

嵌入式综合管理系统

WEB 使用手册

广州市瑞东电子科技有限公司

目 录

一.	WEB 概述.....	1
1.1	概述.....	1
1.2	主机与设备连接示意图.....	3
二.	操作流程说明.....	4
2.1	WEB 操作.....	4
2.1.1	打开 IE 浏览器.....	4
2.1.2	登录账号.....	5
2.2	SNMP 配置.....	6
2.2.1	添加告警目标主机.....	6
三.	WEB 界面介绍.....	6
3.1	设备信息.....	7
3.1.1	刷新视图.....	7
3.1.2	机箱信息.....	7
3.1.3	单元盘列表.....	8
3.1.4	设备名称/类型.....	9
3.1.5	更改光模块波长.....	10
3.1.6	更改模块发射光功率.....	10
3.1.7	更改光模块业务模式.....	10
3.2	告警管理.....	11
3.2.1	当前告警.....	11
3.2.2	历史告警.....	13
3.2.3	告警策略.....	14
3.2.4	告警配置.....	15
3.2.5	告警发送模式.....	15
3.3	系统配置.....	16
3.3.1	系统时间.....	16
3.3.2	网络配置.....	17
3.3.3	HTTP 配置.....	18
3.3.4	Websocket 配置.....	18
3.3.5	级联卡映射.....	19
3.3.6	网管卡配置.....	20
3.4	SNMP 配置.....	21
3.4.1	共同体配置.....	21
3.4.2	告警目标主机配置.....	21
3.4.3	连通性测试.....	24
3.4.4	版本配置.....	24
3.5	系统维护.....	25
3.5.1	进程查看.....	25
3.5.2	进程启动配置.....	26
3.5.3	网管卡升级.....	28
3.5.4	业务卡升级.....	29
3.5.5	恢复出厂设置.....	29

3.5.6	重启系统.....	34
3.6	安全管理.....	34
3.6.1	防火墙白名单管理.....	34
3.6.2	端口转发.....	38
3.6.3	用户管理.....	39
3.6.4	修改密码.....	42
3.6.5	退出登录.....	42
3.7	日志管理.....	42
3.7.1	异常日志.....	42
3.7.2	操作日志.....	43
3.7.3	日志配置.....	43

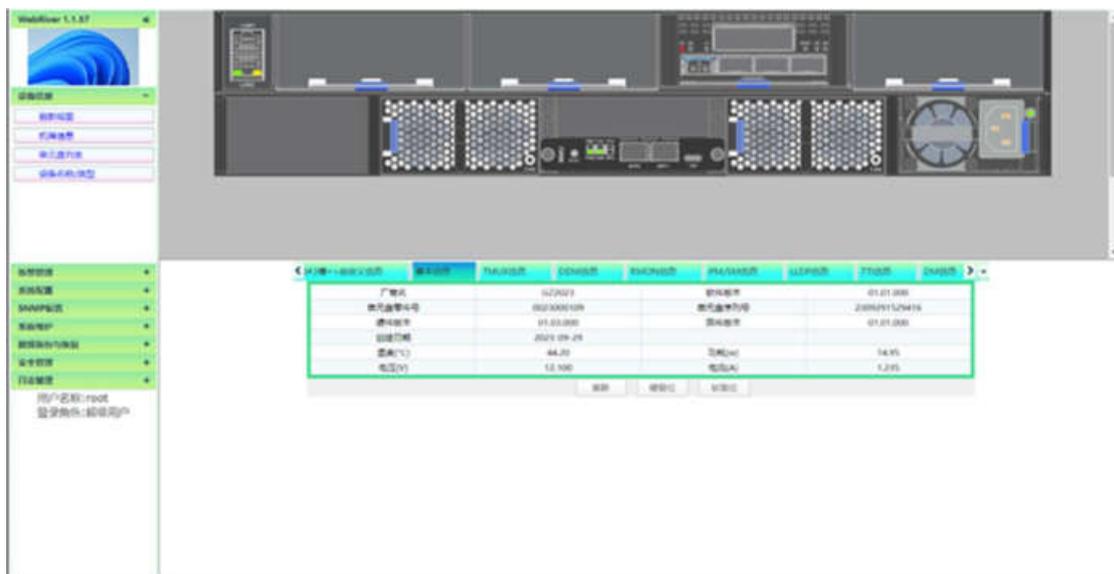
一.WEB 概述

1.1 概述

网管管理系统是一个综合网络信息处理平台(WEB),提供可视化界面,监控设备运行状况,快速定位故障设备与推送故障信息等实用功能。以下说明以 DCI-BOX 设备为例,其他设备也一致。

(1) 设备状态查看:

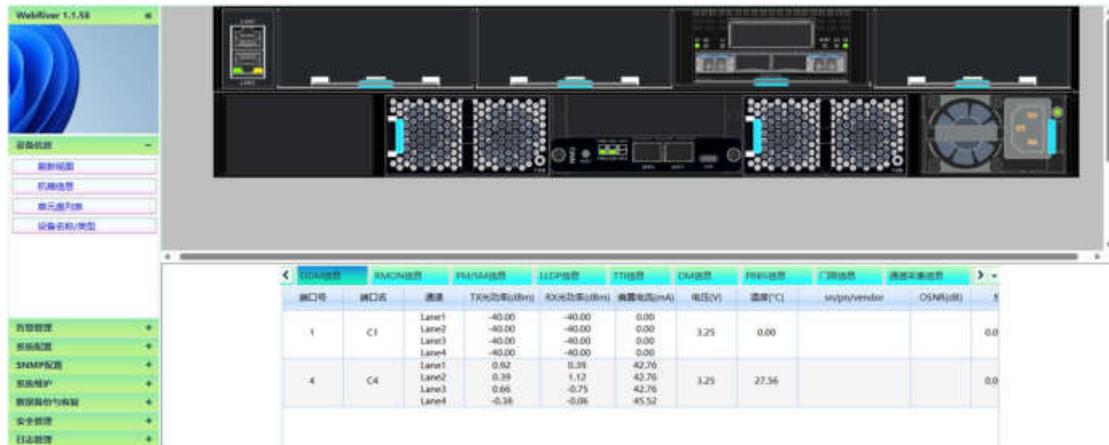
☆ 查看板卡的状态信息:



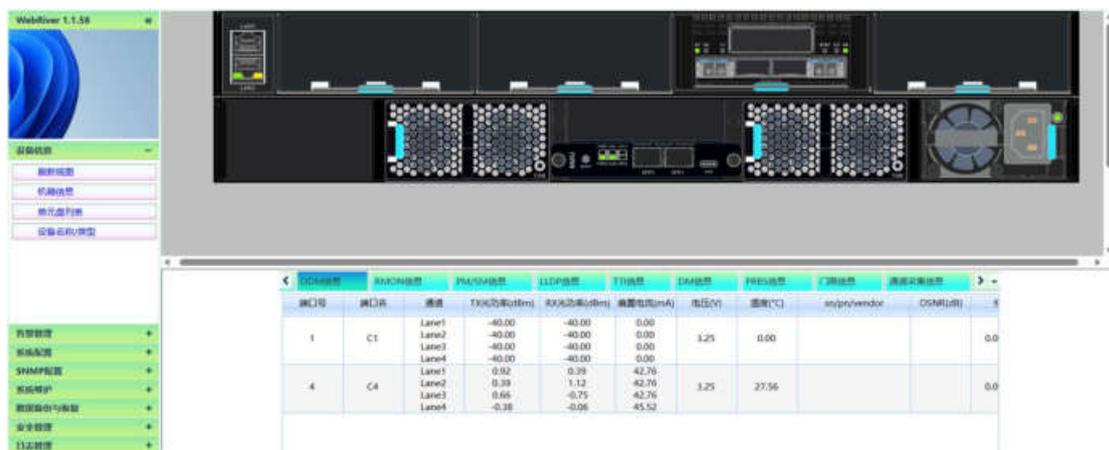
☆ 查看板卡的光功率信息:



☆ 查看板卡的工作状态：



☆ 查看光模块的状态：



(2) 告警管理：

☆ 显示告警；

☆ 实时记录设备所产生的的告警；

(3) 安全管理：

☆ 提供登陆账户角色的操作权限限制，能根据级别来分配可操作访问内容，杜绝可能发生的恶意破坏通讯秩序的行为；

☆ 提供添加新用户新权限的功能

(4) 日志管理：

☆ 实时记录登陆软件的主机与用户；

☆ 实时记录操作 WEB 功能与内容的主机与用户；

(5) 其他功能：

☆ 直观查看设备运行情况；

☆ 提供实时修改配置功能；

☆ 一键设备状态；

1.2 主机与设备连接示意图

使用网线把网管卡的“RJ45”接口和交换机(个人 PC)连接起来,此时“RJ45”接口的指示灯  亮起来或者闪烁,如果“RJ45”接口指示灯不闪烁不亮则说明网线无法通信需排除连接问题。

确定设备和个人 PC 通过网线正常连接后,在 IE 浏览器输入设备 IP (设备出厂 IP:192.168.1.228),输入账号密码(默认账号有 root、admin、guest,密码分别对应为 root@8989、admin@8989、guest@8989)进入设备界面。

每个网管上共有 4 个接口能进行通信,分别是两个光口和两个电口(新款的设备是 3 个光口 2 个电口);通过连接的方式不同,每个网管设备都可以使用 1 个网口(光口)连接上层设备,并使用另一个网口(光口)连接下层设备;两个网口(光口)间提供数据交换与拓展连接的作用,由于光口有百兆千兆的速率,所以当前只能用百兆的去连接百兆的光口,千兆的去连接千兆的光口进行通信连接。

通过网管之间的串联,使用一根网线(光纤)便可以访问所有串联的设备,但最终所有的设备不可串成环,否则会导致网络瘫痪!

下图为接线的示意图,蓝色(红色)为网线,黄色为光缆连接。



图 1-1 1U 设备的网口连接示意图

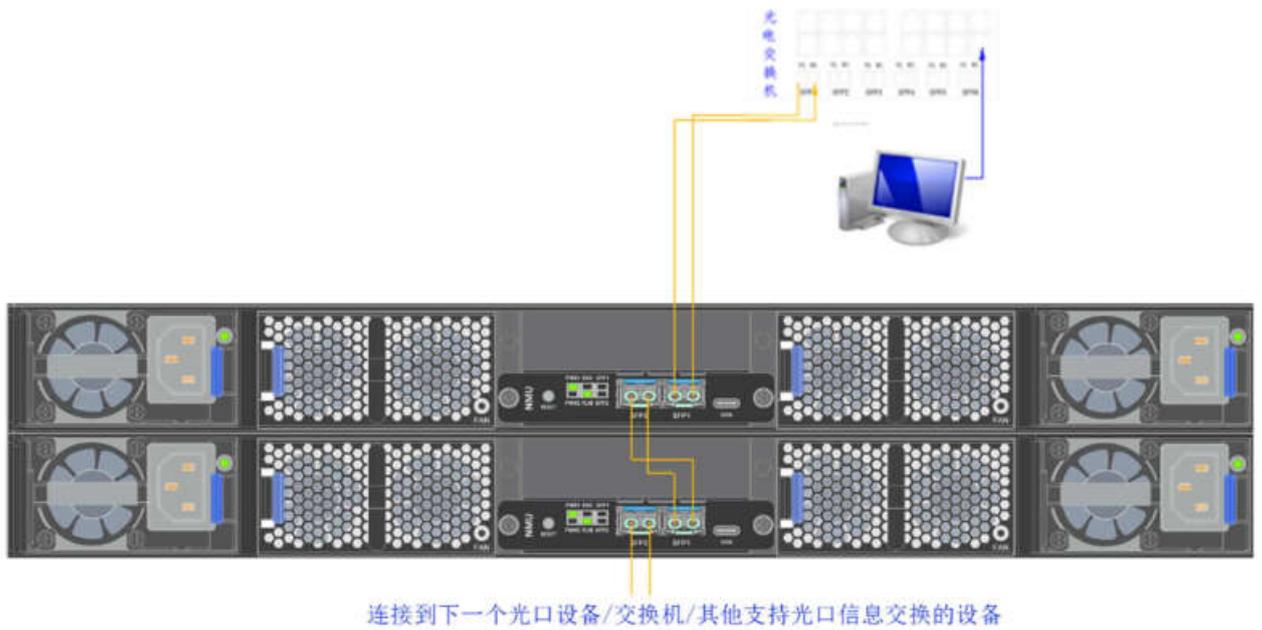


图 1-2 1U 设备的光口连接示意图

二. 操作流程说明

2.1 WEB 操作

注：设备与个人 PC 必须通过网络或者无线连接，如果无法访问，建议使用 PING 工具进行连接判断，WEB 的其他功能介绍请查看附录一的详细介绍

2.1.1 打开 IE 浏览器

注：建议使用 IE 浏览器，并使用 IE8.0 以上的版本。

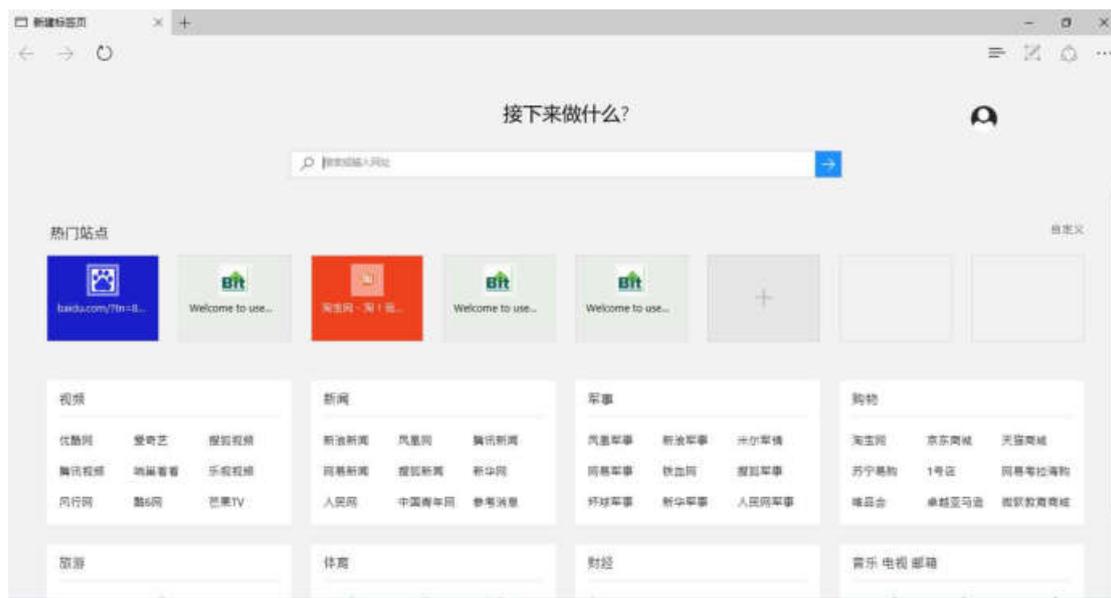


图 1-3 浏览器界面

2.1.2 登录账号

在网址框中输入“192.168.1.228”回车，在弹出的对话框中输入默认账号密码“admin”回车

注：出厂设备默认 IP 为 192.168.1.228，登录默认账号有 root、admin、guest，密码分别对应为 root@8989、admin@8989、guest@8989，如果修改了 IP、账号、密码则需要使用新的 IP、账号、密码登录。



图 2-1 验证账号密码

2.2 SNMP 配置

在 WEB 界面中点击“SNMP 配置”。



图 2-2 WEB 功能界面

2.2.1 添加告警目标主机

在功能菜单中点击“告警目标主机配置”，点击  增加 输入当前使用的个人 PC 的 IP 地址，点击  提交 保存。



图 2-3 SNMP 目标主机设置

三.WEB 界面介绍

注：从界面显示区可以显示 1U 的设备，当前以 1U 作为说明，板卡功能说明参考下文。



图 3-1 网管界面

☆ WEB 版本显示:

显示网管界面的功能版本，通过版本号可以快捷的定位信息。

☆ 功能选择区:

选择网管功能，进行设备的管理与设置。

☆ 界面显示区:

实时同步显示实体设备的界面状态显示，更直观的获取设备运行状态信息。

☆ 功能操作区:

操作功能视图区域，功能内容的拓展。

3.1 设备信息

设备信息

点击该功能可进入查看机箱系统信息的操作和设置，在此功能里面可以查看系统资讯和系统运行的情况，也可以一键刷新同步设备界面和对设备名称及类型的设置。

3.1.1 刷新视图

刷新视图

该功能是一键刷新同步设备界面显示，刷新的是界面显示区的显示界面，如果插拔光模块或者需要查看状态灯，可使用该刷新功能刷新界面的实际显示。

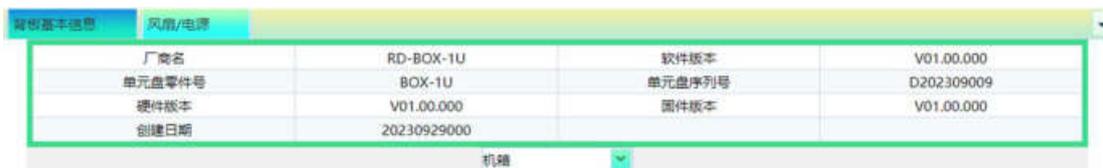
3.1.2 机箱信息

机箱信息

点击该功能可进入查看系统硬件框架信息和版本和风扇/电源的运行状态，通过这些硬件信息可以给维护和排查带来更多有用的资料，同时也可以可以在背板基本信息一栏进行修改自定义信息。通过这些硬件信息可以给维护和排查带来更多有用的资料。

3.1.2.1 背板基本信息设置

该功能提供设置系统的名称，以便更加容易定位到设备的位置。



厂商名	RD-BOX-1U	软件版本	V01.00.000
单元盘零件号	BOX-1U	单元盘序列号	D202309009
硬件版本	V01.00.000	固件版本	V01.00.000
创建日期	20230929000		

图 3-2 背板基本信息

3.1.2.2 风扇/电源



图 3-3 风扇/电源

3.1.3 单元盘列表



点击该功能可进入查看设备内所使用的单元盘板卡的槽位、模块型号、模块序列号、创建日期、硬件版本和固件版本等信息，通过这些硬件信息可以给维护和排查带来更多有用的资料。

槽位号	厂商名	模块序列号	模块零件号	创建日期	硬件版本	固件版本
0	RD-BOX-1U	D202309009	BOX-1U	20230929000	V01.00.000	V01.00.000
6	GLOBAL	1907221529511	1020000240	2022-07-20	01.01.000	1.1.57

关闭

图 3-4 单元盘列表

3.1.4 设备名称/类型

设备名称/类型

点击该功能可进入设置设备名称、设备类型和网管卡槽位号，其中网管卡槽位号的选择被设备类型所限定。设备名称输入名字后，点击应用保存，在 WEB 的界面左上角会显示修改后的位置。

设备名称/类型
×

设备名称	<input type="text" value="WebRiver"/>
页面标题	<input type="text" value="Web NMS"/>
设备类型	<input type="text" value="自动"/>
网管卡槽位号	<input type="text" value="自动"/>

图 3-5 设备名称/类型

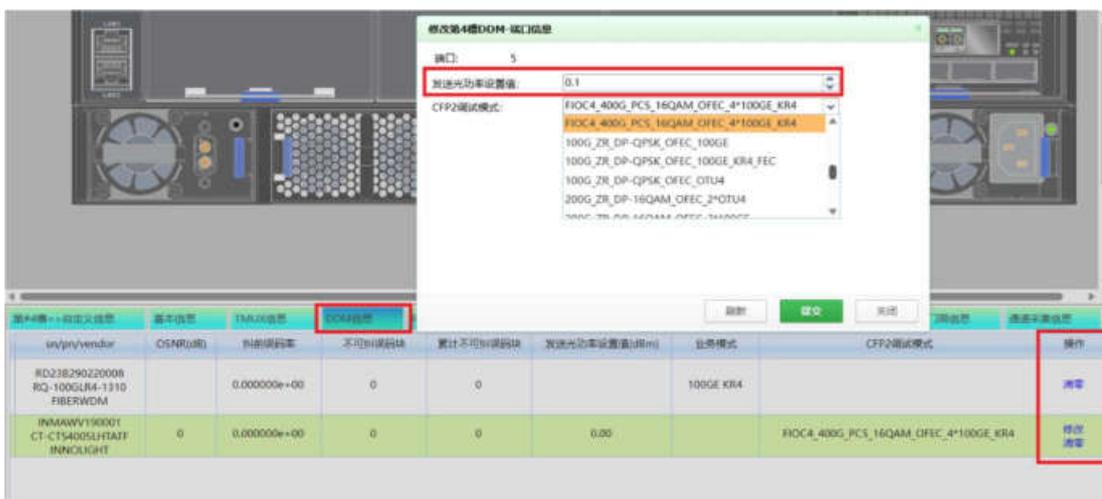
3.1.5 更改光模块波长

根据实际使用需求更改波长，点击板卡视图，在菜单栏点击“TMUX 信息”，在信息表格最右侧点击“修改”，在弹出窗口中勾选“是否设置”，根据需要更改波长之后点击提交生效。



3.1.6 更改模块发射光功率

CFP2 光模块可以修改发射光功率



点击板卡视图，在菜单栏中点击“DDM 信息”，在信息表格最右侧点击修改选项，在弹出的窗口中可以设置发射光功率值，点击提交生效。

3.1.7 更改光模块业务模式

CFP2 光模块可以修改的业务模式有：带 FEC、不带 FEC 和 OTU4 等，可根据不同的 CFP2 光模块进行设置。



点击板卡视图，在菜单栏中点击“DDM 信息”，在信息表格最右侧点击修改选项，在弹出的窗口中可以设置 CFP2 调试模式，根据使用光模块的型号选择对应的模式点击提交，其中模式后缀带“KR4”或“FEC”即支持 FEC 模式；模式后缀为 100GE 的是不带 FEC。

3.2 告警管理

告警管理

该功能是提供所有的操作告警记录，对于一些被定义为告警操作的行为在完成之后将以文字显示的方式提醒操作者，以便在后面的排查中根据告警信息获取当时的操作行为。产生告警后，经操作者或者上级监控者的确定和清除告警，可以把当前产生的告警转移到历史告警中去，以便日后的查阅。以及可以对告警策略和配置进行相应的选择和设置。

3.2.1 当前告警

当前告警

当前告警是指设备在最近的时间内产生的告警信息，并且没有经过维护人员的清除和确认，只要告警没经过清除和确认，就一直都处于当前告警的分类中，除非当前告警的数量达到系统的容纳数才被移除。

位置	告警信息	告警名称	告警状态	发生时间	清除时间	确认时间	告警级别	告警类型	操作
PORT-1-4-C4 Lane4	输入光功率过期	TCA_OPT_INPUT_POWER	已清除未确认	2023-08-16 10:53:20	2023-08-16 10:53:30		主要告警	LOCAL	清除 确认
PORT-1-4-C4 Lane1	输入光功率过期	TCA_OPT_INPUT_POWER	已清除未确认	2023-08-16 10:53:20	2023-08-16 10:53:30		主要告警	LOCAL	清除 确认
PORT-1-4-C4 Lane2	输入光功率过期	TCA_OPT_INPUT_POWER	已清除未确认	2023-08-16 10:53:20	2023-08-16 10:53:30		主要告警	LOCAL	清除 确认
PORT-1-4-C4 Lane3	输入光功率过期	TCA_OPT_INPUT_POWER	已清除未确认	2023-08-16 10:53:20	2023-08-16 10:53:30		主要告警	LOCAL	清除 确认
PORT-1-4-C4 Lane1	接收信号丢失	RX_LOS	已清除未确认	2023-08-16 10:53:20	2023-08-16 10:53:30		紧急告警	LOCAL	清除 确认
PORT-1-4-C4 Lane4	接收信号丢失	RX_LOS	已清除未确认	2023-08-16 10:53:20	2023-08-16 10:53:30		紧急告警	LOCAL	清除 确认
PORT-1-4-C4 Lane1	接收信号丢失	RX_LOS	已清除未确认	2023-08-16 10:53:20	2023-08-16 10:53:30		紧急告警	LOCAL	清除 确认
PORT-1-4-C4 Lane2	接收信号丢失	RX_LOS	已清除未确认	2023-08-16 10:53:20	2023-08-16 10:53:30		紧急告警	LOCAL	清除 确认
PORT-1-4-C4	以太网物理端口信号丢失	ETH_LOS	未清除未确认	2023-08-16 10:53:18			紧急告警	ETH	清除 确认
PORT-1-4-C4	以太网物理端口信号丢失	ETH_LOS	已清除未确认	2023-08-15 10:39:30	2023-08-15 10:39:35		紧急告警	ETH	清除 确认
PORT-1-4-C4	输入总功率过期	TCA_OPT_TOTAL_INPUT_P	未清除未确认	2023-08-15 10:39:28			主要告警	LOCAL	清除 确认
PORT-1-4-C4	输出总功率过期	TCA_OPT_TOTAL_OUTPUT_	已清除未确认	2023-08-15 10:39:28	2023-08-15 10:39:30		次要告警	LOCAL	清除 确认
PORT-1-4-C4 Lane4	输入光功率过期	TCA_OPT_INPUT_POWER	已清除未确认	2023-08-15 10:39:28	2023-08-15 10:39:35		主要告警	LOCAL	清除 确认
PORT-1-4-C4 Lane1	输入光功率过期	TCA_OPT_INPUT_POWER	已清除未确认	2023-08-15 10:39:28	2023-08-15 10:39:35		主要告警	LOCAL	清除 确认
PORT-1-4-C4 Lane2	输入光功率过期	TCA_OPT_INPUT_POWER	已清除未确认	2023-08-15 10:39:28	2023-08-15 10:39:35		主要告警	LOCAL	清除 确认
PORT-1-4-C4 Lane3	输入光功率过期	TCA_OPT_INPUT_POWER	已清除未确认	2023-08-15 10:39:28	2023-08-15 10:39:35		主要告警	LOCAL	清除 确认
PORT-1-4-C4 Lane1	接收信号丢失	RX_LOS	已清除未确认	2023-08-15 10:39:28	2023-08-15 10:39:35		紧急告警	LOCAL	清除 确认
PORT-1-4-C4 Lane4	接收信号丢失	RX_LOS	已清除未确认	2023-08-15 10:39:28	2023-08-15 10:39:35		紧急告警	LOCAL	清除 确认
PORT-1-4-C4 Lane1	接收信号丢失	RX_LOS	已清除未确认	2023-08-15 10:39:28	2023-08-15 10:39:35		紧急告警	LOCAL	清除 确认
PORT-1-4-C4 Lane3	接收信号丢失	RX_LOS	已清除未确认	2023-08-15 10:39:28	2023-08-15 10:39:35		紧急告警	LOCAL	清除 确认
PORT-1-4-C4 Lane2	接收信号丢失	RX_LOS	已清除未确认	2023-08-15 10:39:28	2023-08-15 10:39:35		紧急告警	LOCAL	清除 确认
PORT-1-4-C3	以太网物理端口信号丢失	ETH_LOS	已清除未确认	2023-08-15 10:28:32	2023-08-15 10:28:41		紧急告警	ETH	清除 确认

图 3-6 当前告警主界面

3.2.1.1 当前告警的名词说明

位置：指在设备内部定义的位置，如光口 1，SFP2，对应的都是设备内部的端口。

告警信息：指提醒的信息，如“发送光功率偏低（-11.1）”。

告警状态：如果告警只清除未确认或者确认未清除，则该位置显示对应的信息。

发生时间：发生该告警的记录时间。

清除时间：操作“清除”功能的时间。

确认时间：操作“确认”功能的时间。

告警级别：提示该信息的严重或者重要的级别。

告警原因：触发产生该变化的告警信息原因。

操作：单个告警信息的清除和确认功能。

起始日期：选择要查询某段时间内告警信息的开始时间。

截止日期：选择要查询某段时间内告警信息的结束时间。

槽位号：显示“位置”为槽位号的告警信息。

查询：显示告警信息。

重置：清空起始日期、截止日期和槽位号数据。

按日期清除：清除从起始日期到截止日期时间内的告警信息。

按日期确认：确认从起始日期到截止日期时间内的告警信息。

清除勾选项：清除所勾选的告警信息。

确认勾选项：确认所勾选的告警信息。

（注：点击列表头可以对当前列表框数据进行排序，按首字母、数字递增或递减排序）

3.2.1.2 当前告警操作说明

提供了查询条件和快速清除告警信息/确定告警信息。

根据个人需求去对单条告警或者全部告警去筛选、清除和确认

3.2.2 历史告警

历史告警

所有被清除并确认的告警(处理后的告警)都会移入该栏目,如果在历史告警中删除全部告警,则无法再从系统中查找删除后的告警信息。



图 3-7 历史告警主界面

3.2.2.1 历史告警名词说明:

位置: 指在设备内部定义的位置,如光口 1, SFP2, 对应的都是设备内部的端口。

告警信息: 指提醒的信息,如“发送光功率偏低(-11.1)”。

告警状态: 如果告警只清楚未确认或者确认未清楚,则该位置显示对应的信息。

发生时间: 发生该告警的记录时间。

清除时间: 操作“清除”功能的时间。

确认时间: 操作“确认”功能的时间。

告警级别: 提示该信息的严重或者重要的级别。

告警原因: 触发产生该变化的告警信息原因。

删除: 单个告警信息的删除功能。

起始日期: 选择要查询某段时间内告警信息的开始时间。

截止日期: 选择要查询某段时间内告警信息的结束时间。

槽位号: 显示“位置”为槽位号的告警信息。

查询: 显示告警信息。

重置: 清空起始日期、截止日期和槽位号数据。

按日期删除: 删除从起始日期到截止日期时间内的告警信息。

删除勾选项: 删除所勾选的告警信息。

(注：点击列表头可以对当前列表框数据进行排序，按首字母、数字递增或递减排序)

3.2.2.2 历史告警操作说明：

提供了查询条件和快速删除告警信息。

根据个人需求去对单条告警或者全部告警去筛选和删除。

3.2.3 告警策略



根据客户需求屏蔽其他不需要的告警，提高维护专注性。

告警代码	告警信息	物理实体	告警级别	是否发送?	是否保存?	屏蔽槽位	操作
121	Power supply abnormal	Power supply	次要告警	发送	保存		
123	Fan locked-rotor	Fan	次要告警	发送	保存		
125	Fan communication interrupt	Fan	主要告警	发送	保存		
127	Fan abnormal speed	Fan	主要告警	发送	保存		
129	Fan failure	Fan	主要告警	发送	保存		
2001	Ethernet physical port signal	Optical port	紧急告警	发送	保存		
2003	CRC error packet over limit	Optical port	次要告警	发送	保存		
2005	Sync lost	Optical port	紧急告警	发送	保存		
2007	Receiving bad packets over	Optical port	次要告警	发送	保存		
2009	Link local failure	Optical port	紧急告警	发送	保存		
2011	Link far end failure	Optical port	紧急告警	发送	保存		
2013	Excessive background error	Optical port	主要告警	发送	保存		
2015	RS frame loss	Optical port	紧急告警	发送	保存		
2017	JO mismatch	Optical port	次要告警	发送	保存		
2019	RS_DEG	Optical port	主要告警	发送	保存		
2021	MS_AIS	Optical port	紧急告警	发送	保存		
2023	MS_RDI	Optical port	次要告警	发送	保存		
2025	OTUK frame loss	Optical port	紧急告警	发送	保存		
2027	OTUK multiframe loss	Optical port	紧急告警	发送	保存		
2029	OTUK_AIS	Optical port	紧急告警	发送	保存		

显示从1到20, 总 162 条, 每页显示: 20

关闭

图 3-8 告警策略主界面

3.2.3.1 告警策略名词说明：

告警代码：告警信息的代码编号。

告警信息：指告警提醒的信息。

物理实体：告警信息来源的实体。

告警级别：告警信息根据轻重程度划分的级别。

是否发送？：当出现告警信息时是否发送提醒消息。

是否保存？：当出现告警信息时是否保存告警信息。

屏蔽槽位：屏蔽掉此种告警信息的槽位。

操作：提交保存和取消告警信息是否发送及是否保存。

3.2.3.2 告警策略操作说明

根据个人需求去选择关闭或打开一些告警信息的发送和保存的功能。

3.2.4 告警配置

告警策略

注：务必选择“是否保存告警”并打勾，否则没有告警，建议默认不去操作该功能。

告警配置主要是进行告警信息的设置，是否需要告警信息，保存每一条信息还是只保存最新的信息等；如果不需要告警信息，则系统发生的所有工作状态变化都不会有告警产生；如果选择了“相同位置相同告警只保存一次”那么系统就只会保存在相同位置相同告警产生的最新告警，详细说明请参考当前告警的名词说明；如果选择了保存每次告警，那么每一次发生的告警信息都会保存下来，直到系统超出了最大条数的限制，最大条数可设为 1000。

告警配置
✕

告警配置	
是否保存告警	<input checked="" type="checkbox"/>
保存每次告警	<input checked="" type="radio"/>
相同位置相同告警只保存一次	<input type="radio"/>
最大条数	<input style="width: 80%;" type="text" value="1000"/> ^ v
说明:配置后需要重启系统方能生效	

应用
刷新
关闭

图 3-9 告警配置设置

3.2.5 告警发送模式

告警发送模式

选择网管卡告警信息的发送模式，有 SNMP 或者 TCP 两种模式可选。一般常用 SNMP 模式发送。



图 3-10 告警发送模式

3.3 系统配置

系统配置

点击该功能可进入查看系统信息的操作和设置，在此功能里面可以查看系统时间的设置、网络地址的设置、HTTP 端口的配置、OBP 保护板的心跳设置和 UDP 配置等。

3.3.1 系统时间

系统时间

时间设置有两种设置的方法，一种是手动去设置，设置的时间来源可以获取当前电脑的电脑时间为设备时间，也可以根据当前时间计量单位设备的时间手动进行设置；另一种是设备自动向互联网获取时间，每隔 2 个小时进行更新一次，这种方法需要设备能够连接到外网进行通信。

由于设备自带的时钟供电电源的供电能力有限，所以设备在运输后时间可能会恢复系统初始时间，所以设备上电后需查看时间并修改时间，以便正常定位到告警发生记录的实际时间。

3.3.1.1 手动设置时间



图 3-11 手动设置时间

3.3.1.2 自动从互联网获取时间

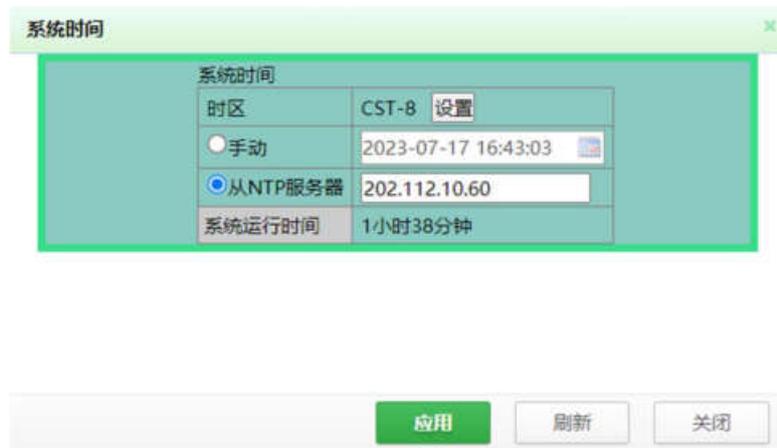
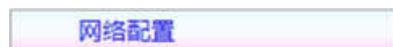


图 3-12 自动获取时间

3.3.2 网络配置



网络地址设置可以直接更改网管卡的 IP 地址、IPV6 地址、子网掩码和默认网关，点击“应用”保存更改，更改后需要重启网管卡系统方可有效。



图 3-13 网络配置

3.3.3 HTTP 配置

HTTP配置

网页 HTTP 的端口默认为 80，直接使用如 http://192.168.1.228 的地址即可登录 webs，如果 HTTP 端口更改过，登录 webs 时所使用的地址如 http://192.168.1.228:端口值。（注：不要选用一些常用软件或网页的端口，否则会造成端口冲突导致 webs 或软件无法使用。）



图 3-14 HTTP 配置

3.3.4 Websocket 配置

Websocket配置

Websocket 协议属于服务端推送技术，本质是一种应用层协议，可以实现持久连接的全双工双向通信。当设备产生告警信息时，会有弹窗提示告警信息，以及会在相应板卡识图的最顶端显示告警铃铛图标。



图 3-15 Websocket 配置

3.3.5 级联卡映射

级联卡映射

在主卡之下添加相关的级联网管卡，在单一主卡对主卡及其所有的级联卡进行管理，统一接收告警信息等。

注：通过级联卡映射界面给予作为主卡的网管卡附加 snmp 协议的级联卡，在使用网管软件时只需将主卡的数据导入即可得到相关级联设备。



图 3-16 级联卡映射

网管卡模式包括普通卡、主卡和级联卡，正常情况只需选择普通卡即可，当需要接通级联设别时则要在主卡上添加端口，映射到级联卡上去。

增加端口映射

协议: snmp

映射IP:

映射端口:

启用/禁用: 启用

提交 关闭

图 3-17 增加端口映射

端口映射的协议分别有 snmp、http、https、telnet、ssh 五种；

snmp 协议用于网管软件的级联设备；

http 和 https 协议用于网页端口映射，比如主卡 IP 地址为 192.168.1.227，添加了 http 协议的级联卡，IP 地址为 192.168.2.150，映射端口为 1630，在网页上只需输入 192.168.1.227:1630 即可访问 IP 地址 192.168.2.150。

3.3.6 网管卡配置

网管卡配置

配置网管卡的串口设置和 telnet 设置。

串口设置：机箱背板默认只能读取一个网管卡的串口信息，如果同时读取第二个网管卡会很慢或者串口信息错乱，所以可以选择更改串口数据的模式为双卡后才同时读取同一个背板上的两个网管卡的串口信息。

telnet 设置：限制同时打开 telnet 客户端界面的数量。

网管卡配置

-----telnet-----

最大连接数 5

-----ccenter-----

从YANG恢复板卡数据 是

应用 刷新 关闭

图 3-18 网管卡配置

3.4 SNMP 配置

SNMP配置

该配置主要是配置告警目标主机，便于使用网管软件去管理设备的时候网管软件所在的主机可以获取到实时的设备告警信息。

3.4.1 共同体配置

共同体配置

网管卡共同体配置默认“读团体名”为 public，“写团体名”为 private。共同体配置有所修改的话，网管软件将无法正常显示该设备视图。



图 3-19 共同体配置

3.4.2 告警目标主机配置

告警目标主机配置

为网管软件增加、修改或删除告警目标主机，网管软件的告警目标主机会随着 webs 的告警目标主机配置来更新配置数据。还可以向网管软件发送 SNMP 告警测试。



图 3-20 告警目标主机配置

3.4.2.1 告警目标主机的名词说明

增加：增加告警目标主机。

修改：修改告警目标主机。

删除勾选：删除所勾选的告警目标主机。

🚨：发送 SNMP 告警测试。

🔔：发送 UDP 告警测试。

✏️：修改告警目标主机。

🗑️：删除告警目标主机。

3.4.2.2 告警目标主机的操作说明

增加：点击“增加”，输入目标地址名称和 IP 地址，UDP 端口默认为 9162，选择“启用”，然后点击“提交”保存。

图 3-21 添加告警目标主机

修改：点击，输入要修改的数据，点击“提交”保存修改。

修改告警目标主机

目标主机名称:

目标主机IP地址:

UDP端口:

启用/禁用:

ip类型:

图 3-22 修改告警目标主机

删除：点击“删除勾选”或，弹窗提示后，再点击“是”后删除目标告警主机。

告警目标主机配置

增加

ID	目标主机名称	目标主机IP地址	UDP端口	启用/禁用	操作
1	1	192.168.1.22	9162	启用	  
2	2		9162	启用	  

提示

告警目标主机:192.168.1.128,确定要删除吗?

图 3-23 删除告警目标主机

3.4.3 连通性测试

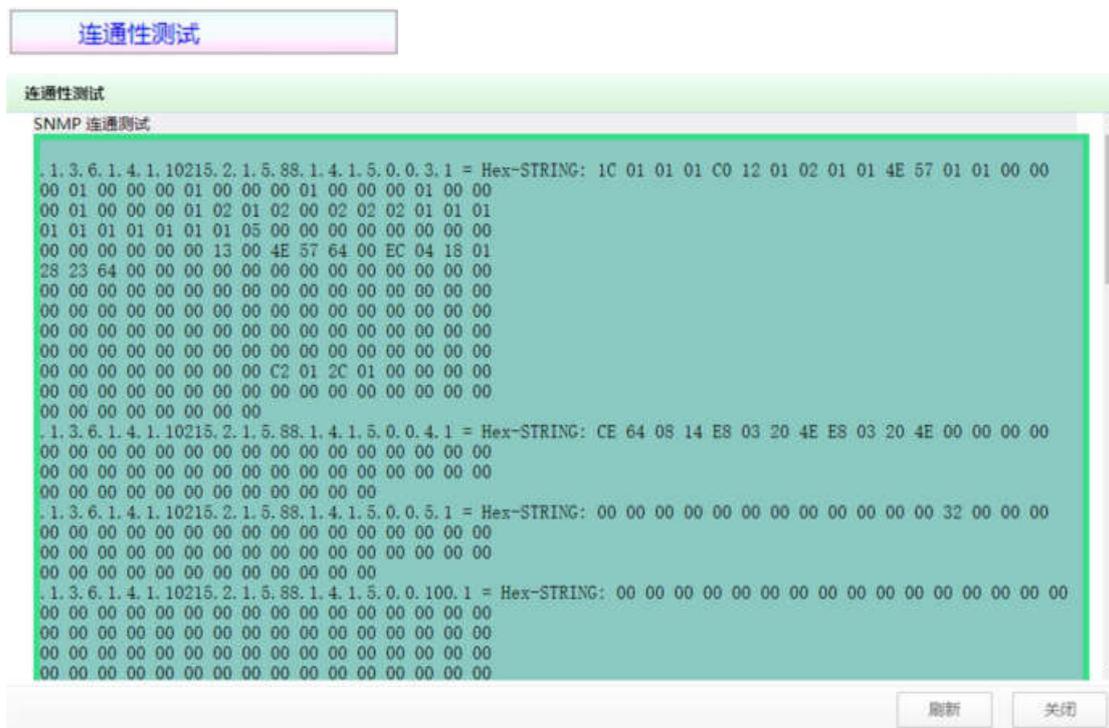


图 3-24 测试 SNMP 连通性

3.4.4 版本配置



版本配置分为专用版和通用版，通用版就是在专用版的基础上对接各种板卡的 mib 库，选择“通用版”后，勾选想对接的板卡，然后重启网管卡即可生效。

注：版本配置默认为专用版，如客户有特殊要求进行第三方对接，则可选择完整版。



图 3-25 版本配置

3.5.2 进程启动配置

进程启动配置

说明:配置后,需要重启系统方能生效

进程启动设置对 WEB、SNMP、Telnet/CLI、掉电告警、PON 断纤告警、UDP 等功能可进行选择启动或不启动,帮用户关闭某些不需要用到的功能。

注: WEB、SNMP、Telnet/CLI 三个进程必须至少有一个处于启动状态,否则三者都不启动,无法通过正常渠道管理网管卡系统;

服务名称	启动状态
WEB:	启动
SNMP:	启动
Telnet/CLI:	启动
Websocket:	不启动
动态IP:	不启动
Netconf:	不启动

说明:配置后,需要重启系统方能生效

应用 刷新 关闭

图 3-28 进程启动配置

3.5.2.1 进程启动配置的名词说明

WEB:网管卡系统网页版,方便管理网管卡系统信息。

SNMP:网管软件接收网管卡信息,显示设备视图,接收告警信息。

Telnet/CLI:命令指示符管理网管卡后台命令;

掉电告警:设备断电后,网管卡在最短时间内向网管软件发送提醒告警消息。

3.5.2.2 进程启动配置的操作说明

WEB:默认为“启动”,选择“不启动”的话,重启网管卡后,网管卡将无法登陆 webs 网页。

进程启动配置

WEB:	不启动
SNMP:	启动
Telnet/CLI:	启动
Websocket:	不启动
动态IP:	不启动
Netconf:	不启动

说明:配置后,需要重启系统方能生效

应用 刷新 关闭

图 3-29 进程启动配置 WEB

SNMP: 默认为“启动”，选择“不启动”后，网管软件将无法显示设备视图和接收到告警信息。

进程启动配置

WEB:	启动
SNMP:	不启动
Telnet/CLI:	启动
Websocket:	不启动
动态IP:	不启动
Netconf:	不启动

说明:配置后,需要重启系统方能生效

应用 刷新 关闭

图 3-30 进程启动配置 SNMP

Telnet/CLI: 默认为“启动”，选择“不启动”后，无法通过 Telnet 客户端进入网管卡后台。



图 3-31 进程启动配置 Telnet/CLI

3.5.3 网管卡升级

网管卡升级

注：升级 NMU 建议由专业技术服务人员进行升级！

在操作界面中点击“选择上传文件”寻找升级文件并添加，添加完后点击“升级”在升级的过程中不能刷新界面或者关闭界面，否则会导致升级失败。



图 3-32 升级网管卡版本

3.5.4 业务卡升级

业务卡升级

注：升级业务板建议由专业技术服务人员进行升级，防止导致业务中断！

在操作界面中勾选需要升级的单元盘，然后点击“选择升级文件”寻找升级文件并添加，添加完后点击“升级”在升级的过程中不能刷新界面或者关闭界面，否则会导致升级失败。

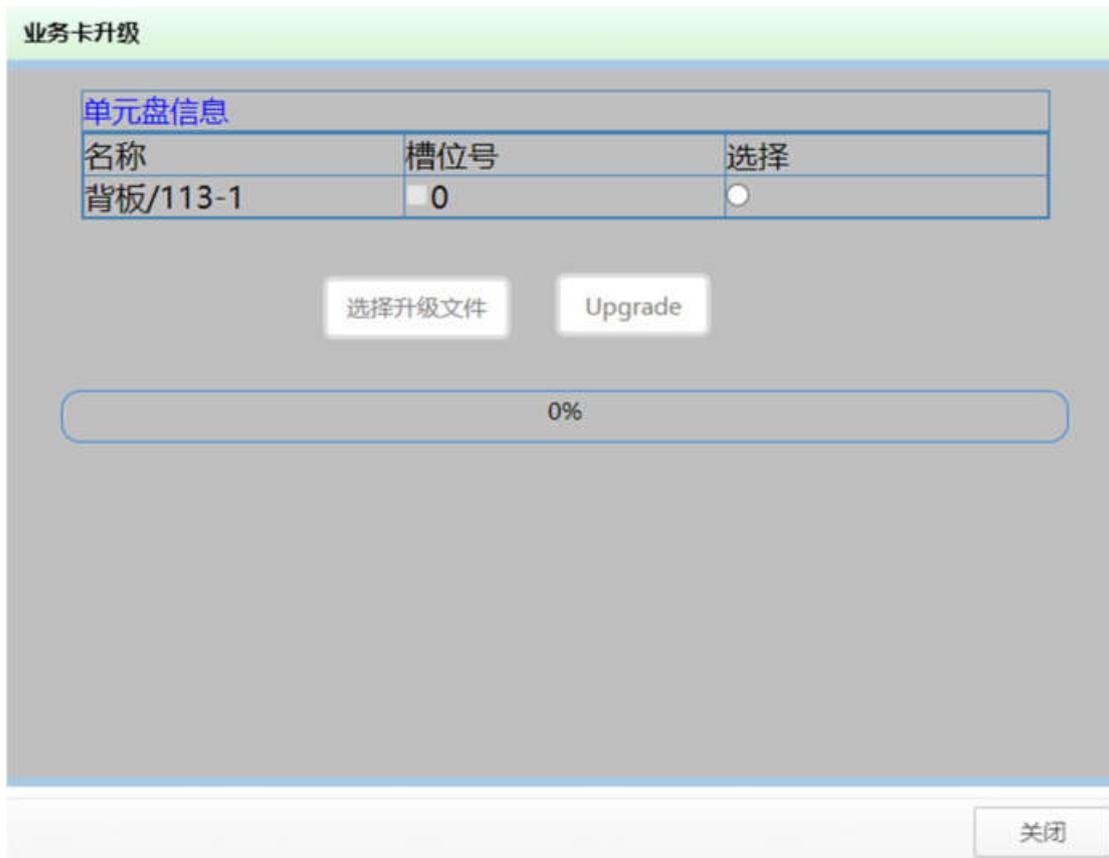


图 3-33 升级业务卡版本

3.5.5 恢复出厂设置

恢复出厂设置

注：慎用该功能！

在对话页面中选择需要恢复的出厂设置，选择后点击“应用”便可恢复设备的最初始状态，重启网管卡方可生效。

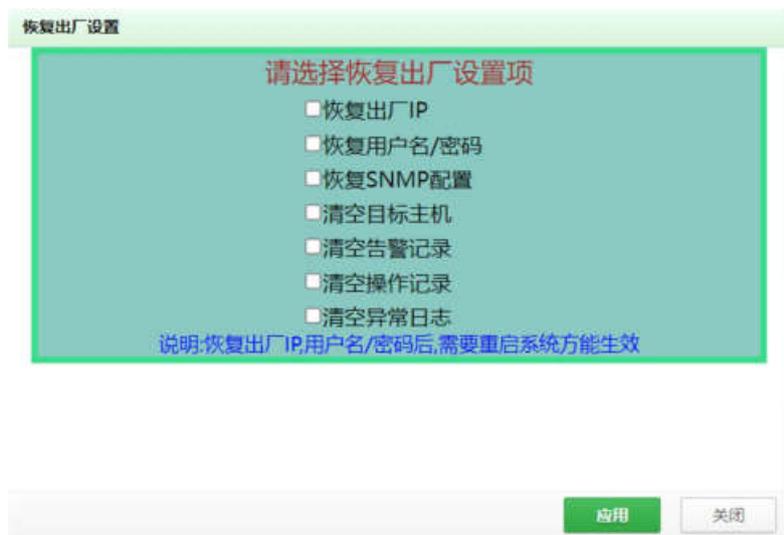


图 3-34 恢复出厂设置选择

3.5.5.1 恢复出厂设置的名词说明

恢复出厂 IP: 将网管卡 IP 恢复到出厂 IP (192.168.1.288)。

恢复用户名/密码: 恢复默认的系统账号 (root、admin、guest)，默认密码 (xx@8989)。

恢复 SNMP 配置: 恢复默认的 SNMP 共同体配置，读团体名为 public，写团体名为 private。

清空目标主机: 删除目标告警主机列表。

清空告警记录: 删除当前告警和历史告警的所有记录。

清空操作记录: 删除操作日志列表的所有记录。

清空异常日志: 删除异常日志列表的所有记录。

3.5.5.2 恢复出厂设置的操作说明

勾选“恢复出厂 IP”，点击“应用”，即可网管卡 IP 恢复到出厂 IP (192.168.1.288)，重启网管卡方可生效。



图 3-35 选择恢复出厂 IP

勾选“恢复用户名/密码”，点击“应用”，即可恢复默认的系统账号（root、admin、guest），默认密码（xx@8989），重启网管卡方可生效。



图 3-36 选择恢复初始用户名/密码

勾选“恢复 SNMP 配置，点击“应用”，即可恢复默认的 SNMP 共同体配置，读团体名为 public，写团体名为 private。



图 3-37 选择恢复初始 SNMP 配置

勾选“清空目标主机”，点击“应用”，便可删除目标告警主机列表。



图 3-38 清空告警目标主机

勾选“清空告警记录”，点击“应用”，便可删除当前告警和历史告警的所有记录。



图 3-39 清空告警记录

勾选“清空操作记录”，点击“应用”，便可删除操作日志列表的所有记录。



图 3-40 清空操作日志记录

勾选“清空异常记录”，点击“应用”，便可删除异常日志列表的所有记录。



图 3-41 清空异常日志记录

3.5.6 重启系统



在操作界面中点击“重启”可以软重启设备的网管，该重启功能对设备的其他板卡工作不构成影响。

3.6 安全管理



3.6.1 防火墙白名单管理



防火墙白名单类似操作系统的防火墙，选择允许一些 IP 地址通过认证可以访问网管卡系统，当白名单启用后，不在白名单内的 IP 地址或 MAC 地址都不能通过其他方式访问到网管卡系统。



图 3-42 防火墙白名单管理界面

3.6.1.1 防火墙白名单管理的名词说明

IP 地址白名单: 已通过认证的 IP 地址列表。

MAC 地址白名单: 已通过认证的 MAC 地址列表。

启用: 白名单开始生效。

保存: 保存白名单的 IP 和 MAC 数据。

清除: 清除白名单的 IP 和 MAC 数据。

增加: 白名单增加新的 IP 地址和 MAC 地址数据。

删除勾选: 删除所勾选的 IP 地址或 MAC 地址数据。

: 修改 IP 地址或 MAC 地址数据。

: 删除 IP 地址或 MAC 地址数据。

3.6.1.2 防火墙白名单管理的操作说明

增加: 白名单增加新的 IP 地址和 MAC 地址数据。

(1) IP 地址白名单: 勾选“IP 地址白名单”, 点击“增加”, 输入 IP 地址和选择 IP 类型, 点击“提交”保存。

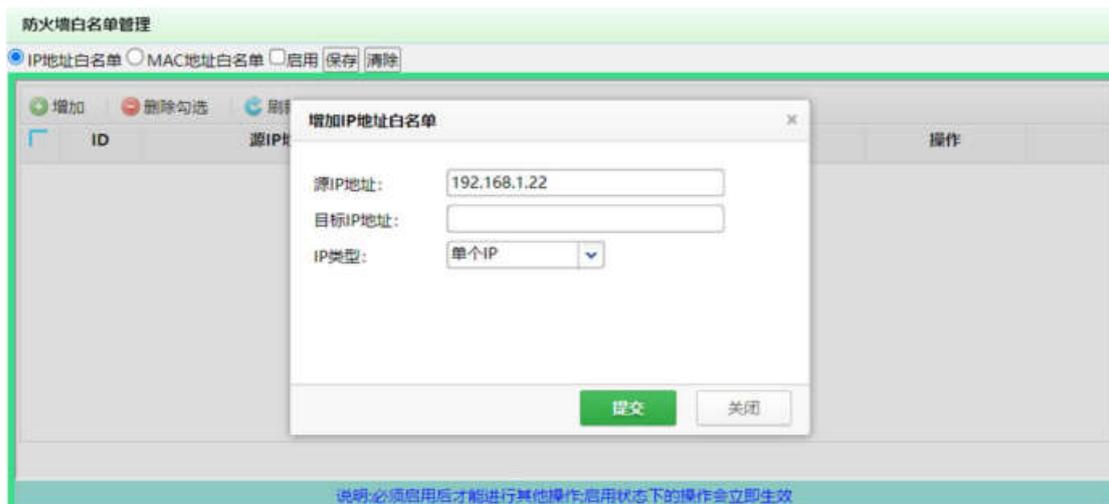


图 3-43 白名单增加新的 IP 地址

(2) MAC 地址白名单: 勾选“MAC 地址白名单”, 点击“增加”, 输入 MAC 地址, 点击“提交”保存。

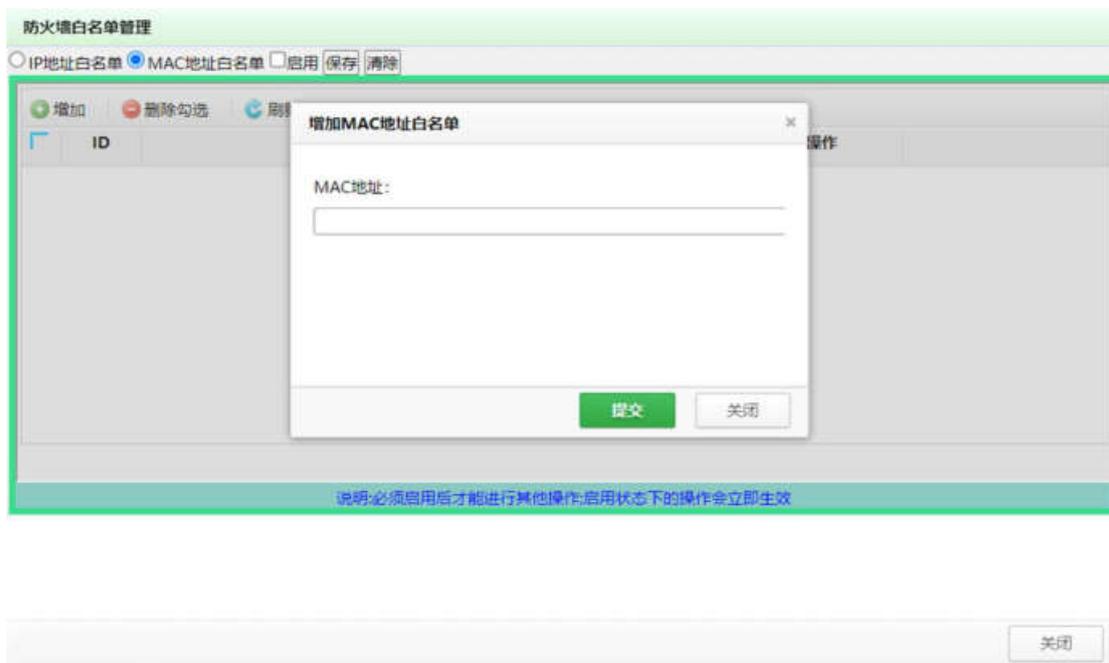


图 3-44 白名单增加新的 MAC 地址

删除: 勾选一条 IP 信息, 点击“删除勾选”按钮, 或者直接点击 IP 信息操作一栏的删除图标。

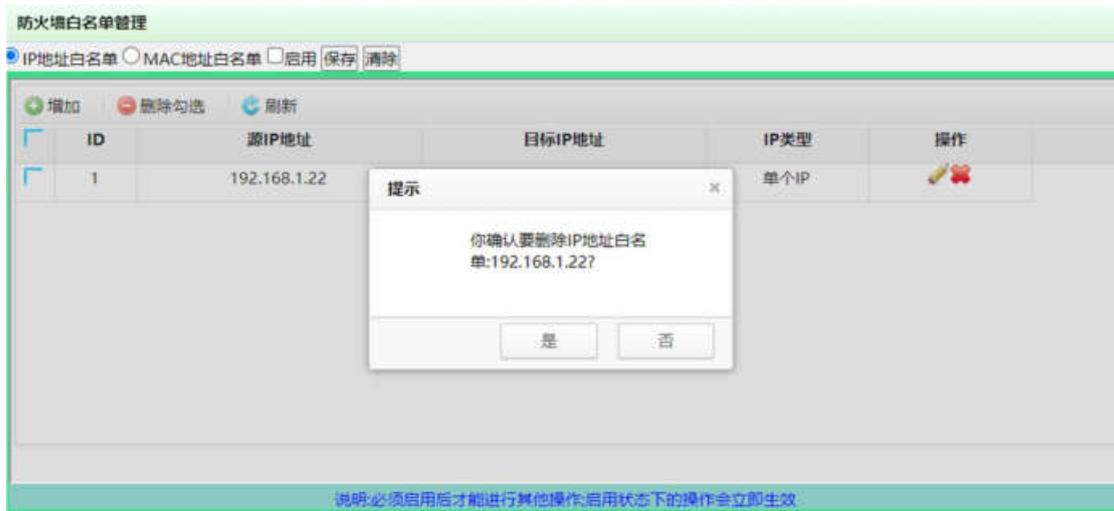


图 3-45 白名单删除 IP 地址

启用：IP 地址白名单开始启用，只允许满足白名单的 IP 可以访问该网管卡系统。

注：切记白名单不能乱添加不适合用户的 IP 数据，否则启用后会被网管卡系统率先屏蔽掉本机；



图 3-46 启动白名单，防火墙生效

保存：保存白名单的 IP 信息。

注：白名单的 IP 信息没有保存的话，网管卡系统重启后会不存在；

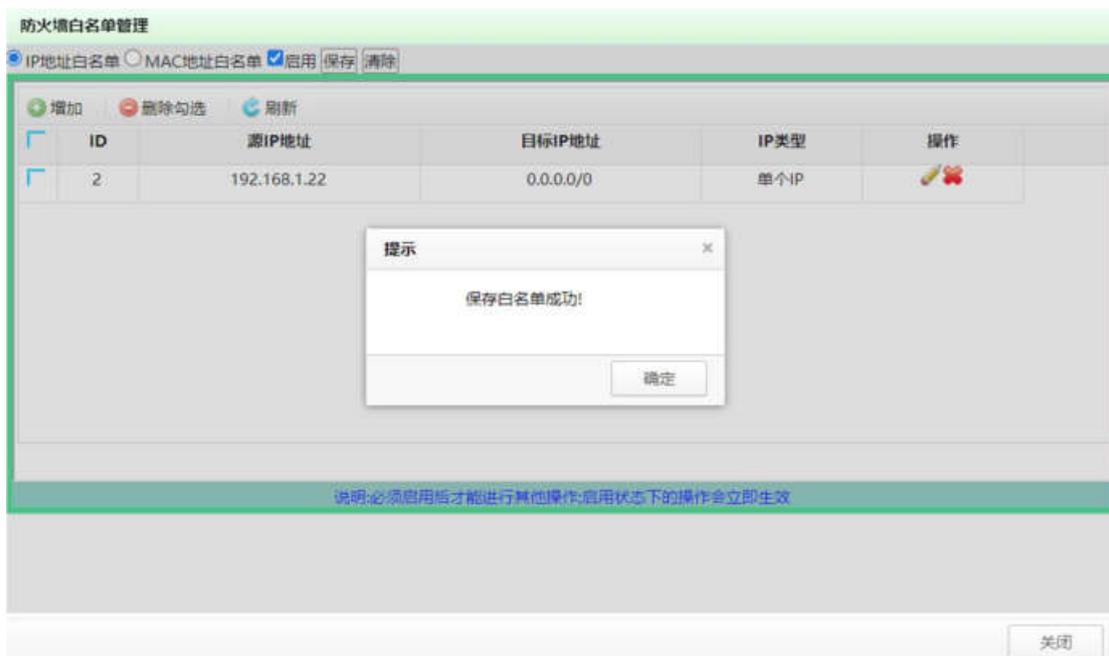


图 3-47 保存白名单信息，防火墙生效
清除：清空白名单的 IP 信息。

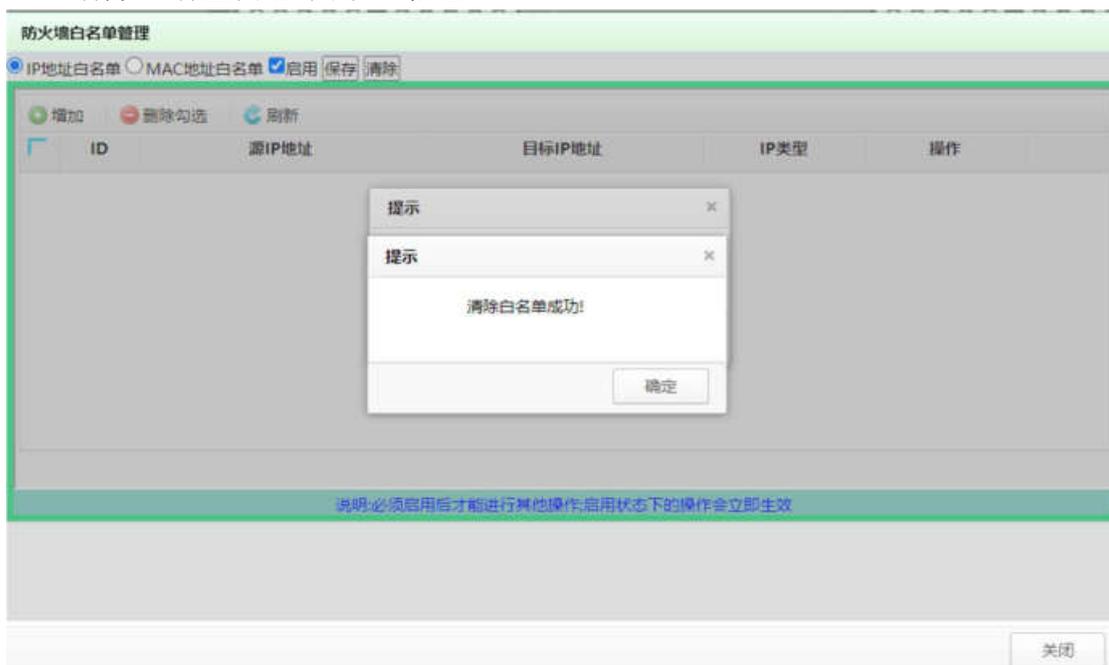


图 3-48 清除白名单信息，防火墙生效

3.6.2 端口转发

端口转发

端口转发是转发一个网络端口从一个网络节点到另一个网络节点的行为，其使一个外部用户从外部经过一个被激活的 NAT 路由器到达一个在私有内部 IP 地址(局域网内部)上的一个端口。

3.6.3 用户管理

用户管理

提供增加能访问系统的用户权限，查看能访问系统的用户名称和数量，修改用户密码，设置能访问系统的用户的权限。

注:修改了密码之后务必进行“保存”设置并重启系统生效，否则只是临时保存修改后的密码，当系统运行到一定时间后进行刷新密码会恢复修改前的密码。



图 3-49 用户管理界面

3.6.3.1 用户管理的名词说明

增加: 增加新的 webs 用户。

修改: 修改所勾选的用户的角色类型或密码。

删除: 删除所勾选的用户。

角色: 访问系统的用户的权限。

 : 修改该用户的角色类型或密码。

 : 删除该用户。

3.6.3.2 用户管理的操作说明

增加: 为访问该系统添加新的账户密码，在用户对话界面中输入用户名，用户角色和密码等并“提交”保存。

用户管理

新增

新增用户

用户名: root

角色: 管理员

新密码:

确认密码:

提交 重置 关闭

关闭

图 3-50 新增用户

修改: 修改当前账户的密码或者角色类型, 修改完毕后点击“提交”保存。

用户管理

新增

修改用户

用户名: admin

角色: 管理员

旧密码:

新密码:

确认密码:

提交 重置 关闭

关闭

图 3-51 修改用户

删除：删除所勾选的用户。



图 3-52 删除用户

角色：设置角色的类型，角色类型分管理员与普通用户两种，管理员的权限允许访问的功能更多一些。



图 3-53 用户权限选择

3.6.4 修改密码

修改密码

注：修改了密码，新增的权限务必在这里继续保存并重启系统！否则密码不起效

修改完的用户密码或者权限，在应用保存之后还需要进入该界面进行保存设置并重启设备起效。



The screenshot shows a web interface for changing a password. It features a title bar labeled '修改密码'. Below the title bar, there are four input fields arranged vertically. The first field is labeled '用户名:' and contains the text 'root'. The second field is labeled '旧密码:', the third is '新密码:', and the fourth is '确认密码:'. At the bottom right of the form area, there are two buttons: a green '应用' (Apply) button and a grey '关闭' (Close) button.

图 3-54 修改密码

3.6.5 退出登录

退出登录

点击“退登”后，网页退出到登录界面，需要重新输入账号密码登录。

3.7 日志管理

日志管理

3.7.1 异常日志

异常日志

记录系统故障的时间，远程重启的记录等。

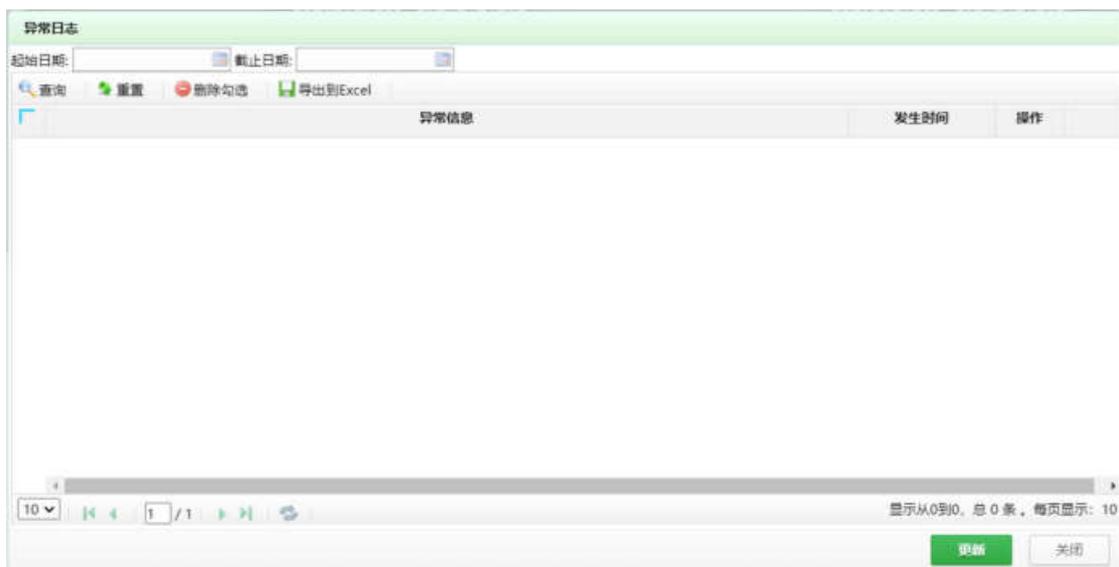


图 3-55 异常日志界面

3.7.2 操作日志

操作日志

提供设备所有被登陆系统后用户操作的行为，如修改密码之类的。

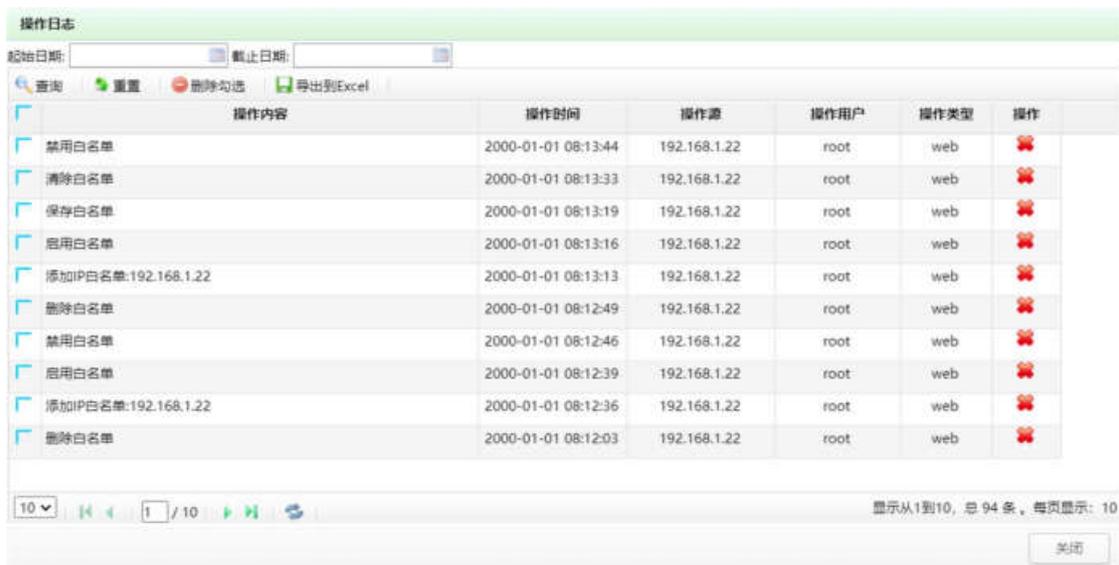


图 3-56 操作日志界面

3.7.3 日志配置

日志配置

勾选“启用”后，日志开始记录异常与各种操作的行为。

日志配置

发送日志到服务器

服务器IP: 端口: 514

保存异常日志

保存操作日志

说明:配置日志后,需要重启系统方能生效

图 3-57 日志配置