Modicon

MCSESM, MCSESM-E, MCSESP 管理型交换机
组态用户手册

QGH59083.02

www.schneider-electric.com

Schneider Electric

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

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

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

当设备用于具有技术安全要求的应用场合时，必须遵守有关的使用说明。

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

不遵守此信息可能导致人身伤害或设备损坏。

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

目录

安全提示

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

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

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

⚠ 危险

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

⚠ 警告

警告 提示请注意可能发生的危险，如未避免会造成死亡或重伤 **的后果**。

⚠ 小心

小心 提示请注意可能发生的危险，如未避免会造成轻伤**的后果**。

提示

提示 提供能避免受伤的工作方法。

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

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

关于本手册

适用范围

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

用户意见

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

更多文档

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

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

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

“命令行界面”参考手册包含了关于使用命令行界面操作设备各种功能的详细信息。

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

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

重要说明

本手册中使用的图标具有以下含义：

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

图形用户界面中的执行

命令行界面中的执行

更换设备

该设备提供以下即插即用解决方案，用于用相同类型的设备更换设备，例如，如果检测到故障或进行预防性维护：

- 新设备从外部存储器加载更换的设备的配置概要文件。
  参考 “从外部存储器加载配置概要文件” 页 98.
- 新设备使用 DHCP *Option 82* 获得其 IP 地址。
  参考 “DHCP 第二层中继” 页 292.
  参考 “设置具有选项 82 的 DHCP 服务器” 页 335.

对于每个解决方案，在重新启动时，新设备会获得已更换的设备的相同 IP 设置。

- 对于使用 HTTPS 访问设备管理，设备使用数字证书。您可以选择将自己的证书导入到设备。
  参考 “HTTPS 证书管理” 页 341.
- 对于使用 SSH访问设备管理，设备使用 RSA 主机密钥。您可以选择将自己的 PEM 格式的主机密钥导入到设备。
  参考 “将您自己的密钥加载到设备上” 页 338.

1 用户界面

设备允许用户使用以下用户界面指定设备的设置。

表格 1: 用于访问设备管理的用户界面

用户界面	可通过以下方式访问 …	前提条件
图形用户界面	以太网（带内）	Web 浏览器
命令行界面	以太网（带内） 串行接口（带外）	终端仿真软件
系统监控器	串行接口（带外）	终端仿真软件

1.1 图形用户界面

系统要求

要打开图形用户界面，您需要一个支持 HTML5 的桌面版本的 Web 浏览器。

提示： Web 浏览器等第三方软件根据到期日和当前密码参数建议等标准对证书进行验证。过时的证书可能会由于无效或过时的信息而导致问题。示例：过期的证书或更改的加密建议。为了解决与第三方软件的验证冲突，请将您自己的最新证书转移到设备上或使用最新固件重新生成证书。

启动图形用户界面

启动图形用户界面的前提条件是，在设备中配置了 IP 参数。参考 “指定 IP 参数” 页 41.

请执行以下步骤：

- ☐ 启动 Web 浏览器。
- ☐ 在 Web 浏览器的地址字段中输入设备的 IP 地址。
  请使用以下格式：https://xxx.xxx.xxx.xxx
  Web 浏览器建立与设备的连接并显示登录对话框。
- ☐ 若要更改图形用户界面的语言，请点击登录对话框右上角的相应链接。
- ☐ 输入用户名。
- ☐ 输入密码。
- ☐ 点击 *Login* 按钮。
  Web 浏览器会显示图形用户界面。

1.2 命令行界面

您可利用命令行界面通过本地或远程连接使用设备功能。

命令行界面为 IT 专业人员提供了一种配置 IT 设备的熟悉环境。作为资深用户或管理员，您拥有关于基本原理和使用 Schneider Electric 设备的相关知识。

1.2.1 准备数据连接

有关设备组装和启动的信息，请参阅“安装”用户手册。
☐ 将设备与网络连接起来。数据连接成功的前提条件是正确设置网络参数。

您可以使用例如 *PuTTY* 的免费软件程序访问命令行界面的用户界面。
☐ 在您的计算机上安装 *PuTTY* 程序。

1.2.2 使用 Telnet 访问命令行界面

使用 Windows 建立 Telnet 连接

Telnet 作为标配只安装在 Windows Vista 之前的 Windows 版本中。

请执行以下步骤：
☐ 启动您计算机上的 *Command Prompt* 程序。
☐ 输入命令 `telnet <IP_address>`。

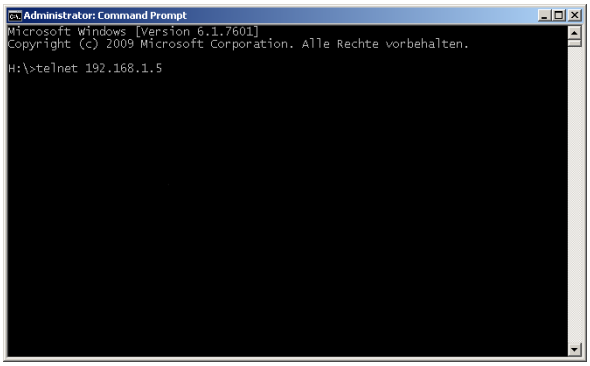


图 1: Command Prompt：建立至设备的 Telnet 连接

使用 PuTTY 建立 Telnet 连接

请执行以下步骤：

☐ 启动您计算机上的 *PuTTY* 程序。

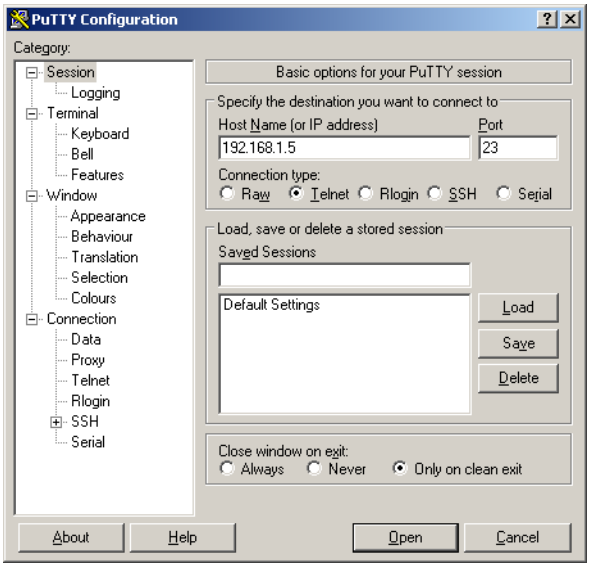


图 2: PuTTY 输入屏幕

☐ 在 *Host Name (or IP address)* 字段中，可以输入您设备的 IP 地址。
该 IP 地址由 4 个数值范围为 0 到 255 的十进制数字组成。这 4 个十进制数字由点隔开。

☐ 要选择连接类型，请在 *Connection type* 选项列表中选择 *Telnet* 单选按钮。

☐ 点击 *Open* 按钮，建立至您设备的数据连接。
屏幕上会出现命令行界面，其中有用于输入用户名的窗口。设备最多允许 5 名用户同时访问命令行界面。

提示：此设备是一种安全相关产品。在首次启动过程中请更改密码。

请执行以下步骤：

☐ 输入用户名。
默认用户名为 admin。

☐ 按下 <Enter> 键。

- 输入密码。
  默认密码为 private。
- 按下 <Enter> 键。

```
                    Copyright (c) 2011-2022 Schneider Electric

                                All rights reserved

                             MCSESM-E Release 08.7.00

                            (Build date 2022-07-11 16:30)


                    System Name    :  MCSESM-646038d5e846
                    Management IP  :  192.168.1.5
                    Subnet Mask    :  255.255.255.0
                    Base MAC       :  64:60:38:01:02:03
                    USB IP         :  91.0.0.100
                    USB Mask       :  255.255.255.0
                    System Time    :  2022-07-13 19:41:57


NOTE: Enter '?' for Command Help.  Command help displays all options
      that are valid for the particular mode.
      For the syntax of a particular command form, please
      consult the documentation.

MCSESM-E>
```

图 3: 命令行界面的启动屏幕

1.2.3 使用 SSH（Secure Shell）访问命令行界面

在以下示例中，我们使用 *PuTTY* 程序。使用 SSH 访问设备的另一个选项是 OpenSSH 套件。

请执行以下步骤：

- ☐ 启动您计算机上的 *PuTTY* 程序。

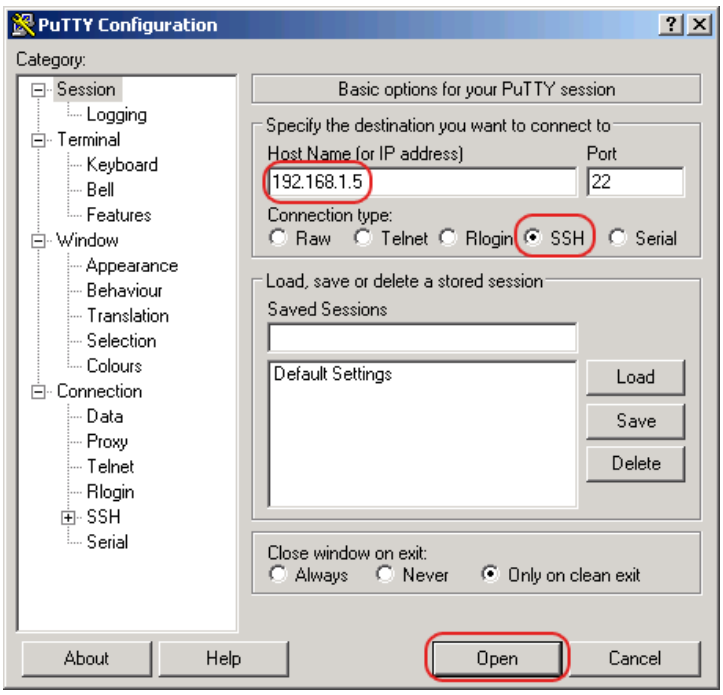


图 4: PuTTY 输入屏幕

- ☐ 在 *Host Name (or IP address)* 字段中，可以输入您设备的 IP 地址。
  该 IP 地址由 4 个数值范围为 0 到 255 的十进制数字组成。这 4 个十进制数字由点隔开。
- ☐ 要指定连接类型，请在 *Connection type* 选项列表中选择 *SSH* 单选按钮。
  选择并设置所需参数后，设备允许您使用 SSH 建立数据连接。
- ☐ 点击 *Open* 按钮，建立至您设备的数据连接。
  视设备以及配置 SSH 的时间而定，建立连接最多需要一分钟。
  首次登录时，在连接设置即将结束时，*PuTTY* 程序会显示一条安全警告消息，并允许您检查密钥指纹。

图 5: 针对指纹的安全警告提示

- ☐ 检查指纹。
  这可帮助您防止非法访问。
- ☐ 当指纹与设备密钥指纹匹配时，点击 *Yes* 按钮。
  设备允许用户使用命令 `show ssh` 或在 *Device Security* > *Management Access* > *Server* 对话框的 *SSH* 选项卡中显示设备密钥的指纹。
  屏幕上会出现命令行界面，其中有用于输入用户名的窗口。设备最多允许 5 名用户同时访问命令行界面。
- ☐ 输入用户名。
  默认用户名为 admin。
- ☐ 按下 <Enter> 键。
- ☐ 输入密码。
  默认密码为 private。
- ☐ 按下 <Enter> 键。

提示：此设备是一种安全相关产品。在首次启动过程中请更改密码。

```
login as: admin
admin@192.168.1.5's password:


                        Copyright (c) 2011-2022 Schneider Electric

                                All rights reserved

                             MCSESM-E Release 08.7.00

                            (Build date 2022-07-11 16:30)


                    System Name    :  MCSESM-646038d5e846
                    Management IP  :  192.168.1.5
                    Subnet Mask    :  255.255.255.0
                    Base MAC       :  64:60:38:01:02:03
                    USB IP         :  91.0.0.100
                    USB Mask       :  255.255.255.0
                    System Time    :  2022-07-13 19:41:57


NOTE: Enter '?' for Command Help.  Command help displays all options
      that are valid for the particular mode.
      For the syntax of a particular command form, please
      consult the documentation.

MCSESM-E>
```

图 6: 命令行界面的启动屏幕

1.2.4 使用串行接口访问命令行界面

串行接口用于在本地连接外部网络管理站（VT100 终端或具有终端仿真的 PC）。该接口允许用户建立与命令行界面和系统监控器的数据连接。

请执行以下步骤：

- ☐ 使用串行接口将设备连接到一个终端。或者，使用基于 VT100 的终端仿真将设备连接到 PC 的一个 COM 端口，然后按下任意键。
- ☐ 也可使用 *PuTTY* 程序通过串行接口建立至设备的串行数据连接。按下 <Enter> 键。

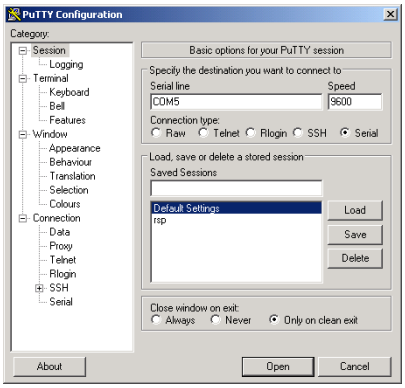


图 7: 使用 PuTTY 程序通过串行接口建立串行数据连接

- ☐ 按下终端键盘上的任意键若干次，直到登录屏幕指示 CLI 模式为止。
- ☐ 输入用户名。
  默认用户名为 admin。
- ☐ 按下 <Enter> 键。
- ☐ 输入密码。
  默认密码为 private。
- ☐ 按下 <Enter> 键。

提示：此设备是一种安全相关产品。在首次启动过程中请更改密码。

```
                    Copyright (c) 2011-2022 Schneider Electric

                                All rights reserved

                             MCSESM-E Release 08.7.00

                            (Build date 2022-07-11 16:30)


          System Name   :  MCSESM-646038d5e846
          Management IP :  192.168.1.5
          Subnet Mask   :  255.255.255.0
          Base MAC      :  64:60:38:01:02:03
          USB IP        :  91.0.0.100
          USB Mask      :  255.255.255.0
          System Time   :  2022-07-13 19:41:57


NOTE: Enter '?' for Command Help.  Command help displays all options
      that are valid for the particular mode.
      For the syntax of a particular command form, please
      consult the documentation.

MCSESM-E>
```

图 8: 命令行界面的启动屏幕

1.2.5 基于模式的命令层次结构

在命令行界面中，命令根据其类型被分组到相关模式中。每种命令模式都支持特定的 Schneider Electric 软件命令。

您作为用户可以使用的命令取决于您的权限级别（管理员、操作员、访客、审核员）。它们还取决于您当前工作所处的模式。当您切换到一种特定模式时，您可以使用该模式的命令。

User Exec 模式命令为例外。命令行界面还允许用户在 Privileged Exec 模式下执行这些命令。

下图显示了命令行界面的各种模式。

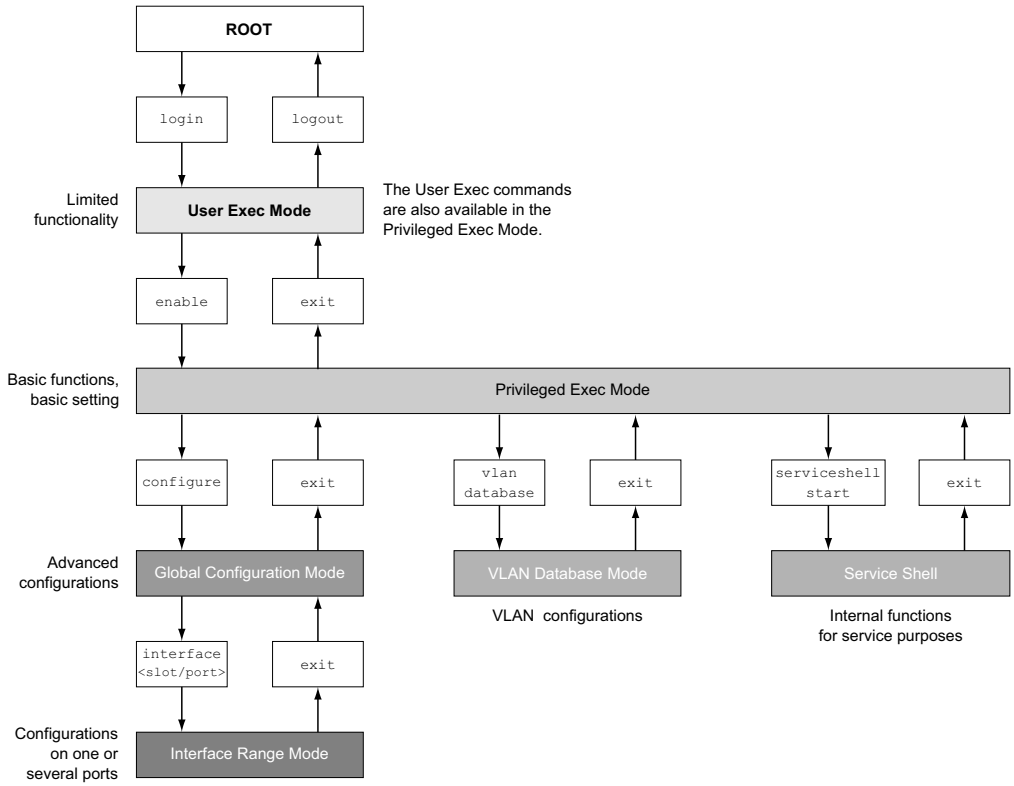


图 9: 命令行界面的结构

视用户级别而定，命令行界面支持以下模式：

- User Exec 模式
  使用命令行界面登录时，将进入 User Exec 模式。User Exec 模式包含有限范围的命令。
  命令提示符：(MCSESM-E) >
- Privileged Exec 模式
  要访问整个范围的命令，请进入 Privileged Exec 模式。如果以特权用户身份登录，则可以进入 Privileged Exec 模式。在 Privileged Exec 模式下，您还可以执行 User Exec 模式命令。
  命令提示符：(MCSESM-E) #
- VLAN 模式
  VLAN 模式包含与 VLAN 相关的命令。
  命令提示符：(MCSESM-E) (VLAN)#
- Service Shell
  Service Shell 为服务专用。
  命令提示符：/mnt/fastpath #

- Global Config 模式
  Global Config 模式允许用户对当前配置进行修改。此模式对一般设置命令进行分组。
  命令提示符：(MCSESM-E) (config)#
- Interface Range 模式
  Interface Range 模式中的命令对设备的一个特定端口、一组选定的多个端口或所有端口产生影响。这些命令对一个或多个特定端口上的一个值进行修改或对一个功能进行开启/关闭。
  - 设备中的所有物理端口
    命令提示符：(MCSESM-E) ((interface) all)#
    示例：当您从 Global Config 模式切换到 Interface Range 模式时，命令提示符变化如下：
    (MCSESM-E) (config)#interface all
    (MCSESM-E) ((Interface)all)#
  - 一个接口上的一个端口
    命令提示符：(MCSESM-E) (interface <slot/port>)#
    示例：当您从 Global Config 模式切换到 Interface Range 模式时，命令提示符变化如下：
    (MCSESM-E) (config)#interface 2/1
    (MCSESM-E) (interface 2/1)#
  - 一个接口上的一系列端口
    命令提示符：(MCSESM-E) (interface <interface range>)#
    示例：当您从 Global Config 模式切换到 Interface Range 模式时，命令提示符变化如下：
    (MCSESM-E) (config)#interface 1/2-1/4
    (MCSESM-E) ((Interface)1/2-1/4)#
  - 单个端口的列表
    命令提示符：(MCSESM-E) (interface <interface list>)#
    示例：当您从 Global Config 模式切换到 Interface Range 模式时，命令提示符变化如下：
    (MCSESM-E) (config)#interface 1/2,1/4,1/5
    (MCSESM-E) ((Interface)1/2,1/4,1/5)#
  - 端口范围和单个端口的列表
    命令提示符：(MCSESM-E) (interface <complex range>)#
    示例：当您从 Global Config 模式切换到 Interface Range 模式时，命令提示符变化如下：
    (MCSESM-E) (config)#interface 1/2-1/4,1/6-1/9
    (MCSESM-E) ((Interface)1/2-1/4,1/6-1/9)

下表显示了命令模式、相应模式下可见的命令提示符（输入请求字符）以及退出此模式时使用的选项。

表格 2: 命令模式

命令模式	访问方式	退出或启动下一个模式
User Exec 模式	第一个访问级别。执行基本任务并列出系统信息。	要退出，请输入 logout： (MCSESM-E) >logout Are you sure (Y/N) ?y
Privileged Exec 模式	从 User Exec 模式，输入命令 enable： (MCSESM-E) >enable (MCSESM-E) #	要退出 Privileged Exec 模式并返回 User Exec 模式，请输入 exit： (MCSESM-E) #exit (MCSESM-E) >

表格 2: 命令模式

命令模式	访问方式	退出或启动下一个模式
VLAN 模式	从 Privileged Exec 模式，输入命令 vlan database： (MCSESM-E) #vlan database (MCSESM-E) (Vlan)#	要结束 VLAN 模式并返回 Privileged Exec 模式，请输入 exit 或按下 Ctrl Z。 (MCSESM-E) (Vlan)#exit (MCSESM-E) #
Global Config 模式	从 Privileged Exec 模式，输入命令 configure： (MCSESM-E) #configure (MCSESM-E) (config)# 从 User Exec 模式，输入命令 enable，然后在 Privileged Exec 模式下输入命令 Configure： (MCSESM-E) >enable (MCSESM-E) #configure (MCSESM-E) (config)#	要退出 Global Config 模式并返回 Privileged Exec 模式，请输入 exit： (MCSESM-E) (config)#exit (MCSESM-E) # 然后，要退出 Privileged Exec 模式并返回 User Exec 模式，请再次输入 exit： (MCSESM-E) #exit (MCSESM-E) >
Interface Range 模式	从 Global Config 模式，输入命令 interface {all|<slot/port>|<interface range> |<interface list>|<complex range>}。 (MCSESM-E) (config)#interface <slot/port> (MCSESM-E) (interface slot/port)#	要退出 Interface Range 模式并返回 Global Config 模式，请输入 exit。要返回 Privileged Exec 模式，请按下 Ctrl Z。 (MCSESM-E) (interface slot/port)#exit (MCSESM-E) #

当您在提示符之后输入问号 (?) 时，命令行界面会显示可用命令的列表和命令的简短描述。

```
(MCSESM-E)>
  cli               Set the CLI preferences.
  enable            Turn on privileged commands.
  help              Display help for various special keys.
  history           Show a list of previously run commands.
  logout            Exit this session.
  ping              Send ICMP echo packets to a specified IP address.
  show              Display device options and settings.
  telnet            Establish a telnet connection to a remote host.

(MCSESM-E)>
```

图 10: User Exec 模式中的命令

1.2.6 执行命令

语法分析

使用命令行界面登录时，将进入 User Exec 模式。命令行界面会在屏幕上显示 (MCSESM-E)> 提示符。

当您输入一条命令并按下 <Enter> 键时，命令行界面会开始进行语法分析。命令行界面在命令树中搜索所需的命令。

当该命令在命令行界面命令范围以外时，一条消息会通知您检测到的错误。

示例：

用户希望执行 `show system info` 命令，但已输入不带 `info` 的 `f` 并按下 〈Enter〉 键。

命令行界面随后显示消息：

```
(MCSESM-E)>show system ino

Error: Invalid command 'ino'
```

命令树

命令行界面中的命令中以树状结构进行组织。这些命令以及可能适用的相关参数不断进行分支，直到该命令被完全定义并成为可执行为止。命令行界面会对输入进行检查。当您正确且完整地输入了命令和参数时，可以使用 〈Enter〉 键执行该命令。

输入命令和所需参数之后，输入的其他参数会被视为可选参数。当其中一个参数为未知时，命令行界面将显示一条语法消息。

命令树对所需参数进行分支，直到所需参数到达结构中的最后一个分支为止。

借助可选参数，命令树进行分支，直到所需参数和可选参数到达结构中的最后一个分支为止。

1.2.7 命令的结构

本节介绍了语法、约定和术语，并使用示例对其进行呈现。

命令的格式

多数命令都包含参数。

当缺少命令参数时，命令行界面会通知用户检测到错误的命令语法。

本手册使用 Courier 字体显示命令和参数。

参数

参数的顺序与命令的正确语法密切相关。

参数指的是所需值、可选值、各种选择或其组合。表示形式指示参数的类型。

表格 3: 参数和命令语法

`<command>`	尖括号（◇）中的命令为必填。
`[command]`	方括号（[]）中的命令为可选。
`<parameter>`	尖括号（◇）中的参数为必填。
`[parameter]`	方括号（[]）中的参数为可选。
...	一个元素之后的省略号（连续 3 个点，之间无空格）表示可以重复该元素。

表格 3: 参数和命令语法

[Choice1 | Choice2]	括号内的一个竖线表示一个选择选项。选择一个值。 由竖线隔开并括在方括号内的元素表示一个可选选择（Option1、Option2 或无选择）。
{list}	大括号（{}）表示需要从选项列表中选择一个参数。
{Choice1 | Choice2}	由竖线隔开并括在大括号（{}）内的元素表示一个必填选择选项（option1 或 option2）。
[param1 {Choice1 | Choice2}]	显示一个包含必填选择的可选参数。
<a.b.c.d>	小写字母为通配符。可以输入采用 a.b.c.d 标志法并带有小数点的参数（如：IP 地址）
<cr>	按下 <Enter> 键，创建一个换行符（回车符）。

以下列表显示了命令行界面中可能的参数值：

表格 4: 命令行界面中的参数值

值	描述
IP 地址	此参数表示一个有效的 IPv4 地址。该地址由 4 个数值范围为 0 到 255 的十进制数字组成。这 4 个十进制数字由小数点隔开。IP 地址 0.0.0.0 是一个有效条目。
MAC 地址	此参数表示一个有效的 MAC 地址。该地址由 6 个数值范围为 00 到 FF 的十六进制数字组成。这些数字用冒号隔开，如 00:F6:29:B2:81:40。
string	长度在指定范围内的用户自定义文本，如最多 32 个字符。
character string	使用双引号表示一个字符串，如 “System name with space character”。
number	指定范围内的整数，如 0..999999。
date	采用 YYYY-MM-DD 格式的日期。
time	采用 HH:MM:SS 格式的时间。

网络地址

网络地址是建立至远程工作站、服务器或另一个网络的数据连接的必要条件。需要区分 IP 地址和 MAC 地址。

IP 地址是由网络管理员分配的地址。IP 地址在一个网络区域中是唯一的。

MAC 地址是由硬件制造商分配的地址。MAC 地址在全世界都是唯一的。

下表显示了地址类型的表示形式和范围：

表格 5: 网络地址的格式和范围

地址类型	格式	范围	示例
IP 地址	nnn.nnn.nnn.nnn	nnn：0 到 255（十进制）	192.168.11.110
MAC 地址	mm:mm:mm:mm:mm:mm	mm：00 到 ff（十六进制数字对）	A7:C9:89:DD:A9:B3

文本串

文本串由引号表示。如 “System name with space character”。空格符不是有效的用户自定义文本串。可以在引号之间的参数中输入空格符。

示例：

```
*(MCSESM-E)#cli prompt Device name
Error: Invalid command 'name'

*(MCSESM-E)#cli prompt 'Device name'

*(Device name)#
```

1.2.8 命令示例

示例 1：clear arp-table-switch

用于清除管理代理（缓存）的 ARP 表的命令。

`clear arp-table-switch` 为命令名称。无需任何其他参数，只需按下 <Enter> 键即可执行该命令。

示例 2：radius server timeout

用于配置 RADIUS 服务器超时数值的命令。

```
(MCSESM-E) (config)#radius server timeout
 <1..30>               Timeout in seconds (default: 5).
```

`radius server timeout` 为命令名称。

该参数为必填。值范围为 1..30。

示例 3：radius server auth modify <1..8>

用于为 RADIUS 身份验证服务器 1 设置参数的命令。

```
(MCSESM-E) (config)#radius server auth modify 1
 [name]                RADIUS authentication server name.
 [port]                RADIUS authentication server port.
                       (default: 1812).
 [msgauth]             Enable or disable the message authenticator
                       attribute for this server.
 [primary]             Configure the primary RADIUS server.
 [status]              Enable or disable a RADIUS authentication
                       server entry.
 [secret]              Configure the shared secret for the RADIUS
                       authentication server.
 [encrypted]           Configure the encrypted shared secret.
  <cr>                 Press Enter to execute the command.
```

`radius server auth modify` 为命令名称。

参数 <1..8>（RADIUS 服务器索引）为必填。值范围为 1..8（整数）。

参数 [name]、[port]、[msgauth]、[primary]、[status]、[secret] 和 [encrypted] 为可选。

1.2.9 输入提示符

命令模式

借助输入提示符，命令行界面会显示您处于三种模式中的哪种模式：

- (MCSESM-E) >
  User Exec 模式
- (MCSESM-E) #
  Privileged Exec 模式
- (MCSESM-E) (config)#
  Global Config 模式
- (MCSESM-E) (Vlan)#
  VLAN Database mode
- (MCSESM-E) ((Interface)all)#
  Interface Range 模式/设备的所有端口
- (MCSESM-E) ((Interface)2/1)#
  Interface Range 模式/一个接口上的一个端口
- (MCSESM-E) ((Interface)1/2-1/4)#
  Interface Range 模式/一个接口上的一系列端口
- (MCSESM-E) ((Interface)1/2,1/4,1/5)#
  Interface Range 模式/单个端口的列表
- (MCSESM-E) ((Interface)1/1-1/2,1/4-1/6)#
  Interface Range 模式/端口范围和单个端口的列表

星号、井号和感叹号

- 星号 *
  处于输入提示符第一位或第二位的星号 * 向用户显示非永久性存储器中的设置与永久存储器中的设置不同。在您的配置中，设备检测到尚未保存的修改。
  *(MCSESM-E)>
- 井号 #
  处于输入提示符开头的井号 # 向用户显示启动参数与启动阶段期间的参数不同。
  *#(MCSESM-E)>
- 感叹号 !
  处于输入提示符开头的感叹号 ! 显示：user 或 admin 用户帐户的密码符合默认设置。
  !(MCSESM-E)>

通配符

设备允许用户更改命令行提示符。

命令行界面支持以下通配符：

表格 6: 在命令行界面输入提示符中使用通配符

通配符	描述
%d	系统日期
%t	系统时间
%i	设备的 IP 地址
%m	设备的 MAC 地址。
%p	设备的产品名称

```
!(MCSESM-E)>enable

!(MCSESM-E)#cli prompt %i

!192.168.1.5#cli prompt (MCSESM-E)%d

!*(MCSESM-E)2022-07-13#cli prompt (MCSESM-E)%d%t

!*(MCSESM-E)2022-07-13 19:41:57#cli prompt %m

!*AA:BB:CC:DD:EE:FF#
```

1.2.10 按键组合

用户可以使用以下按键组合，更轻松地使用命令行界面：

表格 7: 命令行界面中按键组合

按键组合	描述
<CTRL> + <H>、<退格键>	删除之前的字符
<CTRL> + <A>	转到行的开头
<CTRL> + <E>	转到行的末尾
<CTRL> + <F>	前进一个字符
<CTRL> + <B>	后退一个字符
<CTRL> + <D>	删除当前字符
<CTRL> + <U>、<X>	删除到行的开头
<CTRL> + <K>	删除到行的末尾
<CTRL> + <W>	删除之前的单词
<CTRL> + <P>	转到历史缓冲区的前一行
<CTRL> + <R>	重写或粘贴该行
<CTRL> + <N>	转到历史缓冲区的下一行

表格 7: 命令行界面中按键组合

按键组合	描述
<CTRL> + <Z>	返回到根命令提示符
<CTRL> + <G>	中止正在运行的 tcpdump 会话
<Tab> 键、<SPACE>	命令行补全
Exit	转到下一级命令提示符
<?>	列出选择

帮助命令会在屏幕上显示命令行界面中可能的按键组合：

```
(MCSESM-E) #help

HELP:
Special keys:

  Ctrl-H, BkSp delete previous character
  Ctrl-A  .... go to beginning of line
  Ctrl-E  .... go to end of line
  Ctrl-F  .... go forward one character
  Ctrl-B  .... go backward one character
  Ctrl-D  .... delete current character
  Ctrl-U, X .. delete to beginning of line
  Ctrl-K  .... delete to end of line
  Ctrl-W  .... delete previous word
  Ctrl-P  .... go to previous line in history buffer
  Ctrl-R  .... rewrites or pastes the line
  Ctrl-N  .... go to next line in history buffer
  Ctrl-Z  .... return to root command prompt
  Ctrl-G  .... aborts running tcpdump session
  Tab, <SPACE> command-line completion
  Exit    .... go to next lower command prompt
  ?       .... list choices

(MCSESM-E) #
```

图 11: 使用帮助命令列出按键组合

1.2.11 数据条目元素

命令补全

为了简化命令的键入，命令行界面允许用户使用命令补全（Tab 键补全）。因此，用户可以对关键词进行缩写。

- 输入关键词的起始字母。当输入的字符中识别到关键词时，在您按下 Tab 键或空格键之后，命令行界面将补全该关键词。当存在补全的一个以上选项时，请输入唯一标识关键词所需的一个或多个字母。再次按下 Tab 键或空格键。之后，系统对该命令或参数进行补全。
- 当您输入非唯一关键词并按下两次 <Tab 键>或<空格键>时，命令行界面会显示选项的列表。
- 当您输入非唯一关键词并按下 <Tab 键>或<空格键>时，命令行界面会补全命令，直至出现非唯一选项。在存在若干个命令的情况下再次按下 <Tab 键>或<空格键>时，命令行界面会显示选项的列表。
  示例：
  ```
  (MCSESM-E) (Config)#lo
  (MCSESM-E) (Config)#log
  logging logout
  ```
  当您输入 `lo` 并按下 <Tab 键>或<空格键>时，命令行界面会将该命令补全为 `log`，之后出现非唯一选项。
  当您再次按下 <Tab 键>或<空格键>时，命令行界面会显示选项的列表（`logging logout`）。

可能的命令/参数

可以通过输入 `help` 或 `?` 获得命令或可能参数的列表，如通过输入 `(MCSESM-E) >show ?`

当您输入显示的命令时，可以获得可用于命令 `show` 的参数的列表。

当您在问号之前输入不带空格符的命令时，设备会显示命令本身的帮助文本：

```
!*#(MCSESM-E)(Config)#show?

   show          Display device options and settings.
```

1.2.12 使用案例

保存配置

为了帮助确保在设备重置之后或电压供应中断之后能够保留您的密码设置和其他配置更改，您需要保存配置。为此，请执行以下步骤：

- ☐ 输入 `enable`，切换到 Privileged Exec 模式。
- ☐ 输入以下命令：
  ```
  save [profile]
  ```
- ☐ 按下 <Enter> 键，执行该命令。

“radius server auth add”命令的语法

使用此命令添加一个 RADIUS 身份验证服务器。
- 模式：Global Config 模式
- 权限级别：Administrator
- 格式：`radius server auth add <1..8> ip <a.b.c.d> [name <string>] [port <1..65535>]`
  - [name]：RADIUS 身份验证服务器名称。
  - [port]：RADIUS 身份验证服务器端口（默认值： 1813

参数	含义	可能的值
<1..8>	RADIUS 服务器索引。	1..8
<a.b.c.d>	RADIUS 记账服务器 IP 地址。	IP 地址
<string>	输入一个用户自定义文本，最多 32 个字符。	
<1..65535>	输入 1 至 65535 之间的端口编号。	1..65535

模式和权限级别：
- 执行该命令的前提条件：用户处于 Global Config 模式。参考 “基于模式的命令层次结构” 页 24.
- 执行该命令的前提条件：用户拥有 Administrator 访问角色。

命令和参数的语法：参考 “命令的结构” 页 28.

可执行命令示例：
- `radius server auth add 1 ip 192.168.30.40`
- `radius server auth add 2 ip 192.168.40.50 name radiusserver2`
- `radius server auth add 3 ip 192.168.50.60 port 1813`
- `radius server auth add 4 ip 192.168.60.70 name radiusserver4 port 1814`

1.2.13 Service Shell

Service Shell 为服务专用。

Service Shell 允许用户访问设备的内部功能。当您在使用设备过程中需要协助时，服务人员会使用 Service Shell 对交换机或 CPU 寄存器等内部状况进行监控。

注意

设备无法运行的风险

不要执行删除非易失性存储器（*NVM*）没有维修技术人员的说明。

不遵守这些说明可能会导致设备无法工作。

启动 Service Shell

前提条件是用户处于 User Exec 模式。(MCSESM-E) >

请执行以下步骤：
- ☐ 输入 enable，然后按下 <Enter> 键。
  为减少输入操作，您可以：
  - 输入 e，然后按下 <Tab> 键。
- ☐ 输入 serviceshell start，然后按下 <Enter> 键。
  为减少输入操作，您可以：
  - 输入 ser，然后按下 <Tab> 键。
  - 输入 s，然后按下 <Tab> 键。

```
!MCSESM-E >enable

!*MCSESM-E #serviceshell start
 WARNING! The service shell offers advanced diagnostics and functions.
 Proceed only when instructed by a service technician.

 You can return to the previous mode using the 'exit' command.

 BusyBox v1.31.0 (2022-07-13 19:41:57 UTC) built-in shell (ash)
 Enter 'help' for a list of built-in commands.

!/mnt/fastpath #
```

使用 Service Shell

当 Service Shell 激活时，命令行界面超时被停用。为帮助防止配置不一致，请在任何其他用户开始向设备传送新配置之前结束 Service Shell。

显示 Service Shell 命令

前提条件是用户已经启动了 Service Shell。

请执行以下步骤：
- ☐ 输入 help，然后按下 <Enter> 键。

```
/mnt/fastpath # help
Built-in commands:
------------------
        . : [ [[ alias bg break cd chdir command continue echo eval exec
        exit export false fg getopts hash help history jobs kill let
        local pwd read readonly return set shift source test times trap
        true type ulimit umask unalias unset wait
/mnt/fastpath #
```

结束 Service Shell

请执行以下步骤：
☐ 输入 exit，然后按下 <Enter> 键。

永久停用设备中的 Service Shell

停用 Service Shell 后，用户仍然可以配置设备。但服务人员只能进行系统诊断。服务技术人员将不再能够访问设备的内部功能。

这种停用是不可撤销的。Service Shell 将保持永久停用状态。**为了重新激活 Service Shell，需要由制造商对设备进行拆卸。**

前提条件是：
- Service Shell 未启动。
- 用户处于 User Exec 模式： (MCSESM-E) >

请执行以下步骤：
☐ 输入 enable，然后按下 <Enter> 键。
为减少输入操作，您可以：
- 输入 e，然后按下 <Tab> 键。

☐ 输入 serviceshell deactivate，然后按下 <Enter> 键。
为减少输入操作，您可以：
- 输入 ser，然后按下 <Tab> 键。
- 输入 dea，然后按下 <Tab> 键。

☐ **此步骤是不可撤销的！**
按下 <Y> 键。

```
!MCSESM-E >enable

!*MCSESM-E #serviceshell deactivate
Notice: If you continue, then the Service Shell is permanently deactivated.
This step is irreversible!
For details, refer to the Configuration Manual.
Are you sure (Y/N) ?
```

1.3 系统监控器

系统监控器允许用户在启动操作系统之前设置基本操作参数。

1.3.1 功能范围

在系统监控器中，可以执行以下任务，例如：
- 管理操作系统和验证软件镜像
- 更新操作系统
- 启动操作系统
- 删除配置概要文件，将设备重置为出厂默认值
- 检查启动代码信息

1.3.2 启动系统监控器

您可以使用 USB-C 接口与设备建立串行连接。在启动过程中，设备的串口不可用。因此，启动系统监视器的工作方式与其他方式不同 Schneider Electric 设备。要启动系统监视器，请将设备设置为恢复模式。

将设备设置为恢复模式

所需配件：
- 外部存储器（推荐： ACA22-USB-C
- USB-C 到 USB-A 适配器（仅当您使用与推荐的不同的外部存储器时）
- 用于连接设备的 USB-C 端口与计算机的 USB 数据线
- 带有 VT100 终端仿真的计算机（例如e PuTTY）或串行终端

请执行以下步骤：
- ☐ 将外部存储器插入计算机。
- ☐ 在外部存储器的根目录下，创建一个名为 recovery.txt.
- ☐ 将外部存储器插入设备。
- ☐ 重新启动设备。
- ☐ 在设备启动时观察 LED。当e *Status* LED 红绿交替闪烁，设备已成功启动进入恢复模式。

提示：您可以在“安装”用户手册中找到显示元素的说明。

访问系统监视器

请执行以下步骤：
- ☐ 从设备中移除外部存储器。
- ☐ 使用 USB 电缆将您的计算机连接到设备。
- ☐ 在计算机上打开 VT100 终端仿真以显示系统监视器。
- ☐ 选择适当的 COM 端口。

计算机和设备连接成功后，您会看到黑屏。

请执行以下步骤：

- 请按〈Enter〉键显示系统监视器。
  您会在计算机上看到以下视图：

```
System Monitor 1
(Selected OS: ...-8.7 (2022-07-11 16:30))

1  Manage operating system
3  Start selected operating system
4  Manage configurations
5  Show boot code information
q  End (reset and reboot)




sysMon1>
```

图 12: System Monitor 视图

- 要选择菜单条目，请输入相应的数字。
- 要离开子菜单并返回主菜单，请按〈ESC〉键。

提示：下次要正常开机，只需要添加外存，不要 recovery.txt文件。

2 指定 IP 参数

首次安装设备时，需要输入 IP 参数。

设备为首次安装期间输入 IP 参数提供了以下选项：

- 使用命令行界面进行输入。
  当您在设备的工作环境以外对其进行预配置或恢复对设备的网络访问（“带内”）时，请选择这种“带外”方法。
- 使用 Ethernet Switch Configurator 协议的条目。
  当您拥有一个以前安装的网络设备或在您的 PC 与设备之间拥有另一个以太网连接时，可以选择这种“带内”方法。
- 使用外部存储器进行配置。
  当您使用相同类型的设备更换一个设备并且已经将配置保存到外部存储器中时，可以选择这种方法。
- 使用 BOOTP。
  要使用 BOOTP 对已安装设备进行配置，可以选择这种“带内”方法。对于这种方法，需要一台 BOOTP 服务器。BOOTP 服务器会使用其 MAC 地址向设备分配配置数据。DHCP 模式是配置数据引用的默认模式。
- 使用 DHCP 进行配置。
  要使用 DHCP 对已安装设备进行配置，可以选择这种“带内”方法。对于这种方法，需要一台 DHCP 服务器。DHCP 服务器会使用其 MAC 地址或系统名称向设备分配配置数据。
- 使用图形用户界面进行配置。
  当设备已经拥有 IP 地址且可以使用网络访问设备时，图形用户界面为用户提供了配置 IP 参数的另一个选项。

2.1 IP 参数基础

2.1.1 IPv4

IP 地址

IP 地址由 4 个字节组成。以十进制表示法输入这 4 个字节，之间以小数点隔开。

1992 年编写的 RFC 1340 定义了 5 种 IP 地址类别。

表格 8: IP 地址类别

类别	网络地址	主机地址	地址范围
A	1 Byte	3 Bytes	0.0.0.0 至 127.255.255.255
B	2 Bytes	2 Bytes	128.0.0.0 至 191.255.255.255
C	3 Bytes	1 Byte	192.0.0.0 至 223.255.255.255
D			224.0.0.0 至 239.255.255.255
E			240.0.0.0 至 255.255.255.255

一个 IP 地址的第一个字节是网络地址。全球领先的网络地址分配监管委员会是 IANA ("Internet Assigned Numbers Authority")。当您需要 IP 地址块时，请与您的 Internet Service Provider (ISP) 联系。您的 ISP 将与其当地更高级别组织联系，以保留一个 IP 地址块：

- APNIC (Asia Pacific Network Information Center)
  亚太地区
- ARIN (American Registry for Internet Numbers)
  美洲和撒哈拉沙漠以南非洲
- LACNIC (Regional Latin-American and Caribbean IP Address Registry)
  拉丁美洲和某些加勒比岛国
- RIPE NCC (Réseaux IP Européens)
  欧洲及周边地区

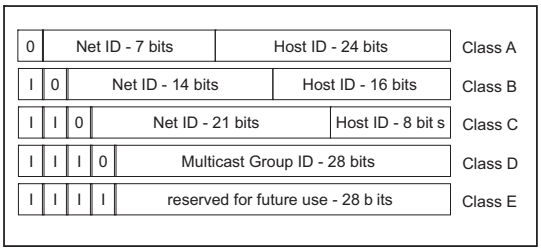


图 13: IP 地址的位表示

例如，当一个 IP 地址的第一个位为零时，它属于类别 A，第一个八位字节小于 128。

例如，当一个 IP 地址的第一个位为一、第二个位为零时，它属于类别 B，第一个八位字节在 128 和 191 之间。

例如，当一个 IP 地址的前两个位为一时，它属于类别 C，第一个八位字节大于 191。

网络运营商负责分配主机地址 (host ID)。网络运营商独自负责确保所分配 IP 地址的唯一性。

子网掩码

路由器和 Gateways 会将大型网络细分成子网。子网掩码会将单个设备的 IP 地址分配给一个特定子网。

可以通过与将网络地址 (net id) 划分成类别 A 至 C 基本相同的方式使用子网掩码进行子网划分。

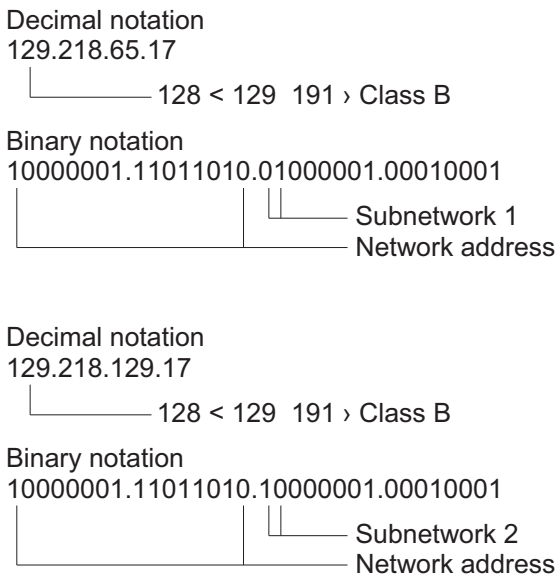
将主机地址 (host id) 中代表掩码的位设置为一。将剩余的主机地址位设置为零（参见以下示例）。

子网掩码示例：

Decimal notation
255.255.192.0

Binary notation
11111111.11111111.11000000.00000000
Subnetwork mask bits
Class B

为子网分配将子网掩码应用到 IP 地址的示例：



子网掩码使用方法示例

在一个大型网络中，Gateways 和路由器可能会将管理代理与其网络管理站分隔开。在这种情况下，寻址功能如何工作呢？

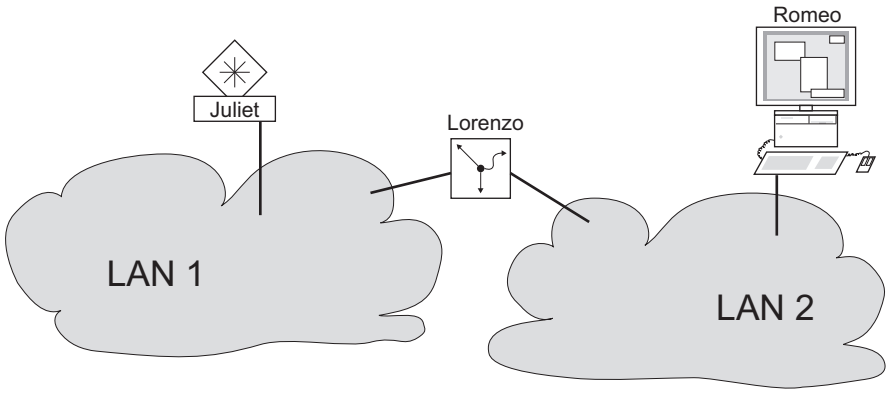


图 14: 一个路由器将管理代理与其网络管理站分隔开

网络管理站“Romeo”希望向管理代理“Juliet”发送数据。Romeo 知道 Juliet 的 IP 地址，同时也知道路由器“Lorenzo”知道至 Juliet 的路径。

因此，Romeo 将其消息放入一个信封中，并写上 Juliet 的 IP 地址作为目标地址；对于源地址，他在信封上写上自己的 IP 地址。

然后，Romeo 将该信封放入以 Lorenzo 的 MAC 地址作为目标地址并且以他自己的 MAC 地址作为源地址的第二个信封中。这个过程相当于从 ISO/OSI 基本参考模型的第三层进到第二层。

最后，Romeo 将整个数据包放入邮箱中，这相当于从第二层进到第一层，即，通过以太网发送数据包。

Lorenzo 收到信函，拆掉外层信封，并根据内层信封得知该信函是写给 Juliet 的。他将内层信封放入一个新的外层信封中，并在他的地址列表（ARP 表）中搜索 Juliet 的 MAC 地址；他在外层信封上写上 Juliet 的 MAC 地址作为目标地址，并写上他自己的 MAC 地址作为源地址。然后，他将整个数据包放入邮箱中。

Juliet 收到信函并拆掉外层信封。她在内层信封上看到 Romeo 的 IP 地址。打开内层信封并阅读其内容相当于将消息传送到 ISO/OSI 分层模型中更高的协议层。

现在，Juliet 希望向 Romeo 发送应答。她将自己的应答放入一个以 Romeo 的 IP 地址作为目标地址并且以她自己的 IP 地址作为源地址的信封中。但是，她要将应答发送到哪里呢？因为她并没有接收到 Romeo 的 MAC 地址。该地址丢失了，因为 Lorenzo 更换了外层信封。

在 MIB 中，Juliet 发现变量 `NetGatewayIPAddr` 项下将 Lorenzo 列为与 Romeo 进行通信的一种方式。因此，她将带有 IP 地址的信封放入另一个带有 Lorenzo 的 MAC 目标地址的信封中。

现在，该信函通过 Lorenzo 送回到 Romeo，方式与第一封信函从 Romeo 传送到 Juliet 相同。

Classless Inter-Domain Routing

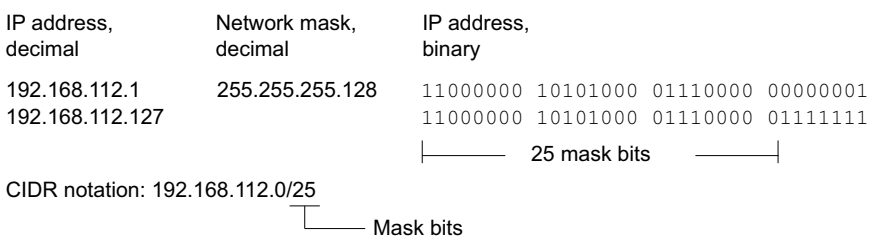
对于多数用户而言，具有最多 254 个地址的类别 C 太小，而具有最多 65534 个地址的类别 B 又太大。这就导致可用类别 B 地址的利用效率较低。

类别 D 包含预留的 Multicast 地址。类别 E 用于实验目的。非参与 Gateway 会忽略带有这些目标地址的实验数据报。

自 1993 年以来，RFC 1519 一直在使用 Classless Inter-Domain Routing (CIDR) 提供解决方案。CIDR 克服了这些类别界限并支持无类地址范围。

借助 CIDR，可以输入指定 IP 地址范围的位的数量。以二进制格式表示 IP 地址范围，并统计指定子网掩码的掩码位。这些掩码位等于用于一个给定 IP 地址范围内的子网的位的数量。

示例：



“超网”一词系指将一些类别 C 地址范围组合起来。超网允许用户在更细的程度上对类别 B 地址范围进行划分。

2.1.2 IPv6

IP 参数基础

互联网协议第 6 版 (IPv6) 是互联网协议第 4 版 (IPv4) 的新版本。之所以实施 IPv6，是因为在当今互联网不断发展的背景下，IPv4 地址已经无法满足正常需求。RFC 8200 中介绍了此 IPv6 协议。

与 IPv4 相比，IPv6 的不同之处在于：
- 不同的地址表示方法和长度
- 不存在广播地址类型
- 简化了报头结构

- 分片仅由源主机执行
- 增加了网络中数据包流识别的功能

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

提示：如果希望设备仅使用 IPv4 功能，请禁用设备中的 IPv6 功能。

在设备中，IPv6 协议具有以下限制：
- 用户可指定最多 8 个 IPv6 单播地址，如下所示：
  - 4 个通过手动配置的 IPv6 地址
  - 选择 *Auto* 单选按钮时的 2 个 IPv6 地址
  - 1 个使用 DHCPv6 服务器的 IPv6 地址
  - 1 个链路本地地址
- IPv6 功能只能在管理接口上启用。可在接口上同时使用全部可配置的 IPv6 地址。
- IPv6 地址可用于设置设备的管理 IP 地址。其他可以使用 IPv6 地址的服务还包括 SNTP、SYSLOG、DNS 和 LDAP 等。

地址的表示方法

IPv6 地址由 128 位组成。它表示为 8 组 4 位十六进制数，每组表示 16 位，进一步称为十六进制字符串。这些十六进制字符串用冒号 (:) 隔开。IPv6 地址不区分大小写，采用大写形式或小写形式均可。

根据 RFC 4291，IPv6 地址的首选格式为 x:x:x:x:x:x:x:x。每个“x”由 4 个十六进制值组成，表示一个十六进制字符串。下图显示了 IPv6 地址的首选格式示例。

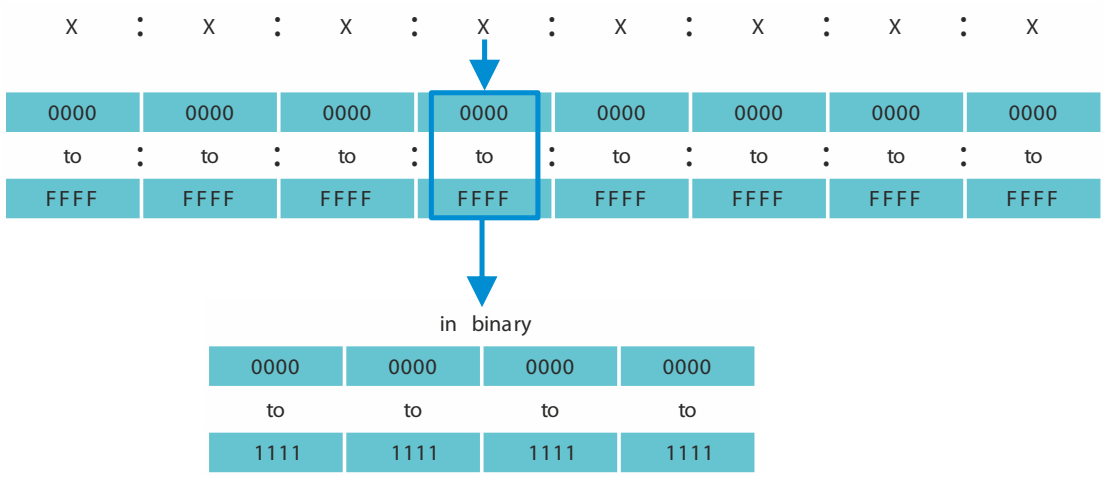


图 15: IPv6 地址表示方法

如上图所示，IPv6 地址通常包含许多个零。为了缩短包含 0 位的 IPv6 地址，必须遵循以下 2 条写入规则：
- 第一个规则是丢弃每个十六进制字符串中的前导零。这一规则仅适用于前导零，而不适用于十六进制字符串中的尾随零。如果尾随零也被丢弃，则结果地址将模糊不清。
- 第二条规则是使用特殊语法来压缩零。您可以使用 2 个相邻的冒号“::”来替换仅包含零的相邻十六进制字符串。“::”符号在一个地址中只能使用一次。如果在地址表示中多次使用“::”符号，则可能会从该表示法中扩展出多个地址。

应用这两个规则后，结果通常称为压缩格式。

您可以在下表中找到 2 个有关如何应用这些规则的示例：

表格 9: IPv6 地址压缩

首选	CC03:0000:0000:0000:0001:AB30:0400:FF02
无前导零	CC03: 0: 0: 0: 1:AB30: 400:FF02
压缩	CC03::1:AB30:400:FF02

首选	2008:00B7:0000:DEF0:DDDD:0000:E604:0001
无前导零	2008: B7: 0:DEF0:DDDD: 0:E604: 1
压缩	2008:B7::DEF0:DDDD:0:E604:1

前缀长度

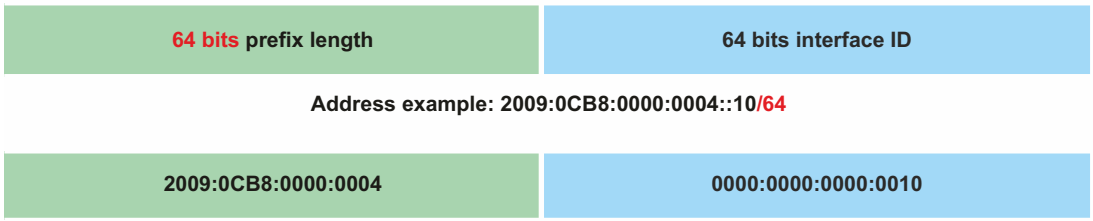
与 IPv4 地址不同，IPv6 地址不使用子网掩码来识别地址的网络部分。相反，IPv6 协议使用前缀长度进行识别。

IPv6 地址前缀的文本表示方法与 Classless Inter-Domain Routing (CIDR) 中 IPv4 地址前缀的编写方式类似：

<ipv6-address>/<prefix-length>

前缀长度范围为 0..128。LAN 和其他类型网络的常见 IPv6 前缀长度为 /64。也就是说，地址的网络部分的长度为 64 位。其余的 64 位表示接口 ID，类似于 IPv4 地址的主机部分。

您可以在下图中找到前缀长度位分配的示例。



地址类型

RFC 4291 中介绍了此 IPv6 地址类型。

IPv6 地址类型由地址的高阶位标识，如下表所示：

表格 10: IPv6 地址类型

地址类型	二进制前缀	IPv6 表示法
未指定	00...0 (128 bits)	::/128
回环	00...1 (128 bits)	::1/128
Multicast ‹多播›	11111111	FF00::/8
链路本地单播	1111111010	FE80::/10
全局单播	(everything else)	

未指定地址

每个位都设置为 0 的 IPv6 地址称为未指定地址，它对应于 IPv4 中的 0.0.0.0。未指定地址仅用于指示不存在的地址。在尚未确定唯一地址时，通常将其用作源地址。

提示：未指定的地址不能分配给接口或用作目标地址。

回环地址

单播地址 0:0:0:0:0:0:0:1 称为回环地址。设备可通过该地址向其自身发送 IPv6 数据包。无法将其分配给物理接口。

多播地址

与 IPv4 不同，IPv6 不具备广播地址。但是，实际上存在一个 IPv6 全节点多播地址，可以提供相同的结果。

IPv6 多播地址用于将 IPv6 数据包发送到多个目标。多播地址的结构如下：后 4 位用于识别多播地址的范围（数据包的传输距离）。

- 前 8 位被设为 FF。
- 后 4 位表示地址的租约时间：0 表示永久，1 表示临时。
- 后 4 位用于识别多播地址的范围，即数据包通过网络的传输距离。

链路本地地址

链路本地地址用于与相同链路上的其他设备进行通信，“链路”一词系指子网。路由器不会将带有链路本地源或目标地址的数据包转发到其他链路。

链路本地地址用于在单链路上传输数据包，范围包括诸如自动地址配置、邻居发现或不存在路由器等。格式如下：

表格 11: 链路本地地址格式

10 位	54 位	64 位
1111111010	0	接口 ID

链路本地地址始终处于配置状态，无法更改。

全局单播地址

全局单播地址在全局范围内唯一，并可以通过互联网进行路由。这类地址等同于公共 IPv4 地址。当前，仅分配了前三位为 001 或 2000::/3 的全局单播地址。

全局单播地址由 3 部分组成：

- 全局路由前缀
- 子网 ID
- 接口 ID。

全局路由前缀是地址的网络部分。

组织可使用子网 ID 识别其子网，子网 ID 长度最多为 16 位。子网 ID 的长度取决于全局路由前缀的长度。

接口 ID 用于识别特定节点的接口。使用“接口 ID”一词是因为一个主机可以有多个接口，每个接口有一个或多个 IPv6 地址。

下图显示了 IPv6 全局单播地址的一般格式。

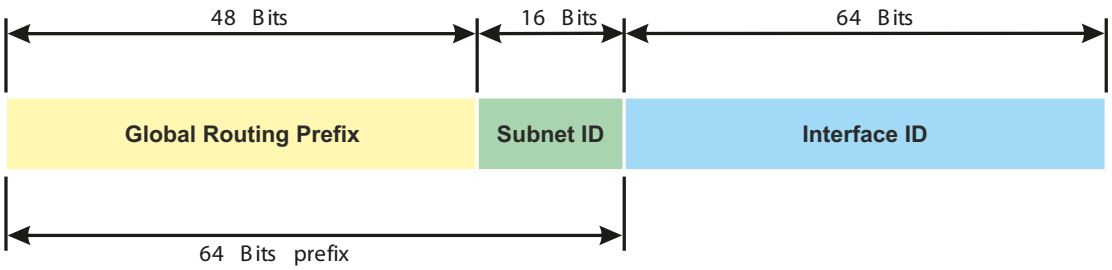


图 16: IPv6 全局单播地址的一般格式

2.2 使用命令行界面指定 IP 参数

2.2.1 IPv4

可以使用以下方法输入 IP 参数：

- BOOTP/DHCP
- Ethernet Switch Configurator协议
- External memory ‹外部存储器›
- 使用串行连接的命令行界面

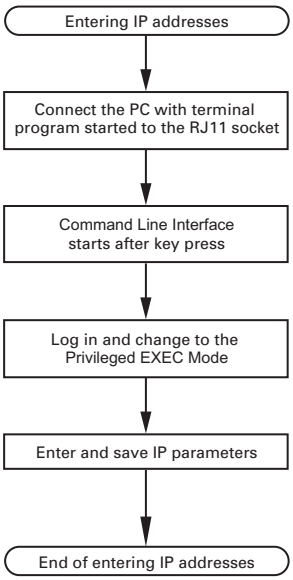


图 17: IP 地址输入流程图

提示：如果安装位置附近没有可用的终端或具有终端仿真的 PC，用户可以在自己的工作站上对设备进行配置，然后将其转移到最终安装位置。

请执行以下步骤：

☐ 建立至设备的连接。
启动屏幕会出现。

☐ 停用 DHCP。

☐ 输入 IP 参数。
- ▶ 本地 IP 地址
  在默认设置下，本地 IP 地址为 0.0.0.0。
- ▶ 子网掩码
  当您将网络划分成若干子网时，这些子网均带有子网掩码标识符，可在此输入子网掩码。在默认设置下，本地子网掩码为 0.0.0.0。
- ▶ Gateway 的 IP 地址。
  只有当设备和网络管理站或 TFTP 服务器位于不同子网时，才需要此条目(参阅页 43 “子网掩码使用方法示例”)。
  指定带有设备的子网与至网络管理站的路径之间 Gateway 的 IP 地址。
  在默认设置下，该 IP 地址为 0.0.0.0。

☐ 使用 copy config running-config nvm 保存指定的配置。

enable	切换到特权执行模式。
network protocol none	停用 DHCP。
network parms 10.0.1.23 255.255.255.0	为设备分配 IP 地址 10.0.1.23 和子网掩码 255.255.255.0。还可以选择分配一个 Gateway 地址。
copy config running-config nvm	将当前设置保存到永久存储器 (nvm) 的“选定”配置概要文件中。

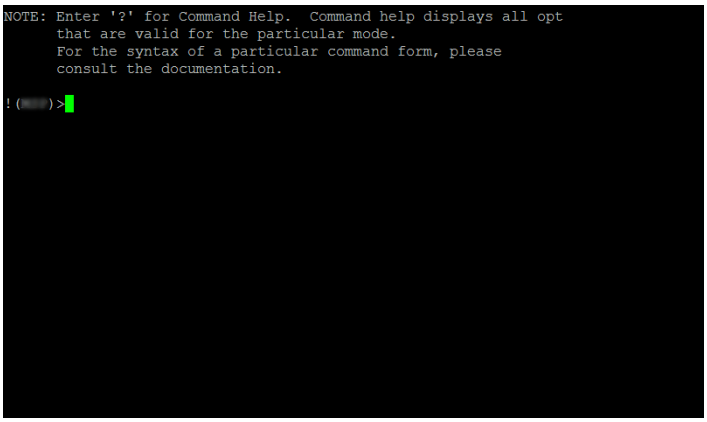
输入 IP 参数之后，可以使用图形用户界面轻松对设备进行配置。

2.2.2 IPv6

设备允许用户通过串行接口使用命令行界面指定 IPv6 参数。访问命令行界面的另一种方法是使用 SSH 连接和 IPv4 管理地址。

请执行以下步骤：

☐ 建立至设备的连接。
启动屏幕会出现。



☐ 如果该协议被禁用，则启用 IPv6 协议。
☐ 输入 IPv6 参数。
- IPv6 地址
  有效的 IPv6 地址。IPv6 地址以压缩格式显示。
- 前缀长度
  与 IPv4 地址不同，IPv6 地址不使用子网掩码来识别地址的网络部分。此角色在 IPv6 中由前缀长度执行 （参阅页 46 “前缀长度”）。
- *EUI option* 功能
  可以使用 *EUI option* 功能自动配置 IPv6 地址的接口 ID。设备使用其接口的 MAC 地址，并在第 3 和第 4 个字节之间添加值 ff 和 fe ，以生成 64 位接口 ID。
  仅可为前缀长度等于 64 的 IPv6 地址选择此选项。
- IPv6 网关地址
  IPv6 网关地址是路由器的地址，设备通过该地址访问自己网络以外的其他设备。
  用户可指定任何 IPv6 地址，回环和 *Multicast* 地址除外。
  在默认设置下，IPv6 网关地址为 ::。

`enable`	切换到特权执行模式。
`network ipv6 operation`	如果该协议被禁用，则启用 IPv6 协议。在默认设置下，IPv6 协议为启用状态。
`network ipv6 address add 2001::1 64 eui-64`	将 IPv6 地址分配为 2001::1，前缀长度为 64。 eui-64 参数为可选。 用户也可选择分配网关地址。
`copy config running-config nvm`	将当前设置保存到永久存储器 (nvm) 的“选定”配置概要文件中。

输入 IPv6 参数之后，可以使用图形用户界面轻松对设备进行配置。若要在 URL 中使用 IPv6 地址，请使用以下 URL 语法：https://[<ipv6_address>]。

2.3 指定 IP 参数：使用 Ethernet Switch Configurator

Ethernet Switch Configurator 协议允许用户使用以太网向设备分配 IP 参数。

您可以使用图形用户界面轻松配置其他参数。

在您的 PC 上安装 Ethernet Switch Configurator 软件。

请执行以下步骤：
- ☐ 启动 Ethernet Switch Configurator 程序。

Ethernet Switch Configurator 启动后，Ethernet Switch Configurator 将在网络中自动搜索支持 Ethernet Switch Configurator 协议的设备。

Ethernet Switch Configurator 使用在 PC 上找到的第一个网络接口。当您的计算机具有多个网卡时，可以在 Ethernet Switch Configurator 工具栏中选择一个。

Ethernet Switch Configurator 为对 Ethernet Switch Configurator 协议查询作出响应的每个设备显示一行信息。

Ethernet Switch Configurator 让用户能够识别显示的设备。
- ☐ 选择一个设备行。
- ☐ 要将 LED 指示灯设置为对所选设备进行闪烁，请点击工具栏上的 *Signal* 按钮。要停止闪烁，请再次点击 *Signal* 按钮。
- ☐ 双击一个行，可以打开一个可在其中指定设备名称和 IP 参数的窗口。

提示：在将 IP 参数分配给设备后，禁用设备中的 Ethernet Switch Configurator 功能。

提示：保存设置，以便重启之后仍然能保留条目。

2.4 使用图形用户界面指定 IP 参数

2.4.1 IPv4

请执行以下步骤：

- ☐ 打开 *Basic Settings > Network > Global* 对话框。

在此对话框中，指定可在其中访问设备管理的 VLAN，并配置 Ethernet Switch Configurator 访问。

- ☐ 在 *VLAN ID* 列中，指定可在其中通过网络访问设备管理的 VLAN。

在此请注意，您只能使用属于相关 VLAN 成员的端口访问设备管理。

MAC address 字段显示您通过网络访问设备时使用的设备的 MAC 地址。

- ☐ 在 *Ethernet Switch Configurator protocol v1/v2* 框中，您可以指定使用 Ethernet Switch Configurator 软件访问设备的设置。
- ☐ Ethernet Switch Configurator 协议允许用户根据设备的 MAC 地址向其分配 IP 地址。如果用户希望用 PC 中的 Ethernet Switch Configurator 软件将 IP 地址分配给设备，则激活 Ethernet Switch Configurator 协议。
- ☐ 打开 *Basic Settings > Network > IPv4* 对话框。

在此对话框中，指定设备在启动之后从其获得 IP 参数的源。

- ☐ 在 *Management interface* 框中，首先指定设备从哪里获得其 IP 参数：

▶ 在 *BOOTP* 模式下，该配置会根据设备的 MAC 地址使用 BOOTP 或 DHCP 服务器。
▶ 在 *DHCP* 模式下，该配置会根据设备的 MAC 地址或设备名称使用 DHCP 服务器。
▶ 在 *Local* 模式下，设备会使用来自内部设备存储器的网络参数。

提示：当您更改 IP 地址的分配模式时，设备会在您点击 ✔ 按钮之后立即激活新的模式。

- ☐ 如果需要，可以在 *IP parameter* 框中输入 IP 地址、子网掩码和 Gateway。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

2.4.2 IPv6

请执行以下步骤：

- ☐ 打开 *Basic Settings > Network > IPv6* 对话框。
- ☐ 默认已启用 IPv6 协议。验证 *Operation* 框中的 *On* 单选按钮是否已被选中。
- ☐ 在 *Configuration* 框中，指定设备从哪里获得其 IPv6 参数：

- 如果选择 *None* 单选按钮，则设备手动接收其 IPv6 参数。
  用户可手动指定最多 4 个 IPv6 地址。无法将环回、链路本地和 *Multicast* 地址指定为静态 IPv6 地址。
- 如果选择 *Auto* 单选按钮，则设备动态接收其 IPv6 参数，例如通过使用路由器通告守护程序 (radvd)。
  设备接收最多 2 个 IPv6 地址。
- 如果选择 *DHCPv6* 单选按钮，则设备从 DHCPv6 服务器接收其 IPv6 参数。
  设备仅可从 DHCPv6 服务器接收一个 IPv6 地址。
- 如果选择 *All* 单选按钮，则设备使用动态和手动分配的每个替代项来接收其 IPv6 参数。

提示：当您更改 IPv6 地址的分配模式时，设备会在您点击 按钮之后立即激活新的模式。

☐ 如有必要，在 *IP parameter* 框中输入 *Gateway address*。

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

☐ 在 *Duplicate Address Detection* 框中，用户可指定设备为 *Duplicate Address Detection* 功能发送的连续 *Neighbor Solicitation* 消息的数量 (参阅页 60 “Duplicate Address Detection”)。

暂时保存更改。为此，请单击 按钮。

手动指定 IPv6 地址。为此，请执行以下步骤：

☐ 打开 *Basic Settings* > *Network* > *IPv6* 对话框。

☐ 点击 按钮。
该对话框显示 *Create* 窗口。

☐ 在 *IP address* 字段中输入 IPv6 地址。

☐ 在 *PrefixLength* 字段中输入 IPv6 地址的前缀长度。

☐ 点击 *Ok* 按钮。
设备添加一个新的表格条目。

2.5 使用 BOOTP 指定 IP 参数

当 *BOOTP* 功能激活时，设备会向 BOOTP 服务器发送一条启动请求消息。该启动请求消息包含在 *Basic Settings > Network > IPv4*对话框中配置的客户端 ID。BOOTP 服务器会将该客户端 ID 输入到一个数据库中并分配一个 IP 地址。该服务器会使用一条启动应答消息进行应答。该启动应答消息包含分配的 IP 地址。

2.6 指定 IP 参数：使用 DHCP

2.6.1 IPv4

DHCP（动态主机配置协议）是 BOOTP 的进一步发展并代替了 BOOTP。DHCP 进一步允许使用名称而非 MAC 地址对 DHCP 客户端进行配置。

对于 DHCP，此名称称为“Client Identifier”，它符合 RFC 2131。

设备使用在 MIB II 系统组中 sysName 项下输入的名称作为 Client Identifier。可以使用图形用户界面（参见对话框 *Basic Settings > System*）、命令行界面或 SNMP 更改系统名称。

设备会将其系统名称发送到 DHCP 服务器。然后，DHCP 服务器会使用系统名称分配一个 IP 地址，作为 MAC 地址的替代地址。

除 IP 地址之外，DHCP 服务器还会发送
- 子网掩码
- 默认 Gateway（如果有的话）
- 配置文件的 TFTP URL（如果有的话）。

设备会将配置数据应用到相应参数。当 DHCP 服务器分配 IP 地址时，设备会将配置数据永久保存到永久存储器中。

表格 12: 设备请求的 DHCP 选项

选项	含义
1	Subnet Mask
2	Time Offset
3	Router
4	Time server
12	Host Name
42	NTP server
61	Client Identifier
66	TFTP Server Name
67	Bootfile Name

与 BOOTP 相比，使用 DHCP 的优点在于，DHCP 服务器可以将配置参数的有效期（“租期”）限制在特定时间段（所谓的动态地址分配）。在此期限（“租期”）结束之前，DHCP 客户端可以尝试续展此租期。此外，客户端还可以协商新的租期。然后，DHCP 服务器会分配一个随机空闲地址。

为帮助避免这种情况，DHCP 服务器提供了根据唯一硬件 ID 为特定客户端分配相同 IP 地址的明确配置选项（所谓的静态地址分配）。

在默认设置下，DHCP 已激活。只要 DHCP 已激活，设备就会尝试获取 IP 地址。当设备在重新启动之后无法找到 DHCP 服务器时，则设备没有 IP 地址。*Basic Settings > Network > IPv4* 对话框可用于激活或停用 DHCP。

提示: 使用 ConneXium Network Manager 网络管理时，请验证 DHCP 是否向每个设备都分配原始 IP 地址。

附录中包含了 BOOTP/DHCP 服务器配置示例。

DHCP 配置文件示例：

```
# /etc/dhcpd.conf for DHCP Daemon
#
subnet 10.1.112.0 netmask 255.255.240.0 {
option subnet-mask 255.255.240.0;
option routers 10.1.112.96;
}
#
# Host berta requests IP configuration
# with her MAC address
#
host berta {
hardware ethernet 00:80:63:08:65:42;
fixed-address 10.1.112.82;
}
#
# Host hugo requests IP configuration
# with his client identifier.
#
host hugo {
#
option dhcp-client-identifier "hugo";
option dhcp-client-identifier 00:68:75:67:6f;
fixed-address 10.1.112.83;
server-name "10.1.112.11";
filename "/agent/config.dat";
}
```

以 # 字符开始的行包含备注。

在单独列出的设备之前的行指的是应用于以下设备的设置。

固定地址行向设备分配一个永久 IP 地址。

有关更多信息，请参阅 DHCP 服务器手册。

2.6.2 IPv6

动态主机配置协议第 6 版 (DHCPv6) 是用于动态指定 IPv6 地址的网络协议。此 IPv6 协议等同于 IPv4 的 DHCP 协议。RFC 8415 中介绍了 DHCPv6 协议。

设备会使用 DHCP 唯一标识符 (DUID) 向 DHCPv6 服务器发送请求。在设备中，DUID 表示 DHCPv6 服务器识别请求 IPv6 地址设备所使用的 *Client ID*。

Client ID 显示在 *DHCP* 框的 *Basic Settings* > *Network* > *IPv6* 对话框中。

设备仅可从 DHCPv6 服务器接收一个 *PrefixLength* 为 128 的 IPv6 地址。不提供 *Gateway address* 信息。如有需要，可以手动指定 *Gateway address* 信息。

在默认设置下，DHCPv6 协议为停用状态。可在 *Basic Settings* > *Network* > *IPv6* 对话框中激活或停用协议。验证 *DHCPv6* 框中的 *Configuration* 单选按钮已被选中。

如果想要动态获取 *PrefixLength* 并非为 128 的 IPv6 地址，则请选择 *Auto* 单选按钮。以下为路由器通告守护程序 (radvd) 的使用示例。radvd 使用 *Router Solicitation* 和 *Router Advertisement*消息自动配置 IPv6 地址。

在默认设置下，选择 *Auto* 单选按钮。可以在 *Configuration* 框中的 *Basic Settings* > *Network* > IPv6对话框中选择或取消选择 *Auto* 单选按钮。

如果选择 *All* 单选按钮，则设备使用动态和手动分配的每个替代项来接收其 IPv6 参数。

2.7 管理地址冲突检测

可以使用几种不同的方法为设备分配 IP 地址。此功能可帮助设备在启动之后检测网络上的 IP 地址冲突，此外，设备在运行期间也会定期进行检查。RFC 5227 中介绍了此功能。

启用后，设备会发送一个 SNMP 陷阱，向您告知它检测到一个 IP 地址冲突。

以下列表包含了此功能的默认设置：
- *Operation*: *On*
- *Detection mode*: *active and passive*
- *Send periodic ARP probes*：勾选
- *Detection delay [ms]*: 200
- *Release delay [s]*: 15
- *Address protections*: 3
- *Protection interval [ms]*: 200
- *Send trap*：勾选

2.7.1 主动和被动检测

对网络进行主动检查有助于防止设备使用重复 IP 地址连接到网络。将设备连接到网络之后或配置 IP 地址之后，设备会立即检查网络中是否存在其 IP 地址。为了检查网络有无地址冲突，设备会向网络中发送 4 个检测延迟为 200 毫秒的 ARP 探测器。当该 IP 地址存在时，设备会尝试恢复之前的配置，并在配置的发布延迟时间之后进行另一次检查。

当您禁用主动检测时，设备会以 2 秒间隔发送 2 条免费 APR 公告。在被动检测启用的情况下使用 ARP 公告时，设备会对网络进行轮询，以确定是否存在地址冲突。在解决地址冲突之后或到期的发布延迟时间之后，设备会重新连接到网络。在检测到 10 个冲突之后，当配置的发布延迟间隔小于 60 秒时，设备会将发布延迟间隔设置为 60 秒。

在设备进行主动检测或您禁用主动检测功能之后，在被动检测启用的情况下，设备会在网络上侦听使用相同 IP 地址的其他设备。当设备检测到重复 IP 地址时，设备首先会在被动检测模式下使用 ACD 机制保护其地址，并发送出免费 ARP。设备发送的保护的数量以及保护间隔都是可配置的。为了解决冲突，如果远程设备仍然连接到网络，则本地设备的网络接口会与网络断开连接。

当 DHCP 服务器向设备分配 IP 地址且发生地址冲突时，设备会返回一条 DHCP 拒绝消息。

设备使用 ARP 探测器方法。这有以下优点：
- 其他设备上的 ARP 缓存保持不变
- 该方法能够经受多次 ARP 探测器传输

2.8 Duplicate Address Detection

Duplicate Address Detection 功能用于确定接口上的 IPv6 单播地址的唯一性。当使用手动、*DHCPv6* 或 *Auto* 方法配置 IPv6 地址时，会执行此功能。链路状态发生变化时也会触发此功能，例如链路状态从下行改为上行。

Duplicate Address Detection 功能使用 *Neighbor Solicitation* 和 *Neighbor Advertisement* 消息。用户可指定设备发送的连续 *Neighbor Solicitation* 消息的数量。为此，请执行以下步骤：

- ☐ 打开 *Basic Settings* > *Network* > *IPv6* 对话框。
- ☐ 在 *Duplicate Address Detection* 框，设定 *Number of neighbor solicitants* 字段中的必要值。
  可能的值：
  - 0
    该功能已禁用。
  - 1..5 （默认设置：1）
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`enable`	切换到特权执行模式。
`network ipv6 dad-transmits <0..5>`	设定设备发送的 *Neighbor Solicitation* 消息的数量。 值为 0 时禁用功能。

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

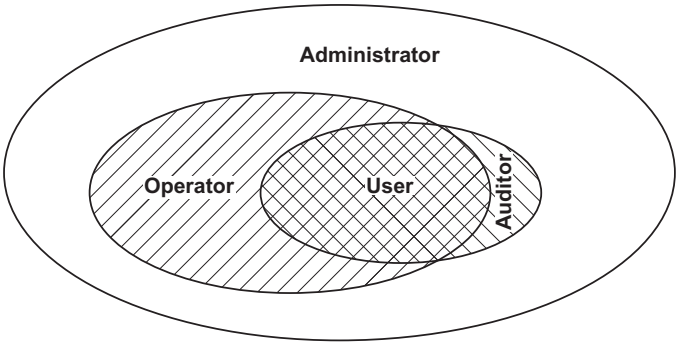
3 访问设备

3.1 访问角色

您作为用户可以使用的设备功能取决于您的访问角色。当您以某个特定访问角色登录时，可以使用该访问角色的功能。

您作为用户可以使用的命令还取决于您当前工作所处的命令行界面模式。参考 “基于模式的命令层次结构” 页 24.

设备提供以下访问角色：



表格 13: 访问角色和用户授权范围

访问角色	用户授权
User	以访问角色 User 登录的用户有权对设备进行监控。
Auditor	以访问角色 Auditor 登录的用户有权对设备进行监控并在 *Diagnostics* > Report > *Audit Trail* 对话框中保存日志文件。
Operator	以访问角色 Operator 登录的用户有权对设备进行监控并更改设置 – 针对设备访问的安全设置除外。
Administrator	以访问角色 Administrator 登录的用户有权对设备进行监控并更改设置。
Unauthorized	未经授权的用户会被阻止，设备会拒绝用户登录。分配此值以临时锁定用户帐户。如果在访问角色更改期间发生检测到的错误，则设备会将此访问角色分配给用户帐户。

3.2 首次登录（密码更改）

为帮助防止对设备不必要的访问，请务必在初始设置期间更改默认密码。

请执行以下步骤：

- ☐ 在首次登录时，打开图形用户界面，SE View 应用程序或命令行界面。
- ☐ 使用默认密码登录。
  设备提示您输入新密码。
- ☐ 输入您的新密码。
  为帮助提高安全性，请选择包含至少 8 个字符的密码，包括大小写字母、数字和特殊字符。
- ☐ 使用命令行界面登录时，设备将提示您确认新密码。
- ☐ 使用您的新密码重新登录。

提示：如果密码丢失，请您联系当地支持团队。

3.3 身份验证列表

当用户使用特定连接访问设备时，设备会对包含设备应用于身份验证的策略的身份验证列表中的用户登录凭证进行验证。

用户访问设备管理的前提条件是，至少有一个策略被分配给通过其进行访问的应用程序的身份验证列表。

3.3.1 应用程序

设备为用户通过其访问设备的每种类型的连接提供一个应用程序：
- 使用串行连接访问命令行界面：Console(V.24)
- 使用 SSH 访问命令行界面：SSH
- 使用 Telnet 访问命令行界面：Telnet
- 访问图形用户界面：WebInterface

设备还提供一个用于控制从使用基于端口的访问控制的相连终端设备访问网络的应用程序：8021x

3.3.2 策略

当用户使用有效登录数据进行登录时，设备允许用户访问其设备管理。设备使用以下策略对用户进行身份验证：
- 设备的用户管理
- LDAP
- RADIUS

当终端设备使用有效登录数据进行登录时，设备允许相连终端设备访问使用符合 IEEE 802.1X 的基于端口的访问控制的网络。设备使用以下策略对终端设备进行身份验证：
- RADIUS
- IAS (Integrated Authentication Server)

设备为用户提供后退解决方案选项。为此，可在身份验证列表中指定一个以上的策略。使用当前策略进行身份验证不成功时，设备会应用下一个指定的策略。

3.3.3 管理身份验证列表

您可以在图形用户界面中或命令行界面中管理身份验证列表。为此，请执行以下步骤：

□ 打开 *Device Security > Authentication List* 对话框。

该对话框显示已经设置的身份验证列表。

`show authlists`	显示已经设置的身份验证列表。

☐ 为没有通过其对设备进行访问的应用程序停用身份验证列表，如 8021x。

☐ 在身份验证列表 defaultDot1x8021AuthList 的 *Active* 列中，取消勾选复选框。

☐ 暂时保存更改。为此，请单击 按钮。

`authlists disable defaultDot1x8021AuthList`	停用身份验证列表 defaultDot1x8021AuthList。

3.3.4 调整设置

示例：为身份验证列表 WebInterface 中默认包括的应用程序 defaultLoginAuthList 设置一个单独的身份验证列表。

设备向网络中的一个 RADIUS 服务器转发身份验证请求。作为一种后退解决方案，设备使用本地用户管理对用户进行身份验证。为此，请执行以下步骤：

☐ 创建一个身份验证列表 loginGUI。

☐ 打开 *Device Security > Authentication List* 对话框。

☐ 点击 按钮。
该对话框显示 *Create* 窗口。

☐ 在 *Name* 字段中输入一个有意义的名称。
在此示例中，输入名称 loginGUI。

☐ 点击 *Ok* 按钮。
设备添加一个新的表格条目。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`authlists add loginGUI`	创建身份验证列表 loginGUI。

☐ 为身份验证列表 loginGUI 选择策略。

☐ 在 *Policy 1* 列中，选择值 *radius*。

☐ 在 *Policy 2* 列中，选择值 *local*。

☐ 在 *Policy 3* 至 *Policy 5* 列中，选择值 *reject*，以帮助防止进一步的后退。

☐ 在 *Active* 列中，勾选复选框。

☐ 暂时保存更改。为此，请单击 按钮。

`authlists set-policy loginGUI radius local reject reject reject`	将策略 radius、local 和 reject 分配给身份验证列表 loginGUI。
`show authlists`	显示已经设置的身份验证列表。
`authlists enable loginGUI`	激活身份验证列表 loginGUI。

☐ 将一个应用程序分配给身份验证列表 loginGUI。

☐ 在 *Device Security > Authentication List* 对话框中，突出显示身份验证列表 loginGUI。

☐ 点击 ☰ 按钮，然后点击 *Allocate applications* 项目。
该对话框显示 *Allocate applications* 窗口。

☐ 在左侧列中，突出显示应用程序 WebInterface。

☐ 点击 ▶ 按钮。
右侧列中现在显示应用程序 WebInterface。

☐ 点击 *Ok* 按钮。
该对话框显示更新的设置：
- 身份验证列表 loginGUI 的 *Dedicated applications* 列中显示应用程序 WebInterface。
- 身份验证列表 defaultLoginAuthList 的 *Dedicated applications* 列中不再显示应用程序 WebInterface。

☐ 暂时保存更改。为此，请单击 ✓ 按钮。

`show applists`	显示应用程序和分配的列表。
`applists set-authlist WebInterface loginGUI`	将 loginGUI 应用程序分配给身份验证列表 WebInterface。

3.4 用户管理

当用户使用有效登录数据进行登录时，设备允许用户访问其设备管理。设备使用本地用户管理或使用网络中的 RADIUS 服务器对用户进行身份验证。要使设备能够使用用户管理，请将 local 策略分配给一个身份验证列表，参见 *Device Security > Authentication List* 对话框。

在本地用户管理中，可以管理用户帐户。通常为每个用户分配一个用户帐户。

3.4.1 访问角色

设备允许用户使用基于角色的授权模型来具体控制对设备管理的访问。被分配了特定授权概要文件的用户，可以使用来自相同或较低的授权概要文件的命令和功能。

设备在可以访问设备管理的每个应用程序上使用授权概要文件。

每个用户帐户都链接到一个管控对设备各个功能的访问的访问角色。视相应用户的计划活动而定，可以向用户分配一个预定义访问角色。设备区分以下访问角色。

表格 14: 用户帐户的访问角色

Role	描述	有权进行以下活动
Administrator	用户有权对设备进行监控和管理。	具有读/写权限的所有活动，包括为管理员保留的以下活动： ▶ 添加、修改或删除用户帐户 ▶ 激活、停用或解锁用户帐户 ▶ 更改每个密码 ▶ 配置密码管理 ▶ 设置或更改系统时间 ▶ 向设备加载文件，如设备配置、证书或软件镜像 ▶ 将设置和安全相关设置重置为交付时的状态 ▶ 配置 RADIUS 服务器和身份验证列表 ▶ 使用命令行界面应用脚本 ▶ 启用/禁用 CLI 记录和 SNMP 记录 ▶ 外部存储器激活和停用 ▶ 系统监控器激活和停用 ▶ 启用/禁用设备管理访问服务（如 SNMP）。 ▶ 为图形用户界面或命令行界面配置基于 IP 地址的访问限制
Operator	用户有权对设备进行监控和配置 – 安全相关设置除外。	具有读/写权限的所有活动，为管理员保留的以上活动除外：

表格 14: 用户帐户的访问角色

Role	描述	有权进行以下活动
Auditor	用户有权对设备进行监控并在 *Diagnostics* > *Report* > Audit Trail 对话框中保存日志文件。	对具有读权限的活动进行监控。
Guest	用户有权对设备进行监控 – 安全相关设置除外。	对具有读权限的活动进行监控。
Unauthorized	不允许访问设备。 ▶ 作为管理员，您可以分配此访问角色，对用户帐户进行暂时锁定。 ▶ 如果管理员为用户帐户分配不同的访问角色并且检测到错误，则设备会将此访问角色分配给用户帐户。	不允许任何活动。

3.4.2 管理用户帐户

您可以在图形用户界面或命令行界面中管理用户帐户。为此，请执行以下步骤：

□ 打开 *Device Security* > *User Management* 对话框。

该对话框显示已经设置的用户帐户。

show users	显示已经设置的用户帐户。

3.4.3 默认设置

在交付状态下，设备中已经设置了用户帐户 admin 和 user。

表格 15: 出厂设置用户帐户的默认设置

参数	默认设置	
User name	admin	user
Password	private	public
Role	administrator	guest
User locked	未勾选	未勾选
Policy check	未勾选	未勾选
SNMP auth type	hmacmd5	hmacmd5
SNMP encryption type	des	des

在使设备对网络可用之前更改 admin 用户帐户的密码。

3.4.4 更改默认密码

为帮助防止越权访问，请更改默认用户帐户的密码。为此，请执行以下步骤：
☐ 更改 admin 和 user 用户帐户的密码。

☐ 打开 *Device Security > User Management* 对话框。
该对话框显示已经设置的用户帐户。
☐ 要获得复杂度更高的密码，请勾选 *Policy check* 列中的复选框。
保存前，设备会根据 *Password policy* 框中指定的策略对密码进行检查。
提示：完成密码检查后，*Basic Settings > System* 对话框的 *Security status* 框中会出现一条消息。可在 *Basic Settings > System* 对话框中指定导致出现此消息的设置。
☐ 点击 *Password* 字段中相关用户帐户的行。输入至少包含 6 个字符的密码。
允许最多 64 个字母数字字符。
▶ 设备区分大小写。
▶ 在 *Configuration* 框中可以指定密码最小长度。设备会不断检查密码最小长度。
☐ 暂时保存更改。为此，请单击 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`users password-policy-check <user> enable`	激活根据指定策略对 <user> 用户帐户的密码进行检查。通过这种方式，可以获得复杂度更高的密码。

提示：显示安全状态时，密码检查会导致出现 (`show security-status all`) 消息。可使用 `security-status monitor pwd-policy-inactive` 命令指定导致出现此消息的设置。

`users password <user> SECRET`	指定 <user> 用户帐户的密码 SECRET。输入至少 6 个字符。
`save`	将设置保存到永久存储器 (nvm) 的“选定”配置概要文件中。

3.4.5 设置新的用户帐户

向访问设备管理的每个用户分配一个单独的用户帐户。通过这种方式，可以具体控制对访问的授权。

在以下示例中，我们将为具有 USER 角色的 operator 用户设置用户帐户。具有 operator 角色的用户有权对设备进行监控和配置 - 安全相关设置除外。为此，请执行以下步骤：
☐ 创建一个新的用户帐户。

☐ 打开 *Device Security > User Management* 对话框。
☐ 点击 按钮。
该对话框显示 *Create* 窗口。
☐ 在 *User name* 字段中输入名称。
在此示例中，我们将用户帐户命名为 USER。
☐ 点击 *Ok* 按钮。
☐ 要获得复杂度更高的密码，请勾选 *Policy check* 列中的复选框。
保存前，设备会根据 *Password policy* 框中指定的策略对密码进行检查。

- ☐ 在 *Password* 字段中，输入至少包含 6 个字符的密码。
  允许最多 64 个字母数字字符。
  - ▶ 设备区分大小写。
  - ▶ 在 *Configuration* 框中可以指定密码最小长度。设备会不断检查密码最小长度。
- ☐ 在 *Role* 列中，选择用户角色。
  在此示例中，我们选择值 operator。
- ☐ 要激活该用户帐户，请勾选 *Active* 列中的复选框。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。
  该对话框显示已经设置的用户帐户。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`users add USER`	创建 USER 用户帐户。
`users password-policy-check USER enable`	激活根据指定策略对 USER 用户帐户的密码进行检查。通过这种方式，可以获得复杂度更高的密码。
`users password USER SECRET`	指定用户帐户 USER 的密码 SECRET。输入至少 6 个字符。
`users access-role USER operator`	将用户角色 operator 分配给用户帐户 USER。
`users enable USER`	激活用户帐户 USER。
`show users`	显示已经设置的用户帐户。
`save`	将设置保存到永久存储器 (nvm) 的“选定”配置概要文件中。

提示：在命令行界面中设置新的用户帐户时，请记得分配密码。

3.4.6 停用用户帐户

用户帐户被停用后，设备会拒绝相关用户访问设备管理。与完全删除帐户不同，停用一个用户帐户后，可以保留设置以便将来重新使用。为此，请执行以下步骤：

☐ 要保留用户帐户设置并在将来重新使用，可以暂时停用用户帐户。

- ☐ 打开 *Device Security > User Management* 对话框。
  该对话框显示已经设置的用户帐户。
- ☐ 在相关用户帐户的行中，取消勾选 *Active* 列中的复选框。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`users disable <user>`	禁用用户帐户。
`show users`	显示已经设置的用户帐户。
`save`	将设置保存到永久存储器（nvm）的“选定”配置概要文件中。

☐ 要永久停用用户帐户设置，可以删除该用户帐户。

☐ 突出显示相关用户帐户的行。

☐ 点击 按钮。

`users delete <user>`	删除用户帐户 <user>。
`show users`	显示已经设置的用户帐户。
`save`	将设置保存到永久存储器（nvm）的“选定”配置概要文件中。

3.4.7 调整密码策略

设备允许用户检查用户帐户的密码是否符合指定的策略。当密码符合策略时，可以获得复杂度更高的密码。

设备的用户管理允许用户在每个用户帐户中分别激活或停用检查。当勾选了复选框且新的密码符合策略要求时，设备会接受密码更改。

在默认设置下，设备中设置了策略的实际值。可以选择调整策略使之符合您的要求。为此，请执行以下步骤：

☐ 调整密码策略，使之符合您的要求。

☐ 打开 *Device Security > User Management* 对话框。

在 *Configuration* 框中，可以指定设备锁定用户之前用户登录尝试次数。还可以指定定义密码的最小字符数。

提示：设备只允许具有 *administrator* 权限的用户解除锁定。

仅当通过以下方式访问设备管理时，登录尝试次数以及可能的用户锁定才适用：

- 图形用户界面
- SSH 协议
- Telnet 协议

提示：当通过串行连接使用命令行界面来访问设备管理时，登录尝试的次数为无限。

☐ 指定符合您要求的数值。

- I可以在 *Login attempts* 字段中指定用户尝试登录的次数。该字段允许用户将此值定义在 0..5 范围内。
  在以上示例中，值 0 可停用该功能。
- *Min. password length* 字段允许用户输入 1..64 范围内的值。

该对话框显示在 *Password policy* 框中设置的策略。

☐ 调整数值，使之符合您的要求。

▶ 允许 1 到 16 范围内的值。
值 0 可停用相关策略。

要应用 *Configuration* 和 *Password policy* 框中指定的条目，请为某个特定用户勾选 *Policy check* 列中的复选框。

☐ 暂时保存更改。为此，请单击  按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`passwords min-length 6`	指定密码最小长度策略。
`passwords min-lowercase-chars 1`	指定密码中小写字母最小数量策略。
`passwords min-numeric-chars 1`	指定密码中位数最小数量策略。
`passwords min-special-chars 1`	指定密码中特殊字符最小数量策略。
`passwords min-uppercase-chars 1`	指定密码中大写字母最小数量策略。
`show passwords`	显示已经设置的策略。
`save`	将设置保存到永久存储器（nvm）的“选定”配置概要文件中。

3.5 LDAP

服务器管理员管理其中包含在办公环境中使用的应用程序的用户登录凭证的 Active Directory。Active Directory 本质上是分层的，其中包含用户名、密码以及每个用户的授权读/写权限级别。

此设备使用轻量级目录访问协议 (LDAP) 从 Active Directory 检索用户登录信息和权限级别。这为网络设备提供了“单点登录”。如果从 Active Directory 检索登录凭证，则允许用户使用在办公环境中使用的相同登录凭证登录。

LDAP 会话从设备与目录系统代理 (DSA) 通信以搜索 LDAP 服务器的 Active Directory 开始。如果服务器在用户的 Active Directory 中找到多个条目，则服务器将发送找到的更高权限级别。DSA 监听信息请求，并通过 SSL (LDAPS) 在 LDAP 的 TCP 端口 389 或 LDAP 的 TCP 端口 636 上发送响应。客户端和服务器使用基本编码规则 (BER) 对 LDAPS 请求和响应进行编码。设备会为每个请求打开一个新连接，并在收到来自服务器的响应后关闭该连接。

设备允许用户上传 CA 证书，以验证服务器的安全套接字级别 (SSL) 和传输层安全性 (TLS) 会话。因此，该证书对于 TLS 会话为可选。

设备在存储器中最多可以缓存 1024 个用户的登录凭证。如果无法访问活动目录服务器，则用户仍然可以使用其办公登录凭证登录。

3.5.1 请与服务器管理员协调

配置 *LDAP* 功能需要网络管理员向服务器管理员请求以下信息：

- 服务器名称或 IP 地址
- 服务器上 Active Directory 的位置
- 使用的连接类型
- TCP 监听端口
- 需要时，CA 证书的位置
- 包含用户登录名的属性名称
- 包含用户权限级别的属性名称

服务器管理员可以使用诸如 description 之类的属性来单独分配权限级别，也可以使用 memberOf 属性来为组分配权限级别。用户可在 *Device Security > LDAP > Role Mapping* 对话框中指定接收各种权限级别的属性。

用户还可以选择使用 LDAP 浏览器（例如 JXplorer 或 Softerra）检索包含用户登录名和权限级别的属性名称。

3.5.2 配置示例

设备仅使用服务器名称即可建立到本地服务器的加密链路，也可以使用 IP 地址建立到不同网络上的服务器的加密链路。服务器管理员使用属性来识别用户的登录凭证并分配单个和组权限级别。

使用从服务器管理员接收的信息，指定 Active Directory 中包含用户登录凭证和权限级别的属性。然后，设备将用户登录凭证与设备中指定的权限级别进行比较，从而允许用户以分配的权限级别登录。

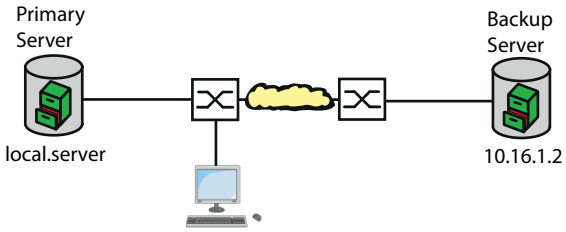


图 18: LDAP 示例配置

在本示例中，服务器管理员已发送以下信息：

信息	Primary Server	Backup Server
服务器名称或 IP 地址	local.server	10.16.1.2
服务器上 Active Directory 的位置	国家/城市/用户	国家/公司/用户
使用的连接类型	TLS（含证书）	SSL
服务器管理员已通过电子邮件发送 CA 证书。	本地保存的主服务器 CA 证书	本地保存的备份服务器 CA 证书
TCP 监听端口	389 (tls)	636 (ssl)
包含用户名的属性名称	userPrincipalName	userPrincipalName
包含用户权限级别的属性名称	OPERATOR ADMINISTRATOR	OPERATOR ADMINISTRATOR

请执行以下步骤：

- ☐ 打开 *Device Security > Authentication List* 对话框。
- ☐ 要配置设备以检索用户登录凭证，请在使用图形用户界面登录期间，首先从 Active Directory 中为 defaultLoginAuthList 列表指定 *Policy 1* 列中的值 ldap。
- ☐ 打开 *Device Security > LDAP > Configuration* 对话框。
- ☐ 设备允许用户指定将用户登录凭证保存在缓存中的时长。要将用户登录凭证缓存一天时间，请在 *Configuration* 框的 *Client cache timeout [min]* 字段中输入值 1440。
- ☐ *Bind user* 条目为可选。指定后，用户仅输入其用户名即可登录。服务用户可以是具有在 Active Directory 中在 *User name attribute* 列中指定的属性下列出的登录凭证的任何人。在 *Bind user* 列中，输入用户名和域。
- ☐ *Base DN* 是域组件 (dc) 与组织单元 (ou) 的组合。*Base DN* 可使设备在域 (dc) 中找到服务器并找到 Active Directory (ou)。指定 Active Directory 的位置。在 *Base DN* 列中，指定值 ou=Users,ou=City,ou=Country,dc=server,dc=local。
- ☐ 在 *User name attribute* 列中，输入值 userPrincipalName 以指定服务器管理员在其下列出用户的属性。

设备使用 CA 证书来验证服务器。

- ☐ 当证书位于用户 PC 中或网络驱动器上时，将该证书拖放到 区域中。也可点击该区域内部选择该证书。
- ☐ 要将 CA 证书传输到设备上，请点击 *Start* 按钮。
- ☐ 要添加一个表格条目，请点击 按钮。
- ☐ 要指定描述，请在 *Description* 列中输入值 Primary AD Server。
- ☐ 要指定主服务器的服务器名称和域，请在 *Address* 列中输入值 local.server。
- ☐ 主服务器使用 TCP 端口 389 进行通信，这是 *Destination TCP port* 默认值。
- ☐ 主服务器使用 TLS 进行加密通信，并使用 CA 证书进行服务器验证。在 *Connection security* 列中，指定值 startTLS。
- ☐ 要激活该条目，请勾选 *Active* 列中的复选框。
- ☐ 使用从服务器管理员接收的有关备份服务器的信息，添加、配置并激活另一行。

- ☐ 打开 *Device Security* > *LDAP* > *Role Mapping* 对话框。
- ☐ 要添加一个表格条目，请点击 按钮。

当用户使用配置并启用的 LDAP 进行登录时，设备会在 Active Directory 中搜索该用户的登录凭证。如果设备找到用户名并且密码正确无误，则设备将搜索在 *Type* 列中指定的值。如果设备找到该属性，并且 *Parameter* 列中的文本与 Active Directory 中的文本相匹配，则设备允许用户以分配的权限级别登录。在 *Type* 列中指定 attribute 值后，请以如下形式在 *Parameter* 列中指定该值：attributeName=attributeValue

- ☐ 在 *Role* 列中，输入 operator 值以指定用户角色。
- ☐ 要激活该条目，请勾选 *Active* 列中的复选框。
- ☐ 点击 按钮。
  该对话框显示 *Create* 窗口。
  输入从服务器管理员接收的用于 administrator 角色的值。
  要激活该条目，请勾选 *Active* 列中的复选框。
- ☐ 打开 *Device Security* > *LDAP* > *Configuration* 对话框。
- ☐ 要启用该功能，请选择 *Operation* 框中的 *On* 单选按钮。

下表描述了如何使用命令行界面在设备中配置 *LDAP* 功能。该表显示了 Index 1 的命令。要配置 Index 2，请使用相同的命令并替换相应的信息。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`ldap cache-timeout 1440`	指定一天后要清除永久存储器的设备。
`ldap client server add 1 local.server port 389`	将连接添加到主机名称为 local.server 且 UDP 端口为 389 的远程身份验证客户端服务器。
`ldap client server modify 1 security startTLS`	指定用于连接的安全类型。
`ldap client server modify 1 description Primary_AD_Server`	指定条目的配置名称。
`ldap basedn ou=Users,ou=City,ou=Country,dc=server,dc=local`	指定用于在服务器上查找 Active Directory 的基本域名。
`ldap search-attr userPrincipalName`	在包含用户登录凭证的 Active Directory 中指定要搜索的属性。
`ldap bind-user user@company.com`	指定服务用户的名称和域。

`ldap bind-passwd Ur-123456`	指定服务用户的密码。
`ldap client server enable 1`	启用远程身份验证客户端服务器连接。
`ldap mapping add 1 access-role operator mapping-type attribute mapping-parameter OPERATOR`	为 Operator 角色添加远程身份验证角色映射条目。将 operator 角色映射到包含 OPERATOR 一词的属性。
`ldap mapping enable 1`	启用远程身份验证角色映射条目。
`ldap operation`	启用远程身份验证功能。

3.6 SNMP 访问

SNMP 协议允许用户使用网络管理系统通过网络对设备进行监控，并更改其设置。

3.6.1 SNMPv1/v2 访问

使用 SNMPv1 或 SNMPv2，网络管理系统与设备进行不加密通信。每个 SNMP 数据包都包含明文团体名称以及发送者的 IP 地址。

设备中预设了具有读权限的团体名称 user 和具有写权限的团体名称 admin。如果 SNMPv1/v2 已启用，则设备允许知道团体名称的任何人访问设备。

提高越权访问设备的难度。为此，请执行以下步骤：

- ☐ 更改设备中的默认团体名称。
  请谨慎处理团体名称。
  知道具有写权限的团体名称的任何人均可更改设备的设置。
- ☐ 为读/写权限指定与读权限不同的团体名称。
- ☐ 只在具有窃听保护的环境中使用 SNMPv1 或 SNMPv2。这些协议不使用加密。
- ☐ 我们建议在设备中使用 SNMPv3 并禁用使用 SNMPv1 和 SNMPv2 的访问。

3.6.2 SNMPv3 访问

使用 SNMPv3，网络管理系统与设备进行加密通信。网络管理系统使用一个用户的登录凭证向设备进行自我身份验证。SNMPv3 访问的前提条件是，网络管理系统使用设备中定义的相同设置。

设备允许用户在每个用户帐户中分别指定 *SNMP auth type* 和 *SNMP encryption type* 参数。

在设备中设置新的用户帐户时，这些参数均已预设，因此，网络管理系统 ConneXium Network Manager 可以立即访问设备。

设备中设置的用户帐户在图形用户界面、命令行界面和 SNMPv3 中使用相同的密码。

要将用户帐户设置的 SNMPv3 参数调整为您网络管理系统中的设置，请执行以下步骤：

- ☐ 打开 *Device Security > User Management* 对话框。

该对话框显示已经设置的用户帐户。

- ☐ 点击 *SNMP auth type* 字段中相关用户帐户的行。选择所需设置。
- ☐ 点击 *SNMP encryption type* 字段中相关用户帐户的行。选择所需设置。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`users snmpv3 authentication <user> md5 | sha1`	将用于身份验证请求的 HMAC-MD5 或 HMACSHA 协议分配给 <user> 用户帐户。

users snmpv3 encryption <user> des | aescfb128 | none	将 DES 或 AES-128 算法分配给 <user> 用户帐户。借助此算法，设备对身份验证请求进行加密。值 none 可取消加密。
show users	显示已经配置的用户帐户。
save	将设置保存到永久存储器 (nvm) 的“选定”配置概要文件中。

3.7 Out of Band 访问

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

前提条件是将管理站直接连接到 USB 端口。使用 Microsoft Windows 时，如有必要，请安装 RNDIS 驱动程序。管理站一经连接即可通过虚拟网络连接与设备管理通信。

在默认设置下，您可以使用以下 IP 参数，通过此端口访问设备管理：
- *IP address* 91.0.0.100
- *Netmask* 255.255.255.0

设备允许您使用以下协议访问设备管理：
- SNMP
- Telnet
- SSH
- HTTP
- HTTPS
- FTP
- SCP
- TFTP
- SFTP

3.7.1 指定 IP 参数

通过 USB 端口连接管理站时，设备会将 USB 网络接口的 IP 地址增加 1 后分配给管理站（默认设置中为 91.0.0.101）。设备允许您更改 IP 参数，以使设备适应您的环境要求。

验证此网络接口的 IP 子网与连接到设备另一个接口的任何子网是否不重叠：
- 管理接口

如果管理站通过 USB 端口访问设备管理，则设备会在您执行更改后立即断开图形用户界面和命令行界面。

请执行以下步骤：

- ☐ 打开 *Basic Settings* > *Out of Band over USB* 对话框。
- ☐ 覆盖 *IP parameter* 框的 *IP address* 字段中的 IP 地址。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`enable`	切换到特权执行模式。
`network usb parms 192.168.1.1 255.255.255.0`	为 USB 网络接口指定 IP 地址 192.168.1.1 和子网掩码 255.255.255.0。

```
show network usb                                显示 USB 网络接口设置。
Out-of-band USB management settings
-----------------------------------
Management operation.....................enabled
IP address...............................192.168.1.1
Subnet mask..............................255.255.255.0
Host MAC address.........................64:60:38:1f:85:85
Device MAC address.......................64:60:38:1f:85:86

save                                            将设置保存到永久存储器（nvm）的“选定”配置
                                                概要文件中。
```

3.7.2 禁用 USB 网络接口

在默认设置下，USB 网络接口已启用。如果您不希望有人通过 USB 端口访问设备管理，设备允许您禁用 USB 网络接口。

如果管理站通过 USB 端口访问设备管理，则设备会在您执行更改后立即断开图形用户界面和命令行界面。

请执行以下步骤：

- ☐ 打开 *Basic Settings > Out of Band over USB* 对话框。
- ☐ 要禁用 USB 网络接口，请选择 *Operation* 框中的 *Off* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

```
enable                                          切换到特权执行模式。
no network usb operation                        禁用 USB 网络接口。
Out-of-band USB management settings
-----------------------------------
Management operation.....................disabled
IP address...............................192.168.1.1
Subnet mask..............................255.255.255.0
Host MAC address.........................64:60:38:1f:85:85
Device MAC address.......................64:60:38:1f:85:86

save                                            将设置保存到永久存储器（nvm）的“选定”配置
                                                概要文件中。
```

4 同步网络中的系统时间

很多应用程序都依赖于尽可能正确的时间。必要的精度以及因此允许的与实际时间的偏差视应用领域而定。

应用领域的例子包括：
- 日志条目
- 为生产数据标注时间戳
- 过程控制

设备允许用户使用以下选项对网络上的时间进行同步：
- 简单网络时间协议（SNTP）是一种针对较低精度要求的简单解决方案。在理想条件下，SNTP 可实现毫秒范围的精度。精度取决于信号延迟。
- IEEE 1588 利用精确时间协议（PTP）达到亚微秒范围内的准确性。即使是要求严苛的应用程序，包括过程控制，这种方法均可适用。

当涉及的设备支持 PTP 协议时，PTP 是更好的选择。因为 PTP 更准确，纠正错误的方法更高级，造成的网络负载更低。而且 PTP 的执行相对更简单。

提示：根据 PTP 和 SNTP 标准，网络中可同时存在两种协议功能。然而，两种协议均会影响设备的系统时间，因此，可能出现两种协议冲突的情况。

4.1 基本设置

在 *Time > Basic Settings* 对话框中，可以指定时间的一般设置。

4.1.1 设置时间

当没有基准时间源可用时，可以选择在设备中设置时间。

在冷启动或重新启动之后，如果没有实时时钟可用或实时时钟包含无效时间，则设备会以 1 月 1 日 00:00h 对其时钟进行初始化。在电源关闭之后，设备会缓冲 24 小时以内的实时时钟设置。

此外，还可以对设备中的设置进行配置，使设备自动从 PTP 时钟或 SNTP 服务器获取当前时间。

此外，还可以对设备中的设置进行配置，使设备自动从一个 SNTP 服务器获取当前时间。

请执行以下步骤：

☐ 打开 *Time > Basic Settings* 对话框。

- *System time (UTC)* 字段显示设备的当前 UTC（协调世界时）。UTC 是与协调世界时间测量相关的时间。UTC 在全世界都是相同的，不会考虑本地时间偏移。
- *System time* 字段中的时间等于 *System time (UTC)* 加 *Local offset [min]* 值，再加上夏令时导致的可能的偏移。

提示：PTP 发送国际原子时间（TAI）。截至 2020 年 7 月 1 日，TAI 时间比 UTC 时间快 37 秒。在正确设置 UTC 偏移量的 PTP 参考时间源后，设备会自动纠正显示屏上 *System time (UTC)* 字段中的这一偏差。

- ☐ 为了使设备将您 PC 的时间应用到 *System time* 字段，请点击 *Set time from PC* 按钮。
  根据 *Local offset [min]* 字段中的值，设备会计算 *System time (UTC)* 字段中的时间：*System time (UTC)* 等于 *System time* 减 *Local offset [min]* 值，再减去夏令时导致的可能的偏移。
- ▶ *Time source* 字段显示时间数据的来源。设备会自动选择精度最高的时间源。
  时间源最初是 local。
  当 SNTP 已激活且设备接收到一个有效的 SNTP 数据包时，设备会将其时间源设置为 sntp。
  当 PTP 已激活且设备接收到有效的 PTP 消息时，设备会将其时间源设置为 ptp。PTP 的优先级高于 SNTP。
- ▶ *Local offset [min]* 值指定本地时间与 *System time (UTC)* 之间的时间差。
- ☐ 为了使设备确定您 PC 上的时区，请点击 *Set time from PC* 按钮。设备会计算与 UTC 之间的本地时间差并将该时间差输入到 *Local offset [min]* 字段中。

提示：设备提供了从 DHCP 服务器获取本地偏移量的选项。

- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`clock set <YYYY-MM-DD> <HH:MM:SS>`	设置设备的系统时间。
`clock timezone offset <-780..840>`	输入本地时间和收到的 UTC 时间之间的时间差（分钟）。
`save`	将设置保存到永久存储器（nvm）的“选定”配置概要文件中。

4.1.2 自动夏令时转换

当您在一个有夏季时间变化的时区操作设备时，可以在 *Daylight saving time* 选项卡上设置自动夏令时转换。

当夏令时启用时，设备会在夏令时开始时将本地系统时间向前设置 1 小时。夏令时结束时，设备会再次将本地系统时间向后设置 1 小时。为此，请执行以下步骤：

- ☐ 打开 *Time* > *Basic Settings* 对话框的 *Daylight saving time* 选项卡。
- ☐ 要为夏令时开始和结束选择一个预设概要文件，请点击 *Operation* 框中的 *Profile...* 按钮。
- ☐ 当没有匹配的夏令时概要文件可用时，可以在 *Summertime begin* 和 *Summertime end* 字段中指定转换时间。
  针对这两个时间点，需要指定月份、该月份中的星期、星期几和一天中的时间。
- ☐ 要启用该功能，请选择 *Operation* 框中的 *On* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`clock summer-time mode <disable|recurring|eu|usa>`	配置自动夏令时转换：使用一个概要文件启用/禁用或激活。

`clock summer-time recurring start`	输入转换的开始时间。
`clock summer-time recurring end`	输入转换的结束时间。
`save`	将设置保存到永久存储器（nvm）的“选定”配置概要文件中。

4.2 SNTP

简单网络时间协议（SNTP）允许用户对网络中的系统时间进行同步。设备支持 SNTP 客户端和 SNTP 服务器功能。

SNTP 服务器提供 UTC（协调世界时）。UTC 是与协调世界时间测量相关的时间。UTC 在全世界都是相同的，它会忽略本地时间偏移。

SNTP 是 NTP（网络时间协议）的一个简化版本。SNTP 和 NTP 的数据包完全相同。因此，NTP 和 SNTP 服务器均可作为 SNTP 客户端的时间源。

提示：本章中与外部 SNTP 服务器相关的陈述也适用于 NTP 服务器。

SNTP 知道针对时间传输的以下运行模式：

- *Unicast*
  在 *Unicast* 运行模式下，一个 SNTP 客户端向一个 SNTP 服务器发送请求，并希望获得来自此服务器的响应。
- *Broadcast*
  在 *Broadcast* 运行模式下，一个 SNTP 服务器以指定间隔向网络发送 SNTP 消息。SNTP 客户端会接收这些 SNTP 消息并对其进行评估。

在 IPv6 环境中，*Broadcast* 运行模式的工作方式如下：

- SNTP 客户端仅监听那些将设置为 ff05::101 的 IPv6 *Multicast* 地址作为 IPv6 目标地址的 SNTP 服务器消息。
- SNTP 服务器仅向 *Multicast* 地址 ff05::101 发送 SNTP 消息。SNTP 服务器不会发送链路本地地址为 IPv6 源地址的 SNTP 消息。

表格 16: Broadcast 运行模式的目标 IPv4 地址类别

IPv4 目标地址	发送 SNTP 数据包至
0.0.0.0	无人
224.0.1.1	SNTP 消息的 *Multicast* 地址
255.255.255.255	*Broadcast* 地址

提示：*Broadcast* 运行模式下的 SNTP 服务器还可使用 *Unicast* 对来自 SNTP 客户端的直接请求作出响应。与此相反，SNTP 客户端在 *Unicast* 或 *Broadcast* 运行模式下工作。

4.2.1 准备

请执行以下步骤：

☐ 为了简单了解时间的传递方式，可以使用参与 SNTP 的设备绘制一份网络规划图。
绘制规划图时，请记住，时间精度取决于 SNTP 消息的延迟。为了最大限度减少延迟及其偏差，请在每个网段中放置一个 SNTP 服务器。其中每个 SNTP 服务器都作为一个 SNTP 客户端将其自己的系统时间与其上级 SNTP 服务器进行同步（SNTP 级联）。SNTP 级联中级别最高的 SNTP 服务器对基准时间源的访问最直接。

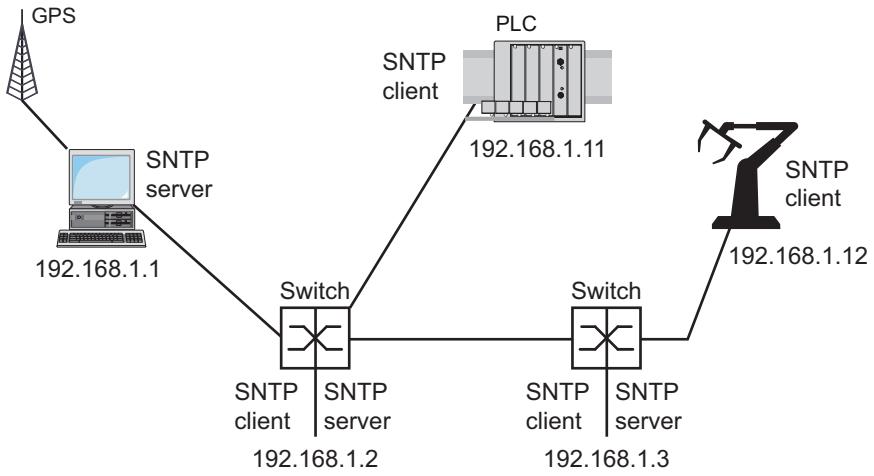


图 19: SNTP 级联示例

提示：为实现精确的时间分布，在 SNTP 服务器和 SNTP 客户端之间，最好使用以较短、较均匀的传输时间（延时）转发 SNTP 数据包的网络组件（路由器和交换机）。

▶ 一个 SNTP 客户端可向最多 4 个已配置的 SNTP 服务器发送请求。当第一个 SNTP 服务器没有响应时，SNTP 客户端会向第二个 SNTP 服务器发送请求。当此请求也失败时，它会向第三个、最后向第四个 SNTP 服务器发送请求。如果这些 SNTP 服务器都没有响应，则 SNTP 客户端失去同步。SNTP 客户端定期向每个 SNTP 服务器发送请求，直到某个服务器交付一个有效时间为止。

提示：设备提供了从 DHCP 服务器获取 SNTP 服务器 IP 地址列表的选项。

☐ 如果没有基准时间源可用，则可将一台带有 SNTP 服务器的设备确定为基准时间源。请定期调整其系统时间。

4.2.2 定义 SNTP 客户端的设置

作为 SNTP 客户端，设备从 SNTP 或 NTP 服务器获得时间信息，并相应对其系统时钟进行同步。为此，请执行以下步骤：

☐ 打开 *Time* > *SNTP* > *Client* 对话框。

☐ 设置 SNTP 运行模式。
在 *Configuration* 框中，选择 *Mode* 字段中的以下值之一：
▶ unicast
设备向一个 SNTP 服务器发送请求，并希望获得来自此服务器的响应。
▶ broadcast
设备等待来自网络上 SNTP 服务器的 *Broadcast* 或 *Multicast* 消息。

☐ 要对时间只进行一次同步，请勾选 *Disable client after successful sync* 复选框。
同步后，设备会禁用 *SNTP Client* 功能。

▶ 表中显示了 SNTP 客户端在 *Unicast* 运行模式下向其发送请求的 SNTP 服务器。表中包含了最多 4 个 SNTP 服务器定义。

☐ 要添加一个表格条目，请点击  按钮。

☐ 指定 SNTP 服务器的连接数据。

☐ 要启用该功能，请选择 *Operation* 框中的 *On* 单选按钮。

☐ 暂时保存更改。为此，请单击  按钮。

▶ *State* 字段显示 *SNTP Client* 功能的当前状态。

表格 17: 针对示例的 SNTP 客户端设置

设备	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
SNTP Client 功能	*Off*	*On*	*On*	*On*	*On*
Configuration: *Mode*	unicast	unicast	unicast	unicast	unicast
Request interval [s]	30	30	30	30	30
SNTP Server 地址	-	192.168.1.1	192.168.1.219 2.168.1.1	192.168.1.219 2.168.1.1	192.168.1.319 2.168.1.2192. 168.1.1

4.2.3 指定 SNTP 服务器设置

当设备作为 SNTP 服务器工作时，它会以网络中的协调世界时 (UTC) 提供其系统时间。为此，请执行以下步骤：

- ☐ 打开 *Time* > *SNTP* > *Server* 对话框。
- ☐ 要启用该功能，请选择 *Operation* 框中的 *On* 单选按钮。
- ☐ 要启用 *Broadcast* 运行模式，请选择 *Configuration* 框中的 *Broadcast admin mode* 单选按钮。
  在 *Broadcast* 运行模式下，SNTP 服务器以指定间隔向网络发送 SNTP 消息。在 *Unicast* 运行模式下，SNTP 服务器还对来自 SNTP 客户端的请求作出响应。
  - ☐ 在 *Broadcast destination address* 字段中，可以设置 SNTP 服务器向其发送 SNTP 数据包的 IPv4 地址。设置一个 *Broadcast* 地址或一个 *Multicast* 地址。
    在 IPv6 环境中，可以设置 SNTP 服务器向其发送 SNTP 数据包的 IPv6 地址。SNTP 服务器使用 *Multicast* 地址 ff05::101 作为 IPv6 目标地址。
  - ☐ 在 *Broadcast UDP port* 字段中，可以指定 SNTP 服务器在 *Broadcast* 运行模式下向其发送 SNTP 数据包的 UDP 端口的编号。
  - ☐ 在 *Broadcast VLAN ID* 字段中，可以指定 SNTP 服务器在 *Broadcast* 运行模式下向其发送 SNTP 数据包的 VLAN 的 ID。
  - ☐ 在 *Broadcast send interval [s]* 字段中，可以输入设备的 SNTP 服务器发送 SNTP *Broadcast* 数据包的时间间隔。

提示：除 *Broadcast destination address* 字段外，剩余设置对 IPv4 和 IPv6 SNTP 服务器均适用。

- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。
- ▶ *State* 字段显示 *SNTP Server* 功能的当前状态。

表格 18: 示例设置

设备	192.168.1.1	192.168.1.2	192.168.1.3	192.168.1.11	192.168.1.12
SNTP Server 功能	*On*	*On*	*On*	*Off*	*Off*
UDP port	123	123	123	123	123
Broadcast admin mode	未勾选	未勾选	未勾选	未勾选	未勾选
Broadcast destination address	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0
Broadcast UDP port	123	123	123	123	123
Broadcast VLAN ID	1	1	1	1	1
Broadcast send interval [s]	128	128	128	128	128
Disable server at local time source	未勾选	未勾选	未勾选	未勾选	未勾选

4.3 PTP

为使 LAN 控制应用程序不出现延迟，则需要精确的时间管理。使用 PTP（精确时间协议）时，IEEE 1588 描述了一种方法，可以实现网络中时钟的精确同步。

PTP 可以使同步精确到数百 ns。PTP 将 Multicasts 用于同步消息，可以保持较低的网络负载。

4.3.1 时钟类型

PTP 定义了网络中时钟的“主/从”角色。

- 主时钟（基准时间源）分发时间。
- 从时钟将其时间与从主时钟接收的时间信号进行同步。

边界时钟

路由器和交换机中的传输时间（延迟）对时间传输的精度具有显著影响。为纠正这种不准确性，PTP 定义了所谓的边界时钟。

在网段中，边界时钟是下级从时钟同步的基准时间源（主时钟）。通常由路由器和交换机担任边界时钟的角色。

反之，边界时钟同时也从更高级的基准时间源（最优主时钟）获取时间。

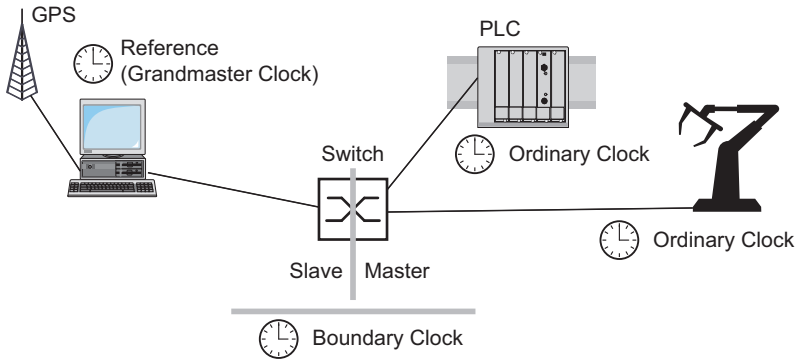


图 20: 边界时钟在网络中的位置

Transparent Clock

通常由交换机担任 Transparent Clock 的角色，以在级联中实现较高的准确性。Transparent Clock 属于 Slave 时钟，可以在转发收到的同步消息时纠正自己的传输时间。

Ordinary Clock

PTP 将终端设备中的时钟指定为“Ordinary Clock”。Ordinary Clock 可以作为主时钟或从时钟。

4.3.2 最佳主时钟算法

参与 PTP 的设备将网络中的一个设备指定为基准时间源（最优主时钟）。此处使用“Best Master Clock”算法，用于确定网络中可用时钟的准确性。

“Best Master Clock”算法用于评估以下标准：
- *Priority 1*
- *Clock class*
- *Clock accuracy*
- *Clock variance*
- *Priority 2*

算法首先评估参与设备的 *Priority 1* 字段中的值。*Priority 1* 字段中值最小的设备将成为基准时间源 (Grandmaster)。如果该值对于多个设备都是相同的，则算法采用下一个标准。如果下一个值也相同，则再采用下一个标准。如果这些值对于多个设备都相同，则 *Clock identity* 字段中最小的值将决定哪个设备成为基准时间源 (Grandmaster)。

在边界时钟的设置中，设备允许用户单独指定 *Priority 1* 和 *Priority 2* 的值。这样用户就可以参与决定将网络中的哪个设备指定为基准时间源 (Grandmaster)。

4.3.3 延迟测量

设备间同步消息的延迟会影响准确性。延迟测量可以让设备将平均延迟考虑在内。

PTP 版本 2 提供以下几种延迟测量方法：
- *e2e* (End to End)
  从时钟可测量同步消息到主时钟的延迟。
- *e2e-optimized*
  从时钟可测量同步消息到主时钟的延迟。
  此方法仅可用于透明时钟。设备使用 Multicast 仅将发送的同步消息转发至主时钟，将网络负载保持在较低水平。当设备从另一个主时钟接收到同步消息时，设备仅将同步消息转发至此新端口。
  当设备没有主时钟时，则将同步消息转发至所有端口。
- *p2p* (Peer to Peer)
  从时钟可测量同步消息到主时钟的延迟。
  此外，主时钟还会测量到每个从时钟的延迟，甚至通过被阻塞端口。这需要主从时钟支持点对点 (*p2p*)。
  例如，在冗余环中断的情况下，从时钟成为主时钟，而主时钟成为从时钟。发生此转换时不会丧失精度，因为时钟已经考虑到在另一个方向中的延迟。

4.3.4 PTP 域

只有处于同一个 PTP 域中的设备之间会相互传输同步消息。设备允许用户为边界时钟和透明时钟分别建立域。

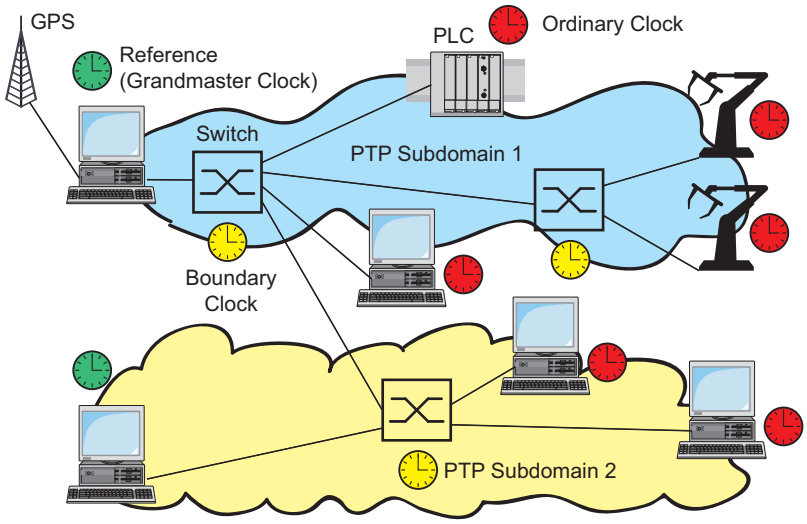


图 21: PTP 域示例

4.3.5 使用 PTP

为使用 PTP 精确同步时钟，请仅使用具有边界时钟或透明时钟的交换机作为节点。

请执行以下步骤：

- ☐ 要获得时钟分布的概览，请使用 PTP 中涉及的设备绘制网络规划。
- ☐ 为每台参与的交换机指定角色（边界时钟或透明时钟）。在设备中，此设置称为 *PTP mode*。

表格 19: PTP 模式的可行设置

PTP 模式	应用
v2-boundary-clock	对于边界时钟，设备将同步消息分发至下级网段的从时钟。 反之，边界时钟同时也从更高级的基准时间源（最优主时钟）获取时间。
v2-transparent-clock	对于透明时钟，接收到的同步消息经过透明时钟延迟纠正后，设备再其转发。

- ☐ 在每台参与的交换机上启用 PTP。
  随后 PTP 将在很大程度上自动进行配置。
- ☐ 启用终端设备上的 PTP。
- ☐ 设备允许用户参与决定将网络中的哪个设备指定为参考时钟（最优主时钟）。因此，请更改 *Boundary ClockPriority 1* 和 *Priority 2* 字段的默认值。

5 管理配置概要文件

如果在操作过程中更改设备的设置，则设备会将更改存储到其存储器中（*RAM*）。重新启动后，设置将丢失。

为了在重新启动后保留更改，设备允许用户将设置保存在永久存储器（*NVM*）中的配置概要文件中。为了能够快速切换到其他设置，永久存储器会为多个配置概要文件提供存储空间。

如果连接了一个外部存储器，则设备会自动在外部存储器（*ENVM*）中保存配置概要文件的副本。可以禁用此功能。

5.1 检测更改的设置

设备将操作期间对设置进行的更改存储到其非永久性存储器（*RAM*）中。永久存储器（*NVM*）中的配置概要文件一直保持不变，直到您明确保存已更改的设置为止。在此之前，存储器和永久存储器中的配置概要文件不同。设备可帮助用户识别更改的设置。

5.1.1 非永久存储器（RAM）和永久存储器（NVM）

您可以识别非永久存储器（*RAM*）中的配置概要文件何时与永久存储器（*NVM*）中的“选定”配置概要文件不同。为此，请执行以下步骤：

- ☐ 检查菜单顶部的状态栏：
  - 当闪烁的  图标可见时，配置概要文件不同。
  - 当  图标不可见时，配置概要文件匹配。

或：

- ☐ 打开 *Basic Settings > Load/Save* 对话框。
- ☐ 检查 *Information* 框中的复选框的状态。
  - 当复选框未勾选时，配置概要文件不同。
  - 当复选框已勾选时，配置概要文件匹配。

```
show config status

Configuration Storage sync State
--------------------------------
running-config to NV.......................out of sync
...
```

5.1.2 外部存储器 (EAM) 和永久存储器 (NVM)

您还可以识别外部存储器 (EAM) 中的副本何时与永久存储器 (*NVM*) 中的“选定”配置概要文件不同。为此，请执行以下步骤：

- ☐ 打开 *Basic Settings* > *Load/Save* 对话框。
- ☐ 检查 *Information* 框中的复选框的状态。
  - 当复选框未勾选时，配置概要文件不同。
  - 当复选框已勾选时，配置概要文件匹配。

```
show config status

Configuration Storage sync State
--------------------------------
...
NV to EAM.................................out of sync
...
```

5.2 保存设置

5.2.1 保存设备中的配置概要文件

如果在操作过程中更改设备的设置，则设备会将更改存储到其存储器中（RAM）。为了在重新启动后保留更改，请将配置概要文件保存到永久存储器（*NVM*）中。

保存配置概要文件

设备将“选定”配置概要文件中的设置存储在永久存储器（*NVM*）中。

请执行以下步骤：

- ☐ 打开 *Basic Settings > Load/Save* 对话框。
- ☐ 验证所需的配置概要文件是否为“选定”。
  可以识别“选定”配置概要文件，因为 *Selected* 列中的复选框为勾选。
- ☐ 点击  按钮。

`show config profiles nvm`	显示永久存储器（nvm）中包含的配置概要文件。
`enable`	切换到特权执行模式。
`save`	将设置保存到永久存储器（nvm）的“选定”配置概要文件中。

将设置复制到配置概要文件

设备允许用户将存储器（RAM）中保存的设置存储到与“选定”配置概要文件不同的配置概要文件中。通过这种方式，可以在永久存储器（*NVM*）中创建一个新的配置概要文件或覆盖现有的配置概要文件。

请执行以下步骤：

- ☐ 打开 *Basic Settings > Load/Save* 对话框。
- ☐ 点击  按钮，然后点击 *Save as..* 项目。
  该对话框显示 *Save as..* 窗口。
- ☐ 在 *Name* 字段中，更改配置概要文件的名称。如果保留建议的名称，设备将覆盖相同名称的现有配置概要文件。
- ☐ 点击 *Ok* 按钮。

新的配置概要文件被指定为“选定”。

`show config profiles nvm`	显示永久存储器（nvm）中包含的配置概要文件。
`enable`	切换到特权执行模式。
`copy config running-config nvm profile <string>`	将名称为 <string> 的配置概要文件中的当前设置保存到永久存储器（nvm）中。如果存在相同名称的配置概要文件，则设备会对其进行覆盖。新的配置概要文件被指定为“选定”。

选择配置概要文件

当永久存储器（*NVM*）包含多个配置概要文件时，可以选择其中的任何配置概要文件。设备将设置存储在“选定”配置概要文件中。重新启动时，设备会将“选定”配置概要文件的设置加载到存储器（RAM）中。

请执行以下步骤：

- ☐ 打开 *Basic Settings* > *Load/Save* 对话框。

  该表格显示设备中存在的配置概要文件。可以识别“选定”配置概要文件，因为 *Selected* 列中的复选框为勾选。
- ☐ 在该表格中，选择永久存储器（*NVM*）中存储的所需配置概要文件的条目。
- ☐ 点击 ☰ 按钮，然后点击 *Select* 项目。

  在 *Selected* 列中，该配置概要文件的复选框现在为勾选。

`enable`	切换到特权执行模式。
`show config profiles nvm`	显示永久存储器（nvm）中包含的配置概要文件。
`configure`	切换到配置模式。
`config profile select nvm 1`	配置概要文件的标识符。 记下该配置概要文件的相邻名称。
`save`	将设置保存到永久存储器（nvm）的“选定”配置概要文件中。

5.2.2 将配置概要文件保存到外部存储器中

当连接了外部存储器且保存了配置概要文件时，设备会自动将副本保存到 *Selected external memory* 中。在默认设置下，该功能为启用。可以禁用此功能。

请执行以下步骤：

- ☐ 打开 *Basic Settings* > *External Memory* 对话框。
- ☐ 勾选 *Backup config when saving* 列中的复选框，使设备能够在保存过程中自动将副本保存到外部存储器中。
- ☐ 要停用该功能，请取消勾选 *Backup config when saving* 列中的复选框。
- ☐ 暂时保存更改。为此，请单击 ✓ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`config envm config-save usb`	启用该功能。 保存配置概要文件时，设备会将副本保存到外部存储器中。 usb = 外部 USB 存储器
`save`	将设置保存到永久存储器（nvm）的“选定”配置概要文件中。

5.2.3 在远程服务器上备份配置概要文件

设备允许用户将配置概要文件自动备份到远程服务器。前提条件是用户在保存配置概要文件之前激活该功能。

将配置概要文件保存到永久存储器（*NVM*）中之后，设备会将一份副本发送到指定的 URL。

请执行以下步骤：

- ☐ 打开 *Basic Settings* > *Load/Save* 对话框。
  在 *Backup config on a remote server when saving* 框中，执行以下步骤：
- ☐ 在 *URL* 字段中，指定服务器以及所备份配置概要文件的路径和文件名。
- ☐ 点击 *Set credentials* 按钮。
  该对话框显示 *Credentials* 窗口。
- ☐ 输入在远程服务器上进行身份验证所需的登录凭证。
- ☐ 在 *Operation* 选项列表中，启用该功能。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`enable`	切换到特权执行模式。
`show config remote-backup`	检查该功能的状态。
`configure`	切换到配置模式。
`config remote-backup destination`	为配置概要文件备份输入目标 URL。
`config remote-backup username`	输入在远程服务器上进行身份验证的用户名。
`config remote-backup password`	输入在远程服务器上进行身份验证的密码。
`config remote-backup operation`	启用该功能。

如果向远程服务器进行的传输不成功，则设备会将此事件记录在日志文件（System Log）中。

5.2.4 导出配置概要文件

设备允许用户将配置概要文件作为 XML 文件保存到服务器上。如果使用图形用户界面，则可选择将该 XML 文件直接保存到您的 PC。

前提条件：
- 要将该文件保存到服务器上，您需要一个在网络上配置好的服务器。
- 要将该文件保存到 SCP 或 SFTP 服务器上，您还需要用于访问此服务器的用户名和密码。

请执行以下步骤：

- ☐ 打开 *Basic Settings > Load/Save* 对话框。
- ☐ 在该表格中，选择所需配置概要文件的条目。

将配置概要文件导出到您的 PC。为此，请执行以下步骤：

- ☐ 点击 *Profile name* 列中的链接。
- ☐ 选择存储位置并指定文件名。
- ☐ 点击 *Ok* 按钮。

该配置概要文件现在另存为指定位置的 XML 文件。

将配置概要文件导出到远程服务器。为此，请执行以下步骤：

- ☐ 点击 ☰ 按钮，然后点击 *Export...* 项目。
  该对话框显示 *Export...* 窗口。
- ☐ 在 *URL* 字段中，指定远程服务器上的文件 URL：
  - ☐ 要将该文件保存到 FTP 服务器上，请以如下形式指定该文件的 URL：
    `ftp://<??>:<??>@<IP ??>:<??>/<???>`
  - ☐ 要将该文件保存到 TFTP 服务器上，请以如下形式指定该文件的 URL：
    `tftp://<IP ??>/<??>/<???>`
  - ☐ 要将该文件保存到 SCP 或 SFTP 服务器上，请以如下任一形式指定该文件的 URL：
    `scp://` 或 `sftp://<??>:<??>@<IP ??>/<??>/<???>`
    `scp://` 或 `sftp://<IP ??>/<??>/<???>`
    点击 *Ok* 按钮后，设备会显示 *Credentials* 窗口。在此，可以输入 *User name* 和 *Password* 登录服务器。
- ☐ 点击 *Ok* 按钮。
  该配置概要文件现在另存为指定位置的 XML 文件。

`show config profiles nvm`	显示永久存储器 (nvm) 中包含的配置概要文件。
`enable`	切换到特权执行模式。
`copy config running-config remote tftp://<IP_address>/ <path>/ <file_name>`	将当前设置保存到 TFTP 服务器上。

```
copy config nvm remote  sftp://
<user_name>:<password>@<IP_address>/
<path>/<file_name>
```

将所选配置概要文件保存到 SFTP 服务器上的永久存储器（nvm）中。

```
copy config nvm  profile config3
remote tftp://<IP_address>/   <path>/
<file_name>
```

将配置概要文件 config3 保存到 TFTP 服务器上的永久存储器（nvm）中。

```
copy config nvm  profile config3
remote ftp://<IP_address>:<port>/
<path>/<file_name>
```

将配置概要文件 config3 保存到 FTP 服务器上的永久存储器（nvm）中。

5.3 加载设置

如果将多个配置概要文件保存到存储器中，则可以选择加载不同的配置概要文件。

5.3.1 激活配置概要文件

设备的永久存储器中可以包含多个配置概要文件。如果激活永久存储器（*NVM*）中存储的一个配置概要文件，则您立即更改设备中的设置。设备不需要重新启动。

请执行以下步骤：

- ☐ 打开 *Basic Settings* > *Load/Save* 对话框。
- ☐ 在该表格中，选择所需配置概要文件的条目。
- ☐ 点击 ☰ 按钮，然后点击 *Activate* 项目。

设备将设置复制到存储器（RAM）并与图形用户界面断开连接。设备立即使用配置概要文件的设置。

- ☐ 重新加载图形用户界面。
- ☐ 再次登录。

在 *Selected* 列中，之前激活的配置概要文件的复选框为勾选。

`show config profiles nvm`	显示永久存储器（nvm）中包含的配置概要文件。
`enable`	切换到特权执行模式。
`copy config nvm profile config3 running-config`	激活永久存储器（config3）中配置概要文件 nvm 的设置。 设备将设置复制到非永久性存储器并与命令行界面断开连接。设备立即使用配置概要文件 config3 的设置。

5.3.2 从外部存储器加载配置概要文件

如果连接了一个外部存储器，则设备在重新启动时会从外部存储器自动加载一个配置概要文件。设备允许用户将这些设置保存到永久存储器的配置概要文件中。

当外部存储器包含相同设备的配置概要文件时，可以将设置从一个设备转移到另一个设备。

请执行以下步骤：

- ☐ 验证设备在重新启动时是否从外部存储器加载一个配置概要文件。
  在默认设置下，该功能为启用。如果该功能被禁用，请按照以下步骤再次启用该功能：

- ☐ 打开 *Basic Settings* > *External Memory* 对话框。
- ☐ 在 *Config priority* 列中，选择值 first。
- ☐ 暂时保存更改。为此，请单击 ✓ 按钮。

```
enable                                  切换到特权执行模式。
configure                               切换到配置模式。
config envm load-priority usb  first    启用该功能。
                                        重新启动时，设备会从外部存储器加载一个配置概
                                        要文件。
                                        usb = 外部 USB 存储器
show config envm settings               显示外部存储器 (envm) 的设置。

Type   Status      Auto Update Save Config Config Load Prio
------ ----------- ----------- ----------- ----------------
usb    ok          [x]         [x]           first
save                                    将配置概要文件中的设置保存到设备的永久存储器
                                        (NVM) 中。
```

使用命令行界面，设备允许用户将设置从外部存储器直接复制到永久存储器 (*NVM*) 中。

```
show config profiles nvm                显示永久存储器 (nvm) 中包含的配置概要文件。
enable                                  切换到特权执行模式。
copy config envm profile  config3 nvm   将配置概要文件 config3 从外部存储器 (envm) 复
                                        制到永久存储器 (nvm) 中。
```

设备在启动过程中还可以从脚本文件自动加载配置概要文件。

前提条件：
- 在启动设备之前验证外部存储器是否已连接。
- 外部存储器的根目录中包含一个内容为 `uetkrv?>hkngapcog@` 的文本文件 `startup.txt`。占位符 `>hkngapcog@` 表示设备在启动过程中执行的脚本文件。
- 外部存储器的根目录中包含该脚本文件。可以选择使用用户指定的名称保存该脚本。使用文件扩展名 `.cli` 保存该文件。

提示：验证保存在外部存储器中的脚本是否不为空。如果该脚本为空，则设备根据配置优先级设置加载下一个配置概要文件。

应用该脚本后，设备会自动将脚本文件中的配置概要文件作为 XML 文件保存到外部存储器中。在向脚本文件中键入适当命令时，可以选择禁用此功能：

☐ `no config envm config-save usb`
设备不在外部 USB 存储器中创建副本。

当脚本文件包含一个错误的命令时，设备在启动过程中不会应用此命令。设备将事件记录到日志文件 (System Log) 中。

5.3.3 导入配置概要文件

设备允许用户从服务器导入另存为 XML 文件的配置概要文件。如果使用图形用户界面，则可从您的 PC 直接导入 XML 文件。

前提条件：
- 要将该文件保存到服务器上，您需要一个在网络上配置好的服务器。
- 要将该文件保存到 SCP 或 SFTP 服务器上，您还需要用于访问此服务器的用户名和密码。

请执行以下步骤：

- ☐ 打开 *Basic Settings* > *Load/Save* 对话框。
- ☐ 点击  按钮，然后点击 *Import...* 项目。
  该对话框显示 *Import...* 窗口。
- ☐ 在 *Select source* 下拉列表中，选择设备导入配置概要文件的来源位置。
  - *PC/URL*
    设备从本地 PC 或远程服务器导入配置概要文件。
  - *External memory*
    设备从外部存储器导入配置概要文件。

从本地 PC 或远程服务器导入配置概要文件。为此，请执行以下步骤：

- ☐ 导入配置概要文件：
  - ☐ 当该文件位于 FTP 服务器上时，请以如下形式指定该文件的 URL：
    `ftp://<??>:<??>@<IP ??>:<??>/<???>`
  - ☐ 当该文件位于 TFTP 服务器上时，请以如下形式指定该文件的 URL：
    `tftp://<IP ??>/<??>/<???>`
  - ☐ 当该文件位于 SCP 或 SFTP 服务器上时，请以如下任一形式指定该文件的 URL：
    `scp://` 或 `sftp://<IP ??>/<??>/<???>`
    点击 *Start* 按钮后，设备会显示 *Credentials* 窗口。在此，可以输入 *User name* 和 *Password* 登录服务器。
    `scp://` 或 `sftp://<??>:<??>@<IP ??>/<??>/<???>`
- ☐ 在 *Destination* 框中，指定设备在哪里保存导入的配置概要文件：
  - ☐ 在 *Profile name* 字段中，指定设备用以保存配置概要文件的名称。
  - ☐ 在 *Storage type* 字段中，指定配置概要文件的存储位置。
- ☐ 点击 *Ok* 按钮。

设备将配置概要文件复制到指定的存储器中。

如果在 *Destination* 框中指定了值 ram，则设备会与图形用户界面断开连接并立即使用这些设置。

从外部存储器导入配置概要文件。为此，请执行以下步骤：

- ☐ 在 *Import profile from external memory* 框的 *Profile name* 下拉列表中，选择要导入的配置概要文件的名称。
  前提条件是外部存储器中包含一个导出的配置概要文件。
- ☐ 在 *Destination* 框中，指定设备在哪里保存导入的配置概要文件：
  - ☐ 在 *Profile name* 字段中，指定设备用以保存配置概要文件的名称。
- ☐ 点击 *Ok* 按钮。

设备将配置概要文件复制到设备的永久存储器 (*NVM*) 中。

如果在 *Destination* 框中指定了值 ram，则设备会与图形用户界面断开连接并立即使用这些设置。

`enable`	切换到特权执行模式。
`copy config remote ftp://<IP_address>:<port>/<path>/<file_name> running-config`	导入并激活保存在 FTP 服务器上的配置概要文件的设置。 设备将设置复制到非永久性存储器并与命令行界面断开连接。设备立即使用导入的配置概要文件的设置。
`copy config  remote tftp://<IP_address>/   <path>/<file_name> running-config`	导入并激活保存在 TFTP 服务器上的配置概要文件的设置。 设备将设置复制到非永久性存储器并与命令行界面断开连接。设备立即使用导入的配置概要文件的设置。
`copy config remote  sftp://<user name>:<password>@<IP_address>/<path>/<file_name> running-config`	导入并激活保存在 SFTP 服务器上的配置概要文件的设置。 设备将设置复制到非永久性存储器并与命令行界面断开连接。设备立即使用导入的配置概要文件的设置。
`copy config  remote ftp://<IP_address>:<port>/<path>/<file_name>  nvm profile config3`	导入保存在 FTP 服务器上的配置概要文件的设置并将配置概要文件 config3 中的设置保存到永久存储器 (nvm) 中。
`copy config  remote tftp://<IP_address>/<path>/<file_name> nvm profile config3`	导入保存在 TFTP 服务器上的配置概要文件的设置并将配置概要文件 config3 中的设置保存到永久存储器 (nvm) 中。

5.4 将设备重置为出厂默认值

如果将设备中的设置重置为交付状态，则设备会删除非永久性存储器和永久存储器中的配置概要文件。

如果连接了外部存储器，则设备也会删除外部存储器中保存的配置概要文件。

然后，设备会重新启动并加载出厂设置。

5.4.1 使用图形用户界面或命令行界面

请执行以下步骤：

- ☐ 打开 *Basic Settings > Load/Save* 对话框。
- ☐ 点击 按钮，然后点击 *Back to factory...*。
  该对话框显示一条消息。
- ☐ 点击 *Ok* 按钮。

设备删除存储器（RAM）和永久存储器（*NVM*）中的配置概要文件。

如果连接了外部存储器，则设备也会删除外部存储器中保存的配置概要文件。

稍后，设备会重新启动并加载交付设置。

`enable`	切换到特权执行模式。
`clear factory`	删除永久存储器和外部存储器中的配置概要文件。 如果连接了外部存储器，则设备也会删除外部存储器中保存的配置概要文件。 稍后，设备会重新启动并加载交付设置。

5.4.2 使用系统监控器

前提条件：
- 使用终端电缆将您的 PC 连接到设备的串行连接。

请执行以下步骤：
- ☐ 重新启动设备。
- ☐ 要切换到系统监控器，请在重新启动期间看到提示后 3 秒内按下 <1> 键。
  设备加载系统监控器。
- ☐ 要从主菜单切换到 `Manage configurations` 菜单，请按下 <4> 键。
- ☐ 要执行 `Clear configs and boot params` 命令，请按下 <1> 键。
- ☐ 要加载出厂设置，请按下 <Enter> 键。
  设备删除存储器（RAM）和永久存储器（*NVM*）中的配置概要文件。
  如果连接了外部存储器，则设备也会删除外部存储器中保存的配置概要文件。
- ☐ 要切换到主菜单，请按下 <q> 键。
- ☐ 要使用出厂设置重新启动设备，请按下 <q> 键。

6 加载软件更新

Schneider Electric 不断致力于软件的开发和完善。请定期检查是否有能为您带来更多益处的软件更新版本。可以在 www.schneider-electric.com网站的 Schneider Electric 产品页面中找到相关信息和软件下载。

设备提供以下设备软件更新选项：
- 从 PC 进行软件更新
- 从服务器进行软件更新
- 从外部存储器进行软件更新
- 加载以前的软件版本

提示：设备软件更新后将保留设备设置。

您可以在图形用户界面的登录对话框中看到已安装设备软件的版本。

要在您已登录时显示已安装的软件的版本，请执行以下步骤：

- ☐ 打开 *Basic Settings* > *Software* 对话框。
  Running version 字段显示设备在上一次重新启动时加载且目前正在运行的设备软件的版本号和创建日期。

`enable`	切换到特权执行模式。
`show system info`	显示设备在上一次重新启动时加载且目前正在运行的设备软件的版本号和创建日期等系统信息。

6.1 从 PC 进行软件更新

前提条件是，已将设备软件的镜像文件保存在可从您 PC 访问的数据载体中。

请执行以下步骤：

- ☐ 导航至保存有设备软件镜像文件的文件夹。
- ☐ 打开 *Basic Settings* > *Software* 对话框。
- ☐ 将该镜像文件拖放到 区域。也可点击该区域以选择该文件。
- ☐ 要开始更新过程，请点击 *Start* 按钮。
  更新过程成功完成后，设备会显示一条软件已成功更新的信息。
  重新启动时，设备会加载安装的设备软件。

6.2 从服务器进行软件更新

要使用 SFTP 或 SCP 对软件进行更新，您需要一台保存有设备软件镜像文件的服务器。

要使用 TFTP、SFTP 或 SCP 对软件进行更新，您需要一台保存有设备软件镜像文件的服务器。

请执行以下步骤：

- ☐ 打开 *Basic Settings > Software* 对话框。
- ☐ 在 *Software update* 框的 *URL* 字段中，以如下形式输入该镜像文件的 URL：
  - ▶ 当镜像文件保存在 FTP 服务器上时：
    `ftp://<IP_address>:<port>/<path>/<image_file_name>.bin`
  - ▶ 当镜像文件保存在 TFTP 服务器上时：
    `tftp://<IP_address>/<path>/<image_file_name>.bin`
  - ▶ 当镜像文件保存在 SCP 或 SFTP 服务器上时：
    `scp://` 或 `sftp://<IP_address>/<path>/<image_file_name>.bin`
    `scp://` 或 `sftp://<username>:<password>@<IP_address>/<path>/<image_file_name>.bin`
    当您输入不带用户名和密码的 URL 时，设备会显示 *Credentials* 窗口。在此，您可以输入登录服务器所需的登录凭证。
- ☐ 要开始更新过程，请点击 *Start* 按钮。
  设备将目前正在运行的设备软件复制到备份存储器中。
  更新过程成功完成后，设备会显示一条软件已成功更新的信息。
  重新启动时，设备会加载安装的设备软件。

`enable`	切换到特权执行模式。
`copy firmware remote tftp://10.0.1.159/product.bin system`	将 product.bin 文件从 IP 地址为 10.0.1.159 的 TFTP 服务器传送到设备。

6.3 从外部存储器进行软件更新

6.3.1 手动 — 由管理员发起

设备允许用户通过点击几下鼠标对设备软件进行更新。前提条件是，设备软件的镜像文件位于外部存储器中。

请执行以下步骤：

- ☐ 打开 *Basic Settings > Software* 对话框。
- ☐ 在表格中，勾选显示外部存储器中所需镜像文件的名称的行。
- ☐ 右键点击显示上下文菜单。
- ☐ 要开始更新过程，请点击上下文菜单中的 *Update* 项目。
  设备将目前正在运行的设备软件复制到备份存储器中。
  更新过程成功完成后，设备会显示一条软件已成功更新的信息。
  重新启动时，设备会加载安装的设备软件。

6.3.2 自动 — 由设备发起

当在重新启动期间以下文件位于外部存储器中时，设备会自动更新设备软件：

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

前提条件是，在 *Basic Settings > External Memory* 对话框中，用户勾选 *Software auto update* 列中的复选框。这是设备中的默认设置。

请执行以下步骤：

- ☐ 将新设备软件的镜像文件复制到外部存储器的主目录中。只能使用适合设备的镜像文件。
- ☐ 在外部存储器的主目录中创建一个文本文件 `startup.txt`。
- ☐ 在文本编辑器中打开 `startup.txt` 文件，并添加以下行：

  ```
  autoUpdate=<Image_file_name>.bin
  ```

- ☐ 将外部存储器安装到设备中。

☐ 重新启动设备。
在启动过程中，设备会自动检查以下条件：
- 是否连接了外部存储器？
- 外部存储器的主目录中是否存在 startup.txt 文件？
- 是否存在 startup.txt 文件中指定的镜像文件？
- 该镜像文件的软件版本是否比设备中目前正在运行的软件更新？

满足这些条件后，设备即开始更新过程。
设备将目前正在运行的设备软件复制到备份存储器中。
更新过程成功完成后，设备会自动重启并加载新的软件版本。

☐ 检查更新过程的结果。*Diagnostics > Report > System Log* 对话框中的日志文件包含以下任一消息：
- S_watson_AUTOMATIC_SWUPDATE_SUCCESS
  软件更新成功完成
- S_watson_AUTOMATIC_SWUPDATE_ABORTED
  软件更新失败
- S_watson_AUTOMATIC_SWUPDATE_ABORTED_WRONG_FILE
  镜像文件错误导致软件更新失败
- S_watson_AUTOMATIC_SWUPDATE_ABORTED_SAVING_FILE
  设备未保存镜像文件导致软件更新失败。

6.4 加载以前的软件版本

设备允许用户将设备软件替换为以前的版本。替换设备软件后将保留设备中的基本设置。

提示：只有更新设备软件版本中可用的功能的设置会丢失。

7 配置端口

提供了以下端口配置功能。
- 启用/禁用端口
- 选择运行模式
- 端口的千兆以太网模式

7.1 启用/禁用端口

在默认设置下，每个端口均已启用。要获得更高级别的访问安全性，请禁用未连接的端口。为此，请执行以下步骤：

- ☐ 打开 *Basic Settings* > *Port* 对话框的 *Configuration* 选项卡。
- ☐ 要启用端口，请勾选 *Port on* 列中的复选框。
- ☐ 要禁用端口，请取消勾选 *Port on* 列中的复选框。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`interface 1/1`	切换到接口 1/1 的接口配置模式。
`no shutdown`	启用接口。

7.2 选择运行模式

在默认设置下，端口被设为 *Automatic configuration* 运行模式。

提示：活动的自动配置优先级高于手动配置。

请执行以下步骤：

- ☐ 打开 *Basic Settings* > *Port* 对话框的 *Configuration* 选项卡。
- ☐ 如果连接到此端口的设备需要固定设置，请执行以下步骤：
  - ☐ 停用该功能。取消勾选 *Automatic configuration* 列中的复选框。
  - ☐ 在 *Manual configuration* 列中，输入所需的运行模式（传输速率、双工模式）。
- ☐ 暂时保存更改。为此，请单击  按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`interface 1/1`	切换到接口 1/1 的接口配置模式。
`no auto-negotiate`	禁用自动配置模式。
`speed 100 full`	端口速度 100 MBit/s，全双工

7.3 端口的千兆以太网模式

在采用以下任一 2.5 收发器的若干接口上，设备支持 SFP Gbit/s：
- M-SFP-2.5-MM/LC EEC
- M-SFP-2.5-SM-/LC EEC
- M-SFP-2.5-SM/LC EEC
- M-SFP-2.5-SM+/LC EEC

插入插槽的收发器的类型决定了端口速度。设备没有手动设置速度的选项。端口速度为 2.5 Gbit/s 的端口无法支持 100 Mbit/s 数据速率。

提示：有关收发器订单编号的更多信息，请参阅“安装”用户手册的“配件”一章。

7.3.1 示例

使用千兆以太网模式为上行链路获得更高带宽。要使用此功能，请向相应插槽中插入一个适当类型的收发器。

请执行以下步骤：

☐ 打开 *Basic Settings* > *Port* 对话框的 *Configuration* 选项卡。

Manual configuration 列为插入了 2.5 Gbit/s FDX Gbit/s 2.5 收发器的端口显示值 SFP。用户无法更改速度。

```
show port 1/1
```

显示插槽 1 端口 1 的参数。Physical Mode 列表条目为插入了 2500 full Gbit/s 2.5 收发器的端口显示值 SFP。

```
Interface.....................1/1
Name..........................My interface
--
Cable-crossing Setting........-
Physical Mode.................2500 full
Physical Status...............-
```

8 协助防止未经授权的访问

设备提供可帮助用户防止设备遭到未授权访问的功能。

安装设备后，请执行以下步骤，以降低对设备进行未授权访问的可能性。
- 更改 SNMPv1/v2 团体
- 禁用 SNMPv1/v2
- 禁用 HTTP
- 使用您自己的 HTTPS 证书
- 使用您自己的 SSH 密钥
- 禁用 Telnet
- 禁用 Ethernet Switch Configurator
- 启用 IP 访问限制
- 调整会话超时

8.1 更改 SNMPv1/v2 团体

SNMPv1/v2 以不加密方式进行工作。每个 SNMP 数据包都包含发送者的 IP 地址以及发送者访问设备时使用的明文团体名称。如果 SNMPv1/v2 已启用，则设备允许知道团体名称的任何人访问设备。

读取权限 admin 和写入权限的团体名称 user 已预设。如果您正在使用 SNMPv1 或 SNMPv2，则请更改默认团体名称。请谨慎处理团体名称。为此，请执行以下步骤：

☐ 打开 *Device Security > Management Access > SNMPv1/v2 Community* 对话框。

该对话框显示已经设置的团体。

☐ 对于 Write 团体，可在 *Name* 列中指定团体名称。
- 允许最多 32 个字母数字字符。
- 设备区分大小写。
- 指定与读权限不同的团体名称。

☐ 暂时保存更改。为此，请单击 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`snmp community rw <community name>`	为读/写权限指定团体。
`show snmp community`	显示已经配置的团体。
`save`	将设置保存到永久存储器 (nvm) 的“选定”配置概要文件中。

8.2 禁用 SNMPv1/v2

如果您需要 SNMPv1 或 SNMPv2，则只在具有窃听保护的环境中使用这些协议。SNMPv1 和 SNMPv2 不使用加密。SNMP 数据包以明文形式包含团体。我们建议在设备中使用 SNMPv3 并禁用使用 SNMPv1 和 SNMPv2 进行访问。为此，请执行以下步骤：

- ☐ 打开 *Device Security > Management Access > Server* 对话框的 *SNMP* 选项卡。

该对话框显示 SNMP 服务器的设置。

- ☐ 要停用 SNMPv1 协议，请取消勾选 *SNMPv1* 复选框。
- ☐ 要停用 SNMPv2 协议，请取消勾选 *SNMPv2* 复选框。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`no snmp access version v1`	停用 SNMPv1 协议。
`no snmp access version v2`	停用 SNMPv2 协议。
`show snmp access`	显示 SNMP 服务器设置。
`save`	将设置保存到永久存储器 (nvm) 的“选定”配置概要文件中。

8.3 禁用 HTTP

网络服务器使用 HTTP 或 HTTPS 协议提供图形用户界面。HTTPS 连接是加密的，而 HTTP 连接则是未加密的。

默认已启用 HTTP 协议。如果禁用 HTTP，则无法对图形用户界面进行不加密访问。为此，请执行以下步骤：

- ☐ 打开 *Device Security > Management Access > Server* 对话框的 *HTTP* 选项卡。
- ☐ 要禁用 HTTP 协议，请选择 *Operation* 框中的 *Off* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`no http server`	禁用 HTTP 协议。

如果禁用 HTTP 协议，则只能通过 HTTPS 访问设备的图形用户界面。在 Web 浏览器的地址栏中，在设备的 IP 地址之前输入字符串 `https://`。

如果用户同时禁用 HTTPS 和 HTTP 协议，则无法访问图形用户界面。要使用图形用户界面，请使用命令行界面启用 HTTPS 服务器。为此，请执行以下步骤：

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`https server`	启用 HTTPS 协议。

8.4 禁用 Telnet

设备允许用户使用 Telnet 或 SSH 远程访问设备管理。Telnet 连接是未加密的，而 SSH 连接则是加密的。

设备中默认启用了 Telnet 服务器。如果禁用 Telnet，则无法对命令行界面进行不加密远程访问。为此，请执行以下步骤：

- ☐ 打开 *Device Security > Management Access > Server* 对话框的 *Telnet* 选项卡。
- ☐ 要禁用 Telnet 服务器，请选择 *Operation* 框中的 *Off* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`no telnet server`	禁用 Telnet 服务器。

如果 SSH 服务器已禁用并且用户还禁用了 Telnet，则只可能通过设备的串行接口访问命令行界面。要远程操作命令行界面，请启用 SSH。为此，请执行以下步骤：

- ☐ 打开 *Device Security > Management Access > Server* 对话框的 *SSH* 选项卡。
- ☐ 要启用 *SSH* 服务器，请选择 *Operation* 框中的 *On* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`ssh server`	启用 SSH 服务器。

8.5 禁用 Ethernet Switch Configurator 访问

Ethernet Switch Configurator 允许用户在调试期间通过网络向设备分配 IP 参数。Ethernet Switch Configurator 在设备管理 VLAN 中进行未加密和未经身份验证的通信。

在调试设备之后，我们建议将 Ethernet Switch Configurator 设置为只读或者完全禁用 Ethernet Switch Configurator 访问。为此，请执行以下步骤：

- ☐ 打开 *Basic Settings > Network* 对话框。
- ☐ 要从 Ethernet Switch Configurator 软件中取消写权限，请在 *Ethernet Switch Configurator protocol v1/v2* 框的 *Access* 字段中指定值 readOnly。
- ☐ 要完全禁用 Ethernet Switch Configurator 访问，请选择 *Ethernet Switch Configurator protocol v1/v2* 框中的 *Off* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`enable`	切换到特权执行模式。
`network ethernet-switch-conf mode read-only`	禁用 Ethernet Switch Configurator 软件的写入权限。
`no network ethernet-switch-conf operation`	禁用 Ethernet Switch Configurator 访问。

8.6 激活 IP 访问限制

在默认设置下，您可以从任何 IP 地址使用支持的协议访问设备管理。

IP 访问限制允许用户将针对设备管理的访问限制到选定的 IP 地址范围和选定的基于 IP 的协议。

示例：

设备只允许使用图形用户界面通过公司网络进行访问。管理员可以使用 SSH 进行更多的远程访问。公司网络的地址范围为 192.168.1.0/24，从移动网络进行远程访问的 IP 地址范围为 109.237.176.0/24。SSH 应用程序知道 RSA 密钥的指纹。

表格 20: IP 访问限制的参数

参数	公司网络	移动电话网络
网络地址	192.168.1.0	109.237.176.0
子网掩码	24	24
所需协议	https, snmp	ssh

请执行以下步骤：

- ☐ 打开 *Device Security > Management Access > IP Access Restriction* 对话框。
- ☐ 为该条目取消勾选 *Active* 列中的复选框。
  此条目允许用户从任何 IP 地址并通过支持的协议对设备进行访问。

公司网络的地址范围：

- ☐ 要添加一个表格条目，请点击 按钮。
- ☐ 在 *IP address range* 列中指定公司网络的地址范围：192.168.1.0/24
- ☐ 对于企业网络的地址范围，请停用不需要的协议。*HTTPS*、*SNMP* 和 *Active* 复选框保持勾选。

移动电话网络的地址范围：

- ☐ 要添加一个表格条目，请点击 按钮。
- ☐ 在 *IP address range* 列中指定移动网络的地址范围：109.237.176.0/24
- ☐ 对于移动网络的地址范围，请停用不需要的协议。*SSH* 和 *Active* 复选框保持勾选。

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

- ☐ 要启用 IP 访问限制，请选择 *Operation* 框中的 *On* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 按钮。

`enable`	切换到特权执行模式。
`show network management access global`	指定 IP 访问限制是已启用还是已禁用。
`show network management access rules`	显示已配置的条目。
`no network management access operation`	禁用 IP 访问限制。
`network management access add 2`	为公司网络的地址范围创建条目。 本示例中下一个可用索引的编号：2。
`network management access modify 2 ip 192.168.1.0`	指定公司网络的 IP 地址。

network management access modify 2 mask 24	指定公司网络的子网掩码。
network management access modify 2 ssh disable	为公司网络的地址范围停用 SSH。 对每个不需要的协议重复此操作。
network management access add 3	为移动电话网络的地址范围创建条目。 本示例中下一个可用索引的编号：3。
network management access modify 3 ip 109.237.176.0	指定移动电话网络的 IP 地址。
network management access modify 3 mask 24	指定移动电话网络的子网掩码。
network management access modify 3 snmp disable	为移动电话网络的地址范围停用 SNMP。 对每个不需要的协议重复此操作。
no network management access status 1	停用默认条目。 此条目允许用户从任何 IP 地址并通过支持的协议对设备进行访问。
network management access status 2	为公司网络的地址范围激活条目。
network management access status 3	为移动电话网络的地址范围激活条目。
show network management access rules	显示已配置的条目。
network management access operation	启用 IP 访问限制。

8.7 调整会话超时

设备允许用户在登录用户不活动时自动终止会话。会话超时是最后一项用户操作之后的不活动时期。

可以为以下应用程序指定会话超时：
- 使用 SSH 连接的命令行界面会话
- 使用 Telnet 连接的命令行界面会话
- 使用串行连接的命令行界面会话
- 图形用户界面

使用 SSH 连接的命令行界面会话的超时

请执行以下步骤：

- ☐ 打开 *Device Security > Management Access > Server* 对话框的 *SSH* 选项卡。
- ☐ 在 *Configuration* 框的 *Session timeout [min]* 字段中指定超时期限（分钟）。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`ssh timeout <0..160>`	为使用 SSH 连接的命令行界面会话指定超时期限（分钟）。

使用 Telnet 连接的命令行界面会话的超时

请执行以下步骤：

- ☐ 打开 *Device Security > Management Access > Server* 对话框的 *Telnet* 选项卡。
- ☐ 在 *Configuration* 框的 *Session timeout [min]* 字段中指定超时期限（分钟）。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`telnet timeout <0..160>`	为使用 Telnet 连接的命令行界面会话指定超时期限（分钟）。

使用串行连接的命令行界面会话的超时

请执行以下步骤：

- ☐ 打开 *Device Security > Management Access > CLI* 对话框的 *Global* 选项卡。
- ☐ 在 *Configuration* 框的 *Serial interface timeout [min]* 字段中指定超时期限（分钟）。
- ☐ 暂时保存更改。为此，请单击 ✓ 按钮。

`enable`	切换到特权执行模式。
`cli serial-timeout <0..160>`	为使用串行连接的命令行界面会话指定超时期限（分钟）。

图形用户界面的会话超时

请执行以下步骤：

- ☐ 打开 *Device Security > Management Access > Web* 对话框。
- ☐ 在 *Configuration* 框的 *Web interface session timeout [min]* 字段中指定超时期限（分钟）。
- ☐ 暂时保存更改。为此，请单击 ✓ 按钮。

`enable`	切换到特权执行模式。
`network management access web timeout <0..160>`	为图形用户界面会话指定超时期限（分钟）

9 控制数据流量

设备根据定义的规则对要转发的数据包进行检查。应用这些规则的数据包要么由设备转发，要么被阻塞。如果数据包不符合任何规则，则设备将阻塞数据包。

没有分配任何规则的路由端口允许数据包通过。一旦分配了规则，首先会处理分配的规则。然后，设备的指定标准操作生效。

设备提供以下用于控制数据流的功能：
- 服务请求控制 (Denial of Service, DoS)
- 根据 IP 或 MAC 地址拒绝访问设备（访问控制列表）

设备对数据流进行观察和监控。设备获取观察和监控的结果并将这些结果与网络安全规则结合起来，创建一个所谓的状态表。根据此状态表，设备决定是否接受、丢弃或拒绝数据。

数据包按照以下顺序通过设备的筛选器功能：
- DoS … 如果 permit 或 accept，则转到下一个规则
- ACL … 如果 permit 或 accept，则转到下一个规则

9.1 帮助防止未经授权的访问

借助此功能，设备可帮助您防止针对某些服务或设备的无效或伪造数据包。用户可以选择指定用于限制数据流的筛选器，以防止拒绝服务攻击。激活的筛选器对发入数据包进行检查，一旦发现与筛选条件匹配，立即予以丢弃。

Network Security > DoS > Global 对话框包含 2 个框，您可在其中激活不同的筛选器。要激活筛选器，请勾选相应复选框。

在 *TCP/UDP* 框中，可以激活最多 4 个仅影响 TCP 和 UDP 数据包的筛选器。使用此筛选器，可以停用攻击者用以尝试识别所提供的设备和服务的端口扫描。筛选器的工作方式如下：

表格 21: 针对 TCP 数据包的 DoS 筛选器

筛选器	操作
激活 Null 扫描筛选器	设备检测并丢弃具有以下属性的传入 TCP 数据包： ▶ 未设置任何 TCP 标志。 ▶ TCP 序列号为 0。
激活 Xmas 筛选器	设备检测并丢弃具有以下属性的传入 TCP 数据包： ▶ 同时设置了 TCP 标志 *FIN*、*URG* 和 *PSH*。 ▶ TCP 序列号为 0。
激活 SYN/FIN 筛选器	设备检测并丢弃同时设置了 TCP 标志 *SYN* 和 *FIN* 的传入 TCP 数据包。
激活最小报头筛选器	如果接收到的 TCP 报文的 TCP 报头过短，设备会将其丢弃。

ICMP 框提供两个用于 ICMP 数据包的筛选器选项。发入 ICMP 数据包的分片是攻击的迹象。如果激活此筛选器，则设备检测并丢弃分片 ICMP 数据包。使用 *Allowed payload size [byte]* 参数，还可以指定 ICMP 数据包的有效载荷的最大允许大小。设备丢弃超过此字节规格的数据包。

提示：可以在 *Network Security > DoS > Global* 对话框中以任何方式对多个筛选器进行组合。当选择若干个筛选器时，将应用一个逻辑或：如果第一个或第二个（或第三个，等等）筛选器应用于一个数据包，则设备丢弃该数据包。

9.2 ACL

在此菜单中，可以为访问控制列表 (ACL) 输入参数。

设备使用 ACL 对在 VLAN 上或者单个或多个端口上收到的数据包进行筛选。在一个 ACL 中，可以指定设备用于筛选数据包的规则。当这样一个规则应用于一个数据包时，设备将该规则中指定的操作应用于该数据包。可用操作如下：

- 允许 (permit)
- 丢弃 (deny)
- 重定向到某个端口（参见 *Redirection port* 字段）
- 映射（参见 *Mirror port* 字段）

以下列表包含了对数据包进行筛选时可以应用的条件：

- 数据包的源地址或目标地址 (MAC)
- 数据包的源地址或目标地址 (IPv4)
- 数据包的源端口或目标端口 (IPv4)

可以指定以下 ACL 类型：

- 用于 VLAN 的 IP ACL
- 用于端口的 IP ACL
- 用于 VLAN 的 MAC ACL
- 用于端口的 MAC ACL

向同一接口同时分配 IP ACL 和 MAC ACL 后，设备首先会使用 IP ACL 对数据流进行筛选。只有在通过 IP ACL 对数据包进行筛选后，设备才会应用 MAC ACL 规则。ACL 的优先级与规则的索引无关。

在一个 ACL 中，设备会按顺序对规则进行处理。相应规则的索引决定了设备对数据流进行筛选的顺序。向端口或 VLAN 分配 ACL 时，可以使用索引指定其优先级。数字越小，优先级越高。设备首先处理优先级较高的规则。

如果 ACL 中指定的任何规则都不应用于数据包，则应用隐式 deny 规则。因此，设备会丢弃接收到的数据包。

请记住，设备会直接实施隐式 deny 规则。

提示：可用 ACL 的数量视设备而定。有关 ACL 值的更多信息，请参阅“技术数据” 页 349一章。

提示：可以将一个 ACL 分配给任意数量的端口或 VLAN。

ACL 菜单包含以下对话框：

- *ACL IPv4 Rule*
- *ACL MAC Rule*
- *ACL Assignment*

这些对话框提供了以下选项：

- 为各种 ACL 类型指定规则。
- 为规则提供所需优先级。
- 向端口或 VLAN 分配 ACL。

9.2.1 创建和编辑 IPv4 规则

对 IPv4 数据包进行筛选时，设备允许用户：
- 创建新的组和规则
- 向现有组中添加新规则
- 编辑现有规则
- 激活和停用组和规则
- 删除现有的组和规则
- 更改现有规则的顺序

请执行以下步骤：

- ☐ 打开 *Network Security* > *ACL* > *IPv4 Rule* 对话框。
- ☐ 点击  按钮。
  该对话框显示 *Create* 窗口。
- ☐ 要创建一个组，请在 *Group name* 字段中指定一个有意义的名称。可以在一个组中组合多个规则。
- ☐ 要向现有组中添加规则，请在 *Group name* 字段中选择该组的名称。
- ☐ 在 *Index* 字段中，可以指定该规则在 ACL 中的编号。
  此编号定义了该规则的优先级。
- ☐ 点击 *Ok* 按钮。
  设备将该规则添加到表中。
  组和角色均立即激活。
  要停用组或规则，请取消勾选 *Active* 列中的复选框。
  要删除规则，请突出显示受影响的表格条目并点击  按钮。
- ☐ 编辑表中的规则参数。
  要更改值，请双击相关字段。
- ☐ 暂时保存更改。为此，请单击  按钮。

提示：设备允许用户使用具有 *Source IP address* 和 *Destination IP address* 参数的通配符。例如，如果输入 192.168.?.?，则设备允许使用以 192.168 开始的地址。

提示：更改 *Source TCP/UDP port* 和 *Destination TCP/UDP port* 列中值的前提条件是，用户在 *Protocol* 列中指定值 tcp 或 udp。

提示：更改 *Redirection port* 和 *Mirror port* 列中值的前提条件是，用户在 *Action* 列中指定值 permit。

9.2.2 使用命令行界面创建和配置 IP ACL

在以下示例中，配置 ACL 以阻止通过 IP（TCP、UDP 等）从计算机 B 和 C 到计算机 A 的通信。

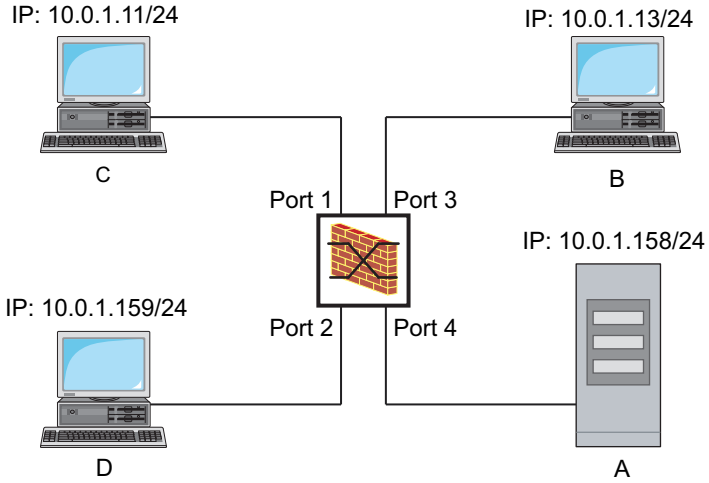


图 22: IP ACL 示例

请执行以下步骤：

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`ip access-list extended name filter1 deny src 10.0.1.11-0.0.0.0 dst 10.0.1.158-0.0.0.0 assign-queue 1`	添加名称为 `filter1` 的 IP ACL。添加拒绝从 `10.0.1.11` 到 `10.0.1.158` 的 IP 数据包的规则。优先级 `1`（最高优先级）。
`ip access-list extended name filter1 permit src any dst any`	将规则添加到允许 IP 数据包的 IP ACL。
`show access-list ip filter1`	显示 IP ACL `filter1` 的规则。
`ip access-list extended name filter2 deny src 10.0.1.13-0.0.0.0 dst 10.0.1.158-0.0.0.0 assign-queue 1`	添加名称为 `filter2` 的 IP ACL。添加拒绝从 `10.0.1.13` 到 `10.0.1.158` 的 IP 数据包的规则。优先级 `1`（最高优先级）。
`show access-list ip filter2`	显示 IP ACL `filter2` 的规则。

9.2.3 创建和编辑 MAC 规则

对 MAC 数据包进行筛选时，设备允许用户：

- 创建新的组和规则
- 向现有组中添加新规则
- 编辑现有规则
- 激活和停用组和规则
- 删除现有的组和规则
- 更改现有规则的顺序

请执行以下步骤：

- ☐ 打开 *Network Security* > *ACL* > *MAC Rule* 对话框。
- ☐ 点击  按钮。
  该对话框显示 *Create* 窗口。
- ☐ 要创建一个组，请在 *Group name* 字段中指定一个有意义的名称。可以在一个组中组合多个规则。
- ☐ 要向现有组中添加规则，请在 *Group name* 字段中选择该组的名称。
- ☐ 在 *Index* 字段中，可以指定该规则在 ACL 中的编号。
  此编号定义了该规则的优先级。
- ☐ 点击 *Ok* 按钮。
  设备将该规则添加到表中。
  组和角色均立即激活。
  要停用组或规则，请取消勾选 *Active* 列中的复选框。
  要删除规则，请突出显示受影响的表格条目并点击  按钮。
- ☐ 编辑表中的规则参数。
  要更改值，请双击相关字段。
- ☐ 暂时保存更改。为此，请单击  按钮。

提示： 在 *Source MAC address* 和 *Destination MAC address* 字段中，可以使用 FF:??:??:??:??:?? 或 ??:??:??:??:00:01 形式的通配符。此处请使用大写字母。

9.2.4 使用命令行界面创建和配置 MAC ACL

以下示例将从整个网络中筛除 AppleTalk 和 IPX。为此，请执行以下步骤：

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`mac acl add 1 macfilter`	添加一个 ID 为 1 及名称为 macfilter 的 MAC ACL。
`mac acl rule add 1 1 deny src any any dst any any etype appletalk`	在 ID 为 1 的 MAC ACL 的位置 1 处添加一个拒绝 EtherType 为 0x809B (AppleTalk) 的数据包的规则。
`mac acl rule add 1 2 deny src any any dst any any etype ipx-old`	在 ID 为 2 的 MAC ACL 的位置 1 处添加一个拒绝 EtherType 为 0x8137 (IPX alt) 的数据包的规则。
`mac acl rule add 1 3 deny src any any dst any any etype ipx-new`	在 ID 为 3 的 MAC ACL 的位置 1 处添加一个拒绝 EtherType 为 0x8138 (IPX) 的数据包的规则。
`mac acl rule add 1 4 permit src any any dst any any`	在 ID 为 4 的 MAC ACL 的位置 1 处添加一个转发数据包的规则。
`show acl mac rules 1`	显示 ID 为 1 的 MAC ACL 的规则。
`interface 1/1,1/2,1/3,1/4,1/5,1/6`	切换到接口 1/1 至 1/6 的接口配置模式。
`acl mac assign 1 in 1`	将 ID 为 1 的 MAC ACL 分配给接口 1/1 至 1/6 上的发入数据包 (in)。
`exit`	离开接口模式。
`show acl mac assignment 1`	显示 ID 为 1 的分配给接口或 VLAN 的 MAC ACL。

9.2.5 将 ACL 分配给端口或 VLAN

向端口或 VLAN 分配 ACL 时，设备为用户提供以下选项：
- 选择端口或 VLAN。
- 指定 ACL 优先级。
- 使用组名称选择 ACL。

请执行以下步骤：

- ☐ 打开 *Network Security > ACL > Assignment* 对话框。
- ☐ 点击 按钮。
  该对话框显示 *Create* 窗口。
  - ☐ 在 *Port/VLAN* 字段中，指定所需端口或所需 VLAN。
  - ☐ 在 *Priority* 字段中，指定优先级。
  - ☐ 在 *Direction* 字段中，指定设备对其应用规则的数据包。
  - ☐ 在 *Group name* 字段中，指定设备分配给端口或 VLAN 的规则。
- ☐ 点击 *Ok* 按钮。
- ☐ 暂时保存更改。为此，请单击 按钮。

9.3 MAC 身份验证绕过

MAC authorized bypass 允许不支持 802.1X 的客户端（如打印机和传真机）使用 MAC 地址在网络中进行身份验证。设备允许用户指定 MAC 地址的格式，以对 RADIUS 服务器上的客户端进行身份验证。

示例：

将 MAC 地址分为 6 组，每组 2 个字符。使用大写字母，将冒号字符作为分隔符：
AA:BB:CC:DD:EE:FF

使用密码 xY-45uM_e为此，请执行以下步骤：

- ☐ 打开 *Network Security* > *802.1X Port Authentication* > *Global* 对话框。
  在 *MAC authentication bypass format options* 框中，执行以下步骤：
- ☐ 在 *Group size* 下拉列表中，选择值 *2*。
  设备将 MAC 地址分为 6 组，每组 2 个字符。
- ☐ 在 *Group separator* 下拉列表中，选择 *:* 字符。
- ☐ 在 *Upper or lower case* 下拉列表中，选择 *upper-case* 项目。
- ☐ 在 *Password* 字段中，输入密码 xY-45uM_e。
  设备将此密码用于对 RADIUS 服务器进行身份验证的每个客户端。如果此字段留空，则设备也将使用格式化的 MAC 地址作为密码。
- ☐ 要临时保存设置，请点击 ✔ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`dot1x mac-authentication-bypass format group-size 2`	指定组大小 2。
`dot1x mac-authentication-bypass format group-separator :`	指定组分隔符 :。
`dot1x mac-authentication-bypass format letter-case upper-case`	指定设备将用大写字母来格式化身份验证数据。
`dot1x mac-authentication-bypass password xY-45uM_e`	指定密码 xY-45uM_e。设备使用密码在 RADIUS 服务器上对每个客户端进行身份验证。

10 网络负载控制

设备具备一些可帮助降低网络负载的功能：
- 直接数据包分发
- Multicasts
- 速率限制器
- 优先级 - QoS
- 流量控制

10.1 直接数据包分发

设备使用直接数据包分发降低网络负载。

在每个端口上，设备会学习接收到的数据包的发送者 MAC 地址。设备将“端口和 MAC 地址”组合存储在其 MAC 地址表 (FDB) 中。

通过应用 “Store and Forward” 方法，设备对接收到的数据进行缓冲，并在转发前检查其有效性。设备会拒绝无效和有缺陷的数据包。

10.1.1 学习 MAC 地址

当设备接收数据包时，它会检查发送者的 MAC 地址是否已存储在 MAC 地址表 (FDB) 中。当发送者的 MAC 地址未知时，设备会生成一个新的条目。然后，设备会将数据包的目标 MAC 地址与 MAC 地址表 (FDB) 中存储的条目进行比较：
- 设备将具有已知目标 MAC 地址的数据包直接转发到已经从该 MAC 地址接收过数据包的端口。
- 设备大量发送具有未知目标地址的数据包，即，设备将这些数据包转发到每个端口。

10.1.2 示教 MAC 地址的老化

设备将从 MAC 地址表 (FDB) 中删除其在一段可调时间期限（老化时间）内没有检测到的地址。如果进行重新启动或重置 MAC 地址表，则将删除 MAC 地址表 (FDB) 中的条目。

10.1.3 静态地址条目

除学习发送者 MAC 地址之外，设备还提供手动设置 MAC 地址的选项。这些 MAC 地址会保持配置状态，在 MAC 地址表 (FDB) 重置以及设备重新启动后仍然有效。

静态地址条目允许设备将数据包直接转发到选定的端口。如果没有指定目标端口，则设备会丢弃相应的数据包。

您可以在图形用户界面中或命令行界面中管理静态地址条目。

请执行以下步骤：

☐ 创建一个静态地址条目。

☐ 打开 *Switching > Filter for MAC Addresses* 对话框。

☐ 添加一个用户可配置的 MAC 地址：

▶ 点击  按钮。
该对话框显示 *Create* 窗口。

▶ 在 *Address* 字段中，指定目标 MAC 地址。

▶ 在 *VLAN ID* 字段中，指定 VLAN 的 ID。

▶ 在 *Port* 列表中，选择设备使用指定 VLAN 中的指定目标 MAC 地址向其转发数据包的端口。
在 *Address* 字段中定义了一个 Unicast MAC 地址后，只选择一个端口。
在 *Address* 字段中定义了一个 Multicast MAC 地址后，选择一个或多个端口。
如果希望设备丢弃具有目标 MAC 地址的数据包，则不选择任何端口。

▶ 点击 *Ok* 按钮。

☐ 暂时保存更改。为此，请单击  按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`mac-filter <MAC address> <VLAN ID>`	创建由 MAC 地址和 VLAN ID 组成的 MAC 地址筛选器。
`interface 1/1`	切换到接口 1/1 的接口配置模式。
`mac-filter <MAC address> <VLAN ID>`	将端口分配给之前创建的 MAC 地址筛选器。
`save`	将设置保存到永久存储器 (nvm) 的“选定”配置概要文件中。

☐ 将学习到的 MAC 地址转换为静态地址条目。

☐ 打开 *Switching > Filter for MAC Addresses* 对话框。

☐ 要将学习到的 MAC 地址转换为静态地址条目，请选择 *Status* 列中的值 permanent。

☐ 暂时保存更改。为此，请单击  按钮。

☐ 禁用一个静态地址条目。

☐ 打开 *Switching > Filter for MAC Addresses* 对话框。

☐ 要禁用一个静态地址条目，请选择 *Status* 列中的值 invalid。

☐ 暂时保存更改。为此，请单击  按钮。

enable	切换到特权执行模式。
configure	切换到配置模式。
interface 1/1	切换到接口 1/1 的接口配置模式。
no mac-filter <MAC address> <VLAN ID>	取消端口上 MAC 地址筛选器的分配。
exit	切换到配置模式。
no mac-filter <MAC address> <VLAN ID>	删除由 MAC 地址和 VLAN ID 组成的 MAC 地址筛选器。
exit	切换到特权执行模式。
save	将设置保存到永久存储器 (nvm) 的“选定”配置概要文件中。

□ 删除学习到的 MAC 地址。

□ 要从 MAC 地址表 (FDB) 中删除学习到的地址，请打开 *Basic Settings* > *Restart* 对话框并点击 *Reset MAC address table* 按钮。

clear mac-addr-table	从 MAC 地址表 (FDB) 中删除学习到的 MAC 地址。

10.2 Multicasts

默认状态下，设备大量发送具有 Multicast 地址的数据包，即，设备将这些数据包转发到每个端口。这会导致网络负载增加。

使用 IGMP 窥探可以降低 Multicast 数据流量导致的网络负载。IGMP 窥探允许设备只在连接了对 Multicast“有兴趣的”设备的端口上发送 Multicast 数据包。

10.2.1 Multicast 应用示例

监视摄像头将图像传输到机房和监控室中的监控器。使用 IP Multicast 传输，摄像头以 Multicast 数据包的形式通过网络传输图形数据。

互联网组管理协议 (IGMP) 对 Multicast 路由器和监控器之间的 Multicast 数据流量进行组织。网络中 Multicast 路由器和监控器之间的交换机对 IGMP 数据流量进行持续监控 (“IGMP Snooping”)。

交换机对登录进行注册，以接收 Multicast 数据流（IGMP 报告）。然后，设备在 MAC 地址表 (FDB) 中创建一个条目，并将 Multicast 数据包只转发到设备之前在其上接收到 IGMP 报告的端口。

10.2.2 IGMP 窥探

互联网组管理协议 (IGMP) 描述了第 Multicast 层上路由器和相连接收器之间 3 信息的分发。IGMP Snooping 描述了交换机持续监控 IGMP 流量并优化自身针对此数据流量的传输设置的功能。

设备中的 *IGMP Snooping* 功能根据 RFC 4541 (Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches) 进行工作。

具有活动 *IGMP* 功能的 Multicast 路由器定期请求（查询）Multicast 数据流的注册，以确定相关 IP Multicast 组成员。IP Multicast 组成员使用报告消息进行应答。此报告消息包含 *IGMP* 功能需要的参数。Multicast 路由器将报告消息中的 IP Multicast 组地址输入到其路由表中。这将使它根据其路由表对目标地址字段中包含此 IP Multicast 组的数据包进行转发。

离开一个 Multicast 组时（IGMP 版本 2 及以上），接收器使用“离开”消息进行注销，且不再发送任何报告消息。如果它在一段时间（老化时间）内没有接收到来自该接收器的任何更多报告消息，则 Multicast 路由器会删除一个接收器的路由表条目。

当同一网络中存在多个 IGMP Multicast 路由器时，IP 地址较小的设备将接替查询功能。当网络上没有 Multicast 路由器时，可以选择在适当配备的交换机中启用查询功能。

将一个 Multicast 接收器与一个 Multicast 路由器连接起来的交换机会使用 IGMP 窥探方法对 IGMP 信息进行分析。

IGMP 窥探方法还使交换机能够使用 *IGMP* 功能。交换机将从 Multicast 接收器的 IP 地址中获得的 MAC 地址作为识别的 Multicast 地址存储到其 MAC 地址表 (FDB) 中。此外，交换机还针对特定 Multicast 地址对通过其接收到报告的端口进行标识。通过这种方式，交换机将 Multicast 数据包只转发到连接了 Multicast 接收器的端口。其他端口不接收这些数据包。

设备的一个特殊功能在于，有可能确定具有未知 Multicast 地址的数据包的处理。视设置而定，设备会丢弃这些数据包或将其转发到每个端口。默认状态下，设备将数据包只传输到具有相连设备的端口，后者反过来则接收查询数据包。还可以选择另外将已知 Multicast 数据包发送到查询端口。

设置 IGMP 窥探

请执行以下步骤：

- ☐ 打开 *Switching* > *IGMP Snooping* > *Global* 对话框。
- ☐ 要启用该功能，请选择 *Operation* 框中的 *On* 单选按钮。

IGMP Snooping 功能禁用时，设备行为如下：

- ▶ 设备忽略接收到的查询和报告消息。
- ▶ 设备将接收到的以 Multicast 地址作为目标地址的数据包转发（大量发送）到每个端口。

- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

☐ 指定一个端口的设置：

- ☐ 打开 *Switching* > *IGMP Snooping* > *Configuration* 对话框的 *Port* 选项卡。
- ☐ 要激活端口上的 *IGMP Snooping* 功能，请为相关端口勾选 *Active* 列中的复选框。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

☐ 指定一个 VLAN 的设置：

- ☐ 打开 *Switching* > *IGMP Snooping* > *Configuration* 对话框的 *VLAN ID* 选项卡。
- ☐ 要为一个特定 VLAN 激活 *IGMP Snooping* 功能，请为相关 VLAN 勾选 *Active* 列中的复选框。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

设置 IGMP 查询器功能

设备本身可以选择发送活动查询消息；此外，设备可以响应查询消息或检测网络中的其他 Multicast 查询器（*IGMP Snooping Querier* 功能）。

前提条件：

已全局启用 *IGMP Snooping* 功能。

请执行以下步骤：

- ☐ 打开 *Switching > IGMP Snooping > Querier* 对话框。
- ☐ 在 *Operation* 框中，全局启用/禁用设备的 *IGMP Snooping Querier* 功能。
- ☐ 要为一个特定 VLAN 激活 *IGMP Snooping Querier* 功能，请为相关 VLAN 勾选 *Active* 列中的复选框。
- ▶ 设备执行简单的选择过程：当另一个 Multicast 查询器的 IP 源地址小于设备自己的地址时，设备切换到被动状态，在此状态下，设备不再发送任何查询请求。
- ▶ 在 *Address* 列中，可以指定设备将其作为发送者地址插入到生成的查询请求之中的 IP Multicast 地址。可以使用 Multicast 路由器的地址。
- ☐ 暂时保存更改。为此，请单击 按钮。

IGMP 窥探增强（表）

Switching > IGMP Snooping > Snooping Enhancements 对话框允许用户访问 *IGMP Snooping* 功能的增强设置。可以激活或停用 VLAN 中每个端口上的设置。

可以进行以下设置：

▶ Static

使用此设置将端口设置为静态查询端口。即使设备以前在一个静态查询端口上没有接收到任何 IGMP 查询消息，设备仍在该端口上转发所有 IGMP 消息。当静态选项被禁用且设备之前接收到过 IGMP 查询消息时，设备会在此端口上转发 IGMP 消息。当存在这种情况时，该条目会显示 L（“learned”）。

▶ Learn by LLDP

具有此设置的端口会自动发现其他使用 LLDP（链路层发现协议）的 Schneider Electric 设备。然后，设备从这些 Schneider Electric 设备学习此端口的 IGMP 查询状态，然后相应地配置 *IGMP Snooping Querier* 功能。ALA 条目表示 Learn by LLDP 功能已激活。当设备在此 VLAN 的这个端口上发现其他 Schneider Electric 设备时，该条目还会显示一个 A（“automatic”）。

▶ Forward All

使用此设置，设备将指向一个 Multicast 地址的数据包转发到此端口。例如，该设置适用于以下情况：

- 用于诊断目的。
- 用于 MRP 环网中的设备：环网进行切换后，利用 Forward All 功能，可以为具有注册的 Multicast 目标地址的数据包快速对网络进行重新配置。激活每个环网端口上的 Forward All 功能。

前提条件：

已全局启用 *IGMP Snooping* 功能。

请执行以下步骤：

- ☐ 打开 *Switching > IGMP Snooping > Snooping Enhancements* 对话框。
- ☐ 双击所需 VLAN 中的所需端口。
- ☐ 要激活一项或多项功能，请选择相应的选项。
- ☐ 点击 *Ok* 按钮。
- ☐ 暂时保存更改。为此，请单击 按钮。

`enable`	切换到特权执行模式。
`vlan database`	切换到 VLAN 配置模式。
`igmp-snooping vlan-id 1 forward-all 1/1`	为 VLAN 1 中的端口 1/1 激活 Forward All 功能。

配置 Multicasts

设备允许用户对 Multicast 数据包的交换进行配置。视要将数据包发送到未知还是已知 Multicast 接收器而定，设备提供了不同的选项。

针对未知 Multicast 地址的设置对于整个设备是全局的。可以选择以下选项：

- 设备丢弃未知 Multicasts。
- 设备向所有端口转发未知 Multicasts。

提示：针对未知 Multicast 地址的交换设置也适用于 “Local Network Control Block” (224.0.0.0..224.0.0.255) 中的保留 IP 地址。这种行为会影响更高级别的路由协议。

对于每个 VLAN，可以指定将 Multicast 数据包分别发送到已知 Multicast 地址。可以选择以下选项：

- 设备将已知 Multicasts 转发到之前接收到查询消息的端口（查询端口）和注册端口。注册端口指的是向相应 Multicast 组注册了 Multicast 接收器的端口。此选项有助于确保这种传输无需进一步配置即可用于基本应用程序。
- 设备将已知 Multicasts 只转发到注册端口。此设置的优点在于，它可通过直接分发对可用带宽进行最优利用。

前提条件：

已全局启用 *IGMP Snooping* 功能。

请执行以下步骤：

- ☐ 打开 *Switching* > *IGMP Snooping* > *Multicasts* 对话框。
- ☐ 在 *Configuration* 框中，可以指定设备如何将数据包发送到未知 Multicast 地址。
  - *send to registered ports*
    设备将具有未知 Multicast 地址的数据包转发到所有查询端口。
- ☐ 在 *Known multicasts* 列中，可以指定设备如何将数据包发送到相应 VLAN 中的已知 Multicast 地址。单击相关字段并选择所需的值。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

10.3 速率限制器

速率限制器功能有助于通过限制端口上的流量确保即使当流量很高时运行也能保持稳定。速率限制对于每个端口是分别执行的，对于输入和输出流量也是单独执行的。

如果端口上的数据速率超过定义的限制，则设备会丢弃该端口上的过载。

速率限制完全在第二层上进行。在此过程中，速率限制器功能会忽略 IP 或 TCP 等更高级别上的协议信息。这会影响到 TCP 流量。

要最大限度降低这些影响，请使用以下选项：

- 将速率限制限制于某些数据包类型，例如，具有未知目标地址的 Broadcasts、Multicasts 和 Unicasts。
- 限制输出数据流量，而非输入流量。采用 TCP 流量控制时，由于设备内部对数据包进行缓冲，输出速率限制能发挥更好的作用。
- 延长示教 Unicast 地址的老化时间。

请执行以下步骤：

- □ 打开 *Switching* > *Rate Limiter* 对话框。
- 激活速率限制器并为数据速率设置范围。这些设置的适用性视端口而定，并按流量类型进行细分：
  - 接收到的 Broadcast 数据包
  - 接收到的 Multicast 数据包
  - 接收到的具有未知目标地址的 Unicast 数据包

  要激活一个端口上的速率限制器，请勾选至少一个类别的复选框。在 *Threshold unit* 列中，指定设备将阈值解释为端口带宽的百分比还是每秒数据包数量。阈值 0 可停用速率限制器。
- □ 暂时保存更改。为此，请单击 按钮。

10.4 QoS/优先级

QoS（服务质量）是 IEEE 802.1D 中定义的用于在网络中分配资源的一项程序。QoS 允许用户对必要应用程序的数据进行优先级排序。

当存在较高的网络负载时，优先级排序有助于防止优先级较低的数据流量干扰对延迟敏感的数据流量。例如，对延迟敏感的数据流量包括语音、视频和实时数据。

10.4.1 优先级排序说明

对于数据流量优先级排序，设备中定义了各种流量类别。根据设备中的定义，较高的流量类别的优先级高于较低的流量类别。流量类别的数量视设备类型而定。

要为对延迟敏感的数据实现最优的数据流量，可以为此数据分配较高的流量类别。可以为对延迟较不敏感的数据分配较低的流量类别。

为数据分配流量类别

设备自动为输入数据分配流量类别（流量分类）。设备会考虑以下分类标准：

- 设备据以将接收到的数据包分配给不同流量类别的方法：
  - trustDot1p
    设备使用 VLAN 标签中包含的数据包的优先级。
  - trustIpDscp
    设备使用 IP 报头中包含的 QoS 信息 (ToS/DiffServ)。
  - untrusted
    设备忽略数据包中可能的优先级信息，直接使用接收端口的优先级。
- 分配给接收端口的优先级。

这两个分类标准均可配置。

在流量分类过程中，设备使用以下规则：

- 当接收端口设置为 trustDot1p（默认设置）时，设备会使用 VLAN 标签中包含的数据包优先级。当数据包不包含 VLAN 标签时，设备会遵循接收端口的优先级。
- 当接收端口设置为 trustIpDscp 时，设备会使用 IP 报头中的 QoS 信息 (ToS/DiffServ)。当数据包不包含 IP 数据包时，设备会遵循接收端口的优先级。
- 当接收端口设置为 untrusted 时，设备会遵循接收端口的优先级。

确定流量类别的优先级

对于各种流量类别的优先级排序，设备会使用以下方法：

- Strict
  当不再传输流量类别较高的数据或相关数据仍在队列中时，设备会发送相应流量类别的数据。如果每个流量类别的优先级都是按照 Strict 方法确定的，则在较高网络负载下，设备可以永久阻塞流量类别较低的数据。
- Weighted Fair Queuing
  为流量类别分配特定的带宽。这有助于确保，即使存在大量流量类别较高的数据流量，设备仍会发送此流量类别的数据流量。

10.4.2 处理接收到的优先级信息

应用程序使用以下优先级排序信息为数据包添加标签：

- 基于 IEEE 802.1Q/802.1D 的 VLAN 优先级（第二层）
- 针对 VLAN 管理 IP 数据包的服务类型（ToS）或区分服务（DSCP）（第三层）

设备允许用户使用以下选项对此优先级信息进行评估：

- trustDot1p
  设备根据其 VLAN 优先级将带有 VLAN 标签的数据包分配给不同的流量类别。相应分配为可配置。设备将接收端口的优先级分配给设备接收到的不带 VLAN 标签的数据包。
- trustIpDscp
  即使 IP 数据包也带有 VLAN 标签，设备仍根据 IP 报头中的 DSCP 值将这些数据包分配给不同的流量类别。相应分配为可配置。设备根据接收端口的优先级确定非 IP 数据包的优先级。
- untrusted
  设备忽略数据包中的优先级信息，并将接收端口的优先级分配给数据包。

10.4.3 VLAN 标签

对于 VLAN 和优先级排序功能，IEEE 802.1Q 标准允许将一个 MAC 帧集成到 VLAN 标签中。VLAN 标签由 4 个字节组成，并且介于源地址字段（“源地址字段”）和类型字段（“长度/类型字段”）之间。

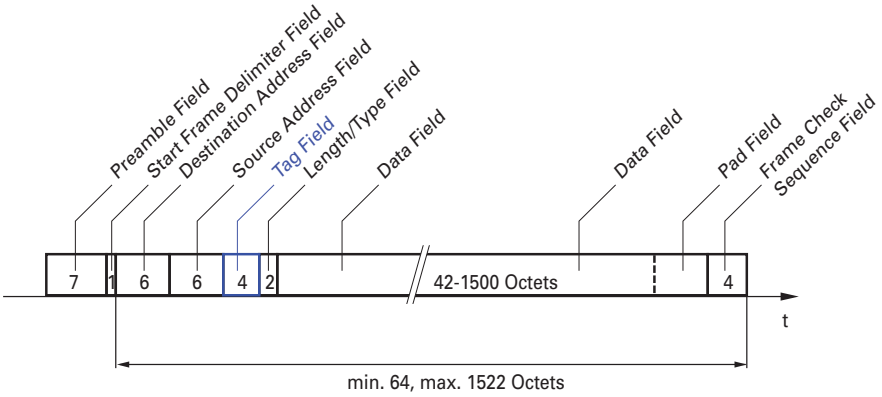


图 23: 带有标签的以太网数据包

对于带有 VLAN 标签的数据包，设备会对以下信息进行评估：

- 优先级信息
- VLAN 标签（配置了 VLAN 时）

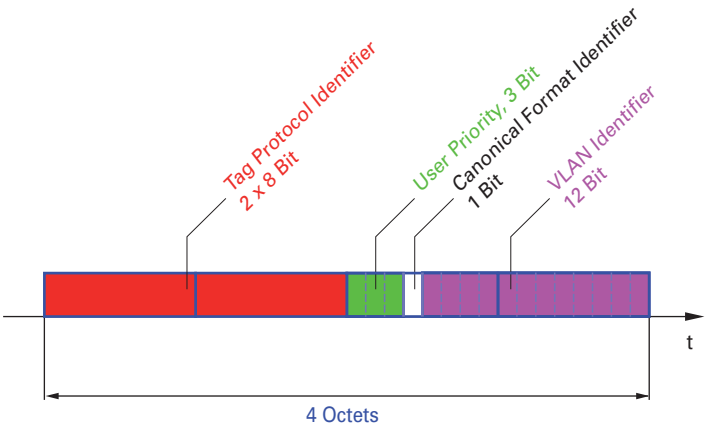


图 24: VLAN 标签的结构

包含优先级信息但不包含 VLAN 信息（VLAN ID = 0）的带有 VLAN 标签的数据包称为优先级标记帧。

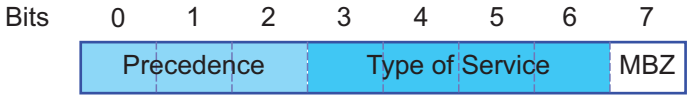
提示：网络协议和冗余机制使用最高流量类别 7。因此，为应用程序数据选择其他流量类别。

使用 VLAN 优先级排序时，请考虑以下特殊功能：
- 端到端优先级排序要求将 VLAN 标签传输到整个网络。前提条件是每个网络组件都支持 VLAN。
- 路由器不能通过基于端口的路由器接口发送和接收带有 VLAN 标签的数据包。

10.4.4 IP ToS（服务类型）

IP 报头中的服务类型字段（ToS）从一开始就已经是 IP 协议的一部分，目前用于区分 IP 网络中的不同服务。即使在当初，由于可用带宽有限和连接路径不可靠，也有人考虑过对 IP 数据包进行区分处理。因为可用带宽不断增加，已经没有必要使用 ToS 字段。

只是随着当今网络实时需求的出现，ToS 字段才再次变得重要起来。通过选择 IP 报头的 ToS 字节，可以对不同服务进行区分。但是，这个字段在实践中应用并不广泛。



表格 22: IP 报头中的 ToS 字段

Bits (0-2): IP Precedence Defined	Bits (3-6): Type of Service Defined	Bit (7)
111 - Network Control	0000 - [all normal]	0 - Zero
110 - Internetwork Control	1000 - [minimize delay]	
101 - CRITIC / ECP	0100 - [maximize throughput	
100 - Flash Override	0010 - [maximize reliability]	
011 - Flash	0001 - [minimize monetary cost]	
010 - Immediate		
001 - Priority		
000 - Routine		

10.4.5 流量类别的处理

设备提供以下处理流量类别的选项：
- Strict Priority
- Weighted Fair Queuing
- Strict Priority 结合 Weighted Fair Queuing
- 队列管理

Strict Priority 描述

使用 Strict Priority 设置，设备首先会传输流量类别较高（优先级较高）的数据包，然后再传输下一级流量类别较高的数据包。当队列中再也没有其他数据包时，设备会传输流量类别最低（优先级最低）的数据包。在不利情况下，如果此端口上有大量高优先级流量等待发送，则设备不会发送优先级低的数据包。

在 VoIP 或视频等对延迟敏感的应用程序中，Strict Priority 允许立即发送数据。

Weighted Fair Queuing 描述

通过 Weighted Fair Queuing（也称为 Weighted Round Robin (WRR)），可向每个流量级别分配最小或预留带宽。这有助于确保即使当网络非常繁忙时也能发送优先级较低的数据包。

预留值的范围为可用带宽的 0% 至 100%，步长为 1%。
- 预留值为 0 等同于“无带宽”设置。
- 单个带宽之和最大可以达到 100%。

将 Weighted Fair Queuing 分配给每个流量类别后，可以使用相应端口的整个带宽。

将 Strict Priority 与 Weighted Fair Queuing 相结合

将 Weighted Fair Queuing 与 Strict Priority 相结合时，请验证 Weighted Fair Queuing 的最高流量类别是否低于 Strict Priority 的最低流量类别。

如果将 Weighted Fair Queuing 与 Strict Priority 相结合，则较高的 Strict Priority 网络负载会显著降低 Weighted Fair Queuing 可用的带宽。

10.4.6 队列管理

Queue Shaping

Queue Shaping 可调整队列传输数据包的速率。例如，使用 Queue Shaping，用户可限制高优先级队列的速率，使低优先级队列能够发送数据包，而且高优先级数据包仍用于传输。设备允许用户为任何队列设置 Queue Shaping。通过分配可用带宽的百分比，用户可将 Queue Shaping 指定为流量通过队列的最大速率。

为队列管理定义设置

请执行以下步骤：

- ☐ 打开 *Switching* > *QoS/Priority* > *Queue Management* 对话框。

Min. bandwidth [%] 列中的总分配带宽为 100%。

- ☐ 要为 *Traffic class* = 0 激活 Weighted Fair Queuing，请按照以下步骤进行操作：
  - ▶ 取消勾选 *Strict priority* 列中的复选框。
  - ▶ 在 *Min. bandwidth [%]* 列中，指定值 5。
- ☐ 要为 *Traffic class* = 1 激活 Weighted Fair Queuing，请按照以下步骤进行操作：
  - ▶ 取消勾选 *Strict priority* 列中的复选框。
  - ▶ 在 *Min. bandwidth [%]* 列中，指定值 20。
- ☐ 要为 *Traffic class* = 2 激活 Weighted Fair Queuing，请按照以下步骤进行操作：
  - ▶ 取消勾选 *Strict priority* 列中的复选框。
  - ▶ 在 *Min. bandwidth [%]* 列中，指定值 30。
- ☐ 要为 *Traffic class* = 3 激活 Weighted Fair Queuing，请按照以下步骤进行操作：
  - ▶ 取消勾选 *Strict priority* 列中的复选框。
  - ▶ 在 *Min. bandwidth [%]* 列中，指定值 20。
- ☐ 要为 *Traffic class* = 4 激活 Weighted Fair Queuing 和 Queue Shaping，请按照以下步骤进行操作：
  - ▶ 取消勾选 *Strict priority* 列中的复选框。
  - ▶ 在 *Min. bandwidth [%]* 列中，指定值 10。
  - ▶ 在 *Max. bandwidth [%]* 列中，指定值 10。

  为特定流量类别使用 Weighted Fair Queuing 和 Queue Shaping 的组合时，请在 *Max. bandwidth [%]* 列中指定一个高于 *Min. bandwidth [%]* 列中指定值的值。
- ☐ 要为 *Traffic class* = 5 激活 Weighted Fair Queuing，请按照以下步骤进行操作：
  - ▶ 取消勾选 *Strict priority* 列中的复选框。
  - ▶ 在 *Min. bandwidth [%]* 列中，指定值 5。
- ☐ 要为 *Traffic class* = 6 激活 Weighted Fair Queuing，请按照以下步骤进行操作：
  - ▶ 取消勾选 *Strict priority* 列中的复选框。
  - ▶ 在 *Min. bandwidth [%]* 列中，指定值 10。
- ☐ 要为 *Traffic class* = 7 激活 Strict Priority 和 Queue Shaping，请按照以下步骤进行操作：
  - ▶ 勾选 *Strict priority* 列中的复选框。
  - ▶ 在 *Max. bandwidth [%]* 列中，指定值 10。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`cos-queue weighted 0`	为流量类别 Weighted Fair Queuing 启用 0。
`cos-queue min-bandwidth: 0 5`	将 5% 权重分配给流量类别 0。
`cos-queue weighted 1`	为流量类别 Weighted Fair Queuing 启用 1。
`cos-queue min-bandwidth: 1 20`	将 20% 权重分配给流量类别 1。
`cos-queue weighted 2`	为流量类别 Weighted Fair Queuing 启用 2。
`cos-queue min-bandwidth: 2 30`	将 30% 权重分配给流量类别 2。

```
cos-queue weighted 3                    为流量类别 Weighted Fair Queuing 启用 3。
cos-queue min-bandwidth: 3 20           将 20% 权重分配给流量类别 3。
show cos-queue
Queue Id  Min. bandwidth  Max. bandwidth  Scheduler type
--------  --------------  --------------  --------------
0         5               0               weighted
1         20              0               weighted
2         30              0               weighted
3         20              0               weighted
4         0               0               strict
5         0               0               strict
6         0               0               strict
7         0               0               strict
```

将 Weighted Fair Queuing 与 Queue Shaping 相结合

请执行以下步骤：

```
enable                                  切换到特权执行模式。
configure                               切换到配置模式。
cos-queue weighted 4                    为流量类别 Weighted Fair Queuing 启用 4。
cos-queue min-bandwidth: 4 10           将 10% 权重分配给流量类别 4。
cos-queue max-bandwidth: 4 10           将 10% 权重分配给流量类别 4。
cos-queue weighted 5                    为流量类别 Weighted Fair Queuing 启用 5。
cos-queue min-bandwidth: 5 5            将 5% 权重分配给流量类别 5。
cos-queue weighted 6                    为流量类别 Weighted Fair Queuing 启用 6。
cos-queue min-bandwidth: 6 10           将 10% 权重分配给流量类别 6。
show cos-queue
Queue Id  Min. bandwidth  Scheduler type
--------  --------------  --------------  --------------
0         5               0               weighted
1         20              0               weighted
2         30              0               weighted
3         20              0               weighted
4         10              10              weighted
5         5               0               weighted
6         10              0               weighted
7         0               0               strict
```

设置 Queue Shaping

请执行以下步骤：

```
enable                                  切换到特权执行模式。
```

```
configure
```
切换到配置模式。

```
cos-queue max-bandwidth: 7 10
```
将 10% 权重分配给流量类别 7。

```
show cos-queue
Queue Id  Min. bandwidth  Scheduler type
--------  --------------  --------------  --------------
0         5               0               weighted
1         20              0               weighted
2         30              0               weighted
3         20              0               weighted
4         10              10              weighted
5         5               0               weighted
6         10              0               weighted
7         0               10              strict
```

10.4.7 管理优先级排序

为了确保用户即使在网络负载较高的情况下仍能访问设备管理，设备允许用户对管理数据包进行优先级排序。

对管理数据包进行优先级排序时，设备会发送具有优先级信息的管理数据包。
- 在第二层上，设备会修改 VLAN 标签中的 VLAN 优先级。
  此功能的前提条件是，将相应端口设置为允许发送带有 VLAN 标签的数据包。
- 在第三层上，设备会修改 IP-DSCP 值。

10.4.8 设置优先级

分配端口优先级

请执行以下步骤：

- ☐ 打开 *Switching* > *QoS/Priority* > *Port Configuration* 对话框。
- ☐ 在 *Port priority* 列中，可以指定设备转发在此端口上接收到的不带 VLAN 标签的数据包时使用的优先级。
- ☐ 在 *Trust mode* 列中，可以指定设备向接收到的数据包分配流量类别时使用的标准。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

```
enable
```
切换到特权执行模式。

```
configure
```
切换到配置模式。

```
interface 1/1
```
切换到接口 1/1 的接口配置模式。

```
vlan priority 3
```
向接口 1/1 分配端口优先级 3。

```
exit
```
切换到配置模式。

向流量类别分配 VLAN 优先级

请执行以下步骤：

- ☐ 打开 *Switching > QoS/Priority > 802.1D/p Mapping* 对话框。
- ☐ 要将流量类别分配给 VLAN 优先级，请在 *Traffic class* 列中插入关联值。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`classofservice dot1p-mapping 0 2`	将 VLAN 优先级 0 分配给流量类别 2。
`classofservice dot1p-mapping 1 2`	将 VLAN 优先级 1 分配给流量类别 2。
`exit`	切换到特权执行模式。
`show classofservice dot1p-mapping`	显示分配。

向接收到的数据包分配端口优先级

请执行以下步骤：

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`interface 1/1`	切换到接口 1/1 的接口配置模式。
`classofservice trust untrusted`	向接口分配 untrusted 模式。
`classofservice dot1p-mapping 0 2`	将 VLAN 优先级 0 分配给流量类别 2。
`classofservice dot1p-mapping 1 2`	将 VLAN 优先级 1 分配给流量类别 2。
`vlan priority 1`	为端口优先级指定值 1。
`exit`	切换到配置模式。
`exit`	切换到特权执行模式。
`show classofservice trust`	显示端口/接口的信任模式。

```
 Interface Trust Mode
 --------- -------------
 1/1       untrusted
 1/2       dot1p
 1/3       dot1p
 1/4       dot1p
 1/5       dot1p
 1/6       dot1p
 1/7       dot1p
```

向流量类别分配 DSCP

请执行以下步骤：

- ☐ 打开 *Switching > QoS/Priority > IP DSCP Mapping* 对话框。
- ☐ 在 *Traffic class* 列中指定所需的值。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

```
enable                                  切换到特权执行模式。
configure                               切换到配置模式。
classofservice  ip-dscp-mapping cs1 1   将 DSCP 值 CS1 分配给流量类别 1。
show classofservice  ip-dscp-mapping    显示 IP DSCP 分配
    IP DSCP       Traffic Class
 -------------    -------------
   be                  2
   1                   2
   .                   .
   .                   .
   (cs1)               1
   .                   .
```

向接收到的 IP 数据包分配 DSCP 优先级

请执行以下步骤：

```
enable                                  切换到特权执行模式。
configure                               切换到配置模式。
interface 1/1                           切换到接口 1/1 的接口配置模式。
classofservice trust ip-dscp            全局分配 trust ip-dscp 模式。
exit                                    切换到配置模式。
show classofservice trust               显示端口/接口的信任模式。
 Interface     Trust Mode
 ----------    -------------
 1/1           ip-dscp
 1/2           dot1p
 1/3           dot1p
 .             .
 .             .
 1/5           dot1p
 .             .
```

配置端口上的流量成形

请执行以下步骤：

```
enable                                  切换到特权执行模式。
configure                               切换到配置模式。
interface 1/2                           切换到接口 1/2 的接口配置模式。
traffic-shape bw 50                     将端口 1/2 的最大带宽限制为 50%。
exit                                    切换到配置模式。
exit                                    切换到特权执行模式。
show traffic-shape                      显示流量成形配置。

Interface  Shaping rate
---------  ------------
1/1        0  %
1/2        50 %
1/3        0  %
1/4        0  %
```

配置第二层管理优先级

请执行以下步骤：

- ☐ 打开 *Switching > QoS/Priority > Global* 对话框。
- ☐ 在 *VLAN priority for management packets* 字段中，指定设备发送管理数据包时使用的 VLAN 优先级。
- ☐ 暂时保存更改。为此，请单击 ✓ 按钮。

```
enable                                  切换到特权执行模式。
network management priority dot1p 7     将 VLAN 优先级 7 分配给管理数据包。设备以最高优先级发送管理数据包。
show network parms                      显示设备管理所在的 VLAN 的优先级。

IPv4 Network
------------
...
Management VLAN priority.....................7
...
```

配置第三层管理优先级

请执行以下步骤：

- ☐ 打开 *Switching > QoS/Priority > Global* 对话框。
- ☐ 在 *IP DSCP value for management packets* 字段中，指定设备发送管理数据包时使用的 DSCP 值。
- ☐ 暂时保存更改。为此，请单击 ✓ 按钮。

`enable`	切换到特权执行模式。
`network management priority ip-dscp 56`	将 DSCP 值 56 分配给管理数据包。设备以最高优先级发送管理数据包。
`show network parms`	显示设备管理所在的 VLAN 的优先级。

```
IPv4 Network
------------
...
Management IP-DSCP value.....................56
```

10.5 流量控制

如果在一个端口的优先队列中同时接收到大量数据包，则这会导致端口内存溢出。例如，当设备在千兆端口上接收数据并将其转发到带宽较低的端口时，就会发生这种情况。设备会丢弃多余的数据包。

IEEE 802.3 标准中介绍的流量控制机制有助于确保端口内存溢出不会导致数据包丢失。在端口内存完全占满之前不久，设备会示意相连设备注意它不再接受来自这些设备的任何数据包。

- 在全双工模式下，设备会发送一个暂停数据包。
- 在半双工模式下，设备会模拟一次冲突。

下图显示了流量控制的工作原理。工作站 1、2 和 3 希望同时向工作站 4 传输大量数据。工作站 1、2 和 3 的总带宽大于工作站 4 的带宽。这将导致端口 4 接收队列上的溢出。左侧漏斗即表示这种状态。

当设备的端口 1、2 和 3 上的流量控制功能启用时，设备会在漏斗发生溢出之前作出反应。右侧漏斗表示端口 1、2 和 3 向传输设备发送一条消息，对传输速度进行控制。这将导致接收端口不再不堪重负，并能够处理发入流量。

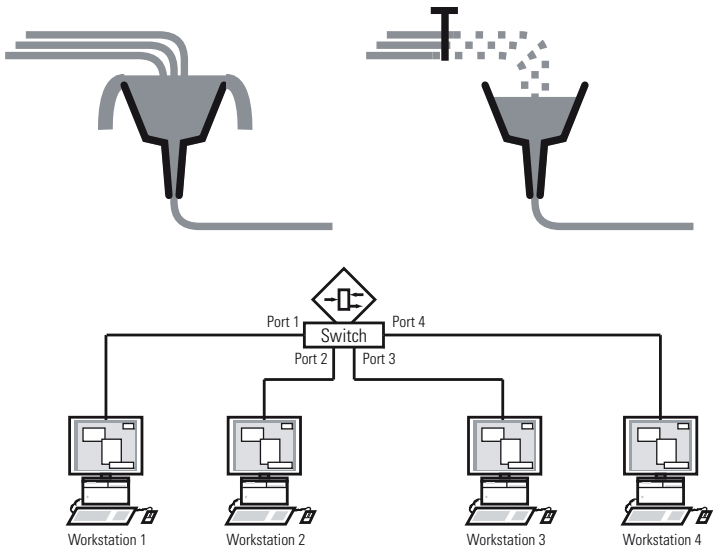


图 25: 流量控制示例

10.5.1 半双工或全双工链路

使用半双工链路的流量控制

在示例中，工作站 2 和设备之间有一个半双工链路。

在端口 2 的发送队列发生溢出之前，设备将数据发回到工作站 2。工作站 2 检测到冲突并停止传输。

使用全双工链路的流量控制

在示例中，工作站 2 和设备之间有一个全双工链路。

在端口 2 的发送队列发生溢出之前，设备会向工作站 2 发送一个请求，以在发送传输中包含一个小的中断。

10.5.2 设置流量控制

请执行以下步骤：

- ☐ 打开 *Switching > Global* 对话框。
- ☐ 勾选 *Flow control* 复选框。
  使用此设置，可以在设备中启用流量控制。
- ☐ 打开 *Basic Settings > Port* 对话框的 *Configuration* 选项卡。
- ☐ 要启用端口上的流量控制，请勾选 *Flow control* 列中的复选框。
- ☐ 暂时保存更改。为此，请单击  按钮。

提示：使用冗余功能时，请停用参与端口上的流量控制。如果流量控制和冗余功能同时激活，则冗余功能的运行可能与预期有所不同。

11 配置基于模板的 TSN

11.1 底层真相

用户使用 *TSN* 功能时，以下基本条件适用：

- 设备采用“Store and Forward”方法进行工作。因此，设备在作出转发决定之前必须先接收完整的数据包。
- 用户可以在设备中一次性指定基准时间和周期时间。这两张设置对于参与 TSN 的每个端口均有效。
- 用户可以基于预定义的模板为每个端口配置门控制列表以简化设置。
- 验证门控制列表条目时间的总和是否小于或等于指定的周期时间。
- 设备使用保护带来帮助保护高优先级数据包的时间段免受从前一个时间段“泄漏”的数据包的影响。保护带间隔长度的决定性因素是发送端口的端口速度。
  我们建议采用以下保护带间隔长度。这些值基于端口速度和以太网数据包的最大允许大小：
  - 2.5 Gbit/s: 5 µs
  - 1 Gbit/s: 13 µs
  - 100 Mbit/s: 124 µs
- 周期时间范围为 50 000..10 000 000 ns。
- 门控制列表间隔范围为 1 000..10 000 000 ns。
- 验证周期时间和门控制列表间隔是否为 1 µs、2 µs 或 4 µs 的倍数。

表格 23: 周期时间与间隔尺寸之间存在依赖关系

周期时间	间隔尺寸
50 µs..4 ms	1 µs
4.002 ms..8 ms	2 µs
8.004 ms..10 ms	4 µs

11.2 示例

本示例描述了如何为具有以下条件的场景设置设备：
- 周期时间 =1 ms
- 高优先级数据包的时间段 =500 µs
- 低优先级数据包的时间段 =487 µs

在此示例中，每个设备均以1 Gbit/s 的端口速度连接到网络。

表格 24: 周期结构

时间段	流量类别	持续时间
高优先级数据包	7	500 µs
低优先级数据包	0, 1, 2, 3, 4, 5, 6	487 µs
保护带	-	13 µs

11.2.1 时间计算

设备自动计算低优先级数据包的时间段持续时间。基于以下参数进行计算：
- 周期时间
- 高优先级数据包的时间段持续时间
- 保护带的持续时间

11.2.2 设置设备

使用先前指定的时间，用户可以使用图形用户界面或命令行界面设置设备。对于涉及的每个设备，请执行以下步骤。

检查并调整周期时间

请执行以下步骤：

☐ 打开 *Switching > TSN > Configuration* 对话框。

☐ 在 *Configuration* 框中，检查 *Cycle time [ns]* 字段中的值。

☐ 根据需要调整该值。

☐ 暂时保存更改。为此，请单击 ✓ 按钮。

```
enable                                          切换到特权执行模式。
configure                                       切换到配置模式。
show tsn configuration
Port  Status                 Conf. cycle time[ns]  Conf. base time
      Default gate states    Curr. cycle time[ns]  Curr. base time
      Config change pending                        Time of last activation
----  ---------------------  --------------------  ----------------------------
 1/1  [x]           disabled              1000000  1970-01-01 00:00:00.000000000
      7,6,5,4,3,2,1,0                     1000000  1970-01-01 00:00:00.000000000
      [ ]                                          2018-07-12 08:10:58.813000000

 1/2  [x]           disabled              1000000  1970-01-01 00:00:00.000000000
      7,6,5,4,3,2,1,0                     1000000  1970-01-01 00:00:00.000000000
      [ ]                                          2018-07-11 07:24:35.204000000

 1/3  [ ]           disabled              1000000  1970-01-01 00:00:00.000000000
      7,6,5,4,3,2,1,0                           0  1970-01-01 00:00:00.000000000
      [ ]                                          1970-01-01 00:00:00.000000000

 1/4  [ ]           disabled              1000000  1970-01-01 00:00:00.000000000
      7,6,5,4,3,2,1,0                           0  1970-01-01 00:00:00.000000000
      [ ]                                          1970-01-01 00:00:00.000000000

tsn cycle-time 1000000                          根据需要调整该值。
```

选择模板并设置门控制列表

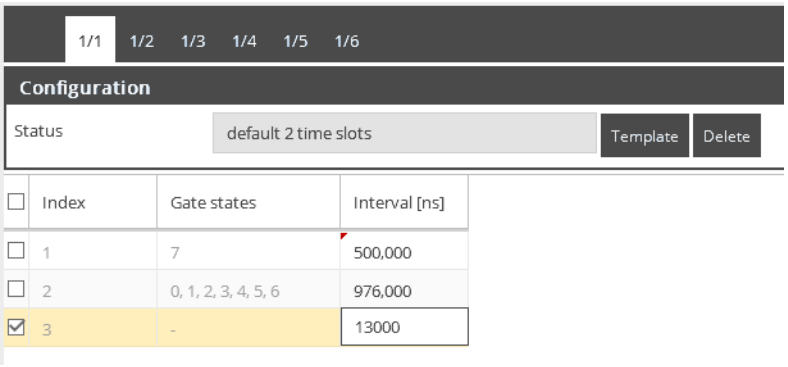
设备提供了可帮助用户设置门控制列表的预定义模板。在此示例中，我们使用模板 *default 2 time slots*。选择模板后，用户可以调整时间段的持续时间。对要使用 *TSN* 功能的每个端口执行以下步骤。

请执行以下步骤：

- ☐ 打开 *Switching > TSN > Gate Control List > Configured* 对话框。
- ☐ 选择要为其指定设置的端口的选项卡。

☐ 在 *Configuration* 框中选择一个模板。
请执行以下步骤：
- 点击 *Template* 按钮。
- 选择 *default 2 time slots* 项目。
- 点击 *Ok* 按钮。

☐ 调整 *Interval [ns]* 列中的值：
- 在高优先级数据包的行中输入值 500000。
- 在保护带的行中输入值 13000。
- 保存更改后，设备会自动计算第三个值。



☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`interface 1/1`	切换到接口 1/1 的接口配置模式。
`tsn gcl modify 1 interval 500000`	调整高优先级数据包时间段的持续时间（纳秒）。
`tsn gcl modify 3 interval 13000`	调整保护带时间段的持续时间（纳秒）。 设备自动计算低优先级数据包时间段的持续时间。 用户无法设置低优先级数据包的时间段。

12 VLAN

在最简单的情况下，一个虚拟局域网 (VLAN) 由一个网段中的一组网络参与者组成，它们可以相互通信，就像分别属于不同的 LAN 一样。

更加复杂的 VLAN 会跨越多个网段，并且也基于网络参与者之间的逻辑（而非仅是物理）连接。VLAN 是灵活网络设计的基本组成部分。与电缆连接相比，以集中方式对逻辑连接进行重新配置更加容易。

设备支持符合定义 *VLAN* 功能的 IEEE 802.1Q 标准的独立 VLAN 示教。

使用 VLAN 具有诸多好处。以下列表显示了最重要的优点：

- 网络负载限制
  VLAN 可以极大降低网络负载，这是因为，设备只在虚拟 LAN 内部传输具有未知（未示教）目标地址的 Broadcast、Multicast 和 Unicast 数据包。数据网络的其余部分照常转发流量。
- 灵活
  除物理位置或介质之外，您还可以选择根据参与者的功能建立用户组。
- 清晰
  VLAN 为网络提供了一个清晰的结构，使维护更加容易。

12.1 VLAN 示例

以下实际示例简单介绍了 VLAN 的结构。

提示：配置 VLAN 时，可以使用一个将保持不变的接口来访问设备管理。对于此示例，可以使用接口 1/6 或串行连接对 VLAN 进行配置。

12.1.1 示例 1

该示例显示了一个最低 VLAN 配置（基于端口的 VLAN）。管理员将多个终端设备连接到一个传输设备，并将它们分配给两个 VLAN。这实际上禁止了 VLAN 之间的任何数据传输，其成员只能在它们自己的 VLAN 中进行通信。

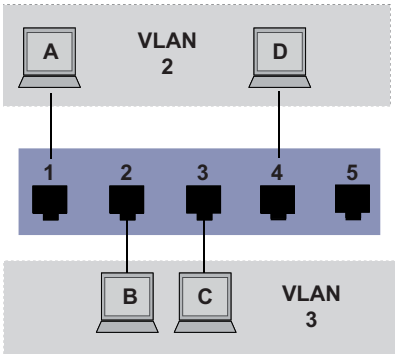


图 26: 基于端口的简单 VLAN 示例

建立 VLAN 时，可以为每个端口创建通信规则，并将其输入到入口（发入）表和出口（发出）表中。

入口表可指定一个端口将哪个 VLAN ID 分配给发入数据包。在此，可以使用终端设备的端口地址将其分配到一个 VLAN。

出口表可指定设备在哪些端口上发送来自此 VLAN 的数据包。
- T = 带标签（具有标签字段，已勾选）
- U = 不带标签（没有标签字段，未勾选）

对于此示例，数据包的 TAG 字段的状态没有意义，因此，使用设置 U。

表格 25: 入口表格

终端	端口	端口 VLAN 标识符 (PVID)
A	1	2
B	2	3
C	3	3
D	4	2
	5	1

表格 26: 出口表格

VLAN ID	端口				
	1	2	3	4	5
1					U
2	U			U	
3		U	U		

请执行以下步骤：
☐ 建立 VLAN

☐ 打开 *Switching > VLAN > Configuration* 对话框。

☐ 点击  按钮。
该对话框显示 *Create* 窗口。

☐ 在 *VLAN ID* 字段中，指定值 2。

☐ 点击 *Ok* 按钮。

☐ 对于该 VLAN，指定名称 VLAN2。
双击 *Name* 列并指定名称。
对于 VLAN 1，在 *Name* 列中，将值 Default 更改为 VLAN1。

☐ 重复之前的步骤，创建名称为 3 的 VLAN VLAN3。

`enable`	切换到特权执行模式。
`vlan database`	切换到 VLAN 配置模式。
`vlan add 2`	创建一个 VLAN ID 为 2 的新 VLAN。
`name 2 VLAN2`	将名称 2 分配给 VLAN VLAN2。
`vlan add 3`	创建一个 VLAN ID 为 3 的新 VLAN。
`name 3 VLAN3`	将名称 3 分配给 VLAN VLAN3。
`name 1 VLAN1`	将名称 1 分配给 VLAN VLAN1。
`exit`	切换到特权执行模式。
`show vlan brief`	显示当前 VLAN 配置。

```
Max. VLAN ID..................................... 4042
Max. supported VLANs............................. 128
Number of currently configured VLANs............ 3
vlan unaware mode................................ disabled
VLAN ID VLAN Name                       VLAN Type VLAN Creation Time
---- -------------------------------- --------- -------------------
1       VLAN1                           default    0 days, 00:00:05
2       VLAN2                           static     0 days, 02:44:29
3       VLAN3                           static     0 days, 02:52:26
```

☐ 建立端口

☐ 打开 *Switching > VLAN > Port* 对话框。

☐ 要将端口分配给一个 VLAN，请在相应列中指定所需值。
可能的值：
- T = 端口是 VLAN 的成员。端口传输带有标签的数据包。
- U = 端口是 VLAN 的成员。端口传输不带标签的数据包。
- F = 端口不是 VLAN 的成员。
  使用 *GVRP* 功能进行的更改已禁用。
- - = 端口不是此 VLAN 的成员。
  使用 *GVRP* 功能进行的更改已允许。

由于终端设备一般都对不带标签的数据包进行解释，因此指定值 U。

☐ 暂时保存更改。为此，请单击 ✔ 按钮。

☐ 打开 *Switching > VLAN > Port* 对话框。

☐ 在 *Port-VLAN ID* 列中，指定相关 VLAN 的 VLAN ID：
2 或 3

☐ 由于终端设备一般都对不带标签的数据包进行解释，因此在 *Acceptable packet types* 列中，为终端设备端口指定值 admitAll。

☐ 暂时保存更改。为此，请单击 ✔ 按钮。

Ingress filtering 列中的值对此示例如何工作没有影响。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`interface 1/1`	切换到接口 1/1 的接口配置模式。
`vlan participation include 2`	端口 1/1 成为 VLAN 2 的成员并传输不带 VLAN 标签的数据包。
`vlan pvid 2`	将端口 VLAN ID 1/1 分配给端口 2。
`exit`	切换到配置模式。

`interface 1/2`	切换到接口 1/2 的接口配置模式。
`vlan participation include 3`	端口 1/2 成为 VLAN 3 的成员并传输不带 VLAN 标签的数据包。
`vlan pvid 3`	将端口 VLAN ID 1/2 分配给端口 3。
`exit`	切换到配置模式。
`interface 1/3`	切换到接口 1/3 的接口配置模式。
`vlan participation include 3`	端口 1/3 成为 VLAN 3 的成员并传输不带 VLAN 标签的数据包。
`vlan pvid 3`	将端口 VLAN ID 1/3 分配给端口 3。
`exit`	切换到配置模式。
`interface 1/4`	切换到接口 1/4 的接口配置模式。
`vlan participation include 2`	端口 1/4 成为 VLAN 2 的成员并传输不带 VLAN 标签的数据包。
`vlan pvid 2`	将端口 VLAN ID 1/4 分配给端口 2。
`exit`	切换到配置模式。
`exit`	切换到特权执行模式。
`show vlan id 3`	显示 VLAN 3 的详细信息。

```
VLAN ID           : 3
VLAN Name         : VLAN3
VLAN Type         : Static
Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1            -      Autodetect   Tagged
1/2         Include   Include      Untagged
1/3         Include   Include      Untagged
1/4            -      Autodetect   Tagged
1/5            -      Autodetect   Tagged
```

12.1.2 示例 2

第二个示例显示了具有三个 VLAN（1 至 3）的更复杂的配置。除示例 1 中的交换机之外，在此还使用第二个交换机（本例中右侧）。

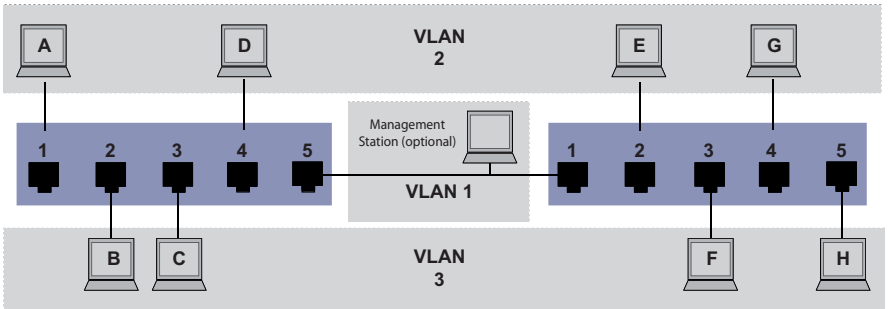


图 27: 更复杂的 VLAN 配置示例

各个 VLAN（A 至 H）的终端设备跨越两个传输设备（交换机）。因此，这种 VLAN 称为分布式 VLAN。如果正确配置了 VLAN，则还会显示一个允许访问每个网络组件的可选网络管理站。

提示：在这种情况下，VLAN 1 对于终端设备通信没有意义，但是，它却是通过所谓的管理 VLAN 对传输设备进行管理的必要环节。

与上一个示例一样，将相连终端设备的端口唯一地分配给一个 VLAN。借助两个传输设备之间的直接连接（上行链路），这些端口传输这两个 VLAN 的数据包。为了区分这些上行链路，可以使用能相应处理数据包的“VLAN 标签”。这样，即可保持对相应 VLAN 的分配。

请执行以下步骤：

- ☐ 将上行链路端口 5 添加到示例 1 的入口表和出口表中。
- ☐ 如第一个示例所示，为右侧交换机创建新的入口表和出口表。

出口表可指定设备在哪些端口上发送来自此 VLAN 的数据包。

- ▶ T = 带标签（具有标签字段，已勾选）
- ▶ U = 不带标签（没有标签字段，未勾选）

在此示例中，传输设备之间的通信使用带有标签的数据包 (Uplink)，这是因为，这些端口上对不同 VLAN 的数据包进行了区分。

表格 27: 左侧设备入口表格

终端	端口	端口 VLAN 标识符 (PVID)
A	1	2
B	2	3
C	3	3
D	4	2
Uplink	5	1

表格 28: 右侧设备入口表格

终端	端口	端口 VLAN 标识符 (PVID)
Uplink	1	1
E	2	2
F	3	3
G	4	2
H	5	3

表格 29: 左侧设备出口表格

VLAN ID	端口				
	1	2	3	4	5
1					U
2	U			U	T
3		U	U		T

表格 30: 右侧设备出口表格

VLAN ID	端口				
	1	2	3	4	5
1	U				
2	T	U		U	
3	T		U		U

这里的通信关系如下：左侧设备端口 1 和 4 上的终端设备以及右侧设备端口 2 和 4 上的终端设备是 VLAN 2 的成员，因此可以彼此进行通信。左侧设备端口 2 和 3 上的终端设备以及右侧设备端口 3 和 5 上的终端设备的行为是相同的。这些都属于 VLAN 3。

终端设备“能看到”它们在网络中的相应部分。无法访问此 VLAN 以外的参与者。设备也仅在一个 VLAN 内部发送具有未知（未示教）目标地址的 Broadcast、Multicast 和 Unicast 数据包。

在此，设备在 ID 为 1 的 VLAN 内部使用 VLAN 标签 (IEEE 801.1Q)（上行链路）。端口出口表中的字母 T 表示 VLAN 标签。

右侧设备的示例配置与此相同。以相同方式进行操作，使用前面创建的入口表和出口表使之前配置的左侧设备适应新的环境。

请执行以下步骤：

☐ 建立 VLAN

- ☐ 打开 *Switching > VLAN > Configuration* 对话框。
- ☐ 点击  按钮。
  该对话框显示 *Create* 窗口。
- ☐ 在 *VLAN ID* 字段中，指定 VLAN ID，如 2。
- ☐ 点击 *Ok* 按钮。
- ☐ 对于该 VLAN，指定名称 VLAN2。
  双击 *Name* 列并指定名称。
  对于 VLAN 1，在 *Name* 列中，将值 Default 更改为 VLAN1。
- ☐ 重复之前的步骤，创建名称为 3 的 VLAN VLAN3。

```
enable                                  切换到特权执行模式。
vlan database                           切换到 VLAN 配置模式。
vlan add 2                              创建一个 VLAN ID 为 2 的新 VLAN。
name 2 VLAN2                            将名称 2 分配给 VLAN VLAN2。
vlan add 3                              创建一个 VLAN ID 为 3 的新 VLAN。
name 3 VLAN3                            将名称 3 分配给 VLAN VLAN3。
name 1 VLAN1                            将名称 1 分配给 VLAN VLAN1。
exit                                    切换到特权执行模式。
show vlan brief                         显示当前 VLAN 配置。
Max. VLAN ID..................................... 4042
Max. supported VLANs............................. 128
Number of currently configured VLANs............ 3
vlan unaware mode................................ disabled
VLAN ID VLAN Name                       VLAN Type VLAN Creation Time
---- -------------------------------- --------- -------------------
1       VLAN1                           default    0 days, 00:00:05
2       VLAN2                           static     0 days, 02:44:29
3       VLAN3                           static     0 days, 02:52:26
```

☐ 建立端口

☐ 打开 *Switching > VLAN > Port* 对话框。

☐ 要将端口分配给一个 VLAN，请在相应列中指定所需值。
可能的值：
- T = 端口是 VLAN 的成员。端口传输带有标签的数据包。
- U = 端口是 VLAN 的成员。端口传输不带标签的数据包。
- F = 端口不是 VLAN 的成员。
  使用 *GVRP* 功能进行的更改已禁用。
- - = 端口不是此 VLAN 的成员。
  使用 *GVRP* 功能进行的更改已禁用。

由于终端设备一般都对不带标签的数据包进行解释，因此指定值 U。
在各个 VLAN 通过其相互通信的上行链路端口上指定 T 设置。

☐ 暂时保存更改。为此，请单击 ✔ 按钮。

☐ 打开 *Switching > VLAN > Port* 对话框。

☐ 在 *Port-VLAN ID* 列中，指定相关 VLAN 的 VLAN ID：
1、2 或 3

☐ 由于终端设备一般都对不带标签的数据包进行解释，因此在 *Acceptable packet types* 列中，为终端设备端口指定值 admitAll。

☐ 对于上行链路端口，在 *Acceptable packet types* 列中，指定值 admitOnlyVlanTagged。

☐ 勾选 *Ingress filtering* 列中的复选框，使上行链路端口对此端口上的 VLAN 标签进行评估。

☐ 暂时保存更改。为此，请单击 ✔ 按钮。

```
enable                                  切换到特权执行模式。
configure                               切换到配置模式。
interface 1/1                           切换到接口 1/1 的接口配置模式。
```

vlan participation include 1	端口 1/1 成为 VLAN 1 的成员并传输不带 VLAN 标签的数据包。
vlan participation include 2	端口 1/1 成为 VLAN 2 的成员并传输不带 VLAN 标签的数据包。
vlan tagging 2 enable	端口 1/1 成为 VLAN 2 的成员并传输带有 VLAN 标签的数据包。
vlan participation include 3	端口 1/1 成为 VLAN 3 的成员并传输不带 VLAN 标签的数据包。
vlan tagging 3 enable	端口 1/1 成为 VLAN 3 的成员并传输带有 VLAN 标签的数据包。
vlan pvid 1	将端口 VLAN ID 1 分配给端口 1/1。
vlan ingressfilter	激活端口 1/1 上的入口筛选。
vlan acceptframe vlanonly	端口 1/1 只转发带有 VLAN 标签的数据包。
exit	切换到配置模式。
interface 1/2	切换到接口 1/2 的接口配置模式。
vlan participation include 2	端口 1/2 成为 VLAN 2 的成员并传输不带 VLAN 标签的数据包。
vlan pvid 2	将端口 VLAN ID 2 分配给端口 1/2。
exit	切换到配置模式。
interface 1/3	切换到接口 1/3 的接口配置模式。
vlan participation include 3	端口 1/3 成为 VLAN 3 的成员并传输不带 VLAN 标签的数据包。
vlan pvid 3	将端口 VLAN ID 3 分配给端口 1/3。
exit	切换到配置模式。
interface 1/4	切换到接口 1/4 的接口配置模式。
vlan participation include 2	端口 1/4 成为 VLAN 2 的成员并传输不带 VLAN 标签的数据包。
vlan pvid 2	将端口 VLAN ID 2 分配给端口 1/4。
exit	切换到配置模式。
interface 1/5	切换到接口 1/5 的接口配置模式。
vlan participation include 3	端口 1/5 成为 VLAN 3 的成员并传输不带 VLAN 标签的数据包。
vlan pvid 3	将端口 VLAN ID 3 分配给端口 1/5。
exit	切换到配置模式。

```
exit
```

切换到特权执行模式。

```
show vlan id 3
```

显示 VLAN 3 的详细信息。

```
VLAN ID.....................3
VLAN Name...................VLAN3
VLAN Type...................Static
VLAN Creation Time...........0 days, 00:07:47 (System Uptime)
VLAN Routing................disabled

Interface   Current   Configured   Tagging
----------  --------  -----------  --------
1/1         Include   Include      Tagged
1/2         -         Autodetect   Untagged
1/3         Include   Include      Untagged
1/4         -         Autodetect   Untagged
1/5         Include   Include      Untagged
```

12.2 访客 LAN/未经身份验证的 VLAN

访客 VLAN 允许设备向不支持 802.1x 的申请者提供基于端口的网络访问控制 (IEEE 802.1x)。此功能提供了一种允许访客只访问外部网络的机制。如果将不支持 802.1x 的申请者连接到一个活动的未授权 802.1x 端口，则申请者不对 802.1x 请求作出响应。由于申请者不发送任何响应，端口将保持未经授权的状态。申请者无法访问外部网络。

访客 VLAN 申请者属于基于端口的配置。当您将一个端口配置为访客 VLAN 并将不支持 802.1x 的申请者连接到此端口时，设备会将这些申请者分配给该访客 VLAN。向一个访客 VLAN 添加申请者可使端口变为授权状态，从而允许申请者访问外部网络。

未经身份验证的 VLAN 允许设备向未正确进行身份验证、支持 802.1x 的申请者提供服务。此功能允许未经授权的申请者访问有限的服务。如果在一个具有 802.1x 端口身份验证功能的端口上配置一个未经身份验证的 VLAN 且全局运行已启用，则设备会将该端口放入一个未经身份验证的 VLAN 中。当一个支持 802.1x 的申请者在端口上未正确进行身份验证时，设备会将该申请者添加到未经身份验证的 VLAN 中。如果在端口上还配置一个访客 VLAN，则不支持 802.1x 的申请者可以使用该访客 VLAN。

如果已向该端口分配一个未经身份验证的 VLAN，则重新身份验证计时器开始倒计时。当 *Reauthentication period [s]* 列中指定的时间到期且端口上存在申请者时，未经身份验证的 VLAN 会重新进行身份验证。当不存在申请者时，设备会将该端口放入已配置的访客 VLAN 中。

以下示例解释了如何创建访客 VLAN。以相同方式创建一个未经授权的 VLAN。

请执行以下步骤：

- ☐ 打开 *Switching* > *VLAN* > *Configuration* 对话框。
- ☐ 点击 按钮。
  该对话框显示 *Create* 窗口。
- ☐ 在 *VLAN ID* 字段中，指定值 10。
- ☐ 点击 *Ok* 按钮。
- ☐ 对于该 VLAN，指定名称 Guest：
  双击 *Name* 列并指定名称。
- ☐ 点击 按钮。
  该对话框显示 *Create* 窗口。
- ☐ 在 *VLAN ID* 字段中，指定值 20。
- ☐ 点击 *Ok* 按钮。
- ☐ 对于该 VLAN，指定名称未经授权：
  双击 *Name* 列并指定名称。
- ☐ 打开 *Network Security* > *802.1X Port Authentication* > *Global* 对话框。
- ☐ 要启用该功能，请选择 *Operation* 框中的 *On* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 按钮。
- ☐ 打开 *Network Security* > *802.1X Port Authentication* > *Port Configuration* 对话框。
- ☐ 为端口 1/4 指定以下设置：
  - *Port control* 列中的值 auto
  - *Guest VLAN ID* 列中的值 10
  - *Unauthenticated VLAN ID* 列中的值 20
- ☐ 暂时保存更改。为此，请单击 按钮。

`enable`	切换到特权执行模式。
`vlan database`	切换到 VLAN 配置模式。
`vlan add 10`	创建 VLAN 10。
`vlan add 20`	创建 VLAN 20。
`name 10 Guest`	将 VLAN 10 重命名为 Guest。
`name 20 Unauth`	将 VLAN 20 重命名为 Unauth。
`exit`	切换到特权执行模式。
`configure`	切换到配置模式。
`dot1x system-auth-control enable`	全局启用 *802.1X Port Authentication* 功能。
`dot1x port-control auto`	启用端口 1/4 上的端口控制。
`interface 1/4`	切换到接口 1/4 的接口配置模式。
`dot1x guest-vlan 10`	将访客 vlan 分配给端口 1/4。
`dot1x unauthenticated-vlan 20`	将未经授权的 vlan 分配给端口 1/4。
`exit`	切换到配置模式。

12.3 RADIUS VLAN 分配

RADIUS VLAN 分配功能可以将一个 RADIUS VLAN ID 属性与一个经过身份验证的客户端关联起来。当一个客户端成功进行身份验证且 RADIUS 服务器发送一个 VLAN 属性时，设备会将该客户端与 RADIUS 分配的 VLAN 关联起来。因此，设备会将物理端口作为成员添加到相应的 VLAN，并使用给定值设置端口 VLAN ID (PVID)。端口传输不带 VLAN 标签的数据包。

12.4 创建语音 VLAN

使用语音 VLAN 功能按 VLAN 和/或优先级将端口上的语音流量和数据流量分开。使用语音 VLAN 的一个主要优点是，在端口上的数据流量较高的情况下，可以保证 IP 电话的音质。

设备使用源 MAC 地址对语音数据流进行标识和优先级排序。使用 MAC 地址对设备进行标识，有助于防止流氓客户端连接到同一端口，导致语音流量恶化。

语音 VLAN 功能的另一个优点是，VoIP 电话可以使用 LLDP-MED 获取 VLAN ID 或优先级信息。因此，VoIP 电话会发送带有标签、带有优先级标签或不带标签的语音数据。这取决于语音 VLAN 接口配置。

可能的语音 VLAN 接口模式如下。前三种方法对语音和数据流量进行隔离和优先级排序。在流量较高的时间段，流量隔离可以提高语音流量质量。

- 将端口配置为使用 vlan 模式，可使设备使用用户自定义语音 VLAN ID 为来自 VoIP 电话的语音数据添加标签。设备会将常规数据分配给默认端口 VLAN ID。
- 将端口配置为使用 dot1p-priority 模式，可使设备使用 VLAN 0 和用户自定义优先级为来自 VoIP 电话的数据添加标签。设备会将端口的默认优先级分配给常规数据。
- 将语音 VLAN ID 和优先级都配置为使用 vlan/dot1p-priority 模式。在此模式下，VoIP 电话会发送带有用户自定义语音 VLAN ID 和优先级信息的语音数据。设备会将端口的默认 PVID 和优先级分配给常规数据。
- 配置为 untagged 时，电话会发送不带标签的数据包。
- 配置为 none 时，电话会使用自己的配置发送语音流量。

13 冗余

13.1 网络拓扑与冗余协议

使用以太网时，一个重要的前提条件是，数据包遵循从发送者到接收者的单一（唯一）路径。以下网络拓扑支持此前提条件：

- 线形拓扑
- 星形拓扑
- 树形拓扑

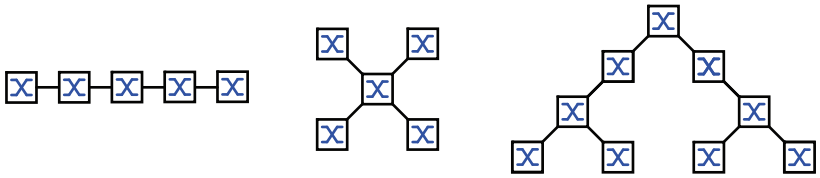


图 28: 采用线形、星形和树形拓扑的网络

要在检测到连接故障时保持通信，请在网络节点之间安装额外的物理连接。冗余协议有助于确保在原始连接仍然工作时额外连接保持关闭状态。当检测到连接失败时，冗余协议会通过替代连接生成从发送方到接收方的新路径。

要在网络的第二层上引入冗余，请首先确定您需要何种网络拓扑。然后根据所选的网络拓扑，选择可以与这种网络拓扑一起使用的冗余协议。

13.1.1 网络拓扑

网状拓扑

对于采用星形或树形拓扑的网络，只可能在物理环路创建时执行冗余过程。结果就是一个网状拓扑。

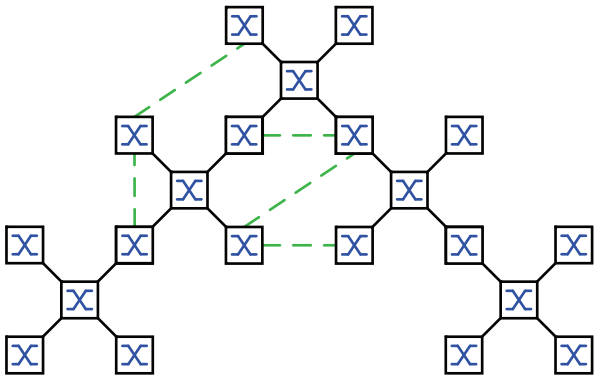


图 29: 网状拓扑：具有物理环路的树形拓扑

对于这种网络拓扑中的操作，设备为用户提供以下冗余协议：
- 快速生成树 (RSTP)

环形拓扑

在采用线形拓扑的网络中，可以通过连接线路的两端来使用冗余过程。这可创建一个环形拓扑。

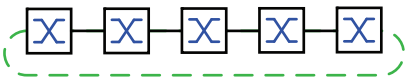


图 30: 环形拓扑：具有相连两端的线形拓扑

对于这种网络拓扑中的操作，设备为用户提供以下冗余协议：
- 介质冗余协议 (MRP)
- 快速生成树 (RSTP)

13.1.2 冗余协议

对于不同网络拓扑中的操作，设备为用户提供以下冗余协议：

表格 31: 冗余协议概述

冗余协议	网络拓扑	注释
MRP	环形	可以选择切换时间，该时间实际上与设备的数量无关。 一个 MRP 环网由支持符合 IEC 62439 的 MRP 协议的多达 50 台设备组成。 当用户仅使用 Schneider Electric 设备时，MRP 环网中可以连接最多 100 台设备。
子环网	环形	*Sub Ring* 功能允许用户将网段轻松耦合到现有冗余环网。
环网/网络耦合	环形	
RCP	环形	
RSTP	随机结构	切换时间视网络拓扑和设备数量而定。 - 使用 RSTP 时的典型 < 1 秒 - 使用 RSTP 时的典型 < 30 秒
链路聚合	随机结构	一个链路聚合组是在一个交换机上以相同速率工作的两个或更多全双工点到点链路的组合，可以增加带宽。
链路备份	随机结构	当设备检测到一级链路上的错误时，会将流量传输到备份链路。一般在服务提供商或企业网络中使用链路备份。
HIPER 环网客户端	环形	对现有 HIPER 环网进行扩展，或替换已经作为客户端参与 HIPER 环网的设备。
LAG 上的 HIPER 环网	环形	通过链路聚合组 (LAG) 将设备链接在一起。环网客户端和环网管理器的行为方式与没有 LAG 实例的环网相同。

如果流量控制和冗余功能同时激活，则冗余功能的运行可能与预期有所不同。

⚠ 警告

不允许的设备操作

如果用户正在使用冗余功能，则将停用参与设备端口上的流量控制。

如果不遵循这些说明，则会导致死亡、重伤或设备损坏。

13.1.3 冗余组合

表格 32: 冗余协议概述

	MRP	RSTP	????	????	???	HIPER ??
MRP	▲	– – –	– – –	– – –	– – –	– – –
RSTP	▲1)	▲	– – –	– – –	– – –	– – –
????	▲2)	▲2)	▲	– – –	– – –	– – –
????	▲	▲	▲	▲	– – –	– – –
???	▲	▲	▲2)	▲	▲	– – –
HIPER ??	▲	▲1)	▲2)	▲	▲	▲

▲ 适用的组合

1) 这些网络拓扑之间的冗余耦合可能会导致环路。
要冗余耦合这些拓扑，请参阅 “FuseNet” 页 207 一章。

2) 同一端口上适用的组合

13.2 介质冗余协议 (MRP)

自 2008 年 5 月以来，介质冗余协议 (MRP) 一直都是针对工业环境中环网冗余的标准化解决方案。

MRP 与冗余环网耦合兼容，支持 VLAN，并且重新配置时间非常短。

一个 MRP 环网由支持符合 IEC 62439 的 MRP 协议的多达 50 台设备组成。当用户仅使用 Schneider Electric 设备时，MRP 环网中可以连接最多 100 台设备。

当您使用固定 MRP 冗余端口（Fixed Backup）并检测到主环链路故障时，环管理器将数据转发到辅助环链路。当一级链路恢复时，二级链路将继续保持使用状态。

13.2.1 网络结构

环网冗余概念允许用户构建高可用性的环形网络结构。

借助 RM（**环**网**管**理器）功能，可以将线形结构中一个骨干的两端闭合起来，形成冗余环网。只要线形结构完好无损，环网管理器就会使冗余线路保持打开。当某个网段无法工作时，环网管理器会立即将冗余线路闭合起来，线形结构再次变得完好无损。

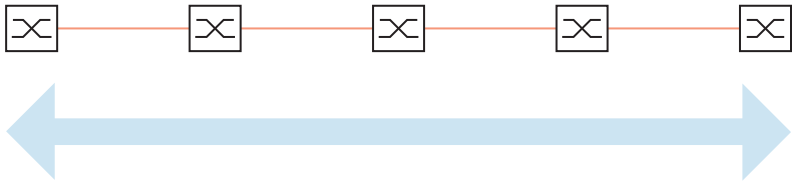


图 31: 线形结构

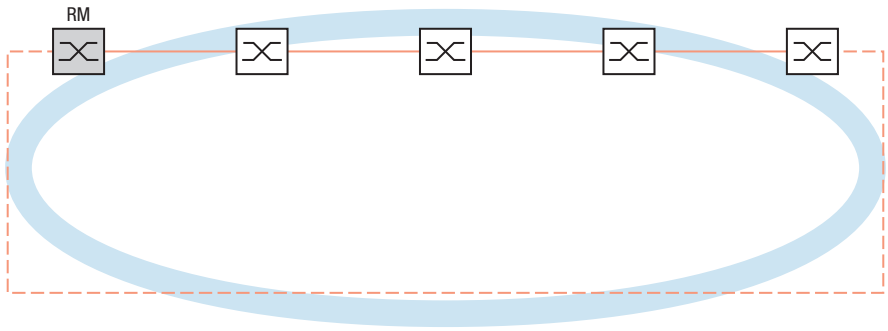


图 32: 冗余环形结构
RM = 环网管理器
—— 主线路
- - - 冗余线路

13.2.2 重新配置时间

当检测到线路部分故障时，环管理器将 MRP-Ring 更改回线路结构。可以在环网管理器中定义线路重新配置的最大时间。

最大延迟时间的可能值：

- *500ms*
- *30ms*

提示：如果环网中的每个设备都支持较短的延迟时间，则可以配置数值小于 *500ms* 的重新配置时间。

否则，过载可能会导致无法访问只支持较长延迟时间的设备。因此，可能会形成环路。

13.2.3 高级模式

对于比指定重新配置时间更短的时间，设备提供了高级模式。当环网参与者通过链路关闭通知向环网管理器告知环网中断时，高级模式会加快链路故障识别。

Schneider Electric 设备支持链路关闭通知。因此，一般应激活环网管理器中的高级模式。

当您正在使用不支持链路关闭通知的设备时，环网管理器会重新配置所选最大重新配置时间中的线路。

13.2.4 MRP 的前提条件

在设置 MRP 环网之前，请先确认是否满足以下条件：
- ▶ 所有环网参与者都支持 MRP。
- ▶ 环网参与者通过环网端口彼此连接。除设备的相邻设备之外，没有其他环网参与者连接到相应设备。
- ▶ 所有环网参与者都支持环网管理器中指定的配置时间。
- ▶ 环网中只有一个环网管理器。

如果您正在使用 VLAN，则请使用以下设置配置每个环网端口：
- ☐ 停用入口过滤 - 参见 *Switching > VLAN > Port* 对话框。
- ☐ 定义端口 VLAN ID (PVID) - 参见*Switching > VLAN > Port* 对话框。
  - 当设备传输不带标签的 MRP 数据包时，PVID = 1 （0 对话框中 VLAN ID = *Switching > L2-Redundancy > MRP*）
    通过设置 PVID = 1，设备会将接收到的不带标签的数据包自动分配到 VLAN 1。
  - 当设备在一个 VLAN 中传输 MRP 数据包时，PVID = any（1 对话框中 VLAN ID ≥ *Switching > L2-Redundancy > MRP*
- ☐ 定义出口规则 - 参见 *Switching > VLAN > Configuration* 对话框。
  - 当设备传输不带标签的 MRP 数据包时，VLAN 1 的环网端口为 U（不带标签）（0 对话框中 VLAN ID = *Switching > L2-Redundancy > MRP*，MRP 环网没有分配到 VLAN）。
  - 为 MRP 环网分配的 VLAN 的环网端口为 T（带标签）。当设备在一个 VLAN 中传输 MRP 数据包时，请选择 T（1 对话框中 VLAN ID ≥ *Switching > L2-Redundancy > MRP*）。

13.2.5 配置示例

一个骨干网络在线形结构中包含 3 个设备。为了提高网络可用性，您将线形结构转换成冗余环网结构。使用来自不同制造商的设备。所有设备都支持 MRP。在每个设备上，将端口 1.1 和 1.2 定义为环网端口。

当检测到主环链路故障时，环管理器在辅助环链路上发送数据。当一级链路恢复时，二级链路会恢复到备用模式。

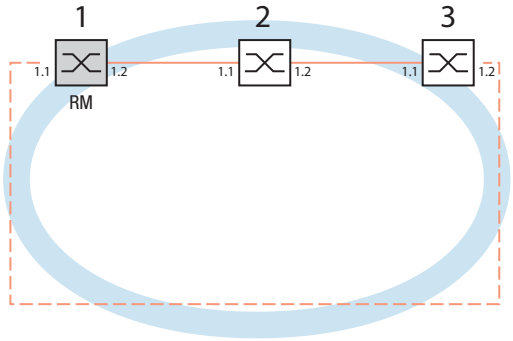


图 33: MRP 环网示例
RM = 环网管理器
—— 主线路
- - - 冗余线路

以下示例配置描述了环网管理器设备 (1) 的配置。按照同样方式对其他两个设备（2 到 3）进行配置，但是不激活 *Ring manager* 功能。此示例不使用 VLAN。将值 *30ms* 指定为环网恢复时间。每个设备都支持环网管理器的高级模式。

- ☐ 根据您的需求设置网络。
- ☐ 配置每个端口，使线路的传输速度和双工设置符合下表要求：

表格 33: 环网端口的端口设置

端口类型	比特率	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	勾选	未勾选	*100 Mbit/s FDX*
TX	1 Gbit/s	勾选	勾选	-
光学	100 Mbit/s	勾选	未勾选	*100 Mbit/s FDX*
光学	1 Gbit/s	勾选	勾选	-
光学	2.5 Gbit/s	勾选	–	*2.5 Gbit/s FDX*

提示: 可以配置不支持自动协商（自动配置）且具有 100 Mbit/s 全双工 (FDX) 或 1000 Mbit/s 全双工 (FDX) 的光学端口。

提示: 可以配置不支持自动协商（自动配置）且具有 100 Mbit/s 全双工 (FDX) 的光学端口。

提示: 分别配置 MRP 环网的每个设备。在连接冗余线路之前，请验证您已完成了 MRP 环网的每个设备的配置。这样有助于避免在配置阶段出现环路。

⚠ 警告

不允许的设备操作

为帮助避免在配置阶段出现环路，请分别配置 *MRP* 配置的每个设备。在连接冗余线路之前，应完成环网配置的其他设备的配置。

如果不遵循这些说明，则会导致死亡、重伤或设备损坏。

可以停用参与端口上的流量控制。

如果流量控制和冗余功能同时激活，则冗余功能的运行可能与预期有所不同。（默认设置：流量控制被全局禁用并在每个端口上被激活。）

禁用网络中每个设备中的 *Spanning Tree* 功能：为此，请执行以下步骤：

- ☐ 打开 *Switching* > *L2-Redundancy* > *Spanning Tree* > *Global* 对话框。
- ☐ 禁用该功能。
  在交付状态下，设备中启用了生成树。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`no spanning-tree operation`	关闭生成树。
`show spanning-tree global`	显示需要检查的参数。

启用网络中每个设备上的 MRP。为此，请执行以下步骤：

- ☐ 打开 *Switching* > *L2-Redundancy* > *MRP* 对话框。
- ☐ 指定所需环网端口。

在命令行界面中，首先定义一个额外参数，即 MRP 域 ID。使用相同的 MRP 域 ID 配置每个环网参与者。该 MRP 域 ID 为 16 个数字块（8 位值）序列。

使用图形用户界面进行配置时，设备会使用默认值 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255 255。

`mrp domain add default-domain`	创建一个 ID 为 default-domain 的新的 MRP 域。
`mrp domain modify port 1/1 primary`	将端口 *1/1* 指定为环网端口 1。
`mrp domain modify port 1/2 secondary`	将端口 *1/2* 指定为环网端口 2。

启用 *Fixed backup* 端口。为此，请执行以下步骤：

- ☐ 启用环网管理器。
  对于环网中的其他设备，将该设置留为 *Off*。
- ☐ 要使设备在环网恢复后继续在二级端口上发送数据，请勾选 *Fixed backup* 复选框。

提示：当设备恢复到一级端口时，可以超过最大环网恢复时间。

当您取消勾选 *Fixed backup* 复选框且环网恢复时，环网管理器将阻塞二级端口并取消阻塞一级端口。

```
mrp domain modify port secondary 1/2
fixed-backup enable
```

激活二级端口上的 *Fixed backup* 功能。环网恢复后，二级端口会继续转发数据。

- ☐ 启用环网管理器。
  对于环网中的其他设备，将该设置留为 *Off*。

```
mrp domain modify mode   manager
```

指定设备作为 *Ring manager* 进行工作。对于环网中的其他设备，将使用默认设置。

- ☐ 选择 *Advanced mode* 字段中的复选框。

```
mrp domain modify   advanced-mode
enabled
```

激活高级模式。

- ☐ 在 *Ring recovery* 字段中，选择值 *30ms*。

```
mrp domain modify   recovery-delay
200ms
```

将值 *30ms* 指定为环网重新配置的最大延迟时间。

提示：如果为环网恢复选择值 *30ms* 不能提供满足您网络需求所需的环网稳定性，则选择值 *500ms*。

- ☐ 开启 MRP 环网的运行。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

```
mrp domain modify operation   enable
```

激活 MRP 环网。

对每个环网参与者都进行配置后，闭合至环网的线路。为此，可以通过设备的环网端口将线路两端的设备连接起来。

检查来自设备的消息。为此，请执行以下步骤：

`show mrp` 显示需要检查的参数。

Operation 字段显示环网端口的工作状态。

可能的值：
- forwarding
  端口已启用，存在连接。
- blocked
  端口已阻塞，存在连接。
- disabled
  端口已禁用。
- not-connected
  不存在连接。

Information 字段显示冗余配置的消息以及检测到错误的可能原因。

当设备作为环网客户端或环网管理器进行工作时，可能会显示以下消息：
- *Redundancy available*
  冗余已设置。当环网的某个组件发生故障时，冗余线路会接替其功能。
- *Configuration error: Error on ringport link.*
  在环网端口的布线中检测到错误。

当设备作为环网管理器进行工作时，可能会显示以下消息：
- *Configuration error: Packets from another ring manager received.*
  环网中存在另一个作为环网管理器工作的设备。
  只在环网中的一个设备上激活 *Ring manager* 功能。
- *Configuration error: Ring link is connected to wrong port.*
  环网中的一条线路连接至不同的端口，而非环网端口。设备仅在一个环端口上接收测试数据包。

如果适用的话，将 MRP 环网集成到一个 VLAN 中。为此，请执行以下步骤：

☐ 在 *VLAN ID* 字段中，定义 MRP VLAN ID。该 MRP VLAN ID 确定设备在配置的哪个 VLAN 中传输 MRP 数据包。
要设置 MRP VLAN ID，首先请在*Switching* > *VLAN* > *Configuration* 对话框中配置 VLAN 和相应的出口规则。
- 如果 MRP 环网未被分配给一个 VLAN（如本例中的情况），则将该 VLAN ID 留为 0。
  在 *Switching* > *VLAN* > *Configuration* 对话框中，为 VLAN U 中的环网端口将 VLAN 成员资格指定为 1（不带标签）。
- 如果 MRP 环网被分配给一个 VLAN，则输入一个 >0 的 VLAN ID。
  在 *Switching* > *VLAN* > *Configuration* 对话框中，为所选 VLAN 中的环网端口将 VLAN 成员资格指定为 T（带标签）。

`mrp domain modify vlan <0..4042>` 分配 VLAN ID。

13.2.6 LAG 上的 MRP

Schneider Electric设备允许用户合并链路聚合组 (LAG)，以通过提供冗余的介质冗余协议 (MRP) 来提高带宽。该功能允许用户提高各个网段或整个网络上的带宽。

Link Aggregation 功能可以帮助用户克服单个端口的带宽限制。LAG 允许用户以并行方式将两个或更多链路组合起来，从而在两个设备之间创建一个逻辑链路。这些并行链路可以提高两个设备之间的数据流的带宽。

一个 MRP 环网由支持符合 IEC 62439 的 MRP 协议的多达 50 台设备组成。仅使用 Schneider Electric 设备时，该协议允许用户配置包含最多 100 台设备的 MRP 环网。

可在以下情况下使用 LAG 上的 MRP：
- 仅提高 MRP 环网的特定网段上的带宽
- 提高整个 MRP 环网上的带宽

网络结构

通过 LAG 配置 MRP 环网时，环网管理器 (RM) 会监控骨干两端的连续性。只要骨干完好无损，RM 就会阻止辅助（冗余）端口上的数据。当 RM 检测到环网上的数据流中断时，它会开始在恢复骨干连续性的辅助端口上转发数据。

可在 MRP 环网中使用 LAG 实例来仅提高带宽，在此情况下，MRP 提供冗余。

为使 RM 检测到环网上的中断，MRP 需要设备在 LAG 实例中的端口关闭的情况下阻止该实例中的每个端口。

MRP 环网的单个网段上的 LAG

设备允许用户在 MRP 环网的特定网段上配置 LAG 实例。

可将 LAG 单交换机方法用于 MRP 环网中的设备。单交换机方式为用户提供了一种扩大网络的廉价方式，在网段的每一端仅使用一台设备来提供物理端口。可将设备端口分组为 LAG 实例，以在需要更高带宽的特定网段上提供更高带宽。

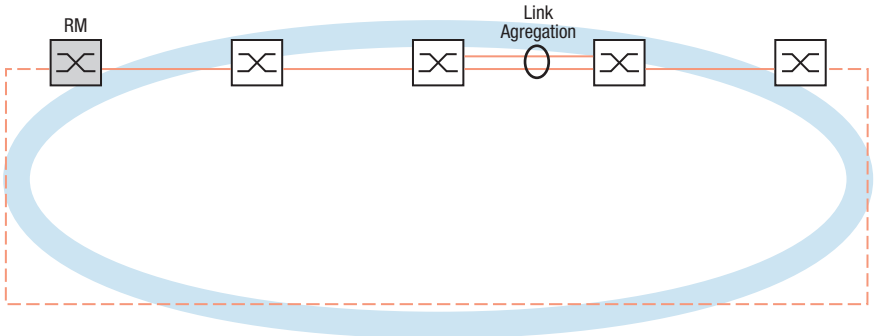


图 34: MRP 环网的单个链路上的链路聚合。

整个 MRP 环网上的 LAG

除了能够在 MRP 环网的特定网段上配置 LAG 实例，Schneider Electric 还允许用户在每个网段上配置 LAG 实例，这样可提高整个 MRP 环网上的带宽。

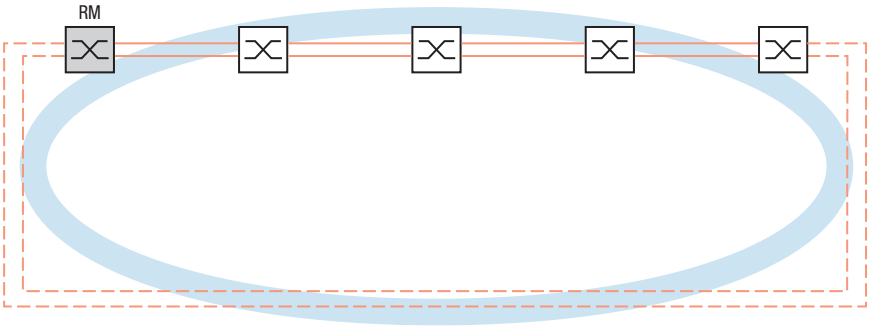


图 35: 整个 MRP 环网上的链路聚合。

检测环网上的中断

配置 LAG 实例时，将 *Active ports (min.)* 值配置为等于 LAG 实例中使用的端口总数。当设备在 LAG 实例中的端口上检测到中断时，它会阻止该实例上的其他端口上的数据。阻止实例的每个端口后，RM 会感知环网已打开，并开始在辅助端口上转发数据。这样一来，RM 就能够为已中断的网段的另一端上的设备恢复连续性。

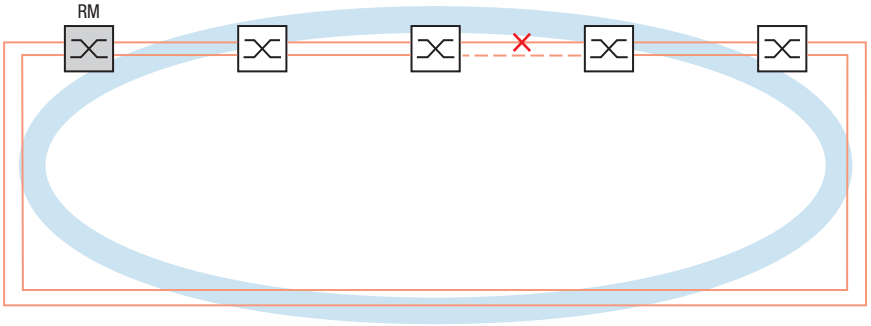


图 36: MRP 环网中的链路中断。

配置示例

在以下示例中，交换机 A 和 交换机 B 将两个部门链接在一起。这些部门产生的流量太高，单个端口带宽无法处理。可为 MRP 环网的单个网段配置 LAG 实例，从而提高该网段的带宽。

示例配置的前提条件是从正常运行的 MRP 环网开始。

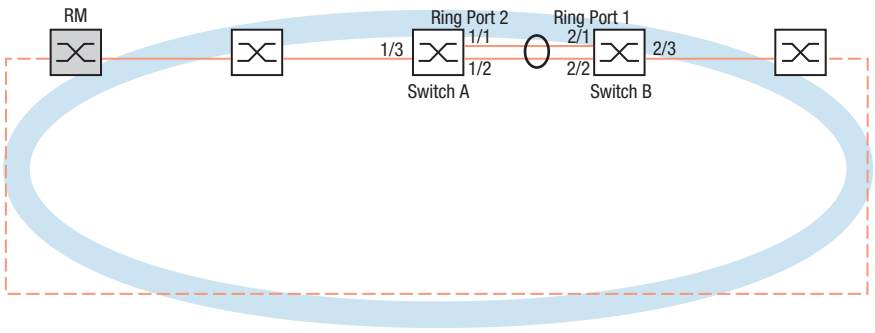


图 37: LAG 上的 MRP 配置示例

首先配置交换机 A。为此，请执行以下步骤。然后使用相同的步骤配置 交换机B，替换相应的端口和环网端口编号。

- ☐ 打开 *Switching > L2-Redundancy > Link Aggregation* 对话框。
- ☐ 点击  按钮。
  该对话框显示 *Create* 窗口。
- ☐ 在 *Trunk port* 下拉列表中，选择链路聚合组的实例编号。
- ☐ 在 *Port* 下拉列表中，选择端口 *1/1*。
- ☐ 点击 *Ok* 按钮。
- ☐ 重复以上步骤并选择端口 *1/2*。
- ☐ 点击 *Ok* 按钮。
- ☐ 在 *Active ports (min.)* 列中输入 2，在此情况下是实例中的端口总数。将 MRP 和 LAG 组合时，可将端口总数指定为 *Active ports (min.)*。当设备在端口上检测到中断时，它会阻止导致环网打开的实例中的其他端口。环网管理器感知环网已打开，然后开始在恢复与网络中其他设备的连接的辅助环网端口上转发数据。
- ☐ 暂时保存更改。为此，请单击  按钮。
- ☐ 打开 *Switching > L2-Redundancy > MRP* 对话框。
- ☐ 在 *Ring port 2* 框中，在 *Port* 下拉列表中选择端口 lag/1。
- ☐ 暂时保存更改。为此，请单击  按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`link-aggregation add lag/1`	创建一个链路聚合组 lag/1。
`link-aggregation modify lag/1 addport 1/1`	将端口 *1/1* 添加到链路聚合组。
`link-aggregation modify lag/1 addport 1/2`	将端口 *1/2* 添加到链路聚合组。
`mrp domain modify port secondary lag/1`	将端口 lag/1 指定为环网端口 2。
`copy config running-config nvm`	将当前设置保存到永久存储器 (nvm) 的“选定”配置概要文件中。

13.3 HIPER 环网客户端

⚠ 警告

不允许的设备操作

为帮助避免在配置阶段出现环路，请分别配置 *HIPER Ring* 配置的每个设备。在连接冗余线路之前，应完成环网配置的其他设备的配置。

如果不遵循这些说明，则会导致死亡、重伤或设备损坏。

HIPER 环网冗余概念允许构建高可用性的环形网络结构。*HIPER Ring* 客户端功能允许网络管理员对现有 HIPER 环网进行扩展或替换已经参与 HIPER 环网的客户端设备。

当设备感测到某个环网端口上的链路中断时，设备会向环网管理器 (RM) 发送一个 LinkDown 数据包并清除 FDB 表。一旦 RM 接收到 LinkDown 数据包，将立即同时通过一级和二级环网端口转发数据流。因此，RM 能够保持 HIPER 环网的完整性。

设备只支持将快速以太网和千兆以太网端口作为环网端口。此外，还可以将环网端口包括到 LAG 实例中。

在默认状态下，HIPER 环网客户端为停用，一级和二级端口被设为 no Port。

提示: 在 *Switching > L2-Redundancy > Spanning Tree > Port* 对话框中为环网端口停用生成树协议 (STP)，因为 STP 和 HIPER 环网具有不同的反应时间。

表格 34: 环网端口的端口设置

端口类型	比特率	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	勾选	未勾选	*100 Mbit/s FDX*
TX	1 Gbit/s	勾选	勾选	-
光学	100 Mbit/s	勾选	未勾选	*100 Mbit/s FDX*
光学	1 Gbit/s	勾选	勾选	-
光学	2.5 Gbit/s	勾选	–	*2.5 Gbit/s FDX*

13.3.1 HIPER 环网上的 VLAN

设备允许用户通过 HIPER 环网转发 VLAN 数据。因此，设备为您的 VLAN 数据提供冗余。环网设备在环网中转发管理数据，例如在 VLAN 1 上。为了使数据能够到达管理站，环网设备会在环网端口上转发不带标签的管理数据。此外，请将环网端口指定为 VLAN 1. 中的成员。

如果您还有其他穿过您的环网设备的 VLAN，则环网设备还会以带标签的形式转发其他 VLAN 数据。

指定 VLAN 设置。为此，请执行以下步骤：

- ☐ 打开 *Switching > VLAN > Configuration* 对话框。
- ☐ 在环网端口上转发不带标签的 VLAN 管理数据。
  在 VLAN 1 行中，在与环网端口相关的列中的下拉列表中选择 U 项目。
- ☐ 阻止将管理数据包转发到非环网端口。
  在 VLAN 1 行中，在与环网端口不相关的列中的下拉列表中选择 - 项目。
- ☐ 允许环网设备在与具有 VLAN 成员资格的端口之间转发 VLAN 数据。
  在 VLAN 行中，在与环网端口相关的列中的下拉列表中选择 T 项目。
- ☐ 打开 *Switching > VLAN > Port* 对话框。
- ☐ 将 VLAN 1 成员资格分配给环网端口。
  在环网端口行的 *Port-VLAN ID* 列中输入值 1。
- ☐ 将 VLAN 成员资格分配给非环网端口。
  在非环网端口行的 *Port-VLAN ID* 列中输入相应的 VLAN ID。

13.3.2 LAG 上的 HIPER 环网

HIPER Ring 功能允许用户通过链路聚合组 (LAG) 将设备链接在一起。环网客户端和环网管理器的行为方式与没有 LAG 实例的环网相同。

如果 LAG 链路关闭，则实例中的其他链接也会关闭，从而在环路中造成中断。在环网中检测到中断之后，受影响的端口会将“链路中断”数据包发送到环网管理器。环网管理器取消阻止辅助端口，在环网的两个方向上发送数据，并回复“删除”数据包。在收到“删除”数据包时，环网参与清除其 FDB。

13.4 生成树

提示：生成树协议是一种用于 MAC 网桥的协议。因此，以下描述使用网桥一词代表设备。

本地网络的规模越来越大。这同时适用于地域的扩大和网络参与者的数量。因此，使用多个网桥十分有益，例如：
- 降低子区域中的网络负载，
- 建立冗余连接以及
- 克服距离限制。

但是，使用多个在子网络之间具有多个冗余连接的网桥会导致环路，进而导致网络之间通信中断。为了帮助避免这种情况，可以使用生成树。生成树可通过冗余连接的系统化停用来实现无环路切换。冗余可以根据需要对各个连接进行系统化重新激活。

RSTP 是生成树协议 (STP) 的进一步发展，并与之兼容。当一个连接或一个网桥无法工作时，STP 最多需要 30 秒进行重新配置。这在对时间敏感的应用程序中不再被接受。RSTP 的平均重新配置时间能够小于一秒。在一个由 10 至 20 台设备组成的环网拓扑中使用 RSTP 时，重新配置时间甚至能够达到毫秒数量级。

提示：RSTP 可以将一个具有冗余路径的第二层网络拓扑简化成不再包含任何冗余路径的树形结构（生成树）。在这里，其中一个设备接替根网桥角色。一个活动分支中允许的最大设备数量（从根网桥到分支端部）由当前根网桥的变量 *Max age* 指定。*Max age* 的预设值为 20，该值最大可以增加到 40。

如果作为根工作的设备无法工作且另一个设备接替其功能，则新的根网桥的 *Max age* 设置将决定一个分支中允许的设备最大数量。

提示：RSTP 标准要求一个网络中的所有设备都要使用（快速）生成树算法进行工作。当同时使用 STP 和 RSTP 时，在混合运行的网段中，使用 RSTP 进行更快重新配置的优势将会丧失。

只支持 RSTP 的设备可以与 MSTP 设备一起工作，前提是，将 CST（公共生成树）而非 MST 区域分配给它自己。

13.4.1 基本原理

由于 RSTP 是 STP 的进一步发展，关于 STP 的以下所有描述也都适用于 RSTP。

STP 的任务

生成树算法可以简化使用网桥建立并且由于至树形结构的冗余链路而包含环形结构的网络拓扑。在此过程中，STP 停用冗余路径，进而根据预设规则打开环形结构。当网络组件无法工作导致一个路径中断时，STP 将再次重新激活之前停用的路径。这使冗余链路能够提高通信的可用性。

STP 确定了代表 STP 树形结构根基的网桥。这个网桥被称为根网桥。

STP 算法的特点：
- 当网桥无法工作或数据路径中断时对树形结构进行自动重新配置
- 在最大网络规模以下树形结构保持稳定，
- 拓扑在较短时间内可保持稳定
- 拓扑可以由管理员指定和重新产生

- 终端设备透明
- 借助创建的树形结构可降低相对于可用传输容量的网络负载

网桥参数

在生成树的背景下，通过以下参数对每个网桥及其连接进行唯一描述：
- 网桥标识符
- 网桥端口的根路径开销，
- 端口标识符

网桥标识符

网桥标识符由 8 个字节组成。数值最高的两个字节为优先级。配置网络时，管理员可以更改优先级编号的默认设置，即 32768 (8000H)。网桥标识符数值最低的六个字节为该网桥的 MAC 地址。MAC 地址允许每个网桥具有唯一的网桥标识符。

网桥标识符数字最小的网桥具有最高的优先级。

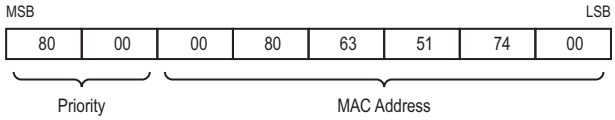


图 38: 网桥标识符，示例（数值采用十六进制表示法）

根路径开销

向连接两个网桥的每个路径分配一个传输开销（路径开销）。设备根据传输速度确定此值（参阅表格 35）。传输速度越低的路径，设备分配的路径开销就越高。

此外，管理员还可以设置路径开销。与设备一样，管理员向传输速度较低的路径分配较高的路径开销。由于管理员最终可以自由选择该值，所以他可以使用一个工具为冗余路径中的某条特定路径设置优先权。

根路径开销是数据包从一个相连网桥的端口到根网桥需要穿越的所有路径的单独开销之和。

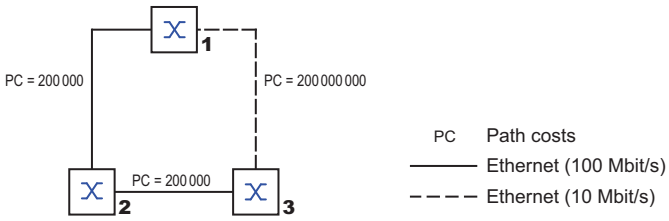


图 39: 路径开销

表格 35: 根据数据速率为 RSTP 推荐的路径开销。

数据速率	建议值	建议范围	可能的范围
≤100 kbit/s	200 000000[1]。	20000000-200000000	1-200000000
1 Mbit/s	20000000[a]	2000000-200000000	1-200000000
10 Mbit/s	2000000[a]	200000-20000000	1-200000000

表格 35: 根据数据速率为 RSTP 推荐的路径开销。

数据速率	建议值	建议范围	可能的范围
100 Mbit/s	200000[a]	20000-2000000	1-200000000
1 Gbit/s	20000	2000-200000	1-200000000
10 Gbit/s	2000	200-20000	1-200000000
100 Gbit/s	200	20-2000	1-200000000
1 TBit/s	20	2-200	1-200000000
10 TBit/s	2	1-20	1-200000000

1. 验证符合 IEEE 802.1D-1998 且仅支持过去成本的 16 位值的网桥，在与支持 32 位值的网桥一起使用的情况下，将值 65535 (FFFFH) 用于路径成本路径成本.

端口标识符

端口标识符由 2 个字节组成。字节数值较低的一部分包含物理端口编号。这为此网桥的端口提供了唯一标识符。数值较高的第二部分为端口优先级，由管理员指定（默认值：128此处适用的规律还包括，端口标识符数字最小的端口具有最高优先级。

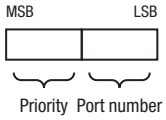


图 40: 端口标识符

最大老化时间和直径

“最大老化时间”和“直径”值在很大程度上决定了一个生成树网络的最大扩展范围。

直径

网络中彼此相距最远的设备之间的连接数量称为网络直径。

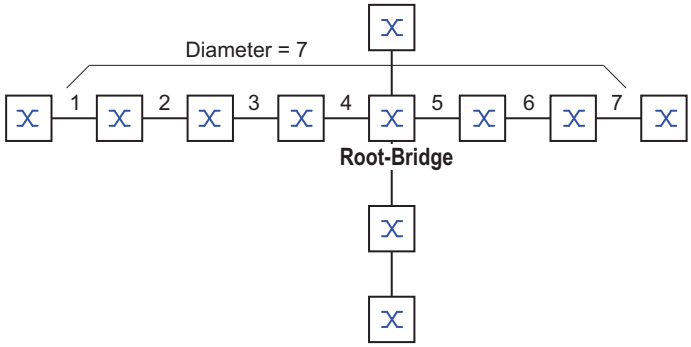


图 41: 直径的定义

在网络中可以实现的网络直径为 MaxAge - 1.

在交付状态下，MaxAge = 20，可以实现的最大直径 = 19。将 MaxAge 的最大值设为 40 时，可以实现的最大直径 = 39。

MaxAge

每个 STP-BPDU 都包含一个“MessageAge”计数器。穿越一个网桥后，该计数器递增 1。

在转发一个 STP-BPDU 之前，网桥会将“MessageAge”计数器与设备中指定的“MaxAge”值进行比较：

- 当 MessageAge < MaxAge 时，网桥会将该 STP-BPDU 转发到下一个网桥。
- 当 MessageAge = MaxAge 时，网桥会丢弃该 STP-BPDU。

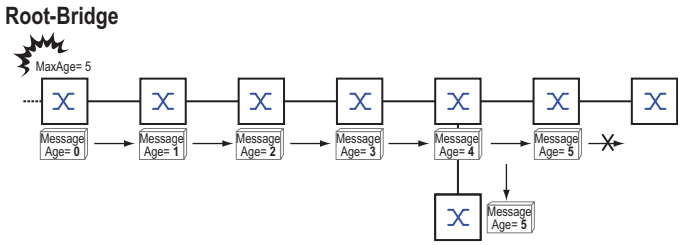


图 42: STP-BPDU 的传输视 MaxAge 而定

13.4.2 树形结构创建规则

网桥信息

要确定树形结构，网桥需要获得有关位于网络中的其他网桥的更多详细信息。

为获得这些信息，每个网桥都会向其他网桥发送一个 BPDU（网桥协议数据单元）。

一个 BPDU 的内容包括：

- 网桥标识符
- 根路径开销
- 端口标识符

（参见 IEEE 802.1D）

建立树形结构

网桥标识符数字最小的网桥称为根网桥。它是（或将成为）树形结构的根。

树的结构视根路径开销而定。在选择结构时，生成树会确保每个单独网桥与根网桥之间的路径开销尽可能较小。

- 当多个路径具有相同的根路径开销时，与根相距较远的网桥将决定它要阻塞哪个端口。为此，它会使用与根相距较近的网桥的网桥标识符。该网桥会阻塞指向 ID 数字较大的网桥的端口（数字较大的 ID 是逻辑上较差的 ID）。当两个网桥具有相同的优先级时，具有数字较大的 MAC 地址的网桥会具有数字较大的 ID，即逻辑上较差的 ID。
- 当具有相同根路径开销的多个路径从一个网桥连接到同一个网桥时，与根相距较远的网桥会使用另一个网桥的端口标识符作为最后一个标准(参阅图 40)。在此过程中，该网桥会阻塞指向 ID 数字较大的端口的端口（数字较大的 ID 是逻辑上较差的 ID）。当两个端口具有相同的优先级时，端口编号较高的端口具有数字较大的 ID，即逻辑上较差的 ID。

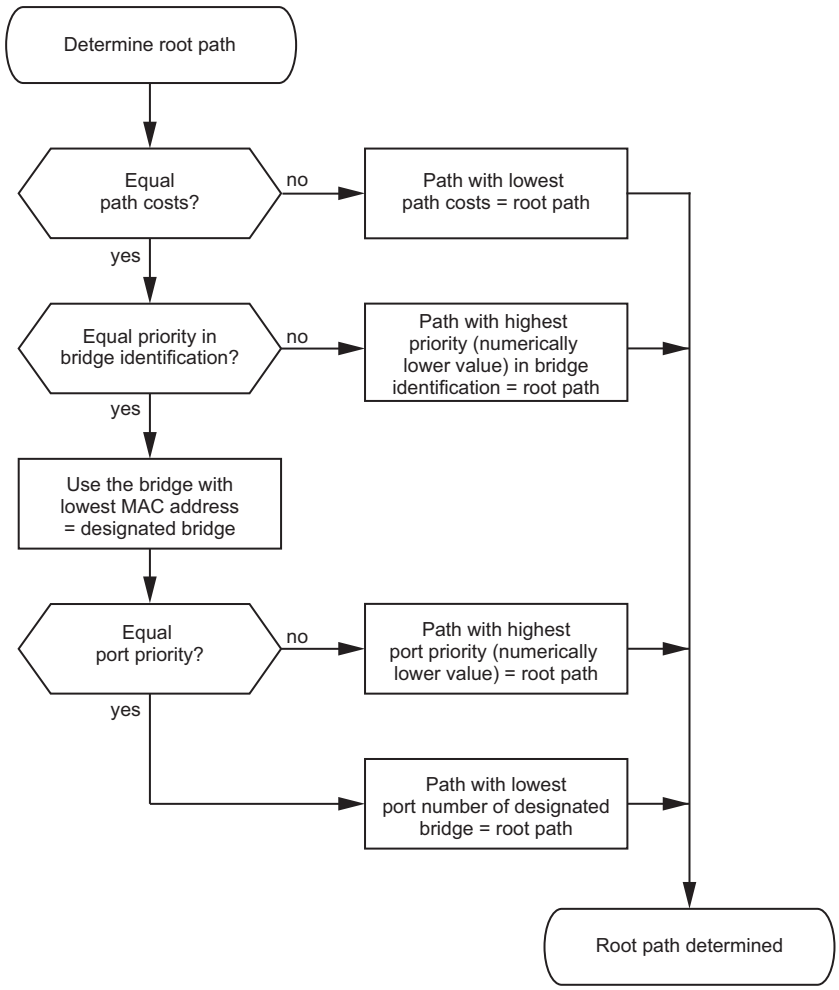


图 43: 根路径指定流程图

13.4.3 示例

确定根路径的示例

可以使用网络规划(参阅图 44)遵循流程图(参阅图 43)确定根路径。管理员在网桥标识中为每个网桥指定了一个优先级。网桥标识中数值最小的网桥扮演根网桥的角色，在本例中，即网桥 1。在此示例中，每个子路径都有相同的路径开销。协议阻塞网桥 2 和网桥 3 之间的路径，这是因为，从网桥 3 经过网桥 2 指向根网桥的连接会产生更高的路径开销。

从网桥 6 到根网桥的路径值得注意：

- 经过网桥 5 和网桥 3 的路径会产生与经过网桥 4 和网桥 2 的路径相同的根路径开销。
- STP 使用网桥标识中 MAC 地址最低的网桥进行路径选择（图中网桥 4）。
- 网桥 6 和网桥 4 之间也有两个路径。
  在此，端口标识符是决定性的（端口 1 < 端口 3）。

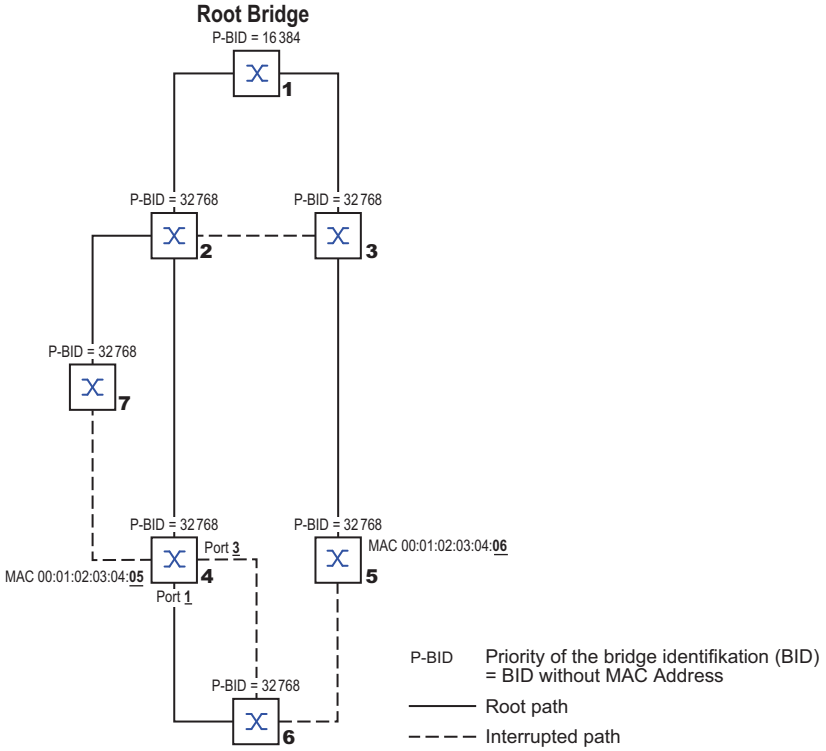


图 44: 确定根路径的示例

提示：当前根网桥出现故障时，网桥标识符中的 MAC 地址本身就能确定哪个网桥将成为新的根网桥，这是因为，除根网桥的值以外，管理员并未更改网桥标识符中网桥优先级的默认值。

处理根路径的示例

可以使用网络规划(参阅图 45)遵循流程图(参阅图 43)确定根路径。管理员执行了以下操作：

- 为除网桥 1 和网桥 5 以外的所有网桥保留了 32768 (8000H) 默认值，并将
- 值 16384 (4000H) 分配给网桥 1，因此使之成为根网桥。
- 管理员将值 28672 (7000H) 分配给网桥 5。

协议阻塞网桥 2 和网桥 3 之间的路径，这是因为，从网桥 3 经过网桥 2 指向根网桥的连接意味着更高的路径开销。

从网桥 6 到根网桥的路径值得注意：

- 这些网桥选择经过网桥 5 的路径，这是因为，网桥标识符中的优先级数值 28672 小于数值 32768。

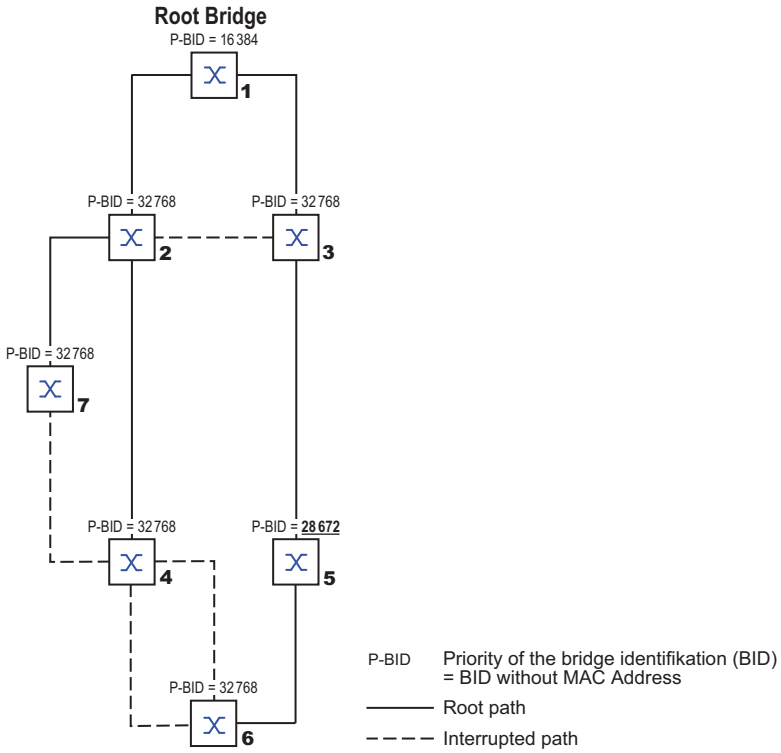


图 45: 处理根路径的示例

处理树形结构的示例

管理员很快就发现，使用网桥 1 作为根网桥的这种配置是无效的。在从网桥 1 到网桥 2 以及从网桥 1 到网桥 3 的路径上，根网桥向所有其他网桥发送的控制数据包会累加起来。

当管理员将网桥 2 配置为根网桥时，控制数据包在子网络上产生的负担分布会更加均匀。结果就是此处显示的配置(参阅图 46)。从多数网桥到根网桥的路径开销均有所减少。

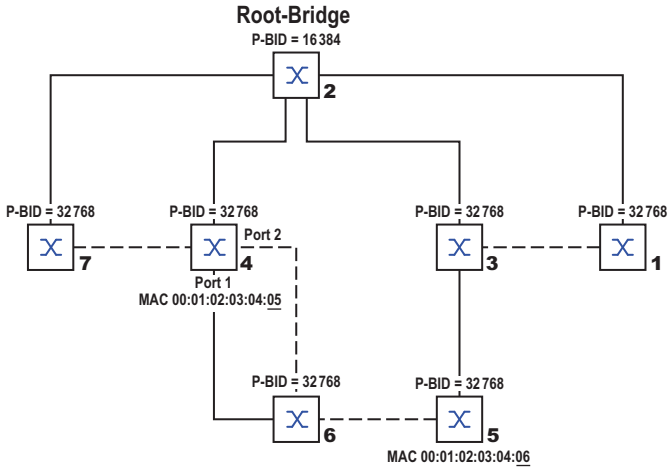


图 46: 处理树形结构的示例

13.5 快速生成树协议

RSTP 使用与 STP 相同的算法来确定树形结构。当一个链路或网桥无法工作时，RSTP 只是更改一些参数，并添加一些旨在加快重新配置的新参数和机制。

在这种情况下，端口发挥着重要作用。

13.5.1 端口角色

RSTP 向每个网桥端口分配以下任一角色(参阅图 47)：

- 根端口：
  这是一个网桥以最低路径开销从根网桥接收数据包的端口。
  当存在路径开销同样较低的多个端口时，指向根（指定网桥）的网桥的网桥 ID 将决定与根相距较远的网桥将根端口角色分配给它的哪个端口。
  当一个网桥具有指向同一网桥的路径开销同样较低的多个端口时，该网桥会使用指向根（指定网桥）的网桥的端口 ID 来决定它在本地选择哪个端口作为根端口(参阅图 43)。
  根网桥本身没有根端口。
- 指定端口：
  根路径开销最低的网段中的网桥就是指定网桥。
  当一个以上的网桥具有相同的根路径开销时，网桥标识符数值最小的网桥即成为指定网桥。此网桥上的指定端口就是连接一个离开根网桥的网段的端口。当一个网桥（通过集线器等）连接到一个具有一个以上端口的网段时，该网桥会将指定端口角色分配给端口 ID 更优的端口。
- 边缘端口
  没有额外 RSTP 网桥的每个网段都只与一个指定端口连接。在这种情况下，此指定端口也是一个边缘端口。边缘端口的特点在于，它不接收任何 RST BPDU（快速生成树网桥协议数据单元）。
- 备选端口
  当至根网桥的连接中断时，此被阻塞端口会接替根端口的任务。备选端口为至根网桥的连接提供一个备份。

- 备份端口
  这是一个当至此网段指定端口的连接（没有任何 RSTP 网桥）中断时作为备份的被阻塞端口
- 被禁用的端口
  这是一个不参与生成树操作的端口，即，该端口关闭或没有任何连接。

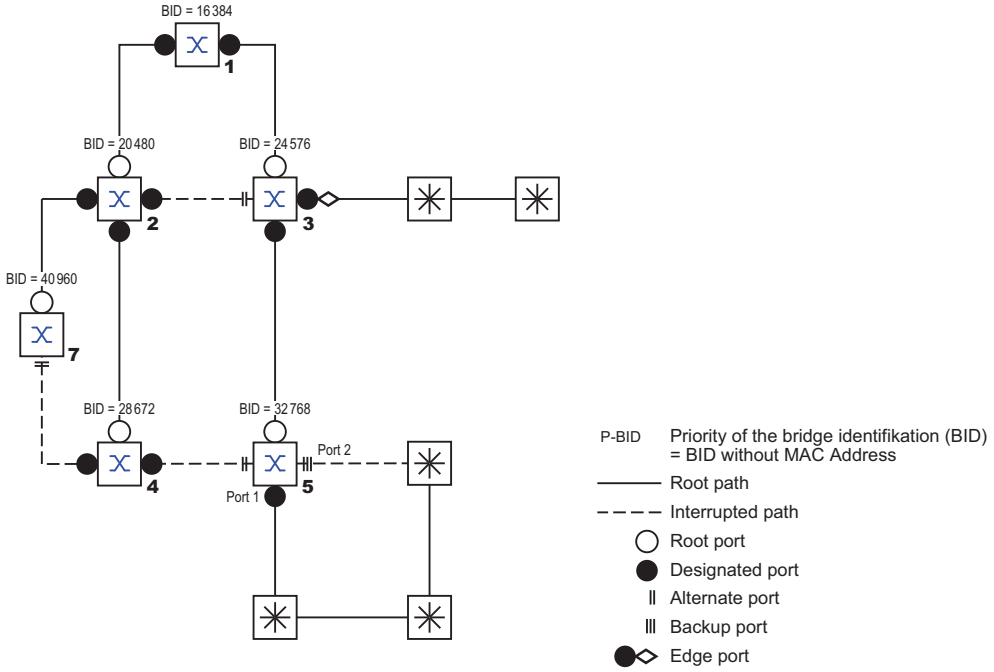


图 47: 端口角色分配

13.5.2 端口状态

视树形结构以及所选连接路径的状态而定，RSTP 向端口分配状态。

表格 36: STP 和 RSTP 的端口状态值之间的关系

STP 端口状态	管理网桥端口状态	MAC 处于工作状态	RSTP 端口状态	活动拓扑（端口角色）
DISABLED	禁用	FALSE	Discarding[1]	除外（禁用）
DISABLED	启用	FALSE	Discarding[a]	除外（禁用）
BLOCKING	启用	TRUE	Discarding[2]	除外（备选，备份）
LISTENING	启用	TRUE	Discarding[b]	包括（根，指定）
LEARNING	启用	TRUE	Learning	包括（根，指定）
FORWARDING	启用	TRUE	Forwarding	包括（根，指定）

1. dot1d-MIB 显示“禁用”
2. dot1d-MIB 显示“阻塞”

RSTP 端口状态的含义：
- 禁用：端口不属于活动拓扑
- 丢弃：FDB 中无地址示教，除 STP-BPDU 以外无数据流量
- 示教：地址示教已激活 (FDB)，除 STP-BPDU 以外无数据流量
- 转发：地址示教已激活 (FDB)，发送和接收每种数据包类型（不仅包括 STP-BPDU）

13.5.3 生成树优先向量

为了给端口分配角色，RSTP 网桥相互交换配置信息。这些信息被称为生成树优先向量。它们是 RSTP BPDU 的组成部分，并包含下列信息：

- 根网桥的网桥标识
- 发送网桥的根路径开销
- 发送网桥的网桥标识
- 通过其发送消息的端口的端口标识符
- 通过其接收消息的端口的端口标识符

根据此信息，参与 RSTP 的网桥能够自行确定端口角色并定义自己端口的端口状态。

13.5.4 快速重新配置

为什么 RSTP 对根路径中断的反应比 STP 更快？

- 边缘端口的引入：
  在重新配置期间，RSTP 会在 3 秒钟之后将一个边缘端口设置为传输模式（默认设置）。为了确定没有连接任何发送 BPDU 的网桥，RSTP 会等待“Hello Time”消逝。
  当用户验证一个终端设备已经并保持连接到此端口时，在进行重新配置的情况下，此端口处没有等候时间。
- 备选端口的引入：
  鉴于在正常操作时已经分配了端口角色，至根网桥的连接中断后，一个网桥可以立即从根端口切换到备选端口。
- 与相邻网桥的通信（点到点连接）：
  相邻网桥之间的分散式直接通信允许用户不经等待时间就对生成树拓扑中的状态变化作出反应。
- 地址表：
  借助 STP，FDB 中条目的年龄决定了通信是否更新。RSTP 立即删除受到重新配置影响的端口中的条目。
- 对事件的反应：
  RSTP 对连接中断、连接恢复等事件立即作出反应，而无需遵循任何时间规范。

提示： 在 RSTP 拓扑重新配置期间，数据包可能重复并/或以错误的顺序到达接收者。您还可以使用生成树协议或选择本手册中介绍的其他快速冗余过程。

13.5.5 配置设备

⚠ 警告

不允许的设备操作

为帮助避免在配置阶段出现环路，请分别配置 *Spanning Tree* 配置的每个设备。在连接冗余线路之前，应完成 *Spanning Tree* 配置的其他设备的配置。

如果不遵循这些说明，则会导致死亡、重伤或设备损坏。

RSTP 完全自主地对网络拓扑进行配置。网桥优先级最低的设备将自动成为根网桥。但是，为了定义特定的网络结构，用户仍需将一个设备指定为根网桥。一般而言，骨干中的一个设备将承担此角色。

请执行以下步骤：

- ☐ 根据您的需求设置网络，最初不建立冗余线路。
- ☐ 可以停用参与端口上的流量控制。
  如果流量控制和冗余功能同时激活，则冗余功能的运行可能与预期有所不同。（默认设置：流量控制被全局禁用并在每个端口上被激活。）
- ☐ 禁用每个设备上的 MRP。
- ☐ 启用网络中每个设备上的生成树。
  在交付状态下，设备中开启了生成树。

请执行以下步骤：

- ☐ 打开 *Switching* > *L2-Redundancy* > *Spanning Tree* > *Global* 对话框。
- ☐ 启用该功能。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`spanning-tree operation`	启用生成树。
`show spanning-tree global`	显示需要检查的参数。

现在连接冗余线路。

为接替根网桥角色的设备定义设置。

请执行以下步骤：

- ☐ 在 *Priority* 字段中，可以输入一个数值较小的值。
  网桥 ID 数值最小的网桥具有最高的优先级并成为网络的根网桥。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`spanning-tree mst priority 0 <0..61440>`	指定设备的网桥优先级。 **提示：**在 `0..61440` 范围中指定网桥优先级，步长为 4096。

保存后，该对话框会显示以下信息：

- *Bridge is root* 复选框已勾选。
- *Root port* 字段显示值 0.0。
- *Root path cost* 字段显示值 0。

`show spanning-tree global`	显示需要检查的参数。

- ☐ 如果适用，则请更改 *Forward delay [s]* 和 *Max age* 字段中的值。
  - 根网桥将更改后的值传输到其他设备。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`spanning-tree forward-time <4..30>`	为状态变化指定延迟时间（秒）。
`spanning-tree max-age <6..40>`	指定最大允许分支长度，如连接到根网桥的设备的数量。
`show spanning-tree global`	显示需要检查的参数。

提示： 参数 *Forward delay [s]* 与参数 *Max age* 有以下关系：

Forward delay [s] ≥ (*Max age*/2) + 1

如果在这些字段中输入违反这种关系的值，则设备会将这些值替换为最后一个有效值或默认值。

提示： 如果可能，请不要更改“Hello Time”字段中的值。

检查其他设备中的以下值：
- 相应设备和根网桥的网桥 ID（网桥优先级和 MAC 地址）。
- 指向根网桥的设备端口的编号。
- 从设备的根端口到根网桥的路径开销。

请执行以下步骤：

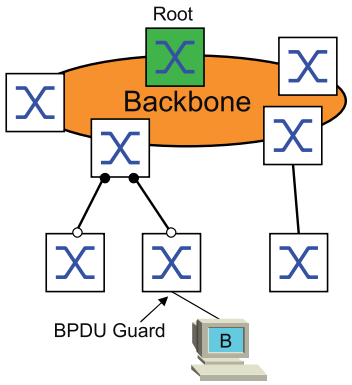
`show spanning-tree global`	显示需要检查的参数。

13.5.6 保护

设备允许用户激活设备端口中的各种保护功能（保护）。

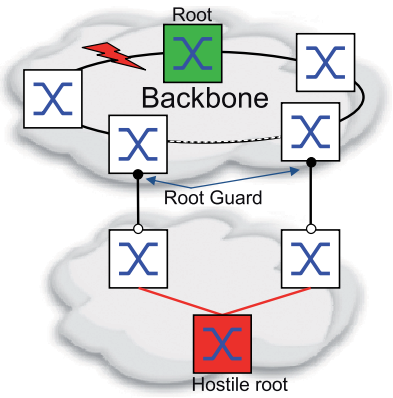
以下保护功能可以帮助保护用户网络免遭错误配置、环路形成和使用 STP-BPDU 的攻击：

▶ BPDU 保护 - 用于手动指定的边缘端口（终端设备端口）
可以在设备中全局激活此保护功能。



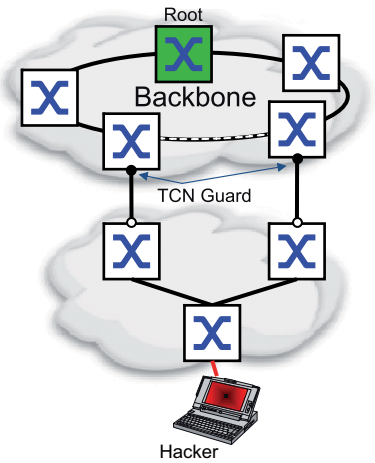
终端设备端口一般不接收任何 STP-BPDU。如果攻击者仍然试图在此端口上输入 STP-BPDU，则设备将停用该设备端口。

- 根保护 - 用于指定端口
  可以为每个设备端口单独激活此保护功能。



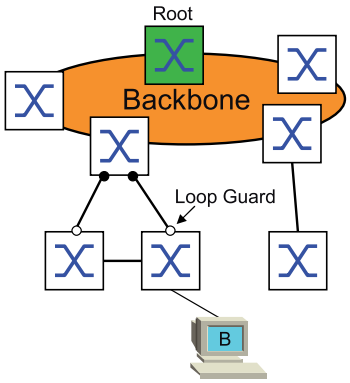
当指定端口接收到一个至根网桥的具有更优路径信息的 STP-BPDU 时，设备将丢弃该 STP-BPDU 并将端口传输状态设置为 discarding 而非 root。
当不存在至根网桥的具有更优路径信息的 STP-BPDU 时，经过 2 x *Hello time [s]* 之后，设备会将端口状态重置为符合端口角色的值。

- TCN 保护 - 用于接收带有拓扑更改标志的 STP-BPDU 的端口
  可以为每个设备端口单独激活此保护功能。



如果保护功能已激活，则设备会忽略接收到的 STP-BPDU 中的拓扑更改标志。这不会更改设备端口的地址表 (FDB) 的内容。但是，设备将对 BPDU 中更改拓扑结构的附加信息进行处理。

- 环路保护 - 用于根、备选和备份端口
  可以为每个设备端口单独激活此保护功能。



如果该端口不再接收到任何 STP-BPDU，则此保护功能有助于防止一个端口的传输状态被无意间更改为 forwarding。如果出现这种情况，则设备会将该端口的环路状态指定为不一致，但不会转发任何数据包。

激活 BPDU 保护

请执行以下步骤：

- ☐ 打开 *Switching > L2-Redundancy > Spanning Tree > Global* 对话框。
- ☐ 勾选 *BPDU guard* 复选框。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`spanning-tree bpdu-guard`	激活 BPDU 保护。
`show spanning-tree global`	显示需要检查的参数。

- ☐ 打开 *Switching > L2-Redundancy > Spanning Tree > Port* 对话框。
- ☐ 切换到 *CIST* 选项卡。
- ☐ 对于终端设备端口，勾选 *Admin edge port* 列中的复选框。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`interface <x/y>`	切换到接口 <x/y> 的接口配置模式。
`spanning-tree edge-port`	将该端口指定为终端设备端口（边缘端口）。
`show spanning-tree port x/y`	显示需要检查的参数。
`exit`	离开接口模式。

当一个边缘端口收到一个 STP-BPDU 时，设备行为如下：

- ▶ 设备停用此端口。
  在 *Basic Settings > Port* 对话框的 *Configuration* 选项卡中，*Port on* 列中针对此端口的复选框为未勾选。
- ▶ 设备指定该端口。

可以确定端口是否因为接收到 BPDU 而自行禁用。为此，请执行以下步骤：

在 *Switching > L2-Redundancy > Spanning Tree > Port* 对话框的 *Guards* 选项卡中，*BPDU guard effect* 列中的复选框为勾选。

`show spanning-tree port x/y`	显示需要检查的端口的参数。*BPDU guard effect* 参数的值为 enabled。

将设备端口的状态重置为值 forwarding。为此，请执行以下步骤：

- ☐ 当端口仍然接收 BPDU 时：
  - 删除作为边缘端口（终端设备端口）的手动定义。
    或者
  - 停用 BPDU 保护。
- ☐ 再次激活设备端口。

激活根保护/TCN 保护/环路保护

请执行以下步骤：

- ☐ 打开 *Switching > L2-Redundancy > Spanning Tree > Port* 对话框。
- ☐ 切换到 *Guards* 选项卡。
- ☐ 对于指定端口，选择 *Root guard* 列中的复选框。
- ☐ 对于接收带有拓扑更改标志的 STP-BPDU 的端口，选择 *TCN guard* 列中的复选框。
- ☐ 对于根、备选或备份端口，勾选 *Loop guard* 列中的复选框。

提示： *Root guard* 和 *Loop guard* 功能互相排斥。如果在 *Loop guard* 功能激活的情况下尝试激活 *Root guard* 功能，则设备将停用 *Loop guard* 功能。

- ☐ 暂时保存更改。为此，请单击  按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`interface <x/y>`	切换到接口 〈x/y〉 的接口配置模式。
`spanning-tree guard-root`	开启指定端口上的根保护。
`spanning-tree guard-tcn`	开启接收带有拓扑更改标志的 STP-BPDU 的端口上的 TCN 保护。
`spanning-tree guard-loop`	开启根、备选或备份端口上的环路保护。
`exit`	离开接口模式。
`show spanning-tree port x/y`	显示需要检查的端口的参数。

13.6 Dual RSTP (MCSESM-E)

工业应用要求用户网络具有较高的可用性。这也涉及到当任一网络组件无法工作时为通信保持确定的、较短的中断时间。

环网拓扑有助于以最少的资源使用提供较短的中断时间。使用 *Spanning Tree* 协议时，中断时间视网络规模而定。要优化中断时间，可以将大型 *Spanning Tree* 网络分割成较小的环形网段。

Dual RSTP 功能与 *RCP* 功能一起使用。使用 *RCP* 功能，可以选择将一个或多个 RSTP 环网与一级环网中的 RSTP 实例耦合起来。对两个 *Spanning Tree* 网段进行耦合时，二级环网代表 *Dual RSTP* 功能设置适用的一个不同的 RSTP 实例。此 *Dual RSTP* 实例在工作时独立于一级环网的 RSTP 实例以及其他二级环网。当 RSTP 是仅在要耦合的一个环网中使用的协议时，不需要 *Dual RSTP* 功能。

13.7 链路聚合

采用单交换机方式的 *Link Aggregation* 功能可以帮助用户克服以太网链路的两大限制，即带宽和冗余。

Link Aggregation 功能可以帮助用户克服单个端口的带宽限制。*Link Aggregation* 功能允许用户以并行方式将两个或更多链路组合起来，从而在两个设备之间创建一个逻辑链路。这些并行链路可以提高两个设备之间流量的带宽。

一般在网络骨干上使用 *Link Aggregation* 功能。该功能为用户提供了一种逐步增加带宽的廉价方式。

此外，*Link Aggregation* 功能还可提供具有无缝故障转移功能的冗余。当一个链路中断时，借助并行配置的两个或更多链路，组中的其他链路将继续转发流量。

新的 *Link Aggregation* 实例的默认设置如下：
- 在 *Active* 列中，复选框为勾选。
- 在 *Send trap (Link up/down)* 列中，复选框为勾选。
- 在 *Static link aggregation* 列中，复选框为未勾选。
- 在 *Active ports (min.)* 列中，数值为 1。

13.7.1 操作方法

设备以单交换机方式进行工作。单交换机方式为用户提供了一种扩大网络的廉价方式。单交换机方式规定，用户需要在链路的每一端各有一个设备，以提供物理端口。设备对组成员端口之间的流量负载进行平衡。

设备还采用相同链路速度方法，其中，组成员端口为具有相同传输速率的全双工点到点链路。用户向组中添加的第一个端口为主端口，它决定了链路聚合组其他成员端口的带宽。

设备允许用户设置最多 2 个链路聚合组 (LAG)。每个链路聚合组的可用端口数量视设备而定。

13.7.2 链路聚合示例

⚠ 警告

不允许的设备操作

为帮助避免在配置阶段出现环路，请分别配置 *Link Aggregation* 配置的每个设备。在连接冗余线路之前，应完成 *Link Aggregation* 配置的其他设备的配置。

如果不遵循这些说明，则会导致死亡、重伤或设备损坏。

使用一个聚合链路组在交换机 1 和 2 之间连接多个工作站。通过对多个链路进行聚合，无需硬件升级即可实现更高的速度。

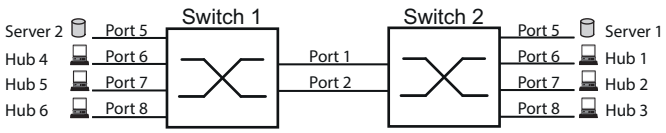


图 48: 交换机到交换机网络链路聚合

在图形用户界面中配置交换机 1 和 2。为此，请执行以下步骤：

- ☐ 打开 *Switching* > *L2-Redundancy* > *Link Aggregation* 对话框。
- ☐ 点击 按钮。
  该对话框显示 *Create* 窗口。
- ☐ 在 *Trunk port* 下拉列表中，选择链路聚合组的实例编号。
- ☐ 在 *Port* 下拉列表中，选择端口 *1/1*。
- ☐ 点击 *Ok* 按钮。
- ☐ 重复以上步骤并选择端口 *1/2*。
- ☐ 点击 *Ok* 按钮。
- ☐ 暂时保存更改。为此，请单击 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`link-aggregation add lag/1`	创建一个链路聚合组 `lag/1`。
`link-aggregation modify lag/1 addport 1/1`	将端口 *1/1* 添加到链路聚合组。
`link-aggregation modify lag/1 addport 1/2`	将端口 *1/2* 添加到链路聚合组。

13.8 链路备份

链路备份为第二层设备上的流量提供一个冗余链路。当设备检测到一级链路上的错误时，会将流量传输到备份链路。一般在服务提供商或企业网络中使用链路备份。

可以成对设置备份链路，一个作为主链路，另一个作为备份链路。例如，为企业网络提供冗余时，设备允许用户设置一对以上的备份链路。链路备份对的最大数量为：物理端口总数 / 2。此外，当参与链路备份对的端口的状态发生改变时，设备会发送一个 SNMP 陷阱。

配置链路备份对时，请记住以下规则：
- 一个链路对由物理端口的任意组合构成。例如，一个端口为 100 Mbit 端口，另一个端口为 1000 Mbit SFP 端口。
- 一个特定端口在任意给定时间都是一个链路备份对的成员。
- 验证一个链路备份对的端口是否是同一个 VLAN 的具有相同 VLAN ID 的成员。当主端口或备份端口是一个 VLAN 的成员时，会将该对的第二个端口分配给同一个 VLAN。

此功能的默认设置为不活动，没有任何链路备份对。

提示：验证链路备份端口上的生成树协议是否已禁用。

13.8.1 故障恢复描述

链路备份还允许用户设置一个故障恢复选项。当您激活故障恢复功能且一级链路恢复正常运行时，设备首先会阻塞备份端口上的流量，然后转发主端口上的流量。此过程有助于防止设备在网络中形成环路。

当主端口恢复链路开启和活动状态时，设备支持两种操作模式：
- 当您停用 *Fail back* 时，主端口将保持阻塞状态，直到备份连路中断为止。
- 当您激活 *Fail back* 时，在 *Fail back delay [s]* 计时器到期之后，主端口会恢复转发状态且备份端口会变为关闭。

在上述情况下，端口强制其链路转发流量，首先向远程设备发送一个“清除 FDB”数据包。该清除数据包可帮助远程设备快速重新学习 MAC 地址。

13.8.2 配置示例

⚠ 警告

不允许的设备操作

为帮助避免在配置阶段出现环路，请分别配置 *Link Backup* 配置的每个设备。在连接冗余线路之前，应完成 *Link Backup* 配置的其他设备的配置。

如果不遵循这些说明，则会导致死亡、重伤或设备损坏。

在如下示例网络中，将交换机 *2/3* 上的端口 *2/4* 和 A 连接到上行链路交换机 B 和 C。将这两个端口设置为一个链路备份对时，其中一个端口会转发流量，另一个端口则处于阻塞模式。

交换机 A 上的主端口 *2/3* 为活动端口，并且向交换机 B 上的端口 1 转发流量。交换机 A 上的端口 *2/4* 为备份端口，并且阻塞流量。

当交换机 A 因为检测到错误而禁用端口 *2/3* 时，交换机 A 上的端口 *2/4* 开始向交换机 C 上的端口 2 转发流量。

当端口 *2/3* 恢复活动状态时，“不关闭”，*Fail back* 被激活且 *Fail back delay [s]* 设为 30 秒。计时器到期之后，端口 *2/4* 首先阻塞流量，随后，端口 *2/3* 开始转发流量。

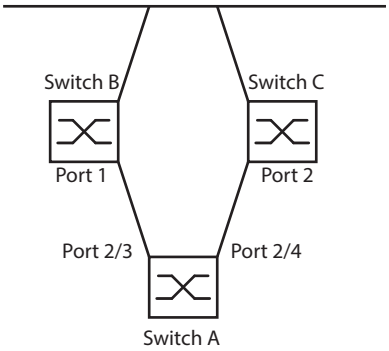


图 49: Link Backup 示例网络

下表包含用于交换机 A 的参数的示例。

请执行以下步骤：

- ☐ 打开 *Switching* > *L2-Redundancy* > *Link Backup* 对话框。
- ☐ 在表中输入一个新的链路备份对：
  - ☐ 点击 按钮。
    该对话框显示 *Create* 窗口。
  - ☐ 在 *Primary port* 下拉列表中，选择端口 *2/3*。
    在 *Backup port* 下拉列表中，选择端口 *2/4*。
  - ☐ 点击 *Ok* 按钮。
- ☐ 在 *Description* 文本框中，输入 Link_Backup_1 作为备份对的名称。
- ☐ 要激活链路备份对的 *Fail back* 功能，请勾选 *Fail back* 复选框。
- ☐ 为链路备份对设置故障恢复计时器，在 *Fail back delay [s]* 中输入 30 秒。
- ☐ 要激活链路备份对，请勾选 *Active* 复选框。
- ☐ 要启用该功能，请选择 *Operation* 框中的 *On* 单选按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`interface 2/3`	切换到接口 *2/3* 的接口配置模式。
`link-backup add 2/4`	创建一个链路备份实例，以端口 *2/3* 作为主端口，并以端口 *2/4* 作为备份端口。
`link-backup modify 2/4 description Link_Backup_1`	指定字符串 Link_Backup_1 作为备份对的名称。
`link-backup modify 2/4 failback-status enable`	启用故障恢复计时器。
`link-backup modify 2/4 failback-time 30`	将故障恢复延迟时间指定为 30 秒。

`link-backup modify 2/4 status enable`	启用链路备份实例。
`exit`	切换到配置模式。
`link-backup operation`	全局启用设备中的 *Link Backup* 功能。

13.9 FuseNet

FuseNet 协议允许用户对使用以下任一冗余协议工作的环网进行耦合：

- MRP
- HIPER 环网
- RSTP

提示： 使用 *Ring/Network Coupling* 协议将网络耦合到主环网的前提条件是已连接的网络仅包含支持 *Ring/Network Coupling* 协议的网络设备。

使用下表选择要在用户网络中使用的 *FuseNet* 耦合协议：

主环网	连接的网络		
	MRP	HIPER 环网	RSTP
MRP	*Sub Ring*[1)]	- *Redundant Coupling Protocol* - *Ring/Network Coupling*	- *Redundant Coupling Protocol* - *Ring/Network Coupling*
HIPER 环网	*Sub Ring*	*Ring/Network Coupling*	- *Redundant Coupling Protocol* - *Ring/Network Coupling*
RSTP	*Redundant Coupling Protocol*	*Redundant Coupling Protocol*	*Dual RSTP* + *Redundant Coupling Protocol*

- 无适用的耦合协议

1) 使用在不同 VLAN 上配置的 *MRP*

13.10 子环网

Sub Ring 功能是介质冗余协议（MRP）的扩展。此功能允许用户使用各种网络结构将子环网与主环网耦合起来。

子环网协议将本为扁平的网络的两端与主环网耦合起来，从而为设备提供冗余。

建立子环网具有以下优点：
- 通过耦合过程，可以将新的网段包括到冗余概念中。
- 子环网允许将新的区域轻松集成到现有网络之中。
- 子环网允许用户对网络拓扑中一个区域的组织结构轻松进行映射。
- 在一个 MRP 环网中，冗余情况下子环网的故障转移时间一般少于 100 毫秒。

13.10.1 子环网描述

子环网概念允许用户将新的网段与现有环网（主环网）中的适当设备耦合起来。用户将子环网耦合到主环网时所使用的设备是子环网管理器（SRM）。

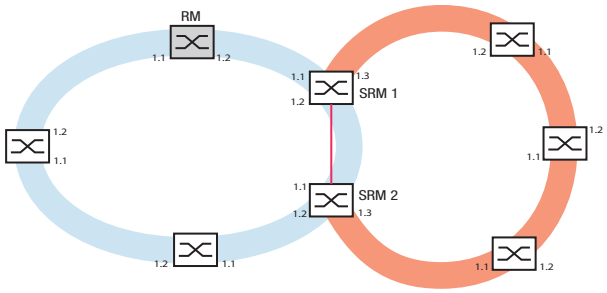


图 50: 子环网结构示例
蓝色环网 = 主环网
橙色环网 = 子环网
红色线 = 子环网的冗余链路
SRM = 子环网管理器
RM = 环网管理器

具有子环网管理器功能的设备支持最多 8 个实例，因此可最多同时管理 8 个子环网。

Sub Ring 功能允许用户集成作为参与者支持 MRP 的设备。用户将子环网耦合到主环网时所使用的设备需要 *Sub Ring* 管理器功能。

每个子环网由最多 200 个参与者组成，子环网管理器本身以及主环网中子环网管理器之间的设备除外。

下图显示了可能的子环网拓扑的示例：

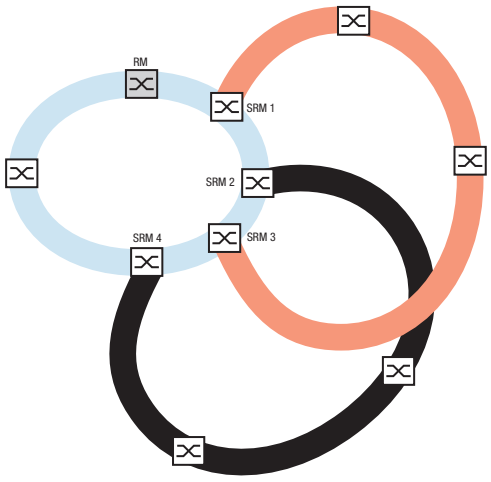


图 51: 子环网结构重叠示例

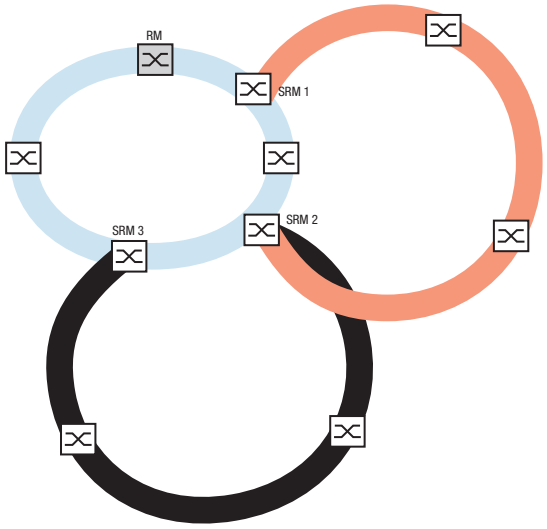


图 52: 特例：一个子环网管理器管理两个子环网（两个实例）。子环网管理器能够管理最多 8 个实例。

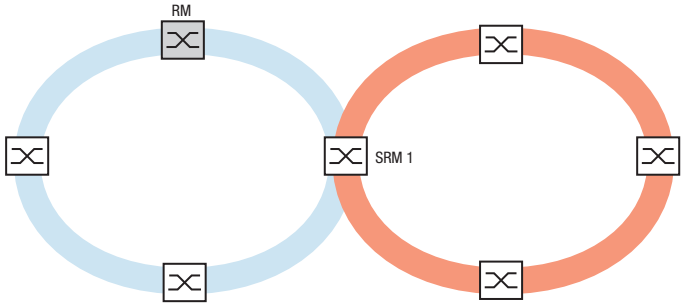


图 53: 特例：一个子环网管理器管理不同端口上子环网的两端（单一子环网管理器）。

提示：在以上示例中，子环网管理器只将子环网耦合到现有主环网。*Sub Ring* 功能禁止级联子环网，例如，将一个新的子环网耦合到另一个现有子环网。

如果将 MRP 用于主环网和子环网，则请按如下方式指定 VLAN 设置：

▶ 主环网的 VLAN X
  – 在主环网参与者的环网端口上
  – 在子环网管理器的主环网端口上
▶ 子环网的 VLAN Y
  – 在子环网参与者的环网端口上
  – 在子环网管理器的子环网端口上

可以对多个子环网使用相同的 VLAN。

13.10.2 子环网示例

在以下示例中，将一个具有三个设备的新网段耦合到一个使用 MRP 协议的现有主环网。在两端而非一端对网络进行耦合时，具有相应配置的子环网可提供更高的可用性。

将新网段作为一个子环网进行耦合。可以使用以下配置类型将子环网耦合到主环网的现有设备。

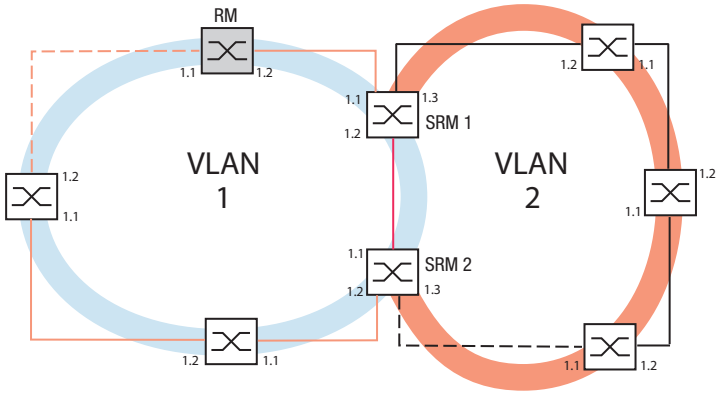


图 54: 子环网结构示例
橙色线 = VLAN 1 中的主环网成员
黑色线 = VLAN 2 中的子环网成员
橙色虚线 = 主环网开环
黑色虚线 = 子环网开环
红色线 = VLAN 1 中的冗余链路成员
SRM = 子环网管理器
RM = 环网管理器

要配置子环网，请执行以下步骤：

☐ 将新网段的三个设备配置为一个 MRP 环网的参与者：
  – 根据下表为环网端口配置传输速率和双工模式：

表格 37: 子环网端口的端口设置

端口类型	比特率	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	勾选	未勾选	*100 Mbit/s FDX*
TX	1 Gbit/s	勾选	勾选	–
光学	100 Mbit/s	勾选	未勾选	*100 Mbit/s FDX*
光学	1 Gbit/s	勾选	勾选	–
光学	2.5 Gbit/s	勾选	–	*2.5 Gbit/s FDX*

以下步骤包含了子环网配置的附加设置：

- ☐ 为了帮助防止配置期间出现环路，请停用主环网和子环网设备上的子环网管理器功能。在完全配置了参与主环网和子环网的每个设备之后，激活全局 *Sub Ring* 功能和子环网管理器。
- ☐ 禁用子环网中使用的 MRP 环网端口上的 RSTP 功能。
- ☐ 验证参与主环网和子环网的端口上的 *Link Aggregation* 功能是否已停用。
- ☐ 即使主环网在使用 MRP 协议，仍为主环网端口和子环网端口指定一个不同的 VLAN 成员资格。例如，对主环网和冗余链路使用 VLAN ID 1，然后对子环网使用 VLAN ID 2。
  - 例如，对于参与主环网的设备，打开 *Switching > VLAN > Configuration* 对话框。在静态 VLAN 表中创建 VLAN 1。在相应端口列的下拉列表中选择 1 项目，为主环网端口添加 VLAN T 成员资格标签。
  - 对于参与子环网的设备，请使用以上步骤并在静态 VLAN 表中将端口添加到 VLAN 2。
- ☐ 为主环网和子环网设备激活 *MRP* 功能。
  - 在 *Switching > L2-Redundancy > MRP* 对话框中，在主环网设备上配置两个参与主环网的环网端口。
  - 对于参与子环网的设备，请使用以上步骤并在子环网设备上配置两个参与子环网的环网端口。
  - 向主环网和子环网设备分配相同的 MRP 域 ID。当用户仅使用 Schneider Electric 设备时，默认值即可满足 MRP 域 ID 的要求。

提示： *MRP domain* 是一个范围从 0 到 255 的 16 个数字的序列。默认值为 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255 . 255。全部为零的 *MRP domain* 无效。

Sub Ring 对话框可用于更改 MRP 域 ID。或者，使用命令行界面。为此，请执行以下步骤：

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`mrp domain delete`	删除当前的 MRP 域。
`mrp domain add domain-id 0.0.1.1.2.2.3.4.4.111.222.123.0.0.66.99`	生成一个具有指定 MRP 域 ID 的新 MRP 域。任何后续的 MRP 域更改都适用于此域 ID。

13.10.3 子环网配置示例

⚠ 警告

不允许的设备操作

为帮助避免在配置阶段出现环路，请分别配置 *Sub Ring* 配置的每个设备。在连接冗余线路之前，应完成环网配置的其他设备的配置。

如果不遵循这些说明，则会导致死亡、重伤或设备损坏。

提示： 在配置期间注意避免形成环路。分别配置子环网的每个设备。在激活冗余链路之前，请完全配置好每个子环网设备。

配置示例中的两个子环网管理器。为此，请执行以下步骤：

- ☐ 打开 *Switching* > *L2-Redundancy* > *Sub Ring* 对话框。
- ☐ 要添加一个表格条目，请点击  按钮。
- ☐ 在 *Port* 列中，选择将设备耦合到子环网的端口。
  对于此示例，请使用端口 *1/3*。
  对于耦合，使用任一可用端口，已经连接到主环网的端口除外。
- ☐ 在 *Name* 列中，向子环网分配一个名称。
  对于此示例，请输入 Test。
- ☐ 在 *SRM mode* 列中，选择子环网管理器模式。
  由此，可以指定用于将子环网耦合到主环网的哪个端口成为冗余管理器。
  耦合选项为：
  - ▶ manager
    当您指定两个具有相同值的子环网管理器时，MAC 地址较高的设备将管理冗余链路。
  - ▶ redundant manager
    此设备负责管理冗余链路，条件是，已将另一个子环网管理器指定为 manager。否则，MAC 地址较高的设备将管理冗余链路。

  根据此示例示意图将子环网管理器 1 指定为 manager.
- ☐ 将 *VLAN* 列和 *MRP domain* 列中的值保留不变。
  对于示例配置，默认值是正确的。
- ☐ 暂时保存更改。为此，请单击  按钮。

enable	切换到特权执行模式。
configure	切换到配置模式。
sub-ring add 1	创建一个子环网 ID 为 1 的新子环网。
sub-ring modify 1 port 1/3	将端口 *1/3* 指定为子环网端口。
sub-ring modify 1 name Test	将名称 Test 分配给子环网 1。
sub-ring modify 1 mode manager	将 manager 模式分配给子环网 1。
show sub-ring ring	在此设备上显示子环网状态。
show sub-ring global	在此设备上显示子环网全局状态。

- ☐ 以相同方式配置第二个子环网管理器。
  根据此示例示意图将子环网管理器 2 指定为 redundant manager。

- ☐ 要激活子环网管理器功能，请勾选相应行中的 *Active* 复选框。
- ☐ 对两个子环网管理器以及参与子环网的设备进行配置后，启用该功能并关闭冗余链路。
- ☐ 暂时保存更改。为此，请单击  按钮。

enable	切换到特权执行模式。
configure	切换到配置模式。
sub-ring enable 1	激活子环网 1。
sub-ring enable 2	激活子环网 2。
exit	切换到特权执行模式。

`show sub-ring ring <Domain ID>`	显示所选子环网的设置。
`show sub-ring global`	显示全局子环网设置。
`copy config running-config nvm profile Test`	将当前设置保存到永久存储器（Test）中名称为 nvm 的配置概要文件中。

13.11 采用 LAG 的子环网

⚠ 警告

不允许的设备操作

为帮助避免在配置阶段出现环路，请分别配置 *Sub Ring* 配置的每个设备。在连接冗余线路之前，应完成环网配置的其他设备的配置。

如果不遵循这些说明，则会导致死亡、重伤或设备损坏。

当两台设备之间存在至少两条并行冗余连接线路（称为中继）并且这些线路合并为一个逻辑连接时，这就是链路聚合组（LAG）连接。

设备允许用户通过 *Sub Ring* 协议将 LAG 端口用作环网端口。

13.11.1 示例

以下示例是 MRP 环网与子环网之间的简单设置。

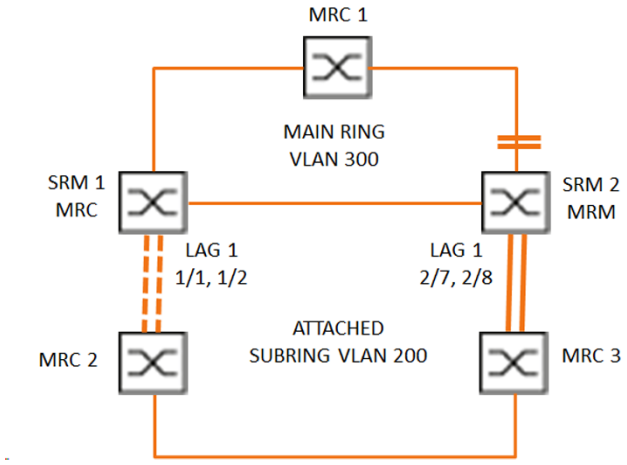


图 55: 采用链路聚合的子环网

下表描述上图中显示的设备角色。该表提供关于如何将环网端口和子环网端口用作 LAG 端口的信息。

表格 38: 设备、端口和角色

设备名称	环网端口	主环网角色	子环网角色	子环网端口
MRC1	1/3, 1/4	MRP 客户端›	-	-
SRM1	1/3, 1/4	MRP 客户端›	冗余管理器	lag/1

表格 38: 设备、端口和角色

设备名称	环网端口	主环网角色	子环网角色	子环网端口
SRM2	2/4, 2/5	MRP 管理器	管理器	lag/1
MRC2	lag/1, 1/3	-	MRP 客户端›	-
MRC3	lag/1, 1/3	-	MRP 客户端›	-

MRP 环网配置

参与主环网的设备是 VLAN 300 的成员。

请执行以下步骤：

SRM2

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`mrp domain add default-domain`	创建一个 ID 为 default-domain 的新的 MRP 域。
`mrp domain modify port primary 2/4`	将端口 *2/4* 指定为环网端口 1。
`mrp domain modify port secondary 2/5`	将端口 *2/5* 指定为环网端口 2。
`mrp domain modify mode manager`	指定设备作为 *Ring manager* 进行工作。不要激活任何其他设备上的 *Ring manager* 功能。
`mrp domain modify operation enable`	激活 MRP 环网。
`mrp domain modify vlan 300`	将 VLAN ID 指定为 300。
`mrp operation`	启用设备中的 *MRP* 功能。

MRC1, SRM1

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`mrp domain add default-domain`	创建一个 ID 为 default-domain 的新的 MRP 域。
`mrp domain modify port primary 1/3`	将端口 *1/3* 指定为环网端口 1。
`mrp domain modify port secondary 1/4`	将端口 *1/4* 指定为环网端口 2。
`mrp domain modify mode client`	将设备角色指定为环网客户端。
`mrp domain modify operation enable`	激活 MRP 环网。
`mrp domain modify vlan 300`	将 VLAN ID 指定为 300。
`mrp operation`	启用设备中的 *MRP* 功能。

子环网配置

参与附加的子环网的设备是 VLAN 200 的成员。

请执行以下步骤：

SRM1

enable	切换到特权执行模式。
configure	切换到配置模式。
link-aggregation add lag/1	创建一个链路聚合组 lag/1。
link-aggregation modify lag/1 addport 1/1	将端口 *1/1* 添加到链路聚合组。
link-aggregation modify lag/1 addport 1/2	将端口 *1/2* 添加到链路聚合组。
link-aggregation modify lag/1 adminmode	激活链路聚合组。

enable	切换到特权执行模式。
configure	切换到配置模式。
sub-ring add 1	创建一个子环网 ID 为 1 的新子环网。
sub-ring modify 1 name SRM1	将名称 SRM1 分配给子环网 1。
sub-ring modify 1 mode redundant-manager vlan 200 port lag/1	为设备分配子环网 1 中的角色 Sub-ring redundant manager。如果子环网闭合，则设备阻止环网端口。VLAN 200 设置为域的 VLAN ID。lag/1 端口设置为 VLAN 200 中的成员。
sub-ring enable 1	激活子环网 1。
sub-ring operation	在此设备上启用全局子环网管理器功能。

SRM2

enable	切换到特权执行模式。
configure	切换到配置模式。
link-aggregation add lag/1	创建一个链路聚合组 lag/1。
link-aggregation modify lag/1 addport 2/7	将端口 *2/7* 添加到链路聚合组。
link-aggregation modify lag/1 addport 2/8	将端口 *2/8* 添加到链路聚合组。
link-aggregation modify lag/1 adminmode	激活链路聚合组。

enable	切换到特权执行模式。
configure	切换到配置模式。
sub-ring add 1	创建一个子环网 ID 为 1 的新子环网。
sub-ring modify 1 mode manager vlan 200 port lag/1	为设备分配子环网 1 中的角色 Subring manager。VLAN 200 设置为域的 VLAN ID。lag/1 端口设置为 VLAN 200 中的成员。
sub-ring modify 1 name SRM2	将名称 SRM2 分配给子环网 1。
sub-ring enable 1	激活子环网 1。
sub-ring operation	在此设备上启用全局子环网管理器功能。

MRC 2, 3

enable	切换到特权执行模式。
configure	切换到配置模式。
mrp domain add default-domain	创建一个 ID 为 default-domain 的新的 MRP 域。
mrp domain modify port primary lag/1	将端口 lag/1 指定为环网端口 1。
mrp domain modify port secondary 1/3	将端口 *1/3* 指定为环网端口 2。
mrp domain modify mode client	将设备角色指定为环网客户端。
mrp domain modify operation enable	激活 MRP 环网。
mrp domain modify vlan 200	将 VLAN ID 指定为 200。
mrp operation	启用设备中的 *MRP* 功能。

禁用 STP

在指定为 MRP 或子环网端口的每个端口上禁用 *Spanning Tree* 功能。以下示例使用端口 *1/3*。

请执行以下步骤：

enable	切换到特权执行模式。
configure	切换到配置模式。
interface 1/3	切换到接口 *1/3* 的接口配置模式。
no spanning-tree operation	禁用端口上的 *Spanning Tree* 功能。

13.12 Ring/Network Coupling

根据特定环网，*Ring/Network Coupling* 功能对环网或网段进行冗余耦合。*Ring/Network Coupling* 通过两个不同路径连接两个环网/网段。

当耦合网络中的设备为 Schneider Electric 设备时，*Ring/Network Coupling* 功能将支持在一级和二级环网中按照环网协议进行耦合：

- HIPER 环网
- Fast HIPER 环网
- MRP

Ring/Network Coupling 功能还可对总线和网状结构的网段进行耦合。

13.12.1 Ring/Network Coupling 方式

单交换机耦合

第一个环网/网络中的**一个**设备的两个端口连接到第二个环网/网络中两个设备上的各一个端口(参阅图 56)。在单交换机耦合方式中，主线路转发数据，设备阻塞冗余线路。

当主线路不再工作时，设备会立即取消阻塞冗余线路。当主线路恢复时，设备会阻塞冗余线路上的数据。主线路会再次转发数据。

环网耦合可在 500 毫秒（一般为 150 毫秒）之内检测和处理错误。

双交换机耦合

第一个环网/网络中的**两个**设备的各一个端口连接到第二个环网/网段中两个设备上的各一个端口(参阅图 58)。

冗余线路中的设备与主线路中的设备通过以太网或控制线路使用控制数据包相互告知各自的工作状态。

当主线路不再工作时，冗余设备（待机）会立即取消阻塞冗余线路。当主线路恢复时，主线路上的设备会立即向冗余设备告知此情况。待机设备会阻塞冗余线路上的数据。主线路会再次转发数据。

环网耦合可在 500 毫秒（一般为 150 毫秒）之内检测和处理错误。

耦合配置的类型主要由网络拓扑和所需可用性级别决定(参阅表格 39)。

表格 39: 冗余耦合配置类型选择标准

	单交换机耦合	双交换机耦合	具有控制线路的双交换机耦合
应用	两个设备所处拓扑位置不切实际。 因此，对于双交换机耦合而言，在二者之间布置一个链路会涉及很大的工作量。	两个设备所处拓扑位置切合实际。 控制线路安装会涉及很大的工作量。	两个设备所处拓扑位置切合实际。 控制线路安装不会涉及较大的工作量。
缺点	如果为冗余耦合配置的交换机无法工作，则网络之间不再有连接。	（与单交换机耦合相比）将两个设备连接到网络需要更大的工作量。	（与单交换机和双交换机耦合相比）将两个设备连接到网络需要更大的工作量。
优点	（与双交换机耦合相比）将两个设备连接到网络涉及的工作量减少。	当为冗余耦合配置的设备之一无法工作时，耦合网络仍保持连接。	当为冗余耦合配置的设备之一无法工作时，耦合网络仍保持连接。 与没有控制线路的情况相比，耦合设备之间伙伴机的确定可以更安全、更快速地完成。

13.12.2 准备 Ring/Network Coupling

⚠ 警告

不允许的设备操作

为帮助避免在配置阶段出现环路，请分别配置 *Ring/Network Coupling* 配置的每个设备。在连接冗余线路之前，应完成环网配置的其他设备的配置。

为帮助避免环路，请仅在已停用快速生成树协议的端口上使用 *Ring/Network Coupling* 功能。

如果不遵循这些说明，则会导致死亡、重伤或设备损坏。

利用对话框中的图像，可以定义设备在 *Ring/Network Coupling* 中的角色。

在以下屏幕截图和示意图中，采用以下准则：
- 蓝色方框和线条表示当前正在描述的设备或项目连接。
- 实线表示主要连接。
- 虚线表示备用连接。
- 点线表示控制线路。

请执行以下步骤：

- ☐ 打开 *Switching > L2-Redundancy > Ring/Network Coupling* 对话框。
- ☐ 在 *Mode* 框的 *Type* 选项列表中，选择所需的单选按钮。
  - ▶ *one-switch coupling*
  - ▶ *two-switch coupling, master*
  - ▶ *two-switch coupling, slave*
  - ▶ *two-switch coupling with control line, master*
  - ▶ *two-switch coupling with control line, slave*

单交换机耦合

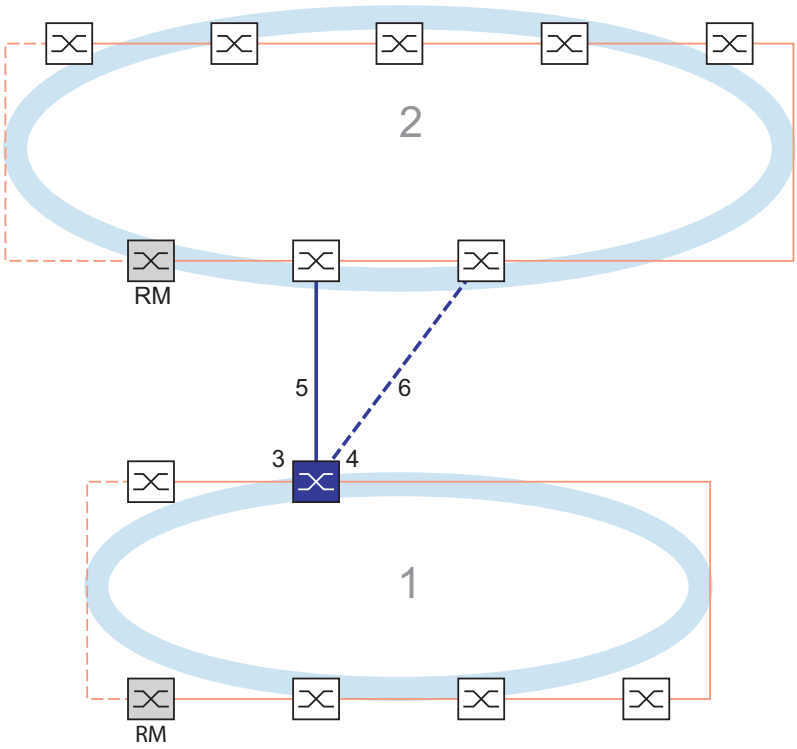


图 56: 单交换机耦合示例
1：环网
2：骨干
3：伙伴机耦合端口
4：耦合端口
5：主线路
6：冗余线路

以蓝色实线表示并且连接到伙伴机耦合端口的主线路在正常工作模式下在两个网络之间提供耦合。如果主线路无法工作，则以蓝色虚线表示并且连接到耦合端口的冗余线路将接替环网/网络耦合。一个交换机执行耦合切换。

以下设置适用于所选图形中以蓝色显示的设备。

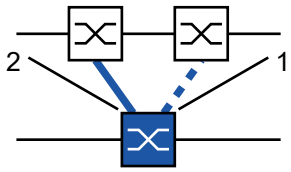


图 57: 单交换机耦合
1：耦合端口
2：伙伴机耦合端口

请执行以下步骤：

- ☐ 打开 *Switching* > *L2-Redundancy* > *Ring/Network Coupling* 对话框。
- ☐ 在 *Mode* 框的 *Type* 选项列表中，选择 *one-switch coupling* 单选按钮。

提示：配置不同端口上的 *Partner coupling port* 和环网端口。

- ☐ 在 *Coupling port* 框中，在 *Port* 下拉列表中选择要在其上连接冗余线路的端口。
- ☐ 在 *Partner coupling port* 框中，在 *Port* 下拉列表中选择要在其上连接主线路的端口。
- ☐ 要启用该功能，请选择 *Operation* 框中的 *On* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。
- ☐ 将冗余线路连接到伙伴机耦合端口。
  在 *Partner coupling port* 框中，*State* 字段显示伙伴机耦合端口的状态。
- ☐ 将主线路连接到耦合端口。
  在 *Coupling port* 框中，*State* 字段会显示耦合端口的状态。

在 *Information* 框中，*Redundancy available* 字段会显示冗余是否可用。*Configuration failure* 字段会显示设置是否已完成以及是否正确。

对于耦合端口，执行以下步骤：

提示：耦合端口需要以下设置。

- ☐ 打开 *Basic Settings* > *Port* 对话框的 *Configuration* 选项卡。
- ☐ 对于被选为耦合端口的端口，请根据下表中的参数指定设置。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

表格 40: 环网端口的端口设置

端口类型	比特率	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	勾选	未勾选	*100 Mbit/s FDX*
TX	1 Gbit/s	勾选	勾选	-
光学	100 Mbit/s	勾选	未勾选	*100 Mbit/s FDX*
光学	1 Gbit/s	勾选	勾选	-
光学	2.5 Gbit/s	勾选	–	*2.5 Gbit/s FDX*

如果已经配置了耦合端口上的 VLAN，则指定耦合端口和伙伴机耦合端口上的 VLAN 设置：为此，请执行以下步骤：

- ☐ 打开 *Switching > VLAN > Port* 对话框。
- ☐ 将 *Port-VLAN ID* 设置更改为端口上配置的 VLAN ID 的值。
- ☐ 取消勾选两个耦合端口的 *Ingress filtering* 复选框。
- ☐ 打开 *Switching > VLAN > Configuration* 对话框。
- ☐ 要为冗余连接添加 VLAN 1 和 VLAN 成员资格标签，请在对应 T 行中两个耦合端口的单元格中输入值 VLAN 1。
- ☐ 暂时保存更改。为此，请单击 按钮。

耦合设备在 VLAN 1 上以最高优先级发送冗余数据包。

- ☐ 在 *Configuration* 框的 *Redundancy mode* 选项列表中，指定冗余类型：
  - ▶ 使用 *redundant ring/network coupling* 设置时，主线路或冗余线路已激活。该设置允许设备在两个线路之间进行切换。
  - ▶ 当您激活 *extended redundancy* 设置时，主线路和冗余线路会同时激活。该设置允许用户向耦合网络添加冗余。当第二个网络中耦合设备之间的连接无法工作时，耦合设备将继续传输和接收数据。

提示：在重新配置期间，会出现数据包重复。因此，如果用户设备检测到数据包重复，则可选择此设置。

Coupling mode 描述了与环网相连的骨干网络的类型(参阅图 56)。

- ☐ 在 *Configuration* 框的 *Coupling mode* 选项列表中，指定第二个网络的类型：
  - ☐ 如果连接到环网，则请选择 *ring coupling* 单选按钮。
  - ☐ 如果连接到总线或网状结构，则请选择 *network coupling* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 按钮。

将耦合设置重置为默认状态。为此，请执行以下步骤：

- ☐ 点击 按钮，然后点击 *Reset* 项目。

双交换机耦合

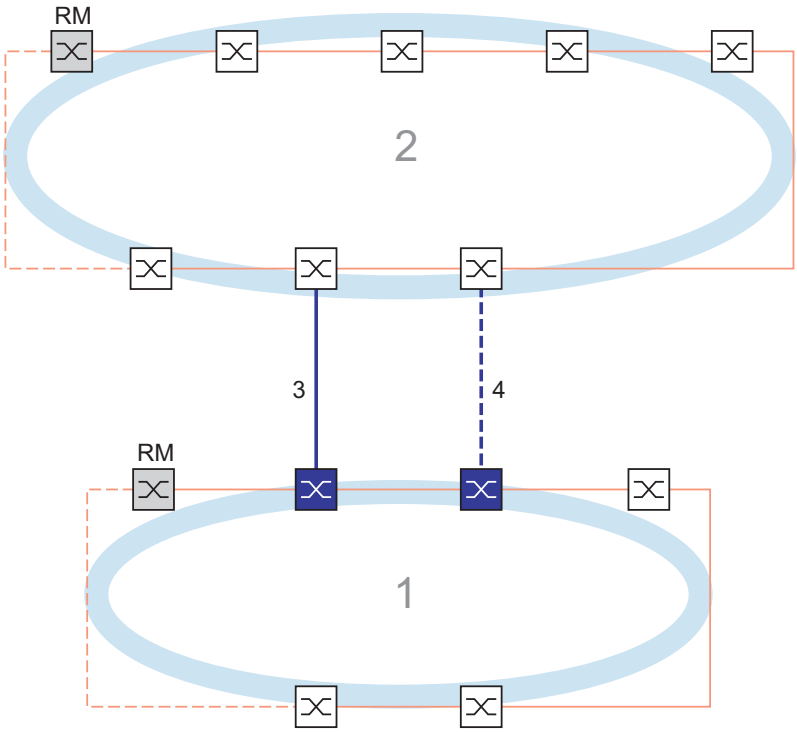


图 58: 双交换机耦合示例
1：环网
2：骨干
3：主线路
4：冗余线路

两个网络之间的耦合由蓝色实线表示的主线路执行。如果主线路或相邻设备之一无法工作，则黑色虚线表示的冗余线路会接替网络耦合。耦合由两个设备执行。

设备通过以太网相互发送控制数据包。

就耦合而言，连接到主线路的主设备与连接到冗余线路的待机设备互为伙伴机。
□ 使用环网端口连接两台伙伴机。

双交换机耦合，主设备

以下设置适用于所选图形中以蓝色显示的设备。

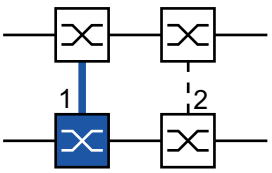


图 59: 双交换机耦合，主设备
1：耦合端口
2：伙伴机耦合端口

请执行以下步骤：

- ☐ 打开 *Switching* > *L2-Redundancy* > *Ring/Network Coupling* 对话框。
- ☐ 在 *Mode* 框的 *Type* 选项列表中，选择 *two-switch coupling, master* 单选按钮。
- ☐ 在 *Coupling port* 框中，在 *Port* 下拉列表中选择要在其上连接网段的端口。
  配置不同端口上的 *Coupling port* 和环网端口。
- ☐ 要启用该功能，请选择 *Operation* 框中的 *On* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。
- ☐ 将主线路连接到 *Coupling port*。
  在 *Coupling port* 框中，*State* 字段会显示耦合端口的状态。
  当伙伴机在网络中已经工作时，*Partner coupling port* 框中的 *IP address* 字段会显示伙伴机端口的 IP 地址。

在 *Information* 框中，*Redundancy available* 字段会显示冗余是否可用。*Configuration failure* 字段会显示设置是否已完成以及是否正确。

提示：如果在同一个设备上操作 *Ring manager* 功能和双交换机耦合功能，则可能会造成环路。

为了帮助防止当环网耦合端口上的连接正在工作时形成连续环路，请执行以下任一操作。设备将耦合端口的端口状态设置为“关”：

- 禁用操作
- 更改配置

对于耦合端口，执行以下步骤：

- ☐ 打开 *Basic Settings* > *Port* 对话框的 *Configuration* 选项卡。
- ☐ 对于被选为耦合端口的端口，请根据下表中的参数指定设置。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

表格 41: 环网端口的端口设置

端口类型	比特率	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	勾选	未勾选	*100 Mbit/s FDX*
TX	1 Gbit/s	勾选	勾选	-
光学	100 Mbit/s	勾选	未勾选	*100 Mbit/s FDX*
光学	1 Gbit/s	勾选	勾选	-
光学	2.5 Gbit/s	勾选	–	*2.5 Gbit/s FDX*

如果已经配置了耦合端口上的 VLAN，则指定耦合端口和伙伴机耦合端口上的 VLAN 设置：为此，请执行以下步骤：

- ☐ 打开 *Switching* > *VLAN* > *Port* 对话框。
- ☐ 将 *Port-VLAN ID* 设置更改为端口上配置的 VLAN ID 的值。
- ☐ 取消勾选两个耦合端口的 *Ingress filtering* 复选框。
- ☐ 打开 *Switching* > *VLAN* > *Configuration* 对话框。

- ☐ 要为冗余连接添加 VLAN 1 和 VLAN 成员资格标签，请在对应 T 行中两个耦合端口的单元格中输入值 VLAN 1。
- ☐ 暂时保存更改。为此，请单击 ✓ 按钮。

耦合设备在 VLAN 1 上以最高优先级发送冗余数据包。

双交换机耦合，待机设备

以下设置适用于所选图形中以蓝色显示的设备。

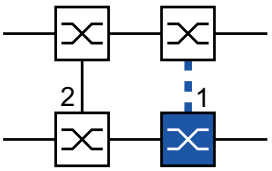


图 60: 双交换机耦合，待机设备
1：耦合端口
2：伙伴机耦合端口

请执行以下步骤：

- ☐ 打开 *Switching* > *L2-Redundancy* > *Ring/Network Coupling* 对话框。
- ☐ 在 *Mode* 框的 *Type* 选项列表中，选择 *two-switch coupling, slave* 单选按钮。
- ☐ 在 *Coupling port* 框中，在 *Port* 下拉列表中选择要在其上连接网段的端口。
  配置不同端口上的 *Coupling port* 和环网端口。
- ☐ 要启用该功能，请选择 *Operation* 框中的 *On* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 ✓ 按钮。
- ☐ 将冗余线路连接到 *Coupling port*。
  在 *Coupling port* 框中，*State* 字段会显示耦合端口的状态。
  当伙伴机在网络中已经工作时，*Partner coupling port* 框中的 *IP address* 字段会显示伙伴机端口的 IP 地址。

在 *Information* 框中，*Redundancy available* 字段会显示冗余是否可用。*Configuration failure* 字段会显示设置是否已完成以及是否正确。

提示：如果在同一个设备上操作 *Ring manager* 功能和双交换机耦合功能，则可能会造成环路。

为了帮助防止当环网耦合端口上的连接正在工作时形成连续环路，请执行以下任一操作。设备将耦合端口的端口状态设置为“关”：

- 禁用操作
- 更改配置

对于耦合端口，执行以下步骤：

- ☐ 打开 *Basic Settings* > *Port* 对话框的 *Configuration* 选项卡。
- ☐ 对于被选为耦合端口的端口，请根据下表中的参数指定设置。
- ☐ 暂时保存更改。为此，请单击 ✓ 按钮。

表格 42: 环网端口的端口设置

端口类型	比特率	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	勾选	未勾选	*100 Mbit/s FDX*
TX	1 Gbit/s	勾选	勾选	-
光学	100 Mbit/s	勾选	未勾选	*100 Mbit/s FDX*
光学	1 Gbit/s	勾选	勾选	-
光学	2.5 Gbit/s	勾选	–	*2.5 Gbit/s FDX*

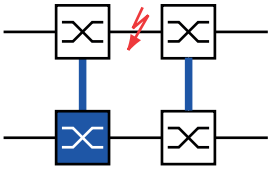
如果已经配置了耦合端口上的 VLAN，则指定耦合端口和伙伴机耦合端口上的 VLAN 设置：为此，请执行以下步骤：

- ☐ 打开 *Switching* > *VLAN* > *Port* 对话框。
- ☐ 将 *Port-VLAN ID* 设置更改为端口上配置的 VLAN ID 的值。
- ☐ 取消勾选两个耦合端口的 *Ingress filtering* 复选框。
- ☐ 打开 *Switching* > *VLAN* > *Configuration* 对话框。
- ☐ 要为冗余连接添加 VLAN 1 和 VLAN 成员资格标签，请在对应 T 行中两个耦合端口的单元格中输入值 VLAN 1。
- ☐ 暂时保存更改。为此，请单击 按钮。

耦合设备在 VLAN 1 上以最高优先级发送冗余数据包。

指定 *Redundancy mode* 和 *Coupling mode* 设置。为此，请执行以下步骤：

- ☐ 打开 *Switching* > *L2-Redundancy* > *Ring/Network Coupling* 对话框。
- ☐ 在 *Configuration* 框的 *Redundancy mode* 选项列表中，选择以下单选按钮之一：
  - ▶ *redundant ring/network coupling*
    使用此设置时，主线路或冗余线路已激活。该设置允许设备在两个线路之间进行切换。
  - ▶ *extended redundancy*
    使用此设置时，主线路和冗余线路同时激活。该设置允许用户向第二个网络添加冗余。当第二个网络中耦合设备之间的连接无法工作时，耦合设备将继续传输和接收数据。



    在重新配置期间，会出现数据包重复。因此，只有当您的设备检测到数据包重复时方可选择此设置。
- ☐ 在 *Configuration* 框的 *Coupling mode* 选项列表中，选择以下单选按钮之一：
  - ☐ 如果连接到环网，则请选择 *ring coupling* 单选按钮。
  - ☐ 如果连接到总线或网状结构，则请选择 *network coupling* 单选按钮。

  Coupling mode 描述了与环网相连的骨干网络的类型(参阅图 58)。
- ☐ 暂时保存更改。为此，请单击 按钮。

将耦合设置重置为默认状态。为此，请执行以下步骤：

- ☐ 点击 按钮，然后点击 *Reset* 项目。

具有控制线路的双交换机耦合

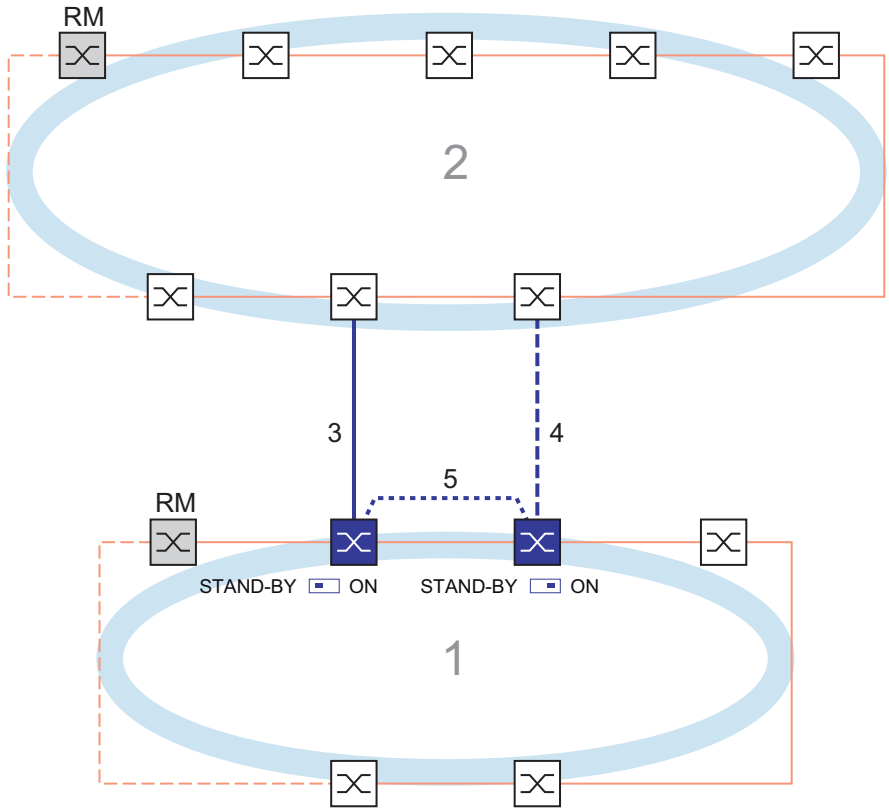


图 61: 具有控制线路的双交换机耦合示例

1：环网
2：骨干
3：主线路
4：冗余线路
5：控制线路

两个网络之间的耦合由蓝色实线表示的主线路执行。如果主线路或相邻设备之一无法工作，则蓝色虚线表示的冗余线路会接替两个网络的耦合。环网耦合由两个设备执行。

设备通过下图中蓝色点线表示的控制线路发送控制数据包(参阅图 62)。

就耦合而言，连接到主线路的主设备与连接到冗余线路的待机设备互为伙伴机。
□ 使用环网端口连接两台伙伴机。

具有控制线路的双交换机耦合，主设备

以下设置适用于所选图形中以蓝色显示的设备。

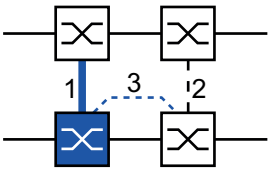


图 62: 双交换机耦合，主设备

1：耦合端口
2：伙伴机耦合端口
3：控制线路 Control line

请执行以下步骤：

- ☐ 打开 *Switching > L2-Redundancy > Ring/Network Coupling* 对话框。
- ☐ 在 *Mode* 框的 *Type* 选项列表中，选择 *two-switch coupling with control line, master* 单选按钮。
- ☐ 在 *Coupling port* 框中，在 *Port* 下拉列表中选择要在其上连接网段的端口。
  配置不同端口上的 *Coupling port* 和环网端口。
- ☐ 在 *Control port* 框中，在 *Port* 下拉列表中选择要在其上连接控制线路的端口。
  配置不同端口上的 *Coupling port* 和环网端口。
- ☐ 要启用该功能，请选择 *Operation* 框中的 *On* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。
- ☐ 将冗余线路连接到耦合端口。
  在 *Coupling port* 框中，*State* 字段会显示耦合端口的状态。
  当伙伴机在网络中已经工作时，*Partner coupling port* 框中的 *IP address* 字段会显示伙伴机端口的 IP 地址。
- ☐ 将控制线路连接到控制端口。
  在 *Control port* 框中，*State* 字段会显示控制端口的状态。
  当伙伴机在网络中已经工作时，*Partner coupling port* 框中的 *IP address* 字段会显示伙伴机端口的 IP 地址。

在 *Information* 框中，*Redundancy available* 字段会显示冗余是否可用。*Configuration failure* 字段会显示设置是否已完成以及是否正确。

提示：如果在同一个设备上操作 *Ring manager* 功能和双交换机耦合功能，则可能会造成环路。

为了帮助防止当环网耦合端口上的连接正在工作时形成连续环路，请执行以下任一操作。设备将耦合端口的端口状态设置为“关”：

- 禁用操作
- 更改配置

对于耦合端口，执行以下步骤：

- ☐ 打开 *Basic Settings > Port* 对话框的 *Configuration* 选项卡。
- ☐ 对于被选为耦合端口的端口，请根据下表中的参数指定设置。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

表格 43: 环网端口的端口设置

端口类型	比特率	Port on	Automatic configuration	Manual configuration
TX	100 Mbit/s	勾选	未勾选	*100 Mbit/s FDX*
TX	1 Gbit/s	勾选	勾选	-
光学	100 Mbit/s	勾选	未勾选	*100 Mbit/s FDX*
光学	1 Gbit/s	勾选	勾选	-
光学	2.5 Gbit/s	勾选	–	*2.5 Gbit/s FDX*

如果已经配置了耦合端口上的 VLAN，则指定耦合端口和伙伴机耦合端口上的 VLAN 设置：为此，请执行以下步骤：

- ☐ 打开 *Switching* > *VLAN* > *Port* 对话框。
- ☐ 将 *Port-VLAN ID* 设置更改为端口上配置的 VLAN ID 的值。
- ☐ 取消勾选两个耦合端口的 *Ingress filtering* 复选框。
- ☐ 打开 *Switching* > *VLAN* > *Configuration* 对话框。
- ☐ 要为冗余连接添加 VLAN 1 和 VLAN 成员资格标签，请在对应 T 行中两个耦合端口的单元格中输入值 VLAN 1。
- ☐ 暂时保存更改。为此，请单击 按钮。

耦合设备在 VLAN 1 上以最高优先级发送冗余数据包。

具有控制线路的双交换机耦合，待机设备

以下设置适用于所选图形中以蓝色显示的设备。

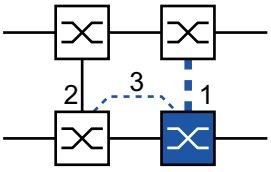


图 63: 双交换机耦合，待机设备
1：耦合端口
2：伙伴机耦合端口
3：控制线路

请执行以下步骤：

- ☐ 打开 *Switching* > *L2-Redundancy* > *Ring/Network Coupling* 对话框。
- ☐ 在 *Mode* 框的 *Type* 选项列表中，选择 *two-switch coupling with control line, slave* 单选按钮。
- ☐ 在 *Coupling port* 框中，在 *Port* 下拉列表中选择要在其上连接网段的端口。
  配置不同端口上的 *Coupling port* 和环网端口。
- ☐ 在 *Control port* 框中，在 *Port* 下拉列表中选择要在其上连接控制线路的端口。
  配置不同端口上的 *Coupling port* 和环网端口。
- ☐ 要启用该功能，请选择 *Operation* 框中的 *On* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 按钮。
- ☐ 将冗余线路连接到耦合端口。
  在 *Coupling port* 框中，*State* 字段会显示耦合端口的状态。
  当伙伴机在网络中已经工作时，*Partner coupling port* 框中的 *IP address* 字段会显示伙伴机端口的 IP 地址。
- ☐ 将控制线路连接到控制端口。
  在 *Control port* 框中，*State* 字段会显示控制端口的状态。
  当伙伴机在网络中已经工作时，*Partner coupling port* 框中的 *IP address* 字段会显示伙伴机端口的 IP 地址。

在 *Information* 框中，*Redundancy available* 字段会显示冗余是否可用。*Configuration failure* 字段会显示设置是否已完成以及是否正确。

提示：如果在同一个设备上操作 *Ring manager* 功能和双交换机耦合功能，则可能会造成环路。

为了帮助防止当环网耦合端口上的连接正在工作时形成连续环路，请执行以下任一操作。设备将耦合端口的端口状态设置为“关”：

- 禁用操作
- 更改配置

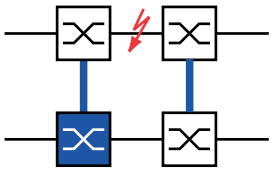
对于耦合端口，执行以下步骤：

- ☐ 打开 *Switching* > *VLAN* > *Port* 对话框。
- ☐ 将 *Port-VLAN ID* 设置更改为端口上配置的 VLAN ID 的值。
- ☐ 取消勾选两个耦合端口的 *Ingress filtering* 复选框。
- ☐ 打开 *Switching* > *VLAN* > *Configuration* 对话框。
- ☐ 要为冗余连接添加 VLAN 1 和 VLAN 成员资格标签，请在对应 T 行中两个耦合端口的单元格中输入值 VLAN 1。
- ☐ 暂时保存更改。为此，请单击 按钮。

耦合设备在 VLAN 1 上以最高优先级发送冗余数据包。

指定 *Redundancy mode* 和 *Coupling mode* 设置。为此，请执行以下步骤：

- ☐ 打开 *Switching* > *L2-Redundancy* > *Ring/Network Coupling* 对话框。
- ☐ 在 *Configuration* 框的 *Redundancy mode* 选项列表中，选择以下单选按钮之一：
  - ▶ *redundant ring/network coupling*
    使用此设置时，主线路或冗余线路已激活。该设置允许设备在两个线路之间进行切换。
  - ▶ *extended redundancy*
    使用此设置时，主线路和冗余线路同时激活。该设置允许用户向第二个网络添加冗余。当第二个网络中耦合设备之间的连接无法工作时，耦合设备将继续传输和接收数据。



    在重新配置期间，会出现数据包重复。因此，只有当您的设备检测到数据包重复时方可选择此设置。
- ☐ 在 *Configuration* 框的 *Coupling mode* 选项列表中，选择以下单选按钮之一：
  - ☐ 如果连接到环网，则请选择 *ring coupling* 单选按钮。
  - ☐ 如果连接到总线或网状结构，则请选择 *network coupling* 单选按钮。

  Coupling mode 描述了与环网相连的骨干网络的类型(参阅图 61)。
- ☐ 暂时保存更改。为此，请单击 按钮。

将耦合设置重置为默认状态。为此，请执行以下步骤：

- ☐ 点击 按钮，然后点击 *Reset* 项目。

13.13 RCP

工业应用要求用户网络具有较高的可用性。这也涉及到当某个网络设备无法工作时为通信保持确定的、较短的中断时间。

环网拓扑的特点是过渡时间短、资源使用最少。但是，环网拓扑结构也带来了将这些环网冗余耦合在一起的挑战。

冗余耦合协议 *RCP* 允许用户对使用以下任一冗余协议工作的环网进行耦合：

- MRP
- HIPER 环网
- RSTP

RCP 功能还允许用户将多个二级环网耦合到一个一级环网(参阅图 64)。只有对环网进行耦合的交换机才需要 *RCP* 功能。

用户还可使用耦合网络中除 Schneider Electric 设备以外的其他设备。

RCP 功能使用一个主设备和一个从设备在网络之间传输数据。只有主设备才会在环网之间转发帧。

使用 Schneider Electric 专有多播消息，*RCP*主设备和从设备可以互相告知各自的工作状态。将环网中不是耦合设备的设备配置为转发以下多播地址：

- 01:80:63:07:00:09
- 01:80:63:07:00:0A

将主设备和从设备作为直接相邻设备连接起来。

使用每个设备的 4 个端口创建冗余耦合。在每个网络中安装具有 2 个内部端口和 2 个外部端口的耦合设备。

- 内部端口将主设备和从设备连接在一起。
- 外部端口将这些设备连接到网络。

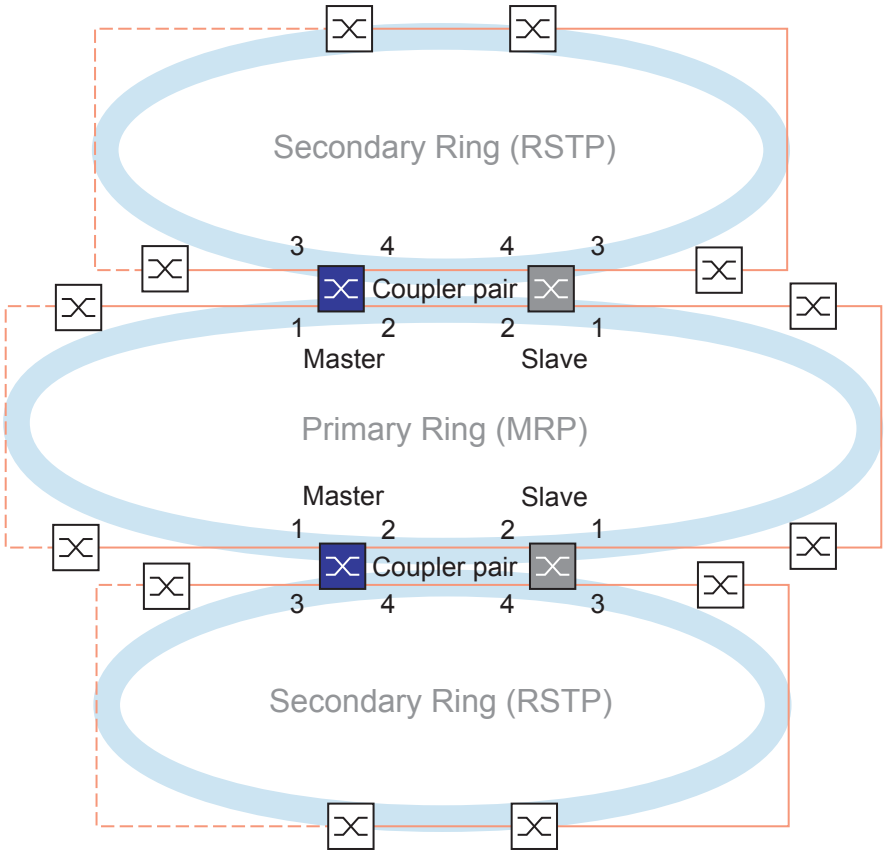


图 64: 双交换机冗余耦合示例

1: 一级环网中的外部耦合端口
2: 一级环网中的内部耦合端口
3: 二级环网中的外部耦合端口
4: 二级环网中的内部耦合端口

当角色被设置为值 *auto* 时，耦合器设备会将其角色自动选择为 *master* 或 *slave*。当您需要永久主设备或从设备时，请手动配置这些角色。

提示: single 角色只能与 *Dual RSTP* 功能一起使用。参考 “使用 Dual RSTP 功能对两个 RSTP 环网进行耦合” 页 236.

如果使用内部耦合端口不再能访问到主设备，则从设备会等待超时期限过期，然后再接替主设备角色。在指定超时期限期间，从设备会尝试使用外部耦合端口访问主设备。当仍然无法访问到主设备时，从设备将承担主设备角色。要在连接到外部耦合端口的网络中保持稳定性，请将超时期限配置为比耦合环网中恢复时间更长的时间段。

提示: 禁用未连接到 RSTP 环网的 *RCP* 冗余耦合内部和外部端口上的 RSTP。在示例配置中，禁用每个设备端口 1 和 2 上的 RSTP。

13.13.1 RCP 耦合应用示例

⚠ 警告

不允许的设备操作

为帮助避免在配置阶段出现环路，请分别配置 *RCP* 配置的每个设备。在连接冗余线路之前，应完成环网配置的其他设备的配置。

如果不遵循这些说明，则会导致死亡、重伤或设备损坏。

Schneider Electric 设备支持双交换机冗余耦合协议方式。例如，可以使用 *RCP* 功能提供一个安装在火车中的网络。该网络可为乘客提供有关列车位置或沿途不同站点的信息。例如，利用视频监控，该网络还有助于为乘客提供安全性。

图中所示一级环网代表一节车厢中的一个 *MRP* 环网。图中所示二级环网为 RSTP 环网。每个环网都包含 4 个设备(参阅图 65)。

为了简化图中的列车拓扑结构，为 *MRP* 环网端口以及 *RCP* 内部和外部端口分配了相同的端口编号。根据这些端口在网络中的功能，为其参数指定相同的值。例如，将交换机 1D 和 1C 上的端口 *1/1* 和 *1/2* 指定为 MRP 环网端口。端口 *1/4* 作为 *RCP* 内部端口，端口 *1/3* 作为 *RCP* 外部端口。

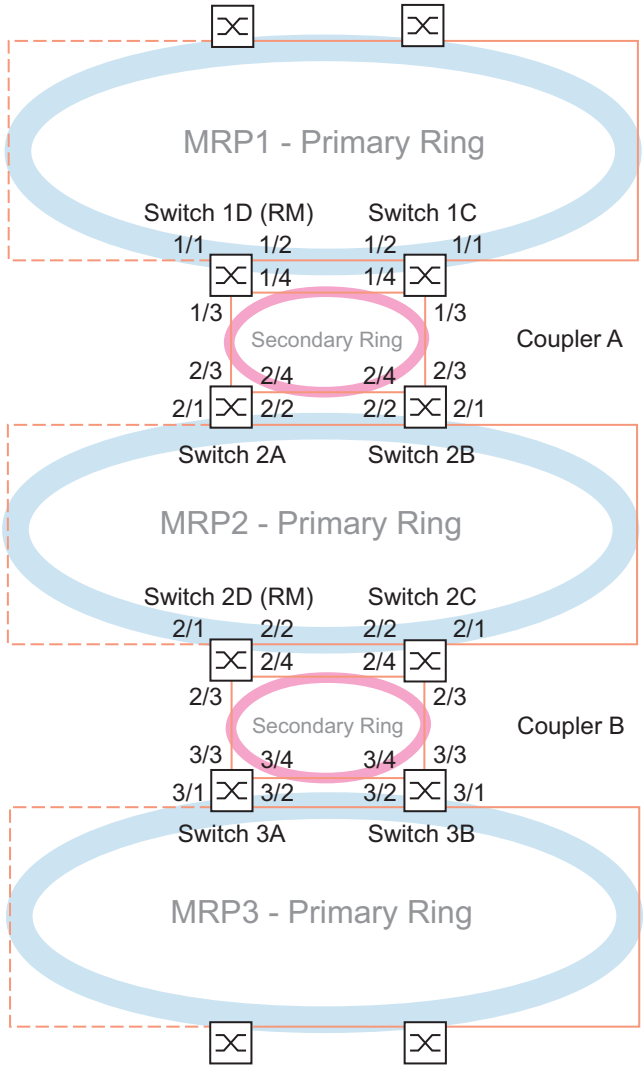


图 65: 冗余耦合协议列车拓扑结构

以下列表指定了每个设备上端口的角色。
1：端口 1 和 2 为 MRP 环网端口
2：端口 3 为 RCP 外部端口
3：端口 4 为 RCP 内部端口

以下步骤描述了如何为耦合器 A 中的交换机 1D 指定参数。以相同方式配置用于耦合器 A 的其他设备和耦合器 B 中使用的设备。

禁用 MRP 环网中的 RSTP 功能

MRP 和 RSTP 不能一起工作。因此，请停用 *MRP* 环网中使用的 *RCP* 端口上的 RSTP 功能。在示例配置中，端口 x/1 和 x/2 用于 *MRP* 环网。只激活二级环网中使用的 *RCP* 内部和外部端口上的 RSTP 功能。例如，激活端口 x/3 和 x/4 上的 RSTP 功能。

请执行以下步骤：

- ☐ 打开 *Switching* > *L2-Redundancy* > *Spanning Tree* > *Port* 对话框的 *CIST* 选项卡。
- ☐ 在默认设置下，这些端口上的 RSTP 功能已激活。要停用 *MRP* 环网端口上的 RSTP 功能，请取消勾选端口 x/1 和 x/2 的 *STP active* 复选框。
- ☐ 打开 *Switching* > *L2-Redundancy* > *Spanning Tree* > *Global* 对话框。
- ☐ 要启用该功能，请选择 *Operation* 框中的 *On* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`interface x/1`	切换到接口 x/1 的接口配置模式。
`no spanning-tree mode`	禁用端口上的 *Spanning Tree* 功能。
`exit`	切换到配置模式。
`interface x/2`	切换到接口 x/2 的接口配置模式。
`no spanning-tree mode`	禁用端口上的 *Spanning Tree* 功能。
`exit`	切换到配置模式。
`spanning-tree operation`	启用 *Spanning Tree* 功能。

指定 MRP 环网中的环网主设备

图中，每个 *MRP* 环网的交换机 D 都被指定为环网管理器(参阅图 65)。将环网中的其他交换机指定为环网客户端。

请执行以下步骤：

- ☐ 打开 *Switching* > *L2-Redundancy* > *MRP* 对话框。
- ☐ 在 *Ring port 1* 框中指定第一个环网端口。
  在 *Port* 下拉列表中，选择端口 x/1。
- ☐ 在 *Ring port 2* 框中指定第二个环网端口。
  在 *Port* 下拉列表中，选择端口 x/2。
- ☐ 要将设备指定为环网管理器，请在 *Ring manager* 框中激活该功能。
- ☐ 要启用该功能，请选择 *Operation* 框中的 *On* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`mrp domain add default-domain`	创建一个 ID 为 default-domain 的新 *MRP* 域。
`mrp domain modify port primary x/1`	将端口 x/1 指定为环网端口 1。

`mrp domain modify port secondary x/2`	将端口 x/2 指定为环网端口 2。
`mrp domain modify mode manager`	指定设备作为 *Ring manager* 进行工作。对于环网中的其他设备，将使用默认设置。
`mrp domain modify operation enable`	启用 *MRP* 功能。

指定冗余耦合器中的设备

请执行以下步骤：

- ☐ 打开 *Switching* > *L2-Redundancy* > *RCP* 对话框。
- ☐ 在 *Primary ring/network* 框中指定 *Inner port*。选择端口 x/2。
- ☐ 在 *Primary ring/network* 框中指定 *Outer port*。选择端口 x/1。
- ☐ 在 *Secondary ring/network* 框中指定 *Inner port*。选择端口 x/4。
- ☐ 在 *Secondary ring/network* 框中指定 *Outer port*。选择端口 x/3。

- ☐ 要启用该功能，请选择 *Operation* 框中的 *On* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`redundant-coupling port primary inner x/2`	将端口 x/2 指定为一级内部端口。
`redundant-coupling port primary outer x/1`	将端口 x/1 指定为一级外部端口。
`redundant-coupling port secondary inner x/4`	将端口 x/4 指定为二级内部端口。
`redundant-coupling port secondary outer x/3`	将端口 x/3 指定为二级外部端口。
`redundant-coupling operation`	启用设备中的 *RCP* 功能。
`copy config running-config nvm`	将当前设置保存到永久存储器 (nvm) 的“选定”配置概要文件中。

13.13.2 使用 Dual RSTP 功能对两个 RSTP 环网进行耦合

如果您希望对一级和二级环网使用 RSTP，则 *RCP* 功能会将二级环网的端口分配给 *Dual RSTP* 实例。这会创建通过 *RCP* 耦合的两个独立的 RSTP 网络。

在一个二级环网中可以选择最多操作 16 个 MCSESM-E 设备。这包括连接辅助环的主环的 2 个设备。当辅助环中的网络组件无法运行时， *RCP*功能通常可以获得低于 50 ms 的重新配置时间。

在一个一级环网中可以选择最多操作 16 个 MCSESM-E 设备。就这样 *RCP* 和 *Dual RSTP* 功能通常还可以在主环中获得低于 50 ms 的重新配置时间。可以将最多 8 个二级环网连接到一个一级环网。因此，可以连接最多 128 个网桥 (8 × 14 + 16)。在此网络中，您通常可以获得低于 50 ms 的端到端重新配置时间，并具有设备冗余。

当针对一级环网中的重新配置时间的要求较低时，用户拥有以下选项：
- 增加一级环网中网桥的数量。
- 将更多的二级环网连接到一级环网。

用户还可使用环网中除 MCSESM-E 以外的其他设备，但前提条件是，这些设备更新 RSTP 拓扑更改的速度要足够快。例如，当某个网络组件无法工作时。

实例的一级和二级端口的属性

对于一级或二级实例的端口，请考虑以下说明：
- 只有 *RCP* 网桥中被配置为二级环网的外部或内部环网端口的那些端口才属于 *Dual RSTP* 实例。其他端口则属于该网桥的一级实例。
- 可以选择将不运行 *Spanning Tree* 的终端设备或网络连接到一个隐式属于 *RCP* 网桥的一个一级实例的端口。
  这些拓扑既不提供设备冗余也不提供链路冗余。
- 可以选择在同一个实例的端口之间建立更多链路，从而在一级或二级环网中建立一个网状网络。
  在这些拓扑结构中，所定义的 50 毫秒的最大端到端重新配置时间不适用。

只使用一个 RCP 网桥对两个 RSTP 环网进行耦合

如果您希望只使用一个网桥对两个 RSTP 环网进行耦合，请使用 single 角色。

对于角色为 single 的 *RCP* 网桥，内部和外部端口具有相同的功能。您可以互换特定实例的内部和外部端口。

当使用一个网桥对若干环网进行连接时，可以将最多 16 个二级环网连接到一个一级环网。这也包括负责连接环网的 *RCP* 网桥。因此，可以连接最多 256 个网桥 (16 × 15 + 16)。在此网络中，借助连接冗余，可以在网络中获得 50 毫秒的最大端到端重新配置时间。

当针对一级环网中的重新配置时间的要求较低时，用户拥有以下选项：
- 增加一级环网中网桥的数量。
- 将更多的二级环网连接到一级环网。

针对 Dual RSTP 功能的拓扑选项

以下示例显示了与三个二级环网相连的一个一级环网的基本结构。二级环网 1 和 2 分别使用两个 *RCP* 网桥连接到一级环网，而二级环网 3 则使用一个 *RCP* 网桥进行连接。假设一个环网中每个连接的路径开销均相同。

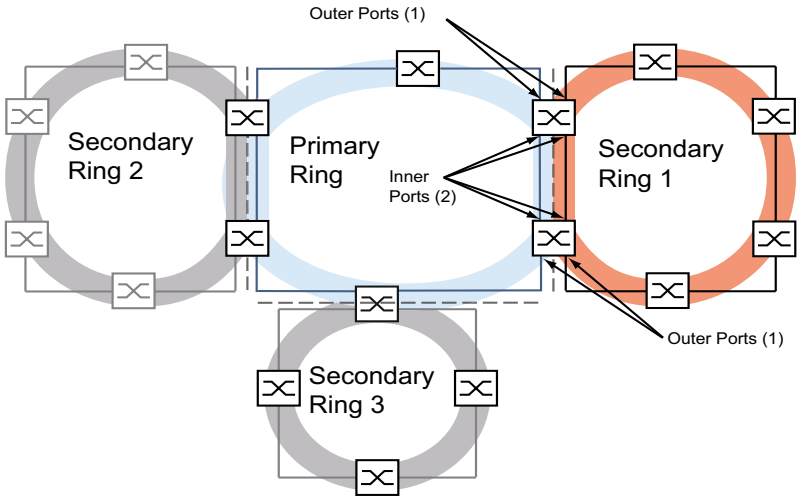


图 66: 使用 3 个辅助环连接的主环 RCP

一级环网的配置

以下章节对配置进行原理性介绍，因此不包括工作步骤。

⚠ 警告

不允许的设备操作

进行实际配置时，应采取措施帮助避免形成环路。

如果不遵循这些说明，则会导致死亡、重伤或设备损坏。

要指定一级环网中的根网桥和备用根网桥，请配置其全局 RSTP 网桥优先级。当一级环网中的根网桥和备用根网桥彼此相对时，可以在一级环网中获得最短的重新配置时间。当备用根网桥有两个路径连接到根网桥且二者分支长度之差最大为 1 时，就属于这种情况。

对一级环网中位于根网桥和备用根网桥之间的其他网桥进行配置，请确保与根网桥之间的距离越大，网桥优先级就越低（即，数字越大）。

下图通过示例显示了一级环网的 RSTP 详细信息。拓扑结构简化为一级环网和一个二级环网。在配置过程中，管理站连接到一级环网，以帮助避免与二级环网中网桥的通信出现中断。

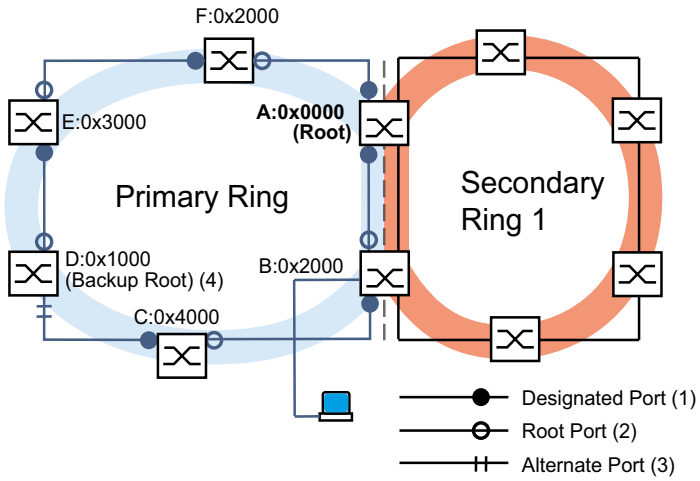


图 67: 主环与一个连接的辅助环
A..F，以及主环的详细信息：桥标识符s
0x0000..0x4000：主环网桥优先级

二级环网的配置

要指定二级环网中的根网桥和备用根网桥，请为 *Dual RSTP* 网桥配置 *RCP* 网桥优先级。对于二级环网中的其他网桥，只配置其全局 RSTP 网桥优先级。当二级环网中的根网桥和备用根网桥彼此相对时，可以在二级环网中获得最短的重新配置时间。

另请配置二级环网中的其他网桥，确保与根网桥之间的距离越大，网桥优先级就越低（即，数字越大）。

下图通过示例显示了二级环网的 RSTP 详细信息。

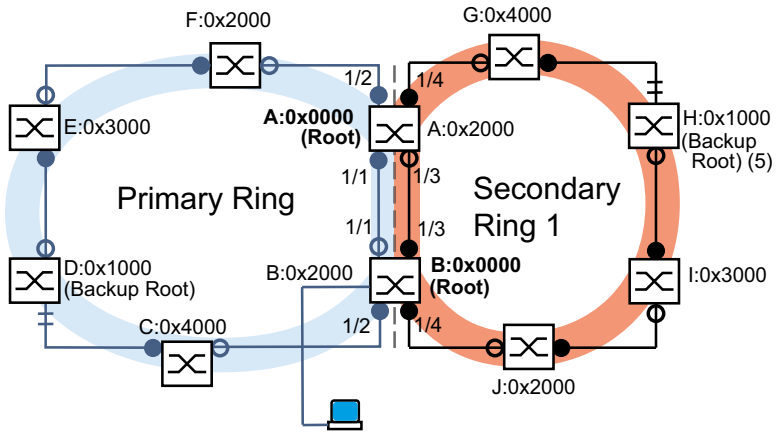


图 68: 连接一个二级环网的一级环网，并显示二级环网的详细信息
A、B、G 至 J：二级环网中的网桥标识符
0x0000..0x4000：网桥优先级
对于网桥 A 和 B：Dual RSTP 网桥优先级
对于网桥 G 到 J：全局 RSTP 网桥优先级
5：二级环网的备用根网桥

一级环网和二级环网中的根网桥角色是相互独立的。一个网桥可以是以下环网的 RSTP 根：
- 这两种环网
- 其中一种环网
- 都不是

只使用 RSTP 操作二级环网。

环网耦合配置

对于 *RCP* 网桥，为一级和二级环网定义内部和外部端口。

表格 44: RCP 网桥的环网端口

端口	RCP 主 (B)	RCP 从 (A)
一级环网		
内部端口	1/1	1/1
外部端口	1/2	1/2
二级环网		
内部端口	1/3	1/3
外部端口	1/4	1/4

之后，为每个 *RCP* 网桥配置角色。

下图显示了一个示例。

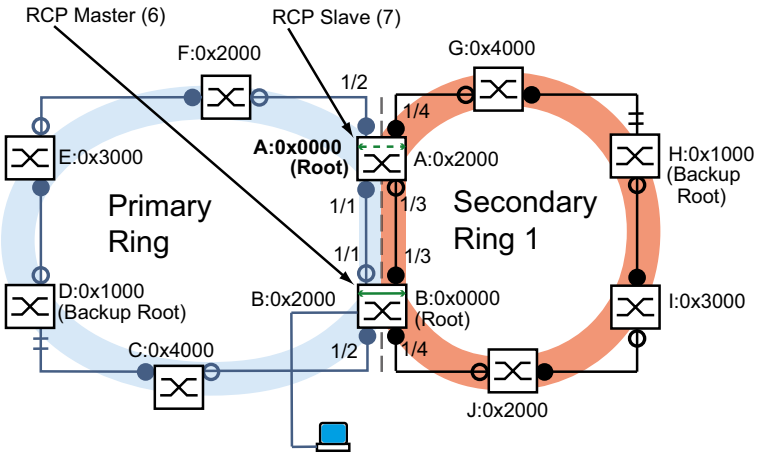


图 69: 连接一个二级环网的一级环网，并显示端口编号和 RCP 角色
6：RCP 主
7：RCP 从

根网桥角色和耦合角色是相互独立的。一个网桥可以是 *RCP* 主，同时作为以下环网的 RSTP 根进行工作：
- 这两种环网
- 其中一种环网
- 都不是

这也适用于 *RCP* 从。

之后，启用 *RCP* 功能。

13.13.3 使用 Dual RSTP 进行 RCP 耦合的应用示例

在一个生产车间中，存在多个生产单元。一个生产单元中的设备通过线形网络结构连接起来。这个网络连接到生产车间中的更高级别网络。该生产车间网络以冗余方式互连起来，并支持 RSTP。每个设备均为 MCSESM-E 类型。

您的需求：

- 为生产单元中的现有线形网络提供快速设备冗余。
- 以冗余方式将生产单元连接到生产车间网络。
- 对生产车间网络进行重新配置，以帮助提供确定的、较短的重新配置时间。

现有网络拓扑，简化到一个生产单元：

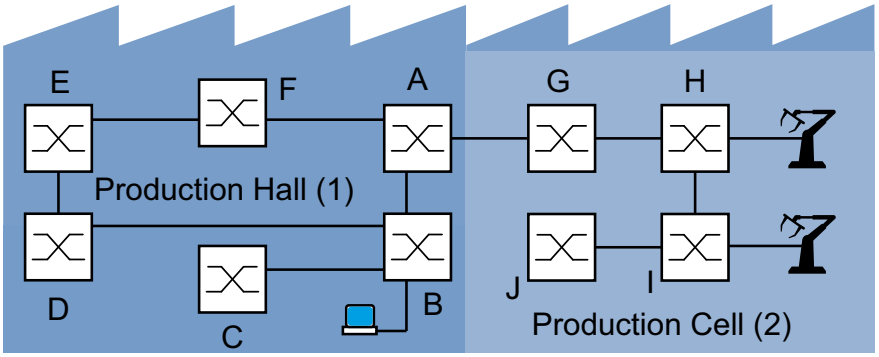


图 70: 生产车间中生产单元的示例，使用 RCP 和 Dual RSTP 功能之前的拓扑
1：生产车间
2：生产单元

所需的 *Dual RSTP* 网络拓扑：

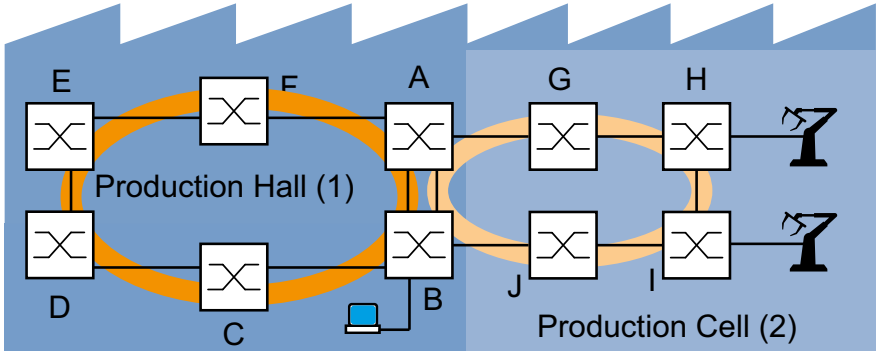


图 71: 生产车间中生产单元的示例，使用 RCP 和 Dual RSTP 功能时的拓扑
1：生产车间
2：生产单元

所需 *Dual RSTP* 网络拓扑的示意图：

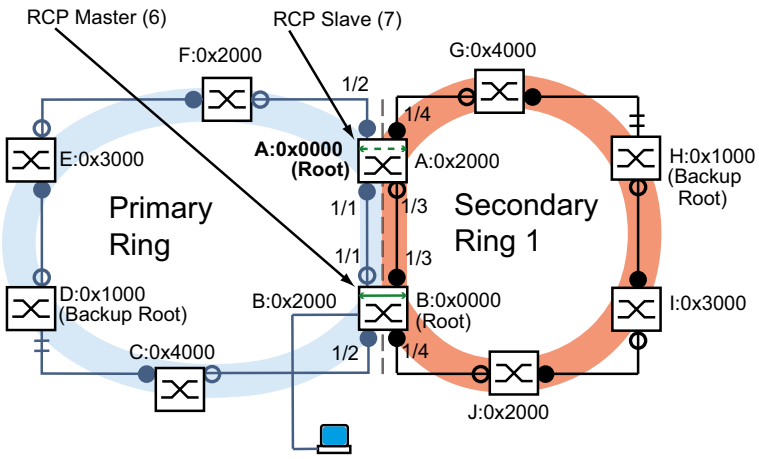


图 72: Dual RSTP 网络拓扑的示意图
6：RCP主
7：RCP从

下表显示，数量不多的设置对于新拓扑的配置已经足够了。只需在设备 A 和 B 上输入 *Dual RSTP* 设置。

表格 45: 用于 Dual RSTP 示例交换机配置的值

参数	A	B	C	D	E	F	G	H	I	J
RSTP 设置										
网桥优先级（十六进制）[1]	0x0000	0x2000	0x4000	0x1000	0x3000	0x2000	0x4000	0x1000	0x3000	0x2000
Dual RSTP 设置										
网桥优先级（十六进制）[a]	0x2000	0x0000	-	-	-	-	-	-	-	-
RCP 设置										
一级环网，内部端口	1/1	1/1	-	-	-	-	-	-	-	-
一级环网，外部端口	1/2	1/2	-	-	-	-	-	-	-	-
二级环网，内部端口	1/3	1/3	-	-	-	-	-	-	-	-
二级环网，外部端口	1/4	1/4	-	-	-	-	-	-	-	-
耦合角色	Slave	Master	-	-	-	-	-	-	-	-

1. 有关以十六进制和十进制表示法表示的网桥优先级，请参见 表格 46。

表格 46: 以十六进制和十进制表示法表示的可能的网桥优先级

网桥优先级								
十六进制	0x0000	0x1000	0x2000	0x3000	0x4000	0x5000	0x6000	0x7000
十进制	0	4096	8192	12288	16384	20480	24576	28672

表格 46: 以十六进制和十进制表示法表示的可能的网桥优先级

网桥优先级								
十六进制	0x8000	0x9000	0xA000	0xB000	0xC000	0xD000	0xE000	0xF000
十进制	32768	36864	40960	45056	49152	53248	57344	61440

进一步配置的前提条件：
- 二级环网中旧的拓扑结构下网桥 B 和 D 之间现有互连的连接已停用。例如，进行此操作的方法可以是，手动停用网桥 B 和 D 上的相应端口或拔下链路插头。
- 网桥 C 和 D 之间以及网桥 J 和 B 之间的连接已停用。例如，进行此操作的方法可以是，在插入链路插头之前手动停用网桥上的相应端口。
- 网桥 A 和 B 之间二级环网的连接已停用。
- 每个设备上的 RSTP 均已激活，且参数处于交付状态。
- 您的管理站已连接到一级环网。
- 您已经打开了设备 A 和 B 的图形用户界面或命令行界面。
- 您能够访问设备 C 至 J 的用户界面。

⚠ 警告

环路危险
- 分别配置 *RCP* 和 *Dual RSTP* 配置的每个设备。在连接冗余线路之前，应完成环网配置的其他设备的配置。
- 将 *RCP* 耦合配置中的超时配置为长于针对冗余协议的更快速实例的最长假设中断时间。
- 在一个具有两个耦合网桥的拓扑中，将两个设备的耦合角色只配置为 *master*、*slave* 或 *auto*。
- 只通过 1 个 *RCP* 网桥（对于具有 1 个 *RCP* 网桥的拓扑）或通过 2 个 *RCP* 网桥（对于具有 2 个 *RCP* 网桥的拓扑）对主实例和辅助实例进行耦合。将主实例的端口与每个辅助实例的端口分开。
- 只在有终端设备连接到端口的情况下激活端口上的 *Admin edge port* 设置。

如果不遵循这些说明，则会导致死亡、重伤或设备损坏。

配置 RCP 网桥的全局 RSTP 参数

根据 表格 45 中的任务说明，您需要网桥 A 和 B 的 RSTP 网桥优先级。下表包含了这些值的汇总。

表格 47: 网桥 A 和 B 的 RSTP 网桥优先级

RSTP 参数	A	B
网桥优先级（十六进制）	0x0000	0x2000
网桥优先级（十进制）	0	8192

提示：以下说明详细描述了 *RCP* 网桥（A 和 B）的配置；对于其他网桥（C 至 J）的配置仅作简要描述。

配置设备 A。为此，请执行以下步骤：

- ☐ 打开 *Switching > L2-Redundancy > Spanning Tree > Global* 对话框。
- ☐ 在 *Bridge configuration* 框中，选择 *Priority* 下拉列表中的值 0。
- ☐ 暂时保存更改。为此，请单击 ✓ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`spanning-tree mst priority 0 0`	将 MST 实例 0 的 RSTP 网桥优先级设置为值 0。MST 实例 0 为全局 MST 实例或默认实例。

配置设备 B。为此，请执行以下步骤：

- ☐ 打开 *Switching > L2-Redundancy > Spanning Tree > Global* 对话框。
- ☐ 在 *Bridge configuration* 框中，选择 *Priority* 下拉列表中的值 8192。
- ☐ 暂时保存更改。为此，请单击 ✓ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`spanning-tree mst priority 0 8192`	将全局 MST 实例的 RSTP 网桥优先级设置为值 8192。

配置其他网桥的全局 RSTP 参数

现在配置其他网桥。根据任务说明，您需要 RSTP 网桥优先级。下表包含了这些值的汇总。

表格 48: 网桥 C 至 J 的 RSTP 网桥优先级

RSTP 参数	C	D	E	F	G	H	I	J
网桥优先级（十六进制）	0x4000	0x1000	0x3000	0x2000	0x4000	0x1000	0x3000	0x2000
网桥优先级（十进制）	16384	4096	12288	8192	16384	4096	12288	8192

请执行以下步骤：

- ☐ 将设备 C 的 RSTP 网桥优先级设置为 16384 (0x4000) 并激活设置。
- ☐ 将设备 D 的 RSTP 网桥优先级设置为 4096 (0x1000) 并激活设置。
- ☐ 将设备 E 的 RSTP 网桥优先级设置为 12288 (0x3000) 并激活设置。
- ☐ 将设备 F 的 RSTP 网桥优先级设置为 8192 (0x2000) 并激活设置。
- ☐ 将设备 G 的 RSTP 网桥优先级设置为 16384 (0x4000) 并激活设置。
- ☐ 将设备 H 的 RSTP 网桥优先级设置为 4096 (0x1000) 并激活设置。
- ☐ 将设备 I 的 RSTP 网桥优先级设置为 12288 (0x3000) 并激活设置。
- ☐ 将设备 J 的 RSTP 网桥优先级设置为 8192 (0x2000) 并激活设置。

配置 Dual RSTP 网桥的 RCP 参数

根据任务说明，您需要网桥 A 和 B.的具体 *Dual RSTP* 参数。这些参数为 *Dual RSTP* 网桥优先级、环网端口和耦合角色。下表包含了这些值的汇总。

表格 49: 网桥 A 和 B 的 Dual RSTP 参数

Dual RSTP 参数	A	B
Dual RSTP 网桥优先级（十六进制）	0x2000	0x0000
Dual RSTP 网桥优先级（十进制）	8192	0

表格 50: 网桥 A 和 B 的 RCP 参数

Dual RSTP 参数	A	B
一级环网，内部端口	1/1	1/1
一级环网，外部端口	1/2	1/2
二级环网，内部端口	1/3	1/3
二级环网，外部端口	1/4	1/4
耦合角色	Slave	Master

配置设备 A。为此，请执行以下步骤：

- ☐ 打开 *Switching > L2-Redundancy > FuseNet > RCP* 对话框。
- ☐ 在 *Primary ring/network* 框中，选择 *Inner port* 下拉列表中的值 1/1。
- ☐ 在 *Primary ring/network* 框中，选择 *Outer port* 下拉列表中的值 1/2。
- ☐ 在 *Secondary ring/network* 框中，选择 *Inner port* 下拉列表中的值 1/3。
- ☐ 在 *Secondary ring/network* 框中，选择 *Outer port* 下拉列表中的值 1/4。
- ☐ 在 *Coupler configuration* 框中，选择 *Role* 下拉列表中的值 *slave*。
- ☐ 要启用该功能，请选择 *Operation* 框中的 *On* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。
- ☐ 打开 *Switching > L2-Redundancy > Spanning Tree > Dual RSTP* 对话框。
- ☐ 在 *Bridge configuration* 框中，选择 *Priority* 下拉列表中的值 8192。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`spanning-tree drstp mst priority 0 8192`	将 *Dual RSTP* 实例的 RSTP 网桥优先级设置为值 8192。
`redundant-coupling port primary inner 1/1`	选择端口 *1/1* 作为 *RCP* 一级环网的内部端口。
`redundant-coupling port primary outer 1/2`	选择端口 *1/2* 作为 *RCP* 一级环网的外部端口。
`redundant-coupling port secondary inner 1/3`	选择端口 *1/3* 作为 *RCP* 二级环网的内部端口。
`redundant-coupling port secondary outer 1/4`	选择端口 *1/4* 作为 *RCP* 二级环网的外部端口。
`redundant-coupling role slave`	将此设备配置为 *RCP* 从。
`exit`	切换到特权执行模式。

配置设备 B。为此，请执行以下步骤：

- ☐ 打开 *Switching* > *L2-Redundancy* > *FuseNet* > *RCP* 对话框。
- ☐ 在 *Primary ring/network* 框中，选择 *Inner port* 下拉列表中的值 1/1。
- ☐ 在 *Primary ring/network* 框中，选择 *Outer port* 下拉列表中的值 1/2。
- ☐ 在 *Secondary ring/network* 框中，选择 *Inner port* 下拉列表中的值 1/3。
- ☐ 在 *Secondary ring/network* 框中，选择 *Outer port* 下拉列表中的值 1/4。
- ☐ 在 *Coupler configuration* 框中，选择 *Role* 下拉列表中的值 *master*。
- ☐ 要启用该功能，请选择 *Operation* 框中的 *On* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。
- ☐ 打开 *Switching* > *L2-Redundancy* > *Spanning Tree* > *Dual RSTP* 对话框。
- ☐ 在 *Bridge configuration* 框中，选择 *Priority* 下拉列表中的值 0。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`spanning-tree drstp mst priority 0 0`	将 *Dual RSTP* 实例的 RSTP 网桥优先级设置为值 0。
`redundant-coupling port primary inner 1/1`	选择端口 *1/1* 作为 *RCP* 一级环网的内部端口。
`redundant-coupling port primary outer 1/2`	选择端口 *1/2* 作为 *RCP* 一级环网的外部端口。
`redundant-coupling port secondary inner 1/3`	选择端口 *1/3* 作为 *RCP* 二级环网的内部端口。
`redundant-coupling port secondary outer 1/4`	选择端口 *1/4* 作为 *RCP* 二级环网的外部端口。
`redundant-coupling role master`	将此设备配置为 *RCP* 主。
`exit`	切换到特权执行模式。

检查配置

激活新的冗余连接：
- ▶ 设备 A 端口 *1/3* 与设备 B 端口 *1/3* 之间二级环网的内部端口的连接。
- ▶ 设备 G 和 H 之间二级环网的环网闭合。
- ▶ 设备 C 和 D 之间一级环网的环网闭合。

将一级环网中的当前网桥角色与必要的网桥角色进行比较：

网桥 A 应是根网桥。

请执行以下步骤：

- ☐ 打开 *Switching* > *L2-Redundancy* > *Spanning Tree* > *Global* 对话框。
- ☐ 在 *Topology information* 框中，勾选 *Bridge is root* 复选框的设置。

```
show spanning-tree global

Spanning Tree Information:
--------------------------
Spanning Tree Mode.....................RSTP
Spanning Tree Trap Mode.....................enabled
Bridge is root.............................true
...
```

将您配置为一级和二级环网中的内部和外部端口的四个端口与表格 45 中的规格进行比较。

请执行以下步骤：

- 打开 *Switching > L2-Redundancy > FuseNet > RCP* 对话框。
- 在 *Primary ring/network* 和 *Secondary ring/network* 框中，勾选显示的端口。

```
show redundant-coupling global

Redundant coupling protocol global settings
-------------------------------------------
RCP global state.........................enabled
RCP device configured role..................slave
RCP inner primary interface.................1/1
RCP outer primary interface.................1/2
RCP inner secondary interface...............1/3
RCP outer secondary interface...............1/4
RCP timeout.................................45 milliseconds
```

将辅助环中的当前网桥角色与必要的网桥角色进行比较。网桥 B 应是根网桥。

请执行以下步骤：

- 打开 *Switching > L2-Redundancy > Spanning Tree > Dual RSTP* 对话框。
- 在 *Topology information* 框中，勾选 *Bridge is root* 复选框的设置。

```
show spanning-tree drstp

Dual Spanning Tree Information:
-------------------------------
Spanning Tree Mode.....................RSTP
Spanning Tree Trap Mode.....................enabled
Bridge is root.............................true
...
```

将一级环网中网桥的当前端口角色与必要的端口角色进行比较：

- 对于桥 D 通向桥 C 的端口：
  角色*alternate*。
- 对于网桥中指向根网桥 A 方向的其他端口，选择角色：
  角色*root*。
- 对于网桥中指向备用根网桥 D 方向的其他端口，选择角色。
  角色*designated*。

请执行以下步骤：

- ☐ 打开 *Switching* > *L2-Redundancy* > *Spanning Tree* > *Port* 对话框。
- ☐ 如上所述，在 *Port role* 列中，选择值 *alternate*、*root* 或 *designated*。

```
show spanning-tree mst port 0 1/<port>
```

将二级环网中网桥的当前端口角色与必要的端口角色进行比较：

- 对于桥 H 通向桥 G 的端口：
  角色*alternate*。
- 对于网桥中指向根网桥 B 方向的其他端口，选择角色：
  角色*root*。
- 对于网桥中指向备用根网桥 H 方向的其他端口，选择角色。
  角色*designated*。

请执行以下步骤：

- ☐ 打开 *Switching* > *L2-Redundancy* > *Spanning Tree* > *Port* 对话框。
- ☐ 如上所述，在 *Port role* 列中，选择值 *alternate*、*root* 或 *designated*。

```
show spanning-tree mst port 0 1/<port>
```

如果要么 *RCP* 或者 *Spanning Tree* 功能被禁用，然后设备自动禁用 *Dual RSTP* 功能。

检查状态 *Dual RSTP* 功能。

请执行以下步骤：

- ☐ 打开 *Switching* > *L2-Redundancy* > *Spanning Tree* > *Dual RSTP* 对话框。
  在 *Operation* 帧 *Off* 单选按钮被选中。

```
show redundant-coupling status

Redundant coupling protocol status
------------------------------------------
RCP global state.........................forwarding
RCP device actual role...................disabled
Redundancy state availability............redNotAvailable
Primary ring protocol....................NONE
Secondary ring protocol..................NONE
```

结束配置

对于设备 A 至 J，将设置保存到永久存储器中。请遵循“保存配置概要文件” 页 93一节中的说明。

14 运行诊断

设备为用户提供以下诊断工具：
- 发送 SNMP 陷阱
- 监控设备状态
- 使用信号触点发送带外信号
- 端口状态指示
- 端口级别的事件计数器
- 检测不匹配的双工模式
- Auto-Disable
- 显示 SFP 状态
- 拓扑识别
- 检测 IP 地址冲突
- 检测环路
- 帮助防止发生第二层网络环路
- 报告
- 监控端口上的数据流量（端口镜像）
- 系统日志
- 事件日志
- 自检期间的原因和行动管理

14.1 发送 SNMP 陷阱

设备立即向网络管理站报告正常运行期间发生的异常事件。这是通过绕过轮询过程的称为 SNMP 陷阱的消息实现的。（“轮询”指的是定期查询数据站）。SNMP 陷阱允许用户对异常事件快速做出反应。

此类事件的例子包括：
- 硬件复位
- 对配置的更改
- 端口的分片

设备向不同主机发送 SNMP 陷阱，以提高消息的传输可靠性。未经确认的 SNMP 陷阱消息由一个包含关于异常事件的信息的数据包组成。

设备向在陷阱目标表中输入的主机发送 SNMP 陷阱。设备允许用户通过使用 SNMP 的网络管理站对陷阱目标表进行配置。

14.1.1 SNMP 陷阱的列表

下表显示了设备发送的可能的 SNMP 陷阱。

表格 51: 可能的 SNMP 陷阱

SNMP 陷阱的名称	含义
authenticationFailure	当一个站试图在未经授权的情况下访问代理时，会发送此陷阱。
coldStart	重新启动之后发送。
sa2DevMonSenseExtNvmRemoval	当移除了外部存储器时，会发送此陷阱。
linkDown	当至端口的连接中断时，会发送此陷阱。
linkUp	当建立了至端口的连接时，会发送此陷阱。
sa2DevMonSensePSState	当电源单元的状态改变时，会发送此陷阱。
sa2SigConStateChange	当信号触点的状态在运行监控过程中发生变化时，会发送此陷阱。
newRoot	当发送代理成为生成树新的根时，会发送此陷阱。
topologyChange	当端口从 blocking 变为 forwarding 或从 forwarding 变为 blocking 时，会发送此陷阱。
alarmRisingThreshold	当 RMON 输入超过其阈值上限时，会发送此陷阱。
alarmFallingThreshold	当 RMON 输入低于其阈值下限时，会发送此陷阱。
sa2AgentPortSecurityViolation	当在此端口上检测到的 MAC 地址与参数 sa2AgentPortSecurityEntry 的当前设置不匹配时，会发送此陷阱。
sa2DiagSelftestActionTrap	当根据配置的设置对“任务”、“资源”、“软件”和“硬件”这四个类别进行自检时，会发送此陷阱。
sa2MrpReconfig	当 MRP 环网的配置发生改变时，会发送此陷阱。
sa2DiagIfaceUtilizationTrap	当接口的阈值超过指定的阈值上限或低于指定的阈值下限时，会发送此陷阱。
sa2LogAuditStartNextSector	当审计跟踪在完成一个扇区之后开始一个新的扇区时，会发送此陷阱。
sa2PtpSynchronizationChance	当 PTP 同步的状态已更改时，会发送此陷阱。
sa2ConfigurationSavedTrap	在设备成功地在本地保存了配置之后，会发送此陷阱。
sa2ConfigurationChangedTrap	当您在本地保存设备的配置之后首次对其进行更改时，会发送此陷阱。
sa2PlatformStpInstanceLoopInconsistentStartTrap	当此 STP 实例中的端口切换到“loop inconsistent”状态时，会发送此陷阱。
sa2PlatformStpInstanceLoopInconsistentEndTrap	当此 STP 实例中的端口在接收 BPDU 数据包之后离开“loop inconsistent”状态时，会发送此陷阱。

14.1.2 用于配置活动的 SNMP 陷阱

将一个配置保存到存储器中之后，设备会发送一个 sa2ConfigurationSavedTrap。此 SNMP 陷阱同时包含指示正在运行的配置与永久存储器和外部存储器是否同步的永久存储器 (*ENVM*) 和外部存储器 (*NVM*) 的状态变量。也可通过将一个配置文件复制到设备，替换掉活动的已保存配置来触发此 SNMP 陷阱。

此外，设备会发送一个 sa2ConfigurationChangedTrap，表示正在运行的配置与已保存的配置之间不匹配。

14.1.3 SNMP 陷阱设置

设备允许用户发送 SNMP 陷阱作为对特定事件的响应。创建至少一个接收 SNMP 陷阱的陷阱目标。

请执行以下步骤：

- ☐ 打开 *Diagnostics > Status Configuration > Alarms (Traps)* 对话框。
- ☐ 点击  按钮。
  该对话框显示 *Create* 窗口。
- ☐ 在 *Name* 框中，指定设备用以将自己标识为 SNMP 陷阱的源的名称。
- ☐ 在 *Address* 框中，指定设备向其发送 SNMP 陷阱的陷阱目标的 IP 地址。
- ☐ 在 *Active* 列，选择设备在发送 SNMP 陷阱时考虑的条目。
- ☐ 暂时保存更改。为此，请单击  按钮。

例如，在以下对话框中，可以指定设备何时触发 SNMP 陷阱：

- *Basic Settings > Port* 对话框
- *Basic Settings > Power over Ethernet > Global* 对话框
- *Network Security > Port Security* 对话框
- *Switching > L2-Redundancy > Link Aggregation* 对话框
- *Diagnostics > Status Configuration > Device Status* 对话框
- *Diagnostics > Status Configuration > Security Status* 对话框
- *Diagnostics > Status Configuration > Signal Contact* 对话框
- *Diagnostics > Status Configuration > MAC Notification* 对话框
- *Diagnostics > System > IP Address Conflict Detection* 对话框
- *Diagnostics > System > Selftest* 对话框
- *Diagnostics > Ports > Port Monitor* 对话框
- *Advanced > Digital IO Module* 对话框

14.1.4 ICMP 消息收发

设备允许用户使用互联网控制消息协议 (ICMP) 来执行 ping 和 trace route 等诊断应用程序。设备还使用 ICMP 来发送设备在其中将 ICMP 消息转发回数据包源设备的生存时间和丢弃等消息。

使用 ping 网络工具对指向 IP 网络上特定主机的路径进行测试。traceroute 诊断工具会显示数据包在网络上的路径和传输延迟。

14.2 监控设备状态

设备状态提供了设备整体状况的概览。很多过程可视化系统都会记录设备的设备状态，以便以图形形式呈现设备的状况。

设备在 *Device status* 框中将其当前状态显示为 *error* 或 *ok*。设备根据各个监控结果确定这种状态。

设备允许用户：
- 使用信号触点发送带外信号
- 通过发送 SNMP 陷阱显示更改后的设备状态
- 在图形用户界面的 *Basic Settings* > *System* 对话框中检测设备状态
- 在命令行界面中查询设备状态

Diagnostics > *Status Configuration* > *Device Status* 对话框的 *Global* 选项卡允许用户将设备配置为在发生以下事件时向管理站发送一个陷阱：
- 供电电压错误
  - 两个供电电压中至少有一个不工作
  - 内部供电电压不工作
- 当设备在用户定义的温度阈值以外工作时
- 冗余丧失（在环网管理器模式下）
- 链路连接中断
  请为此功能配置至少一个端口。当链路中断时，可以在 *Diagnostics* > *Status Configuration* > *Device Status* 对话框 *Port* 选项卡的 *Propagate connection error* 行中指定设备向哪些端口发送信号。
- 外部存储器被移除。
  外部存储器中的配置与设备中的配置不同步。

选择相应条目，以决定设备状态包含哪些事件。

提示：使用非冗余电压电源时，设备会报告没有供电电压。要禁用此消息，请同时通过两个输入馈送供电电压或忽略监控。

14.2.1 可以监控的事件

表格 52: Device Status 事件

名称	含义
Temperature	在温度超过或低于指定值的情况下进行监控。
Ring redundancy	当存在环网冗余时，请启用此功能。
Connection errors	启用此功能，对其中 *Propagate connection error* 复选框已激活的每个端口链路事件进行监控。
External memory removal	启用此功能，对有无外部存储设备进行监控。
External memory not in sync	设备会监控设备配置和存储在外部存储器（*ENVM*）中的配置之间的同步。
Power supply	启用此功能，对电源进行监控。

14.2.2 配置设备状态

请执行以下步骤：

- ☐ 打开 *Diagnostics > Status Configuration > Device Status* 对话框的 *Global* 选项卡。
- ☐ 对于要监控的参数，请勾选 *Monitor* 列中的复选框。
- ☐ 要向管理站发送 SNMP 陷阱，请激活 *Traps* 框中的 *Send trap* 功能。
- ☐ 在 *Diagnostics > Status Configuration > Alarms (Traps)* 对话框中，创建至少一个接收 SNMP 陷阱的陷阱目标。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。
- ☐ 打开 *Basic Settings > System* 对话框。
- ☐ 要对温度进行监控，可在 *System data* 框的底部指定温度阈值。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`device-status trap`	当设备状态发生改变时，发送一个 SNMP 陷阱。
`device-status monitor envm-not-in-sync`	对设备和外部存储器中的配置概要文件进行监控。 在以下情况下，*Device status* 会变为 *error*： • 配置概要文件只存在于设备中。 • 设备中的配置概要文件与外部存储器中的配置概要文件不同。
`device-status monitor envm-removal`	对活动的外部存储器进行监控。从设备中删除活动的外部存储器时，*Device status* 框中的值会变为 *error*。
`device-status monitor power-supply 1`	对电源单元 1 进行监控。设备检测到电源故障时，*Device status* 框中的值会变为 *error*。
`device-status monitor ring-redundancy`	对环网冗余进行监控。 在以下情况下，*Device status* 会变为 *error*： • 冗余功能变为活动状态（冗余储备丧失）。 • 设备是一个普通的环网参与者，并检测到其设置中的错误。
`device-status monitor temperature`	对设备中的温度进行监控。当温度高于或低于指定限度时，*Device status* 框中的值会变为 *error*。

为了启用设备以便对没有连接的活动链路进行监控，请首先启用全局功能，然后启用各个端口。

请执行以下步骤：

- ☐ 打开 *Diagnostics > Status Configuration > Device Status* 对话框的 *Global* 选项卡。
- ☐ 对于 *Connection errors* 参数，请勾选 *Monitor* 列中的复选框。
- ☐ 打开 *Diagnostics > Status Configuration > Device Status* 对话框的 *Port* 选项卡。
- ☐ 对于 *Propagate connection error* 参数，请勾选要监控的端口的列中的复选框。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`device-status monitor link-failure`	对端口/接口链路进行监控。当被监控的端口/接口上发生链路中断时，*Device status* 框中的值会变为 *error*。
`interface 1/1`	切换到接口 1/1 的接口配置模式。
`device-status link-alarm`	对端口/接口链路进行监控。当端口/接口上发生链路中断时，*Device status* 框中的值会变为 *error*。

提示：以上命令会激活针对支持的组件的监控和捕获。当您想要激活或停用针对单个组件的监控时，可在“命令行界面”参考手册或命令行界面控制台帮助中找到相应语法。要显示命令行界面中的帮助，请输入一个问号（?）并按下 <Enter> 键。

14.2.3 显示设备状态

请执行以下步骤：

□ 打开 *Basic Settings* > *System* 对话框。

`show device-status all`	在执行特权模式下：显示设备状态和用于确定设备状态的设置。

14.3 安全状态

安全状态提供了设备整体安全的概览。很多进程都能记录设备的安全状态，然后以图形形式呈现设备状况，从而帮助实现系统可视化。设备在 *Basic Settings > System* 对话框的 *Security status* 框中显示整体安全状态。

在 *Diagnostics > Status Configuration > Security Status* 对话框的 *Global* 选项卡中，设备在 *Security status* 框中将其当前状态显示为 *error* 或 *ok*。设备根据各个监控结果确定这种状态。

设备允许用户：
- 使用信号触点发送带外信号
- 通过发送 SNMP 陷阱显示更改后的安全状态
- 在图形用户界面的 *Basic Settings > System* 对话框中检测安全状态
- 在命令行界面中查询安全状态

14.3.1 可以监控的事件

请执行以下步骤：
- ☐ 指定设备监控的事件。
- ☐ 对于相应参数，请勾选 *Monitor* 列中的复选框。

表格 53: Security Status 事件

名称	含义
Password default settings unchanged	安装后更改密码以提高安全性。当活动密码和默认密码保持不变时，设备会显示一个警报。
Min. password length < 8	创建长度超过 8 个字符的密码以保持较高的安全状态。激活时，设备会对 *Min. password length* 设置进行监控。
Password policy settings deactivated	设备根据密码策略要求对位于 *Device Security > User Management* 对话框中的设置进行监控。
User account password policy check deactivated	设备对 *Policy check* 复选框的设置进行监控。当 *Policy check* 停用时，设备会发送一个 SNMP 陷阱。
Telnet server active	设备对用户何时启用 *Telnet* 功能进行监控。
HTTP server active	设备对用户何时启用 *HTTP* 功能进行监控。
SNMP unencrypted	设备对用户何时启用 *SNMPv1* 或 *SNMPv2* 功能进行监控。
Access to system monitor with serial interface possible	设备对系统监控器状态进行监控。
Saving the configuration profile on the external memory possible	设备对将配置保存到外部永久存储器的可能性进行监控。
Link interrupted on enabled device ports	设备对活动端口的链路状态进行监控。
Access with Ethernet Switch Configurator possible	设备对用户何时启用 Ethernet Switch Configurator 读/写访问功能进行监控。
Load unencrypted config from external memory	设备对用于从外部 NVM 加载配置的安全设置进行监控。
IEC61850-MMS active	设备对 IEC 61850-MMS 协议激活设置进行监控。
Modbus TCP active	设备对 Modbus TCP/IP 协议激活设置进行监控。
Self-signed HTTPS certificate present	设备针对自我创建的数字证书对 HTTPS 服务器进行监控。

14.3.2 配置安全状态

请执行以下步骤：

- ☐ 打开 *Diagnostics > Status Configuration > Security Status* 对话框的 *Global* 选项卡。
- ☐ 对于要监控的参数，请勾选 *Monitor* 列中的复选框。
- ☐ 要向管理站发送 SNMP 陷阱，请激活 *Traps* 框中的 *Send trap* 功能。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。
- ☐ 在 *Diagnostics > Status Configuration > Alarms (Traps)* 对话框中，创建至少一个接收 SNMP 陷阱的陷阱目标。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`security-status monitor pwd-change`	对本地设置的用户帐户 user 和 admin的密码进行监控。当 user 或 admin 用户帐户的密码为默认设置时，*Security status* 框中的值会变为 *error*。
`security-status monitor pwd-min-length`	对 *Min. password length* 策略中指定的值进行监控。当 *Min. password length* 策略的值小于 8 时，*Security status* 框中的值会变为 *error*。
`security-status monitor pwd-policy-config`	对密码策略设置进行监控。 当以下至少一个策略的值被指定为 0 时，*Security status* 框中的值会变为 *error*。 • *Upper-case characters (min.)* • *Lower-case characters (min.)* • *Digits (min.)* • *Special characters (min.)*
`security-status monitor pwd-policy-inactive`	对密码策略设置进行监控。当以下至少一个策略的值被指定为 0 时，*Security status* 框中的值会变为 *error*。
`security-status monitor telnet-enabled`	对 Telnet 服务器进行监控。当您启用 Telnet 服务器时，*Security status* 框中的值会变为 *error*。
`security-status monitor http-enabled`	对 HTTP 服务器进行监控。当您启用 HTTP 服务器时，*Security status* 框中的值会变为 *error*。
`security-status monitor snmp-unsecure`	对 SNMP 服务器进行监控。 当以下至少一个条件适用时，*Security status* 框中的值会变为 *error*。 • *SNMPv1* 功能已启用。 • *SNMPv2* 功能已启用。 • SNMPv3 加密已禁用。 可在 *Device Security > User Management* 对话框的 *SNMP encryption type* 字段中启用加密。
`security-status monitor sysmon-enabled`	监控设备中 System Monitor 功能的激活。
`security-status monitor extnvm-upd-enabled`	监控外部永久存储器更新的激活。
`security-status monitor iec61850-mms-enabled`	监控 *IEC61850-MMS* 功能。当您启用 *IEC61850-MMS* 功能时，*Security status* 框中的值会变为 *error*。
`security-status trap`	当设备状态发生改变时，设备会发送一个 SNMP 陷阱。

为了启用设备以便对没有连接的活动链路进行监控，请首先启用全局功能，然后启用各个端口。

请执行以下步骤：

- ☐ 打开 *Diagnostics > Status Configuration > Security Status* 对话框的 *Global* 选项卡。
- ☐ 对于 *Link interrupted on enabled device ports* 参数，请勾选 *Monitor* 列中的复选框。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。
- ☐ 打开 *Diagnostics > Status Configuration > Device Status* 对话框的 *Port* 选项卡。
- ☐ 对于 *Link interrupted on enabled device ports* 参数，请勾选要监控的端口的列中的复选框。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`security-status monitor no-link-enabled`	对活动端口上的链路进行监控。当活动端口上发生链路中断时，*Security status* 框中的值会变为 *error*。
`interface 1/1`	切换到接口 1/1 的接口配置模式。
`security-status monitor no-link`	对接口/端口 1 上的链路进行监控。

14.3.3 显示安全状态

请执行以下步骤：

- ☐ 打开 *Basic Settings > System* 对话框。

`show security-status all`	在执行特权模式下，显示安全状态和用于确定安全状态的设置。

14.4 发送带外信号

设备使用信号触点控制外部设备和监控设备功能。功能监控可用于执行远程诊断。

设备针对所选模式在无电位信号触点（中继触点、闭合电路）中使用一个中断，以此报告工作状态。设备对以下功能进行监控：

- 供电电压错误
  - 两个供电电压中至少有一个不工作
  - 内部供电电压不工作
- 当设备在用户定义的温度阈值以外工作时
- 环网冗余事件
  冗余丧失（在环网管理器模式下）
  在默认设置下，环网冗余监控为停用。设备是一个普通的环网参与者并检测到本地设置中的错误。
- 链路连接中断
  请为此功能配置至少一个端口。在 *Propagate connection error* 框中，可以指定设备向哪些端口发送链路中断信号。在默认设置下，链路监控为停用。
- 外部存储器被移除。
  外部存储器中的配置与设备中的配置不匹配。

选择相应条目，以决定设备状态包含哪些事件。

提示：使用非冗余电压电源时，设备会报告没有供电电压。要禁用此消息，请同时通过两个输入馈送供电电压或忽略监控。

14.4.1 控制信号触点

使用 *Manual setting* 模式，可以远程控制此信号触点。

应用选项：

- 模拟在 SPS 错误监控期间检测到的错误
- 使用 SNMP 对设备进行远程控制，例如开启摄像头

请执行以下步骤：

- ☐ 打开 *Diagnostics* > *Status Configuration* > *Signal Contact* 对话框的 *Global* 选项卡。
- ☐ 要手动控制信号触点，请在 *Configuration* 框中的 *Mode* 下拉列表中选择 *Manual setting* 项目。
- ☐ 要打开信号触点，请选择 *Configuration* 框中的 *open* 单选按钮。
- ☐ 要关闭信号触点，请选择 *Configuration* 框中的 *close* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`signal-contact 1 mode manual`	为信号触点 1 选择手动设置模式。
`signal-contact 1 state open`	打开信号触点 1。
`signal-contact 1 state closed`	关闭信号触点 1。

14.4.2 监控设备和安全状态

在 *Configuration* 字段中，可以指定信号触点指示哪些事件。

- *Device status*
  使用此设置，信号触点可以指示在 *Diagnostics > Status Configuration > Device Status* 对话框中监控的参数的状态。
- *Security status*
  使用此设置，信号触点可以指示在 *Diagnostics > Status Configuration > Security Status* 对话框中监控的参数的状态。
- *Device/Security status*
  使用此设置，信号触点可以指示在 *Diagnostics > Status Configuration > Device Status* 对话框和 *Diagnostics > Status Configuration > Security Status* 对话框中监控的参数的状态。

配置运行监控

请执行以下步骤：

- ☐ 打开 *Diagnostics > Status Configuration > Signal Contact* 对话框的 *Global* 选项卡。
- ☐ 要使用信号触点对设备功能进行监控，请在 *Configuration* 框的 *Mode* 字段中指定值 *Monitoring correct operation*。
- ☐ 对于要监控的参数，请勾选 *Monitor* 列中的复选框。
- ☐ 要向管理站发送 SNMP 陷阱，请激活 *Traps* 框中的 *Send trap* 功能。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。
- ☐ 在 *Diagnostics > Status Configuration > Alarms (Traps)* 对话框中，创建至少一个接收 SNMP 陷阱的陷阱目标。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。
- ☐ 可在 *Basic Settings > System* 对话框中为温度监控指定温度阈值。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`signal-contact 1 monitor temperature`	对设备中的温度进行监控。当温度高于/低于阈值时，信号触点打开。
`signal-contact 1 monitor ring-redundancy`	对环网冗余进行监控。 信号触点在以下情况下打开： • 冗余功能变为活动状态（冗余储备丧失）。 • 设备是一个普通的环网参与者，并检测到其设置中的错误。
`signal-contact 1 monitor link-failure`	对端口/接口链路进行监控。当被监控的端口/接口上发生链路中断时，信号触点打开。
`signal-contact 1 monitor envm-removal`	对活动的外部存储器进行监控。用户从设备中删除活动的外部存储器时，信号触点打开。
`signal-contact 1 monitor envm-not-in-sync`	对设备和外部存储器中的配置概要文件进行监控。 信号触点在以下情况下打开： • 配置概要文件只存在于设备中。 • 设备中的配置概要文件与外部存储器中的配置概要文件不同。
`signal-contact 1 monitor power-supply 1`	对电源单元 1 进行监控。当设备检测到电源故障时，信号触点打开。

`signal-contact 1 monitor module-removal 1`	对模块 1 进行监控。当用户从设备中删除模块 1 时，信号触点打开。
`signal-contact 1 trap`	启用设备以便在运行监控状态发生改变时发送一个 SNMP 陷阱。
`no signal-contact 1 trap`	禁用 SNMP 陷阱

为了启用设备以便对没有连接的活动链路进行监控，请首先启用全局功能，然后启用各个端口。

请执行以下步骤：

- ☐ 在 *Monitor* 列中，激活 *Link interrupted on enabled device ports* 功能。
- ☐ 打开 *Diagnostics > Status Configuration > Device Status* 对话框的 *Port* 选项卡。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`signal-contact 1 monitor link-failure`	对端口/接口链路进行监控。当被监控的端口/接口上发生链路中断时，信号触点打开。
`interface 1/1`	切换到接口 1/1 的接口配置模式。
`signal-contact 1 link-alarm`	对端口/接口链路进行监控。当端口/接口上发生链路中断时，信号触点打开。

可以监控的事件

表格 54: Device Status 事件

名称	含义
Temperature	当温度超过或低于指定值时。
Ring redundancy	当存在环网冗余时，请启用此功能以进行监控。
Connection errors	启用此功能，对其中 *Propagate connection error* 复选框已激活的每个端口链路事件进行监控。
External memory not in sync with NVM	设备会监控设备配置和存储在外部存储器 (*ENVM*) 中的配置之间的同步。
External memory removed	启用此功能，对有无外部存储设备进行监控。
Power supply	启用此功能，对电源进行监控。

显示信号触点状态

设备为用户提供了用于显示信号触点状态的额外选项：

- ▶ 在图形用户界面中显示
- ▶ 在命令行界面中进行查询

请执行以下步骤：

☐ 打开 *Basic Settings* > *System* 对话框。
Signal contact status 框显示信号触点状态并通知用户已发生的警报。当前存在警报时，此框突出显示。

`show signal-contact 1 all`	显示指定信号触点的信号触点设置。

14.5 端口状态指示

要查看端口的状态，请执行以下步骤：

□ 打开 *Basic Settings > System* 对话框。

该对话框显示使用当前配置的设备。此外，该对话框还指示带有符号的单个端口的状态。

以下符号代表单个端口的状态。在某些情况下，这些符号会相互冲突。将鼠标指针置于端口图标之上时，气泡帮助会显示端口状态的详细描述。

表格 55: 标识端口状态的符号

标准	符号
端口带宽	10 Mbit/s 端口已激活，连接正常，全双工模式 100 Mbit/s 端口已激活，连接正常，全双工模式 1000 Mbit/s 端口已激活，连接正常，全双工模式
工作状态	半双工模式已启用 参见 *Basic Settings > Port* 对话框 *Configuration* 选项卡 *Automatic configuration* 复选框的 *Manual configuration* 字段和 *Manual cable crossing (Auto. conf. off)* 字段。 自动协商已启用 参见 *Basic Settings > Port* 对话框 *Configuration* 选项卡的 *Automatic configuration* 复选框。 端口已被冗余功能阻塞。
AdminLink	端口已停用，连接正常 端口已停用，未建立连接 参见 *Basic Settings > Port* 对话框 *Configuration* 选项卡的 *Port on* 复选框和 *Link/Current settings* 字段。

14.6 端口事件计数器

端口统计表允许经验丰富的网络管理员识别网络中可能检测到的问题。

此表显示各种事件计数器的内容。数据包计数器会对发送的事件和接收的事件进行累加。在 *Basic Settings > Restart* 对话框中，可以重置事件计数器

表格 56: 指示已知薄弱点的示例

计数器	已知可能薄弱点的指示
接收到的碎片	• 相连设备的控制器不工作 • 传输介质中的电磁干扰
CRC 错误	• 相连设备的控制器不工作 • 传输介质中的电磁干扰 • 网络中的组件不工作
冲突	• 相连设备的控制器不工作 • 网络规模过大/线路太长 • 数据包存在冲突或检测到的故障

请执行以下步骤：

- ☐ 要显示事件计数器，请打开 *Basic Settings > Port* 对话框的 *Statistics* 选项卡。
- ☐ 要重置计数器，请在 *Basic Settings > Restart* 对话框中点击 *Clear port statistics* 按钮。

14.6.1 检测不匹配的双工模式

当彼此直接连接的两个端口具有不匹配的双工模式时，会出现问题。这些问题是很难追踪的。针对这种情况的自动检测和报告的优点是，可在问题发生之前识别出不匹配的双工模式。

例如，停用远程端口上的自动配置等错误配置会导致这种情况。

这种不匹配的典型影响是，在低数据速率下，连接似乎正常工作，但在较高的双向流量级别时，本地设备记录了大量检测到的 CRC 错误，并且连接明显低于其标称容量。

设备允许用户检测这种情况并向网络管理站报告。在此过程中，设备会根据端口设置评估检测到的端口错误计数器。

端口错误事件的可能原因

下表列出了 TX 端口的各种双工工作模式以及可能的故障事件。表中使用的术语的含义如下：

- 冲突
  在半双工模式下，冲突表示正常运行。
- 双工问题
  不匹配的双工模式。
- EMI
  电磁干扰。
- 网络扩展
  网络扩展过大或级联集线器太多。

- 冲突，Late Collisions
  在全双工模式下，冲突或 Late Collisions 不导致端口计数器递增。
- CRC 错误
  设备将这些检测到的错误评估为手动全双工模式中不匹配的双工模式。

表格 57: 双工模式不匹配的评估

编号	自动配置	当前双工模式	检测到的错误事件（链路建立后大于等于 10 个）	双工模式	可能的原因
1	勾选	半双工	无	OK	
2	勾选	半双工	冲突	OK	
3	勾选	半双工	Late Collisions	检测到双工问题	双工问题，EMI，网络扩展
4	勾选	半双工	CRC 错误	OK	EMI
5	勾选	全双工	无	OK	
6	勾选	全双工	冲突	OK	EMI
7	勾选	全双工	Late Collisions	OK	EMI
8	勾选	全双工	CRC 错误	OK	EMI
9	未勾选	半双工	无	OK	
10	未勾选	半双工	冲突	OK	
11	未勾选	半双工	Late Collisions	检测到双工问题	双工问题，EMI，网络扩展
12	未勾选	半双工	CRC 错误	OK	EMI
13	未勾选	全双工	无	OK	
14	未勾选	全双工	冲突	OK	EMI
15	未勾选	全双工	Late Collisions	OK	EMI
16	未勾选	全双工	CRC 错误	检测到双工问题	双工问题，EMI

14.7 Auto-Disable

设备可以出于几种可配置的原因禁用一个端口。每种原因都会导致端口“关闭”。为了使端口从关闭状态中恢复，可以手动清除导致端口关闭的条件或指定自动重新启用端口的计时器。

如果配置显示一个端口已启用，但设备检测到错误或条件变化，则软件将关闭该端口。换言之，由于检测到错误或条件变化，设备软件将禁用该端口。

如果一个端口已自动禁用，则设备实际上将关闭该端口且该端口将阻塞流量。端口 LED 指示灯每个周期以绿色闪烁 3 次，并标识关闭的原因。此外，设备还会创建一个列出停用原因的日志文件条目。当您使用 *Auto-Disable* 功能在超时后重新启用端口时，设备会生成一个日志条目。

Auto-Disable 功能提供一种恢复功能，可在用户定义的时间之后自动启用一个被自动禁用的端口。当此功能启用一个端口时，设备会发送一个带有端口编号但不带有 *Reason* 参数的值的 SNMP 陷阱。

Auto-Disable 功能的目的如下：
- 它可协助网络管理员进行端口分析。
- 它可降低该端口导致网络不稳定的可能性。

Auto-Disable 功能可用于以下功能：
- *Link flap*（*Port Monitor* 功能）
- *CRC/Fragments*（*Port Monitor* 功能）
- Duplex Mismatch 检测（*Port Monitor* 功能）
- *DHCP Snooping*
- *Dynamic ARP Inspection*
- *Spanning Tree*
- *Port Security*
- *Overload detection*（*Port Monitor* 功能）
- *Link speed/Duplex mode detection*（*Port Monitor* 功能）

在以下示例中，将设备配置为因检测到不符合 *Diagnostics* > *Ports* > *Port Monitor* 对话框 *CRC/Fragments* 选项卡中指定的阈值而禁用一个端口，然后再自动重新启用被禁用的端口。

请执行以下步骤：

- ☐ 打开 *Diagnostics* > *Ports* > *Port Monitor* 对话框的 *CRC/Fragments* 选项卡。
- ☐ 验证该表中指定的阈值是否符合您针对端口 1/1 的首选项。
- ☐ 打开 *Diagnostics* > *Ports* > *Port Monitor* 对话框的 *Global* 选项卡。
- ☐ 要启用该功能，请选择 *Operation* 框中的 *On* 单选按钮。
- ☐ 要允许设备因检测到错误而禁用端口，请为端口 1/1 勾选 *CRC/Fragments on* 列中的复选框。
- ☐ 在 *Action* 列中，可以选择设备如何对检测到的错误作出反应。在此示例中，设备因违反阈值而禁用端口 1/1，然后自动重新启用该端口。
  - 要允许设备禁用并自动重新启用端口，请选择值 *auto-disable* 并配置 *Auto-Disable* 功能。值 *auto-disable* 只能配合 *Auto-Disable* 功能一起使用。

  设备还可以不经自动重新启用就禁用端口。
  - 要允许设备只禁用该端口，请选择值 *disable port*。

  要手动重新启用被禁用的端口，请突出显示该端口。

  点击 ☰ 按钮，然后点击 *Reset* 项目。
  - 配置 *Auto-Disable* 功能时，值 *disable port* 也会自动重新启用该端口。
- ☐ 打开 *Diagnostics* > *Ports* > *Port Monitor* 对话框的 *Auto-disable* 选项卡。

- ☐ 要允许设备在因检测到违反阈值而禁用端口之后自动重新启用该端口，请勾选 *CRC error* 列中的复选框。
- ☐ 打开 *Diagnostics* > *Ports* > *Port Monitor* 对话框的 *Port* 选项卡。
- ☐ 在 *Reset timer [s]* 列中为想要启用的端口将延迟时间指定为 120 秒。

提示： *Reset* 项目允许用户在 *Reset timer [s]* 列中指定的时间开始倒计时之前启用端口。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`interface 1/1`	切换到接口 1/1 的接口配置模式。
`port-monitor condition crc-fragments count 2000`	将 CRC 碎片计数器指定为百万分之 2000。
`port-monitor condition crc-fragments interval 15`	将 CRC 碎片检测的测量间隔设置为 15 秒。
`auto-disable timer 120`	将 *Auto-disable* 功能重新启用端口之前的等待期指定为 120 秒。
`exit`	切换到配置模式。
`auto-disable reason crc-error`	激活自动禁用 CRC 功能。
`port-monitor condition crc-fragments mode`	激活触发操作的 CRC 碎片条件。
`port-monitor operation`	激活 *Port Monitor* 功能。

当设备因违反阈值而禁用一个端口时，设备允许用户使用以下命令手动重置被禁用的端口。

请执行以下步骤：

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`interface 1/1`	切换到接口 1/1 的接口配置模式。
`auto-disable reset`	允许用户在计时器开始倒计时之前启用端口。

14.8 显示 SFP 状态

SFP 状态显示允许用户查看当前 SFP 模块连接及其属性。属性包括：

- 模块类型
- 介质模块的序列号
- 以 C 为单位的温度
- 以 mW 为单位的发送功率
- 以 mW 为单位的接收功率

执行以下步骤：

1. 打开 *Diagnostics > Ports > SFP* 对话框。

14.9 拓扑识别

IEEE 802.1AB 描述了链路层发现协议 (Link Layer Discovery Protocol, LLDP)。LLDP 允许用户自动检测 LAN 网络拓扑。

具有活动 LLDP 的设备：
- 将其连接和管理信息广播到共享 LAN 上的相邻设备。当接收设备激活了自己的 *LLDP* 功能时，设备评估开始进行。
- 从共享 LAN 上的相邻设备接收连接和管理信息，条件是，这些相邻设备也都激活了 LLDP。
- 建立用于存储关于激活了 LLDP 的相邻设备的信息的管理信息数据库和对象定义。

作为主要元素，连接信息包含连接端点的精确、惟一标识符：MAC（服务访问点）。这是由一个在整个网络上都是唯一的设备标识符以及用于该设备的唯一端口标识符组成的。
- 机箱标识符（其 MAC 地址）
- 端口标识符（其端口 MAC 地址）
- 端口描述
- 系统名称
- 系统描述
- 支持的系统功能
- 当前活动的系统功能
- 管理地址的接口 ID
- 端口的 VLAN-ID
- 端口上的自动协商状态
- 介质、半/全双工设置和端口速度设置
- 关于设备中安装的 VLAN 的信息（VLAN-ID 和 VLAN 名称，与端口是否为 VLAN 参与者无关）。

网络管理站可以从激活了 LLDP 的设备中调用此信息。此信息允许网络管理站映射网络拓扑。

非 LLDP 设备一般会阻塞用于信息交换的特殊 Multicast LLDP IEEE MAC 地址。因此，非 LLDP 设备会丢弃 LLDP 数据包。如果将不支持 LLDP 的设备放置在两个支持 LLDP 的设备之间，则该不支持 LLDP 的设备会禁止这两个支持 LLDP 的设备之间的信息交换。

具有 LLDP 功能的设备的管理信息库 (MIB) 会将 LLDP 信息保留在 lldp MIB 中，以及私有 SA2-LLDP-EXT-HM-MIB 和 SA2-LLDP-MIB 中。

14.9.1 显示拓扑识别结果

显示网络的拓扑结构。为此，请执行以下步骤：

□ 打开 *Diagnostics* > *LLDP* > *Topology Discovery* 对话框的 *LLDP* 选项卡。

例如，通过集线器使用一个端口连接多个设备时，每个相连设备在该表中分别占一行。

通过激活表格底部的显示 FDB 条目，可以在表格中显示没有活动 LLDP 支持的设备。在这种情况下，设备还包括来自其 FDB（转发数据库）的信息。

如果将端口连接到激活了拓扑识别功能的设备，则这些设备会交换 LLDP 数据单元 (LLDPDU) 且拓扑表会显示这些相邻设备。

当一个端口只连接没有活动拓扑识别的设备时，表中包含代表连接的设备的该端口的一行。此行包含连接的设备的数量。

FDB 地址表包含拓扑表为了清晰起见而隐藏的设备的 MAC 地址。

14.9.2 LLDP-Med

用于介质端点设备的 LLDP (LLDP-MED) 是对 LLDP 的扩展，它在端点设备之间运行。端点包括 IP 电话等设备、其他 IP 语音 (VoIP) 设备或服务器以及交换机等网络设备。它专门为 VoIP 应用程序提供支持。LLDP-MED 使用一组额外的公共类型长度值 (TLV) 广告消息为功能发现、网络策略、以太网供电、库存管理和位置信息提供这种支持。

设备支持以下 TLV 消息：

- 功能 TLV
  允许 LLDP-MED 端点确定相连设备支持的功能以及设备启用了哪些功能。
- 网络策略 TLV
  允许网络连通性设备和端点都为该端口上的特定应用程序发布 VLAN 配置和相关属性。例如，设备可向一个电话通知 VLAN 编号。电话连接到交换机，获得其 VLAN 编号，然后开始与呼叫控制进行通信。

LLDP-MED 提供以下功能：

- 网络策略发现，包括 VLAN ID、802.1p 优先级和区分服务代码点 (DSCP)
- 基于 LAN 级 MAC/端口信息的设备位置和拓扑识别
- 端点移动检测通知，从网络连通性设备到相关的 VoIP 管理应用程序
- 用于库存管理的扩展设备识别
- 具有嵌入式交换机或网桥功能的多端口 IP 电话等端点网络连通性功能的识别
- 与 LLDP 协议元素的应用程序级交互，提供 LLDP 的及时启动，以支持紧急呼叫服务的快速可用性
- LLDP-MED 对无线 LAN 环境的适用性，对无线 LAN 语音的支持

14.10 检测环路

网络中的环路会导致连接中断或数据丢失。这也适用于临时环路。针对这种情况的自动检测和报告允许用户进行更快速的检测和更轻松的诊断。

⚠ 警告

不允许的设备操作

为帮助避免在配置阶段出现环路，请分别配置环网的每个设备。在连接冗余线路之前，应完成环网配置的其他设备的配置。

如果不遵循这些说明，则会导致死亡、重伤或设备损坏。

停用生成树等错误配置会导致环路。

设备允许用户检测一般由环路造成的影响，并自动向网络管理站报告这种情况。在此，可以选择指定触发设备发送报告的环路影响的程度。

从指定端口发送、在同一设备的不同端口或同一端口上短时间内收到的 BPDU 帧，就是环路的一种常见影响。

要检查设备是否已检测到环路，请执行以下步骤：

- ☐ 打开 *Switching > L2-Redundancy > Spanning Tree > Port* 对话框的 *CIST* 选项卡。
- ☐ 检查 *Port state* 和 *Port role* 字段中的值。如果 *Port state* 字段显示值 discarding 且 *Port role* 字段显示值 backup，则端口处于环路状态。

  或者
- ☐ 打开 *Switching > L2-Redundancy > Spanning Tree > Port* 对话框的 *Guards* 选项卡。
- ☐ 勾选 *Loop state* 列中的值。如果该字段显示值 true，则端口处于环路状态。

14.11 帮助防止发生第二层网络环路

设备帮助防止发生第二层网络环路。

网络环路可能因过载而导致网络停顿。一个可能的原因是，由错误配置造成的数据包持续复制。例如，原因可能是电缆连接不良或设备中的设置不正确。

例如，如果没有活动的冗余协议，则在以下情况下可能会发生第二层网络环路：
- 同一个设备的两个端口直接相互连接。
- 两个设备之间建立了多个活动连接。

⚠ 警告

不允许的设备操作

为帮助避免在配置阶段出现环路，请分别配置第二层网络的每个设备。在连接冗余线路之前，应完成第二层网络的其他设备的配置。

如果不遵循这些说明，则会导致死亡、重伤或设备损坏。

14.11.1 应用示例

该图显示网络中可能的第二层环路的示例。每个设备中的 *Loop Protection* 功能已启用。

- A: *主动模式*
  用于连接终端设备的端口在 *active* 模式下运行。设备在这些端口上评估和发送*环路检测*数据包。
- P: *被动模式*
  属于冗余环网的端口在 *passive* 模式下运行。设备在这些端口上仅评估*环路检测*数据包。
- **环路 1..环路 4**
  意外配置的第二层网络环路。

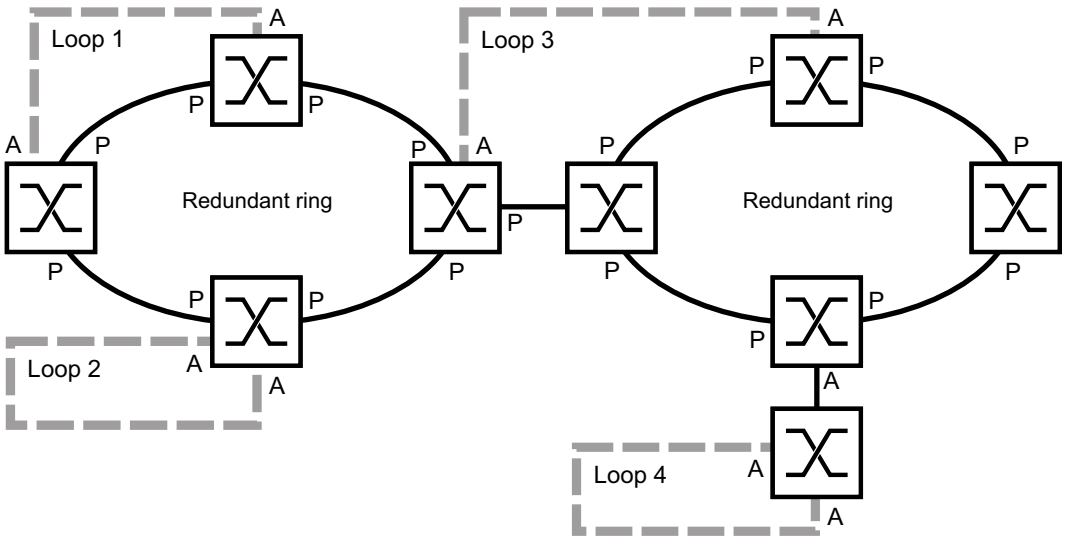


图 73: 意外的第二层网络环路的示例

将 Loop Protection 设置分配给端口

对于每个*主动*端口和每个*被动*端口，分配 *Loop Protection* 功能的设置。

请执行以下步骤：

- ☐ 打开 *Diagnostics* > *Loop Protection* 对话框。
- ☐ 在 *Global* 中，*Transmit interval* 字段，根据需要调整该值。
- ☐ 在 *Global* 中，*Receive threshold* 字段，根据需要调整该值。
- ☐ 在 *Mode* 列中，指定端口上的 *Loop Protection* 功能的行为：
  - *active* 对于用于连接终端设备的端口
  - *passive* 对于属于冗余环网的端口
- ☐ 在 *Action* 列中，指定值 *all*。
  当设备在此端口上检测到第二层环路时，它将发送陷阱并使用 *Auto-Disable* 功能来禁用端口。根据需要调整该值。
- ☐ 在 *Active* 列中，勾选复选框。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`loop-protection tx-interval 5`	根据需要指定传输间隔。
`loop-protection rx-threshold 1`	根据需要指定接收阈值。
`interface 1/1`	更改到接口模式。 示例：端口 *1/1*。
`loop-protection mode active`	为用于连接终端设备的端口指定模式 `active`。
`loop-protection mode passive`	为属于冗余环网的端口指定模式 `passive`。
`loop-protection action all`	指定设备在此端口上检测到第二层环路时执行的操作。
`loop-protection operation`	激活端口上的 *Loop Protection* 功能。
`exit`	切换到配置模式。

激活 Auto-Disable 功能

在将 *Loop Protection* 设置分配给设备之后，激活 *Auto-Disable* 功能。

请执行以下步骤：

- ☐ 在 *Configuration* 框中，勾选 *Auto-disable* 复选框。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`loop-protection auto-disable`	激活 *Auto-Disable* 功能。

启用设备中的 Loop Protection 功能

完成后，启用设备中的 *Loop Protection* 功能。

请执行以下步骤：

- ☐ 在 *Operation* 框中，选择 *On* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`loop-protection operation`	启用设备中的 *Loop Protection* 功能。

14.11.2 冗余端口建议

根据 *Loop Protection* 设置，设备在检测到第二层网络环路时使用 *Auto-Disable* 功能来禁用端口。

如果端口上的冗余功能已激活，则不要在此功能上激活 *active* 模式。否则，结果可能是冗余网络路径上的端口关闭。在以上示例中，这些是属于冗余环网的端口。

验证冗余网络路径是否可用作备份介质。设备在主路径中断的情况下对冗余路径进行更改。

以下设置帮助避免冗余网络路径上的端口关闭：
- ☐ 禁用冗余端口上的 *Loop Protection* 功能。
  或者
- ☐ 启用冗余端口上的 *passive* 模式。

Loop Protection 功能和 *Spanning Tree* 功能可能会彼此影响。以下步骤帮助避免设备产生意外行为：
- ☐ 在要启用 *Loop Protection* 功能的端口上禁用 *Spanning Tree* 功能。参见 *Switching* > *L2-Redundancy* > *Spanning Tree* > *Port* 对话框的 *STP active* 列。
- ☐ 在每个已连接的设备上的每个已连接的端口上禁用 *Spanning Tree* 功能。参见 *Switching* > *L2-Redundancy* > *Spanning Tree* 对话框。

14.12 使用 Email Notification 功能

设备让您能够通过电子邮件向用户通知已发生的事件。前提条件是可通过设备传输电子邮件的网络访问邮件服务器。

要将设备设置为发送电子邮件，请执行以下章节中的步骤：

- ☐ 指定发送者地址
- ☐ 指定触发事件
- ☐ 指定收件人
- ☐ 指定邮件服务器
- ☐ 启用/禁用 Email Notification 功能
- ☐ 发送测试电子邮件

14.12.1 指定发送者地址

发送者地址是指示发送电子邮件的设备的电子邮件地址。在设备中，默认设置为 。

更改预设值。为此，请执行以下步骤：

- ☐ 打开 *Diagnostics* > *Email Notification* > *Global* 对话框。
- ☐ 在 *Sender* 框中，更改 *Address* 字段中的值。
  添加有效的电子邮件地址。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`logging email from-addr <user@doma.in>`	更改发送者地址。

14.12.2 指定触发事件

设备区分以下严重程度：

表格 58: 事件的严重程度的含义

严重程度	含义
emergency	设备未处于运行准备就绪状态
alert	需要立即进行用户干预
critical	重要状态
error	错误状态
warning	警告
notice	重要正常状态
informational	非正式消息
debug	调试消息

您可以选择指定设备向您通知的事件。为此，请将所需的最低严重程度分配给设备的通知级别。

设备以如下方式通知收件人：

- *Notification immediate*
  当分配的严重程度或更严重的事件发生时，设备会立即发送电子邮件。
- *Notification periodic*
  - 当分配的严重程度或更严重的事件发生时，设备会在缓冲区中记录事件。
  - 如果缓冲区已满，设备会定期发送包含日志文件的电子邮件。
  - 当更低严重程度的事件发生时，设备不会记录此事件。

请执行以下步骤：

☐ 打开 *Diagnostics > Email Notification > Global* 对话框。

在 *Notification immediate* 框中，可以指定设备立即发送的电子邮件的设置。
☐ 在 *Severity* 字段中，可以指定最低严重程度。
☐ 在 *Subject* 字段中，可以指定电子邮件的主题。

在 *Notification periodic* 框中，您可以指定设备定期发送的电子邮件的设置。
☐ 在 *Severity* 字段中，可以指定最低严重程度。
☐ 在 *Subject* 字段中，可以指定电子邮件的主题。

☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`logging email severity immediate <level>`	指定设备立即为其发送电子邮件的事件的最低严重程度。
`logging email severity periodic <level>`	指定设备定期为其发送电子邮件的事件的最低严重程度。
`logging email subject add <immediate | periodic> TEXT`	使用内容 `TEXT` 创建主题行。

14.12.3 更改发送间隔

设备让您能够指定其发送包含日志文件的电子邮件的间隔。默认设置为 `30` 分钟。

请执行以下步骤：

☐ 打开 *Diagnostics > Email Notification > Global* 对话框。

在 *Notification periodic* 框中，您可以指定设备定期发送的电子邮件的设置。
☐ 更改 *Sending interval [min]* 中的值以更改间隔。

☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`logging email duration <30..1440>`	指定设备发送包含日志文件的电子邮件的间隔。

14.12.4 指定收件人

设备允许指定最多 10 个收件人。

请执行以下步骤：

- ☐ 打开 *Diagnostics* > *Email Notification* > *Recipients* 对话框。
- ☐ 要添加一个表格条目，请点击 按钮。
- ☐ 在 *Notification type* 列中，指定设备是立即还是定期向此收件人发送电子邮件。
- ☐ 在 *Address* 列中，指定收件人的电子邮件地址。
- ☐ 在 *Active* 列中，勾选复选框。
- ☐ 暂时保存更改。为此，请单击 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`logging email to-addr add <1..10> addr <user@doma.in> msgtype <immediately | periodically>`	使用电子邮件地址 user@doma.in 指定收件人。设备管理存储器 1..10 中的设置。

14.12.5 指定邮件服务器

设备支持与邮件服务器建立加密和未加密的连接。

请执行以下步骤：

- ☐ 打开 *Diagnostics* > *Email Notification* > *Mail Server* 对话框。
- ☐ 要添加一个表格条目，请点击 按钮。
- ☐ 在 *IP address* 列中，指定服务器的 IP 地址或 DNS 名称。
- ☐ 在 *Encryption* 列中，指定对设备与邮件服务器之间的连接进行加密的协议。
- ☐ 当邮件服务器使用非公认端口时，在 *Destination TCP port* 列中指定 TCP 端口。

当邮件服务器请求身份验证时：

- ☐ 在 *User name* 和 *Password* 列中，指定设备用于在邮件服务器上进行身份验证的帐户凭证。
- ☐ 在 *Description* 列中，为邮件服务器输入有意义的名称。
- ☐ 在 *Active* 列中，勾选复选框。
- ☐ 暂时保存更改。为此，请单击 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`logging email mail-server add <1..5> addr <IP ADDRESS> [security <none|tlsv1>] [username <USER NAME>] [password <PASSWORD>] [port <1..65535>]`	使用 IP 地址 IP ADDRESS 指定邮件服务器。设备管理存储器 1..5 中的设置。

14.12.6 启用/禁用 Email Notification 功能

请执行以下步骤：

- ☐ 打开 *Diagnostics > Email Notification > Global* 对话框。
- ☐ 要启用该功能，请选择 *Operation* 框中的 *On* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 ✓ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`logging email operation`	启用电子邮件发送。
`no logging email operation`	禁用电子邮件发送。

14.12.7 发送测试电子邮件

设备让您能够通过发送测试电子邮件来检查设置。

前提条件：
- ▶ 已完整指定电子邮件设置。
- ▶ *Email Notification* 功能已启用。

请执行以下步骤：

- ☐ 打开 *Diagnostics > Email Notification > Mail Server* 对话框。
- ☐ 点击 ☰ 按钮，然后点击 *Connection test* 项目。
  该对话框显示 *Connection test* 窗口。
- ☐ 在 *Recipient* 下拉列表中，选择设备向其发送测试电子邮件的收件人。
- ☐ 在 *Message text* 字段中，指定测试邮件的文本。
- ☐ 点击 *Ok* 按钮以发送测试电子邮件。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`logging email test msgtype <urgent|non-urgent> TEXT`	将包含内容 `TEXT` 的电子邮件发送给收件人。

当您没有看到任何检测到的错误消息并且收件人收到电子邮件时，设备设置是正确的。

14.13 报告

以下列出了可用于诊断的报告和按钮：

- 系统日志文件
  日志文件是一个设备在其中写入设备内部事件的 HTML 文件。
- 审计跟踪
  记录成功的命令和用户备注。该文件还包括 SNMP 日志记录。
- 持久记录
  当存在外部存储器时，设备会将日志条目保存到外部存储器中的一个文件中。这些文件在电源关闭后可用。可保留文件的最大大小、最大数量和所记录事件的严重程度都是可配置的。在获得用户定义的可保留文件的最大大小或最大数量后，设备会对条目进行存档并启动一个新的文件。设备会删除最老的文件并对其他文件进行重命名，以保持配置的文件数量。要查看这些文件，请使用命令行界面或将其复制到外部服务器供今后参考。
- *Download support information*
  此按钮可用于将系统信息下载为 ZIP 文档。

在服务情况下，这些报告可为技术人员提供必要的信息。

14.13.1 全局设置

使用此对话框，您可以启用或禁用设备的报告发送目标，例如控制台、系统日志服务器或命令行界面连接。还可以设置设备写入报告中的事件的严重级别。

请执行以下步骤：

- ☐ 打开 *Diagnostics* > *Report* > *Global* 对话框。
- ☐ 要向控制台发送报告，请在 *Console logging* 框的 *Severity* 字段中指定所需的级别。
- ☐ 要启用该功能，请选择 *Console logging* 框中的 *On* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

设备将记录的事件缓冲到两个单独的存储区域中，使紧急事件的日志条目得到保留。为设备在缓冲存储区域中记录的具有较高优先级的事件指定最低严重程度。

请执行以下步骤：

- ☐ 要向缓冲区发送事件，请在 *Buffered logging* 框的 *Severity* 字段中指定所需的级别。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

激活 SNMP 请求的记录时，设备会将请求作为事件记录到系统日志中。*Log SNMP get request* 功能会记录针对设备配置信息的用户请求。*Log SNMP set request* 功能会记录设备配置事件。为设备在系统日志中记录的事件指定最低级别。

请执行以下步骤：

- ☐ 为设备启用 *Log SNMP get request* 功能，以便将 SNMP 读请求作为事件发送到系统日志服务器。
  要启用该功能，请选择 *SNMP logging* 框中的 *On* 单选按钮。
- ☐ 为设备启用 *Log SNMP set request* 功能，以便将 SNMP 写请求作为事件发送到系统日志服务器。
  要启用该功能，请选择 *SNMP logging* 框中的 *On* 单选按钮。
- ☐ 为 get 和 set 请求选择所需的严重级别。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

激活后，设备会将使用命令行界面进行的配置更改记录到审计跟踪中。此功能基于用于变电所智能电子装置的 IEEE 1686 标准。

请执行以下步骤：

- ☐ 打开 *Diagnostics > Report > Global* 对话框。
- ☐ 要启用该功能，请选择 *CLI logging* 框中的 *On* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

设备允许用户将以下系统信息数据保存到用户 PC 上的一个 ZIP 文件中：

- audittrail.html
- defaultconfig.xml
- script
- runningconfig.xml
- supportinfo.html
- systeminfo.html
- systemlog.html

设备以 <IP_address>_<system_name>.zip 格式自动创建该 ZIP 文档的文件名。

请执行以下步骤：

- ☐ 点击 ☰ 按钮，然后点击 *Download support information* 项目。
- ☐ 选择要保存支持信息的目录。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

14.13.2 系统日志

设备允许用户将关于设备内部事件的消息发送到一个或多个系统日志服务器（最多 8 个）。此外，还可以将向设备发出的 SNMP 请求作为事件包括在系统日志中。

提示：要显示记录的事件，请打开 *Diagnostics > Report > Audit Trail* 对话框或 *Diagnostics > Report > System Log* 对话框。

请执行以下步骤：

- ☐ 打开 *Diagnostics > Syslog* 对话框。
- ☐ 要添加一个表格条目，请点击  按钮。
- ☐ 在 *IP address* 列中，输入系统日志服务器的 IP 地址 或 *Hostname*.
  可以为系统日志服务器指定有效的 IPv4 或 IPv6 地址。
- ☐ 在 *Destination UDP port* 列中，指定系统日志服务器期望日志条目所在的 TCP 或 UDP 端口。
- ☐ 在 *Min. severity* 列中，指定设备向此系统日志服务器发送日志条目所需的事件的最低严重级别。
- ☐ 勾选 *Active* 列中的复选框。
- ☐ 要启用该功能，请选择 *Operation* 框中的 *On* 单选按钮。
- ☐ 暂时保存更改。为此，请单击  按钮。

在 *SNMP logging* 框中，为读和写 SNMP 请求配置以下设置：

请执行以下步骤：

- ☐ 打开 *Diagnostics > Report > Global* 对话框。
- ☐ 为设备启用 *Log SNMP get request* 功能，以便将 SNMP 读请求作为事件发送到系统日志服务器。
  要启用该功能，请选择 *SNMP logging* 框中的 *On* 单选按钮。
- ☐ 为设备启用 *Log SNMP set request* 功能，以便将 SNMP 写请求作为事件发送到系统日志服务器。
  要启用该功能，请选择 *SNMP logging* 框中的 *On* 单选按钮。
- ☐ 为 get 和 set 请求选择所需的严重级别。
- ☐ 暂时保存更改。为此，请单击  按钮。

```
enable                                          切换到特权执行模式。
configure                                       切换到配置模式。
logging host add 1 addr 10.0.1.159              在系统日志服务器列表中添加一个新的接收者。值
severity 3                                      3 可指定设备记录的事件的严重级别。值 3 表示
                                                error。
logging host add 2 addr 2001::1 severity        在系统日志服务器列表中添加新的 IPv6 收件人。
4                                               值 4表示 warning。
logging syslog operation                        启用 Syslog 功能。
exit                                            切换到特权执行模式。
show logging host                               显示系统日志主机设置。
No.    Server IP      Port   Max. Severity   Type        Status
-----  -------------- -----  --------------  ----------  -------
1      10.0.1.159     514    error           systemlog   active
2      2001::1        514    warning         systemlog   active
configure                                       切换到配置模式。
logging snmp-requests get operation             记录 SNMP GET 请求。
logging snmp-requests get severity 5            值 5 可指定设备在 SNMP GET 请求的情况下记录的
                                                事件的严重级别。值 5 表示 notice。
```

```
logging snmp-requests set operation          记录 SNMP SET 请求。
logging snmp-requests set severity 5         值 5 可指定设备在 SNMP SET 请求的情况下记录的
                                             事件的严重级别。值 5 表示 notice。
exit                                         切换到特权执行模式。
show logging snmp                            显示 SNMP 日志记录设置。
Log SNMP GET requests              : enabled
Log SNMP GET severity              : notice
Log SNMP SET requests              : enabled
Log SNMP SET severity              : notice
```

14.13.3 系统日志

设备允许用户调用系统事件的日志文件。*Diagnostics > Report > System Log* 对话框中的表格列出了记录的事件。

请执行以下步骤：

- ☐ 要更新日志的内容，请点击 按钮。
- ☐ 要将日志的内容另存为 html 文件，请点击 按钮，然后点击 *Reset* 项目。
- ☐ 要删除日志的内容，请点击 按钮，然后点击 *Reset* 项目。
- ☐ 要在日志内容中搜索一个关键词，请使用 Web 浏览器的搜索功能。

提示：还可以选择将记录的事件发送到一个或多个系统日志服务器。

14.13.4 TLS 上的系统日志

传输层安全（TLS）是为在计算机网络上提供通信安全而设计的密码协议。TLS 协议的主要目标是提供两个通信的计算机应用程序之间的隐私和数据完整性。

在发起与系统日志服务器的连接之后，设备使用 TLS 握手对从服务器接收的证书进行验证。为此，可将 PEM 证书从远程服务器或外部存储器传输到设备上。验证已配置的服务器 IP 地址或 DNS 名称是否匹配证书中提供的信息。可在证书的通用名或使用者可选名称字段中找到这些信息。

设备通过 *Destination UDP port* 列中指定的 TCP 端口发送 TLS 加密系统日志消息。

提示：指定服务器上的 IP 地址或 DNS 名称，以匹配服务器证书中提供的 IP 地址或 DNS 名称。可在通用名或使用者可选名称中找到在证书中输入的值。

示例

给出的示例描述 *Syslog* 功能的配置。通过以下这些步骤，设备让您能够通过 *Destination UDP port* 列中指定的 TCP 端口发送 TLS 加密系统日志消息。

从设备发送到系统日志服务器的系统日志消息可能通过不安全的网络传递。要配置 TLS 上的系统日志服务器，请将证书颁发机构（CA）证书传输到设备上。

提示：为使更改在加载新的证书之后生效，请重新启动 *Syslog* 功能。

请执行以下步骤：

- ☐ 打开 *Diagnostics* > *Syslog* 对话框。
- ☐ 要发起与系统日志服务器的连接，请选择 *Operation* 框中的 *On* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

设备对收到的证书进行验证。设备还对服务器进行身份验证并开始发送系统日志消息。

- ☐ 将 PEM 证书从远程服务器或外部存储器传输到设备上。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`logging host add 1 addr 192.168.3.215`	将索引 1 添加使用 IPv4 地址 192.168.3.215 的系统日志服务器。
`logging host add 2 addr 2001::1`	将索引 2 添加使用 IPv4 地址 2001::1. 的系统日志服务器。
`logging host modify 1 port 6512 type systemlog`	指定端口编号 6512 并在系统日志中记录事件。
`logging host modify 1 transport tls`	将传输类型指定为 tls。
`logging host modify 1 severity informational`	将要记录到系统日志中的事件类型指定为 informational。
`exit`	切换到特权执行模式。
`copy syslogcacert evmm`	将 CA 证书从外部存储器复制到设备。
`show logging host`	显示系统日志主机设置。

14.13.5 审计跟踪

Diagnostics > *Report* > *Audit Trail* 对话框包含系统信息以及通过命令行界面和 SNMP 对设备配置进行的更改。在设备配置更改的情况下，该对话框会显示进行更改的人员、更改的内容和时间。

Diagnostics > *Syslog* 对话框允许用户指定最多 8 个设备向其发送审计跟踪的系统日志服务器。

以下列表包含了日志事件：

- 对配置参数的更改
- 使用命令行界面发出的命令（`show` 命令除外）
- 使用记录备注的命令行界面发出的 `logging audit-trail <string>` 命令
- 对系统时间的自动更改
- 看门狗事件
- 几次登录尝试失败后锁定用户
- 使用命令行界面的本地或远程用户登录
- 用户发起的手动注销
- 在用户定义的命令行界面不活动期间之后的定时注销
- 固件更新等文件传输操作
- 配置更改，来自 Ethernet Switch Configurator
- 使用外部存储器的自动配置或固件更新
- 因无效登录而被封锁的设备管理访问
- 重启
- 通过 HTTPS 隧道打开和关闭 SNMP
- 检测到的电源故障

14.14 使用 TCPdump 进行网络分析

Tcpdump 是一种网络管理员用以嗅探和分析网络上的流量的数据包嗅探 UNIX 实用程序。对网络上的流量进行嗅探的一些原因包括，验证主机之间的连通性或对通过网络的流量进行分析。

设备中的 TCPDump 可以对管理 CPU 接收和发送的数据包进行解码或捕获。可通过 `debug` 命令使用此功能。有关 TCPDump 功能的更多信息，请参阅“命令行界面”参考手册。

14.15 监控数据流量

设备允许用户将通过设备的数据包转发到目标端口。在此，可以对数据包进行监控和评估。

设备为用户提供以下选项：
▶ Port Mirroring

14.15.1 Port Mirroring

Port Mirroring 功能允许用户将数据包从物理源端口复制到物理目标端口。

可以利用 RMON 探测器等连接到目标端口的管理工具对源端口上发送和接收方向的数据流量进行监控。该功能对源端口上运行的数据流量没有影响。

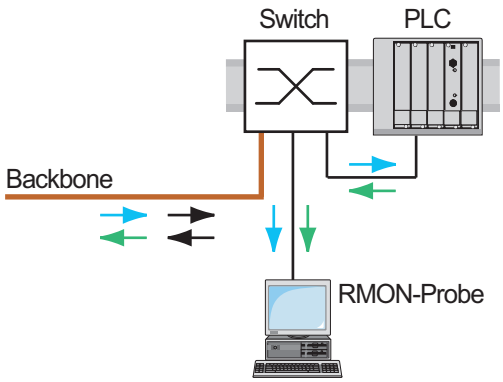


图 74: 示例

在目标端口上，设备只转发从源端口复制的数据包。

在开启 *Port Mirroring* 功能之前，请勾选 *Allow management* 复选框，以允许通过目标端口访问设备管理。设备允许用户在不中断活动 *Port Mirroring* 会话的前提下通过目标端口访问设备管理。

提示： 设备在目标端口上复制多播、广播和未知单播。

目标端口上的 VLAN 设置保持不变。通过目标端口访问设备管理的前提条件是，目标端口是设备管理 VLAN 的成员。

启用 Port Mirroring 功能

请执行以下步骤：

- ☐ 打开 *Diagnostics > Ports > Port Mirroring* 对话框。
- ☐ 指定源端口。
  为相关端口勾选 *Enabled* 列中的复选框。
- ☐ 指定目标端口。
  在 *Destination port* 框中，在 *Primary port* 下拉列表中选择所需端口。
  该下拉列表只显示可用端口。已经被指定为源端口的端口不可用。
- ☐ 如果需要，指定辅助目标端口。
  在 *Destination port* 框中，在 *Secondary port* 下拉列表中选择所需端口。
  前提条件是已指定主目标端口。
- ☐ 为通过目标端口访问设备管理：
  在 *Destination port* 框中，请勾选 *Allow management* 复选框。
- ☐ 暂时保存更改。为此，请单击  按钮。

要停用 *Port Mirroring* 功能并恢复默认设置，请点击  按钮，然后点击 *Reset config* 项目。

14.16 自检

设备在启动过程中会检查其资产，之后也会偶尔进行检查。设备会检查系统任务可用性或终止以及可用的内存量。此外，设备还会检查应用程序功能以及芯片组中的任何硬件退化。

如果设备检测到完整性丧失，则设备会通过用户自定义操作对退化作出响应。可以使用以下类别进行配置。

- task
  任务失败时需要执行的操作。
- resource
  资源短缺时需要执行的操作。
- software
  代码段校验和或访问违规等软件完整性丧失时需要执行的操作。
- hardware
  硬件退化时需要执行的操作。

将每个类别配置为在设备检测到完整性丧失时产生一种操作。可以使用以下操作进行配置。

- log only
  此操作会向日志文件中写入一条消息。
- send trap
  向陷阱目标发送 SNMP 陷阱。
- reboot
  如果激活，则在类别中检测到错误将导致设备重新启动。

请执行以下步骤：

- ☐ 打开 *Diagnostics > System > Selftest* 对话框。
- ☐ 在 *Action* 列中，指定针对某个原因需要执行的操作。
- ☐ 暂时保存更改。为此，请单击 ✓ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`selftest action task log-only`	任务失败时向事件日志发送一条消息。
`selftest action resource send-trap`	资源不足时，发送一个 SNMP 陷阱。
`selftest action software send-trap`	软件完整性丧失时，发送一个 SNMP 陷阱。
`selftest action hardware reboot`	发生硬件退化时重新启动设备。

禁用这些功能后，可以缩短冷启动后重启设备所需的时间。可在 *Diagnostics > System > Selftest* 对话框的 *Configuration* 框中找到这些选项。

- *RAM test*
  激活/停用冷启动期间的 *RAM test* 功能。
- *SysMon1 is available*
  激活/停用冷启动期间的系统监控器功能。
- *Load default config on error*
  激活/停用在重新启动期间没有可用的可读配置时默认设备配置的加载。

当设备在重新启动期间没有检测到任何可读的配置概要文件时，以下设置会永久阻止用户访问设备。

- *SysMon1 is available* 复选框为未勾选。
- *Load default config on error* 复选框为未勾选。

例如，当用户正在加载的配置概要文件的密码与设备中设置的密码不同时，就属于这种情况。要使设备再次解锁，请与您的销售合作伙伴联系。

请执行以下步骤：

`selftest ramtest`	启用冷启动期间的 RAM 自检。
`no selftest ramtest`	禁用“ramtest”功能。
`selftest system-monitor`	启用“SysMon1”功能。
`no selftest system-monitor`	禁用“SysMon1”功能。
`show selftest action`	显示设备退化时需要执行的操作的状态。
`show selftest settings`	显示进行冷启动时“ramtest”和“SysMon”设置的设置。

14.17 铜电缆测试

使用此功能测试连接至接口的铜电缆是否短路或开路。测试进行时会中断此端口上的流量。

此表格显示每一对铜电缆的状态和长度。设备返回具有以下含义的结果：
- 正常 – 表示电缆运行正常
- 开路 – 表示电缆中断
- 短路 – 表示电缆短路
- 未经测试 – 表示电缆未经测试
- 未知 – 电缆未插拔

15 高级设备功能

15.1 使用设备作为 DHCP 服务器

DHCP（“动态主机配置协议”）服务器可向客户端分配 IP 地址、Gateways 以及 DNS 和 NTP 参数等其他联网定义。

DHCP 运行分为四个基本阶段：IP 发现、IP 租赁提供、IP 请求和 IP 租赁确认。请使用代表发现、提供、请求和确认的首字母缩略词 DORA 帮助您记住这些阶段。服务器通过 UDP 端口 67 接收客户端数据，并通过 UDP 端口 68 向客户端转发数据。

DHCP 服务器提供可从中向客户端分配 IP 地址的一个或多个 IP 地址库。地址库由多个条目的列表组成。一个条目定义一个特定的 IP 地址或一个 IP 地址范围。

设备允许用户以全局方式以及按接口激活 DHCP 服务器。

15.1.1 按端口或按 VLAN 分配的 IP 地址

DHCP 服务器向连接到端口或 VLAN 的客户端分配一个静态 IP 地址或动态 IP 地址范围。设备允许用户为一个端口或一个 VLAN 创建条目。当创建一个条目以向 VLAN 分配 IP 地址时，端口条目会变为灰色。当创建一个条目以向端口分配 IP 地址时，VLAN 条目会变为灰色。

静态分配指的是，DHCP 服务器向一个特定客户端分配相同的 IP 地址。DHCP 服务器通过唯一的硬件 ID 识别客户端。一个静态地址条目包含一个 IP 地址，并将该地址应用到服务器通过其接收来自特定客户端的请求的端口或 VLAN。对于静态分配，可为多个端口或一个特定端口创建一个地址库条目，输入 IP 地址，并将 *Last IP address* 列留为空白。指定 DHCP 服务器用于明确识别客户端的硬件 ID。该 ID 可以是 MAC 地址、客户端 ID、远程 ID 或电路 ID。当客户端使用已配置硬件 ID 与服务器联系时，DHCP 服务器会分配静态 IP 地址。

设备还允许用户向 DHCP 服务器从其分配来自地址库的空闲 IP 地址的端口或 VLAN 分配一个动态 IP 地址范围。要为端口或 VLAN 添加动态地址库条目，可指定 IP 地址范围的第一个和最后一个 IP 地址，然后将 *MAC address*、*Client ID*、*Remote ID* 和 *Circuit ID* 列留为空白。通过创建多个地址库条目，可以获得包含空缺的 IP 地址范围。

15.1.2 DHCP 服务器静态 IP 地址示例

在此示例中，将设备配置为向端口分配静态 IP 地址。设备通过唯一硬件标识识别客户端。在本例中，硬件 ID 是客户端 MAC 地址 00:24:E8:D6:50:51。为此，请执行以下步骤：

- ☐ 打开 *Advanced* > *DHCP Server* > *Pool* 对话框。
- ☐ 要添加一个表格条目，请点击  按钮。
- ☐ 在 *IP address* 列中，指定值 192.168.23.42。
- ☐ 在 *Port* 列中，指定值 1/1。
- ☐ 在 *MAC address* 列中，指定值 00:24:E8:D6:50:51。

- ☐ 要将 IP 地址无限期分配给客户端，请在 *Lease time [s]* 列中指定值 4294967295。
- ☐ 勾选 *Active* 列中的复选框。
- ☐ 打开 *Advanced* > *DHCP Server* > *Global* 对话框。
- ☐ 对于端口 1/1，请勾选 *DHCP server active* 列中的复选框。
- ☐ 要启用该功能，请选择 *Operation* 框中的 *On* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`dhcp-server pool add 1 static 192.168.23.42`	创建一个带有索引 1 的条目并将 IP 地址 192.168.23.42 添加到静态地址库。
`dhcp-server pool modify 1 mode interface 1/1`	将索引 1 中的静态地址分配给接口 1/1。
`dhcp-server pool modify 1 mode mac 00:24:E8:D6:50:51`	将索引 1 中的 IP 地址分配给具有 MAC 地址 00:24:E8:D6:50:51 的设备。
`dhcp-server pool mode 1`	启用索引 1 地址库条目。
`dhcp-server pool modify 1 leasetime infinite`	要将 IP 地址无限期分配给客户端，请修改带有索引 1 的条目。
`dhcp-server operation`	全局启用 DHCP 服务器。
`interface 1/1`	切换到接口 1/1 的接口配置模式。
`dhcp-server operation`	激活此端口上的 *DHCP Server* 服务器功能。

15.1.3 DHCP 服务器动态 IP 地址范围示例

设备允许用户创建动态 IP 地址范围。将 *MAC address*、*Client ID*、*Remote ID* 和 *Circuit ID* 字段留为空白。要创建彼此之间存在空缺的动态 IP 地址范围，请向表格中添加几个条目。为此，请执行以下步骤：

- ☐ 打开 *Advanced* > *DHCP Server* > *Pool* 对话框。
- ☐ 要添加一个表格条目，请点击 按钮。
- ☐ 在 *IP address* 列中，指定值 192.168.23.92。这是该范围的第一个 IP 地址。
- ☐ 在 *Last IP address* 列中，指定值 192.168.23.142。
  这是该范围的最后一个 IP 地址。

在 *Lease time [s]* 列中，默认设置为 60 天。

- ☐ 在 *Port* 列中，指定值 1/2。
- ☐ 勾选 *Active* 列中的复选框。
- ☐ 打开 *Advanced* > *DHCP Server* > *Global* 对话框。
- ☐ 对于端口 1/2，请勾选 *DHCP server active* 列中的复选框。
- ☐ 要启用该功能，请选择 *Operation* 框中的 *On* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`dhcp-server pool add 2 dynamic 192.198.23.92 192.168.23.142`	添加一个 IP 范围为 192.168.23.92 到 192.168.23.142 的动态地址库。
`dhcp-server pool modify 2 leasetime {seconds | infinite}`	输入 Lease Time（秒或无限期）。
`dhcp-server pool add 3 dynamic 192.198.23.172 192.168.23.180`	添加一个 IP 范围为 192.168.23.172 到 192.168.23.180 的动态地址库。
`dhcp-server pool modify 3 leasetime {seconds | infinite}`	输入 Lease Time（秒或无限期）。
`dhcp-server pool mode 2`	启用索引 2 地址库条目。
`dhcp-server pool mode 3`	启用索引 3 地址库条目。
`dhcp-server operation`	全局启用 DHCP 服务器。
`interface 2/1`	切换到接口 2/1 的接口配置模式。
`dhcp-server operation`	激活此端口上的 *DHCP Server* 服务器功能。

15.2 DHCP 第二层中继

在设备的前置面板上，可以看到以下危险信息：

⚠ 警告

非预期操作

如果 DHCP 选项 82 已启用，请勿改变电缆位置。检修前请查看用户手册。

如果不遵循这些说明，则会导致死亡、重伤或设备损坏。

网络管理员使用 DHCP 第二层*中继代理*添加 DHCP 客户端信息。第三层*中继代理*和 DHCP 服务器需要使用此信息向客户端分配地址和配置。

当 DHCP 客户端和服务器位于同一 IP 子网中时，它们会直接交换 IP 地址请求和应答。但是，在每个子网上都配备一个 DHCP 服务器，成本比较高昂，而且往往也不切实际。针对在每个子网中都配备一个 DHCP 服务器的一种替代方法是，使用网络设备对位于不同子网中的 DHCP 客户端和 DHCP 服务器之间的数据包进行中继传输。

第三层*中继代理*一般是一个在客户端和服务器子网中都有 IP 接口并在二者之间路由传输流量的路由器。但是，在第二层交换网络中，在客户端和第三层*中继代理*或 DHCP 服务器之间存在交换机等一个或多个网络设备。在这种情况下，本设备提供一个第二层*中继代理*，以添加第三层*中继代理*和 DHCP 服务器执行其地址和配置分配角色所需的信息。

以下列表包含了此功能的默认设置：
- 全局设置：
  - 活动设置：禁用
- 接口设置：
  - 活动设置：禁用
  - 可信端口：禁用
- VLAN 设置：
  - 活动设置：禁用
  - *电路 ID*：启用
  - *远程 ID* 类型：mac
  - *远程 ID*：空白

对于 DHCPv6 协议，可使用*中继代理*将*中继代理*选项添加到在客户端与 DHCPv6 服务器之间交换的 DHCPv6 数据包中。RFC 6221 中介绍了轻量级 DHCPv6 中继代理 (LDRA)。

LDRA 处理 2 种类型的消息：
- 第一种消息是其中包含有关客户端唯一信息的*中继转发*消息。
- 第二种消息是 DHCPv6 服务器发送到*中继代理*的*中继应答*消息。然后，*中继代理*验证该消息，以包含在初始*中继转发*消息中封装的信息，如果有效，则将数据包发送到客户端。

*中继转发*消息包含也称为 *Option 18* 的*接口 ID* 信息。此选项提供的信息可用于识别在其上发送客户端请求的接口。设备丢弃不包含 *Option 18* 信息的 DHCPv6 数据包。

15.2.1 电路和远程 ID

在 IPv4 环境中，在将客户端的请求转发到 DHCP 服务器之前，设备会向 DHCP 请求数据包的 *Option 82* 字段添加*电路 ID* 和*远程 ID*。

- *电路 ID* 会存储设备通过哪个端口接收到客户端的请求。
- *远程 ID* 包含 MAC 地址、IP 地址、系统名称或一个用户自定义字符串。使用该 ID，参与设备可以识别接收到客户端请求的*中继代理*。

设备和其他*中继代理*使用此信息将来自 DHCP *中继代理*的应答重定向到原始客户端。例如，DHCP 服务器可以对此数据进行分析，进而向客户端分配一个来自特定地址库的 IP 地址。

此外，DHCP 服务器的重播数据包还包含*电路 ID* 和*远程 ID*。在向客户端转发应答之前，设备会从 *Option 82* 字段中删除信息。

15.2.2 DHCP 第二层中继配置

Advanced > DHCP L2 Relay > Configuration 对话框允许用户激活活动端口和 VLAN 上的功能。在 *Operation* 框中，选择*On* 单选按钮。然后点击 按钮。

设备通过在 *DHCP L2 Relay* 列中和*Trusted port* 列中为其勾选复选框的端口转发包含 *Option 82* 信息的 数据包和包含*Option 18* 信DHCPv4息 的DHCPv6数据包。 通常，这些是 DHCP 服务器网络中的端口。

对于 DHCP 客户端所连接到的端口，可以激活 *DHCP L2 Relay* 功能，但应将 *Trusted port* 复选框留为未勾选。在这些端口上，设备会丢弃包含*Option 82*信息 的 DHCPv4 数据包和包含*Option 18* 信息的 DHCPv6 数据包。

DHCPv4 L2 中继功能的示例配置如下所示。除了仅可为 *Option 82* 指定的*电路 ID* 和*远程 ID* 条目外，DHCPv6 L2 中继功能的配置步骤与 DHCPv4 类似。

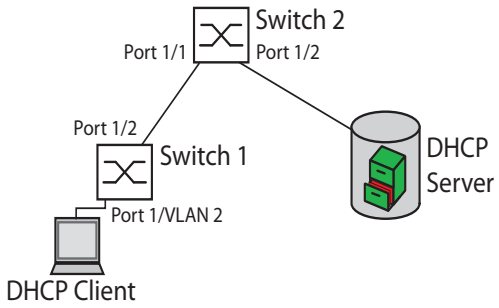


图 75: DHCP 第二层示例网络

请在交换机 1 上执行以下步骤：

- ☐ 打开 *Advanced > DHCP L2 Relay > Configuration* 对话框的 *Interface* 选项卡。
- ☐ 对于端口 1/1，请按如下方式指定设置：
  - 勾选 *Active* 列中的复选框。
- ☐ 对于端口 1/2，请按如下方式指定设置：
  - 勾选 *Active* 列中的复选框。
  - 勾选 *Trusted port* 列中的复选框。
- ☐ 打开 *Advanced > DHCP L2 Relay > Configuration* 对话框的 *VLAN ID* 选项卡。

- ☐ 按如下方式指定 VLAN 2 的设置：
  - 勾选 *Active* 列中的复选框。
  - 勾选 *Circuit ID* 列中的复选框。
  - 要将设备的 IP 地址用作*远程 ID*，请在 *Remote ID type* 列中指定值 ip。
- ☐ 要启用该功能，请选择 *Operation* 框中的 *On* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

请在交换机 2 上执行以下步骤：

- ☐ 打开 *Advanced* > *DHCP L2 Relay* > *Configuration* 对话框的 *Interface* 选项卡。
- ☐ 对于端口 1/1 和 1/2，请按如下方式指定设置：
  - 勾选 *Active* 列中的复选框。
  - 勾选 *Trusted port* 列中的复选框。
- ☐ 要启用该功能，请选择 *Operation* 框中的 *On* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

验证 VLAN 2 是否存在。然后在交换机 1 上执行以下步骤：
☐ 配置 VLAN 2，并将端口 1/1 指定为 VLAN 2 的成员。

`enable`	切换到特权执行模式。
`vlan database`	切换到 VLAN 配置模式。
`dhcp-l2relay circuit-id 2`	激活 VLAN 2 上的电路 ID 和 DHCP 选项 82。
`dhcp-l2relay remote-id ip 2`	将设备的 IP 地址指定为 VLAN 2 上的远程 ID。
`dhcp-l2relay mode 2`	激活 VLAN 2 上的 *DHCP L2 Relay* 功能。
`exit`	切换到特权执行模式。
`configure`	切换到配置模式。
`interface 1/1`	切换到接口 1/1 的接口配置模式。
`dhcp-l2relay mode`	激活端口上的 *DHCP L2 Relay* 功能。
`exit`	切换到配置模式。
`interface 1/2`	切换到接口 1/2 的接口配置模式。
`dhcp-l2relay trust`	将端口指定为 *Trusted port*。
`dhcp-l2relay mode`	激活端口上的 *DHCP L2 Relay* 功能。
`exit`	切换到配置模式。
`dhcp-l2relay mode`	启用设备中的 *DHCP L2 Relay* 功能。

请在交换机 2 上执行以下步骤：

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`interface 1/1`	切换到接口 1/1 的接口配置模式。
`dhcp-l2relay trust`	将端口指定为 *Trusted port*。
`dhcp-l2relay mode`	激活端口上的 *DHCP L2 Relay* 功能。
`exit`	切换到配置模式。
`interface 1/2`	切换到接口 1/2 的接口配置模式。
`dhcp-l2relay trust`	将端口指定为 *Trusted port*。

`dhcp-l2relay mode`	激活端口上的 *DHCP L2 Relay* 功能。
`exit`	切换到配置模式。
`dhcp-l2relay mode`	启用设备中的 *DHCP L2 Relay* 功能。

15.3 将设备用作 DNS 客户端

域名系统 (DNS) 客户端查询 DNS 服务器以解析网络设备的主机名和 IP 地址。与电话簿类似，DNS 客户端将设备名称转换为 IP 地址。当 DNS 客户端接收到解析新名称的请求时，会首先查询其内部静态数据库，然后再查询分配的 DNS 服务器以获取该信息。DNS 客户端将查询到的信息保存在缓存中，以供未来请求使用。

设备允许用户使用设备管理 VLAN 从 DHCP 服务器配置 DNS 客户端。设备还允许用户将主机名称静态分配给 IP 地址。

DNS 客户端提供以下用户功能：
- DNS 服务器列表，具有用于将 4 个域名服务器 IP 地址
- 静态主机名称映射到 IP 地址的空间，具有用于 64 个可配置
- 静态主机的主机缓存空间，具有用于 128 个条目的空间

15.3.1 配置 DNS 服务器示例

命名 DNS 客户端，并将其配置为可查询 DNS 服务器以解析主机名称。为此，请执行以下步骤：

- ☐ 打开 *Advanced > DNS > Client > Static* 对话框。
- ☐ 在 *Configuration* 框的 *Configuration source* 字段中，指定值 user。
- ☐ 在 *Configuration* 框的 *Domain name* 字段中，指定值 device1。
- ☐ 要添加一个表格条目，请点击 按钮。
- ☐ 在 *Address* 列中，将值 192.168.3.5 指定为 DNS 服务器的 IPv4 地址。 用户还可以将有效的 IPv6 地址指定为 DNS 服务器的 IP 地址。
- ☐ 勾选 *Active* 列中的复选框。
- ☐ 打开 *Advanced > DNS > Client > Global* 对话框。
- ☐ 要启用该功能，请选择 *Operation* 框中的 *On* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`dns client source user`	指定用户手动配置 DNS 客户端设置。
`dns client domain-name device1`	指定字符串 device1 作为设备的唯一域名。
`dns client servers add 1 ip 192.168.3.5`	添加 IPv4 地址为 192.168.3.5 的 DNS 名称服务器作为索引 1。
`dns client servers add 2 ip 2001::1`	添加 IPv6 地址为 2001::1 的 DNS 名称服务器作为索引 2。
`dns client adminstate`	全局启用 *DNS Client* 功能。

配置 DNS 客户端以通过 IP 地址映射静态主机。为此，请执行以下步骤：

- ☐ 打开 *Advanced > DNS > Client > Static Hosts* 对话框。
- ☐ 要添加一个表格条目，请点击  按钮。
- ☐ 在 *Name* 列中，输入值 example.com。
  这是设备在网络中的名称。
- ☐ 在 *IP address* 列中，指定值 192.168.3.9。
- ☐ 勾选 *Active* 列中的复选框。
- ☐ 暂时保存更改。为此，请单击  按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`dns client host add 1 name example.com ip 192.168.3.9`	添加 example.com 作为 IP 地址为 192.168.3.9 的静态主机。
`dns client adminstate`	全局启用 *DNS Client* 功能。

15.4 GARP

IEEE 定义的通用属性注册协议（*GARP*）提供了一个通用框架，使交换机能够注册和注销 VLAN 标识符和 Multicast 组成员资格等属性值。

如果根据 *GARP* 功能注册或注销一个参与者的一个属性，则根据特定规则对该参与者进行修改。参与者是一组可达的终端站和网络设备。在任意给定时间定义的参与者集合及其属性是网络拓扑子集的可达性树。设备只向注册终端站转发数据帧。站注册有助于防止向不可达终端站发送数据的企图。

15.4.1 配置 GMRP

GARP 多播注册协议（*GMRP*）是一种提供了允许网络设备和终端站动态注册组成员资格的机制的通用属性注册协议（*GARP*）。这些设备向连接到同一局域网段的设备注册组成员资格信息。*GARP* 功能还允许这些设备向支持扩展筛选服务的网络设备分发信息。

提示：启用 *GMRP* 功能之前，请验证 *MMRP* 功能是否已禁用。

以下示例描述了 *GMRP* 功能的配置。设备在选定端口上提供一个受约束的多播泛洪设施。为此，请执行以下步骤：

- ☐ 打开 *Switching* > *GARP* > *GMRP* 对话框。
- ☐ 要在端口上提供受约束的 Multicast Flooding，请勾选 *GMRP active* 列中的复选框。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`interface 1/1`	切换到接口 1/1 的接口配置模式。
`garp gmrp operation`	启用端口上的 *GMRP* 功能。
`exit`	切换到配置模式。
`garp gmrp operation`	全局启用 *GMRP* 功能。

15.4.2 配置 GVRP

可以使用 *GVRP* 功能允许设备与其他 *GVRP* 设备交换 VLAN 配置信息。如此可减少不必要的 Broadcast 和未知的 Unicast 流量。此外，*GVRP* 功能还可在通过 802.1Q 中继端口连接的设备上动态创建和管理 VLAN。

以下示例描述了 *GVRP* 功能的配置。设备允许用户与其他 *GVRP* 设备交换 VLAN 配置信息。为此，请执行以下步骤：

- ☐ 打开 *Switching* > *GARP* > *GVRP* 对话框。
- ☐ 要与其他 *GVRP* 设备交换 VLAN 配置信息，请为端口勾选 *GVRP active* 列中的复选框。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`interface 3/1`	切换到接口 3/1 的接口配置模式。
`garp gvrp operation`	启用端口上的 *GVRP* 功能。
`exit`	切换到配置模式。
`garp gvrp operation`	全局启用 *GVRP* 功能。

15.5 MRP-IEEE

针对 IEEE 802.1Q 标准的 IEEE 802.1ak 修订引入了多重注册协议 (MRP)，以此替代通用属性注册协议 (*GARP*)。IEEE 还修改了 *GARP* 应用程序、*GARP* 多播注册协议 (*GMRP*) 和 *GARP* VLAN 注册协议 (*GVRP*)，并将其替换为多重 MAC 注册协议 (*MMRP*) 和多重 VLAN 注册协议 (*MVRP*)。

为了将流量限制在网络的所需区域，MRP 应用程序会将属性值分发给横贯 LAN 的启用了 MRP 的设备。MRP 应用程序会注册并注销 Multicast 组成员资格和 VLAN 标识符。

提示：多重注册协议 (MRP) 需要无环路的网络。为帮助防止用户网络中出现环路，请对 MRP 使用介质冗余协议、生成树协议或快速生成树协议等网络协议。

15.5.1 MRP 运行

每个参与者都包含一个申请者组件和一个 MRP 属性声明 (MAD) 组件。申请者组件负责形成属性值及其注册和注销。MAD 组件生成用于传输的 MRP 消息，并处理从其他参与者接收到的消息。MAD 组件对属性进行编码，并将其传输到 MRP 数据单元 (MRPDU) 中的其他参与者。在交换机中，MRP 属性传播 (MAP) 组件将属性分发到参与端口。

对于每个 MRP 应用程序和每个 LAN 端口都存在一个参与者。例如，终端设备上存在一个参与者应用程序，交换机端口上存在另一个应用程序。申请者状态机在终端设备或交换机上记录针对每个 MRP 参与者声明的属性和端口。申请者状态机变量的更改会触发 MRPDU 的传输，以传达声明或撤销。

为了建立 *MMRP* 实例，终端设备首先会发送带有适当属性的加入空 (JoinMt) 消息。然后，交换机将 JoinMt 大量发送到参与端口和相邻交换机。相邻交换机将该消息大量发送到其参与端口，依此类推，从而为组流量建立路径。

15.5.2 MRP 计时器

默认计时器设置有助于防止不必要的属性声明和撤销。计时器设置允许参与者在 Leave（离开）或 LeaveAll（离开全部）计时器过期之前接收和处理 MRP 消息。

对计时器进行重新配置时，可以维护以下关系：
- 即使出现消息丢失时，要在 Leave（离开）或 LeaveAll（离开全部）事件后进行重新注册，可将 LeaveTime（离开时间）的值设置为：≥ (2x JoinTime) + 60 in 1/100 s
- 要最大限度减少 LeaveAll（离开全部）后产生的重新加入流量的数量，可将 LeaveAll（离开全部）计时器的值指定为大于 LeaveTime（离开时间）。

以下列表包含了设备传输的各种 MRP 事件：
- 加入 - 控制下一个加入消息传输的间隔
- 离开 - 控制交换机在切换到撤销状态之前在离开状态下等待的时间长度
- 离开全部 - 控制交换机生成 LeaveAll（离开全部）消息的频率

到期后，周期性计时器会发起一个加入请求 MRP 消息，交换机将该消息发送到 LAN 上的参与者。交换机使用此消息来帮助防止不必要的撤销。

15.5.3 MMRP

当设备在端口上接收到 Broadcast、Multicast 或未知流量时，设备会将流量大量发送到其他端口。此过程会导致不必要地使用 LAN 上的带宽。

多重 MAC 注册协议 (*MMRP*) 允许用户将属性声明分发给 LAN 上的参与者，从而对流量泛洪进行控制。MAD 组件编码并通过 LAN 在 MRP 消息中传输的属性值是组服务需求信息和 48 位 MAC 地址。

交换机将这些属性作为 MAC 地址注册条目存储在筛选数据库中。转发过程使用筛选数据库条目只是为了通过访问组成员 LAN 所需的端口传输数据。

交换机促进了基于开放主机组概念的组分发机制，在活动端口上接收数据包，以及只向具有组成员的端口进行转发。如此，需要将数据包传输到一个或多个特定组的任何 *MMRP* 参与者都请求该组中的成员资格。MAC 服务用户从 LAN 的任何位置向特定组发送数据包。一个组在附加到注册 *MMRP* 参与者的 LAN 上接收这些数据包。因此，*MMRP* 和 MAC 地址注册条目将这些数据包限制到无环路 LAN 的所需网段。

为了保持注册和注销状态并接收流量，端口定期发布兴趣声明。LAN 上启用 *MMRP* 功能的每个设备都会维护一个筛选数据库，并将具有组 MAC 地址的流量转发到列出的参与者。

MMRP 示例

在此示例中，主机 A 打算侦听指向组 G1 的流量。交换机 A 处理从主机 A 接收到的 *MMRP* 加入请求，并将该请求同时发送给相邻交换机。LAN 上的设备现在知道，有一个主机对接收指向组 G1 的流量感兴趣。当主机 B 开始传输指向组 G1 的数据时，数据在注册的路径上流动，主机 A 接收到该数据。

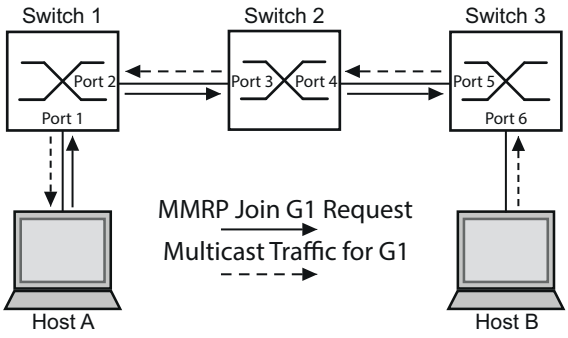


图 76: 用于 MAC 地址注册的 MMRP 网络

启用交换机上的 *MMRP* 功能。为此，请执行以下步骤：

- ☐ 打开 *Switching* > *MRP-IEEE* > *MMRP* 对话框的 *Configuration* 选项卡。
- ☐ 要将端口 1 和端口 2 激活为 *MMRP* 参与者，请为交换机 1 上的端口 1 和端口 2 勾选 *MMRP* 列中的复选框。
- ☐ 要将端口 3 和端口 4 激活为 *MMRP* 参与者，请为交换机 2 上的端口 3 和端口 4 勾选 *MMRP* 列中的复选框。
- ☐ 要将端口 5 和端口 6 激活为 *MMRP* 参与者，请为交换机 3 上的端口 5 和端口 6 勾选 *MMRP* 列中的复选框。
- ☐ 要发送允许设备保持 MAC 地址组注册的周期性事件，请启用 *Periodic state machine*。选择 *Configuration* 框中的 *On* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

要启用交换机 1 上的 *MMRP* 端口，请使用以下命令。替换命令中的相应接口，并启用交换机 2 和 3 上的 *MMRP* 功能和端口。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`interface 1/1`	切换到接口 1/1 的接口配置模式。
`mrp-ieee mmrp operation`	启用端口上的 *MMRP* 功能。
`interface 1/2`	切换到接口 1/2 的接口配置模式。
`mrp-ieee mmrp operation`	启用端口上的 *MMRP* 功能。
`exit`	切换到配置模式。
`mrp-ieee mrp periodic-state-machine`	全局启用 *Periodic state machine* 功能。
`mrp-ieee mmrp operation`	全局启用 *MMRP* 功能。

15.5.4 MVRP

多重 VLAN 注册协议 (*MVRP*) 是一种在 LAN 上提供动态 VLAN 注册和撤销服务的 MRP 应用程序。

MVRP 功能为动态 VLAN 注册条目以及向其他设备传输信息提供了一种维护机制。此信息允许支持 *MVRP* 的设备建立和更新其 VLAN 成员资格信息。当 VLAN 上存在成员时，该信息会指示交换机通过哪些端口转发流量以抵达这些成员。

MVRP 功能的主要目的在于，使交换机能够发现一些可能需要用户手动设置的 VLAN 信息。通过发现这些信息，交换机可以克服大型 VLAN 网络中带宽消耗和收敛时间的限制。

MVRP 示例

设置一个网络，使用支持 MVRP 的交换机 (1 – 4)，采用环网拓扑连接，划分 A1、A2、B1 和 B2 等终端设备组，分为 A 和 B 两个不同的 VLAN。在交换机上启用 STP 后，将交换机 1 连接到交换机 4 的端口处于丢弃状态，有助于防止出现环路。

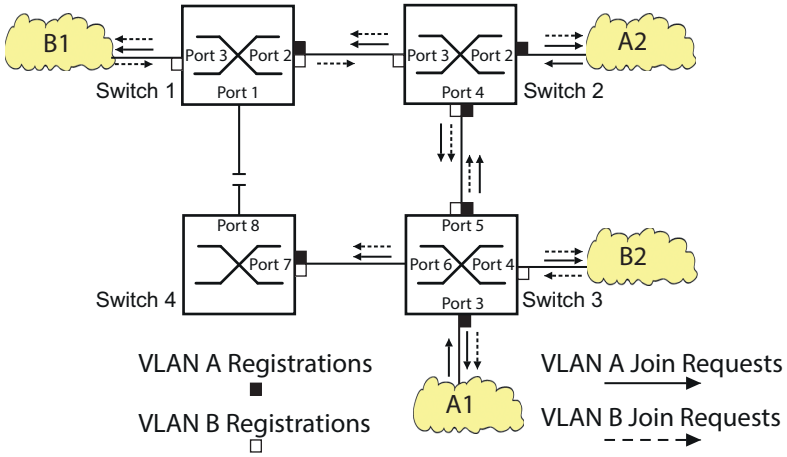


图 77: 用于 VLAN 注册的 MVRP 示例网络

在 MVRP 示例网络中，这两个 LAN 首先向交换机发送一个加入请求。交换机将针对接收帧的端口的 VLAN 注册输入到转发数据库中。

然后，交换机将该请求转发到其他端口，并将该请求发送到相邻 LAN 和交换机。这个过程会继续进行，直到这些交换机将 VLAN 注册到接收端口的转发数据库中为止。

启用交换机上的 MVRP。为此，请执行以下步骤：

- 打开 *Switching* > *MRP-IEEE* > *MVRP* 对话框的 *Configuration* 选项卡。
- 要将端口 1 至 3 激活为 *MVRP* 参与者，请为交换机 1 上的端口 1 至 3 勾选 *MVRP* 列中的复选框。
- 要将端口 2 至 4 激活为 *MVRP* 参与者，请为交换机 2 上的端口 2 至 4 勾选 *MVRP* 列中的复选框。
- 要将端口 3 至 6 激活为 *MVRP* 参与者，请为交换机 3 上的端口 3 至 6 勾选 *MVRP* 列中的复选框。
- 要将端口 7 和端口 8 激活为 *MVRP* 参与者，请为交换机 4 上的端口 7 和端口 8 勾选 *MVRP* 列中的复选框。
- 要保持 VLAN 注册，请启用 *Periodic state machine*。
  选择 *Configuration* 框中的 *On* 单选按钮。
- 要启用该功能，请选择 *Operation* 框中的 *On* 单选按钮。
- 暂时保存更改。为此，请单击 按钮。

要启用交换机 1 上的 *MVRP* 端口，请使用以下命令。替换命令中的相应接口，并启用交换机 2、3 和 4 上的 *MVRP* 功能和端口。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`interface 1/1`	切换到接口 1/1 的接口配置模式。
`mrp-ieee mvrp operation`	启用端口上的 *MVRP* 功能。
`interface 1/2`	切换到接口 1/2 的接口配置模式。
`mrp-ieee mvrp operation`	启用端口上的 *MVRP* 功能。
`exit`	切换到配置模式。
`mrp-ieee mvrp periodic-state-machine`	全局启用 *Periodic state machine* 功能。
`mrp-ieee mvrp operation`	全局启用 *MVRP* 功能。

16 工业协议

16.1 IEC 61850/MMS

IEC 61850/MMS 是国际电工委员会（IEC）发布的标准化工业通信协议。该协议还用于变电所自动化中，例如能源供应商所采用的控制技术。

这种面向数据包的协议基于 TCP/IP 传输协议，使用制造报文规范（MMS）来执行客户端服务器通信。该协议面向对象，定义了一种标准化配置语言，而且还包括适用于 SCADA、智能电子装置（IED）和网络控制系统的功能。

IEC 61850 标准的第 6 部分定义了配置语言 SCL（变电所配置语言）。SCL 以可自动处理的形式介绍了设备的属性和系统结构。使用 SCL 描述的设备属性储存在设备的 ICD 文件中。

16.1.1 IEC 61850 的交换机模型

IEC 61850 90-4 技术报告指定了网桥模型。网桥模型代表了交换机作为智能电子装置（IED）的对象的功能。MMS 客户端（例如控制室软件）使用这些对象来监控和配置设备。

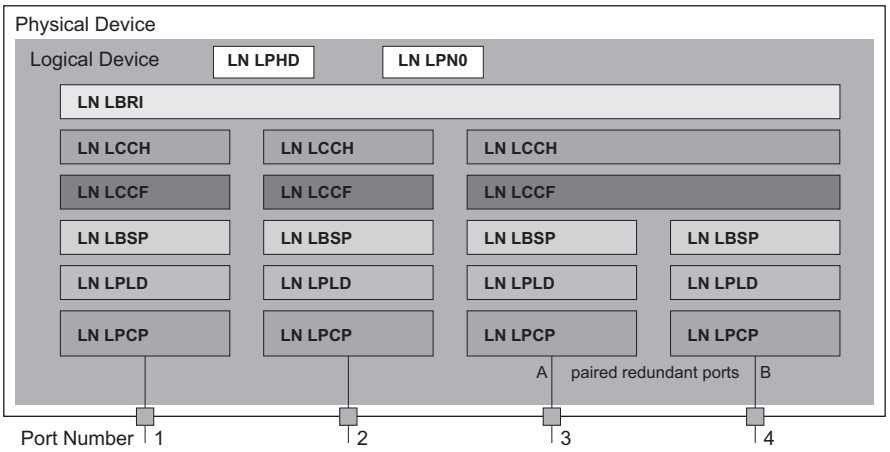


图 78: 基于 IEC 61850 90-4 技术报告的网桥模型

表格 59: 基于 TR IEC61850 90-4 的网桥模型类别

类别	描述
LN LLN0	Zero IED 的 Bridge 逻辑节点： 定义设备的逻辑属性。
LN LPHD	Physical Device IED 的 Bridge 逻辑节点： 定义设备的物理属性。
LN LBRI	Bridge 逻辑节点： 代表设备的网桥功能的一般设置。
LN LCCH	Communication Channel 逻辑节点： 定义包含一个或多个物理设备端口的逻辑 Communication Channel。
LN LCCF	Channel Communication Filtering 逻辑节点： 定义高级别 Communication Channel 的 VLAN 和多播设置。

表格 59: 基于 TR IEC61850 90-4 的网桥模型类别

类别	描述
LN LBSP	Port Spanning Tree Protocol 逻辑节点： 定义相关物理设备端口的生成树状态和设置。
LN LPLD	Port Layer Discovery 逻辑节点： 定义相关物理设备端口的 LLDP 状态和设置。
LN LPCP	Physical Communication Port 逻辑节点： 代表相关物理设备端口。

16.1.2 集成在控制系统内

设备准备

请执行以下步骤：

- ☐ 检查是否为设备分配了 IP 地址。
- ☐ 打开 *Advanced > Industrial Protocols > IEC61850-MMS* 对话框。
- ☐ 要启动 MMS 服务器，请在 *Operation* 框中选择 *On* 单选按钮，然后点击 ✓ 按钮。
  然后，MMS 客户端能够连接到设备，并读取和监控网桥模型中定义的对象。

IEC61850/MMS 不提供任何身份验证机制。如果激活 IEC61850/MMS 的写访问，则每个能使用 TCP/IP 访问设备的客户端都能够更改设备的设置。这反过来又会导致设备的不正确配置和网络中可能出现的问题。

注意

未经授权的设备访问风险

请仅在采取了额外措施（例如防火墙、VPN 等）的情况下激活写访问，以减少可能的未经授权的访问。

不遵守这些指示可能导致设备损坏。

- ☐ 要允许 MMS 客户端更改设置，请勾选 *Write access* 复选框，然后点击 ✓ 按钮。

离线配置

设备允许您使用图形用户界面下载 ICD 文件。此文件包含用 SCL 描述的设备属性，使您能够对变电所进行配置，无需直接连接到设备。

- ☐ 打开 *Advanced > Industrial Protocols > IEC61850-MMS* 对话框。
- ☐ 要将 ICD 文件加载到您的 PC，请点击 ≡ 按钮，然后点击 *Download* 项目。

监控设备

集成到设备中的 IEC61850/MMS 服务器使您能够通过报告控制块（RCB）监控设备的多个状态。报告控制块最多可同时注册 5 个 MMS 客户端。

设备允许用户监控以下状态：

表格 60: 可使用 IEC 61850/MMS 监控的设备状态

类别	RCB 对象	描述
LN LPHD	TmpAlm	当设备中测量的温度超出或低于设置的温度阈值时，状态会发生变化。
	PhyHealth	当 LPHD.TmpAlm RCB 对象的状态发生变化时，状态会发生变化。
LN LPHD	TmpAlm	当设备中测量的温度超出或低于设置的温度阈值时，状态会发生变化。
	PwrSupAlm	当其中一个冗余电源停止运行或再次开始运行时，状态会发生变化。
	PhyHealth	当 LPHD.PwrSupAlm 或 LPHD.TmpAlm RCB 对象的状态发生变化时，状态会发生变化。
LN LBRI	RstpRoot	当设备接替或撤回根网桥的角色时，状态会发生变化。
	RstpTopoCnt	当拓扑因根网桥更改而发生变化时，状态会发生变化。
LN LCCH	ChLiv	当物理端口的链路状态发生变化时，状态会发生变化。
LN LPCP	PhyHealth	当物理端口的链路状态发生变化时，状态会发生变化。

16.2 Modbus TCP

Modbus TCP 是应用层消息协议，可在以太网 TCP/IP 网络中连接的客户端与设备之间提供客户端/服务器通信。

Modbus TCP 功能允许用户在已使用 *Modbus TCP* 的网络中安装设备，并检索设备寄存器中保存的信息。

16.2.1 客户端/服务器 Modbus TCP/IP 模式

设备支持 Modbus TCP/IP 的客户端/服务器模型。设备在此状态中作为服务器工作，并响应客户端发出的对寄存器中保存的信息的请求。

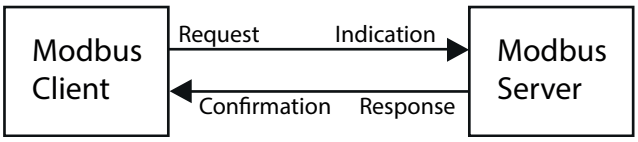


图 79: 客户端/服务器 Modbus TCP/IP 模式

客户端/服务器模型使用四种消息类型在客户端与服务器之间交换数据：

- Modbus TCP/IP 请求，客户端创建对信息的请求，并发送给服务器。
- Modbus TCP/IP 指示，服务器接收请求，并将其视作客户端请求信息的指示。
- Modbus TCP/IP 响应，若请求的信息可用，则服务器发送包含所需信息的应答。若请求的信息不可用，则服务器发送异常响应，将向客户端通知在处理期间检测到的错误。异常响应包含异常代码，用于指示检测到的错误的原因。
- Modbus TCP/IP 确认，客户端接收来自服务器的响应，其中包含所需信息。

16.2.2 支持的功能和存储器映射

设备支持公共代码为 0x03 (Read Holding Registers) 和 0x05 (Write Single Coil) 的功能。这些代码让您能够读取寄存器中保存的信息，例如系统信息，包括系统名称、系统位置、软件版本、IP 地址 和 MAC 地址。这些代码还让您能够读取端口信息和端口统计数据。0x05 代码让您能够重置单个或所有端口计数器。

以下列表包含在 Format 列中输入的值的定义：

- Bitmap：以大端字节序编码的一组 32 位数据，保存在 2 个寄存器中。在大端系统中，具有最大权重的字节保存在最低的地址处，具有最低权重的字节保存在最高的地址处。
- F1: 16-bit unsigned integer
- F2: Enumeration - power supply alarm
  - 0 = power supply good
  - 1 = power supply failure detected
- F3: Enumeration - OFF/ON
  - 0 = Off
  - 1 = On

- F4: Enumeration - port type
  - 0 = Giga - Gigabit Interface Converter (GBIC)
  - 1 = Copper - Twisted Pair (TP)
  - 2 = Fiber - 10 Mb/s
  - 3 = Fiber - 100 Mb/s
  - 4 = Giga - 10/100/1000 Mb/s (triple speed)
  - 5 = Giga - Copper 1000 Mb/s TP
  - 6 = Giga - Small Form-factor Pluggable (SFP)
- F9: 32-bit unsigned long
- String：以序列保存的八位字节，每个寄存器中保存 2 个八位字节。

Modbus TCP/IP 代码

下表列出了允许客户端重置端口计数器以及从设备寄存器检索特定信息的地址。

端口信息

表格 61: 端口信息

地址	数量	描述	最小	最大	步长	单元	格式
0400	1	Port 1 Type	0	6	1	-	F4
0401	1	Port 2 Type	0	6	1	-	F4
		...					
043F	1	Port 64 Type	0	6	1	-	F4
0440	1	Port 1 Link Status	0	1	1	-	F1
0441	1	Port 2 Link Status	0	1	1	-	F1
		...					
047F	1	Port 64 Link Status	0	1	1	-	F1
0480	1	Port 1 STP State	0	1	1	-	F1
0481	1	Port 2 STP State	0	1	1	-	F1
		...					
04BF	1	Port 64 STP State	0	1	1	-	F1
04C0	1	Port 1 Activity	0	1	1	-	F1
04C1	1	Port 2 Activity	0	1	1	-	F1
		...					
04FF	1	Port 64 Activity	0	1	1	-	F1
0500	1	Port 1 Counter Reset	0	1	1	-	F1
0501	1	Port 2 Counter Reset	0	1	1	-	F1
		...					
053F	1	Port 64 Counter Reset	0	1	1	-	F1

端口统计

表格 62: 端口统计

地址	数量	描述	最小	最大	步长	单元	格式
0800	1	Port1 - Number of bytes received	0	4294967295	1	-	F9
0802	1	Port1 - Number of bytes sent	0	4294967295	1	-	F9
0804	1	Port1 - Number of frames received	0	4294967295	1	-	F9

表格 62: 端口统计

地址	数量	描述	最小	最大	步长	单元	格式
0806	1	Port1 - Number of frames sent	0	4294967295	1	-	F9
0808	1	Port1 - Total bytes received	0	4294967295	1	-	F9
080A	1	Port1 - Total frames received	0	4294967295	1	-	F9
080C	1	Port1 - Number of broadcast frames received	0	4294967295	1	-	F9
080E	1	Port1 - Number of multicast frames received	0	4294967295	1	-	F9
0810	1	Port1 - Number of frames with CRC error	0	4294967295	1	-	F9
0812	1	Port1 - Number of oversized frames received	0	4294967295	1	-	F9
0814	1	Port1 - Number of bad fragments rcvd(<64 bytes)	0	4294967295	1	-	F9
0816	1	Port1 - Number of jabber frames received	0	4294967295	1	-	F9
0818	1	Port1 - Number of collisions occurred	0	4294967295	1	-	F9
081A	1	Port1 - Number of late collisions occurred	0	4294967295	1	-	F9
081C	1	Port1 - Number of 64-byte frames rcvd/sent	0	4294967295	1	-	F9
081E	1	Port1 - Number of 65-127 byte frames rcvd/sent	0	4294967295	1	-	F9
0820	1	Port1 - Number of 128-255 byte frames rcvd/sent	0	4294967295	1	-	F9
0822	1	Port1 - Number of 256-511 byte frames rcvd/sent	0	4294967295	1	-	F9
0824	1	Port1 - Number of 512-1023 byte frames rcvd/sent	0	4294967295	1	-	F9
0826	1	Port1 - Number of 1023-MAX byte frames rcvd/sent	0	4294967295	1	-	F9
0828	1	Port1 - Number of Mac Error Packets	0	4294967295	1	-	F9
082A	1	Port1 - Number of dropped received packets	0	4294967295	1	-	F9
082C	1	Port1 - Number of multicast frames sent	0	4294967295	1	-	F9
082E	1	Port1 - Number of broadcast frames sent	0	4294967295	1	-	F9
0830	1	Port1 - Number of <64 byte fragments w/ good CRC	0	4294967295	1	-	F9
		...					
147E	1	Port64 - Number of <64 byte fragments w/ good CRC	0	4294967295	1	-	F9

16.2.3 配置示例

在此示例中，您将设备配置为响应客户端请求。此配置的前提条件是，已为客户端设备配置指定范围内的 IP 地址。此示例中，*Write access* 功能将保持停用。激活 *Write access* 功能后，设备将允许您仅重置端口计数器。在默认设置下，*Modbus TCP* 和 *Write access* 功能停用。

Modbus TCP 协议不提供任何身份验证机制。如果激活 *Modbus TCP* 的写访问，则每个能使用 TCP/IP 访问设备的客户端都能够更改设备的设置。这反过来又会导致设备的不正确配置和网络中可能出现的问题。

注意

未经授权的设备访问风险

请仅在采取了额外措施（例如防火墙、VPN 等）的情况下激活写访问，以减少可能的未经授权的访问。

不遵守这些指示可能导致设备损坏。

请执行以下步骤：

- ☐ 打开 *Device Security* > *Management Access* > *IP Access Restriction* 对话框。
- ☐ 添加一个表格条目。为此，请单击 按钮。
- ☐ 在 *Index* 列的值为 2 的行中指定 IP 地址范围。为此，请输入以下值：
  - 在 *Address* 列中：10.17.1.0
  - 在 *Netmask* 列中：255.255.255.248
- ☐ 验证是否已勾选 *Modbus TCP* 列中的复选框。
- ☐ 激活 IP 地址范围。为此，请勾选 *Active* 列中的复选框。
- ☐ 暂时保存更改。为此，请单击 按钮。
- ☐ 打开 *Diagnostics* > *Status Configuration* > *Security Status* 对话框的 *Global* 选项卡。
- ☐ 验证是否已勾选与参数 *Modbus TCP active* 相关的复选框。
- ☐ 打开 *Advanced* > *Industrial Protocols* > *Modbus TCP* 对话框。
- ☐ 标准 *Modbus TCP* 监听端口（端口 502）为默认值。如果想监听其他 TCP 端口，请在 *TCP port* 字段中输入监听端口的值。
- ☐ 要启用该功能，请选择 *Operation* 框中的 *On* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 按钮。

启用 *Modbus TCP* 功能后，*Security Status* 功能会检测激活并在 *Basic Settings* > *System* 对话框的 *Security status* 框中显示警报。

`enable`	切换到特权执行模式。
`network management access add 2`	为网络中的地址范围创建条目。本示例中下一个可用索引的编号：2。
`network management access modify 2 ip 10.17.1.0`	指定 IP 地址。
`network management access modify 2 mask 29`	指定子网掩码。
`network management access modify 2 modbus-tcp enable`	指定设备允许 *Modbus TCP* 访问设备管理。
`network management access operation`	启用 IP 访问限制。

```
configure                                   切换到配置模式。
security-status monitor modbus-tcp-enabled  指定设备对 Modbus TCP 服务器的激活进行监控。
modbus-tcp operation                        激活 Modbus TCP 服务器。
modbus-tcp port <1..65535>                  指定用于 Modbus TCP 通信的 TCP 端口（可选）。
                                            默认值为端口 502。
show modbus-tcp                             显示 Modbus TCP 服务器设置。
Modbus TCP/IP server settings
--------------------------
Modbus TCP/IP server operation.............enabled
Write-access...............................disabled
Listening port.............................502
Max number of sessions.....................5
Active sessions............................0
show security-status monitor                显示安全状态设置。
Device Security Settings
Monitor
---------------------------------
Password default settings unchanged..........monitored
...
Write access using Ethernet Switch Configurator is possible....monitored
Loading unencrypted configuration from ENVM...monitored
IEC 61850 MMS is enabled.....................monitored
Modbus TCP/IP server active..................monitored
show security-status event                  显示已发生的安全状态事件。
Time stamp             Event                      Info
--------------------   ------------------------   ------
2014-01-01 01:00:39   password-change(10)           -
.....................................................
2014-01-01 01:00:39   ext-nvm-load-unsecure(21)     -
2014-01-01 23:47:40   modbus-tcp-enabled(23)        -
show network management access rules 1      显示索引 1 的受限的管理访问规则。
Restricted management access settings
-------------------------------------
Index.....................................1
IP Address................................10.17.1.0
Prefix Length.............................29
HTTP......................................yes
SNMP......................................yes
Telnet....................................yes
SSH.......................................yes
HTTPS.....................................yes
IEC61850-MMS..............................yes
Modbus TCP/IP.............................yes
Active....................................[x]
```

16.3 EtherNet/IP

EtherNet/IP 是全球广泛接受的标准化工业通信协议，由开放式网络设备供应商协会（ODVA）维护。此协议基于广泛使用的标准以太网传输协议 TCP/IP 和 UDP/IP。*EtherNet/IP* 由主要制造商提供支持，为工业领域的高效数据通信提供了广泛的基础。

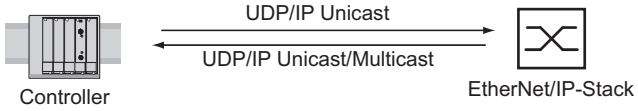


图 80: EtherNet/IP 网络

EtherNet/IP 将工业协议 CIP（通用工业协议）添加到了标准以太网协议。*EtherNet/IP* 在会话层及更高层实施 CIP，并调整 CIP 以在传输层及更低层应用特定的 *EtherNet/IP* 技术。在自动化应用中，*EtherNet/IP* 在应用级实施 CIP。因此，*EtherNet/IP* 是工业控制技术领域的理想选择。

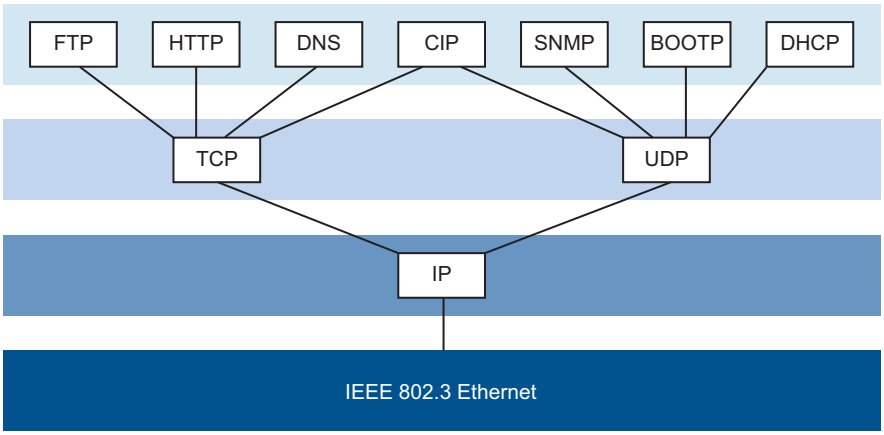


图 81: IEEE802.3 EtherNet/IP

有关 *EtherNet/IP* 的详细信息，请参见 ODVA 网站：www.odva.org。

16.3.1 集成在控制系统内

请执行以下步骤：

- ☐ 打开 *Switching > IGMP Snooping > Global* 对话框。
  确认已启用 *IGMP Snooping* 功能。
- ☐ 打开 *Advanced > Industrial Protocols > EtherNet/IP* 对话框。
  确认已启用 *EtherNet/IP* 功能。
- ☐ 打开 *Advanced > Industrial Protocols > EtherNet/IP* 对话框。
- ☐ 要将 EDS 以 ZIP 存档形式保存到您的 PC，请点击 *Download*。
  ZIP 存档包含 *EtherNet/IP* 配置文件和用于配置控制器与设备间连接的图标。

16.3.2 EtherNet/IP 实体参数

以下段落标识设备支持的对象和操作。

支持的操作

表格 63: 支持的 EtherNet/IP 对象示例请求概览

Service Code	Identity Object	TCP/IP Interface Object	Ethernet Link Object	Switch Agent Object	Base Switch Object
0x01 Get Attribute All	All attributes	All attributes	All attributes	All attributes	All attributes
0x02 Set Attribute All	–	Settable attributes (0x3, 0x5, 0x6, 0x8, 0x9, 0xA)	Settable attributes (0x6, 0x9)	–	–
0x0e Get Attribute Single	All attributes	All attributes	All attributes	All attributes	All attributes
0x10 Set Attribute Single	–	Settable attributes (0x3, 0x5, 0x6, 0x8, 0x9, 0xA, 0x64)	Settable attributes (0x6, 0x9, 0x65, 0x67, 0x68, 0x69, 0x6C)	Settable attributes (0x5, 0x7)	–
0x05 Reset	Parameter (0x0, 0x1)	–	–	–	–
0x35 Save Configuration Vendor specific	–	–	–	Save switch configuration	–
0x36 Mac Filter Vendor specific	–	–	–	Add MAC filter STRUCT of: USINT VlanId ARRAY of: 6 USINT Mac DWORD PortMask	–

标识对象

设备支持 *EtherNet/IP* 的标识对象 (Class Code 0x01)。Schneider Electric 制造商 ID 为 634。Schneider Electric 使用 ID 44 (0x2C) 来指示产品类型“Managed Ethernet Switch”。

表格 64: 实例属性（仅实例 1 可用）

Id	Attribute	Access Rule	Data type	Description
0x1	Vendor ID	Get	UINT	Schneider Electric634
0x2	Device Type	Get	UINT	Managed Ethernet Switch 44 (0x2C) (0x2C)
0x3	Product Code	Get	UINT	Product Code: mapping is defined for every device type
0x4	Revision	Get	STRUCT of: USINT Major USINT Minor	Revision of the EtherNet/IP implementation, 2.1.
0x5	Status	Get	WORD	Support for the following Bit status only: 0: Owned (always 1) 2: Configured (always 1) 4: Extend Device Status 5: 0x3: No I/O connection established 6: 0x7: At least one I/O connection established, all in idle mode. 7:
0x6	Serial number	Get	UDINT	Serial number of the device (contains last 3 Bytes of MAC address).
0x7	Product name	Get	SHORT-STRING	Displayed as "Schneider Electric" + product family + product ID + software variant.

TCP/IP 界面对象

设备仅支持 *EtherNet/IP* 的 TCP/IP 界面对象 (Class Code 0xF5) 的实例 1。

根据写访问状态，设备将完整配置存储在其闪存中。保存配置文件可能最多需要 10 秒。如果保存过程被中断，例如，由于电源不工作，那么设备的操作可能是不可能的。

提示：设备会向配置更改 Get Request 发送带有 Response 的应答，尽管配置可能未完整保存。

表格 65: 类属性

Id	Attribute	Access Rule	Data type	Description
0x1	Revision	Get	UINT	Revision of this object: 3
0x2	Max Instance	Get	UINT	Maximum instance number: 1
0x3	Number of instance	Get	UINT	Number of object instances currently created: 1

表格 66: 实例 1 的属性

Id	Attribute	Access Rule	Data type	Description
0x1	Status	Get	DWORD	0: Interface Status (0=Interface not configured, 1=Interface contains valid config) 6: ACD status (default 0) 7: ACD fault (default 0)
0x2	Interface Capability flags	Get	DWORD	0: BOOTP Client 1: DNS Client 2: DHCP Client 3: DHCP-DNS Update 4: Configuration setable (within CIP) Other bits reserved (0) 7: ACD capable (0=not capable, 1=capable)
0x3	Config Control	Set/Get	DWORD	0: 1: 2: 3: 0x0=using stored config 0x1=using BOOTP 0x2=using DHCP 4: One device uses DNS for name lookup (always 0 because it is not supported) Other bits reserved (0)
0x4	Physical Link Object	Get	STRUCT of: UINT PathSize EPATH Path	Path to the Physical Link Object, always {0x20, 0xF6, 0x24, 0x01} describing instance 1 of the Ethernet Link Object.
0x5	Interface Configuration	Set/Get	STRUCT of: UDINT IpAddress UDINT Netmask UDINT GatewayAddress UDINT NameServer1 UDINT NameServer2 STRING DomainName	IP Stack Configuration (IP-Address, Netmask, Gateway, 2 Name servers (DNS, if supported) and the domain name).
0x6	Host Name	Set/Get	STRING	Host Name (for DHCP DNS Update)
0x7	Safety Network Number			Not supported
0x8	TTL Value	Get/Set	USINT	Time to live value for IP multicast packets Range 1..255 (default = 1)

表格 66: 实例 1 的属性

Id	Attribute	Access Rule	Data type	Description
0x9	Mcast Config	Get/Set	STRUCT of: USINT AllocControl USINT reserved UINT NumMcast UDINT McastStartAddr	Alloc Control = 0 Number of IP multicast addresses = 32 Multicast start address = 239.192.1.0
0xA	Selected Acd	Get/Set	BOOL	0=ACD disable 1=ACD enable (default)
0xB	Last Conflict Detected	Get	STRUCT of: USINT AcdActivity ARRAY of: 6 USINT RemoteMac ARRAY of: 28 USINT ArpPdu	ACD Diagnostic Parameters

表格 67: TCP/IP 界面对象的 Schneider Electric 扩展

Id	Attribute	Access Rule	Data type	Description
0x64	Cable Test	Set/Get	STRUCT of: USINT Interface USINT Status	Interface Status (1=Active, 2=Success, 3=Failure, 4=Uninitialized)
0x65	Cable Pair Size	Get	USINT	Size of the Cable Test Result STRUCT of: 2 Pair for 100BASE 4 Pair for 1000BASE

表格 67: TCP/IP 界面对象的 Schneider Electric 扩展

Id	Attribute	Access Rule	Data type	Description

0x66	Cable Test Result	Get	STRUCT of:
			USINT Interface
			USINT CablePair
			USINT CableStatus
			USINT CableMinLength
			USINT CableMaxLength
			USINTCableFailureLocation
				100BASE:{
				{Interface, CablePair1, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair2, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				}
				1000BASE:{
				{Interface, CablePair1, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair2, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair3, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				{Interface, CablePair4, CableStatus, CableMinLength, CableMaxLength, CableFailureLocation}
				}

以太网链接对象

以下两个表格中的信息是以太网链接对象的一部分。要访问这些信息，请使用以下数值。

- Class(####)
- Instance(###)
- Attribute(#)

例如，应用*class*、*instance*和*attribute*的数值来访问使用明确消息的利用率警报。

- Class = 0xF6
- Instance = 1
- Attribute = 6

表格 68: 实例属性和Schneider Electric扩展到以太网链接对象

Id	Attribute	Access Rule	Data type	Description
实例属性				
0x1	Interface Speed	Get	UDINT	Used interface speed in MBit/s (10, 100, 1000, …). 0 is used when the speed has not been determined or is invalid because of detected errors.
0x2	Interface Flags	Get	DWORD	Interface Status Flags: 0: Link State (0=No link, 1=Link) 1: Duplex mode (0=Half, 1=Full) 2: Auto-Negotiation Status 3: 4: 0x0=Auto-Negotiation in progress 0x1=Auto-Negotiation failed 0x2=Failed but speed detected 0x3=Auto-Negotiation success 0x4=No Auto-Negotiation 5: Manual configuration require reset (always 0 because it is not needed) 6: Hardware error
0x3	Physical Address	Get	ARRAY of: 6 USINT	MAC address of physical interface
0x4	Interface Counters	Get	STRUCT of: UDINT MibIICounter1 UDINT MibIICounter2 …	InOctets, InUcastPackets, InNUcastPackets, InDiscards, InErrors, InUnknownProtos, OutOctets, OutUcastPackets, OutNUcastPackets, OutDiscards, OutErrors
0x5	Media Counters	Get	STRUCT of: UDINT EthernetMib Counter1 UDINT EthernetMib Counter2 …	检测到的错误： Alignment, FCS, single collision, multiple collision, SQE Test, deferred transmissions, late collisions, excessive collisions, MAC TX, carrier sense, frame too long, MAC RX
0x6	Interface Control	Get/Set	STRUCT of: WORD ControlBits	Control Bits: 0: Auto-negotiation enable/disable (0=disable, 1=enable) 1: Duplex mode (0=Half, 1=Full), if Auto-negotiation disabled
			UINT ForcedInterface Speed	Interface speed in MBits/s: 10,100,…, if Auto-negotiation disabled

表格 68: 实例属性和Schneider Electric扩展到以太网链接对象

Id	Attribute	Access Rule	Data type	Description
0x7	Interface type	Get	USINT	Type of interface: 0: Unknown interface type 1: The interface is internal 2: Twisted-pair 3: Optical fiber
0x8	Interface state	Get	USINT	Current state of the interface: 0: Unknown interface state 1: The interface is enabled 2: The interface is disabled 3: The interface is testing
0x9	Admin State	Set/Get	USINT	Administrative state: 1: Enable the interface 2: Disable the interface
0xA	Interface label	Get	SHORT-STRING	Human readable ID
以太网链接对象的 Schneider Electric 扩展				
0x64	Ethernet Interface Index	Get	USINT	Interface/Port Index (ifIndex out of MIBII)
0x65	Port Control	Get/Set	DWORD	0: Link state (0=link down, 1=link up)
				1: Link admin state (0=disabled, 1=enabled)
				8: Access violation alarm (read-only)
				9: Utilization alarm (read-only)
0x66	Interface Utilization	Get	USINT	The existing Counter out of the private MIB hm2IDiagfaceUtilization is used. Utilization in percentage (Unit 1%=100, %/100). RX Interface Utilization.
0x67	Interface Utilization Alarm Upper Threshold	Get/Set	USINT	Within this parameter the variable hm2DiagIfaceUtilizationAlarmUpperThreshold can be accessed. Utilization in percentage (Unit 1%=100). RX Interface Utilization Upper Limit.
0x68	Interface Utilization Alarm Lower Threshold	Get/Set	USINT	Within this parameter the variable hm2DiagIfaceUtilizationAlarmLowerThreshold can be accessed. Utilization in percentage (Unit 1%=100). RX Interface Utilization Lower Limit.
0x69	Broadcast limit	Get/Set	USINT	Broadcast limiter Service (Egress BC-Frames limitation, 0=disabled), Frames/second
0x6A	Ethernet Interface Description	Get/Set	STRING	Interface/Port Description (from MIB II ifDescr), for example "Unit: 1 Slot: 2 Port: 1 - 10/100 Mbit TX" or "unavailable", max. 64 Bytes.

表格 68: 实例属性和Schneider Electric扩展到以太网链接对象

Id	Attribute	Access Rule	Data type	Description
0x6B	Port Monitor	Get/Set	DWORD	0: Link Flap (0=Off, 1=On) 1: CRC/Fragment (0=Off, 1=On) 2: Duplex Mismatch (0=Off, 1=On) 3: Overload-Detection (0=Off, 1=On) 4: Link-Speed/ Duplex Mode (0=Off, 1=On) 5: Deactivate port action (0=Off, 1=On) 6: Send trap action (0=Off, 1=On) 7: Active Condition (displays which condition caused an action to occur) 8: 9: 00001_B: Link Flap 10: 00010_B: CRC/Fragments 11: 00100_B: Duplex Mismatch 01000_B: Overload-Detection 10000_B: Link-Speed/ Duplex mode 12: Reserved (always 0) 13: Reserved (always 0) 14: Reserved (always 0) 15: Reserved (always 0)
0x6C	Quick Connect	Get/Set	USINT	Quick Connect on the interface (0=Off, 1=On) If you enable Quick Connect, then the device sets the port speed to 100FD, disables Auto-Negotiation, and Spanning Tree on the interface.
0x6D	SFP Diagnostics	Get	STRUCT of:	
			STRING ModuleType	
			SHORT-STRING SerialNumber	
			USINT Connector	
			USINT Supported	
			DINT Temperature	in °C
			DINT TxPower	in mW
			DINT RxPower	in mW
			DINT RxPower	in dBm
			DINT TxPower	in dBm

表格 69: 以太网链接对象实体的端口分配

Ethernet Port	Ethernet Link Object Instance
CPU	1
1	2
2	3
3	4
4	5
…	…

提示: 端口的数量取决于使用的硬件类型。只有连接端口后才存在以太网链接对象。

交换机代理对象

设备支持特定于 Schneider Electric 的以太网交换机代理对象 (Class Code 0x95) 以用于设备配置和实例 1 的信息参数。

表格 70: 类属性

Id	Attribute	Access Rule	Data type	Description	
0x1	Switch Status	Get	DWORD	0:	Like the signal contact, the value indicates the Device Overall state (0=ok, 1=failed)
				1:	Device Security Status (0=ok, 1=failed)
				2:	Power Supply 1 (0=ok, 1=failed)
				3:	Power Supply 2 (0=ok, 1=failed or not existing)
				4:	Reserved
				5:	Reserved
				6:	Signal Contact 1 (0=closed, 1=open)
				7:	Signal Contact 2 (0=closed, 1=open or not existing)
				8:	Reserved
				9:	Temperature (0=ok, 1=failure)
				10:	Module removed (1=removed)
				11:	EAM removed (1=removed)
				12:	EAM-SD removed (1=removed)
				13:	Reserved
				14:	Reserved
				15:	Reserved
				16:	Reserved
				17:	Reserved
				18:	Reserved
				19:	Reserved
				20:	Reserved
				21:	Reserved
				22:	Reserved
				23:	MRP (0=disabled, 1=enabled)
				24:	Reserved
				25:	Reserved
				26:	RSTP (0=disabled, 1=enabled)
				27:	LAG (0=disabled, 1=enabled)
				28:	Reserved
				29:	Reserved
				30:	Reserved
				31:	Connection Error (1=failure)

表格 70: 类属性

Id	Attribute	Access Rule	Data type	Description
0x2	Switch Temperature	Get	STRUCT of:	
			INT TemperatureF	in °F
			INT TemperatureC	in °C
0x3	Reserved	Get	UDINT	Reserved for future use (always 0)
0x4	Switch Max Ports	Get	UINT	Maximum number of Ethernet Switch Ports
0x5	Multicast Settings (IGMP Snooping)	Get/Set	WORD	0: IGMP Snooping (0=disabled, 1=enabled) 1: IGMP Querier (0=disabled, 1=enabled) 2: IGMP Querier Mode (read-only) (0=Non-Querier, 1=Querier) 3: 4: 5: 6: 7: IGMP Querier Packet Version Off=0 IGMP Querier disabled V1=1 V2=2 V3=3 8: 9: 10: Treatment of Unknown Multicasts: 0=Send To All Ports 2=Discard
0x6	Switch Existing Ports	Get	ARRAY of: DWORD	Bitmask of existing switch ports Per bit starting with Bit 0 (=Port 1) (0=Port not available, 1=Port existing) Array (bit mask) size is adjusted to the size of maximum number of switch ports (for max. 28 Ports 1 DWORD is used)
0x7	Switch Port Control	Get/Set	ARRAY of: DWORD	Bitmask Link Admin Status switch ports Per bit starting with Bit 0 (=Port 1) (0=Port enabled, 1=Port disabled) Array (bit mask) size is adjusted to the size of maximum number of Switch ports (for max. 28 Ports 1 DWORD is used)
0x8	Switch Ports Mapping	Get	ARRAY of: USINT	Instance number of the Ethernet-Link-Object Starting with Index 0 (=Port 1) All Ethernet Link Object Instances for the existing Ethernet Switch Ports (1..N, maximum number of ports). When the entry is 0, the Ethernet Link Object for this port does not exist

表格 70: 类属性

Id	Attribute	Access Rule	Data type	Description
0x9	Switch Action Status	Get	DWORD	Status of the last executed action (for example config save, software update, etc.) 0: Flash Save Configuration In Progress/Flash Write In Progress 1: Flash Save Configuration Failed/Flash Write Failed 4: Configuration changed (configuration not in sync. between running configuration

特定于 Schneider Electric 的以太网交换机代理对象让您可以使用更多特定于供应商的服务，并可以使用 Service Code 0x35 保存交换机配置。从您的 PC 发送保存设备配置的请求时，设备会在将配置保存到闪存后发送应答。

基本交换机对象

基本交换机对象提供连接到管理型以太网交换机（修订版本 1）基本状态信息的 CIP 应用级接口。

仅基本交换机 (Class Code 0x51) 的实例 1 可用。

表格 71: 实例属性

Id	Attribute	Access Rule	Data type	Description
0x1	Device Up Time	Get	UDINT	Time since the device powered up
0x2	Total port count	Get	UDINT	Number of physical ports
0x3	System Firmware Version	Get	SHORT-STRING	Human readable representation of System Firmware Version
0x4	Power source	Get	WORD	Status of switch power source
0x5	Port Mask Size	Get	UINT	Number of DWORD in port array attributes
0x6	Existing ports	Get	ARRAY of: DWORD	Port Mask
0x7	Global Port Admin State	Get	ARRAY of: DWORD	Port Admin Status
0x8	Global Port link Status	Get	ARRAY of: DWORD	Port Link Status
0x9	System Boot Loader Version	Get	SHORT-STRING	Readable System Firmware Version
0xA	Contact Status	Get	UDINT	Switch Contact Closure

表格 71: 实例属性

Id	Attribute	Access Rule	Data type	Description
0xB	Aging Time	Get	UDINT	Range 10..1000000 · 1/10 seconds (default=300) 0=Learning off
0xC	Temperature C	Get	UINT	Switch temperature in degrees Celsius
0xD	Temperature F	Get	UINT	Switch temperature in degrees Fahrenheit

RSTP 网桥对象 (MCSESM-E)

RSTP 是第 2 层协议，它允许使用冗余以太网拓扑（例如环网）。在 IEEE 802.1D-2004 第 17 章对 RSTP 进行了详细的说明。

设备支持配置和信息参数 Schneider Electric特有的 RSTP 网桥对象（分类码 64_H，100）。

设备支持 2 个实体：
- 实体 1 代表网桥的主 RSTP 实体，
- 实体 2 代表二级 RSTP（双）实体。

这些参数的详细信息和参数设置方法请参见“图形用户界面”参考手册。

表格 72: Schneider Electric RSTP 网桥对象

Id	Attribute	Access rule	Data type	Description
1	Bridge Identifier Priority	Set	UDINT	Range: 0 to 61,440 in steps of 4,096, default: 32,768 (refer to IEEE, 802.1D-2004, § 17.13.7)
2	Transmit Hold Count	Set	UINT	Range: 1 to 40, default: 10 (refer to IEEE 802.1D-2004, §17.13.12)
3	Force Protocol Version	Set	UINT	Default:2 (refer to IEEE 802.1D-2004, §17.13.4 and dot1dStpVersion in RFC 4318)
4	Bridge Hello Time	Set	UDINT	Range: 100 to 200, unit: centi-seconds (1/100 of a second), default: 200 (refer to IEEE 802.1D-2004, §17.13.6 and dot1dStpHoldTime in RFC 4188)
5	Bridge Forward Delay	Set	UDINT	Range: 400 to 3000, unit: centi-seconds, default: 2100 (refer to IEEE 802.1D-2004, §17.13.5 and dot1dStpForwardDelay in RFC 4188)
6	Bridge Max. Age	Set	UINT	Range: 600 to 4000, unit: centi-seconds, default: 4000 (refer to IEEE 802.1D-2004, §17.13.8 and dot1dStpBridgeMaxAge in RFC 4188)
7	Time Since Topology Change	Get	UDINT	Unit: centi-seconds (refer to dot1dStpTimeSinceTopologyChange in RFC 4188)

表格 72: Schneider Electric RSTP 网桥对象

Id	Attribute	Access rule	Data type	Description
8	Topology Change	Get	UDINT	Refer to dot1dStpTopChanges in RFC 4188
100	InnerPort	Get	UINT	Schneider Electric-specific object. ▶ For instance 1, it holds the port number of the DRSTP Primary instance ‘s inner port. ▶ For instance 2, it holds the port number of the DRSTP Secondary instance ‘s inner port.
101	OuterPort	Get	UINT	Schneider Electric-specific object. ▶ For instance 1, it holds the port number of the DRSTP Primary instance ‘s outer port. ▶ For instance 2, it holds the port number of the DRSTP Secondary instance ‘s outer port.

RSTP 端口对象 (MCSESM-E)

设备支持 RSTP 端口配置及信息参数和至少一个实体 (instance 1) 的Schneider Electric 特有 RSTP 端口对象（分类码 65_H，101）。

实体 1 代表 CPU 以太网接口，实体 2 代表第 1 个物理端口，实体 3 代表第 2 个物理端口等等。

这些参数的详细信息和参数设置方法请参见“图形用户界面”参考手册。

表格 73: Schneider Electric RSTP 端口对象

Id	Attribute	Access rule	Data type	Description
1	Port Identifier Priority	Set	UDINT	Range: 0 to 240 in steps of 16, default: 128 (refer to IEEE, 802.1D-2004, § 17.13.10).
2	mcheck	Set	BOOL	True (1), False (2) (refer to IEEE 802.1D-2004, §17.19.13 and dot1dStpPortProtocolMigration in RFC 4318).
3	Port Path Cost	Set	UDINT	Range: 1 to 200,00,000, default:auto (0) (refer to IEEE 802.1D-2004, §17.13.11 and dot1dStpPortAdminPathCost in RFC 4318).
4	Port Admin Edge Port	Set	BOOL	True (1), False (2) (refer to IEEE 802.1D-2004, §17.13.1 and dot1dStpPortAdminEdgePort in RFC 4318).
5	Port Oper Edge Port	Get	BOOL	True (1), False (2) (refer to dot1dStpPortOperEdgePort in RFC 4318).
6	Port Admin PointToPoint	Set	UINT	forceTrue (0), forceFalse (1), auto (2) (refer to dot1dStpPortAdminPointToPoint in RFC 4318).
7	Port Oper PointToPoint	Get	UINT	True (1), False (2) (refer to dot1dStpPortOperPointToPoint in RFC 4318).
8	Port Enable	Set	UINT	Enabled (1), Disabled (2) (Refer to dot1dStpPortEnable in RFC 4188).

表格 73: Schneider Electric RSTP 端口对象

Id	Attribute	Access rule	Data type	Description
9	Port State	Get	UINT	Disabled (1), Blocking (2), Listening (3), Learning (4), Forwarding (5), Broken (6) (refer to dot1dStpPortState in RFC 4188).
10	Port Role	Get	UNT	Unknown (0), Alternate/Backup (1), Root (2), Designated (3) (refer to dot1dStpTopChanges in RFC 4188).
100	DRSTP	Get	UINT	Schneider Electric-specific object. True (1), False (2).

服务、连接和 I/O 数据

设备支持以下连接类型和参数。

表格 74: 集成新模块的设置

Setting	I/O connection	Input only	Listen only
Comm Format:	Data - DINT	Data - DINT	Input Data - DINT - Run/Program
IP Address	IP address of the device	IP address of the device	IP address of the device
Input Assembly Instance	100	100	100
Input Size	32	32	32
Output Assembly Instance	150	152	153
Output Size	32	0	0
Configuration Assembly Instance	151	151	151
Data Size	10	10	10

表格 75: 设备 I/O 数据结构

I/O Data	Value (data types and sizes to be defined)	Direction	Size[1]
Device Status	Bitmask (see Switch Agent Attribute 0x1)	Input	DWORD
Link Status	Bitmask, 1 Bit per port (0=No link, 1=Link up)	Input	DWORD
Output Links Admin State applied	Bitmask (1 Bit per port) to acknowledge output. Link state change can be denied, for example for controller access port. (0=Port enabled, 1=Port disabled)	Input	DWORD
Utilization Alarm[2]	Bitmask, 1 Bit per port (0=No alarm, 1=Alarm on port)	Input	DWORD
Access Violation Alarm[3]	Bitmask, 1 Bit per port (0=No alarm, 1=Alarm on port)	Input	DWORD
Multicast Connections	Integer, number of connections	Input	DINT

表格 75: 设备 I/O 数据结构

I/O Data	Value (data types and sizes to be defined)	Direction	Size[1]
TCP/IP Connections	Integer, number of connections	Input	DINT
Quick Connect Mask	Bitmask (1 Bit per port) (0=Quick Connect disabled, 1=Quick Connec enabled)	Input	DINT
Link Admin State	Bitmask, 1 Bit per port (0=Port enabled, 1=Port disabled)	Output	DWORD

1. 端口位掩码的默认大小为 32 位 (DWORD)。对于端口为 28 个以上的设备，位掩码扩展为 n * DWORD。
2. 您可以在 *Basic Settings > Port* 对话框的 *Utilization* 选项卡中指定利用率警报。阈值上限是激活警报条件的界限。阈值下限是激活的警报条件被停用的界限。
3. 您可以在 *Network Security > Port Security* 对话框中指定访问违规警报。阈值上限是激活警报条件的界限。阈值下限是激活的警报条件被停用的界限。

表格 76: 将数据类型映射为位大小

对象类型	位大小
BOOL	1 bit
DINT	32 bit
DWORD	32 bit
SHORT-STRING	max. 32 bytes
STRING	max. 64 bytes
UDINT	32 bit
UINT	16 bit
USINT	8 bit
WORD	16 bit

A 建立配置环境

A.1 设置 DHCP/BOOTP 服务器

以下示例描述了使用 haneWIN DHCP Server 软件对 DHCP 服务器进行的配置。这款共享软件是 IT-Consulting Dr. Herbert Hanewinkel 的产品。您可以从 www.hanewin.net 下载该软件。该软件试用期为首次安装之日起 30 个日历日，之后您可以决定是否希望购买许可证。

请执行以下步骤：

- ☐ 在你的电脑上安装DHCP服务器。
  要进行安装，请遵循安装助手的说明。
- ☐ 启动 *haneWIN DHCP Server* 程序。

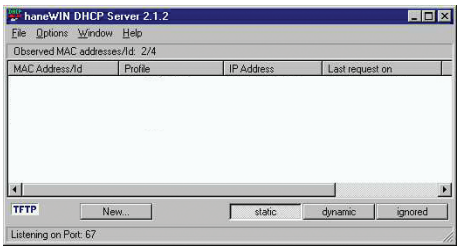


图 82: haneWIN DHCP Server 程序的启动窗口

提示： Windows 启动后，安装过程包括一项在基本配置中自动启动的服务。即使该程序本身尚未启动，此软件也能激活。启动后，该服务会对 DHCP 查询作出响应。

- ☐ 在菜单栏中，点击项目 *Options > Preferences* 以打开程序设置窗口。
- ☐ 选择 *DHCP* 选项卡。
- ☐ 指定图中显示的设置。

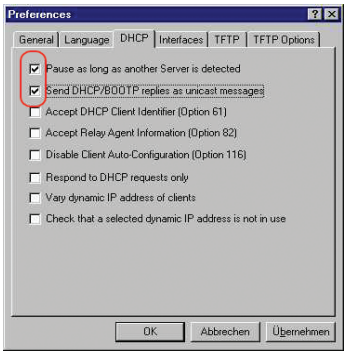


图 83: DHCP 设置

- ☐ 点击 *OK* 按钮。
- ☐ 要输入配置概要文件，请在菜单栏中点击项目 *Options > Configuration Profiles*。

☐ 指定新配置概要文件的名称。

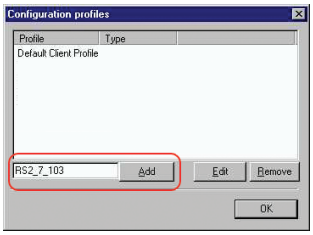


图 84: 添加配置概要文件

☐ 点击 *Add* 按钮。
☐ 指定子网掩码。

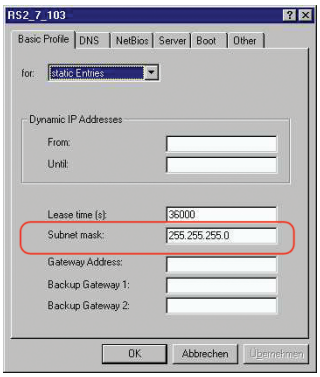


图 85: 配置概要文件中的子网掩码

☐ 点击 *Apply* 按钮。
☐ 选择 *Boot* 选项卡。
☐ 输入您的 TFTP 服务器的 IP 地址。
☐ 输入配置概要文件的路径和文件名。

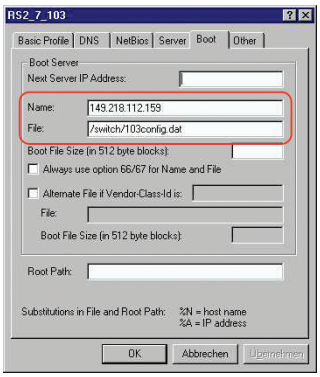


图 86: TFTP 服务器上的配置文件

☐ 点击 *Apply* 按钮，然后点击 *OK* 按钮。

☐ 为每种设备类型添加一个概要文件。
当相同类型的设备具有不同配置时，可以为每种配置添加一个概要文件。

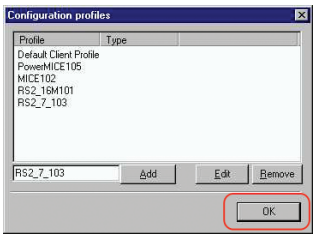


图 87: 管理配置概要文件

☐ 要完成添加配置概要文件的操作，请点击 *OK* 按钮。
☐ 要输入静态地址，请在主窗口中点击 *Static* 按钮。

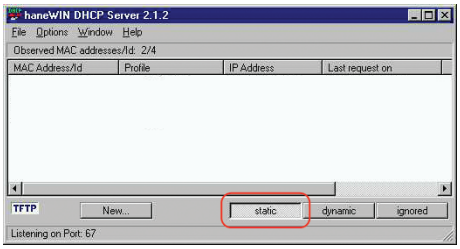


图 88: 静态地址输入

☐ 点击 *Add* 按钮。

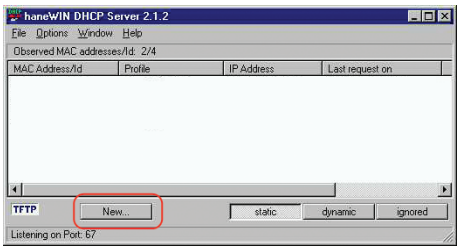


图 89: 添加静态地址

☐ 输入设备的 MAC 地址。
☐ 输入设备的 IP 地址。

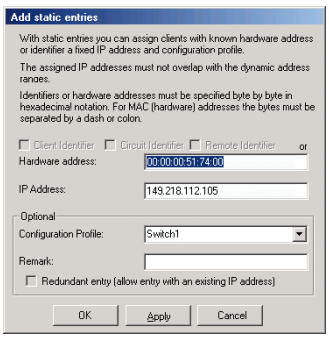


图 90: 静态地址条目

☐ 选择设备的配置概要文件。

- ☐ 点击 *Apply* 按钮，然后点击 *OK* 按钮。
- ☐ 为将从 DHCP 服务器获取参数的每个设备添加一个条目。

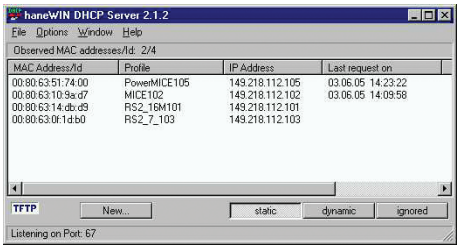


图 91: 带有条目的 DHCP 服务器

A.2 设置具有选项 82 的 DHCP 服务器

以下示例描述了使用 haneWIN DHCP Server 软件对 DHCP 服务器进行的配置。这款共享软件是 IT-Consulting Dr. Herbert Hanewinkel 的产品。您可以从 www.hanewin.net 下载该软件。该软件试用期为首次安装之日起 30 个日历日，之后您可以决定是否希望购买许可证。

请执行以下步骤：

- ☐ 在你的电脑上安装DHCP服务器。
  要进行安装，请遵循安装助手的说明。
- ☐ 启动 *haneWIN DHCP Server* 程序。

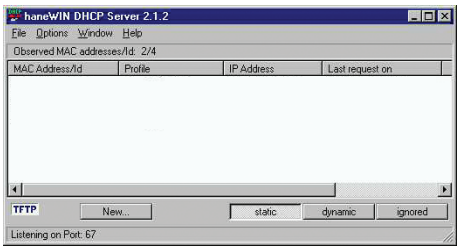


图 92: haneWIN DHCP Server 程序的启动窗口

提示： Windows 启动后，安装过程包括一项在基本配置中自动启动的服务。即使该程序本身尚未启动，此软件也能激活。启动后，该服务会对 DHCP 查询作出响应。

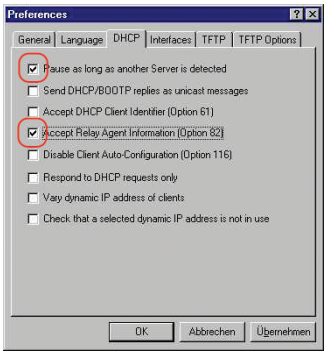


图 93: DHCP 设置

- 要输入静态地址，请点击 *Add* 按钮。

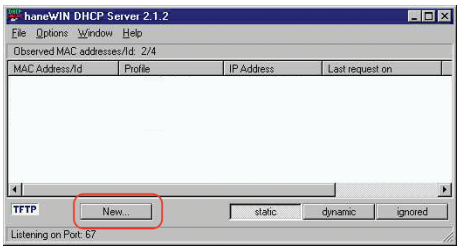


图 94: 添加静态地址

- 勾选 *Circuit Identifier* 复选框。
- 勾选 *Remote Identifier* 复选框。

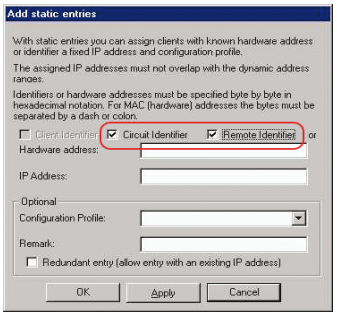


图 95: 固定地址分配的默认设置

- 在 *Hardware address* 字段中，分别为交换机和端口指定值 *Circuit Identifier* 和值 *Remote Identifier*。
  DHCP 服务器会将 *IP address* 字段中指定的 IP 地址分配给连接到 *Hardware address* 字段中指定的端口的设备。
  硬件地址采用以下格式：
  ciclvvvvssmmpprirlxxxxxxxxxxxx
  - ci
    电路 ID 类型的子标识符
  - cl
    电路 ID 的长度。
  - Schneider Electric 标识符：
    01（Schneider Electric 设备连接到该端口时），00（其他情况）。
  - vvvv
    DHCP 请求的 VLAN ID。
    默认设置：0001 = VLAN 1
  - ss

具有该端口的模块所在且与设备相连的设备插座。指定值 00。

- mm
  具有与设备相连的端口的模块。
- pp
  与设备相连的端口。
- ri
  远程 ID 类型的子标识符
- rl
  远程 ID 的长度。
- xxxxxxxxxxxx
  与一个设备相连的设备的远程 ID（如：MAC 地址）。

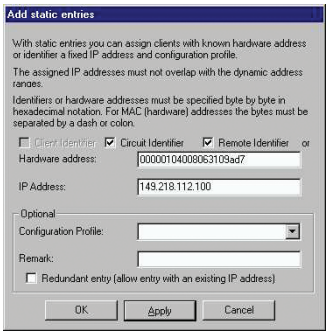


图 96: 指定地址

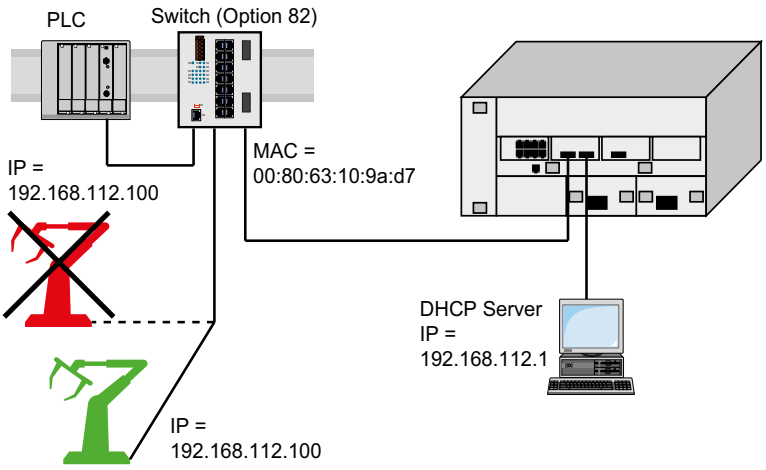


图 97: 使用选项 82 的应用示例

A.3 做好通过 SSH 进行访问的准备

您可以使用 SSH 连接到设备。为此，请执行以下步骤：
- ▶ 在设备中生成一个密钥。
  或者
- ▶ 将您自己的密钥转移到设备上。
- ▶ 做好在 SSH 客户端程序中访问设备的准备。

提示：在默认设置下，密钥已经存在，使用 SSH 进行访问的功能已启用。

A.3.1 在设备中生成一个密钥

设备允许用户在设备中直接生成密钥。为此，请执行以下步骤：

- ☐ 打开 *Device Security > Management Access > Server* 对话框的 *SSH* 选项卡。
- ☐ 要禁用 SSH 服务器，请选择 *Operation* 框中的 *Off* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 ✓ 按钮。
- ☐ 要创建一个 RSA 密钥，请在 *Signature* 框中点击 *Create* 按钮。
- ☐ 要启用 SSH 服务器，请选择 *Operation* 框中的 *On* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 ✓ 按钮。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`ssh key rsa generate`	生成一个新的 RSA 密钥。

A.3.2 将您自己的密钥加载到设备上

OpenSSH 允许资深网络管理员选择生成一个自己的密钥。要生成密钥，请在您的 PC 上输入以下命令：

```
ssh-keygen(.exe) -q -t rsa -f rsa.key -C '' -N ''
rsaparam -out rsaparam.pem 2048
```

设备允许用户将自己的 SSH 密钥转移到设备上。为此，请执行以下步骤：

- ☐ 打开 *Device Security > Management Access > Server* 对话框的 *SSH* 选项卡。
- ☐ 要禁用 SSH 服务器，请选择 *Operation* 框中的 *Off* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 ✓ 按钮。
- ☐ 当主机密钥位于用户 PC 中或网络驱动器上时，将包含密钥的文件拖放到 区域中。也可点击该区域以选择该文件。

- ☐ 点击 *Key import* 框中的 *Start* 按钮，将密钥加载到设备上。
- ☐ 要启用 SSH 服务器，请选择 *Operation* 框中的 *On* 单选按钮。
- ☐ 暂时保存更改。为此，请单击 ✔ 按钮。

请执行以下步骤：
- ☐ 将自己生成的密钥从您的 PC 复制到外部存储器。
- ☐ 将该密钥从外部存储器复制到设备中。

`enable`	切换到特权执行模式。
`copy sshkey envm <file name>`	将您自己的密钥从外部存储器加载到设备上。

A.3.3 准备 SSH 客户端程序

PuTTY 程序允许用户使用 SSH 访问设备。您可以从 www.putty.org下载该软件。

请执行以下步骤：
- ☐ 双击启动该程序。

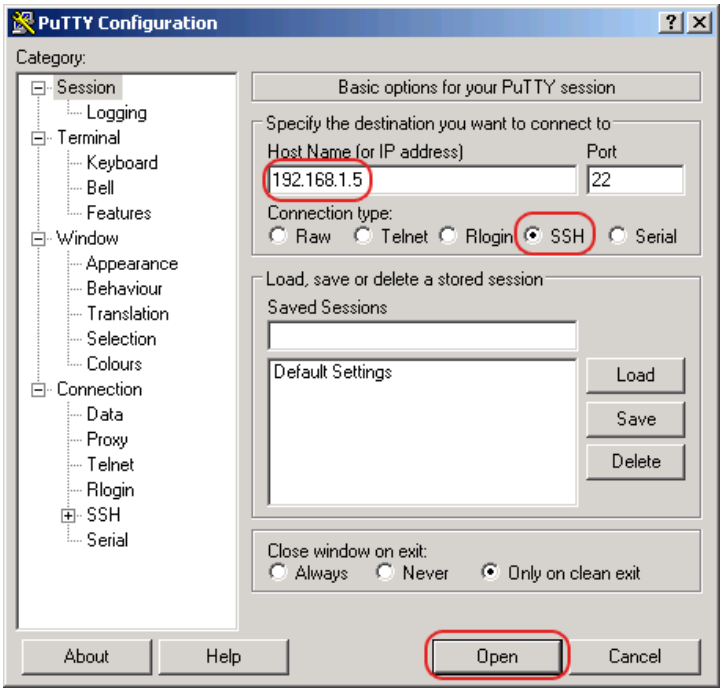


图 98: PuTTY 输入屏幕

- ☐ 在 *Host Name (or IP address)* 字段中，可以输入您设备的 IP 地址。
  该 IP 地址 (a.b.c.d) 由 4 个数值范围为 0 到 255 的十进制数字组成。这 4 个十进制数字由点隔开。
- ☐ 要选择连接类型，请在 *Connection type* 选项列表中选择 *SSH* 单选按钮。
- ☐ 点击 *Open* 按钮，建立至您设备的数据连接。

在连接建立之前，*PuTTY* 程序会显示一条安全警报消息，并允许您检查密钥指纹。

图 99: 针对指纹的安全警告提示

在连接建立之前，*PuTTY* 程序会显示一条安全警报消息，并允许您检查密钥指纹。

- ☐ 检查密钥指纹，以帮助确保您确实已经连接到所需设备。
- ☐ 当指纹与您的密钥匹配时，点击 *Yes* 按钮。

对于资深网络管理员，通过 SSH 访问设备的另一种方法就是使用 OpenSSH 套件。要建立数据连接，请输入以下命令：

```
ssh admin@10.0.112.53
```

admin 是用户名。

10.0.112.53 是您设备的 IP 地址。

A.4 HTTPS 证书

您的 Web 浏览器使用 HTTPS 协议建立至设备的连接。前提条件是，您已启用 *Device Security* > Management Access > *Server* 对话框 *HTTPS server* 选项卡中的 *HTTPS* 功能。

提示： Web 浏览器等第三方软件根据到期日和当前密码参数建议等标准对证书进行验证。过时的证书可能会由于无效或过时的信息而导致问题。示例：过期的证书或更改的加密建议。为了解决与第三方软件的验证冲突，请将您自己的最新证书转移到设备上或使用最新固件重新生成证书。

A.4.1 HTTPS 证书管理

加密需要符合 X.509/PEM（公钥基础设施）的标准证书。在默认设置下，设备中已经存在一个自我生成的证书。为此，请执行以下步骤：

- ☐ 打开 *Device Security* > *Management Access* > *Server* 对话框的 *HTTPS* 选项卡。
- ☐ 要创建一个 X509/PEM 证书，请在 *Certificate* 框中点击 *Create* 按钮。
- ☐ 暂时保存更改。为此，请单击 ✓ 按钮。
- ☐ 重新启动 HTTPS 服务器，激活该密钥。使用命令行界面重新启动服务器。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`https certificate generate`	生成一个 https X.509/PEM 证书。
`no https server`	禁用 *HTTPS* 功能。
`https server`	启用 *HTTPS* 功能。

☐ 设备还允许用户将一个外部生成的 X.509/PEM 证书转移到设备上：

- ☐ 打开 *Device Security* > *Management Access* > *Server* 对话框的 *HTTPS* 选项卡。
- ☐ 当证书位于用户 PC 中或网络驱动器上时，将该证书拖放到 区域中。也可点击该区域内部选择该证书。
- ☐ 点击 *Start* 按钮，将该证书复制到设备。
- ☐ 暂时保存更改。为此，请单击 ✓ 按钮。

`enable`	切换到特权执行模式。
`copy httpscert envm <file name>`	将 HTTPS 证书从外部永久存储器复制到设备中。
`configure`	切换到配置模式。
`no https server`	禁用 *HTTPS* 功能。
`https server`	启用 *HTTPS* 功能。

提示： 要在创建或转移之后激活证书，请重新启动设备或重新启动 HTTPS 服务器。使用命令行界面重新启动 HTTPS 服务器。

A.4.2 通过 HTTPS 进行访问

HTTPS 数据连接的默认设置是 TCP 端口 443。如果您更改 HTTPS 端口的编号，则请重新启动设备或 HTTPS 服务器。如此，更改即可生效。为此，请执行以下步骤：

- ☐ 打开 *Device Security > Management Access > Server* 对话框的 *HTTPS* 选项卡。
- ☐ 要启用该功能，请选择 *Operation* 框中的 *On* 单选按钮。
- ☐ 要通过 HTTPS 访问设备，请在您的浏览器中输入 HTTPS 而非 HTTP，然后输入设备的 IP 地址。

`enable`	切换到特权执行模式。
`configure`	切换到配置模式。
`https port 443`	指定网络服务器通过其接收来自客户端的 HTTP 请求的 TCP 端口编号。
`https server`	启用 *HTTPS* 功能。
`show https`	显示 *HTTPS* 服务器的状态和端口编号。

当您对 HTTPS 端口编号进行更改时，请禁用然后再次启用 HTTPS 服务器，以使更改生效。

设备会使用 HTTPS 协议并建立一个新的数据连接。当您在会话结束后注销时，设备将终止数据连接。

B 附录

B.1 管理信息库 (MIB)

管理信息库 (MIB) 是以抽象树形结构的形式设计的。

分支点就是对象类别。MIB 的“树叶”被称为通用对象类别。

当针对唯一标识提出此要求时，则通过指定端口或源地址对通用对象类别进行实体化，即，将抽象结构映射到现实中。

为这些实例分配值（整数、对时信号、计数器或八位字节字符串）；这些值可以读取，在某些情况下也可以修改。对象描述或对象 ID (OID) 可以标识对象类别。子标识符 (SID) 用于对其进行实体化。

示例：

通用对象类别 sa2PSState (OID = 1.3.6.1.4.1.3833.1.1.11.11.1.1.2.1) 是抽象信息电源状态的描述。但是，不可能从此信息中读取任何值，因为系统不知道所指的是哪个电源。

如果指定子标识符 2，则将此抽象信息映射到现实中（对其进行实体化），进而将其标识为电源 2 的工作状态。为此实例分配一个值，该值可以读取。实例 get 1.3.6.1.4.1.3833.1.1.11.11.1.1.2.1 返回响应 1，这意味着该电源处于运行准备就绪状态。

所用语法术语的定义：	
Integer	-2^{31} – $2^{31}-1$ 范围内的一个整数
IP 地址	xxx.xxx.xxx.xxx （xxx = 0..255 范围内的整数）
MAC 地址	符合 ISO/IEC 8802-3 的 12 位十六进制数
Object Identifier	x.x.x.x…（例如 1.3.6.1.1.4.1.3833...）
Octet String	ASCII 字符串
PSID	电源标识符（电源单元的编号）
TimeTicks	秒表，经过的时间 = 数字值/100（秒） 数字值 = 0-$2^{32}-1$ 范围内的整数
Timeout	时间值（百分之一秒） 时间值 = 0-$2^{32}-1$ 范围内的整数
类型字段	符合 ISO/IEC 3-4 的 8802 位十六进制数
计数器	整数 (0-$2^{32}-1$)，当某些事件发生时，值增加 1。

B.2 RFC 列表

RFC 768	UDP
RFC 783	TFTP
RFC 791	IP
RFC 792	ICMP
RFC 793	TCP
RFC 826	ARP
RFC 854	Telnet
RFC 855	Telnet Option
RFC 951	BOOTP
RFC 1112	IGMPv1
RFC 1157	SNMPv1
RFC 1155	SMIv1
RFC 1212	Concise MIB Definitions
RFC 1213	MIB2
RFC 1493	Dot1d
RFC 1542	BOOTP-Extensions
RFC 1643	Ethernet-like -MIB
RFC 1757	RMON
RFC 1867	Form-Based File Upload in HTML
RFC 1901	Community based SNMP v2
RFC 1905	Protocol Operations for SNMP v2
RFC 1906	Transport Mappings for SNMP v2
RFC 1945	HTTP/1.0
RFC 2068	HTTP/1.1 protocol as updated by draft-ietf-http-v11-spec-rev-03
RFC 2131	DHCP
RFC 2132	DHCP-Options
RFC 2233	The Interfaces Group MIB using SMI v2
RFC 2236	IGMPv2
RFC 2246	The TLS Protocol, Version 1.0
RFC 2346	AES Ciphersuites for Transport Layer Security
RFC 2365	Administratively Scoped IP Multicast
RFC 2578	SMIv2
RFC 2579	Textual Conventions for SMI v2
RFC 2580	Conformance statements for SMI v2
RFC 2613	SMON
RFC 2618	RADIUS Authentication Client MIB
RFC 2620	RADIUS Accounting MIB
RFC 2674	Dot1p/Q
RFC 2818	HTTP over TLS
RFC 2851	Internet Addresses MIB
RFC 2863	The Interfaces Group MIB
RFC 2865	RADIUS Client
RFC 2866	RADIUS Accounting

RFC 2868	RADIUS Attributes for Tunnel Protocol Support
RFC 2869	RADIUS Extensions
RFC 2869bis	RADIUS support for EAP
RFC 2933	IGMP MIB
RFC 3164	The BSD Syslog Protocol
RFC 3376	IGMPv3
RFC 3410	Introduction and Applicability Statements for Internet Standard Management Framework
RFC 3411	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC 3412	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413	Simple Network Management Protocol (SNMP) Applications
RFC 3414	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3415	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC 3418	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)
RFC 3580	802.1X RADIUS Usage Guidelines
RFC 3584	Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework
RFC 3621	Power Ethernet MIB
RFC 4022	Management Information Base for the Transmission Control Protocol (TCP)
RFC 4113	Management Information Base for the User Datagram Protocol (UDP)
RFC 4188	Definitions of Managed Objects for Bridges
RFC 4251	SSH protocol architecture
RFC 4291	IPv6 Addressing Architecture
RFC 4252	SSH authentication protocol
RFC 4253	SSH transport layer protocol
RFC 4254	SSH connection protocol
RFC 4293	Management Information Base for the Internet Protocol (IP)
RFC 4318	Definitions of Managed Objects for Bridges with Rapid Spanning Tree Protocol
RFC 4330	Simple Network Time Protocol (SNTP) Version 4 for IPv4, IPv6 and OSI
RFC 4363	Definitions of Managed Objects for Bridges with Traffic Classes, Multicast Filtering, and Virtual LAN Extensions
RFC 4541	Considerations for Internet Group Management Protocol (IGMP) and Multicast Listener Discovery (MLD) Snooping Switches
RFC 4836	Definitions of Managed Objects for IEEE 802.3 Medium Attachment Units (MAUs)
RFC 4861	Neighbor Discovery for IPv6
RFC 5321	Simple Mail Transfer Protocol
RFC 6221	Leightweight DHCPv6 Relay Agent
RFC 8200	IPv6 Specification
RFC 8415	DHCPv6

B.3 基本 IEEE 标准

IEEE 802.1AB	Station and Media Access Control Connectivity Discovery
IEEE 802.1D	MAC Bridges (switching function)
IEEE 802.1Q	Virtual LANs (VLANs, MRP, Spanning Tree)
IEEE 802.1X	Port Authentication
IEEE 802.3	Ethernet
IEEE 802.3ac	VLAN Tagging
IEEE 802.3x	Flow Control
IEEE 802.3af	Power over Ethernet

B.4 基本 IEC 规范

IEC 62439	High availability automation networks MRP - Media Redundancy Protocol based on a ring topology

B.5 基本 ANSI 规范

ANSI/TIA-1057	Link Layer Discovery Protocol for Media Endpoint Devices, April 2006

B.6 技术数据

16.3.3 交换

MAC 地址表的大小（包括静态筛选器）	16384
静态配置的 MAC 地址筛选器的最大数量	100
可通过 IGMP 窥探示教的 MAC 地址筛选器的最大数量	1024
MAC 地址条目 (MMRP) 的最大数量	64
优先级队列的数量	8 队列
可设置的端口优先级	0..7
MTU （端口可接收或传输的数据包的最大允许长度）	9720 个字节

16.3.4 VLAN

VLAN ID 范围	1..4042
VLAN 的数量	每个设备同时最大 128 个 每个端口同时最大 128 个

16.3.5 访问控制列表 (ACL)

ACL 的最大数量	50
每个 ACL 的规则的最大数量	256
每个端口的规则的最大数量	256
可配置规则的总数	2048 (8 × 256)
VLAN 分配的最大数量	12
记录事件的规则的最大数量	128
入口规则的最大数量	514

B.7 集成软件的版权

除其他内容之外，产品还包含第三方开发并且根据开源软件许可证获得许可的开源软件文件。

可在 *Help > Licenses* 对话框的图形用户界面中找到许可条款。

B.8 使用的缩写

ACL	Access Control List
BOOTP	Bootstrap Protocol
CLI	Command Line Interface
DHCP	Dynamic Host Configuration Protocol
DHCPv6	Dynamic Host Configuration Protocol for IPv6
DUID	DHCP Unique Identifier
EUI	Extended Unique Identifier
FDB	Forwarding Database
GUI	Graphical User Interface
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IPv6	Internet Protocol version 6
LDRA	Lightweight DHCPv6 Relay Agent
LED	Light Emitting Diode
LLDP	Link Layer Discovery Protocol
MAC	Media Access Control
MIB	Management Information Base
MRP	Media Redundancy Protocol
NDP	Neighbor Discovery Protocol
NMS	Network Management System
PC	Personal Computer
PTP	Precision Time Protocol
QoS	Quality of Service
RFC	Request For Comment
RM	Redundancy Manager
RSTP	Rapid Spanning Tree Protocol
SCP	Secure Copy
SFP	Small Form-factor Pluggable
SFTP	SSH File Transfer Protocol
SNMP	Simple Network Management Protocol
SNTP	Simple Network Time Protocol
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
TP	Twisted Pair
UDP	User Datagram Protocol

URL	Uniform Resource Locator
UTC	Coordinated Universal Time
VLAN	Virtual Local Area Network

C 关键词目录