大华5.8G电梯网桥

使用说明书



浙江大华技术股份有限公司

V1.0.0

前言

适用型号

DH-WBD5-60AC-01LC

符号约定

在本文档中可能出现下列标识，代表的含义如下。

标识	说明
 警告	表示有中度或低度潜在危险，如果不能避免，可能导致人员轻微或中等伤害。
 注意	表示有潜在风险，如果忽视这些文本，可能导致设备损坏、数据丢失、设备性能降低或不可预知的结果。
 窍门	表示能帮助您解决某个问题或节省您的时间。
 说明	表示是正文的附加信息，是对正文的强调和补充。

修订记录

版本号	修订内容	发布日期
V1.0.0	首次发布。	2020.10

使用安全须知

下面是关于产品的正确使用方法、为预防危险、防止财产受到损失等内容，使用设备前请仔细阅读本说明书并在使用时严格遵守，阅读后请妥善保存说明书。

使用要求

- 请勿将设备放置和安装在阳光直射的地方或发热设备附近。
- 请勿将设备安装在潮湿、有灰尘或煤烟的场所。
- 请保持设备的水平安装，或将设备安装在稳定场所，注意防止本产品坠落。
- 请勿将液体滴到或溅到设备上，并确保设备上没有放置装满液体的物品，防止液体流入设备。
- 请将设备安装在通风良好的场所，切勿堵塞设备的通风口。
- 仅可在额定输入输出范围内使用设备。
- 请勿随意拆卸设备。
- 请在允许的湿度和温度范围内运输、使用和存储设备。
- 拆卸电缆时，请先将设备断电，以免造成人身伤害。
- 稳压器和防雷器根据现场供电和周边环境情况选装。

电源要求

- 请务必按照要求使用电池，否则可能导致电池起火、爆炸或燃烧的危险！
- 更换电池时只能使用同样类型的电池！
- 产品必须使用本地区推荐使用的电线组件（电源线），并在其额定规格内使用！
- 请务必使用设备标配的电源适配器，否则引起的人员伤害或设备损害由使用方自己承担。
- 请使用满足SELV（安全超低电压）要求的电源，并按照IEC60950-1符合Limited Power Source（受限制电源）的额定电压供电，具体供电要求以设备标签为准。
- 请务必将设备端接地（必须使用横截面不小于2.5mm^{2}的铜线接入，对地电阻≤4Ω）。
- 器具耦合器为断开装置，正常使用时请保持方便操作的角度。

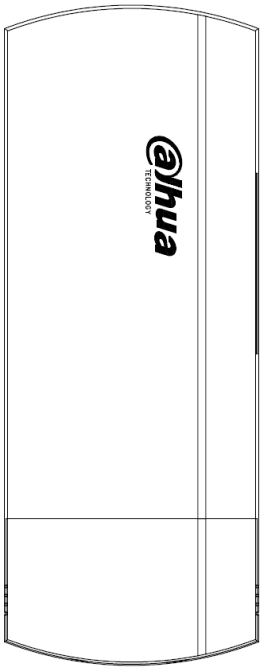
目 录

前言 ..... **I**
使用安全须知 ..... **II**
第 1 章 外观结构 **1**
1.1 设备外观 1
1.2 设备结构 1
第 2 章 安装与连接 **3**
2.1 设备安装 3
2.2 设备连接 4
第 3 章 基本配置 **6**
3.1 配置主从模式 6
3.1.1 配置主模式 6
3.1.2 配置从模式 8
3.2 管理员设置 9
3.3 固件升级 10
3.4 系统配置 10
第 4 章 技术规格 **12**
第 5 章 常见问题 **13**
附录1 法律声明 **14**
附录2 网络安全声明和建议 **16**

第 1 章 外观结构

1.1 设备外观

图1-1 设备外观



1.2 设备结构

指示灯

图1-2 指示灯

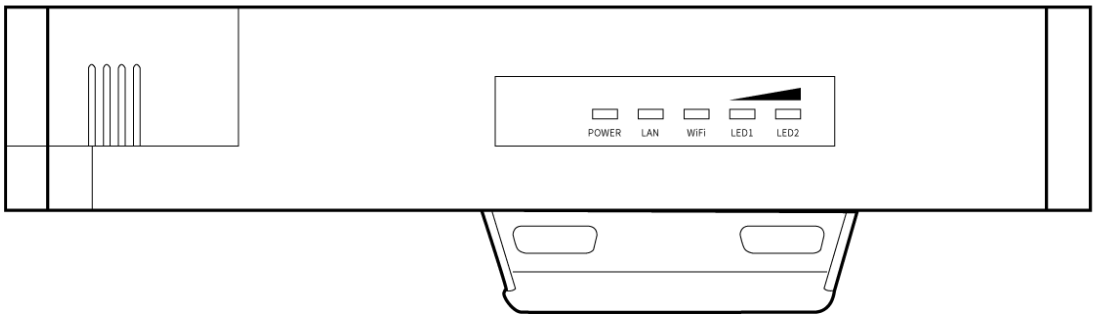


表1-1 指示灯说明

指示灯	状态	说明
LED1/LED2（接收信号强度指示灯）	灯灭	网桥没有通过无线连接到任何设备。
	灯常亮	● 主模式：默认常亮。 ● 从模式：LED1、LED2均常亮：信号强度≥-60dbm；LED1常亮、LED2不亮：信号强度-60dbm～-80dbm。
WiFi	闪烁	设备正常启动。
LAN	灯灭	未连接终端设备。
	灯常亮	已连接终端设备。
POWER	灯灭	设备未上电或供电异常。
	灯常亮	设备正常上电。

接口/按钮

图1-3 接口/按钮

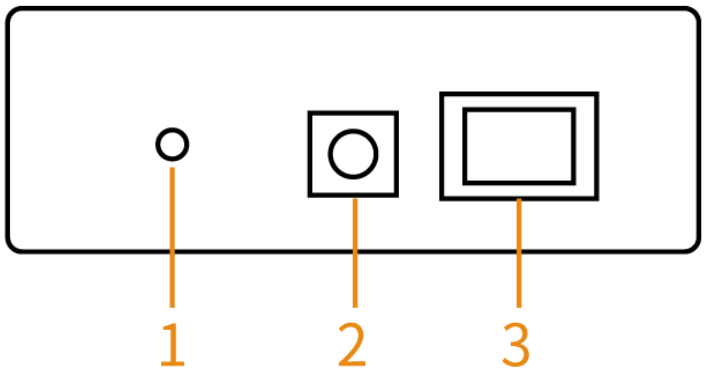


表1-2 接口说明

序号	接口/按钮	说明
1	Reset复位键	长按Reset键5s以上，可恢复出厂设置。
2	DC 12V供电接口	通过DC 12V给设备供电。
3	设备网口	● 1×10/100M RJ45。 ● 与电源的PoE口连接，为设备供电并传输数据，支持24V非标PoE供电。 ● 当无线设备使用DC 12V供电时，可通过此网口连接网络摄像机或其他终端设备。

第 2 章 安装与连接

2.1 设备安装

开箱清单

开箱未提及的工具或配件，请用户自行按需购买。

表2-1 开箱清单

名称	数量
网桥	2
PoE电源适配器	2
扎带	4
使用说明书	1
有害物质含量表	

安装方式

图2-1 壁装

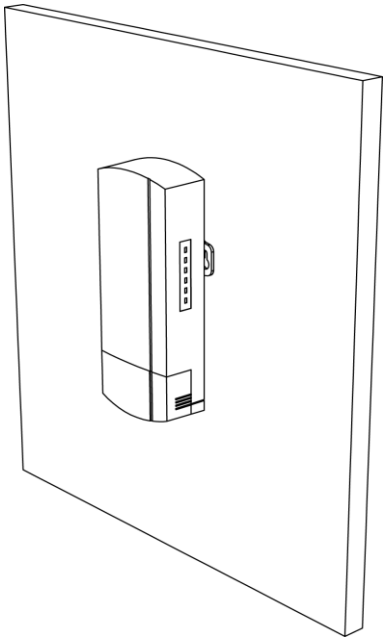
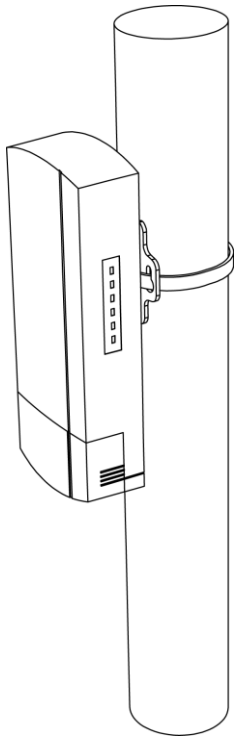


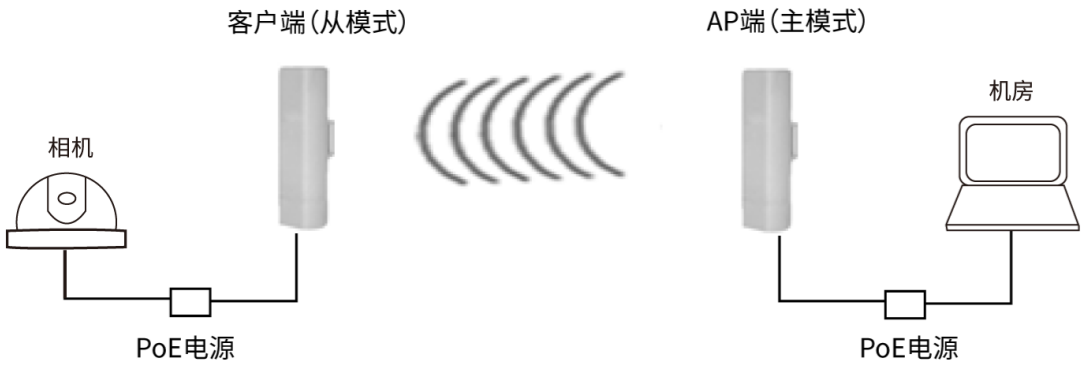
图2-2 柱装



2.2 设备连接

网络拓扑图

图2-3 网络拓扑图



设备连接示意图

图2-4 机房端连接

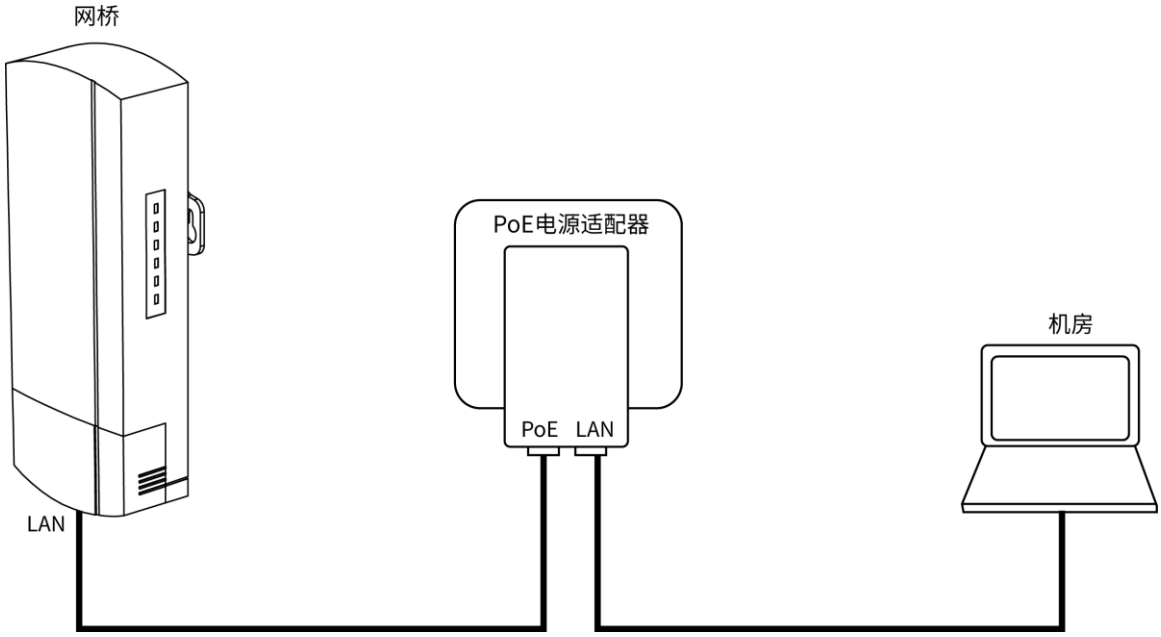
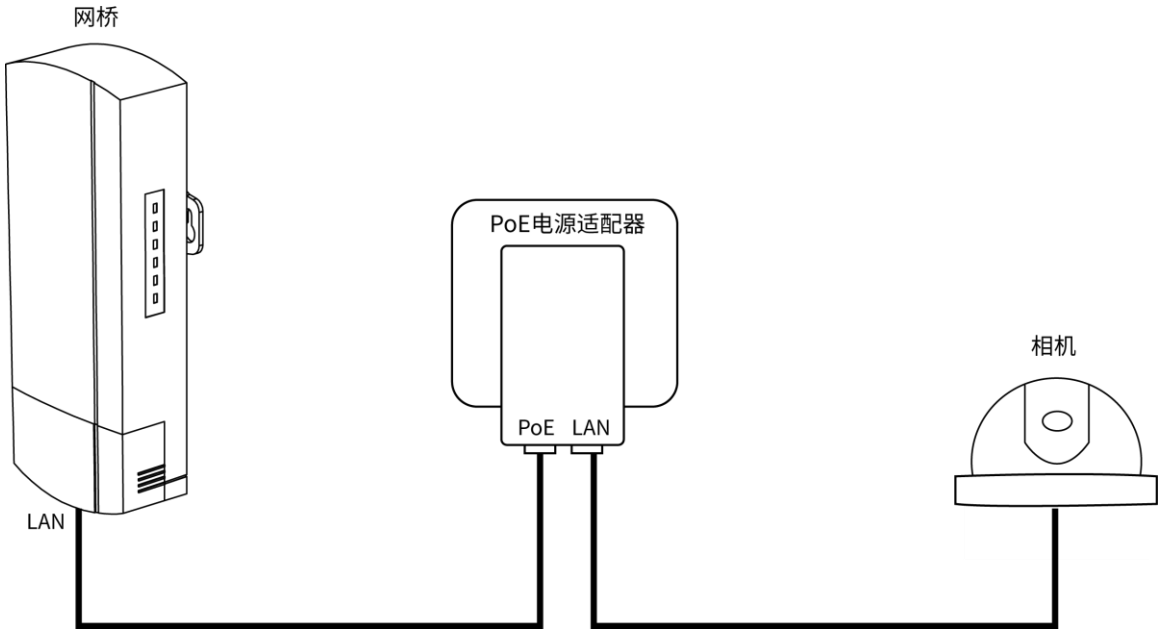


图2-5 相机端连接



第 3 章 基本配置

介绍通过WEB界面配置设备，包括配置设备主从模式、设置登录密码、升级固件、重启系统和恢复出厂设置等。

3.1 配置主从模式

前提条件

- 请确认PC与设备的LAN接口已连接。
- 已设置PC的IP地址与设备的IP地址在同一网段。

3.1.1 配置主模式

步骤1　打开IE浏览器，在地址栏输入主模式（机房端）设备IP地址（默认IP地址为192.168.1.35），按【Enter】键。

步骤2　输入密码，单击“登陆”。

说明

出厂默认密码为admin，建议设置高安全性密码并定期更改密码。

图3-1 登陆界面



步骤3　在WEB主界面，选择“系统模式 > 主模式”，单击“应用”。

图3-2 主模式



步骤4 在WEB主界面，选择“无线设置 > 基础设置”。

设置主模式设备的无线基本参数，单击“应用”。

说明

常用参数为SSID（Service Set Identifier，服务集标识）和密钥：默认SSID为Dahua_Wifi_MAC地址后六位，默认密钥为1234abcd。

图3-3 基础设置



步骤5 在WEB主界面，选择“网络设置”，输入主模式设备IP地址和子网掩码，单击“应用”。

图3-4 网络设置



3.1.2 配置从模式

步骤1 打开IE浏览器，在地址栏输入从模式（相机端）设备IP地址（默认IP地址为192.168.1.36），按【Enter】键。

步骤2 输入密码，单击“登陆”。

说明

出厂默认密码为admin，建议设置高安全性密码并定期更改密码。

图3-5 登陆界面



步骤3 在WEB主界面，选择“系统模式 > 从模式”。

在系统自动扫描出的主模式设备列表中，选择需要连接的设备，在设备操作栏单击“选择”。

说明

若扫描的列表中没有目标设备，可单击“重新扫描”。如果长时间无扫描结果，请确认该网桥是否支持WLAN基站或主模式设备当前的（频率）信道，另外请检查网桥与主模式设备的无线协议是否匹配，必要时恢复出厂设置后再设置连接。

步骤5　输入需要连接的主模式设备密钥，单击“应用”。

图3-6 设置从模式



3.2 管理员设置

步骤1　在WEB主界面，选择“系统设置 > 管理员设置”。

步骤2　设置管理员密码，单击“应用”。

图3-7 管理员设置



3.3 固件升级

步骤1　在WEB主界面，选择“系统设置 > 固件升级”。

步骤2　单击“选择”，选择升级文件。

步骤3　单击“升级”。

图3-8 固件升级



3.4 系统配置

步骤1　在WEB主界面，选择“系统设置 > 系统配置”。

步骤2　根据实际需要，单击“重启”，可重启系统；单击“恢复”，可恢复出厂设置。

图3-9 系统配置


系统状态
系统模式
网络设置
无线设置
系统设置
管理员设置
固件升级
系统配置
系统日志
定时重启
系统配置
重启系统
重启
恢复出厂设置
恢复

第 4 章 技术规格

表4-1 技术规格

参数	说明
CPU	660MHz
内存	64MB
FLASH	8MB
网络接口	1个LAN口
天线	1根定向天线
指示灯	2个配对灯/1个无线灯/1个LAN灯/1个电源灯
按钮	1个Reset按钮
电源输入	• DC 12V/1A 供电 • 24V POE供电
工作环境	• 工作温度：-10℃～+55℃ • 工作湿度：10%～90%RH 无凝结
存储环境	• 存储温度：-40℃～+75℃ • 存储湿度：5%～90%RH 无凝结

第 5 章 常见问题

1. **NVR端不能找到摄像头？**

   解决方法：PC连接上接NVR的交换机，ping摄像头端的网桥IP，如果能ping通则说明网桥节点没问题，排查其它网线接口是否接好。

2. **修改设备IP后忘记WEB登录IP地址？**

   解决方法：PC接上网桥LAN口，然后单击PC本地连接，查看自动获取到的网关地址即是网桥当前IP，或者按住复位键5秒松开进行复位，复位后的默认IP机房端设备为192.168.1.35，相机端设备为192.168.1.36。

附录1 法律声明

版权声明

© 2020 浙江大华技术股份有限公司。版权所有。
在未经浙江大华技术股份有限公司（下称“大华”）事先书面许可的情况下，任何人不能以任何形式复制、传递、分发或存储本文档中的任何内容。
本文档描述的产品中，可能包含大华及可能存在的第三人享有版权的软件。除非获得相关权利人的许可，否则，任何人不能以任何形式对前述软件进行复制、分发、修改、摘录、反编译、反汇编、解密、反向工程、出租、转让、分许可等侵犯软件版权的行为。

商标声明

- alhua、alhua、alhua、alhua、HDCVI是浙江大华技术股份有限公司的商标或注册商标。
- HDMI标识、HDMI和High-Definition Multimedia Interface 是HDMI Licensing LLC的商标或注册商标。本产品已经获得HDMI Licensing LLC授权使用HDMI技术。
- VGA是IBM公司的商标。
- Windows标识和Windows是微软公司的商标或注册商标。
- 在本文档中可能提及的其他商标或公司的名称，由其各自所有者拥有。

责任声明

- 在适用法律允许的范围内，在任何情况下，本公司都不对因本文档中相关内容及描述的产品而产生任何特殊的、附随的、间接的、继发性的损害进行赔偿，也不对任何利润、数据、商誉、文档丢失或预期节约的损失进行赔偿。
- 本文档中描述的产品均“按照现状”提供，除非适用法律要求，本公司对文档中的所有内容不提供任何明示或暗示的保证，包括但不限于适销性、质量满意度、适合特定目的、不侵犯第三方权利等保证。

出口管制合规声明

大华遵守适用的出口管制法律法规，并且贯彻执行与硬件、软件、技术的出口、再出口及转让相关的要求。就本手册所描述的产品，请您全面理解并严格遵守国内外适用的出口管制法律法规。

隐私保护提醒

您安装了我们的产品，您可能会采集人脸、指纹、车牌、邮箱、电话、GPS等个人信息。在使用产品过程中，您需要遵守所在地区或国家的隐私保护法律法规要求，保障他人的合法权益。如，提供清晰、可见的标牌，告知相关权利人视频监控区域的存在，并提供相应的联系方式。

关于本文档

- 本文档供多个型号产品使用，产品外观和功能请以实物为准。
- 如果不按照本文档中的指导进行操作而造成的任何损失由使用方自己承担。
- 本文档会实时根据相关地区的法律法规更新内容，具体请参见产品的纸质、电子光盘、二维码或官网，如果纸质与电子档内容不一致，请以电子档为准。
- 本公司保留随时修改本文档中任何信息的权利，修改的内容将会在本文档的新版本中加入，恕不另行通知。
- 本文档可能包含技术上不准确的地方、或与产品功能及操作不相符的地方、或印刷错误，以公司最终解释为准。
- 如果获取到的PDF文档无法打开，请使用最新版本或最主流的阅读工具。

附录2 网络安全声明和建议

安全声明

- 若您将产品接入互联网需自担风险，包括但不限于可能遭受网络攻击、黑客攻击、病毒感染等，请您加强网络、设备数据和个人信息等的保护，采取保障设备网络安全的必要措施，包括但不限于修改出厂默认密码并使用强密码、定期修改密码、将固件更新至最新版本等。本公司不对因此造成的产品工作异常、信息泄露等问题承担任何责任，但本公司会提供产品相关安全维护。
- 在适用法律未明令禁止的程度下，对于因使用或无法使用本产品或服务而引起的任何利润、收入、销售损失、数据丢失或采购替代商品或服务的成本、财产损害、人身伤害、业务中断、商业信息损失，或者任何特殊的、直接的、间接的、附带的、经济性、覆盖性、惩罚性、特殊或从属损害，无论是基于何种责任理论（合同、侵权、过失或其他），本公司及其员工、许可方或附属公司都不承担赔偿责任，即使其已被告知存在此种损害的可能性也是如此。某些司法管辖区不允许对人身伤害、附带或从属损害等进行责任限制，则此限制可能不适用于您。
- 本公司对您的所有损害承担的总责任限额（除了因本公司过失导致人身伤亡的情况，需遵循适用法律规定）不超过您购买本公司产品所支付的价款。

安全建议

保障设备基本网络安全的必须措施：

1. **使用复杂密码**

   请参考如下建议进行密码设置：

   - 长度不小于8个字符。
   - 至少包含两种字符类型，字符类型包括大小写字母、数字和符号。
   - 不包含账户名称或账户名称的倒序。
   - 不要使用连续字符，如123、abc等。
   - 不要使用重叠字符，如111、aaa等。

2. **及时更新固件和客户端软件**

   - 按科技行业的标准作业规范，设备的固件需要及时更新至最新版本，以保证设备具有最新的功能和安全性。设备接入公网情况下，建议开启在线升级自动检测功能，便于及时获知厂商发布的固件更新信息。
   - 建议您下载和使用最新版本客户端软件。

增强设备网络安全的建议措施：

1. **物理防护**

   建议您对设备（尤其是存储类设备）进行物理防护，比如将设备放置在专用机房、机柜，并做好门禁权限和钥匙管理，防止未经授权的人员进行破坏硬件、外接设备（例如U盘、串口）等物理接触行为。

2. **定期修改密码**

建议您定期修改密码，以降低被猜测或破解的风险。

3. **及时设置、更新密码重置信息**

   设备支持密码重置功能，为了降低该功能被攻击者利用的风险，请您及时设置密码重置相关信息，包含预留手机号/邮箱、密保问题，如有信息变更，请及时修改。设置密保问题时，建议不要使用容易猜测的答案。

4. **开启账户锁定**

   出厂默认开启账户锁定功能，建议您保持开启状态，以保护账户安全。在攻击者多次密码尝试失败后，其对应账户及源IP将会被锁定。

5. **更改HTTP及其他服务默认端口**

   建议您将HTTP及其他服务默认端口更改为1024～65535间的任意端口，以减小被攻击者猜测服务端口的风险。

6. **使能HTTPS**

   建议您开启HTTPS，通过安全的通道访问Web服务。

7. **MAC地址绑定**

   建议您在设备端将其网关设备的IP与MAC地址进行绑定，以降低ARP欺骗风险。

8. **合理分配账户及权限**

   根据业务和管理需要，合理新增用户，并合理为其分配最小权限集合。

9. **关闭非必需服务，使用安全的模式**

   - 如果没有需要，建议您关闭SNMP、SMTP、UPnP等功能，以降低设备面临的风险。
   - 如果有需要，强烈建议您使用安全的模式，包括但不限于：
     - SNMP：选择SNMP v3，并设置复杂的加密密码和鉴权密码。
     - SMTP：选择TLS方式接入邮箱服务器。
     - FTP：选择SFTP，并设置复杂密码。
     - AP热点：选择WPA2-PSK加密模式，并设置复杂密码。

10. **音视频加密传输**

    如果您的音视频数据包含重要或敏感内容，建议启用加密传输功能，以降低音视频数据传输过程中被窃取的风险。

11. **安全审计**

    - 查看在线用户：建议您不定期查看在线用户，识别是否有非法用户登录。
    - 查看设备日志：通过查看日志，可以获知尝试登录设备的IP信息，以及已登录用户的关键操作信息。

12. **网络日志**

    由于设备存储容量限制，日志存储能力有限，如果您需要长期保存日志，建议您启用网络日志功能，确保关键日志同步至网络日志服务器，便于问题回溯。

13. **安全网络环境的搭建**

    为了更好地保障设备的安全性，降低网络安全风险，建议您：

    - 关闭路由器端口映射功能，避免外部网络直接访问路由器内网设备的服务。
    - 根据实际网络需要，对网络进行划区隔离：若两个子网间没有通信需求，建议使用VLAN、网闸等方式对其进行网络分割，达到网络隔离效果。
    - 建立802.1x接入认证体系，以降低非法终端接入专网的风险。
    - 开启设备IP/MAC地址过滤功能，限制允许访问设备的主机范围。

更多内容

请访问大华官网安全应急响应中心，获取安全公告和最新的安全建议。

「让社会更安全 让生活更智能」

ENABLING A SAFER SOCIETY AND SMARTER LIVING

浙江大华技术股份有限公司 | 地址：杭州市滨江区滨安路1187号 | 网址：www.dahuatech.com | 服务热线：400-672-8166