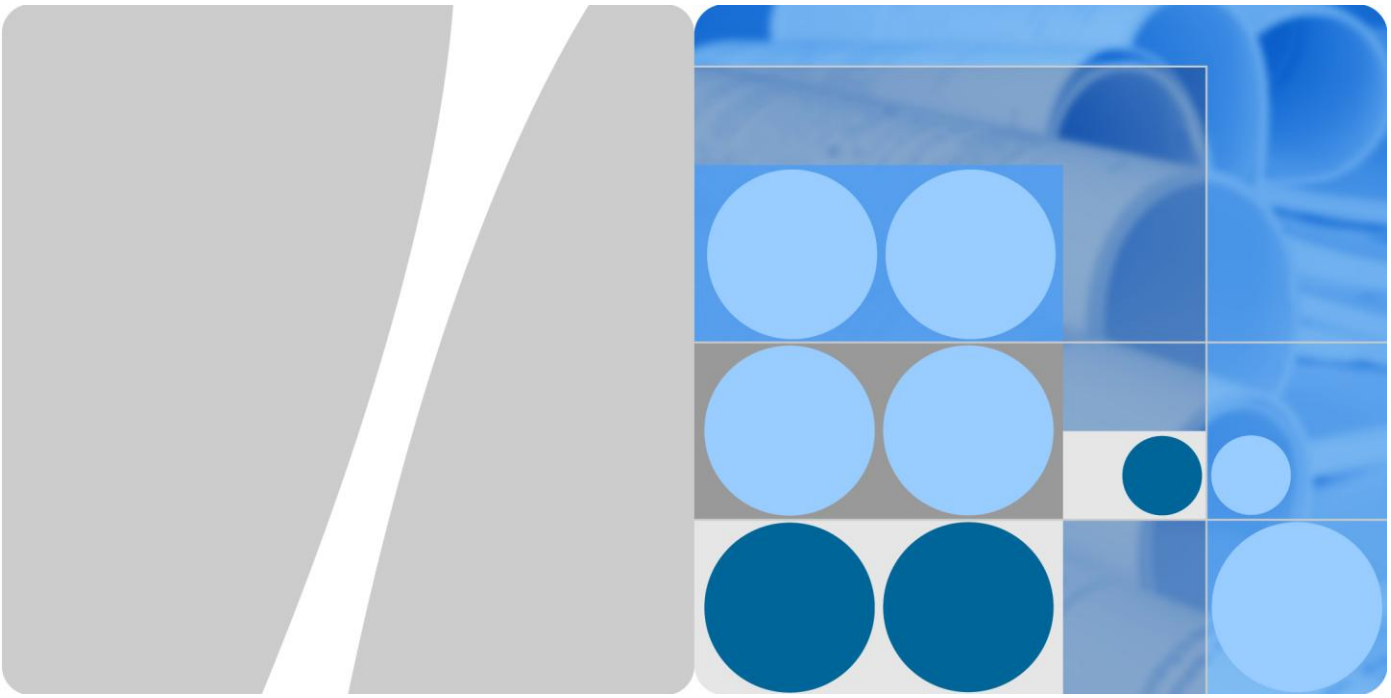


eSight V300R001C10 产品描述

文档版本 01

发布日期 2013-12-10

华为技术有限公司

商标声明


和其他华为商标均为华为技术有限公司的商标。

本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： http://enterprise.huawei.com

前 言

概述

本文档介绍了 eSight ICT 统一管理系统（以下简称 eSight）的网络地位、产品架构、组网应用和功能特性。同时提供了 eSight 的配置要求和技术指标。

本文档指导用户了解 eSight 的功能特性。

读者对象

本文档主要适用于以下工程师：

- 网络规划工程师
- 数据配置工程师
- 系统维护工程师

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
	用于警示紧急的危险情形，若不避免，将会导致人员死亡或严重的人身伤害。
	用于警示潜在的危险情形，若不避免，可能会导致人员死亡或严重的人身伤害。
	用于警示潜在的危险情形，若不避免，可能会导致中度或轻微的人身伤害。
	用于传递设备或环境安全警示信息，若不避免，可能会导致设备损坏、数据丢失、设备性能降低或其它不可预知的结果。 “注意”不涉及人身伤害。

符号	说明
说明	用于突出重要/关键信息、最佳实践和小窍门等。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。

修订记录

修改记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

文档版本 01 (2013-12-10)

第一次正式发布。

目 录

1 产品定位和特点

1.1 产品定位

eSight 系统是华为公司研制的新一代面向企业基础网络、统一通信、智真会议、视频监控和数据中心的整体运维管理解决方案，支持对多厂商和多类型的设备进行统一的监控和配置管理，并对网络和业务质量进行监视和分析，实现对企业资源、业务、用户的统一管理以及关联分析。同时，eSight 提供灵活的开放平台，支持企业通过定制开发，量身打造自己的智能管理系统。

1.2 产品特点

eSight 系统具有客户端轻量化、客户端 Web 化、跨操作系统产品和子系统独立等特点。eSight 系统最多可管理 20000 个网元，可支持 100 个客户端同时在线。

多厂商设备管理能力

eSight 能够统一管理华为、H3C、CISCO、ZTE 等厂商的设备，以及 IBM、HP、SUN 等厂商的 IT 设备。eSight 预置对 H3C、CISCO、ZTE 等厂商主流设备的管理能力，同时提供灵活的自定义能力。

- 对于支持标准 MIB（RFC1213-MIB，Entity-MIB，SNMPv2-MIB，IF-MIB）的非华为设备，eSight 通过自定义设置就能达到与预置的非华为设备同样的管理能力。
- 对于不支持标准 MIB 的非华为设备，可以通过打网元适配包的方式进行适配。

差异化的版本

eSight 提供精简版、标准版和专业版等多版本形态，相应的功能简单介绍如下。

版本类型	功能
精简版（网络设备）	• 网络设备的告警管理、性能管理、拓扑管理、配置文件管理、网元管理、链路管理、日志管理、物理资源、电子标签、IP 拓扑、智能配置工具、自定义设备管理、安

版本类型	功能
	全管理、终端资源、MIB 管理、VLAN 管理 ● 系统监控工具、数据库备份/恢复工具
标准版	● 精简版（网络设备）功能 ● 分级网管 ● 设备管理组件（统一通信、智真、视频监控、存储、主机、eLTE 终端） ● 业务管理组件：OpenSDK 组件、智能报表组件、存储报表管理组件、WLAN 管理组件、MPLS VPN 管理组件、MPLS Tunnel 管理组件、SLA 管理组件、网络流量分析管理组件、Secure Center 安全策略管理组件、IPSec VPN 管理组件、基础设施管理组件
专业版	● 标准版功能 ● 数据中心 nCenter 管理组件 ● Linux 双机系统支持双机热备份功能

多业务管理组件

eSight 基于组件化设计，用户可按需构建专属管理系统。eSight 支持的组件如表 1-1 所示。

表1-1 eSight 组件

组件类别	组件名称	组件描述
管理平台	eSight 管理平台	提供基础网络管理功能，如资源管理、拓扑管理、故障管理、性能管理等。
设备管理组件	eSight 网络设备管理组件	网络设备管理提供网络设备的基本管理和配置功能，包括网络设备的发现和维护、路由配置、接口管理、二层链路管理、IP 拓扑、设备配件等。
	eSight 存储设备管理组件	存储设备管理提供多类型、多厂商存储设备的统一管理，包括存储设备的发现、维护、查询等。
	eSight UC/CC 设备管理组件	提供方便、快捷的统一通信设备配置功能，并提供向导式的业务安装配置，一站完成业务部署，实现端到端的可视化监控网络信息，并能直观地展示故障信息，快速定位解决问题。
	eSight 视频监控设备管理组件	提供对视频监控业务资源的发现、业务拓扑、性能和数据分析的端到端管理，能有效

组件类别	组件名称	组件描述
		提升视频监控设备管理的质量和效率。用户通过对业务的性能、告警、等多种监控手段，监控当前业务的运行状况，快速定位业务故障。
	eSight 智真设备管理组件	提供对智真会议资源的发现、业务拓扑、性能的端到端管理，能有效提升智真会议设备管理的质量和效率。用户通过对业务的性能、告警、等多种监控手段，监控当前业务的运行状况，快速定位业务故障。
	eSight eLTE 设备管理组件	提供华为 eLTE 终端设备 PnP 方式接入、设备固件升级、设备配置管理、设备远程维护等。
业务管理组件	eSight Open SDK 组件	提供 SNMP、HTTP 等被集成接口，供第三方系统进行集成。
	eSight 智能报表组件	预置了丰富的报表模板，满足大部分管理场景；同时提供专业报表设计工具，满足个性化统计报表定制的需要。
	eSight 存储报表管理组件	提供存储容量，性能分析报表，满足客户分析性能瓶颈，实施均衡策略，扩容存储。
	eSight WLAN 管理组件	提供对园区无线网络资源（AC/AP）的管理，以及无线网络的故障诊断，有线无线一体化 TOPO 展示。
	eSight MPLS VPN 组件	提供对 MPLS VPN 配置的自动发现、展现 VPN 网络逻辑结构，并提供对 VPN 的业务状态和质量的监控统计。
	eSight MPLS Tunnel 管理组件	自动发现网络中已部署的 MPLS TE 隧道、LDP 隧道，动态呈现网络隧道运行状态的变化，实现网络路由的可视化管理。
	eSight 网络 SLA 管理组件	自动对网络线路进行周期诊断和临时诊断，协助用户评估网络服务质量。
	eSight 数据中心 nCenter 管理组件	对数据中心网络进行统一管理的系统，主要用于管理部署虚拟化的数据中心接入网络。
	eSight 网络流量分析管理组件	基于报文来源/目的、协议、应用对网络流量报文进行分析，协助用户了解网络流量分布。
	eSight IPSec VPN 管理组件	提供 IPSec VPN 业务的图形化管理，主要功能为：IPSec VPN 发现和 IPSec VPN 拓扑，查看 VPN 通道信息。
	eSight 安全策略管理	提供对华为网络安全设备进行集中策略管理

组件类别	组件名称	组件描述
	组件	的功能，主要用于管理防火墙等设备的安全策略、IPS 策略和 AV 策略等。
	eSight 基础设施管理组件	提供机房内供电、制冷、机柜、门禁、物理安全、环境、消防、采集器、照明等基础设施管理功能，以及增强的机房能效管理功能、机房温度云图功能和机房容量管理功能。

支持多种操作系统

eSight 基于华为公司统一的 B/S 架构应用平台 iEMP，支持 Windows、SUSE Linux 操作系统，支持 Oracle 、MySQL、SQL Server、GaussDB 数据库。

客户端轻量化、Web 化

eSight 系统是基于 Web 的，客户端运行在浏览器之上，系统升级或维护时只需更新服务器端软件即可，这样就大大减轻了客户端电脑载荷，减少了系统维护与升级的成本和工作量。

系统可靠性

eSight 系统支持进程异常自动重启功能。

eSight 系统提供的维护工具可监控 eSight 进程，当检测到这些进程异常中止时，将重启 eSight 进程。进程异常自动重启保障了在无人值守时的系统能正常运行，减少故障恢复时间。

eSight 支持数据备份恢复功能，包括自动备份和手工备份。系统可以自动周期备份数据，备份周期可以设定。此外，用户可以通过手工备份功能，随时进行备份。备份数据可被保存到外部设备中。恢复机制为防止因系统崩溃或升级失败所造成的系统数据破坏，可以使用恢复功能来恢复到最近一次备份的数据。

安全性

eSight 从系统、网络、数据、操作维护等多个层面提供了多种安全保障机制。

- 系统安全性

  系统安全包括操作系统、数据库、中间件可以正常运行，以支撑应用各个应用软件的运行。

  - 补丁策略
  - 加固策略
  - 密码策略
  - 认证和鉴权
  - 数据加密

- 安全日志
- 最低权限原则
- 文件权限管理

- 网络安全性

  网络安全包括交换机、路由器、防火墙等网络设备的正常运行，以确保网络层的安全策略得到落实。

  安全策略包括：

  - 网络隔离，通过路由器将局域网与外部网隔离，增强数据通信安全。
  - 系统配置网络防火墙，以保证系统网络的安全。
  - 对外部能够访问的服务权限进行控制和管理。

- 数据安全性

  数据安全包括用户身份信息、系统正常运行的配置信息、系统运行的日志、数据库数据等数据的存储、传输、管理的安全性。

  - 加密策略：密感数据加密存储和传输
  - 用户管理策略：最小授权
  - 备份\恢复策略：定时备份关键数据
  - 数据存储安全：支持 HA 双机倒换机制，及时恢复系统运行

- 操作维护安全

  从用户、应用、审计等多个层面提供安全机制，构建操作维护的安全性。

  - 分组、分权限访问机制

    采用分组、分权限访问机制，操作员登录系统必须提供用户名和密码，登录后只能进行其权限内的操作。利用集中管理和身份认证，实现不同的用户通过不同的权限管理，利用信任机制来有效控制共享信息和资源，有效防止用户非法进入或越权进入系统。

  - 登录访问控制策略：密码策略、登录锁定解锁、鉴权策略
  - 审计日志：安全日志、操作日志、系统日志
  - 客户端自动注销机制

    当操作员中断操作一定时间，客户端将自动注销，防止非法用户的操作。

  - 应用软件安全机制

    提供密码和身份认证，采用高强度的数据加密算法对敏感的用户信息数据进行加密保存。系统为每个用户分配一个密码，在为用户提供各种服务时，系统对用户密码进行校验，以保护用户信息的安全性。

弹性扩展架构

支撑弹性扩展架构能力，做到增加服务器能够增加网管系统管理容量，解决现网扩容实现老硬件利旧问题，保护客户已有投资，实现平滑扩容。

被集成能力

基于开放总线、开放接口和信息建模，支持异构系统集成，实现与第三方系统快速对接。

2 产品架构

2.1 Web 化架构

eSight 系统采用 B/S 架构，拥有 B/S 架构的先天优势，通过客户端的浏览器即可访问 eSight 系统，当系统升级或维护时只需更新服务器端软件，减轻了客户端电脑载荷，简化了系统维护与升级操作，降低了用户的总体成本（TCO）。

另外，B/S 架构还具有如下优点：

- 具有分布性特点，可以随时随地进行查询、浏览等操作。
- 免客户端，新业务发布时只需要更新服务端。

2.2 组件化

eSight 采用组件化架构，在统一的 eSight 管理平台之上，提供丰富多样的组件，客户可以根据自己的情况选择所需要的组件。

2.3 独立的网元适配

eSight 采用扩展点机制实现了功能的增量开发与网元版本适配包的增量开发，达到不用修改原有发布包代码即可增加新的功能或新的网元适配包。基于 OSGI 平台的模块化框架使得各业务组件都可做到独立升级、打补丁。

当需要支持新的功能时，可以开发新的功能插件包部署到系统中；当需要适配新的设备时只需要增加新的网元适配包即可。功能插件包及网元适配包都以 Bundle（可理解为插件）的形态部署到 eSight 的 OSGI 容器中。

2.4 北向接口

通过 eSight 北向接口可以灵活的将 eSight 集成到不同的 OSS 管理系统中，满足不同的 OSS 系统集成的需求。

2.5 南向接口

eSight 南向接口实现 eSight 与设备之间的对接，完成 eSight 对设备的管理功能。eSight 支持的南向接口类型，包括 SNMP、Telnet/STelnet、FTP/SFTP/FTPS、TR069、华为 MML（Man-Machine Language）、SMI-S 接口、Modbus 接口等。

SNMP 接口

eSight 支持标准的 SNMP V1/V2C/V3 接口，通过 SNMP 接口可以实现 eSight 同网络设备的链接。用于发现网络设备，实现业务配置数据同步、故障管理和性能管理等基本管理功能。SNMP 是基于 TCP/IP 的应用层网络管理协议，它使用 UDP 协议作为传输层协议，能管理支持代理进程的网络设备。

Telnet/STelnet 接口

Telnet 接口和 STelnet（SSH Telnet）接口是管理网络设备的基本接口之一，用于远程登录和管理设备。通过 Telnet/Stelnet 接口弥补通过 SNMP 接口管理的不足，并增加部分额外的管理功能。eSight 通过 Telnet/STelnet 接口，可以与网络设备连接。

- Telnet 用于从 eSight 智能配置工具或网管启动命令窗口访问网元，直接使用 CLI 命令行对网元进行维护配置操作。Telnet 是基于 TCP/IP 的应用层网络管理协议，它使用 TCP 协议作为传输层协议，给网络通信提供服务。

说明

Telnet 采用明文传输通信数据，存在安全隐患，建议和 SSH 等安全协议配合使用。

- SSH（Secure Shell）是一种类似于 Telnet 的工具。但是 SSH 在数据传输的过程中使用加密的数据。通过提供认证、加密和鉴别来保证网络通信的安全性，支持 password 和 RSA 认证，而且 SSH 传输的数据是经过压缩的，可以加快传输的速度。SSH 也是 TCP/IP 的应用层网络管理协议，在传输层使用 TCP 协议，但在应用层对数据进行了加密。

TFTP/FTP/SFTP/FTPS 接口

TFTP/FTP/SFTP/FTPS 接口用于备份设备数据。TFTP/FTP/SFTP/FTPS 是基于 TCP/IP 的应用层网络管理协议。

- FTP（File Transfer Protocol）是用于在网络上进行文件传输的一套标准协议。

说明

FTP 协议本身有安全风险，建议使用 SFTP 和 FTPS 等安全协议。

- SFTP（SSH FTP）通过 SSH 协议提供安全的文件传输和处理功能。使用 SFTP 方式备份时，指令与数据在传输过程中都是经过加密的。
- FTPS（FTP over SSL）为 FTP 及数据通道增加了 SSL 安全功能，是一个在客户机和具有 SSL 功能的服务器之间的安全连接中数据进行加密与解密的协议。
- TFTP（Trivial File Transfer Protocol，简单文件传输协议）是 TCP/IP 协议族中的一个用来在客户机与服务器之间进行简单文件传输的协议，提供不复杂、开销不大的文件传输服务。

TR069 接口

TR069 是数字用户线（DSL）论坛（已改名为 Broadband Forum）制定的一个面向终端设备的网管协议，称为“用户终端设备广域网管理协议（CWMP）”，DSL 论坛的文档编号为 TR069。

该接口用于 IP Phone、EGW、AT、SBC、eLTE 终端等相关设备的接入。

MML 接口

MML：Human-Machine Language(Formerly Man-Machine Language)，华为公司的 MML 接口主要有两方面的功能：一是日常的操作维护，相比图形界面而言，命令行简捷、方便，也便于脚本支持；二是用于网管接入，相比内部的二进制协议，MML 协议更加透明、规范，便于上层网管进行分析处理。以上两方面的需求决定了对 MML 命令格式的两大要求：既要方便操作人员在字符终端上直接输入（人机接口），也要方便网管接入时计算机的解析识别（机机接口）。要达到这两方面的要求，MML 命令在格式上必须严格遵守一定的规范，否则不仅人类输入困难，计算机也无法解析。

MML 一般有三个端口：维护端口、告警端口、性能端口。

- 维护端口用于下发命令用的，例如登录命令、创建性能统计任务的命令、获取信息命令等。
- 告警端口是用于 MML 设备上报告警用。
- 性能端口是用 MML 设备上报性能报文用。

这三个端口是 TCP 连接，MML 设备是服务端，Med 是 MML 的客户端，当鉴权通过时，就可以开始接受性能和告警数据了。

一些设备只有告警和性能端口，而没有维护端口，因设备而定。

SMI-S 接口

eSight 支持通过标准的 SMI-S 接口接入和管理存储设备，以提供存储设备的资源监控、性能分析、故障监控等基本功能。

SMI-S，是存储管理建议规范（Storage Management Initiative Specification）的简称，由美国存储网络工业协会（SNIA）制定。SMI-S 是一种中间件性质的规范，定义了存储管理软件和受管对象之间的交互机制。它提供了多种特性以简化存储区域网（SAN）的管理。SMI-S 是在 CIM/WBEM 基础上实现存储网络管理。CIM/WBEM 实际上是对资源管理的一种通用模型，WBEM 是基于管理技术的工具集，它使用 CIM 作为数据格式，使用 XML 作为数据编码和传输，使用 HTTP 作为接口。

Modbus 接口

Modbus 协议是应用于电子控制器上的一种通用语言。通过此协议，控制器相互之间、控制器经由网络（例如以太网）和其它设备之间可以通信。它已经成为一通用工业标准。有了它，不同厂商生产的控制设备可以连成工业网络，进行集中监控。

Modbus 协议支持传统的 RS-232、RS-422、RS-485 和以太网设备。许多工业设备，包括 PLC，DCS，智能仪表等都在使用 Modbus 协议作为他们之间的通讯标准。

3 产品和应用场景

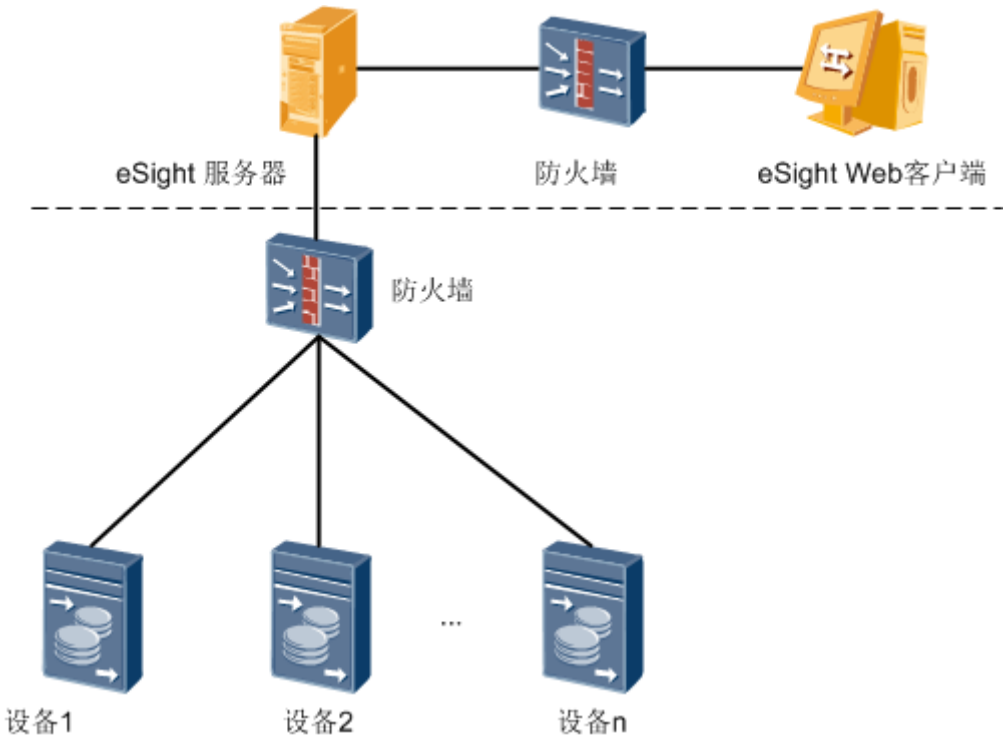
3.1 eSight 部署模式

eSight 部署模式包括单服务器部署、分机部署和高可用性系统部署。

3.1.1 单服务器部署

eSight 单机系统由单个服务器、多个客户端和其他网络设备构成，如图 3-1 所示。

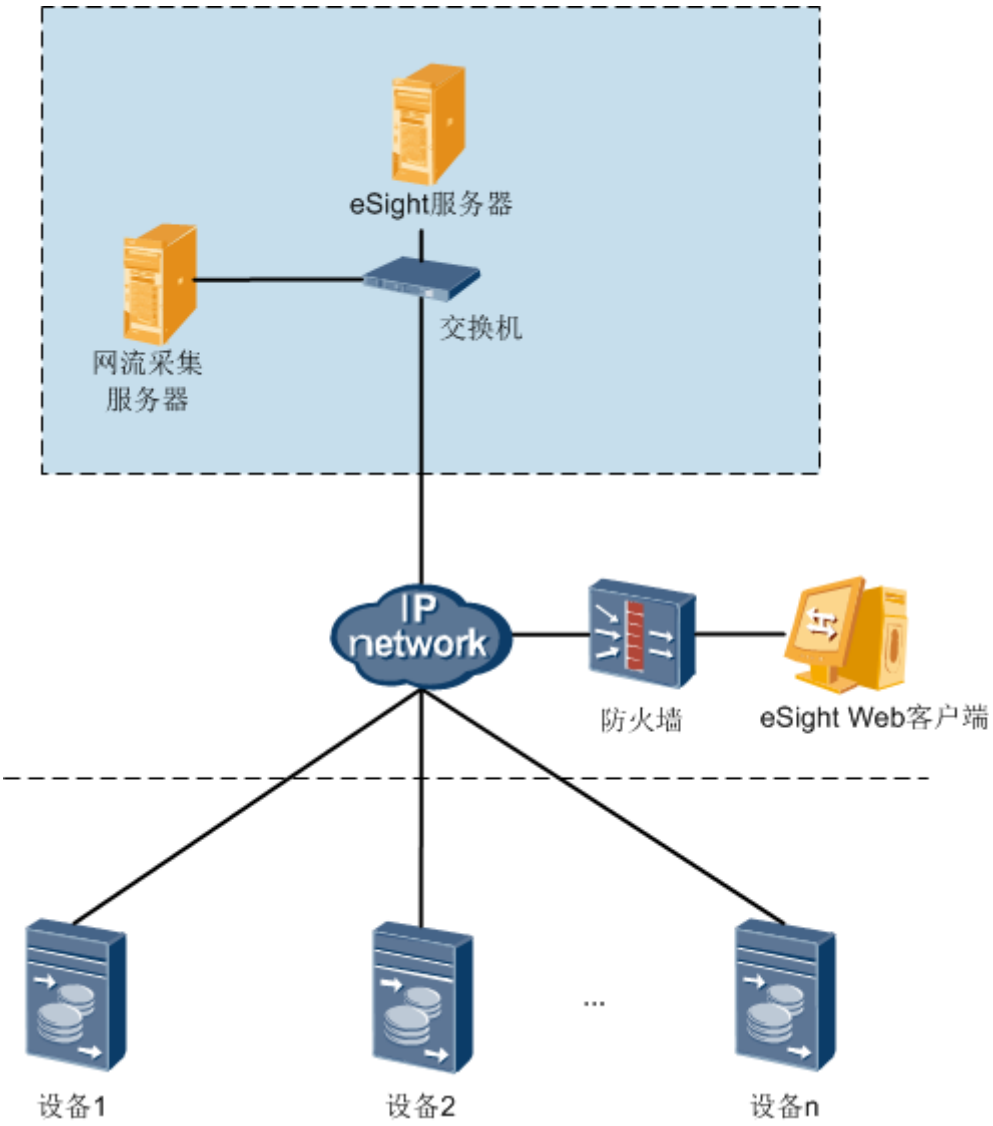
图3-1 单服务器部署



3.1.2 分机部署

在大规模网络管理场景下，eSight 支持将网络流量采集器部署在独立的服务器上，与 eSight 管理平台形成分机部署模式，如图 3-2 所示。

图3-2 分机部署



说明

eSight 分机部署时，最多支持 1 台网络流量采集服务器。

3.1.3 高可用性系统部署

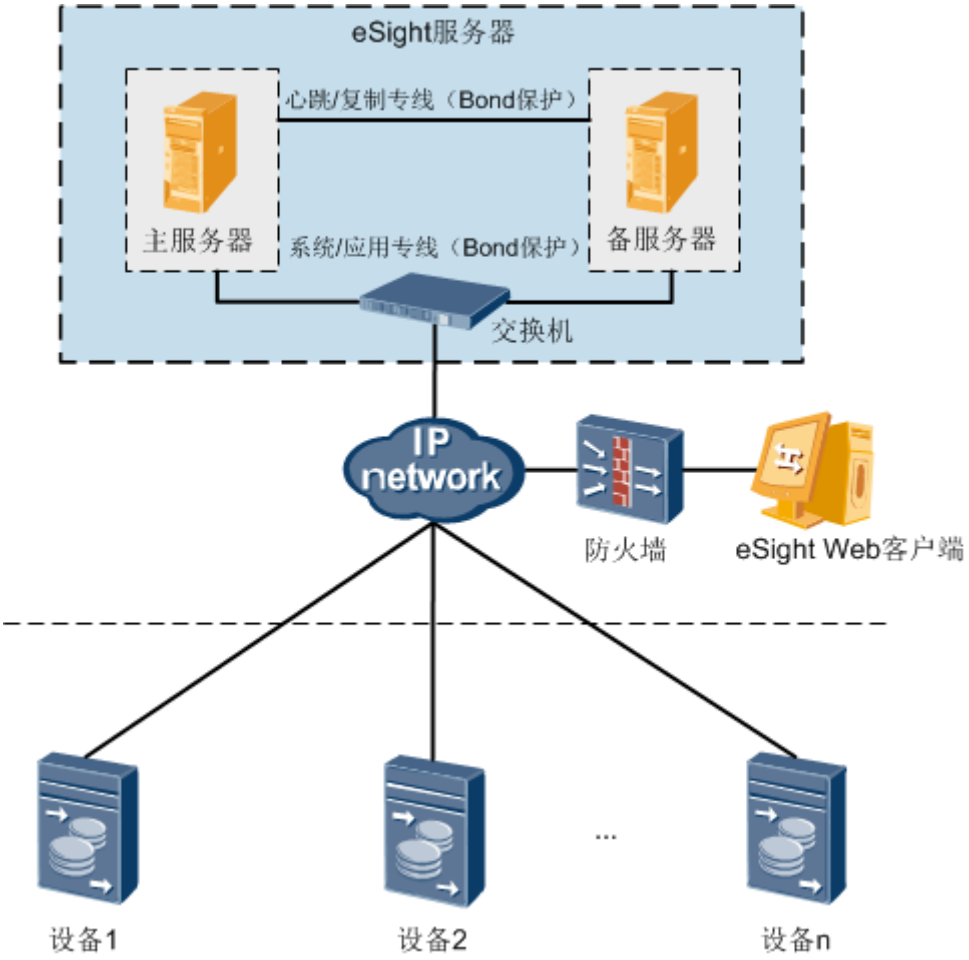
高可用性部署模式适用于对可靠性要求高的场景，eSight 高可用性系统分为本地高可用性系统和异地高可用性系统

本地高可用性系统

eSight 本地高可用性系统由一台主服务器和一台备服务器组成，主服务器和备服务器上分别安装一套 eSight，主、备服务器之间的数据通过复制专线进行同步。当主服务器故障时，系统自动切换到备服务器，保证 eSight 系统运行正常。

本地高可用性系统的主服务器和备服务器之间设置浮动 IP，主、备切换后，设备不需要重新和网管建立连接。

图3-3 本地高可用性系统组网

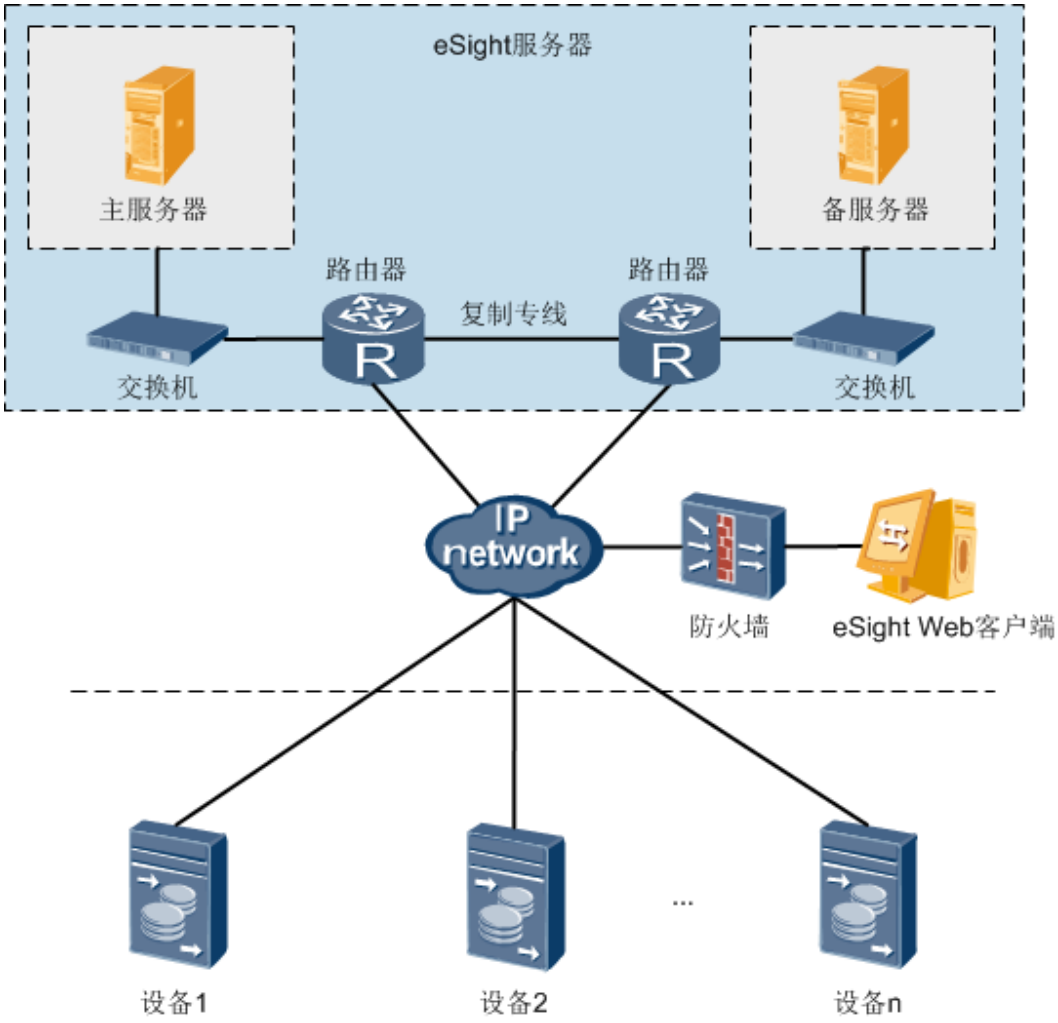


异地高可用性系统

eSight 异地高可用性系统同样由一台主服务器和一台备服务器组成，主服务器和备服务器上分别安装一套 eSight，两台服务器可以部署在远近不同的地点，当主服务器故障时，系统自动切换到备服务器，主、备服务器之间的数据通过复制专线进行同步，保证 eSight 系统运行正常。

由于异地高可用性系统的两个 eSight 服务器使用的是不同的 IP 地址，部署高可用性系统后，被管的设备上需同时设置主、备服务器的 IP 地址，在主、备服务器切换后，设备上的告警等信息会自动发送到备服务器，以保证设备的正常监控和管理。

图3-4 异地高可用性系统组网



3.2 eSight 与设备的组网方式

eSight 可管理华为自研设备和非华为设备，如表 3-1 所示。

表3-1 eSight 管理的设备

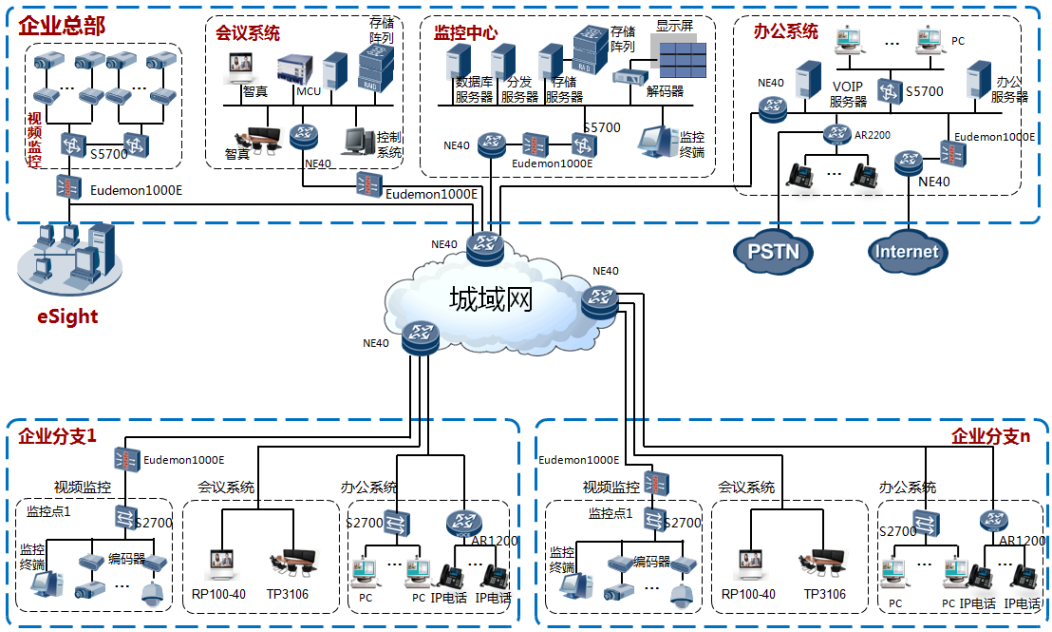
领域	设备
交换机	S 系列交换机，CE 系列交换机
路由器	NE 系列路由器、AR 系列路由器
安全系列设备	安全设备 Eudemon 系列、安全设备 SRG 系列、安全设备 SVN 系列
统一通信设备	eSpace 系列网关设备、UC 外购设备、eSpace UC 应用、eSpace CC 应用

领域	设备
视频监控设备	华为 eSpace IVS V100R100C02 系列视频监控应用
智真会议设备	华为智真会议终端、MCU、TP、GK 等
存储设备	华为阵列、统一存储、虚拟智能存储、海量存储、云存储、虚拟磁带库、第三方存储、FC 交换机等
主机	支持 Windows、Redhat、SUSE 等主流操作系统
eLTE 设备	华为 eA660、eA661 系列 CPE 设备
基础设施	支持对数据中心基础设施层的电源供配电、机房空调、环境、机柜、安防等系统进行管理
非华为设备	预集成的非华为设备：H3C、Cisco 等设备 打印机、服务器等

说明
eSight 与设备的详细配套关系请参见随版本发布的版本说明书中的"与设备的版本配套说明"。

eSight 采用 SNMP、FTP/SFTP、TR069 等多种协议，与各个被管设备进行通讯，eSight 故障对被管理的设备组网和业务没有影响。

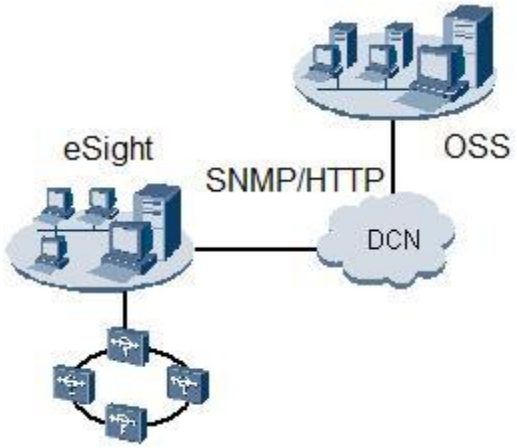
图3-5 eSight 与网元组网方式



3.3 eSight 与 OSS 系统的组网方式

eSight 支持同上层 OSS 等第三方系统的集成，第三方系统可通过 SNMP 或者 HTTP 接口，获取 eSight 系统中管理的网络资源、告警等信息。

图3-6 eSight 与 OSS 系统组网方式图

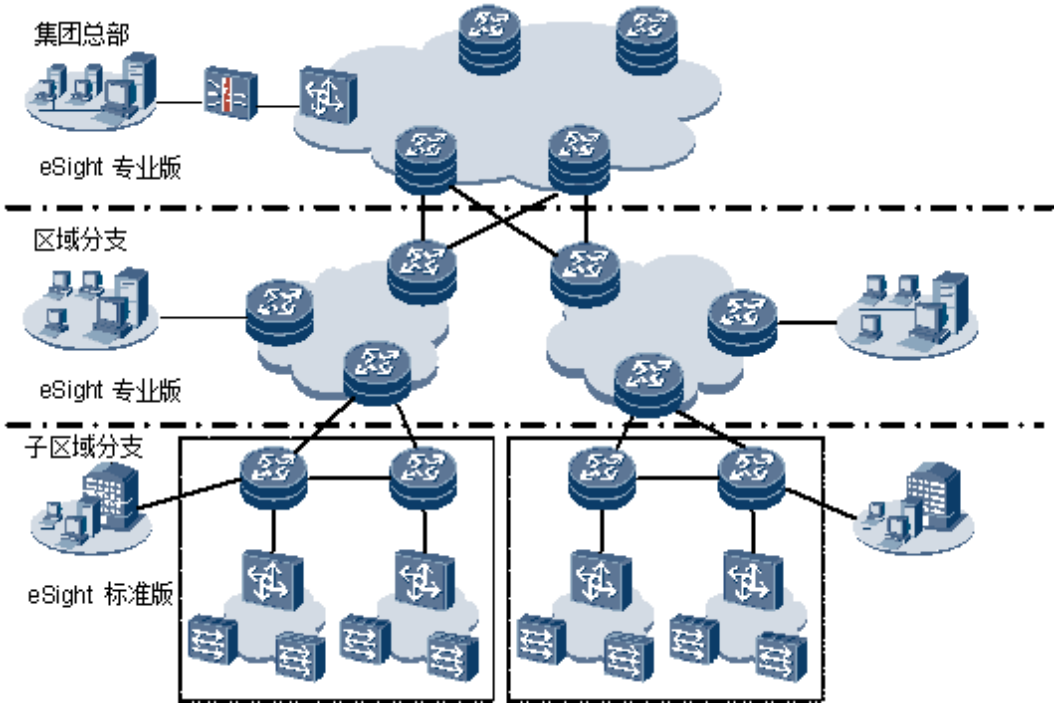


3.4 eSight 分级网管组网方式

eSight 支持分级管理，以满足企业总部监管各地区网络的需求。

在分级部署模式下，上级网管可以把下级网管加入到系统中，并提供打开下级网管界面的链接。当用户单击下级网管链接时，将会弹出一个新的浏览器窗口，在新的浏览器窗口中打开下级网管的登录界面。

图3-7 分级部署模式



4 功能特性

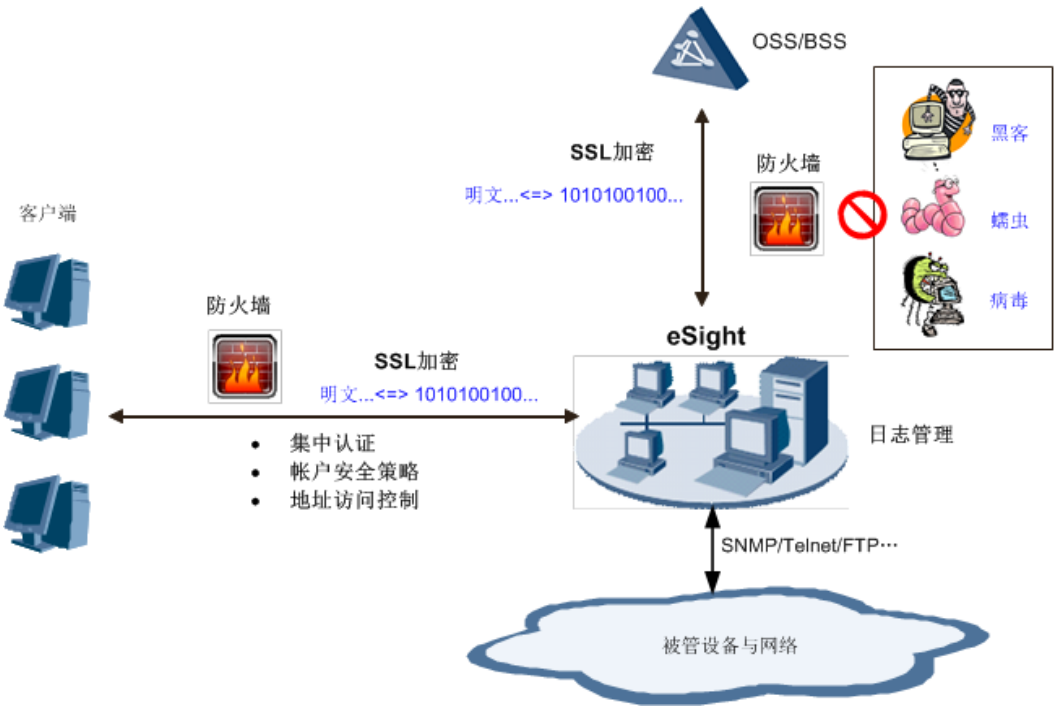
4.1 管理平台

4.1.1 安全管理

安全管理实现对 eSight 系统本身的安全控制，通过对用户管理、角色管理（授权管理——分权分域）、用户登录管理和一系列其他的安全策略，来保证 eSight 的安全。同时，eSight 支持对用户登录、操作和 eSight 运行过程中的日志进行管理，支持数据库备份，进一步完善安全解决方案。

安全管理的实现机制如图 4-1 所示。

图4-1 安全管理实现机制



说明

本节主要描述网管用户安全相关内容。

- 关于日志管理的安全方案，请参见 4.1.2 日志管理。
- 关于数据库备份和恢复，请参见 4.1.7 维护工具一节的备份恢复。

用户管理

用户需拥有合法的用户帐号和密码，才能成功登录 eSight 客户端并进行维护管理操作。eSight 通过用户名及其密码唯一确定了网管用户的登录和操作权限。

eSight 用户密码使用不可逆算法 SHA256 加密，并存储在数据库中。eSight 安装完成后，只提供一个缺省用户：admin 用户。admin 用户拥有所有的操作权限和管理权限。其他用户都是直接或间接地由 admin 用户创建的。

用户属性包含用户名、密码、所属角色、描述和访问控制。用户从其“所属角色”继承了对应的操作和管理权限。“访问控制”属性限定了用户只能在特定时间段、从特定 IP 地址登录 eSight，以确保 eSight 访问安全性。

用户管理包括以下功能：

- 创建用户：eSight 支持创建单个用户和批量创建用户两种创建方式。
- 删除用户
- 查看、修改用户属性
- 修改用户密码
  - 重置密码

    当用户登录 eSight 客户端忘记密码时，可联系拥有用户管理权限的管理员重置密码。密码重置后，用户可以使用新密码登录 eSight 客户端。

说明

admin 用户的密码不能被重置。

  - 修改当前用户密码

    用户可以在 eSight 客户端修改自己的密码。周期性的修改密码，可提高用户信息的安全性。
- 停用、启用用户

  帐号长时间未使用且达到帐号策略设置的帐号连续未使用天数时，帐号会被自动停用。暂时不使用某用户时，也可手工停用该用户。

  若需重新使用该用户时，可启用被停用的用户。

角色管理（权限管理）

角色是权限的集合，用于对用户进行授权。通过角色来对用户进行授权，可以使权限管理更有条理，避免权限管理的混乱。规划了网管用户后，需要给用户设置角色，使其具有对应角色的权限来管理设备。

eSight 角色管理支持创建、修改、删除角色及查看角色属性。

eSight 提供了一个缺省角色：Administrators。“Administrators”是管理员角色，拥有所有管理对象的所有操作权限，且不可修改。

角色属性包含角色名、包含用户、管理对象、操作和描述等。

- 管理对象：指角色可以管理的对象及其配置数据范围。如果 A 角色不可管理 C 设备和 D 对象组，则在拓扑视图上，C 设备和属于 D 对象组的设备对于只属于 A 角色的用户都是不可见的。对象组是多个设备的集合，eSight 支持创建、修改和删除对象组。
- 操作：指角色可以执行的具体操作。将一个设备的多个操作分配给不同的角色，可以达到各角色对同一设备拥有不同的操作权限。

通过设置角色的“管理对象”和“操作”属性，eSight 支持分权分域管理，即只允许用户将权限范围内的操作下发到网元。只有 Administrators 角色下的用户或者拥有“用户管理”权限的用户具备为其它用户分权分域的操作权限。

- 分域是指将网络中的管理对象分配给不同的角色，使每个角色拥有的管理对象范围不尽相同。通过分域，可以实现不同运维部门的人员管理不同范围内的网络对象。
- 分权是指将对管理对象的操作分配给不同的角色，使每个角色拥有的操作权限不尽相同。通过分域基础上的分权，可以实现同一区域不同职责（岗位/运维部门）的管理人员，对区域内管理对象可执行的操作权限不同。

eSight 的分权分域管理实现了网络设备和功能的统一管理，基于设备为单位实现分域管理，基于设备上的功能进行分配权限。

网管用户鉴权管理

eSight 的用户鉴权管理包含 3 种方案：本地认证方式、RADIUS 认证、LDAP 认证。

- 本地认证：网管用户管理、登录鉴权、安全策略完全由 eSight 服务器来集中独立完成。该方式是默认的网管用户登录鉴权管理方式，详细参见基于本地认证的网管用户鉴权。
- RADIUS 认证：用户登录时，eSight 通过 RADIUS 服务器对用户的登录请求进行校验和认证；并根据 RADIUS 服务器上用户所属用户组，映射到 eSight 系统中该用户的所属角色为登录用户授权。详细参见基于 RADIUS 认证的网管用户鉴权。
- LDAP 认证：用户登录时，eSight 通过 LDAP 服务器对用户的登录请求进行校验和认证；并根据 LDAP 服务器上用户所属用户组，映射到 eSight 系统中该用户的所属角色来为登录用户授权。基于 LDAP 的认证方式同基于 RADIUS 的认证方式类似，只是基于的认证协议不同，参见基于 LDAP 认证的网管用户鉴权。

基于本地认证的网管用户鉴权

在本地认证方式下，用户安全管理包括本地用户管理、权限管理、密码策略、帐户策略、登录控制等，从多方面保障 eSight 系统的安全运行。其中，账户策略和密码策略设置后对 eSight 所有的帐户生效。

- 密码策略
  - 密码最小字符个数（系统默认为 8 字符）。
  - 密码不能与历史密码重复次数（系统默认为 3 次）。
  - 密码中允许同一字符出现的次数（系统默认为 3 次）。
  - 密码修改最短时间间隔（系统默认为 5 分钟）。
  - 是否限制密码中至少包含一个特殊字符（系统默认为不限制）。

  - 密码的时效性：包含密码有效天数（系统默认为 90 天）和密码到期提前提醒用户修改的天数（系统默认为 7 天）。
- 帐号策略
  - 帐号名最小字符个数（系统默认为 6 字符）。
  - 帐号停用策略：连续多天（系统默认为 60 天）未使用停用帐号。
  - 帐号锁定策略：限定时间段内连续登录多次失败时，自动锁定帐号一段时间（系统默认为：10 分钟内连续登录 5 次失败后，锁定帐号 30 分钟）。
- 登录控制：登录控制包括用户登录时间段控制和用户登录 IP 地址控制。
  - 用户登录时间段的控制指如果当前时间不在登录时间段内时，用户将不能登录 eSight。
  - 登录 IP 地址的控制是指用户只能从特定 IP 地址的客户端登录 eSight 服务器。这样即使在某些情况下用户 ID 与密码被盗，盗号者也无法登录到 eSight 服务器上，从而进一步提高了 eSight 安全性。
- 客户端自动注销

  为了防止其他人员在用户离开时进行非法操作，eSight 提供设置客户端自动注销的功能。如果在指定时间段内不做任何操作，客户端将被自动注销。

基于 RADIUS 认证的网管用户鉴权

eSight 采用 RADIUS 模式对用户认证时，eSight 用户帐号不再需要管理员预先在 eSight 中创建。登录 eSight 的用户帐号是复用企业已有的、可以被 RADIUS 服务器认证通过的帐号信息。

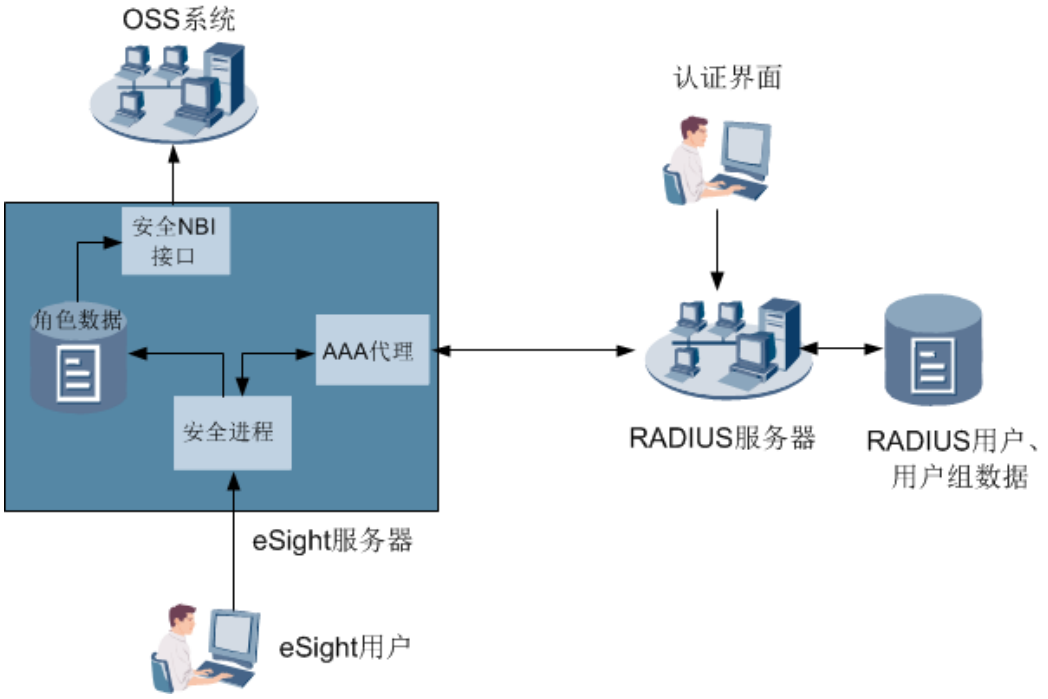
当用户输入用户名、密码登录时，eSight 服务器的安全进程将用户名、密码发送给 RADIUS 服务器。对于通过 RADIUS 认证的用户，eSight 安全进程将会从 RADIUS 服务器上获知用户所属的用户组，并映射到本地角色，实现用户授权。

说明

集成 RADIUS 的认证模式之前，必须保证 eSight 定义的角色名称与 RADIUS 服务器的用户帐号数据库的用户组名称一致，并保证将被授权登录 eSight 的帐号已经划定到了隶属的角色。

基于 RADIUS 认证的用户鉴权流程如图 4-2 所示。

图4-2 RADIUS 用户鉴权



基于 LDAP 认证的网管用户鉴权

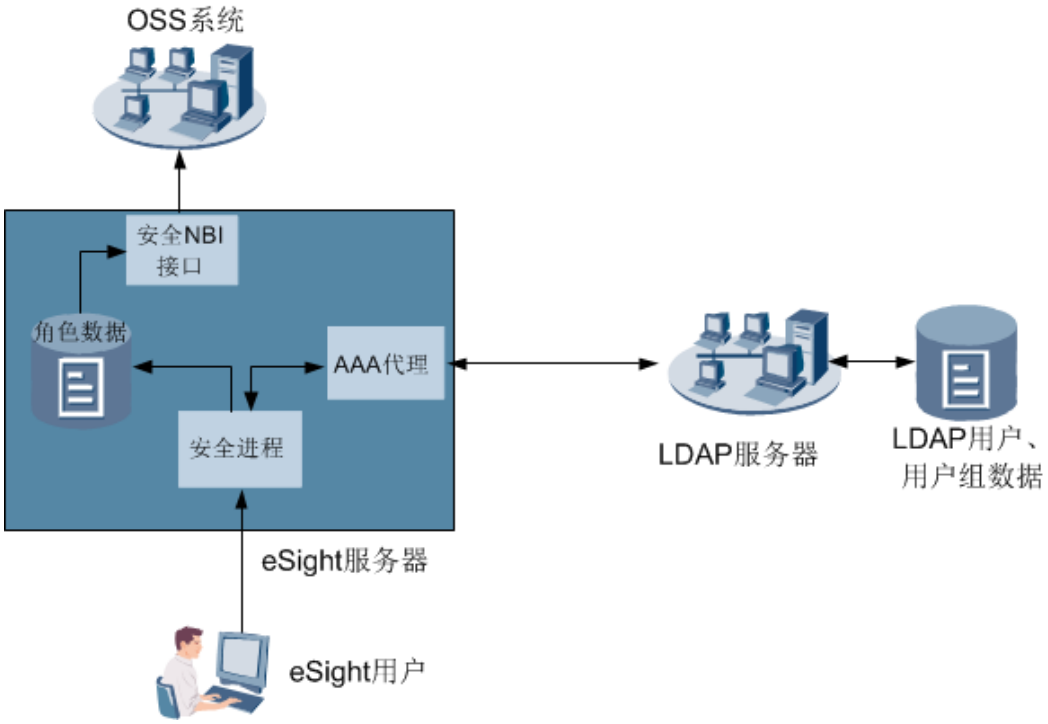
LDAP 在 VPN 和 WAN 中被广泛使用来控制用户连接的各个方面，是一个分布式客户端/服务器系统协议，可以防止未授权的用户访问网络。

基于 LDAP 的认证方式与基于 RADIUS 的认证方式类似，只是基于的认证协议不同。相对于 RADIUS 认证，LDAP 认证支持：

- eSight 和 LDAP 服务器之间的通信支持普通方式（不带加密）、SSL 方式和 TLS 方式。
- 支持多个 LDAP 认证服务器。

基于 LDAP 认证的用户鉴权流程如图 4-3 所示。

图4-3 LDAP 用户鉴权



在线用户管理

- 查看在线用户

  通过查看在线用户，能了解当前登录用户以及登录时间、登录 IP 等信息。

- 强制注销用户

  查看在线用户时，可以通过强制注销操作将用户注销，避免非法登录用户在 eSight 客户端中执行非法操作。

- 用户登录模式切换

  用户登录模式指是否允许多用户同时登录 eSight，一般情况下 eSight 运行在多用户模式下，但如果需要对 eSight 服务器进行特别操作时，可以将 eSight 设置为单用户模式，防止其他用户的操作造成干扰。

  - 进入单用户模式后，eSight 只允许当前用户登录 eSight 客户端，其他所有的在线用户会被强制注销。
  - 退出单用户模式后，其他用户可重新登录 eSight 客户端。

4.1.2 日志管理

eSight 日志信息记录了用户进行的一些重要操作，用户可以查询日志列表并查看日志的详细信息，还可以导出操作日志、安全日志和系统日志。eSight 提供提示、一般和危险三种级别的日志信息

安全日志

安全日志记录用户在 eSight 客户端上进行的影响 eSight 安全的操作，如登录服务器、修改密码、创建用户和退出服务器等。

可以通过查询安全日志了解涉及 eSight 安全操作的相关信息，及时发现潜在的安全隐患并进行处理。

系统日志

记录 eSight 发生的事件，如 eSight 运行异常、网络故障、eSight 受到攻击等，有利于分析 eSight 运行状态，排除故障。

可以通过查询系统日志了解涉及 eSight 系统操作的相关信息。

操作日志

记录用户触发的各种修改网管数据的操作，如新增监视图、修改资源管理器等。

可以通过查询操作日志了解涉及用户执行操作的相关信息。

4.1.3 资源管理

资源管理包括添加设备、子网以及设备和子网管理。

添加设备

- 自动发现设备：通过网元自动发现功能，可以根据指定的协议信息在指定 IP 网段中搜索网元，并把发现的网元增加到 eSight 中。

  eSight 支持 SNMP 协议、IPMI 协议、UC-SNMP、UC-TR069、UC-TCP、ICMP 协议、SMI-S 协议、TLV 协议以及 REST 协议。
- 添加单个设备：当需要添加到 eSight 的设备数量较少且已获取设备的 IP 和协议等信息时，可以通过添加设备的方式在 eSight 添加新设备。
- 批量导入设备：通过将设备的信息录入“.xls”文件，可以批量导入设备。避免在较多设备需要添加时，使用手工添加设备而降低工作效率。

设备/子网管理

设备/子网管理包括以下功能：

- 查询设备/子网

  支持设置查询条件查询所关注的设备/子网。
- 创建/修改/删除子网
  - 通过创建子网，可以根据用户的自定义逻辑将设备归类管理。
  - 当子网信息变更时，可以修改子网的属性。
  - 当网络结构调整，不再需要 eSight 管理某些子网，可以删除该子网。
- 查看子网信息

  支持查看子网的基本信息等。

- 查看设备信息

  支持查看设备的基本信息和协议信息等。
- 调整设备所属子网或者子网所属子网

  当网络结构发生变动时，可以根据实际情况，调整设备/子网，以便正确的体现设备、子网之间的关系。

分组管理

创建分组

通过将多个设备创建为一个分组，从而达到将不在同一个子网下的多个设备作为一个对象分配给用户管理，提升为用户批量分配设备的效率。

- 查看分组

  通过查看分组，可了解分组的详细信息。
- 修改分组

  编辑分组信息以满足最新的管理要求。
- 删除分组

  当不再需要使用分组时，可删除分组。

设备资源管理

- 提供用户对设备资源按网络业务进行分类查询浏览的功能，如网络设备、存储设备、统一通信、主机、eLTE 设备等。
- 提供用户对设备进行单个和批量业务操作的功能，如删除、配置协议参数、同步设备、移动到子网等。

4.1.4 告警管理

当网络运行异常时，网管系统需要及时通知维护人员，采取有效措施，恢复网络的正常运行。

告警管理包含以下功能：

- 告警管理提供全网告警监控、远程告警通知等方式第一时间通知维护人员，保证故障处理的实时有效性。
- 告警管理提供告警屏蔽、维护经验库等功能，提高告警处理的准确性和效率。
- 告警管理还提供告警同步功能，保证告警的可靠性。
- 告警管理还提供告警过滤、级别重定义等个性化定制功能，满足不同场景下的个性化需求。

告警级别

根据影响业务的严重性，告警级别分为紧急、重要、次要和提示，如表 4-1 所示。根据不同的告警级别可以采取对应的处理策略。

表4-1 告警级别

告警级别	说明
紧急	已经影响业务，需要立即采取纠正措施的告警。
重要	已经影响业务，如果不及时处理会产生较为严重后果的告警。
次要	目前对业务没有影响，但需要采取纠正措施，以防止产生严重故障的告警。
提示	检测到潜在的或即将发生的影响业务的故障，但是目前对业务还没有影响的告警。

告警状态

- 告警确认和告警清除
  - 告警确认：告警确认表示有用户已经对此告警进行了跟踪或处理。
  - 告警清除：当告警产生的条件消除，设备恢复正常，告警的状态将标识为清除。
- 告警状态分类

  根据告警是否被确认以及清除，告警可分为不同的状态。告警状态的分类如表 4-2 所示。

表4-2 告警状态分类

告警类别	告警状态
当前告警	未确认未清除
	已确认未清除
	未确认已清除
历史告警	已确认已清除

- 告警状态转换

  告警状态转换分类的说明如表 4-3 所示。

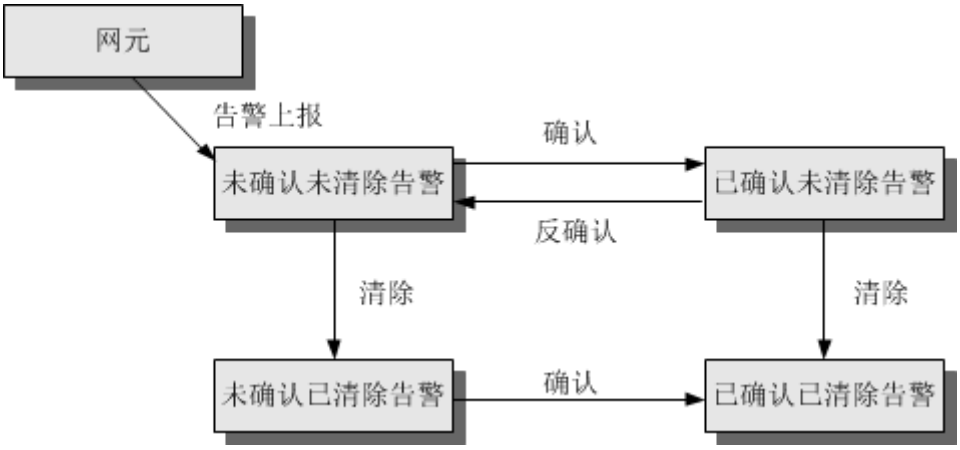
表4-3 告警状态转换分类

告警状态转换类别	说明
清除状态转换	当告警产生的条件消除，设备恢复正常，此时设备将上报对应的清除告警，告警由未清除状态变成清除状态。
确认状态转换	对告警进行确认表示告警即将或已经被处理。告警被确认

告警状态转换类别	说明
	后，由未确认状态变成已确认状态。 如果要重新关注已确认的告警，可以对该告警进行反确认操作。告警被反确认后，由已确认状态变成未确认状态。

告警状态转换关系模型如图 4-4 所示。

图4-4 告警状态转换关系模型



故障、告警和事件

- 故障和告警

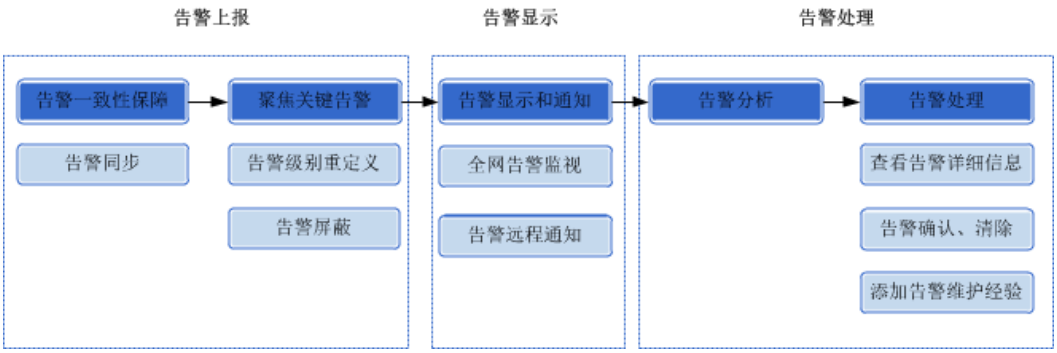
  告警是系统检测到故障而产生的通知。并不是系统中所有故障都会产生告警，只有系统能够检测到的故障才会产生告警，对于不能检测到的故障，不会产生告警，但是该故障依然存在。

- 告警和事件
  - 相同点：在 eSight 中，告警和事件都是指 eSight 检测到被管理的对象发生变化后产生的通知。
  - 不同点：告警是指 eSight 检测到故障而产生的通知。事件是指被管对象除故障外发生变化的统称。告警发生时，用户必须进行排障处理，否则会导致由于 eSight 或设备异常而引起业务的异常。事件的发生只是告诉用户被管对象发生了变化，不一定会引起业务的异常。

告警上报和处理流程

eSight 告警上报和处理流程如图 4-5 所示。以下各小节按照流程介绍 eSight 告警相关功能。

图4-5 告警上报和处理流程



告警同步

正常情况下，设备产生一条告警，在很短的时间内（一般不大于 10 秒）就会上报到 eSight 并且在其告警列表中显示出来。当 eSight 与网元通讯中断恢复后或者 eSight 重新启动后，网元侧的告警未及时上报到 eSight，造成 eSight 侧和网元侧的告警状态不一致，这时就需要执行同步告警操作，保证 eSight 侧真实地反映网元当前的运行状态。

告警同步规则如下：

- 如果网元侧某告警已清除，eSight 侧告警未清除，则清除 eSight 侧该告警。
- 如果网元侧有该告警，eSight 侧没有，则增加该告警。

告警级别重定义

eSight 提供对网元侧的告警进行级别重定义功能，用户可以根据实际需要重新设置某些告警的级别，提高或者降低告警的关注度。

告警屏蔽

- 通过设置屏蔽规则（属性包含日期、时段、告警源、具体告警）可以对某些不重要的告警进行屏蔽，使其不在当前告警列表中显示，避免大量的冗余信息。
- 网元在维修、测试或者开局期间，网元上报的告警会特别多，但此时不需要关心上报的告警，因此对处于这种状态的网元上报的告警信息要予以屏蔽，既不显示，也不保存。

全网告警监视

传统的分域维护，跨域的故障排除完全靠人工，定位效率低。eSight 提供丰富的全网告警监控功能，可以实时了解全网的运行状况。eSight 还提供模板化功能，根据需要将常用的查询条件设置为告警查询过滤模板，可以根据产生告警的设备所属的地域、设备类型、所属的网络层级等建立各种告警查询模板，方便日后查询和监控。

eSight 提供按级别和按设备两种维度的告警监控手段。

- 按级别监控告警，旨在帮助用户监控全网各级别告警的总体情况。具体请参见按级别监控告警。

- 按设备监控告警，旨在帮助用户从设备的维度，查看全网设备的告警情况。如某类或某台设备的所有当前告警（含各种级别）情况。具体请参见按设备监控告警。

按级别监控告警

按级别监控告警的途径有：告警板、告警声音和当前告警列表。告警板如图 4-6 所示。

图4-6 告警板

表4-4 按级别监控告警功能说明

功能	说明
告警板	按照级别显示被管理对象的当前告警总数，简要的提供系统的故障状况，可作为监视面板。
告警声音	支持为不同级别的告警指定告警提示声音。当告警发生时，主机上的音箱会发出对应的声音。
当前告警列表	浏览当前告警：支持设置过滤条件和搜索关键字查找在此前未处理（未确认或未清除）的故障告警。

浏览当前告警时，还提供了多项客户化功能，具体如图 4-7 和表 4-5 所示

图4-7 浏览当前告警

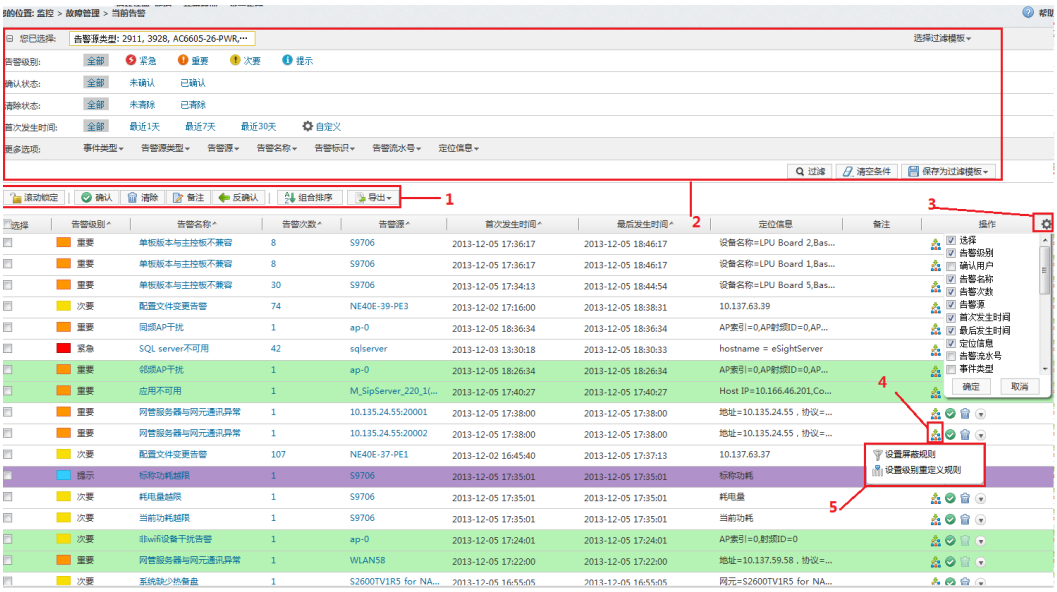


表4-5 当前告警浏览页面功能说明

编号	功能说明
1	全局操作按钮，对选中的多条告警生效。 • 滚动锁定/滚动解锁 滚动锁定状态下，新上报的告警不会更新到当前列表中。锁定状态下确认且清除的告警不会列入到历史告警列表，解锁后才会更新到历史列表中。 • 导出：将告警信息导出，方便其他用户定位故障和备份数据。 • 确认：标识该告警已有用户处理，其他用户不需要关注。 • 清除 手工清除告警：当告警无法自动清除或已确认网元上不存在该告警的时候，可以单击按钮进行手工清除。 • 备注：供用户备注一些自己想记录的注意事项等信息，如告警处理进度及状态。
2	选择或设置过滤条件，浏览当前告警。 eSight 默认提供了 6 个过滤条件，从选择过滤模板下拉框中查看： • 所有告警 • 未确认的紧急告警 • 未确认的严重告警 • 未清除的紧急告警 • 未清除的严重告警 • 最近一天的告警 也可以在“选择”区域选择过滤条件，设置自己需要的过滤条件。
3	定制告警列表显示列。
4	将告警定位到拓扑视图中产生告警的对象。
5	其他针对该告警的操作，如告警屏蔽规则、告警级别重定义等。

按设备监控告警

按设备监控告警，旨在帮助用户从设备的维度，查看全网设备的告警情况。如某类或某台设备的所有当前告警（含各种级别）情况。当设备上存在故障时，拓扑视图中设备图标将被渲染成告警级别对应的颜色。

告警远程通知

通过设置告警/事件远程通知规则，在产生符合通知规则的告警/事件时，eSight 通过短消息、邮件方式将告警/事件信息发送给指定人员，便于不在现场的维护人员及时了解到设备告警情况从而采取相应措施。

远程通知支持自定义通知内容模板和通知用户组。

告警分析

通过查询并分析历史告警、事件和被屏蔽告警可以了解设备的告警情况，以便对设备的性能进行优化。eSight 能按照用户所设的统计条件对告警信息进行统计。统计条件包括子网或网元、告警/事件名称、首次发生时间、告警级别，也可以是以上各项的组合。

告警处理

- 查看告警详情

  在 eSight 系统中通过单击告警列表中的某条告警，可以查看当前告警详情、历史告警详情和被屏蔽告警详情。查看告警详情可以获取告警名称、修复建议和定位信息等告警信息。
- 告警确认、清除：方法参见图 4-7。
- 添加维护经验

  在“告警详情”对话框中用户还可以添加维护经验，供以后处理同一种告警时参考。

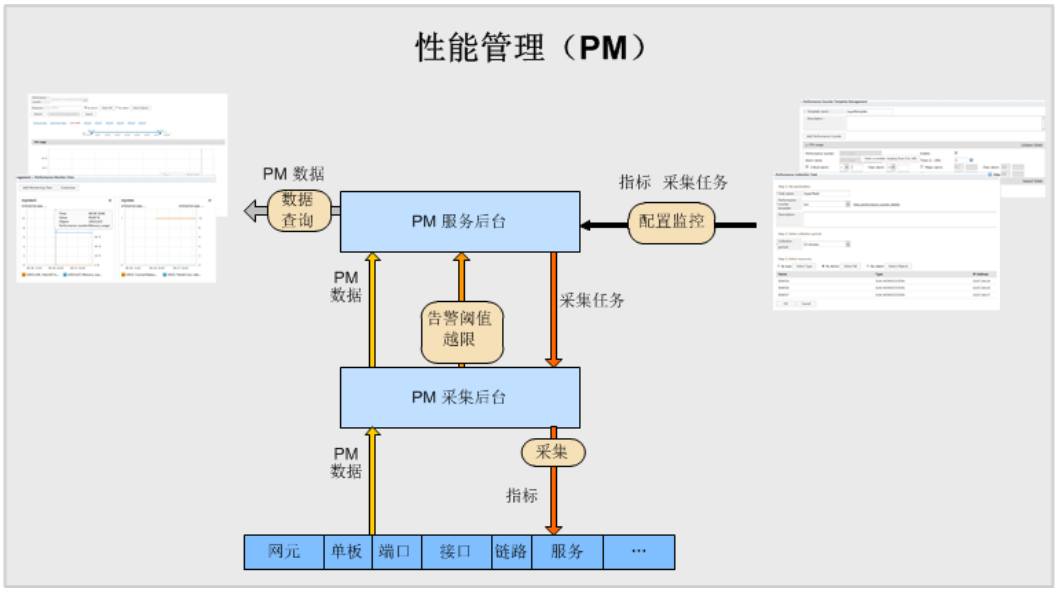
4.1.5 性能管理

网络在正常运行过程中，内部与外部的原因可能会影响网络性能的下降，引发网络故障。为保证当前网络在低成本下的性能足够，并为网络性能未来需求作准备，需要规划、监控与衡量网络效率，如通断率、利用率等。通过性能管理可以提前发现这种劣化的趋势，并在故障发生前解决掉这些隐患，规避网络故障风险。

工作过程

eSight 通过可视化的操作界面对网络的关键性能指标进行监控，并对采集到的性能数据进行统计，方便用户对网络性能进行管理。如图 4-8 所示。

图4-8 统一性能处理过程



eSight 性能管理提供了指标模板管理、采集任务管理、历史性能查询、实时性能查询、性能指标采集状态监控等功能。如下是对性能管理各模块功能的大体介绍。

指标模板管理

同一类型的设备具有相同的指标属性，将这些指标设置为一个指标模板，创建性能采集任务时直接加载，可以快速设置指定设备的采集指标。

eSight 指标模板管理支持：

- 增、改、删指标模板。
- 在指标模板中设置指标，即收集网络资源的哪些性能数据
- 在指标模板中设置性能指标的阈值。如果指标连续多次满足阈值条件，网管会产生告警。用户通过告警，可以监控指定资源的性能。

  阈值包括上限触发值、下限触发值、上限清除值、下限清除值。相应的阈值告警分为上限阈值告警和下限阈值告警。指标、阈值、告警的关系如表 4-6 所示。

表4-6 性能指标阈值告警

指标与阈值的关系	阈值告警
下限触发值<=or <性能指标<or<=上限清除值	下限阈值告警
下限清除值<=or <性能指标<or<=上限触发值	上限阈值告警

采集任务管理

eSight 以任务形式统一管理性能数据采集。采集任务定义了对哪些设备的哪些指标进行采集。设备的指标被采集后，就能查看到该设备的此项历史性能数据。

eSight 默认提供以下全局采集任务，采集全网所有设备的对应性能指标。

- CPU 使用率采集任务
- 丢包率采集任务
- 端口占用率采集任务
- 内存使用率采集任务
- 设备通断采集任务
- 响应时间采集任务

全局采集任务支持如下的用户定制功能：

- 启动、停止采集任务
- 修改采集周期
- 查看各设备的指标采集状态是否正常

eSight 采集任务管理还包括以下功能：

- 支持增、删、启、停、修改性能采集任务。
- 支持查看性能指标的采集状态。

性能指标采集状态监控

创建性能采集任务后，定期监控设备性能指标的采集状态，可以及时发现并解决采集异常问题，确保性能采集任务能采集到性能数据供用户查看和分析。

eSight 支持按资源类型、采集任务两个维度查看设备的性能指标采集状态。

通过显示的性能指标数据，可以直接跳转到历史性能页面，查看该指标的历史数据曲线。

查看历史性能数据

eSight 通过性能采集任务采集设备性能数据后，用户可以通 eSight 客户端指定指标、资源来查看历史性能数据，以了解设备历史性能趋势并预防故障发生。

eSight 提供数据曲线图展示历史性能数据。

- 指定采集对象查看历史性能数据
  - 支持设置指标、资源、时间周期查询历史性能数据。其中资源的设置支持按设备和按对象两种方式。两种方式的说明如表 4-7 所示。

表4-7 资源选择方式

资源选择方式	说明
按设备	直接选择设备，选择后设备上所有同类对象的数据均可以查看

资源选择方式	说明
	到。例如指标选择了 CPU 占用率后，使用“按设备”方式选中一台多 CPU 的设备后，则历史性能数据曲线图中将显示该设备上所有 CPU 的历史 CPU 占用率。
按对象	选择设备中的对象。如多 CPU 设备上的某一个或多个 CPU。

  - 支持导出查询结果到“.csv”文件。
  - 支持将查询另存为首页视图，在首页中监控历史性能。

    由于二维曲线图最多能显示两个纵轴，因此 eSight 每张性能数据曲线图中最多只能显示 2 种数据单位。另，自定义采集对象查看历史性能时，每张性能数据曲线图最多只能显示 6 条性能数据线。因此，当所选指标的数据单位超过 2 种，或者性能数据线超过 6 条时，eSight 将分图显示历史性能数据。

    将查询另存为首页视图功能仅在查询结果为一张曲线图时可用。当查询结果为多张曲线图时，若要使用此功能，请分解查询为多次。

- 通过性能监控视图查看历史性能数据

  eSight 支持用户将设备关键性能指标增加为监控视图，方便用户在“性能监控视图”页面中直接监控设备性能状态。同时，增加的监控视图还支持显示在首页中。

查看实时性能数据

通过监控设备实时性能，可以了解设备的当前运行状态，以便确认设备当前是否异常并及时采取措施。例如，当有阈值告警（如 CPU 占用率高）上报后，通过查看实时性能，可以确认设备当前是否存在对应问题。

eSight 提供数据曲线图实时查看性能数据。

- 支持设置查询条件查看实时性能数据。
- 支持导出查询结果到“.csv”文件。

4.1.6 物理拓扑管理

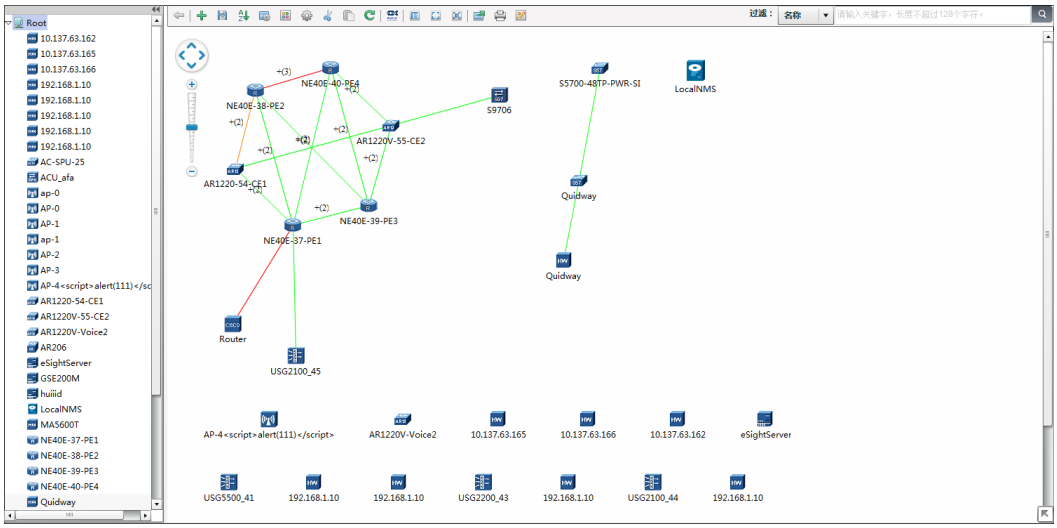
拓扑管理用于构造并管理整个网络的拓扑结构，以反映设备的组网情况和运行状态。通过物理视图中网元图标所显示的颜色及状态，可以实时监控整个网络的运行情况。

表4-8 拓扑管理基本概念

术语	说明
网元	拓扑管理的核心单位，用来标识被管理的设备。在拓扑视图中，不同的图标代表各种网元类型。
子网	按照某种原则（如按地域或按设备类型划分）将一个比较大的网络结构分解为几个相对较小的网络结构，以便网络管理。

术语	说明
链路	标识通信设备之间的物理或者逻辑连接。

图4-9 拓扑管理界面示意图



管理拓扑对象

拓扑对象包含子网、物理网元、虚拟网元、链路和下级资源。

- 创建/删除虚拟网元

  虚拟网元是指整个网络中不能通过 eSight 进行管理的网元的映射。

  - 通过将虚拟网元增加到物理视图中，可以更清楚地了解整个网络情况。
  - 当网络结构调整，不再需要管理某些虚拟网元，可以将其从物理视图中删除。
- 创建/删除虚拟链路

  虚拟链路不是网络中实际存在的链路，用于表示拓扑对象之间的逻辑连接。

  - 通过创建虚拟链路，可以更清楚地了解拓扑对象之间的关系。
  - 当网络结构调整，不再需要管理某些虚拟链路，可以将其从物理视图中删除。
- 删除子网

  当网络结构调整，不再需要 eSight 管理某些子网，可以删除该子网。

调整物理视图

调整物理视图包括以下功能：

- 调整网元/子网位置

  当网络结构发生变动时，可以调整网元/子网在物理视图中的位置，以便正确地体现它与其他拓扑对象的关系。调整网元/子网位置包括：

  - 调整网元/子网所在物理视图中的物理位置
  - 调整子网所属子网
  - 调整网元所属子网
- 设置拓扑背景图

  根据拓扑对象的布局设置合适的背景图，可以直观地了解拓扑对象所在的位置。
- 布局拓扑对象

  提供以下布局方式：
  - 环形：将拓扑对象排列成环形。
  - 星形：将拓扑对象排列成星形。
  - 对称：将拓扑对象排列成对称。
  - 上下树形：将拓扑对象排列成上下树形。

浏览物理视图

- 查找拓扑对象

  支持设置搜索条件快速定位到所关注的网元、链路、子网等拓扑对象。
- 缩放物理视图

  物理视图可以根据需要，放大、缩小、还原显示、适合屏幕显示或全屏显示。
- 全屏/鸟瞰查看物理视图

  支持通过全屏/鸟瞰图查看物理视图，浏览物理视图的全貌，并定位拓扑窗口所显示的区域。
- 打印、导出、保存物理视图
- 设置设备标签

  支持设置设备图标下显示的信息（如设备的名称、IP 地址和系统名称），以便直观的了解设备基本信息。

通过物理拓扑视图监控网络运行状态

- 监控网络设备的告警状态。
- 支持通过对于设备图标颜色的渲染展示设备当前的运行状态。当设备上存在故障时，设备图标将被渲染成告警级别对应的颜色。
- 监控设备的离在线状态。
- 支持通过对于设备图标颜色的渲染展示设备当前的离在线状态。当设备处于离线状态时，设备图标将被渲染成灰色。
- 监控子网下属设备集的告警状态。
- 支持通过对于子网图标颜色的渲染展示子网下属设备集的运行状态。当子网下属设备中存在处于故障状态的设备时，子网图标的颜色将被渲染成下属设备集中存在的最高级别的告警的颜色。
- 监控子网下属设备集的离在线状态。
- 支持通过对于子网图标颜色的渲染展示子网下属设备集的离在线状态。当子网下属设备中存在处于离线状态的设备时，子网图标的颜色将被渲染成灰色。

- 监控链路的性能状态。物理拓扑中提供了链路两端标签的显示能力，通过二次开发，产品能够在其中扩展显示链路的性能状况，例如，链路两端的出口流量、入口流量等。同时，物理拓扑中亦提供了链路颜色、粗细的渲染能力。通过二次开发，产品能够通过为链路进行颜色、粗细的渲染体现链路限制带宽、带宽的利用率等。

4.1.7 维护工具

通过维护工具可以管理 eSight 服务器，包括服务器的数据库和进程信息。可以了解 eSight 服务器当前运行状况，以便及早发现并解决异常，保障 eSight 服务器高效运行。

系统监控

- 查看维护工具管理的所有产品状态。
- 查看产品的分布式部署情况。
- 提供按照产品启动停止。
- 提供按照进程启动停止。

管理服务器

- 查看 eSight 服务器基本信息。
- 查看 eSight 服务器进程信息。
- 监控 eSight 服务器资源使用率。

  维护工具支持对 eSight 服务器的 CPU、内存、磁盘、数据库的使用率进行监控，并在使用率达到一定门限值时，上报告警到 eSight。

管理数据库

- 数据库监控

  通过监控 eSight 服务器数据库状态查看数据库名、服务器名和数据库状态等信息。
- 修改数据库密码

  通过维护工具可周期性修改数据库用户密码，以确保数据库用户密码的安全性。
  - 修改数据库管理员密码

  说明
  不同的数据库的管理员的名称不同，MySQL 数据库的管理员为“root”，SQL Server 数据库的管理员为“sa”，Oracle 数据库的管理员为“system”，GuassDB 数据库的管理员为“gussdba”。
  - 修改数据库网管用户“commonuser”的密码

管理高可用性系统

- 连接主备服务器

  高可用性系统安装完成后，可以通过维护工具连接主、备服务器，组成高可用性系统。
- 强制为主服务器

在高可用性系统处于双主待修复状态时，可以通过维护工具进行强制为主服务器的操作，将其中一台服务器强制为主服务器，保证高可用性系统能够正常使用。

- 分离主备服务器

  当卸载 eSight 或不需要组成高可用性系统时，需要通过维护工具分离主、备服务器。

备份恢复

提供备份策略定制、手工备份和手工恢复的功能，备份内容包括系统运行时的配置文件和数据库数据。

维护工具管理

- 修改维护工具用户密码

  周期性地修改维护工具用户 sys 的密码，可提高用户信息的安全性。

- 查询维护工具操作日志

  记录用户 sys 在维护工具客户端上的操作信息，如启停 eSight、修改用户密码等。

说明

维护工具最多记录 2 万条操作日志。当超过 2 万条记录时，维护工具将自动删除最早的 1000 条记录。

4.1.8 分级网管管理

eSight 支持用户建立分级分层的网络管理方案。在上级网管统一维护下级网管列表，通过链接可以直接打开下级网管的界面。从而实现查看下级网管告警、拓扑、性能和报表等功能。

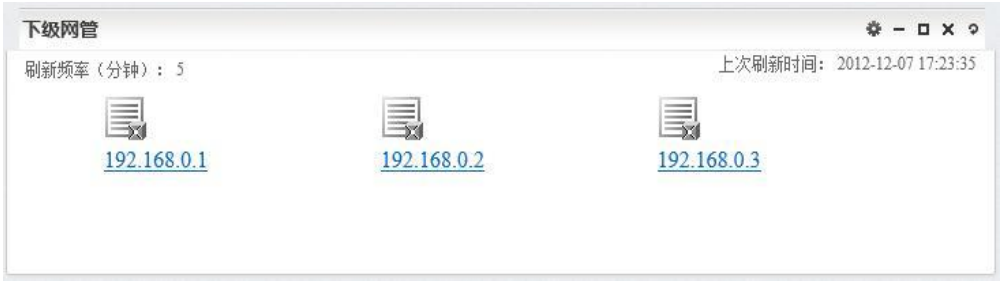
分级网管提供如下管理下级网管的方式：

- 通过分级网管管理界面，完成下级网管的增加、删除、修改和手工连通性检测功能

图4-10 分级网管管理界面

- 通过下级网管 Portal 首页，可以实时监控各下级网管的连通性，并且可以单击各下级网管的链接，直接打开下级网管的界面

图4-11 下级网管 Portal 首页



4.1.9 License 管理

License 是 eSight 管理容量、客户端接入数和使用时间等方面的许可。License 管理包括查询 License 信息、获取 ESN、设置 License 失效和导入 License 等。

License 管理所包含的主要功能有：

查询 License 信息

通过 eSight 客户端可以方便地查询 eSight 的 License 授权和消耗情况。

获取 ESN

通过 eSight 客户端获取 ESN，在申请新 License 时，需要提供 ESN。

设置当前 License 失效

当 ESN 变更或者网络调整时，可以设置当前 License 失效，并可以使用生成的失效码申请新的 License 文件。

说明
只有具备“失效 License”操作权限的用户才能设备当前 License 失效。
试用 License 不支持设置当前 License 失效。

导入 License

通过 eSight 客户端可以方便地将新申请的 License 更新应用到 eSight 服务器上。

说明
只有具备“更新 License”操作权限的用户才能导入 License 文件。

发送 License 告警

在 License 状态异常的情况下，会提示用户 License 的状态并且发送 License 告警，避免 License 过期等原因对业务产生的影响。

4.1.10 首页视图展示

eSight 通过首页上的 Portlet 视图展示设备关键数据，方便监控设备状态，及时发现设备的异常状态并处理，保证设备的正常运行。

首页管理

- 创建首页

  eSight 缺省只提供一个首页。支持创建多个首页，将需要关注的 Portlet 视图分类显示在不同首页中。
- 修改首页名称

  可以修改首页名称来重新标识该首页。
- 置顶首页

  可以将重点关注的首页移动到前面。
- 删除首页

  支持删除冗余的首页。

Portlet 管理

Portlet 是指以列表、曲线图、柱状图等方式展现设备状态、全网状态等的视图，即显示在首页中各小区域。

- 创建自定义 Portlet

  将非 eSight 的第三方界面集成在 eSight 首页中进行监控。
- 定制显示/隐藏 Portlet

  将需要关注的 Portlet 显示在首页中，将不需要关注的 Portlet 从首页中隐藏。
- 手动刷新或设置定时刷新 Portlet 中的数据

  适时更新监控数据。
- 放大/缩小 Portlet

  支持 Portlet 放大/缩小，适应不同的查看需求。

eSight 支持的 Portlet 如表 4-9 所示。

表4-9 eSight Portlet

类型	Portlet	功能
基础管理	网络设备终端在线趋势	展示最近一段时间内，在线终端数的变化趋势。
	存储设备状态	显示存储设备的当前状态。
	FC 交换机端口连接状态	显示 FC 交换机的端口连接状态。
	eLTE 设备统计	显示 eLTE 终端设备的在/离线统计数
	下级网管	显示部分下级网管及其状态。

类型	Portlet	功能
监控	当前告警	显示当前告警中各级别的告警数量。
	TopN 网元告警统计	显示网元或设备当前告警中的统计数。
	TopN 平均接口流入带宽利用率	显示近 1 小时、近 24 小时、近 7 天流入带宽利用率 TopN 的接口。
	TopN 平均接口流出带宽利用率	显示近 1 小时、近 24 小时、近 7 天流出带宽利用率 TopN 的接口。
	TopN 平均 CPU 利用率	显示最近 1 小时内 CPU 利用率最高的 10 个在线设备。
	CPU 趋势图	显示用户所选择设备的最近 24 小时内 CPU 利用率。
	TopN 平均内存利用率	显示最近 1 小时内存利用率最高的 10 个在线设备。
WLAN	WLAN 全网在线用户统计	显示全网无线用户在线趋势。
	TopN AP 上行端口流量与信道利用率	显示 TopN AP 上行口流量与射频信道使用情况。
	TopN WLAN 平均 CPU 利用率	显示 TopN AC 或 AP 近 1 小时、近 24 小时、近 7 天平均 CPU 使用情况。
	非法设备与非法客户端统计	显示全网无线非法设备与非法客户端统计情况。
	干扰源统计	显示全网干扰源统计情况。
	TopN WLAN 平均内存利用率	显示 TopN AC 或 AP 近 1 小时、近 24 小时、近 7 天平均内存使用情况。
	客户端射频类型用户统计	显示客户端接入射频类型用户统计情况。
	TopN WLAN 最新告警	显示 TopN WLAN 最新告警。
	TopN 区域统计	显示 TopN 区域中，AP 及用户在线情况。
	TopN SSID 用户统计	显示 TopN 接入 SSID 用户数分布情况。
	TopN AP 用户关联失败率	显示 TopN AP 关联用户的失败率。
	WLAN 信道利用率	显示信道利用率趋势。
	全网无线资源统计	显示全网 AC、AP 资源及状态。

类型	Portlet	功能
数据中心 nCenter	TopN 物理服务器 CPU 利用率	展示虚拟网络管理的 TopN 物理服务器 CPU 利用率情况。
	TopN 物理服务器内存利用率	展示虚拟网络管理的 TopN 物理服务器内存利用率情况。
	TopN 虚拟机 CPU 利用率	展示虚拟网络管理的 TopN 虚拟机器 CPU 利用率情况。
	TopN 虚拟机内存利用率	展示虚拟网络管理的 TopN 虚拟机内存利用率情况。
MPLS VPN	BGP/MPLS VPN 状态统计	显示当前 BGP/MPLS VPN 业务运行状态。
	BGP/MPLS VPN 告警统计	显示当前 BGP/MPLS VPN 业务告警状态。
SLA	TopN SLA 最低符合度	显示最近一段时间 SLA 符合度最低的 N 项任务信息。
	TopN SLA LSP PING 指标	显示最近一段时间 SLA LSP PING 指标的 N 项任务信息。
	TopN SLA DNS 指标	显示最近一段时间 SLA DNS 指标的 N 项任务信息。
	TopN SLA TCP 指标	显示最近一段时间 SLA TCP 指标的 N 项任务信息。
	TopN SLA UDP 指标	显示最近一段时间 SLA UDP 指标的 N 项任务信息。
	TopN SLA UDP JITTER 指标	显示最近一段时间 SLA UDP JITTER 指标的 N 项任务信息。
	TopN SLA SNMP 指标	显示最近一段时间 SLA SNMP 指标的 N 项任务信息。
	最近智能策略任务	最近智能策略任务。
	TopN SLA DHCP 指标	显示最近一段时间 SLA DHCP 指标的 N 项任务信息。
	TopN SLA HTTP 指标	显示最近一段时间 SLA HTTP 指标的 N 项任务信息。
	TopN SLA ICMP JITTER 指标	显示最近一段时间 SLA ICMP JITTER 指标的 N 项任务信息。
	TopN SLA LSP JITTER 指标	显示最近一段时间 SLA LSP JITTER 指标的 N 项任务信息。

类型	Portlet	功能
	TopN SLA ICMP 指标	显示最近一段时间 SLA ICMP 指标的 N 项任务信息。
	TopN SLA FTP 指标	显示最近一段时间 SLA FTP 指标的 N 项任。
QoS	TopN 平均丢弃速率	显示最近一段时间 QoS 性能指标最高的 N 项任务信息。
	TopN 平均尾部丢包数	显示最近一段时间 QoS 性能指标最高的 N 项任务信息。
	TopN 平均超出承诺带宽速率	显示最近一段时间 QoS 性能指标最高的 N 项任务信息。
	TopN 平均随机丢包数	显示最近一段时间 QoS 性能指标最高的 N 项任务信息。
	TopN 平均匹配速率	显示最近一段时间 QoS 性能指标最高的 N 项任务信息。
	TopN 平均流分类带宽利用率	显示最近一段时间 QoS 性能指标最高的 N 项任务信息。
	TopN 平均通过速率	显示最近一段时间 QoS 性能指标最高的 N 项任务信息。
网络流量管理	TopN DSCP 流量	显示 DSCP 流量的排行。
	TopN DSCP 组流量	显示 DSCP 组流量的排行。
	TopN 设备流量	显示设备流量的排行。
	TopN IP 组流量	显示 IP 组流量的排行。
	TopN 主机流量	显示主机流量的排行。
	TopN 会话流量	显示会话流量的排行。
	TopN 接口流量	显示接口流量的排行。
	TopN 接口组流量	显示接口组流量的排行。
	TopN 应用流量	显示应用流量的排行。
	TopN 应用组流量	显示应用组流量的排行。
	TopN 接口利用率	显示接口利用率的排行。
	TopN 接口组利用率	显示接口组利用率的排行。

4.1.11 数据库数据溢出转储

为了避免数据库表空间不足而影响业务运行，eSight 提供了数据溢出自动转储功能。系统对于存在大数据量的模块每日定时检测数据库容量，在超出时系统自动将数据转储到指定的路径下。

数据溢出转储包括日志数据库溢出转储、告警数据库溢出转储、性能数据库溢出转储、SLA 数据溢出转储、数据中心 nCenter 数据溢出转储、终端接入数据溢出转储、配置文件管理数据库溢出转储、网络流量数据库溢出转储。

4.1.12 高可用性系统管理

eSight 高可用系统提供双机热备和倒换的全新功能。主、备服务器的软硬件配置要求完全一致，通过 Veritas 远程热备份技术，实现主、备服务器数据实时同步，并动态监视 eSight 的运行状态。当主服务器发生硬件故障、操作系统故障、网管关键应用故障时，系统会自动倒换到备份服务器，倒换时间不超过 15 分钟。

高可用系统部署

高可用系统部署包括磁盘的 RAID 划分、Linux 操作系统、Veritas 软件、Oracle 数据库以及 eSight 软件的安装。为了降低安装难度，提高安装效率，Linux 操作系统定制成一键式安装，Veritas 和 Oracle 集成安装。

高可用系统主备关联

主备关联功能用于将完成安装部署的两台机器建立主备关联关系。

图4-12 建立主备关联

高可用系统主备断连

主备断连功能用于将两台已经建立了主备关联关系的机器拆分。

图4-13 主备断连

4.2 设备管理

4.2.1 网络设备管理

网络设备管理提供网络设备的基本管理和配置功能，包括网络设备的发现和维护、路由配置、接口管理、二层链路管理、IP 拓扑、设备配件等。

4.2.1.1 网络设备管理

网元管理

提供网络设备的基本管理功能，将单个网元的相关信息和维护操作入口集中在一个管理页面中，便于用户针对单个网元的监控和维护。

图4-14 网元管理器

- 查看
  - 基本信息：显示网元的概览信息，包括基本信息、性能 KPI、TOPN 告警和接口流量。
  - 设备面板：以图形化方式显示该网元。
  - 告警列表：显示当前网元的当前告警。
  - 性能状态：显示当前网元的性能指标数据。
- 配置
  - WEB 网管：打开该网元内嵌的 WEB 管理界面。
  - 业务配置：打开智能配置工具对该网元进行配置。
  - 接口管理：查看当前网元的接口列表，可以对接口进行启用、禁用、告警屏蔽、告警去屏蔽。
  - IP 地址管理：查看当前网元的 IP 地址列表。
  - 配置文件：查看、备份当前网元的配置文件。
- 协议参数
  - Telnet 参数设置：修改网元的 Telnet/STelnet 参数。
  - SNMP 参数设置：修改网元的 SNMP 参数。
  - NetConf 参数设置：修改网元的 NetConf 参数(部分设备支持)。

轮询参数设置

图4-15 轮询参数设置

提供轮询参数设置界面，可以设置定时同步时间、接口状态轮询、IP 地址轮询、设备状态轮询的时间间隔。

- 设备定时同步：设备定时同步会同步设备上接口、实体、IP 地址等特性数据（不同设备可能存在差异），定时同步属于比较耗费系统资源的操作，一般将设备定时同步放在系统闲时执行。

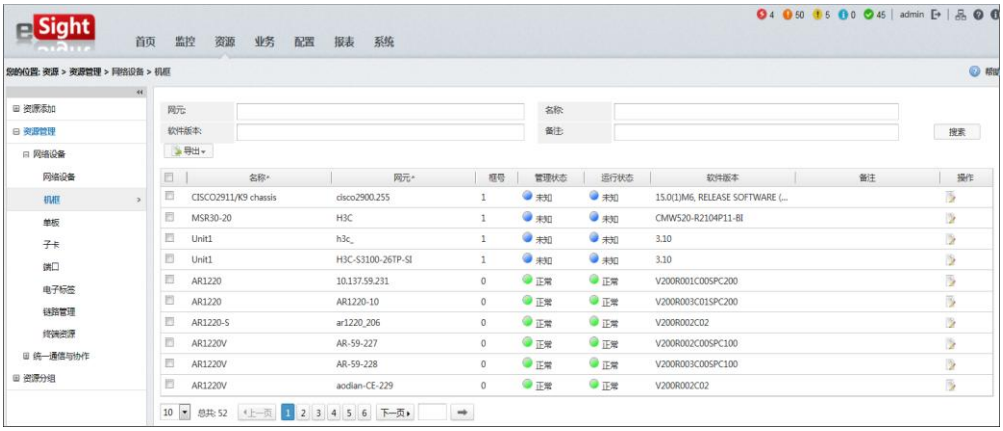
- 接口状态轮询：轮询设备接口状态，不依赖设备 Trap 上报能产生“link up/down”告警，拓扑管理、IP 拓扑管理界面上对应的设备和链路状态根据告警刷新。
- IP 地址轮询：轮询设备接口 IP，主动感知设备接口 IP 地址变更，并刷新 IP 拓扑管理界面上对应设备，生成 IP 地址变更标记。
- 设备状态轮询：通过 ICMP Ping 轮询设备在线、离线状态，主动感知设备状态变更，如设备离线系统会产生”网管服务器与网元通讯异常“告警，并刷新拓扑管理和 IP 拓扑管理界面对应设备。

物理资源管理

- 机框管理

  提供用户对设备机框资源的查询、导出功能，及对机框备注进行修改功能。

  图4-16 机框资源



- 单板资源

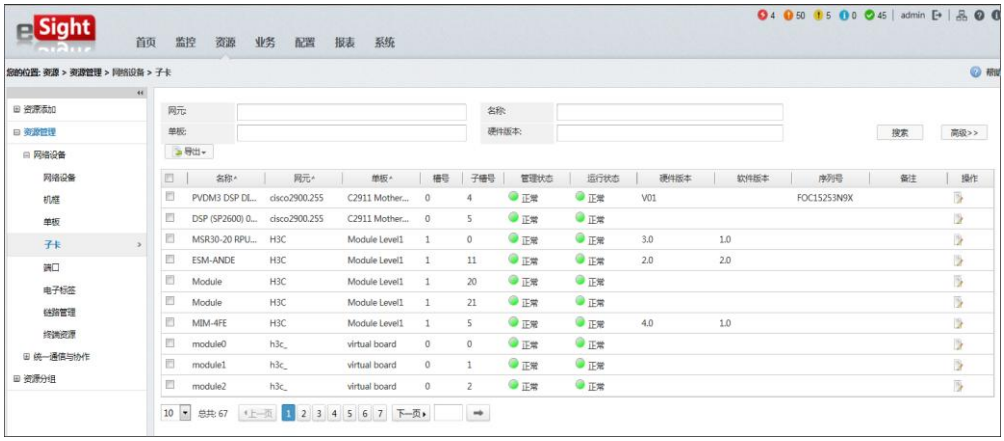
  提供用户对设备单板资源的查询、导出功能，及对单板备注进行修改的功能。

  图4-17 单板资源

- 子卡资源

提供用户对设备子卡资源的查询、导出功能，及对子卡备注进行修改的功能。如图 4-10 所示。

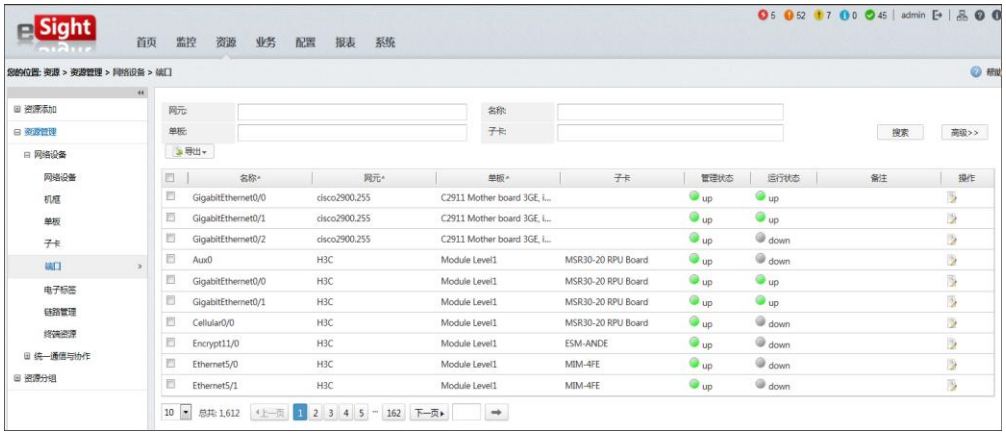
图4-18 子卡资源



- 端口资源

  提供用户对设备端口资源的查询、导出功能，及对端口备注进行修改的功能。如图 4-11 所示。

图4-19 端口资源



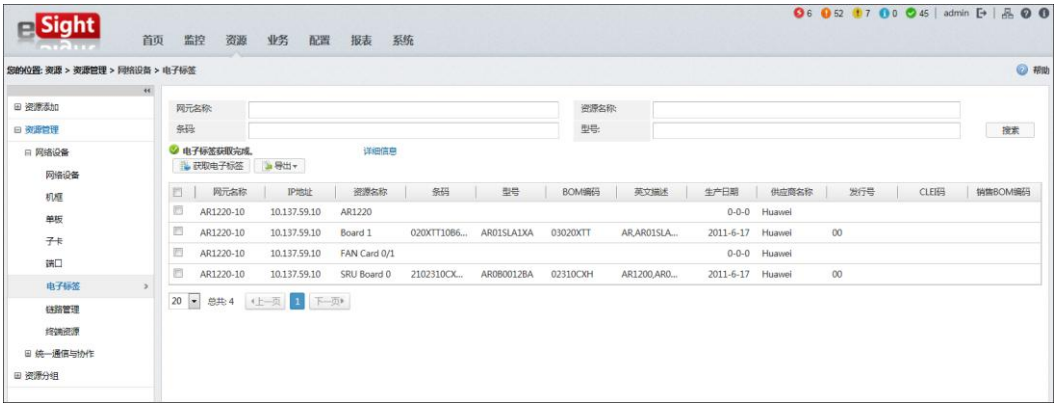
电子标签

支持设备的电子标签查询和导出。

说明

电子标签是以电子数据形式存储的用于标识设备的标签，可以应用于客户的网络设计、规划和维护、资产管理（含备件管理）、订单、帐务管理、清算、投资跟踪、保修等业务活动中。

图4-20 电子标签

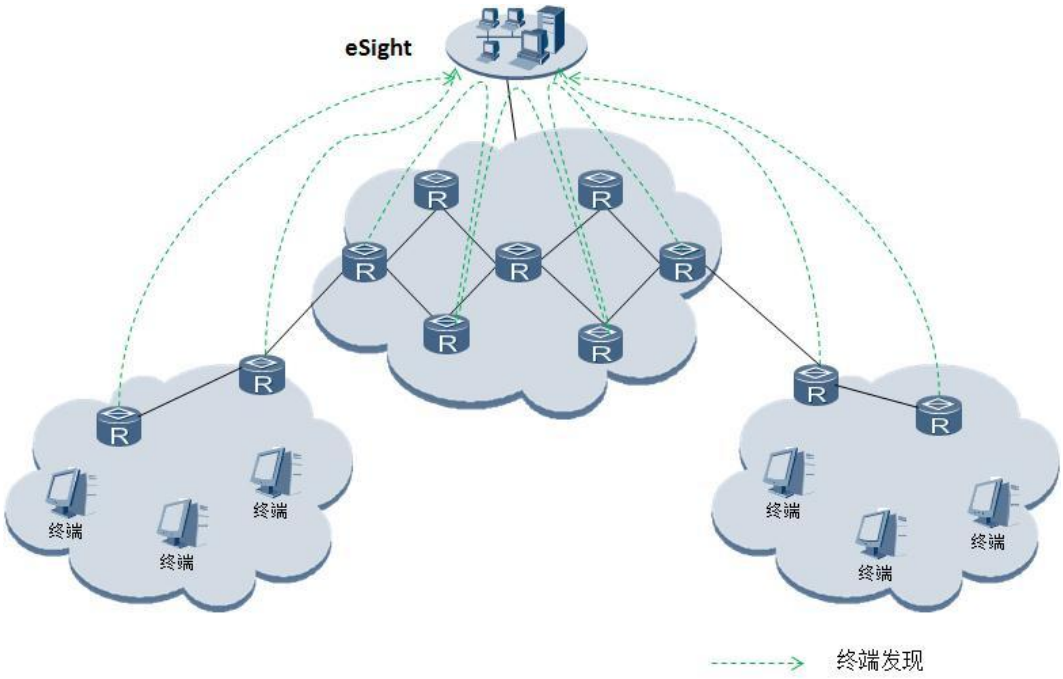


4.2.1.2 网络终端资源

终端接入管理提供对网络中接入终端的统一管控手段。通过浏览终端接入历史、可疑终端日志、非法接入管理、远程通知等手段，便于网络管理员及时掌握终端的接入情况。

终端资源作为终端接入管理的基础，用户可通过两种方式进行终端资源的发现：用户手工触发的立即发现、系统周期执行的自动发现。

图4-21 终端接入解决方案



终端发现配置

- 支持设定是否解析终端名称

- 支持设定是否启用终端自动发现
- 支持设定终端自动发现的周期
- 支持设定需要发现接入终端的设备范围，该范围同时适用于立即发现和自动发现

白名单

用户将合法的 IP 地址和 MAC 地址在白名单中进行配置后，网管就会在发现终端的过程中，依据配置生效后的白名单，检测接入终端是否合法，并记录所有非法接入终端的详细信息，为用户审计非法接入情况提供依据。

接入绑定规则

用户可以配置 PORT-IP 或 PORT-MAC 规则以限制设备端口下准许接入的终端，可以配置 IP-MAC 规则以限制 IP 地址与 MAC 地址的对应关系，网管会将违反这些规则的终端识别为非法终端，并记录下详细的接入信息。

终端接入记录

- 查看终端接入详细信息和接入历史
- 查看终端的非法接入日志
- 跳转至物理拓扑中定位终端的接入设备
- 接入接口跳转到接口管理
- 跳转至设备面板中查看终端的接入端口
- 配置终端的备注信息

可疑终端日志

- 查看端口多 MAC 地址，识别端口下私接设备
- 查看重复 MAC 地址，识别 MAC 地址盗用
- 查看重复 IP 地址，识别 IP 地址盗用

非法接入管理

网管根据用户设定的 IP/MAC 地址白名单，自动识别出所有非法的接入终端。

- 查看非法接入终端的详细信息和非法日志
- 导出非法接入终端的详细信息
- 确认非法终端的处理状态

远程通知

用户通过配置远程通知，在系统发现非法接入终端的时候，发送邮件通知，帮助用户及时掌握非法接入情况。

4.2.1.3 链路管理

链路是指连接各个信令点、信令转接点，传送信令消息的通道。一条通信路径，有多段链路组成。通过链路管理，可以及时查看链路的状态，便于对网络链路进行维护。

同时链路在拓扑视图上进行展现，用户可以根据网管链路拓扑了解现网中的网络拓扑结构的变化。

用户可通过两种方式进行链路的发现：用户手工触发的手工发现、添加完设备之后触发的自动链路发现。

链路发现

当前 eSight 主要支持 LLDP，CDP，MAC，Side-By-Side 四种发现算法，其中 LLDP，CDP，Side-By-Side 这个三种算法支持自动发现和手动发现；MAC 当前只支持手动发现。

发现算法约束：

- LLDP 链路约束：LLDP 协议是公有协议，发现时需要链路两端设备都支持 LLDP 协议，并且设备使能 LLDP 功能，同时设备上配置 iso 视图。
- CDP 链路约束：CDP 协议是 Cisco 私有协议，发现需要链路两端设备都是 Cisco 设备，并且设备使能 CDP 功能。
- MAC 链路约束：当设备未使能 LLDP、CDP 功能时，同样可通过 MAC 转发表发现链路。MAC 链路发现基于设备 MAC 转发表（公有 MIB，不涉及设备差异）数据做链路发现，第三方设备间链路同样可以发现。MAC 发现的约束主要在于组网约束，要求链路至少一端端口为二层口。
- IP 链路约束：IP 链路发现要求链路两端 IP 地址为 30 位掩码 IP 地址。

链路发现的协议用户不感知后台链路发现算法的优先级，优先级顺序是 LLDP 发现，CDP 链路发现，MAC 链路发现（针对二层链路而言）。

显示规则

用户可以在“显示规则”的弹出窗口中，选择新的链路名称规则和 Tips 规则所需的字段，其中 Tips 在拓扑中的链路上展示。

图4-22 显示规则设置

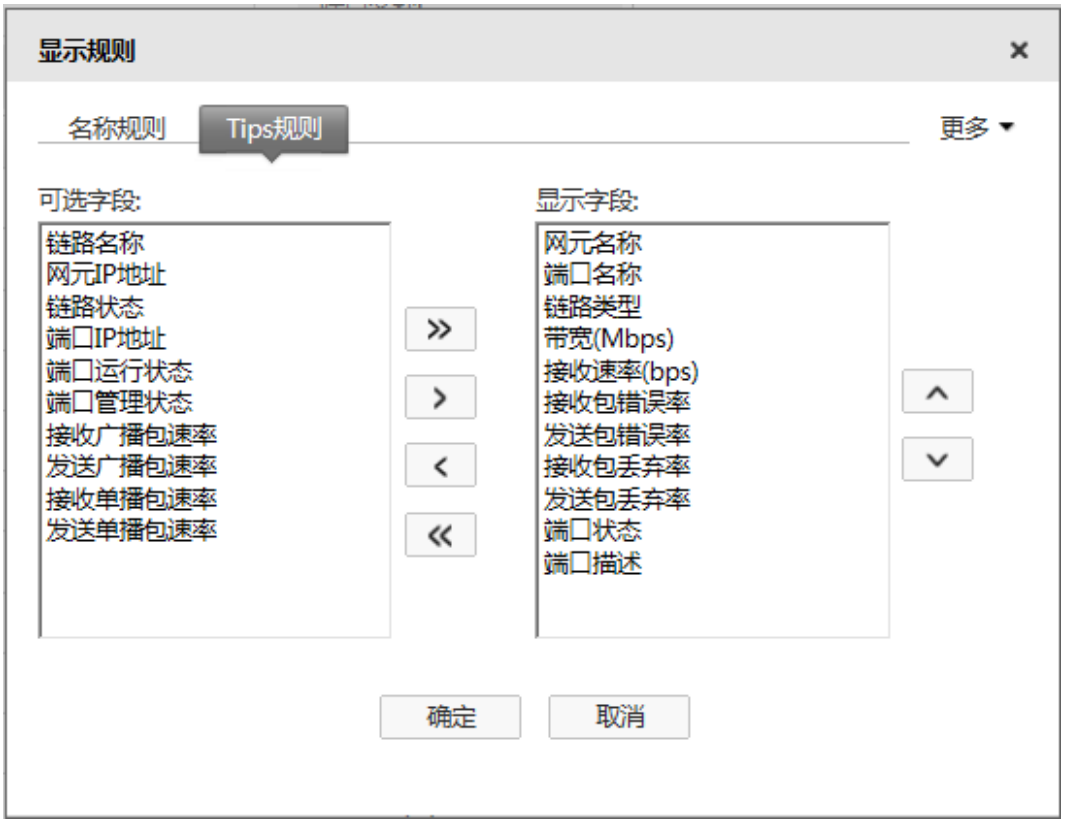
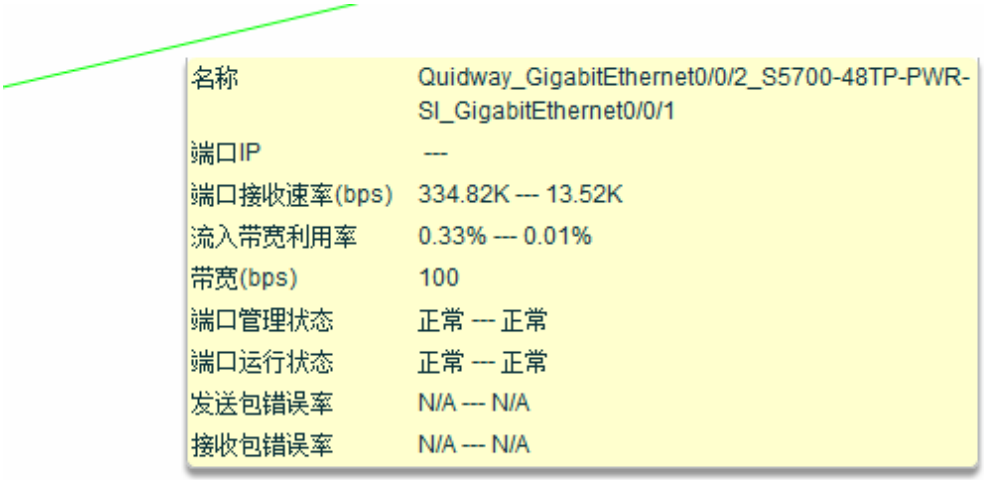


图4-23 链路 tips 默认显示效果

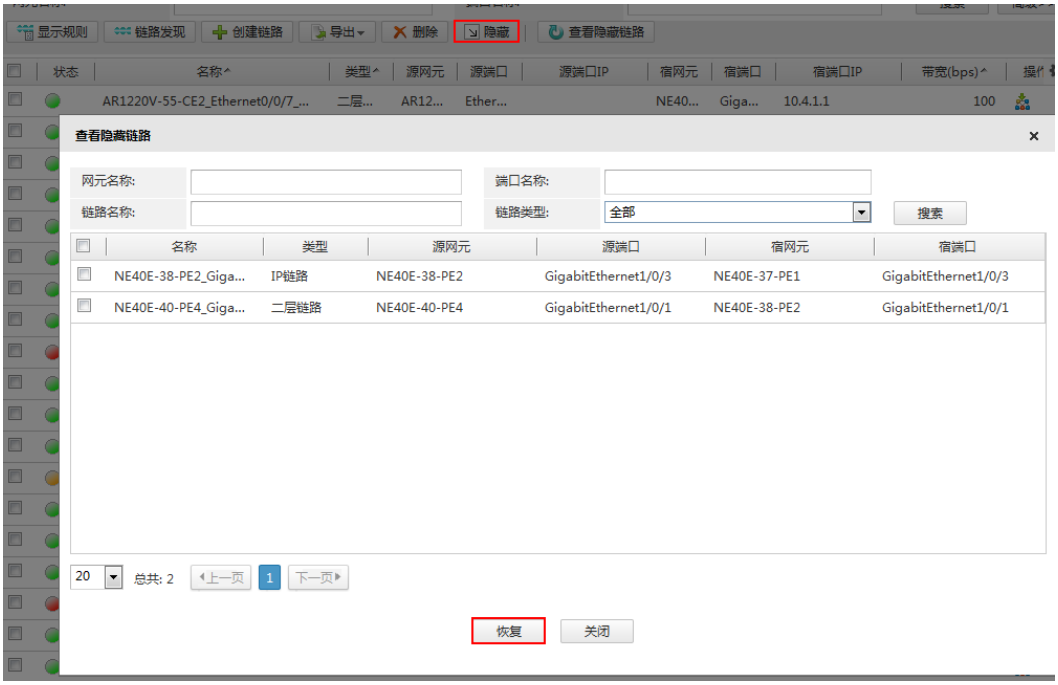


链路隐藏

链路隐藏功能主要应用场景有两个：（1）物理拓扑上存在用户不想显示的某条链路，用户想将其隐藏起来，并且在自动发现或者手动发现时，都不显示；（2）拓扑中可能会存在发现错误的链路，此时需要将错误的链路隐藏不显示。

链路隐藏功能使用：如果用户不想显示某条链路，可以在物理拓扑或者链路管理中将其“隐藏”，则在网管中就不会对用户展现此链路；如果用户想恢复展现此链路，可以在链路管理的“查看隐藏链路”中进行链路恢复操作，如图 4-24 所示。

图4-24 链路恢复功能



4.2.1.4 IP 拓扑管理

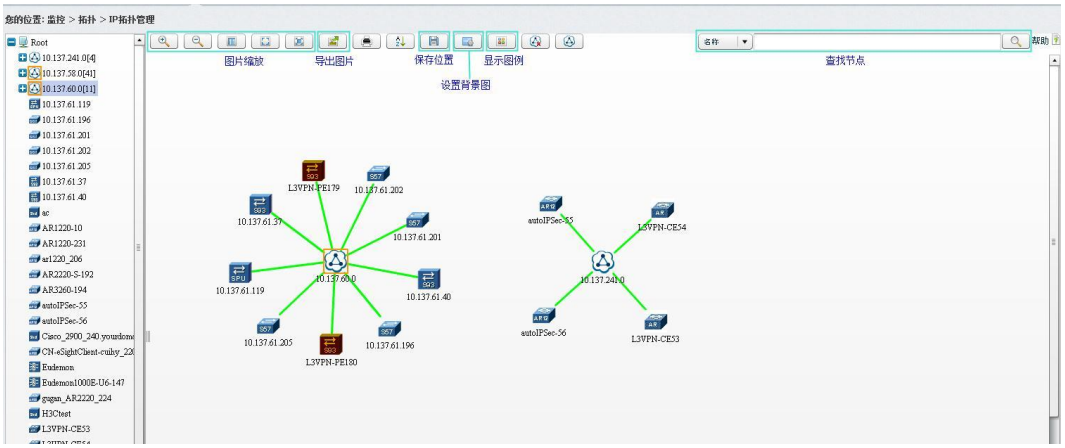
用户可以通过 IP 拓扑的菜单，进入 IP 拓扑界面，查看路由设备和二层设备及其之间链路连接。

表4-10 IP 拓扑管理基本概念

术语	说明
网元	拓扑管理的核心单位，用来标识被管理的设备。在拓扑视图中，不同的图标代表各种网元类型。
IP 子网	根据 IP 地址和子网掩码划分出的 IP 地址段。
链路	标识通信设备之间的物理或者逻辑连接。
路由设备	具备路由能力，可以连接多个网络或网段的网络设备。
二层设备	工作在 OSI/RM 网络体系结构中数据链路层的网络设

术语	说明
	备。

图4-25 IP 拓扑管理界面示意图



浏览拓扑图

- 拓扑界面上分成左树右图的方式，对拓扑对象按所属 IP 子网进行分层展示。
- 提供鸟瞰、全屏进行拓扑图整体、局部观测能力。
- 显示网元、链路的告警状态及 Tips 信息。

拓扑图操作

- 支持拓扑图的缩放操作。
- 支持拓扑图图片导出、图片打印、设置背景图。
- 支持拓扑图节点的移动，并保存设置。
- 提供其他功能的快捷操作入口。

告警级别显示

拓扑节点的颜色直观的反映该节点相应的最高告警级别，且是动态更新显示的。用户可以根据图标颜色了解到全网设备的告警情况，如有紧急告警，可以第一时间确认和处理。

网元管理集中入口

用户可以通过拓扑视图中网元的快捷菜单，快速进入到该设备的单网元管理界面。

IP 变更显示

- 支持查看网元/全网的 IP 变更情况

- 支持清除网元/全网的 IP 变更记录

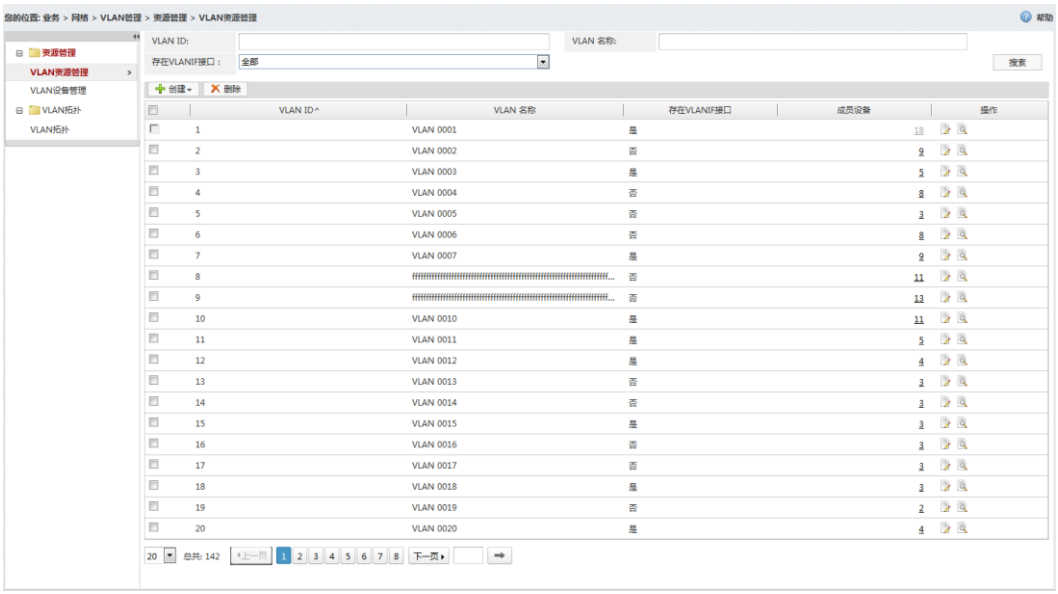
4.2.1.5 VLAN 管理

VLAN 管理模块是对 eSight 网管内的 VLAN 资源进行统一管理配置的应用。主要包括管理全网 VLAN 资源；向各设备的端口下发 VLAN 配置（对于 Access 类型的端口，仅下发 PVID，对于 Trunk 类型的端口，下发 PVID 和允许通过的 VLAN；对于 Hybrid 类型的端口，下发 PVID，Tagged VLAN 和 Untagged VLAN)； 自动计算路径展示设备和链路的 VLAN 拓扑 ； 同时提供单设备下 VLAN 管理的功能。

VLAN 资源管理

提供统一 VLAN 资源管理入口。如图 4-26 所示。

图4-26 VLAN 资源管理示意图



提供统一查询模式，可以通过 VLANID 和是否存在 VLANIF 接口等条件查询当前存在的所有 VLAN 资源。

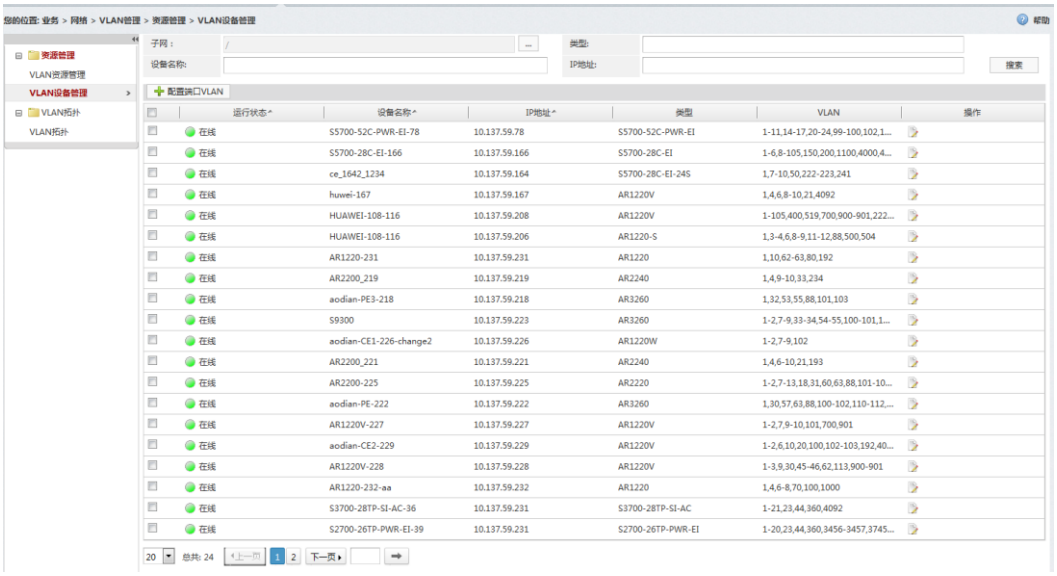
通过创建 VLAN，可以在全网范围内选择多个设备，将创建的 VLAN 资源直接下发到设备；支持一次批量创建多个 VLAN 资源。

通过删除 VLAN，可以在全网范围内将此 VLAN 删除；如果该 VLAN 在某个端口上已经被设置为 PVID，则可以将这个端口的 PVID 重新设置为另外一个 VLAN，默认重设值为 1。

VLAN 设备管理

提供从设备角度管理 VLAN 的入口。如图 4-27 所示。

图4-27 VLAN 设备管理示意图



提供统一查询模式，可以通过子网、设备类型、设备名称、设备 IP 地址等条件过滤查询符合条件的设备。

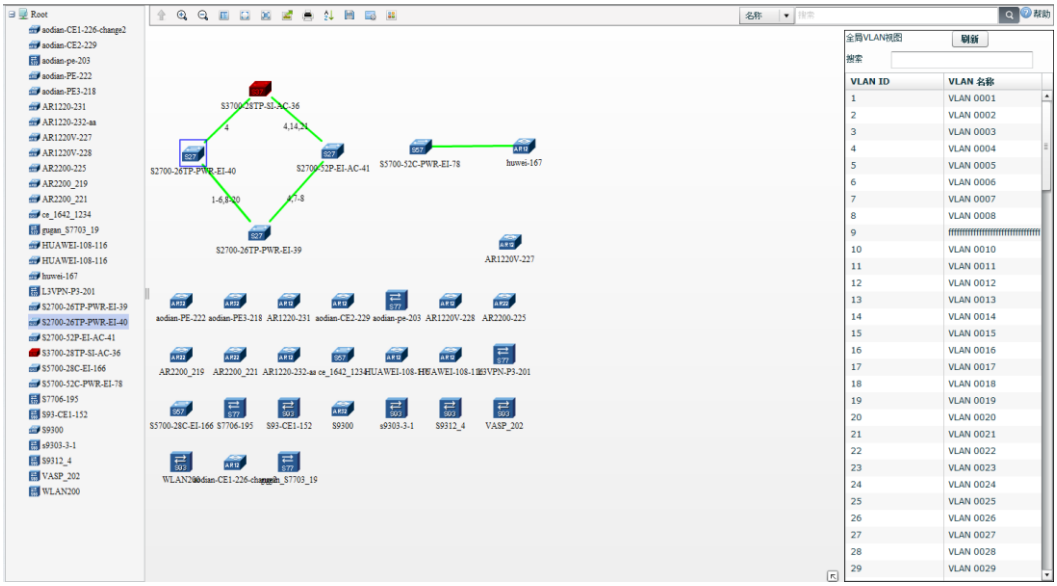
通过配置端口 VLAN，可以在全网范围内选择多个设备的多个端口，并将 VLAN 参数统一下发到这些端口上。

可以跳转到设备管理器中进行单设备 VLAN 的管理。

VLAN 拓扑

提供全网 VLAN 资源相关的设备和链路的统一拓扑视图。如图 4-28 所示。

图4-28 VLAN 拓扑示意图



可以在拓扑上查看某一条链路两端的设备接口类型以及接口 VLAN 详细信息；同时查看该链路上现在允许通过的 VLAN 报文信息。

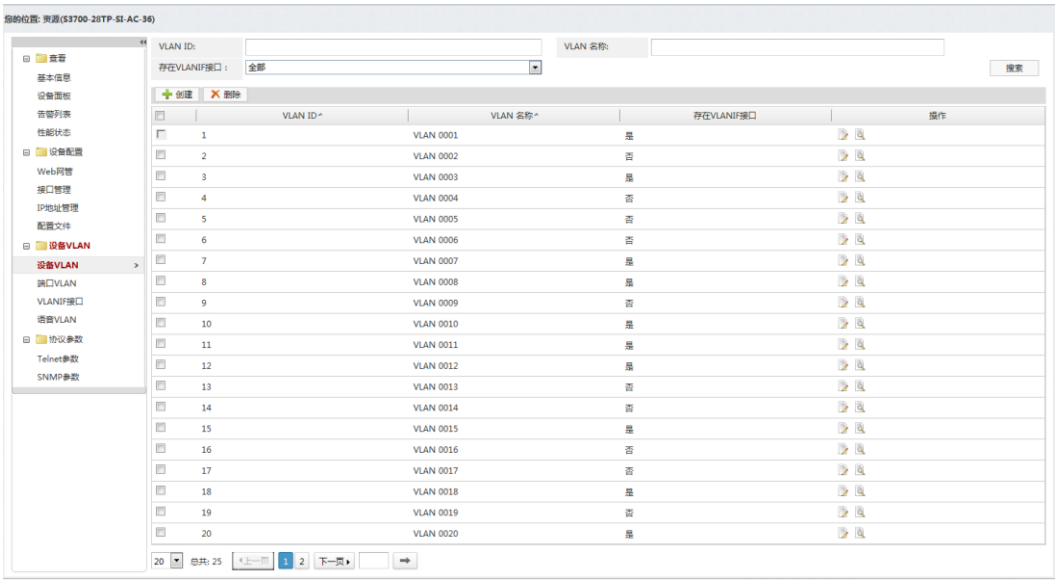
提供按照 VLAN ID 过滤相关的设备和链路的功能；可以通过不同的 VLAN 查看哪些设备和链路允许该 VLAN 通过。

可以在拓扑上直接将某一个设备加入或者从某个 VLAN 中去除。

单设备 VLAN 管理

单设备 VLAN 管理在设备管理器中提供对该设备上 VLAN 资源的管理能力。如图 4-29 所示。

图4-29 单设备 VLAN 管理示意图



可以在该设备上创建和删除 VLAN。

删除 VLAN 时，如果该 VLAN 已经被某个端口设为 PVID，则用户可以将这个端口的 PVID 重新设置为另外一个 VLAN，默认重设值为 1。

提供批量修改该设备下多个端口的 VLAN 参数的功能；可以统一修改一批端口的类型和 VLAN 参数。

可以在该设备上新建/删除 VLAN IF。

提供对该设备上的语音 VLAN 进行管理的功能；包括设置设备上的语音 VLAN 的通信参数，包括生命周期以及协议优先级（802.1P/DSCP）；语音流源 MAC 地址和掩码；接收语音流的端口参数。

4.2.1.6 智能配置工具

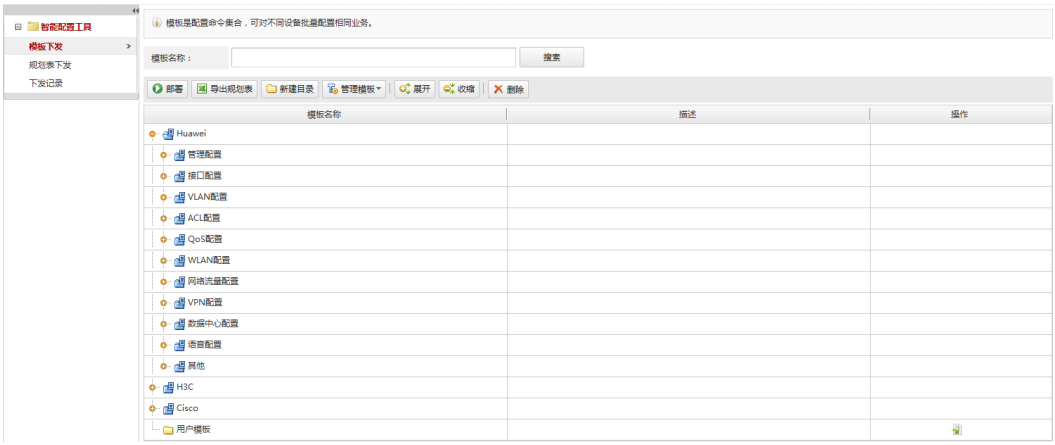
智能配置工具用于对设备进行业务配置，支持配置模板和规划表对设备批量下发业务配置。

模板主要用于对多个网元进行相同业务配置的批量下发；规划表主要用于对多个网元进行相似业务配置的批量下发。对于定时的下发任务，可以通过邮件通知执行结果。

模板下发

通过配置系统预定义模版、导入模版与自定义模板，以向导方式下发，对设备实现批量配置，并且可进行命令校验。如图 4-30 所示。

图4-30 模板下发图



模板规划表下发

通过模板规划表方式对华为设备实现批量配置下发，用户在导出模板的规划表中填写业务配置参数，导入智能配置工具后以向导方式下发设备。如图 4-31 所示。

图4-31 模板规划表下发图

命令规划表下发

通过命令规划表方式对华为以及第三方设备实现批量配置下发，用户下载命令规划表模版，填写业务配置命令行，导入智能配置工具后以向导方式下发设备。如图 4-32 所示。

图4-32 命令规划表下发图

4.2.1.7 配置文件管理

配置文件管理指对设备的配置信息进行管理，提供对设备配置文件的导入、备份、恢复、比较、基线化管理。当网络出现问题时，可以根据之前备份的网络可运行时的配置文件与当前设备正在运行的配置进行比较，帮助您快速定位并恢复当前出现的故障。同时还支持配置变更管理，配置文件备份后会自动进行差异比较，获取配置变更，支持告警与邮件通知配置变更，帮助你即时了解网络的配置变更情况。

设备配置管理

- 备份任务

  按日、周、月为周期，按设定时间对任务所包含设备的运行配置文件进行备份。支持设置设备配置变更告警触发备份配置文件。备份任务可以按照定制的时间进行定时备份，也可以对备份任务进行立即备份操作，同时支持设备变更告警触发备份。备份的执行结果支持 Email 远程通知，备份任务的执行结果以邮件的方式通知用户，邮件当中以附件的方式告知用户执行备份失败的设备列表。如图 4-33 所示。

  图4-33 设备配置管理界面示意图

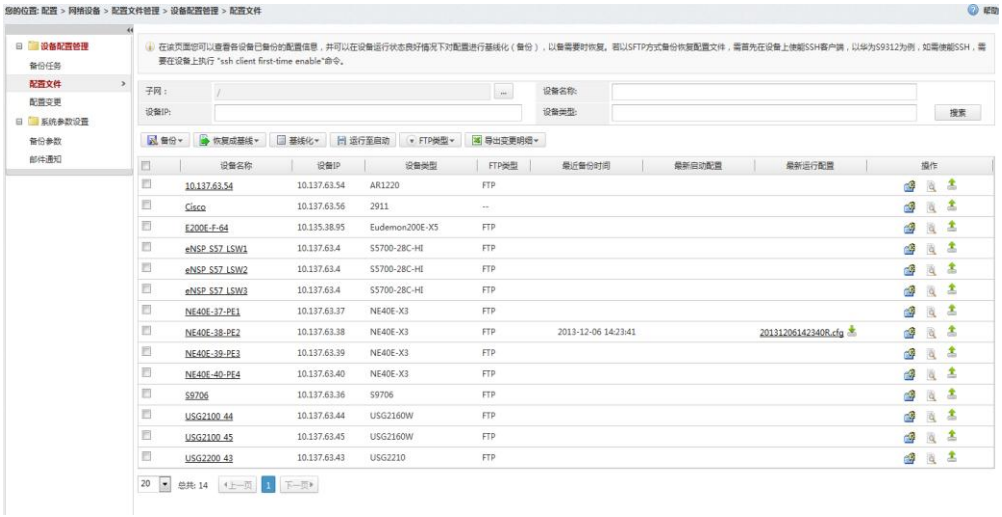
  

- 配置文件

  对指定设备的运行配置/启动配置进行备份，将选定的设备的配置文件恢复成设备的运行配置/启动配置，对选定的配置文件进行基线化，对选定的设备更改 FTP 操作类型(第三方设备不支持)，同时能够方便地查看设备上面已经备份到网管服务器

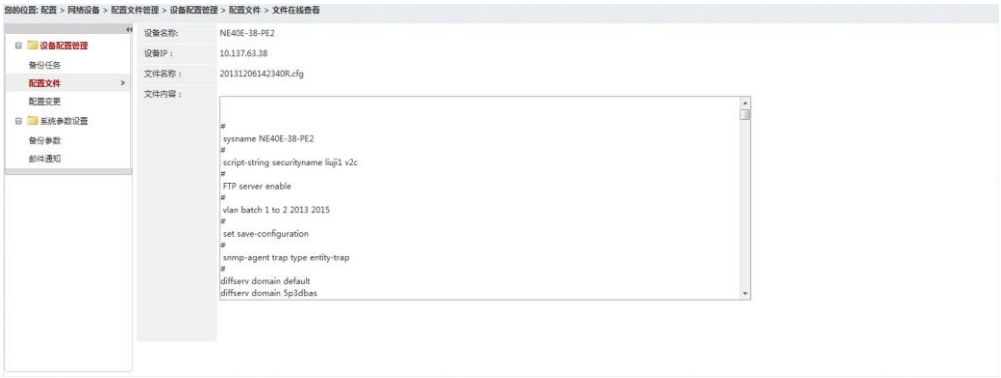
的运行配置文件和启动配置文件，还支持以 Excel 形式导出配置变更统计报告。如图 4-34 所示。

图4-34 配置文件示意图



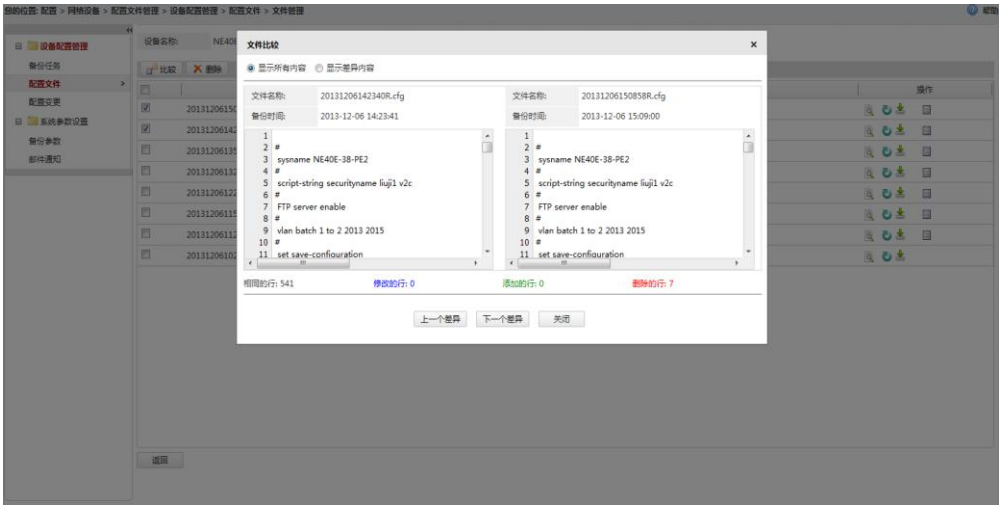
对于已经备份到本地的配置文件，可以进行配置文件在线查看，如图 4-35 所示。

图4-35 配置文件在线查看示意图



并进行比较配置文件差异和配置文件下载、导入配置文件以及配置文件删除操作。文件比较功能当前提供了已经备份到网管服务器的配置文件之间的比较。如图 4-36 所示。

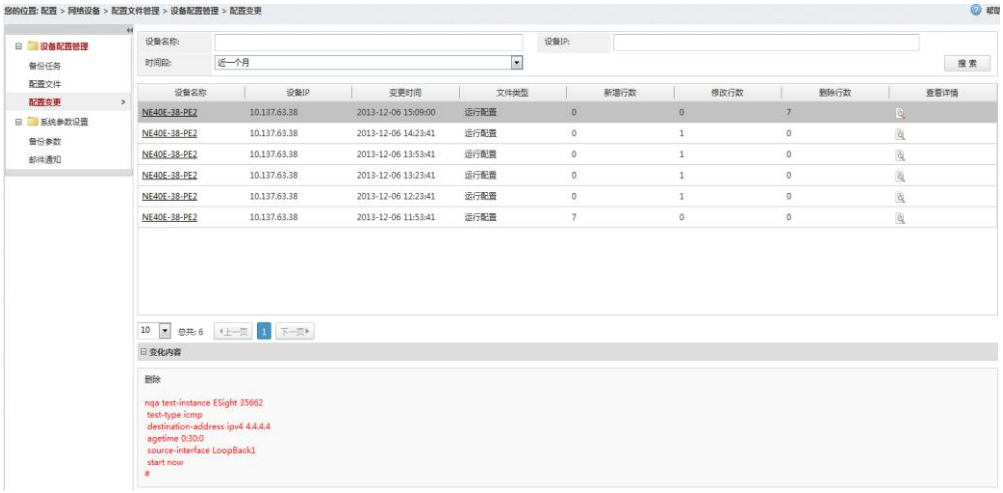
图4-36 配置文件比较操作示意图



- 配置变更

  对配置文件备份后网管会自动进行差异比较获取配置变更，配置变更界面可以方便地查询出配置变更的差异，快速地查看一个配置的增、删、改信息。通过查看详情弹出文件比较页面 了解配置变更的具体情况。如图 4-37 所示。

图4-37 配置变更查询示意图



系统参数管理

- 备份参数

  配置每一台设备在网管服务器上保存的配置文件的数量的上限，该上限应用于网管服务器所管理的所有设备。对设备配置变更是否触发配置文件备份进行配置。

- 邮件通知

  配置文件备份任务执行结果提醒以及设备配置文件变更提醒。 支持收件人设置，配置文件变更提醒支持邮件主题及发送时间的设置。如图 4-38 所示。

图4-38 邮件通知设置示意图

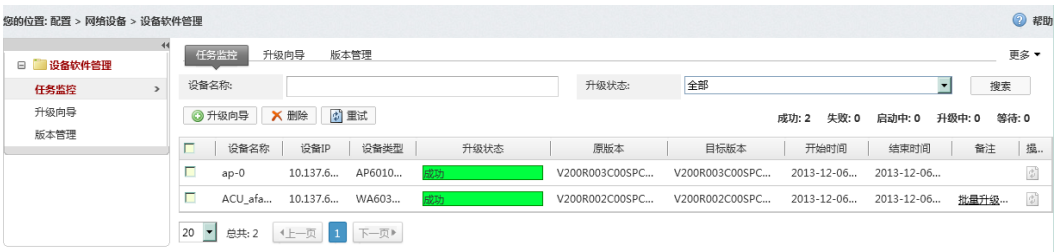
4.2.1.8 设备软件管理

设备软件管理是 eSight 网管对于管理设备的软件版本进行升级操作的功能模块，当前版本支持通过 AC 来升级瘦 AP 的软件版本，包括任务监控、升级向导和版本管理三个子功能。任务监控管理当前网管中所有的设备升级任务，实时反映升级状态；升级向导通过向导式创建设备升级任务；版本管理按照设备类型粒度统一管理设备软件映像文件。

任务监控

统一管理所有的设备升级任务，实时反馈升级状态。如图 4-39 所示。

图4-39 任务监控示意图



- 目前版本支持瘦 AP 的软件升级，主菜单加鉴权处理，在 WLAN 业务组件安装的情况下展示。
- 瘦 AP 的升级支持单个与批量任务，若选取的瘦 AP 为 AC 下某种类型的全量 AP 则生成一条批量任务，提升效率并降低设备 telnet 连接通道负担。
- 升级任务当前进展有更新时实时刷新页面，对于失败的任务可进行重试操作。

升级向导

通过向导式创建升级任务。如图 4-40 所示。

图4-40 升级向导示意图

- 三步向导式创建升级任务并汇总任务详情。
- 可重置继续创建任务，亦可跳转至监控主界面查看任务执行实时情况。
- 选择升级版本步骤中增加版本管理创建链接，增加操作易用性。

版本管理

统一管理设备的软件映像文件。如图 4-41 所示。

图4-41 版本管理示意图

4.2.1.9 MIB 管理

eSight 网管中提供 MIB 工具可以读取一个 MIB(.mib)文件进行编译，产生的目标文件将自动被放到 MIB 工具要使用的目录下供 MIB 工具使用。 支持 SNMP 协议版本 V1/V2c/V3 协议的查询操作，通过它可以有效、安全地对 MIB 数据进行读取和监控，从而实现对网络的有效管理。

MIB 编译

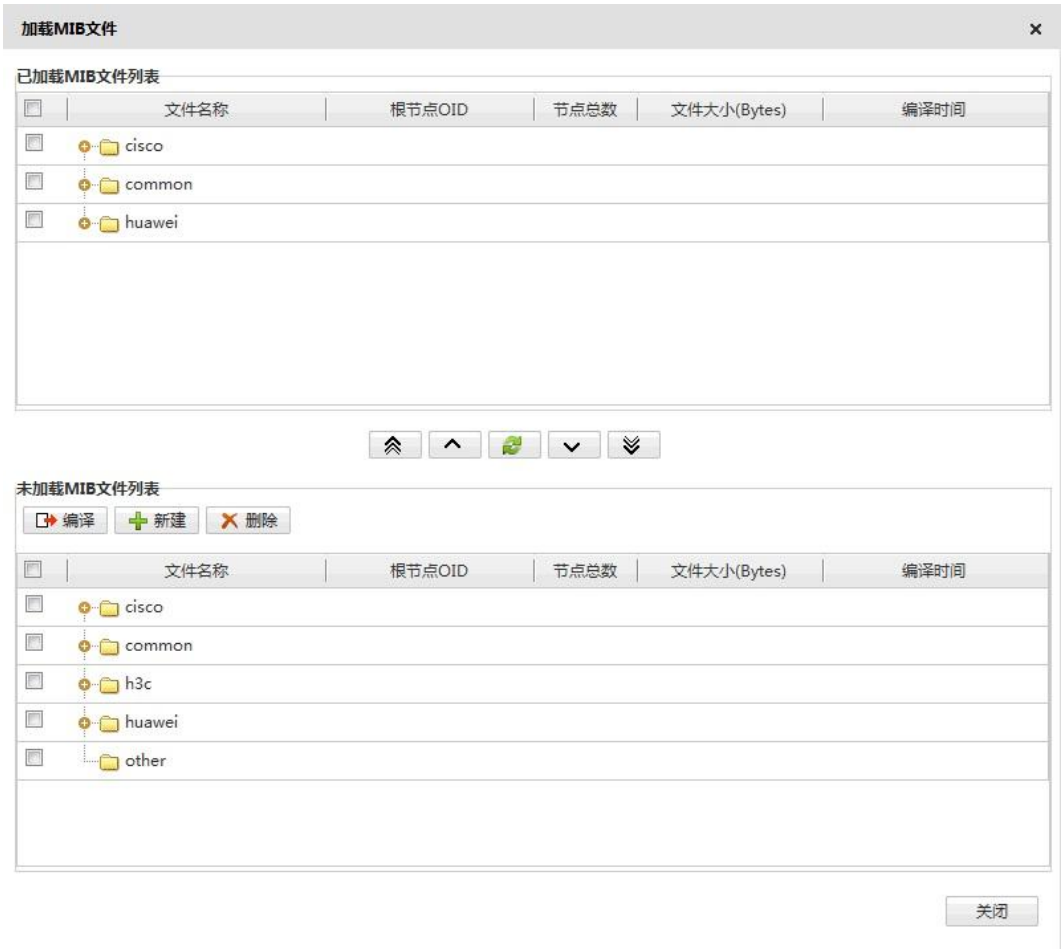
支持选择一个 MIB 文件执行编译操作，编译完成后可以选择结果文件的保存目录，具体 MIB 文件的编译结果显示在编译结果界面上。

图4-42 MIB 编译界面

MIB 加载

MIB 节点管理，支持 MIB 节点的上传、编译、加载、卸载、新建文件目录、删除操作。

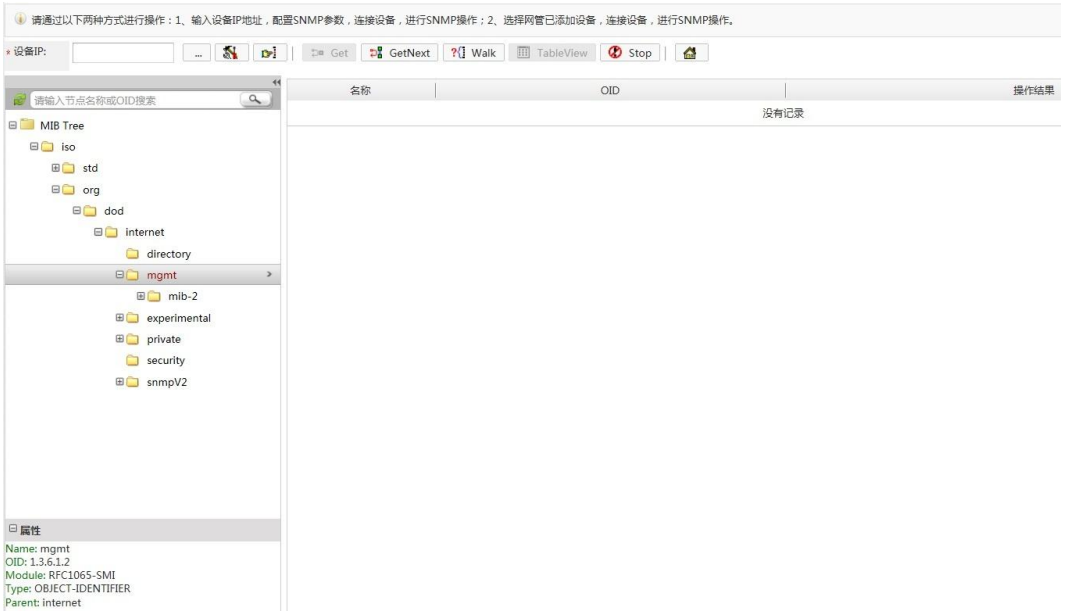
图4-43 MIB 加载界面



MIB 操作

在设备 IP 框当中输入设备 IP 后，使用 SNMP 设备，设备连通后可以通过工具对设备做 Get/GetNext/Walk/TableView 等操作，操作过程当中如果用户想终止操作可以点击 Stop 操作按钮停止数据获取。

图4-44 MIB 操作界面



4.2.1.10 自定义设备管理

针对企业网用户需要管理的多种厂商的设备类型，eSight 提供了自定义管理功能。用户通过自定义管理模块，完成对设备类型、性能指标、告警参数、Telnet 定制、配置文件管理、网元面板定制，增强对设备基本能力的管理。

厂商基本信息定制

厂商基本信息定制，完成对设备厂商的基本信息的定制功能，包括增加、删除以及修改功能。如图 4-45 所示。

图4-45 厂商基本信息定制

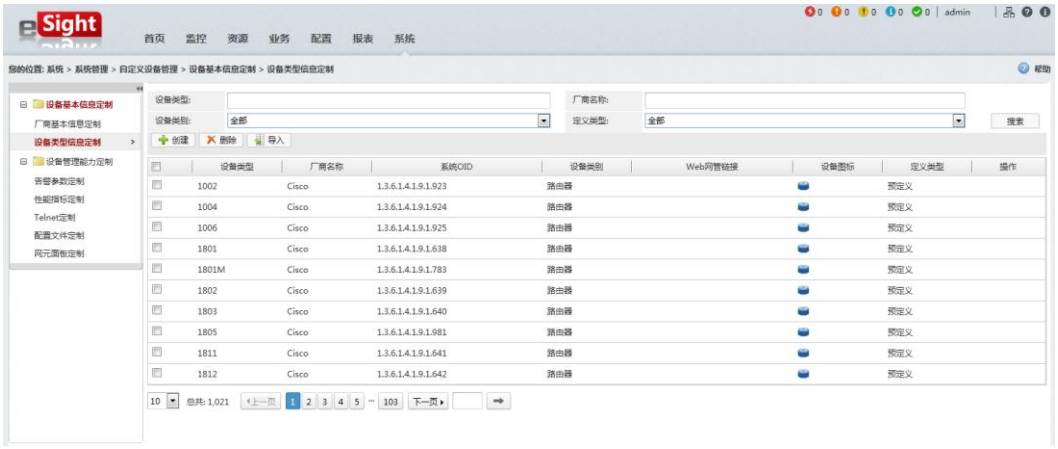
- 厂商名称：当前要定制的厂商的名称。

- 厂商描述：记录用户关注的厂商信息。（可选择是否定制）
- 厂商电话：厂商的服务电话。（可选择是否定制）
- 厂商联系人：一般是厂商设备的维护人员。（可选择是否定制）
- 定义类型：区分当前厂商基本信息是由网管开发人员定制还是由用户定制，分为预定义和自定义两种类型，前者标识厂商基本信息在网管发布之前由开发人员定制，后者标识该厂商基本信息由用户定制的。

设备类型信息定制

提供对设备类型的定制功能。设备在加载到网管之前，如果系统中没有预定义信息，在网管显示此设备为 unknown 设备，网管只提供对当前设备基本信息的查看能力，不具备对设备告警、性能等的管理能力，用户通过自定义设备管理定制完设备类型信息之后，网管界面显示此设备的真实的类型信息，并能够对设备的标准告警、性能进行监控。如图 4-46 所示。

图4-46 设备类型信息定制



- 设备 OID：用于区分设备类型的标识。
- 设备类别：用于区分当前设备的特性，目前区分为交换机、路由器、服务器、打印机、安全设备等几种类别。
- WEB 网管链接：部分设备提供了 web 网管的功能，用户定制 web 网管链接之后，通过网元管理器提供的访问接口，自动链接到设备的 web 网管。
- 设备图标：可标识当前设备类型的图标，用户可任意定制。
- 定义类型：同厂商基本信息定制。

告警参数定制

提供按照 SNMP v1 和 SNMP v2c/v3 两种不同的 SNMP 版本定制告警参数的功能，包括增加、删除、修改功能。用户可通过此功能定制关注的告警信息。对于没有预定义的告警，在定制之前，网管丢弃设备上报的告警，用户定制之后，告警模块解析并上报此告警。

用户删除定制的告警参数，网管不会删除对应告警的历史告警信息，但是在删除之后，告警模块不再处理设备上报的此告警信息。

提供修改告警级别、事件类型、告警原因、修复建议、详细信息、告警定位参数的功能。如图 4-47 所示。

图4-47 告警参数定制

- 厂商名称：由于各个厂商的设备的告警参数不一致，告警信息的定制按厂商进行区分。
- 告警名称：告警信息的名称。
- 告警级别：告警的紧急级别，与告警模块一致，分为紧急、重要、次要、提示四个级别。
- 通知类型：设备上报的告警的通知类型，分为告警、恢复告警和事件三种类型。
- 事件类型：分为通信告警、设备告警、处理出错告警、业务质量告警、环境告警、完整性告警、操作告警、物理资源告警、安全告警以及时间域告警。
- SNMP 版本：根据设备支持的 SNMP 版本的不同，提供 SNMPv1 和 SNMP v2c/v3 两种不同的 SNMP 版本告警的定制功能。
- generic、specific、企业 ID：用户定位一条 SNMP v1 告警的关键参数。
- 告警 OID：用于定位一条 SNMP v2c/v3 版本告警信息的参数，对应告警数据包的 Trap oid 值。
- 告警原因：当前告警产生的可能原因。
- 修复建议：修复当前告警的可能的途径和方法。
- 详细信息：告警的详细信息。
- 定位参数：解析一条告警所需要的定位参数信息。

性能指标定制

提供定制用户关注的指标的功能，包括增加、删除以及修改指标的能力。用户定制指标之后在性能管理模块定制此指标的监控实例，性能模块在下一个采集周期采集定制的指标的数据。如图 4-48 所示。

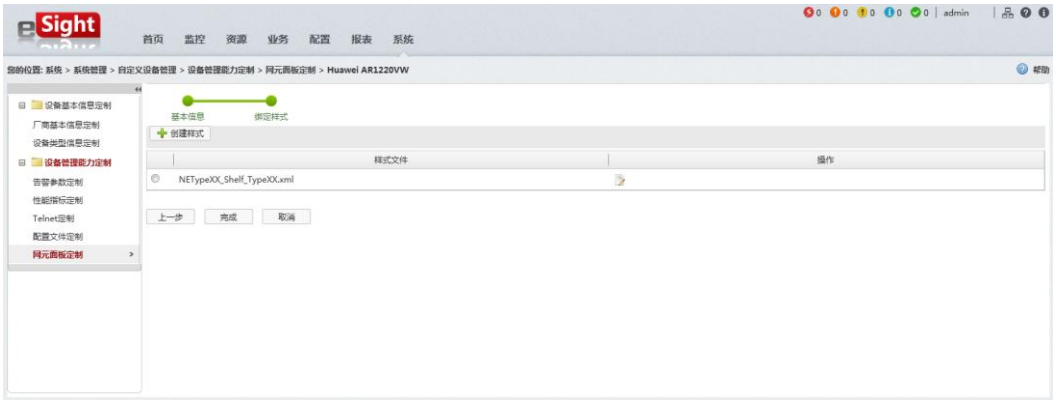
图4-48 性能指标定制

- 指标名称：标识当前指标采集内容的指标名称。
- 指标组：根据指标采集对象的不同，分为不同的指标组。例如：用户自定义设备指标组、用户自定义机框指标组、用户自定义单板指标组、用户自定义接口指标组等。如果用户定制采集接口某个性能的指标，需要选择“用户自定义接口指标组”。
- 设备类型：当前定制的指标可用于采集的设备类型。
- 指标单位：指标显示的度量单位。
- 指标公式：是用户要监视的 MIB 节点及其运算的一个表达式。

网元面板定制

对于用户自定义的设备类型，网管提供默认的设备面板显示功能。用户可通过网元面板定制功能，实现使用设备照片或者高仿真图对设备面板的定制，包括机框、面板、子卡以及端口的定制功能。定制完毕，用户打开属于当前设备类型的设备面板之后，设备面板显示的就是定制后的高仿真设备面板。如图 4-49 所示。

图4-49 网元面板定制

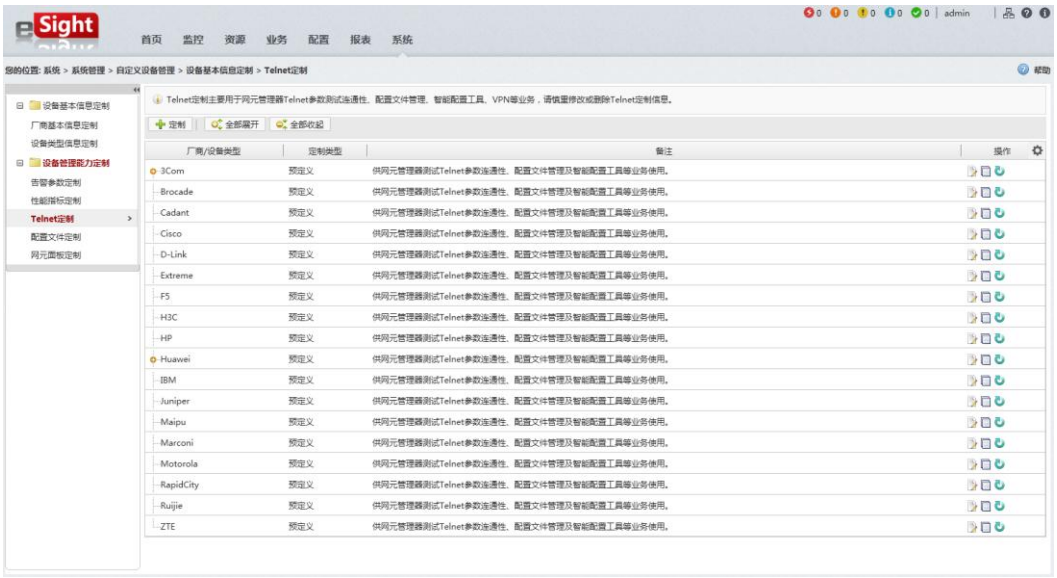


Telnet 定制

Telnet 定制提供不同设备类型的 Telnet 参数定制功能。Telnet 参数定制可以定制设备 Telnet 基本信息：包括登录用户名提示符、登录密码提示符、登录失败提示符、下发命令提示符、退出命令、备注信息。以及 Telnet 的特权模式信息：包括特权命令、特权密码提示符、More 提示符、回显控制命令、交互式选择提示符、交互式选择命令、失败提示、排除失败。

用户通过完成 Telnet 参数定制，可以对设备进行 Telnet 连通性检测。通过读取定制的 Telnet 参数完成配置文件管理对设备进行配置文件的备份，完成智能配置工具对设备下发配置命令，用于 VPN 等业务的配置和解析。如图 4-50 所示

图4-50 Telnet 定制



配置文件定制

配置文件定制提供对设备的配置文件管理的命令的定制功能，包括备份配置文件命令、恢复设备配置文件命令以及重启设备命令。用户完成配置文件定制之后，在设备配置文件管理模块定制属于当前设备类型的设备的备份任务，网管就可以对设备的配置文件进行备份管理。如图 4-51 所示。

图4-51 配置文件定制

- 设备类型：要定制的配置文件命令的设备类型。
- 备份命令：备份运行命令、备份启动命令。
- 恢复命令：恢复运行命令、恢复启动命令。
- 重启命令：重启设备的命令。

4.2.2 主机管理

提供 OS 查看、查询、删除、统计等管理功能，用户可以根据实际的运维需求对操作系统进行监控和维护。

4.2.3 存储设备管理

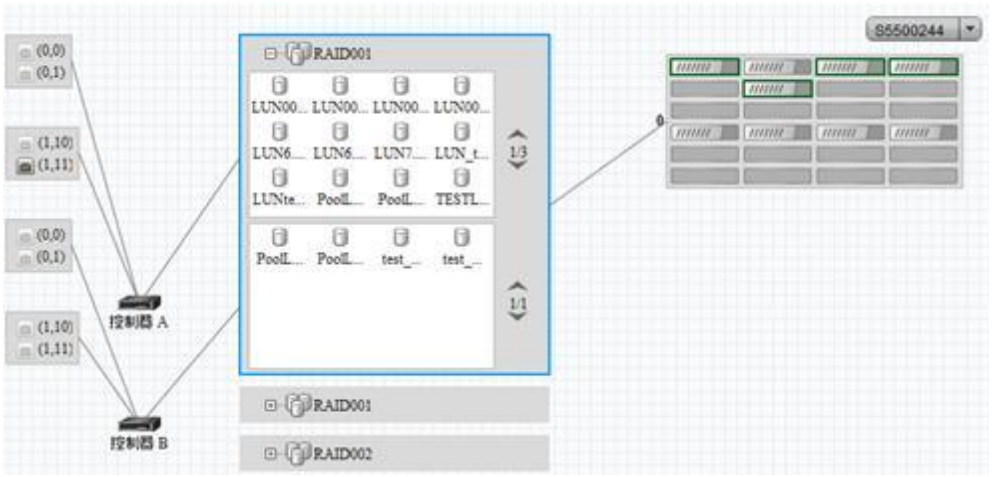
存储设备管理提供多类型、多厂商存储设备的可视化统一管理，提升运维效率，同时降低运维人员的技术门槛。

存储系统内部组件管理

以可视化方式，展现存储系统内部的物理和逻辑组件间的关联关系，使设备状态一目了然，以便故障发生时能够精确定位，快速恢复业务。

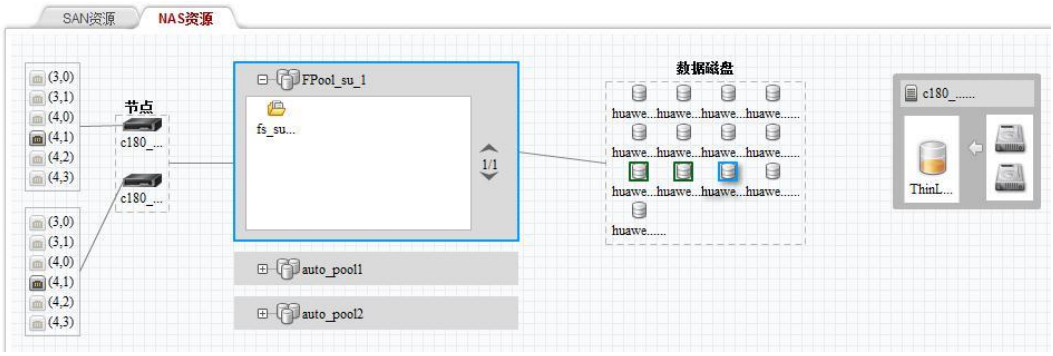
- 针对块存储：存储阵列前端端口、控制器、RAID 组、LUN、硬盘之间的逻辑关系。

图4-52 存储系统内部组件的逻辑关系（块存储）



- 针对文件存储：NAS 引擎前端端口、NAS 引擎节点、文件系统、文件存储池、数据磁盘、以及存储单元上的 LUN 和硬盘之间的逻辑关系。

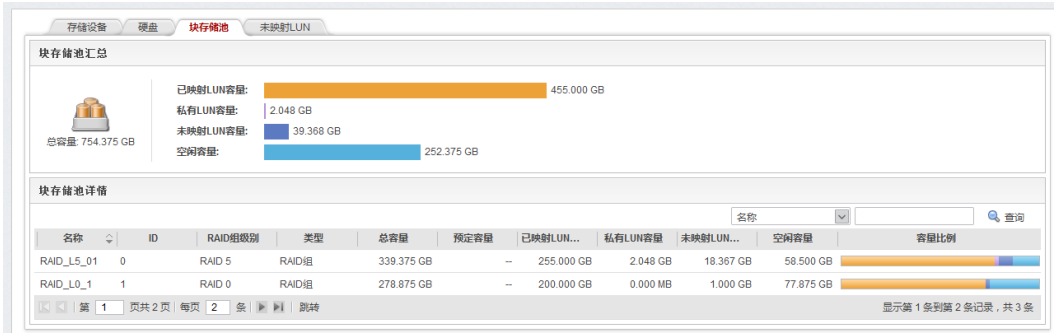
图4-53 存储系统内部组件的逻辑关系（文件存储）



存储系统容量管理

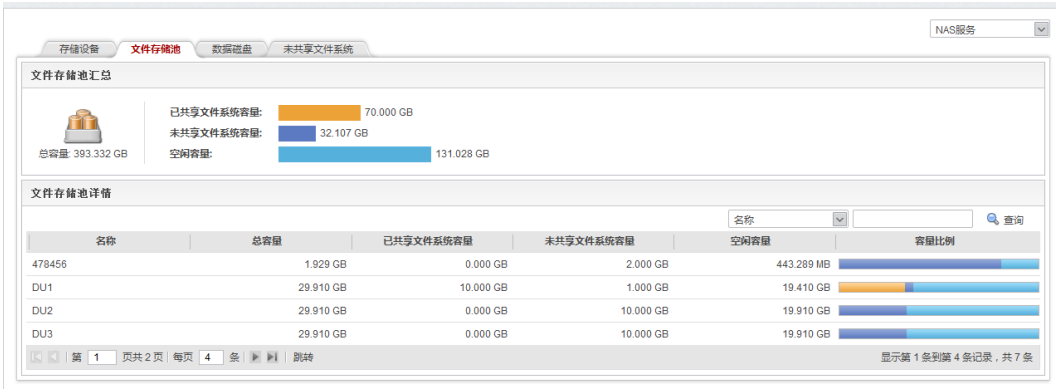
- 针对块存储：从存储设备、硬盘、块存储池、未映射 LUN 四个维度管理容量使用状况。

图4-54 存储系统容量使用状况管理（块存储）



- 针对文件存储：从存储设备、文件存储池、数据磁盘、未共享文件系统四个维度管理容量使用状况。

图4-55 存储系统容量使用状况管理（文件存储）



4.2.4 统一通信管理

统一通信管理提供方便、快捷的统一通信设备配置功能，并提供向导式的业务安装配置，一站完成业务部署，实现端到端的可视化监控网络信息，并能直观地展示故障信息，快速定位解决问题。

说明
统一通信管理功能需要安装 eSight UC/CC 设备管理组件。

4.2.4.1 统一通信设备管理

eSight 支持对统一通信设备进行管理，包括 IP PBX、U2900、EGW、IAD、UAP3300 设备。

4.2.4.1.1 IP PBX 管理

eSight 支持的 IP PBX 管理功能包括：业务管理、配置管理、设备面板管理、日志管理。

管理界面

图4-56 IP PBX 管理界面

业务管理

- 设备信息

  通过 eSight 可以查看 IP PBX 的基本信息、License 信息、版本信息、补丁信息。
- Ping 测试

  通过 Ping 命令，测试 IP PBX 设备与其他设备的连通性。
- 信令跟踪

  eSight 支持对 IP PBX 的协议消息、端口信令链路的接续过程、业务流程等进行实时动态跟踪与监视，支持将信令导出为 csv 格式，当后期 IP PBX 离线时，用户也可以查看信令的详细信息。
- 话务统计

  eSight 支持统计 IP PBX 的话务数据、设置话务统计任务的采集周期、设置话务统计任务的起始时间和结束时间、导出话务数据、删除话务数据。统计范围包括：全局 RTP（Real-time Transfer Protocol）消息包数量、SIP 话务数量、中继出局 SIP 话务数量、中继入局 SIP 话务数量及 SIP 通话时长。
- 配置数据备份与还原

  eSight 提供了对 IP PBX 配置数据（data.bin 文件）的备份、还原和另存为功能，您可以设置定时或手动备份配置数据。
- 中继跟踪

  eSight 支持按局向跟踪中继资源，包括查看实时数据和查看历史数据。
- 补丁管理

  通过 eSight 可以查看、加载、激活、去激活、保存和删除补丁。

配置管理

eSight 提供对 IP PBX 的批量配置和单个配置功能。

- 批量配置

  提供批量配置 IP PBX 的 SIP 中继、主备服务和离线前转软件参数。

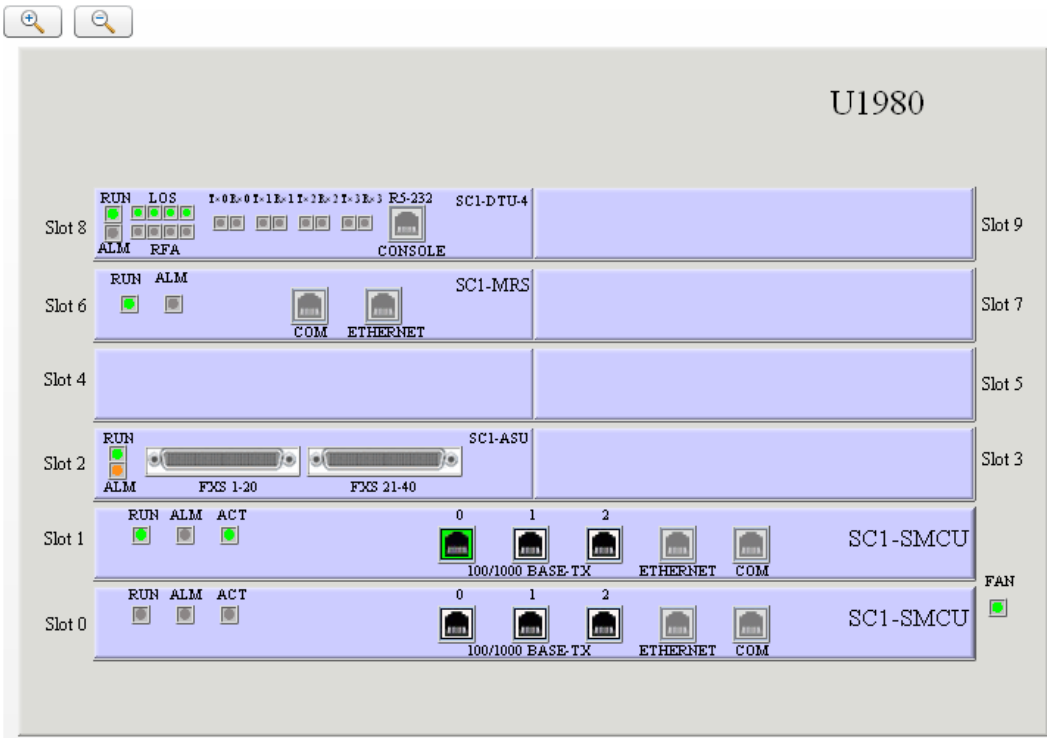
- 单个配置

  命令树中包含了 IP PBX 的命令，用户可以通过命令树对单个 IP PBX 进行配置。

设备面板管理

IP PBX 设备面板提供了一个直观的设备仿真界面，用户可通过设备面板查看设备的运行状态，并对单板进行增加、修改、删除等。

图4-57 IP PBX 设备面板



日志管理

- 操作日志

  操作日志记录了用户对 IP PBX 执行的操作。eSight 支持搜索并导出操作日志。

- 运行日志

  运行日志记录了 IP PBX 运行时的信息、警告和错误。eSight 支持增加、修改、暂停、重启、删除运行日志任务，搜索和导出运行日志。

网元自动连接

当网元之间存在 SIP 注册关系、SIP 中继或 IP PBX 间存在主备服务时，eSight 可以自动在拓扑中创建连接。

4.2.4.1.2 U2900 管理

eSight 支持的 U2900 管理的设备面板管理功能。

了解 U2900

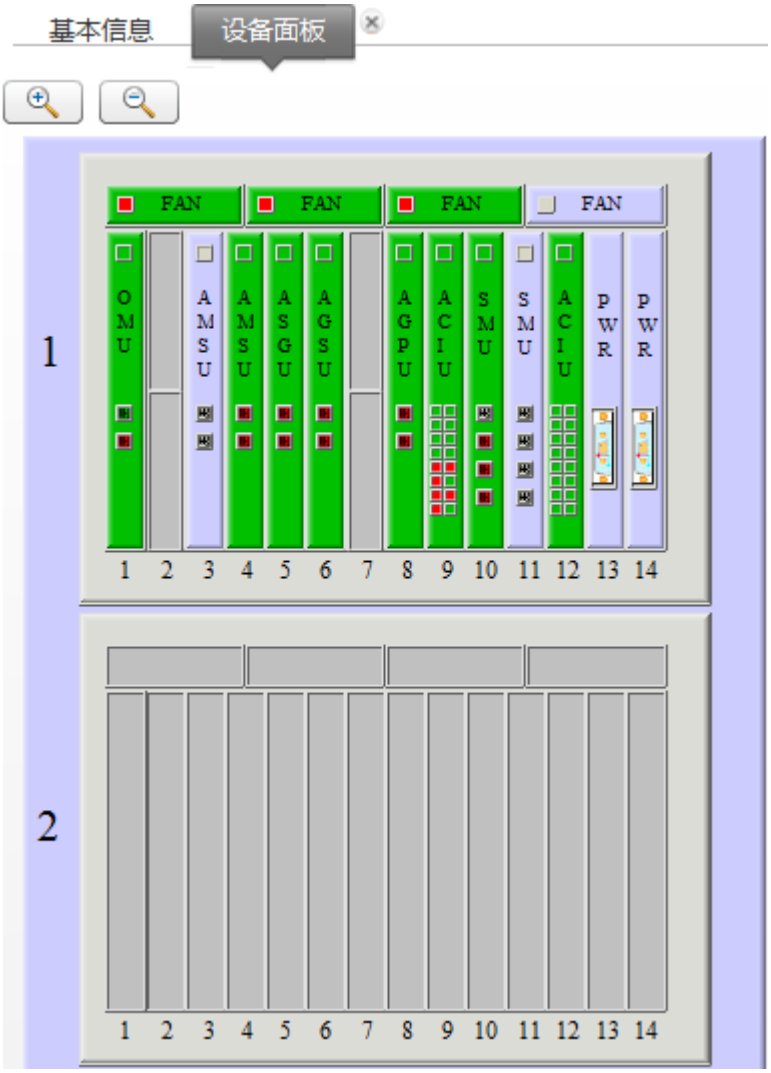
U2900 是 U2980、U2990 的统称。U2900 网元下挂接了两种子网元，分别是 CDE（Common Desktop Environment）和 UAP。添加 U2900 网元时，eSight 会自动添加 CDE 和 UAP 子网元。

设备面板管理

U2900 设备面板提供了一个直观的设备仿真界面，设备面板的功能包括：

- 查看单板的实时状态
- 切换前/后插板的仿真面板
- 查看 CIU（Circuit Interface Unit）单板的时序状态

图4-58 U2900 设备面板



4.2.4.1.3 EGW 管理

eSight 支持的 EGW 管理功能包括：配置管理、维护管理。

管理界面

图4-59 EGW 管理界面

配置管理

- 基本配置
  查看设备基本信息、配置文件加载、设备重启等。
- LAN 配置
  LAN 基本配置、防火墙配置、DHCP 配置。
- 语音配置
  SIP 服务器配置、FXO 出局字冠配置、数据同步服务器配置。

维护管理

eSight 支持批量升级 EGW。用户可以选择立即升级或定时升级。

4.2.4.1.4 IAD 管理

eSight 支持的 IAD 管理功能包括：配置管理、维护管理。

管理界面

图4-60 IAD 管理界面

配置管理

说明
不同协议、不同型号的 IAD，支持的功能有部分差异，以下所列为 eSight 支持 IAD 管理的所有功能，具体型号的 IAD 设备所支持的功能请参见《eSight 规格清单》。

- 单个配置
  - 基本配置

    包括网络参数配置、网管配置、设备时间配置。
  - 高级配置

    包括协议切换、Trap 开关配置、端口锁定告警时长配置。
  - 业务配置

    包传真参数配置、DTMF 收号方式配、MGC 配置等。
  - 系统工具

    包括版本信息查询、端口统计、保存配置、恢复配置、设备重启、国家码查询等。
- 批量配置
  - 网络参数配置
  - 代理服务器配置
  - 网管配置
  - 读写团体配置
  - 保存配置

维护管理

- 设备升级
  - 手动升级

    手动升级包括 CPLD 版本升级（只适用于 IAD132E(T) 设备）和主机软件升级。eSight 支持批量升级 IAD。用户可以选择立即升级或定时升级。
  - 自动升级

    启动自动升级功能后，IAD 能定时检测 FTP 服务器上的升级文件，如果检测到升级文件和现有版本不匹配，则执行自动升级。
- 备份与还原

  eSight 可以将 IAD 配置数据或者 SIP 用户信息备份至 eSight 文件服务器上，或者将 eSight 文件服务器上的数据还原至 IAD，还可以将数据保存至本地计算机。
- Ping 测试

通过 Ping 命令，测试 IAD 设备与其他设备的连通性。

4.2.4.1.5 UAP3300 管理

eSight 支持的 UAP3300 的业务管理功能。

管理界面

图4-61 UAP3300 管理界面

业务管理

- 设备信息

  通过 eSight 可以查看 UAP3300 的基本信息、License 信息、版本信息、补丁信息。
- Ping 测试

  通过 Ping 命令，测试 UAP3300 设备与其他设备的连通性。
- 补丁管理

通过 eSight 可以查看、加载、激活、去激活、保存和删除补丁。

4.2.4.2 终端设备管理

eSight 支持对终端设备进行管理，包括 IP Phone、AT 设备。

4.2.4.2.1 IP Phone 管理

eSight 支持的 IP Phone 管理功能包括创建 IP Phone 子网、自动部署、设备管理、配置管理、业务管理和证书管理。

说明
不同型号的 IP Phone，支持的功能有部分差异，以下所列为 eSight 支持 IP Phone 管理的所有功能，

创建 IP Phone 子网

创建 IP Phone 子网，将所属 IP 地址范围的 IP Phone 统一管理起来，可以关联到配置文件，便于配置文件的批量下发。

自动部署

- 自动归集 IP Phone 到指定子网

  用户在 eSight 中创建 IP Phone 子网。当 IP Phone 初始注册到 eSight 时，eSight 自动添加 IP Phone 到相应子网中。当 IP Phone 的 IP 地址变更时，eSight 自动将 IP Phone 移动到对应 IP 地址范围的子网中。

- 自动下发配置文件

  创建子网后，用户可以为每个子网分别创建配置文件。当 IP Phone 被添加至子网中时，eSight 自动向 IP Phone 下发子网对应的配置文件。

- 自动升级版本文件

  在 eSight 中上传 IP Phone 的版本文件后，通过自动部署添加至 eSight 的 IP Phone 将自动与 eSight 中版本文件的版本号进行比较，如果不匹配，则自动升级 IP Phone 版本文件。

- 查询未匹配子网的 IP Phone

  通过查询未匹配子网的 IP Phone，用户可以发现有哪些 IP Phone 的 IP 地址不包含在当前 IP Phone 子网的 IP 地址范围中，后续通过增加 IP Phone 子网或者修改原有 IP Phone 子网的 IP 地址范围，将这些 IP Phone 添加至相应的 IP Phone 子网中。

配置管理

配置管理包括批量对 IP Phone 进行设备重启。

设备管理

eSight 支持对 IP Phone 进行“设备重启”、“Web 页面管理”等功能。

图4-62 IP Phone 设备管理界面

业务管理

- 升级管理

  eSight 支持立即或者定时批量升级 eSpace 6800 系列 IP Phone、eSpace 7800 系列 IP Phone 和 eSpace 8850 系列 IP Phone 的主程序，eSpace 7900 系列 IP Phone 的主程序、语言包、字库、证书文件和信号音。

  上传目标版本文件和配置文件，对 IP Phone 的版本文件和配置文件进行批量升级。

  说明

  IP Phone 的版本文件存放在文件服务器上，使用 eSight 内置的文件服务器。

- 接入扫描

  当大量 IP Phone 接入 eSight 时，通过接入扫描功能向 IP Phone 发送 ACS 地址和证书路径等信息。IP Phone 自动修改配置后，自动接入对应的 IP Phone 子网。

注意

支持的 IP Phone 型号为 eSpace 7910 和 eSpace 7950，并且版本必须是 V100R001C02 及以上。

- 语音质量管理

  通过终端语音质量功能评估 IP Phone 的通话语音质量，并通过报表形式展现出来，便于定位和排查现场故障。

- 未匹配子网的 IP Phone 管理

  如果添加的 IP Phone 的 IP 地址不在各个 IP Phone 子网管理 IP 网管的范围，则该 IP Phone 自动进入“未匹配子网的设备”，可以修改子网管理的 IP 地址范围或者创建新的子网，将 IP Phone 添加到对应的子网中。

证书管理

由于证书更新或者现场客户要求使用客户的证书，需要进行证书管理操作，使得 IP Phone 可以和 eSight 通过鉴权。

4.2.4.2.2 AT 管理

eSight 支持对 AT 进行自动部署、批量配置和维护管理。

管理界面

图4-63 AT 管理界面

自动部署

- 自动归集 AT 到指定子网

  用户在 eSight 中创建 AT 子网。当 AT 初始注册到 eSight 时，eSight 自动添加 AT 至相应子网中。当 AT 的 IP 地址变更后，eSight 自动将 AT 移动到对应 IP 范围的子网中。

- 查询未匹配子网的 AT

  通过查询未匹配子网的 AT，用户可以发现有哪些 AT 的 IP 地址不包含在当前 AT 子网的 IP 范围中，后续通过增加 AT 子网或修改原有 AT 子网的 IP 范围，将这些 AT 添加至相应的 AT 子网中。

配置管理

- 批量导出 AT 物理序列号

  申请 AT 网元的 License 时，需要提供 AT 网元的物理序列号。用户可以通过 eSight 批量导出 AT 网元的物理序列号，以便用户批量申请 AT 的 License。

- 批量加载 AT 的 License 文件

  申请并获取 AT 的 License 文件后，用户可以通过 eSight 批量加载 AT 的 License。

- License 文件加载记录

  查看 AT 的 License 文件的历史加载记录。

- 导出主机信息

  单个或者批量导出 AT 网元的主机信息，以便用户安装 AT 的业务软件。

维护管理

通过 eSight，可以对 AT 设备进行重启、关机等操作。

4.2.4.3 统一通信应用管理

eSight 支持对 eSpace 统一通信应用进行管理，主要包括配置管理、日志管理、业务跟踪及单点登录。

管理界面

图4-64 统一通信应用管理界面（AA）

可管理设备

- BMP 应用

  BMP 对 eSpace 统一通信客户端提供统一的业务管理平台，支持多种业务组合。企业管理员登录后，可进行企业信息维护、企业成员开销户等操作。

- Portal 应用

  Portal 是企业用户的个人业务门户，提供给企业内已经开通 eSpace UC 帐号的成员使用。eSpace UC 用户可以登录 Portal 界面，维护个人信息，设置来电免打扰、呼叫转移、经理秘书等业务功能。

- AA 应用

  AA 负责 eSpace Desktop（eSpace PC 客户端）的接入和鉴权。eSpace Desktop 从 AA 上获取登录信息，并通过调用 AA 接口，使用呼叫、即时消息、会议等业务能力。

- OBG 应用

  OBG 对外提供业务开放集成平台，支持与企业 IT 系统、企业 SNS（Social Networking Site）系统和互联网系统对接集成。

- Call AS 应用

  Call AS 提供业务呼叫控制、业务处理能力，是 eSpace UC 核心能力部件。

- PGM 应用

  PGM 提供 Presence、Message、Group 能力，与统一通信软终端配合提供如下功能：

  - 状态呈现：企业用户状态呈现在 eSpace Desktop、eSpace Mobile、eSpace Mobile HD 等界面上，用户可以实时查看相关联系人状态，并根据联系人状态选择合适的方式沟通。
  - 即时消息：企业用户之间可以发起点对点即时消息、讨论组即时消息和固定群即时消息。

- 企业通讯录：企业通讯录用于存放部门和员工的通讯信息，企业管理员在 BMP 上管理和维护企业通讯录信息。
- 个人通讯录：个人通讯录用来保存用户的联系人信息，用户可在统一通信软终端上管理和维护联系人信息。

- Meeting AS 应用

  Meeting AS 作为会议控制服务器，提供会议控制和管理功能。

- Meeting MS 应用

  Meeting MS 作为视频/数据会议应用服务器，提供多媒体会议能力，包括视频、屏幕共享、文件传输、电子白板、文字交流等丰富的会议协同功能。

- TCPAdapter 应用

  TCPAdapter 是处理移动终端业务模块，负责和移动终端保持会话，处理移动终端的 TCP 消息。

配置管理

eSight 支持对 AA、OBG、Call AS、PGM 应用进行配置管理，包括数据库配置、业务配置、系统配置等。

业务跟踪

eSight 支持对 AA、OBG、Call AS、PGM 等模块间消息传送进行跟踪，从而了解各应用的消息传递和通信情况，帮助定位和分析故障。

日志管理

eSight 提供对 BMP 应用的日志管理，包括安全日志、操作日志的查询及下载。

单点登录

eSight 支持单点登录功能，通过 BMP 系统无需再次安全验证，可以直接登录 eSight。

4.2.4.4 会议系统应用管理

eSight 支持对 eSpace 会议系统进行配置管理。

管理界面

图4-65 会议系统管理界面（eConf AS）

可管理设备

- eConf AS

  eConf AS 作为 eSpace 会议系统的核心组件，提供会议系统内部资源的控制和交互功能，其集合了会议业务管理、会议系统级联和交互网关对接、 License 读取、话单记录和统一对外接口功能于一体。

- eConf Portal

  eConf Portal 为企业用户提供创建即时会议、创建延时会议、管理已创建的会议等功能。用户在创建会议时，可设置会议主题、会议时长、与会者等各种会议信息。用户可创建语音会议以及多媒体会议。

- Media Server

  Media Server 作为会议服务器，为 eSpace 会议系统提供多媒体会议功能，并提供包括视频、屏幕共享、文件传输、电子白板、文字交流等丰富的会议协同功能。

4.2.4.5 联络中心应用管理

eSight 支持对 eSpace CC 解决方案（联络中心解决方案）进行管理，主要提供故障定位和告警信息管理。

管理界面

图4-66 联络中心解决方案应用管理界面（Agent）

可管理设备

- Agent 应用

Agent 是基于华为呼叫中心平台开发的综合呼叫处理系统。他可以为拥有华为呼叫中心平台的企业提供座席服务，为企业的业务代表提供呼叫处理、录音文件管理和实时监控来话等功能。

- HPS 应用

  HPS 是一款面向外呼服务业务的产品，能够帮助企业有效提升座席操作效率和运营效率，降低客户流失和 OPEX （Operating Expense），提高服务质量和客户满意度。

- CMS 应用

  CMS 配套 eSpace CC 解决方案，主要提供质检功能和监控功能。

- ICS 应用

  ICS 是基于华为呼叫中心平台开发的社交媒体服务系统。它可以在海量的微博信息中，收集到企业关心的信息（通过搜索关键字），并将微博信息存放在 ICS 系统中，供企业业务代表解答和处理。

- BIR 应用

  BIR 报表系统是一个 B/S（Browser/Server）结构的系统，提供了基于 Web 的报表生成、分发、管理的一整套灵活方便的报表应用服务。报表系统不仅支持生成手工报表和周期报表，还拥有完善的报表分发机制，具有强大的数据采集能力。

- Intelligent Scripting 应用

  Intelligent Scripting 是问卷系统，用户可以使用 SDT 组件做问卷设计，发布到问卷服务器后，问卷就可以被访问了。Intelligent Scripting 可以和坐席集成，有热线呼入时，系统弹出对应的问卷给坐席，指导坐席进行问卷调查。

- OBG 应用

  OBG 对外提供业务开放集成平台，支持与企业 IT 系统、企业 SNS （Social Networking Site）系统和互联网系统对接集成。

4.2.4.6 远程银行设备管理

eSight 支持对 eSpace VTM 远程银行解决方案的 VTM Manager 和 VTM 设备进行管理，主要包括故障定位和告警信息的管理。

可管理设备

- VTM Manager

  VTM Manager 是 VTC（Virtual Teller Center）的部件之一，用于远程监控、维护和管理 VTM 终端，提供状态监控信息，VTM 终端服务报表信息等。

- VTC

  即虚拟柜员中心，包含 MCC 和 MCMS，用于处理远程银行虚拟柜台业务。MCC 为媒体控制中心，提供呼叫接续控制接口，信息接口（包括银行帐号权限和呼叫信息等）； MCMS 为监控和质检服务的平台，提供监控、质检和管理功能。

4.2.4.7 UC 外围设备管理

eSight 支持对 SBC（SX1000）、VCLOG、Movius（Movius Interactive Corporation 注册商标） UMS 及 GS8 的管理，主要包括配置管理和升级管理。

管理界面

图4-67 外购件管理界面（SBC）

配置管理

eSight 支持对 SBC 进行系统配置、网络配置及路由配置，还可以单个或者批量重启设备。

升级管理

eSight 支持批量升级 SBC 设备。用户可以选择立即升级或定时升级。

4.2.4.8 语音质量监控

eSight 支持监控网关和终端设备的语音质量，支持阈值告警。

了解语音质量监控

语音质量监控包括：

- 网关语音质量监控

  可监控如下设备：eSpace U1980、eSpace U1960、eSpace U1930、eSpace U1910、SoftCo9500、SoftCo5500 和 IAD1224。

- 终端语音质量监控

  可监控如下设备：eSpace Desktop、eSpace 7910 和 eSpace 7950。

监控网关语音质量

网关语音质量监控的功能包括：

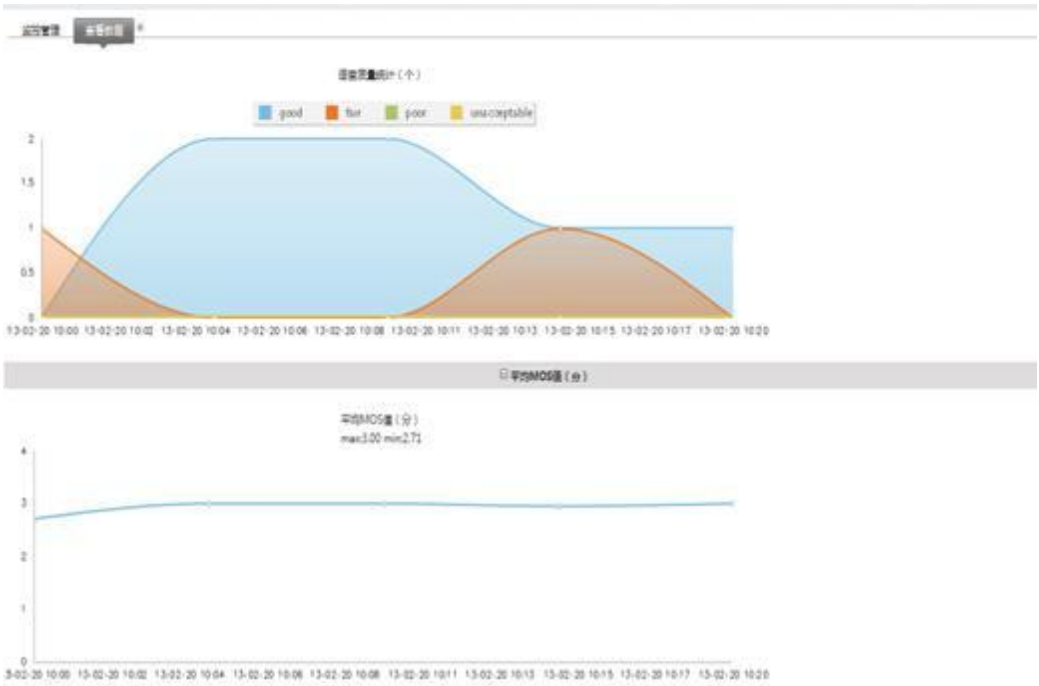
- 监控管理

  用户配置监控的子网或网元、监控任务的起始时间和结束时间、数据的采集周期。eSight 将配置的数据下发至相应的网元，网元上报 QoS 数据给 eSight。

- 查看数据

  eSight 提供了详细数据、报表数据、报表视图三种方式，查看语音质量、MOS（Mean Opinion Score）值、时延、抖动、丢包率等。支持按主被叫区域、主被叫设备、主被叫号码和时间范围搜索数据。

图4-68 网关数据报表视图



- 抽样数据

  eSight 支持查看最大 MOS 值和最小 MOS 值的主被叫用户、最大时延和最小时延的主被叫用户、最大抖动和最小抖动的主被叫用户、最大丢包率和最小丢包率的主被叫用户。

- 导出图表

  eSight 支持导出报表数据和报表视图，以便后期查看或审计。

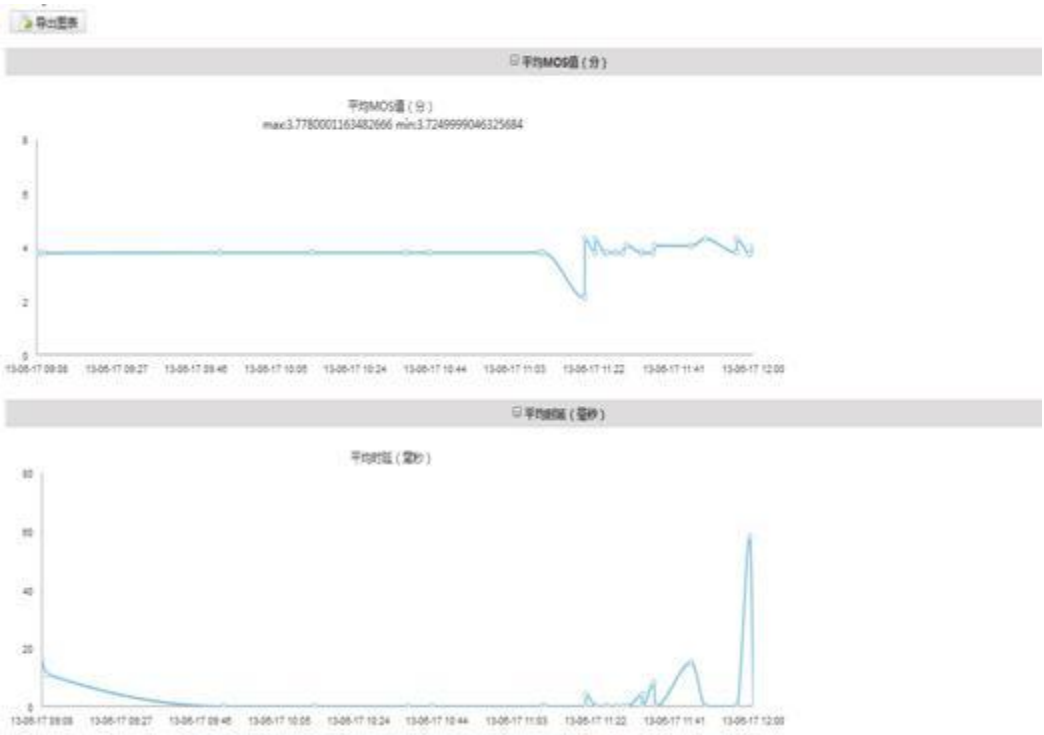
监控终端语音质量

终端语音质量监控的功能包括：

- 查看数据

  eSight 提供了详细数据和报表视图两种方式，查看 MOS 值、时延、抖动、丢包率等。支持按主被叫区域、主被叫号码和时间范围搜索数据。

图4-69 终端数据报表视图



- 抽样数据

  eSight 支持查看最大 MOS 值和最小 MOS 值的主被叫用户、最大时延和最小时延的主被叫用户、最大抖动和最小抖动的主被叫用户、最大丢包率和最小丢包率的主被叫用户。

- 导出图表

  eSight 支持导出报表数据和报表视图，以便后期查看或审计。

设置告警阈值

设置告警的产生条件、恢复条件和重复次数。当 MOS 值连续 n 次超过告警阈值时，eSight 自动产生告警。

图4-70 设置告警阈值

4.2.4.9 证书管理

eSight 支持 TLS（Transport Layer Security，安全传输层协议）证书管理，满足系统运行中网络设备证书变更需求。

eSight 提供证书上传及设备重启功能，能将 TLS 证书上传到文件服务器和 eSight 自带的 SFTP 服务器，设备能够从文件服务器和 SFTP 服务器获取到更新后的证书。

说明
建议在安装完 eSight 之后，将默认证书和公私钥对替换为企业客户提供的证书和公私钥对。

TLS 证书管理支持的设备包括 eSpace U19 系列、IAD、EGW、IP Phone 79 系列、U29 系列、eSpace 客户端等多款设备，具体支持设备型号请参见《eSight 规格清单》。

4.2.4.10 设备信息导出

eSight 支持将网管中的物理设备信息导出为 csv 或者 xls 格式。内容包括设备的名称、类型、IP 地址、版本信息、型号和描述信息。

4.2.5 视频监控管理

视频监控管理提供了对视频监控业务资源的发现、业务拓扑、性能和数据分析的管理，能有效提升视频监控设备管理的质量和效率。用户通过对业务的性能、告警、等多种监控手段，监控当前业务的运行状况，快速定位业务故障。

说明
视频监控管理功能需要安装 eSight 视频监控设备管理组件。

4.2.5.1 视频监控应用管理

eSight 支持对 eSpace IVS 解决方案和 eSpace CAD 解决方案进行管理，主要提供故障管理和配置管理。

管理界面

图4-71 视频监控解决方案应用管理界面（MAU）

可管理设备

- eSpace IVS 解决方案
  - MAU：智能分析的主控单元，提供智能分析的任务管理、规则管理、负载均衡。
  - MBU：媒体备份单元。
  - MPU：媒体处理单元。
  - MTU：媒体转码单元，负责媒体数据的重新编码和分发。
  - TAU：终端接入单元。
  - VMU：视频管理单元。
  - 前端设备：视频采集设备。
- eSpace CAD 解决方案
  - CAD Appserver：CAD 应用服务器
  - AAG：非话务报警网关
  - DAG：数据交换网关
  - mPortal：管理 Portal
  - KBS：知识库
  - SNS：二级处警子系统

配置管理

eSight 支持视频监控各应用模块配置文件的配置，通过 UOA 的配置接口进行转发，实现各模块与 eSight 的数据同步。

eSpace IVS 解决方案的应用模块包括：OMU、DCG、SCU、MU、PCG、MAUS 和 SMU，模块具体信息请参见《eSpace IVS 产品文档》。

eSpace CAD 解决方案的应用模块包括：CAD Appserver、AAG、DAG、KBS 和 SNS，模块具体信息请参见《eSpace CAD 产品文档》。

业务跟踪

eSight 支持对视频监控应用进行跟踪，包括前端注册/注销跟踪、实时浏览跟踪、录像下载跟踪、录像回放跟踪、实时录像跟踪等，另外，还提供跟踪文件的备份、删除、检索、下载等操作。

4.2.5.2 视频监控数据分析

eSight 通过查询一段时间内设备在线率、离线率、设备故障率等信息生成报表，支持周期报表任务、即时报表任务；支持报表导出为 EXCEL 文件格式。eSight 满足常见的网络运维报表需求，为设备的信息统计提供数据依据。

数据分析管理

用户可以在数据分析管理界面中，创建和管理所有的报表任务。

报表任务分为即时任务和周期任务两种。

- 即时任务

  即时任务，需要用户手工执行，反映的是即时的统计结果。任务执行成功后，用户单击“查看报表详情”，可以打开生成的报表。用户在查看生成的报表时，可以将报表以指定的格式导出。

- 周期任务

  周期任务，系统会按照用户指定的运行周期执行，反映的是一个周期内的统计结果。任务执行成功后，会将生成的报表保存下来。用户可以管理和查看某个周期任务生成的所有报表。

图4-72 数据分析管理示意图

4.2.6 智真会议管理

智真会议管理提供了对智真会议资源的发现、业务拓扑的端到端管理功能，能有效提升智真会议设备管理的质量和效率。用户通过对业务的告警等多种监控手段，监控当前业务的运行状况，快速定位业务故障。

说明
智真会议管理功能需要安装 eSight 智真设备管理组件。

4.2.6.1 智真会议设备管理

eSight 支持对智真会议设备进行管理，主要提供故障定位和告警信息的管理。

管理界面

图4-73 智真会议设备管理界面（VCT）

可管理设备

- 终端设备

  智真会议终端设备是一种能够将视音频信号进行编码与解码的设备。

- MCU 设备

  MCU （Multipoint Control Unit）是视/音频通信中的多点控制单元，用于对各点视讯终端送来的音频、视频和数据等信息的混合和交换。

- TP 设备

  TP 是华为公司的远程呈现系统，使用高清视频编解码技术，支持真人大小图像的远程呈现、全方位的声像同位，能够为用户提供舒适的会议室环境，让用户拥有面对面的远程会议体验。

- GK 设备

  GK 是智真会议系统的核心组件之一，处于网络控制层中，主要功能是对节点进行管理，节点类型包括终端、MCU、网关。GK 对节点的管理包括地址解析、区域管理、接入控制、注册管理、呼叫管理、带宽管理、路由管理。

配置查询

通过 eSight 可以查询 MCU、TP 及终端设备的配置信息，避免逐个登录设备查询配置的操作。

4.2.6.2 智真会议网络诊断

eSight 支持对智真会议系统中的交换机和路由器进行数据收集，由 eSight 计算和处理后，将结果呈现在 eSight 客户端上，以帮助管理员了解智真会议系统的设备状态和网络状况。

连接配置

eSight 可以对 SMC 的网络连接进行配置管理，实现智真会议系统的网络诊断功能。

会议管理

eSight 支持从 SMC 设备获取会议信息，呈现在 eSight 客户端上，供管理员查看。

网络诊断

会议诊断分为会议前诊断和会议中诊断：

- 会议前诊断

  选择任意两个已经预约的会场，对会场对应的 MCU 设备进行网络诊断。
- 会议中诊断

  SMC 设备通过 MCU 设备获取 MCU 设备的相关参数，eSight 从 SMC 设备获取会议和媒体流信息，同时对路由路径中的交换机和路由器进行数据统计。

网络路径管理

eSight 支持从 MCU 设备获取路由路径，从而获取路由路径上支持网络诊断的交换机和路由器设备。

4.2.7 eLTE 设备管理

eLTE CPE 管理功能包括：自动部署、升级管理、配置管理、维护管理。

CPE 管理界面

CPE 管理界面为管理 CPE 设备提供一个统一入口，包含以下功能：

- 终端基本信息

  查看 CPE 的基本信息，支持刷新更新。
- 终端通用配置

  通过 TR069 的数据模型树，实现对参数的修改。
- Web 页面跳转

  用户可以通过 Web 页面跳转功能直接跳转到 CPE 的 Web 管理页面。
- 配置文件导出

  用户可以用该功能导出、下载备份 CPE 的配置文件。
- 配置文件加载

  用户可以选择配置文件，加载到 CPE，实现 CPE 使用指定配置文件的目的。

自动部署

- 自动归集 CPE 到指定子网

  用户在 eSight 中创建 CPE 子网。当 CPE 初始注册到 eSight 时，根据终端合法清单的配置，自动添加 CPE 到相应子网中。

- 自动下发配置文件

  创建 CPE 子网后，用户可以为每个子网分别创建配置文件。当 CPE 被添加到子网中时，eSight 自动向 CPE 下发子网对应的配置文件。

- 自动升级版本文件

  用户上传 CPE 的固件版本文件，自动部署查询 CPE 的固件版本，与用户配置上传的目标版本进行比较，如果不匹配，则自动升级 CPE 固件。

批量加载配置文件

支持用户批量选择 CPE，下载指定的配置文件。

批量升级

支持立即或者定时批量升级 CPE 固件版本。

远程维护

用户可以远程重启 CPE，将 CPE 的配置恢复到出厂配置，使用 Ping 检测连通性。

4.3 业务管理

4.3.1 网络报表管理

eSight 通过任务执行报表生成，支持周期报表任务、即时报表任务；支持报表导出为 PDF、Excel、Word 等常见文件格式。eSight 预集成了丰富的报表模板，可以满足常见的网络运维报表需求；同时支持用户自定制的报表模板，以实现个性化的报表需求。

报表任务管理

用户可以在报表任务管理界面中，创建和管理所有的报表任务。

报表任务分为即时任务和周期任务两种。用户可以在任务中设置 Email 转发相关信息，在任务执行成功后，eSight 会将生成的报表通过 Email 发送给指定的收件人。

- 即时任务

  即时任务，需要用户手工执行，反映的是即时的统计结果。任务执行成功后，用户单击“查看报表”，即打开生成的报表。用户在查看生成的报表时，可以将报表以指定的格式导出。

- 周期任务

  周期任务，系统会按照用户指定的运行周期执行，反映的是一个周期内的统计结果。任务执行成功后，会将生成的报表保存下来。用户可以管理和查看某个周期

任务生成的所有报表。用户可以将所生成的报表批量导出、删除或通过 Email 发送。

图4-74 报表任务管理示意图

自定义报表

eSight 支持用户上传和运行自定制的报表模板。

用户可根据自身的需求，通过开源的报表设计工具 Birt，设计符合自己需要的报表设计文件。用户可以将设计好的设计文件上传到 eSight 中使用。

4.3.2 存储报表管理

存储报表管理通过提供长时间的存储设备性能和容量分析报表，帮助用户进行性能瓶颈分析以及容量使用规划。

预置报表

预置的性能与容量报表，方便用户快速、定期查看存储系统的性能。存储系统级别的性能概况，报告 LUN/端口/控制器/文件系统等最近 24 小时、7 天、30 天的性能概况。对象级别的性能详情，对硬盘、端口、CPU、LUN、文件系统等对象，报告最近 24 小时、7 天、30 天的性能详情，并按照 IOPS（Input And Output Operations Per Second）/带宽/时延等维度进行排序，报告需要查看的硬盘/端口/CPU/LUN/文件系统信息。对文件系统、存储池、精简 LUN 等对象，报告最近 24 小时、7 天、30 天的容量利用率。

图4-75 预置报表

自定义报表

用户自定义的性能和容量报表，满足用户对性能与容量报告的定制化需求。存储系统的性能概况，自定义报告 LUN/控制器/端口/硬盘等过去一段时间的整体性能概况。对象级别的性能详情，自定义报告端口、控制器、LUN、磁盘、CPU、文件系统、存储池等对象一段时间的性能详情。存储系统及对象级别的容量利用报告，自定义报告存储系统、文件系统、存储池、Thin LUN 等对象一段时间的容量利用状况。

任务报表

利用自定义报表、辅助周期执行策略，定期执行用户关心的性能与容量报表。报表执行结果自动发送到指定管理员。

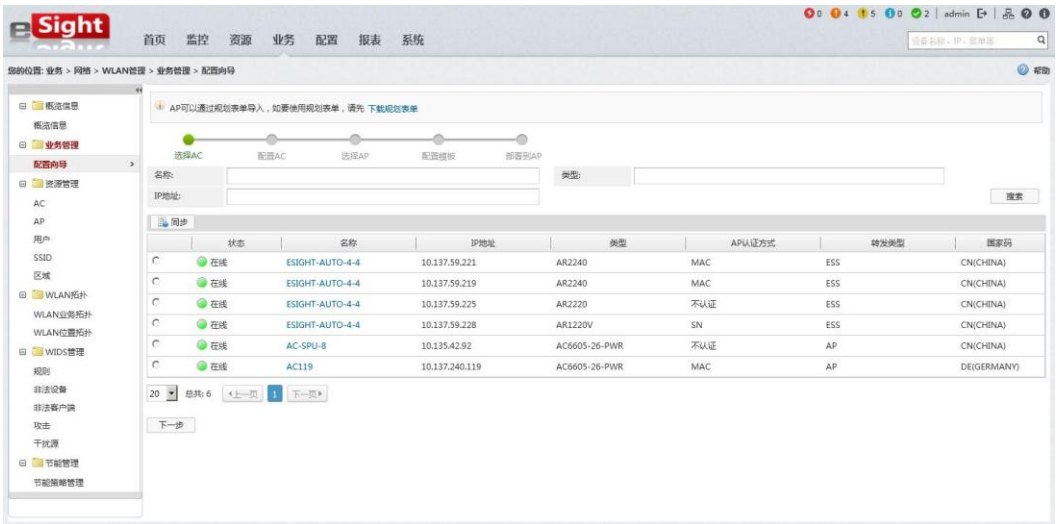
4.3.3 WLAN 管理

eSight WLAN 通过业务部署，端到端、批量、快速地完成无线业务部署；通过业务监控帮助用户准确、快速了解当前无线网络质量和网络设备资源分配及负载情况；通过业务调整为用户网络扩容、调整及合理利用、分配设备资源；通过故障诊断帮助快速识别故障原因，找到故障点；同时提供故障处理手段，方便运维人员维护。

业务管理

提供向导式的业务配置，基于 AP 规划表单，端到端实现 AP 业务的统一下发与部署，大幅提升部署效率（相比手工部署效率提升约 90%）。

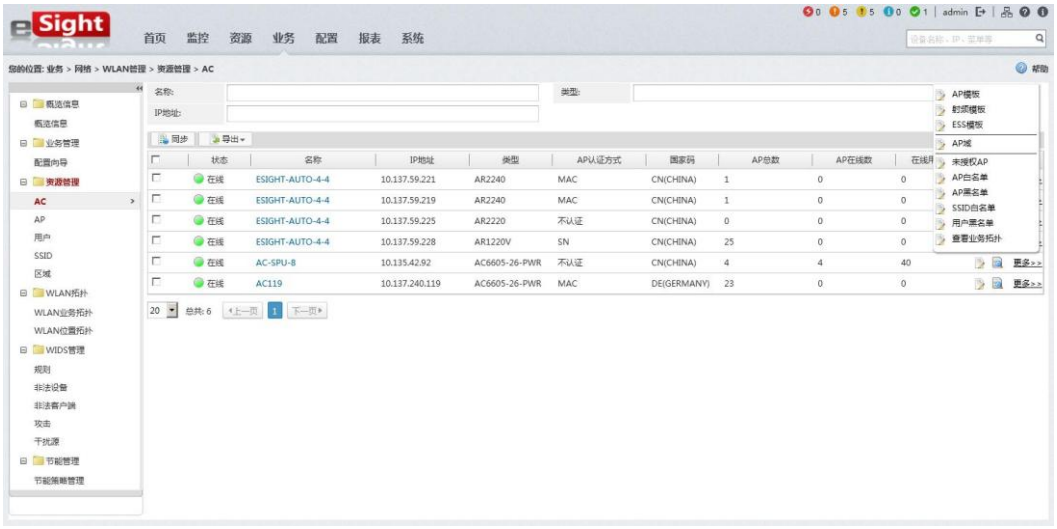
图4-76 AC 配置向导



配置管理

AC 管理界面如图 4-87 所示。

图4-77 AC 管理界面示意图



WLAN 管理，提供 WLAN 设备配置，通过在线确认（未授权 AP 上线）、离线部署（添加部署离线 AP）、自动上线（符合白名单的 AP 自动上线）三种形式，方便、快捷完成 AP 与 AC 互通配置。

- AC 基本信息

  无线控制器对无线局域网中的所有 AP 进行控制和管理。AC 管理提供源接口、AP 认证方式、转发类型、国家码等业务配置。

- AP

  AP 提供无线终端到局域网的桥接功能，进行无线到有线和有线到无线的帧转换。AP 管理提供 AP 基本信息配置、射频配置、模板绑定；支持预定义表单批量导入 AP、批量绑定模板；支持对 AP 重启、恢复出厂配置、替换、配置反制。

- AP 白名单

  网络管理员通过配置 AP 白名单确认合法 AP，完成 AP 上线。AP 白名单为合法 AP 的 MAC 或 SN 的列表。若 AC 的认证方式设置为 MAC 或 SN， 则当 AP 的 MAC 或 SN 在白名单中时，AP 自动上线。

- 未授权 AP

  当 AC 自动发现的 AP 对应的 MAC 或 SN 不在白名单中时，用户可在未授权 AP 列表界面查看当前 AC 自动发现的未授权 AP；同时，可通过批量方式在线确认，将 AP 加入白名单，实现 AP 上线。

- AP 域

  为了尽量减少 AP 参数调整的持续时间和影响范围，将 AP 划分成若干个域，将影响范围限定有这个域，减轻调整算法的开销。AP 域展示 ID、名称、布放类型、别名信息，并提供指定默认域、射频调优操作。

- AP 黑名单

  网络管理员通过配置 MAC 地址抑制 AP 上线。MAC 地址在 AP 黑名单中的 AP 无法上线。

- 用户黑名单

网络管理员通过配置 MAC 地址抑制无线用户接入。MAC 地址在用户黑名单中的用户无法关联 AP。同时，可将非法用户添加至用户黑名单并配置 AP 的反制模式为用户黑名单，发起对用户黑名单中设备的反制操作。

- SSID 白名单

  网络管理员通过配置 SSID 白名单过滤对非法设备的探测。将无线网络周围一直存在、对网络环境无影响的 SSID 信号添加至白名单以后，则不会被识别为非法设备。

模板管理，提供网元级的预定义模板配置。

- AP 模板

  通过 AP 模板指定 AP 上行太网接口最大传输单元及日志备份相关设置。

- 射频模板

  通过射频模板配置无线传输数据过程中需要抢占信道、射频类型、速率、功率等相关参数。

- ESS 模板

  服务集是一个业务参数集合（SSID 名称、业务 VLAN、数据转发 ESS 接口、接入最大用户数、WLAN 用户接入安全管理等）。当它被绑定到指定 AP 的指定射频上时，即将它所有的业务参数应用到无线业务功能实体 VAP（Virtual Access Point）上。

网络监控

提供全网物理资源、统计数据、性能数据、用户接入历史、频谱分析等相关信息查看。

- 物理资源

  AC：包括状态、名称、IP 地址、类型、AP 认证方式、转发类型、国家码、区域位置信息

  AP：包括状态、名称、别名、类别、类型、SN、MAC、IP 地址、反制开关、接入 AC 名称、所属域、布放位置、定位开关、区域位置信息

  用户：包括 MAC、IP 地址、用户名、接入 AC 名称、AP 名称、AP IP、认证方式、射频、SSID、区域位置信息

  SSID：包括 SSID、接入 AC 名称、接入 Fat AP 名称、ESS 模板名称信息

  区域：包括名称、状态信息

- 统计数据

  全网概览：包括用户在线趋势统计、Top 接入 SSID 用户统计、无线资源统计、WLAN 最新告警等，详细列表参见 4.1.10 首页视图展示。

  AC 统计：包括 AP 总数、AP 在线数、在线用户数；域总数、默认域名称；AC Top5 当前重要告警；用户在线趋势图（最近 1 小时、最近 24 小时、最近 7 天）。

  AP 统计：AP Top 告警、AP 性能统计指标。

  SSID 统计： AP 数量、VAP 数量、用户数量。

- 性能数据

  AP 关联终端、AP 物理资源、AP 流量、射频流量、用户流量、WIDS 攻击数量实时性能统计。

- 用户接入历史

  用户接入历史查询依赖 Linux 服务器的日志（syslog）接收功能，eSight 对日志做定　时解析，提取登录信息，并将日志信息批量入库，记录用户接入历史信息

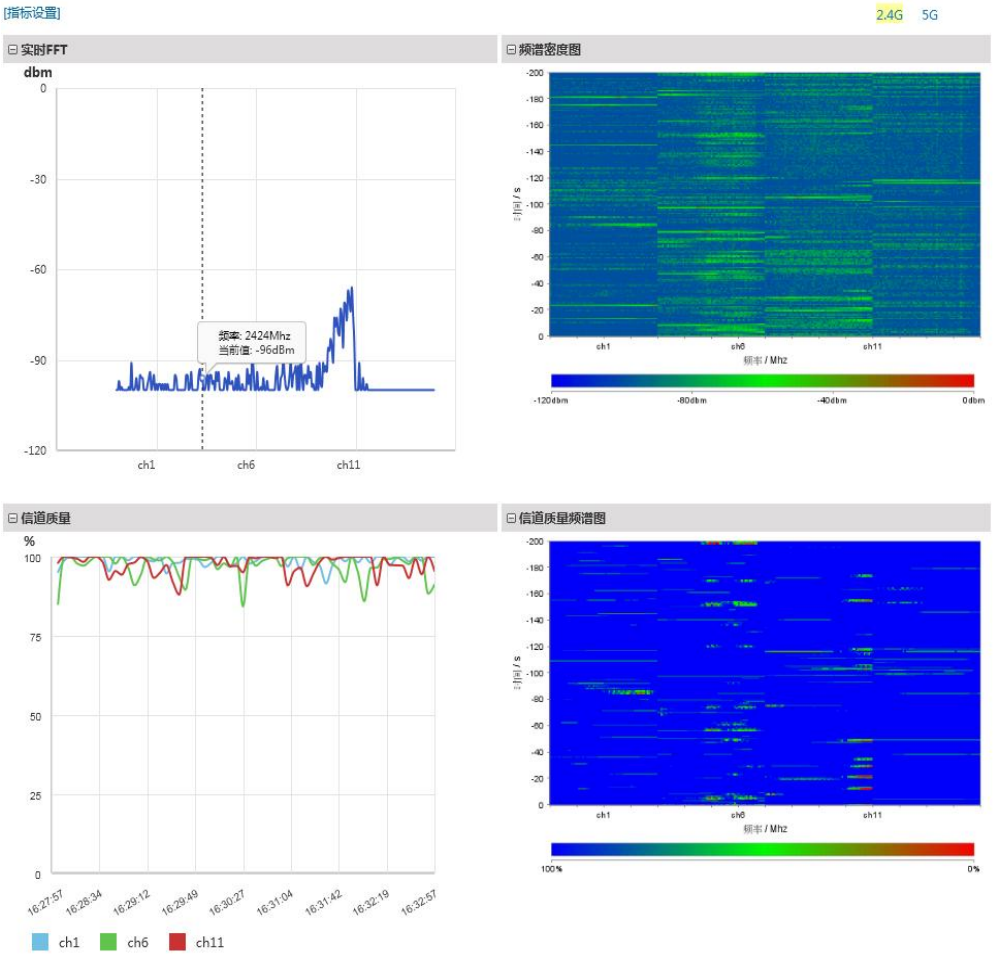
  说明

  仅在 Linux + Oracle 环境下，支持用户接入历史查询。

- 频谱分析

  在设备上使能 AP 射频的频谱功能后，在网管上可以查看 AP 周围的信号干扰情况，用户可从频谱图中识别信道质量以及周边环境的干扰源。频谱图包括信号实时图、深度图、信道质量图、信道质量趋势图、设备占空比。

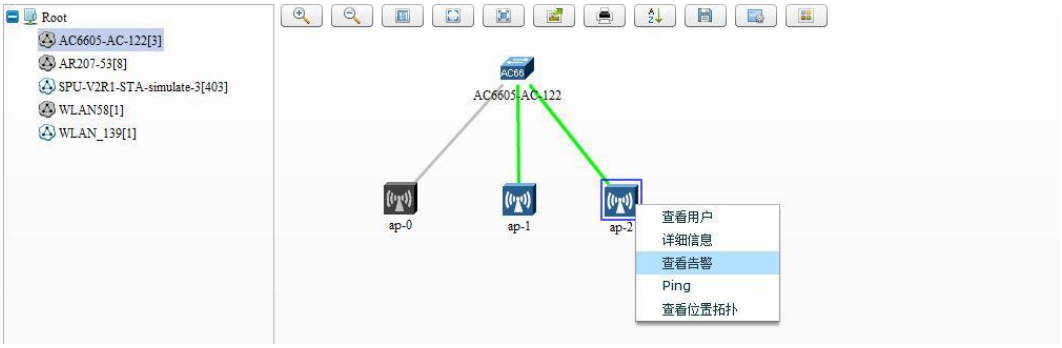
  图4-78 AP 频谱图



业务拓扑

提供可视化网络监控，以拓扑图方式显示 AC、AP、用户的业务逻辑关系， 并支持展示无线设备故障状态，同时提供告警查看的操作快捷入口。

图4-79 WLAN 业务拓扑界面

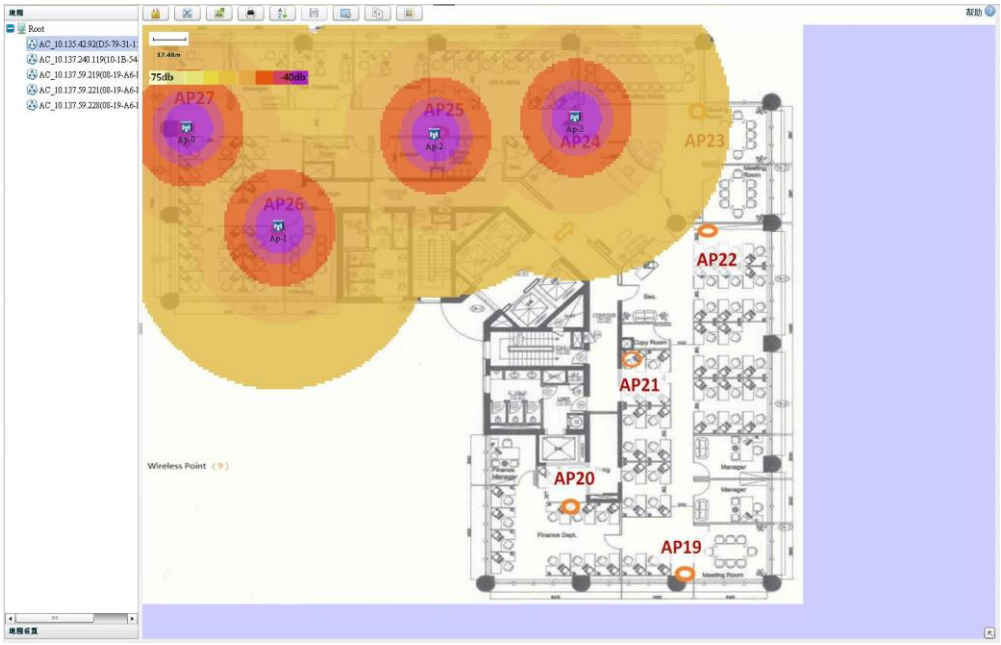


位置拓扑

位置拓扑支持依据物理位置按区域进行 AP 布放，热图覆盖可视化展现，帮助运维人员及时发现信号覆盖盲点与信道冲突域。对于具有定位 License 并使能定位的区域，拓扑刷新定位节点（用户、非法设备和非 WIFI 干扰源）的位置。

- 通过位置拓扑查看当前热点位置及射频信号覆盖范围，并标识冲突域。
- 添加预部署 AP，查看模拟的射频覆盖范围；AP 部署上线后切换真实 AP，显示 AP 的真实覆盖范围。

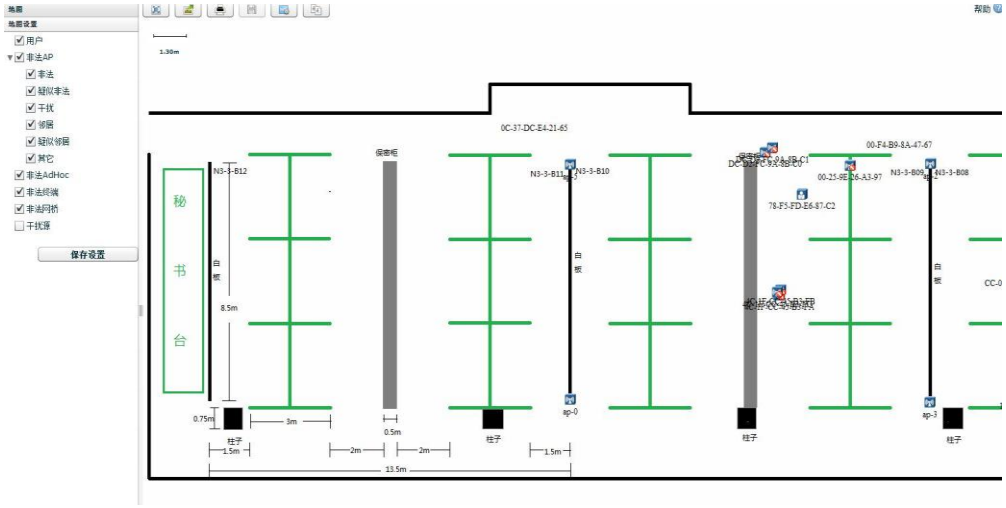
图4-80 WLAN 位置拓扑界面



- 地图设置：便于运维人员控制区域内节点的隐藏与显示。过滤项包括用户、非法 AP、非法用户、非法 Adhoc、非法网桥、干扰源；其中非法 AP 支持更细粒度的按照规则分类控制显示。

- 拓扑图中的用户、非法设备位置、干扰源位置在具备 AP 定位 license，并且该区域使能定位后，定位并刷新节点的最新坐标。

图4-81 位置拓扑定位显示

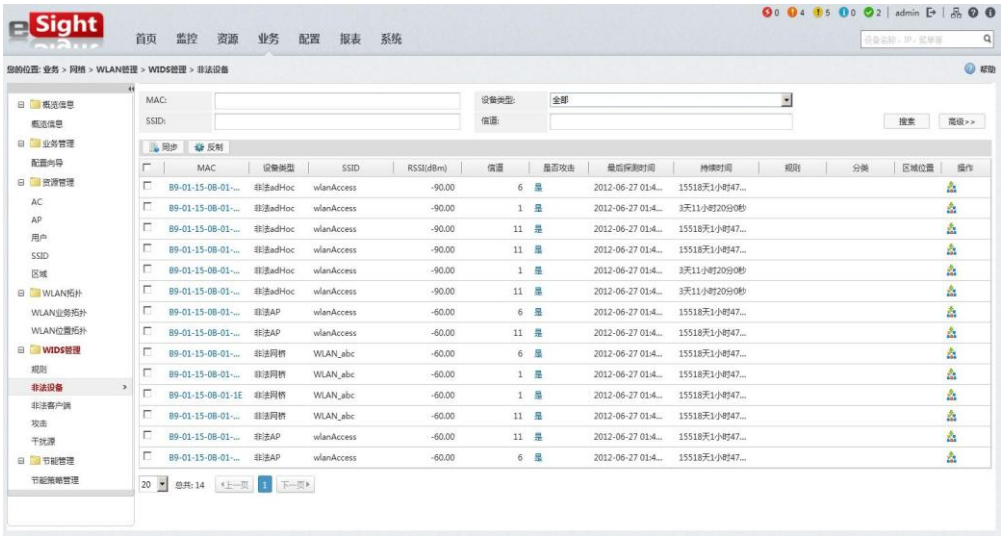


WIDS 管理

无线入侵检测（WIDS）管理，监控网络中存在的非法设备、非法客户端、干扰源、攻击信息，支持用户通过定义规则分类识别、远程告警通知并提供对入侵的保护措施。

- 支持非法设备的统计、展示和反制
- 支持非法客户端的展示、反制和抑制接入保护
- 支持非 WIFI 干扰源的统计和展示
- 支持攻击信息的统计、展示和保护
- 支持用户通过定义规则对非法 AP 进行分类，类别分为非法、疑似非法、邻居、疑似邻居、干扰。支持的规则匹配指标为：邻频同频干扰 、信号强度、 SSID（模糊匹配/正则表达式匹配）、探测 AP 数量、是否攻击

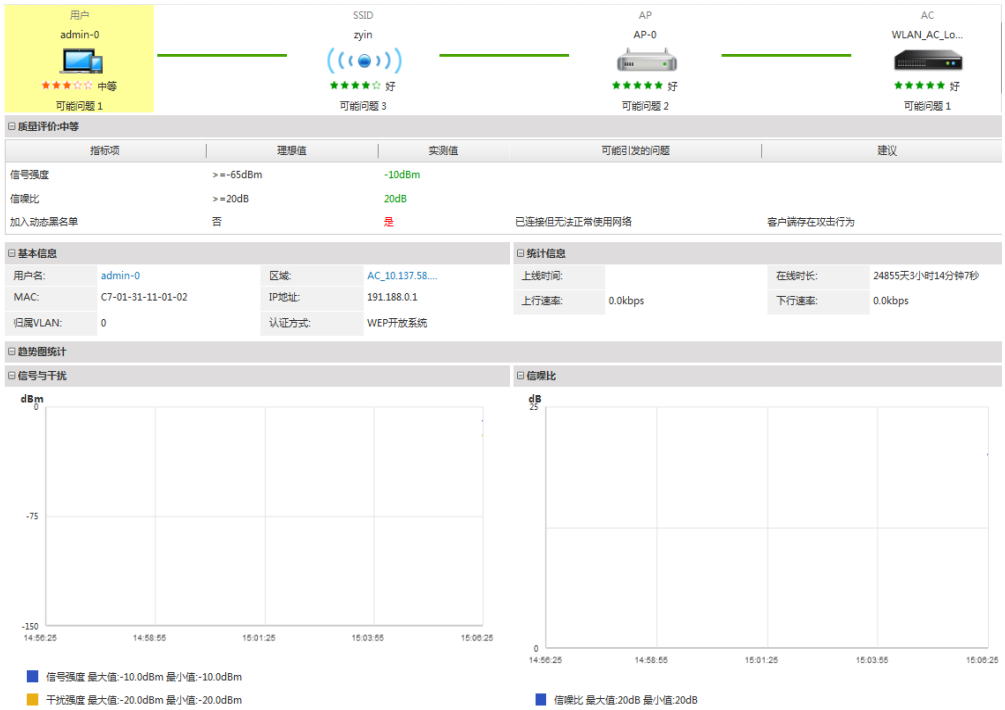
图4-82 非法设备列表



故障诊断

- WLAN 用户故障诊断：从用户、SSID、AP、AC 四个无线组网层面对在线用户的网络质量进行诊断。对于诊断出的异常问题，给出可能引发的问题与修复建议，指导用户排查故障。

图4-83 用户故障诊断

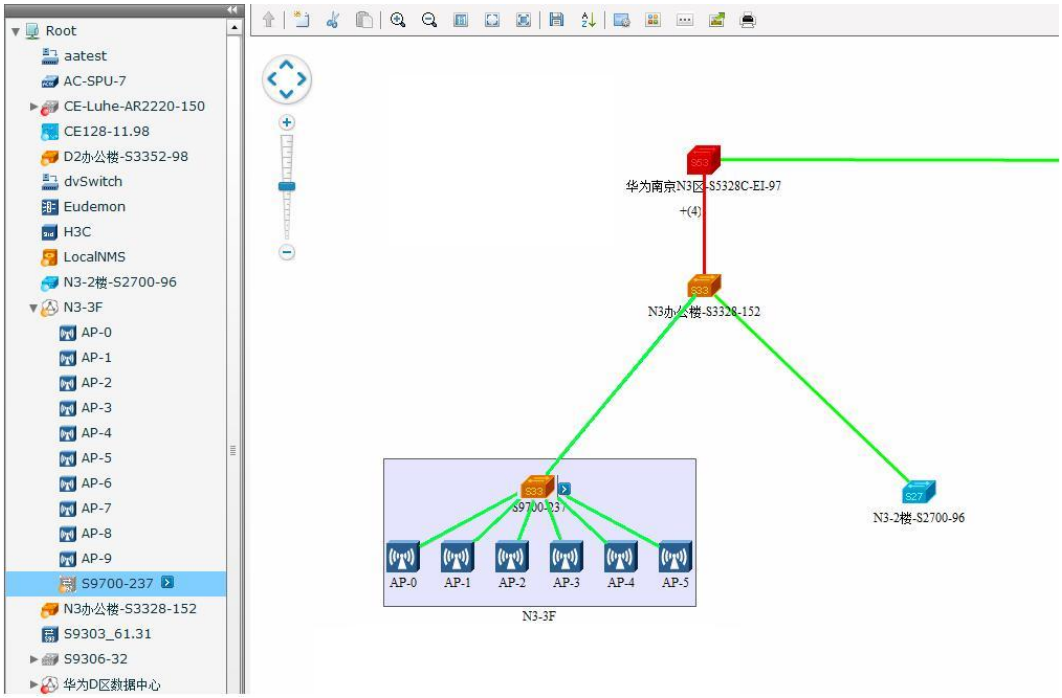


- 提供通讯、环境、非法设备、非 WIFI 干扰源、攻击等相关故障告警帮助用户故障点定位、解决。

有线无线一体化管理

在使能 AP 的 LLDP 链路发现后，用户在物理拓扑中，可以查看有线侧 POE 交换机与无线侧 AP 之间的链路，实现有线无线统一管理。

图4-84 物理拓扑管理界面



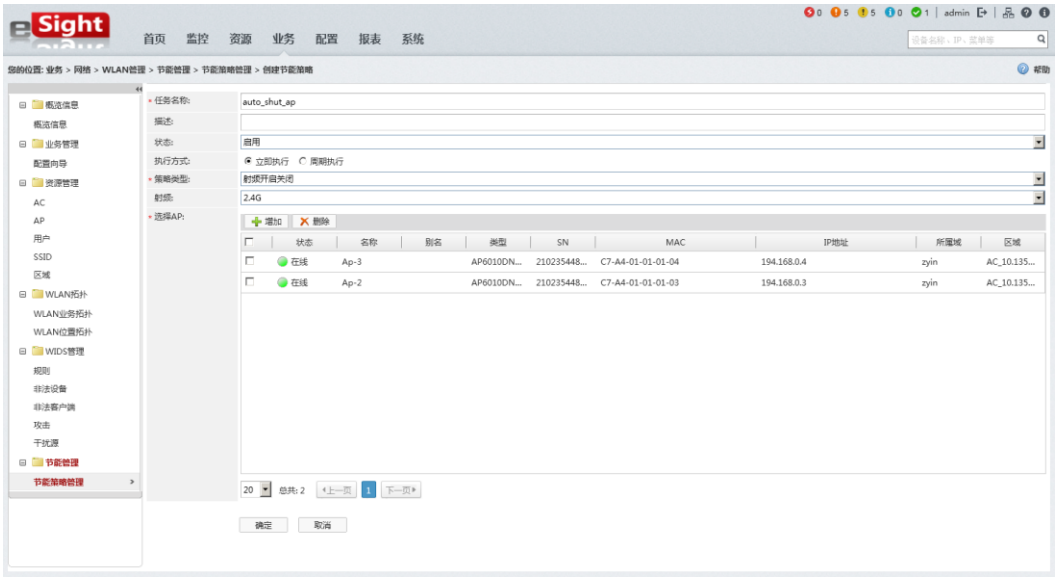
业务报表

提供 AP 上行口流量、信道利用率、射频在线用户数、无线在线用户等预定义报表，以及 AP 关联统计、AP 流量统计、AP 速率统计的快速报表。其中在 Linux+Orcale 环境，还支持 TopN 用户接入失败率和 TopN 用户接入总次数预定义报表

节能管理

提供 AP、射频、SSID 维度的节能策略定制。支持节能任务管理，方便用户立即、周期性开启、关闭无线信号。

图4-85 创建节能策略



4.3.4 BGP/MPLS VPN 管理

BGP/MPLS VPN 管理组件提供对 VPN 业务的部署、监控和故障诊断端到端解决方案。

- 向导式业务批量部署：批量部署 PE、CE 设备 VRF、接口、路由等业务数据
- 方便快捷自动发现：无需指定设备角色，自动发现网络中已部署的 VPN 业务
- 可视化业务拓扑：直观展示业务 PE-PE、PE-CE 业务逻辑结构，并实时显示业务告警
- 多维度业务监控：从告警、性能、业务链路 SLA 等多个方面监控业务的运行状况
- 一键式故障诊断：分段分层多手段诊断 VPN 业务故障

业务部署

提供图形化、向导式、端到端的业务部署能力，帮助用户简单快速开通新 VPN 业务、增加新的 VPN 接入点以及调整已有的 VPN 业务，提升用户业务维护的效率。支持对 Full-mesh、Hub-Sopke、MCE、自定义组网类型的业务开通，支持在 PE-CE 间部署 OSPF、ISIS、静态以及 EBGP 路由协议。如图 4-96，图 4-97 所示。

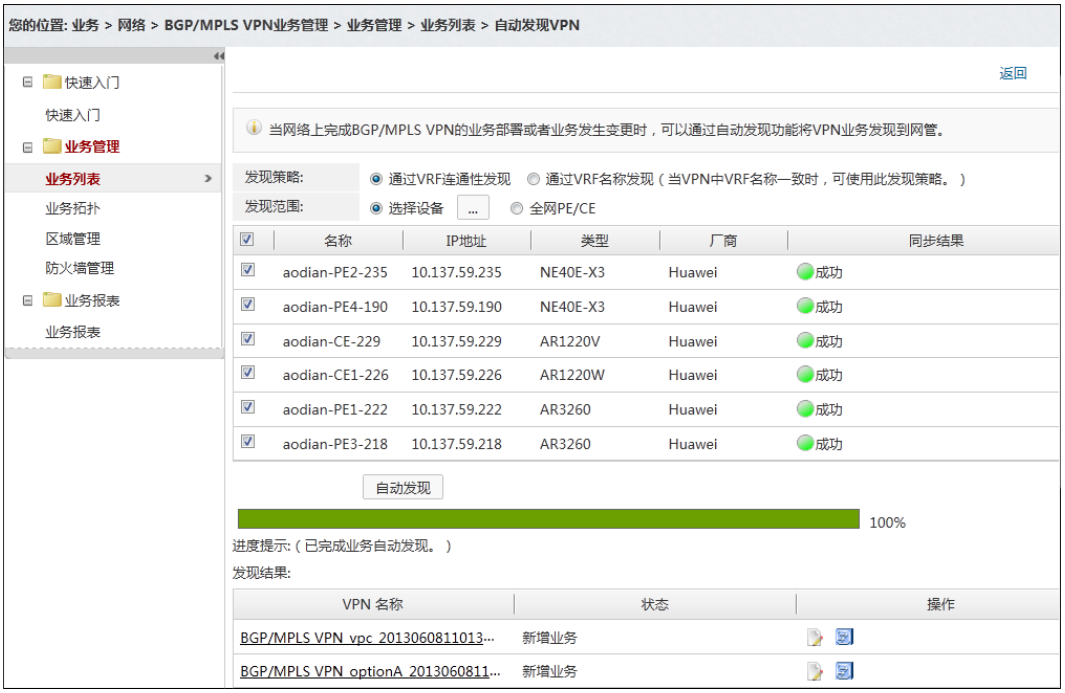
图4-86 MPLS VPN 业务部署

图4-87 创建详细配置

自动发现

自动发现网络中已部署的 MPLS VPN 业务，支持 Full-Mesh、Hub-Spoke、MCE、HoVPN、跨域 OptionA、跨域 OptionB 组网类型的业务自动发现。在进行自动发现的时候，用户无需指定 PE 和 CE 设备，系统能够根据业务配置信息自动识别设备角色并发现 PE-PE、PE-CE 之间的业务逻辑关系。自动发现如图 4-98 所示。

图4-88 MPLS VPN 自动发现



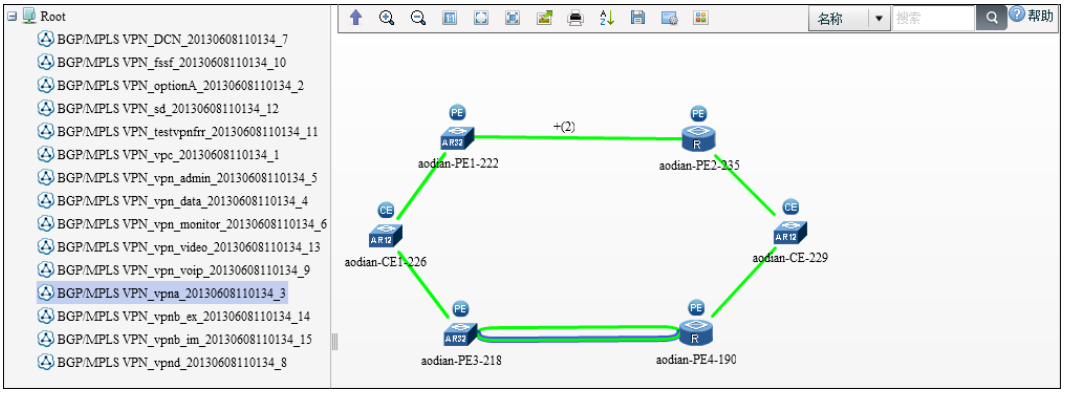
业务监控

- 提供 MPLS VPN 业务监控能力，查看 MPLS VPN 业务配置信息，包括 PE-PE 链路、PE-CE 链路、VRF 实例、路由配置信息。
- 提供 MPLS VPN 性能监控，支持 TopN 流入/流出流量性能统计、PE-CE 流量性能统计、VRF 流量性能统计、VRF 路由性能统计。通过与网流组件联动，用户能够查看哪些应用和终端消耗了当前接口的流量，实现对 VPN 流量的精细化管理。
- 提供 MPLS VPN 业务质量监控。通过和 SLA 组件联动，监控 VPN 业务的 PE-PE、PE-CE、CE-CE 等各段链路的传输质量，一旦有业务链路出现质量问题，能即时预警。

业务拓扑

通过 MPLS VPN 业务拓扑可直观展示 VPN 网络逻辑结构。提供自定义区域管理。如图 4-99 所示。

图4-89 MPLS VPN 业务拓扑



快速诊断

提供一键式故障诊断，分段对 PE-PE、PE-CE、CE-CE、PE-remoteCE 链路从三层路由和 MPLS 转发层通过 ping、trace、路由信息采集等多种手段进行故障诊断，诊断结束之后系统给出具体的失败原因，帮助用户快速定位故障点和故障原因。如图 4-100 所示。

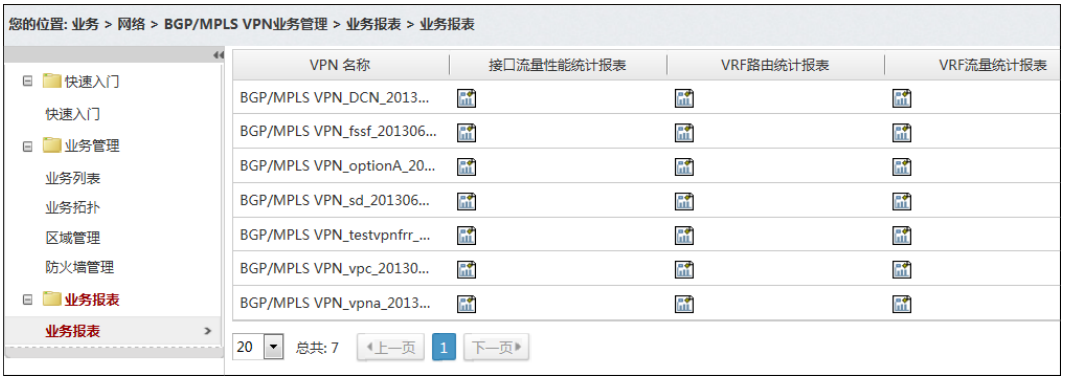
图4-90 MPLS VPN 快速诊断

业务报表

提供接口流量性能统计表、VRF 流量统计报表、VRF 路由统计报。用户通过查看接口流量统计报表，能够了解当前 VPN 业务所有接入接口的历史数据走势，通过查看 VRF 流量统计报表能够了解 VPN 流量在每个 PE 设备上的分布，通过查看 VRF 路由统计报

表能够了解当前 VPN 业务 CE 接入的路由变化。上述三个报表从流量和路由的角度给用户扩容等操作提供数据依据。如图 4-101 所示。

图4-91 MPLS VPN 业务报表



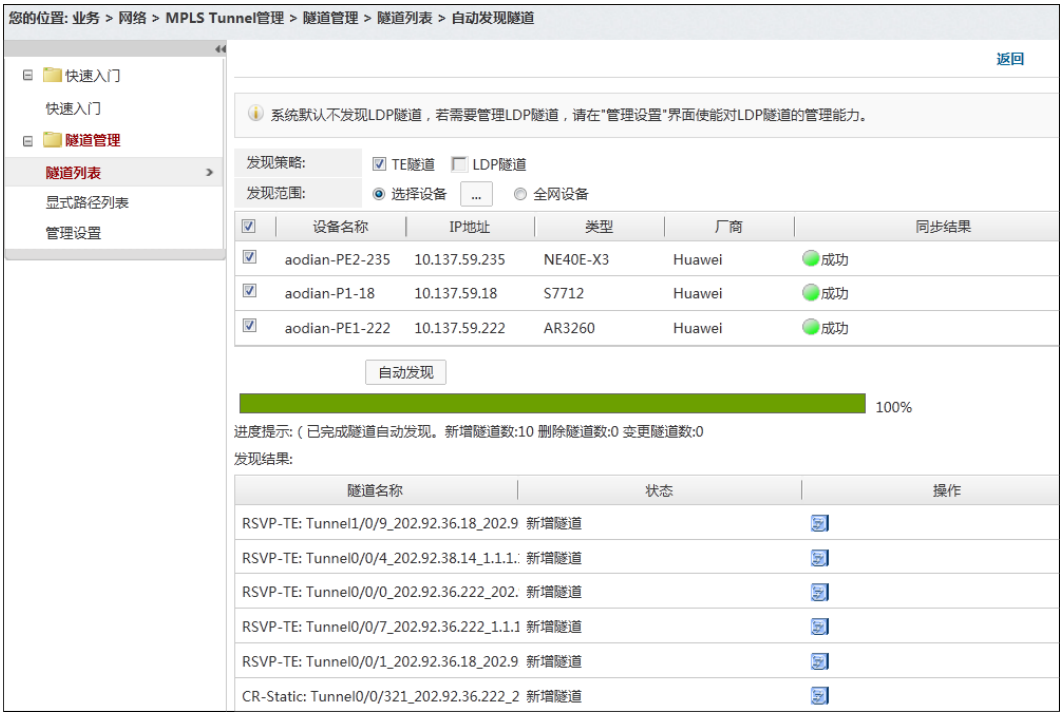
4.3.5 BGP/MPLS Tunnel 管理

MPLS Tunnel 管理组件提供对 MPLS TE 隧道和 LDP 隧道的监控能力，包括隧道的运行状态、备份状态、隧道拓扑、隧道告警、故障诊断以及查看与隧道相关的 VPN 业务。

自动发现

自动发现网络中的 MPLS 隧道，支持 MPLS TE 隧道及 MPLS LDP 虚隧道的自动发现。如图 4-102 所示。

图4-92 MPLS Tunnel 自动发现



隧道监控

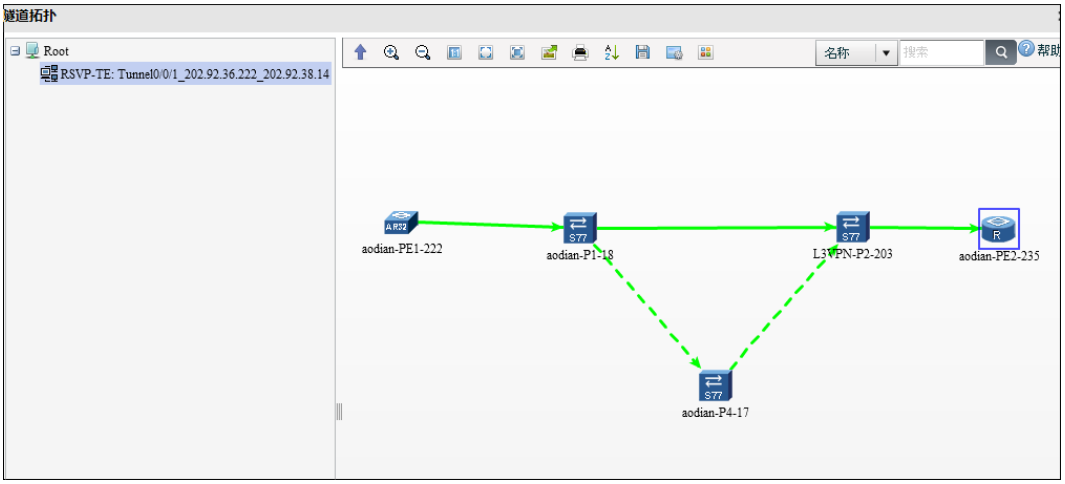
提供 MPLS 隧道监控能力，支持 MPLS TE 动态隧道主备保护和旁路保护、MPLS TE Static-CR 隧道的监控，包括隧道的备份状态、运行状态、隧道告警。

提供 MPLS 隧道与 L3VPN 的联动能力，支持查看 TE 隧道承载的 VPN 业务。

隧道拓扑

通过隧道拓扑能可视化监控隧道状态、链路状态、节点状态等关键状态信息，并能够查看和设备相关的 MPLS 信息。如图 4-103 所示。

图4-93 隧道拓扑



- 支持对 MPLS TE 隧道设备 MPLS 能力、接口 MPLS 能力、DS-TE 信息、链路带宽信息查看。
- 支持对 MPLS LDP 虚隧道设备 MPLS 能力、接口 MPLS 能力信息查看。

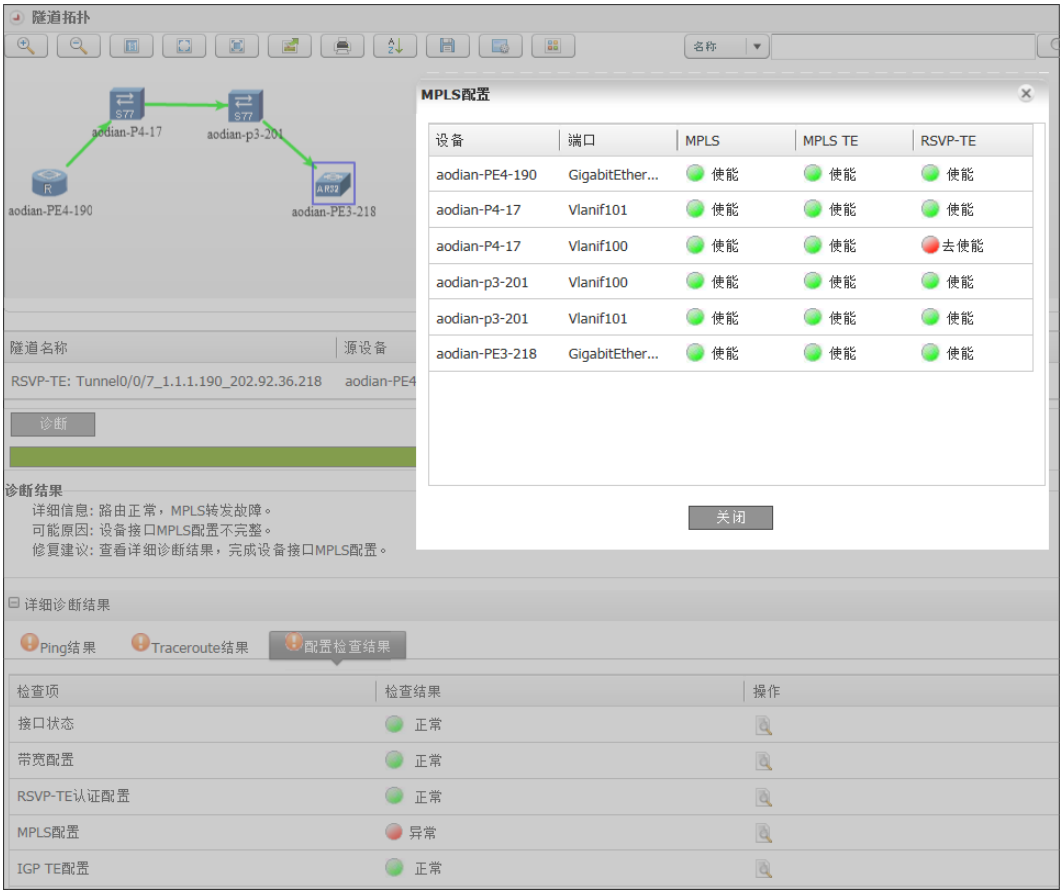
显式路径

提供显式路径查看，支持显式路径列表以及显式路径每一条详细信息的查看。

快速诊断

提供 MPLS 隧道诊断功能。eSight 可诊断隧道中沿途各节点路由转发是否正常，标签转发是否正常，各节点隧道相关配置是否正确。如隧道存在故障，eSight 可精确定位发生故障的节点和原因，并给出详细的诊断结果。如图 4-104 所示。

图4-94 隧道诊断



4.3.6 SLA 管理

SLA 管理提供网络性能度量与诊断功能，用户通过创建 SLA 任务可周期性监控网络的时延、丢包、抖动情况，并根据 SLA 服务中提供的服务来计算出当前网络的符合度情况。

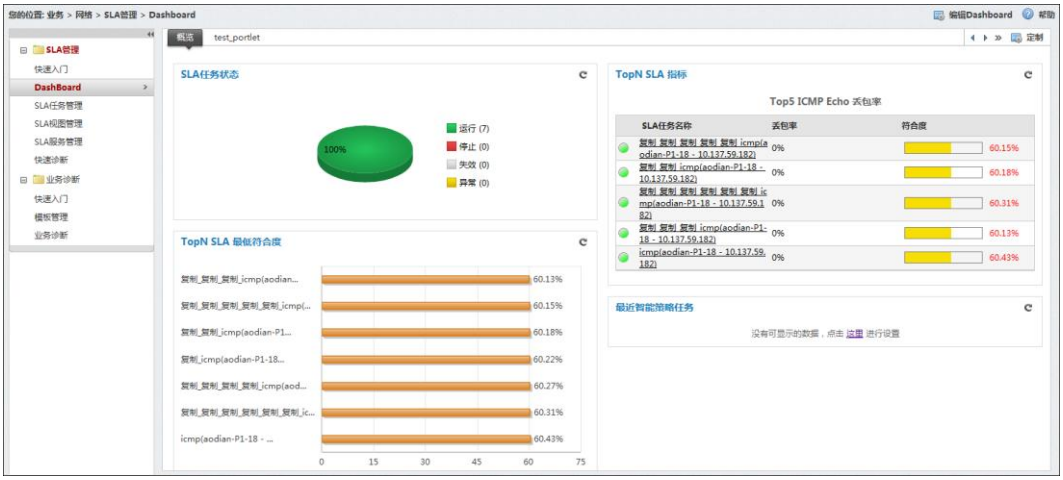
SLA 服务默认提供了 24 种服务，用户也可以根据需求自定义服务。Dashboard 提供了全局监控 SLA 任务的能力，可通过 Dashboard 快速了解所有业务的全网的质量总体情况，也可以查看某一地区或者是某一种业务的全网质量。SLA 视图界面可以将多个任务建立一个视图，对任务数据进行对比。快速诊断用于临时发起源宿设备间的链路及其承载的业务的诊断，可快速定位网络故障。

图4-95 SLA 快速入门

Dashboard

通过 SLA Dashboard 全局监控 SLA 任务情况，可以监控最近触发智能策略的任务、SLA 测试例指标以及 SLA 任务最低符合度的情况。Dashboard 支持添加、删除功能，并可设置过滤条件，对展现在 Dashboard 中的 SLA 任务进行过滤。

图4-96 SLA Dashboard



SLA 服务管理

SLA 服务管理提供对业务的服务质量定义，提供常用业务如语音、视频、数据等二十四种预定义模板，同时支持用户自定义，可根据用户运维需求和网络状况定制符合度和各种网络质量指标阈值。

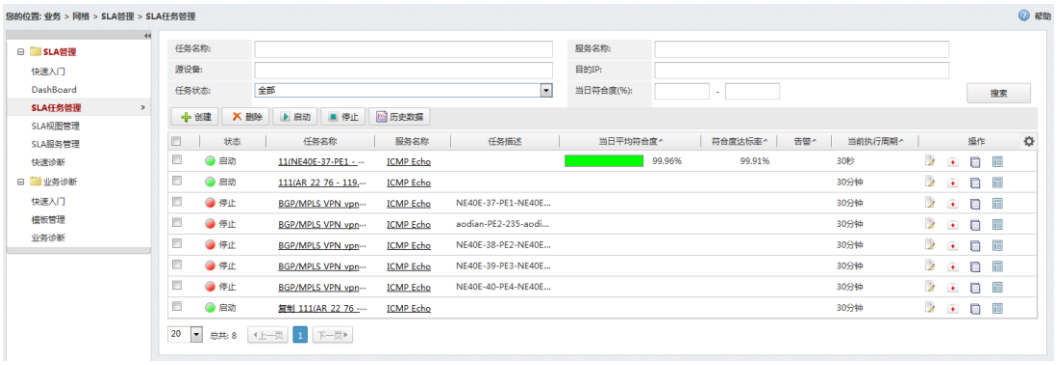
图4-97 SLA 服务管理

图4-98 创建 SLA 服务

SLA 任务管理

SLA 任务可周期性监控网络的时延、抖动、丢包率各项指标。SLA 任务管理界面提供 SLA 任务的管理功能，实现对任务的创建、复制创建、删除、启动、停止等操作。提供查看历史数据、告警、快速诊断的快捷操作入口。SLA 任务的采集周期支持智能调节，可以在网络质量发生劣化时，自动调高采集频率，使用户了解质量劣化的详细信息。

图4-99 SLA 任务管理



SLA 视图管理

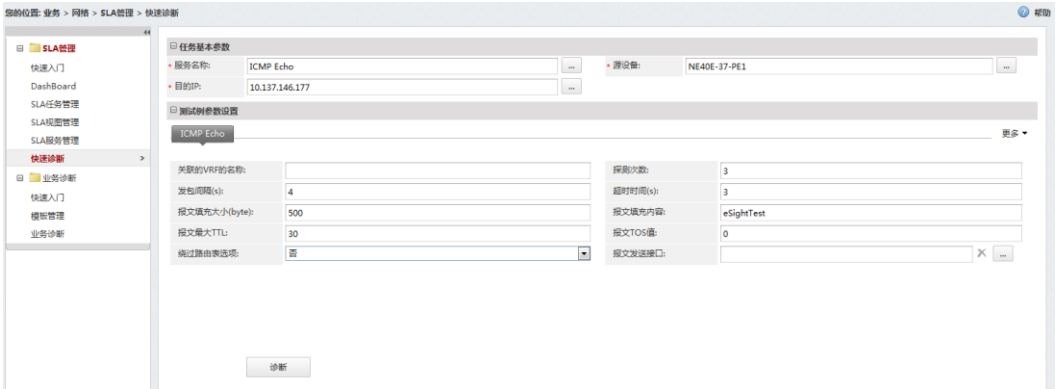
提供对 SLA 任务进行分组管理的功能，方便用户进行多任务历史数据查看。

图4-100 SLA 视图管理

快速诊断

在无需创建任务的条件下，提供快速进行 SLA 服务质量检测的能力。

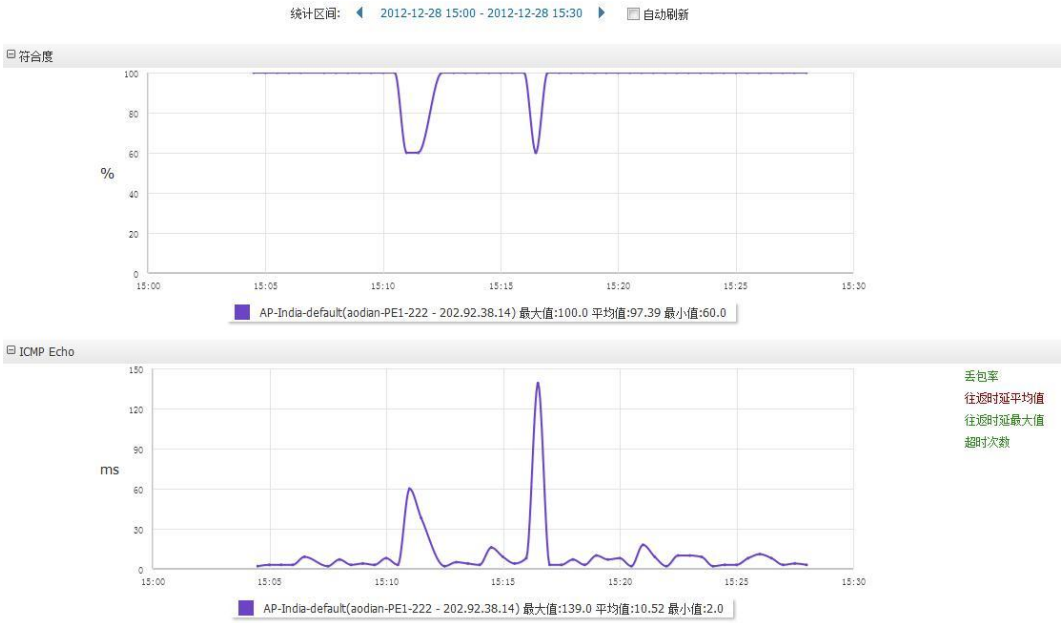
图4-101 快速诊断



历史数据

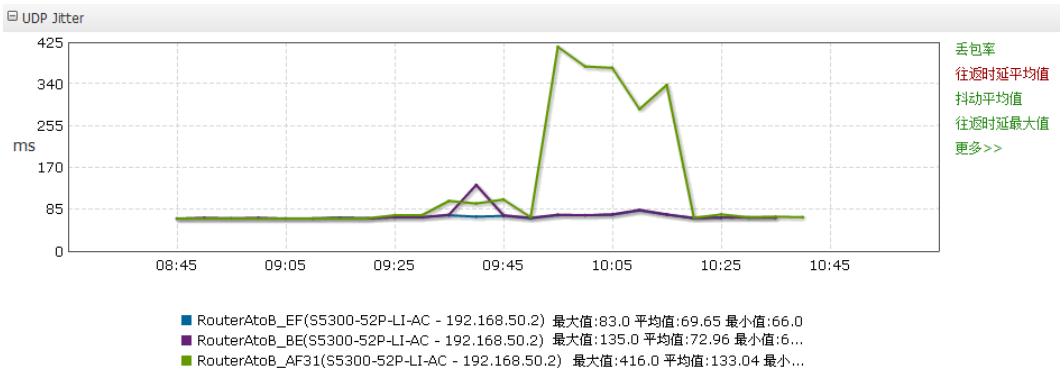
提供业务质量数据图表，支持总体符合度、单网络指标的数据展示。 在SLA 任务界面点击 SLA 任务名称即可跳转到历史数据页面。

图4-102 历史数据查看页面



多任务历史数据查看可以同时展现多个任务的历史数据。

图4-103 多任务历史数据查看页面



SLA 业务报表

提供 SLA 业务质量统计报表、SLA 任务指标统计报表和 TopN SLA 符合度报表。

业务诊断

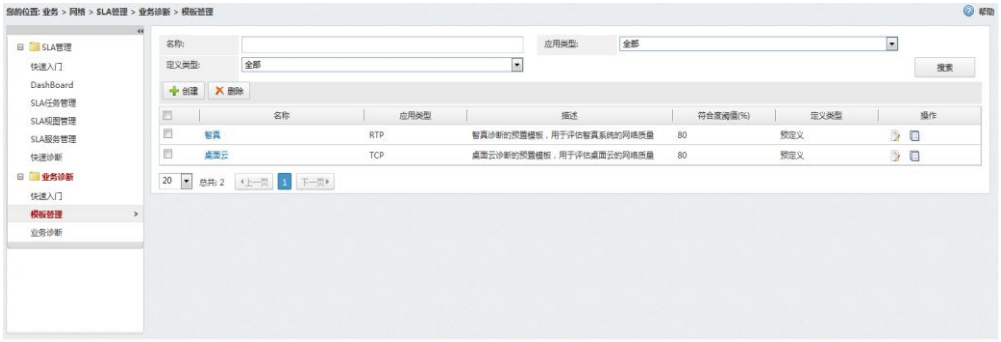
业务诊断实现了对网络质量的检测，将采集到的时延、抖动、丢包率、DSCP 值分段展现出来，帮助用户完成对业务质量的评估，同时基于采集到的数据，定位出现质量问题的网络位置，帮助用户排除故障，保障业务的畅通性。

- 模板管理

  系统提供缺省的网络业务质量（时延、抖动、丢包率等网络性能指标）评估标准，用户可根据需求自定义模板，默认提供两个预定义的模板：

  - 智真诊断的预置模板，用于评估智真系统的网络质量。
  - 桌面云诊断的预置模板，用于评估桌面云的网络质量。

  图4-104 模板管理

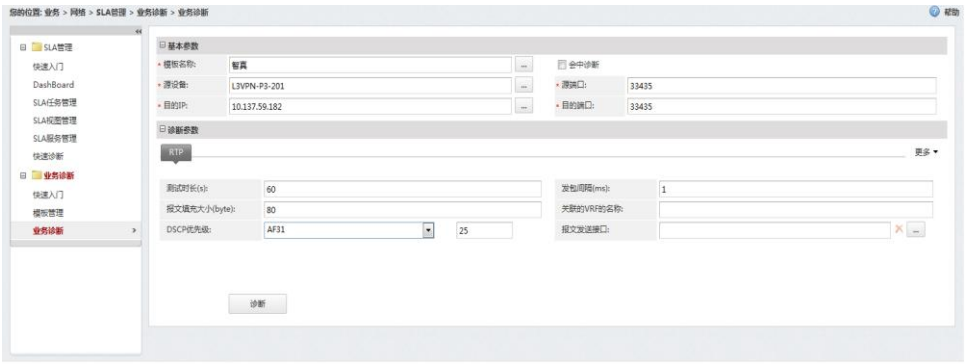
  

- 业务诊断

  对业务质量进行诊断，快速有效地支撑用户对网络故障的定位及质量评估。进行业务诊断之前首先要选择对应的模板。

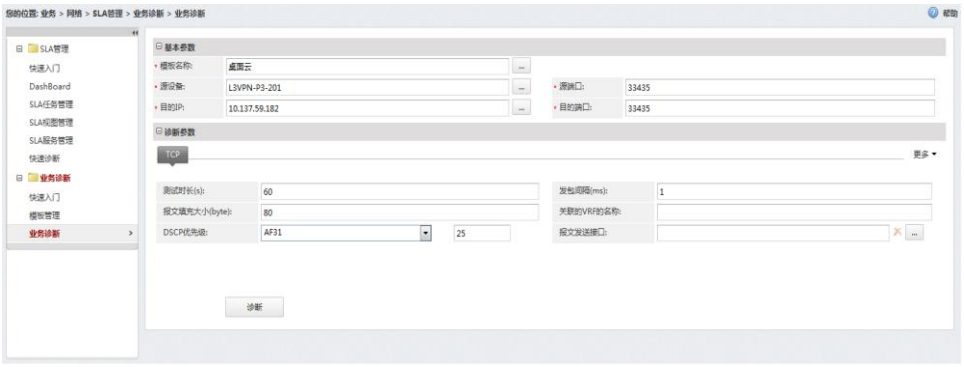
  - 选择智真诊断模板，进行智真诊断。

    图4-105 智真诊断参数设置

  - 选择桌面云诊断模板，进行桌面云网络诊断。

图4-106 桌面云诊断参数设置



诊断结果以分段的形式进行展示。表格中的每一条数据表示从源设备到目的设备之间的网络状况。

图4-107 诊断结果界面

4.3.7 QoS 管理

eSight QoS 管理提供了基于 QoS 流量的监控工具，对于配置了流策略的接口，提供匹配速率、丢弃速率、超出承诺带宽速率、带宽利用率等网络性能指标的度量。

Dashboard

QoS 的 Dashboard 展示了 QoS 性能指标 TopN 任务，可以帮助网络运维人员快速发现有可能出现 QoS 流量异常的区域。

图4-108 QoS Dashboard

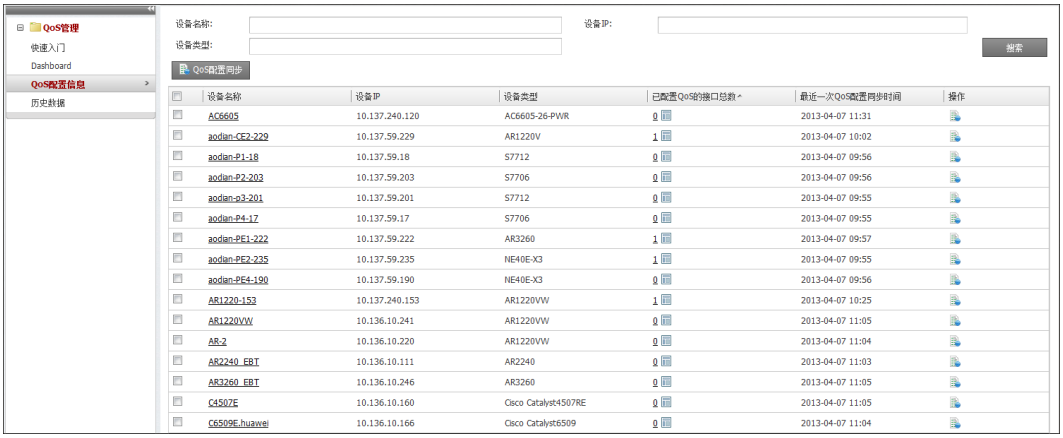
TopN 平均流分类带宽利用率

设备名称	接口	方向	流分类	利用率
gugan_AR2220_225--	HUAWEI, AR Series, GigabitEthernet5/0/15 Interface	流入	juzi	0.00%
gugan_AR2220_225--	HUAWEI, AR Series, Vlanif18 Interface	流入	juzi	0.00%
gugan_AR2220_225--	HUAWEI, AR Series, Vlanif18 Interface	流出	juzi	0.00%
gugan_AR2220_225--	#HUAWEI, AR Series, GigabitEthernet0/0/0 Interface~!@#$%	流出	huawei	0.00%
gugan_AR2220_225--	HUAWEI, AR Series, GigabitEthernet0/0/1 Interface	流入	huawei	0.00%
gugan_AR2220_225--	HUAWEI, AR Series, GigabitEthernet0/0/1 Interface	流出	huawei	0.00%

QoS 配置信息

查看设备的 QoS 配置信息。

图4-109 QoS 配置信息



历史数据

QoS 流量历史数据可以展现 QoS 流量的历史趋势情况，帮助网络运维人员了解 QoS 流量的历史情况。

图4-110 QoS 历史数据

4.3.8 数据中心 nCenter 管理

数据中心 nCenter 是对数据中心网络进行统一管理的系统，主要用于管理部署虚拟化的数据中心接入网络。统一管理、监控数据中心资源，动态感知资源变更并自动部署网络策略，自动计算拓扑路径展示数据中心全网扑图。

资源管理

提供统一的数据中心虚拟资源管理功能，如图 4-121 所示。

图4-111 虚拟资源管理

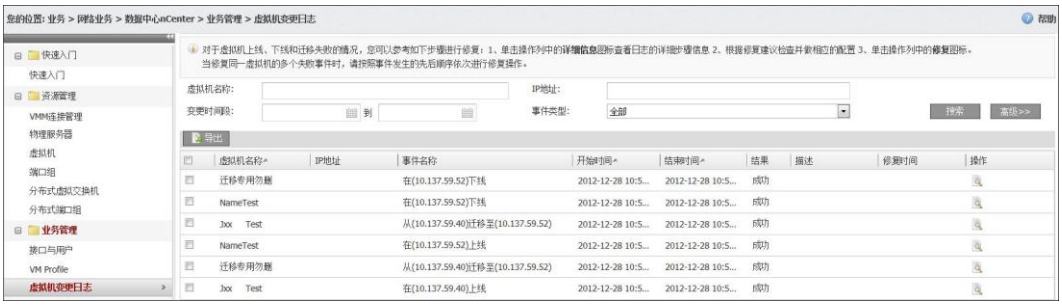
- 通过创建 VMM，可以自动发现同步 VMM 下所有虚拟资源（物理服务器、虚拟机、虚拟交换机、分布式虚拟交换机等）。
- 提供统一查询模式，可以查询、导出当前 VMM 下管理的物理服务器、虚拟机、端口组、分布式虚拟交换机、分布式端口组。
- 支持 VMM、物理服务器单独、批量手工同步功能。

- 支持标准虚拟交换机、端口组的创建、删除、修改功能。
- 支持分布式虚拟交换机、分布式端口组的创建、删除、修改功能。

业务管理

提供虚拟资源业务配置、变更日志管理功能，如图 4-122 所示。

图4-112 虚拟资源业务管理

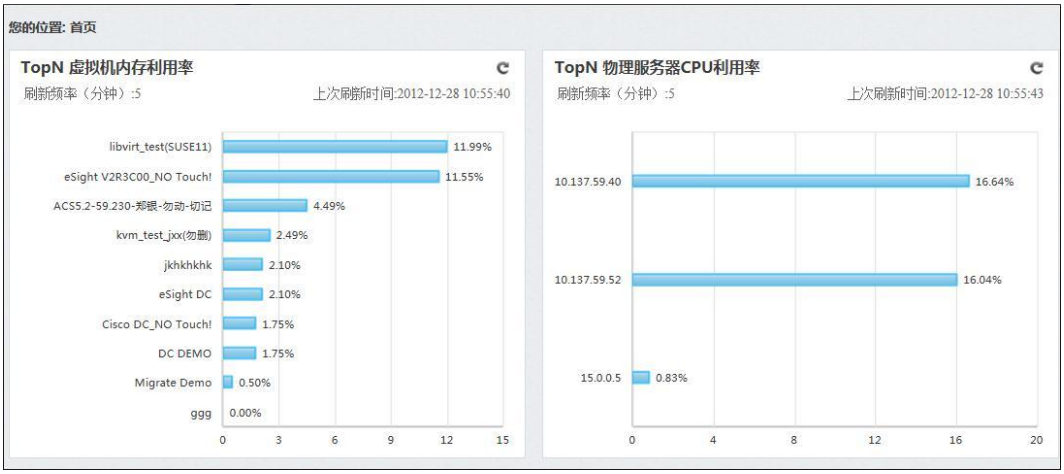


- 通过创建 VM Profile 方式，可统一配置虚拟机所需 ACL、QoS 等物理策略。
- 通过端口组绑定 VM Profile，用于统一部署自动下发网络策略。
- 通过虚拟机变更日志界面，可以查看虚拟机变更记录并对失败的虚拟机变更进行修复。
- 通过接口与用户界面，可以查看 TOR 接口上线虚拟机用户详细信息。

业务监控

提供统一的虚拟资源指标监控功能，如图 4-123 所示。

图4-113 虚拟资源业务监控



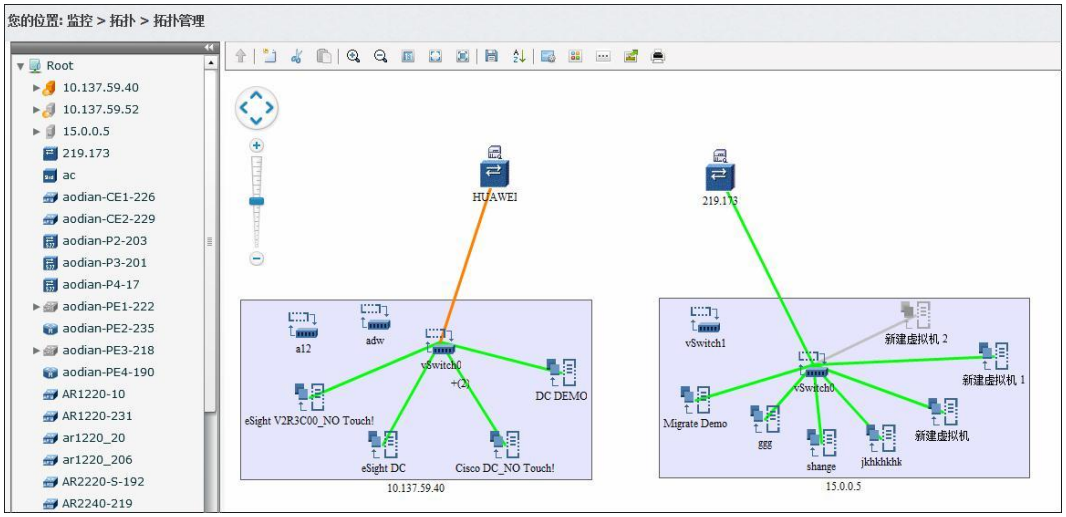
- 通过性能管理可以自动、手工创建物理服务器、虚拟机 CPU 利用率、内存利用率、磁盘 IO 速率、网卡 IO 速率的性能指标监控。

- 通过告警管理可以查看 VMM 上产生的告警信息。
- 通过定制 portal 可以查看物理服务器、虚拟机 TopN 性能指标。

拓扑查看

提供统一的虚拟资源拓扑查看功能，如图 4-124 所示。

图4-114 虚拟资源拓扑关系展示



- 通过拓扑视图可以查看 TOR 交换机、物理服务器、虚拟交换机、分布式虚拟交换机、虚拟机之间的组网关系。
- 通过拓扑跳转可以查看虚拟资源对应的详细信息及告警列表。

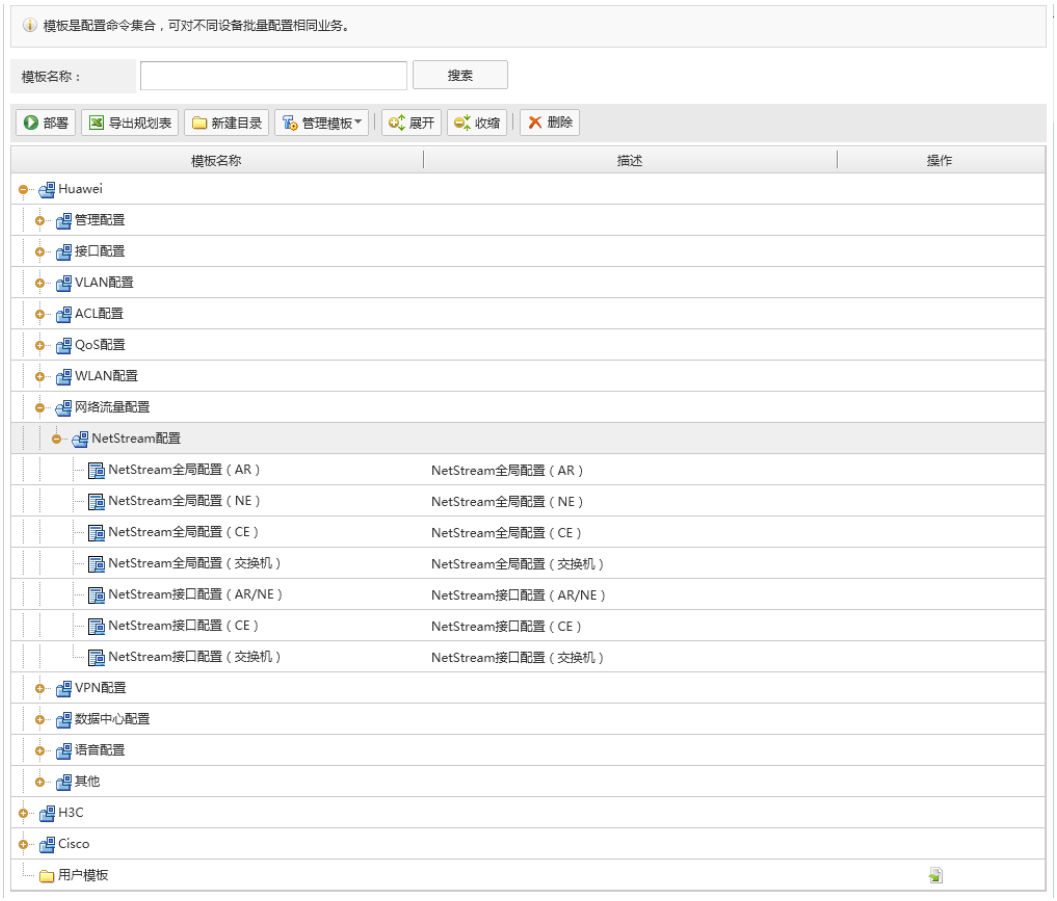
4.3.9 网络流量分析管理

eSight NTA 组件提供了一种便捷、经济的网络流量分析方法，能深入分析网络中的流量数据并提供详细的流量分析报告。用户利用 NTA 能实时监控全网应用流量分布，能及时发现网络中异常流量，根据长期的流量分布做好网络规划，做到流量可视、故障可查、规划可依的网络透明化管理。

设备接口 NetStream 使能

网流通过智能配置工具向设备下发 NetStream 命令，用户不再需要手工登录一个个设备 Netstream 配置，实现快速部署。

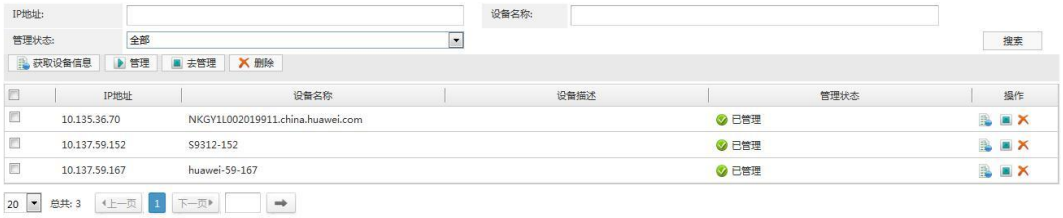
图4-115 接口 NetStream 使能



流量配置

网流配置提供设备配置、接口配置、协议配置、应用配置、DSCP 配置、IP 组配置、应用组配置、接口组配置以及 DSCP 组配置能力。

图4-116 设备配置界面



- 设备配置

  展示全网有流量上报的设备，用户可选择性地对设备进行监控。
- 接口配置

展示全网有流量的接口，用户可对接口流入速率、流出速率和采样比进行配置，保证网流流量数据的正确性；其中，采样率的配置值要与设备端采样率保持一致，以还原设备的真实流量。

- 协议配置

  用户根据实际需要，选择性地对协议进行监控。

- 应用配置

  列举常用的 542 个网络应用，分为系统预定义应用、协议应用和用户自定义应用，用户可自定义重要应用。

  - 用户自定义应用：用户添加的应用，根据指定的协议(UDP/TCP)、端口范围和 IP 范围来定义应用。
  - 系统预定义应用：系统预置好的应用，是网络中常用的一些应用，通过协议和端口来标识。
  - 协议应用：不区分端口，直接根据协议来标识的应用。

- DSCP 配置

  列举常见的 22 种 DSCP，并且用户可自定义 DSCP 名称。

- IP 组配置

  用户可将有关联的一组 IP 地址分为一组，如一个部门或一个楼层，方便查看该 IP 组的流量信息。

- 应用组配置

  用户可将按照自己关注的点进行应用分类，如邮件类应用组，便于查看该应用组的流量信息。

- DSCP 组配置

  用户可将有关联的服务类型进行分组，如语音类，便于查看该 DSCP 类的流量信息。

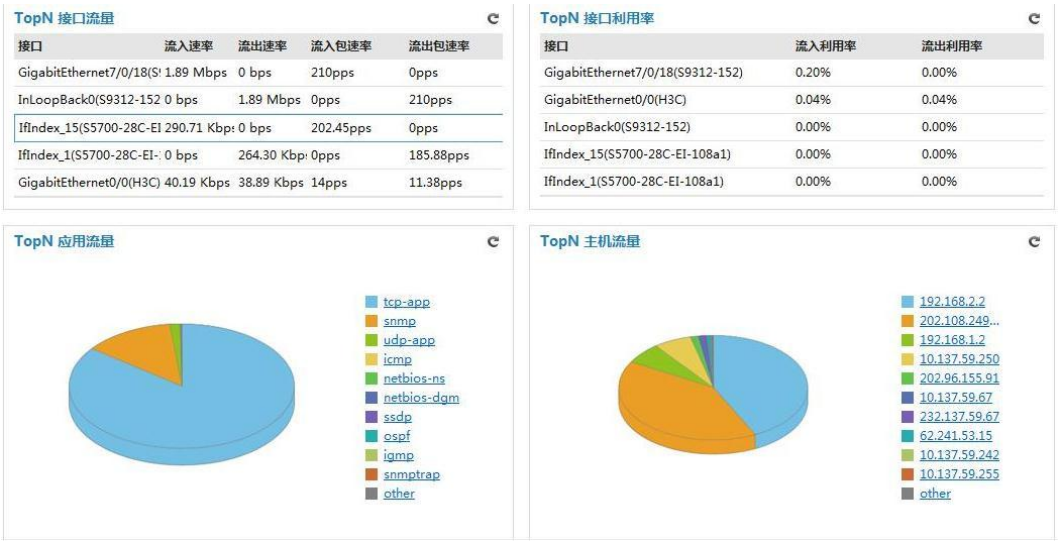
- 接口组配置

  用户可将相关联的接口定义成一个接口组，方便查看接口组流量信息。

流量概览

提供全网流量概览，多维度、实时展现全网流量动态，用户可快速的查看到各维度的流量信息。如下图：

图4-117 操控板流量分析



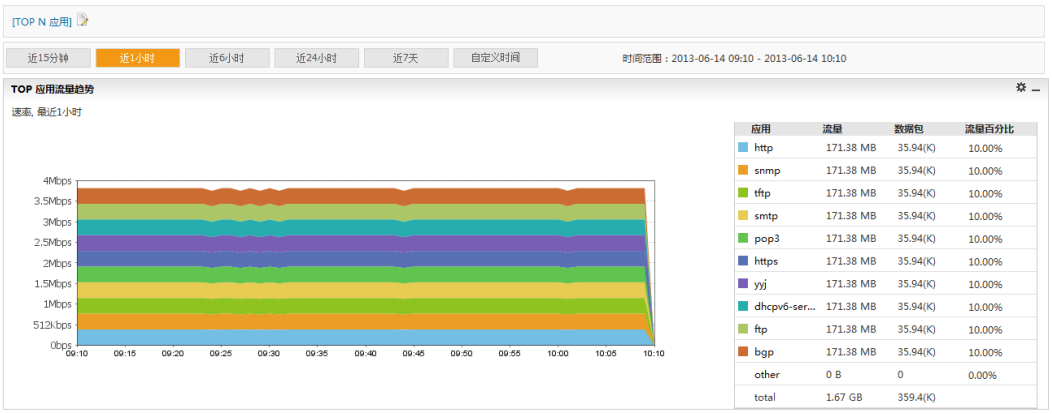
- 界面包括接口流量排行、接口利用率排行、设备流量排行、应用流量排行、主机流量排行、DSCP 流量排行、会话流量排行等内容；
- 展现形式、展现内容、内容排版可自定制，支持自定义“窗件”操作， 窗件支持Tooltips，超链接，最小化/最大化等操作。

流量分析

提供钻取式流量分析能力，用户可通过逐步选择查看条件，查看需要关注的流量信息。系统提供了设备流量、接口流量、应用流量、DSCP 流量、主机流量、会话流量、接口组流量、IP 组流量、应用组流量等维度详细的流量分析能力。

用户可通过设备、应用、DSCP 等不同的维度查看全网流量信息，以应用流量为例，可看到全网的应用流量分布：

图4-118 应用流量分析示意图

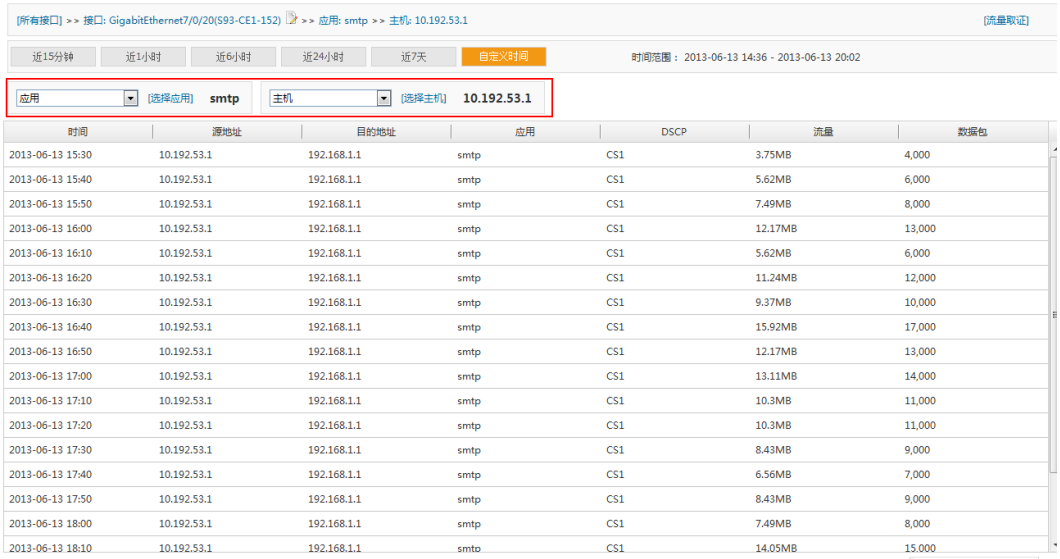


用户可通过进一步的下钻，查看某一具体对象的流量信息，以接口流量分析为例，可选择某一具体接口，查看该接口详细的流量信息；

图4-119 接口流量分析示意图

另外，提供了强大的数据下钻能力，用户可通过设置不同的过滤条件，层层下钻，最终定位查看详细的会话信息；

图4-120 接口流量详细会话信息示意图



网流报表

提供向导式的自定义报表能力，用户灵活定制所关注的流量报表。提供报表的导出和邮件发送能力，用户可通过报表，及时地了解网络中的流量分布信息。

图4-121 创建网流报表界面

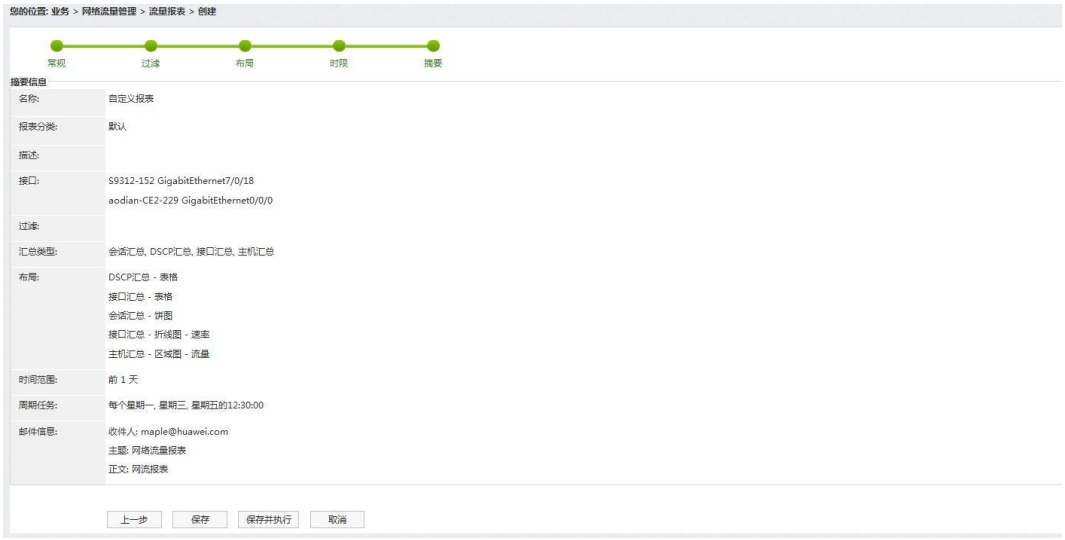
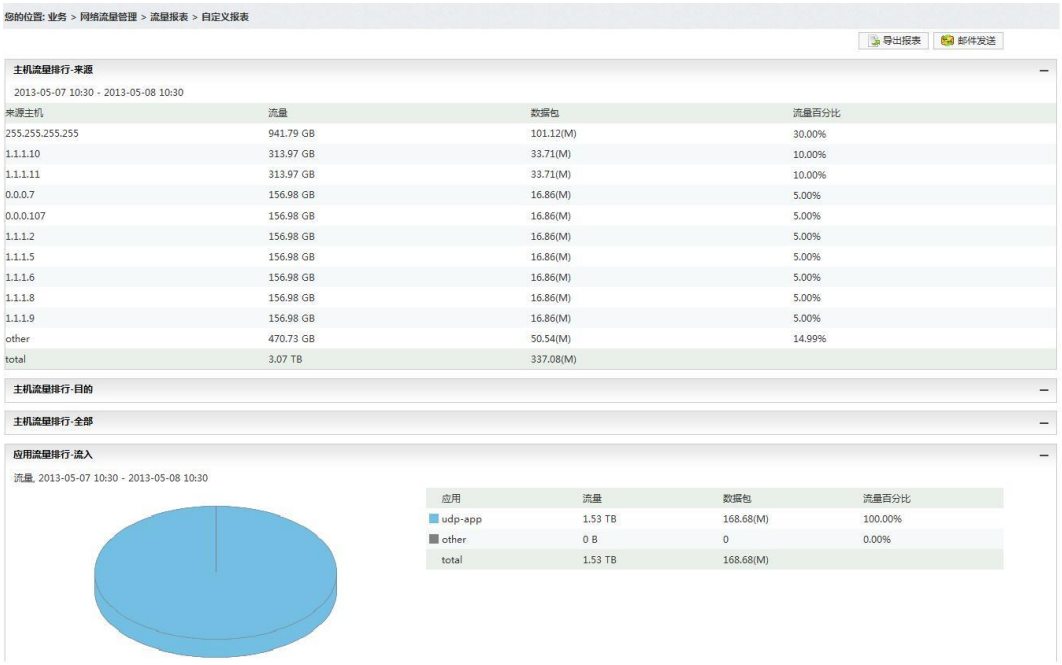


图4-122 查看网流报表界面



- 支持多种报表数据展示方式：饼图、表格、折线图、区域图。
- 支持多种汇总类型：应用、会话、DSCP、主机、接口汇总。
- 支持多个过滤条件：源地址、目的地址、应用、DSCP。
- 支持即时任务和周期任务：
  - 即时任务

    即时任务，需要用户手工执行，反映的是即时的统计结果。任务执行成功后，界面上会有状态提示，打开报表会展示详细的数据和图形供用户查看。

- 周期任务

  周期任务，系统会按照用户指定的运行周期执行，反映的是一个周期内的统计结果。

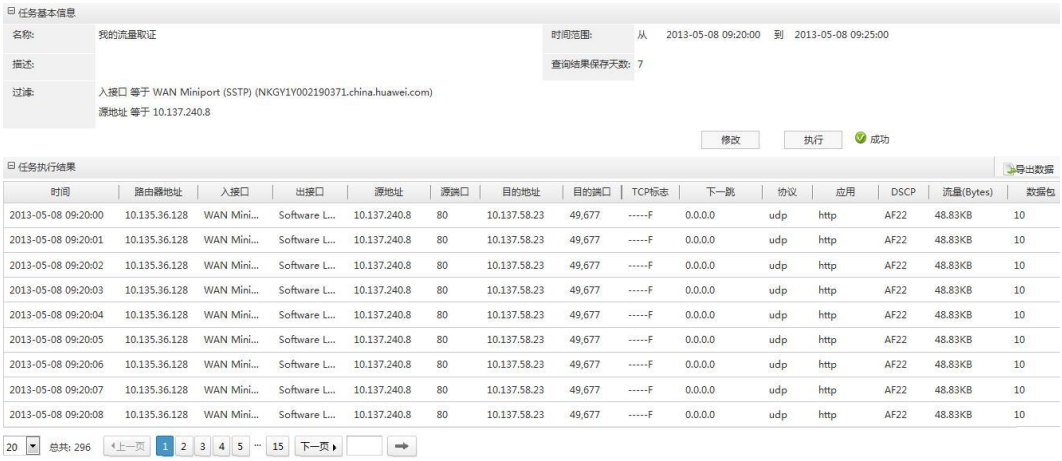
- 支持单个和批量导出报表。
- 支持报表的邮件发送功能

流量取证

发现网络中存在异常流量，需要进一步进行定位时，系统提供获取流量原始数据的能力，协助定位网络故障。

取证结果以七元组的维度分组审计数据，清晰直观的展现任务的流量信息；如：用户可通过比对协议、端口及包速率，查看是否存在病毒威胁；通过 TCP 标志位，确认是否存在协议攻击威胁。

图4-123 流量取证界面



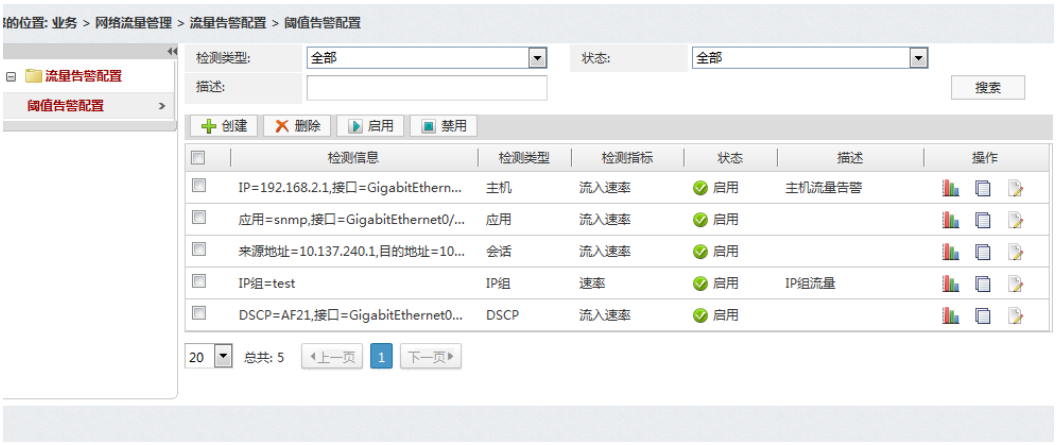
- 支持按照时间范围进行原始报文获取；
- 支持多个过滤条件：源地址、目的地址、入接口、出接口、源端口、目的端口、协议、应用、DSCP、TCP 标志；
- 支持设置查询结果保存期限，最多可保存 30 天；
- 支持查询结果导出，可选择分页或全部导出。

流量告警

支持对应用、服务器、会话等七种类型的流量创建阈值告警，当流量在规定的时间内超过阈值次数满足条件时，会自动生成告警，当流量在规定时间内满足恢复条件时，告警自动清除。触发告警和清除告警均可发送邮件通知用户。

流量阈值告警配置界面提供了阈值告警的管理能力，实现了创建、复制创建、删除、启用、禁用等操作，用户可选择需要监控的对象，参照历史流量数据设定告警级别、阈值、重复次数等基本信息。

图4-124 阈值告警配置界面



当前告警页面可以查看网流告警信息，并且支持从当前告警跳转至流量分析页面查看告警生成时间段的详细流量信息。

图4-125 查看网络流量告警

4.3.10 安全策略管理

eSight Secure Center 安全策略管理组件能有效管理大规模华为防火墙/UTM 部署环境中设备的安全策略，主要功能包括：

- 安全策略集中批量配置：支持对物理和虚拟防火墙进行集中或者分域策略配置
- 公共对象配置：支持集中配置地址集、时间段、服务和上网用户等公共对象
- 内容安全策略配置：支持集中配置 IPS 策略和 AV 策略
- 安全策略发现：支持从防火墙设备同步设备侧策略和公共对象
- 策略部署/拆除：支持对多个防火墙的策略进行批量部署和拆除

快速入门

快速入门提供策略管理的配置流程，查看目前已经 license 授权管理的设备。

策略管理

提供访问控制策略、内容安全策略、上网行为策略的集中配置、下发。

- 策略查看

  策略总览界面，可以查看策略的部署状态，策略的上下文环境，即域间策略的优先级，排在前面的安全年策略优先被命中

- 策略部署

  提供策略的集中、批量式部署操作，用户完成策略集中配置后，点击“部署”按钮，选择需要部署的设备，一键式批量下发安全策略，大大节省运维人员的维护时间和操作成本

- 策略发现

  提供策略的集中、批量式发现操作，将现网设备上的策略同步到网管中集中管理。

- 策略拆除

  提供策略的集中、批量式拆除操作，用户网络整改或搬迁时，对于不再需要的配置，可以通过拆除操作，一键式清理安全策略配置，保证企业信息安全。

- 策略基本配置

  提供策略名称，策略的描述，批量选择需要配置的设备

- 策略业务配置

  传统防火墙的五元组配置，提供网络访问控制功能配置，可以通过源地址、目的地址、服务、时间段配置访问数据流的动作为放行或阻断

- 内容安全策略配置

  提供 IPS、AV 策略的配置，实现对于不同安全区域的内容安全控制，避免黑客入侵和病毒传播，保证企业网络的安全。

- 其他配置

  提供策略日志记录、开启会话流量统计功能等

全局配置

提供内容安全全局开关配置及 IPS、AV 策略的全局配置。

- 安全策略全局配置

  提供过载保护功能开关，提供溢出分片报文、溢出 TCP 分段报文的处理方式配置为丢弃或转发

- 安全策略全局配置—入侵防御

  提供 IPS 入侵防御功能开关，IPS 的工作模式配置、设备全局的 IPS 特权策略配置。

- 安全策略全局配置—反病毒

  提供反病毒功能开关，扫描等级配置，最大解压层数配置，病毒统计功能开关配置

公共对象

支持集中配置地址集、时间段、服务、上网用户、IPS、AV 等公共对象的新建、删除、修改、查看等操作。

4.3.11 基础设施管理

eSight 基础设施管理支持对数据中心基础设施层的电源供配电、机房空调、环境、机柜、安防等系统进行管理。

- 电源设备：精密空调、不间断电源（UPS）、配电柜（PDU）、自动切换开关（ATS）等。并可查看电源设备的运行状态、运行参数、告警信息等实时数据。
- 机房空调：支持精密空调、行式空调、加湿器等设备运行状态的监视和管理。eSight 基础设施管理组件支持在远端管理精密空调机的启动、停止，或者改变温度与湿度工作点。
- 机柜：支持机柜微环境的管理，可实时查看机柜环境信息，掌握机柜的空间、供电、散热、承重等资源的使用。
- 环境：通过采集器接入，实现机房的烟感、温湿度、水浸等环境参数的监测。eSight 基础设施管理组件支持查看机房或模块内的气体浓度是否存在告警，并支持查看温湿度等参数的实时数据。
- 安防设备：eSight 基础设施管理组件支持视频摄像头的接入和管理，支持视频的实时查看、存储与回放。
- 门禁系统：集成的门禁解决方案，实现以卡为基础的用户、用户组管理，访问权限可控制，可审计。

资源管理

eSight 基础设施管理支持以下资源管理功能：

- 支持以下三种形式列举所选管理对象下的子管理对象以及对象信息。
  - 全部：列举所有管理对象。
  - 管理域：列举对应节点下的所有管理域。
  - 物理设备：列举对应管理域中的所有设备。
- 支持以不同的图标表示不同的管理对象类型。
- 支持管理域的添加、删除、修改等功能。
- 支持按名称或类型查询管理域。
- 支持单个创建或批量导入管理域。

视图管理

视图管理，以设备视图直观的反映设备的物理位置信息和运行状态，实时监控整个网络中设备的运行情况。

能效管理

包括能耗统计、PUE、电价计费、能耗报表、能耗历史分析，可以查看不同管理域的各种能耗状态，包括 IT 耗电、照明耗电、总耗电等。用户可以了解能耗实时状态，历史状态以及各个子系统的能耗分布，从而为数据中心的能耗优化提供依据。

- 分层、分级的能耗评估：在配电系统视图中可按照需求定制能耗节点，满足从园区到机房不同管理域，不同管理粒度的能耗统计。
- 能耗分析的 dashboard 展示：以统一的页面展示某个管理域的所有能效信息。
- 历史数据分析：查询某一个时间段的历史数据，用于趋势分析。
- 阶梯电价：通过策略配置，直观展示数据中心的能耗成本。
- 可以根据需要自定义电价策略可以增加月电价策略或时间段电价策略，也可对电价策略进行修改，删除等操作。

视频管理

eSight 基础设施管理支持以下视频管理功能：

- eSight 具有 IP Camera 的接入能力。
- eSight 可集成 IVS 客户端，在客户端可直接访问视频服务器，并实现视频展示模式的管理。
- eSight 可集成 IVS 服务器，提供 NVR 功能。
- eSight 通过界面集成方式，实现独立部署的视频系统集成。
- 支持实时视频查看，提供视频源配置信息并保存。
- 摄像头管理

  可以根据摄像头名称或 IP 地址搜索对应的摄像头，查看摄像头的名称、编码、视频位置、供应商、IP 地址、型号、状态等详细信息，可进行创建、删除、修改、查询等操作。
- 分组管理

  对视频分组管理，方便对视频进行批量处理，创建新组需设置好组名称、分屏数等。可以根据组名称搜索对应的组，对该组进行创建、删除、修改、查询等操作，还可以查看该组的视频。
- 参数配置

  配置服务器端 IP 地址、服务器端端口号、登录用户、登录密码、显示比例等参数。

报表管理

eSight 基础设施管理提供基本报表信息的显示和下载的界面，根据不同的报表类型，可以将报表展示成曲线图、饼图、柱状图等不同的图形，方便用户直观了解到报表的信息。

- 报表信息可以导出成 Excel 和 PDF 文档，也可将报表进行打印。
- 提供系统配置功能，当用户对报表的存储容量、LOGO 和数据源有特殊要求时，可以通过系统配置功能，修改报表的存储容量和上传 LOGO。

- 支持根据报表任务生成报表，并自动将周期报表保存到存储区，并根据配置将报表以 Email 方式发送给客户。

门禁管理

通过 eSight 基础设施管理提供的门禁系统功能，可以实现对门禁控制器、机柜级门禁控制器的持卡用户进行管理。

- 支持对门禁控制器和事件监控进行管理。能够完成对门禁控制器 IP 的配置，支持管理服务器的配置。

说明
机柜级门禁不支持时间管理功能。

- 时间管理支持在指定时间内或节假日有对门禁进行管理。
- 人员管理支持对用户和用户组进行管理。

容量统计与分析

机房、机柜的空间、机位、散热、配置、承重的能力分析，全面掌控机房资源使用信息，支撑投资决策。

- 机房机位、机架空间、配电能力、散热能力和承重相关的信息统计与分析。
- 基于变更（扩容，迁移等场景）管理的容量信息同步。

容量优化设计

根据设备的物理属性，优化设备在机柜中的最优配置。

- 提供机柜内设备的迁移、增加、变更等场景的设计能力。
- 机柜内设备变更最佳机位分析和自动选择最佳的配置资源。

温度云图

以云图模式直观、全局展示机房温度的分布，支持冷热孤岛的有效识别。

- 支持机柜的上、中、下三个水平面的温度分布分析。
- 云图提供鼠标当前点的温度检出功能，同时提供该点上的设备信息展示。
- 提供 TOP5 温度点（过热点、过冷点）分析。

联动控制

通过联动管理，提升 IDC 机房的运维服务品质。目前提供两种联动策略的定制能力。

- 天窗自动控制策略。
- 集装箱加湿器自动控制策略。

5 配置要求

5.1 软件配置要求

- eSight 精简版支持 Windows 7（32 位） + MySQL 5.5
- eSight 标准版和专业版支持如下操作系统和数据库的组合：
  - Windows Server 2008 R2 标准版（64 位）+ MySQL 5.5
  - Windows Server 2008 R2 标准版（64 位）+ Microsoft SQL Server 2008 R2 标准版
  - SUSE Linux 11 SP1（64 位） + Oracle 11g R2 标准版
  - SUSE Linux 11 SP1（64 位） + GaussDB

  eSight 组件对操作系统和数据库的具体配置要求如表 5-1 所示。

表5-1 操作系统和数据库要求

组件类别	组件名称	Windows Server 2008 + MySQL	Windows Server 2008 + SQL Server	SUSE + Oracle	SUSE + GaussDB
管理平台	eSight 管理平台	√	√	√	√ 说明 分级网管不支持。
设备管理组件	eSight 网络设备管理组件	√	√	√	×
	eSight 主机管理组件	√	√	√	√
	eSight 存储设备管理组件	√	√	√	√
	eSight UC/CC 设备管理组件	√	√	√	√

组件类别	组件名称	Windows Server 2008 + MySQL	Windows Server 2008 + SQL Server	SUSE + Oracle	SUSE + GaussDB
	eSight 视频监控设备管理组件	√	√	√	√
	eSight 智真设备管理组件	√	√	√	×
	eSight eLTE 设备管理组件	√	×	√	×
业务管理组件	eSight Open SDK 组件	√	√	√	√
	eSight 智能报表管理组件	√	√	√	×
	eSight 存储报表管理组件	√ 说明 使用独立的 MySQL 数据库。	×	×	√ 说明 使用独立的 MySQL 数据库。
	eSight WLAN 管理组件	√	√	√	×
	eSight MPLS VPN 组件	√	√	√	×
	eSight MPLS Tunnel 管理组件	√	√	√	×
	eSight 网络 SLA 管理组件	√	√	√	×
	eSight 数据中心 nCenter 管理组件	√	√	√	×
	eSight 网络流量分析管理组件	√	√	×	×
	eSight IPSec VPN 管理组件	√	√	√	×
	eSight 安全策略管理组件	√	√	×	×
	eSight 基础设施管理组件	×	×	√ 说明 使用独立	×

组件类别	组件名称	Windows Server 2008 + MySQL	Windows Server 2008 + SQL Server	SUSE + Oracle	SUSE + GaussDB
				的 MySQL 数据库。	

说明
- √：表示该组件支持对应操作系统和数据库。
- ×：表示该组件不支持对应操作系统和数据库。

5.2 硬件配置要求

eSight 管理平台和组件在不同组合下，对硬件配置的要求详细说明如下。

表5-2 eSight 基础管理

版本	管理规模	服务器配置要求	发货服务器配置
精简版（网络设备）	40 节点（固定值）	• CPU：1*双核 2G 以上 • 内存：4GB • 硬盘空间：40GB	—
标准版	0-200 节点（管理平台 + 设备管理，不包括增值组件）	• CPU：1*双核 2G 以上 • 内存：4GB • 硬盘空间：40GB 说明 请选用 PC Server。	• X3650 M4-1*E5-2640 6c2.5GHz 或以上-8G(2*4G)-2*300G(双 6Gbps SAS 端口)-DVDRW-1*集成四口千兆网卡-ServeRAID M5110e(512M)带电池保护功能-无显示器-2*750W HE(1+1)-100V~240VAC • Tecal RH2288 V2-BC1M13SRSB-eSight S(2*E5-2640 CPU,2*4G,2*300G SAS 2.5,4*GE LOM,SR320BC+电池,DVD-RW,2*750W 电源)
	200-500（管理平台 + 设备管理，不包括增值组件）	• CPU：2*双核 2G 以上 • 内存：4GB • 硬盘空间：60GB 说明 请选用 PC Server。	
	500-2000 节点	• CPU：2*四核 2G 以上	• X3650 M4-2*Xeon 6C E5-2640 2.5G 或以上-

版本	管理规模	服务器配置要求	发货服务器配置
		• 内存：8GB • 硬盘空间：120GB 说明 请选用 PC Server。	32G(4*8G)-3*300G(双6Gbps SAS 端口)-DVDRW-1*集成四口千兆网卡-1*四口千兆网卡-ServeRAID M5110e(512M)电池保护-机架式-2*750W HE(1+1)-100V~240VAC • Tecal RH2288 V2-BC1M12SRSB-eSight M(2*E5-2640 CPU,4*8G,3*300G SAS 2.5,4*GE LOM,1*4*GE NIC,SR320BC+电池,2*750W 电源)
	2000-5000 节点	• CPU：2*四核 2G 以上 • 内存：16GB • 硬盘空间：250GB 说明 请选用 PC Server。	
专业版	0-200 节点（管理平台 + 设备管理，不包括增值组件）	• CPU：1*双核 2G 以上 • 内存：4GB • 硬盘空间：40GB 说明 请选用 PC Server。	• X3650 M4-1*E5-2640 6c2.5GHz 或以上-8G(2*4G)-2*300G(双6Gbps SAS 端口)-DVDRW-1*集成四口千兆网卡-ServeRAID M5110e(512M)带电池保护功能-无显示器-2*750W HE(1+1)-100V~240VAC • Tecal RH2288 V2-BC1M13SRSB-eSight S(2*E5-2640 CPU,2*4G,2*300G SAS 2.5,4*GE LOM,SR320BC+电池,DVD-RW,2*750W 电源)
	200-500 节点（管理平台 + 设备管理，不包括增值组件）	• CPU：2*双核 2G 以上 • 内存：4GB • 硬盘空间：60GB 说明 请选用 PC Server。	
	500-2000 节点	• CPU：2*四核 2G 以上 • 内存：8GB • 硬盘空间：120GB 说明 请选用 PC Server。	• X3650 M4-2*Xeon 6C E5-2640 2.5G 或以上-32G(4*8G)-3*300G(双6Gbps SAS 端口)-DVDRW-1*集成四口千兆网卡-1*四口千兆网卡-ServeRAID M5110e(512M)电池保护-机架式-2*750W HE(1+1)-100V~240VAC • Tecal RH2288 V2-
	2000-5000 节点	• CPU：2*四核 2G 以上 • 内存：16GB • 硬盘空间：250GB	

版本	管理规模	服务器配置要求	发货服务器配置
		说明 请选用 PC Server。	BC1M12SRSB-eSight M(2*E5-2640 CPU,4*8G,3*300G SAS 2.5,4*GE LOM,1*4*GE NIC,SR320BC+电池,2*750W 电源)
	5000-20000 节点	• CPU：4*四核 2G 以上 • 内存：32GB • 硬盘空间：320GB 说明 请选用 PC Server。	• X3850 X5-4*Xeon 8C E7-4820 2.0G 或以上-64G(8*8G)-8*300G-DVDRW-1*集成双口千兆网卡-1*双口千兆网卡-1*4 口千兆网卡-ServeRAID M5015(512M)-iMM 系统管理卡-3Y5*8-2*1975W(1+1)-100V~240VAC • Tecal RH5885 V2-CH91M05RGPU-eSight L(4*E7-4820 CPU,8*8G,8*300G SAS,4*GE LOM,1*4*GE NIC,RAID 卡+电池,DVDRW,2*3000W 电源)

说明
- eSight 基础管理指：管理平台 + 设备管理（网络设备、UC、TP、IVS、存储、主机、eLTE 终端管理 ）+ WLAN 管理 + nCenter 管理 + MPLS VPN/MPLS Tunnel 管理 + SLA 管理 + IPSec VPN 管理 + 安全策略管理
- 管理节点数折算：终端设备（IP 话机、eLTE 终端设备） 1:5 ，存储高端设备 160:1，存储中端设备 40:1，存储低端设备数 10:1，存储异构设备 10:1，其他设备 1:1

表5-3 eSight 基础管理 + 存储报表管理

管理规模	服务器配置要求	发货服务器配置
0-500 节点	• CPU：2*四核 2G 以上 • 内存：8GB • 硬盘空间：120GB 说明 请选用 PC Server。	• X3650 M4-2*Xeon 6C E5-2640 2.5G 或以上-32G(4*8G)-3*300G(双 6Gbps SAS 端口)-DVDRW-1*集成四口千兆网卡-1*四口千兆网卡-ServeRAID M5110e(512M)电池保护-机架式-2*750W HE(1+1)-100V~240VAC
500-2000 节点	• CPU：2 * 6 核 2.5G 以上	

管理规模	服务器配置要求	发货服务器配置
	• 内存：16GB • 硬盘空间：250GB 说明 请选用 PC Server。	• Tecal RH2288 V2-BC1M12SRSB-eSight M(2*E5-2640 CPU,4*8G,3*300G SAS 2.5,4*GE LOM,1*4*GE NIC,SR320BC+电池,2*750W 电源)
2000-5000 节点	• CPU：2 * 6 核 2.5G 以上 • 内存：24GB • 硬盘空间：250GB 说明 请选用 PC Server。	
5000-20000 节点	• CPU：4*四核 2G 以上 • 内存：32GB • 硬盘空间：320GB 说明 请选用 PC Server。	• X3850 X5-4*Xeon 8C E7-4820 2.0G 或以上-64G(8*8G)-8*300G-DVDRW-1*集成双口千兆网卡-1*双口千兆网卡-1*4 口千兆网卡-ServeRAID M5015(512M)-iMM 系统管理卡-3Y5*8-2*1975W(1+1)-100V~240VAC • Tecal RH5885 V2-CH91M05RGPU-eSight L(4*E7-4820 CPU,8*8G,8*300G SAS,4*GE LOM,1*4*GE NIC,RAID 卡+电池,DVDRW,2*3000W 电源)

表5-4 eSight 基础管理 + 网络流量分析管理

组合	管理规模	服务器配置要求	发货服务器配置
• 组合 1：eSight 基础管理 + 网流分析 + 网流采集器同机部署 • 组合 2：eSight 基础管理 + 网流分析同机部署，不含采集器 说明 两种场景配置要	• 基础网管：0-500 节点 • 网流：0-10 节点(2000 FLow/S)	• CPU：2*四核 2G 以上 • 内存：8GB • 硬盘空间：120GB 说明 请选用 PC Server。	• X3650 M4-2*Xeon 6C E5-2640 2.5G 或以上-32G(4*8G)-3*300G(双 6Gbps SAS 端口)-DVDRW-1*集成四口千兆网卡-1*四口千兆网卡-ServeRAID M5110e(512M)电池保护-机架式-2*750W HE(1+1)-100V~240VAC • Tecal RH2288 V2-BC1M12SRSB-eSight M(2*E5-2640 CPU,4*8G,3*300G SAS 2.5,4*GE LOM,1*4*GE
	• 基础网管：500-2000 节点 • 网流：0-10 节点(2000	• CPU：2*四核 2G 以上 • 内存：16GB • 硬盘空间：250GB	

组合	管理规模	服务器配置要求	发货服务器配置
求一致	FLow/S)	说明 请选用 PC Server。	NIC,SR320BC+电池,2*750W 电源)
	• 基础网管：2000-5000 节点 • 网流：0-10 节点(2000 FLow/S)	• CPU：4*四核 2G 以上 • 内存：32GB • 硬盘空间：320GB 说明 请选用 PC Server。	• X3850 X5-4*Xeon 8C E7-4820 2.0G 或以上-64G(8*8G)-8*300G-DVDRW-1*集成双口千兆网卡-1*双口千兆网卡-1*4 口千兆网卡-ServeRAID M5015(512M)-iMM 系统管理卡-3Y5*8-2*1975W(1+1)-100V~240VAC • Tecal RH5885 V2-CH91M05RGPU-eSight L(4*E7-4820 CPU,8*8G,8*300G SAS,4*GE LOM,1*4*GE NIC,RAID 卡+电池,DVDRW,2*3000W 电源)
网流采集器独立部署	0-100 节点 (0-10000flows/s)	• CPU：1*四核 2G 以上 • 内存：4GB • 硬盘空间：120GB 说明 请选用 PC Server。	• X3650 M4-1*E5-2640 6c2.5GHz 或以上-8G(2*4G)-2*300G(双 6Gbps SAS 端口)-DVDRW-1*集成四口千兆网卡-ServeRAID M5110e(512M)带电池保护功能-无显示器-2*750W HE(1+1)-100V~240VAC • Tecal RH2288 V2-BC1M13SRSB-eSight S(2*E5-2640 CPU,2*4G,2*300G SAS 2.5,4*GE LOM,SR320BC+电池,DVD-RW,2*750W 电源)
	100-350 节点 (10000-30000flows/s)	• CPU：2*四核 2G 以上 • 内存：16GB • 硬盘空间：250GB 说明	• X3650 M4-2*Xeon 6C E5-2640 2.5G 或以上-32G(4*8G)-3*300G(双 6Gbps SAS 端口)-DVDRW-1*集成四口千兆网卡-1*四口千兆网卡-ServeRAID

组合	管理规模	服务器配置要求	发货服务器配置
		请选用 PC Server。	M5110e(512M)电池保护-机架式-2*750W HE(1+1)-100V~240VAC • Tecal RH2288 V2-BC1M12SRSB-eSight M(2*E5-2640 CPU,4*8G,3*300G SAS 2.5,4*GE LOM,1*4*GE NIC,SR320BC+电池,2*750W 电源)

说明
基础网管管理设备数超过 5000 时，网流采集组件必须分机部署。

表5-5 eSight 基础管理 + 存储报表 + 网络流量分析管理

组合	管理规模	服务器配置要求	发货服务器配置
• 组合 1：eSight 基础管理 + 网流分析 + 网流采集器同机部署 • 组合 2：eSight 基础管理 + 网流分析同机部署，不含采集器 说明 两种场景配置要求一致	• 基础网管：0-2000 节点 • 网流：0-10 节点(2000 FLow/S)	• CPU：2*四核 2G 以上 • 内存：24GB • 硬盘空间：250GB 说明 请选用 PC Server。	• X3650 M4-2*Xeon 6C E5-2640 2.5G 或以上-32G(4*8G)-3*300G(双 6Gbps SAS 端口)-DVDRW-1*集成四口千兆网卡-1*四口千兆网卡-ServeRAID M5110e(512M)电池保护-机架式-2*750W HE(1+1)-100V~240VAC • Tecal RH2288 V2-BC1M12SRSB-eSight M(2*E5-2640 CPU,4*8G,3*300G SAS 2.5,4*GE LOM,1*4*GE NIC,SR320BC+电池,2*750W 电源)
	• 基础网管：2000-5000 节点 • 网流：0-10 节点(2000 FLow/S)	• CPU：4*四核 2G 以上 • 内存：32GB • 硬盘空间：320GB 说明 请选用 PC Server。	• X3850 X5-4*Xeon 8C E7-4820 2.0G 或以上-64G(8*8G)-8*300G-DVDRW-1*集成双口千兆网卡-1*双口千兆网卡-1*4 口千兆网卡-ServeRAID M5015(512M)-iMM 系统管理卡-3Y5*8-2*1975W(1+1)-100V~240VAC • Tecal RH5885 V2-

组合	管理规模	服务器配置要求	发货服务器配置
			CH91M05RGPU-eSight L(4*E7-4820 CPU,8*8G,8*300G SAS,4*GE LOM,1*4*GE NIC,RAID 卡+电池,DVDRW,2*3000W 电源)
网流采集器独立部署	0-100 节点 (0-10000flows/s)	• CPU：1*四核 2G 以上 • 内存：4GB • 硬盘空间：120GB 说明 请选用 PC Server。	• X3650 M4-1*E5-2640 6c2.5GHz 或以上-8G(2*4G)-2*300G(双 6Gbps SAS 端口)-DVDRW-1*集成四口千兆网卡-ServeRAID M5110e(512M)带电池保护功能-无显示器-2*750W HE(1+1)-100V~240VAC • Tecal RH2288 V2-BC1M13SRSB-eSight S(2*E5-2640 CPU,2*4G,2*300G SAS 2.5,4*GE LOM,SR320BC+电池,DVD-RW,2*750W 电源)
	100-350 节点 (10000-30000flows/s)	• CPU：2*四核 2G 以上 • 内存：16GB • 硬盘空间：250GB 说明 请选用 PC Server。	• X3650 M4-2*Xeon 6C E5-2640 2.5G 或以上-32G(4*8G)-3*300G(双 6Gbps SAS 端口)-DVDRW-1*集成四口千兆网卡-1*四口千兆网卡-ServeRAID M5110e(512M)电池保护-机架式-2*750W HE(1+1)-100V~240VAC • Tecal RH2288 V2-BC1M12SRSB-eSight M(2*E5-2640 CPU,4*8G,3*300G SAS 2.5,4*GE LOM,1*4*GE NIC,SR320BC+电池,2*750W 电源)

表5-6 eSight 基础管理 + 基础设施管理

管理规模	服务器配置要求	发货服务器配置
0-500 节点	• CPU：2*四核 2G 以上 • 内存：8GB • 硬盘空间：120GB。 说明 请选用 PC Server。	• X3650 M4-2*Xeon 6C E5-2640 2.5G 或以上-32G(4*8G)-3*300G(双 6Gbps SAS 端口)-DVDRW-1*集成四口千兆网卡-1*四口千兆网卡-ServeRAID M5110e(512M)电池保护-机架式-2*750W HE(1+1)-100V~240VAC • Tecal RH2288 V2-BC1M12SRSB-eSight M(2*E5-2640 CPU,4*8G,3*300G SAS 2.5,4*GE LOM,1*4*GE NIC,SR320BC+电池,2*750W 电源)
500-5000 节点	• CPU：2*6 核 2.5G 以上 • 内存：16GB • 硬盘空间：250GB。 说明 请选用 PC Server。	

表5-7 全组件同机部署配置（基础管理 + 存储报表管理 + 网流分析管理），不含基础设施管理

管理规模	服务器配置要求	发货服务器配置
• 基础网管：0-200 节点 • 网流：0-10 节点（2000 Flow/s）	• CPU：2*4 核 2G 以上 • 内存：16GB • 硬盘空间：4T（可用硬盘空间推荐 3TB） 说明 请选用 PC Server。	• Tecal RH2288H V2-BC1M67SRSG-单机服务器 RH2288H V2(2*E5-2640 CPU,4*8GB 内存,2*1TB SATA 硬盘,4*GE,SR320BC-512MB+电池,2*750W AC 电源) • 服务器产品-BC1HDD66-硬盘-1TB-SATA-7200rpm-3.5"-64M • 服务器产品-BC1HDD67-硬盘-2TB-SATA-7200rpm-3.5"-64M • 服务器产品-BC1HDD68-硬盘-3TB-SATA-7200rpm-3.5"-64M

5.3 客户端配置要求

eSight Web 客户端对操作系统没有特殊要求，对浏览器版本以及内存需要如下条件：

- 浏览器版本：IE 8/9、Firefox 22。

说明
推荐 IE 9、Firefox 22。

- 内存：至少 1G 以上

5.4 网络带宽要求

为了保障 eSight 系统正常运行，网络带宽必须满足基本的带宽要求。

在大规模网络管理（管理 20000 节点、接入 100 客户端）的环境下，eSight 系统对客户端的接入带宽要求为 512 kbit/s，对服务器端的接入带宽要求为 30 Mbit/s。

6 技术指标

介绍 eSight 系统的技术指标。

eSight 系统最多可管理 20000 个网元，最多可支持 100 个客户端同时在线。

表6-1 技术指标

指标项	指标值
当前告警存储容量(条)	2 万
历史告警存储容量(条)	1500 万
事件告警存储容量 (条)	200 万
审计日志存储容量(条)	300 万
告警处理能力(条/秒)	100
单个子网支持拓扑对象个数(个)	500
拓扑管理支持的拓扑对象最大层数(层)	11

7 遵从的标准和协议

介绍 eSight 系统遵从的标准和协议。

- 与设备的接口遵从 SNMP、MIBII 标准
  - RFC1155 基于 TCP/IP 的互联网管理信息的结构和标识。
  - RFC1157 基于简单网络管理协议 SNMP。
  - RFC1213 基于 TCP/IP 的互联网的网络管理信息库 MIB-II。
- XML 1.0
- ITU-T X.733 故障管理规范
- JSR-286 Portlets 规范： the Java Portlet specification v2.0
- HTTP/1.0|HTTP/1.1：超文本传输协议
- HTTPS：超文本传输安全协议
- 会话初始化协议（SIP） RFC3261
- TCP 传输控制协议 RFC0872
- TCP、UDP 用户数据包协议 RFC1356
- SMI-S 存储管理建议规范
- Modbus 协议

A 术语

术语	解释
A	
安全日志	记录用户在 eSight 上进行的安全操作（如登录 eSight、修改密码和退出 eSight）的日志信息。
AAA	Authentication, Authorization and Accounting：一个用于配置认证、授权和计费的机制。认证是指对用户的身份与可使用的网络服务进行确认；授权（Authorization）是指依据认证结果开放网络服务给用户；计费是指记录用户对各种网络服务的用量并提供给计费系统。
ACL	Access Control List：访问控制列表
B	
NBI	NorthBound Interface：北向接口。连接上级网管系统和设备的接口，用于实现发放业务、上报告警、上报性能指标数据等功能。
B/S	browser/server：浏览器/服务器模式
被屏蔽告警	在告警相关性分析中，相关性动作被设置为屏蔽的告警。
C	
CLI	Command Line Interface：命令行接口，以命令行的方式对云存储系统进行管理。
CPU	Central Processing Unit：中央处理器。
CPE	Customer Premises Equipment：用户驻地设备
CWMP	CPE WAN Management Protocol：CPE 广域网管理协议
采集周期	测量结果每隔多长时间输出一次。在任务运行的测量时段内，eSight 将以选定的周期为粒度进行测量并输出结果。

术语	解释
操作日志	记录操作事件的信息表。
D	
单点登录	对于多个相关但又相互独立的软件系统的访问控制的属性。单点登录允许用户登录一次，就可访问所有的软件系统。
E	
eLTE	Enterprise Long Term Evolution
ESN	Equipment Serial Number：设备序列号。
eWL	Enterprise Wireless：企业无线。
F	
FTP	File Transfer Protocol：文件传输协议。
G	
告警	设备或 eSight 轮询发现故障时所上报的信息，每个告警都对应的有恢复告警，收到恢复告警后，告警提示将显示为恢复状态。
告警板	客户端界面上显示的一个面板，以不同颜色框及统计数据方式显示 eSight 当前告警数据。通过告警板可以实时监视全网的告警，了解所发生告警的级别及相应的统计数据。
告警定位	用户选中一条告警，通过该功能可以将显示的焦点定位到产生该告警的拓扑对象。
告警屏蔽	一种管理告警的方法，网管不显示指定对象的告警或不监视某些不重要的网管告警。
故障	某一功能无法按指定操作正常实现。不包括由于预防性维护和外部资源缺乏以及故意设定造成的无法操作。
高可用性	通常指采用主、备两个相同的模块以热备份的方式完成指定功能，以提高可靠性的方式。在主用模块故障时，备用模块会自动接替主用模块执行系统功能。
管理域	管理域是指用户可以管理的物理资源和逻辑资源，或者用户所属用户组可以管理的指定区域。
H	
HTTP	Hypertext Transfer Protocol：超文本传输协议

术语	解释
HTTPS	Hypertext Transfer Protocol Secure：超文本传输安全协议
I	
ICT	information and communications technology：信息和通信技术
IDC	Internet Data Center：Internet 数据中心
iEMP	Intelligent Enterprise Management Platform：企业运营维护系统。
IP	Internet Protocol：传输控制协议/互联网协议。
IP PBX	IP private branch exchange：IP 的企业小型交换网
IPMI	ntelligent Platform Management Interface：智能平台管理接口
ITU-T	International Telecommunication Union-Telecommunication Standardization Sector：国际电联电信标准化部门。
IVS	intelligent video system：智能视频系统
J	
加密	一种变换数据的功能，目的是掩藏信息内容从而防止未经授权的使用。
K	
KVM	keyboard, video, and mouse：键盘，显示器，鼠标三合一
客户端	发送请求，接收响应，从服务器端获取服务的通讯设备。
L	
LDAP	Lightweight Directory Access Protocol：轻型目录访问协议
LLDP	Link Layer Discovery Protocol：链路层发现协议
LUN	logical unit number：逻辑单元号
M	
MAC	Media Access Control：媒体接入控制
MCU	multipoint control unit：多点控制单元
MGC	media gateway controller：媒体网关控制器
MIB	management information base：管理信息库

术语	解释
MPLS	management information base：多协议标记交换
MPLS VPN	multi-protocol label switching virtual private network：利用 MPLS 构造的虚拟私有网
明文	指密码术中被加密之前的文本内容。
N	
南向接口	连接下级网管系统和设备的接口，用于实现发放业务、传输性能指标数据等功能。
鸟瞰图	eSight 物理拓扑视图中的一个浮动窗口，以缩略图的方式显示当前拓扑视图的全貌。
O	
OSS	Operating Support System：运营支撑系统。
P	
PnP	plug and play：即插即用标准
PUE	power usage effectiveness：能源使用效率
Q	
QoS	quality of service：服务质量
R	
RADIUS	Remote Authentication Dial-In User Service：拨号用户远程认证服务
RAID	redundant array of independent disks：独立磁盘冗余阵列
RSA	Revist-Shamir-Adleman Algorithm：RSA 加密算法。
S	
SAN	storage area network：存储区域网络
SFTP	Secure File Transfer Protocol：安全文件传输协议。
SLA	service level agreement：服务水平协议
SNMP	Simple Network Management Protocol：简单网络管理协议。

术语	解释
SOAP	Simple Object Access Protocol：简单对象访问协议。
SSH	Secure Shell：安全外壳
SSL	Secure Sockets Layer：安全套接层
STelnet	Secure Shell Telnet：安全 Telnet
事件	被管对象发生的任何情况的通称。例如对象的增加、删除、修改、状态改变等。
数据备份	将重要数据拷贝到备用存储区中的方法，用以防止原存储空间损坏或崩溃。
T	
TCP	Transmission Control Protocol：传输控制协议。
TFTP	Trivial File Transfer Protocol：简单文件传输协议
拓扑对象	eSight 拓扑视图中的基本元素，包括子图、节点和链接（连接）等。
拓扑视图	人机交互界面的一个基本组成部分。拓扑视图直观地显示网络的组网情况和网络中各网元、子网的告警、通讯状态，反映网络运行的基本情况。
U	
UC	unified communication：统一通信业务
UDP	User Datagram Protocol：用户数据报协议。
V	
VLAN	Virtual Local Area Network：虚拟本地局域网
VMM	virtual machine manager：虚拟机管理
VPN	virtual private network：虚拟专用网
VTC	virtual teller center：虚拟柜员中心
VTM	virtual teller machine：虚拟柜员机
W	
WLAN	wireless local area network：无线局域网
网元	网元即网络单元，包含硬件设备及运行其上的软件。通常一个网络单元至少具有一块主控板，负责整个网络单元的管理和监控。

术语	解释
	主机软件运行在主控板上。
网络流量采集器	一个运行于 Unix 或者 Windows 上的应用程序，负责接收和处理来自 NTE（Network Traffic Exporter）的 UDP 报文，然后将统计数据发送到 NTA 进行进一步的分析。
物理视图	用来呈现网络中所有设备以及拓扑划分（例如按照地域、维护关系等）的缺省视图。
X	
XML	eXtensible Markup Language：可扩展标记语言。
系统日志	系统日志追踪包括启动、关闭，及硬件和控制器故障在内的各种系统事件。
性能告警	当测量指标实测数据满足预设的阈值逻辑表达式或超过预设的梯度阈值时，系统产生的告警。
虚拟链路	eSight 拓扑图中表示拓扑对象之间逻辑连接关系的连接。
虚拟网元	虚拟网元是指整个网络中不能通过 eSight 进行管理的网元的映射。虚拟网元在视图上的显示与实际网元一样是采用图标显示，但它只是一个根据实际情况模拟的网元，不代表一个实际网元，所以不能查询该网元的实际状态，和通过颜色等来显示其告警状态。
Z	
转储	将存在于某个系统中的数据转存到另一个系统或介质中，并且将被转储的数据从原系统中删除。
子网	可以按照某种原则（如按地域划分）将一个比较大的网络结构分解为几个相对较小的网络结构，以方便操作员对网络的管理。在拓扑视图中，把这种相对较小的网络结构称为子网。