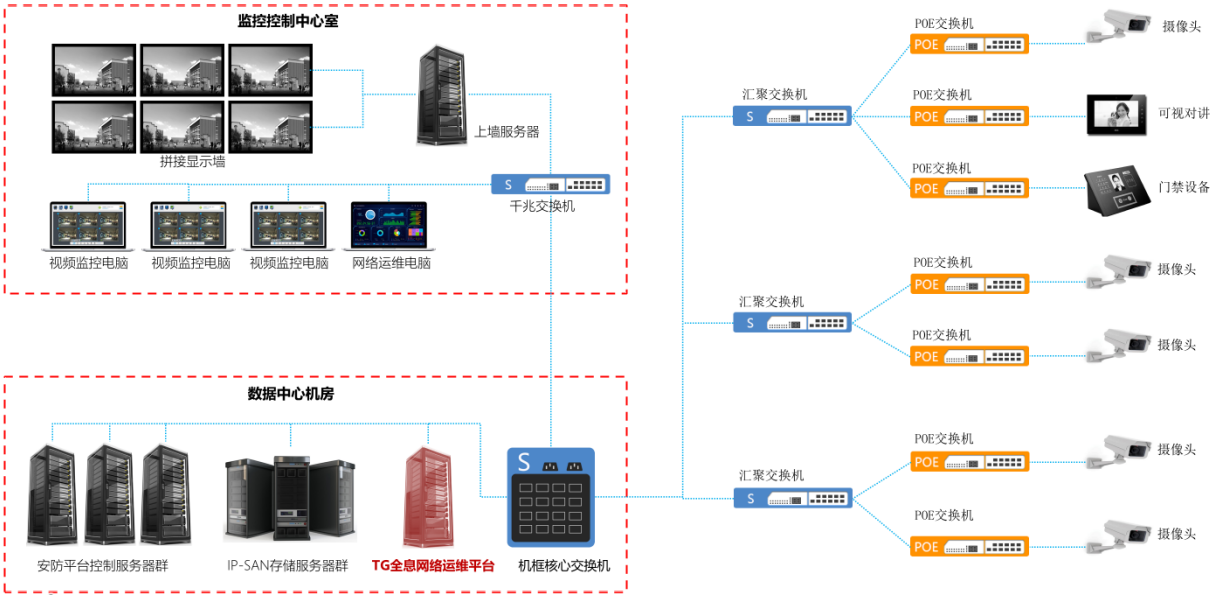
TG 多业务云智能管理平台

NMSS 系列操作手册



封面供参考使用

声 明

©copyright 2011 by Shenzhen TG-NET Botone Technology Co.,Ltd. All rights reserved.

事先未征得深圳市万网博通科技有限公司（以下简称 TG-NET）的书面同意，任何人不得以任何方式拷贝或复制本文档中的任何内容。

TG-NET 不做与本文档相关的任何保证，不做商业性、质量或特定用途适用性的任何隐含保证。本文档中的信息随时可能变更，而不另行通知。TG-NET 保留对本出版物做修订而不通知任何个人或团体此类变更的权利。

深圳市万网博通科技有限公司

地　　址：深圳市南山区西丽中山园路 1001 号 TCL 高新科技园 E3 栋 4 楼

服务电话：400-088-7500

电　　话：0755-86963722/66/99

传　　真：0755-86963733

网　　址：http://www.tg-net.cn

邮　　编：518109

目 录

1、交换机管理 5

1.1 TG 交换机加入平台 5

1.2 第三方交换机加入平台 6

1.3 交换机管理 7

1.4 监控管理 9

2、IPC 管理 10

2.1 IPC 识别与数据获取 10

2.2 OUI 管理 12

2.3 IPC 数据手动获取 12

2.4 IPC 参数修改 12

2.5 分组管理 13

3、自定义设备 13

3.1 设备类型 13

3.2 自定义设备 14

4、优先保障 15

5、流量整形 16

6、安全防护 17

6.1 防护配置 17

6.2 授权配置 18

7、环路防护 19

8、网络健康指数 20

9、实时监测告警 21

9.1 告警 21

9.2 告警开关配置 23

10、多层可视化动态拓扑 23

10.1 可视化告警 24

10.2 拓扑图生成 25

10.3 编辑拓扑 25

11、账号权限管理 26

12、TG 云端远程管理 27

13、手机微信小程序随时随地 28

1、交换机管理

1.1 TG 交换机加入平台

NMSS 平台支持基于 A-scan 技术对网络中的网络设备进行统一的管理，并支持以交换机为基础在局域网内部实现逐级探测，然后再利用 ARP、MAC 地址以及流量特征识别出其它各个节点设备类型。

NMSS 平台管理的交换机，可修改交换机 IP 地址、掩码以及登录密码，可以对交换机执行重启、升级、恢复出厂操作，可以对 POE 交换机设置定时重启、供电关闭/开启操作，对 POE 交换机端口设置定时重启、供电关闭/开启、端口禁用/使能操作，并且可以实时监控交换机端口的流量情况以及 POE 交换机端口的供电情况；

NMSS 平台与交换机在同一广播域，只需要 NMSS 平台与交换机的管理密钥相同，交换机则会自动加入平台，平台即可对交换机进行管理；

NMSS 平台与交换机不在一个广播域中，交换机平台跨广播域，交换机加入平台则需要执行三层管理相应的配置：

（1）保证 NMSS 平台与交换机的通信正常，交换机与 NMSS 平台之间的路由可达；

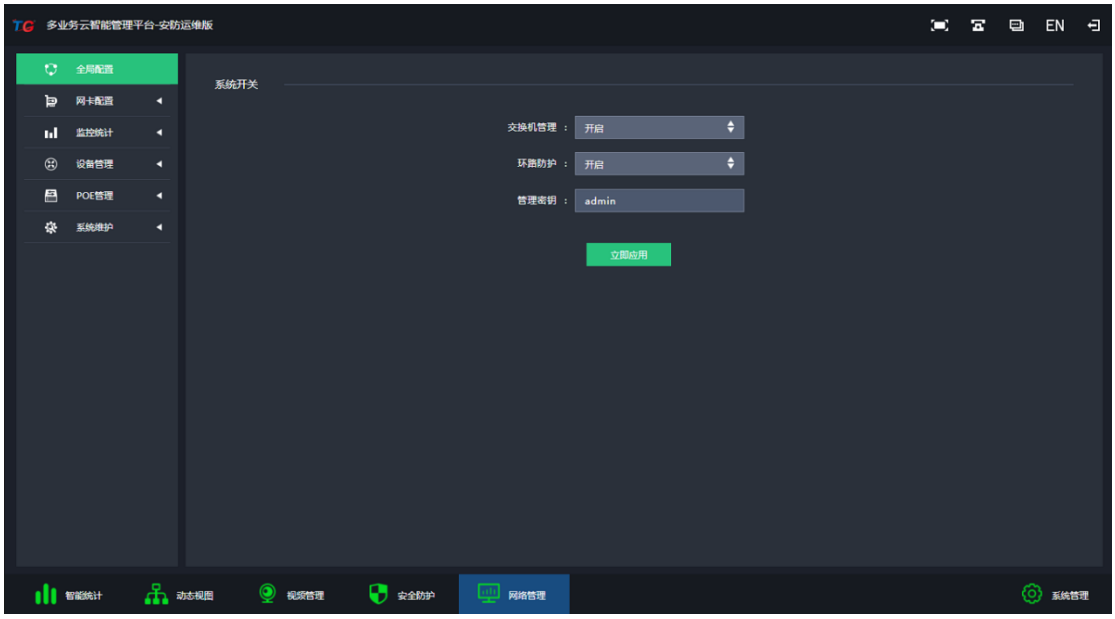
（2）NMSS 平台与交换机的管理密钥相同；

NMSS 平台与交换机默认管理密钥均为“admin”，NMSS 平台在网络管理->全局管理页面，可修改管理密钥，修改后则会同步下发至当前管理的交换机，在交换机页面也可以修改交换机本身的管理密钥。

（3）NMSS 平台与交换机均要开启三层管理功能；

NMSS 平台开启三层管理交换机功能：通过 telnet 访问 NMSS 平台，在配置模式下，执行 switch udp enable 命令（TGOS(config)# switch udp enable）；

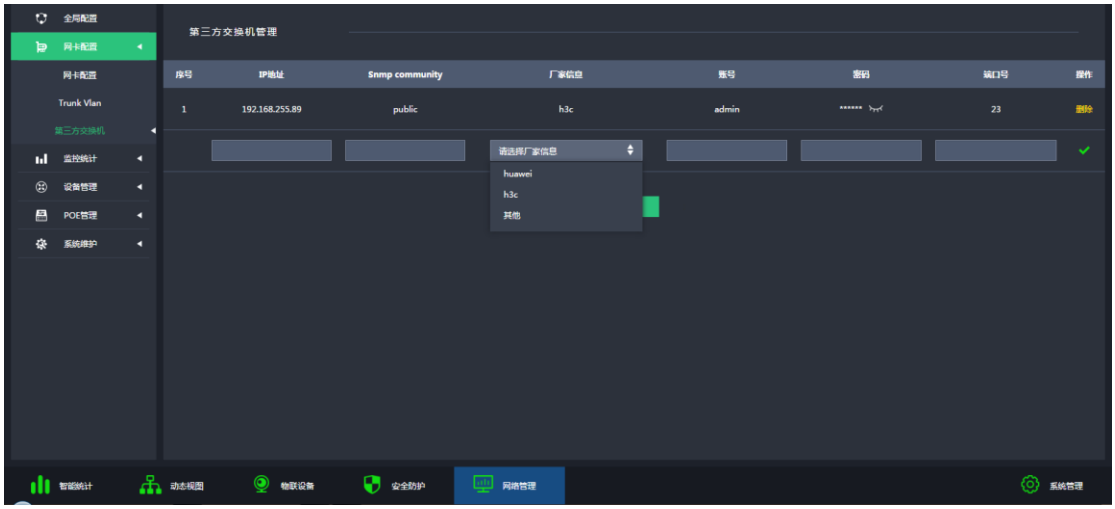
交换机开启三层管理功能：有两种方式可开启交换机的三层管理功能。通过 web 页面访问交换机，在系统配置->云盒子管理页面，开启三层管理开关，并配置平台的 IP 地址；或者，通过 telnet 访问交换机，在配置模式下，执行 tnmp udp on X.X.X.X 命令（X.X.X.X 为 NMSS 平台的 IP 地址），如 switch(config)# tnmp udp on 192.168.255.254 。



1.2 第三方交换机加入平台

若网络中存在其他厂商，则可通过第三方交换机管理的方式，将交换机加入到平台中，被管理的第三方交换机需满足两个条件：①NMSS 平台与交换机通信正常，路由可达；②交换机需支持 snmpV2。

在网络管理->网卡配置->第三方交换机页面，点击新增按钮，输入交换机的 IP 地址、SNMP community、厂家（huawei、h3c 或其他）、telnet 的账号密码以及端口号，配置完成后，点击进行保存即可。

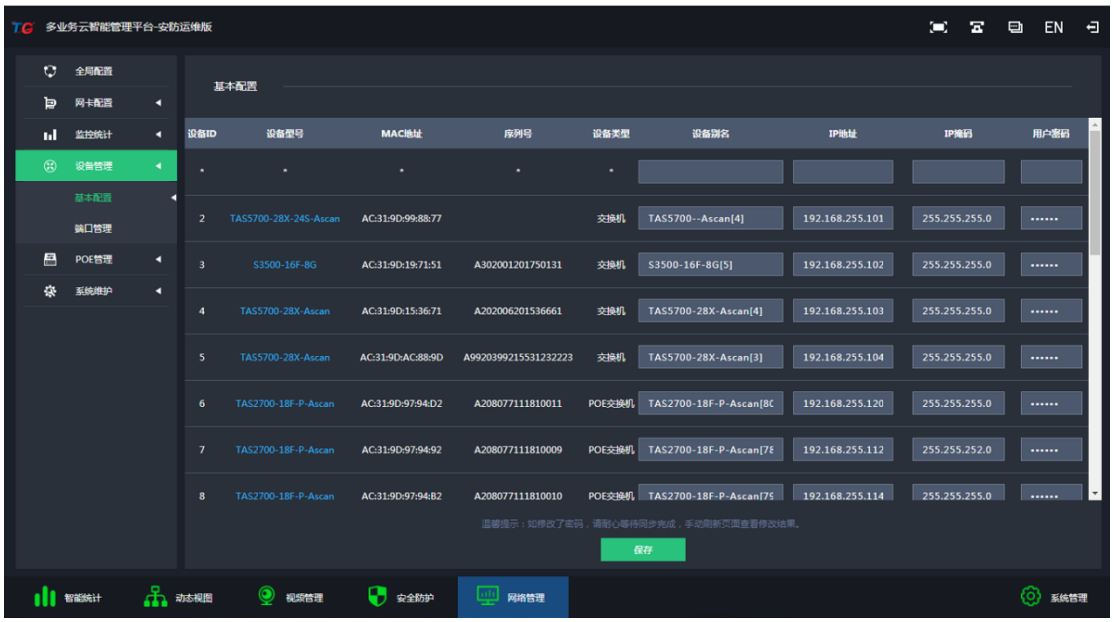


1.3 交换机管理

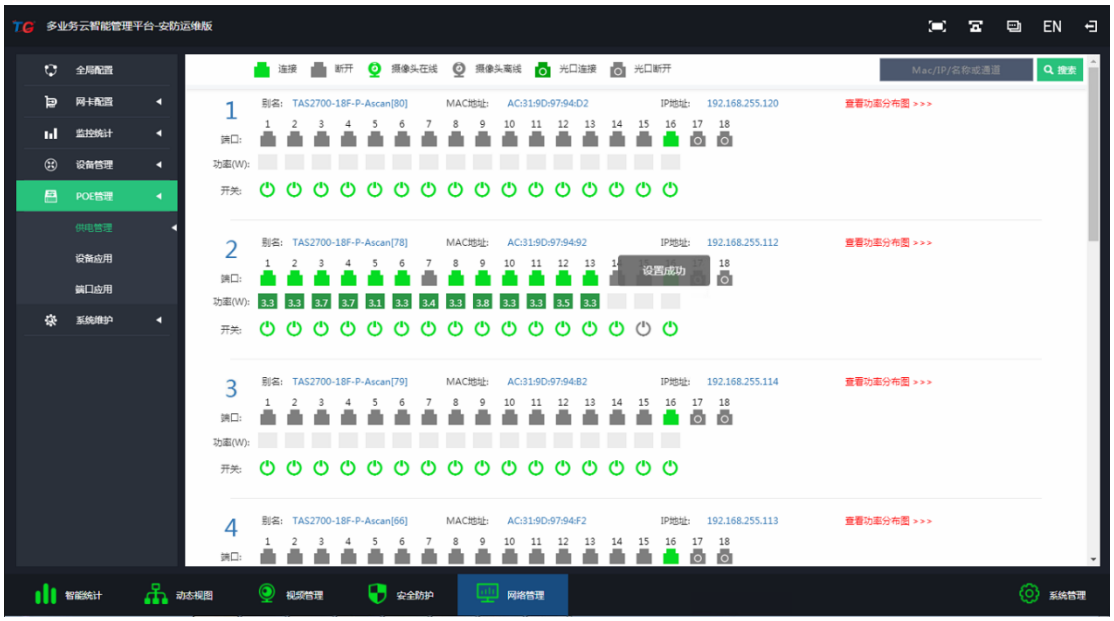
交换机加入平台后，双方管理密钥相同，平台即可对交换机执行 IP 修改或重启等操作。

在网络管理->系统维护页面，可对交换机执行重启、复位、升级操作；

在网络管理->设备管理->基本配置页面，可修改交换机的别名、IP 地址/掩码、交换机登录密码；



在网络管理->POE 管理->供电管理页面，点击端口对应的开关，即可修改 POE 交换机的供电开关，开关图标显示为绿色，则会开启状态，点击该图标，则立即关闭供电，关闭后图标显示为灰色，关闭状态下点击时即开启供电；

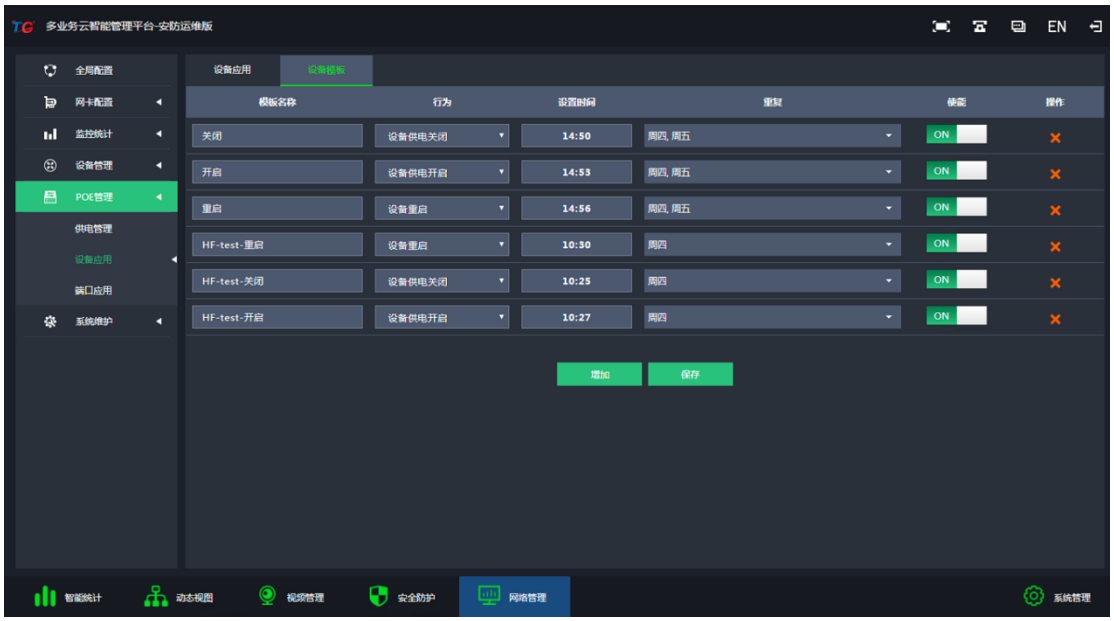


可对 POE 交换机进行定时重启、定时供电关闭/开启，以及对 POE 交换机端口定时重启、定时供电关闭/开启、定时禁用/使能端口、端口智能重启操作。

在网络管理->POE 管理页面，设备应用中设置的定时操作，是针对整个交换机执行的，而端口应用中则是针对所选择的端口执行定时操作；

在设备模版（或端口模板）中添加定时行为，添加成功后，在设备应用（或端口应用）中，将所添加的模板应用到对应交换机或端口中，保存即可，到达设定时间，设备（或端口）就会自动执行应用的行为。

智能重启，平台会对设置智能重启的端口进行实时检测，当检测到端口一定时间之内没有流量，则会将端口强制重启，因此智能重启行为不需要设置时间。

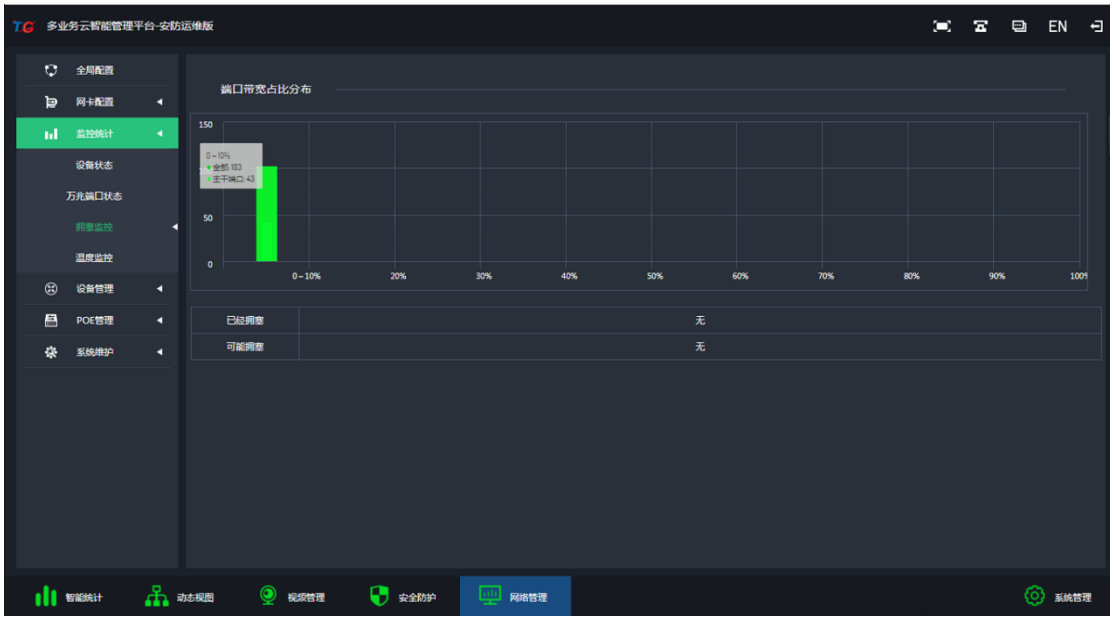


1.4 监控管理

实时监测交换机在线端口的流量情况，当端口出现流量带宽占比过大时进行告警及精准定位，便于及时对网络进行调整，避免带宽不足而导致数据丢失的情况。

实时监测交换机工作温度（内置的温度探测装置），尤其是工作在室外的交换机，避免工作温度异常而导致网络不稳定。并且在低温环境下，可以通过内置的温度加热装置，自动对交换机进行加热，保障交换机的稳定运行。

在网络管理->监控统计页面，可以查看当前所有交换机的在线端口拥塞情况，以及当前交换机的温度情况。



2、IPC 管理

NMSS 平台支持 ONVIF 等协议对安防系统的前端设备进行识别和管理，会自动获取摄像机的通道名称、厂家信息、序列号/MAC 地址、IP 地址以及所连接交换机的基本信息。

要实现自动识别 IPC 功能 ,需对 NMSS 平台进行功能配置 ,且默认仅支持与 NMSS 平台同一广播域内的摄像机识别，若需跨广播域识别，则需开启三层 IPC 识别功能。而若要获取摄像机的通道名称以及厂家等信息，需要配置相应的 OUI。

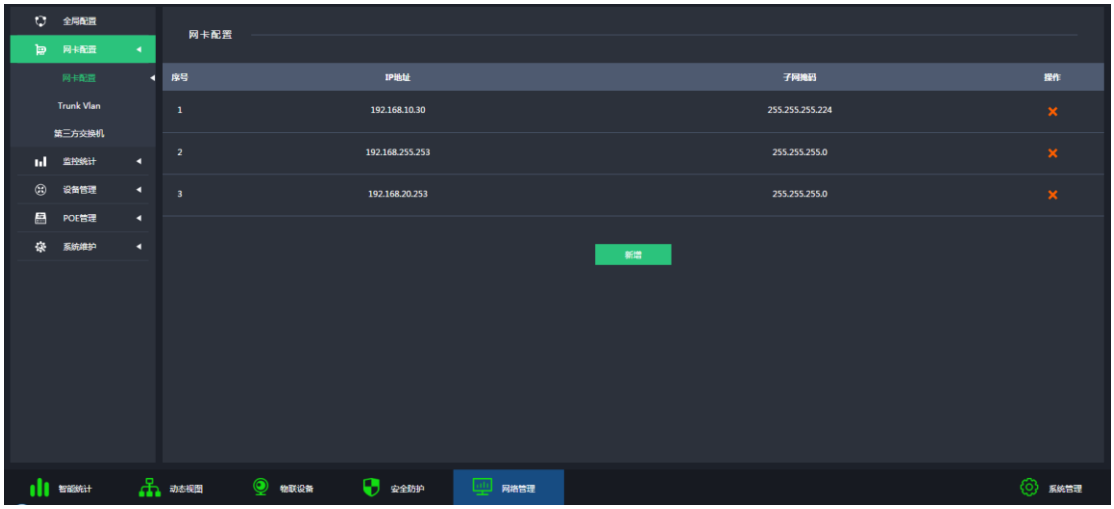
2.1 IPC 识别与数据获取

摄像机接入平台，与平台通信正常，平台即可自动识别为摄像机，但若需获取摄像机的通道名称等信息，需要设置摄像机对应的 OUI 信息，才可获取成功。

设置 OUI，在物联设备->摄像机配置页面，点击新增按钮，输入摄像机对应的 OUI 信息、摄像机登录用户名以及密码，点击保存即可完成创建，创建成功后，即会自动获取摄像机的通道名称、厂家等信息。

同广播域识别 IPC 配置：

（1）NMSS 平台与摄像机的通信配置，配置 NMSS 平台的 IP 地址与摄像机同网段，或在网络管理->网卡配置中添加一个与摄像机同网段的网卡地址；



（2）配置摄像机 OUI 的用户名以及密码，用于获取摄像机的通道以及厂家信息，OUI 则为摄像机 MAC 地址的前 3 位；

跨广播域识别 IPC 配置：

（1）开启 NMSS 平台跨三层识别 IPC 功能，通过 telnet 访问 NMSS 平台，在配置模式下，执行 ws-discovery enable switch 命令；

（2）保证 NMSS 平台与摄像机的通信正常，摄像机与 NMSS 平台的路由可达；

（3）在物联设备-摄像机配置页面，配置缺省 OUI 的用户名以及密码，OUI 为 00:00:00，用户名密码则为摄像机的登录用户名与密码

（4）配置摄像机 OUI 的用户名以及密码，用于获取摄像机的通道以及厂家信息

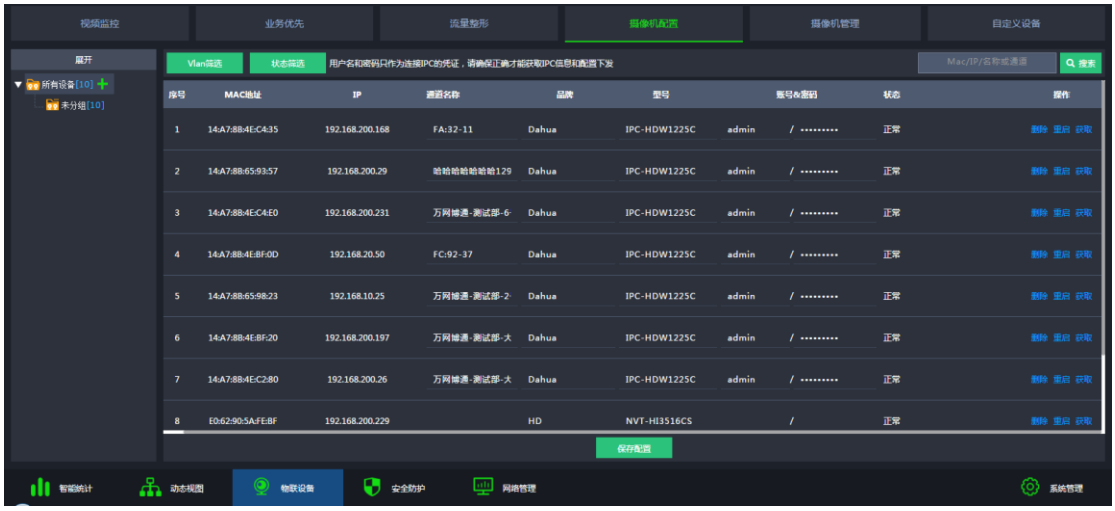
2.2 OUI 管理

摄像机接入平台，与平台通信正常，平台即可自动识别为摄像机，但若需获取摄像机的通道名称等信息，需要设置摄像机对应的 OUI 信息，才可获取成功。

设置 OUI，在物联设备->摄像机配置页面，点击新增按钮，输入摄像机对应的 OUI 信息、摄像机登录用户名以及密码，点击保存即可完成创建，创建成功后，即会自动获取摄像机的通道名称、厂家等信息。

2.3 IPC 数据手动获取

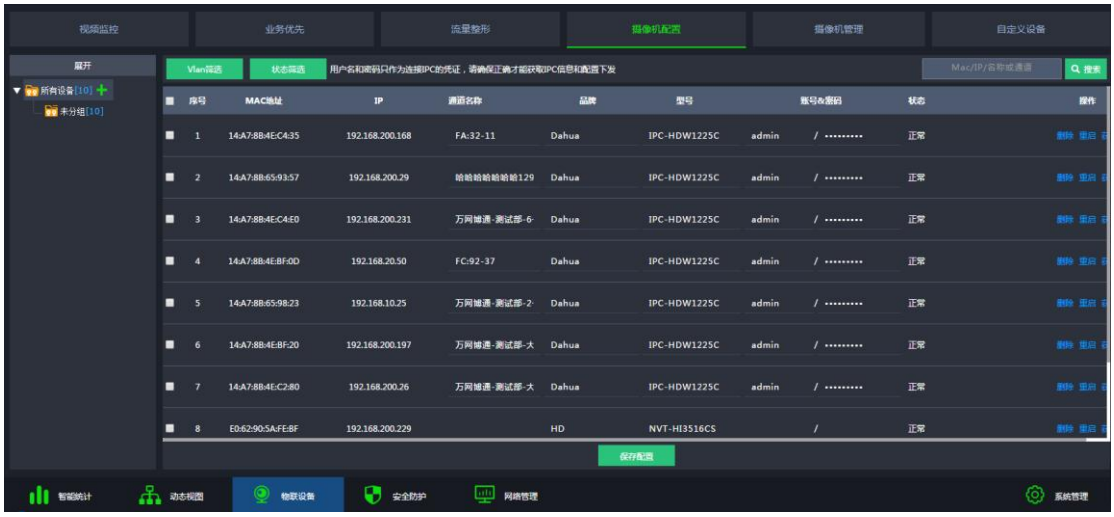
若摄像机进行了通道名称或其他参数的变更，则需在物联设备->摄像机配置页面点击获取按钮，手动进行获取，平台才会将数据变更为修改后的参数。



2.4 IPC 参数修改

在摄像机配置页面，可对 IPC 的通道信息、品牌以及型号进行修改，输入修改后的参数，点击“保存配置”按钮即可。

注意：修改的配置不会下发至 IPC，仅在平台有效。



2.5 分组管理

每个视频监控系统中都有大量的视频监控点，查看某个区域或特定的摄像机困难，因此，我司支持将摄像机进行分组显示。

（1）添加分组：在物联设备->视频监控页面，将鼠标移动至左侧分组列表名称上，点击绿色加号，即可添加分组成功；

（2）编辑分组名称：点击编辑分组按钮，即可修改分组名称；

（3）移动分组：勾选列表中需要移动的摄像机，点击移动分组移出分组，在弹出的分组列表中，选择分组，即可移动成功。

3、自定义设备

3.1 设备类型

NMSS 平台支持通过自定义的方式定义类型，可通过自定义类型的方式，配置平台不支持的终端类型；默认已支持无需自定义的类型有 AP、摄像机、NVR、DVS、服务器、路由器、可视对讲、门禁、PC。

在自定义设备->设备类型页面中，点击新增按钮，配置类型的名称、检测方式、间隔时间，点击保存按钮。

新增自定义类型成功后，需导入相应的在线、离线、告警图片，设置成功后，所有选择配置为此类型的终端，在拓扑图中将会显示相应的图片。

3.2 自定义设备

将网络中需要自定义的终端，添加到 NMSS 平台中，那么在拓扑图中将会显示自定义终端的位置，以及流量显示，并且当终端出现异常时，平台将会进行告警。

在物联设备->自定义设备页面中，点击新增按钮，选择终端类型，输入终端 MAC 地址、名称、IP 地址，点击保存按钮即可。

类型：默认支持的类型以及自定义的类型，均可进行选择；

支持批量配置，点击右上角的模板下载，下载文档模板，配置好设备信息保存文档，再通过点击批量导入按钮进行文档导入即可。

点击一键导出按钮，可导出当前已设置好的自定义设备。

所有自定义的终端，在拓扑图中将会有对应显示，以及流量信息，出现异常时会有告警提示，如离线时，提示离线告警。

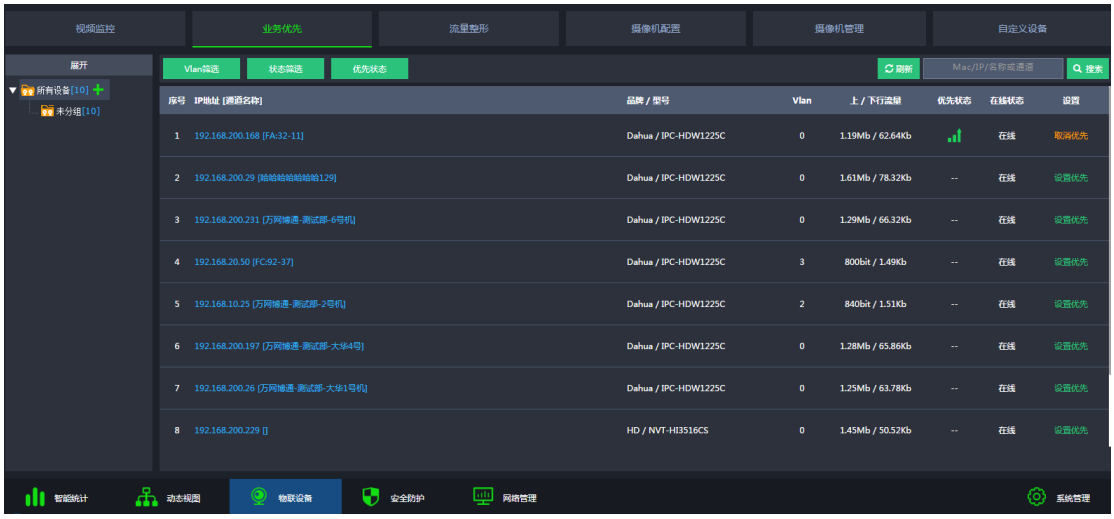
在智能统计页面，自定义终端出现异常，也会有告警提示。

4、优先保障

每个视频监控系统中都有大量的视频监控点，并且一定会有部份视频监控点是关键重要监控点(例如公安行业的重要公共区域及道口、司法行业中的枪械库、金融行业中的金库内库及柜台、楼宇行业中的单元门和大门、企业的财务室等），针对这些重点监控点都必须实时 24 小时监管查看，视频流不能出现任何卡顿和丢失。

通过使用关键视频流的优先保障功能，基于对视频流网络传输协议层的优化，可以在网络上确保关键视频流的优先传输，保证关键视频不因网络问题而丢帧卡顿。

在物联设备->业务优先页面，对需要重点监控的摄像机，点击摄像机对应的设置优先设置优先，摄像机即为优先状态，若需取消优先，则点击已优先摄像机对应的取消优先取消优先即可。

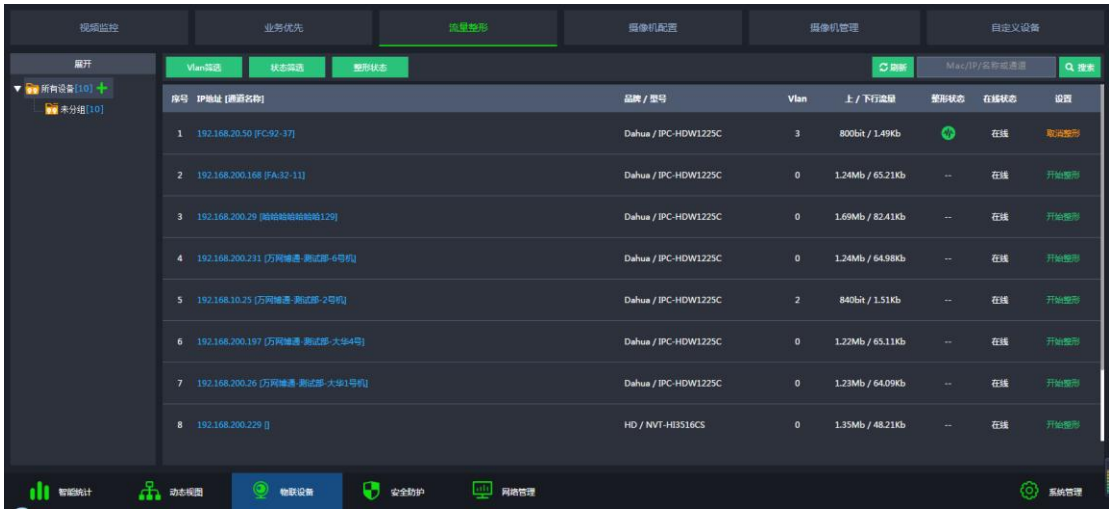


5、流量整形

视频卡顿是安防系统中最常见，也是最为难以解决的故障。一旦出卡顿故障，只能从摄像机到网络到服务器一一去排查。很多时候，交换机工作状态看上去是正常的，而摄像机单机工作也正常，服务器也正常，可是视频就是卡顿，无从下手，各个系统厂家之间相互推诿，只能不断的尝试重启设备，更换设备等。

通过 A-Scan 创新技术，当视频流卡顿时，可以将视频流从摄像机到流媒体服务器传输过程中所经过的网络节点单独可视化的呈现出来。如果有网络传输故障点，系统会告警并精准定位故障点的位置。并且可以针对卡顿的视频流开启流量整形功能，对该视频流的网络传输协议进行优化整形，有效的解决因网络导致卡顿的问题。

在物联设备->流量整形页面，对摄像机设置流量整形即可。



6、安全防护

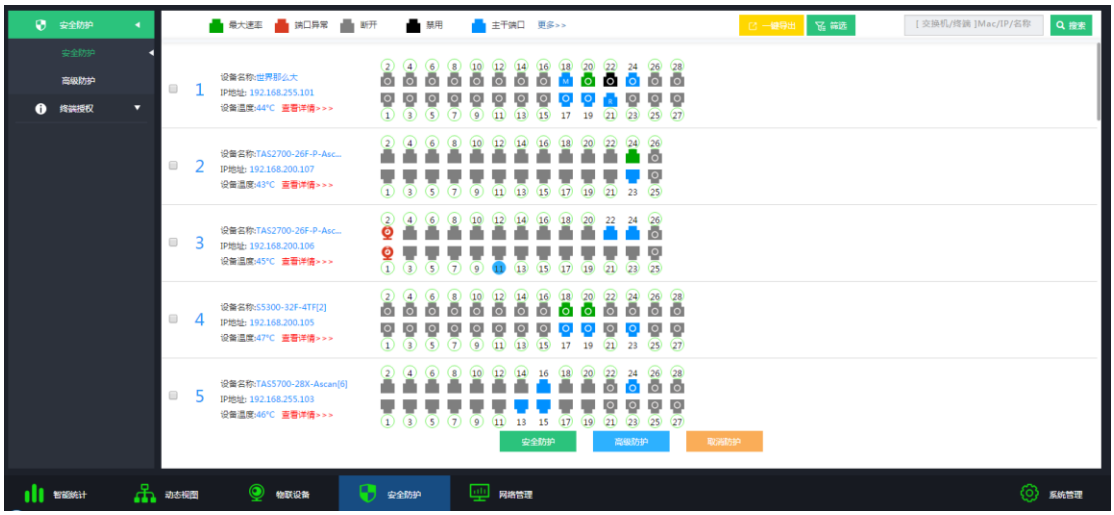
现有的安防网络多数都没有严格的保护措施。由于安装位置没有条件进行严密的锁定，尤其是室外放置的接入层交换机很容易被打开接触。通过接入任一交换机的任一端口，就可以轻易的与系统中的所有设备进行通信，包括关键服务器等，风险隐患很大。通过使用网络的入侵告警及安全防护功能，不仅可以有效的阻止未经授权的非法设备接入安防网络，保护网络的安全性和信息的安全性。还可以对非法设备的入侵动作进行实时告警和定位。

安全防护有两种类型，分别是一般防护和高级防护。一般防护仅对端口接入的设备进行限制，而高级防护不但对端口接入的设备有限制，对设备的数据也会进行限制，高级防护的已授权设备若发出与摄像机不相符的数据报文，端口会将报文丢弃。

6.1 防护配置

在安全防护页面，对需要进行防护的端口开启防护功能，当端口遭遇设备入侵时，则会对入侵设备进行限流以及告警提示，一般防护端口号为绿色 ，高级防护端口号为蓝色 ，均为防护状态。

可对交换机所有端口（交换机级联口不可配置）或个别端口进行防护配置，勾选交换机对应的左侧方框，或点击需要配置的端口号 ，选择完成后，点击安全防护 则启用一般防护，而点击高级防护 则是启用高级防护，确认防护即可完成防护配置。

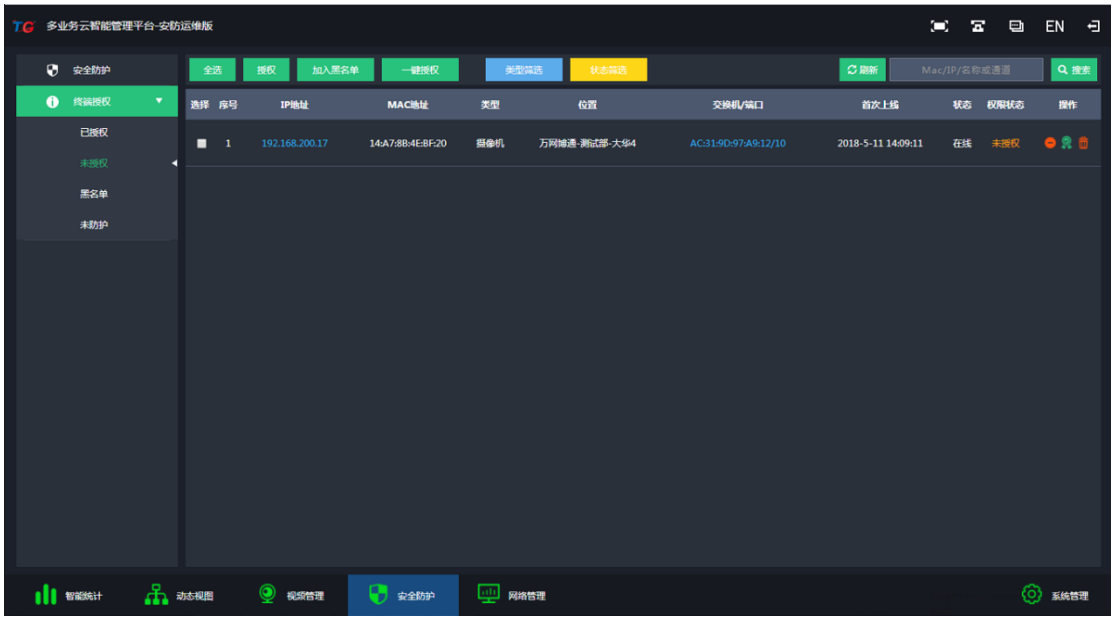


6.2 授权配置

若端口有连接在线终端时，开启端口的安全防护，那么平台会自动为当前终端进行授权；若开启端口防护后再接入终端，则平台会有终端入侵告警，将丢弃终端发送的数据并且对端口进行限流；

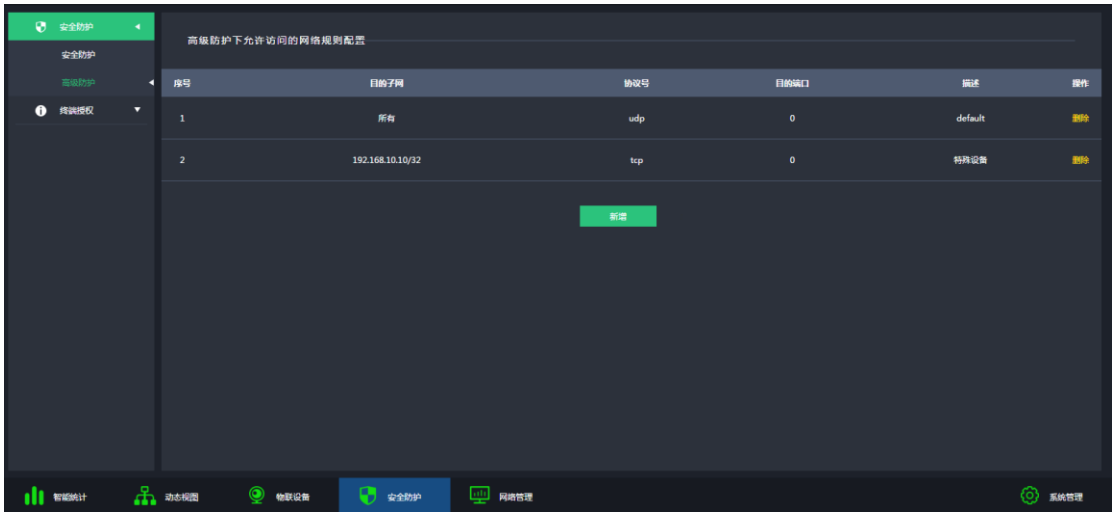
授权成功后，终端将在已授权页面显示；防护端口接入的终端未授权，终端将在未授权页面显示；未防护端口接入的终端，则在未防护页面显示。

若要对端口进行授权，在终端授权-未授权页面，点击一键授权 对所有终端授权，或点击授权按钮 对单个终端进行授权。



若端口启用高级防护，而接入的终端为已授权的非摄像机的特殊设备，需要取消其数据的限制，可在安全防护->高级防护页面，通过配置，使设备的数据流不受高级防护限制。

如下图中的第 2 条规则 ,表示可接收来自目的子网 192.168.10.10 发送的所有 TCP 报文。



7、环路防护

环路防护，当网络形成环路时，NMSS 平台将会将形成环路的端口阻塞，有效的抑制环路引起的广播风暴对网络的影响，并且有相应的告警提示。

支持两种环路防护方式，分别是私有和通用型，私有型的环路防护仅适用于不存在三层管理的交换机的网络环境，而通用型则适用于所有网络环境。

配置：在网络管理-全局配置中，选择适用于网络的环路防护即可；

8、网络健康指数

独创的 360 式智能网络监控巡检诊断，实时对网络环境、视频状态、网络链路状态、安全状况进行扫描，并且明确出现异常所有的设备信息，能够及时发现问题及时解决问题。

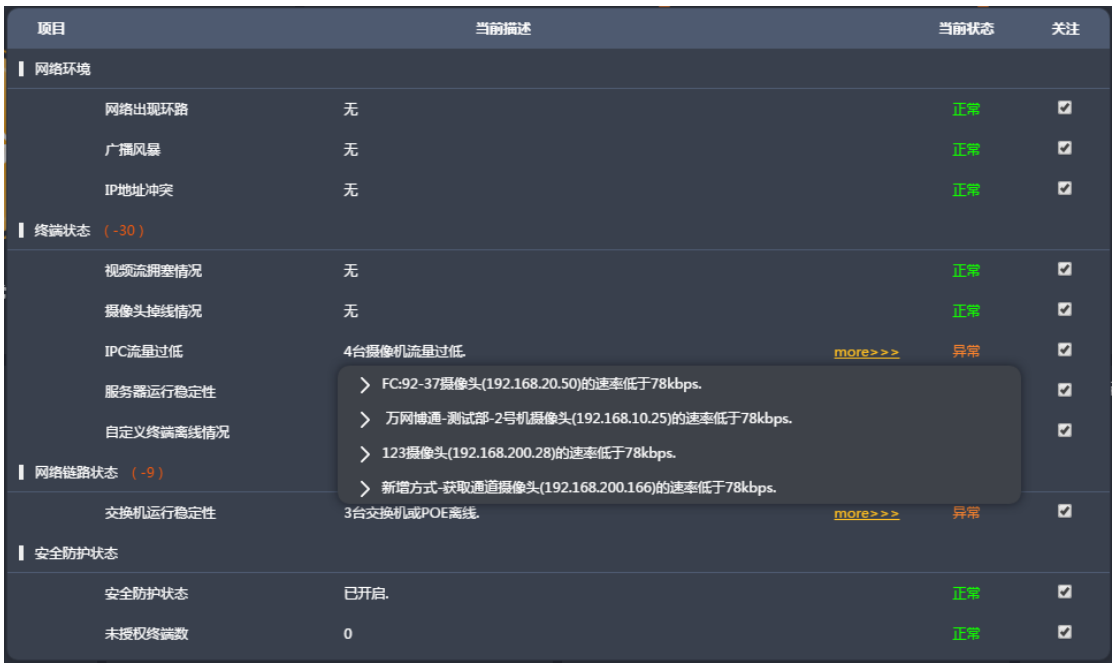
网络环境检查项包括环路检测、广播风暴检测、IP 地址冲突检测；

终端状态检查项包括视频流拥塞情况、摄像机掉线情况、IPC 流量检测、服务器运行稳定性、自定义终端离线情况；

网络链路状态主要检测交换机的运行情况；

安全状况主要检测安全防护开启状态以及入侵设备检测。

出现异常项，网络健康指数分值会进行相应的扣分，点击查看详情即可查看异常情况，而点击异常项对应的 more 按钮more >>>，可定位到实际设备，若存在个别项不需要进行关注，则可将对应关注框取消勾选，取消关注后，该项出现异常也不会进行分数的变更。

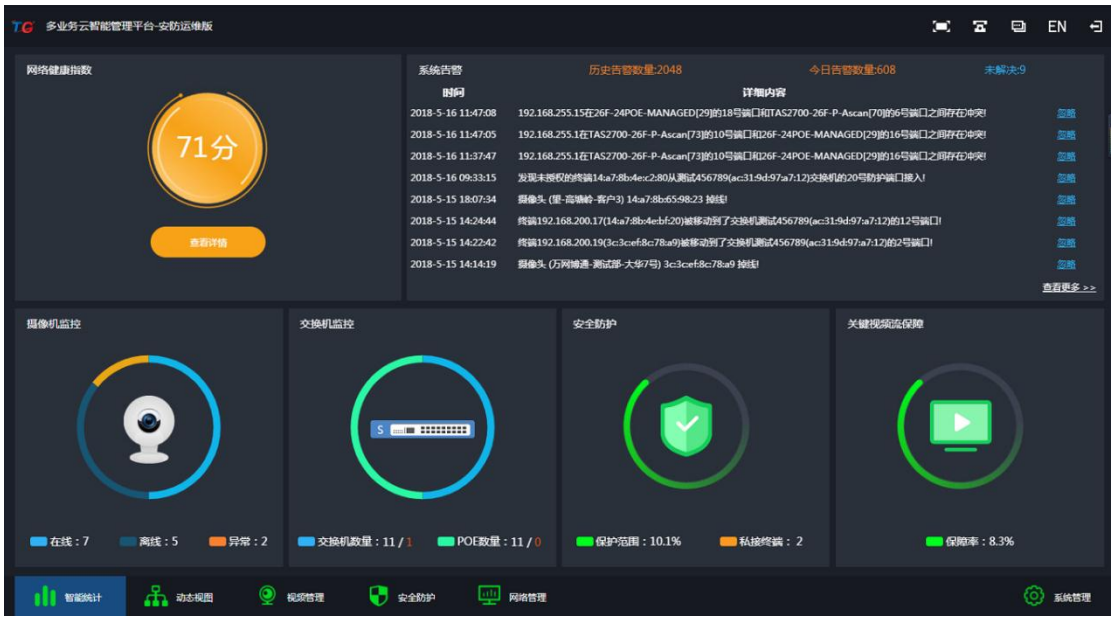


9、实时监测告警

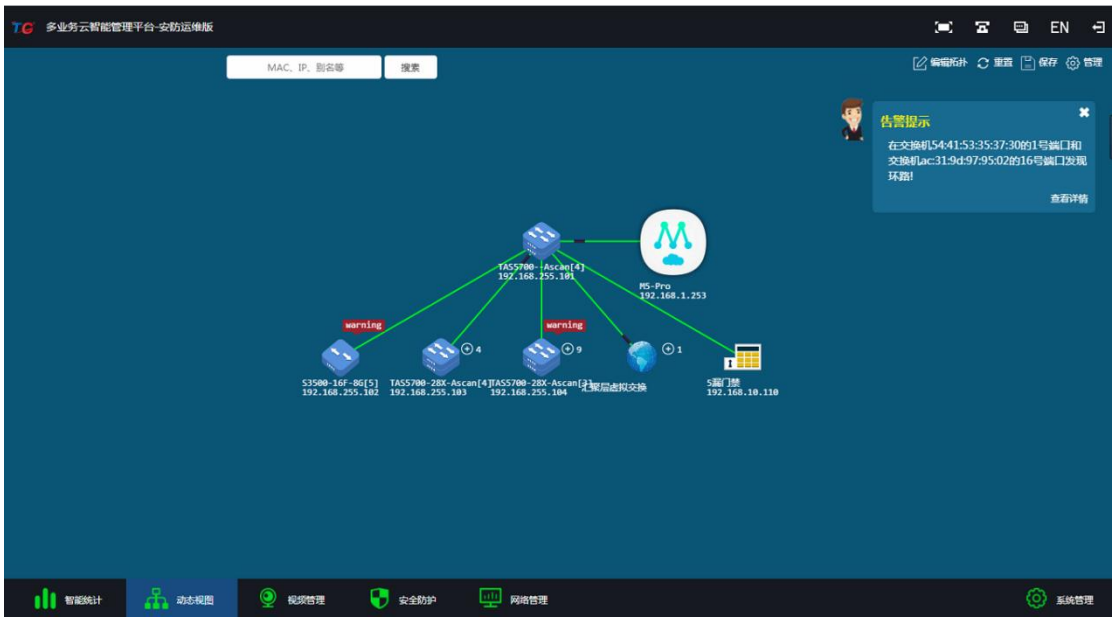
9.1 告警

实时对网络进行监测，出现环路、IP 冲突、广播风暴、交换机或前端设备掉线、服务器掉线、私接终端接入、已防护终端被移动等异常问题，会及时进行告警，且会将告警记录在日志中，便于数据统计。

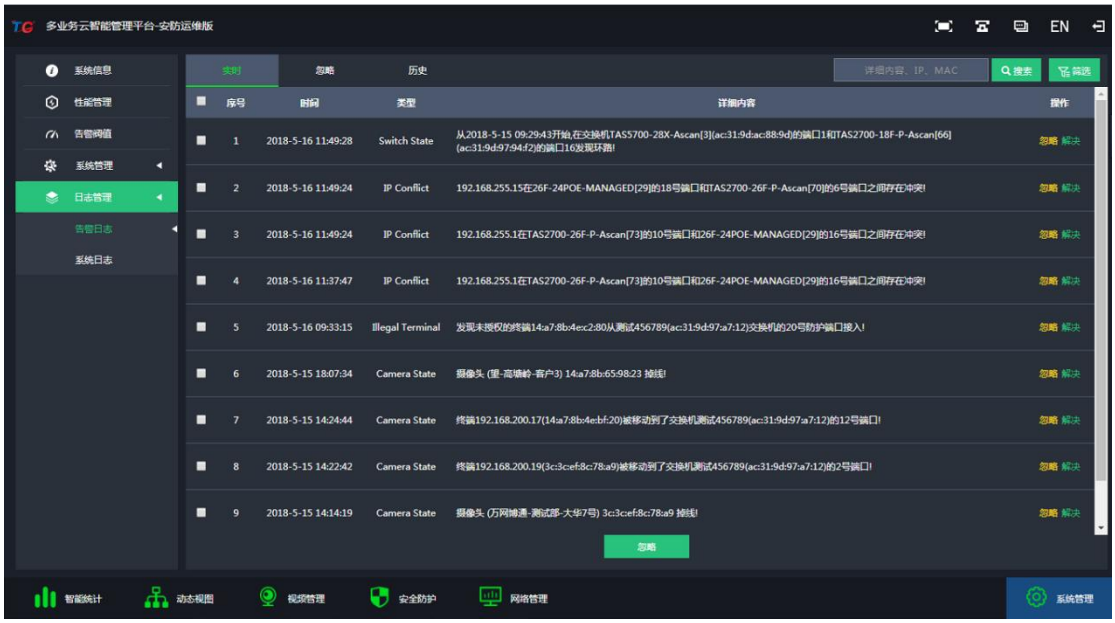
在智能统计->系统告警页面，出现上述异常问题时，会实时进行告警，且点击告警项可查看详情，环路和私接终端接入告警，可在详情页面直接进行禁用环路端口或对私接终端授权操作，并且，问题得到解决时，告警提示会自动取消，若告警项为已知且无需解决的问题，可点击告警项对应的忽略按钮进行忽略显示；



在动态视图页面，出现上述异常问题时，会实时进行弹窗告警，且会定位至具体位置具体设备中，有利于问题排查与解决；

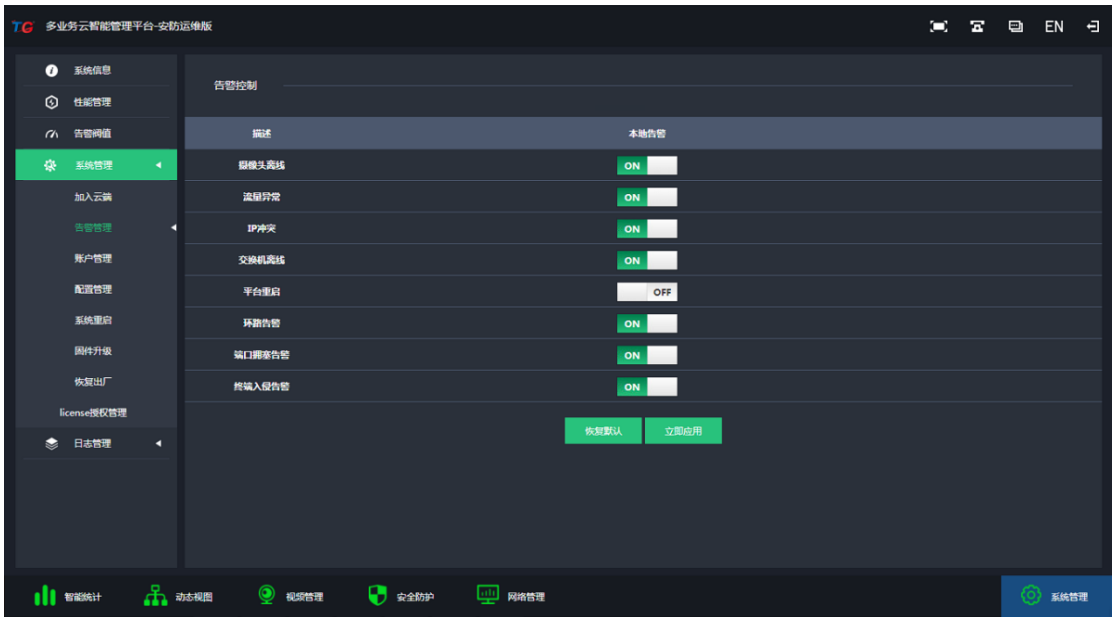


在系统管理->日志管理->告警日志页面，可查看所有未解决、已解决或已忽略的告警项。



9.2 告警开关配置

默认所有类型的告警均为开启状态，出现异常会有相应的告警提示，而在系统管理->告警管理页面，可关闭任意类型的告警，关闭后，出现已关闭类型的告警，不会有告警提示。（ ON ON 为开启告警， OFF OFF 为关闭告警）

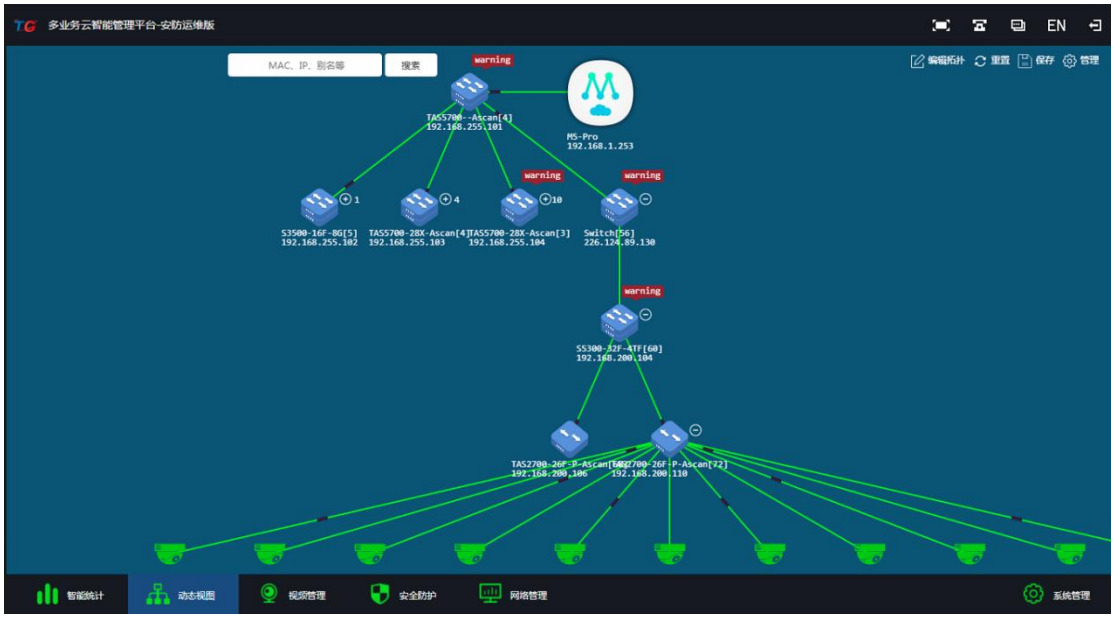


10、多层可视化动态拓扑

在平安城市或者大型企事业单位、园区等二层、三层网络监控环境下，整个网络环境涉及服务器、交换机（包括 POE 交换机）、摄像头、可视对讲、NVR 等设备累计少则几百台多则上万台，TG“多层可视化动态拓扑”能够整体实现对内部网络各个节点监控和管理，识别不同设备类型、IP 地址、MAC 地址等等，并生成网络拓扑。支持对每个交换端口流量、链路状态等进行数据分析。在拓扑中点击任一接入层的交换机，可以查看该交换机下每台摄像头上下流量的抖动情况，通过对比数据，网维人员能够清晰判断摄像头状态是否正常。同时，当网络异常时可以在拓扑上进行故障的快速定位，支持设备搜索、网络告警等功能。

10.1 可视化告警

当网络中出现异常时，如摄像机离线、交换机离线、IP 冲突、出现环路、端口丢包、网络拥塞、终端入侵、自定义设备离线等告警，则会在拓扑图中进行可视化告警，一出现时会有弹窗告警，后续查看即可通过点击 warning warning进行查看，可明确异常项所处位置具体设备，快速的解决问题。



10.2 拓扑图生成

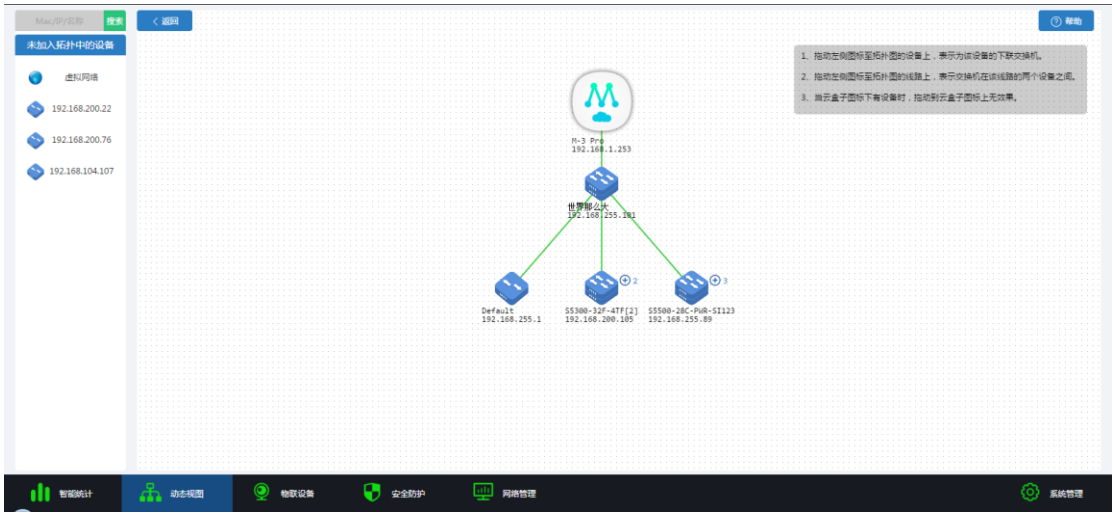
通过点击右上角的“重置”按钮，自动学习拓扑关系并生成，拓扑建立完成后，需要点击保存按钮，进行拓扑保存，否则平台重启，拓扑图需要重新进行学习。

10.3 编辑拓扑

当网络环境中存在交换机无法以重置的方式加入到拓扑中时，可通过拓扑编辑的方式，完善无法自动学习的拓扑关系。

点击“编辑拓扑”按钮，左侧设备栏将会显示所有未加入到拓扑图中的交换机，亦可选择虚拟交换机（一般非管理型交换机可使用虚拟交换机来替代），拖动至右侧拓扑图相应的位置中：①拖动至交换机图标中，表示拖动的交换机在目标交换机的下联；②拖动至拓扑图的链路中，表示拖动的交换机在该链路之间。

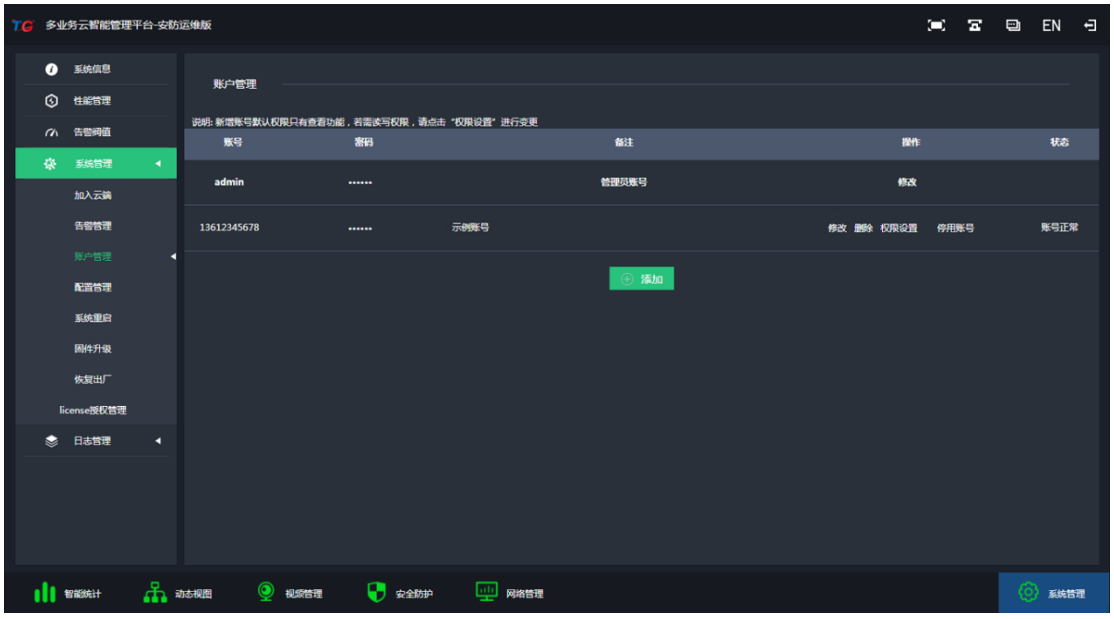
注意：①受第三方管理的交换机，需要手动加入拓扑图中，且该交换机的下联交换机也需要手动加入到拓扑图中；②手动加入的拓扑图，端口号默认为 255，修改需要在动态视图中双击链路进行修改。



11、账号权限管理

平台支持不同账号拥有不同的操作权限，最高权限为管理员账号，使用管理员账号登录平台页面，可在系统管理->账户管理页面，添加不同权限的账号，解决了多人员维护，不同的人员对平台操作权限不同的需求。

点击添加按钮 添加 ，输入账号的名称以及密码，以及对账号的备注信息，点击保存按钮即可完成账号添加。添加的账号默认仅有查看平台的权限，无操作权限，若需要为账号赋予操作权限，则可点击账号对应的“权限修改”按钮，勾选需要赋予模块的操作权限，保存即可。（勾选则赋予操作权限，未勾选则仅有查看权限）



12、TG 云端远程管理

TG 多业务云智能管理平台 NMSS 系列全面支持 TG 云端，通过虚拟化技术，可让每个客户通过手机、平板、PC 任何时间任何地点远程管理自己分布在全国各地安防项目网络，可以通过丰富详细的多维度统计了解项目整体运行情况，也可通过全球范围内地图定位项目所在地精准位置，亦或通过项目集权化管理或设备分类管理、一键跳转任意设备后台等等，解决故障不再需要亲临现场，完全可以远程解决。

配置 NMSS 平台的 IP 地址，使其可访问外网，并在 NMSS 平台的系统管理->加入云端页面，输入商户名称、配置所属行业与联系地址，输入云端账号，保存即可加入云端。

13、手机微信小程序随时随地

专为多业务云智能管理平台系列产品开发的 “云端”微信小程序，可以让用户随时随地对网络运行情况实时监控、管理、智能告警，让用户真正体验到 TG 云服务，特别适合大型网维商及企业 IT 管理员。