RG-WIS云网

技术白皮书

如有疑问
扫一扫在线咨询

Ruijie Networks 锐捷

目录

Ruijie 锐捷 Networks

2020-2021中国云管理网络市场接入量第一

数据来源： CCW，2022Q3

WIS云管理网络

800万+ 在线设备，**30000+** 客户接入

累计服务**13亿**的终端

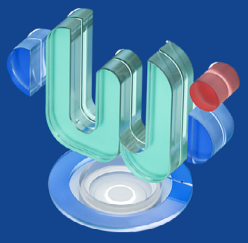
数据来源: WIS云，2023年3月

Wi-Fi魔盒

覆盖全球**100多个**国家和地区

Wi-Fi检测工具**下载量和日活第一**

数据来源: 友盟，2023年3月



识别左侧二维码 ▶
获取更多资料

概述

WIS云管理网络方案（以下简称WIS云网）基于大数据、云计算、人工智能等技术，提供采购、规划、部署、验收、运营的全生命周期云管理网络服务，致力提高网络建设和运维管理效率。同时，WIS云网还提供了丰富的开放接口，支持公有云、私有云等部署方式，帮助企业机构更好地运营管理网络，助力数字化转型。

网络业务的变化趋势

近些年，全球企业机构在持续地推进数字化转型，进一步拥抱云计算、移动连接、大数据分析以及物联网（IoT）部署等技术。在网络层面的变化具体表现在以下三个方面：

- 终端数量的急剧增长。2021年，IoT Analytics预计全球联网的物联网设备数量将增长9%，达到123亿个活跃终端。此外，网络业务呈现多样化和复杂化，智能装备、数字化办公、生产、视频监控等终端通过Wi-Fi等方式接入到网络中，增加了网络的管理运维难度。与此同时，IT人员数量却没有显著增加，管理运维人员负担越来越重。
- 网络管理上云的趋势。Gartner估计到2025年，超过95%的新数字工作负载将被部署在云原生平台上，而在2021年这一比例只有30%。到2025年，超过85%的企业机构将接受云优先原则，并且如果不使用云原生架构和技术，他们将无法完全执行其数字战略。越来越多的企业选择依赖基于云的平台来管理网络。根据IDC的预测，目前超过 25%的 WLAN是通过云进行管理。
- 智能化技术在网络的应用。网络技术作为企业数字化的底座，服务于重要性与日俱增的应用程序和数据，它必须具备无处不在的实时遥测和可见性，以实现对网络安全事件提供更快的识别、隔离和自动化解决。企业需要掌握网络基础架构的自动化配置和弹性扩展，这样才能支持数字化业务的动态变化，同时，企业在网络部署后，需要对可能影响网络可用性和性能的问题，提供更快的故障解决和修复服务。

传统的网络架构，难以高效地处理这些对企业有关键意义的技术问题，因此目前企业都在寻求网络转型，以确保能满足数字化业务的需求。

网络管理面临的挑战

管理成本高

传统网络管理面临着管理难的问题，如很多网管系统使用SNMP读取设备数据，在跨广域网时无法访问到设备，而且实时性较差，无法实现高精度采集。对于大型园区和多分支连锁企业，整网上万台的设备接入量，也超过传统网管的管理能力。另外，为了管理有线、无线、出口、安全等，需要部署多套专门的管理软件，对于企业来说成本较高，且难以维护。

网络服务少

好的网络从最初的采购阶段就需要专业人士来进行规划，整个生命周期过程中需要投入大量的人力资源。高昂的部署成本、学习成本、运维成本，都成为阻碍企业数字化转型的拦路虎，比如，不同的场景需要采购不同型号的设备，进行不同的网络优化策略；部署网络时，需要专业人士到现场进行开局调优等工作；日常运维中报障处理，配置变更等，都需要消耗大量专业IT资源……企业IT团队极其希望能从日常网络管理中解放出来，投入更多时间专注创新和提供业务价值。

运维排障难

稳定的网络，需要快速响应处理故障，需要持续不断的巨大投入。而传统的网络管理软件无法解决复杂网络优化、故障定位的问题，例如：传统网络优化需要专业人士在现场，不断地重复测试、观察、分析、调整全过程，整个优化工作周期长、效率低。除此之外，无线网络运维中的排障工作是又一难题，一方面，无线射频环境的不确定性，导致故障现场很难被保留和复现；另一方面，设备本地无法保存历史记录，这进一步提升了排障工作的难度。

网络扩展慢

企业的网络业务面临着快速变化的挑战。比如突然的疫情带来了混合办公模式，对网络业务和网络安全带来了新的变化。连锁门店的快速扩张，需要门店网络能快速地交付上线。直播、视频会议等业务的增加，对网络的体验带来了新的要求。这些都需要一个灵活的网络架构，能应对网络拓扑、性能容量、业务的快速变化。

WIS云管理网络介绍

WIS云管理网络是基于云的全新的网络部署和管理模式。在这种部署模式下，网络硬件仍然部署在本地，但管理功能迁移到了云端（一般指公有云），管理员可以在任意位置，通过Web页面或移动终端APP等图形化方式，对网络进行集中管理。

另外，WIS云网支持网络服务商将传统的网络架构中的管理、控制和运维功能移到云端，并将其转变为一项服务内容提供给不同的企业、组织，本地网络基础设施只提供数据转发能力，成为一种网络即服务的商业模式。

WIS云管理网络的优势

WIS云管理网络架构相比传统网络管理架构，具有以下优势：

- **分散到集中**

传统网络各分支之间独立部署，独立管理，而WIS云管理网络可以实现远程集中部署和管理，提升管理效率。

- **现场运维到随时随地运维**

传统网网络需要专业 IT 人员去现场，而WIS云管理网络可以跨越Internet 实现远程管理、远程运维和移动运维。

- **被动式响应到主动式预防**

传统的网络都是产生故障后，IT人员被动响应去处理。而借助WIS云管理网络的全流程数字化，可以做到数据留痕，并主动发现异常，将风险扼杀在摇篮中。

- **人工经验到数据智能**

传统的运维需要靠专业的IT人员去完成，开局、运维、故障处理都依赖人工经验。WIS云管理网络使用大数据和人工智能技术，通过机器学习来固化专业的经验，降低出错概率。

- **有限规模到弹性扩容**

传统网络的设备规模受网管平台可管理规格的限制，而WIS云管理网络使用大数据和云原生架构，可以实现弹性扩容，支撑百万级以上设备的管理。

WIS云管理网络关键价值

全生命周期服务

WIS云网提供对网络的采购、规划、部署、验收、运维的全生命周期智能网络管理服务，每个阶段都通过数字化、智能化工具进行赋能，例如在规划阶段的地勘仿真，部署阶段的移动端极简开局，验收阶段的一键报告，可实现快速远程交付和运维，极大地降低了企业无线网络的使用成本和门槛，节省了人力资源的投入，提高了网络建设和管理的效率。

全生命周期服务

全网云管理

WIS云网支持NetConf、TR069、MQTT等多种标准化配置或管理协议，实现对交换机、路由器、AP、AC、网关、防火墙、5G小站等多种设备跨广域网的一体化管控。支持对多分支网络进行设备添加、在线状态监控、下发配置、升级、重启、配置备份和恢复等丰富的远程运维操作，支持整网拓扑自动发现及拓扑状态监控，实现人、场、网、终端的云连接。

全网云管驾驶舱

智能运维

WIS云网告别传统的基于设备状态运维的思路，从用户网络使用体验的角度出发去构造运维的闭环，创新性地引入机器学习算法，使用大量样本数据度量不同场景下的网络体验，结合专家知识，从接入、认证、流量、应用、覆盖、漫游等多个维度分析体验差的原因。WIS云网还能主动监控到信号覆盖盲区、无线连接异常、上网体验异常、网络过度饱和等问题，帮助客户提前预防网络体验风险。

传统的运维方式，需要进行现场蹲点式的观察和问题复现，WIS云网平台在云端收集设备上报的所有数据，通过对特定时间、特定终端的信息、网络指标、流量等多维度的提炼和聚合，呈现可视化的故障信息（如故障类型、故障时间、故障原因等），同时支持进入专家模式下查看终端的原始数据。WIS云网忠实记录了所有终端，在过去时间里网络的完整运行情况，为故障定位提供了精准有效的信息，助力业务快速响应，节省人员投入和运维成本。

网络增值

WIS云网也是智能终端的连接平台，屏蔽安全、性能、可靠连接的复杂性，通过标准化的开放接口，赋能合作伙伴和客户。平台的南向可以定制对接纳管第三方网络设备、物联网终端，实现统一监控管理、终端识别等功能。平台的北向提供设备、终端、应用等数据接口和管理接口，支持对接第三方业务系统，满足客户的运营、管理维护、科研分析等需求。

技术原理

管理协议

WIS云网方案通过将控制器、分析器等网络管理功能部件部署在公有云上，实现整网设备的配置、监控、告警、升级等管理动作在云端即可完成。企业不再需要在本地部署软件和服务器，大大降低了IT成本。

WIS云网方案具备较好的兼容性，传统的本地管理模式，可通过简单配置后，实现快速切换为云管理网络模式，不需要更换设备或变更网络架构，可以较好地保护客户的原有设备投资。当设备无法接入公有云的平台时，也可以快速回退到本地管理模式。

为了更好地实现管理功能上云，WIS云网引入了CWMP、NETCONF、MQTT等新一代的网络管理技术，相比SNMP等传统的网管技术，新技术具备安全、可靠、易扩展、易操作、更开放等优点。

对比项	传统网管技术	云管理技术
管理方式	本地网管+远程登录管理	云端管理
部署方式	本地部署	云端部署
网管协议	SNMP	CWMP/MQTT/NETCONF
监控技术	SNMP	Telemetry
配置方式	eweb、Telnet	WEB、APP、 API
第三方对接	本地对接	云化应用
商业模式	软件License	服务订阅

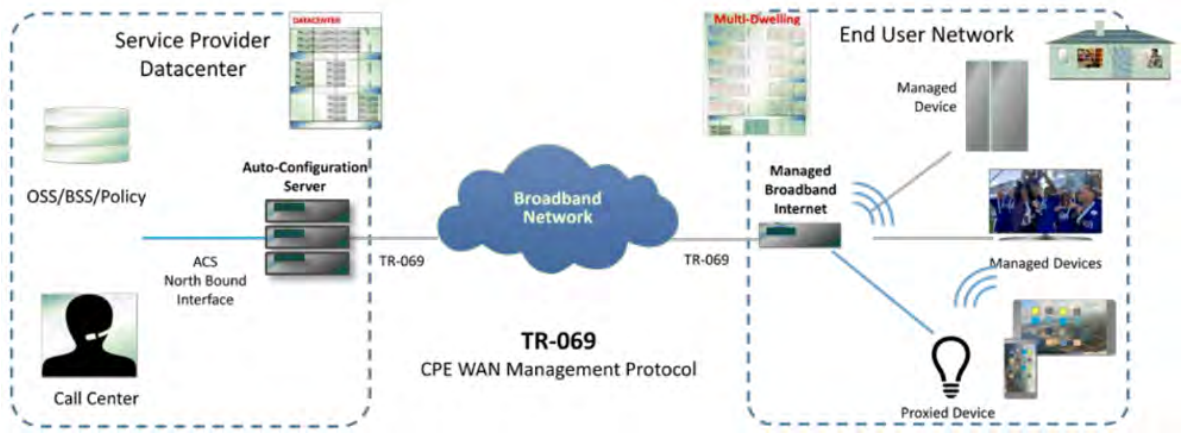
传统网管技术 VS 云管理技术

WIS云网通过模型抽象和消息层解耦，已实现应用层和协议层的解耦，可以同时支持拥有三种协议的设备进行管理运维。

CWMP

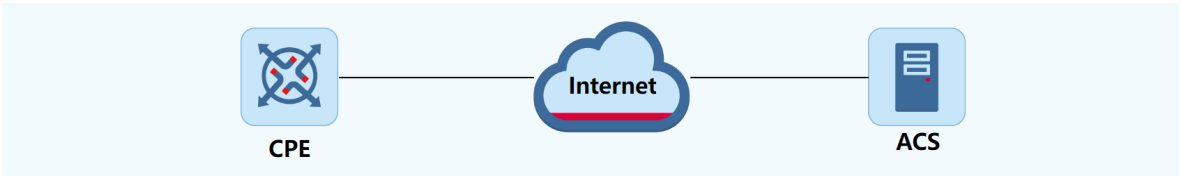
简介

CWMP（CPE WAN Management Protocol，CPE广域网管理协议），又称为TR-069协议，是由DSL（Digital Subscriber Line，数字用户线路）论坛发起开发的远程网络设备管理协议。CWMP协议可通过服务器对数量众多、分布较广的设备进行远程自动部署、配置和管理，可用于包括以太网在内的不同网络中。



CWMP管理协议模型

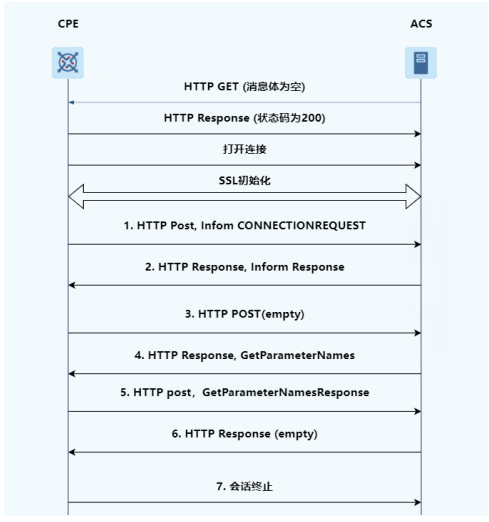
网络架构



CWMP网络模型包括：

- ACS：网络中的管理设备，可以完成对CPE设备的管理和维护操作。
- CPE：网络中的被管理设备。

工作原理



流程详细说明如下：

- CPE设备发起Inform请求，并说明该会话是由ACS要求而建立的；
- ACS返回Inform Response；
- CPE设备发起一条空的Http Post请求；
- ACS发起GetParameterNames要求，查询CPE设备的配置参数名称；
- CPE设备响应GetParameterNamesResponse，携带ACS指定查询的配置参数名称结果；
- ACS向CPE设备发送一条空的Http Post响应；
- CPE设备断开连接，该会话结束。

ACS可多次重复调用GetParameterNames方法。

■ 对设备的管理功能

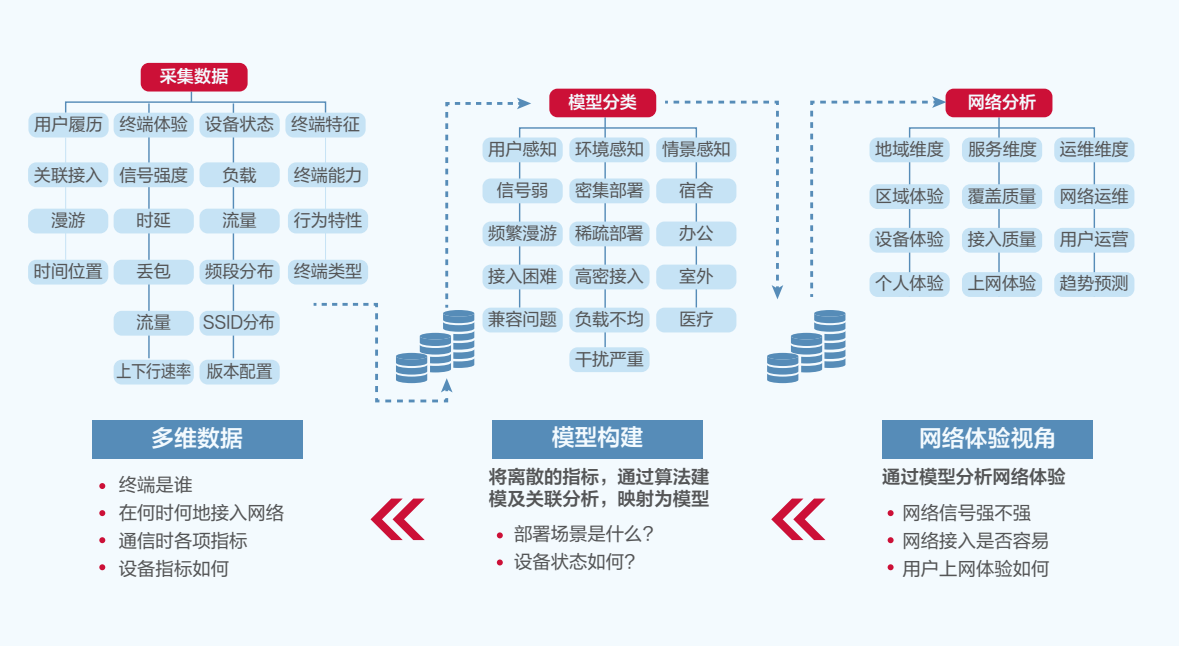
支持对多分支网络进行设备添加、在线状态监控、下发配置、升级、重启、配置备份和恢复等丰富的远程运维操作，支持整网拓扑自动发现及拓扑状态监控，实现人、场、网、终端的云连接。

■ 对设备的管理功能

企业分支连接互联网。在企业总部和分支间部署CWMP协议，分支作为CPE设备，企业总部通过ACS完成对分支设备的控制和管理。ACS与分支设备建立连接后，ACS支持对设备系统启动文件和配置文件的管理、对设备进行配置、对设备状态和性能进行监控并进行故障诊断。

体验可视化

“以用户体验为中心”的运维理念是WIS云网在业界首先提出的，它告别传统基于设备状态的运维方式，以一种更加贴近实际运维场景的方式进行。WIS云网从网络运营、故障定位等角度拆解出需要的上网体验分析模型，包括用户感知模型、环境感知模型、情景感知模型，进而结合遥测技术和AI技术，采集到用户的接入及漫游履历数据、终端的体验数据、设备的状态数据、终端的特征数据等数据指标用于训练感知模型。



体验运维模型

体验概览

WIS云网通过海量的数据积累和专家知识，化繁为简，抽象出六个维度来综合评估网络体验，用户可以直观地通过雷达图来判断当前网络是否存在风险。

■ 设备稳定度

通过周期性采样网络设备的性能参数和状态，检测作为网络基础的AP、AC设备是否存在掉线、CPU、内存等异常。

■ 信号覆盖度

通过体验预测中因信号覆盖原因导致的体验差数量，计算出整网无线网络的信号覆盖水平，是否存在风险。

■ 关联稳定度

根据终端的关联成功、关联异常、认证成功、认证异常、正常下线、异常下线、正常漫游、漫游异常等指标，计算出整网终端的接入成功率和正常下线率，得出无线网络是否易于连接。

■ 在线体验

根据体验预测算法计算出每个终端的在线体验，进而综合得出整网用户的体验水平。

■ 用户活跃度

根据用户的流量和上网时长，将用户划分为不活跃、轻微、轻度、中度、重度和骨灰级六种活跃程度，再根据不同活跃程度的占比和权重计算出整网联网终端的综合活跃水平。

■ 网络饱和度

根据信道利用率计算出各区域网络的拥塞程度，综合得出整网的饱和度，网络是否已经饱和。

体验可视化

终端体验感知

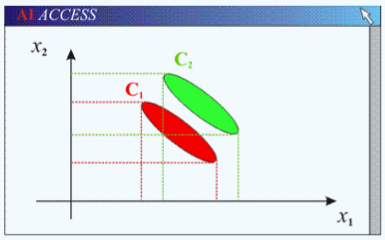
WIS云网将用户上网体验划分为以下代表性的应用场景：文字聊天、图片/网页、视频聊天，游戏、高清视频，传统体验感知情况如下表所示。

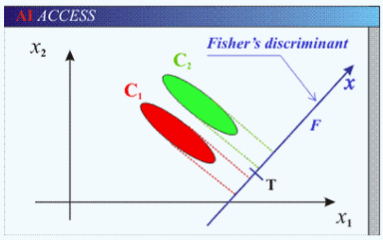
应用	最低时延	最低丢包	最低带宽	体验
文字聊天	100ms	8%	5Kbps	转圈可发出
图片、网页	80ms	5%	150Kbps	10s内可刷出
VOIP电话	70ms	2%	50Kbps	可通话
视频聊天	60ms	1%	70Kbps	可接受
游戏(LOL)	30ms	5%	8Kbps	基本接受
高清视频	20ms	3%	6Mbps	基本流畅

WIS基于机器学习算法——线性判别式分析（Linear Discriminant Analysis），简称为LDA。无线性能参数训练出评估模型，可直接度量无线使用体验，实验室数据精度达到90%以上。

- 线性判别式分析（Linear Discriminant Analysis），简称为LDA。也称为Fisher线性判别（Fisher Linear Discriminant，FLD），是模式识别的经典算法，在1996年由Belhumeur引入模式识别和人工智能领域，主要应用在人脸识别和图像识别。

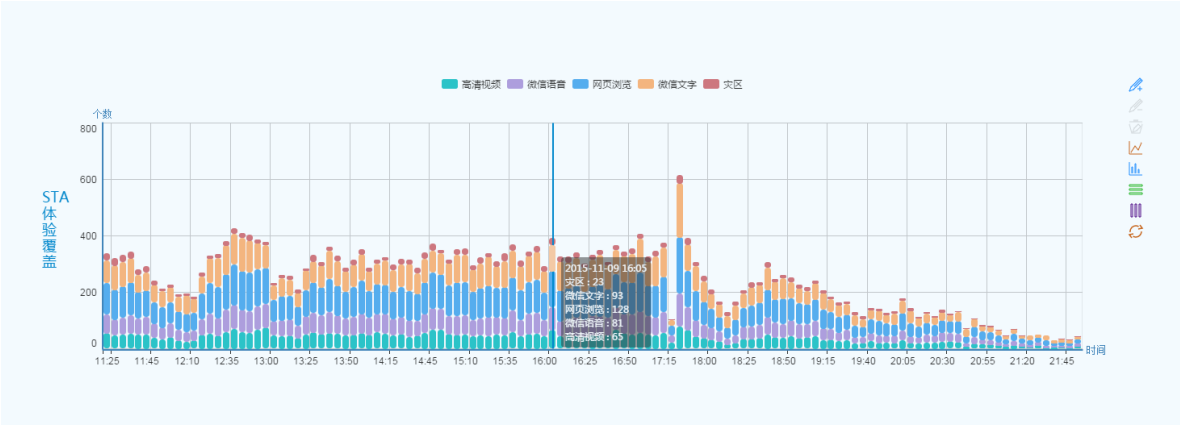
Rssi
上行速率
下行速率
信道利用率
底噪
时延
丢包





- 投影后模式样本的类间散布矩阵最大
- 类内散布矩阵最小
- → 模式在该空间中有最佳的可分离性

体验得分综合评估：将接入网络的每个终端的通信过程中的各类指标作为基础，评估成用户可感知的网络体验。其中指标包括信号强度、时延、丢包、流量、信道质量、接入过程等，而用户可感知的体验分为优质、良好、有点卡、上线难、不活跃；



不同应用的体验覆盖分析

体验问题原因

有线网络的运维管理一般围绕设备展开，而在无线网络中，设备的正常运转无法代表用户和业务体验的正常，看不透摸不着的无线总会出现各种复杂多样的体验问题，一般有以下原因：

■ 覆盖

有线是有界的，只要满足具体端口上网要求，而无线是无界的，信号传播越远，能量会不断向更多空间扩散，随着距离增加，单位面积的能量会逐渐地衰弱。由于障碍物的遮挡，部分信号产生反射和折射现象，信号强度会下降。不同区域可能受到障碍物和距离等因素的影响，信号变弱，从而引发体验变差。

■ 干扰

有线是独享的，而无线是开放共享的，由于信号的四处传播，无线设备间存在互相的影响。对于一个需要多台AP部署的网络，当网络规划不合理时，将导致AP之间互相干扰，从而影响终端体验。

■ 接入

接入过程的一半选择权在终端，终端差异化个性化造成的无法接入、掉线问题层出不穷。

■ 漫游

有的终端自身漫游判断机制不合理，即便移动远离了原有AP，仍然保持关联，随着通信的信号强度下降，无线体验急剧下降。

同时，规划部署不合理也可能导致终端即使静止不动，也会频繁在不同AP之间漫游，由于频繁切换带来的开销，可能出现掉线卡顿等现象。

■ 认证方面

AP和终端分别由不同的厂商开发，可能会遇到兼容性问题。

智能网优

传统无线网优

■ 划分信道

无线网络中的设备需要在802.11标准中规定的频段、规定的信道中接收、发送信号以实现通信。由于无线频谱资源有限，网络环境中的无线热点（AP）不可避免地将会重复使用信道。如果两个近距离的无线热点工作在同一个信道上，或者工作在频段存在重叠的两个相邻信道上，这时网络中将存在同频或者邻频干扰，同一个时刻只能有一个无线热点接、收发数据，因此它们将共享原来单个热点时的网络吞吐量。将有限的频谱资源分配给多个AP，进行信道规划，使得AP之间的干扰尽量小，是无线网络部署和运维的重要内容。

2.4G信道在非高密部署场景推荐采用1、6、11 共3个不重叠的信道进行规划，若为高密部署场景推荐采用1、5、9、13 共4个信道进行规划；5G信道推荐采用149、153、157、161、165，36、 40、44、48、52、56、60、64 共13个不重叠的信道进行规划；AP点位规划采用蜂窝状部署。

■ 调整功率

发射功率是指数据帧的传输功率，用于优化传输速率和控制干扰范围。功率过低，终端吞吐率下降，体验变差；而功率过高，又将对周边AP产生干扰，因此需要在高传输速率的同时，尽可能减少对周边AP的干扰。

绝大多数场景，在无线WLAN覆盖区域内95%以上信号强度应大于-75dBm，条件允许的情况下，边缘覆盖场强可以大于-70dBm，其中重点覆盖区域推荐信号强度控制在-40dBm~65dBm。边缘信号场强低于-75dBm时，只能满足最低无线接入需求；不同手机灵敏度不一样，检测结果有差别，信号跌落到-75dBm以下时，部分手机无法稳定地连接无线网络，容易掉线。

覆盖功率指beacon，probe response等帧的发射功率，主要是控制AP覆盖范围，用于优化终端的接入和漫游效果。当AP配置的beacon功率过高，覆盖过大时，容易导致终端出现远端关联或漫游粘滞，终端上网卡顿。合理的覆盖功率，能确保终端可优先接入近端最合适的AP，同时可在两个AP之间顺畅漫游，从而避免远端关联和漫游粘滞所导致的用户上网卡顿等问题。

■ 流量控制

目的合理利用带宽，减少大流量用户对其他用户的影响；针对不同的场景下WLAN的带宽需求开启每用户限速，避免AP下方网卡性能好的终端一直抢占信道导致网卡差的终端体验不好，也可减少隐藏节点造成的影响。

■ 清除干扰

无线干扰源，通常分为两种：802.11干扰源及非802.11干扰源。

802.11干扰源，主要来自802.11标准的WLAN设备，如家用无线路由器、其他公共Wi-Fi设备，通常建议与业主进行协调沟通，统一进行WLAN部署或设计规划，友好协商，避免相互干扰。比如，统一部署一套无线网络进行共享；如在信道资源规划时，相互协商，错开无线频段，比如楼上5G使用149-165信道，楼下使用36-64信道。

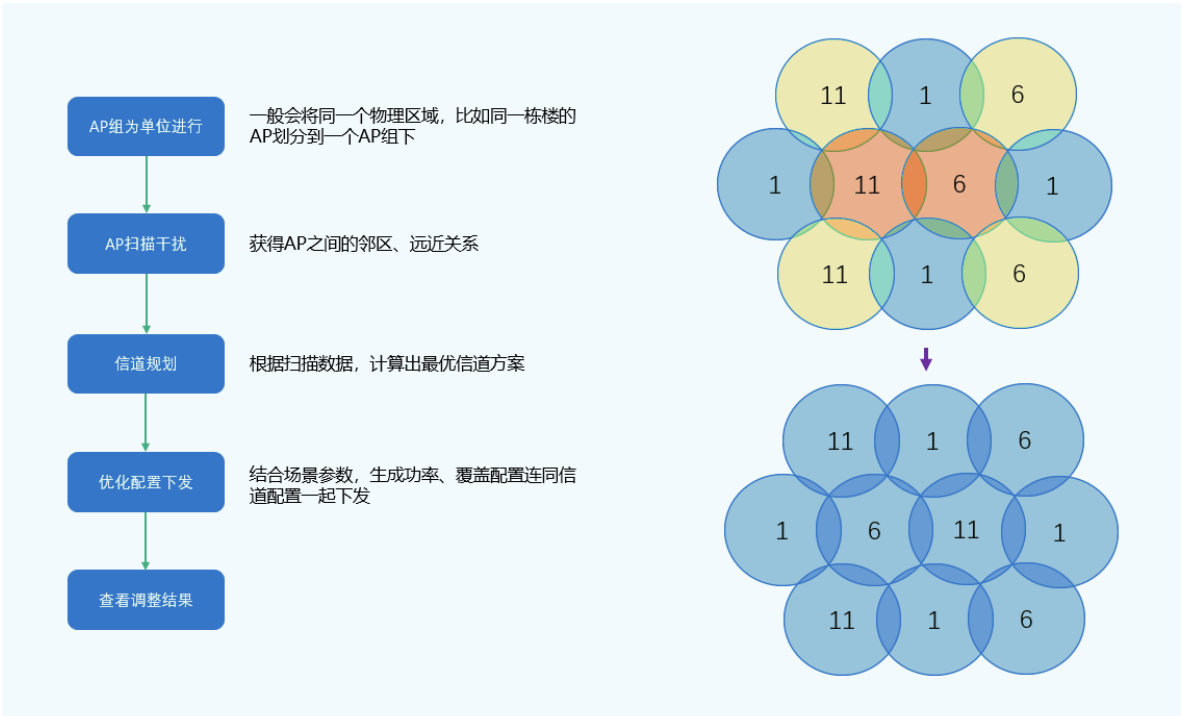
非802.11干扰源，是指工作在2.4Ghz或5Ghz频段的非WLAN设备，比如微波炉、蓝牙、微波治疗仪等。该类设备非802.11标准的设备，因此不会遵循CSMA/CA检测机制，不会主动退避，只要处于工作状态，就会强制占用空口，干扰Wi-Fi信号，造成无线体验下降。

传统的无线网优工作，需要由有丰富的工勘经验与网优经验的技术人员来执行，采取人工、手动的方式来进行规划和调优，工作量大、效率较低，尤其是在AP数量多、高密部署的情况下，需要频繁地跑现场、测点位、调整方案，而最终效果往往差强人意。一旦遇到环境（部署）发生变化，原有规划不再适用，又将产生一笔巨大的资源开销。

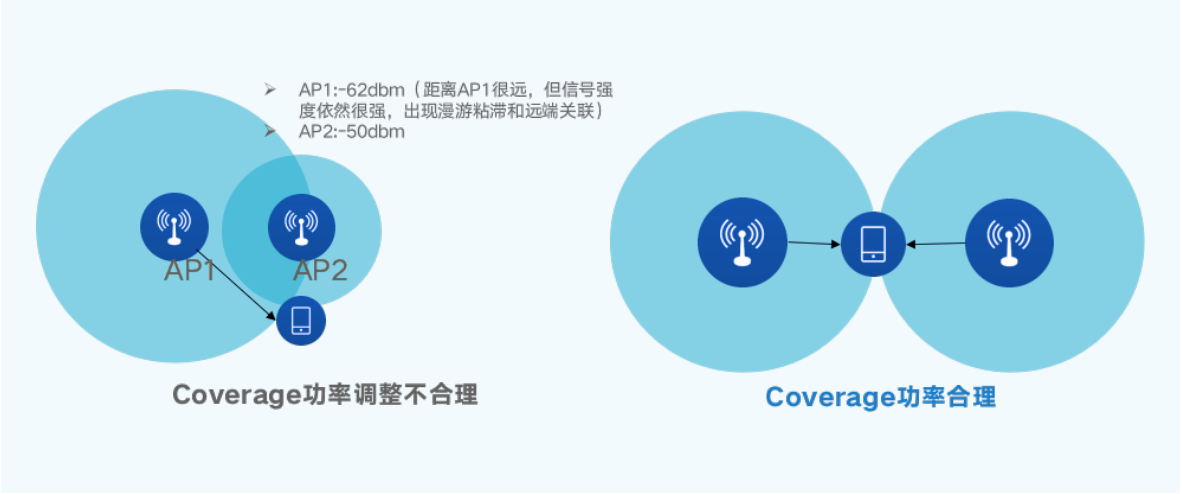
智能网优

WIS云网的智能网优功能，是基于multi-agent的无线接入点（Access Point, AP）信道分配算法，实现通过扫描全网AP及私设Wi-Fi，计算出所有设备之间相互干扰的水平，规划得出一套整网干扰水平最低的信道方案；后台计算引擎在执行信道规划的同时，结合大数据分析、专家经验以及当前网络负载等情况，给出不同场景下的最佳功率建议；同时，环境感知模块，自动收集全网干扰，将网络环境中的干扰风险和详情按用户容易理解的方式直观地呈现出来，帮助用户持续不断地感知环境、了解风险，针对问题主动出击。

■ 信道分配原理



■ 功率调整原理



WIS云网的智能网优功能，对整体网络进行准确地集中式信道分配和功率控制，主动发现干扰，对于减少网络运维的工作量、提高网络吞吐量、服务质量具有十分重要的意义。

用户触发一键智能网优功能后，系统将自动进行网络优化，系统工作流程大致如下：

- 深度体检
  经过深度体检扫描后，得到信号干扰数据（可基于场所开启扫描）
- 网络优化
  根据扫描数据，后台计算出符合各种场景的信道、功率、漫游参数、流控配置等优化方案（为确保优化方案的准确性，需要手动选择场所的所属场景）
- 下发优化配置
  优化配置生成后，将由WIS云网自动下发给设备（瘦AP模式下发到AC，胖AP模式直接下发给各AP）
- 完成后查看效果
  展示网优前后配置对比和干扰改善情况
  说明：因AP探测到的邻居信息（同频信号及其强度）变化较大，不同时刻进行网优效果可能会存在小幅波动；如果无线网络信道冲突较少，采用本方案调优的效果可能不明显。

智能网优方案支持以下调优方式：

- 手动模式：用户手动点击触发网优
- 定时模式：系统在指定的时间点进行无人值守的调优

效果

根据实验数据以及大量的实际客户数据反映执行WIS云网的智能网优功能后，单点STA性能提升2-15倍不等、整体性能提升20%-50%不等。

智能诊断

无线网络管理和运维的难点，在于无线的复杂性和不确定性，异常时有发生，如何及时发现、准确定位并快速解决这些异常，对无线网络的运维至关重要。

传统运维方式下，异常发现往往依赖于被动投诉，缺乏主动发现问题的手段。运维关注点也只是聚焦于设备参数，无法感知用户的真实体验和网络的实际性能。出现故障后，通常需要专业的IT人员到现场登陆设备查询日志、收集终端信息，可即使如此往往也难以精确复原故障场景，这就导致故障修复效率低下。

大数据时代，传统的运维方式已经无法支撑规模日益壮大的无线网络运营，自动化运维的重要性日益凸显。利用网络中的大量数据进行智能运维、提升运维效率，已刻不容缓。WIS云网一键巡检方案，目的正是为了解决无线网络传统运维的痛点，帮助用户及时发现问题、缓解运维压力、提高解决问题效率、改善网络体验。

终端诊断

无线用户使用过程偶发出现无法接入、掉线、卡顿等无线体验问题，运维人员或工程师很难抓到故障现象，且故障现象难复现，工程师需要花费大量时间精力去蹲点收集故障信息，导致无法及时定位和解决客户问题，该类问题的特性表现：

- 无线体验类问题通常是偶发性
- 故障现象的出现与现场环境有强相关性
- 具体关联的因素存在较大的不确定性
- 导致后续在相同环境、用相同步骤也难以复现故障现象

WIS引入终端接入诊断功能，实时收集终端接入过程数据，持续监控和分析终端的接入行为和探测行为，按照时间轴将终端接入过程图形化呈现回放，使得偶发性的接入故障能随时随地进行追溯。用户通过查看终端接入协议回放，可以看到每个接入过程的耗时、上线流畅度、关联认证情况、DHCP情况等，极大提升故障定位效率；

技术上，设备默认采集上报WIS的频率是5分钟； DHCP相关事件是从AP采集，其余事件是从AC采集。记录事件涵盖：

	关联	1X认证	RSNA握手	DHCP过程	上下线	漫游
1	AUTH	D1X_AUTH	RSNA_KEY_START	DHCP_DISCOVER	TSR_STA_DOWN	STA_UPDOWN_MODIFY
2	DEAUTH	D1X_DEAUTH	RSNA_KEY_SUCCESS	DHCP_OFFER		STA_ROAM_ADD
3	ASSOC_REQ	D1X_OFFLIN	RSNA_KEY_F_1_4	DHCP_REQUEST		STA_ROAM_MODIFY
4	ASSOC_RESP	D1X_AUTH_START	RSNA_KEY_F_2_4	DHCP_DECLINE		
5	AP_AUTH	D1X_REAUTH_START	RSNA_KEY_F_3_4	DHCP_ACK		
6	AP_DEAUTH	MAB_AUTH	RSNA_KEY_F_4_4	DHCP_NAK		
7	AP_DISASSOC	MAB_OFFLINE	RSNA_KEY_F_1_2	DHCP_RELEASE		
8	REASSOC_REQ	MAB_REAUTH	RSNA_KEY_F_2_2	DHCP_INFORM		

一键巡检

一键巡检方案，从以下3个维度对用户网络进行监控和诊断：

■ 设备问题

无线设备是无线网络的基石，设备稳定是用户体验的最根本保障。巡检内容包括：高CPU/内存占用、单AP频繁上下线、批量AP掉线

■ 配置异常

日常使用中，用户往往由于缺乏专业的网络运维知识和对无线网络的了解，对AC进行了不当的配置，例如：

- 用户开启了5G优先，结果导致实际2.4G用户接入缓慢（2.4G网卡扫描到无线信号耗时变长）。而实际上由于5G信道一般都是比较空闲的，所以大部分5G网卡可以自动关联到5G信号，所以如果不是5G终端较多或应用/环境要求，一般建议关闭5G优先功能；
- 用户配置了错误的AP工作模式，导致终端体验下降。实际上如果没有反制、频谱分析等功能需求，AP工作模式应当设置为normal；
- 用户未配置禁用低速率集，结果可能由于低速的使用，拖慢了整个空口的性能，导致终端体验下降。实际上，在信号覆盖正常且不是有特殊业务或终端需求的场景（如某些业务或终端只能使用/支持低速率报文，就不能禁用），建议禁用低速率报文以提升用户体验；
- DHCP地址池已经快用尽，而用户并未发觉，则新终端接入后可能存在无法获取IP地址的风险；

配置问题如以上等等，在此不一一列举。

■ 空口问题

由于无线空口环境的复杂多变，出现异常时的空口环境往往难以被用户察觉和记录，进行故障回溯尤为艰难。WIS云网提供对覆盖异常、空口繁忙、高干扰三个方面的持续巡检。

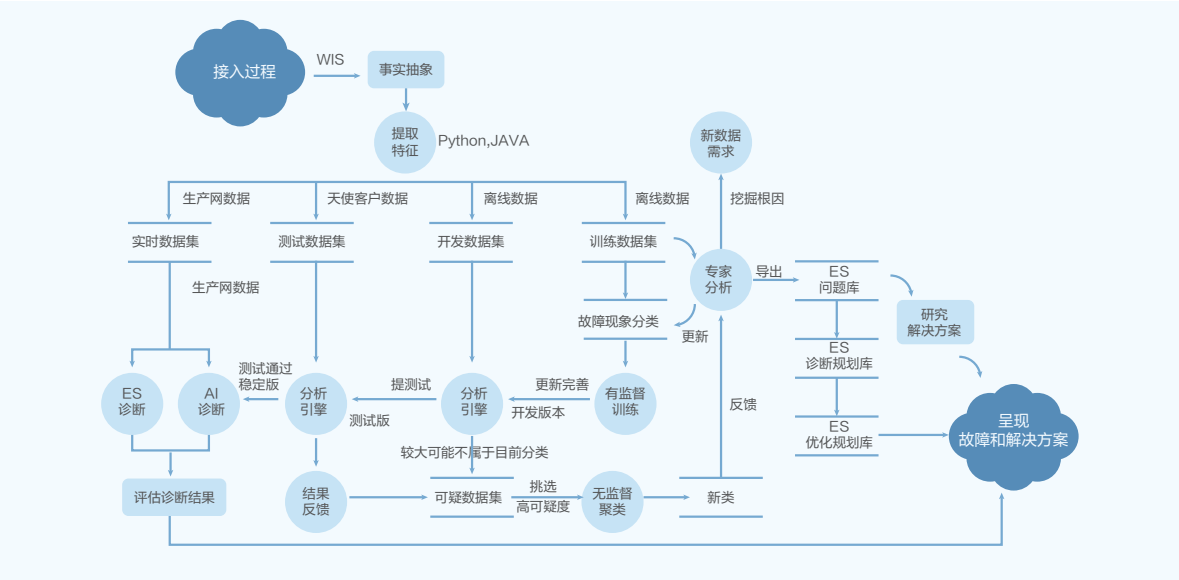
WIS云网综合以上维度的巡检结果，给出无线网优的综合健康指数得分，并针对发现的问题提供网优建议，适用于无线项目建设完成后的验收前自检，及无线运营过程的日常故障防范。

一键巡检提供两种巡检模式：

- 定期模式：系统自动在每日夜间对前一天的无线网络运行情况进行巡检（无需人工触发）。
- 实时模式：用户触发后，系统收集实时配置信息，立即对现网进行巡检。

故障诊断系统

WIS云网对体验故障构造了一个自动化的系统，持续扩充采集故障数据维度和故障规则，对应到设备、环境和终端侧强相关的特征数据，结合因子分析和专家知识库，实现持续更新的故障识别模型。在限定条件下，训练输出的模型，在10万组测试集上的准确率可达90%左右。使用训练好的模型，只要输入新的接入过程的报文信息，模型就能预测出其所属的故障类别。人工检验分类100万组数据的效果，其准确率还在95%左右。



自动化诊断模型

WLAN安全

安全威胁

随着黑客技术的提高，WLAN受到越来越多的威胁。配置无线基站的失误导致会话劫持，以及拒绝服务攻击(DOS)都像瘟疫一般影响着无线局域网的安全。无线网络不但因为基于传统有线网络TCP/IP架构而受到攻击，还有可能受到基于国际电气和电子工程师协会（IEEE）发行802.11标准本身的安全问题而受到威胁。典型的无线安全检测和防御场景分析包括钓鱼Wi-Fi、私设Wi-Fi、Wi-Fi攻击。为了更好地检测和防御这些潜在的威胁，我司提出安全雷达方案来解决这个问题。

安全雷达模型

■ 钓鱼Wi-Fi

无线网络的开放性使得攻击者能够利用简单的第三方工具、非常轻易地释放与企业网络相同的Wi-Fi信号，即钓鱼信号，一旦员工接入该信号就很可能造成内网账号、密码泄露。很多攻击者为了绕开传统WIDS只会检测相同SSID信号的防御手段，释放了一个极具迷惑性的SSID，例如本网络的信号名office-Wi-Fi，攻击者放出的钓鱼信号名为Office-Wi-Fi，员工稍不注意很可能被钓鱼成功，进而导致信息泄露。

钓鱼Wi-Fi 示意图

■ 私设Wi-Fi

员工出于扩展或建私网的目的，可能将普通家用路由器插入到公司内网有线口中，并释放私设Wi-Fi信号；另一方面，当前市面上360Wi-Fi、猎豹Wi-Fi等第三方软AP非常普遍，员工不经意间可能就将内网共享出去了。这些行为无疑将暴露公司内网，攻击者很可能连上私设Wi-Fi信号，并扫描内网服务器端口，窃取内网信息。传统的方式无法做到私设Wi-Fi的定位管理，最多只能给出私设信号所处的大致位置，实际定位管理存在很大难度。

私设Wi-Fi 示意图

■ Wi-Fi 攻击

目前，Wi-Fi攻击的成本越来越低，有很多开源的软件如aircrack-ng以及MDK3等工具都可以很轻易的发起DDOS攻击/FLOOD攻击/SPOOF攻击等，例如BEACON FLOOD攻击、DEAUTH SPOOF攻击等。这些攻击轻则引起单台AP的信道拥塞，用户体验不佳或频繁掉线，重则可能影响整网AC宕机，影响整网用户使用，不得不防，网络管理员需要能够及时检测出攻击现象并排除Wi-F i攻击。

Wi-Fi攻击示意图

安全雷达

无线AP在提供用户接入服务时，通常工作于固定的信道。传统的WIDS（无线入侵检测）为了实现对射频环境的感知，往往需要全信道切换扫描。这就意味着在切换信道扫描的时候，不可避免的会对当前信道的用户体验造成影响，表现为时延大、丢包率上升。

传统的做法是，单独使用一台AP作为专用的WIDS设备，但这么做无疑又会造成成本的提升。所以当前客户往往为了保证体验而选择关闭 WIDS 功能，这就造成大多数企业无线网络默认情况下不具备无线入侵检测与防御能力，安全风险很大。

安全雷达功能在传统的瘦AP架构下，通过WIS云开启AP端的空口扫描收集数据，并结合认证信息及交换机的相关信息综合分析判断及大数据处理运算，为客户提供安全策略、信号分类、信号定位以及受害终端呈现等安全相关价值，保障无线局域网的安全。

根据Wi-Fi的安全检测类型，我们将Wi-Fi分为以下几类：

■ 钓鱼Wi-Fi

蓄意伪造的钓鱼信号，根据扫描到的信息，SSID与本网一样的私设信号定义为钓鱼Wi-Fi，若BSSID也伪造成合法本网络信号，则进一步比对友好标记位，无友好标记位的也判定为钓鱼Wi-Fi。

■ 疑似钓鱼Wi-Fi

SSID名称与本网络SSID名称非常相近，相似度达到一定阈值（不同安全模式，对应不同的相似度阈值），列为疑似钓鱼AP。

■ 流氓Wi-Fi

指连在本网络有线口的未经授权的私设路由器。第一种方法是AP 根据扫描到的SSID等信息，与有线口的MAC地址表项对比，从相似度判断是否是连在本网络的私设路由器，这种类型一般针对家用路由器。另一种方法是AP 扫描到该SSID下关联的终端MAC地址与交换机网络学习到的终端MAC地址一致，说明该网络连在了有线网上，属于流氓 AP。支持手动添加可信 AP 的信号白名单。

■ 疑似流氓Wi-Fi

指终端已经或曾经连接过本无线网络，并采用360WiFi或猎豹WiFi等软AP放出来的私设WiFi信号。放出该种类型信号的终端很可能当前通过有线连接到了内网，对内网的危害可能比较大。

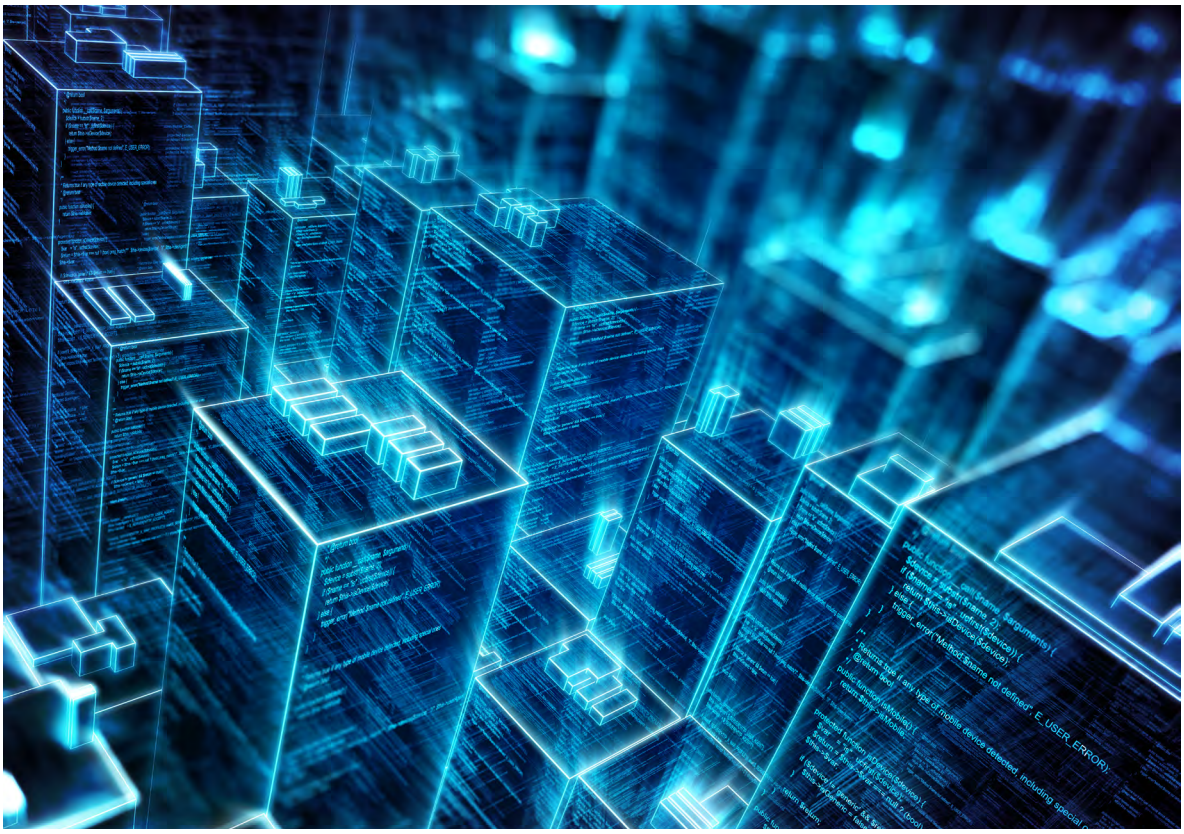
AD-HOC网络：AD-HOC信号和WDS信号可能导致内网信息泄露，根据AD-HOC和WDS的特征进行识别。

■ 干扰Wi-Fi

未能进一步分类的非本网AP，大部分为未接入内网的私设Wi-Fi信号，且又非钓鱼信号，对现网的影响主要是信号干扰及用户体验。根据OUI可进一步区分手机热点和路由器热点等。

■ 信任Wi-Fi

根据厂商OUI、同一SSID扫描到的 AP 数量、在本网络存在的时间等特征区分出该信号可能为邻居合法企业信号。例如公司楼下每天都能扫描到的的 KFC-WiFi。支持手动添加邻居合法AP信号白名单。



云地勘

随着网络设备和规模不断增加，相应的网络复杂度也急剧增加，售前网络地勘规划被越来越多的客户所重视。对于无线网络来说，根据客户实际场景的不同，提前进行地勘规划，能有效的避免设备部署太稀疏导致的信号覆盖不足的问题，以及设备部署太密集导致的信号干扰问题。传统的地勘规划都是通过人工实地勘察，依赖规划人员的个人经验进行点位设计。客户无法感知到地勘规划的点位是否是满足实际的网络覆盖需求。

WIS云地勘是一款基于公有云的网页版的无线网络地勘规划工具，支持多个企业客户同时使用，不同企业客户的地勘规划数据相互隔离。云地勘在无线项目的售前、售后阶段均可使用，在售前阶段，通过信号仿真热图，一键导出仿真报告交付给客户，让客户一目了然确认 AP 型号和数量是否满足覆盖需求；在售后阶段，通过信号仿真支撑概要设计，确定 AP 安装位置和信号覆盖情况。

云地勘界面示意图

WIS云地勘的典型操作步骤：

■ **新建规划**

导入客户提供的图纸（已支持png、jpg、dwg、pdf、bmp等格式）

■ **设置障碍物**

根据现场情况，手动绘制障碍物

■ **放置AP**

■ 根据覆盖需求放置 AP、自动规划和配置信道

■ **查看仿真**

查看场强/信噪比仿真图，确认信号覆盖是否满足要求

■ **导出报告**

导出 Word 版报告，包括热图仿真、物料清单，用于报价或者交付

WIS云地勘的优点：

■ **免安装**

WIS云地勘部署在公有云上，企业客户只需具备上网条件，无需购买和安装软件。

■ **全场景**

支持室内、室外、智分、高密度等全场景的热图仿真。

■ **数据安全**

数据云端保存，不怕数据丢失，随时随地导出报告。

■ **高质量**

支撑上万台AP规模的无线项目，质量值得信赖。

■ **多人协作**

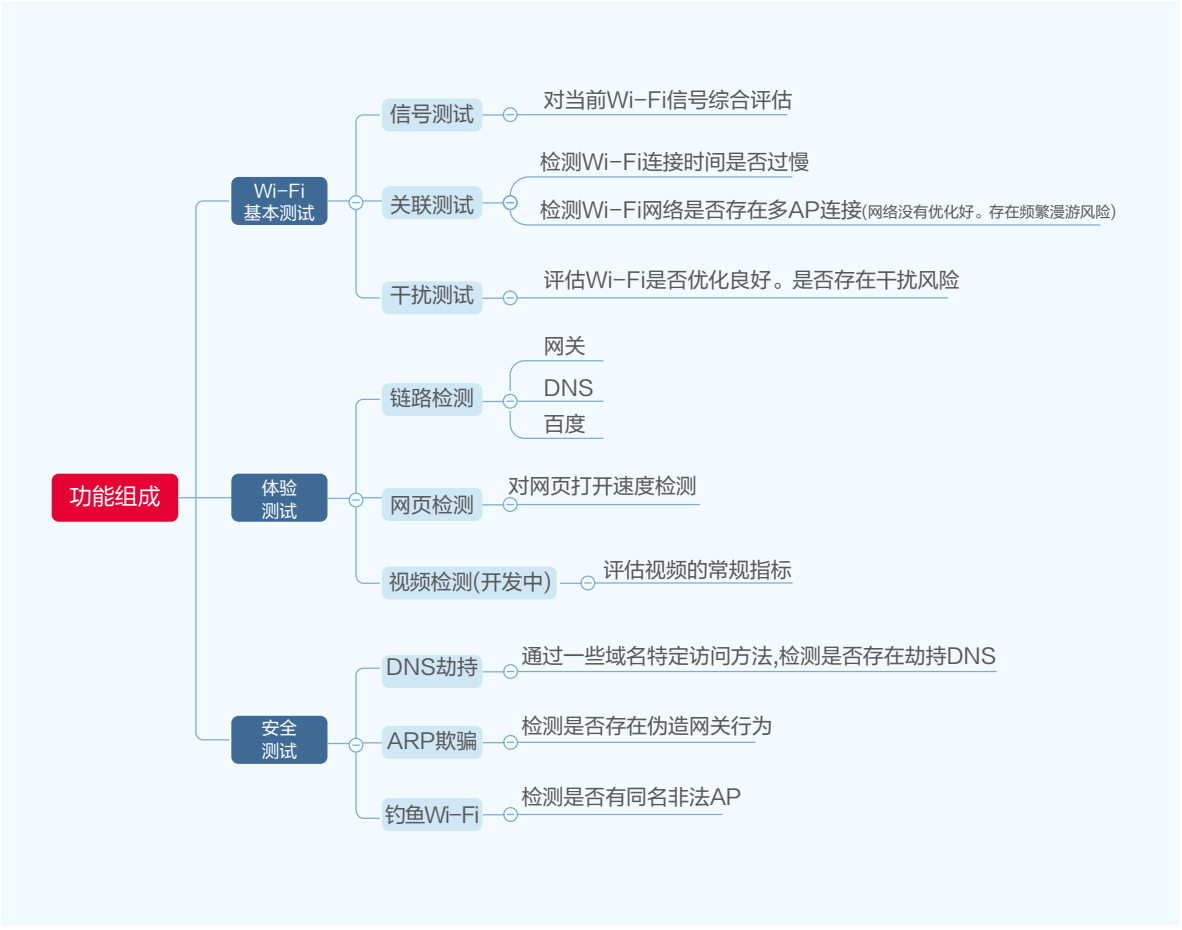
通过规划共享，支持多人协作一起地勘规划，数据实时同步。

Wi-Fi魔盒一键检测

在无线项目的验收、运维阶段中，网络工程师一般都是携带自己的笔记本电脑进行无线环境的勘查和检测的。一般情况下，无线项目覆盖的范围跨度比较大，工程师不可避免地需要携带笔记本电脑到处走，显得异常的笨重，增加了额外的工作负担。随着移动智能手机/平板的普及，通过手机APP来实现无线检测的需求就变得越来越强烈。

Wi-Fi魔盒APP就是解决这个强烈的需求而诞生的手机端运行的可测试Wi-Fi的应用软件。一键检测工具：针对运维阶段的场景，普通用户可以通过一键检测工具进行全面的Wi-Fi检测，根据最终的检测结果了解Wi-Fi网络的好坏以及如何解决问题。如果有网络运维人员，用户还能方便地分享检测结果给运维人员，帮助运维人员定位网络问题。

Wi-Fi魔盒一键检测支持的检测项目：



考虑到一键检测用户群体的技术水平和使用目的不同，一键检测功能提供简化版和专业版两种页面。

优先展示的是简化版页面，提供最重要的几项网络指标结果。对于可以展开的子项，例如Wi-Fi干扰、在线终端，这两项都是可以点击展开的。Wi-Fi干扰可以跳转工具箱的看干扰功能查看干扰详情；在线终端可以弹窗显示在线终端扫描结果列表。

简化界面支持的功能	说明
Wi-Fi的SSID、厂商名称和厂商LOGO	如果BSSID查OUI表没找到，则使用魔盒默认LOGO
信号强度	显示平均值并做出简要评价（强、一般、差）
Wi-Fi干扰	根据扫描的同频和邻频的信号个数以及强度来衡量干扰严重程度（无干扰、少干扰、干扰严重），点击可以展现详细干扰图。
网速	基本的下行速率具体值
安全等级	根据安全检测项的检测结果进行概括
在线终端	显示同网段终端数目，点击可以查看同网段终端列表。

在简化版的结果页面提供查看详情的跳转按钮，用来查看详细信息，提供各个测试项的具体结果，以及相应的优化建议。

魔盒界面示意图

平台安全

用户数据、业务系统、网络系统等面临着来自线下及线上的各种安全威胁挑战，WIS云网在云、管、端多方面都做了充分安全防护，通过积极主动的安全措施，保障企业用户的网络安全和数据隐私。

平台安全可靠

- 平台上的租户之间相互隔离，除非把账号添加到租户内作为子账号，否则其他租户的都用户无法访问到租户内的任何设备、配置、用户等数据。
- 平台侧使用kerberos安全认证技术，外包连接要访问平台中的数据必须有凭据，保障数据安全。
- 平台会定期邀请白帽子做渗透测试，监控互联网中的安全漏洞及风险，第一时间修复。
- 平台提供角色提供完善的角色和权限功能，保证不同用户可以访问到恰当的数据和设备。
- 平台提供完整的安全审计功能，对于用户的关键操作都能进行完整的审计和回溯。
- 平台使用高可用集群架构，即使出现部分磁盘或服务器故障，也不会导致数据丢失或服务中断。

隐私保护

- 在平台端，用户所有的安全隐私信息，如密码等，都使用MD5加密存储和密文传输，任何人都不会拿到用户的管理密码。
- 未经许可，平台不会泄露任何网络和用户数据给第三方。

访问安全

- 平台使用HTTPS安全协议访问。
- 设备与平台之间的管理通道都使用认证、加密、证书等多重安全机制保护。
- 不管是设备端还是平台侧，都不会预留后门账号。除为用户提供的唯一账号外，在设备出厂后不应以任何形式在设备中预留任何其他账号。
- 访问口令支持足够复杂的策略，口令应满足至少8位长度要求，且包含字符、数字和特殊字符等。
- 设备默认禁用SSH和telnet等远程管理协议，包括标准和非标准端口的SSH和telnet协议。如在特殊情况下需要打开SSH和telnet远程管理协议，要求满足账户口令验证措施，不应出现空口令或弱口令登录的情况。
- 控制与转发分离，线下业务数据不需要绕行到公有云的平台，直接到达本地目的地，实现业务数据的安全隔离。

平台开放

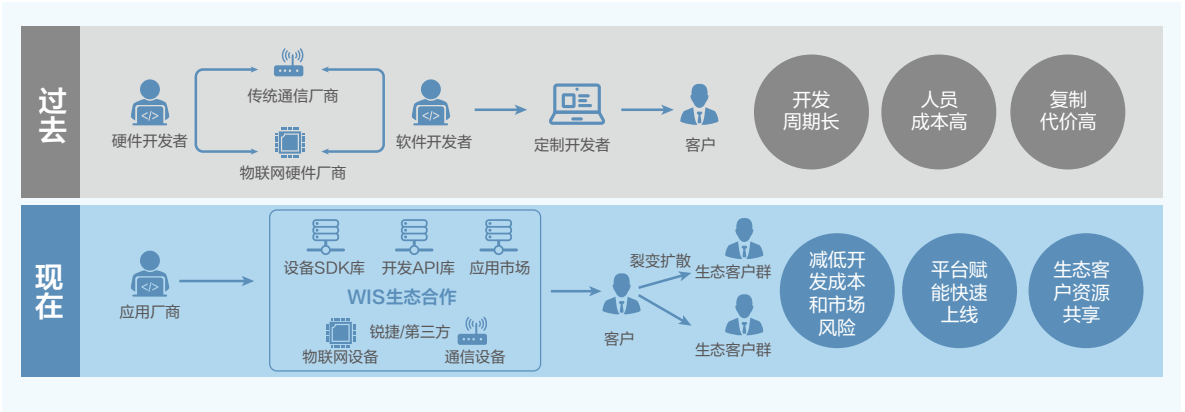
网络作为业务的底座，和上层业务系统是密不可分的，开放的网络平台可以为上层业务进行赋能。WIS云网提供一个开放的云平台，秉持能力共享，开放共赢的原则，在安全合规的前提下把平台的数据和能力赋予客户或合作伙伴，达到网络价值的最大化。

平台开放的应用场景，包括：

- 客户希望构建自运营平台去管理运维网络业务。
- 客户希望能把网络系统对接到自己的业务系统中，支撑业务的数字化流程。
- 合作伙伴基于网络数据API 开发上层增值业务。
- 合作伙伴或客户希望把第三方设备快速接入到云平台中管理或进行数据透传。

WIS云网基于标准化的HTTP RESTFULAPI、MQTT等接口格式，提供了组织结构、设备监控、终端体验、终端位置、应用行为、上网认证、网络编排管理等北向接口，可以支持对接第三方业务系统或开发增值应用，满足客户的运营、管理维护、科研分析等需求。

对于合作伙伴，WIS云网支持以定制的方式接入第三方的设备，实现第三设备的快速接入。可以大大降低开发成本和市场风险，上线效率更高。



生态合作示意图

典型应用

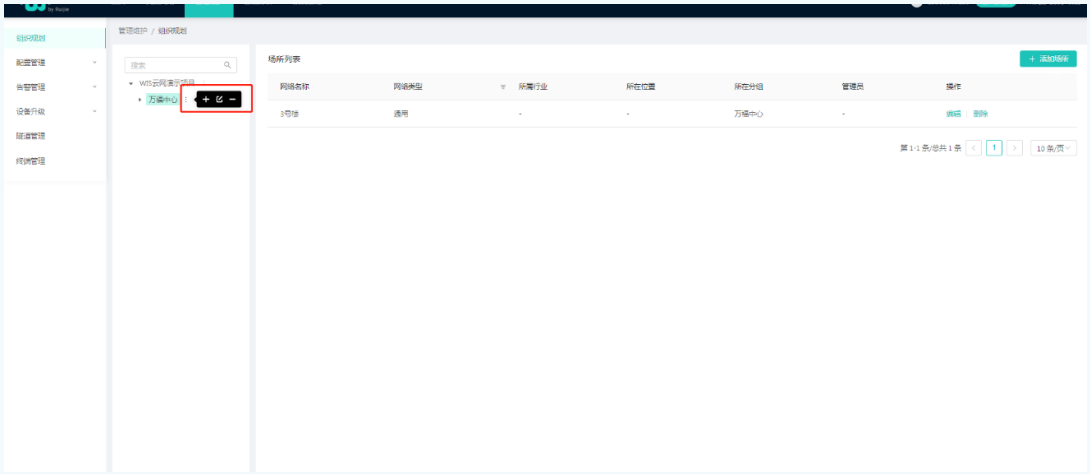
极简开局

新建网络项目可通过web端和移动端两种方案实现极简开局，小规范网络推荐使用移动端极简开局进行单点开局降低门槛，大规模连锁门店网络推荐使用web端极简开局，提高效率。

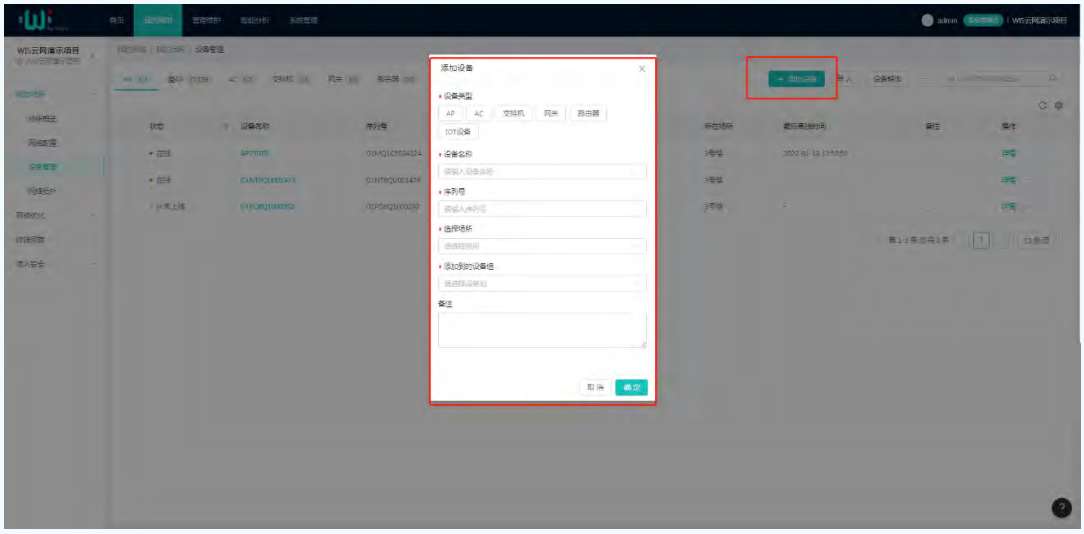
WEB端极简开局

登录WIS官网（https://wis.ruijie.com.cn），注册账号（如果已有WIS账号，无需注册）

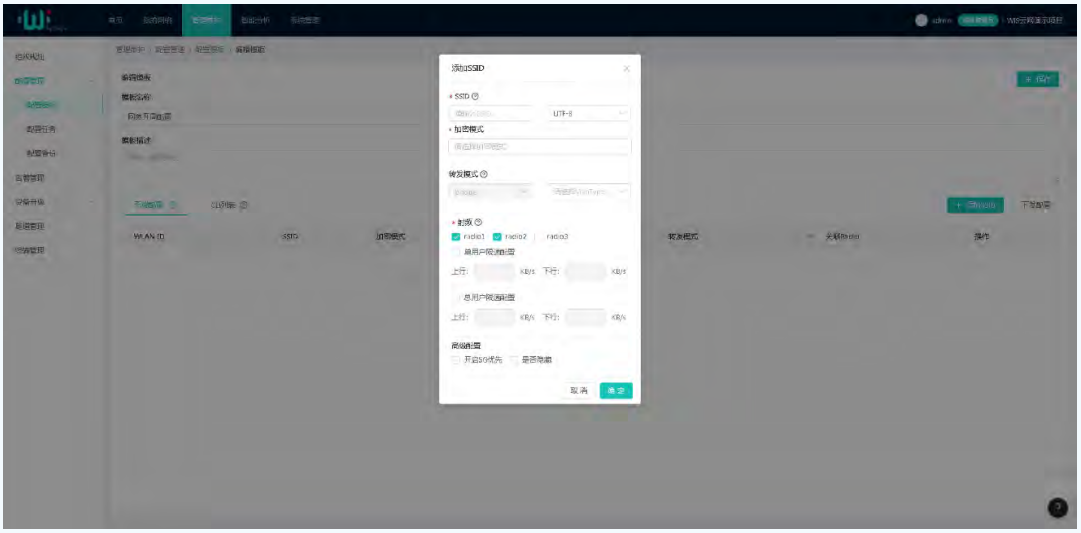
· 在管理维护的组织规划菜单中，按实际情况创建好网络各分支结构。



· 然后通过添加或者批量导入设备序列号的方式添加设备



· 创建好配置模板并应用到相关场所



· 设备上电，并接入WIS云平台后，设备会自动获取配置，AP放出无线信号

移动端极简开局

①. 打开“小锐云网”App（通过各移动端应用商店下载）并登录，登录成功后进入APP首页。

②. 点击首页顶部极简开局模块，进入极简开局。

③. 点击“我准备好了”，进入“连接Wi-Fi”页面。

④. 点击“去连接”按钮，跳转到系统Wi-Fi列表页面，选择正确Wi-Fi进行连接。

⑤. 点击“开始配置”按钮，进入“项目配置”页面。

⑥. 在“项目配置”页面中可以根据自己的需求选择配置Wi-Fi信号、修改管理密码、快速网优功能。

⑦. 点击右上角完成按钮，即可完成项目配置。

终端接入故障诊断

某用户多次尝试接入无线网络失败使用WIS云网诊断过程如下所示：

· 在WIS云网的终端详情页面（在智能分析中搜索终端MAC进入）查询该用户的关联详情，提示1X认证失败

· 查看终端接入协议回放，提示1x认证失败

· 进一步查询1x服务器认证日志，发现是密码输入错误导致认证失败，问题定位；

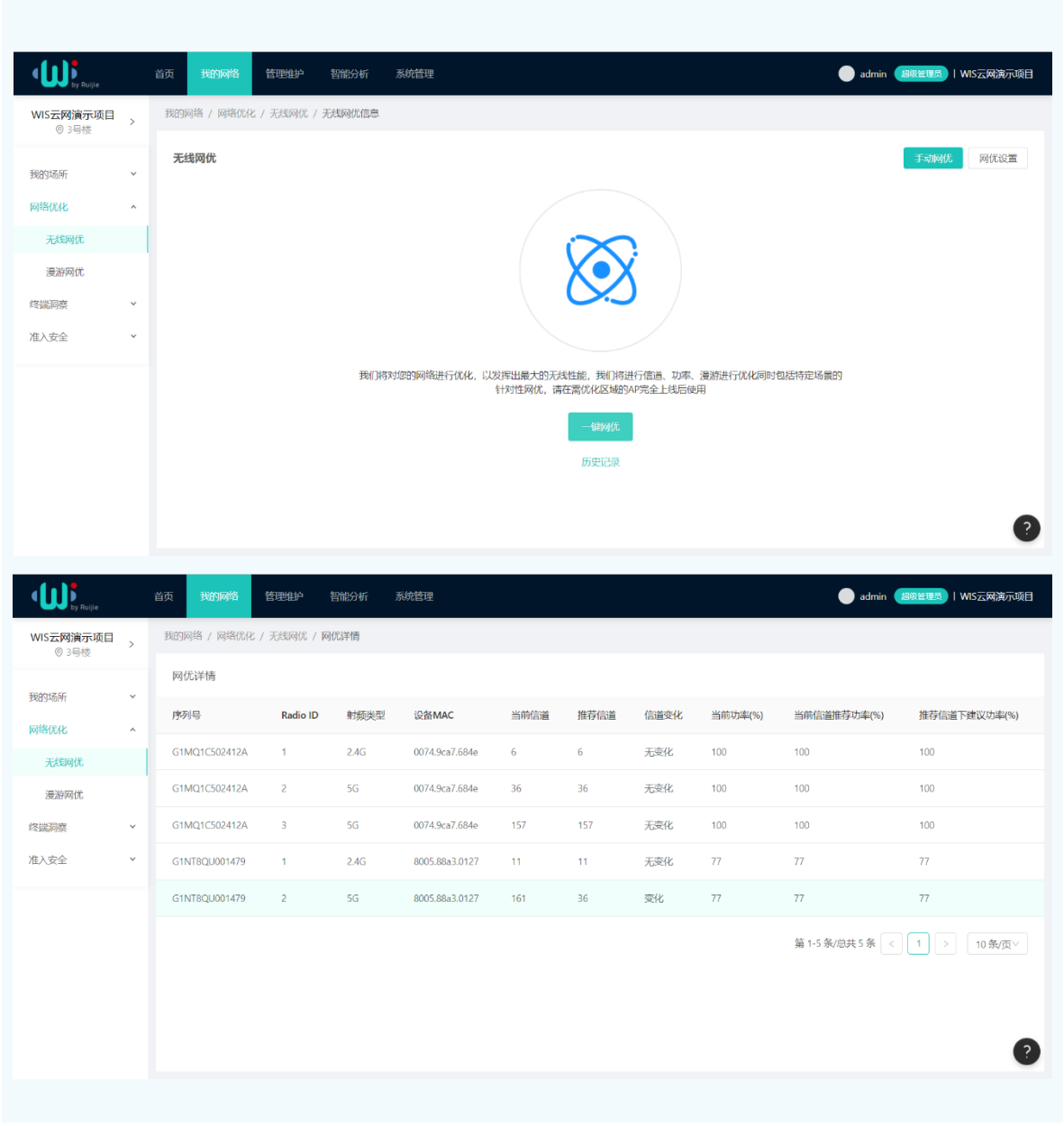
无线网优

无线网络在开局实施完成后，网络的无线参数都是默认的（如有的AP信道一样，功率默认100%运行），为了达到最佳的无线使用体验，需要对无线网络进行优化，可以使用智能分析的无线网优功能进行优化；根据网络组网方式的不同，可以分为云AP模式的网优和本地AC+ 瘦AP模式的网优；

云AP模式网优

通过收集场所中AP扫描所得的空口信息，对设备的信道和功率进行自动规划，可以发挥出最大的无线性能。

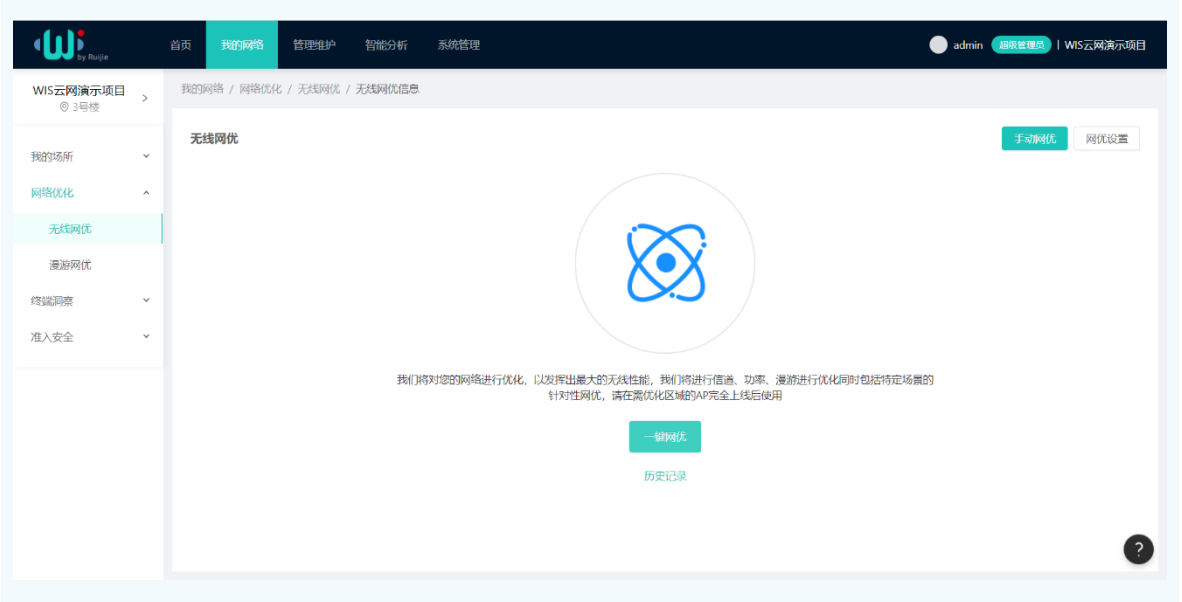
进入“我的网络->无线网优”，点击一键网优后即开始网优，网优过程15-30分钟，网络结束后，查看网优结果，从网优结果可以发现相邻AP的信道错开，功率不再100%运行。



本地AC模式网优

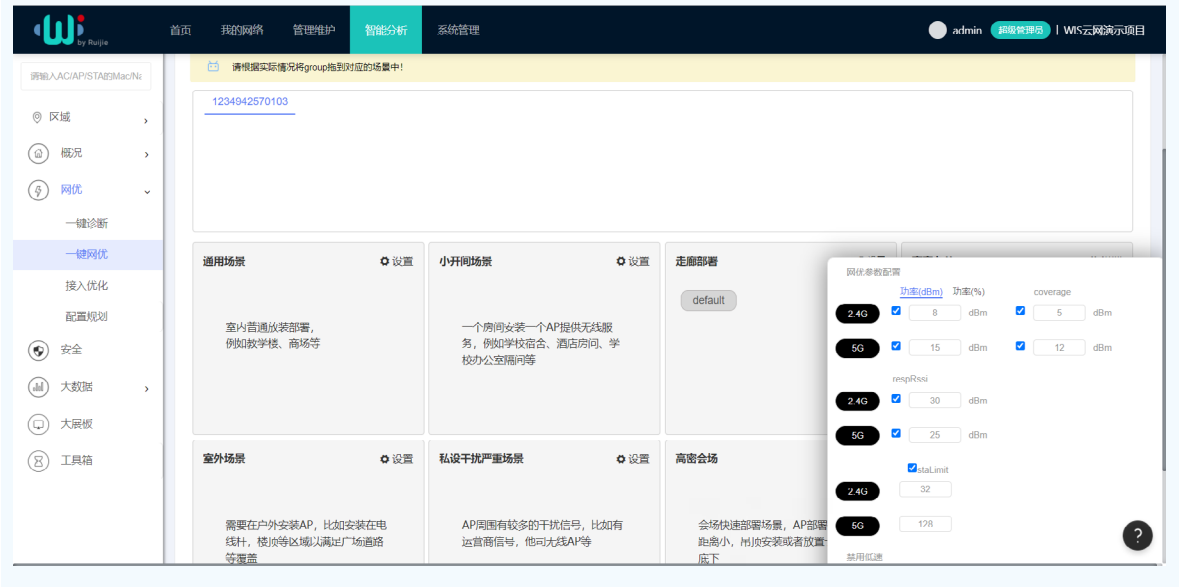
■ 信息完整性检查

在“智能分析”->“网优”->“一键网优”中开始网优，会开始检查网优所需的信息，如版本号、型号、分组信息等是否完整，如果不完整，可点击“更新分组信息”来主动收集。



选择场景

下一步可以选择场景进行针对性优化。WIS云网提供了7种常见的无线覆盖场景，你只需根据实际情况，将AP分组拖动到对应场景中即可。



每个场景的背后，实际上是基于海量项目提炼出来的一套配置模型，源于专业人员的宝贵经验。只要AP的点位规划和工程实施没有硬伤，按场景模型推理出的配置基本没问题。如果没有匹配的场景，或者IT人员对自己负责的场景非常熟悉，也可以在WIS上自定义一个场景，人为设定各种参数。

深度体检（扫描阶段）

选择场景后，就要正式进入扫描阶段了，这个步骤一旦开始就不能停止或回退。接下来的40分钟时间里，WIS云网的网优引擎会调度AC、AP扫描收集空口数据，生成优化方案，再直接推送到设备，全程不再需要人工参与。

Ruijie Networks 锐捷

锐捷网络股份有限公司

欲了解更多信息，欢迎登录www.ruijie.com.cn，咨询电话：400-620-8818