该交换机上运行的 IOS 的版本。升级交换机固件后，该信息将更新。
Contact	该交换机的管理联系人。可以在 Configure > SNMP 窗口中设置该参数。
Location	该交换机的物理位置。可以在 Configure > SNMP 窗口中设置该参数。

交换机运行状态

可以使用以下运行状态状态测量表监视交换机。

CPU 利用率

CPU 利用率量表显示交换机使用的 CPU 处理能力百分比。每 60 秒刷新一次系统时会采集数据。当交换机上存在设备通过网络发送数据的网络活动时，量表的示数将发生变化。随着网络活动的增加，设备之间通过网络发送数据的连接也会增加。

监视交换机的使用率时，注意观察给定网络活动时间内的使用百分比与预期值是否相同。如果利用率高于预期值，可能存在问题。监视交换机时，注意带宽利用率是否持续偏高。如果持续偏高，可能意味着网络出现拥堵。如果交换机达到最大带宽（利用率超过 90%）且缓冲区已满，交换机将开始丢弃接收到的数据包。网络中有有一些数据包丢失是正常现象，而且交换机的配置也可以帮助恢复丢失的数据包，例如向其它设备发送重发数据的信号。不过，大量数据包丢失可能导致数据包错误，进而降低整体网络性能。

为减少拥堵，可以考虑将网络分为多个子网，并使用其它交换机或路由器连接子网。查找其它原因，例如可能会引起交换机带宽利用率上升的故障设备或连接。

温度

温度量表显示交换机的内部温度。有关交换机温度范围和工作环境准则的详细信息，请参见 Stratix Ethernet Device Specifications Technical Data，出版物 1783-TD001。

端口利用率

可以选择要显示的网络通信类型和显示格式：

- 通信类型 — 默认情况下，将显示所有接口的所有通信。单击显示区域上方的链接将显示所有通信、错误、接收到的通信和已发送的通信。
- 格式 — 单击显示区域下方的按钮可以图标模式或网格模式查看数据。
- 图表详情 — 显示图表时，将鼠标指针放到条上或图表的一点上即可查看数据。

监视端口的使用情况时，注意观察给定网络活动时间内的百分比与预期值是否相同。如果利用率高于预期值，可能存在问题。也可以根据连接在半双工还是全双工模式下运行来分配带宽。

交换机端口接收或发送数据时出现错误的部分原因如下：

- 电缆连接不当
- 端口故障
- 软件问题
- 驱动程序问题

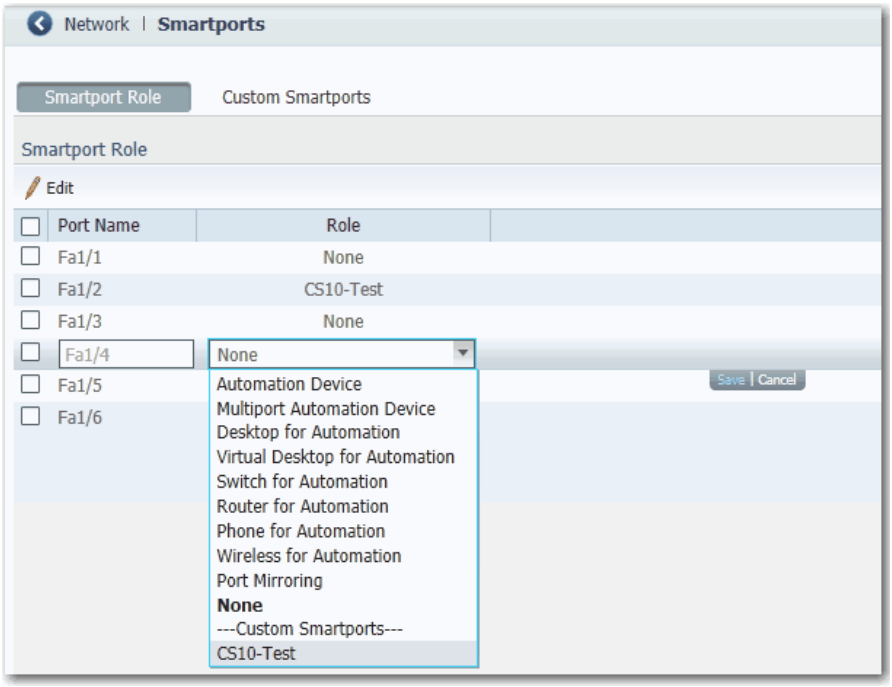
每 60 秒刷新一次系统时会采集数据。

请参见第 127 页上的监视趋势中的图示，查看各端口随时间增量实例（60 秒、1 小时、1 天或 1 周）的变化情况。

有关各端口上检测到的特定端口错误的详细信息，请参见第 128 页上的监视端口统计。

配置智能端口

要为交换机端口分配智能端口角色，从 Configure 菜单中选择 Smartports。



使用智能端口角色时，需遵循以下准则：

- 使用智能端口角色前，确定交换机端口要连接到的设备类型。
- 将设备与端口相连或重新连接已移动的设备前，验证端口上应用的智能端口角色。

重要信息	我们建议您在启用端口的智能端口角色后不要再更改端口设置。任何端口设置的更改都可能改变智能端口角色的有效性。

- 当用户试图在 Smartport 窗口中将端口角色应用于路由端口时，将显示以下错误消息：

  无法在路由端口上配置端口角色。

要应用智能端口角色，按以下步骤操作。

1. 从 Configure 菜单中，选择 Smartports。
2. 选择一个端口。
3. 从 Role 列的下列菜单中选择一个智能端口角色。
4. 单击 Save。

自定义端口角色属性

每个交换机端口都是一个 VLAN 成员。与属于同一 VLAN 的交换机端口相连的设备共享相同的数据广播和系统资源。

根据网络要求，将所有端口分配给名称为 default 的默认 VLAN 可能就已足够。小型网络中一个 VLAN 即可满足要求。

更改虚拟局域网 (VLAN) 成员资格前，需了解 VLAN 的概念、目的和创建方法。有关 VLAN 的详细信息，请参见第 64 页。

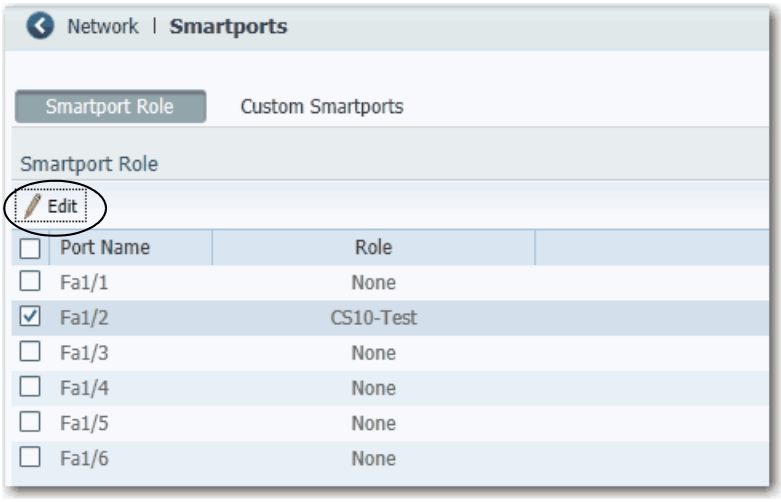
将端口分配到 *VLAN*（*VLAN* 成员资格）

每个交换机端口都是一个 VLAN 成员。与属于同一 VLAN 的交换机端口相连的设备共享相同的数据广播和系统资源。在 VLAN 间通信需要使用第 3 层设备（如路由器或第 3 层交换机）。

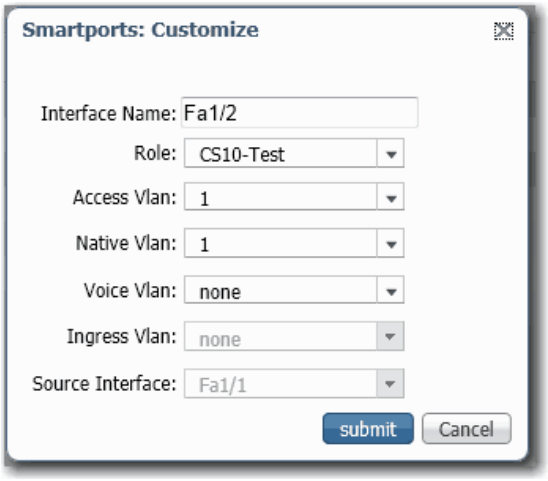
根据网络要求，将所有端口分配给名称为 default 的默认 VLAN 可能就已足够。如果已创建其它 VLAN，则必须确定端口最适合的 VLAN。

要更改 VLAN 分配，按以下步骤操作。

1. 从 Configure 菜单中，选择 Smartports。
2. 选中端口旁边的复选框来更改 VLAN。
3. 单击 Edit。



4. 根据需要修改 VLAN 分配：
   - 对于应用支持 QoS 的 Automation Device、 Switch For Automation、Router For Automation 或 Wireless For Automation 端口角色的端口，从 Native VLAN 列表中选择一个 VLAN。
   - 对于应用 Automation Device、Desktop For Automation、Phone For Automation 或 None 端口角色的端口，从 Access VLAN 列表中选择一个 VLAN。
   - 对于应用 Phone For Automation 端口角色的端口，从 Voice VLAN 列表中选择一个 VLAN。
   - 对于应用 Port Mirroring 端口角色的端口，从 Ingress VLAN 列表中选择一个 VLAN，并从 Source Interface 列表中选择要监视的端口。



5. 单击 Submit。

管理自定义的智能端口宏

要创建一个自定义的智能端口宏，按以下步骤操作。

1. 单击 Custom Smartports 选项卡。
2. 单击 Add。
3. 输入宏的名称。

   宏名称区分大小写。该字符串最多包含 31 个字母数字字符。字符串不可包含问号、空格或制表符。
4. 选择宏图标（CS1 到 CS10）。
5. 输入宏定义。

   定义中最多可包含 3000 个字符。输入宏命令，每行一个命令。要在宏中输入注释文本，需在行的开头使用 # 字符。

   可用的宏参数有 $native_vlan、$access_vlan 和 $voice_vlan
6. 输入一个反宏定义。

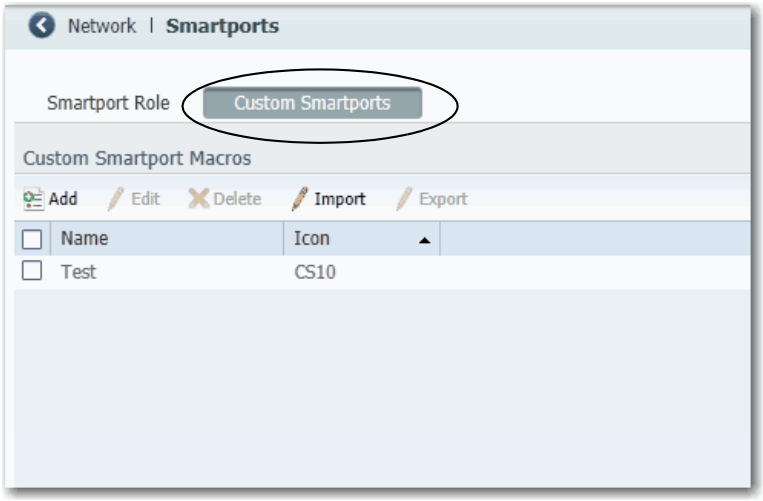
   反宏定义是所应用宏的一部分，当您改为其它宏或通过 None 智能端口角色将宏删除时，反宏会将宏删除。在将宏定义应用到端口前，首先必须使用适当的命令定义反宏，以便将端口设置回原始状态。

   定义中最多可包含 3000 个字符。输入反宏命令，每行一个命令。使用 @ 字符结束宏。要在宏中输入注释文本，需在行的开头使用 # 字符。
7. 单击 Submit。
8. 要丢弃任何未保存的更改，单击 Cancel。

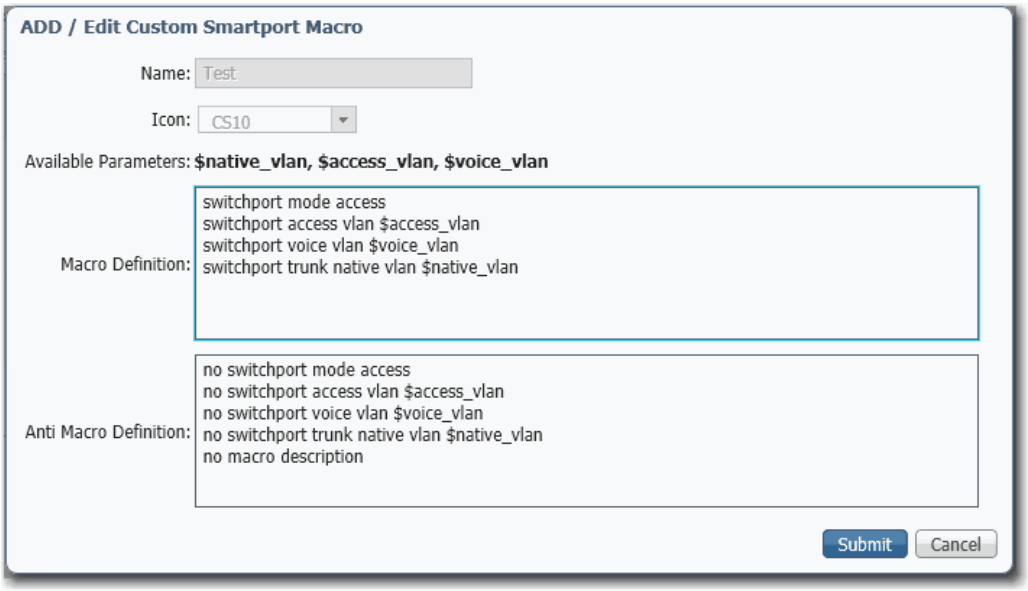
修改自定义的智能端口宏的定义

无法修改当前正在使用的自定义智能端口宏。

1. 从 Configure 菜单中，选择 Smartports。
2. 单击 Custom Smartports 选项卡。



3. 选中要修改的宏旁边的复选框。
4. 单击 Edit。

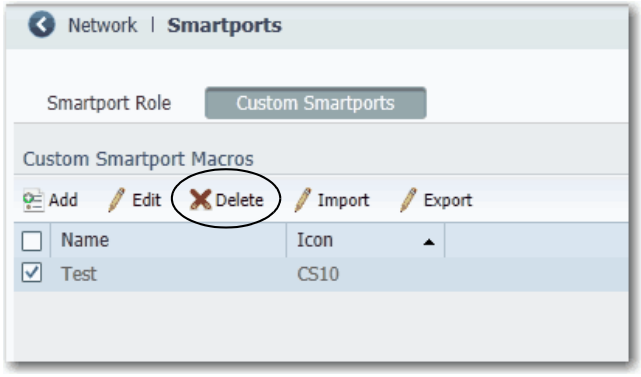


5. 根据需要更改定义。
6. 单击 Submit。

删除自定义的智能端口宏

无法删除当前正在使用的自定义智能端口宏。

1. 从 Configure 菜单中，选择 Smartports。
2. 单击 Custom Smartports 选项卡。
3. 选中要删除的宏旁边的复选框。

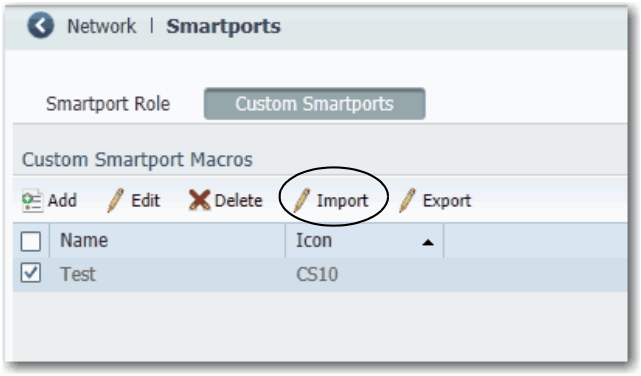


4. 单击 Delete。

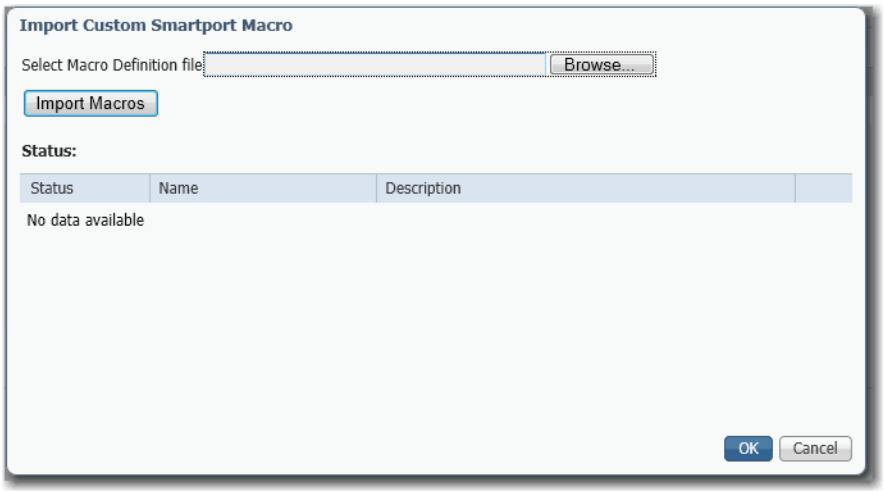
导入自定义的智能端口宏

必须使用 Firefox 3.6 或更高版本才能导入自定义的智能端口宏。

1. 从 Configure 菜单中，选择 Smartports。
2. 单击 Custom Smartports 选项卡。
3. 单击 Import。



4. 单击 Browse。



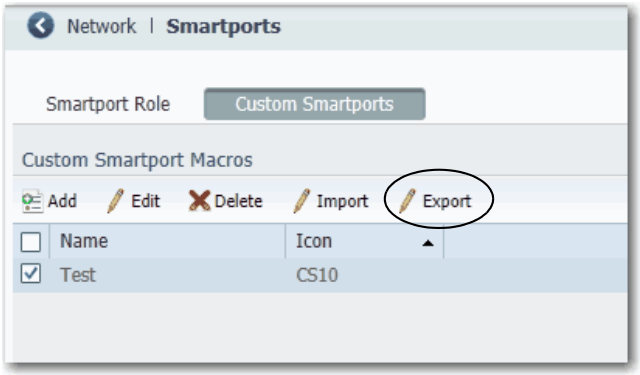
5. 选择计算机或网络驱动器上的宏文件。

   文件必须为相应格式的 .xml 文件。
6. 单击 Import Macros。
7. 单击 OK。

导出自定义的智能端口宏

必须使用 Firefox 3.6 或更高版本才能导出自定义的智能端口宏。

1. 从 Configure 菜单中，选择 Smartports。
2. 单击 Custom Smartports 选项卡。
3. 选中要导出的宏旁边的复选框。
4. 单击 Export。

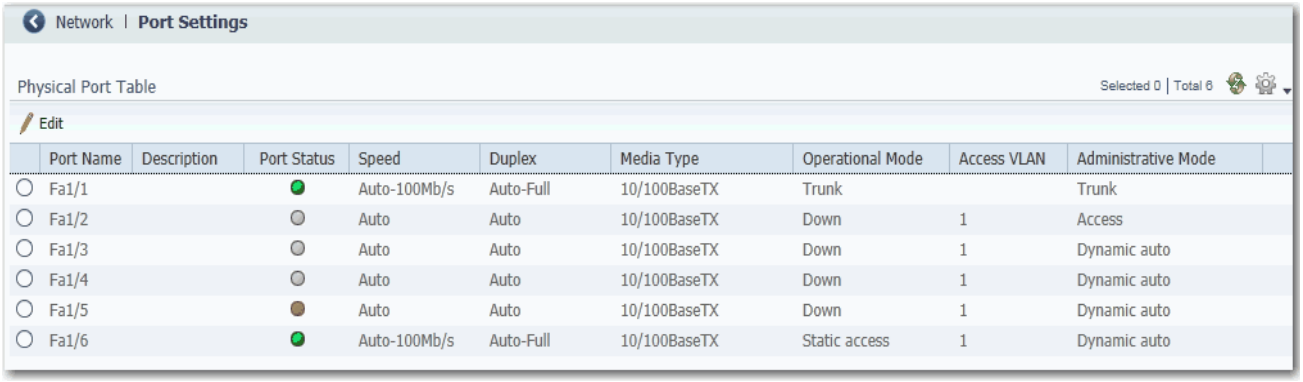


5. 保存生成的文件。

配置端口设置

基本端口设置决定交换机与相连设备之间的数据接收和发送方式。可以更改这些设置，以满足您的网络需求并处理网络问题。交换机端口上的设置与相连设备的端口设置必须兼容。

要更改基本端口设置，从 Configure 菜单中选择 Port Settings。



Port Name	Description	Port Status	Speed	Duplex	Media Type	Operational Mode	Access VLAN	Administrative Mode
Fa1/1			Auto-100Mb/s	Auto-Full	10/100BaseTX	Trunk		Trunk
Fa1/2			Auto	Auto	10/100BaseTX	Down	1	Access
Fa1/3			Auto	Auto	10/100BaseTX	Down	1	Dynamic auto
Fa1/4			Auto	Auto	10/100BaseTX	Down	1	Dynamic auto
Fa1/5			Auto	Auto	10/100BaseTX	Down	1	Dynamic auto
Fa1/6			Auto-100Mb/s	Auto-Full	10/100BaseTX	Static access	1	Dynamic auto

表 9 列出了交换机端口的基本设置。要更改设置，单击端口名称旁边的单选按钮，然后单击 Edit 显示 Edit Physical Port 窗口。

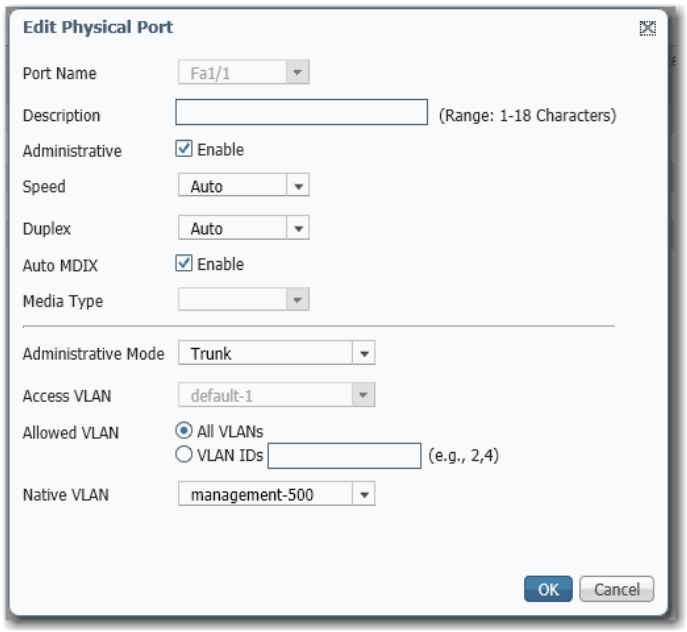

Edit Physical Port
Port Name
Fa1/1
Description
(Range: 1-18 Characters)
Administrative
Enable
Speed
Auto
Duplex
Auto
Auto MDIX
Enable
Media Type
Administrative Mode
Trunk
Access VLAN
default-1
Allowed VLAN
All VLANs
VLAN IDs
(e.g., 2,4)
Native VLAN
management-500
OK
Cancel

表 9 - 端口设置

字段	描述
Port Name	交换机端口的编号，包括端口类型（如 Fa 表示高速以太网，Gi 表示千兆以太网）和特定端口编号： • Gi/1 为交换机的千兆端口 1。 • Fa1/1 为交换机的高速以太网端口 1。
Description	交换机端口的描述。 我们建议您提供端口描述以便在监视和故障处理期间帮助确定端口。描述可以是相连设备的位置或使用相连设备的人员姓名。
Port Status	交换机端口的状态。默认设置为 Enabled。可以在 Edit Physical Port 窗口中通过选中或清除 Administrative 复选框来更改此设置。 如果端口未使用且未与任何设备相连，我们建议禁用该端口。 例如，处理故障时需要更改此设置。可以通过管理方式禁用端口来处理疑似未经授权连接的问题。
Speed	交换机端口的运行速度。如果所连设备可以与交换机端口协商链路速度，则可以选择 Auto（自动协商）。默认设置为 Auto。 建议使用默认设置，这样交换机端口的速度设置就能自动与相连设备的设置匹配。如果相连的设备需要特定的速度，则更改交换机端口速度。 例如，处理故障时需要更改此设置。如果正在处理连接问题，则可以更改此设置，查看交换机端口与连接设备之间的速度是否匹配。
Duplex	交换机端口的双工模式： • 如果相连设备可以与交换机协商，选择 Auto （自动协商）。 • 如果两台设备可同时发送数据，选择 Full （全双工模式）。 • 如果两台设备不能同时发送数据，选择 Half （半双工模式）。 默认设置为 Auto。 在千兆以太网端口上，如果端口速度设置为 Auto，则不可以将端口设为半双工模式。 建议使用默认设置，这样交换机端口的双工设置就能自动与相连设备的设置匹配。如果相连的设备要求使用特定模式，则需要更改交换机上的双工模式。 例如，处理故障时需要更改此设置。如果正在处理连接问题，则可以更改此设置，查看交换机端口与连接设备之间的双工是否匹配。
Auto-MDIX	自动线序交叉（自动 MDIX）功能是否可以自动检测所需的电缆连接类型（直通或交叉）并正确配置连接。默认设置为 Enable。 该设置在 SFP 模块端口上不可用。
Media Type	两用上行端口的活动端口类型（RJ45 端口或 SFP 模块端口）。 默认情况下，交换机会检测两用端口连接的是 RJ45 端口还是 SFP 模块端口并使用相应的端口。每次只有一个端口可以处于活动状态。如果同时连接了两个端口，则优先使用 SFP 模块端口。用户无法更改优先级设置。 从下列介质类型中选择： • SFP — SFP 模块端口处于活动状态。 如果选择该选项，速度和双工将显示当前设置，自动 MDIX 显示不适用。 • RJ45 — RJ45 端口处于活动状态。 如果选择该选项，则可以设置端口速度、双工和自动 mdix 值。 • Auto（自动协商）— 任一端口可以处于活动状态。 如果选择该选项，速度和双工将设为自动，而自动 MDIX 显示不适用。 默认设置为 Auto。
Operational Mode	端口的运行状态。显示管理模式或 Down（若禁用）。
Access VLAN	当链路被配置为或充当非主干接口时接口所属或为其传送通信的 VLAN。
Administrative Mode	显示以下任一管理模式： • Access — 即使相邻接口为主干接口，此接口仍永久处于非主干模式并通过协商将相邻链路转换为非主干链路。如果选择该选项，还需选择一个访问 VLAN。访问端口只属于一个 VLAN 并只为一个 VLAN 传送通信（除非配置为语音 VLAN 端口）。 • Trunk — 即使相邻的接口不是主干接口，该接口也将永久处于主干模式并通过协商将相邻的链路转换为主干链路。如果选择该选项，还需选择允许全部 VLAN 还是指定的 VLAN ID。 • Dynamic Auto — 如果将相邻接口设为主干或所需模式，该接口会将链路转换为主干链路。此模式为默认设置。如果选项该选项，则在链路处于访问模式时指定一个要使用的访问 VLAN。当链路处于主干模式时，还需指定允许全部 VLAN 还是指定的 VLAN ID。 • Dynamic Desirable — 如果相邻接口设为 Trunk、Dynamic Desirable 或 Auto 模式，该接口会将链路转换为主干链路。如果选项该选项，则在链路处于访问模式时指定一个要使用的访问 VLAN。当链路处于主干模式时，还要选择允许全部 VLAN 还是指定的 VLAN ID。

配置端口阈值

配置端口阈值，以免 LAN 上的通信被其中一个物理接口上的广播、多播或单播风暴中断。

要配置端口阈值，从 Configure 菜单中选择 Port Thresholds。

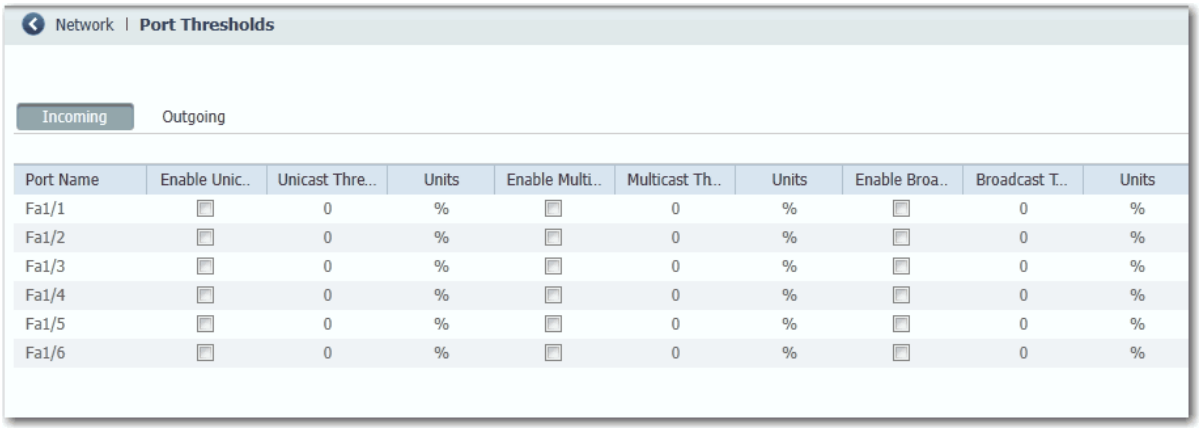


表 10 - 端口阈值字段

字段	描述
Incoming	
Unicast Multicast Broadcast	对各个端口执行下列操作： 1. 选中或清除 Enable 复选框。 2. 输入阈值。 3. 在以下单位中选择一项： – PPS（0…100 亿） – BPS（0…100 亿） – %（0…100）
Outgoing	
All Traffic	对各个端口执行下列操作： 1. 选中或清除 Enable 复选框。 2. 输入阈值。 3. 单击 Save。

配置 EtherChannel

EtherChannel（或端口组）是捆绑为一个逻辑链路的两个或多个交换机端口组，可在两个交换机之间创建一条更高带宽的链路。

例如，四个 10/100 交换机端口可以分配给一个 EtherChannel 来提供全双工带宽，速度可达 800 Mb/s。如果 EtherChannel 中有一个端口不可用，将使用 EtherChannel 中的其余端口传递通信。

同一个 EtherChannel 中所有端口的特性必须相同：

- 所有端口均应用 Smartports IE Switch 端口角色并属于同一个 VLAN。
- 所有端口均为 10/100 端口或均为 10/100/1000 端口。不能在 EtherChannel 中混合 10/100 和 10/100/1000 端口。
- 所有端口均已启用。EtherChannel 中禁用的端口会被视为链路故障，其通信将传送到 EtherChannel 中其余的一个端口中。

重要信息　　请勿在物理 EtherChannel 接口上启用第 3 层地址。

要创建、修改和删除 EtherChannel，从 Configure 菜单中选择EtherChannels。

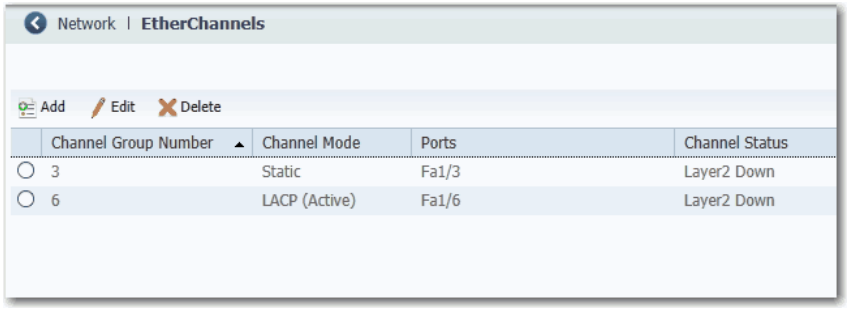


表 11 - EtherChannel 字段

字段	描述
Channel Group Number	标识该 EtherChannel 的数字，范围为 1 到 6。最多可以配置六个 EtherChannel。
Channel Mode	确定端口的激活方式。除 On 外的所有选项，均通过协商确定要激活的端口。不兼容的端口将被置于独立状态并继续传送数据通信，但不参与 EtherChannel。 **重要信息：**确保将 EtherChannel 中的所有端口配置为相同的速度和双工模式。 以下为可用模式： • Static — 所有端口均加入 EtherChannel，无协商。如果远程设备不支持其它模式所需的协议（见下方），可以使用该模式。链路两端的交换机都必须配置为 On 模式。 • PAgP — 该模式将启用端口聚合协议 (PAgP)，后者为思科专有协议。端口响应创建 EtherChannel 的请求，但不会启动相应协商。如果端口与可能不发送 PAgP 数据包的设备（如文件服务器或数据包分析器）相连，建议采用该 " 静默 " 模式。处于 Auto 模式的端口可与处于 Desirable 模式的另一端口组成 EtherChannel。 • PAgP (non-silent) — 该模式与 Auto 模式相同，但建议当端口与在启动 EtherChannel 时应激活的设备相连时使用该模式。处于 Auto 模式的端口可与处于 Desirable 模式的另一端口组成 EtherChannel。 • PAgP Desirable — 该模式将启用端口聚合协议 (PAgP)，后者为思科专有协议。端口通过向其它端口发送 PAgP 数据包发起协商来组成 EtherChannel。如果端口与可能不发送 PAgP 数据包的设备（如文件服务器或数据包分析器）相连，建议采用该 " 静默 " 模式。处于 Desirable 模式的端口可与处于 Desirable 或 Auto 模式的另一端口组成 EtherChannel。 • PAgP Desirable (non-silent) — 该模式与 Desirable 模式相同，但建议当端口与在启动 EtherChannel 时应激活的设备相连时使用该模式。 • LACP (Active) — 该模式将无条件启用链路聚合控制协议 (LACP)。端口向其它端口发送 LACP 数据包，发起协商来创建 EtherChannel。处于 Active 模式的端口可与处于 Active 或 Passive 模式的另一端口组成 EtherChannel。端口必须配置为全双工。 • LACP (Passive) — 只有在链路的另一端检测到 LACP 设备时，该模式才会启用链路聚合控制协议。端口响应创建 EtherChannel 的请求，但不会启动相应协商。端口必须配置为全双工。
Ports	可以参与该 EtherChannel 的端口。
Channel Status	组的状态。

配置 DHCP

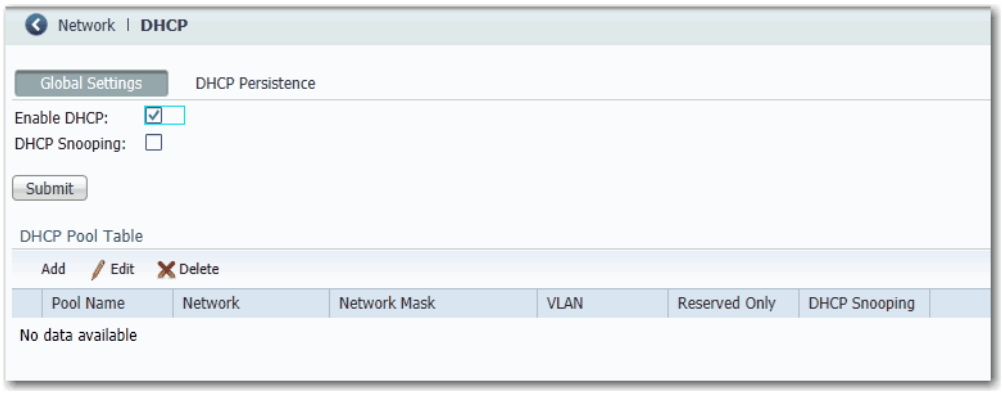
要使用 DHCP 持久性，必须先启用 DHCP 并设置 IP 地址池。然后，必须为各个端口分配特定的 IP 地址。

设置 DHCP 服务器。

要在交换机上启用 DHCP 服务器模式，执行以下操作。

1. 从 Configure 菜单中，选择 DHCP。
2. 选中 Enable DHCP 复选框。
3. 要启用 DHCP 监听，选中 DHCP Snooping 复选框。

   DHCP 监听将限制所连接交换机之外的 DHCP 请求广播。也就是说，设备只可以接收来自相连交换机的地址分配。此选项仅在 VLAN 接口上可用。要在特定的 VLAN 上启用 DHCP 监听，在 DHCP 池表格中选中特定 VLAN 的 DHCP Snooping 复选框。



4. 要仅为 DHCP 持久性表中指定的设备预留地址池，在 DHCP 池表格中选中 Reserved Only 复选框。

   将忽略来自持久性表之外端口的 DHCP 请求或来自其它设备（交换机）的 DHCP 请求。默认情况下，该选项处于禁用状态，且 Reserved Only 复选框处于清除状态。

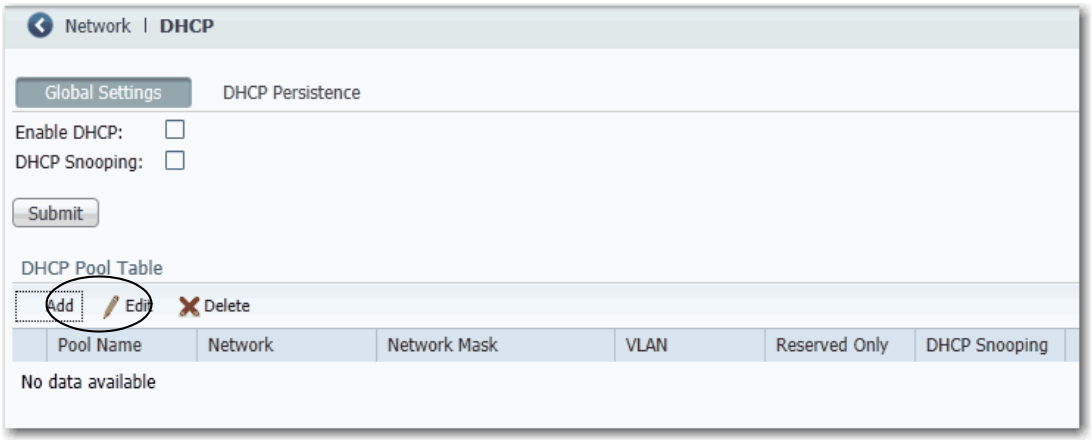
5. 单击 Submit。

配置 DHCP IP 地址池

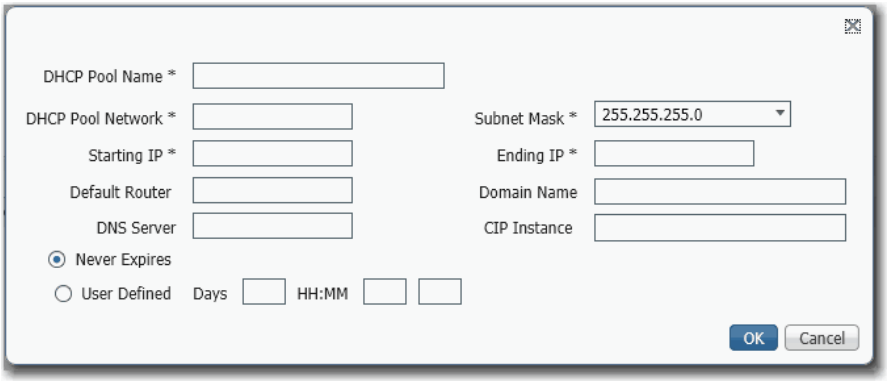
启用 DHCP 后，可以创建 DHCP 地址池。

要配置 DHCP IP 地址池，按以下步骤操作：

1. 从 Configure 菜单中，选择 DHCP。
2. 单击 Add。



3. 按如下所述填写字段，然后单击 OK。



字段	描述
DHCP Pool Name	交换机上配置的 DHCP IP 地址池的名称。名称最多包含 31 个字母数字字符。名称中不可包含问号或制表符。该字段为必填字段。 DHCP IP 地址池是交换机可为已连接设备分配的可用 IP 地址范围（或地址池）。
DHCP Pool Network	DHCP IP 地址池的子网 IP 地址。IP 地址的格式是一个 32 位数字地址，共四组数字，之间用句点分隔。每组数字的范围都是 0...255。该字段为必填字段。
Subnet Mask	标识 DHCP IP 地址池子网的网络地址。子网将网络中的设备划分为更小的组。默认值为 255.255.255.0。 该字段为必填字段。
Starting IP	用于定义 DHCP IP 地址池地址范围的起始 IP 地址。IP 地址的格式是一个 32 位数字地址，共四组数字，之间用句点分隔。每组数字的范围都是 0...255。 确保分配的 IP 地址均未被网络中的其它设备使用。 该字段为必填字段。
Ending IP	用于定义 DHCP IP 地址池地址范围的结束 IP 地址。IP 地址的格式是一个 32 位数字地址，共四组数字，之间用句点分隔。每组数字的范围都是 0...255。 确保分配的 IP 地址均未被网络中的其它设备使用。 该字段为必填字段。
Default Router	使用该服务器的 DHCP 客户端的默认路由器 IP 地址。IP 地址的格式是一个 32 位数字地址，共四组数字，之间用句点分隔。每组数字的范围都是 0...255。
Domain Name	DHCP 客户端的域名。名称最多包含 31 个字母数字字符。名称中不可包含问号或制表符。
DNS Server	DHCP 客户端可用的域名系统 (DNS) IP 服务器的 IP 地址。IP 地址的格式是一个 32 位数字地址，共四组数字，之间用句点分隔。每组数字的范围都是 0...255。
CIP Instance	标识地址池的数字，范围为 1…15。
[租用期]	分配给 DHCP 客户端的 IP 地址的租用持续时间。单击以下任意一项： • Never Expires • User Defined 如果单击 User Defined，则输入租用持续时间的天数、小时数和分钟数。此租用期将用于所有分配。

通过 DHCP 持久性预留 IP 地址

可以从 IP 地址池为特定交换机端口预留和预分配 IP 地址，这样无论其 MAC 地址如何，与该交换机端口相连的设备就能始终接收到相同的 IP 地址。

DHCP 持久性在预先设置的网络中起着很大作用，这类网络中部分设备实际的 IP 地址存在关联性。当所连设备需充当特定角色或其它设备已知其 IP 地址时，使用 DHCP 持久性。如果更换设备，为替换设备分配相同的 IP 地址，网络中的其它设备则不需要重新配置。

启用 DHCP 持久性功能后，交换机充当同一子网中其它设备的 DHCP 服务器，其中包括与其它交换机相连的设备。如果交换机接收到 DHCP 请求，它将使用池中任意一个未分配的 IP 地址响应。为防止此类事件发生，选中 DHCP 窗口中的 Reserve Only 复选框。这样可阻止交换机在接收到请求时发出响应。

如果在端口上启用了 DHCP 持久性且该端口上连接的设备发出 DHCP 请求，交换机将在 DHCP 窗口为该端口分配 IP 地址。还会向网络中的其它设备广播该 DHCP 请求。如果网络中存在另一个具有可用地址的 DHCP 服务器并接收到该请求，它也可以尝试进行响应。这可能会覆盖交换机分配的初始 IP 地址，具体情况决绝于终端设备的工作方式（使用第一个还是最后一个 IP 地址响应）。为防止 IP 地址被覆盖，可以启用相应 VLAN 上的 DHCP 监听。这样可阻挡该 DHCP 请求的广播，因此包括启用 DHCP 持久性的另一个 Stratix 交换机在内的其它服务器都不会响应。

如果正在使用 DHCP 持久性，建议先为终端设备分配静态 IP 地址。如果终端设备发生故障或被更换，DHCP 持久性功能将从 DHCP 持久性表分配 IP 地址。设备可使用此 IP 地址正常工作，但是我们建议为替换设备重新分配一个静态 IP 地址。

下面的图片和表格说明了 DHCP 持久性行为。

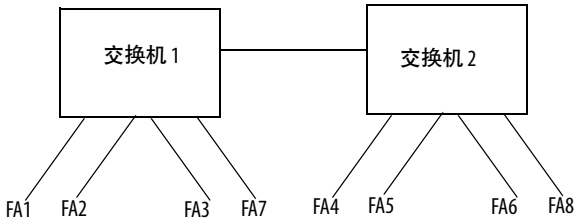


表 12 - DHCP 持久性行为

如果	则
• 交换机 1 的持久性表中有端口 FA1…FA3 • 交换机 2 的持久性表中有 FA4、FA5、FA6 和 FA8 • 未选择 Reserve Only 且 DHCP 监听已关闭	交换机 1 FA1 上连接的新设备将接收来自交换机 1 持久性表的 IP 地址。还会通过网络发送广播请求。交换机 2 将响应（如果池中存在未分配的地址）。可能会覆盖交换机 1 执行的分配。
• 交换机 1 的持久性表中有端口 FA1…FA3 • 交换机 2 的持久性表中有 FA4、FA5、FA6 和 FA8 • 两台交换机均选择 Reserve Only 且 DHCP 监听已关闭	交换机 1 FA1 上连接的新设备将接收来自交换机 1 持久性表的 IP 地址。还会通过网络发送广播请求。交换机 2 不响应该请求。注意，如果设备与交换机 1 的 FA7 相连，由于未在持久性表中定义，它将不接收来自交换机池的 IP 地址，池中未使用的地址将被阻止。
• 交换机 1 的持久性表中有端口 FA1…FA3 • 交换机 2 的持久性表中有 FA4、FA5、FA6 和 FA8 • 交换机 1 中选择 Reserve Only 且 DHCP 监听已关闭，但 DHCP 监听关闭时交换机 2 中不选择 Reserve Only	与 FA1 相连的新设备将接收来自持久性表的 IP 地址。还会通过网络发送广播请求。交换机 2 不响应该请求。此外，与 FA4 相连的设备会接收来自交换机 2 持久性表的 IP 地址，并发送广播请求，交换机 1 使用其池中未分配的 IP 地址进行响应。这将覆盖已分配的端口。
• 交换机 1 的持久性表中有端口 FA1…FA3 • 交换机 2 的持久性表中有 FA4、FA5、FA6 和 FA8 • 选择 DHCP Snooping • 选中 Reserve Only	交换机 1 FA1 上连接的新设备将接收来自交换机 1 持久性表的 IP 地址。不通过网络发送广播请求，因此交换机 2 不响应。注意，如果设备与交换机 1 的 FA7（未在 DHCP 持久性表中定义）相连，则由于 FA7 未在持久性表中定义，该设备将不接收来自交换机池的 IP 地址，池中未使用的地址将被阻止。
• 交换机 1 的持久性表中有端口 FA1…FA3 • 交换机 2 的持久性表中有 FA4、FA5、FA6 和 FA8 • 选择 DHCP Snooping • 未选中 Reserve Only	交换机 1 FA1 上连接的新设备将接收来自交换机 1 持久性表的 IP 地址。不通过网络发送广播请求，因此交换机 2 不响应。注意，如果设备与交换机 1 的 FA7（未在 DHCP 持久性表中定义）相连，它将接收来自交换机 1 池的未分配 IP 地址。

要分配、修改或删除交换机端口 IP 地址，单击 DHCP Persistence 选项卡。

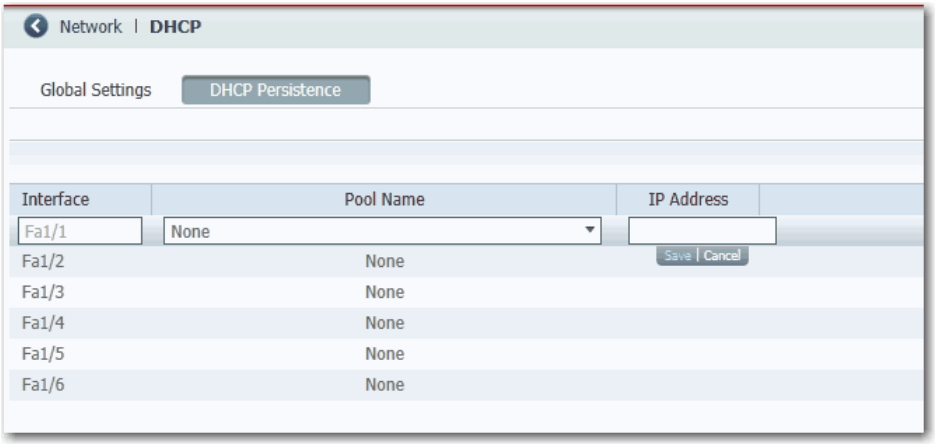
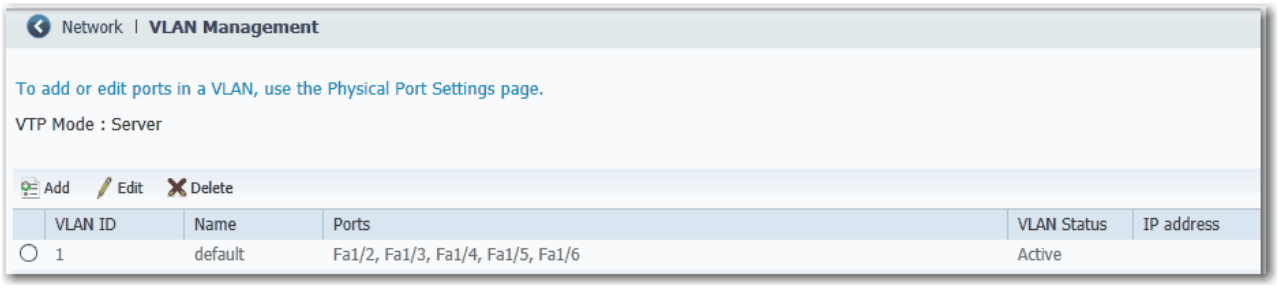


表 13 - DHCP 持久性字段

字段	描述
Interface	交换机端口的编号，包括端口类型（如 Fa 表示高速以太网，Gi 表示千兆以太网）和特定端口编号。例如，Fa1/1 为交换机的高速以太网端口 1。
Pool Name	交换机上配置的 DHCP IP 地址池的名称。
IP Address	分配给交换机端口的 IP 地址。您分配的 IP 地址将为所选端口保留，该 IP 地址将不会用于常规 DHCP 动态分配。IP 地址必须来自 DHCP Pool Name 字段中指定的池。

配置 VLAN

要创建、修改和删除 VLAN，从 Configure 菜单中选择VLAN Management。



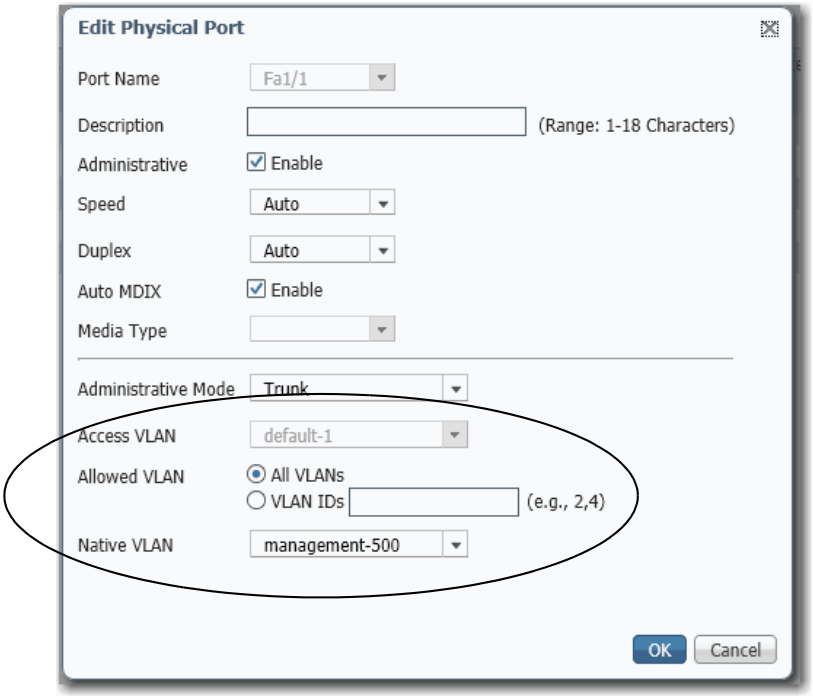
默认 VLAN ID 为 1，而管理 VLAN 的默认名称为 default。根据网络的规模和要求，默认 VLAN 就已足够。我们建议您先确定 VLAN 需求，再创建 VLAN。

创建 VLAN，必须指定 VLAN 名称和唯一的 ID 编号。可以修改 VLAN 的名称，但无法修改其编号。无法修改或删除默认 VLAN。

创建 VLAN 后，可以将端口分配到 VLAN。将端口分配到 VLAN 前，应确保各个端口都已应用合适的端口角色。

将端口分配到 VLAN

要将端口分配到 VLAN 分配端口，按第 96 页所述使用 Edit Physical Ports 窗口。



配置以太网供电 (PoE) 端口

连接正确的电源后，带有 PoE 端口的交换机支持 PoE 和 PoE+ 功能。有关电源要求，请参加第 36 页。

可以通过 PoE 窗口执行以下操作：

- 限制支持的总功率。
- 配置各个端口的模式和电源设置。

对于大多数应用，默认配置（Auto 模式）足以满足要求，不需要进行其它配置。但是，可以自定义设置来满足您的特殊需求。例如，提高 PoE 端口的电源优先级，将模式设置为 Static 以及分配要使用的电源。又如，禁用端口上的大功率设备，将模式设置为 Auto 和指定最大功率限值。

重要信息　**更改端口的 PoE 配置时，端口将掉电。端口能否再次上电取决于新配置、其它 PoE 端口的状态和功率预算的状态。**

例如，如果端口 1 的模式为 Auto 且状态为 On，则要将其配置为 Static 模式，交换机将断开端口 1 的电源，检测受电设备然后重新为端口供电。

如果端口 1 的模式为 Auto 且状态为 On，则要将其配置为最大功能功率 10 W，交换机将断开端口电源，然后重新检测受电设备。只有受电设备为 1 类、2 类或思科专用受电设备时，交换机才会重新为端口供电。

要配置 PoE 端口，从 Configure 菜单中选择 Power Management。

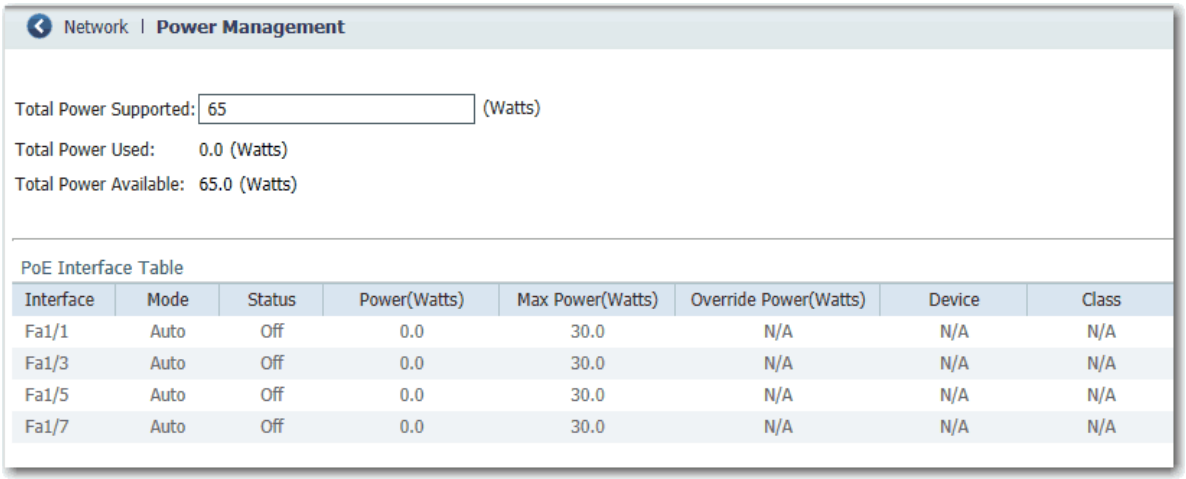


表 14 - 电源管理字段

字段	描述
Total Power Supported	要限制总 PoE 功率预算，根据电源输入相应值： • 48V 电源最大支持 65 W。 • 54V 电源最大支持 130 W。 保存该设置后，将更改总 PoE 功率预算并重置受电设备，以满足新的预算要求。 **重要信息：**如果支持的总功率与电源不匹配，将损坏交换机。注意不要超额登记电源： • 如果要将交换机与电源相连，且该电源支持的功率大于配置值，首先应更换电源，然后配置支持的总功率。 • 如果要将交换机与电源相连，且该电源支持的功率小于配置值，首先将支持的总支持功率更改为适当的值，然后更换电源。
Total Power Used	显示模块当前使用的功率量。
Total Power Available	显示模块可用但尚未使用的功率量。

表 14 - 电源管理字段

字段	描述
Interface	显示端口编号。
Mode	显示端口的 Power Management 模式： • Auto — 启用受电设备检测，如果已连接设备，将自动为 PoE 端口分配功率。默认情况下选择此设置。要限制该端口使用的功率，调整 Max Power 设置。 • Static— 即使没有连接任何设备也会为该端口保留功率，以确保检测到设备时可立即分配功率。也可以选择 Static 模式来提高端口的优先级。交换机先为 Static 模式的端口分配功率，然后再为 Auto 模式的端口分配功率。 • Off — 禁用 PoE。 有关详细信息，请参见第 62 页上的电源管理模式。
Status	显示 PoE 在该端口上是启用 (on) 还是禁用 (off)。
Power (Watts)	显示分配给端口的功率量。
Max Power (Watts)	显示端口可以使用的最大功率量： PoE 端口：4…15.4 W PoE+ 端口：4…30 W
Override Power (Watts)	显示为该端口配置的功率超控。该配置将超控 Class 列显示的 IEEE 分类和功率协商。如果未配置超控，该字段将显示 N/A。 只能使用命令行接口 (CLI) 配置功率超控。有关详细信息，请参见《Cisco IE-3000 软件配置指南》(Cisco IE-3000 Software Configuration Guide)。 **示例：**当相连设备的功率要求已知且小于该等级的最大值时，管理员可以选择配置超控。例如，如果设备所需功率只有 5 W 而该设备所属的 0 类允许的最大值为 15.4 W，配置超控可以允许其它设备获得更多功率。
Device	显示端口上连接的设备。如果端口上未连接设备，该字段将显示 N/A。
Class	显示受电设备 (PD) 的功率分类。 有关功率分类的介绍，请参见第 61 页上的表 4。

配置 PTP 时间同步

IEEE 1588 标准定义了一种名为精密时间协议 (PTP) 的协议，通过该协议可以使测量系统和控制系统的时钟实现精密同步。时钟通过 EtherNet/IP 通信网络相互通信。PTP 协议可以使包含各种固有精度、分辨率和稳定性的时钟的不同系统同步。PTP 在系统的各个时钟之间生成主从关系。所有时钟的时间最终都会与选作主时钟的时钟一致。

默认情况下，交换机的所有高速以太网和千兆以太网端口上的 PTP 均处于禁用状态。

交换机支持下列同步时钟模式：

- **端到端透明模式** — 交换机使所有从时钟与其连接的主时钟实现透明同步。

  交换机会修正每个数据包通过交换机所引起的延迟（此延迟也称为驻留时间）。该模式引起的抖动和误差累积比边界模式小。

  在端到端透明模式下，默认启用所有交换机端口。

- **边界模式** — 交换机成为其它与交换机相连设备的父时钟，并同步这些设备的内部时钟。

  交换机会与相连设备不断交换定时消息，更正由时钟偏移和网络延迟引起的时滞。

  此模式可消除延迟波动的影响。由于级联拓扑中的抖动和误差可以累积，该模式只能用于级联设备少于四层的网络。

  在边界模式下，可以有一个或多个交换机端口启用 PTP。

- **转发模式（默认）**— 通过交换机转发通信（按 QoS 确定优先级），但不是由交换机执行操作。

重要信息　请记住，更改 PTP 定时消息设置时，除非系统中所有设备的值都相同，否则系统将无法正常工作。

要配置 PTP，从 Configure 菜单中选择 PTP。

选择模式后，即可编辑各个端口的设置。参数取决于所选模式。如果交换机处于边界模式或端到端透明模式，可以配置每个端口的 PTP。

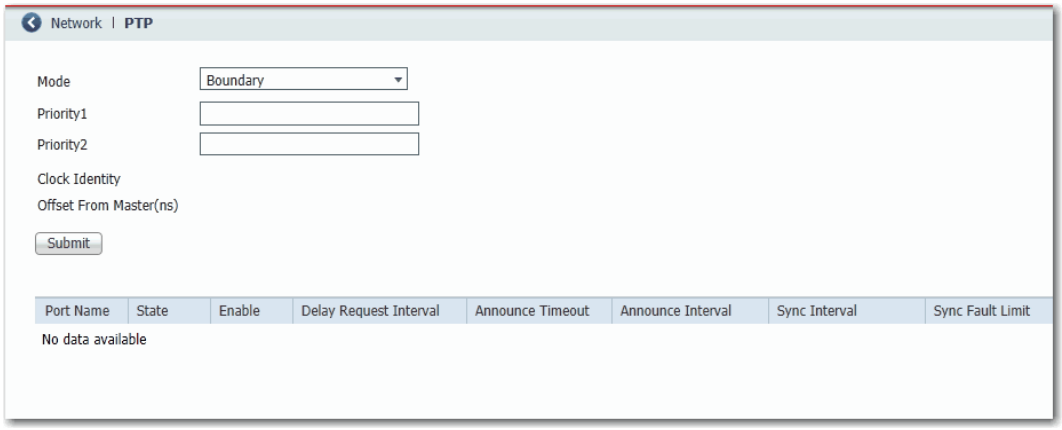


表 15 - PTP 字段

字段	描述
Mode	选择 PTP 模式： • Boundary — 利用 IEEE 1588 V 2 边界时钟机制实现所有交换机端口与主时钟的同步。 • End-to-End Transparent — 利用 IEEE 1588 V 2 端到端透明时钟机制计算交换机延迟并添加到 PTP 数据包中。在该模式下，所有交换机端口均启用 PTP。在边界模式下，可以有一个或多个交换机端口启用 PTP。可以启用或禁用各个端口的 PTP。 • Forward（默认）— 无扰传递 PTP 数据包。
Priority 1	为选择最佳的主时钟，用于取代默认标准（如时钟质量或时钟等级）的交换机。
Priority 2	两台设备同时符合默认标准的要求时用于决定取舍的交换机。例如，可以为特定交换机分配高于其它同类交换机的优先级。范围为 0…255。较小的值优先。默认值为 128。
Clock Identity	时钟源。
Offset from Master (ns)	相对于主时钟的精度，以纳秒为单位。
Port Name	交换机端口的编号，包括端口类型（如 Fa 表示高速以太网，Gi 表示千兆以太网）、基本交换机编号 (1) 和特定端口编号。例如：Fa1/1 为基本交换机的高速以太网端口 1。
State	（仅限边界模式）。交换机端口与父时钟或主时钟的同步状态： • Listening — 选择父时钟或主时钟后，交换机端口正在等待。 • Pre-master — 交换机端口正在向 Master 状态转换。 • Master — 交换机充当与其端口相连的设备的父时钟。 • Passive — 交换机检测到父时钟或主时钟的冗余路径。例如，两个不同的交换机端口声明同一个父时钟或主时钟。为防止网络中出现环路，将其中一个端口更改为 Passive 状态。 • Uncalibrated — 交换机端口无法与父时钟或主时钟同步。 • Slave — 交换机端口已连接父时钟或主时钟并正在进行同步。 • Faulty — PTP 未能在交换机端口上正常工作。 • Disabled — 交换机端口未启用 PTP。
Enable	至少有一个交换机端口启用 PTP 时，将默认选择 Forward 模式： 可以启用或禁用各个端口的 PTP。

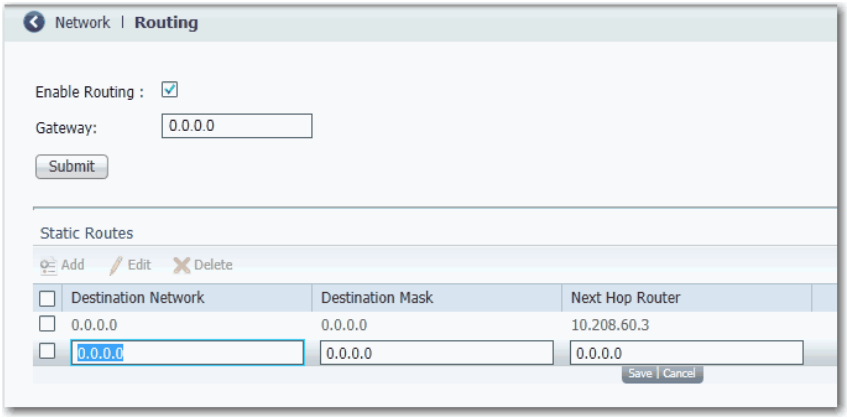
表 15 - PTP 字段 （续）

字段	描述
Delay Request Interval	交换机端口处于主时钟状态时所连设备发送延迟请求消息的建议时间间隔。 • **-1** 表示 0.5 秒 • **0** 表示 1 秒 • **1** 表示 2 秒 • **2** 表示 4 秒 • **3** 表示 8 秒 • **4** 表示 16 秒 • **5** 表示 32 秒 • **6** 表示 64 秒 默认值为 5（32 秒）。
Announce Timeout	交换机选择新主时钟前，从主时钟接收不到发布消息的情况下，必须经过的发布间隔数。该数字介于 2...10 之间。默认值为 3。
Announce Interval	发送发布消息的时间间隔： • **0** 表示 1 秒 • **1** 表示 2 秒 • **2** 表示 4 秒 • **3** 表示 8 秒 • **4** 表示 16 秒 默认值为 1（2 秒）。
Sync Interval	发送同步消息的时间间隔： • **-1** 表示 0.5 秒 • **0** 表示 1 秒 • **1** 表示 2 秒 默认值为 0（1 秒）。
Sync Fault Limit	PTP 尝试重新实现同步前的最大时钟偏移。该值的范围为 50…500,000,000 纳秒。默认值为 50,000 纳秒。 建议不要将同步限值设定在默认值（50,000 纳秒）以下。 仅在具有极高精度主时钟的网络中使用低于 50,000 纳秒的值。此类网络对极敏感设备保持同步有着严格的要求。

启用和配置路由

启用路由前，必须按第 136 页所述重新为路由分配交换机内存。

要启用路由，从 Configure 菜单中选择 Routing。



从 Routing 窗口中，可以只启用直连路由或同时启用静态路由和直连路由。如果启用静态路由，默认情况下将启用直连路由。有关这些路由类型的详细信息，请参见第 82 页上的路由。

仅启用直连路由。

要仅启用直连路由，选中 Enable Routing 然后单击 Submit。

对于直连路由，无需再执行其它操作。

同时启用静态路由和直连路由

要同时启用静态路由和直连路由，按以下步骤操作。

1. 选中 Enable Routing，然后单击 Submit。
2. 按如下所述配置静态路由信息。

字段	描述
Destination Network	目标的 IP 地址。
Destination Mask	目标的子网掩码。
Next Hop Router	其中的设备要为特定目标发送数据包的路由器的 IP 地址。

配置 STP

生成树协议 (STP) 模式的特性包括：

- 多生成树协议（MST）通过只启用一条活动通信路径来防止网络回路。如果活动路径不可用，MST 还会提供冗余路径。此为默认 STP 模式。
- 支持最大数量的交换机各个 VLAN 上运行的每 VLAN 生成树增强版 (PVST+)，确保整个网络路径无回路。
- 快速每 VLAN 生成树增强版（PVST+）在接收到拓扑变化后将立即删除动态学习的 MAC 地址条目。相反，PVST+ 将为动态学习的 MAC 地址使用较短的老化时间。

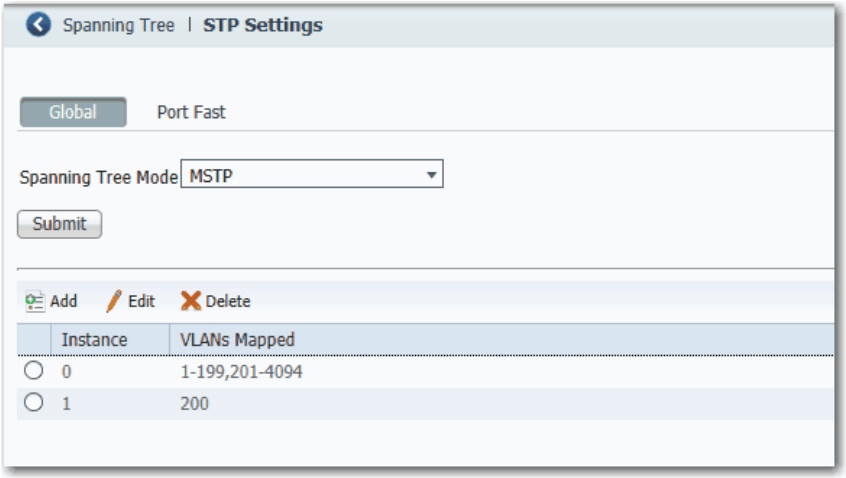
我们建议您启用 STP，以防止网络回路，并在活动路径不可用时提供冗余路径。

重要信息　　禁用 STP 可能会影响网络连接。

要配置生成树协议设置，从 Configure 菜单中选择 STP。

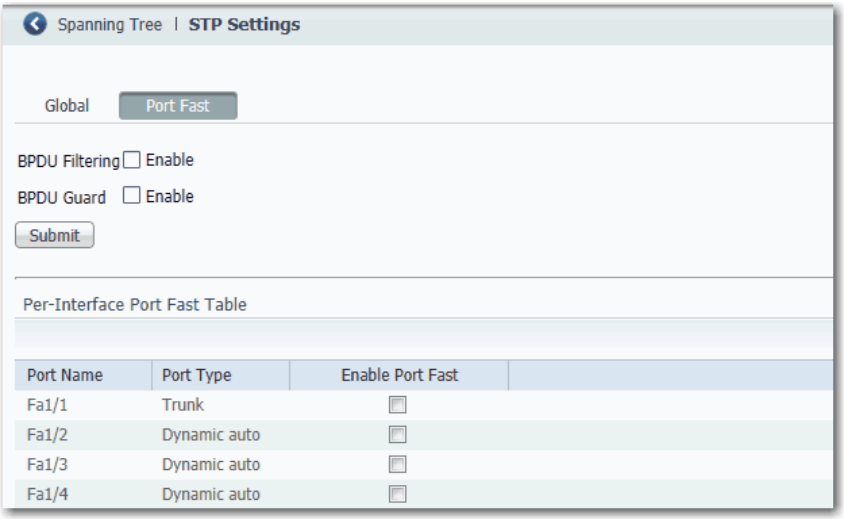
全局设置

要选择交换机的 STP 模式或配置各个 VLAN 上的 STP，单击 Global 选项卡。在 Global 选项卡上，可以添加、编辑或删除实例。如果选择 PVST+ 或 Rapid PVST+ 模式，则可以在各个实例上启用或禁用 STP。



PortFast 设置

要启用 PortFast 及相关功能，单击 PortFast 选项卡。在 PortFast 选项卡上，可以更改各个端口上 STP 的实施方式。



通常仅启用访问端口上的 PortFast 功能，该端口与个人计算机、接入点和不发送桥接协议数据单元 (BPDU) 的服务器等设备相连。由于可能会出现生成树回路，与交换机相连的端口上通常不启用这些功能。

BPDU 功能

交换机通过交换名为 BPDU 的特殊帧实现网络信息通信、跟踪更改以及创建 STP 拓扑。由于发送的 BPDU 会显示网络信息而接收的 BPDU 可能影响 STP 拓扑，需要在访问端口上启用 BPDU 筛选和 BPDU 防护。这两个功能可防止恶意设备干扰 STP 拓扑。不过，我们建议您小心使用这些功能：

- BPDU 筛选 — 该 PortFast 功能可阻止所有通过启用 PortFast 的端口发送和接收 BPDU。该功能可有效禁用这些端口的 STP，但是会产生回路。如果接收到 BPDU，将禁用端口上的 PortFast 并应用全局 STP 设置。要在所有启用 PortFast 的端口上启用 BPDU Filtering，选中 Enable。
- BPDU 防护 — 该 PortFast 功能将在端口接收到 BPDU 后关闭端口。要在所有启用 Port Fast 的端口上启用 BPDU 防护，选中 Enable。

注意，如果同时启用这两个功能，由于 BPDU 筛选会阻止端口接收任何 BPDU，BPDU 防护不起作用。

每接口 *PortFast* 表

生成树要求一个接口完成监听和学习状态、交换信息并建立一个无回路的路径后，才能转发帧。在与工作站和服务器等设备相连的端口上，可以实现立即连接。建立链路后，PortFast 会立即将端口转换为 STP 转发模式。

要在接口上启用 PortFast 并对接口应用选择的 BPDU 功能，选择接口，然后选中 Enable Port Fast。

配置 REP

要配置弹性以太网协议 (REP)，从 Configure 菜单中选择 REP。

要创建 REP 网段，在目标端口上设置网段 ID 和端口类型。

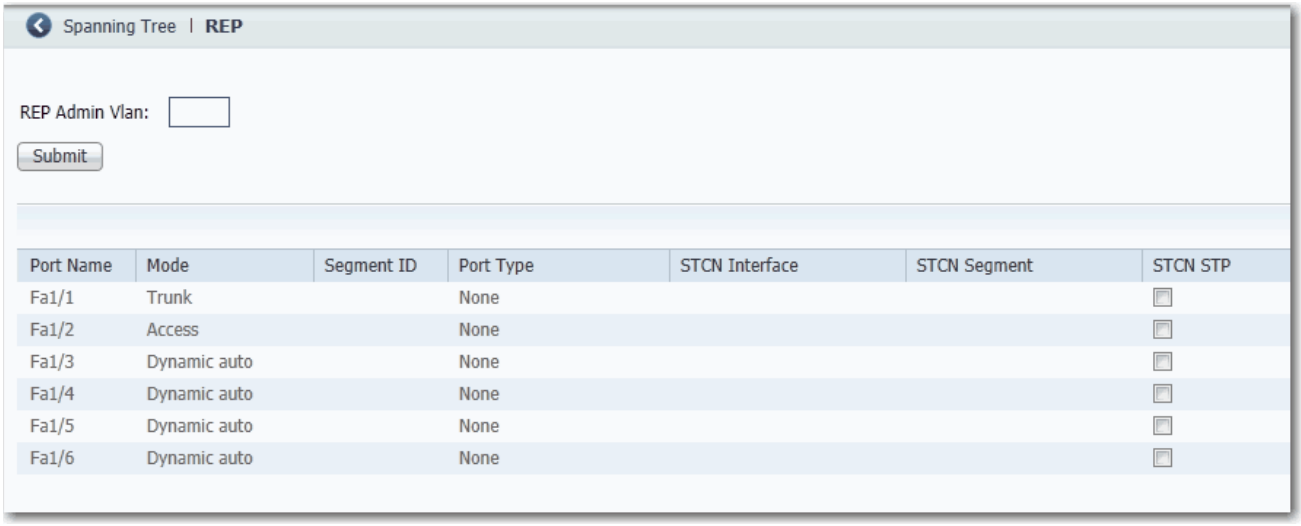


表 16 - REP 字段

字段	描述
REP Admin VLAN	管理 VLAN。范围为 2…4094。默认为 VLAN 1。 REP 端口将分配到同一 REP Admin VLAN。如果 REP Admin VLAN 发生变化，所有 REP 端口都将自动分配到新的 REP Admin VLAN。
Port Name	交换机端口的编号，包括端口类型（如 Fa 表示高速以太网，Gi 表示千兆以太网）。
Mode	管理模式。要设置该模式，从 Configure 菜单中选择 Port Settings。
Segment ID	网段的 ID。网段 ID 的范围为 1…1024。如果未设置任何网段 ID，则将禁用 REP。
Port Type	每个 REP 网段必须拥有两个主边缘端口，在主边缘端口发生故障时也使用次端口。可以指定首选的主端口和次端口。将端口配置为首选端口并不能保证其为备用端口，但能使其在平等的竞争者中占有优势。还可以指定与不支持 RDP 的交换机相连的端口。 选择以下任一端口类型： • Edge — 参与 VLAN 负载均衡的次边缘端口。 • Edge no-neighbor — 与非 REP 交换机相连的次边缘端口。 • Edge no-neighbor preferred — 与非 REP 交换机相连的次边缘端口，是 VLAN 负载均衡的首选备用端口。 • Edge no-neighbor primary — 始终参与该 REP 网段的 VLAN 负载均衡的次边缘端口，与非 REP 交换机相连。 • Edge no-neighbor primary preferred — 始终参与该 REP 网段中的 VLAN 负载均衡的次边缘端口，与非 REP 交换机相连，是 VLAN 负载均衡的首选端口。 • Edge preferred — 次边缘端口，是 VLAN 负载均衡的首选备用端口。 • Edge primary — 始终参与该 REP 网段中的 VLAN 负载均衡的边缘端口。 • Edge primary preferred — 始终参与该 REP 网段中的 VLAN 负载均衡的边缘端口，是 VLAN 负载均衡的首选端口。 • None — 此端口不在 REP 网段中。默认为 None。 • Preferred — 次边缘端口，是 VLAN 负载均衡的首选备用端口。
STCN Interface	配置端口的网段拓扑变更通知 (STCN)。默认为 None。 在网段中使用 TCN 向 REP 邻居发送拓扑变更通知。在网段边缘，REP 可将通知传播到 STP 或其它 REP 网段。
STCN Segment	为网段 ID 配置 STCN。默认情况下，该字段为空。 在网段中使用 TCN 向 REP 邻居发送拓扑变更通知。在网段边缘，REP 可将通知传播到 STP 或其它 REP 网段。
STCN STP	为 STP 网络配置 STCN。默认情况下，复选框处于清除状态。 在网段中使用 TCN 向 REP 邻居发送拓扑变更通知。在网段边缘，REP 可将通知传播到 STP 或其它 REP 网段。

配置 NAT

要配置 NAT，请根据应用按以下步骤之一操作：

- 为通过第 3 层交换机或路由器路由的通信创建 NAT 实例

  有关此应用的一个示例，请参见第 73 页上的图 4。
- 为通过第 2 层交换机或路由器进行路由的通信创建 NAT 实例

  有关此应用的一个示例，请参见第 74 页上的图 5。

重要信息 创建 NAT 实例前，设置所有的智能端口角色和 VLAN。

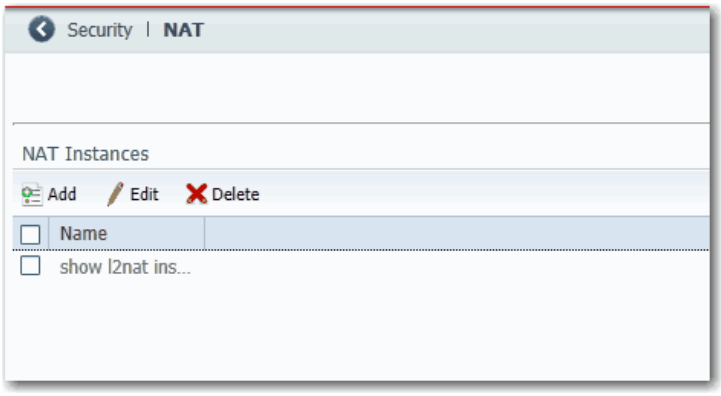
如果为与 NAT 实例关联的端口更改了智能端口角色或本机 VLAN，则必须将 VLAN 重新分配到 NAT 实例。

重要信息 由于第 2 层转发，当前通信会话会在手动断开前保持已建立状态。如果更改现有转换，则必须在新的转换生效之前，手动断开所有相关的通信会话。

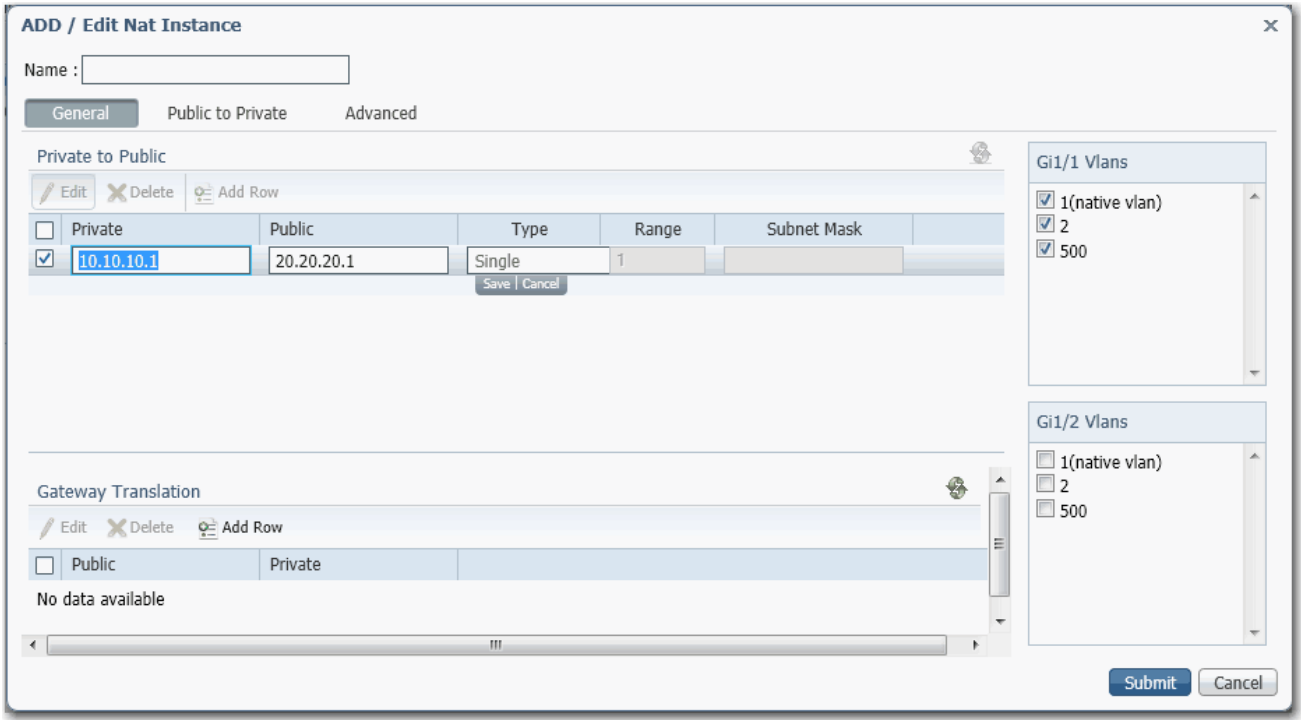
为通过第 3 层交换机或路由器路由的通信创建 NAT 实例

要为通过第 3 层交换机或路由器进行路由的通信创建 NAT 实例，请遵循以下步骤。

1. 从 Configure 菜单中，选择 NAT 以显示 NAT 窗口。



2. 单击 Add 显示 Add/Edit NAT Instance 窗口的 General 选项卡。



3. 在 Name 字段中，为实例输入唯一的名称。

   实例名称不能包含空格，不可超过 32 个字符。

4. 从右侧的 VLAN 列表中，选中每个 VLAN 旁边的复选框，将其分配到实例。

   有关 VLAN 分配的详细信息，请参见第 75 页。

5. 在 Private to Public 区域，单击 Add Row 填写字段，然后单击 Save。

字段	描述	
Private IP Address	键入一个专用的 IP 地址： • 要转换单个地址，为专用子网上的设备键入现有地址。 • 要转换一个地址范围，键入连续地址范围内的第一个地址。 • 要转换子网内的多个地址，为专用子网上的设备键入现有起始地址。为进行转换，该地址必须与子网掩码大小相对应，如下所示。	
	子网掩码	**起始专用子网地址**
	255.255.0.0	最后两个八位字节必须为 0。 **示例：** 192.168.0.0
	255.255.255.0	最后一个八位字节必须为 0。 **示例：** 192.168.1.0
	255.255.255.128	最后一个八位字节必须为 0 或 128。 **示例：** 192.168.1.0 或 192.168.1.128
	255.255.255.192	最后一个八位字符必须为以下之一：0、64、128、192。 **示例：** 192.168.1.64
	255.255.255.224	最后一个八位字符必须为以下之一：0、32、64、96、128、160、192、224。 **示例：** 192.168.1.32
	255.255.255.240	最后一个八位字符必须为以下之一：0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240。 **示例：** 192.168.1.16
Public IP Address	键入一个公共的 IP 地址： • 要转换单个地址，键入一个唯一的公共地址来表示该设备。 • 要转换一个地址范围，键入连续地址范围内的第一个地址。 • 要转换子网中的多个地址，键入一个唯一的起始公共地址来表示这些设备。为进行转换，该地址必须与子网掩码大小相对应，如下所示。	
	子网掩码	**起始公共子网地址**
	255.255.0.0	最后两个八位字节必须为 0。 **示例：** 10.200.0.0
	255.255.255.0	最后一个八位字节必须为 0。 **示例：** 10.200.1.0。
	255.255.255.128	最后一个八位字节必须为 0 或 128。 **示例：** 10.200.1.0 或 10.200.1.128
	255.255.255.192	最后一个八位字符必须为以下之一：0、64、128、192。 **示例：** 10.200.1.64
	255.255.255.224	最后一个八位字符必须为以下之一：0、32、64、96、128、160、192、224。 **示例：** 10.200.1.32
	255.255.255.240	最后一个八位字符必须为以下之一：0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240。 **示例：** 10.200.1.16
Type	在以下值中选择一项： • Single — 转换单个地址。 • Range — 转换一个地址范围。 • Subnet — 转换专用子网或专用子网某一部分中的所有地址。	
Range	键入要转换的地址数。该字段只有在 Type 字段中选择 Range 时可用。 有效值：1…128 默认值 = 1 **重要信息：**范围中的每个地址计作一个转换条目。交换机最多支持 128 个转换条目。	
Subnet Mask	为要转换的地址键入子网掩码。 有效值： • B 类：255.255.0.0 • C 类：255.255.255.0 • C 类部分： – 255.255.255.128 （每个转换条目提供 128 个地址） – 255.255.255.192 （每个转换条目提供 64 个地址） – 255.255.255.224 （每个转换条目提供 32 个地址） – 255.255.255.240 （每个转换条目提供 16 个地址）	

6. 在 Gateway Translation 区域中，单击 Add Row 填写字段，然后单击 Save。

   网关转换使公共子网上的设备可与专用子网上的设备通信。

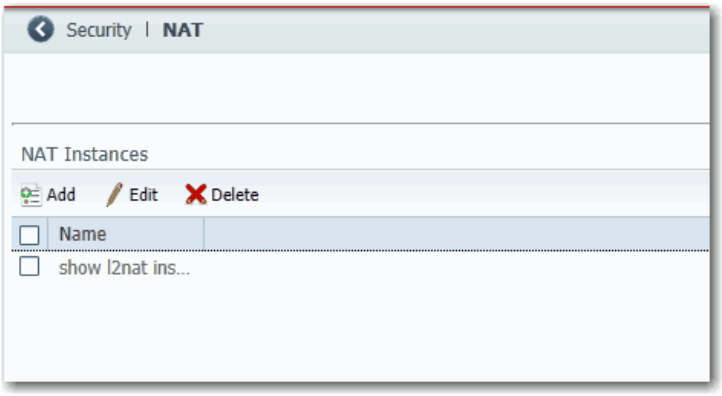
字段	描述
Public	键入第 3 层交换机或连接到交换机上行端口的路由器的默认网关地址。
Private	键入一个唯一的 IP 地址来表示第 3 层交换机或专用网络上的路由器。

7. （可选）。要配置通信许可和数据包修复，请转到第 120 页上的配置通信许可和修复。
8. 单击 Submit。

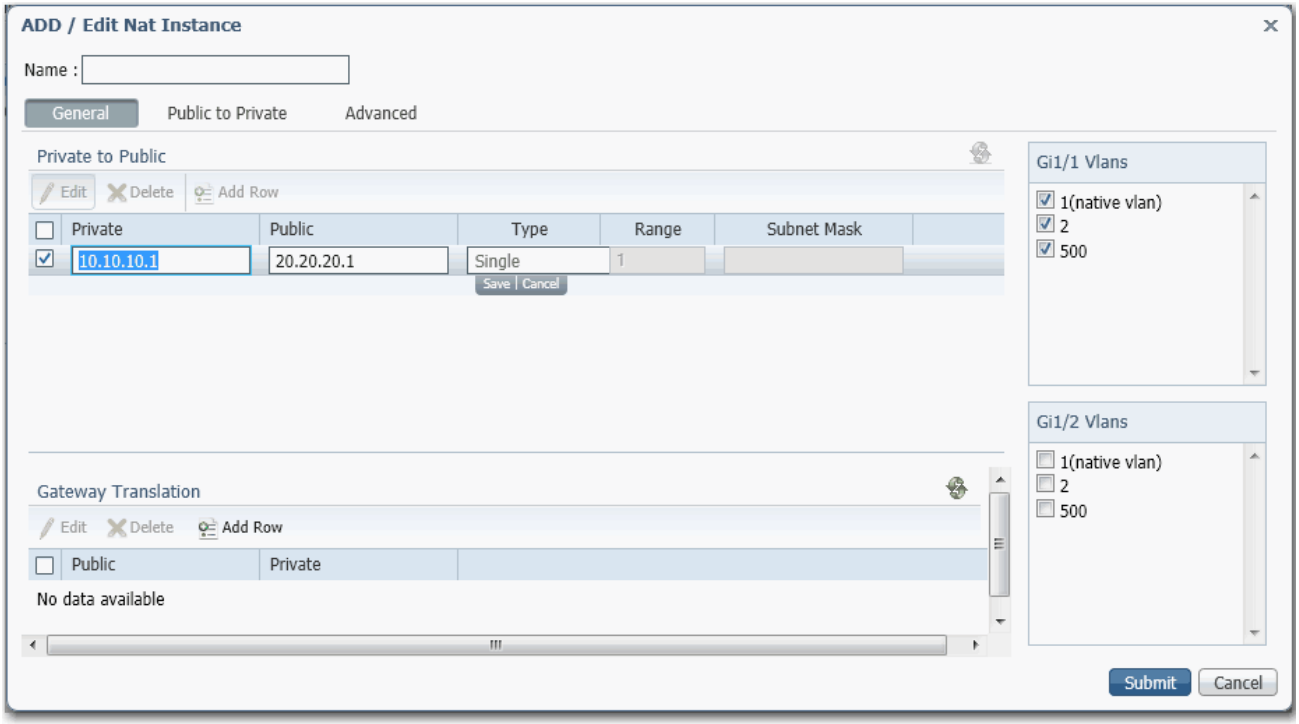
为通过第 2 层交换机或路由器进行路由的通信创建 NAT 实例

要为通过第2层交换机进行路由的通信创建 NAT 实例，请遵循以下步骤。

1. 从 Configure 菜单中，选择 NAT 以显示 NAT 窗口。



2. 单击 Add 显示 Add/Edit NAT Instance 窗口的 General 选项卡。



3. 在 Name 字段中，为实例输入唯一的名称。

   实例名称不能包含空格，不可超过 32 个字符。

4. 从右侧的 VLAN 列表中，选中每个 VLAN 旁边的复选框，将其分配到实例。

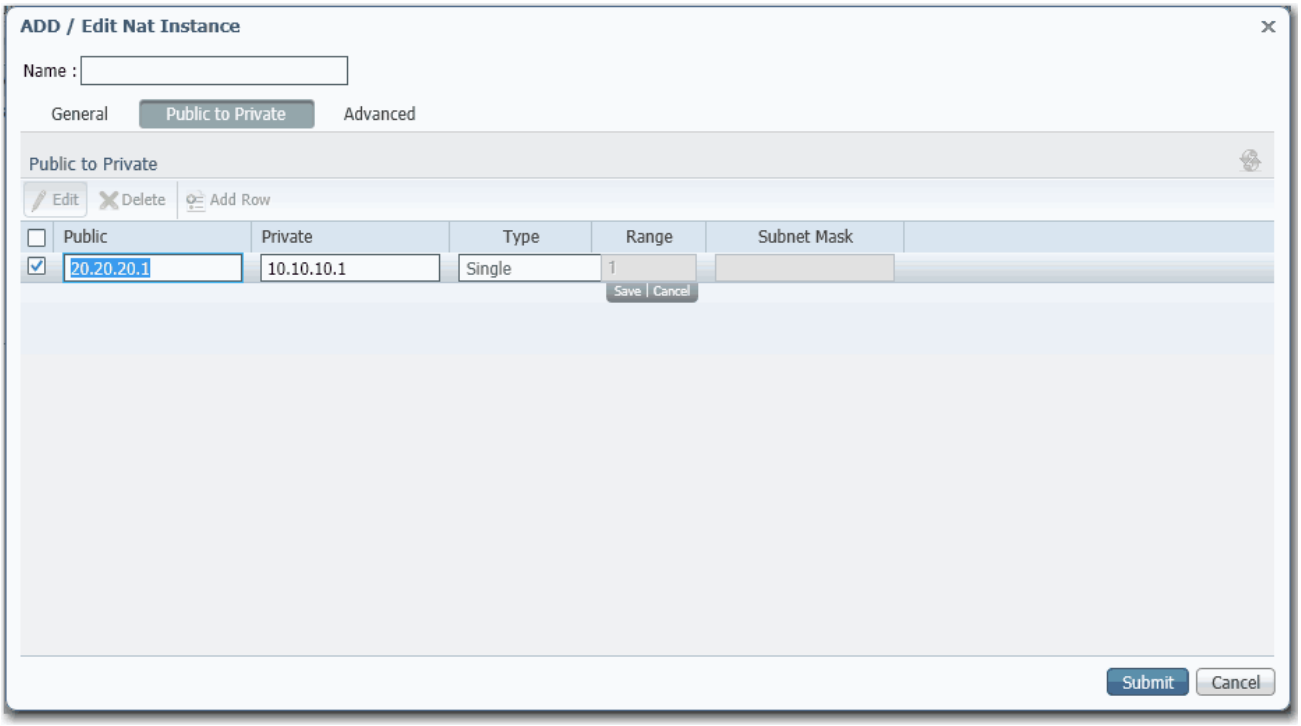
   有关 VLAN 分配的详细信息，请参见第 75 页。

5. 在 Private to Public 区域，单击 Add Row 填写字段，然后单击 Save。

<table>
<tr><th>字段</th><th colspan="2">描述</th></tr>
<tr><td>Private IP Address</td><td colspan="2">键入一个专用的 IP 地址:
• 要转换单个地址，为专用子网上的设备键入现有地址。
• 要转换一个地址范围，键入连续地址范围内的第一个地址。
• 要转换子网内的多个地址，为专用子网上的设备键入现有起始地址。为进行转换，该地址必须与子网掩码大小相对应，如下所示。</td></tr>
<tr><td></td><td>子网掩码</td><td>起始专用子网地址</td></tr>
<tr><td></td><td>255.255.0.0</td><td>最后两个八位字节必须为 0。
示例： 192.168.0.0</td></tr>
<tr><td></td><td>255.255.255.0</td><td>最后一个八位字节必须为 0。
示例： 192.168.1.0</td></tr>
<tr><td></td><td>255.255.255.128</td><td>最后一个八位字节必须为 0 或 128。
示例： 192.168.1.0 或 192.168.1.128</td></tr>
<tr><td></td><td>255.255.255.192</td><td>最后一个八位字符必须为以下之一：0、64、128、192。
示例： 192.168.1.64</td></tr>
<tr><td></td><td>255.255.255.224</td><td>最后一个八位字符必须为以下之一：0、32、64、96、128、160、192、224。
示例： 192.168.1.32</td></tr>
<tr><td></td><td>255.255.255.240</td><td>最后一个八位字符必须为以下之一：0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240。
示例： 192.168.1.16</td></tr>
<tr><td>Public IP Address</td><td colspan="2">键入一个公共的 IP 地址:
• 要转换单个地址，键入一个唯一的公共地址来表示该设备。
• 要转换一个地址范围，键入连续地址范围内的第一个地址。
• 要转换子网中的多个地址，键入一个唯一的起始公共地址来表示这些设备。为进行转换，该地址必须与子网掩码大小相对应，如下所示。</td></tr>
<tr><td></td><td>子网掩码</td><td>起始公共子网地址</td></tr>
<tr><td></td><td>255.255.0.0</td><td>最后两个八位字节必须为 0。
示例： 10.200.0.0</td></tr>
<tr><td></td><td>255.255.255.0</td><td>最后一个八位字节必须为 0。
示例： 10.200.1.0。</td></tr>
<tr><td></td><td>255.255.255.128</td><td>最后一个八位字节必须为 0 或 128。
示例： 10.200.1.0 或 10.200.1.128</td></tr>
<tr><td></td><td>255.255.255.192</td><td>最后一个八位字符必须为以下之一：0、64、128、192。
示例： 10.200.1.64</td></tr>
<tr><td></td><td>255.255.255.224</td><td>最后一个八位字符必须为以下之一：0、32、64、96、128、160、192、224。
示例： 10.200.1.32</td></tr>
<tr><td></td><td>255.255.255.240</td><td>最后一个八位字符必须为以下之一：0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240。
示例： 10.200.1.16</td></tr>
</table>

字段	描述
Type	在以下值中选择一项： • Single — 转换单个地址。 • Range — 转换一个地址范围。 • Subnet — 转换专用子网或专用子网某一部分中的所有地址。
Range	键入要转换的地址数。该字段只有在 Type 字段中选择 Range 时可用。 有效值：1…128 默认值 = 1 **重要信息：**范围中的每个地址计作一个转换条目。交换机最多支持 128 个转换条目。
Subnet Mask	为要转换的地址键入子网掩码。 有效值： • B 类：255.255.0.0 • C 类：255.255.255.0 • C 类部分： – 255.255.255.128 （每个转换条目提供 128 个地址） – 255.255.255.192 （每个转换条目提供 64 个地址） – 255.255.255.224 （每个转换条目提供 32 个地址） – 255.255.255.240 （每个转换条目提供 16 个地址）

6. 单击 Public to Private 选项卡。



7. 单击 Add Row 填写字段，然后单击 Save。

字段	描述	
Public IP Address	键入一个公共的 IP 地址： • 要转换单个地址，为公共子网上的设备键入现有地址。 • 要转换一个地址范围，键入连续地址范围内的第一个地址。 • 要转换子网内的多个地址，为公共子网上的设备范围键入现有起始地址。为进行转换，该地址必须与子网掩码大小相对应，如下所示。	
	子网掩码	**起始公共子网地址**
	255.255.0.0	最后两个八位字节必须为 0。 **示例：** 10.200.0.0
	255.255.255.0	最后一个八位字节必须为 0。 **示例：** 10.200.1.0。
	255.255.255.128	最后一个八位字节必须为 0 或 128。 **示例：** 10.200.1.0 或 10.200.1.128
	255.255.255.192	最后一个八位字符必须为以下之一：0、64、128、192。 **示例：** 10.200.1.64
	255.255.255.224	最后一个八位字符必须为以下之一：0、32、64、96、128、160、192、224。 **示例：** 10.200.1.32
	255.255.255.240	最后一个八位字符必须为以下之一：0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240. **示例：** 10.200.1.16
Private IP Address	键入一个专用的 IP 地址： • 要转换单个地址，键入一个唯一的专用地址来表示该设备。 • 要转换一个地址范围，键入连续地址范围内的第一个地址。 • 要转换子网中的多个地址，键入一个唯一的起始专用地址来表示这些设备。为进行转换，该地址必须与子网掩码大小相对应，如下所示。	
	子网掩码	**起始专用子网地址**
	255.255.0.0	最后两个八位字节必须为 0。 **示例：** 192.168.0.0
	255.255.255.0	最后一个八位字节必须为 0。 **示例：** 192.168.1.0
	255.255.255.128	最后一个八位字节必须为 0 或 128。 **示例：** 192.168.1.0 或 192.168.1.128
	255.255.255.192	最后一个八位字符必须为以下之一：0、64、128、192。 **示例：** 192.168.1.64
	255.255.255.224	最后一个八位字符必须为以下之一：0、32、64、96、128、160、192、224。 **示例：** 192.168.1.32
	255.255.255.240	最后一个八位字符必须为以下之一：0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240。 **示例：** 10.200.1.16
Type	在以下值中选择一项： • Single — 转换单个地址。 • Range — 转换一个地址范围。 • Subnet — 转换公共子网或公共子网某一部分中的所有地址。	
Range	键入要转换的地址数。该字段只有在 Type 字段中选择 Range 时可用。 有效值：1…128 默认值 = 1 **重要信息：**范围中的每个地址计作一个转换条目。交换机最多支持 128 个转换条目。	
Subnet Mask	为要转换的地址键入子网掩码。 有效值： • B 类：255.255.0.0 • C 类：255.255.255.0 • C 类部分： – 255.255.255.128 （每个转换条目提供 128 个地址） – 255.255.255.192 （每个转换条目提供 64 个地址） – 255.255.255.224 （每个转换条目提供 32 个地址） – 255.255.255.240 （每个转换条目提供 16 个地址）	

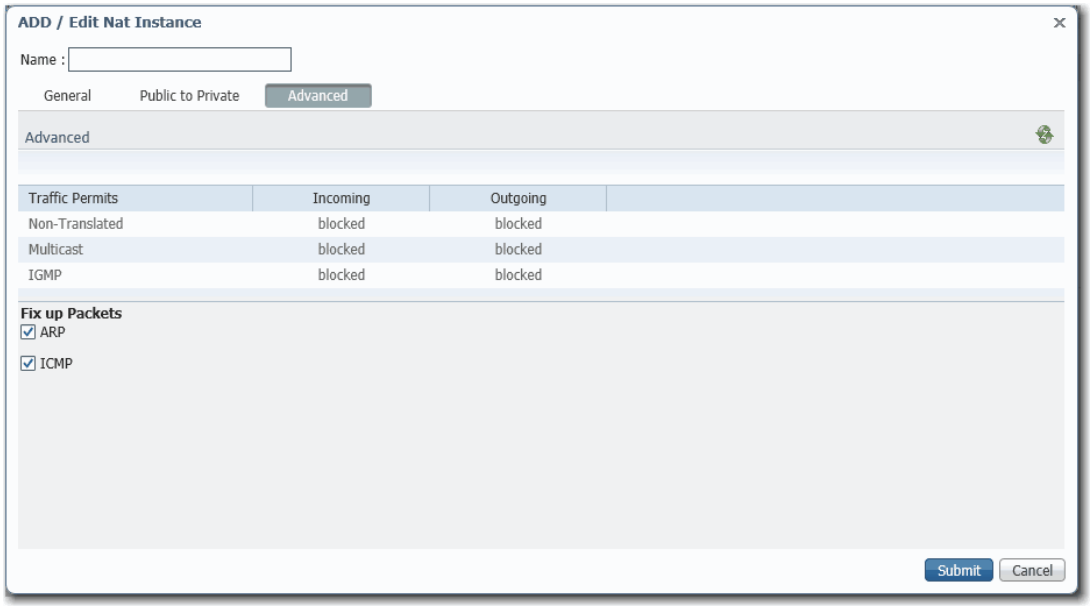
8. （可选）。要配置通信许可和数据包修复，请转到下面的配置通信许可和修复。
9. 在 NAT 窗口上，单击 Submit。

配置通信许可和修复

配置通信许可和修复时应小心谨慎。建议使用默认值。

要配置通信许可和修复，请按以下步骤操作。

1. 单击 Advanced 选项卡。



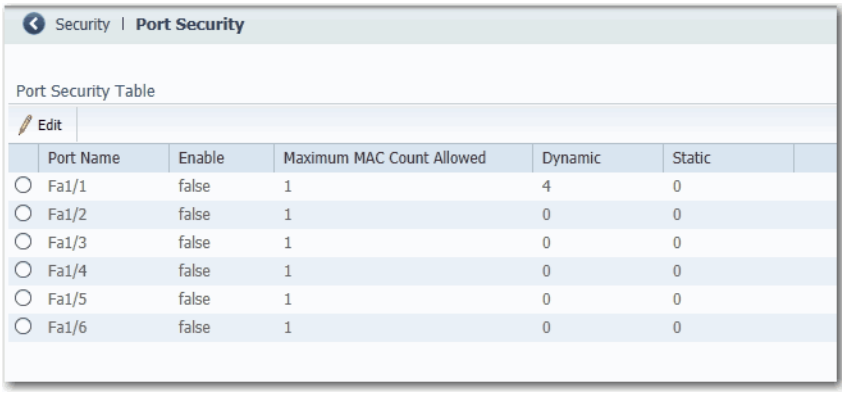
2. 为不由 NAT 处理的传入和传出数据包选择其中一个选项：
   - Pass-through — 允许数据包通过 NAT 边界。
   - Blocked — 丢弃数据包。
3. 在 Fix up Packets 区域中，选中或清除该复选框可以启用或禁用 ARP 和 ICMP 的修复。

   默认情况下，ARP 和 ICMP 的修复处于启用状态。
4. 单击 Submit。

配置端口安全性

配置端口安全性以限制可访问给定端口的 MAC 地址 (MAC ID)。端口安全性基于所支持的 MAC 地址数（这些地址都不是静态定义的）。静态端口安全性使您可以指定 MAC 地址为自动学习还是手动定义的。

要配置端口安全性，从 Configure 菜单中选择 Port Security。



端口安全性限制并指明了可通过交换机端口发送通信的设备的 MAC 地址。交换机端口不会转发来自已定义设备组以外设备的通信。出现以下任何情况时会发生安全侵犯：

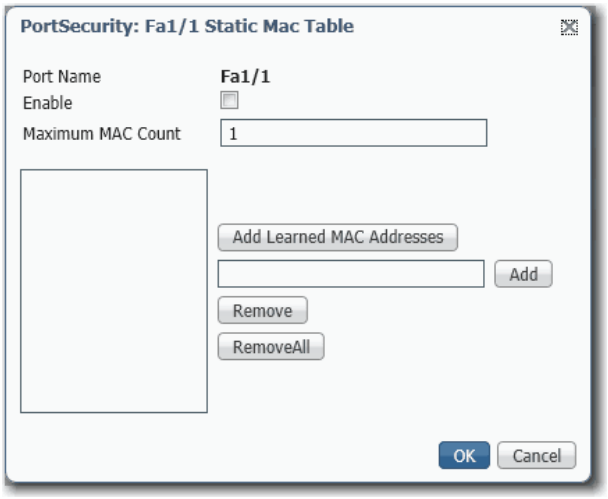
- MAC 地址不同于任何指明的安全 MAC 地址的设备试图访问交换机端口。
- 端口上的 MAC 地址数超出该端口支持的最大数值。

端口安全性支持多个安全级别：

- 定义连接到给定端口设备数的能力。IP 按照设备先到先得的原则分配，如果在一段时间内未激活将失效。
- 通过选择静态 MAC 地址表上的 Add Learned MAC Addresses，轻松存储现有 MAC 地址配置的能力。
- 手动添加和移除每个端口上的 MAC 地址的能力。

要更改端口的静态 MAC 地址表，请按以下步骤操作：

1. 单击端口旁边的单选按钮进行配置。
2. 单击 Edit。
3. 清除或选中 Enable 复选框。
4. 按以下方法配置 MAC 地址：
   - 要添加当前连接到端口的设备的现有 MAC 地址，单击 Add Learned MAC Addresses。
   - 要将特定的 MAC 地址添加到该表，在格式字段中键入 MAC 地址，然后单击 Add。
   - 要从表中移除 MAC 地址，选择该 MAC 地址，然后单击 Remove。
   - 要清除 MAC 地址表，单击 Remove All。



5. 单击 OK。

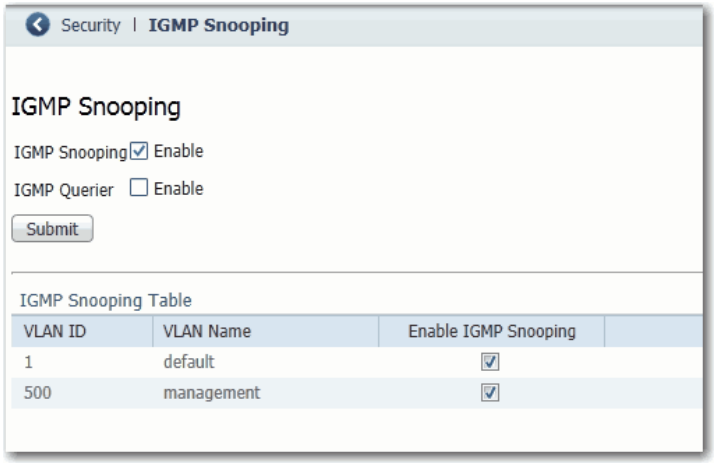
配置 IGMP 监听

Internet 组管理协议 (IGMP) 的监听功能可以将 IP 多播通信转发到特定交换机端口，而不是填满所有端口，这就减少了网络上的重复和过量通信。

凭借 IGMP 监听功能，仅隶属于特定 IP 多播组的端口才可接收到多播消息。因此，带宽的使用效率得到提升。

要配置 IGMP 监听，从 Configure 菜单中选择 IGMP Snooping：

- 要为所有 VLAN ID 启用 IGMP 监听，选中 IGMP Snooping 旁边的 Enable。
- 要为所有 VLAN ID 启用 IGMP 查询器，选中 IGMP Querier 旁边的 Enable。
- 要启用或禁用 VLAN 上的 IGMP 监听，选择该 VLAN，然后选中或清除 Enable IGMP Snooping 复选框。

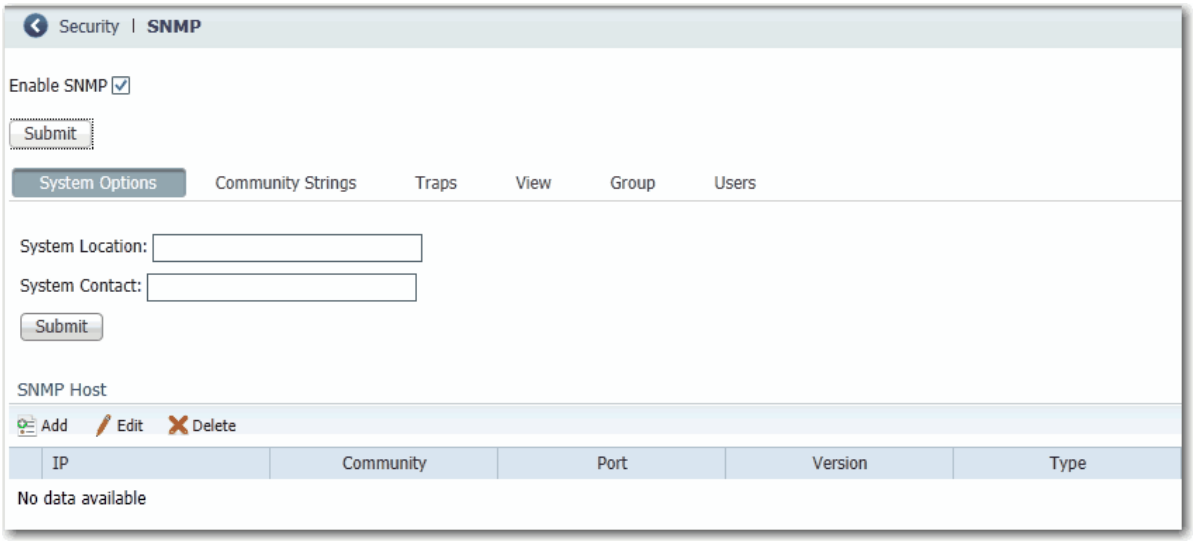


配置 SNMP

如果要通过其它网络管理应用程序管理交换机，则启用 SNMP。默认情况下，SNMP 处于禁用状态。

其它常规 SNMP 设置还包括交换机名称、网络管理员姓名和交换机位置。系统名称和系统联系信息位于 Dashboard 上的 Switch Information 区域中。

要配置 SNMP，从 Configure 菜单中选择 SNMP。



社区字符串是交换机管理信息库 (MIB) 的密码。可以创建相应的社区字符串，将远程管理员对交换机的访问权限设置为只读- 或可读写。

要创建、修改和删除社区字符串，单击 Community Strings 选项卡。

只读社区字符串使交换机可以验证来自网络管理站的获取（只读- ）请求。如果设置 SNMP 只读社区，则用户仅可访问 MIB 对象，不能对其进行更改。

读写社区字符串使交换机可以验证来自网络管理站的设置（读- 写）请求。

使用 SNMP 管理应用程序

可以使用 SNMP 管理应用程序（如 IntraVue 或 HP OpenView）来配置和管理此交换机。有关详细信息，请参见第 80 页上的SNMP。

配置报警设置

交换机软件将监视每个端口或全部端口的状况。如果状况与设定的参数不符，将触发报警或系统消息。默认情况下，交换机会将系统消息发送到记录设备。可以配置交换机，使其将 SNMP 陷阱发送到 SNMP 服务器。也可通过使用两个独立的报警继电器配置交换机，使其触发外部报警装置。

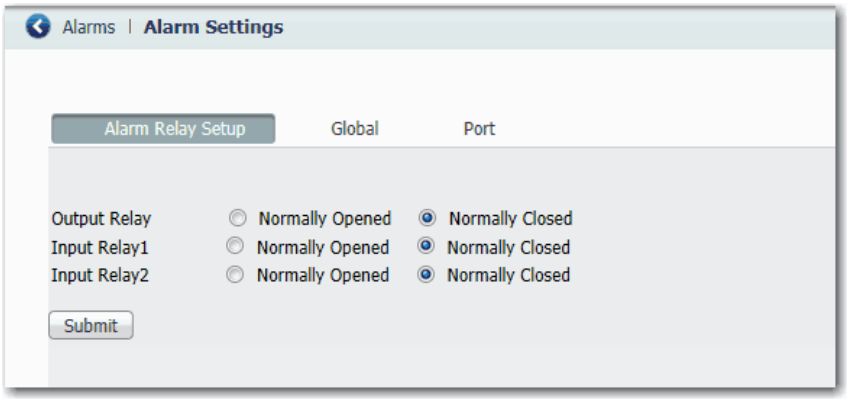
报警继电器设置

可以配置交换机，使其触发外部报警装置。交换机支持两个报警输入和一个报警输出。配置后，交换机软件可以检测使继电器线圈通电的故障，并更改继电器两个触点的状态。常开触点会闭合，而常闭触点则断开。

要配置报警继电器设置，从 Configure 菜单中选择 Alarm Settings。

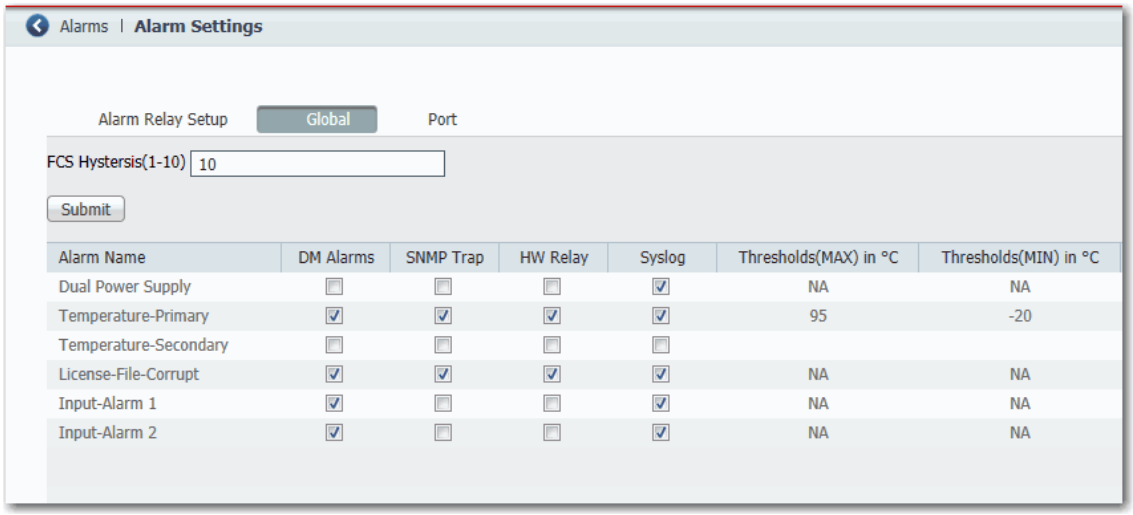
在 Alarm Relay Setup 选项卡上，针对每个报警继电器类型单击其中一个选项：

- Normally Opened — 正常情况下没有电流经过触点。当电流经过时，将生成报警。
- Normally Closed — 正常情况下有电流经过触点。当电流停止时，将生成报警。



全局报警

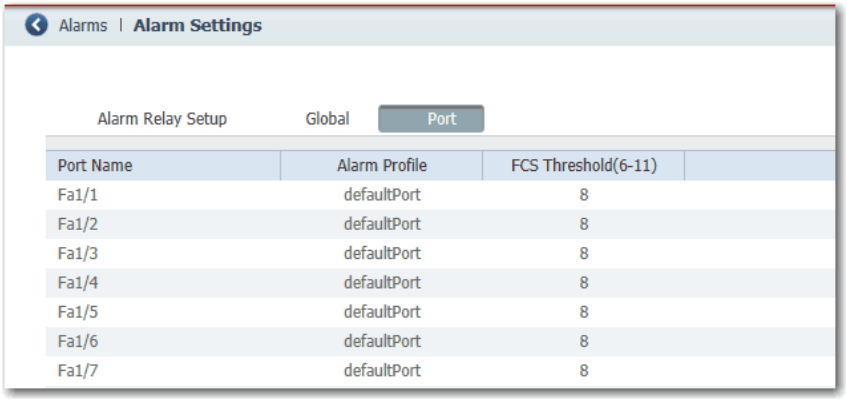
要配置全局报警（也称为设备报警），从 Configure 菜单中选择 Alarm Settings 并单击 Global 选项卡。



字段	描述
FCS Hysteresis (1-10)	帧校验序列 (FCS) 错误滞值阈值用于确定清除报警条件的时间。该值以 FCS 误码率的波动百分比形式表示。默认设置为 8%。 可以调整这一百分比，防止 FCS 误码率的波动接近配置误码率时切换报警条件。全局设置的有效百分比为 1…10。也可通过单击 Port 选项卡在各个端口上对该设置进行配置。
Alarm Name	可启用或禁用以下报警类型： • Dual Power Supply — 交换机监视直流电源电平。如果系统配置为在双电源模式下运行，则当其中一个电源发生故障或丢失时，将触发报警。当电源出现或处于运行状态时，将自动清除报警。可以将电源报警配置为连接到硬件继电器。 • Temperature-Primary — 当系统温度高于或低于配置的温度阈值时将触发这些报警。默认情况下，主温度报警与主继电器关联。 • Temperature-Secondary — 当系统温度高于或低于配置的温度阈值时将触发这些报警。 • License-File-Corrupt — 许可文件损坏时会触发报警。 • Input-Alarm 1 — 根据外部输入报警情况触发报警。 • Input-Alarm 2 — 根据外部输入报警情况触发报警。
DM Alarms	报警信息将出现在设备管理器 Web 界面的操控板上。
SNMP Trap	如果在 Configure > Security > SNMP 窗口中启用了 SNMP，则报警陷阱会被发送到 SNMP 服务器。
HW Relay	交换机报警继电器被触发后，会将故障信号发送到已连接的外部报警装置（如警铃、报警灯或其它已配置的信号设备）。
Syslog	报警陷阱记录在 syslog 中。可以在 Monitor > Syslog 窗口中查看 syslog。
Thresholds (MAX) in ℃	启用后，相应主温度或副温度报警的最大温度阈值。
Thresholds (MIN) in ℃	启用后，相应主温度或副温度报警的最小温度阈值。

端口报警

要为各个端口创建报警配置文件，从 Configure 菜单中选择 Alarm Settings 并单击 Port 选项卡。



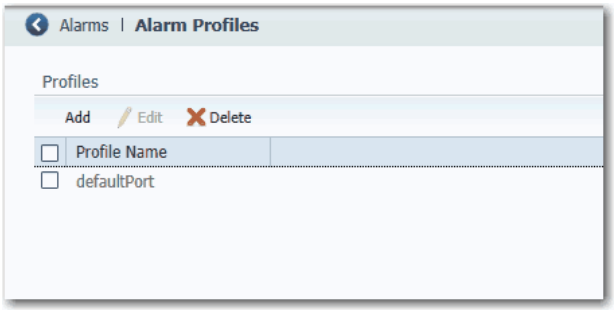
针对每个端口，选择一个报警配置文件并设置 FCS 阈值。帧校验序列 (FCS) 错误滞值阈值以 FCS 误码率的波动百分比形式表示。默认设置为 8%。可以调整这一百分比，防止 FCS 误码率的波动接近配置误码率时切换报警条件。端口设置的有效百分比为 6%...11%。

配置报警配置文件

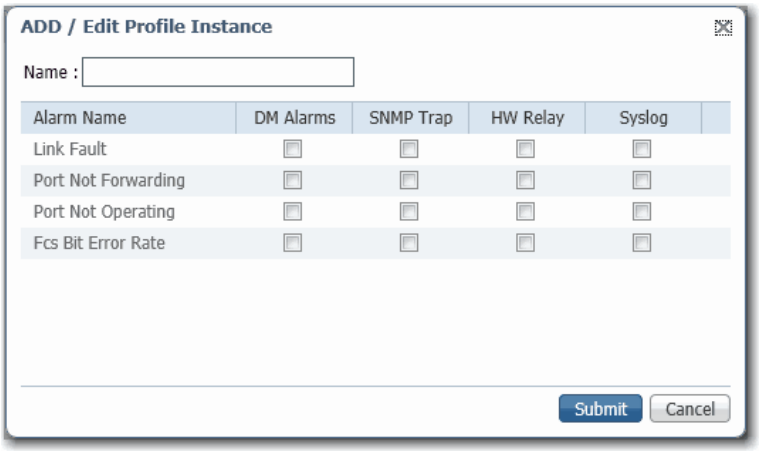
可使用报警配置文件将一组报警设置应用到多个接口。为您创建了以下报警配置文件：

- defaultPort
- ab-alarm （在快速设置过程中创建）

要创建、修改或删除报警配置文件，从 Configure 菜单中选择 Alarm Profiles。



在 Add/Edit Profile Instance 窗口中，可为报警配置文件配置报警和操作。



字段	描述
Name	报警配置文件的唯一名称。
Alarm Name	这些类型的报警可触发一个动作。
DM Alarms	报警信息将出现在设备管理器 Web 界面的操控板上。
SNMP Trap	如果在 Configure > Security > SNMP 窗口中启用了 SNMP，则报警陷阱会被发送到 SNMP 服务器。
HW Relay	交换机报警继电器被触发后，会将故障信号发送到已连接的外部报警装置（如警铃、报警灯或其它已配置的信号设备）。
Syslog	报警陷阱记录在 syslog 中。可以在 Monitor > Syslog 窗口中查看 syslog。

监视趋势

可以查看历史数据，以协助您分析通信模式并找出问题。可按照秒、分钟、小时或天的增量方式显示数据。

要查看表中数据，单击该区域下方的 Grid Mode 按钮。要显示图表，单击 Chart Mode 按钮。使用 60s、1 h、1 d 和 1 w 链接，按照 60 秒、1 小时、1 天或 1 周的增量方式显示数据。

要监视趋势，从 Monitor 菜单中选择 Trends。

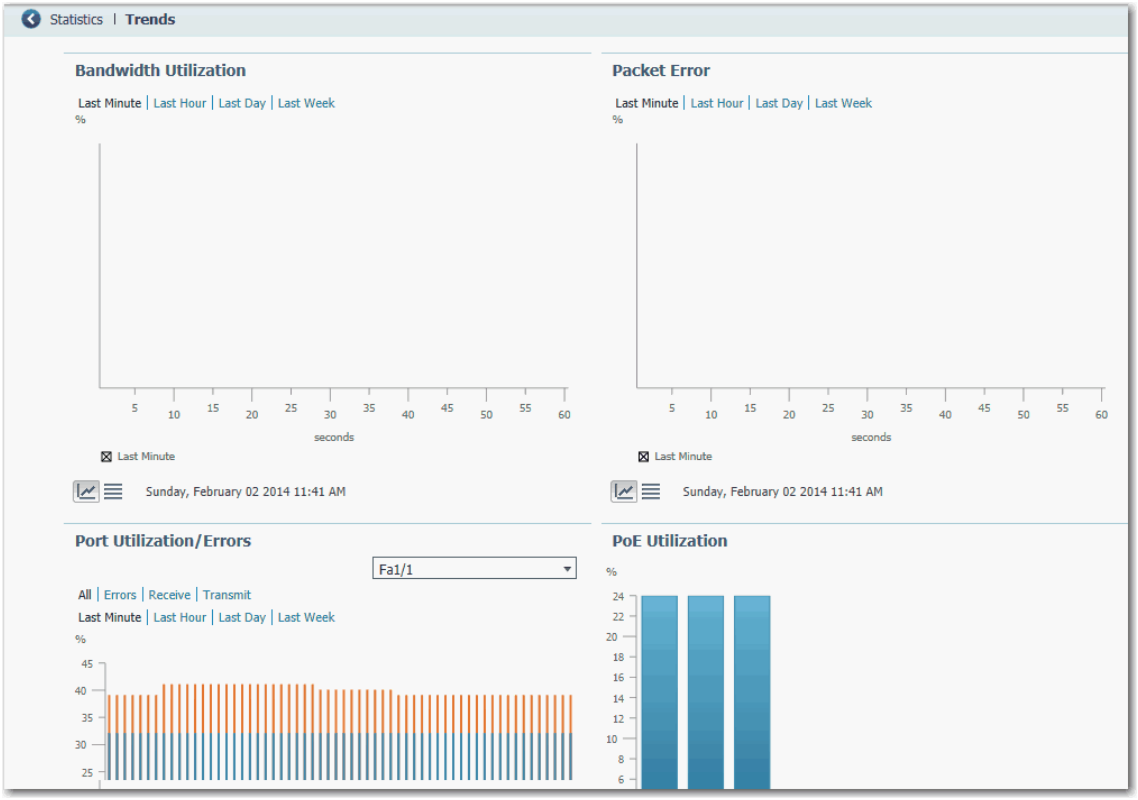


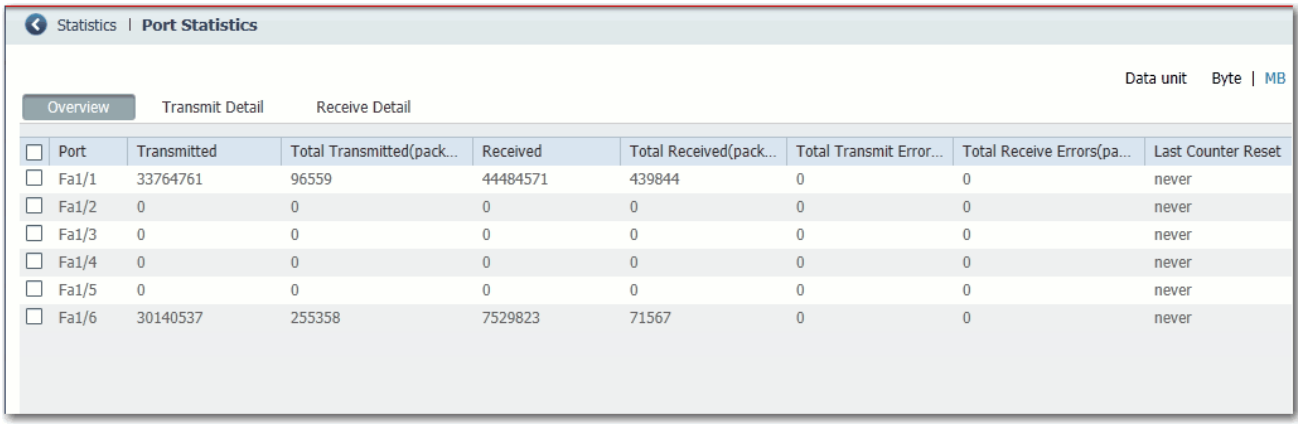
表 17 - 趋势图

图	描述
Bandwidth Utilization	Bandwidth Utilization 图指示已使用的带宽占可用带宽的百分比。该图可按时间的增量实例（每 60 秒、60 分钟、24 小时或 14 天）显示带宽使用情况。此图也标记达到的最高峰值。默认时间为 60 秒。 可以使用该数据确认网络利用率为高或低的时间。
Packet Error	Packet Error 图可按时间的增量实例（每 60 秒、60 分钟、24 小时或 14 天）显示采集的数据包错误百分比。默认时间为 60 秒。 使用此图可以审计所连接的设备对交换机性能或网络产生的影响。例如，如果怀疑所连接的设备正在发送错误数据包，可通过断开可疑设备然后重新连接该设备的方式验证图上的数据是否发生变化。
Port Utilization/Errors	Port Utilization/Errors 图可按时间的增量实例（每 60 秒、60 分钟、24 小时或 14 天）显示特定端口的使用情况。默认时间为 60 秒。 要显示特定端口的趋势，可从 Port 列表中选择该端口。 使用这些图可以观查特定端口的性能。例如，如果网络用户的网络连接发生间歇性中断，则可使用 Port Utilization 图来观查连接用户个人电脑的端口的通信模式，还可使用 Port Errors 图来判断该端口是否正在接收或发送错误数据包。
PoE Utilization	对于 PoE 交换机，PoE Utilization 图显示已分配到所连接设备的电源。

监视端口统计

可查看自交换机上一次接通电源、重启或上一次清除统计以来交换机端口发送和接收的数据统计。

要监视端口统计，从 Monitor 菜单中选择 Port Statistics。更多信息，请参见设备管理器 Web 界面的在线帮助。



Port	Transmitted	Total Transmitted(pack...	Received	Total Received(pack...	Total Transmit Error...	Total Receive Errors(pa...	Last Counter Reset
Fa1/1	33764761	96559	44484571	439844	0	0	never
Fa1/2	0	0	0	0	0	0	never
Fa1/3	0	0	0	0	0	0	never
Fa1/4	0	0	0	0	0	0	never
Fa1/5	0	0	0	0	0	0	never
Fa1/6	30140537	255358	7529823	71567	0	0	never

在设备管理器 Web 界面的 Port Statistics 窗口中，收集和显示的端口统计类型按以下选项卡分组：

- Overview 选项卡 — 使用此选项卡可以显示端口接收和发送的错误数据包的具体数量，操控板中图的信息达不到这种详细程度。

  错误数据包的数量可能意味着双工模式不匹配、与端口及相连设备不兼容，以及电缆或相连设备存在故障。上述任何问题都可能导致网络性能降低、数据丢失或连接中断。

- Transmit Detail 选项卡 — 使用此选项卡可以处理网络通信中流量异常变化的问题。此选项卡显示以下统计：

  – 每个端口发送的单播、多播和广播数据包
  – 发送到每个端口的错误的详细统计信息

  如果端口正在发送异常高的通信量（例如多播或广播数据包），则可监视相连的设备，检查此通信模式是否正常，或是否会导致故障。

- Receive Detail 选项卡 — 使用此选项卡可以处理网络通信中流量异常变化的问题。此选项卡显示以下统计：

  – 每个端口接收的单播、多播和广播数据包
  – 每个端口接收的错误的详细统计信息

  如果端口正在接收异常高的通信量（例如多播或广播数据包），则可监视相连的设备，检查此通信模式对相连设备来说是否正常，或是否会导致故障。

监视 NAT 统计

可以监视以下类型的 NAT 统计：

- 针对所有实例的全局统计
- 每个实例的统计
- 每个实例详细的专用转换
- 每个实例详细的公共转换

要显示 NAT Statistics 窗口，从 Monitor 菜单中选择 NAT Statistics。

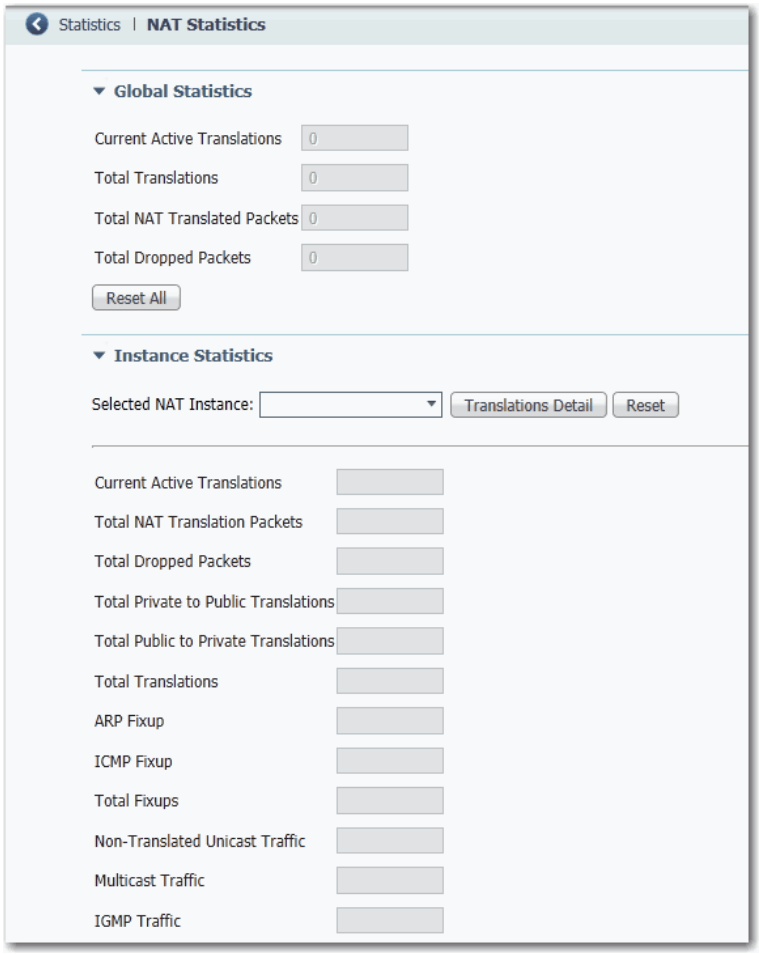


表 18 - NAT 全局统计

字段	描述
Current Active Translations	所有 NAT 实例中最后 90 秒内被转换的 IP 地址数。
Total Translations	所有 NAT 实例中的转换总数。
Total NAT Translated Packets	所有 NAT 实例中的数据包总数。
Total Dropped Packets	所有 NAT 实例中被丢弃的数据包总数。

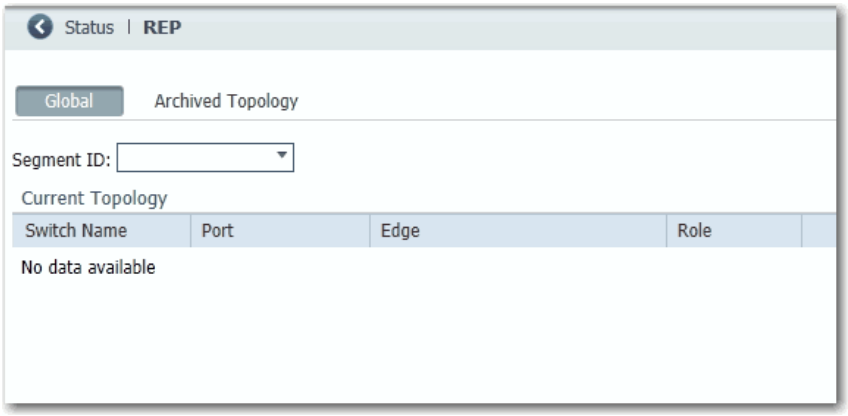
表 19 - 实例统计

字段	描述
Selected Instance	从下拉菜单中，选择要查看其统计的实例。
Current Active Translations	该实例在最后 90 秒内发生的转换数。
Total NAT Translated Packets	已为该实例转换的数据包总数。
Total Dropped Packets	已为该实例丢弃的数据包总数。
Total Private to Public Address Translations	针对专用子网上的设备配置的转换总数。
Total Public to Private Address Translations	针对公共子网上的设备配置的转换总数。
Total Translations	已为该实例配置的转换总数。
ARP Fixup	已为该实例修复的 ARP 数据包数。
ICMP Fixup	已为该实例修复的 ICMP 数据包数。
Total Fixups	已为该实例修复的 ARP 和 ICMP 数据包总数。
Non-Translated Unicast Traffic	该实例未转换的单播通信的数据包数。
Multicast Traffic	该实例的多播通信的数据包数。
IGMP Traffic	该实例的 IGMP 通信的数据包数。

监视 REP 拓扑

要查看一个或所有网段的 REP 拓扑，从 Monitor 菜单中选择 REP。

要显示归档的 REP 拓扑，单击 Archived Topology 选项卡，然后选择 Segment ID。



监视 CIP 状态

通用工业协议 (CIP) 是一种各种工业自动化和控制设备用来作为控制系统的一部分进行通信的应用层信息传输协议。CIP 是 EtherNet/IP 网络的应用层。Stratix 交换机包含 EtherNet/IP 服务器，这使其可以作为工业自动化和控制系统的一部分执行基本的管理和监视工作。

CIP Status 窗口显示 CIP 状态的相关信息（Overview 字段）和交换机自最近一次接通电源、重启或计数器最近一次重置以来的统计信息（Request Details 字段）。

要处理故障，先重置 CIP 计数器，查看计数器是否显示问题仍然存在。

重要信息　**除 Active Multicast Groups 以外，所有其它类别都与交换机中的 CIP 服务器相关，即与作为 CIP 目标设备而专门指向交换机的 CIP 通信相关。它们并不涉及流过交换机的各种 CIP 控制器、HMI 设备、配置工具或其它 CIP 目标设备（例如驱动器、I/O 模块、电机启动器、传感器和阀门）之间的 CIP (EtherNet/IP) 通信。**

要监视 CIP 状态，从 Monitor 菜单中选择 CIP Status。

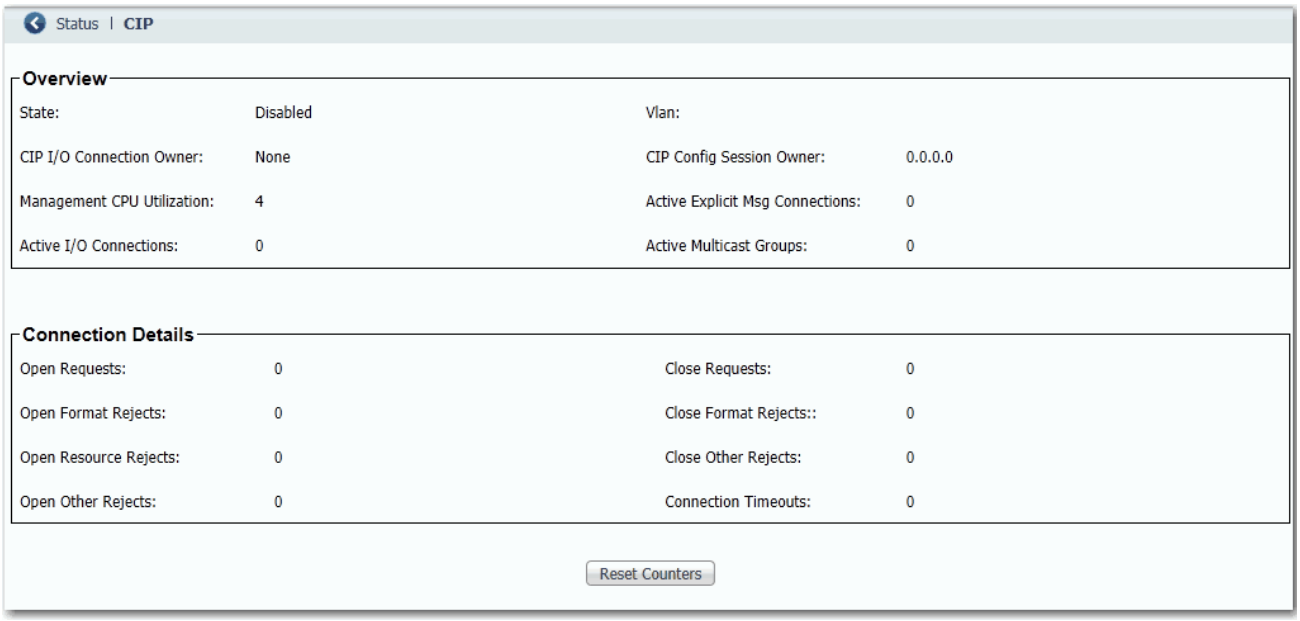


表 20 - CIP Status 字段

字段	描述
Overview	
State	CIP 连接的状态（Enabled 或 Disabled）。
Vlan	VLAN ID。
CIP I/O Connection Owner	向其发送和从其接收应用特定 I/O 输出数据的设备的 IP 地址。
CIP Config Session Owner	控制 CIP 配置会话的设备的 IP 地址。
Management CPU Utilization (%)	管理功能占用管理 CPU 的百分比。交换机功能具有不受管理功能影响的专用 ASIC。
Active Explicit Msg Connections	到交换机的活动、显式报文通信连接的数量。
Active I/O Connections	到交换机的活动 I/O 连接的数量。
Active Multicast Groups	多播组的数量，其中包括流过交换机的 CIP 多播组。
Connection Details	
Open Requests	交换机接收到的与其建立连接的 " 正向打开 " 请求的数量。
Close Requests	交换机在与其成功建立连接后接收到的 " 正向关闭 " 请求的数量。
Open Format Rejects	因为请求的格式不正确而失败的指向交换机的 " 正向打开 " 请求的数量。
Close Format Rejects	因为请求的格式不正确而失败的指向交换机的 " 正向关闭 " 请求的数量。
Open Resource Rejects	由于建立新连接时内存不足等原因而失败的 " 正向打开 " 请求的数量。
Close Other Rejects	因为电子匹配功能不兼容等原因而失败的 " 正向关闭 " 请求的数量。
Open Other Rejects	因为电子匹配功能不兼容等原因而失败的 " 正向打开 " 请求的数量。
Connection Timeouts	由于未激活原因而超时的 CIP 连接的数量。

诊断电缆问题

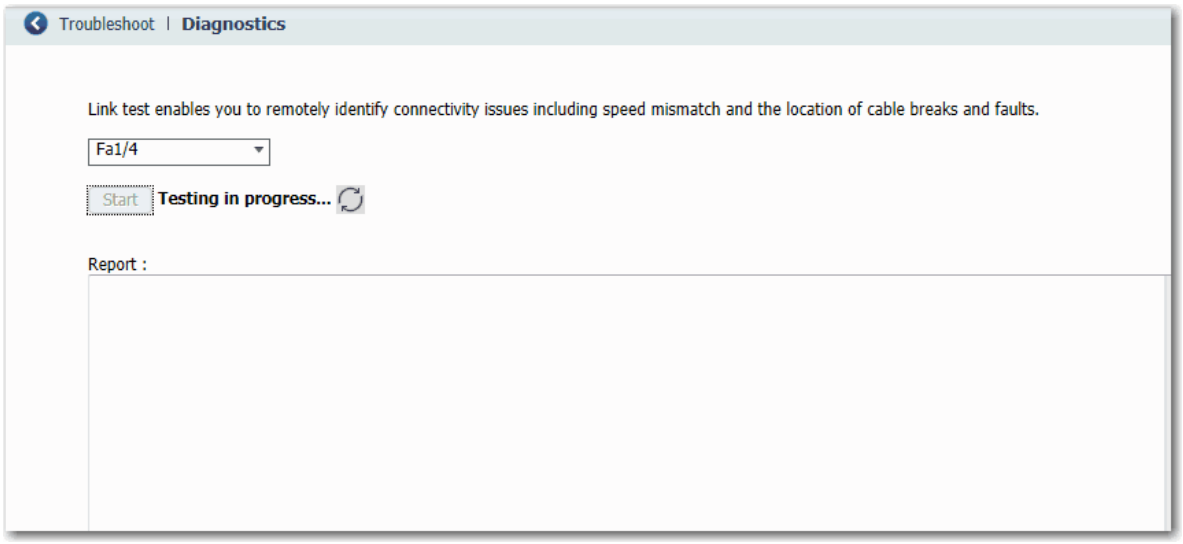
使用 Diagnostics 窗口可以运行断线检测测试，当中会使用时域反射 (TDR) 检测方法找出，诊断并解决电缆问题。电口 Ethernet 10/100 和 10/100/1000 端口支持 TDR 检测。小型可插拔 (SFP) 模块端口不支持 TDR。

链路测试会中断端口和所连接设备间的通信。仅在怀疑存在问题的端口运行该测试。运行链路测试前，使用 Front Panel 视图、Port Status 和 Port Statistics 窗口收集有关潜在问题的信息。

重要信息　**要在千兆端口上运行有效测试，必须先将千兆端口配置为 RJ45 介质类型，如第 96 页上的配置端口设置所述。**

要诊断电缆，从 Monitor 菜单中选择 Diagnostics。

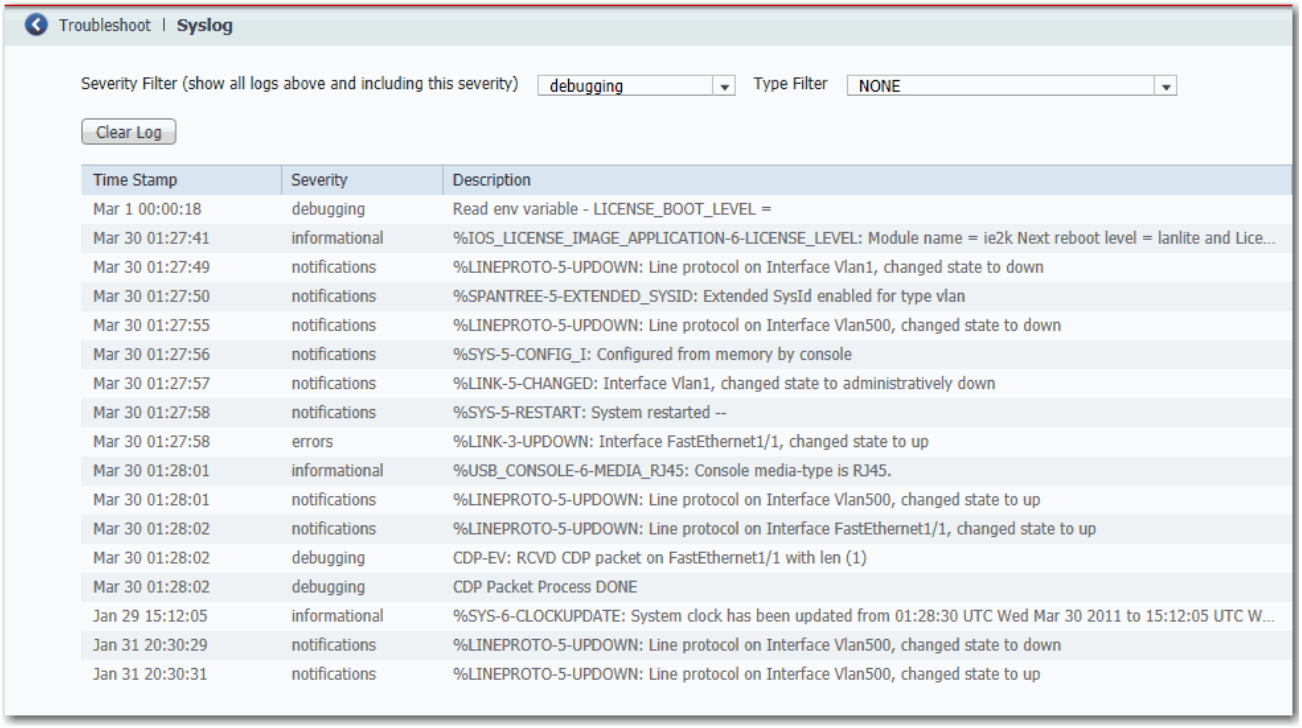
要运行测试，选择一个端口，然后单击 Start。



查看系统日志消息

根据在 Configure > Alarm Settings 窗口中对 Alarm Settings 进行的配置，系统日志显示发生在设备及其端口上的事件。

要查看系统日志消息，从 Monitor 菜单中选择 Syslog。



要过滤历史事件，选择严重性过滤器或类型过滤器：

- Debugging — 调试消息。
- Informational — 信息消息。
- Notifications — 交换机运行正常，但存在值得注意的情况。
- Warnings — 交换机处于警告状态。
- Errors — 交换机有错误。
- Critical — 交换机有严重问题。

- Alerts — 交换机需要立即检修。
- Emergencies — 交换机不可用。

单击 Clear Log 可以确认已阅读该报警信息。单击 Clear Log 并不能解决问题。

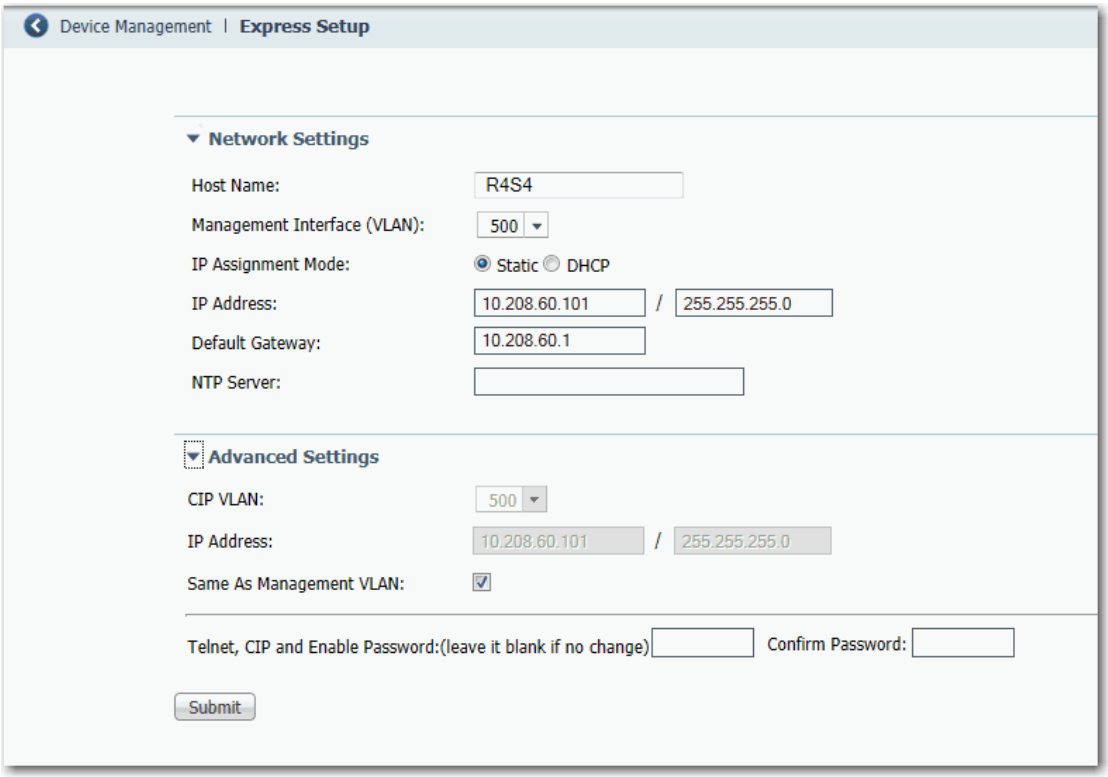
表 21 - Syslog 字段

字段	描述
Time Stamp	事件发生的日期和时间。 使用 Express Setup 窗口将设备连接到 NTP 服务器。如过交换机断电，时间设置将丢失。
Severity Level	事件的类型和严重性。
Description	对问题的描述，包括检测到问题的端口。

使用快速设置更改交换机设置

网络设置使交换机能够以其标准的默认设置运行，并能通过设备管理器的 Web 界面进行管理。这些设置在初始设置过程中设定。如果要将交换机移到不同的管理 VLAN 或不同的网络，请更改这些设置。

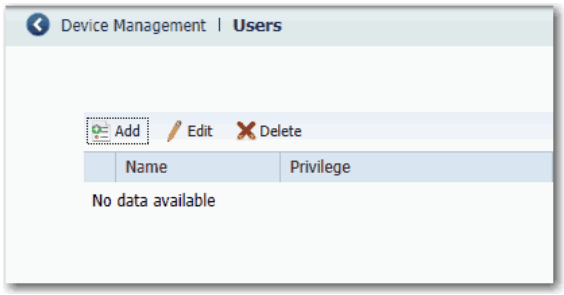
要更新交换机的 IP 信息，从 Admin 菜单中选择 Express Setup。



字段	描述
Network Settings	
Host Name	设备的名称。
Management Interface (VLAN ID)	用于管理交换机的管理 VLAN 的名称和 ID。选择已有的 VLAN 作为管理 VLAN。 默认 ID 为 1。管理 VLAN 的默认名称为 default。该组数字的范围是 1...1001。请确保交换机和网络管理站位在同一 VLAN 中。否则，交换机的管理连接便会丢失。 管理 VLAN 是管理通信在特定用户或设备之间进行传送所通过的广播域。它为必须限定于特定用户组（例如网络管理员）使用的管理通信提供了广播控制及安全功能。它还可以确保任何时候对所有网络设备进行安全的管理访问。
IP Assignment Mode	IP 分配模式决定交换机的 IP 信息为手动分配（静态）还是由动态主机配置协议 (DHCP) 服务器自动分配。默认设置为 Static。 建议单击 Static 并手动为交换机分配 IP 地址。此后，如需访问设备管理器 Web 界面，则可随时使用该 IP 地址。 如果单击 DHCP，则 DHCP 服务器会自动为交换机分配 IP 地址、子网掩码和默认网关。只要交换机未重启，它便可继续使用已分配的 IP 信息，同时可以使用此 IP 地址访问设备管理器 Web 界面。 如果手动分配交换机 IP 地址，但网络使用了 DHCP 服务器，则需确保分配给交换机的 IP 地址不在 DHCP 服务器自动分配给其它设备的地址范围之内。这样可防止交换机与其它设备之间发生 IP 地址冲突。
IP Address	IP 地址和相应的子网掩码是交换机在网络中的唯一标识符： • IP 地址的格式是一个 32 位数字地址，共四组数字，之间用句点分隔。每组数字的范围都是 0...255。 • 子网掩码是标识交换机所属子网络（子网）的网络地址。子网用于在网络中将设备分成更小的组。默认值为 255.255.255.0。 此字段只有在 IP Assignment Mode 为 Static 时才可用。 确保为交换机分配的 IP 地址未被网络中的其它设备使用。IP 地址和默认网关不可相同。
Default Gateway（可选）	默认网关的 IP 地址。网关是交换机和其它网络或子网络中的设备实现通信所需的路由器或专用网络设备。默认网关的 IP 地址必须与交换机 IP 地址在同一子网中。交换机 IP 地址和默认网关 IP 地址不可相同。 如果所有设备都在同一网络中，且未使用默认网关，则无需在此字段中输入 IP 地址。此字段只有在 IP Assignment Mode 为 Static 时才可用。 如果网络管理站和交换机在不同的网络或子网络中，则必须指定默认网关。否则，交换机和网络管理站之间不能相互通信。
NTP Server	网络时间协议 (NTP) 服务器的 IP 地址。NTP 是实现数据包交换、可变延时数据网络上各计算机系统时钟同步的网络协议。
Advanced Settings	
CIP VLAN	启用通用工业协议 (CIP) 的 VLAN。CIP VLAN 可与管理 VLAN 相同，也可在设备上配置的另一个 VLAN 中单独进行 CIP 通信。
IP Address	CIP VLAN 的 IP 地址和子网掩码（CIP VLAN 与管理 VLAN 不同时）。IP 地址的格式是一个 32 位数字地址，共四组数字，之间用句点分隔。每组数字的范围都是 0...255。 确保为设备分配的 IP 地址未被网络中的其它设备使用。
Same As Management VLAN	指示 CIP VLAN 的设置是否与管理 VLAN 相同。
Telnet, CIP and Enable Password（可选）	用于 Telnet 和 CIP 安全性的密码。
Confirm Password	与以上密码相同。

管理用户

要添加、修改或删除交换机的用户和用户登录信息，从 Admin 菜单中选择 Users。



可为每个用户指定下表中的信息。

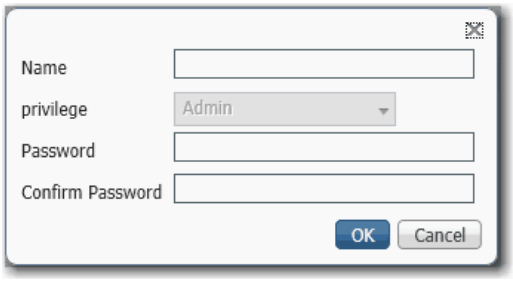


表 22 - 添加用户字段

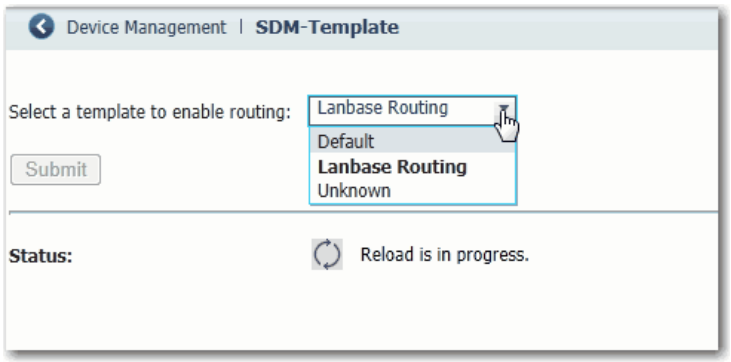
字段	描述
Name	此用户的用户名。
Privilege	此用户的访问级别。为所有用户分配了管理权限，且用户可对任何参数进行更改。
Password	使用此用户名访问时需要的密码。
Confirm Password	与以上密码相同。

为路由重新分配交换机内存

交换机管理数据库 (SDM) 模版针对特定功能（如路由）分配交换机内存的方式进行了优化。要启用路由，必须将默认的 SDM 模版更改为 Lanbase Routing 模版。

要应用 SDM 模版，请按以下步骤操作。

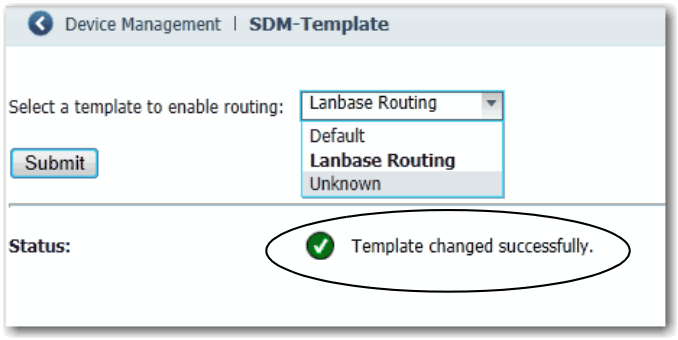
1. 从 Admin 菜单中选择 SDM-Template。
2. 从下拉菜单中选择一个模版：
   - Default — 对第 2 层的所有功能进行平衡
   - Lanbase Routing — 为 IPv4 单播路由最大化系统资源，启用路由时需要这一操作
   - Unknown — 用户从 CLI 配置



3. 单击 Submit。
4. 出现消息提示您继续时，单击 OK。

重要信息　更改模版的过程会导致交换机自动重启。

过程结束后会出现一条消息。



5. 要启用路由，转到第 109 页上的启用和配置路由。

重启交换机

重启或重置交换机会中断设备与网络之间的连接。

要重启或重置交换机，从 Admin 菜单中选择 Restart/Reset。

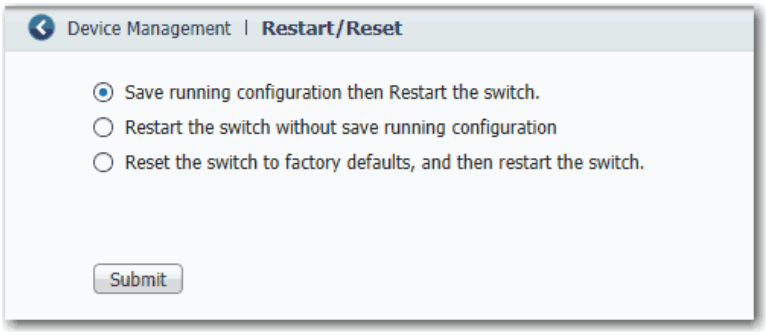


表 23 - 重启 / 重置字段

字段	描述
Save running configuration and then restart the switch.	确保在交换机重启前保存对运行配置的所有更改。
Restart the switch without saving running configuration	使用之前保存的配置设置重启交换机。
Reset the switch to factory defaults, and then restart the switch	将设备重置为出厂默认设置（这会删除当前配置设置），然后重启该设备。 该设备将断开连接，需要启动快速设置才能重新配置该设备。

升级交换机固件

必须具有 Internet 访问权才能从http://www.rockwellautomation.com 将交换机固件下载到计算机或网络驱动器中。

要将交换机的软件和功能升级到最新，从 Admin 菜单中选择 Software Update。

可在设备管理器 Web 界面对交换机逐一进行升级。

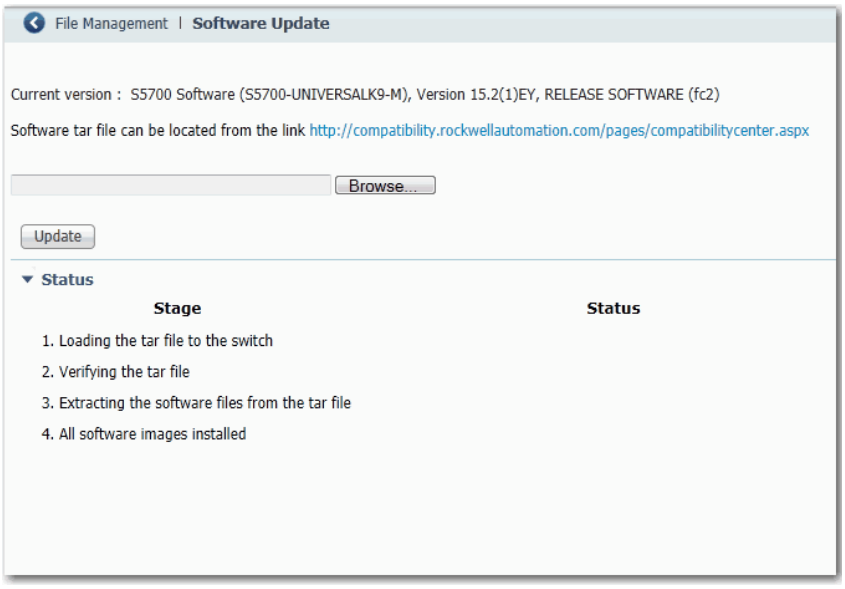
对于固件版本 2.001 或更高，固件升级安装在运行的非易失性内存位置：

- 如果在插入 SD 卡的情况下启动交换机，则升级会被安装在 SD 卡上。
- 如果在未插入 SD 卡的情况下从板载内存启动交换机，则升级会被安装在板载闪存上。

重要信息　**等待升级过程结束。在设备管理器 Web 界面处于激活状态时，不要使用或关闭浏览器会话。不要在另一个浏览器会话中访问设备管理器 Web 界面。**

当升级过程完成后，会显示成功消息，而且交换机将自动重启。配有新固件的交换机重启过程将需要几分钟的时间。

验证交换机最新的固件版本出现在操控板 Switch Information 区域的 Software 字段中。



有关其它准则和步骤，请参见设备管理器 Web 界面的在线帮助。

使用 SD 卡同步配置或 IOS 文件

使用 Sync 窗口可以同步带有板载内存的 SD 卡。在 Manual Sync 选项卡上，可以查看以下内容：

- 是否存在 SD 卡
- 卡的状态
- 如果存在，该卡即为交换机的启动源

可以选择将配置或软件 IOS 从 SD 卡同步到板载内存，或从板载内存同步到 SD 卡。

重要信息　如果同步的方向错误，可覆盖配置。

Auto Sync 选项卡使您可以设置对更改配置或升级 IOS 后设备管理器 Web 界面向用户发出提示的方式的默认选项。

要显示此窗口，从 Admin 菜单中选择 Sync。

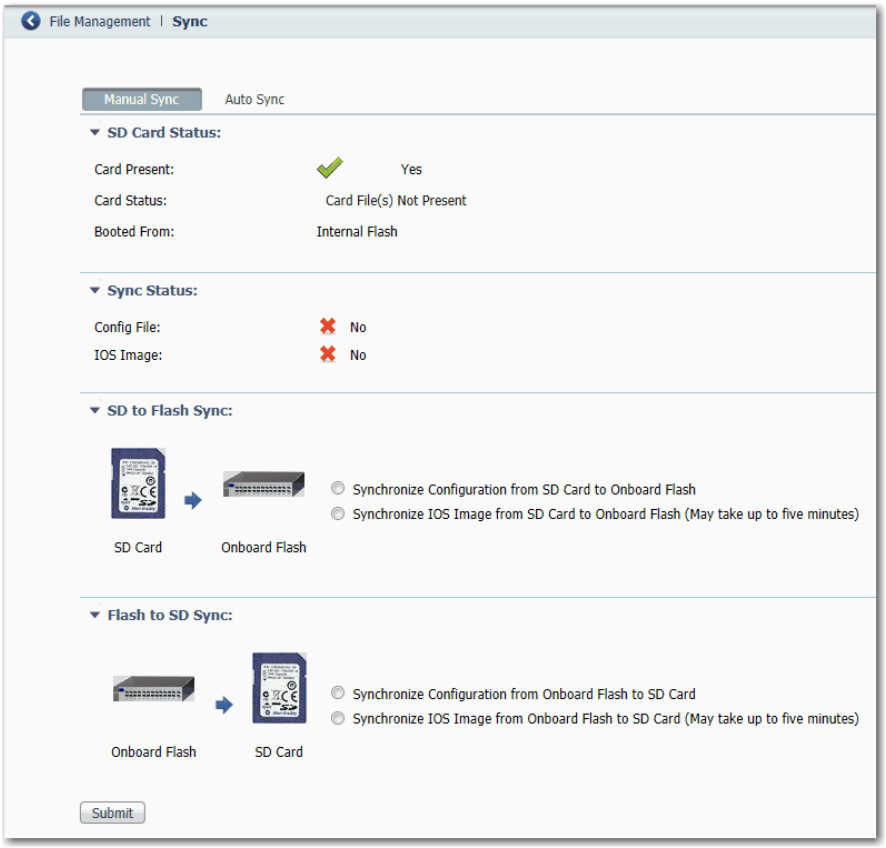


表 24 - 手动同步选项卡字段

字段	描述
SD Card Status	指示 SD 卡是否存在、卡的状态及其配置启动的位置。
SD to Flash Sync	从以下两个选项中选择： • Synchronize configuration from SD card to onboard flash • Synchronize IOS image from SD card to onboard flash
Flash to SD Sync	从以下两个选项中选择： • Synchronize configuration from onboard flash to SD card • Synchronize IOS image from onboard flash to SD card

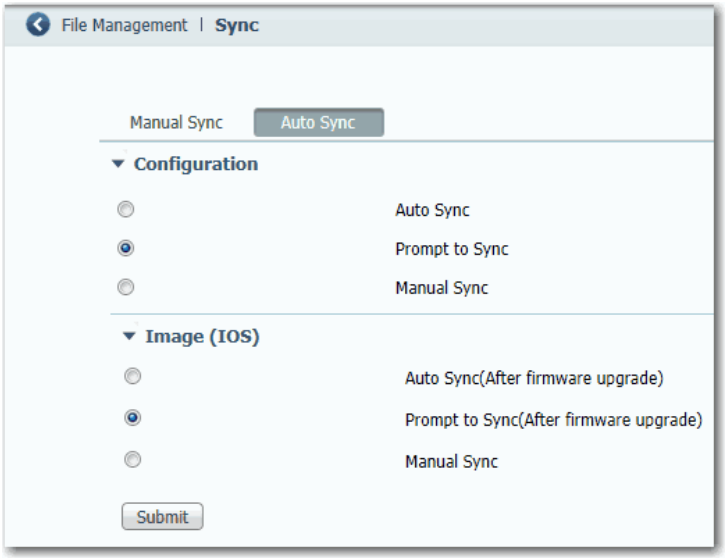


表 25 - 自动同步选项卡字段

字段	描述
Configuration	Auto Sync — 在更改设备管理器 Web 界面的配置时自动同步该配置。 此为默认配置。
	Prompt to Sync — 提交配置更改后，用户会收到一条消息，提示您确认该同步。
	Manual Sync — 除非用户执行手动同步，否则不会对配置更改进行同步。
Image (IOS)	Auto Sync (After firmware upgrade) — 升级固件后，自动同步更改的配置。
	Prompt to Sync (After upgrade) — 升级固件后，用户会收到一条消息，提示您确认该配置。 此为默认配置。
	Manual Sync — 除非用户执行手动同步，否则升级固件后不会进行同步。

上传和下载配置文件

要从其它设备（如 PC）的文件中将配置文件复制到板载内存，可在交换机上输入文件夹的目录名称，浏览并选择该文件，然后单击 Upload。

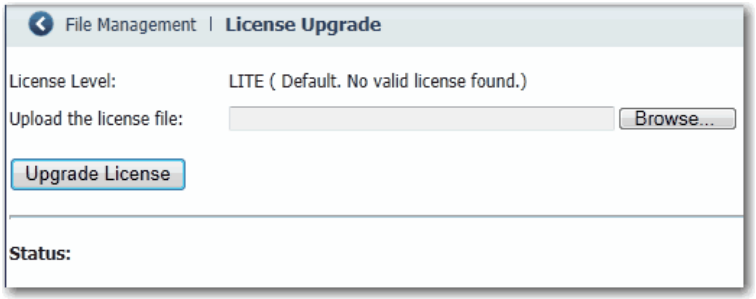
要从板载内存将配置文件下载到计算机，右键单击链接并选择 Save Link As。

升级许可证文件

获取许可证文件后，通过 License Upgrade 窗口将其安装到交换机上。

1. 单击 Browse，选择该许可证文件。
2. 单击 Upgrade License，启动升级过程。

   出现一条指示进度的消息。升级结束后，交换机将重启。



注：

第 5 章

通过 Studio 5000 环境管理交换机

完成“快速设置”后，可在 Studio 5000 环境下使用 Logix 设计器应用程序管理交换机。

EtherNet/IP CIP 接口

Stratix 5700 交换机包含一个 EtherNet/IP 网络接口。EtherNet/IP 网络协议是由开放式设备网络供应商协会 (ODVA) 维护的工业自动化网络技术规范。其应用层使用通用工业协议 (CIP)，其传输层和网络层使用 TCP/UDP/IP。可以使用交换机的 IP 地址通过交换机的任一以太网端口访问此接口。

CIP 网络连接

CIP 是面向对象的基于连接的协议，支持两种基本类型的报文通信：显式和隐式 (I/O) 连接。最多可以建立 32 个连接。两种连接类型在写入任何交换机参数前都必须使用交换机密码。该密码与“快速设置”期间输入的密码相同。

表 26 - CIP 网络连接

连接	描述
显式报文通信	显式报文通信连接在两个设备之间提供通用的多用途通信路径。这些连接通常称为报文通信连接。显式报文提供面向请求 / 响应的网络通信。各个请求通常针对不同的数据项。显式报文可用于对交换机进行配置、监视和故障处理。 显示报文通信接口供 Logix 设计器应用程序使用。
I/O （隐式报文通信）	I/O 连接在生产应用与一个或多个消费应用之间提供专用的特殊用途通信路径。在这些连接之间流动的应用特定 I/O 数据通常是固定的循环结构。 交换机支持两种 I/O 连接。 • 仅输入 • 独占所有者 两种连接都是循环连接，并且周期可在 300...5000 ms 之间调整。 “ 仅输入 ” 连接包含的数据结构中含有交换机的常规信息和各个端口的具体状态。此连接是多播连接，可被多个控制器 （连接发起者）共享。 “ 独占所有者 ” 连接使用与 “ 仅输入 ” 连接相同的输入数据结构，但增加了输出数据结构。输出数据中对每个端口都提供了一个位，可用于单独启用或禁用各个端口。此连接的输入数据可被多个控制器共享（通过多播）时，只能有一个控制器拥有输出数据。如果再有控制器尝试打开此连接，连接将被拒绝。

重要信息　由于输出数据由控制器循环发送，因此它将使其它软件工具或可视化站启用或禁用端口的任何其它尝试无效。

RSLinx 软件和网络 Who 支持

EtherNet/IP 网络接口还支持 List Identity 命令，基于 CIP 的网络工具（如 RSLinx® 软件的 RSWho 功能）使用该命令。RSWho 允许您使用电子数据表 (EDS) 文件在网络上定位和标识交换机。

要执行 RSWho 功能，请从 RSLinx 软件工具栏中选择 Communications > RSWho。

重要信息　在使用了 RSWho 功能后，如果访问交换机并查看以太网链路计数器，则只能看到第一个端口 （端口 Gi1/1）的计数。

电子数据表 (EDS) 文件

电子数据表 (EDS) 文件是网络配置工具（如 RSNetWorx™ for EtherNet/IP 软件）使用的简单文本文件，帮助您标识产品并在网络上轻松调试。EDS 文件包含设备的可读取和可配置参数的详细信息。这些文件还提供有关设备支持的 I/O 连接的信息以及相关联数据结构的内容。

如果在没有罗克韦尔自动化 Logix 控制器的系统中使用交换机，不能通过该控制器监视或控制交换机，则将无法使用随 Logix 控制器提供的 AOP。必须使用 EDS 文件中的信息建立 I/O 连接。

向“主题”（交换机）添加项目（OPC 标签）时，RSLinx Classic 软件中包含的 OPC Server 也使用 EDS 文件提供参数列表。

Stratix 5700 交换机的 EDS 文件包括在以下软件包中：

- RSLinx 软件，版本 2.54 或更高版本
- RSLogix 5000 软件，版本 16 或更高版本； Logix 设计器应用程序，版本 21.00.00 或更高版本
- RSNetWorx for EtherNet/IP 软件，版本 9.0 或更高版本

还可以通过以下两种方式之一获取 EDS 文件：

- 从 http://www.rockwellautomation.com/resources/eds/ 处获取。

  提示 **要找到特定 EDS 文件，请执行以下操作：**
  - **从 Network type 字段中选择 EtherNet/IP。**
  - **在 Keyword 字段中输入 Stratix 5700。**
  - **其它字段保留默认输入。**

- 使用 “RSLinx EDS 硬件安装工具 ” 从交换机获取。

要通过网络直接从交换机上传 EDS 文件，请按照以下步骤操作。

1. 从 Start 菜单选择 Programs > Rockwell Software > RSLinx > Tools > EDS Hardware Installation Tool。
2. 单击 Add 启动 “EDS 向导 ”，然后添加所选硬件描述和关联文件。

可通过 CIP 访问的数据

通过 CIP 接口可访问以下信息：

- 通过 I/O 连接的输入数据
  - 各端口的链路状态：未连接，已连接
  - 各端口的未授权设备：正常，不正常
  - 各端口是否超过单播阈值：正常，超过
  - 各端口是否超过多播阈值：正常，超过
  - 各端口是否超过广播阈值：正常，超过

  - 各端口的端口带宽利用率：以 % 表示的值
  - 主报警继电器：正常，脱扣
  - 活动多播组：数量

- 通过 I/O 连接的输出数据

  - 各端口的端口禁用情况：启用，禁用

- 其它状态数据

  - 交换机内部温度：摄氏度
  - 电源 A 是否通电：是，否
  - 电源 B 是否通电：是，否
  - 标识信息：供应商 ID、设备类型、产品代码、产品名称、版本、序列号
  - IOS 发布版本
  - 交换机正常运行时间 （自上次重新启动以来）
  - 管理 CPU 利用率：以百分比表示
  - CIP 连接计数器：打开 / 关闭请求次数、打开 / 关闭拒绝次数、超时次数
  - 各端口的端口报警状态：正常、不转发、不运行、 FCS 错误过多
  - 各端口的端口故障状态：错误禁用、SFP 错误、本机 VLAN 不匹配、MAC 地址翻动情况、安全侵犯
  - 各端口的端口诊断计数器：以太网接口计数器（10），以太网介质计数器 (12)

- 配置数据 （需要密码）

  - IP 编址方法：DHCP，静态
  - IP 地址、子网掩码、默认网关 （如果选择静态，则包括全部）
  - 主机名称
  - 联系人姓名
  - 地理位置
  - 各端口的端口配置：启用 / 禁用、自动协商、强制速度 / 双工
  - 各端口的认证 MAC ID
  - 各端口的单播速率限制阈值：以每秒数据包数、每秒位数或百分比表示
  - 多播速率限制阈值：以每秒数据包数、每秒位数或百分比表示
  - 广播速率限制阈值：以每秒数据包数、每秒位数或百分比表示

- 各端口的智能端口分配：角色和 VLAN

- 保存和恢复交换机配置 （通过文件对象）

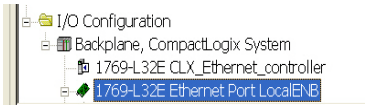
向 I/O 配置树添加交换机

要将交换机添加到控制器的 I/O 树，按以下步骤操作。

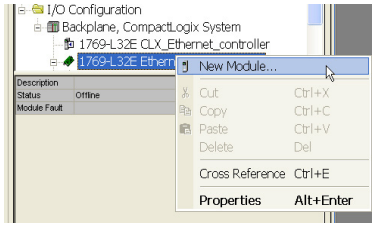
重要信息　必须先完成以下步骤，然后才能在线配置和监视交换机。

1. 打开项目文件，找到用于监视交换机的控制器。
2. 选择控制器与交换机通信所使用的以太网模块。

   在本例中，交换机通过 1769-L32E CompactLogix EtherNet/IP 控制器进行通信。



3. 右键单击所创建的以太网端口，然后选择 New Module。

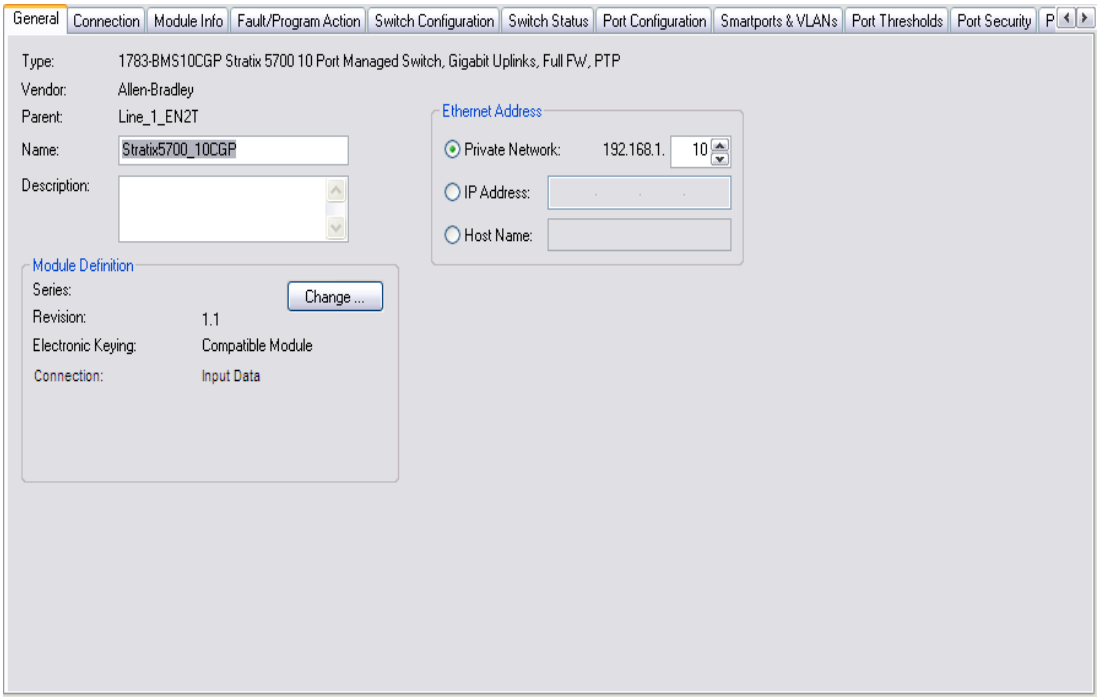


4. 单击 Communications。
5. 单击 + 号并向下滚动，直到看见想要配置的交换机。

   如果在列表中未看到所需交换机，可从罗克韦尔自动化支持网站获得 AOP。

   a. 转到 http://www.rockwellautomation.com/support/。
   b. 单击 Downloads/RSLogix 5000 I/O Modules Add-on Profiles。
   c. 选择 1783-Stratix 5700 Managed Switches Add-on Profile。
6. 单击 OK 显示 Module Properties 对话框。

配置常规属性

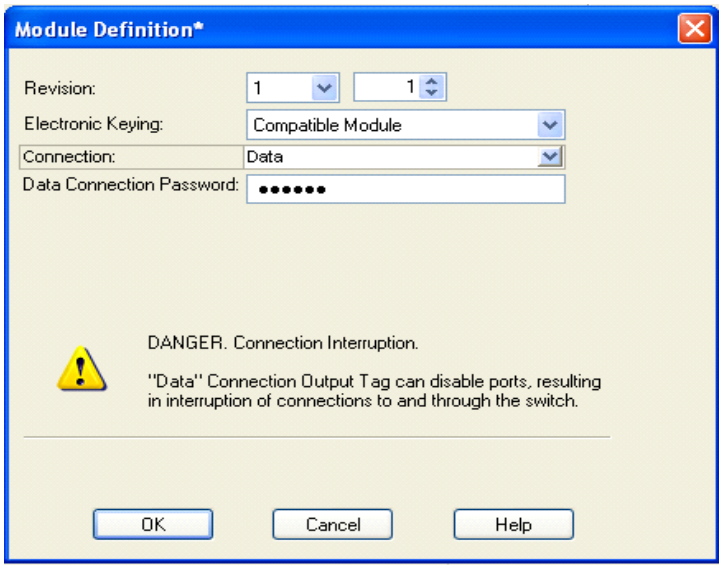


要配置常规属性，请按以下步骤操作。

1. 在 Module Properties 对话框中填写下述字段。

字段	描述
Name	所选交换机的名称。
Description	可帮助您记住有关交换机的重要信息的说明。
Ethernet Address	在以下各项中选择一项： • Private Network — 交换机所属的专用网络。 • IP Address — 执行 " 快速设置 " 时输入的 IP 地址。控制器使用此 IP 地址进行通信。 • Host Name — 执行 " 快速设置 " 时在初始配置中提供的主机名称。选择主机名称时，您必须已在网络中为控制器的以太网接口模块配置了 DNS 服务器。 **重要信息：**请确保 IP 地址和主机名称与执行 " 快速设置 " 时提供的信息相同。

2. 单击 OK。
3. 选择 Communications > Go online 使交换机转到在线状态。
4. 双击交换机以查看 Module Properties 对话框。
5. 单击 Change。
6. 填写 Module Definition 对话框中的字段。



字段	Description
Revision	交换机的主版本和次版本： • 主版本：介于 1...128 之间的数字 • 次版本：介于 1...255 之间的数字
Electronic Keying	• Compatible Module（默认） • Exact Match • Disable Keying
Connection	• Input Data（默认）仅启用输入数据连接 • Data：启用输入和输出数据连接 **注意：**此选择将启用输出标签，这会禁用端口并中断与交换机的连接以及通过交换机的连接。您可以禁用交换机端口，在输出标签中设置相应位即可。当控制器处于运行模式时，交换机每次从控制器接收到输出数据都会应用输出位。当控制器处于程序模式时，不会应用输出位。 如果相应的输出位为 0，则会启用端口。如果使用设备管理器 Web 界面或 CLI 来启用或禁用端口，则在下次循环更新 I/O 连接时，端口设置可能被控制器的输出位覆盖。无论是使用设备管理器 Web 界面还是使用 CLI 来启用或禁用端口，这些输出位始终优先。
Data Connection Password	输入访问交换机的密码。仅数据连接需要。

连接属性

可在 Connection 选项卡上对交换机的连接属性进行定义。

表 27 - Connection 选项卡字段

字段	描述
Requested Packet Interval (RPI)	输入一个介于 300…5000 之间的值。
Inhibit Module	选中则禁用控制器和交换机之间的通信。取消选中该复选框即恢复通信。
Major Fault on Controller If Connection Fails While in Run mode	选中时，如果在运行模式下连接失败，则控制器创建主要故障。
Use Unicast Connections over EtherNet/IP	选中则通过 EtherNet/IP 网络使用单播连接。
Module Fault	显示从控制器返回的故障代码（与正在配置的交换机相关），以及详细说明发生的模块故障的文本。

模块信息

可从 Module Info 选项卡中监视和重置交换机。

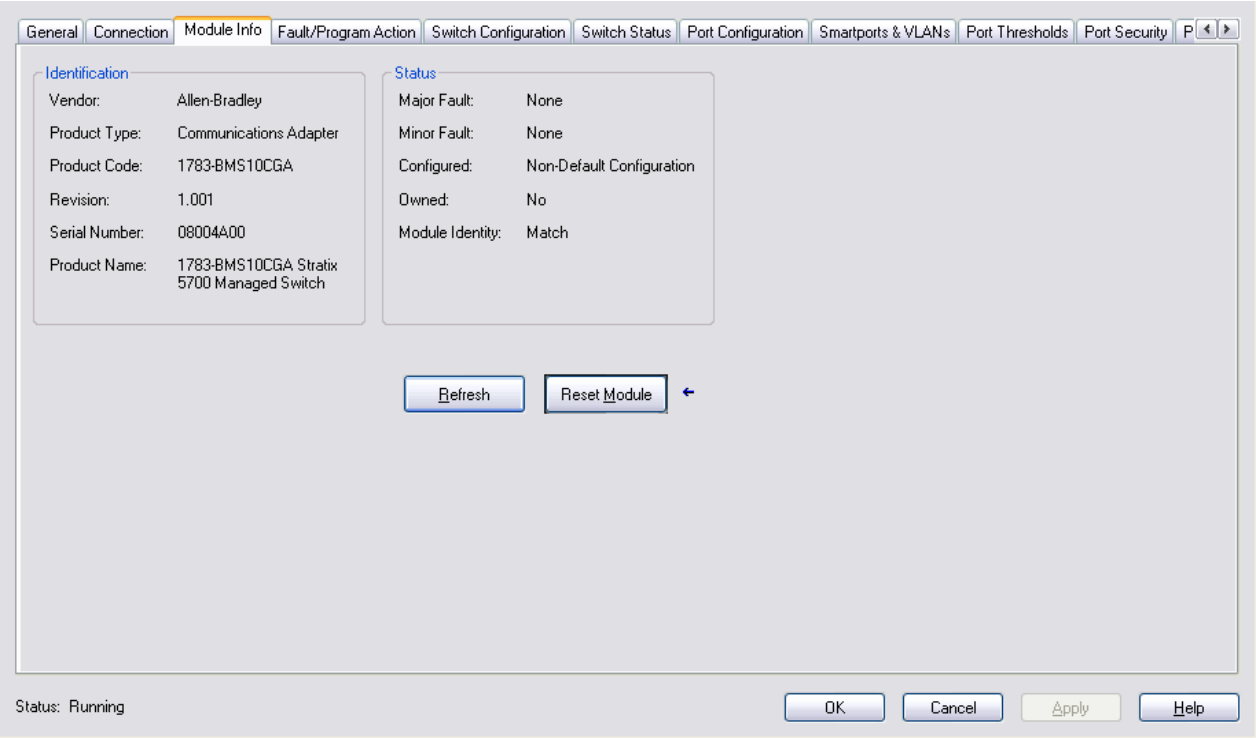


表 28 - Module Info 选项卡字段

字段	描述
Identification	显示交换机的以下信息： • Vendor • Product type • Product code • Revision • Serial number • Product name
Status	显示以下状态： • Major Fault 和 Minor Fault 状态： – None – Recoverable – Non-recoverable • Configuration： – Non-default configuration – Default configuration • Owned。指示是否存在 I/O 连接： – Yes – No • Module identity： – Match。与 General 选项卡上指定的内容一致。Match 的条件是供应商、产品类型、产品代码和主板本必须一致。 – Mismatch。与 General 选项卡上指定的内容不一致。 Module Identify 字段不考虑 General 选项卡上指定的交换机 Electronic Keying 或 Minor Revision 选项。
Refresh	单击以用模块的新数据刷新选项卡。
Reset Module	单击则使用当前配置文件执行交换机重置（循环上电）。将出现 Password Confirmation 对话框。 **注意：**重置模块将导致所有与模块建立的连接或通过模块的连接断开。这种情况可能会导致失控。

交换机配置属性

可在 Switch Configuration 选项卡上对 IP 设置和管理参数进行配置。必须在线执行这些配置。在离线模式下，此选项卡不会显示任何内容。

IP 地址可以手动分配（静态），也可以由动态主机配置协议 (DHCP) 服务器自动分配。默认设置为 Static。建议选择 Static 并为交换机手动分配 IP 地址。此后，如需访问交换机，则可随时使用该 IP 地址。

- Static — 手动输入 IP 地址、子网掩码和网关。
- DHCP — 交换机自动从 DHCP 服务器获取 IP 地址、默认网关和子网掩码。只要交换机未重新启动，就会继续使用分配的 IP 信息。

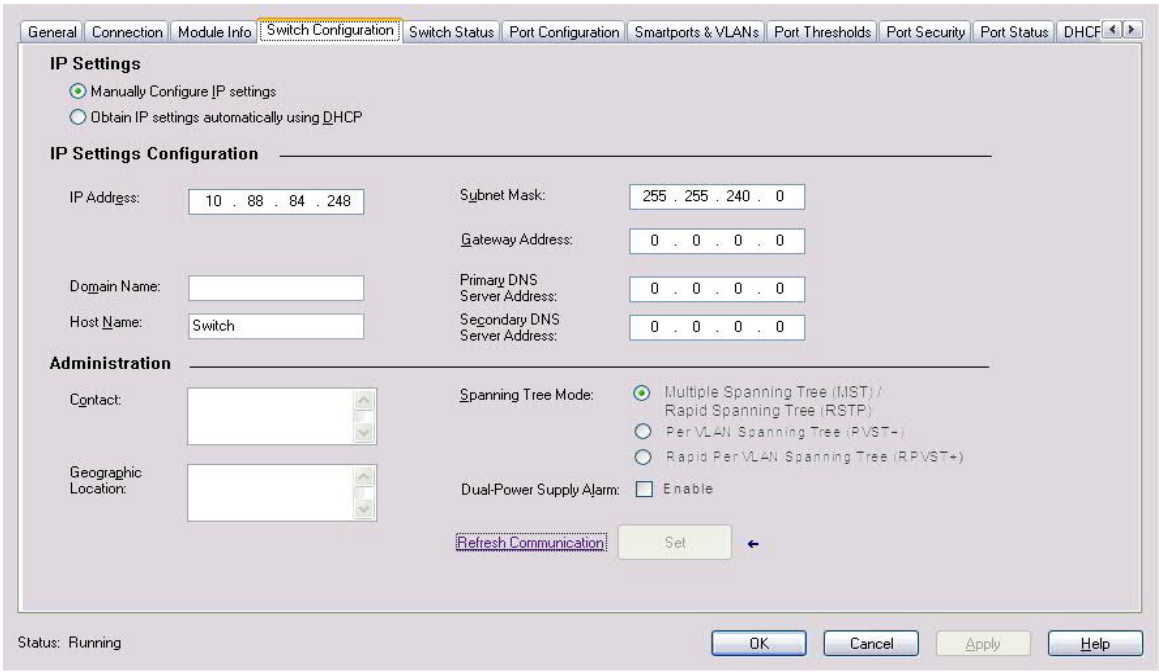


表 29 - Switch Configuration 选项卡字段

字段	描述
IP Address	该值必须与 General 选项卡上的 IP 地址匹配。 如果为交换机重新配置的是不同的 IP 地址，则单击 Set 后将失去与交换机的通信。要更正此问题，必须返回到 " 快速设置 " 和 General 选项卡，设置新的 IP 地址，然后下载到控制器。
Subnet Mask	为交换机输入相应的子网掩码。子网掩码是一个 32 位数字。将每个 8 位字节设置在 0 和 255 之间。默认值为 255.255.255.0。
Gateway Address	网关是交换机与其它网络或子网络上的设备进行通信所使用的路由器或其它网络设备。 网关 IP 地址应同交换机 IP 地址在同一子网中。交换机 IP 地址和默认网关 IP 地址不可相同。 **重要信息:** 更改网关 (IP) 地址后通信将中断。
Primary DNS Server Address	输入主域名服务器 (DNS) 的 IP 地址。将每个 8 位字节设置在 0 和 255 之间。第一个 8 位字节不能为 127 或大于 223 的数字。
Secondary DNS Server Address	输入次域名服务器 (DNS) 的 IP 地址。将每个 8 位字节设置在 0 和 255 之间。第一个 8 位字节不能为 127 或大于 223 的数字。
Domain Name	输入模块所属的域名。域名由一连串由句点分隔的名称标签组成，如 example.com。域名具有 48 个字符的长度限制，并且只能使用 ASCII 字母 a 到 z、数字 0 到 9 以及句点和连字符。
Host Name	（可选）。输入在监视或处理故障问题时用于标识交换机的名称。该名称最多允许 64 个字符，可包括字母数字和特殊字符（逗号和破折号）。
Contact	（可选）。输入交换机的联系人信息，最多 200 个字符。联系人信息可包括字母数字和特殊字符（破折号和逗号）以及回车。
Geographic Location	（可选）。输入交换机的地理位置，最多 200 个字符。地理位置可包括字母数字和特殊字符（破折号和逗点）以及回车。
Spanning Tree Mode	在以下各项中选择一项: • RSTP/MST • PVST+ • RPVST+ 默认值为 RSTP/MST。
Dual-Power Supply Alarm	选中此复选框即启用该功能。默认情况下该功能处于禁用状态。
Refresh	单击即刷新选项卡，以显示新的交换机数据。
Set	单击即可将设置保存到交换机和 SD 卡（如果已安装）。正确输入密码后的 10 分钟内可进行更改，并且不会出现 Enter Password 对话框提示您输入密码。

交换机状态

可在 Switch Status 选项卡中查看交换机的各状态参数。

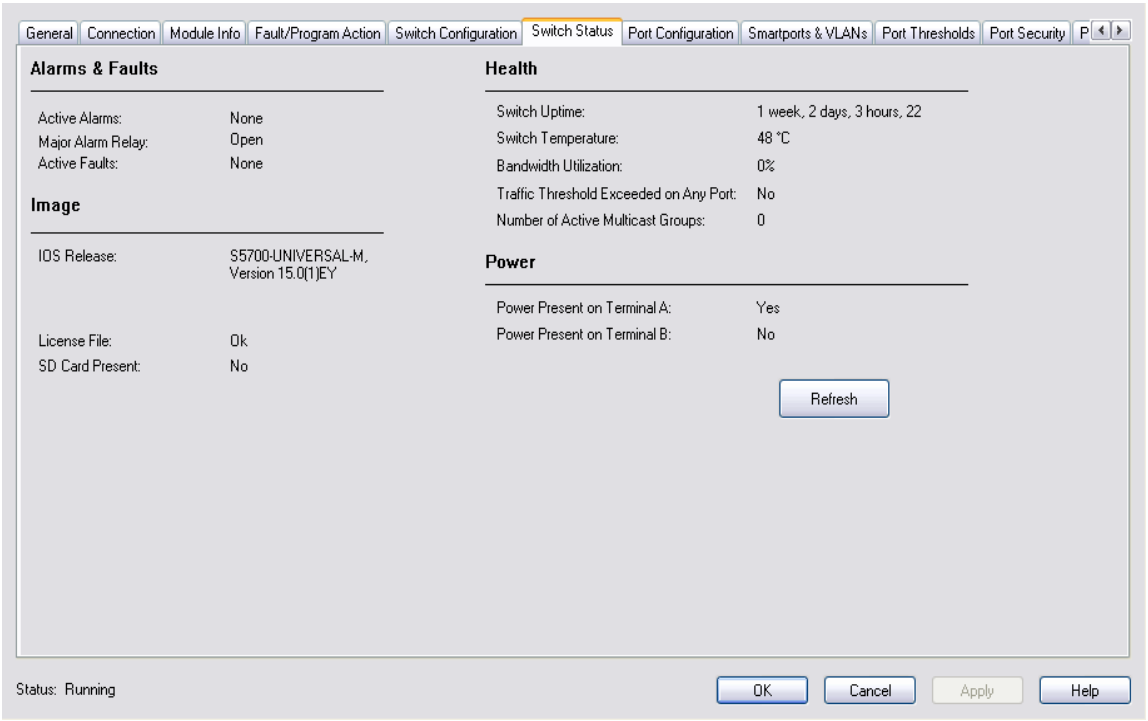


表 30 - Switch Status 选项卡字段

字段	描述
Active Alarms	显示这些值中的一个： • None • Port alarm • Dual Mode Power Supply alarm • Primary Temperature alarm
Major Alarm Relay	显示这些值中的一个： • Open • Closed
Active Faults	显示这些值中的一个： • None • Port fault • Hardware fault 如果端口和硬件故障均处于活动状态，则显示 Hardware fault 状态。
Traffic Threshold Exceeded on Any Port	显示 Yes 或 No 值，指示是否已超过任一端口的当前单播、多播和广播阈值。 要查看活动端口的状态，请单击 Port Status 选项卡。要查看阈值，请单击 Advanced - Port Threshold 选项卡。
Switch Uptime	显示交换机自上次重新启动以来已运行的天数、小时数和分钟数。
Switch Temperature	显示交换机的当前内部温度（以摄氏度表示）。
Bandwidth Utilization	显示交换机使用的带宽的所占总百分比。
Power Present on Terminal A	显示 Yes 或 No 值，指示端子 A 是否通电。
Power Present on Terminal B	显示 Yes 或 No 值，指示端子 B 是否通电。
Number of Active Multicast Groups	显示活动多播组的数量。
IOS Release	显示交换机操作系统的当前版本。

端口配置

端口配置设置决定交换机与连接的设备之间数据的接收和发送方式。

必须在线配置端口功能。如果离线，此选项卡上的大多数信息不会显示。

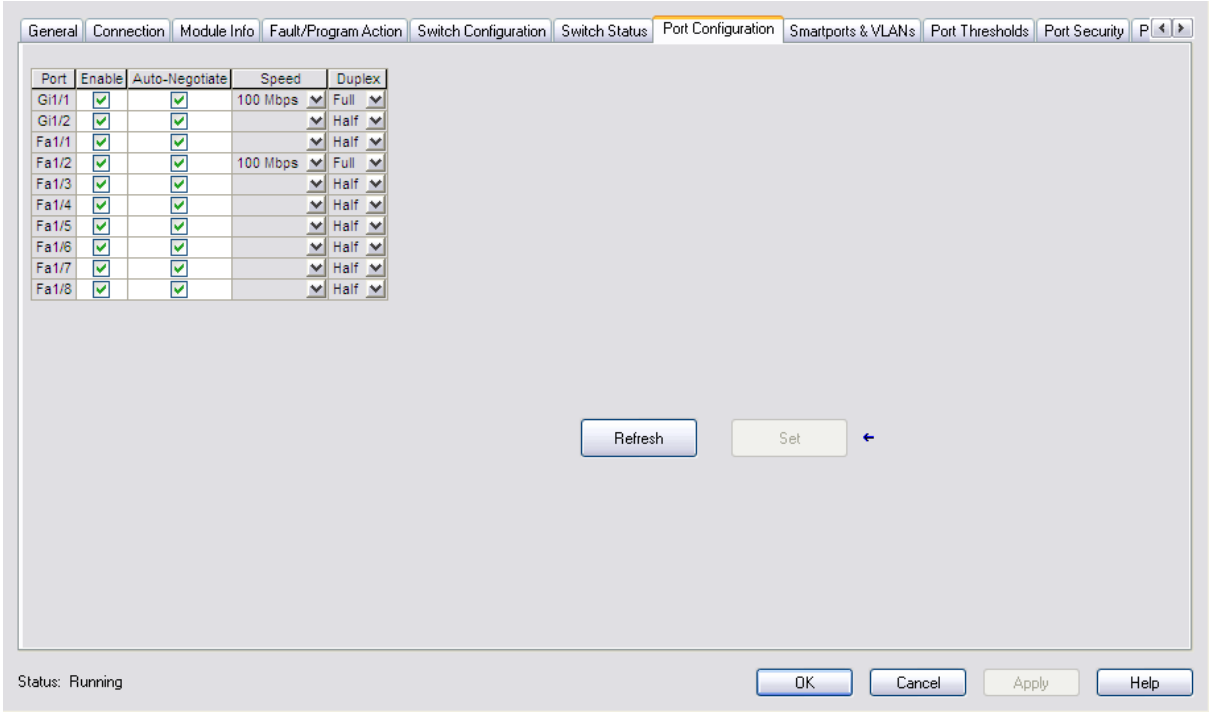


表 31 - Port Configuration 选项卡字段

字段	描述
Port	为配置选择的端口。端口号包括端口类型（Fa 表示高速以太网，Gi 表示千兆以太网）以及具体的端口号。 **示例：** Gi1/1 表示千兆以太网端口 1。
Enable	选中此复选框即启用该端口。 清除此复选框则手动禁用（关闭）端口。 如果端口未使用且未与任何设备相连，则建议禁用该端口。可以通过手动禁用端口来处理疑似未经授权连接的问题。
Auto-negotiate	如果想要端口和终端设备自动协商链接速度和双工模式，则选中此复选框。 取消选中此复选框后即可手动指定所需端口速度和双工模式。 建议使用默认设置（自动协商），这样交换机端口的速度和双工设置便会自动与相连设备的设置进行匹配。如果相连的设备需要特定的速度和双工，则可更改交换机端口速度和双工。如果设置交换机端口的速度和双工，相连设备也必须配置完全相同的速度和双工，且不能设置为自动协商，否则会出现速度 / 双工不匹配问题。 光纤接口不支持自动协商。
Speed	选择端口的工作速度。 千兆 (Gi)： • 10 Mbps • 100 Mbps • 1 Gbps 高速以太网 (Fa)： • 10 Mbps • 100 Mbps
Duplex	选择如下双工模式中一种： • Half-duplex — 两个设备不能同时发送数据。速度设置为 1 Gbps 时半双工不可用。 • Full-duplex — 两个设备可以同时发送数据。

智能端口和 VLAN

可在 Smartports & VLANs 选项卡中向交换机的端口分配智能端口角色和 VLAN。还可以创建、编辑和删除 VLAN。必须在线配置这些端口功能。如果离线，此选项卡上的大多数信息不会显示。

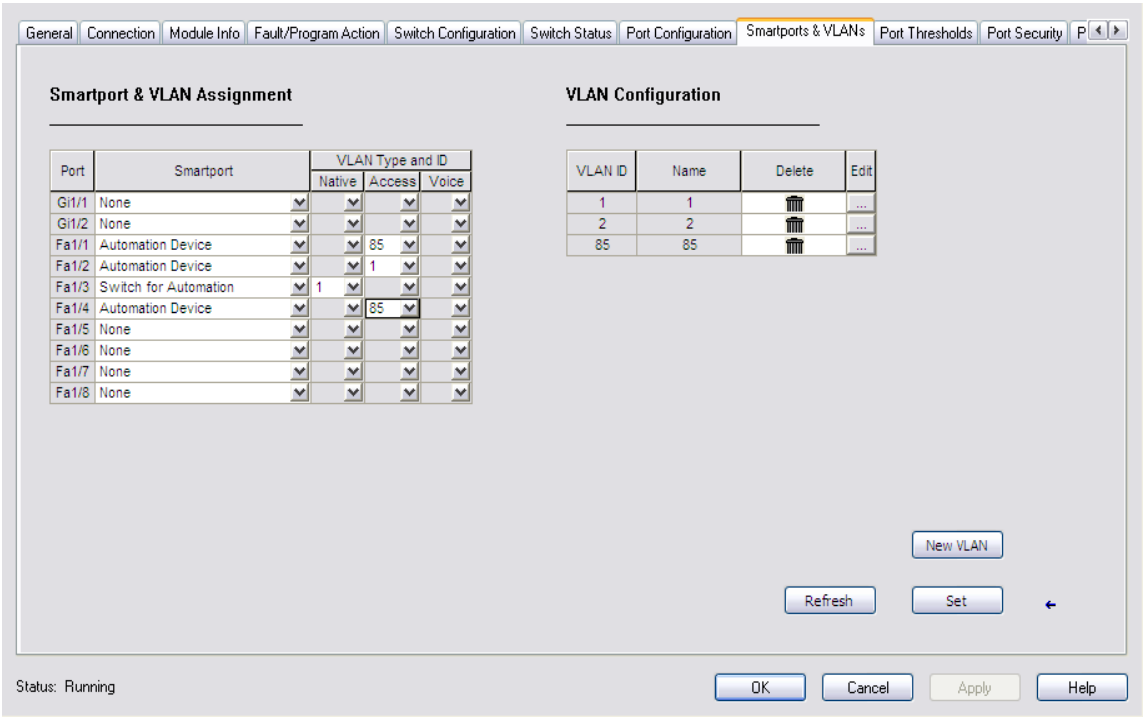


表 32 - Smartports and VLANs 选项卡字段

字段	描述
Port	为配置选择的端口。端口号包括端口类型（Fa 表示高速以太网，Gi 表示千兆以太网）以及具体的端口号。 **示例：** Gi1/1 表示千兆以太网端口 1。
Smartport	智能端口角色是建议使用的端口配置。这些配置称为端口角色。它们将优化交换机连接，并确保交换机端口通信的安全性、传输质量和可靠性。这些配置还可防止许多由端口配置错误产生的问题。 端口角色取决于连接到交换机端口的设备类型。先确保已决定哪个端口连接到哪种类型的设备，再选择智能端口角色。从这些智能端口角色中选择一个用于相连端口： • Automation Device — 此角色适用于与 EtherNet/IP 设备连接的端口。可将其用于工业自动化设备，如逻辑控制器和 I/O。 – 端口被设为访问模式。 – 只允许一个 MAC ID 以确保端口安全性。 – 优化 CIP 通信的队列管理。 • Desktop for Automation — 此角色适用于与桌面设备 （如桌面计算机、工作站、笔记本电脑及其它基于客户端的主机）连接的端口。此角色不适用于与交换机、路由器或接入点连接的端口。 – 端口被设为访问模式。 – 启用快速端口。 – 只允许一个 MAC ID 以确保端口安全性。 • Switch for Automation — 此角色适用于与其它交换机相连的端口。 – 端口被设为干线模式。 – 启用快速端口。 • Router for Automation — 此角色适用于与启用了路由服务的第三层交换机连接的路由器或端口。 • Phone for Automation — 此角色适用于与 IP 电话连接的端口。可以将桌面设备 （如计算机）与 IP 电话连接。 IP 电话与连接的计算机均通过此端口访问网络。此角色将语音通信的优先级排在常规数据通信之前，以确保 IP 电话接收到清晰的语音。 – 端口被设为干线模式。 – 端口安全性设置支持三个 MAC ID 使用此端口。 • Wireless For Automation — 此角色适用于与无线接入点连接的端口。接入点最多可以为 30 个移动（无线）用户提供网络接入。 • Port Mirroring — 此角色适用于受网络分析器监视的端口。有关端口镜像的详细信息，请参见第 82 页上的端口镜像。 • None — 如果不想在端口上应用专门的智能端口角色，则对端口应用此角色。此角色可用于与任何设备的连接，包括上述角色中的设备。 • Custom— 针对应用创建角色。可设置所采用 VLAN（如果有）的类型。 – 输入宏的名称。宏名称区分大小写。该字符串最多包含 31 个字母数字字符。字符串不可包含问号、空格或制表符。 – 选择宏图标（CS1 到 CS10）。
VLAN Configuration	显示 VLAN ID 和名称： • VLAN ID — 通过单击 Add New VLAN 所创建的 VLAN 的唯一标识符（范围 2…4094； 1002…1005 保留）。默认值为 VLAN ID 1。 • Name — 通过单击 Add New VLAN 所创建的 VLAN 的唯一名称（最多 20 个字符）。

端口阈值

可在 Port Thresholds 选项卡上为每个活动端口的广播、单播和多播通信配置阈值限制。仅完整版固件具有此功能。将正在发送的数据包数目与阈值进行比较。这些限制有助于防止单个设备发送过多的通信。有关此功能的详细信息，请参见第 67 页上的端口阈值。

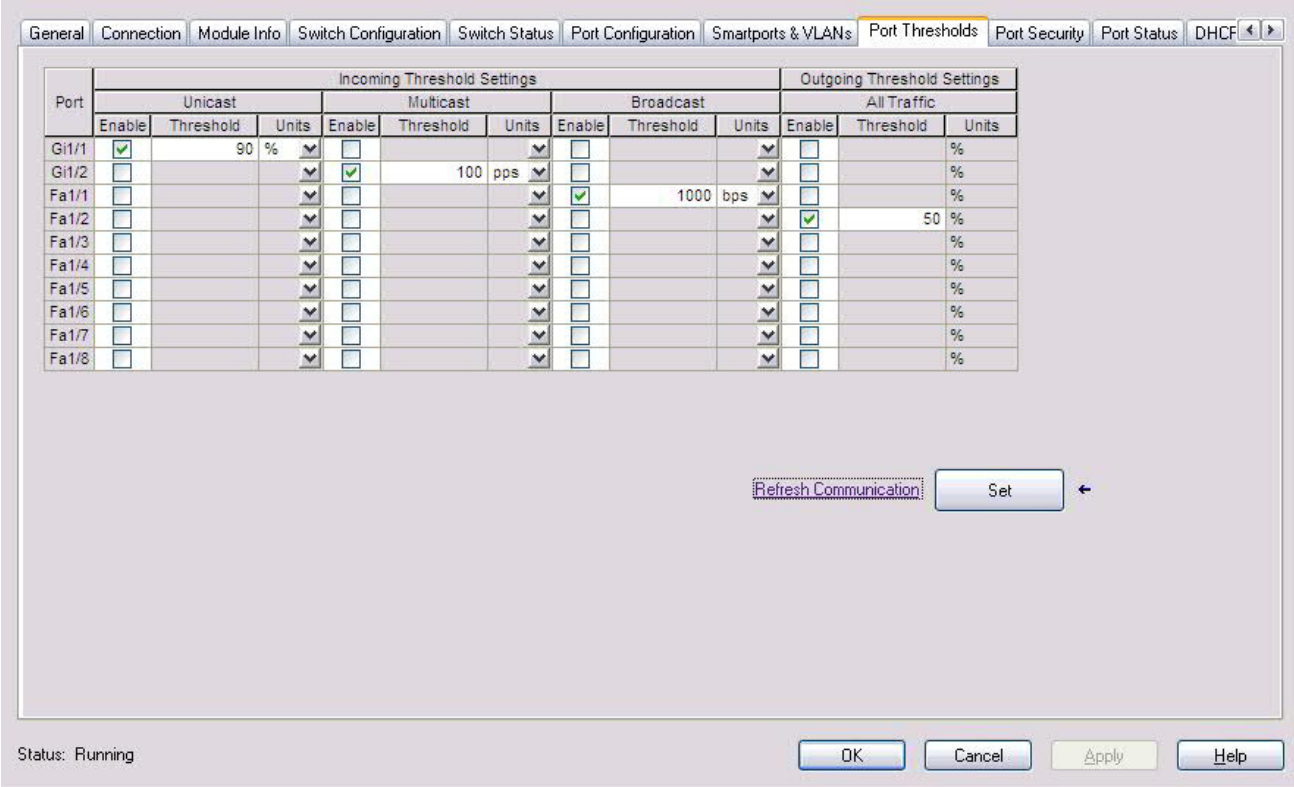


表 33 - Port Threshold 选项卡字段

字段	描述
Port	为配置选择的端口。端口号包括端口类型（Fa 表示高速以太网，Gi 表示千兆以太网）以及具体的端口号。 **示例：** Gi1/1 表示千兆以太网端口 1。
Incoming Threshold Settings	启用传入阈值并设置每个端口的单播、多播和广播通信的阈值。 各单元有效值： • 每秒数据包数 (pps) • 带宽所占的总百分比 (%) • 每秒位数 (pps)
Outgoing Threshold Settings	启用传出阈值并设置每个端口通信的阈值。 单元 % = 带宽所占的总百分比

端口安全性

端口安全性功能仅适用于完整版固件。有关详细信息，请参见第 69 页上的端口安全性。

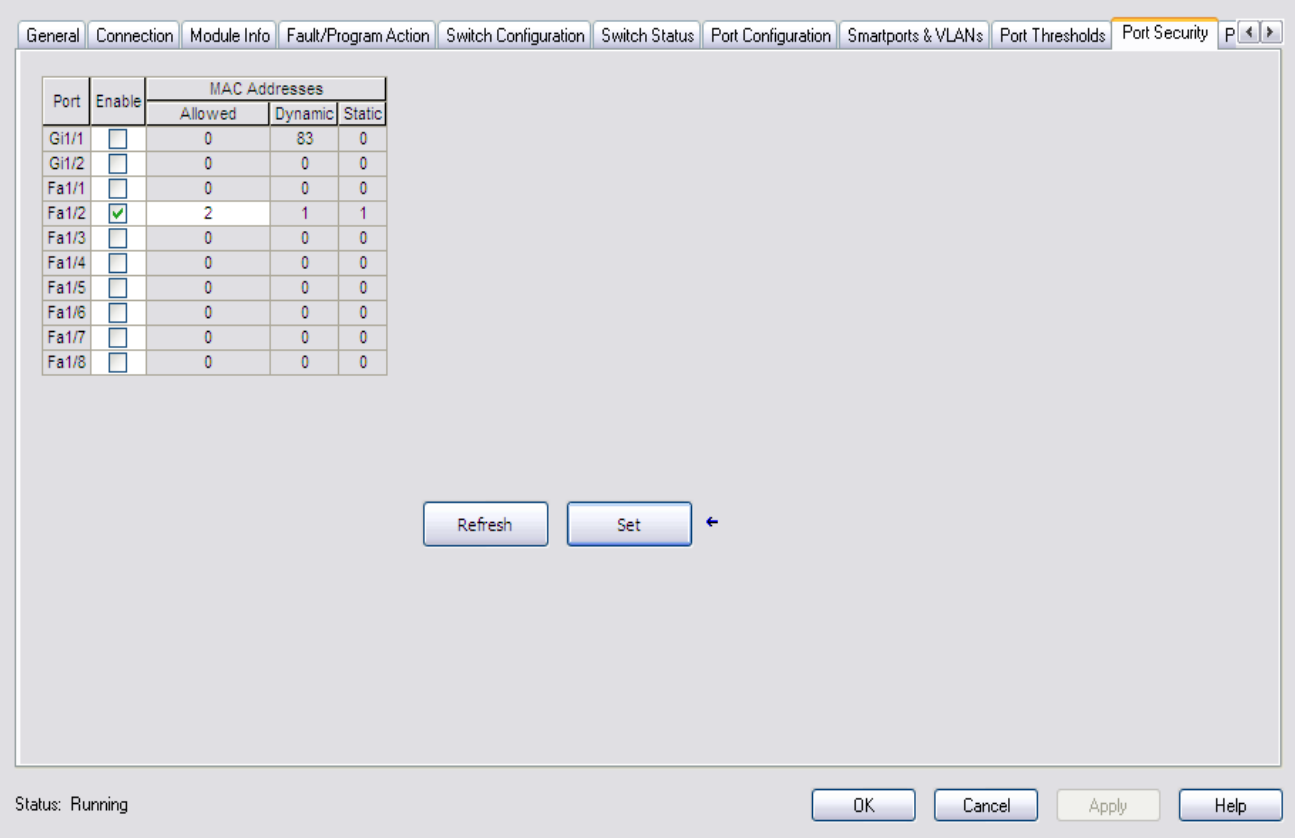


表 34 - Port Security 选项卡字段

字段	描述
Port	要启用或禁用安全功能的端口。
Enable	选中此复选框即启用端口安全功能。
MAC Addresses	支持的动态或静态 MAC 地址数。 • 允许 — 1…80 个。 • 动态 — 当前与端口相连的 MAC 地址（设备）数，非手动（静态）定义。 • 静态 — 通过 Device Manager Web 界面静态定义的 MAC 地址（设备）数。 请注意，此数量必须大于给定端口的静态和动态 MAC 地址数的总和。如果要减少此地址数量，可断开适当数量的设备连接并使其进入端口安全表超时。

端口状态

可在 Port Status 选项卡中监视报警、状态、阈值和带宽利用率。还可以查看端口和电缆诊断。

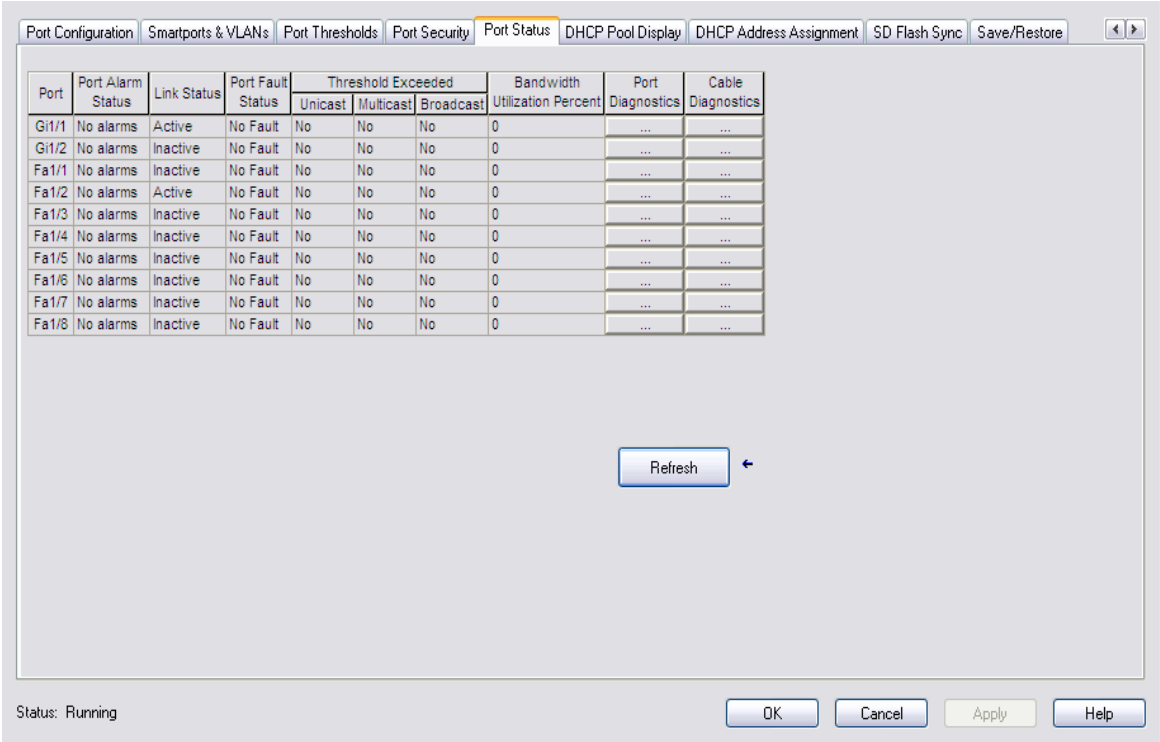


表 35 - Port Status 选项卡字段

字段	描述
Port	显示所选端口。端口号包括端口类型（Fa 表示高速以太网，Gi 表示千兆以太网）以及具体的端口号。 **示例：** Gi1/1 表示千兆以太网端口 1。
Port Alarm Status	显示端口报警的当前状态。 有效值： • Link fault alarm • Port not forwarding alarm • Port not operating alarm • High bit error rate alarm • No alarms
Link Status	显示链接是处于活动状态还是非活动状态。
Port Fault Status	显示端口报警的当前状态。 有效值： • Error - Disable event • SFP error - Disabled • CDP native VLAN mismatch • MAC address flap • Port security violation • No fault
Threshold Exceeded	显示以下类型网络通信中的不寻常变更： • Unicast — 显示值 yes 或 no 以显示当前单播通信是否超过阈值。 • Multicast — 显示值 yes 或 no 以指示当前多播通信是否超过阈值。 • Broadcast — 显示值 yes 或 no 以指示当前多播通信是否超过阈值。
Bandwidth Utilization Percent	显示所用带宽的百分比。请注意利用率百分比是否为给定时间网络活动的预期值。如果使用百分比高于预期值，则可能存在问题。
Port Diagnostics	单击即显示相应端口的 Port Diagnostics 对话框。Port Diagnostics 对话框提供用于诊断网络性能问题的信息。
Cable Diagnostics	单击即显示相应端口的 Cable Diagnostics 对话框。Cable Diagnostics 对话框提供用于诊断电缆问题的信息。

Port Diagnostics

使用 Port Diagnostics 对话框可查看链路性能的状态。

- 查看 8 位字节和数据包计数器
- 查看链路上的冲突
- 查看链路上的错误
- 重置和清除所有状态计数器

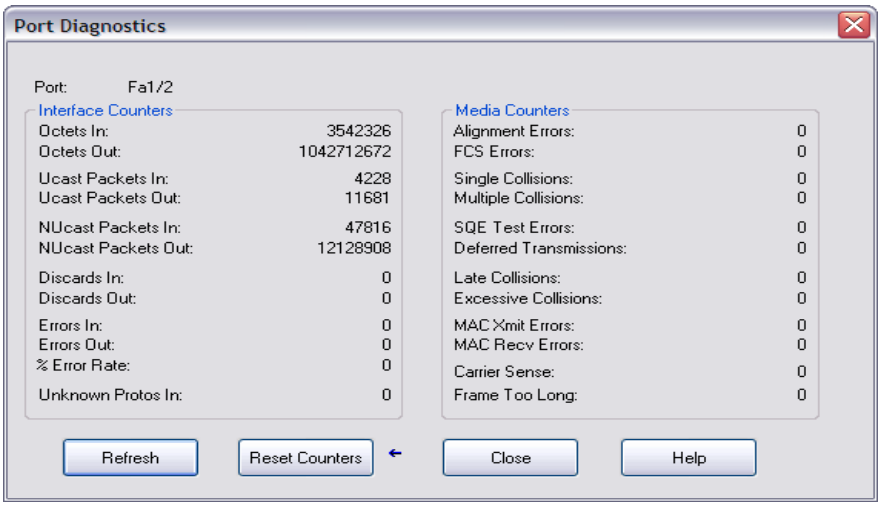
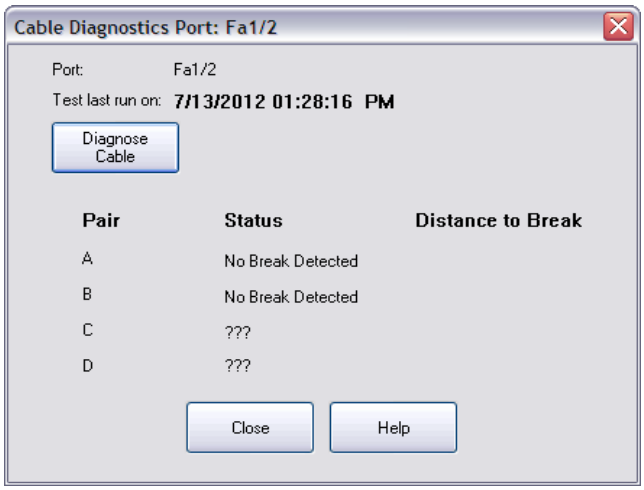


表 36 - Port Diagnostics 对话框字段

字段	描述
Port	为配置选择的端口。端口号包括端口类型（Fa 表示高速以太网，Gi 表示千兆以太网）以及具体的端口号。 **示例：** Gi1/1 表示千兆以太网端口 1。
Interface Counters	这些计数器可用于查看收到和发送的 8 位字节的状态，以及收到和发送的数据包的状态： • Octets In — 端口收到的 8 位字节数。 • Octets Out — 端口发送的 8 位字节数。 • Ucast Packets In — 端口收到的单播数据包数。 • Ucast Packets Out — 端口发送的单播数据包数。 • NUcast packets In — 端口收到的多播数据包数。 • NUcast packets Out — 端口发送的多播数据包数。 • Discards In — 丢弃的入站数据包数。 • Discards Out — 丢弃的出站数据包数。 • Errors In — 包含错误的入站数据包数。 • Errors Out — 包含错误的出站数据包数。 • Unknown Protos (Protocols) In — 包含未知协议的入站数据包数。
Media Counters	这些计数器可用于查看链路上的冲突数： • Single — 单一冲突数。 • Multiple — 多个冲突数。 • Late — 后期冲突数。 • Excessive — 由于过量冲突而传输失败的帧数。 • 以下计数器可用来查看错误数： • Alignment — 收到的不是 8 位字节长度的整数倍的帧数。 • FCS (Frame Check Sequence) — 收到的未通过 FCS 检查的帧数。 • SQE Test Errors — 生成 SQE TEST ERROR 消息的次数。 • Deferred Transmissions— 由于网络忙而延迟的传输计数。 • MAC Xmit Errors — 由于内部 MAC 子层发送错误而导致发送失败的帧数。 • MAC Recv Errors — 由于内部 MAC 子层接收错误而导致接收失败的帧数。 • Carrier Sense — 尝试发送帧时丢失或从未声明载波监听条件的次数。 • Frame Too Long — 收到的超过最大允许帧大小的帧数。

电缆诊断

Cable Diagnostics 对话框提供用于诊断电缆问题的信息。



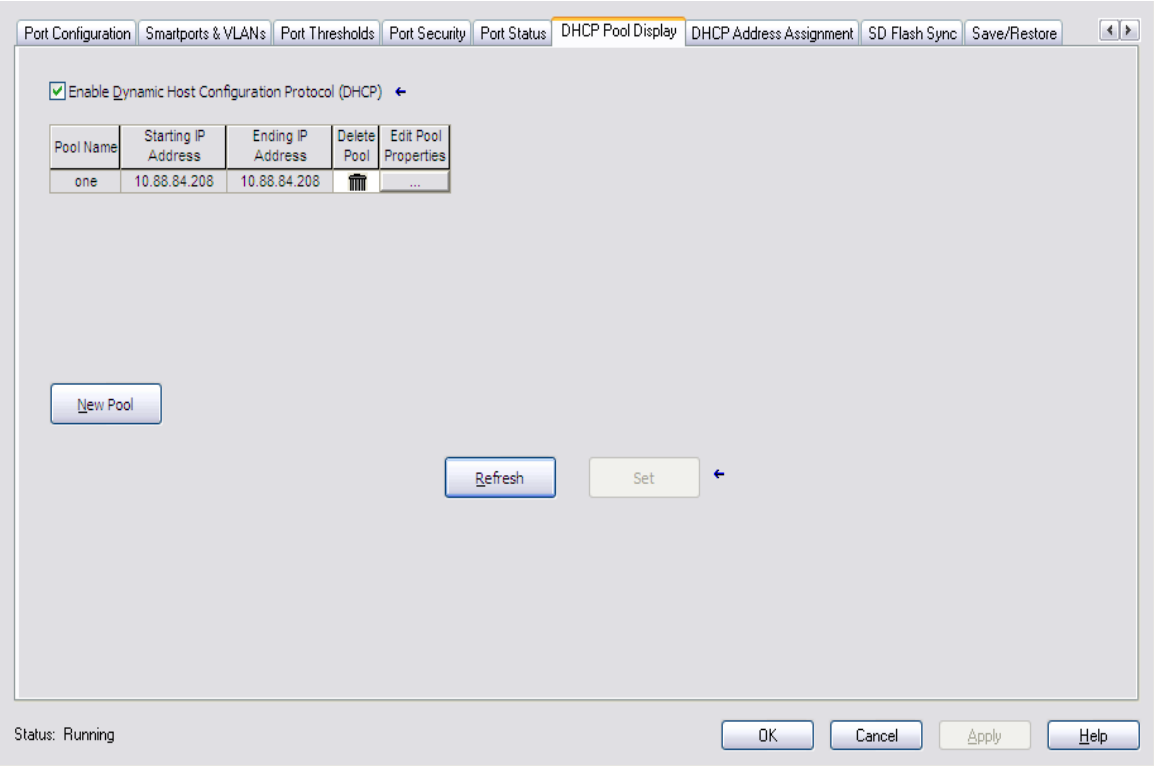
提示 如果离线，此选项卡上的信息将不会显示。

表 37 - Cable Diagnostics Port 对话框字段

字段	描述
Port	为配置选择的端口。端口号包括端口类型（Fa 表示高速以太网，Gi 表示千兆以太网）以及具体的端口号。 **示例：** Gi1/1 表示千兆以太网端口 1。
Test last run on	最后一次执行测试的时间。日期时间格式为 mm/dd/yy hh:mm:ss tt。如果从未进行过测试，则时间以及所有的距离和状态信息都将为空。
Pair	单独列出的各条双绞线（网络中成对的电缆）。如果不存在双绞线或从未运行过测试，则该项为空。
Status	指示最后一次执行测试时的链路状态。如果不存在双绞线或测试没有运行，则该项为空。至于距离，如果双绞线处于正常状态，则显示 “No Break Detected”。不显示任何距离。
Distance to Break	对于各预计的双绞线，从交换机到断开处的距离，并将单独列出正负误差值。仅现有双绞线状态为不正常时才显示值。如果从未运行过测试，则该字段为空。如果不存在双绞线，则出现 “???”。
Diagnose Cable	单击以运行 Diagnose Cable 测试。将出现连接中断警告： • 如果确定要继续进行测试，则单击 Yes。准备好输入有效密码以运行测试。 • 如果不想运行测试，则单击 No 或将窗口关闭。 **重要信息：** 要在千兆端口端口上运行有效测试，首先必须在 Device Manager Web 界面将千兆端口配置为 RJ45 介质类型，如第 96 页上的配置端口设置所述。 **重要信息：** 该测试可能会中断与模块的连接，以及所有通过该模块进行的与其它模块的连接。同样，工作站与控制器之间的连接也会中断。要运行此测试必须拥有恰当的权限。

DHCP 池显示

可在 DHCP Pool Display 选项卡中查看交换机的 DHCP 地址池信息。可查看 0...15 个池。此信息直接收集自交换机。每行代表一个实例，且实例值不连续。



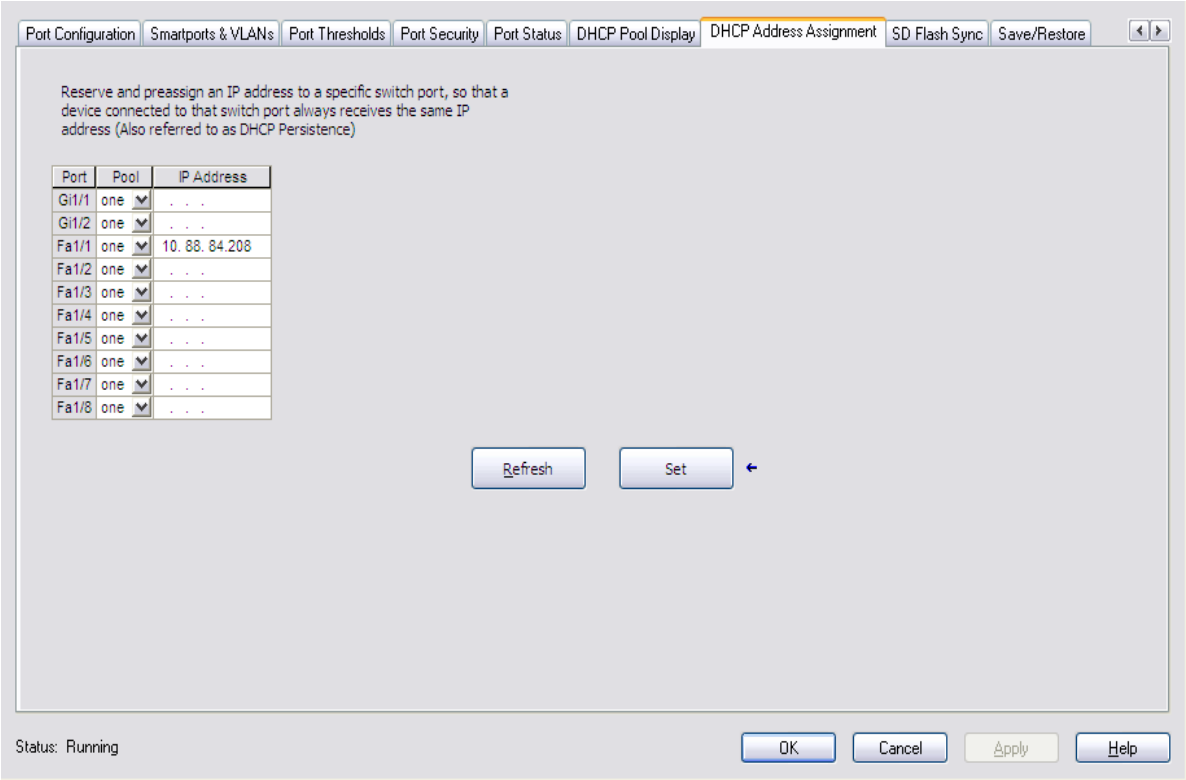
提示　　如果离线，此选项卡上的信息将不会显示。

表 38 - DHCP Pool Dislay 选项卡字段

字段	描述
Enable Dynamic Host Configuration Protocol (DHCP)	启用或禁用池。如果选中，则网格的所有控件都将设为在线，并且将从交换机处获取相应值并进行显示。如果取消选中，则网格的所有控件都将设为离线。键盘操作：按 Alt-D。
Pool Name	显示在交换机上配置的 DHCP IP 地址池名称。DHCP IP 地址池是交换机可为已连接设备分配的可用 IP 地址范围（或地址池）。名称最多包含 31 个字母数字字符。名称中不可包含问号或制表符。
Starting IP Address	显示用于定义 DHCP IP 地址池中地址范围的起始 IP 地址。格式是 32-位数字地址，共四组数字，之间用句点分隔（如 255.255.255.255）。每组数字的范围都是 0...255。
Ending IP Address	显示用于定义 DHCP IP 地址池中地址范围的结束 IP 地址。格式是 32 位数字地址，共四组数字，之间用句点分隔（如 255.255.255.255）。每组数字的范围都是 0...255。
Delete Pool	单击即删除当前选择的 DHCP 池行。之后，单击 Set 时将出现确认对话框，然后所有与所选 DHCP 池行相关的持久性地址也将被删除。 Delete Pool 可用条件：交换机在线、Enable Dynamic Host Configuration Protocol (DHCP) 复选框已选中并且相应行已填充。 Delete Pool 在以下情况下灰显：交换机离线、Enable Dynamic Host Configuration Protocol (DHCP) 复选框已取消选中。
Refresh	单击即刷新网格控件以显示直接从交换机获取的新数据。键盘操作：按 Alt-R。 如果更改了网格中的值并且在单击 Set 之前单击了 Refresh，则网格中的所有值都将恢复为之前设置的值。 Refresh 仅当交换机在线时可用。Refresh 按钮在交换机离线时灰显。
Edit Pool Properties	单击即显示 DHCP Pool Definition and Edit 对话框并会根据当前行对应的实例填充其中的值。 Edit 列按钮可用条件：交换机在线、Enable Dynamic Host Configuration Protocol (DHCP) 复选框已选中并且相应行已填充。 Edit 列按钮在以下情况下灰显：交换机离线、Enable Dynamic Host Configuration Protocol (DHCP) 复选框已取消选中。
New Pool	单击即显示 DHCP Pool Definition and Edit 对话框（所有字段均为空并且 Custom 单选按钮未选中）。此外，Module Properties 对话框的网格中将增加一个新行 / 实例 - DHCP Pool Display。键盘操作：按 Alt-N。 New 按钮仅在满足以下条件时可用：交换机在线、Enable Dynamic Host Configuration Protocol (DHCP) 复选框已选中。New 按钮在以下情况下灰显：交换机离线、Enable Dynamic Host Configuration Protocol (DHCP) 复选框已取消选中。
Set	单击即可将在该对话框中所做的属性更改应用于交换机。只有修改过的属性会应用于交换机。将出现 Enter Password 对话框。 如果设置属性时出错，则 Set 操作将终止并且所有后续属性值将不会应用于交换机。此外，Set 按钮仍可用。 Set 按钮仅在满足以下条件时可用：交换机在线并且存在属性更改。在交换机离线时，Set 按钮将灰显。

DHCP 地址分配

可在 DHCP Address Assignment 选项卡上查看并配置 DHCP 持久性。利用 DHCP 持久性，可以为每个端口分配一个特定的 IP 地址，从而确保连接到特定端口的设备将获得该端口的 IP 地址。



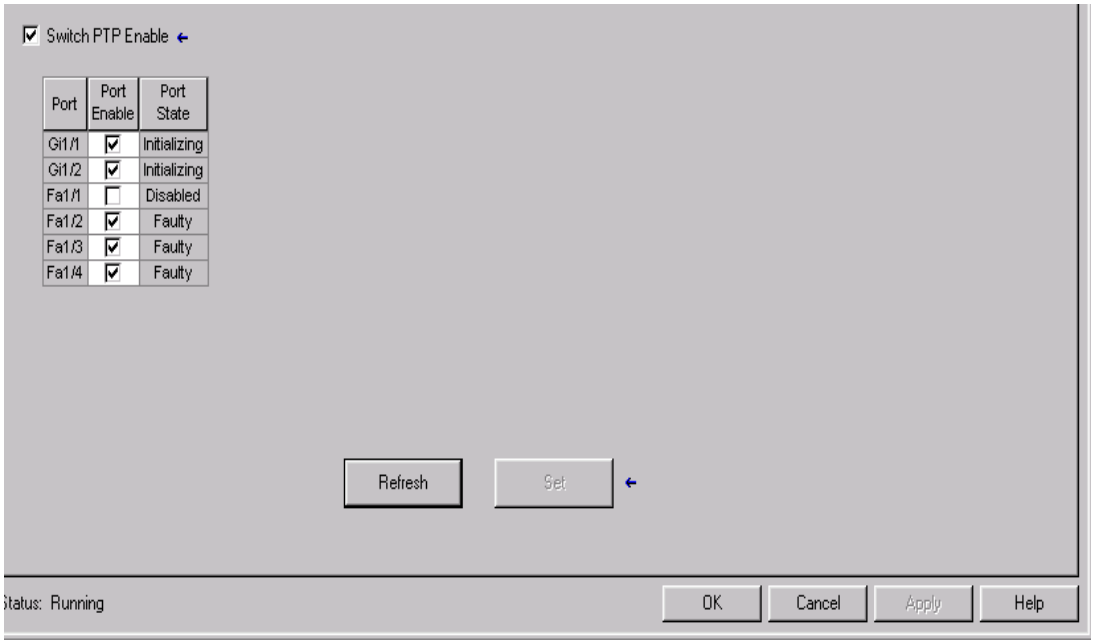
提示 如果离线，此选项卡上的信息将不会显示。

表 39 - DHCP Address Assignment 选项卡字段

字段	描述
Port	显示可供配置的端口。端口号包括端口类型（Fa 表示高速以太网，Gi 表示千兆以太网）、交换机编号 (1) 以及具体的端口号。 **示例：** • Gi1/1 表示千兆以太网端口 1。 • Fa1/1 表示高速以太网端口 1。
Pool	显示 DHCP IP 地址池中与交换机中可用实例相对应的池名称。 如果在 Module Properties 对话框的 DHCP Pool Display 选项卡中删除所有包含池的行，并且单击了 Refresh，则 Pool 字段将为空。 Pool 字段在交换机在线时可用，在交换机离线时灰显。
IP Address	显示分配给交换机端口的 IP 地址。格式是 32 位数字地址，共四组数字，之间用句点分隔（如 255.255.255.255）。每组数字的范围都是 0...255。 IP Address 字段仅在交换机在线时可用，交换机离线即灰显。
Refresh	单击即刷新网格控件以显示直接从交换机获取的新数据。键盘操作：按 Alt-R。 如果更改了网格中的值并且在在单击 Set 之前单击了 Refresh，则网格中的所有值都将恢复为之前设置的值。 Refresh 按钮仅当交换机在线时可用。Refresh 按钮在交换机离线时灰显。
Set	单击即可将在该对话框中所做的更改应用于交换机。将出现 Enter Password 对话框。

时间同步配置

该功能可通过 PTP 同步端口。PTP 可在网络中以纳秒级精度对设备的实时时钟进行同步。通过使用最佳主时钟选择，交换机可识别出带有最佳时钟源的设备所连接的交换机端口。然后，交换机会将其内部时钟与最佳时钟源进行同步，并且该交换机端口将设置为主时钟状态。网络中最精确的时钟源称为主时钟。有关此功能的详细信息，请参见第 72 页上的CIP Sync时间同步（精密时间协议）。



提示　　如果离线，此选项卡上的信息将不会显示。

表 40 - Time Sync Configuration 选项卡字段

字段	描述
Switch PTP Enable	选中此复选框即在设备上启用 PTP。默认情况下，交换机的所有高速以太网和千兆以太网端口都启用 PTP。 取消选中此复选框即在设备上禁用 PTP。 取消选中 Switch PTP Enable 复选框时，Port Enable 和 Port State 功能灰显。
Port	显示为配置选择的端口。端口号包括端口类型（Fa 表示高速以太网，Gi 表示千兆以太网）以及具体的端口号。 **示例：** Gi1/1 表示千兆以太网端口 1。
Port Enable	选中此复选框即在设备上启用端口配置。 取消选中此复选框即在设备上禁用端口配置。 取消选中 Switch PTP Enable 复选框时，Port Enable 功能灰显。
Port State	显示设备 PTP 端口的当前状态。 有效值： • Initializing • Faulty • Disabled • Listening • Pre-Master • Master • Uncalibrated • Slave 取消选中 Switch PTP Enable 复选框时，Port State 字段为空且灰显。
Refresh	单击即刷新选项卡，以显示新的交换机数据。
Set	单击以将设置发送到交换机。将出现 Enter Password 对话框。 准备好输入有效密码以进行配置设置。 在交换机离线时，Set 按钮将灰显。

NAT 配置

可在 NAT 选项卡中创建 NAT 实例。

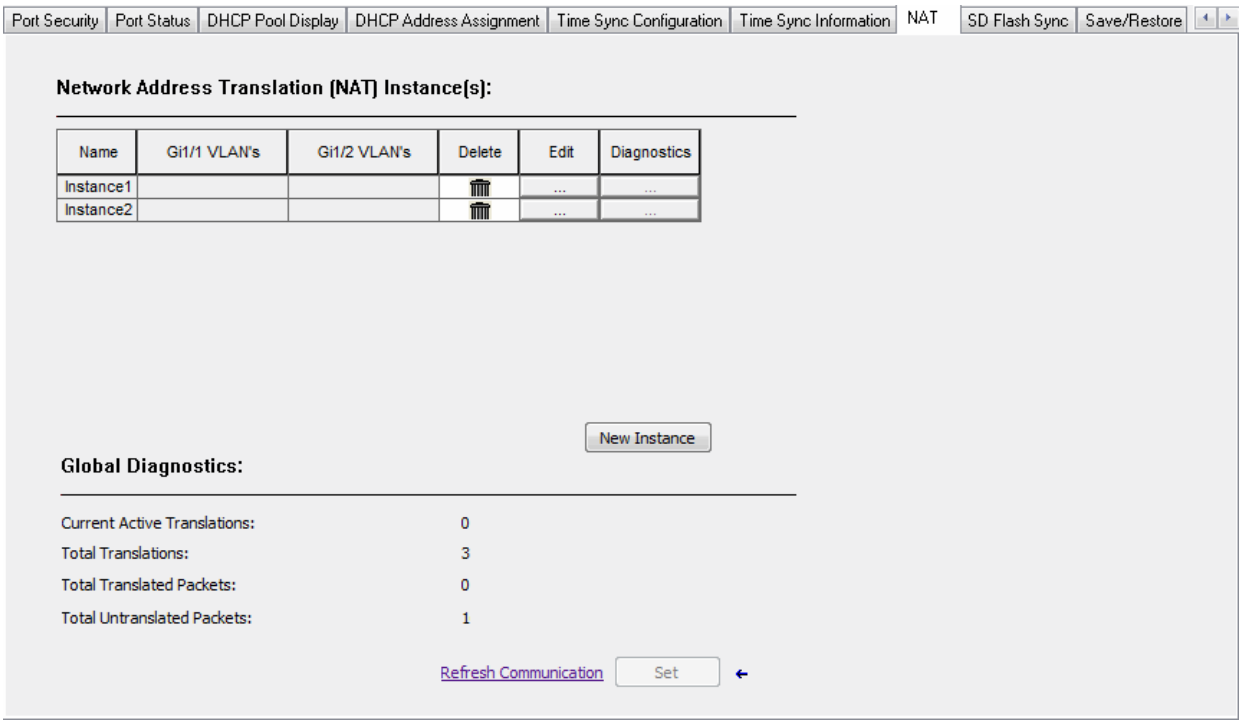


表 41 - NAT 选项卡字段

字段	描述
名称	显示 NAT 实例的唯一名称。
Gi1/1 VLANs	显示分配给端口 Gi1/1 上各 NAT 实例的 VLAN。
Gi1/2 VLANs	显示分配给端口 Gi1/2 上各 NAT 实例的 VLAN。
Delete	单击即永久删除 NAT 实例。单击 Set 后，交换机将删除该实例。
Edit	单击即可对 NAT 实例的配置进行修改。
Diagnostics	单击即可查看实例的转换诊断。请参见第 175 页。
New Instance	单击即可创建 NAT 实例。请参见第 166 页。
Current Active Translations	显示所有 NAT 实例中上 90 秒内所发生转换的总数。
Total Translations	显示所有 NAT 实例的转换总数。
Total Translated Packets	显示所有 NAT 实例中转换后数据包的总数。
Total Untranslated Packets	显示所有 NAT 实例中被忽略的数据包的总数。
Refresh Communication	单击即可刷新选项卡中的所有数据。
Set	在单击实例旁的 Trash 图标后，单击 Set 即可将 NAT 实例从交换机中删除。

要配置 NAT，请根据应用按以下步骤之一操作：

- 为通过第 3 层交换机或路由器进行路由的通信创建 NAT 实例

  有关此应用的示例，请参见第 73 页上的图 4。
- 为通过第 2 层交换机或路由器进行路由的通信创建 NAT 实例

  有关此应用的示例，请参见第 74 页上的图 5。

重要信息　创建 NAT 实例前，设置所有的智能端口角色和 VLAN。

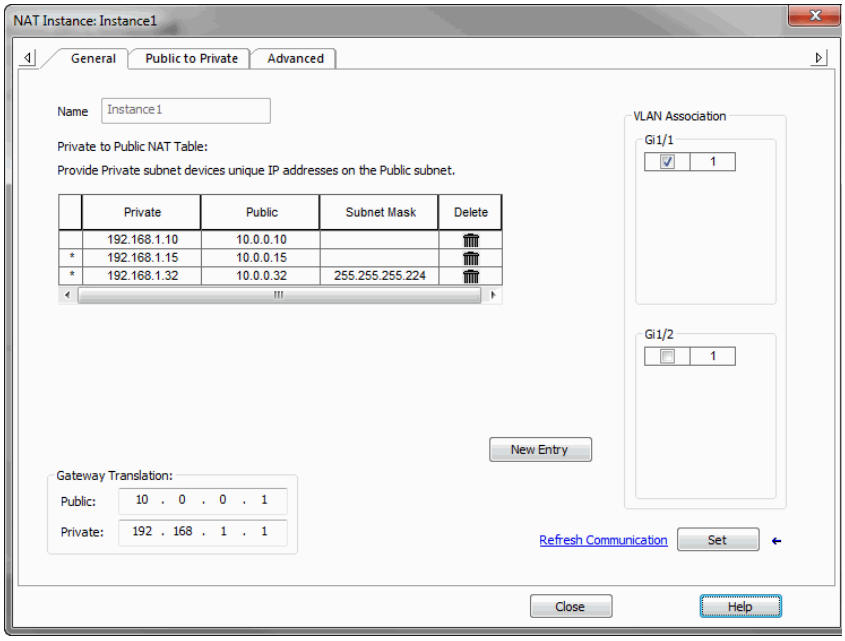
如果为与 NAT 实例关联的端口更改了智能端口角色或本机 VLAN，则必须将 VLAN 重新分配到 NAT 实例。

重要信息　由于第 2 层转发，当前通信会话会在手动断开前保持已建立状态。如果更改现有转换，则必须在新的转换生效之前，手动断开所有相关的通信会话。

为通过第 3 层交换机或路由器进行路由的通信创建 NAT 实例

要为通过第 3 层交换机或路由器进行路由的通信创建 NAT 实例，请遵循以下步骤。

1. 在 NAT 选项卡中单击 New Instance 以显示 NAT Instance 对话框中的 General 选项卡。



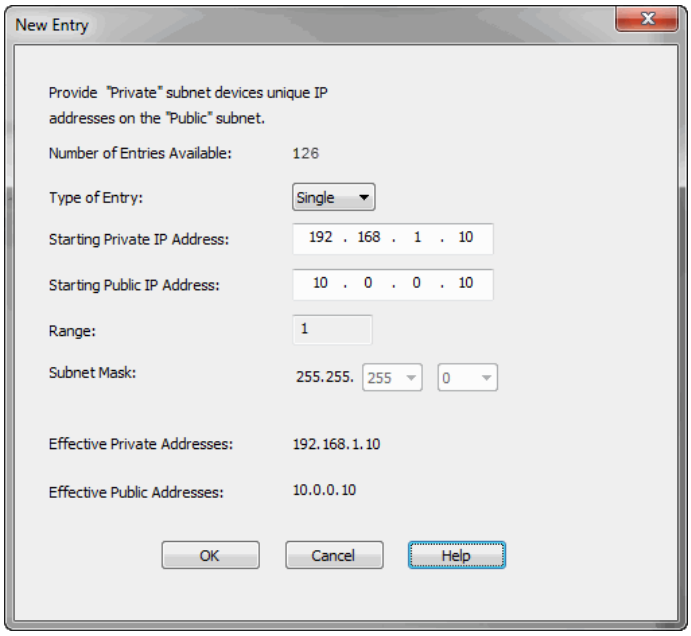
2. 在 Name 字段中，为实例输入唯一的名称。

   实例名称不能包含空格，不可超过 32 个字符。

3. 在 VLAN Association 区域中，选中将要分配给实例的 VLAN 所对应的复选框。

   有关 VLAN 分配的详细信息，请参见第 75 页。

4. 单击 New Entry 显示 New Entry 对话框。



5. 执行以下操作之一：

- 如需对要在公共子网中进行通信的专用子网中的一个设备进行地址转换，需填写以下字段。

字段	描述
Type of Entry	选择 Single。此为默认值。
Starting Private IP Address	键入该设备在专用子网中的现有地址。
Starting Public IP Address	键入代表该设备的唯一公共地址。
Effective Private Addresses	显示将进行转换的设备在专用子网中的现有地址。 如为空，则需验证以上字段中的值是否有效。
Effective Public Addresses	显示代表该设备的唯一公共地址。 如为空，则需验证以上字段中的值是否有效。

- 如需对要在公共子网中进行通信的专用子网中的一组设备进行地址转换，需填写以下字段。

字段	描述
Type of Entry	选择 Range。
Starting Private IP Address	键入该设备在专用子网中的现有起始地址。
Starting Public IP Address	键入代表该设备的唯一起始公共地址。
Range	键入范围中要包含的地址数量。 有效值：1…128 默认值 = 1 **重要信息：**范围中的每个地址计作一个转换条目。交换机最多支持 128 个转换条目。
Effective Private Addresses	显示将进行转换的设备在专用子网中的现有地址范围。 如为空，则需验证以上字段中的值是否有效。
Effective Public Addresses	显示代表该设备的唯一公共地址范围。 如为空，则需验证以上字段中的值是否有效。

- 要对专用子网中的全部地址或部分地址进行转换，需填写以下字段。

字段	描述	
Type of Entry	选择 Subnet。	
Starting Private IP Address	键入该设备在专用子网中的现有起始地址。为进行转换，该地址必须与子网掩码大小相对应，如下所示。	
	Subnet Mask	**起始专用子网地址**
	255.255.0.0	最后两个八位字节必须为 0。 **示例：** 192.168.0.0
	255.255.255.0	最后一个八位字节必须为 0。 **示例：** 192.168.1.0
	255.255.255.128	最后一个八位字节必须为 0 或 128。 **示例：** 192.168.1.0 或 192.168.1.128
	255.255.255.192	最后一个八位字符必须为以下之一：0、64、128、192. **示例**：192.168.1.64
	255.255.255.224	最后一个八位字符必须为以下之一：0、32、64、96、128、160、192、224. **示例：** 192.168.1.32
	255.255.255.240	最后一个八位字符必须为以下之一：0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240. **示例：** 192.168.1.16
Starting Public IP Address	键入可代表这些设备的唯一起始公共地址。为进行转换，该地址必须与子网掩码大小相对应，如下所示。	
	Subnet Mask	**起始公共子网地址**
	255.255.0.0	最后两个八位字节必须为 0。 **示例：** 10.200.0.0
	255.255.255.0	最后一个八位字节必须为 0。 **示例：** 10.200.1.0
	255.255.255.128	最后一个八位字节必须为 0 或 128。 **示例：** 10.200.1.0 或 10.200.1.128
	255.255.255.192	最后一个八位字符必须为以下之一：0、64、128、192. **示例：** 10.200.1.64
	255.255.255.224	最后一个八位字符必须为以下之一：0、32、64、96、128、160、192、224. **示例：** 10.200.1.32
	255.255.255.240	最后一个八位字符必须为以下之一：0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240. **示例：** 10.200.1.16
Subnet Mask	在下拉菜单中，选择要转换的地址的子网掩码。 有效值： • B 类：255.255.0.0 • C 类：255.255.255.0 • C 类部分： – 255.255.255.128 （每个转换条目提供 128 个地址） – 255.255.255.192 （每个转换条目提供 64 个地址） – 255.255.255.224 （每个转换条目提供 32 个地址） – 255.255.255.240 （每个转换条目提供 16 个地址）	
Effective Private Addresses	显示将进行转换的设备在专用子网中的现有地址范围。 如为空，则需验证以上字段中的值是否有效。	
Effective Public Addresses	显示代表该设备的唯一公共地址范围。 如为空，则需验证以上字段中的值是否有效。	

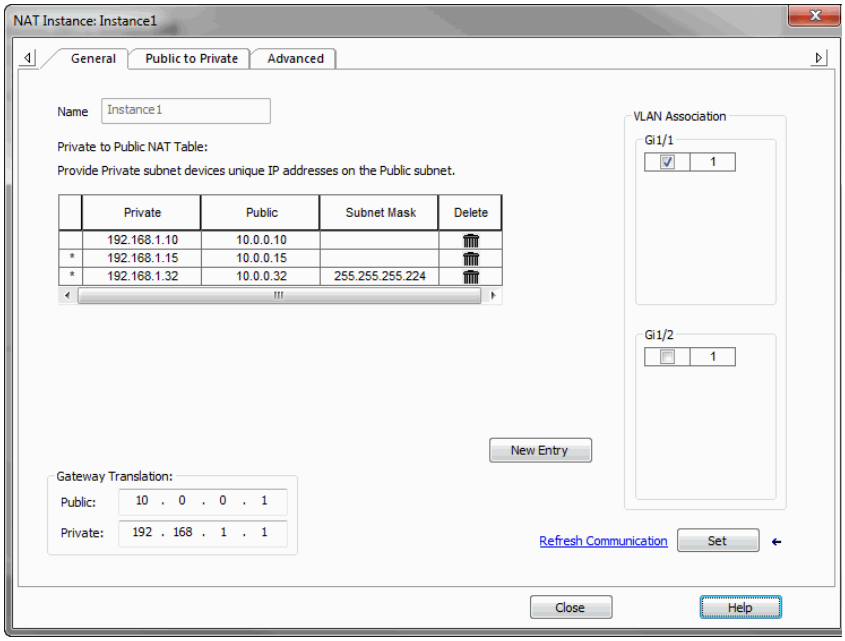
6. 单击 OK。

7. 填写 Gateway Translation 下的各个字段，以使公共子网中的设备能够与专用子网中设备进行通信：
   - Public— 键入连接到交换机上行链路端口的第 3 层交换机或路由器的默认网关地址。
   - Private— 键入专用网络上代表第 3 层交换机或路由器的唯一 IP 地址。
8. 要配置通信许可和数据包修复，请执行第 174 页上的配置通信许可和修复。
9. 单击 Set。

为通过第 2 层交换机或路由器进行路由的通信创建 NAT 实例

要为通过第 2 层交换机进行路由的通信创建 NAT 实例，请遵循以下步骤。

1. 在 NAT 选项卡中单击 New Instance 以显示 NAT Instance 对话框。

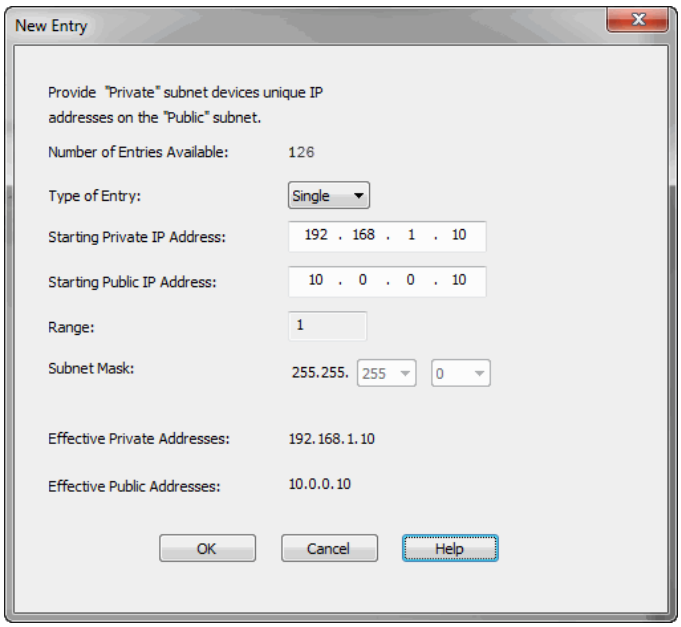


2. 在 Name 字段中，为实例输入唯一的名称。

   实例名称不能包含空格，不可超过 32 个字符。
3. 从右侧的 VLAN 列表中，选中每个 VLAN 旁边的复选框，将其分配到实例。

   有关 VLAN 分配的详细信息，请参见第 75 页。

4. 单击 New Entry 显示 New Entry 对话框。



5. 执行以下操作之一：

- 如需对要在公共子网中进行通信的专用子网中的一个设备进行地址转换，需填写以下字段。

字段	描述
Type of Entry	选择 Single。此为默认值。
Starting Private IP Address	键入该设备在专用子网中的现有地址。
Starting Public IP Address	键入代表该设备的唯一公共地址。
Effective Private Addresses	显示将进行转换的设备在专用子网中的现有地址。 如为空，则需验证以上字段中的值是否有效。
Effective Public Addresses	显示代表该设备的唯一公共地址。 如为空，则需验证以上字段中的值是否有效。

- 如需对要在公共子网中进行通信的专用子网中的一组设备进行地址转换，需填写以下字段。

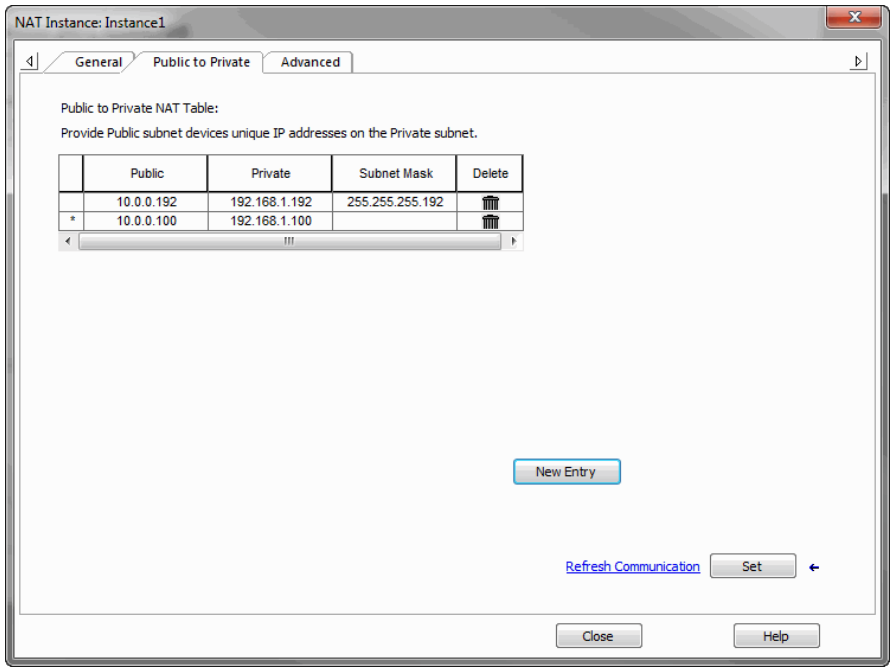
字段	描述
Type of Entry	选择 Range。
Starting Private IP Address	键入该设备在专用子网中的现有起始地址。
Starting Public IP Address	键入可代表这些设备的唯一起始公共地址。
Range	键入范围中要包含的地址数量。 有效值：1…128 默认值 = 1 **重要信息：** 范围中的每个地址计作一个转换条目。交换机最多支持 128 个转换条目。
Effective Private Addresses	显示将进行转换的设备在专用子网中的现有地址范围。 如为空，则需验证以上字段中的值是否有效。
Effective Public Addresses	显示代表该设备的唯一公共地址范围。 如为空，则需验证以上字段中的值是否有效。

- 要对专用子网中的全部地址或部分地址进行转换，需按下表所示填写以下字段。

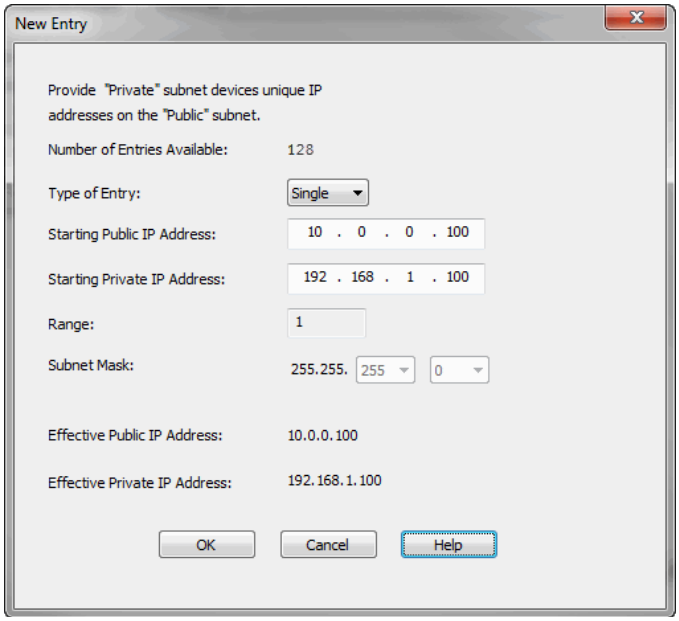
字段	描述	
Type of Entry	选择 Subnet。	
Starting Private IP Address	键入该设备在专用子网中的现有起始地址。为进行转换，该地址必须与子网掩码大小相对应，如下所示。	
	Subnet Mask	**起始专用子网地址**
	255.255.0.0	最后两个八位字节必须为 0。 **示例：** 192.168.0.0
	255.255.255.0	最后一个八位字节必须为 0。 **示例：** 192.168.1.0
	255.255.255.128	最后一个八位字节必须为 0 或 128。 **示例：** 192.168.1.0 或 192.168.1.128
	255.255.255.192	最后一个八位字符必须为以下之一：0、64、128、192. **示例：** 192.168.1.64
	255.255.255.224	最后一个八位字符必须为以下之一：0、32、64、96、128、160、192、224. **示例：** 192.168.1.32
	255.255.255.240	最后一个八位字符必须为以下之一：0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240. **示例：** 192.168.1.16
Starting Public IP Address	键入可代表这些设备的唯一起始公共地址。为进行转换，该地址必须与子网掩码大小相对应，如下所示。	
	Subnet Mask	**起始公共子网地址**
	255.255.0.0	最后两个八位字节必须为 0。 **示例：** 10.200.0.0
	255.255.255.0	最后一个八位字节必须为 0。 **示例：** 10.200.1.0
	255.255.255.128	最后一个八位字节必须为 0 或 128。 **示例：** 10.200.1.0 或 10.200.1.128
	255.255.255.192	最后一个八位字符必须为以下之一：0、64、128、192. **示例：** 10.200.1.64
	255.255.255.224	最后一个八位字符必须为以下之一：0、32、64、96、128、160、192、224. **示例：** 10.200.1.32
	255.255.255.240	最后一个八位字符必须为以下之一：0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240. **示例：** 10.200.1.16
Subnet Mask	在下拉菜单中，选择要转换的地址的子网掩码。 有效值： • B 类：255.255.0.0 • C 类：255.255.255.0 • C 类部分： – 255.255.255.128 （每个转换条目提供 128 个地址） – 255.255.255.192 （每个转换条目提供 64 个地址） – 255.255.255.224 （每个转换条目提供 32 个地址） – 255.255.255.240 （每个转换条目提供 16 个地址）	
Effective Private Addresses	显示将进行转换的设备在专用子网中的现有地址范围。 如为空，则需验证以上字段中的值是否有效。	
Effective Public Addresses	显示代表该设备的唯一公共地址范围。 如为空，则需验证以上字段中的值是否有效。	

6. 单击 OK。

7. 单击 Public to Private 选项卡。



8. 单击 New Entry 显示 New Entry 对话框。



9. 执行以下操作之一：

- 如需对要在专用子网中进行通信的公共子网中的一个设备进行地址转换，需填写以下字段。

字段	描述
Type of Entry	选择 Single。此为默认值。
Starting Public IP Address	键入该设备在公共子网中的现有地址。
Starting Private IP Address	键入代表该设备的唯一专用地址。
Effective Public Addresses	显示将进行转换的设备在公共子网中的现有地址。 如为空，则需验证以上字段中的值是否有效。
Effective Private Addresses	显示代表该设备的唯一专用地址。 如为空，则需验证以上字段中的值是否有效。

- 如需对要在专用子网中进行通信的公共子网中的一组设备进行地址转换，需填写以下字段。

字段	描述
Type of Entry	选择 Range。
Starting Public IP Address	键入该设备在公共子网中的现有起始地址。
Starting Private IP Address	键入可代表这些设备的唯一起始专用地址。
Range	键入范围中要包含的地址数量。 有效值：1…128 默认值 = 1 **重要信息：** 范围中的每个地址计作一个转换条目。交换机最多支持 128 个转换条目。
Effective Public Addresses	显示将进行转换的设备在公共子网中的现有地址范围。 如为空，则需验证以上字段中的值是否有效。
Effective Private Addresses	显示代表该设备的唯一专用地址范围。 如为空，则需验证以上字段中的值是否有效。

- 要对公共子网中的全部地址或部分地址进行转换，需按下表所示填写以下字段。

字段	描述	
Type of Entry	选择 Subnet。	
Starting Public IP Address	键入该设备在公共子网中的现有起始地址。为进行转换，该地址必须与子网掩码大小相对应，如下所示。	
	Subnet Mask	**起始公共子网地址**
	255.255.0.0	最后两个八位字节必须为 0。 **示例：** 10.200.0.0
	255.255.255.0	最后一个八位字节必须为 0。 **示例：** 10.200.1.0
	255.255.255.128	最后一个八位字节必须为 0 或 128。 **示例：** 10.200.1.0 或 10.200.1.128
	255.255.255.192	最后一个八位字符必须为以下之一：0、64、128、192. **示例：** 10.200.1.64
	255.255.255.224	最后一个八位字符必须为以下之一：0、32、64、96、128、160、192、224. **示例：** 10.200.1.32
	255.255.255.240	最后一个八位字符必须为以下之一：0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240. **示例：** 10.200.1.16
Starting Private IP Address	键入可代表这些设备的唯一起始专用地址。为进行转换，该地址必须与子网掩码大小相对应，如下所示。	
	Subnet Mask	**起始专用子网地址**
	255.255.0.0	最后两个八位字节必须为 0。 **示例：** 192.168.0.0
	255.255.255.0	最后一个八位字节必须为 0。 **示例：** 192.168.1.0
	255.255.255.128	最后一个八位字节必须为 0 或 128。 **示例：** 192.168.1.0 或 192.168.1.128
	255.255.255.192	最后一个八位字符必须为以下之一：0、64、128、192. **示例：** 192.168.1.64
	255.255.255.224	最后一个八位字符必须为以下之一：0、32、64、96、128、160、192、224. **示例：** 192.168.1.32
	255.255.255.240	最后一个八位字符必须为以下之一：0、16、32、48、64、80、96、112、128、144、160、176、192、208、224、240. **示例：** 192.168.1.16

字段	描述
Subnet Mask	在下拉菜单中，选择要转换的地址的子网掩码。 有效值： • B 类：255.255.0.0 • C 类：255.255.255.0 • C 类部分： – 255.255.255.128（每个转换条目提供 128 个地址） – 255.255.255.192（每个转换条目提供 64 个地址） – 255.255.255.224（每个转换条目提供 32 个地址） – 255.255.255.240（每个转换条目提供 16 个地址）
Effective Public Addresses	显示将进行转换的设备在公共子网中的现有地址范围。 如为空，则需验证以上字段中的值是否有效。
Effective Private Addresses	显示代表该设备的唯一专用地址范围。 如为空，则需验证以上字段中的值是否有效。

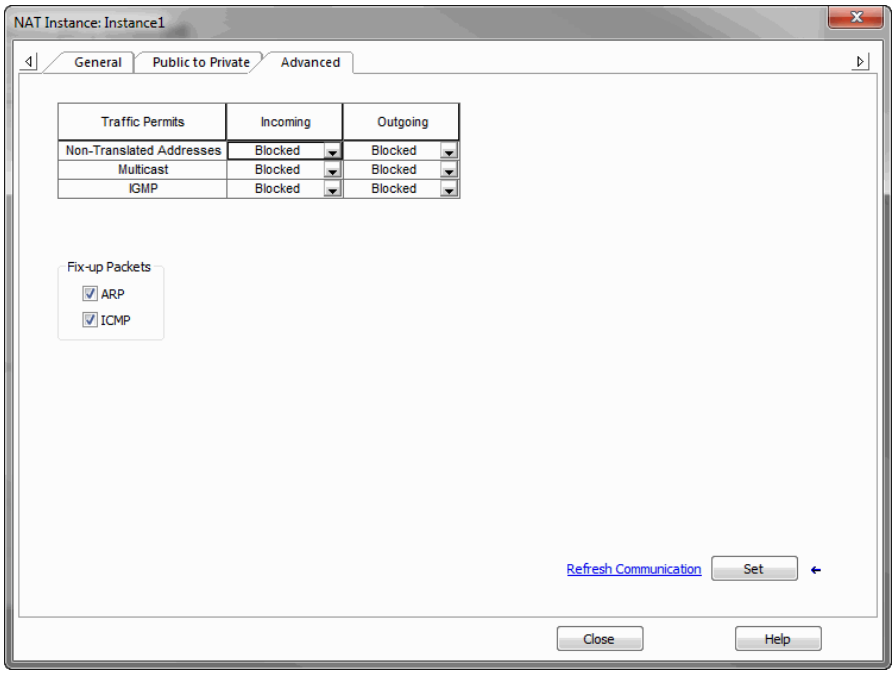
10. 单击 OK。
11. （可选）。要配置通信许可和数据包修复，请执行第 174 页上的配置通信许可和修复。
12. 单击 Set。

配置通信许可和修复

配置通信许可和修复时应小心谨慎。建议使用默认值。

要配置通信许可或数据包修复，请按以下步骤操作。

1. 单击 Advanced 选项卡。



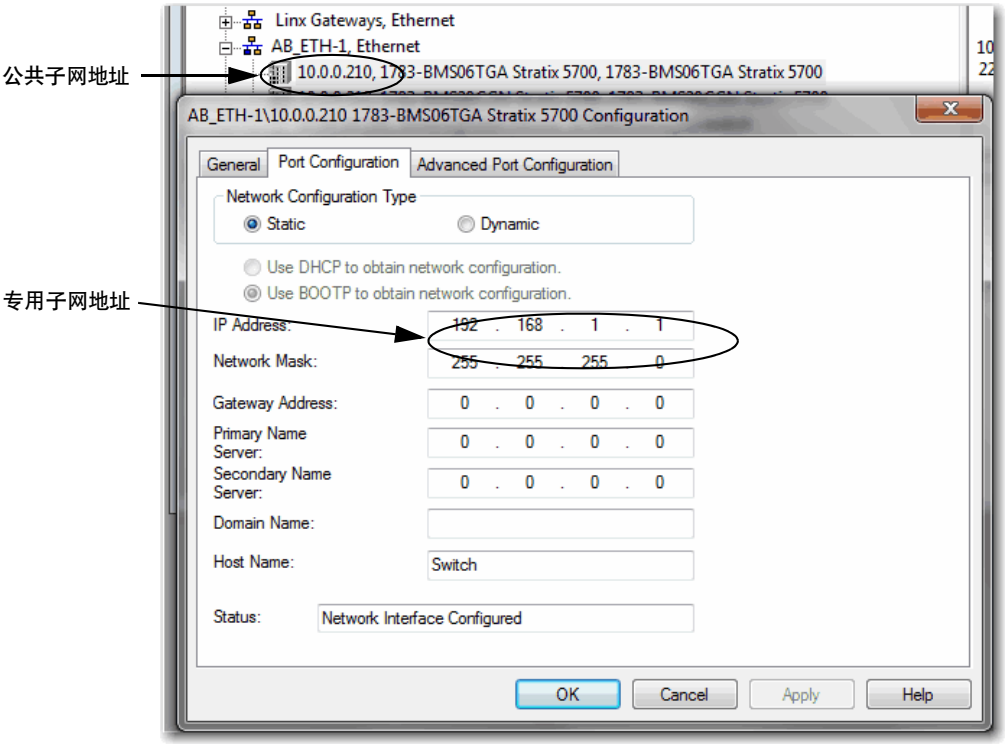
2. 在 Traffic Permits 网格中，为不经 NAT 处理的传入和传出数据包选择以下选项之一：
   - Pass-Through — 允许数据包通过 NAT 边界。
   - Blocked — 丢弃数据包。
3. 在 Fix-up Packets 区域中，选中或取消选中复选框来启用或禁用 ARP 和 ICMP 协议的修复。

   默认情况下，ARP 和 ICMP 的修复处于启用状态。

在 RSLinx 软件中查看地址转换

RSLinx 软件的以太网驱动程序支持设备的地址转换。如果设备地址已配置为进行转换，则该设备的公共子网地址将在 RSLinx 软件的主对话框中显示。而其专用子网地址则会在设备的配置属性中显示。

图 9 - RSLinx 软件中的公共和专用子网地址

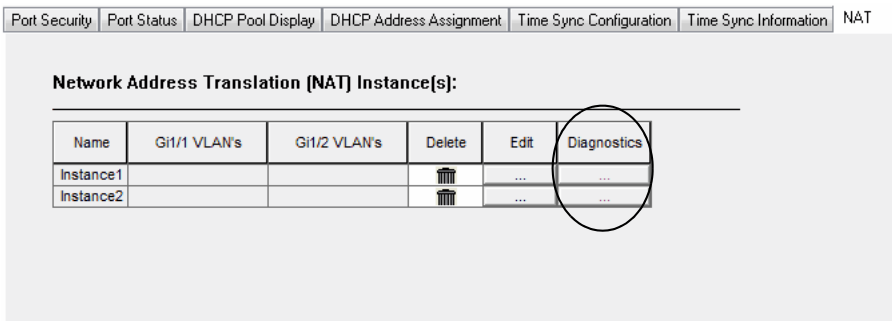


NAT 诊断

针对 NAT 实例，可监视以下诊断:

- 针对公共转换和专用转换的诊断
- 仅针对专用转换的诊断
- 仅针对公共转换的诊断

要访问实例的诊断信息，请在 NAT 选项卡上单击 Diagnostics 列中椭圆圈中的区域。



NAT Diagnostics 对话框中将显示所选实例的诊断信息。

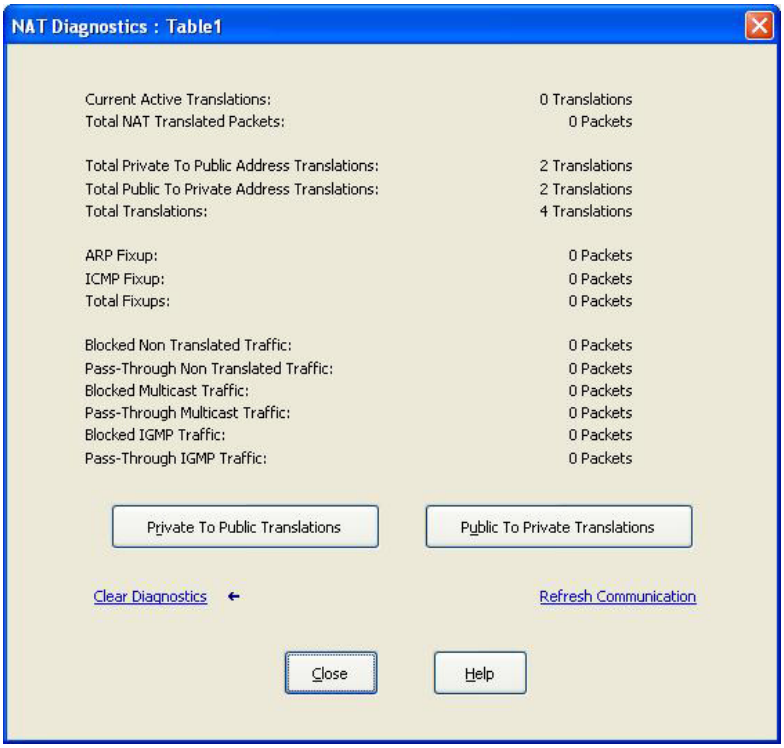


表 42 - 具体实例的 NAT 诊断

字段	描述
Current Active Translations	显示所有 NAT 实例中上 90 秒内所发生的转换数。
Total NAT Translated Packets	显示已为该实例转换的数据包总数。
Total Private to Public Address Translations	显示该实例所进行的 " 专用到公共 " 转换的总数。
Total Public to Private Address Translations	显示该实例所进行的 " 公共到专用 " 转换的总数。
ARP Fixup	显示该实例的已修复 ARP 数据包数。
ICMP Fixup	显示该实例的已修复 ICMP 数据包数。
Total Fixups	显示该实例的已修复 ARP 和 ICMP 数据包数。
Incoming Non Translated Traffic (Pass-Through)	显示该实例中未转换通信已通过 NAT 的传入数据包数。
Outgoing Non Translated Traffic (Blocked)	显示该实例中已被 NAT 阻断未转换通信的传出数据包数。
Incoming Multicast Traffic (Blocked)	显示该实例中已被 NAT 阻断多播通信的传入数据包数。
Outgoing Multicast Traffic (Pass-Through)	显示该实例中多播通信已通过 NAT 的传出数据包数。
Incoming IGMP Traffic (Blocked)	显示该实例中 IGMP 通信已被 NAT 阻断的传入数据包数。
Outgoing IGMP Traffic (Blocked)	显示该实例中 IGMP 通信已被 NAT 阻断的传出数据包数。
Private to Public Translations	单击即可查看该实例中 " 专用到公共 " 转换的诊断信息。请参见第 177 页上的 " 专用到公共 " 转换诊断。
Public to Private Translations	单击即可查看该实例中 " 专用到公共 " 转换的诊断信息。请参见第 177 页上的 " 专用到公共 " 转换诊断。
Refresh Communication	单击即可刷新该实例的所有诊断信息。

“ 专用到公共 ” 转换诊断

可在实例的 Private to Public Translations 对话框中查看前 90 秒内由 NAT 更改的各 IP 地址。

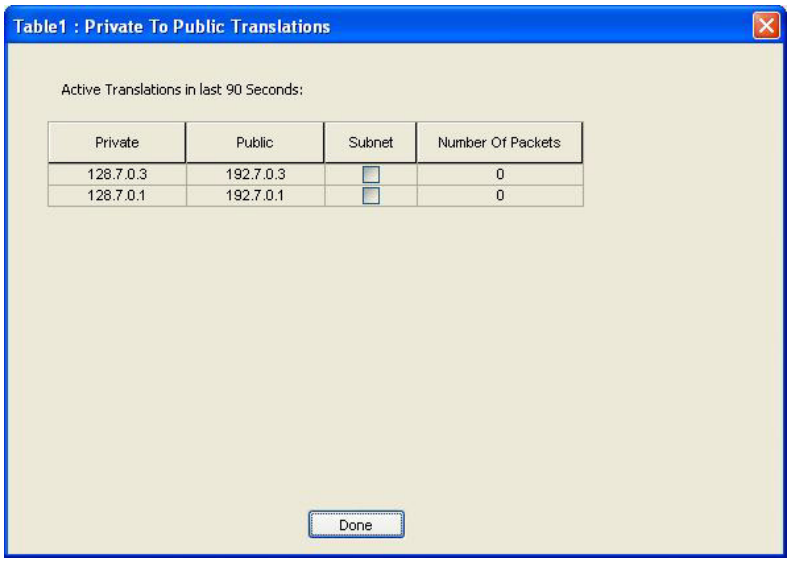


表 43 - “ 专用到公共 ” 转换诊断

字段	描述
Private	显示设备在专用子网中的现有地址。
Public	显示在专用子网中代表相应设备的唯一公共地址。
Subnet	指示该转换是否属于 Subnet 条目类型。
Number of Packets	显示包含转换的数据包的数量。

“ 公共到专用 ” 转换诊断

可在实例的 Public to Private Translations 对话框中查看前 90 秒内由 NAT 更改的 IP 地址列表。

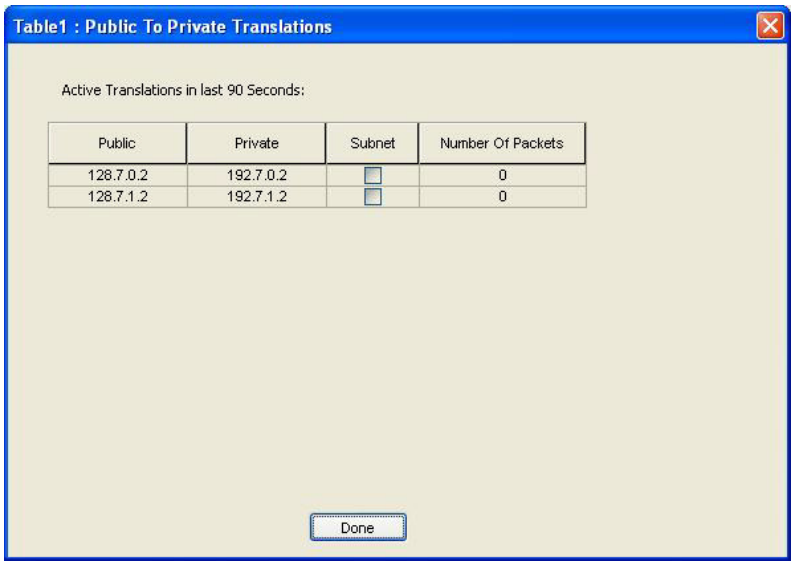


表 44 - “ 公共到专用 ” 转换诊断

字段	描述
Public	显示与专用子网 IP 地址相对应的公共子网中的唯一 IP 地址。
Private	显示已更改为公共子网唯一 IP 地址的原专用子网 IP 地址。
Subnet	指示该转换是否属于 Subnet 条目类型。
Number of Packets	显示包含转换的数据包的数量。

SD 闪存同步

可针对配置文件或整个画面进行 SD 卡同步。

重要信息　如果同步的方向错误，可覆盖配置。

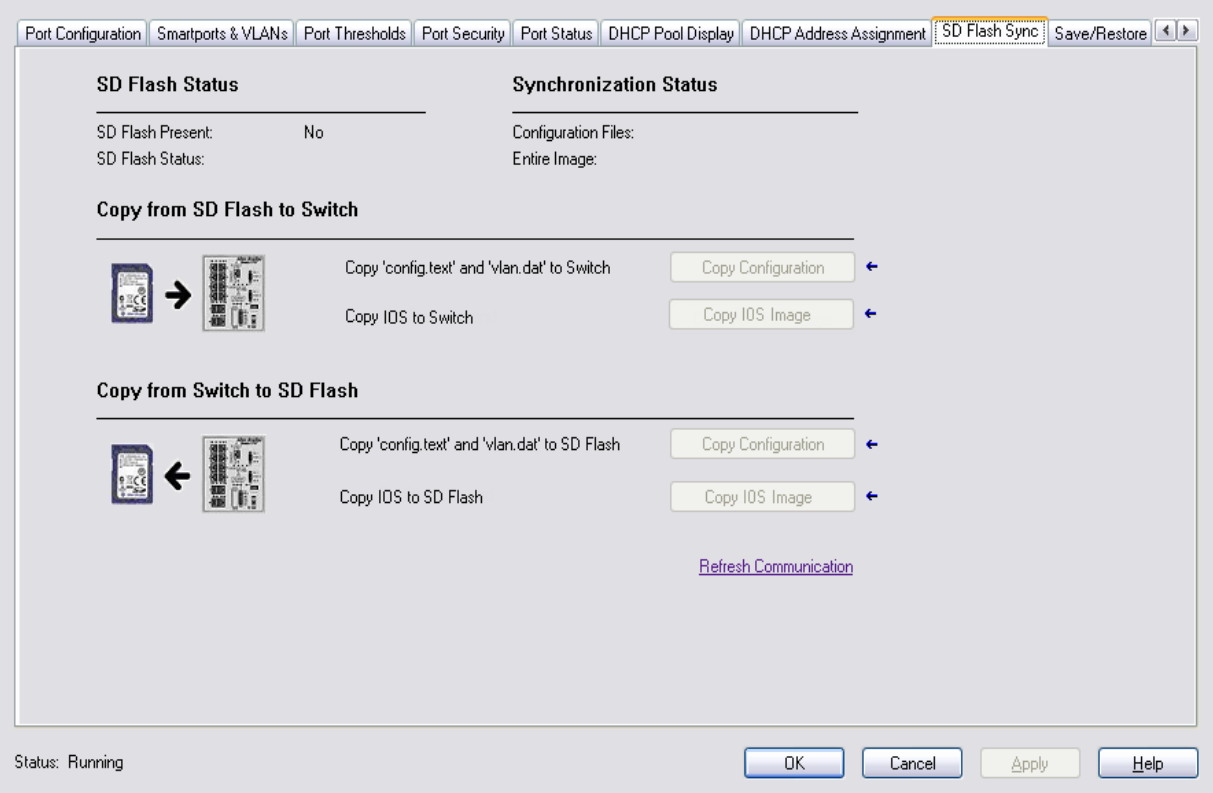


表 45 - SD Flash Sync 选项卡字段

字段	描述
SD Flash Status	指示是否存在 SD 卡以及卡的状态。
Synchronization Status	指示配置文件和 IOS 是处于已同步状态还是未同步状态。
Copy from SD Flash to Switch	从以下两个选项中选择： • Copy Configuration • Copy IOS Image
Copy from Switch to SD Flash	从以下两个选项中选择： • Copy Configuration • Copy IOS Image

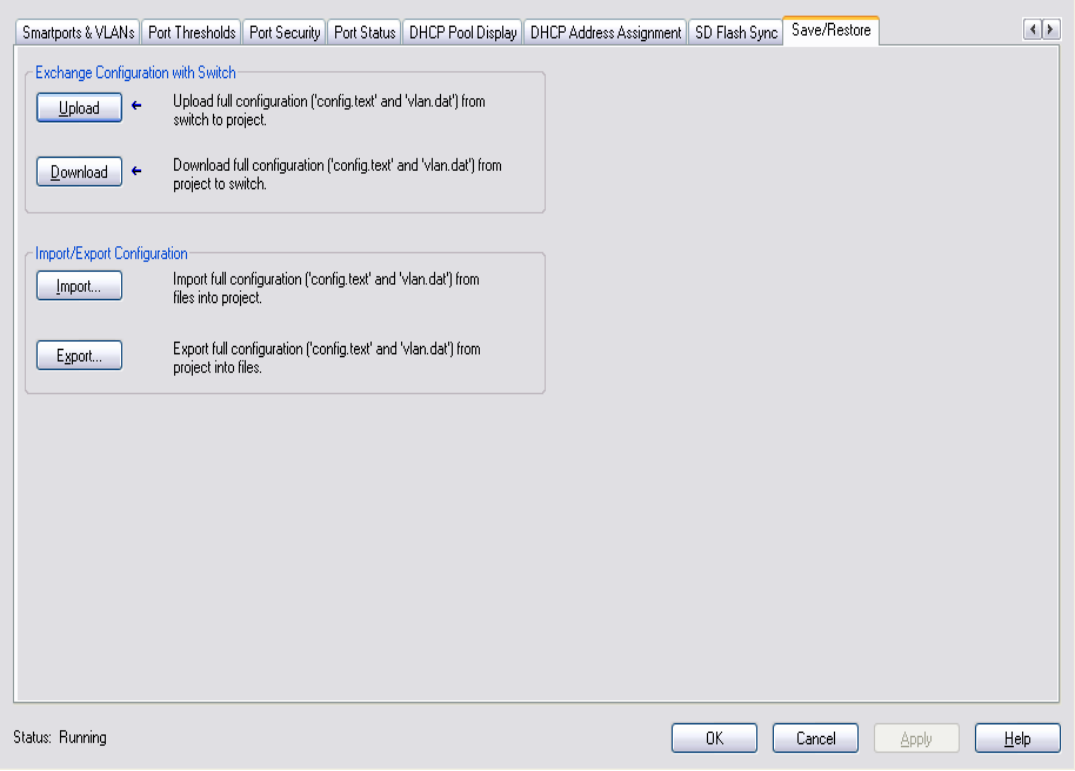
保存和恢复交换机配置

使用此选项卡执行下列操作:

- 将交换机配置保存为文档以作为归档。
- 恢复计算机上本地存储的交换机配置，或恢复 Logix 设计器应用程序项目中存储的交换机配置。

必须在线保存和恢复配置文件。交换机处于离线状态时，大部分设置均为灰显。

准备输入有效的交换机密码，以便进行交换机配置的保存和恢复。



交换机配置由以下两个文件组成:

- 包含配置参数的文本文件
- 包含 VLAN 信息的二进制文件

交换机配置上传到 Logix 设计器应用程序的项目文件中之后，可通过 Export 按钮将交换机配置以计算机文件的形式导出。

通过使用交换机 AOP 上的 Import 按钮，可以将交换机配置从计算机上的相应文件导入到项目中。然后，可以使用 AOP 上的 Download 按钮将配置下载到交换机。有关保存和恢复功能的详细信息，请参见第 179 页上的 保存和恢复交换机配置。

注：

处理交换机故障

本章可帮助您解决 Stratix 5700 交换机的相关问题，同时也可帮助执行交换机重置等常见功能。

有关故障处理的更多信息，请参见：

- 第 132 页上的诊断电缆问题
- 第 133 页上的查看系统日志消息

验证快速启动

快速启动故障是交换机的潜在致命故障。如果您的交换机无法成功完成快速启动，请联系您的罗克韦尔自动化代表。您可以使用 CLI 禁用快速启动，并运行上电自检 (POST)。

IP 地址问题

以下是交换机 IP 地址相关问题的基本处理技巧。

问题	解决方案
未从 DHCP 服务器接收到 IP 地址	如果交换机未从作为 DHCP 服务器工作的上游设备处接收到 IP 地址，则应确保上游设备正作为 DHCP 服务器工作，然后再次按照第 1 章，关于交换机所述步骤设置交换机。
交换机 IP 地址错误	如果交换机已安装到网络中，但由于其 IP 地址错误而导致无法访问交换机，则可为其分配一个新 IP 地址，请参见第 182 页上的访问直接管理模式来分配 IP 地址，然后在设备管理器 Express Setup 窗口中更新交换机的 IP 地址。

设备管理器 Web 界面问题

以下是设备管理器 Web 界面显示相关问题的基本处理技巧。

问题	解决方案
设备管理器 Web 界面不能正常显示	如果您的计算机或笔记本电脑上无法显示设备管理器 Web 界面，请确保您在浏览器中输入正确的交换机 IP 地址。 如果您在浏览器中输入的交换机 IP 地址正确，请确保交换机与您的计算机或笔记本电脑位于同一网络或子网中： • 例如，如果您的交换机 IP 地址为 172.20.20.85，您的计算机或笔记本电脑 IP 地址为 172.20.20.84，则两台设备位于同一网络中。 • 例如，如果您的交换机 IP 地址为 172.20.20.85，而您的计算机或笔记本电脑 IP 地址为 10.0.0.2，则两台设备位于不同网络中，没有路由器无法直接通信。您必须更改交换机 IP 地址与计算机或笔记本电脑 IP 地址中的一个。 • 如果问题仍然存在，请按照第 182 页上访问直接管理模式部分所述的步骤操作，然后在设备管理器的 Express Setup 窗口更新交换机网络设置。 • 如果问题仍然存在，请按照第 185 页上恢复交换机固件和还原出厂默认设置部分所述的步骤操作。
设备管理器 Web 界面未正常工作	如果设备管理器 Web 界面未正常工作（例如，设备管理器未响应），则按照第 182 页访问直接管理模式部分所述的步骤操作，然后在设备管理器 Web 界面 Express Setup 窗口上更新交换机网络设置。 如果问题仍然存在，请按照第 185 页上恢复交换机固件和还原出厂默认设置部分所述的步骤操作。
无法通过网络访问设备管理器 Web 界面	如果您无法通过 Web 浏览器远程访问设备管理器，请按照第 182 页上访问直接管理模式部分所述的步骤操作。

交换机性能

以下是交换机性能相关问题的基本处理技巧。

问题	解决方案
速度、双工和自动协商	如果端口统计中显示大量的定位错误、帧校验序列 (FCS) 或后冲突错误，则可能存在速度或双工不匹配的情况。 交换机与交换机之间、交换机与路由器之间或交换机与工作站或服务器之间的双工设置不匹配时通常会出现速度和双工问题。手动设置速度和双工模式或两个设备之间发生自动协商问题时，都会出现这种情况。下列情形下可能发生不匹配问题： • 手动设置的速度或双工参数与相连端口中手动设置的速度或双工参数不一致。 • 端口设置为自动协商，而相连端口却设置为无自动协商的全双工模式。 要实现交换机的最佳性能并确保链路正常运行，则在更改双工和速度设置时遵循以下准则之一： • 使两个端口自动协商速度和双工。 • 在连接的两个末端的端口上，将相同的速度和双工参数手动设置为相同值。 • 如果远程设备不自动协商，则将两个端口上的双工设置配置为相同值。 即使相连端口不自动协商，速度参数也可进行自我调整。
自动协商和网络接口卡 (NIC)	交换机和第三方网络接口卡 (NIC) 之间有时会出现问题。默认情况下，交换机的端口和接口都设置为自动协商。通常，笔记本电脑或其它类似设备也会设置为自动协商，但是有时候会出现自动协商问题。 要解决自动协商问题，可以尝试手动设置连接的两端。如果问题仍未得到解决，则可能是 NIC 的固件或软件问题。此时，将 NIC 驱动程序升级为制造商提供的最新固件或软件便可解决问题。
电缆长度	如果端口统计显示 FCS、后冲突或定位错误过多，则验证交换机到相连设备的电缆长度是否符合建议的准则。

访问直接管理模式

将交换机的一个端口与计算机或笔记本电脑建立物理连接后，便可显示设备管理器 Web 界面并对交换机进行管理。这种管理连接类型称为直接管理模式。在交换机的 IP 地址未知时，通常在该模式下使用设备管理器 Web 界面来连接交换机。

在访问直接管理模式前，必须确保以下事项：

- 必须能够实际访问交换机。
- 确保至少已启用一个交换机端口并且它未与设备相连。

要访问直接管理模式，请按以下步骤操作。

1. 按住 Express Setup 按钮，直到 Setup 状态指示灯呈绿色闪烁，而且交换机下行链路可用端口的状态指示灯也呈绿色闪烁时再松开。

   状态指示灯呈绿色闪烁的端口便为指定的直接管理模式端口。通过以下条件确定此端口：

   - 如果所有下行链路端口都未连接设备，或如果有多个下行链路端口与设备相连，则选择首个可用的下行链路端口作为直接管理模式端口。
   - 如果仅有一个下行链路端口与设备相连，则选择该端口作为直接管理模式端口。

   如果没有可连接计算机或笔记本电脑的交换机下行链路端口，则断开交换机一个下行链路端口与设备的连接，然后再次按住 Setup 按钮，直到 Setup 状态指示灯和端口状态指示灯均呈绿色闪烁时松开。

2. 使用 5 类以太网电缆将计算机或笔记本电脑连接到端口状态指示灯闪烁的交换机端口上。
3. 等待交换机和计算机或笔记本电脑上的端口状态指示灯变为绿色常亮。

   端口状态指示灯变为绿色常亮表示两个设备之间的连接已成功。

4. 在计算机或笔记本电脑中启动 Web 浏览器。

   密码输入提示与设备管理器 Web 界面的页面将相继出现。

   如果设备管理器 Web 界面未出现，则确保已禁用浏览器软件中的所有弹出窗口阻止程序或代理设置，并且已禁用计算机或笔记本电脑中运行的所有无线客户端。

   如果设备管理器 Web 界面仍然未出现，则在浏览器中输入一个 URL，例如 http://www.rockwellautomation.com。浏览器将跳转到设备管理器 Web 界面。

重启或重置交换机

如果重新配置功能仍不能解决问题，则重启或重置交换机或许可以解决问题，即使不能解决，也可排除可能的故障原因。如果在将交换机重置为默认设置后问题仍存在，则问题的原因可能不在交换机。

选项	描述
重启	此选项可在电源开启状态下重启交换机。交换机在重启过程中将保持已保存的配置设置。不过，在此过程中设备管理器 Web 界面将无法使用。此过程完成后，交换机便会显示设备管理器 Web 界面。 **重要信息：**重启交换机会中断设备与网络之间的连接。
将交换机重置为出厂默认设置	此选项将重置交换机、删除当前的配置设置、返回出厂默认设置，并在此之后重启交换机。 **注意：**重置交换机会删除包括 IP 地址在内的所有自定义交换机设置，并使交换机返回出厂默认设置。软件映像将保持不变。但需重新配置基本的交换机设置。请参见第 47 页上的通过快速设置对交换机进行初始设置。 **注意：**重置交换机会中断设备与网络之间的连接。

重要信息 重启或重置交换机会中断设备与网络之间的连接。

从设备管理器 Web 界面中重启交换机

在设备管理器 Web 界面的 Restart/Reset 对话框中，单击 Restart the Switch。

此选项可在电源开启状态下重启交换机。在重启过程中设备管理器 Web 界面将无法使用。此过程完成后，交换机便会显示设备管理器 Web 界面。

如果不知道交换机 IP 地址，请按照第 182 页上访问直接管理模式部分所述的步骤操作来访问直接管理模式。

从 Logix 设计器应用程序中重启交换机

在 Logix 设计器应用程序的 Module Properties 对话框中，执行如下操作。

1. 单击 Module Info 选项卡。
2. 单击 Reset Module。

   将出现密码输入提示。
3. 输入密码并单击 Enter。

将交换机重置为出厂默认设置

注意：重置交换机会删除包括 IP 地址在内的所有自定义交换机设置，并使交换机返回出厂默认设置。软件映像将保持不变。要管理交换机或显示设备管理器，需重新配置基本的交换机设置（如第 4 章，通过设备管理器 Web 界面管理交换机所述）并使用新的 IP 地址。

重要信息	**重启交换机会中断设备与网络之间的连接。**

在设备管理器 Web 界面中，执行以下操作。

1. 访问设备管理器 Web 界面的 Restart/Reset 对话框。
2. 单击 Reset the Switch。

   此选项将重置交换机、删除当前的配置设置、返回出厂默认设置，并在此之后重启交换机。

   如果不知道交换机 IP 地址，请按照第 182 页上访问直接管理模式部分所述的步骤操作来访问直接管理模式。然后回到第 1 步。

恢复交换机固件和还原出厂默认设置

在恢复交换机固件之前，必须确保以下事项：

- 必须能够实际访问交换机。
- 确保至少已启用一个交换机端口并且它未与设备相连。

如果映像损坏，您可以恢复交换机固件。固件损坏的一个征兆便是交换机不断尝试重启。

导致需要恢复交换机固件的其他原因还包括因固件升级失败而将映像删除和忘记交换机密码。

恢复交换机固件的操作将删除所有交换机配置设置并使交换机返回出厂默认设置。要使交换机返回出厂默认设置，按以下步骤操作。

1. 在交换机已上电且启动后，按住 Express Setup 按钮，直到 Setup 和 EIP Net 状态指示灯变为红色时松开。

   该过程大约持续 18...20 秒。

2. 松开 Express Setup 按钮。
3. 等待交换机重启。

   交换机完成重启后，Express Setup 指示灯将开始闪烁。此时交换机已返回至出厂默认设置。

4. 按照第 47 页上的通过快速设置对交换机进行初始设置所述操作设置交换机。
5. 请参见第 185 页上的处理固件升级问题并按照其中所述步骤升级固件。

处理固件升级问题

在尝试升级交换机固件时，如果收到升级失败的消息，则应确定是否仍可访问交换机。如果可以访问交换机，则按照以下步骤操作。

1. 确保已从 http://www.rockwellautomation.com 下载正确的 .tar 文件。
2. 如果下载的 .tar 文件正确，则刷新设备管理器 Web 界面浏览器会话，确保交换机同计算机、笔记本电脑或网络驱动器之间仍存在连接。
   - 如果与交换机之间存在连接，并可访问设备管理器 Web 界面，则再次尝试升级。
   - 如果与交换机之间不存在连接，并且无法访问设备管理器 Web 界面，请参见第 185 页上的恢复交换机固件和还原出厂默认设置。

注：

模块定义的数据类型

在 Logix 设计器应用程序中，输入和输出数据类型的预定义标签的结构与将其添加到 I/O 树时所选的交换机相对应。它的成员根据端口名称进行命名。

您可以禁用交换机端口，在输出标签中设置相应位即可。当控制器处于运行模式时，交换机每次从控制器接收到输出数据都会应用输出位。当控制器处于程序模式时，不会应用输出位。

如果相应的输出位为 0，则会启用端口。如果使用设备管理器 Web 界面或 CLI 来启用或禁用端口，则在下次应用端口时，端口设置可能被输出位覆盖。无论是使用设备管理器 Web 界面还是使用 CLI 来启用或禁用端口，这些输出位始终优先。

本附录中的表列出了用于 Stratix 5700 交换机的模块定义的数据类型。以下各表中包含有关输入（用 I 表示）和输出（用 O 表示）的信息。

模块定义的输入数据类型（6端口千兆交换机）

AB:STRATIX_5700_6PORT_GB_MANAGED:I:0			
成员名称	类型	默认显示样式	有效值
Fault	DINT	二进制	
AnyPortConnected	BOOL	十进制	LinkStatus:0
PortFa1_1Connected	BOOL	十进制	LinkStatus:1
PortFa1_2Connected	BOOL	十进制	LinkStatus:2
PortFa1_3Connected	BOOL	十进制	LinkStatus:3
PortFa1_4Connected	BOOL	十进制	LinkStatus:4
PortGi1_1Connected	BOOL	十进制	LinkStatus:5
PortGi1_2Connected	BOOL	十进制	LinkStatus:6
AnyPortUnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:4
PortGi1_1UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:5
PortGi1_2UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:6
AnyPortThreshold	BOOL	十进制	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	十进制	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	十进制	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	十进制	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	十进制	ThresholdExceeded:4
PortGi1_1Threshold	BOOL	十进制	ThresholdExceeded:5
PortGi1_2Threshold	BOOL	十进制	ThresholdExceeded:6
AllPortsUtilization	SINT	十进制	
PortFa1_1Utilization	SINT	十进制	
PortFa1_2Utilization	SINT	十进制	
PortFa1_3Utilization	SINT	十进制	
PortFa1_4Utilization	SINT	十进制	
PortGi1_1Utilization	SINT	十进制	
PortGi1_2Utilization	SINT	十进制	
MajorAlarmRelay	BOOL	十进制	AlarmRelay:0
MulticastGroupsActive	DINT	二进制	

模块定义的输出数据类型（6 端口千兆交换机）

AB:STRATIX_5700_6PORT_GB_MANAGED:O:0			
成员名称	**类型**	**默认显示样式**	**有效值**
AllPortsDisabled	BOOL	十进制	DisablePort:0
PortFa1_1Disable	BOOL	十进制	DisablePort:1
PortFa1_2Disable	BOOL	十进制	DisablePort:2
PortFa1_3Disable	BOOL	十进制	DisablePort:3
PortFa1_4Disable	BOOL	十进制	DisablePort:4
PortGi1_1Disable	BOOL	十进制	DisablePort:5
PortGi1_2Disable	BOOL	十进制	DisablePort:6

模块定义的输入数据类型（6 端口交换机）

AB:STRATIX_5700_6PORT_MANAGED:I:0			
成员名称	**类型**	**默认显示样式**	**有效值**
Fault	DINT	二进制	
AnyPortConnected	BOOL	十进制	LinkStatus:0
PortFa1_1Connected	BOOL	十进制	LinkStatus:1
PortFa1_2Connected	BOOL	十进制	LinkStatus:2
PortFa1_3Connected	BOOL	十进制	LinkStatus:3
PortFa1_4Connected	BOOL	十进制	LinkStatus:4
PortFa1_5Connected	BOOL	十进制	LinkStatus:5
PortFa1_6Connected	BOOL	十进制	LinkStatus:6
AnyPortUnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:6
AnyPortThreshold	BOOL	十进制	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	十进制	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	十进制	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	十进制	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	十进制	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	十进制	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	十进制	ThresholdExceeded:6
AllPortsUtilization	SINT	十进制	
PortFa1_1Utilization	SINT	十进制	
PortFa1_2Utilization	SINT	十进制	
PortFa1_3Utilization	SINT	十进制	
PortFa1_4Utilization	SINT	十进制	
PortFa1_5Utilization	SINT	十进制	
PortFa1_6Utilization	SINT	十进制	
MajorAlarmRelay	BOOL	十进制	AlarmRelay:0
MulticastGroupsActive	DINT	二进制	

模块定义的输出数据类型（6 端口交换机）

AB:STRATIX_5700_6PORT_MANAGED:0:0			
成员名称	类型	默认显示样式	有效值
AllPortsDisabled	BOOL	十进制	DisablePort:0
PortFa1_1Disable	BOOL	十进制	DisablePort:1
PortFa1_2Disable	BOOL	十进制	DisablePort:2
PortFa1_3Disable	BOOL	十进制	DisablePort:3
PortFa1_4Disable	BOOL	十进制	DisablePort:4
PortFa1_5Disable	BOOL	十进制	DisablePort:5
PortFa1_6Disable	BOOL	十进制	DisablePort:6

模块定义的输入数据类型（10 端口千兆交换机）

AB:STRATIX_5700_10PORT_GB_MANAGED:I:0			
成员名称	类型	默认显示样式	有效值
Fault	DINT	二进制	
AnyPortConnected	BOOL	十进制	LinkStatus:0
PortFa1_1Connected	BOOL	十进制	LinkStatus:1
PortFa1_2Connected	BOOL	十进制	LinkStatus:2
PortFa1_3Connected	BOOL	十进制	LinkStatus:3
PortFa1_4Connected	BOOL	十进制	LinkStatus:4
PortFa1_5Connected	BOOL	十进制	LinkStatus:5
PortFa1_6Connected	BOOL	十进制	LinkStatus:6
PortFa1_7Connected	BOOL	十进制	LinkStatus:7
PortFa1_8Connected	BOOL	十进制	LinkStatus:8
PortGi1_1Connected	BOOL	十进制	LinkStatus:9
PortGi1_2Connected	BOOL	十进制	LinkStatus:10
AnyPortUnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:8
PortGi1_1UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:9
PortGi1_2UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:10
AnyPortThreshold	BOOL	十进制	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	十进制	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	十进制	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	十进制	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	十进制	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	十进制	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	十进制	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	十进制	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	十进制	ThresholdExceeded:8
PortGi1_1Threshold	BOOL	十进制	ThresholdExceeded:9
PortGi1_2Threshold	BOOL	十进制	ThresholdExceeded:10

AB:STRATIX_5700_10PORT_GB_MANAGED:I:0			
成员名称	**类型**	**默认显示样式**	**有效值**
AllPortsUtilization	SINT	十进制	
PortFa1_1Utilization	SINT	十进制	
PortFa1_2Utilization	SINT	十进制	
PortFa1_3Utilization	SINT	十进制	
PortFa1_4Utilization	SINT	十进制	
PortFa1_5Utilization	SINT	十进制	
PortFa1_6Utilization	SINT	十进制	
PortFa1_7Utilization	SINT	十进制	
PortFa1_8Utilization	SINT	十进制	
PortGi1_1Utilization	SINT	十进制	
PortGi1_2Utilization	SINT	十进制	
MajorAlarmRelay	BOOL	十进制	AlarmRelay:0
MulticastGroupsActive	DINT	二进制	

模块定义的输出数据类型（10 端口千兆交换机）

AB:STRATIX_5700_10PORT_MANAGED:O:0			
成员名称	**类型**	**默认显示样式**	**有效值**
AllPortsDisabled	BOOL	十进制	DisablePort:0
PortFa1_1Disable	BOOL	十进制	DisablePort:1
PortFa1_2Disable	BOOL	十进制	DisablePort:2
PortFa1_3Disable	BOOL	十进制	DisablePort:3
PortFa1_4Disable	BOOL	十进制	DisablePort:4
PortFa1_5Disable	BOOL	十进制	DisablePort:5
PortFa1_6Disable	BOOL	十进制	DisablePort:6
PortFa1_7Disable	BOOL	十进制	DisablePort:7
PortFa1_8Disable	BOOL	十进制	DisablePort:8
PortGi1_1Disable	BOOL	十进制	DisablePort:9
PortGi1_2Disable	BOOL	十进制	DisablePort:10

模块定义的输入数据类型（10 端口交换机）

AB:STRATIX_5700_10PORT_MANAGED:I:0			
成员名称	**类型**	**默认显示样式**	**有效值**
Fault	DINT	二进制	
AnyPortConnected	BOOL	十进制	LinkStatus:0
PortFa1_1Connected	BOOL	十进制	LinkStatus:1
PortFa1_2Connected	BOOL	十进制	LinkStatus:2
PortFa1_3Connected	BOOL	十进制	LinkStatus:3
PortFa1_4Connected	BOOL	十进制	LinkStatus:4
PortFa1_5Connected	BOOL	十进制	LinkStatus:5
PortFa1_6Connected	BOOL	十进制	LinkStatus:6
PortFa1_7Connected	BOOL	十进制	LinkStatus:7
PortFa1_8Connected	BOOL	十进制	LinkStatus:8
PortFa1_9Connected	BOOL	十进制	LinkStatus:9
PortFa1_10Connected	BOOL	十进制	LinkStatus:10

AB:STRATIX_5700_10PORT_MANAGED:I:0			
成员名称	类型	默认显示样式	有效值
AnyPortUnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:8
PortFa1_9UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:9
PortFa1_10UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:10
AnyPortThreshold	BOOL	十进制	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	十进制	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	十进制	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	十进制	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	十进制	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	十进制	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	十进制	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	十进制	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	十进制	ThresholdExceeded:8
PortFa1_9Threshold	BOOL	十进制	ThresholdExceeded:9
PortFa1_10Threshold	BOOL	十进制	ThresholdExceeded:10
AllPortsUtilization	SINT	十进制	
PortFa1_1Utilization	SINT	十进制	
PortFa1_2Utilization	SINT	十进制	
PortFa1_3Utilization	SINT	十进制	
PortFa1_4Utilization	SINT	十进制	
PortFa1_5Utilization	SINT	十进制	
PortFa1_6Utilization	SINT	十进制	
PortFa1_7Utilization	SINT	十进制	
PortFa1_8Utilization	SINT	十进制	
PortFa1_9Utilization	SINT	十进制	
PortFa1_10Utilization	SINT	十进制	
MajorAlarmRelay	BOOL	十进制	AlarmRelay:0
MulticastGroupsActive	DINT	二进制	

模块定义的输出数据类型（10 端口交换机）

AB:STRATIX_5700_10PORT_MANAGED:O:0			
成员名称	类型	默认显示样式	有效值
AllPortsDisabled	BOOL	十进制	DisablePort:0
PortFa1_1Disable	BOOL	十进制	DisablePort:1
PortFa1_2Disable	BOOL	十进制	DisablePort:2
PortFa1_3Disable	BOOL	十进制	DisablePort:3
PortFa1_4Disable	BOOL	十进制	DisablePort:4
PortFa1_5Disable	BOOL	十进制	DisablePort:5

AB:STRATIX_5700_10PORT_MANAGED:O:0			
成员名称	**类型**	**默认显示样式**	**有效值**
PortFa1_6Disable	BOOL	十进制	DisablePort:6
PortFa1_7Disable	BOOL	十进制	DisablePort:7
PortFa1_8Disable	BOOL	十进制	DisablePort:8
PortFa1_9Disable	BOOL	十进制	DisablePort:9
PortFa1_10Disable	BOOL	十进制	DisablePort:10

模块定义的输入数据类型（20 端口千兆交换机）

AB:STRATIX_5700_20PORT_GB_MANAGED:I:0			
成员名称	**类型**	**默认显示样式**	**有效值**
Fault	DINT	二进制	
AnyPortConnected	BOOL	十进制	LinkStatus:0
PortFa1_1Connected	BOOL	十进制	LinkStatus:1
PortFa1_2Connected	BOOL	十进制	LinkStatus:2
PortFa1_3Connected	BOOL	十进制	LinkStatus:3
PortFa1_4Connected	BOOL	十进制	LinkStatus:4
PortFa1_5Connected	BOOL	十进制	LinkStatus:5
PortFa1_6Connected	BOOL	十进制	LinkStatus:6
PortFa1_7Connected	BOOL	十进制	LinkStatus:7
PortFa1_8Connected	BOOL	十进制	LinkStatus:8
PortFa1_9Connected	BOOL	十进制	LinkStatus:9
PortFa1_10Connected	BOOL	十进制	LinkStatus:10
PortFa1_11Connected	BOOL	十进制	LinkStatus:11
PortFa1_12Connected	BOOL	十进制	LinkStatus:12
PortFa1_13Connected	BOOL	十进制	LinkStatus:13
PortFa1_14Connected	BOOL	十进制	LinkStatus:14
PortFa1_15Connected	BOOL	十进制	LinkStatus:15
PortFa1_16Connected	BOOL	十进制	LinkStatus:16
PortFa1_17Connected	BOOL	十进制	LinkStatus:17
PortFa1_18Connected	BOOL	十进制	LinkStatus:18
PortGi1_1Connected	BOOL	十进制	LinkStatus:19
PortGi1_2Connected	BOOL	十进制	LinkStatus:20
AnyPortUnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:8
PortFa1_9UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:9
PortFa1_10UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:10
PortFa1_11UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:11
PortFa1_12UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:12
PortFa1_13UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:13

AB:STRATIX_5700_20PORT_GB_MANAGED:I:0			
成员名称	类型	默认显示样式	有效值
PortFa1_14UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:14
PortFa1_15UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:15
PortFa1_16UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:16
PortFa1_17UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:17
PortFa1_18UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:18
PortGi1_1UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:19
PortGi1_2UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:20
AnyPortThreshold	BOOL	十进制	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	十进制	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	十进制	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	十进制	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	十进制	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	十进制	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	十进制	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	十进制	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	十进制	ThresholdExceeded:8
PortFa1_9Threshold	BOOL	十进制	ThresholdExceeded:9
PortFa1_10Threshold	BOOL	十进制	ThresholdExceeded:10
PortFa1_11Threshold	BOOL	十进制	ThresholdExceeded:11
PortFa1_12Threshold	BOOL	十进制	ThresholdExceeded:12
PortFa1_13Threshold	BOOL	十进制	ThresholdExceeded:13
PortFa1_14Threshold	BOOL	十进制	ThresholdExceeded:14
PortFa1_15Threshold	BOOL	十进制	ThresholdExceeded:15
PortFa1_16Threshold	BOOL	十进制	ThresholdExceeded:16
PortFa1_17Threshold	BOOL	十进制	ThresholdExceeded:17
PortFa1_18Threshold	BOOL	十进制	ThresholdExceeded:18
PortGi1_1Threshold	BOOL	十进制	ThresholdExceeded:19
PortGi1_2Threshold	BOOL	十进制	ThresholdExceeded:20
AllPortsUtilization	SINT	十进制	
PortFa1_1Utilization	SINT	十进制	
PortFa1_2Utilization	SINT	十进制	
PortFa1_3Utilization	SINT	十进制	
PortFa1_4Utilization	SINT	十进制	
PortFa1_5Utilization	SINT	十进制	
PortFa1_6Utilization	SINT	十进制	
PortFa1_7Utilization	SINT	十进制	
PortFa1_8Utilization	SINT	十进制	
PortFa1_9Utilization	SINT	十进制	
PortFa1_10Utilization	SINT	十进制	
PortFa1_11Utilization	SINT	十进制	
PortFa1_12Utilization	SINT	十进制	
PortFa1_13Utilization	SINT	十进制	
PortFa1_14Utilization	SINT	十进制	
PortFa1_15Utilization	SINT	十进制	
PortFa1_16Utilization	SINT	十进制	
PortFa1_17Utilization	SINT	十进制	

AB:STRATIX_5700_20PORT_GB_MANAGED:I:0			
成员名称	**类型**	**默认显示样式**	**有效值**
PortFa1_18Utilization	SINT	十进制	
PortGi1_1Utilization	SINT	十进制	
PortGi1_2Utilization	SINT	十进制	
MajorAlarmRelay	BOOL	十进制	AlarmRelay:0
MulticastGroupsActive	DINT	二进制	

模块定义的输入数据类型（18 端口千兆交换机）

AB:STRATIX_5700_18PORT_GB_MANAGED:I:0			
成员名称	**类型**	**默认显示样式**	**有效值**
Fault	DINT	二进制	
AnyPortConnected	BOOL	十进制	LinkStatus:0
PortFa1_1Connected	BOOL	十进制	LinkStatus:1
PortFa1_2Connected	BOOL	十进制	LinkStatus:2
PortFa1_3Connected	BOOL	十进制	LinkStatus:3
PortFa1_4Connected	BOOL	十进制	LinkStatus:4
PortFa1_5Connected	BOOL	十进制	LinkStatus:5
PortFa1_6Connected	BOOL	十进制	LinkStatus:6
PortFa1_7Connected	BOOL	十进制	LinkStatus:7
PortFa1_8Connected	BOOL	十进制	LinkStatus:8
PortFa1_9Connected	BOOL	十进制	LinkStatus:9
PortFa1_10Connected	BOOL	十进制	LinkStatus:10
PortFa1_11Connected	BOOL	十进制	LinkStatus:11
PortFa1_12Connected	BOOL	十进制	LinkStatus:12
PortFa1_13Connected	BOOL	十进制	LinkStatus:13
PortFa1_14Connected	BOOL	十进制	LinkStatus:14
PortFa1_15Connected	BOOL	十进制	LinkStatus:15
PortFa1_16Connected	BOOL	十进制	LinkStatus:16
PortGi1_1Connected	BOOL	十进制	LinkStatus:19
PortGi1_2Connected	BOOL	十进制	LinkStatus:20
AnyPortUnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:8
PortFa1_9UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:9
PortFa1_10UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:10
PortFa1_11UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:11
PortFa1_12UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:12
PortFa1_13UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:13
PortFa1_14UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:14
PortFa1_15UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:15

AB:STRATIX_5700_18PORT_GB_MANAGED:I:0			
成员名称	类型	默认显示样式	有效值
PortFa1_16UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:16
PortGi1_1UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:19
PortGi1_2UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:20
AnyPortThreshold	BOOL	十进制	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	十进制	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	十进制	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	十进制	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	十进制	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	十进制	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	十进制	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	十进制	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	十进制	ThresholdExceeded:8
PortFa1_9Threshold	BOOL	十进制	ThresholdExceeded:9
PortFa1_10Threshold	BOOL	十进制	ThresholdExceeded:10
PortFa1_11Threshold	BOOL	十进制	ThresholdExceeded:11
PortFa1_12Threshold	BOOL	十进制	ThresholdExceeded:12
PortFa1_13Threshold	BOOL	十进制	ThresholdExceeded:13
PortFa1_14Threshold	BOOL	十进制	ThresholdExceeded:14
PortFa1_15Threshold	BOOL	十进制	ThresholdExceeded:15
PortFa1_16Threshold	BOOL	十进制	ThresholdExceeded:16
PortGi1_1Threshold	BOOL	十进制	ThresholdExceeded:19
PortGi1_2Threshold	BOOL	十进制	ThresholdExceeded:20
AllPortsUtilization	SINT	十进制	
PortFa1_1Utilization	SINT	十进制	
PortFa1_2Utilization	SINT	十进制	
PortFa1_3Utilization	SINT	十进制	
PortFa1_4Utilization	SINT	十进制	
PortFa1_5Utilization	SINT	十进制	
PortFa1_6Utilization	SINT	十进制	
PortFa1_7Utilization	SINT	十进制	
PortFa1_8Utilization	SINT	十进制	
PortFa1_9Utilization	SINT	十进制	
PortFa1_10Utilization	SINT	十进制	
PortFa1_11Utilization	SINT	十进制	
PortFa1_12Utilization	SINT	十进制	
PortFa1_13Utilization	SINT	十进制	
PortFa1_14Utilization	SINT	十进制	
PortFa1_15Utilization	SINT	十进制	
PortFa1_16Utilization	SINT	十进制	
PortGi1_1Utilization	SINT	十进制	
PortGi1_2Utilization	SINT	十进制	
MajorAlarmRelay	BOOL	十进制	AlarmRelay:0
MulticastGroupsActive	DINT	二进制	

模块定义的输出数据类型（18 端口千兆交换机）

AB:STRATIX_5700_20PORT_GB_MANAGED:O:0			
成员名称	**类型**	**默认显示样式**	**有效值**
AllPortsDisabled	BOOL	十进制	DisablePort:0
PortFa1_1Disable	BOOL	十进制	DisablePort:1
PortFa1_2Disable	BOOL	十进制	DisablePort:2
PortFa1_3Disable	BOOL	十进制	DisablePort:3
PortFa1_4Disable	BOOL	十进制	DisablePort:4
PortFa1_5Disable	BOOL	十进制	DisablePort:5
PortFa1_6Disable	BOOL	十进制	DisablePort:6
PortFa1_7Disable	BOOL	十进制	DisablePort:7
PortFa1_8Disable	BOOL	十进制	DisablePort:8
PortFa1_9Disable	BOOL	十进制	DisablePort:9
PortFa1_10Disable	BOOL	十进制	DisablePort:10
PortFa1_11Disable	BOOL	十进制	DisablePort:11
PortFa1_12Disable	BOOL	十进制	DisablePort:12
PortFa1_13Disable	BOOL	十进制	DisablePort:13
PortFa1_14Disable	BOOL	十进制	DisablePort:14
PortFa1_15Disable	BOOL	十进制	DisablePort:15
PortFa1_16Disable	BOOL	十进制	DisablePort:16
PortGi1_1Disable	BOOL	十进制	DisablePort:19
PortGi1_2Disable	BOOL	十进制	DisablePort:20

模块定义的输入数据类型（20 端口千兆交换机）

AB:STRATIX_5700_20PORT_GB_MANAGED:I:0			
成员名称	**类型**	**默认显示样式**	**有效值**
Fault	DINT	二进制	
AnyPortConnected	BOOL	十进制	LinkStatus:0
PortFa1_1Connected	BOOL	十进制	LinkStatus:1
PortFa1_2Connected	BOOL	十进制	LinkStatus:2
PortFa1_3Connected	BOOL	十进制	LinkStatus:3
PortFa1_4Connected	BOOL	十进制	LinkStatus:4
PortFa1_5Connected	BOOL	十进制	LinkStatus:5
PortFa1_6Connected	BOOL	十进制	LinkStatus:6
PortFa1_7Connected	BOOL	十进制	LinkStatus:7
PortFa1_8Connected	BOOL	十进制	LinkStatus:8
PortFa1_9Connected	BOOL	十进制	LinkStatus:9
PortFa1_10Connected	BOOL	十进制	LinkStatus:10
PortFa1_11Connected	BOOL	十进制	LinkStatus:11
PortFa1_12Connected	BOOL	十进制	LinkStatus:12
PortFa1_13Connected	BOOL	十进制	LinkStatus:13
PortFa1_14Connected	BOOL	十进制	LinkStatus:14
PortFa1_15Connected	BOOL	十进制	LinkStatus:15
PortFa1_16Connected	BOOL	十进制	LinkStatus:16
PortFa1_17Connected	BOOL	十进制	LinkStatus:17
PortFa1_18Connected	BOOL	十进制	LinkStatus:18
PortGi1_1Connected	BOOL	十进制	LinkStatus:19

AB:STRATIX_5700_20PORT_GB_MANAGED:I:0			
成员名称	类型	默认显示样式	有效值
PortGi1_2Connected	BOOL	十进制	LinkStatus:20
AnyPortUnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:8
PortFa1_9UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:9
PortFa1_10UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:10
PortFa1_11UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:11
PortFa1_12UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:12
PortFa1_13UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:13
PortFa1_14UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:14
PortFa1_15UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:15
PortFa1_16UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:16
PortFa1_17UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:17
PortFa1_18UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:18
PortGi1_1UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:19
PortGi1_2UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:20
AnyPortThreshold	BOOL	十进制	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	十进制	ThresholdExceeded:1
PortFa1_2Threshold	BOOL	十进制	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	十进制	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	十进制	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	十进制	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	十进制	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	十进制	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	十进制	ThresholdExceeded:8
PortFa1_9Threshold	BOOL	十进制	ThresholdExceeded:9
PortFa1_10Threshold	BOOL	十进制	ThresholdExceeded:10
PortFa1_11Threshold	BOOL	十进制	ThresholdExceeded:11
PortFa1_12Threshold	BOOL	十进制	ThresholdExceeded:12
PortFa1_13Threshold	BOOL	十进制	ThresholdExceeded:13
PortFa1_14Threshold	BOOL	十进制	ThresholdExceeded:14
PortFa1_15Threshold	BOOL	十进制	ThresholdExceeded:15
PortFa1_16Threshold	BOOL	十进制	ThresholdExceeded:16
PortFa1_17Threshold	BOOL	十进制	ThresholdExceeded:17
PortFa1_18Threshold	BOOL	十进制	ThresholdExceeded:18
PortGi1_1Threshold	BOOL	十进制	ThresholdExceeded:19
PortGi1_2Threshold	BOOL	十进制	ThresholdExceeded:20
AllPortsUtilization	SINT	十进制	
PortFa1_1Utilization	SINT	十进制	
PortFa1_2Utilization	SINT	十进制	

AB:STRATIX_5700_20PORT_GB_MANAGED:I:0			
成员名称	**类型**	**默认显示样式**	**有效值**
PortFa1_3Utilization	SINT	十进制	
PortFa1_4Utilization	SINT	十进制	
PortFa1_5Utilization	SINT	十进制	
PortFa1_6Utilization	SINT	十进制	
PortFa1_7Utilization	SINT	十进制	
PortFa1_8Utilization	SINT	十进制	
PortFa1_9Utilization	SINT	十进制	
PortFa1_10Utilization	SINT	十进制	
PortFa1_11Utilization	SINT	十进制	
PortFa1_12Utilization	SINT	十进制	
PortFa1_13Utilization	SINT	十进制	
PortFa1_14Utilization	SINT	十进制	
PortFa1_15Utilization	SINT	十进制	
PortFa1_16Utilization	SINT	十进制	
PortFa1_17Utilization	SINT	十进制	
PortFa1_18Utilization	SINT	十进制	
PortGi1_1Utilization	SINT	十进制	
PortGi1_2Utilization	SINT	十进制	
MajorAlarmRelay	BOOL	十进制	AlarmRelay:0
MulticastGroupsActive	DINT	二进制	

模块定义的输出数据类型（20 端口千兆交换机）

AB:STRATIX_5700_20PORT_GB_MANAGED:O:0			
成员名称	**类型**	**默认显示样式**	**有效值**
AllPortsDisabled	BOOL	十进制	DisablePort:0
PortFa1_1Disable	BOOL	十进制	DisablePort:1
PortFa1_2Disable	BOOL	十进制	DisablePort:2
PortFa1_3Disable	BOOL	十进制	DisablePort:3
PortFa1_4Disable	BOOL	十进制	DisablePort:4
PortFa1_5Disable	BOOL	十进制	DisablePort:5
PortFa1_6Disable	BOOL	十进制	DisablePort:6
PortFa1_7Disable	BOOL	十进制	DisablePort:7
PortFa1_8Disable	BOOL	十进制	DisablePort:8
PortFa1_9Disable	BOOL	十进制	DisablePort:9
PortFa1_10Disable	BOOL	十进制	DisablePort:10
PortFa1_11Disable	BOOL	十进制	DisablePort:11
PortFa1_12Disable	BOOL	十进制	DisablePort:12
PortFa1_13Disable	BOOL	十进制	DisablePort:13
PortFa1_14Disable	BOOL	十进制	DisablePort:14
PortFa1_15Disable	BOOL	十进制	DisablePort:15
PortFa1_16Disable	BOOL	十进制	DisablePort:16
PortFa1_17Disable	BOOL	十进制	DisablePort:17
PortFa1_18Disable	BOOL	十进制	DisablePort:18
PortGi1_1Disable	BOOL	十进制	DisablePort:19
PortGi1_2Disable	BOOL	十进制	DisablePort:20

模块定义的输入数据类型（20 端口交换机）

AB:STRATIX_5700_20PORT_MANAGED:I:0			
成员名称	类型	默认显示样式	有效值
Fault	DINT	二进制	
AnyPortConnected	BOOL	十进制	LinkStatus:0
PortFa1_1Connected	BOOL	十进制	LinkStatus:1
PortFa1_2Connected	BOOL	十进制	LinkStatus:2
PortFa1_3Connected	BOOL	十进制	LinkStatus:3
PortFa1_4Connected	BOOL	十进制	LinkStatus:4
PortFa1_5Connected	BOOL	十进制	LinkStatus:5
PortFa1_6Connected	BOOL	十进制	LinkStatus:6
PortFa1_7Connected	BOOL	十进制	LinkStatus:7
PortFa1_8Connected	BOOL	十进制	LinkStatus:8
PortFa1_9Connected	BOOL	十进制	LinkStatus:9
PortFa1_10Connected	BOOL	十进制	LinkStatus:10
PortFa1_11Connected	BOOL	十进制	LinkStatus:11
PortFa1_12Connected	BOOL	十进制	LinkStatus:12
PortFa1_13Connected	BOOL	十进制	LinkStatus:13
PortFa1_14Connected	BOOL	十进制	LinkStatus:14
PortFa1_15Connected	BOOL	十进制	LinkStatus:15
PortFa1_16Connected	BOOL	十进制	LinkStatus:16
PortFa1_17Connected	BOOL	十进制	LinkStatus:17
PortFa1_18Connected	BOOL	十进制	LinkStatus:18
PortFa1_19Connected	BOOL	十进制	LinkStatus:19
PortFa1_20Connected	BOOL	十进制	LinkStatus:20
AnyPortUnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:0
PortFa1_1UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:1
PortFa1_2UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:2
PortFa1_3UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:3
PortFa1_4UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:4
PortFa1_5UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:5
PortFa1_6UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:6
PortFa1_7UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:7
PortFa1_8UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:8
PortFa1_9UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:9
PortFa1_10UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:10
PortFa1_11UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:11
PortFa1_12UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:12
PortFa1_13UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:13
PortFa1_14UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:14
PortFa1_15UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:15
PortFa1_16UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:16
PortFa1_17UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:17
PortFa1_18UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:18
PortFa1_19UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:19
PortFa1_20UnauthorizedDevice	BOOL	十进制	UnauthorizedDevice:20
AnyPortThreshold	BOOL	十进制	ThresholdExceeded:0
PortFa1_1Threshold	BOOL	十进制	ThresholdExceeded:1

AB:STRATIX_5700_20PORT_MANAGED:I:0			
成员名称	**类型**	**默认显示样式**	**有效值**
PortFa1_2Threshold	BOOL	十进制	ThresholdExceeded:2
PortFa1_3Threshold	BOOL	十进制	ThresholdExceeded:3
PortFa1_4Threshold	BOOL	十进制	ThresholdExceeded:4
PortFa1_5Threshold	BOOL	十进制	ThresholdExceeded:5
PortFa1_6Threshold	BOOL	十进制	ThresholdExceeded:6
PortFa1_7Threshold	BOOL	十进制	ThresholdExceeded:7
PortFa1_8Threshold	BOOL	十进制	ThresholdExceeded:8
PortFa1_9Threshold	BOOL	十进制	ThresholdExceeded:9
PortFa1_10Threshold	BOOL	十进制	ThresholdExceeded:10
PortFa1_11Threshold	BOOL	十进制	ThresholdExceeded:11
PortFa1_12Threshold	BOOL	十进制	ThresholdExceeded:12
PortFa1_13Threshold	BOOL	十进制	ThresholdExceeded:13
PortFa1_14Threshold	BOOL	十进制	ThresholdExceeded:14
PortFa1_15Threshold	BOOL	十进制	ThresholdExceeded:15
PortFa1_16Threshold	BOOL	十进制	ThresholdExceeded:16
PortFa1_17Threshold	BOOL	十进制	ThresholdExceeded:17
PortFa1_18Threshold	BOOL	十进制	ThresholdExceeded:18
PortFa1_19Threshold	BOOL	十进制	ThresholdExceeded:19
PortFa1_20Threshold	BOOL	十进制	ThresholdExceeded:20
AllPortsUtilization	SINT	十进制	
PortFa1_1Utilization	SINT	十进制	
PortFa1_2Utilization	SINT	十进制	
PortFa1_3Utilization	SINT	十进制	
PortFa1_4Utilization	SINT	十进制	
PortFa1_5Utilization	SINT	十进制	
PortFa1_6Utilization	SINT	十进制	
PortFa1_7Utilization	SINT	十进制	
PortFa1_8Utilization	SINT	十进制	
PortFa1_9Utilization	SINT	十进制	
PortFa1_10Utilization	SINT	十进制	
PortFa1_11Utilization	SINT	十进制	
PortFa1_12Utilization	SINT	十进制	
PortFa1_13Utilization	SINT	十进制	
PortFa1_14Utilization	SINT	十进制	
PortFa1_15Utilization	SINT	十进制	
PortFa1_16Utilization	SINT	十进制	
PortFa1_17Utilization	SINT	十进制	
PortFa1_18Utilization	SINT	十进制	
PortFa1_19Utilization	SINT	十进制	
PortFa1_20Utilization	SINT	十进制	
MajorAlarmRelay	BOOL	十进制	AlarmRelay:0
MulticastGroupsActive	DINT	二进制	

模块定义的输出数据类型（20 端口交换机）

AB:STRATIX_5700_20PORT_MANAGED:0:0			
成员名称	类型	默认显示样式	有效值
AllPortsDisabled	BOOL	十进制	DisablePort:0
PortFa1_1Disable	BOOL	十进制	DisablePort:1
PortFa1_2Disable	BOOL	十进制	DisablePort:2
PortFa1_3Disable	BOOL	十进制	DisablePort:3
PortFa1_4Disable	BOOL	十进制	DisablePort:4
PortFa1_5Disable	BOOL	十进制	DisablePort:5
PortFa1_6Disable	BOOL	十进制	DisablePort:6
PortFa1_7Disable	BOOL	十进制	DisablePort:7
PortFa1_8Disable	BOOL	十进制	DisablePort:8
PortFa1_9Disable	BOOL	十进制	DisablePort:9
PortFa1_10Disable	BOOL	十进制	DisablePort:10
PortFa1_11Disable	BOOL	十进制	DisablePort:11
PortFa1_12Disable	BOOL	十进制	DisablePort:12
PortFa1_13Disable	BOOL	十进制	DisablePort:13
PortFa1_14Disable	BOOL	十进制	DisablePort:14
PortFa1_15Disable	BOOL	十进制	DisablePort:15
PortFa1_16Disable	BOOL	十进制	DisablePort:16
PortFa1_17Disable	BOOL	十进制	DisablePort:17
PortFa1_18Disable	BOOL	十进制	DisablePort:18
PortFa1_19Disable	BOOL	十进制	DisablePort:19
PortFa1_20Disable	BOOL	十进制	DisablePort:20

CIP 数据的端口分配

下表指明了与交换机各端口关联的以太网链路对象的实例编号。实例 0 并不像在位映射中那样对所有端口都适用。

所有端口组成的结构中（例如，输出组件中）的各个位编号用于标识每个端口。位 0 代表任何或所有端口。

实例 / 位	6 端口交换机	6 端口千兆交换机	10 端口交换机	10 端口千兆交换机	18 端口千兆交换机	20 端口交换机	20 端口千兆交换机
位 0	任何 / 所有端口	任何 / 所有端口	任何 / 所有端口	任何 / 所有端口	任何 / 所有端口	任何 / 所有端口	任何 / 所有端口
实例 / 位 1	Fa1/1	Fa/1	Fa1/1	Fa1/1	Fa1/1	Fa1/1	Fa1/1
实例 / 位 2	Fa1/2	Fa1/2	Fa1/2	Fa1/2	Fa1/2	Fa1/2	Fa1/2
实例 / 位 3	Fa1/3	Fa1/3	Fa1/3	Fa1/3	Fa1/3	Fa1/3	Fa1/3
实例 / 位 4	Fa1/4	Fa1/4	Fa1/4	Fa1/4	Fa1/4	Fa1/4	Fa1/4
实例 / 位 5	Fa1/5	Gi1/1	Fa1/5	Fa1/5	Fa1/5	Fa1/5	Fa1/5
实例 / 位 6	Fa1/6	Gi1/2	Fa1/6	Fa1/6	Fa1/6	Fa1/6	Fa1/6
实例 / 位 7			Fa1/7	Fa1/7	Fa1/7	Fa1/7	Fa1/7
实例 / 位 8			Fa1/8	Fa1/8	Fa1/8	Fa1/8	Fa1/8
实例 / 位 9			Fa1/9	Gi1/1	Fa1/9	Fa1/9	Fa1/9
实例 / 位 10			Fa1/10	Gi1/2	Fa1/10	Fa1/10	Fa1/10
实例 / 位 11					Fa1/11	Fa1/11	Fa1/11
实例 / 位 12					Fa1/12	Fa1/12	Fa1/12
实例 / 位 13					Fa1/13	Fa1/13	Fa1/13
实例 / 位 14					Fa1/14	Fa1/14	Fa1/14
实例 / 位 15					Fa1/15	Fa1/15	Fa1/15
实例 / 位 16					Fa1/16	Fa1/16	Fa1/16
实例 / 位 17						Fa1/17	Fa1/17
实例 / 位 18						Fa1/18	Fa1/18
实例 / 位 19					Gi1/1	Fa1/19	Gi1/1
实例 / 位 20					Gi1/2	Fa1/20	Gi1/2
实例 / 位 27	SVI1	SVI1	SVI1	SVI1	SVI1	SVI1	SVI1

注：

电缆和连接器

10/100 和 10/100/1000 端口

交换机上的 10/100 和 10/100/1000 以太网端口使用标准 RJ45 连接器和以太网引脚进行内部交叉。

提示 **自动 MDIX 功能在默认情况下处于启用状态。**

图 10 - 10/100 连接器引脚分布

引脚	标签
1	RD+
2	RD-
3	TD+
4	NC
5	NC
6	TD-
7	NC
8	NC

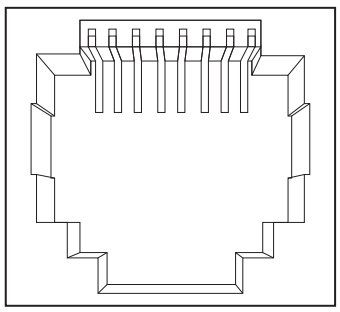
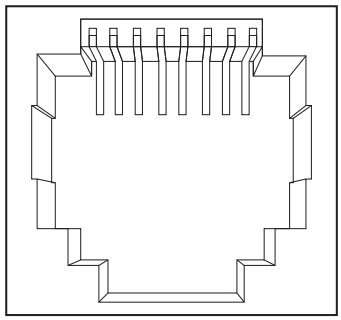


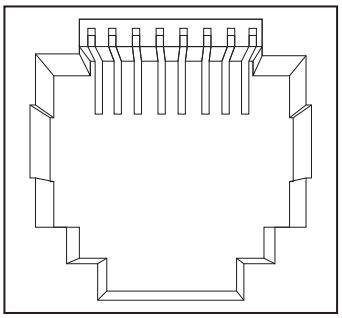
图 11 - 10/100/1000 连接器引脚分布

引脚	标签
1	TP0+
2	TP0-
3	TP1+
4	TP2+
5	TP2-
6	TP1-
7	TP3+
8	TP3-



PoE 端口可将电源信号和数据信号集成到相同的导线上。端口使用标准 RJ45 连接器和以太网引脚进行内部交叉。

图 12 - 10/100 PoE 连接器引脚分布和电源供应设备 (PSE) 电压

引脚	标签	替代 A (MDI)	1 2 3 4 5 6 7 8
1	RD+	正极 V PSE	
2	RD-	正极 V PSE	
3	TD+	负极 V PSE	
4	NC		
5	NC		
6	TD-	负极 V PSE	
7	NC		
8	NC		

连接到 10BASE-T 和 100BASE-TX 兼容设备

自动 MDIX 功能在默认情况下处于启用状态。当自动 MDIX 功能已禁用时，请遵循下述接线准则。

将端口连接到 10BASE-T 和 100BASE-TX 兼容设备（例如服务器、工作站和路由器）时，可使用符合 10BASE-T 和 100BASE-TX 接线标准的具有两对或四对双绞线的直通电缆。

要识别交叉电缆，可以对电缆的两个模块化末端进行比较。拿住电缆两端并排放置，使标签朝后。左插头外部引脚所连接的电线颜色必须与右插头内部引脚所连接的电线颜色不同。

下面几个图展现的是这两种电缆的示意图：

- 具有两对双绞线的直通电缆
- 具有四对双绞线的直通电缆

图 13 - 具有两对双绞线的直通电缆示意图

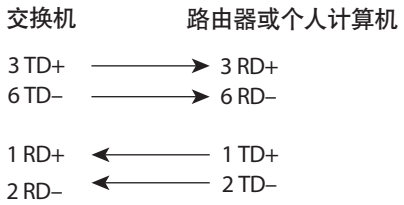
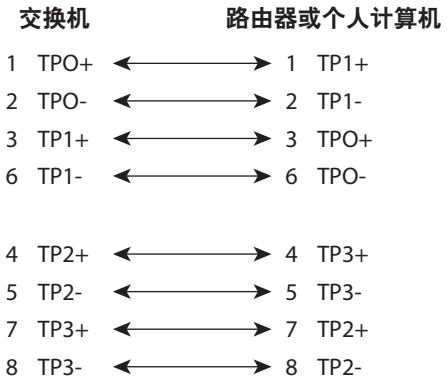


图 14 - 具有四对双绞线的直通电缆示意图



将端口连接到 10BASE-T 和 100BASE-TX 兼容设备 （例如交换机或中继器）时，可使用具有两对或四对双绞线的交叉电缆。

下面几个图展现的是这两种电缆的示意图：

- 具有两对双绞线的交叉电缆示意图
- 具有四对双绞线的交叉电缆示意图

在连接两个端口时，只有在其中一个端口被指定为 X 时，才可使用直通电缆进行连接。如果两个端口都被指定为 X，或两个端口均没有被指定为 X，则使用交叉电缆进行连接。

连接 10BASE-T 兼容设备时，可使用 3 类、4 类或 5 类电缆。连接 100BASE-TX 兼容设备时，必须使用 5 类电缆。

重要信息 **当连接 1000BASE-T 兼容设备或 PoE 时，请使用具有四对双绞线的 5 类电缆。**

图 15 - 具有两对双绞线的交叉电缆示意图

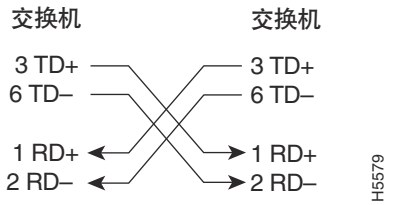
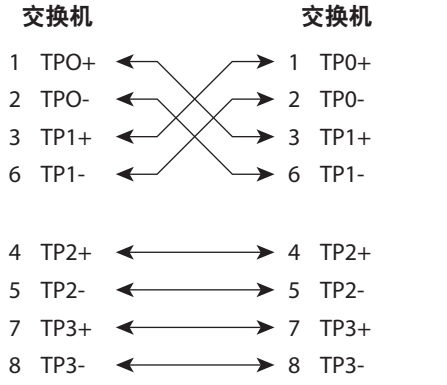


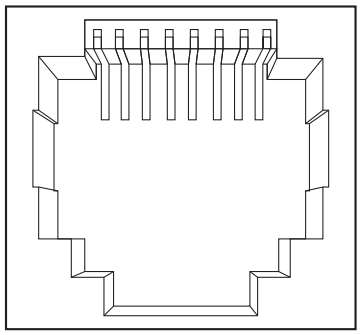
图 16 - 具有四对双绞线的交叉电缆示意图



两用端口（组合端口）

两用端口上的以太网端口使用标准 RJ45 连接器。下图显示了引脚分布。

图 17 - 以太网端口 RJ45 连接器

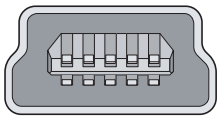
引脚	标签	1 2 3 4 5 6 7 8
1	TP0+	
2	TP0-	
3	TP1+	
4	TP2+	
5	TP2-	
6	TP1-	
7	TP3+	
8	TP3-	

两用端口上的 SFP 模块插槽使用 SFP 模块来配置光缆端口。

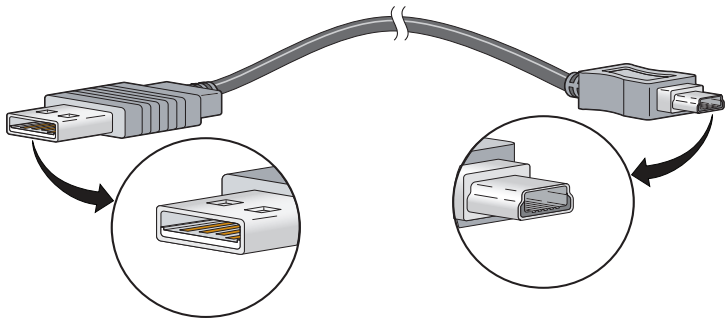
重要信息　**自动 MDIX 功能在默认情况下处于启用状态。有关此功能的配置信息，请参见交换机软件配置指南或交换机命令参考。**

控制台端口

交换机具有两个控制台端口：一个是前面板上的 USB 5 引脚小型 B 类端口，另一个是后面板上的 RJ45 控制台端口。但一次仅一个控制台端口可处于激活状态。

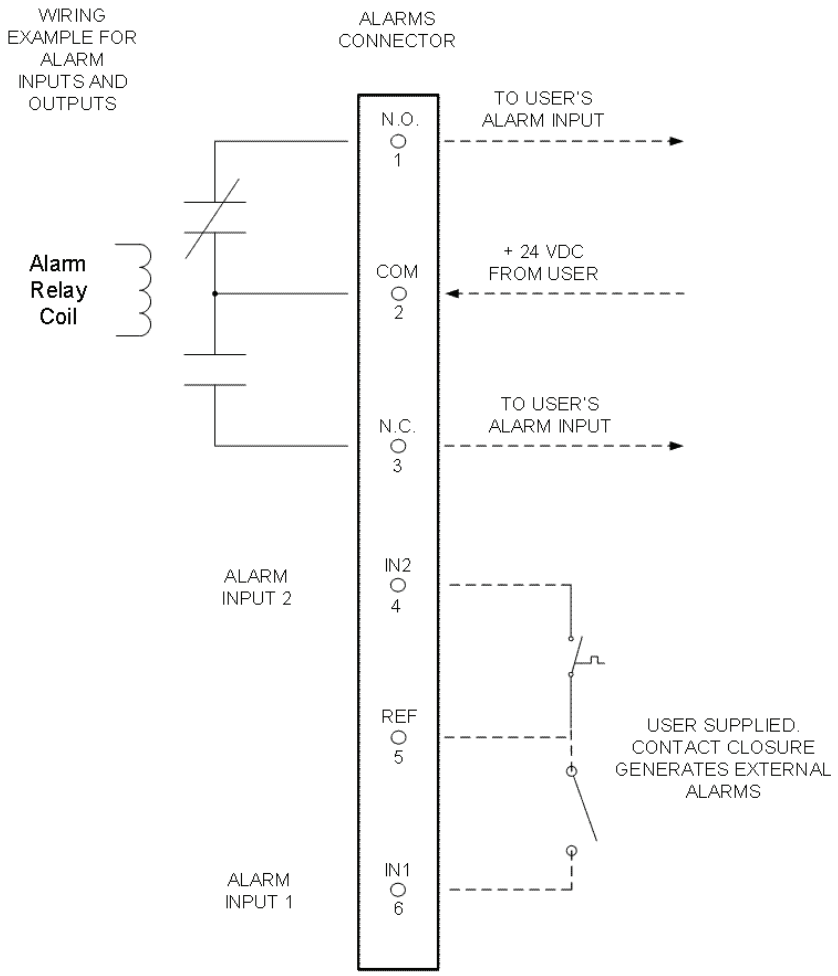


USB 控制台端口使用 USB A 类转 5 引脚小型 B 类电缆。不提供 USB A 类转 USB 小型 B 类电缆。



报警端口

下面的图和表介绍了前面板报警继电器连接器端口。



标签	连接
NO	报警输出常开 (NO) 连接
COM	报警输出公共端连接
NC	报警输出常闭 (NC) 连接
IN2	报警输入 2
REF	报警输入参考接地连接
IN1	报警输入 1

电缆和适配器规格

以下各节将介绍交换机使用的电缆和适配器。

SFP 模块电缆规格

下面列出了耐用光纤 SFP 模块连接所使用的电缆规格。每个端口与电缆另一端的波长规格必须匹配，为确保可靠的通信，电缆长度不能超出额定的最大长度。

表 46 - 光纤 SFP 模块端口电缆规格

SFP 模块类型	目录号	波长 (nm)	光纤类型	纤芯尺寸 / 包层尺寸 （微米）	模态带宽 (MHz/km)(1)	电缆距离
100BASE-FX	1783-SFP100FX	1310	MMF	50/125 62.5/125	500 500	2 km (6562 ft) 2 km (6562 ft)
100BASE-LX	1783-SFP100LX	1310	SMF	G.652[2]	—	10 km (32,810 ft)
1000BASE-SX	1783-SFP1GSX	850	MMF	62.5/125 62.5/125 50/125 50/125	160 200 400 500	220 m (722 ft) 275 m (902 ft) 500 m (1640 ft) 550 m (1804 ft)
1000BASE-LX/LH	1783-SFP1GLX	1310	SMF	G.652[2]	—	10 km (32,810 ft)

(1) 模态带宽仅适用于多模光纤。

PoE 端口电缆规格

对于 PoE 端口，可使用 5 类电缆，距离最远达 100 m (328 ft)。

适配器引脚分布

下表列出了控制台端口、 RJ45 转 DB-9 适配器电缆和控制台设备的引脚分布。

表 47 - DB-9 引脚的引脚分配

交换机控制台端口 (DTE)	RJ45 转 DB-9 终端适配器	控制台设备
信号	DB-9 引脚	信号
RTS	8	CTS
DTR	6	DSR
TxD	2	RxD
GND	5	GND
GND	5	GND
RxD	3	TxD
DSR	4	DTR
CTS	7	RTS

下表列出了控制台端口、RJ45 转 DB-25 母头 DTE 适配器和控制台设备的引脚分布。交换机未附带 RJ45 转 DB-25 母头 DTE 适配器。

表 48 - DB-25 引脚的引脚分配

交换机控制台端口 (DTE)	RJ45 转 DB-25 终端适配器	控制台设备
信号	DB-25 引脚	信号
RTS	5	CTS
DTR	6	DSR
TxD	3	RxD
GND	7	GND
GND	7	GND
RxD	2	TxD
DSR	20	DTR
CTS	4	RTS

变更记录

本附录汇总了本手册的各个版本。如果您需要获取信息用于确定已对不同版本做出哪些更改，请参见本附录。如果您需要根据本手册之前版本所增加的信息升级硬件或软件，本附录将特别有用。

1783-UM004C-ZH-P，2013 年 12 月

变更
访问产品版本说明
以太网供电 (PoE) 交换机介绍
PoE 交换机尺寸
PoE 端口说明
用于连接外部接地螺丝的 AWG 线规
连接 PoE 电源
连接 PoE 电源连接器
连接至 PoE 端口
快速设置与 SD 卡
PoE 交换机上的端口编号
PoE 特性介绍
通过设备管理器 Web 界面配置 PoE
PoE 端口连接器引脚分布和电缆规格

1783-UM004B-ZH-P，2013 年 6 月

变更
Studio 5000 Logix 设计器应用程序是 RSLogix 5000 软件的换代产品
1783-BMS10CGN 和 1783-BMS20CGN 交换机介绍
网络地址转换 (NAT) 软件功能
1783-BMS10CGN 和 1783-BMS20CGN 交换机的端口编号
NAT 概述
通过设备管理器 Web 界面配置 NAT
通过设备管理器 Web 界面监视 NAT 统计信息
通过 Logix 设计器应用程序配置 NAT
通过 Logix 设计器应用程序监视 NAT 诊断

注：

数字

英文

J

K

L

M

Q

R

S

T

W

Y

Z

罗克韦尔自动化支持

罗克韦尔自动化在网站上提供技术信息，以帮助您使用我们的产品。
访问 http://www.rockwellautomation.com/support，可找到技术和应用说明、示例代码与软件服务包链接。也可访问支持中心 https://rockwellautomation.custhelp.com/ 获取软件更新，查找支持对话与支持论坛、技术信息、FAQ，并登记参与产品通知更新。

此外，我们还提供多种安装、配置和故障处理支持计划。有关详细信息，请与本地分销商或罗克韦尔自动化销售代表联系，或者访问 http://www.rockwellautomation.com/services/online-phone。

安装协助

如果您在安装后的最初 24 小时内遇到问题，请查阅本手册中包含的信息。您可以联系客户支持来获取首次帮助，以协助您安装好产品并完成试运行。

美国或加拿大	1.440.646.3434
美国或加拿大以外地区	**使用 http://www.rockwellautomation.com/rockwellautomation/support/overview.page 上的 Worldwide Locator，或联系当地的罗克韦尔自动化代表。**

新产品退货

在所有产品出厂前，罗克韦尔自动化公司都会进行测试，以确保产品完全可用。但是，如果您的产品不能正常工作需要退货，请遵循下列步骤。

美国	**请联系您的分销商。必须向分销商提供客户支持案例号码（可拨打以上电话号码获取）才能完成退货流程。**
美国以外地区	**请联系您当地的罗克韦尔自动化代表，了解退货程序。**

文档反馈

您的意见将帮助我们更好地满足您的文档需求。若有任何关于如何改进本文档的建议，
请填写 http://www.rockwellautomation.com/literature/ 上提供的表格，出版物 RA-DU002。

罗克韦尔自动化在其网站：http://www.rockwellautomation.com/rockwellautomation/about-us/sustainability-ethics/product-environmental-compliance.page 上维护最新的产品环境信息。

中文网址 **www.rockwellautomation.com.cn**
新浪微博 **www.weibo.com/rockwellchina**

动力、控制与信息解决方案总部
美洲地区：罗克韦尔自动化，南二大街1201号，密尔沃基市，WI 53204-2496 美国，电话：(1) 414.382.2000，传真：(1) 414.382.4444
欧洲/中东/非洲：罗克韦尔自动化，NV, Pegasus Park, De Kleetlaan 12a, 1831布鲁塞尔，比利时，电话：(32) 2 663 0600, 传真：(32) 2 663 0640
亚太地区：罗克韦尔自动化，香港数码港道100号数码港3座F区14楼1401-1403 电话：(852)2887 4788 传真：(852)2508 1486
中国总部：上海市徐汇区虹梅路1801号宏业大厦 邮编：200233 电话：(86 21)6128 8888 传真：(86 21)6128 8899
客户服务电话：400 620 6620 (中国地区)　　+852 2887 4666 (香港地区)

出版物 1783-UM004D-ZH-P - 2014 年 3 月