AXIS T8504–E Outdoor PoE Switch

用户手册

目录

关于本手册

目标

AXIS T8504–E 是室外 PoE 网络交换机。本产品的主要优点是其室外功能以及将网络最大范围延长至交换机和受电设备之间的 200 米内，增加了 100 米，同时还能为其网络供电 PoE 设备提供高达 2x60 W 和 2x30 W 的功率。

本用户手册提供了有关如何通过 AXIS IPv4/IPv6、VLAN、RADIUS、TACACS +、网页界面、SNMP 和 SSH 管理 AXIS T8504–E 的信息。

目标读者

本用户手册旨在为网络管理员、主管和安装技术人员提供相关知识：

- 网络基本概念和术语
- 网络拓扑包括 VLAN
- 网络协议
- 用户身份验证协议，包括 RADIUS 和 TACACS+

相关文档

有关其他信息，请参见以下文档：

- 产品安装指南
- RFC3621 SNMP MIB 和专用 MIB
- 为 T8504–E 安全 Web 服务器创建证书

缩写

缩写	说明
8021.Q	与 VLAN 相同
DES	数据加密标准
DGW	默认网关
DHCPv4	动态 IPv4 主机配置协议
DHCPv6	动态 IPv46 主机配置协议
IPv4	32 字节长的 IP 地址
IPv6	128 字节长的 IP 地址
MD5	消息摘要算法
MDI	媒体相关接口
MIB	管理信息库
PoE	以太网供电

关于本手册

RADIUS	远程身份验证拨入用户服务
SFP	光纤接口，外形小巧插头
SHA	消息摘要算法
SNMP	简单网络管理协议
SSH	安全护罩
SSL	安全套接字层
SysLog	系统日志
TACACS+	终端访问控制器访问控制
TFTP	小型文件传输协议
TLS	传输层安全
VLAN	虚拟局域网

一般信息

一般信息

功能

通过系统网络管理提供一系列功能。

- 在运行期间轻松进行软件更新，而不影响活动 PoE 端口
- 使用远程设备的图形方式进行配置和实时监控
- 系统状态显示
- PoE 事件、无效的远程用户访问、初始 DHCPv4/v6 地址等的 SysLog 报告。
- SNMP 陷阱报告各种 PoE 事件，例如 PoE 受电设备的加入或删除

以太网网络交换机网络功能

- 四个全天候密封的 RJ45 以太网端口，能够提供 10 Mbit、100 Mbit、1000 Mbit 半双工和 1000 Mbit 全双工的以太网速度
- 单个全天候密封的 SFP 以太网端口
- 8K 内部 MAC 地址查找引擎
- VLAN – 访问、中继和已筛选的中继
- 自动 MDIX
- 10KB 巨型帧

PoE 功能

提供以下 PoE 选项：

- 两个 4对 PoE 端口，可提供高达 60 W/端口的功率
- PoE 端口上有两个 IEEE 802.3，每端口可提供高达 30 W 的功率
- PoE 启用/禁用可启用或禁用 PoE 端口电源输出。以太网数据长时间处于启用状态。
- 远程设备重置可重置附加受电设备。设备暂时关闭电源，然后重新打开。

支持的网络协议

支持以下网络协议：

- IPv4 – 32 字节长的 IP 地址（静态/DHCPv4）
- IPv6 – 128 字节长的 IP 地址（静态/DHCPv6）
- VLAN – 访问、中继和已筛选的中继

用户访问和安全

访问选项

您可通过不同界面访问装置：

- 通过 Web 浏览器访问网页界面 – 查看设备 PoE 状态、网络状态、装置配置和装置生产信息

HTTP 是基于 Web 的友好配置界面。

HTTPS–TLS 是一种基于 web 的安全友好配置界面。

- SNMP（通过 SNMP 管理器应用）– 通过网络监控设备 (MIB–II RFC1213) 以及监控或配置设备 PoE 功能 (RFC3621)

  用于非加密的 SNMP 管理的 SNMPv2c

  用于安全和加密管理的 SNMPv3

  用于网络统计的 RFC1213 MIB–II

  用于 PoE SNMP MIB 的 RFC3621

  用于 RFC3621 PoE MIB 的专用 MIB 扩展

  各种基础设施和网络 MIB，如 IP–MIB、TCP–MIB、UDP–MIB 等。

- SSH 通过 SSH 客户端 – 查看装置 PoE 电源报告、网络状态、装置配置和生产信息；更新软件、启用或禁用 PoE 功能以及 ping 远程网络设备以进行连接测试

远程用户身份验证

可通过以下方式管理用户访问：

- 本地 – 用户名和密码由设备在本地管理
- RADIUS – 用户名和密码由 RADIUS 服务器通过网络进行身份验证
- TACACS+ – 用户名和密码由 TACACS+ 服务器通过网络进行身份验证

安全协议

用于访问装置的 Web HTTP 和 HTTPS、SNMPv2、SNMPv3 和 SSH 提供不同级别的安全保护。此外，RADIUS 和 TACACS+ 用于远程用户身份验证，提供不同的安全级别。

SNMPv1 和 SNMPv2 使用用于获取/设置/陷阱身份验证的团体字符串。SNMPv1 和 SNMPv2 被视为不安全协议，因为团体字符串密码可被网络嗅探设备轻松截获。

SNMPv3 通过在 SNMP 数据包上添加身份验证和加密层来解决 SNMPv1/v2 的安全问题。

默认装置 IP、用户名和密码

该装置随附有以下工厂默认用户名和密码：

装置默认 IPv4 地址
IP = 192.168.0.254
掩码 = 255.255.255.0

网页 HTTP/HTTPS 和 SSH
用户名 = root
密码 = 在设备上的标签上查找默认密码

SNMPv2
获取团体字符串 = 公共
设定团体字符串 = 写入
读取团体 = 公共
写入社区 = 写入
陷阱社区 = 公共

SNMPv3
用户名 = admin

身份验证密码 (MD5) = password
隐私密码 (DES) = password
身份验证和加密模式 = MD5 + DES

SNMPv3 通知
用户名 = trap
身份验证密码 = password
隐私密码 = password
身份验证和加密模式 = 无

有关如何恢复用户名和密码的信息，请参见 *恢复用户名和密码 7*。

恢复用户名和密码

注

恢复过程只能从本地 LAN 执行，而不能通过互联网或其他 IP 网络执行。用户应该能够在需要时关闭装置的电源。PoE 端口必须断开连接，且装置只能有一个单一的主动以太网链路。

注

您可能需要在 Windows 7 或 Windows 8 中添加 Telnet 客户端服务。

注

在应用用户名和密码之前，从装置电源进行的整个恢复过程必须少于 120 秒。

1. 断开除一根以太网线外的大多数PoE接口。只有一个单独以太网端口应该处于活动状态。
2. 关闭防火墙或启用 UDP 端口 514。然后在您的计算机上运行支持 IPv4 的 SysLog 服务器。
3. 关闭装置。等待 10 秒，然后重新打开装置。
4. 大约 15 秒后会显示一条 SysLog 消息。识别装置链接 – Link–local IPv6 地址。Link–local IPv6 地址以 FE80 开头。
5. 在您的计算机上打开一个命令提示符窗口。
   - 对于 Windows 7，请转到开始菜单并键入 cmd 。
   - 对于 Windows 8，请按下 Windows 键和 R 键，然后键入 cmd。
6. 键入 ipconfig 识别 Link–local IPv6 地址的虚拟界面索引。虚拟界面索引由 % 之后的数字表示。示例： fe80::9c39:db8b:62de:7bv4%17
7. 通过键入 Telnet 来准备 SSH 连接 [装置 Local–link IPv6 地址][% 虚拟接口编号] 2525，但不要按下 进入. 示例： Telnet fe80::9c39:db8b:62de:7bv4%17 2525
8. 关闭装置。等待 10 秒，然后重新打开装置。
9. 等待 30 秒，然后按下 进入 在 TCP 端口 2525 上启动 Telnet 会话。
10. 在用户名处键入 axispasswordrecovery，并在密码处输入 axispasswordrecovery。提供恢复选项将整个装置恢复为出厂默认设置，包括装置网络配置。
11. 按下 Y 恢复装置。装置将使用默认的 IPv 4 192.168.0.254 重新启动，键入 root 用户名，并使用您设备上的标签上所打印的默认密码。

首次配置

首次配置装置时，请执行下列步骤：

1. 将 PC 以太网网络接口配置为以下 IPv4 参数：

PC IPv4 地址： 192.168.0.40

PC IPv4 掩码： 255.255.255.0

2. 将 PC 以太网网络接口连接到装置的以太网端口。
3. 打开 Web 浏览器并在地址字段中键入 192.168.0.254。
4. 使用默认用户名和密码登录。请参见*默认装置 IP、用户名和密码 6*。
5. 配置装置。建议将用户名和密码更改为默认值以外的其他值。

通过 IP 网络的装置识别

要通过 IP 网络定位设备，设备在开机时发送广播格式的 IPv4 SysLog 消息 #0 (255.255.255.255)。通过 LAN 连接的 SysLog 服务器均会收到此 SysLog 消息。同样的 SysLog 消息也会发送至可选 SysLog 服务器 1 和 2（如果已配置）。

该装置发送消息两次。这是为了确保 SysLog 服务器收到 Syslog 消息，而无论网络配置如何。该消息首先在 VLAN 配置前发送，随后在 VLAN 配置完成后再次发送。

SysLog 消息 #0 包含能够通过网络提供对设置的访问所需的信息。

示例： `MsgID#000 - System UP. APP:v3.51.06 BOOT:v3.16 RST:Power-On BOOT:0=[APP OK] Host:axis-00055A034B49 MAC:00:05:5a:03:4b:49 VLAN:YES VLAN_MNGR:5 VLAN_UPLINK_PORT:3 VLAN_UPLINK_MODE:TRUNK DHCPv4:No IP1v4:192.168.0.254/24 DHCPv6:No IP1v6:2345::205:5AFF:FE03:4B49/64 IP2v6:FE80::205:5AFF:FE03:4B49/64`

字段	值	说明
`MsgID#000 - System UP`		SysLog 消息编号
应用：	`v3.51.06`	装置应用软件版本
`BOOT:`	`v3.16`	用于软件更新的装置启动版本
`RST:`	`Power-On`	重置原因
`BOOT:`	`0=[APP OK]`	
`Host:`	`axis-00055A034B49`	Axis 后跟装置 MAC 地址
`MAC:`	`00:05:5a:03:4b:49`	装置 MAC 地址
`VLAN:`	`YES`	VLAN 状态已启用或已禁用
`VLAN_UPLINK_PORT:`	`3`	用于装置管理的以太网端口编号
`VLAN_UPLINK_MODE:`	`TRUNK`	管理端口配置为访问或中继
`DHCPv4:`	`No`	DHCPv4 是或否
`IP1v4:`	`192.168.0.254/24`	装置 IPv4 地址
`DHCPv6:`	`No`	DHCPv6 是或否
`IP1v6:`	`2345::205:5AFF:FE03:4B49/64`	装置 IPv6 地址
`IP2v6:`	`FE80::205:5AFF:FE03:4B49/64`	装置链接 – 本地 IPv6 地址

网页界面

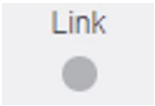
网页界面菜单

状态

转到状态，查看装置状态。该页每隔几秒就会自动更新。

注

无论 PoE 配置如何（启用或禁用），以太网网络链接皆处于启用状态。

参数	说明
	蓝色符号 – PoE 供电 灰色符号 – 无 PoE 供电
	蓝色符号 – 启用 PoE 端口 灰色符号 – 禁用 PoE 端口
	蓝色符号 – 以太网链路已打开 灰色符号 – 无以太网链路
	蓝色符号 – 上行端口插入 SFP 模块 灰色符号 – 上行端口没有插入 SFP 模块
网络	报告以太网链路速度 (10/100/1000 MB) 以及网络连接是否正常
状态	报告 PoE 端口状态（如果已启用、已禁用、正在供电等）。
功率使用情况	报告实际功率消耗及其可提供的最大功率
PoE 重置	单击重置以关闭 PoE 端口电源，然后重新恢复 PoE 电源。 注 重置 PoE 后，将启用由 SSH 或 SNMP 禁用的 PoE 端口。
总功率使用	报告 PoE 端口消耗的总功率以及消耗的功率相对于内部电源功率的百分比。

基本

转到基本以查看有关产品的基本信息。

使用中的 IP 地址 – 转到使用中的 IP 地址，查看有关 IPv4 和 IPv6 地址、掩码、默认网关和域名服务器 (DNS) 的信息。

产品信息 – 转到产品信息查看一般产品信息，如产品名称、序列号、软件版本和 PoE 固件版本以及 SFP 模块信息，如 SFP 类型、供应商、零件号和序列号。

网络配置 – 转到网络配置启用或禁用 DHCP，配置 IPv4、IPv6 和网络主机名。IPv4 和 IPv6 均使用主机名在 DHCPv4/v6 服务器中注册装置名称。请注意，IPv6 使用 FQDN 术语作为主机名称。

网络服务 IPv4/IPv6 – 转到网络服务 IPv4/IPv6 以配置 DNS 和 SysLog 服务器。

PoE 配置 – 转到 PoE 配置以配置 PoE 端口功率。四个 PoE 功率方案在四个 PoE 端口之间提供不同的功率分配。四个选项均符合设备最大功率。

- 60 W：通过以太网电缆内的四个线对传输功率。每一对传输高达 30 W。
- 30 W：通过以太网电缆内的四个线对中的两个传输功率
- 15.4 W：通过以太网电缆内的四个线对中的两个传输功率
- – –: 无 PoE 供电。以太网端口已启用且可正常工作，但 PoE 被禁用。

安全

安全配置

转到安全配置以配置远程网页或 SSH 访问的装置用户名和密码。

注

仅 ASCII 字符 33–90 和 94–122 可用于用户名和密码字段。

HTTPS

转到 HTTPS 配置是否应使用 HTTP 或 HTTPS（安全网站）。当启用 HTTPS 时，TLSv 1.2 用于加密网页网络流量。

注

要在通过 HTTPS 访问装置时消除 Web 浏览器警告，请向 Web 浏览器添加例外规则，以通知 Web 浏览器网站合法或上传设备自签名/CA 签名证书。

RADIUS/TACACS+

当用户通过网页或 SSH 访问装置时，RADIUS/TACACS+ 可实现远程用户身份验证。用户名和密码，然后由 RADIUS/TACACS+ 服务器进行身份验证。

RADIUS/TACACS+ 的优势在于，用户名和密码易于更新，尤其是要管理多个网络设备时更是如此。

RADIUS/TACACS+ 的缺点是，如果 RADIUS/TACACS+ 服务器都关闭，则无法访问该装置。可以启用本地登录后备功能，当 RADIUS/TACACS+ 服务器没有回复时，允许装置使用其本地用户名和密码。

RADIUS/TACACS+ 公共参数

参数	说明
启用身份验证	配置是否应启用或禁用 RADIUS/TACACS+。禁用 RADIUS/TACACS+ 时，将使用本地用户名和密码。
启用本地登录后备	本地登录后备启用时，当 RADIUS/TACACS+ 服务器没有回复时，将使用本地用户名和密码。当服务器停机或出现网络问题时，可能会出现这种情况。
身份验证协议	选择 RADIUS 或 TACACS+ 身份验证协议。
共享的机密	必须同时在装置和 RADIUS/TACACS+ 服务器上配置相同的私钥字符串。
主服务器 IP 地址	配置用于访问主 RADIUS/TACACS+ 服务器的主要 IPv4、IPv6 或主机名。

辅助服务器 IP 地址	配置用于访问辅助 RADIUS/TACACS+ 服务器的主要 IPv4、IPv6 或主机名。
超时（秒）	配置答复超时的时间。

RADIUS 额外参数

参数	说明
身份验证 UDP 端口	配置 RADIUS 服务器使用的 UDP 端口。

TACACS+ 额外参数

参数	说明
身份验证 TCP 端口	配置 TACACS+ 服务器使用的 TCP 端口。

注

软件版本 3.51.06 仅支持通过 IPv4 访问 RADIUS/TACACS+ 服务器，或者使用 IPv4 地址或主机来解析 DNS 服务器。

测试 RADIUS/TACACS+

在激活 RADIUS/TACACS+ 之前，转到测试 RADIUS/TACACS+ 以验证其配置。

注

在测试期间，应禁用启用身份验证 。

1. 配置 RADIUS/TACACS+ 参数，让启用身份验证保持禁用。
2. 保存配置。如果不这样做，每次测试后，参数将恢复到保存值，并擦除未保存的值。
3. 键入用户名和密码。
4. 单击测试配置。系统将显示一个等待消息，接下来是正常或失败。
5. 如果需要，请更改并保存配置并再次进行测试。
6. 当测试结果正常时，将启用身份验证设置为启用。保存用于激活 RADIUS/TACACS+ 配置的相关配置。

VLAN 配置

VLAN 配置健全检查是在装置通电时，以及在网络上请求 VLAN 配置更改时完成的。健全检查旨在确保应用 VLAN 配置后装置在网络上保持可管理。如果新 VLAN 配置可能导致装置变得无法管理，则网页上将显示有关网络请求的错误消息。当在开机时侦测到问题时，装置配置将恢复为出厂默认设置。

VLAN 启用 & 管理端口

参数	说明
启用 VLAN	启用或禁用 VLAN 功能。

管理上行端口	此参数对实际 VLAN 流量没有影响。如果新 VLAN 配置可能阻止通过 VLAN 从此端口管理装置，则管理上行链路端口可帮助装置进行评估。如果检测到可能存在的冲突，则会显示一条错误消息，并且新的 VLAN 配置将会被拒绝。
管理 VLAN ID	当启用 VLAN 时，请配置管理装置时要使用的 VLAN ID。

VLAN 端口配置

参数	说明
VLAN 模式	将每个以太网端口的 VLAN 模式设置为访问或中继。 访问 – VLAN 仅在装置内用于分割或仅限于特定端口的数据包访问。VLAN 访问端口接收的附带 VLAN 标记的数据包都将被丢弃。VLAN 标记将添加到装置数据包中，以便 VLAN 访问传入数据包。装置内部 VLAN 标记已为 VLAN 访问传出数据包而剥离。 中继 – 以太网数据包均为 VLAN 标记。VLAN 中继端口收到的未加标签的 VLAN 数据包都将被丢弃。
访问模式 VLAN ID	当端口配置为访问时，配置要使用的 VLAN ID。装置内部管理端口仅用作访问。只能通过管理 VLAN ID 到达。
中继 – 过滤未知 VLAN	将 VLAN 中继端口配置为已筛选或未筛选。 已启用 – 仅来自"中继 VLAN"列表中指定的来自某些 VLAN ID 的数据流通过 VLAN 中继端口传递。其他 VLAN 标记的流量将被丢弃。 禁用 – 来自 VLAN ID 的数据流都通过 VLAN 中继端口。
中继 VLAN	当启用中继 – 过滤未知 VLAN 时，列出允许通过 VLAN 中继端口的 VLAN ID。

SNMP 配置

转到 SNMP 配置，配置适用于 SNMPv2c 和 SNMPv3 的参数。

SNMPv2c

参数	说明
启用 SNMPv2c	启用或禁用 SNMPv2c 支持。
读取团队	配置 SNMPv2c 获取团体字符串。示例： 公共。
写入团队	配置 SNMPv2c 设定团体字符串。示例： 私有。
陷阱团队	配置 SNMPv2c 陷阱团体字符串。示例： 公共。

系统信息 (MIB–II, v2c/v3)

参数	说明
系统联系人	配置 SNMP MIB–II 系统联系人 OiD 字符串。示例： 约翰。
系统名称	配置 SNMP MIB–II 系统名称。例如： 我的装置。
系统位置	配置 SNMP MIB–II 系统位置。示例： 大学。

网页界面

PoE MIB (RFC3621, v2c/v3)

参数	说明
启用通知	启用或禁用以下 PoE 陷阱报告： • PoE 供电/从受电设备上移除 • 装置总功率消耗超过了最大装置功率的 xy% • 装置总功率消耗已恢复为小于最大装置功率的 xy%
超过功率使用 (1–99%) 时通知	如果启用本功能，则只要装置总功率消耗与装置最大功率的占比 (xy%) 超过或低于指定值，就会通知用户。

SNMPv3

参数	说明
启用 SNMPv3	启用或禁用 SNMPv3 支持。
用户名	配置 SNMPv3 用户名字符串。
身份验证密码	配置将由 MD5/SHA 使用的 SNMPv3 密码。
隐私密码	配置将由 DES/AES 使用的 SNMPv3 密码。
身份验证和加密模式	配置 SNMPv3 身份验证和加密模式。 无 – 无身份验证或加密，这意味着没有安全性。 MD5 – MD5 身份验证，不加密。数据包可通过网络嗅探者轻松进行分析来进行更改。 SHA – 不加密的 SHA 身份验证。 MD5 + DES – MD5 身份验证和 DES 加密 SHA + DES – SHA 身份验证和 DES 加密 MD5 + AES – MD5 身份验证和 AES 加密 SHA + AES – SHA 身份验证和 AES 加密

SNMPv3 通知（陷阱）

参数	描述
用户名	配置 SNMPv3 通知用户名字符串。
身份验证密码	配置将由 MD5/SHA 使用的 SNMPv3 通知密码。
隐私密码	配置将由 DES/AES 使用的 SNMPv3 通知密码。
身份验证和加密模式	配置 SNMPv3 通知身份验证和加密模式。 无 – 无身份验证或加密，这意味着没有安全性。 MD5 – MD5 身份验证，不加密。数据包可通过网络嗅探者轻松进行分析来进行更改。 SHA – 不加密的 SHA 身份验证。 MD5 + DES – MD5 身份验证和 DES 加密 SHA + DES – SHA 身份验证和 DES 加密 MD5 + AES – MD5 身份验证和 AES 加密 SHA + AES – SHA 身份验证和 AES 加密

远程 IPv4/IPv6 SNMP 陷阱管理器 (v2c/v3)

参数	说明
陷阱管理器 #1	配置远程 SNMP 管理器服务器的首个 IPv4/IPv6/DNS 名称，接收单元陷阱报告，如冷启动等。
陷阱管理器 #2	配置远程 SNMP 管理器服务器的第二个 IPv4/IPv6/DNS 名称，接收单元陷阱报告，如冷启动等。

维护

重置 – 有四种不同的重置选项：

- 在不切断 PoE 电源的情况下进行安全重启重置内部网络管理器和内部以太网交换机（网络将关闭几秒），PoE 电源无变化。受电设备继续正常运行，就像没有进行过复位一样。
- 进行安全重启将重置内部网络管理器、内部 PoE 控制器和内部以太网交换机。
- 恢复出厂值，但保留 IP 设置会将设备配置重置为出厂默认设置，从而使 IPv4/IPv6 网络配置保持不变。VLAN 和 RADIUS/TACACS+ 已禁用。通过之前的网络配置访问装置的选项得到保留。
- 恢复出厂值将装置恢复为默认出厂设置。装置 IP 设置为 192.168.0.254 并禁用 VLAN。

固件升级 – 固件升级仅升级内部网络管理器。PoE 固件未更改。升级可能耗时 10 分钟。在此期间，网络交换机功能保持不会间断，但装置无法管理。PoE 功能保持激活状态，但网络流量可能会在几秒后中断。

产品配置 – 转到产品配置下载或上载产品配置文件。此功能可用于备份装置配置、脱机修改装置配置或创建主配置文件，以便轻松配置多个装置。

SSH 串行接口

SSH 串行接口

SSH 接口旨在实现各种维护任务，如 PoE 固件更新等。它旨在为熟悉 SSH 的 IT 经理提供简单便捷的界面。为了简化 SSH 使用，SSH 接口是由菜单驱动的。

SSH 受密码保护，并共享与 Web 访问相同的用户名和密码。

SSH 支持 RADIUS 和 TACACS+ 用户名和密码身份验证。

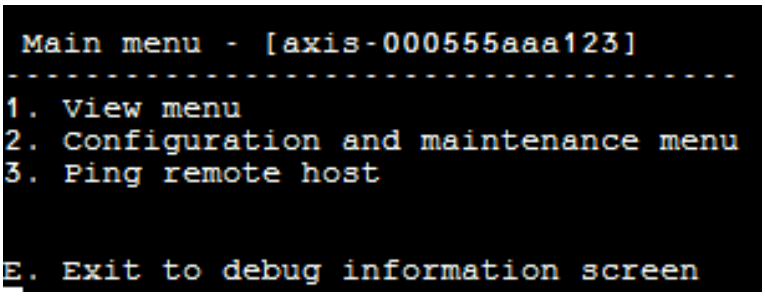
注

一次仅有一个远程用户能够通过 SSH 访问装置。如果第二个远程 SSH 用户尝试在首个 SSH 用户仍处于活动状态时访问该装置，则会向第二个 SSH 用户显示一条消息，请求用户稍后尝试通过 SSH 重新连接。

注

非活动 SSH 会话（远程用户没有键盘活动）将在三分钟后自动终止。

主菜单



为了轻松识别访问的装置，装置主机名字符串显示在主菜单标题的右侧。当用户拥有多个装置时，此功能尤其有用。

查看菜单

查看菜单提供有关 PoE 端口状态、网络参数和设备信息。

菜单项	说明
1. 查看 PoE 端口状态	转到此菜单项获取以下信息： • 网络 – 有关以太网链路速度 (10/100/1000) 和 HD/FD 连接类型的信息 • PoE – 有关每台已连接设备的功率消耗信息 • 总功率 – 有关连接到主动 PoE 端口的受电设备的总功率消耗信息。还显示最大可用功率。 • 电源 – 关于装置的内部电源电压的信息

2. 查看网络参数	转到此菜单项获取以下信息： • 使用中的 IPv4 网络参数 – 显示是否启用或禁用了 DHCPv4。还显示使用中的 IPv4 地址、IPv4 掩码和 IPv4 默认网关。 • 使用中的 IPv6 网络参数 – 显示是否启用或禁用了 DHCPv6。还显示使用中的 IPv6 地址、IPv6 前缀和 IPv6 默认网关。除了静态/DHCPv6 IPv6 地址外，IPv6 还可以报告多个已自动获取的 IPv6 地址。 • 使用中的 DNS 网络参数 — 有关使用中的 IPv4/IPv6 域名服务器 IP 的信息，这些 IP 是静态配置或由 DHCPv4/DHCPv6 获取的。 • 更多网络参数 – 关于装置 MAC 地址的信息
3. 查看装置信息	转到此菜单项获取装置生产参数的摘要： • 部件编号 – 有关装置营销零件号 (T8504–E) 的信息 • S/N – 有关装置六位数序列号的信息 • 产品编号 – 有关装置生产编号的信息（仅供内部使用） • 应用版本 – 有关网络管理器软件版本的信息 • 启动版本 – 有关网络管理器启动版本的信息 • 固件 – PoE 固件版本 • 系统正常运行时间 – 装置重置或通电后的时间信息 • 系统 GMT 时间 – 从 NTP 服务器获取的有关装置 GMT 时间的信息。当装置无法从 NTP 服务器获取 NTP 时间时，将显示消息“不正确”。 • 系统本地时间 – 有关装置本地时间（GMT 加上时区转换）的信息。当装置无法从 NTP 服务器获取 NTP 时间时，将显示消息“不正确”。

配置和维护菜单

转到 配置和维护菜单配置或重置装置或更新软件。

菜单项	说明
1. 启用/禁用 PoE 端口	启用或禁用 PoE 端口。即使未接通电源，以太网链路仍保持启用状态。
2. 从 TFTP 服务器下载 WEB SSL 证书（仅重置 Web 服务器）	从 TFTP 服务器下载自签名或 CA 签名证书，以允许在 Web 浏览器安全确认（Web 浏览器 URL 区域中显示绿色锁图标）情况下对装置进行安全的 Web 浏览。
3. 更新装置 PoE 固件（重置装置）	更新 PoE 固件。更新文件可从 TFTP 服务器下载。PoE 功能在固件更新期间不可用（大约 5–10 分钟）。
4. 将装置恢复到半出厂默认设置（不包括 IP 配置）	将装置配置恢复为出厂默认设置，但保留 IPv4/IPv6 网络配置。此选项保留了通过之前的网络配置访问装置的选项。
5. 恢复装置为完全出厂默认设置	将整个装置恢复为出厂默认设置。
6. 仅重置网络管理器	仅重置内部网络管理器，它负责装置网络管理界面，如 Web、SSH、SNMP 等。内部以太网交换机也会重置；网络将关闭几秒。仅 PoE 电源不会改变。受电设备继续正常运行，就像没有进行过复位一样。
7. 重置装置	重置整个装置，包括内部网络管理器、PoE 控制器和内部的以太网交换机。
8. 启用/禁用自动 Ping 默认网关以确保网络连接	启用或禁用自动 Ping到默认网关。启用时，设备将通过每隔 12 秒（IPv4 DGW 或 IPv6 DGW）Ping 默认网关来验证网络连接是否正常。在 10 个连续的 Ping 故障之后，网络管理模块会重置自身，而不会影响 PoE 端口。

SSH 串行接口

Ping 远程主机

转到 Ping 远程主机测试网络连接问题。

SNMP 监控和配置

通过使用第三方标准网络管理工具（如 HP Openview、IBM Tivoli、SNMPc 等），可监控和管理多个装置。

启用 SNMP

网络管理器接口支持 SNMPv1、SNMPv2 和 SNMPv3。该装置接受并回复 SNMPv1 数据包，但由于 SNMPv1 已过时，因此 SNMP 陷阱和通知是以 SNMPv2、SNMPv3 的形式发送或同时发送。

注

出于安全原因，该装置默认禁用 SNMPv2、SNMPv3。在启用 SNMP 之前，强烈建议先修改 SNMP 团体字符串，然后再启用 SNMP。

启用 SNMP 的方法：

- 转到安全 > SNMMP 配置，并启用 SNMPv2 或 SNMPv3。
- 确保 SNMPv2 团体字符串与 SNMP 管理器配置相匹配。
- 请确保 SNMPv3 用户名、身份验证密码、隐私密码和加密方法与 SNMP 管理器的配置相匹配。

启用陷阱的方法：

- 转到远程 IPv4/IPv6 SNMP 陷阱管理器并配置远程管理器 IP 地址。
- 请确保 SNMPv3 通知、用户名、身份验证密码、隐私密码和加密方法与 SNMP 陷阱管理器的配置相匹配。
- 转到 PoE MIB 并启用 PoE 通知以获取有关 PoE 端口状态更改的通知，装置电源消耗超出或低于特定级别等。

SNMP MIB

SNMP 管理器支持多个 MIB。

网络 MIB – 各种网络 MIB（如 RFC1213 MIB–II）可用于提供网络统计。请注意，这些 MIB 不适合用于 SNMP 上的网络配置。

RFC3621 – POE 供电 (PoE) MIB 提供各种 PoE 功能。请参见*RFC3621 PoE MIB 18*。

私有 MIB – 增强 PoE 功能，超越 RFC3621 PoE MIB。请参见*私有 MIB 18*。

RFC3621 PoE MIB

RFC3621 PoE MIB 位于 1.3.6.1.2.1.105 SNMP MIB 树下。MIB 分为三个部分。

端口参数 – 第一部分处理 PoE 端口，并提供诸如启用和禁用端口、读取端口状态、类等功能。每个 OiD 均以二维数组表的形式访问。

主要 PSE 参数 – 第二部分处理为一组 PoE 端口供电的电源。它能够读取总功耗和电源状态等。

PoE 陷阱 – 第三部分启用和禁用发送至远程 SNMP 管理器的 PoE 陷阱。

私有 MIB

SNMP 专用 MIB 支持以下 SNMP OID：

SNMP 监控和配置

OiD 名称	类型 (R/W)	说明
poePortConsumptionPower	R	PoE 端口功耗 [瓦特]
poePortMaxPower	R	PoE 端口最大可用功率 [瓦特]
poePortType	R	PoE 端口类型 – 两对、30 [瓦特]、四对、60 [瓦特]
mainVoltage	R	装置电源电压 [伏特]

SysLog 消息

SysLog 消息

该装置向运行 SysLog 守护应用的外部 IPv4/IPv6 主机发送各种事件报告。IPv4/IPv6 主机会记录事件，以备将来使用。如果要发送系统日志事件，通过浏览装置配置网页来配置 SysLog 服务器 IP 地址。

日志事件类别有三种：

广播 IPv4 SysLog 事件 – 这些日志事件将被局域网上的其他 SysLog 服务器截获，而不管装置 SysLog 配置如何。这有助于查找网络上的装置 IP 并报告重大事件，如电源故障等装置恢复。

RFC3621 PoE 陷阱 – RFC3621 PoE 陷阱也作为 SysLog 消息发送，从而方便了远程用户阅读此类事件。

专有 SysLog 事件 – 这些日志事件包括可能发生的故障或潜在的安全漏洞，例如远程用户尝试通过网页/SSH 等不正确的用户名进行访问等情况。

SysLog 消息类型

消息 ID	说明	提供的信息	备注
0	发送 System UP 消息表示装置通电或内部网络管理器自动重置。	• 应用版本 • 启动版本 • 重置原因 • 启动状态 • 装置主机名 • 装置 MAC 地址 • VLAN（是/否）如果是，则还提供 VLAN ID。VLAN ID 用于管理装置。哪个端口，以及端口是否配置为访问或中继。 • IPv4 地址（静态/HDCPv4） • IPv6 地址（静态/DHCPv6）	消息以 255.255.255.255 广播格式发送到通过 LAN 连接的 SysLog 服务器以及 SysLog 服务器 1 和 2。
1	发送 PoE 端口状态更改消息表示 PoE 端口的状态更改，例如当设备被插入或移除时。	在 RFC3621（搜索、供电、故障等）中定义的新的 PoE 状态	RFC3621 SNMP PoE MIB、陷阱对等 SysLog 报告
2	发送 PoE 使用功率超过电源最大功率的 xy% 消息表示 PoE 使用功率超过设定值。	使用功率占电源最大功率的百分比	RFC3621 SNMP PoE MIB、陷阱对等 SysLog 报告
3	发送 PoE 使用功率低于电源最大功率的 xy% 消息表示 PoE 使用功率低于设定值。	使用功率占电源最大功率的百分比	RFC3621 SNMP PoE MIB、陷阱对等 SysLog 报告
6	发送默认配置消息表示装置恢复为默认配置		将装置恢复为默认配置时，SysLog 服务器 IP 不变。
7	发送装置配置更改消息表示装置配置已更改。		
9	发送 PoE 控制器重置消息表示 PoE 控制器发生重置。		

SysLog 消息

10	发送 PoE 控制器无固件消息表示 PoE 控制器的固件清除或损坏。		
11	发送无效的 SSH 消息表示一个远程用户试图用不正确的用户名或密码通过 SSH 访问装置。	远程用户 IPv4/IPv6 地址	
12	DHCPv4 只在初次获得 DHCPv4 地址时发送，无论是从静态切换到 DHCPv4 还是开机时。	• 装置主机名 • 装置 MAC 地址 • DHCPv4 地址	消息以 255.255.255.255 广播格式发送到通过 LAN 连接的 SysLog 服务器以及 SysLog 服务器 1 和 2。
13	DHCPv6 只在初次获得 DHCPv6 地址时发送，无论是从静态切换到 DHCPv6 还是开机时。	• 装置主机名 • 装置 MAC 地址 • DHCPv6 地址	消息以 255.255.255.255 广播格式发送到通过 LAN 连接的 SysLog 服务器以及 SysLog 服务器 1 和 2。
14	发送无效的 VLAN 配置消息表示在开机时，设备检测到当前的 VLAN 配置使装置无法通过网络进行管理。这可能是由于上传到装置的新配置文件出错所致。该装置将自身恢复为半出厂默认设置，关闭 VLAN 并将其大部分配置参数恢复为出厂默认设置，但保持装置的网络 IP 参数不变。然后，装置将重新启动。		消息以 255.255.255.255 广播格式发送到通过 LAN 连接的 SysLog 服务器以及 SysLog 服务器 1 和 2。

故障排查

下面的故障排查表格将指导您解决常见的问题。如果您无法找到所需的信息，请联系当地经销商寻求进一步的帮助。

问题	修正步骤
Ping 装置 IP 地址失败。	1. 验证您的 PC 和装置是否共享相同的 IP 网络。 2. 启动 SysLog 服务器。 3. 关闭设备，然后将其重新打开。等待 SysLog 消息 #0 出现，并报告装置 IP 地址。
可从本地主机 Ping 到装置，但在尝试使用装置的 Ping 功能时，没有响应。	1. 关闭主机防火墙。 2. 如果 Ping 确定，请转到高级防火墙选项并启用 Ping 选项、TFTP（UDP 端口 69）和 SNMP 陷阱端口（UDP 端口 162）。
无法通过 TFTP 更新软件。	1. 使用装置的 Ping 功能 Ping 运行 TFTP 服务器应用的主机。 2. 关闭防火墙或启用 UDP 端口 69。 3. 验证是否已将相应的更新文件包复制到 TFTP 服务器的根文件夹。
通过 SSH 可以登录到装置，但 SSH 会话将在一段时间后终止。	如果未按下按键且不发生活动，则 SSH 会话将在三分钟后终止。
未接收到 SNMP 陷阱事件。	1. 使用 Web 浏览器查看装置配置。 2. 验证是否已选择 SNMP。 3. 验证远程 SNMP 管理器 IP 是否匹配。 4. 验证陷阱团体字符串是否与远程 SNMP 管理器陷阱配置相匹配。 5. 关闭 SNMP 管理器工作站上的防火墙或允许 UDP 端口 162 通过它。
SysLog 服务器 IP 已正确设置，但未接收到日志消息。	关闭主机防火墙或允许 UDP 端口 514 通过它。
启用 RADIUS/TACACS+ 后，无法正常登录装置。	1. 请按*恢复用户名和密码 7*中的说明操作 。 2. 配置包括 RADIUS/TACACS+ 值的设置，保持启用身份验证为禁用状态。 3. 请使用 RADIUS/TACACS+ 网页上的“测试用户名和密码”功能验证远程用户是否可以登录到装置。 4. 将启用身份验证设置为启用。
PoE SNMP 陷阱不发送。	1. 在 SNMP 配置网页上启用 RFC3621 通知。 2. 配置 SNMP 陷阱管理器 IP。 3. 启用 SNMPv2 或 SNMPv3。

支持

如果您需要技术帮助，请与您的 Axis 经销商联系。如果不能立即回答您的问题，经销商将会通过适当的渠道转发您的疑问，从而确保响应迅速。如果您连接到互联网，则可以：

- 下载用户文档和软件更新
- 在常见问题数据库中查找已解决问题的答复，通过产品、目录或词组来进行搜索
- 通过登录到您的个人支持区域，向 Axis 支持人员报告问题
- 与 Axis 支持人员聊天

故障排查

- 通过 *axis.com/support* 访问安讯士支持部门

如果您需要技术帮助，请根据您的 AVHS 许可协议与相应渠道联系，以确保能够得到快速响应。

如果您需要技术帮助，请与 ADP 帮助台联系以确保能够得到快速响应。

了解更多!

访问 Axis 学习中心 *axis.com/learning*，获取有用的培训、在线研讨会、教程和指南。

用户手册
AXIS T8504–E Outdoor PoE Switch
© Axis Communications AB, 2018 – 2024
版本 M3.2
日期： 六月 2024
零件号 T10126544