SIEMENS

SIMATIC NET

Industrial Wireless LAN SCALANCE W780/W740 符合 IEEE 802.11n 基于 Web 的管理

配置手册

10/2020

C79000-G8952-C267-16

法律资讯

警告提示系统

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

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

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

⚠小心
表示如果不采取相应的小心措施，可能导致轻微的人身伤害。

注意
表示如果不采取相应的小心措施，可能导致财产损失。

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

合格的专业人员

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

按规定使用 Siemens 产品

请注意下列说明：

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

商标

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

责任免除

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

Siemens AG
Digital Industries
Postfach 48 48
90026 NÜRNBERG
德国

C79000-G8952-C267-16
Ⓟ 10/2020 本公司保留更改的权利

目录

简介

1

1.1 有关组态手册的信息

组态手册的有效性

本组态手册涵盖了以下产品：

- SCALANCE W748-1 M12
- SCALANCE W748-1 RJ-45
- SCALANCE W788-1 M12
- SCALANCE W788-2 M12
- SCALANCE W788-2 M12 EEC
- SCALANCE W788-1 RJ-45
- SCALANCE W788-2 RJ-45
- SCALANCE W786-1 RJ-45
- SCALANCE W786-2 RJ-45
- SCALANCE W786-2IA RJ-45
- SCALANCE W786-2 SFP

本组态手册适用于以下软件版本：

- SCALANCE W700 固件版本 V 6.5 及以上版本

本组态手册的用途

本组态手册旨在为您提供正确调试和运行 SCALANCE W700 设备所需的信息。它说明了如何对 SCALANCE W700 设备进行组态，以及如何将设备集成到 WLAN 网络中。

如需了解如何正确安装和连接设备，请参见设备的操作说明。

文档说明

除了您当前阅读的组态手册外，还可以从 SIMATIC NET 的工业无线 LAN 主题下获取以下文档：

- 组态手册 SCALANCE W780/W740 命令行接口

  本文档包含 SCALANCE W700 设备支持的 CLI 命令。

- 802.11abgn PCIe Minicard MPCIE-R1-ABGN-U3 性能数据

  本文档包含有关无线卡的频率、调制、发射功率和接收器灵敏度的信息。

- SCALANCE W788-x/W748-1 操作说明

  本文档包含下列产品安装、连接及认证方面的信息：

  – SCALANCE W788-1 RJ-45

  – SCALANCE W788-1 M12

  – SCALANCE W788-2 RJ-45

  – SCALANCE W788-2 M12

  – SCALANCE W788-2 M12 EEC

  – SCALANCE W748-1 RJ-45

  – SCALANCE W748-1 M12

- SCALANCE W786-x 操作说明

  本文档包含下列产品安装、连接及认证方面的信息：

  – SCALANCE W786-1 RJ-45

  – SCALANCE W786-2 RJ-45

  – SCALANCE W786-2IA RJ-45

  – SCALANCE W786-2 SFP

- 系统手册工业无线 LAN 的结构

  除介绍了物理基础以及主要的 IEEE 标准外，本手册还包含有关数据安全的信息以及无线 LAN 的工业应用说明。
  如果要建立结构更加复杂的 WLAN 网络（不仅是两台设备之间的连接），请阅读本手册。

- 系统手册 RCoax

  该系统手册解释了基本技术方面的情况，还介绍了各个 RCoax 组件及其功能。还介绍了 RCoax 组件的安装/调试和连接及其工作原理。同时也介绍了各种 SIMATIC NET 组件的可能应用。

- 系统手册 - 无源网络组件 IWLAN

  此系统手册介绍了 IWLAN 应用所需的整个 IWLAN 布线。为了实现在室内和室外灵活组合和安装各个 IWLAN 组件，可以在广泛的兼容同轴附件中选择。该系统手册还涵盖了连接电缆以及各种插件连接器、防雷保护器、功率分配器和衰减器。

使用的术语

标识 . . .	代表 . . .
IPv4 地址	IPv4 地址
IPv6 地址	IPv6 地址
IP 地址	IPv4/IPv6 地址
IPv4 接口	支持 IPv4 的接口。
IPv6 接口	支持 IPv6 的接口。此接口可拥有多个 IPv6 地址。这些 IPv6 地址具有不同的范围，例如，链路本地地址
IP 接口	既支持 IPv4 又支持 IPv6 的接口。默认情况下，已激活对 IPv4 的支持。如要支持 IPv6，需要另外激活。

SIMATIC NET 手册

Siemens 工业在线支持的 Internet 页面上提供了 SIMATIC NET 手册：

- 使用搜索功能：

  西门子工业在线支持 (https://support.industry.siemens.com/cs/ww/zh/)

  输入相关手册的条目 ID 作为搜索项。

- 在“工业通信”(Industrial Communication) 区域左侧的导航面板中：

  工业通信 (https://support.industry.siemens.com/cs/ww/zh/ps/15247/man)

  转到所需产品组并进行以下设置：
  选项卡“条目列表”(Entry list)，条目类型“手册”(Manuals)

更多文档

《SIMATIC NET 工业以太网网络手册》包含有关在工业以太网网络中可以与该产品系列的设备一起使用的其它 SIMATIC NET 产品的信息。其中还包含安装产品所需的通信伙伴的光学性能数据。

《SIMATIC NET 工业以太网网络手册》可以在 Siemens 工业在线支持的 Internet 页面中通过以下条目 ID 获取：
27069465 (https://support.industry.siemens.com/cs/ww/zh/view/27069465)

培训、服务与支持

有关培训、服务和支持的信息，请参见本文档随附的数据媒体上的多语言文档“DC_support_99.pdf”。

回收和处置

该产品的污染物含量低，可以回收利用并且符合 WEEE 指令 2012/19/EU 对电子电气设备的处置要求。

请勿将产品丢弃在公共场所。

为了使旧设备的回收和处置更符合环境要求，请联系一家经认证的电子废料处理公司或联系西门子的联系人（产品回收 (https://support.industry.siemens.com/cs/ww/zh/view/109479891)）。

请注意不同国家的法规。

安全性信息

Siemens 为其产品及解决方案提供了工业信息安全功能，以支持工厂、系统、机器和网络的安全运行。

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

客户负责防止其工厂、系统、机器和网络受到未经授权的访问。只有在必要时并采取适当安全措施（例如，使用防火墙和网络分段）的情况下，才能将系统、机器和组件连接到企业网络或 Internet。

关于可采取的工业信息安全措施的更多信息，请访问 链接 (https://www.siemens.com/industrialsecurity)

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

要及时了解有关产品更新的信息，请订阅 Siemens 工业信息安全 RSS 源，网址为 链接 (https://www.siemens.com/industrialsecurity)

商标

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

SIMATIC NET, SCALANCE, C-PLUG, RCoax

固件

固件已签名且加密。这可确保只能将 Siemens 创建的固件下载到设备。

SIMATIC NET 词汇表

对于本文档中所用的许多专业术语，SIMATIC NET 词汇表部分都给出了解释。

用户可在以下位置找到 SIMATIC NET 词汇表：

- SIMATIC NET 手册集或产品 DVD

  该 DVD 随一些 SIMATIC NET 产品一起提供。

- Internet 上的以下地址：

  50305045 (https://support.industry.siemens.com/cs/ww/zh/view/50305045)

许可证条款

说明

开源软件

在使用本产品之前，请仔细阅读开源软件的许可证条款。

在所提供的数据介质中，下列文档提供有许可证条款：

- OSS_Scalance-W700_86.pdf

1.2 型号标识

所使用的缩写

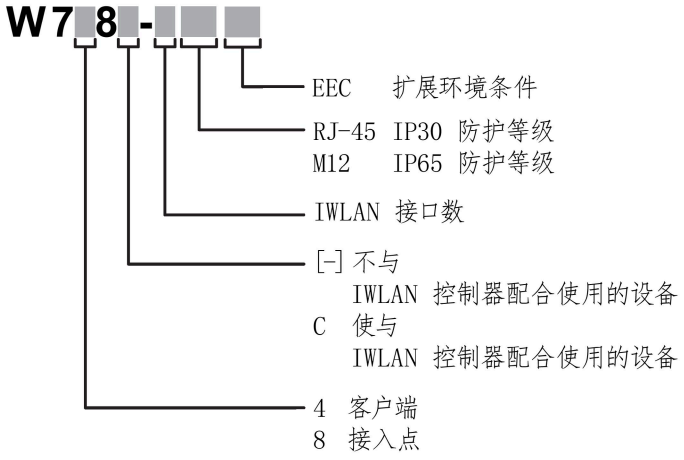
SCALANCE W700 产品系列手册中的信息通常适用于多个产品型号。 在这种情况下，对产品标识采用缩写处理，就不必列出所有的型号标识。 下表列出了缩写与产品型号之间的对应关系。

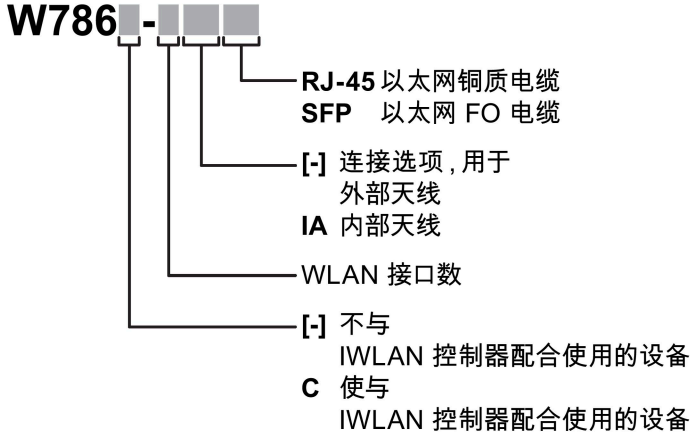
产品组	标识. . . 代表. . .	产品名称
客户端（IP30 和 IP65）	W748-1	SCALANCE W748-1 RJ-45 SCALANCE W748-1 M12
接入点（IP30 和 IP65）	W788-x	SCALANCE W788-1 M12 SCALANCE W788-2 M12 SCALANCE W788-2 M12 EEC SCALANCE W788-1 RJ-45 SCALANCE W788-2 RJ-45
接入点（IP65）	W786-x	SCALANCE W786-1 RJ-45 SCALANCE W786-2 RJ-45 SCALANCE W786-2IA RJ-45 SCALANCE W786-2 SFP
所有 SCALANCE W 接入点	W78x	SCALANCE W788-1 M12 SCALANCE W788-2 M12 SCALANCE W788-2 M12 EEC SCALANCE W788-1 RJ-45 SCALANCE W788-2 RJ-45 SCALANCE W786-1 RJ-45 SCALANCE W786-2 RJ-45 SCALANCE W786-2IA RJ-45 SCALANCE W786-2 SFP

产品组	标识. . . 代表. . .	产品名称
SCALANCE W（W786-x 除外）	W7x8	SCALANCE W788-1 RJ-45 SCALANCE W788-1 M12 SCALANCE W788-2 RJ-45 SCALANCE W788-2 M12 SCALANCE W748-1 RJ-45 SCALANCE W748-1 M12
所有 SCALANCE W 设备	W700	SCALANCE W748-1 M12 SCALANCE W748-1 M12 SCALANCE W788-1 M12 SCALANCE W788-2 M12 SCALANCE W788-2 M12 EEC SCALANCE W788-1 RJ-45 SCALANCE W788-2 RJ-45 SCALANCE W786-1 RJ-45 SCALANCE W786-2 RJ-45 SCALANCE W786-2IA RJ-45 SCALANCE W786-2 SFP

1.3 型号标识的结构

SCALANCE W700 的型号标识由多个部分组成，各部分的含义如下：





说明 2

说明

WLAN 通信中断

WLAN 通信可能受到高频干扰信号的影响，并可能完全中断。
请牢记此点，并采取适当操作。

2.1 网络结构

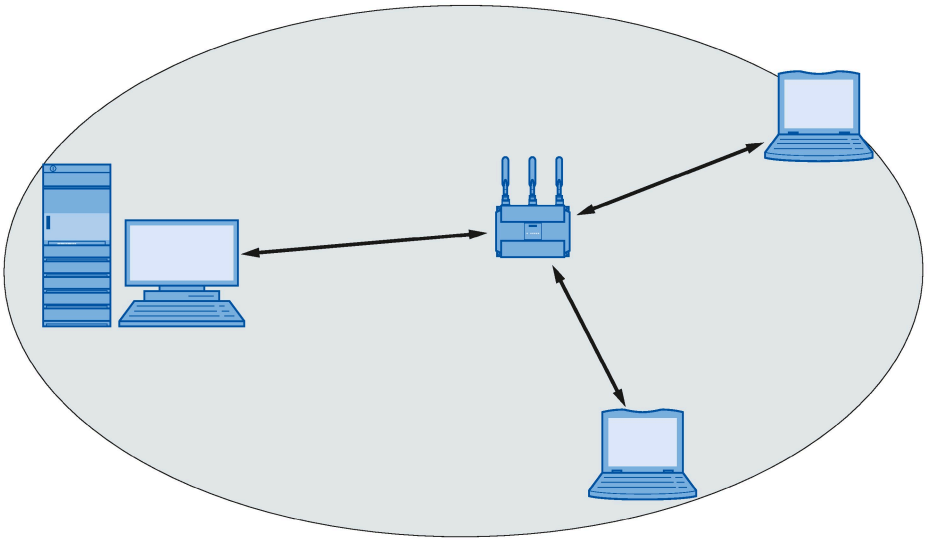
下文介绍如何使用接入点和客户端建立各种网络结构。在客户端模式下，客户端也是接入点。

使用接入点的独立组态

该组态不需要服务器，且接入点不连接到有线以太网。在其传输范围内，接入点将数据由一个 WLAN 节点转发到另一个 WLAN 节点。

无线网络具有唯一的名称。所有在该网络中交换数据的 SCALANCE W700 设备必须用该名称进行组态。

图中的灰色区域代表接入点的无线覆盖范围。



对有线以太网网络进行无线访问

如果有一个（或多个）接入点能够访问有线以太网，则支持以下应用：

- 单个设备作为网关：

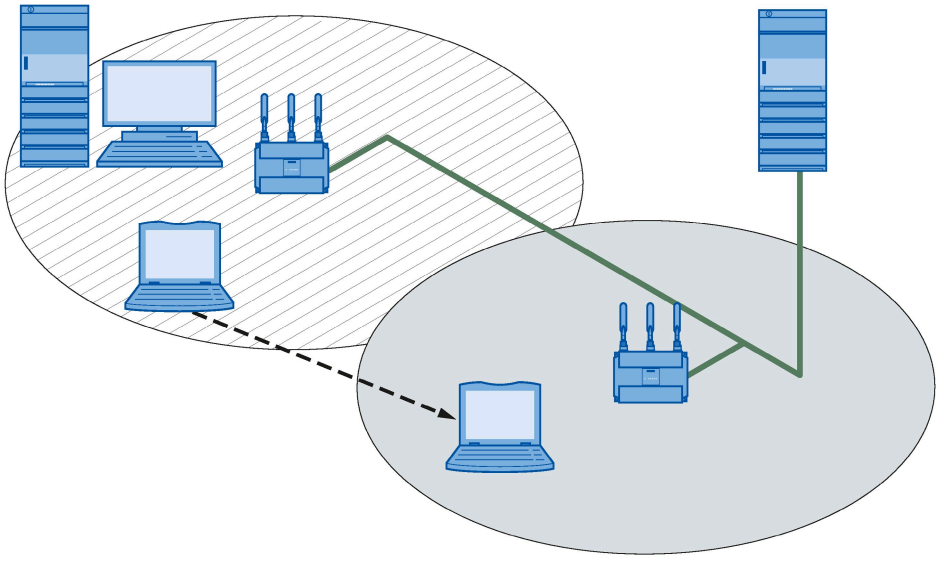
  无线网络可通过接入点连接到有线网络。

- 包含多个接入点的无线网络的无线覆盖范围：

  全部接入点都组态了同一个唯一的 SSID（网络名称）。所有要通过该网络进行通信的节点也必须组态有该 SSID。

  如果移动站从一个接入点的覆盖范围移动另一个接入点的覆盖范围，将保持无线链路（漫游）。

  下图显示了跨两个无线蜂窝区的移动站的无线连接（漫游）。



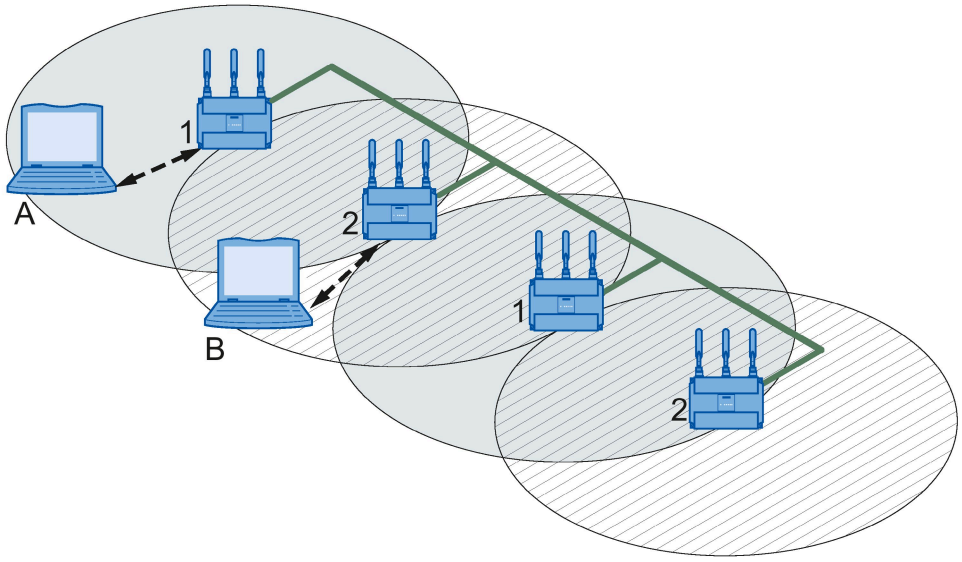
多通道组态

如果相邻接入点使用同一频道，则可能会因为任何可能发生的冲突而导致响应时间延长。如果将图中所示的组态当作单通道系统来实现，则计算机 A 和 B 无法同时与其无线蜂窝区内的接入点通信。

如果相邻接入点采用不同的频率，将显著提高通信性能。每个相邻无线蜂窝区因此都有其自身的可用介质，将不再产生因时间偏移传输导致的延迟。

通道间隔应尽可能大；实际值为 25 MHz。即使在一个多通道组态中，也可为全部的接入点组态同一个网络名称。

下图显示了通道 1 和通道 2 上有四个接入点的多通道组态。

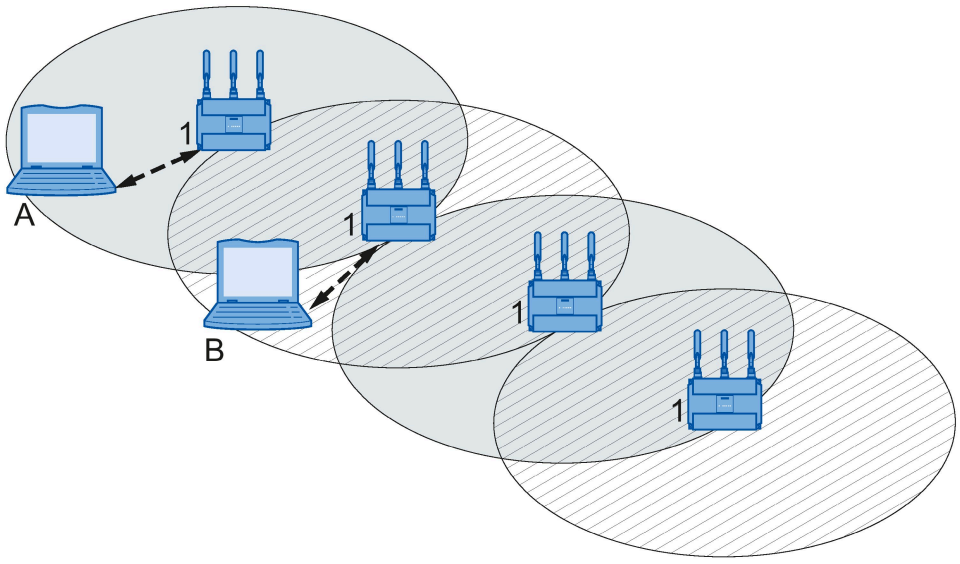


无线分布式系统 (Wireless Distribution System, WDS)

WDS 允许接入点之间或接入点与其它 WSD 兼容设备之间的直接连接。用这些连接来创建无线骨干，或用来将单独的接入点连接到由于其位置原因而无法直接连接到电缆基础结构的网络。

有两种组态可供选择。WDS 伙伴可通过 WDS ID 或通过其 MAC 地址进行组态。

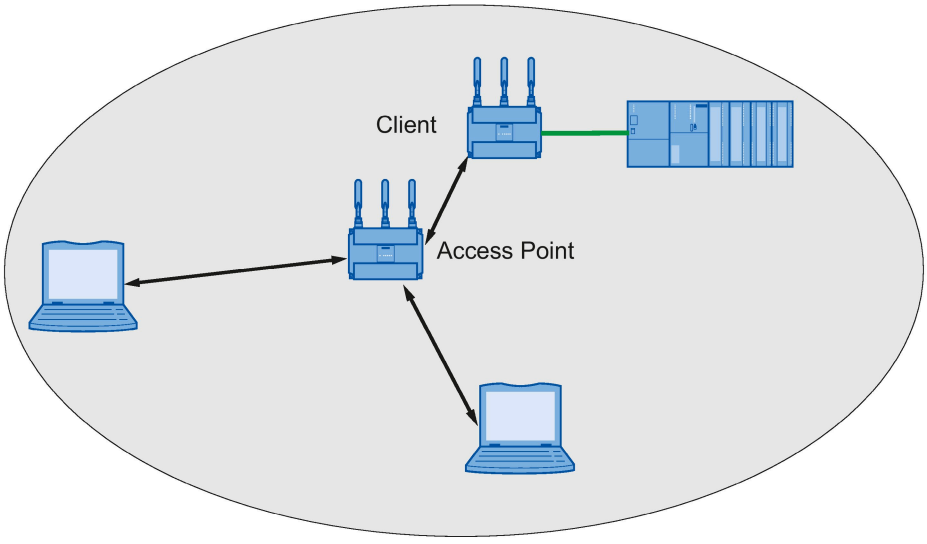
下图显示了具有四个接入点的 WDS 实现。



通过客户端或客户端模式下的接入点访问网络

SCALANCE W700 设备可用于在无线网络中集成有线以太网设备（例如 SIMATIC S7 PLC）。

下图显示了将 SIMATIC S7 PLC 接入无线 LAN。



2.2 SCALANCE W700 设备的可能应用

说明

SIMATIC NET WLAN 产品使用 OpenSSL。
它是包含许可条款的开放源代码 (BSD)。
请参见最新的许可条款。
由于该驱动程序包含加密软件，因此还应遵守具体国家/地区的相应法规。

SCALANCE W788 的可能应用

SCALANCE W788 配有一个以太网接口和一个或两个 WLAN 接口。 该设备因此适合以下应用：

- SCALANCE W788 在其传输范围内将数据由一个节点转发到另一个节点时不需要连接到有线以太网。
- SCALANCE W788 可用作从有线网络到无线网络的网关。
- SCALANCE W788 可用作两个网络之间的无线网桥。
- SCALANCE W788 也可用作两个不同频段之间的网桥。
- SCALANCE W788 支持防护等级 IP65 和防护等级 IP30。
  提供两个版本的接入点：
  - IP65 防护等级的 M12
  - IP30 防护等级的 RJ-45

使用带两个 WLAN 接口的 SCALANCE W788，还可实现冗余无线连接到带两个 WLAN 接口的 SCALANCE W78x。

SCALANCE W786 的可能应用

SCALANCE W786 最多带有两个以太网接口，最多有两个 WLAN 接口。 该设备因此适合以下应用：

- 由于其具有扩展的温度范围，特别推荐在户外应用 SCALANCE W786。
- SCALANCE W786 在其传输范围内将数据由一个节点转发到另一个节点时不需要连接到有线以太网。
- SCALANCE W786 可用作从有线网络到无线网络的网关。
- SCALANCE W786 可用作两个网络之间的无线网桥。
- SCALANCE W786 可用作以不同频率工作的两个蜂窝区之间的网桥。

使用带有多个 WLAN 接口的 SCALANCE W786，还可实现冗余无线连接到最多带有两个 WLAN 接口的 SCALANCE W78x。

SCALANCE W748 的可能应用

SCALANCE W748 配有一个以太网接口和一个 WLAN 接口。 该设备因此适合以下应用：

- SCALANCE W748 在其传输范围内将数据由一个节点转发到另一个节点时不需要连接到有线以太网。
- SCALANCE W748 可用作从有线网络到无线网络的网关。
- SCALANCE W748 可用作两个网络之间的无线网桥。

该设备还可以将以太网端口上支持 IP 通信的最多 8 个站连接到无线蜂窝区。

2.3 产品特征

SCALANCE W700 设备的属性

- 以太网接口支持以下模式：
  - 全双工和半双工 10 Mbps 和 100 Mbps
  - 1000 Mbps 全双工
  - 自动跨接
  - 自动极性变换
- WLAN 接口在 2.4 GHz 和 5 GHz 频段中工作。
- WLAN 接口兼容 IEEE 802.11a、IEEE 802.11b 和 IEEE 802.11g 标准。在 802.11a 和 802.11g 模式下，总传输率最高可达 54 Mbps。
- IEEE 802.11n
  最高可达 450 Mbps 的高速 WLAN 标准（无线 LAN），可在 2.4 GHz 和 5 GHz 范围内工作。
- IEEE 802.11h - 对 IEEE 802.11a 的补充
  在 802.11h 模式下，在 5.25 - 5.35 和 5.47 - 5.75 GHz 范围内使用"发射功率控制 (TPC)"以及"动态频率选择 (DFS)"方法。在一些国家/地区，即使发射功率较高，也允许在户外使用子频段 5.47 - 5.725 GHz。
  TPC 是调整发射功率的一种方法。
  通过 DFS，接入点将用 60 秒的时间搜索主要用户，然后开始在所选通道上通信。在此期间，接入点不会发送信标。如果在通道上发现信号，则该通道将被阻断 30 分钟，接入点将更改通道并重复该检查。在运行过程中也会搜索主要用户。
- 支持 WPA、WPA-PSK、WPA2、WPA2-PSK 和 IEEE 802.1x 验证标准，并支持 WEP、AES 和 TKIP 加密方法。

说明

传输标准 IEEE 802.11 n（"802.11n"或"仅 802.11 n"设置）仅支持采用 AES 安全设置的 WPA2/ WPA2-PSK。

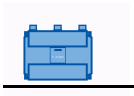
- 为实现更好的 WLAN 传输，应启用 WMM（wireless multimedia，无线多媒体）功能。各个帧将根据优先级进行评估，然后通过 WLAN 接口按优先级发送。
- 适合增加 RADIUS 服务器来执行验证。
- 对无线连接执行与设备相关以及与应用相关的监视。
- 彻底测试过本设备与其他供应商提供的 Wi-Fi 设备的互操作性。
- 调试 SCALANCE W700 前，请检查现场的无线条件。如果要在 2.4 GHz 频段使用工业无线 LAN 系统和 WirelessHART 系统，则需要规划通道的使用。应全力避免同时使用重叠频率范围的情况。工业无线 LAN 和 WirelessHART 存在以下重叠：

IWLAN 通道 IEEE 802.11 b/g/n	**WHART 通道 IEEE 802.15.4**
1	11 - 16
6	15 - 20
7	16 - 21
11	20 - 25
13	21 - 25

说明

所有 SCALANCE W700 接入点都可重新组态成客户端模式。

SCALANCE W700 的特征



型号	WLAN 端口数	天线	以太网接口的数量及类型	防护等级	订货号
SCALANCE W748-1 M12	1	外部	1 个千兆位以太网（铜缆）	IP65	6GK5748-1GD00-0AA0 6GK5748-1GD00-0AB0 (1)
SCALANCE W748-1 RJ-45	1	外部	1 个千兆位以太网（铜缆）	IP30	6GK5748-1FC00-0AA0 6GK5748-1FC00-0AB0 (1)

型号	WLAN 端口数	天线	以太网接口的数量及类型	防护等级	订货号
SCALANCE W786-1 RJ-45	1	外部	1 个千兆位以太网（铜缆）	IP65	6GK5786-1FC00-0AA0 6GK5786-1FC00-0AB0 (1)
SCALANCE W786-2 RJ-45	2	外部	1 个千兆位以太网（铜缆）	IP65	6GK5786-2FC00-0AA0 6GK5786-2FC00-0AA0 (1) 6GK5786-2FC00-0AC0 (2)
SCALANCE W786-2IA RJ-45	2	内部	1 个千兆位以太网（铜缆）	IP65	6GK5786-2HC00-0AA0 6GK5786-2HC00-0AB0 (1)
SCALANCE W786-2 SFP	2	外部	2 x SFP 插槽	IP65	6GK5786-2FE00-0AA0 6GK5 786-2FE00-0AB0 (1)
SCALANCE W788-1 M12	1	外部	1 个千兆位以太网（铜缆）	IP65	6GK5788-1GD00-0AA0 6GK5788-1GD00-0AB0 (1)
SCALANCE W788-2 M12	2	外部	1 个千兆位以太网（铜缆）	IP65	6GK5788-2GD00-0AA0 6GK5788-2GD00-0AB0 (1)
SCALANCE W788-2 M12 EEC	2	外部	1 个千兆位以太网（铜缆）	IP65	6GK5788-2GD00-0TA0 6GK5788-2GD00-0TB0 (1) 6GK5 788-2GD00-0TC0 (2)
SCALANCE W788-1 RJ-45	1	外部	1 个千兆位以太网（铜缆）	IP30	6GK5788-1FC00-0AA0 6GK5788-1FC00-0AB0 (1)
SCALANCE W788-2 RJ-45	2	外部	1 个千兆位以太网（铜缆）	IP30	6GK5788-2FC00-0AA0 6GK5788-2FC00-0AB0 (1) 6GK5788-2FC00-0AC0 (2)

(1) 美国型号

(2) 以色列型号

2.4 IEEE 802.11n

概述

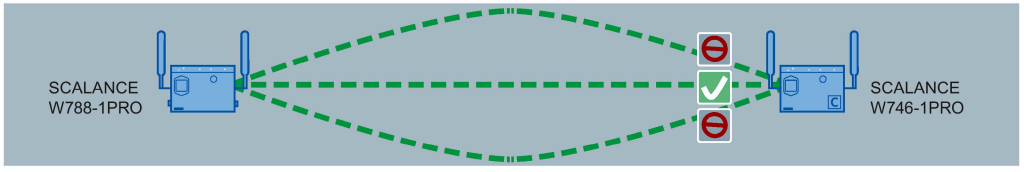
标准 IEEE 802.11n 是 802.11 标准的扩展，于 2009 获得批准。
之前的标准或者适用于 2.4 GHz 频段 (IEEE 802.11g/b)，或者适用于 5 GHz 频段 (IEEE 802.11a)。IEEE 802.11n 适用于两个频段。
在 IEEE 802.11n 标准中存在在 PHY 层和 MAC 层实施的机制，可提高数据吞吐量并增大无线覆盖范围。

- MIMO 天线技术
- 最大比合并 (MRC)
- 空间多路复用
- 通道联结
- 帧聚合
- 加速防护间隔
- 调制和编码方案
- 数据吞吐量最高达 450 Mbps（总计）。
  所有 SCALANCE W700 设备不可能都能实现这一点。

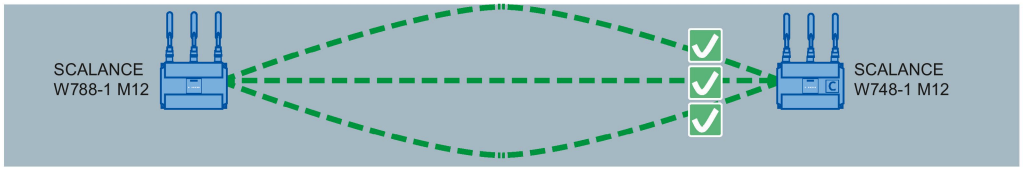
MIMO 天线技术

MIMO（Multiple Input - Multiple Output，多输入多输出）基于智能多天线系统。发送器和接收器具有多个在空间上彼此分离的天线。这些空间分离的天线用于同时传输数据流。最多可传输四个数据流。由于衍射、折射、衰减和反射，数据流的传输路径在空间上彼此分离，返回的路径也各自不同（多路传播）。多路传播意味着，在接收点处一个复杂的与空间和时间相关的模式将被解读为一个由所发送的单独信号组成的总信号。MIMO 通过检测特征信号的空间位置来应用此特有的模式。在此处每个空间位置都不同于其相邻位置。通过为各发送器添加特征，接收器能够将多个信号彼此分隔。

使用 IEEE 802.11a/b/g 的多路传播



多路传播 IEEE□802.11n (MIMO)



最大比合并 (MRC)

在多天线系统中，无线信号由单独的天线接收，然后合并形成一个信号。使用 MRC 方法合并无线信号。MRC 方法会根据无线信号的信噪比对其进行加权，然后组合这些无线信号以形成一个信号。信噪比得到改善，错误率得以降低。

空间多路复用

通过空间多路复用，不同的信息可使用相同频率进行发送。将数据流分布到 n 个发射天线上；换句话说，每个天线仅发送 1/n 的数据流。数据流的划分受天线数量的限制。在接收器端，信号将被重组。

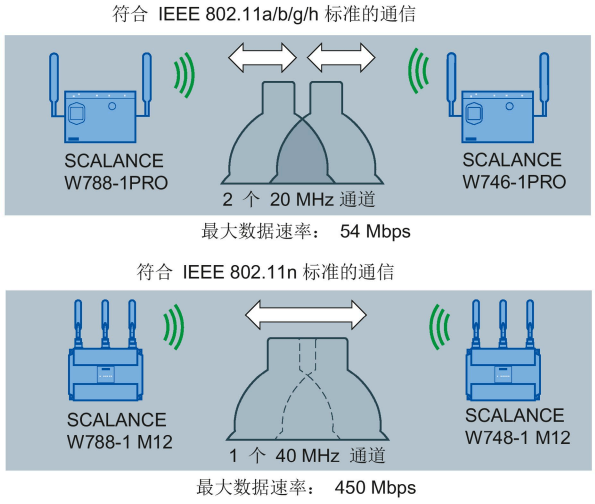
由于空间多路复用，信噪比和数据吞吐量都将更高。

通道联结

借助于 IEEE 802.11n，数据可通过两个直接相邻的通道进行传送。这两条 20 MHz 通道组合在一起形成一条 40 MHz 通道。这使通道带宽增加了一倍，从而提高了数据吞吐量。

为能够使用通道联结，接收器必须支持 40 MHz 传输。如果接收器不支持 40 MHz 传输，则带宽将自动降至 20 MHz。这意味着 IEEE 802.11n 也可与 IEEE 802.11a/b/g 设备通信。

通道绑定在“AP (页 370)”WBM 页面上通过“HT 通道宽度 [MHz]”(HT Channel Width [MHz]) 参数进行设置。



帧聚合

借助于 IEEE 802.11n，可将各数据包组合到一起形成一个更大的数据包；这也称为帧聚合。有两种类型的帧聚合：

- 聚合的 MAC 协议数据单元 (A-MADU)

  借助 A-MPDU，具有相同目标地址的多个 MPDU 数据包捆绑在一起并作为一个大的 A-MPDU 发送。

- 聚合的 MAC 服务数据单元 (A-MSDU)

  借助 A-MSDU，具有相同目标地址的多个 MSDU 数据包捆绑在一起并发送。

SCALANCE W 设备支持两种帧聚合。可在 WBM 页面"AP 802.11n (页 368)"中进行设置。

加速防护间隔

防护间隔可防止不同的传输混到一起。在电信方面，这种混合也称为码间干扰 (ISI)。当发送时间过后，必须保持发送暂停（防护间隔），然后开始下次传输。

IEEE 802.11a/b/g 的防护间隔为 800 ns。IEEE 802.11n 可使用降低的 400 ns 防护间隔。在"AP 802.11n (页 368)"WBM 页面上指定防护间隔。

调制和编码方案

IEEE 802.11n 标准支持不同的数据速率。数据速率取决于空间流的数量、调制方式和通道编码。调制和编码方案中介绍有多种组合。

2.5 SCALANCE W 设备的安装和操作要求

必须具有能够联网的 PG/PC，才能对 SCALANCE W 设备进行组态。如果没有可用的 DHCP 服务器，则必须使用安装了 SINEC PNI 的 PC 来为 SCALANCE W 设备首次分配 IP 地址。对于其他组态设置，需要使用有 Telnet 和 Web 浏览器的计算机。

2.6 C-PLUG 和 KEY-PLUG

PLUG 为移动介质，在更换设备时，用于将旧设备的组态传送到新设备中。

PLUG 有以下版本：

- C-PLUG：可交换存储介质仅可保存设备的组态数据。
- KEY-PLUG：除组态数据外，可交换存储介质还包含许可证，可通过该许可证启用 iFeatures 等特定功能。

工作原理

注意
操作期间请勿插拔 C-PLUG/KEY-PLUG！ 只有在设备关闭情况下才可以插拔 PLUG。 设备以 1 秒的间隔检查 PLUG 是否存在。如果检测到 PLUG 被拔出，则会重启。 如果在设备中插入了有效 KEY-PLUG，设备会在重启后切换到预定的错误状态。在这种情况下，SCALANCE W 会禁用可用的无线接口。 若设备先前组态了 PLUG，则该设备在缺少此 PLUG 的情况下无法继续使用。为再次使用该设备，请将设备复位为出厂设置。

设备支持以下操作模式：

- 不带 PLUG

  设备将组态数据保存在内部存储器中。未插入 PLUG 时会激活此模式。

- 带 PLUG

  如果使用未写入数据的 PLUG（出厂状态或已使用"清理"功能删除），则设备中已存在的本地组态将自动存储到插入的 PLUG 中。如果 PLUG 包含许可证，还可启用其他功能。

  已写入并已接受 PLUG（"ACCEPTED"状态）的设备将在启动时自动使用 PLUG 中的组态数据。但是，仅当通过兼容设备类型写入数据时才可能接受。

  其中一个例外情况是 IP 组态，如果使用 DHCP 设置 IP 组态，且 DHCP 服务器没有进行相应的重新组态。如果使用基于 MAC 地址的功能，则需要重新进行组态。

  通过用户界面显示存储在 PLUG 中的组态。

  如果更改了组态，则设备会将组态信息直接存储在 PLUG（如果处于"ACCEPTED"状态）上。不会对内部存储器执行读写操作。

错误响应

如果插入的 PLUG 不包含兼容设备类型的组态、意外拔出 PLUG/KEY-PLUG 或者 PLUG 出现常规故障，设备的诊断机制（LED、基于 Web 的管理 (WBM)、SNMP、命令行接

口 (CLI) 和 PROFINET 诊断）将发出相关信号。用户随即可以选择再次取出该 PLUG，或者选择重新格式化该 PLUG。

说明

插入的 PLUG 组态与先前版本不兼容

在安装先前版本固件的过程中，组态数据可能丢失。在这种情况下，安装固件后，设备会使用出厂设置启动。如果此时设备中插入了 PLUG，则重启后，由于 PLUG 仍具有之前最新固件的组态数据，因此状态为"NOT ACCEPTED"。此时，您可以返回之前的最新固件而不丢失任何组态数据。如果不再需要 PLUG 上的原始组态，则可使用"系统 > PLUG"(System > PLUG) 手动删除或重写 PLUG。

KEY-PLUG 上的许可证信息

除组态外，KEY-PLUG 也包含一个支持使用 iFeatures 功能的许可证。

带预设功能的 PLUG (PRESET-PLUG)

借助 PRESET-PLUG，可以在多个设备上安装相同的组态及其所含固件。

说明

通过使用 DHCP 的组态

仅通过使用 DHCP 的设备组态创建 PRESET-PLUG。否则，将会因为存在多个相同的 IP 地址而导致网络中断。

可以在完成基本安装后额外分配固定的 IP 地址。

在被组态为 PRESET-PLUG 的 PLUG 中，存储了设备组态、用户帐户、证书和固件。

说明

在插有 PRESET PLUG 的情况下恢复出厂默认设置并重启

如果将设备复位为出厂默认设置，则在设备重启时，插入的 PRESET PLUG 会被格式化，PRESET PLUG 功能将丢失。之后，需要创建新的 PRESET PLUG。

建议您先拔出 PRESET PLUG，然后再将设备复位为出厂默认设置。

有关创建和使用 PRESET PLUG 的更多详细信息，请参见保养和维护 (页 547)部分。

2.7 数字量输入/输出

简介

RJ-45 型号的 SCALANCE W788-x/W748-x 设备有一个数字量输入/输出。

通过 4 针接线盒进行连接。有关引脚分配的信息，请参见设备的操作说明。

应用示例

- 数字量输入通过信号传递一个信息项，例如“门打开”、“门关闭”。
- 数字量输出，例如针对自动导向式传送系统上的设备的“转为休眠”。

数字量输出的控制

使用 CLI 和专有 MIB 变量 snMspsDigitalOutputLevel，可控制数字量输出 (DO/1L)。

说明

不可通过基于 Web 的管理 (WBM) 组态数字量输出。
如果数字量输入的状态有所更改，则会在事件协议表中创建一个条目。

- 专有 MIB 变量 snMspsDigitalOutputLevel 的 OID：

  iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).siemens(4329).industrialComProducts(20).iComPlatforms(1).simaticNet(1).snMsps(1).snMspsCommon(1).snMspsDigitalIO(39).snMspsDigitalIOObjects(1).snMspsDigitalOutputTable(3).snMspsDigitalOutputEntry(1).snMspsDigitalOutputLevel(6)

- MIB 变量的值
  - 1：数字量输出打开（DO 和 1L 中断）。
  - 2：数字量输出关闭（DO 和 1L 连接跳线）。

数字量输入

使用专有 MIB 变量 snMspsDigitalInputLevel，可读出数字量输入的状态。

说明

如果数字量输出的状态有所更改，则会在事件协议表中创建一个条目。

- 专有 MIB 变量 snMspsDigitalInputLevel 的 OID：

  iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).siemens(4329).industrialComProducts(20).iComPlatforms(1).simaticNet(1).snMsps(1).snMspsCommon(1).snMspsDigitalIO(39).snMspsDigitalIOObjects(1).snMspsDigitalInputTable(2).snMspsDigitalInputEntry(1).snMspsDigitalInputLevel(6)

- MIB 变量的值
  - 1：数字量输入 (DI) 处为信号 0
  - 2：数字量输入 (DI) 处为信号 1

MIB 文件

MIB 变量可在文件“SN-MSPS-DIGITAL-IO-MIB”中找到，该文件是专有 MIB 文件“snMspsWlan.mib”的一部分。有关更多详细信息，请参见“SCALANCE W 设备的专有 MIB 变量 (页 569)”。

2.8 以太网供电 (PoE)

概述

“以太网供电”(Power over Ethernet, PoE) 是一种符合 IEEE 802.3af 或 IEEE 802.3at 标准的网络组件供电技术。通过将各种网络组件连接在一起的以太网电缆进行供电。如此就无需额外的电源线。PoE 可用于所有 PoE 兼容网络组件，它们通常需要很小的功率（最大 12.95 W）。

设备的哪一个以太网接口支持 PoE 在相关设备的操作说明中进行了介绍。

用于供电的电缆

- **型号 1（冗余电线）**
  在快速以太网中，电线对 1、2 和 3、6 用于传输数据。电线对 4、5 和 7、8 用于供电。如果仅有四根线可用，则会将电压调制到电线 1、2 和 3、6 上（参见型号 2）。这种选择适合数据传输率为 10/100 Mbps 的情况。这种供电类型不适合数据传输率为 1 Gbps 的情况，这是因为在千兆位中，全部的 8 根电线都用于数据传输。
- **型号 2（幻象电源）**
  应用幻象电源时，会通过用于数据传输的电线对来供电，即全部的八根 (1 Gbps) 或四根 (10/100 Mbps) 电线既用于数据传输，又用于供电。

设备支持型号 1 和型号 2 还是只支持型号 2，请参见相关设备的操作说明。

支持 PoE 的交换机可以使用以下电缆为终端设备供电：

- 型号 1 或
- 型号 2 或
- 型号 1 和型号 2。

端跨

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

中跨

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

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

⚠警告

仅当符合以下条件时使用电源插头：

- 采用超低电压 SELV，即符合 IEC 60364-4-41 的 PELV
- 在美国/加拿大，采用符合 NEC 的 2 类电源
- 在美国/加拿大，布线必须符合 NEC/CEC 的要求
- 电源负载最大 0.5 A。

电缆长度

表格 2- 1　允许的电缆长度（铜质电缆 - 快速以太网）

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

表格 2- 2　允许的电缆长度（铜质电缆 - 千兆位以太网）

电缆类型	**附件（插头、插座和 TP 线）**	**允许的电缆长度**
IE FC 标准电缆，4x2，24 AWG	带有 IE FC RJ-45 插头 180，4x2	0 到 90 m
IE FC 软电缆，4x2，24 AWG	带有 IE FC RJ-45 插头 180，4x2	0 到 60 m
IE FC 标准电缆，4x2，22 AWG	带有 IE FC 插座 RJ-45 + 10 m TP 线	0 到 100 m + 10 m TP 线

表格 2- 3　安装接头

引脚	CAT5 导线的 颜色	CAT6a 导线的 颜色	应用	
			通过未使用的电线供电（仅 10/100 Mbps）	幻象电源
1	黄色	绿色/白色	数据	数据/电源
2	橙色	绿色	数据	数据/电源
3	白色	橙色/白色	数据	数据/电源
6	蓝色	橙色	数据	数据/电源
4		蓝色	电源	10/100 Mbps 情况下不使用
5		蓝色/白色	电源	10/100 Mbps 情况下不使用
7		棕色/白色	电源	10/100 Mbps 情况下不使用
8		棕色	电源	10/100 Mbps 情况下不使用

SCALANCE W700 设备上 PoE 的 LED

当 SCALANCE W700 设备由 PoE 供电时，SCALANCE W700 设备上的绿色“PoE”LED 将亮起。

安全建议

3

为防止未授权访问，请注意以下安全建议。

常规

- 应定期进行检查以确保设备符合以下建议内容和/或其它安全准则。
- 从安全角度对工厂进行整体评估。将单元保护机制与适当的产品 (https://www.industry.siemens.com/topics/global/en/industrial-security/pages/default.aspx)配合使用。
- 断开内部和外部网络时，攻击者无法从外部访问内部数据。因此请仅在受保护的网络区域内运行该设备。
- 通过非安全网络进行通信时，需额外使用具有 VPN 功能的设备来加密和验证通信。
- 正确终止管理连接（WBM、Telnet、SSH 等）。

物理访问

- 应将该设备限制为仅允许合格人员进行物理访问。
- 存储卡或 PLUG（C-PLUG、KEY-PLUG 和安全 PLUG）中包含可读取和修改的敏感数据，如证书、密钥等。

软件（安全功能）

- 保持固件为最新。定期检查产品的安全更新。
  相关信息请参见 Internet 页面“工业安全 (http://www.siemens.com/industrialsecurity)”。
- 请持续关注由 Siemens ProductCERT (http://www.siemens.com/cert/cn/cert-security-advisories.htm) 出版的安全建议与公告。

- 仅激活使用设备真正需要的协议。
- 使用安全功能（例如，通过 NAT（网络地址转换）或 NAPT（网络地址端口转换）进行地址转换）来防止第三方访问接收端口。
- 通过防火墙或访问控制列表（ACL - 访问控制列表）中的规则限制对设备的访问。
- 如果通过远程访问进行 RADIUS 验证，请确保通信处于安全的网络区域内，或者确保通过安全通道进行通信。
- VLAN 结构化选项可针对 DoS 攻击和未经授权的访问提供良好的保护。请检查该功能在您的环境下是否实用或有效。
- 通过中央记录服务器对更改和访问操作进行记录。在受保护的网络区域内运行记录服务器，并定期检查记录信息。
- 使用具有 AES 的 WPA2/WPA2-PSK 保护 WLAN。如果使用了 iPCF 或 iPCF-MC，请使用 AES 加密。

密码

- 定义密码分配规则。
- 定期更改密码以提高安全性。
- 使用密码强度高的密码。
- 确保所有密码都受到保护，未授权人员无法访问。
- 如果已知或者疑似有未经授权的人员知道了密码，则必须更改密码。
- 请勿将同一密码用于不同用户和系统。

密钥和证书

- 设备带有含密钥的预装证书。将该证书替换为自制的含密钥证书。建议您使用由可靠外部或内部认证机构签署的证书。可通过 WBM（“系统 > 加载和保存”(System > Load and Save)）安装证书。
- 使用认证机构，包括密钥撤销与管理，来签署证书。

- 确保用户自定义的私人密钥均受到保护，未授权人员无法访问。
- 验证服务器和客户端上的证书和指纹，避免"中间人"攻击。
- 建议使用 PKCS#12 格式的受密码保护的证书。
- 建议使用密钥长度至少为 2048 位的证书。
- 如果怀疑发生泄露，请立即更改密钥和证书。

安全/非安全协议和服务

- 应避免使用并禁用非安全协议，例如 Telnet 和 TFTP。由于历史原因，这些协议仍然可用，但并不适用于安全应用。请慎重对设备使用非安全协议。
- 检查是否有必要使用以下协议和服务：
  - 非授权和未加密的端口
  - LLDP
  - Syslog
  - DHCP 选项 66/67
  - TFTP
- 以下协议具有安全备选方法：
  - SNMPv1/v2c → SNMPv3

    检查是否有必要使用 SNMPv1/v2c。SNMPv1/v2c 的分类为非安全协议。使用阻止写访问的选项。产品会为您提供适合的设置选项。

    如果 SNMP 已启用，请更改团体名称。如果不需要不受限制的访问，请通过 SNMP 限制访问。

    配合使用 SNMPv3 和密码。
  - HTTP → HTTPS
  - Telnet → SSH
  - TFTP → SFTP

- 在物理保护措施未阻止设备访问时使用安全协议。
- 为防止对设备或网络的未授权访问，应针对非安全协议采取适当的保护措施。
- 如果需要非安全协议和服务，请仅在受保护的网络区域内运行该设备。
- 将可用于外部的服务和协议限制到最少。
- 要使用 DCP 功能，请在调试后启用"只读"(Read Only) 模式。

可用服务列表

以下是所有可用服务及其端口的列表，通过这些服务和端口可对设备进行访问。

该表包括以下列：

- **服务**

  设备支持的服务

- **默认端口状态**

  此为交付状态（出厂设置）下的端口状态。

- **可组态端口/服务**

  指示是否可通过 WBM/CLI 组态端口号或服务。

- **验证**

  指定是否对通信伙伴进行验证。

  如果可选，可根据需要组态验证。

- **加密**

  指定传输是否加密。

  如果可选，可根据需要组态加密。

服务	协议/端口号	默认端口状态	可组态		验证	加密
			端口	服务		
DHCP 客户端	UDP/68	仅传出	--	✓	--	--
DHCP 服务器	UDP/67	关闭	--	✓	--	--
DNS 客户端	TCP/53 UDP/53	仅传出	--	✓	--	--
EthernetIP	TCP/44818, UDP/2222 UDP/44818	关闭	--	✓	--	--
HTTP	TCP/80	打开	✓	✓	✓	--
HTTPS	TCP/443	打开	✓	✓	✓	✓
NTP 客户端	UDP/123	仅传出	✓	✓	--	--
PROFINET	UDP/34964 UDP/49154 UDP/49155	打开	--	✓	--	--
RADIUS	UDP/1812	关闭	✓	✓	✓	--
远程采集	TCP/2002	关闭	--	✓	--	--
SFTP 客户端	TCP/22	关闭	✓	✓	✓	✓
SMTP 客户端	TCP/25	关闭	✓	✓	--	--
SNMPv1/V2c	UDP/161	打开	✓	✓	--	--
SNMPv3	UDP/161	打开	✓	✓	可选	可选
SNMP 陷阱	UDP/162	仅传出	--	✓	--	--
SNTP 客户端	UDP/123	仅传出	✓	✓	--	--
SSH	TCP/22	打开	✓	✓	✓	✓
Syslog 客户端	UDP/514	关闭	✓	✓	--	--
Syslog（安全）客户端	TCP/6514	关闭	✓	✓	--	✓
Telnet	TCP/23	打开	✓	✓	✓	--
TFTP 客户端	UDP/69	关闭	✓	✓	--	--
DCP	--	打开	--	✓	--	--

服务	协议/端口号	默认端口状态	可组态		验证	加密
			端口	服务		
LLDP	--	打开	--	✓	--	--
RSTP	--	打开	--	✓	--	--
iPRP	--	打开	--	✓	--	--
MSTP	--	关闭	--	✓	--	--
IPv6	--	关闭	--	✓	--	--
SIMATIC NET TIME	--	关闭	--	✓	--	--

技术基础

4

4.1 WBM 和 CLI 的组态限制

设备的组态限制

下表列出了设备基于 Web 的管理和命令行接口的组态限制。

根据您的设备，某些功能不可用。

	可组态的功能		最大数量
System	Syslog 服务器		3
	DNS 服务器	manual (IPv4/IPv6)	3
		learned (IPv4/IPv6)	2
		总计	7
	SMTP 服务器		2
	SNMPv1 陷阱接收方		10
	SNMP 查询		50
	SNTP 服务器 (SNTP server)		2
	NTP 服务器		1
	DHCP 池		1
	DHCP 服务器管理的 IPv4 地址（动态 + 静态）		100
	每个 DHCP 池的 DHCP 静态分配		20
	DHCP 选项		20
接口 (Interface)	强制目标地址漫游		10
	每个 VAP 连接的客户端		100
Layer 2	虚拟 LAN（基于端口，包括 VLAN 1）		24
	多重生成树实例		16

	可组态的功能	最大数量
Security	RADIUS 服务器的 IP 地址	• AAA：4 • WLAN：2
	管理 ACL（管理性访问规则）	10
	MAC ACL 规则组态	20
	MAC ACL 的入站和出站规则（全部）	每个接口 40 条（20 条入站规则/20 条出站规则） • 客户端：80（P1、WLAN） • 接入点：680（P1、WDS 1,Y、VAP 1,Y） • 双接入点：1320（P1、WDS X,Y、VAP X,Y）
	IP ACL 规则组态	20
	端口 ACL IP 的入站和出站规则（全部）	每个接口 40 条（20 条入站规则/20 条出站规则） • 客户端：120（P1、WLAN、管理 VLAN） • 接入点：720 (P1、WDS 1,Y、VAP 1,Y、管理 VLAN） • 双接入点：1360（P1、WDS X,Y、VAP X,Y、管理 VLAN）
	用户角色	28
	用户组	32
	用户	28

4.2 接口和系统功能

接口的可用性

下表列出了物理和逻辑接口的可用性。请注意，该表中列出了所有接口。根据系统功能，某些接口不可用。在 WBM 页面上，只能选择可用的接口。

我们保留进行技术更改的权利。

	客户端设备 **W748-1 M12** **W748-1 RJ-45**	**接入点** **W786-1 RJ-45** **W788-1 M12** **W788-1 RJ-45**	**接入点** **W786-2 RJ-45** **W786-2IA RJ-45** **W786-2 SFP** **W788-2 M12** **W788-2 M12 EEC** **W788-1 RJ-45** **W788-2 RJ-45**
无线接口 (WLAN)	WLAN 1	WLAN 1	• WLAN 1（在客户端模式下，只有一个 WLAN 接口可用） • WLAN 2
IP 接口： LAN 接口 VLAN	 P1 管理 VLAN	 P1 管理 VLAN	 P1 管理 VLAN
VAP 接口 1)	-	VAP 1.Y Y = 1 ... 8	VAP X.Y X = 1 ... 2 Y = 1 ... 8
WDS 接口 1)	_	WDS 1.Y Y = 1 ... 8	WDS X.Y X = 1 ... 2 Y = 1 ... 8
VLAN	24	24	24

1) 仅限接入点模式

系统功能的可用性

下表列出了设备上系统功能的可用性。请注意，本组态手册和在线帮助中介绍了所有功能。根据模式和 KEY-PLUG，某些功能不可用。

我们保留进行技术更改的权利。

			接入点模式	**客户端模式下的接入点。 客户端设备**
Information	**Security**	AP 间阻塞	✓ W780 iFeatures (MLFB 6GK5 907-8PA00) W700 Security (MLFB 6GK5907-0PA00)	-
	WLAN	AP 概述	✓	-
		客户端列表	✓	-
		WDS 列表	✓	-
		AP 重叠	✓	-
		强制漫游	✓	✓
		客户端概述	-	✓
		可用 AP	-	✓
		IP 分配	-	✓
		背景噪声	✓	✓
	WLAN statistics	错误	✓	✓
		已发送管理帧	✓	✓
		已接收管理帧	✓	✓
		已发送数据	✓	✓
		已接收数据	✓	✓
	WLAN iFeatures	iREF 客户端列表	✓ W780 iFeatures (MLFB 6GK5 907-8PA00)	-

			接入点模式	客户端模式下的接入点。 客户端设备
		iREF WDS 列表	✓ W780 iFeatures (MLFB 6GK5 907-8PA00)	-
		AeroScout	✓ W780 iFeatures (MLFB 6GK5 907-8PA00)	-
System		PROFINET	✓	-✓
		EtherNet/IP	✓	✓
Interfaces	**WLAN**	基本	✓	-✓
		扩展	✓	✓
		天线	✓	✓
		允许的通道	✓	✓
		802.11n	✓	✓
		AP	✓	-
		AP WDS	✓	-
		AP 802.11a/b/g 数据传输速率	✓	-
		AP 802.11n 数据传输速率	✓	-
		客户端 802.11a/b/g 数据传输速率	-	✓
		客户端 802.11n 数据传输速率	-	✓
		强制漫游	✓	✓
		信号记录器	-	✓
		频谱分析仪	✓	-

			接入点模式	**客户端模式下的接入点。 客户端设备**
Layer 3	**NAT**	基本	-	✓
		NAPT	-	✓
Security	**WLAN**	基本	✓	✓
		接入点通信	✓	-
		AP RADIUS 验证器	✓	-
		客户端 RADIUS 请求者	-	✓
		密钥	✓	✓
	Inter AP Blocking	基本	✓ W780 iFeatures (MLFB 6GK5 907-8PA00) W700 Security (MLFB 6GK5907-0PA00)	-
		允许的 IP 地址	✓ W780 iFeatures (MLFB 6GK5 907-8PA00) W700 Security (MLFB 6GK5907-0PA00)	-

			接入点模式	客户端模式下的接入点。 客户端设备
iFeatures	**iPCF**		✓ W780 iFeatures (MLFB 6GK5 907-8PA00)	✓ 客户端模式下的接入点： W780 iFeatures (MLFB 6GK5 907-8PA00) 客户端：W740 iFeatures (MLFB 6GK5 907-4PA00)
	iPCF-MC		✓ 仅限双 AP W780 iFeatures (MLFB 6GK5 907-8PA00)	✓ 客户端模式下的接入点： W780 iFeatures (MLFB 6GK5 907-8PA00) 客户端：W740 iFeatures (MLFB 6GK5 907-4PA00)
	iPRP		✓ W780 iFeatures (MLFB 6GK5 907-8PA00)	✓ 客户端模式下的接入点： W780 iFeatures (MLFB 6GK5 907-8PA00) 客户端：W740 iFeatures (MLFB 6GK5 907-4PA00)
	iREF		✓ W780 iFeatures (MLFB 6GK5 907-8PA00)	-

			接入点模式	**客户端模式下的接入点。** **客户端设备**
	AeroScout		✓ W780 iFeatures (MLFB 6GK5 907-8PA00)	-

支持 IPv6

以下系统功能不支持 IPv6 地址：

- AP 间阻塞
- 强制漫游

4.3 EtherNet/IP

EtherNet/IP

EtherNet/IP（以太网/工业协议）是基于 TCP/IP 和 UDP/IP 的工业实时以太网开放式工业标准。通过 EtherNet/IP，应用层中的通用工业协议（Common Industrial Protocol，CIP）可扩展以太网。在 EtherNet/IP 中，OSI 参考模型的低层由以太网通过物理网络和传输功能采用。

在"系统 > EtherNet/IP (页 332)"(System > EtherNet/IP) 中组态 EtherNet/IP。

通用工业协议

通用工业协议 (CIP) 是一种自动化应用协议，支持工业以太网和 IP 网络中现场总线的转换。现场总线/工业网络（如 DeviceNet、ControlNet 和 EtherNet/IP）将此工业协议用作应用层中的接口以连接确定性现场总线领域和自动化应用（控制器、I/O、HMI、OPC ...）。CIP 位于传输层上方，通过自动化工程的通信服务来扩展纯传输服务。其中包括周期性、时间要求严格和事件控制的数据通信服务。CIP 区分时间要求严格的 I/O 消息（隐式消息）和用于组态与数据采集的各个查询/响应帧（显式消息）。CIP 面向对象；所有从外部"可见"的数据都可通过对象的形式进行访问。CIP 具有通用组态基础：EDS（电子数据表）。

电子数据表

电子数据表（Electronic Data Sheet，EDS）是描述设备的电子数据表。

可在"系统 > 加载和保存 (页 246)"(System > Load&Save) 中找到 EtherNet/IP 操作所需的 EDS。

4.4 PROFINET

PROFINET

PROFINET 是基于工业以太网的工业自动化开放式标准 (IEC 61158/61784)。
PROFINET 使用现有 IT 标准，支持现场级到管理级以及工厂范围的工程系统的端到端通信。PROFINET 还具有下列特性：

- 使用 TCP/IP 协议
- 满足实时要求的自动化应用
  - 实时 (RT) 通信
  - 等时实时 (IRT) 通信
- 无缝集成现场总线系统

在“系统 > PROFINET”(System > PROFINET) (页 329) 中组态 PROFINET。

PROFINET IO

在 PROFINET 的框架内，PROFINET IO 是实现模块化、分布式应用的通信机制。
PROFINET IO 由可编程控制器的 PROFINET 标准 (IEC 61158-x-10) 实现。

4.5 VLAN

与节点的空间位置无关的网络定义

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

VLAN 的独特优势是可减少其它 VLAN 的节点和网段的网络负载。

为确定将哪个帧分配到哪个 VLAN，请将帧扩展 4 个字节（VLAN 标记）。除了 VLAN-ID，此扩展还包括优先级信息。

VLAN 分配选项

对 VLAN 分配有多种选项。

- 基于端口的 VLAN

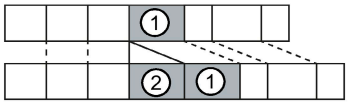
  为设备的每个端口分配一个 VLAN ID。可在“第 2 层 > VLAN”(Layer 2 > VLAN) (页 426) 中组态基于端口的 VLAN。

- 基于协议的 VLAN
  为设备的每个端口分配一个协议组。

- 基于子网的 VLAN
  为设备的 IP 地址分配一个 VLAN ID。

双重标记的帧 (Q-in-Q)

有些设备（例如 SCALANCE XR500）支持 Q-in-Q 功能。借助 Q-in-Q 功能，传入数据通信被视为无标记。如果帧已标记 ①，则意味着它们将扩展有第二个 VLAN 标记（外部 VLAN 标记 ②）。



当 SCALANCE W 设备接收到双重标记的帧时，会使用外部 VLAN 标记 ② 的 VLAN ID 和内部 VLAN 标记 ① 的优先级信息。然后帧会被转发给相关 VLAN。

4.6 基于 MAC 的通信

由客户端发往接入点的帧始终将 WLAN 客户端的 MAC 地址作为源 MAC 地址。因此，在接入点的"学习表"中，只包含 WLAN 客户端的 MAC 地址。

MAC 模式"自动"、"手动"和"自身"

如果采用（自动）或手动设置（手动）连接到客户端的设备的 MAC 地址，则基于 MAC 和基于 IP 的帧两者都只能为该设备找到其目标地址。如果使用（自身）WLAN 客户端的以太网接口的 MAC 地址，则基于 MAC 和基于 IP 的帧只能访问 WALN 客户端。

接入点会检查目标 MAC 地址是否与所连接客户端的 MAC 地址匹配。由于 WLAN 客户端只能使用一个 MAC 地址，因此 MAC 地址级别（ISO/OSI 第 2 层）最多可连接客户端下游或客户端本身的一个节点。

通过 IP 映射，可基于 IP 协议寻址客户端下游的多个节点。按照内部表将 IP 数据包分解，并将其转发到所连接的设备。

与客户端下游第 2 层通信的以太网结点的最大可能数：1

"自动"(Automatic) 设置的注意事项：

- 只要以太网接口上没有链路，设备就会使用以太网接口的 MAC 地址，从而可在该状态下对设备进行访问。在该状态下，可使用 SINEC PNI 找到设备，可使用 WBM 或 CLI 对其进行组态。
- 一旦以太网接口上存在链路，设备就会采用接收到的第一个帧的源 MAC 地址。

说明

从设备采用其他 MAC 地址（手动或自动）时开始，当设备通过 WLAN 接口接收到 SINEC PNI 发来的查询时，就不再对查询进行响应。但仍会响应通过以太网接口收到的 SINEC PNI 查询。

MAC 模式"第 2 层隧道"

WLAN 客户端的 WLAN 接口使用以太网接口的 MAC 地址。

同时也会将连接到 WLAN 客户端以太网接口的 MAC 地址通知给接入点。这样就可以在接入点"学习表"(learning table) 中输入这些设备的 MAC 地址。接入点可以为客户端下游的设备将基于 MAC 的帧转发到适当的客户端。

与 WSD 非常相似，将为 L2T 客户端创建一个独立的端口，从而不需要改变目标 MAC 地址，就可以通过该端口发送以太网帧。

客户端下游以太网节点的最大可能数：8

4.7 iPCF/iPCF-HT/iPCF-MC

可以用多个接入点来扩大 IWLAN 系统的无线覆盖范围。如果客户端从一个接入点的覆盖范围移动另一个接入点的覆盖范围，将在短时间的中断后保持无线链路（漫游）。

如果需要很短的更新时间（例如 PROFINET 通信），则需要使用接入点和客户端模块，它们采用专有方法 iPCF/iPCF-HT 或 iPCF-MC 来进行快速漫游和确定性数据通信。

iPCF/iPCF-HT/iPCF-MC 只能单独工作。彼此之间不能组合，例如不允许 iPCF 与 iPCF-HT 或 iPCF-MC 组合。

工作原理

iPCF

使用 iPCF 时，接入点周期性检查无线蜂窝区中的所有节点。同时，还会扫描该节点下行链路的流量。在回复中，节点会发送上行链路数据。接入点至少每 5 ms 扫描一次新节点。

蜂窝区中的所有其它节点都可看到该节点扫描结果。这样，即使客户端没有与接入点本身进行通信，也可以检测与接入点的无线链路质量。如果客户端在一定时间内未收到接入点发来的任何数据帧，它就开始搜索新的接入点。

在 iPCF 模式下，搜索新接入点与注册此接入点都可得到时间方面的优化。从而实现了切换时间明显低于 50 ms。

“Legacy Free (iPCF-LF)”设置可防止 IEEE 802.11 a/b/g 设备系列导致性能降低。启用该设置后，仅接受按照 IEEE 802.11n 标准进行通信并启用了“Legacy Free (iPCF-LF)”设置的设备。但无需为此启用 WLAN 模式 IEEE 802.11n。

只有在 WLAN 客户端始终处于高于 60%（或 -65 dBm）信号强度的无线蜂窝区时，才能实现稳定的 PROFINET 通信。可通过激活和停用不同无线蜂窝区来对此进行检查。

这并不表示信号强度低于 60 % (< -65 dBm) 时需要对客户端进行改变。确保接入点有足够的信号强度。

在“iFeatures > iPCF > iPCF”中组态 iPCF。

iPCF-HT

如果 iPCF 需要较高的数据吞吐量，则使用 iPCF-HT。例如，还可借此使用 PROFINET 传输视频数据。这通过使用帧突发 (A-MPDU) 更有效地传输数据包来实现。将用于同一接收站（客户端）且具有相同优先级的单独数据包组合在一起。

在“iFeatures > iPCF > iPCF-HT”中组态 iPCF-HT。

iPCF-MC

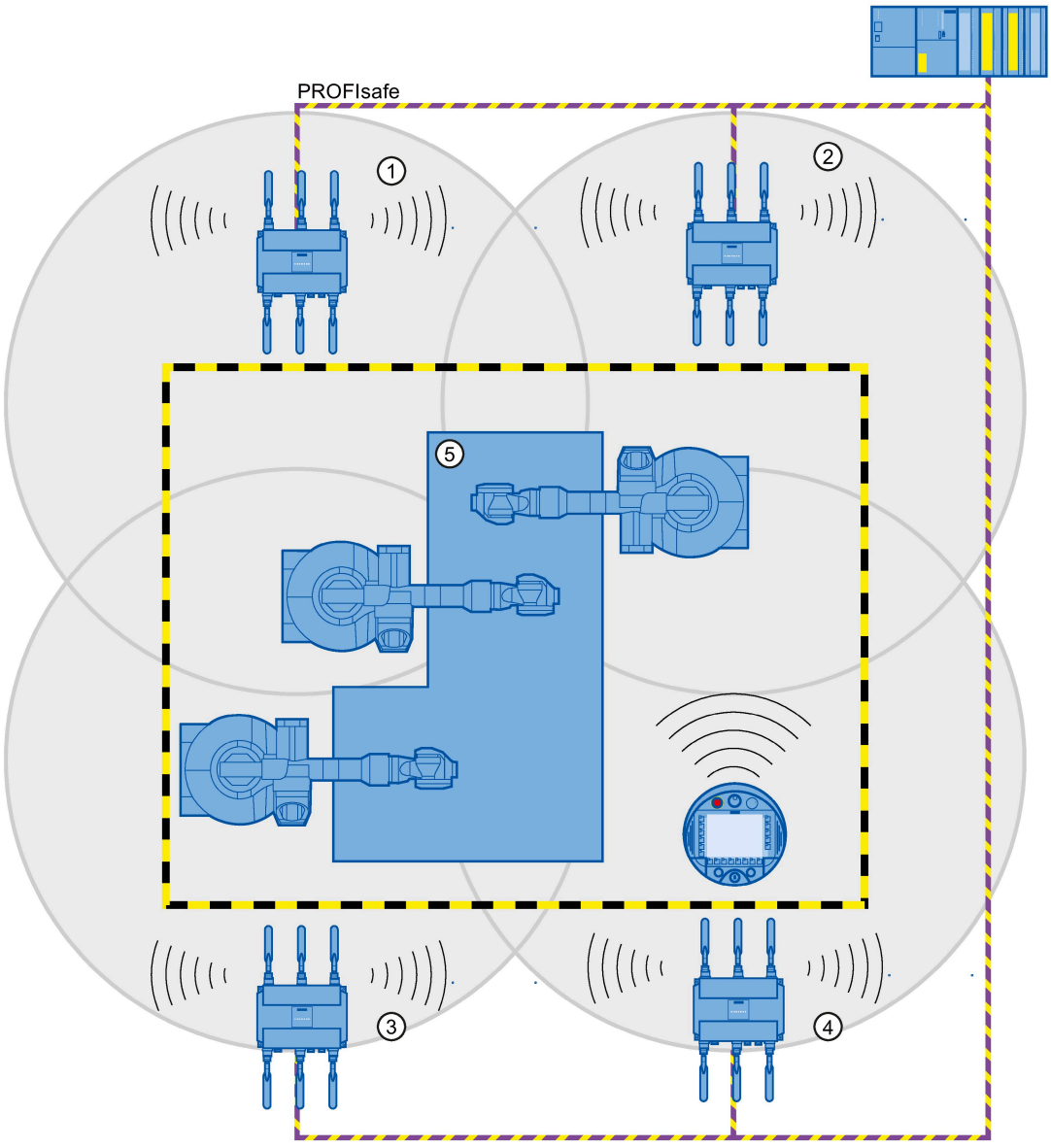
对于独立于 RCoax 电缆或定向天线进行通信的自由移动节点，应使用 iPCF-MC。使用 iPCF-MC 时，在客户端收到接入点发来的 iPCF 查询，且存在与接入点的有效连接的情况下，客户端也会搜索潜在的合适接入点。这就意味着在需要切换到另一个接入点时，可以极快地实现切换。与 iPCF 不同的是，iPCF-MC 的切换时间不取决于正在使用的无线通道数。

需要使用具有两个无线接口的接入点，即所谓的双接入点。其中一个接口作为管理通道，用于发送具有管理信息（例如 SSID 和数据通道的通道设置）的短帧（信标）。另一个接口（数据通道）专用于传送用户数据。

“Legacy Free (iPCF-LF)”设置可防止 IEEE 802.11 a/b/g 设备系列导致性能降低。启用该设置后，仅接受按照 IEEE 802.11n 标准进行通信并启用了“Legacy Free (iPCF-LF)”设置的设备。但无需为此启用 WLAN 模式 IEEE 802.11n。

在“iFeatures > iPCF > iPCF-MC”中组态 iPCF-MC。

下图显示了 iPCF-MC 组态示例。



① 接入点 1 的无线蜂窝区
② 接入点 2 的无线蜂窝区
③ 接入点 3 的无线蜂窝区
④ 接入点 4 的无线蜂窝区
⑤ 设备

限制

- iPCF/iPCF-HT 和 iPCF-MC 由 Siemens AG 开发，仅对实施了 iPCF/iPCFv2/iPCF-MC 的节点起作用。
- 具有一个 WLAN 接口的接入点无法参与 iPCF-MC 过程，但可使用 iPCF。
- iPCF-HT 仅在 WLAN 接口 1 上可用，且只能用于 WLAN 模式为“（仅）IEEE 802.11n”的 5 GHz 频段。

说明

对于带有两个 WLAN 接口的接入点，如果两接口以相同频率范围运行：

- 则连接 R1A1、R1A2、R1A3 的天线之间与连接 R2A1、R2A2、R2A3 的天线之间的距离必须至少为 1 m。
- 如果传输功率高于 15 dB，则一个或两个 WLAN 接口都可能有无线干扰。

说明

SCALANCE W788-2 和 SCALANCE W786-2

在实时通信过程中，如果接入点带有两个 WLAN 接口，则可通过 IPCF-MC 建立管理通道。但使用 iPCF 时，不建议使用另一个 WLAN 接口。

iPCF-MC 的使用要求

iPCF-MC 以不同的方式使用接入点的两个无线接口：一个接口用作管理接口，每五毫秒发送一个信标。另一个接口传送用户数据。

在使用 iPCF-MC 之前，必须满足以下要求：

- 仅具有两个 WLAN 接口的 SCALANCE W700 设备才能用作接入点
- 数据接口 (WLAN1) 和管理接口 (WLAN2) 必须工作在同一频段，并且在无线覆盖方面必须匹配。如果两个无线接口均配备了覆盖不同区域的定向天线，则 iPCF-MC 无法工作。
- 客户端可切换到的所有接入点的管理接口必须使用同一通道。客户端仅扫描这一通道，以找到可访问的接入点。

- 管理接口不能使用基于 IEEE 802.11h (DFS) 的传输。802.11h (DFS) 可用于数据接口。
- 客户端的 WLAN 接口必须支持此功能。

4.8 iREF

工作原理

若一个接入点有多根已激活的天线，则发射功率被平均分配到这些天线上。发射功率是受国家/地区法律限制的。最大允许功率取决于所连接天线的增益。若所连接的天线增益不同，则实际上由最大天线增益限制允许的发射功率。

iREF（工业范围扩展功能）可确保用最适合的天线来处理接入点和每个独立客户端之间的数据通信。最适合的天线由接入点根据所接收数据包的 RSSI 值来确定。

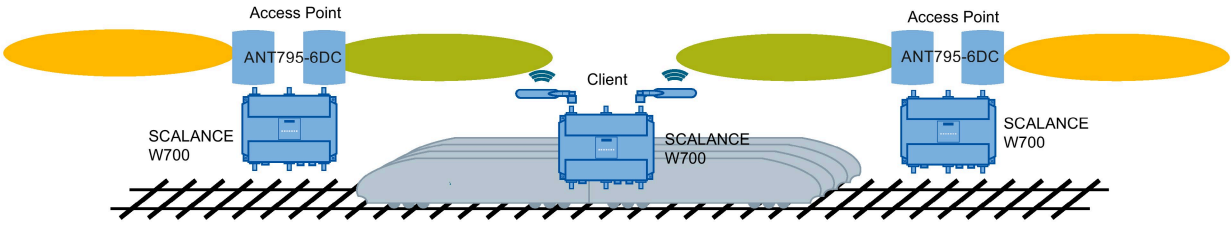
考虑到天线的增益和可能的电缆损耗，数据包只通过可让客户端获得最大信号强度的天线发送。

在此期间，其它天线停用，法律允许的发射功率仅适用于所选天线。停用的天线不会限制允许的发射功率。

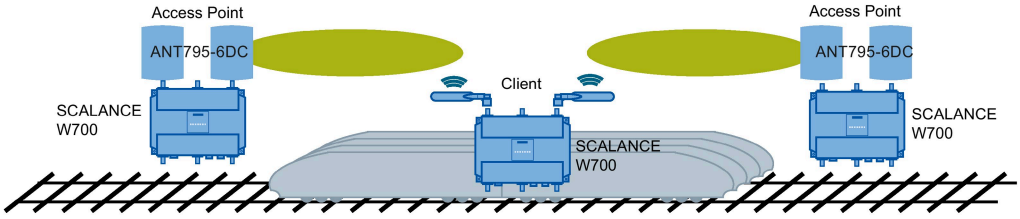
特别是对于 MIMO 无法使用或不具任何优势的应用，这使得数据能够以最高可能的数据传输率传输。

在“iFeatures > iREF (页 544)”中组态 iREF。

无 iREF



其中 iREF



要求

- 要使用 iREF，SCALANCE W700 设备必须至少有 2 根已激活的天线。

限制

- 最大数据传输率最高只能达到 150 Mbps（MCS 0 - 7 或 1 x 空间流）。
- iREF 不能与其它 iFeatures（例如 iPCF 或 iPCF-MC）一起使用

优点

- 由于采用定向数据传输和动态停用不向该特定客户端方向发射信号的天线，因此可减少干扰。
- 信号强度也会提高，因为激活天线总是能分配到最大允许发射功率。

4.9 iPRP

“并行冗余协议”(PRP) 是用于有线网络的冗余协议。它是在 IEC 62439 标准的第 3 部分中定义的。

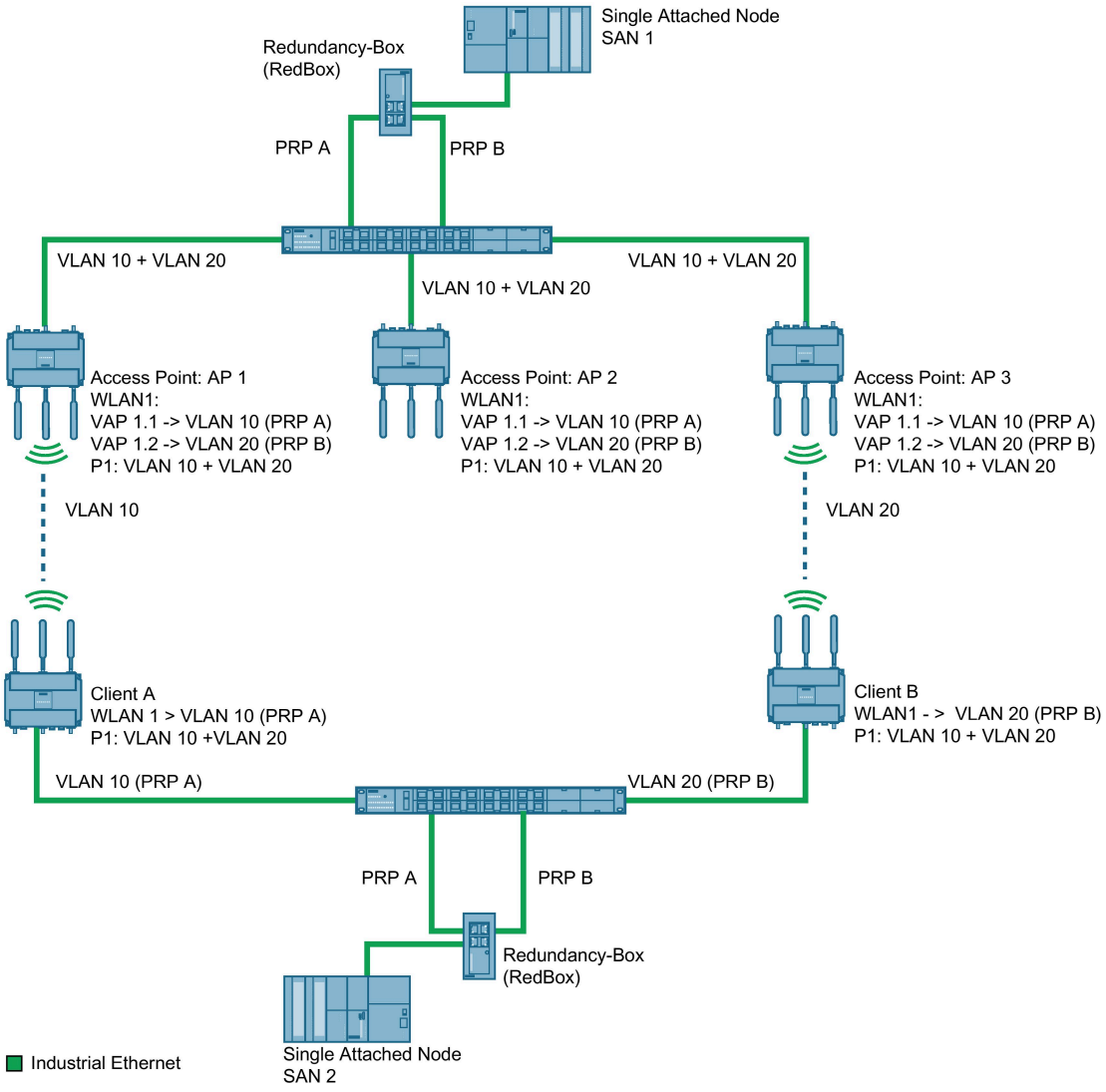
借助"工业并行冗余协议"(iPRP)，可在无线网络中使用 PRP 技术。这增强了无线通信的可用性。

工作原理

PRP 网络包含两个完全独立的网络。如果其中一个网络中断，则会通过并行冗余网络发送帧，且不会中断/无需进行重新组态。为此，将通过两个网络向接收方重复发送以太网帧。具备 PRP 功能的设备至少有两个独立的以太网接口，这些接口分别连接于独立的网络。

对于不具备 PRP 功能的设备，在上游连接了冗余盒 (RedBox)。这样，所谓的单连接节点 (SAN) 便可访问 PRP 网络。RedBox 会复制待发送的每个以太网帧，还会将 PRP 尾部添加至相应帧（包含序列号）。RedBox 同时将帧的副本发送到 PRP A 和 PRP B 网络。在接收端，重复的帧被 RedBox 丢弃。为此，RedBox 需要专用于以太网的特定传送时间。因此在 WLAN 网络中使用 PRP 会导致帧重复和延迟。

使用 iPRP 可以解决此问题，并且可以在包含 SCALANCE W700 设备的 WLAN 中使用 PRP



接入点（AP 1、AP 2 和 AP 3）与 AP 端的 RedBox 通过交换机彼此相连。PRP 网络 A 和 B 通过 VLAN 彼此分开。

如果 SAN1 将帧发送至 SAN2，则该帧由 AP 端的 RedBox 复制，并且两个冗余帧通过交换机传送到接入点。通过两种不同的无线路径，将冗余 PRP 帧传送到客户端的 RedBox。客户端也通过交换机与其 RedBox 相连。这会将到达的第一个 PRP 帧转发给 SAN2，并丢弃第二个帧。

说明

在连接至 SCALANCE W700 设备的交换机接口中，只能组态在 SCALANCE W700 设备的 VAP 或者 WLAN 接口上设置的 VLAN。

使用 iPRP 时，冗余伙伴（这里为：AP1 和 AP3 或者客户端 A 和客户端 B）通过交换机彼此进行通信，以防止两个冗余 PRP 帧到达 RedBox 所用的时间相差过大。

例如，如果 AP1 和客户端 A 之间的通信速度非常慢，则在接收端将丢弃较慢的帧。

在“iFeatures > iPRP (页 540)”中组态 iPRP。

要求

- 设置了基础网桥模式“802.1Q VLAN 网桥”(802.1Q VLAN Bridge)。
- 已创建 VLAN。
- 接入点模式：VAP 接口已启用。
- 在客户端模式下：
  - 对于“MAC 模式”(MAC Mode)，已设置“第 2 层隧道”(Layer 2 Tunnel)。
  - 对于“后台扫描模式”(Background Scan mode)，已设置“始终”(Always)、“取消激活”(Deactivated) 或“当前通道”(Current channel)。
- 无论组态如何，客户端都可与每个接入点进行通信。

4.10 AeroScout

AeroScout 标签

SCALANCE W700 设备支持 AeroScout 公司的标签。这些标签是用电池供电的 RFID 传感器，可周期性地将其数据以组播帧的形式发出。

此外，AeroScout 标签具有以下特征：

- **环境温度**

  如果将标签安装到 SCALANCE W700 设备或材料中，则可以监视是否保持了所选的环境温度。

- **运动**

  标签还可以提供用于指示其处于运动还是静止状态的信息。物料流和物料加工工程区域体现了该功能的可能应用。

- **按钮**

  尽管会周期性发送帧，用户仍可以通过按下按钮来发送消息。

- **LED**

  可提供有关标签工作状态的信息。

说明

要获得更多详细信息，请参见 AeroScout 文档 (www.aeroscout.com)。

工作原理

标签可发送 AeroScout 帧形式的数据。标签与接入点在 2.4 GHz 频段下通信。

如果接入点的 WLAN 接口接收到 AeroScout 帧，则会将其转换为 UDP 数据报。SCALANCE W700 设备会将 UDP 数据报连同信号强度 (RSSI) 的信息转发至 PC。AeroScout Engine 在 PC 上运行，可对接收到的信息进行评估。

说明

最好**不要**在同一个无线接口上同时使用 PROFINET 通信和 AeroScout。

定位精度

为了在 AeroScout 标签的定位中获得最佳精度，

- 建议使用具有全向特性的天线
- 如果信号应被至少 3 个接入点接收。

4.11 NAT/NAPT

什么是 NAT?

网络地址转换 (NAT) 是一种简化的源 NAT，也称 IP 地址伪装。对于通过该接口发送的每个传出数据包，源 IP 地址均替换为该接口的 IP 地址。调整后的数据包发送到目标 IP 地址。对于目标主机，查询似乎始终来自同一发送方。外部网络无法直接访问内部节点。

在“第 3 层 > NAT > 基础”(Layer 3 > NAT > Basic) (页 450) 中组态 NAT。

什么是 NAPT?

NAPT（网络地址和端口转换）是一种目标 NAT，也称为端口转发。设备将终端设备的外部 IP 地址替换为设备的内部 IP 地址。设备还会更改端口号。

分配的 IP 地址和端口号存储在 NAT 表中。如果设备在某个端口上接收到数据包，则将在 NAT 表中搜索相应的条目。如果存在条目，则会添加 IP 地址和端口号作为目标并转发数据包。

说明

NAT/NAPT 仅在 ISO/OSI 参考模型的第 3 层可用。要使用 NAT 功能，网络必须使用 IP 协议。
使用运行在第 2 层的 ISO 协议时，不能使用 NAT。

在“第 3 层 > NAT > NAPT”(Layer 3 > NAT > NAPT) (页 455) 中组态 NAT 表。

4.12 SNMP

简介

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

SNMP 的任务：

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

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

如果只需对访问权限进行简单控制而无需考虑安全性，则可使用团体字符串。

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

团体字符串的标准值：

- public
  具有只读权限
- private
  具有读写权限

说明

由于 SNMP 团体字符串用于访问保护，请勿使用标准值“public”或“private”。请在初始调试之后更改这些值。

设备级的更多简单保护机制：

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

SNMP 数据包未加密，其他用户可轻松读取。

中央站也称为管理站。SNMP 代理安装在与管理站交换数据的被监视设备上。

管理站发送以下类型的数据包：

- GET
  向 SNMP 代理请求数据记录
- GETNEXT
  调用下一条数据记录。
- GETBULK （自 SNMPv2c 起可用）
  每次请求多条数据记录，例如，表中的多行。
- SET
  包含相关设备的参数分配数据。

SNMP 代理发送以下类型的数据包：

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

SNMPv1/v2c/v3 使用 UDP（User Datagram Protocol，用户数据包协议）并使用 UDP 端口 161 和 162。管理信息库 (Management Information Base, MIB) 对该数据进行了介绍。

SNMPv3

与先前版本 SNMPv1 和 SNMPv2c 比较，SNMPv3 引入了广义的安全概念。

SNMPv3 支持：

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

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

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

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

使用该功能时的限制

仅可在更换设备时使用"SNMPv3 用户移植"(SNMPv3 User Migration) 功能将组态的 SNMPv3 用户传送到替代设备。
请勿使用该功能将组态的 SNMPv3 用户传送到多个设备。如果将具有已创建的 SNMPv3 用户的组态加载到多个设备，则这些设备会使用相同的 SNMP 引擎 ID。如果在同一网络中使用这些设备，则组态会与 SNMP 标准相矛盾。

与旧产品的兼容性

如果您已将用户创建为可移植用户，则可以将已组态的 SNMPv3 用户传送至不同的设备。为创建可移植用户，创建时必须激活"SNMPv3 用户移植"(SNMPv3 User Migration) 功能。

4.13 生成树

避免回路

生成树算法会检测冗余物理网络结构，并通过禁用冗余路径的方式来防止构成回路。它会评估连接的距离和性能，或根据用户的设置作出决定。这样，只会通过剩余的网络路径来交换数据。

如果首选数据路径出现故障，生成树算法会搜索由剩余节点构成的最有效的可用路径。

根网桥和网桥优先级

最佳连接的识别总是与根网桥相关，根网桥是可视为树状网络结构根元素的网络组件。可以用“网桥优先级”(Bridge Priority) 参数来控制根网桥的选择。该参数具有最低设置值的计算机将自动成为根网桥。如果两台计算机的优先级值相同，则 MAC 地址较小的计算机成为根网桥。

对网络拓扑变化的响应

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

使组态信息保持最新

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

网桥不会立即使用新的组态数据，而是在经过“转发延迟”(Forward Delay) 参数中指定的时间之后才使用。这样可确保在所有网桥都收到所需的信息之后才开始使用新拓扑运行。

4.13.1 RSTP、MSTP、CIST

快速生成树协议 (RSTP)

STP 的一个缺点是如果出现中断或设备故障，网络需要对自身进行重新组态：仅当出现中断时设备才会开始协商新路径。这最多需要 30 秒钟的时间。为此，STP 得到了扩展以创建"快速生成树协议"（RSTP，IEEE 802.1w）。设备在正常运行期间已经收集到有关备选路径的信息，不需要在发生中断后再收集此信息，这点与 STP 有本质区别。这意味着，由 RSTP 控制的网络的重新组态时间可以缩短至几秒钟。
通过使用以下功能可以实现这一点：

- 边缘端口（终端节点端口）
  边缘端口是指连接到终端设备的端口。
  定义为边缘端口的端口会在建立连接后立即激活。如果在边缘端口接收到生成树 BPDU，该端口将失去其作为边缘端口的角色，并重新参与 (R)STP。如果经过特定的时间（3 倍呼叫时间）后没有再接收到任何 BPDU，则该端口返回到边缘端口状态。
- 点对点（两个邻近设备之间直接通信）
  通过直接连接两个设备，可以无延迟地进行状态变化（重新组态端口）
- 备用端口（根端口的替代端口）
  组态根端口的替代端口。如果失去与根网桥的连接，设备可以通过备用端口建立连接，不存在由重新组态导致的延迟。
- 对事件的反应
  快速生成树可无延迟地对事件（例如连接中止）做出反应。不用像在生成树中一样等待计时器。
- 最大网桥跳跃计数器
  数据包自动变为无效之前所允许的网桥跳跃数。

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

多重生成树协议 (MSTP)

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

公共内部生成树 (CIST)

CIST 可识别交换机使用的在原理上与 RSTP 内部实例类似的内部实例。

4.14 用户管理

用户管理概述

通过可组态的用户设置来管理对设备的访问。使用密码设置用户以供验证。为用户分配具有适当权限的角色。

用户的身份验证可在本地由设备执行，也可由外部 RADIUS 服务器执行。可在“安全 > AAA > 常规”(Security > AAA > General) 页面中组态身份验证的处理方式。

本地登录

用户本地登录时设备的工作方式如下：

1. 用户通过用户名和密码在设备上登录。
2. 设备检查是否存在该用户的条目。

   → 如果存在条目，该用户成功登录并具有所关联角色的权限。

   → 如果不存在相应的条目，则拒绝该用户登录。

通过外部 RADIUS 服务器登录

RADIUS（Remote Authentication Dial-In User Service，拨入用户远程认证服务）是通过集中存储用户数据的服务器来验证用户和为用户授权的协议。

根据您在“安全 > AAA > RADIUS 客户端”(Security > AAA > RADIUS Client) 页面中所选择的 RADIUS 验证模式，设备可评估 RADIUS 服务器的不同信息。

RADIUS 身份验证模式“Standard”

如果已设置身份验证模式“conventional”，则用户在 RADIUS 服务器上的身份验证将按如下方式运行：

1. 用户通过用户名和密码在设备上登录。
2. 设备将带有登录数据的身份验证请求发送到 RADIUS 服务器。
3. RADIUS 服务器执行检查并将结果发送回设备。
   - RADIUS 服务器报告身份验证成功，并向设备的属性“Service Type”返回值“Administrative User”。

     → 用户登录并带有管理员权限。
   - RADIUS 服务器会报告身份验证成功，并会向设备的属性“Service Type”返回差异或甚至是无值。

     → 用户登录并具有读取权限。
   - RADIUS 服务器向设备报告身份验证失败：

     → 用户被拒绝访问。

RADIUS 模式“SiemensVSA”

要求

对于 RADIUS 验证模式“Siemens VSA”，需要在 RADIUS 服务器上设置以下需求：

- 制造商代码：4196
- 属性编号：1
- 属性格式：字符型字符串（组名称）

步骤

如果已设置身份验证模式“SiemensVSA”，则用户在 RADIUS 服务器上的身份验证将按如下方式运行：

1. 用户通过用户名和密码在设备上登录。
2. 设备将带有登录数据的身份验证请求发送到 RADIUS 服务器。
3. RADIUS 服务器执行检查并将结果发送回设备。

情况 A：RADIUS 服务器报告身份验证成功，并向设备返回已为用户分配的组。

– 组已在设备中已知，但用户并未在表“外部用户帐户”中输入。

→ 用户将登录并具有所分配组的权限。

– 组已在设备中已知，且用户并已在表“外部用户帐户”中输入。

→ 已为用户分配了更高的权限，用户会登录并拥有这些权限。

– 组已在设备中未知，且用户并已在表“外部用户帐户”中输入。

→ 用户将登录并具有已链接到用户帐户的角色所对应的权限。

– 组已在设备中未知，但用户并未已在表“外部用户帐户”中输入。

→ 用户将登录并具有“Default”角色的权限。

情况 B：RADIUS 服务器会报告身份验证成功，但不会向设备返回一个组。

– 用户已在“外部用户帐户”表中输入：

→ 用户将登录并具有所链接角色的权限。

– 用户未在“外部用户帐户”表中输入：

→ 用户将登录并具有“Default”角色的权限。

情况 C：RADIUS 服务器向设备报告身份验证失败：

– 用户被拒绝访问。

IP 地址

5

5.1 IPv4/IPv6

有哪些本质区别？

	IPv4	IPv6
IP 组态	• DHCP 服务器 • 手册	• 无状态地址自动配置 (SLAAC)：采用 NDP（邻居发现协议）的无状态自动配置 – 为各个在链路中无需路由器的接口创建链路本地地址。 – 检查在链路中无需路由器的链路地址的唯一性。 – 指定是否通过无状态机制、有状态机制或两种机制获得全局地址。（在链路中需要路由器。） • 手册 • DHCPv6（有状态）
可用 IP 地址	32 位：4.29 * 10^9 个地址	128 位：3.4 * 10^{38} 个地址
地址格式	十进制：192.168.1.1 端口为： 192.168.1.1:20	十六进制：2a00:ad80::0123 端口为：[2a00:ad80::0123]:20
回送	127.0.0.1	::1
接口的 IP 地址	4 个 IP 地址	多个 IP 地址 • LLA：每个接口的链路本地地址（自动形成） fe80::/128 • ULA：每个接口的多个唯一本地单播地址 • GUA：每个接口的多个全局单播地址
标头	• 校验和 • 可变长度 • 报头分片 • 无安全性	• 在较高层检查 • 固定大小 • 扩展报头分片

	IPv4	**IPv6**
分片	主机和路由器	仅通信的端点
服务质量	服务类型 (ToS) 的优先级	在报头字段"通信类别"(Traffic Class) 中指定优先级。
帧类型	广播、组播、单播	组播、单播、任播
DHCP 客户端/服务器的标识	客户端 ID： • MAC 地址 • DHCP 客户端 ID • 系统名称 • PROFINET 站名称 • IAID 和 DUID	DUID + IAID 恰好为主机的一个接口 DUID = DHCP 唯一标识符 服务器和客户端的唯一标识符 IAID = 身份关联标识符 每个接口至少有一个由客户端生成，且在 DHCP 客户端重新启动时保持不变 获取 DUID 的三种方法 • DUID-LLT • DUID-EN • DUID-LL

	IPv4	**IPv6**
DHCP	通过 UDP 广播	通过 UDP 单播 RFC 3315、RFC 3363 **有状态的 DHCPv6** 有状态组态，在其中传送 IPv6 地址和组态设置。 客户端和服务器之间交换以下四种 DHVPv6 消息： 1. SOLICIT: 由 DHCPv6 客户端发送，用于定位 DHCPv6 服务器。 2. ADVERTISE 可用的 DHCPv6 服务器对此做出应答。 3. REQUEST DHCPv6 客户端从 DHCPv6 服务器请求 IPv6 地址和组态设置。 4. REPLY DHCPv6 服务器发送 IPv6 地址和组态设置。 如果客户端和服务器支持"Rapid commit"功能，本步骤将缩短为两种 DHCPv6 消息 SOLICIT 和 REPLY。 **无状态 DHCPv6** 在无状态 DHCPv6 中，仅传送组态设置。 **前缀代理** DHCPv6 服务器将 IPv6 前缀的分配委托给 DHCPv6 客户端。DHCPv6 客户端也称为 PD 路由器。
硬件地址中 IP 地址的解析	ARP（地址解析协议）	NDP（邻居发现协议）

5.2 IPv4 地址

5.2.1 IPv4 地址的结构

IPv4 地址由 4 个十进制数字组成，各数字间用点分隔。每个十进制数字均可介于 0 到 255 之间。

示例：192.168.16.2

IPv4 地址包括：

- （子）网络的地址
- 节点（通常也称为终端节点、主机或网络节点）地址

子网掩码

子网掩码由四个范围在 0 到 255 之间的十进制数字组成，每个数字以句点分隔；例如：255.255.0.0

在用二进制表达子网掩码的 4 个十进制数字时，表达式必须包含从左侧起的一系列连续的“1”和从右侧起的一系列连续的“0”。

“1”值确定 IPv4 地址内的网络地址。“0”值确定 IPv4 地址内的设备地址。

示例：

正确值

255.255.0.0 D = 1111 1111.1111 1111.0000 0000.0000 0000 B

255.255.128.0 D = 1111 1111.1111 1111.1000 0000.0000 0000 B

255.254.0.0 D = 1111 1111.1111 1110.0000 0000.0000.0000 B

不正确值：

255.255.1.0 D = 1111 1111.1111 1111.0000 0001.0000 0000 B

子网掩码：255.255.0.0 = 11111111.11111111.00000000.00000000

在上述 IP 地址示例中，此处显示的子网掩码具有以下含义：

IP 地址的前 2 个字节确定子网，即 192.168。后两个字节寻址设备，即 16.2。

通常情况下，以下规则适用：

- 网络地址来自 IPv4 地址和子网掩码的“与”逻辑组合。
- 设备地址来自 IPv4 地址和子网掩码的“与非”逻辑组合。

无类域间路由 (CIDR)

CIDR 是一种方法，其结合子网掩码表示 IPv4 地址，将多个 IPv4 地址集成到一个地址范围。为此，通过在 IPv4 上附加后缀将网络掩码位数设置指定为 1。CIDR 表示法可减小路由表大小并更好地利用可用地址范围。

示例：

IPv4 地址为 192.168.0.0，对应子网掩码为 255.255.255.0

以二进制表示时，地址的网络部分包含 3 x 8 位；即 24 位。

CIDR 表示法的结果为 192.168.0.0/24。
按二进制表示法时，主机部分包含 1 x 8 位。这使得地址范围变为 2 的 8 次方，即包含 256 个可能的地址。

屏蔽其他子网

使用子网掩码，可以进一步构造分配给地址类别 A、B 或 C 之一的子网，并通过将子网掩码的其他低位数字设置为“1”来形成“专用”子网。对于设置为“1”的每个位，“专用”网络的数量加倍，并且其中包含的节点数减半。从外部看，该网络仍然看起来像单一的网络。

示例：

可以对地址类别 B 的子网（例如 IP 地址 129.80.xxx.xxx）的默认子网掩码进行如下更改：

掩码	十进制	二进制
默认子网掩码	255.255.0.0	11111111.11111111.00000000.00000000
子网掩码	255.255.128.0	11111111.11111111.10000000.00000000

结果：

地址范围为 129.80.001.xxx 到 129.80.127.xxx 的所有设备均位于一个 IP 子网中，地址范围为 129.80.128.xxx 到 129.80.255.xxx 的所有设备均位于另一个 IP 子网中。

网络网关（路由器）

网络网关（路由器）的任务是连接 IP 子网。如果要将 IP 数据报发送到另一个网络，则必须先将其发送到路由器。为此，需要为 IP 子网的每个成员输入路由器地址。

子网中设备的 IP 地址与网络网关（路由器）的 IP 地址唯一可能不同的位置是子网掩码设置为“0”的点。

5.2.2 IPv4 地址的初始分配

组态选项

不能使用基于 Web 的管理 (MBM) 或命令行接口 (CLI) 通过 Telnet 为 SCALANCE W 分配初始 IP 地址，因为这些组态工具要求事先已经有 IP 地址。

可通过以下方式将 IP 地址分配给当前尚没有 IP 地址的未组态设备：

- DHCP（默认）
- SINEC PNI

- STEP 7
- SINEC NMS

说明

产品出厂时以及在"恢复存储器默认设置并重启"后，DHCP 都处于启用状态。
如果局域网中有 DHCP 服务器，且其能回应 SCALANCE W 设备的 DHCP 请求，则在初次启动设备时会自动分配 IP 地址、子网掩码和网关。"恢复出厂默认设置并重启"不会删除由 DHCP 或用户分配的 IP 地址。

5.2.3 通过 DHCPv4 分配地址

DHCP 属性

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

- 启动设备时和设备运行期间均可使用 DHCP。
- 分配的 IP 地址仅在有限时间（称为租用时间）内有效。当有效时间段过半后，DHCP 客户端可延长所分配 IPv4 地址的有效时间。当整个时间段过期后，DHCP 客户端需要请求新的 IPv4 地址。

- 通常不会分配固定的地址；即，当客户端再次请求 IP 地址时，它通常会接收到一个与之前不同的地址。可以对 DHCP 服务器进行组态，使得 DHCP 客户端发出请求后，总是接收到同一个固定地址。用来将 DHCP 客户端标识为固定地址分配的参数在 DHCP 客户端上设置。可以通过 MAC 地址、DHCP 客户端 ID、PROFINET 设备名称或设备名称分配地址。在“System > DHCP Client”中组态参数。
- 支持以下 DHCP 选项：
  - DHCP 选项 3：分配路由器地址
  - DHCP 选项 6：分配 DNS 服务器地址
  - DHCP 选项 66：分配动态 TFTP 服务器名称
  - DHCP 选项 67：分配动态引导文件名称

说明

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

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

5.2.4 用 SINEC PNI 进行地址分配

简介

SINEC PNI 能够为没有组态 IP 地址的设备分配一个地址。

SINEC PNI

- 要使用 SINEC PNI 将 IP 地址分配给设备，必须能通过以太网访问该设备。
- 可在 Internet 的西门子工业在线支持页面上获取 SINEC PNI，地址为：(hhttps://support.industry.siemens.com/cs/cn/en/ps/26672/dl)
- 有关使用 SINEC PNI 分配 IP 地址的详细信息，请参见在线帮助或“SINEC PNI 网络管理”操作说明。

5.2.5 用 STEP 7 进行地址分配

在 STEP 7 中，可以组态拓扑、设备名称和 IP 地址；即，可以为设备的 MAC 地址指定 IP 地址。如果将未组态的设备连接至控制器，则控制器会自动为该设备分配已组态的设备名称和 IP 地址。

STEP 7 V5.x 及更早版本

有关使用 STEP 7 V5.x 及更早版本分配 IP 地址的详细信息，请参见文档《组态硬件和通信连接 STEP 7》的“PROFINET IO 系统组态步骤”部分。

STEP 7 V13 及更高版本

有关使用 STEP 7 V13 及更高版本分配 IP 地址的更多信息，请参见在线帮助“信息系统”的“寻址 PROFINET 设备”部分。

5.3 IPv6 地址

5.3.1 IPv6 术语

网络节点

网络节点是一种通过一个或多个接口连接至一个或多个网络的设备。

路由器

转发 IPv6 数据包的网络节点。

主机

代表 IPv6 通信关系端点的网络节点。

链路

根据 IPv6 术语，链路是 IPv6 网络内的第 3 层直接连接。

邻居

若两个网络节点位于同一链路，则称这两个网络节点为邻居。

IPv6 接口

激活 IPv6 的物理接口或逻辑接口。

路径 MTU

从发送方到接收方的路径上允许的最大数据包大小。

路径 MTU 发现

从发送方到接收方的整个路径上用于确定允许的最大数据包大小的机制。

LLA

链路本地地址 FE80::/10

在接口上激活 IPv6 后，会立即自动形成链路本地地址。 此地址仅位于同一链路中的节点可以访问。

ULA

唯一本地地址

在 RFC 4193 中进行了定义。通过此地址，可在 LAN 中访问 IPv6 接口。

GUA

全局单播地址

通过此地址，可访问 IPv6 接口（例如，通过 Internet 访问）。

接口 ID

可通过 EUI-64 方法或手动生成接口 ID。

EUI-64

扩展唯一标识符 (RFC 4291)；用于形成接口 ID 的过程。在以太网内，接口 ID 由接口的 MAC 地址形成。将 MAC 地址分为制造商特定部分 (OUI) 和网络特定部分 (NIC)，并在两者之间插入 FFFE。

示例：

MAC 地址 = AA:BB:CC:DD:EE:FF

OUI =AA:BB:CC

NIC = DD:EE:FF

EUI-64 = OUI + **FFFE** + NIC = AA:BB:CC:**FF:FE**:DD:EE:FF

范围

定义 IPv6 地址的范围。

5.3.2 IPv6 地址的结构

IPv6 地址的格式表示法

IPv6 地址由 8 个字段组成，每组均包含 4 个字符形式的十六进制数（总共 128 位）。各字段之间由冒号分隔。

示例：

fd00:0000:0000:ffff:02d1:7d01:0000:8f21

规则/简化规范：

- 如果一个或多个字段的值为 0，可以缩写方式代替。

  地址 fd00:**0000:0000**:ffff:02d1:7d01:0000:8f21 还可缩写为：

  fd00**::**ffff:02d1:7d01:0000:8f21

  为确保唯一性，此缩写形式在整个地址中仅可使用一次。

- 字段开头的零可以省略。

  地址 fd00:0000:0000:ffff:**02d1**:7d01:0000:8f21 还可缩写为：

  fd00**::**ffff:**2d1**:7d01:0000:8f21

- 以句点分隔的十进制表示法

  最后 2 个字段或 4 个字节可通过句点分隔的常规十进制表示法表示。

  示例：IPv6 地址 fd00::ffff.125.1.0.1 相当于 fd00::ffff:7d01:1

IPv6 地址的结构

IPv6 协议分为以下三种地址类型：单播、任播和组播。以下部分介绍了全局单播地址的结构。

IPv6 前缀		**后缀**
全局前缀： n 位	子网 ID m 位	接口 ID 128 - n - m 位
分配的地址范围	位置说明，还包括子网前缀或子网	网络中主机的唯一分配。 ID 根据 MAC 地址生成。

链路本地地址的前缀始终为 fe80:0000:0000:0000。此前缀还可以以以下缩写形式表示：fe80::

IPv6 前缀

指定标准：RFC 4291

IPv6 前缀代表子网标识符。

前缀和 IPv6 地址的指定方式与用于 IPv4 的 CIDR 表示法（无类域间路由）的指定方式相同。

设计

IPv6 地址/前缀长度

示例

IPv6 地址：2001:0db8:1234::1111/48

前缀：2001:0db8:1234::/48

接口 ID：::1111

输入和显示

IPv6 地址可按上述介绍的表示法输入。IPv6 地址始终以十六进制表示法显示。

使用“基于 Web 的管理”进行组态 6

6.1 基于 Web 的管理

工作原理

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

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

这种方法的优势在于只需要在客户端上安装 Web 浏览器。

说明

安全连接

WBM 也可用来通过 HTTPS 建立安全连接。
可使用 HTTPS 保护数据传输。如果希望只通过安全连接访问 WBM，则请只激活“系统 > 组态”(System > Configuration) 下的 HTTPS 服务器。

要求

WBM 显示

- 设备具有 IP 地址
- 设备与客户端设备之间存在连接。可以通过 Windows ping 命令检查是否存在连接。
- 已启用通过 HTTPS 进行的访问。
- 已在 Web 浏览器中激活 JavaScript。
- Web 浏览器不应设置成每次访问页面时都从服务器重载页面。页面动态内容的更新是通过其它机制来确保的。在 Internet Explorer 中，可以在“选项 > Internet 选

项 > 常规"(Options > Internet Options > General) 菜单的"浏览历史记录"(Browsing history) 部分，用"设置"(Settings) 按钮进行适当的设置。在"检查所存网页的较新版本："(Check for newer versions of stored pages:) 下，选择"自动"(Automatically)。

- 如果使用了防火墙，则必须打开相关端口。
  - 若使用 HTTP 进行访问：标准接口 80 或已组态接口
  - 若使用 HTTPS 进行访问：标准接口 443 或已组态接口

  WBM 的显示情况已使用如下桌面 Web 浏览器测试过：
  - Microsoft Internet Explorer 11

    说明

    兼容性视图

    为确保显示正确和使用 WBM 组态顺利，请在 Microsoft Internet Explorer 中禁用兼容性视图。
  - Mozilla Firefox 38 ESR
  - Chrome V46

在移动设备上显示 WBM

对于移动设备，必须满足以下最低要求：

分辨率	操作系统	Internet 浏览器
960 x 640 像素	Android（自版本 4.2.1 起） iOS（自版本 6.0.2 起）	基于 Android 的 Chrome（自版本 18 起） 基于 iOS 的 Safari（自版本 6 起）

- 已在移动设备上使用以下 Internet 浏览器执行过测试：
  - 基于 iOS（自版本 V8.1.3 起）的 Safari（自版本 8 起）（iPad Mini 型号 A1432）
  - 基于 Android（自版本 5.0.2 起）的 Chrome（自版本 46 起）(Nexus 7C Asus)
  - 基于 Android（自版本 5.0.2 起）的 Firefox（自版本 35 起）

说明

在移动设备上使用 WBM 及其显示

在移动设备上显示和操作 WBM 页面的方式与桌面设备相比可能有所不同。一些页面的显示还针对移动设备进行过优化。

6.2 登录

建立与设备的连接

使用 Internet 浏览器按照以下步骤与设备建立连接：

1. 设备与 PC 之间存在连接。可以通过 ping 命令检查是否可以访问设备。
2. 在 Internet 浏览器的地址框中，输入设备的 IP 地址或 URL。

   默认启用通过 HTTPS 进行的访问。如果通过 HTTP 访问设备，地址将自动跳转到 HTTPS。

   说明

   有关安全证书的信息
   因为设备只能使用加密访问进行管理，所以会与自签名证书一起交付。如果使用的证书包含操作系统无法识别的签名，则会显示一条安全消息。可以显示证书。

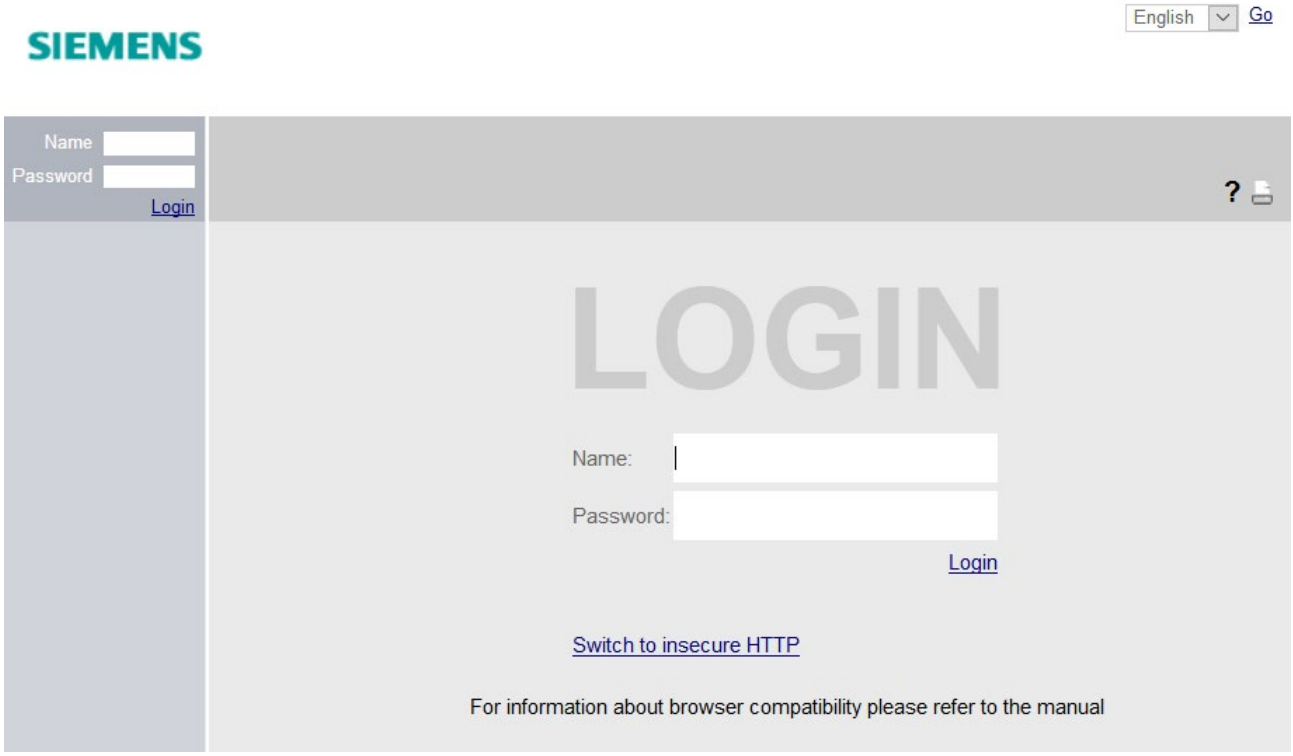
   将显示一条与安全证书相关的消息。确认该消息然后继续加载页面。

   如果使用非标准端口，则请在 IP 地址与端口号之间输入":"作为分隔符。

   示例：https://192.168.16.178:49152

   在"系统 > 组态"(System > Configuration) 中更改端口。
3. 如果设备存在连接，就会显示基于 Web 的管理 (Web Based Management, WBM) 的登录页面。

   如果希望通过 HTTP 连接访问 WBM，请在"系统 > 组态"(System > Configuration) 中将"HTTP 服务"(HTTP Services) 组态为"HTTP & HTTPS"。



更改语言

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

说明

可用语言

提供的语言有英语和德语。后续版本将添加其他语言。

个性化登录页面

可以在登录页面上显示附加文本。

1. 创建一个包含所需文本或 ASCII 类型的 txt 文件。对于 ASCII 类型，根据可用字符显示象形图，例如西门子公司徽标。

   说明

   不支持使用以下特殊字符：

   - 反斜线 (\)
   - 问号 (?)
   - Tab 制表符：使用空格代替制表符

2. 使用"系统 > 加载和保存"(System > Load&Save) 将文本文件加载到设备。
3. 注销。组态的文本显示在登录页面的登录数据下方。

登录 WBM

1. "名称"(Name) 输入框：
   - 如果是首次登录或是在"恢复出厂默认设置并重启"(Restore Factory Defaults and Restart) 后登录，则输入出厂时预设的用户"admin"。

     使用这种用户帐户时，可以更改设备的设置（对组态数据进行读写访问）。
   - 输入已创建用户帐户的用户名。可在"安全 > 用户"(Security > Users) 中组态本地用户帐户和角色。
2. "密码"(Password) 输入框：
   - 如果是首次登录或是在"恢复出厂默认设置并重启"(Restore Factory Defaults and Restart) 后登录，则输入出厂时预设的默认用户"admin"的密码"admin"。

     说明

     在美国版本的设备中，"admin"用户的密码已更改。从事专业 WLAN 安装的专业人员可从西门子支持部门获得密码。
   - 输入相关用户帐户的密码。

3. 单击"登录"(Login) 按钮或按"Enter"键确认输入内容。

说明

如果是首次登录或是在"恢复出厂默认设置并重启"(Restore Factory Defaults and Restart) 后登录，则可以对出厂时预设的用户"admin"进行一次重命名。之后，不可再重命名"admin"。在相应的文本框中输入新名称。

如果是首次登录或是在"恢复出厂默认设置并重启"(Restore Factory Defaults and Restart) 之后登录，则会提示您更改密码。

新密码必须符合"高强度"密码策略：

- 密码长度：至少 8 个字符，最长 128 个字符
- 至少 1 个大写字母
- 至少 1 个特殊字符
- 至少 1 个数字

您需要重新输入密码进行确认。密码输入必须匹配。

4. 单击"设置值"(Set Values) 按钮完成操作。该更改立即生效。

成功登录后，将显示起始页面。

防范暴力破解

为了防范暴力破解，在 11 次登录尝试失败后，将拒绝用户或用户的 IP 地址登录设备。

维修技术人员登录

该设备还具有用于维修目的的维修技术人员登录帐户。只有在管理员激活后才可用，并且只能由西门子支持人员使用。

6.3 "Wizard"菜单

6.3.1 Basic Wizard

简介

使用 Basic Wizard，菜单将引导您完成最重要参数的组态。

在 Basic Wizar 页面上，只能组态基本功能的重要参数。完成 Basic Wizard 操作后，可执行进一步设置。

要求

- 设备所处状态与发货时相同，并可通过以太网接口访问。
- 已为设备分配了 IP 地址。有关更多详细信息，请参见"IP 地址 (页 81)"部分。
- 用户以具有管理员权限的用户身份登录到 WBM。有关更多详细信息，请参见"登录 (页 99)"部分。

启动 Basic Wizard

单击导航区中的"Wizard > Basic Wizard"启动 Basic Wizard。

如果是首次登录或是在"恢复出厂默认设置"(Restore Factory Defaults) 之后登录，则在更改默认密码后会自动启动"基本向导"(Basic Wizard)。

常用按钮

Basic Wizard 的 WBM 页面包含以下按钮：

按钮	说明
Next	转到下一页
Previous	返回到上一页

按钮	说明
Abort	关闭 Basic Wizard，不采用设置。
Set Values	保存组态并退出向导。

只能使用"上一步"(Previous) 和"下一步"(Next) 按钮在"基本向导"(Basic Wizard) 页面内进行导航。

6.3.1.1 系统设置

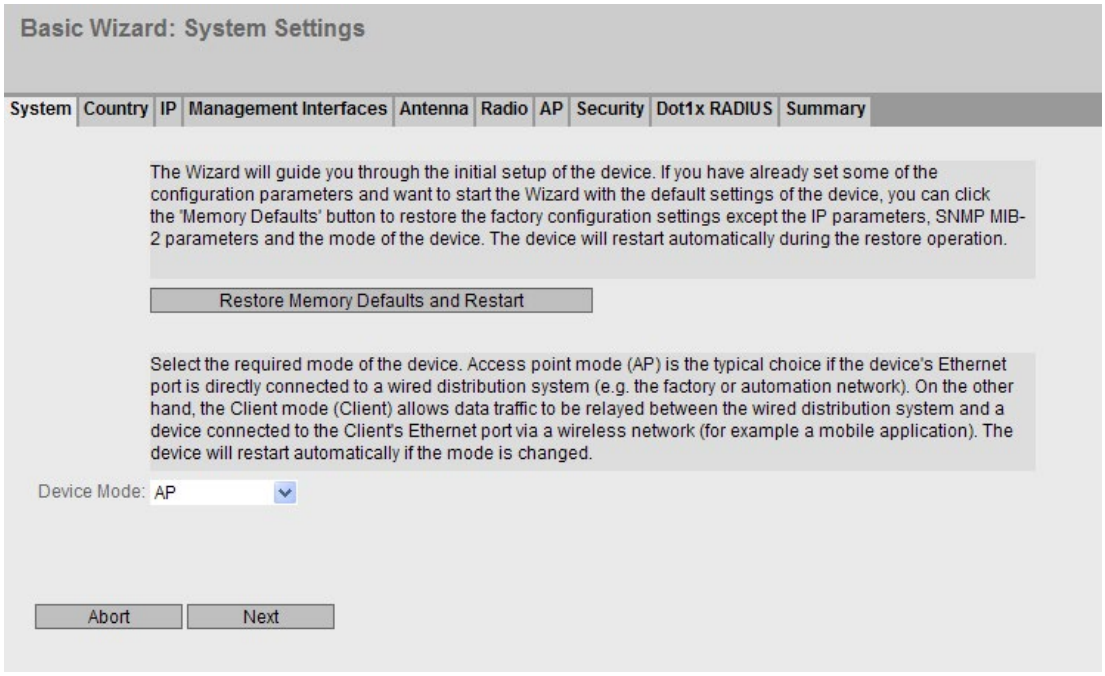
简介

在此 Basic Wizard 页面上，可指定设备的模式。更改模式后，将显示一条消息。

如果单击"确定"(OK) 确认消息，则设备将以出厂设置组态重启。再次登录并启动基本向导以在所选模式下继续组态设备。

说明

因为也只有接入点可在客户端模式下工作，所以仅可为这些设备选择此模式。


Basic Wizard: System Settings
System
Country
IP
Management Interfaces
Antenna
Radio
AP
Security
Dot1x RADIUS
Summary
The Wizard will guide you through the initial setup of the device. If you have already set some of the configuration parameters and want to start the Wizard with the default settings of the device, you can click the 'Memory Defaults' button to restore the factory configuration settings except the IP parameters, SNMP MIB-2 parameters and the mode of the device. The device will restart automatically during the restore operation.
Restore Memory Defaults and Restart
Select the required mode of the device. Access point mode (AP) is the typical choice if the device's Ethernet port is directly connected to a wired distribution system (e.g. the factory or automation network). On the other hand, the Client mode (Client) allows data traffic to be relayed between the wired distribution system and a device connected to the Client's Ethernet port via a wireless network (for example a mobile application). The device will restart automatically if the mode is changed.
Device Mode:
AP
Abort
Next

说明

Basic Wizard 页面包含以下框：

- **恢复存储器默认设置并重启** (Restore Memory Defaults and Restart)

  如果单击此按钮，将恢复出厂组态设置（以下参数除外）并重启设备。

  – IP 地址
  – 子网掩码
  – 默认网关的 IP 地址。
  – DHCP 客户端 ID
  – DHCP
  – 系统名称
  – 系统位置
  – 系统联系人
  – 用户名和密码
  – 设备的模式

重启设备后，您需要再次登录并再次启动基本向导以组态设备。

- **设备模式 (Device Mode)**

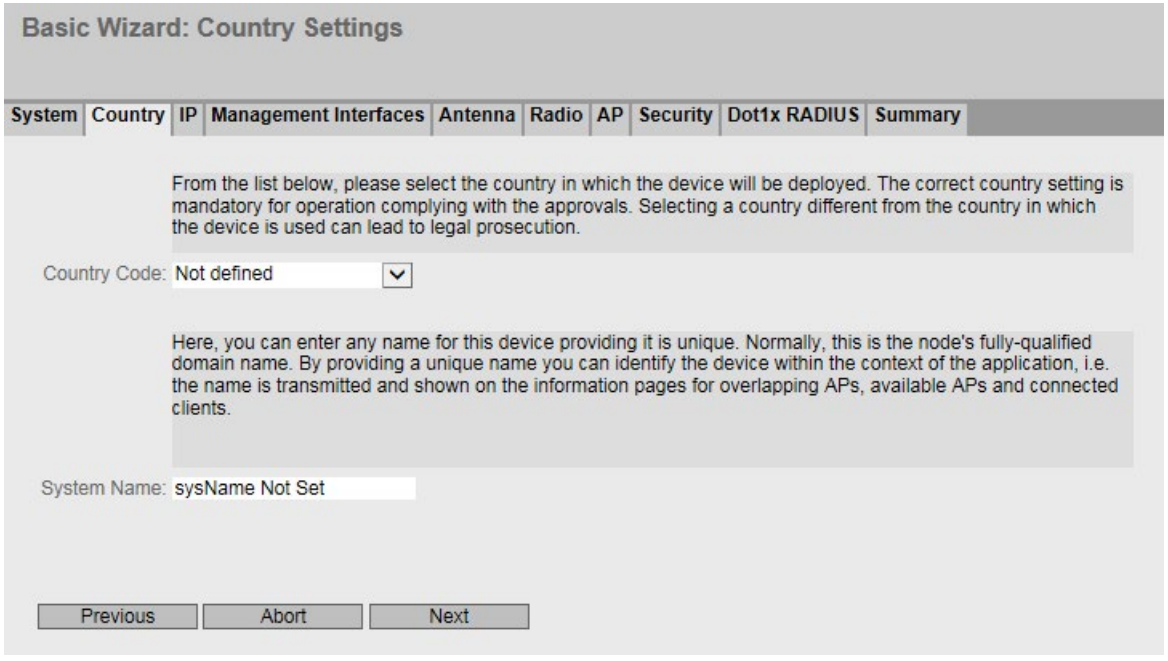
  选择设备的模式。此选择仅适用于接入点。
  存在以下工作模式：

  – AP：接入点模式
  – 客户端：客户端模式

6.3.1.2 国家/地区设置

简介

在此 Basic Wizard 页面上，可组态国家/地区和系统名称。



说明

Basic Wizard 页面包含以下框

- **国家/地区代码 (Country Code)**

  在此下拉列表中选择部署的设备所在的国家/地区。无需了解特定国家/地区的数据，设备会根据您所选择的国家/地区设置通道划分和输出功率。

  说明

  区域设置
  为使操作符合认证，必须正确设定国家/地区设置。选择与设备使用地所在国家/地区不同的国家/地区会导致法律纠纷。

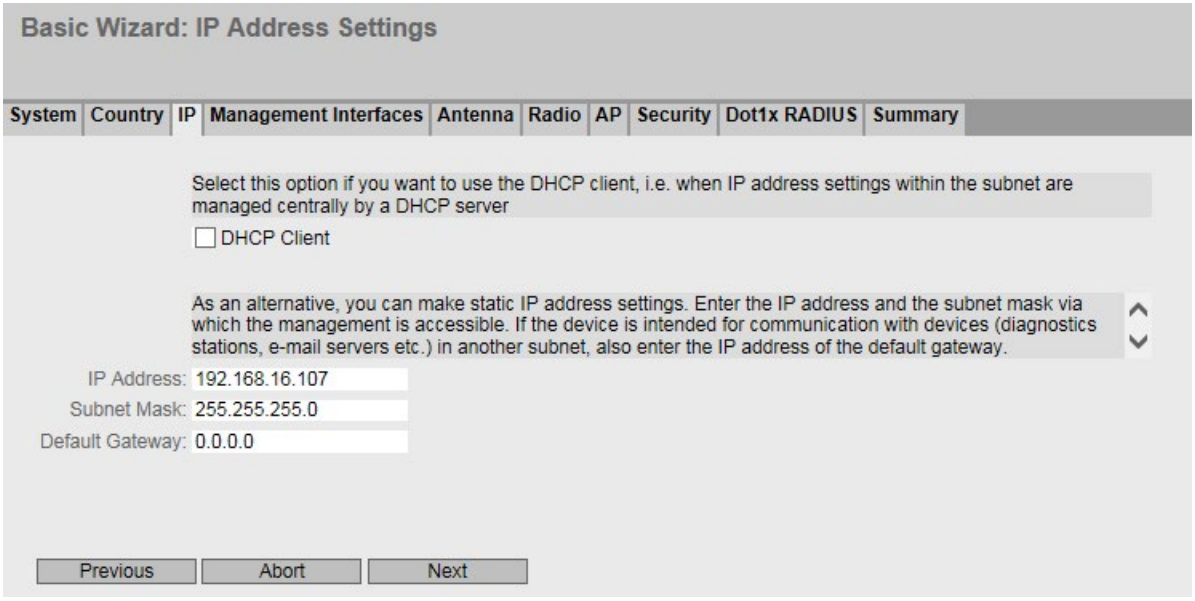
- **系统名称 (System Name)**

  可以输入设备的名称。如果组态此输入框，则系统会采用该组态并显示在选择区中。最多支持 255 个字符。
  系统名称还显示在 CLI 输入提示中。CLI 输入提示中的字符数是有限的。系统名称前 16 个字符后面的部分将被截断。

6.3.1.3 IP 地址设置

简介

组态设备的基本步骤之一是设置 IP 地址。IP 地址用于在网络中唯一地标识一台设备。



说明

"基本向导"(Basic Wizard) 页面包含以下框：

- **DHCP 客户端 (DHCP Client)**

  指定 IP 地址的分配方式。有两种分配 IP 地址的方法：

  – 启用

    设备从 DHCP 服务器获得动态 IP 地址。

  – 禁用

    在"IP 地址"(IP Address) 和"子网掩码"(Subnet Mask) 输入框中输入 IP 设置。

- **IP 地址 (IP Address)**

  输入网络中唯一的 IP 地址。

- **子网掩码 (Subnet Mask)**

  输入设备的子网掩码。

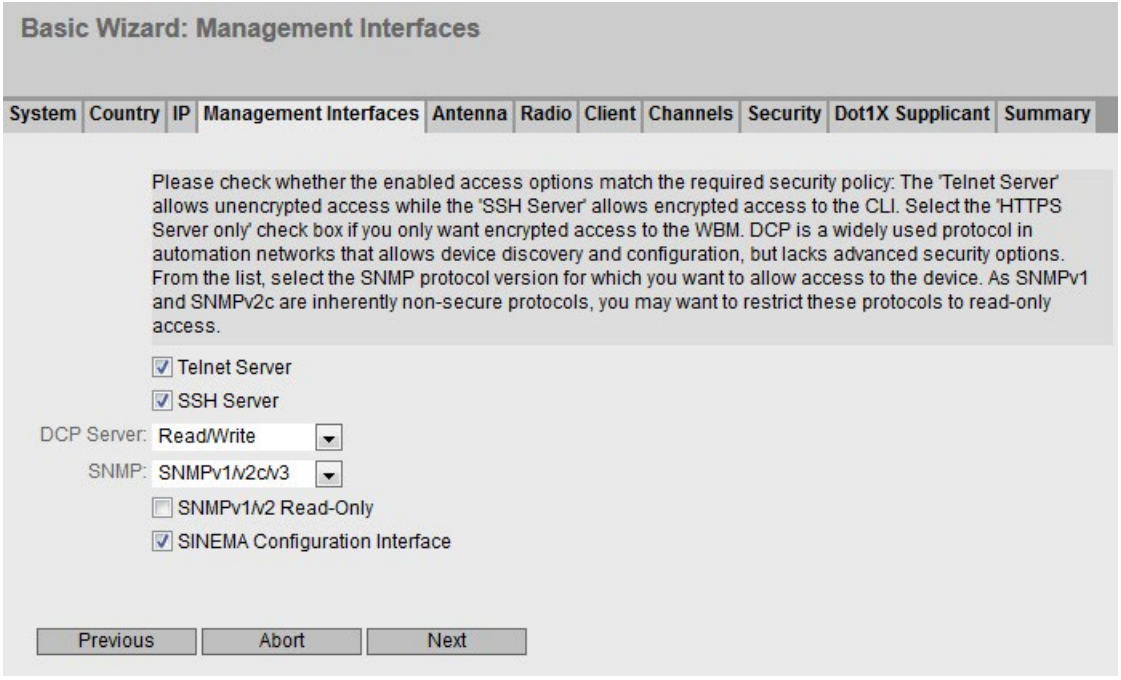
- **默认网关 (Default gateway)**

  输入默认网关的 IP 地址，以便设备可以与其它子网内的设备（如诊断站、电子邮件服务器）进行通信。

6.3.1.4 管理接口

系统组态

在此 Basic Wizard 页面上，可指定用来访问设备的服务。对于某些服务提供了更多组态页面，可在其中进行更加具体的设置。完成 Basic Wizard 后组态这些服务。



说明

该页面包含以下框：

- **Telnet 服务器 (Telnet Server)**

  启用或禁用"Telnet 服务器"(Telnet Server) 服务，以便不加密访问 CLI。

- **SSH 服务器 (SSH Server)**

  启用或禁用"SSH 服务器"(SSH Server) 服务，以便加密访问 CLI。

- **DCP 服务器 (DCP Server)**

  指定是否可用 DCP（发现和组态协议）访问设备：

  – "-"（已禁用）
    DCP 已禁用。既不能读取也不能修改设备参数。

  – 读/写 (Read/Write)
    借助 DCP，既可以读取设备参数又可以对其进行修改。

  – 只读
    通过 DCP，可读取但不能修改设备参数。

- **SNMP**

  从下拉列表中选择协议。可能的设置如下：

  – "-"（SNMP 已禁用）
    不能通过 SNMP 访问设备参数。

  – SNMPv1/v2c/v3
    可以通过 SNMP 版本 1、2c 或 3 访问设备参数。可以在"System > SNMP > 常规"(System > SNMP > General) 中组态其它设置。

  – SNMPv3
    可通过 SNMP 版本 3 访问设备参数。可以在" System > SNMP > 常规"(System > SNMP > General) 中组态其它设置。

- **SNMPv1/v2 只读 (SNMPv1/v2 Read-Only)**

  启用或禁用通过 SNMPv1/v2c 对 SNMP 变量进行写访问。

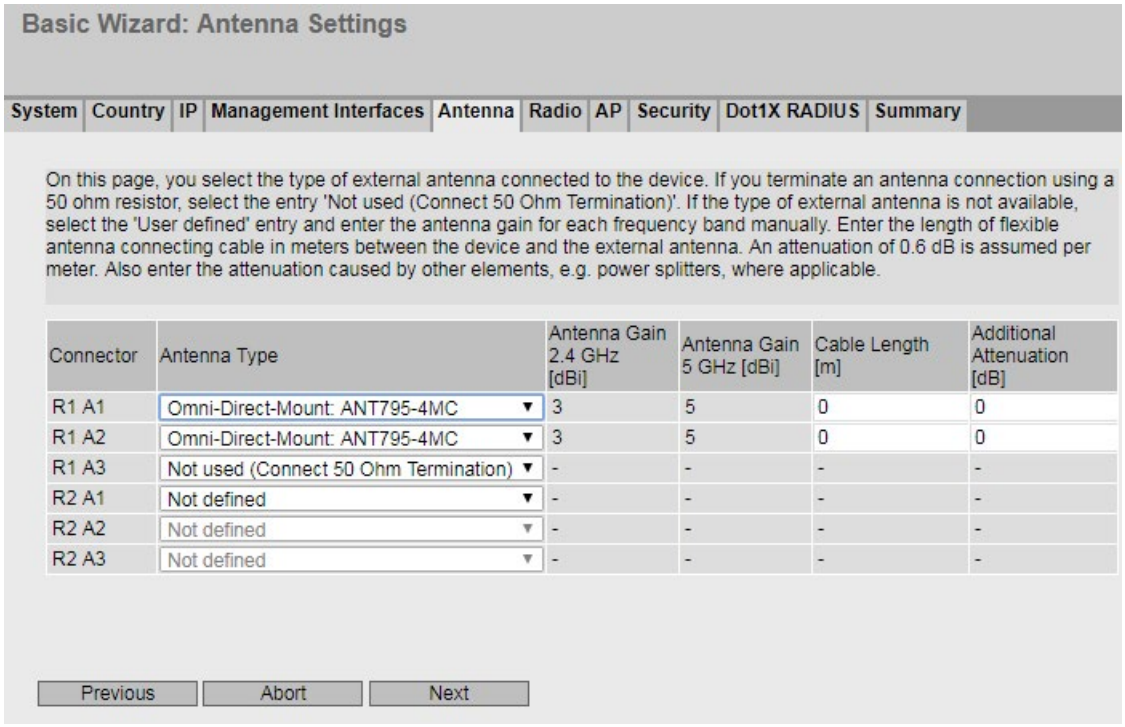
- **SINEMA 组态接口 (SINEMA configuration interface)**

  如果启用了 SINEMA 组态接口，可通过 TIA Portal 将组态下载到设备中。

6.3.1.5 天线设置

简介

在此"基本向导"(Basic Wizard) 页面上，可组态外部天线的设置。



说明

该表包含以下列：

- **连接器 (Connector)**

  显示相关天线连接器的名称。

- **天线类型 (Antenna Type)**

  选择连接到设备的外部天线的类型。如果没有您的天线类型，请选择条目"用户自定义"(User defined)。

未使用的连接器必须安装 50 Ω 端接电阻。选择条目"未使用（连接 50 欧姆端子）"(Not used (Connect 50 Ohm Termination))。

说明

50 Ω 端接电阻

每个 WLAN 接口有三个天线连接器。相关 WLAN 接口开启后，天线 R1A1 和 R2A1 必须始终处于连接状态。如果未连接任何天线，还必须禁用相应接口的 RX 和 TX。否则可能发生传输中断。

- **天线增益 [dBi] (Antenna Gain [dBi])**

  如果在"天线类型"(Antenna Type) 中选择了"用户自定义"(User defined) 条目，则需手动输入以"dBi"为单位的天线增益。

  – 天线增益 2.4 GHz [dBi] (Antenna Gain 2.4 GHz [dBi])
    输入天线在 2.4 GHz 频段内的天线增益。

  – 天线增益 5 GHz [dBi] (Antenna Gain 5 GHz [dBi])
    输入天线在 5 GHz 频段内的天线增益。

- **电缆长度 [m] (Cable length [m])**

  输入设备和外部天线之间的柔性天线连接电缆的长度（以米为单位）。

- **其它衰减 [dB] (Additional Attenuation [dB])**

  在此处指定其它衰减，例如由其它分配器造成的衰减。

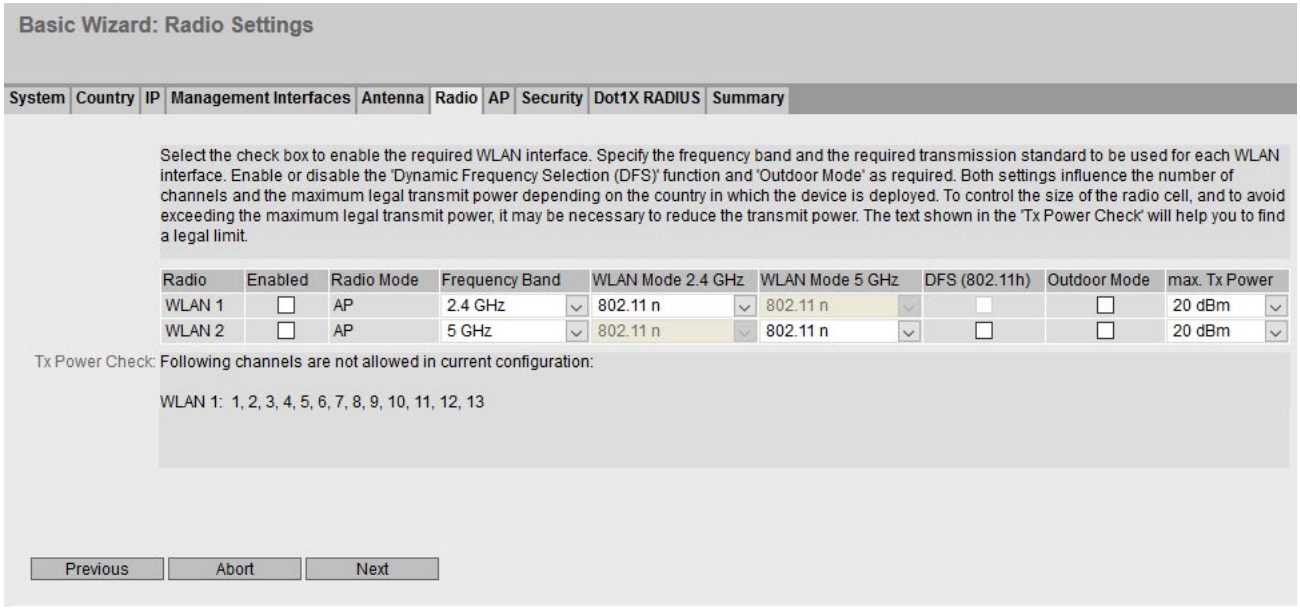
说明

如果使用其它 WLAN 接口，请确保具有足够的通道间隔。

6.3.1.6 无线设置

简介

在此 Basic Wizard 页面上，可指定 WLAN 接口的组态。



描述

该表包含以下各列：

- **无线 (Radio)**

  显示可用的 WLAN 接口。

- **启用 (Enabled)**

  启用或禁用 WLAN 接口。提供设备时 WLAN 接口处于禁用状态。

- **无线模式 (Radio Mode)**

  显示 WLAN 接口的模式。

- **频段 (Frequency Band)**

  指定频段。在客户端模式下也可以进行双频操作。

  说明

  将 W786-2IA RJ-45 的 WLAN 接口组态为不同频段

  如果将该设备上的两个 WLAN 接口组态为相同频段，则这两个接口会相互影响或干扰。在数据吞吐量较高时，这种情况尤其突出。

- **WLAN 模式 (WLAN Mode)**

  为组态的频段选择所需的传输标准。

  – WLAN 模式 2.4 GHz (WLAN Mode 2.4 GHz)

    为 2.4 GHz 频段指定传输标准。该选择取决于国家/地区设置。

  – WLAN 模式 5 GHz (WLAN Mode 5 GHz)

    为 5 GHz 频段指定传输标准。该选择取决于国家/地区设置。

- **DFS (802.11h)**

  – 激活 (Activated)

    使用 DFS 功能，还可以使用更高的 5 Ghz 通道。这些通道为国家/地区特定的通道，需要遵守特定 DFS 规范。有关更多信息，请参见国家/地区特定的 DFS 文档。

    接入点通过其中一条通道进行发射信号之前，会借助 CAC（通道可用性检查）进行为期 60 秒的搜索，检查是否存在竞争雷达信号。接入点在搜索期间不会发送任何信标。对于气象雷达通道 (5.6 - 5.65 GHz)，搜索持续时间为 10 分钟。如果经过搜索周期后未检测到任何雷达信号，接入点会通过此通道发射信号。否则，接入点将更改通道并重复该检查过程。运行期间，接入点还会持续搜索雷达信号。

    如果接入点发现当前通道上有雷达信号，则会自动切换到备用 DFS 通道，当前通道将被阻断 30 分钟。

  – 禁用 (Disabled)

    未使用 DFS 功能。

- **户外模式 (Outdoor Mode)**

  – 启用

    在户外模式下，可扩展选择国家/地区规定供户外使用的通道和发射功率。

  – 禁用

    目前在户内模式下运行设备。在室内模式下，只能选择与国家/地区相关的供建筑内使用的通道和发射功率。

- **最大发射功率 (max. Tx Power)**

  指定设备的发射功率。在使用天线时，为避免超出法定的最大发射功率，可能有必要降低发射功率。降低发射功率可有效地减小蜂窝区大小。

说明

可实现的最大发射功率因通道和数据速率的不同而异。有关发射功率的更多详细信息，请参见文档"无线电接口特性"。

说明

如果带有两个 WLAN 接口的接入点的两个接口都运行在相同的频率范围内，这可能在发射功率高于 15 dBm 时导致一个接口或两个接口上有无线干扰。

- **发射功率检查 (Tx power check)**

  指示所做的设置是否违反所选国家/地区允许的发射功率限制。检查"max. EIRP"的计算值以确定此值是否违反所设置国家/地区特定通道允许的发射功率限制。如果设置"仅使用允许的通道"(Use Allowed Channels only)，则仅检查在此选择的通道。

  – -

    通道可在当前设置下使用。

  – 通道数

    表示当前发射功率超出最大允许发射功率的通道。

6.3.1.7 接入点设置

简介

在此 Basic Wizard 页面上，可指定 Access Point 的组态。

说明

此页面仅在接入点模式下可用。

描述

表 1 包含以下列：

- **无线 (Radio)**

  显示可用的 WLAN 接口。

- **通道 (Channel)**

  指定主通道。如果希望接入点自行搜索空闲通道，请使用"自动"(Auto)。如果要使用固定通道，请从下拉列表中选择所需的通道。

- **备用 DFS 通道 (Alternative DFS Channel)**

  如果在"无线设置"(Radio Settings) 基础向导页面中启用了"DFS"功能，则在此处指定备用通道。如果希望接入点自行搜索空闲通道，请使用"自动"(Auto)。如果要使用固定通道，请从下拉列表中选择所需的通道。

- **HT 通道宽度 [MHz] (HT Channel Width [MHz])**

  可以指定符合 IEEE 802.11n 传输标准的通道带宽。
  可能的设置如下。

  – 20
    通道带宽为 20 MHz

  – 40 up
    通道带宽 40 MHz。使用组态的通道以及高于其带宽的相邻通道。

  – 40 down
    通道带宽 40 MHz。使用组态的通道以及低于其带宽的相邻通道。

表 2 包含以下列：

- **端口 (Port)**

  显示每个 WLAN 接口的第一个 VAP 接口。

- **SSID**

  输入 SSID。SSID 的字符串长度为 1 到 32 个字符。
  SSID 使用 ASCII 码 0x20 至 0x7e。

完成"基本向导"(Basic Wizard) 后，可通过"接口 > WLAN > 接入点设置"(Interfaces > WLAN > Access Point Settings) 定义更多 SSID。

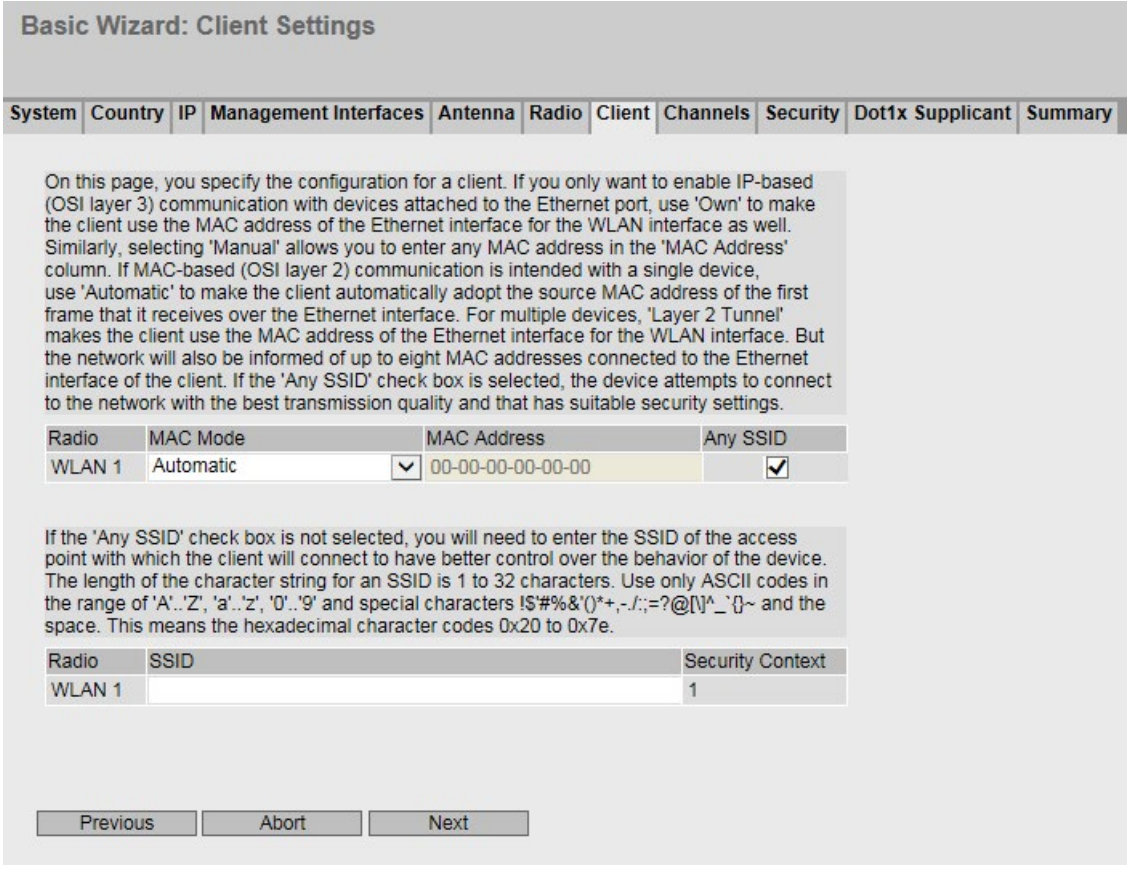
6.3.1.8 客户端设置

简介

在此 Basic Wizard 页面上，可指定客户端的组态，例如 MAC 地址的分配。

说明

此页面仅在客户端模式下可用。



说明

表 1 包含以下列：

- **无线 (Radio)**

  显示可用的 WLAN 接口。

- **MAC 模式 (MAC mode)**

  指定向客户端分配 MAC 地址的方式。可能的方式包括：

  – 自动 (Automatic)

    客户端自动采用其通过以太网接口接收的第一帧的源 MAC 地址。

– 手动 (Manual)

如果选择"手动"(Manual)，则在"MAC 地址"(MAC Address) 列中输入 MAC 地址。

– 自身 (Own)

客户端的 WLAN 接口使用以太网接口的 MAC 地址。

– 第 2 层隧道 (Layer 2 Tunnel)

客户端的 WLAN 接口使用以太网接口的 MAC 地址。同时也会将连接到客户端以太网接口的 MAC 地址通知给网络。最多可使用八个 MAC 地址。

- **MAC 地址 (MAC Address)**

输入客户端的 MAC 地址。仅当将"MAC 模式"(MAC Mode) 设置为"手动"(Manual) 时才能编辑该输入框。

- **任意 SSID (Any SSID)**

– 启用

在客户端模式下，设备尝试连接到具有合适的安全设置且传输质量最高的网络。

– 禁用

客户端尝试连接到 SSID 列表中传输质量最好的网络。

表 2 包含以下列：

- **无线 (Radio)**

  显示可用的 WLAN 接口。

- **SSID**

  输入要与客户端相连的接入点的 SSID。在"基本向导"(Basic Wizard) 中，仅可指定一个 SSID。完成"基本向导"(Basic Wizard) 后，可使用"接口 > WLAN > 客户端"(Interfaces > WLAN > Client) 定义更多 SSID。

- **安全上下文 (Security Context)**

  显示分配的安全上下文。在"基本向导"(Basic Wizard) 中，只有一个安全上下文可用。完成基本向导后，可以在"安全 > WLAN > 基本"(Security > WLAN > Basic) 中创建并组态更多安全上下文。

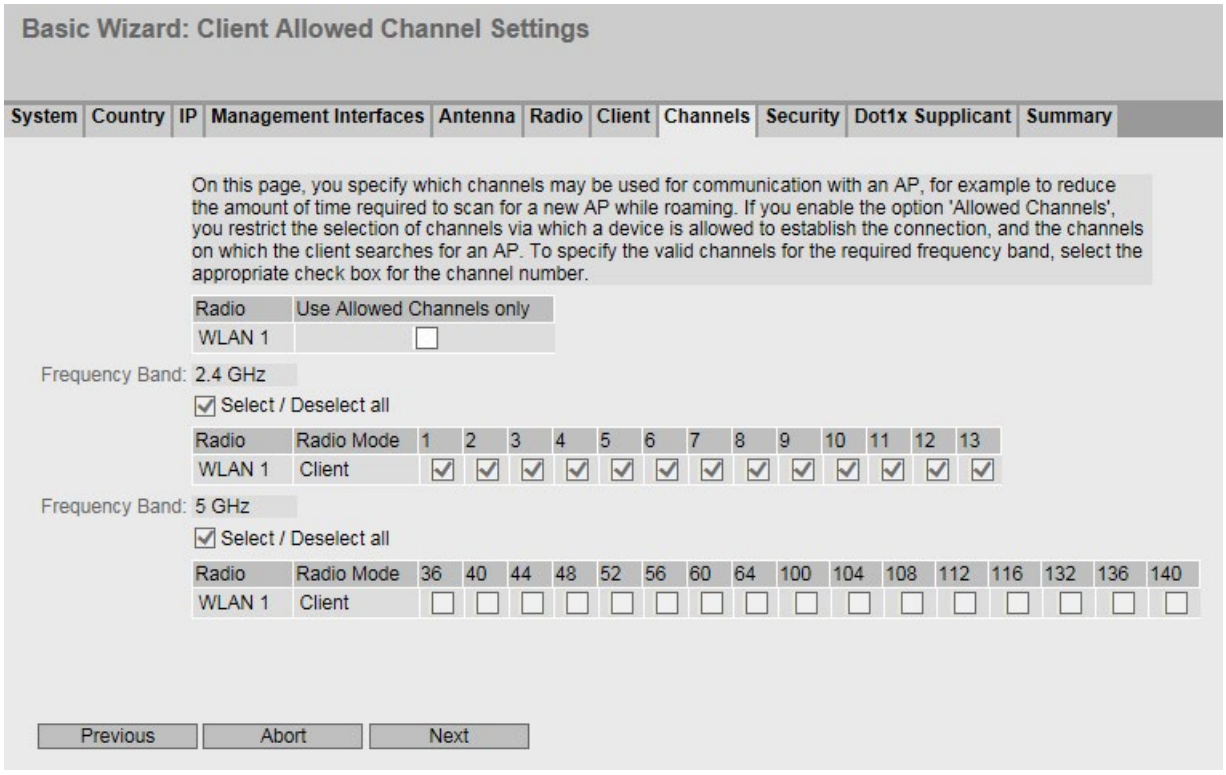
6.3.1.9 客户端允许的通道设置

简介

为进行通信，将在频段内使用一个特定的通道。在此页面上，可以具体设置此通道，也可以组态为自动选择通道。

说明

只有客户端或处于客户端模式下的接入点可使用此页面。



说明

表 1 包含以下列：

- **无线 (Radio)**

  显示可用的 WLAN 接口。

- **仅使用允许的通道 (Use Allowed Channels only)**

  如果启用此选项，则限制了客户端建立连接时允许使用的通道的选择。

  在以下表格中，定义客户端搜索 AP 时所处的通道。

  表格根据频段进行划分。

  如果禁用该选项，则将使用基于设置（国家/地区代码、天线、发射功率等）的可用通道。

在各频段表格的上方，可看到以下复选框：

- **全选/取消全选 (Select/Deselect all)**
  - Enabled
    如果启用该复选框，将选中所有通道。
  - Disabled
    如取消选中该复选框，则频段内仅第一个有效通道将保持启用状态。

频段表具有以下列：

- **无线 (Radio)**

  显示可用的 WLAN 接口。

- **无线模式 (Radio Mode)**

  显示设备的操作模式。

- **Channel number**
  要为所需的频段指定有效通道，请选中通道号所对应的相应复选框。
  该表格显示了相应国家/地区允许的通道。只能启用有效的通道。无效通道将灰显且无法启用。

说明
要指定通道，必须启用设置"仅使用允许的通道"(Use Allowed Channels only)。

6.3.1.10 安全设置

简介

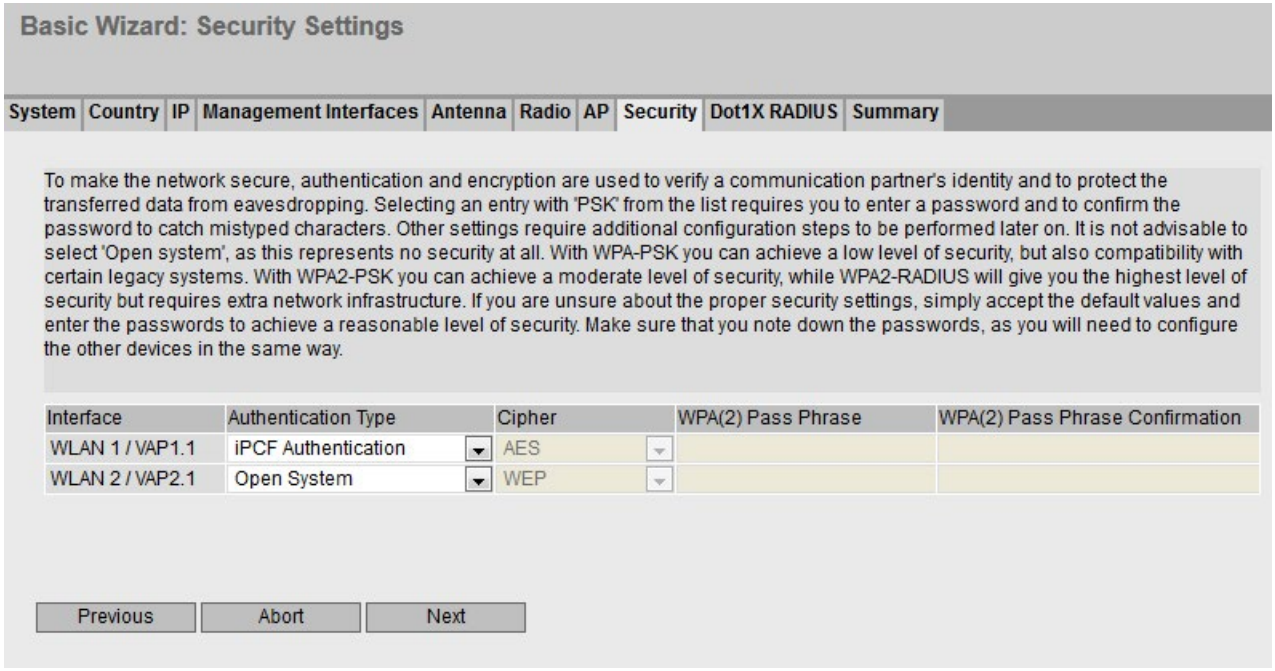
为确保网络安全，请使用验证和加密。通过验证类型和加密程序指定安全等级。

使用 WPA2/AES 可防止滥用 WPA2 (RADIUS)/WPA2-PSK 密码，因为 AES 可提供最高的安全性。有关安全性的详细信息，请参见组态手册中的"安全网络设计说明"。

两个设备上的安全设置必须相匹配，才允许客户端与接入点进行通信。

说明

在接入点和客户端模式下，此页面具有不同的列。



说明

该表包含以下各列：

- **接口 (Interface)**（仅限接入点模式）

  显示与设置相关的接口。

- **安全上下文 (Security Context)**（仅限客户端模式）

  显示与设置相关的安全上下文。

- **验证类型 (Authentication Type)**

  选择验证类型。

说明

WLAN 模式 IEEE 802.11 n

以 WLAN 模式 IEEE8002.11n 运行的设备只可以使用 WPA2（WPA2-PSK 和 WPA2 Radius）加密。

– Open System
  无验证

– **WEP**

– WPA-PSK
  使用 WPA 密钥的 WPA 验证。在"WPA(2) 通行口令"(WPA(2) Pass Phrase) 中输入 WPA 密钥。

– WPA (RADIUS)
  RADIUS 服务器的 WPA 验证。在下一 Basic Wizard 页面上组态访问数据。

– WPA2-PSK
  使用 WPA2 密钥的 WPA2 验证。在"WPA(2) 通行口令"(WPA(2) Pass Phrase) 中输入 WPA2 密钥。

– WPA2 (RADIUS)
  RADIUS 服务器的 WPA2 验证。在下一 Basic Wizard 页面上组态访问数据。

– iPCF authentication
  在相应的 WLAN 接口上启用 iPCF、iPCF-HT 或 iPCF-MC 模式时，将显示验证类型.
  可以在"iFeatures (页 526)"菜单中启用 iPCF 验证。

- **密码 (Cipher)**

选择加密方法。

– AUTO
  根据其它站的功能选择使用 AES 或 TKIP。

– TKIP (Temporal Key Integrity Protocol)
  一种使用 RC4 算法 (Ron's Code 4) 的对称加密方法。与较弱的 WEP 加密相反，TKIP 采用从主密钥派生的变化密钥。TKIP 还可以识别受损的数据帧。

– AES (Advanced Encryption Standard)
  一种基于进一步改进 TKIP 功能的 Rijndael 算法的较强对称区块加密方法。

- **WPA(2) 通行口令 (WPA(2) Pass Phrase)**

  输入 WPA(2) 密钥。密钥长度可以是 8 至 63 个 ASCII 字符，或者正好是 64 个十六进制字符。该 WPA(2) 密钥必须为客户端和接入点所知，并由用户在两端输入。

说明

WPA(2) 密钥长度可以是 8 至 63 个 ASCII 字符，或者正好是 64 个十六进制字符。应选择复杂密钥，例如包含随机数字、字母（大写/小写），并且几乎无重复及特殊字符。请勿使用可能被猜中的已知名称、单词或术语。如果设备丢失或密钥泄露，应更改所有设备的密钥，以保持安全性。

- **WPA(2) 通行口令确认 (WPA(2) Pass Phrase Confirmation)**

  确认输入的 WPA(2) 通行口令。

6.3.1.11 Dot1x 请求者设置

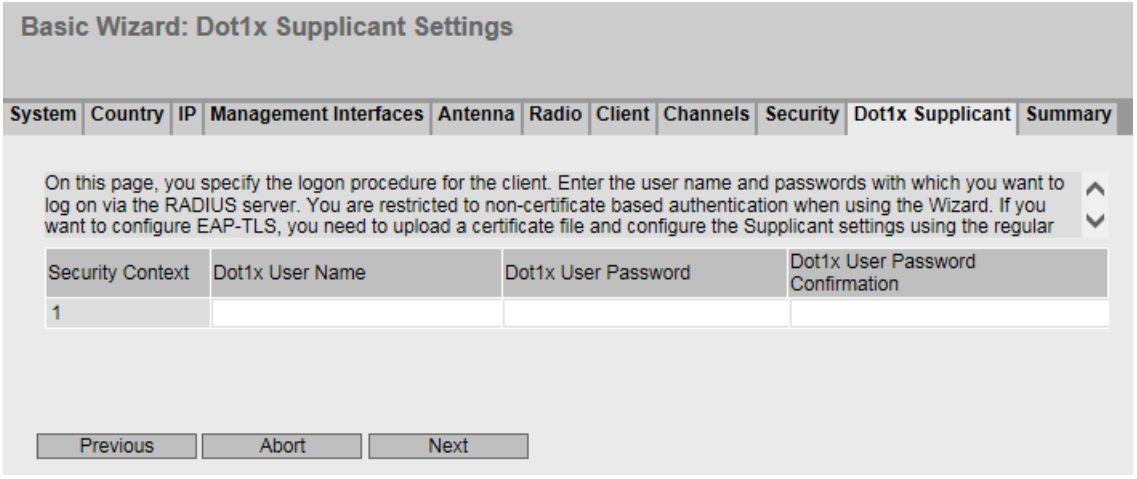
简介

在此 Basic Wizard 页面上，可组态客户端登录 RADIUS 服务器时使用的用户名和密码。

如果需要使用其它验证方法，可以在完成 Basic Wizard 后使用"Security > WLAN > Client Radius Supplicant"进行组态。

说明

只有客户端或处于客户端模式下的接入点可使用此页面。



说明

表 1 包含以下列：

- **安全上下文 (Security Context)**

  显示安全上下文 1。

- **Dot1x 用户名 (Dot1x User Name)**

  输入客户端登录 RADIUS 服务器时使用的用户名。

- **Dot1x 用户密码 (Dot1x User Password)**

  输入上面所选用户名的密码。客户端使用该用户名和密码组合登录 RADIUS 服务器。

  密码分配使用 ASCII 码 0x20 至 0x7e。

- **Dot1x 用户密码确认 (Dot1x User Password Confirmation)**

  在此输入框中再次输入密码。

6.3.1.12 Dot1x RADIUS Server Settings

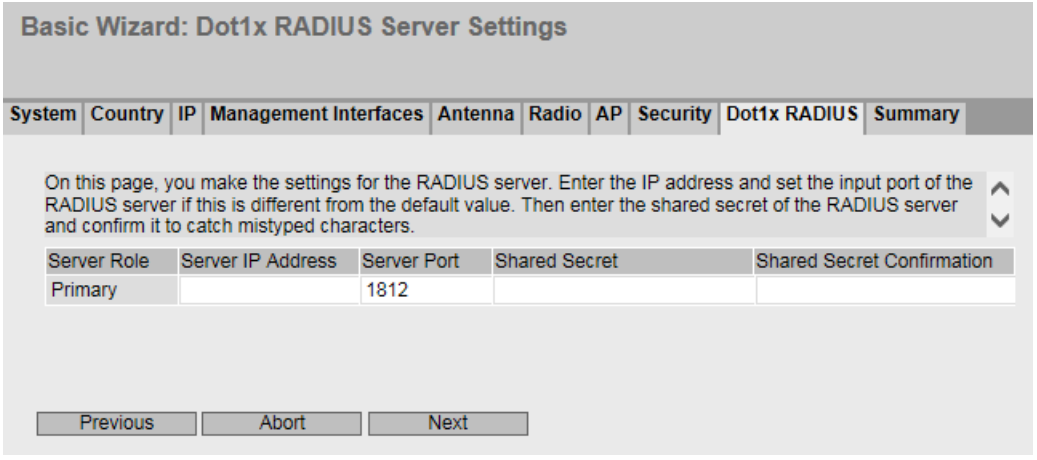
简介

在此 Basic Wizard 页面上，可组态主 RADIUS 服务器的设置。

完成基本向导后，可使用"Security> WLAN > AP Radius 验证器"(Security> WLAN > AP Radius Authenticator) 组态备用服务器以及其它设置，例如尝试登录的次数。

说明

此页面仅在接入点模式下可用。



说明

该表包含以下各列：

- **服务器角色 (Server Role)**

  显示服务器的角色。

- **服务器 IP 地址 (Server IP Address)**

  输入 RADIUS 服务器的 IP 地址。不支持使用计算机名称（使用 DNS 进行名称解析）代替 IP 地址。

- **服务器端口 (Server Port)**

  输入 RADIUS 服务器的端口。

- **共享密钥 (Shared Secret)**

  输入 RADIUS 服务器的密码。

- **共享密钥确认 (Shared Secret Conf)**

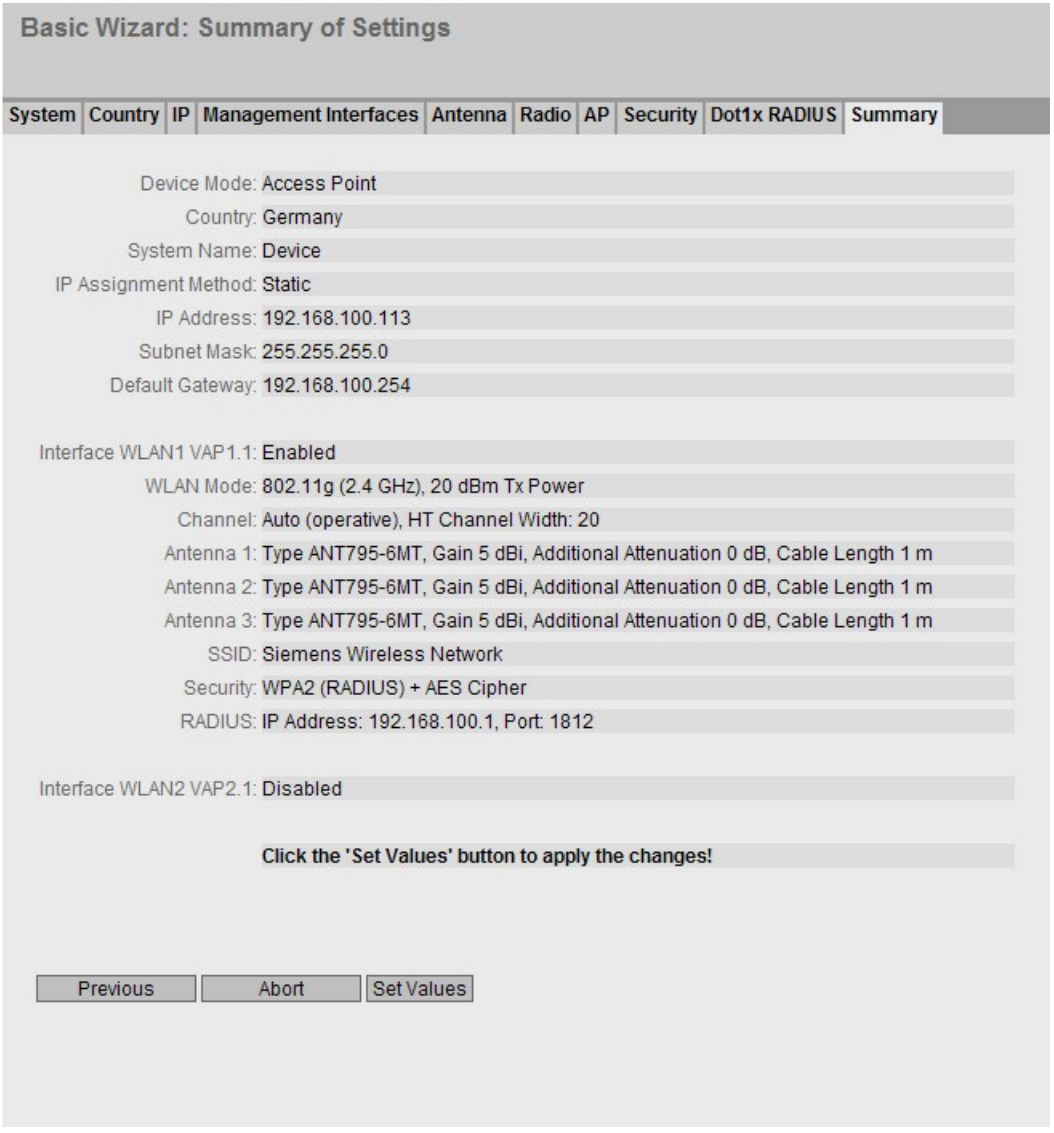
  在此输入框中再次输入密码。

6.3.1.13 设置汇总

简介

此页面汇总了设置。页面内容取决于设置的参数和设备的模式。

在使用"设置值"(Set Values) 按钮退出基本向导前请检查设置。如果设置错误，使用"上一页"(Prev) 按钮返回，然后将设置更改为所需设置。



设置值

单击"设置值"(Set Values) 按钮可退出基本向导。将采用 WLAN 设置。

6.4 "Information"菜单

6.4.1 起始页

起始页面视图

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

WBM 页面的常规布局

每个 WBM 页面通常都会有以下几个区域：

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

选择区 (1)

选择区中有以下内容：

- Siemens AG 徽标
- 显示："系统位置/系统名称"(System Location/System Name)。
  - "系统位置"包含设备的位置。
    如果使用设备出厂时的设置，则会显示以太网接口的 IP 地址。
  - "系统名称"是设备名称。如果使用设备出厂时的设置，则会显示设备类型。

  可以通过"系统 > 常规 > 设备"(System > General > Device) 更改显示的内容。
- 用于选择语言的下拉列表
- 系统时间和日期

  可以通过"系统 > 系统时间"(System > System Time) 更改该显示的日期和时间。

  若未设置系统时间，则状态为 。若组态了系统时间但系统时间无法同步，则会显示黄色三角警告 。检查是否能够访问时间服务器。如有必要，请调整组态。若系统时间已设置和/或能够同步，则状态为 。

显示区 (2)

在显示区的上半部分，您可以看到当前登录用户的名称和当前所选菜单项的完整标题。

显示区的下半部分包含以下项：

- **注销**(Logout)
  可以单击"注销"(Logout) 链接从任何 WBM 页面注销。
- **设备名称 (Device name)**
  显示设备的名称。
- **模式 (Mode)**
  显示设备是接入点还是客户端。

- **LED 仿真 (LED simulation)** 

  每个设备都具有一个或多个 LED，用于提供有关设备工作状态的信息。根据其安装位置，可能不是总能直接访问设备。因此"基于 Web 的管理"显示的是仿真 LED。未使用的连接器会显示为灰显 LED。各种 LED 显示的含义在操作说明中进行了说明。

  单击该按钮后，可以打开 LED 仿真窗口。可以在切换菜单过程中显示该窗口，并根据需要进行移动。要关闭 LED 仿真，请单击 LED 仿真窗口中的关闭按钮。

- **帮助** (Help) 

  单击此按钮时，将在新的浏览器窗口中打开当前所选菜单项的帮助页面。

  在每个帮助页面的顶部，都有一个用于搜索的输入框。在此输入框中，输入需要更多相关信息的条目，然后按 Enter 键开始搜索。随即出现一个对话框，其中会列出包含搜索条目的 WBM 页面。单击其中一个列表元素后，将在浏览器的新标签页中打开相应的 WBM 页面。

- **打印机 (Printer)** 

  如果单击此按钮，将打开一个弹出窗口。此弹出窗口包含针对打印机优化过的页面内容视图。

说明

打印较大的表格

如果要打印较大的表格，请使用 Internet 浏览器的"打印预览"功能。

- **收藏夹 (Favorites)**

  交付产品时，该按钮在所有页面上均为禁用状态 。

  如果单击该按钮，符号会变为 ，当前打开的页面或选项卡被标记为收藏内容。启用该按钮后，导航区域将分为两个选项卡。第一个选项卡"菜单"(Menu) 包含启用该按钮前的所有可用菜单。第二个选项卡"收藏夹"(Favorites) 包含用户选作收藏内容的所有页面/选项卡。在"收藏夹"(Favorites) 选项卡上，页面/选项卡按照"菜单"(Menu) 选项卡中的结构排列。

  如果禁用已创建的所有收藏夹，"收藏夹"(Favorites) 选项卡将再次被移除。为此，单击相关页面/选项卡中的 按钮。

  可以在"系统 > 加载和保存"(System > Load&Save) 页面使用 HTTP 或者 TFTP 保存、上传和删除设备的收藏夹组态。

- **更新开启 (Update on) On/更新关闭 (Update off) Off**
  具有总览列表的 WBM 页面还可以具有附加的"更新"(Update) 按钮。

  使用此按钮可以启用或禁用更新内容区域。如果开启更新，将每 2 秒更新一次显示。要禁用更新，请单击"On"。将显示"Off"取代"On"。默认情况下，始终在 WBM 页面上启用更新。

浏览区 (3)

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

内容区 (4)

内容区显示设备图形。该图形始终显示 WBM 已被调用的设备。

以下信息显示在设备图片的下方：

- **站的 PROFINET 名称 (PROFINET Name of Station)**
  显示 PROFINET 设备名称。
- **诊断模式 (Diagnostics Mode)**
  显示启用 EtherNet/IP 还是 PROFINET。
- **系统名称 (System Name)**
  显示设备名称。
- **设备类型 (Device Type)**
  显示设备的型号标识。
- **PROFINET AR 状态 (PROFINET AR Status)**
  显示 PROFINET 应用关系状态。
  - 在线 (Online)
    存在与 PROFINET 控制器的连接。PROFINET 控制器已将其组态数据下载到设备。设备可以将状态数据发送到 PROFINET 控制器。
    在这种状态下，无法在设备上组态 PROFINET 控制器所设置的参数。
  - 离线 (Offline)
    不存在与 PROFINET 控制器的连接。
- **电源线路 1 (Power Line 1)/电源线路 2 (Power Line 2)/以太网供电 (Power over Ethernet)**
  电源线路 1 和 2 或以太网供电的状态。仅在硬件支持的情况下才能显示电源线路 2 和以太网供电。有关详细信息，请参见操作说明。
- **PLUG 组态 (PLUG Configuration)**
  显示 PLUG 上组态数据的状态，请参见"系统 > PLUG > 组态"(System > PLUG > Configuration) 部分。

- **故障状态 (Fault Status)**

  显示设备的故障状态。

- **远程采集 (Remote Capture)**

  显示是否已启用该功能。

常用按钮

WBM 页面中包含下列标准按钮：

- **使用"Refresh"刷新显示画面**

  在显示当前参数的"基于 Web 的管理"页面底部有一个"刷新"(Refresh) 按钮。单击该按钮可为当前页面请求设备的最新信息。

  说明

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

- **使用"Set Values"保存条目**

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

  说明

  仅在以"admin"身份登录后才可以更改组态数据。

- **使用"创建"(Create) 创建条目**

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

- **使用"删除"(Delete) 删除条目**

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

- **使用"取消"(Cancel) 按钮取消操作**

  Basic Wizard 页面底部有一个"取消"(Cancel) 按钮。单击此按钮可关闭 Basic Wizard 而无需应用设置。

- **使用"下一页"(Next) 向下翻页**

  页面上能够显示的数据记录数受到限制。单击"下一页"(Next) 按钮，可向下翻页查看数据记录。

- **使用"上一页"(Prev) 向上翻页**

  页面上能够显示的数据记录数受到限制。单击"上一页"(Prev) 按钮，可向上翻页查看数据记录。

- **使用"清除"(Clear) 删除显示画面**

  无论是否选择了过滤器，在有序列日志的页面中，可以同时清除所有表格条目。此操作可清除显示画面。仅当将设备恢复为出厂设置并重启设备后，才会复位重启计数器。

  单击"清除"(Clear) 按钮可完全删除数据记录。

- **按钮"全部显示"(Show all)**

  可以在包含大量数据记录的页面上显示所有条目。单击"全部显示"(Show all) 按钮可在页面上显示所有条目。请注意，显示所有消息可能会花费一些时间。

- **用于页面切换的下拉列表**

  在包含大量数据记录的页面中，可以导航至所需页面。从下拉列表中选择要显示的相关页面。

- **"复位计数器"(Reset counter) 按钮**

  单击"复位计数器"(Reset counter) 可复位所有计数器。计数器会在重启后复位。

消息

如果您已启用"自动保存"(Automatic Save) 模式并且更改了一个参数，则显示区域中将出现如下消息"所做更改将在 x 秒内自动保存。按下'写启动组态'可立即保存更改"(Changes will be saved automatically in x seconds. Press 'Write Startup Config' to save the changes immediately)。

说明

中断保存

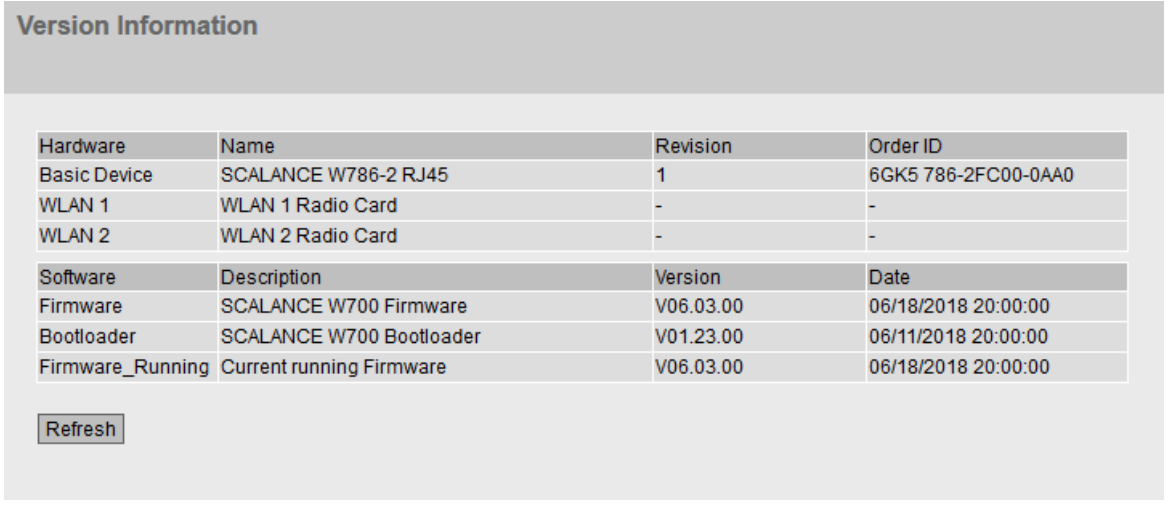
只有消息中的定时器到期后，才会启动保存。保存所需的时间取决于设备。
保存过程中将显示如下消息："正在保存组态数据。请勿关闭设备"(Saving configuration data in progress. Please do not switch off the device)。

- 不要在定时器到期后立即关闭设备。

6.4.2 版本

硬件和软件的版本

该页面会显示设备的硬件和软件版本。无法对该页面上的任何内容进行组态。



说明

表 1 包含以下列：

- **硬件 (Hardware)**
  - 基本设备 (Basic Device)
    显示基本设备
  - WLAN1 / WLAN 2
    显示可用无线卡
- **名称 (Name)**
  显示设备或模块的名称。
- **版本 (Revision)**
  显示设备的硬件版本。对于无线卡，如果启用了 WLAN 接口，将仅显示一个版本。
- **部件编号 (Article number)**
  显示设备或所述模块的部件编号。

表 2 包含以下列：

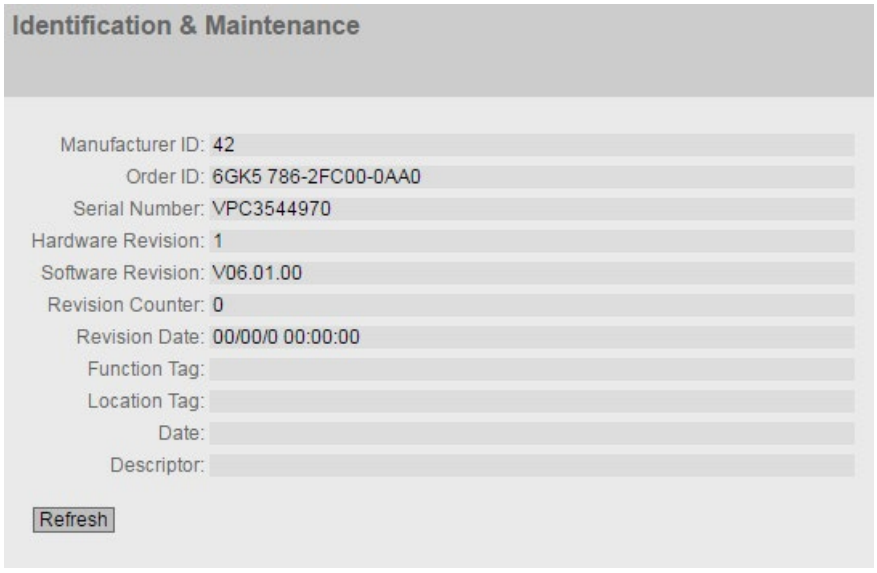
- **软件 (Software)**
  - 固件 (Firmware)
    显示当前固件版本。如果下载了新的固件文件，并且尚未重启设备，则在此处显示已下载固件文件的固件版本。下次重启后会激活并使用下载的固件。
  - 引导加载程序 (Bootloader)
    显示存储在设备上的引导软件的版本。
  - Firmware_Running
    显示设备上当前使用的固件版本。
- **说明 (Description)**
  显示软件的简要说明。

- **版本 (Version)**
  显示软件版本的版本号。
- **日期 (Date)**
  显示软件版本的创建日期。

6.4.3 I&M

标识和维护数据

该页面包含具体设备的供应商信息以及维护数据（如部件编号、序列号、版本号等）。无法对该页面上的任何内容进行组态。



显示值说明

该表格包括以下行：

- **制造商 ID (Manufacturer ID)**
  显示制造商 ID。
- **部件编号 (Article number)**
  显示部件编号。

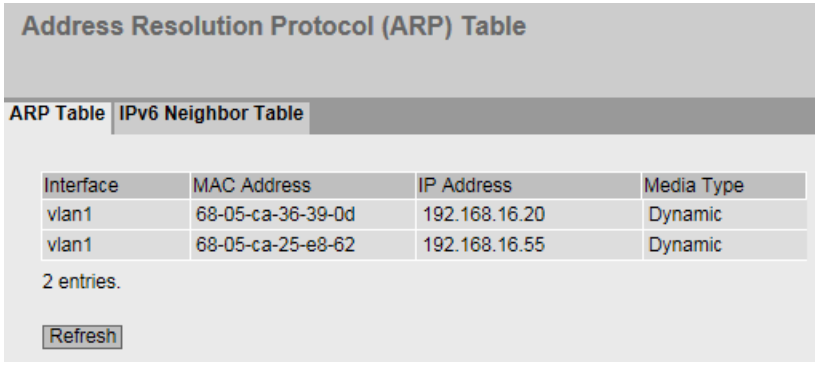
- **序列号 (Serial Number)**
  显示序列号。
- **硬件版本 (Hardware Revision)**
  显示硬件版本。
- **软件版本 (Software Revision)**
  显示软件版本。
- **修订计数器 (Revision Counter)**
  自固件版本 4.0 起，此处将始终显示值"0"而不受版本更改影响。
- **修订日期 (Revision date)**
  修订的日期：上次修订的日期和时间
- **功能标签 (Function Tag)**
  显示设备的功能标签（工厂标识）。工厂标识 (HID) 是通过 STEP 7 的 HW Config 在设备组态过程中创建的。
- **位置标签 (Location tag)**
  显示设备的位置标签。位置标识符 (LID) 是通过 STEP 7 的 HW Config 在设备组态过程中创建的。
- **日期 (Date)**
  显示通过 STEP 7 的 HW Config 组态设备时创建的日期。
- **说明 (Description)**
  显示通过 STEP 7 的 HW Config 组态设备时创建的说明。

6.4.4 ARP/邻居

6.4.4.1 ARP 表

MAC 地址和 IPv4 地址的分配

使用地址解析协议 (Address Resolution Protocol, ARP) 时，MAC 地址到 IPv4 地址的分配具有唯一性。该分配情况由各网络节点记录在自己的 ARP 表中。此 WBM 页面显示设备的这个 ARP 表。



显示值说明

该表格包括以下列：

- **"接口"(Interface)**

  显示获取行条目所用的接口。

- **MAC Address**

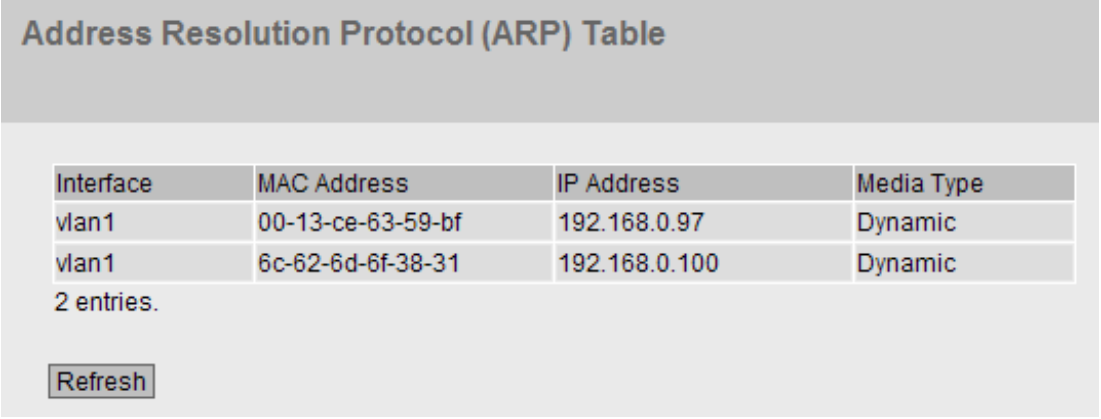
  显示目标设备或源设备的 MAC 地址。

- **IP Address**
  显示接收方的 IP 地址。
- **"介质类型"(Media Type)**
  显示连接的类型。
  – "动态"(Dynamic)
    设备自动识别到地址数据。
  – "静态"(Static)
    地址作为静态地址输入。

6.4.4.2 IPv6 邻居表

MAC 地址和 IPv6 地址的分配

借助 IPv6 邻居表，MAC 地址到 IPv6 地址的分配具有唯一性。该分配情况由各网络节点记录在自己的邻居表中。



显示值说明

该表格包括以下列：

- **Interface**

  显示获取行条目所用的接口。

- **MAC Address**

  显示目标设备或源设备的 MAC 地址。

- **IP Address**

  显示目标设备的 IPv6 地址。

- **Media Type**

  显示连接的类型。

  – "动态"(Dynamic)
  设备自动识别到地址数据。

  – "静态"(Static)

  地址作为静态地址输入。

6.4.5 日志表

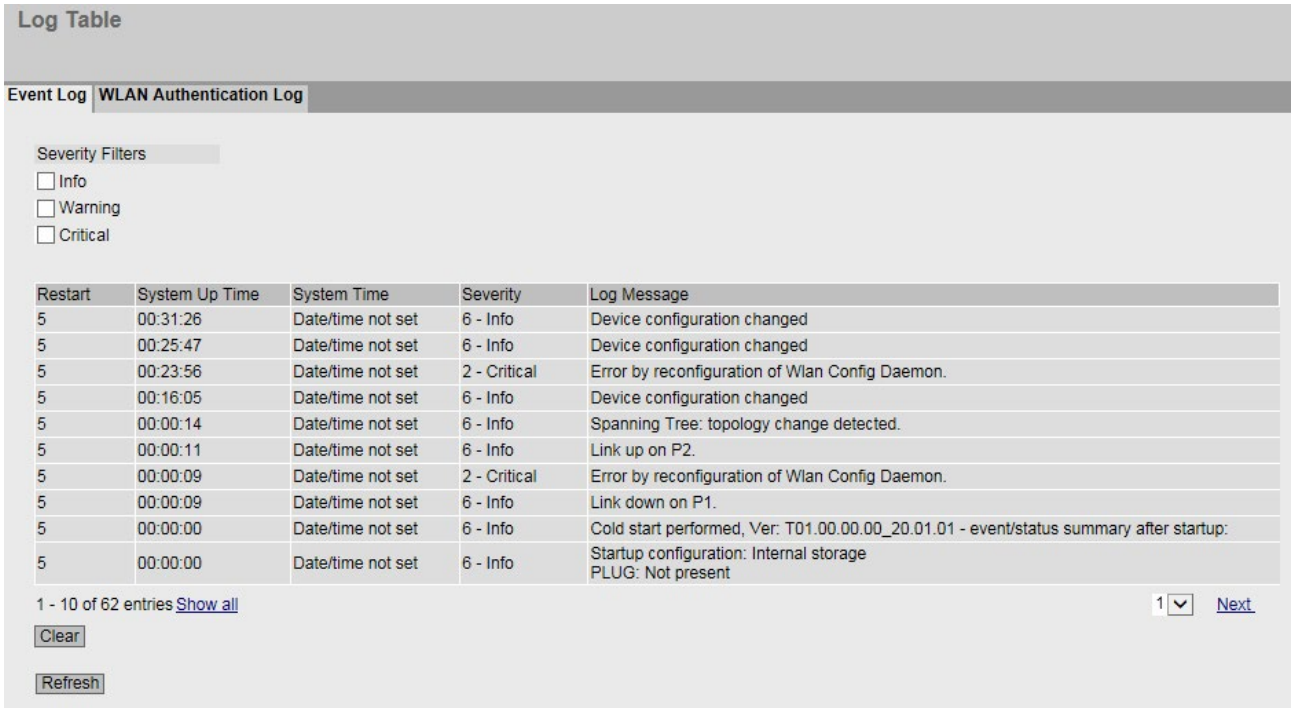
6.4.5.1 事件日志

记录事件

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

即使在设备关闭后，事件日志表的内容仍可保留。

无法对该页面上的任何内容进行组态。



Log Table

Event Log | WLAN Authentication Log

Severity Filters
- [ ] Info
- [ ] Warning
- [ ] Critical

Restart	System Up Time	System Time	Severity	Log Message
5	00:31:26	Date/time not set	6 - Info	Device configuration changed
5	00:25:47	Date/time not set	6 - Info	Device configuration changed
5	00:23:56	Date/time not set	2 - Critical	Error by reconfiguration of Wlan Config Daemon.
5	00:16:05	Date/time not set	6 - Info	Device configuration changed
5	00:00:14	Date/time not set	6 - Info	Spanning Tree: topology change detected.
5	00:00:11	Date/time not set	6 - Info	Link up on P2.
5	00:00:09	Date/time not set	2 - Critical	Error by reconfiguration of Wlan Config Daemon.
5	00:00:09	Date/time not set	6 - Info	Link down on P1.
5	00:00:00	Date/time not set	6 - Info	Cold start performed, Ver: T01.00.00.00_20.01.01 - event/status summary after startup:
5	00:00:00	Date/time not set	6 - Info	Startup configuration: Internal storage PLUG: Not present

1 - 10 of 62 entries Show all 1 Next

Clear

Refresh

说明

- **严重程度过滤器 (Severity Filters)**

  可以根据严重程度过滤表中的条目。要显示所有条目，请启用或禁用所有参数。

  说明

  每种严重程度最多支持在表中包含 400 个条目。如果一种严重程度已达到条目的最大数目，则会覆盖表中最早有关此严重程度的条目。该表会永久保存在内存中。

  – Info

    信息

    如果启用该参数，则会显示"信息"(Info) 类别的所有条目。

  – Warning

    警告

    如果启用该参数，则会显示"警告"(Warning) 类别的所有条目。

  – Critical

    严重

    如果启用该参数，则会显示"严重"(Critical) 类别的所有条目。

该表包括以下列：

- **重启 (Restart)**

  统计自上次复位为出厂设置以来的重启次数，并显示与发生的事件对应的设备重启。

- **系统运行时间 (System Up Time)**

  显示在所描述的事件发生时设备自上次重启以来已持续运行的时间。

- **系统时间 (System Time)**

  显示所描述事件发生的日期和时间。

- **严重程度 (Severity)**

  显示消息的严重程度。

- **日志消息 (Log Message)**

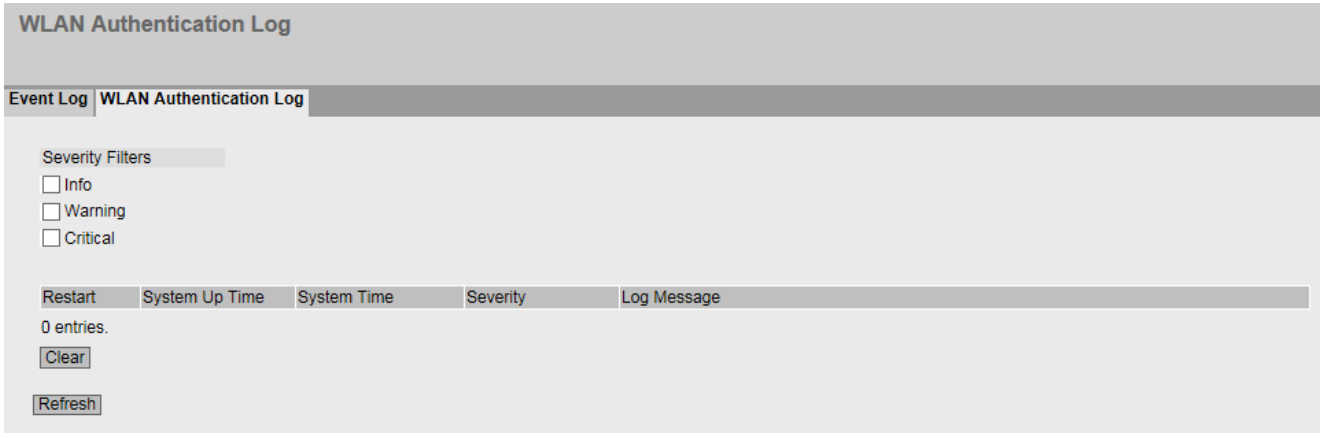
  显示已发生事件的简要说明。可在组态手册的附录 D (页 573) 中找到可能消息的列表。

如果已设定系统时间，则还会显示事件发生的时间。

6.4.5.2 WLAN 验证日志

记录验证尝试

此页面通过表格形式显示验证尝试成功或失败的信息。



无法对该页面上的任何内容进行组态。

说明

- **严重程度过滤器 (Severity Filters)**

  可以根据严重程度过滤表中的条目。要显示所有条目，请启用或禁用所有参数。

  说明

  每种严重程度最多支持在表中包含 400 个条目。如果一种严重程度已达到条目的最大数目，则会覆盖表中最早有关此严重程度的条目。该表会永久保存在内存中。

  – Info

    信息

    如果启用该参数，则会显示"信息"(Info) 类别的所有条目。

  – Warning

    警告

    如果启用该参数，则会显示"警告"(Warning) 类别的所有条目。

  – Critical

    严重

    如果启用该参数，则会显示"严重"(Critical) 类别的所有条目。

该表包括以下列：

- **重启 (Restart)**

  统计自上次复位为出厂设置以来的重启次数，并显示与发生的事件对应的设备重启。

- **系统运行时间 (System up time)**

  显示在所描述的事件发生时设备自上次重启以来已持续运行的时间。

- **系统时间 (System Time)**

  显示所描述事件发生的日期和时间。

- **严重程度 (Severity)**

  显示消息的严重程度。

- **日志消息 (Log Message)**

  显示已发生事件的简要说明。可在组态手册的附录 D (页 573) 中找到可能消息的列表。

如果已设定系统时间，则还会显示事件发生的时间。

6.4.6 故障

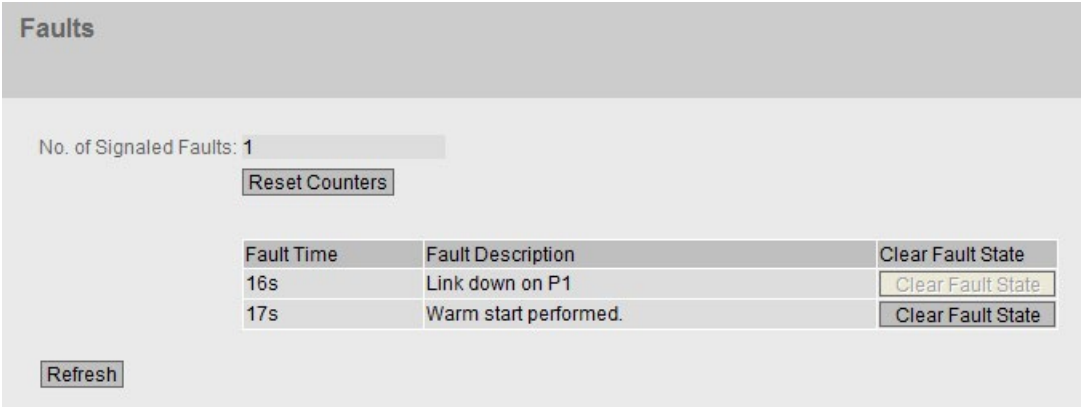
错误状态

如果出现故障，则会显示在此页面。在设备上，通过红色故障 LED 点亮来指示故障。

将指示设备的内部故障以及在下列页面上组态的故障：

- "系统 > 事件"(System > Events)
- "系统 > 故障监视"(System > Fault Monitoring)

始终从上次系统启动后开始计算故障时间。如果没有故障，则故障 LED 将熄灭。



说明

该页面包含以下框：

- **已通知故障数 (No. of Signaled Faults)**

  指示故障 LED 点亮的频率，而不是出现故障的次数。

- **"复位计数器"(Reset Counters) 按钮**

  此按钮用于重置编号。重启后，计数器将复位。

该表包含以下列：

- **故障时间 (Fault Time)**

  显示在所描述的故障发生时设备自上次重启以来已持续运行的时间。

- **故障描述 (Fault Description)**

  显示已发生错误/故障的简要说明。

- **清除故障状态 (Clear Fault State)**

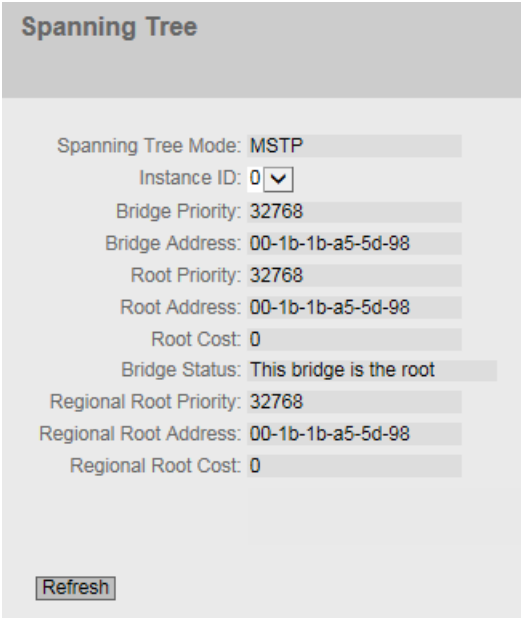
  有些故障可以确认，并将它们从错误列表中删除，例如，"冷/热启动"事件中的故障。可以通过"清除故障状态"(Clear Fault State) 按钮确认这些故障，或将其从故障列表中删除。

6.4.7 冗余

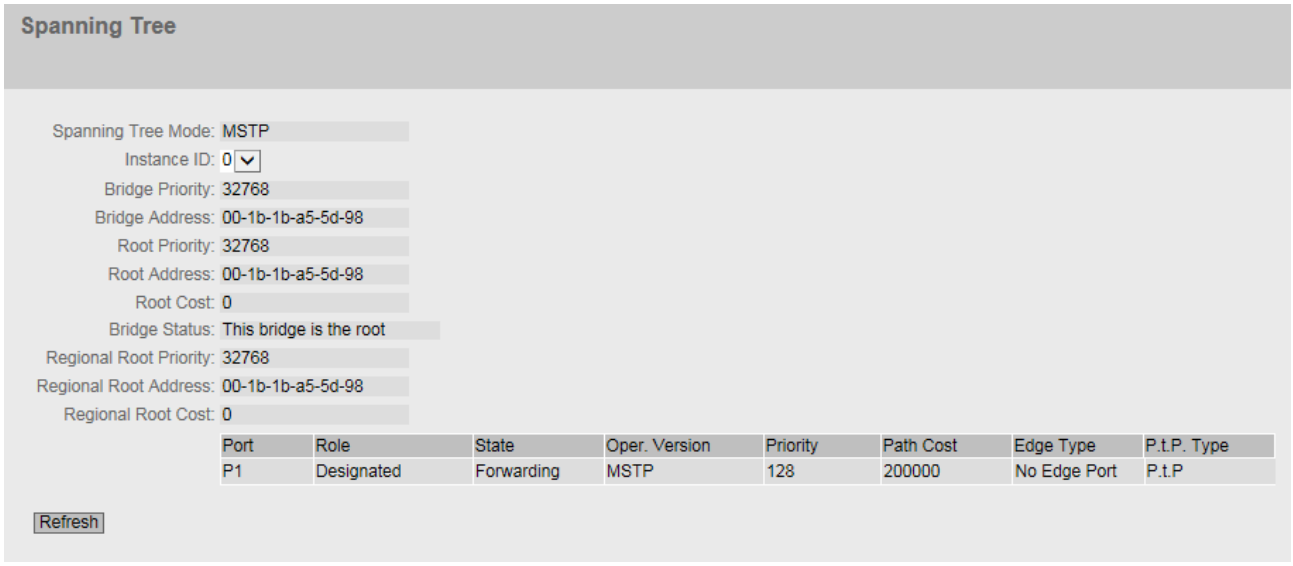
简介

该页面显示有关生成树和根网桥设置的最新信息。

如果关闭"生成树"，则只显示有关该设备的基本信息。


Spanning Tree
Spanning Tree Mode: MSTP
Instance ID: 0
Bridge Priority: 32768
Bridge Address: 00-1b-1b-a5-5d-98
Root Priority: 32768
Root Address: 00-1b-1b-a5-5d-98
Root Cost: 0
Bridge Status: This bridge is the root
Regional Root Priority: 32768
Regional Root Address: 00-1b-1b-a5-5d-98
Regional Root Cost: 0
Refresh

如果打开"生成树"(Spanning Tree)，则会显示"实例 ID"(Instance ID) 下拉列表中选择的实例状态的相关信息，并在表格中显示已组态端口的相关信息。显示的信息取决于生成树模式。



说明

该页面包含以下框：

- **生成树模式 (Spanning Tree Mode)**

  显示设置模式。在"第 2 层 > 组态"(Layer 2 > Configuration) 和"第 2 层 > MSTP > 常规"(Layer 2 > MSTP > General) 中指定模式。
  可以使用以下值：

  – '-'

  – STP

  – RSTP

  – MSTP

- **实例 ID (Instance ID)**

  显示实例编号。该参数取决于组态的模式。

- **网桥优先级 (Bridge Priority)/根优先级 (Root Priority)**

  根据网桥优先级来确定哪台设备会成为根网桥。优先级最高的网桥（换句话说，此参数的值最小）将成为根网桥。如果网络中有多个设备具有相同优先级，则 MAC 地址数值最小的设备将成为根网桥。网桥优先级和 MAC 地址这两个参数一起构成网桥标识符。由于根网桥管理所有路径的变更，出于帧延迟的考虑，根网桥应该尽可能处在中心位置。网桥优先级的值是 4096 的整数倍数，值范围从 0 到 32768。

- **网桥地址 (Bridge Address)/根地址 (Root Address)**

  网桥地址显示设备的 MAC 地址，根地址显示根网桥的 MAC 地址。

- **根开销 (Root Cost)**

  从该设备到根网桥的路径开销。

- **网桥状态 (Bridge Status)**

  显示网桥的状态，例如，设备是否为根网桥。

- **区域根优先级 (Regional root priority)**（仅适用于 MSTP）

  相关描述，请参见"网桥优先级"(Bridge priority)/"根优先级"(Root priority) 部分

- **区域根地址 (Regional root address)**（仅适用于 MSTP）

  显示区域根网桥的 MAC 地址。

- **区域根开销 (Regional Root Cost)**（仅适用于 MSTP）

  显示从设备到区域根网桥的路径开销。

该表格包含以下框：

- **端口 (Port)**

  显示设备通信所用的端口。

- **角色 (Role)**

  显示端口的状态。可能的值包括：

  – Disabled

    已从生成树中手动移除端口，生成树将不再考虑该端口。

– Designated

端口从根网桥中转移数据。

– Alternate

端口具有指向网段的备用路径。

– Backup

如果交换机具有多个指向同一网段的端口，则"较差"端口将变为备用端口。

– Root

端口提供指向根网桥的最佳路径。

– Master

此端口指向 MST 区域外部的根网桥。

- **状态 (State)**

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

– Discarding

该端口接收 BPDU 帧。其它进入或离开的帧会被丢弃。

– Listening

该端口接收和发送 BPDU 帧。端口包括在生成树算法中。其它离开或进入的帧会被丢弃。

– Learning

端口主动学习拓扑；即学习节点地址。其它离开或进入的帧会被丢弃。

– Forwarding

在重新组态时间后，端口在网络中激活。该端口接收和发送数据帧。

- **运行版本 (Oper. Version)**

介绍了端口以何种生成树类型运行

- **优先级 (Priority)**

  如果由生成树计算出的路径可能经过设备的多个端口，则选择优先级最高的端口（也就是此参数值最小的端口）。可输入的优先级数值介于 0 和 240 之间，步长为 16。如果输入的值不能被 16 整除，则会自动调整该值。默认值为 128。

- **路径开销 (Path Cost)**

  此参数用于计算将要选择的路径。选择值最小的路径作为路径。如果设备的多个端口具有相同的值，则选择端口号最小的端口。
  如果"开销计算"(Cost Calc.) 框的值为"0"，则显示自动计算出的值。否则会显示"开销计算"(Cost Calc) 框的值。
  主要根据传输速度来计算路径开销。可达到的传输速度越高，路径开销的值就越小。

  快速生成树的典型路径开销值如下：

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

- **边缘类型 (Edge Type)**

  显示连接类型。可能的值包括：

  – Edge Port

    边缘端口连接到此端口。

  – No Edge Port

    此端口上有生成树或快速生成树设备。

- **点对点类型 (P.t.P.类型 (P.t.P. Type)**

  显示点对点链路类型。可能的值包括：

  – P.t.P.

    对于半双工，认为是点对点链路。

  – Shared Media

    对于全双工连接，不采用点对点链路。

  说明

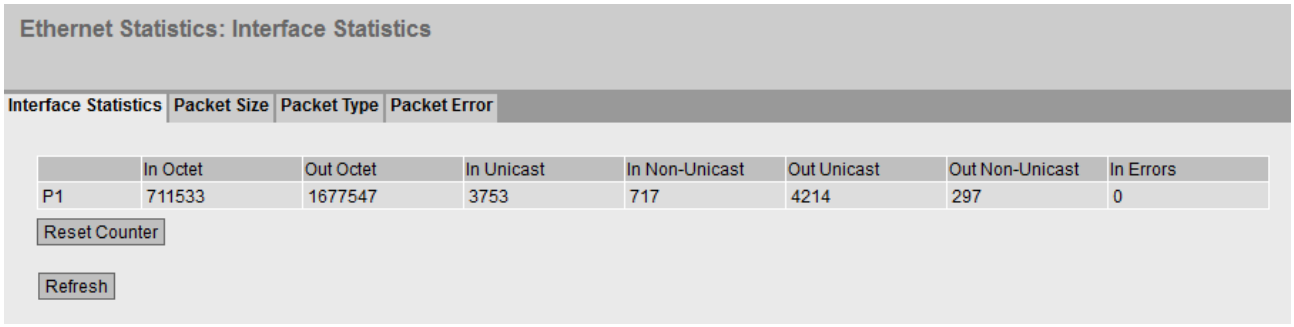
  点对点链路表示在两个设备之间直接连接。而共享介质连接可以是与集线器的连接。

6.4.8 以太网统计信息

6.4.8.1 接口统计信息

接口统计信息

此页面显示管理信息库 (MIB) 的接口表中的统计信息。



显示值

该表包括以下列：

- **输入八位位组 (In Octet)**

  显示接收到的字节数。

- **输出八位位组 (Out Octet)**

  显示发送的字节数。

- **输入单播 (In Unicast)**

  显示已接收的单播帧数。

- **输入非单播 (In Non Unicast)**

  显示接收到的非单播类型帧的数目。

- **输出单播 (Out Unicast)**

  显示已发送的单播帧数。

- **输出非单播 (Out Non Unicast)**

  显示发送的非单播类型帧的数目。

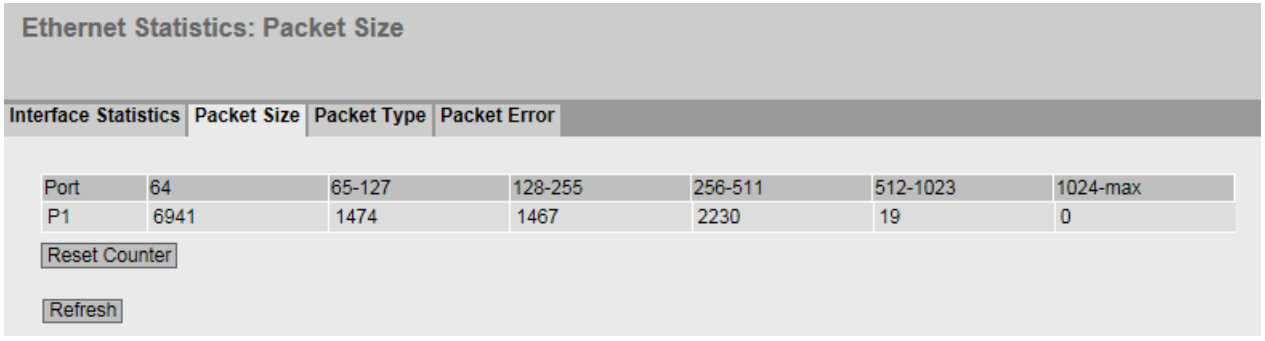
- **输入错误 (In Errors)**

  显示所有可能的 RX 错误数，请参见"数据包错误"(Packet Error) 选项卡。

6.4.8.2 数据包大小

按长度分类的帧

该页面会显示各个端口接收的各种大小的帧数。无法对该页面上的任何内容进行组态。



说明

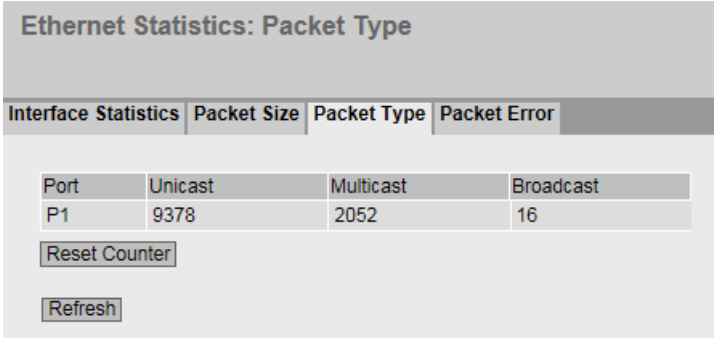
该表包括以下列：

- **端口 (Port)**
  显示可用端口。
- **帧长度 (Frame lengths)**
  端口号后面的其它各列包含按照帧长度分类的进入帧的绝对数量。
  帧长度分为以下几类：
  - 64 字节
  - 65 - 127 字节
  - 128 - 255 字节
  - 256 - 511 字节
  - 512 - 1023 字节
  - 1024 - 最大值

6.4.8.3 帧类型

按类型分类的已接收帧

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



描述

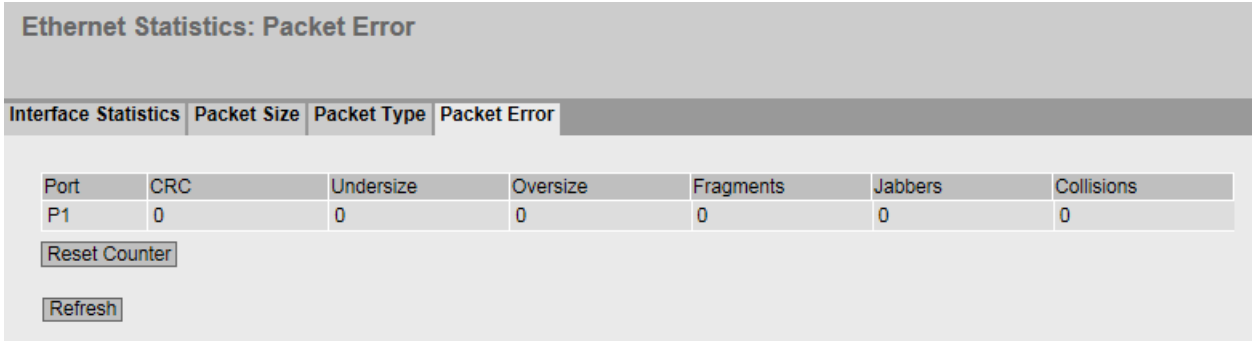
该表格包括以下列：

- **端口 (Port)**
  显示可用端口。
- **Unicast/Multicast /Broadcast**
  端口号之后的其他各列包括按照其帧类型"Unicast"、"Multicast"和"Broadcast"分类的入站帧的绝对数量。

6.4.8.4 数据包错误

接收到的坏帧

该页面显示每个端口接收到多少坏帧。无法对该页面上的任何内容进行组态。



说明

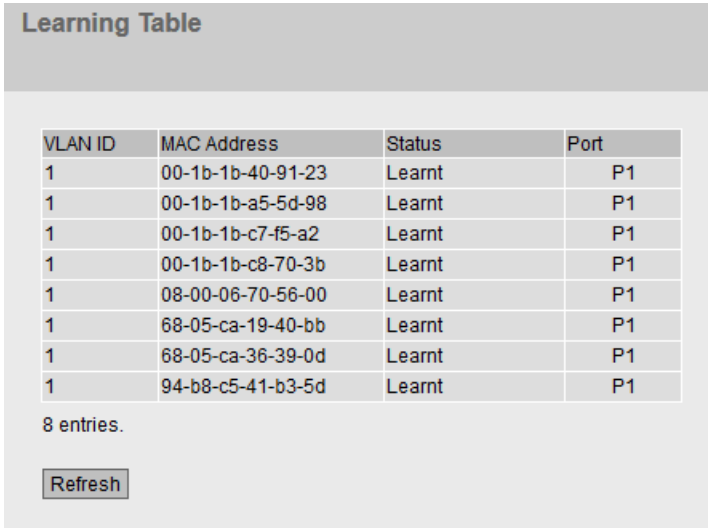
该表包括以下列：

- **Port**
  显示可用端口。
- **错误类型**
  端口号之后的其它各列包括按照其错误类型分类的到达帧的绝对数量。
  在该表的各列中，将根据以下错误类型进行区分：
  - CRC (Cyclic Redundancy Code)
    数据包长度在 64 到 1518 字节之间。数据包的 CRC 无效。
  - 过小 (Undersize)
    数据包长度小于 64 个字节。数据包的 CRC 有效。
  - 过大 (Oversize)
    数据包长度超过 1518 字节。数据包的 CRC 有效。
  - 分段 (Fragments)
    数据包长度小于 64 个字节。数据包的 CRC 无效。
  - 长帧 (Jabbers)
    帧长度超过 1518 个字节。数据包的 CRC 无效。
  - 冲突 (Collisions)
    在帧中检测到冲突事件。

6.4.9 学习表

地址过滤

此 WBM 页面显示学习表的当前内容。该表列出了单播地址帧的源地址。



说明

该表包含以下各列：

- **VLAN ID**

  显示节点的 VLAN ID。

  说明

  只有完成 VLAN 组态，表格中才会显示此列。

- **MAC 地址 (MAC Address)**

  显示节点的 MAC 地址。

- **状态 (State)**

  显示每个地址条目的状态：

  – Learnt

    通过从节点接收帧，学习相应的地址；如果从此节点再没接收到数据包，则在老化时间结束时删除该地址。

  – Invalid

    不评估这些值。

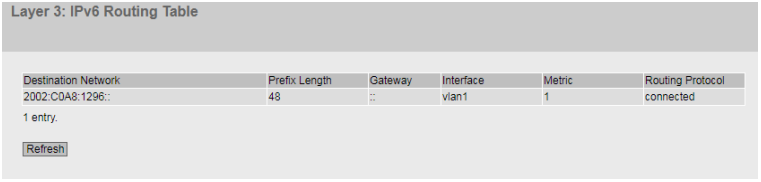
- **端口 (Port)**

  显示访问指定地址的节点时所使用的端口。设备接收到的目标地址与此地址相匹配的帧将被转发到此端口。

6.4.10 IPv6 路由

简介

该页面显示了当前使用的 IPv6 路由。



说明

该表包括以下列：

- **目标网络 (Destination Network)**

  显示此路由的目标地址。

- **前缀长度 (Prefix Length)**

  显示此路由的前缀长度。

- **网关 (Gateway)**

  显示此路由的网关。

- **接口 (Interface)**

  显示此路由的接口。

- **度量 (Metric)**

  显示路由的度量。值越大，数据包到达目的地所需的距离越长。

- **路由协议 (Routing Protocol)**

  显示产生路由表条目的路由协议。可以是以下条目：

  – Connected：已连接路由

  – Static：静态路由

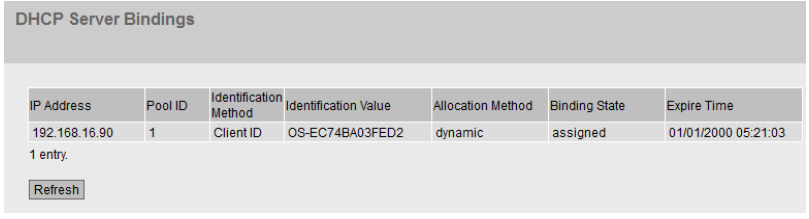
  – RIPng：通过 RIPng 路由

  – OSPFv3：通过 OSPFv3 路由

  – Other：其它路由

6.4.11 DHCP-Server

此页面显示通过 DHCP 服务器分配给设备的 IPv4 地址。



说明

- **IP 地址 (IP Address)**

  显示分配给 DHCP 客户端的 IPv4 地址。

- **池 ID (Pool ID)**

  显示 IPv4 地址段编号。

- **标识方法 (Identification Method)**

  显示标识 DHCP 客户端的方法。

- **标识值 (Identification value)**

  显示 DHCP 客户端的 MAC 地址或客户端 ID。

- **分配方法 (Allocation Method)**

  显示 IPv4 地址是以静态方式分配还是以动态方式分配。可在"系统 > DHCP > 静态租用"(System > DHCP > Static Leases) 中组态静态条目。

- **绑定状态 (Binding State)**

  显示分配的状态。

  – 已分配 (Assigned)
    已使用分配。

  – 未使用 (Not used)
    未使用分配。

  – 检查 (Probing)
    正在检查分配。

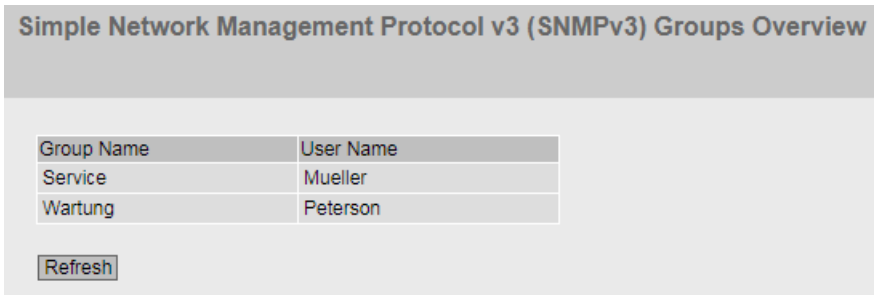
  – 未知 (Unknown)
    分配状态未知。

- **过期时间 (Expire Time)**

  显示所分配的 IPv4 地址保持有效的时长。超过该时间后，DHCP 客户端必须请求新的 IPv4 地址或扩展所分配的 IPv4 地址的租用时间。

6.4.12 SNMP

该页面显示所创建的 SNMPv3 组。在"系统 > SNMP"(System > SNMP) 中组态 SNMPv3 组。



说明

该表格包括以下列：

- **组名称 (Group Name)**

  显示组名称。

- **用户名 (User Name)**

  显示分配到该组的用户。

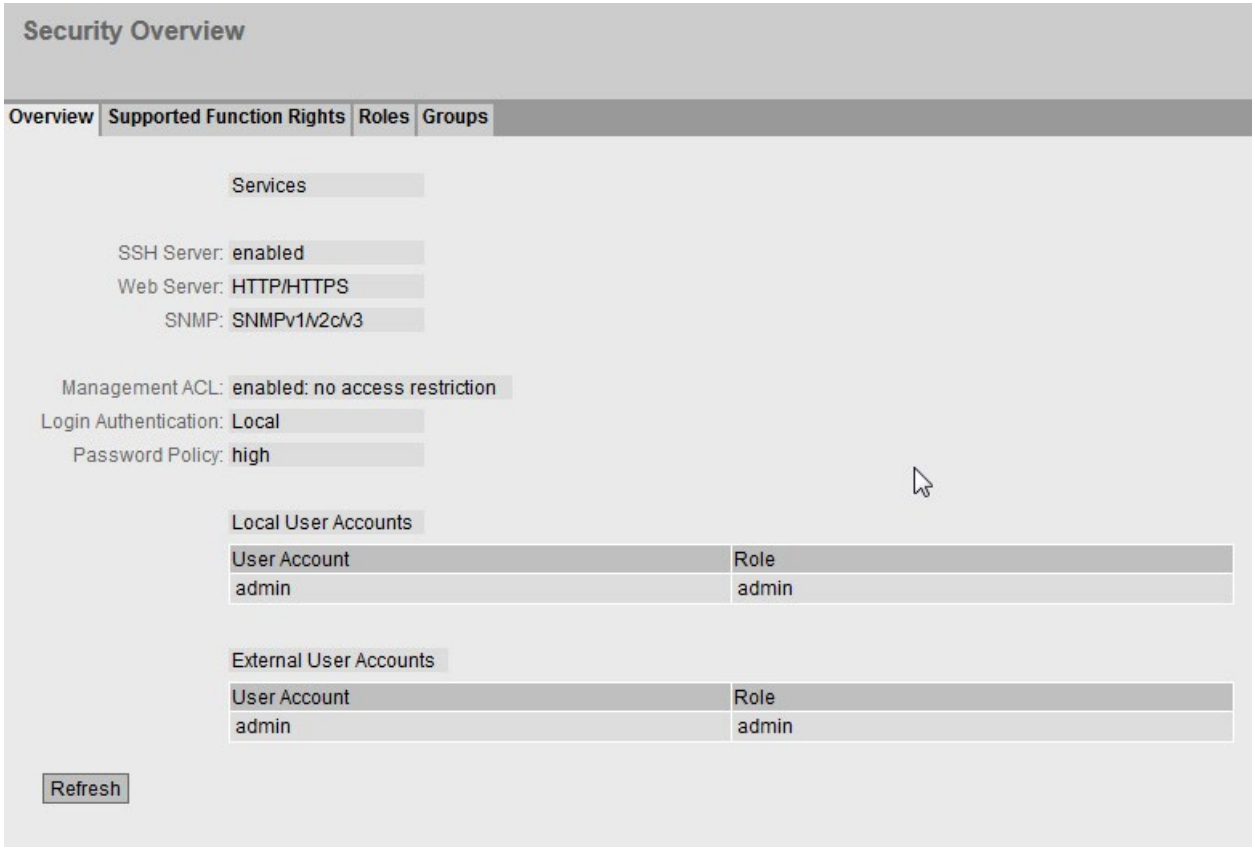
6.4.13 Security

6.4.13.1 概述

说明

所显示的值取决于登录的用户的权限。

该页面显示了安全设置和本地以及外部用户帐户。



说明

服务

"Services"列表显示了安全设置。

- **SSH Server**

  在"系统 > 组态"(System > Configuration) 中组态设置。

  – 启用：对 CLI 进行加密形式的访问。

  – 禁用：无法对 CLI 进行加密形式的访问。

- **Web Server**

  在"System > Configuration"中组态设置。

  – HTTP/HTTPS：可以通过 HTTP 和 HTTPS 访问 WBM。

  – HTTPS：现在，只能通过 HTTPS 访问 WBM。

- **SNMP**

  可以在"System > SNMP > General"中组态设置。

  – "-"（SNMP 已禁用）
    不能通过 SNMP 访问设备参数。

  – SNMPv1/v2c/v3
    可以通过 SNMP 版本 1、2c 或 3 访问设备参数。

  – SNMPv3
    只可通过 SNMP 版本 3 访问设备参数。

- **管理 ACL (Management ACL)**

  在"安全 > 管理 ACL"(Security > Management ACL) 中组态设置。

  – 启用：仅受限访问 (Enabled: Restricted access only)：使用访问控制列表 (ACL) 访问受限。

  – 禁用：无访问限制 (Disabled: No access restriction)：管理 ACL 未启用。

  – 启用：无访问限制 (Enabled: No access restriction)：管理 ACL 启用，但使用访问控制列表 (ACL) 访问受限。

- **Login Authentication**

  在"安全 > AAA > 常规"(Security > AAA > General) 中组态设置。

  – Local

    必须在设备上进行本地验证。

  – RADIUS

    必须通过 RADIUS 服务器处理验证。

  – Local and RADIUS

    使用设备上的用户（用户名和密码）以及通过 RADIUS 服务器都可以进行验证。

    首先在本地数据库中搜索用户。如果本地数据库中不存在该用户，将发送 RADIUS 查询。

  – RADIUS and fallback local

    必须通过 RADIUS 服务器处理验证。

    只有无法在网络中访问 RADIUS 服务器时，才会执行本地验证。

- **密码策略 (Password Policy)**

  显示当前正在使用的密码策略。

本地和外部用户帐户

可以在"Security > User Accounts"中组态本地用户帐户和角色。

创建本地用户帐户时，会自动生成外部用户帐户。

本地用户帐户所涉及的各个用户均具备登录设备所需的密码。

在表"External User Accounts"中，用户与角色相关联。在该示例中，用户"Observer"与"user"角色相关联。用户在 RADIUS 服务器上进行定义。角色在设备上进行本地定义。RADIUS 服务器对用户进行了授权，但相应的组未知或不存在，则设备会检查表"External User Accounts"中是否存在用户条目。如果存在相应的条目，则表示用户已使用相关角色的权限进行了登录。如果相应的组在设备上为已知状态，则对两个表进行了评估。为用户分配了较高权限的角色。

说明

只有将"SiemensVSA"设为"RADIUS Authorization Mode"时，才会对表"External User Accounts"进行评估。

借助 CLI 可以访问外部用户帐户。

"本地用户帐户"(Local User Accounts) 表包括以下列：

- **用户帐户 (User Account)**

  显示本地用户的名称。

- **角色 (Role)**

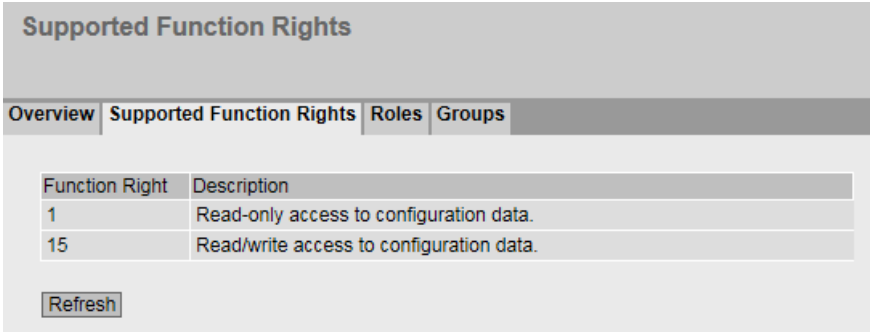
  显示用户角色。在"信息 > 安全 > 角色"(Information > Security > Roles) 中可以了解有关角色的功能权限的更多信息。

6.4.13.2 所支持的功能权限

说明

所显示的值取决于登录的用户的角色。

此页面显示了可在设备上本地使用的功能权限。



显示值说明

- **Function Right**

  显示功能权限的编号。将与设备参数相关的不同权限分配给不同的编号。

- **Description**

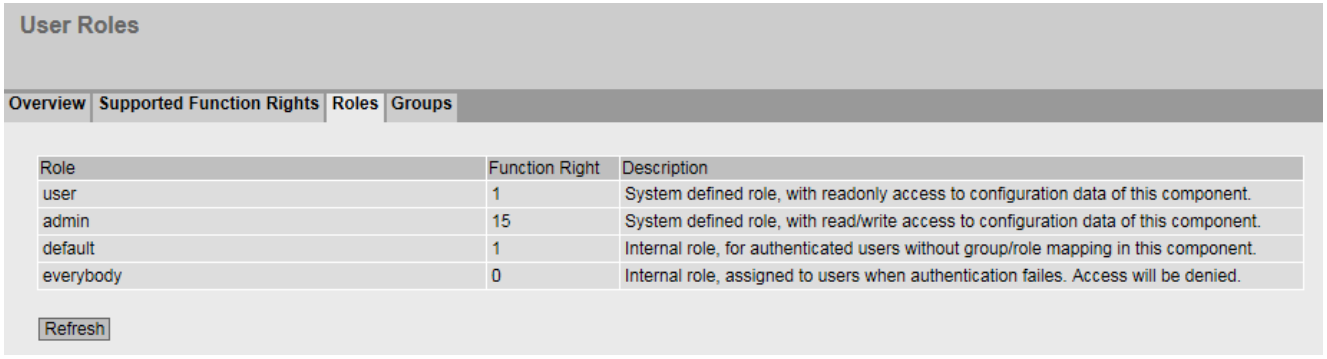
  显示功能权限的说明。

6.4.13.3 角色

说明

所显示的值取决于登录的用户的角色。

此页面显示了在设备上本地有效的角色。



说明

该表包含以下列：

- **Role**

  显示角色的名称。

- **Function Right**

  显示角色的功能权限：

  – 1

    具备该角色的用户可以读取设备参数但不能对其进行更改。

  – 15

    具备该角色的用户可以读取和更改设备参数。

  – 0

    该角色是在无法对用户进行身份验证时设备在内部分配的角色。用户被拒绝访问设备。

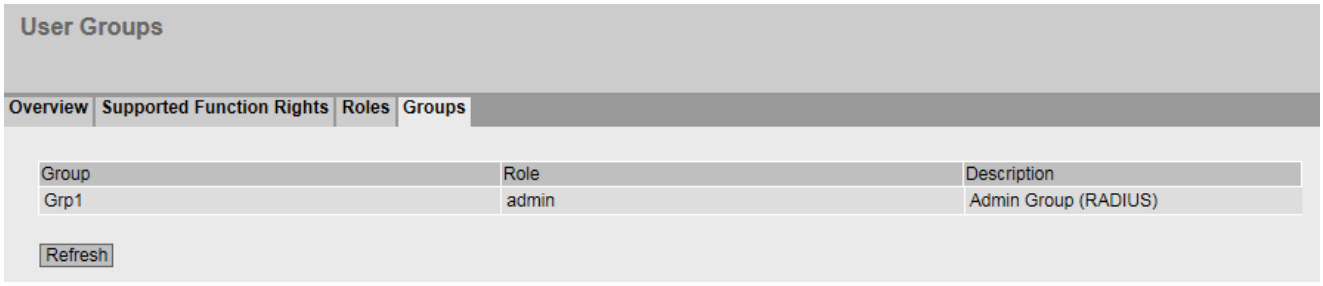
- **Description**

  显示角色的说明。

6.4.13.4 组

说明
所显示的值取决于登录的用户的角色。

该页面显示了组与角色之间的对应关系。组在 RADIUS 服务器上定义。角色在设备上本地定义。



显示值说明

该表格包括以下列：

- **Group**

  显示组的名称。名称与 RADIUS 服务器上的组相匹配。

- **Role**

  显示角色的名称。使用 RADIUS 服务器上的链接组进行了验证的用户将获得设备上本地有效的该角色的权限。

- **Description**

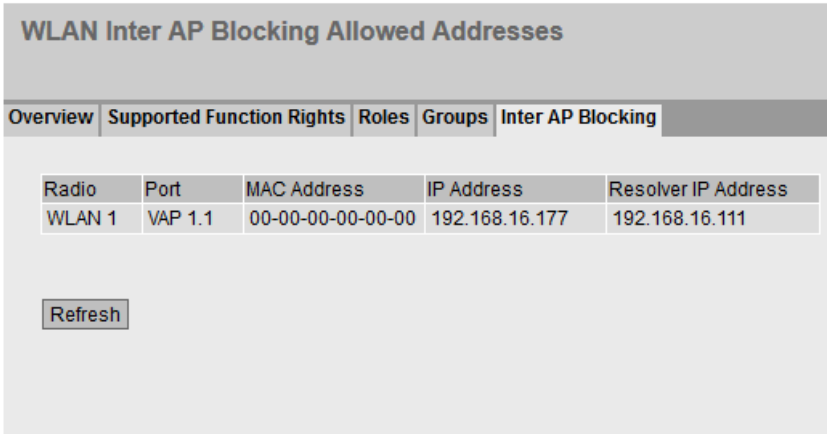
  显示链接的说明。

6.4.13.5 AP 间阻塞

说明

- 该 WBM 页面仅在接入点模式下可用。
- 可使用以下 KEY-PLUG 启用此 WBM 页面：
  - W780 iFeatures (MLFB 6GK5 907-8PA00)
  - W700 Security (MLFB 6GK5907-0PA00)

WBM 页面显示允许与客户端进行通信的设备列表。



说明

该表包括以下列：

- **无线 (Radio)**

  显示与设置相关的可用 WLAN 接口。

- **端口 (Port)**

- 显示与设置相关的 VAP 接口。

- **MAC 地址 (MAC Address)**

  显示可以与客户端通信的设备的 MAC 地址。

- **IP 地址 (IP Address)**

  显示可以与客户端通信的 SCALANCE W 设备的 IPv4 地址。

- **解析器 IP 地址 (Resolver IP Address)**

  显示接入点用来解析允许的 IPv4 地址的 IPv4 地址。

6.4.14 WLAN

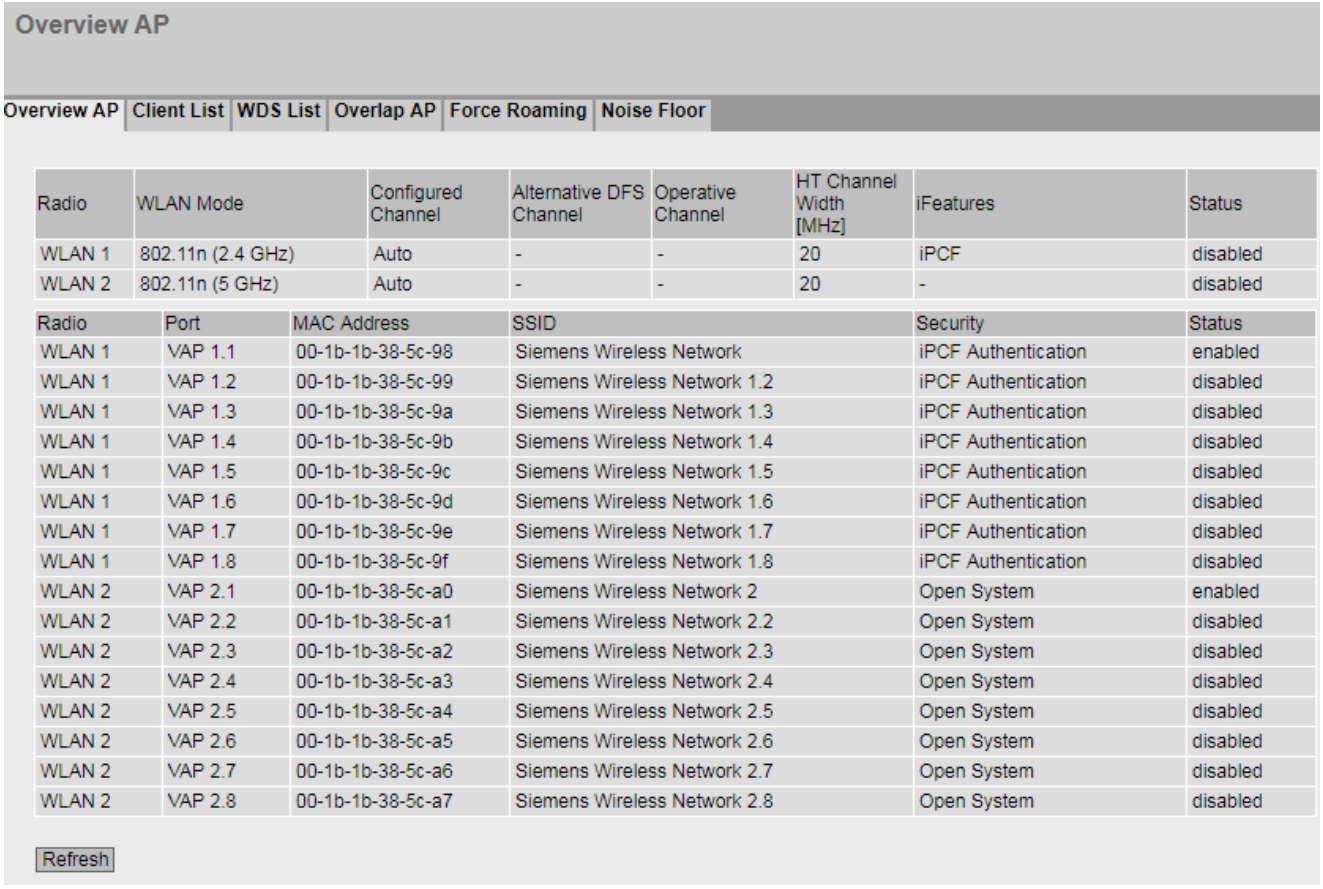
6.4.14.1 接入点概述

组态概述

此页面显示了 WLAN 或 WLAN 接口的这些设置/属性。

说明

该 WBM 页面仅在接入点模式下可用。



Radio	WLAN Mode	Configured Channel	Alternative DFS Channel	Operative Channel	HT Channel Width [MHz]	iFeatures	Status
WLAN 1	802.11n (2.4 GHz)	Auto	-	-	20	iPCF	disabled
WLAN 2	802.11n (5 GHz)	Auto	-	-	20	-	disabled

Radio	Port	MAC Address	SSID	Security	Status
WLAN 1	VAP 1.1	00-1b-1b-38-5c-98	Siemens Wireless Network	iPCF Authentication	enabled
WLAN 1	VAP 1.2	00-1b-1b-38-5c-99	Siemens Wireless Network 1.2	iPCF Authentication	disabled
WLAN 1	VAP 1.3	00-1b-1b-38-5c-9a	Siemens Wireless Network 1.3	iPCF Authentication	disabled
WLAN 1	VAP 1.4	00-1b-1b-38-5c-9b	Siemens Wireless Network 1.4	iPCF Authentication	disabled
WLAN 1	VAP 1.5	00-1b-1b-38-5c-9c	Siemens Wireless Network 1.5	iPCF Authentication	disabled
WLAN 1	VAP 1.6	00-1b-1b-38-5c-9d	Siemens Wireless Network 1.6	iPCF Authentication	disabled
WLAN 1	VAP 1.7	00-1b-1b-38-5c-9e	Siemens Wireless Network 1.7	iPCF Authentication	disabled
WLAN 1	VAP 1.8	00-1b-1b-38-5c-9f	Siemens Wireless Network 1.8	iPCF Authentication	disabled
WLAN 2	VAP 2.1	00-1b-1b-38-5c-a0	Siemens Wireless Network 2	Open System	enabled
WLAN 2	VAP 2.2	00-1b-1b-38-5c-a1	Siemens Wireless Network 2.2	Open System	disabled
WLAN 2	VAP 2.3	00-1b-1b-38-5c-a2	Siemens Wireless Network 2.3	Open System	disabled
WLAN 2	VAP 2.4	00-1b-1b-38-5c-a3	Siemens Wireless Network 2.4	Open System	disabled
WLAN 2	VAP 2.5	00-1b-1b-38-5c-a4	Siemens Wireless Network 2.5	Open System	disabled
WLAN 2	VAP 2.6	00-1b-1b-38-5c-a5	Siemens Wireless Network 2.6	Open System	disabled
WLAN 2	VAP 2.7	00-1b-1b-38-5c-a6	Siemens Wireless Network 2.7	Open System	disabled
WLAN 2	VAP 2.8	00-1b-1b-38-5c-a7	Siemens Wireless Network 2.8	Open System	disabled

说明

表 1 包含以下列：

- **无线 (Radio)**

  显示可用的 WLAN 接口。

- **端口 (Port)**

  显示可用 VAP 接口。

- **WLAN 模式 (WLAN Mode)**

  显示传输标准。如果激活了 DFS，则仅显示组态的传输标准"802.11a"，而不额外显示传输标准"802.11h"。

- **已组态通道 (Configured Channel)**

  显示组态的通道。如果显示"Auto"，则接入点将自行搜索空闲通道。

- **备用 DFS 通道 (Alternative DFS Channel)**

  如果 DFS 功能已启用，则显示为接入点组态的备用通道。
  如果显示"自动"(Auto)，则接入点将自行搜索备用通道。
  如果已启用 DFS 功能，并且接入点在花费 60 秒时间搜索主要用户后才开始使用所选通道进行通信，将显示文本"scanning ..."而不是通道。

- **运行通道 (Operational channel)**

  显示接入点通信时所使用的接入点通道。

- **HT 通道宽度 [MHz] (HT Channel Width [MHz])**

  显示通道带宽。

  – 20

    通道带宽为 20 MHz

  – 40 up

    通道带宽 40 MHz。使用组态的通道以及高于其带宽的相邻通道。

  – 40 down

    通道带宽 40 MHz。使用组态的通道以及低于其带宽的相邻通道。

  说明

  通道带宽 40 MHz 和频段 2.4 GHz

  如果接入点在组态的通道中或者在相邻的通道中检测到其它接入点，则原接入点会将通道带宽从 40 MHz 更改为 20 MHz。如果在接入点上设置"空闲"通道，则该接入点将使用 40 MHz 的通道带宽。

- **iFeatures**

  显示使用哪些 iFeatures。

  – -

    不使用 iFeatures。

  – iPCF

  – iPCF-HT

  – iPCF-MC

  – iPRP

  – iREF

  – AeroScout

- **状态 (State)**

  显示 WLAN 接口的状态。

  – enabled

    WLAN 接口已启用。

  – disabled

    WLAN 接口已禁用。

表 2 包含以下列：

- **无线 (Radio)**

  在此列中显示可用的 WLAN 接口。

- **端口 (Port)**

  显示虚拟接入点的端口。

- **MAC 地址 (MAC Address)**

  显示虚拟接入点的 MAC 地址。

- **SSID**

  显示 SSID。

- **安全 (Security)**
  显示所采用的验证方法。
  - 如果采用的验证方法是"开放式系统 + 加密"(Open System + Encryption) 或 "Shared Key"，则这两种验证方法都会显示"已加密 (WEP/AES)"(Encrypted (WEP/AES))。
  - 如果在 WLAN 接口上启用了 iPCF、iPCF-HT 或 iPCF-MC 模式，则根据加密状态显示以下内容：

    iPCF 加密 (AES)：加密已启用。

    iPCF 验证：加密已禁用。

- **状态 (State)**
  显示 WLAN 接口的状态。
  - enabled
    WLAN 接口已启用。
  - disabled
    WLAN 接口已禁用。

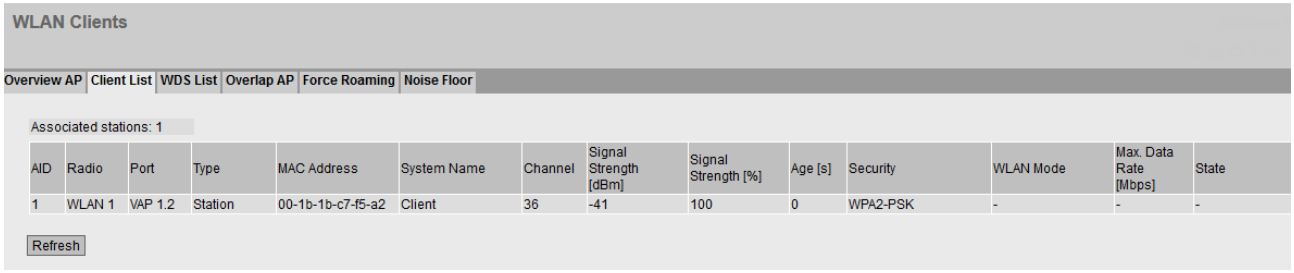
6.4.14.2 客户端列表

登录的客户端

WBM 页面显示了登录到接入点的客户端以及状态、信号强度、MAC 地址等其它信息。

说明

该 WBM 页面仅在接入点模式下可用。



说明

- **登录的客户端 (Logged-on clients)**

  显示登录到接入点的客户端的数量。

该表包括以下列：

- **AID** (Associated ID)

  显示客户端的连接 ID。如果客户端通过 VAP 接口与接入点相连，则为该客户端分配一个连接 ID。此连接 ID 在 VAP 接口内是唯一的。如果两个客户端在不同的 VAP 接口登录，则两个客户端都可接收同样的 ID。

- **无线 (Radio)**

  显示可用的 WLAN 接口。

- **端口 (Port)**

  显示 VAP 接口。

- **类型 (Type)**

  显示客户端类型，例如"Sta"代表 IEEE 802.11 标准客户端。

- **MAC 地址 (MAC Address)**

  显示客户端的 MAC 地址。

- **系统名称 (System Name)**

  如果客户端将其系统名称告知接入点，则将显示客户端的系统名称。不是所有客户端都支持此参数。

- **通道 (Channel)**

  显示客户端与接入点进行通信时所使用的通道。

- **信号强度 [dBm] (Signal Strength [dBm])**

  显示所连接客户端的信号强度（单位：分贝毫瓦）。

- **信号强度 [%] (Signal strength [%])**

  显示所连接客户端的信号强度百分数。

- **老化时间 [s] (Age [s])**

  显示自客户端上次活动以来所经过的时间。

- **安全性 (Security)**

  显示所采用的验证方法。

  – 如果采用的验证方法是"开放式系统 + 加密"(Open System + Encryption) 或 "Shared Key"，则这两种验证方法都会显示"已加密 (WEP/AES)"(Encrypted (WEP/AES))。

  – 如果在 WLAN 接口上启用了 iPCF、iPCF-HT 或 iPCF-MC 模式，则根据加密状态显示以下内容：

    iPCF 加密 (AES)：加密已启用。

    iPCF 验证：加密已禁用。

- **WLAN 模式 (WLAN Mode)**

  显示传输标准。如果激活了 DFS，则仅显示组态的传输标准"802.11a"，而不额外显示传输标准"802.11h"。

- **最大数据传输速率 (Mbps) (Max. Data Rate (Mbps))**

  显示最大的数据传输速度（单位：兆位每秒）。

- **状态 (State)**

  显示连接的当前状态，例如"已连接"(connected) 表示客户端已连接到 AP，并随时可与 AP 进行通信。

6.4.14.3 WDS 列表

接入点之间的通信

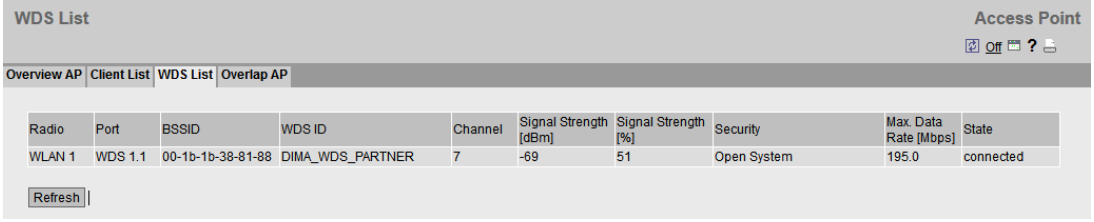
在正常运行时，接入点将充当网络的接口与客户端通信。但是，有时会存在多个接入点需要彼此互相通信的情况，例如，在需要扩展无线覆盖范围或设置无线骨干时。WDS（Wireless Distributed System，无线分布式系统）支持此模式。

默认情况下，每 2 秒更新一次列表。要禁用更新，请单击"On"。将显示"Off"取代"On"。默认情况下，始终在 WBM 页面上启用更新。

说明

该 WBM 页面仅在接入点模式下可用。

此页面显示接入点 WDS 连接的相关信息。



说明

该表包括以下列：

- **无线 (Radio)**

  显示可用的 WLAN 接口。

- **端口 (Port)**

  显示端口。

- **BSSID**

- 显示 WDS 伙伴的 MAC 地址。

- **WDS ID**

  显示 WDS 伙伴的名称。

- **通道 (Channel)**

  显示接入点与 WDS 伙伴进行通信时所使用的通道。

- **信号强度 [dBm] (Signal Strength [dBm])**

  显示所连接接入点的信号强度（单位：bBm）。

- **信号强度 [%] (Signal strength [%])**

  显示所连接接入点的信号强度百分比。

- **安全性 (Security)**

  显示所采用的验证方法。

  – 如果采用的验证方法是"开放式系统 + 加密"(Open System + Encryption) 或 "Shared Key"，则这两种验证方法都会显示"已加密 (WEP/AES)"(Encrypted (WEP/AES))。

  – 如果在 WLAN 接口上启用了 iPCF、iPCF-HT 或 iPCF-MC 模式，则根据加密状态显示以下内容：

    iPCF 加密 (AES)：加密已启用。

    iPCF 验证：加密已禁用。

- **最大数据传输速率 (Mbps) (Max. Data Rate (Mbps))**

  显示相关 WDS 伙伴的最大数据传输速度。

- **状态 (State)**

  显示 WDS 连接的当前状态。

6.4.14.4 重叠 AP

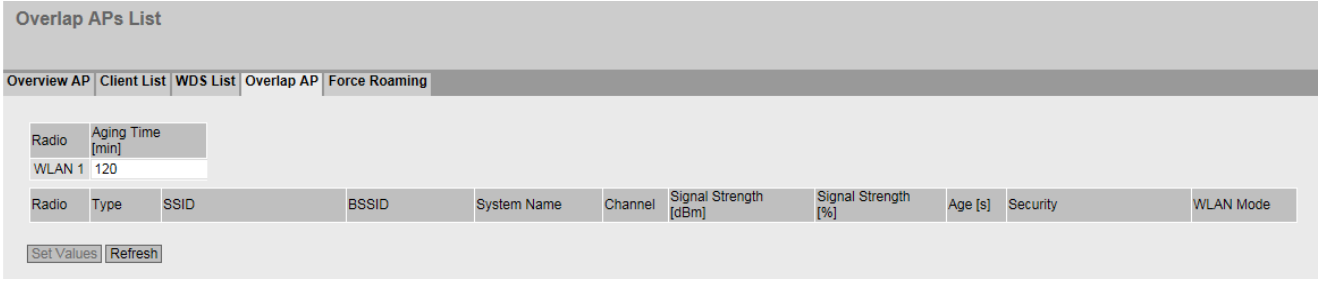
重叠通道

说明

该 WBM 页面仅在接入点模式下可用。

为实现最佳数据吞吐量，所设置的无线通道不能被其它接入点使用。在 2.4 GHz 频段（802.11b 或 802.11g）中，通道存在重叠现象，因此接入点不仅占用设置的通道，还会占用两条或三条相邻通道。因此，应确保与邻近的接入点间具有足够大的通道间隔。

此 WBM 页面显示设置的通道或相邻通道 (2.4 GHz) 上可见的所有接入点。如果此处有输入内容，则接入点的最大数据吞吐量以及接入点的通信链接可用性都有可能被削弱。



说明

表 1 包含以下列：

- **无线 (Radio)**

  显示可用的 WLAN 接口。

- **Aging Time [min]**

  指定列表中条目的生命周期。如果接入点未激活的时间超过设定的时间，则将其从列表中删除。

说明

更改老化时间

老化时间即为 WLAN 设置。因此，如果更改老化时间，则会短暂中断 WLAN 连接以接受新值。

该表包括以下列：

- **无线 (Radio)**

  在此列中显示可用的 WLAN 接口。

- **类型 (Type)**

  显示 WLAN 接口的模式。

- **SSID**

  显示接入点的 SSID。

- **BSSID**

  显示接入点的 MAC 地址。

- **系统名称 (System Name)**

  显示 SCALANCE W700 设备的系统名称。输入内容取决于接入点。不是所有接入点都支持这一参数。

- **通道 (Channel)**

  显示客户端与接入点进行通信时所使用的通道。

- **信号强度 [dBm] (Signal Strength [dBm])**

  显示客户端的信号强度（单位：bBm）。

- **信号强度 [%] (Signal strength [%])**

  显示客户端的信号强度百分数。

- **Age [s]**

  显示自上次接入点活动以来所经过的时间。

- **安全性 (Security)**

  显示所采用的验证方法。

  – 如果采用的验证方法是"开放式系统 + 加密"(Open System + Encryption) 或 "Shared Key"，则这两种验证方法都会显示"已加密 (WEP/AES)"(Encrypted (WEP/AES))。

  – 如果在 WLAN 接口上启用了 iPCF、iPCF-HT 或 iPCF-MC 模式，则根据加密状态显示以下内容：

    iPCF 加密 (AES)：加密已启用。

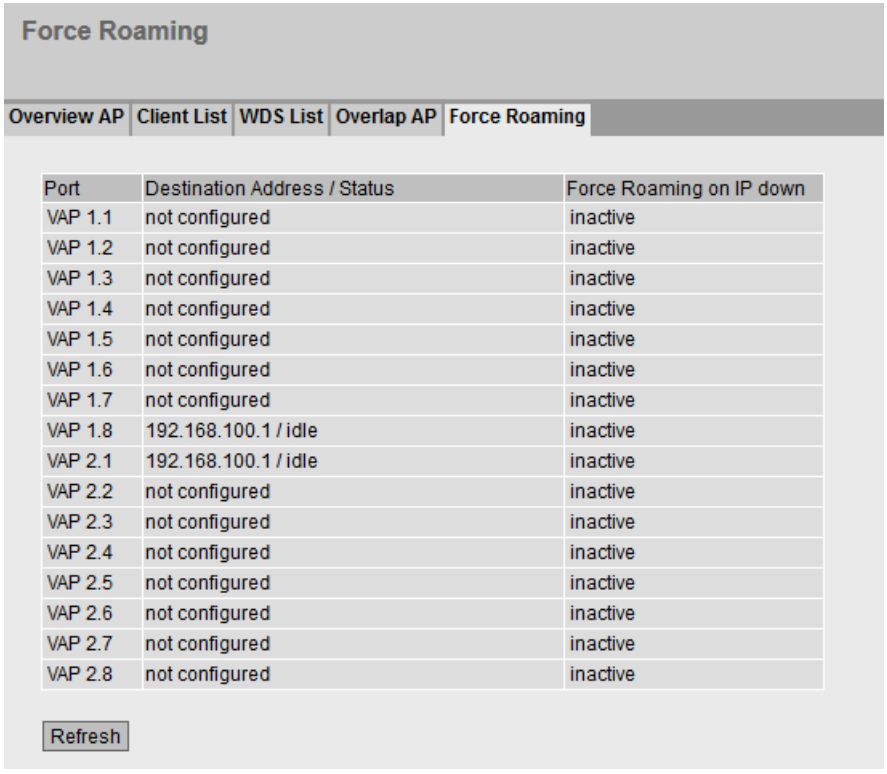
    iPCF 验证：加密已禁用。

- **WLAN 模式 (WLAN Mode)**

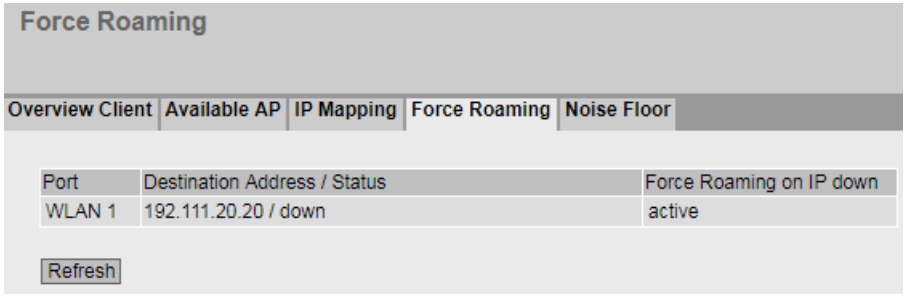
  显示传输标准。如果激活了 DFS，则仅显示组态的传输标准"802.11a"或 "802.11n"，而不额外显示传输标准"802.11h"。

6.4.14.5 强制漫游

在接入点模式下：



在客户端模式下：



此 WBM 页面显示了连接的当前状态。还显示了当前是否存在漫游。

设备会周期性监视与特定地址的连接。为此，设备会以固定时间间隔向已组态的目标地址发送回送消息 (ping)。

说明

该表包括以下列：

- **端口 (Port)**

  显示可用接口。

  – VAP X.Y（在接入点模式下）。

  – WLAN 0/X（在客户端模式下）

- **目标地址/状态 (Destination Address / State)**

  显示监视的目标地址以及连接状态。在"接口 > WLAN > 强制漫游"(Interfaces > WLAN > Force Roaming) 中组态目标地址。

  – not configured：未组态目标地址。

  – idle：组态不完整。

  – up:目标地址可访问。

  – down：目标地址不可访问。

- **IP 故障时强制漫游 (Force Roaming on IP down)**

  指示当前是否在执行漫游。

  – 未激活：未执行漫游。WLAN 接口无变化。

  – 激活：目标地址均不可访问。为了强制已登陆客户端/已连接接入点进入漫游状态，设备已禁用相应接口。

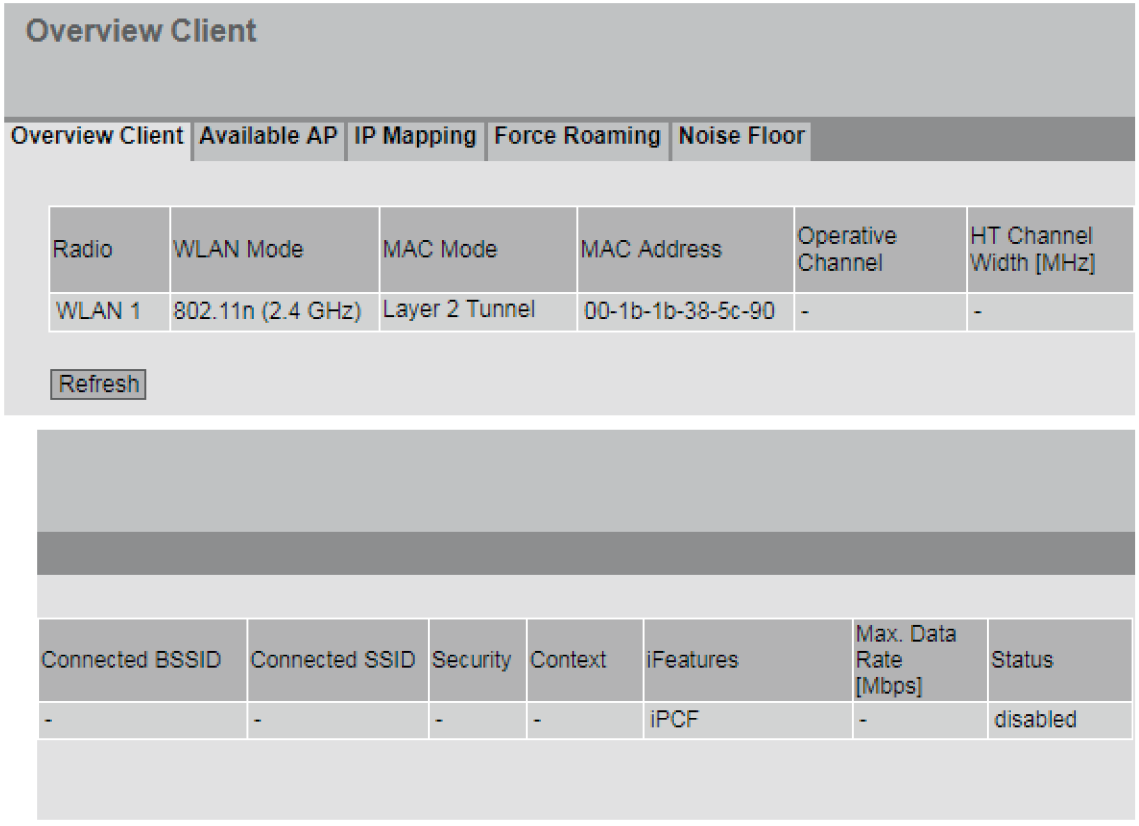
6.4.14.6 客户端概述

组态概述

说明

只有客户端或处于客户端模式下的接入点可使用此页面。

此页面显示现有客户端及其组态的概述。



说明

- **无线 (Radio)**

  显示可用的 WLAN 接口。

- **WLAN 模式 (WLAN Mode)**

  显示传输标准。

- **MAC 模式 (MAC Mode)**

  显示向接口分配 MAC 地址的方式。

  – 自动 (Automatic)

    客户端自动采用其通过以太网接口接收的第一帧的源 MAC 地址。

  – 手动 (Manual)

    手动输入地址。

  – 自身 (Own)

    客户端的 WLAN 接口使用以太网接口的 MAC 地址。

  – 第 2 层隧道 (Layer 2 Tunnel)

    客户端的 WLAN 接口使用以太网接口的 MAC 地址。同时也会将连接到客户端以太网接口的 MAC 地址通知给网络。最多可使用八个 MAC 地址。

- **MAC 地址 (MAC Address)**

  显示 WLAN 接口的 MAC 地址。

- **运行通道 (Operational channel)**

  显示与客户端相连接的接入点的通道。

- **HT 通道宽度 [MHz] (HT Channel Width [MHz])**

  显示通道带宽。

  – 20

    通道带宽为 20 MHz

  – 40up

    通道带宽为 40 MHz。使用组态的通道以及高于其带宽的相邻通道。

  – 40down

    通道带宽为 40 MHz。使用组态的通道以及低于其带宽的相邻通道。

  说明

  通道带宽 40 MHz 和频段 2.4 GHz

  如果接入点在组态的通道中或者在相邻的通道中检测到其它接入点，则原接入点会将通道带宽从 40 MHz 更改为 20 MHz。如果在接入点上设置"空闲"通道，则该接入点将使用 40 MHz 的通道带宽。

- **已连接的 BSSID (Connected BSSID)**

  显示与客户端相连的接入点的 MAC 地址。

- **已连接的 SSID (Connected BSSID)**

  显示与客户端相连接的接入点的 SSID。

- **Security**

  显示所采用的验证方法。

  – 如果采用的验证方法是"开放式系统 + 加密"(Open System + Encryption) 或 "Shared Key"，则这两种验证方法都会显示"已加密 (WEP/AES)"(Encrypted (WEP/AES))。

  – 如果启用了 iPCF、iPCF-HT 或 iPCF-MC 模式，则根据加密状态显示以下内容：

    iPCF 加密 (AES)：加密已启用。

    iPCF 验证：加密已禁用。

- **上下文 (Context)**
  显示使用的安全上下文。
- **iFeatures**
  显示使用哪些 iFeatures。
  - -
    不使用 iFeatures。
  - iPCF
  - iPCF-HT
  - iPCF-MC
  - iPRP
  - iREF
  - AeroScout
- **状态 (State)**
  显示 WLAN 接口的状态。
  - enabled
    WLAN 接口已启用。
  - disabled
    WLAN 接口已禁用。

6.4.14.7 可用 AP

可用接入点 (Available access points)

说明

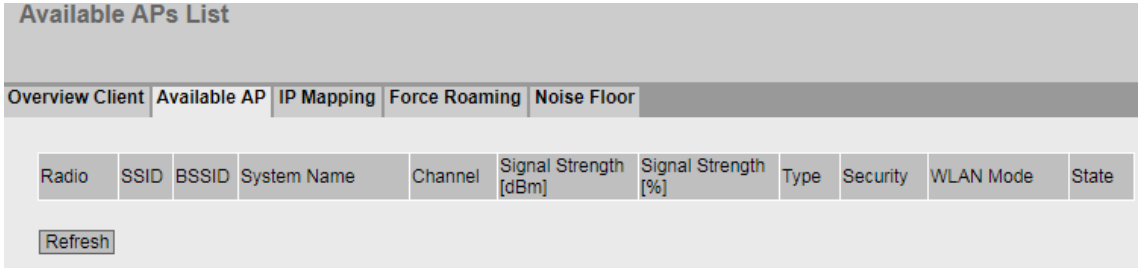
只有客户端或处于客户端模式下的接入点可使用此页面。

此页面显示对客户端可见的所有接入点。列表中还包括客户端因组态而无法连接的接入点。

说明

激活 iPCF 模式后的显示内容

如果通过 SCALANCE W700 激活 iPCF 模式，显示内容会有所不同。由于客户端在这种情况下不会运行后台扫描，因此仅会显示当前已经与客户端建立连接的接入点。



说明

该表包括以下列：

- **无线 (Radio)**

  显示对接入点可见的 WLAN 接口。

- **SSID**

  显示接入点的 SSID。

- **BSSID**

  显示接入点的 MAC 地址。

- **系统名称 (System Name)**

  显示接入点的系统名称。输入内容取决于接入点。不是所有接入点都支持这一参数。

- **通道 (Channel)**

  显示接入点传输或通信时所使用的通道。

- **信号强度 [dBm] (Signal Strength [dBm])**

  显示以 dBm 为单位的接入点信号强度。

- **信号强度 [%] (Signal strength [%])**

  显示接入点的信号强度百分比。

- **类型 (Type)**

  显示 WLAN 接口的模式。

- **安全性 (Security)**

  显示所采用的验证方法。

  – 如果采用的验证方法是"开放式系统 + 加密"(Open System + Encryption) 或 "Shared Key"，则这两种验证方法都会显示"已加密 (WEP/AES)"(Encrypted (WEP/AES))。

  – 如果在 WLAN 接口上启用了 iPCF、iPCF-HT 或 iPCF-MC 模式，则根据加密状态显示以下内容：

    iPCF 加密 (AES)：加密已启用。

    iPCF 验证：加密已禁用。

- **WLAN 模式 (WLAN Mode)**

  显示传输标准。如果激活了 DFS，则仅显示组态的传输标准"802.11a"或 "802.11n"，而不额外显示传输标准"802.11h"。

- **状态 (State)**

  显示接入点的状态，例如接入点是否可用。

6.4.14.8 IP 映射表

多台设备通过一台客户端访问 WLAN

说明

只有客户端或处于客户端模式下的接入点才可使用此 WBM 页面。

如果使用 IP 映射，则能够实现多台设备通过一台客户端访问 WLAN。这意味着不需要为每台设备都配备专用的 WLAN 客户端。IP 映射只有在连接的设备仅通过 IP 帧进行寻址时才可用。MAC 地址级别（ISO/OSI 第 2 层）的通信可以通过以下方式建立：

- 通过其 MAC 地址在客户端上进行组态的一个组件建立，
- 通过最多八个组件来建立（如果选择"第 2 层隧道"(Layer 2 Tunnel) 功能）。

对于客户端下游多台设备进行基于 MAC 地址的通信的工业应用而言，"第 2 层隧道"(Layer 2 Tunnel) 设置可满足要求。采用此设置的客户端无法连接标准 Wifi 接入点。

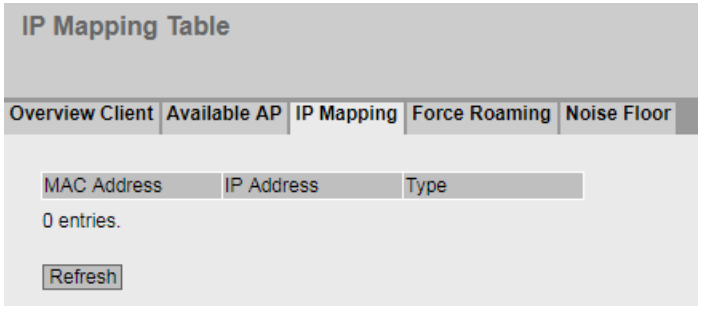
MAC 地址/IPv4 地址分配

客户端会维护一份 MAC 地址和 IPv4 地址分配表，以将入站的 IP 帧发送到正确的 MAC 地址。此 WBM 页面显示了该表。

说明

IP 映射表

如果为客户端组态"第 2 层隧道"(Layer 2 Tunnel)，则不会显示 IP 映射表。



MAC 模式

由客户端发送到接入点的 IP 帧始终将 WLAN 客户端的 MAC 地址作为源 MAC 地址。因此，在接入点的"学习表"中，只包含 WLAN 客户端的 MAC 地址。

如果客户端下游有其他设备，则不应启用"自动"(Automatic) 选项。在这种情况下，MAC 地址将无条件分配给通过以太网发送信号的第一台设备。如果接入点和客户端之间仅存在 IP 通信，则可以保留默认设置"自身"(Own)。如果基于 MAC 地址的帧还由客户端下游的设备发送，则需要选择设置"手动"(Manual)、"自动"(Automatic) 或者"第 2 层隧道"(Layer 2 Tunnel)。

描述

该表格包括以下列

- **MAC 地址 (MAC Address)**

  从接入点的角度来看位于 WLAN 客户端下游的设备的 MAC 地址。

- **IP 地址 (IP Address)**

  由 WLAN 客户端管理的此设备 IP 地址。

- **类型 (Type)**

  有两种类型可供选择：

  – system

    信息与 WLAN 客户端自身相关。

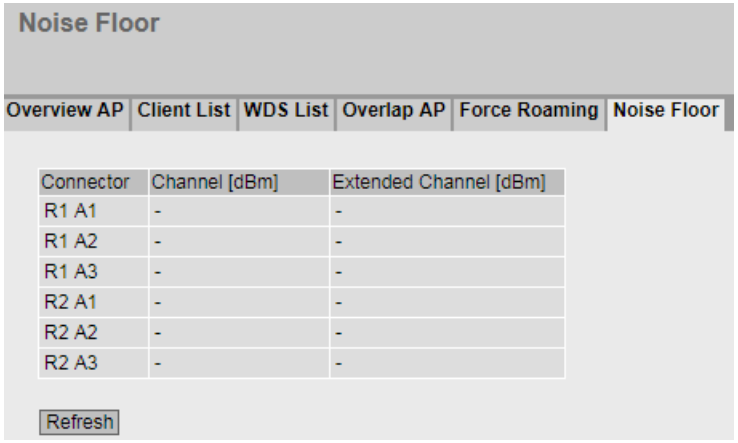
  – learned

    信息与 WLAN 客户端下游的设备相关。

6.4.14.9 背景噪声

说明

该 WBM 页面仅在接入点模式下可用。



该页面显示通道的背景噪声。

描述

- **连接器 (Connector)**

  显示相关天线连接器的名称。

- **通道 [dBm]** (Channel [dBm])

  显示设置通道的背景噪声。

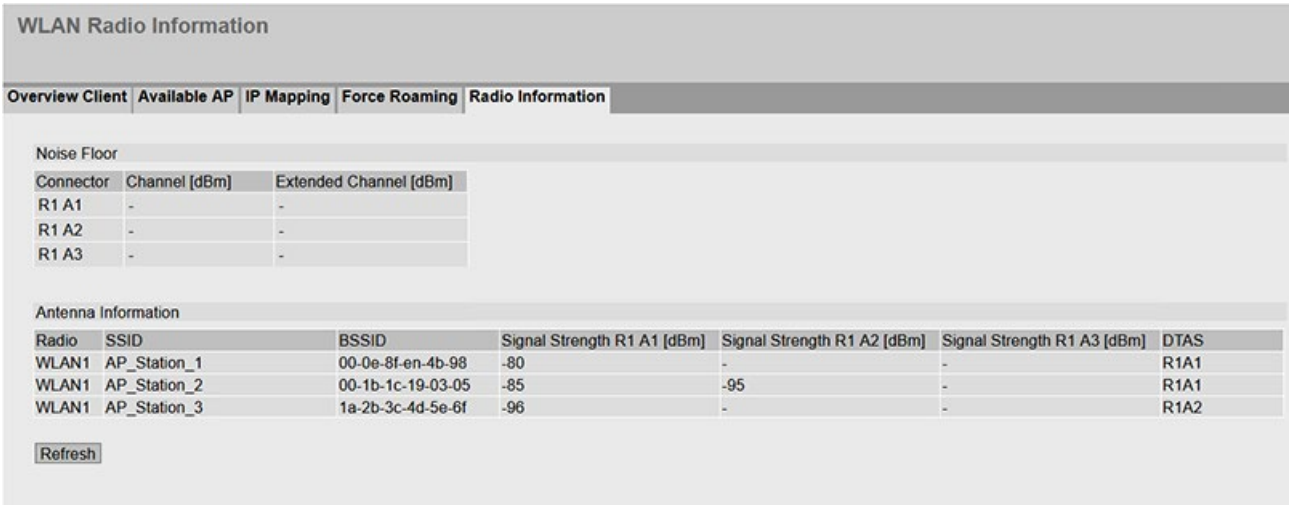
- **扩展通道 [dBm]** (Extended Channel [dBm])

  显示扩展通道 (HT-40) 的背景噪声。

6.4.14.10 无线电接口信息

说明

只有客户端或处于客户端模式下的接入点可使用此页面。



该页面包含有关通道和天线背景噪声的信息。

描述

"背景噪声"(Background noise) 表包含以下列：

- 连接器 (Connector)

  显示相关天线连接器的名称。

- 通道 [dBm] (Channel [dBm])

  显示设置通道的背景噪声。

- 扩展通道 [dBm] (Extended Channel [dBm])

  显示扩展通道 (HT-40) 的背景噪声。

"天线信息"(Antenna information) 表包含以下列：

- 无线电接口

  显示可用的 WLAN 接口。

- SSID

  显示接入点的网络名称。

- BSSID

  显示接入点的 MAC 地址。

- 信号强度 R1Ax

  显示每条天线的信号强度（单位为 dBm）。

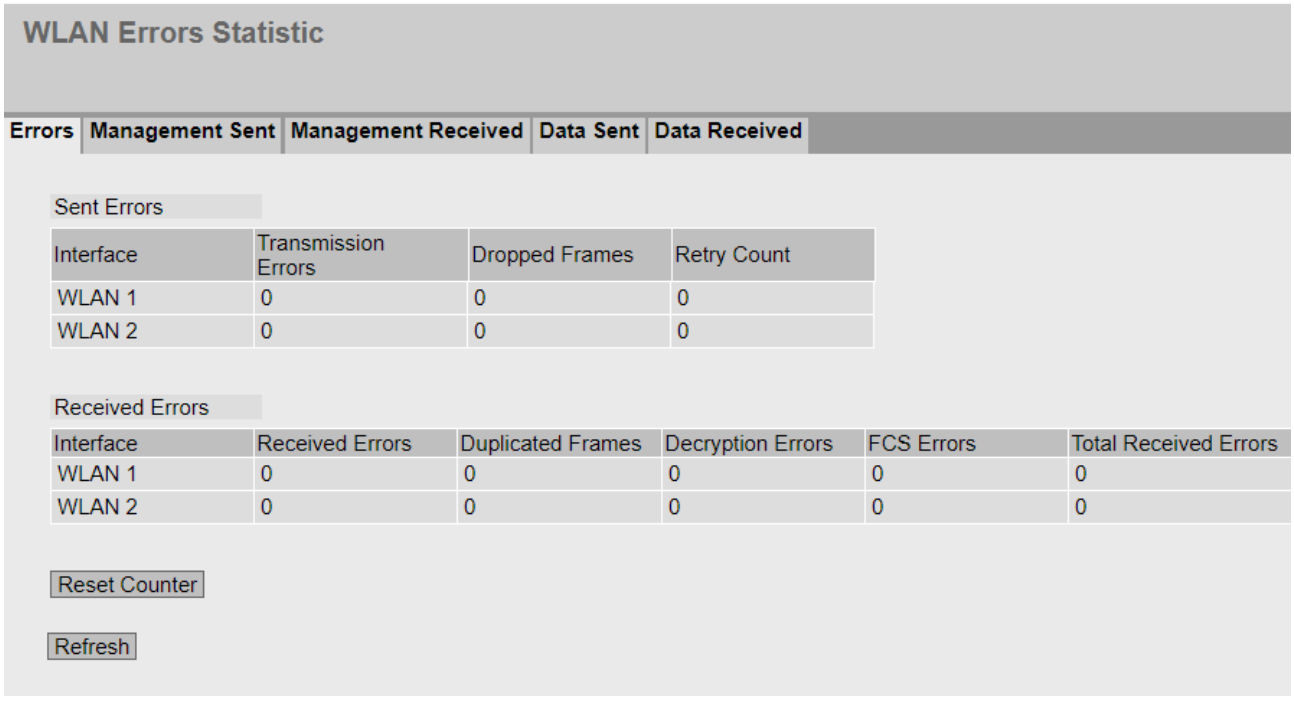
- DTAS

  显示当前使用的发射天线。

6.4.15 WLAN 统计信息

6.4.15.1 错误

WBM 页面显示每个 WLAN 接口已收发的错误帧数量。如果错误数增加，则应检查 WLAN 接口的设置、SCALANCE W 设备的安装及连接质量。



描述

"已发送错误"(Sent Errors) 表包含以下列：

- **接口 (Interface)**

  显示应用条目的 WLAN 接口。

- **错误类型**

  WLAN 接口之后的其他各列包括按照其错误类型分类的发送帧绝对数量。

  表中的列包含以下错误类型：

  – 传输错误 (Transmission Errors)

    显示已发送的错误帧的数量和百分比。

– 丢弃的帧 (Dropped Frames)

显示已丢弃的帧的数量和百分比。

重试过后仍无法成功发送帧。

尚未发送帧，但期间接收方已注销。

– 发送重试 (Send Retries)

显示需要一次或多次重试才成功发送的帧的数量和百分比。

"接收错误"(Receive Errors) 表包括以下列：

- **接口 (Interface)**

  显示应用条目的 WLAN 接口。

- **错误类型**

  WLAN 接口之后的其他各列包括按照其错误类型分类的接收帧绝对数量。
  表中的列包含以下错误类型：

  – 接收错误 (Receive errors)

  仅显示现有连接期间接收的错误帧的数量和百分比。

  – 重复帧 (Duplicated Frames)

  显示已接收两次的帧的数量和百分比。

  – 解密错误 (Decryption Errors)

  显示已错误加密的帧的数量和百分比。

  – FCS 错误 (FCS Errors

  显示校验和错误的帧的数量和百分比。

  – 接收错误总计 (Total receive errors)

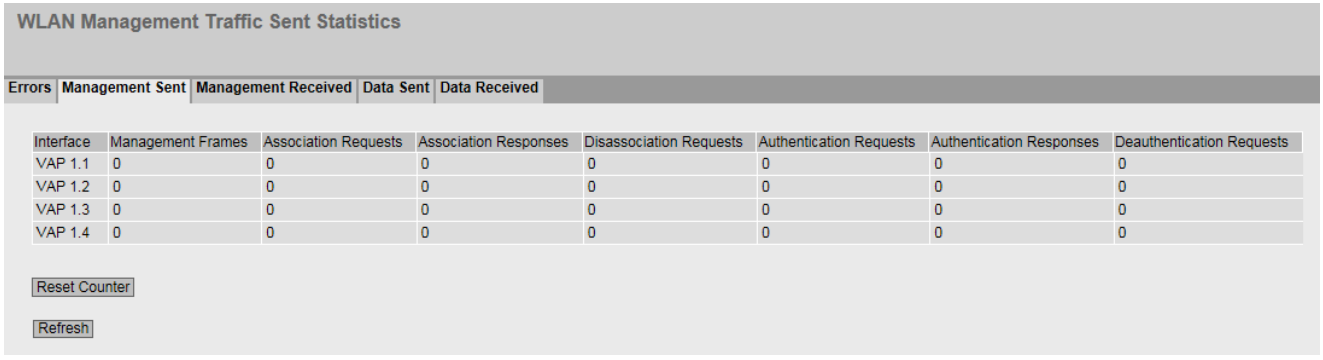
  显示已接收的全部错误帧的数量和百分比。

6.4.15.2 已发送管理帧

WBM 页面显示按每个接口计数的登录或注销响应帧数量。

说明

该 WBM 页面仅在接入点模式下可用。



描述

该表格包括以下列：

- **接口 (Interface)**

  显示应用条目的接口。

- **帧**

  – 管理帧 (Management Frames)

    显示管理帧数

  – 关联请求 (Association Requests)

    显示与登录相关的请求关联帧数。

  – 关联响应 (Association Responses)

    显示与登录相关的响应关联帧数。

  – 取消关联请求 (Disassociation Requests)

    显示与注销相关的请求取消关联帧数。

  – 验证请求 (Authentication Requests)

    显示与登录相关的请求验证帧数。

  – 验证响应 (Authentication Responses)

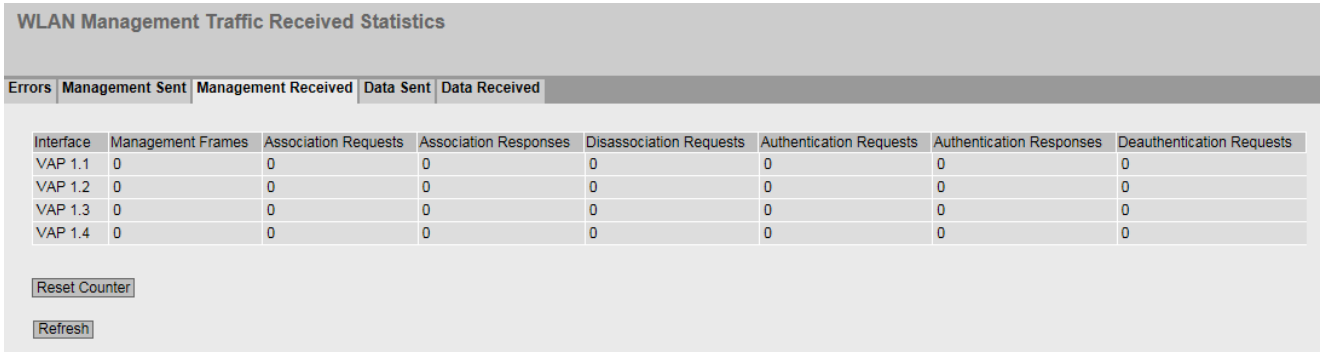
    显示与登录相关的响应验证帧数。

  – 取消验证请求 (Deauthentication Requests)

    显示与注销相关的取消验证帧数。

6.4.15.3 已接收管理帧

WBM 页面显示按每个接口计数的登录或注销响应帧数量。



描述

该表格包括以下列：

- **接口 (Interface)**

  显示应用条目的接口。

- **帧**

  – 管理帧 (Management Frames)

    显示管理帧数

  – 关联请求 (Association Requests)

    显示与登录相关的请求关联帧数。

  – 关联响应 (Association Responses)

    显示与登录相关的响应关联帧数。

  – 取消关联请求 (Disassociation Requests)

    显示与注销相关的请求取消关联帧数。

  – 验证请求 (Authentication Requests)

    显示与登录相关的请求验证帧数。

  – 验证响应 (Authentication Responses)

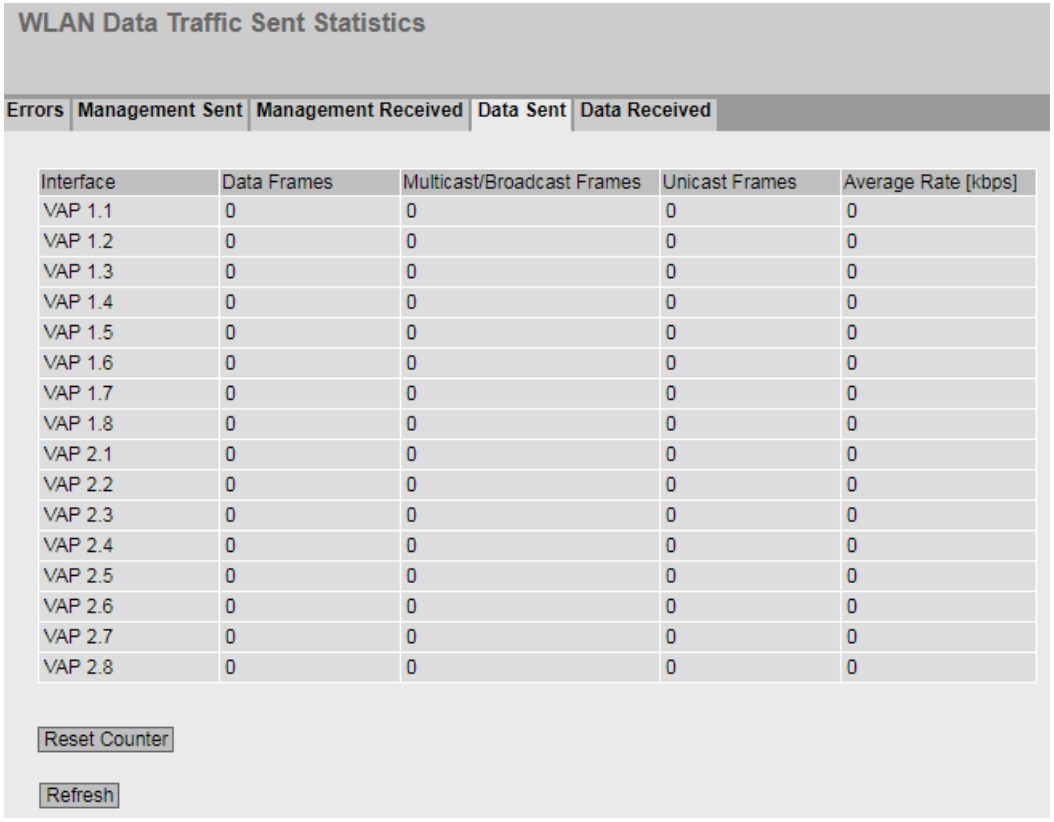
    显示与登录相关的响应验证帧数。

  – 取消验证请求 (Deauthentication Requests)

    显示与注销相关的取消验证帧数。

6.4.15.4 已发送数据

WBM 页面显示每个接口发送的帧数量。



描述

该表格包括以下列：

- **接口 (Interface)**

  显示应用条目的接口。

- **帧类型**

  接口之后的其他各列包括按照帧类型分类的发送帧绝对数量。

在该表的各列中，根据以下帧类型进行区分：

– 数据帧

  显示发送的数据帧数。

– 组播/广播帧 (Multicast/Broadcast Frames)

  显示已发送的组播帧和广播帧数。

– 单播帧 (Unicast Frames)

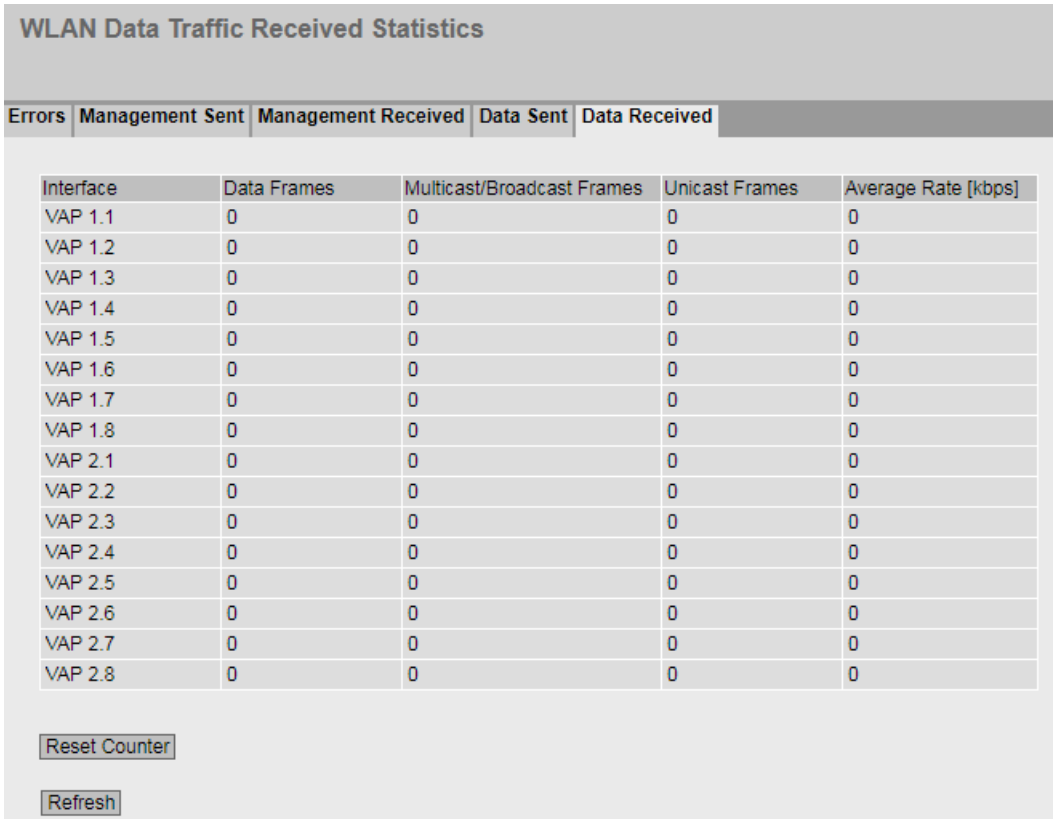
  显示已发送的单播帧数。

– 平均数据传输速率 (Average Data Rate)

  显示最后发送的数据帧的平均数据传输速率。

6.4.15.5 已接收数据

WBM 页面显示每个接口接收的帧数量。



描述

该表格包括以下列：

- **接口 (Interface)**

  显示应用条目的接口。

- **帧类型**

  接口之后的其他各列包括按照帧类型分类的接收帧绝对数量。

  在该表的各列中，根据以下帧类型进行区分：

  – 数据帧

    显示发送的数据帧数。

  – 组播/广播帧 (Multicast/Broadcast Frames)

    显示已发送的组播帧和广播帧数。

  – 单播帧 (Unicast Frames)

    显示已发送的单播帧数。

  – 平均数据传输速率 (Average Data Rate)

    显示最后发送的数据帧的平均数据传输速率。

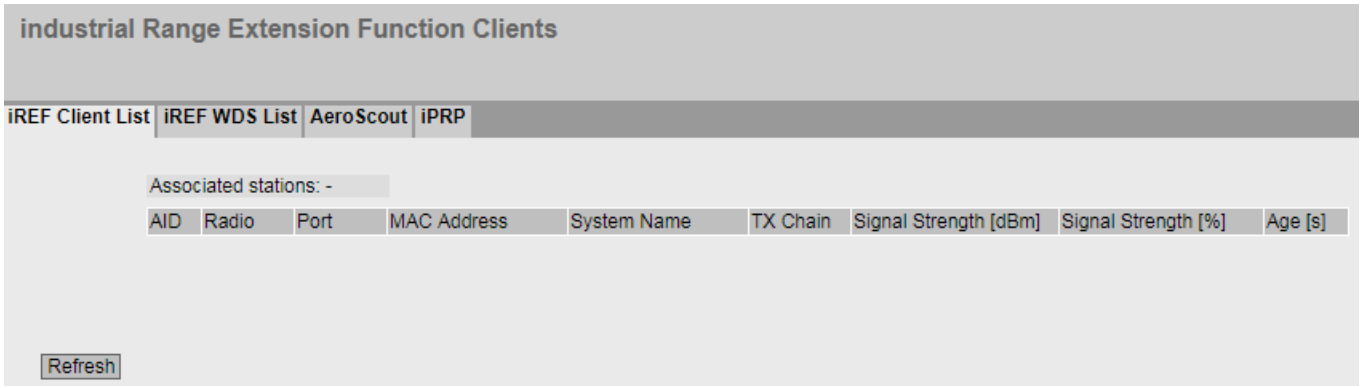
6.4.16 WLAN iFeatures

6.4.16.1 iREF 客户端列表

该 WBM 页面显示登录到接入点的客户端用来通信的天线连接器。也显示 WLAN 接口的信号强度和 MAC 地址等信息。

说明

- 该 WBM 页面仅在接入点模式下可用。
- 此 WBM 页面仅可通过以下 KEY-PLUG 组态：
  – 接入点：W780 iFeatures (MLFB 6GK5 907-8PA00)



说明

该页面包含以下框：

- **登录的客户端 (Logged-on Clients)**

  显示登录到接入点的客户端的数量

该表包括以下列：

- **AID** (Associated ID)

  显示客户端的连接 ID。如果客户端通过 VAP 接口与接入点相连，则为该客户端分配一个连接 ID。此连接 ID 在 VAP 接口内是唯一的。如果两个客户端在不同的 VAP 接口登录，则两个客户端都可接收同样的 ID。

- **无线 (Radio)**

  显示可用的 WLAN 接口。

- **端口 (Port)**

  显示 VAP 接口。

- **MAC 地址 (MAC address)**

  显示客户端的 MAC 地址。

- **系统名称 (System Name)**

  如果客户端将其系统名称告知接入点，则将显示客户端的系统名称。不是所有客户端都支持此参数。

- **Tx Chain**

  显示客户端与接入点进行通信时所使用的天线连接器。

- **信号强度 [dBm] (Signal Strength [dBm])**

  显示所连接客户端的信号强度（单位：分贝毫瓦）。

- **信号强度 [%] (Signal strength [%])**

  显示所连接客户端的信号强度百分数。

- **Age [s]**

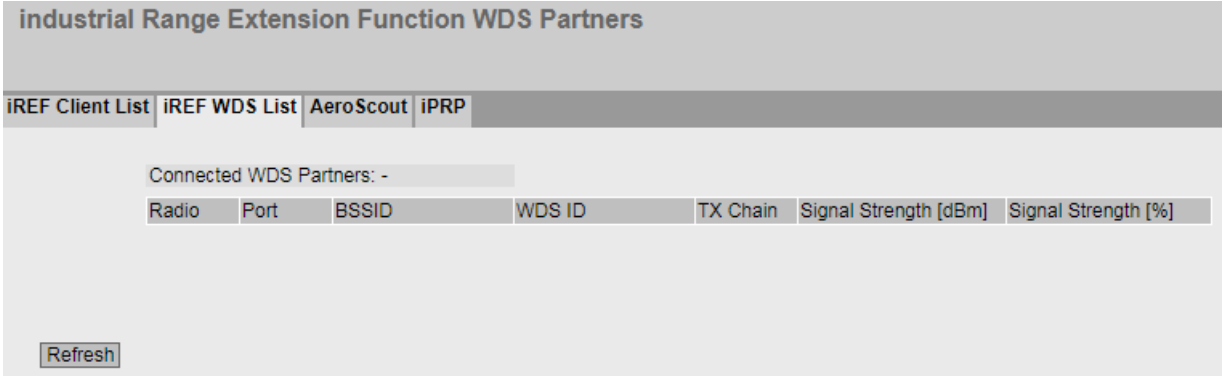
- 显示所列客户端的老化时间。

6.4.16.2 iREF WDS 列表

该 WBM 页面显示通过 WDS 链路登录到接入点的接入点。此页面也显示所使用的天线和 WLAN 接口的信号强度等信息。

说明

- 该 WBM 页面仅在接入点模式下可用。
- 此 WBM 页面仅可通过以下 KEY-PLUG 组态：
  – 接入点：W780 iFeatures (MLFB 6GK5 907-8PA00)



说明

该页面包含以下框：

- **已连接的 WDS 伙伴 (Connected WDS partners)**

  显示登录到接入点的接入点数量

该表格包括以下列：

- **无线 (Radio)**

  显示可用的 WLAN 接口。

- **端口 (Port)**

  显示 WDS 接口。

- **BSSID**

  显示 WDS 伙伴的 MAC 地址。

- **WDS ID**

  显示 WDS 伙伴的名称。

- **Tx Chain**

  显示两个接入点相互通信时所使用的天线连接器。

- **信号强度 [dBm] (Signal Strength [dBm])**

  显示所连接接入点的信号强度（单位：分贝毫瓦）。

- **信号强度 [%] (Signal strength [%])**

  显示所连接接入点的信号强度百分比。

6.4.16.3 AeroScout

此页面显示有关转发 AeroScout 帧的信息。

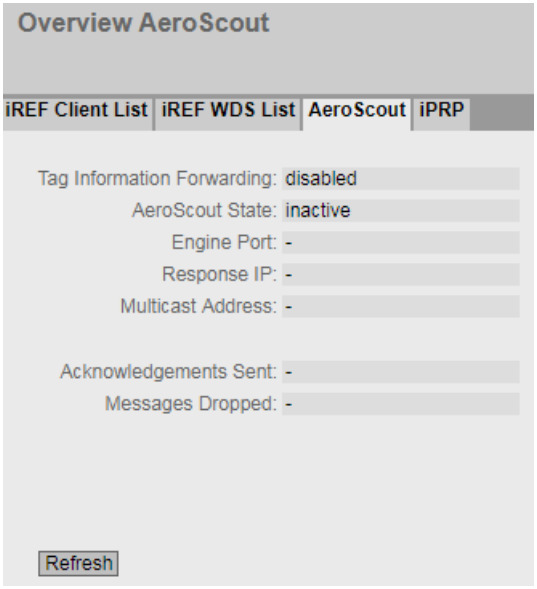
说明

- 该 WBM 页面仅在接入点模式下可用。
- 此 WBM 页面仅可通过以下 KEY-PLUG 组态：
  访问点：W780 iFeatures (MLFB 6GK5 907-8PA00)

说明

AeroScout 功能无法与其它 iFeatures（iPCF、iPCF-MC,、iREF）搭配使用。根据 IEEE 802.11g、IEEE 802.11n 和 IEEE 802.11n-only 标准，AeroScout 仅可在 2.4 GHz 频段使用。

有关详细信息，请参见 AeroScout 公司 (www.aeroscout.com) 的文档。



说明

- **变量信息转发 (Tag Information Forwarding)**

  在评估 AeroScout 帧的管理程序中，可指定 SCALANCE W700 设备是否转发帧。在此处可查看在管理程序中进行了哪项设置。

  说明

  通过适当的组态，SCALANCE W700 可转发 AeroScout 帧，但自身不会对其进行处理或评估。这只能在"AeroScout System Manager"程序中完成。

- **AeroScout 状态 (AeroScout status)**

  显示 AeroScout 是处于启用状态还是禁用状态。

- **引擎端口 (Engine Port)**

  SCALANCE W700 设备在端口 1144 处等待管理程序发出的 UDP 包。

- **响应 IP (Response IP)**

  运行评估 AeroScout 帧的管理程序的计算机 IP 地址。

- **组播地址 (Multicast address)**

  变量以组播形式发送帧。该组播地址在管理程序中进行组态，并在此处显示。

- **已发送确认 (Acknowledgements sent)**

  SCALANCE W700 设备向管理程序发送的确认数目（由于循环查询或在管理程序（UDP 数据包）中手动更改了组态）。

- **丢弃的消息 (Messages dropped)**

  未转发的帧数。例如，如果将 AeroScout 变量组态为在通道 1 上发送，则 SCALANCE W700 设备不会转发在通道 6 上接收到的帧。

6.4.16.4 iPRP

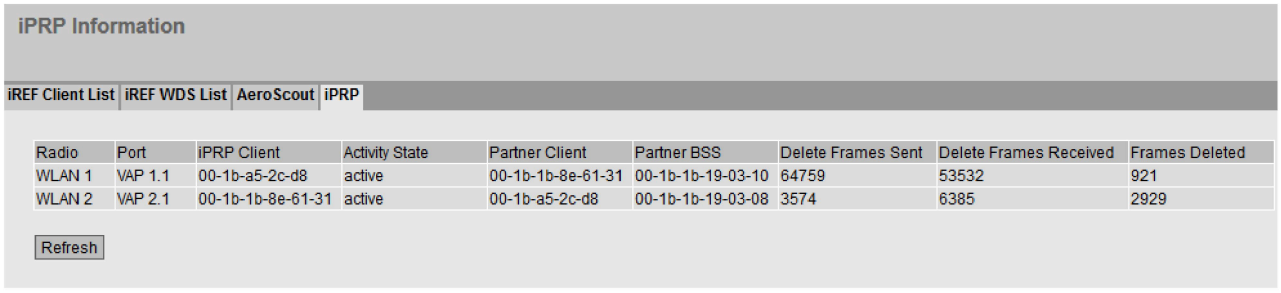
在此 WBM 页面中可以检查 iPRP 的设置是否正确。例如，您可以查看哪个设备是伙伴客户端。

说明

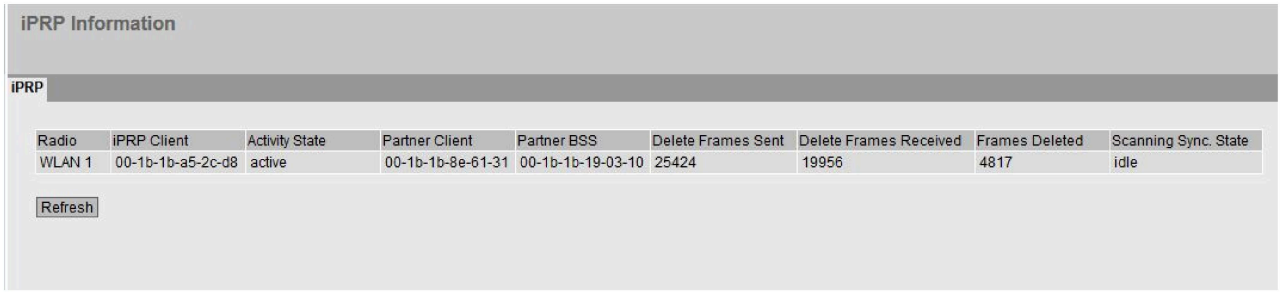
此 WBM 页面仅可通过以下 KEY-PLUG 组态：

- 接入点：W780 iFeatures (MLFB 6GK5 907-8PA00)
- 客户端：W740 iFeatures (MLFB 6GK5 907-4PA00)

Display in access point mode



Display in client mode



说明

该表包括以下列：

- **无线 (Radio)**

  显示客户端与接入点相连所用的 WLAN 接口

- **端口 (Port)**（仅限接入点模式）

  显示登录 iPRP 客户端所用的 VAP 接口。

- **iPRP 客户端 (iPRP Client)**

  显示 iPRP 客户端的 MAC 地址。

- **激活状态 (ActivationState)**

  显示是否已启用 iPRP。

- **伙伴客户端 (Partner Client)**

  显示伙伴客户端的 MAC 地址。

- **伙伴 BSS (Partner BSS)**

  显示与伙伴客户端相连的接入点的 MAC 地址。

- **已发送删除帧 (Delete Frames Sent)**

  显示设备（接入点/客户端）已发送至其伙伴设备的 iPRP 删除帧的数目。

- **已接收删除帧 (Delete Frames Received)**

  显示设备（接入点/客户端）已从其伙伴设备接收到的 iPRP 删除帧的数目。

- **已删除帧 (Frames Deleted)**

  显示由于 iPRP 删除帧而从队列中删除的尚未发送的帧的数目。

- **扫描同步状态 (Scanning Sync State)**（仅限客户端模式）

  两个客户端不会在彼此同步的同时搜索接入点和切换到扫描模式。

  同步过程具有以下状态：

  – idle：空闲，无扫描

  – requested：向伙伴客户端询问是否可以扫描。

  – pending：允许扫描。等待开始扫描，然后切换到状态"foreground"或"background"。

  – background：执行后台扫描。

  – foreground：例如，客户端刚刚启动并正在运行前台扫描。

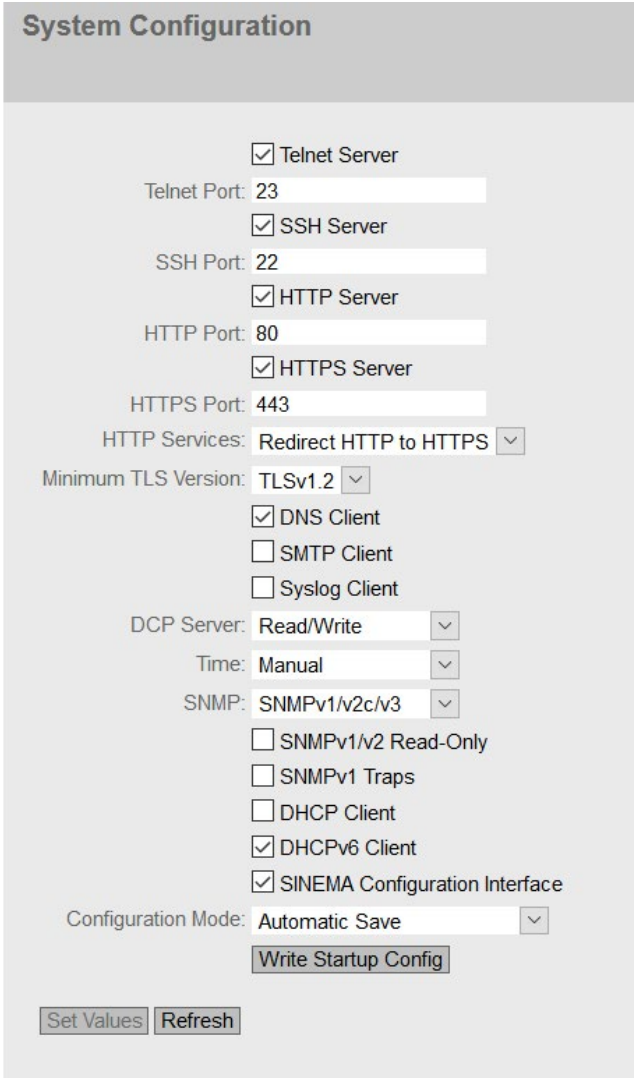
6.5 "System"菜单

6.5.1 组态

系统组态

该 WBM 页面包含设备访问选项的组态概览。

指定用于访问设备的服务。对于某些服务提供了更多组态页面，可在其中进行更加具体的设置。



描述

该页面包含以下框：

- **Telnet 服务器 (Telnet Server)**

  启用或禁用"Telnet 服务器"(Telnet Server) 服务，以便不加密访问 CLI。

- **Telnet 端口 (Telnet Port)**

  指定对 CLI 进行 Telnet 访问的端口。

- **SSH 服务器 (SSH Server)**

  启用或禁用"SSH 服务器"(SSH Server) 服务，以便加密访问 CLI。

- **SSH 端口 (SSH Port)**

  指定对 CLI 进行 SSH 访问的端口

- **HTTP 服务器 (HTTP Server)**

  启用或禁用对 WBM 的 HTTP 访问。

- **HTTP 端口 (HTTP Port)**

  指定对 WBM 进行 HTTP 访问的端口。

- **HTTPS 服务器 (HTTPS Server)**

  启用或禁用对 WBM 的 HTTPS 访问。

- **HTTPS 端口 (HTTPS Port)**

  启用或禁止使用 HTTPS 进行访问。

- **HTTP 服务 (HTTP Services)**

  指定 WBM 的访问方式：

  – HTTPS

    只能通过 HTTPS 访问 WBM。

  – HTTP/HTTPS

    可以通过 HTTP 和 HTTPS 访问 WBM。

  – 将 HTTP 重定向到 HTTPS

    通过 HTTP 的访问自动转移到 HTTPS。

- **最低 TLS 版本**

  指定将使用的最低 TLS 版本。

- **DNS 客户端 (DNS Client)**

  启用或禁用 DNS 客户端。可以在"系统 > DNS"(System > DNS) 中组态其他设置。

- **SMTP 客户端 (SMTP Client)**

  启用或禁用 SMTP 客户端。可以在"系统 > SMTP 客户端"(System > SMTP Client) 中组态其他设置。

- **Syslog 客户端 (Syslog Client)**

  启用或禁用 Syslog 客户端。可以在"系统 > Syslog 客户端"(System > Syslog Client) 中组态其他设置。

- **DCP 服务器 (DCP Server)**

  指定是否可用 DCP（发现和组态协议）访问设备：

  – "-"（已禁用）

    DCP 已禁用。既不能读取也不能修改设备参数。

  – 读/写 (Read/Write)

    借助 DCP，既可以读取设备参数又可以对其进行修改。

  – 只读 (Read Only)

    借助 DCP，可以读取设备参数，但不能对其进行修改。

- **时间 (Time)**

  从下拉列表中选择设置。可能的设置如下：

  – 手动 (Manual)

    手动设置系统时间。可以在"系统 > 系统时间 > 手动设置"(System > System Time > Manual Setting) 中组态其他设置。

  – SIMATIC Time

    通过 SIMATIC 时间发送器设置系统时间。可以在"系统 > 系统时间 > SIMATIC 时间客户端"(System > System Time > SIMATIC Time Client) 中组态其他设置。

  – SNTP 客户端 (SNTP Client)

    通过 SNTP 服务器设置系统时间。可以在"系统 > 系统时间 > SNTP 客户端"(System > System Time > SNTP Client) 中组态其他设置。

  – NTP 客户端 (NTP Client)

    通过 NTP 服务器设置系统时间。可以在"系统 > 系统时间 > NTP 客户端"(System > System Time > NTP Client) 中组态其他设置。

- **SNMP**

  从下拉列表中选择协议。可能的设置如下：

  – "-"（SNMP 已禁用）
    不能通过 SNMP 访问设备参数。

  – SNMPv1/v2c/v3
    可以通过 SNMP 版本 1、2c 或 3 访问设备参数。可以在"系统 > SNMP > 常规"(System > SNMP > General) 中组态其他设置。

  – SNMPv3
    只可通过 SNMP 版本 3 访问设备参数。可以在"系统 > SNMP > 常规"(System > SNMP > General) 中组态其他设置。

- **SNMPv1/v2 只读 (SNMPv1/v2 Read-Only)**

  启用或禁用通过 SNMPv1/v2c 对 SNMP 变量进行写访问。

- **SNMPv1 陷阱 (SNMPv1 Traps)**

  启用或禁用发送陷阱（报警帧）。可以在"系统 > SNMP > 陷阱"(System > SNMP > Traps) 中组态其他设置。

- **DHCP 客户端 (DHCP Client)**

  启用或禁用 DHCP 客户端。可以在"系统 > DHCP"(System > DHCP) 中组态其他设置。

- **DHCPv6 客户端** (DHCPv6 Client)

  启用或禁用 DHCPv6 客户端。

- **SINEMA 组态接口 (SINEMA configuration interface)**

  如果启用了 SINEMA 组态接口，可通过 TIA Portal 将组态下载到设备中。

- **组态模式 (Configuration Mode)**

  从下拉列表中选择模式。可能的模式如下：

  – 自动保存 (Automatic Save)
    自动备份模式。在最后修改参数的约 1 分钟后或重启设备时，自动保存组态。

此外，显示区域中将出现如下消息"将在 x 秒内自动保存更改。按下'写入启动组态'可立即保存"(Changes will be saved automatically in x seconds. Press 'Write Startup Config' to save immediately)。

说明

中断保存

只有消息中的定时器到期后，才会启动保存。保存所需的时间取决于设备。
保存过程中将显示如下消息："正在保存组态数据。请勿关闭设备"(Saving configuration data in progress. Please do not switch off the device)。

- 不要在定时器到期后立即关闭设备。

– Trial

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

要将更改保存在组态文件中，请使用"写入启动组态"(Write startup config) 按钮。设置了试用模式时会显示"写入启动组态"(Write startup config) 按钮。此外，只要存在未保存的更改内容，每次更改参数后，就都会在显示区域显示以下消息："试用模式已激活 - 请按'写入启动组态'按钮保存设置"(Trial Mode Active – Press "Write Startup Config" button to make your settings persistent)。可以在每个 WBM 页面上看到这条消息，直至所做的更改已保存或设备已重启。

步骤

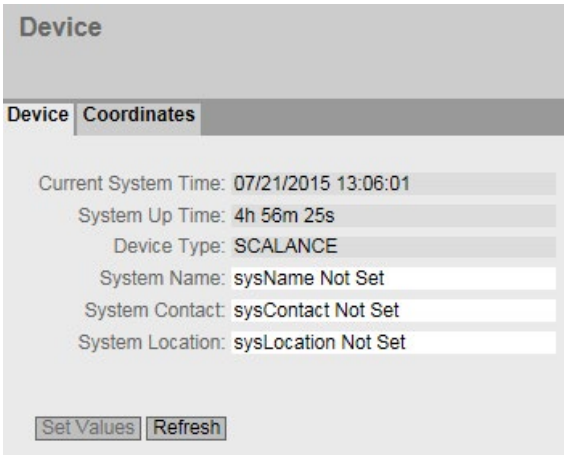
1. 要使用所需功能，请选中相应的复选框。
2. 从下拉列表中选择所需选项。
3. 单击"设置值"(Set Values) 按钮。

6.5.2 常规

6.5.2.1 设备

常规设备信息

该页面包含常规设备信息。



无法更改"当前系统时间"(Current System Time)、"系统运行时间"(System Up Time)和"设备类型"(Device Type) 框。

说明

该页面包含以下框：

- **Current System Time**
  显示当前系统时间。系统时间由用户或时钟帧设置：即 SINEC H1 时钟帧、NTP 或 SNTP。（只读）
- **System Up Time**
  显示设备自上次重启以来的运行时间。（只读）
- **Device Type**
  显示设备的型号标识。（只读）
- **System Name**
  可在此框中输入设备的名称。输入的名称显示在选择区域中。最多支持 255 个字

符。

系统名称还显示在 CLI 输入提示中。CLI 输入提示中的字符数是有限的。系统名称前 16 个字符后面的部分将被截断。

- **System Contact**

  可输入设备管理责任人的名字。最多支持 255 个字符。

- **System Location**

  可输入设备的安装位置。输入的安装位置显示在选择区域中。最多支持 255 个字符。

说明

输入框中使用 ASCII 码 0x20 至 0x7e。

步骤

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

6.5.2.2 坐标

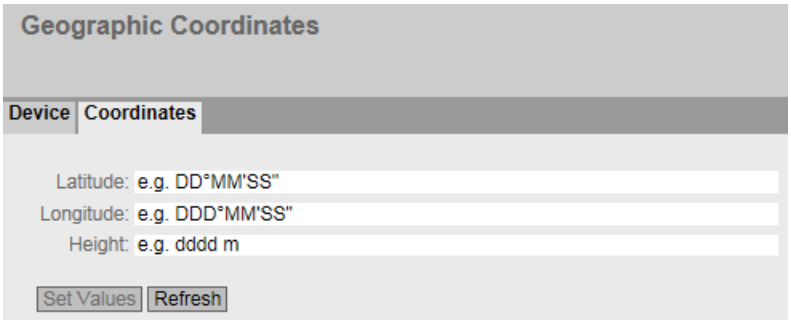
有关地理坐标的信息

在"地理坐标"(Geographic Coordinates) 窗口中，可以输入地理坐标的相关信息。可以在"地理坐标"(Geographic Coordinates) 窗口的输入框中直接输入地理坐标的参数（符合 WGS84 的椭球面纬度、经度和高度）。

获取坐标

使用适当的地图来获取设备的地理坐标。

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



说明

该页包含以下输入框，这些输入框最多可包含 32 个字符。

- **"Latitude"输入框**

  地理纬度：在此输入设备位置的北纬值或南纬值。

  例如，值 +49° 1´31.67" 表示设备位于北纬 49 度、1 弧分和 31.67 弧秒。

  通过在前面加上负号显示南纬度。

  还可以在数字信息后面附加字母 N（北纬）或 S（南纬），如 49° 1´31.67" N。

- **"Longitude"输入框**

  地理经度：在此输入设备位置的东经或西经值。

  +8° 20´58.73" 表示设备位于东经 8 度、20 分和 58.73 秒。

  通过在经度前面加上负号表示西经。

  还可以在数字信息前面加上字母 E（东经）或 W（西经），如 8° 20´58.73" E。

- **输入框："Height"**

  在此输入地理海拔高度的米数值。

  例如，158 m 表示设备位于海平面上 158 m 高的位置。

  对于低于海平面的高度（例如死海），可在前面添加负号来进行表示。

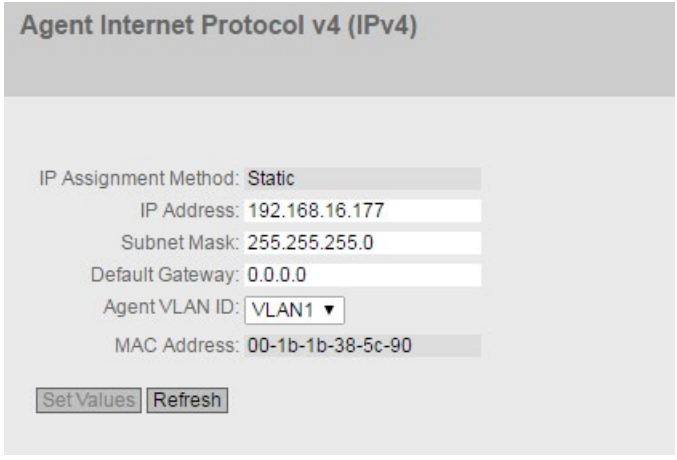
步骤

1. 在"Latitude"输入框中输入计算得出的纬度。
2. 在"Longitude"输入框中输入计算得出的经度。
3. 在"Height"输入框中输入海拔高度。
4. 单击"Set Values"按钮。

6.5.3 Agent IPv4

组态 IP 地址

在此 WBM 页面上，可组态设备的 IPv4 地址。



说明

该页面包含以下框：

- **IP 分配方法 (IP Assgn. Method)**
- 显示 IPv4 地址的分配方法。
  - 静态 (Static)
    IPv4 地址是静态的。在"IP 地址"(IP Address) 和"子网掩码"(Subnet Mask) 输入框中输入 IP 设置。
  - 动态 (DHCP) (Dynamic (DHCP))
    设备从 DHCP 服务器获取动态 IPv4 地址。
- **IP 地址 (IP Address)**

  输入设备的 IPv4 地址。
  单击"设置值"(Set Values) 按钮后，此 IPv4 地址也将显示在 Web 浏览器的地址栏中。如果未自动显示，则需要手动在 Web 浏览器的地址栏中输入该 IPv4 地址。
- **子网掩码 (Subnet Mask)**

  输入设备的子网掩码。
- **默认网关 (Default Gateway)**

  输入默认网关的 IPv4 地址，以便可以与其它子网内的设备（如诊断站、电子邮件服务器）进行通信。

- **代理 VLAN ID (Agent VLAN ID)**

  从下拉列表中选择 VLAN ID。只有将"基础网桥模式"(Base Bridge Mode) 参数设置为"802.1 Q VLAN Bridge"时才可使用该下拉列表。在"第 2 层 > VLAN > 常规"(Layer 2 > VLAN > General) 中组态该参数。只可以选择已组态的 VLAN。

  说明

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

- **MAC 地址 (MAC Address)**

  显示设备的 MAC 地址。MAC 地址链接到了硬件，无法修改。

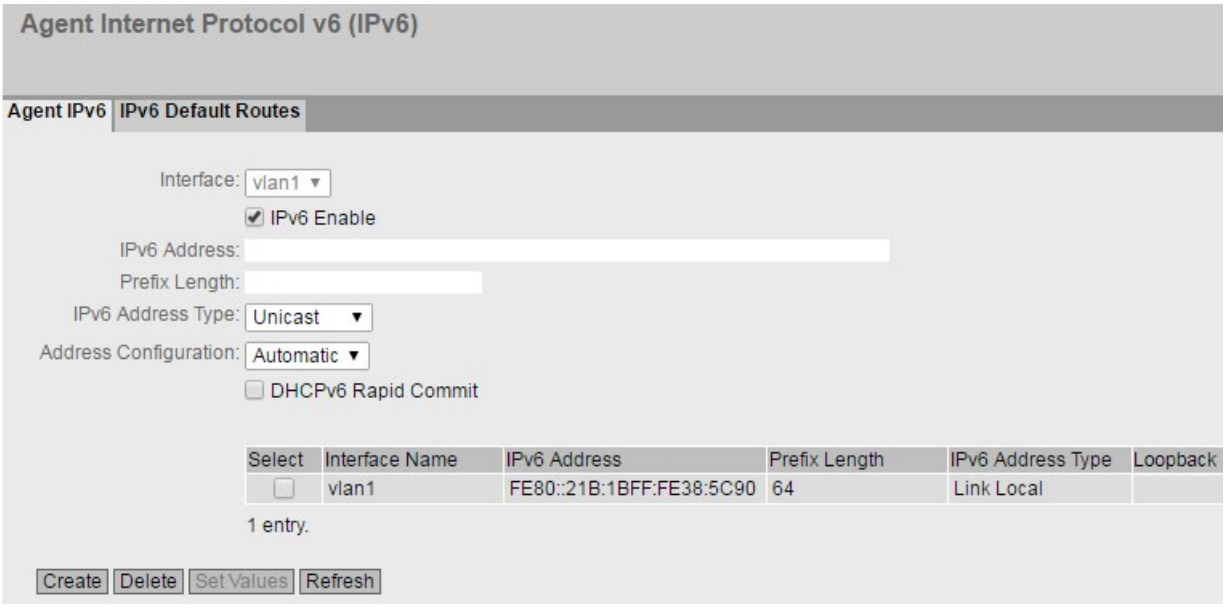
步骤

1. 在输入框中输入 IP 地址、子网掩码和默认网关。
2. 从"代理 VLAN ID"(Agent VLAN ID) 下拉列表中选择分配的 VLAN ID。如果无法启用该下拉列表，请检查是否将"基础网桥模式"(Base Bridge Mode) 参数设置为"802.1 Q VLAN Bridge"。在"第 2 层 > VLAN > 常规"(Layer 2 > VLAN > General) 中组态该参数。
3. 单击"设置值"(Set Values) 按钮。

6.5.4 代理 IPv6

组态 IP 地址

在此页面上，可启用管理 VAN 上的 IPv6。此 VLAN 接口还被称为 IPv6 接口。IPv6 接口可以具备多个 IPv6 地址。



描述

该页面包含以下内容：

- **接口 (Interface)**

  显示要启用其 IPv6 的 VLAN 接口。

- **启用 IPv6 (IPv6 Enable)**

  启用或禁用接口上的 IPv6。启用并接受该设置后，会自动创建链路本地地址。

- **IPv6 地址** (IPv6 Address)

  输入 IPv6 地址。输入内容取决于所选地址类型。

- **前缀长度** (Prefix Length)

  输入属于前缀的左侧位数

- **IPv6 地址类型** (IPv6 Address Type)

  选择地址类型:

  – 单播 (Unicast)

  – 链路本地 (Link Local)：IPv6 地址仅对该链路有效。

- **地址组态** (Address Configuration)

  指定地址组态机制:

  – 自动（默认）
  使用无状态机制或有状态机制创建 IPv6 地址。

  – DHCPv6

  与状态相关：从 DHCPv6 服务器中获取 IPv6 地址和组态文件。

  – SLAAC（无状态地址自动组态）

  采用 NDP（邻居发现协议）的无状态自动组态

  – 静态

  输入静态 IPv6 地址。

- **DHCPv6 快速提交 (DHCPv6 Rapid Commit)**

  启用了 IPv6 程序后，将缩短地址分配。仅使用 2 条 DHCPv6 消息（SOLICIT 和 REPLY），而不是 4 条 DHCPv6 消息（SOLICIT、ADVERTISE、REQUEST 和 REPLY）。有关消息的更多信息，请参见 RFC 3315。

该表格包括以下列:

- **选择 (Select)**

  选中要删除的行中的复选框。

- **接口名称** (Interface Name)

  显示 VLAN 接口的名称。

- **IPv6 地址** (IPv6 Address)

  显示 IPv6 地址。

- **前缀长度** (Prefix Length)

  显示前缀长度。

- **IPv6 地址类型** (IPv6 Address Type)

  显示地址类型。可能的值包括：

  – 单播 (Unicast)

  – 链路本地 (Link Local)

- **回送 (Loopback)**
  显示是否已启用"回送"(loopback) 属性。

步骤

自动形成链接本地地址

1. 启用 IPv6。
2. 单击"创建"(Create) 按钮。在表格中，创建并自动形成了带有接口的条目，并显示了链路本地 IPv6 地址。

分配链路本地地址

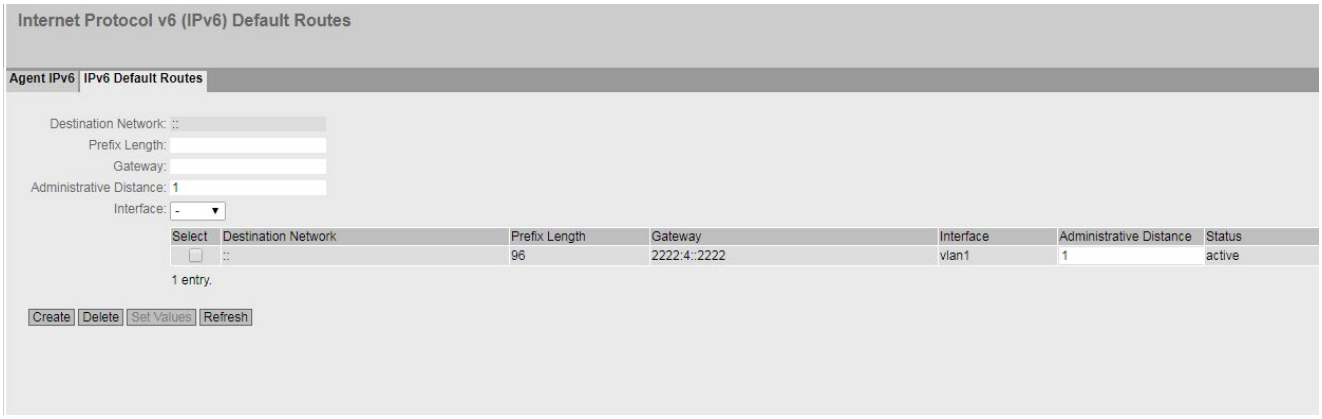
1. 启用 IPv6。
2. 在"IPv6 地址"(IPv6 Address) 中输入链路本地地址，例如：
   FE80::21B:1BFF:FE40:9155
3. 在"前缀长度"(Prefix Length) 中输入"128"。
4. 对于"IPv6 地址类型"(IPv6 Address Type)，选择条目"链路本地"(Link Local)。
5. 对于"地址组态"(Address Configuration)，选择条目"静态"(Static)。
6. 单击"创建"(Create) 按钮。在表格中，创建了带有接口的条目，并显示了 IPv6 地址。

   将覆盖自动创建的本地地址。

6.5.4.1 IPv6 默认路由

可以在本页组态 IPv6 的默认路由。IPv6 默认路由是适用于所有 IPv6 地址的 IPv6 路由。设备仅需了解默认网关，并向其发送所有 IPv6 数据包。

默认网关了解其本身的所有路由，或者具有至其它默认网关的默认路由。



说明

该页面包含以下内容：

- **Destination Network**

  目标网络（::或者 0:0:0:0:0:0:0:0:0:0:0:0:0:0:0:0）适用于所有 IPv6 地址。

- **Prefix Length**

  输入属于前缀的左侧位数

- **Gateway**

  输入要向其发送 IPv6 数据包的网关的 IPv6 地址。

- **管理距离**

  输入路由的度量。度量对应于基于速度或成本等参数的连接质量。如果存在多条等效路由，则会使用度量值最小的路由。
  值范围：1 - 254

- **Interface**

  指定用于获取目标的网络地址的接口。

该表包含以下各列：

- **Select**

  选中要删除的行中的复选框。

- **Destination Network**

  显示目标的网络地址。

- **Prefix Length**

  显示前缀长度。

- **Gateway**

  显示下一个网关的 IPv6 地址。

- **Interface**

  显示路由的接口。

- **管理距离**

  输入路由的度量。创建路由时，会自动输入"not used"。度量对应于基于速度或成本等参数的连接质量。如果存在多条等效路由，则会使用度量值最小的路由。
  值范围：1 - 254

- **状态 (Status)**

  显示路由是否激活。

组态步骤

1. 输入前缀长度。
2. 输入网关的 IPv6 地址。
3. 选择所需接口。
4. 输入路由的度量。

5. 单击"创建"(Create) 按钮。会在表中生成一个新条目。

6. 单击"设置值"(Set Values) 按钮。

6.5.5 DNS

在该页面，可通过 IPv4 或 IPv6 地址手动组态最多 3 个 DNS 服务器。为手动组态的各 DNS 服务器分配索引 1 到 3。设备可通过 DHCP 学习 2 个带 IPv4 地址的 DNS 服务器。对已学习的 DNS 服务器自动分配索引 4 到 7。

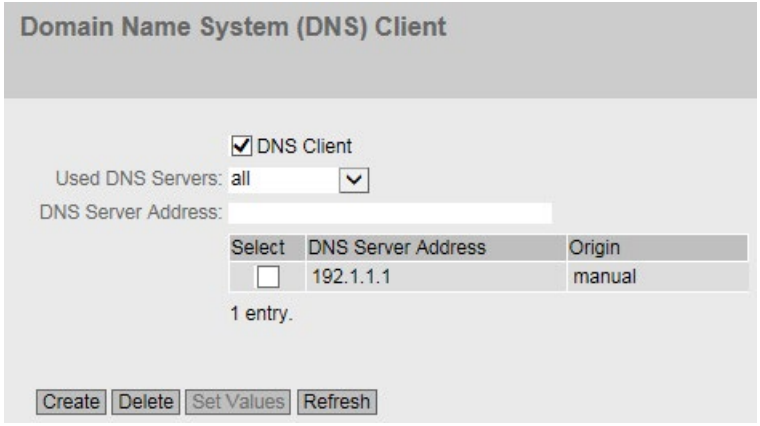
如果有多个 DNS 服务器，则表中的顺序可以指定服务器的查询顺序。最上面的服务器最先查询。设备上最多可组态 7 个 DNS 服务器。手动组态的 DNS 服务器优先级较高。

DNS 服务器（域名系统）可将域名分配给某个 IP 地址，以便唯一标识设备。

如果启用此功能，设备可以作为 DNS 客户端与 DNS 服务器通信。您可以在 IP 地址对话框中输入名称。

说明

只有在网络中存在 DNS 服务器时才能使用"DNS 客户端"功能。



说明

该页面包含以下框：

- **DNS 客户端 (DNS client)**

  如果选中了该复选框，则会启用"DNS 客户端"(DNS client) 功能。

- **使用的 DNS 服务器 (Used DNS Servers)**

  在此指定设备使用的 DNS 服务器：

  – learned only
    设备仅使用 DHCP 分配的 DNS 服务器。

  – manual only
    设备仅使用手动组态的 DNS 服务器。DNS 服务器必须连接 Internet。最多可组态三个 DNS 服务器。

  – all
    设备使用所有可用的 DNS 服务器。

- **DNS 服务器地址 (DNS Server Address)**

  输入 DNS 服务器的 IP 地址。

DNS 服务器表具有以下表列：

- **选择 (Select)**

  选中要删除的行中的复选框。

- **DNS 服务器地址 (DNS Server Address)**

  显示 DNS 服务器的 IP 地址。

- **来源 (Origin)**

  该列用于显示 DNS 服务器为手动组态还是由 DHCP 分配。

步骤

激活 DNS

1. 选中"DNS 客户端"(DNS Client) 复选框。
2. 单击"设置值"(Set Values) 按钮。

创建 DNS 服务

1. 在"DNS 服务器地址"(DNS Server Address) 框中，输入 DNS 服务器的 IP 地址。
2. 单击"创建"(Create) 按钮。

过滤 DNS 服务器

1. 在"使用的 DNS 服务器"(Used DNS Servers) 下拉列表中，选择要使用的 DNS 服务器。
2. 单击"设置值"(Set Values) 按钮。

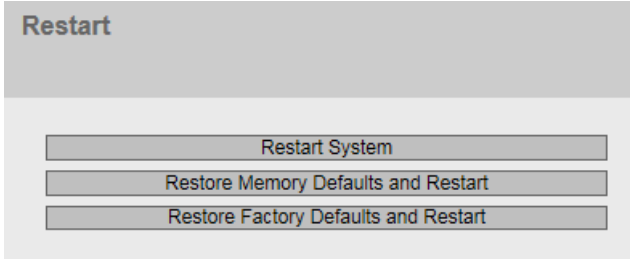
删除 DNS 服务器

1. 启用要删除的行中的"选择"(Select)。
2. 单击"删除"(Delete) 按钮。删除了相关条目。

6.5.6 重启

复位为默认设置

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



说明

对于重启设备，请注意以下几点：

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

说明

为重启设备，该页面上的按钮提供了以下选项：

- **重启 (Restart)**

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

- **恢复存储器默认设置并重启 (Restore Memory Defaults and Restart)**

  单击此按钮可以恢复除以下参数外的出厂组态设置并重启：

  – IP 地址
  – 子网掩码
  – 默认网关的 IP 地址
  – DHCP 客户端 ID
  – DHCP
  – 系统名称
  – 系统位置
  – 系统联系人
  – 用户名和密码
  – 设备的模式
  – DHCPv6 Rapid Commit

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

  单击此按钮可以恢复组态的出厂默认设置。同时会复位受保护的默认设置。

  将触发自动重启。

说明

将所有默认设置复位为出厂组态设置时，IP 地址也会丢失。之后，只能通过 Primary Setup Tool 或 DHCP 访问设备。

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

6.5.7 提交控制

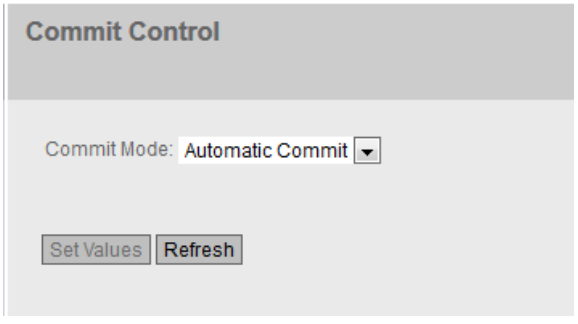
变更管理

在此页面中，可指定 WLAN 设置在 SCALANCE W 设备上生效的时间。
如果更改 WLAN 设置并通过"设置值"(Set Values) 确认更改，则该更改将被采用并立即生效。因此，会短暂中断 WLAN 连接。也就是说，在完全组态前会中断 WLAN 与 SCALANCE W 设备的连接。

使用"手动提交"(Manual Commit) 设置，您可以先对 SCALANCE W 设备进行完全组态。更改已接受，但并未立即激活。更改只有在通过"提交更改"(Commit Changes) 按钮确认后才会生效。

说明

如果通过 WLAN 接口组态 SCALANCE W 设备，则建议使用"手动提交"(Manual Commit) 设置。再次检查参数，然后通过"提交更改"(Commit Changes) 按钮确认更改。



说明

该页面包含以下框：

- **提交模式 (Commit Mode)**

  从该下拉列表中选择所需的设置。

  – 自动提交 (Automatic Commit)

    单击"设置值"(Set Values) 按钮时，对 WLAN 设置的每项更改都将被采用并立即生效。在默认情况下，将 SCALANCE W 设备设置为"自动提交"(Automatic Commit)。

– 手动提交 (Manual Commit)

更改已被接受，但并未立即生效。更改只有在单击"提交更改"(Commit Changes) 按钮确认后才会生效。如果设置"手动提交"(Manual Commit)，将显示"提交更改"(Commit Changes) 按钮。此外，WLAN 发生变更后，将显示消息"手动提交模式激活 - 按下'提交更改'按钮为驱动程序提供当前组态"(Manual Commit Mode active - Press 'Commit Changes' button to provide current configuration to driver)。可以在每个 WBM 页面上看到这条消息，直至所做的更改已生效或 SCALANCE W 设备已重启。

说明

更改生效后，所有 WLAN 接口的 WLAN 连接都将暂时中断。WLAN 驱动程序以新的设置启动。

6.5.8 加载和保存

说明

可从设备加载的文件取决于登录用户的角色。

文件类型概述

表格 6- 1 HTTP

文件类型	描述	下载	保存	删除
Config	此文件包含启动组态。 此外，该文件还包含用户、角色、组和功能权限的相关定义。密码存储在"用户"(Users) 文件中。	X	X	--
ConfigPack	详细组态信息。例如，启动组态、用户、证书、收藏夹和设备固件（如果已保存）。 有关创建和使用 ConfigPack（包括固件）的更多详细信息，请参见"维护 (页 547)"部分。	X	X	--

文件类型	描述	下载	保存	删除
CountryList	此 zip 文件中包含 csv 和 pdf 格式的国家/地区列表文件。	--	X	--
Debug	此文件包含有关 Siemens 支持的信息。 它已被加密，可通过电子邮件发送给 Siemens 支持且不会带来安全风险。	--	X	X
EDS	电子数据表 (EDS) 电子数据表用于描述 EtherNet/IP 模式下的设备	--	X	--
固件	固件已签名且加密。这可确保只能将 Siemens 创建的固件下载到设备。	X	X	--
GSDML	有关设备属性 (PROFINET) 的信息	--	X	--
HTTPS Cert	包含密钥的默认 HTTPS 证书 预设及自动创建的 HTTPS 证书均为自签署证书。 强烈建议您创建自己的 HTTPS 证书并使用它们。建议您使用由可靠外部或内部认证机构签署的 HTTPS 证书。HTTPS 证书会检查设备的身份并控制加密数据交换。 可将以下文件类型加载至设备中： • .pem 要将具有此数据类型的 HTTPS 证书成功下载到设备中，该证书必须包含未加密的私钥。 • .p12 对于具有此文件类型的 HTTPS 证书，私钥已加密并受到密码保护。 要将具有此文件类型的证书成功下载至设备，请在"系统 > 下载和保存 > 密码"(System > Load & Save > Passwords) WBM 页面中组态为该证书指定的密码。 不能导入不同格式的证书。 最大文件大小：8192 位	X	X	X
LogFile	带有事件日志表中条目的文件	--	X	--
LoginWelcomeMessage	txt 文件包含所需的文本或 ASCII 类型。仅支持 ASCII 格式的纯文本文件。	X	X	X

文件类型	描述	下载	保存	删除
MIB	专有 MSPS MIB 文件"Scalance_w_msps.mib"	--	X	--
RunningCLI	包含 CLI 命令的文本文件 此文件包含 CLI 命令形式的当前组态概览。密码在此文件中的隐藏方式如下：[PASSWORD] 可下载此文本文件。如果此文件未更改，则不会再次上传。	--	X	--
RunningSINEMAConfig	将当前设备组态保存为此文件类型，以便传送到 STEP 7 Basic/Professional。该文件可导入 STEP 7 Basic/Professional 并可安装在具有相同订货号和固件版本的设备上。 在保存文件之前，必须在 WBM 中的"系统 > 加载和保存 > 密码"(System > Load&Save > Passwords) 下为"RunningSINEMAConfig"分配一个密码。另外，将文件导入 STEP7 Basic/Professional 时还需要该密码。 另请参见"SINEMAConfig"	--	X	--
Script	包含 CLI 命令的文本文件 可以在设备中上传脚本文件。会相应地执行其中包含的 CLI 命令。 用于保存和加载文件的 CLI 命令不能使用 CLI 脚本文件来执行。	X	--	--
SINEMAConfig	加载通过 STEP 7 Basic/Professional 导出的组态数据，以使用该文件类型传送到 WBM。 要加载文件，必须在"系统 > 加载和保存 > 密码"(System > Load&Save > Passwords) 下为"SINEMAConfig"分配一个密码。另外，将文件从 STEP 7 Basic/Professional 导出时还需要该密码。 另请参见"RunningSINEMAConfig"	X	--	--
StartupInfo	启动日志文件 该文件包含上次启动时已在日志文件中输入的消息。	--	X	--
用户	带有用户名和密码的文件	X	X	--

文件类型	描述	下载	保存	删除
WBMFav	WBM 收藏夹 该文件包含用户在 WBM 中创建的收藏夹。可以下载该文件并将其上传至其他设备。	X	X	X
WLANAuthlog	带有 WLAN 验证日志中条目（有关验证尝试成功或失败的信息）的文件	--	X	--
WLANCert（仅限客户端模式）	用户证书。可在 WBM 页面"加载和保存 > 密码"(Load&Save > Password) 中为用户证书指定密码。 最大文件大小：8192 位	X	X	X
WLANServCert（仅限客户端模式）	服务器证书 最大文件大小：8192 位	X	X	X
WLANSigRec（仅限客户端模式）	该 zip 文件包含以下文件： • csv 文件，具有信号记录器的测量值 • pdf 文件，具有测量值及其附加图形表示。 有关测量值及其图形表示的信息，请参见"信号记录器 (页 396)"部分。	--	X	X

表格 6- 2　TFTP/SFTP

文件类型	描述	保存	下载
Config	此文件包含启动组态。 此外，该文件还包含用户、角色、组和功能权限的相关定义。密码存储在"用户"(Users) 文件中。	X	X
ConfigPack	详细组态信息。例如，启动组态、用户、证书和设备固件（如果已保存）。 有关创建和使用 ConfigPack（包括固件）的更多详细信息，请参见"维护 (页 547)"部分。	X	X
CountryList	此 zip 文件中包含 csv 和 pdf 格式的国家/地区列表文件。	X	--

文件类型	描述	保存	下载
Debug	此文件包含有关 Siemens 支持的信息。它已被加密，可通过电子邮件发送给 Siemens 支持且不会带来安全风险。	X	--
EDS	电子数据表 (EDS) 电子数据表用于描述 EtherNet/IP 模式下的设备	X	--
固件	固件已签名且加密。这可确保只能将 Siemens 创建的固件下载到设备。	X	X
GSDML	有关设备属性 (PROFINET) 的信息	X	--
HTTPS Cert	包含密钥的默认 HTTPS 证书 预设及自动创建的 HTTPS 证书均为自签署证书。 强烈建议您创建自己的 HTTPS 证书并使用它们。建议您使用由可靠外部或内部认证机构签署的 HTTPS 证书。HTTPS 证书会检查设备的身份并控制加密数据交换。 可将以下文件类型加载至设备中： • .pem 要将具有此数据类型的 HTTPS 证书成功下载到设备中，该证书必须包含未加密的私钥。 • .p12 对于具有此文件类型的 HTTPS 证书，私钥已加密并受到密码保护。 要将具有此文件类型的证书成功下载至设备，请在"系统 > 下载和保存 > 密码"(System > Load & Save > Passwords) WBM 页面中组态为该证书指定的密码。 不能导入不同格式的证书。 最大文件大小：8192 位	X	X
LogFile	带有事件日志表中条目的文件	X	--
LoginWelcomeMessage	txt 文件包含所需的文本或 ASCII 类型。仅支持 ASCII 格式的纯文本文件。	X	X
MIB	专有 MSPS MIB 文件"Scalance_w_msps.mib"	X	--

文件类型	描述	保存	下载
RunningCLI	包含 CLI 命令的文本文件 此文件包含 CLI 命令形式的当前组态概览。密码在此文件中的隐藏方式如下：[PASSWORD] 可下载此文本文件。如果此文件未更改，则不会再次上传。	X	--
RunningSINEMAConfig	将当前设备组态保存为此文件类型，以便传送到 STEP7 Basic/Professional。该文件可导入 STEP 7 Basic/Professional 并可安装在具有相同订货号和固件版本的设备上。在保存文件之前，必须在 WBM 中的"系统 > 加载和保存 > 密码"(System > Load&Save > Passwords) 下为"RunningSINEMAConfig"分配一个密码。另外，还需要该密码以将文件导入 STEP 7 Basic/Professional；另请参见"SINEMAConfig"。	--	X
Script	包含 CLI 命令的文本文件 可以在设备中上传脚本文件。会相应地执行其中包含的 CLI 命令。 用于保存和加载文件的 CLI 命令不能使用 CLI 脚本文件来执行。	--	X
SINEMAConfig	加载通过 STEP 7 Basic/Professional 导出的组态数据，以使用该文件类型传送到 WBM。要加载文件，必须在"系统 > 加载和保存 > 密码"(System > Load&Save > Passwords) 下为"SINEMAConfig"分配一个密码。另外，还需要该密码以将文件从 STEP 7 Basic/Professional 导出；另请参见"RunningSINEMAConfig"。	X	--
StartupInfo	启动日志文件 该文件包含上次启动时已在日志文件中输入的消息。	X	--
用户	带有用户名和密码的文件	X	X
WBMFav	WBM 收藏夹 该文件包含用户在 WBM 中创建的收藏夹。可以下载该文件并将其上传至其他设备。	X	X

文件类型	描述	保存	下载
WLANAuthlog	带有 WLAN 验证日志中条目（有关验证尝试成功或失败的信息）的文件	X	--
WLANCert（仅限客户端模式）	用户证书。可在 WBM 页面"加载和保存 > 密码"(Load&Save > Password) 中为用户证书指定密码。 最大文件大小：8192 位	X	X
WLANServerCert（仅限客户端模式）	服务器证书 最大文件大小：8192 位	X	X
WLANSigRec（仅限客户端模式）	该 zip 文件包含以下文件： • csv 文件，具有信号记录器的测量值 • pdf 文件，具有测量值及其附加图形表示。 有关测量值及其图形表示的信息，请参见"信号记录器 (页 396)"部分。	X	--

参见

频谱分析仪 (页 410)

密码 (页 468)

6.5.8.1 HTTP

通过 HTTP 加载和保存数据

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

说明

此 WBM 页面在通过 HTTP 或 HTTPS 建立连接时均可用。

固件

固件已签名且加密。这可确保只能将 Siemens 创建的固件下载到设备。

说明

与先前版本的不兼容性

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

插入的 PLUG 组态与先前版本不兼容

在安装先前版本的过程中，组态数据和日志文件可能丢失。在这种情况下，安装固件后，设备会使用出厂设置启动。如果此时设备中插入了 PLUG，则重启后，由于 PLUG 仍具有之前最新固件的组态数据，因此状态为"Not Accepted"。此时，您可以返回之前的最新固件而不丢失任何组态数据。如果不再需要 PLUG 上的原始组态，则可使用 WBM 页面系统 > PLUG"(System > PLUG) 手动删除或重写 PLUG。

组态文件

说明

组态文件和试用模式/自动保存模式

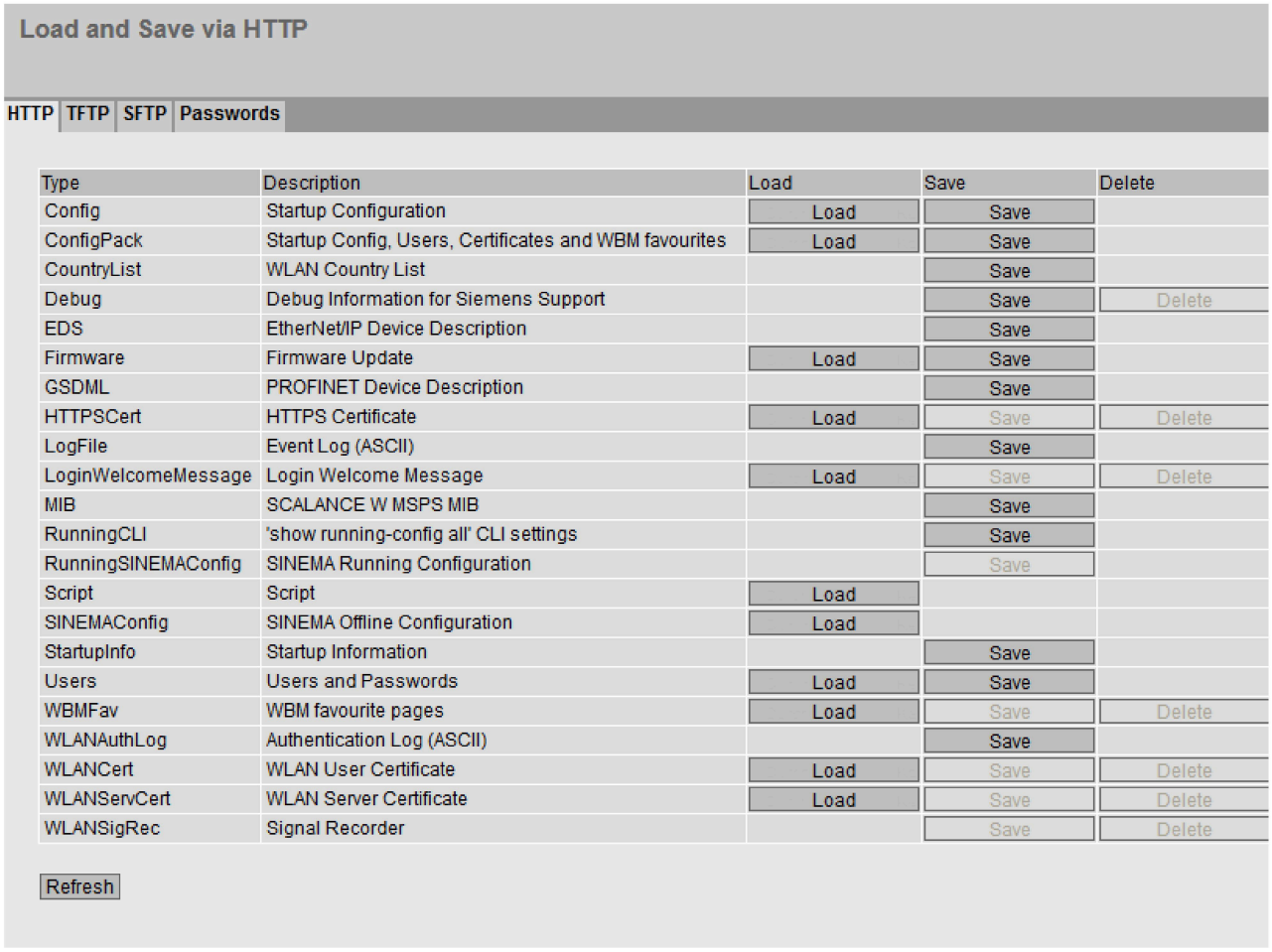
在自动保存模式下，组态文件（ConfigPack 和 Config）传输前数据会自动保存。
在试用模式下，虽然会采用更改，但不会将更改保存在组态文件（ConfigPack 和 Config）中。在"系统 > 组态"(System > Configuration) WBM 页面中使用"写入启动组态"(Write Startup Config) 按钮将更改保存在组态文件中。

CLI 脚本文件

可下载现有 CLI 组态 (RunningCLI) 并上传您自己的 CLI 脚本 (Script)。

说明

如果可下载的 CLI 脚本 (RunningCLI) 未更改，则不会再次上传。



Example of a device in client mode

描述

该表格包括以下列：

- **文件类型 (File type)**

  显示文件的名称。

  说明

  证书文件的大小
  证书文件仅支持最大为 8192 位的证书。

- **描述 (Description)**

  显示文件类型的简要说明。

- **加载 (Load)**

  可以使用此按钮将文件加载到设备。如果文件类型支持该功能，将启用该按钮。

- **保存 (Save)**

  可以使用此按钮保存设备中的文件。仅当文件类型支持该功能且文件存在于设备上时，才会启用该按钮。

- **删除 (Delete)**

  可以使用此按钮删除设备中的文件。仅当文件类型支持该功能且文件存在于设备上时，才会启用该按钮。

  说明
  更新固件之后，请删除 Web 浏览器的缓存。

步骤

使用 HTTP 加载文件

1. 单击"Load"按钮之一启动加载功能。

   将打开文件加载对话框。

2. 转至要加载的文件。

3. 单击对话框中的"Open"按钮。

   文件现已加载完毕。

是否需要重启取决于加载的文件。如果需要重启，将输出相应消息。其他文件（如 CLI 脚本文件）将立即执行，且无需重启即可应用新设置。

使用 HTTP 保存文件

1. 单击"Save"按钮之一启动保存功能。根据文件大小，这可能需要一些时间。

2. 根据浏览器组态，系统将提示您选择存储位置和文件名称。或者可以接受推荐的文件名。若要进行选择，请使用浏览器中的对话框。进行选择之后，单击"保存"(Save)按钮。

使用 HTTP 删除文件

1. 单击"Delete"按钮之一启动删除功能。

   文件将被删除。

复用组态数据

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

要复用组态数据，请按以下步骤操作：

1. 将已组态设备的组态数据保存在 PC 上。

2. 将该组态文件下载到要组态的所有其他设备中。

3. 如果有必要对特定设备进行单独设置，则必须在相关设备上在线进行设置。

说明

组态数据具有校验和。如果编辑这些文件，将无法再将这些文件上传到设备。

6.5.8.2 TFTP

通过 TFTP 服务器加载和保存数据

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

固件

固件已签名且加密。这可确保只能将 Siemens 创建的固件下载到设备。

说明

与先前版本的不兼容性

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

插入的 PLUG 组态与先前版本不兼容

在安装先前版本的过程中，组态数据和日志文件可能丢失。在这种情况下，安装固件后，设备会使用出厂设置启动。如果此时设备中插入了 PLUG，则重启后，由于 PLUG 仍具有之前最新固件的组态数据，因此状态为"Not Accepted"。此时，您可以返回之前的最新固件而不丢失任何组态数据。如果不再需要 PLUG 上的原始组态，则可使用 WBM 页面系统 > PLUG"(System > PLUG) 手动删除或重写 PLUG。

组态文件

说明

组态文件和试用模式/自动保存模式

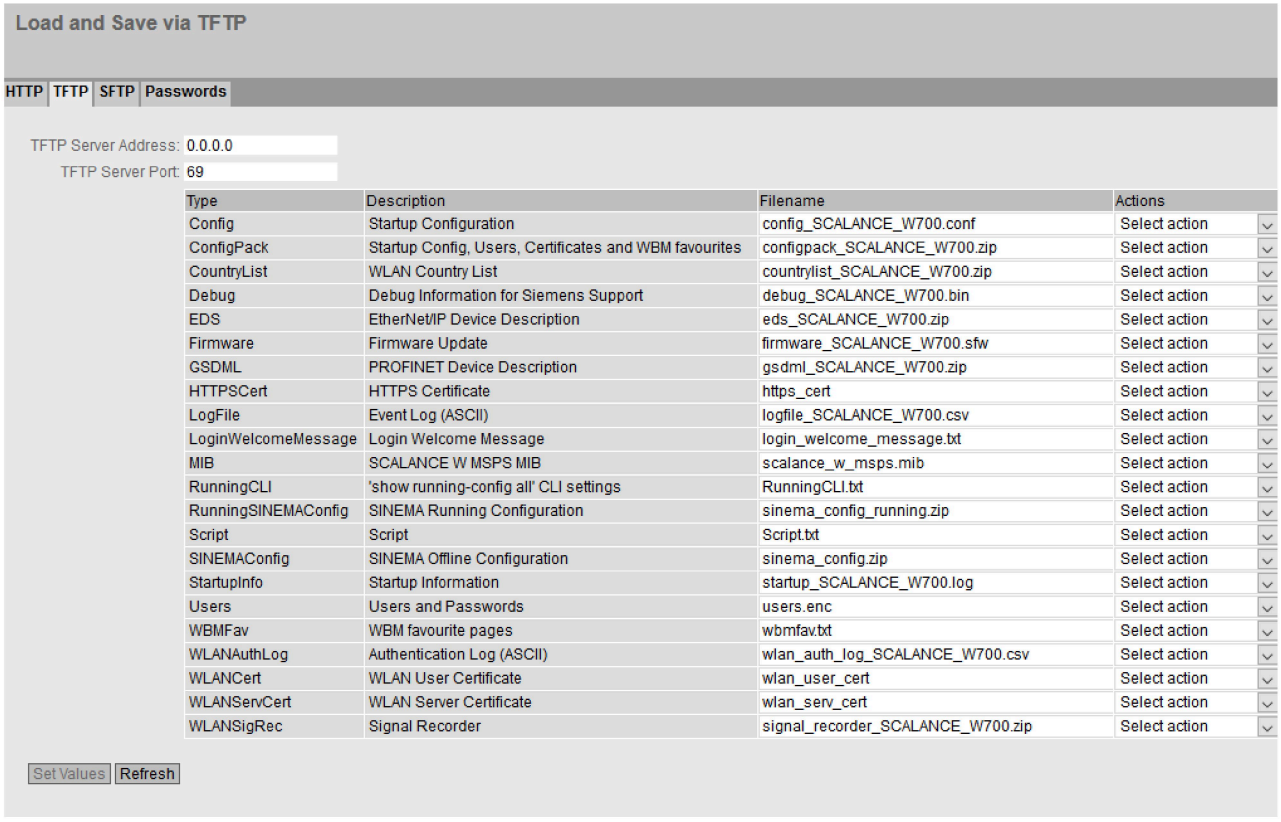
在自动保存模式下，组态文件（ConfigPack 和 Config）传输前数据会自动保存。
在试用模式下，虽然会采用更改，但不会将更改保存在组态文件（ConfigPack 和 Config）中。在"系统 > 组态"(System > Configuration) WBM 页面中使用"写入启动组态"(Write Startup Config) 按钮将更改保存在组态文件中。

CLI 脚本文件

可下载现有 CLI 组态 (RunningCLI) 并上传您自己的 CLI 脚本 (Script)。

说明

如果可下载的 CLI 脚本 (RunningCLI) 未更改，则不会再次上传。



Example of a device in client mode

描述

该页面包含以下框：

- **TFTP 服务器地址 (TFTP Server Address)**

  在此处输入用于交换数据的 TFTP 服务器的 IP 地址或 FQDN（完全限定域名）。

- **TFTP 服务器端口 (TFTP Server Port)**

  在此输入 TFTP 服务器要用于交换数据的端口。如有必要，可以将默认值 69 更改为适合您需要的值。

该表格包括以下列：

- **类型 (Type)**

  显示文件的名称。

  说明

  证书文件的大小
  证书文件仅支持最大为 8192 位的证书。

- **描述 (Description)**

  显示文件类型的简要说明。

- **文件名 (Filename)**

  输入文件名。

- **操作 (Actions)**

  从下拉列表中选择操作。可供选择的选项取决于所选文件类型，例如，只能保存日志文件。
  相关选项如下：

  – **保存文件 (Save file)**

    通过该选项将文件保存到 TFTP 服务器上。

  – **加载文件 (Load file)**

    通过该选项加载 TFTP 服务器中的文件。

步骤

通过 TFTP 加载或保存数据

1. 在"TFTP Server Address"输入框中输入 TFTP 服务器的 IP 地址或者 FQDN 名称。
2. 在"TFTP 服务器端口"(TFTP server port) 输入框中输入要使用的服务器端口。
3. 在"文件名"(File name) 输入框中输入用于保存数据或从中获取数据的文件的名称。

4. 从"操作"(Actions) 下拉列表中选择要执行的操作。
5. 单击"设置值"(Set Values) 按钮启动所选操作。根据文件大小，这可能需要一些时间。
6. 加载组态和 SSL 证书之后，重启设备。更改只在重启后生效。

复用组态数据

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

要复用组态数据，请按以下步骤操作：

1. 将已组态设备的组态数据保存在 PC 上。

2. 将该组态文件下载到要组态的所有其他设备中。

3. 如果有必要对特定设备进行单独设置，则必须在相关设备上在线进行设置。

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

6.5.8.3 SFTP

通过 SFTP 服务器加载和保存数据

SFTP（SSH 文件传输协议）传输加密文件。在此页面中组态 SFTP 服务器的访问数据。

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

在此页面上，还可以加载建立安全 VPN 连接所需的证书。

固件

固件已签名且加密。这可确保只能将 Siemens 创建的固件下载到设备。

组态文件

说明

组态文件和 Trial 模式/自动保存

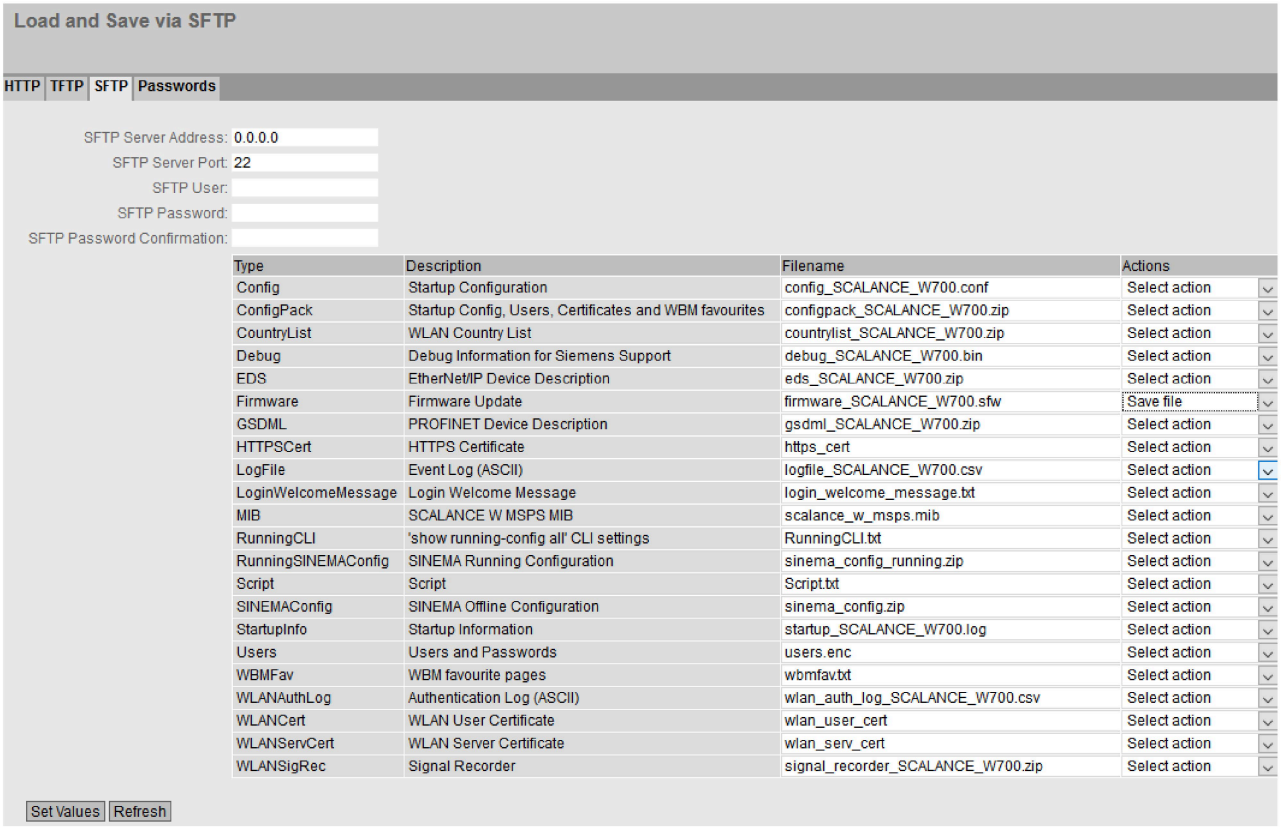
在"自动保存"模式下，数据会在传输组态文件（ConfigPack 和 Config）前自动保存。在"Trial"模式下，虽然会采用更改，但不会将更改保存在组态文件（ConfigPack 和 Config）中。在"系统 > 组态"(System > Configuration) WBM 页面中使用"写入启动组态"(Write Startup Config) 按钮将更改保存在组态文件中。

CLI 脚本文件

可下载现有 CLI 组态 (RunningCLI) 并上传您自己的 CLI 脚本 (Script)。

说明

如果可下载的 CLI 脚本未更改，则不会再次上传。



Example of a device in client mode

描述

该页面包含以下框：

- **SFTP 服务器地址 (SFTP Server Address)**
  输入要与其交换数据的 SFTP 服务器的 IP 地址或 FQDN。
- **SFTP 服务器端口 (SFTP Server Port)**
  输入 SFTP 服务器要用于交换数据的端口。如有必要，可以将默认值 22 更改为适合您需要的值。
- **SFTP 用户 (SFTP User)**
  输入访问 SFTP 服务器的用户。这里假设已在 SFTP 服务器中创建具有相应权限的用户。
- **SFTP 密码 (SFTP Password)**
  输入用户的密码。
- **SFTP 密码确认 (SFTP Password Confirmation)**
  确认密码。

该表格包括以下列：

- **类型 (Type)**
  显示文件类型。
- **说明 (Description)**
  显示文件类型的简要说明。

- **文件名 (Filename)**

  在此为每种文件类型预设一个文件名。

  说明

  更改文件名

  可以更改此列中预设的文件名。单击"设置值"(Set Values) 按钮后，更改后的文件名会保存在设备上，并且还可用于命令行接口。

- **操作 (Actions)**

  从下拉列表中选择操作。可供选择的选项取决于所选文件类型，例如，只能保存日志文件。

  可能的操作包括：

  – **保存文件 (Save file)**

    通过该选项将文件保存到 SFTP 服务器上。

  – **加载文件 (Load file)**

    通过该选项加载 SFTP 服务器中的文件。

步骤

通过 SFTP 加载或保存数据

1. 在"SFTP 服务器地址"(SFTP Server Address) 中输入 SFTP 服务器地址。
2. 在"SFTP 服务器端口"(SFTP Server Port) 中输入要使用的 SFTP 服务器端口。
3. 输入访问 SFTP 服务器所需的用户数据（用户名和密码）。
4. 如果适用，在"文件名"(Filename) 中输入要保存数据或从中获取数据的文件的名称。

说明

访问受密码保护的文件

为了能够在设备上成功加载这些文件，需要在"系统 > 加载和保存 > 密码"(System > Load&Save > Passwords) 中输入为文件指定的密码。

5. 从"操作"(Actions) 下拉列表中选择要执行的操作。
6. 单击"设置值"(Set Values) 启动所选操作。
7. 如果需要重启，将输出相应消息。单击"确定"(OK) 按钮运行重新启动。如果单击"中止"(Abort) 按钮，设备将不会重启。所做的更改只在重启后生效。

复用组态数据

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

要复用组态数据，请按以下步骤操作：

1. 将已组态设备的组态数据保存在 PC 上。
2. 按这种方式将这些组态文件加载到要组态的所有其他设备中。
3. 如果有必要对特定设备进行单独设置，则必须在相关设备上在线进行设置。

说明

组态数据具有校验和。如果修改这些数据，将无法再将其上传到工业以太网交换机。

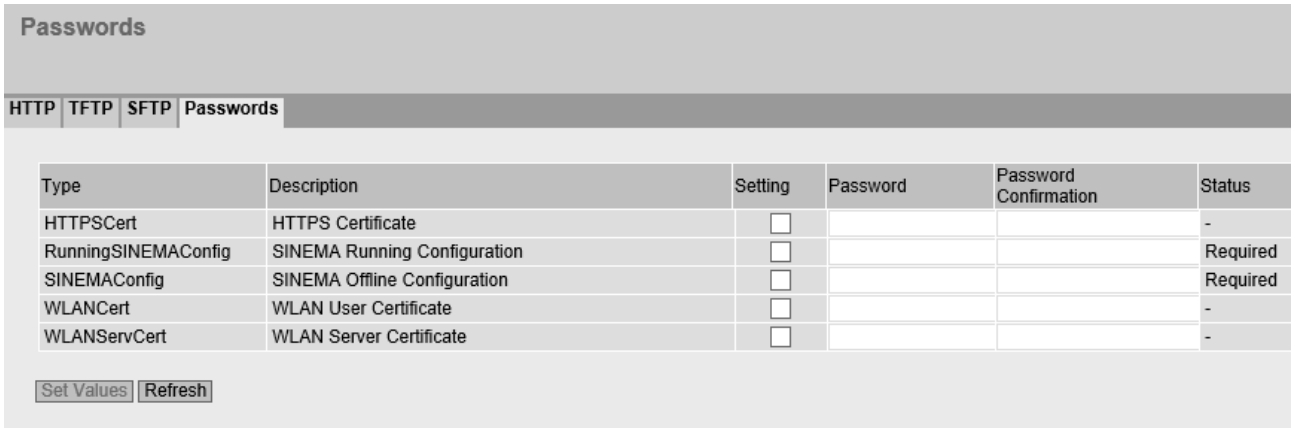
6.5.8.4 密码

有些文件的访问受密码保护。例如，为了能够使用 HTTPS 证书，需要在 WBM 页面上指定相应的密码。

说明

一个文件中的用户和服务器证书

如果用户和服务器证书位于同一文件中，则会在设备上将此文件作为用户证书和服务器证书加载。



描述

该表格包括以下列：

- **类型 (Type)**

  显示文件类型。

- **描述 (Description)**

  显示文件的简要描述。

- **设置 (Setting)**

  只有在组态了密码的情况下才能启用。

  启用后，将在加载期间执行检查，确保密码与为文件设置的密码相匹配。

- **密码 (Password)**

  输入为文件设置的密码。

说明

分配密码时，只能使用以下可读的 ASCII 字符：0x20 - 0x7e。

- **密码确认 (Password Confirmation)**

  确认密码。

- **状态 (Status)**

  – **"-"**

    未指定密码，或者已启用密码但尚未加载文件。

  – 有效 (Valid)

    已使用密码并与文件匹配。

  – 无效 (Invalid)

    已使用密码，但密码与文件不匹配。

  – 必选项 (Required)

    必须提供密码才能加载或保存。

步骤

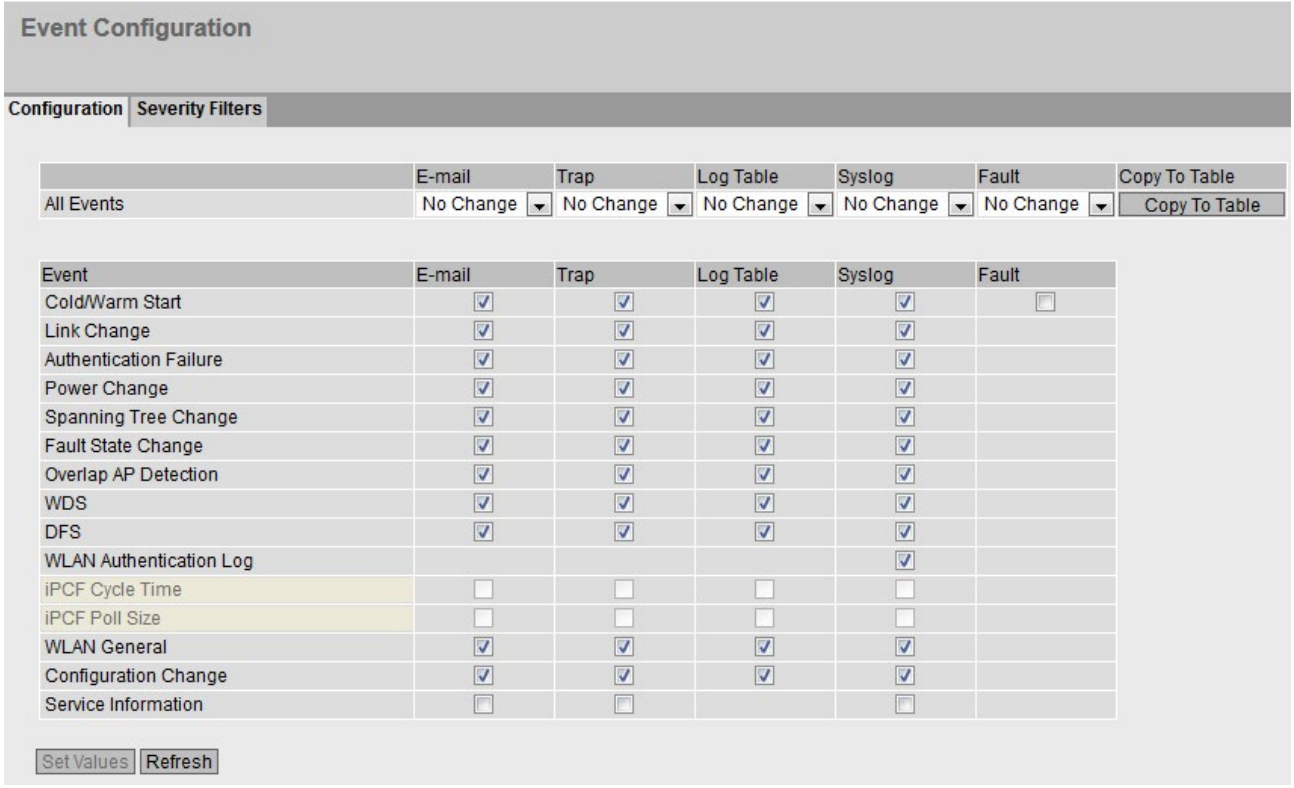
1. 在"密码"(Password) 中输入密码。
2. 要确认密码，在"密码确认"(Password Confirmation) 中再次输入密码。
3. 选择"启用"(Enabled) 选项。
4. 单击"设置值"(Set Values) 按钮。

6.5.9 事件

6.5.9.1 组态

选择系统事件

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



描述

利用表 1，可以一次启用或禁用表 2 中某个列的所有复选框。表 1 包含以下列：

- **所有事件 (All Events)**

  说明设置对于表 2 的所有事件都有效。

- **电子邮件 (E-mail)/陷阱 (Trap)/日志表 (Log Table)/Syslog/故障 (Faults)**

  启用或禁用所有事件的所需通知类型。如果选中"无变化"(No Change)，则表 2 中相应列的条目保持不变。

- **复制到表 (Copy to Table)**

  如果单击此按钮，则为表 2 的所有事件应用此设置。

表 2 包含以下列：

- **事件 (Event)**

  此列包含以下值：

  – **冷/热启动 (Cold/Warm Start)**
    用户打开或重启设备。

  – **链路变化 (Link Change)**
    仅当对端口状态进行监视和更改时才会发生该事件，请参见"系统 > 故障监视 > 链路变化"(System > Fault Monitoring > Link Change)。

- **验证错误 (Authentication error)**
  当试图用错误的密码访问时会发生该事件。
- 电源变化 (Power Change)
  仅当对电源线路 1 和 2 进行监视时才会发生该事件。这表示线路 1 或线路 2 发生了变化。在 PoE 电源发生故障时，会发生该事件，请参见"系统 > 故障监视 > 电源"(System > Fault Monitoring > Power Supply)。
- 生成树变化 (Spanning Tree Change)
  STP、RSTP 或 MSTP 拓扑发生变化。
- 故障状态变化 (Fault State Change)
  故障状态发生变化。故障状态可能涉及已激活的端口监视、信号触点的响应或电源监视。
- 重叠 AP 监测 (Overlap AP Detection)（仅限接入点模式）
  当"重叠 AP"(Overlap AP) 列表中存在条目时，会触发此事件。
- WDS（仅限接入点模式）
  WDS 链路的连接状态发生了变化。
- DFS（仅限接入点模式）
  接收到雷达信号时或 DFS 扫描启动或者停止时，会发生此事件。
- WLAN 验证日志 (WLAN Authentication Log)
  将 WLAN 验证日志中的条目转发给系统协议服务器。
- WLAN 验证/取消验证 (WLAN De/Authentication)（仅限客户端模式）
  WLAN 验证尝试成功或失败。
- iPCF 周期时间 (iPCF Cycle Time)（仅限接入点模式）
  仅在插入 KEY-PLUG 后才可用。
  设定的 iPCF 周期时间内登录的客户端数量过多或在一个周期内部分客户端无法访问时，则会发生此事件。
- iPCF 轮询大小 (iPCF Poll Size)
  仅在插入 KEY-PLUG 后才可用。
  因 PROFINET 数据太大而无法传送时，会发生此事件。

  - WLAN 常规 (WLAN General)（仅限接入点模式）
    通道带宽发生变化时会发生此事件。
  - 组态更改 (Configuration Change)
    当设备组态发生更改时会发生此事件。
  - 服务信息 (Service Information)
    出现的一些系统事件输入到事件日志表中且无组态。对于这些事件，用户可组态其他类型的通知。

- **E-Mail**
  设备发送电子邮件。仅当已设置 SMTP 服务器并已启用"SMTP client"功能时，该功能才可用。
- **Trap**
  设备发送 SNMP 陷阱。仅当已在"系统 > 组态"(System > Configuration) 中启用"SNMPv1 陷阱"(SNMPv1 Traps) 时，该功能才可用。
- **日志表 (Log Table)**
  设备在事件日志表中写入一个条目。
- **Syslog**
  设备将一个条目写入系统日志服务器。仅当已设置系统日志服务器并已启用"Syslog 客户端"(Syslog client) 功能时，该功能才可用。
- **故障 (Faults)**
  设备触发一个错误。错误 LED 亮起

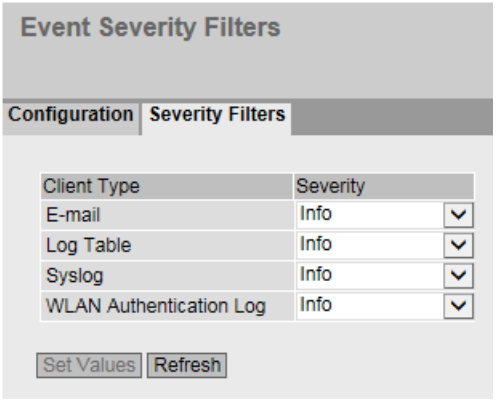
步骤

请按照以下步骤更改条目：

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

6.5.9.2 严重程度过滤器 (Severity Filters)

在此页面上组态决定系统事件通知发送方式的严重程度。



说明

该表包括以下列：

- **客户端类型 (Client Type)**

  选择要设置的客户端类型：

  – **E-mail**

    通过电子邮件发送系统事件消息

  – **Log Table**

    在日志表中输入系统事件

  – **Syslog**

    在 Syslog 文件中输入系统事件

  – **WLAN 验证日志**

    在 WLAN 验证日志中输入系统事件

- **Severity**

  选择所需级别。可能的设置如下：

  – **Critical**

    处理严重程度不低于"Critical"级别的系统事件。

  – **Warning**

    处理严重程度不低于"Warning"级别的系统事件。

  – **Info**

    处理严重程度不低于"Info"级别的系统事件。

步骤

按以下步骤组态所需级别：

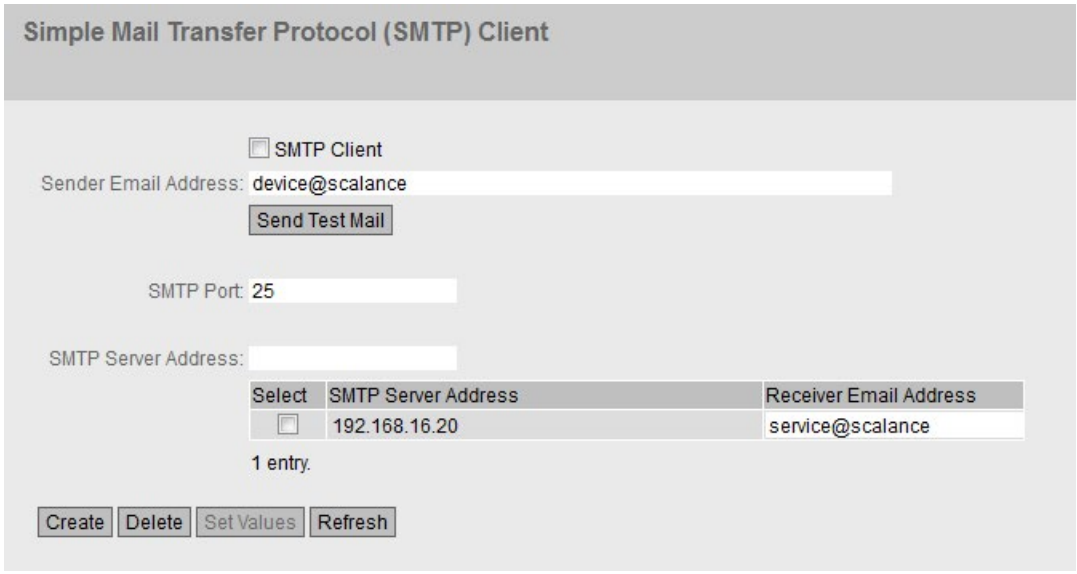
1. 组态客户端类型后，从表格第二列的下拉列表中选择所需值。
2. 单击"设置值"(Set Values) 按钮。

6.5.10 SMTP 客户端

通过电子邮件进行网络监视

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

在此页可组态最多三个 SMTP 服务器和相应的电子邮件地址。



说明

该页面包含以下框：

- **SMTP Client**

  启用或禁用 SMTP 客户端。

- **Sender Email Address**

  输入电子邮件中的发送方名称，如设备名称。

  此设置适用于所有已组态的 SMTP 服务器。

- **Send Test Mail**

  发送一封测试电子邮件检查组态。

- **SMTP Port**

  输入可用来访问 SMTP 服务器的端口。

  出厂设置：25

  此设置适用于所有已组态的 SMTP 服务器。

- **SMTP 服务器地址**

  输入 SMTP 服务器的 IP 地址、FQDN（完全限定域名，Fully Qualified Domain Name）或主机名。

该表包含以下列：

- **Select**
  启用要删除的行中的复选框。
- **SMTP Server Address**
  显示 SMTP 服务器的 IP 地址、FQDN（完全限定域名，Fully Qualified Domain Name）或主机名。
- **Receiver Email Address**
  输入电子邮件地址，发生故障时，设备会将电子邮件发送到该地址。

步骤

1. 启用"SMTP Client"选项。
2. 在"SMTP 服务器地址 (SMTP Server Address)"输入框中输入 SMTP 服务器的 IP 地址、FQDN 或主机名称。
3. 单击"创建"(Create) 按钮。会在表中生成一个新条目。
4. 在"接收电子邮件地址"(Receiver Email Address) 输入框中，输入电子邮件地址，发生故障时，设备会将电子邮件发送到该地址。
5. 单击"设置值"(Set Values) 按钮。

说明

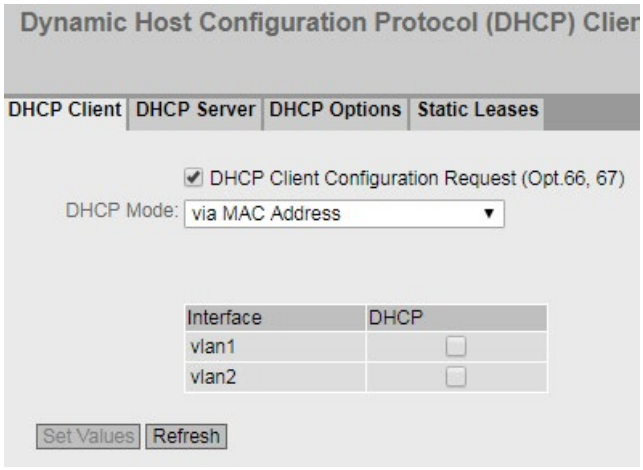
根据 SMTP 服务器属性和组态，可能需要针对电子邮件修改"Sender E-Mail Address"输入框。请与 SMTP 服务器的管理员联系。

6.5.11 DHCPv4

6.5.11.1 DHCP 客户端

DHCP 模式设置

如果设备组态为 DHCP 客户端，则它将启动 DHCP 查询。作为对查询的回复，设备将从 DHCP 服务器接收 IPv4 地址。服务器管理从它分配 IPv4 地址的地址范围。还可以对服务器进行组态，使得客户端发出请求后，总是接收到同一个 IPv4 地址。



说明

该页面包含以下框：

- **DHCP 客户端组态文件请求（选项 66、67）**
  如果想要 DHCP 客户端使用选项 66 和 67 进行下载并随后启用某个组态文件，则选择此选项。
- **DHCP Mode**
  从下拉列表中选择 DHCP 模式。可能的模式如下：
  - via MAC Address
    基于 MAC 地址识别设备。
  - via DHCP Client ID
    基于自由定义的 DHCP 客户端 ID 识别设备。

– via System Name
基于系统名称进行标识。如果系统名称的长度为 255 个字符，则最后一个字符不用于识别设备。

– 通过站的 PROFINET 名称 (via PROFINET Name of Station)
使用 PROFINET 设备名称识别。

该表包括以下列：

- **Interface**
与设置相关的接口。
- **DHCP**
为相关接口启用或禁用 DHCP 客户端。

步骤

1. 从"DHCP 模式"(DHCP Mode) 下拉列表中选择所需模式。如果选择 DHCP 模式"通过 DHCP 客户端 ID"(via DHCP Client ID)，则将出现输入框。
   – 在启用的"DHCP 客户端 ID"(DHCP client ID) 输入框中，输入用于识别设备的字符串。DHCP 服务器随即会评估该字符串。
2. 选择"DHCP 客户端组态请求（选项 66、67）"(DHCP Client Configuration Request (Opt. 66, 67))，如果想要 DHCP 客户端使用选项 66 和 67 进行下载并随后启用某个组态文件，则选择此选项。
3. 在表中启用"DHCP"选项。
4. 单击"设置值"(Set Values) 按钮。

说明

如果下载组态文件，这会触发系统重启。如果当前运行的组态和所已下载的配置文件中的配置不同，则系统将重启。
确保不再设置选项"DHCP 客户端组态请求（选项 66，67）"。

6.5.11.2 DHCP 服务器

可将设备用作一个 DHCP 服务器，从而可自动为相连的设备分配 IPv4 地址。既可以从指定的地址段动态分配 IPv4 地址，也可以将一个指定的 IPv4 地址（静态）分配给一个特定设备。

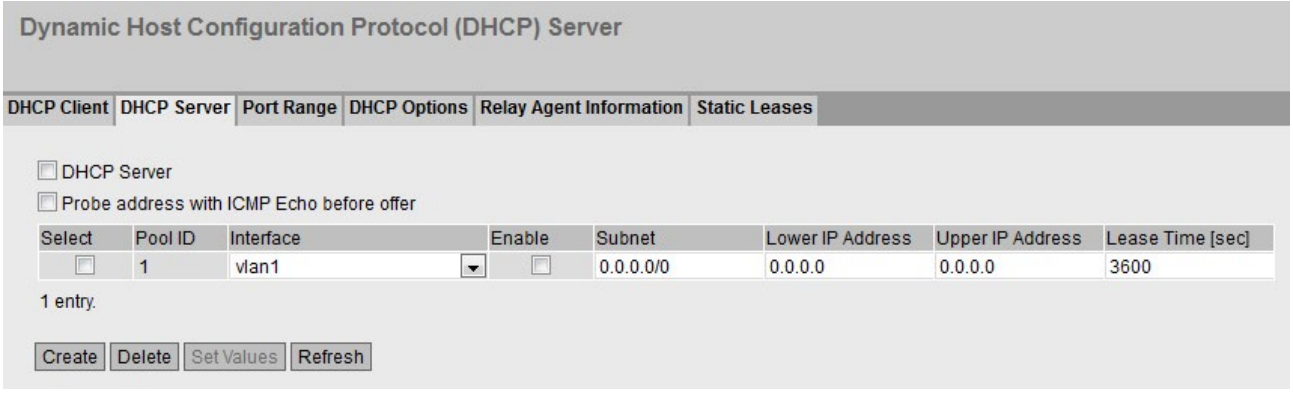
在此页面上指定 IPv4 地址段，设备接收该地址段的任一 IPv4 地址。

在"静态租用"(Static Leases) 中组态 IPv4 地址的静态分配。

说明

IP 地址的最大数量

DHCP 服务器所支持的 IPv4 地址最大数为 100。换言之，IPv4 地址总数为 100（动态 + 静态）。
使用静态分配，最多可以创建 20 个条目。



DHCP 服务器的要求

- 在接入点模式下
  - 将所连设备组态成从 DHCP 服务器中获取 IPv4 地址。
- 在客户端模式下
  - 将所连设备组态成从 DHCP 服务器中获取 IPv4 地址。
  - NAT 已启用。可在"第 3 层 > NAT"(Layer 3 > NAT) 中启用 NAT。

说明

该页面包含以下框：

- **DHCP 服务器 (DHCP Server)**

  启用或禁用设备上的 DHCP 服务器。

  说明

  为避免 IPv4 地址发生冲突，在网络中只能将一个设备组态为 DHCP 服务器。

  说明

  接入点

  对于接入点，只能在分配给管理的 VALN（代理 VLAN ID）上使用"DHCP 服务器"功能。

- **提供服务前通过 ICMP 回送检查地址 (Probe address with ICMP echo before offer)**

  选中后，DHCP 服务器会检查是否已经分配 IP 地址。为此，DHCP 服务器会向特定 IPv4 地址发送 ICMP 回送消息 (ping)。如果未收到应答，则 DHCP 服务器可分配 IPv4 地址。

  说明

  如果网络中存在回送服务默认被禁用的设备，则可能发生 IPv4 地址冲突。为避免这种情况发生，请为这样的设备分配 IPv4 地址段以外的 IPv4 地址。

该表包括以下列：

- **选择 (Select)**

  选中要删除的行中的复选框。

- **池 ID (Pool ID)**

  显示 IPv4 地址段编号。如果单击"创建"(Create) 按钮，则会创建一个具有唯一编号的新行（池 ID）。

  说明

  只能创建一个池 ID (ID = 1)。

- **接口 (Interface)**

  指定用来动态分配 IPv4 地址的接口。

  分配要求接口的 IPv4 地址放置于 IPv4 地址段范围内。如果不是这样，接口不会分配任何 IPv4 地址。

- **启用 (Enable)**

  指定是否会使用此 IPv4 地址段。

  说明

  如果启用 IPv4 地址段，则此选项卡和其它 DHCP 选项卡中的设置将呈灰显状态，不能进行编辑。

- **子网 (Subnet)**

  输入要分配给设备的网络地址范围。使用 CIDR 表示法。

- **低位 IP 地址 (Lower IP address)**

  输入用于指定动态 IPv4 地址段起始的 IPv4 地址。此 IPv4 地址必须处于为"子网"(Subnet) 组态的网络地址范围内。

- **高位 IP 地址 (Upper IP address)**

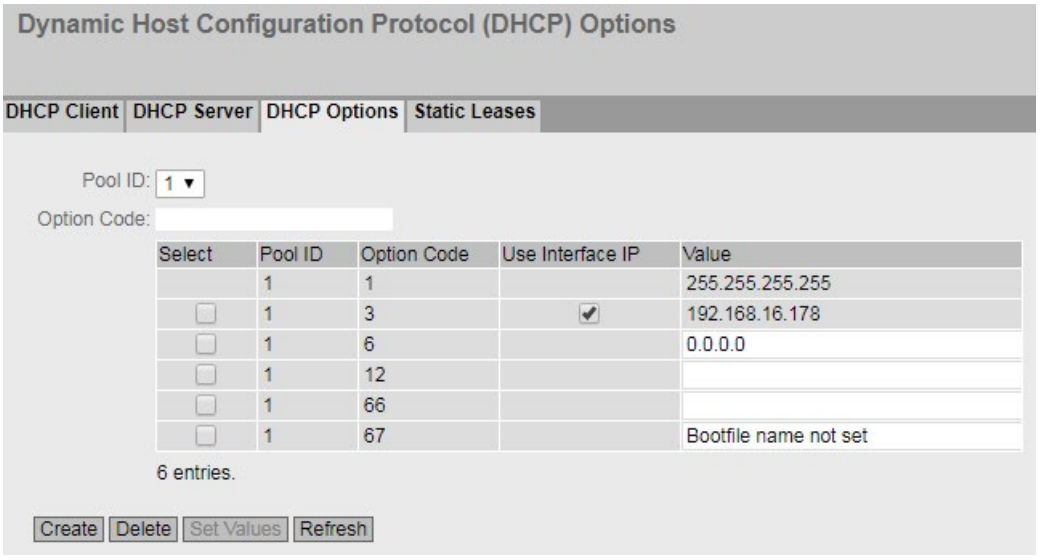
  输入用于指定动态 IPv4 地址段结束的 IPv4 地址。此 IPv4 地址必须处于为"子网"(Subnet) 组态的网络地址范围内。

- **租用时间（秒） (Lease Time (sec))**

  指定分配的 IPv4 地址保持有效的秒数。当租用时间过半后，DHCP 客户端可延长所分配 IPv4 地址的有效时间。当整个时间段过期后，DHCP 客户端需要请求新的 IPv4 地址。

6.5.11.3 DHCP 选项

在此页面上指定 DHCP 服务器支持的 DHCP 选项。RFC 2132 中定义了各种 DHCP 选项。



说明

该页面包含以下框：

- **池 ID (Pool ID)**

  选择所需的 IPv4 地址段。

- **选项代码 (Option Code)**

  输入所需 DHCP 选项的编号。最多可能有 20 个 DHCP 选项。
  RFC 2132 中定义了各种 DHCP 选项。创建 IPv4 地址段后，会自动创建 DHCP 选项 1、3、6、12、66 和 67。除了选项 1 以外，其它选项均可被删除。

  在使用 DHCP 选项 3 时，会将设备的内部 IPv4 地址自动设置为 DHCP 参数。

  说明

  不支持的 DHCP 选项
  不支持 DHCP 选项 50 - 60 和 255。

该表包括以下列：

- **选择 (Select)**

  选中要删除的行中的复选框。

- **池 ID (Pool ID)**

  显示 IPv4 地址段编号。

- **选项代码 (Option Code)**

  显示 DHCP 选项的编号。

- **使用接口 IP (Use interface IP)**

  指定是否使用设备的内部 IPv4 地址。

- **值 (Value)**

  输入要传输至 DHCP 客户端的 DHCP 参数。内容取决于 DHCP 选项。

  – DHCP 选项 67（引导文件名称）

    以字符串格式输入引导文件的名称。

  – DHCP 选项 3（路由器）和 6 (DNS)：

    输入一个 DHCP 参数作为 IPv4 地址，例如 192.168.100.2。对于 DHCP 选项 6，可指定多个 IPv4 地址，地址之间以逗号分隔。

  – DHCP 选项 12（主机名称）：

    以字符串格式输入主机名称。

  – DHCP 选项 66（TFTP 服务器）：

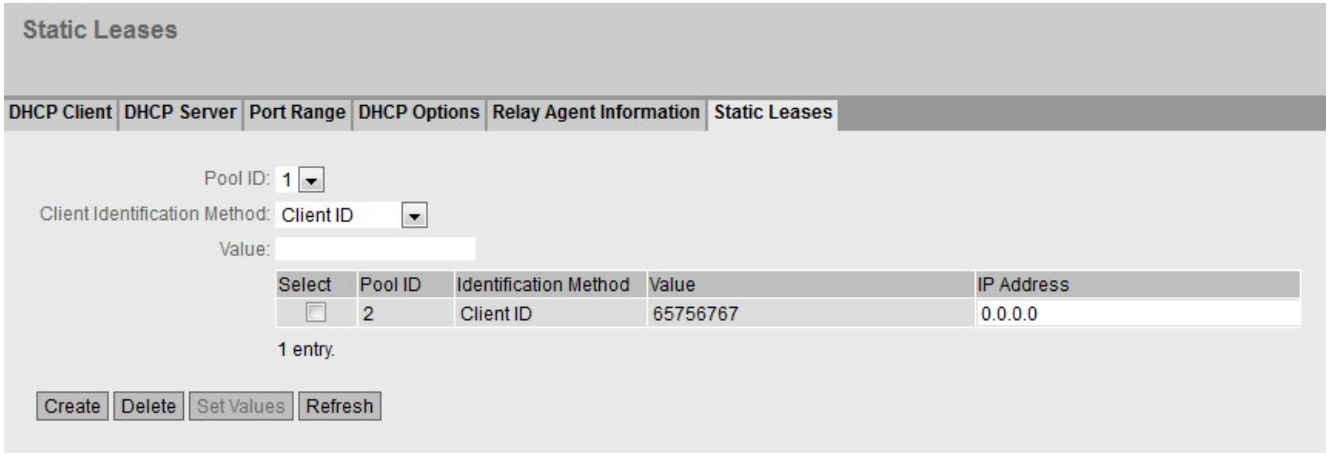
    输入 TFTP 服务器作为 IPv4 地址，例如 192.168.100.2 或 FQDN 名称。

  – 所有其它 DHCP 选项

    输入十六进制的 DHCP 参数，例如，IPv4 地址 192.168.100.2 对应 "C0A86402"。

6.5.11.4 静态租用

在此页面上为具有特定 MAC 地址的设备分配所选的 IPv4 地址。



描述

该页面包含以下框：

- **池 ID (Pool ID)**

  从下拉列表中选择所需 IPv4 地址段。

- **硬件类型 (Hardware Type)**

  选择用于标识客户端的方法。

  – Ethernet MAC

    客户端按照其 MAC 地址进行标识。

  – 客户端 ID (Client ID)

    客户端按照自由定义的 DHCP 客户端 ID 进行标识。客户端 ID 的最大长度可为 254 个字符。

- **值 (Value)**

  输入 MAC 地址或客户端 ID，然后单击"创建"(Create) 按钮创建该条目。

说明

最多支持 20 个条目。

该表格包括以下列：

- **选择 (Select)**

  选中要删除的行中的复选框。

- **池 ID (Pool ID)**

  显示 IPv4 地址段编号。

  说明
  仅支持池 ID = 1。

- **硬件类型 (Hardware Type)**

  显示客户端是根据其 MAC 地址还是客户端 ID 进行标识。

- **值 (Value)**

  显示分配了 IPv4 地址的 MAC 地址。

- **IP 地址 (IP Address)**

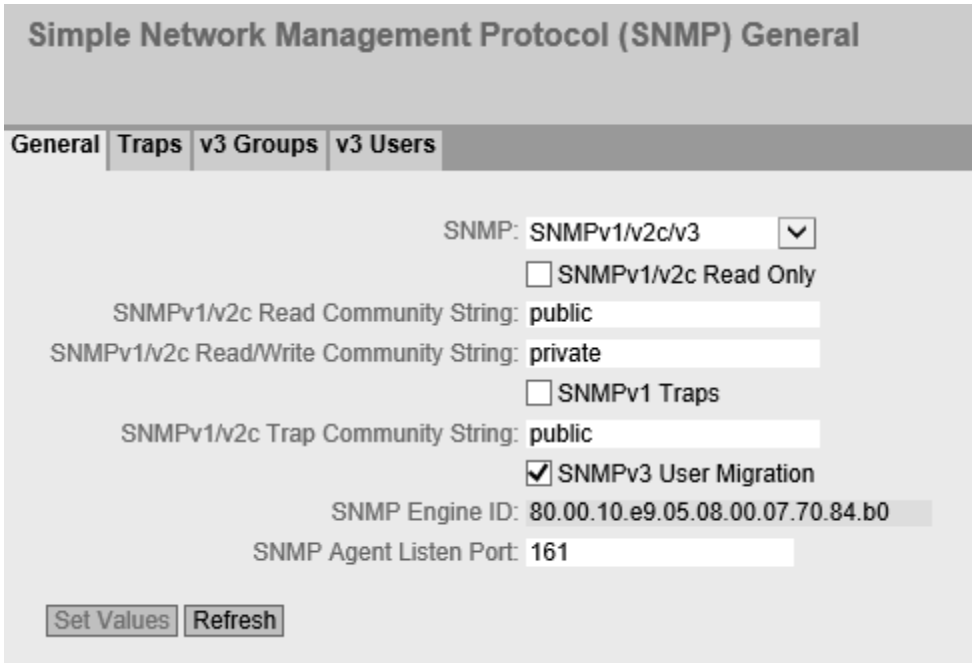
  指定 IPv4 地址。IPv4 地址必须与 IPv4 地址段子网相匹配。

6.5.12 SNMP

6.5.12.1 常规

SNMP 组态

在该页面对 SNMP 进行基本设置。根据希望应用的功能启用相应的复选框。



说明

该页面包含以下框：

- **SNMP**

  从下拉列表中选择 SNMP 协议。可能的设置如下：

  – "-"（禁用）

    禁用 SNMP。

  – SNMPv1/v2c/v3

    支持 SNMPv1/v2c/v3。

    说明

    注意版本 1 和 2c 的 SNMP 不包含任何安全机制。

– SNMPv3

仅支持 SNMPv3。

- **SNMPv1/v2c Read-Only**

如果启用此选项，则 SNMPv1/v2c 仅可读取 SNMP 变量。

说明

团体字符串

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

建议团体字符串的最小长度为 6 个字符。

出于安全原因，只能通过 SNMPv1/v2c Read Community String 对 SNMPCommunityMIB 的对象进行有限访问。通过 SNMPv1/v2c Read/Write Community String，可以对 SNMPCommunityMIB 进行完全访问。

- **SNMPv1/v2c Read Community String**

输入框输入 SNMP 协议的读访问团体字符串。

- **SNMPv1/v2c Read/Write Community String**

输入 SNMP 协议的读写访问团体字符串。

- **SNMPv1 陷阱 (SNMPv1 Traps)**

启用或禁用发送 SNMPv1 陷阱（报警帧）。在"陷阱"(Trap) 选项卡上，指定 SNMPv1 陷阱将发送到的设备的 IP 地址。

- **SNMPv1/v2c Trap Community String**

输入用于发送 SNMPv1/v2c 消息的团体字符串。

- **SNMPv3 用户移植 (SNMPv3 User Migration)**
  - 启用

    如果启用该功能，会生成一个可移植的 SNMP 引擎 ID。可以将已组态的 SNMPv3 用户传送至不同的设备。

    如果启用该功能并将设备的组态加载到另一个设备，将保留组态的 SNMPv3 用户。
  - 禁用

    如果禁用该功能，会生成一个设备特定的 SNMP 引擎 ID。要生成此 ID，需要使用设备的代理 MAC 地址。不得将此 SNMP 用户组态传送至其它设备。

    如果将设备的组态加载到另一个设备，将删除所有组态的 SNMPv3 用户。
- **SNMP 引擎 ID (SNMP Engine ID)**

  显示 SNMP 引擎 ID。
- **SNMP 代理监听端口 (SNMP Agent Listen Port)**

  指定 SNMP 代理等待 SNMP 查询所使用的端口。

步骤

1. 从"SNMP"下拉列表中选择所需选项：
   - "-"（禁用）
   - SNMPv1/v2c/v3
   - SNMPv3
2. 只有希望使用 SNMPv1/v2c 对 SNMP 变量进行读访问时才启用"SNMPv1/v2c 只读"(SNMPv1/v2c Read Only) 复选框。
3. 在"SNMPv1/v2c Read Community String"输入框中输入所需字符串。
4. 在"SNMPv1/v2c Read/Write Community String"输入框中输入所需字符串。

5. 如有必要，可以启用"SNMPv3 用户移植"(SNMPv3 User Migration)。

6. 单击"设置值"(Set Values) 按钮。

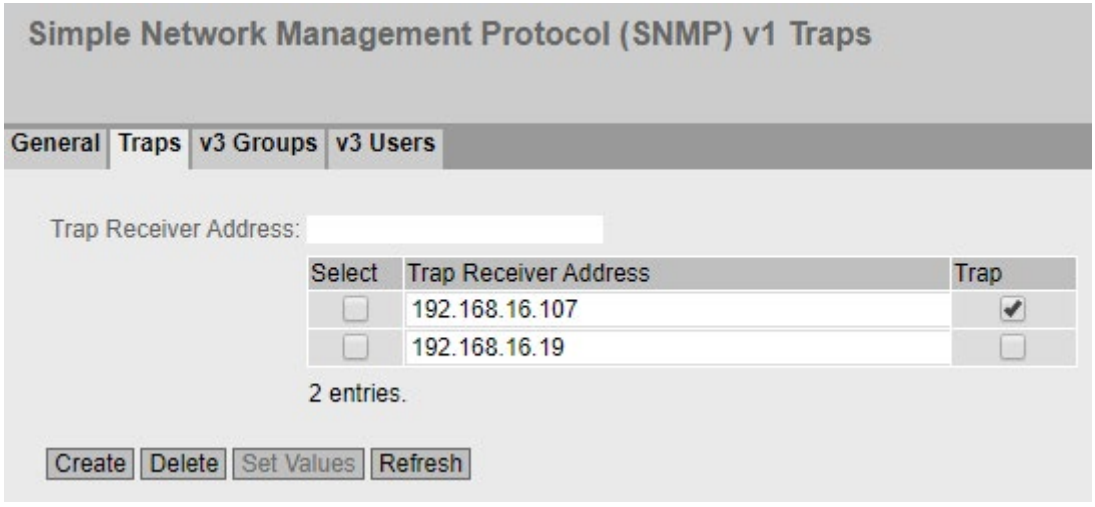
6.5.12.2 Traps

报警事件的 SNMP 陷阱

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

说明

只有已在"General"选项卡或"System > Configuration"中启用选项"SNMPv1 Traps"时，才会发送陷阱。



说明

- **陷阱接收方地址**

  输入设备发送 SNMP 陷阱的目标站的 IP 地址或 FQDN（完全限定域名，Fully Qualified Domain Name）。最多可指定十个不同的接收方服务器。

该表包括以下列：

- **选择 (Select)**
  选择要删除的行。
- **陷阱接收方地址 (Trap Receiver Address)**
  根据需要更改目标站的 IP 地址或 FQDN（完全限定域名，Fully Qualified Domain Name）。
- **陷阱 (Trap)**
  启用或禁止发送陷阱。已输入但未选择的工作站不会接收 SNMP 陷阱。

步骤

创建陷阱条目

1. 在"陷阱接收方地址"(Trap Receiver Address) 中，输入设备发送陷阱的目标站的 IP 地址或 FQDN。
2. 单击"创建"(Create) 按钮以创建新的陷阱条目。
3. 选中所需行"陷阱"(Trap) 列中的复选框。
4. 单击"设置值"(Set Values) 按钮。

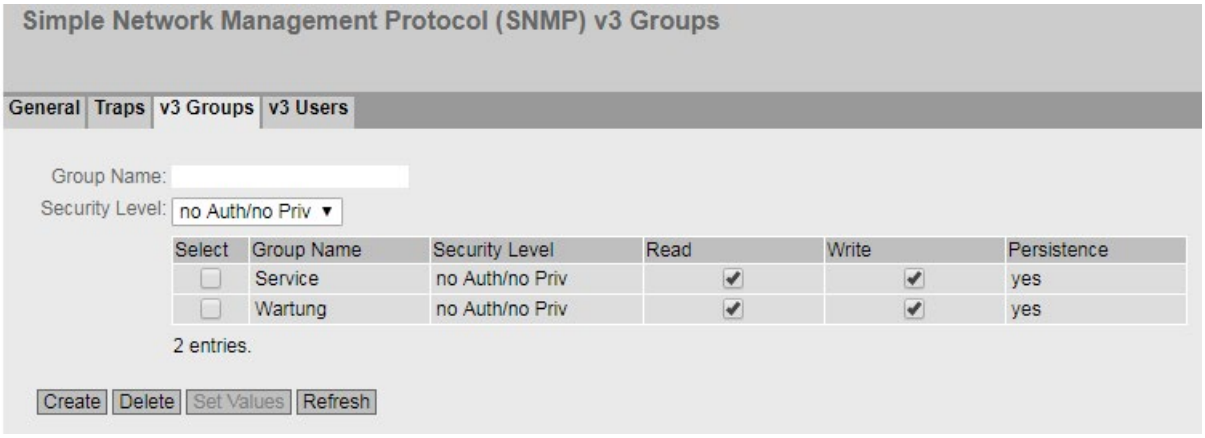
删除陷阱条目

1. 启用要删除的行中的"选择"(Select)。
2. 单击"删除"(Delete) 按钮。删除了相关条目。

6.5.12.3 v3 组

安全设置和权限分配

SNMP 版本 3 允许在协议级分配权限，以及身份验证和加密。安全等级和读/写权限按照组来分配。这些设置会自动应用到组内的每个成员。



说明

该页面包含以下框：

- **Group Name**
  输入组名称。最大长度为 32 个字符。
- **安全等级 (Security Level)**
  选择对所选组有效的安全等级（验证、加密）。可用选项如下：
  - 无身份验证/不加密 (no Auth/no Priv)
    未启用验证，未启用加密。
  - 身份验证/不加密 (Auth/no Priv)
    启用验证/未启用加密。
  - 身份验证/加密 (Auth/Priv)
    启用验证/启用加密。

该表包括以下列：

- **选择 (Select)**
  选择要删除的行。
- **Group Name**
  显示定义的组名称。
- **Security Level**
  显示组态的安全等级。
- **Read**
  启用或禁用所需组的读访问。
- **Write**
  启用或禁用所需组的写访问。

  说明
  要实现写访问，还需启用读访问。
- **Persistence**
  显示组是否已分配至 SNMPv3 用户。如果组未分配至 SNMPv3 用户，则不会触发自动保存，并且在重启设备之后会删除该组态的组。
  - 是 (Yes)
    该组被分配到 SNMPv3 用户。
  - 否 (No)
    该组未被分配到 SNMPv3 用户。

步骤

创建新组

1. 在"Group Name"中输入所需的组名称。
2. 从"Security Level"下拉列表中选择所需安全等级。
3. 单击"Create"按钮以创建新条目。

4. 在"读"(Read) 中为组指定所需的读权限。
5. 在"写"(Write) 中为组指定所需的写权限。
6. 单击"设置值"(Set Values) 按钮。

修改组

1. 在"读"(Read) 中为组指定所需的读权限。
2. 在"写"(Write) 中为组指定所需的写权限。
3. 单击"设置值"(Set Values) 按钮。

说明

指定了组名称和安全等级之后，在组创建之后再无法对其进行修改。如果要更改组名称或安全等级，将必须删除该组并重新创建，然后重新指定新名称。

删除组

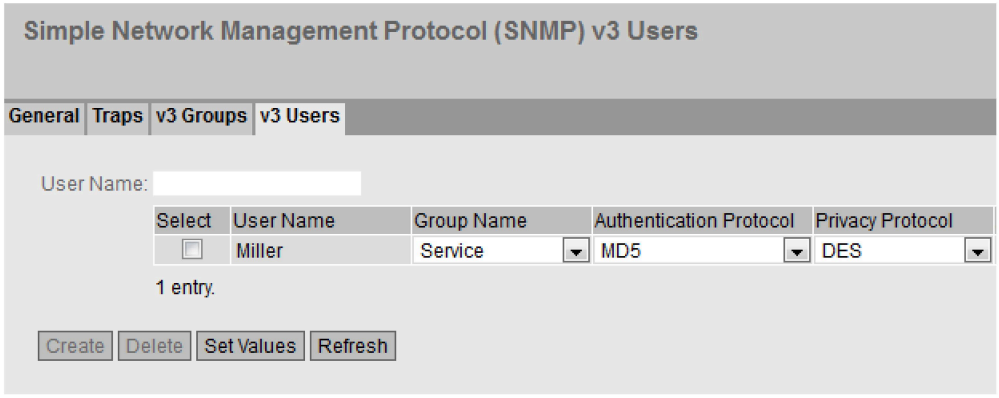
1. 启用要删除的行中的"Select"。

   对所有要删除的组重复此步骤。
2. 单击"删除"(Delete) 按钮。将删除相关条目。

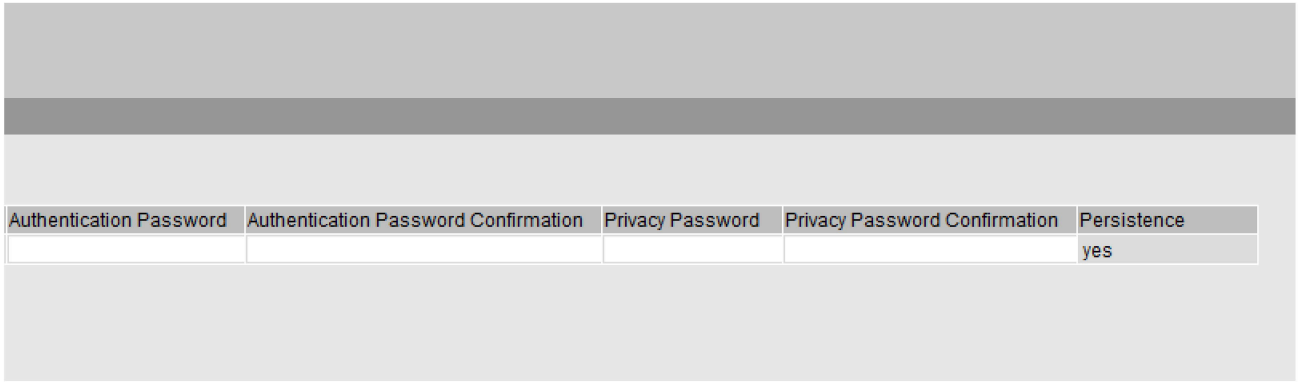
6.5.12.4 v3 用户

用户特定的安全设置

在 WBM 页上，可以创建新的 SNMPv3 用户以及修改或删除现有用户。基于用户的安全模型采用用户名概念；换言之，所有帧中都会加入用户 ID。发送方和接收方均会检查此用户名和适用的安全设置。



SNMPv3 Users - 表的第一部分



SNMPv3 Users - 表的第二部分

说明

该页面包含以下框：

- **User Name**

  输入可自由选择的用户名。输入相关数据之后，不可以再修改该名称。

该表格包括以下列：

- **Select**

  选择要删除的行。

- **User Name**

  显示已创建的用户。

- **Group Name**

  选择待分配用户的组。

- **验证协议 (Authentication Protocol)**

  指定验证协议以为其存储密码。

  可使用以下设置：

  – None

  – MD5

  – SHA

- **加密协议 (Encryption Protocol)**

  指定是否应为使用 DES 算法的加密存储密码。仅在已选择验证协议后方可启用。

- **Authentication Password**

  在第一个输入框中输入身份验证密码。该密码必须至少 1 个字符，最多 32 个字符。

  说明

  密码的长度

  作为实现最优安全性的重要举措，我们建议，密码的最小长度为 6 个字符，且应包含特殊字符、大/小写字母和数字。

- **Authentication Password Confirmation**

  重复输入以确认密码。

- **Privacy Password**

  输入加密密码。该密码必须至少 1 个字符，最多 32 个字符。

说明

密码的长度

作为实现最优安全性的重要举措，我们建议，密码的最小长度为 6 个字符，且应包含特殊字符、大/小写字母和数字。

- **Privacy Password Confirmation**

  再次输入加密密码以进行确认。

- **Persistence**

  显示用户是否已分配至 SNMPv3 组。如果用户未分配至 SNMPv3 组，则不会触发自动保存，并且在重启设备之后会删除该组态的用户。

  – Yes

    用户已分配至 SNMPV3 组。

  – No

    用户未分配至 SNMPV3 组。

步骤

创建新用户

1. 在"User Name"输入框中输入新用户的名称。
2. 单击"Create"按钮。会在表中生成一个新条目。
3. 在"Group Name"中，选择新用户将所属的组。

   如果尚未创建组，则切换至"v3 Groups"页面并对该组进行设置。
4. 如果有必要对所选的组进行身份验证，请从"Authentication Protocol"中选择身份验证算法。

   在相关输入框中，输入身份验证密码并确认。

5. 如果已为该组指定了加密，请从"Privacy Protocol"中选择算法。在相应的输入框中，输入加密密码和确认密码。
6. 单击"Set Values"按钮。

删除用户

1. 启用要删除的行中的"Select"。
   对所有要删除的用户重复此步骤。
2. 单击"Delete"按钮。删除了相关条目。

6.5.13 系统时间

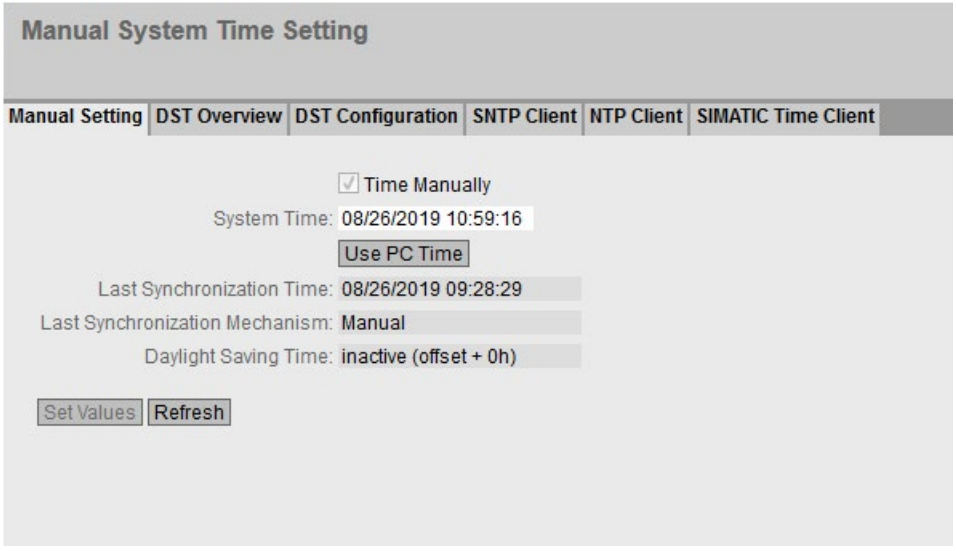
可以采用不同的方法来设置设备的系统时间。 每次只能采用一种方法。

激活一种方法后，将自动禁止之前激活的方法。

6.5.13.1 手动设置

手动设置系统时间

在此页面上设置系统本身的日期和时间。要使用此设置，请启用"手动设置时间"(Time Manually)。



说明

该页面包含以下框：

- **手动设置时间 (Time Manually)**
  启用手动时间设置。如果启用该选项，则可以编辑"System Time"输入框。
- **系统时间 (System Time)**
  按"MM/DD/YYYY HH:MM:SS"格式输入日期和时间。
  重启之后，时钟从 01/01/2000 00:00:00 开始。
- **使用 PC 时间 (Use PC Time)**
  单击该按钮以使用 PC 的时间设置。
- **上次同步时间 (Last Synchronization Time)**
  显示上一次时钟同步发生的时间。如果无法进行时钟同步，该框会显示"Date/time not set"。

- **上次同步机制 (Last Synchronization Mechanism)**

  显示上次时钟同步的执行方式。

  – 未设置 (Not set)

    未设置时间。

  – 手动 (Manual)

    手动设置时间

  – SNTP

    使用 SNTP 自动进行时钟同步

  – NTP

    使用 NTP 自动进行时钟同步

  – SIMATIC

    使用 SIMATIC 时钟帧自动进行时钟同步

- **夏令时 (DST) (Daylight Saving Time (DST))**

  显示夏令时切换是否已激活。

  – active (offset +1 h)

    系统时间已更改为夏令时；即增加了一小时。您可在 WBM 选择区域的顶部看到当前系统时间。

    当前时间（包括夏令时）显示在"系统时间"(System Time) 框中。

  – inactive (offset +0 h)

    不会更改当前系统时间。

步骤

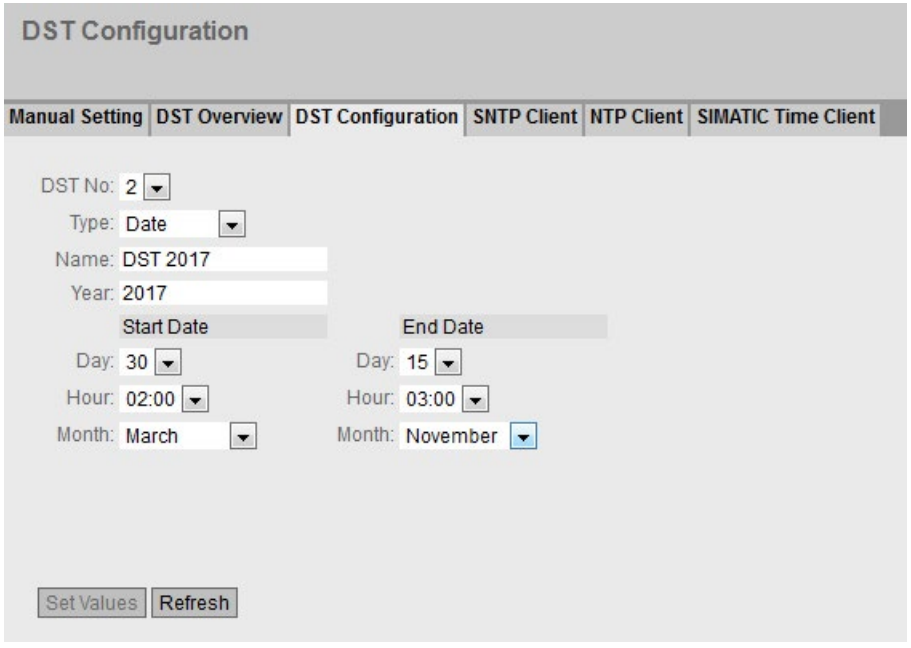
1. 启用"手动设置时间"(Time Manually) 选项。
2. 在"系统时间"(System Time) 输入框中，按"MM/DD/YYYY HH:MM:SS"格式输入日期和时间。
3. 单击"设置值"(Set Values) 按钮。
   将采用该日期和时间，并在"上次同步机制"(Last Synchronization Mechanism) 框中输入"手动"(Manual)。

6.5.13.2 DST 概述

在此页面中，您可以创建新的夏令时切换条目。

该表显示了现有条目的概览。

设置



- **选择 (Select)**

  选择要删除的行。

- **DST 编号 (DST No.)**

  显示条目编号。

  如果创建新的条目，会创建一个带有唯一编号的新行。

- **名称 (Name)**

  显示条目名称。

- **年 (Year)**

  显示条目的创建年份。

- **起始日期 (Start Date)**

  显示夏令时的起始月、日和时间。

- **结束日期 (End Date)**

  显示夏令时的结束月、日和时间。

- **重复日期 (Recurring Date)**

  对于"规则"(Rule) 类型的条目，将显示夏令时激活的时间段，其中包括周、日、月和时钟。

  对于"日期"(Date) 类型的条目，将显示"-"。

- **状态 (State)**

  显示条目的状态：

  – 启用 (Enabled)

    条目已正确创建。

  – 无效 (Invalid)

    新建条目，但起始和结束日期完全相同。

- **类型 (Type)**

  显示如何进行夏令时切换：

  – 日期 (Date)

    输入固定日期作为夏令时切换的时间。

  – 规则 (Rule)

    定义夏令时切换的规则。

步骤

创建条目

1. 单击"创建"(Create) 按钮。

   随即会在表中创建一个新条目。

2. 在"DST No"列中单击所需的条目。

   切换到"DST 组态"(DST Configuration) 页面。

3. 从"类型"(Type) 下拉列表中选择所需的类型。

   根据选择的类型，将提供各种设置。

4. 在"名称"(Name) 框中输入一个名称。

5. 如果已选择类型"日期"(Date)，则填写以下框。

   – 年

   – 日（对于起始日期和结束日期）

   – 小时（对于起始日期和结束日期）

   – 月（对于起始日期和结束日期）

6. 如果已选择类型"规则"(Rule)，则填写以下框。

   – 小时（对于起始日期和结束日期）

   – 月（对于起始日期和结束日期）

   – 周（对于起始日期和结束日期）

   – 日（对于起始日期和结束日期）

7. 单击"设置值"(Set Values) 按钮。

删除条目

1. 启用要删除的行中的"选择"(Select)。

2. 单击"删除"(Delete) 按钮。删除了相关条目。

6.5.13.3 DST 组态

可在此页面组态夏令时切换条目。切换到夏令时或标准时间后，可以按当地时区正确设置系统时间。

可定义夏令时切换规则，也可指定固定日期。

设置

说明

此页面包含的内容取决于您在"类型"(Type) 框中做出的选择。
始终都会显示"DST 编号"(DST No.)、"类型"(Type) 和"名称"(Name) 框。

- **DST 编号 (DST No.)**

  选择条目的类型。

- **类型 (Type)**

  选择夏令时切换方式：

  – 日期 (Date)

    您可以设置固定日期作为夏令时切换的时间。

    此设置适用于没有夏令时切换管理规则的地区。

  – 规则 (Rule)

    可以定义夏令时切换的规则。

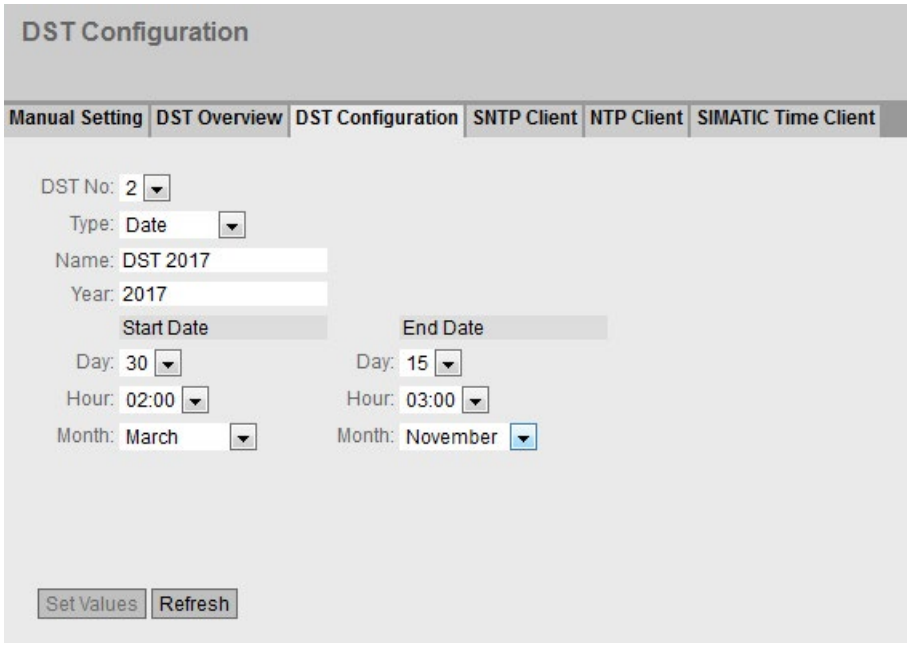
    此设置适用于夏令时起始和结束日期始终为特定工作日的地区。

- **名称 (Name)**

  输入条目名称。

  名称最长为 16 个字符。

选择**"日期"(Date) 时的设置**


DST Configuration
Manual Setting
DST Overview
DST Configuration
SNTP Client
NTP Client
SIMATIC Time Client
DST No: 2
Type: Date
Name: DST 2017
Year: 2017
Start Date
End Date
Day: 30
Hour: 02:00
Month: March
Day: 15
Hour: 03:00
Month: November
Set Values
Refresh

可设置夏令时开始和结束的固定日期。

- **年 (Year)**

  输入夏令时切换的年份。

- **起始日期 (Start Date)**

  输入以下值作为夏令时的起点：

  – 日 (Day)

    指定日期。

  – 时 (Hour)

    指定小时。

  – 月 (Month)

    指定月份。

- **结束日期 (End Date)**

  输入以下值作为夏令时的终点：

  – 日 (Day)

    指定日期。

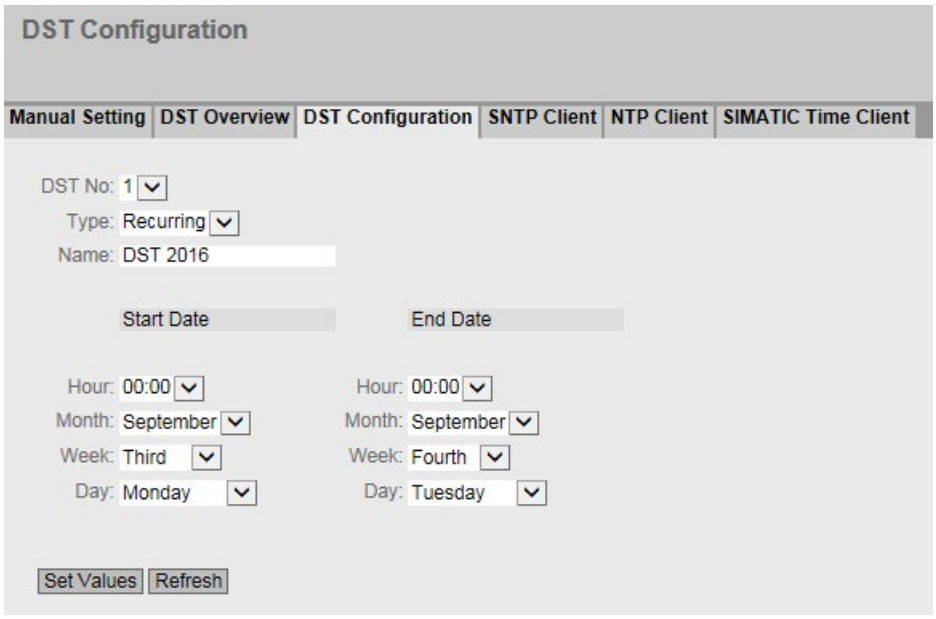
  – 时 (Hour)

    指定小时。

  – 月 (Month)

    指定月份。

选择**"规则"(Rule) 时的设置**



可以创建夏令时切换规则。

- **起始日期 (Start Date)**

  输入以下值作为夏令时的起点：

  – 时 (Hour)

    指定小时。

  – 月 (Month)

    指定月份。

  – 周 (Week)

    指定周。

    可以选择一个月中的第 1 周到第 5 周或最后一周。

  – 日 (Day)

    指定工作日。

- **结束日期 (End Date)**

  输入以下值作为夏令时的终点：

  – 时 (Hour)

    指定小时。

  – 月 (Month)

    指定月份。

  – 周 (Week)

    指定周。

    可以选择一个月中的第 1 周到第 5 周或最后一周。

  – 日 (Day)

    指定工作日。

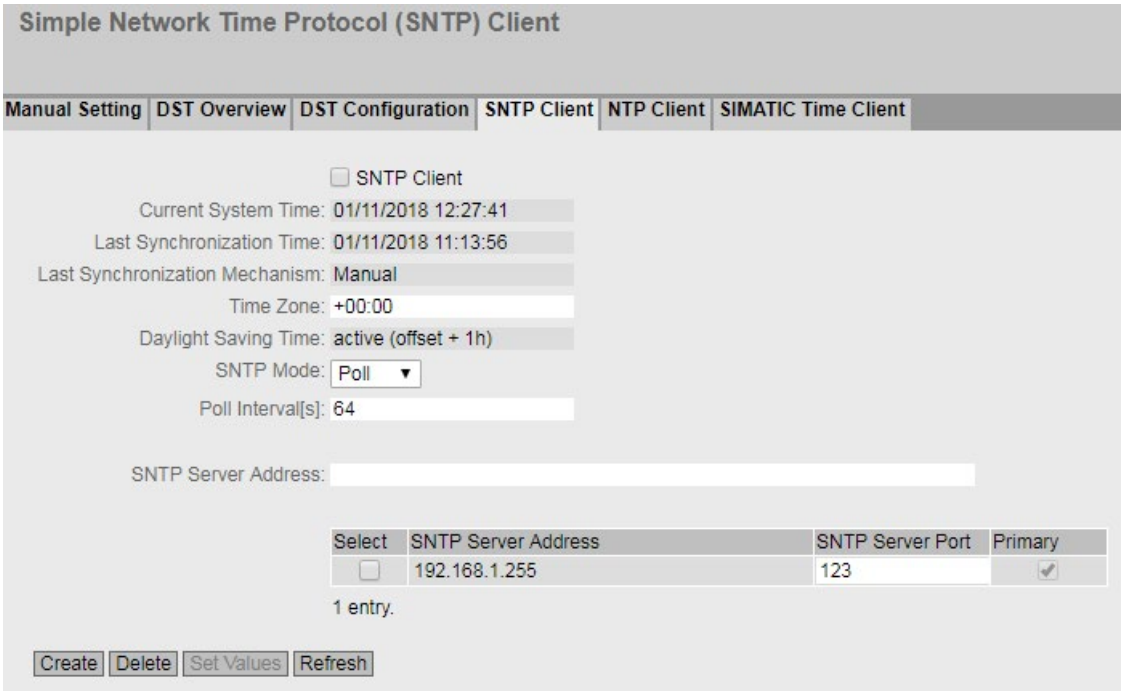
6.5.13.4 SNTP 客户端

网络中的时间同步

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

说明

为避免时间跳跃，需确保网络中只有一台时间服务器。



说明

该页面包含以下框：

- **SNTP 客户端 (SNTP Client)**
  启用或禁用使用 SNTP 自动进行时钟同步。
- **当前系统时间 (Current System Time)**
  显示由设备接收的当前日期和当前标准时间。如果指定了时区，则会相应调整时间信息。

- **上次同步时间 (Last Synchronization Time)**
  显示上一次时钟同步发生的时间。
- **上次同步机制 (Last Synchronization Mechanism)**
  显示上次时钟同步的执行方式。提供以下方法：
  - 未设置 (Not set)
    未设置时间。
  - 手动 (Manual)
    手动设置时间
  - SNTP
    使用 SNTP 自动进行时钟同步
  - NTP
    使用 NTP 自动进行时钟同步
  - SIMATIC
    使用 SIMATIC 时钟帧自动进行时钟同步
- **时区 (Time Zone)**
  在此框中，以"+/- HH:MM"的格式输入所使用的时区。时区与 UTC 标准世界时间相关。

  相应调整"当前系统时间"(Current System Time) 框中的时间。
- **夏令时 (DST) (Daylight Saving Time (DST))**
  显示夏令时切换是否已激活。
  - active (offset +1 h)

    系统时间已更改为夏令时；即增加了一小时。您可在 WBM 选择区域的顶部看到当前系统时间。

    当前时间（包括夏令时）显示在"系统时间"(System Time) 框中。
  - inactive (offset +0 h)
    不会更改当前系统时间。

- **SNTP 模式 (SNTP Mode)**
  从下拉列表中选择同步模式。可以使用下列同步类型：
  - Listen
    在该模式下，设备处于被动状态，且会接收传递时钟的 SNTP 帧。在该模式下，输入框"SNTP 服务器地址"(SNTP Server Address)、"SNTP 服务器端口"(SNTP Server Port) 中的设置没有影响。
    在此模式下，仅支持 IPv4 地址。
  - Poll
    如果选择该模式，则会显示输入框"轮询间隔[s]"(Poll Interval[s])，以便进一步进行组态。在该模式下，需考虑输入框"SNTP 服务器地址"(SNTP Server Address) 和"SNTP 服务器端口"(SNTP Server Port) 中的设置。若使用该同步类型，设备会激活，并向 SNTP 服务器发送时间查询。
    在此模式下，支持 IPv4 和 IPv6 地址。
- **轮询间隔[s] (Poll Interval[s])**
  在此输入两次时间查询之间的时间间隔。在此框中输入查询间隔的秒数值。可能的值介于 16 到 16284 秒之间。
- **SNTP 服务器地址 (SNTP Server Address)**
  输入 SNTP 服务器的 IP 地址或 FQDN（完全限定域名，Fully Qualified Domain Name）。
- **SNTP 服务器端口 (SNTP Server Port)**
  输入 SNTP 服务器的端口。
  可能的端口包括：
  - 123（标准端口）
  - 1025 到 36564
- **主 (Primary)**
  为第一个创建的 SNTP 服务器设置此复选标记。如果已创建多个 SNTP 服务器，将首先查询主服务器。

步骤

1. 单击"SNTP 客户端"(SNTP Client) 复选框以启用自动时间设置。
2. 在"时区"(Time Zone) 输入框中输入当地时间与世界时间 (UTC) 的时差。由于 SNTP 服务器始终发送 UTC 时间，因此输入格式为"+/-HH:MM"（例如，对于 CEST 是 +02:00）。该时间随后会被重新计算并根据指定的时区显示为当地时间。可以在"系统 > 系统时间 > DST 概述"(System > System Time > DST Overview) 和"系统 > 系统时间 > DST 组态"(System > System Time > DST Configuration) 页面组态夏令时切换。在"时区"(Time Zone) 输入框输入时，还需要考虑到这一点。
3. 从"SNTP 模式"(SNTP Mode) 下拉列表中选择下列选项之一：
   - Poll

     对于该模式，需要组态以下内容：
     - 时区时差（第 2 步）
     - 查询间隔（第 4 步）
     - 时间服务器（第 5 步）
     - 端口（第 7 步）
     - 通过第 8 步完成组态。
   - Listen

     对于该模式，需要组态以下内容：
     - 与服务器发送的时间之间的时差（第 2 步）
     - 通过第 8 步完成组态。
4. 在"轮询间隔[s]"(Poll Interval[s]) 输入框中，输入以秒为单位的时间值，经过这段时间后，会向时间服务器发送新的时间查询。
5. 在"SNTP 服务器地址"(SNTP Server Address) 输入框中，输入 SNTP 服务器的 IP 地址或 FQDN，该服务器的帧将用于同步时钟。
6. 单击"创建"(Create) 按钮。

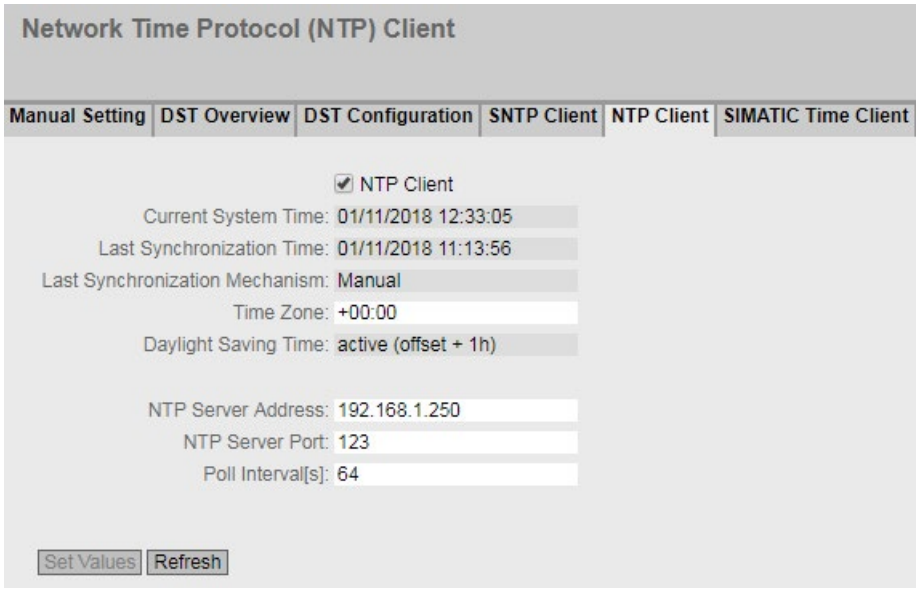
   将在表中为 SNTP 服务器插入一个新行。

7. 在"SNTP 服务器端口"(SNTP Server Port) 列中，输入可用来使用 SNTP 服务器的端口。仅当输入 SNTP 服务器的 IPv4 地址或 FQDN 名称之后，才可以修改该端口。
8. 单击"设置值"(Set Values) 按钮将更改传输到设备。

6.5.13.5 NTP 客户端

使用 NTP 自动设置时钟

如果需要使用 NTP 进行时钟同步，可以在此做相关设置。



说明

该页面包含以下框：

- **NTP 客户端 (NTP Client)**
  选中此复选框可启用使用 NTP 自动进行时钟同步。
- **当前系统时间 (Current System Time)**
  显示由设备接收的当前日期和当前标准时间。如果指定了时区，则会相应调整时间信息。

- **上次同步时间 (Last Synchronization Time)**
  显示上一次时钟同步发生的时间。
- **上次同步机制 (Last Synchronization Mechanism)**
  显示上次时间同步的执行方式。以下方法可用：
  - 未设置 (Not set)
    未设置时间。
  - 手动 (Manual)
    手动设置时间
  - SNTP
    使用 SNTP 自动进行时钟同步
  - NTP
    使用 NTP 自动进行时钟同步
  - SIMATIC
    使用 SIMATIC 时钟帧自动进行时钟同步
- **时区 (Time Zone)**
  在此框中，以"+/- HH:MM"的格式输入所使用的时区。时区与 UTC 标准世界时间相关。

  相应调整"当前系统时间"(Current System Time) 框中的时间。
- **夏令时 (DST) (Daylight Saving Time (DST))**
  显示夏令时切换是否已激活。
  - active (offset +1 h)

    系统时间已更改为夏令时；即增加了一小时。您可在 WBM 选择区域的顶部看到当前系统时间。

    当前时间（包括夏令时）显示在"系统时间"(System Time) 框中。
  - inactive (offset +0 h)
    不会更改当前系统时间。

- **NTP 服务器地址 (NTP Server Address)**
  输入 NTP 服务器的 IP 地址或 FQDN（完全限定域名）。
- **NTP 服务器端口 (NTP Server Port)**
  输入 NTP 服务器的端口。
  可能的端口包括：
  – 123（标准端口）
  – 1025 到 36564
- **轮询间隔[s] (Poll Interval[s])**
  在此字段输入两次时间查询之间（查询间隔）的时间间隔（以秒为单位）。可能的值介于 64 到 1024 秒之间。

步骤

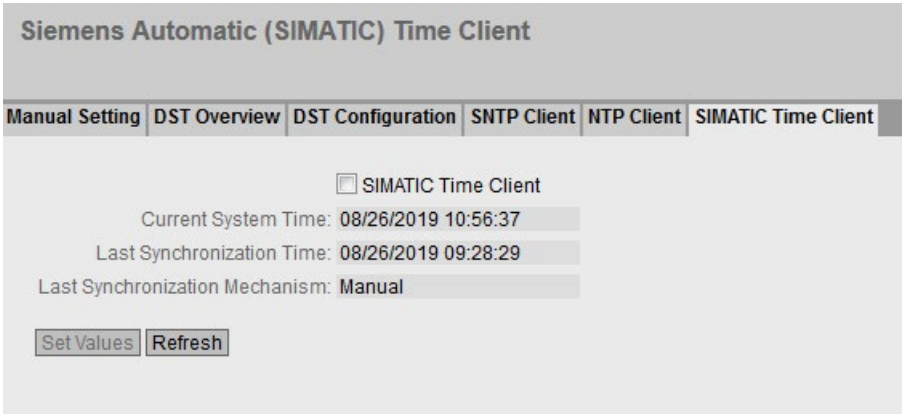
1. 单击"NTP 客户端"(NTP Client) 复选框，启用使用 NTP 自动进行时间设置。
2. 在以下框中输入需要的值：
   – 时区
   – NTP 服务器的 IP 地址或 FQDN
   – NTP 服务器端口
   – 查询间隔
3. 单击"设置值"(Set Values) 按钮。

6.5.13.6 SIMATIC Time Client

通过 SIMATIC 时间客户端设置时间

说明

为避免时间跳跃，需确保网络中只有一台时间服务器。



说明

该页面包含以下框：

- **SIMATIC Time Client**
  选中此复选框可启用设备作为 SIMATIC 时间客户端。
- **当前系统时间 (Current System Time)**
  显示当前系统时间。
- **上次同步时间 (Last Synchronization Time)**
  显示上一次时钟同步发生的时间。

- **上次同步机制 (Last Synchronization Mechanism)**
  显示上次时钟同步的执行方式。提供以下方法：
  - 未设置 (Not set)
    未设置时间。
  - 手动 (Manual)
    手动设置时间
  - SNTP
    使用 SNTP 自动进行时钟同步
  - NTP
    使用 NTP 自动进行时钟同步
  - SIMATIC
    使用 SIMATIC 时钟帧自动进行时钟同步

步骤

1. 单击"SIMATIC Time Client"复选框可启用 SIMATIC Time Client。
2. 单击"设置值"(Set Values) 按钮。

6.5.14 自动注销

设置自动注销

在该页面，设置在用户不活动后自动从 WBM 或 CLI 注销所需经过的时间。

如果您已经自动注销，则需要再次登录。

说明

不从 CLI 自动注销

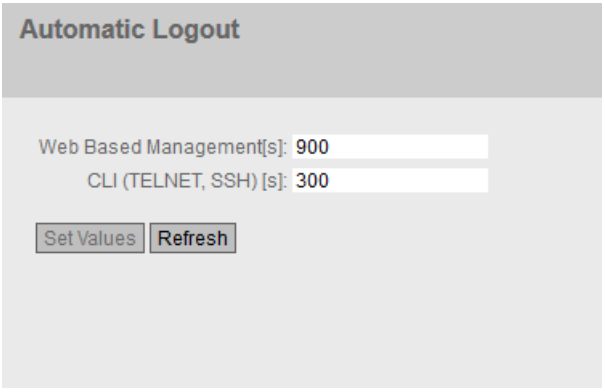
如果在设置时间后未终止连接，请检查 Telnet 客户端上"保持连接"的设置。

如果"保持连接"间隔时间短于所组态的时间，则即使未传输任何用户数据也将保持连接。例如，为自动注销设置了 300 秒，为"保持连接"功能设置了 120 秒。在这种情况下，每 120 秒发送一次数据包，以保持连接不中断。

- 关闭"保持连接"功能（间隔时间 = 0）

  或

- 将时间间隔设置得足够长，以便在不传送数据时终止下级连接。



步骤

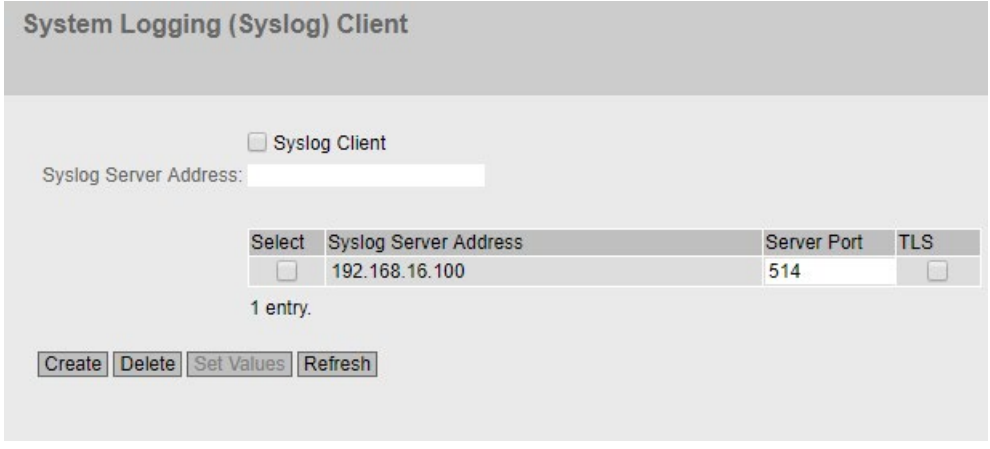
1. 在"Web Base Management [s]"输入框中输入值 60 到 3600 秒。如果输入值 0，则禁用自动注销。
2. 在"CLI (TELNET, SSH) [s]"输入框中输入值 60 到 600 秒。如果输入值 0，则禁用自动注销。
3. 单击"设置值"(Set Values) 按钮。

6.5.15 Syslog 客户端

在此页面中组态 Syslog 客户端。可将 Syslog 消息以不加密或加密的形式发送到 Syslog 服务器。

发送 Syslog 消息的要求

- 已启用 Syslog 客户端。
- 在"系统 > 事件 > 组态"(System > Events > Configuration) 中，已针对相关事件激活"Syslog"。
- 接收 Syslog 消息的网络中存在 Syslog 服务器。
- 已组态 Syslog 服务器的地址。



描述

该页面包含以下框：

- **Syslog 客户端 (Syslog Client)**

  在设备上启用或禁用 Syslog 客户端。

- **Syslog 服务器地址 (Syslog Server Address)**

  输入 Syslog 服务器的 IP 地址、FQDN（完全限定域名，Fully Qualified Domain Name）或主机名。

该表包含以下各列

- **选择 (Select)**

  选择要删除的行。

- **Syslog 服务器地址 (Syslog Server Address)**

  显示 Syslog 服务器的 IP 地址、FQDN（完全限定域名，Fully Qualified Domain Name）或主机名。

- **服务器端口 (Server Port)**

  输入要使用的 Syslog 服务器端口。

- **TLS**

  – 启用 (Enabled)

    基于 TCP 以 TLS 加密形式发送 syslog 消息。

  – 禁用 (Disabled)

    基于 UDP 以非加密形式发送 Syslog 消息。

步骤

启用功能

1. 选择"Syslog 客户端"(Syslog Client) 复选框。
2. 单击"设置值"(Set Values) 按钮。

创建新条目

1. 在"Syslog 服务器地址"(Syslog Server Address) 输入框中，输入 Syslog 消息所发送到的 Syslog 服务器地址。
2. 单击"创建"(Create) 按钮。将在表中插入一个新行。
3. 在"服务器端口"(Server Port) 输入框中，输入服务器端口号。
4. 单击"设置值"(Set Values) 按钮。

说明
服务器端口的默认设置是 514。

更改条目

1. 删除条目。
2. 创建新条目。

删除条目

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

6.5.16 故障监视

6.5.16.1 电源

监视电源的设置

组态是否通过消息系统监视电源。根据硬件型号，会有一个或两个电源连接器（电源 1/电源 2）和一个 PoE 电源。带冗余电源时，应对每个单独的进线线路分别组态监视。

当所监视的连接（电源线路 1、电源线路 2 或 PoE）未通电或所施加的电压过低时，消息系统将发出故障信号。

说明

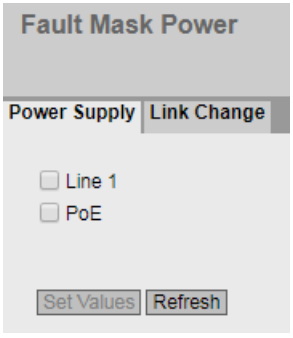
设备的操作说明中包含允许的工作电压限值。

如果出现故障，设备的错误 LED 将点亮。当前未决错误显示在"信息 > 错误"(Information > Errors) 中。

此外，在结果日志表中输入对应的错误消息。事件日志表的内容显示在"信息 > 日志表> 事件日志"(Information > Log Tables> Event Log) 中。

说明

此 WBM 页面在 SCALANCE W786-2 SFP 上不可用。



步骤

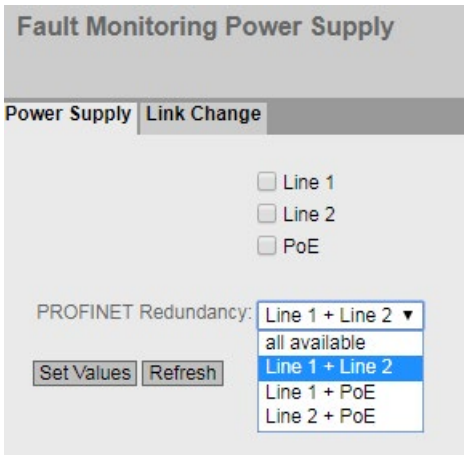
1. 单击要监视的线路名称前的复选框，启用或禁用监视功能。
2. 单击"设置值"(Set Values) 按钮。

通过 PROFINET 监视冗余电源

对于以下设备，还可组态要通过 PROFINET 监视的电源：

- SCALANCE W788-x（RJ-45 型号）
- SCALANCE W748-1 RJ-45

- SCALANCE W774-1（RJ-45 和 M12 型号）
- SCALANCE W734-1 RJ-45



步骤

1. 单击要监视的线路名称前的复选框，启用或禁用监视功能。
2. 从"PROFINET 冗余"(PROFINET Redundancy) 下拉列表中，选择待 PROFINET 监视的冗余电源的所需条目。
3. 单击"设置值"(Set Values) 按钮。

6.5.16.2 Link Change

连接状态变化的故障监视组态

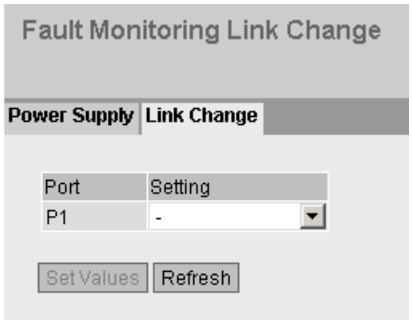
在此页面上组态出现网络连接状态变化时是否触发错误信息。

如果启用连接监视，则发出错误信号

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

如果出现故障，设备的错误 LED 将点亮。当前未决错误显示在"信息 > 错误"(Information > Errors) 中。

此外，在结果日志表中输入对应的错误消息。事件日志表的内容显示在"信息 > 日志表> 事件日志"(Information > Log Tables> Event Log) 中。



说明

该表包括以下列：

- **Port**

  显示可用端口。

- **设置 (Setting)**

  从下拉列表中选择设置。可做以下选择：

  – Up

    当端口变为激活状态时触发错误处理。

    （从"Link down"到"Link up"）

  – Down

    当端口变为未激活状态时触发错误处理。

    （从"Link up"到"Link down"）

  – "-"（禁用）

    不触发错误处理。

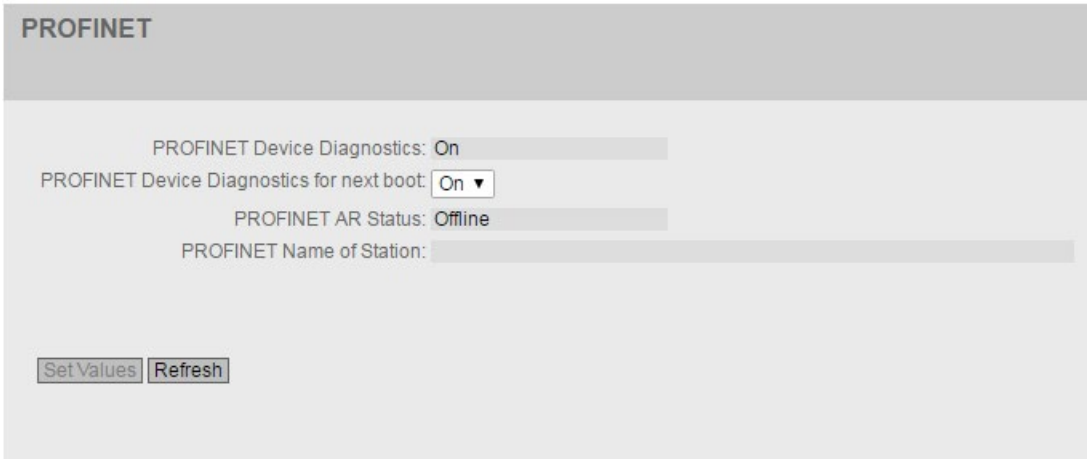
步骤

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

6.5.17 PROFINET

PROFINET 的设置

此页面显示 PROFINET AR 状态和设备名称。



显示框说明

该页面包含以下框：

- **PROFINET 设备诊断 (PROFINET Device Diagnostics)**

  显示启用（"开启"(On)）还是禁用（"关闭"(Off)）PROFINET。

- **下次启动时的 PROFINET 运行模式 (PROFINET runtime mode for next boot)**

  设置下次设备重启后是启用（"开启"(On)）还是禁用（"关闭"(Off)）PROFINET。

说明

PROFINET 和 EtherNet/IP

开启 PROFINET 时，EtherNet/IP 将关闭。PROFINET 和 EtherNet/IP 的切换对 DCP 无影响。

说明

PROFINET AR 状态

如果已建立 PROFINET 连接，即 PROFINET AR 状态为"在线"，则无法禁用 PROFINET。

- **PROFINET AR 状态 (PROFINET AR Status)**

  此框显示了 PROFINET 连接的状态；也就是说，设备是与 PROFINET 控制器之间的连接是处于"在线"(Online) 状态还是"离线"(Offline) 状态。
  在此处，在线即表示存在到 PROFINET IO 控制器的连接，即它的组态数据已经下载到设备并且设备可以向 PROFINET IO 控制器发送状态数据。在这种称为"正在进行数据交换"的状态下，无法对 PROFINET 控制器的参数集进行组态。

- **站的 PROFINET 名称 (PROFINET Name of Station)**

  此框根据 STEP 7 的 HW Config 中的组态显示 PROFINET 设备名称。

说明

带有两个以太网端口的设备

对于带有两个以太网接口的设备，仅接口 P1 可用于 PROFINET 组态，原因是 LLPD 帧只能通过接口 1 进行发送和接收。LLPD 帧在接口 P2 处会被阻止且无法在两个接口之间进行转发。

这适用于以下设备：

- SCALANCE W786-2 SFP
- SCALANCE W774-1 RJ45
- SCALANCE W774-1 M12 EEC
- SCALANCE W778-1 M12
- SCALANCE W778-1 M12 EEC
- SCALANCE W734-1 RJ-45
- SCALANCE W738-1 M12

SCALANCE W700 和 STEP 7

如果满足以下要求，则可在 STEP 7 中组态以太网接口：

- 采用 HSP0107 的 STEP 7 V13 Update 3 或
- 采用 GSDML 版本 2.31 的 STEP7 版本 5.5.4

还可以使用诊断功能。但无法使用 STEP 7 来组态 WLAN 接口。

客户端设备的 PROFINET

如果某客户端将被用作 PROFINET 设备，则必须按以下方式指定该客户端的 MAC 地址（MAC 模式）：

- 自身 (Own)

  在设备以外的网络中，只能进行 IP 通信，而无法实现 PROFINET。

- 第 2 层隧道 (Layer 2 Tunnel)

  客户端及其下游设备均可用作 PROFINET 设备。

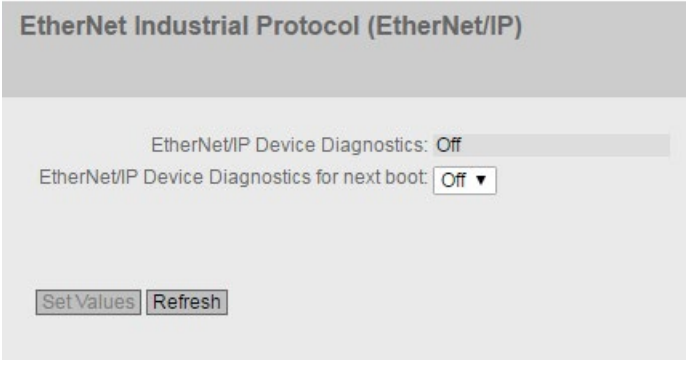
说明

如果将客户端的 MAC 模式设置为"自动"(Automatic) 或"手动"(Manual)，则该设备便不能被用作 PROFINET 设备。

6.5.18 EtherNet/IP

EtherNet/IP

在此页面上组态 EtherNet/IP 的模式。



说明

带有两个以太网端口的设备

对于带有两个以太网接口的设备，只能将一个接口（P1 或 P2）用于以太网组态。
这适用于以下设备：

- SCALANCE W786-2 SFP
- SCALANCE W774-1 RJ45
- SCALANCE W774-1 M12 EEC
- SCALANCE W778-1 M12
- SCALANCE W778-1 M12 EEC
- SCALANCE W734-1 RJ-45
- SCALANCE W738-1 M12

说明

该页面包含以下框：

- **EtherNet/IP 设备诊断 (EtherNet/IP Device Diagnostics)**

  显示启用（"On"）还是禁用（"Off"）EtherNet/IP。

- **下一次启动的 EtherNet/IP 设备诊断 (EtherNet/IP Device Diagnostics for next boot)**

  设置下次设备重启后是启用（"On"）还是禁用（"Off"）EtherNet/IP。

说明

EtherNet/IP 和 PROFINET

开启 EtherNet/IP 时，PROFINET 将关闭。EtherNet/IP 和 PROFINET 的切换对 DCP 无影响。

说明

PROFINET AR 状态

如果已建立 PROFINET 连接，即 PROFINET AR 状态为"Online"，则无法启用 EtherNet/IP。

6.5.19 PLUG

6.5.19.1 组态

注意

操作期间请勿插拔 C-PLUG/KEY-PLUG！

只允许在设备关闭后取出或插入 PLUG。

设备会以一秒为间隔检查是否已插入 PLUG。如果检测到 PLUG 被拔出，则会重启。如果在设备中插入了有效 KEY-PLUG，设备会在重启后切换到预定的错误状态。在这种情况下，SCALANCE W 会禁用可用的无线接口。

若设备先前组态了 PLUG，则该设备在缺少此 PLUG 的情况下无法继续使用。为再次使用该设备，请将设备复位为出厂设置。

C-PLUG/KEY-PLUG 组态的相关信息

此页面提供了有关 C-PLUG 或 KEY-PLUG 上存储的组态的详细信息。还可以将 PLUG 复位为"出厂默认设置"或向其中加载新内容。

说明

只有在单击"设置值"(Set Values) 按钮后，才会执行此操作。

此操作无法撤销。

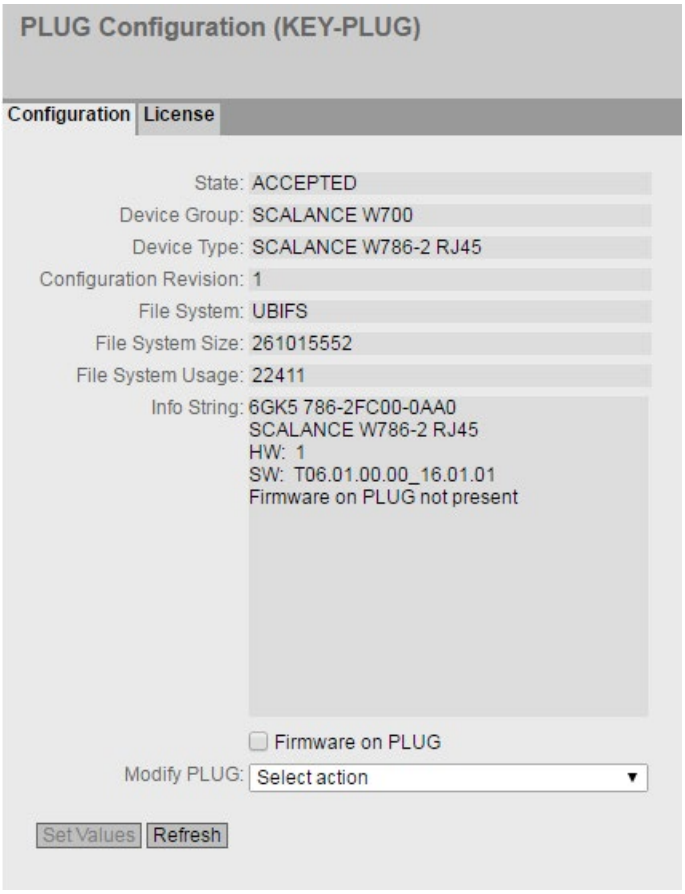
如果进行选择之后您决定不执行此功能，则单击"刷新"(Refresh) 按钮。随后将再次从设备中读取此页面数据，并会取消选择。

说明

插入的 PLUG 组态与先前版本不兼容

在安装先前版本的过程中，组态数据可能丢失。在这种情况下，安装固件后，设备会使用出厂设置启动。如果此时设备中插入了 PLUG，则重启后，由于 PLUG 仍具有之前最新固件的组态数据，因此状态为"NOT ACCEPTED"。此时，您可以返回之前的最新固件而不丢失任何组态数据。

如果不再需要 PLUG 上的原始组态，则可使用"System > PLUG"手动删除或重写 PLUG。



描述

该表格包括以下行：

- **状态 (State)**

  显示 C-PLUG 的状态。可能的方式包括：

  – ACCEPTED

    设备中存在具有有效且适当组态的 C-PLUG。

  – NOT ACCEPTED

    插入的 C-PLUG 上的组态无效或不兼容。

– NOT PRESENT

设备中未插入 C-PLUG。

– FACTORY

C-PLUG 已插入，但不包含组态。如果在操作过程中对 C-PLUG 进行了格式化，则也会显示此状态。

– MISSING

未插入 C-PLUG。将在需要许可证的设备上组态功能。

- **设备组 (Device Group)**

  显示先前使用 C-PLUG 或 KEY-PLUG 的 SIMATIC NET 产品线。

- **设备类型 (Device Type)**

  显示先前使用 C-PLUG 或 KEY-PLUG 的产品线的设备类型。

- **组态版本 (Configuration Revision)**

  组态结构的版本。此信息与设备支持的组态选项相关，而与具体的硬件配置无关。因此，在添加或移除附加组件（模块或扩展器）时，此版本信息不会改变，但是如果更新固件，则该信息可能会发生改变。

- **文件系统 (File System)**

  显示 PLUG 上的文件系统类型。

注意
新文件系统 UBI 自 SCALANCE W 固件版本 2.0 起，用于 C-PLUG 或 KEY-PLUG 的标准文件系统为 UBI。如果在这类设备中检测到了带有先前文件系统 IECP 的 C-PLUG，则会将此 C-PLUG 格式化为 UBI 文件系统，并将数据重写到 C-PLUG 中。 对于 SCALANCE W，固件更新至 V2.0 后文件系统也会发生变化。若之后降级到相应固件的先前版本，则会引发故障。固件既无法读取也无法写入 C-PLUG 或 KEY-PLUG，甚至无法"恢复为出厂默认设置"(Restore factory defaults)。

注意
更换带固件为 V1.0 的 C-PLUG 的设备 工厂中的设备装有固件 V1.0。已使用该固件创建 C-PLUG。该工厂中的设备出现故障并需要更换为新设备。出现故障的设备只能更换为装有固件 V6.0 或更旧版本的设备。 在需要时，可在更换设备后，将其升级到当前的固件版本。

- **文件系统大小 [字节] (File System Size [bytes])**

  显示 PLUG 上文件系统的最大存储容量。

- **文件系统利用率 [字节] (File System Usage [bytes])**

  显示 PLUG 上文件系统的存储器使用情况。

- **信息字符串 (Info String)**

  显示有关之前使用该 PLUG 的设备的所有附加信息，例如：订货号、型号标识以及硬件与软件的版本。显示的软件版本与上次更改了组态的版本相对应。状态为 "NOT ACCEPTED"时，将显示有关问题原因的更多信息。

  如果已将 PLUG 组态为 PRESET PLUG，则该信息字符串会作为附加信息显示在此处的第一行。有关创建和使用 PRESET PLUG 的更多详细信息，请参见"维护 (页 547)"部分。

- **PLUG 上的固件 (Firmware on PLUG)**

  默认启用该功能。

  启用后，固件存储在 PLUG 上。这意味着可通过 PLUG 自动进行固件升级/降级。

- **修改 PLUG (Modify PLUG)**

  从该下拉列表中选择所需的设置。用户可使用以下选项更改 C-PLUG 或 KEY-PLUG 上的组态：

  – 将当前组态写入 PLUG (Write Current Configuration to the PLUG)

    仅当 PLUG 的状态为"未接受"(NOT ACCEPTED) 或"出厂设置"(FACTORY) 时，此选项才可用。

    会将设备内部闪存中的组态复制到 PLUG。

  – 将 PLUG 恢复为出厂默认设置 (Erase PLUG to factory default)

    删除 PLUG 中的所有数据并触发低级格式化功能。

步骤

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

6.5.19.2 许可证

注意
操作期间请勿拔出或插入 C-PLUG/KEY-PLUG！ 只有在设备关闭情况下才可以插拔 PLUG。 设备以 1 秒的间隔检查 PLUG 是否存在。如果检测到 PLUG 被拔出，则会重启。如果在设备中插入了有效 KEY-PLUG，设备会在重启后切换到预定的错误状态。在这种情况下，SCALANCE W 会禁用可用的无线接口。 若设备先前组态了 PLUG，则该设备再无法在缺少此 PLUG 的情况下使用。为再次使用该设备，请将设备重置为出厂设置。

说明

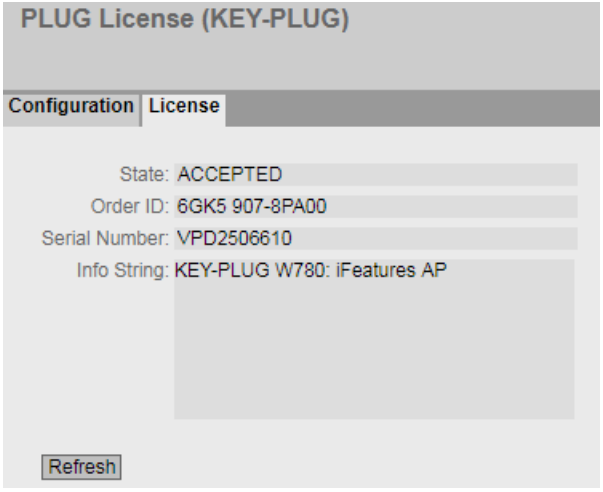
插入的 PLUG 组态与先前版本不兼容

在安装先前版本的过程中，组态数据可能丢失。在这种情况下，安装固件后，设备会使用出厂设置启动。如果此时设备中插入了 PLUG，则重启后，由于 PLUG 仍具有之前最新固件的组态数据，因此状态为"NOT ACCEPTED"。这样，您便可以返回之前的最新固件而不丢失任何组态数据。

如果不再需要 PLUG 上的原始组态，则可使用"系统 > PLUG"(System > PLUG) 手动删除或重写 PLUG。

KEY-PLUG 许可证的相关信息

C-PLUG 只能存储设备的组态。除组态外，KEY-PLUG 还包含一个可启用 SIMATIC NET 设备的特定功能的许可证。



显示框说明

- **状态 (State)**

  显示 KEY-PLUG 的状态。可能的状态包括：

  – ACCEPTED

    设备中存在具有有效且适当组态的 KEY-PLUG。

  – NOT ACCEPTED

    插入的 KEY PLUG 上的组态无效或不兼容。

  – NOT PRESENT

    设备中未插入 KEY-PLUG。

  – MISSING

    插入了 KEY-PLUG。将在需要许可证的设备上组态功能。

  – WRONG

    插入的 KEY-PLUG 不适用于设备。

  – UNKNOWN

    KEY-PLUG 的内容未知。

  – DEFECTIVE

    KEY-PLUG 的内容包含错误。

- **部件编号** (Article number)
- 显示 KEY-PLUG 的部件编号。KEY-PLUG 可用于各种功能增强和各种目标系统。
- **序列号 (Serial number)**

  显示 KEY-PLUG 的序列号。

- **信息字符串 (Info String)**

  显示有关之前使用该 KEY-PLUG 的设备的所有附加信息，例如：部件编号、型号标识以及硬件与软件的版本。显示的软件版本与上次更改了组态的版本相对应。状态为"NOT ACCEPTED"时，将显示有关问题原因的更多信息。

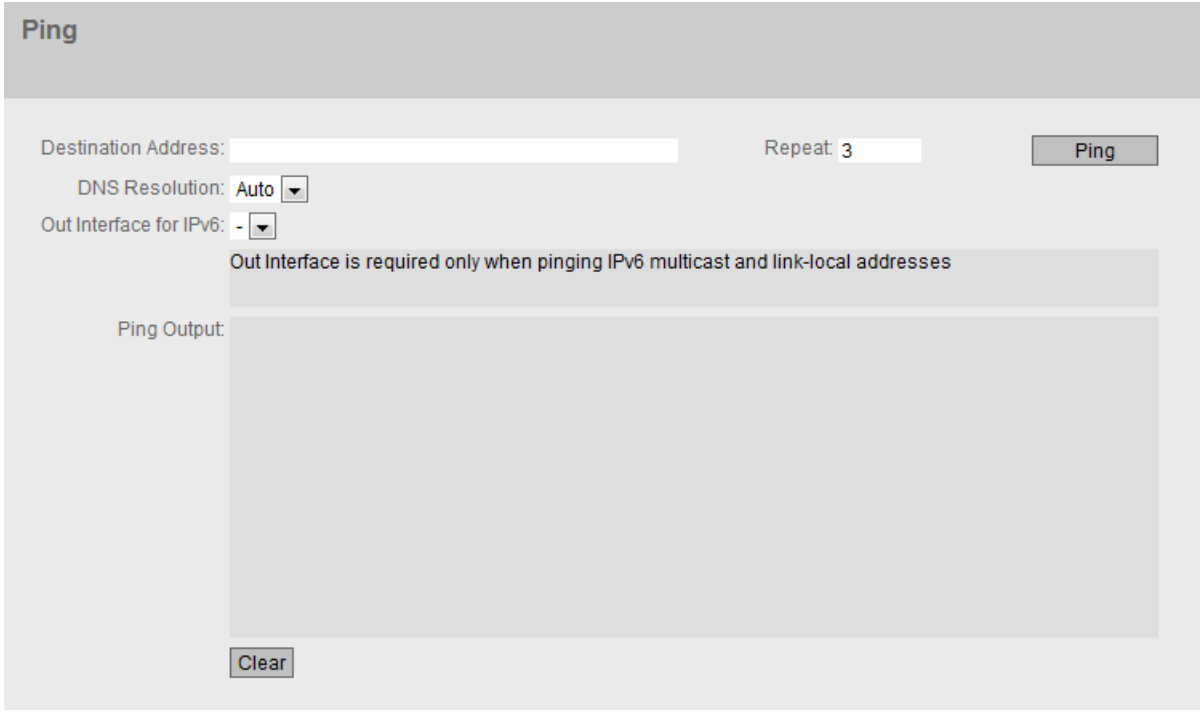
说明

保存组态时，将同时保存当时设备中是否插入了 KEY-PLUG 的信息。之后，只有插入了具有相同部件编号/许可证的 KEY-PLUG 时，该组态才起作用。这与是否组态了 iFeatures 无关。

6.5.20 Ping

IP 网络中地址的可达性

通过 ping 功能，可检查某一 IP 地址在网络中是否可到达。



说明

该页面包含以下框：

- **目标地址 (Destination Address)**

  输入设备的 IPV4、IPv6 地址或 FQDN（完全限定域名）。

- **重复** (Repeat)

  输入 ping 请求的数量。

- **DNS 分辨率**

  选择要在其中解析已输入的 FQDN 的 IP 地址类型。

  – 自动

    在该模式中，会自动选择 IP 地址类型。

  – IPv4

    将在 IPv4 地址中解析已输入的 FQDN。

  – IPv6

    将在 IPv6 地址中解析已输入的 FQDN。

- **IPv6 的输出接口** (Out Interface for IPv6)

  仅在目标地址为组播或链路本地地址时才要求做出此选择。

  – "-"（出厂设置）

  – 选择相应的 IPv6 接口。

- **Ping**

  单击该按钮可启动 ping 功能。

- **Ping 输出** (Ping Output)

  该框会显示 ping 功能的输出。

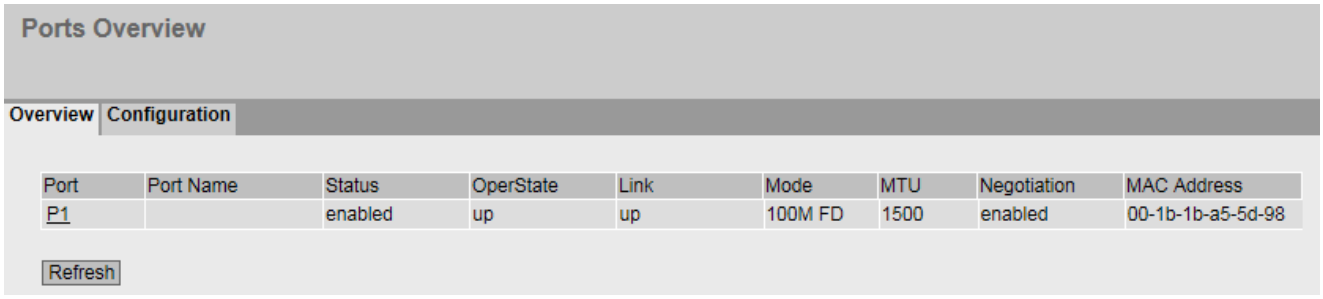
6.6 "接口"菜单

6.6.1 Ethernet

6.6.1.1 概述

端口组态概述

此页面显示设备所有端口的数据传送组态。无法对该页面上的任何内容进行组态。



说明

该表包括以下列：

- **端口 (Port)**

  显示可组态端口。如果单击该链接，相应组态页便会打开。

- **端口名称 (Port name)**

  显示端口的名称。

- **状态 (State)**

  显示端口是开启还是关闭状态。数据通信只能通过已启用的端口进行。

- **OperState**

  显示当前运行状态。运行状态取决于已组态的"状态"(Status) 和"链接"(Link)。可用选项如下：

  – "有效"(up)
    已将端口的状态组态为"启用"(enabled)，且端口与网络之间存在有效的连接。

  – "无效"(down)
    已将端口的状态组态为"禁用"(disabled) 或"链路中断"(Link down)，或者端口不存在连接。

- **链路 (Link)**

  显示网络连接状态。有以下连接状态：

  – up

    端口与网络之间存在有效链路，正在接收链路完整性信号。

  – down

    链路中断，例如由于关闭了所连接的设备。

- **模式 (Mode)**

  显示端口的传输速度和传输方法。

- **MTU (Maximum Transmission Unit)**

  显示包大小。

- **Negotiation**

  显示自动组态是启用还是禁用状态。

- **MAC 地址 (MAC Address)**

  显示端口的 MAC 地址。

6.6.1.2 组态

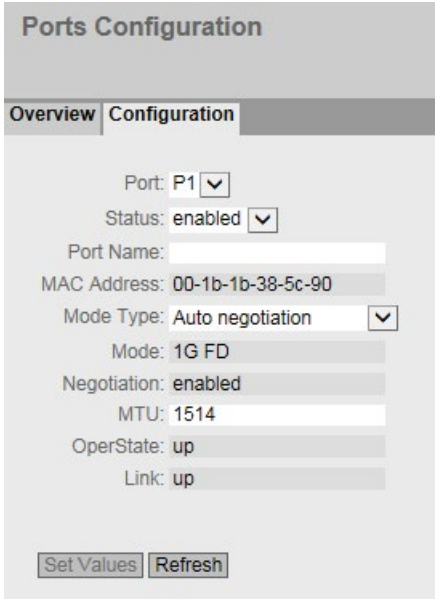
组态端口

通过此页面组态设备的以太网端口。

说明

SCALANCE W786-2 SFP

无法对 SCALANCE W786-2 SFP 的两个 SFP 端口单独进行参数分配或诊断。



说明

该表格包括以下行：

- **端口 (Port)**

  从下拉列表中选择要组态的端口。

- **状态 (State)**

  指示端口处于启用还是禁用状态。

  – enabled
    端口已启用。数据通信只能通过已启用的端口进行。

  – disabled
    端口已禁用。

- **端口名称 (Port name)**

  输入端口名称。

- **MAC 地址 (MAC Address)**

  显示端口的 MAC 地址。

- **模式类型 (Mode Type)**

说明

在 SCALANCE W786-2 SFP 上无法组态此参数。

从此下拉列表中选择端口的传输速度和传输方法。传输速度可以是 10 Mbps、100 Mbps 或 1000 Mbps。对于传输模式，可以组态为全双工 (FD) 或半双工 (HD)。如果将模式设置为"Auto negotiation"，会自动与连接的终端设备协商这些参数。还必须处于"Autonegotiation"模式。

说明

在某个端口与伙伴端口相互通信之前，两端必须都有匹配的设置。

说明

如果将传输速度组态为 10 Mbps 或将传输模式组态为半双工 (HD)，将导致 PROFINET 通信受限。如果希望设备处理 PROFINET 通信，则应始终选择 100 Mbps 及以上带宽和全双工 (FD) 或"自动协商"(Autonegotiation)。

- **模式 (Mode)**

显示端口的传输速度和传输方法。

- **Negotiation**

显示对伙伴端口连接的自动组态是处于已启用状态还是处于已禁用状态。

- **MTU（最大传输单元）**

输入包大小，超过此大小的数据包将被分片。

- **OperState**

  显示当前运行状态。运行状态取决于已组态的"状态"(Status) 和"链接"(Link)。可用选项如下：

  – "有效"(up)
    已将端口的状态组态为"启用"(enabled)，且端口与网络之间存在有效的连接。

  – "无效"(down)
    已将端口的状态组态为"禁用"(disabled) 或"链路中断"(Link down)，或者端口不存在连接。

- **链路 (Link)**

  显示网络连接状态。可用选项如下：

  – Up
    端口与网络之间存在有效链路，正在接收链路完整性信号。

  – Down
    链路中断，例如由于关闭了所连接的设备。

步骤

说明

更改端口组态

利用各个自动功能，设备可以在某个端口过载时，防止或降低对其它端口和优先级 (Class of Service) 的影响。这意味着即使启用流量控制，帧也可能被丢弃。
当设备接收的帧多于它可以发送的帧时（例如由于不同的传输速度），会发生端口过载。

按照下列步骤更改端口组态：

1. 单击相应的框更改组态。
2. 单击"设置值"(Set Values) 按钮。

6.6.2 WLAN

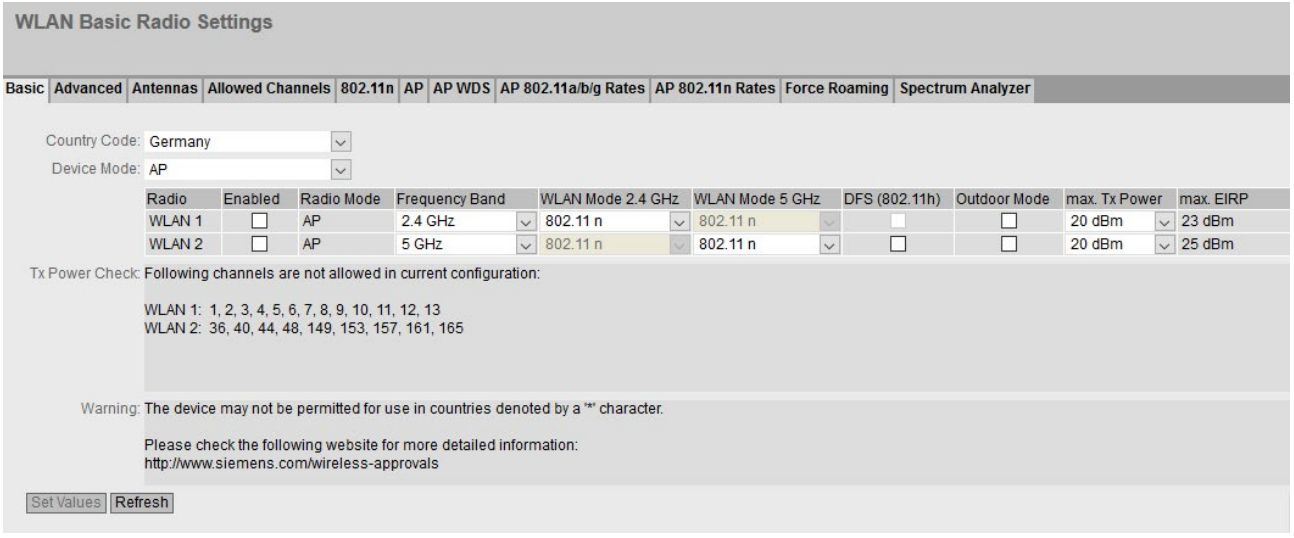
6.6.2.1 Basic

基本设置

在该页面上进行设备的几项基本设置，例如国家/地区设置和模式。

说明

要组态 WLAN 接口，必须始终首先指定国家/地区代码。有些参数取决于国家/地区设置，例如传输标准。



描述

- **国家/地区代码 (Country Code)**

  从该下拉列表中选择设备运行时所在的国家/地区。

  无需了解特定国家/地区的数据，设备会根据您所选择的国家/地区设置通道划分和输出功率。

说明

区域设置

为使操作符合认证，必须正确设定国家/地区设置。选择与设备使用地所在国家/地区不同的国家/地区会导致法律纠纷。

- **设备模式 (Device Mode)**

  选择设备的模式。此选择仅适用于接入点。

  存在以下工作模式：

  – AP：接入点模式

  – Client：客户端模式

说明

更改模式后，将显示一条消息。如果单击"确定"(OK) 确认消息，则设备将在更改的模式下以出厂设置组态重启。

如果在更改模式后已重启设备，则需要再次登录以继续进行组态。

该表格包括以下列：

- **无线 (Radio)**

  显示可用的 WLAN 接口。

  说明

  对于具有两个无线接口的设备 (W78x-2)，两个接口均可用于接入点模式。在客户端模式下，只有一个 WLAN 接口可用。

- **启用 (Enabled)**

  WLAN 接口的状态。要启用 WLAN 接口，请选中该复选框。

  说明

  启用 WLAN 接口

  提供设备时 WLAN 接口处于禁用状态。在国家/地区和天线设置组态完毕后可启用 WLAN 接口。

- **无线模式 (Radio Mode)**

  显示 WLAN 接口的模式。

- **频段 (Frequency Band)**

  指定频段。在客户端模式下也可以进行双频操作。

  – 2.4 GHz

  – 5 GHz

  – 2.4 GHz + 5 GHz（仅限客户端模式）

  说明

  将 W786-2IA RJ-45 的 WLAN 接口组态为不同频段

  如果将该设备上的两个 WLAN 接口组态为相同频段，则这两个接口会相互影响或干扰。在数据吞吐量较高时，这种情况尤其突出。

- **WLAN 模式 2.4 GHz (WLAN Mode 2.4 GHz)/WLAN 模式 5 GHz (WLAN Mode 5 GHz)**

  为组态的频段选择所需的传输标准。该选择取决于国家/地区设置。

  – Auto（仅限客户端模式）

    自动确定传输标准（2.4 GHz、5 GHz 和 2.4 GHz + 5 GHz）

  – 802.11a

    已设置传输标准 IEEE 802.11a (5 GHz)。

  – 802.11g

    已设置传输标准 IEEE 802.11g (2.4 GHz)。此传输标准与 IEEE 802.11b 向下兼容

  – 802.11n

    已设置传输标准 IEEE 802.11n（2.4 GHz 和 5 GHz）。此传输标准与 IEEE 802.11a 和 IEEE 802.11g 向下兼容。

  – 仅 802.11 (802.11 only)

    已设置传输标准 IEEE 802.11n（2.4 GHz 和 5 GHz）。此传输标准与 IEEE 802.11a 和 IEEE 802.11g 向下兼容。

说明

如果选择传输标准"802.11n"、"仅 802.11n"(802.11n only) 或"自动"(Auto)（仅限客户端模式），则无法设置分片长度的阈值，请参见"接口 > WLAN > 高级"(Interfaces > WLAN > Advanced) 中的"分片长度阈值"(Fragmentation Length Threshold)。

- **DFS (802.11h)**

  启用或禁用"动态频率选择 (DFS)"功能。

  – 启用

    使用 DFS 功能，还可以使用更高的 5 Ghz 通道。

    这些通道为国家/地区特定的通道，需要遵守某些 DFS 规范。有关更多信息，请参见国家/地区特定的 DFS 文档。

    接入点通过其中一条通道进行发射信号之前，会借助 CAC（通道可用性检查）进行为期 60 秒的搜索，检查是否存在竞争雷达信号。接入点在搜索期间不会发送任何信标。对于气象雷达通道 (5.6 - 5.65 GHz)，搜索持续时间为 10 分钟。

    如果经过搜索周期后未检测到任何雷达信号，接入点会通过此通道发射信号。否则，接入点将更改通道并重复该检查过程。

    运行期间，接入点还会持续搜索雷达信号。

    如果接入点发现当前通道上有雷达信号，则会自动切换到备用 DFS 通道，当前通道将被阻断 30 分钟。

  – 禁用

    未使用 DFS 功能。

说明

RCoax 5 GHz 和 DFS

在美国和其他遵循 FCC（美国联邦通信委员会）的国家/地区使用 DFS（动态频率选择）时，不能使用 IWLAN RCoax 电缆 5 GHz。可通过以下 Internet 地址查看当前认证状态：
http://www.siemens.com/wireless-approvals

- **户外模式 (Outdoor Mode)**

  – 启用

    如果已启用户外模式，则只能使用可在户外运行的通道。

  – 禁用

如果已禁用户外模式，则只能使用可在建筑物内运行的通道。

- **最大发射功率 (max. Tx Power)**

  指定设备可实现的最大发射功率。

  如果将发射功率设置的过大，则客户端处的接收信号可能会被过调。检查客户端处的接收信号强度 (dBm)。

  为避免超出法定的最大发射功率，可能有必要根据所使用的天线降低发射功率。降低发射功率可有效地减小蜂窝区大小。

  说明

  可实现的最大发射功率因通道和数据速率的不同而异。有关发射功率的更多详细信息，请参见文档"无线电接口特性"。

  说明

  如果带有两个 WLAN 接口的接入点的两个接口都运行在相同的频率范围内，这可能在发射功率高于 15 dBm 时导致一个接口或两个接口上有无线干扰。

- **max. EIRP (Effective Isotropic Radiated Power)**

  显示天线的当前辐射功率，与非定向天线相关（各向同性）。天线增益产品，天线连接器数量，电缆长度，其他衰减以及设置的 Tx 功率。

- **发射功率检查 (Tx power check)**

  指示所做的设置是否违反所选国家/地区允许的发射功率限制。检查"max. EIRP"的计算值以确定此值是否违反所设置国家/地区特定通道允许的发射功率限制。如果设置"仅使用允许的通道"(Use Allowed Channels only)，则仅检查在此选择的通道。

  – -

    通道可在当前设置下使用。

  – 通道数

    表示当前发射功率超出最大允许发射功率的通道。

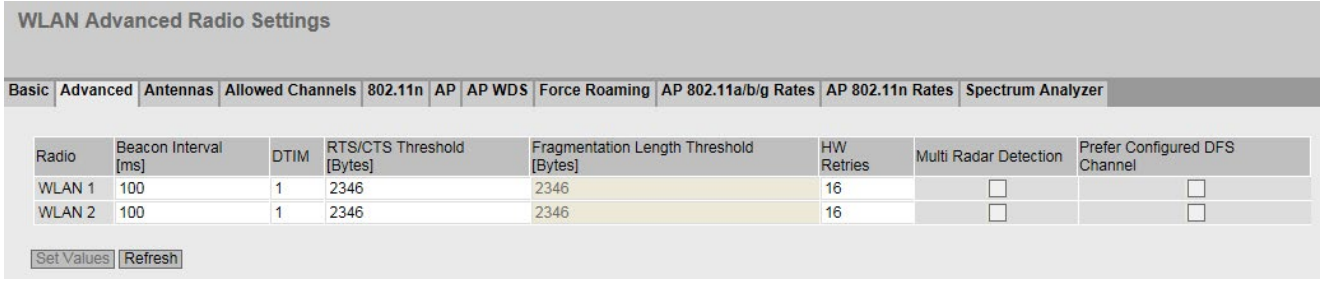
步骤

1. 要组态 WLAN 接口，必须始终首先指定国家/地区。在"国家/地区代码"(Country Code) 下拉列表中选择设备运行时所在的国家/地区。
2. 从"频段"(Frequency Band) 下拉列表中选择所需频段。
3. 从"WLAN 模式"(WLAN Mode) 下拉列表中为组态的频段选择所需传输标准。
4. 单击"设置值"(Set Values) 按钮。

6.6.2.2 高级

更多可能设置

在此页面中，可指定传输特性的具体内容。仅当通过默认设置无法按预期使用 SCALANCE W700 设备时，才需要调整此页面上的参数。



描述

该表格包括以下列：

- **无线 (Radio)**

  在此列中显示可用的 WLAN 接口。

- **信标间隔 [ms] (Beacon Interval [ms])（仅限接入点模式）**

  指定接入点发送信标的间隔 (40 - 1000 ms)。信标是由接入点周期性发送的数据包，用于向客户端通知接入点的存在。

- **DTIM（仅限接入点模式）**

  DTIM 时间间隔 (1-15) 指定接入点向客户端发送收集的数据包（广播、单播、组播）之前要发送的信标的数量。

  – 如果在此框中输入"1"，则接入点将在发送每个信标后立即传输广播、单播和多播包（常规网络环境的推荐设置）。

  – 如果在此字段输入"5"，则表示接入点每 5 个信标进行一次数据包的收集与发送。

  增大此值将允许客户端有更长时间处于休眠模式，但也意味着数据包的延迟更大。

- **RTS/CTS 阈值 [字节] (RTS/CTS Threshold [Bytes])**

  RTS/CTS（请求发送/允许发送）是一种避免冲突的方法。该方法基于实际数据发送前的状态信息交换（隐藏的节点问题）。出于减小由于其他协议通信造成的网络负载而使用此方法时，应仅限于特定大小以上的数据包。使用"RTS/CTS 阈值"(RTS/CTS Threshold) 参数指定数据包大小。

- **分片长度阈值 [字节] (Fragmentation Length Threshold [Bytes])**

  指定无线链路传送的最大数据包大小。大数据包会被分割为小数据包后再进行传输，并在接收后重组成原始大小。这在传输质量不良时较有帮助，因为较大的数据包更难传输。但是，分片为小数据包意味着吞吐量更低。

  说明

  仅当设置了传输标准"802.11g" (2.4 GHz) 或"802.11 a"(5 GHz) 时，才能编辑该值，请参见"接口 > WLAN > 基本"(Interfaces > WLAN > Basic) 中的"WLAN 模式"(WLAN Mode)。

- **硬件重试 (HW Retries)**

  指定硬件重试次数。在 WLAN 芯片尝试立即重复发送未确认的数据包时，硬件重复由 WLAN 芯片本身执行。

  如果所有硬件重复均未成功，则该数据包将被删除。

- **多雷达检测 (Multi Radar Detection)（仅限接入点模式）**
  - 已启用

    只有在"Basic"页面中启用了"DFS"功能后，该功能才可用。

    该功能适合如下系统：具有通过一个以太网连接的几个接入点，并且这些接入点在相同通道上发送信息。

    当一个接入点检测到雷达信号时，它将该信息分发给所有连接的接入点。如果至少还有一个接入点在 40 ms 内验证了雷达信号，则会通知所有连接的接入点。该通道上的所有设备发送操作均切换至另一个通道。对于网络中的接入点，该通道将被阻断 30 分钟。

    如果已在"接口 > WLAN > AP"(Interfaces > WLAN > AP) 页面上为通道组态"自动"(Auto)，将无法可靠地使用该功能。在这种情况下，仅当至少两个连接的接入点恰巧在同一个通道上发送时，才可能进行雷达信号的验证。如果只有一个接入点检测到了通道上的信号，则会将其视为有效的雷达信号。

  - 已禁用

    未使用该功能。当一个接入点检测到雷达信号时，它将切换到另一个通道上。不再考虑组态的通道。

- **首选组态的 DFS 通道 (Prefer Configured DFS Channel)（仅限接入点模式）**

  – 已启用

    只有在"Basic"页面中启用了"DFS"功能后，该功能才可用。

    如果 WLAN 接口的组态通道因雷达侦测而被阻断，并在 30 分钟后又恢复通畅，则接入点会自动切换至组态的通道。

    在接入点开始在组态的通道上进行通信之前，将花费 60 秒的时间在该通道上搜索主要用户。在此期间，接入点不会发送信标。如果在通道上发现信号，则接入点将更改通道并重复该检查过程。只有在 60 秒钟后未检测到主要用户的信号时，接入点才会在该通道上进行发送操作。

    如果已在"接口 > WLAN > AP"(Interfaces > WLAN > AP) 页面上为通道组态"自动"(Auto)，则设备不具有可返回的组态通道。

  – 已禁用

    未使用该功能。

步骤

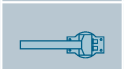
1. 在以下输入框中输入要设置的值。
2. 选中所需功能的选项复选标记。
3. 单击"设置值"(Set Values) 按钮。

6.6.2.3 天线

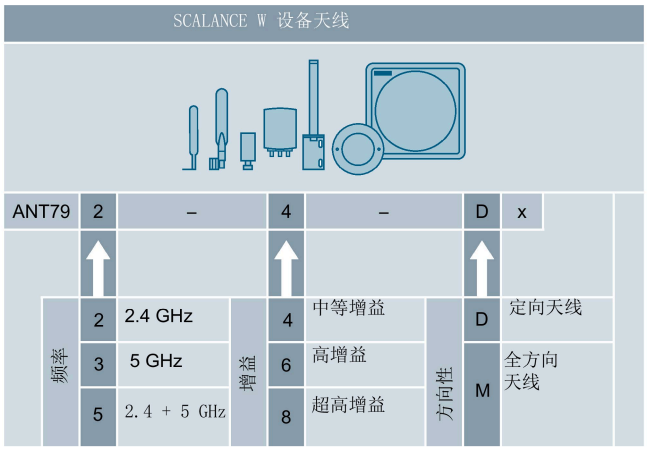
总览

IWLAN 天线总览：

天线类型	频率（GHz）	天线		SCALANCE W780/W740	SCALANCE W770/W730	SCALANCE W760/W720	SCALANCE W1780/W1740
全方向	2.4		ANT792-6MN	●	●	●	●
	2.4 和 5		ANT795-4MA	●	●	●	●
			ANT795-4MB	●	●	●	●
			ANT795-4MC	●	●		●
			ANT795-4MD	●	●		●
			ANT795-4MX	●	●		●
			ANT795-6MN	●	●	●	●
			ANT795-6MT	●			●
			ANT795-6MP	●	●	●	●
	5		ANT793-6MN	●	●	●	●
扇形	2.4 和 5		ANT795-6DC	●	●	●	●
	5		ANT793-6DG	●	●		●
			ANT793-6DT	●			●

天线类型	频率（GHz）	天线		SCALANCE W780/W740	SCALANCE W770/W730	SCALANCE W760/W720	SCALANCE W1780/W1740
定向	2.4		ANT792-8DN	●			●
	5		ANT793-8DP	●	●	●	●
			ANT793-8DJ	●	●		●
			ANT793-8DK	●	●		●
			ANT793-8DL	●	●		●
RCoax	2.4		RCoax 波导 2.4 GHz	●	●	●	●
			ANT792-4DN	●	●	●	●
	5		RCoax 波导 5 GHz	●	●	●	●
			ANT793-4MN	●	●	●	●
GSM 移动无线	2.4 和 5		ANT896-6MM				●

天线名称提供了在 IWLAN 天线总览中列出的天线属性的信息：



外部天线的组态

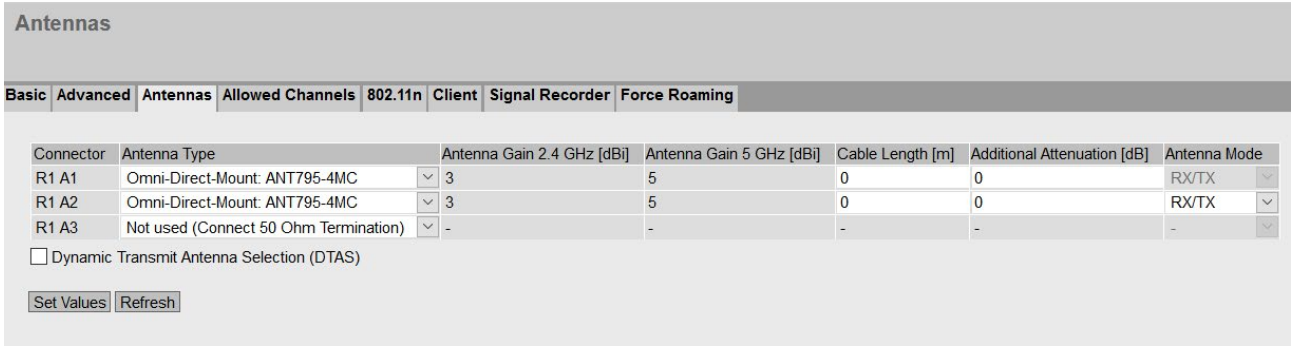
在此页面组态已连接的外部天线的设置。

只有内部天线可以组态天线模式。

说明

50 Ω 端接电阻

每个 WLAN 接口有三个天线连接器。未使用的连接器必须安装 50 Ω 端接电阻。
相关 WLAN 接口开启后，天线 R1A1 和 R2A1 必须始终处于连接状态。如果未连接任何天线，还必须禁用相应接口的 Rx 和 Tx。否则可能发生传输中断。



描述

该表格包括以下列：

- **连接器 (Connector)**

  显示相关天线连接器的名称。

- **天线类型 (Antenna Type)**

  选择连接到设备的外部天线的类型。如果外部天线的类型不可用，请选择条目"用户自定义"(User defined)。
  如果要使用 50 Ω 端接电阻端接某天线连接，请选择"未使用（连接 50 欧姆端子）"(Not used (Connect 50 Ohm Termination))。

- **天线增益 (Antenna Gain)**

  如果在"天线类型"(Antenna Type) 中选择了"用户自定义"(User defined) 条目，则手动输入天线增益（以"dBi"为单位）。

  – **天线增益 2.4 GHz [dBi] (Antenna Gain 2.4 GHz [dBi])**
    在此输入天线在 2.4 GHz 频段内的天线增益。

  – **天线增益 5 GHz [dBi] (Antenna Gain 5 GHz [dBi])**
    在此处输入天线在 5 GHz 频段内的天线增益。

- **电缆长度 [m] (Cable length [m])**

  输入设备和外部天线之间的柔性天线连接电缆的长度（以米为单位）。

- **其他衰减 [dB] (Additional Attenuation [dB])**

  在此处指定其他衰减，例如由其他分配器造成的衰减。

- **天线模式 (Antenna Mode)**

  指定天线的用途。对于天线连接器 1（R1 A1 和 R2 A1），输入不可更改。

  – Tx

    仅限发送

  – Rx

    仅限接收

  – Rx\Tx

    接收和发送

  下表显示了可能的各种组合：

索引 1 **R1 A1** **R2 A1**	**索引 2** **R1 A2** **R2 A2**	**索引 3** **R1 A3** **R2 A3**	**索引 4** **R1 A4** **R2 A4**
Rx\Tx	Rx\Tx	Rx\Tx	Rx\Tx
Rx\Tx	Rx\Tx	Rx\Tx	Rx
Rx\Tx	Rx\Tx	Rx	Rx
Rx\Tx	Rx	Rx	Rx
Rx\Tx	Rx\Tx	Rx\Tx	Tx
Rx\Tx	Rx\Tx	Tx	Tx
Rx\Tx	Tx	Tx	Tx
Rx\Tx	Rx\Tx	Rx\Tx	--[1)]
Rx\Tx	Rx\Tx	Rx	--[1)]
Rx\Tx	Rx\Tx	Tx	--[1)]
Rx\Tx	Tx	Tx	--[1)]
Rx\Tx	Rx	Rx	--[1)]
Rx\Tx	Rx\Tx	--[1)]	--[1)]
Rx\Tx	Tx	--[1)]	--[1)]
Rx\Tx	Rx	--[1)]	--[1)]
Rx\Tx	--[1)]	--[1)]	--[1)]

1) 天线类型为"未使用（连接 50 欧姆端子）"。

- **动态选择发射天线 (DTAS)（仅限客户端模式）**

  启用后，将自动选择可为接入点提供更强信号的天线进行数据传输。

  两条天线的信号强度显示在"信息 > WLAN > 无线电接口信息"(Information > WLAN > Radio interfaces information) 下。

  DTAS 要求：

  – 在接入点处设置 MCS < = 7。

  – 两条天线已组态天线模式"RX/TX"。

  – 如果有三条天线可用，则必须为第三条天线设置"天线类型""未使用（50 Ω 端接电阻）"(Not used (50 Ohm terminating resistor))。

步骤

要组态两个天线，请按以下步骤操作：

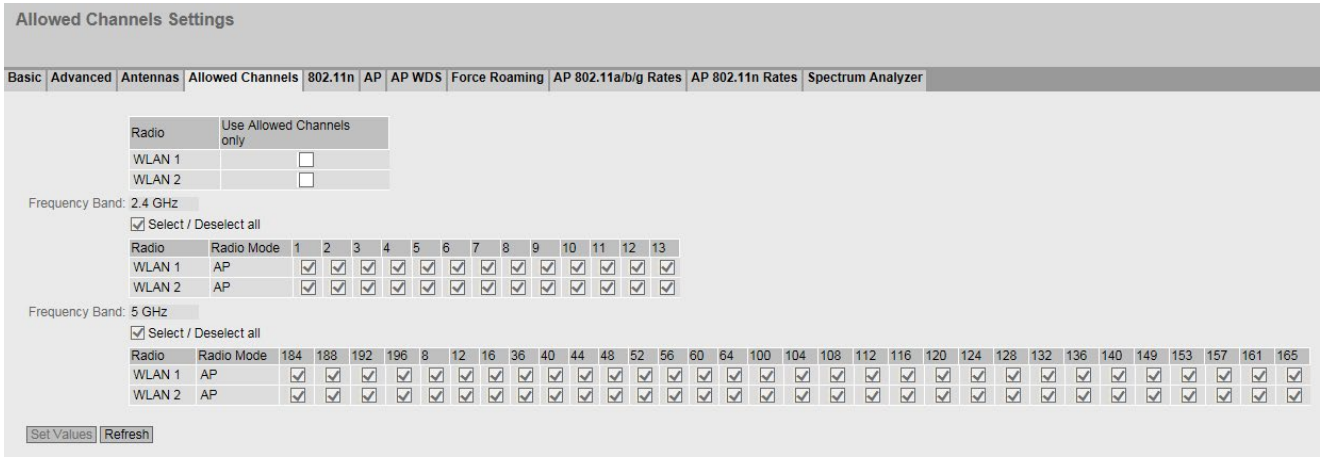
1. 对于第一个天线连接器 (R1 A1)，在"天线类型"(Antenna Type) 下拉列表中选择天线类型。
2. 在"电缆长度"(Cable Length) 输入框中，输入您所使用的连接电缆的长度（以米为单位）。对于天线连接器 1（R1 A1 和 R2 A1），"天线模式"(Antenna Mode) 条目不可更改。
3. 对于第二个天线连接器 (R1 A2)，在"天线类型"(Antenna Type) 下拉列表中选择天线类型。
4. 在"电缆长度"(Cable Length) 输入框中，输入您所使用的连接电缆的长度（以米为单位）。
5. 在"天线模式"(Antenna Mode) 下拉列表中选择天线的使用方式。
6. 单击"设置值"(Set Values) 按钮。

6.6.2.4 允许的通道

通道设置

为进行通信，将在频段内使用一个特定的通道。用户既可以具体设置此通道，也可以组态为自动选择通道。

在此页面指定可能用于通信的通道。



说明

表 1 包含以下列：

- **无线 (Radio)**

  显示可用的 WLAN 接口。

- **仅使用允许的通道 (Use Allowed Channels only)**

  如果启用此选项，则限制了对 AP 或客户端建立连接时允许使用的通道的选择。在下表中，可定义以下内容：

  – 在"自动"(Auto) 通道设置处于启用状态时，AP 可用于建立无线蜂窝区的通道。

  – 客户端进行 AP 搜索时所处的通道。

  表格根据频段进行划分。
  如果禁用该选项，则将使用在设置（国家/地区代码、天线、发射功率等）条件下的可用通道。

在各频段表格的上方，可看到以下复选框：

- **全选/取消全选 (Select/Deselect all)**
  - Enabled
    如果启用该复选框，将选中所有通道。
  - Disabled
    如取消选中该复选框，则频段内第一个有效通道将保持启用状态。启用所需的通道。

频段表具有以下列：

- **无线 (Radio)**

  显示可用的 WLAN 接口。

- **无线模式 (Radio Mode)**

  显示模式。

- **通道号 (Channel number)**

  要为所需的频段指定有效通道，请选中通道号所对应的相应复选框。
  该表格显示了相应国家/地区允许的通道。只能启用有效的通道。无效通道将灰显且无法启用。

说明
要指定通道，必须启用设置"仅使用允许的通道"(Use Allowed Channels only)。

步骤

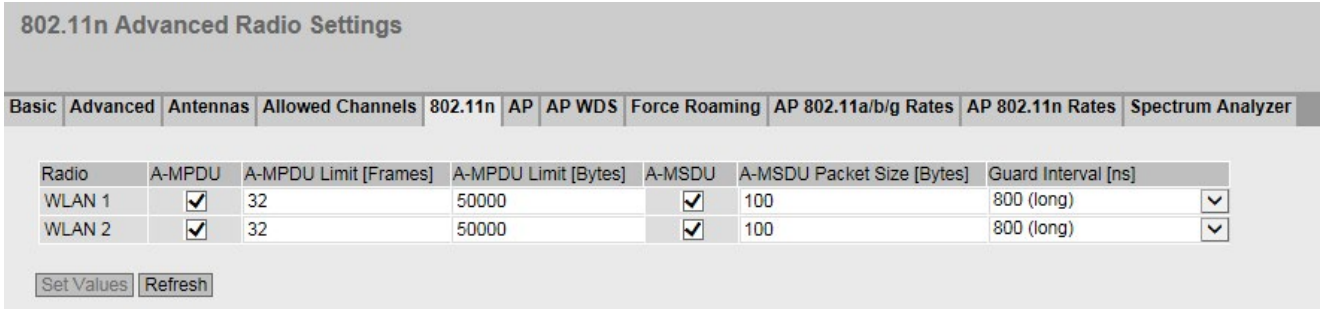
1. 为所需 WLAN 接口选择"仅使用允许的通道"(Use Allowed Channels only) 选项。
2. 取消选中"全选/取消全选"(Select/Deselect all) 复选框。
3. 选择所需通道号所对应的相关复选框。
4. 单击"Set Values"按钮。

6.6.2.5 802.11n

802.11n 的属性

按照 IEEE 802.11n 标准，可将单独的数据包集中到一起，放到一个更大的数据包（即 A-MPDU 和 A-MSDU 数据包）中。这可带来更高的数据吞吐量。

在此页面中可进行 A-MPDU 和 A-MSDU 数据包设置。部分设置取决于设置的传输标准和所选的通道宽度。



说明

该表格包括以下列：

- **无线 (Radio)**

  显示可用的 WLAN 接口。

- **A-MPDU**

  聚合的 MAC 协议数据单元 (A-MADU)

  启用或禁用具有相同目标地址的几个 MPDU 以大 A-MPDU 的形式发送。这使得总吞吐量得以提高。

  如果禁用此复选框，则将接收但不发送 A-MPDU 数据包。

- **A-MPDU Limit [Frames]**

  指定在一个 A-MPDU 数据包中组合在一起的单独数据包的数量。

  取值范围：2 - 64 帧

- **A-MPDU Limit [Bytes]**

  指定 A-MPDU 数据包的最大大小。

  取值范围：1024 - 65535 字节

  默认值：50000 字节

- **A-MSDU**

  聚合的 MAC 服务数据单元 (A-MSDU)

  启用或禁用如下操作：具有相同目标地址的几个 MSDU 被捆绑到一个 A-MSDU 中，并同时发送。这会减少网络负载。A-MSDU 具有更短的最大长度，因此更适合捆绑几个更短的帧。

  如果禁用此复选框，将接收但不发送 A-MSDU 数据包。

- **A-MSDU 数据包大小 [字节] (A-MSDU Packet Size [Bytes])**

  指定 A-MSDU 数据包的最大大小。

  取值范围：50 - 200 字节

  默认值：100 字节

- **防护间隔 [ns] (Guard Interval [ns])（仅限接入点模式）**

  选择两个传送的 OFDM 符号之间必须保持的发送暂停时间。
  可能的设置如下。该选择取决于所选的传输标准。

  – 400（短）/800（长）：设置 400 ns 可选。可使用 400 ns 或 800 ns 的发送暂停时间来发送数据包，具体取决于信号质量。

  – 800（长）：发送暂停时间为 800 ns。

步骤

在接入点上组态 802.11n 设置

1. 启用"A-MPDU"选项。
2. 在"A-MPDU 限值 [帧]"(A-MPDU Limit [Frames]) 和"A-MPDU 限值 [字节]"(A-MPDU Limit [Bytes]) 输入框中输入所需的值。
3. 启用选项"A-MSDU"。
4. 在"A-MSDU 数据包大小"(A-MSDU Packet Size) 输入框中输入所需值。
5. 从"防护间隔 [ns]"(Guard Interval [ns]) 下拉列表中选择所需的值。
6. 单击"Set Values"按钮。

在客户端上组态 802.11n 设置

1. 启用"A-MPDU"选项。
2. 在"A-MPDU 限值 [帧]"(A-MPDU Limit [Frames]) 和"A-MPDU 限值 [字节]"(A-MPDU Limit [Bytes]) 输入框中输入所需的值。
3. 启用选项"A-MSDU"。
4. 在"A-MSDU 数据包大小"(A-MSDU Packet Size) 输入框中输入所需值。
5. 单击"Set Values"按钮。

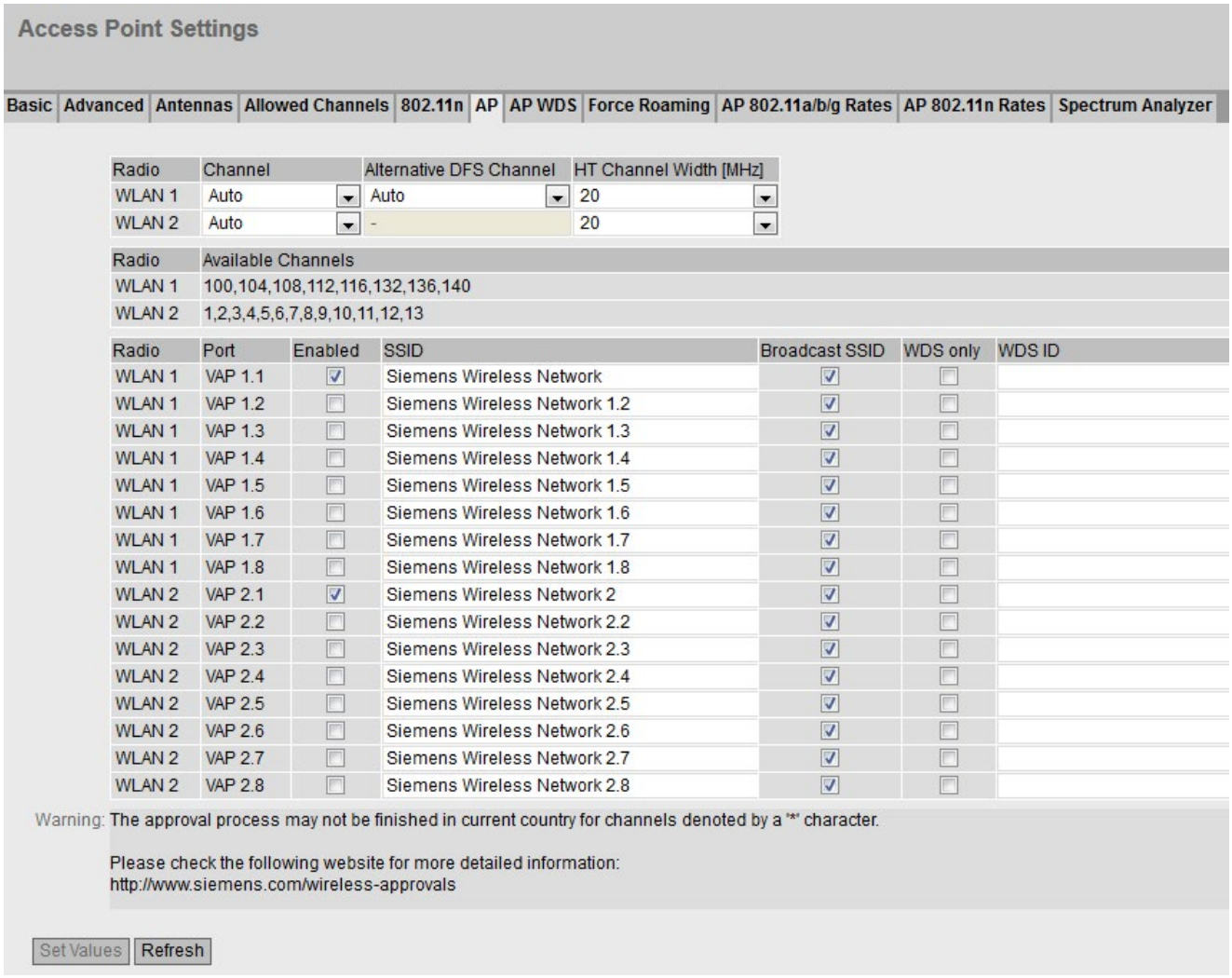
6.6.2.6 AP

组态

在该 WBM 页面上指定接入点的组态。

说明

该 WBM 页面仅在接入点模式下可用。



描述

表 1 包含以下列：

- **无线 (Radio)**

  显示可用的 WLAN 接口。

- **通道 (Channel)**

  指定主通道。

  如果希望接入点自行搜索空闲通道，请使用"自动"(Auto)。可限制在建立无线蜂窝区时接入点可使用的通道。为此，在"允许的通道"(Allowed Channels) 页面中，选

中"仅使用允许的通道"(Use Allowed Channels only) 复选框。
如果要使用固定通道，请从下拉列表中选择所需的通道。

说明

WLAN 接口的通道间隔
如果使用第二个 WLAN 接口，请确保具有足够的通道间隔。

- **备用 DFS 通道 (Alternative DFS Channel)**
  如果在"基本"(Basic) 页面中启用了"DFS"功能，则在此处指定备用通道。如果希望接入点自行搜索空闲通道，请使用"自动"(Auto)。
  如果在主通道和备用通道都检测到主要用户，则接入点将自动搜索空闲通道。
  如果要使用固定通道，请从下拉列表中选择所需的通道。
- **HT 通道宽度 [MHz] (HT Channel Width [MHz])**
  只能指定符合 IEEE 802.11n 传输标准的通道带宽。
  可能的设置如下。
  - 20
    通道带宽为 20 MHz
  - 40 up
    通道带宽 40 MHz。使用组态的通道以及高于其带宽的相邻通道。

– 40 down

通道带宽 40 MHz。使用组态的通道以及低于其带宽的相邻通道。

说明

通道带宽 40 MHz 和频段 2.4 GHz

如果接入点在组态的通道中或者在相邻的通道中检测到其他接入点，则原接入点会将通道带宽从 40 MHz 更改为 20 MHz。如果在接入点上设置"空闲"通道，则该接入点将使用 40 MHz 的通道带宽。

表 2 包含以下列：

- **无线 (Radio)**

  显示可用的 WLAN 接口。

- **可用通道 (Available Channels)**

  此框显示允许的通道。显示的内容取决于当前所选国家/地区的无线认证，以及"允许的通道"(Allowed Channels) 页面上的设置。

表 3 包含以下列：

- **无线 (Radio)**

  显示 WLAN 接口。

- **端口 (Port)**

  显示 VAP 接口。

- **启用 (Enabled)**

  要使用所需的 VAP 接口，请选中此复选框。

- **SSID**

  输入 WLAN 的 SSID。SSID 的字符串长度为 1 到 32 个字符。

  SSID 使用 ASCII 码 0x20 至 0x7e。

- **广播 SSID (Broadcast SSID)**

  – 取消激活

  SSID 再也不在接入点的信标帧中发送。这意味着 SSID 对其他设备不可见。只有

获知接入点的 SSID 并使用它来进行组态的客户端才可连接到该接入点。必须在这些客户端上禁用"任意 SSID"(Any SSID) 选项。

– 激活

SSID 在接入点的信标帧中发送，并对其他设备可见。也就是说，启用了"任意 SSID"(Any SSID) 选项的客户端也可连接到该接入点。

说明

由于 SSID 传输不进行加密，因此该功能只能对未经授权的访问提供基本保护。使用验证方法（例如 WPA2 (RADIUS)，或者 WPA2-PSK）可以提高安全性。另外，必须考虑到某些终端设备可能无法访问隐藏的 SSID。

- **仅 WDS (WDS only)**

  如果启用此选项，接入点将仅支持通过 WDS 进行的通信。在 WDS 模式下，所有接入点必须使用同一个通道。

- **WDS ID**

  输入 WDS ID。WDS ID 的最大长度为 32 个字符。
  要建立 WDS 连接，请在 WDS 伙伴上输入此 WDS ID。
  WDS ID 使用 ASCII 码 0x20 至 0x7e。

步骤

1. 从"通道"(Channel) 下拉列表中选择所需的通道。
2. 在"SSID"输入框中为相应的 WLAN 接口和端口输入网络名称。
3. 为相关 WLAN 接口和端口选中"启用"(Enabled) 复选框。
4. 单击"设置值"(Set Values) 按钮。

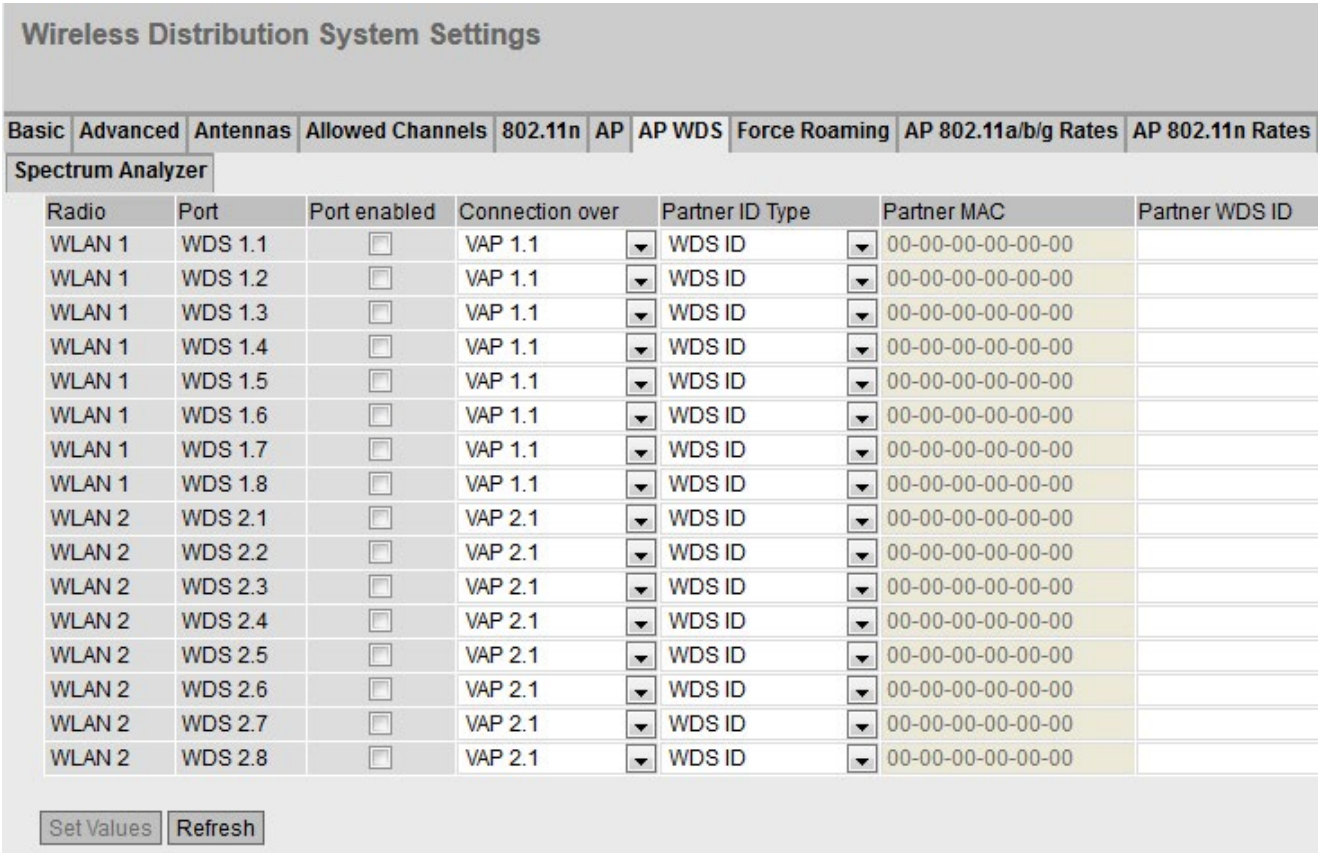
6.6.2.7 AP WDS

通信

在正常运行时，接入点将充当网络的接口与客户端通信。但是，有时会存在多个接入点需要彼此互相通信的情况，例如，在需要扩展无线覆盖范围或设置无线骨干时。WDS（Wireless Distributed System，无线分布式系统）支持此模式。

说明

该 WBM 页面仅在接入点模式下可用。



说明

该表格包括以下列：

- **无线 (Radio)**

  显示可用的 WLAN 接口。

- **Port**

  显示 WDS 接口。

- **启用端口 (Port enabled)**

  启用 WDS 接口。

- **连接所用接口 (Connection over)**

  指定建立 WDS 连接时所经由的 VAP 接口。使用 VAP 的 MAC 地址和安全设置（例如 WPA2）。

- **伙伴 ID 类型 (Partner ID Type)**

  指定 WDS 通信的类型。

  – MAC 地址 (MAC Address)
  使用 MAC 地址。"伙伴 WDS ID"(Partner WDS ID) 输入框将灰显。对于"伙伴 MAC"(Partner MAC)，输入 WDS 伙伴的 MAC 地址。

  – WDS ID
  使用 WDS ID。"伙伴 MAC"(Partner MAC) 输入框将灰显。对于"伙伴 WDS ID"(Partner WDS ID)，输入 WDS 伙伴的 WDS ID。如果以后要使用 C-PLUG 或 KEY-PLUG 替换接入点，则使用此选项。

- **伙伴 MAC (Partner MAC)**

  输入 WDS 伙伴的 MAC 地址。

- **伙伴 WDS ID (Partner WDS ID)**

  输入 WDS 伙伴的 WDS ID。对于 WDS ID，允许 ASCII 字符 0x20 至 0x7e。

说明

匹配 WDS 模式下的安全设置

在 WDS 模式下，确保安全设置与所有相关设备均匹配。如果设置不正确或与具体设备不兼容，则会因为验证错误而无法进行数据交换。应避免使用基本向导页面"安全设置 2"(Security Settings 2) 上的"自动"(Auto) 设置。因为使用该设置后，将无法实现接入点之间的安全设置同步。

说明

在 WDS 操作中，涉及的所有接入点均存在以下限制：

- 所有要彼此通信的接入点必须使用相同的通道、传输步骤和数据传输速率。
- 可选择 WEP 或 WPA(2)-PSK 作为加密方法。
  在以下位置组态已分配 VAP 接口的安全设置："安全 > WLAN > 基本"(Security > WLAN > Basic)
  对于 WDS 连接，不能使用 RADIUS 服务器的验证。
- 在 IEEE 802.11h 传输模式下，选择"WDS"模式并不现实。在 WDS 模式下，所有接入点必须使用同一个通道。如果某个接入点检测到主要用户的信号，则会自动切换该通道，从而导致现有连接中断。

步骤

1. 从"连接所用接口"(Connection over) 下拉列表中选择所需的 VAP 接口。
2. 从"伙伴 ID 类型"(Partner ID Type) 下拉列表中选择条目"WDS ID"。
3. 在"伙伴 WDS ID"(Partner WDS ID) 输入框中输入 WDS 伙伴的 WDS ID。"MAC 地址"(MAC Address) 输入框将灰显。
4. 单击"设置值"(Set Values) 按钮。

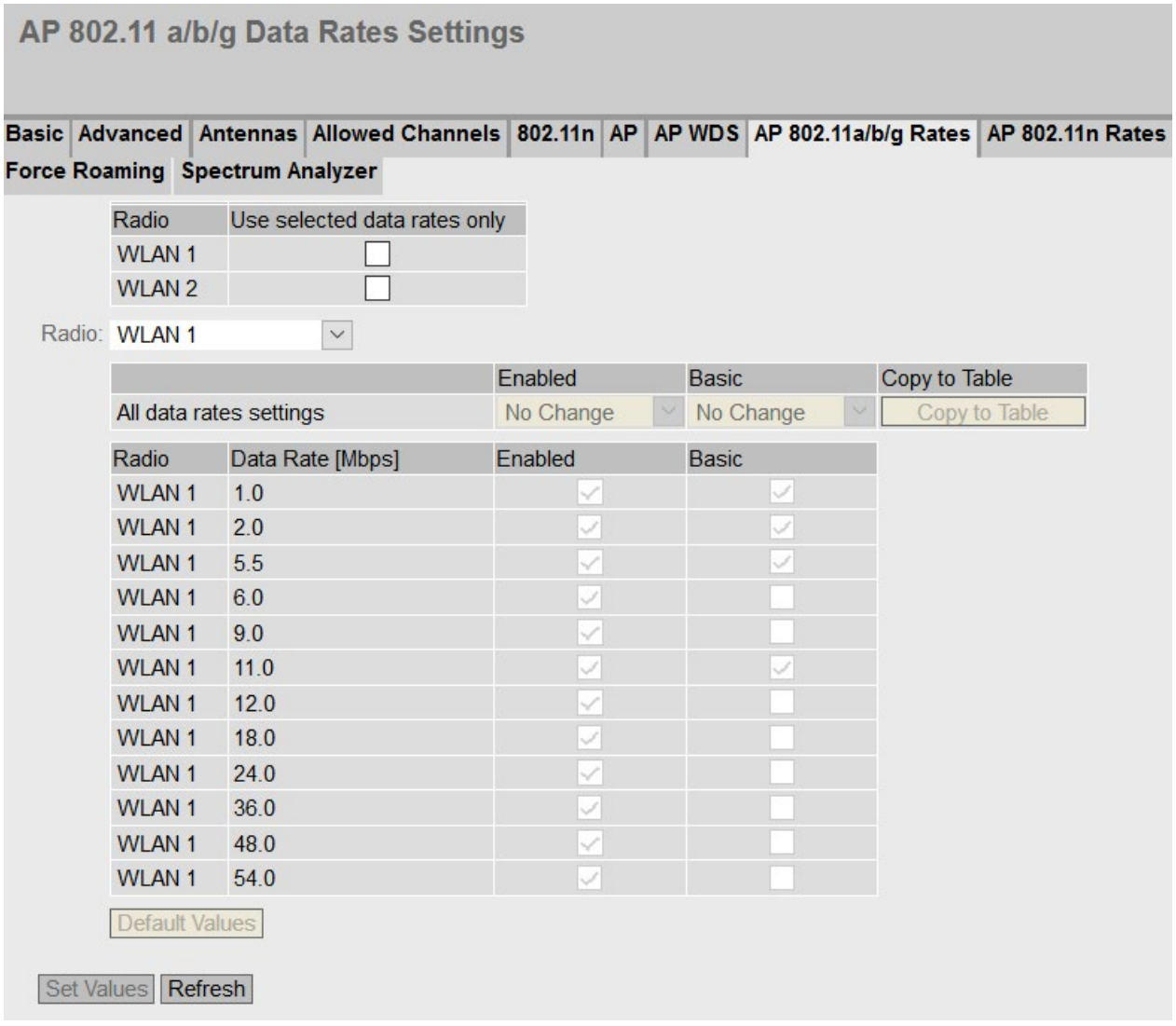
6.6.2.8 AP 802.11a/b/g 数据传输速率

IEEE 802.11a/b/g 的数据传输速度

说明

该 WBM 页面仅在接入点模式下可用。
WBM 页面只有在已为 WLAN 模式设置"802.11a"、"802.11g"或"802.11n"时才可组态。

此 WBM 页面会显示 WLAN 模式 802.11a/b/g 的可用数据传输速度。如有必要，可以更改数据传输速度。否则，建议保留数据传输速度的默认设置。这样接入点便仅使用所选的数据传输速度与客户端通信。



描述

表 1 包含以下列：

- **无线 (Radio)**

  指定信息所关联的 WLAN 接口。

- **仅使用所选的数据传输速率 (Use selected data rates only)**

  若启用此选项，则可为所需的 WLAN 接口指定数据传输速度。
  如果禁用了此选项，则会使用默认值。默认情况下会禁用此选项。

"无线 (Radio)" 下拉列表

在此下拉列表中，选择表 3（数据传输速率）中显示的 WLAN 接口。

利用表 2，可以一次启用或禁用表 3（数据速率）中某个列的所有复选框。表 2 包含以下列：

- **所有数据传输速率设置 (All data rates settings)**

  说明设置对于表 3 的所有条目都有效。

- **启用 (Enabled)/基本 (Basic)**

  在此下拉列表中，选择适用于所有条目的设置。如果选择"无变化"(No Change)，则表 3 中的条目保持不变。

- **复制到表 (Copy to Table)**

  如果单击此按钮，则为表 3 的所有条目应用此设置。

表 3（数据速率）由以下列组成：

- **无线 (Radio)**

  指定信息所关联的 WLAN 接口。

- **数据传输速率 [Mbps] (Data Rate [Mbps])**

  显示支持的数据传输速度（单位：兆位每秒）。

- **启用 (Enabled)**

  启用此选项，以便将所需的数据传输速度分配给 WLAN 接口。

  说明

  至少需要启用一个数据传输速度。

- **基本 (Basic)**

  启用此选项，以便将所需的数据传输速度声明为"基本"(Basic)。"Basic"参数指定客户端必须能够达到此速度方可连接到接入点。只有选择了可用的数据传输速度后，才可启用"Basic"选项。

  说明

  至少需将一个数据传输速度指定为"Basic"。

步骤

要组态 WLAN 1 的数据传输速度：

1. 为"WLAN 1"启用"仅使用所选的数据传输速率"(Use selected data rates only) 选项。
2. 在"Radio"(无线) 下拉列表中，选择"WLAN 1"条目。
3. 为所需的数据传输速度选中"启用"(Enabled) 列和"基本"(Basic) 列中的相应复选框。
4. 单击"设置值"(Set Values) 按钮。

要复位所做选择：

1. 单击"默认值"(Default Values) 按钮。这样选择即会重置为默认值。

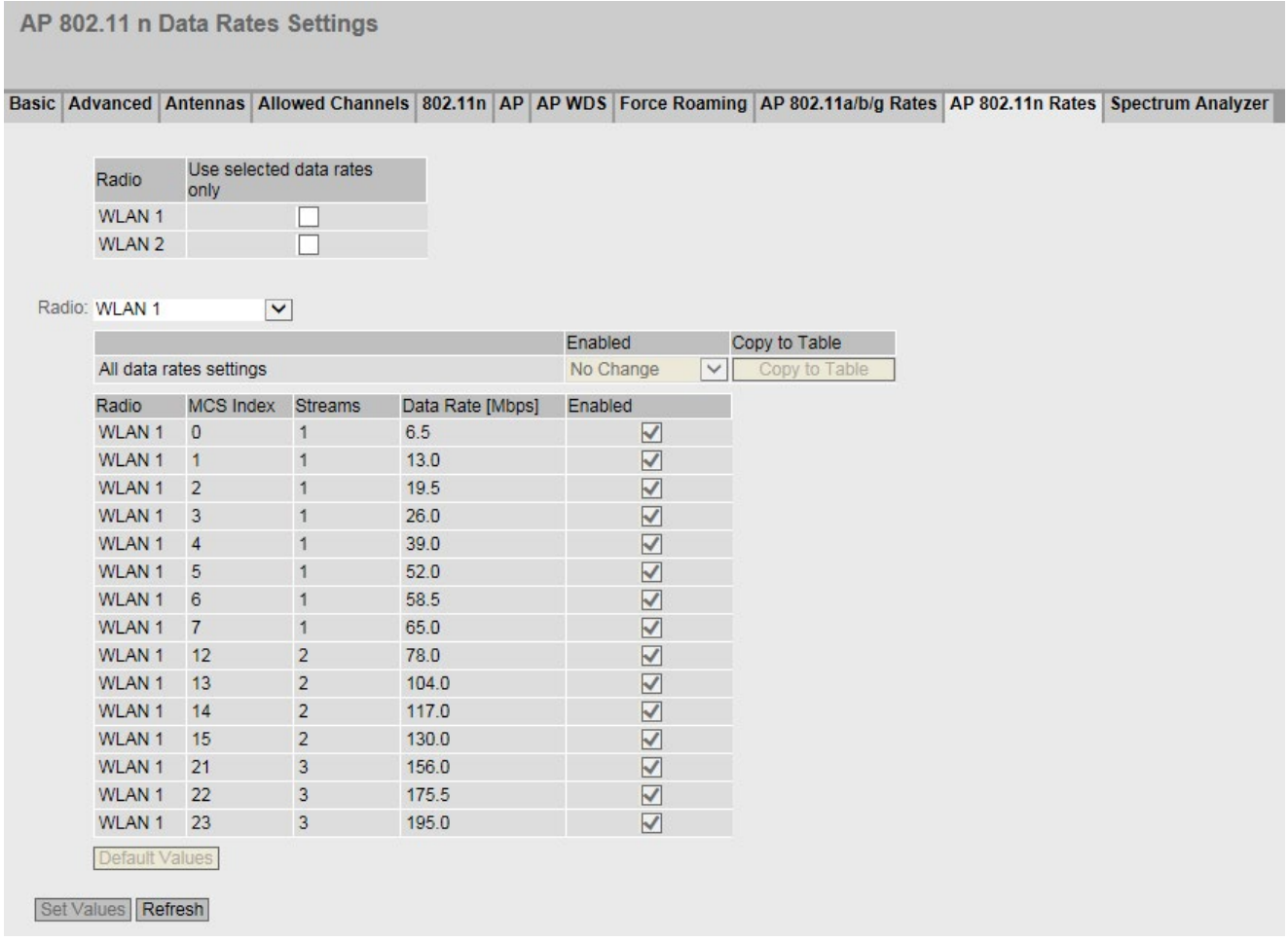
6.6.2.9 AP 802.11n 数据传输速率

IEEE 802.11n 的数据传输速度

说明

该 WBM 页面仅在接入点模式下可用。
WBM 页面只有在已为 WLAN 模式设置"仅限 802.11n"(802.11n only) 或 802.11n 时才可组态。

WBM 页面显示 WLAN 模式 802.11n 可使用的数据传输速度（MCS = 调制和编码方案）。可选择这些数据传输速度的任意选择。这样接入点便仅使用所选的数据传输速度与客户端通信。



描述

表 1 包含以下列：

- **无线 (Radio)**

  指定信息所关联的 WLAN 接口。

- **仅使用所选的数据传输速率 (Use selected data rates only)**

  若启用此选项，则可为所需的 WLAN 接口指定数据传输速度。
  如果禁用了此选项，则会使用默认值。默认情况下会禁用此选项。

无线 (Radio) 下拉列表

在此下拉列表中，选择表 3（MCS 索引）中显示的 WLAN 接口。

利用表 2，可以一次启用或禁用表 3（MCS 索引）中某个列的所有复选框。表 2 包含以下列：

- **所有数据传输速率设置 (All data rates settings)**

  说明设置对于表 3 的所有条目都有效。

- **启用 (Enabled)**

  在此下拉列表中，选择适用于所有条目的设置。如果选择"无变化"(No Change)，则表 3 中的条目保持不变。

- **复制到表 (Copy to Table)**

  如果单击此按钮，则为表 3 的所有条目应用此设置。

表 3（MCS 索引）由以下列组成：

- **无线 (Radio)**

  指定信息所关联的 WLAN 接口。

- **MCS 索引 (MCS Index)**

  显示支持的 MCS 索引。显示的 MCS 索引取决于"天线类型"(Antenna Type) 和"天线模式"(Antenna Mode) 设置。可在"接口 > WLAN > 天线"(Interfaces > WLAN >

Antennas) 中找到这两个设置。例如，如果仅使用一个天线，则将仅显示 MCS 0 到 7。

- **数据流 (Streams)**

  显示可通过所选 MCS 索引传送的并行数据流的最大可能数目。

- **数据传输速率 [Mbps] (Data Rate [Mbps])**

  显示支持的数据传输速度（单位：兆位每秒）。显示的数据传输速度取决于"防护间隔"(Guard Interval) 和"HT 通道宽度"(HT Channel Width) 设置。可在"接口 > WLAN > AP"(Interfaces > WLAN > AP) 中找到"HT 通道宽度"(HT Channel Width) 设置。可在"接口 > WLAN > 802.11n"(Interfaces > WLAN > 802.11n) 中找到"防护间隔"(Guard Interval) 设置。

- **启用 (Enabled)**

  启用此选项，以便将所需的数据传输速度分配给 WLAN 接口。

说明
至少需要启用一个 MCS 索引。

步骤

要组态 WLAN 1 的数据传输速度：

1. 为"WLAN 1"启用"仅使用所选的数据传输速率"(Use selected data rates only) 选项。
2. 在"Radio"(无线) 下拉列表中，选择"WLAN 1"条目。
3. 为所选的 MCS 索引选中"Enabled"列下的复选框。
4. 单击"设置值"(Set Values) 按钮。

要复位所做选择：

1. 单击"默认值"(Default Values) 按钮。这样选择即会重置为默认值。

或

1. 禁用表 1 中的"仅使用所选的数据传输速率"(Use selected data rates only) 选项。
2. 单击"设置值"(Set Values) 按钮。

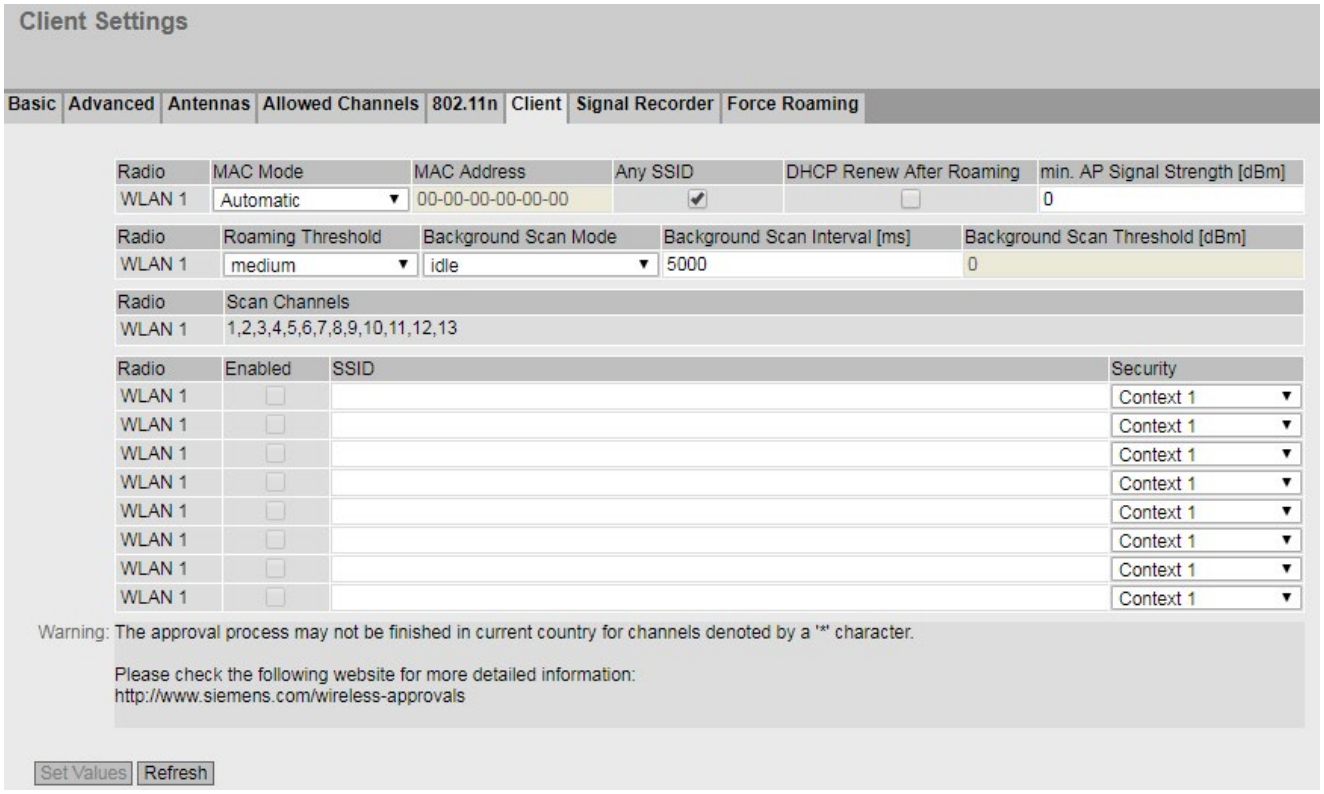
6.6.2.10 Client

连接到网络

可在此 WBM 页面上指定设备作为客户端连接到网络的方式。

说明

此 WBM 页面仅在客户端模式下可用。



说明

禁用 WLAN 接口

除非至少组态了一个 SSID，或者启用了设置"任意 SSID"(Any SSID)，否则将禁用 WLAN 接口。

说明

表 1 包含以下列：

- **无线 (Radio)**

  显示可用的 WLAN 接口。

- **MAC 模式 (MAC Mode)**

  指定向客户端分配 MAC 地址的方式。可能的方式包括：

  – 自动 (Automatic)
    客户端自动采用其通过以太网接口接收的第一帧的源 MAC 地址。

  – 手动 (Manual)
    如果选择"手动"(Manual)，则在"MAC 地址"(MAC Address) 列中输入 MAC 地址。

  – 自身 (Own)

    客户端的 WLAN 接口使用以太网接口的 MAC 地址。

  – 第 2 层隧道 (Layer 2 Tunnel)
    客户端的 WLAN 接口使用以太网接口的 MAC 地址。同时也会将连接到客户端以太网接口的 MAC 地址通知给网络。最多可使用八个 MAC 地址。

- **MAC 地址 (MAC Address)**

  如果已为"MAC 模式"(MAC Mode) 选择"手动"(Manual)，则输入客户端的 MAC 地址。

- **任意 SSID (Any SSID)**
  - 启用

    在客户端模式下，SCALANCE W 设备尝试连接到对应于安全上下文 1 的安全设置的接入点。客户端只可连接启用了"广播 SSID"(Broadcast SSID) 选项的接入点。
  - 禁用 (Disabled)

    客户端尝试连接到安全设置与定义的安全上下文之一相匹配的 SSID 列表中的接入点。
- **漫游后的 DHCP 续订** (DHCP Renew After Roaming)
  - 启用

    更改为不同的接入点后，进行检查以确定客户端的 IPv4 地址是否仍然有效。如果 IPv4 地址无效，DHCP 服务器会请求新的 IPv4 地址。
  - 禁用

    如果客户端更改为不同的接入点，将不会检查 IPv4 地址。
- **最低 AP 信号强度 (min. AP signal strength)**

  客户端可设置信号强度。

说明

已启用 iPCF/iPCF-HT/IPCF-MC

启用 iPCF/iPCF-HT/IPCF-MC 时，无法设置信号强度。

客户端必须接收接入点传入的信号（其特定强度应足以连接该接入点）。

信号强度可能由于客户端的移动和其它影响因素而暂时产生波动。为过滤信号波动，使用迟滞指定该值附近的一个范围。客户端在信号低于该范围前不更改接入点。

如果来自接入点的信号低于此范围，客户端将断开与接入点的连接并搜索新接入点。

- **漫游阈值 (Roaming Threshold)**

  指定客户端漫游到新接入点时所依据的阈值。

  – 高 (High)
    仅在场强明显高出时切换到信号更强的接入点。

  – 中 (Medium)
    在场强中等高时切换到信号更强的接入点。

  – 低 (Low)
    在场强稍高时便切换到信号更强的接入点。

- **后台扫描模式 (Background Scan Mode)**

  在客户端与一个接入点相连期间，它会在后台扫描可在必要时连接的其它接入点。指定扫描的模式。

  可使用以下选项：

  – 始终 (Always)
    如果低于后台扫描阈值，客户端会继续搜索接入点。

  – 空闲 (Idle)
    如果特定时间内没有数据传送，则将开始扫描其它接入点。

– 禁用 (Disabled)

只要客户端已连接，就不会扫描其它接入点。

– 当前通道 (Current channel)

客户端根据在当前通道上接收的信标（管理帧）更新其扫描列表。将在后台扫描间隔内评估扫描列表。如果包含来自更优接入点的信标，则客户端在评估之后会切换到此接入点而不改变当前通道。

说明

已启用 iPRP

启用 iPRP 后，客户端会针对每个漫游操作向其冗余伙伴发送特殊漫游广播帧。收到此广播帧后，冗余伙伴在 500 ms 内可能不会自行执行漫游。

- **后台扫描间隔 [ms] (Background Scan Interval [ms])**

  指定扫描其它接入点的时间间隔。

- **后台扫描阈值 [dBm]** (Background Scan Threshold [dBm])

  指定阈值。如果低于阈值，客户端会搜索较远的接入点。

表 2 包含以下列：

- **无线 (Radio)**

  显示 WLAN 接口。

- **扫描通道 (Scan Channels)**

  显示客户端搜索接入点时所在的通道。显示的内容取决于所选国家/地区的无线认证，以及"允许的通道"(Allowed Channels) 的设置。

表 3 包含以下列：

- **无线 (Radio)**

  显示 WLAN 接口。

- **启用 (Enabled)**

  启用或禁用相关 SSID。

- **SSID**

  输入要与客户端相连的接入点的 SSID。

  对于 SSID，使用 ASCII 码 0x20 至 0x7e。

- **Security**

  选择安全上下文。在"安全 > WLAN > 基本"(Security > WLAN > Basic) 中创建并组态安全上下文。

  默认设置：上下文 1

说明

已启用 iPCF/iPCF-HT/IPCF-MC

如果启用了 iPCF、iPCF-HT 或 iPCF-MC 模式，则只能选择安全上下文 1。

步骤

1. 从"MAC 模式"(MAC Mode) 下拉列表中选择所需的 MAC 地址分配模式。
2. 在表 3 中，为"SSID"输入一个 SSID。
3. 选择安全上下文。
4. 启用所需 SSID。

   禁用"任意 SSID"(Any SSID) 功能。
5. 单击"设置值"(Set Values) 按钮。

6.6.2.11 强制漫游

在此页面中可指定何时执行漫游。

- **在连接端子上（仅限接入点模式）**

  如果通过以太网接口的连接终止，则通过无线网络登录的客户端将不会注意到任何内容。连接终止的可能原因包括断线、网络组件故障、插头拔出等。接入点可通过在连接终止时禁用相关 WLAN 接口来强制登录的客户端进入漫游状态。客户端开始漫游，然后连接到另一个接入点。只要以太网接口再次可用，接入点就会重新打开其 WLAN 接口。

- **未访问目标地址时**

  为了对这种情况进行监视，设备会以固定时间间隔向已组态的目标地址发送 ping。

  – 接口由一个目标地址监视

    若此目标地址未发送 ping 响应，接入点将关闭相应的 VAP 接口，或者客户端将重新启动 WLAN 接口。

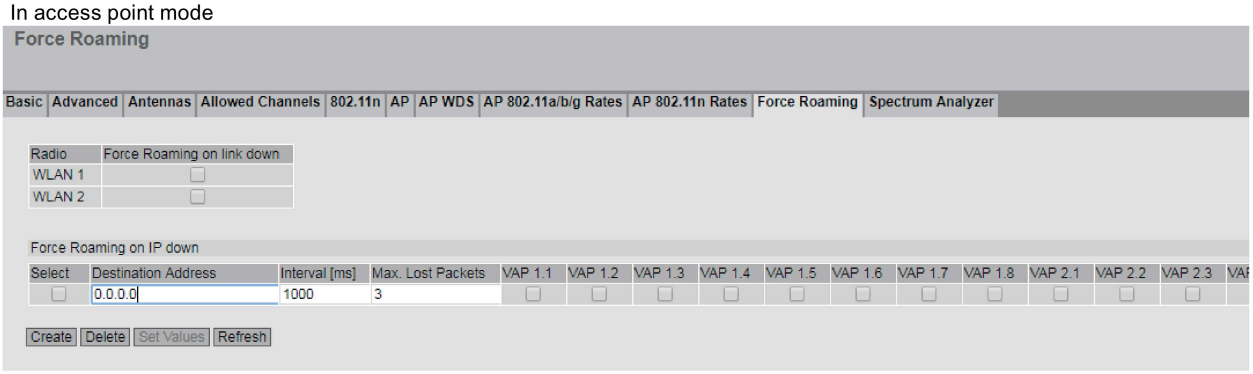
  – 接口由多个目标地址监视

    仅当所组态的任一目标地址均未发送 ping 响应时，接入点才会关闭相应的 VAP 接口，或者客户端重新启动 WLAN 接口。只要至少有一个目标地址可访问，接口就会保持激活状态。

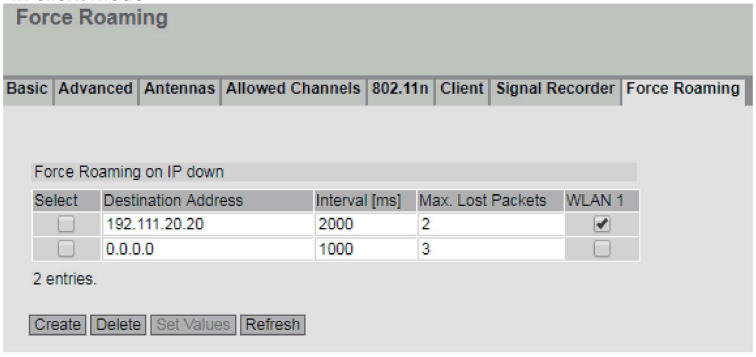
    例如，接入点通过此 VAP 接口向连接的 WLAN 客户端发送取消关联帧。WLAN 客户端将进行漫游并连接至另一个 VAP 接口。如果地址再次可访问，则会通过此 VAP 接口重新建立连接。

接入点和客户端的可能设置有所不同。

In access point mode



In client mode



描述

表 1 仅在接入点模式下可用，分为以下列：

- **无线 (Radio)**

  显示可用的 WLAN 接口。

- **链路中断时强制漫游 (Force roaming on link down)**

  如果启用该列，则当通过以太网接口建立的连接中断时，会关闭 WLAN 接口。

表格"IP 故障时强制漫游"(Force Roaming on IP down) 包含以下列：

- **选择 (Select)**

  选中要删除的行中的复选框。

- **目标地址 (Destination Address)**

  输入将要检查其可访问性的目标的 IPv4 地址或 FQDN（完全限定域名）。

  说明

  代理 IP 子网中无目标地址

  如果代理 IP 子网中没有目标地址，则必须在"第 2 层 > 代理 IP"(Layer 2 > Agent IP) 中输入网关。

  基础网桥模式"802.1Q VLAN 网桥"

  如果在"第 2 层 > VLAN"(Layer 2 > VLAN) 中组态了"基础网桥模式"(Based Bridge Mode)"802.1Q VLAN Bridge"，则会向管理 VLAN 发送 ping。

- **间隔 [ms] (Interval [ms])**

  指定发送 ping 的时间间隔。

- **丢失数据包的最大数目 (Max. Lost Packets)**

  指定连续丢失 ping 响应的最大数目。达到该数值的目标地址被视为不可访问 (down)。

- **VAP X.Y**（在接入点模式下）

  指定要监视的 VAP 接口。

- **WLAN** 0/X（在客户端模式下）

  指定要监视的 WLAN 接口。

步骤

创建强制漫游

1. 单击"创建"(Create) 按钮。
2. 进行以下设置：
   - 目标地址
   - 时间间隔
   - 丢失数据包的最大数目
3. 指定监视以下接口时采用的目标地址：
   - VAP 接口（在接入点模式下）
   - WLAN 接口（在客户端模式下）
4. 单击"设置值"(Set Values) 按钮。

删除强制漫游

1. 选中要删除的行中的复选框。
2. 单击"删除"(Delete) 按钮。将删除条目并更新页面。

6.6.2.12 信号记录器

记录有效的用户信号

信号记录器用于记录接入点和客户端之间的有效用户信号。利用此数据，可以定位用户信号不强的区域。当客户端沿固定路径移动时，信号记录器特别有用。

说明

此 WBM 页面仅在客户端模式下可用。
必须启用 SCALANCE W700 设备的 WLAN 接口，否则无法进行记录。

描述

显示分为两个区域。

- 客户端

  表示客户端的测量。

- 接入点

  显示客户端当前连接的接入点的测量。这要求启用"双向记录"(Bidirectional Recording) 设置，而且接入点上安装的固件版本要在 6.1 以上。接入点将其数据发送给最多 3 个运行信号记录器的客户端。接入点数据不会显示在其他客户端上。

两个区域分别包含两个图形。

第一个图形包含下列元素：

- 滚动条

  借助该滚动条，可以浏览整个测量情况。为此，可使用"<<"和">>"按钮或者键盘上的箭头键。

- 左侧栏

  在左侧栏中，可根据颜色方案实时显示客户端/接入点的用户信号。灰线显示背景噪声。

  如果客户端具有 iPCF-MC 连接，则显示的管理通道的用户信号将带有黑线。

- 颜色方案

  大于 -35 dBm（蓝色）的范围属于过调制范围，即 WLAN 信号过强并且经过调制后接收。自 -60 dBm 左右（黄色）起，WLAN 信号变弱。

- x 轴

  X 轴显示随机样本中的测量过程（单位为秒）。

- 测量数据

  – 客户端

    测量数据根据所显示的颜色方案显示了有效用户信号的值。灰线显示背景噪声。

    如果在测量（漫游）期间客户端更改了接入点或重新连接，则会通过黑色竖线进行显示。在该线上将显示新的 AP 系统名称和 BSSID。

    如果在测量期间客户端未连接到某个接入点，则不会显示用户信号。要明确表示不存在到接入点的连接，BSSID 将被设为 00:00:00:00:00:00 并以红色进行显示。

    如果客户端具有 iPCF-MC 连接，则显示的管理通道的用户信号将带有附加黑线。

  – 接入点

    测量数据根据所显示的颜色方案显示了有效用户信号的值。灰线显示背景噪声。

    如果在测量（漫游）期间客户端更改了接入点或重新连接，则会通过黑色竖线进行显示。

    如果接入点不支持"双向记录"设置，将不会显示任何用户信号

第二个图形包含下列元素：

- 左侧栏

  在左侧栏中，可根据颜色方案显示客户端/接入点的传输尝试和数据速率。

- 颜色方案

  大于 -35 dBm（蓝色）的范围属于过调制范围，即 WLAN 信号过强并且经过调制后接收。自 -60 dBm 左右（黄色）起，WLAN 信号变弱。在该图形下再次对各个颜色进行说明。

- x 轴

  X 轴显示随机样本中的测量过程（单位为秒）。

- 测量数据

  – 客户端

    测量数据根据所显示的颜色方案显示传输尝试。传输尝试显示为一栏。发送数据包的数据速率用一条线表示。如果在测量（漫游）期间客户端更改了接入点或重新连接，则会通过黑色竖线进行显示。

  – 接入点

    测量数据根据所显示的颜色方案显示传输尝试。传输尝试显示为一栏。发送数据包的数据速率用一条线表示。

    如果在测量（漫游）期间客户端更改了接入点或重新连接，则会通过黑色竖线进行显示。如果接入点不支持"双向记录"(Bidirectional Recording) 设置，将不会显示任何数据。

除了图形还加将显示以下值：

- 状态

  显示信号记录器是否在记录值。

- Current Sample

  当前测量的编号

- CL RX-Signal [dBm] / AP RX-Signal [dBm]

  客户端/接入点的有效用户信号，单位为 dBm

- CL NF [dBm] / AP NF [dBm]

  客户端/接入点的背景噪音，单位为 dBm

- CL Retries [%] / AP Retries [%]

  客户端/接入点的传输重复率用百分比表示。

- CL RSSI / AP RSSI

  客户端/接入点的 RSSI（接收信号强度指示）的原始值

- CL TX-Rate [Mbps] / AP TX-Rate [Mbps]

  在当前随机测试期间，发送的数据包的平均数据传输速率

- CL M-Signal [dBm]

  如果客户端具有 iPCF-MC 连接，则会显示管理通道的用户信号。

- Roaming Counter

  漫游计数器显示在记录过程中客户端更改接入点的频率。在 4 294 967 295 次更改后，该计数器将复位。

- Operative Channel

  当前通道或客户端与接入点相连所用的通道

- AP System Name

  接入点的系统名称

- BSSID

  接入点的 BSSID（基本服务集标识）。

- Connected Stations

  通过同一 VAP 接口连接到接入点的客户端数量。

- Bidirectional Status

  显示接入点的数据是否也被记录。

图形下方的表格包含以下列：

- **无线 (Radio)**

  显示应用信息的 WLAN 接口。由于每个客户端仅具有一个 WLAN 接口，因此该表中始终只有一行用于"WLAN 1"。

- **间隔 [ms] (Interval [ms])**

  指定采集两次测量值之间的时间间隔，以毫秒为单位。第一个测量值仅在经过设置的时间间隔后才会显示。

- **样本 (Samples)**

  指定应该进行的测量数。

- **无限 (Endless)**

  如果启用此选项复选标记，则测量次数没有限制。"样本"(Samples) 框呈灰显。信号记录器将一直运行，直到手动停止记录器或重新组态设备。

  只有在以 ≥ 100 毫秒的时间间隔开始时，才能选择该选项。

  如果记录包含超过 10000 次测量，则后 10000 次测量将列在 csv 文件和 PDF 文件中。

- **双向记录** (Bidirectional Recording)

  如果启用了将接入点的值设置为时间间隔为 10 毫秒及以上时可用。

  以下版本的接入点均支持该设置：SCALANCE W700 11n > V6.1 和 SCALANCE W1700 11ac > V1.0。

- **开始 (Start)**

  单击此列中的按钮开始记录所需信号。

  说明

  - 如果开始新记录，则会覆盖先前的记录。
  - 如果记录的持续时间短于 10 分钟并且尚未完成（例如由于重启或断电），则将删除测量值。

  信号记录器每 10 分钟自动保存一次记录的数据。重新启动后，记录将包含截至上次保存操作的所有值。

- **停止 (Stop)**

  单击此列中的按钮提前停止记录所需信号。如果已完成指定的测量次数，则将自动停止记录用户数据信号。

- **显示的样本 (Displayed Samples)**

  选择将在图中进行显示的测量数。

使用注意事项

注意以下几点提示，它们可帮助您使用信号记录器获取有用测量值：

- 在接入点上设置固定的数据传输速率。
- 如果已激活 iPCF，则尽可能在接入点上为测量设置较小的周期时间。
- 确保在测量期间可进行足够的数据通信，因为统计功能会对进入数据帧进行评估。
- 测量路径应以相同参数运行 2 至 3 次，以查明是否总是在同一位置出现用户数据信号损失的情况。
- 应在较长一段时间内在固定位置进行选择性测量。

步骤

1. 输入两次测量之间的时间间隔。
2. 在"样本"(Samples) 中输入测量数。
3. 在"显示的样本"(Displayed Samples) 中选择将在图中进行显示的测量数。
4. 单击"开始"(Start) 按钮。

   状态（图形右侧）用于指示信号记录器是否正在运行。第一个测量值仅在经过设置的时间间隔后才会显示。
5. 要停止记录，请单击"停止"(Stop) 按钮。
6. 切换到以下菜单项之一以调用记录结果：
   - 系统 > 加载和保存 > HTTP (System > Load&Save > HTTP)
     单击"WLANSigRec"表行中的"保存"(Save) 按钮，将文件"signal_recorder_SCALANCE_W700.zip"保存在所连接 PC 的文件系统中。
   - 系统 > 加载和保存 > TFTP (System > Load&Save > TFTP)
     必要时，可在"WLANSigRec"表行中更改文件名"signal_recorder_SCALANCE_W700.zip"。在表行"WLANSigRec"中，从最后一列的下拉列表中选择"保存文件"(Save file) 条目，然后单击"保存值"(Save Values) 按钮。
7. ZIP 文件中包含两个带有记录结果的文件：
   - PDF 文件：输出限于 300 页。
   - CSV 文件：完整的记录列表。

测量结果

PDF 文件

PDF 文件包含有效用户数据信号（单位为 dBm）的图形表示以及数据传输速率（单位为 Mbps）的图形表示。在颜色方面，该图与"基于 Web 的管理"的外观相对应。如果客户端在测量期间更改了接入点（漫游），则由顶部带黑色方块的垂直黑条指示。

显示分为两个区域：

- 客户端

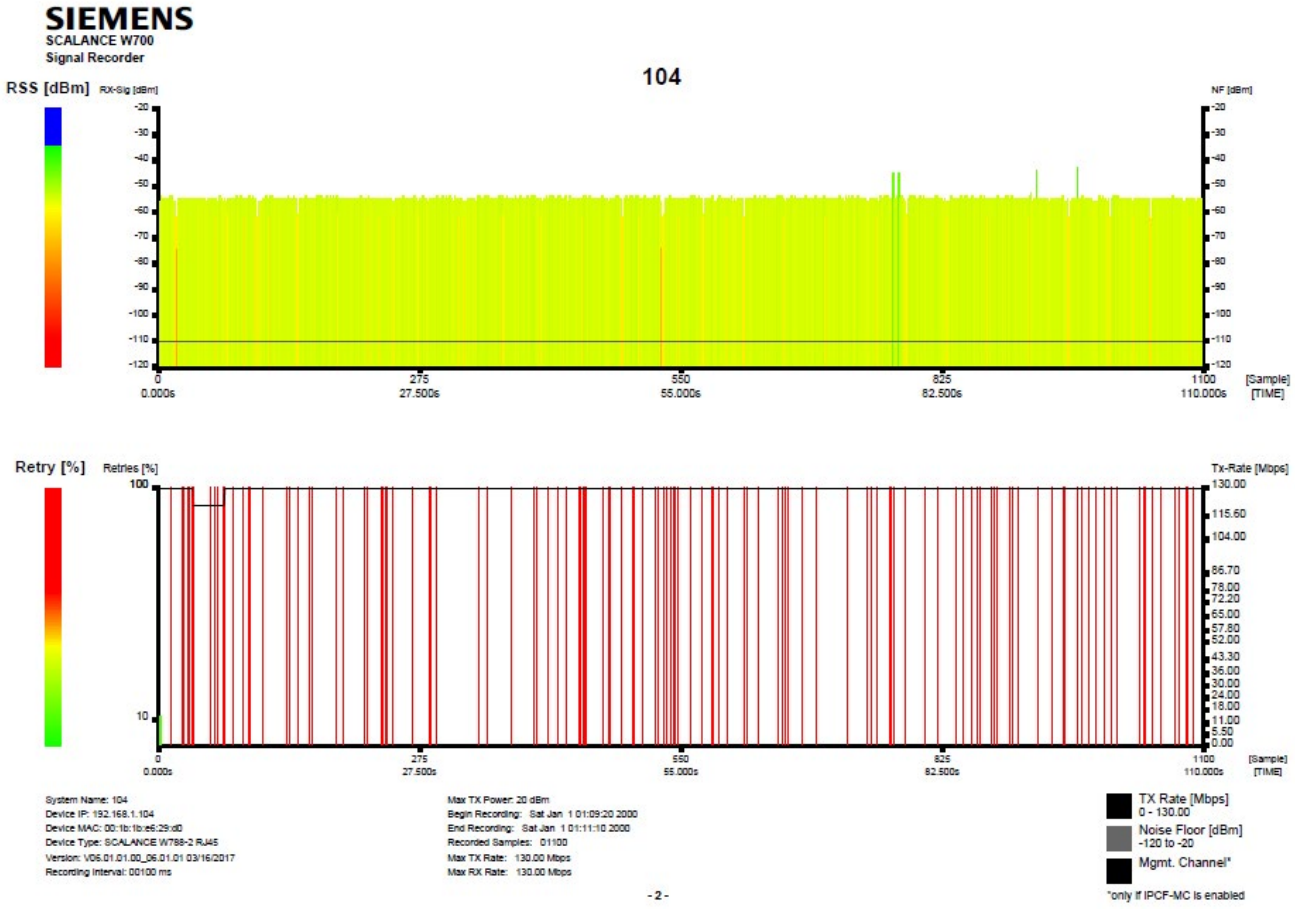
  表示客户端的测量。

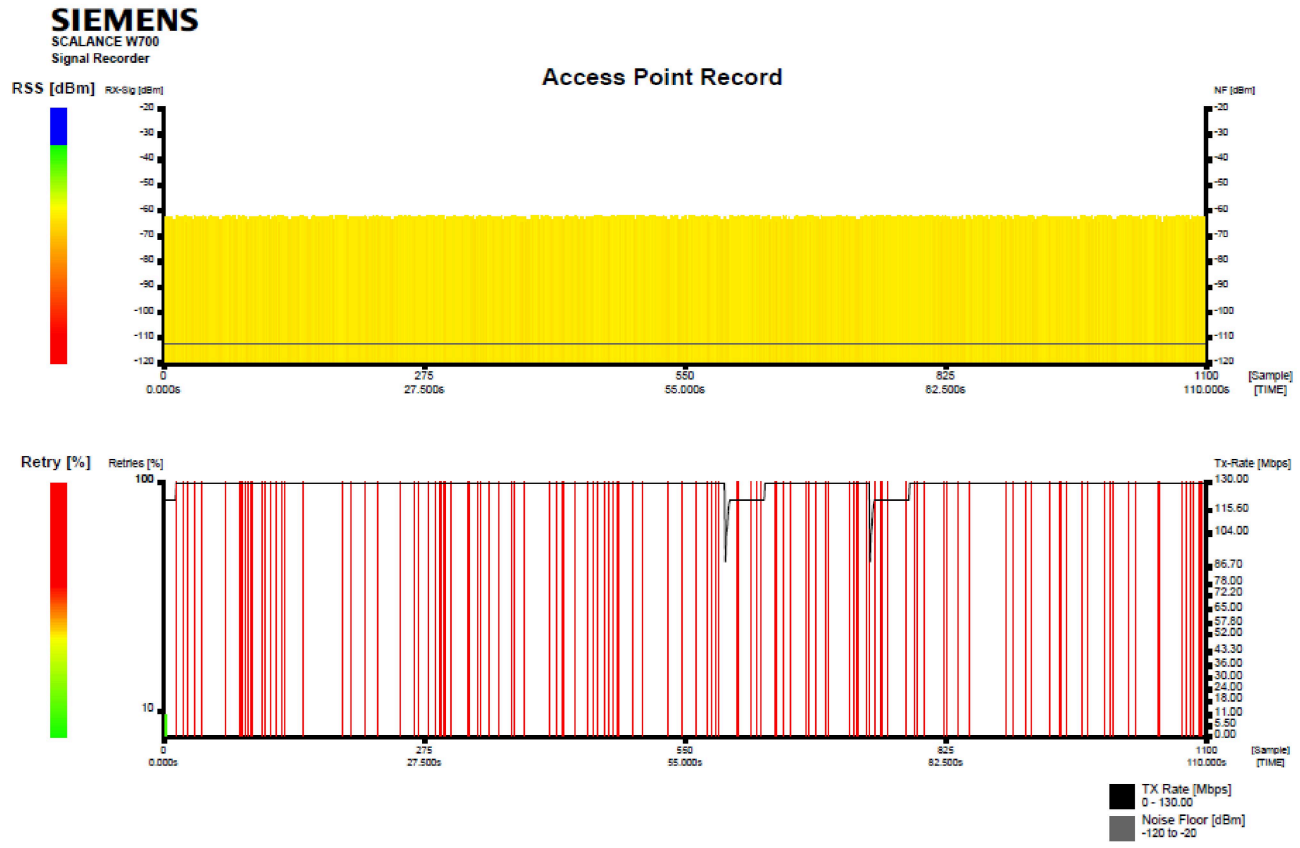
- 接入点

  显示客户端当前连接的接入点的测量。这要求启用"双向记录"(Bidirectional Recording) 设置，而且接入点上安装的固件版本要在 6.1 以上。接入点将其数据发送给最多 3 个运行信号记录器的客户端。接入点数据不会显示在其他客户端上。

如果客户端具有 iPCF-MC 连接，则显示的管理通道的用户信号将带有附加黑线。

在图形下方，显示了客户端的组态数据。





生成的 PDF 文件示例

以下页面以表格的形式包含了每次测量的详细信息。

标题行显示了客户端的 IP 地址以及接入点的 BSSID 和系统名称。

对于每次测量，该表均包含两行。客户端的数据位于第一行，属于接入点的数据位于第二行。

Sample	Timestamp	Sig%	dBm	NF	RSSI	Roam	Ch	Retry%	HT-40	TX-Rate	RX-Rate	Con-St	M-Sig	M-Ch	M-NF
1	01:09:20:090	76	-56	-110	39	0	161	11	-	130.00	121.50	1	---	---	---
		63	-63	-112	32			8							

第 2 页显示了表格中缩略语的说明。客户端更改接入点时，数据将重新另起一页。

说明

请注意 CSV 文件中各个列的说明。这些内容还适用于 PDF 文件的列。

CSV 文件

CSV 文件包含 SCALANCE W700 设备的组态信息以及每次测量的详细信息，可分为两个区域：第一个区域包含已组态的设置：

- System Name

  客户端的系统名称

- Device IP

  客户端的 IP 地址

- Device MAC

  客户端的 MAC 地址

- Recording Interval

  两次采集测量值之间的时间间隔

- Max TX Power

  设备的最大发射功率

- Begin Recording

  开始记录

- End Recording

  结束记录

- Recorded Samples

  测量总数

- Max. TX Rate

  发送数据包的最大数据速率。

- Max. RX Rate

  接收数据包的最大数据速率。

- Rx Antenna x type

  外部天线的设置

第二个区域是表格。表格包含每个测量值的以下内容：

- Sample

  客户端 (CL)/接入点 (AP) 上的当前测量数量

- Timestamp

  时间戳

- BSSID

  接入点的 BSSID（基本服务集标识）

- CL / AP RX-Signal [%]

  客户端 (CL)/接入点 (AP) 的有效用户数据信号，以 % 表示

- CL / AP RX-Signal [dBm]

  客户端 (CL)/接入点 (AP) 的有效用户数据信号，单位为 dBm

- CL / AP NF [dBm]

  背景噪声，单位为 dBm

- CL / AP RSSI

  RSSI（接收信号强度指示）的原始值

- Roam

  漫游计数器显示在记录过程中客户端更改接入点的频率。在 4 294 967 295 次更改后，该计数器将复位。

- CL / AP Retry

  客户端 (CL)/接入点 (AP) 的传输重复率

- Con Stations

  连接到接入点的客户端数量。

- Operating Ch.

  当前通道或客户端与接入点相连所用的通道

- HT-40

  通道带宽 40 MHz

- Scan CH

  客户端进行当前扫描时所在的通道。

- TX-Rate

  发送数据包的平均数据速率

- RX-Rate

  接收的数据包的平均数据传输速率

说明

如果存在 iPCF-MC 连接，则与管理通道相关的列仅包含一个值。

- M-Ch

  管理通道

- M-Sig

  管理通道的有效用户数据信号

- M-NF

  管理通道的背景噪声

- AP System Name

  接入点的系统名称

System Name: 104
Device IP: 192.168.1.104
Device MAC: 00:1b:1b:e6:29:d0
Device Type: SCALANCE W788-2 RJ45
Version: V06.01.01.00_06.01.01 03/16/2017
Recording Interval: 00100 ms
Max TX Power: 20 dBm
Begin Recording: Sat Jan 1 01:09:20 2000
End Recording: Sat Jan 1 01:11:10 2000
Recorded Samples: 01100
Max TX Rate: 130.00 Mbps
Max RX Rate: 130.00 Mbps

R1 Anten Gain: 3 dBi Add. Attenua Cable length: 0 m
R1 Anten Gain: 3 dBi Add. Attenua Cable length: 0 m
R1 Anten Gain: 0 dBi Add. Attenua Cable length: 0 m

Sample	Timestamp	BSSID	CL RX-Signal	AP RX-Sign	CL RX-Sign	AP RX-Sign	CL NF [dBm	AP NF [dBm	CL RSSI	AP RSSI	Roam	CL Retry	AP Retry	Con Stations	Operating Ch.	HT-40	Scan Ch	TX-Rate	RX-Rate	M-Ch	M-Sig	M-NF	AP System Name
1	01:09:20:090	00:1b:1b:e6:	76	63	-56	-63	-110	-112	39	32	0	11	8	1	161	-	161	130.	121.	---	---	---	106
2	01:09:20:190	00:1b:1b:e6:	80	63	-54	-63	-110	-112	41	32	0	0	0	1	161	-	161	130.	121.	---	---	---	106
3	01:09:20:290	00:1b:1b:e6:	76	63	-56	-63	-110	-112	39	32	0	0	0	1	161	-	161	130.	121.	---	---	---	106
4	01:09:20:390	00:1b:1b:e6:	78	63	-55	-63	-110	-112	40	32	0	0	0	1	161	-	161	130.	121.	---	---	---	106
5	01:09:20:490	00:1b:1b:e6:	78	63	-55	-63	-110	-112	40	32	0	0	0	1	161	-	161	130.	121.	---	---	---	106

生成的 CSV 文件示例

6.6.2.13 频谱分析仪

技术信息

频率范围取决于组态。

参数		值
振幅精度	对于 2.4 GHz	3 dBm
	对于 5 GHz	7 dBm
分辨带宽		330 KHz
最小信号强度		-100 dBm
最大信号强度		0 dBm
分析时间	40 MHz 时	120 ms
	20 MHz 时	95 ms
更新时间		1 s

表示频率范围的信号

通过频谱分析仪，您可以识别和表示频率范围的电磁信号。您可以测量位于接入点环境的所有信号的强度。

说明

该 WBM 页面仅在接入点模式下可用。
必须启用设备的 WLAN 接口，否则无法扫描频率范围。

说明

不建议在"手动提交"(Manual Commit) 更改模式下使用频谱分析仪。

说明

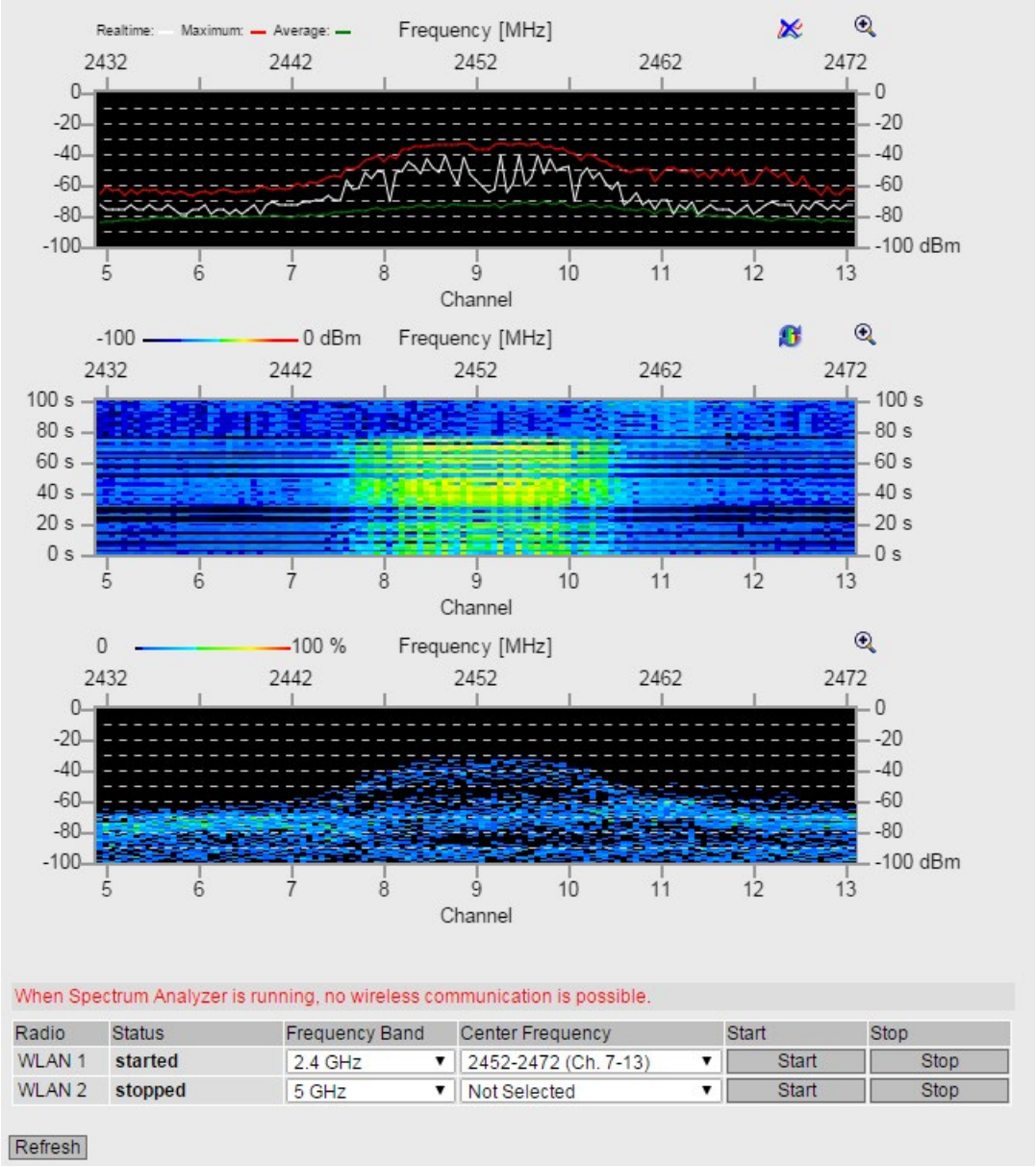
启动频谱分析仪时，所有 WLAN 连接均在两个 WLAN 接口处端接。接入点也不会发送任何信标。

说明

如果设备高效运行，请勿启用频谱分析仪。这会影响设备的性能。

说明

频谱分析仪的功能不会取代专用频谱分析仪。

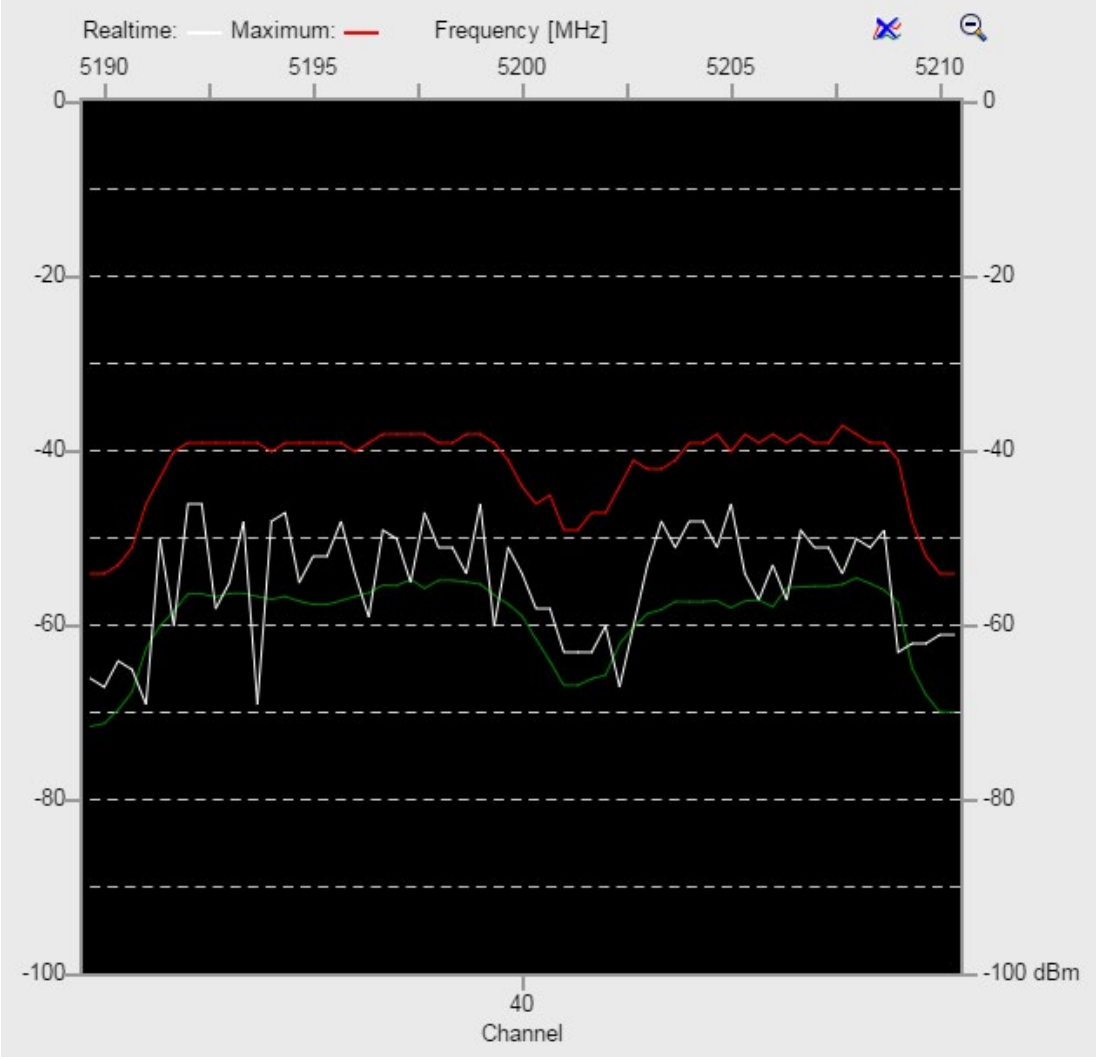


描述

该页面包含以下图形：

在所有图形中，下面的 x 轴显示了进行测量的所选中心频率周围的通道。上面的 x 轴显示了频率范围。Y 轴的显示内容取决于所选图形。

- 实时

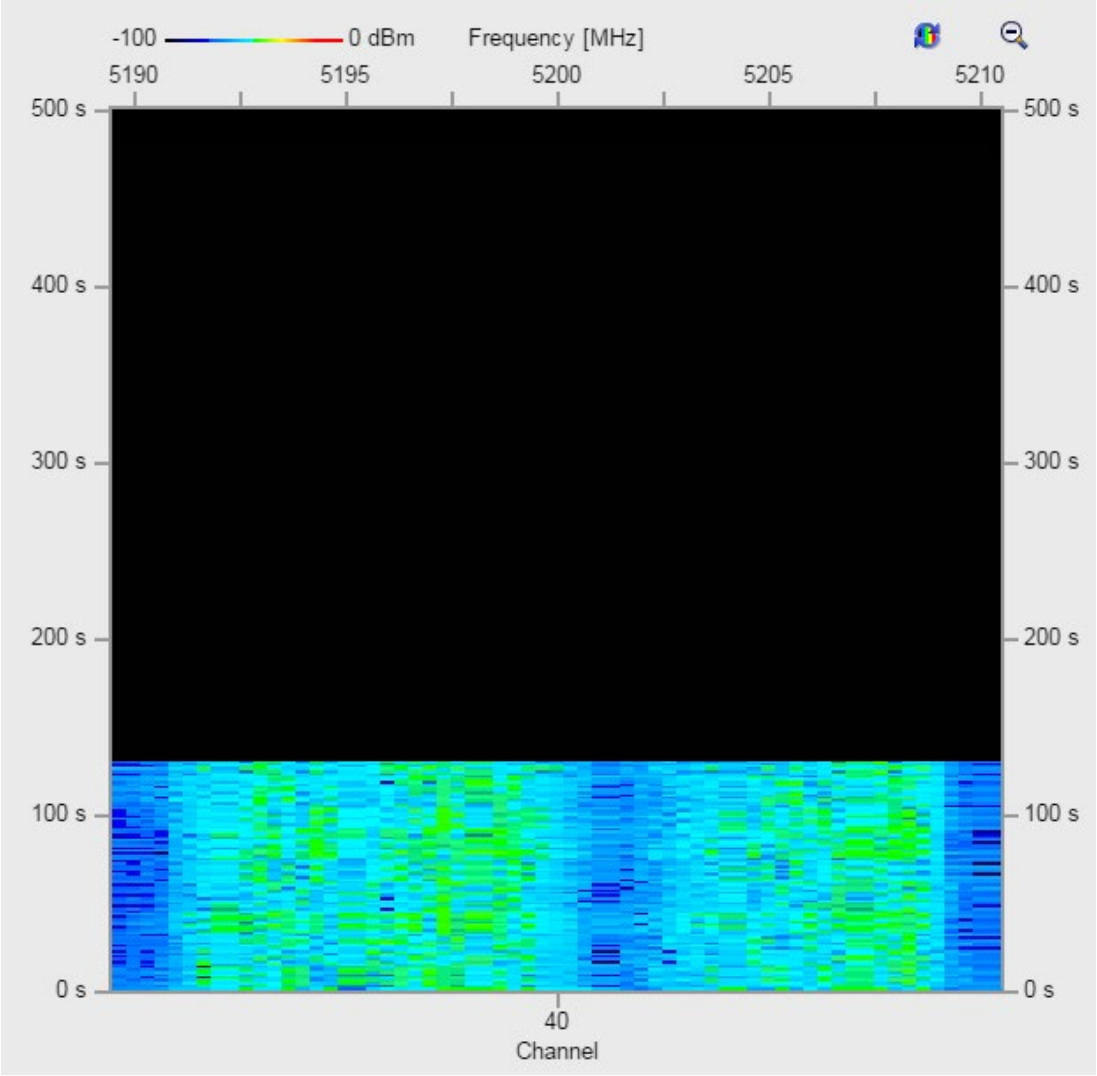


Y 轴显示信号强度（单位为 dBm）。

该图显示了在所组态的频率范围内接入点在其环境下接收的所有信号的强度。

红线显示自开始测量起的最大值。白线显示当前值。绿线显示平均值。

- 光谱图

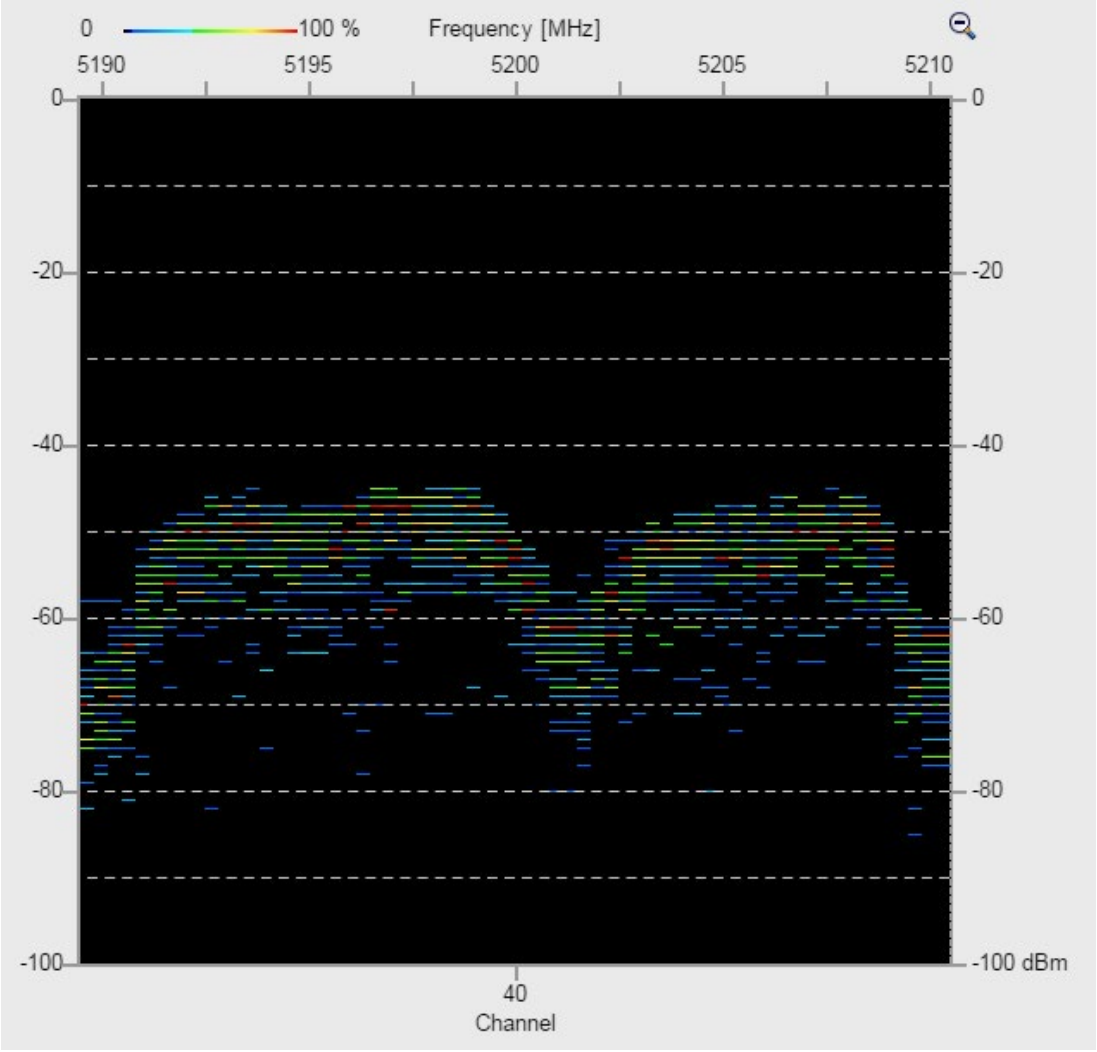


Y 轴显示测量值随时间（从当前值 (0 s) 到 500 s 前接收的值）的变化情况。

该图显示了在所组态的频率范围内接入点在其环境下接收的所有信号的强度。

颜色取决于"颜色方案"(Color Scheme) 的设置。

- 密度图



Y 轴显示信号强度（单位为 dBm）。

该图显示了在所组态的频率范围内某强度信号的出现频率。

颜色从最低值（0%，以黑色表示）到最高值（100%，以红色表示）变化。

该页面包含以下按钮：

- 放大 (Zoom in)

  借助该图标，只能在该页面上以大格式显示一个图形类型。

- 缩小 (Zoom out)

  借助该图标，可以返回到带有全部三个图形类型的视图。

- 颜色方案 (Color Scheme)

  借助该图标，可以更改图形类型"光谱图"的颜色方案：

  – 颜色从最低值（-100 dBm，以黑色表示）到最高值（0 dBm，以红色表示）变化。

  – 颜色从最低值（-100 dBm，以红色表示）到最高值（0 dBm，以黑色表示）变化。

- 复位 (Reset)

  借助该图标，可以复位"实时"图形类型的最大值和平均值。

该表包含以下各列：

- **无线 (Radio)**
  显示应用信息的 WLAN 接口。
- **状态 (State)**

  显示测量的状态。可能的值包括：

  – 已停止 (Stopped)

    测量已停止。

  – 已开始 (Started)

    正在进行测量。

- **频段 (Frequency Band)**

  指定频段。

- **中心频率 (Center Frequency)**
  选择中心频率。
- **开始 (Start)**
  单击此列中的按钮开始测量。
- **停止 (Stop)**
  单击此列中的按钮结束测量。

步骤

1. 从"频段"(Frequency Band) 下拉列表中选择所需频段。
2. 从"中心频率"(Center Frequency) 下拉列表中选择所需的中心频率。
3. 单击"开始"(Start) 按钮。
4. 要停止测量，请单击"停止"(Stop) 按钮。
5. 可以在测量期间调整第二个表中的设置。
6. 切换到以下菜单项之一以调用测量结果：
   - 系统 > 加载和保存 > HTTP (System > Load&Save > HTTP)
     单击"WLANSpectrumAnalyzer"表行中的"保存"(Save) 按钮，以将文件"wlan_spectrum_analyzer_SCALANCE_W700.zip"保存在所连接 PC 的文件系统中。
   - 系统 > 加载和保存 > TFTP (System > Load&Save > TFTP)
     必要时，可在"WLANSpectrumAnalyzer"表行中更改文件名"wlan_spectrum_analyzer_SCALANCE_W700.zip"。在表行"WLANSpectrumAnalyzer"中，从最后一列的下拉列表中选择"保存文件"(Save file) 条目，然后单击"保存值"(Save Values) 按钮。
7. ZIP 文件包含带有测量结果的 CSV 文件。

测量结果

CSV 文件

CSV 文件包含设备组态信息和每次测量的详细信息，可分为两个区域。第一个区域包含已组态的设置：

- 系统名称

  接入点的系统名称

- 设备 IP

  设备的 IP 地址

- 设备 MAC

  设备的 MAC 地址

- 记录间隔

  两次采集测量值之间的时间间隔

第二个区域是表格。表格包含每个测量值的以下内容：

- 样本 (Sample)

  测量的顺序号

- 时间戳 (Timestamp)

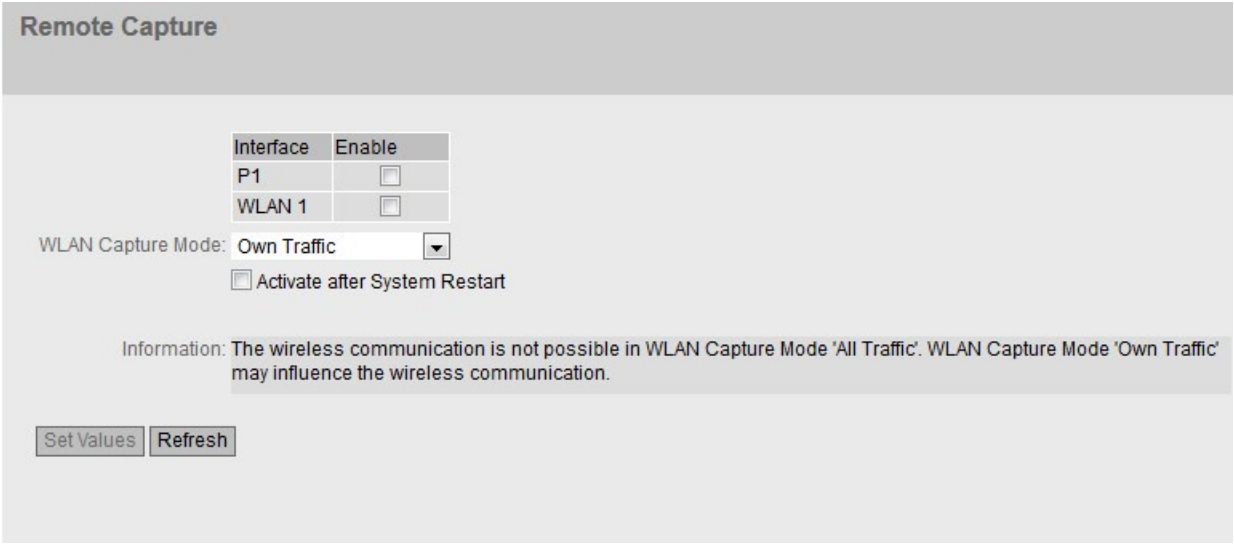
  时间戳

- 以下各列显示了所选频段的所有频率。只能为值已测量的频率填写单元格。测量值显示信号强度（单位为 dBm）。

6.6.3 Remote Capture

在此 WBM 页面激活接口（以太网、WLAN）上的"远程采集"(Remote Capture) 功能。该功能用于通过连接的 PC 进行网络诊断，例如，检测传输错误。

还可同时为多个接口启用该功能。启用该功能后，可在 Wireshark 中链接接口。在一段时间内，Wireshark 通过接口记录数据通信。之后，可从记录中查看帧的内容或根据特定内容进行过滤。



说明

该表包含以下列：

- **接口 (Interface)**

  与条目相关的接口。

- **启用 (Enable)**

  启用或禁用"远程采集"(Remote Capture) 功能。默认情况下会禁用该功能。

  说明

  性能

  仅启用该功能以进行诊断。增加的数据通信会影响设备的性能。

该页面包含以下框：

- **WLAN 采集模式 (WLAN Capture Mode)（仅限接入点模式）**

  指定 WLAN 接口的记录模式：

  – 自身通信 (Own Traffic)

    在这种情况下，记录由设备接收和发送的帧。

    例外情况：不显示由硬件直接处理的数据包，例如硬件重复、确认帧。

  – 所有通信 (All Traffic)

    接入点不再发送帧，但会记录所有传入数据包。

  说明

  接入点与客户端之间无 WLAN 通信
  如果使用"所有通信"(All Traffic) 设置，其它节点不再能够访问接入点，且接入点会失去连接的客户端。

- **系统重启后激活 (Activate after System Restart)**

  – 禁用

    重新启动后，组态复位为默认设置。

  – 启用

    重新启动后，组态将被保存并保留。

Wireshark 中的接口链接

要求：

- 已在 PC 上安装 Wireshark V2.0.0。
- PC 和设备必须可通过 IP（第 3 层）访问。

步骤

例如，要分析 Wireshark 中 WLAN 接口 1 的数据通信，请按以下步骤操作：

1. 激活 WLAN 接口的设备中的"远程采集"(Remote Capture) 功能。
2. 在接收模式下，选择"自身通信"(Own Traffic)。
3. 单击"设置值"(Set Values) 启用该功能。
4. 启动 Wireshark。
5. 单击"采集"(Capture) 菜单中的"选项"(Options)。随即打开"Wireshark - 采集接口"(Wireshark - Capture Interfaces) 窗口。
6. 单击"输入"(Input) 选项卡上的"管理接口..."(Manage Interfaces...) 按钮。在以下对话框中，单击"远程接口"(Remote Interfaces) 选项卡。
7. 要添加接口，请单击"远程接口"(Remote Interfaces) 选项卡上的加号。
8. 在随后的对话框中，为"主机"(Host) 输入设备的 IPv4 地址，为"端口"(Port) 输入 2002。
9. 为"验证"(Authentication) 启用"空验证"(Null authentication)，然后单击"确定"(OK) 按钮。
10. 在"远程接口"(Remote Interfaces) 选项卡上，将显示之前启用了"远程采集"(Remote Capture) 功能的主机和接口。
11. 选择接口，然后单击"确定"(OK) 按钮。
12. 要开始记录，请单击"开始"(Start)。可以从 Wireshark 中获得有关处理程序的更多信息。

如果要分析多个接口，可以为每个接口使用一个 Wireshark 实例。

6.7 "Layer 2"菜单

6.7.1 VLAN

6.7.1.1 常规

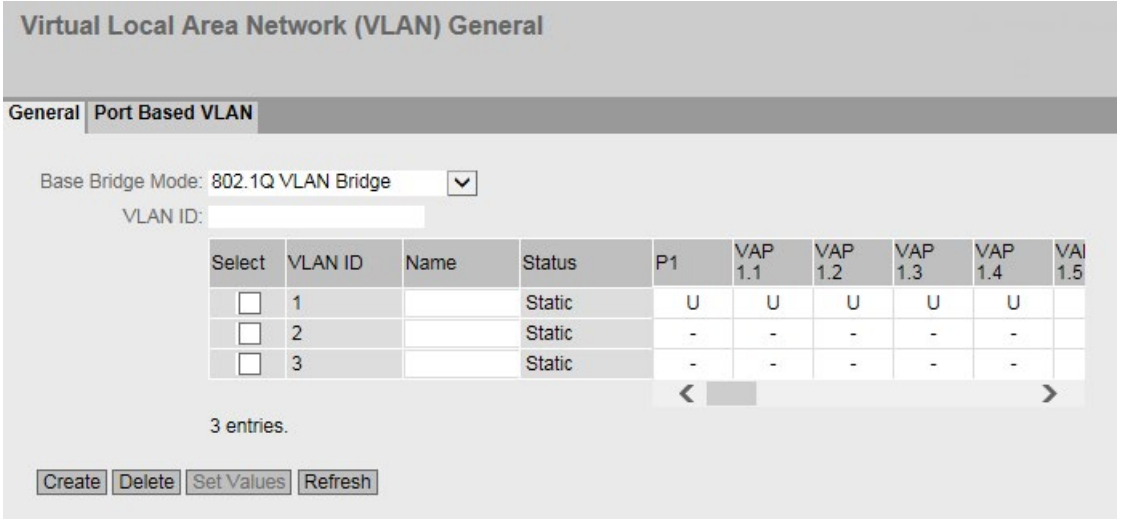
VLAN 组态页面

在该页面，可以指定设备是否以透明方式转发带有 VLAN 标记的帧（IEEE 802.1D/VLAN 非感知模式），或者指定设备是否考虑 VLAN 信息（IEEE 802.1Q/VLAN 感知模式）。如果设备处于"802.1Q VLAN 网桥"模式下，则可以定义 VLAN 并指定端口的使用。

说明

更改代理 VLAN ID

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



描述

该页面包含以下框：

- **基础网桥模式 (Base Bridge Mode)**

  从下拉列表中选择需要的模式。可能的模式如下：

  说明

  切换基础网桥模式
  请参见"切换基础网桥模式"部分。此部分介绍模式切换对现有组态的影响。

  – 802.1Q VLAN Bridge

    将设备模式设置为"VLAN 识别"。在此模式下，会将 VLAN 信息考虑在内。在此模式下，可创建附加 VLAN。

  – 802.1D Transparent Bridge

    将设备模式设置为"VLAN 不识别"。在此模式下，不会更改 VLAN 标记，而会以透明方式转发这些标记。为 CoS 评估 VLAN 优先级。在此模式下，无法创建任何 VLAN。仅管理 VLAN 可用：VLAN 1。

- **VLAN ID**

  在"VLAN ID"输入框中输入 VLAN ID。
  取值范围：1 ... 4094

该表格包括以下列：

- **选择 (Select)**

  选中要删除的行中的复选框。

- **VLAN ID**

  显示 VLAN ID。VLAN ID（介于 1 到 4094 之间的数字）只能在创建新数据记录时被分配一次，之后不能更改。如要更改，必须删除整个数据记录并重新创建。可最多定义 8 个 VLAN。

- **名称 (Name)**

  输入 VLAN 的名称。此名称仅提供信息，对组态没有影响。最大长度为 32 个字符。

- **状态 (Status)**

  显示端口过滤器表中条目的状态类型。此处，"静态"(static) 表示地址由用户作为静态地址输入。

- **List of ports**

  指定端口的使用方式。可使用以下选项：

  – "-"

    该端口不是指定 VLAN 的成员。

    对于新定义，所有端口的标识符均为"-"。

  – M

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

  – U（大写）

    此端口是无标记的 VLAN 成员。此 VLAN 中发送的帧在转发时不带 VLAN 标记。不带 VLAN 标记的帧通过此端口发送。

  – u（小写）

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

  – F

    此端口不是指定 VLAN 的成员。可以在"Layer 2 > VLAN > 基于 VLAN 的端口"中组态其他设置。

  – T

    该选项只显示，无法在 WBM 中选择。

    此端口是中继端口，可成为所有 VLAN 的成员。

    可在 CLI（命令行接口）中使用"`switchport mode trunk`"命令组态此功能。

切换基础网桥模式

VLAN 不识别（802.1D 透明网桥）→ VLAN 识别（802.1Q VLAN 网桥）

如果将"基础网桥模式"从 VLAN 不识别切换为 VLAN 识别，则会产生以下影响：

- 所有静态和动态单播条目都将被删除。

VLAN 识别（802.1Q VLAN 网桥）→ VLAN 不识别（802.1D 透明网桥）

若将基础网桥模式从"VLAN 识别"切换为"VLAN 不识别"，则会产生以下影响：

- 所有 VLAN 组态均被删除。
- 将创建一个管理 VLAN：VLAN 1。
- 所有静态和动态单播条目都将被删除。

802.1Q VLAN 网桥：VLAN 的重要规则

组态和运行 VLAN 时，确保遵守以下规则：

- VLAN ID 为"0"的帧会按照无标记帧处理，但会保留其优先级值。
- 默认情况下，设备上的所有端口均发送不带 VLAN 标记的帧，以确保终端节点可接收这些帧。
- 对于 SCALANCE W 设备，所有端口的 VLAN ID 都默认为 1。
- 如果终端节点连接到端口，发送的离开帧不应带标记（静态访问端口）。但是，如果此端口有另一台交换机，则发送的帧应添加标记（中继端口）。
- 对于中继端口，VLAN 分配是动态的。除中继端口属性外，仅当端口也作为相关 VLAN 中的成员以静态方式输入时，才能创建静态组态。静态组态的一个示例是某些 VLAN 中多个组播组的分配。

步骤

要求：

设置了基础网桥模式"802.1Q VLAN Bridge"。

创建新 VLAN

1. 在"VLAN ID"输入框内输入一个 ID。
2. 单击"创建"(Create) 按钮。会在表中生成一个新条目。默认情况下，各个框均输入"-"。
3. 在"名称"(Name) 下输入 VLAN 的名称。
4. 指定 VLAN 中端口的使用方式。例如，如果选择 M，则该端口是 VLAN 的成员。在此 VLAN 中发送的帧在转发时带有相应 VLAN 标记。
5. 指定设备的模式。
6. 单击"设置值"(Set Values) 按钮。

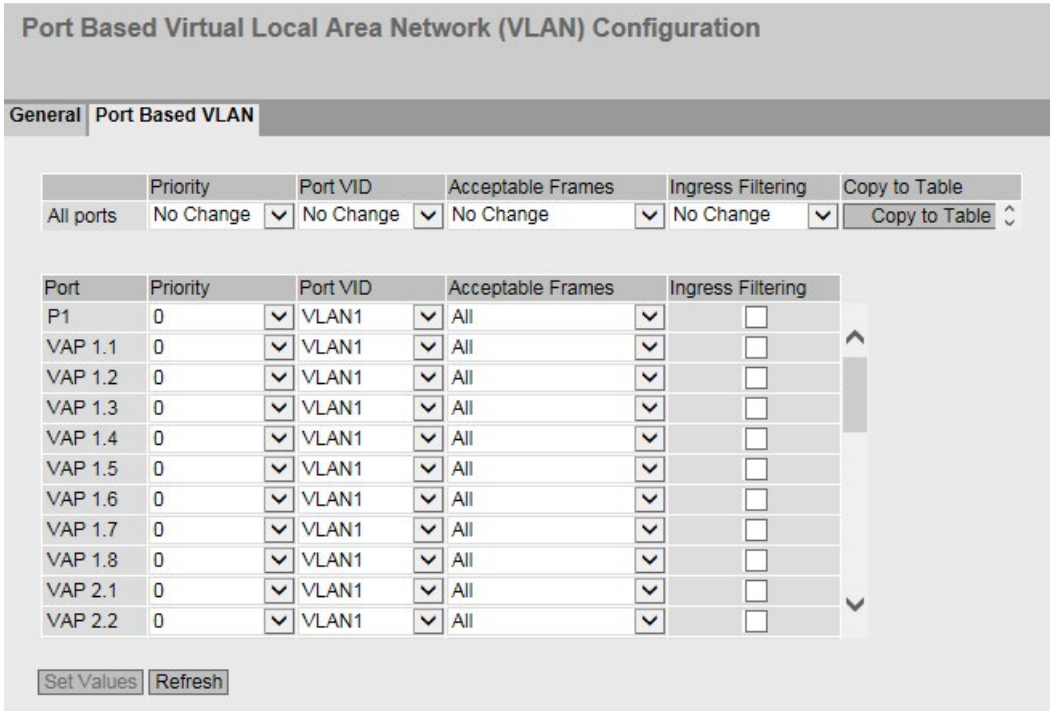
6.7.1.2 基于端口的 VLAN

处理接收到的帧

在此页面中，指定用于接收帧的端口属性组态。

要求：

- 在"常规"(General) 页面中，将"基础网桥模式"(Base Bridge Mode) 设为"802.1Q VLAN Bridge"。



说明

表 1 包含以下列：

说明

表 1 仅在至少组态了一个 VLAN 时才可用。

- **端口 (Port)**

  说明设置对于表 2 的所有端口都有效。

- **优先级/端口 VID/可接受帧/入站过滤 (Priority / Port VID / Acceptable Frames / Ingress Filtering)**

  在此下拉列表中，选择适用于所有端口的设置。如果选择"No Change"，则表 2 中相应列的条目保持不变。

- **复制到表 (Copy to Table)**

  如果单击此按钮，则为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **端口 (Port)**

  显示可用的端口和接口。

- **优先级 (Priority)**

  从下拉列表中选择分配给无标记帧的优先级。

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

- **端口 VID (Port VID)**

  从下拉列表中选择 VLAN ID。只能选择在"VLAN > 常规"(VLAN > General) 页面中定义的 VLAN ID。
  如果接收到的帧没有 VLAN 标记，则会为其添加此处指定的 VLAN ID 作为标记，然后按照端口规则发送出去。

- **可接受帧 (Acceptable Frames)**

  指定将接受哪些类型的帧。可能的选项如下：

  – 仅限带标记的帧 (Tagged Frames Only)
    设备会丢弃所有无标记帧。否则，按照组态应用转发规则。

  – 全部 (All)
    设备会转发所有帧。

  – 不变 (No Change)
    如果选中"不变"(No Change)，则表 2 中相应列的条目保持不变。

- **入站过滤 (Ingress Filtering)**

  指定是否评估接收到帧的 VID。
  可做以下选择：

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

  – 禁用 (Disabled)
    转发所有帧。

  – 不变 (No Change)
    如果选中"不变"(No Change)，则表 2 中相应列的条目保持不变。

步骤

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

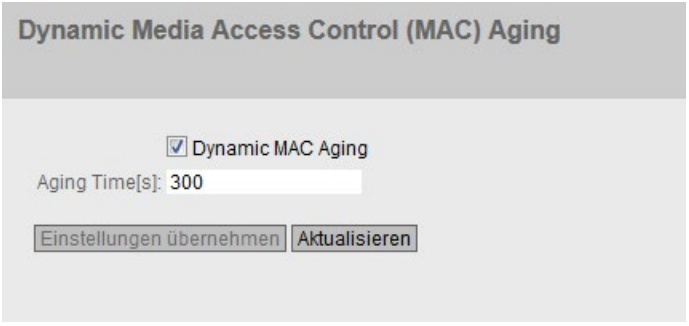
6.7.2 Dynamic MAC Aging

协议设置和交换机功能

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

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

如果未启用该复选框，则设备不会自动删除学习的地址。



说明

该页面包含以下框：

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

步骤

1. 选中"动态 MAC 老化"(Dynamic MAC Aging) 复选框。
2. 在"老化时间 [s]"(Aging Time [s]) 输入框中输入时间（以秒为单位）。
3. 单击"设置值"(Set Values) 按钮。

6.7.3 Spanning Tree

6.7.3.1 常规

生成树的常规设置

这是生成树的基本页面。从下拉列表中选择兼容模式。默认情况下会启用多重生成树。

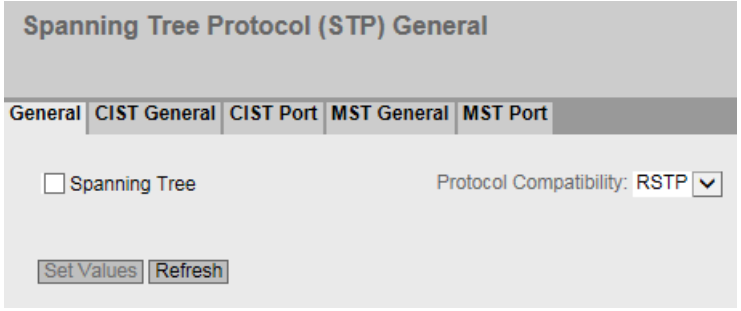
在这些功能的组态页面，可进行详细设置。

根据具体的兼容性模式，可以在相关组态页面组态相应的功能。

说明

客户端设备不可作为根节点

通过组态优先级和路径开销，确保客户端设备始终不会成为根节点。如果客户端设备成为根节点，则"快速生成树"功能将不可用。



说明

该页面包含以下框：

- **Spanning Tree**

  启用或禁用 MSTP。

- **协议兼容性 (Protocol Compatibility)**

  选择 MSTP 的兼容模式。例如，如果选择 RSTP，则 MSTP 将发挥 RSTP 的功能。

  可使用以下设置：

  – STP

  – RSTP

  – MSTP

说明
如果已启用 iPCF 模式，则将仅支持 STP 和 RSTP 兼容模式。

步骤

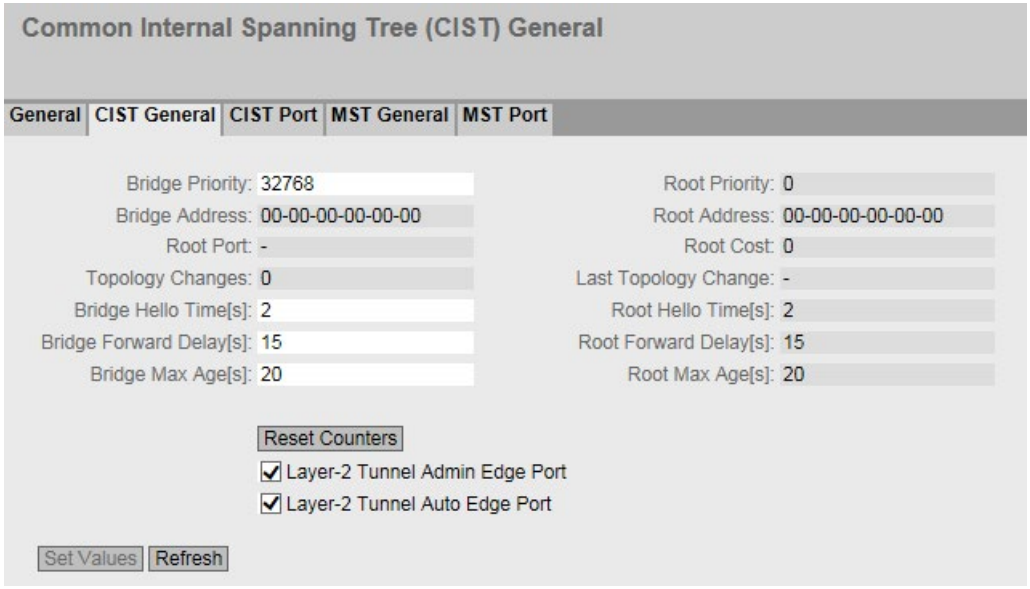
1. 选中"MSTP"复选框。
2. 从"协议兼容性"(Protocol Compatibility) 下拉列表中选择兼容模式。
3. 单击"Set Values"按钮。

6.7.3.2 CIST 常规

MSTP-CIST 组态

此页面由以下几部分组成。

- 页面的左侧显示设备的组态。
- 中间部分显示根网桥的组态，该组态可从设备接收到的生成树帧获得。
- 右侧显示区域根网桥的组态，该组态可从设备接收到的 MSTP 帧获得。只有在"常规"(General) 页面上启用了"Spanning Tree"并且"协议兼容性"(Protocol Compatibility) 被设置为"MSTP"时，显示的数据才可见。这也适用于"Bridge Max Hop Count"参数。如果设备是根网桥，则左右两侧显示的信息相匹配。



描述

该页面包含以下框：

- **网桥优先级 (Bridge Priority)/根优先级 (Root Priority)**

  根据网桥优先级来确定哪台设备会成为根网桥。优先级最高的网桥会成为根网桥。数值越小，优先级越高。如果网络中有多个设备具有相同优先级，则 MAC 地址数值最小的设备将成为根网桥。网桥优先级和 MAC 地址这两个参数一起构成网桥标

识符。由于根网桥管理所有路径的变更，出于帧延迟的考虑，根网桥应该尽可能处在中心位置。网桥优先级的值是 4096 的整数倍数，值范围从 0 到 61440。

- **网桥地址 (Bridge Address)/根地址 (Root Address)**

  网桥地址显示设备的 MAC 地址，根地址显示根网桥的 MAC 地址。

- **根端口 (Root port)**

  显示交换机与根网桥通信时所使用的端口。

- **根开销 (Root Cost)**

  从该设备到根网桥的路径开销。

- **拓扑变更 (Topology Changes)/上次拓扑变更 (Last Topology Change)**

  该设备条目显示自上次启动以来，由于生成树机制而执行的重新组态操作次数。对于根网桥，自上次重新组态到现在的时间显示如下：

  – 秒：数字后面采用的单位为 sec

  – 分钟：数字后面采用的单位为 min

  – 小时：数字后面采用的单位为 hr

- **拓扑变更 (Topology Changes)/上次拓扑变更 (Last Topology Change)**

  每个网桥都会定期发送组态帧 (BPDU)。呼叫时间即为两个此类帧之间的时间间隔。此参数的默认值为 2 秒。

- **网桥转发延迟 [s] (Bridge Forward Delay[s])/根转发延迟 [s] (Root Forward Delay[s])**

- 网桥不会立即使用新的组态数据，而是在经过转发延迟参数中指定的时间之后才使用。这样可确保在所有网桥都收到所需的信息之后才开始使用新拓扑运行。此参数的默认值为 15 秒。

- **网桥最大老化时间 (Bridge Max Age)/根最大老化时间 (Root Max Age)**

  "网桥最大老化时间"定义接收到的 BPDU 可被交换机作为有效信息接受的最长"期限"。此参数默认为 20。

- **Bridge Max Hop Count**

  此参数指定 BPDU 可通过多少个 MSTP 节点。如果接收到一个 MSTP BPDU 并且其跳跃计数超过此处组态的值，则会将其丢弃。此参数默认为 20。

- **区域根优先级 (Regional root priority)**

  有关显示值的描述，请参见网桥优先级 (Bridge priority)/根优先级 (Root priority)

- **区域根地址 (Regional root address)**

  显示区域根网桥的 MAC 地址。

- **区域根开销 (Regional Root Cost)**

  显示从设备到区域根网桥的路径开销。

- **区域名称 (Region Name)**

  输入此设备所属的 MSTP 区域的名称。默认情况下，在此处输入此设备的 MAC 地址。所有属于相同 MSTP 区域的设备上的值必须相同。

- **区域版本 (Region Version)**

  输入设备所在的 MSTP 区域的版本号。所有属于相同 MSTP 区域的设备上的值必须相同。

- **复位计数器 (Reset Counters)**

  单击该按钮可复位此页面上的计数器。

- **第 2 层隧道管理边缘端口 (Layer-2 Tunnel Admin Edge Port)（仅在接入点模式下可用）**

  如果第 2 层隧道端口上可能有终端设备，请选中此复选框。否则只要修改到此端口的链路，就将触发对网络的重新组态。L2T 客户端应互连。

- **第 2 层隧道自动边缘端口 (Layer-2 Tunnel Auto Edge Port)（仅在接入点模式下可用）**

  如果想要自动检测所有第 2 层隧道端口上是否连接了终端设备，请选中此复选框。

步骤

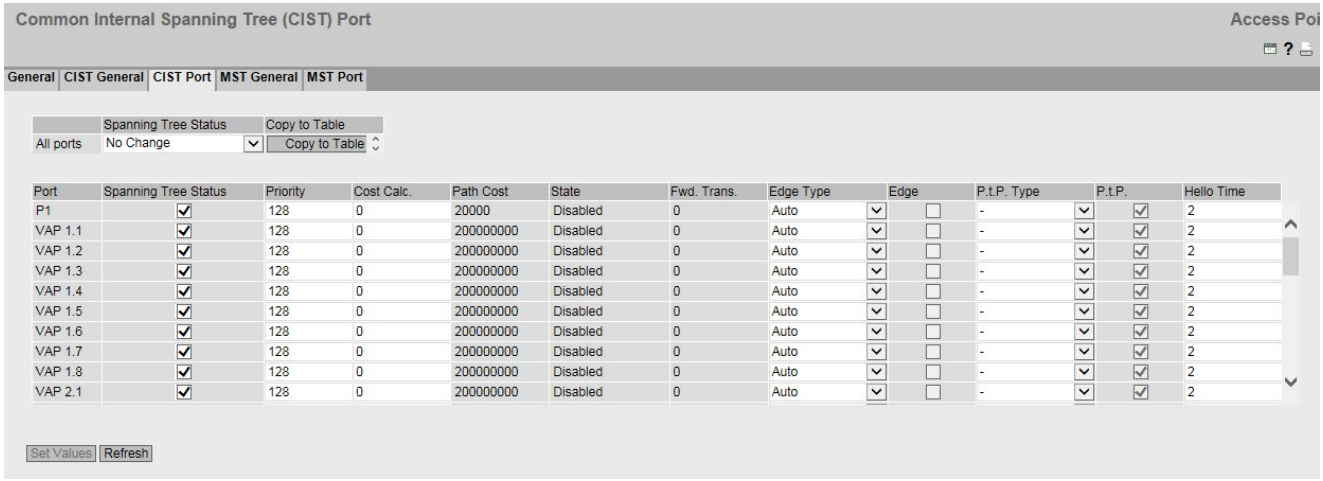
1. 在输入框中输入组态所需的数据。
2. 单击"设置值"(Set Values) 按钮。

6.7.3.3 CIST 端口

MSTP-CIST 端口组态

调用此页面时，表中显示端口参数组态的当前状态。

要进行组态，请单击端口表中的相关单元格。



说明

表 1 包含以下列：

- **列 1 (Column 1)**

  说明设置对于表 2 的所有端口都有效。

- **生成树状态 (Spanning Tree Status)**

  在此下拉列表中，选择适用于所有端口的设置。如果选中"无变化"(No Change)，则表 2 中相应列的条目保持不变。

- **复制到表 (Copy to Table)**

  如果单击此按钮，则为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **端口 (Port)**

  显示可用的端口和接口。

  – Port X

  – WLAN X

  – VAP X.Y

  – WDS X.Y

- **生成树状态 (Spanning Tree Status)**

  指定是否将端口集成到生成树中。

  说明

  如果禁用端口的"生成树状态"(Spanning Tree Status) 选项，可能导致形成环路。必须留意拓扑。

- **优先级 (Priority)**

  输入端口的优先级。仅当路径成本相同时才评估优先级。

  该值必须能被 16 整除。如果该值不能被 16 整除，则会自动调整该值。

取值范围：0 - 240。

默认值为 128。

- **开销计算 (Cost Calc.)**

  输入路径开销计算。如果在此输入值"0"，则自动计算出的值会显示在"路径开销"(Path Cost) 框中。

- **路径开销 (Path Cost)**

  从端口到根网桥的路径开销。选择值最小的路径作为路径。如果设备的多个端口具有相同的值，则会选择端口号最小的端口。

  如果"开销计算"(Cost Calc.) 框的值为"0"，则显示自动计算出的值。

  否则会显示"开销计算"(Cost Calc.) 框的值。

  主要根据传输速度来计算路径开销。可达到的传输速度越高，路径开销的值就越小。

  快速生成树的典型路径开销值如下：

  – 1000 Mbps = 20,000

  – 100 Mbps = 200,000

  – 10 Mbps = 2,000,000

  但是，也可以单独设置各个值。

- **状态 (State)**

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

  – Disabled

    该端口仅接收，未包括在 STP、MSTP 和 RSTP 中。

  – Discarding

    在"丢弃"模式下，接收 BPDU 帧。其它进入或离开的帧会被丢弃。

  – Listening

    在此状态下，接收和发送 BPDU。端口包括在生成树算法中。

  – Learning

    转发状态之前的阶段，端口主动学习拓扑（换句话说，节点寻址）。

  – Forwarding

    在重新组态时间后，端口在网络中激活；端口接收和转发数据帧。

- **Fwd. Trans**

  指定从"Discarding"状态变为"Forwarding"状态的次数。

- **边缘类型 (Edge Type)**

  指定边缘端口的类型。可做以下选择：

  – "-"

    禁用边缘端口。端口被视为"无边缘端口"。

  – Admin

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

  – Auto

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

  – Admin/Auto

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

- **Edge**

  显示端口的状态。

  – 启用

    将终端设备连接到此端口。

  – 禁用

    此端口上有生成树或快速生成树设备。

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

- **P.t.P. 类型 (P.t.P. type)**

  从下拉列表中选择所需选项。该选择取决于所设置的端口。

  – P.t.P.

    即使为半双工，也认为是点对点链路。

  – Shared Media

    即使为全双工连接，也不认为是点对点链路。

  说明

  点对点链路表示在两个设备之间直接连接。而共享介质连接可以是与集线器的连接。

  – "-"

    自动确定点对点。如果端口被设置为半双工，则不认为是点对点链路。

- **P.t.P.**

  – 启用

    表示点对点链路存在。

  – 禁用

    表示点对点链路不存在。

- **Hello Time**

  输入网桥发送组态 BPDU 前所需经过的时间间隔。默认情况下，会设置 2 秒。

  取值范围：1-2 秒

  说明

  只有在 MSTP 兼容模式下才能对呼叫时间进行端口特定的设置。

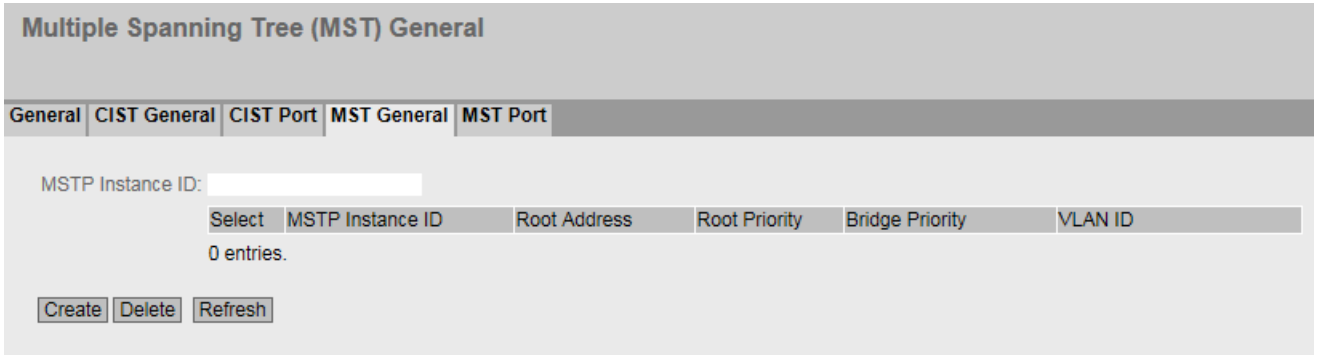
步骤

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

6.7.3.4 MST 常规

多重生成树组态

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



说明

该页面包含以下框：

- **MSTP 实例 ID (MSTP Instance ID)**

  输入 MSTP 实例编号。

  允许的值：1 - 64

  最多可以定义 16 个 MSTP 实例。

该表格包括以下列：

- **选择 (Select)**

  选择要删除的行。

- **MSTP 实例 ID (MSTP Instance ID)**

  显示 MSTP 实例编号。

- **根地址 (Root Address)**

  显示根网桥的 MAC 地址

- **根优先级 (Root Priority)**

  显示根网桥的优先级。

- **网桥优先级 (Bridge Priority)**

  在此框中输入网桥优先级。网桥优先级的值是 4096 的整数倍数，值范围从 0 到 61440。

- **VLAN ID**

  输入 VLAN ID。在此处还可以通过"起始 ID"、"-"、"结束 ID"来指定范围。用","分隔多个范围或 ID。
  允许值：1- 4094

步骤

创建新条目

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

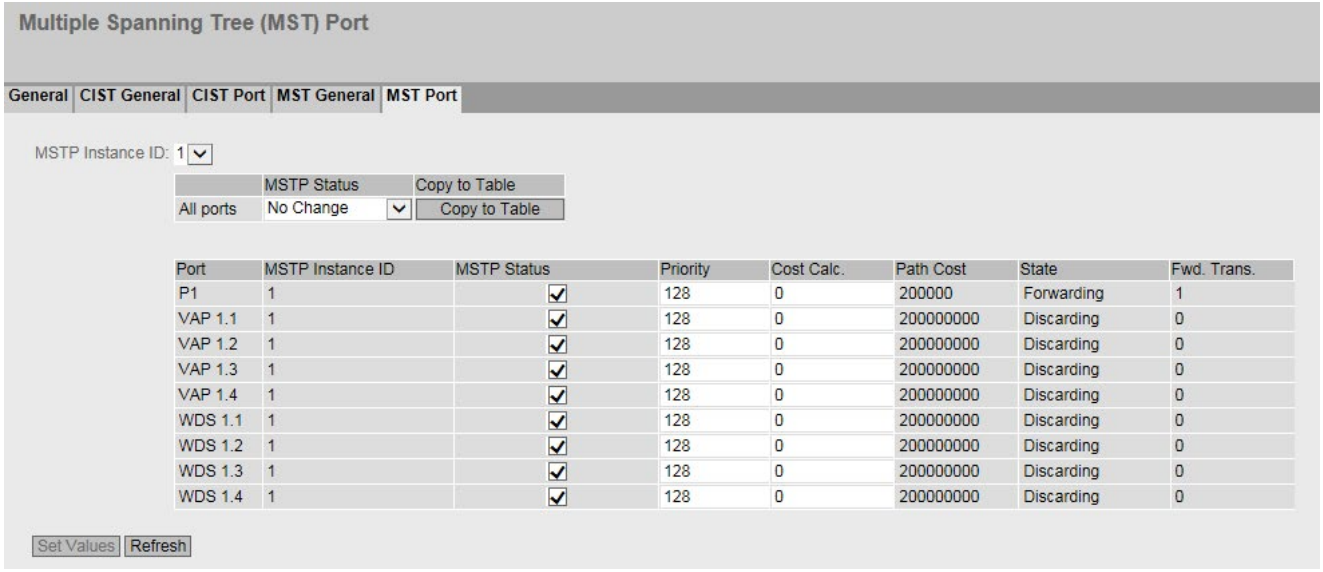
删除条目

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

6.7.3.5 MST 端口

组态多重生成树端口参数

在此页面，设置所组态多重生成树实例的端口参数。



说明

该页面包含以下框：

- **MSTP 实例 ID (MSTP Instance ID)**

  在该下拉列表中选择 MSTP 实例的 ID。

表 1 包含以下列：

- **列 1 (Column 1)**
  说明设置对于表 2 的所有端口都有效。
- **MSTP 状态 (MSTP Status)**

  在此下拉列表中，选择适用于所有端口的设置。如果选中"无变化"(No Change)，则表 2 中相应列的条目保持不变。
- **复制到表 (Copy to Table)**
- 如果单击此按钮，则为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **端口 (Port)**

  显示所有可用的端口和接口。
- **MSTP 实例 ID (MSTP instance ID)**
  显示 MSTP 实例的 ID。
- **MSTP 状态 (MSTP Status)**

  单击此复选框可启用或禁用此选项。
- **优先级 (Priority)**

  输入端口的优先级。仅当路径成本相同时才评估优先级。
  该值必须能被 16 整除。如果该值不能被 16 整除，则会自动调整该值。
  取值范围：0 - 240。
  默认值为 128。
- **开销计算 (Cost Calc.)**

  在输入框中输入路径开销计算。如果在此输入值"0"，则"路径开销"(Path Costs) 框中会显示自动计算出的值。
- **路径开销 (Path Cost)**

  从端口到根网桥的路径开销。选择值最小的路径作为路径。如果设备的多个端口具有相同的值，则会选择端口号最小的端口。

如果"开销计算"(Cost Calc.) 框的值为"0"，则显示自动计算出的值。

否则会显示"开销计算"(Cost Calc.) 框的值。

主要根据传输速度来计算路径开销。可达到的传输速度越高，路径成本的值就越低。

快速生成树的典型值如下：

– 1000 Mbps = 20,000

– 100 Mbps = 200,000

– 10 Mbps = 2,000,000

但是，也可以单独设置各个值。

- **状态 (Status)**

  显示端口的当前状态。这些值只能显示，但无法组态。可能的状态有：

  – Discarding

    端口会交换 MSTP 信息，但不会参与数据通信。

  – Blocked

    在阻止模式下，接收 BPDU 帧。

  – Forwarding

    该端口接收和发送数据帧。

- **Fwd. Trans.**

  指定状态变化的次数 Discarding - Forwarding 或 Forwarding - Discarding。

步骤

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

6.7.4 DCP 转发

应用

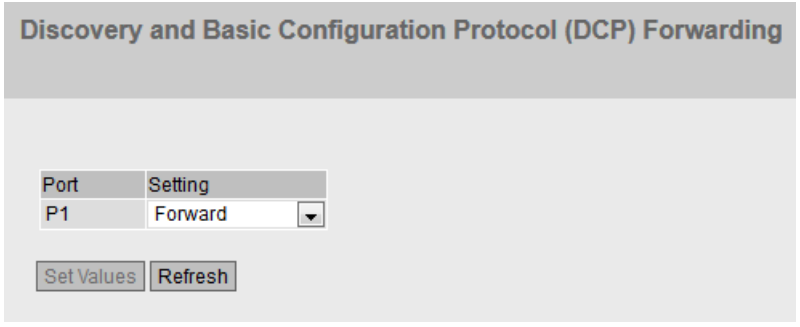
STEP 7 和 PST 工具使用 DCP 协议组态和诊断。发货时，对所有端口都启用 DCP；换句话说，在所有端口都转发 DCP 帧。利用此选项，可以针对每个端口禁止发送这些帧，例如，防止使用 PST 工具组态网络的各个部分，或者将整个网络分成多个较小部分，以进行组态和诊断。

设备的所有端口都在此 WBM 页面上显示。

说明

空表

如果设备上启用了 NAT，则该表为空或者将被清空。



说明

该表包括以下列：

- **端口 (Port)**

  显示可用以太网端口。

- **设置 (Setting)**

  指定端口是应阻止还是转发出站 DCP 帧。可做以下选择：

  – Block
    不通过此端口转发出站 DCP 帧。不过，仍可通过此端口接收帧。

  – Forward
    通过此端口转发 DCP 帧。

步骤

1. 指定端口是阻止还是转发 DCP 帧。
2. 单击"设置值"(Set Values) 按钮。

6.7.5 LLDP

识别网络拓扑

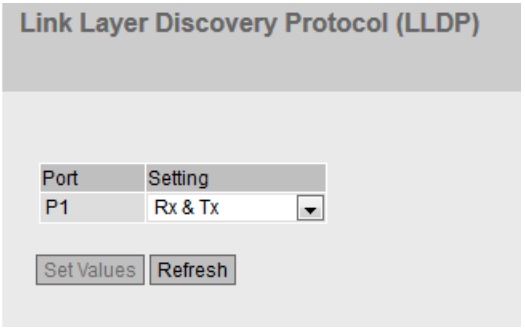
IEEE 802.AB 标准中定义了 LLDP（Link Layer Discovery Protocol，链路层发现协议）。

LLDP 是一种用来发现网络拓扑的方法。网络组件使用 LLDP 与其相邻设备交换信息。

支持 LLDP 的网络组件具有 LLDP 代理。LLDP 代理会定期发送与其自身有关的信息，并从所连接设备接收信息。接收到的信息存储在 MIB 中。

应用

PROFINET 使用 LLDP 进行拓扑诊断。在默认设置中，对所有端口都启用 LLDP；换句话说，所有端口都发送和接收 LLDP 帧。利用此功能，可以为每个端口选择启用或禁用发送和/或接收。



说明

该表格包括以下列：

- **Port**

  显示端口。

- **设置 (Setting)**

  指定 LLDP 功能。可使用以下选项：

  – Tx

    此端口只能发送 LLDP 帧。

  – Rx

    此端口只能接收 LLDP 帧。

  – Rx & Tx

    此端口可以接收和发送 LLDP 帧。

  – "-"（禁用）

    此端口既不接收也不发送 LLDP 帧。

步骤

1. 从下拉列表中选择所需的 LLDP 功能。
2. 单击"设置值"(Set Values) 按钮。

6.8 "Layer 3 (IPv4)"菜单

6.8.1 NAT

6.8.1.1 Basic

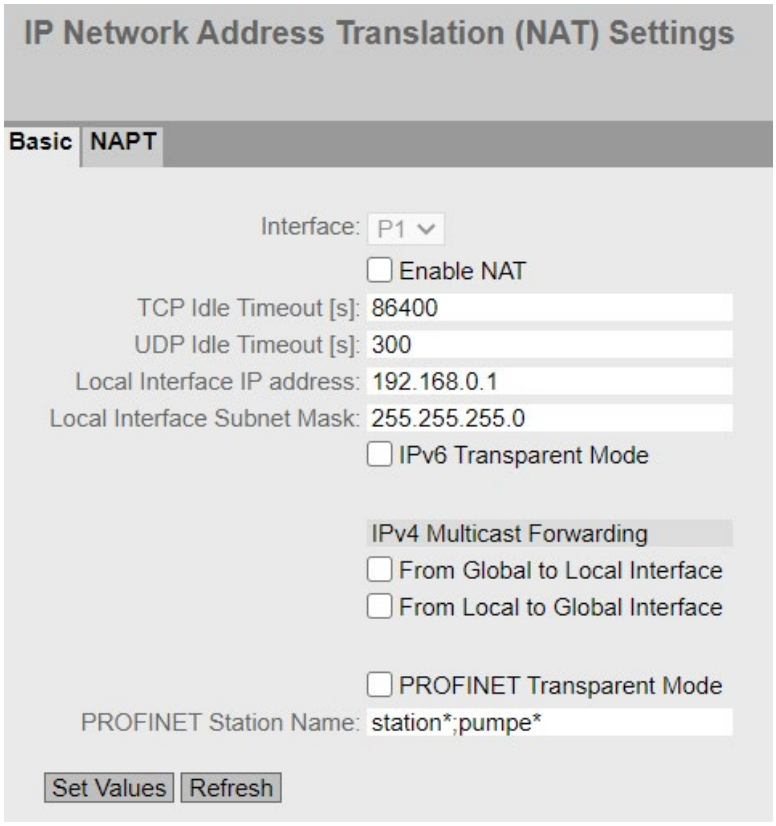
说明

只有客户端或处于客户端模式下的接入点才可使用此 WBM 页面。

在此页面中可指定 NAT 的基本设置。

说明

可通过以下地址找到 NAT 和 NAPT 的应用示例：
https://support.industry.siemens.com/cs/ww/en/view/37593580



描述

该页面包含以下框：

- **接口 (Interface)**

  从此下拉列表中选择所需的以太网接口。

- **启用 NAT (Enable NAT)**

  为以太网接口启用或禁用 NAT。

- **TCP 空闲超时 [s]** (TCP Idle Timeout [s])

  输入所需时间（以秒为单位）。如果未发生任何数据交换，则 TCP 连接将会在该时间结束后从转换表中删除。

  值范围为 1 到 2147483。

  默认设置：86400 秒

- **UDP 空闲超时 [s] (UDP Idle Timeout [s])**

  输入所需时间（以秒为单位）。如果未发生任何数据交换，则 UDP 连接将会在该时间结束后从转换表中删除。
  值范围为 1 到 2147483。
  默认设置：300 秒

- **本地接口 IP 地址 (Local Interface IP address)**

  输入以太网接口的本地 IP 地址。此 IP 地址是本地设备的网关地址。

- **本地接口子网掩码 (Local Interface Subnet Mask)**

  输入本地以太网的子网掩码。

- **IPv6 透明模式** (IPv6 Transparent Mode)

  启用时，IPv6 帧在以太网和 WLAN 之间转发时保持不变。

  这需要 MAC 模式未设置为"自身"(Own) 且已关闭 IPv6。

  如果已将 MAC 模式设置为"手动"(Manual)，则需要输入接收或发送 IPv6 帧的 IPv6 设备的 MAC 地址。

- **IPv4 组播转发 (IPv4 Multicast Forwarding)**

  指定是否转发传入的组播帧。

  – 从全局到本地接口 (From Global to Local Interface)

    WLAN 接口上传入的组播帧通过以太网接口转发到内部网络。

  – 从本地到全局接口 (From Local to Global Interface)

    本地以太网接口上传入的组播帧通过 WLAN 接口转发到外部网络。

- **PROFINET 透明模式 (PROFINET Transparent Mode)**

  仅在插入 KEY-PLUG iFeatures 后才可用。

  使用 NAT 时，无法通过 WLAN 与连接的 PROFINET 设备进行通信，因为这些设备对外部不可见。

  如果选择此设置，则可将各 PROFINET 设备重新设为可见。并且会以透明方式转发帧。使用 PROFINET 设备名称的情况例外。

  对于 PROFINET 透明模式，必须在 MAC 模式下设置"第 2 层隧道"(Layer 2 tunnel)。

说明

PROFINET 设备

如果激活了 PROFINET 透明模式，则连接的 PROFINET 设备无法从 DHCP 服务器获取 IP 地址。为这些设备使用固定的 IP 地址。

- **PROFINET 设备名称 (PROFINET device name)**

  PROFINET 设备名称确定允许与外部设备进行通信的 PROFINET 设备（无论 NAT 如何）。

  最大长度：240 个字符。框不得为空。

  允许使用下列字符：[a ... z]、[0 ... 9] 和 [. ; - *]。不允许使用大写字母。

  对于设备名称，可以使用通配符星号 (*) 替换任意数量的字符。星号可在任何位置，但每个设备名称中只能出现一次。

  可指定多个设备名称，并用分号隔开。

  示例：

  – *（星号）

    可以与所有连接的 PROFINET 设备进行通信。

  – pump1

    只能与此 PROFINET 设备进行通信。

  – pump*

    表示以"pump"开头的设备名称，例如 pump1，pump2。

    例如，一个工厂中有两个泵站。站 1 包含"pump1"，站 2 包含"pump2"。如果使用此输入，则可以在两个 WLAN 客户端上导入组态。

  – pump*;controller*

    表示以"pump"或"controller"开头的所有设备名称。

步骤

1. 在"本地接口 IP 地址"(Local Interface IP address) 输入框中，输入以太网接口的本地 IP 地址。
2. 在"本地接口子网掩码"(Local Interface Subnet Mask) 输入框中，输入本地以太网的子网掩码。

3. 为以太网接口启用 NAT。
4. 输入 PROFINET 设备名称。
5. 单击"设置值"(Set Values) 按钮。

6.8.1.2 NAPT

说明

只有客户端或处于客户端模式下的接入点才可使用此 WBM 页面。

在此 WBM 页面中，可为全局到本地网络的通信定义转换列表。每个 WLAN 客户端（NAT 网关）最多可支持 60 个条目。

说明

该页面包含以下框：

- **接口 (Interface)**

  与该设置相关的接口。仅在设备具有多个接口时才可选择。

- **通信类型 (Traffic Type)**

  指定地址分配对其有效的协议。必须分别设置 TCP 和 UDP 帧的参数。

- **全局端口 (Global Port)**

  输入全局端口。转发将此端口作为目标端口的到达帧。如果要将该设置用于某一端口范围，则以起始端口"-"结束端口的形式输入范围，例如 30 - 40。

  说明

  如果端口已被本地服务占用（如 Telnet），将显示一条警告。在这种情况下，应避免将 TCP 端口 23 (Telnet)、端口 22 (SSH) 和端口 80/443（http/https：使用 WBM 的客户端可访问性）和 UDP 端口 161 (SNMP) 用作全局端口。

- **本地 IP 地址 (Local IP Address)**

  输入本地网络中节点的 IP 地址。

- **本地端口 (Local Port)**

  输入端口的编号。此端口为将向其转发到达帧的新目标端口。如果要将该设置用于某一端口范围，则以起始端口"-"结束端口的形式输入范围，例如 30 - 40。

  如果本地端口与全局端口相同，则将在不进行端口转换的情况下转发帧。

该表包括以下列：

- **选择 (Select)**

  选中要删除的行中的复选框。

- **激活 (Activate)**

  选中所需行中的复选框。该条目用于地址分配

- **接口 (Interface)**

  显示与设置相关的接口。

- **动态全局 IP (Dynamic Global IP)**

  显示是否使用动态地址转换。

- **通信类型 (Traffic Type)**

  显示要为全局端口分配 UDP 帧还是 TCP 帧。

- **全局 IP 地址 (Global IP Address)**

  显示本地 IP 地址将要转换成的全局 IP 地址。

- **全局端口 (Global Port)**

  显示全局端口。

- **本地 IP 地址 (Local IP Address)**

  显示本地网络中节点的 IP 地址。

- **本地端口 (Local Port)**

  显示本地端口的编号。

步骤

1. 从"通信类型"(Traffic Type) 下拉列表中，选择地址分配对其有效的协议。
2. 在"全局端口"(Global Port) 中输入全局端口编号或端口范围。
3. 在"本地 IP 地址"(Local IP Address) 中输入本地网络中节点的 IP 地址。
4. 在"本地端口"(Local Port) 中输入本地端口编号或端口范围。
5. 单击"创建"(Create) 按钮。会在表中生成一个新条目。
6. 单击"设置值"(Set Values) 按钮。重启设备。

6.9 "Security"菜单

6.9.1 用户

6.9.1.1 本地用户

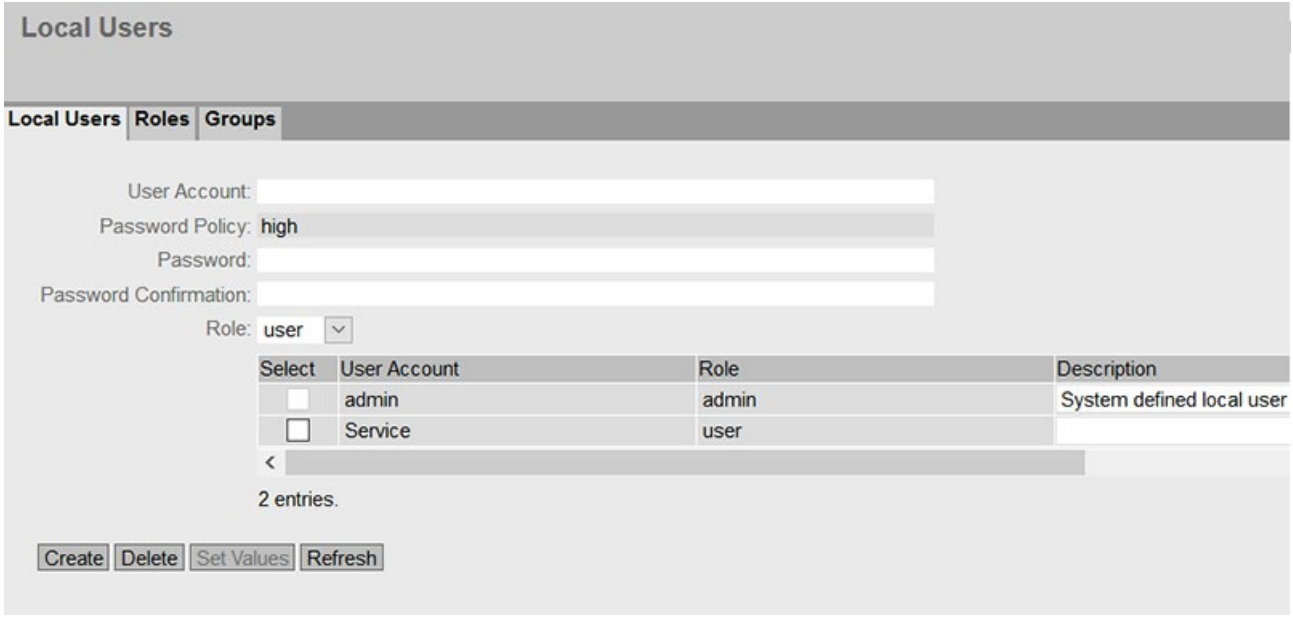
本地用户

在此页面上，创建具有相应权限的本地用户。

在创建或删除本地用户时，此更改也将自动在表"External User Accounts"中进行。如要通过更直接的方式在内部或外部用户表中进行更改，可使用 CLI 命令。

说明

显示的值取决于已登录用户的权限。



描述

该页面包含以下内容：

- **用户帐户 (User Account)**

  输入用户的名称。该名称必须满足以下条件：

  – 名称必须唯一。

  – 名称长度必须在 1 到 250 个字符之间。

  – 不能包含以下字符： |?";:

    Space 和 Delete 字符也不能包含在内。

说明

用户名无法更改

创建用户后，无法再修改用户名称。

如果需要更改用户名，则必须删除该用户并创建一个新用户。

说明

用户名：admin

可使用该用户名组态设备。

如果是首次登录或是在"恢复出厂默认设置并重启"(Restore Factory Defaults and Restart) 之后登录，则会提示您更改预定义密码"admin"。有一次重命名出厂预设用户"admin"的机会。之后，不可再重命名"admin"。

说明

出厂时设置的**默认用户"user"**

自固件版本 V6.0 起，出厂时设置的默认用户"user"在产品交付后不再可用。

如果将设备固件版本升级到 V6.0，出厂时设置的默认用户"user"起初仍然可用。如果将设备复位为出厂设置（"恢复出厂默认设置并重启"(Restore Factory Defaults and Restart)），则出厂时设置的默认用户"user"将被删除。

可以使用"user"角色创建新用户。

- **密码策略 (Password Policy)**

  显示当前使用的密码策略。

  – 高

    密码长度：至少 8 个字符，最长 128 个字符

    至少 1 个大写字母

    至少 1 个特殊字符

    至少 1 个数字

  – 低

    密码长度：至少 6 个字符，最长 128 个字符

  在"安全 > 密码 > 选项"(Security > Passwords > Options) 页面组态密码策略。

- **密码 (Password)**

  输入密码。密码强度取决于密码的长度和复杂度。

- **密码确认 (Password Confirmation)**

  再次输入该密码以进行确认。

- **角色 (Role)**

  选择一个角色。

  您可在系统定义的角色和自定义的角色之间选择，请参见页面"Security > Users > Roles"。

该表包含以下列：

- **选择 (Select)**

  选中要删除的行中的复选框。

  说明
  预设用户以及已登录的用户无法删除或更改。

- **用户帐户 (User Account)**

  显示用户名。

- **角色 (Role)**

  显示用户角色。

- **描述 (Description)**

  显示用户帐户的说明。说明文本最长 100 个字节。

步骤

说明

"Trial"模式下的更改
即使设备处于"Trial"模式，在此页面上执行的更改也会立即保存。

创建用户

1. 输入用户的名称。
2. 输入用户的密码。
3. 再次输入该密码以进行确认。
4. 选择用户角色。
5. 单击"创建"(Create) 按钮。

6. 输入用户的说明。

7. 单击"设置值"(Set Values) 按钮。

删除用户

1. 选中要删除的行中的复选框。

2. 单击"删除"(Delete) 按钮。将删除条目并更新页面。

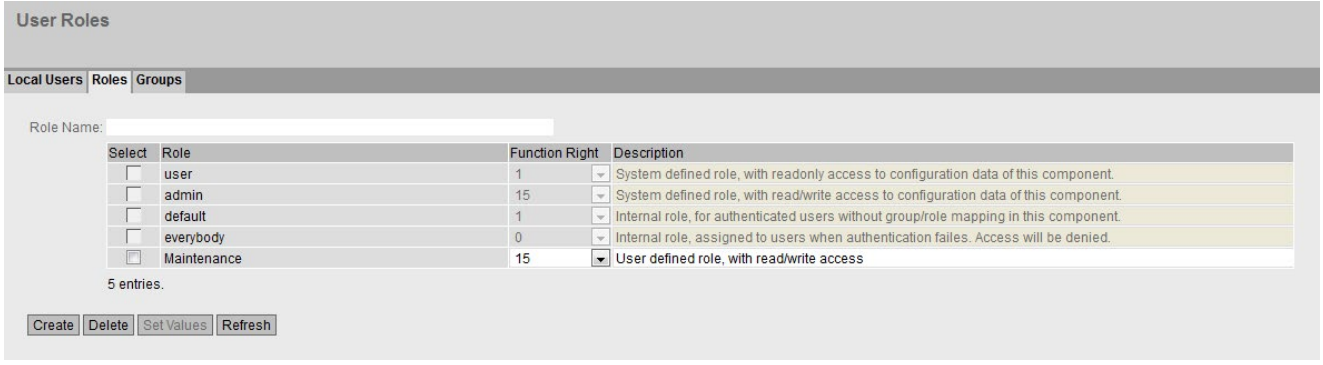
6.9.1.2 角色

角色

在此页面中，可创建在设备本地有效的角色。

说明

显示的值取决于已登录用户的权限。



说明

该页面包含以下内容：

- **Role Name**

  输入角色的名称。该名称必须满足以下条件：

  – 名称必须唯一。

  – 名称长度必须在 1 到 64 个字符之间。

  说明

  角色名不可更改
  在创建角色后，角色的名称便不可更改。
  如果角色的名称需要更改，则必须删除该角色并创建一个新角色。

该表包含以下列：

- **Select**

  选中要删除的行中的复选框。

  说明
  重新定义的的角色和已分配的角色无法删除或修改。

- **Role**

  显示角色的名称。

- **Function Right**

  选择角色的功能权限。

  – 1

    拥有此角色的用户可读取设备参数，但不可更改这些参数。拥有此角色的用户可以更改他们自己的密码。

  – 15

    拥有此角色的用户既可读取也可更改设备参数。

说明

功能权限无法更改

如果您已分配了一个角色，则您无法再更改该角色的功能权限。
如果要更改角色的功能权限，按照以下列出的步骤操作：

1. 删除所有已分配的用户。
2. 更改角色的功能权限：
3. 再次分配该角色。

- **Description**

  输入角色的说明。对于预定义的角色，将显示一个说明。说明文本最长 100 个字节。

步骤

Creating a role

1. 输入角色的名称。
2. 单击"创建"(Create) 按钮。
3. 选择角色的功能权限。
4. 输入角色的说明。
5. 单击"设置值"(Set Values) 按钮。

Deleting a role

1. 选中要删除的行中的复选框。
2. 单击"删除"(Delete) 按钮。将删除条目并更新页面。

6.9.1.3 组

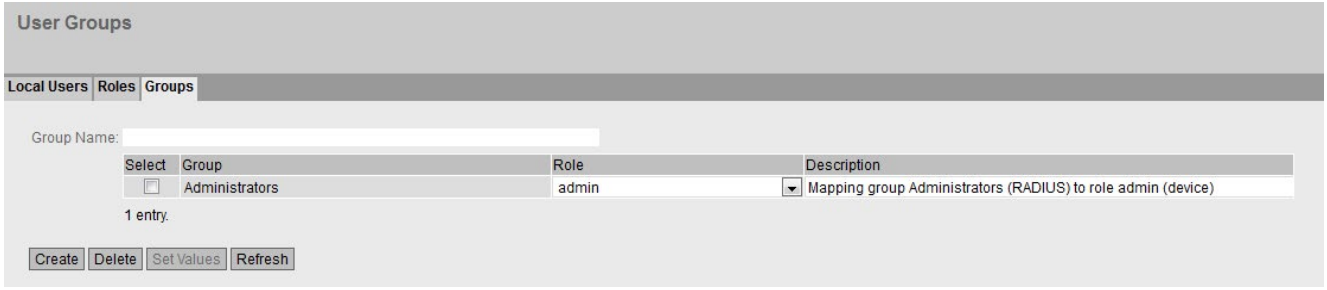
用户组

在此页面中，可将一个组链接到一个角色。

在此示例中，组"Administrators"被链接到"admin"角色：组在 RADIUS 服务器上进行定义。角色在设备上进行本地定义。当 RADIUS 服务器为用户授权，并将用户分配到"Administrators"组时，此用户便拥有"admin"角色。

说明

显示的值取决于已登录用户的权限。



说明

该页面包含以下内容：

- **Group Name**

  输入组的名称。此名称必须与 RADIUS 服务器上的组相匹配。

  该名称必须满足以下条件：

  – 名称必须唯一。

  – 名称长度必须在 1 到 64 个字符之间。

  – 不允许使用以下字符：§ ? " ; :

该表包含以下列：

- **选择 (Select)**

  选中要删除的行中的复选框。

- **Group**

  显示组的名称。

- **Role**

  选择一个角色。通过 RADIUS 服务器上所链接的组进行身份验证的用户会在设备本地获得此角色的权限。

  您可在系统定义的角色和自定义的角色之间选择，请参见页面"Security > Users > Roles"。

- **Description**

  为组与角色的链接输入说明。说明文本最长 100 个字节。

步骤

将组链接到一个角色。

1. 输入组的名称。
2. 单击"Create"按钮。

3. 选择一个角色。

4. 为组与角色的链接输入说明。

5. 单击"Set Values"按钮。

删除组合角色之间的链接

1. 选中要删除的行中的复选框。

2. 单击"Delete"按钮。将删除条目并更新页面。

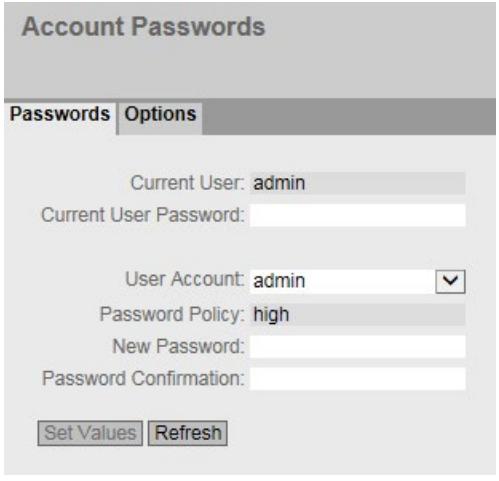
6.9.2 密码

用户密码的组态

说明

如果通过 RADIUS 服务器登录，则无法更改任何密码。

在此页面上，可以更改用户密码。如果以有权更改设备参数的帐户登录，则可更改所有用户帐户的密码。如果以用户身份登录，则只能更改您自己的密码。



描述

- **当前用户 (Current User)**

  显示当前已登录的用户。

- **当前用户密码 (Current User Password)**

  输入当前已登录的用户的密码。

- **用户帐户 (User Account)**

  选择要更改其密码的用户。

- **密码策略 (Password Policy)**

  显示分配新密码时正在使用的密码策略。

  – 高 (High)

    密码长度：至少 8 个字符，最长 128 个字符

    至少 1 个大写字母

    至少 1 个特殊字符

    至少 1 个数字

  – 低 (Low)

    密码长度：至少 6 个字符，最长 128 个字符

- **新密码 (New Password)**

  为所选用户输入新密码。

  不能包含以下字符：

  – § ? " ; :

  – 也不能包含 Space 和 Delete 字符。

- **密码确认 (Password Confirmation)**

  再次输入新密码以进行确认。

步骤

1. 在"当前用户密码"(Current User Password 输入框中输入当前已登录的用户的有效密码。
2. 从"用户帐户"(User Account) 下拉列表中，选择要更改其密码的用户。
3. 在"New Password"输入框中为所选用户输入新密码。
4. 在"Password Confirmation"输入框中重复输入新密码。
5. 单击"设置值"(Set Values) 按钮。

说明

设备出厂时的密码设置如下：

- "管理员"(admin)：admin

如果是以预设用户"admin"的身份首次登录，或是在"恢复出厂默认设置并重启"之后登录，系统会提示您更改密码。

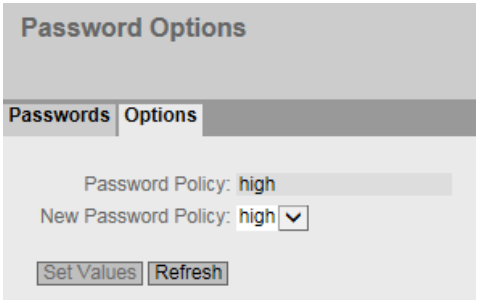
说明

在试用模式下更改密码

即使在试用模式下更改密码，此更改也会立即保存。

6.9.2.1 选项

在此页面指定分配新密码时将使用的密码策略。



说明

- **密码策略 (Password Policy)**

  显示当前正在使用的密码策略。

- **新密码策略 (New Password Policy)**

  从该下拉列表中选择所需的设置。

  – 高

    密码长度：至少 8 个字符，最长 128 个字符

    至少 1 个大写字母

    至少 1 个特殊字符

    至少 1 个数字

  – 低

    密码长度：至少 6 个字符，最长 128 个字符

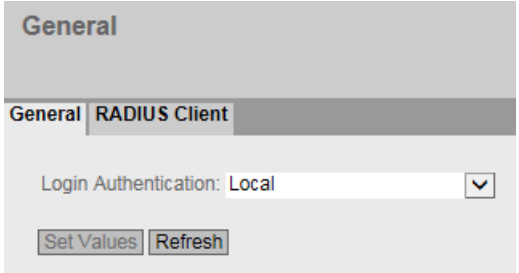
6.9.3 AAA

6.9.3.1 常规

网络节点登录

标志"AAA"代表"验证、授权、审计"(Authentication, Authorization, Accounting)。该功能用于标识和允许网络节点，为它们提供适当的可用服务并确定使用的范围。

在此页面中组态登录信息。



说明

该页面包含以下框：

说明

要使用登录验证模式"RADIUS"、"本地和 RADIUS"(Local and RADIUS) 或"RADIUS 和本地回退"(RADIUS and fallback Local)，必须存储和组态 RADIUS 服务器，以供用户验证。

- **登录验证 (Login Authentication)**

  指定登录方式：

  – Local

    必须在设备上进行本地验证。

  – RADIUS

    必须通过 RADIUS 服务器处理验证。

  – Local and RADIUS

    使用设备上的用户（用户名和密码）以及通过 RADIUS 服务器都可以进行验证。

    首先在本地数据库中搜索用户。如果用户不存在，则将发送 ADIUS 请求。

  – RADIUS and fallback Local

    必须通过 RADIUS 服务器处理验证。

    只有无法在网络中访问 RADIUS 服务器时，才会执行本地验证。

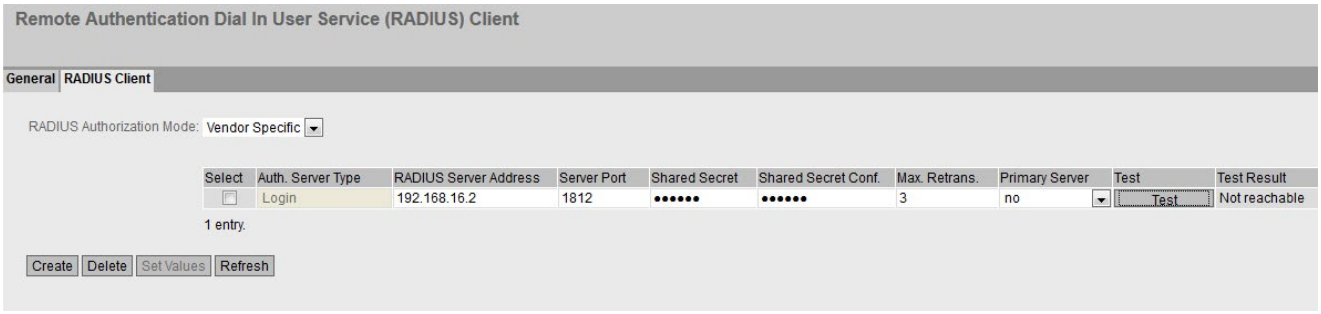
6.9.3.2 RADIUS 客户端

通过外部服务器进行验证

RADIUS 的概念基于外部验证服务器。

表中的每一行包含一台服务器的访问数据。按照搜索顺序，将首先查询主服务器。如果无法访问主服务器，则会以服务器的输入顺序查询其它辅助服务器。

如果没有服务器响应，则表示没有验证。



显示框说明

该页面包含以下框：

- **RADIUS Authorization Mode**

  对于登录验证，RADIUS 验证模式会指定如何为已成功通过身份验证的用户分配权限。

  – Conventional

    在此模式下，如果服务器为属性"Service Type"返回值"Administrative User"，用户将以管理员权限登录。在所有其它情况下，用户将按照读取权限登录。

  – SiemensVSA

    在此模式下，权限的分配取决于服务器是否为用户返回一个组和返回的具体哪个组，以及在"External User Accounts"表中该用户是否存在对应条目。

该表格包括以下列：

- **Select**

  选择要删除的行。

- **RADIUS Server Address**

  输入 RADIUS 服务器的 IPv4 地址或 FQDN。

- **服务器端口** (Server Port)

  在此处输入 RADIUS 服务器的输入端口。默认情况下，输入端口设置为 1812。值范围是 1 到 65535。

- **共享密钥 (Shared Secret)**
  在此处输入访问 ID。值范围是 1...128 个字符。
- **Shared Secret Conf.**
  再次输入访问 ID 以进行确认。
- **最大重传次数 (Max. Retrans.)**
  在此，输入尝试请求的最大重试次数。
  初始连接请求将重试此处指定的次数，然后才会查询另一个已组态的 RADIUS 服务器或将登录视为失败。由于默认设置为 3 次重试，这意味着会尝试进行 4 次连接。值范围是 1 到 5。
- **主服务器** (Primary Server)
  使用该下拉列表中的选项，指定此服务器是否是主服务器。可以从"是"(yes) 或"否"(no) 选项中选择一个。
- **测试 (Test)**
  可以使用此按钮测试指定的 RADIUS 服务器是否可用。该测试执行一次，并非循环执行。
- **测试结果 (Test Result)**
  显示 RADIUS 服务器是否可用：
  – 不可访问 (Not reachable)
    无法访问 IP 地址。
    可以访问 IP 地址，但 RADIUS 服务器尚未运行。
  – 可访问，但不接受密钥 (Reachable, key not accepted)
    可以访问 IP 地址，但 RADIUS 服务器不接受共享密钥。
  – 可访问，且接受密钥 (Reachable, key accepted)
    可以访问 IP 地址，且 RADIUS 服务器接受指定的共享密钥。

组态步骤

输入新服务器

1. 单击"创建"(Create) 按钮。会在表中生成一个新条目。
   在表中将输入以下默认值：
   - RADIUS 服务器地址：0.0.0.0
   - 服务器端口：1812
   - 最大重传次数：3
   - 主服务器：否 (No)
2. 在相关行中，在输入框中输入以下数据：
   - RADIUS 服务器地址
   - 服务器端口
   - Shared Secret
   - 共享密钥确认 (Shared Secret Conf)
   - 最大重传次数：3
   - Primary server：No
3. 如果必要，检查 RADIUS 服务器的可访问性。
4. 单击"设置值"(Set Values) 按钮。

对每个要输入的服务器重复此步骤。

修改服务器

1. 在相关行中，在输入框中输入以下数据：
   - RADIUS 服务器地址
   - 服务器端口
   - Shared Secret
   - 共享密钥确认 (Shared Secret Conf)
   - 最大重传次数 (Max. Retrans.)
   - 主服务器 (Primary Server)
2. 如果必要，检查 RADIUS 服务器的可访问性。
3. 单击"设置值"(Set Values) 按钮。

对每个要修改其输入内容的服务器重复此步骤

删除服务器

1. 单击第一列中要删除的行前的复选框，以选择要删除的条目。
   对所有要删除的条目重复此操作。
2. 单击"删除"(Delete) 按钮。将从设备内存中删除此数据并更新该页面。

6.9.4 WLAN

6.9.4.1 Basic（接入点）

安全等级

为确保网络安全，请使用验证和加密。在此页面中可指定安全设置。

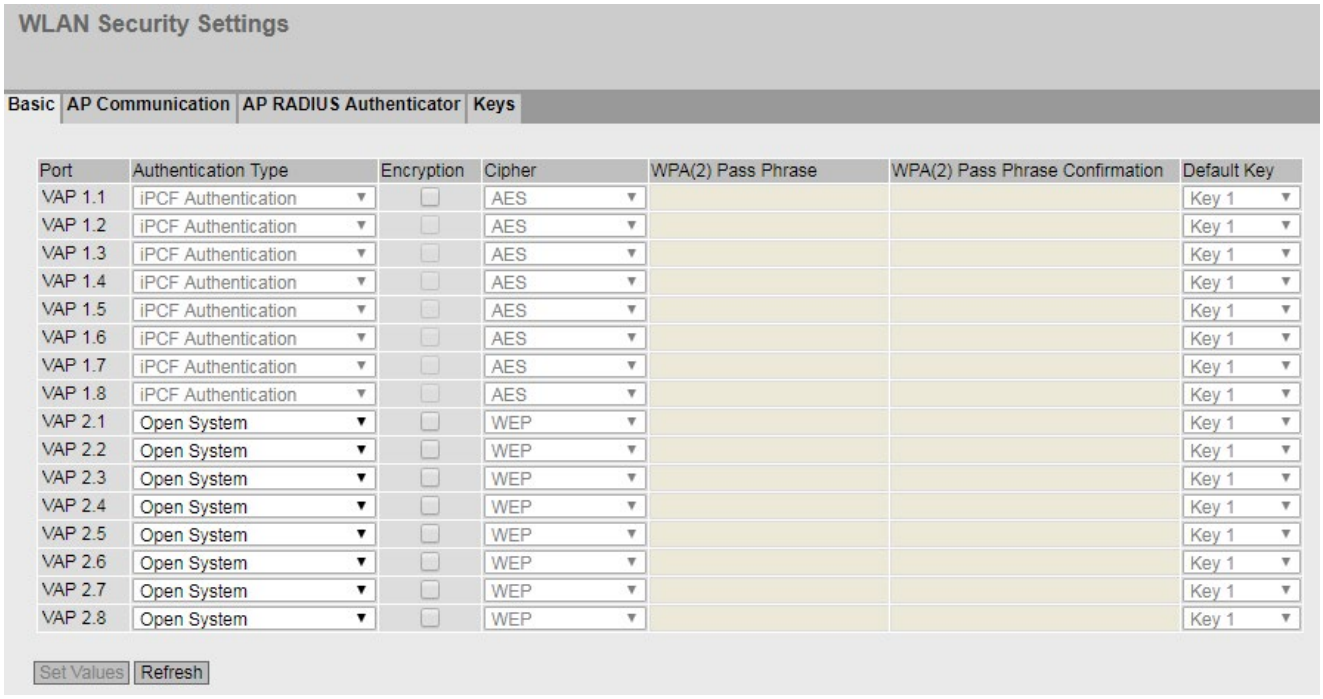
说明

WLAN 模式 IEEE 802.11 n

以 WLAN 模式 IEEE8002.11n 运行的设备只可以使用 WPA2（WPA2-PSK 和 WPA2 Radius）加密。

iPCF、iPCF-HT 或 iPCF-MC 模式已激活

如果已启用 iPCF、iPCF-HT 或 iPCF-MC 模式，则安全上下文 1 仅支持采用或不采用 AES 加密的"iPCF 验证"。



描述

该表格包括以下列：

- **端口 (Port)**

  显示可用端口。

- **验证类型 (Authentication Type)**

  选择验证类型。该选择取决于工作模式和传输标准。

  – Open System

  没有验证。可选择使用固定（不变）的 WEP 密钥加密。要使用密钥，请启用"加密"(Encryption)。在"密钥"(Keys) 页面上定义 WEP 密钥。

  – Shared Key

  在"共享密钥"(Shared Key) 验证中，客户端和接入点上存储了固定的密钥。随后该 WEP 密钥将用于验证和加密。在"密钥"(Keys) 页面上定义 WEP 密钥。

  说明

  如果对"开放式系统"(Open System) 使用"加密"(Encryption) 或"共享密钥"(Shared Key)，则必须始终在"密钥"(Keys) 页面上设置密钥 1。

  – WPA (RADIUS)

  Wi-Fi 保护接入 (WPA) 是 Wi-Fi 联盟指定的一种填补 WEP 安全漏洞的方法。规定必须使用服务器进行验证 (802.1x)。每个数据帧的动态密钥交换会进一步加强安全性。

  – WPA-PSK

  WPA 预共享密钥 (WPA-PSK) 是 WPA 的弱化形式。在此方法中，验证不是由服务器设立的，但它基于密码。在客户端或服务器上手动组态密码。

  – WPA2 (RADIUS)

  WPA2（Wi-Fi 保护接入 2）是 WPA 的进一步发展，实现了 IEEE 802.11i 安全标准的功能。但 WPA 验证无需 RADIUS 服务器。

  – WPA2-PSK

  WPA2-PSK 基于 802.11i 标准。但是，WPA 验证无需 RADIUS 服务器。与此不同

的是，WPA(2) 密钥 (WPA(2) Pass phrase) 存储在各客户端和接入点上。WPA(2) Pass phrase 用于验证和进一步加密。

– WPA/WPA2-Auto-PSK
使用此设置，接入点可处理"WPA-PSK"和"WPA2-PSK"两种验证类型。当接入点与不同客户端进行通信，且其中一些客户端使用"WPA-PSK"而其他客户端使用"WPA2-PSK"时，此功能十分必要。在客户端上设置同一加密方法。

– WPA/WPA2-Auto
使用此设置，接入点可处理"WPA"和"WPA2"两种验证类型。当接入点与不同客户端进行通信，且其中一些客户端使用"WPA"而其他客户端使用"WPA2"时，此功能十分必要。在客户端上设置同一加密方法

– **iPCF authentication**
采用可选 AES 加密进行验证。如果在 WLAN 接口上启用了 iPCF、iPCF-HT 或 iPCF-MC 模式，则会自动设置验证。如果要采用 AES 加密方法，则仅支持长度为 128 位的密钥。

- **加密 (Encryption)**

加密可保护传输的数据免遭窃取和破坏。只有选择了"开放式系统"(Open System) 作为验证类型时，才能禁用加密功能。所有其他安全方法都包括验证和加密。

- **密码 (Cipher)**

  选择加密方法。该选择取决于传输标准。

  – AUTO

    根据其他站的功能自动选择使用 AES 或 TKIP。

  – WEP

    WEP（有线等效加密）

    一种基于 RC4 算法 (Ron's Code 4) 的对称流加密方法，密钥长度仅为 40 位或 104 位。

  – TKIP (Temporal Key Integrity Protocol)

    一种使用 RC4 算法 (Ron's Code 4) 的对称加密方法。与较弱的 WEP 加密相反，TKIP 采用从主密钥派生的变化密钥。TKIP 还可以识别受损的数据帧。

  – AES (Advanced Encryption Standard)

    一种基于进一步改进 TKIP 功能的 Rijndael 算法的较强对称区块加密方法。

  说明

  为更好地保护数据以防止攻击，请使用采用 AES 的 WPA2/WPA2-PSK。

- **WPA(2) 通行口令 (WPA(2) Pass Phrase)**

  在此处输入 WPA(2) 密钥。该 WPA(2) 密钥必须为客户端和接入点所知，并由用户在两端输入。

  对于包含 8 到 63 个字符的密钥，只能使用以下可读的 ASCII 字符:0x20 - 0x7e。

  对于恰好包含 64 个字符的密钥，可以使用以下 ASCII 字符：0 - 9、 a - f 和 A - F。

- **WPA(2) 通行口令确认 (WPA(2) Pass Phrase Confirmation)**

  确认输入的 WPA(2) 通行口令。

- **默认密钥 (Default Key)**

  指定用于加密数据的 WEP 密钥。在"密钥"(Keys) 页面上定义 WEP 密钥。

步骤

1. 选择必需的安全设置。可用的设置取决于已选择的"验证类型"(Authentication Type)。

验证类型	加密	密码	加密密钥源
开放式系统	禁用	--	--
开放式系统	启用	WEP	默认密钥
共享密钥	启用	WEP	默认密钥
WPA (RADIUS)	启用	自动/TKIP/AES	RADIUS 服务器
WPA-PSK	启用	自动/TKIP/AES	WPA(2) 通行口令
WPA2 (RADIUS)	启用	自动/TKIP/AES	RADIUS 服务器
WPA2-PSK	启用	自动/TKIP/AES	WPA(2) 通行口令
WPA/WPA2-AutoPSK	启用	自动/TKIP/AES	WPA(2) 通行口令
WPA/WPA2-Auto (RADIUS)	启用	自动/TKIP/AES	RADIUS 服务器
iPCF 验证 [1)]	启用	AES	默认密钥（128 位）

[1)] 仅当选择 iPCF 和 iPCF-HT 或 iPCF-MC 时：预设采用可选加密的验证

2. 单击"设置值"(Set Values) 按钮。

6.9.4.2 Basic（客户端）

安全等级

为确保网络安全，请使用验证和加密。在此页面中可指定安全设置。

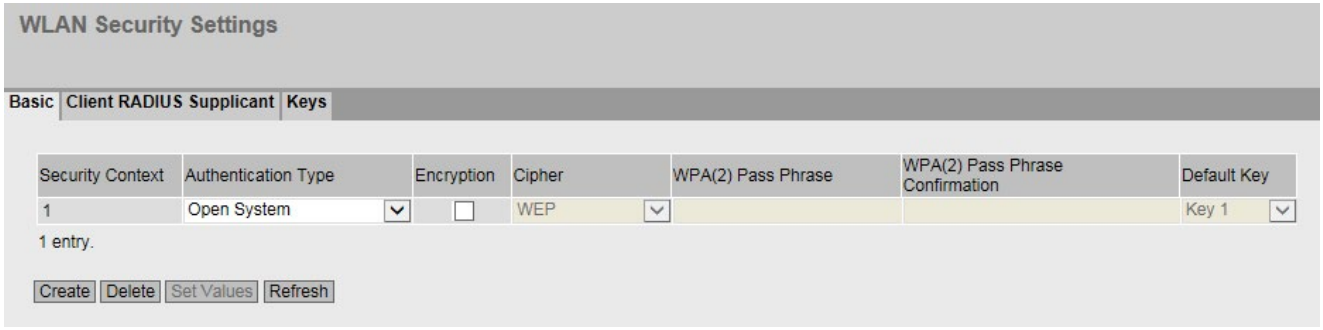
说明

WLAN 模式 IEEE 802.11 n

以 WLAN 模式 IEEE8002.11n 运行的设备只可以使用 WPA2（WPA2-PSK 和 WPA2 Radius）加密。

iPCF、iPCF-HT 或 iPCF-MC 模式已激活

如果已启用 iPCF、iPCF-HT 或 iPCF-MC 模式，则安全上下文 1 仅支持采用或不采用 AES 加密的"iPCF 验证"。



描述

该表格包括以下列：

- **选择 (Select)**

  选择要删除的行。选择此列中的复选框，单击"删除"(Delete) 按钮即可删除列表中的条目。

- **安全上下文 (Security Context)**

  显示条目编号。如果创建新的条目，会创建一个带有唯一编号的新行。

  最多可以创建 8 个安全上下文。无法删除安全上下文 1。

- **验证类型 (Authentication Type)**

  选择验证类型。该选择取决于工作模式和传输标准。

  – **Open System**

    没有验证。可选择使用固定（不变）的 WEP 密钥加密。要使用密钥，请启用"加密"(Encryption)。在"密钥"(Keys) 页面上定义 WEP 密钥。

  – **Shared Key**

    在"共享密钥"(Shared Key) 验证中，客户端和接入点上存储了固定的密钥。随后该 WEP 密钥将用于验证和加密。在"密钥"(Keys) 页面上定义 WEP 密钥。

  – **WPA (RADIUS)**

    Wi-Fi 保护接入是 Wi-Fi 联盟指定的一种填补 WEP 安全漏洞的方法。规定必须使用服务器进行验证 (802.1x)。每个数据帧的动态密钥交换会进一步加强安全性。

    说明

    最初在"安全 > WLAN > 客户端 Radius 请求者"(Security > WLAN > Client Radius Supplicant) 页面上进行相关的 RADIUS 设置。

  – **WPA-PSK**

    WPA 预共享密钥 (WPA-PSK) 是 WPA 的弱化形式。在此方法中，验证不是由服务器设立的，但它基于密码。在客户端或服务器上手动组态密码。

  – **WPA2 (RADIUS)**

    WPA2（Wi-Fi 保护接入 2）是 WPA 的进一步发展，实现了 IEEE 802.11i 安全标准的功能。但 WPA 验证无需 RADIUS 服务器。

    说明

    最初在"安全 > WLAN > 客户端 Radius 请求者"(Security > WLAN > Client Radius Supplicant) 页面上进行相关的 RADIUS 设置。

  – **WPA2-PSK**

    WPA2-PSK 基于 802.11i 标准。但是，WPA 验证无需 RADIUS 服务器。与此不同

的是，WPA(2) 密钥（WPA(2) 通行口令）存储在各客户端和接入点上。WPA(2) 通行口令用于验证和进一步加密。

– **WPA/WPA2-Auto-PSK**
使用此设置，接入点可处理"WPA-PSK"和"WPA2-PSK"两种验证。当接入点与一些使用"WPA-PSK"而另一些使用"WPA2-PSK"的不同客户端进行通信时，此功能十分必要。在客户端上设置同一加密方法。

– **WPA/WPA2-Auto**
使用此设置，接入点可处理"WPA"和"WPA2"两种验证。当接入点与一些使用"WPA"而另一些使用"WPA2"的不同客户端进行通信时，此功能十分必要。在客户端上设置同一加密方法。

– **iPCF authentication**
采用可选 AES 加密进行验证。如果在 WLAN 接口上启用了 iPCF、iPCF-HT 或 iPCF-MC 模式，则会自动设置验证。如果要采用 AES 加密方法，则仅支持长度为 128 位的密钥。

- **加密 (Encryption)**

加密可保护传输的数据免遭窃取和破坏。只有选择了"开放式系统"(Open System) 作为验证类型时，才能禁用加密功能。所有其他安全方法都包括验证和加密。

- **密码 (Cipher)**

  选择加密方法。该选择取决于传输标准。

  – **AUTO**

    根据其他站的功能自动选择 AES 或 TKIP。

  – **WEP**

    WEP（有线等效加密）

    一种基于 RC4 算法 (Ron's Code 4) 的对称流加密方法，密钥长度仅为 40 位或 104 位。

  – **TKIP (Temporal Key Integrity Protocol)**

    一种使用 RC4 算法 (Ron's Code 4) 的对称加密方法。与较弱的 WEP 加密相反，TKIP 采用从主密钥派生的变化密钥。TKIP 还可以识别受损的数据帧。

  – **AES (Advanced Encryption Standard)**

    一种基于进一步改进 TKIP 功能的 Rijndael 算法的较强对称区块加密方法。

    说明

    为更好地保护数据以防止攻击，请使用采用 AES 的 WPA2/WPA2-PSK。

- **WPA(2) 通行口令 (WPA(2) Pass Phrase)**

  在此处输入 WPA(2) 密钥。该 WPA(2) 密钥必须为客户端和接入点所知，并由用户在两端输入。

  对于包含 8 到 63 个字符的密钥，只能使用以下可读的 ASCII 字符:0x20 - 0x7e。

  对于恰好包含 64 个字符的密钥，可以使用以下 ASCII 字符：0 - 9、 a - f 和 A - F。

- **WPA(2) 通行口令确认 (WPA(2) Pass Phrase Confirmation)**

  确认输入的 WPA(2) 通行口令。

- **默认密钥 (Default Key)**

  指定用于加密数据的 WEP 密钥。在"密钥"(Keys) 页面上定义 WEP 密钥。

步骤

1. 要创建新的安全上下文，请单击"创建"(Create) 按钮。
2. 选择必需的安全设置。可用的设置取决于已选择的"验证类型"(Authentication Type)。
   如果启用了 iPCF、iPCF-HT 或 iPCF-MC 模式，则无法选择"验证类型"(Authentication Type)。
3. 单击"设置值"(Set Values) 按钮。

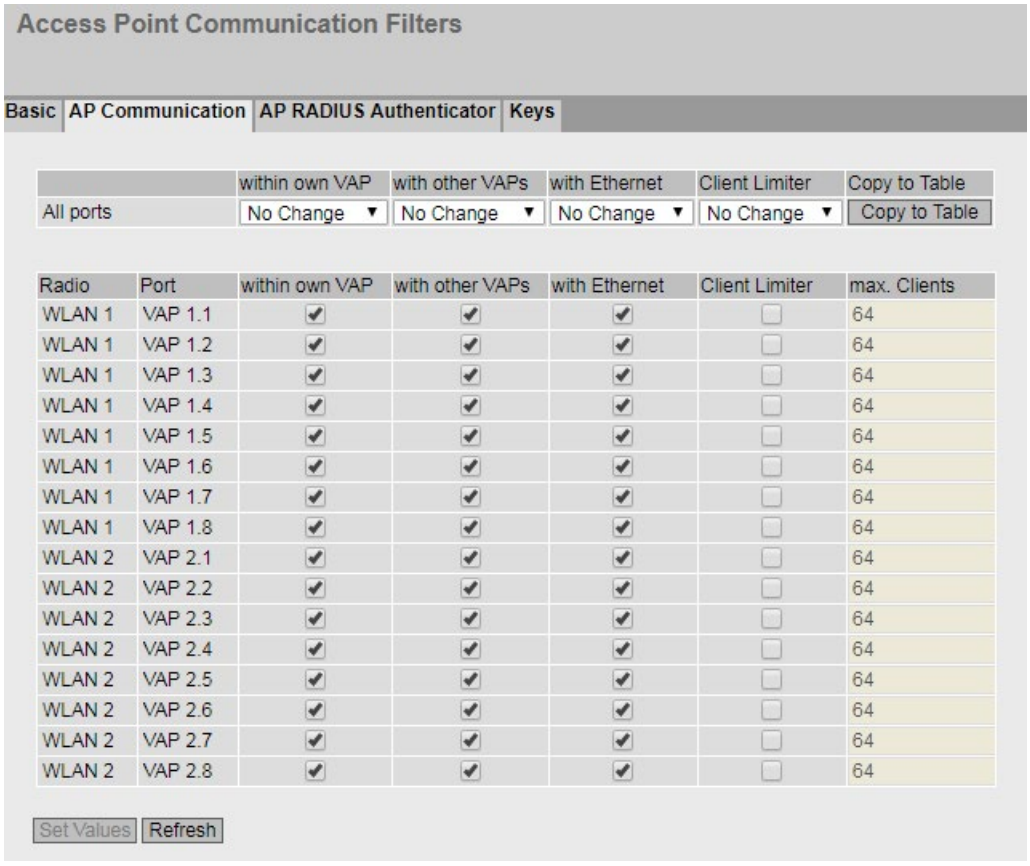
6.9.4.3 接入点通信

通信选项

在此 WBM 页中指定接入点所允许的通信类型。

说明

该 WBM 页面仅在接入点模式下可用。



说明

表 1 包含以下列：

- **列 1 (Column 1)**

  说明设置对于表 2 的所有端口都有效。

- **在自身 VAP 内 (within own VAP)/通过其它 VAP (with other VAPs)/通过以太网 (with Ethernet)/客户端限制器 (Client Limiter)**

  在此下拉列表中，选择适用于所有端口的设置。如果选择"不变"(No Change)，则表 2 中的条目保持不变。

- **复制到表 (Copy to Table)**

  如果单击此按钮，则为表 2 的所有端口应用此设置。

表 2 包含以下列：

- **无线 (Radio)**

  显示可用的 WLAN 接口。

- **端口 (Port)**

  显示 VAP 接口。

- **在自身 VAP 内 (within own VAP)**

  – 启用

    登录某接入点的同一 VAP 接口的客户端可彼此通信。

  – 禁用

    禁用此选项。

- **通过其它 VAP (with other VAPs)**

  – 启用

    登录某接入点的不同 VAP 接口的客户端可彼此通信。

    说明

    对于接入点，需要在所有 WLAN 接口或所有 VAP 接口上都启用"通过其它 VAP"(with other VAPs)，才允许在该接入点的不同 VAP 接口上登录的客户端之间进行通信。

– 禁用

禁用此选项。

说明

禁用"在自身 VAP 内"(within own VAP) 或"通过其它 VAP"(with other VAPs) 功能

如果禁用了"在自身 VAP 内"(within own VAP) 或"通过其它 VAP"(with other VAPs) 功能，则各个 WLAN 客户端将无法再看到彼此。这意味着，地址冲突检测 (ACD) 功能也无法再可靠运行。

- **通过以太网 (with Ethernet)**

  – 启用

  客户端可通过接入点的以太网接口通信。

  – 禁用

  禁用此选项。

- **客户端限制器 (Client limiter)**

  – 启用

  可同时登录的 WLAN 客户端数量有限。

  – 禁用

  禁用此选项。

- **最大客户端数 (Max. clients)**

  设置可同时连接到此接口的的最大客户端数。如果超过该数量，则拒绝其它客户端。

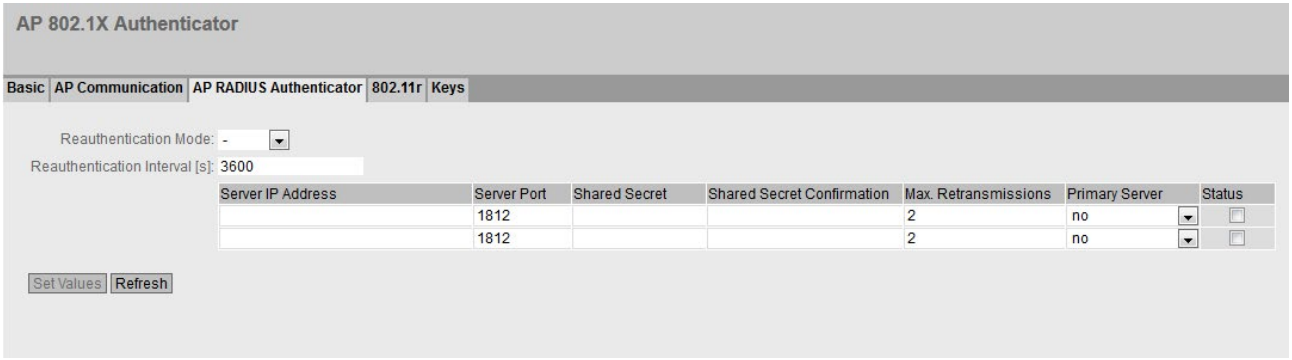
6.9.4.4 AP RADIUS 验证器

RADIUS 服务器的组态

在此 WBM 页面中可定义接入点的 RADIUS 服务器和 RADIUS 验证方式。可输入两台 RADIUS 服务器的数据。

说明

该 WBM 页面仅在接入点模式下可用。



说明

该页面包含以下框：

- **重新验证模式 (Reauthentication Mode)**

  指定设置强制客户端进行重新验证前所需时间的对象。

  – -（禁用）
    禁用重新验证模式。

  – 服务器 (Server)
    在服务器上启用时间管理。

  – 本地 (Local)
    启用本地时间管理。在"重新验证间隔"(Reauthentication Interval) 中，指定有效期。

- **重新验证间隔 [s] (Reauthentication Interval [s])**

  如果采用本地时间管理，则以秒为单位输入验证有效期。最短时间是 1 分钟（输入 60），最长时间是 12 小时（输入 43200）。默认值为 1 小时（3,600 秒）。

该表包括以下列：

- **服务器 IP 地址 (Server IP Address)**

  在此输入 RADIUS 服务器的 IP 地址或 FQDN 名称。

- **服务器端口 (Server Port)**

  在此处输入 RADIUS 服务器的输入端口。

- **Shared Secret**

  输入 RADIUS 服务器的密码。
  对于密码，使用 ASCII 码 0x20 至 0x7e。

- **共享密钥确认 (Shared Secret Conf)**

  确认密码。

- **最大重传次数 (Max. Retransmissions)**

  输入最大连接尝试次数。

- **主服务器 (Primary Server)**

  指定此服务器是否是主服务器。

  – 是 (Yes)：主服务器

  – 否 (No)：备份服务器。

- **状态 (State)**

  使用此复选框，可启用或禁用 RADIUS 服务器

步骤

输入新服务器

要显示新服务器，请按以下步骤操作：

1. 在相关行中，在输入框中输入以下数据：

   – RADIUS 服务器的 IP 地址或 FQDN 名称。

   – 输入端口的端口号

   – 密码

   – 密码确认

   – 传输重试的最大次数

   – 主服务器

2. 单击"设置值"(Set Values) 按钮。

修改服务器

1. 在相关行中，在输入框中输入以下数据：
   - 服务器 IP 地址
   - 输入端口的端口号
   - 密码
   - 密码确认
   - 传输重试的最大次数
   - 主服务器
2. 单击"设置值"(Set Values) 按钮。

对要修改的输入内容所属的每台服务器重复此步骤。

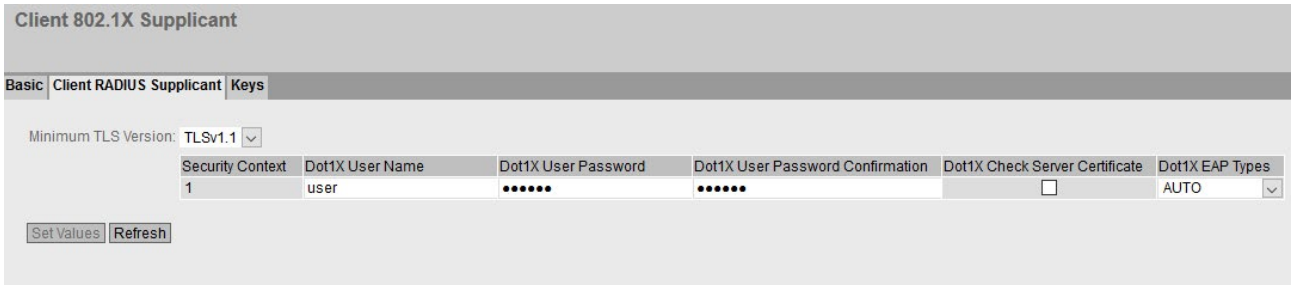
6.9.4.5 客户端 RADIUS 请求者

客户端请求者

在此 WBM 页面中，可组态客户端的 RADIUS 验证设置。

说明

只有客户端或处于客户端模式下的接入点可使用此页面。



描述

- **最低 TLS 版本 (Minimum.TLS version)**

  指定 WLAN RADIUS 验证将使用的最低 TLS 版本。

  说明

  RADIUS 服务器
  仅当 RADIUS 服务器支持相应 TLS 版本时才可实现。

该表格包括以下列：

- **安全上下文 (Security Context)**

  显示安全上下文。

- **Dot1x 用户名 (Dot1x User Name)**

  输入要在 RADIUS 服务器登录时使用的用户名。

- **Dot1x 用户密码 (Dot1x User Password)**

  输入上面所选用户名的密码。客户端使用使用该用户名和密码组合登录 RADIUS 服务器。
  密码分配使用 ASCII 码 0x20 至 0x7e。

- **Dot1x 用户密码确认 (Dot1x User Password Confirmation)**

  确认密码。

说明

Dot1X 用户名和 Dot1X 用户密码
使用 WPA (RADIUS)、WPA2 (RADIUS)、EAP-TLS、EAP-TTLS 和 PEAP 时，必须组态 Dot1X 用户名和 Dot1X 用户密码。
使用设置"自动"(Auto) 时，必须加载证书或必须组态 Dot1X 用户名和 Dot1X 用户密码。

- **Dot1X 服务器证书 (Dot1X Server Certificate)**

  指定 RADIUS 服务器是否通过证书向客户端证实自身。

  说明

  使用证书

  在证书过期前延长证书期限。如果不及时延长证书期限，证书过期后将无法建立连接。

- **Dot1x EAP 类型 (Dot1x EAP Types)**

  指定验证方法。存在以下方法：

  – Auto

    客户端为 RADIUS 服务器提供所有方法。

  – EAP-TLS

    Extensible Authentication Protocol - Transport Layer Security

    使用证书进行验证。

  – EAP-TTLS

    Extensible Authentication Protocol - Tunnel Transport Layer Security

    建立 TLS 隧道后，使用 MS-CHAPv2 进行内部验证。

  – PEAP

    Protected Extensible Authentication Protocol

    EAP-TTLS 的 IETF 备用协议草案

步骤

1. 在输入框中输入必需的值。
2. 在"Dot1x EAP 类型"(Dot1x EAP Types) 下拉列表中选择所需条目。
3. 单击"设置值"(Set Values) 按钮。

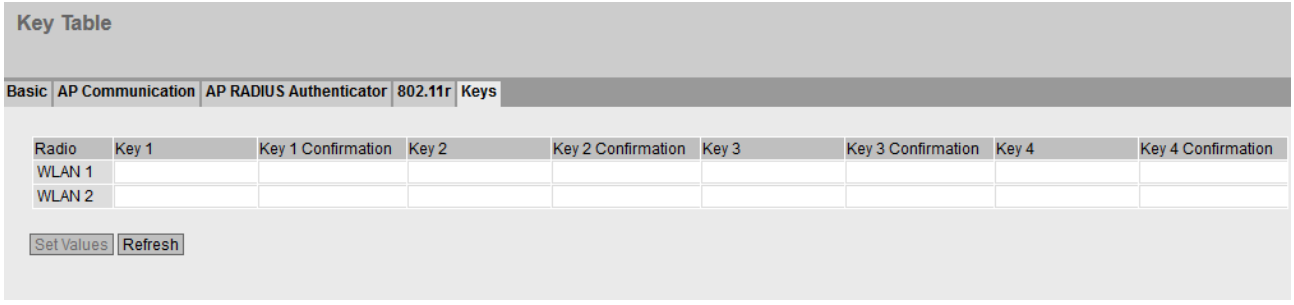
参见

RADIUS 验证支持的安全机制 (页 595)

6.9.4.6 密钥

指定 WEP 密钥

为允许用户能够对"开放式系统"(Open System) 和"共享密钥"(Shared Key) 验证方法进行加密，首先必须在密钥表中输入至少一个密钥。



说明

该表包括以下列：

- **无线 (Radio)**

  显示可用的 WLAN 接口。

- **密钥 1 - 4 (Key 1 - 4)**

  输入 WEP 密钥或 AES 密钥。

  对于 WEP 密钥，允许使用 ASCII 码字符 0x20 至 0x7E 或十六进制字符 0x00 至 0xFF。

  如果已启用 iPCF 或 iPCF-MC 模式，则仅支持密钥长度为 128 位的 AES 加密方法。

  可在以下密钥长度中进行选择：

  – 5 或 13 个 ASCII 字符，或者 10 或 26 个十六进制字符（40/104 位）

  – 16 个 ASCII 字符或 32 个十六进制字符（128 位）

  说明

  输入十六进制字符时，前面不加"0x"。一个十六进制字符代码占四位。因此，条目"ABCDE"（ASCII 字符）和"4142434445"（十六进制字符）等价，因为 ASCII 字符"A"的十六进制代码为"0x41"。

- **Key 1 - 4 Confirmation**

  确认 WEP 密钥。

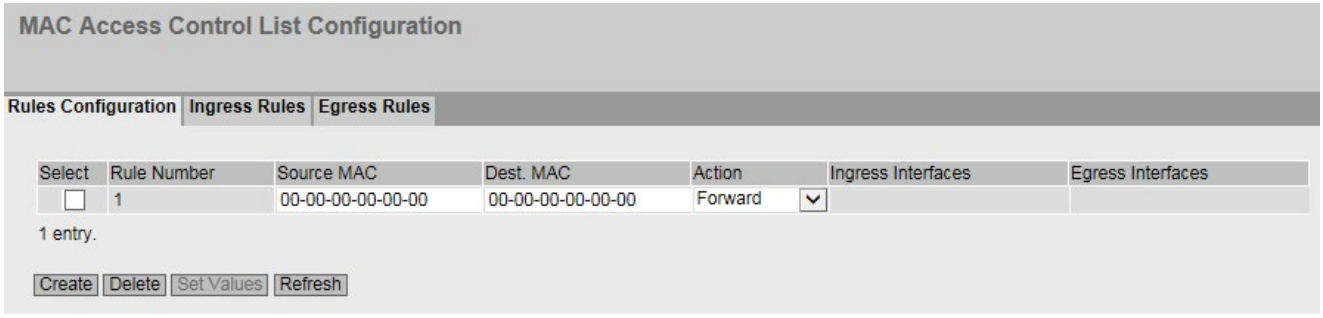
步骤

1. 输入至少一个 WEP 密钥。
2. 单击"设置值"(Set Values) 按钮。

6.9.5 MAC ACL

6.9.5.1 规则组态

在此页面上为基于 MAC 的访问控制列表指定访问规则。使用基于 MAC 的 ACL，可指定是转发还是丢弃特定 MAC 地址的帧。



描述

该表格包括以下列：

- **选择 (Select)**
  选择要删除的行。如果使用该条目，则呈灰显且无法删除。
- **规则编号 (Rule Number)**
  显示 ACL 规则的编号。如果创建新的条目，会创建一个带有唯一编号的新行。
- **源 MAC 地址 (Source MAC Address)**
  输入源的 MAC 地址。
- **目标 MAC 地址 (Dest. MAC Address)**
  输入目标的 MAC 地址。
- **Action**
  选择在帧符合 ACL 规则时是转发帧还是拒绝帧。
  - 转发 (Forward)
    如果帧符合 ACL 规则，则转发该帧。
  - 丢弃 (Discard)
    如果帧符合 ACL 规则，则不转发该帧。

- **入站接口 (Ingress Interfaces)**

  显示应用此规则的所有入站接口的列表。

- **出站接口 (Egress Interfaces)**

  显示应用此规则的所有出站接口的列表。

说明

输入 MAC 地址

可以为 MAC 地址组态访问规则。

只有在为源和/或目标 MAC 地址输入地址"00-00-00-00-00-00"时，才能将采用此方法创建的规则应用到所有源或目标 MAC 地址。

说明

没有适用于本地支持协议的 ACL 规则

ACL 规则不适用于来自本地支持协议的数据包。此限制适用于以下协议：

- DCP
- LLDP
- RSTP

在相应协议的组态页面上直接为这些协议设置用于接收和发送数据包的规范。

组态步骤

1. 单击"创建"(Create) 按钮。会在表中创建一个具有唯一编号（规则编号）的新行。
2. 在"源 MAC 地址"(Source MAC Address) 中输入源的 MAC 地址。
3. 在"目标 MAC 地址"(Dest. MAC Address) 中输入目标的 MAC 地址。
4. 在"操作"(Action) 下拉列表中选择在符合 ACL 规则时是转发帧还是拒绝帧。
5. 单击"设置值"(Set Values) 按钮。

删除条目

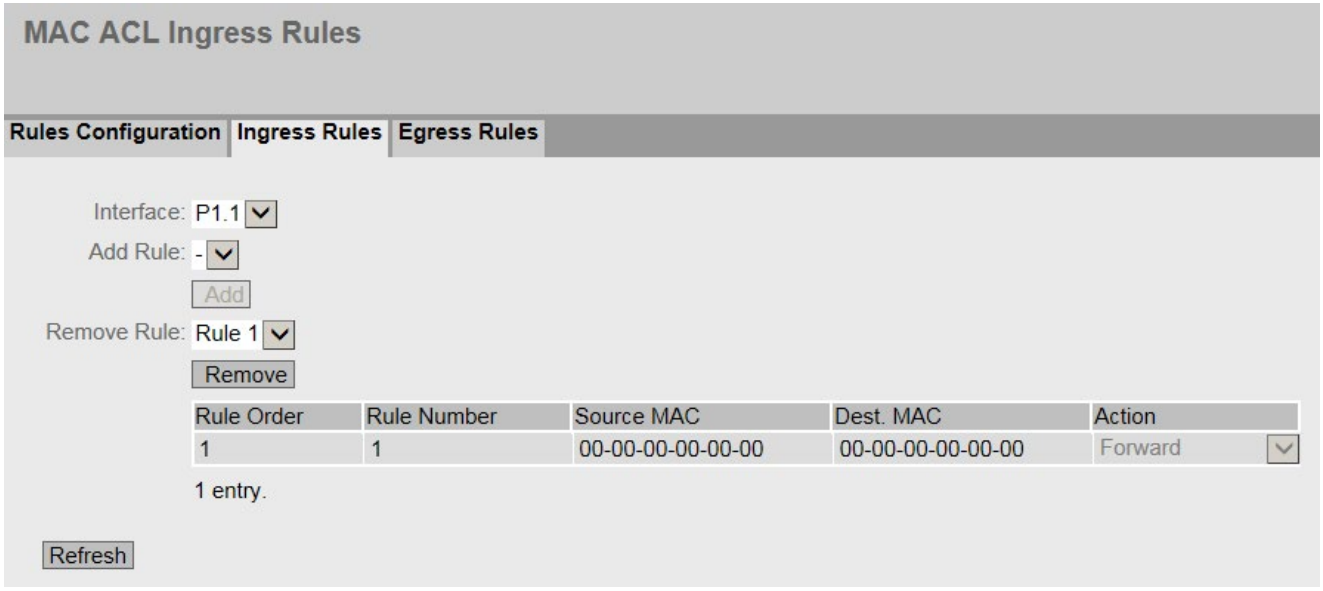
无法删除激活条目。

1. 启用要删除的行中的"选择"(Select)。
2. 单击"删除"(Delete) 按钮。删除了相关条目。

6.9.5.2 Ingress Rules

简介

在此页面上指定 ACL 规则，接口将根据此规则过滤入站帧。在"规则组态"(Rules Configuration) 选项卡中指定 ACL 规则。



显示框说明

该页面包含以下框：

- **接口 (Interface)**
  从该下拉列表中选择所需接口。根据具体设备显示可用接口 (页 51)。
- **添加规则 (Add Rule)**
  从该下拉列表中选择要分配给接口的 ACL 规则。

- **添加 (Add)**

  要将 ACL 规则分配给接口，请单击"添加"(Add) 按钮。组态会显示在表中。

- **删除规则 (Remove Rule)**

  从"删除规则"(Remove Rule) 下拉列表中选择要删除的 ACL 规则。

- **删除 (Remove)**

  要删除接口的 ACL 规则，请单击"删除"(Remove) 按钮。

该表格包括以下列：

- **规则顺序 (Rule Order)**

  显示 ACL 规则的顺序。

- **规则编号 (Rule Number)**

  显示 ACL 规则的编号。

- **源 MAC 地址 (Source MAC Address)**

  显示源的 MAC 地址。

- **目标 MAC 地址 (Dest. MAC Address)**

  显示目标的 MAC 地址。

- **操作 (Action)**

  显示操作。

  – Forward

    如果帧符合 ACL 规则，则转发该帧。

  – Discard

    如果帧符合 ACL 规则，则不转发该帧。

组态步骤

按照以下步骤为接口分配 ACL 规则：

1. 从"接口"(Interface) 下拉列表中选择接口。
2. 在"添加规则"(Add Rule) 下拉列表中选择 ACL 规则。
3. 单击"Add"按钮。会在表中生成一个新条目。

按照以下步骤删除接口的 ACL 规则：

说明

激活规则

无法删除激活规则。

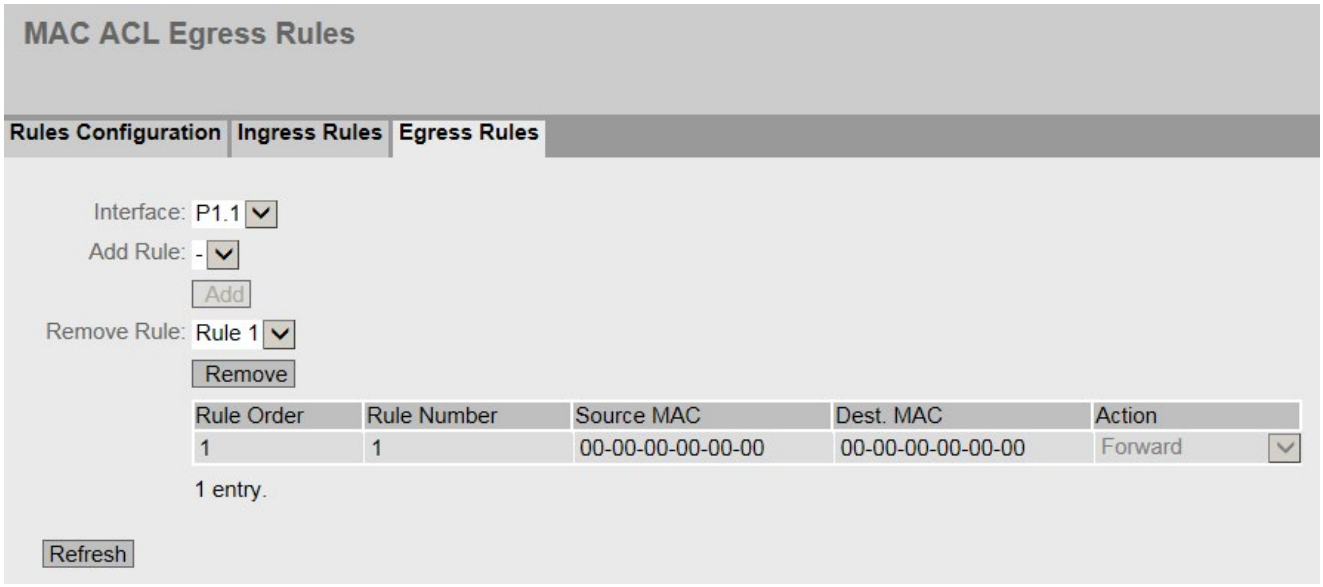
---

1. 从"接口"(Interface) 下拉列表中选择接口。
2. 在"删除规则"(Remove Rules) 下拉列表中选择 ACL 规则。
3. 单击"Remove"按钮。将从表中删除相应的条目。

6.9.5.3 Egress Rules

简介

在此页面上指定 ACL 规则，接口将根据此规则过滤出站帧。在▸"规则组态"(Rules Configuration) 选项卡中指定 ACL 规则。



显示框说明

该页面包含以下框：

- **接口 (Interface)**
  从该下拉列表中选择所需接口。根据具体设备显示可用接口 (页 51)。
- **添加规则 (Add Rule)**
  从该下拉列表中选择要分配给接口的 ACL 规则。
- **添加 (Add)**
  要将 ACL 规则分配给接口，请单击"添加"(Add) 按钮。组态会显示在表中。

- **删除规则 (Remove Rule)**

  从"删除规则"(Remove Rule) 下拉列表中选择要删除的 ACL 规则。

- **删除 (Remove)**

  要删除接口的 ACL 规则，请单击"删除"(Remove) 按钮。

该表格包括以下列：

- **规则顺序 (Rule Order)**

  显示 ACL 规则的顺序。

- **规则编号 (Rule Number)**

  显示 ACL 规则的编号。

- **源 MAC 地址 (Source MAC Address)**

  显示源的 MAC 地址。

- **目标 MAC 地址 (Dest. MAC Address)**

  显示目标的 MAC 地址。

- **操作 (Action)**

  显示操作。

  – Forward

    如果帧符合 ACL 规则，则转发该帧。

  – Discard

    如果帧符合 ACL 规则，则不转发该帧。

组态步骤

按照以下步骤为接口分配 ACL 规则：

1. 从"接口"(Interface) 下拉列表中选择接口。
2. 在"添加规则"(Add Rule) 下拉列表中选择 ACL 规则。
3. 单击"Add"按钮。会在表中生成一个新条目。

按照以下步骤删除接口的 ACL 规则：

说明

激活规则

无法删除激活规则。

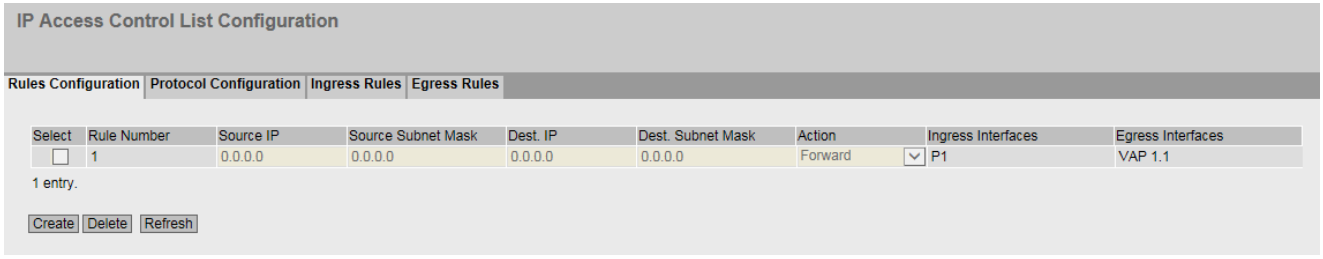
1. 从"接口"(Interface) 下拉列表中选择接口。
2. 在"删除规则"(Remove Rules) 下拉列表中选择 ACL 规则。
3. 单击"Remove"按钮。将从表中删除相应的条目。

6.9.6 IP ACL

6.9.6.1 Rules Configuration

简介

在此页面上为基于 IP 的 ACL 指定规则。通过使用基于 IP 的 ACL，您可指定是转发还是丢弃特定 IPv4 地址的帧。



显示框说明

该表格包括以下列：

- **Select**

  选择要删除的行。如果使用该条目，则呈灰显且无法删除。

- **规则编号 (Rule Number)**

  显示 ACL 规则的编号。如果创建新的条目，会创建一个带有唯一编号的新行。

- **Source IP**

  输入源的 IPv4 地址。

- **源子网掩码 (Source Subnet Mask)**

  输入源的子网掩码。

- **目标 IP**

  输入目标的 IPv4 地址。

- **Dest.Subnet Mask**

  输入目标的子网掩码。

- **Action**

  选择在帧符合 ACL 规则时是转发帧还是拒绝帧。

  – Forward

    如果帧符合 ACL 规则，则转发该帧。

  – Discard

    如果帧符合 ACL 规则，则不转发该帧。

- **入站接口 (Ingress Interfaces)**

  显示应用此规则的所有入站接口的列表。

- **出站接口 (Egress Interfaces)**

  显示应用此规则的所有出站接口的列表。

说明

各主机的子网掩码

如果为单一系统创建规则（一个 IPv4 地址），指定子网掩码"255.255.255.255"。

组态步骤

1. 单击"创建"(Create) 按钮。会在表中创建一个具有唯一编号（规则编号）的新行。
2. 在"源 IP"(Source IP) 和"源子网掩码"(Source Subnet Mask) 中输入源的数据。
3. 在""目标 IP"(Dest. IP) 和"目标子网掩码"(Dest. Subnet Mask) 中输入目标的数据。
4. 在"操作"(Action) 下拉列表中选择在帧符合 ACL 规则时是转发帧还是拒绝帧。
5. 单击"设置值"(Set Values) 按钮。

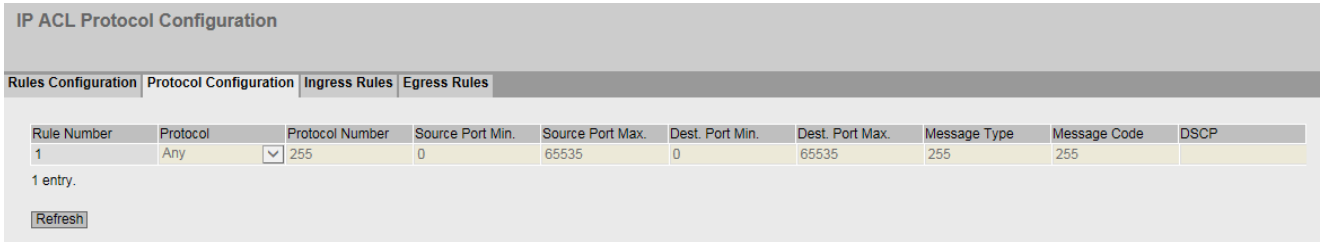
删除条目

无法删除激活条目。

1. 启用要删除的行中的"选择"(Select)。
2. 单击"删除"(Delete) 按钮。删除了相关条目。

6.9.6.2 协议组态

可在此页面中为协议指定规则。



说明

该表格包括以下列：

- **Rule Number**

  显示协议规则的编号。创建规则时，会创建一个具有唯一编号的新行。

- **协议 (Protocol)**

  选择该规则对其有效的协议。

- **Protocol Number**

  输入协议编号以定义其它协议。

  只有为协议设置了"Other Protocol"时才能编辑该框。

- **Source Port Min.**

  输入源端口可能的最小端口号。

  只有为协议设置了"TCP"或"UDP"时才能编辑该框。

- **Source Port Max.**

  输入源端口可能的最大端口号。

  只有为协议设置了"TCP"或"UDP"时才能编辑该框。

- **目标 Port Min.**

  输入目标端口可能的最小端口号。

  只有为协议设置了"TCP"或"UDP"时才能编辑该框。

- **目标 Port Max.**

  输入目标端口可能的最大端口号。

  只有为协议设置了"TCP"或"UDP"时才能编辑该框。

- **Message Type**

  输入消息类型以决定消息的格式。

  只有为协议设置了"ICMP"时才能编辑该框。

- **Message Code**

  输入消息代码以指定消息的功能。

  只有为协议设置了"ICMP"时才能编辑该框。

- **DSCP**

  输入用于划分优先级的值。

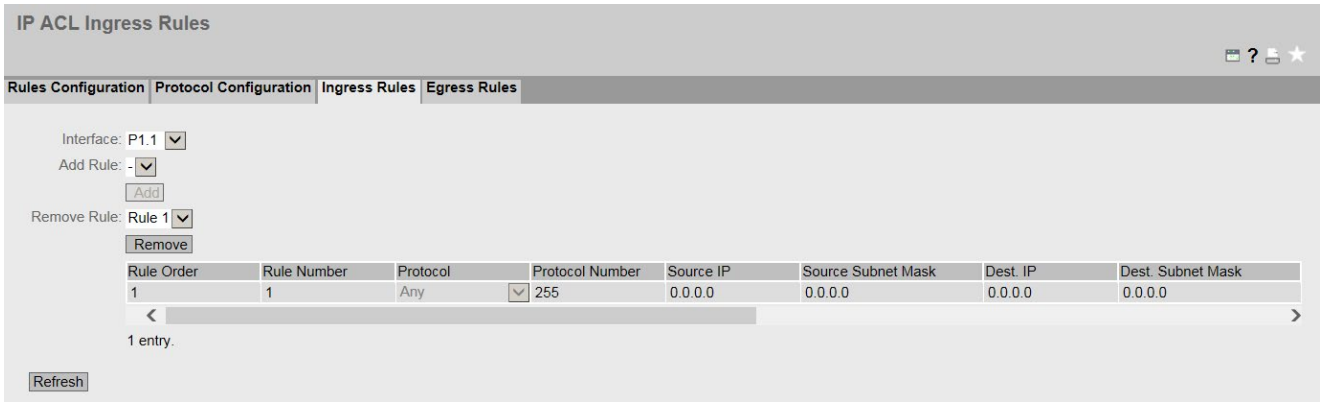
  如果为协议设置了"ICMP"，则无法编辑该框。

6.9.6.3 入站规则

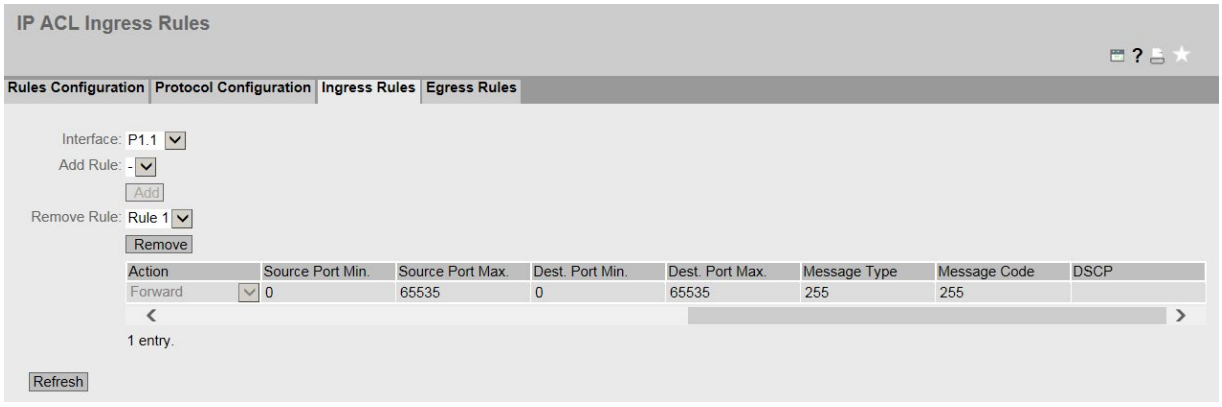
简介

在此页面上指定 ACL 规则，接口将根据此规则处理入站帧。在"规则组态"(Rules Configuration) 选项卡中指定 ACL 规则。

IP ACL 入站规则 - 表的第一部分：



IP ACL 入站规则 - 表的第二部分：



显示框说明

该页面包含以下框：

- **接口 (Interface)**

  从该下拉列表中选择所需接口。根据具体设备显示可用接口 (页 51)。

  要选择 VLAN 接口，则必须组态 IP 接口。

  说明

  如果使用 VLAN 接口，ACL 规则将适用于属于 VLAN 的所有端口。

- **添加规则 (Add Rule)**

  从该下拉列表中选择要分配给接口的 ACL 规则。

- **添加 (Add)**

  要将 ACL 规则永久分配给接口，请单击"添加"(Add) 按钮。组态会显示在表中。

- **删除规则 (Remove Rule)**

  从"删除规则"(Remove Rule) 下拉列表中选择要删除的 ACL 规则。

- **删除 (Remove)**

  要删除接口的 ACL 规则，请单击"删除"(Remove) 按钮。

该表格包括以下列：

- **规则顺序 (Rule Order)**
  显示 ACL 规则的顺序。
- **规则编号 (Rule Number)**
  显示 ACL 规则的编号。
- **Protocol**
  显示该规则对其有效的协议。
- **Protocol Number**
  显示协议编号。
- **Source IP**
  显示源的 IPv4 地址。
- **源子网掩码 (Source Subnet Mask)**
  显示源的子网掩码。
- **Dest IP**
  显示目标的 IP 地址。
- **Dest.Subnet Mask**
  显示目标的子网掩码。
- **Action**
  选择在帧符合 ACL 规则时，是转发还是拒绝该帧。
  - Forward
    如果帧符合 ACL 规则，则转发该帧。
  - Discard
    如果帧符合 ACL 规则，则不转发该帧。
- **Source Port Min.**
  显示源端口可能的最小端口号。

- **Source Port Max.**

  显示源端口可能的最大端口号。

- **Dest.Port Min.**

  显示目标端口可能的最小端口号。

- **Dest.Port Max.**

  显示目标端口可能的最大端口号。

- **Message Type**

  显示消息类型以决定消息的格式。

- **Message Code**

  显示消息代码以指定消息的功能。

- **DSCP**

  显示用于划分优先级的值。

组态步骤

按照以下步骤为接口分配 ACL 规则：

1. 从"接口"(Interface) 下拉列表中选择接口。
2. 在"添加规则"(Add Rule) 下拉列表中选择 ACL 规则。
3. 单击"Add"按钮。会在表中生成一个新条目。

按照以下步骤为接口分配 ACL 规则：

说明

激活规则

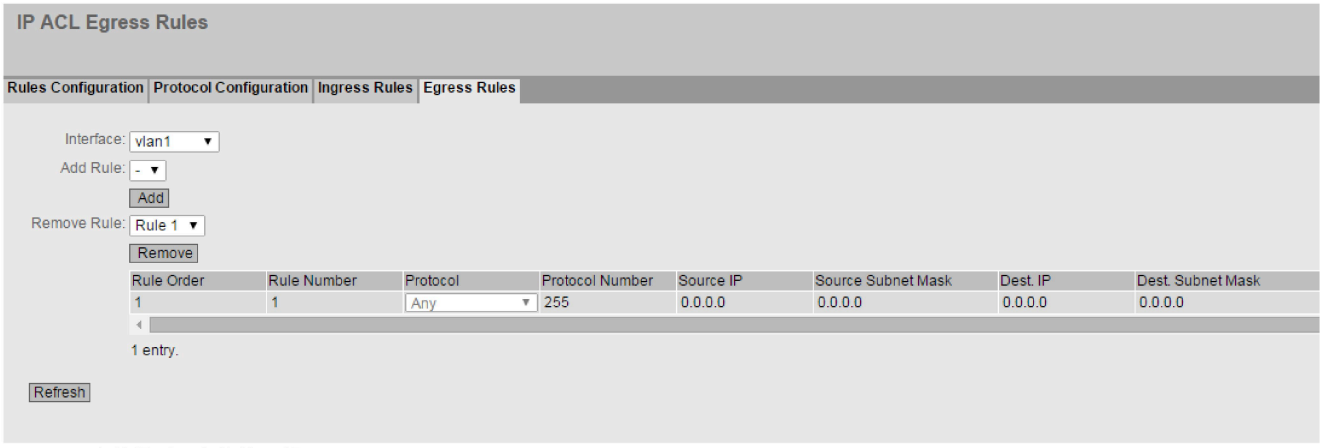
无法删除激活规则。

1. 从"接口"(Interface) 下拉列表中选择接口。
2. 在"删除规则"(Remove Rules) 下拉列表中选择 ACL 规则。
3. 单击"Remove"按钮。删除相应的条目。

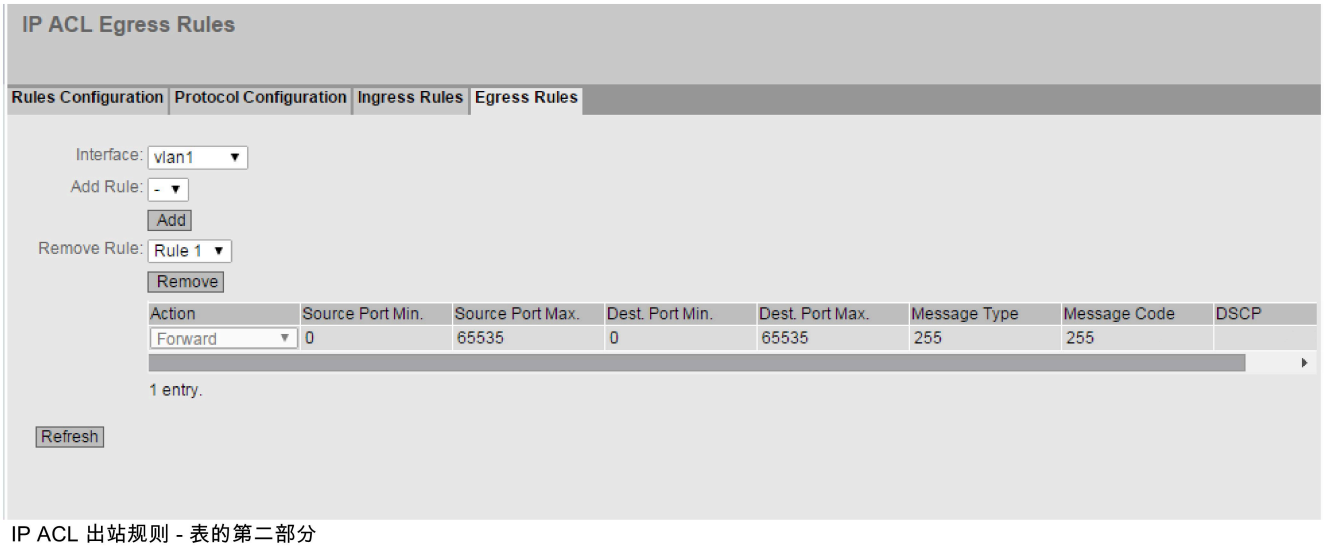
6.9.6.4 出站规则

简介

在此页面上指定 ACL 规则，端口将根据此规则处理出站帧。在"规则组态"(Rules Configuration) 选项卡中指定 ACL 规则。



IIP ACL 出站规则 - 表的第一部分



IP ACL 出站规则 - 表的第二部分

显示框说明

该页面包含以下框：

- **接口 (Interface)**

  从该下拉列表中选择所需接口。可用的接口 (页 51)取决于具体设备。

  要选择 VLAN 接口，则必须组态 IP 接口。

  说明

  如果使用 VLAN 接口，ACL 规则将适用于属于 VLAN 的所有端口。

- **添加规则 (Add Rule)**

  从该下拉列表中选择要分配给接口的 ACL 规则。

- **添加 (Add)**

  要将 ACL 规则分配给接口，请单击"添加"(Add) 按钮。组态会显示在表中。

  说明

  不得对出站帧应用内容为"无论如何都拒绝"(deny any) 的 ACL 规则。

- **删除规则 (Remove Rule)**

  从"删除规则"(Remove Rule) 下拉列表中选择要删除的 ACL 规则。

- **删除 (Remove)**

  要删除接口的 ACL 规则，请单击"删除"(Remove) 按钮。

该表包括以下列：

- **规则顺序 (Rule Order)**

  显示 ACL 规则的顺序。

- **规则编号 (Rule Number)**

  显示 ACL 规则的编号。

- **Protocol**

  显示该规则对其有效的协议。

- **Protocol Number**

  显示协议编号。

- **Source IP**

  显示源的 IPv4 地址。

- **源子网掩码 (Source Subnet Mask)**

  显示源的子网掩码。

- **Dest IP**

  显示目标的 IP 地址。

- **Dest.Subnet Mask**

  显示目标的子网掩码。

- **Action**

  选择在帧符合 ACL 规则时，是转发还是拒绝该帧。

  – Forward

    如果帧符合 ACL 规则，则转发该帧。

  – Discard

    如果帧符合 ACL 规则，则不转发该帧。

- **Source Port Min.**

  显示源端口可能的最小端口号。

- **Source Port Max.**

  显示源端口可能的最大端口号。

- **Dest.Port Min.**

  显示目标端口可能的最小端口号。

- **Dest.Port Max.**

  显示目标端口可能的最大端口号。

- **Message Type**

  显示消息类型以决定消息的格式。

- **Message Code**

  显示消息代码以指定消息的功能。

- **DSCP**

  显示用于划分优先级的值。

组态步骤

按照以下步骤为接口分配 ACL 规则：

1. 从"接口"(Interface) 下拉列表中选择接口。
2. 在"添加规则"(Add Rule) 下拉列表中选择 ACL 规则。
3. 单击"Add"按钮。会在表中生成一个新条目。

按照以下步骤删除接口的 ACL 规则：

说明

激活规则

无法删除激活规则。

1. 从"接口"(Interface) 下拉列表中选择接口。
2. 在"删除规则"(Remove Rules) 下拉列表中选择 ACL 规则。
3. 单击"Remove"按钮。将从表中删除相应的条目。

6.9.7 管理 ACL

组态说明

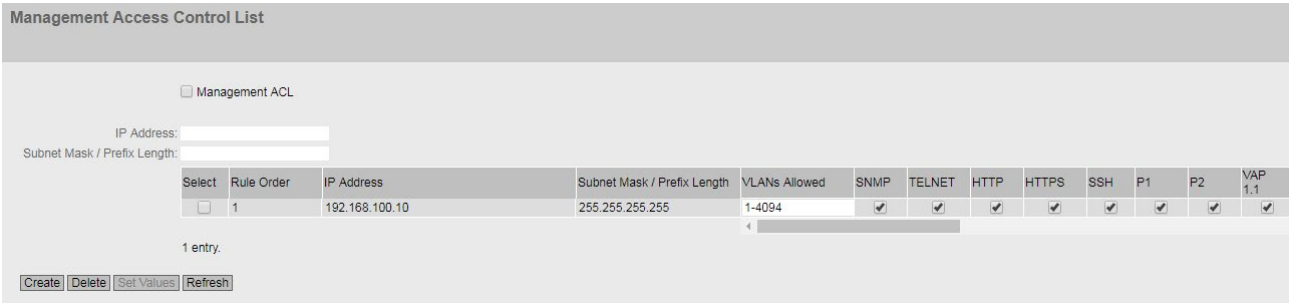
在此页面上，可提高设备的安全性。要指定具有哪个 IP 地址的工作站允许访问设备，必须组态相应的 IP 地址或一个地址范围。

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

说明

如果启用此功能，请注意以下几点

"Management Access Control List"页面上的不正确组态可能会导致无法访问设备。因此应组态一个访问规则，以便在启用该功能前可对管理功能进行访问。



说明

该页面包含以下框：

- **管理 ACL (Management ACL)**

  启用或禁用此功能。

  说明

  如果禁用了该功能，则对设备管理功能的访问不受限制。组态的访问规则仅在该功能启用后有效。

- **IP 地址 (IP Address)**

  输入将应用该规则的 IP 地址或网络地址。

  – 如果使用 IPv4 地址 0.0.0.0，则设置将适用于所有 IPv4 地址。

  – 如果使用 IPv6 地址：该设置适用于所有 IPv6 地址。

- **子网掩码/前缀长度 (Subnet Mask / Prefix Length)**

  输入子网掩码或前缀长度。

  子网掩码 255.255.255.255 适用于特定的 IPv4 地址。如果要允许使用子网（如 C 子网），则输入 255.255.255.0。子网掩码 0.0.0.0 适用于所有子网。

该表包括以下列：

- **选择 (Select)**

  选中要删除的行中的复选框。

- **规则顺序 (Rule Order)**

  显示规则编号。如果单击"创建"(Create) 按钮，会创建一个具有唯一编号的新行。

- **IP 地址 (IP Address)**

  显示 IP 地址。

- **子网掩码/前缀长度 (Subnet Mask / Prefix Length)**

  显示子网掩码或前缀长度。

- **允许的 VLAN (VLANs Allowed)**

  仅当在"Layer 2 > VLAN > 常规"(Layer 2 > VLAN > General) 中设置了 802.1Q VLAN Bridge 时才可用。

  输入设备所在 VLAN 的编号。仅当设备位于该组态 VLAN 中时，站才能访问该设备。如果该输入框留空，则没有关于 VLAN 的限制。

- **SNMP**

  指定工作站（或 IP 地址）是否使用 SNMP 协议访问设备。

- **TELNET**

  指定工作站（或 IP 地址）是否使用 TELNET 协议访问设备。

- **HTTP**

  指定工作站（或 IP 地址）是否使用 HTTP 协议访问设备。

- **HTTPS**

  指定工作站（或 IP 地址）是否使用 HTTPS 协议访问设备。

- **SSH**

  指定工作站（或 IP 地址）是否使用 SSH 协议访问设备。

- **Px**

  指定该站点（或 IP 地址）是否通过此端口访问设备。

- **VAP X.Y**

  指定该站点（或 IP 地址）是否通过 VAP 接口访问设备。

- **WDS X.Y**

  指定该站点（或 IP 地址）是否通过 WDS 接口访问设备。

步骤

说明

请注意，错误的组态可能意味着您再不能访问设备。
只能通过将设备先复位到出厂默认设置，然后重新组态来解决此问题。

更改条目

1. 组态要修改的条目数据。
2. 单击"设置值"(Set Values) 按钮将更改传输到设备。

创建新条目

1. 在"IP 地址"(IP Address) 输入框中输入设备的 IP 地址，在"子网掩码/前缀长度"(Subnet Mask/Prefix Length) 输入框中输入相应的子网掩码。
2. 单击"创建"(Create) 按钮在表中创建新行。
3. 组态新行的条目。
4. 单击"设置值"(Set Values) 按钮将新条目传输到设备。

删除条目

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

6.9.8 AP 间阻塞

6.9.8.1 基本

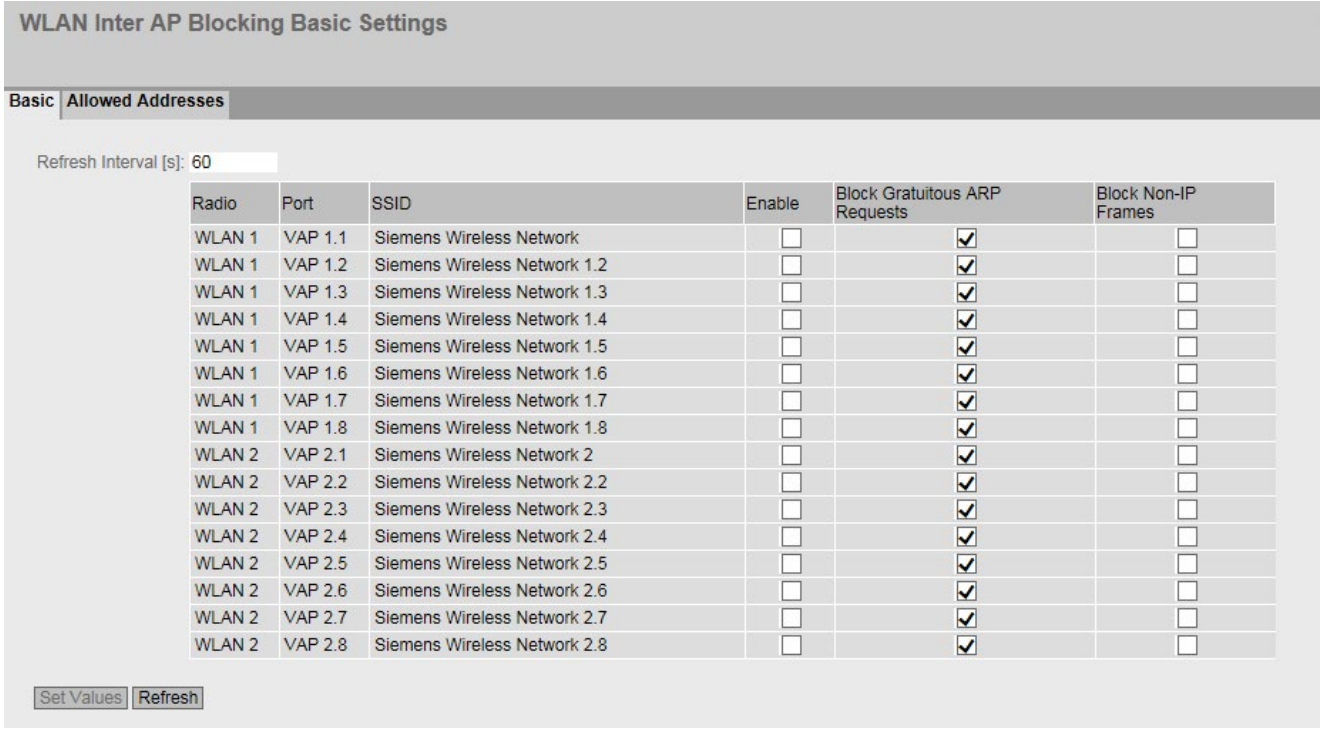
说明

- 该 WBM 页面仅在接入点模式下可用。
- 此 WBM 页面仅可通过以下 KEY-PLUG 组态：
  - W780 iFeatures (MLFB 6GK5 907-8PA00)
  - W700 Security (MLFB 6GK5907-0PA00)

何时应使用 AP 间阻塞？

与接入点相连的客户端通常可以与第 2 层有线网络的所有设备进行通信。

使用 AP 间阻塞时，与接入点相连的客户端的通信会受到限制。只有在接入点的"允许地址"(Allowed Addresses) 中组态了 IP 地址的设备才可以访问客户端。因此，将阻止与网络中其它节点的通信。



说明

该页面包含以下框：

- **更新间隔 [s] (Update interval [s])**

  输入允许的 IP 地址的 ARP 解析更新间隔。

  解析的 MAC 地址显示在"信息 > 安全 > AP 间阻塞"(Information > Security > Inter AP Blocking) 下。

该表包括以下列：

- **无线 (Radio)**

  指定设置所关联的 WLAN 接口。

- **Port**

  指定与设置相关的 VAP 接口。

- **SSID**

  指定与设置相关的 SSID。

- **激活 (Activate)**

  启用后，会启用访问限制。在"安全 > AP 间阻塞 > 允许的地址"(Security > Inter AP Blocking > Allowed Addresses) 中组态客户端可以访问的设备。

- **拦截不必要的 ARP 请求 (Block Gratuitous ARP Requests)**

  当启用后，不会将来自此 VAP 接口的主动 ARP 数据包转发到以太网。

- **阻止非 IP 帧 (Block Non-IP Frames)**

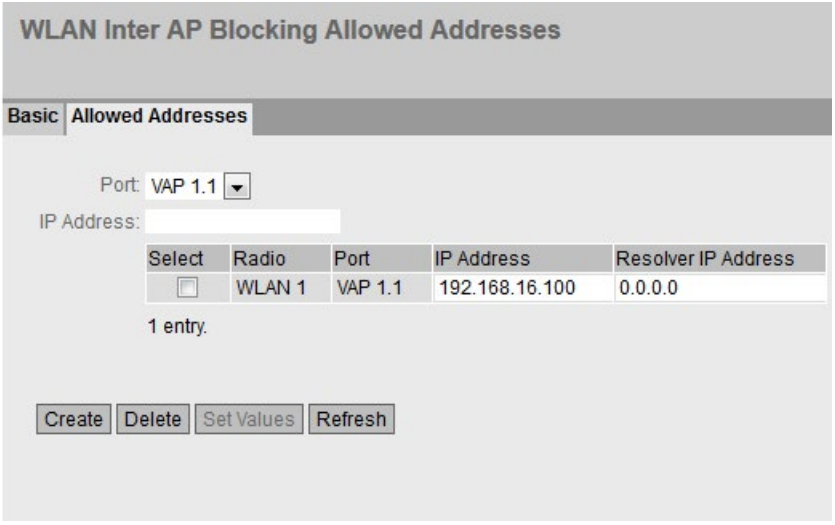
  启用后，客户端与在接入点上组态为允许的通信伙伴的设备之间不会发生非 IP 数据包（例如第 2 层数据包）交换。

6.9.8.2 允许的地址

说明

- 该 WBM 页面仅在接入点模式下可用。
- 此 WBM 页面仅可通过以下 KEY-PLUG 组态：
  - W780 iFeatures (MLFB 6GK5 907-8PA00)
  - W700 Security (MLFB 6GK5907-0PA00)

在此 WBM 页面中指定可以访问客户端的设备。



说明

该页面包含以下框：

- **Port**

  从下拉列表中选择所需端口。

- **IP 地址 (IP Address)**

  输入客户端可以访问的设备的 IP 地址。

该表包括以下列：

- **选择 (Select)**

  选中要删除的行中的相应复选框

- **无线 (Radio)**

  指定与设置相关的 WLAN 接口

- **Port**

  指定与设置相关的 VAP 接口

- **IP 地址 (IP Address)**

  可以访问客户端的设备的 IP 地址。如有必要，可以更改 IP 地址。

- **解析器 IP 地址 (Resolver IP Address)**

  接入点用来解析允许的 IP 地址的 IP 地址。当接入点的管理 IP 地址位于不同的子网时，必须输入此地址。
  如果为"解析器 IP 地址"(Resolver IP Address) 组态了 IP 地址"0.0.0.0"，则使用管理 IP 地址进行解析。

步骤

创建条目

1. 从"端口"(Port) 下拉列表中选择端口。
2. 在"IP 地址"(IP Address) 框中，输入可以访问客户端的 IP 地址。
3. 单击"创建"(Create) 按钮。随即会在表中创建一个新条目。

删除条目

1. 启用要删除的行中的"选择"(Select)。
2. 单击"删除"(Delete) 按钮。删除了相关条目。

6.10 "iFeatures"菜单

6.10.1 iPCF

说明

此 WBM 页面仅可通过以下 KEY-PLUG 组态：

- 接入点：W780 iFeatures (MLFB 6GK5 907-8PA00)
- 客户端：W740 iFeatures (MLFB 6GK5 907-4PA00)

何时应使用 iPCF？

说明

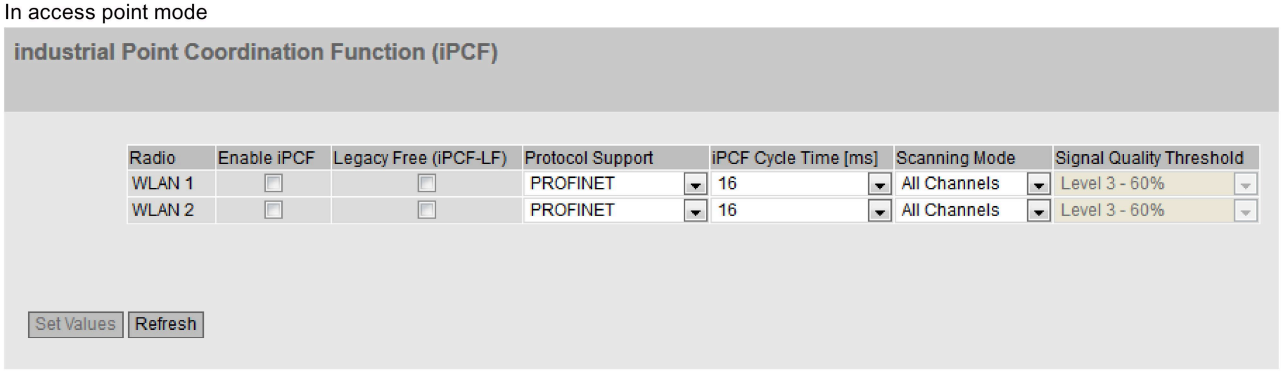
iPCF 与其它 iFeatures 配合使用

iPCF 和其它 iFeatures（例如，iPCF-MC、iPCF-HT 和 iPRP）互不兼容，无法在设备上同时使用。

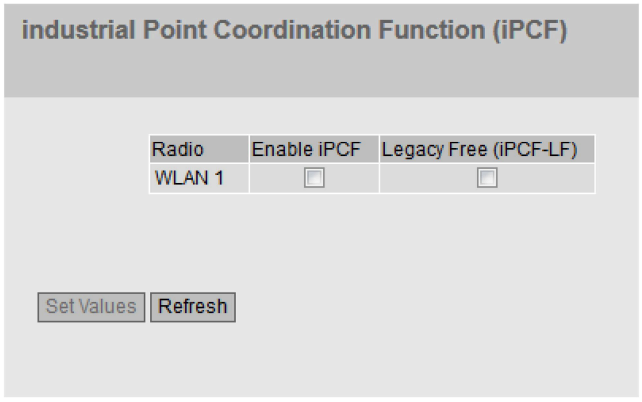
在具有大量的节点或者想要实施高确定性的操作时，尤其建议采用 iPCF。例如，采用 PROFINET 或其它循环协议时，这很有必要。有关 iPCF 的更多详细说明，请参见"iPCF/iPCF-HT/iPCF-MC"的"技术基础"部分。

接入点和客户端的可能设置有所不同。下文介绍了这两种模式。

In access point mode



In client mode



描述

在两种模式下，该表都具有以下表列：

- **无线 (Radio)**

  指定设置所关联的 WLAN 接口。

- **启用 iPCF (Enable iPCF)**

  启用或禁用 iPCF 模式。对于 PROFINET 通信，我们建议用户启用 iPCF 模式。通过启用 iPCF，可调整由接入点提供的数据速率。强烈建议保留数据速率的默认设置（802.11 a/b/g = 12 Mbps，802.11n = MCS 2）。

- **Legacy Free (iPCF-LF)**

  此设置确定可以建立与此设备的连接的设备系列。

  – 启用

    仅接受按照 IEEE 802.11n 标准进行通信并启用了"Legacy Free (iPCF-LF)"设置的设备。但无需为此启用 WLAN 模式 IEEE 802.11n。

    此设置可防止 IEEE 802.11 a/b/g 设备系列导致性能降低。

  – 禁用

    接受所有设备系列 (IEEE 802.11 a/b/g/n)。

在接入点模式下，该表具有下列附加列：

- **协议支持 (Protocol Support)**

  指定 WLAN 接口优先处理的协议。

  – PROFINET

    如果设置了 PROFINET，则客户端下游不能有中央 PROFINET 控制器。

  – EtherNet/IP

    如果设置了 EtherNet/IP，则客户端下游不能有扫描器。

  – 禁用

    将禁用该功能。

- **iPCF 周期时间 [ms] (iPCF Cycle Time [ms])**

  从该下拉列表中选择所需的周期时间。
  设置循环时间时，需考虑以下几点。否则可能无法建立稳定的通信。

  – 系统中只有一个接入点，也就是说，客户端只在一个无线蜂窝区中移动。在这种情况下，支持大于等于 16 ms 的更新时间。

  – 系统中有多个接入点，可在不同的通道中进行通信。客户端在接入点之间漫游。在此情况下，选择大于等于 32 ms 的更新时间。

  除了以上所示的指导值外，还需记住，要设置的最短循环时间是根据公式"2 ms * 最大节点数"计算得出的。

- **扫描模式 (Scanning mode)**

  所选设置会影响对已登录客户端的扫描。

  可使用以下设置：

  – 所有通道 (All Channels)
    客户端扫描所有允许的通道，并选择信号强度最好的接入点进行连接。

  – 下一个通道 (Next Channel)
    客户端从其允许的通道列表中扫描下一通道。如果存在接入点，则进行连接。
    如果在此通道上未找到接入点，则扫描下一通道。

- **信号质量阈值 (Signal Quality Threshold)**

  只有在将"扫描模式"(Scanning Mode) 设置为"下一个通道"(Next Channel) 时才可组态。

  接入点为客户端指定信号质量。扫描时，客户端必须接收质量至少达到指定信号质量的接入点的信号。只有这样，才会建立连接。

  信号质量由客户端根据所接收数据包的 RSSI 值（接收信号强度指示器）来确定。RSSI 值指示到达的信号的强度，并显示在信号记录器中。

  以下阈值适用于信号强度：

范围	百分比信号质量	RSSI 信号质量
1	40	20
2	50	25
3	60	30
4	70	35
5	80	40

步骤

在接入点模式下

1. 为所需的 WLAN 接口选择"启用 iPCF"(Enable iPCF) 选项。
2. 如有需要，启用选项"Legacy Free (iPCF-LF)"。

3. 从"iPCF 周期时间 [ms]"(iPCF Cycle Time [ms]) 下拉列表中为接入点选择所需的周期时间。
4. 例如，从"扫描模式"(Scanning Mode) 下拉列表中选择"所有通道"(All Channels)。
5. 单击"设置值"(Set Values) 按钮。在"安全 > WLAN > 基本"(Security > WLAN > Basic) 中组态安全设置。

在客户端模式下

1. 为所需的 WLAN 接口选择"启用 iPCF"(Enable iPCF) 选项。
2. 如有需要，启用选项"Legacy Free (iPCF-LF)"。
3. 单击"设置值"(Set Values) 按钮。

在"安全 > WLAN > 基本"(Security > WLAN > Basic) 中组态安全设置。在"安全 > WLAN > 基本"(Security > WLAN > Basic) 中组态安全设置。

6.10.2 iPCF-HT

说明

此 WBM 页面仅可通过以下 KEY-PLUG 组态：

- 接入点：W780 iFeatures (MLFB 6GK5 907-8PA00)
- 客户端：W740 iFeatures (MLFB 6GK5 907-4PA00)

应何时使用 iPCF-HT（大吞吐量）？

说明

iPCF-HT 的使用

iPCF-HT 功能

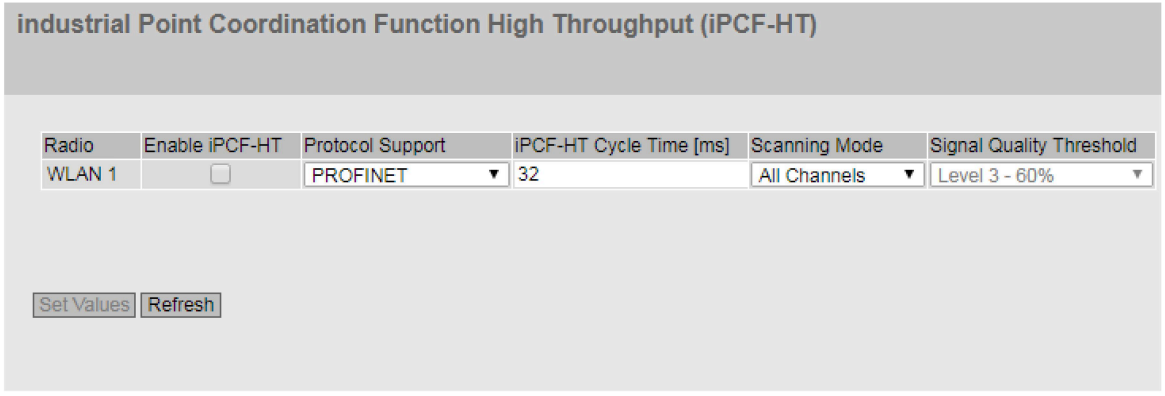
- 和其他 iFeatures（例如，iPCF、iPCF-MC 和 iPRP）互不兼容，无法在设备上同时使用。
- 只能在 5 GHz 频段和"（仅）IEEE 802.11n"WLAN 模式下使用。
- 仅在 WLAN 接口 1 上可用。

建议只使用一个 MCS 索引。

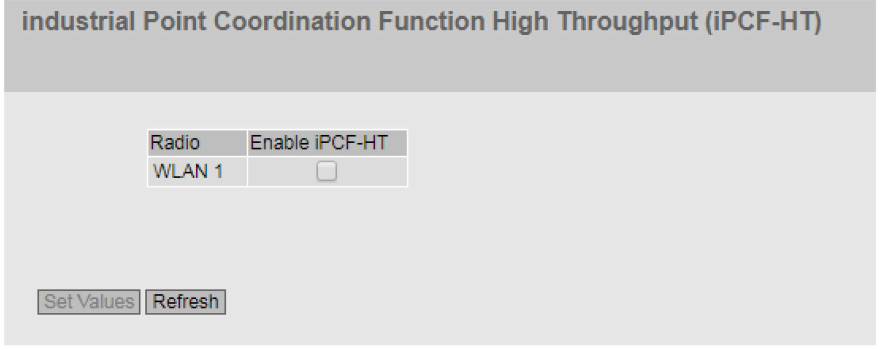
如果需要较高的数据吞吐量，尤其建议使用 iPCF-HT。例如，您可以使用 PROFINET 传输视频数据。PROFINET 的实时性被保留。

接入点和客户端的可能设置有所不同。

Display in access point mode



Display in client mode



描述

在两种模式下，该表都具有以下表列：

- **无线 (Radio)**

  指定设置所关联的 WLAN 接口。

- **启用 iPCF-HT (Enable iPCF-HT)**

  启用或禁用 iPCF-HT。启用后，可调整由接入点提供的数据速率。我们强烈建议保留数据速率的默认设置 (802.11n = MCS 2)。

在接入点模式下，该表具有下列附加列：

- **协议支持 (Protocol Support)**

  指定 WLAN 接口优先处理的协议。

  – PROFINET

    如果设置了 PROFINET，则客户端下游不能有中央 PROFINET 控制器。

  – EtherNet/IP

    如果设置了 EtherNet/IP，则客户端下游不能有扫描器。

  – 禁用

    将禁用该功能。

- **iPCF-HT 周期时间 [ms] (iPCF-HT Cycle Time [ms])**

  指定周期时间。
  设置循环时间时，需考虑以下几点。否则可能无法建立稳定的通信。

  – 值范围是 16 - 512。设置值应对应于 PROFINET 或 EtherNet/IP 的周期时间。

  – 系统中只有一个接入点，也就是说，客户端只在一个无线蜂窝区中移动。在这种情况下，支持大于等于 16 ms 的更新时间。

  – 系统中有多个接入点，可在不同的通道中进行通信。客户端在接入点之间漫游。在此情况下，选择大于等于 32 ms 的更新时间。

  除了以上所示的指导值外，还需记住，要设置的最短周期时间是根据公式"4 ms * 最大节点数"计算得出的。

- **扫描模式 (Scanning mode)**

  所选设置会影响对已登录客户端的扫描。

  可使用以下设置：

  – 所有通道 (All Channels)

    客户端扫描所有允许的通道，并选择信号强度最好的接入点进行连接。

  – 下一个通道 (Next Channel)

    客户端从其允许的通道列表中扫描下一通道。如果存在接入点，则进行连接。

    如果在此通道上未找到接入点，则扫描下一通道。

- **信号质量阈值 (Signal Quality Threshold)**

  只有在将"扫描模式"(Scanning Mode) 设置为"下一个通道"(Next Channel) 时才可组态。

  接入点为客户端指定信号质量。扫描时，客户端必须接收质量至少达到指定信号质量的接入点的信号。只有这样，才会建立连接。

  信号质量由客户端根据所接收数据包的 RSSI 值（接收信号强度指示器）来确定。RSSI 值指示到达的信号的强度，并显示在信号记录器中。

  以下阈值适用于信号强度：

范围	RSSI 信号质量	百分比信号质量
1	20	40
2	25	50
3	30	60
4	35	70
5	40	80

步骤

在接入点模式下

1. 为所需的 WLAN 接口选择"启用 iPCF-HT"(Enable iPCF-HT) 选项。
2. 对"iPCF-HT 周期时间 [ms]"(iPCF-HT Cycle Time [ms]) 输入所需周期时间。

3. 例如，从"扫描模式"(Scanning Mode) 下拉列表中选择"所有通道"(All Channels)。
4. 单击"设置值"(Set Values) 按钮。在"安全 > WLAN > 基本"(Security > WLAN > Basic) 中组态安全设置。

在客户端模式下

1. 为所需的 WLAN 接口选择"启用 iPCF-HT"(Enable iPCF-HT) 选项。
2. 单击"设置值"(Set Values) 按钮。

在"安全 > WLAN > 基本"(Security > WLAN > Basic) 中组态安全设置。

6.10.3 iPCF-MC

说明

iPCF 与其它 iFeatures 配合使用

iPCF-MC 功能和其它 iFeatures（例如，iPCF、iPCF-HT 和 iPRP）互不兼容，无法在设备上同时使用。

接口的分配

使用 11n 设备时，请记住对于 iPCF-MC 的 WLAN 接口分配是固定的。

- WLAN1：数据接口
- WLAN2：管理接口

使用 iPCF-MC 需要满足的要求：

- 接入点至少有两个 WLAN 接口（双 AP）。
- 接入点模式：仅限 KEY-PLUG W780 iFeatures (MLFB 6GK5 907-8PA00) 实现的双 AP
- 客户端模式：KEY-PLUG W740 iFeatures (MLFB 6GK5 907-4PA00) 实现的客户端
- 管理接口和数据接口必须工作在同一频段和模式，并且在无线覆盖方面必须匹配。如果两个无线接口均配备了覆盖不同区域的定向天线，则 iPCF-MC 无法工作。

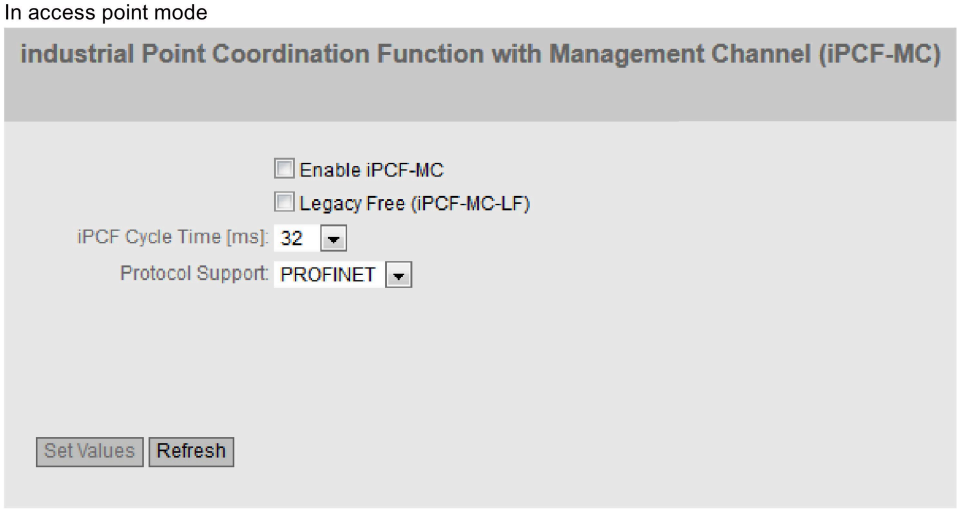
- 客户端可切换到的所有接入点的管理接口必须使用同一通道。客户端仅扫描这一通道，以找到可访问的接入点。
- 基于 IEEE801.11h (DFS) 的传输不能用于管理接口。可将 801.11h (DFS) 用于数据接口。
- 客户端运行时不能启用"仅使用允许的通道"(Use Allowed Channels only)。
- 在第二个接口处会自动镜像"链路中断时强制漫游"(Force roaming on link down)。
- 以下规则适用于客户端：必须将所有已组态和激活的 SSID 分配给安全上下文 1。在"接口 > WLAN > 客户端"(Interfaces > WLAN > Client) 页面上选中相应的"启用"(Enabled) 复选框时，SSID 将处于激活状态。
- 在日本，如果数据或管理接口使用了 4920 MHz - 5080 MH 频段的频率，则无法启用 iPCF-MC。

何时应使用 iPCF-MC？

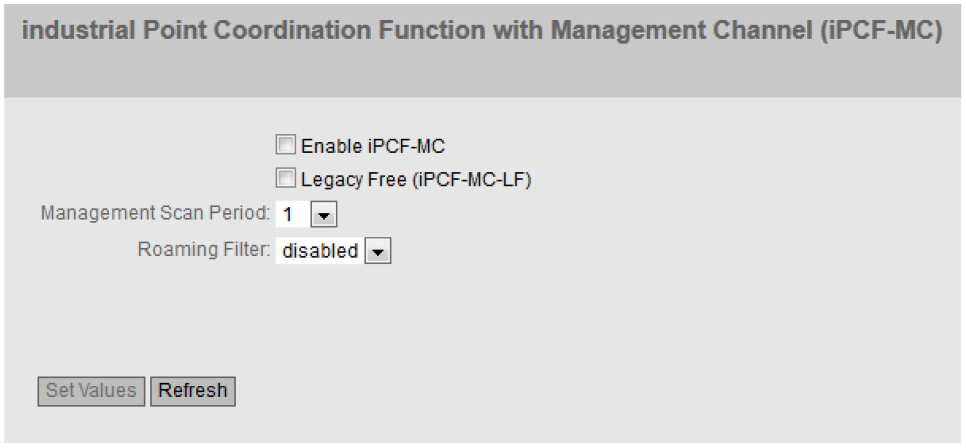
开发 iPCF 的目的是在蜂窝区间漫游时实现较短的切换时间。即便对于自由移动的客户端以及在涉及许多蜂窝区或使用大量通道的情况下，iPCF-MC 技术也可以实现较短的切换时间。

接入点和客户端的可能设置有所不同。下文介绍了这两种模式。

In access point mode



In client mode



描述

该页面包含以下框：

- **启用激活的 iPCF-MC (Enable iPCF-MC activated)**

  启用或禁用 SCALANCE W700 设备的 iPCF-MC 模式。
  对于 PROFINET 通信，建议启用 iPCF-MC 模式。通过启用 iPCF-MC，可调整由接入点提供的数据速率。
  强烈建议保留数据速率的默认设置（802.11 a/b/g = 6、9 和 12 Mbps，802.11n = MCS 2）。

- **Legacy Free (iPCF-MC-LF)**

  此设置确定可以建立与此设备的连接的设备系列。

  – 启用

    仅接受按照 IEEE 802.11n 标准进行通信并启用了"Legacy Free (iPCF-MC-LF)"设置的设备。但无需为此启用 WLAN 模式 IEEE 802.11n。

    此设置可防止 IEEE 802.11 a/b/g 设备系列导致性能降低。

  – 禁用

    接受所有设备系列 (IEEE 802.11 a/b/g/n)。

- **iPCF 周期时间 (iPCF Cycle Time)**（仅限接入点模式）

  选择为接入点所连接的网络组态的 PROFINET 更新时间。更新时间最小值为 32 ms。

- **协议支持 (Protocol Support)**（仅限接入点模式）

  指定优先处理的协议。

  – PROFINET

    如果设置了 PROFINET，则客户端下游不能有中央 PROFINET 控制器。

  – EtherNet/IP

    如果设置了 EtherNet/IP，则客户端下游不能有扫描器。

- **管理扫描周期 (Management Scan Period)**（仅限客户端模式）

  此参数指定两次管理通道扫描之间相隔的时间（以 iPCF 周期指定）。例如，如果选择二，则每两个 iPCF 周期客户端均会运行管理通道扫描。
  较小的扫描间隔值为快速漫游提供了基础，但是这意味着无法实现大数据吞吐量。应选择较大值，以实现大数据吞吐量。

- **漫游过滤器 (Roaming Filter)**（仅限客户端模式）

  通过此设置，可指定用于确定中值的 RSSI 单次测量的数量。如果使用 5，将考虑后 5 个 RSSI 测量值。

  – 测量数目为奇数时的中值

    这些值按升序排列。正中间的值即为中值。

  – 测量数目为偶数时的中值

    这些值按升序排列。中值根据两个中间数的平均值计算而得。

  如果偶尔出现传入信号的极端异常值，可使用此漫游过滤器滤除最严重的波动。这样可避免客户端过早漫游。

6.10.4 iPRP

说明

此 WBM 页面仅可通过以下 KEY-PLUG 组态：

- 接入点：W780 iFeatures (MLFB 6GK5 907-8PA00)
- 客户端：W740 iFeatures (MLFB 6GK5 907-4PA00)

使用 iPRP 的要求

- 设置了基础网桥模式"802.1Q VLAN Bridge"。
- 已创建 VLAN。

- 接入点模式：VAP 接口已启用。
- 客户端模式：
  - 对于"MAC 模式"(MAC Mode)，已设置"第 2 层隧道"(Layer 2 Tunnel)。
  - 对于"后台扫描模式"(Background Scan mode)，已设置"始终"(Always)、"取消激活"(Deactivated) 或"当前通道"(Current channel)。

何时应使用 iPRP？

说明

iPRP 与其他 iFeatures 配合使用

IPRP 和其他 iFeatures（例如，iPCF、iPCF-HT、iPCF-MC）互不兼容，无法在设备上同时使用。

使用超大型帧（巨型帧）的 iPRP

要使用超大型帧，必须为网络中的所有设备组态超大型帧（巨型帧）。

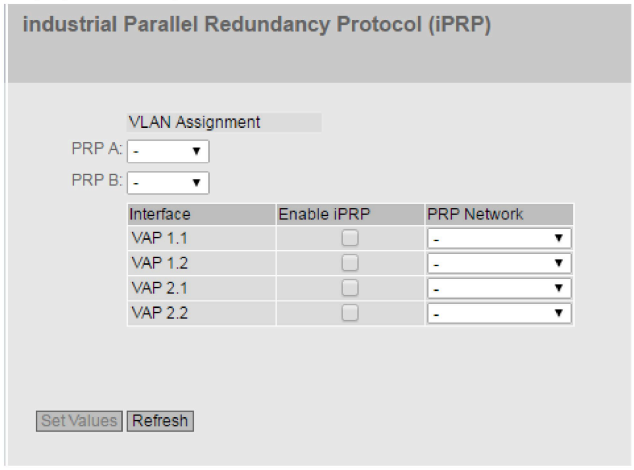
使用 iPRP 代理 VLAN（管理 VLAN）

iPRP VLAN 可用作代理 VLAN。这取决于设备的位置。

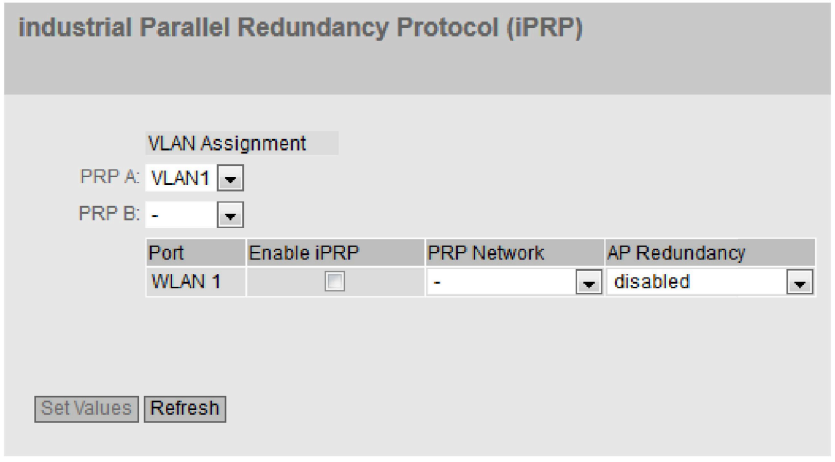
- 如果设备位于 PRP 网络 A 或 PRP 网络 B 中，则使用分配了 PRPA 或 PRPB 的 VLAN 作为代理 VLAN。
- 如果接入点位于两个 PRP 网络中，则可以使用两个 VLAN 之一作为代理 VLAN。您也可以使用其他 VLAN 作为代理 VLAN。PRP 网络 A 和 B 的划分必须保留。如果没有进一步措施，网络 A 和 B 中所有设备的单一管理 VLAN 是不可实现的。

借助"工业并行冗余协议"(iPRP)，可在无线网络中使用 PRP 技术。使用 IPRP 可通过两个无线链路并行传送 PRP 帧。凭借并行传送，当一个无线链路的传送中断时，可由另一个无线链路进行补偿。

Display in access point mode



Display in client mode



描述

该页面包含以下内容：

- **PRP A**

  从下拉列表中选择 PRP 的 VLAN 分配。

- **PRP B**

  从下拉列表中选择 PRP B 的 VLAN 分配。

该表包含以下各列：

- **端口 (Port)**

  显示可用端口。

- **启用 iPRP (Enable iPRP)**

  为所需端口启用或禁用 iPRP。

- **PRP 网络 (PRP Network)**

  指定端口所属的 PRP 网络。

- **AP 无线冗余 (AP Radio Redundancy)（仅限客户端模式）**

  – 无线 (Radio)

    避免在接入点的同一 WLAN 接口上，连接一个客户端对的两个客户端。

  – 禁用 (Disabled)

    当客户端的最佳接入点与伙伴客户端的最佳接入点相同（同一 WLAN 接口）时，检查是否存在其他接入点，其信号强度比最佳接入点的信号强度差 10 dB。在这种情况下，客户端连接到此接入点，否则它将连接到与伙伴客户端相同的最佳接入点。

  – 设备 (Device)

    无论使用哪个接口，都要避免在同一接入点上连接一个客户端对的两个客户端。

步骤

1. 从"PRP A"下拉列表中选择 PRP A 的 VLAN 分配。
2. 从"PRP B"下拉列表中选择 PRP B 的 VLAN 分配。
3. 指定端口所属的 PRP 网络。

4. 对"AP 无线冗余"(AP Radio Redundancy) 进行设置。
5. 选择"启用 iPRP"(Enable iPRP) 设置。单击"设置值"(Set Values) 按钮。

   将自动进行相应的 VLAN 设置。

6.10.5 iREF

说明

- 该 WBM 页面仅在接入点模式下可用。
- 此 WBM 页面仅可通过以下 KEY-PLUG 组态：
  - 接入点：W780 iFeatures (MLFB 6GK5 907-8PA00)

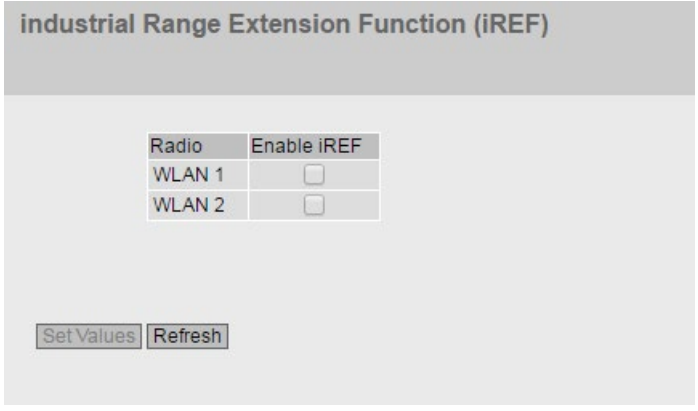
何时应使用 iREF？

说明

iREF 与其它 iFeatures 配合使用

iREF 和其它 iFeatures（例如，iPCF 和 iPCF-HT, iPCF-MC, iPRP）互不兼容，无法在设备上同时使用。

使用 iREF 时，可以最高的发射功率发送数据。特别是对于 MIMO 无法使用或不具任何优势的应用，这使得数据能够以最高可能的数据传输速率传输。



说明

该表包括以下列：

- **无线 (Radio)**

  指定设置所关联的 WLAN 接口。

- **启用 iREF (Enable iREF)**

  启用或禁用所需 WLAN 接口的 iREF。结果在"Information > WLAN >iFeatures"中显示。

说明

要使用 iREF，必须至少有两根天线。
启动 iREF 后，天线将自动切换到 Mode RX/TX。

6.10.6 AeroScout

说明

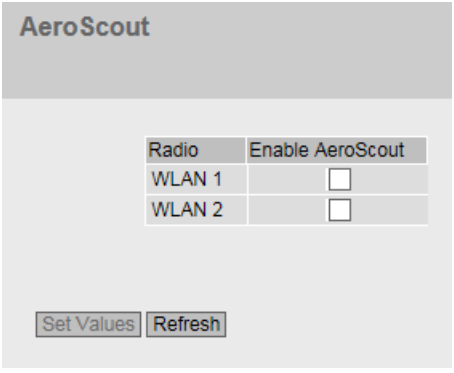
- 该 WBM 页面仅在接入点模式下可用。
- 此 WBM 页面仅可通过以下 KEY-PLUG 组态：
  访问点：W780 iFeatures (MLFB 6GK5 907-8PA00)

说明

使用 Aeroscout

- AeroScout 和其它 iFeatures（例如，iREF, iPCF, iPCF-HT, iPCF-MC, iPRP）互不兼容，无法在设备上同时使用。
- 根据 IEEE 802.11g、IEEE 802.11n 和仅 IEEE 802.11n 标准，AeroScout 仅可在 2.4 GHz 频段使用。

  有关详细信息，请参见 AeroScout 公司 (www.aeroscout.com) 的文档。



说明

该表包括以下列：

- **无线 (Radio)**

  指定设置所关联的 WLAN 接口。

- **启用 AeroScout (Enable AeroScout)**

  启用或禁用所需 WLAN 接口的 AeroScout。结果显示在"信息 > WLAN iFeatures > AeroScout"(Information > WLAN iFeatures > AeroScout) 中。

保养和维护 7

7.1 固件更新 - 通过 WBM

要求

- 设备具有 IP 地址。
- 用户以“管理员”身份进行登录。

说明

设备的固件版本需至少为 5.1。如果设备上的固件版本低于 5.1，则无法进行固件更新。

通过 HTTP 进行固件更新

1. 在导航区域中，单击“系统 > 加载和保存”(System > Load&Save)。单击“HTTP”选项卡。
2. 单击“固件”(Firmware) 表行中的“加载”(Load) 按钮。
3. 转到固件文件的存储位置。
4. 单击对话框中的“打开”(Open) 按钮。上传文件。

固件更新 - 通过 TFTP

1. 在导航区域中，单击“系统 > 加载和保存”(System > Load&Save)。单击“TFTP”选项卡。
2. 在“TFTP 服务器地址”(TFTP Server Address) 输入框中输入 TFTP 服务器的 IP 地址。
3. 在“TFTP 服务器端口”(TFTP Server Port) 输入框中输入 TFTP 服务器的端口。
4. 单击“固件”(Firmware) 表行中的“加载文件”(Load file) 按钮。

5. 转到固件文件的存储位置。
6. 单击对话框中的"打开"(Open) 按钮。上传文件。

通过 SFTP 进行固件更新

1. 在导航区域中，单击"系统 > 加载和保存"(System > Load&Save)。单击"SFTP"选项卡。
2. 在"SFTP 服务器地址"(SFTP Server Address) 输入框中输入 SFTP 服务器的 IP 地址。
3. 在"SFTP 服务器端口"(SFTP Server Port) 输入框中输入 SFTP 服务器的端口。
4. 单击"固件"(Firmware) 表行中的"加载文件"(Load file) 按钮。
5. 转到固件文件的存储位置。
6. 单击对话框中的"打开"(Open) 按钮。上传文件。

结果

固件已完全传送到设备中。

并且在"信息 > 版本"(Information > Versions) 上也存在条目"固件"(Firmware) 和"运行中固件"(Firmware Running)。"运行中固件"(Firmware Running) 显示当前固件的版本。"固件"(Firmware) 显示固件加载后所存储的固件版本。要激活该固件，通过"系统 > 重启"(System > Restart) 重启设备。

7.2 使用 PRESET-PLUG 进行设备组态

请注意设备操作说明中的附加信息和安全说明。

注意
切勿在运行期间插拔 PLUG 只允许在设备关闭后取出或插入 PLUG。

说明

V6.0 及更高版本的支持

V6.0 及更高版本的固件支持 PRESET-PLUG 功能。

借助 PRESET-PLUG，可以在多个设备上安装包含相应固件在内的相同设备组态（启动组态、用户帐户和证书）。

PRESET PLUG 受写保护。

通过命令行接口 (CLI) 组态 PRESET PLUG。

创建 PRESET-PLUG

通过命令行接口 (CLI) 创建 PRESET PLUG。可通过任意 PLUG 创建 PRESET-PLUG。为此，请按照下面列出的步骤进行操作：

说明

通过使用 DHCP 的组态

仅通过使用 DHCP 的设备组态创建 PRESET-PLUG。否则，将会因为存在多个相同的 IP 地址而导致网络中断。
可以在完成基本安装后额外分配固定的 IP 地址。

要求

- 已将 PLUG 插入到您想要对其组态 PRESET-PLUG 功能的设备中。

步骤

1. 使用 Telnet (CLI) 启动远程组态，并以“admin”用户身份登录。
2. 使用“configure terminal”命令切换至全局组态模式。
3. 使用“plug”命令切换至 PLUG 组态模式。

4. 使用“presetplug”命令创建 PRESET-PLUG。
   设备的固件版本以及当前设备组态（其中包括用户帐户和证书）存储在 PLUG 中，PLUG 受写保护。
5. 关闭设备的电源。
6. 拔出 PRESET-PLUG。
7. 启动插有新的 PLUG 或者含内部组态的设备。

借助 PRESET-PLUG 时的安装步骤

1. 关闭设备的电源。
2. 如果存在 PLUG，请将其从插槽中拔出。有关详细信息，请参见设备的操作说明。
3. 按正确的方向将 PRESET-PLUG 插入插槽中。如果 PRESET-PLUG 完全在设备内部并且没有伸出插槽，则表示其已正确插入。
4. 再次接通设备的电源。
   如果待安装设备的固件版本与 PRESET-PLUG 中的固件版本不同，则会执行固件升级/降级操作。可通过红色 F-LED 闪烁来识别（闪烁间隔：2 s 点亮/0.2 s 熄灭）。之后，设备会重新启动，PRESET-PLUG 上的设备组态（包括用户和证书）会被传送到设备。
5. 请等待设备完全启动。
   （红色 F-LED 熄灭）
6. 完成安装后，切断设备电源。

7. 拔出 PRESET-PLUG。
8. 启动插有新的 PLUG 或者含内部组态的设备。

说明

KEY-PLUG

如果通过 KEY-PLUG 创建 PRESET-PLUG，则为了使用该组态，需要插入 KEY-PLUG。在这种情况下，需要插入相关的 KEY-PLUG，然后再对设备进行重新调试。

说明

在插有 PRESET PLUG 的情况下恢复出厂默认设置并重启

如果将设备复位为出厂默认设置，则在设备重启时，插入的 PRESET PLUG 会被格式化，PRESET PLUG 功能将丢失。之后，需要创建新的 PRESET PLUG。KEY-PLUG 上存储的用于实现相关功能的密钥将被保留。

建议您先拔出 PRESET PLUG，然后再将设备复位为出厂默认设置。

格式化 PRESET-PLUG（复位预设功能）

使用命令行接口 (CLI) 格式化 PRESET PLUG，以复位预设功能。为此，请按照下面列出的步骤进行操作：

1. 使用 Telnet (CLI) 启动远程组态，并以“admin”用户身份登录。
2. 使用“configure terminal”命令切换至全局组态模式。
3. 使用“plug”命令切换至 PLUG 组态模式。
4. 输入命令“factoryclean”。
   将格式化 PRESET-PLUG 并复位预设功能。
5. 使用“write”命令写入设备的当前组态。

7.3 在 ConfigPack 中嵌入固件

请注意设备操作说明中的附加信息和安全说明。

借助嵌有固件文件的 ConfigPack，可以在一个或多个设备上安装设备组态及其所含固件。

创建嵌有固件的 ConfigPack

要在 ConfigPack 中嵌入固件，需要在命令行接口 (CLI) 中进行设置。为此，请按照下面列出的步骤进行操作：

说明

通过使用 DHCP 的组态

如果要使用嵌有固件的 ConfigPack 调试多个具备相同组态和固件的设备，则只能通过采用 DHCP 的设备组态创建 ConfigPack。否则，将会因为存在多个相同的 IP 地址而导致网络操作中断。

可以在完成基本安装后额外分配固定的 IP 地址。

---

1. 使用 Telnet (CLI) 启动远程组态，并以“admin”用户身份登录。
2. 使用“configure terminal”命令切换至全局组态模式。
3. 使用命令“loadsave”切换至 loadsave 组态模式。
4. 输入“firmware-in-configpack”命令（无参数）。
   在您保存此设备上的当前固件时，会将其作为单独的文件包含在 ConfigPack 内。

   说明

   在 ConfigPack 中嵌入固件

   设备重启时，该功能会再次丢失，必须重新将其激活。

如果在 WBM 或 CLI 中保存 ConfigPack，则会嵌入固件。

请参见加载和保存 (页 246)部分中的信息。

安装嵌有固件的 ConfigPack

说明

安装使用 DHCP 选项 66 和 67 的 ConfigPack

另外，也可以安装使用已激活选项 66 和 67 的 DHCP 的 ConfigPack。
在菜单"系统 > DHCP > DHCP 客户端"(System > DHCP > DHCP Client) 中激活相关选项。

如果使用 WBM 或 CLI 安装 ConfigPack，则还会安装其中存储的固件。

WBM 中的步骤

1. 以管理员身份连接至您想要在其中安装 ConfigPack 的设备 WBM。
2. 转至菜单"系统 > 加载和保存"(System > Load&Save)。
3. 在"ConfigPack"行中，单击"加载"(Load) 按钮。
4. 选择要安装的 ConfigPack。
5. 通过"系统 > 重启"(System > Restart) 重启设备。
   如果待安装设备的固件版本与 ConfigPack 中的固件版本不同，则会执行固件升级/降级操作。可通过红色 F-LED 闪烁（闪烁间隔；点亮 2 秒/熄灭 0.2 秒）来识别。之后，设备会重新启动，ConfigPack 中存储的设备组态（包括用户和证书）会被传送到设备。
6. 请等待设备完全启动。
   （红色 F-LED 熄灭）
7. 可以重新登录设备或退出 WBM。

7.4 恢复出厂设置

注意
之前的设置 如果执行复位，进行的所有设置将被出厂默认设置覆盖。

注意
意外复位 意外复位会在已组态的网络中产生干扰和故障，从而引发其他后续问题。

使用复位按钮

对该按钮进行按压操作时，请确保遵守操作说明中“复位按钮”部分的信息。

按照以下步骤将设备参数复位为出厂设置：

1. 关闭设备的电源。
2. 拧松盖板上的螺钉。
3. 卸下盖板。
4. 现在按“复位”(Reset) 按钮并按住，同时重新连接设备的电源。
5. 按住按钮，直至约 10 秒后红色故障 LED (F) 停止闪烁并持续点亮。
6. 现在松开按钮并等待至故障 LED (F) 再次熄灭。
7. 随后设备自动使用出厂设置启动。

通过 SINEC PNI

使用 SINEC PNI 将设备参数复位为出厂设置，操作步骤如下：

1. 选择要复位其参数的设备。
2. 单击“复位设备”(Reset device) 按钮。
3. 在以下对话框中选择“复位为出厂设置”(Reset to factory settings) 选项。

通过组态

有关使用 WBM 和 CLI 复位设备参数的详细信息，请参见组态手册：

- 基于 Web 的管理，“重启”部分
- 命令行接口，“复位和默认设置”部分

故障排除/FAQ

8

8.1 不能通过 WBM 或 CLI 进行固件更新

原因

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

对该按钮进行按压操作时，请确保遵守操作说明中“复位按钮”部分的信息。

解决方法

随后还可以使用 TFTP 将固件分配给 SCALANCE W。
按照以下步骤使用 TFTP 加载新固件：

1. 关闭设备的电源。
2. 现在按“复位”(Reset) 按钮并按住，同时重新连接设备的电源。
3. 按住按钮，直至约 2 秒后红色故障 LED (F) 开始闪烁。
4. 现在松开按钮。在此状态下，引导加载程序将等待您可通过 TFTP 下载的新固件文件。
5. 通过以太网接口将 PC 连接到 SCALANCE W。
6. 使用 SINEC PNI 为 SCALANCE W 分配一个 IP 地址。
7. 打开 DOS 框并切换到保存新固件文件的路径，然后执行命令“tftp -i <ip 地址> PUT <固件>”。也可以使用不同的 TFTP 客户端。
8. 关闭盖板，确保设备关闭且防水防尘。

说明

在 Windows 10 中使用 CLI 和 TFTP

如果在 Windows 10 中访问 CLI 或 TFTP，需确保 Windows 10 中已启用相关的功能。

结果

将固件传送到设备。

说明

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

固件完全传送到设备后，设备将自动重启。

8.2 由于接收功率过高而中断数据传输

过高接收功率的原因及影响

如果 SCALANCE W 设备输入端接收的功率过高，则会使放大器电路过载。过载可发生在客户端或接入点上。如果 SCALANCE W 设备上接收的功率大于 -35 dBm，则可能导致通信中断。

在 WBM 中，有关信号强度 [以 dBm 为单位] 的信息显示在以下选项卡中：

接入点模式：

- “信息 > WLAN > 客户端列表”(Information > WLAN > Client List)

客户端模式：

- “信息 > WLAN > 可用 AP”(Information > WLAN > Available AP)
- “接口 > WLAN > 信号记录器”(Interfaces > WLAN > Signal recorder)

SCALANCE W 设备输入信号的功率受以下因素影响：

- WLAN 伙伴之间的距离
- 部分建筑物的电磁波反射
- “最大发射功率”(max. Tx Power)（发射功率）的设置（“接口 > WLAN > 基本”(Interfaces > WLAN > Basic)）以及所使用的天线设置（“接口 > WLAN > 天线”(Interfaces > WLAN > Antennas)）。

解决方法

如果通信由于信号强度过高（大于 -35 dBm）而中断，可以通过以下方式消除问题：

- 增加发送器和接收器之间的距离。
- 通过在 WBM 或 CLI 中的适当设置降低 IWLAN 伙伴的发射功率。

8.3 与旧产品的兼容性

混合模式

可与旧产品 (6GK57xx-xAA60-xAx0) 混合工作。

有关旧产品的更多信息，请通过 Internet 访问 SIEMENS 工业自动化与驱动产品部门的服务与支持中心，并输入 ID：42784493 (https://support.industry.siemens.com/cs/ww/zh/view/42784493)

为能够混合使用，请注意以下几点：

- 传输标准 IEEE 802.11a/b/g/n
  传输标准 IEEE 802.11a/b/g/n 与旧产品兼容。“802.11n only”设置与旧产品不兼容。不支持旧产品的传输标准 IEEE 802.11a/g/h Turbo。
- 安全设置
  传输标准 IEEE 802.11a/b/g 支持与旧产品相同的安全设置。
  采用“802.11n”或“802.11n only”设置的传输标准 IEEE 802.11n 仅支持采用 AES 安全设置的 WPA2/WPA2-PSK。
- SSID
  对于 SSID，请仅使用以前产品支持的字符。
- Management only over wired Ethernet interface
  以前的产品具有“Management only over wired Ethernet interface”功能。在新设备中，此功能被“管理 ACL”功能覆盖。

- iPCF/iPCF-MC

  不支持将 IEEE 802.11b 传输方法与 iPCF 配合使用。

  混合使用时，不能采用 IEEE 802.11b 运行模式组态 SCALANCE W700-xRR 设备。

- WDS ID

  使用 WDS ID 时，请勿使用 ASCII 字符 0x22 (")。

- WEP 或 AES 密钥

  对于最高固件版本为 3.2 的设备，WEP 或 AES 密钥只可包含 ASCII 字符或十六进制字符 0x20 至 0x7E。

- WPA(2)-PSK 密钥

  对于最高固件版本为 5.0 的设备，WPA(2)-PSK 密钥只可包含 ASCII 字符十六进制字符 0x20 至 0x7E。

  对于固件版本为 5.1 或更高的设备，以下规范适用于 WPA(2)-PSK 密钥：

  – 对于包含 8 到 63 个字符的密钥，只能使用以下可读的 ASCII 字符:0x20 - 0x7e。

  – 对于恰好包含 64 个字符的密钥，可以使用以下 ASCII 字符：0 - 9、 a - f 和 A - F。

8.4 安全网络设计的说明

为保护网络免受攻击，请注意以下信息：

- **使用基于 HTTPS 的安全连接**

  与 HTTP 不同的是，HTTPS 可实现在通过“基于 Web 的管理”组态 WLAN 客户端和接入点时的安全访问。有关更多详细信息，请参见“加载和保存 (页 246)”部分。

- **使用具有 AES 的 WPA2/WPA2-PSK**

  仅使用 WPA2/AES 来防止密码滥用。带 AES 的 WPA2/WPA2-PSK 可提供最大的安全性。有关更多详细信息，请参见“Basic（接入点） (页 477)”部分。

- **保护网络免受中间人攻击**

  要保护网络免受中间人攻击，建议使用令攻击者更难访问两个终端设备之间通信路径的网络设置。

  – 例如，可将代理 IP 设置为仅可通过单一管理 VLAN 访问，从而保护设备。有关更多详细信息，请参见"Agent IPv4 (页 231)"部分。

  – 此外还可以选择在 WLAN 客户端/接入点上安装单独的 HTTPS 证书。HTTPS 证书会检查设备的身份并控制加密数据交换。可以通过 HTTP 安装 HTTPS 证书。有关更多详细信息，请参见"HTTP (页 253)"部分。

- **使用 SNMPv3**

  通过 SNMP 访问设备时，SNMPv3 可提供可能实现的最高安全等级。有关更多详细信息，请参见"SNMP (页 289)"部分。

注意
使用 STEP 7 组态后更改默认密码 如果仅使用 STEP 7 组态处于默认状态的设备，则无法更改默认密码。 必须使用 WBM 或 CLI 直接在设备上更改密码。 否则，将保留默认密码，而且任何用户都能使用默认密码登录。

8.5 WLAN 客户端通过 SNMP 触发切换

如果漫游阈值、后台扫描阈值等其它切换机制不合适，则可以通过设置 MIB 变量 snMspsWlanForceHandover 来触发特定切换。

例如，WLAN 客户端沿存在多个接入点的延伸进行驱动。当 WLAN 客户端通过某一特定点时，MIB 变量的值从 0 变为 1。WLAN 客户端从连接的接入点注销，并搜索可访问的接入点。它会登录到最佳可访问接入点。MIB 变量的值复位为 0。

触发切换

使用专有 MIB 变量 snMspsWlanForceHandover 可强制切换。

说明

使用基于 Web 的管理 (WBM) 或命令行接口 (CLI) 无法组态此功能。

专有 MIB 变量 snMspsWlanForceHandover 的 OID：

```
iso(1).org(3).dod(6).internet(1).private(4).enterprises(1).siemens(4329).industrialComProducts(20).iComPlatforms(1).simaticNet(1).snMsps(1).snMspsCommon(1).snMspsWlan(27).snMspsWlanObjects(1). snMspsWlanSmt(1). snMspsWlanRoamingConfigTable(4). snMspsWlanRoamingConfigEntry(1). snMspsWlanForceHandover(14)
```

MIB 变量的值

- 0：功能已禁用。
- 1：触发切换。

MIB 文件

MIB 变量 snMspsWlanForceHandover 可在专有 MIB 文件“Scalance_w_msps.mib”中找到。

8.6 使用 TIA Portal 组态设备

插入网络组件后，即可离线编辑属性和参数，例如设备名称。离线即表示与设备之间无连接。

为了查看设备的更改，必须先编译更改然后再将其加载到设备上。

可以采用以下两种方式启动编译和加载：

- 使用快捷菜单“下载至设备 > 硬件配置”(Download to device > Hardware configuration)
- 使用工具栏中的“下载”(Download) 按钮。

要求

- 已在项目中创建了网络组件。
- 网络组件的硬件配置与设备的硬件配置相匹配。否则会出错，进而导致下载操作中止。
- 网络组件的固件版本与设备的固件版本相匹配。
- 已设置 IP 地址。
- 设备已连接至组态 PC。
- 已组态所需属性和参数。

说明

激活 SINEMA 组态接口

如果已启用了 WBM 菜单“系统 > 组态”(System > Configuration) 中的“SINEMA 组态接口”(SINEMA configuration interface)，则只能使用 TIA Portal 组态设备。

将属性和参数下载至设备

要将更改属性和参数下载至设备，请按以下步骤操作：

1. 在项目树中选择所需网络组件。
2. 在网络组件的快捷菜单中，选择命令“下载至设备 > 硬件配置”(Download to device > Hardware configuration)。

3. “扩展下载到设备”(Extended download to device) 对话框打开后，组态“下载设置”(Settings for the download)。
   - 选择您使用的协议，例如 HTTPS。
   - 在组态 PC 上组态相关的接口参数。必要时，在操作员面板上进行接口或协议特定的设置。单击“开始搜索”(Start search)

     网络组件及其检测到的 IP 地址会显示在“目标子网中的兼容设备”(Compatible devices in target subnet) 表中。
   - 选择表中的地址条目，然后单击“加载”(Load) 按钮。
4. “加载预览”(Load preview) 对话框随即打开。同时会编译硬件配置。此对话框会显示相关消息和加载所需的修改建议（例如，需要密码）。

   检查消息，必要时启用“操作”(Action) 列中的操作。

   一旦可以进行加载，该按钮就会变为激活状态。
5. 单击“加载”(Load) 按钮。

   执行加载操作，并会显示“加载结果”(Load results) 对话框。
6. 如果加载操作成功完成，请选择“操作”(Action) 中的“保存组态”(Save configuration)。
7. 单击“完成”(Finish) 按钮。

结果

成功加载后，即可在网络组件上运行项目。

更新网络组件的 SCALANCE 组态

要更新网络组件的 SCALANCE 组态，请按以下步骤操作：

1. 打开“设备和网络”(Devices & Networks) 编辑器，然后设置网络视图。
2. 在网络视图中选择网络组件。
3. 在网络组件的快捷菜单中，选择命令“SCALANCE 组态 > 上传至 PG/PC”(SCALANCE configuration > Upload to PG/PC)。

结果

与设备建立连接后，系统会提示您登录设备。如果登录成功，则会将 SCALANCE 组态从设备加载至 TIA Portal。之后，会在 TIA Portal 中更新属性和参数。

8.6.1 消息：尚未接受 SINEMA 组态

当显示区域中显示以下消息时，说明在将组态从 STEP 7 Basic / Professional（自版本 V13 起）传送到设备的过程中发生了错误：

“尚未接受 SINEMA 组态。重启设备后，所有组态更改都将丢失”(SINEMA Configuration not accepted yet. With restart of device, all configuration changes will be lost.)

其中一个可能原因是，设备在传输期间无法访问。

如果现在直接更改设备 (WBM/CLI/SNMP) 上的参数，这些更改将在设备重启时丢失。

解决方法

1. 在 STEP 7 Basic / Professional 中打开相关的 STEP 7 项目
2. 打开项目视图。
3. 在项目树中选择设备。
4. 在快捷菜单中选择“转到网络视图”(Go to network view) 命令。
5. 在网络视图中选择设备。
6. 在所选设备的快捷菜单中，选择命令“SCALANCE 组态 > 另存为启动组态”(SCALANCE configuration > Save as start configuration)。

结果

组态保存在设备上。显示区域中不再显示该消息。直接在设备上进行的组态更改不再因设备重启而丢失。

附录 A“支持的 MIB 模块” A

A.1 SCALANCE W 设备支持的 MIB 文件

适用于 SCALANCE W 设备的 MIB 文件

下表显示了适用于 SCALANCE W 设备的 MIB 文件：

MIB	根 OID	参考
AUTOMATION SNTP (Siemens) [1) 2)]	.1.3.6.1.4.1.4329.6.3.11	供应商特定
AUTOMATION SYSTEM MIB (Siemens) [1) 2)]	.1.3.6.1.4.1.4329.6.3.2	供应商特定
AUTOMATION TELNET (Siemens) [1) 2)]	.1.3.6.1.4.1.4329.6.3.8	供应商特定
AUTOMATION TIME MIB (Siemens) [1) 2)]	.1.3.6.1.4.1.4329.6.3.3	供应商特定
BRIDGE MIB	.1.3.6.1.2.1.17	RFC1493
ENTITY-MIB	.1.3.6.1.2.1.47	
EtherLike-MIB	.1.3.6.1.2.1.10.7.2	
IANA-MAU-MIB	.1.3.6.1.2.1.26.1.1	
IEEE8021-PAE-MIB	.1.0.8802.1.1.1	IEEE 802.1X
IEEE802dot11-MIB	.1.2.840.10036	IEEE 802.11
IF-MIB:	.1.3.6.1.2.1.2	RFC2233
P-BRIDGE-MIB	.1.3.6.1.2.1.17.4.5	
Q-BRIDGE-MIB	.1.3.6.1.2.1.17.7	
RADIUS-ACC-CLIENT-MIB	.1.3.6.1.2.1.67.2.2	
RADIUS-AUTH-CLIENT-MIB	.1.3.6.1.2.1.67.1.2	
RFC1213-MIB	.1.3.6.1.2.1.4	
RMON-MIB	.1.3.6.1.2.1.16	
SNMP-COMMUNITY-MIB	.1.3.6.1.6.3.18	
SNMP-FRAMEWORK-MIB	.1.3.6.1.6.3.10.2.1	RFC2571
SNMP NOTIFICATION MIB	.1.3.6.1.6.3.13	RFC2573

MIB	根 OID	参考
SNMP PROXY MIB	.1.3.6.1.6.3.14	
SNMP-TARGET-MIB	.1.3.6.1.6.3.12	RFC2573
SNMP USER-BASED SM MIB	.1.3.6.1.6.3.15	RFC2574
SNMPv2-MIB	.1.3.6.1.2.1.1	RFC1907
SNMP VIEW-BASED ACM MIB	.1.3.6.1.6.3.16	RFC2575
SN-MSPS-ACL-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.30	供应商特定
SN-MSPS-CONFIG-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.1	供应商特定
SN-MSPS-CPLUG-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.23	供应商特定
SN-MSPS-DHCP-CLIENT-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.17 .1	供应商特定
SN-MSPS-DIGITAL-IO-MIB (Siemens) 2)3)	.1.3.6.1.4.1.4329.20.1.1.1.1.39	供应商特定
SN-MSPS-GENERAL-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.2	供应商特定
SN-MSPS-HTTP-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.20	供应商特定
SN-MSPS-IF-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.34	供应商特定
SN-MSPS-IP-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.13	供应商特定
SN-MSPS-KEY-PLUG-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.35	供应商特定
SN-MSPS-LOAD-SAVE-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.26	供应商特定
SN-MSPS-LOG-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.31	供应商特定
SN-MSPS-MSTP-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.6	供应商特定
SN-MSPS-NTP-MIB (Siemens)	.1.3.6.1.4.1.4329.20.1.1.1.1.33	供应商特定
SN-MSPS-PNAC-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.10	供应商特定
SN-MSPS-PORT-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.29	供应商特定
SN-MSPS-RADIUS-SERVER-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.11 .2	供应商特定
SN-MSPS-REPORT-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.28	供应商特定
SN-MSPS-RMON-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.12	供应商特定
SN-MSPS-SINEMA-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.25	供应商特定
SN-MSPS-SNMP-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.4	供应商特定
SN-MSPS-SNTP-CLIENT-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.1.19 .1	供应商特定

MIB	根 OID	参考
SN-MSPS-STP-L2T-MIB (Siemens)	.1.3.6.1.4.1.4329.20.1.1.1.40	供应商特定
SN-MSPS-SYSLOG-CLIENT-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.21.1	供应商特定
SN-MSPS-VLAN-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.3	供应商特定
SN-MSPS-WLAN-MIB (Siemens) 2)	.1.3.6.1.4.1.4329.20.1.1.1.27	供应商特定
SN-MSPS-NAT-MIB	1.3.6.1.4.1.4329.20.1.1.1.45	供应商特定
TCP-MIB	.1.3.6.1.2.1.6	
UDP-MIB	.1.3.6.1.2.1.7	

1) AUTOMATION.MIB 的一部分

可从 SIEMENS 工业自动化与驱动产品部门的服务与支持中心下载 SCALANCE W700 的"AUTOMATION.MIB"，位置在条目 ID 67637278 (https://support.industry.siemens.com/cs/ww/zh/view/67637278) 下

2) 专有 MIB 文件"Scalance_w_msps.mib"的一部分。该文件可在 WBM 中使用"系统 > 加载和保存 > HTTP > MIB"(System > Load&Save > HTTP > MIB) 和"保存"(Save) 按钮进行下载。

3) 无数据输入/输出的设备不支持此 MIB。

附录 B“专有 MIB” B

B.1 SCALANCE W 设备的专有 MIB 变量

通过 WBM 下载 SCALANCE W 的 MIB

SCALANCE W 的 MIB 可在 WBM 的“系统 > 加载和保存 > HTTP > MIB”(System > Load&Save > HTTP > MIB) 下使用“保存”(Save) 按钮下载。

OID

SCALANCE W 的专有 MIB 变量具有以下对象标识符：

```
iso(1).org(3).dod(6).internet(1).private(4). enterprises(1)
siemens(4329) industrialComProducts(20) iComPlatforms(1)
simaticNet(1) snMsps(1) snMspsCommon(1)
```

WLAN 特定的 MIB 变量

WLAN 特定的 MIB 变量可在“snMspsWlan”中找到。您将在 MIB 文件中找到有关设置和值的更多信息。

附录 C“基本标准”

C

C.1 基本标准

SCALANCE W700 设备完全或部分符合的标准

下表列出了 SCALANCE W700 设备的一些标准。

标准名称	主题
IEEE 802.1AB	链路层发现协议 (LLDP)
IEEE 802.1D-1998	介质访问控制 (MAC)，网桥
IEEE 802.1Q	虚拟桥接 LAN（VLAN 标记，基于端口的 VLAN）
IEEE 802.1W-2004	快速生成树协议 (RSTP)
IEEE 802.1X	基于端口的网络访问控制
IEEE 802.3-2002	以太网
IEEE 802.3af	以太网供电 (PoE)
IEEE 802.11	无线局域网
IEEE 802.11a	5 GHz 频段的无线使用标准
IEEE 802.11at	PoE +
IEEE 802.11b/g	2.4 GHz 频段的无线使用标准
IEEE 802.11e	服务质量 (QoS)
IEEE 802.11 h	覆盖半径扩展和发射功率，用于欧洲 5 GHz 频率范围。
IEEE 802.11i	WLANS 的加密
IEEE 802.11n	高传输速率的标准

附录 D“日志消息”

D

D.1 事件日志中的消息

系统启动期间的消息（常规）

报警	说明
已执行热启动，版本：V02.00.00 - 启动后的事件/状态摘要	启动类型和加载的固件版本。
电源： • L1 已连接 • L2 未连接	电源线路 1 和 2 的状态。
未监视任何线路	来自信号系统的电源监视信息。
MSTP 已禁用。 MSTP 已启用。	生成树协议的状态信息。
启动后无未决故障状态	系统启动后的故障状态。

电源状态

在“系统 > 事件”(System > Events) 中启用或禁用“电源变化”(Power Change) 事件。

报警	说明
线路 1/2/PoE 通电。	线路 1、线路 2 或 PoE 存在电力供应。
线路 1/2/PoE 断电。	线路 1、线路 2 或 PoE 上电力供应中断。

以太网接口的状态

在"系统 > 事件"(System > Events) 中启用或禁用"链路变化"(Link Change) 事件。

报警	说明
P1 链路接通	以太网接口上存在连接。
P1 链路中断。	以太网接口上不存在连接。

WLAN 接口的状态（仅限接入点模式）

消息	
VAP X.Y 链路接通。	启用了 WLAN 接口 X 上的 VAP 接口 Y。
VAP X.Y 链路中断。	禁用了 WLAN 接口 X 上的 VAP 接口 Y。
WLAN X 上的 WDS Y 接通。	WLAN 接口 X 上的 WDS 接口 Y 存在连接。
WLAN X 上的 WDS Y 中断。	WLAN 接口 X 上的 WDS 接口 Y 不存在连接。
WLAN X 上发现重叠 AP：通道 <通道编号> <RSSI 值> 上发现 AP <系统名称> <MAC>	在为 WLAN 接口 X 设置的通道上或相邻通道上检测到另一个接入点。
WLAN X 上重叠 AP 老化：通道 <通道编号> <RSSI 值> 上的 AP <系统名称> <MAC>	组态的老化时间内未检测到重叠的接入点，将其从"重叠 AP"列表中删除。
DFS：在 WLAN X 上的通道 <通道编号>（频率 <频率> MHz）中检测到雷达干扰。切换到通道 <通道号>（频率 <频率> MHz）	在为 WLAN 接口 X 设置的通道上或相邻通道上检测到主要用户（例如，雷达或气象站）。该通道将被阻断 30 分钟。接入点切换到组态的备用通道或切换到下一个没有主要用户的空闲通道。
DFS：通道 <通道编号>（频率 <频率> MHz）在 WLAN X 的 NOL 中老化，可再次使用。	通道上再也检测不到主要用户。该通道已从阻断通道列表中删除，并可再次使用
DFS：WLAN X 的通道 <通道号>（频率 <频率> MHz）中检测到雷达干扰。无空闲通道可用！！	在所有的可用通道中都发现了主要用户。没有可用的空闲通道，在有可用的通道前 WLAN 接口 X 将被取消激活。

WLAN 接口的状态（仅限客户端模式）

消息	说明
WLAN X 链路接通。	启用了 WLAN 接口 X。
WLAN X 链路中断。	禁用了 WLAN 接口 X。

有关组态的消息

消息	说明
WBM：验证失败。	通过"基于 Web 的管理"(WBM) 登录时，输入的密码不正确。可在"系统 -> 事件"(System -> Events) 中启用或禁用该事件（验证失败）。
Telnet：验证失败。	通过 Telnet 登录时，输入的密码不正确。可在"系统 -> 事件"(System -> Events) 中启用或禁用该事件（验证失败）。
请求重启	应用户请求重启。可在"系统 -> 事件"(System -> Events) 中启用或禁用该事件（冷/热启动）。

关于文件上传或下载的消息

消息	说明
通过 HTTP(S) 上传文件：文件类型 <文件类型> 加载成功 → 需要重启	通过 HTTP(S) 成功地加载了文件。需要重启。
通过 HTTP(S) 上传文件：文件类型 <文件类型> 加载成功	通过 HTTP(S) 成功地加载了文件。
通过 HTTP(S) 上传文件：文件类型 <文件类型> 经验证完全相同	通过 HTTP(S) 成功地加载了文件。该文件与现有文件完全相同。
通过 HTTP(S) 上传文件：文件类型 <文件类型> 验证失败	通过 HTTP(S) 加载文件失败。该文件包含错误或无效。
通过 TFTP 上传文件：文件类型 <文件类型> 加载成功 → 需要重启	通过 TFTP 成功地加载了文件。需要重启。
通过 TFTP 上传文件：文件类型 <文件类型> 加载成功	通过 TFTP 成功地加载了文件。

消息	说明
通过 TFTP 上传文件：文件类型 <文件类型> 经验证完全相同	通过 TFTP 成功地加载了文件。该文件与现有文件完全相同。
通过 TFTP 上传文件：文件类型 <文件类型> 验证失败	通过 TFTP 加载文件失败。该文件包含错误或无效。
通过 TFTP 上传文件：文件类型 <文件类型> 的文件传送失败	通过 TFTP 加载文件失败。文件名不正确，或者服务器上不存在该文件。
通过 TFTP 上传文件：文件类型 <文件类型> 的文件传送失败。无法连接到给定 IP 地址	通过 TFTP 加载文件失败。无法访问 TFTP 服务器或设置不正确。
通过 TFTP 下载文件：文件类型 <文件类型> 的文件传送失败。无法连接到给定 IP 地址	通过 TFTP 保存文件失败。无法访问 TFTP 服务器或设置不正确。

有关错误状态的消息

消息	说明
	在"系统 > 事件"(System > Events) 中组态事件。 在"系统 > 故障监视"(System > Fault Monitoring) 中组态电源监视和以太网端口上的链接。
新故障状态：<故障描述> <故障描述>："已执行热启动。""已执行冷启动。""P1 链路中断。""P1 链路接通。""线路 L1 (L2) 断电""DFS：WLAN2 上无可用通道"	传入故障。 不是所有事件都会自动引起故障。在"Events"WBM 页面中，可指定要记录的事件，例如设备重启、以太网端口上的链路变化。
故障状态消失：<故障描述> <故障描述>："已执行热启动。""已执行冷启动。""P1 链路中断。""P1 链路接通。""线路 L1 (L2) 断电""DFS：WLAN2 上无可用通道""未接受 C-PLUG"。详情请参见系统 C-PLUG 屏蔽。"	传出故障
新故障状态（重新组态）：<故障描述> <故障描述>："P1 链路中断。""P1 链路接通。""线路 L1 (L2) 断电"	传入故障。 组态中发生变化会触发该事件。

消息	说明
故障状态消失（重新组态）：<故障描述> <故障描述>："P1 链路中断。""P1 链路接通。""线路 L1 (L2) 断电"	传出故障。 组态中发生变化会触发该事件。
故障状态：<故障描述> 已清除。 <故障描述>："已执行热启动""已执行冷启动"。	用户确认了故障。

有关 MSTP 的消息

消息	说明
	在"系统 > 事件"(System > Events) 中启用或禁用"生成树"(Spanning Tree) 事件
生成树：检测到拓扑变化。	更改了网络拓扑；将重组网络。
生成树：检测到新的根网桥 xx:xx:xx:xx:xx:xx。	更改了网络拓扑；网络中存在一个 MAC 地址为 xx:xx:xx:xx:xx:xx 的新根网桥。

有关安全的消息

消息	说明
RADIUS：接受/拒绝客户端 <MAC> 的访问。	客户端验证已成功或未成功。

有关消息系统的消息

消息	说明
无法访问 Syslog 服务器！	无法访问组态的 Syslog 服务器。
无法将消息发送至 syslog 服务器。请检查 syslog 套接字配置。	Syslog 服务器组态不完整。
由于 IP 连接故障，无法发送电子邮件。	发送电子邮件失败。无法访问 SMTP 服务器（例如，网络连接已中断）。
由于 SMTP 验证失败，无法发送电子邮件。	发送电子邮件失败。SMTP 服务器上的客户端验证出错。

消息	说明
由于 SMTP 消息传送失败，无法发送电子邮件。	发送电子邮件失败。SMTP 服务器可访问，但组态不完整或包含错误（例如，收件人电子邮件地址错误/不存在）。
SNMP：验证失败。	SNMP 客户端验证失败；无法访问（例如，将 SNMPv1/v2 组态为只读，或"读取团体字符串"组态不正确）。
可进行 IP 通信。激活远程登录。	可进行 IP 通信。激活了远程记录。
无法进行 IP 通信。取消激活远程记录。请检查 IP 组态和网络连接。	无法进行 IP 通信。远程记录已取消激活。检查设备是否具有 IP 地址。

系统启动期间的消息（PLUG）

报警	说明
启动组态：内部存储 PLUG：不存在	未插入 PLUG。
启动组态：内部存储 PLUG：丢失 PLUG：许可证丢失	未插入 PLUG。设备上组态了需要许可证 (KEY-PLUG) 的功能。
启动组态：内部存储 PLUG：组态未接受 PLUG：许可证丢失	插入的 PLUG 上的组态无效或不兼容。 设备上组态了需要许可证 (KEY-PLUG) 的功能。
启动组态：内部存储 PLUG：出场清空设置 → 使用内部组态填充 PLUG：组态已接受 PLUG：接受许可证	内部组态成功写入空白 KEY-PLUG。
启动组态：内部存储： PLUG：出场清空设置 → 使用内部组态填充 PLUG：接受组态	内部组态成功写入空白 C-PLUG。
启动组态：PLUG 存储 PLUG：组态已接受 PLUG：接受许可证	从 KEY-PLUG 成功加载了组态。
启动组态：PLUG 存储 PLUG：接受组态	从 C-PLUG 成功加载了组态。

有关 PLUG 的消息

消息	说明
找到空 PLUG。	设备中存在一个空的或已格式化的 PLUG。
PLUG：找到有内容的 PLUG。 PLUG：接受组态	设备中存在一个包含有效组态的有效 PLUG。
PLUG：在运行期间被拔出。	在运行期间删除 C-PLUG/KEY-PLUG。
接受 PLUG	接受了 PLUG。

有关数字量输入/输出的消息

消息	说明
开启/关闭数字量输出。	开启或关闭了数字量输出（与设备相关）。
数字量输入的值为 0/1。	对数字量输入应用了低信号或高信号。

D.2 WLAN 验证日志中的消息

接入点模式下的消息

报警	说明
客户端 <MAC 地址> <系统名称> 连接成功。	客户端已成功在接入点上登录。
客户端 <MAC 地址> <系统名称> 因 <原因描述> 断开连接	客户端已从接入点注销。
VAP<Num>：客户端 <MAC> 连接失败；状态（<文本>）	未能成功连接客户端与 VAP。以文本的形式显示原因。
VAP<Num>：客户端 <MAC> 因（<文本>）而断开连接	成功断开客户端与 VAP 的连接。以文本的形式显示原因。
VAP<Num>：客户端 <MAC> 因（<文本>）而取消验证	客户端已从 AP 注销。以文本的形式显示原因。
VAP<编号> 客户端 <MAC> 验证失败；状态（<状态>）	客户端验证失败。以文本的形式显示原因。

报警	说明
VAP<Num>：客户端 <MAC> 未能成功断开连接；状态（<文本>）	无法终止客户端的连接。以文本的形式显示原因。
VAP<Num>：客户端 <MAC> 已成功连接	客户端已成功连接至 VAP，或客户端已成功登录至 VAP。
RADIUS：拒绝客户端 <MAC> 的访问	RADIUS 服务器拒绝该客户端访问。
RADIUS：接受客户端 <MAC> 的访问	RADIUS 服务器允许该客户端访问。
已建立到 AP <MAC> 的 WDS 连接	已成功建立到接入点的 WDS 连接。
WDS 断开与 AP <MAC> 的连接	已终止到接入点的 WDS 连接。

客户端模式下的消息

报警	说明
在通道 <通道编号>（频率 <频率> MHz）成功连接到 AP <MAC 地址> <系统名称>	客户端已成功在接入点上登录。
因故断开与 AP <MAC 地址> <'系统名称'> 的连接（由于发送 STA 正离开（或已离开）BSS，断开连接）	客户端已从接入点注销。
AP <MAC> 验证失败；状态（<文本>）	与接入点相连的客户端的验证失败。以文本的形式显示原因。
未能断开与 AP <MAC> 的连接；状态（<文本>）	无法终止客户端到接入点的连接。以文本的形式显示原因。
未能连接到 AP <MAC>；状态（<文本>）	客户端到接入点的连接失败。以文本的形式显示原因。

附录 E“Syslog 消息”

E

E.1 Syslog 消息的格式

设备按照 RFC 5424 生成的 Syslog 消息（UDP 默认端口 514）包含以下框。

HEADER

- TIMESTAMP（符合 RFC 3339）
- 主机名称
- APPNAME、PROCID 和 MSGID：如果没有已知信息，则输出“-”字符。

PRIORITY

PRIORITY 包含 Syslog 消息的编码优先级，分别填入“严重程度”(Severity) 和“设施”(Facility) 框中。

- 设施 (Facility)
- 严重程度 (Severity)

VERSION

- 设置为 1。

HOSTNAME_CONTENT：

- IPv4 地址（符合 RFC1035）：每个字节由一个十进制数表示，并且用点与前一个字节隔开。XXX.XXX.XXX.XXX
- IPv6 地址（符合 RFC4291 第 2.2 部分）

STRUCTURED DATA

- timeQuality 块

MESSAGE：

- 英文 ASCII 字符串

说明

更多关于框含义的信息，请参见 RFC 5424。

E.2 Syslog 消息中的参数

Syslog 消息可包含以下参数：

参数	说明	可能值或示例
ip address	IPv4 或 IPv6 地址	IP 地址（符合 RFC1035 或 RFC4291 第 2.2 部分）
src port dest port	显示为十进制数的端口。 格式：%d	0 ... 65535
client mac dest mac src mac	MAC 地址 格式：%02x:%02x:%02x;%02x:%02x:%02x	00:0C:29:2F:09:B3
protocol	生成此事件的服务的名称或使用的第 4 层协议的名称。 格式：%s	可能的条目： UDP | TCP | WBM | Telnet | SSH | Console | TFTP | SFTP
group	用于根据名称标识组的字符串 格式：%s	it-service
user name	根据他/她的姓名识别经验证的用户的字符串 （无空格） 格式：%s	maier
action user name	根据他/她的名称识别用户。此用户不是经验证的用户。 格式：%s	Peter.Maier

参数	说明	可能值或示例
role	组角色的符号名 格式：%s	管理员
time minute timeout	分钟数 格式：%d	44
time second	秒数 格式：%d	44
failed login count	登录失败次数 格式：%d	10
max sessions	会话数目 格式：%d	10
vap	虚拟接入点接口的符号名 格式：(%s) 或 (%s %s)	VAP1.1
status reason	以可读字符串形式显示的更多状态信息。可包含多个字。字符串必须以 " 开头，并以 " 结尾，这样才能进行分析。	（无效组密码）（未知对等方）
wlan interface	WLAN 接口的符号名 格式：%s	WLAN1
ssid	以 ASCII 表示的 SSID（任意空格数） 格式：%s	MyWLAN
channel	通道名称 格式：%s	12
signal strength	信号强度 格式：%d	12
version	版本名称（无空格） 格式：%s	V1.0.3SP1
length	网络数据包长度（以字节为单位） 格式：%d	52
network interface	网络接口的符号名称 格式：%s	vlan 1

E.3 Syslog 消息

说明

严重程度

某些严重程度在固件中进行分组：

- Info + Notice = Info
- Warning + Error = Warning
- Critical + Emergency = Critical

用户标识和验证

消息文本	{protocol}: User {User name} has logged in from {ip address}.
示例	WBM: User "Admin" has logged in from 192.168.0.1.
说明	远程登录期间指定的有效登录信息。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 1.1

消息文本	{protocol}: User {User name} failed to log in from {ip address}.
示例	WBM: User "Admin" has failed to log in from 192.168.0.1.
说明	远程登录期间指定的用户名或密码（登录信息）不正确。
Severity	Error
Facility	local0
标准	IEC 62443-3-3 参考：SR 1.1

消息文本	{protocol}: User {User name} has logged out from {ip address}.
示例	SSH: User "Admin" has logged out from 192.168.0.1.
说明	用户会话已完成 - 注销。
Severity	Info

Facility	local0
标准	IEC 62443-3-3 参考：SR 1.1

消息文本	{protocol}: Default user {user name} logged in from {ip address}.
示例	SSH: Default user admin logged in from 192.168.0.1.
说明	默认用户已通过 IP 地址登录。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：n/a (NERC-CIP 007-R5)

消息文本	{Protocol}: {IP address} - No response from the RADIUS server.
示例	WBM: 192.168.1.105 - No response from the RADIUS server.
说明	未对服务器进行访问或服务器无响应。
Severity	Error
Facility	local0
标准	IEC 62443-3-3 参考：SR 1.1

用户帐户管理

消息文本	{protocol}: User {user name} changed own password.
示例	WBM: User admin changed own password.
说明	用户已更改自己的密码。
Severity	Notice
Facility	local0
标准	IEC 62443-3-3 参考：SR1.3

消息文本	{protocol}: User {user name} changed password of user {action user name}.
示例	Telnet: User admin changed password of user test.
说明	用户已更改其它用户的密码。
Severity	Notice

Facility	local0
标准	IEC 62443-3-3 参考：SR1.3

消息文本	{protocol}: User {user name} created user-account {action user name}.
示例	WBM: User admin created user-account service.
说明	用户已创建一个帐户。
Severity	Notice
Facility	local0
标准	IEC 62443-3-3 参考：SR1.3

消息文本	{protocol}: User {user name} deleted user-account {action user name}.
示例	WBM: User admin deleted user-account service.
说明	管理员已删除现有帐户。
Severity	Notice
Facility	local0
标准	IEC 62443-3-3 参考：SR1.3

标识符管理

消息文本	{Protocol}: User {User name} created group {Group} and assigned to role {Role}.
示例	WBM: User admin created group it-service and assigned to role service.
说明	管理员已创建组并为其分配角色。
Severity	注意
Facility	local0
标准	IEC 62443-3-3 参考：SR 1.4

消息文本	{Protocol}: User {User name} deleted group {Group} and the role {Role} assignment.
示例	WBM: User maier deleted group it-service and the role service assignment.
说明	管理员已删除现有组及角色分配。
Severity	Notice
Facility	local0
标准	IEC 62443-3-3 参考：SR 1.4

登录尝试失败

消息文本	{User name} account is locked for {Time minute} minutes after {Failed login count} unsuccessful login attempts.
示例	User service account is locked for 44 minutes after 10 unsuccessful login attempts.
说明	如果登录失败次数过多，则相应的用户帐户将被锁定一段特定的时间。
Severity	Warning
Facility	local0
标准	IEC 62443-3-3 参考：SR 1.11

会话锁定

消息文本	The session of user {user name} was closed after {time} seconds of inactivity.
示例	The session of user admin was closed after 60 seconds of inactivity.
说明	当前会话因非活动状态而被锁定。
Severity	Warning
Facility	local0
标准	IEC 62443-3-3 参考：SR 2.5

无线连接的使用控制

消息文本	{vap}: Client {SRC mac} associated successfully.
示例	VAP1.1: Client 00:0C:29:2F:09:B3 associated successfully.
说明	WLAN 客户端连接到 AP。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 2.2

消息文本	{vap}: Client {SRC mac} failed to associate, status {status}.
示例	VAP1.1: Client 00:0C:29:2F:09:B3 failed to associate, status (Invalid group cipher).
说明	WLAN 客户端到 AP 的连接被拒绝。
Severity	Error
Facility	local0
标准	IEC 62443-3-3 参考：SR 2.2

消息文本	Overlap-AP found on {Wlan interface}: AP {ssid} {Src mac} found on channel {Channel} rssi {Signal strength}.
示例	Overlap-AP found on WLAN1: AP MyWLAN 00:0C:29:2F:09:B3 found on channel 12 rssi 12.
说明	无线频率已在使用中。
Severity	Information
Facility	local0
标准	IEC 62443-3-3 参考：SR 2.2

消息文本	Overlap-AP found on {Wlan interface}: AP {ssid_Hex} {Src mac} found on channel {Channel} rssi {Signal strength}.
示例	Overlap-AP found on WLAN1: AP 050E081234 00:0C:29:2F:09:B3 found on channel 12 rssi 12.
说明	无线频率已在使用中。
Severity	Information

Facility	local0
标准	IEC 62443-3-3 参考：SR 2.2

消息文本	{vap}: Client {SRC mac} disassociated with reason {reason}.
示例	VAP1.1: Client 00:0C:29:2F:09:B3 disassociated with reason (Unknown peer).
说明	WLAN 客户端与 AP 断开连接。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 2.2

消息文本	{vap}: Client {SRC mac} failed to authenticate, status {status}.
示例	VAP1.1: Client 00:0C:29:2F:09:B3 failed to authenticate, status (Invalid group cipher).
说明	WLAN 客户端到 AP 的连接被拒绝。
Severity	Error
Facility	local0
标准	IEC 62443-3-3 参考：SR 2.2

消息文本	{Protocol}: {IP address} - No response from the RADIUS server.
示例	WBM: 192.168.1.105 - No response from the RADIUS server.
说明	未找到 RADIUS 服务器。
Severity	Error
Facility	local0
标准	IEC 62443-3-3 参考：SR 2.2

限制并发会话的数量

消息文本	{Protocol}: The maximum number of {Max sessions} concurrent login session exceeded.
示例	WBM: The maximum number of 10 concurrent login sessions exceeded.

说明	超出并行连接的最大数目。
Severity	Warning
Facility	local0
标准	IEC 62443-3-3 参考：SR 2.7

不可否认性

消息文本	Device configuration changed.
示例	Device configuration changed.
说明	设备组态已永久性更改。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR2.12

在自动系统中备份数据

日志文本	{protocol}: Saved file type ConfigPack.
标准	IEC 62443-3-3 参考：SR7.3
说明	ConfigPack 文件已保存。
示例	TFTP: Saved file type ConfigPack
Severity	Notice
Facility	local0

日志文本	{protocol}: User {user name} failed to save file type ConfigPack.
标准	IEC 62443-3-3 参考：SR7.3
描述	用户无法保存 ConfigPack 文件。
示例	WBM: User admin failed to save file type ConfigPack.
Severity	Info
Facility	local0

日志文本	{protocol}: User {user name} saved file type ConfigPack
标准	IEC 62443-3-3 参考：SR7.3

说明	用户已保存 ConfigPack 文件。
示例	WBM: User admin saved file type ConfigPack..
Severity	Notice
Facility	local0

日志文本	{protocol}: Failed to save file type ConfigPack.
标准	IEC 62443-3-3 参考：SR7.3
说明	ConfigPack 文件无法打开！
示例	TFTP: Failed to save file type ConfigPack.
Severity	Error
Facility	local0

自动化系统恢复

消息文本	{protocol}: User {user name} loaded file type Config (restart required)..
示例	WBM：用户管理员加载的文件类型 Config（需要重新启动）。
说明	已应用组态。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 7.4

消息文本	{protocol}: Loaded file type Config (restart required)..
示例	TFTP：加载的文件类型 Config（需要重新启动）。
说明	已应用组态。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 7.4

消息文本	{protocol}: User {user name} loaded file type ConfigPack (restart required)..
示例	WBM：用户管理员加载的文件类型 ConfigPack（需要重新启动）。

说明	已应用组态。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 7.4

消息文本	{protocol}: Loaded file type ConfigPack (restart required)..
示例	TFTP：加载的文件类型 ConfigPack（需要重新启动）。
说明	已应用组态。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 7.4

消息文本	{protocol}: User {user name} loaded file type Firmware {version} (restart required).
示例	WBM: User admin loaded file type Firmware V02.00.00 (restart required).
说明	固件更新已成功上传。
Severity	Notice
Facility	local0
标准	IEC 62443-3-3 参考：SR 7.4

消息文本	{protocol}: Loaded file type Firmware {version} (restart required).
示例	TFTP: Loaded file type Firmware V02.00.00 (restart required).
说明	固件更新已成功上传。
Severity	Info
Facility	local0
标准	IEC 62443-3-3 参考：SR 7.4

消息文本	{protocol}: Failed to load file type Firmware.
示例	WBM：无法加载文件类型固件。
说明	固件激活失败。

Severity	Error
Facility	local0
标准	IEC 62443-3-3 参考：SR 7.4

附录 F（支持的安全机制）

F

F.1 WLAN 安全机制

下表显示了 SCALANCE W 设备支持的加密和验证方法。

加密方法	
无 (None)	✓
WEP	✓
WPA-TKIP	-
WPA-AES	✓

验证	
密码/PSK	✓
IEEE 802.1X EAP PEAP	✓
IEEE 802.1X EAP TLS	✓
IEEE 802.1X EAP TTLS	✓
IEEE 802.1X EAP 其他	-
EAP 协议：MS-CHAPv2	✓
EAP 协议：TLS	✓
EAP 协议：GTC	✓

F.2 RADIUS 验证支持的安全机制

下表显示 SCALANCE W 设备支持的用于 RADIUS 验证的密码套件和签名算法。

表格 F- 1 WPA/WPA2 RADIUS 验证

密码套件	签名算法
TLS 1.2	
TLS_AES_256_GCM_SHA384	ECDSA with SHA256

密码套件	签名算法
TLS_CHACHA20_POLY1305_SHA256	ECDSA with SHA384
TLS_AES_128_GCM_SHA256	ECDSA with SHA512
ECDHE-ECDSA-AES256-GCM-SHA384	EdDSA ed25519
ECDHE-RSA-AES256-GCM-SHA384	EdDSA ed448
DHE-RSA-AES256-GCM-SHA384	RSASSA-PSS with SHA256
ECDHE-ECDSA-CHACHA20-POLY1305	RSASSA-PSS with SHA384
ECDHE-RSA-CHACHA20-POLY1305	RSASSA-PSS with SHA512
DHE-RSA-CHACHA20-POLY1305	RSASSA-PSS (rsaEncryption) with SHA256
ECDHE-ECDSA-AES128-GCM-SHA256	RSASSA-PSS (rsaEncryption) with SHA384
ECDHE-RSA-AES128-GCM-SHA256	RSASSA-PSS (rsaEncryption) with SHA512
DHE-RSA-AES128-GCM-SHA256	SHA256 with RSA
ECDHE-ECDSA-AES256-SHA384	SHA384 with RSA
ECDHE-RSA-AES256-SHA384	SHA512 with RSA
DHE-RSA-AES256-SHA256	DSA with SHA256
ECDHE-ECDSA-AES128-SHA256	DSA with SHA384
ECDHE-RSA-AES128-SHA256	DSA with SHA512
DHE-RSA-AES128-SHA256	
TLS 1.0/1.1	
AES256-GCM-SHA384	ECDSA with SHA224
AES128-GCM-SHA256	ECDSA with SHA1
AES256-SHA256	SHA224 with RSA
AES128-SHA256	SHA1 with RSA
ECDHE-ECDSA-AES256-SHA	DSA with SHA224
ECDHE-RSA-AES256-SHA	DSA with SHA1
DHE-RSA-AES256-SHA	ECDSA with SHA256
ECDHE-ECDSA-AES128-SHA	ECDSA with SHA384
ECDHE-RSA-AES128-SHA	ECDSA with SHA512

密码套件	签名算法
DHE-RSA-AES128-SHA	EdDSA ed25519
AES256-SHA	EdDSA ed448
AES128-SHA	RSASSA-PSS with SHA256
TLS_AES_256_GCM_SHA384	RSASSA-PSS 与 SHA384
TLS_CHACHA20_POLY1305_SHA256	RSASSA-PSS 与 SHA512
TLS_AES_128_GCM_SHA256	RSASSA-PSS（RSA 加密）与 SHA256
ECDHE-ECDSA-AES256-GCM-SHA384	RSASSA-PSS（RSA 加密）与 SHA384
ECDHE-RSA-AES256-GCM-SHA384	RSASSA-PSS（RSA 加密）与 SHA512
DHE-RSA-AES256-GCM-SHA384	SHA256 与 RSA
ECDHE-ECDSA-CHACHA20-POLY1305	SHA384 与 RSA
ECDHE-RSA-CHACHA20-POLY1305	SHA512 与 RSA
DHE-RSA-CHACHA20-POLY1305	DSA 与 SHA256
ECDHE-ECDSA-AES128-GCM-SHA256	DSA 与 SHA384
ECDHE-RSA-AES128-GCM-SHA256	DSA 与 SHA512
DHE-RSA-AES128-GCM-SHA256	
ECDHE-ECDSA-AES256-SHA384	
ECDHE-RSA-AES256-SHA384	
DHE-RSA-AES256-SHA256	
ECDHE-ECDSA-AES128-SHA256	
ECDHE-RSA-AES128-SHA256	
DHE-RSA-AES128-SHA256	

索引

C

S H

D

M